YSOFT SAFEQ Cloud®

YSOFT SAFEQ CLOUD DOCUMENTATION

Y SOFT CORPORATION

SAFEQ.COM

CONTENT

1	**About this document**	**9**
1.1	**Styles**	**9**
1.2	**Infoboxes**	**9**
2	**Terms and Definitions**	**10**
3	**Personas and roles**	**11**
4	**Release notes**	**12**
4.1	**2025**	**12**
4.1.1	2025.07.10	12
4.1.2	2025.06.26	13
4.1.3	2025.06.12	13
4.1.4	2025.05.29	15
4.1.5	2025.05.15	16
4.1.6	2025.04.30	16
4.1.7	2025.04.17	18
4.1.8	2025.04.03	19
4.1.9	2025.03.20	21
4.1.10	2025.03.06	22
4.1.11	2025.02.20	23
4.1.12	2025.02.06	24
4.1.13	Build 2025.01.23	25
4.2	**2024**	**29**
4.2.1	Build 2024.11.28	29
4.2.2	Build 2024.11.14	33
4.2.3	Build 2024.10.31	34
4.2.4	Build 2024.10.17	36
4.2.5	Build 2024.10.03	37
4.2.6	Build 3.49 [2024-09-19]	38
4.2.7	Build 3.48 [2024-08-22]	40
4.2.8	Build 3.47 [2024-07-25]	42
4.2.9	Build 3.46 [2024-06-27]	44
4.2.10	Build 3.45 [2024-06-11]	45
4.2.11	Build 3.44 [2024-05-09]	47
4.2.12	Build 3.43 [2024-04-04]	48
4.2.13	Build 3.42 [2024-03-07]	49
4.2.14	Build 3.41 [2024-02-08]	50
4.2.15	Build 3.40 [2024-01-15]	51
4.3	**2023**	**53**

4.3.1	Build 3.39.7 [2023-12-01]	53
4.3.2	Build 3.39.5 [2023-11-27]	53
4.3.3	Build 3.39.3 [2023-11-24]	53
4.3.4	Build 3.39 [2023-11-02]	53
4.3.5	Build 3.38 [2023-10-05]	55
4.3.6	Build 3.37 [2023-09-07]	56
4.3.7	Build 3.36 [2023-08-10]	58
4.3.8	Build 3.35.2 [2023-07-25]	58
4.3.9	Build 3.35.1 [2023-07-19]	58
4.3.10	Build 3.35 [2023-07-13]	58
4.3.11	Build 3.34 [2023-06-26]	59
4.3.12	Build 3.33 [2023-05-18]	61
4.3.13	Build 3.32 [2023-04-25]	62
4.3.14	Build 3.31 [2023-03-25]	63
4.3.15	Build 3.30 [2023-03-01]	63
4.3.16	Build 3.29 [2023-02-03]	64
4.3.17	Build 3.28.2 [2023-01-16]	65
4.4	**2022**	**65**
4.4.1	3.28 [2022-12-15]	65
4.4.2	3.27.3 [2022-10-08]	66
4.4.3	3.27 [2022-10-06]	66
4.4.4	3.26.1 [2022-09-30]	67
4.4.5	3.26 [2022-09-08]	67
4.4.6	3.25 [2022-08-04]	67
4.4.7	3.24.1 [2022-07-22]	68
4.4.8	3.24 [2022-07-12]	68
4.4.9	3.23.1 [2022-06-16]	69
4.4.10	3.23 [2022-06-08]	69
4.4.11	3.22.1 [2022-05-20]	69
4.4.12	3.22 [2022-05-12]	69
4.4.13	3.21 [2022-04-05]	70
4.4.14	3.20 HP Workpath Release Only [2022-03-17]	71
4.4.15	3.20 [2022-03-08]	71
4.4.16	3.19.1 [2022-02-11]	72
4.4.17	3.19 [2022-02-04]	72
4.5	**2021**	**73**
4.5.1	3.18.4 [2021-12-21]	73
4.5.2	3.18.3 [2021-12-16]	74
4.5.3	3.18.2 [2021-12-11]	74
4.5.4	3.17.2 [2021-11-19]	74
4.5.5	3.17.1 [2021-11-11]	75

4.5.6	3.17 [2021-11-04]	75
4.5.7	3.16 [2021-10-13]	75
4.5.8	3.15.5 [2021-09-23]	77
4.5.9	3.15.4 [2021-09-09]	77
4.5.10	3.15.0 [2021-09-03]	77
4.5.11	3.14.0 [2021-05-17]	79
4.5.12	3.13.0 [2021-04-08]	79
4.5.13	3.12.0 [2021-03-11]	80
4.5.14	3.11.0 [2021-02-06]	81
4.6	**2020**	**81**
4.6.1	3.10.0 [2020-11-27]	82
4.6.2	3.9.0 [2020-10-13]	82
4.6.3	3.8.0 [2020-09-09]	82
4.6.4	3.7.0 [2020-08-06]	83
4.6.5	3.6.0 [2020-07-07]	83
4.6.6	3.5.0 [2020-06-09]	83
4.6.7	3.4.0 [2020-04-20]	84
4.6.8	3.3.0 [2020-03-10]	84
4.6.9	3.2.0 [2020-02-07]	85
4.7	**2019**	**85**
4.7.1	3.1.2 [2019-12-13]	85
4.7.2	3.1.1 [2019-12-03]	86
4.7.3	3.1.0 [2019-11-19]	86
4.7.4	3.0.3 [2019-10-07]	87
4.7.5	3.0.2 [2019-09-20]	87
4.7.6	3.0.1 [2019-07-01]	87
4.7.7	3.0.0 [2019-06-29]	87
4.7.8	2.5.9 [2019-05-28]	89
4.7.9	2.5.7 [2019-04-10]	89
4.7.10	2.5.6 [2019-03-29]	89
4.7.11	2.5.5 [2019-03-13]	89
4.7.12	2.5.4 [2019-02-28]	89
4.7.13	2.5.3 [2019-02-25]	89
4.7.14	2.5.2 [2019-02-25]	90
4.7.15	2.5.1 [2019-02-24]	90
4.7.16	2.5.0 [2019-02-13]	90
4.8	**2018**	**91**
4.8.1	2.4.1 [2018-11-07]	91
4.8.2	2.4.0 [2018-11-05]	91
4.8.3	2.3.3 [2018-09-17]	92
4.8.4	2.3.2 [2018-09-05]	92

4.8.5	2.3.0 [2018-08-30]	92
4.8.6	2.2.2 [2018-06-05]	93
4.8.7	2.2.1 [2018-06-04]	93
4.8.8	2.2.0 [2018-05-29]	93
4.8.9	2.1.0 [2018-02-19]	94
4.8.10	2.0.1 [2018-01-24]	94
5	**About SAFEQ Cloud**	**95**
5.1	**What is SAFEQ Cloud**	**95**
5.2	**Why SAFEQ Cloud**	**95**
5.3	**Architecture and solution design**	**96**
5.3.1	Introduction	96
5.3.2	Architecture	96
5.3.3	Hosting	112
5.3.4	User identity	112
5.3.5	Availability, security	113
5.3.6	Limitations	113
5.4	**Security and privacy**	**116**
5.4.1	Document Scope and Use	116
5.4.2	Y Soft Security and Risk Focus	116
5.4.3	The Shared Security Responsibilities	121
5.4.4	Y Soft product infrastructure	123
5.4.5	OMNI Bridge security and privacy	125
5.5	**Compatible Card Readers**	**127**
5.6	**Supported languages**	**128**
5.6.1	UI and applications	128
5.6.2	Cloud Terminals	130
5.6.3	Embedded Terminals	133
5.7	**Y Soft hosted cloud addresses**	**135**
5.7.1	EU region (*.eu.ysoft.cloud)	136
5.7.2	EU Central region (*.eu-central.ysoft.cloud)	136
5.7.3	UK region (*.uk.ysoft.cloud)	136
5.7.4	DE region (*.de.ysoft.cloud)	137
5.7.5	US region (*.us.ysoft.cloud)	137
5.7.6	CA region (*.ca.ysoft.cloud)	137
5.7.7	AP region (*.ap.ysoft.cloud)	138
5.7.8	AU region (*.au.ysoft.cloud)	138
5.8	**Trademarks**	**138**
5.9	**Known Issues and Limitations**	**140**
5.9.1	SAFEQ Cloud Known Issues and Limitations	140
5.9.2	Embedded Applications	145
5.10	**Requirements**	**149**

5.10.1	Supported Clients	149
5.10.2	Supported Printers	150
5.10.3	Ports and Protocols	151
5.11	**Licensing**	**162**
5.11.1	Tenant license expiration	162
6	**Quick start for vendors**	**163**
6.1	**Creating a new tenant (customer)**	**163**
6.1.1	Editing the invitation message	165
7	**Quick start for admins**	**167**
7.1	**Prerequisites**	**167**
7.2	**Configuring authentication**	**167**
7.2.1	Example: Setting up Microsoft Entra authentication using the built-in OIDC	167
7.3	**Adding a print queue**	**168**
7.4	**Adding an MFD**	**169**
7.5	**Installing SAFEQ Cloud Client**	**169**
7.6	**Mobile printing**	**171**
7.7	**Releasing a print job at the MFD**	**172**
7.8	**Configuring a password policy**	**172**
7.9	**Gateways (edge devices)**	**172**
8	**Admin guide**	**173**
8.1	**SAFEQ Cloud Web UI**	**173**
8.1.1	Navigation	173
8.1.2	Users menu	173
8.1.3	Printers menu	284
8.1.4	Scan workflows	580
8.1.5	Reports	617
8.1.6	Security section	619
8.1.7	Settings section	647
8.1.8	Services	709
8.1.9	Search functionality	714
8.1.10	Notifications	716
8.1.11	Creating a cloud status widget	716
8.1.12	Overview	719
8.1.13	Installation files	722
8.2	**SAFEQ Cloud Client**	**722**
8.2.1	SAFEQ Cloud Client overview	723
8.2.2	System requirements	725
8.2.3	Installing SAFEQ Cloud Client on macOS	725
8.2.4	Installing SAFEQ Cloud Client in offline mode	735
8.2.5	SAFEQ Cloud Client configuration	735
8.2.6	SAFEQ Cloud Client authorization	740

8.2.7	SAFEQ Cloud Client log download	741
8.2.8	SAFEQ Cloud Client Auto update	742
8.2.9	SAFEQ Cloud Client Upgrade	743
8.2.10	SAFEQ Cloud Client troubleshooting	747
8.2.11	Universal driver settings	748
8.2.12	SAFEQ Cloud Client proxy support	750
8.2.13	SAFEQ Cloud Client Configuration profiles	750
8.2.14	Windows Protected Print mode	753
8.2.15	Installing SAFEQ Cloud Client on Windows	755
8.3	**Gateway Guide**	**766**
8.3.1	Different Gateway options	766
8.3.2	Secondary Gateways Metrics Collection	767
8.3.3	YSoft OMNI Bridge	768
8.3.4	Add a secondary gateway server	791
8.3.5	Gateway on Hardware Appliance	793
8.3.6	Gateway on Software Appliance	793
8.3.7	Configuring a pre-configured gateway	800
8.4	**SAFEQ Cloud Chrome extension**	**807**
8.4.1	Overview	807
8.4.2	System requirements	807
8.4.3	Installation	807
8.4.4	Configuration	808
9	**End user guide**	**817**
9.1	**Submitting a print job**	**817**
9.1.1	Using the SAFEQ Cloud Client	817
9.1.2	Using the Mobile app	819
9.1.3	Using the legacy Mobile app	844
9.1.4	Using the SAFEQ Cloud Chrome Extension	859
9.1.5	Adding IPP print queue manually in Windows	863
9.1.6	Adding IPP print queue manually in Mac OS	867
9.1.7	Printing from SAP	872
9.2	**Using an MFD**	**872**
9.2.1	Card registration at the MFD	873
9.2.2	Using FUJIFILM BI Cloud Terminal	874
9.2.3	Using HP Workpath Gen 2 Cloud Terminal	879
9.2.4	Using Konica Minolta IWS Gen 2 Cloud Terminal	883
9.2.5	Using Ricoh Standard Gen 2 Cloud Terminal	895
9.2.6	Using Sharp Gen 2 Cloud Terminal	905
9.2.7	Using Xerox Gen 2 Cloud Terminal	910
9.3	**SAFEQ Cloud Web UI for end users**	**918**
9.3.1	Registering as a standard user	918

9.3.2	Registering as a guest	920
9.3.3	My profile	924
9.3.4	My documents	930
9.3.5	Reseting forgotten password	933
10	**Reference documents**	**937**
10.1	**Asian fonts support for direct print**	**937**
10.1.1	Solution for CentOS (RHEL)	937
10.2	**Asian fonts support for MS Office documents converted to PDF**	**938**
10.2.1	Solution for CentOS (RHEL)	939
10.3	**Migration of authentication providers and SSO to port 443**	**939**
10.3.1	Microsoft Entra ID	940
10.3.2	Okta	944
10.3.3	PingId	946
10.4	**Install KM Cloud Terminal without MarketPlace**	**946**
11	**Legacy documentation**	**951**
11.1	**Technical Introduction**	**951**
11.1.1	The concept of services	951
11.1.2	Servers	952
11.1.3	Account Types	953
11.1.4	Domain names	953
11.2	**How to..**	**954**
11.2.1	Configure a primary server cluster	954
11.2.2	Integrate Mobile Print for SAFEQ Cloud	961
11.2.3	Scan To Mail	965
11.2.4	How to check VID and PID on cardreader	1015
11.2.5	Use Equitrac embedded clients with SAFEQ Cloud	1019
11.2.6	Containers and access controls	1022
11.2.7	Connect to Azure SSL enabled Postgresql database	1028
11.2.8	Deploy SAFEQ Cloud Client using Microsoft Intune	1031
11.2.9	Configure MDM Airprint integration on Microsoft Intune	1034
11.2.10	Disaster Recovery Procedure For Primary Server	1046
11.2.11	Configure Scan to My Email	1047
11.2.12	Use Network connected card readers	1049
11.2.13	Create Print queues with specific output options	1057
11.2.14	Migrate SAFEQ Cloud bundled PostgreSQL database to external PostgreSQL database	1060
11.2.15	Card enrollment / self-registration	1063
11.2.16	Use your own domain names for SAFEQ Cloud hosted accounts	1067
11.2.17	Configure SAFEQ Cloud environment with trusted certificates	1067
11.2.18	Configure denial of service filtering for web UI	1070

1 ABOUT THIS DOCUMENT

1.1 STYLES

To make the reading of this guide easier, different styles and fonts are used.

Bold style is used to mark elements from the GUI, e.g. "Click **OK**."

Italic style is used to refer to a specific section of the guide, e.g. "...see section *Terms and definitions."*

`Monospace` style is used for paths, keyboard inputs, and code quotations.

1.2 INFOBOXES

Tip – a piece of information that you might find helpful.

Info – additional information which can help you to understand the product or the context better but which isn't necessary to perform the given procedure.

Note – a piece of information that shouldn't escape your attention, such as important settings or limitations.

Warning – warning about a critical situation, such as a security threat risk or a risk of data loss.

2 TERMS AND DEFINITIONS

Term	Description
SAFEQ Cloud	A cloud-based print management service.
Gateway/Edge device	A local device, such as Y Soft OMNI Bridge, installed at the customer site. This device provides site services and serves as a bridge between local users, devices, and SAFEQ Cloud.
YSoft OMNI Bridge	YSoft OMNI Bridge is a piece of hardware manufactured by Y Soft.
Pure Cloud printing	A service with architecture (printing method) based on MFDs that support pure cloud terminals. This scenario does not require edge devices.
Edge printing	A service with architecture (printing method) based on MFDs using standard embedded terminal technology which can connect to a local Edge device (providing site services). Suitable for situations where Pure Cloud printing is unavailable or not wanted (for example, if customers want to keep print job data local to their network, or they have a wider portfolio of devices than is supported by SAFEQ Cloud pure cloud terminals).
MFD	Multi-function device (a copier).
SFD	Single-function device (a printer).
SAFEQ Cloud Web UI	A web interface used by partner admins to create customers (tenants) in SAFEQ Cloud and by customer administrators to manage their tenants centrally.

3 PERSONAS AND ROLES

Persona	Description
Managed Service Provider (MSP)	The role with the highest set of privileges in the SAFEQ Cloud service, responsible for service availability and maintenance. Has access to all customer settings. Is responsible for SAFEQ Cloud web UI maintenance, monitoring, deployment of updates etc.
Partner	A partner of MSP. It can also be a reseller (a partner of a partner).
Customer	The customer of a partner and, at the same time, a representation of the customer in SAFEQ Cloud Web UI. This representation is sometimes called Tenant. Each Customer has its own admin. This can be the partner admin or the customer admin.
Partner admin	An administrator in the SAFEQ Cloud Web UI who can (if agreed with the customer) manage settings in SAFEQ Cloud Web UI on customer's behalf.
Customer admin	An administrator on the customer side with rights to manage settings in SAFEQ Cloud Web UI.
End user	A persona within a Customer's SAFEQ Cloud instance that is permitted to print/copy/scan.

4 RELEASE NOTES

The following pages contain a list of notable changes in YSoft SAFEQ Cloud.

4.1 2025

4.1.1 2025.07.10

Legend:

- Added feature
- Improved/changed feature
- Bug fixed

PC Client

PC Client installer now blocks shutdown, sleep, hibernation, or restart while an update is running, ensuring your installation completes reliably. (HCP-14812)

Web UI

%deviceDescription% now returns the actual device description instead of the generic "Printer" value when the variable is used in scan workflows. (HBT-5433)

New reporting features (Beta) now available for all customers in the Singapore cluster

Xerox Gen 2Cloud Terminal

Terminal Deployment Tool uninstall for Xerox now either omits the -k flag when it isn't needed or correctly populates it as -k restore in kiosk mode. Making sure application access is automatically restored (or no invalid flag is passed) after uninstall. (HBT-5040)

Konica Minolta Gen 2 Cloud Terminal

Konica Minolta Gen 2 Cloud Terminal now processes very large batches of print jobs in smaller, managed requests, mitigating "Failed to fetch" errors on login or risk of memory issues on the device. (HBT-5392)

HP Gen 2 Cloud Terminal

Scanning workflows now display the full workflow names instead of truncating them. (HBT-5164)

Ricoh Gen 2 Cloud Terminal

⚠ Terminal now displays a clear "network unavailable" error if network connection is lost during a print job and correctly times the session out. (HBT-4169)

⚠ Job timestamps now display correctly on the terminal when the MFD is set to a later time zone (e.g., GMT-5), regardless of the device's locale. (HBT-4998)

⚠ Terminal now gracefully handles card swipes on a sleeping MFD. (HBT-5398)

⚠ Terminal no longer loses its registration. (HBT-5523)

4.1.2 2025.06.26

Legend:

✔ Added feature
ℹ Improved/changed feature
⚠ Bug fixed

Sharp Gen 2 Cloud Terminal

✔ There is a new option to "**Enable numeric keypad for PIN entry**" at the terminal template. When enabled, it will show numeric keypad for PIN input field at the terminal, instead of alphabetical one. (HCP-14767)
This new option will become effective with new version of **Sharp Cloud Terminal 2025.07.01**.

KM IWS Gen 2 Cloud Terminal

✔ Added the option to show or hide the Cloud/Native Copy/Scan application quick action. (HCP-14767)
These new options will become effective with new version of **KM IWS Cloud Terminal 2025.07.01**.

Web UI

ℹ Improved localization of PC client auto-update page. (HBT-5474)

⚠ The overview page no longer displays an alert about "PC Clients with storage mode set to 'Cloud Storage' won't be able to print using Instant print and Mobile print". (HBT-5509) (also hotfixed)

PC client

⚠ PC client now correctly authenticates using OAuth 2.0 (e.g. with OKTA) also when connected to a gateway. (HBT-4968)

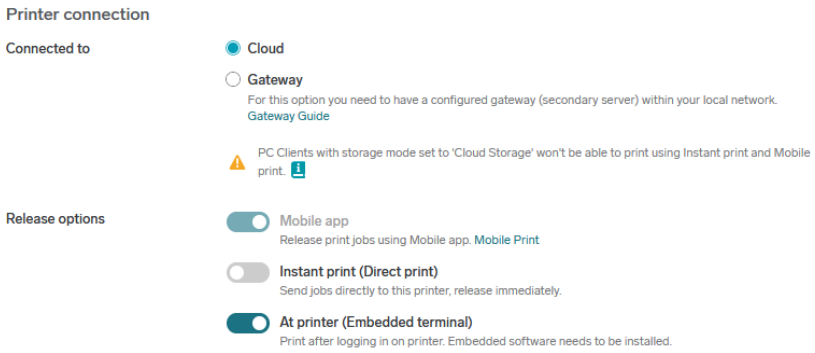
4.1.3 2025.06.12

Legend:

✅ Added feature
ℹ️ Improved/changed feature
⚠️ Bug fixed

Web UI

ℹ️ Adding printers was reworked for better experience. (HCP-14572)



⚠️ Minimal PIN length is now respected and can be lower than 6. (HBT-5454)

Xerox Gen 2 Cloud Terminal

⚠️ Sending large amount of individual scan jobs no longer causes some to fail to deliver. (HBT-5453)

Konica Minolta Gen 2 Cloud Terminal

✅ Added the option to show or hide the Cloud/Native Copy/Scan application quick action. (HCP-14724)

⚠️ Automatic logout timeout now resets with typing or scrolling. (HBT-5441)

Printing

⚠️ Direct offline print is no longer changed when user profiles are applied - it keeps its value. (HBT-5424)

Authentication

⚠️ Built-in OIDC Web UI authentication is now available also on secondary gateway. (HBT-5039)

⚠️ Guest users are now able to use the Mobile App also when SAML SSO is enabled. (HBT-5425)

Upgrading of customer-hosted environments

⚠ When upgrading to version 2025.06.12 from any prior release, manual database-level actions are required. For detailed procedure, please contact Technical Support.

4.1.4 2025.05.29

Legend:

✅ Added feature
ℹ Improved/changed feature
⚠ Bug fixed

PC Client

✅ A new option for security-conscious environments: PC Client can now optionally run under a restricted virtual service account instead of the default Local System. This significantly reduces security risk. To enable this requires `USESERVICEACCOUNT` switch to be used during installation. See Installing SAFEQ Cloud Client on Windows for more details. (HCP-14631)

⚠ PC client login mechanism no longer requires some users to login two times. (HBT-5374)

Web UI

⚠ The waiting print jobs icon no longer shows a spinner. (HBT-5436)

⚠ Automatic endpoint trust was in some cases not applied even when enabled. This is now resolved. (HBT-5246)

Konica Minolta Gen 2 Cloud Terminal

ℹ Performance optimizations were added to limit "Script Busy" error message on older devices. (HBT-5185)

Xerox Gen 2 Cloud Terminal

ℹ Advanced finishing options like booklet printing, punchuing and stapling are now working as expected. (HBT-5383)
⚠ Push print mechanism with PC Client in local storage mode was improved to mitigate a risk of document being printed two times. (HBT-5346)

HP Cloud Terminal Gen2

ℹ Improved support for printing multiple copies via HP Universal Print Driver (UDP) over IPP in Pull Print; jobs now correctly respect requested copy counts where possible (HBT-5368)

IPP printing

⚠ IPP endpoint is now more robust and has better throughput for accepting print jobs. (HBT-4759)

4.1.5 2025.05.15

Legend:

✅ Added feature
ℹ️ Improved/changed feature
⚠️ Bug fixed

Web Admin UI

ℹ️ PC Client Auto-update interface has been refined with clearer indicators for manual updates, updated visuals, improved sorting, and streamlined feedback submission. (HCP-14577)

ℹ️ Final color adjustments across key Web UI components have been applied to ensure a more consistent and accessible user experience. (HCP-14122, HCP-14279)

⚠️ My Profile -> Sessions no longer fails to load the content. (HBT-5415)

Sharp Cloud Terminal

✅ Installation and configuration are now possible using the Terminal Deployment Tool, including advanced deployment scenarios across multiple devices. See Terminal Deployment Tool for more details. (HCP-14585)

Scanning

⚠️ Scan to download scanning workflow now correctly separates pages when using barcodes. (HBT-5330)

⚠️ Barcode processing is much more reliable now. (HBT-4825)

API

⚠️ Creating outputport via API now correctly assigns embedded configuration. (HBT-5408)

Gateways

⚠️ The exceptions with gateways unable to reconnect to the primary cloud servers are now correctly handled (TryConnect exception) and gateways operate as expected. (HBT-5342)

4.1.6 2025.04.30

Legend:

✅ Added feature
ℹ️ Improved/changed feature
⚠️ Bug fixed

Web UI

✅ Shared Print Queues - Users now can share print files with others by using the new shareable option. (HCP-14381)

ℹ️ The Installation Files section of the vendor account now provide an up-to-date link to the latest version of the Universal Print Driver. (HCP-14510)

Xerox Cloud Terminal

ℹ️ Manual configuration is no longer needed—when a Xerox Cloud Terminal is authorized, its printer and embedded configuration is now created automatically using the device's serial number. (HCP-14537)

ℹ️ Xerox Cloud Terminal now supports configurable session timeouts (up to 15 minutes), with smart handling that pauses during active use and logs the users out upon leaving the app. (HCP-14527)

Ricoh Cloud Terminal

ℹ️ You can now install the Ricoh Cloud Terminal using the Terminal Deployment Tool on networks where port 80 is blocked, with updated documentation reflecting this change. (HCP-14606)

Canon Embedded Client

ℹ️ Added support for the Canon Embedded Client specific to the Oceania region. (HCP-14346)

Konica Minolta Gen 2 Cloud Terminal

ℹ️ Both native and in-app scans are now accounted correctly. (HCP-14473)

Sharp Cloud Terminal

⚠️ We've fixed an authentication issue that prevented jobs sent via IPP using a vendor driver from printing on Sharp Cloud devices—these jobs are now properly handled during pull print sessions (HBT-5338)

⚠️HP Cloud Terminal Gen2

Improved performance and reliability of card login to address intermittent black screen issues caused by high printer usage; the terminal now delays initialization until the card is read, reducing SDK load and improving responsiveness (HBT-5308)

Scanning

⚠ Scanned documents with PDF/A compliance other than PDF/A-1a no longer fail to embed fonts correctly. Errors in Adobe Acrobat are no longer happening in such cases. (HBT-5315)

PC Client

⚠ PC client no longer returns a different set of input ports depending on whether it was using API mode (cloud storage) or websocket-channel mode. Ports are now consistent across both. (HBT-5337)

⚠ Default Windows printer set by the client is selected consistently, prioritizing the one with the lowest ID. (HBT-5371)

⚠ When printing A3 documents as booklets, the output is now correctly downscaled to A4 size instead of incorrectly producing A5 on A4 paper. (HBT-5302)

4.1.7 2025.04.17

Legend:

✔ Added feature
ℹ Improved/changed feature
⚠ Bug fixed

Web Admin UI

ℹ Simplified process to add a Konica Minolta Gen. 2 Cloud terminal into the environment. (HCP-14497)

✔ Print and scan delegation improvements. Users can now share documents with people who do not yet have an account. (HCP-14467)

⚠ Renamed Entra ID groups are now correctly displayed. (HBT-4215)

⚠ Fixed an issue where guest users were redirected to an incorrect login page after clicking the 'Go to Login Page' button in the invitation email. (HBT-5213)

PC Client

⚠ Support information package also contains safeqclientcore.conf. (HBT-4966)

Ricoh Embedded Terminal (3.0.5)

✔ Booklet Printing Support, users have a wider range of finishing options.

✅ Supported Languages, users can access the embedded terminal in their own language (Finnish, Welsh, New Zealand Maori, Arabic,Hebrew).

ℹ️ Easier for users to navigate to the Secure Print & Scan application.

ℹ️ Provides more accurate usage reporting based on device counters.

ℹ️ Improved logic for downloading jobs to the MFD to prevent large jobs failing to download properly

⚠️ Fixed issue where user was unable to cancel job or logout if network cable is removed during large print job processing.

⚠️ Fixed issue in UI with terminal version sometimes being pre-fixed with "null"

⚠️ Fixed issue with card login from sleep mode resulting in "You do not have permission to print" error

⚠️ Disabled System Auto Reset during print/scan background activity so that the device will no longer switch to home screen during print/scan processing

⚠️ Fixed issue where application could stop when restart button is pressed during installation from Ricoh Application site

Terminal Deployment Tool

⚠️ Fixed an issue where the Terminal Deployment Tool used unsecured HTTP (port 80) during deployment, configuration, and uninstallation of Xerox terminals, despite documentation stating that only HTTPS (port 443) should be used (HBT-5327)

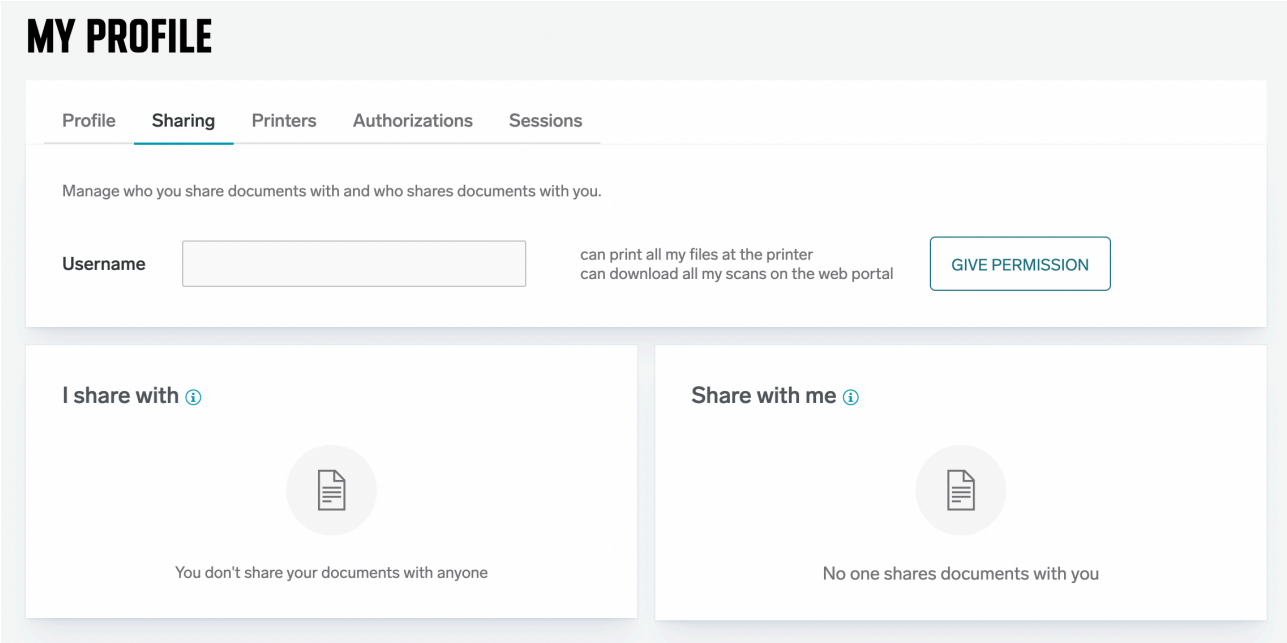
4.1.8 2025.04.03

Legend:

✅ Added feature
ℹ️ Improved/changed feature
⚠️ Bug fixed

✅ Print and scan delegation improvements (HCP-14351)

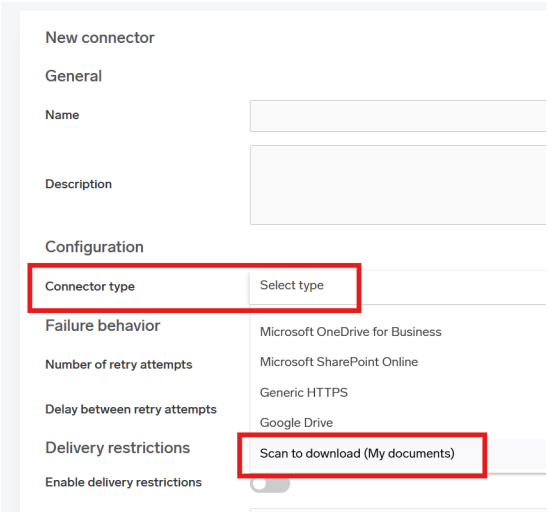
Users now have an easier way to delegate their printing and scanning (scan to download workflow) to other users. Previously, this was only possible by the administrator, now the functionality is also available to users - a new "Sharing" section in "My Profile".

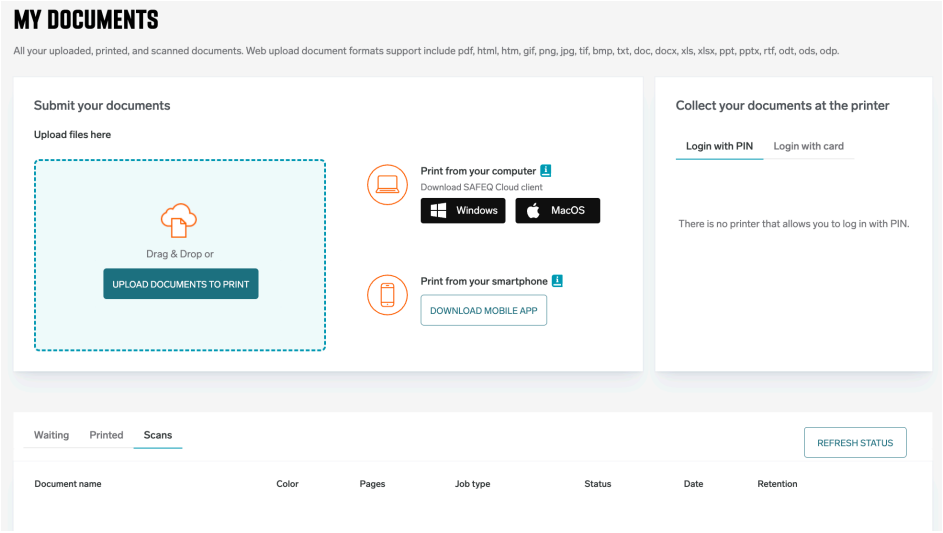


Scan to download (My documents) (HCP-13992)

A new scan connector is now available: scan to download. It's designed for customers who don't use cloud storage and prefer not to send scanned documents via email.

This workflow securely stores the documents in the cloud, the users are notified via email with a download link. The scanned documents are also available via 'My Documents' section in "My Profile".





Web Admin UI

- UI improvements in PC client auto update section. (HCP-14427)
- Cloud option removed from Terminal integrations settings. (HCP-14412)
- The default type of login on default embedded templates changed to "PIN or Card". (HCP-14412)
- The Gateway installer link is available on "Installation files" page. (HCP-14113)
- Adjust license validations on add new printer page. (HCP-14411)

HP Cloud terminal Gen 2

- New language support added (HCP-14020)
- Multiple print jobs are now reliably processed in FIFO (first-in, first-out) order based on submission time (HBT-5258)
- ⚠ Fixed an issue where HP Cloud Terminal Gen 2 incorrectly applied finishing options to print jobs sent via native drivers; such jobs are now passed through unchanged unless they are PDFs (HBT-4789)

Bux fixes:

- ⚠ Fixed an issue where creating a trigger for OTP and/or Short ID would generate multiple codes and send multiple emails—one for each print job sent by the user. (HBT-5061)
- ⚠ Fixed an issue where not all parts of a split scanned document are delivered. This was sometimes happening during the split processing step combined with OCR when the document was split unevenly. (HBT-5202)
- ⚠ Fixed an issue where card registration triggered two consecutive authentication requests to Entra ID, potentially causing false-positive "bruteforce" alerts. (HBT-5236)
- ⚠Fixed an issue on macOS where the client did not persist the logged-in user after reboot due to the remember_login setting not being properly saved to client_config. (HBT-5221)
- ⚠Fixed an issue where case sensitivity in the customer tenant name caused device token validation to fail. (HBT-5313)

4.1.9 2025.03.20

Legend:

Added feature
Improved/changed feature
Bug fixed

Scanning

A new scan to download connector is available. (HCP-13992)

- See the documentation: Scan to download (My documents) connector

Web Admin UI

PC client auto-update report now shows more details. (HCP-14336, HBT-5245)

PC client tab was simplified to show a quick overview of client versions. (HCP-14335)

Document encryption is no longer optional, it is now enabled by default and cannot be disabled. (HCP-14192)

Web upload: documented limitation that only standard fonts are supported, see Web upload . (HBT-5049)

Chrome Extension

Chrome Extension informs users when the server connection is unavailable. (HBT-3677)

Chrome Extension version is now visible in the options window. (HBT-3645)

Konica Minolta Gen 2 Cloud Terminal

Simplified process to add a Konica Minolta Gen. 2 Cloud terminal into the environment. It is created automatically now. (HCP-13692)

Clearer information when print job settings can't be changed (HCP-14179)

Multiple jobs sent to print are always printed in first-in, first-out order (HCP-14185)

Fixed inconsistency of displaying the full name in the scan and print menu (HBT-4580)

Added file rotation for the terminal log files. (HBT-5239)

4.1.10 2025.03.06

Legend:

✅ Added feature
ℹ️ Improved/changed feature
⚠️ Bug fixed

Web Admin UI

✅ A new section "Installation files" is now available for customer admins. (HCP-14177)

ℹ️ Further tooltip visual improvements. (HBT-5251)

PC client

✅ PC client with universal print driver is now ARM 64 compatible. (HCP-14183)

✅ Universal print driver now support a new paper size: Arch B 12 X 18in. (HCP-13522)

⚠️ PC client mechanism to switch to port 443 from legacy 7400 was improved. (HBT-5215)

⚠️ With Windows Protected Print (WPP) enabled the print queue no longer fails to create when renamed at the Admin Web UI. (HBT-5156)

⚠️ PC client auto update report now correctly shows failed instances following the selected time period. (HBT-5193)

Messaging

✅ The messaging configuration now allows modern authentication with Google allowing its use in email messages and scan workflows.

Documentation

ℹ️ Documentation page "Rules - triggers and automation" now lists individual document statuses with description. (HBT-5225)

4.1.11 2025.02.20

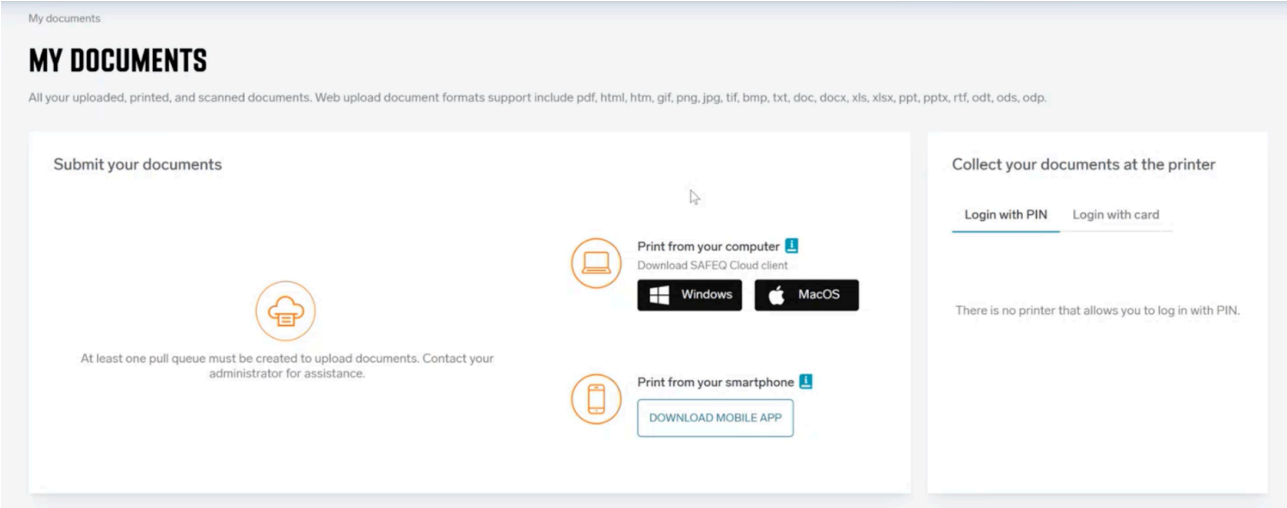
Legend:

✅ Added feature
ℹ️ Improved/changed feature
⚠️ Bug fixed

UI improvements

ℹ️ Web UI fonts, styles and tooltips updated for improved usability. (HCP-14018, HCP-14019)

ℹ️ User is informed why print job Web Upload is not available for them. (HCP-13793)



ℹ A user can go to "My profile" and uncheck a print queue even when it was added with "available by default" checked. (HBT-4803)

⚠ Web UI now correctly displays the number of pages for each print job when WPP (Windows Protected Print) is enabled. (HBT-5158)

PC client

⚠ PC client auto update now cleans up its folder structure after each version. (HBT-5150)

⚠ PC client correctly auto updates to the selected version and automatically restarts. (HBT-5218)

⚠ A user is not allowed to use a blank PIN when logging in(HBT-5107)

Terminals

⚠ KM OpenAPI terminal connected to OMNI bridge no longer stops responding with multiple logout button clicks. (HBT-5188)

4.1.12 2025.02.06

Legend:

✅ Added feature
ℹ Improved/changed feature
⚠ Bug fixed

UI improvements

ℹ PC client auto update report now contains more information, can be exported into multiple formats and filtered by time period. (HCP-14108)

ℹ Web UI informs administrators about implications of using built-in CA. (HCP-14104)

⚠ Locations can now be reordered. (HBT-5058)

Sharp Gen2 Cloud Terminal (v2025.02.01)

ℹ Sharp Gen 2 Cloud Terminal requires admin password to access application settings. (HCP-13789)

ℹ Sharp Gen 2 Cloud Terminal requires admin password to access application logs. (HCP-13931)

ℹ Sharp Gen 2 Cloud Terminal UI improvements when folder-browsing. (HCP-13945)

API

⚠ The system can now process print job types even if they are not recognized as Postscript, PDF or PCL6 jobs. They are no longer rejected. (HBT-5078)

Various performance and security enhancements

⚠ Virtual appliance OVA (Build 20240821_0932) now longer fails on vSphere with: An invalid argument "configSpec.guestId" error. (HBT-5071)

⚠ HTTP Options methods are only used when needed. (HBT-5077)

ℹ Improved security of HTTP headers. (HBT-5076)

ℹ Weak cipher suites were disabled. (HBT-5075)

4.1.13 BUILD 2025.01.23

Legend:

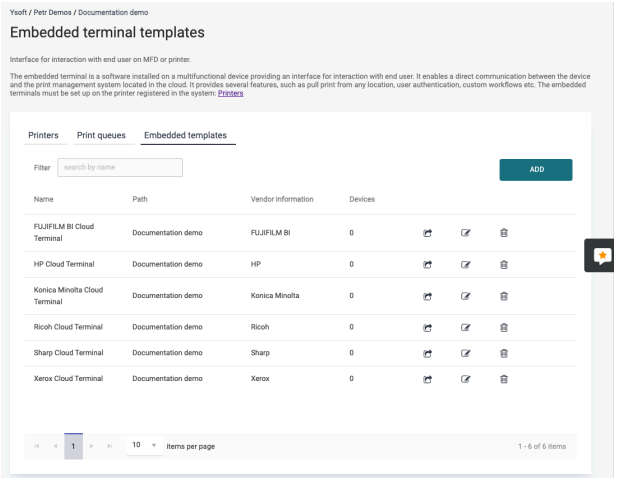
✔ Added feature
ℹ Improved/changed feature
⚠ Bug fixed

PC Client

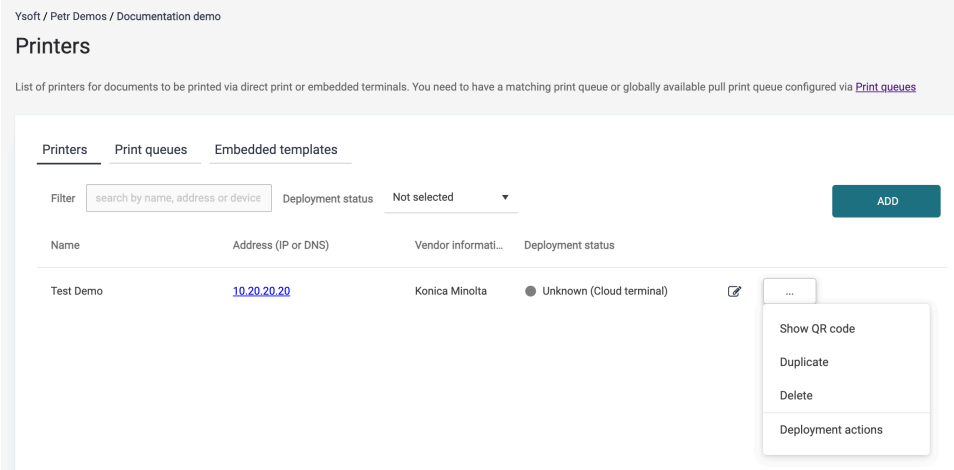
- ✔ When WPP mode is turned on, these Finishing Options are received via IPP and converted into the PJL headers stored in the document.
  - Page range
  - Stapling
  - Punching
  - Input tray
  - Output tray
  - More paper sizes

UI improvements

- ✅ Every new customer has a list of default, preconfigured embedded terminals created.

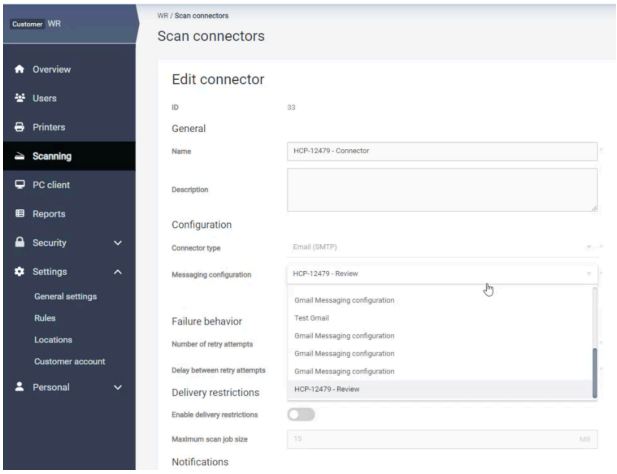


- ✅ Admin now has the link to embedded configuration deployment from the printer list



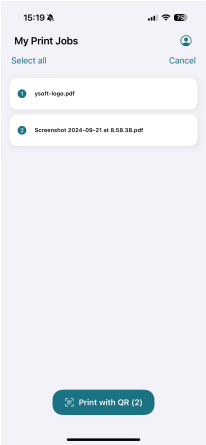
Scanning

- ✅ Scan to email now support OAuth2



SafeQ Mobile application

- ✅ The SafeQ Mobile app now supports releasing documents via a QR code scanned on the printer. This feature is available only in environments with a gateway or when local storage is enabled on the client.



KM IWS Gen2 Cloud Terminal (v2025.01.01)

- ✅Copy accounting is done via Service platform authentication app. Native copy accounting is also supported.
- ✅IWS Cloud terminal terminal gets the information about ISPF integration (Service platform authentication application is installed) from server and avoid asking for ISPF token when not integrated.
- ✅Logout button is hidden when integrated with Service platform. Hardware button must be used to log out. This avoids login user back right after pressing logout, which is a limitation of the integration.
- ⚠️Quick copy action on IT6 machines no longer triggers the "separate scans" native dialog.
- ⚠️Fixing configuration page- port can be added into URL
- ⚠️Users can access settings directly via cogwheel button on internal server error to possibly fix terminal configuration
- ⚠️Amount of copies are limited to 9999 so it behaves same as KM native applications

Various performance and security enhancements

Build 2025.01.09

Legend:

Added feature
Improved/changed feature
Bug fixed

PC Client

- MacOS users can now specify paperSize, duplex and color when installing the PC Client in unattended mode (HCP-13908).
- User no longer gets logged out unexpectedly when the cloud connection is not established fast enough (HBT-5048).
- When PC client cannot operate with the existing token it will drop it and re-register itself (HBT-5031).
- "Domains" field of the "Customer information" is no longer case sensitive and does not cause problems when authorizing clients (HBT-5041).

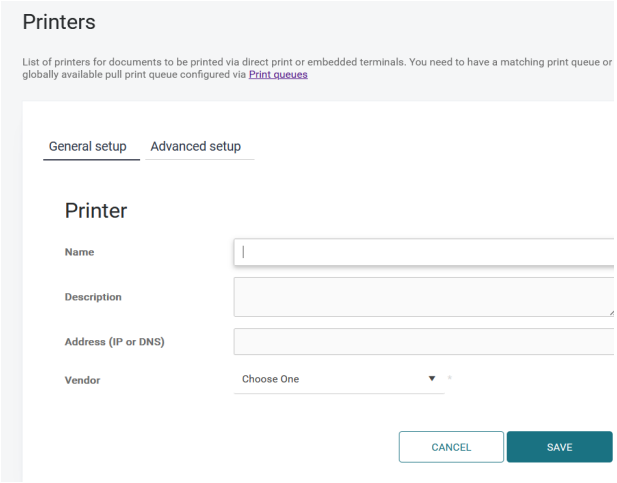
Sharp Gen 2 Cloud Terminal - Production release

- A user can select a destination folder at the Sharp terminal (HCP-13605).

UI improvements

- An administrator can send a test email using the inherited mail configuration (HCP-13855).

- Left menu minor improvements (HCP-13891).
- URL is generated correctly when navigating through the Admin Web UI (HBT-5050).
- Significantly simplified experience to "Add device" (HCP-13801).



Xerox Gen 2 Cloud Terminal

- ℹ VersaLink 2nd Gen devices now correctly install on Windows 11 (HBT-5008).

Kyocera Embeded Terminal

- ℹ Users no longer see internal login "user1" when logged into the terminal. Instead, it shows "Kyocera" so it is less misleading (HBT-4243).

Scanning

- ℹ The OCR engine was updated to the latest ABBYY FRE 12.6 (HCP-13399).

Various performance and security enhancements

- ℹ reCaptcha was added to protect also forgotten password screen (HCP-13791).

4.2 2024

4.2.1 BUILD 2024.11.28

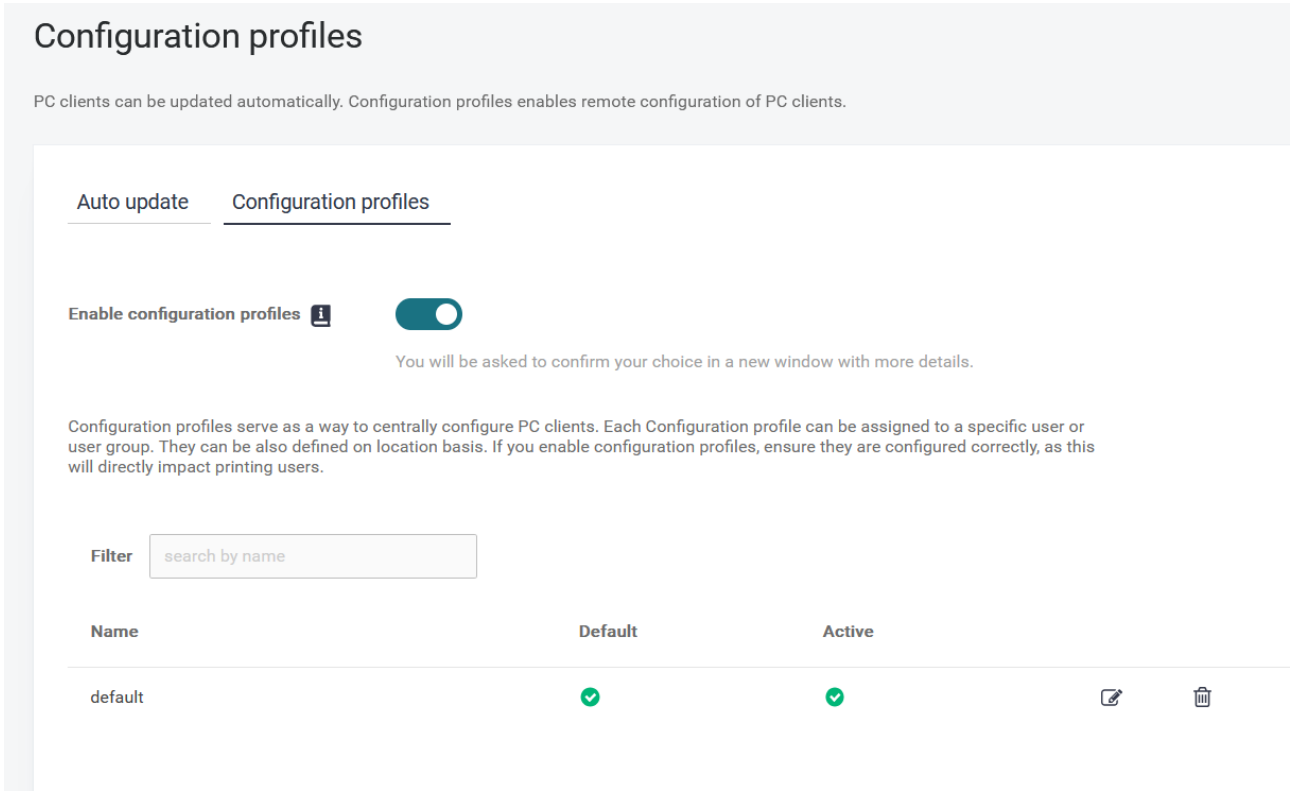
Legend:

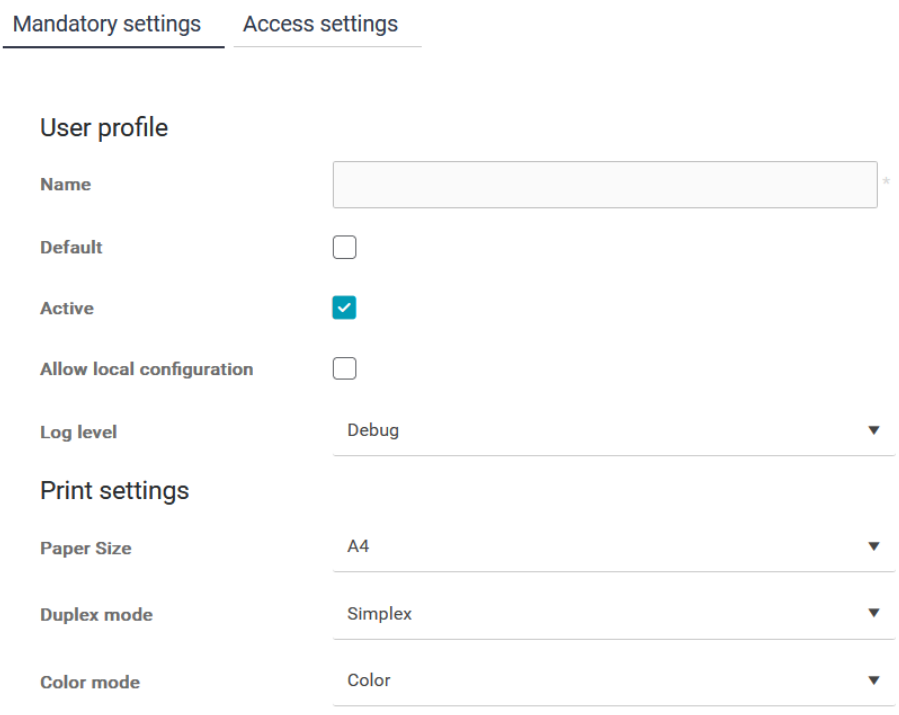
✅ Added feature
ℹ Improved/changed feature
⚠ Bug fixed

PC Client

An administrator can centrally manage PC Client options: (HCP-7738)

- Allow local configuration
- Log level
- Paper Size
- Duplex/simplex
- Color/grayscale



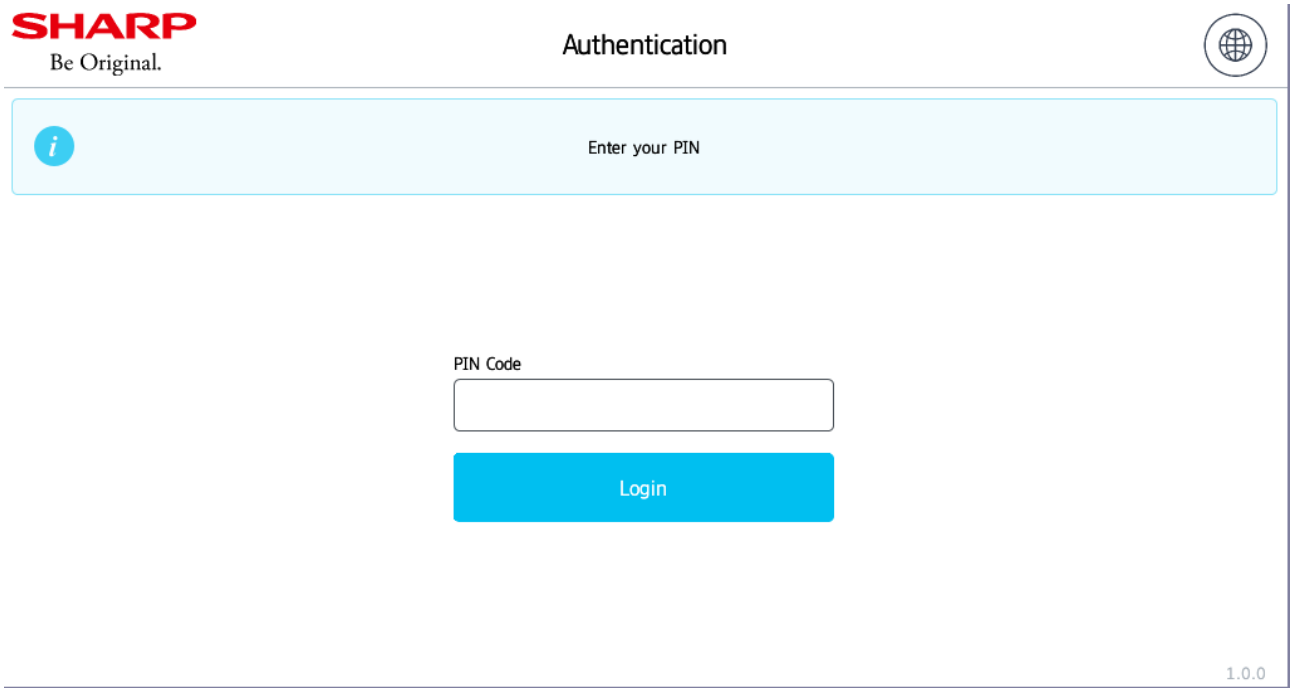


⚠️ PC client in hybrid mode is correctly registered when the "Automatically trust new clients/ servers" is enabled. (HBT-4910)

⚠️ PC client contains correct Ghostscript binaries. (HBT-5016)

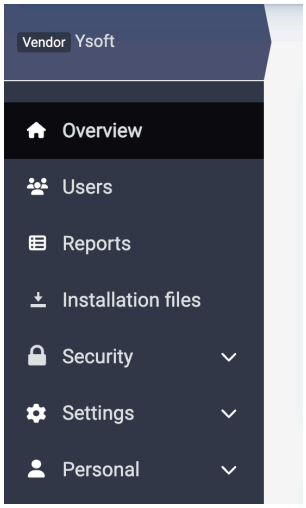
Sharp Gen 2 Cloud Terminal (Public BETA 4)

✅ An administrator can set the custom logo on the terminal (HCP-13845)



UI improvements

✅ Admin Web UI menu has a new structure to simplify the navigation (HCP-13722)



⚠️ More printers with the same IP address (e.g. in different subnets) now work correctly with embedded configuration. (HBT-4920)

KM IWS Gen2 Cloud Terminal

Deployment documentation improvements (HBT-4994)

Various performance and security enhancements (HBT-4835, HBT-4938)

4.2.2 BUILD 2024.11.14

Legend:

Added feature
Improved/changed feature
Bug fixed

- New AWS-based public datacenter in Sweden.

PC Client

- PC Client security is improved by using an intermediate, customer-specific Certificate Authority for self-signed certificates.

  PC Client security is improved by using an intermediate, customer-specific Certificate Authority for self-signed certificates, with no impact on currently deployed clients.

  For new installations or reconfigurations, the specified account domain must be resolvable and signed by a globally trusted CA root (visibility to the cloud server is required).

  If no self-signed certificates are configured, the PC Client will only trust global CA roots. These changes only affect PC Clients where the server address differs from the account domain

Sharp Gen 2 Cloud Terminal (v2024.11.01 Public BETA 3)

- User is able to enter metadata during scanning.
- User can change the terminal language.
- Push print jobs are tracked on the terminal and account printed page counts

KM IWS Gen2 Cloud Terminal (v2024.11.01)

- User knows that the color job will be printed in B&W on their monochrome MFD.
- The terminal now respects permissions on color print restrictions.

HP Gen 2 Cloud terminal (version?)

- HP now correctly applies finishing options for print jobs produced by native driver.

Xerox Gen 2 Cloud terminal

- Improved speed of printing multiple documents on Xerox cloud terminal.

API Changes

- new API available to list of all users (only local and those actually using the solution) /api/v1/users/all

Various performance and security enhancements

- Gateway module for Omnibridge is upgraded to the latest OS version.
- There is now a warning for administrators on the Web UI when they are attempting to delete a token signing certificate which is in use.

4.2.3 BUILD 2024.10.31

Legend:

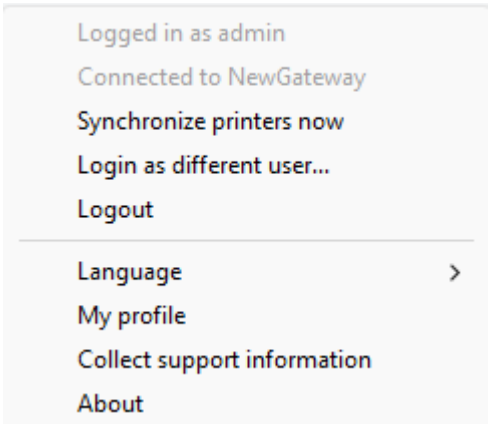
Added feature
Improved/changed feature
Bug fixed

Notifications and scanning

- New customers have email server for notifications and scan workflows configured right out of the box using default email service (HCP-11739)
  - Default mail server is Amazon SES for all public AWS datacenters and OTC SMTP server for European sovereign datacenter
  - Vendors and Customers can still use their own/preferred email service
  - Default email service is also available for existing customers
- All existing customers with an invalid email server configuration will be updated to the default service

SAFEQ Cloud Client

- Users with PC client installed can now see to which gateway is their PC client connected. When connected directly to the cloud, no information is shown. This is available when they right-click the tray icon. (HCP-13689)



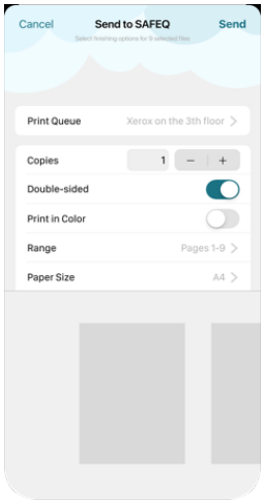
- ⚠ When the PC Client is manually registered to a service multiple times it no longer returns an error "Client registration failed!". (HBT-4872)

Sharp Gen 2 Cloud Terminal (Public BETA) (HCP-12826)

1. ✅ Documentation is available for Sharp Cloud Terminal beta v2 release (HCP-13683)
2. ✅ Reporting of printed pages on Sharp Cloud terminal now includes actual printed pages (not just pages submitted) (HCP-13705)

SafeQ Mobile app

1. ✅ User can select a print queue before submitting a job (HCP-13451, HCP-13450). The default selection is the "secure" roaming print queue. If there is a direct / push print queue available for the user and properly configured to release the documents (using gateway), the documents will be directly released on that printer.



2. ⚠ Fixed issue with print job list refresh caused by expiring tokens (HBT-4877)

Ricoh Cloud Terminal 3.0.4

1. ℹ️ Application name on the Ricoh MFD is now CloudStream PS (was Ricoh CloudStream PrintScan Embedded) (HCP-13461)
2. ✅ Ricoh Cloud Terminal now respects all finishing options from the PC client (stapling, punching,...). (HBT-4777)
    a. *Note: booklet option is missing and will be added in coming versions.*
3. ℹ️ Documents are now released in the order in which they were sent (HBT-4880)
4. ℹ️ Reporting of scanned pages now reflects department assignment of a user scanning with Ricoh Cloud Terminal G2.5 and G3 devices (HBT-4547)
5. ℹ️ All MPF settings are now reverted to default after uninstallation of Ricoh Cloud Terminal (HBT-4796)
6. ⚠️ Fixed scenario when Ricoh Cloud Terminal Gen 2 fails to connect to the server via installation using Terminal Deployment Tool (HBT-4659)
7. ⚠️ Fixed error "Printer with the same endpoint ID already exists on the server" on Ricoh IM350 after authorizing the endpoint (HBT-4524)
8. ⚠️ Fixed error when status of the Cloud Terminal is not updated if the previous status is Failed (HBT-4606)
9. ℹ️ Various performance and security improvements (HCP-13462, HBT-4451,HBT-4023,HBT-4300)

Various performance and security enhancements

1. ℹ️ PC Clients now properly work with custom-created API key (HBT-4918,HBT-4754)
2. ✅ Improved mechanism for handling self signed certificates used for gateways, and clients (HCP-13712)
    a. Self-signed certificates are automatically renewed with a new mechanism of intermediate certificate generated for each account.
    b. Intermediate cert is valid for 10 years
    c. Entity certificate is signed by intermediate
    d. Self-signed certificates does not work with primary servers

4.2.4 BUILD 2024.10.17

Web UI

+ Self-registered users and guests can now reset a forgotten password via the Forgot password button on the login page.

The Mobile app

+ The app now supports communication over the 443 port.

Sharp Gen 2 Cloud Terminal (Beta)

+ Users can now cancel scanning via the Cancel scan button.

Various performance and security enhancements

- Updated 3rd party components to mitigate vulnerabilities

4.2.5 BUILD 2024.10.03

A note regarding SAFEQ Cloud Client for MacOS Sequoia 15:

Due to the changed MacOS 15 security model, the SAFEQ Cloud Client autoupdate functionality from previous versions doesn't work, and the users must update to version 2024.10.03 manually.

After re-installation, the update mechanism will be supported again.

The print functionality of the existing version(s) is not impacted

General improvements

+ The Messaging service now allows modern authentication with Microsoft (and Google, as soon as verified) allowing email messages and scan workflows to use OAuth2 instead of basic authentication.

+ Forward proxy support for the SAFEQ Cloud Client.

SAFEQ Cloud Client

x Improved UI in the auto-update table, notifications, and reporting.

- UPN no longer logs out the user and no longer shows a notification after each re-login when the user's PC goes to sleep.

- After uninstallation, the HCP Port Monitor is now properly deleted.

Web UI

+ The vendor and customer dashboard now shows the Customer Contract ID (MA) and SLA.

+ You can now delete the logo or background image from customer settings.

+ Secondary Gateway OVA (Rocky Linux) download links are now available in the Installation files library

x Printer configuration form improvements: The new printer form is well structured and leads the admin towards the printer creation in a logical and easy way.

x Redesigned UI for the assignment of Access Rights Permissions for user roles and API keys.

x When editing the logged-in user in Users, the newly added values are reflected in the current user session and are visible on the My Profile page.

x The SAFEQ Cloud Client auto-update page now displays correct counts of SAFEQ Cloud Clients connected in the last 90 days

The Mobile app

+ Admins can now configure the Mobile app via MDM.

Sharp Gen 2 Cloud Terminal (Beta)

+ Users can now modify simple workflow settings on the terminal.

+ Users can now modify scan settings on the terminal.

+ Admins can now set the complexity of logging on the terminal.

Various performance and security enhancements

x Updated 3rd party components to mitigate vulnerabilities

4.2.6 BUILD 3.49 [2024-09-19]

SAFEQ Cloud Client

x SAFEQ Cloud Client auto-update improvements - newly created customers can also use the rollback option.

x You can now connect the SAFEQ Cloud Client in cloud storage mode to the secondary gateway with the "Enable secure login for session authentication types" option.

- SAFEQ Cloud Client no longer reports auto-update as failed in the configured "delay" update window.

- Severity: C (no user impact)
- Root cause: Unforeseen impact of the change.
- Bug recurrence defense: n/a

- SAFEQ Cloud Client can now be reinstalled in unattended mode. The "/S /UPGRADE=false" option no longer keeps the existing configuration file and correctly creates a new one.

- Severity: C (no user impact, viable workaround)
- Root cause: A different change caused this.
- Bug recurrence defense: Added to standard test scenarios.

Web UI

+ A new trigger is now available which forces all print to black & white. This trigger is disabled by default and ready for customers to simply enable or modify. This is available for all new customer accounts.

+ Improved Web UI for vendors

- Vendors have a new quick orientation page with direct links to various information sources.
- Vendors now see the list of their customers, including license and expiration directly on the main dashboard

- Vendors now see new "Installation files" link where they can access the downloadable components (without the need to go to YSoft Partner Portal). Note that the files library will grow in upcoming releases.
- After creating a new customer tenant, vendors are offered an email template with customer tenant access.

+ Guest user support

- Users can now self-register in the Web UI.
- Guests can self-register for a temporary user account in the Web UI.

x The page with triggers is now organized for better usability.

x The page with Access control is now organized for better usability.

x Changing the name of a print queue with pending print jobs in it no longer causes those jobs to disappear.

x SAFEQ Cloud Client auto-update tab now uses a more readable font.

- The account health section now correctly links to the SAFEQ Cloud Client section.

- Severity: C (administrator impact with a viable workaround)
- Root cause: Missing tests when the section was moved.
- Bug recurrence defense: Tests were added.

- Administrators are now able to authenticate again at a container level when using the container domain. (HBT-4751)

- Severity: C (administrator impact with a viable workaround)
- Root cause: Database changes in version 3.45
- Bug recurrence defense: Added tests to the standard test suite

The Mobile app

+ New mobile app design
+ User-friendly interface
+ Easy to set and connect to your SAFEQ Cloud account

Sharp Gen 2 Cloud Terminal (Beta)

+ The new Sharp terminal is now available for beta testing
+ Basic print and scan functions

Xerox Gen 2 Cloud Terminal

+ Users no longer need to manually deploy card plugin and card service for Versalink devices. This capability was added to the Terminal Deployment Tool.

x Stapling, folding, and punching are now supported.

HP Workpath Gen 2 Cloud Terminal

- Print jobs with booklet and center stapling finishing option when using cloud storage can now be released correctly.

- Severity: B (medium user impact)
- Root cause: Missing vendor-specific requirements
- Bug recurrence defense: Deeper external cooperation

Printing

x EveryonePrint HCP Extension is now branded as SAFEQ Cloud Chrome Extension.
- PDF documents that were uploaded via API and have an internal /Rotate command are now printed correctly.

- Severity: B (medium user impact)
- Root cause: Unexpected PDF configuration
- Bug recurrence defense: n/a

- When scanning multiple pages with the Page separation processing step, the resulting pages now respect the requested resolution and are no longer significantly bigger.

- Severity: C (some user impact)
- Root cause: There was an unnecessary conversion as a middle step which was removed.
- Bug recurrence defense: n/a

Installation

+ Rocky Linux 9 Software Appliance is now available on YSoft Partner Portal. Note: this will be also available in the Installations Files library in upcoming releases.

API

x Print queues created by API are now enabled by default.

+ Account API was extended with new fields for page size, language, and color. The update option now contains the name and domain name. API responses were improved.

Various performance and security enhancements

x Updated 3rd party components to mitigate vulnerabilities.

x Various performance updates.

4.2.7 BUILD 3.48 [2024-08-22]

Communication via port 443, no additional Internet ports

This is a staged rollout and we will announce the availability per data center via our status page.

+ All SAFEQ Cloud components (all cloud terminals, SAFEQ Cloud Client, and gateways) now support communication via port 443 (HTTPS). Therefore, you don't need to open any additional ports to the Internet. The only exception is the FUJIFILM BI Cloud Terminal, which will be supported later.

⚠ Customers with EntraID OAuth or SAML SSO configured should review this KB article to ensure uninterrupted service.

+ SAFEQ Cloud Web UI is available without the additional 8443 port number in the URL.

+ All cloud terminals, SAFEQ Cloud Client, and gateways on the latest version support communication via proxy servers.

SAFEQ Cloud Client

+ SAFEQ Cloud Client will automatically update to the latest version. This is enabled for new customers. The existing ones can set it up in the SAFEQ Cloud Web UI in Configuration > PC Client.

Xerox Gen 2 Cloud Terminal

+ Xerox Gen 2 Cloud Terminal is now available to all customers.

⚠ There are two known limitations, that will be resolved soon:

- The card reader is not recognized frequently after the device is waken up, and the auth screen falls to the default auth method (PIN, username/password).
- Pull print basic finishing options, simplex short edge print changed to long edge print is printed as simplex.

Web UI

+ For all new customers, a default pull queue is created during the deployment to speed up the initial setup. The queue name is localized.

x Entra ID OIDC authentication now works with single-tenant configuration and no longer requires multi-tenant configuration.

x The Web UI favicon was improved.

x If no signing certificate in PKI and Encryption settings is selected, the users cannot log in to SAFEQ Cloud Client via the manual login method. You are now alerted to such situation in the Account health section.

x You can now hide download links and the news banner. There are two new permissions to allow this: ViewNewReleaseNotification and ViewClientAndMobileDownload.

x The texts and the layout of the document upload section in My documents have been improved.

- The cloud terminal deployment documentation link on the Web UI now correctly opens a page with instructions.

- Severity: C (intuitive workaround)
- Root cause: the documentation page was split per vendor in the documentation which was not reflected in the links on Web UI.
- Bug recurrence defense: adopt a new documentation tool and process.

- Accented letters (ěščřžýáíéů) are now shown in consistent font with the rest of the letters.

- Severity: C (no user impact)
- Root cause: automated tests did not catch the visual difference.

- Bug recurrence defense: no action taken.

Printing

x A3 paper size can be now fetched in job detail from the API reporting endpoint.

Konica Minolta OpenAPI Terminal

x Konica Minolta OpenAPI Terminal can now be used in environments with a load balancer as long as there is X-Forwarded-For header where the origin IP address of the client is stored.

Installation

x Rocky Linux 9.4 is used with image (OVA) for the NUC HW appliance.

Various performance and security enhancements

x Documents sent via API converting to print for over 5 minutes will not be accepted. They are now marked as failed and shown with the respective status in the Web UI. This also applies to MS Office documents over 200MB or Excel files with over 10,000 pages.

x The SAFEQ Cloud Client was updated to use the latest and most secure version of GhostScript 10.03.1.

4.2.8 BUILD 3.47 [2024-07-25]

SAFEQ Cloud Client

+ You can now set SAFEQ Cloud Client with local storage to send pull queue print jobs to cloud storage.

+ The SAFEQ Cloud Client now contains a link to My profile in SAFEQ Cloud Web UI.

- Added info to documentation that if you delete an account of a user who logged in to the SAFEQ Cloud Client and didn't log out, the user may still be able to perform user actions, such as print for up to 1 hour, due to caching on servers.

- The Client installer now writes JSON-compliant values to the json file, no longer causing parsing issues.

Web UI

+ You can now set triggers to rotate a document by 90 degrees clockwise or counterclockwise.

+ Users can now upload documents to be printed in the Web UI. This feature is no longer in the Early Access Program but available to all customers.

x The table with SAFEQ Cloud Client versions that facilitates the auto-update process is now improved.

x The button colors have been changed across the whole Web UI.

x The Authentication provider name has been added to the Access tab in Scan Workflows.

x OIDC-only authentication is not supported with SAML without Service account authentication.

- Fixed an issue that prevented creation of customer account with custom logo, resulting in an error and missing license.

- Localization to German has been improved.

- In Security > Certificates, the action icons stay grouped together even if you zoom the page.

- Fixed the slow loading and internal error on 'My Documents' and 'Reports' pages.

- Fixed the issue with missing permissions for default roles that occurred when migrating database from version 3.35

- Fixed incorrect product name of SAFEQ Cloud in Lexmark Printer administration.

API

- Uploading print job to a non-existing input port via API no longer returns 200 instead of an error.

Printing

- In the Universal Print Driver settings dialogue window, the arrow button to increase the size of the watermark is now above the arrow button to decrease the size.

Konica Minolta IWS Gen 2 Cloud Terminal

- The terminal now supports Norwegian language.

- Registration expiration no longer blocks the whole terminal.

- IWS Marketplace versions can access settings via the header icon.

Xerox Gen 2 Cloud Terminal

x The terminal supports custom logos.

x The terminal supports the Merging originals function.

x The terminal supports accounting of scan jobs.

x If a print job cannot be printed, the terminal displays an error message with the cause of the problem.

x The terminal is versioned.

- Scanning now works at Xerox AltaLink C8030.

Scanning

- New error codes have been added to help admins with troubleshooting.

- A scanned PDF/A document can now be opened in Adobe Acrobat without displaying the "Some characters may not display or print correctly" error.

HP Workpath Gen 2 Cloud Terminal

- Fixed the problem when multi-copy was not working on some HP printers.

- Booklet printing now works in the Download&Print scenario.

The Mobile app

x The Enforce tokens setting has been enabled for existing customers.

- BW print jobs are no longer accounted as color print jobs when submitted from the Mobile app.

Performance and security enhancements

- Security has been improved for session user login.

4.2.9 BUILD 3.46 [2024-06-27]

Scanning

+ Users can now scan to Google Drive.

SAFEQ Cloud Client

+ The SAFEQ Cloud Client now has the auto-update functionality. This feature is currently available upon request in the Early Access Program.

- SAFEQ Cloud Client defaults to the default API key if the API key field is left blank after deleting the optional API key.

- When the SAFEQ Cloud Client is installed with authentication type = 5 (legacy openid), the type no longer changes after rebooting the workstation, and the user stays logged in.

Web UI

+ Users can now upload documents to be printed in the Web UI. This feature is currently available upon request in the Early Access Program.

- When creating an Access control record, the authentication providers dropdown list is now correctly sorted from highest to lowest priority.

- Fixed a problem when the first search after logging in to the Web UI in Mozilla Firefox wasn't working.

- All successfully printed jobs are reported as 'success' in metrics.

Printing

- Direct print jobs are now printed even if they exceed the threshold of 2 minutes.

Konica Minolta IWS Gen 2 Cloud Terminal

- The user experience with scanning has been improved.

- For a booklet with top binding, the orientation is now set to landscape so that the document can be printed correctly.

Ricoh Standard Gen 2 Cloud Terminal

+ You can now configure the card reader PID/VID via the Terminal Deployment Tool.

+ The users now see their full names on the terminal. If the full name is not filled in SAFEQ Cloud, the users will see their usernames.

+ Terminal version is reported to server in login report.

+ The terminal now supports Port 443.

+ You can now select the input tray (limitation removed).

+ Added Norwegian language support.

x Scan app is no longer displayed on Printer-only devices.

- You can now run an instant scan workflow even if its default parameters have invalid values.

- The scan and workflow settings are now scrollable.

- The order of Home and Up folder buttons on the folder browse parameter screen is now correct.

- The terminal uninstallation no longer fails when the terminal was configured to use other authenticaion options than card.

- Scan job accounting endpoint no longer fails with error 500 for unknown user.

- If a document server application scans and the terminal wants to scan simultaneously, a correct error message is displayed.

- Fixed issue where sometimes the "endpoint already exists" screen is misaligned.

- The "Device encountered an issue" error message now has correct spacing.

- After uninstallation from Web UI, the terminal icon no longer remains on the home screen of the MFD.

- When scanning from the glass, the A4 format is now correctly detected; the terminal no longer displays an error message.

- The authentication screen no longer freezes while the terminal attempts to fetch the logo.

4.2.10 BUILD 3.45 [2024-06-11]

Web UI

+ The Embedded clients section displays the buttons for each terminal's available terminal installation options correctly, according to what is supported for the given terminal.

- When a user tries to filter deleted log files, they get the correct error message explaining why the log file is not displayed.

- The keystore loading no longer fails occasionally due to a race condition between the Welcome message and the Reload message.

- Fixed a problem where an authentication provider could not be deleted in some cases.

- Color print jobs submitted to a monochrome print queue are correctly accounted for as monochrome.

- In the Embedded clients section, the Add button is clickable even with a small browser window.

Scanning

- Scan jobs evaluated by OCR as empty documents are now delivered.

Printing

- Universal driver: conversion from XPS to PDF no longer results in a missing font in the document.

- SQTS job accounting endpoint no longer fails with error 500 for unknown users.

Konica Minolta IWS Gen 2 Cloud Terminal

x The "service unreachable" screen has been improved. Now, it always displays the time of the error and the terminal version.

- The Mediatype option is no longer ignored in the download&print scenario while using a pull queue.

- The terminal now indicates that it failed to load the scan workflows available to the user.

HP Workpath Gen 2 Cloud Terminal

- Fixed the slow authentication via PIN.

Ricoh Standard Gen 2 Cloud Terminal (awaiting certification)

- Users now have more than 60 seconds to fill in their username and password when activating an unknown card.

- The terminal no longer breaks the job accounting by trimming usernames.

- The terminal no longer attempts to account copy jobs for UNKNOWN_JOB_OWNER users.

SAFEQ Cloud Client

+ The beta version of SAFEQ Cloud Client with auto-update feature is available for early adopters.

+ The Port Monitor is not reinstalled with every Client update.

+ The update package is not downloaded again if the Client already has it, for example, in case of rollback.

+ Information about update progress is logged to windowsEventLogger.

- If automatic endpoint trust is enabled, the SAFEQ Cloud Client no longer requires manual endpoint authorization.

- Direct offline print no longer fails with SAFEQ Cloud Client 3.43.

- SAFEQ Cloud Client authentication type no longer changes after workstation reboot.

The Mobile app

- Compatibility issues do longer appear after the application update on iOS.

API

- If the request does not contain the "Content-Type: form-data" header, the response status is no longer 500.

Performance and security enhancements

- Since version 3.43, SAFEQ Cloud no longer runs the vulnerable JRE Version 11.0.20.

- The OMNI Bridge no longer goes offline because of OutofMemory error.

- The WebClientCanon vulnerability (deserialization of Untrusted Data in com.fasterxml.jackson.core:jackson-databind) is now resolved.

4.2.11 BUILD 3.44 [2024-05-09]

Web UI

+ The administrator can now see the cloud status and scheduled maintenance.

+ The user's username is pre-filled in the OIDC provider's authentication screen.

+ The administrator is notified about new SAFEQ Cloud version in the Web UI.

x My Profile, My Printers, My Documents, and My Authorizations have been consolidated into two sections (My Documents and My Profile) to improve user experience.

- Fixed an issue where, in specific cases, emails were displayed incorrectly in the Web UI.

- Renamed the "Type of login" to include "Card".

- With the CardManagement role, the users can now edit cards.

Scanning

+ Customers can now use custom SMTP for scan workflows instead of a default service level configuration (Amazon SES or SendGrid).

Printing

- Documents are no longer printed in color if there is a trigger that sets them to B&W.

- All non-local users are now able to print by default.

Konica Minolta IWS Gen 2 Cloud Terminal

x Auto color copy is now supported.

- Fixed the issue when the user could not log in again by card after timeout, not even after waiting for a few minutes.

Ricoh Standard Gen 2 Cloud Terminal

-The installation no longer fails on setting the SP options.

HP Workpath Gen 1 (OXPd) Embedded Terminal

+ The administrator can now configure the terminal from a secondary gateway.

Sharp Embedded Terminal

- Four-hole punching is now working on all devices.

SAFEQ Cloud Client

- The Client no longer has connectivity issues on Mac after it wakes from sleep.

4.2.12 BUILD 3.43 [2024-04-04]

API

x Administrators can now create multiple values per API Access Key, thus streamlining the administration.

x GetAccount API now includes Account UUID.

Scanning

- Fixed issue with SharePoint Connector when scanning to a localized SharePoint destination where column data is not updated.

Printing

x Increased reliability of printed documents with improved document font handling and failover procedures.

Web UI

+ Administrators can now combine the convenience, simplicity, and functions of OIDC and Service Account-based authentication for Microsoft Entra ID and Okta Identity Providers.

- After deleting a secondary server, an internal error is no longer displayed.

- Fixed user group synchronization with Entra ID Single Sign On Authentication causing failure in permissions being applied.- Fixed error incorrectly being displayed when an admin deletes jobs from a queue HBT-4281

- Fixed LDAP authentication for non-Active Directory customers who wish to use userPrincipalName for authentication.

- Fixed Terminal Deployment Tool command generator from creating incorrect commands when a blank password is specified.

Konica Minolta IWS Gen 2 Cloud Terminal
+ Added ID Copy Quick Action to the home screen so that users can now copy ID documents with just one tap.

x Added Finnish and Ukrainian language support.

- Fixed print job synchronization issue causing the terminal to become unresponsive and jobs to be accounted for multiple times.

- Swedish language improvements.

Konica Minolta OpenAPI Terminal

- Fixed log retention for webclientKMOpenAPI.log.

Fujifilm BI Cloud Terminal

- Fixed Edge Erase margin causing grey border to appear on scanned images.

HP Workpath Gen 2 Cloud Terminal

- Card numbers are now stored in decimal format.

HP Workpath Gen 1 (OXPd) Embedded Terminal

- After card swipe, the device UI now displays a loading animation so that users have a better feedback on their authentication request.

- Updated terminal branding and naming to reflecting SAFEQ Cloud brand.

- Fixed a rare scenario which could result in a user being authenticated as the previous user who logged in at the MFD.

Kyocera HyPAS Embedded Terminal

- Fixed issue with LDAP authentication where user1 string is appended to the user's display name.

4.2.13 BUILD 3.42 [2024-03-07]

Scanning

x Users can see the expiration for each failed scan job on the My Documents page, so they know when the document will be deleted.

+ Significant additions to scan connectors and workflows for Konica Minolta IWS, Ricoh, HP Workpath, and FujiFilm BI pure cloud terminals.

+ Users may now search for an email when using scan to email

+ Added Scan to HTTPS scan connector, allowing scanned images and associated metadata to be securely transferred to web services for further processing.

+ Users can set resolution, sides, color, and merging originals (AKA job build) on the MFD panel.

+ Users can now navigate a folder structure when saving documents to OneDrive & SharePoint Online.

+ Users can now enter metadata on the Cloud Terminal. Data types supported include Text, Number, Date, Email, and Select from a List. These metadata fields may be used to name files and provide variable input to scan workflows. For example, a user could enter the document's name and create a folder in OneDrive using the value of the metadata field. These metadata fields may optionally be required to be entered before scanning may proceed.

Konica Minolta IWS Gen 2 Cloud Terminal (version 2024.02.03)

x Added Dispatcher Stratus Single Sign On support. Please note that the availability of this feature is dependent upon Konica Minolta's release to the Konica Minolta Marketplace.

Ricoh Cloud Terminal

x Added link to Native Copy functionality so that a user may utilize the MFD's copier interface.

x Native copy and scan jobs are now accounted allowing more comprehensive reporting.

x Tenant logo is now optionally displayed on the terminal rather than the Y soft logo.

x Scan updates as described above.

Fujifilm BI Cloud Terminal

x Scan updates as described above.

HP Workpath Embedded Terminal

x Scan updates as described above.

This release also contains several performance improvements and bug fixes.

4.2.14 BUILD 3.41 [2024-02-08]

Scanning

+ Added additional Scan Workflow processing steps, including barcode recognition, page separation, and highlighted text extraction and redaction.

x Updated OCR engine for improved document recognition performance.

Web UI

x Added target Server Name to Server Information page to improve the administrator's user experience.

x Added a "search" filter to the Embedded clients deployment page for ease of administration.

x Added Server mode to the Server Information view, allowing admins to differentiate between Primary and Secondary Servers easily.

- Improved user data synchronization with Microsoft Entra ID (Azure).

FUJIFILM BI Cloud Terminal

+ Before releasing a print job, the user can now define print settings at the MFD.

- When printing from the native Fuji driver, print jobs no longer fail because of waiting for the header data.

- Improved user feedback with clear error messages when browsing external directories.

Konica Minolta IWS Cloud Terminal

+ The users can now change the print job finishing options at the MFD (number of copies, mono/color, duplex/simplex options, etc.).

Konica Minolta OpenAPI Terminal

- Fixed authentication issue occurring during specific installation rollback scenarios, causing incorrect user logins.

- Removed sensitive user data from webclientKMOpenAPI.log.

HP Workpath Embedded Terminal

+ Administrators can now view a user's Print, Copy, and Scan transaction data.

+ Users can now delete their waiting print jobs at the MFD.

+ Added the ability to display the custom tenant logo on the terminal.

+ A user can refresh the print job list and see print jobs that have been printed since logging in at the MFD.

+ Users can change the print job finishing options at the MFD, including color/mono, duplex/simplex, number of copies, and tray selection.

+ Added advanced scanning features such as duplex/simplex, merging originals, color/mono, email selection, and folder browsing.

API Enhancements

+ Added a get user by username endpoint.

+ Page orientation now respects the request specified in the API request.

4.2.15 BUILD 3.40 [2024-01-15]

Printing

+ Added the ability to set a trigger condition based on the number of pages in a document.

- Print jobs that are converted from mono to color based on a trigger are now correctly accounted for.

- PDFs without a default page size parameter are now printed correctly.

- Guest printing from the mobile app now works when 'enable token access' is enabled.

Web UI

+ Added a new Quick Start panel menu guiding admins to set up push printing in a fast way.

+ Admins can now anonymize sensitive end-user personal information in the dashboard, reports, and all related interfaces.

+ Page separation is now available as a processing step in scan workflows.

x Redesigned the Add and Edit Printers menu to simplify configuration tasks.

x Added the ability to filter Printers and Embedded Terminals by name, printer address, or serial number.

+ Added languages: Portuguese, Brazilian Portuguese, Japanese, Simplified Chinese, Danish, Norwegian, Swedish, Thai, Indonesian, Malay, and Korean.

- Account names taking up more than one line no longer prevent the admin from scrolling to the bottom of the navigation menu.

- Changed the font used for one-time API key display to ensure letters are distinguishable.

- Rectified UI language when displaying print job submission times.

Scanning

+ Added page separation as a processing step to scan workflows.

Partner Hosted and On-Premises installations

x Upgraded PostgreSQL version. Due to the nature of the improvement, we removed the auto-updating function of existing PostgreSQL versions for Partner Hosted and On-Premises installations.

Secondary Gateway

x Upgraded PostgreSQL version and removed auto-update of existing instances due to upgrade reliability concerns.

SAFEQ Cloud Client

x Removed the need to authorize SAFEQ Cloud Clients installed using the preconfigured installer.

- On macOS, users don't need to enter their credentials after a reboot anymore.

- Printer synchronization no longer fails when using authentication types with the domain suffix appended.

API

- The Document history endpoint now returns the jobtype property.

- The use of full API access keys is now discouraged to enhance security.

- Whenever the API returns a 403 error due to missing permissions, it also returns the list of the missing permissions.

Fujifilm BI Cloud Terminal (terminal version 1.9.0)

+ The terminal can now display the tenant logo.

+ Added Quick Action scan workflows for end-user efficiency.

+ Added languages: Norwegian, Swedish, Thai, Indonesian, Malay, and Korean. Note that this requires validation by Fujifilm. The estimated completion is mid-January.

- When the terminal is loading OneDrive and SharePoint scan destinations, the user is informed about what is happening.

Konica Minolta IWS Cloud Terminal

x The Dispatcher Paragon branded KM IWS terminal is now published under Production Solution Key.

- The brand versioning is now unified, and this is reflected in the terminal version to ensure proper discoverability.

-Scan and copy jobs are properly accounted for.

- Improved efficiency of releasing many print jobs at once.

+ Added languages: Norwegian, Swedish, Thai, Indonesian, Malay, and Korean. The terminal is released to Konica Minolta. Country-level availability is based on Konica Minolta release processes.

HP Workpath Cloud Terminal (Gen2) (terminal version 3.40.0)

x Added the ability to log, display, and report the installed terminal version. Note that the terminal requires validation by HP. The estimated availability is mid-February.

Sharp Embedded Terminal

- After enrolling their cards, users are no longer stuck on the enrolment page.

Mobile apps

+ The iOS and Android mobile apps now support OAuth authentication.

4.3 2023

The following contains a list of notable changes in YSoft SAFEQ Cloud.

Legend:

+ Added feature
x Improved/changed feature
- Bug fixed

4.3.1 BUILD 3.39.7 [2023-12-01]

Primary Server
- Added authentication performance enhancements.
- Fixed PDF print over IPP affecting bespoke configurations.

4.3.2 BUILD 3.39.5 [2023-11-27]

Primary Server
- Introduced caching to address slow requests for selected secondary server deployments with LDAP authentication enabled.

4.3.3 BUILD 3.39.3 [2023-11-24]

Primary Server
- Optimized User Authentication Caching.
- Optimized document retry tasks for improved performance.
- Optimized automation tasks.
- Added additional metrics logging.

4.3.4 BUILD 3.39 [2023-11-02]

Web UI
x Improved user experience of the Print queues menu.
x Moved SAFEQ Cloud Client download to My profile screen so that the end users can access the pre-configured SAFEQ Cloud Client.

x The Server information tab for a Secondary Gateway was redesigned for easier administration and configuration.
- When clicking a server in the left navigation menu, the server details are now displayed correctly.

PC Client

x The SAFEQ Cloud Client now performs printer synchronization less often.
- Silent install sets all parameters correctly when color, duplex, or paper size is specified.
- The SAFEQ Cloud Client is updated with Ghostscript 10.02 to resolve the CVE-2023-38545 and CVE-2023-38546 vulnerabilities.

Authentication

x Added the ability to track how long authentication takes for specific authentication providers if a user is authenticated by multiple of them.
x OIDC is now compliant with RFC 8414.
- For customers with multiple authentication providers, the amount of SAFEQ Cloud Client failed authentications has been decreased.
- Azure AD authentication provider now handles custom extension attributes correctly.

Scanning

- When disabled, the OCR Output parameters are not saved in the workflow settings in the SAFEQ Cloud Web UI.
- The Reorder button is now visible only to users with ModifyScanWorkflow permission.

Performance

x To further reduce the load on DB, calls to UserFacade are cached (especially the findByName method that is used in hot queries).
- NullPointerException no longer occurs in the document facade when the document is linked to a non-existent printer or provider ID.

Ricoh Cloud Terminal (Gen2)

+ Users can select one or multiple jobs for deletion.
+ User can manually refresh the job list while at the MFD.
+ The Job list shows job attributes (Colour/B&W, Number of pages, Number of copies).
+ The terminal deployment via Secondary Gateway has been improved.
+ The terminal can be deployed via the Ricoh App Store (Pending availability on the Ricoh App Store).
+ The terminal can be manually configured at the MFD by an admin as the admin now can enter the Domain and the API key manually.
+ The terminal installation status is shown in the SAFEQ Cloud Web UI.
x A meaningful error message is shown when job retrieval fails.
x The Registration and Authorization messages are now brand-neutral.
x Admin gets proper feedback when entering wrong credentials during uninstallation on G2 devices.
x The automatic user logout now works correctly when the MFD goes into sleep mode.
x Users without rights to print can no longer open the print application on G2 devices.
x Admin users can now log in using the native login button as this button redirects them to the authentication screen.
x During terminal uninstallation, the User Authentication Management is set back to OFF.
x If entering credentials during card activation times out (takes over 60 seconds), the user is returned to the login screen instead of being shown the error message "You have placed unknown or damaged card."
x The RXOP library is updated to version 3.8.8.
- Fixed issue with jobs taking too long to print if PJL headers are not present.

- Fixed issue with jobs being released from Secondary Gateway storage showing error Status code 404.
- The terminal no longer crashes during manual installation.
- SP option SCAN_SETTINGS__PRINT_DELETE_SCANNER_JOURNAL is correctly set on installation so that scanning is not blocked when the device scan journal is full.
- G2 devices no longer require a manual reboot after terminal installation.

HP OxPD Terminal
- The page count is correct when printing multiple copies of a print job sent via IPP Pull Print to an HP MFD with OxPD terminal.
- When a document is not printed within the maximum expected wait time after a user taps Print, the document's release is canceled.

Konica Minolta IWS Cloud Terminal
x Scan jobs can be merged when the Merging originals option is enabled in the scan workflow settings.
x Added the support for booklets.
- The terminal respects stapling when using pull print.

Konica Minolta OpenAPI Terminal
- When using the KM PCL6 Universal Print driver, the page count is displayed correctly.

FujiFilm BI Cloud Terminal
x The users can now use basic workflow settings at the MFD.

4.3.5 BUILD 3.38 [2023-10-05]

Printing
- Fixed issue on secondary servers causing documents to be rejected when using offline caching.
- Delegated print jobs can now be released at Pure Cloud Terminals.
+ Added the ability to set the default page size per print queue.

Scanning
- Removed SMTP configuration from Embedded client configuration for Pure Cloud terminals, as this setting is unnecessary.
- Added exception information to WPS logs for failed scan processing jobs.
- Added validation for SharePoint connector where Target SharePoint online library is a required field.
x Added the ability to download failed scan jobs.

Web UI
- When clicking on the documentation link, the admin is directed to documentation branded for their variant of the product.
x The theme of the login screen is now modifiable, and the navigation in the tree structure is improved.

Chrome Extension
- Chrome extension no longer removes printers and configuration when clicking test or when a blank api field is used.

Mobile apps
- Removed dependency on external barcode scanning app by embedding its functions in the Android app.

- Print jobs submitted via the Mobile apps can now be released on KM Cloud Terminal even if they originally did not contain PJL headers.

Fujifilm BI Cloud Terminal
- Scanned documents are correctly accounted for even if the user uses the native copy application.
x Added the ability to print booklets.
x Added ability to account for scanned documents.

Canon Embedded Terminal
- The login screen no longer freezes after attempting to log in with invalid credentials.

Sharp Embedded Terminal
- The terminal can now display more than ten print jobs.

Xerox Embedded Terminal
x Login at Xerox Embedded Terminal no longer fails when secondary servers are configured with multiple CPUs.

Konica Minolta IWS Cloud Terminal
x Direct print jobs no longer create duplicate entries in the printed documents list.

API
x Added the ability to manage access rights.
x Improved security of document history API by adding role-based access.
x Increased security by only displaying API keys once when generated. The ability to view existing API keys is removed.

4.3.6 BUILD 3.37 [2023-09-07]

Scanning
+ SAFEQ Cloud Web UI updated so that administrators can see that they can use workflow variables in workflow fields.
x Scan files that failed during workflow processing are stored for 7 days and can be downloaded from My Documents in the SAFEQ Cloud Web UI.
x Improved notifications for administrators when a scan job fails.
- A user who has not yet submitted any print jobs can see My Authorisations in the SAFEQ Cloud Web UI and can authorize connections to Microsft365 applications.

Konica Minolta IWS Cloud Terminal
+ New Konica Minolta Terminal for Konica Minolta IWS devices.
+ Cloud printing with no requirement for a Secondary Gateway.
+ Users can log in to the MFD via username and password (or OTP), PIN, or card.
+ Users can register their card at the Cloud Terminal terminal.
+ Users can access Print and Scan workflows in Quick Actions upon login.
+ Users can select and print one or multiple jobs with finishing options applied at job output.
+ Print jobs can be released from any configured storage location (SAFEQ Cloud Client, Cloud, or Secondary Gateway storage) and will be routed to the MFD in the most efficient way.
+ Users get feedback on print job status (e.g., Waiting, Printing, Downloading, Downloaded and Printing).
+ New scan workflows are available in the Cloud Terminal UI.
+ Users can scan to email, Microsoft OneDrive, and Microsoft Sharepoint.
+ Users can access Quick Copy from My quick actions screen.
+ Administrators have instructions for deployment in the Embedded configuration section of the

SAFEQ Cloud Web UI.
+ Administrators can set configuration options for the terminal.
+ Administrators can register the cloud terminals in SAFEQ Cloud.
+ Administrators can install the Cloud Terminal from Konica Minolta Marketplace
+ Administrators can pre-configure multiple MFDs for installation from Konica Minolta Marketplace.
+ Logs are stored on the MFD and can be retrieved remotely via Konica Minolta Marketplace.

Ricoh Cloud Terminal
+ Ricoh Gen2 terminal can be deployed from the Secondary Gateway.

Fujifilm BI Cloud Terminal
+ Users can delete print jobs at the terminal.
+ Copy and scan jobs are accounted for and can be viewed in the SAFEQ Cloud Web UI in Reports.

Sharp OSA Terminal
- The Print button is no longer hidden behind print jobs when there are multiple jobs in the list.

HP OXpD Terminal
- A new option was added to SAFEQ Cloud Web UI to enable driver (sotware) copy collation so that printing multiple copies works correctly.

Public API
- Adding authentication providers using API (/authproviders) now works correctly.

Authentication
- Azure AD client now handles the AAD on-premise extension attributes in a special way so that administrators can store card numbers stored in Custom Attributes (e.g., extension attributes such as extensionAttribute1).

SAFEQ Cloud Web UI
x The action buttons in the top menu bar are now grouped.
x Workflows now open in edit mode by default, reducing the number of steps required to create or update configuration items.
- Certificate expiration dates are now displayed correctly.

OMNI Bridge
x Landing page from the device's QR code is used to enroll the device in SAFEQ Cloud.

SAFEQ Cloud Client
+ Administrators can download the SAFEQ Cloud Client from the Print queues section of SAFEQ Cloud Web UI.
x The SAFEQ Cloud Client icon now has neutral branding.

Server
- Fixed intermittent authentication issues in EU due to connecting clients overloading the cluster after restart.

Localization
- Updated incorrect French translations for ID in Users.
- Updated incorrect Dutch translation of About in SAFEQ Cloud Client.

Security
x Updated backend API key security.
x Added AUD (audience) claim to API access tokens for improved security.
x Updated JRE version to Version 11.0.20

4.3.7 BUILD 3.36 [2023-08-10]

Scanning
+ Documentation link added to the navigation bar.
x User and admin are notified if workflow processing fails to start.
- OCR improvements for large jobs.
- In scan workflows, it is now possible to change the *From* address.

Web User Interface
x Alerts moved to Overview.
x Admins can see the status of the gateways in the Web UI.
x Cloud Terminal Installation status is displayed in the Web UI.
- Corrected French translations.

SAFEQ Cloud Client
+ Added text with the Client's status next to the Client's icon.
x Simplified the installation and configuration of the Mac Client.

Konica Minolta IWS Embedded Terminal (This feature is in testing, not general production)
+ The terminal now has the scanning functionality.
x Print jobs are delivered more effectively.

Terminal Deployment Tool
- The password parameter is now always visible in the command.

HP Workpath Cloud Terminal (Gen2)
- The terminal now supports Y Soft Card Readers.

4.3.8 BUILD 3.35.2 [2023-07-25]

Core
- Fixed issue related to automation tasks resulting in reduced server performance.

4.3.9 BUILD 3.35.1 [2023-07-19]

Ricoh Cloud Terminal (Gen2)
- Fixed issue during card enrollment for new cards displaying the unknown or damaged card error message.

4.3.10 BUILD 3.35 [2023-07-13]

Printing
+ SAFEQ Cloud Client now has the ability to send a username to the MFD when the print protocol is IPP.
- Improved speed of print job display for embedded terminals connected to YSoft OMNI Bridge
- Cloud Terminals can now print correctly when the selected paper size is Ledger.

Scanning
+ Administrators can add scan metadata to Sharepoint Scan workflows.
+ Administrators can configure file overwrite behavior for OneDrive and Sharepoint Scan workflows.

SAFEQ Cloud Web UI
x Improved user experience of creating new Partner or Customer accounts.
x Improved user experience of creating new Printers and Print Queues.
- Fixed issue when all advanced OCR features are enabled simultaneously.

SAFEQ Cloud Client
x Added auto-configuration for the OIDC authentication provider when installing the SAFEQ Cloud Client.
- The SAFEQ Cloud Client for macOS now includes the user's domain name when using the Store and deliver via gateway option.

Ricoh Cloud Terminal (Gen2)
- Uninstallation of the terminal does not freeze when the admin enters an incorrect device password.
- After uninstallation of the terminal, the User Authentication and Administrator Authentication options are set back to "Off" on the MFD.

HP Workpath Cloud Terminal (Gen2)
x Improved status messages when releasing print jobs at the MFD.

Konica Minolta Embedded terminal
- Fixed deployment of KM Open API for devices located in the US region.
- Fixed KM IWS card login issue when Enforce API Token access is enabled.

Sharp Embedded terminal
- Scrolling through the print job list is no longer slow.

4.3.11 BUILD 3.34 [2023-06-26]

Ricoh Cloud Terminal
+ New Ricoh Cloud Terminal for Ricoh SOP devices
+ Cloud printing with no requirement for Secondary Gateway
+ Users can select one or multiple jobs for printing
+ Users get feedback on print job status (e.g., Waiting, Printing, Downloading, Downloaded and Printing)
+ Print jobs can be released from any configured storage location (SAFEQ Cloud Client, Cloud, or Secondary Gateway storage) and will be routed to the MFD in the most efficient way
+ Users can view recently printed jobs in the Cloud Terminal user interface
+ New scan workflows available in the Cloud Terminal user interface
+ User can scan to email, Microsoft OneDrive, and Microsoft Sharepoint
+ Users can merge multiple documents into a single scan job
+ Users can log in to the device using username and password (or OTP), PIN, or card
+ Users can access scan and print workflows from a single interface
+ Users can register their card at the Cloud Terminal terminal

HP Workpath Cloud Terminal
+ New HP Workpath Cloud Terminal for HP Workpath devices
+ Cloud printing with no requirement for Secondary Gateway
+ Users can select one or multiple jobs for printing
+ Users get feedback on print job status (e.g., Printing, Downloading and Printing)
+ Print jobs can be released from any configured storage location (SAFEQ Cloud Client, Cloud, or Secondary Gateway storage) and will be routed to the MFD in the most efficient way
+ Users can view recently printed jobs in the Cloud Terminal user interface

+ Users can delete print jobs from the Cloud Terminal user interface
+ New scan workflows available in the Cloud Terminal user interface
+ User can scan to email, Microsoft OneDrive, and Microsoft Sharepoint
+ Users can merge multiple documents into a single scan job
+ Users can log in to the device using username and password (or OTP), PIN, or card
+ Users can access scan and print workflows from a single interface
+ Users can register their card at the Cloud Terminal terminal

Fujifilm BI Cloud Terminal

x Updated Fujifilm BI Cloud terminal
+ Cloud printing with no requirement for Secondary Gateway
+ Users can select one or multiple jobs for printing
+ Users get feedback on print job status (e.g., Waiting, Printing, Downloading)
+ Print jobs can be released from any configured storage location (SAFEQ Cloud Client, Cloud or Secondary Gateway storage) and will be routed to the device in the most efficient way
+ Users can view recently printed jobs in the Cloud Terminal user interface
+ Users can delete print jobs from the Cloud Terminal user interface
+ New scan workflows available in the Cloud Terminal user interface
+ User can scan to email, Microsoft OneDrive, and Microsoft SharePoint
+ Users can merge multiple documents into a single scan job
+ Users can log in to the device using username and password (or OTP), PIN, or card
+ Users can access scan and print workflows from a single interface
+ Users can register their card at the Cloud Terminal
x Support added for additional devices (ApeosPort VII gen2 devices) – see the Compatibility List for full details

HP OXPd Embedded terminal

x Improved user interface for HP OXPd embedded terminal
x Streamlined card enrolment workflow by removing pop-up after card swipe
x User login screen reconfigured for ease of use
x Text formatting updated for improved readability
- Fixed login/card enrolment UI for better usability on devices with small screens
+ Baltech card readers can be used with HP devices

Sharp Embedded terminal

- Users can now authenticate after Secondary Gateway was restarted. The MFD must be rebooted after the server update for the fix to be applied.
- Fixed potential vulnerability

Scan Workflows

NOTE: The Scan workflows feature (scan to email, SharePoint, and OneDrive) is available only in the Y Soft-hosted cloud environment and only with pure cloud terminals (FUJIFILM BI, Ricoh, HP Workpath).
+ New scan workflows can be configured for Scan to Email
+ New scan workflows can be configured for Scan to OneDrive
+ New scan workflows can be configured for SharePoint
+ Users can authorize access to their Microsoft 365 storage services (OneDrive & Sharepoint)
+ OCR can be configured for scan workflows
+ The available output formats for scan jobs are: PDF, JPEG, TIFF, Multipage TIFF, Compact PDF, Searchable PDF, docx, xlsx, xls, pptx, txt, rtf, PDF/a-1a, PDF/a-1b, PDF/a-2a, PDF/a-2u, PDF/a-3a, PDF/a-3u
+ PDF MRC Compression can be set for scanned files
+ PDF encryption can be set (automatic or manual password generation)

+ Image optimization can be applied (Dual page splitting, Blank page removal, Detect page orientation, Despeckle pages)
+ Merging originals can be enabled/disabled
+ Document preferences can be applied by workflow (Resolution, simplex/duplex, colour/B&W)
+ Static or variable metadata can be set by workflow for subject, body, and filename

Authentication Providers
+ Auth0 added as a new authentication provider
+ Users can authenticate at SAFEQ Cloud Client with Auth0 credentials using OIDC
+ Auth0 groups can be synchronized and used for Access Control

External Card Repository
+ External card repository option is available in Authentication providers so that customers can use the custom external card repositories integration with SAFEQ Cloud

Secondary Gateway
+ SAFEQ Cloud Gateway can be deployed to YSoft OMNI Bridge (an edge device) from Endpoints in SAFEQ Cloud Web UI
+ Admin Authorisation workflow and automated download and installation of Secondary Gateway can be initiated from Endpoints

SAFEQ Cloud Client
x A5 page size can be set as the default paper size in unattended installations of the SAFEQ Cloud Client in addition to A4 and US Letter

Print Driver
x SAFEQ Cloud job renderer updated to include support for Epson PCL6 and PS devices correctly applying finishing options

User Interface
- Feedback and error handling improved when the admin does not fill out all required fields in SAFEQ Cloud Web UI configuration screens

4.3.12 BUILD 3.33 [2023-05-18]

FujiFilm BI Embedded
+ Updated UI with simplified installation steps for deploying embedded terminal.
x Added ability to set up FujiFilm BI terminal for push print with Output Type "PDF" (no requirement for Postscript to be installed on MFD).
x Added ability to deliver print jobs in the most efficient way from any configured storage (e.g. jobs will be routed directly from PC Client to the MFD if available, otherwise they will be routed via the cloud).
x Card plugin and card service will always be installed.
- Job list order fixed in the terminal UI so that the most recent jobs are at the top of the list.
- Finishing options (Punch & Staple) are now working when using push print with FujiFilm BI devices.

Mobile Apps
+ Enhanced iOS and Android apps and HP Workpath terminal with user_token security.

API
x Added printer information to Documents History API.
- Fixed issue with Access Control List (ACL) inheritance properties when updating ACL via API.

PC Client
- Fixed issue with user being logged out from PC Client for Mac when the client is offline when refreshing OIDC token.

Single Driver
- Fixed issue with landscape documents in non-standard formats (e.g. envelope, ledger, check, etc.) being incorrectly rotated when staple or punch is applied.

Authentication
- Fixed issue with users being unable to authenticate when duplicate group names exist in Google Workspace authentication providers.

Web UI
- Fixed issue with Date/Time picker text being obscured by the cursor when hovering in Reports UI.

4.3.13 BUILD 3.32 [2023-04-25]

Ricoh SDK/J Legacy Embedded
- Ricoh legacy embedded terminal works again after removal of an expired Ubiquitech certificate from the truststore.

FujiFilm BI Cloud Embedded
+ Advanced finishing options defined by user when submitting the print job via {ShortProductName} PC client are respected when the user releases the job at the FUJIFILM BI Cloud terminal.
+ Added Quick scan workflows.
+ Scanning added to Quick action screen.
+ Unified Embedded UI.
+ FujiFilm BI Cloud Terminal UI is unified with other Cloud Terminals.
+ Added card activation at Cloud Terminal.
- Card activation at the Cloud Terminal is now possible.
- Simplex push print is now working.
- Visual bug removed from the UI.
- With a long Fullname, the Logout button is displayed correctly.

Lexmark Embedded
- Card self-registration is now possible for Local users at Lexmark MFDs with YSoft card reader.

Public API
+ {ShortProductName} API endpoint date/time matches the actual job release date/time.
- Documents/history API endpoint is filtering for the "PRINTED" status.

Authentication
- Authenticated users are now prevented from printing jobs of other users via job ID tampering.

Web Client
- The text in the middle panel retains a proper color.

Chromebook extension
- Removed fallback to email authentication when "disableAuthentication" is enabled. Users can only authenticate via token ID.

FMV-Specific Development
- Canceling pending documents is working as expected.

4.3.14 BUILD 3.31 [2023-03-25]

FujiFilm BI Embedded
+ Added the possibility to refresh pending jobs.
+ Added ability to receive simple scan jobs via SwA in SAFEQ Cloud.
+ Fujifilm BI terminal can now release print jobs directly from the cloud.
+ Streamlined installation of the embedded terminal.

Xerox Embedded
- After registering a card with OTP, an "Authentication failed" message is displayed, and users must log in again.

HP OXPD Embedded
+ Enhanced UI

Public API
+ Customer can get information on users' group membership via Public API.

Card Registration
+ Enhanced Refo script allows inactive user cards to be used again.

Admin
+ Improved UX for a better admin experience.
+ Improved Dashboard in web UI.
- In SAFEQ Cloud web UI, the colors in the middle of the panel are not turning gray.

SAFEQ Cloud Android App
- Y Soft App does not overwrite the setting from duplex to simplex.

Web Client
- KM Web Client session at MFD can not be hijacked by other users from a web browser.
- Sharp Web Client session at MFD can not be hijacked by other users from a web browser.

PC Client
- PC Client 3.27 is not randomly logging users out.
- Chrome extension does now sync with Email auth and GSuite.

Message service
- The number of characters in messaging template was increased.

4.3.15 BUILD 3.30 [2023-03-01]

Fujifilm BI Embedded
x Added support for Fujifilm BI embedded terminal.

HP WorkPath Embedded
+ Updated HP Workpath Embedded to version 3.29 (check the documentation for update requirements).
- Enhanced HP WorkPath with user_token security (check the documentation for update requirements).
- Added print options button.

- Fixed changing subject and filename when scanning to show updates while typing.
- French UI update.
- Correction in French localization.

KM IWS Embedded
+ Updated KM IWS terminal to version 3.30.
- Fixed Card swipe becomes irresponsive after the "Back" button is pressed during card registration.

KM OpenAPI Embedded
- Added Security enhancement against XSS attack.

Xerox Embedded
- Fixed error during login for Xerox Altalink devices.
- Jobs are correctly displayed in print queue.

Authentication
- Fixed error message when logging in at printer with card ID imported from common Azure AD attribute.
- Fixed "400 Bad Request" Azure Graph API call error when utilizing custom fields for card ID mapping.

Public API
- In document history, documents are recorded under correct device when the jobs are sent with the "serialnumber" parameter.

PC Client
+ Added option for PC Client to enable custom port monitor instead of IPP.
- Wrong copyright year display in windows client.

SAFEQ Cloud Server
- Fixed correct sorting of job list if requested through "jobs" endpoint.
+ Updated logic so that administrators can't enable WPS on Secondary Server.

4.3.16 BUILD 3.29 [2023-02-03]

PC Client
x Added Czech, Slovak, and Polish language support.
- PC Client 3.27 no longer logs the user out when switching to offline mode during token refresh.
- Fixed the certificate-related connectivity issues when upgrading from versions older than 3.15.
- Fixed memory error on shutdown related to Windows network events handler incorrectly deregistered upon application termination.

Server
x Added Czech, Slovak, and Polish language support.
- Workflow Processing system (WPS) service is now hidden behind a feature flag.

Driver
x Added Czech, Slovak, Portuguese, Polish, and Swedish language support.

KM Open API
x Added Czech, Slovak, Portuguese, Polish, and Swedish language support.
- Fixed the issue with "Internal server error" displayed when the device can't print.

KM IWS
- Card swipe now stays responsive after the "Back" button is pressed during card registration.
- Password containing the "&" character no longer causes failure during card registration.
- Jobs with empty names no longer trigger error messages.

Sharp OSA
x Added Czech, Slovak, Portuguese, Polish, and Swedish language support.
- The users are no longer redirected back to the login screen after logging in.
- Punch function is now working for 4 holes on Sharp.

Ricoh SOP
- Print jobs containing both A4 and A3 pages are printed correctly using their respective formats.

HP OXPd
x Added Czech, Slovak, Portuguese, Polish, and Swedish language support.

4.3.17 BUILD 3.28.2 [2023-01-16]

API
x Enhanced internal API token access control security.

HP OXPd Embedded
- Enhance escaping of invalid characters from document titles.
- Fixed issue with installation failing in specific model configurations with a non-derived FaultException.
- Fixed issue where in some configurations card reader PID/VID issue would occur after sending configuration to device.

4.4 2022

The following contains a list of notable changes in YSoft SAFEQ Cloud.

Legend:

+ Added feature
x Improved/changed feature
- Bug fixed

4.4.1 3.28 [2022-12-15]

API
x Device code workflow requests changed from GET to POST.
x Device code workflow: the public/private keys are optional now.
x Simplified registration of new endpoints (printers, gateways, software clients, etc), usage of client-side keys is now optional.

PC Client
+ Added ability to install PC Client in local storage mode while being offline.
x PC Client is now compatible with cloned Windows images.
x Implemented offline mode registration in the core service.
x Added offline mode selection in the installer.
x The default paper size for printers is set based on the user-selected locale.
x Temporary files are now written in the service data directory instead of the Windows temp

directory.
x Added client UUID display in the about dialog.
x Added authentication type in the service setup dialog.
- Fixed trigger execution when custom capture variables are used.
- Fixed PC client Windows installer UI on HiDPI displays.
- Fixed compatibility with IWS cloud print.

Lexmark
+ Added Lexmark eSF7 device compatibility.
x Implemented alternative Login method.
x Home screen displayed after authentication on Lexmark.
+ Added Refresh Button for Lexmark Job List.

4.4.2 3.27.3 [2022-10-08]

Core
- Fixed a problem with PC client and gateway communication when they reconnected to the same cluster node

4.4.3 3.27 [2022-10-06]

API
x Prevent locations being created/updated using wrong values

Brother
+ Added uninstallation option for Brother application
+ Advanced scanning options added
+ Automation of IP Setup configuration
x Removed IP address from Scan2Email subject
x Improved UI for copy & scan options
x Improved error message on login fail
x Improved reporting for scanning

Core
x Enhanced security for channel messaging on secondary servers

Licensing
- Resolved crashing of license counter update

PC Client
x Prevent users from printing once logged out
x Reinstated ability to switch to PDFA setting

Security
x Prevent login of unauthorised users to Primary Gateways via URLs

UI
+ Addition of confirmation window when entering non-unique printer address

UniDriver
+ New Paper Size: 170mm (width) x 210mm (length)

4.4.4 3.26.1 [2022-09-30]

Core
- Resolved connectivity issue between PC Client & Gateways

4.4.5 3.26 [2022-09-08]

API
+ Add Owning Container ID for Input Ports & Outputs Ports

Authentication
x Improved token refresh for multi domain Azure authentication providers
- Resolved Ricoh SLNX card enrolment error using OTP

Core
x Correct routing of print jobs to device where it shares an IP address with another device

Installer
+ SAFEQ Cloud ARMv7 Support to accommodate future integration with YSoft hardware devices

KM OpenAPI
x Code cleanup to improve maintenance & scalability
x Replaced legacy API EasyTools with CoreAPI
x Removal of old login screens from being displayed
x Prevention of app crash when delete/refresh/print buttons are pressed multiple times

PC Client
x Resolved unnecessary sync events due to PC network changes

Sharp
+ Upgrade to Sharp OSA 6
+ Auto population of installation forms on deployment
+ Pop-up for credential validation on card authentication
+ Display "Logging in" message on submission of authentication
+ Add button to release multiple PullPrint copies
x Display home screen on login if no pending jobs exist for the user
x Prevent button press whilst Print Job List is being refreshed
- Prevent multiple logins on authentication

4.4.6 3.25 [2022-08-04]

Authentication
+ Deletion of Azure/LDAP user records via SAFEQ Cloud Web UI

Lexmark
x Use of SAFEQ Cloud CA generated certificates
- Resolved device crash upon card enrolment

PC Client
x Improved authentication token refresh following extended offline periods

Reporting
+ Group & Department information available in Job History Reports API

API
+ Display Domain ID for listing Containers, Input Ports & Output Ports
+ Display Location for listing Containers

Authentication
+ Multi domain support for authentication providers
+ Use refresh tokens for service accounts for Azure Authentication
+ SSO support for Strict Domain Validation

4.4.7 3.24.1 [2022-07-22]

Security
- Reinstate TLS ciphers removed in 3.24 to support PC Clients run on older versions of Windows (8.1 & 12)

4.4.8 3.24 [2022-07-12]

API
+ Display Domain ID for listing Containers, Input Ports & Output Ports
+ Display Location for listing Containers

Authentication
+ Multi domain support for authentication providers
+ Use refresh tokens for service accounts for Azure Authentication
+ SSO support for Strict Domain Validation

KM IWS
+ Italian Language Support
+ Audio feedback on button press
+ Duplex & Stapling options for Copy function
+ Support for Develop devices
x Removal of Zoom option from Copy function
x Improved error message for incorrect copy options
x Increased timeout for printing to accommodate large print jobs
- Resolved Chrome Extension printing issues

KM OpenAPI
+ Removal of file names on URLs when accessing files on application
x Cookie-based tokens updated to use "http-only"

Kyocera
x Support for smaller screen devices
- Resolved 500 error when switching customers on the same vendor
- Resolved 404 error on device restart

Rendering Engine
+ Booklet printing for Ricoh Devices

Security
+ TLS 1.3 Support
x Disabled TLS 1.0 & 1.1 on port 9444
+ Update of TLS ciphers to address reported TLS vulnerabilities

UniDriver
+ Support for paper size 180mm (width) x 210mm (length)

4.4.9 3.23.1 [2022-06-16]

PC Client
x Remove the requirement for case sensitive domain names for PC Clients in local storage mode

4.4.10 3.23 [2022-06-08]

Authentication
x Prevent multiple authentication attempts for incorrect credentials
- Resolved OTP login locking Azure account on multi node environments

Core
x Upgraded handshake protocol between Primary & Secondary Gateways

PC Client
x Update handshake protocol with gateways for local storage mode
x Prevention of printing for accounts with expired licenses

Xerox
-Resolved configuration error when deploying to Xerox Altalink devices

4.4.11 3.22.1 [2022-05-20]

Sharp
- Resolved critical error with application not being operable

4.4.12 3.22 [2022-05-12]

API
x Update of Input & Output Ports via Public API now possible with id field
- Resolved issue with deletion of accounts & containers in Public API

Authentication
x Replaced MS Azure ADAL with MS Azure MSAL

Brother
+ Duplex & Color copy options
+ Advanced options for Duplex, Color & number of copies for print & copy jobs
+ Print job list is refreshed each time it is accessed
+ Copy statistics available in SAFEQ Cloud Web UI Reports
x Configuration lookup now performed under address 127.0.0.1
- Resolved issue with card enrolment with Azure Oauth2
- Resolved issue with username & OTP authentication with Azure logins
- Resolved an issue with the copy function instability

Core
x Updated logic for gateway certificate expiration check
x Additional logging added for time out events

Embedded Clients
- Resolved issue with Install & Configure not working as expected

HP OXPd
x Print jobs are no longer displayed on the print job once complete

Kyocera
- Resolved issue with 500 error displaying after authentication

Lexmark
- Resolved issue with slow authentication & print jobs
- Resolved local user being deleted after embedded application installation

PC Client
+ 1-click download of PC Client logs & configuration
x Updated installer screens to have consistent language for fields required
- Resolved scaling issue on Installation Configuration window
- Resolved token expiration notification not displaying

Sharp
x Configuration lookup now performed under address 127.0.0.1
x Card enrolment timeout increased to 120 seconds

UI
+ Reset Child Permissions option for Account Control added

UniDriver
- Resolved renderer failure error

Xerox
x Updated Java Spring library to latest version
- Resolved issue with IPP printing

4.4.13 3.21 [2022-04-05]

Authentication
- Resolved issue with LDAP not working over SSL for containers

Brother
x Display the PullPrint application even if there are no jobs pending
x Display of username on application for local users
x Ensure all print jobs are removed from the job list once complete
x User is automatically logged out if the device is powered off
- Resolved an issue with the copy function not loading
- Resolved an issue with "print or delete queued jobs" button disappearing

Chrome Extension
+ Checking for internet connection before attempting to connect to SAFEQ Cloud server
+ Warning message if there is no connection
+ Windows style notifications from Chrome Extension for desktop
x Allow authentication by either PC Client or GSuite credentials
x Improved messaging if invalid credentials are input on login

HP OXPd
- Resolved a 500 error appearing on pressing delete multiple times

KM OpenAPI
- Resolved card enrolment not working with username & password/OTP

Performance
x Update to performance of job retrieval function for Ricoh SLNX, HP Workpath, KM IWS & mobile apps

Ricoh SOP
x Allow Ricoh SOP to be installed with either short id or username/password authentication option
x Automatic login following card enrolment with username & OTP
x Increased stability following log out after printing a document
x Increased stability when swiping on the job list screen
x Improved document name on the job list for longer document names
x UI update for alignment of headers on job list
x Printing continues following logout if jobs are still in the queue
x Ricoh RXOP module updated to version 3.8.7
- Resolved an issue with duplicate printing on job release via card swipe
- Resolved an issue with the wrong date & time displayed on the print queue
- Removed "Please wait" message on login when no jobs are in progress

Sharp
x Reduction of memory consumption on gateways to increase stability

UI
x Improved handling of closing windows & pop-ups to remove JavaScript errors
x On deletion of accounts, users are asked to enter the account name, replacing the previous checkbox

4.4.14 3.20 HP WORKPATH RELEASE ONLY [2022-03-17]

HP Workpath
+ French Language Support
+ Italian Language Support
x Resolved app crashing issues related to HP 5.3 Firmware (Note: device must be upgraded to HP 5.4 firmware)
x Improved printing performance for download & print of large documents
x Resolved stapling issues with gateway mode for PC Client

4.4.15 3.20 [2022-03-08]

API
+ Additional functions for Public API (See API documentation for additional details)
x Check for duplicate domains when creating an account

Brother
x French Language updates

Core
x Migrate document conversion library to Mako SDK

PC Client
+ Italian Language Support
+ Dutch Language Support
- Fixed issue with short ID/OTP not being sent via Office 365 on local storage mode

Performance
+ Additional database indexes added
x Refactoring of caching for improved performance
x Updated thread pool for channel messaging
- Fixed caching issues for propagating/resetting child permission

UI
+ Italian Language Support
+ Dutch Language Support
x Prevent deletion of own root account
x Separate domain names onto new lines
x The dashboard will display a message rather than a loading icon to allow you to access other areas of the account whilst the dashboard is loading.
- Display correct timezone for Australian print jobs
- Display correct days on Print Activity dashboard

Xerox
+ "Authentication UI Language" configuration option added in SAFEQ Cloud UI
x French Language Updates
x Prevent duplicate sign in on Versalink/Altalink
x Updated server address configuration to always use localhost
- Fixed card enrolment issues
- Fixed issue with being able to login following an uninstall
- Fixed issue with WebClientNG not locking/unlocking on Versalink

4.4.16 3.19.1 [2022-02-11]

Core
x Additional logging to identify performance issues

4.4.17 3.19 [2022-02-04]

API
+ Additional functions for Public API (See API documentation for additional details)
+ OTP connection type for Ricoh SLNX

Authentication
- Reduce auto logout occurrence for Azure Oauth2

Core
x Auto reconnect for secondary gateway after connection reinstated
x Deletion of jobs from spooler folder on job expiry
x Disable triggers failed with incorrect exit condition
x Log `BootstrapCompleted` event with INFO level
x Upgraded protobuf library
- Fixed fwutil application missing after updating SAFEQ Cloud Gateway

HP OXPd
+ Exit button added to device UI
x 127.0.0.1 now used for configuration lookup
- Correction of Duplex & Mono behaviour when selected
- Fixed Card enrolment/login issues

KM IWS
- Removal of APAC region for Embedded Configuration

Mobile
- Android Mobile layout fix for Job & History list screens

PC Client
x Passwords with characters å ä ö now accepted
x Added additional retries for setting default printer for offline direct printing
- Fixed printing issues following gateway mode change
- Fixed issue with no location available and local storage printing
- Fixed Event 1000 windows crash error
- Fixed issue with PC client not disconnecting following unauthorisation of user

Performance
x Additional database caching

Security
x Log4j upgraded to version 2.17.1
x Security update for DEBUG logging to remove sensitive information

UI
x API Keys masked by default
x Asterisks displayed for mandatory fields on all forms
- Fixed "my printers" view responsiveness on EU Prod

UniDriver
x Updated SAFEQ Cloud Driver for use with Accessibility Tools

Xerox Embedded
x Updated French Translations on device UI
- Fixed configuration issues for Xerox 7545

4.5 2021

The following contains a list of notable changes in YSoft SAFEQ Cloud.

Legend:

+ Added feature
x Improved/changed feature
- Bug fixed

4.5.1 3.18.4 [2021-12-21]

Core
x Log4j upgraded to version 2.17

4.5.2 3.18.3 [2021-12-16]

Core
x Log4j upgraded to version 2.16

KM IWS Embedded
- Fixed card reader login errors with card readers being removed & not being detected
+ Update to allow OpenAPI & IWS devices to read card numbers in the same way

4.5.3 3.18.2 [2021-12-11]

Authentication
- GSuite Connection Fix
- Fixed authentication errors on UK Clusters
- Addressed password issue on Canon devices

Core
+ Debian 11 Support
x Backported OneQ terminal configuration library
x Log4j critical vulnerability fixed

HP OXPd Embedded
x Update HP OXPd client to the latest libraries, build tools & IDE
- Fixed screen resolution detect error

Kyocera Embedded
- Fixed Simplex printing

Ricoh SOP Embedded
x Updated error messages
x Updated Spanish translation on Device UI
- Fixed Unknown Terminal error post configuration
- Fixed issue with Custom Certificates

PC Client
+ HP "Print from USB"

Performance
x Update Java JRE to latest Java 11
x Cache improvements

UI
+ Ping/Azure Group Sync Prompt
x Primary EU search updated to allow searching from the root account
x Search, Delete & Sort options added to Endpoints page on Web UI
x Updated French translations on Web UI
x Updated German translations on Web UI

4.5.4 3.17.2 [2021-11-19]

x Updated keystore request handling

4.5.5 3.17.1 [2021-11-11]

x Updated thread pool allocation for AutomationTask
- Fixed issue with Azure permissions for SSO
- Fixed issue for LDAP user with group access control gets "Invalid credentials" error when logging into printer

4.5.6 3.17 [2021-11-04]

Licence
x Updated logic for applying licence for Azure user not yet created in SAFEQ Cloud

Core
+ Added data model for Named User Profiles

Sharp
x Updated Sharp embedded client for improved scaling on different screen sizes

Search
+ Added Search by Account ID
+ Added Search by servers
+ Added Search by domain

PC Client
+ Added command line switch for Offline Printing for remote installation
x Updated PC Client for installation of MacOS version 10.14 and earlier
x Updated French translations errors in PC Client
- Fixed issue with locking PC Client to local storage mode

Performance
x Updated thread pool creation for Automations

UI
x Updated French translations in WebUI Endpoints
x Updated French translations in WebUI Reporting
- Fixed issue that allowed addition of blank customer to vendor

4.5.7 3.16 [2021-10-13]

API
+ Extended API with Documents History
x Extended logging with API Request Rate metric
x Added filtering for URI parameter in /gateway/endpoint for imporved security
x Updated DSP API

Authentication
+ Added Ping authenticaiton to available SAFEQ Cloud Authentication providers
x Updated logic to expire unauthenticated sessions faster
x Improved logging for card authentication using client authentication for expired users
x Updated internal messaging despatcher settings to improve performance
- Fixed issue with blank page displaying after successful authentication with Azure AD

HP Workpath Embedded (pending upload to HP Command Centre)

x Improved printing speed for complex jobs stored in cloud on HP Workpath
- Fixed stapling finishing option when using cloud storage for HP Workpath

KM IWS Embedded

+ Added option to remove Copy button from IWS Embedded for SFP devices support
x Enhanced logging for application errors
x Implemented fallback to English translation if language pack not installed
x Updated Swedish translation
x Enhanced user feedback when printing is complete
- Fixed issue with scan error if filename contains special characters

Ricoh SOP Embedded

+ Added mandatory flag for device username and password in Ricoh embedded configuration
x Updated logic for reading card IDs for case sensitivity
x Removed Y Soft branding from Ricoh SOP embedded client
x Updated German translations
- Fixed issue with incorrect branding being displayed if configuration cannot be loaded
- Fixed intermittent 403 error while deploying Ricoh SOP
- Fixed mismatch error with version number in Extended Info feature on printer

Xerox Embedded

x Updated VendorName to prevent installation errors on some Xerox devices

Installer

x Updated installer logic for Linux version detection

Messaging

x Updated TLS version for emails sent using triggers

Mobile

- Fixed ouput options override issue for output release from Mobile app on Android

PC Client

+ Added support for Apple Silicon (ARM) M1 processor devices
+ Added Offline Push-Print option for PC Client in local storage mode
+ Added client-based authentication with Google
+ Added client-based authentication with Ping
+ Added German language
x Updated PC Client front-end technology
x Improved PC Client synchronisation when network status changes
x Updated icons for PC Client
x Updated client-based authentication to use OpenID connect
x Improved Terminal Services/Remote desktop notifications
x Improved logging for network-related issues

UI

+ Added active/expired state of users with client based authentication
x Updated customer user expiration field with input validation

x Increased timeout for UI relay for long-running request
x Deprecated ADFS client identity type in SAFEQ Cloud provider settings
x Updated to sort printers for Push ports in alphabetical order
- Fixed UI issues with newly created items not always displaying immediately
- Fixed incorrect version number in server view after upgrade
- Fixed cache issue with Access Controls
- Fixed intermittent issue with SAFEQ Cloud Portal Internal error when downloading logs

4.5.8 3.15.5 [2021-09-23]

- Fixed issues in UI where newly created/updated/deleted items may be displayed inconsistently

4.5.9 3.15.4 [2021-09-09]

- Fixed cache issue where adding Access Controls on a Vendor could make child items disappear temporarily
- Account without language/locale set fails to load

4.5.10 3.15.0 [2021-09-03]

+ Added support for Brother embedded devices
+ Added search by card ID for users
+ Added Dutch language
+ Added German language
+ Added Spanish language
+ Added integrity check for service used by offline Secondary Gateway
+ Added integrity check for Access Control
+ Added integrity check for domains within multiple authentication providers
+ Enabled DOS filter by default
+ Added source request IP address in URI filter to Debug log
+ Added input validation for SSO XML Metadata URL field
+ Added Ricoh branding for installers
x Enhanced performance for dashboard loading
x Added paging to retrieve more than 200 groups for Google Authentication group sync
x Updated UI to retain selected language as default
x Updated Terminal Service API to be compatible with custom certificates
x Updated logging to include server metrics
x Updated HW ID for SAFEQ Cloud printers in Windows
x Updated workflow for "Download&Print" for local storage mode
x Updated logic for PC Client connection/disconnection events
- Fixed PC Client version mismatch in UI

HP Workpath

+ Added Spanish language support
x Updated Workpath to SDK v1.5.0
x Updated Android to SDK v29 for compatibility with SDK v1.5.0
x Updated manifest files
x Updated application with check for valid server host before getting configuration
x Updated application with check for cached printer configuration
x Updated logic to load configuration screen if cache is empty

x Simplified card reader service start
x Updated error handling for logout workflow
x Minor UI improvments
x Updated logging information
- Fixed issue with card authentication after reboot
- Fixed issue with "Failed print job" message when job printed correctly
- Fixed issue with Scan to My Email button being displayed when disabled in configuration
- Fixed issue with "Loading configuration" message remaining on display
- Fixed issue with card swipe failure requiring multiple swipes or device reboot
- Fixed error when new card is swiped
- Fixed issue with "B&W" trigger not being actioned with PC Client in Gateway mode
- Fixed issue with Workpath app intermittent failure on FW 5.1.0.1

HP OXPd

- HP OXPD: 'Install and configure' issue is fixed
- HP OXPD: colour print issue after the client installation no longer appears
- HP OXPD: application is no longer getting stuck after log in

KM IWS

+ Added Polish language
+ Added Swedish language
+ Added Norwegian language
+ Added Compact Scan option to IWS embedded
x Improved pull print mechanism to execute jobs in background and check and display status
x Added multi-part data transfer for scan jobs
- Fixed Duplex copy issue
- Fixed Script Access Error for Copy when paper tray empty
- Fixed tray selection issue for copy job
- Updated French language translation errors
- Fixed Incorrect duplex parameter from IWS record job
- Fixed memory issues when printing
- Fixed issue when user is automatically logged out during multiple print jobs and printing stops
- IWS – Download and Print – fixed issue with "Preparing job" displayed until printer enters sleep mode
- Fixed issue in print processing view when IWS server is not reachable (Note: "Server not reachable" error message relates to IWS server and not SAFEQ Cloud – error message should be updated to reflect)
- IWS – Month in the default scan file name is wrong
- Fixed scan job runs out of memory errors
- Fixed Scan failed and after MFD reboot all docs are sent to the last logged in user issue
- Fixed issue with display showing "STOPPED" until printer enters sleep mode when paper jamis forced in document feeder
- Fixed UI issue when user has a longer username
- Fixed stapling issue not being applied when printing in the gateway mode

KM OpenAPI

+ KM Open API: Added APACH region support

4.5.11 3.14.0 [2021-05-17]

+ Case-insensitivity for usernames added to SAFEQ Cloud PC Client
+ Added option to trim control characters from card # on SAFEQ Cloud OXPd
+ Several process pop-ups and user feedback added to Ricoh SOP Embedded UX
+ Added Automatic SP Mode configuration on device for Ricoh SOP Embedded installation
+ OSS licensing information added in Server and PC Client
+ Added German language to the driver
x Improved error messages on Chrome Extension
x Improvements to backend reporting
x Improved Load balanced service handling when filtering for distinct service/server combinations
x Logic and behavior of the refresh button on Ricoh SOP has been improved
x Improved French and Dutch language fixes in Ricoh SOP Embedded
x Card enrollment logic on Sharp Embedded has been updated
x Improved Swedish translations in Sharp Embedded
x User handling for users with same username in different authentication providers has been updated
x Improved rendering for PDF's with signature
x Minor Improvements for SAFEQ Cloud Web UI
x Performance enhancements made for SAFEQ Cloud Web UI
- Fixed issue with login and sync of printers in Chromebook
- Fixed issue with cluster membership of gateways or PC clients after irregular connection loss
- 'Unknown Terminal' Bug in Ricoh SOP Embedded fixed (Please see updated Manual)
- Issue with Scan to Portable USB Storage on Ricoh SOP Embedded is fixed (Please see updated Manual)
- Cosmetic issues on Ricoh SOP Embedded has been fixed
- Issue with Logo image quality on Sharp Embedded has been fixed
- Fixed issue with movable UI on Sharp Embedded
- Issues with generating QR code is fixed
- Fixed issue with ignored provider ID when retrieving a list of documents for a specific user

4.5.12 3.13.0 [2021-04-08]

+ Display "Offline" status in job list on embedded for offline jobs
+ Added IPP authentication option and validation to account settings
+ Added support for Ubuntu 20 LTS
+ Added ability to load XML Metadata from a file in non-default conf location
+ Added support for HTTP strict transport security
x Improvements to intercluster communication
x Improved account-servers view for ease of use
x Optimized SAFEQ Cloud Web UI response and performance
x Changed logo upload size to max 200kb
x Improved error messaging for location adding and editing locations
x Added input validation for allowed IP's in API access key
x Added httponly flag for cookies
x Updated x-frame options for protection against Cross-frame scripting (XFS) attacks
x URI upload is no longer supported for documents end point
x HTTP TRACE / TRACK Methods disabled
x Security improvement preventing concurrent sessions by same user in SAFEQ Cloud
x Improved performance on user import
x Enhanced WorkspaceeONE/AirWatch compatibility for Y Soft Mobile APP

x Optimized logic for HP Workpath Embedded for enhanced card reader experience
x Discontinue use of port 7310 (Only relevant for SAFEQ Cloud 2.x server version)
x Updated content security header (CSP)
x Updated x-content-type-Options
- Fixed UI timeout issue for high volume group sync with Microsoft Azure OAuth2 authentication
- Fixed issued with landscape mode from bypass tray on Konica Minolta
- Fixed issue with staple logic for landscape documents
- Fixed issue with triggers for manual tray selection
- Issue with French language in Xerox Embedded fixed
- Updated Ricoh SLNX Share API to to display job properties correctly
- Fixed Ricoh SLNX Share API mapping for short-ID authentication
- Fixed issue with private cloud update for primary and secondary server types assignment
- Fixed issue with embedded UI to show documents as "Offline" when document storage is not available
- Fixed issue with Chrome Extension user authentication token expiration
- Fixed issue with Chromebook extension rejecting certain symbols in the password
- Chromebook extension issue where print queues did not automatically synchronize at login fixed

4.5.13 3.12.0 [2021-03-11]

+ Added password policy option for local users
+ Added API key expiration options
+ Added support of POST on public API /login
x Optimized authentication lookup process for card authentication
x Optimized port/service preloading
x Updated required rights for Azure Authentication provider
x Updated Default Permissions for User & Reporting
- Updated SAFEQ CloudUpdater component directory usage for remote install on Private Cloud
- Fixed issue with User token acquisition
- Fixed XSS prevention in My Printers screen

PC Client:

+ Added connection check prior to submitting print jobs
x Added signature for uninstaller
x Optimised channel disconnection protocol when PC goes into standby mode
- Fixed Unattended installation problem with macOS PC Client on Big Sur
- Fixed reinstall issue macOS PC Client on Big Sur
- Fixed issue with trigger generating Short ID when not set

Chrome Extension:
+ Enhanced Chrome Extension with user_token security
+ Option to bypass login in Chrome extension
- Chromebook extension test connection error message updated

Canon Embedded:
+ Support for new canon devices
+ Added support for DNS configuration

HP OXPd Embedded:
x Update HP OXPd to FutureSmart 5 SDK 1.8.2
x Updated Scan to my email OXPd for 'Ballpark device' compatibility
x Updated OXPd UI to fit "Ballparks devices"

- Updated OXPd to use legacy UI for devices not able to render the updated UI
- Failed history purge bug fixed
- Queue fails to remove document name from queue after printing in offline mode
- Optimized authentication response timing
- HP OXPd Refresh button optimized

Konica Minolta IWS embedded:
+ Add language options for French, Danish and Dutch language

Konica Minolta Open API:
x Updated Dutch language translations

Lexmark Embedded:
x Updated French language translations
- Pull Print icon not showing up on Lexmark printer after embedded installation on new devices

Sharp embedded:
- Fixed card-enrollment issues for wrong username

Xerox Embedded:
+ Added TLS v. 1.2 for Xerox devices that can use TLS 1.2
x Modify Dutch text in the Xerox embedded
x Embedded French Translation on Xerox Embedded enhanced
- Pullprint app did not show after pushing embedded on Xerox AltaLink C8055
- Xerox Altalink C8170 configuration issues fixed

4.5.14 3.11.0 [2021-02-06]

+ Added option to sign SAML requests with private certificate chain
+ Added option to import xml metadata for SAML SSO
+ Extended API with token-based authentication for additional security
+ Extended permissions for API keys
+ Added option for API key to utilise unauthenticated requests
+ Added option for API to allow untrusted endpoints
+ Added option for API keys to automatically trust endpoints
+ Added option for API keys to be restricted to allowed IP ranges and subnets
+ Added new Endpoints view and Endpoint data model
+ Added ability to change filename to KM IWS scan
+ Added user token security to KM IWS embedded
+ Added permission for hiding "propogate to child node/reset child nodes"
x PC Client for Mac signature updated
x PC Client updated to allow installation without active connection to SAFEQ Cloud
x Updated PC Client silent installation configuraton with certificate selection by issuer
x Added check for duplicate short ID on user creation
x Updated UI to indicate when job storage is not available on embedded job list
- Update dropdown width scaling issue for Chrome browsers
- Fixed UI issue for IWS Scan to Email view
- Fixed SAML redirect issue

4.6 2020

The following contains a list of notable changes in YSoft SAFEQ Cloud.

Legend:

+ Added feature
x Improved/changed feature
- Bug fixed

4.6.1 3.10.0 [2020-11-27]

+ Added Search feature
+ Added Google as an authentication provider
+ End of support announcement for PC Client on Windows 7
+ Add option in UI to limit API key functionality (admin vs non-admin API keys)
+ Add ability to restrict API access based on IP address filtering
x Updated Sharp embedded client
x Updated Sharp client to support OSA 5.5
x Update Sharp embedded to support DNS
x Updated Sharp embedded to automatically redirect legacy configuration URLs to new URLs
x Updated Ricoh SDK/J embedded client
x Updated finishing options for HP devices
x Updated finishing options for KM devices
x Enhanced XSS protection in Web UI
- Fixed translations in Sharp embedded
- Fixed issues with Run in Separate JVM
- Fixed timeout issue for printing large documents
- Fixed cosmetic issue with PC Client for Mac

4.6.2 3.9.0 [2020-10-13]

+ Added Remote Update feature for Secondary Gateways
+ Added ModifyPersonalInformation permission
x Updated SAML SSO configuration to include SPID/Issuer
x Updated LDAP-S bind use SASL with SSL/TLS-protected connection
x Updated Konica Minolta OpenAPI embedded client
x Updated HP OXPd embedded client
x Updated Java 11 with option to conntrol max heap size
- Fixed HP OXPd embedded colour print issue
- Fixed HP OXPd scaling issue for small displays
- Fixed KM OpenAPI Short ID issue
- Fixed KM OpenAPI booklet margins issue
- Fixed reporting issue for PC Client jobs in local storage mode for multiple copies
- Fixed UpdateUserDetails API issue

4.6.3 3.8.0 [2020-09-09]

+ Added Server view for status of Secondary Gateways
+ Added Integrity Check feature for identifying configuration issues
+ Added Kyocera embedded client support
x Updated Sharp embedded client
x Updated Lexmark embedded client
x Updated HP OXPd embedded client
x Updated Printer configuration for serial number entry in printer details

x Updated Client-based authentication with increased maximum token header size
x Updated PC Client for dynamic loading of WLAN dll for virtual environments
x Update Java version to Java 11
x Updated Transport Layer Security to support TLS 1.3
- Fixed Lexmark embedded Short-ID error
- Fixed UI issue with authorise/unauthorise server UI update
- Fixed issue in MacOS PC Client for jobs outputting with incorrect settings when offline
- Fixed reporting issue for PC Client jobs in local storage mode for multiple copies

4.6.4 3.7.0 [2020-08-06]

+ Added Group synchronisation for Client-based authentication
x Updated Ricoh SOP embedded client
x Updated Konica Minolta OpenAPI embedded client
x Updated Konica Minolta IWS embedded client
x Updated MDM option to be able to run on SAFEQ Cloud Primary servers (on-premise)
x Updated PC Client DLLs for Windows 7 (32-bit)
x Updated HP Workpath and KM IWS Reporting to include Department
x Updated SAFEQ Cloud zLinux version for backwards compatibility with RHEL7
x Updated Web UI with server view, tabs and path
- Fixed login timeout for Ricoh embedded
- Fixed KM OpenAPI embedded for usernames longer than 39 characters
- Fixed KM IWS scan issue on IT6 devices for paths containing "\.."
- Fixed authentication error on Sharp embedded
- Fixed login error for Ricoh SLNX when password includes "%"
- Fixed SAFEQ Cloud logs for Ricoh SLNX password issue
- Fixed "Color" attribute error in SAFEQ Cloud triggers

4.6.5 3.6.0 [2020-07-07]

x Updated Mobile gateway API to retrieve copy, scan and print reporting for downloaded jobs
x Improved caching for tree and keystores for improved server start-up time
x Implemented database cache pre-loading for all entities
x Added keystore initialisation before server start to improve start-up performance
x Updated Java8 to latest
x Added support for Microsoft Graph API for Azure authentication
x Default value for "Use Separate JVM" updated to "off" for unattended install
x Updated Lexmark embedded client
x Updated HP OXPD client
x Added SNMP community name setting for HP OXPD embedded configuration
- Fixed overlapping keyboard issue in HP OXPD client
- Updated refo file import script with department attribute
- Fixed Oracle DB column issue for refo file import

4.6.6 3.5.0 [2020-06-09]

+ Added Audit Log to capture user and system actions
+ Option to create embedded configuration during printer configuration
+ Card management permission created to specifically enable deletion of Card IDs
+ Added configuration option for KM IWS embedded UI buttons
+ Added access to native functions and other apps fo KM IWS embedded

x Disabled ability to delete authnetication service from Primary server
x Optimised dashboard loading in SAFEQ Cloud Web UI for imporved performance
x Improved keystore loading logic
x Updated API for local user import actions
x Inhibit end user offline/online notifications for PC Client
- Fixed error message for expired licence
- Fixed job auto-deletion issue in cluster environments
- Fixed "Unknown Publisher" error message on PC Client install

4.6.7 3.4.0 [2020-04-20]

+ Add or remove multiple services on Secondary Gateway
+ Option to create required ports during printer configuration
+ Option to add required services during port creation
+ Added option to disable "Store ad deliver via gateway" option in PC Client
+ Added "Media Type" option in SAFEQ Cloud unidriver
x Pre-optimization of print data for improved print speed and quality
x Updated PC Client to enhance hostname validation for trusted configurations
x Enhanced PC Client certificate selection options
x Added retry logic for improved job handling in PC Client (local storage mode)
x Added installer option for Oracle DB to skip configuration
x Updated permissions for rights on certificate creation and deletion
x Changed default value for PC Client Online Certificate Status Protocol to disabled
x Updated Jetty to v9.4.27
x Updated CURL to v7.6.8
x Updated PostgreSQL to v9.6.17
- Updated HP Workpath app (v3.3.1) to fix card reader issue
- Fixed job auto-deletion issue in cluster environments

4.6.8 3.3.0 [2020-03-10]

+ Client-based authentication for Azure and ADFS
+ MFA authentication from PC Client if using Azure or ADFS
+ Added disk space check to installer prior to running
+ Added the option to limit number of cards registered to users
+ Added description field for printers
+ Added option for choosing between PDF and PS->PDF on MacOS PC Client
x Changed management of card ID registration for deleted or amended usernames
x Updated embedded API with finishing options
x Improved logging for triggers and automations
x Added enforcement of output port permission to prevent logging on to MFD
x Updated PDF conversion engine
x Updated HP Workpath to fix card authentication issue
x Updated driver with PDFA conversion option
x Updated paper format specification for PC Client configuration
x Updated driver for KM for print quality enhancements
- Fixed A3 scan to email on HP
- Fixed booklet printing formatting on Konica Minolta
- Fixed Account ID changing in cluster environments
- Fixed error message for Scan to Email failure for KM IWS embedded
- Fixed short-edge duplex issue for KM IWS embedded

- Fixed conversion for PDF file on PC Client for Mac
- Fixed paper format issue for Ricoh Postscript2

4.6.9 3.2.0 [2020-02-07]

+ Oracle database support
+ Department/group reporting
x HP Workpath 3.2 embedded app updated for FutureSmart Bundle 4.10
x Added Print&Hold feature for HP Workpath app
x Updated UI for HP Workpath app
x Additional Role to view One-time password
x Configurable log level via UI
x Many improvements to print driver performance and print job rendering
x Migrated logic from SAFEQ Cloud Server to PC Client
x Added Postscript 2 option
x Enhanced security around passwords displayed in Web UI
x Added device family support for Xerox printers
x Improved performance on log retrieval from Secondary Server
- Fixed wrong version of PC client being shown Web UI
- Fixed My profile page not shown correctly for users with disabled `ViewUserInputPorts` permission
- Fixed API token field still has a value when edited
- Fixed SLNX Share Embedded reporting issue when using card login
- Fixed issue with margins being cut off
- Fixed issue with lost print jobs if gateway not available
- Fixed card authentication issue for HP Workpath
- Fixed scan to email issues for HP Workpath
- Fixed KM IWS scan to email issue
- Fixed KM IWS number of copies not being inherited
- Fixed KM IWS auto-logout issue
- Fixed missing characters on print from Ricoh devices
- Fixed collation issue with Ricoh IMC devices
- Fixed booklet print issue with Xerox device
- Fixed reporting issue with PC Client for Mac
- Fixed changes in DocOut service not propagating to output port entity caches

4.7 2019

The following contains a list of notable changes in YSoft SAFEQ Cloud.

Legend:

+ Added feature
x Improved/changed feature
- Bug fixed

4.7.1 3.1.2 [2019-12-13]

x Improved SAMLv2 support for AD-FS On-Premise
x By default restrict access to Windows SAFEQ Cloud PC Client SAFEQ Cloudclientcore folder to SAFEQ Cloud service account only

x Enforce SSL validation option for PC Client IPPS printing
x Changed MacOS PC client to not share queues on network by default
x Added support for Ysoft, Omnikey and Elatec TWN3 card readers in IP card reader bridge
x Updated curl library used by SAFEQ Cloud PC Client installer
x Improve user authentication when doing OTP authentication
- Fixed miscellaneous issues in KM IWS application
- Fixed issue with PC Client for Mac and server connection failing on macOS Catalina
- Fixed issue with triggers not applied when printing with PC Client in Local Storage mode

4.7.2 3.1.1 [2019-12-03]

- Fixed issue with releasing of jobs stored on PC client didn't work in some configurations when document output service was on the secondary server
- Fixed issue with collation and staple multi-copy printing on HP

4.7.3 3.1.0 [2019-11-19]

+ HP Workpath (formerly Link platform) embedded app
+ Ricoh SOP Android embedded client
+ Konica Minolta IWS embedded App
+ PC Client 3.0 for Mac
+ SAML v2 single sign on
+ New Windows SAFEQ Cloud print driver
+ Support Microsoft SQL Server/SQL Azure for backend database
+ Ability to have local users as part of groups
+ System to self-register swipe cards for users without password
+ Support scan and copy reporting from Ricoh SLNX Share in SAFEQ Cloud
+ One-time password feature for users without password or multi-factor configurations
+ Support SecurityEngineering IP card reader
+ Support RFIDeas 241 IP card reader
+ Support CentOS 8
+ SAFEQ Cloud Driver UI improvements
+ End-user interface to manage Short ID
+ Expand SAFEQ Cloud driver with additional trays up to 6
+ New My Profile end-user Web UI screen
+ Automatically generate a Short ID or One-time password based on trigger
x Many improvements to print driver performance and print job rendering
x Improved validation of Short ID and card ID being unique for an account
x Improvements to primary cluster communication and performance
x Added HP native keyboard as workaround for missing symbols on HP OXP embedded keyboard
x Improved support for very hardened Linux OS distributions used in high security environments
x Disabled copy and scan accounting for Xerox embedded application on some models
- Fixed issue with multiple jobs wouldn't release when user selects all and deselects few of the jobs
- Fixed print issues on Xerox AltaLink with Letter and A3
- Fixed new added private certificate chain not loaded properly for mobile print service
- Fix issue with print queue creation on some macOS configurations
- Fixed issue where after upgrade from SAFEQ Cloud 2.5.x to 3.x, all documents printed before upgrade could appear as printable
- Fixed Lexmark tray selection problem

- Fixed issue with certificate handling with some HP firmware versions which could result in "Server or network problems" error on device

4.7.4 3.0.3 [2019-10-07]

+ Added new setting to control MDM single-sign-on feature enablement in Mobile Print settings
x Changed PC Client to show popup on sync error only once per interruption
x Changed Mac PC Client from "SAFEQ Cloud Client" to "SAFEQ Cloudclient" for plist settings
x Updated Mac PC Client installer for recent macOS versions
x Change utility in PC Client to avoid false positive flag by some antivirus engines
x Updated SAFEQ Cloud client core for Windows 7 compatibility
x Changed lookup of printers on input port configuration, for configuration of push print queues with printers outside container
x Changed OKTA integration to retrieve user email attribute in more configuration scenarios
- Fixed issue with some Sharp printers hanging after booklet printing
- Fixed PC Client Incorrect output bin selection for Ricoh printers

4.7.5 3.0.2 [2019-09-20]

+ Added support for RedHat Enterprise Linux/CentOS 8
x Changed PC Clients list view to not show version for quicker listings
x Major network stability and performance improvement for PC Clients and Secondary Gateway servers
x Improvements to UI behavior when running larger primary cluster configurations
x Major Web UI performance improvements for very large account trees
x Changed print all from embedded clients to not print jobs in random order
- Fixed issue with log rotation, not creating new log files
- Fixed issue where print jobs stored on PC Client sent to release during PC sleep, could be released when waking up
- Fixed issue with trigger Set document attribute to B/W or Color not working.
- Minor UI issues fixed, such as Access control page not refreshing after Local rights are given to a user
- Fixed authentication failing if auth service running on 2 secondary servers and one is unauthorized

4.7.6 3.0.1 [2019-07-01]

+ Added caching of keystores for greatly improved secondary server service performance
x Optimizations for Web UI session cache for cluster configurations

4.7.7 3.0.0 [2019-06-29]

+ New SAFEQ Cloud PC Client 3.0 with local storage and delivery option for serverless deployments
+ Location aware printers
+ Encryption of document data at rest
+ Reporting on scan and copy from embedded clients
+ Ability to restrict and pre-authorize PC clients or secondary servers based on customer PKI
+ Added high performance caching system for major performance improvements throughout SAFEQ Cloud

+ Ability to specify API key for secondary servers and PC clients
+ Release all option on embedded card authentication
+ Support network connected card readers via API
+ Ability to specify an API key during silent unattended installation of primary server
+ Support for OKTA LDAP authentication
+ Add extra authentication option for PC client: User Principal Name
+ Make UI embedded configuration setting for Konica Minolta native card reading
+ Enable the ability to delete and edit the default API key
+ SAFEQ Cloud Web UI in French
+ Possibility to configure duplex/color via the unattended installer options
+ Add Local providers and Local Users group with Users role by default on new accounts
+ Ability to authenticate in SAFEQ Cloud using UserPrincipalName with AD/LDAP
+ Support Debian 9 Stable versions
+ Ability to set new PC client/server trust via API
+ Possibility to select paper sizes A5 and A6 in SAFEQ Cloud single driver
+ Ability to force resync of printers on PC Client update
+ Option to have desktop icons for PC Client Login and Logout created
+ Expand LDAP configuration to include object class for persons and object class for groups
x Major performance improvements for large distributed data transfer
x Improved embedded pull print release performance
x Major performance and quality improvements for SAFEQ Cloud MacOS Universal printer driver
x Numerous Web UI usability improvements
x Disable HTTP trace and track method
x Changed print jobs displayed and printed in reverse order
x Restrict old default API key usability
x Generic branding in Xerox and HP embedded clients
x Added Input Ports option for Containers
x Changed HP embedded to allow locking of everything and unlocking of 3rd party apps
x Improved image quality when printing high graphical jobs to Konica Minolta MFD's
- Fixed issue releasing SAFEQ Cloud print jobs on Equitrac embedded clients when job contain double byte chars
- Fixed issue on Sharp embedded where change to "Copy" when printing would stop print jobs
- Fixed error when deploying HP embedded application on some HP firmware configurations
- Sharp – Copy fails with Limit error in display if copying is interrupted
- Fixed issue with deletion of nested container and input ports
- Improved performance for secondary servers connecting to vendor primaries
- print job with document multi-up settings goes in error
- Fixed issue with Test all auth providers not showing result in UI
- Fixed Universal driver: HD photo images (WDP files) produced by Windows Photo Viewer are not printed correctly
- Fixed issue printing certain PDF documents accurately on Ricoh MFD's
- Fixed Internal error shown when accessing Access Controls after auth provider has been removed
- Fixed issue on some Ricoh MFD's email address of user not showing up in native scan-to-email app
- Fixed issue with Sharp booklet printing + folding + stapling
- Fixed issue printing on Windows 10 in some high security configurations resulting in I/O error
- Fixed issue in PC client and print from Internet Explorer 11
- Fixed issue with printing certain Excel sheets in landscape mode not printing correctly
- Fixed Job count incremented by 2 in the Dashboard sometime when user tries to print very large files
- Fixed macOS SAFEQ Cloud PC client – only 1 copy printed for the job sent with multiple copies

- Fixed macOS SAFEQ Cloud PC client – multicopy print + staple from macOS not printing correctly
- Fixed issue with only one copy getting printed when user tries to give a Pull Job with any number of copies
- Fixed Mobile QR code release: An error occurred, code: 6
- Resolve port conflict for IPM and DSP API terminal services
- User not able to add Access control second time after deleting it once
- Fixed print jobs getting cancelled when user logs out automatically from KM device
- PDF Reports extracting reports of Totals by device even if user is in Totals by user window
- Fixed print jobs getting cancelled when user logs out on a Sharp device
- Fixed KM embedded deployment error when pushing embedded with Scan-to-email feature enabled in US region

4.7.8 2.5.9 [2019-05-28]

x Enhanced performance for releasing multiple pull print jobs from embedded clients
x Modified permission control on HP embedded, to support single-sign-on with third party apps
- Fixed issue deploying HP embedded clients in some network configurations
- Fixed issue printing landscape on Konica Minolta MFD's

2.5.8 [2019-05-09]
+ Ability to authenticate in SAFEQ Cloud using UserPrincipalName with AD/LDAP
+ Added support for OKTA LDAP authentication
- Fixed issue loading certificates on secondaries under a primary vendor

4.7.9 2.5.7 [2019-04-10]

- Authentication error doing scan if users email has changed recently in external auth provider
- Fixed issue with custom Postscript print jobs in some cases being converted causing errors on HP

4.7.10 2.5.6 [2019-03-29]

- Fixed email address of user not showing up in native scan-to-email Ricoh app
- Fixed error sending email in Scan to My Email in some configurations

4.7.11 2.5.5 [2019-03-13]

x Improvements to SSL keystore handling on primary servers

4.7.12 2.5.4 [2019-02-28]

x Improved Ricoh embedded deployment support

4.7.13 2.5.3 [2019-02-25]

- Fix for keystore loading for non-root vendor

4.7.14 2.5.2 [2019-02-25]

x Added input and output port cache
x Improved loading of keystores for services which run on primary vendor server
- Fix for setting PS3 output type when using API on secondary

4.7.15 2.5.1 [2019-02-24]

+ Ability to specify group name attribute for LDAP authentication
- Fixed issue for users with IE11 not able to view all printers in My Printers Web UI
- Fixed issue with printers fail to sync for Azure group membership
- Fixed issue when more than 10 authentication providers, only last 10 are shown
- Optimized performance for servers with single cores

4.7.16 2.5.0 [2019-02-13]

+ Scan to My Email MFD embedded application
+ Ability to add/list/modify/delete access controls on accounts and containers via the API
+ Ability to delete input and output ports via API
+ Ability to import a certificate during installation to establish secure connection to API and for use with internal secure channel
+ Ability to configure Authentication Providers from API
+ Ability for a user to self-service choose which input ports to install on their PC
+ MDM AirPrint Azure Intune support
+ New Message Service for delivering SMTP email
+ Public API to get list of printed documents for user
+ Major print job rendering performance improvements with new Postscript Level 3
+ New security feature to require PKI certificate for secondary server installs
+ Add new rendering backend to remove dependency on CUPS on Linux
+ Deploy PC Client and printers to Windows workstations with Microsoft Intune
+ Support Ubuntu LTS Linux distributions
+ Documented disaster recovery procedure for primary server(s)
+ Add "Available by default" option for input ports
+ Ability to select multiple groups/users when adding access controls
+ Driver and PC client in French and Danish
+ Ability to release both UniPrint and custom driver on same output port
+ Performance enhancements for user authentication
+ Ability to control locked features for HP embedded
x Improved load balancing for many servers with offline secondaries
x Change primary cluster node cloning logic
x Documented process for PC Client deployment on Windows 7
x Documented Azure PostgreSQL configuration
x Changed PC Client to not remove printers during sync if no network connection to gateway available
x Added support for authenticating against Microfocus IDM via LDAP
- Fixed issue with duplicate files in history if offline cache is enabled and both servers are up
- Fixed issue with Azure authentication stops working after some time
- Expanded Canon embedded client device support
- Fixed issue with Wide Area Mobile print failing with mobile service on secondary server
- Fixed issue where .local used in domain name is snipped
- Fixed 4 hole punching option when printing to certain Sharp models

- Fixed issue where unable to send print job when logged in with UPN for Azure AD on PC client
- Fixed error "Unable to find output port" when printing from mobile using QR code scanning
- Fixed number of copies and collation not working for IPP print protocol
- Fixed issue with Sharp client throwing "Terminal Not Found" error when accessed using a DNS

4.8 2018

The following contains a list of notable changes in YSoft SAFEQ Cloud.

Legend:

+ Added feature
x Improved/changed feature
- Bug fixed

4.8.1 2.4.1 [2018-11-07]

+ Added "Monochrome printer" option in the output port settings
+ Add support for keyboard emulation wedge readers on Konica Minolta
- Fixed issue where KM embedded could set incorrect settings on device if another auth already set

4.8.2 2.4.0 [2018-11-05]

+ OKTA authentication support
+ Added new Canon embedded terminal
+ Add support for Ricoh SLNX Share embedded terminal in SAFEQ Cloud
+ Expanded caching for improved login experience on embedded clients on poor connections
+ Ability to have containers
+ Ability to move an account/vendor/printer/service/server from one place in the tree to somewhere else
+ UI for API Access Key management
+ Extend unattended install option with service bootstrapping
+ Increasing security registering a secondary server
+ API function to create input ports
+ Add language selection to account settings (for future use)
+ Ability to configure separate JVM and thread counts for services
+ Support for Canon Postscript universal printing
+ Ability to remain logged in with Custom Login in PC client
+ Popup notification if custom login and user has not signed in to PC client
+ Local users (such as guests) are now part of a local group called [Local users]
x Hide Download buttons in Log view
x Hide options to modify print output settings on KM embedded client
x Adding a new access control will now copy the inherited permissions if new access is first one
x Modify OKTA authentication to allow for username attribute specification
x Set SAFEQ Cloud universal driver to BW as default
x Automatically set default print queue in PC client to pull print or first push queue
x Enhanced authentication caching for quicker MFD login
x Added official support for Sharp
- Fixed Sharp Embedded with missing part in the display
- Fixed issue with password in clear text on display in Sharp Embedded

- Fixed issue where secondary gateway on version earlier than 2.3.1 appeared offline in UI with newer primary
- Fixed issue with passwords containing special characters in PC-Client

4.8.3 2.3.3 [2018-09-17]

- Fixed issue with deploying to Ricoh MFD's not configured for TLS1.2
- Fixed issue authenticating against IBM Domino LDAP

4.8.4 2.3.2 [2018-09-05]

- Fixed issue with conversion service causing delays in some configurations
- Fixed issue with printing multiple copies on HP printers and pull print release
- Changed output of account details outputted in log file

4.8.5 2.3.0 [2018-08-30]

+ Ability to easily configure high availability clusters for primary servers
+ Ability to use Equitrac embedded release terminals with SAFEQ Cloud
+ Ability to run service on multiple servers
+ Unattended installation of SAFEQ Cloud server
+ Extend Users UI to also show and edit non-local users
+ Ability to restrict user access to input ports based on user/group permissions
+ Change SAFEQ Cloud secondary gateways to not use direct DB connection
+ Ability to deliver print job data via IPP and IPPS in document output service
+ Added Strict domain validation feature
+ Ability to delete Pending jobs
+ Allow split of LDAP user and group lookup into different search DN's
x Increase security in configuration files
x Restrict Web TLS security to 1.2
x Add view log permission
x Expand installer connection port check for all required ports for primary
x Changed handling of mobile print jobs if an unknown page size is detected
x Improved loading of left navigation tree
x Changed default permissions for roles Reporting and Users
- Changed starting of secondary servers if restarted in offline cache mode
- Fixed issue where no email address supplied to MFD's for scan to email
- Fixed issue where adding private key chain to the root vendor broke relay document transfer
- Fixed PC Client wrong paper size
- Fixed issue where some jobs could stays in Windows spooler on client
- Fixed Ricoh printing issue with universal printer driver
- Fixed issue where Local auth provider on secondary server configured with primary auth service causes authentication delays
- Various UI improvements when editing printers or viewing print history
- Various UI improvements to installer for more helpful error messages
- Fixed issue where color print job released as BW was counted as color
- Fixed issue when deleting an account

4.8.6 2.2.2 [2018-06-05]

- Fixed issue deleting an account, causing broken deletion of triggers
- Fixed issue with card enrollment failing for certain scenarios of LDAP users

4.8.7 2.2.1 [2018-06-04]

- Sending certain PS jobs registered as PDF

4.8.8 2.2.0 [2018-05-29]

+ New PC client for Windows and MacOS for automatic creation and deletion of SAFEQ Cloud universal driver and print queues on PC workstations
+ Triggers and Automations engine for rule based workflows and automated tasks
+ Improve installer checks for common pitfalls; missing dependencies, firewall ports and similar
+ Ability to set SNMP community names for Xerox embedded configuration
+ Implement job deletion based on retention time (32 hours by default)
+ Added support for Mobile Print from Apple iOS and Android Apps
+ Added support for native Apple iOS AirPrint with Wide Area Mobile Print feature
+ Added ability to optionally specify UserID, username, authentication provider ID and account domain name in IPP URL
+ Added QR code generation for printers
+ Display server version in Server Settings
x Expand API for creating and deleting triggers and automations
x Added option to enable/disable scan application for HP embedded (scan app not relevant for FS4 models)
x Added loading indicator on Access Controls search
x Expand the input and output port Pending Jobs and History with additional data
x Extend public API to accept an extra header as an account domain name
x Preset default HP card reader values in UI to simply HP setup
x Extend API with ability to register cards to existing users and create users with cards
x Enhanced HP client for better compatibility with FS4 generation HP firmware
x Improved error handling for KM embedded deployment when KM device is locked, in use, in error or similar
x Enhanced KM embedded to support strict TLS 1.2
x Many minor Web UI improvements
x Enhancements for future proofing primary servers for backwards version compatibility with old secondaries
x Make email optional when creating user via API
x Enhanced page counting of jobs of certain types
- Fixed issue with document name and number of pages incorrect while printing from the Edge browser directly
- Fixed UI issues with LDAP and OU configuration
- Fixed issue where user in specific cases could create two of same services pointing to the same server
- Fixed issue with duplex printing as simplex if set from HP embedded
- Fixed issue with Scan app on HP gives error on FS4 models
- Fixed issue with Sharp embedded giving no relevant error if wrong login with card registration
- Fixed issue with KM Embedded where clicking Logout in the embedded terminal did not log the user out

4.8.9 2.1.0 [2018-02-19]

+ SAFEQ Cloud Reporting 1.0
+ Azure Active Directory Authentication
+ Ability to delete accounts, servers
+ Major improvements to future backwards compatibility
+ Major performance improvements
+ Added permission to control if users can modify logos on accounts
+ Interface for modifying USB card reader vendor and product ID's for HP MFD's
x Disable Web UI on secondary gateway servers
x Expand public API with output port and account creation calls

4.8.10 2.0.1 [2018-01-24]

+ Added Lexmark embedded support
+ Added Sharp embedded support (BETA)
+ Added region support for KM client (EU vs US)
x Improved secondary server performance when using embedded clients
- Bugfix for secondary server deployment when server hostname was not in /etc/hosts file
- Fixes and improvements for certain LDAP configurations

5 ABOUT SAFEQ CLOUD

As business models change, customers are moving away from existing, often complex, IT infrastructures. They're getting ready to modernize their print infrastructure and source future-proof solutions to take their print to the cloud. With new technology trends, IT is moving away from traditional on-premise data center hosting and towards cloud-native solutions; similar to other cloud services adopted internally (such as Microsoft, Amazon, or Salesforce), customers want to use "pay as you go" services in their print infrastructure.

A cloud solution allows them to simplify their IT infrastructure and get rid of the complexities associated with traditional print, including multiple print servers, additional infrastructure components, and a user setup that is difficult to support and maintain due to the nature of the print driver configuration and device setup. It also gives them the opportunity to unify and centrally manage all printers across an entire fleet, in multiple locations, so they don't have to suffer under the complications traditionally prevalent with legacy systems in large businesses with a broad presence and a need for a distributed infrastructure, resulting in substantial costs in terms of infrastructure investments and IT administration.

Imagine a solution where this administrative hassle and investment are significantly reduced by allowing customers to move the entire print infrastructure to the cloud. By utilizing a highly scalable Linux Server platform, we have developed a new solution to minimizing, or even removing, customer print servers and introducing an easy-to-use single print driver capability that enables customers to reduce or eliminate their print administration and support overhead. Moving the entire print management solution to the cloud enables the customers to capitalize on the benefit of a "pay as you go" OPEX transaction instead of a CAPEX investment.

5.1 WHAT IS SAFEQ CLOUD

SAFEQ Cloud is a true-cloud software platform that takes print infrastructures to the cloud and makes printing easier and more secure – for IT as well as the end users. It is a cloud-native full-stack platform, capable of providing organizations with full-fledged flexibility and all benefits of a Software as a Service (SaaS) offering while accommodating users with all the features of a traditional print management solution. SAFEQ Cloud is designed for elasticity, meaning it easily scales and fits into complex architectures. The solution meets customers wherever they are in their cloud journey, and scales up or down with them–at their pace. The solution offers simplicity, automated workflows, zero-trust security, serverless printing, and a smooth user experience.

SAFEQ Cloud is not only a SaaS offering but also a cloud-native print platform intended to enable solution providers to become a SaaS Print Management provider. YSoft SAFEQ Cloud is designed as a white-label product that enables service providers to offer and maintain their entire customer and reseller portfolio in the same highly scalable multi-tenancy cloud solution. This means that SAFEQ Cloud enables solution providers to become SaaS providers and offer their customers all the benefits of a cloud-based print infrastructure solution.

5.2 WHY SAFEQ CLOUD

SAFEQ Cloud is a cost-effective shortcut for you to become a cloud-first service provider almost instantly and enables you to offer your customers all the benefits of a subscription-based service while eliminating the recurring cost of operating a dedicated Print Management environment.

You will benefit from the same highly scalable Linux technology, be able to reduce or even eliminate print servers, dramatically reduce TCO or CAPEX for your customers, and become the messenger of a strong business case to your customers.

Being able to administer and host your entire customer portfolio from one centralized administration portal will optimize your support efficiency and improve the service level and "time to solution" for your customers.

By selecting SAFEQ Cloud as your print services platform, organizations and service providers will benefit from all the advantages of the newest cloud business models while having all the necessary features available in traditional on-premise print management solutions at their disposal.

5.3 ARCHITECTURE AND SOLUTION DESIGN

5.3.1 INTRODUCTION

This document is meant for solution designers who want to understand how the solution works, and in what ways it can be set up. While it is focused on SAFEQ Cloud hosted by Y Soft, other options are also mentioned.

5.3.2 ARCHITECTURE

In this document, you will find three scenarios represented by three example customer sites:

1. A site using direct print only.
2. A site using a local gateway (edge printing)
3. A site using pure cloud printing

These are the most common use cases, but there are more options for how data flow can be set up.

Note that all of these site options can co-exist in one customer environment.

Data flow and data processing in SAFEQ Cloud

Data input:

- Print jobs from the SAFEQ Cloud Client
- Mobile App
- Print to IPP(S) backend
- Using API
- Scan data from the MFD
- Chrome browser extension

Data processing:

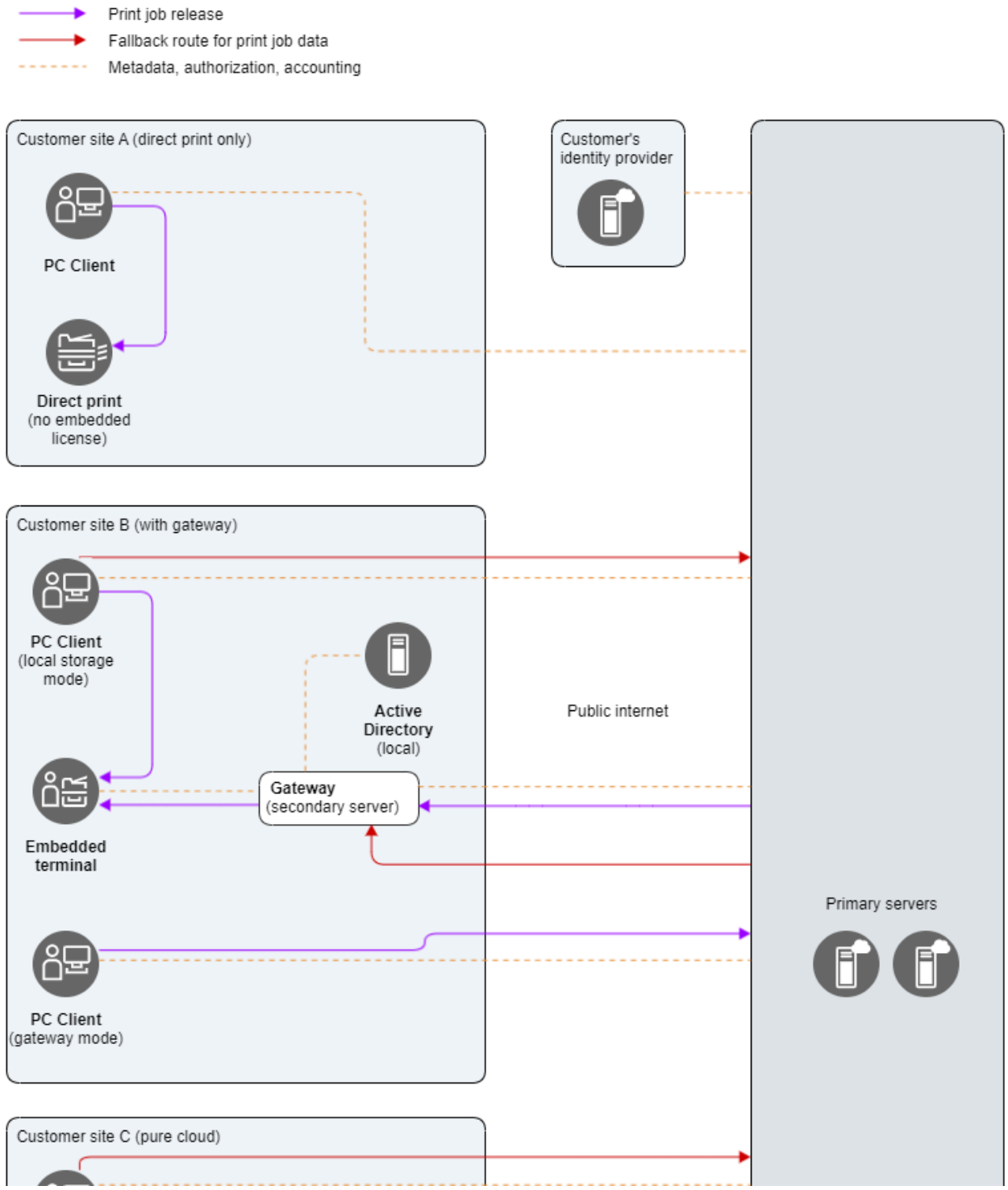
- Printing: additional finishing options can be applied using triggers and automation.

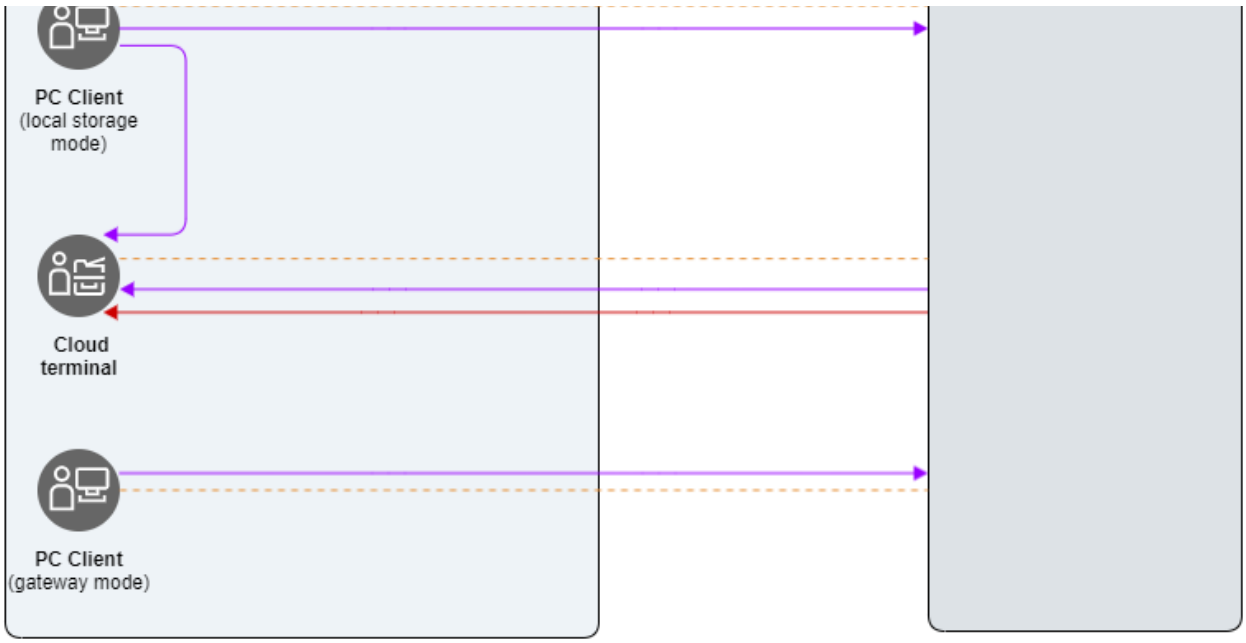
- Scanned documents are optionally processed using ABBYY FineReader OCR Engine (only available with SAFEQ Cloud hosted by Y Soft).

Data output:

- Print jobs are released after authentication, or without authentication, depending on the setup. They can also be held for printing again later.
- Reports on consumption are available in SAFEQ Cloud Web UI or via API.
- Scan connectors to multiple destinations.

Visualization





Customer site A - direct print only

- No embedded license is required for this case. You can add the license later, when the customer is ready to expand the feature set available to users.
- The main benefit is that the customers no longer need print servers. Setting up this scenario is extremely fast - after the printers and users are added to the Web UI, the SAFEQ Cloud Client automatically displays the correct print queues to all users.

Customer site B with a gateway (edge printing)

- Gateway is HW or SW component. For more information on gateways, see the *Gateways* section of this document.
- Print jobs can be routed in the following ways:
  - SAFEQ Cloud Client using local storage and connected to the primary server – the most common deployment.
  - SAFEQ Cloud Client using cloud storage and connected to the primary server – when the print jobs cannot be stored locally on the user's PC, for example, because the PC is set up to go to sleep mode shortly, print jobs can be routed to the cloud.
  - SAFEQ Cloud Client using gateway storage and connected to the secondary server (this scenario is not captured in the diagram schematics) – this setup may be useful if you want your devices to only accept print jobs coming from the Gateway. For example, for compliance reasons.

Customer site C - pure cloud

- No local HW is required for the full feature set of SAFEQ Cloud.
- Print jobs are routed through Cloud servers or using the SAFEQ Cloud Client with local storage.

Features available in each scenario

Feature	Description	Customer site A (direct print only, no embedded license)	Customer site B (with gateway)	Customer site C (pure cloud)
Supported devices	Supported printer vendors for the individual scenarios: Supported printers https://www.ysoft.com/safeq/hardware-compatibility-list/ysoft#cloud	All listed devices with PDF/ Postscript (and some PCL) printing (Brother, Canon, Epson, FujiFilm, HP, Konica Minolta, Kyocera, Lexmark, Ricoh, Sharp, Xerox)	All listed devices with PDF/Postscript (and some PCL) printing (Brother, Canon, FujiFilm, HP, Konica Minolta, Kyocera, Lexmark, Ricoh, Sharp, Xerox)	Fujifilm BI Aip6/7, Konica Minolta e and i series, HP WorkPath, Ricoh SOP (and more to come).
No more print servers! • queue management • driver management	Admin: Configures the locations in the SAFEQ Cloud Web UI. Users' print queues are created automatically. Everyone is using the same universal print driver. Users: their print queues are synchronized automatically by the SAFEQ Cloud Client See SAFEQ Cloud Client.	✅	✅	✅
Direct print	Submitted print jobs are printed at MFDs without authentication. Note: embedded license is not needed for this scenario.	✅	✅	✅

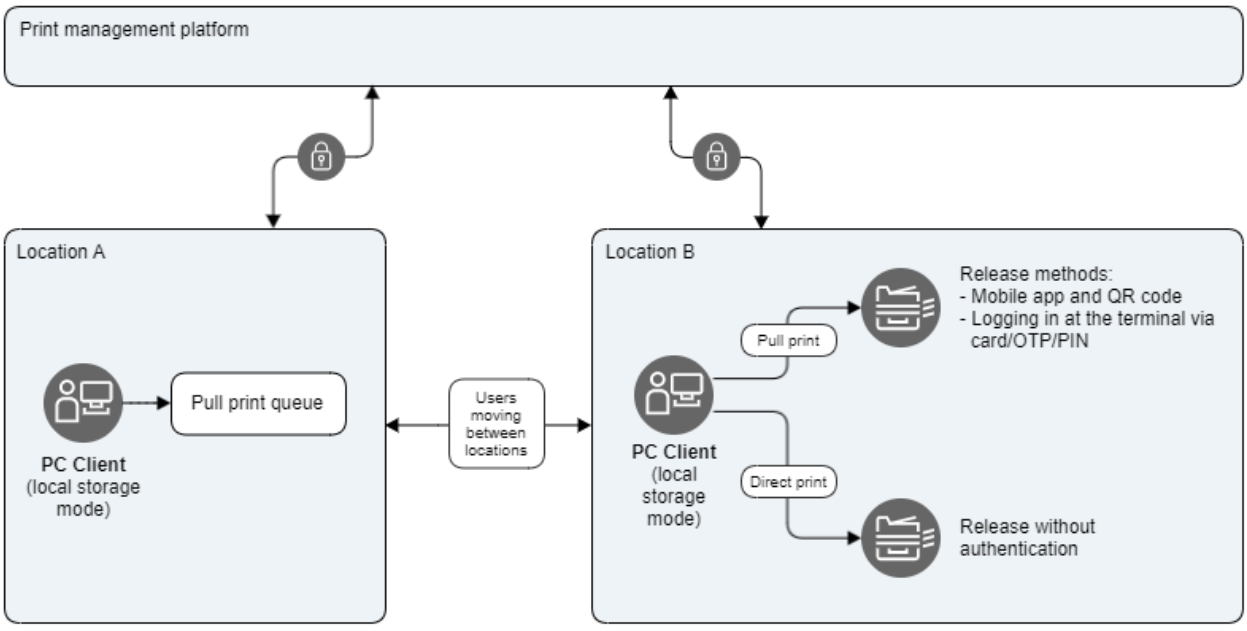
Pull print with embedded terminal (Also known as Print Roaming)	In this scenario, users send a print job to SAFEQ Cloud and authenticate at any connected MFD to release it. The MFD has an embedded terminal (client) deployed.	✗ Not applicable in this scenario.	✓	✓
Pull Print with QR code + mobile app (Also known as Print Roaming)	This scenario does not require a deployed embedded terminal (no need for a license). Authentication is done using a QR code and the mobile app. See Creating QR-codes and Using the Mobile app.	✓	✓	⚠ Available with local storage mode.
Scan Workflows (including OCR)	Scan the file to pre-defined destinations. See Scan workflows.	✗	⚠ Available for Fujifilm BI Aip6/7, HP WorkPath, Konica Minolta *e* and *i* series, and Ricoh	✓
Scan to email	Some devices offer additional scanning options	✗	⚠ • Available per device/ model. See Scan To Mail. • You can also use the native scan to email when available.	⚠ • Available per device/ model. See Scan To Mail. • You can also use the native scan to email when available.
User identity - cloud providers	See Authentication providers.	✓	✓	✓

User identity - local Active Directory (LDAP)	Connect to local Active Directory, Novell eDirectory, and IBM Domino. This requires a gateway to be deployed in the customer's environment. See LDAP authentication.	✗	✓	⚠ Gateway with visibility to the LDAP is required.
Chrome extension printing	SAFEQ Cloud Chrome extension can be installed on Chromebook or in the Chrome browser to allow direct and pull printing. See SAFEQ Cloud Chrome extension.	✗	✓	✓ Direct print not available
Wide Area mobile print (mDNS, AirPrint)	Users with compatible phones will see the available print queues. See Wide area mobile print.	✓	✓	✗
Mobile App	Use your phone to submit print jobs to the solution and release them. See Mobile print and Using the Mobile app.	✗	✓	✓
Reporting	⚠ SAFEQ Cloud does not act as a print accounting solution and only considers the attributes of a print job at the time of submission, whether it was overall sent as color vs. mono, and the total number of pages sent to SAFEQ Cloud. Changes in attributes at print time, print errors, or mixed color/mono jobs are not accounted for. See Reports.	✓	✓	✓
Using API	See API documentation.	✓	✓	✓

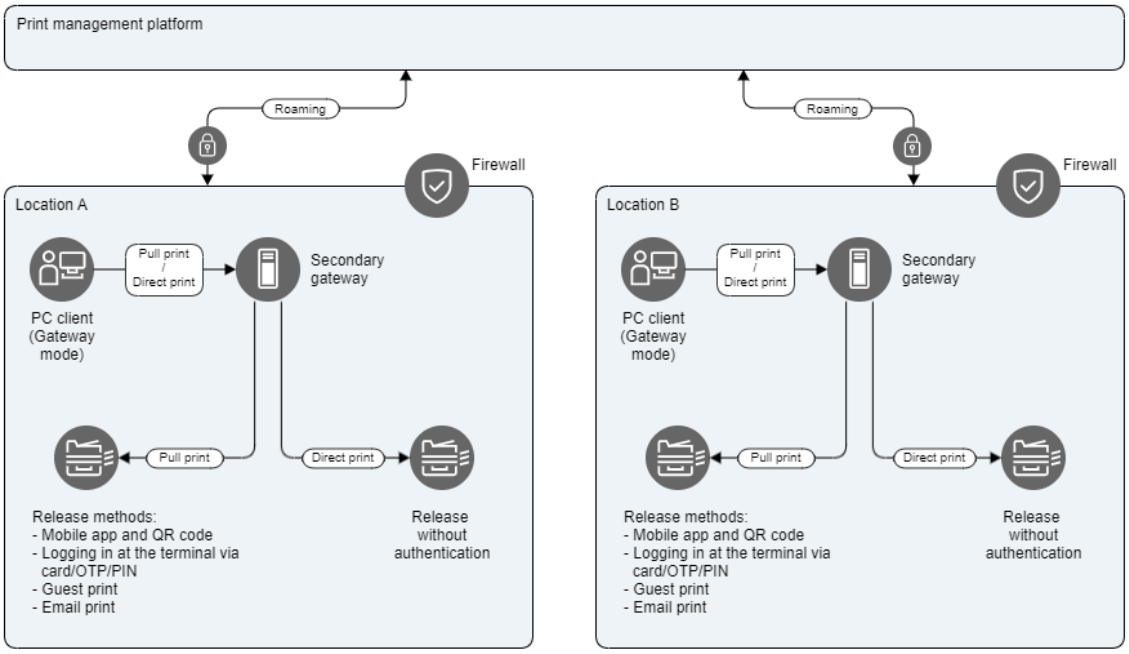
Basic finishing options	Tray selection, stapling, color/ bw, hole punching, simplex/ duplex	✅	✅	✅
Finishing options that perform layout altering changes after the job is submitted • Using triggers • Using API calls • At the embedded terminal screen	Change of paper size, orientation and scaling, booklet	✅	✅	⚠ Only when SAFEQ Cloud Client with local storage is used.

Print roaming

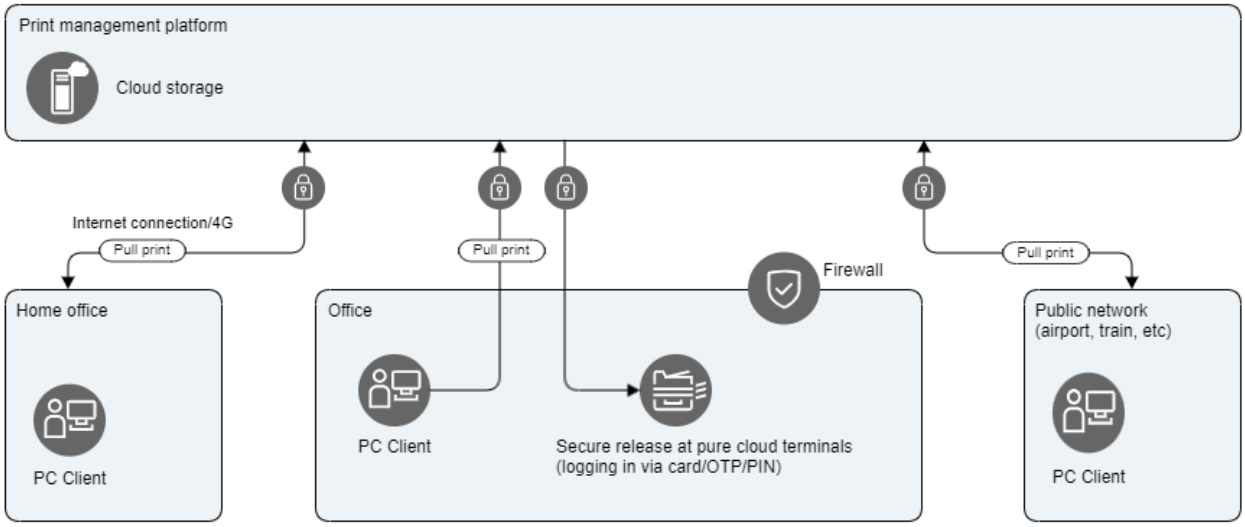
Scenario 1



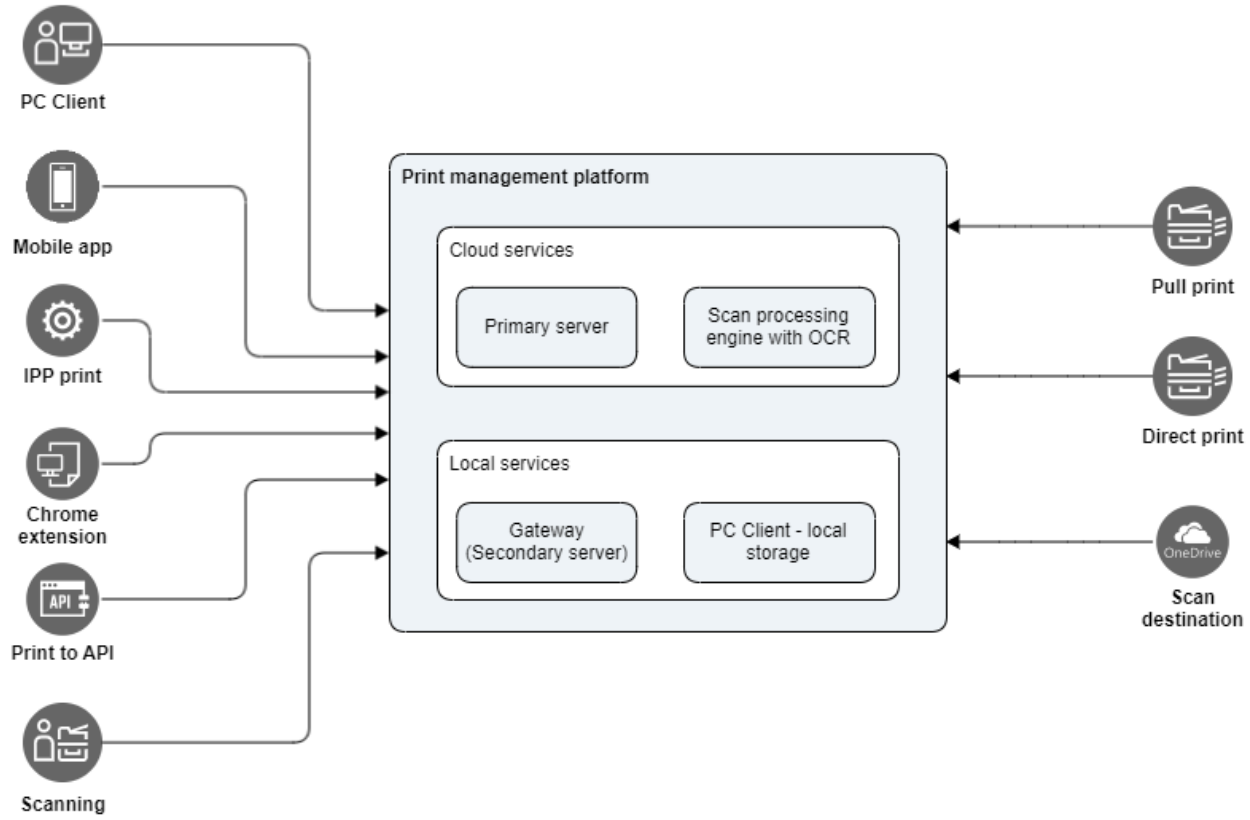
Scenario 2


Print management platform
Roaming
Roaming
Firewall
Firewall
Location A
Location B
Pull print / Direct print
Pull print / Direct print
Secondary gateway
Secondary gateway
PC client (Gateway mode)
PC client (Gateway mode)
Pull print
Direct print
Pull print
Direct print
Release methods:
- Mobile app and QR code
- Logging in at the terminal via card/OTP/PIN
- Guest print
- Email print
Release without authentication
Release methods:
- Mobile app and QR code
- Logging in at the terminal via card/OTP/PIN
- Guest print
- Email print
Release without authentication

Scenario 3


Print management platform
Cloud storage
Internet connection/4G
Pull print
Pull print
Pull print
Firewall
Home office
Office
Public network (airport, train, etc)
PC Client
PC Client
Secure release at pure cloud terminals (logging in via card/OTP/PIN)
PC Client

Data input - getting the data in



SAFEQ Cloud Client

SAFEQ Cloud Client is the most common way for users to submit their print jobs. It contains the Universal print driver. Customers opting for a custom print driver can set up an IPP(s) print queue and select their preferred driver in the configuration process. See Adding IPP print queue manually in Windows and Adding IPP print queue manually in Mac OS.

Print queue deployment

Print queues are automatically created on users' workstations based on the location configured by the administrator. This requires the Universal print driver.

Universal print driver

Universal Print Driver is used for automated print queue creation. See Supported printers.

Delivering the print job

There are two modes of operation:

1. Local storage mode – the SAFEQ Cloud client connects to the primary server via a persistent channel and performs all print and job storage operations locally. Local storage mode requires SAFEQ Cloud client registration and authorization in the SAFEQ Cloud server. When a user

prints, the jobs are stored on the PC. In case of Citrix or other VDI, it depends on where the SAFEQ Cloud Client is running, specifically the underlying SAFEQ Cloud Client service "SAFEQ Cloud Client Core" runs. Jobs are stored on the Citrix server (where client core service runs), and they will remain there when the thin session is terminated, assuming they have session retention etc configured in their VDI environment.

2. Gateway mode – the SAFEQ Cloud client sends all print jobs to the primary SAFEQ Cloud server, and has no persistent connection to the server. When the user prints, the jobs are delivered from the PC to the SAFEQ Cloud server, either primary or secondary gateway, depending on the configuration. Jobs are delivered to MFD using the *Document Output* service.

Jobs are delivered from the SAFEQ Cloud Client to the MFD directly if the SAFEQ Cloud Client can reach the printer. If the SAFEQ Cloud Client cannot reach the MFD, the job will automatically be routed via the primary SAFEQ Cloud server to the appropriate *Document Output* service, which will then deliver it to the MFD.

Supported platforms

OS	Supported
Windows	✅
Mac	✅
Linux	❌ Planned, beta available upon request

For more information, see SAFEQ Cloud Client overview.

Mobile App

The mobile app is available for Android and iOS. It allows users to submit print jobs and release them. For more see Using the Mobile app. and Creating QR-codes.

IPP Printing

You can print to the cloud servers directly using IPPS.

See Adding IPP print queue manually in Windows and Adding IPP print queue manually in Mac OS.

Chrome browser extension

SAFEQ Cloud Chrome extension can be installed on Chromebook or in the Chrome browser to allow direct and pull printing.

- Chromebook user authenticates via Chromebook user email address.
- Print queues are synchronized.

Scanning

Use scan workflows to scan data to the solution. See Scan workflows.

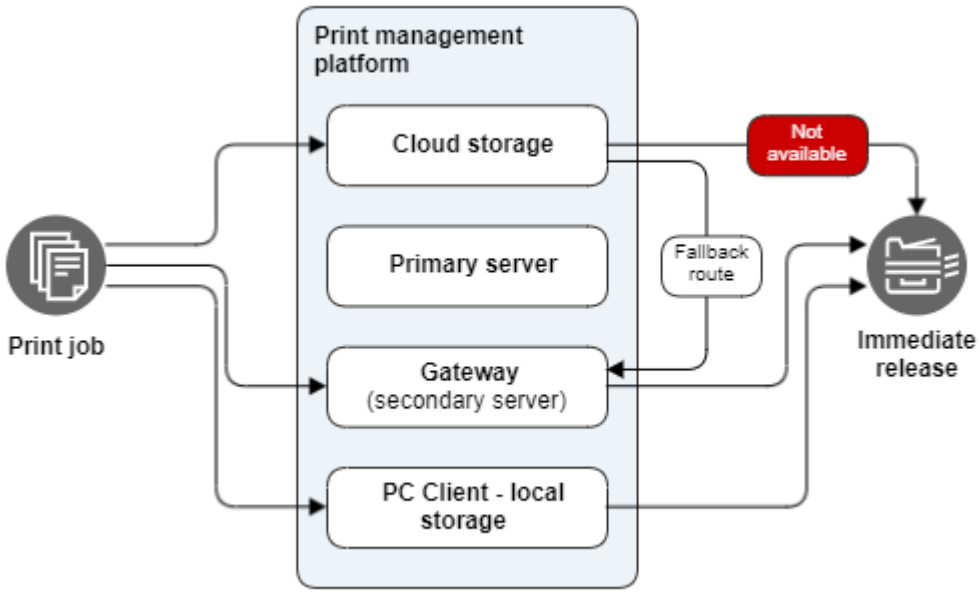
Using API

See API documentation.

Data output – printing

Direct printing

The print job is released immediately – users are not required to authenticate at the MFD. At the time of print job submission, users must select which printer they wish to use by selecting the respective Direct queue. Direct queue can route print jobs using local storage (SAFEQ Cloud Client) or Gateway. User's workstation must have network visibility to the MFD.

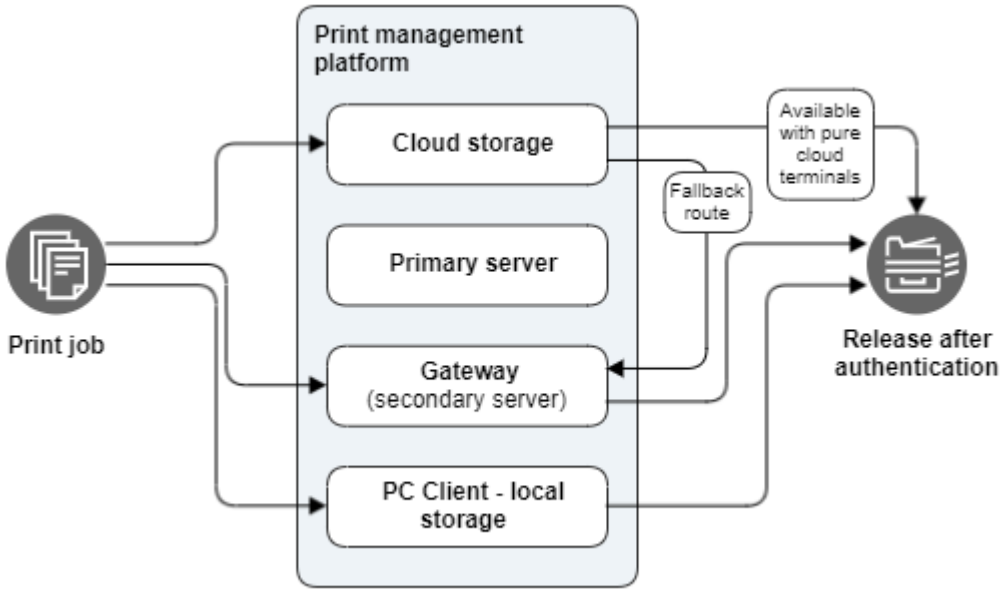


Pull printing

Pull print requires users to authenticate at the MFD, ensuring they are authorized to release the print job. The users send the print jobs to the Pull queue and choose where to release them by going to any compatible and connected MFD.

Users can release the print job via the following methods:

- Authenticating at an MFD with an embedded terminal. The available authentication methods are: card, PIN/Short ID, one-time password, username+password.
- Selecting the printer using the Mobile app.



For the fallback route to work, when the primary server is in the cloud and a document is printed from a secondary server in the local network, storage services must be enabled on both primary and secondary servers.

Data output - Scanning

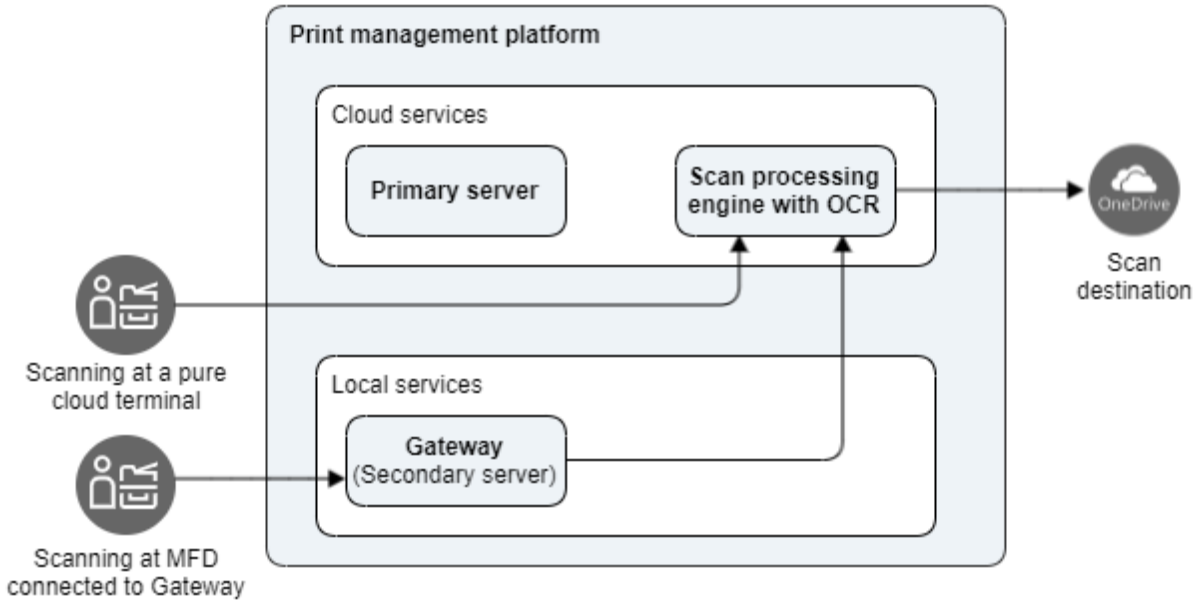
Scan Workflows

⚠ Scan Workflows are only available with the following embedded terminals: FujiFilm Aip6/7, HP WorkPath, Konica Minolta *e* and *i* series, Ricoh.
⚠ Scan Workflows are only available when hosting is provided by Y Soft.

ℹ The scanned data is always processed by Y Soft servers, even when a local gateway is used.

The solution uses ABBYY FineReader OCR Engine.

See Scan workflows. For the available scan connectors, see Connectors.



Scan to email

Available for selected embedded terminals or via native integration. See Scan To Mail.

Data output – MFDs, printers

Device integration	Required license	Capabilities and integration method
MFD	• Core	Direct printing • ✅ Can receive print jobs from SAFEQ Cloud Client • ✅ Can receive print jobs from Gateway • ✅ Mobile App with direct queue Pull printing • ✅ Mobile app with QR code Scan Workflows • ❌ Not available

Device integration	Required license	Capabilities and integration method
MFD with pure cloud terminal • Without a local gateway (most common) • With local gateway	• Core • Embedded	Direct printing • ✅ Can receive print jobs from SAFEQ Cloud Client • ✅ Can receive print jobs from Gateway • ✅ Mobile app with direct queue Pull print • ✅ Mobile app with QR code • ✅ Full terminal client for print job release and management Scan Workflows • ✅ Available
MFD with an embedded terminal with a local gateway	• Core • Embedded	Direct printing • ✅ Can receive print jobs from SAFEQ Cloud Client • ✅ Can receive print jobs from Gateway • ✅ Mobile app with direct queue Pull printing • ✅ Mobile app with QR code • ✅ Full embedded terminal client for print job release and management Scan Workflows • ⚠️ Only available at selected terminals

Gateways

Other terms for gateway are:

- Secondary gateway
- Secondary gateway server
- Secondary server
- Edge device

Architecture

There are two types of server in SAFEQ Cloud:

- Primary server – the primary server runs SAFEQ Cloud Web UI for configuration and management, handles core communication and connection to backend databases and similar master roles.
- Secondary gateway server – the secondary servers are additional server gateways that can run services.

Note that a "server" can take any form. It can be either a hardware or software appliance, or it can be implemented on existing server infrastructure, virtual or physical. It can run anywhere – in the public cloud, private cloud, completely disconnected on-premise, or on-premise connected to a primary in the cloud for central management. Regardless of whether it's primary or secondary, it can run a single service or all services, depending on the features needed for that particular node. There can be any number of primary and secondary gateway servers, from one individual server to tens of thousands of servers in a very large distributed configuration, without a single point of failure.

Gateways allow document storage and processing to remain local, ensuring document integrity and privacy are maintained. Only the print job's selected metadata are transferred to the cloud for management and reporting purposes via an encrypted channel. Document content remains secure because it never leaves your premises and thus never reaches cloud components. Data that are not present in the cloud cannot be externally compromised.

When to use Gateway

Gateways are optional. You only need them in the following scenarios:

- Some printers/MFDs do not support pure cloud terminals yet. A local gateway allows you to install embedded terminals at your MFDs.
- When you use local LDAP service (such as Active Directory, Novell eDirectory, IBM Domino), a gateway allows the primary server to access this local user database for authentication purposes.
- You need to keep your print jobs local for security or regulatory purposes.
- You wish to use mDNS printer discovery (Airprint).
- Your Internet connection parameters cannot support the use of cloud terminals with cloud printing because of low bandwidth, high latency, etc.

Gateway is NOT required for:

- Direct print-only deployments (see Customer site A scenario above).
- Direct or pull print with cloud terminal clients (see Customer site C scenario above).

OMNI Bridge

YSoft OMNI Bridge™ is a serverless Edge device, fully managed by Y Soft. It has been built to significantly simplify the deployment of the gateway.

See Setting up OMNI Bridge.

Virtual Gateway

The virtual software appliance is a pre-configured VM image, ready to run on a hypervisor such as VMWare ESX, Xen, Hyper-V or similar Infrastructure-as-a-Service solutions.

Using virtual appliances allows for extremely rapid provisioning and cleanly decouples the operator from the consumer by encapsulating all knowledge of the application within the virtual appliance. Gateway can be installed as a software appliance such as a Virtual Machine (VM) running at any Infrastructure as a Service (IaaS) provider, e.g. Amazon EC2 or Microsoft Entra ID.

See Gateway on Software Appliance.

Other HW Gateways

See Gateway on Hardware Appliance.

Sizing

YSoft OMNI Bridge™

Based on internal testing, we recommend one OMNI Bridge for every 15 printers. However, the customer's print volume, print job mixture, and volume during peak periods may affect the job processing and authentication timeframes. We will refine the recommendation as we gather more information from customer environments.

Other

There are no universal rules for server scaling, as it all depends on the printing volume, and number of users. The following are general recommendations for most scenarios.

	1-25 printers	26-100 printers	101-500 printers	501-1000 printers

CPU	2 cores/CPU's	4 cores/CPU's	4 cores/CPU's	8 cores/CPU's
Memory	4 GB	16 GB	16 GB	16 GB
Hard disk	SSD 64 GB	SSD 128 GB	SSD 256 GB	SSD 512 GB

5.3.3 HOSTING

SAFEQ Cloud is designed to offer several hosting options depending on which business model is being used. SAFEQ Cloud can accommodate service providers having their own data center, service providers having no data center, and also an on-premise private cloud solution for customers with high-security requirements.

Hosted by Y Soft

The platform can be installed in a Y Soft data center. As a partner, this gives you the ability to provide a hosted print solution without investing in a data center. You have full control of your customers and businesses through the SAFEQ Cloud Web UI as if SAFEQ Cloud was installed in your own data center.

Regions

Y Soft's data center infrastructure is available in the USA, Canada, The European Union, the UK, Singapore, and Australia regions.

Other options

Refer to this section or contact Y Soft for more hosting options.

5.3.4 USER IDENTITY

The following options are available:

- LDAP authentication
  - Requires Gateway to enable the network communication
- Microsoft Entra Authentication
- Google Workspace Authentication
- OKTA Authentication
- Auth0 Authentication
- PingID Authentication
- External card provider API authentication

See Authentication providers.

Single Sign-on

The following Single Sign-on options are available

- Microsoft Entra Single Sign-On
- Okta Single Sign-On
- PingId Single Sign-On

See Single Sign-On.

5.3.5 AVAILABILITY, SECURITY

Cloud services - hosted by Y Soft

Current services status can be seen on status page: https://status.ysoft.cloud/

Cloud services - hosted elsewhere

High Availability considerations for non-Y Soft hosting options are not in scope of this document. Refer to server deployment guides:

- Deployment documentation: Server Installation in custom deployment scenario
- Primary server clustering: Configure a primary server cluster

Security

See Security and privacy.

5.3.6 LIMITATIONS

- Scan Workflows
  - Only available with the new terminals. More terminals will be supported as they are replaced with the new ones.
  - Only available with SAFEQ Cloud hosted by Y Soft.
  - When scan to email is used, the print job is delivered via 3rd party service from a pre-configured email address. Customers cannot change this email source nor use their own email service.
- Modifying finishing options after the print job was sent is not available when the print job is downloaded to the pure cloud terminal. When cloud terminals are configured for cloud, it only works when local client storage is used.
- Reporting accuracy - the solution only considers the attributes of a print job at the time of submission, whether it was overall sent as color vs mono, and the total number of pages sent to SAFEQ Cloud. Changes in attributes at print time, print errors, or mixed color/mono jobs are not accounted for.

General Limitations of the embedded terminals

Vendor	Notes / Limitations	Reference responsiveness (OMNI/EDGE: embedded in the local 1Gbps network. Cloud: public 100Mbps up/down stream network)
Brother	• Always requires a gateway in the local network • GUI version 1 only • Doesn't support scan to my email or advanced scan workflows	• OMNI/EDGE: login to job list: ~3-4sec • OMNI/EDGE: pull print to first page: ~3sec
Canon	• Always requires gateway in the local network • GUI version 1 only • Doesn't support scan to my email or advanced scan workflows	OMNI/EDGE: login to job list: ~4-5sec
Epson	Direct print only	n/a
FujiFilm	Requires a Windows PC with visibility to the printer for initial deployment	• Cloud: login to job list: ~4-5sec • Cloud: pull print to first page: ~10sec • OMNI/EDGE: login to job list: ~8sec

HP	• OxPD variant:
	  • Requires a gateway in the local network (not needed for WorkPath)
	  • Has version 1 GUI only
	  • Doesn't support advanced scan workflows
	• WorkPath variant requires access credentials and deployment via the HP Command Center
		• OxPD: OMNI/EDGE: login to job list: ~5-12sec
		• WorkPath: Cloud: login to job list: ~4-5sec

Konica Minolta	• OpenAPI variant:
	  • Requires a gateway in the local network
	  • Has version 1 GUI only
	  • Doesn't support advanced scan workflows
	• IWS variant:
	  • requires access credentials and deployment via KM Marketplace (or KM IWS deployment tool for Europe & APAC)
		• OpenAPI: OMNI/EDGE: login to job list: ~4-8sec
		• IWS: Cloud: login to job list: ~4-5sec
		• IWS: OMNI/EDGE: login to job list: ~5sec

Vendor	Notes / Limitations	Reference responsiveness (OMNI/EDGE: embedded in the local 1Gbps network. Cloud: public 100Mbps up/down stream network)
Kyocera	• Always requires a gateway in the local network • GUI version 1 only • Doesn't support advanced scan workflows	OMNI/EDGE: login to job list: ~4-5sec
Lexmark	• Always requires a gateway in the local network • GUI version 1 only • Doesn't support advanced scan workflows	OMNI/EDGE: login to job list: ~4-5sec
Ricoh	• GUI version 2 variant requires a local PC with visibility to the printer for initial deployment • GUI version 1 and Java variant always requires a gateway in the local network • GUI version 1 and Java variant doesn't support advanced scan workflows	• version 1: OMNI/EDGE: login to job list: ~3-5sec • version 2: OMNI/EDGE: login to job list: ~3-5sec • version 2: Cloud: login to job list: ~4-5sec
Sharp	• Always requires a gateway on the local network • GUI version 1 only • Doesn't support advanced scan workflows	OMNI/EDGE: login to job list: ~5-6sec
Toshiba	Direct print only	n/a
Xerox	• Always requires a gateway in the local network • GUI version 1 only • Doesn't support advanced scan workflows	OMNI/EDGE: login to job list: ~4-5sec

For more information, see Known Issues and Limitations.

5.4 SECURITY AND PRIVACY

5.4.1 DOCUMENT SCOPE AND USE

This document provides an overview of the security features and practices implemented in YSoft SAFEQ Cloud solution. Information contained in this document is intended to assist Y Soft partners and end customers in understanding how the security of the solution is ensured and how the end customers may leverage the security features of the solution to maintain the confidentiality, integrity, and availability of their data.

The target audience for this document includes IT professionals, security professionals, and decision-makers responsible for selecting and implementing print management solutions in their organizations. This document also provides insight into the security controls implemented by Y Soft to ensure compliance with relevant regulations and standards.

More details about Y Soft secure development practices and other security-related topics are available in the security w hitepaper: https://www.safeq.com/cloud-print-security-whitepaper

5.4.2 Y SOFT SECURITY AND RISK FOCUS

Secure by design for both pure cloud and edge printing

SAFEQ Cloud service delivers cloud-based print, copy and scan services with optional edge components as per customer needs.

Y Soft and its Partners are jointly responsible for the security of their customers' print infrastructure. SAFEQ Cloud can be hosted either by Y Soft, by a Partner (within a Data Centre selected by Partner), or by the Customer.

By utilizing optional Edge virtual appliances or physical devices, we stand by our commitment to privacy even when on-premise infrastructure is required by the customer. Document storage and processing remain local to maintain document integrity and privacy. Only the print job's selected metadata travels encrypted to the cloud for management and reporting purposes. Document content remains secure because it never leaves your premises and thus never reaches cloud components. Data that is not present in the cloud cannot be externally compromised because they simply are not "there."

Customers may choose to implement SAFEQ Cloud in either shared or reserved instances. In a reserved instance, the document processing and storage are dedicated to one customer, so data is never exposed to any other entity. Document content and user identity thus also remain secure.

How does it work

SAFEQ Cloud (software) is embedded on multifunction devices (MFDs) and printers at the customer's business location. There, it is either connected to a Y Soft Edge device, (hardware or

virtual appliance) or directly to a cloud instance. The edge device is responsible for processing print jobs onsite. Even though it does the work of a server, the Edge device, much like a network router, is self-contained and needs no customer maintenance to perform its function – processing print jobs. A Virtual Appliance operates in a similar manner to the Edge hardware device but it runs on a customer-supplied server or virtual machine.

	Zero Trust Infrastructure	SAFEQ Cloud uses software-defined infrastructures in Cloud and Edge to provide auto-scaling and advanced networking and security. In Y Soft view of the Zero Trust approach, there are no trusted networks and zero implicit trust among services, instances, and clients. All system services, components, Edge devices, and (optionally) deployed MFDs are mutually authenticated, and all communication is secured using industry-standard protocols, such as TLS (Transport Layer Security) 1.3. Zero Trust is often perceived as a network-level architectural decision. Yet we believe that the Zero Trust approach needs to be applied holistically. SAFEQ Cloud service provides "beyond the network" Zero Trust capabilities, such as individual service recycling and tenant infrastructure recycling in multi-tenant environments. The following network protocols are primarily used: • HTTPS (HTTP over 1.3 with server authentication) • HTTPS with mTLS (HTTP over 1.3 with mutual-TLS authentication) • IPPS (IPP over HTTPS) • mTLS refers to TCP communication secured with mTLS (mTLS 1.3) Communication happens in 3 tiers: • Cloud : services exposed via publicly accessible endpoints (public cloud) • Edge-to-Cloud : bi-directional communication from Edge devices to Cloud services • On-premise : Edge to Edge, Mobile Clients, and Desktop Clients

	Zero Trust Secure Edge	In the case of optional Edge components, Zero Trust must also be applied on Edge devices. Again, securing only the services/applications running on the Edge device is not enough. Y Soft approach to Secure Edge using the Zero Trust principles provides the following capabilities: Trusted and Secure Device Identity - Each device maintains a trusted bond with its associated cloud tenant for management. Such identity is sufficient for establishing trust and unique identification of the device. This identity includes but is not limited to, secure establishment and storage of encryption and digital signing keys in a specialized secure enclave on the device. Trusted Path - Y Soft secure Edge devices provide trusted boot and trust path capabilities, which ensure that only trusted operating system can be booted and run on the device. This ensures decreased (or zero) attack surface and customer privacy and data integrity protection. Mutual Service Authentication - Once secure cloud and edge environments are established, all services and devices (including optional authentication for MFDs – if supported by the MFD vendor) are performed using mTLS industry standard protocol. Cloud Manageability - All cloud and especially edge deployments are securely manageable from the cloud, including seamless remote deployments and rolling / transitional updates and upgrades. Device-to-Cloud communication is secure, including mutual authentication. Remote Wipe of Customer Data - All customer data hosted on Edge devices can be remotely wiped using the cloud management capabilities.
Data transfer	**Print Job Data in transit: Workstation to Edge device & Edge device to the MFD**	Because the Edge device is secure in your trusted network, all print job data stays safely within your company's boundaries. Data is transferred via secured IPPS protocol for printers that support higher levels of data security. Support for legacy, unsecured protocols, such as LPR is also available, yet disabled by default.
	Print Job Data in transit: Workstation to Cloud & Cloud to the MFD	Data is transferred via secured TCP or HTTPS protocol to the cloud and downloaded from the cloud in the context of a user authenticated to the MFD. The MFD is trusted, using device-authenticated HTTPS protocol.

	Scan Job Data in transit: MFD to Edge/Cloud	Scan data are transferred to cloud services using device-authenticated WebDAV/S or HTTPS protocols, with authentication tied to a specific user context. The choice between WebDAV/S and HTTPS depends on the device vendor, as different manufacturers may implement different transmission methods. For Konica Minolta devices, HTTP2 must be enabled in the MFD WebDAV Client settings to ensure proper communication and data transfer.
	Scan Job Data in transit: Cloud to customer's email	Scan data sent to email are transferred via external email services. Data to the external email services are sent authenticated via TLS protocol. Y Soft uses Twilio SendGrid and Amazon Simple Email Service as external email services. The external email services use the TLS, DKIM, and SPF protocols to deliver the emails securely.
	Print job metadata: Edge device to cloud	Print job metadata is used for reporting purposes. Reports provide insight and an audit of print services use. Metadata includes print, copy, and scan activity on printers or groups of printers, users, or groups of users. It does not include the content of a document.
Data Access Permissions & Limitations	**RBAC**	Access to customer data is limited to authorized Y Soft or Y Soft partner reseller employees who require it for their job and whose data access is logged, and who have access only in specific cases. Secure portal communication between an administrator and the SAFEQ Cloud Web UI using TLS/HTTPS, compatible with the version supported by the client. SAFEQ Cloud may authenticate a user's identity at the print device by verifying against a company's directory. The device connects to Active Directory using an LDAP (Lightweight Directory Access Protocol) connector on the Edge device synchronized to the cloud service via a secured line. The product does not access any user passwords or other private data. For cloud directories (Microsoft Entra ID, Google, ...), standard OAUTH2 protocols are used. Secured separation between tenants' User Directories is in place for shared infrastructure customers.
	SSO	The use of Single Sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials to use SAFEQ Cloud.
	Internet security protocols	Browser access to the SAFEQ Cloud Web UI is through HTTPS, using role-based access within the application, authenticated via SAML, OAUTH2, and OpenID Connect industry standards.

	Cloud SQL Database (metadata)	Application metadata, configuration, job metadata, reporting, and generic user information are stored in the cloud provider's managed SQL database. A very limited number of highly trained specialists responsible for application maintenance and management on an as-needed basis have administrator access to the databases. Access to the data is logged in the cloud provider's audit logs.
	Application Logs	Application logs for troubleshooting are collected in the cloud provider's central log repository and available to support personnel on a need-to-know basis. Logs do not expose any access/credentials or document content information.
	Customer (tenant) specific metadata (users, devices, reporting, print job information, ...)	Role-based administrator access allows management of devices and system reports from the Web UI. This access can be assigned to the customer administrator and/or maintained by a certified Y Soft partner/reseller. Access to the customer application Web UI is limited to support personnel on an as-needed basis upon authorization by the customer during incident management sessions. For (alternative) shared infrastructure deployments, a set of support accounts is granted only to a very limited number of highly trained specialists responsible for application maintenance and management on an as-needed basis. Access to the data is logged in the cloud provider's audit logs.
	Application / Edge Device Updates	Edge device application is managed by industry-standard tools, protocols, and systems provided by the cloud provider platform. Deployment is managed via a tiered environment with separated development, testing, staging, and production environment, plus dedicated deployment plans per customer. Updates are deployed via encrypted and device-authenticated HTTP/S communication. Application components are stored in cloud provider's secured artifact repository and deployed to cloud instances and Edge devices using automated and secured state-of-the are tools (also provided by the cloud platform). All artefacts are created and deployed using a secured development lifecycle process and managed by a team of highly trained specialists responsible for application maintenance and management
Shared Infrastructure	**Shared Infrastructure**	One feature of shared infrastructure that makes it attractive to businesses is its low cost. This is due, in part, to servers managed by the service provider and the sharing of an underlying cloud-based application. The cloud-based application, in this case, SAFEQ Cloud provides services to multiple businesses, each one considered a separate 'tenant.' In this multitenant scenario, each tenant must have its own metadata identification, separation, and protection All the above-mentioned points apply. Each tenant owns a unique security certificate associated with its metadata.

User Identity Management

SAFEQ Cloud is built on modern authentication methods (OAuth 2.0) and utilizes Single sign-on (SSO) provided by external Identity Providers such as Microsoft Entra ID. SSO is a session and user authentication service that permits users to use one set of login credentials to access multiple applications. We recommend that customers who want to use SAFEQ Cloud use an external Identity Provider that manages the Internet identity of all their users. This approach allows admins to define the required level of user identity protection by enforcing multi-factor authentication. Another advantage is that users log in at browsers that they know (and consider secure) via Microsoft's authentication page, and SAFEQ Cloud merely receives information on the results. User credentials are safely confirmed by their external Identity Provider and never shared with the service provider (SAFEQ Cloud). The external Identity Provider provides SAFEQ Cloud with only basic user details such as their first name, last name, and username based on permissions and grants set in the Identity Provider

At MFDs, the users use cards and card readers to authenticate. Upon their first card authentication at the MFD, users are asked to confirm their identity so that the cards may be permanently assigned to their accounts.

Whenever a user logs in, SAFEQ Cloud refreshes the user details from the external Identity Provider – role membership changes, name changes, and account deactivation/reactivation.

5.4.3 THE SHARED SECURITY RESPONSIBILITIES

Y Soft and its Partners are jointly responsible for securing their customers' print infrastructure. SAFEQ Cloud can be hosted either by Y Soft, by a Partner (within a Data Centre selected by Partner), or by the Customer.

Hosted by Y Soft

In this scenario, Y Soft is responsible for the security of the underlying cloud service platform, network connectivity of the application, and physical data centers. Partners/customers are responsible for user management, account management, and data governance and rights management.

The shared security responsibility model differs from the typical security model a customer would see in an on-premises print environment. By using Y Soft's Cloud infrastructure, customers can leverage the underlying security, integrity & availability that SAFEQ Cloud provides, attaining a higher level of security relative to the investment required when managing the environment themselves.

Security responsibilities of Y Soft

In general, Y Soft is responsible for the security of its Virtual infrastructure, OS, and cloud services/products, and provides customers with the technical means necessary to protect their print service.

Y Soft ensures the cloud platform security by:

- Protecting the physical security of cloud data centers by outsourcing this to best-in-class vendors.
- Protecting the security of software, and network of the cloud platform by means of OS- and database-patch management, network access control, Anti-DDoS, and disaster recovery, etc.
- Identifying and fixing security vulnerabilities of the Application or the Cloud service in a timely manner without affecting partners'/customers' service availability.
- Cooperating with independent third-party security regulation to evaluate security and compliance of Y Soft cloud service security
- In Y Soft-hosted solutions, data is hosted by major third parties, who have a contractual obligation with us, ensuring they handle data according to GDPR requirements.

Security responsibility for Partners/Customers

Y Soft Partners/Customers (Data Controller) are required to meet strict safety and security demands, and these requirements naturally involve handling documents through SAFEQ Cloud. We see this as an opportunity and take on a proactive approach to fulfilling our duties, thereby helping you fulfill yours. This section describes individual actions that foster data security during the SAFEQ Cloud lifecycle:

- Y Soft will never use personal data for any other purpose than delivering the SAFEQ Cloud service. Further, it is ensured that any present and future sub-suppliers uphold local or regional data protection laws. For example, this means all data is stored on servers within one region, unless otherwise explicitly agreed upon.

- The Partner administrator or Customer administrator may however choose to retain the document in SAFEQ Cloud for a predefined number of minutes/hours hereafter – for example, to enable re-print. This will not impose a major security risk, other than more data is available in case of a breach.

Y Soft security and risk management objectives

- We have developed our security framework using best practices in the SaaS industry. Our key objectives include Customer Trust and Protection – consistently delivering superior product and service to our customers while protecting the privacy and confidentiality of their information.
- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity.
- Information and Service Integrity – ensure that customer information is never corrupted or inappropriately altered.
- Compliance with Standards – we design our corporate security program around the industry cybersecurity best practice guidelines including the Center for Internet Security (CIS) Critical Security Controls. Our controls governing the availability, confidentiality, and security of customer data are also designed to be SOC 2 compliant.

Y Soft Security Controls

To protect the data that is entrusted to us, Y Soft utilizes a defense-in-depth approach to implement layers of security controls throughout our organization. The following sections describe a subset of our most frequently asked-about controls.

5.4.4 Y SOFT PRODUCT INFRASTRUCTURE

Cloud Infrastructure Security

Y Soft does not host any SAFEQ Cloud within its corporate offices.

Y Soft outsources the hosting of its product infrastructure to leading cloud infrastructure providers. Our hosting provider guarantees between 99.95% and 100% service availability, ensuring all power, network, and HVAC services redundancy.

Y Soft's data center infrastructure is available in the USA, Canada, The European Union, the UK, Singapore, and Australia regions. The data center provider maintains an audited security program and physical, environmental, and infrastructure security protections. Business continuity and disaster recovery plans have been independently validated as part of their SOC 2 Type 2 and ISO 27001 certifications.

Our solution has been set up using three different Availability Zones in each region where the solution is deployed. This means we have multiple servers connected in a cluster environment with failover into different physical locations. If one zone fails for any reason, other servers located in a physically different location will automatically take over, completely seamlessly to users.

Our platform regularly undergoes independent verification of security, privacy, and compliance controls, achieving certifications against global standards to ensure it is the most secure in the industry. Recently our environment was assessed by IBM Nordcloud. Their report, "Well-architected review" confirms a high level of operational excellence, security, reliability, and performance efficiency for the SAFEQ Cloud production environment.

Network Security and Perimeter Protection

The Y Soft product infrastructure enforces multiple layers of filtering and inspection of all connections throughout the platform.

Network-level access control lists are implemented to prevent unauthorized network access to our internal product infrastructure. Firewalls are configured to deny network connections that are not explicitly authorized by default, and traffic monitoring is in place to detect anomalous activity.

Changes to our network security are actively monitored and controlled by standard change control processes. Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured.

To protect our Cloud environment requires the use of several professional tools, including:

- Security Hub evaluates configuration items to assess whether the resources comply with the desired configurations defined by the defined security standards.
- GuardDuty which is a threat detection service that continuously monitors for malicious activity and unauthorized behaviors to protect the account.
- Inspector tools – an automated security assessment service that helps improve the security and compliance of deployed applications. Inspector tools automatically assess applications for exposure, vulnerabilities, and deviations from best practices.
- IAM Access Analyzers help us to identify the resources in the organization, such as storage or Identity Access Management roles, that are shared with an external entity. This lets us identify unintended access to our resources and data, which is a security risk.
- Additionally, we periodically monitor trusted advisor findings to keep best practices for cost management, high availability, security, and performance.

Configuration Management

Automation drives Y Soft's ability to scale with our customers' needs. Server instances are tightly controlled from provisioning through de-provisioning, ensuring that deviations from configuration baselines are detected and reverted at a predefined cadence. If a production server deviates or drifts from the baseline configuration, it will be overwritten with the baseline configuration within 30 minutes.

All server-type configurations are embedded in images and configuration files. When the server is built, server-level configuration management is handled using these images and configuration scripts. Changes to the configuration and standard images are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the deployment of the instance.

Patch management is handled using automated configuration management tools or by removing server instances that are no longer compliant with the expected baseline and provisioning a replacement instance in its place. Rigorous and automated configuration management is baked into our day-to-day infrastructure processing.

Alerting and Monitoring

We also invest heavily in automated monitoring, alerting, and response capabilities to continuously address potential issues. The Y Soft product infrastructure is instrumented to alert engineers and administrators when anomalies occur. In particular, error rates, abuse scenarios, application attacks, and other anomalies trigger automatic responses and alerts to the appropriate teams for

response, investigation, and correction. As unexpected or malicious activities occur, automated systems bring in the right people to rapidly address the issue.

Many automated triggers are also designed into the system to respond immediately to unforeseen situations. Traffic blocking, quarantine, process termination, and similar functions kick in at predefined thresholds to ensure that the Y Soft platform can protect itself against a wide variety of undesirable situations.

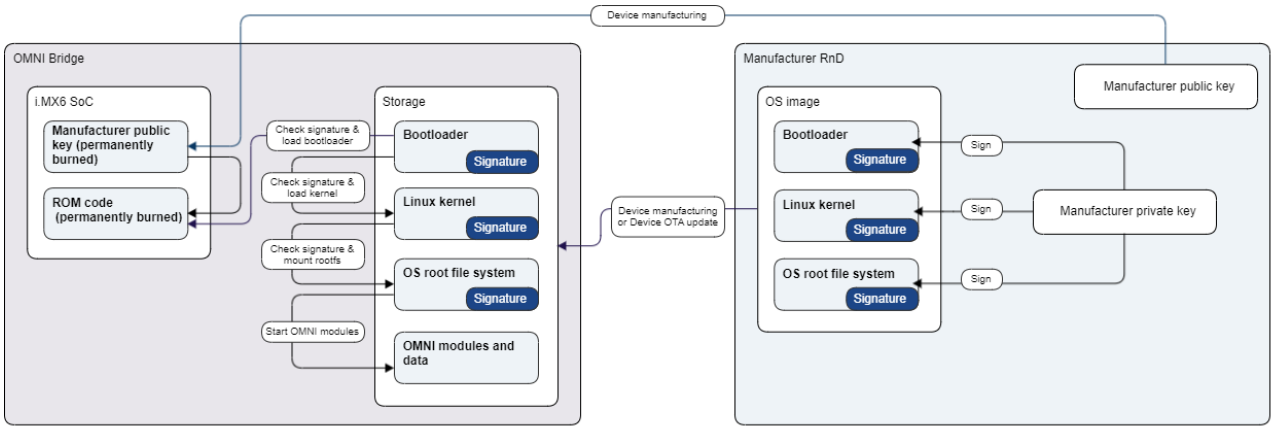
5.4.5 OMNI BRIDGE SECURITY AND PRIVACY

Operating System security

- The OMNI Bridge device is designed so that only OS images signed by the manufacturer can be booted on the device.
- The whole system is based around a security feature of the i.MX6 - High Assurance Boot (HAB)
- HAB provides a mechanism to establish a chain of trust from HW to the remaining SW components.
- HW -> bootloader -> kernel -> OS
- HAB uses public-key cryptography using the RSA algorithm.
- Public keys are permanently burned to the i.MX6 fuses during device manufacturing.
- THe OS images are signed, the public key is permanently and immutably burned to the i.MX6 processor in the device.

OMNI Bridge device boot process

- i.MX6 boot ROM loads and authenticates a bootloader image.
- Bootloader loads and authenticates kernel image with ramdisk.
- Init process in ramdisk authenticates the main read-only rootfs image and mounts it.
- The Init process mounts the read-write data partition.
- OS boot sequence finished.
- Starting OMNI modules (applications).



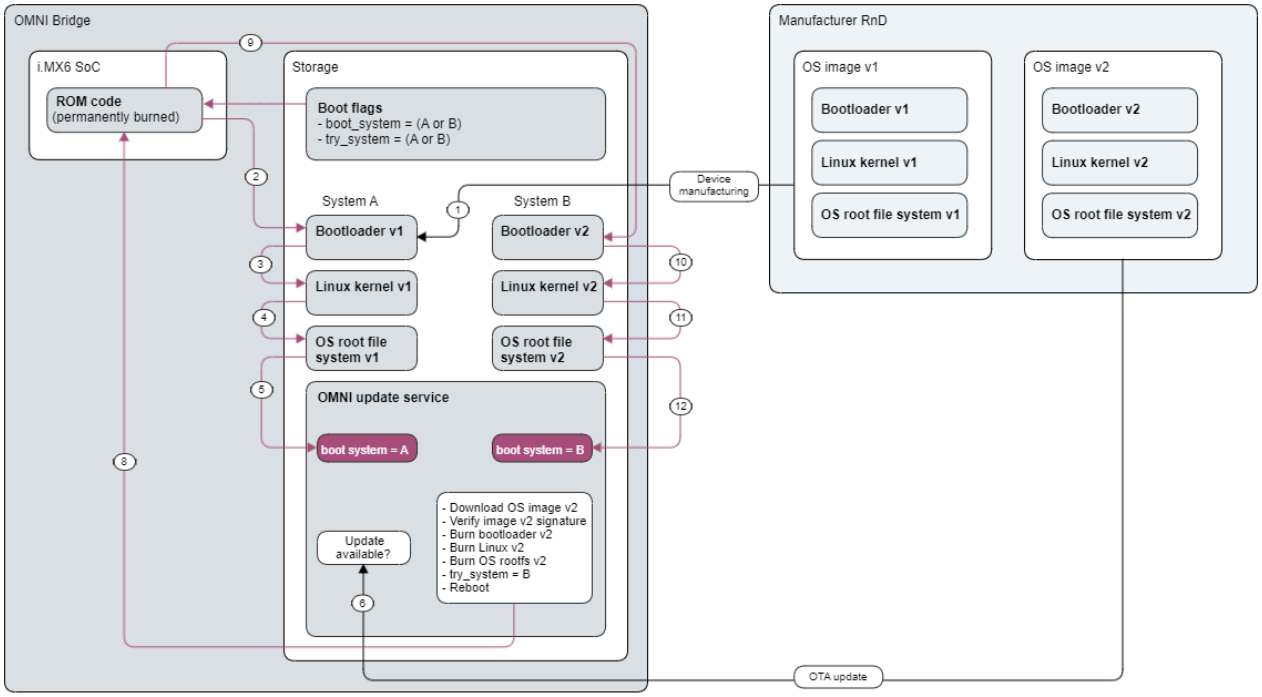
OMNI modules (applications) security

- All OMNI modules are signed.
- OS only allows the installation of modules that are signed by official keys.

- The content of the module image is immutable.
- Each module runs with a pre-defined set of privileges.
- Modules run in separate environments.
- The OMNI Bridge application storage: only authorized apps may access the data. There is no admin access that would be able to access this application data. Having said that, **the storage itself is not encrypted** for performance reasons. Accessing the stored data would require disassembling the device and desoldering the storage chip. Such operation is not possible without specialized equipment and expert HW skills and will likely result in destroying the OMNI Bridge.

OS update process

- The operating system on the device can be safely and securely updated.
- The update mechanism uses a so-called A/B partition scheme for reliability.
- Each component of the OS is duplicated (bootloader, kernel, OS).
- In case the update process fails at any stage, the system is reset and boots the previously working OS version.



OS identity and CA

- Each device has its own identity certificate.
- The private key never leaves the device; it is held in a blob that could be decrypted only on the given device.
  - The process is based on CAAM (Cryptographic Acceleration and Assurance Module) in the i.MX6 CPU.
- Identity certificates are signed by the manufacturer's CA in the factory.
- The device can also act as a CA and exposes necessary API
  - The main use is the signing of intermediate certificates for Azure world.

OMNI Bridge Factory reset process

- Factory reset process clears all application and customer data present on the device.

5.5 COMPATIBLE CARD READERS

In selecting a card reader for use with our systems, it is essential to understand the scope of support and service provided. Y Soft guarantees comprehensive support and assistance exclusively for Y Soft-manufactured card readers. For card readers not manufactured by Y Soft, while they may be compatible, the responsibility for support, including configuration and any required troubleshooting, falls solely upon the customer in cooperation with the manufacturer of the respective card reader. We strongly encourage customers to verify the support terms and services directly with the manufacturer prior to purchase and use with our systems.

Sr	Vendor	Card Reader	VID	PID
1	Y Soft	YSoft MFX-type card readers	214C	• 0202 – keyboard emulation mode • 0203 – KM LDD mode • 0205 – Sharp mode • 0309 – HP mode
2	Y Soft	YSoft USB Reader 3-type card readers	214C	• 0202 – keyboard emulation mode • 0203 – KM LDD mode • 0205 – Sharp mode • 0309 – HP mode
3	PaperCut	TWN3 MIFARE USB	09D8	0310
4	SB	SBR 0993 MIX	04D8	FE86
5	SafeCom	TWN3 Mifare USB	09D8	0206
6	SafeCom	TWN4 Mifare USB	09D8	0410
7	Elatec	TWN4 Mifare USB	09D8	0410
8	RFIDeas	pcProx Plus BLE, RDR-30581BKU	0C27	3BFA

9	RFIDeas	RDR-805H1AKU-X	0C27	3BFA
10	HP	X3D03A	03F0	0045
11	HID	OMNIKEY 5427G2 (Also known as AU-205H GEN2)	0×07 6B	0×5427
12	HID	OMNIKEY 5427G2 in keyboard mode (Also known as AU-205H GEN2)	0×07 6B	0×5428
13	inepro	SCR708 RFID Reader	1DA6	0110
14	inepro	Spider RFID Reader	1DA6	0110

5.6 SUPPORTED LANGUAGES

5.6.1 UI AND APPLICATIONS

Language	SAFEQ Cloud Web UI	SAFEQ Cloud Client	Mobile App	Chrome Extension
Brazilian	✓	✓		
Chinese (Simplified)	✓	✓		
Czech	✓	✓		
Danish	✓	✓		
Dutch	✓	✓		
English	✓	✓	✓	✓
Finnish	✗	✗		

Language	SAFEQ Cloud Web UI	SAFEQ Cloud Client	Mobile App	Chrome Extension
French	✓	✓		
German	✓	✓		
Hungarian	✗	✓		
Indonesian	✓	✓		
Italian	✓	✓		
Japanese	✓	✓		
Korean	✓	✓		
Malay	✓	✓		
Norwegian	✓	✓		
Polish	✓	✓		
Portuguese	✓	✓		
Romanian	✗	✓		
Russian	✗	✓		
Slovak	✓	✓		
Spanish	✓	✓		
Swedish	✓	✓		

Language	SAFEQ Cloud Web UI	SAFEQ Cloud Client	Mobile App	Chrome Extension
Thai	✓	✓		
Turkish	✗	✓		

5.6.2 CLOUD TERMINALS

Language	Konica Minolta IWS Gen 2	Konica Minolta IWS Gen 1	FUJIFILM BI	Xerox Gen 2	Ricoh Standard Gen 2	HP Workpath Gen 2	Sharp Cloud terminal
Arabic	✗	✗			⚠ (limitations apply)	⚠ (limitations apply)	✗
Basque	✓	✗			✓	✓	✓
Bulgarian	✗	✗			✓	✓	✗
Brazilian	✓	✗	✓	✓	✓	✓	✓
Catalan	✗	✗			✓	✓	✗
Chinese (Simplified)	✓	✗	✓	✓	✓	✓	✓
Croatian	✗	✗			✓	✓	✗
Czech	✓	✗	✓	✓	✓	✓	✓
Danish	✓	✓	✓	✓	✓	✓	✓
Dutch	✓	✓	✓	✓	✓	✓	✓

Language	Konica Minolta IWS Gen 2	Konica Minolta IWS Gen 1	FUJIFILM BI	Xerox Gen 2	Ricoh Standard Gen 2	HP Workpath Gen 2	Sharp Cloud terminal
English	✓	✓	✓	✓	✓	✓	✓
Finnish	✓	✗	✗	✗	✓	✓	✓
French	✓	✓	✓	✓	✓	✓	✓
German	✓	✗	✓	✓	✓	✓	✓
Greek	✗	✗			✓	✓	✗
Hebrew	✗	✗			⚠ (limitations apply)	⚠ (limitations apply)	✗
Hungarian	✓	✗	✓	✓	✓	✓	✓
Indonesian	✓	✗	✓	✓	✓	✓	✓
Italian	✓	✓	✓	✓	✓	✓	✓
Japanese	✓	✗	✓	✓	✓	✓	✓
Korean	✓	✗	✓	✓	✓	✓	✓
Malay	✓	✗	✓	✓	✓	✓	✓
Māori (New Zealand)	✗	✗			✓	✗	✗
Norwegian	✓	✓	✓	✓	✓	✓	✓

Language	Konica Minolta IWS Gen 2	Konica Minolta IWS Gen 1	FUJIFILM BI	Xerox Gen 2	Ricoh Standard Gen 2	HP Workpath Gen 2	Sharp Cloud terminal
Polish	✓	✓	✓	✓	✓	✓	✓
Portuguese	✓	✗	✓	✓	✓	✓	✓
Romanian	✓	✓	✓	✓	✓	✓	✓
Russian	✗	✗	✗	✗	✓	✗	✗
Slovak	✓	✗	✓	✓	✓	✓	✓
Spanish	✓	✗	✓	✓	✓	✓	✓
Swedish	✓	✓	✓	✓	✓	✓	✓
Thai	✓	✗	✓	✓	✓	✓	✗
Turkish	✓	✗	✓	✓	✓	✓	✓
Ukrainian	✓	✗	✓	✓	✓	✓	✓
Welsh	✗	✗	✗	✗	✓	✓	✗

5.6.3 EMBEDDED TERMINALS

Language	SAFEQ Cloud Legacy HP Workpath Gen 1 (OxPD), KM OpenAPI	SAFEQ Cloud Legacy Xerox Gen 1, Kyocera	SAFEQ Cloud Legacy Lexmark	SAFEQ Cloud Legacy Brother	SAFEQ Cloud Legacy Sharp Gen 1	SAFEQ Cloud Legacy Canon	SAFEQ Cloud Legacy Embedded Terminals
Brazilian	TBA	TBA					
Chinese (Simplified)	✓	✓		✓	✓	✓	
Catalan				✓	✓		
Czech	✓	TBA			✓		
Danish	✓	✓	✓	✓	✓	✓	
Dutch	✓	✓		✓	✓	✓	
English	✓	✓	✓	✓	✓	✓	✓
Finnish	✓	✓		✓	✓	✓	
French	✓	✓	✓	✓	✓	✓	
German	✓	✓	✓	✓	✓	✓	

Language	SAFEQ Cloud Legacy HP Workpath Gen 1 (OxPD), KM OpenAPI	SAFEQ Cloud Legacy Xerox Gen 1, Kyocera	SAFEQ Cloud Legacy Lexmark	SAFEQ Cloud Legacy Brother	SAFEQ Cloud Legacy Sharp Gen 1	SAFEQ Cloud Legacy Canon	SAFEQ Cloud Legacy Embedded Terminals
Hungarian							
Indonesian	TBA	TBA					
Italian	✓	✓		✓	✓	✓	
Japanese	TBA	TBA					
Korean	TBA	TBA					
Malay	TBA	TBA					
Northern Sami				✓	✓	✓	
Norwegian	TBA	TBA	✓				
Polish	✓	TBA	✓	✓	✓		
Portuguese	✓	TBA			✓		
Romanian							

Language	SAFEQ Cloud Legacy HP Workpath Gen 1 (OxPD), KM OpenAPI	SAFEQ Cloud Legacy Xerox Gen 1, Kyocera	SAFEQ Cloud Legacy Lexmark	SAFEQ Cloud Legacy Brother	SAFEQ Cloud Legacy Sharp Gen 1	SAFEQ Cloud Legacy Canon	SAFEQ Cloud Legacy Embedded Terminals
Russian	✓			✓	✓	✓	
Slovak	✓	TBA			✓		
Spanish	✓	✓	✓	✓	✓		
Swedish	✓	✓		✓	✓		
Thai	TBA	TBA					
Turkish							

5.7 Y SOFT HOSTED CLOUD ADDRESSES

From time to time customers who are hosted in the Y Soft cloud require the inbound and output IP addresses for example for opening only for specific IP addresses, or creating conditional access policies in Microsoft Entra ID or similar.

Below are the currently used IP addresses inbound and outbound for each Y Soft hosted region.

IP addresses are subject to change! Subscribe to service announcements on status.ysoft.cloud to be notified of changes to IP's.

To create your own custom domain names, do not use IP addresses, but instead CNAME. Please refer to Use your own custom domain names for more information.

Inbound IP's are relevant when a client (such as PC, secondary gateway, MFD or similar) connects across the Internet to the hosted SAFEQ Cloud cloud servers.
Outbound IP's are relevant when SAFEQ Cloud makes requests from the hosted SAFEQ Cloud cloud servers and to something across the Internet, such as Microsoft Entra ID.

5.7.1 EU REGION (*.EU.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
52.50.253.210	176.34.88.154
18.202.147.163	54.217.150.104
52.19.122.66	54.155.19.247
52.30.117.6 *(for Xerox devices only)*	-

5.7.2 EU CENTRAL REGION (*.EU-CENTRAL.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
18.159.1.221	18.184.95.83
52.57.32.65	3.66.14.128
3.78.120.145	18.199.47.109
18.197.12.40 *(for Xerox devices only)*	-

5.7.3 UK REGION (*.UK.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
3.8.221.201	18.134.42.232
52.56.154.204	3.11.157.65
18.135.59.42	3.10.114.230

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
18.130.67.94 *(for Xerox devices only)*	-

5.7.4 DE REGION (*.DE.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
80.158.108.210	80.158.110.114

5.7.5 US REGION (*.US.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
23.21.249.252	35.168.89.37
54.225.106.109	35.169.168.199
54.205.27.251	3.225.50.8
3.216.211.5 *(for Xerox devices only)*	-

5.7.6 CA REGION (*.CA.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
15.222.76.70	15.222.53.82
15.156.3.124	3.98.69.134
15.156.139.9	15.156.114.171

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
15.156.22.43 *(for Xerox devices only)*	-

5.7.7 AP REGION (*.AP.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
18.140.149.203	54.179.98.153
52.220.47.220	46.51.216.209
54.255.127.37	18.140.41.81
18.142.213.121 *(for Xerox devices only)*	-

5.7.8 AU REGION (*.AU.YSOFT.CLOUD)

Inbound (from Internet to SAFEQ Cloud cloud)	Outbound (from SAFEQ Cloud cloud to Internet)
54.153.223.24	13.236.170.166
13.237.129.18	3.106.171.162
13.238.29.243	13.237.17.215
54.252.96.106 *(for Xerox devices only)*	-

5.8 TRADEMARKS

Microsoft Azure, Microsoft Windows, Microsoft SQL, Microsoft Word, Microsoft Excel, Microsoft Powerpoint, Azure Intune, Microsoft Entra ID, Hyper-V are registered trademarks of Microsoft Corporation in the United States and/or other countries

AWS and Amazon Web Services are trademarks of Amazon.com Inc. or its affiliates

Mac OS, Apple iOS, Apple Bonjour, iTunes are trademarks of Apple Inc., registered in the U.S. and other countries and regions

Android, Google Chromebook, Google GSuite, Google Workplace, Google Play Store, Google Chrome, Google Gmail, Google Docs, Google Photos, Chrome Web Store, Google Admin Console are trademarks of Google LLC

Firefox is a registered trademark of the Mozilla Foundation

HP is a trademark of HP Hewlett Packard Group LLC

Ricoh is a trademark of Ricoh Company, Ltd.

Konica Minolta is a registered trademarks or trademarks of Konica Minolta, Inc

Sharp is a trademark of Sharp Corporation

Lexmark is a trademark of Lexmark International, Inc

Kyocera is a trademark of Kyocera Corporation

Xerox is a trademark of Xerox Corporation

Canon is a registered trademark of Canon Inc. in the United States and elsewhere

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both

openSUSE is a registered trademark of SUSE LLC in the United States and other countries

Red Hat, Red Hat Enterprise Linux, CentOS are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries
Ubuntu is a registered trademark of Canonical Ltd

Citrix, Xen and XenMobile are registered trademarks of Citrix Systems, Inc. registered with the United States Patent and Trademark Office and in other countries

VMAirWatch, VMware and the AirWatch logo are registered trademarks of VMware and its subsidiaries

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries

Intel is a trademark of Intel Corporation or its subsidiaries

Debian is a registered trademark owned by Software in the Public Interest, Inc

IBM and IBM Z are trademarks or registered trademarks of the International Business Machines Corporation

MobaXterm is a registered trademark of Mobatek

Postgres and PostgreSQL are registered trademarks of the PostgreSQL Community Association of Canada

Oracle and Java are registered trademarks of Oracle and/or its affiliates

OKTA is a trademark of Okta, Inc

MobileIron is a trademark of MobileIron, Inc

Blackberry and Good are the trademarks or registered trademarks of BlackBerry Limited

Adobe is a registered trademark or trademark of Adobe Systems Incorporated in the United States and/or other countries

pcProx is a registered trademark of RF IDeas, Inc

PaperCut logo and PaperCut are trademarks or registered trademark of PaperCut Software International Pty Ltd

Elatec is a trademark of Elatec GmbH

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

5.9 KNOWN ISSUES AND LIMITATIONS

5.9.1 SAFEQ CLOUD KNOWN ISSUES AND LIMITATIONS

API

SAFEQ Cloud Version	Limitation
3.21	Locations can be created/update via API using incorrect formats for the combination of locationData & locationType parameters.
3.0	Enabling plain API port on API service doesn't open port 7303. Workaround is to restart the server hosting the API service.

Core

SAFEQ Cloud Version	Limitation
3.44	When log4j2.xml file is updated, the log level on server is set to the value of SAFEQ CloudLogLevel parameter in this file.
3.38	Offline server cache is currently not working as intended and is under review.
3.10	When using loadbalancer without sticky session, webclients are not supported.
3.0	In some configurations, expired jobs not printed counts as printed in reports.

SAFEQ Cloud Version	Limitation
3.0	Page range print option does not work for TCP and IPP protocols.

Authentication

SAFEQ Cloud Version	Limitation
3.43	For Microsoft Entra and Okta identity providers, SAML is supported when using Service Account configuration.
3.40	Nested/transitional LDAP group memberships are not supported for ACL. Users must be direct members of the group configured in the respective ACL.
3.26	Cannot update an access control entry related to an inactive authentication provider.
3.11	Duplicate Card IDs can be set for the same user via SAFEQ Cloud Web UI & API.
3.10	Google authentication limited to use with Chromebooks for user creation.
3.0	IPP can in some configurations fail with "Authentication error" for Windows workstations joined an Azure domain with Azure AD configured in SAFEQ Cloud. Workaround: Use SAFEQ Cloud Client to distribute IPP queues or specify simple username in IPP path.
3.0	Azure AD authentication does not support multi-factor authentication "MFA". To enable 1FA authentication if 2FA is required, is to whitelist the SAFEQ Cloud server making authentication requests in Azure. Alternative is to use the "One-time password" feature in SAFEQ Cloud or Azure/ADFS single-sign-on.
3.0	Azure AD Authentication – user cannot login to SAFEQ Cloud if they have a 'sharepoint admin' role in Azure AD.

SAFEQ Cloud Web UI

SAFEQ Cloud Version	Limitation
3.39	When using a native scanning feature such as "Scan to my email," the scan job may initially appear as a print job type on the "My documents" page until fully processed.
3.20	Errors appear on Web UI when making modifications concurrently on Access Control by multiple users on the same customer.
3.0	Internal Error in SAFEQ Cloud Web UI when trying to delete pending print job from shutdown SAFEQ Cloud Client running local storage.
3.0	SAFEQ Cloud Web UI screen may become unresponsive after deleting a pending job from a storage which is offline/no longer available.

Mobile Printing

SAFEQ Cloud Version	Limitation
3.24	Airprint is not working with iOs version 15.5

SAFEQ Cloud Client

SAFEQ Cloud Version	Limitation
2024.11.28	Containers are not designed for PC Client connections. If an Account domain name of a container is specified in the configuration, the client will be unable to establish a connection.
3.27	In case of a heavy load, SAFEQ Cloud may start additional nodes and use them to store documents submitted to the cloud. After the load returns to normal, these nodes will shut down in order to conserve resources. As the documents are not stored in a shared cache, it is not possible to release a document stored on a terminated node. This problem can be solved by submitting the document(s) again.
3.19	The default printer within SAFEQ Cloud Client may not always be set.

SAFEQ Cloud Version	Limitation
3.15	At the moment, you can not set up any default driver options on the SAFEQ Cloud Client for Mac OS. For instance, BW/color and simplex/duplex as default. This is possible on the Windows SAFEQ Cloud lient.
3.0	the print queues are not removed if uninstalling just after printing and before logout.
3.0	For Citrix thin clients or Windows Terminal Services clients, user or location specific printers are not supported. Print queues created by the SAFEQ Cloud Client on Windows thin clients, are all created as shared among all sessions on the Citrix or Terminal Services host. When the SAFEQ Cloud Client detects the session is running in a Terminal Services session, it will not delete printers on custom logout.
3.0	macOS SAFEQ Cloud Client – print + staple using Adobe Reader DC with collate option not working as expected.

Search

SAFEQ Cloud Version	Limitation
3.10	Search function does not return results for Servers. You can utilise the Servers view and filter for Secondary Gateways by status (All/Online/Offline/Disabled/Updateable) to view these.
3.0	Nested group lookup not supported.

Security

SAFEQ Cloud Version	Limitation
3.8	TLS 1.3 cannot be enabled for channel communications over Port 2560 (messaging between Primary and Secondary Gateway, SAFEQ Cloud Client in "Local Storage" mode and Primary) – Limitation removed from version 3.24

System Infrastructure

SAFEQ Cloud Version	Limitation
3.0	On SUSE Linux default installations, the Linux servers own hostname doesn't always resolve to itself, depending on outside network DNS/DHCP configuration. Make sure the server can resolve its own hostname.

Users

SAFEQ Cloud Version	Limitation
3.0	Not all permission checks are enforced. Permissions relating to print functionality, such as Color Print, Copy, Scan etc, are not in effect.

Scan Workflows

SAFEQ Cloud Version	Limitation
3.35	Append/Prepend overwrite behavior does not work with PDF/A files produced by OCR.
3.35	The Compact PDF output format doesn't work properly in combination with all processing steps except Scan separation by page count — the scanned file is split into multiple pages.

Printing

SAFEQ Cloud Version	Limitation
3.44	The landscape layout for PDF files does not work properly when the user selects the "Print using system dialog..." option in a web browser.
3.38	Booklet bind direction Left to Right is always used.

5.9.2 EMBEDDED APPLICATIONS

General Embedded Functionality

SAFEQ Cloud Version	Limitation
3.30	One-time passwords can only be used for card enrollment and Web UI. It is not for logging in and printing, scanning, or copying at the terminal.
3.22	Amount of copies cannot be reduced on embedded clients if job is sent with multiple copies.
3.20	Embedded clients are limited to displaying 50 Pull Print jobs at any one time.
3.0	Not able to login to embedded release clients in the offline mode for Azure user.

Brother Embedded Application

SAFEQ Cloud Version	Limitation
3.22	Incorrect pages & totals are displayed on reports for copies using the duplex option.
3.22	Scan reports are not displayed on SAFEQ Cloud Web UI.
3.21	Card enrolment does not work with DNS & secure link.
3.21	Logout by card swipe does not work.
3.18	Unable to uninstall Brother embedded and after uninstalling user can still login & perform print functionalities.
3.15	Card swipe from Brother device home page may not enable login – swipe to login from application screen if affected.

Canon Embedded Application

SAFEQ Cloud Version	Limitation
3.13	The Canon embedded client only works with DNS using HTTP protocol via port 8704.
3.44	Canon Embedded Terminal can be installed only on MFDs in Europe.

HP OXPd Embedded Application

SAFEQ Cloud Version	Limitation
2025.03	When switching Home Screen mode from Secure Print to HP, app needs to be reinstalled
3.22	Color scan jobs are registered as BW under Reports.
3.12	Devices must have a screen size bigger than 2.7 inches.

HP WorkPath Embedded Application

SAFEQ Cloud Version	Limitation
3.25	User department & groups are not displayed on Job History API for Scan jobs.

KM IWS Embedded Application

SAFEQ Cloud Version	Limitation
3.24	Copy jobs not reported for bizhub C227 & C250i.
3.15	Logout by card swipe not working.
3.15	Unable to wake up KM MFD with IWS from sleep mode using card swipe.
3.13	No notification or message if the scanned document is too big to be sent by email.

KM OpenAPI Embedded Application

SAFEQ Cloud Version	Limitation
3.25	Web client is configured with Short ID instead of "username+password" (on the KM Bizhub C250i).
3.21	MS Azure OAuth2 & Okta user login & card enrolment does not work with no domain & OTP.
3.21	Logout by card swipe does not work for the currently logged user.
3.21	Card enrolment fails for LDAP users if no domain is entered.

Kyocera Embedded Application

SAFEQ Cloud Version	Limitation
3.41	Usernames longer than 32 characters are not supported for Kyocera devices.
3.36	Y Soft card reader is not compatible with Kyocera terminals.

Lexmark Embedded Application

SAFEQ Cloud Version	Limitation
3.23	Copy jobs not displaying under Reporting.
3.22	Cannot convert duplex jobs to simplex.
3.22	BW jobs are registered as color jobs under SAFEQ Cloud Web UI Reports.
3.0	The embedded terminal cannot be uninstalled from the administration Web UI.
3.0	Unable to uninstall the Lexmark embedded.

Ricoh SOP Embedded Application Gen1

SAFEQ Cloud Version	Limitation
3.21	ShortID & Password characters are not hidden immediately by asterix on device.
3.21	Using "admin" as a local SAFEQ Cloud admin username cannot login. Workaround is to use a different username for the local SAFEQ Cloud admin user.
3.0	Deployment report in UI as Installed in some rare cases despite Device not reachable error.

Sharp Embedded Application

SAFEQ Cloud Version	Limitation
3.23	Username & ShortID login options are always available even if not included in embedded config.
3.0	User is not logged out by card swipe.
3.0	The Sharp embedded terminal cannot be uninstalled from the administration Web UI.
3.0	While installing the sharp if the printer is rebooting then status on the GUI is struck in "installing".
3.0	Screen is not refreshed automatically when the configuration is changed from UserId login to ShortId login.
3.0	If the card reader is disconnected from the printer, not possible to login with username and password.

Xerox Embedded Application

SAFEQ Cloud Version	Limitation
3.23	Xerox VersaLink C605X – Copy Reporting is not working.
3.23	Xerox VersaLink – Delete job & refresh job list buttons not working.
3.22	Login for previous account still possible after new install & configure.
3.20	Card enrolment is not possible.
3.20	Advanced print button is not working.
3.0	Fails to deploy to C405 and 7845 as these models cannot support DNS/hostname for AuthenticationHostAddress. Workaround is to add secondary servers IP address to Account domains and map to server gateway with terminal service, in which case the IP address is used for Xerox Smart Auth AuthenticationHostAddress.
3.0	Copy and scan reporting not supported for Xerox embedded client.

5.10 REQUIREMENTS

5.10.1 SUPPORTED CLIENTS

The following clients are supported for sending print jobs to YSoft SAFEQ Cloud:

- Windows SAFEQ Cloud Clients with Internet Printing Port enabled, on the following versions of Windows:
  - Windows 10 or later
  - Windows Server 2012 R2 or later
- Mac computer clients, macOS Big Sur – version 11 or later
- Apple iOS devices. iOS 8.0 or later
- Android devices, Android OS version 5.1 or later
- Chrome version 44 or later for the Chrome extension

5.10.2 SUPPORTED PRINTERS

For SAFEQ Cloud to send print job data to printers, a Document Output Service must be able to deliver data to the printers IP address on port 9100 or IPP (for more details see section Ports and Protocols below).

SAFEQ Cloud single driver capability is supported on the following vendors:

Vendor	Driver		
	PostScript	PCL6	PDF
Brother	✔	⛔	⛔
Canon	✔	⛔	⛔
FUJIFILM BI	⚠ (limitations apply)	⛔	✔
HP	✔	⛔	⛔
Konica Minolta	✔	⛔	⛔
Kyocera	✔	⛔	⛔
Lexmark	✔	⛔	⛔
Ricoh	✔	✔	✔
Sharp	✔	⛔	⛔
Xerox	✔	⛔	⛔

Additional printer vendors are added continuously, so this list is not exhaustive. If a vendor/language combination is needed which isn't listed above, contact support.

YSoft SAFEQ Cloud can also receive raw print data streams from an IPP/IPPS client and deliver to a printer using any printer driver.

For more information on supported devices, see Hardware Compatibility List (HCL).

5.10.3 PORTS AND PROTOCOLS

The following is a list of possible ports used in SAFEQ Cloud. Ports required depend on the features, services, and architecture used.

SAFEQ Cloud uses TLS 1.3 for all internal communication (see Limitations for exceptions).

Cloud environments hosted by YSoft

All public AWS data centers, used by new customers.

Only cloud hosted

(Client to Cloud) Web Administration UI

Port	Protocol	From	To	Description
443	TCP HTTPS	Client Web browser	Cloud Primary Server(s)	HTTPS/SSL Web interface of the solution. Replaces port 8443 on environments with standard port 443 support.

(Client to Cloud) PC clients to server

Port	Protocol	From	To	Description
443	TCP HTTPS	SAFEQ Cloud Client, Client IPP	Primary Server	Authenticate users, retrieve printers, messaging exchange, send print jobs, and register as trusted endpoints. Replaces ports 2560, 7300, 7400, and 9631 on environments with standard port 443 support.

(Client to Cloud) Cloud terminal Integration to Server

Port	Protocol	From	To	Description
443	TCP HTTPS	Printer	Cloud Primary Server	Connection from Cloud terminals running on MFDs (e.g. HP Workpath Gen 2, KM IWS Gen 2, Ricoh Gen 2) and for sending scanned jobs (e.g. HP Workpath Gen 2, Ricoh Gen 2, KM IWS Gen 2). Replaces ports 7400, 8705, 8707, and 8711 on environments with standard port 443 support.

(Client to Cloud) Chrome Extension to Server (will be updated in following releases)

Port	Protocol	From	To	Description
7300	TCP HTTPS	Chrome Extension	API Service	Chrome Extension communicates with API to authenticate users, retrieve printers, and send jobs to SAFEQ Cloud.

(Client to Printer) Terminal Deployment Tool to Printer

Port	Protocol	From	To	Description
443	TCP HTTPS	Terminal Deployment Tool (Local PC)	Printer	Connection for installing terminal over HTTPS.
51443	TCP HTTPS	Terminal Deployment Tool (Local PC)	Printer (Ricoh only)	Connection for installing terminal over HTTPS
58070	TCP HTTPS	Terminal Deployment Tool (Local PC)	Printer (FUJIFILM BI only}	Connection for pushing configuration to FUJIFILM BI devices.

(Client to Printer) SAFEQ Cloud Client to printers – print operations

For SAFEQ Cloud Client in "Local Storage" mode:

Port	Protocol	From	To	Description
9100	TCP	SAFEQ Cloud Client (Document Output Service)	Printer	A document output service delivering print jobs to a physical printer.

Port	Protocol	From	To	Description
631	TCP HTTP	SAFEQ Cloud Client (Document Output Service)	Printer	A document output service delivering print jobs to a physical printer via IPP/S.
443	TCP HTTPS	SAFEQ Cloud Client (Document Output Service)	Printer	A document output service delivering print jobs to a physical printer via IPP/S.

(Client to Cloud - Legacy) Legacy Mobile Print to server

Port	Protocol	From	To	Description
7910	TCP HTTPS	Apple iOS clients	SAFEQ Cloud Mobile Print Service	AirPrint print jobs from Apple iOS devices (secure)
9444	TCP HTTPS	Y Soft Mobile App	SAFEQ Cloud Mobile Print Service	Authentication and document data from Apps (secure)

(Client to Cloud) Mobile apps

Port	Protocol	From	To	Description
443	TCP HTTPS	Y Soft Android / iOS Mobile App	API Service	Authentication and document data from Apps (secure)
9444	TCP HTTPS	Y Soft Android / iOS Mobile App	API Service	Authentication and document data from Apps (secure) for cases when a connection to port 443 can't be established
7400	TCP HTTPS	Y Soft Android / iOS Mobile App	Authentication Service	OAuth authentication from Apps (secure) for cases when a connection to port 443 can't be established

With on-premises gateway

Secondary server to Primary server

Port	Protocol	From	To	Description
443	TCP HTTPS	Secondary Server / Gateway	Primary Server	A secondary server communicating with the primary server for messaging exchange and server API. Replaces ports 2560 and 7300 on environments with standard port 443 support.

Secondary server to printers – print operations

Port	Protocol	From	To	Description
9100	TCP	Gateway Document Output Service	Printer	A document output service delivering print jobs to a physical printer.
631	TCP HTTP	Gateway Document Output Service	Printer	A document output service delivering print jobs to a physical printer via IPP/S.
443	TCP HTTPS	Gateway Document Output Service	Printer	A document output service delivering print jobs to a physical printer via IPP/S.

Secondary server to MFD's – embedded deployment

Port	Protocol	From	To	Description
161	UDP	Gateway Terminal Client Service	Printer	SNMP management
443	TCP HTTPS	Gateway Terminal Client Service	Printer	Deployment of the embedded client to MFD (all brands)
80	TCP HTTP	Gateway Terminal Client Service	Ricoh MFDs	Deployment of the embedded client to Ricoh MFDs
8080	TCP HTTP	Gateway Terminal Client Service	Ricoh MFDs	Deployment of the embedded client to Ricoh MFDs

Port	Protocol	From	To	Description
8451	TCP HTTP	Gateway Terminal Client Service	Canon MFDs	Deployment of the embedded client to Canon MFDs
51443	TCP HTTPS	Gateway Terminal Client Service	Ricoh MFDs	Deployment of the embedded client to Ricoh MFDs
8710	UDP	Gateway Terminal Client Service	Ricoh, Lexmark MFDs	Deployment of the embedded client to Ricoh and Lexmark MFDs
80	TCP HTTP	Gateway Terminal Client Service	HP MFDs	Deployment of the embedded client to HP MFDs
7627	TCP HTTP	Gateway Terminal Client Service	HP MFDs	Deployment of the embedded client to HP MFDs
10080	TCP	Gateway Terminal Client Service	Sharp MFDs	Sharp OSA communication, only for Sharp devices with embedded client
50003	TCP	Gateway Terminal Client Service	KM MFDs	Konica Minolta OpenAPI communication, only for KM devices with embedded client
8091	TCP	KM IWS Install Tool (local PC)	KM MFDs	Default port for installing IWS from the IWS Install Tool (not available in the US or Canada)

Embedded clients to a secondary server

Port	Protocol	From	To	Description
8700	SSL	Printer	Gateway Terminal Client Service	Connection from the embedded clients running on the Ricoh and Lexmark MFDs
8703	SSL	Printer	Gateway Terminal Client Service	Connection from the embedded clients running on the MFDs (except Ricoh and Lexmark)

Port	Protocol	From	To	Description
8704	TCP	Printer	Gateway Terminal Client Service	Connection from the embedded clients running on the MFDs (except Ricoh and Lexmark)
7301	TCP HTTPS	Printer	GatewayTerminal Client Service	Connection from the embedded clients running on the HP and Konica Minolta MFDs
7302	TCP HTTP	Printer	Gateway Terminal Client Service	Connection from the embedded clients running on the MFDs
7400	TCP HTTPS	Printer	Gateway Authentication Service	Connection from the embedded clients to Authentication Service OAuth service to register as trusted endpoints
14080	TCP HTTPS	Printer	Gateway Terminal Client Service	Connection from Equitrac server for embedded clients running on the MFDs
14081	TCP HTTP	Printer	Gateway Terminal Client Service	Connection from Equitrac server for embedded clients running on the MFDs
14082	TCP HTTPS	Printer	Gateway Terminal Client Service	Connection from the Ricoh SLNX Share embedded clients running on the MFDs
14083	TCP HTTP	Printer	Gateway Terminal Client Service	Connection from the Ricoh SLNX Share embedded clients running on the MFDs

Embedded clients to Cloud Server or Gateway

Port	Protocol	From	To	Description
7301	TCP HTTPS	Printer	Gateway Terminal Client Service	Connection from the embedded clients, HP Workpath Application and KM IWS, running on the MFDs
7400	TCP HTTPS	Printer	Gateway Authentication Service	Connection from the embedded clients to Authentication Service OAuth service to register as trusted endpoints

Port	Protocol	From	To	Description
9444	TCP HTTPS	Printer	Mobile Gateway Service	Connection from the embedded clients, HP Workpath Gen 1 Application and KM IWS Gen 1, running on the MFDs

OMNI Bridge Edge Gateway to Microsoft IoT Hub

Port	Protocol	From	To	Description
443	SSL	Edge Gateway	mcr.microsoft.com	Microsoft Container Registry
443	SSL	Edge Gateway	*.data.mcr.microsoft.com	Data endpoint providing content delivery
443	SSL	Edge Gateway	*.cdn.azcr.io	Deploy modules from the Marketplace to devices
443	SSL	Edge Gateway	global.azure-devices-provisioning.net	Device Provisioning Service access
443	SSL	Edge Gateway	*.azurecr.io	Personal and third-party container registries

Port	Protocol	From	To	Description
443	SSL	Edge Gateway	*.blob.core.windows.net	Download Azure Container Registry image deltas from blob storage
5671, 8883, 443	AMQP, MQTT, AMQP over WS	Edge Gateway	*.azure-devices.net	IoT Hub access
443	SSL	Edge Gateway	*.docker.io	Docker Hub access
443	SSL	Edge Gateway	*.ysoft.cloud	Platform
443	TCP	Edge Gateway	Primary Server	A secondary server communicating with the primary server for messaging exchange

Port	Protocol	From	To	Description
443	TCP HTTPS	Edge Gateway	Primary Server	A secondary server communicating with the primary server API
443	UDP NTP	Edge Gateway	*.google.com (or anything else you set on OMNI Bridge)	NTP server (time{1-12}.google.com) or any chosen NTP server
80	TCP	Edge Gateway	ports.ubuntu.com	Official Ubuntu package repository for non-x86 architectures
443	TCP	Edge Gateway	cdn.everyoneprint.com	Secondary Installation Files

Mobile device to built-in DNS

Port	Protocol	From	To	Description
53	UDP, TCP	Mobile device	Gateway Mobile Print Service	Needed for AirPrint via DNS-SD (makes only sense for Secondary Server)
8053	UDP, TCP	Mobile device	Gateway Mobile Print Service	Needed for AirPrint via DNS-SD (makes only sense for Secondary Server)

(Client to Cloud - Legacy) IP card reader to Server

Port	Protocol	From	To	Description
7300	TCP HTTPS	IP card reader	Gateway API Service	IP card reader communicate with API to authenticate users
7303	TCP HTTP	IP card reader	Gateway API Service	IP card reader communicate with API to authenticate users

Existing devices connected using legacy ports

Secondary server to Primary server

Port	Protocol	From	To	Description
2560	TCP	Secondary Server / Gateway	Primary Server	A secondary server communicating with the primary server for messaging exchange
7300	TCP HTTPS	Secondary Server / Gateway	Primary Server	A secondary server communicating with the primary server API

Web Administration UI

Port	Protocol	From	To	Description
8443	TCP HTTPS	Client Web browser	Cloud Primary Server	HTTPS/SSL Web interface of the solution

SAFEQ Cloud Clients to server

Port	Protocol	From	To	Description
2560	TCP	PC Client	Primary Server	SAFEQ Cloud Client in the "Local Storage" mode communicating with the primary server for messaging exchange
7300	TCP HTTPS	PC Client	API Service	SAFEQ Cloud Client communicate with API to authenticate users and retrieve printers
7300	TCP HTTPS	PC Client	API Service	SAFEQ Cloud Clients sending standard print jobs to the server

Port	Protocol	From	To	Description
7400	TCP HTTPS	PC Client	Authentication Service	SAFEQ Cloud Client communicate with Authentication Service OAuth service to register as trusted endpoints
8631	TCP HTTP	Client IPP	IPP Service	SAFEQ Cloud Clients sending IPP/HTTP print jobs to the server
9631	TCP HTTPS	Client IPP	IPP Service	SAFEQ Cloud Clients sending IPPS/HTTP print jobs to the server

Cloud terminal Integration to Server

Port	Protocol	From	To	Description
7400	TCP HTTPS	Printer	Authentication Service	Connection from the embedded clients to Authentication Service OAuth service to register as trusted endpoints
8705	HTTPS	Printer	Terminal Client Service	Cloud terminal integration (SQTS) – connection from Cloud terminals running on MFDs (e.g. HP Workpath Gen 2, KM IWS Gen 2, Ricoh Gen 2) and for sending scanned jobs (e.g. HP Workpath Gen 2, Ricoh Gen 2)
8707	TCP HTTPS	Printer	Terminal Client Service	Cloud terminal integration – connection from Cloud terminals running on MFDs which provide scan data using SwA protocol (mainly Fuji terminals)
8711	TCP HTTPS	Printer	Terminal Client Service	Cloud terminal integration – connection from Cloud terminals running on MFDs which provide scan data using WebDAV protocol (KM IWS cloud terminals)

Edge Gateway to Microsoft IoT Hub

Port	Protocol	From	To	Description
2560	TCP	Edge Gateway	Primary Server	A secondary server communicating with the primary server for messaging exchange

Port	Protocol	From	To	Description
7300	TCP HTTPS	Edge Gateway	Primary Server	A secondary server communicating with the primary server API

5.11 LICENSING

5.11.1 TENANT LICENSE EXPIRATION

The expiration time of the customer license is set at 23:59:59 of the expiration date shown on the license information page, local time zone of the data center where the tenant is hosted.

When the trial or the production license expires for the tenant, the following functions will stop working:

- New print jobs will not be accepted by the server or PC client
- It will not be possible to add a new printer to the system

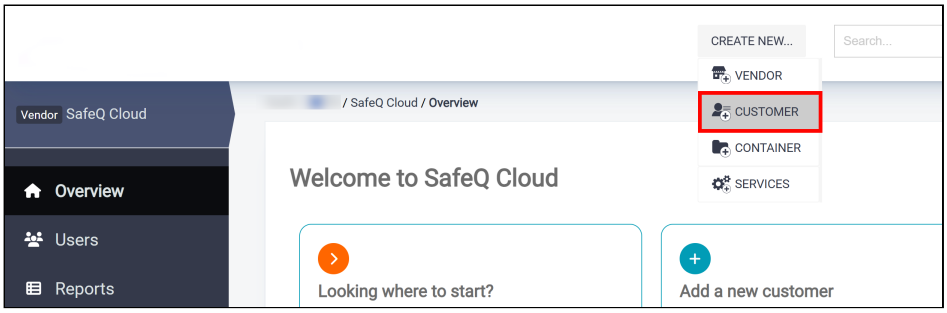
6 QUICK START FOR VENDORS

Target audience: Vendors.

This guide provides you with information on how to create a SAFEQ Cloud tenant for your customer.

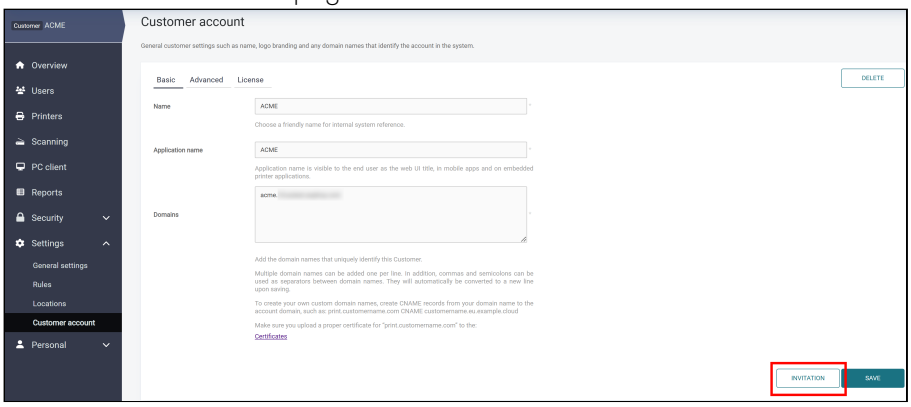
6.1 CREATING A NEW TENANT (CUSTOMER)

1. Log in to SAFEQ Cloud web UI using your vendor account.
2. Click **Create new** and select **Account**.

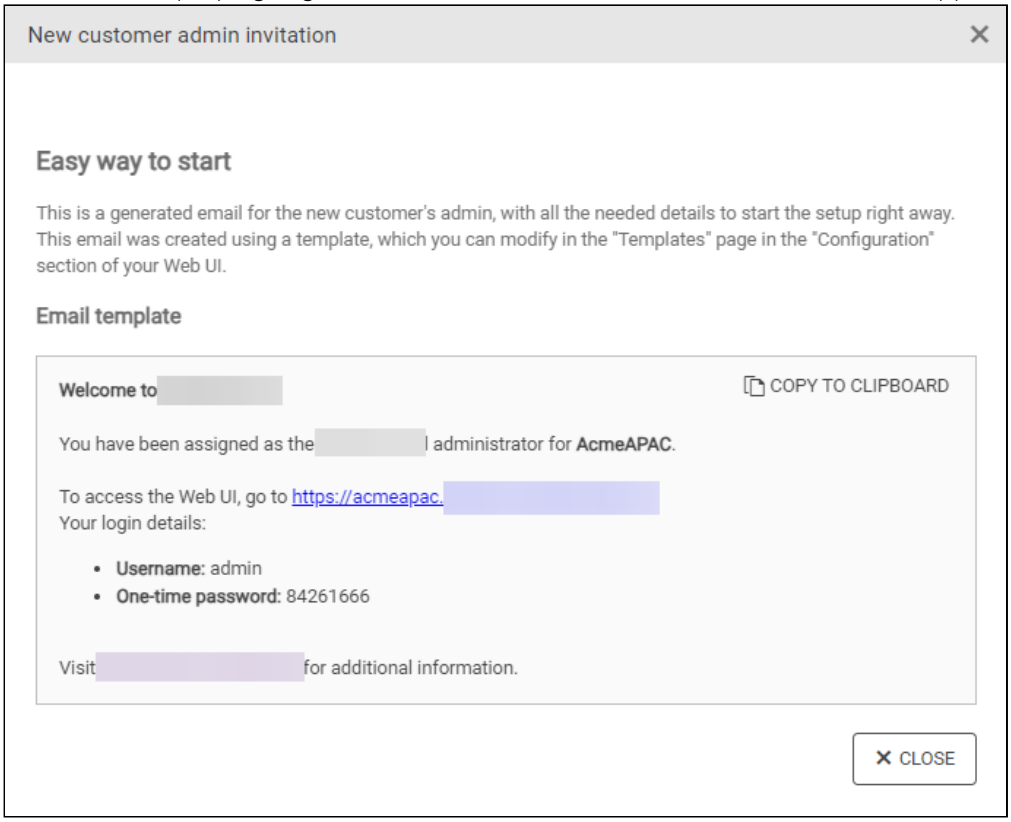


3. Fill in the following information:
   - **Name** – Set a name for the new customer.
   - **Domains** – The format is *<customer>.<region>.ysoft.cloud*
     - *customer* – Replace with the subdomain of the customer account in SAFEQ Cloud.
     - *region* – Data region. This must match with the region where your vendor account was created.
   - **Application name** – This name will be displayed when you hover over the tab with SAFEQ Cloud Web UI in your browser.
   - **Default language** – Select a language from the menu.
   - **Default paper size** – Select paper size from the menu.
   - **OEM Logo** – Upload a file with the customer's logo.
4. Click **Save**.
5. If SAFEQ Cloud is hosted by you as the vendor or by the customer as on-premise solution, enter the license key that you have obtained for the customer in the **License** section of SAFEQ Cloud Web UI.

6. Immediately after creating a new customer, you will see a new **Invitation** button on the Customer information page. Click the button.



7. A window displaying a generated invitation to the customer admin will appear.

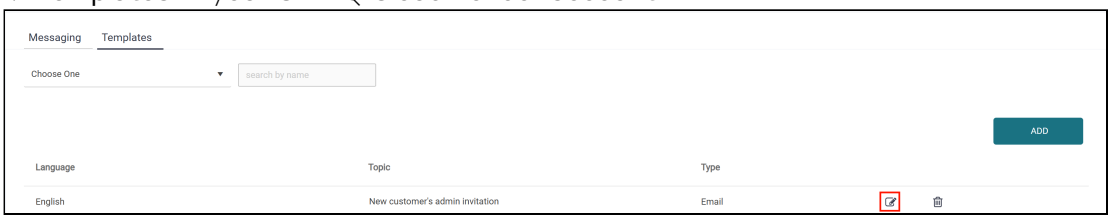


8. Copy the message to your clipboard and send it from your email client.

If you have agreed with the customer to do the configuration for them, log out from your vendor account, log in with the Customer admin account, and continue to Quick start for admins. If your customer will be using OMNI Bridge devices, see Setting up OMNI Bridge.

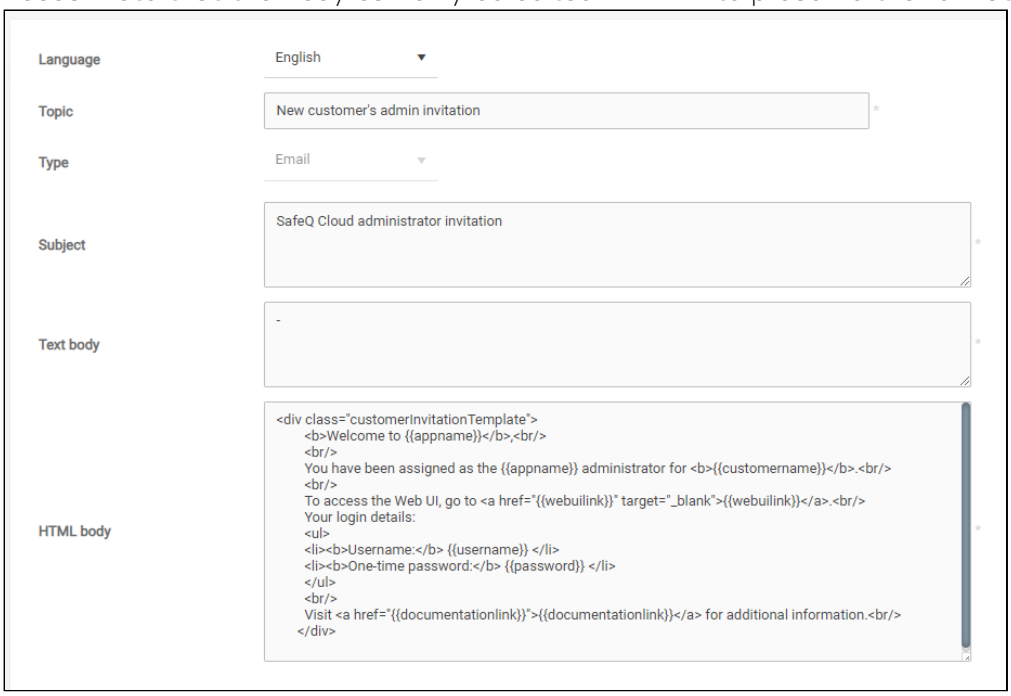
6.1.1 EDITING THE INVITATION MESSAGE

1. If you wish to edit the invitation message to the customer, go to **Settings** → **General settings** → **Templates** in your SAFEQ Cloud vendor account.



2. Click the edit icon next to **New customer's admin invitation**.

3. A new dialog window will open. Edit the **Topic**, the **Subject**, and the **Body** according to your needs. Note that the Body can only be edited in HTML to preserve the formatting.



4. You can use the following variables in the template:

Variable	Value
`{{appname}}`	Name of the application based on the branding
`{{customername}}`	Name of the customer
`{{documentationlink}}`	Link to the documentation based on the branding

Variable	Value
`{{password}}`	One-time password generated for the admin user
`{{username}}`	Name of the admin user
`{{webuilink}}`	Link to the Web UI of the customer

The template name (Topic) is critical for the system to locate and display the correct template. If the name changes, the system may not find the template, and the "Invitation" button will not be shown. Ensure that the template name remains unchanged to avoid any issues.

7 QUICK START FOR ADMINS

The following is an outline of the basic steps to configure your SAFEQ Cloud. Your setup may differ according to what kind of queues, authentication, terminals, etc, you are going to use.

For more advanced concepts and settings, refer to the Admin guide, Reference documents, and Legacy documentation.

7.1 PREREQUISITES

Your tenant in SAFEQ Cloud is created, and you have received your username and password to log in to the SAFEQ Cloud Web UI.

7.2 CONFIGURING AUTHENTICATION

SAFEQ Cloud supports the following types of authentication:

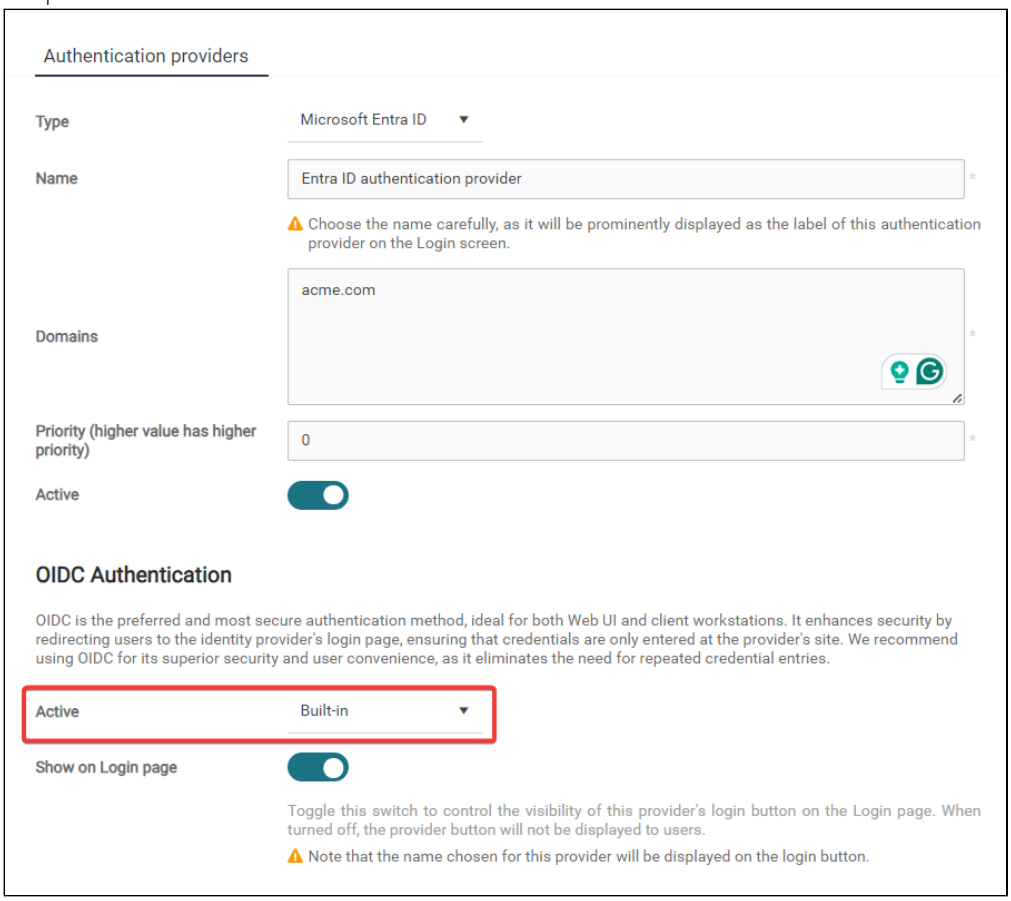
- Local user authentication – you can create user accounts within SAFEQ Cloud. Users then log in to SAFEQ Cloud with these accounts.
- Authentication to external directory – users log in with their existing user accounts from identity providers such as Microsoft Entra, Google, etc. This can be done via:
  - OIDC
  - Service account (Service access)
  - Client-side authentication

For details, see Authentication providers.

7.2.1 EXAMPLE: SETTING UP MICROSOFT ENTRA AUTHENTICATION USING THE BUILT-IN OIDC

1. In SAFEQ Cloud Web UI, go to Users > Authentication.
2. Click Add.
3. Fill in:
   a. Name – Enter an internal name used for identifying the particular authentication provider configuration.
   b. Type – Select Microsoft Entra ID.
   c. Domains – Enter your organization's domain or domains. It should match "@domain" part of the users who will use it to authenticate to SAFEQ Cloud. For example, to allow user john.doe@acme.com to log in via this Authentication provider, enter the *acme.com* domain here.
   d. Priority – A number that determines the order in which authentication providers will be called until one succeeds.
   e. Active – If enabled, this authentication provider will be used for authentication.

f. In the **OIDC Authentication** section, enable the built-in OIDC by selecting **Built-in** from the dropdown list.



4. Click **Save**.

5. By default, every user logged in via this provider will have the **Authenticated Users** group assigned in **Users > Access control** section of SAFEQ Cloud. For more details, see Access Control.

For more information on Entra ID authentication, see Microsoft Entra authentication.

7.3 ADDING A PRINT QUEUE

SAFEQ Cloud offers two types of print queues – Direct queues and Pull queues. A Direct queue sends the print job directly to the output printer. A Pull queue sends the job to the Storage Service in SAFEQ Cloud. When the user wishes to print, goes to an MFD with a SAFEQ Cloud terminal installed, and logs in, the MFD pulls the print job(s) from SAFEQ Cloud.

If you wish to use a direct print queue, the simplest way to add it is when registering your MFD. See the next section of this manual – *Adding an MFD*.

If you wish to use a Pull queue, perform the following steps:

1. In SAFEQ Cloud Web UI, go to **Printers > Print queues**.

2. Click **Add**.
3. In **Name**, enter the name of your queue.
4. In **Queue type**, select **Pull print queue**.
5. Click **Save**.

For more information, see Print queues.

7.4 ADDING AN MFD

If you wish to use Direct print queues, the only step you need to do is to register your MFDs. See Printers.

If you wish to use Pull print queues, your MFDs must have SAFEQ Cloud terminals installed. The installation method differs according to the MFD brand and according to the type of the terminal:

- Pure cloud terminals (for MFDs that can connect to the cloud directly)
- Terminals that require a SAFEQ Cloud secondary gateway in your network

See Embedded Terminals.

In general, the process always consists of:

1. Doing the MFD-specific setup in the MFD UI. Either directly at the MFD, or in the MFD's web interface. This is described in the guide for each brand in the Embedded Terminals section.
2. Creating the Embedded configuration for the particular brand of MFD. See Embedded Terminals' configuration.
3. Registering the MFD in SAFEQ Cloud Web UI. See Printers.
4. Installing the terminal on the MFD. Depending on the type of the terminal and the MFD brand, you can do this by one (or more) of the following options:
   a. Deploying the Embedded configuration to the MFD from SAFEQ Cloud Web UI. See Embedded Terminals' configuration, section *Deploying the configuration*.
   b. Installing the terminal via a command-line tool from your PC. See Terminal Deployment Tool.
   c. Installing the terminal from the vendor's marketplace or app store. E.g. Konica Minolta or Ricoh.

7.5 INSTALLING SAFEQ CLOUD CLIENT

SAFEQ Cloud Client is a desktop application that can be installed on end-user workstations to create print queues and install the SAFEQ Cloud universal driver automatically. For its features, see SAFEQ Cloud Client.

The Client can operate in two modes: Local storage mode and Gateway mode. For details, see SAFEQ Cloud Client overview.

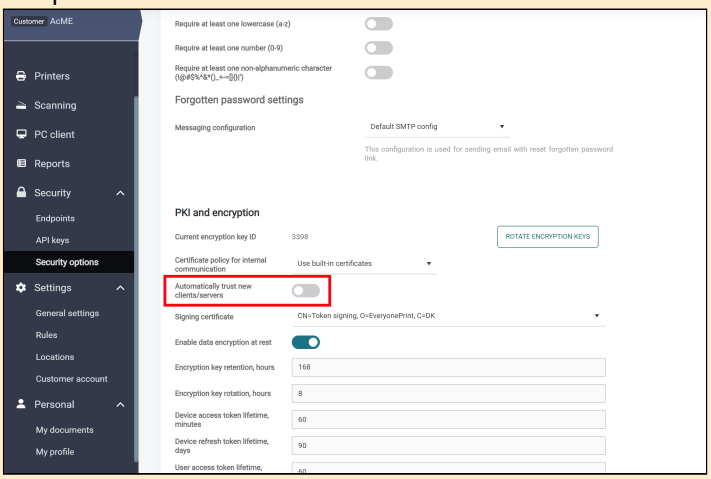
Both modes can be used in the Pure Cloud printing scenario, but we recommend using the Local mode. In the Pure Cloud printing scenario, the Gateway mode has the following limitations:

- Direct printing is not possible.
- Releasing the print job from the Mobile application is not possible.

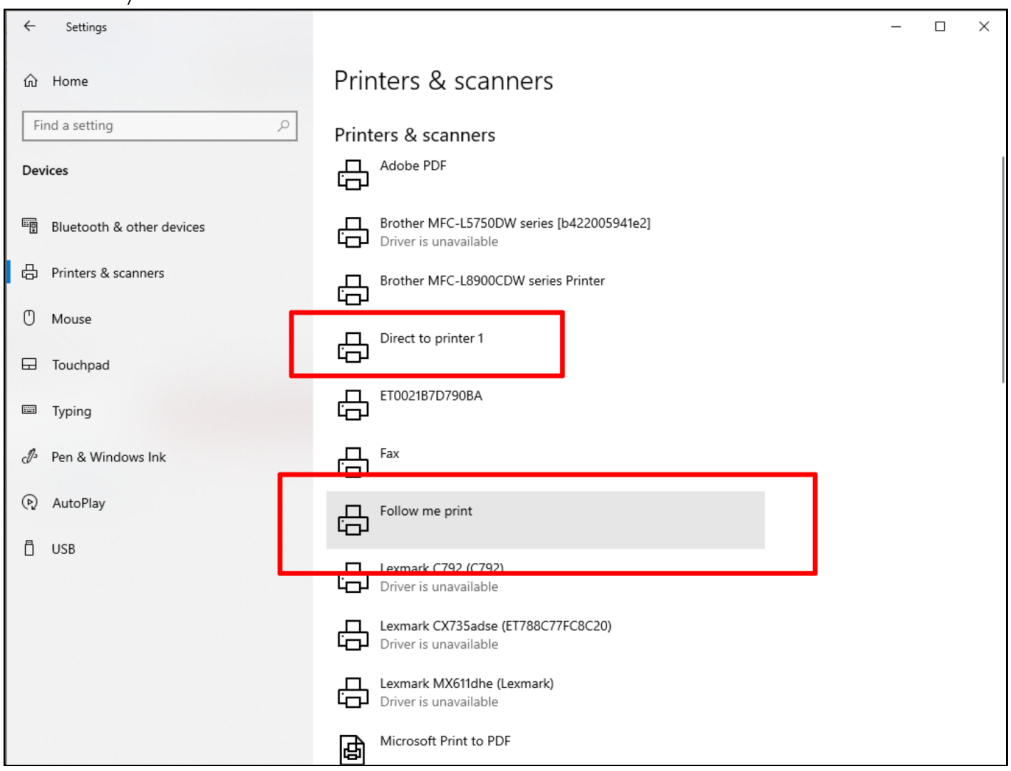
The following steps describe Quick installation (preconfigured installation without advanced options). For more details about the difference between Quick installation and Advanced installation, see Installing SAFEQ Cloud Client on Windows and Installing SAFEQ Cloud Client on macOS.

1. To download the latest version, log in to SAFEQ Cloud Web UI and go to **Personal > My documents**. Click the button corresponding to your operating system and save the Client installation file.
2. Run the saved Client installer file.
3. Follow the installation wizard. On the **Installation Type** screen, select **Quick installation** (you will only see this screen in the Windows installer. The MacOS installer does the Quick installation by default).
4. When the installation finishes, you will see a login screen in your web browser.

Note that if the option to **Automatically trust new clients/servers** is disabled in the **PKI and encryption** section under **Security > Security options** menu of SAFEQ Cloud Web UI, you will need to authorize each end user's SAFEQ Cloud Client in **Security > Endpoints**.



5. After you log in, the print queues you created in SAFEQ Cloud Web UI will be synchronized and visible in your **Printers and scanners**.

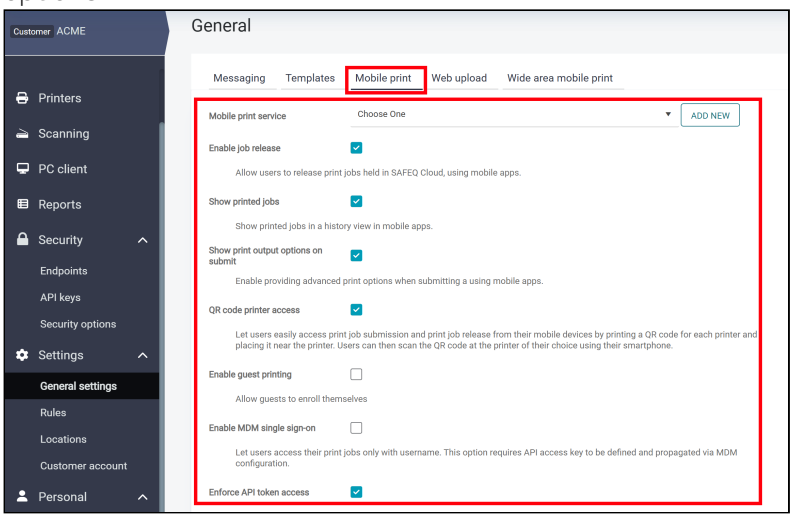


For silent installation and the available command line parameters, see Installing SAFEQ Cloud Client on Windows and Installing SAFEQ Cloud Client on macOS.

For deployment via Microsoft Intune, see Deploy SAFEQ Cloud Client using Microsoft Intune.

7.6 MOBILE PRINTING

1. Log in to SAFEQ Cloud Web UI.
2. Go to **Settings** > **General settings** > **Mobile print**.
3. In **Mobile print service**, select **mobileprint service**. Leave the other settings at their default options.



4. Click **Save**.
5. Download the Mobile app using the links in **Personal** > **My documents** section. See My documents.
6. Submit your print job using the Mobile app.

For more information on how to use the Mobile app see Using the Mobile app.

7.7 RELEASING A PRINT JOB AT THE MFD

You can authenticate at the MFD via card, PIN (short ID), username/password, or combination of these methods.

For generating a PIN, see My profile.

For card self-registration at the MFD, see Card registration at the MFD.

After logging in at the MFD, you will see the My Quick Actions screen. Tap **Print all** or **My print jobs**.

7.8 CONFIGURING A PASSWORD POLICY

If you plan to use local user authentication, we recommend you to configure a password policy. See Password policy.

7.9 GATEWAYS (EDGE DEVICES)

With SAFEQ Cloud, you can use a gateway (secondary server) on your site to route traffic securely between the cloud and the MFDs. Using a local gateway, the print job data do not have to leave the company network, increasing security, responsiveness, and reducing Internet bandwidth. The gateway can be compared to simple devices routing data, such as network routers.

Our recommended option is the OMNI Bridge. For other options, see Gateway Guide.

For more information about YSoft OMNI Bridge, see Setting up OMNI Bridge.

8 ADMIN GUIDE

This section contains:

- A detailed description of all the settings and functions available in SAFEQ Cloud Web UI.
- Installation, setup, functions, and modes of operation of the SAFEQ Cloud Client.

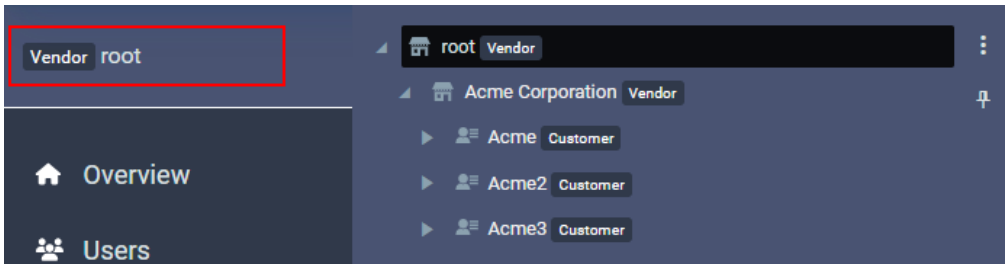
8.1 SAFEQ CLOUD WEB UI

SAFEQ Cloud Web UI is web interface used by vendor administrators to create customers (tenants) in YSoft SAFEQ Cloud and by customer administrators to manage their SAFEQ Cloud settings in one place. For Web UI functions intended for end users, see SAFEQ Cloud Web UI for end users.

The address of the SAFEQ Cloud Web UI consists of the domain set up during the installation/creation of the tenant, or the account domain, and the respective ports, ie, `http://domain:8080` or `https://domain:8443`.

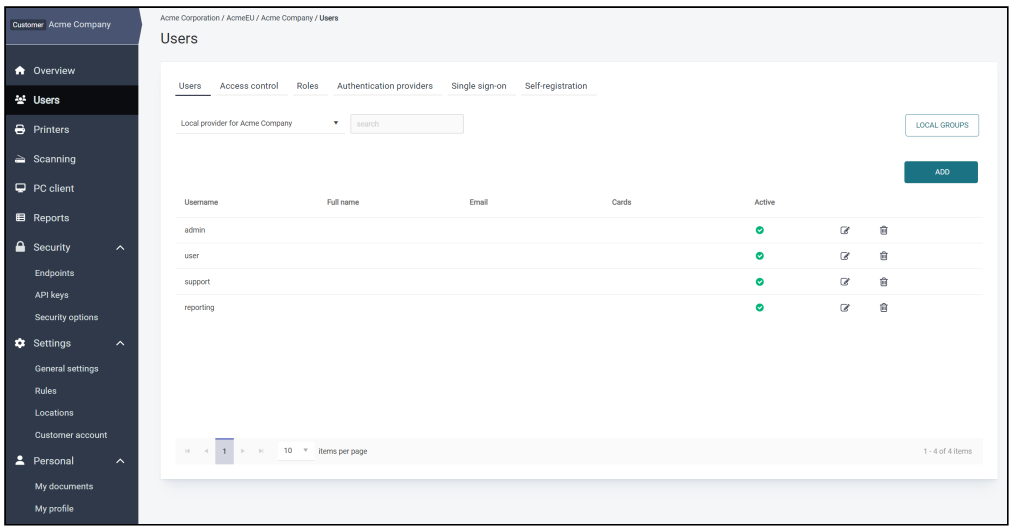
8.1.1 NAVIGATION

Vendor administrators can navigate between individual customer tenants by hovering over the name of their vendor account in the navigation menu. This will display the SAFEQ Cloud system tree. Once you click the customer tenant name in the right part of the tree, the left part of the menu will display information related to that customer, and the right part will be hidden until you hover over the top of the menu again.



8.1.2 USERS MENU

In the Users menu, you can configure Users, Access control, Roles, Authentication providers, Single sign-on and Self-registration.



Access Control

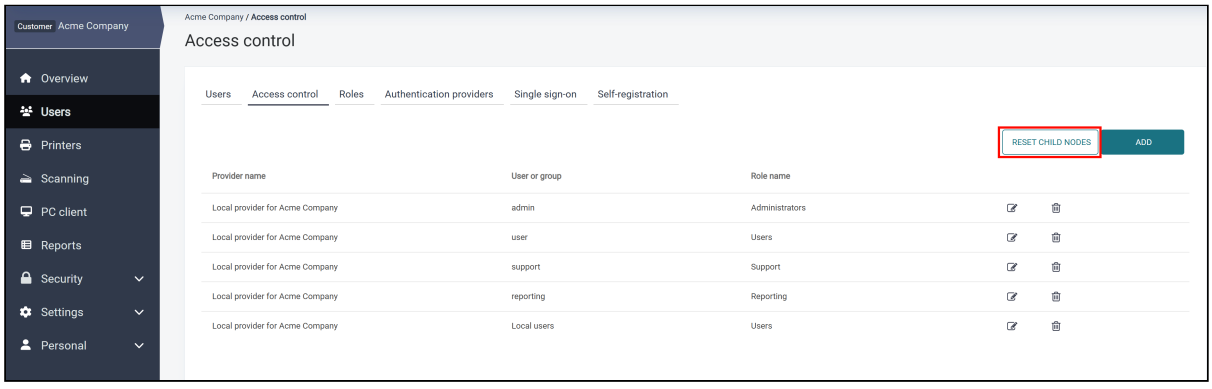
In the SAFEQ Cloud Web UI navigation menu, click **Users** > **Access control** tab.

Access control entries define the security configuration for a given tree node – account, printer, print queue, server, or service. Each entry consists of the security role and a user or group to which this role is granted when accessing this particular tree node. For example, if an access control entry with user **admin** and role **Administrators** exists, it means that user **admin** has full administrative permissions on that tree node.

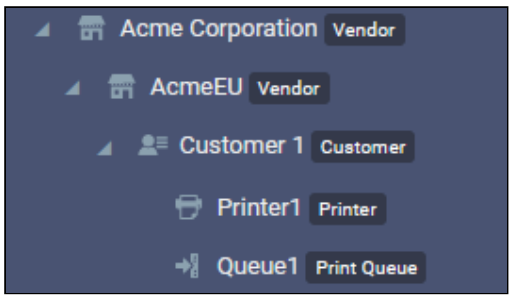
Default settings

Access controls are inherited by default so that all sub-elements of the tree acquire the same configuration. Inherited access controls are greyed out and cannot be modified or deleted. You can override inherited access controls in the child nodes or add more entries for users from sub-accounts.

The following screenshot shows how the access control list is displayed on the **Customer 1** node for the user from **Acme Corporation** vendor:



Which access controls are displayed depends on the user viewing the current node. Given the following hierarchy,



the top-level administrator of the **Acme Corporation** vendor can see all access control definitions for all the nodes. The users who are logged in for **AcmeEU** account will not be able to see, change, or override access control definitions inherited from the parent **Acme Corporation** node. The users from **Customer 1** account will only see and be able to manage access controls defined in that account.

Changing default inheritance of access controls for child nodes

Be careful when changing the default inheritance for the access controls. Make sure you understand the effects of this action beforehand.

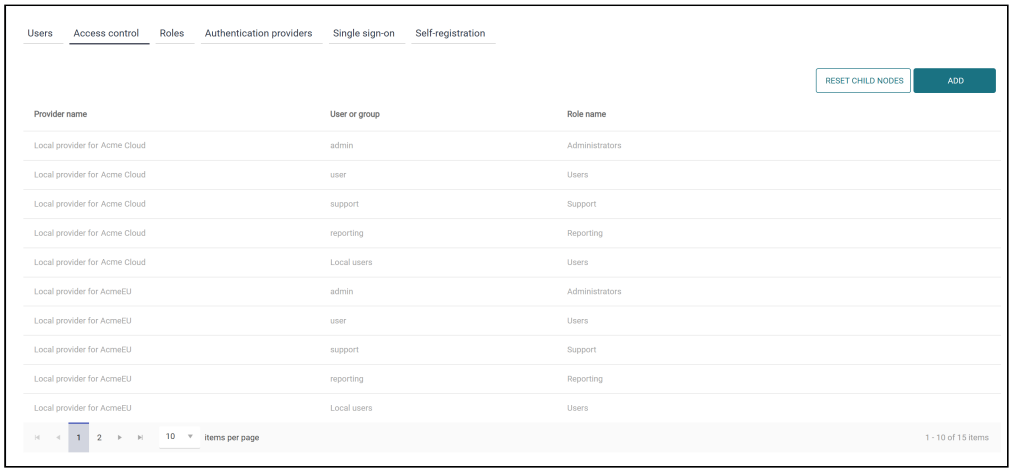
You can restore the default inherited access controls on customer account child nodes by clicking **Reset child nodes**.

To see this button in **Access Control**, you must have the **PropagateAccessControl** permission.

Reset child nodes

The reset child nodes action will remove overridden access controls from child nodes.

Following up on the example above, in the **Customer 1** node, click **Reset child nodes** and confirm the action. You will then see that the access controls originating in the **Customer 1** node are now inherited, as per default:



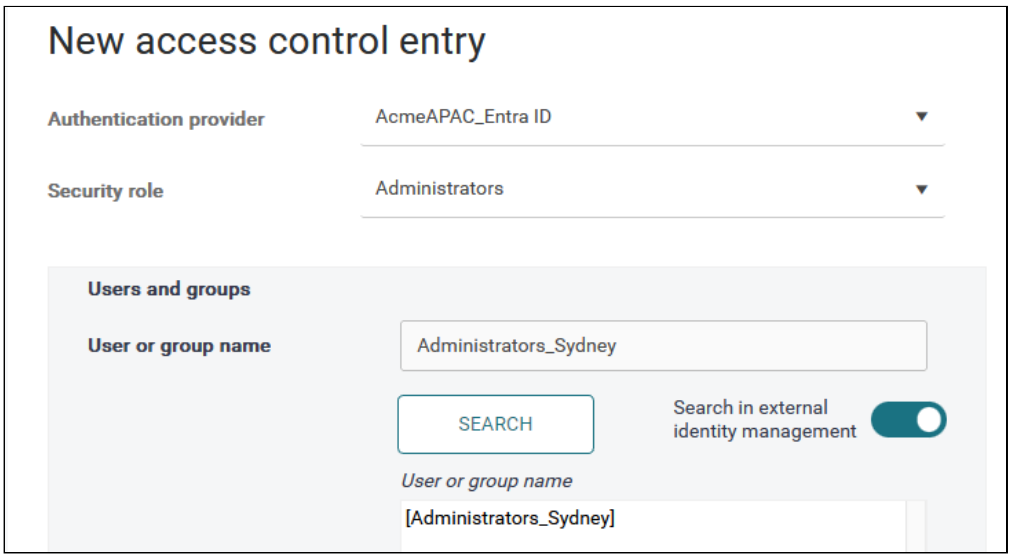
Creating Access control records

If the authentication provider you want to assign security roles to is configured to use OIDC authentication, you can search for users and groups locally, or you

can enable **Search in external identity management** to search in your external identity providers.

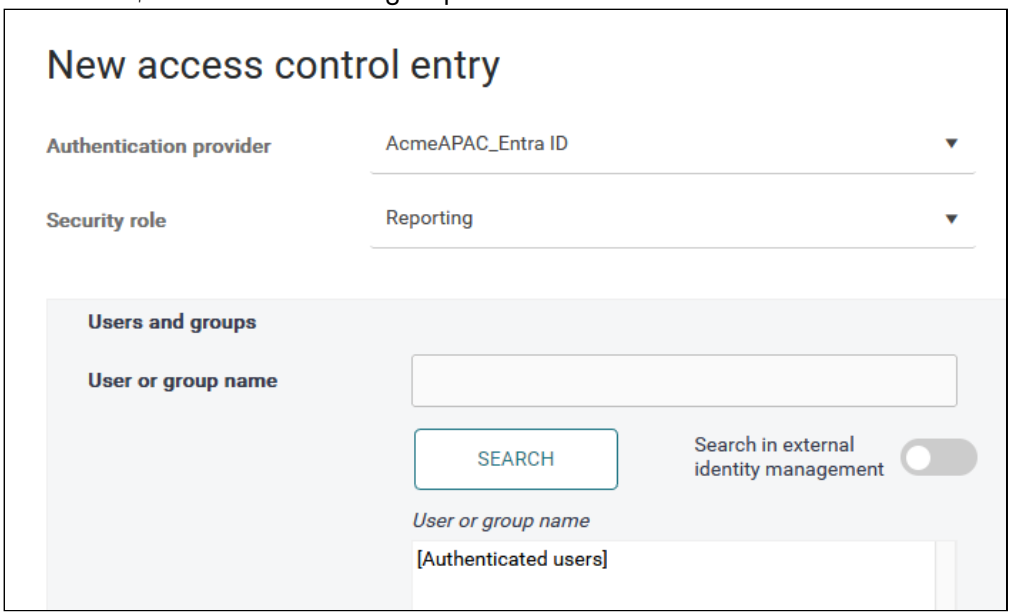
Perform the following steps to assign a role to a user or a group:

1. On the **Users** page in **Access control** tab, click **Add** to create a new Access control entry. A new dialog window will open.
2. In **Authentication provider**, select the authentication provider for which you want to create the new access control entry.
3. In **Security role**, select the role that you want to assign to your users or groups. For creating, editing, or deleting roles see Roles. The roles available by default are:
   - Users
   - Support
   - Reporting
   - Administrators
4. You can assign the Security role either to a particular user/group or to all authenticated users:
   a. If you wish to search for a particular user or group in your external identity provider, enable the **Search in external identity management** toggle and enter the user or group name in the **User or group name** field. In the following example, you have a group called "Administrators_Sydney" in your identity provider, and you wish to assign the Administrators role to its members.



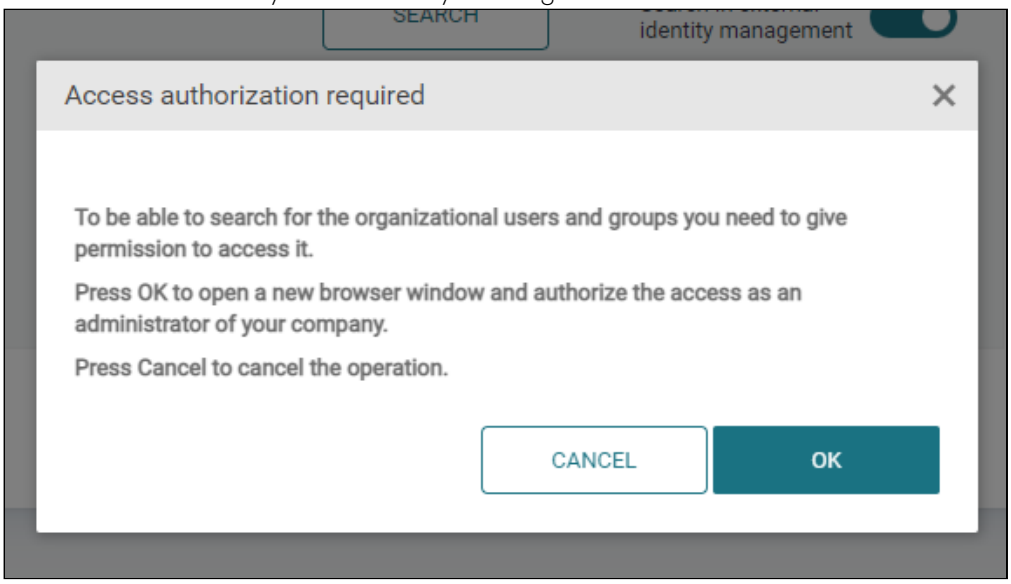
Search in external identity management toggle is shown only for providers relying exclusively on OIDC configuration - i.e. with "Service Account" being disabled.

b. In the following example, you wish to assign the Reporting role to all authenticated users. In such case, leave the **User or group name** field blank and click **Search**.



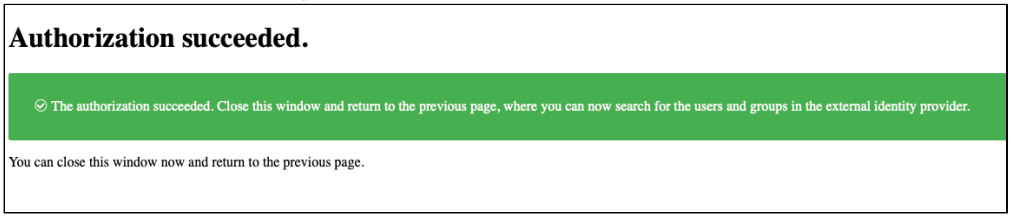
5. Click **Search**.

6. If you enabled **Search in external identity management**, you will need to give permission for the search. Confirm your action by clicking **OK**.



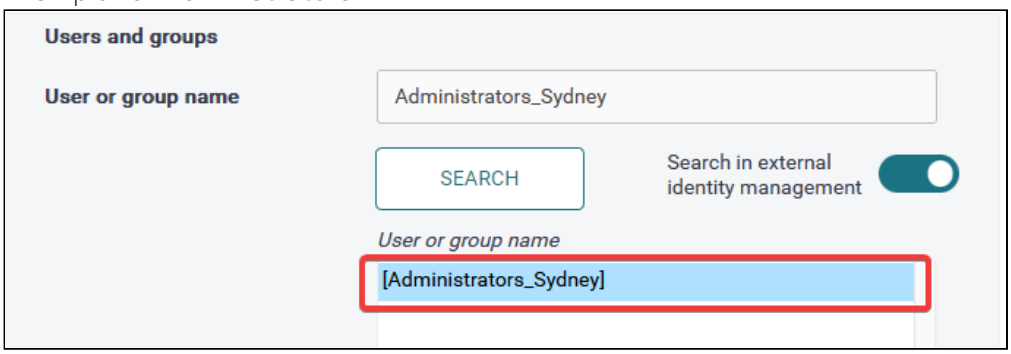
7. Log in with a user account that has the necessary privileges to fetch all users and groups from your external identity provider.

8. After successful authentication, close the browser tab, and click **Search** again to complete the access control mapping.

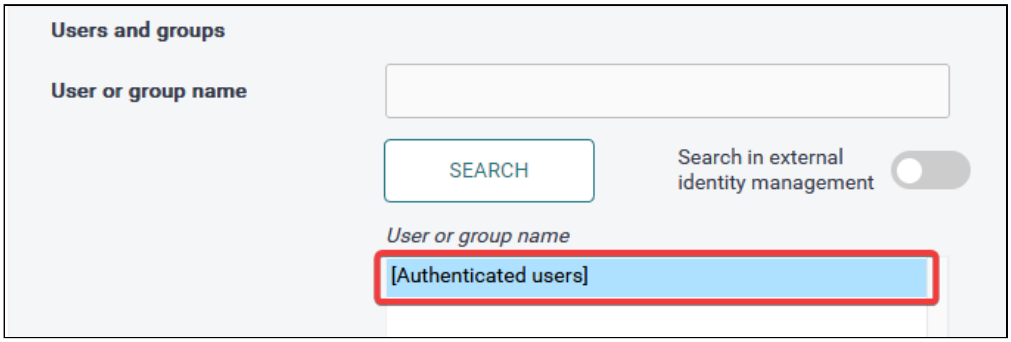


9. Select the user or group that has been found.

   a. Example for Administrators:



   b. Example for all authenticated users:



10. Click **Save** to create the access control record.

Authentication providers

Introduction

To log in to SAFEQ Cloud Web UI, submit print jobs, release print jobs on SAFEQ Cloud terminals, use the Mobile app, etc, the users must be authenticated. Use the **Authentication providers** tab to configure how the users will be authenticated.

SAFEQ Cloud supports two main authentication types:

- Local user authentication
- Authentication to external directory via
  - OIDC
  - Service account (Service access)
  - Client-side authentication

Local user authentication

This is the simplest authentication type where the users are created and managed manually in the SAFEQ Cloud server, under the built-in **Local authentication provider**. By default, there are few users predefined for each created account, including the **admin** user.

We recommend keeping the local admin user as a fallback login in the case of failure of other authentication methods, such as provider misconfiguration, access token expiration, network issues, or a service disruption on the part of your external authentication provider.

Authentication based on OpenID Connect (OIDC)

This type of authentication enables connecting to an external authentication provider through OIDC. SAFEQ Cloud supports the following authentication providers for OIDC:

- Microsoft Entra ID
- Okta

We recommend OIDC as the most secure authentication method, ideal for both Web UI and client workstations. It enhances security by redirecting users to the authentication provider's login page, ensuring that credentials are only entered at the provider's site. Furthermore, it supports multi-factor authentication (MFA) and eliminates the need for repeated credentials entries.

OIDC authentication doesn't allow synchronization of card IDs and PINs. If you have this information stored in your authentication provider (instead of directly in SAFEQ Cloud), you may also want to configure service access for the same provider to allow users to log in at the MFD terminal using their company cards and PINs.

Logging in using the OIDC authentication method

When an authentication provider is configured with the OIDC authentication method, users can log in via such authentication provider in two ways:

- Entering a username matching the authentication provider.
- Clicking Login via <Provider Name> on the login page.

When a user enters a username that matches the authentication provider with enabled OIDC authentication, they are redirected to the provider's login page, where they authenticate and then are redirected back to SAFEQ Cloud.

When the user clicks Login via <Provider Name>, they are also redirected to the provider's login page.

When configuring the authentication, you will be able to choose whether to show the provider-branded Login via <Provider Name> button on the login page.

User details are synchronized during every user login (either via SAFEQ Cloud Web UI, SAFEQ Cloud Client, MFD terminal, or the Mobile app), except for the user logging in within the lifespan of the existing OIDC Access Token (usually 60 minutes after the first login).

Authentication based on the service access

This authentication method requires you to create a service account in your external authentication provider. This account must have permission to search and retrieve users. SAFEQ Cloud supports the following authentication providers for service access type:

- Microsoft Entra ID
- LDAP (including Active Directory)
- Okta

If you choose this authentication method, you must enter the service account details (e.g., username and password) in the authentication provider settings in SAFEQ Cloud. Users can authenticate against the SAFEQ Cloud server using all available login types: username/password, card ID, and PIN.

We do not recommend using the service access authentication method for authentication providers that support OIDC. Set up OIDC for user login to SAFEQ Cloud Web UI and SAFEQ Cloud Client, and if you need users to log in via company cards or PINs stored in your authentication provider, set up the service access authentication in conjunction with OIDC.

Microsoft Entra ID and LDAP do not support multi-factor authentication (MFA). Also, the Okta MFA support is very limited when using service access authentication only. In these cases, we strongly recommend using OIDC authentication.

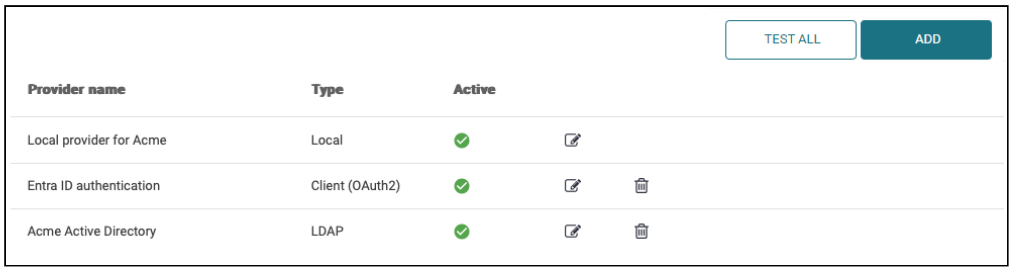
Client-side authentication

This type of authentication requires SAFEQ Cloud Client software, which uses interactive browser-based authentication provided by the external authentication provider. You don't need to create service access. MFA is fully supported.

The limitation of this authentication type is that users cannot log in at SAFEQ Cloud terminals via username and password, card IDs, and PINs stored in the authentication provider. Only local card ID and PIN logins are supported. However, users can log in via the one-time passwords (OTPs) functionality. This is useful, for example, for local card registration. You can generate OTPs manually in the Web UI or automatically by setting up triggers. See the section on My profile for more information.

The SAFEQ Cloud Client automatically refreshes information about users from external authentication providers at periodic intervals. After a successful refresh, the user can log in at the MFD for a time defined in the user expiration policy in the authentication provider. If the SAFEQ Cloud Client is offline (or hasn't successfully refreshed information from the external authentication provider), and the time defined in the user expiration policy has passed, the user won't be able to log in at the MFD.

Authentication configuration



The following authentication provider types are available:

- Local – Local authentication provider. It will authenticate users against the internal user database in SAFEQ Cloud.
- LDAP – LDAP authentication provider enables authentication using LDAP/LDAPS against Active Directory, Novell eDirectory, and IBM Domino.
- Microsoft Entra ID – Microsoft Entra authentication enables authentication against Microsoft Entra ID. See Microsoft Entra authentication.
- OKTA – OKTA authentication enables integration with the OKTA authentication service. See OKTA Authentication.
- Client – Client authentication is a special type of authentication performed by the SAFEQ Cloud Client on the client side. See Client authentication.
- External – SAFEQ Cloud supports external authentication providers where external authentication service such as External Card Repository is used to identify users from different authentication providers.

A newly created vendor or customer accounts always have the Local Authentication Provider added by default. It cannot be removed.

There is no limit to the number of authentication providers you can add.

You can define a priority number for every provider (a higher number means higher priority), which is used for every logical operation where the order of providers matters.

Warning: In a production environment where numerous users are enrolled in the system, deleting an Authentication Provider will result in users' information not being available anymore for authentication, retrieving card numbers, PINs, etc., as user records are bound to the Authentication provider ID that was used when adding them to the database.

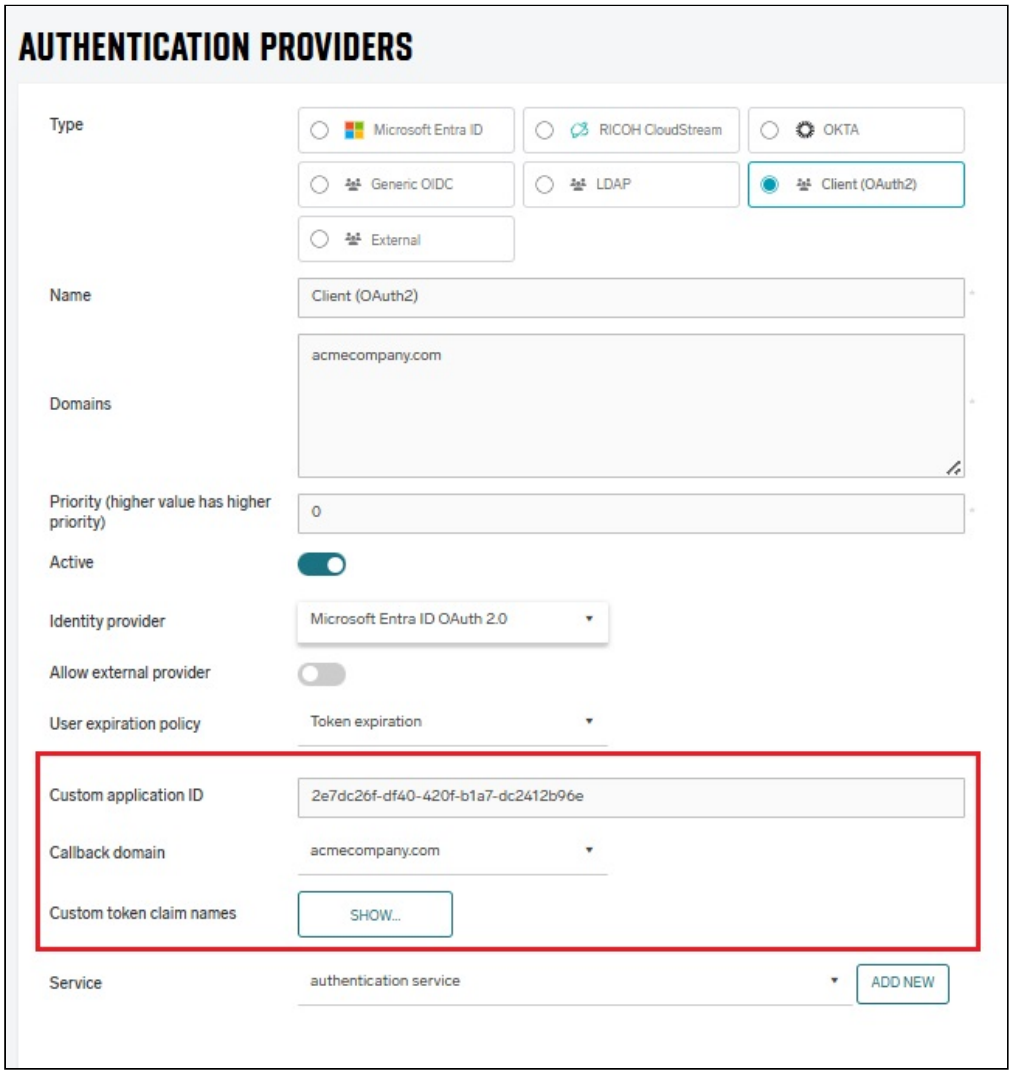
See additional instructions for configuring specific authentication providers:

- LDAP authentication
- Microsoft Entra ID authentication
- OKTA authentication
- Client authentication
- External authentication

Client authentication

SAFEQ Cloud supports client-based authentication where user authenticates against OAuth2 identity provider such as Microsoft Entra ID, Google G Suite or Ping Identity platforms, using SAFEQ Cloud Client. Client-based authentication also allows to use multi-factor authentication in combination with SAFEQ Cloud server.

Client-based authentication must be configured on two sides: the SAFEQ Cloud Client and the server:



- Type – should be set to "Client."
- Name – choose a name for the authentication provider. Should be prefilled with selected type.
- Domains – this field should match the domains of the organization and the "@domain" part of the users which authenticate.
- Priority – A number determining the order in which authentication providers will be called until one succeeds. Higher-priority providers will be called first
- Identity provider – currently the following identity providers are supported: Microsoft Entra ID, Google G Suite, Ping Identity.
- Allow external provider – Used only in combination with External provider. For more details see External authentication.

Common

When the user is authenticated on the client side it will be created in SAFEQ Cloud database and visible under **Users** section, when the corresponding Client provider is chosen from the drop-down list. User properties can be changed by the administrator or this user can be added to Access Controls.

- **User expiration policy** – choose the policy for user records expiration (see below).
- **Custom user expiration, min** – field is visible only when user expiration policy is set to custom one.
- **Service** – choose authentication service in this field. In case no service is already created, it can be added using the **Add** button.

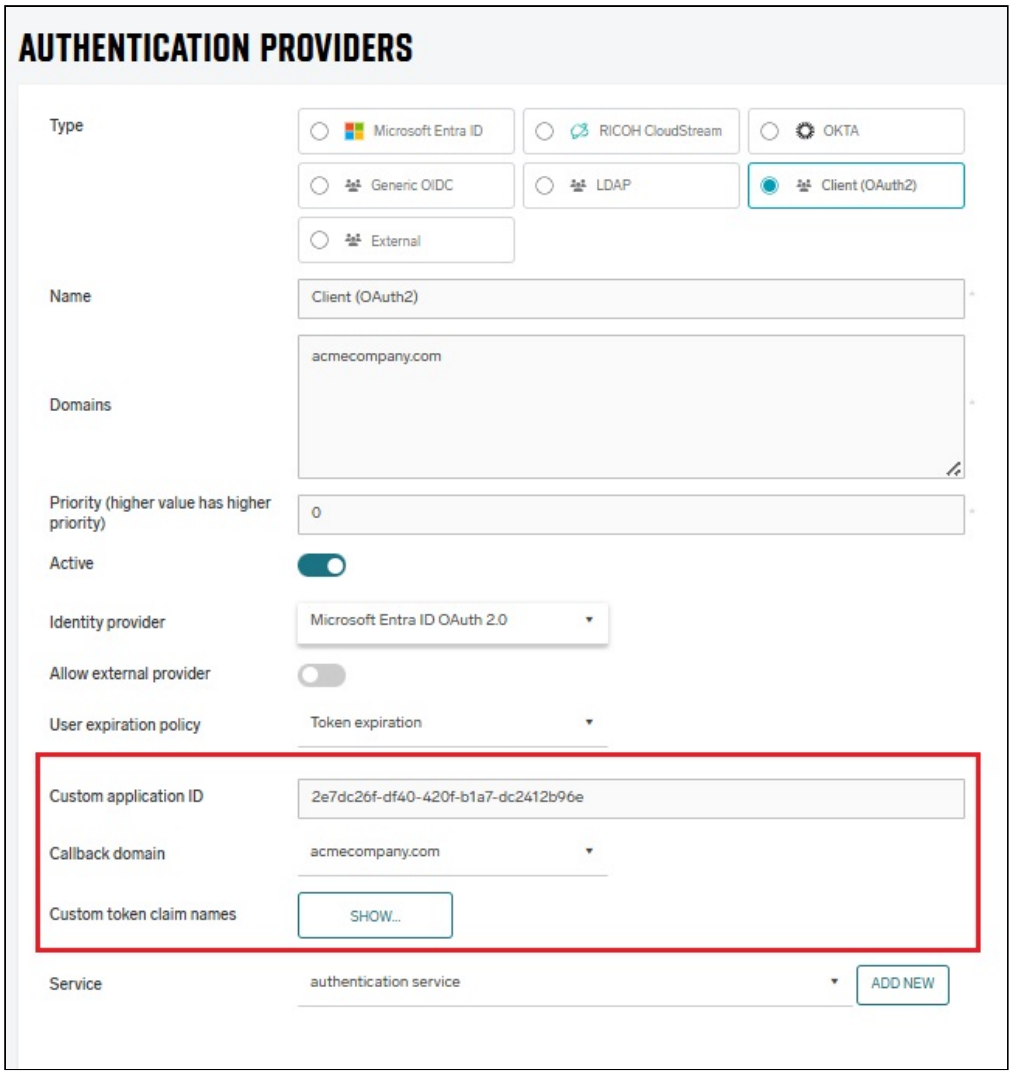
User expiration policy

> Users which are authenticated via Client provider will have an expiration time. This means that after particular time after authentication using SAFEQ Cloud Client or Chrome extension they won't be able to authenticate at printers using cards or short id unless the token is refreshed and user expiration time extended.

Traditionally, this time is defined by the identity provider and delivered as one of the access token fields. The usual expiration time is **one hour** but can be changed by the directory administrator. Users must be refreshed by SAFEQ Cloud Client periodically, otherwise they won't be able to print or authenticate. The SAFEQ Cloud Client tries to refresh the user several minutes before expiration. The user can also be refreshed by manual login to the SAFEQ Cloud Client or Web UI. If the SAFEQ Cloud client is not running or offline, the user will expire.

Another approach for prolonging user lifetime is to change the expiration policy to one of the custom values: **Custom expiration for card login** or **Custom expiration for all login types** and set custom expiration period. For example, if you choose **Custom expiration for card login** and set 480 to **Custom user expiration, mins** field, you'll let to use card for authentication during 8 hours since SAFEQ Cloud Client or Chrome extension login even if SAFEQ Cloud Client is not running.

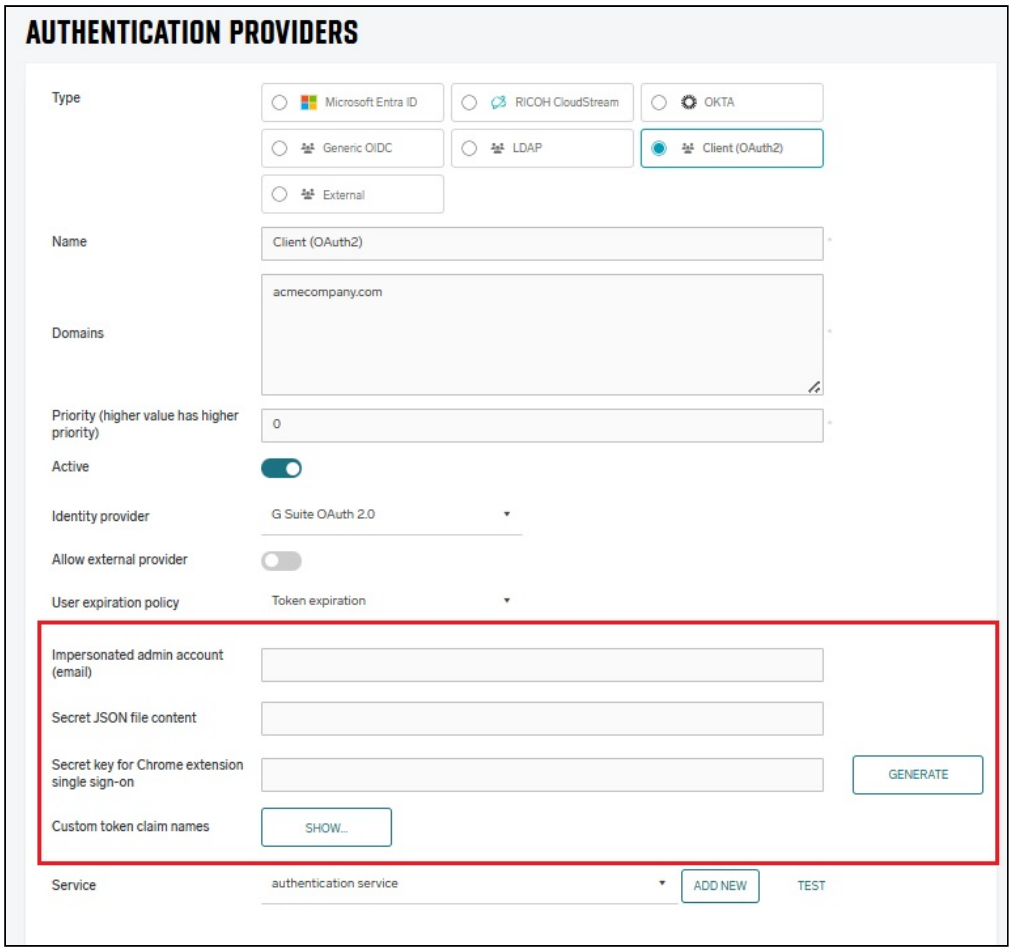
For Microsoft Entra ID



- Custom application id – this field is optional, and it's used for syncing the Entra groups in case of `Identity provider` = Microsoft Azure. In case the value is empty, will be used the SAFEQ Cloud build-in client ID. In case of on-premises installations this value must be set.
- Callback domain for custom application – this field is used only in case the Custom application id is not empty. It should match the Redirect URIs from Entra ID where the custom application is created.
- Custom token claim names – in this section, you can define claim names in the token. Their values will be stored in the user attributes after login.

When a new Client authentication provider is created, it will have a default group added called Authenticated users and the groups from Entra ID (by clicking Sync groups) when Entra identity is used (not ADFS). These groups can be used in access controls to enable permissions for authenticated users.

For Google G Suite



- Impersonated admin account (email) – email of the account with administrative rights in your G Suite domain. Service account that you'll use for authentication will be limited to the scopes you provide, so SAFEQ Cloud won't have full administrative access to your domain.
- Secret JSON file content – paste here the entire content of the secret JSON file that you'll download when creating the service account.
- Secret key for Chrome extension single sign-on – (optional) improves security when you want to use Chrome extension without authentication. The key is used to verify authentication requests. You can either generate or enter your own key. The same key must also be set in the Chrome extension in order to work. The key should never be shared.
- Custom token claim names – in this section, you can define claim names in the token. Their values will be stored in the user attributes after login.

When a new Client authentication provider is created, it will have a default group added called `Authenticated Users` and the groups from G Suite domain (synchronized by clicking Sync groups). These groups can be used in access controls to enable permissions for authenticated users.

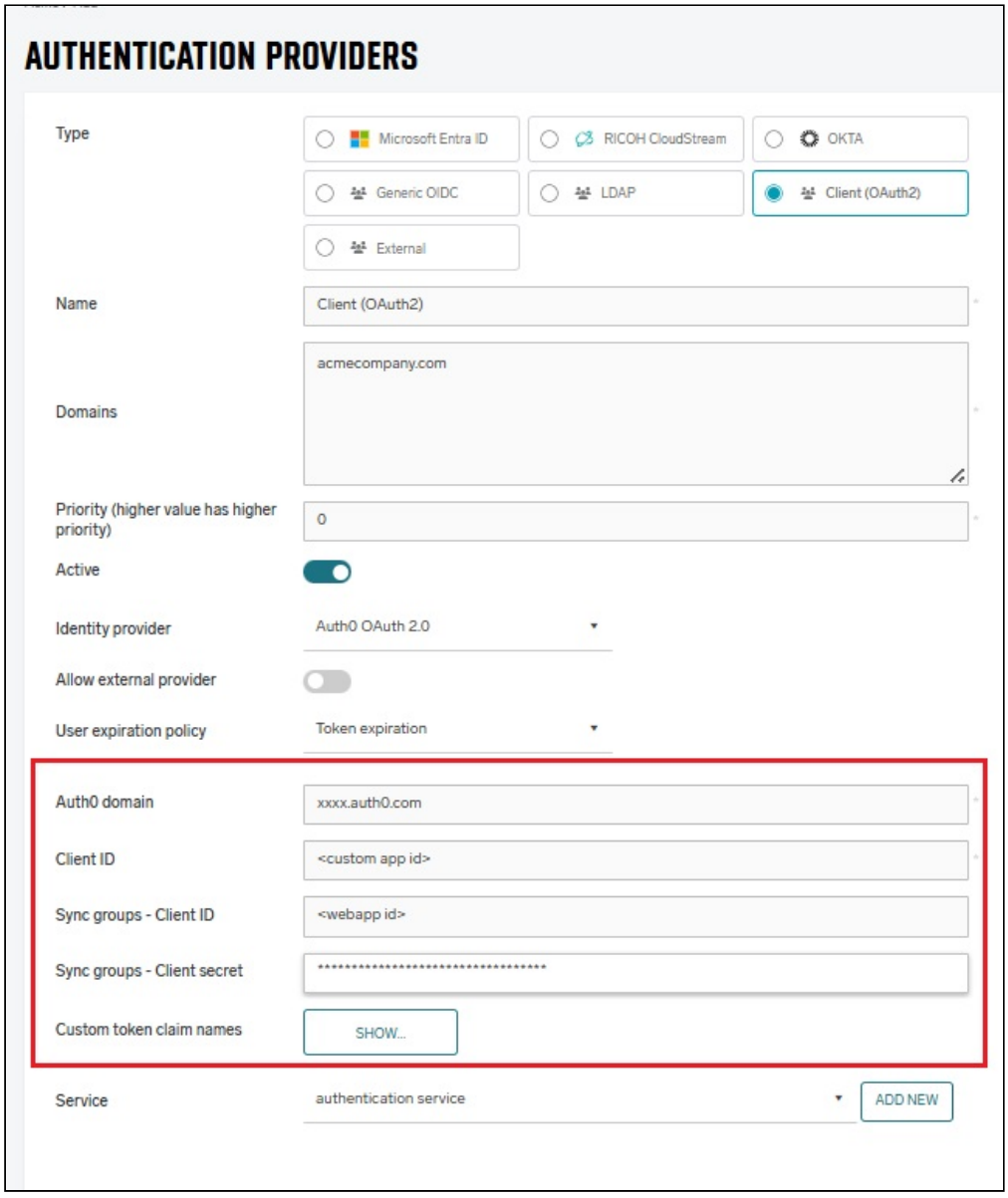
For Ping Identity

- Custom application id – required field, the ID of the application created in the Ping Identity portal.
- Ping environment id – Ping environment ID.

- Ping region – Ping region, one of "eu", "com", "asia"
- Callback domain for custom application – This field should match the Redirect URIs from Ping application configuration.
- Custom token claim names – in this section, you can define claim names in the token. Their values will be stored in the user attributes after login.

For Auth0 Identity

Add a new Auth0 authentication provider with configuration of custom fields as explained below.



- Auth0 Domain – required field, Client ID of Native Application created in the Auth0 Identity management.
- Client ID - Client ID of the Native Application.
- Sync Groups - Client ID - Client ID of Regular Web Application created in the Auth0 Identity management.
- Sync Groups - Client Secret - Client Secret of the Regular Web Application.

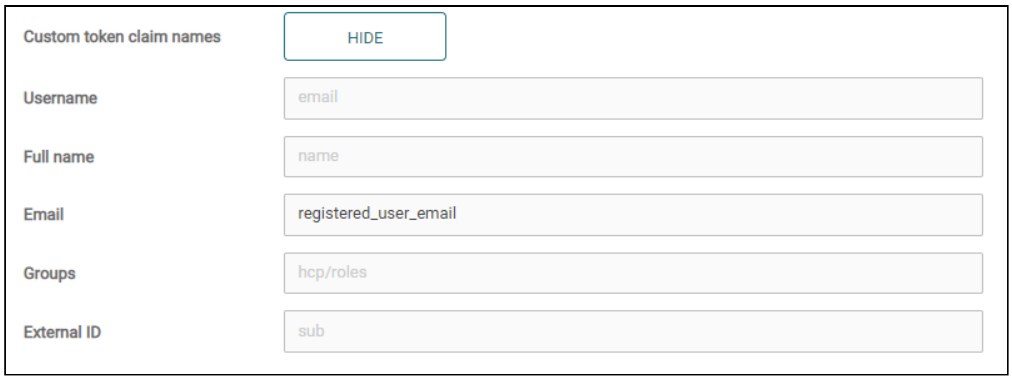
For more info about the above four fields and the relevant Auth0 applications, see Add a custom app in the Auth0 identity platform.

- **Custom token claim names** – in this section, you can define claim names in the token. Their values will be stored in the user attributes after login.

Custom token claim names

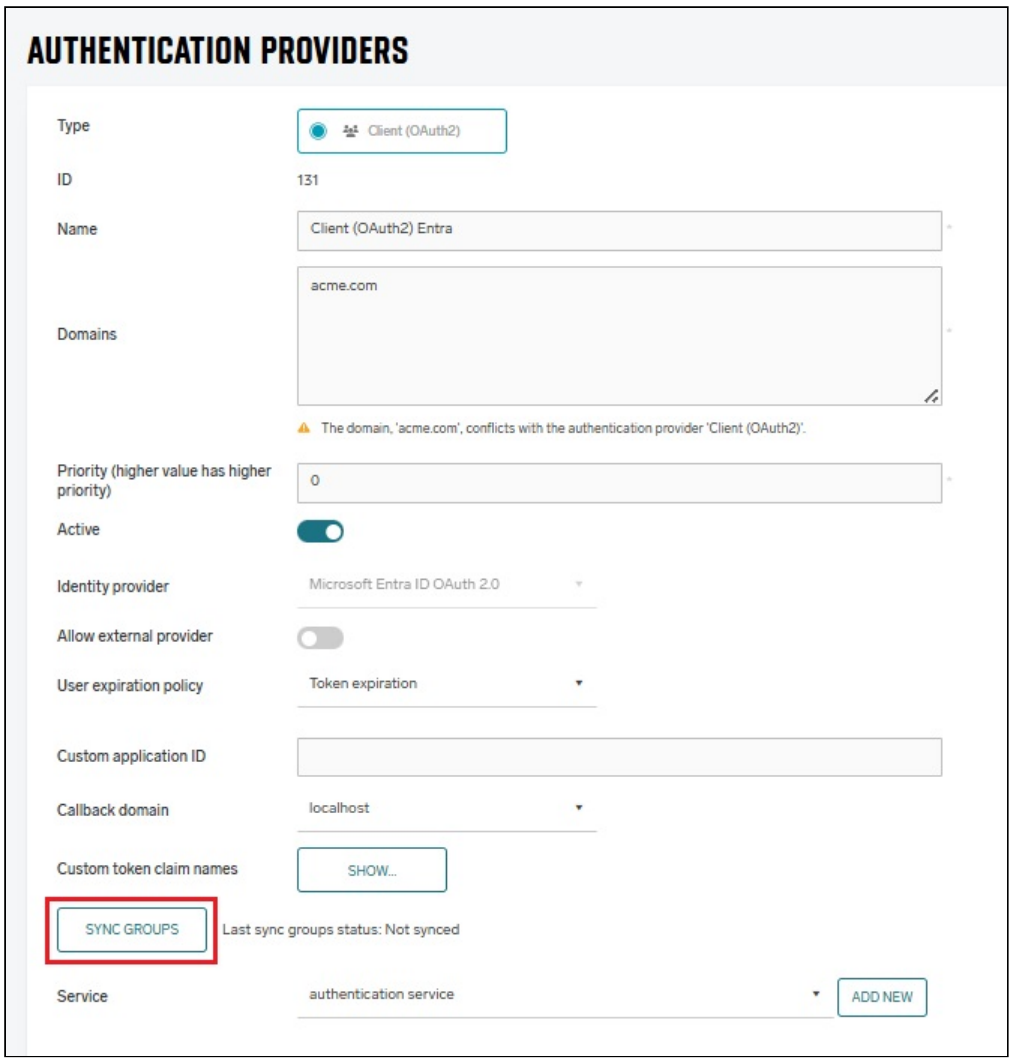
In this section, you can define claim names in the token. Their values will be stored in the user attributes after login.

For example, if the Auth0 provider is returning email value in its token claims (named **registered_user_email**), you can input **registered_user_email** into the **email** field, and upon successful login, the email from the custom token claim will be stored under the **email** user attribute.

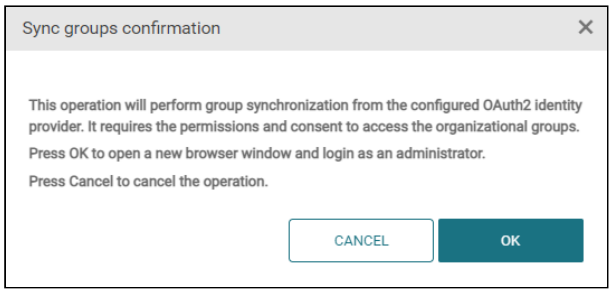


Sync groups

When a new Client authentication provider is created it will have a default group added called **Authenticated Users**. To synchronize more groups, click **Sync groups** in the provider view. These groups can be used then in access controls to enable permissions for authenticated users.



For Microsoft Entra or Ping Identity, the group sync requires an OAuth2-based workflow. By clicking **Sync groups**, a confirmation window will appear:



If you click **OK**, the groups will be retrieved from the identity provider and added or updated in SAFEQ Cloud server.

For Azure AD identity provider, there are two scenarios:

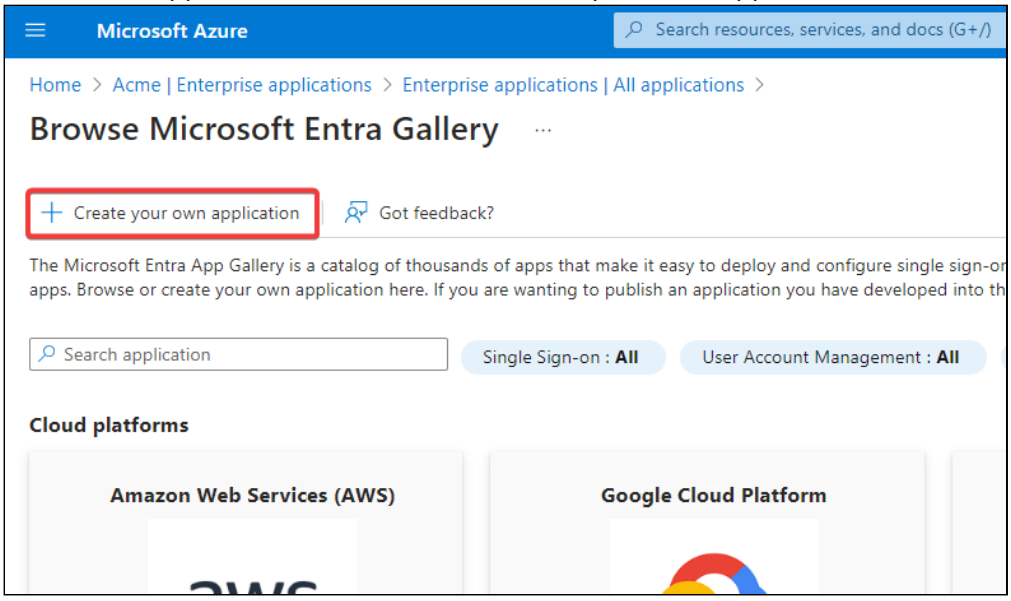
- If the **Custom application id** field is empty in the client authentication provider, then the sync groups will be done using the SAFEQ Cloud build-in client ID (for build-in client ID is mandatory to be on [custom domain].eu/[us]/[uk]/[ap].ysoft.cloud).
- If the **Custom application id** field is not empty, the value should be taken from a native Entra application. Also, should be a match between **Callback domain for custom application** and one

of the Redirect URIs set for the new created Entra application. In this case the sync groups will be done using the new created Entra application.
For more details, see Add a custom app in Microsoft Entra ID.

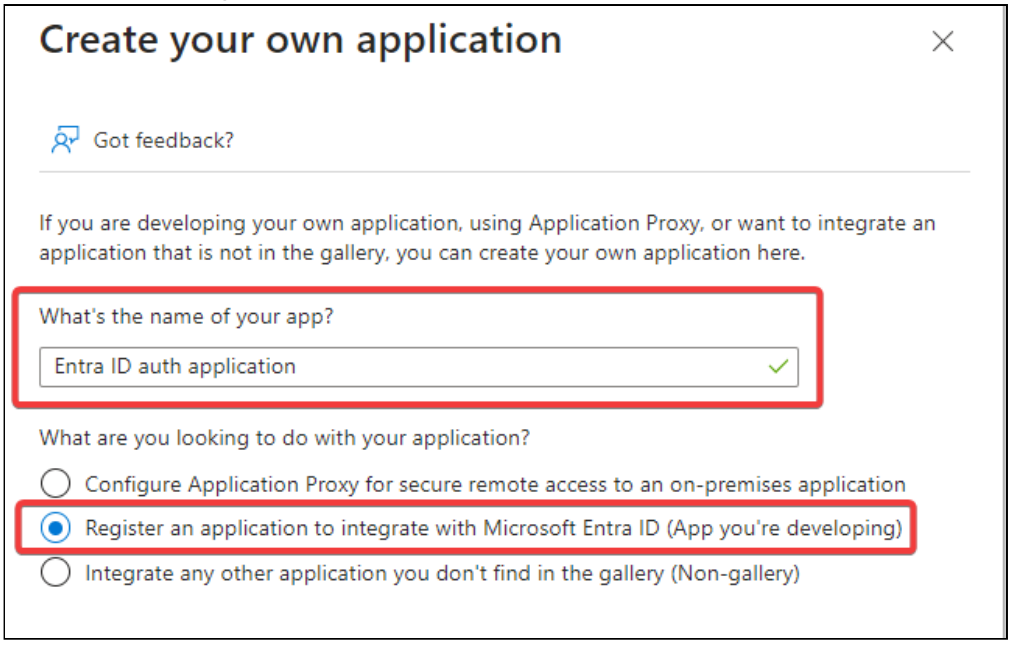
Add a custom app in Microsoft Entra ID

To create a custom application in Microsoft Entra ID, perform the following steps:

1. Log in to the Azure portal and click **Manage Microsoft Entra ID.**
2. Navigate to **Enterprise Applications > All applications**.
3. Click **+New application** and then click **Create your own application.**



4. Name your application, select **Register an application to integrate with Microsoft Entra ID (App you're developing)**, and click **Create**.

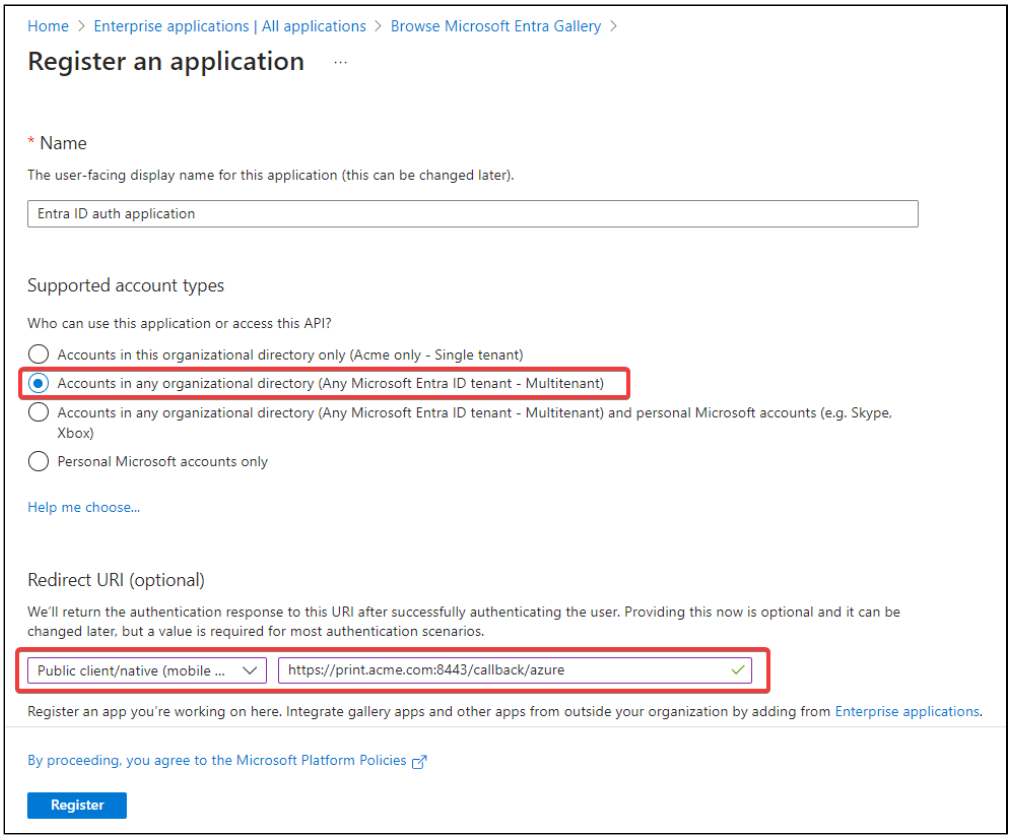


5. On the following screen, fill in the following values:
   a. **Name** – Represents the name of the application.

b. In **Supported account types**, select **Accounts in any organizational directory (Any Microsoft Entra ID tenant – Multitenant)**.

c. In **Redirect URI**, select **Public client/native (mobile & desktop) and enter** the URI. The field value should match this pattern: `https://<domain:port>/callback/azure`. The domain and the port should be the same as the ones of the SAFEQ Cloud website URL. For example, if the SAFEQ Cloud web URL is `https://print.acme.com:8443`, the value should be: `https://print.acme.com:8443/callback/azure`.

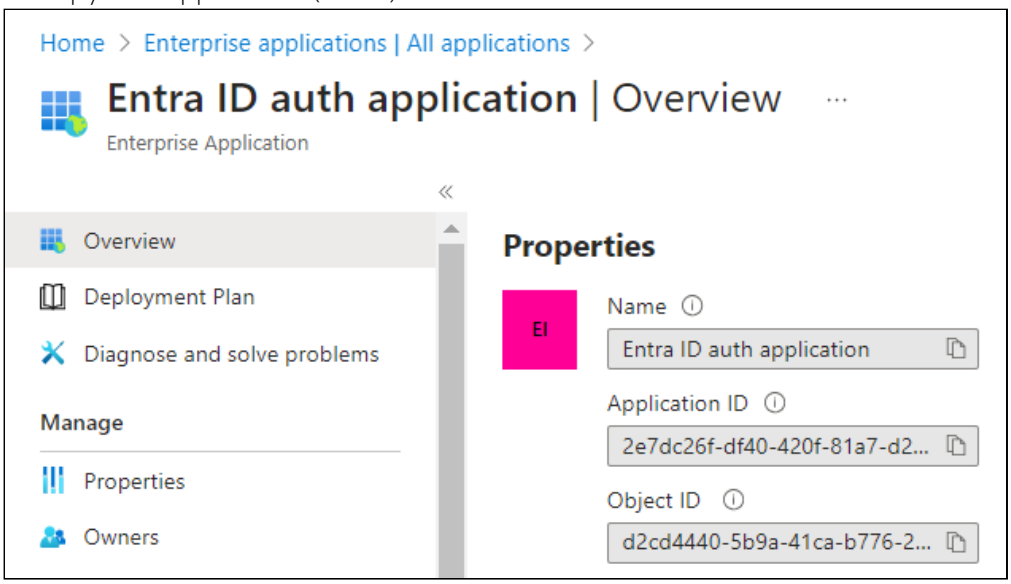
In environments with reverse proxy infrastructure, do not specify the port number in the URL, meaning the default HTTPS port 443 will be used. Example: `https://print.acme.com/callback/azure`.



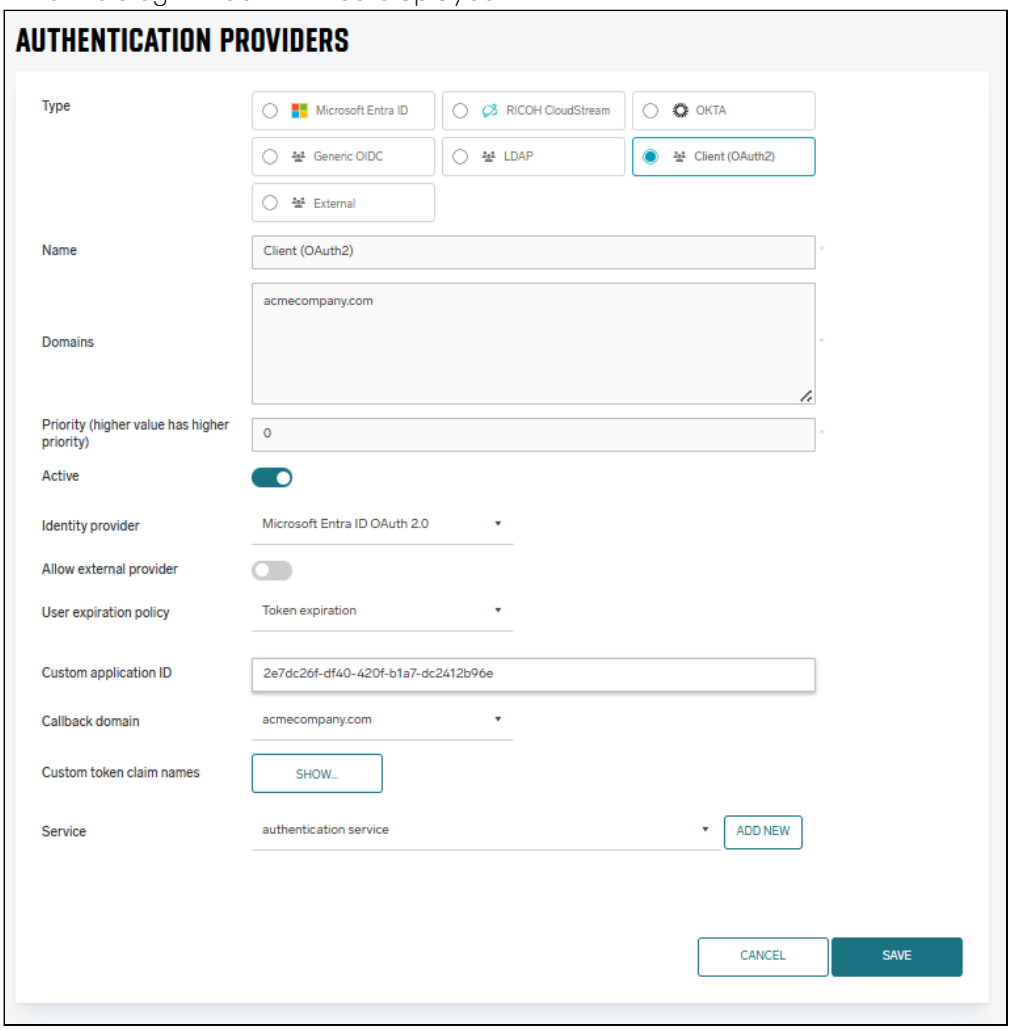
6. Click **Register**.

7. Navigate back to **Microsoft Entra ID** > **Enterprise Applications** > **All applications**.

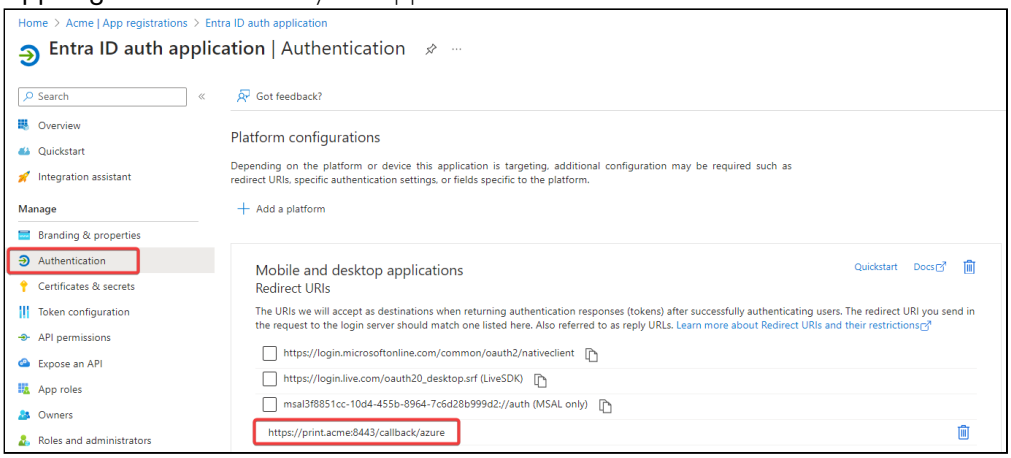
8. Click your application (click refresh if it does not appear at first) to open the application details to copy the Application (client) ID.



9. Log in to the SAFEQ Cloud Web UI and go to **Users**.
10. On the **Authentication providers** tab, click **Add**.
11. A new dialog window will be displayed.



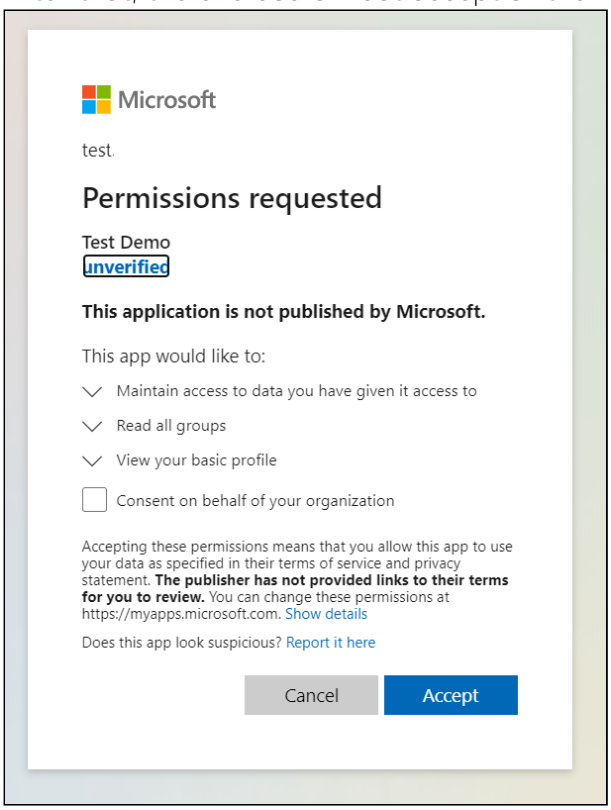
- In **Type**, select **Client (OAuth2)**.
- In **Name**, enter the name of the authentication service. Should be prefilled with the selected Type.
- In **Domains**, enter your Entra ID domain (Example: the "acme.com" part of john.doe@acme.com).
- In **Identity provider**, select **Microsoft Azure OAuth 2.0**.
- In **Custom application ID**, enter the value of the Application (client) ID from the newly created application.
- In the **Callback domain for custom application** drop-down menu, select the domain that matches the one from the Redirect URIs that is already added in Azure application. The pre-selected value represents the domain from the SAFEQ Cloud Web URL. For adding or updating the Entra Redirect URIs, go back to the Entra ID homepage in Azure portal and click **App registrations**. Click your application and then click **Authentication**.



- In **Services**, select **authentication service**.

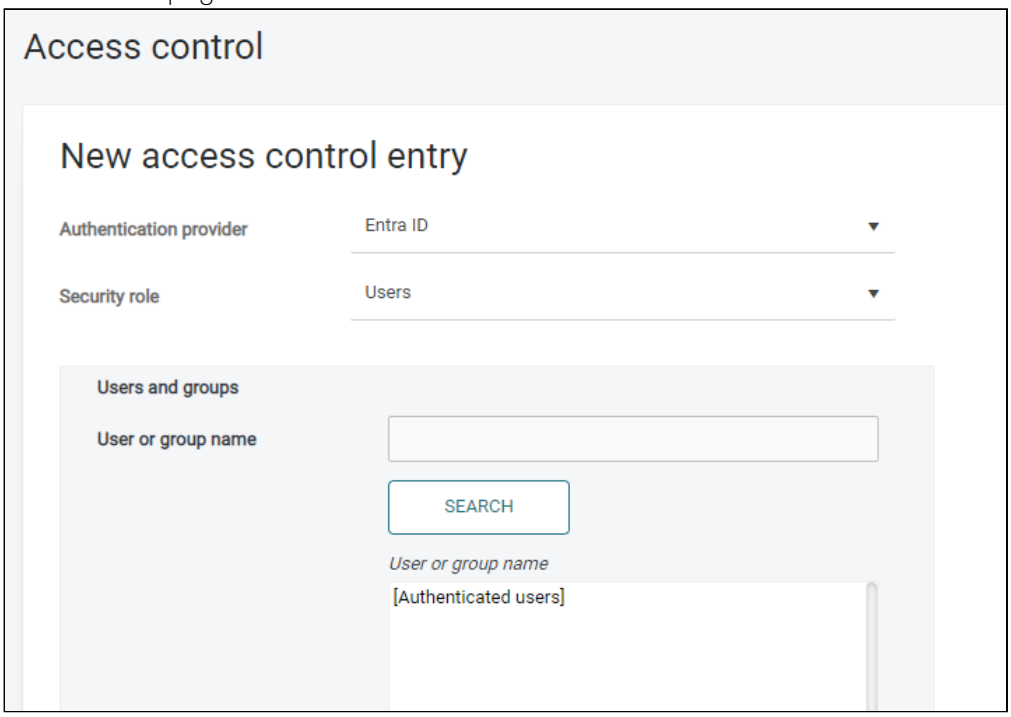
12. Click **Save**.
13. Click **Sync groups**.

14. After that, the end users must accept all the required permissions.



15. When the users accept the permissions, the sync groups operation is done. If you perform the synchronization for the same account/application again, the users will not be required to grant permissions again.

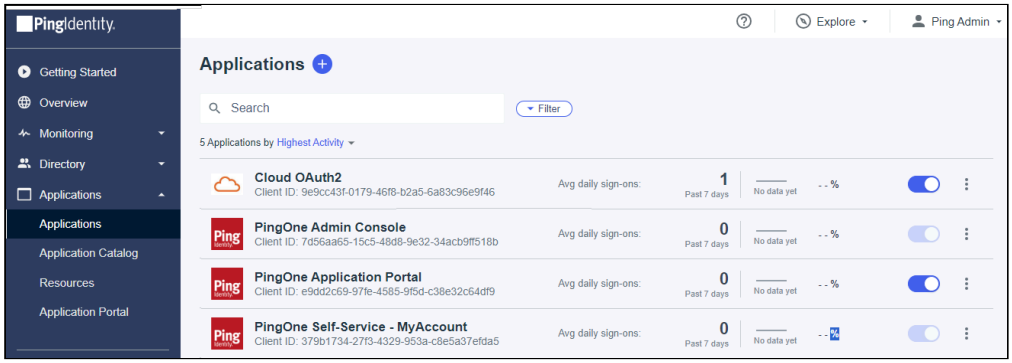
16. Go to **Users** page and to **Access control** tab.



17. Select your newly created authentication provider and click SEARCH. Then, the default group Authenticated Users and the Entra groups are visible. You can use all these groups in access controls to enable permissions for authenticated users.

Add a custom app in the Ping identity platform

To set up authentication and group synchronization with the PingID provider, you must create an OAuth2 Worker application in your PingID environment:



Overview of steps

Make sure to perform the following actions in the correct order, otherwise you might disable your existing authentication to your SAFEQ Cloud tenant. These steps are:

1. Set up the authentication provider in SAFEQ Cloud using a PingID Worker application.
2. Perform group synchronization for your PingID authentication provider.
3. Create Access Control records for the imported groups. Make sure that you will retain an administrative role in SAFEQ Cloud when you log in using your PingID identity. You must create access control records with the Administrator role for the group where you are a member.

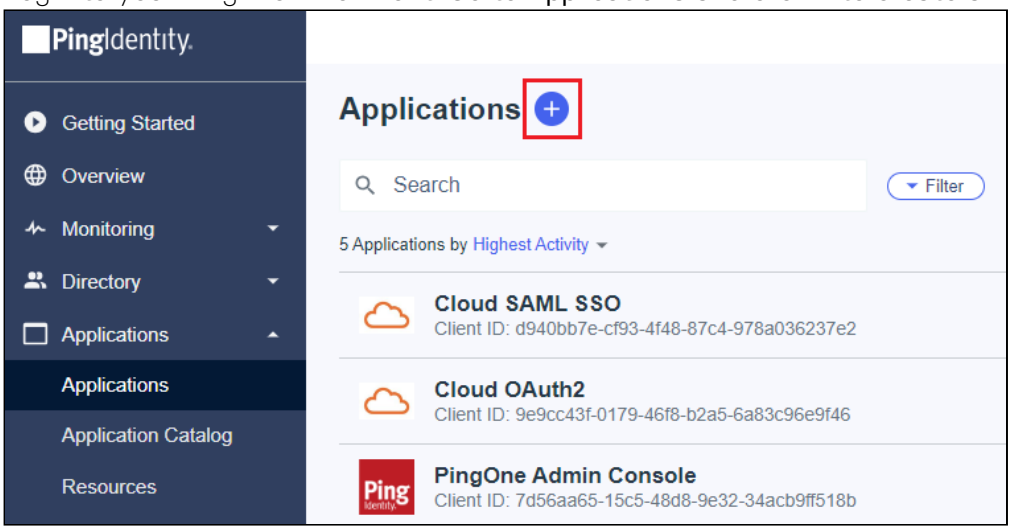
OAuth2 Configuration

Authentication to PingID is done via the PingID OAuth Worker application.

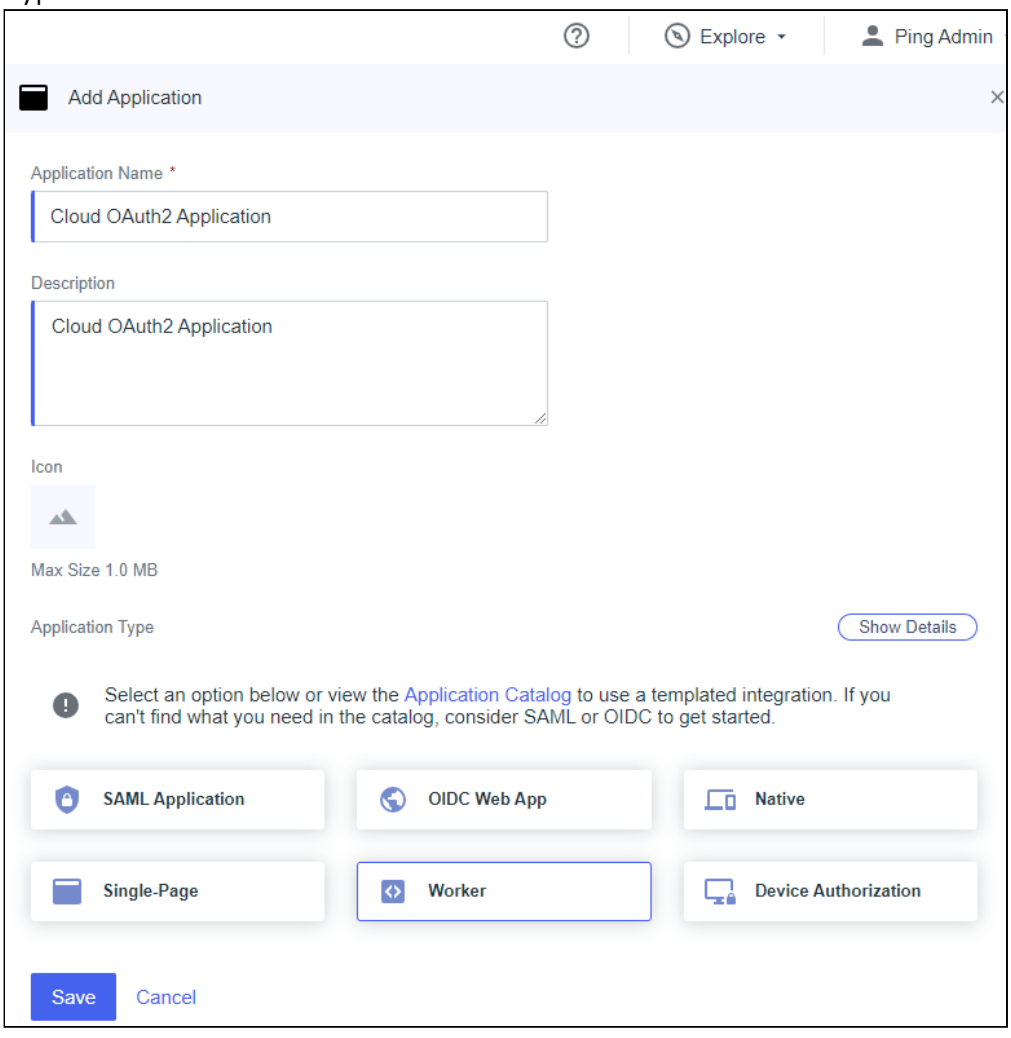
Group synchronization with PingID is done via OAuth2 authentication of a user with administrative privileges for the Worker application.

Creating the Worker application

1. Log into your PingID environment. Go to **Applications** and click **+** to create a new application.



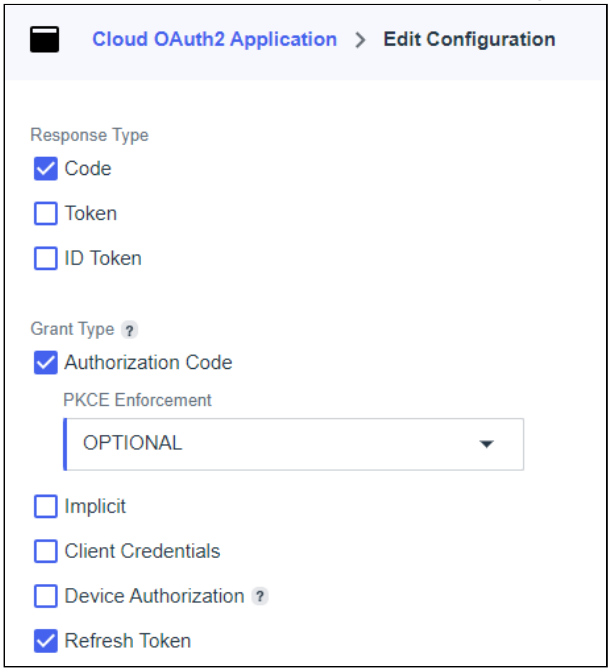
2. Enter the **Application Name** , an optional **Description** , and select **Worker** as the **Application Type**.



3. Click **Save** .

Configuring the Worker application

1. Once saved, select the **Configuration** tab, and click the pencil icon to edit it.
2. In **Response Type**, select **Code.**
3. In **Grant Type**, select:
   a. **Authorization Code**. Also, in the **PKCE Enforcement** field, select **OPTIONAL**.
   b. **Refresh Token**.
4. Disable (uncheck) the **Client Credentials** grant type.

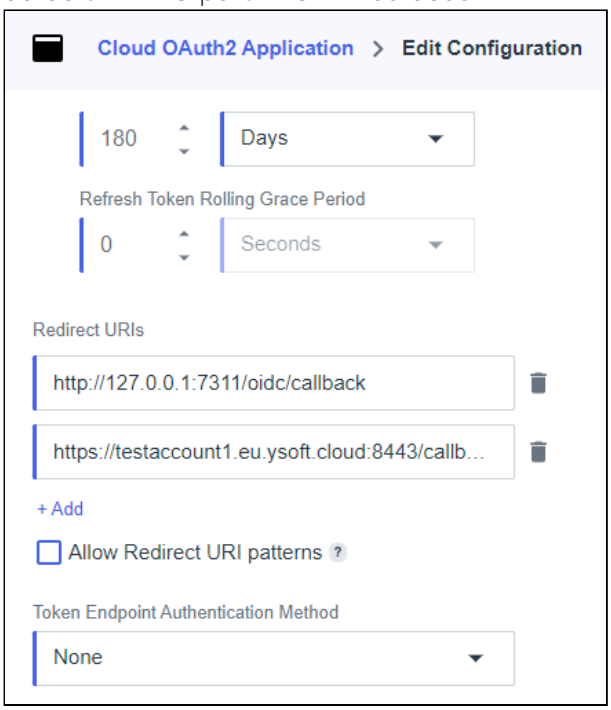


5. In **Redirect URIs**, enter the following:
   a. `http://127.0.0.1:7311/oidc/callback`

   > This redirect address is essential for the SAFEQ Cloud Client to work correctly with PingID authentication.

   b. `https://<your SAFEQ Cloud domain>:8443/callback/ping`. In environments with reverse proxy infrastructure, do not specify the port number in the URL, meaning the

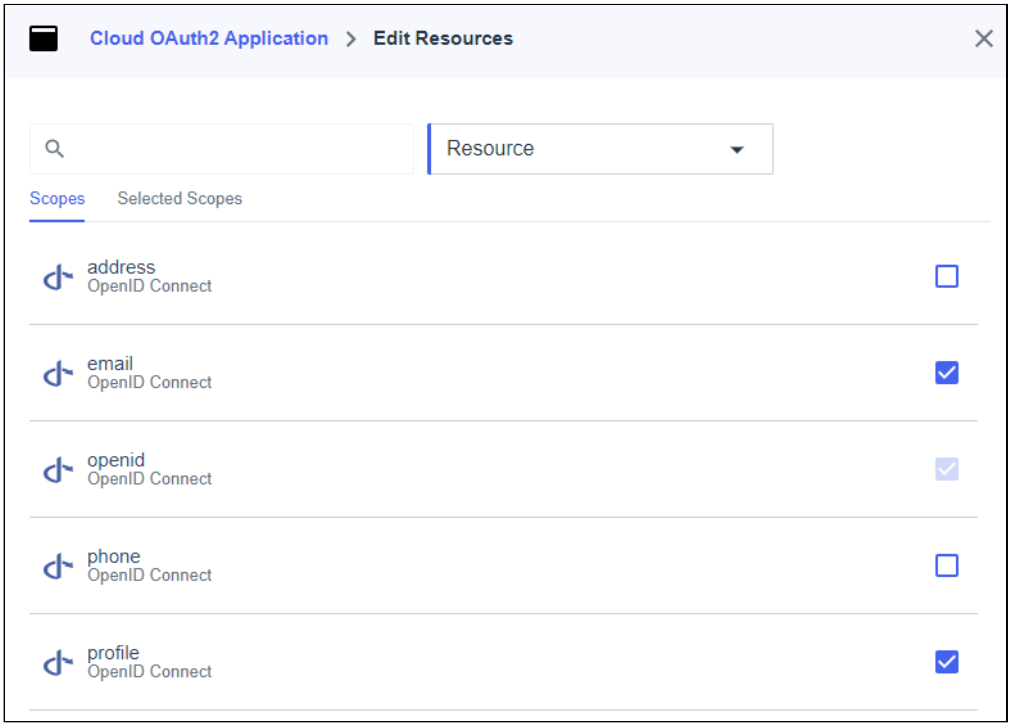
default HTTPS port 443 will be used.



6. In **Token Endpoint Authentication Method**, select **None**.
7. Click **Save**.

Selecting Resources

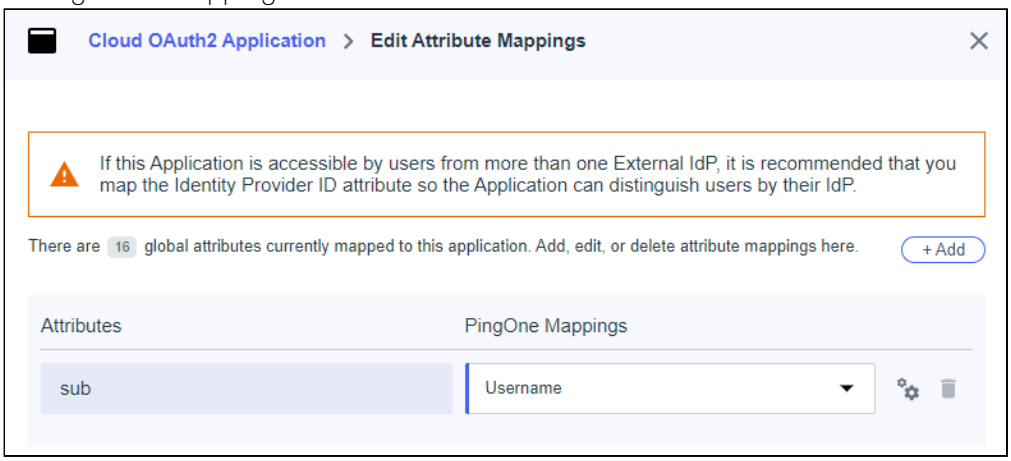
1. Once saved, click the **Resources** tab, then click the pencil icon to edit it. Enable the following scopes:
   a. email (OpenID Connect)
   b. profile (OpenID Connect)



2. Click **Save**.

Mapping the attributes

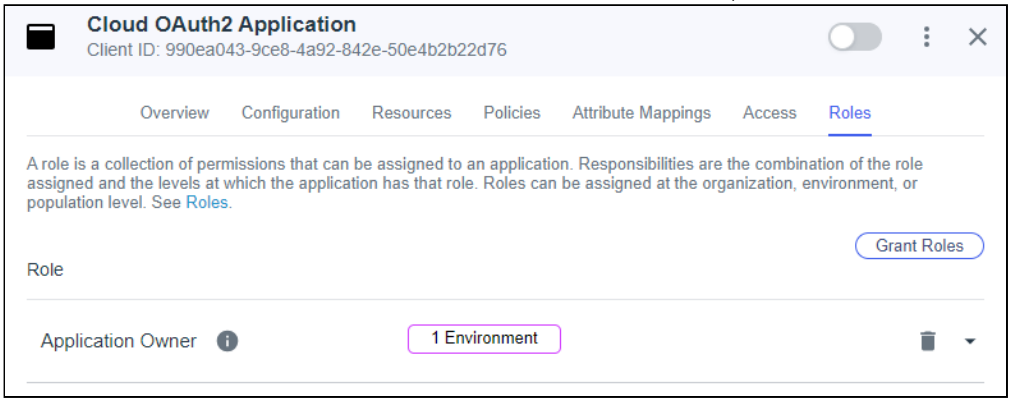
1. Once saved, click the **Attribute Mappings** tab, then click the pencil icon to edit. You should see one Attribute Mapping — **sub = User ID**.
2. Change this mapping to **sub = Username**.



3. Click **Save**.

Removing roles

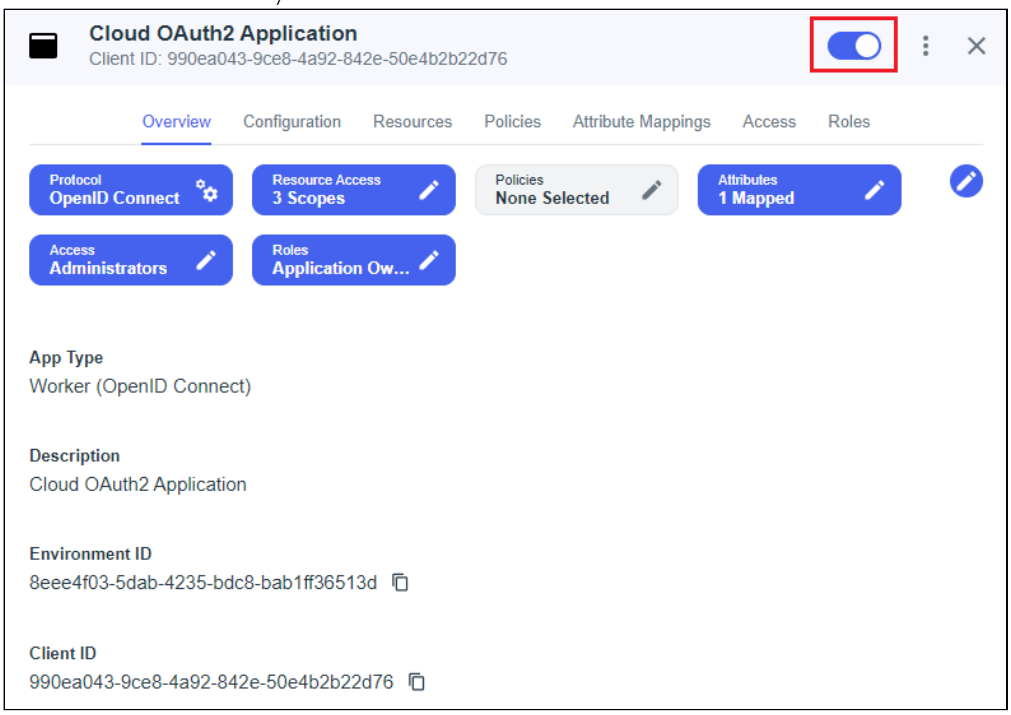
1. Once saved, select the **Roles** tab. If there are any Roles listed, click the **Trash** icon to delete them, and **Save** once all are removed. If none are listed, proceed to the next step.



> For security reasons, it is essential to remove all roles from this application. This will restrict the ability to use the application without an OAuth2 token. OAuth2 token is more secure because it is not stored anywhere and acquired only in interactive mode.

Enabling the Worker application

1. Click the **Overview** tab and click the slider in the top-right corner to enable your application. This will automatically save it.



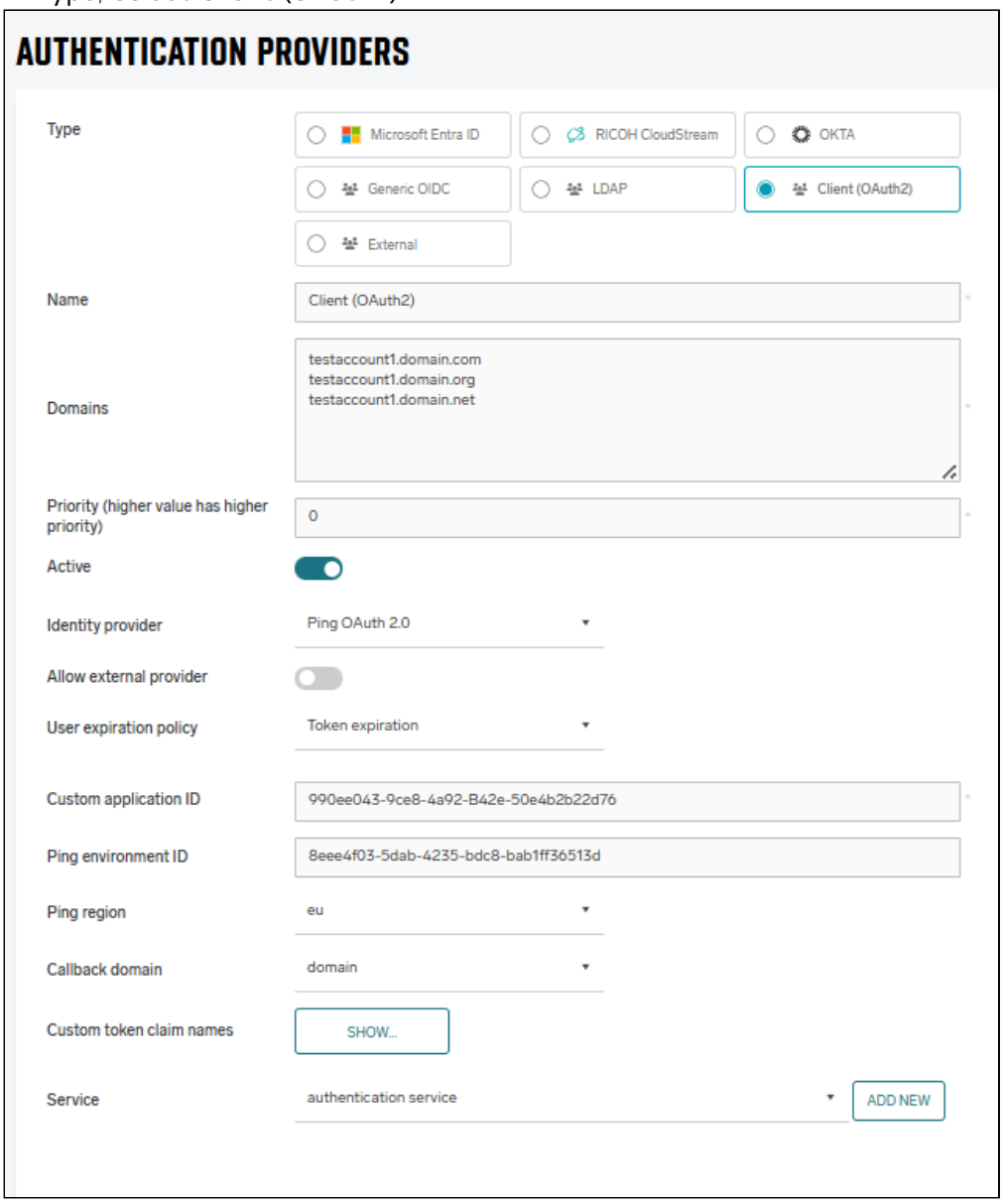
2. Leave this page open as you will need access to some of the application IDs displayed there.

Configuring the PingID Authentication provider in SAFEQ Cloud Web UI

Now that the configuration on the PingID side is complete, proceed to register and configure the Authentication Provider in SAFEQ Cloud.

1. Log into SAFEQ Cloud Web UI and go to **Users** page and to **Authentication providers** tab.
2. Click **Add** to add a new provider.

3. In **Type**, select **Client (OAuth2)**.



4. In **Name**, enter the Authentication provider name. Should be prefilled with the selected type.
5. In **Domains**, list all of the domains present in your PingID environment that will need to authenticate to SAFEQ Cloud. For example, to allow user *john.doe@acme.com* to log in via this Authentication provider, enter the *acme.com* domain here.
6. In **Identity provider**, select **Ping OAuth 2.0**.
7. In **Custom application ID,** paste the **Client ID** from your PingID application **Overview** tab.
8. In **Ping environment ID**, paste the Environment ID from your PingID application **Overview** tab.
9. **Ping region** is the region in which your PingID environment is registered. You can determine it from your PingID Console URL which is in the format of `https://console.pingone.[region].` Alternatively, you can find it in any of the URLs listed under your PingID OAuth

application **Configuration** tab such as `https://auth.pingone.[region]/[client]/as/authorize`

10. In **Callback domain for custom application**, enter the SAFEQ Cloud tenant address you used as the **Redirect URI** in your PingID OAuth application configuration.
11. Click **Save**.

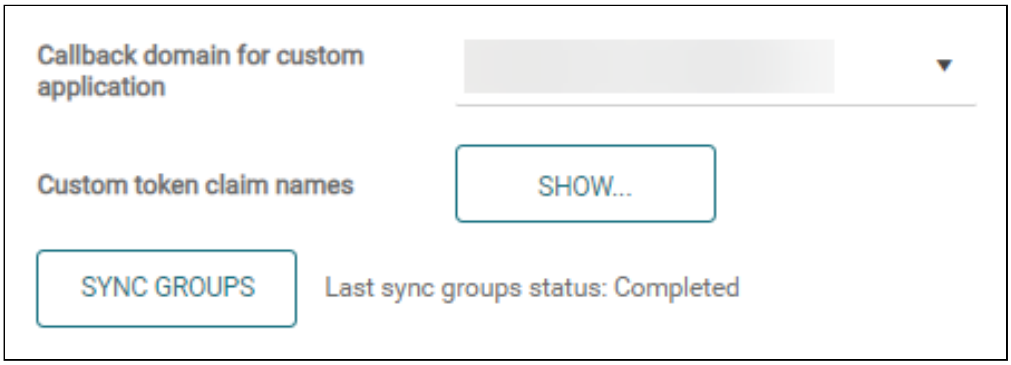
For more details on the available options for OAuth2 authentication, see Client authentication.

Synchronizing groups

After creating and saving your new Authentication provider, you can perform group synchronization, which will allow you to manage Access Control of your SAFEQ Cloud tenant via PingID group membership.

To synchronize groups perform the following steps:

1. On the SAFEQ Cloud Web UI **Users** page, under the **Authentication providers** tab, click the **Edit** icon for your PingID provider.
2. Click **SYNC GROUPS**.



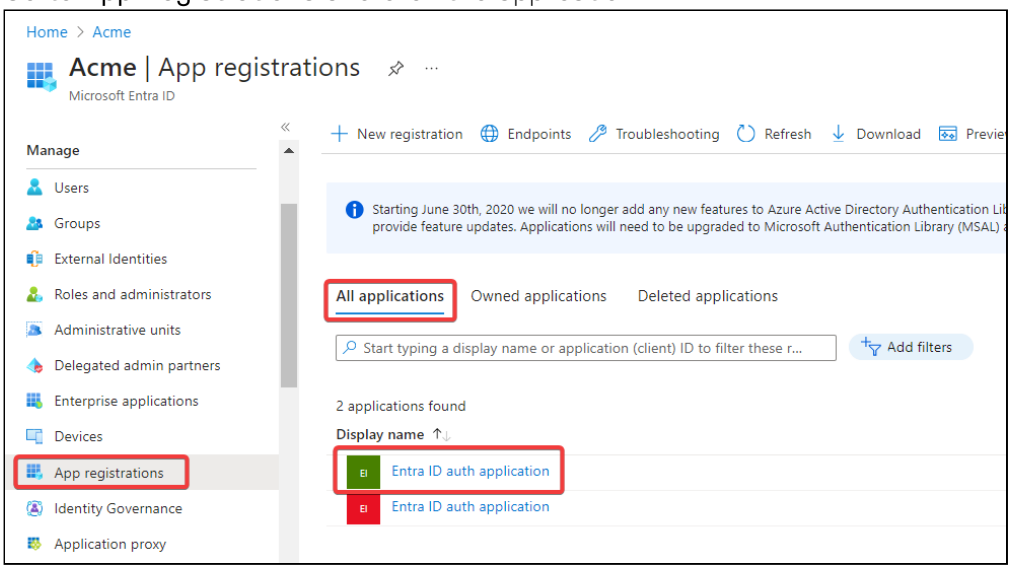
3. You will be redirected to the PingID login page.
4. Log in with an account that has permission to read groups and follow the on-screen instructions. When the form closes, group synchronization is complete. For more details, see Client authentication, section *Sync groups*.
5. You will now be able to search for PingID groups on the **Access Control** tab of the **Users** page. For more details, see Access Control.

Edit a custom app in Microsoft Entra ID

> If the Entra application is not a Native app, we recommend adding a new application from scratch. See Add a custom app in Microsoft Entra ID.

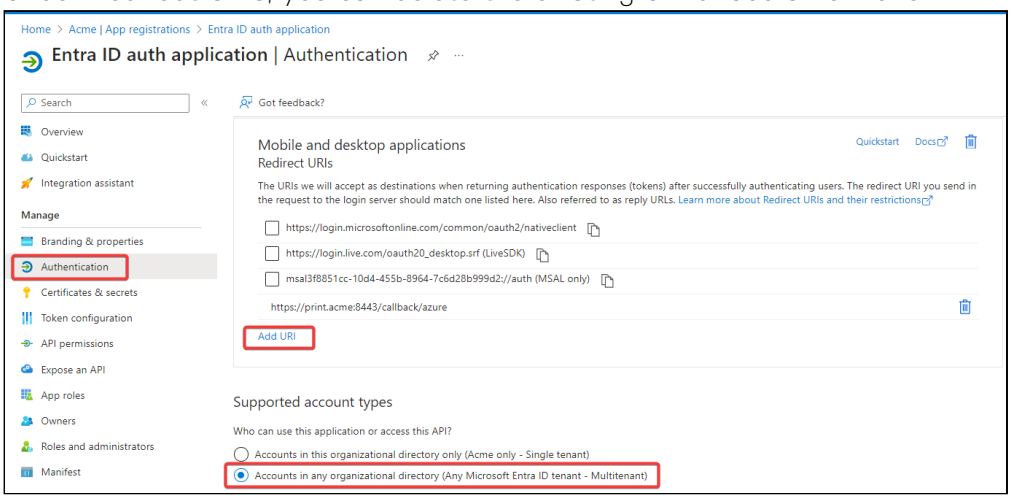
To edit an existing Native Entra application, follow these steps:

1. Go to **App Registrations** and click the application.



2. On the application page, click **Authentication**.

3. Under **Redirect URIs**, you can delete the existing URI or add a new one.



4. In **Supported account types,** select **Accounts in any organizational directory (Any Microsoft Entra ID tenant – Multitenant).**

5. Save your changes.

Google Workspace service account

To use Google Workspace Client authentication, you must create a service account. This will allow you to validate users against Google and synchronize Groups for Access Control.

1. Follow the steps in Google documentation: https://developers.google.com/identity/protocols/oauth2/service-account#creatinganaccount.

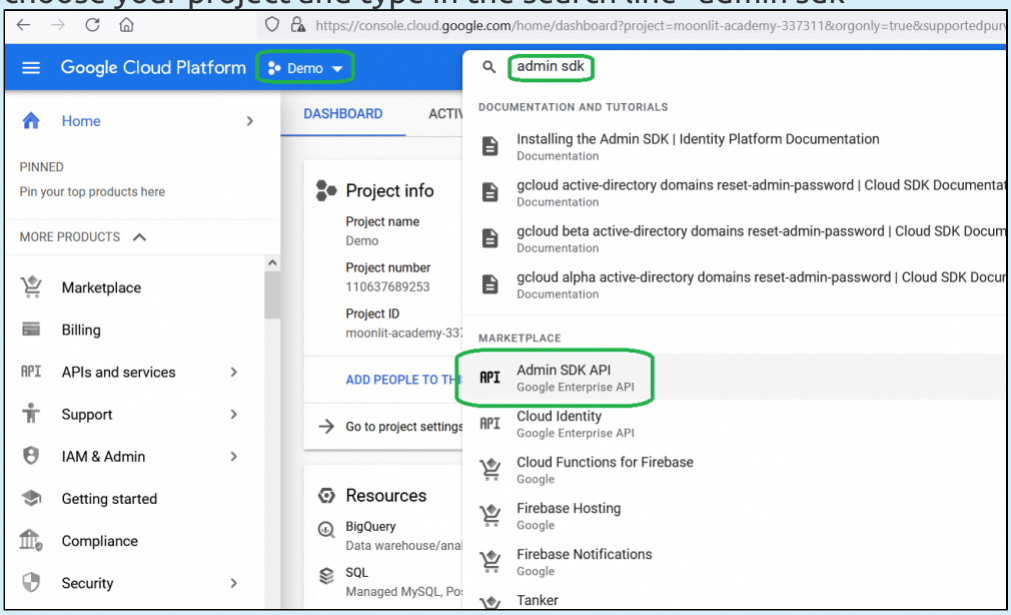
2. As part of the key creation process, a private key is generated as a JSON file. Save it in your PC. You will need to copy its content into **Secret JSON file content** form field.

3. Delegate the service account that you have created for domain-wide authority. Follow the steps from Google documentation: https://developers.google.com/identity/protocols/oauth2/service-account#delegatingauthority .

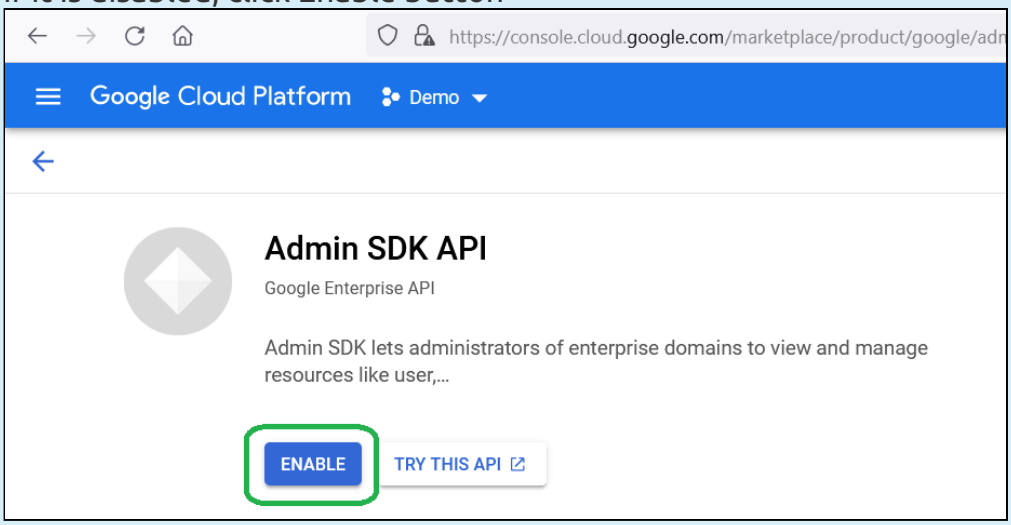
4. You will need the following scopes for SAFEQ Cloud communication:
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.group.member.readonly
   - https://www.googleapis.com/auth/admin.directory.group.readonly
5. In the Google Workspace authentication provider form creation, enter the account name that has a super admin role (not service account name!) and paste the content of the JSON file you saved before. Make sure that the JSON file content is wrapped in curly braces { } when you paste it. Click **Test** to make sure it is working. You can also serialize JSON and paste it as a solid string in between { }.

This approach requires using admin account for service account to impersonate, the possible actions for this impersonation are limited by the scopes you entered for the domain-wide delegation. For more information, see this article by Google.

Check if Admin SDK API is enabled for your project, and if it's not, enable it: choose your project and type in the search line "admin sdk"



if it is disabled, click Enable button

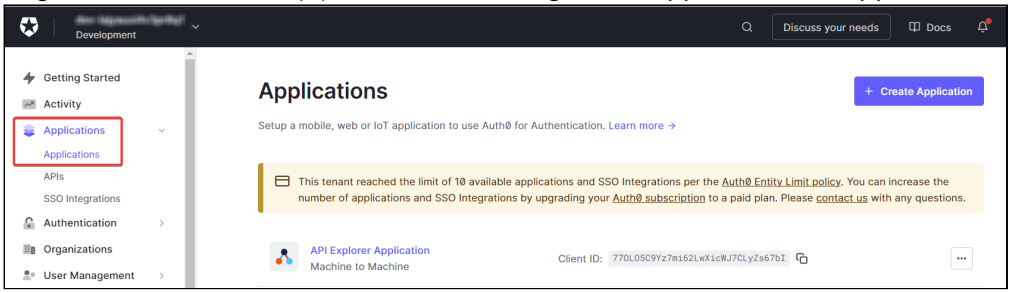


Add a custom app in the Auth0 identity platform

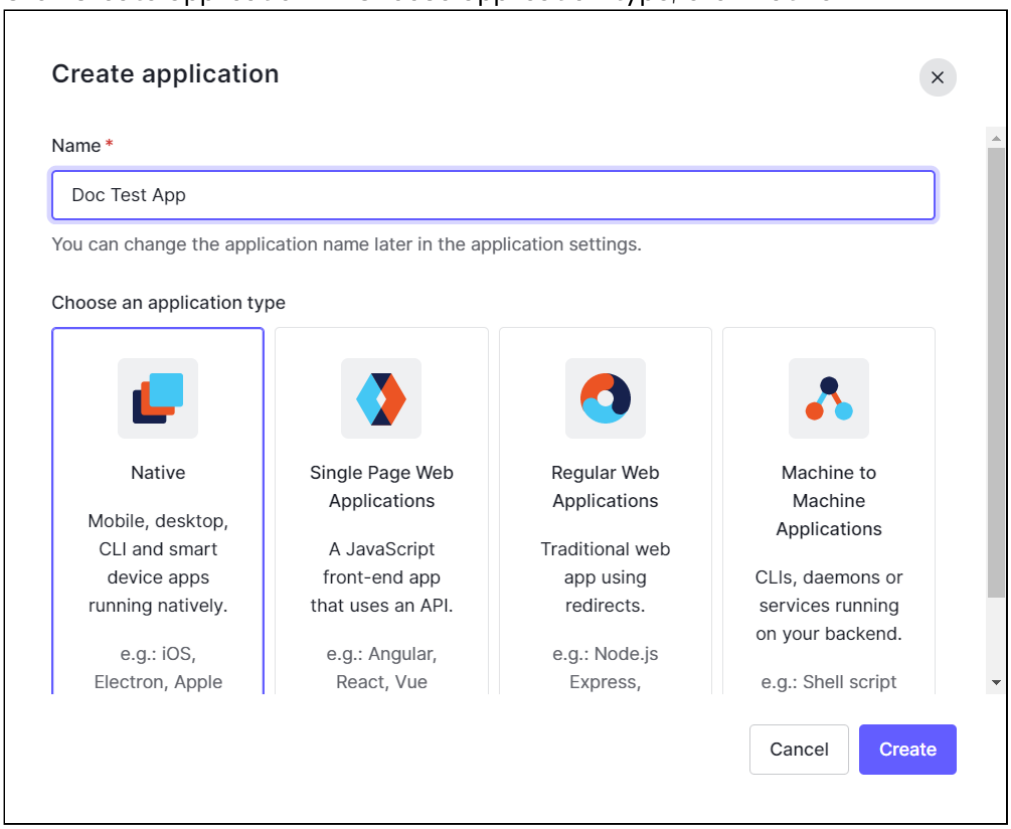
This page describes the steps to create an authentication client application in the Auth0 identity platform.

Creating a Native application

1. Log in to Auth0 identity platform and navigate to Applications > Applications .

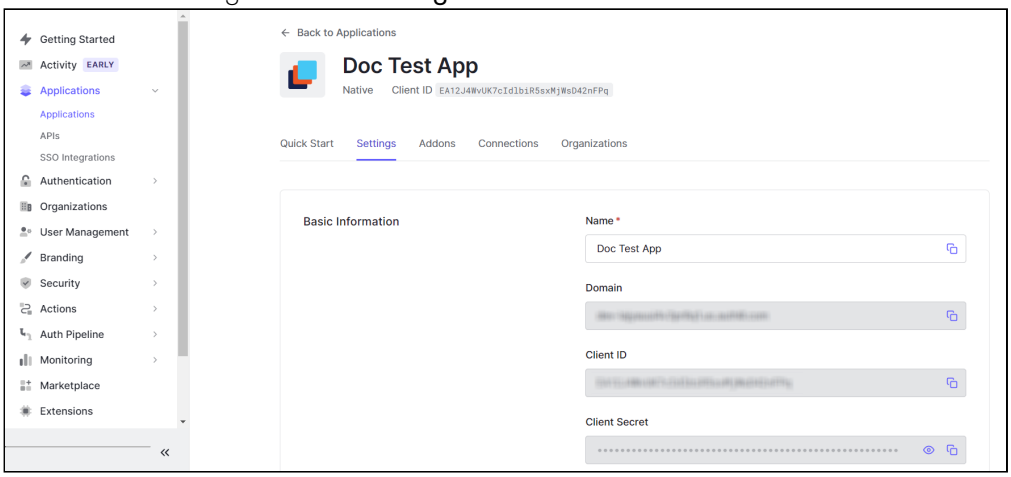


2. Click **Create application**. In **Choose application type**, click **Native** .



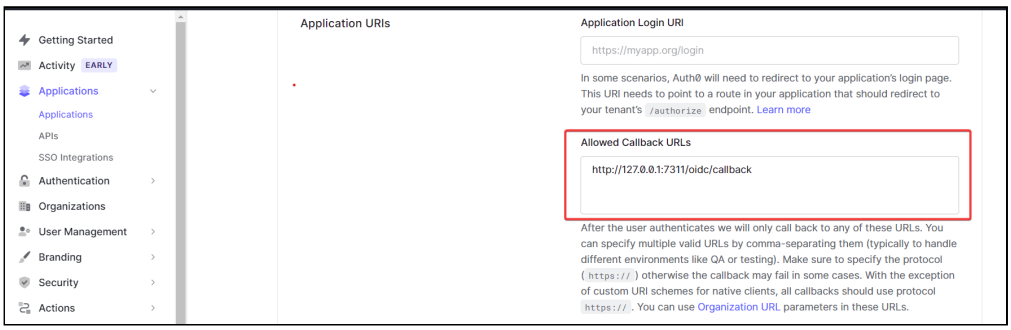
3. In **Name**, enter the application name.

4. Click **Create** and go to the **Settings** tab.



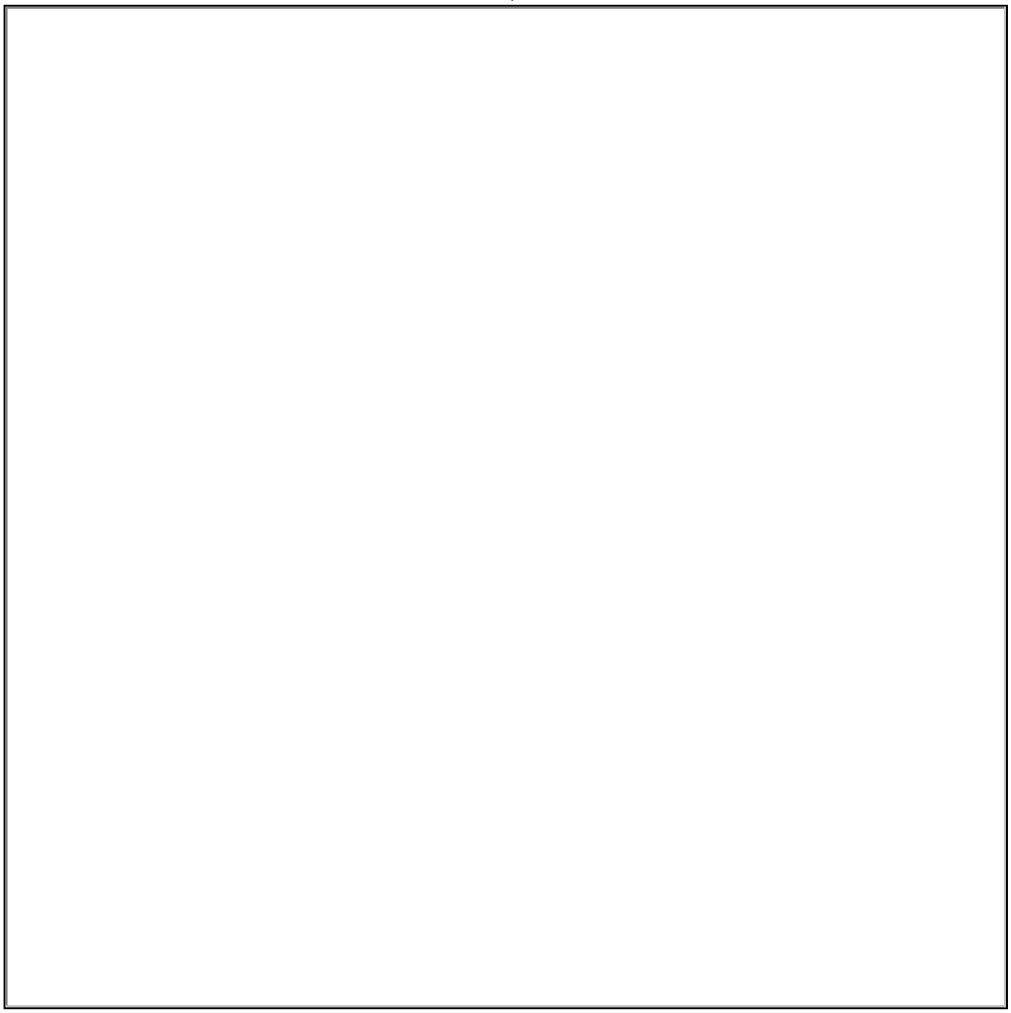
Domain – The domain used for authentication. You will need this value to create the Client Authentication provider in the SAFEQ Cloud web UI.
Client ID – The ID of the application. You will need this value to create the Client Authentication provider in the SAFEQ Cloud web UI.

5. In **Application URIs**, enter the following URL in the Allowed Callback URLs field: http://127.0.0.1:7311/oidc/callback. This is necessary for end users to use the SAFEQ Cloud Client with client-based authentication.



Creating Client Authentication provider in SAFEQ Cloud web UI

1. In the SAFEQ Cloud Web UI, navigate to **Users** page and to **Authentication providers** tab.
2. Click **Add** to add a new Authentication provider.

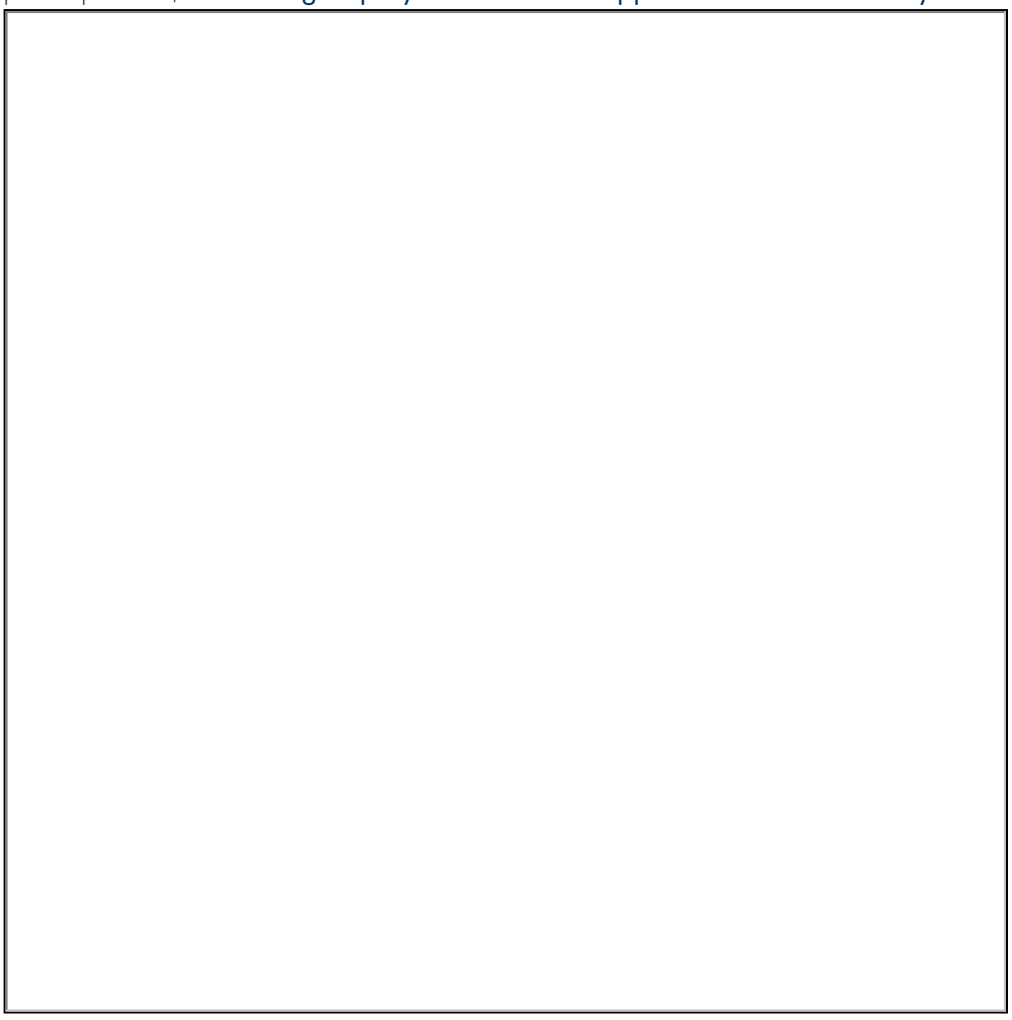


Fill in the following fields:

- **Domains** – Enter the domains of all users (with emails *user@domain*) who will authenticate to SAFEQ Cloud.
- **Custom application id** – Mandatory field. Enter the **Client ID** value of the Native application you created in the Auth0 platform.
- **Auth0 Domain** – Enter the **Domain** of your application in Auth0 platform.
- **Client ID** – Client ID of the application.

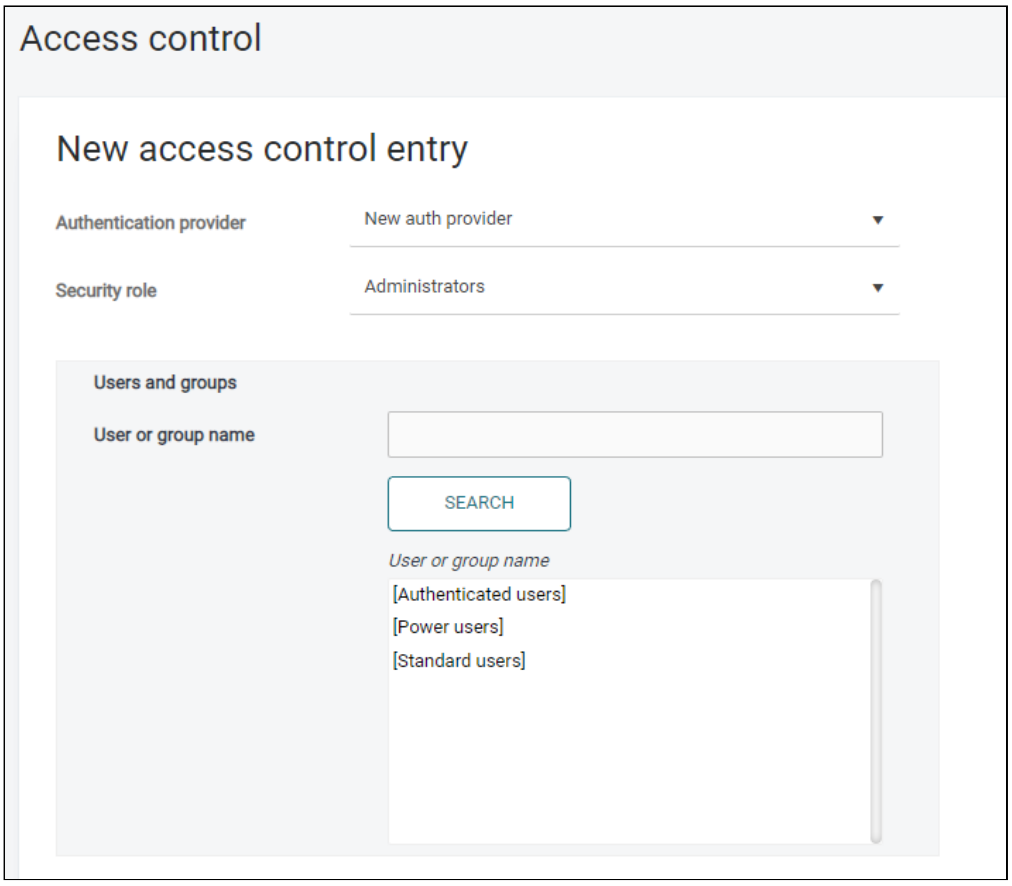
- Sync Groups - Client ID - Client ID of the Regular Web Application. This field requires you to have a synchronization app in the Auth0 identity management. See Add group synchronization app in the Auth0 identity management.
- Sync Groups - Client Secret - Client Secret of Regular Web application. This field requires you to have a synchronization app in the Auth0 identity management. See Add group synchronization app in the Auth0 identity management.
- Custom token claim names - in this section, you can define claim names in the token. Their values will be stored in the user attributes after login.

3. Click Save.
4. (Optional) If you wish to synchronize groups from Auth0:
   a. Click the edit icon next to your newly created Authentication provider.
   b. Click Sync Groups to start synchronization of groups from your Auth0 account. For prerequisites, see Add group synchronization app in the Auth0 identity management.



5. Go to the Users page and to Access control tab.

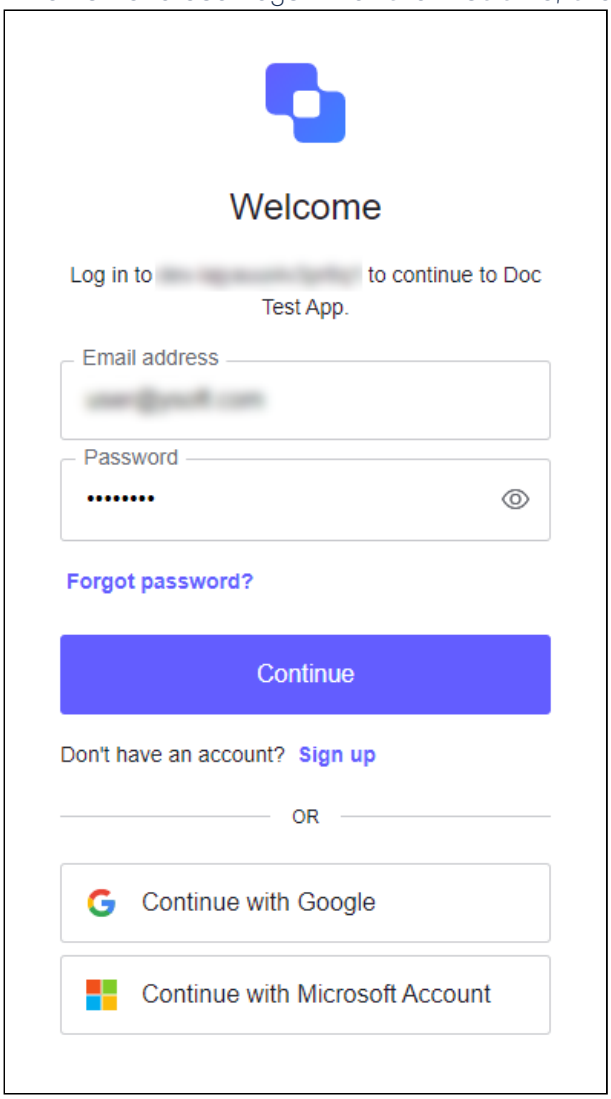
6. Click **Add**.

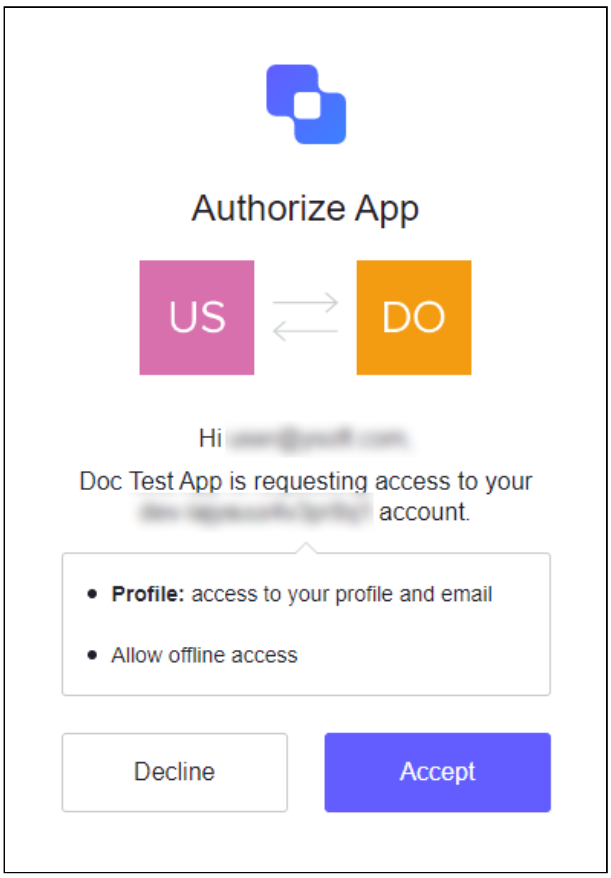


7. In **Authentication provider**, select your newly created Authentication provider and click **Search**.
8. The default group **Authenticated Users** will become visible. You can use this groups and individual users in access controls to enable permissions for authenticated users
9. If the group synchronization is set up, Auth0 Groups will be visible too. For more information about Auth0 Groups see https://auth0.com/docs/manage-users/access-control/configure-core-rbac/roles/create-roles.

Logging in as a user

1. When an end user logs in for the first time, they must authorize the app.



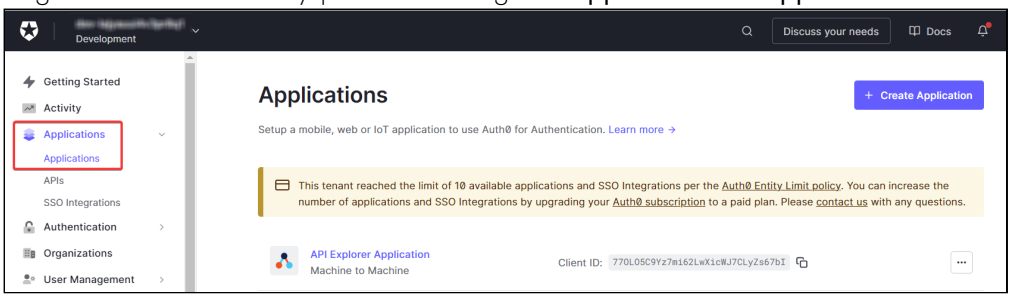


Add group synchronization app in the Auth0 identity management

To synchronize groups from Auth0, you must create a group synchronization application in the Auth0 identity platform.

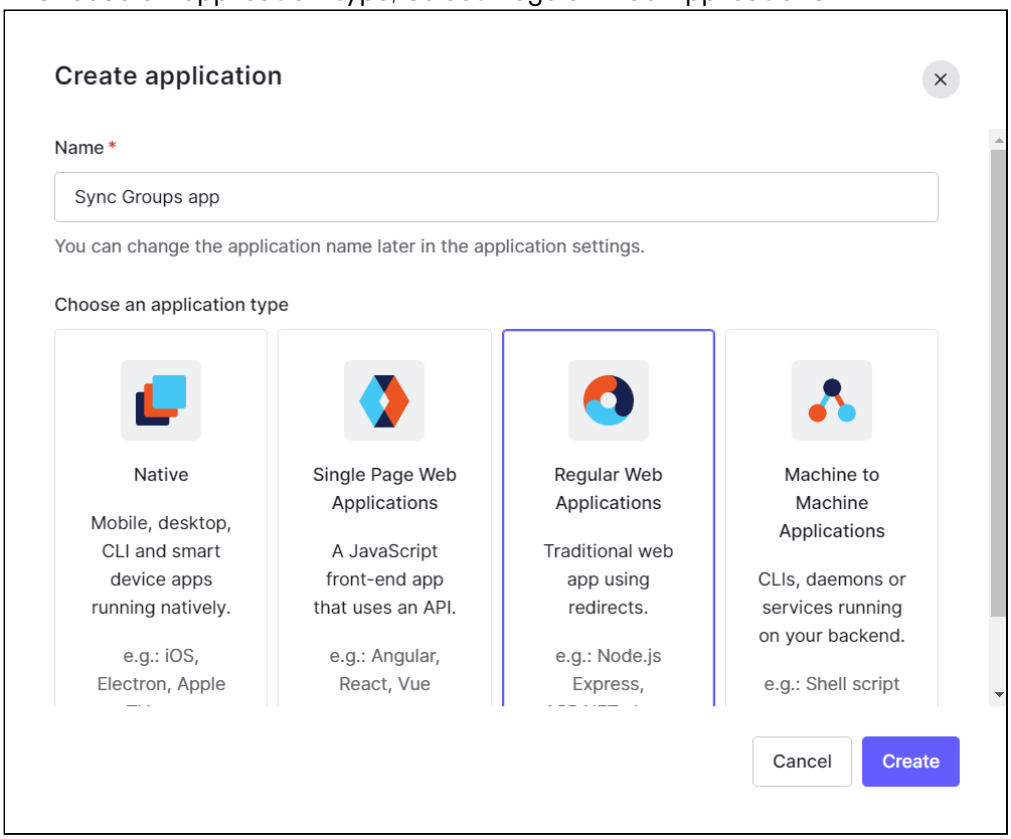
Creating a Regular Web Application in Auth0

1. Log in to Auth0 identity platform and go to Applications > Applications.



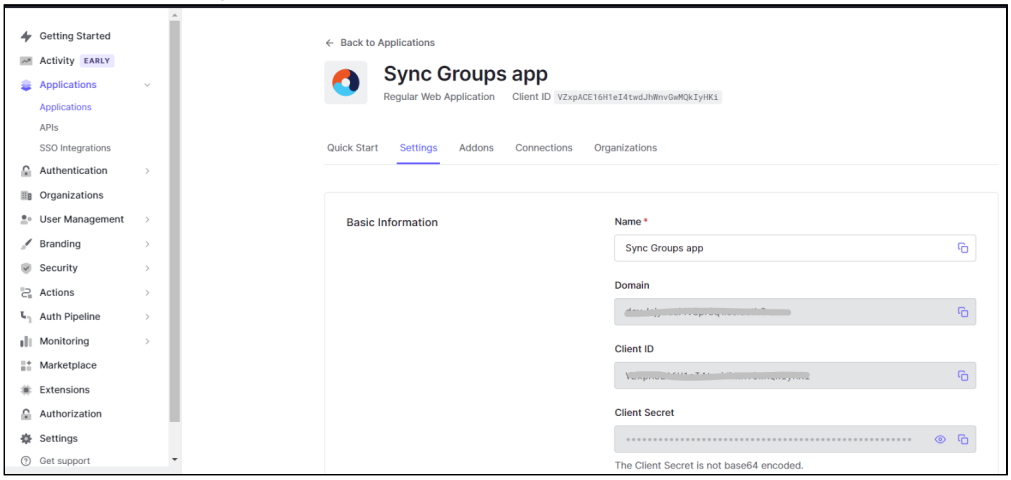
2. Click Create Application.
3. Enter the name of the application.

4. In **Choose an application type**, select **Regular Web Applications**.



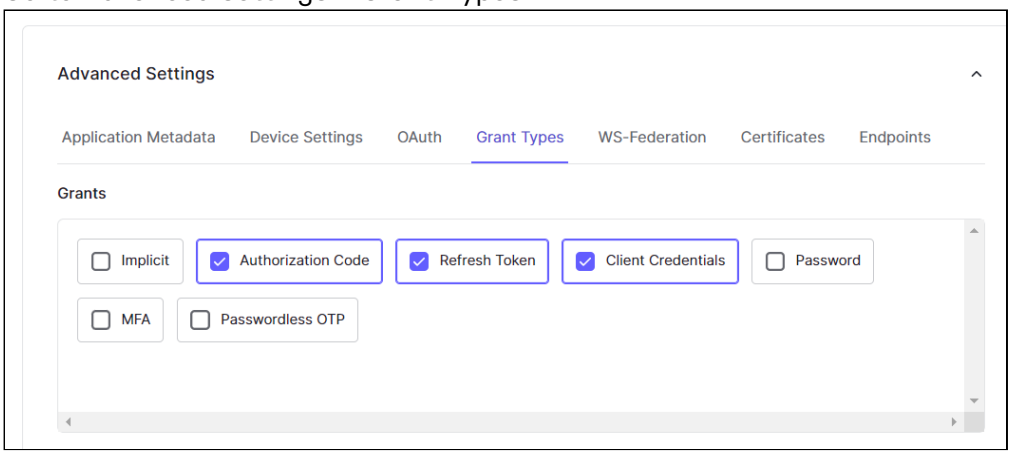
5. Click **Create**.

6. Go to the **Settings** tab.



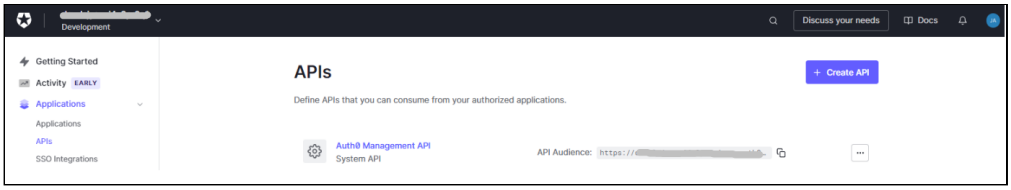
Domain – The domain used for authentication. This is common for all your applications.
Client ID – The ID of the application.
Client Secret – The client secret of the application.

7. Go to **Advanced settings** > **Grant Types**.



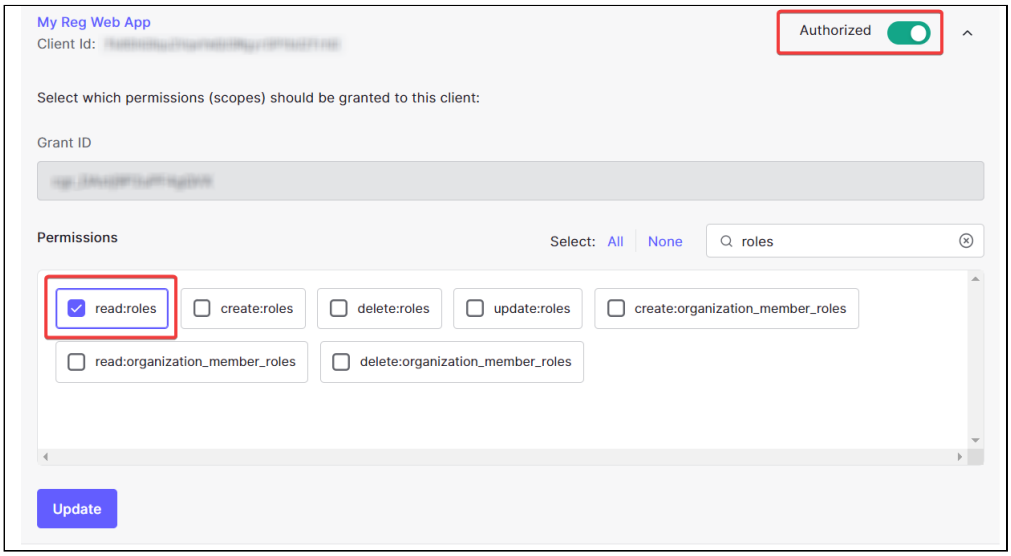
8. Make sure that the following grants are selected:
   - Authorization Code
   - Refresh Token
   - Client Credentials

9. Go to **Applications** > **APIs**.



10. Select the API you want your newly created application to access.

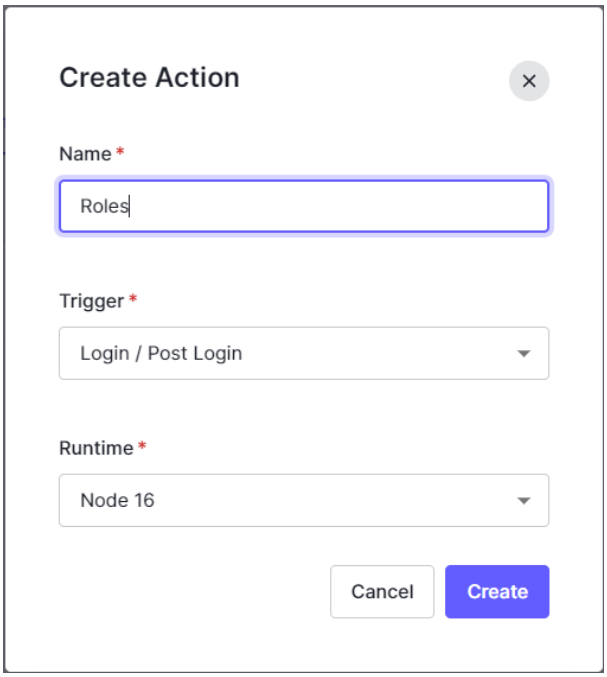
11. Go to to **Machine to Machine Applications** tab and find your newly created application. Authorize it, and in **Permissions**, select **read:roles**.



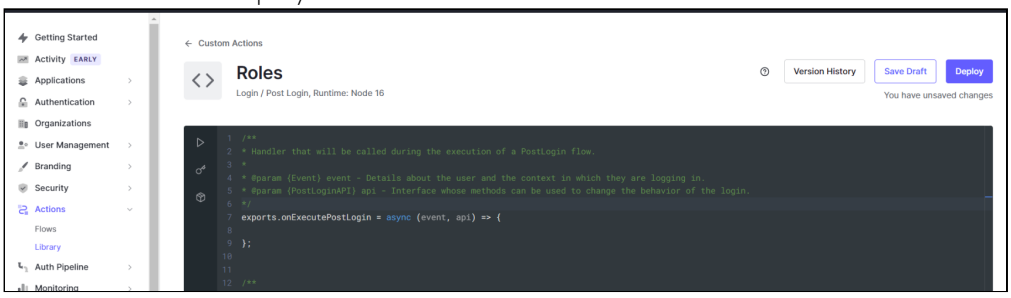
Adding user roles into the JWT token

For more information, see Auth0 documentation: https://auth0.com/docs/manage-users/access-control/sample-use-cases-actions-with-authorization#add-user-roles-to-tokens

1. In Auth0 Identity platform, go to **Actions** > **Library** > **Custom**.
2. Click **Build Custom**.



3. Enter the Action name.
4. In **Trigger**, select **Login / Post Login**.
5. In **Runtime**, select **Node 16**.
6. Click **Create**.
7. An editor will be displayed.

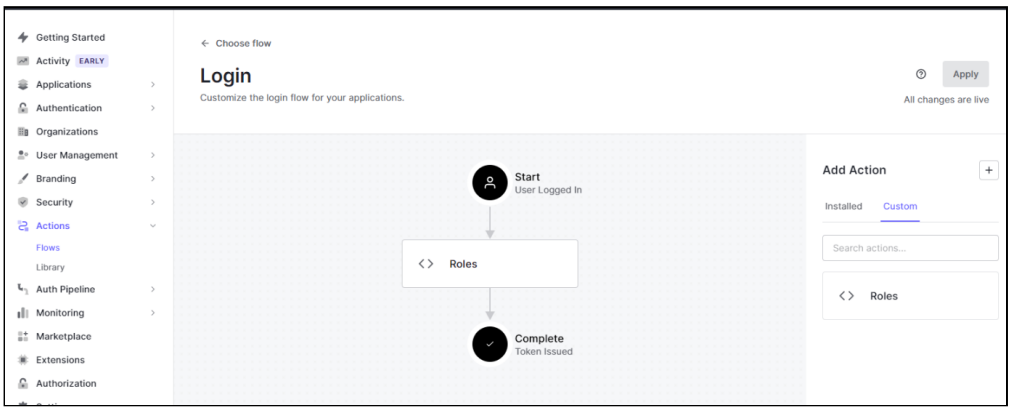


8. Paste the following block of code and click **Deploy**.

```
exports.onExecutePostLogin = async (event, api) => {
  const namespace = 'SAFEQ Cloud';
  if (event.authorization) {
    api.idToken.setCustomClaim(`${namespace}/roles`, event.authorization.roles);
    api.accessToken.setCustomClaim(`${namespace}/roles`, event.authorization.roles);
```

```
  }
};
```

9. Go to Actions > Flows > Login.



10. Drag and drop newly created Action to Login flow.

11. Click Apply.

External authentication

SAFEQ Cloud supports external authentication provider where external authentication service such as External Card Repository is used to identify users from different authentication providers. For more details on how a specific external provider works, see the documentation section dedicated to that external provider.

Adding a new external authentication provider

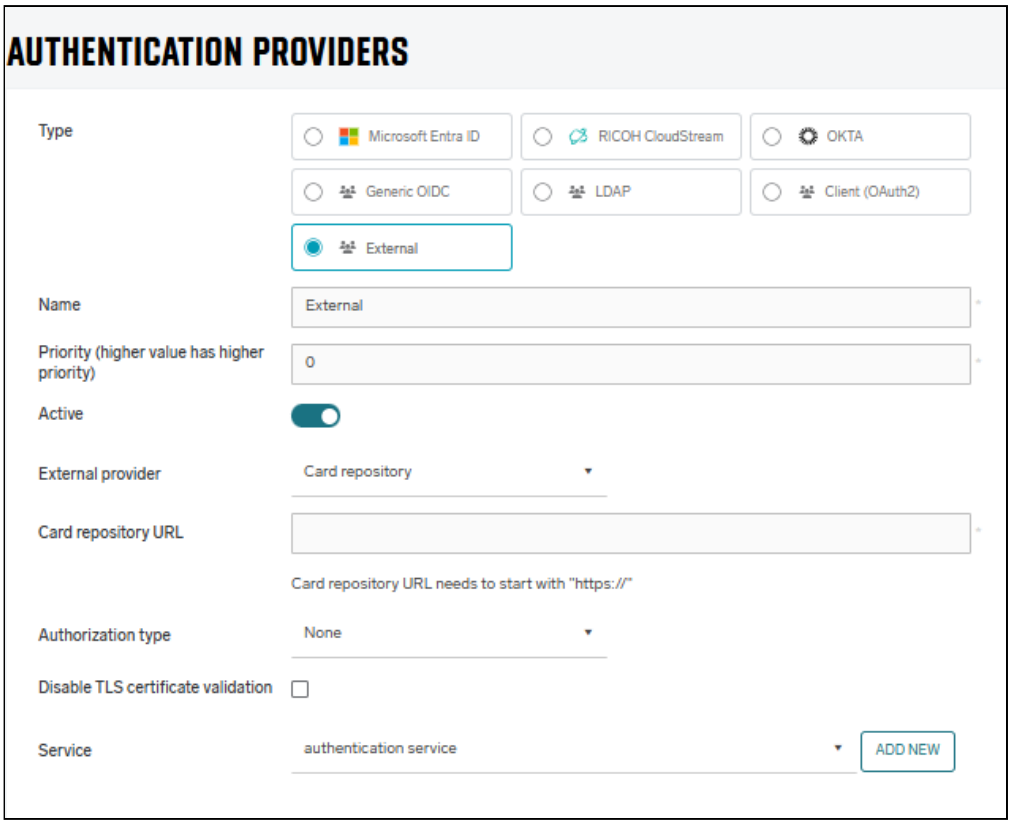
To add a new external authentication provider, perform the following steps:

1. Log in to SAFEQ Cloud Web UI and go to Users page and Authentication providers tab.
2. Click Add.
3. Fill in the following:
   - Type – select External.
   - Name – Name your new authentication provider. Should be prefilled with selected Type.
   - Priority – A number determining the order in which authentication providers will be called until one succeeds. Higher-priority providers will be called first.

     ⚠ When authenticating via card/PIN (Short ID), the user's card/PIN is first searched for in SAFEQ Cloud and only if it is not found, the authentication providers are called in order of their priorities. This means that when using External Card Repository (ECR) and the user has a card assigned in SAFEQ Cloud, they are authenticated without a call to ECR. If you want to call the ECR for every card authentication request, do not assign cards to users in SAFEQ Cloud.

   - External provider – select the external provider.

- Service – Select the authentication service. If no service is already created, you can add it via the Add button. If the primary server has only one authentication service, or if only one authentication service in general exists, it is pre-selected by default.



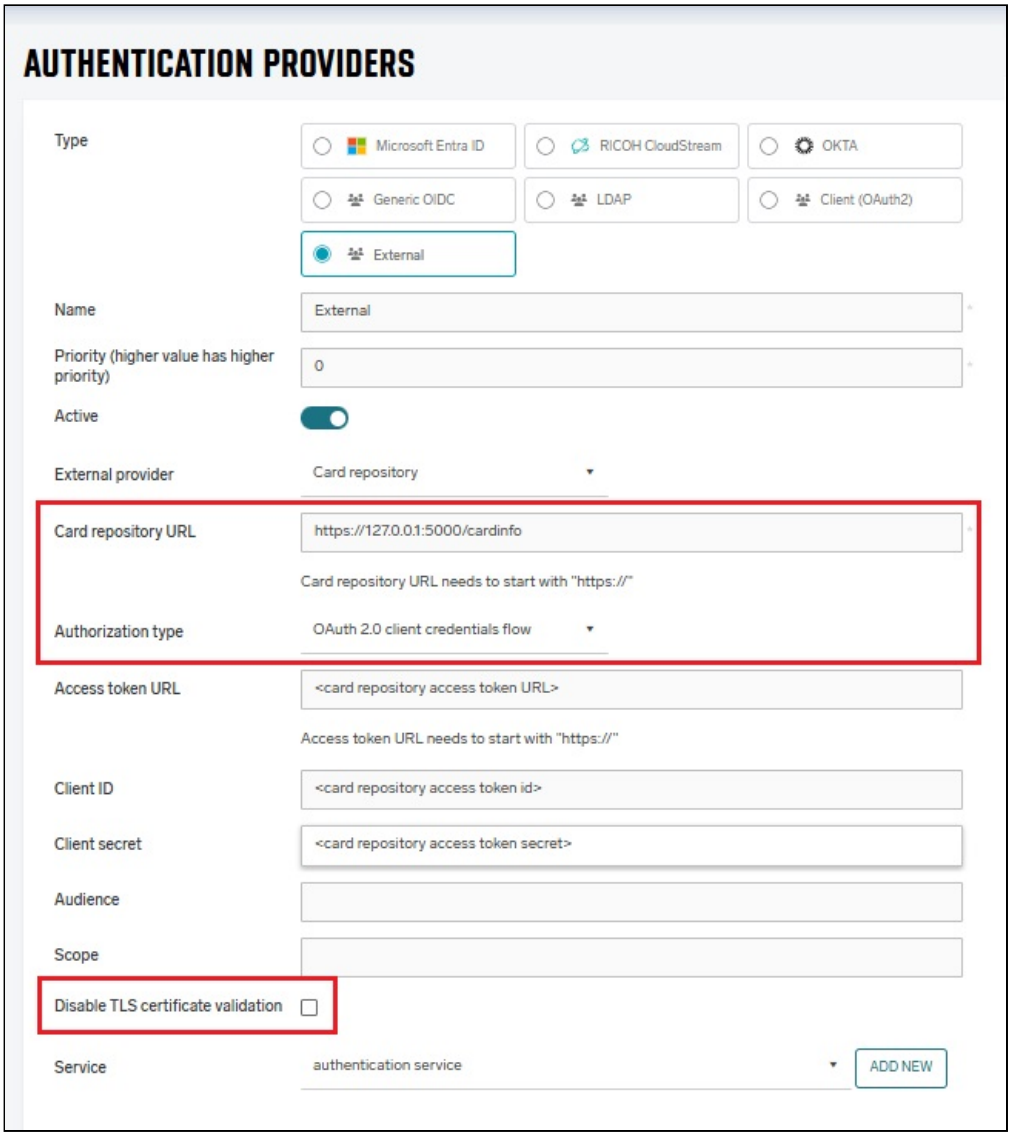
When a user is authenticated using ECR, they will be created in SAFEQ Cloud database under the corresponding Client provider and visible in the Users section, when you choose the corresponding Client provider in the drop-down list.

User properties and Access Control can be modified by administrators.

External Card Repository (ECR)

1. In the External provider, choose Card Repository.
2. Fill in the following information:
   - Card repository URL – The URL of the External Card Repository.
   - Authorization type – the authorization that is used for securing the ECR. Currently, SAFEQ Cloud supports only ECR that is secured using OAuth 2.0 Client Credentials Flow or not secured:
     - OAuth 2.0 Client Credentials Flow – The recommended option used to authenticate requests from SAFEQ Cloud to ECR.
     - None – We strongly recommend not to use unsecured ECR outside of scenarios where both SAFEQ Cloud and ECR are deployed within the customer's LAN.
   - Disable TLS certificate validation – The option to disable validation of HTTPS certificates. We strongly recommend keeping this option disabled and always validating certificates.

- **Service** – Select the authentication service. If no service is already created, you can add it via the **Add** button.



3. If you selected the **OAuth 2.0 Client Credentials Flow**, fill in the following information:
   - **Access Token URL** – A mandatory field. The URL where SAFEQ Cloud can request an access token.
   - **Client ID** – A mandatory field. The Client ID that SAFEQ Cloud will use to get an access token from the ECR.
   - **Client Secret** – A mandatory field. The Client secret that SAFEQ Cloud will use to get an access token from the ECR.
   - **Audience** – An optional field that you can use to restrict the usage of the access token.
   - **Scope** – An optional field which specifies the scope of the access token.

User expiration policy

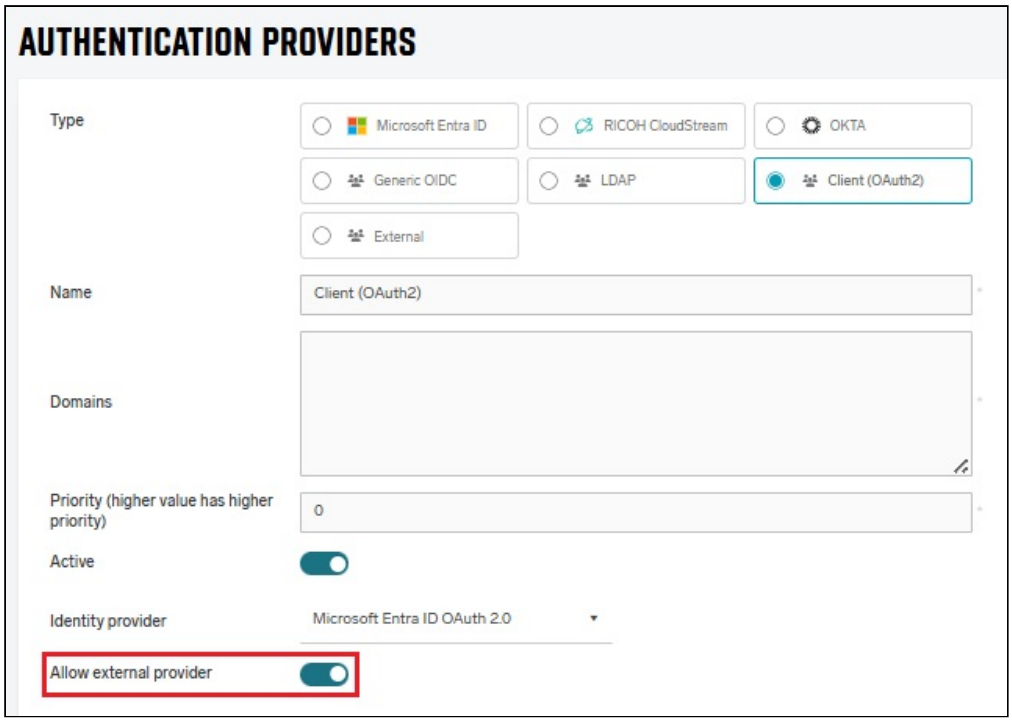
A user who authenticates at the MFD via an External provider will automatically get an expiration value from the user detail. The default value is one hour, unless it is set otherwise in the external provider.

This means that after the defined time since authentication via an External provider (e.g. one hour), the user won't be able to authenticate at MFD via less secure means, such as Short ID (PIN). The user must authenticate in a secure way, such as card number stored in ECR, username/password, or OIDC (for example, via SAFEQ Cloud Client). In this way, the token is refreshed, and the user expiration starts running again.

For more details, see External Card Repository.

Enabling external authentication for a client provider

External authentication must be allowed in each provider where the users will be logging via external authentication. External authentication is only supported for authentication providers where Type is Client. To allow external authentication in your client provider, click Show advanced options, and then select Allow external provider.

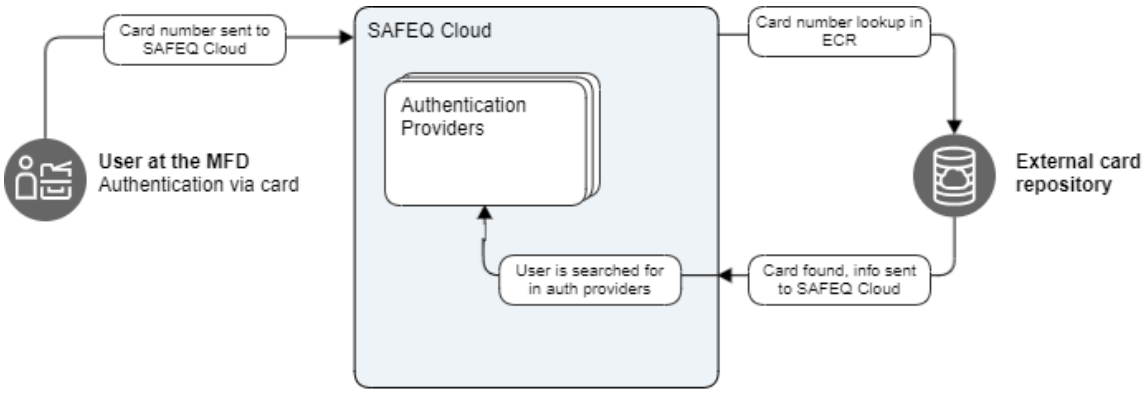


External Card Repository

Overview

An External Card Repository (ECR) refers to a storage or database system that stores and manages a collection of cards or card-like entities. External Card Repository can be accessed by API from SAFEQ Cloud and is used to allow authentication using Card number without assigning the card number manually in SAFEQ Cloud Web UI or using Card enrollment at the MFD.

ECR works as follows:



Technical details

If the ECR is set up in SAFEQ Cloud Web UI and allowed in at least one client provider, SAFEQ Cloud calls the External Card Repository URL as *POST* request with *cardno* parameter.

Example of ECR request:

```
curl -L 'https://external.card.repo:5000/cardinfo' -F 'cardno="1234567890123456"'
```

The content of the response should be in application/json format and should contain:

- **userName**: String Username usually in form of an email address. It must be unique for each user. The field is mandatory.
- [optional] **fullName**: `String`
- [optional] **email**: `String`
- [optional] **department**: `String`
- [optional] **expiration**: `Int` Time in milliseconds, after which the user must log in again.
- [optional] **externalId**: When integrating with Auth0, this field is mandatory. For other providers, this field is not used.
- [optional] **groups**: `list[Group]` List of groups the user is a member of. The user will have access rights according to these groups.

Group:

- **dn**: `String` The distinguished name of the group.

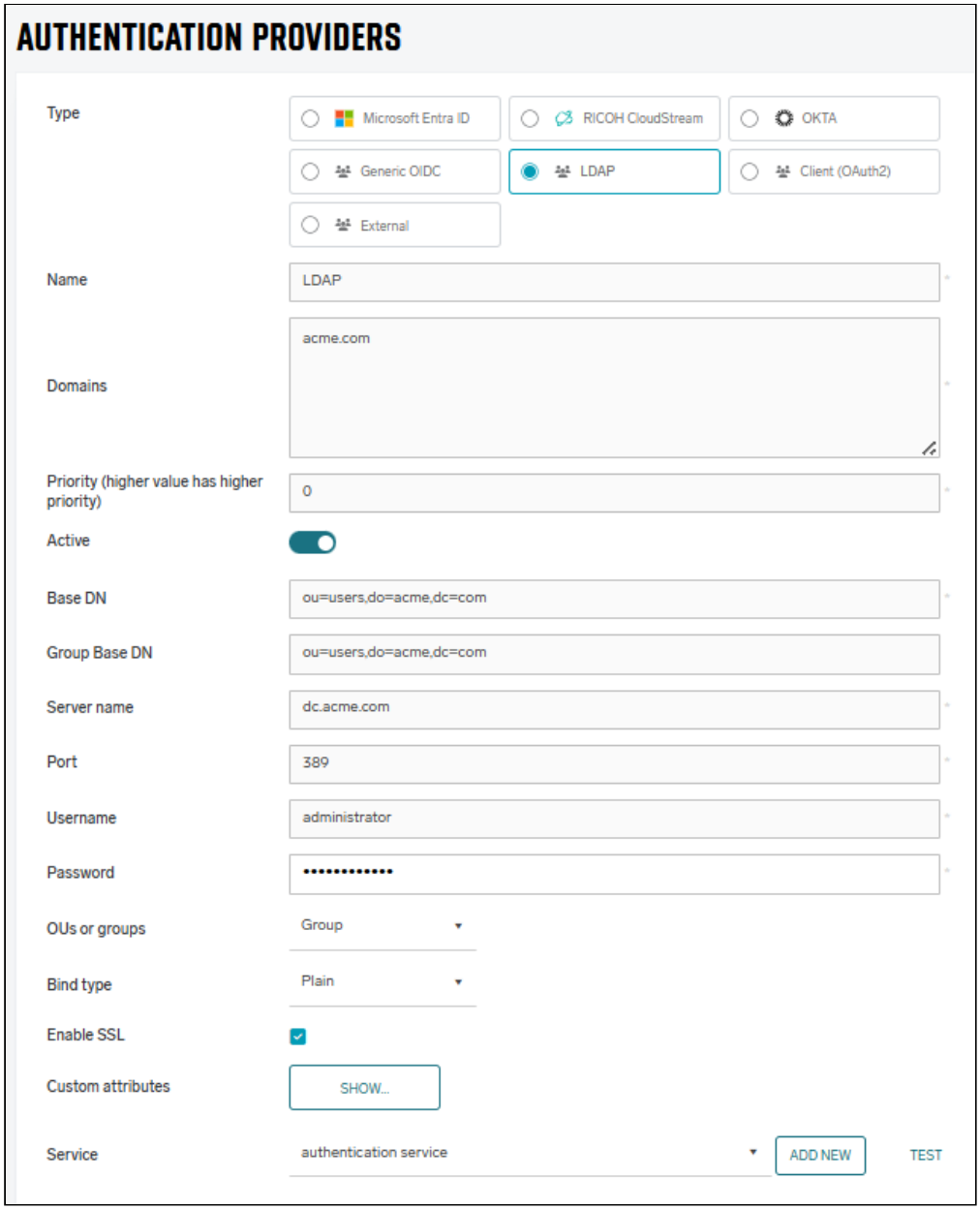
The user in the SAFEQ Cloud database will be updated with all the provided fields. If an optional field is missing, it will not be updated.

Example response:

```
{
   "userName": "johndoe@domain.com",
   "fullName": "John Doe",
   "email": "johndoe@domain.com",
```

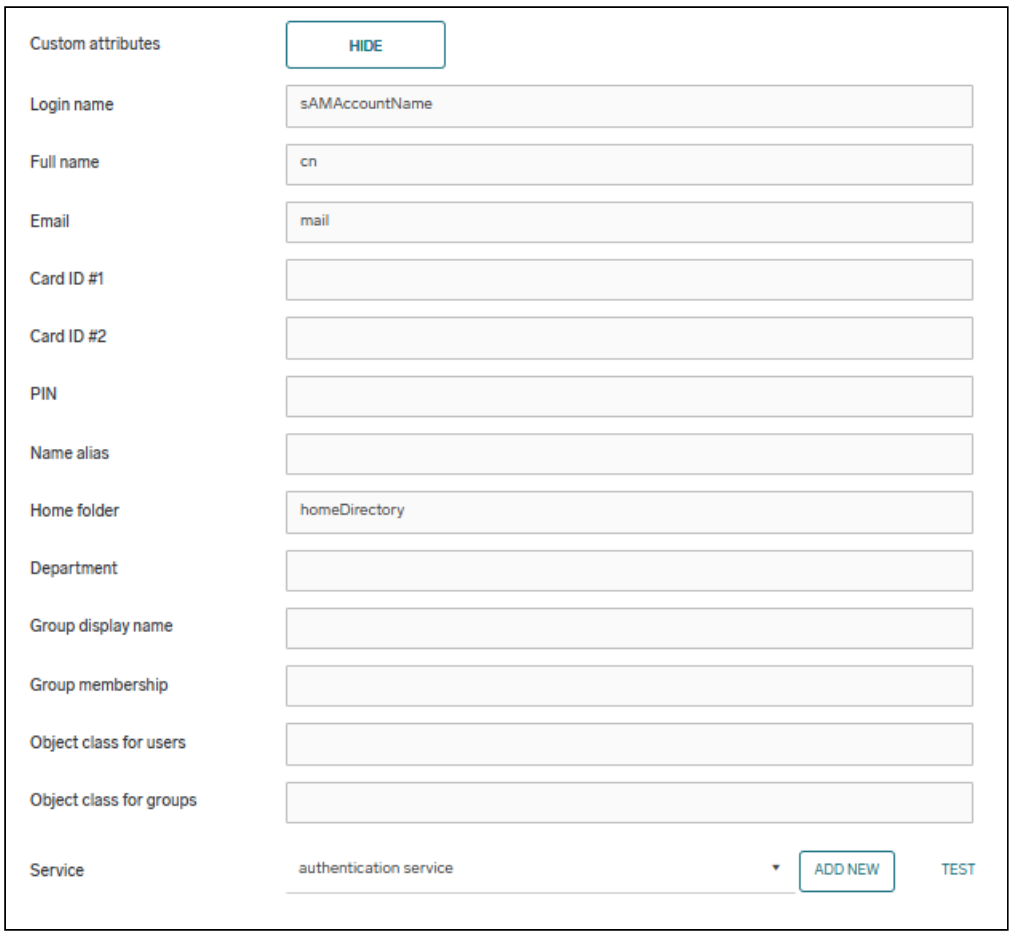
```
    "deparment": "Deparment",
    "expiration": "2592000",
    "externalId": "auth0|0123456789ABCDEF0123456"
    "groups": [
        {
            "dn": "CN=Group1"
        },
        {
            "dn": "CN=Group2"
        }
    ]
}
```

LDAP authentication



- **Name** – An internal name used for identifying the particular authentication provider configuration. Should be prefilled with the selected Type.
- **Domains** – The domain names of the authenticating users. Add here the domain aliases that the users can use to log in. At least one domain in the list should match the domain part of the fully qualified username. If strict domain validation is disabled, SAFEQ Cloud will attempt to authenticate the user with all domains in the list when the username does not contain any domain, in the order defined in the list. If strict domain validation is enabled or the username contains a domain, SAFEQ Cloud will attempt to authenticate only with the domain in the credentials.

  For example, to allow user john.doe@acme.com to log in via this Authentication provider, enter the *acme.com* domain here.
- **Priority** – A number that determines the order in which authentication providers will be called until one succeeds. Higher-priority providers will be called first.
- **Active** – If enabled, this authentication provider will be used for authentication. If disabled, this authentication provider will not be searched.
- **Base DN** – The point in the LDAP where searching will begin. Will apply to both user and group searching, if *Group Base DN* is empty.
- **Group Base DN** – Possible to specify another starting point for LDAP searching for groups. If omitted, the *Base DN* is used for group search.
- **Server name** – The actual address (DNS, hostname or IP) of the LDAP server to which SAFEQ Cloud Authentication Service will connect to search.
- **Port** – Port used for the LDAP service, typically 389 for non-SSL and 636 for SSL.
- **Username** – Username used to connect and search in the LDAP.
- **Password** – Password used to connect and search in the LDAP.
- **OUs or groups** – Choose how to identify groups, for access control management, default is "Groups".
- **Bind type** – Whether to bind with Plain connection, MD5 digest, or Kerberos.
- **Enable SSL** – Whether connection to LDAP should use SSL encryption.
- **Custom attributes** – Expand custom attributes to change the LDAP attributes in which username, card ID's, ShortID's and similar are stored.



When using the *Strict domain validation* feature, make sure to set the **Login attribute** to **userPrincipalName**.

Service – Which Authentication Service will communicate to this LDAP server. If no service is created, it can be added using the Add button.

Note. If you have multiple Active Directory servers, point authentication to the primary domain.

Microsoft Entra authentication

SAFEQ Cloud supports Microsoft Entra ID (formerly Azure AD) authentication for authenticating Microsoft Entra ID users to SAFEQ Cloud.

You can configure Microsoft Entra ID authentication to use either OpenID Connect (OIDC) authentication, service access authentication (implemented via Service Account), or both types simultaneously. Configuring an authorization provider with OIDC and service access can be helpful when you require enhanced security, user convenience, and support for all possible authentication options when authenticating into SAFEQ Cloud (e.g., Web UI, MFD terminal, etc.).

Be aware that OIDC on its own is incompatible with SAML Single sign-on. If you wish to use SAML, enable Service Account Authentication as well.

For the breakdown of the advantages of OIDC and service access authentication methods, refer to the Authentication providers section.

General settings

To add Microsoft Entra ID Authentication provider, perform the following steps:

1. Log in to SAFEQ Cloud Web UI and go to **Users** page and **Authentication providers** tab.
2. Click **Add**.
3. In **Type**, select **Microsoft Entra ID**.
4. Fill in the general settings:
   a. **Name** – An internal name used for identifying the particular authentication provider configuration. Should be prefilled with the selected Type.
   b. **Domains** – The domain names of the authenticating users. Add here the domain aliases that the users can use to log in. At least one domain in the list should match the domain part of the fully qualified username. If strict domain validation is disabled, SAFEQ Cloud will attempt to authenticate the user with all domains in the list when the username does not contain any domain, in the order defined in the list. If strict domain validation is enabled or the username contains a domain, SAFEQ Cloud will attempt to authenticate only with the domain in the credentials.

      For example, to allow user john.doe@acme.com to log in via this Authentication provider, enter the *acme.com* domain here.

      Microsoft Entra ID's limitation is that the domain in the user's email address must match the Microsoft Entra ID tenant domain. Otherwise, SAFEQ Cloud cannot synchronize the email address with the user.

      For example, if your Microsoft Entra ID's tenant domain is *mycompany.com* and there is a user with username *john.doe@mycompany.com* and e-mail *john.doe@privatemail.com*, the *john.doe@privatemail.com* e-mail won't be visible to SAFEQ Cloud.

   c. **Priority** – A number that determines the order in which authentication providers will be called until one succeeds. Higher-priority providers will be tried first.
   d. **Active** – If enabled, the authentication provider will be used for authentication. If disabled, this authentication provider will not be used for authentication. You can use this to disable the Authentication provider temporarily.
5. In the next steps, choose the authentication type or a combination of types.

a. **OIDC Built-in authentication** – The default option suitable for most use cases. We do not recommend disabling it. This is the most convenient option if you don't need any special configuration or don't want to set up your own Microsoft Azure App registration (OIDC client) manually.

b. **OIDC Built-in authentication** together with **Service account authentication** – Choose this option if you have card IDs and/or PINs stored in your authentication provider and you wish the users to be able to log in with cards or PINs at the MFDs.

c. **OIDC Customizable authentication** – Choose this option if you need to configure your own custom Microsoft Azure App registration.

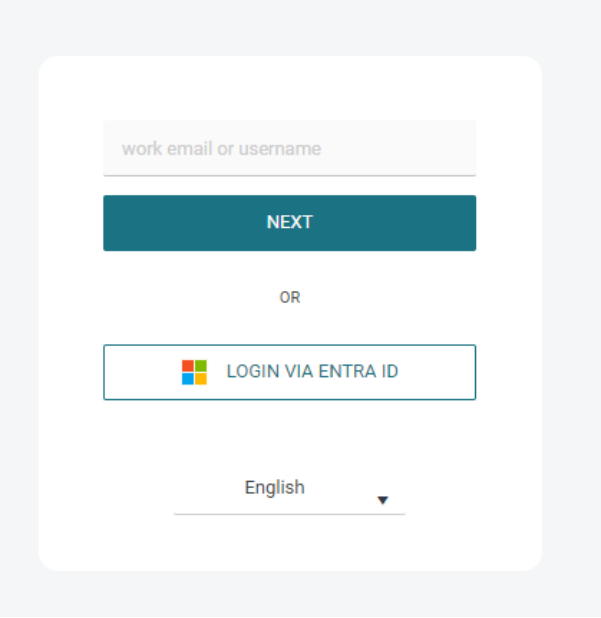
d. Only **Service account authentication** – This is a legacy type of authentication and we do not recommend using it in newly set up Authentication providers.

When the OIDC authentication is enabled (using either **Built-in** or **Customizable** config), you can choose whether to hide a login button for this authentication provider on the Login page via the **Hide on Login page** switch.

OIDC Built-in configuration

When using the built-in OIDC authentication, users will log in via a predefined SAFEQ Cloud Microsoft Azure application (commonly named *SafeQ - Authentication*, with the App ID `c6bddbd5-2151-4fa7-a26a-6b6d573ce604`).

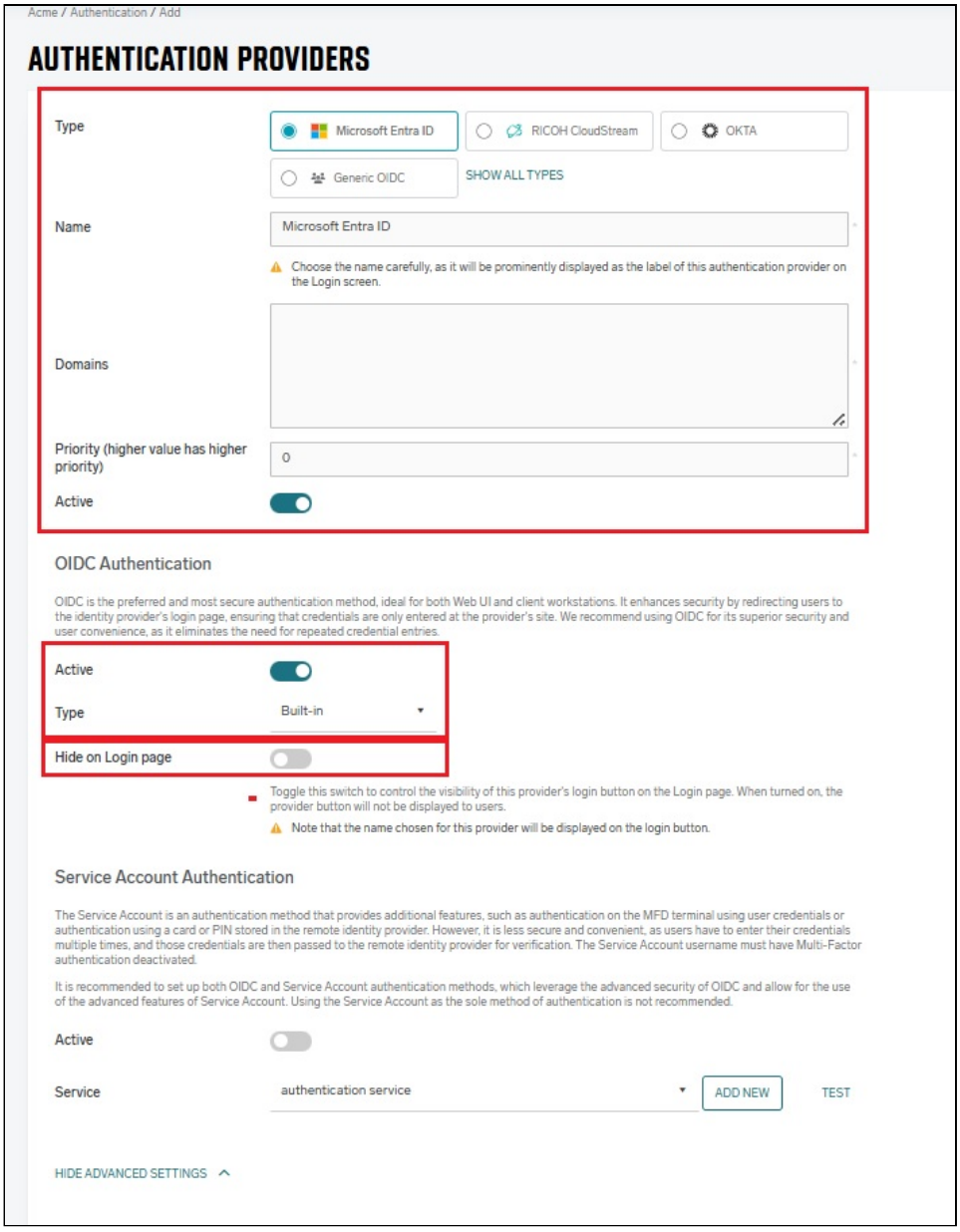
1. Log in to SAFEQ Cloud Web UI and go to **Users** page and **Authentication providers** tab.
2. Click **Add** and fill in the general settings (**Type**, **Name**, **Domains**, **Priority**, and **Active**).
3. **OIDC Authentication** section – Toggle to **Active** if necessary, in **Type** drop-down list, choose **Built-in** and fill in the fields accordingly
   a. **Hide on Login Page - Enable** this option to hide the Microsoft Entra ID button on the SAFEQ Cloud login page. Otherwise the name displayed on the button is taken from the **Name** field. Example:



If the **Hide on Login Page** option is enabled, no "Login via <Provider Name>" button will be displayed on the login screen. To authenticate via such an authentication provider, users need to fill in the username containing a domain matching the authentication provider, which will redirect them to the OIDC authentication flow (the same way as clicking the "Login via <Provider Name>" button.

4. **Service account authentication** section: Enable the **Active** toggle if you wish to use service account together with OIDC. See the *Service account authentication* section of this page.

5. This is an example of the final configuration::



6. Click **Save**.

7. Microsoft Entra ID users can now log in to SAFEQ Cloud.

Every user logged in via this provider will have the **Authenticated Users** group assigned. You can use this group to manage access controls. See Access Control.

When users sign in for the first time, they must consent to the predefined Microsoft Azure application. To prevent prompting each user individually, you can grant tenant-wide admin consent to application in advance.

Note: The predefined Microsoft Azure application will appear in **Enterprise Applications** only after the first consent is granted by any user, or after an administrator approves a user-initiated request.

For more information, see https://learn.microsoft.com/en-us/entra/identity-platform/permissions-consent-overview.

Service account authentication

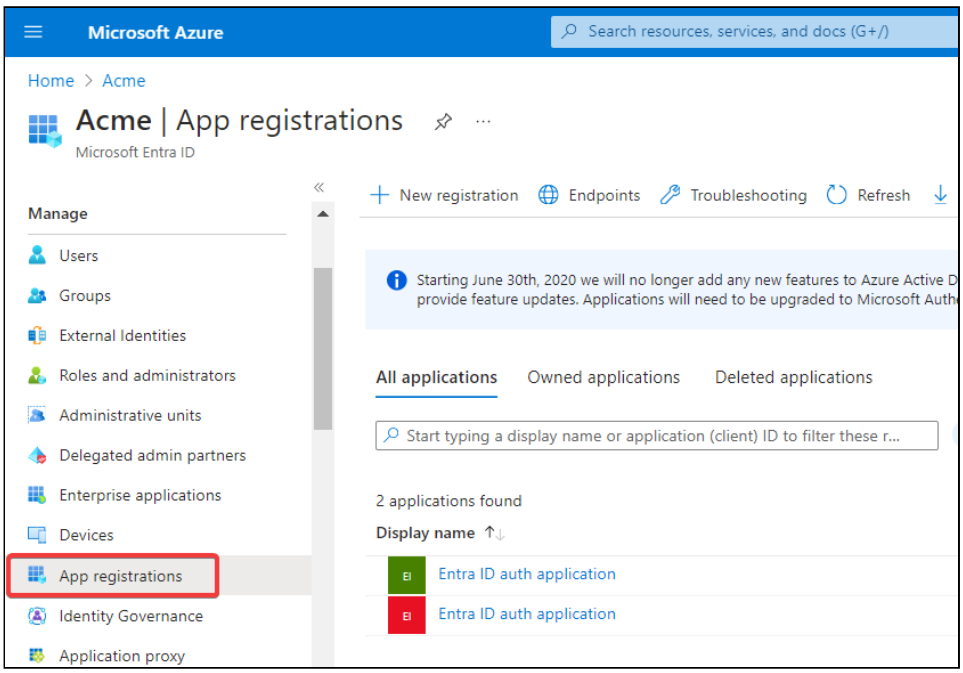
When using the SAFEQ Cloud Microsoft Entra ID Service account authentication without OIDC, multi-factor authentication (MFA) is not supported. If you are using MFA, enable OIDC support for your Microsoft Entra ID authentication provider as explained in the above sections.

This method enables authentication on MFD using data from a remote identity provider (e.g., card, PIN, or credentials). It also allows displaying user department in accounting reports and enables lookup of Microsoft Entra ID users in web UI even before their first interaction with SAFEQ Cloud. Customers who use self-registered cards, API-imported cards, or do not require department reporting typically don't need to activate it.

To configure Microsoft Entra ID authentication using a service account, first, you need to create an App registration in Microsoft Azure. To do that, perform the following steps:

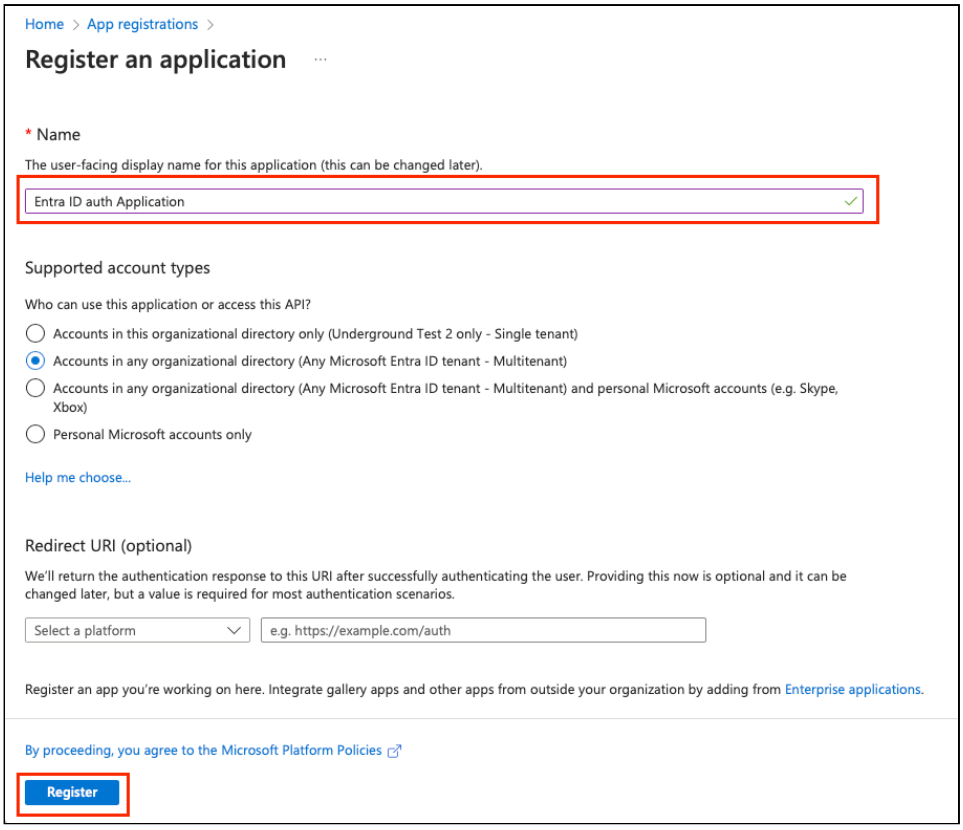
Registering a new Microsoft Azure app

1. Log in to Azure Portal and click **Manage Microsoft Entra ID**.
2. Click **App registrations**.



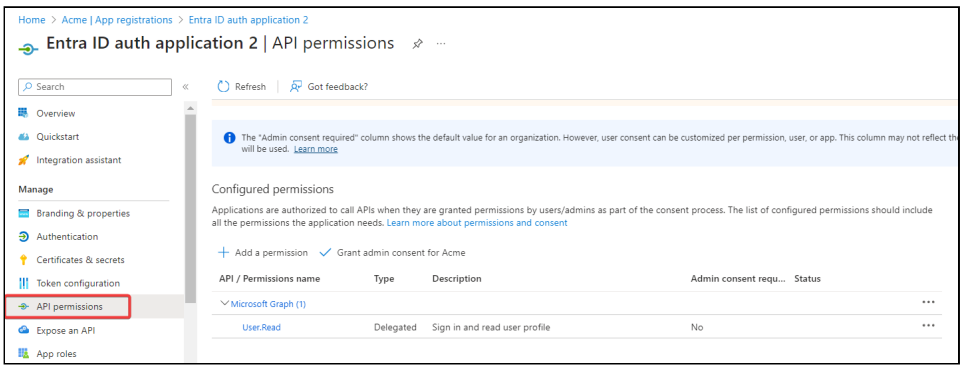
3. Click the **+New registration** button.

4. Enter the name of your new application, select one of the supported account types, and leave the **Redirect URI** field empty.

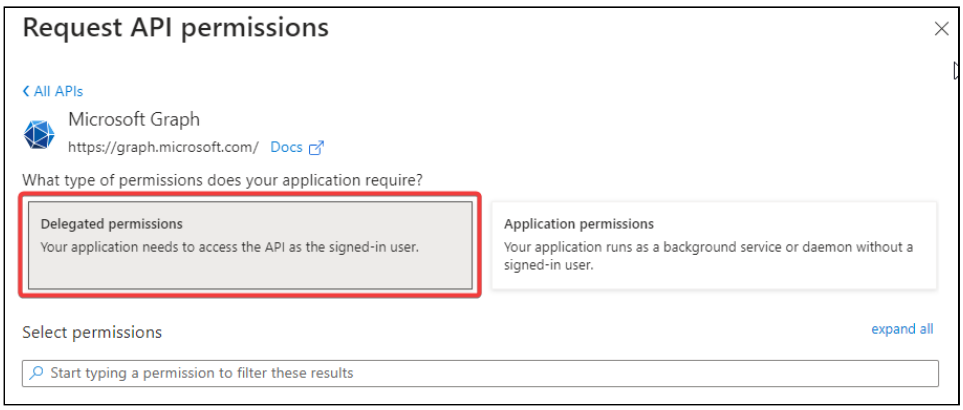


5. Click **Register**.

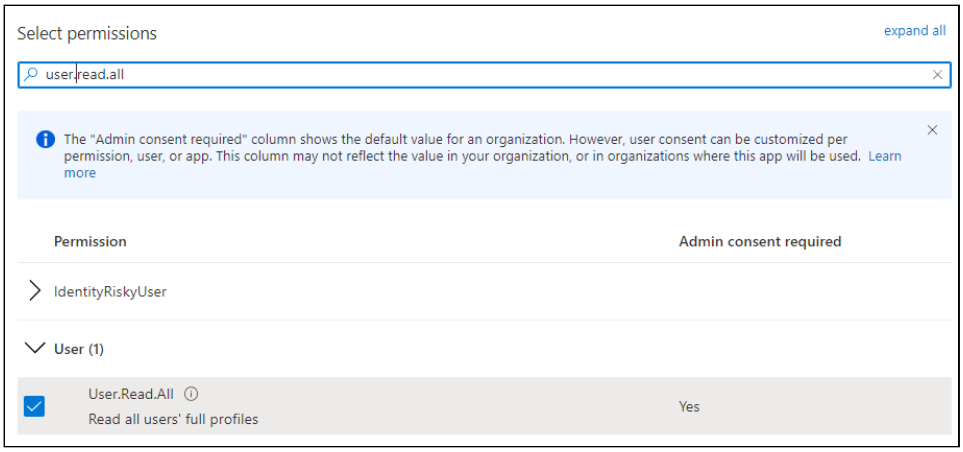
6. Click **API permissions**.



7. Click **Microsoft Graph (1)** and delete the **User.Read** permission.
8. Click **Add a permission**.
9. Select **Microsoft Graph** from **Commonly used Microsoft APIs**.
10. Click **Delegated permissions**.



11. Search for the permissions required, and then click **Add Permissions**.

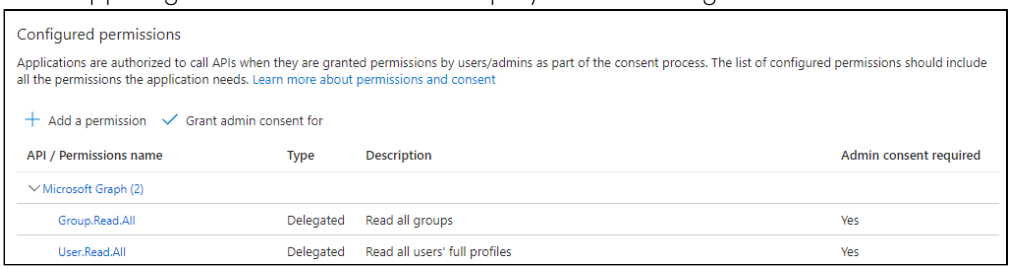


Minimum Permissions Required are:

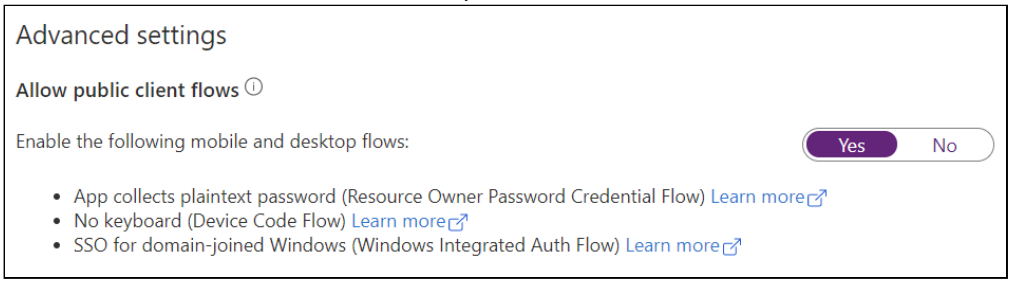
- **Group.Read.All** – Allows the app to list groups and to read their properties and all group memberships on behalf of the signed-in user
- **User.Read.All** – Allows the app to read the full set of profile properties, reports, and managers of other users in your organization on behalf of the signed-in user.

Additional permissions may be required to read custom attributes or similar. Add them based on your specific configuration of Microsoft Entra ID and attribute mapping configured in SAFEQ Cloud.

12. Grant the admin permissions by clicking **Grant admin consent for**, then click **Yes** to approve.
13. Your App Registration should now display the following.



14. Click **Authentication** and Set **Allow public client flows** to **Yes**.



The Service account needs the **Allow public client flow** functionality for fetching information about a particular user or group from Entra ID and for username/password authentication. Namely, the **Username+password** type of login on MFDs, the **Manual login** authentication type in the SAFEQ Cloud Client, and logging in to SAFEQ Cloud Web UI without OIDC. If you wish to use the Service account, the **Allow public client flow** must be enabled

Note that SAFEQ Cloud doesn't store the usernames and passwords, but be aware that they are passed through SAFEQ Cloud to Entra ID for validation. Therefore, they might potentially be intercepted by attackers on the way.

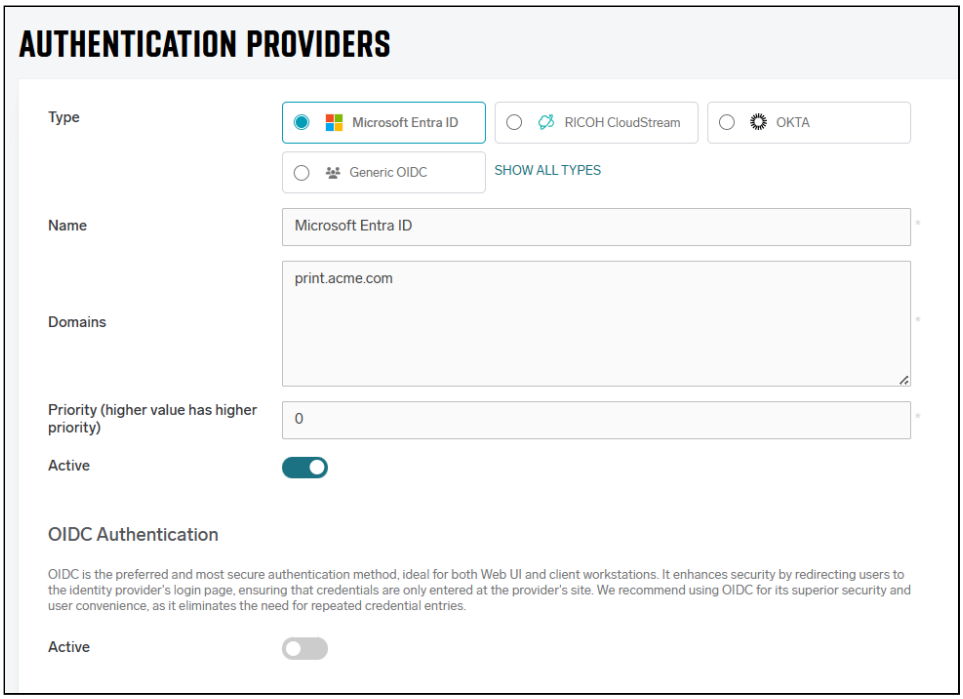
15. Microsoft Entra ID app configuration for Service account authentication is now complete.
16. To allow authentication using PINs and cards stored in Microsoft Entra ID or to display user's department in reports, follow:
Synchronizing user card, PIN or department from Microsoft Entra ID

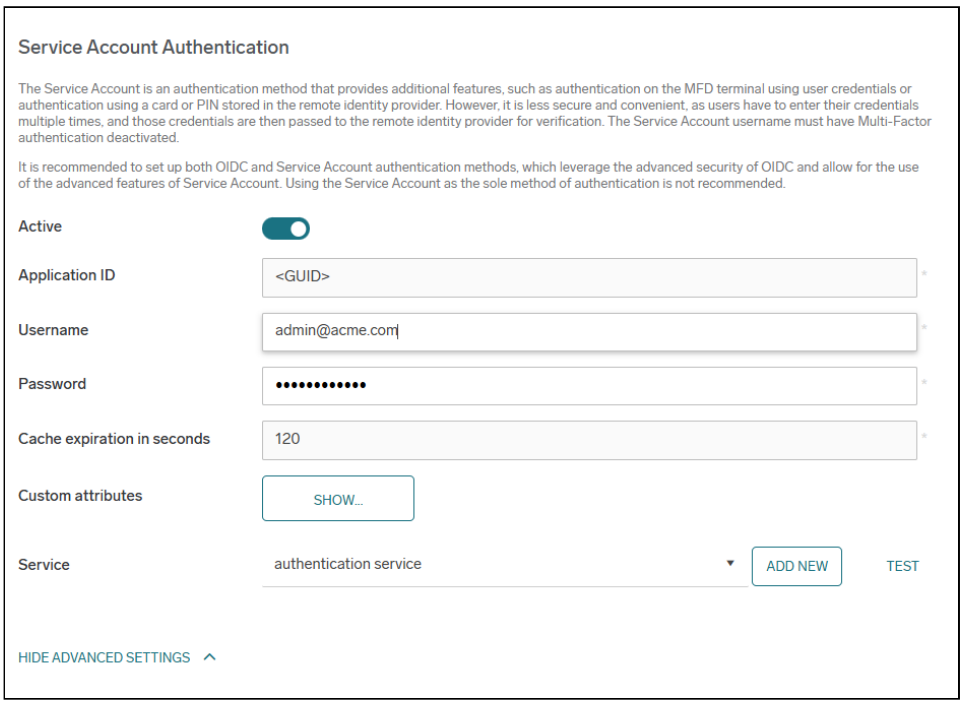
Creating an Authentication provider in SAFEQ Cloud

This Authentication provider will use the app registration which you have just created.

1. Log in to SAFEQ Cloud Web UI and go to **Users** page and **Authentication providers** tab.
2. Click **Add** and fill in the general settings (**Type**, **Name**, **Domains**, **Priority**, and **Active**).

3. **Service Account Authentication** – this section applies to service account settings
   a. **Active** – Activate the switch to enable the service account authentication.
   b. **Application ID** – The ID of your registered Azure App.
   c. **User name** – Name of the user to be used for the Microsoft Graph API access.
   d. **Password** – Password for the above-mentioned user.
   e. **Cache expiration in seconds** – The time the authentication information is kept in the internal cache to reduce the calls from SAFEQ Cloud to Microsoft Entra ID. We recommend at least 2 minutes.
   f. **Custom attributes** – Expand custom attributes to change the Microsoft Entra ID attributes in which usernames, card IDs, ShortIDs, and others are stored.
   g. **Service** – Select which Authentication Service will communicate to this Microsoft Entra ID server. In case no service is already created, you can add it by clicking **Add**. If the primary server has only one authentication service, or if there's only one authentication service in general, it is pre-selected by default.





h. Click **Save**.

4. The Microsoft Entra ID users can now log in to SAFEQ Cloud.

> Every user logged in via this provider will have the **Authenticated Users** group assigned. You can use this group to manage access controls. See Access Control.

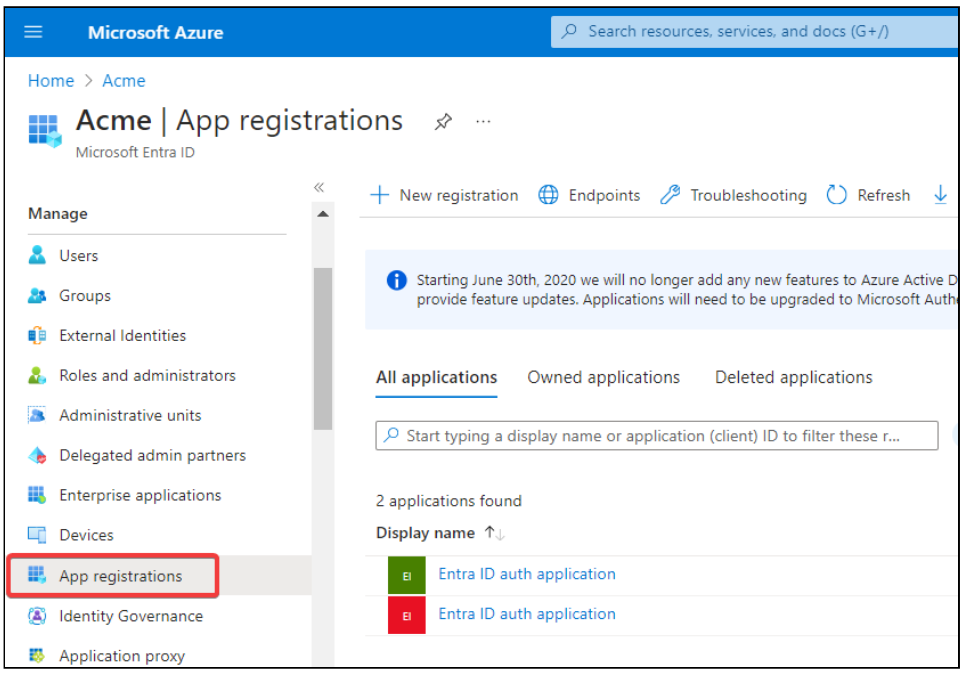
> Card ID and Short ID synchronized through Entra ID are not going to be visible in the user profile in SAFEQ Cloud Web UI. This does not prevent users from using these authentication methods.

OIDC Customizable configuration

If you want to configure custom Microsoft Entra ID OIDC authentication, you must first configure Microsoft Azure App registration and then use it for the authentication provider in SAFEQ Cloud. To create a new Microsoft Azure App registration, perform the following steps:

Registering a new Microsoft Azure app

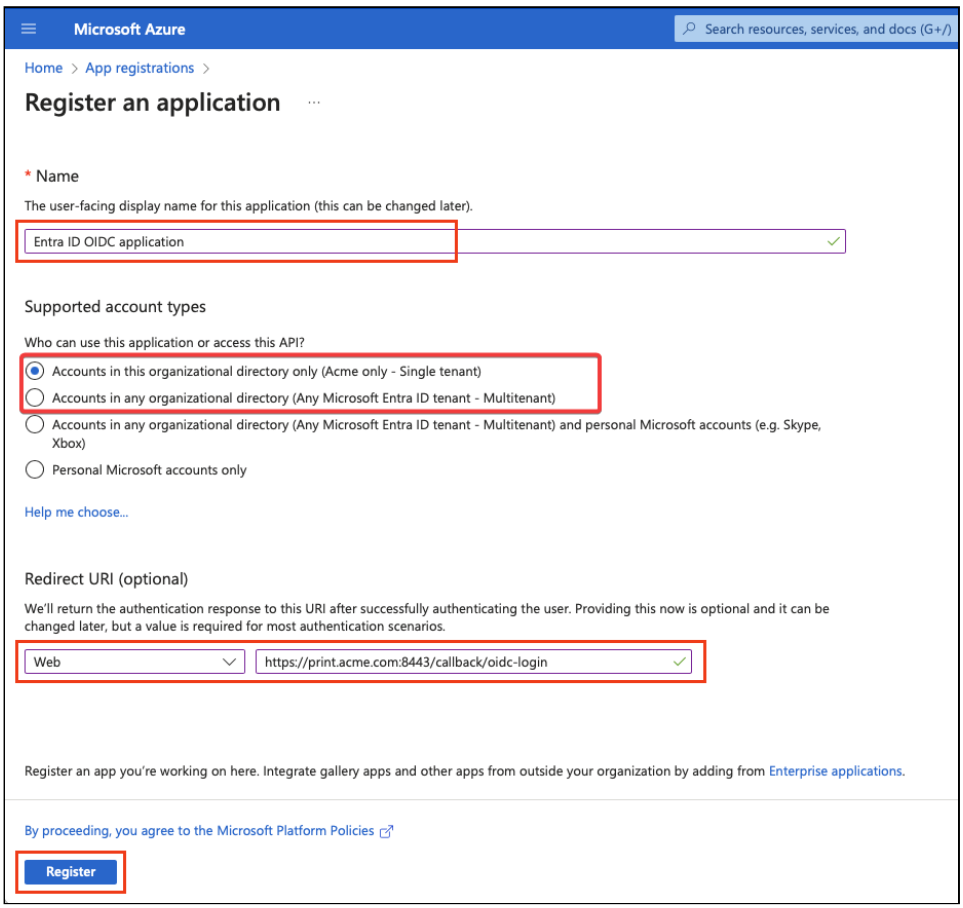
1. Log in to Azure Portal and click **Manage Microsoft Entra ID**.
2. Click **App registrations**.



3. Click the **+New registration** button.

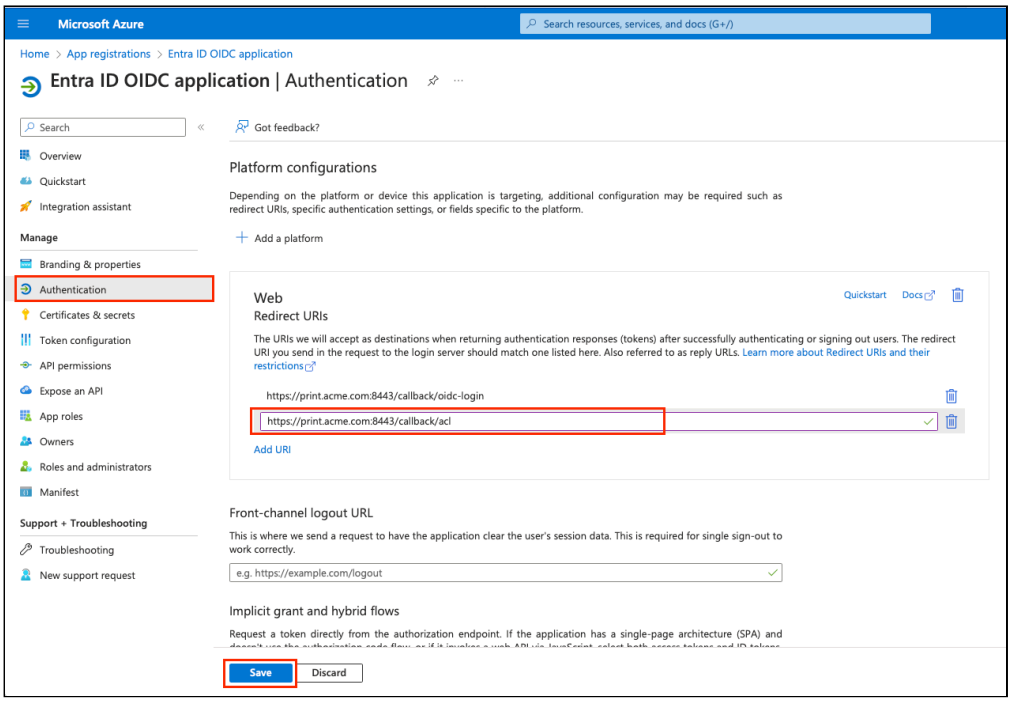
4. Enter your new application's name, choose **Single tenant (Accounts in this organizational directory only)** or **Multitenant (Accounts in any organizational directory)** account type. However, we recommend **Single tenant**. Fill in the **Redirect URI** field. The **Redirect URI** pattern is: *https://<account-domain>:<port>/callback/oidc-login*

   - The port for callback URIs is, by default, 8443. Example: *https://print.acme.com:8443/callback/oidc-login*
   - In environments with reverse proxy infrastructure, do not specify the port number in the URL, meaning the default HTTPS port 443 will be used. Example: *https://print.acme.com/callback/oidc-login*
   - The *account domain* is your domain defined in SAFEQ Cloud. It must be the same as the **Callback domain** selected in the Authentication Provider form, which you will fill in later.



5. Go to **Authentication**. In the **Web** section, click **Add URI** and fill the URI with a pattern: *https://<account-domain>:<port>/callback/acl*

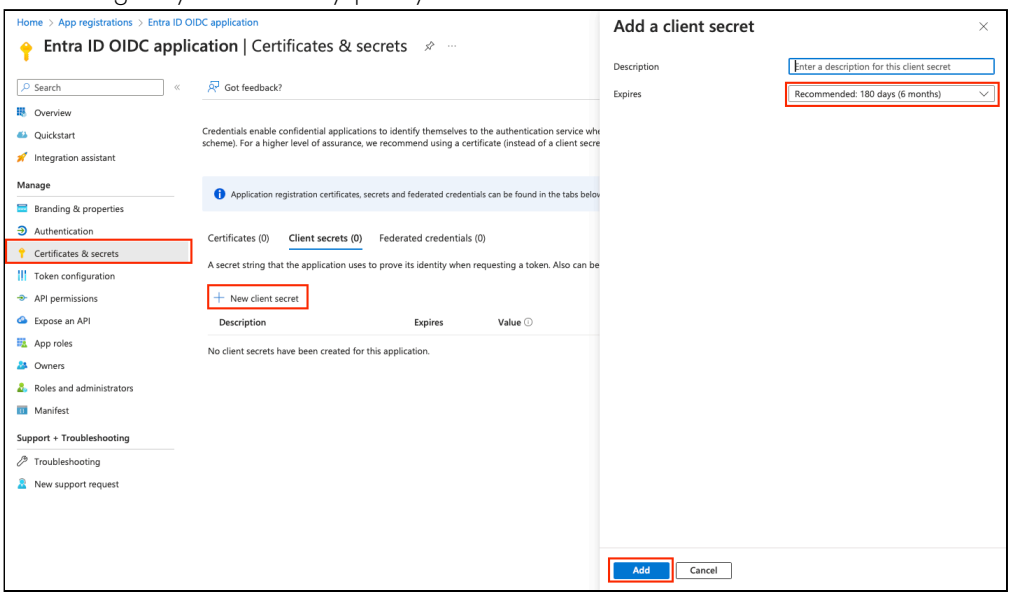
- The port for callback URIs is, by default, 8443. Example: *https://print.acme.com:8443/callback/acl*
- In environments with reverse proxy infrastructure, do not specify the port number in the URL, meaning the default HTTPS port 443 will be used. Example: *https://print.acme.com/callback/acl*
- The domain is your domain defined in SAFEQ Cloud. It must be the same as the domain selected in the Authentication form, which you will fill out later.
- Keep the **Front-channel logout URL** empty.



6. Click **Save**.

> In total, there should be these callback domains defined:
>
> - *https://<domain>:<port>/callback/oidc-login*. For environments with reverse proxy: *https://<domain>/callback/oidc-login*
> - *https://<domain>:<port>/callback/acl*. For environments with reverse proxy *https://<domain>/callback/acl*

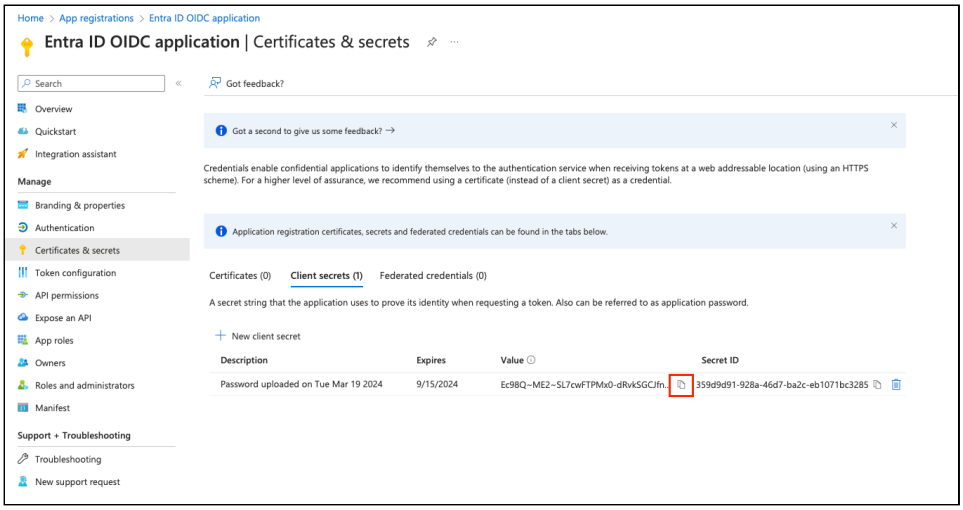
7. Go to **Certificates & secrets** and click **+ New client secret**. Optionally, set the **Expires** value according to your security policy. Click **Add**.



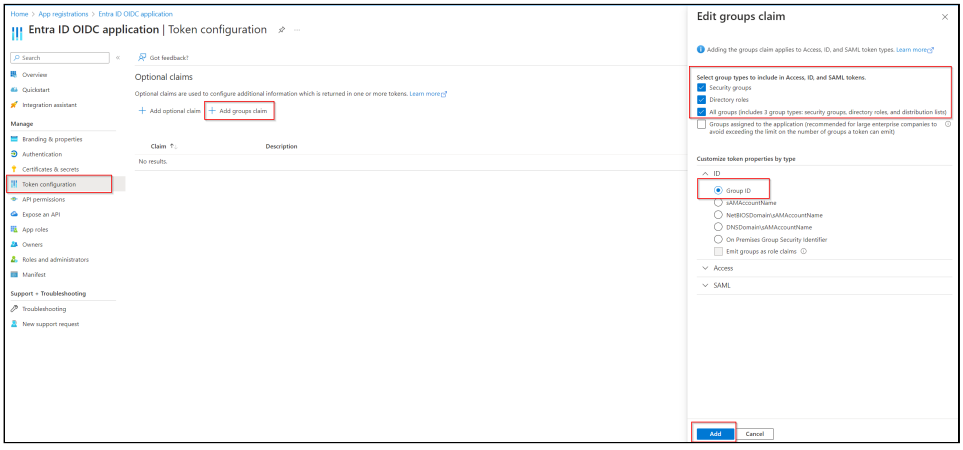
8. Copy the secret value and save it securely. You will need it later for the SAFEQ Cloud authentication provider configuration.

> ⚠ You can only see the secret value during creation time for security reasons. Once you leave the screen, the value will not be shown again.

> ✓ Because the **Client secret** has limited validity, remember to create a new one before it expires and replace the old one either in SAFEQ Cloud Web UI or using SAFEQ Cloud API. See the API documentation > API Functions > section *Authentication provider*.



9. Go to **Token configuration**, click **+ Add groups claim**, and define the groups that will be part of the users' ID Token. This will be used later in the Access Control configuration in SAFEQ Cloud.

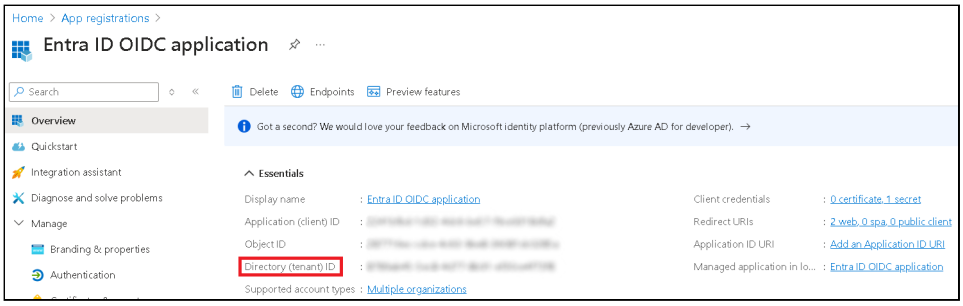


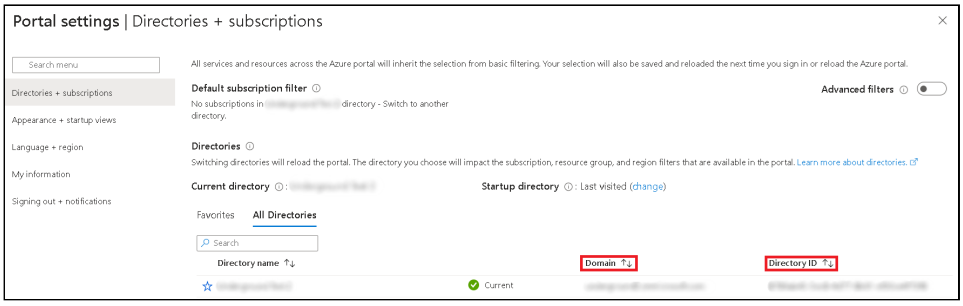
10. The result will look like this. Microsoft Entra ID app configuration for OIDC authentication is now finished.

Next, you must create the Authentication provider in SAFEQ Cloud, which will use the app registration you just created.

Creating an Authentication provider in SAFEQ Cloud

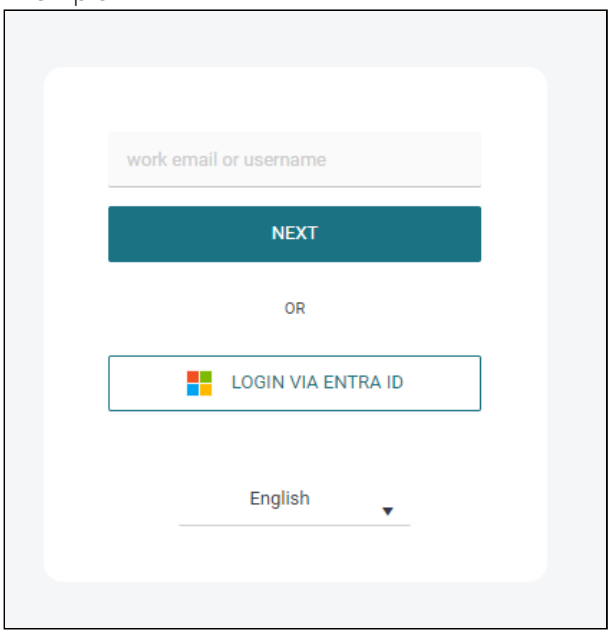
1. Log in to SAFEQ Cloud Web UI and go to **Users** page and **Authentication providers** tab.
2. Click **Add** and fill in the general settings (**Type**, **Name**, **Domains**, **Priority**, and **Active**).
3. **OIDC Authentication** section – Toggle to **Active** if necessary, in **Type** drop-down list, choose **Customizable** and fill in the fields accordingly:
   a. **Client ID** – The ID of the registered Azure App you created in previous steps.
   b. **Client secret** – The secret value you created for the registered Azure App in previous steps.
   c. **Entra directory (tenant) ID or domain** – If you selected the **Multitenant account** type during the Entra App registration, keep this field blank. Fill it only if you selected the **Single tenant** account type. You can find the directory (tenant) ID in the **Overview** section of the registered Entra App or in the **Directories + subscriptions** menu in **Portal settings**.





   d. **Callback domain for custom application** – Select from the list of available domains the one that you defined in Azure App registration as **Redirect URI** in previous steps, e.g. *print.acme.com* .
   e. **Custom token claim names** – Click **Show** to change the mapping between the ID token and Microsoft Entra ID user attributes, such as **preferred_username**, **name**, **email**, and **groups**.
   f. **Hide on Login Page** – Enable this option to hide the Microsoft Entra ID button on the SAFEQ Cloud login page. Otherwise the name displayed on the button is taken from the **Name** field.

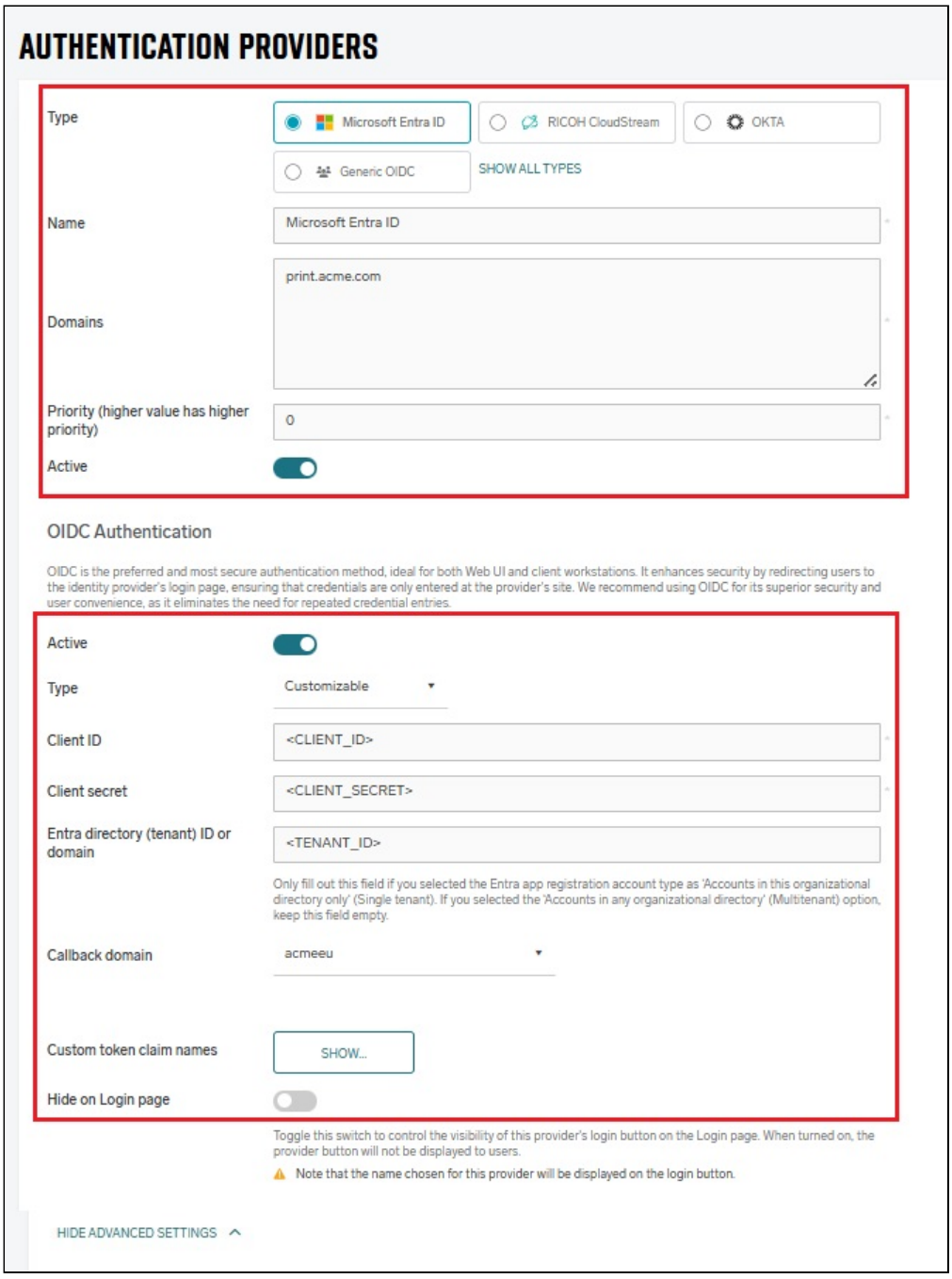
Example:



If the **Hide on Login Page** option is enabled, no "Login via <Provider Name>" button will be displayed on the login screen. To authenticate via such an authentication provider, users need to fill in the username containing a domain matching the authentication provider, which will redirect them to the OIDC authentication flow (the same way as clicking the "Login via <Provider Name>" button.

4. **Service account Authentication** section: Disable the Active toggle if you do not want to use a service account as well.

5. Click **Save**.



6. The Microsoft Entra ID users can now log in to SAFEQ Cloud.

> Every user logged in via this provider will have the **Authenticated Users** group assigned. You can use this group to manage access controls. See Access Control.

When users log in for the first time, they must consent to the SAFEQ Cloud Microsoft Azure application. To prevent this confirmation for each user, you may grant tenant-wide admin consent for the predefined SAFEQ Cloud Microsoft Azure application. For more information, see https://learn.microsoft.com/en-us/entra/identity-platform/permissions-consent-overview.

Synchronizing user card, PIN or department from Microsoft Entra ID

Microsoft Entra ID stores various user information in attributes, such as userPrincipalName (john.doe@sample.com), displayName (John Doe), department (Laboratory), customattributecard (123456789). SAFEQ Cloud can be configured to read them to enhance user experience.

This article demonstrates how to utilize user's department from Microsoft Entra ID for reporting purposes.

The similar approach can be taken to allow usage of cards stored in Microsoft Entra ID for authentication on MFD.

Card and Short ID synchronized through Microsoft Entra ID is not going to be visible on web UI, however users can still use it for authentication without any issue.

Microsoft Entra ID provides so called Directory *Extension,* a custom attribute created by administrator or migrated from on-prem AD. *Directory Extension* has a unique naming convention *extension_<appID>_<extensionProperty-name>*. To ensure SAFEQ Cloud utilizes the value from the Directory Extension, make sure to follow its naming convention when verifying attribute presence via Graph Explorer and when configuring SAFEQ Cloud. Typically *<appID>* is ID of Microsoft Entra ID application used to create the extension, *<extensionProperty-name>* is the custom name of the extension. For details refer to:
https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/custom-attribute-mapping
https://learn.microsoft.com/en-us/azure/active-directory-b2c/user-flow-custom-attributes?pivots=b2c-user-flow

Microsoft Entra ID provides custom attribute *onPremisesExtensionAttributes* with sub-parameters *extensionAttribute1 - extensionAttribute15* (see Microsoft documentation). To ensure SAFEQ Cloud utilizes values from these attributes, set the custom attribute in SAFEQ Cloud to *extensionAttribute1* (or *extensionAttribute2, extensionAttribute3* ...).

You can query the presence of these attributes via Graph Explorer with the following GET request:
https://graph.microsoft.com/v1.0/me?$select=userPrincipalName,onPremisesExtensionAttributes

To check that GraphAPI finds a user with *extensionAttribute1* set to *card123*, use this GET request:
https://graph.microsoft.com/v1.0/users?

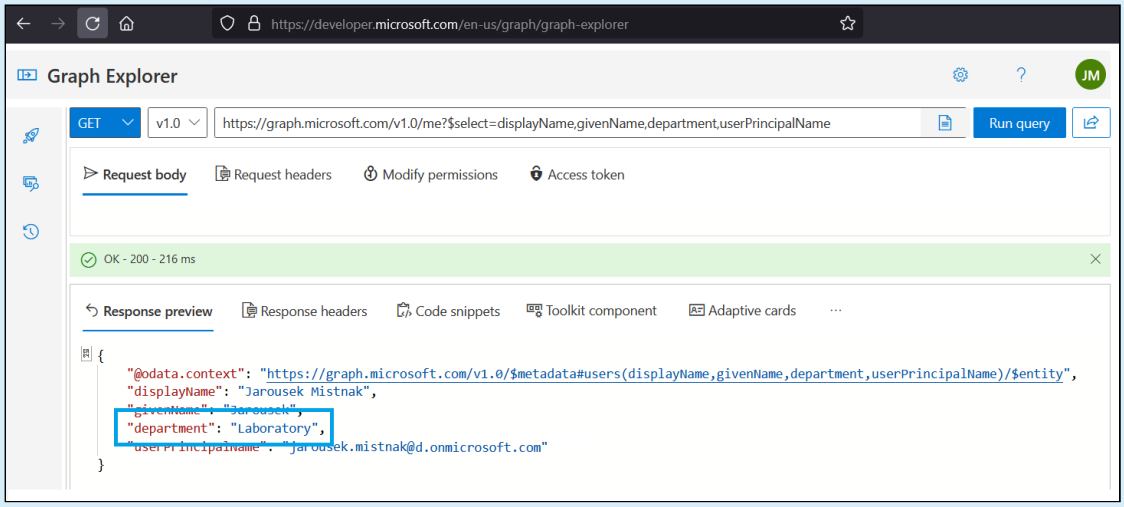
$select=userPrincipalName,onPremisesExtensionAttributes&$count=true&$filter=accountEnabled eq true and ((onPremisesExtensionAttributes/extensionAttribute1 eq 'card123'))
Additionally the header ConsistencyLevel = eventual must be set.

Steps to take:

1. Make sure that "department" is set in Microsoft Entra ID
   - fill in user's department
     - details at https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-user-profile-info
   - verify the attribute exists and has the right value
     - details at https://learn.microsoft.com/en-gb/graph/api/resources/user?view=graph-rest-1

     Example

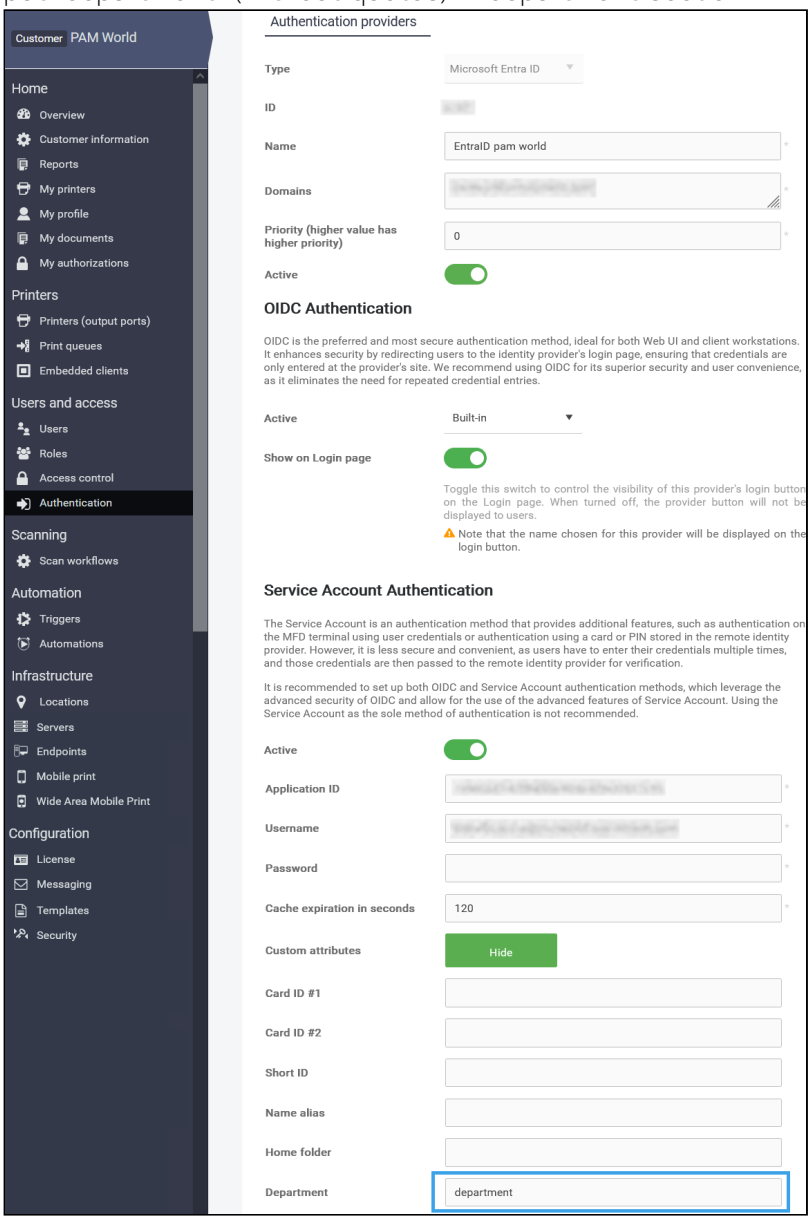
     Go to https://developer.microsoft.com/en-us/graph/graph-explorer
     Authenticate as end user that has "department" filled in
     Run query: https://graph.microsoft.com/v1.0/me?$select=displayName,givenName,department,userPrincipalName



2. Set up authentication provider with enabled "Service Account Authentication"
   - full guide here:
     - Microsoft Entra authentication
   - in brief:
     - create new app in Microsoft Entra ID
     - create new user in Microsoft Entra ID
       - *note: no special roles required, user department will be obtained through permission scope of the new Microsoft Entra ID application*
     - verify that new user can log in to https://portal.azure.com
       - *note: typically a first time password change is required, inability to log in would prevent SAFEQ Cloud from using the account*
     - create "Microsoft Entra ID" provider in SAFEQ Cloud

- enable OIDC authentication Built-in (optional but advised)
- enable "Service Account Authentication and use details of your new app and new user

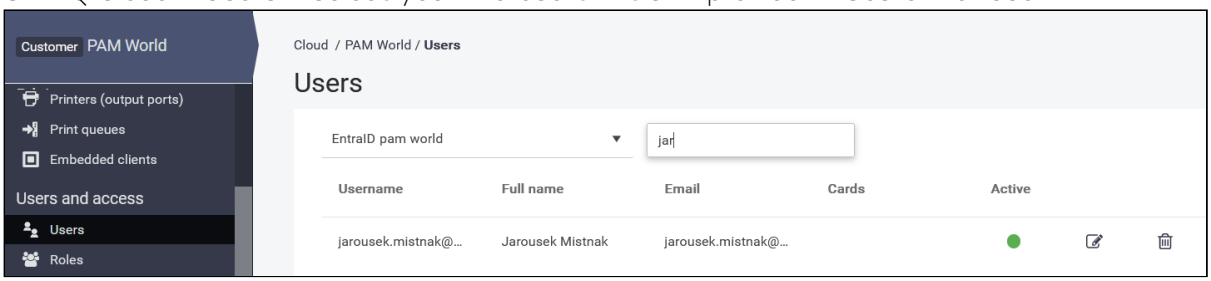
- click "Show" next to "Custom attributes" inside the provider
- put "department" (without quotes) in department section

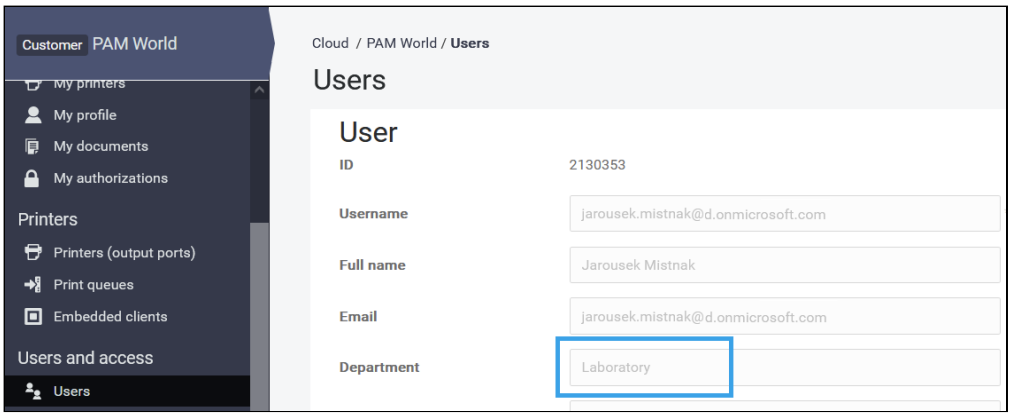


3. Wait for users to authenticate through this provider
   - authentication triggers refresh of user information, user may authenticate e.g. via web or PC client

4. Verify that department is visible in user details

- SAFEQ Cloud > Users > select your Microsoft Entra ID provider > Search for user





5. From this moment jobs performed by this user will have department filled in and visible in reports.

OKTA Authentication

SAFEQ Cloud supports integration with OKTA identity management service for authenticating users, including multi-factor authentication (MFA). Additionally, SAFEQ Cloud supports OKTA's LDAP interface service, see OKTA authentication via LDAP.

Limitations:

- Only OKTA Push MFA is supported, in combination with Okta Verify mobile app

You can configure OKTA authentication to use either OpenID Connect (OIDC) authentication or Service account authentication (using native OKTA APIs), or both types at the same time. This combined type supports MFA.

- With OIDC Authentication users will enter their credentials at OKTA login page where they will be authorized and redirected back to the SAFEQ Cloud. This type does not allow fetching additional user properties, like card IDs or PINs.
- With configured Service account authentication, users will use their OKTA username/password to authenticate into SAFEQ Cloud using their OKTA credentials. This type provides access to all user properties.

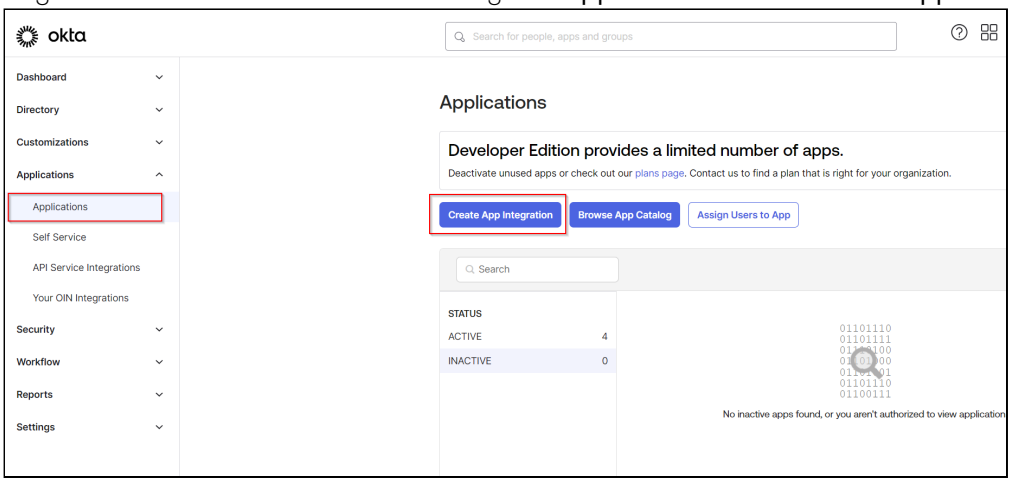
Configuring an authorization provider with both OIDC and service account can be useful in situations where you require enhanced security and user convenience in logging into SAFEQ Cloud, as well as allowing users to log in at the MFDs with cards or PINs.

Be aware that OIDC on its own is incompatible with SAML Single sign-on. If you wish to use SAML, enable Service Account Authentication as well.

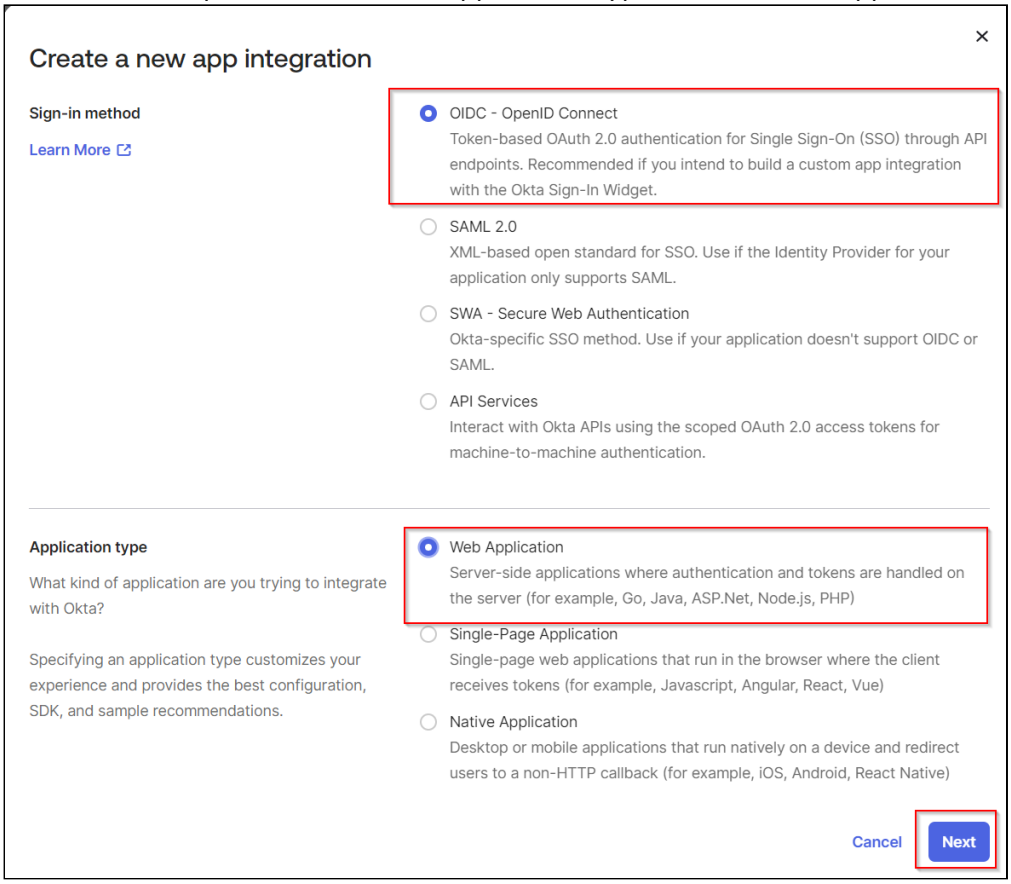
OIDC Authentication

To use OKTA OIDC authentication, you must first create OKTA application and then assign it to SAFEQ Cloud authentication provider. Perform the following steps:

1. Log in to OKTA administration UI and go to **Applications**. Click **Create App Integration**.

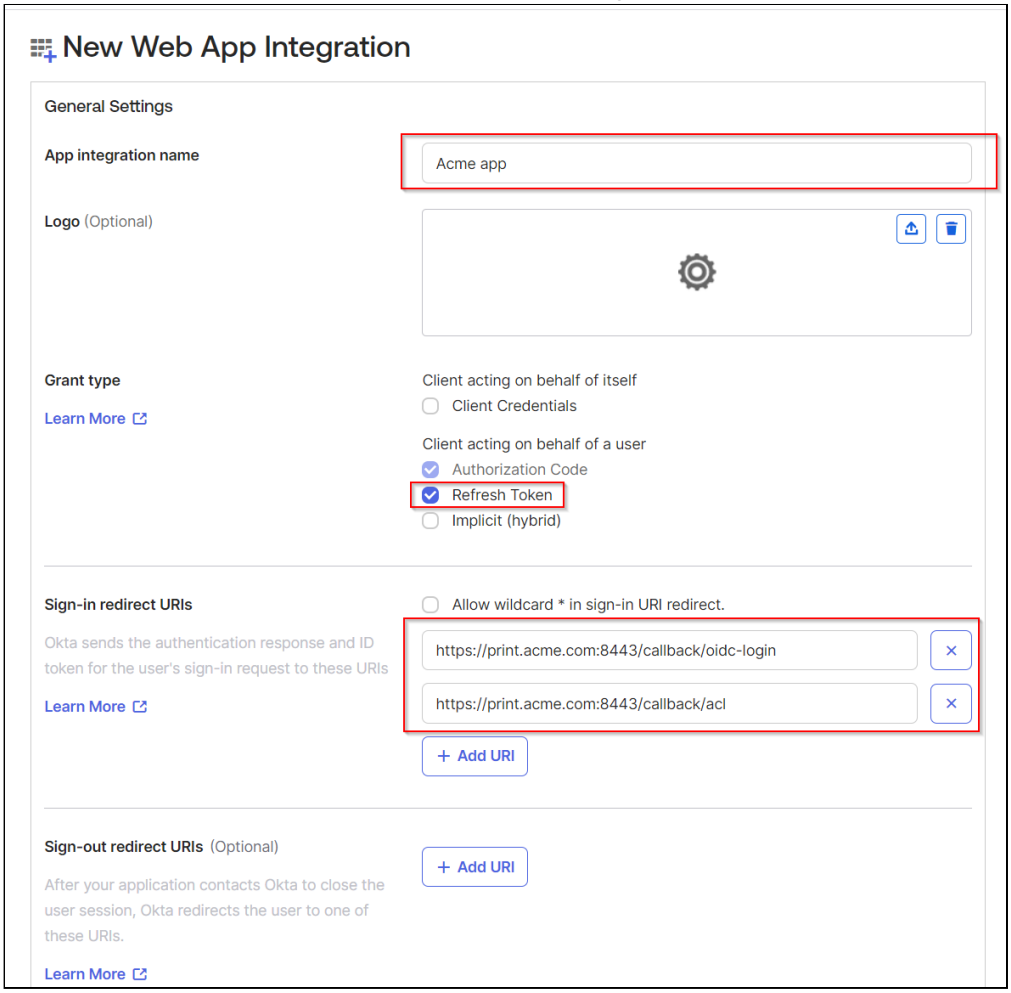


2. Select **OIDC - OpenID Connect**. In **Application type**, choose **Web Application**. Click **Next**.

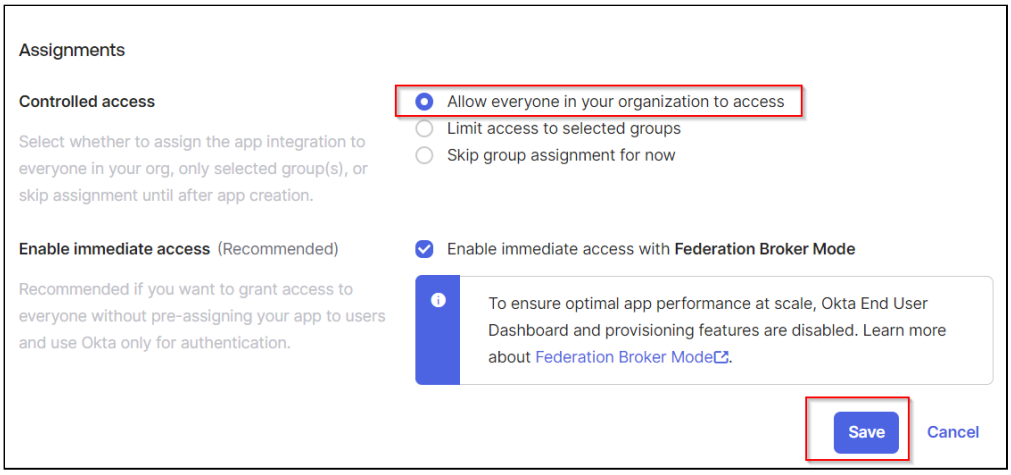


3. Enter the name of your new application. In **Grant type**, select **Refresh Token** (apart from **Authorization Code** which is selected by default). In **Sign-in redirect URIs**, add two URIs:
   - *https://<domain>:<port>/callback/oidc-login*
   - *https://<domain>:<port>/callback/acl*

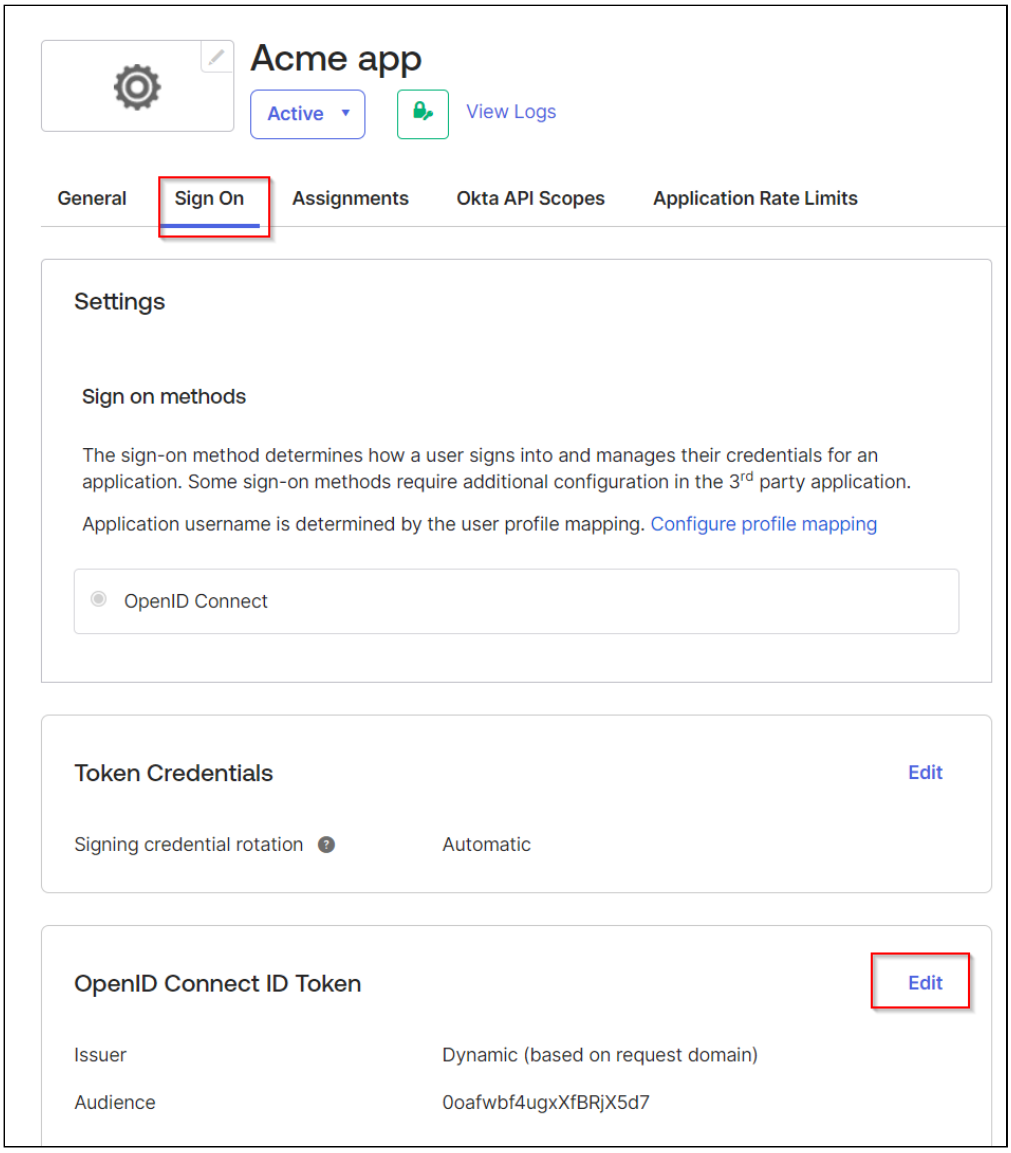
- The **domain** is your domain defined in SAFEQ Cloud. It must be the same as the domain selected in Authentication that you will fill in later.
- The **port** for callback URIs is by default 8443. Example: *https://print.acme.com:8443/callback/oidc-login*. In environments with reverse proxy, do not specify the port number in the URI. Example: *https://print.acme.com/callback/oidc-login.*



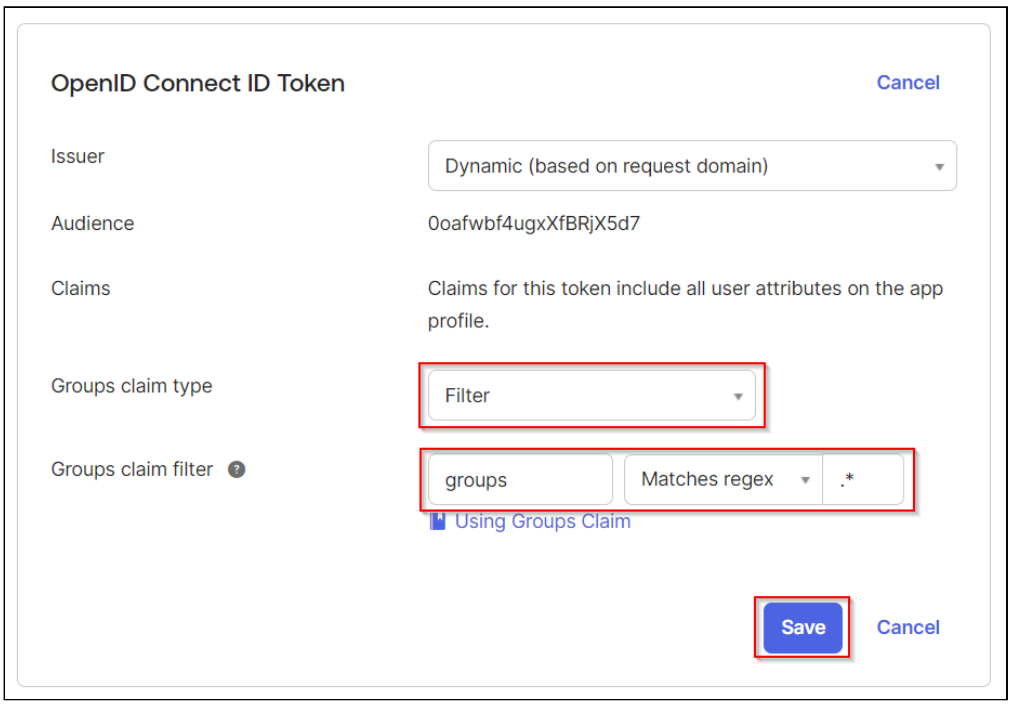
4. On the same page, in **Assignments > Controlled access,** select an option that suits your company policy the most. The default is **Allow everyone in your organization to access.** Click **Save**.



5. Your new application is now created. Navigate to **Sign on** tab go to the **OpenID Connect Token** section and click **Edit**.

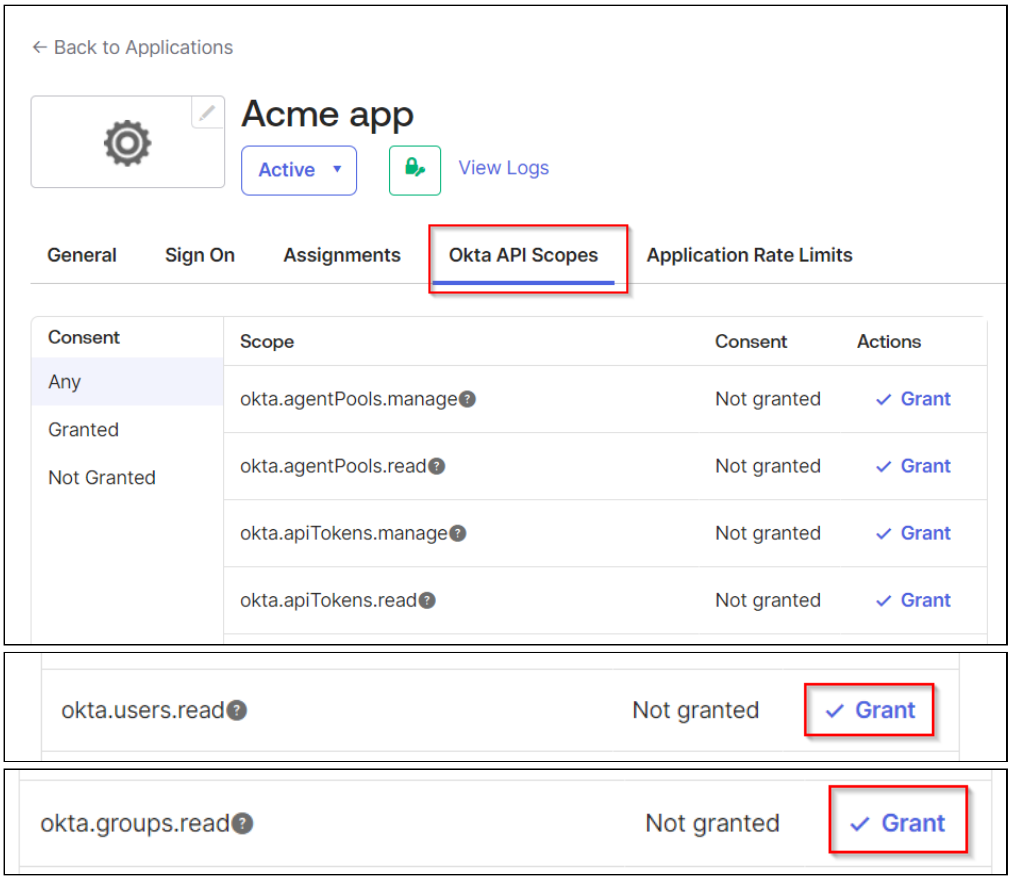


6. In **Groups claim type**, select **Filter**. In **Groups claim filter**, fill in "groups" and "Matches regex" and ".*" Click **Save**.

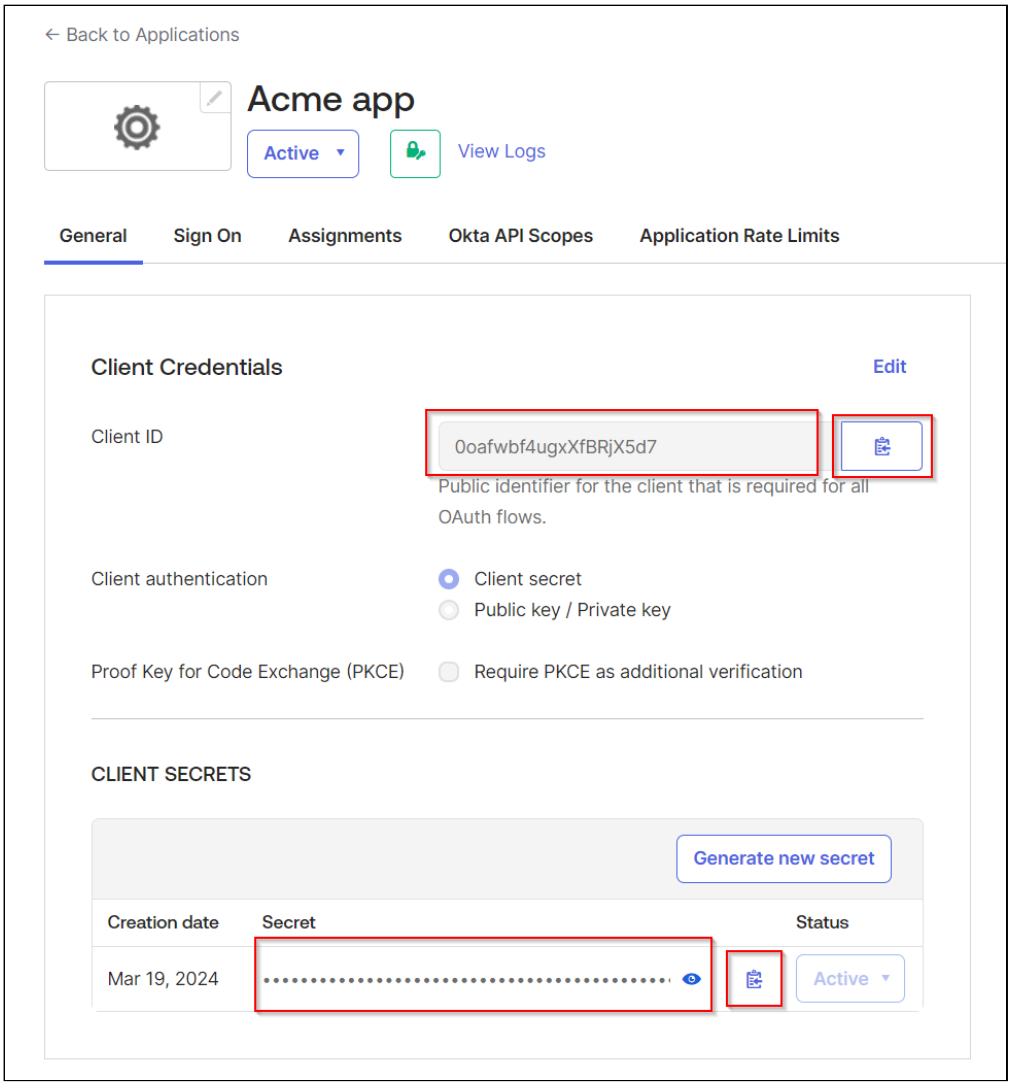


Filter regular expression has to be exactly: .* (dot star) in order to fetch all groups.

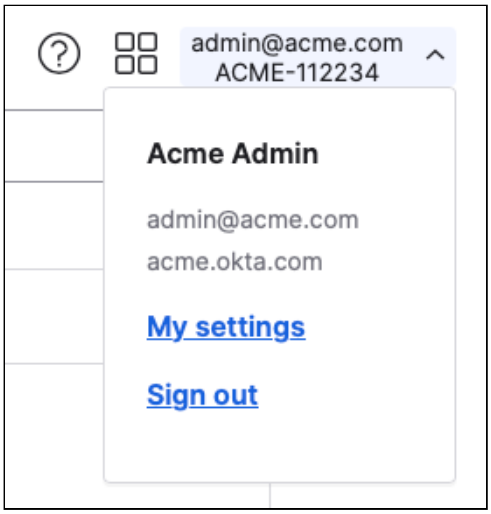
7. Navigate to **Okta API Scopes** tab. Find the **okta.users.read** and **okta.groups.read** consents. Click **Grant**.



8. Navigate to the **General** tab, and copy the **Client ID** and **Client secret** values. You will need them later on.



9. Save the value of your OKTA domain name. You can find it in the top right corner of the OKTA administration UI.



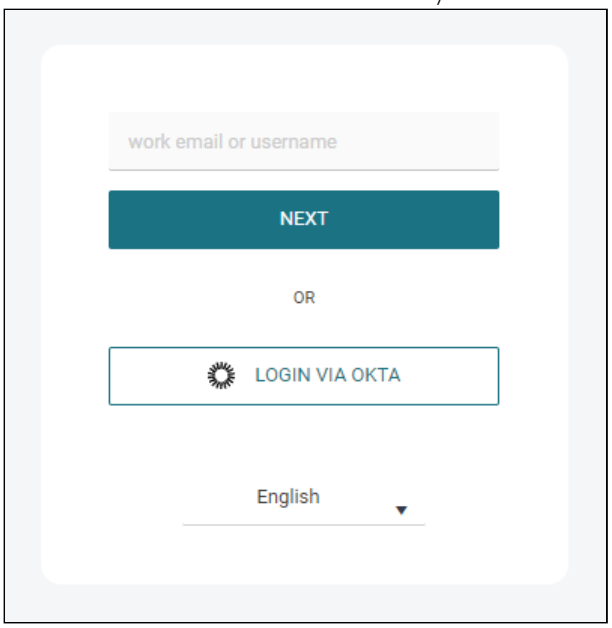
10. This concludes the OKTA application configuration for OIDC authentication.

11. Log in to SAFEQ Cloud Web UI and go to **Users** page and **Authentication providers** tab.
12. Click **Add** and enter the following details:
    a. **Type** – Select **OKTA**.
    b. **Name** – An internal name used for identifying the particular authentication provider configuration. Should be prefilled with the selected Type.
    c. **Domains** – The domain names of the authenticating users. If you have domain aliases that the users can use to log in, add them to this field. At least one domain in the list should match the domain part of the fully qualified user name passed for authentication. If strict domain validation is disabled, SAFEQ Cloud will attempt to authenticate the user with all domains in the list regardless of the domain entered in the credentials, in the order defined in the list. If strict domain validation is enabled, SAFEQ Cloud will attempt to authenticate only with the domain in the credentials. For example, if the domain name of the OKTA authentication provider is *okta.domain.com*, then the user added in Access Control should be *user@okta.domain.com*.

    > Specifying the correct domain name is especially important if using the Strict domain validation feature. Otherwise, it is not possible to detect to which domain a user belongs.

    d. **Priority** – A number that determines the order in which authentication providers will be called until one succeeds. Higher-priority providers will be called first.
    e. **Active** – If enabled, the authentication provider will be used for authentication. If disabled, this authentication provider will not be searched.
    f. **OKTA endpoint address** – The address of the OKTA server for which you created the OKTA application. For example, *acme.okta.com*.
    g. **OIDC Authentication** section - enable **Active** toggle and select **Type Customizable** and fill in the fields accordingly:
        1. **Client ID** – The ID of your application created in OKTA.
        2. **Client secret** – The Secret value for your application created in OKTA.
        3. **Callback domain for custom application** – Select from the list of available domains the one that you defined in OKTA administration UI as **Sign-in redirect URIs**. In the above example, it was *print.acme.com*.
        4. **Custom token claim name** – This allows you to remap Username, Full name, Email, Groups and External ID. Note that all these custom claims need to be defined in the ID token in the OKTA OIDC application.

5. **Hide on Login page** – Keep this disabled to show OKTA button on the login page. The name on the button is the name you entered in the **Name** field.



If the **Hide on Login Page** option is enabled, the username's domain part is still utilized to search for a domain among the configured authorization providers. If a domain is found and has active OIDC Authentication, the user is then directed to the OKTA login page.

h. **Service account Authentication** section – switch off the **Active** toggle, if you don't wish to use service account as well.

i. Click **Save**.

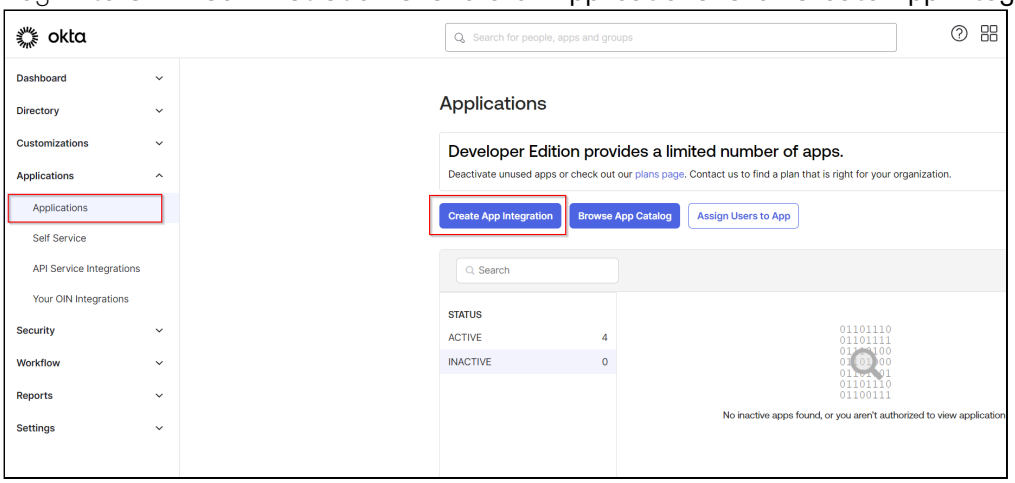
13. The OKTA users will now be able to log in to SAFEQ Cloud.

Every user logged-in via this provider will have **Authenticated Users** group assigned. You can use this group to manage access controls. See Access Control.

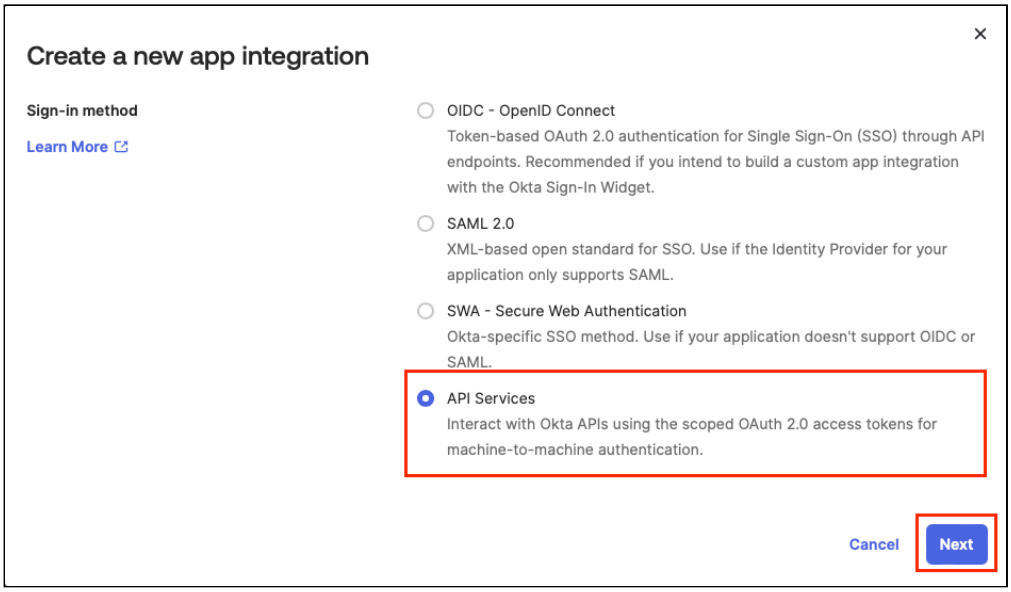
Service account authentication

To configure OKTA authentication using OKTA APIs, perform the following steps:

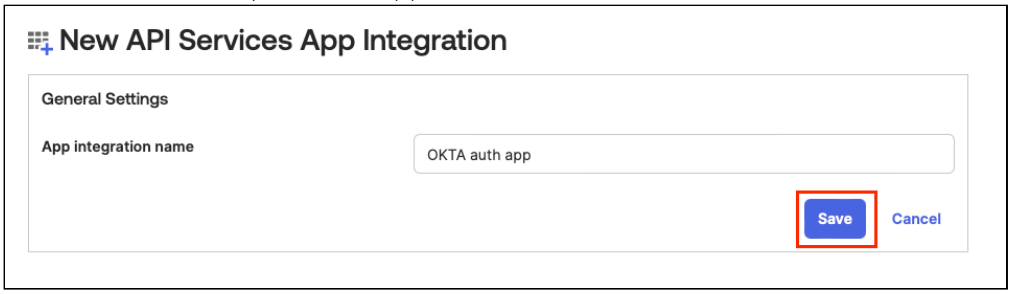
1. Log in to OKTA administration UI and click **Applications**. Click **Create App Integration**.



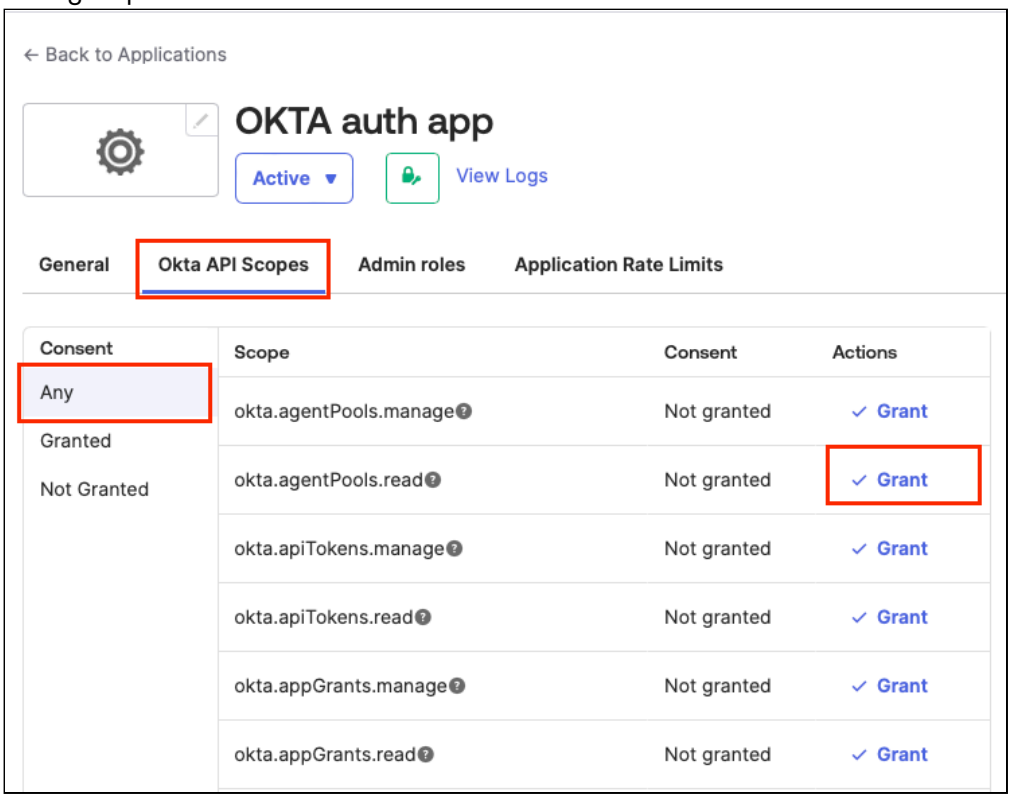
2. Select **API Services**. Click **Next**.



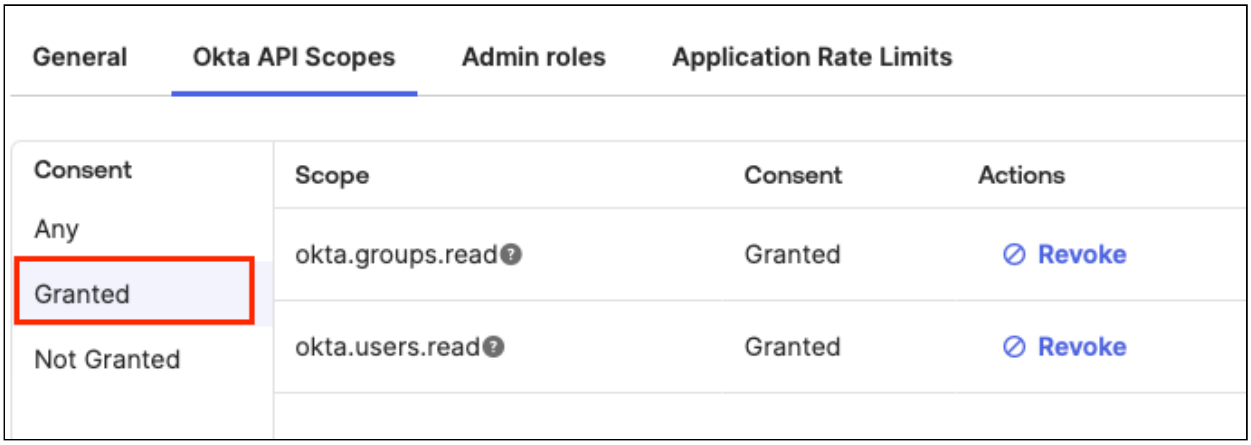
3. Enter the name of your new application and click **Save**.



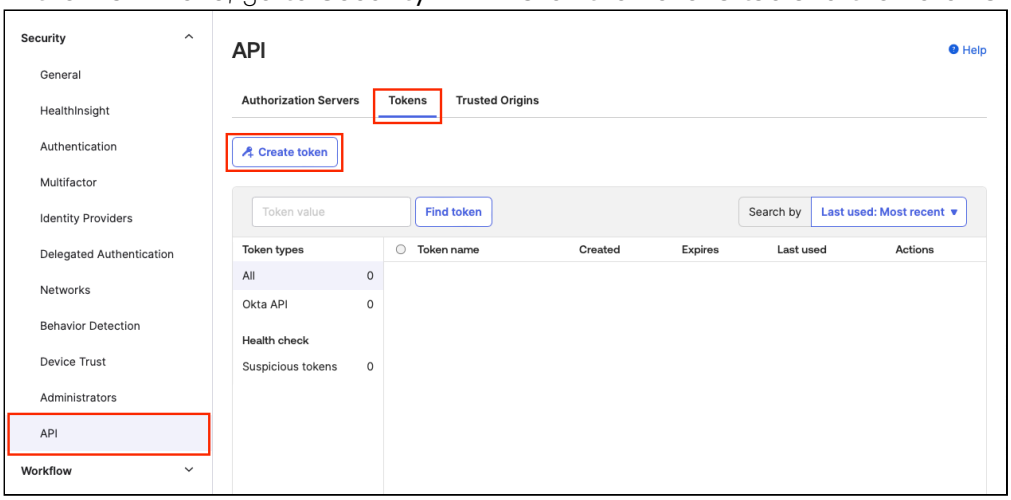
4. Got to the **Okta API Scopes** tab. Under **Consent**, click **Any** and search for **okta.users.read** and **okta.groups.read**. Select **Grant** for both.



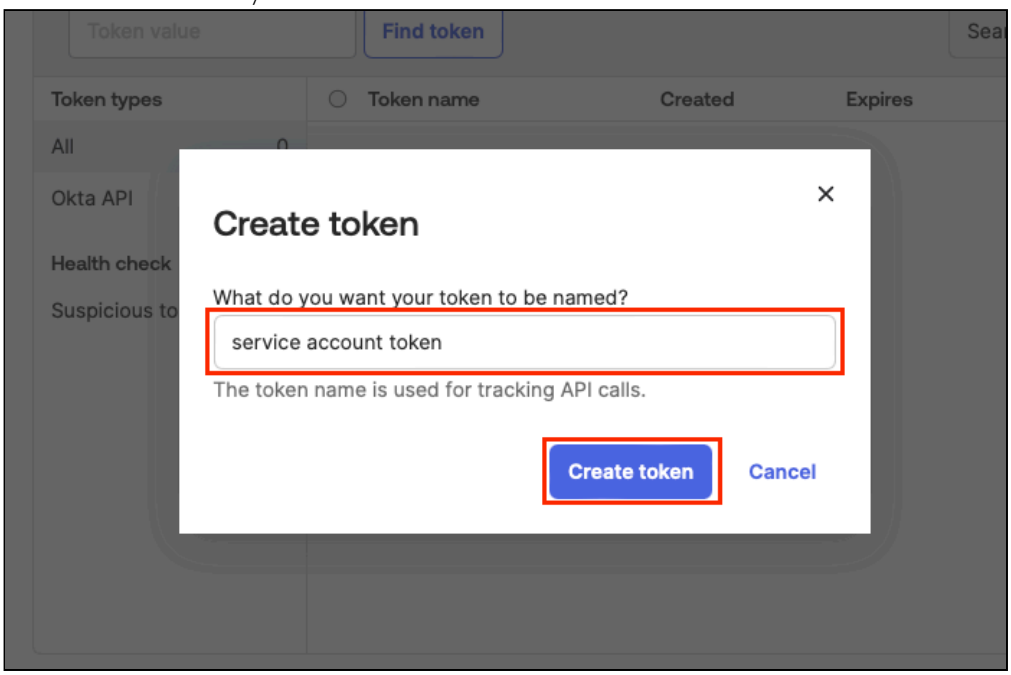
5. The result in Consent **Granted** will look like this:



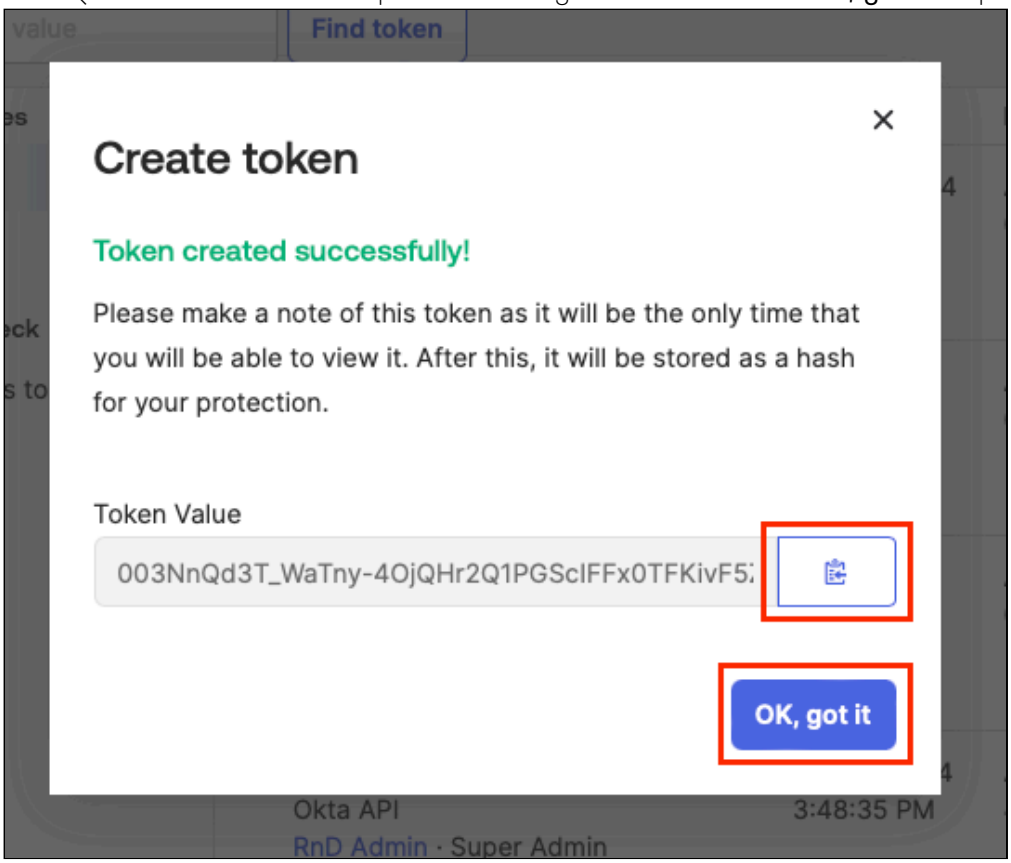
6. In the main menu, go to **Security** > **API.** Click the **Tokens** tab and then click **Create token**.



7. Enter the name of your token and click **Create token**.



8. Copy the **Token value**. Save the secret value in a secure way. You will need it later on in SAFEQ Cloud Authentication provider configuration form. Click **OK, got it** to proceed.



> ⚠ For security reasons, you can only see the secret value at the time of creation. Once you leave the screen, the value will not be shown again.

9. This concludes the OKTA application configuration for Service account authentication.
10. Log in to SAFEQ Cloud Web UI and go to **Users** page and **Authentication providers** tab.
11. Click **Add** and enter the following details:
    a. **Type** – Select **OKTA**.
    b. **Name** – An internal name used for identifying the particular authentication provider configuration. Should be prefilled with the selected Type.
    c. **Domains** – The domain names of the authenticating users. If you have domain aliases that the users can use to log in, add them to this field. At least one domain in the list should match the domain part of the fully qualified user name passed for authentication. If strict domain validation is disabled, SAFEQ Cloud will attempt to authenticate the user with all domains in the list, regardless of the domain entered in the credentials, in the order defined in the list. If strict domain validation is enabled, SAFEQ Cloud will attempt to authenticate only with the domain in the credentials. For example, if the domain name of OKTA authentication provider is *okta.domain.com*, the user added in Access Control should be *user@okta.domain.com*.

Specifying the correct domain name is especially important if using the Strict domain validation feature, as it is otherwise not possible to detect to which domain a user belongs.

d. **Priority** – A number that determines the order in which authentication providers will be called until one succeeds. Higher-priority providers will be called first.

e. **Active** – If enabled, the authentication provider will be used for authentication. If disabled, this authentication provider will not be searched.

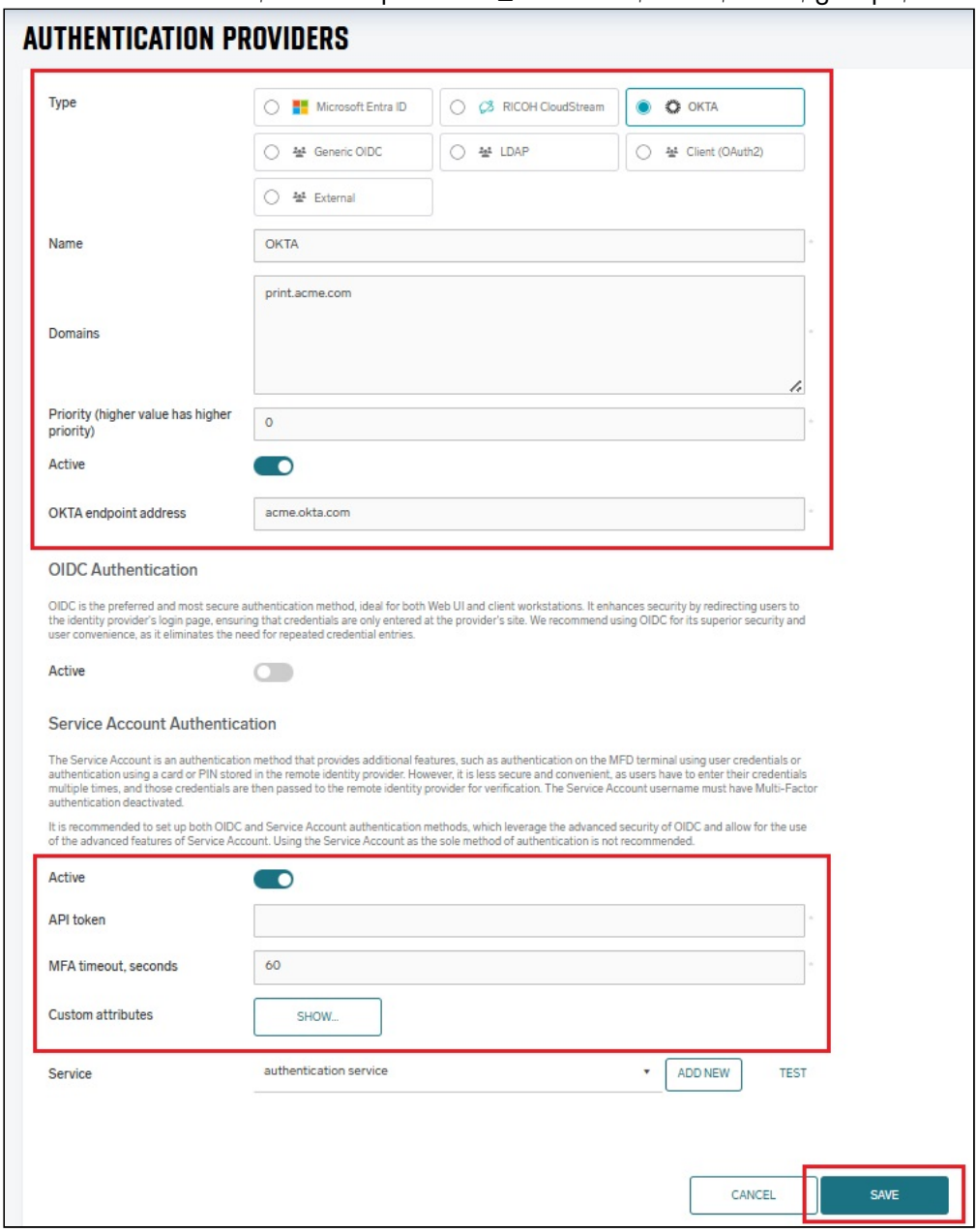
f. **OKTA endpoint address** – The address of the OKTA server for which you created the OKTA application. Example: *acme.okta.com*.

g. **OIDC Authentication** section – Toggle **Active** off if you don't want to use OIDC, otherwise toggle it on and select **Customizable**, see *OIDC Authentication* section above.

h. **Service Account Authentication** – This section applies to service account settings.

   1. **Active** – The service account authentication is used when **Active** is enabled.
   2. **API token** – The Token you created in OKTA application in the previous steps.
   3. **MFA timeout, seconds** – The maximum time in seconds for which the server will wait for Multi-factor authentication to complete.

4. **Custom token claim names** – Click **Show** to change the mapping within ID token and OKTA user attributes, such as **preferred_username**, **name**, **email**, **groups**, and **sub** .



i. Click **Save**.

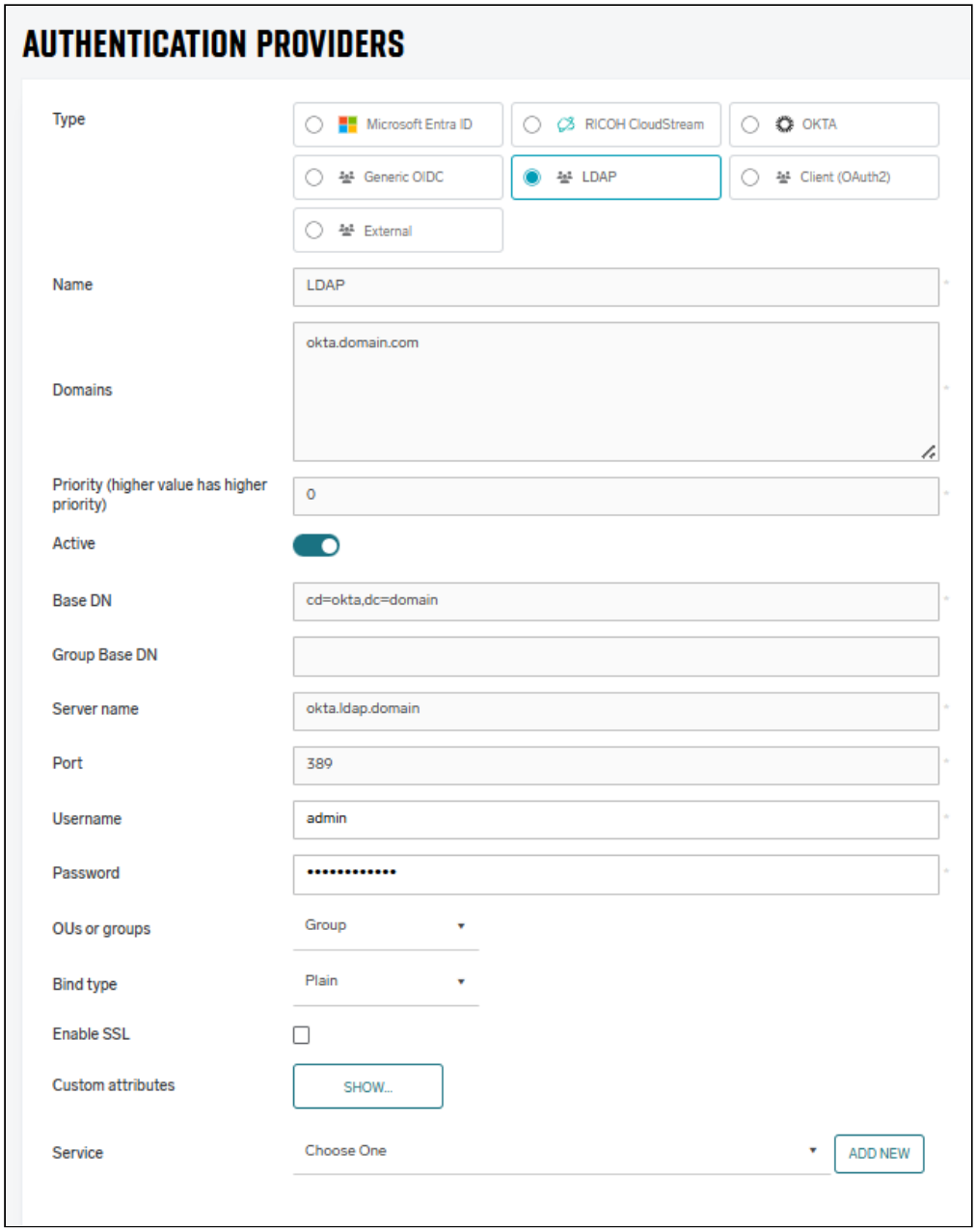
12. The OKTA users can now log in to SAFEQ Cloud.

> ⚠ Every user logged-in via this provider will have **Authenticated Users** group assigned. You can use this group to manage access control. See Access Control.

OKTA authentication via LDAP

The following section outlines the configuration of SAFEQ Cloud integrated with OKTA through LDAP.

Add a new LDAP authentication provider in the SAFEQ Cloud authentication settings, and enter the following details:

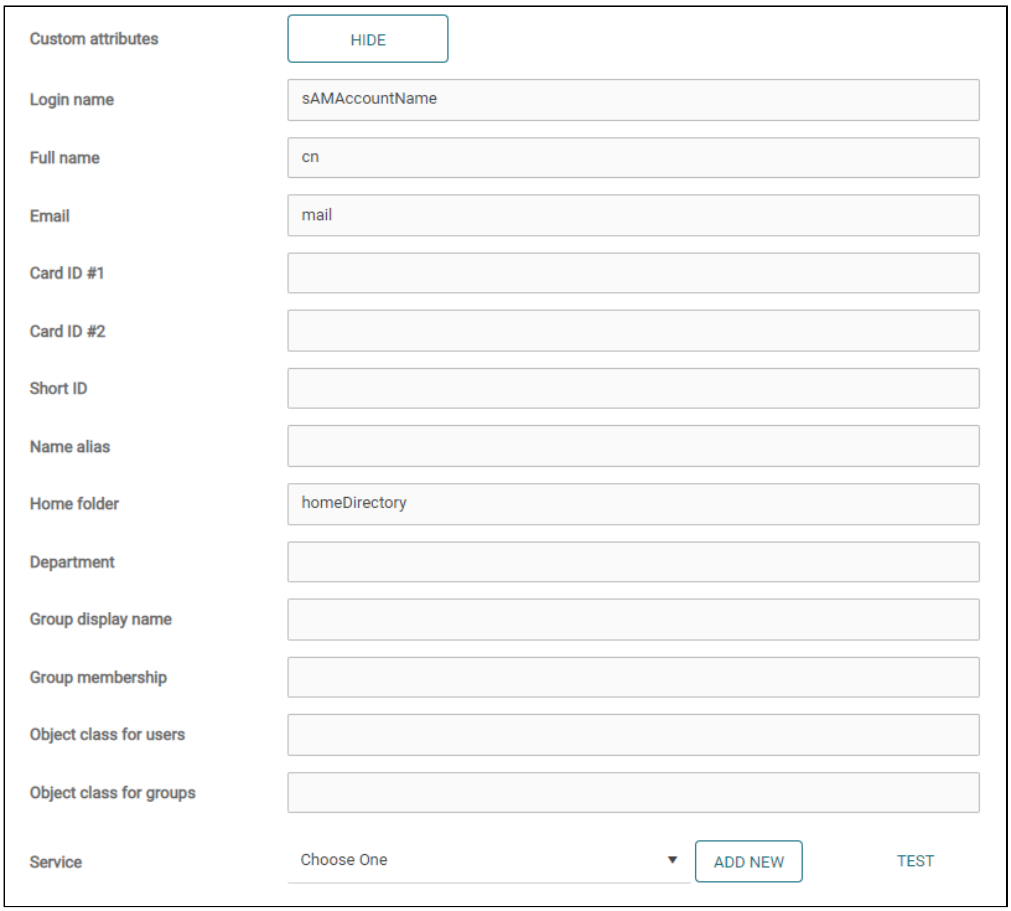


- Name – An internal name used for identifying the particular authentication provider configuration. Should be prefilled with the selected Type.
- Domains – The domain names of the authenticating users. Add here the domain aliases that the users can use to log in. At least one domain in the list should match the domain part of the fully qualified username. If strict domain validation is disabled, SAFEQ Cloud will attempt to authenticate the user with all domains in the list when the username does not contain any domain, in the order defined in the list. If strict domain validation is enabled or the username contains a domain, SAFEQ Cloud will attempt to authenticate only with the domain in the credentials.

For example, to allow user *john.doe@okta.domain.com* to log in via this Authentication provider, enter the *okta.domain.com* domain here.

- Priority – A number that determines the order in which authentication providers will be called until one succeeds. Higher-priority providers will be called first.
- Active – If enabled, the authentication provider will be used for authentication. If disabled, this authentication provider will not be searched.
- Base DN – The point in the OKTA where searching will begin. Will apply to both user and group searching, if *Group Base DN* is empty.
- Server name – The address (DNS, hostname or IP) of the OKTA server to which SAFEQ Cloud Authentication Service will connect to search.
- Port – Port used for the service, 636 must be in this case.
- Username – The username used to connect and search in the OKTA.
- Password – Password used to connect and search in the OKTA.
- OUs or groups – Choose how to identify groups, for access control management, default is "Groups".
- Bind type – Whether to bind with Plain connection, MD5 digest, or Kerberos
- Enable SSL – Whether connection to OKTA should use SSL encryption. In this case, it must be enabled.
- Custom attributes – Expand custom attributes to change the LDAP attributes in which username, card ID's, ShortID's and similar are stored. The login name and email must have "uid"

value.



- **Service** – Which Authentication Service will communicate to this OKTA server via LDAP. If no service is already created, it can be added using the **Add** button.

After saving the new authentication provider, create an access control record for the users who will be authenticating via this provider. See Access Control.

Enabling user self-registration

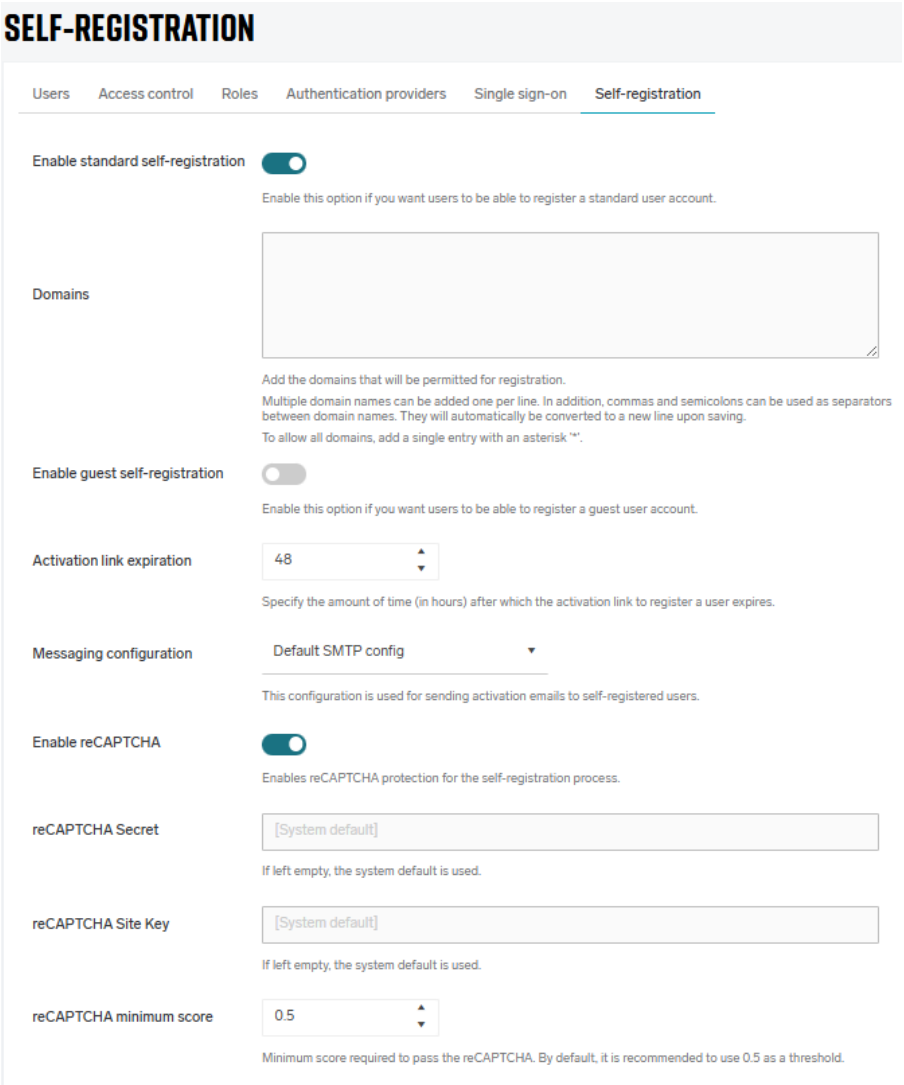
SAFEQ Cloud allows users to self-register as local users (i.e. users created internally in SAFEQ Cloud under the Local authentication provider).

To enable self-registration, perform the following steps:

1. In the SAFEQ Cloud Web UI, go to **Users**. Click the **Self-registration** tab.

> You must have the **ViewSelfRegistrationSettings** and **ModifySelfRegistrationSettings** permission to see this page. Both are assigned to the Administrator role by default.

2. After enabling the standard self-registration toggle, you will see the configuration options.



3. In **Domains**, enter the domains that you want to permit for standard user self-registration. For example, if you want user *john.doe@acme.com* to be able to self-register, enter *acme.com* in this field. To allow all domains, enter an asterisk (*).

4. In **Activation link expiration**, specify the amount of time (in hours) after which the activation link in the Activation Code Email expires.

5. In **Messaging configuration**, select which of your messaging configurations will be used to send transaction emails to self-registered users.

6. Enable the **reCAPTCHA** toggle if you wish to use reCAPTCHA protection for the self-registration process. We strongly recommend keeping this option enabled.

> reCAPTCHA is a security service that protects websites from fraud and abuse. It is used in the self-registration process to secure the procedure and filter out malicious usage or bots. Since version 3 is used, there are no puzzles or any other manual steps for users to complete — everything is hidden and automatic.
>
> You can use your own reCAPTCHA account, or the system default reCAPTCHA one.

7. In **reCAPTCHA Secret**, enter your reCAPTCHA secret if you wish to use your own reCAPTCHA account. If the field is left empty, the system default will be used.
8. In **reCAPTCHA Site Key**, enter your reCAPTCHA site key if you wish to use your own reCAPTCHA account. If the field is left empty, the system default will be used.
9. Click **Save**.
10. The users will see the self-registration option on the SAFEQ Cloud Web UI login page.

> **Note on SAMLv2 and self-registration compatibility**
>
> If your organization is using **SAMLv2 authentication** and you want users to use self-registration, it is important to provide them with a direct link to the SAFEQ Cloud login page using the following format:
> *{login page URL}/login?forcehcplogin*
>
> This ensures that users are **not automatically redirected to the SAML login flow**, allowing them to access the self-registration option instead.

Transaction emails

SAFEQ Cloud sends two types of emails to standard users during the self-registration process. The content of these emails cannot be modified.

1. Activation Code Email: This email is sent to the email address that the user filled in the self-registration form (it must be an address that doesn't exist in SAFEQ Cloud yet). The email contains an activation link that continues the self-registration process. This link has a default expiration time of 2 days but can be changed in the settings (see Activation link expiration above).
2. Account Already Exists Email: This email is sent to the user in case the email address already exists in the system. It directs the user to the login page.

Guest users / guest printing

Introduction

A guest user is a user with a limited set of permissions - by default those that are listed under the Guest role in SAFEQ Cloud.

> Note that SAFEQ Cloud creates the Guest role when the first guest registers.

Default guest role permissions:

- AccessInputPort
- SearchInputPort
- AccessOutputPort
- ColorPrint
- ColorCopy
- OCRDocument

- AirPrint
- ViewJob
- ViewMyProfile
- ModifyMyProfile
- GenerateOTP
- GenerateShortID
- ModifyMyPersonalInformation
- SearchLocation
- AddJob
- ReleaseJob
- WebUploadDocument
- 242px450pxViewClientAndMobileDownload
- AllowPullPrint

Guest accounts also differ from standard user accounts in that you can set an expiration time for them. After they expire, they are deleted from SAFEQ Cloud automatically.

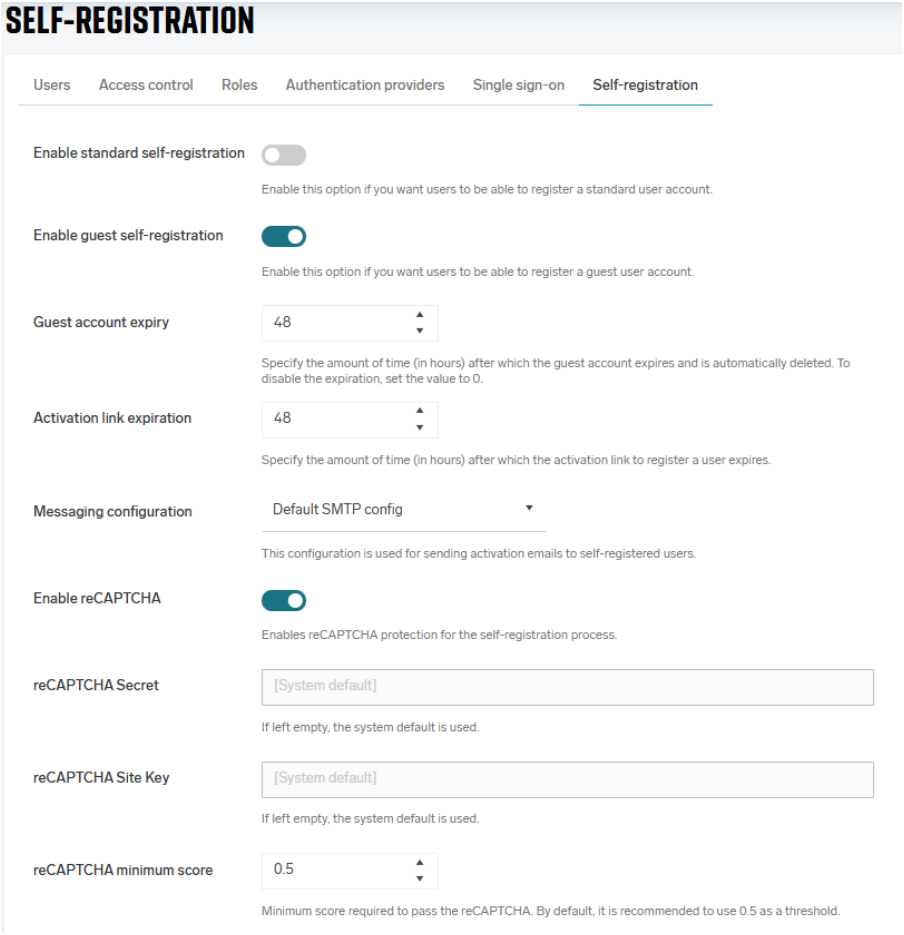
Enabling guest self-registration

To enable guest self-registration, perform the following steps:

1. In the SAFEQ Cloud Web UI, go to **Users**. Click the **Self-registration** tab.

   > You must have the **ViewSelfRegistrationSettings** and **ModifySelfRegistrationSettings** permission to see this page. Both are assigned to the Administrator role by default.

2. Enable the guest self-registration toggle. After that, you will see the configuration options.



3. In **Guest account expiry**, specify the amount of time (in hours) after which the guest account expires and is automatically deleted. To disable the expiration, set the value to 0. Changing this option does not affect guest accounts registered in the past.

4. In **Activation link expiration**, specify the amount of time (in hours) after which the activation link in the Activation Code Email expires.

5. In **Messaging configuration**, select which of your messaging configurations will be used to send transaction emails to self-registered guests and users.

6. Enable the **reCAPTCHA** toggle if you wish to use reCAPTCHA protection for the self-registration process. We strongly recommend keeping this option enabled.

> reCAPTCHA is a security service that protects websites from fraud and abuse. It is used in the self-registration process to secure the procedure and filter out malicious usage or bots. Since version 3 is used, there are no puzzles or any other manual steps for users to complete — everything is hidden and automatic.
>
> You can use your own reCAPTCHA account, or the system default reCAPTCHA one.

7. In **reCAPTCHA Secret**, enter your reCAPTCHA secret if you wish to use your own reCAPTCHA account. If the field is left empty, the system default will be used.

8. In **reCAPTCHA Site Key**, enter your reCAPTCHA site key if you wish to use your own reCAPTCHA account. If the field is left empty, the system default will be used.

9. Click **Save**.

10. The guests will see the self-registration option on the SAFEQ Cloud Web UI login page.

Transaction emails

SAFEQ Cloud sends three types of emails during the guest self-registration process. The content of these emails cannot be modified.

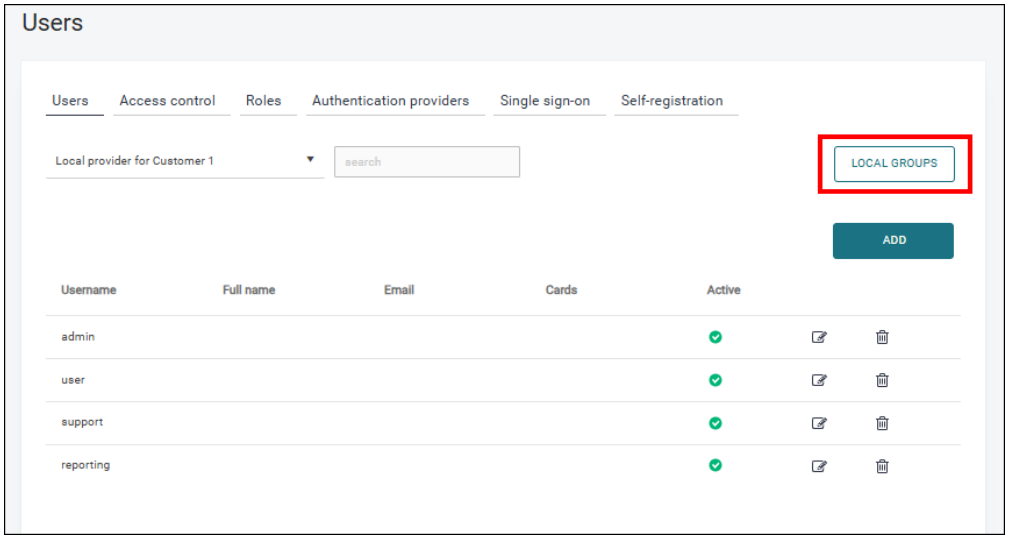
1. Activation Code Email: This email is sent to the email address that the user filled in the self-registration form (it must be an address that doesn't exist in SAFEQ Cloud yet). The email contains an activation link that continues the self-registration process. This link has a default expiration time of 2 days but can be changed in the settings (see Activation link expiration above).

2. Account Already Exists Email: This email is sent to the user in case the email address already exists in the system. It directs the user to the login page.

3. Account Expired Email: This email is sent to the guest's email address after it expires. It informs the guest about the removal of their account and directs them to the login page.

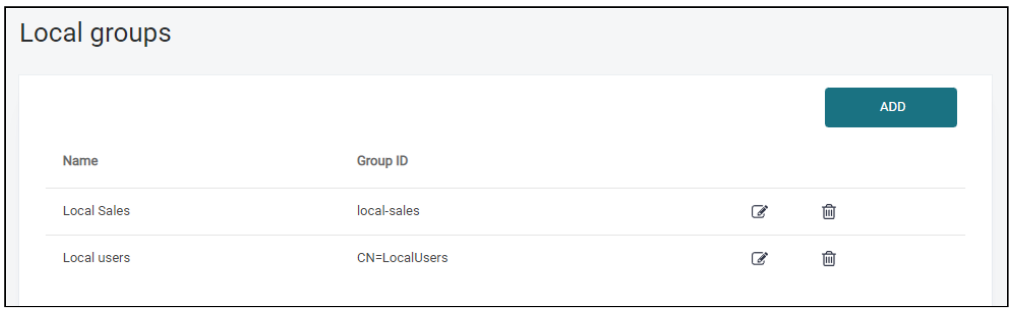
Local groups

For local authentication provider, it is possible to define custom local groups and to edit the user membership for these groups. When you select a local authentication provider in the **Users** tab, you will see the **Local groups** button.

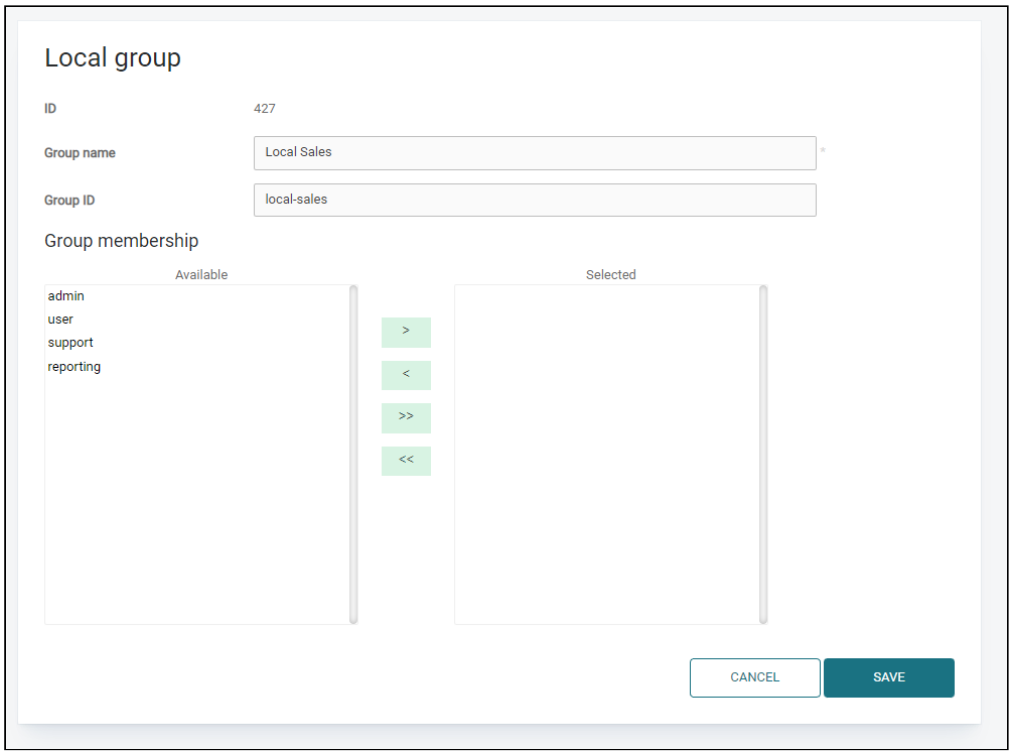


Local groups are helpful in defining access controls for large groups of local users. You can add, delete and modify Local groups in the same way as all other objects in SAFEQ Cloud.

All local users are contained within a default group called **Local users**.



When editing a local group, you can define group membership. Group membership can also be changed in the user settings.



The following group settings are editable:

- Group name
- Group ID – the group ID. It must be unique within one tenant. If left empty, the server will assign a randomly generated ID. This ID can be used in the API calls to lookup the group or change group membership.
- Group membership – allows you to select which users will be part of this group.

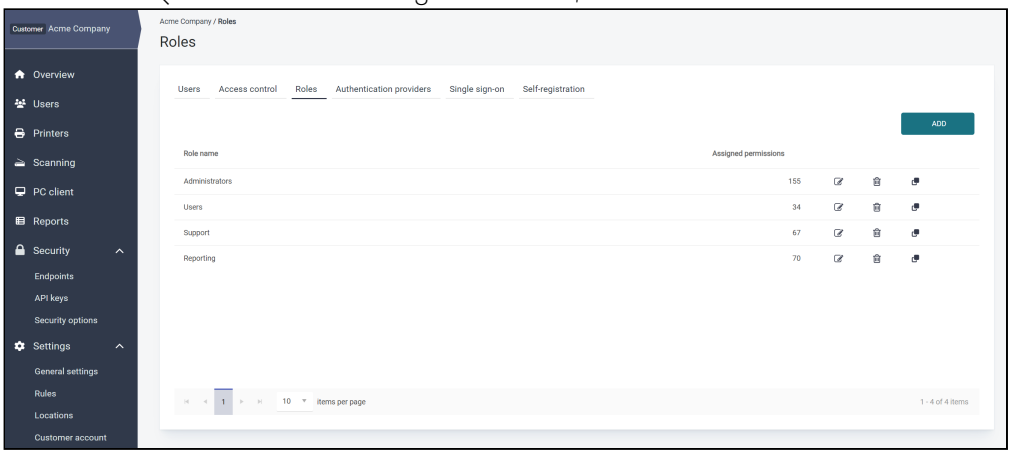
After you create your group, you can add it in the Access Control section to define local user permissions based on group membership.

Roles

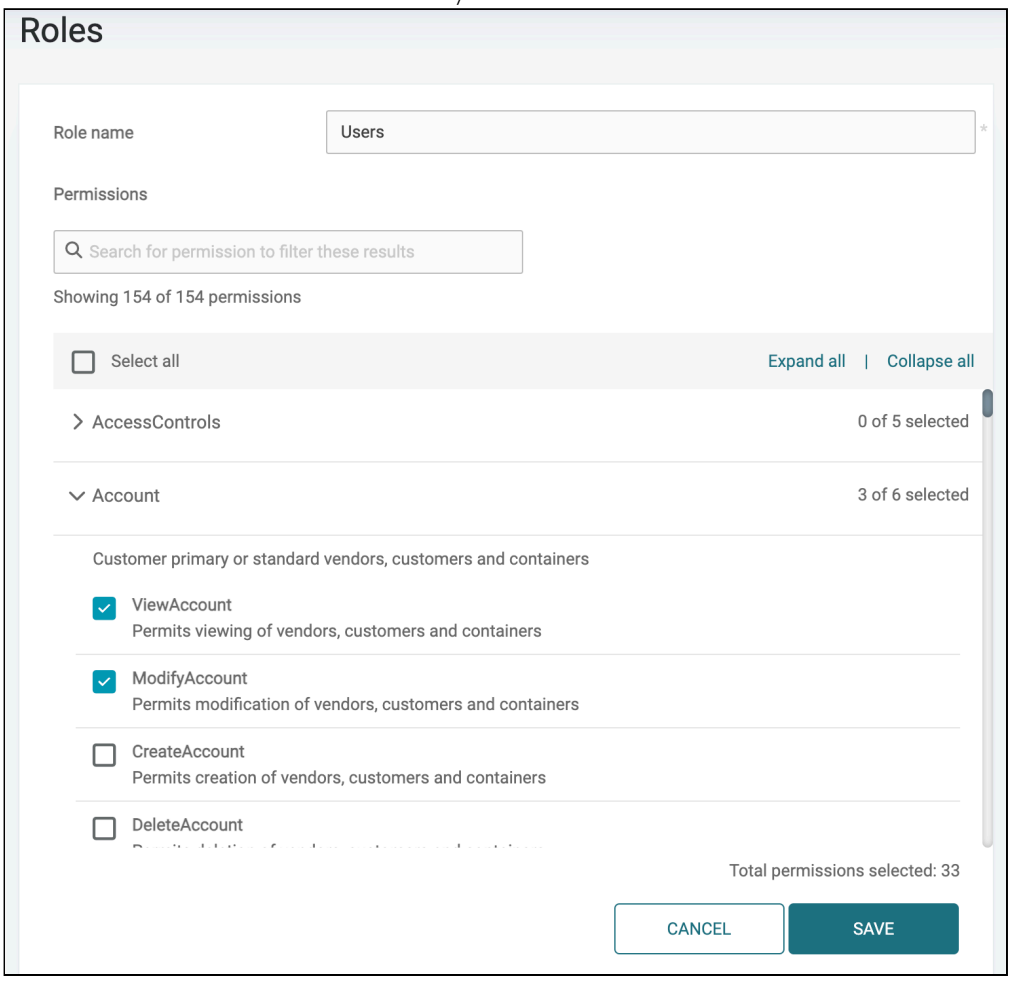
YSoft SAFEQ Cloud has four default security roles. You can modify these roles, or create new one based on the types of users that will access the system. Roles exist at each account level in the system.

Viewing and editing roles

1. In the SAFEQ Cloud Web UI navigation menu, click **Users** and tab **Roles**.



2. Click the edit icon next to the role you wish to edit. You will see the role details.



3. Select the permissions for the role. You can use the search box to filter only permissions that contain a specific word, such as "view."

4. Click **Save**.

Creating a new role

1. In the Roles list, click **Add**.
2. On the Edit Role screen, configure the new role by entering a name and selecting the permissions.
3. Click **Save**.

SQTS specific roles (Cloud terminals)

Scanning rights are handled by access rights to scan workflows.

ReleaseJob right gives the user the right to BW Print and Copy.

Permissions

Permissions are used to limit the actions users/groups can perform in the system. For editing the permissions inside a role, see Roles.

Documents

Available permissions:

- ViewJob
- DeleteJob
- SearchJob
- AddJob
- ReleaseJob

SAFEQ Cloud Web UI

- ViewJob – have access to pending jobs view
- DeleteJob – have access to delete pending jobs
- SearchJob – have access to list jobs when using the page search functionality

API

> If the settings **Allow unauthenticated requests** and **Allow untrusted endpoints** are set to true for the API KEY that is used, the permissions will not be checked.

- ViewJob – have access to list documents in endpoint /documents (GET)
- AddJob – have access to upload documents in endpoint /documents (PUT)
- ReleaseJob – have access to release a job in endpoint /documents/uuid/address (POST)

Mobile Gateway

> The permissions are checked only for api version 5.0.0 or higher

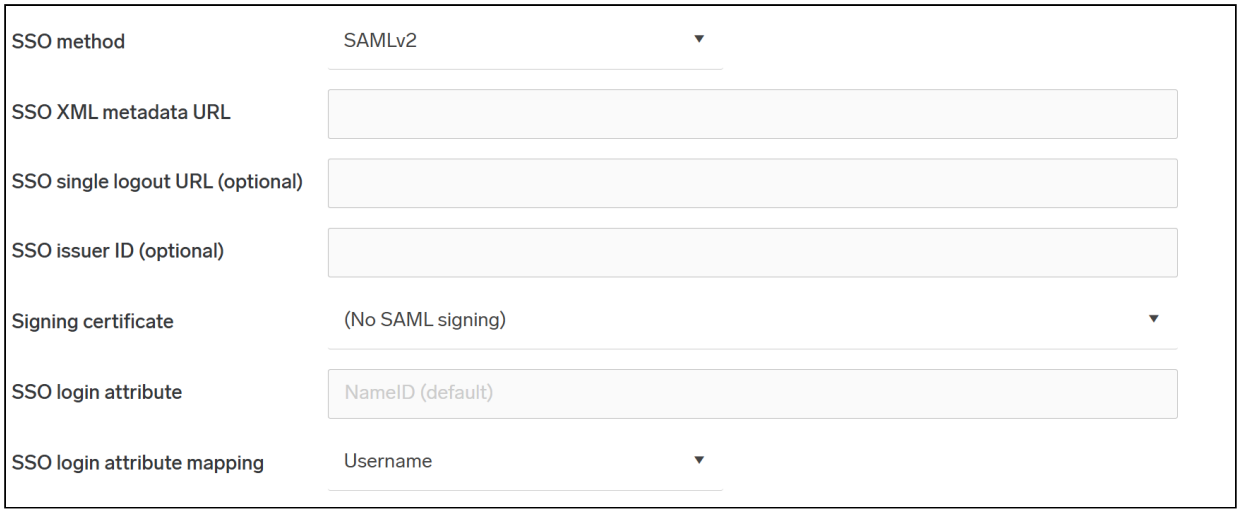
- ViewJob – have access to list documents for action=getprintjobsforusername and action=downloaddocument

- ReleaseJob – have access to release a job for action=printdocument, action=printurl, action=getprintjobsforreleasecode, action=printjobtoprinter, action=printjobidtodeviceserial and downloaddocument

> action=downloaddocument requires both ViewJob permission and ReleaseJob permission

Single Sign-On

Supported SAMLv2 SSO providers are Okta and Azure ADFS. Follow the steps described in sections Microsoft Entra Single Sign-On and Okta Single Sign-On / Logout to configure the corresponding SSO.
You can configure SAMLv2 Single Sign-On on an account basis in the **Users** > **Single sign-on** configuration:



- In **SSO method,** select SAMLv2 to enable SSO. Select **None** to disable SSO. There is no need to add values for the SSO XML Metadata URL if **SSO method** is **None**.

  > SAML will work only if OIDC is disabled in your Authentication providers, or if your Authentication providers use Service Account Authentication in addition to OIDC.

- In **SSO XML Metadata URL**, enter the XML metadata URL from the SSO provider's SAMLv2 configuration.
- In **SSO Single Logout URL**, enter the URL to the logout endpoint of the SSO provider. This field is optional.
- In **SSO Issuer ID**, enter the issuer ID which is sent to SAML SSO provider. If not specified, the URL taken from the browser will be used in the form `https://account:8443/`.
- In **SSO login attribute**, specify the SAML attribute that uniquely identifies the user (e.g., `uid`, `email`). If left empty, the Identity Provider's standard **NameID** will be used instead - this is the recommended and most widely compatible choice.
- In **SSO login attribute mapping**, select the user attribute to match against the SAML login attribute. Keeping the default (`Username`) is recommended.

Notes on the XML Metadata URL:

Instead of an `http/s` URL the metadata can also be specified with a `file` URL like `file:/{filename}` or `file:///{filename}` where `{filename}` refers to a file placed in the SAFEQ Cloud installation folder under `<install-root>/conf/{filename}`.
The file size limit is 1 megabyte. Symbolic links are not allowed. Upon saving the configuration, the specified file is checked for XML validity.
In a cluster setup, this file must be placed on every cluster node.

Identity provider setup guides for Okta

1. Navigate to **Applications** in Okta and select the one that has SAMLv2 configured.
2. Click the **Sign On** section.
3. For SSO XML Metadata URL, go back to the **Sign On** section and copy the URL from Identity Provider metadata.
4. For SSO Single Logout URL, click **View Setup Instructions**, and copy the URL corresponding to Identity Provider Single Logout URL.

   > You only have access to the Logout URL if you have enabled **Single Logout** in the advanced settings of the SAML application.

Okta: `https://developer.okta.com/docs/guides/saml-application-setup/config-saml-in-app/`

Identity provider setup guides for Azure or Client

1. Navigate to **Enterprise applications** and select the one that has SAMLv2 configured.
2. Click **Single sign-on**.
3. For SSO XML Metadata URL, copy the URL from App Federation Metadata XML
4. For SSO Single Logout URL, copy the URL from Logout URL

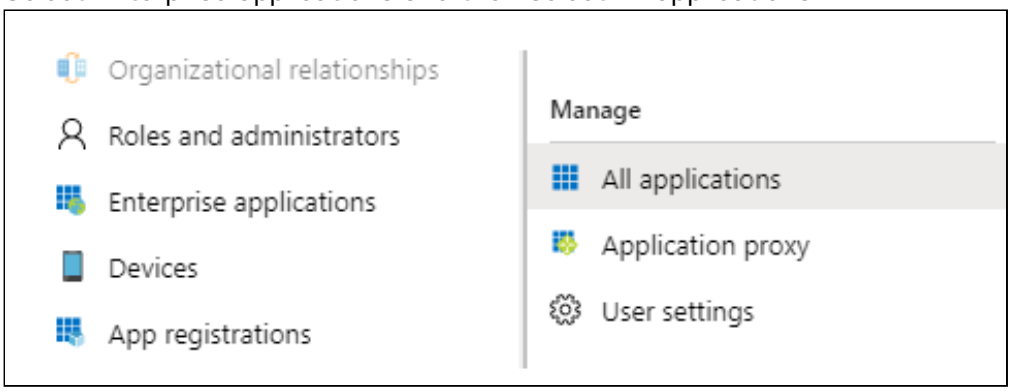
Make sure that **Azure, Client or Okta authentication provider** and its corresponding **access control** are added in SAFEQ Cloud, as well.

Microsoft Entra Single Sign-On

To configure Microsoft Entra Single Sign-On, you must add a new application in your Microsoft Entra tenant.

1. In the Azure portal, on the left navigation panel, click **Microsoft Entra**.

2. Select **Enterprise applications** and then select **All applications**.

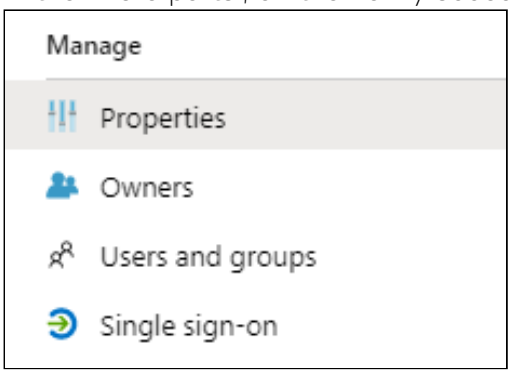


3. Click **New applications** to add a new application.

4. In the search box, type the name of the application you want to use, like Microsoft Entra SAML Toolkit, from the result panel. Click **Add** to add the application.

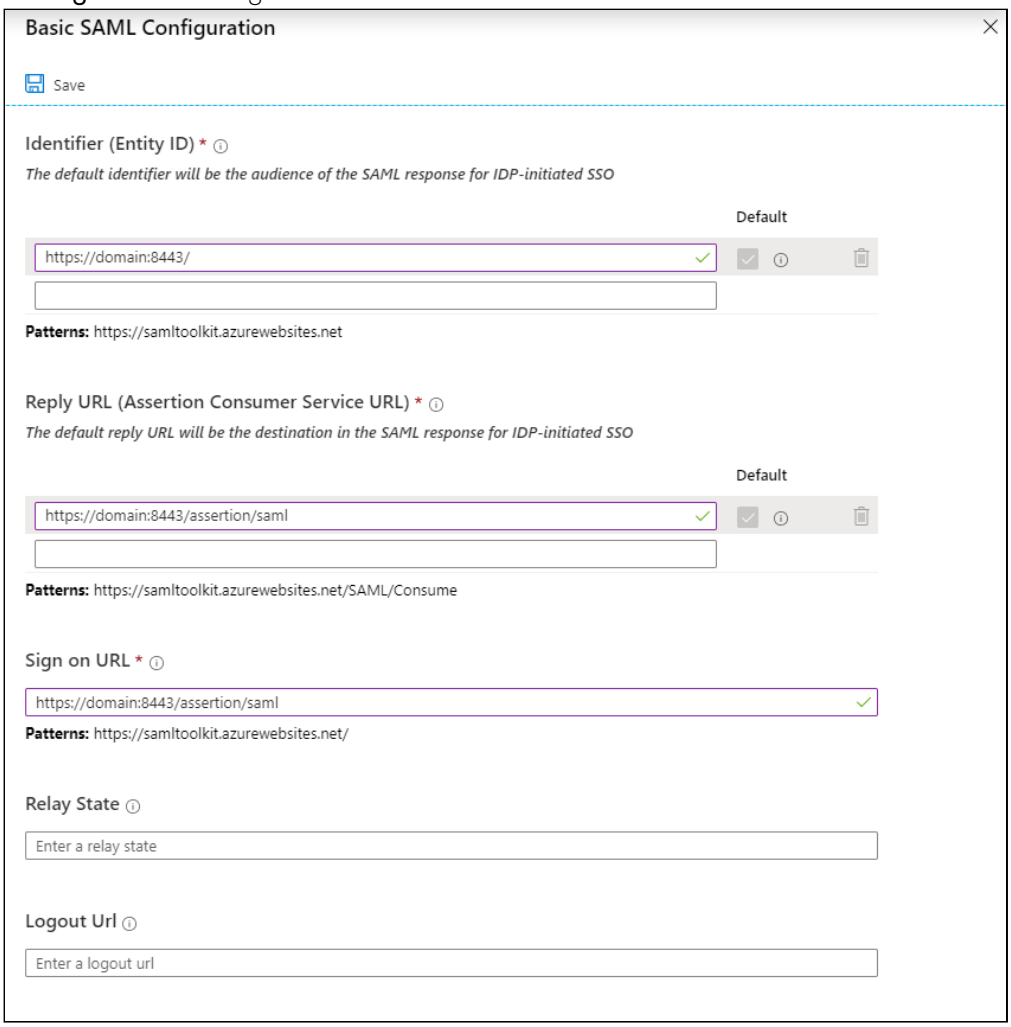
Configure Microsoft Entra Single Sign-On

1. In the Azure portal, on the newly added application integration page, select **Single sign-on**.



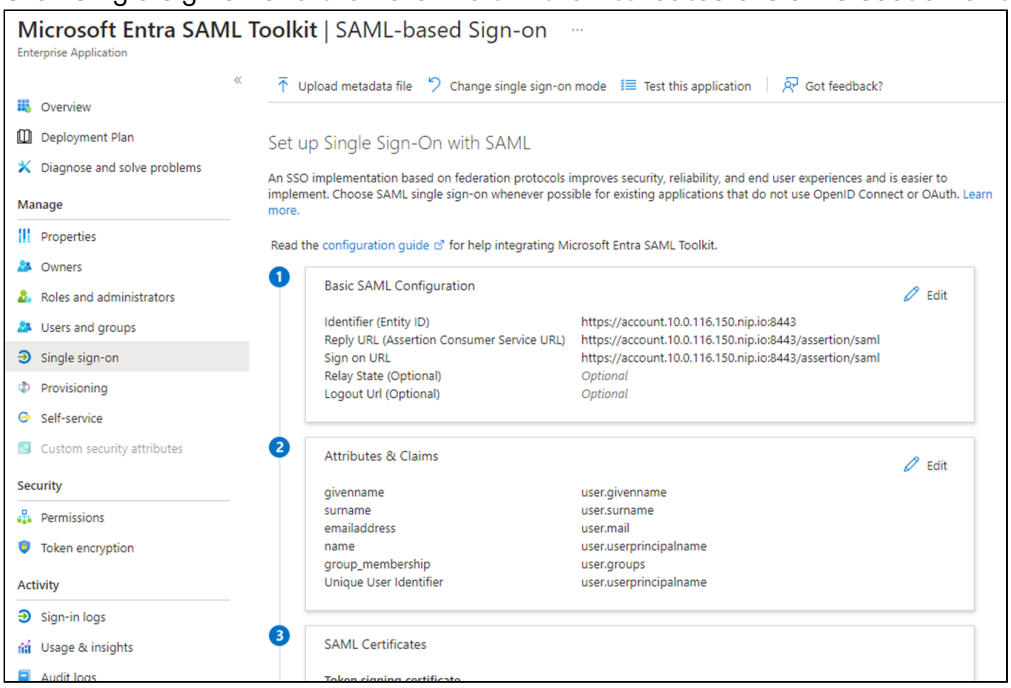
2. In the **Select a Single sign-on method** dialog, select **SAML mode**.

3. On the **Set up Single Sign-On with SAML** page, click the edit icon to open the **Basic SAML Configuration** dialog.

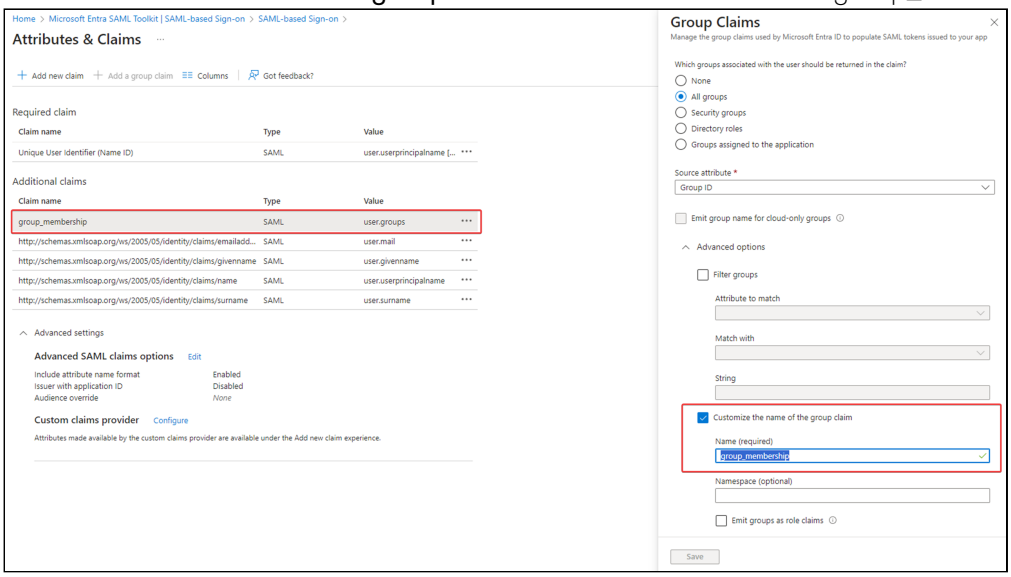


- In the **Identifier (Entity ID)** text box, enter an issuer ID from the SAFEQ Cloud SAML configuration or URL that follows the pattern: `https://<domain_name_that_has_saml_configured>:8443/` (if issuer ID is empty).
- In the **Sign on URL** text box, enter the login URL: `https://<domain_name_that_has_saml_configured>:8443/assertion/saml`
- In the **Reply URL** text box, enter the URL: `https://<domain_name_that_has_saml_configured>:8443/assertion/saml`
- The port is 8443. In environments with reverse proxy, do not specify the port number in the URL. Example: `https://<domain_name_that_has_saml_configured>/assertion/saml.`

4. Click **Single sign-on** and then click **Edit** in the **Attributes & Claims** section of the page.



5. Click the claim with the **user.groups** value. In the dialog window that will be displayed, select **Customize the name of the group claim**. Enter the name of the group_membership.



6. Click **Save**.

Assign the Entra user(s)

1. In the Azure portal, select **Enterprise Applications**, and then select **All applications**.
2. In the applications list, select your added application.
3. In the application's overview page, under the Manage section, select **Users and groups**.
4. Click **Add user**, then select **Users** in the **Add Assignment** dialog.
5. Type the username you want to have access to, then click **Select** at the bottom of the screen.

6. In the Add assignment dialog, click Assign.

Setup guides

https://learn.microsoft.com/en-us/entra/identity/saas-apps/saml-toolkit-tutorial

Okta Single Sign-On / Logout

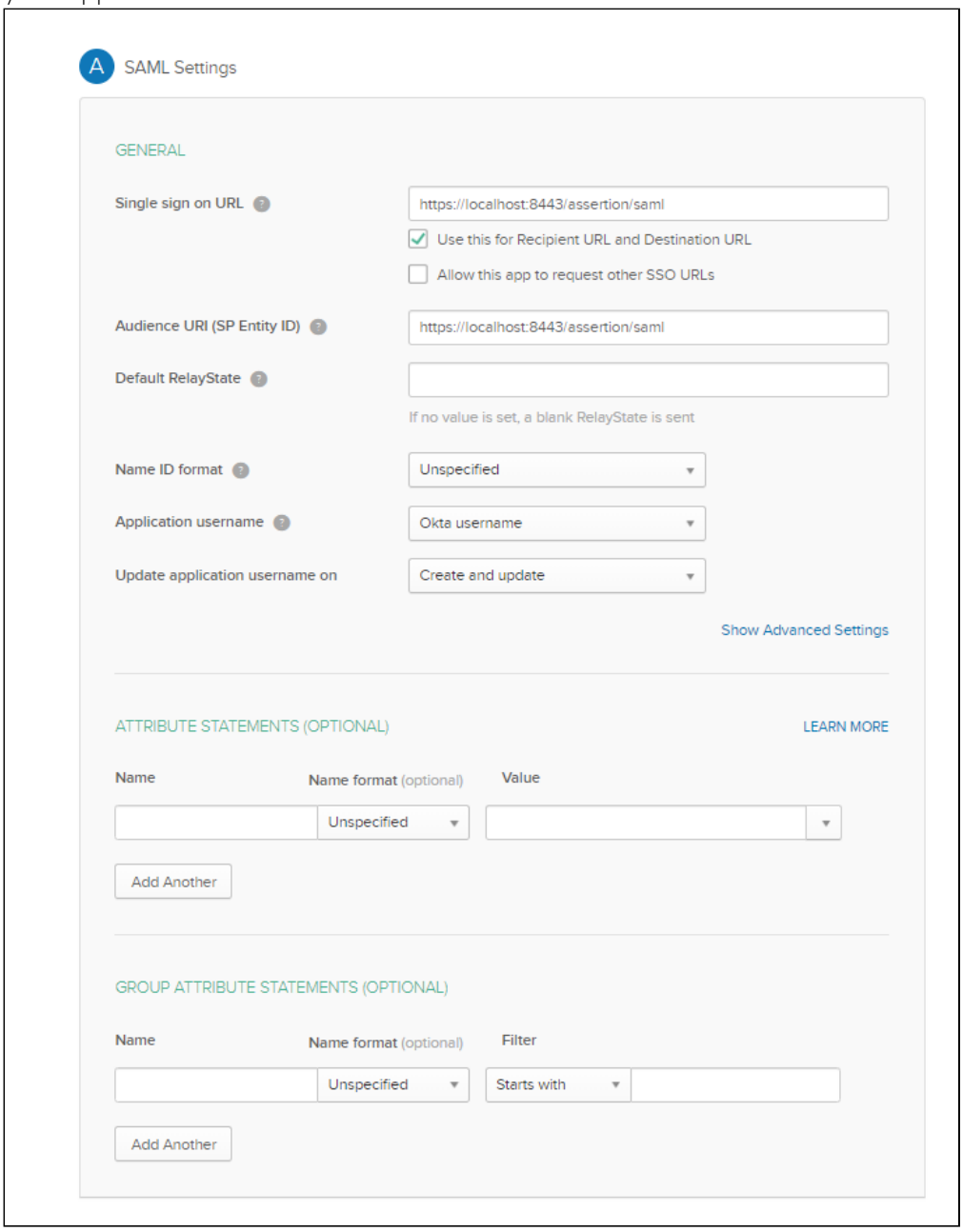
Set up a SAML application in Okta

1. Click Application from the menu bar.
2. Click Add Application and then Create new Application.
3. In the Create a New Application Integration dialog box, leave Web as the platform and select SAML 2.0 as the protocol that you want to use to sign in. Click Create.
4. In General Settings, enter the application name and click Next.

Configure SAML Single Sign-On in Okta

1. In the SAML Settings, paste the Assertion Consumer Service (ACS) URL into the SSO URL field. This URL depends on the account domain but generally looks like this:
   `https://<account-domain>:<port>/assertion/saml`
   The port number is 8443. In environments with reverse proxy infrastructure, do not specify the port number in the URL, meaning the default HTTPS port 443 will be used.
2. Paste the Issuer ID value from the SAFEQ Cloud SAML configuration into the Audience URI (SP Entity ID) field, or use `https://<accountdomain>:<port>/` pattern if the issuer ID is empty.
3. Select the Name ID format and Application username that your application requires. For example, EmailAddress and Email, or leave the defaults.
4. In the Attribute Statements (Optional) section, add the required SAML attributes for your application.

5. In the **Group Attribute Statements (Optional)** section, add the required group attributed for your application.



6. Click **Next**. On the Feedback page, select **I'm an Okta customer adding an internal app**.
7. For the App type, select **This is an internal app that we have created**.
8. Click **Finish**.

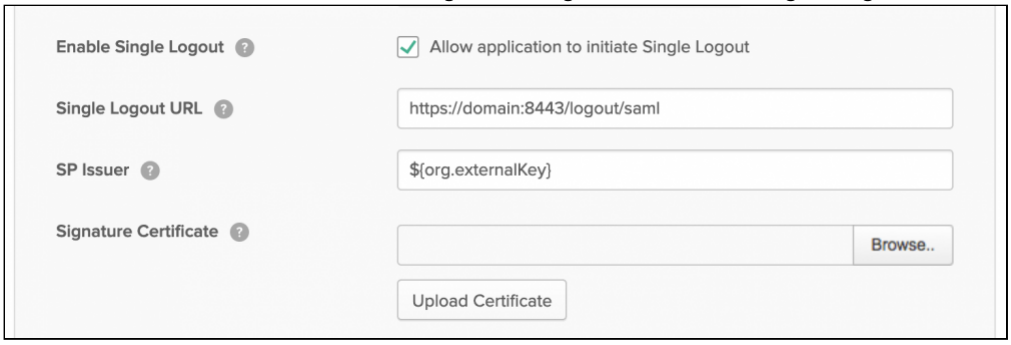
Assign users to the created application

1. Click the **Assignments** tab.
2. Click **Assign**. Select either **Assign to People** or **Assign to Groups**. Enter the people or groups who you want to Single Sign-On into the application. Click **Assign** for each.
3. Verify the user-specific attributes for any people you add, and then select **Save and Go Back**.

4. Click **Done**.

Configure SAML Single Logout in Okta

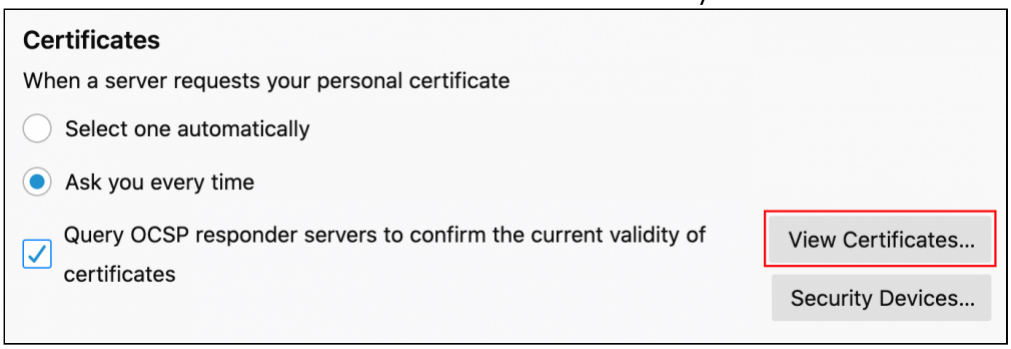
1. The configuration for Single Logout must be done in the advanced settings. On the configuration screen, click on **Show Advanced Settings**.
2. You will then see additional settings. Among them is the Single Logout.



3. Select the **Enable Single Logout** option.
4. Add the **Single Logout URL** . This is a URL that points to the SAFEQ Cloud Web UI. The "domain" host name should be the one you used for the single sign-on URL above.
5. For the **Signature Certificate** , you can use the SAFEQ Cloud Web UI public certificate. Once you have accessed the SAFEQ Cloud Web UI with your browser, the certificate is stored either in your browser or in a key chain application of your operating system. In both cases, you must export the certificate to a file and specify it here to upload.
6. With this configuration, you are automatically logged out of Okta when you click the logout button in SAFEQ Cloud Web UI.

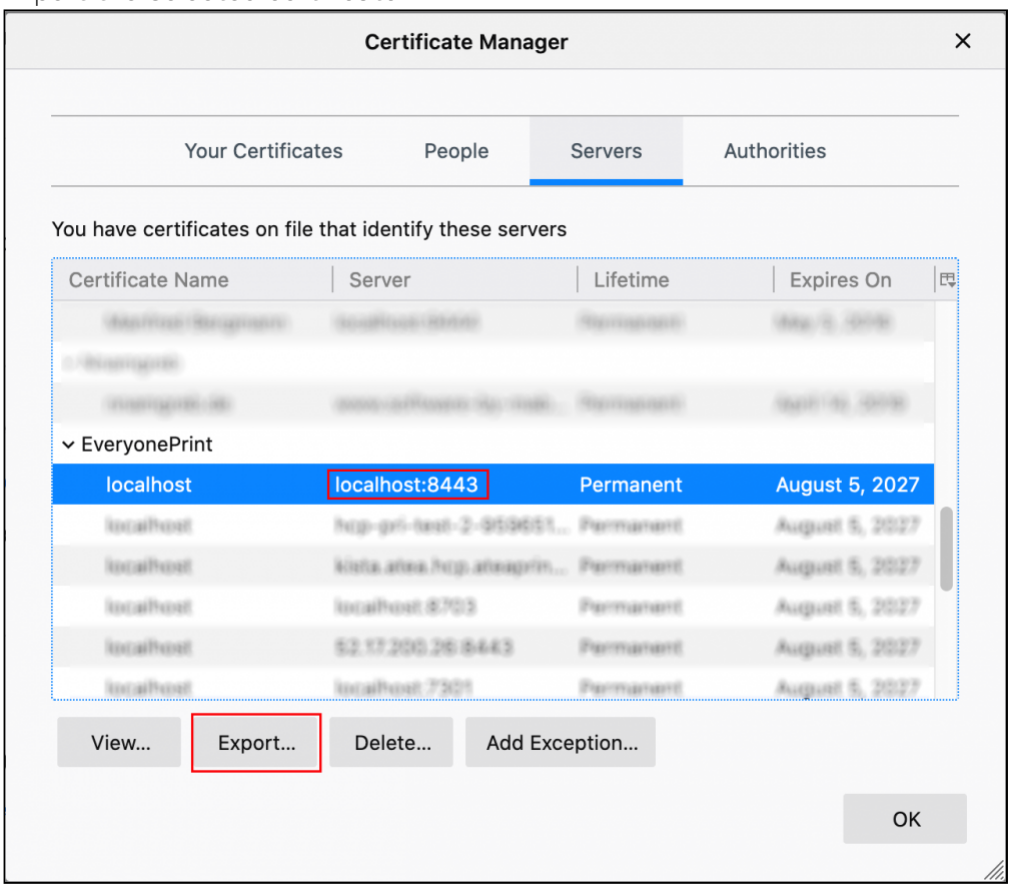
Perform the following steps to export the SAFEQ Cloud Web UI certificate from Firefox:

1. Open Firefox preferences.
2. Go to **Privacy & Security**.
3. Scroll down and click **View Certificates** under **Security** > **Certificates**.



4. Find and select the certificate for the entry with the right hostname and port 8443, which is the SAFEQ Cloud Web UI (unless your setup has a different UI port).

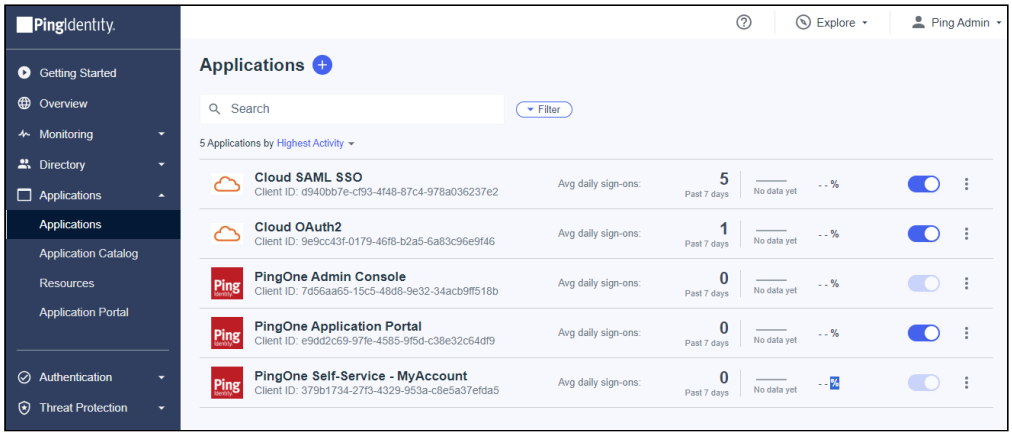
5. Export the selected certificate.



PingID Single Sign-On

To set up a single sign-on (SSO) with the PingID provider, you must create two applications in your PingID environment:

- OAuth2 Worker application for authentication and group synchronization
- SAML application for users' SSO



Overview of steps

Make sure to perform the following actions in the correct order, otherwise you might disable your existing authentication to your SAFEQ Cloud tenant. These steps are:

1. Set up the authentication provider in SAFEQ Cloud using a PingID Worker application.
2. Perform group synchronization for your PingID authentication provider.
3. Create Access Control records for the imported groups. Make sure that you will retain an administrative role in SAFEQ Cloud when you log in using your PingID identity. You must create access control records with the Administrator role for the group where you are a member.
4. Set up SAML SSO for your SAFEQ Cloud tenant.

Setting up the OAuth2 Worker application

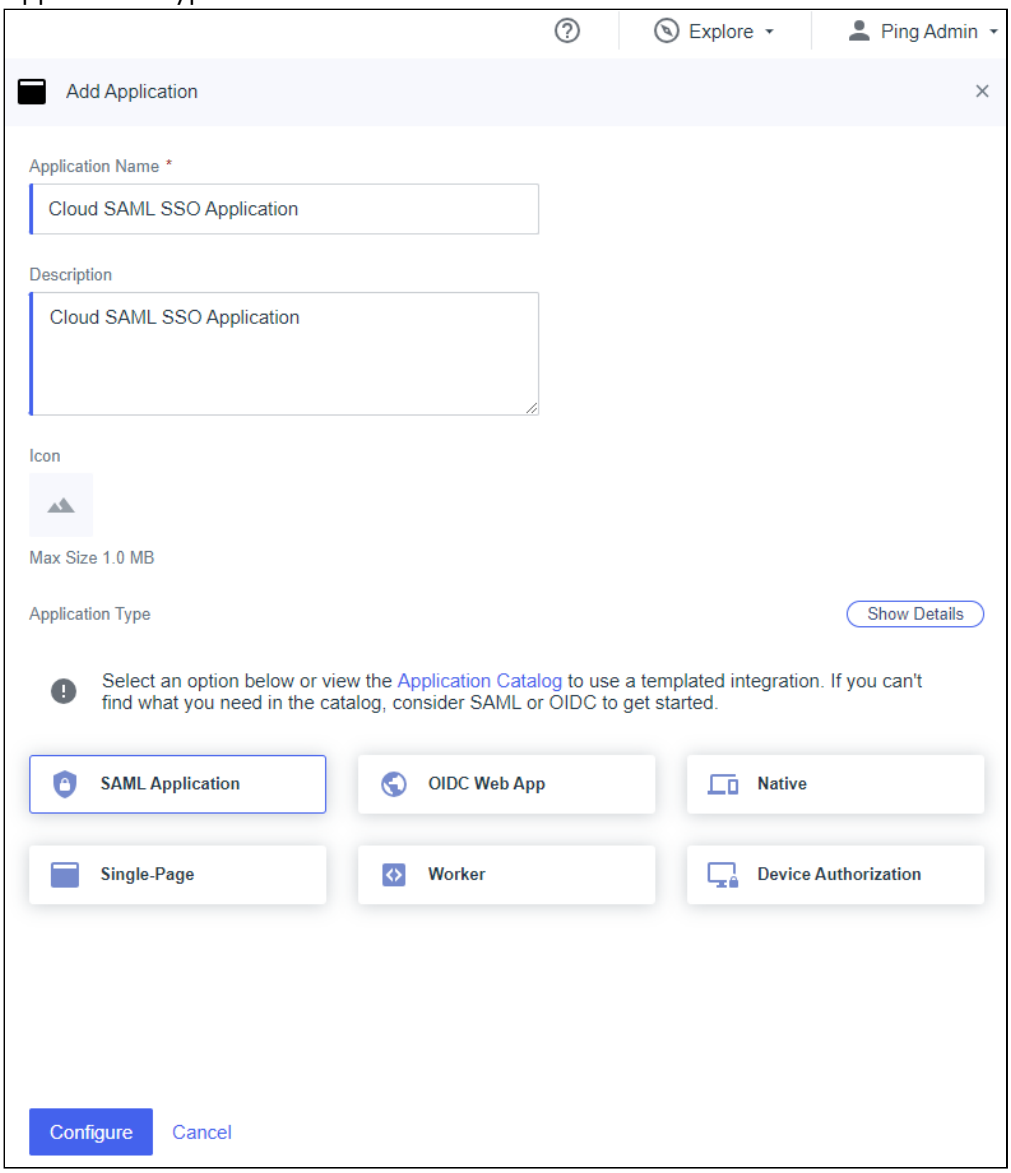
For steps 1-3 from the above overview, see Add a custom app in the Ping identity platform.

SAML Configuration

The redirect URL for the PingID SAML application is `https://<your SAFEQ Cloud domain>:8443/assertion/saml`. For example, `https://acme.eu.ysoft.cloud:8443/assertion/saml`. The port is 8443. In environments with reverse proxy infrastructure, do not specify the port number in the URL (`https://<your SAFEQ Cloud domain>/assertion/saml)`, meaning the default HTTPS port 443 will be used.

1. To create a SAML application, log into your PingID environment and go to Applications. Click + to create a new application.

2. Enter the **Application Name** , and an optional **Description**. Select **SAML Application** as the **Application Type**.

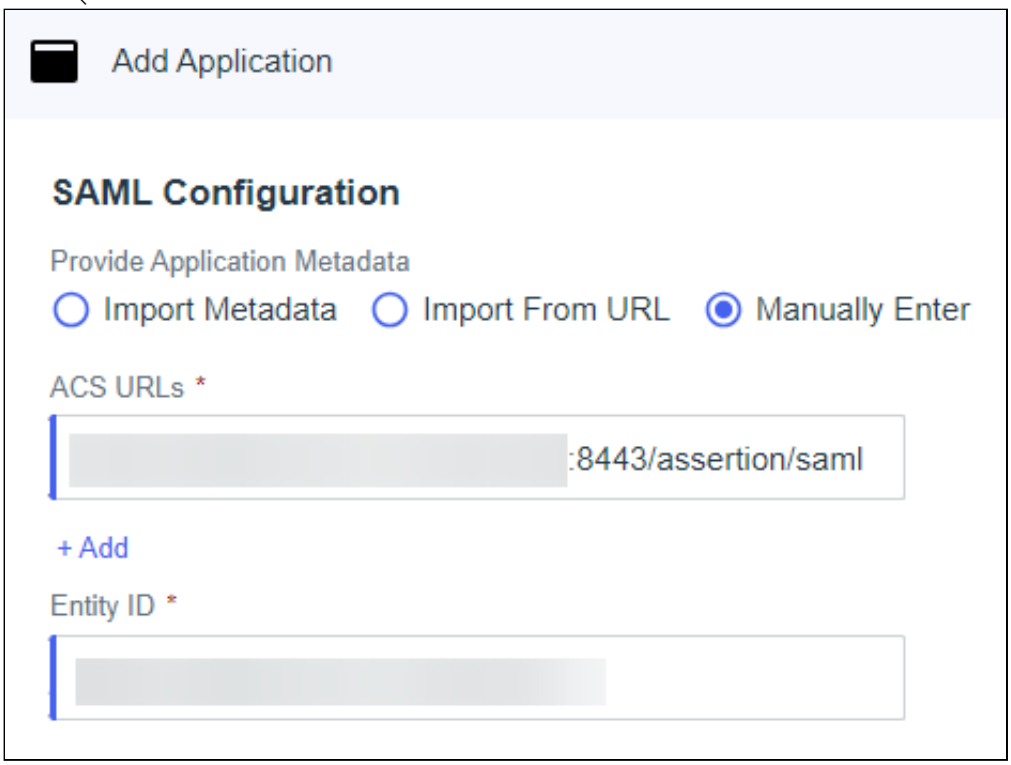


3. Click **Configure** .

4. In **Provide Metadata Configuration**, select **Manually Enter**, and add the following:

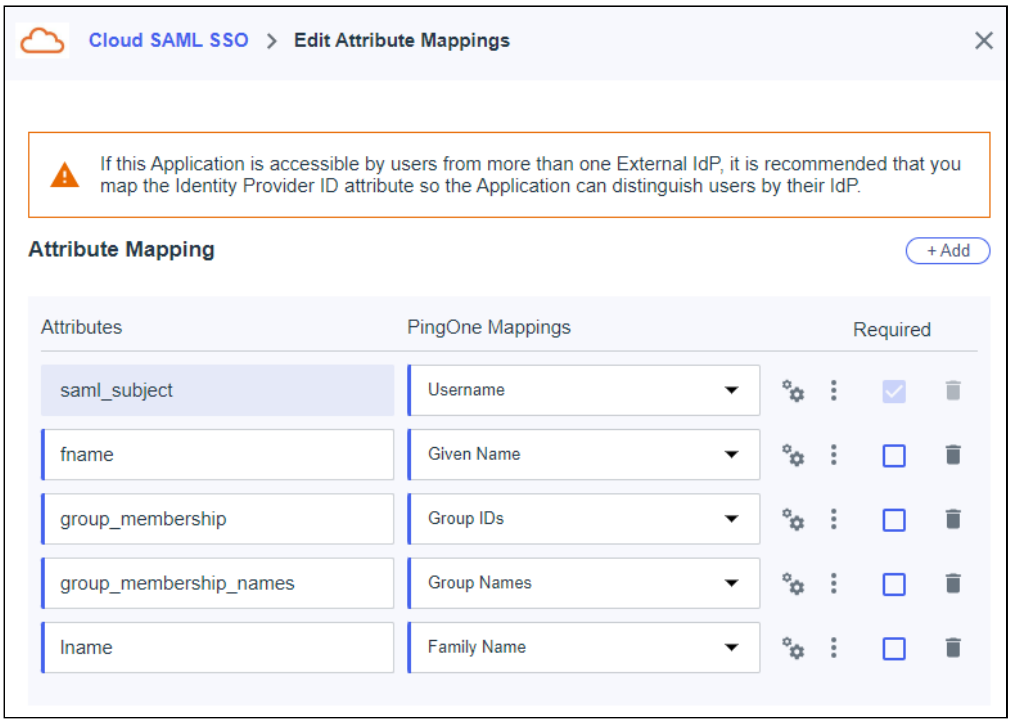
   a. In ACS URL, enter `https://<your SAFEQ Cloud domain>:8443/assertion/saml`. The port is 8443. In environments with reverse proxy infrastructure, do not specify the port number in the URL (`https://<your SAFEQ Cloud domain>/assertion/saml)` , meaning the default HTTPS port 443 will be used.

b. In **Entity ID**, enter a unique identifier for this application. We recommend you to use your SAFEQ Cloud tenant address.



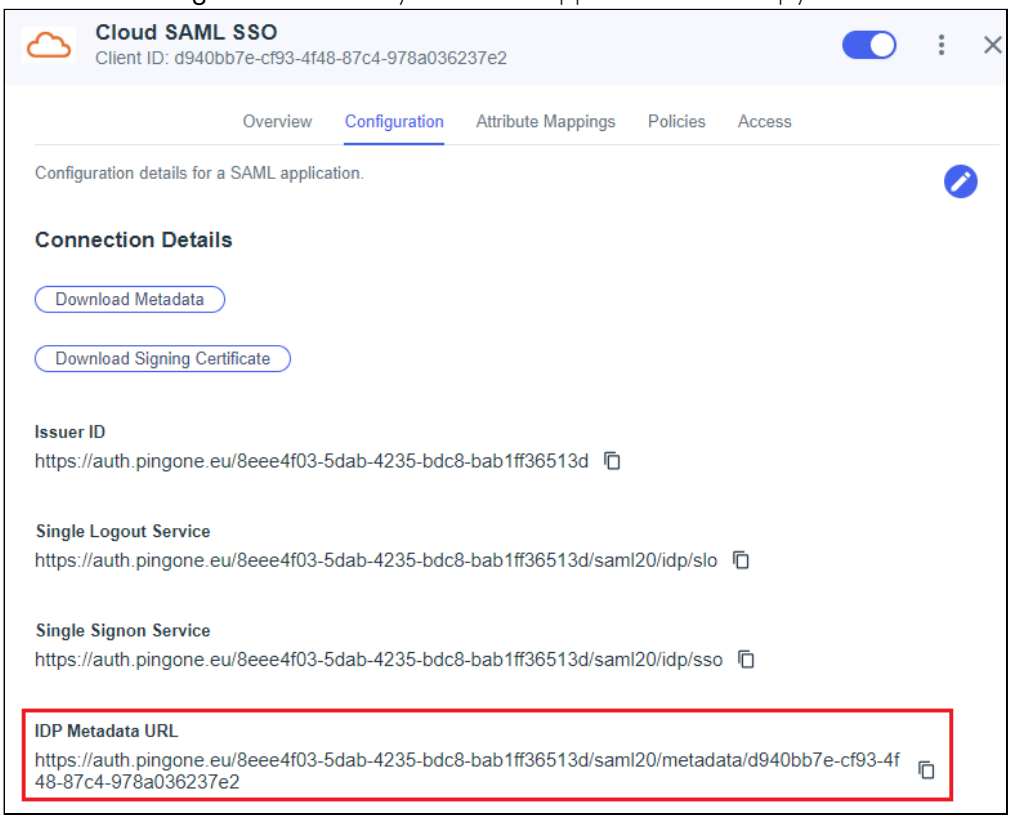
5. Next, click the **Attribute Mappings** tab and create attribute mappings as per the following table. Be aware that it is likely PingID will default the attribute **saml_subject** to **User ID** . You must change it to **Username**.

Attributes	PingOne Mappings
saml_subject	Username
fname	Given Name
group_membership	Groups IDs
group_membership_names	Group Names
lname	Family Name



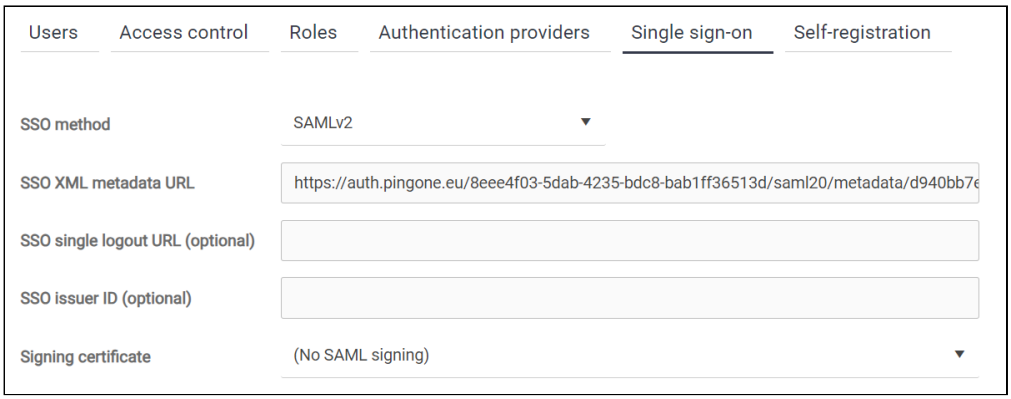
6. Once the attribute mappings are complete, enable the application using the slider in the top right of the page.

7. Click the **Configuration** tab of your SAML application and copy the **IDP Metadata URL** .



8. Log in to SAFEQ Cloud Web UI and go to **Users** page and to **Single sign-on** tab.

9. Paste the **IDP Metadata URL** into the **SSO XML metadata URL** field.



10. The **SSO issuer ID** must be the same string that you entered as the **Entity ID** in your PingID application configuration.
11. Set **SSO method** to **SAMLv2**.
12. Click **Save**.
13. Test your SSO by opening the SAFEQ Cloud Web UI login page. This will redirect you to the PingID authentication page. Log in with any user account from your PingID environment.

Every time a user logs into SAFEQ Cloud using SAML SSO, their given/family names and group membership will be synchronized from PingID.

Users

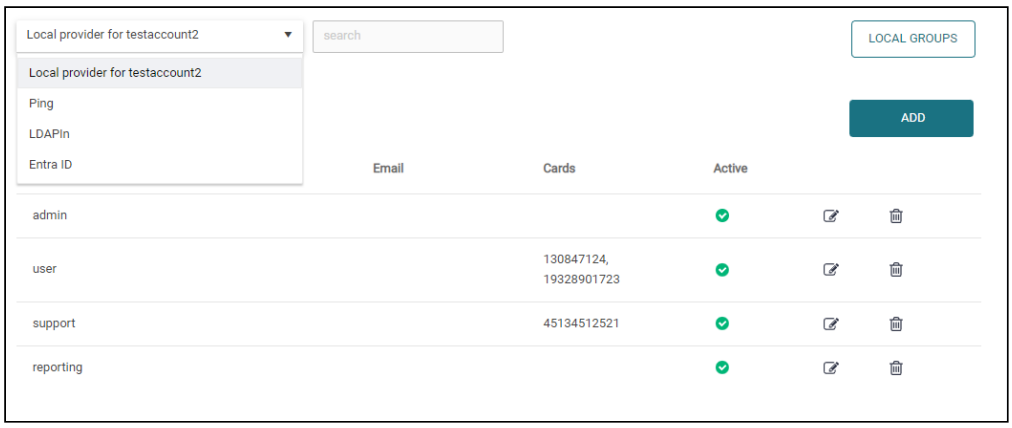
In the SAFEQ Cloud Web UI navigation menu, click **Users**.

The **Users** screen shows users that exist in the internal SAFEQ Cloud database or are synchronized from external authentication providers, such as Windows AD, LDAP, or Microsoft Entra ID.

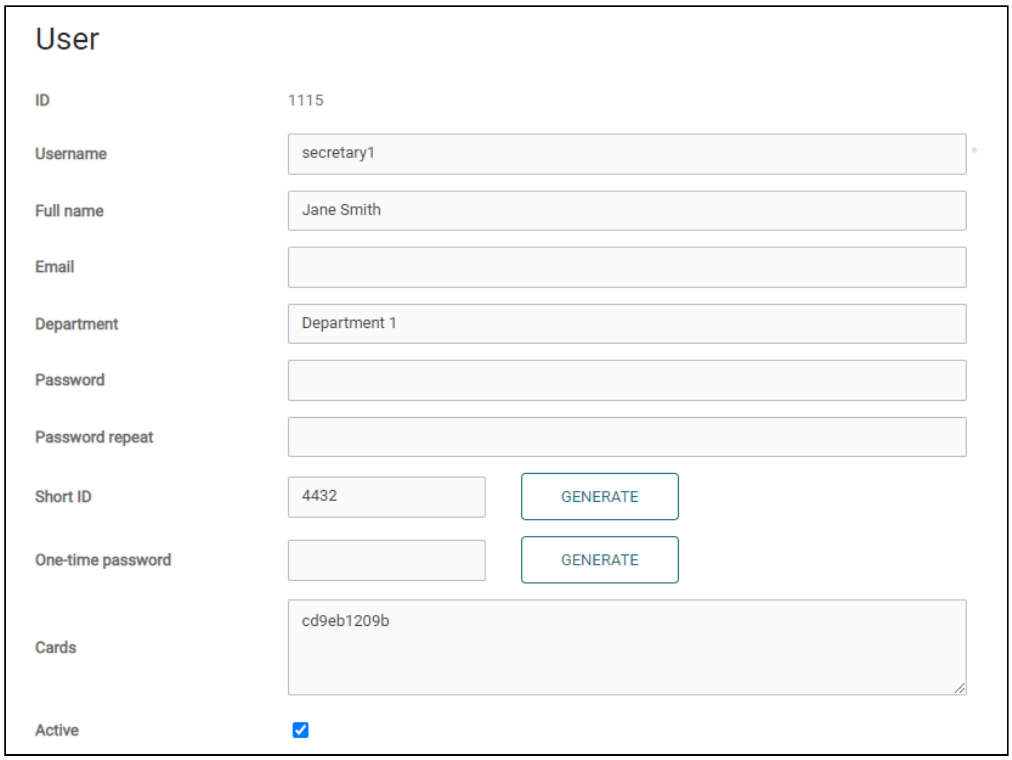
You can allow your users and guest users to self-register, see Enabling user self-registration and Guest users / guest printing.

Any user in the internal database can have rights and access alongside any externally authenticated users, from Active Directory or similar. Internal users could be separate admin accounts, other special internal accounts or temporary guest users, or similar.

> When adding a new sub-vendor or customer account, SAFEQ Cloud will automatically create 4 sample users, which can act as a starting point. To use these user accounts, click the edit icon and set a password for each of them. They can be deleted if not needed.

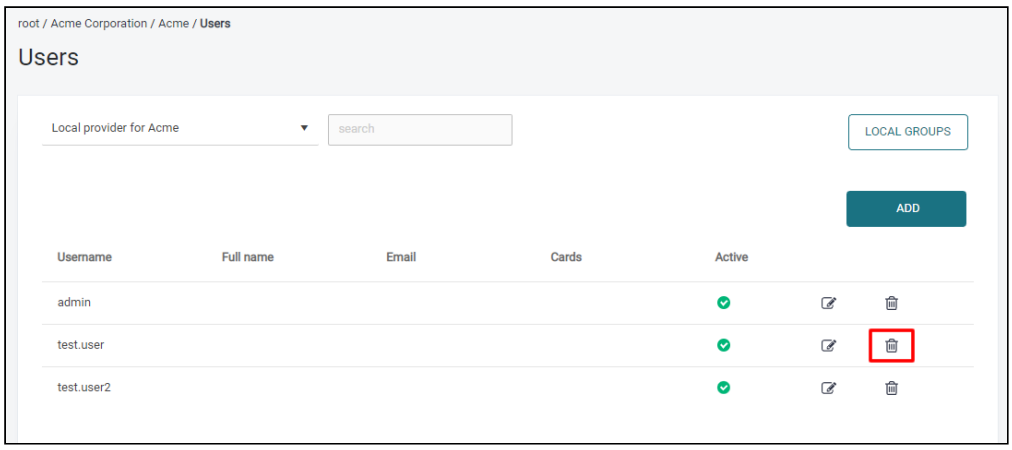


Choose the authentication provider at the top and enter even a partial username or card id to perform a search. Then click to edit the user, to manually modify attributes such as a specific user's password, short ID's or card ID's. To edit card ID's list, you must have the **CardManagement** permission.



For an external user (for example, Microsoft Entra account, a profile is sometimes created in the SAFEQ Cloud database to store specific attributes (short IDs, card ID's, etc).

To delete this profile, click the trash bin icon in the user list.



If you delete an account of a user who logged in to the SAFEQ Cloud Client and didn't log out, the user may still be able to perform user actions, such as print for up to 1 hour, due to caching on servers.

For assigning roles to users (User/Support/Reporting/Administrator or any custom role that you create), see Access Control.

For creating, editing, or deleting roles, see Roles.

Generating One-time passwords

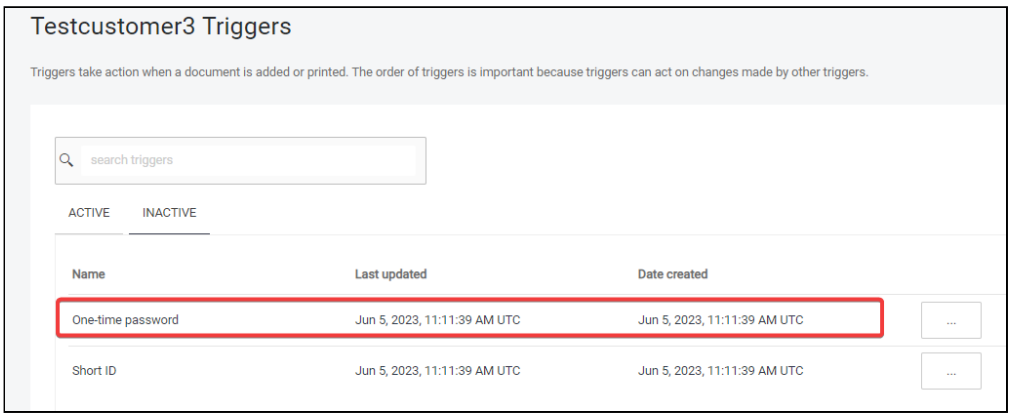
One-time passwords are useful in the following cases:

- Users can generate/view an OTP code and use it to register their cards at the MFDs.
- Administrators can set up an email with OTP to be sent to all users in the company who don't have a card associated with their account upon their first submission of a print job to a pull queue.

One-time password (or OTP) is an authentication method where the generated password can only be used once. After the user successfully authenticates with it, it is removed from their profile.

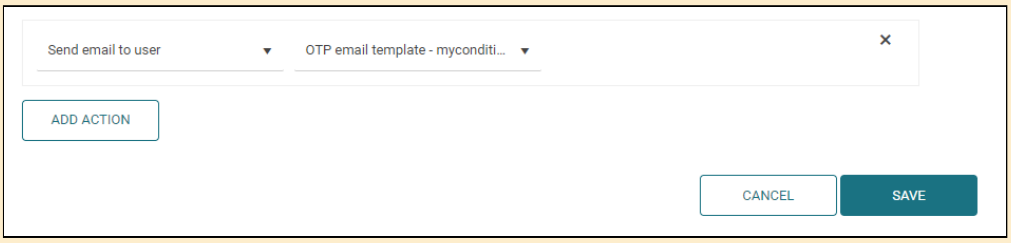
There are two ways to generate one-time passwords:

- Via the **Personal > My Profile** page in SAFEQ Cloud Web UI. The user must have the **EditMyProfile** and **GenerateOTP** permissions.
- Via a trigger rule. By default, SAFEQ Cloud Web UI has a **One-time password** trigger listed under the inactive triggers which generates OTP on a first print job that the user sends to the system and then sends this OTP to the user's email address. Activate the trigger in order to make it operational.



For the email sent, the following conditions must be met:

- At least one valid messaging configuration is defined in the **Settings > General settings > Messaging** section.
- At least one messaging template is defined in the **Settings > General settings > Templates** section.
- A combination of messaging config and template is selected in the **Send email** trigger action.



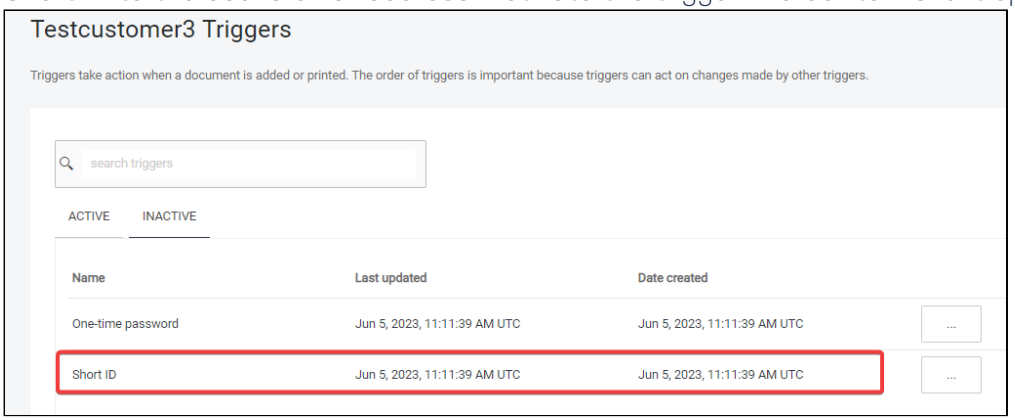
SAFEQ Cloud Web UI contains a sample OTP template and sample messaging config. They are also pre-selected in the trigger configuration so the administrator needs only to edit the messaging config to adjust the SMTP address and other parameters.

Generating Short IDs

Short IDs can be used for authentication at embedded terminals.
The ways to generate a short ID:

- Via the **Personal > My Profile** page in SAFEQ Cloud Web UI. The user must have the **EditMyProfile** and **GenerateShortID** permissions.
- Via a trigger rule. For example, when the users submits their first print job to SAFEQ Cloud. By default, SAFEQ Cloud Web UI has a **Short ID** trigger listed under the inactive triggers which generates a short ID on a first print job that the user sends to the system and then sends this

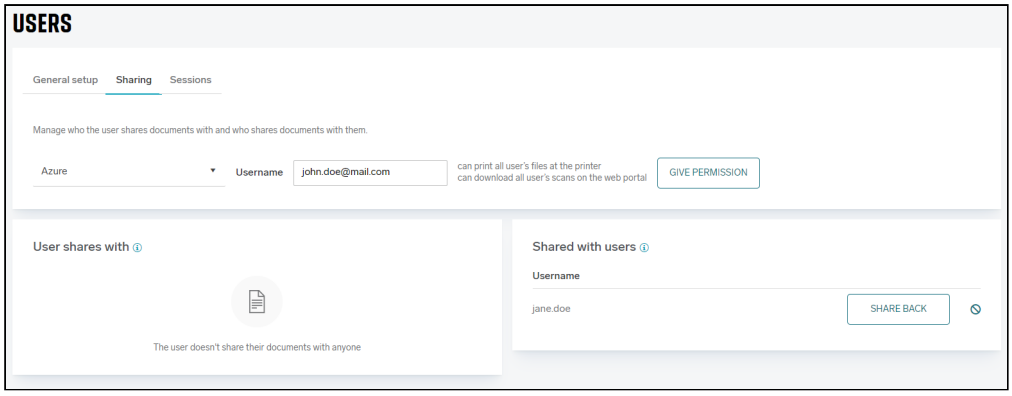
Short ID to the user's email address. Activate the trigger in order to make it operational.



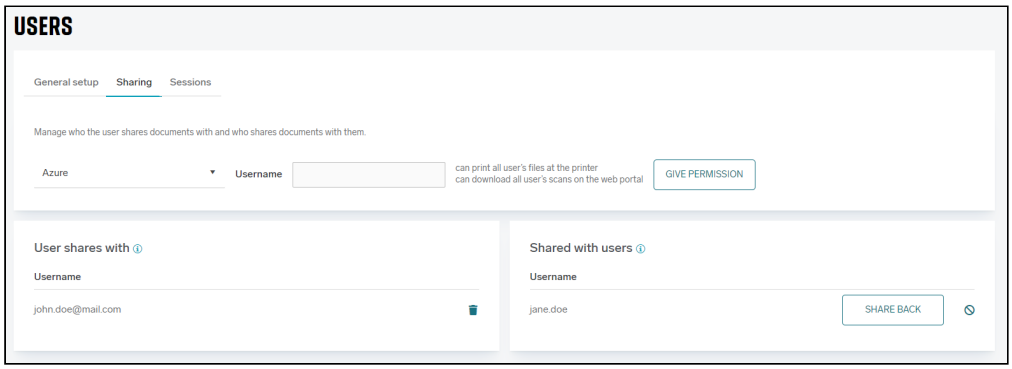
Sharing

In the **Sharing** tab you can add sharing permission to other users, so they can see and print/ download this user documents/scans.

You can add users with whom you want the edited user to share their documents by selecting authentication provider, typing username and clicking on **Give permission** button.



In the bottom part of the page you have two lists which show with whom the edited user is currently sharing their documents and who is sharing theirs with them.

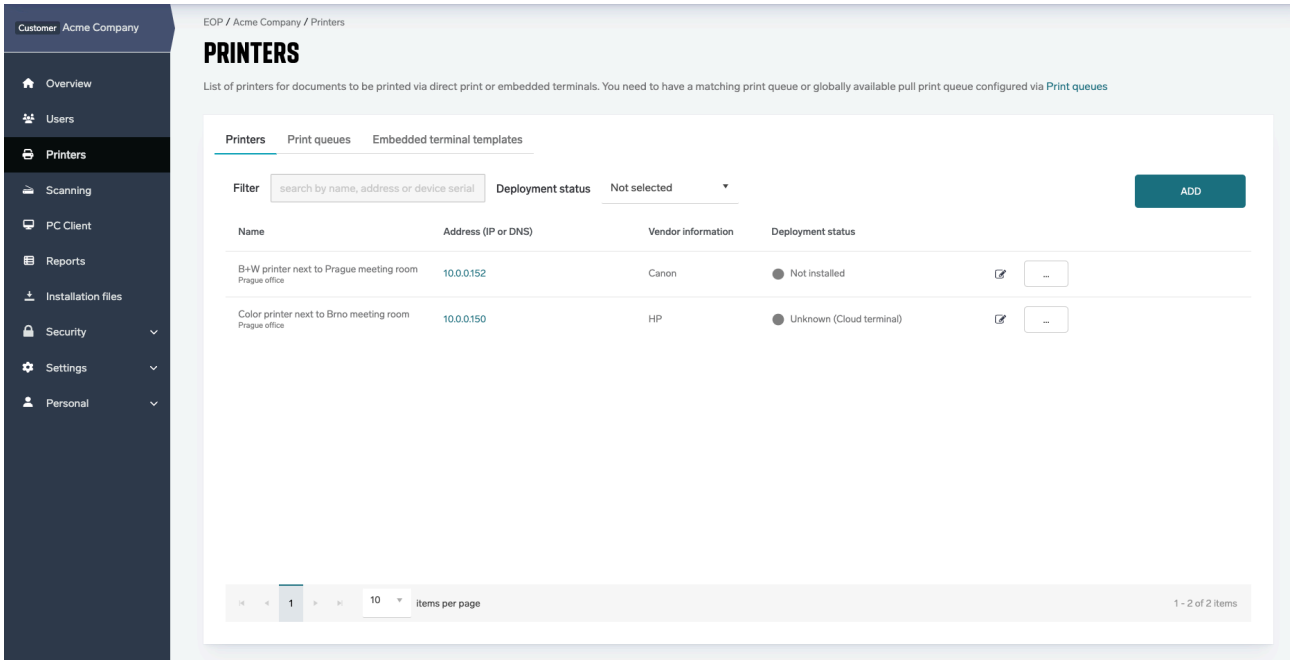


You can remove these sharing permissions by clicking the **delete/deny** buttons. You can also use **Share back** button to quickly create reverse sharing permission with that user.

To see this panel you must have the **ViewUserSharingDocuments** permission and to add or remove sharing permission you must have **ModifyUserSharingDocuments** permission.

8.1.3 PRINTERS MENU

In the **Printers** menu, you can configure **Printers, Print queues** and **Embedded terminal templates** for terminals.



Embedded Terminals

This section contains guides for configuring all terminals supported in SAFEQ Cloud. It is divided according to MFD brands. For some brands, there are only terminals that can connect to the cloud via a secondary gateway only. For some brands, there are also terminals that can connect to the cloud directly (pure cloud terminals).

Pure cloud terminals

For pure cloud terminals, the guide for each MFD brand consists of the following sections:

- Prerequisites
- Limitations
- Device setup
- Cloud Terminal installation
- Registering the Cloud Terminal in the SAFEQ Cloud Web UI
- Adding a printer and Embedded configuration in SAFEQ Cloud Web UI
- Post-installation device setup (necessary only for Fujifilm BI)

Terminals that require a secondary gateway

In general, for terminals that require a secondary gateway, the process of installation consists of the following steps:

1. Do the Secondary Gateway mapping (if not done already).

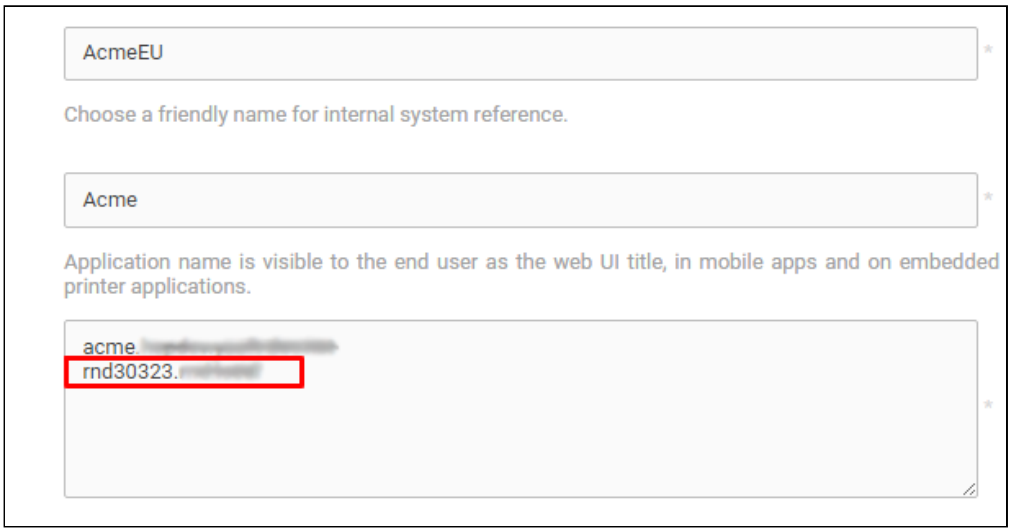
2. Add your MFD(s) to SAFEQ Cloud Web UI. See Printers.
3. Do the MFD-specific setup. The steps and prerequisites are listed in the guide for each terminal.
4. Add an embedded configuration in SAFEQ Cloud Web UI and deploy it to your MFD(s). See Embedded Terminals' configuration.

Secondary Gateway mapping

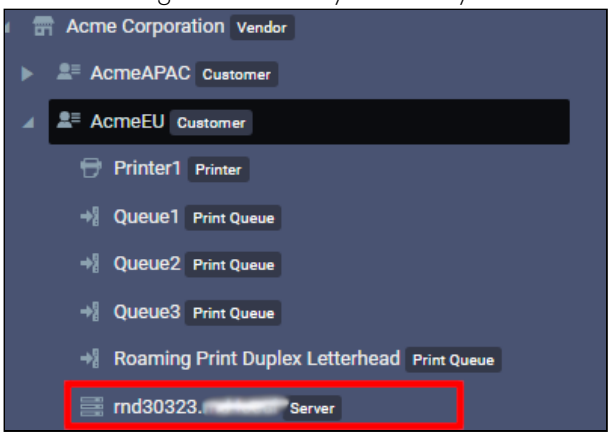
Perform the following steps to configure the Secondary Gateway for use with Embedded terminals:

1. Log in to the SAFEQ Cloud Web UI with your administrator account.
2. In the SAFEQ Cloud tree, select the customer account which contains the Secondary Gateway you wish to configure.
3. Go to **Settings** > **Customer account**.
4. Add the IP address or a domain name of the Gateway to **Domains** on a new line and click **Save.**

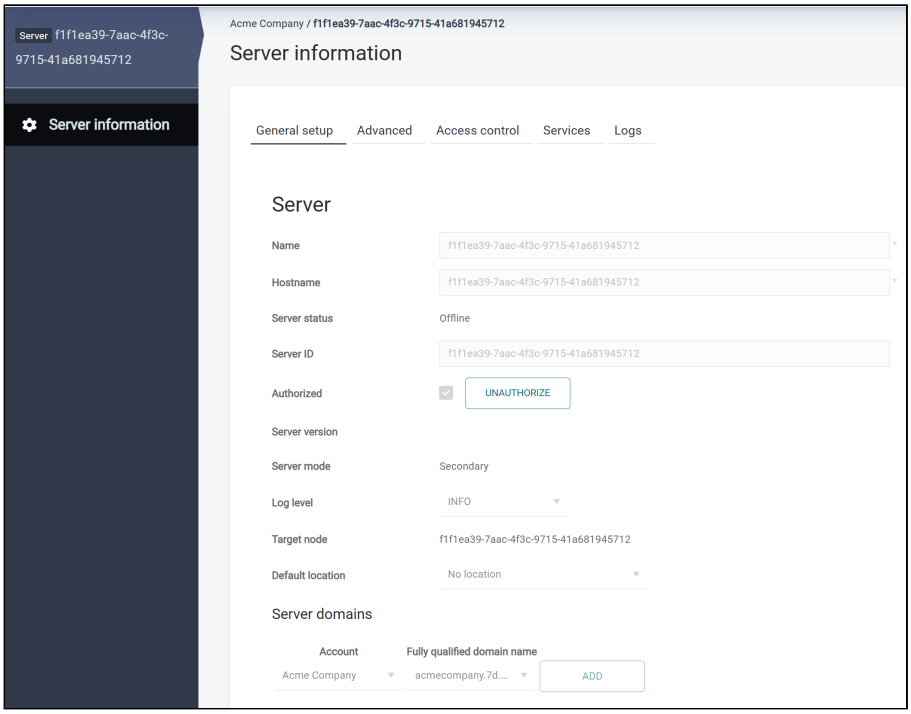
> Whether to use a domain name or IP address for the secondary gateway depends on your MFD vendor.
> - For HP, Ricoh, and Brother) use a domain name.
> - For Canon, use an IP address.
> - For the rest of vendors, we recommend using the domain name.



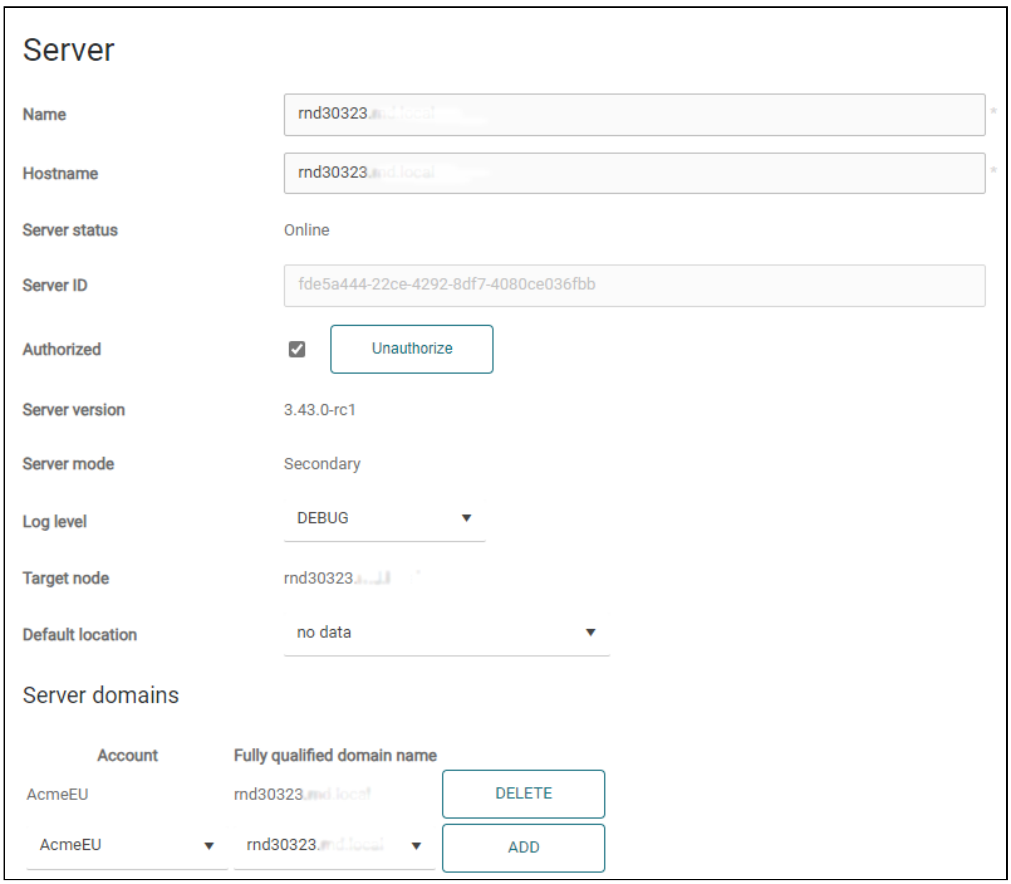
5. The next step is mapping this Secondary Gateway to your account. In the SAFEQ Cloud tree, click the target Secondary Gateway node.



6. Click **Server information**.



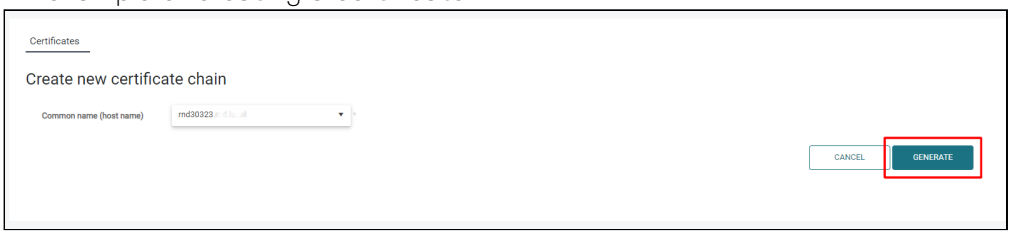
7. In the **Server domains** section, choose the IP address or domain name from the FQDN drop-down list that you've previously entered in the **Customer account** section. After your selection, click **Add**. If the row is created correctly, the **Add** button will change to **Delete** button. This is what the page will look like before saving:



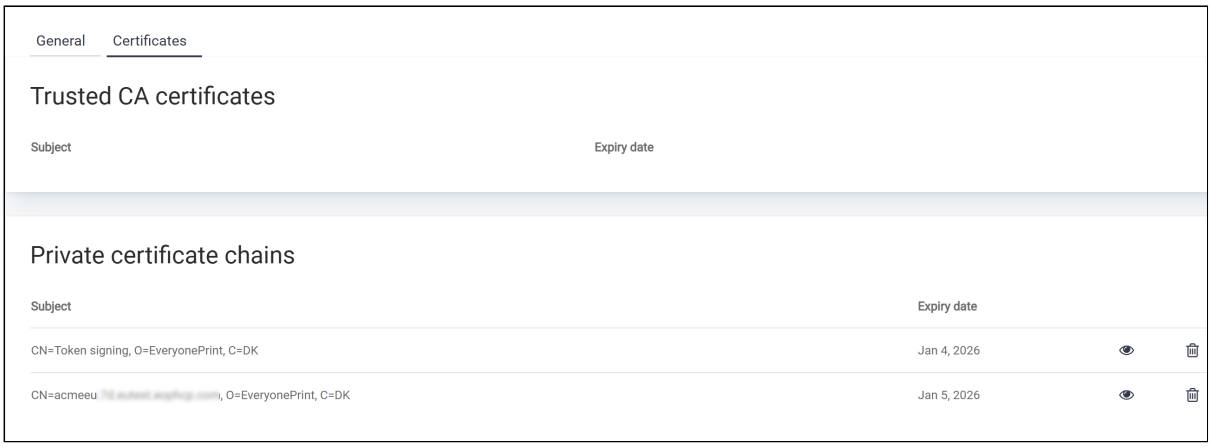
Map only one address for each gateway. You may use the same name for several secondary gateways if you use load balancing.

8. Click **Save**.

9. Go to **Security > Security options** and click the **Certificates** tab. In the **Private certificate chains** section, create or import an SSL certificate for the mapped address.
   - An example of creating a certificate:



10. The result will look like this:

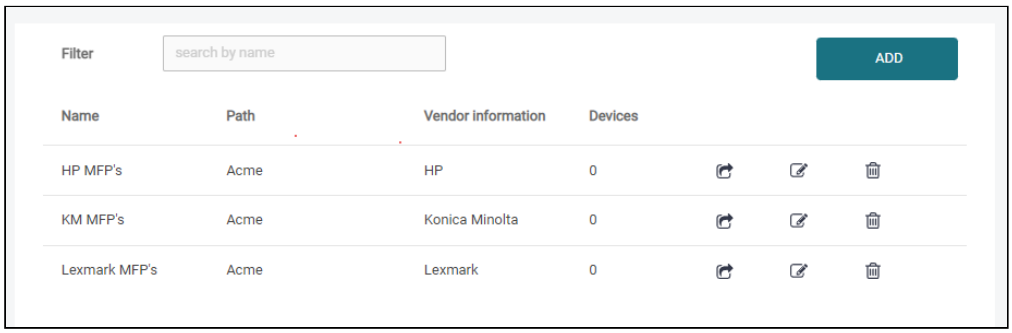


After performing the above steps, you should be able to successfully deploy the embedded client from the specific Embedded configuration screen.

Embedded Terminals' configuration

Before you can install a terminal on an MFD, you must create a configuration for it. This is done in the **Printers > Embedded terminal templates** section of SAFEQ Cloud Web UI. You can have any number of configurations, for example, one configuration for MFDs at one site, and another configuration for MFDs of the same brand at another site.

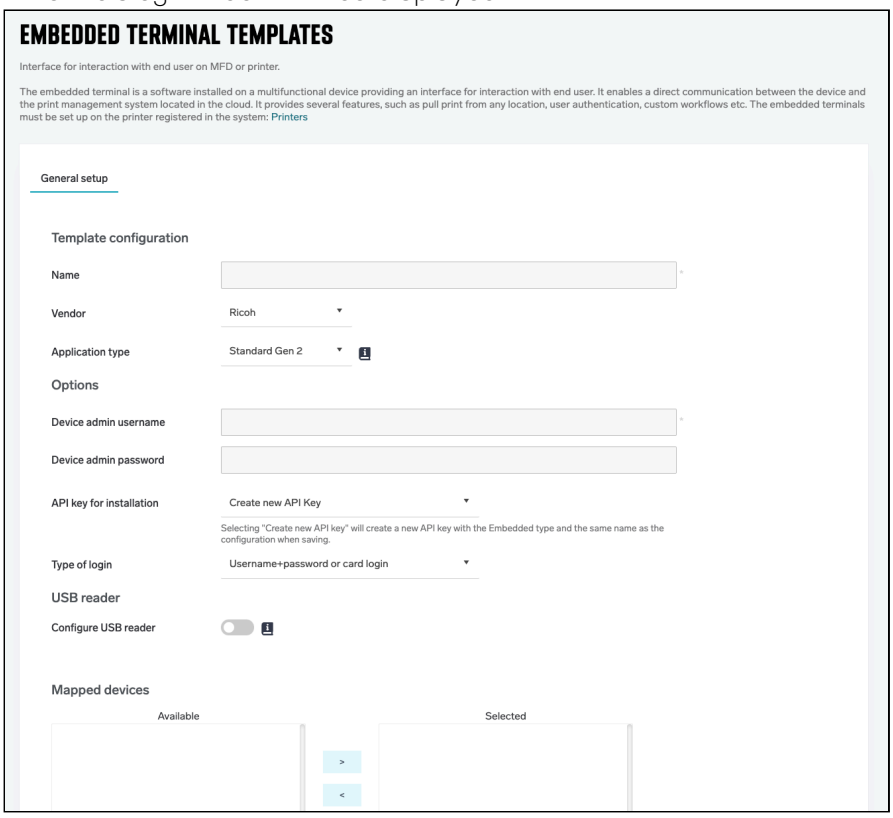
You can use the **Filter** field to search for the already created terminals.



Creating a new embedded configuration

1. Log in to the SAFEQ Cloud Web UI and click **Printers > Embedded terminal templates** tab.
2. Click **Add**.

3. A new dialog window will be displayed.



4. The available options depend on the MFD vendor selected. The general options are:
   - **Device admin username** – user name of the device administrator account
   - **Device admin password** – password of the device administrator account
   - **Automatic logout timeout** – timeout for automatic user logout due to inactivity, in seconds
   - **Print all jobs on card login** – release all jobs from the Pull print queue upon user authentication
   - **Trim zeroes from card ID** – remove leading zeroes from cards upon authentication or card self-enrollment

5. In **Mapped devices**, select the MFD where you want to use the configuration. Alternatively, you can add devices later on if you haven't added them to SAFEQ Cloud yet. For adding printers, see Printers.

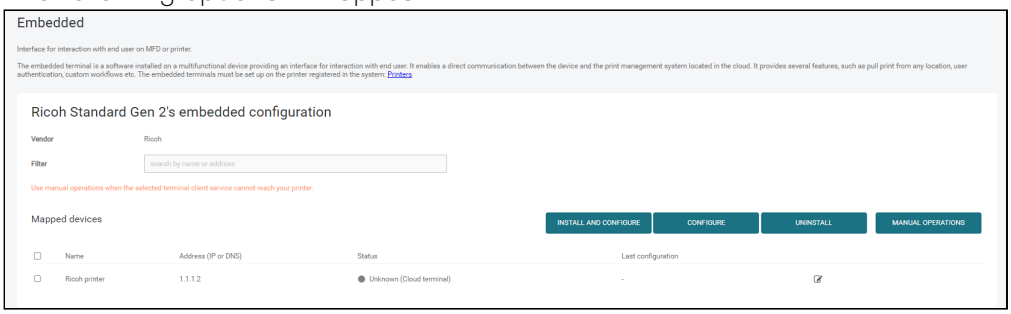
   > If you don't see a particular MFD in the list of available devices, make sure you have configured the Terminal Client Service and that you have enabled the **At printer (Embedded terminal)** release option in the settings of the respective MFD in the **Printers** section of SAFEQ Cloud Web UI.

6. Click **Save**.

Deploying the configuration

1. After you have created the configuration, click the deploy icon .

2. The following options will appear:



a. **Install and Configure** – Deploys (or re-deploys) the embedded application and sets configuration.

b. **Configure** – Sets configuration on previously deployed embedded application.

c. **Uninstall** – Uninstalls the embedded application from the device.

d. **Manual operations** – Describes manual installation steps and links to the documentation.

Terminal Deployment Tool

This tool can only be used to install FUJIFILM BI Terminal, Ricoh Standard Gen 2 Cloud Terminal, Xerox Gen 2 Cloud Terminal and the Sharp Gen 2 Cloud Terminal.

For the FUJIFILM BI Cloud Terminal installation, the tool only works in MS Windows.

Please note that Sharp Cloud Terminal installation is currently in beta phase.

Preparation

For Windows, built-in JAVA is always used, therefore you can skip this step.

- For macOS, it's recommended to have JAVA 11 installed.

  If you want to use built-in JAVA, you must allow libraries `System Preferences > Security & Privacy > Allow Anyway` next to the library name.

- To verify the version, use the `java -version` command in the cmd line/terminal.

```
> java -version
java version "11.0.16.1" 2022-08-18 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.16.1+1-LTS-1)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.16.1+1-LTS-1, mixed mode)
```

- To install Java (optional):
  - on macOS, use Homebrew.
  - on Linux, use `apt-get`.

Prerequisites

The device must be set up according to documentation before using this tool.

If you are installing Ricoh Cloud Terminal against a cloud solution that does not have a publicly trusted Certificate Authority, you need to run the "fetch-certificate" command in your Terminal Deployment Tool. See the *Advanced commands* section below for this function's description and examples.

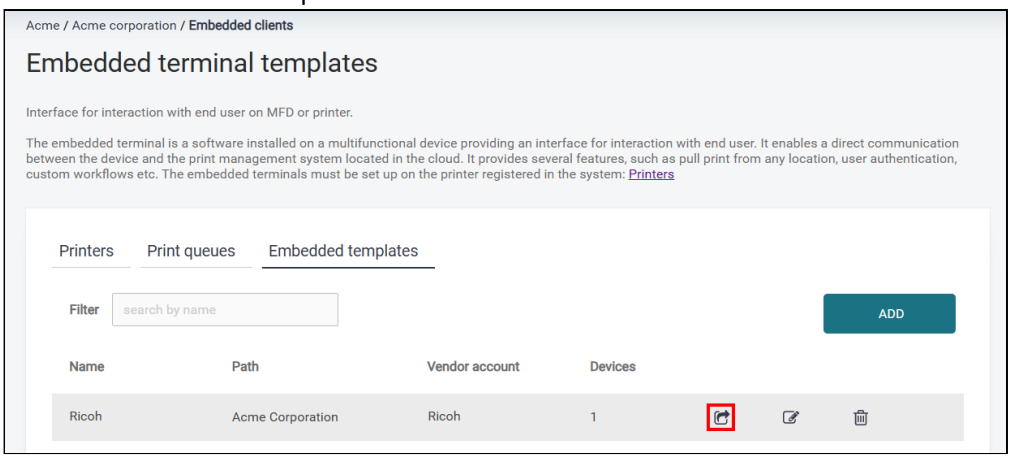
Terminal Deployment Tool options

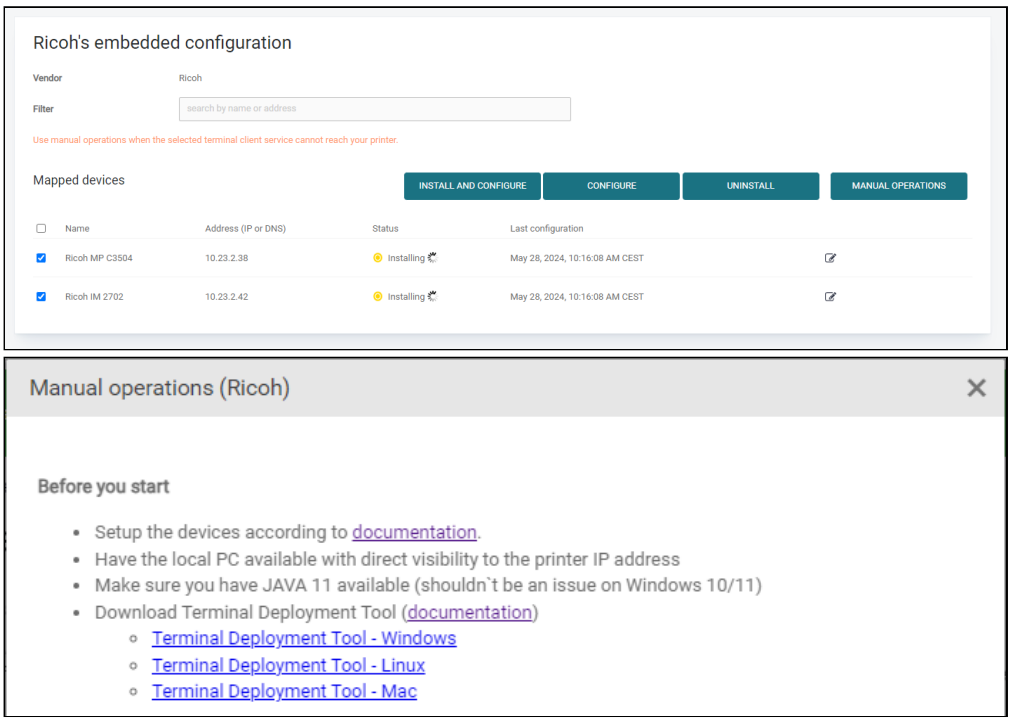
When installing Ricoh Cloud Terminal against an on-premise solution, you can use the deployment tool to push your Certificate Authority to the printer so it will trust your site server. This is only needed when you use a certificate that is not signed by a publicly trusted CA. For how to create and import this CA, see the `CustomCA-README` file located in `<your deployment tool location>\certificates`.

Using Terminal Deployment Tool

Terminal Deployment Tool is available on SAFEQ Cloud Web UI.

1. Deployment tool archive can be downloaded:
   a) Vendor can download it from main menu > Installation files
   b) Customer can download it from main menu Printers > Embedded templates > Deployment action icon > Manual Operations





2. Download an archive according to your operating system.
3. Extract the archive.
4. Run command line / terminal from the root folder of the extracted Terminal Deployment Tool archive.
5. Use commands and parameters from the following sections.

Basic commands

INSTALL

Installs Cloud Terminal to target MFD, configures it, and performs any necessary configuration on the device, such as SP options, or authentication settings.

Mandatory parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Supported vendor values (*case insensitive*): • `RICOH` • `FUJIFILMBI` • `XEROX` • `SHARP`

Short parameter	Long parameter	Description	Note
-i	--ip	MFD IP address	
-a	--apikey	API key	API key obtained from your SAFEQ Cloud account
-m	--server-domain	Server Domain	The domain of the server to which the Cloud Terminal will connect. It can be either the domain of the cloud primary server or the domain of a local gateway. Example: • customer.ap.ysoft.cloud • 10.22.56.21
-u	--username	MFD admin username	
-p	--password	MFD admin password	

Optional parameters

Short parameter	Long parameter	Description	Note
-f	--force-reinstall	Uninstalls the application's prior installation.	This also removes application data. You will need to do the device code flow again. The parameter works for Ricoh and Sharp terminals only. Examples: install RICOH -f -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> install SHARP -f -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -a <API_KEY>

Short parameter	Long parameter	Description	Note
	--vid	VID for card reader configuration. Skip the parameter if you do not wish to do card reader configuration. Set an empty string to configure the USB Reader set in the configuration properties.	Ricoh terminal only. Example: • install RICOH -f -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> --vid=<CARD_READER_VID> --pid=<CARD_READER_PID> • install RICOH -f -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> --vid="" --pid=""
	--pid	PID for card reader configuration. Skip the parameter if you do not wish to do a card reader configuration. Set empty string to configure USB Reader set in configuration properties.	Ricoh terminal only. Example: • install RICOH -f -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> --vid=<CARD_READER_VID> --pid=<CARD_READER_PID> • install RICOH -f -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> --vid="" --pid=""

Short parameter	Long parameter	Description	Note
-hkm	--home-key-mode	Home key mode specifies behaviour of the home key. Possible values: 'general' for General mode, 'change' for UI change mode, 'off' to disable home key configuration. Default is 'general'.	Ricoh terminal only. Example: • install RICOH -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -hkm general • install RICOH -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -hkm general
-cd	--cloud-domain	Specifies the cloud domain of the tenant. Use this parameter only if you are configuring Xerox Terminal to connect a gateway. If specified, this value must reflect the domain of your primary server.	Xerox terminal only. Example: install XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -cd <CLOUD_DOMAIN> -a <API_KEY>

Short parameter	Long parameter	Description	Note
-k		Enables the kiosk mode for Xerox MFDs. This causes all applications, other than the Cloud Terminal and Jobs to be locked and hidden during the installation. If you wish to leave a specific application accessible, modify **xeroxKioskAllowList** in the configuration.properties file. Alternatively you can also run the set-app-access command afterwards to set access to specific applications.	Xerox terminal only. Example: install XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -cd <CLOUD_DOMAIN> -a <API_KEY> -k
-scp	--skip-card-plugin	Skips card plugin installation and disabling of Xerox card plugins during installation on VersaLink Gen 2 devices.	Xerox terminal only. Example: install XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -cd <CLOUD_DOMAIN> -a <API_KEY> -scp
-sp	--skip-proxy-configuration	Skips disabling of EiP Proxy on Xerox Altalink devices during installation	Xerox terminal only. Example: install XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -cd <CLOUD_DOMAIN> -a <API_KEY> -sp

Short parameter	Long parameter	Description	Note
-tap	--terminal-admin-password	Sets custom password for accessing terminal application settings on MFD. If not provided, default value of "Sharp123" is used.	Sharp terminal only. Example: install SHARP -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -a <API_KEY> -tap <TERMINAL_ADMIN_PASSWORD>
-cre	--card-reader-enabled	Enables or disables card reader on MFD. If not provided, default value is true (enabled).	Sharp terminal only. Example: install SHARP -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -a <API_KEY> -cre **false** During installation, card reader authentication is enabled on the MFD by default. If you do not have a card reader connected to the device, always specify *-cre false* parameter, otherwise native error "Can not recognize a card reader" will appear on the MFD panel and it will not be usable.

Short parameter	Long parameter	Description	Note
-pd	--packages-directory	Sets custom directory, from which the terminal packages for installation will be taken (files "SafeqCloudAuth.emo" and "SafeqCloudTerminal.emo"). When not specified, latest terminal packages will be downloaded from CDN and used to install the terminal.	Sharp terminal only. Example: install SHARP -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -m <GATEWAY_DOMAIN> -a <API_KEY> -pd "C:\Temp\Sharp packages"

Optional URL override parameters

Paths to all the needed services are resolved automatically from the `--server-domain` parameter. In case of non-standard deployment, individual paths can be overridden using:

Short parameter	Long parameter	Description	Note
-s	--sqts	Cloud Terminal API URL	Example: • https://customer.ap.safeq.cloud:8705
-d	--idm	Authorization Service URL	Example: • https://customer.ap.safeq.cloud:7400/oauth/v1
-w	--scan	Scan server URL for document delivery	FUJIFILM BI Terminal only Example: • https://customer.ap.safeq.cloud:8707

Command examples

- Ricoh

```
.\terminaldeploymenttool INSTALL RICOH -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- FUJIFILM BI (Cloud print method will be used as a default)

```
.\terminaldeploymenttool INSTALL FUJIFILMBI -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- Xerox

```
.\terminaldeploymenttool INSTALL XEROX -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- Sharp

```
.\terminaldeploymenttool INSTALL SHARP -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

UNINSTALL

Uninstalls an already installed Cloud Terminal.

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Supported vendor values (case insensitive): • `RICOH` • `FUJIFILMBI` • XEROX • SHARP
-i	--ip	MFD IP address	
-p	--password	MFD admin password	
-u	--username	MFD admin username	

Optional parameters

Short parameter	Long parameter	Description	Note

-k	--unlock	Specifies which mode should be used to modify application access after the Cloud Terminal is uninstalled.	XEROX Terminal only
			
			Supported values:
			• restore
			  • Selected by default (when not specified). Restores the previous app states saved during installation with kiosk mode. For more information, see kiosk mode option for the install command.
			• unlockAll
			  • Unlocks all installed applications on the device, including the native ones.
			• lockAll
			  • Locks all installed applications on the device, including the native ones.
			• unlockNative
			  • Unlocks just a set of native applications. Other applications remain untouched
			  • Unlocks: Jobs, Copy, Email, Fax, ScanTo and USB

Command examples

- Ricoh

```
.\terminaldeploymenttool UNINSTALL RICOH -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- FUJIFILM BI

```
.\terminaldeploymenttool UNINSTALL FUJIFILMBI -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

After uninstalling FUJIFILM BI Cloud Terminal from a device, "Authentication/Accounting Type" should be set to "Off".

Follow the process described in FUJIFILM BI Terminal , section *Turn on custom service authentication on the device,* where you change the custom method to "Off" value.

- Xerox

```
.\terminaldeploymenttool UNINSTALL XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p
<MFD_ADMIN_PASSWORD>
```

- Sharp

```
.\terminaldeploymenttool UNINSTALL SHARP -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p
<MFD_ADMIN_PASSWORD>
```

CONFIGURE

Configures or re-configures an already installed Cloud Terminal.

Mandatory parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Supported vendor values (case insensitive): • `RICOH` • `FUJIFILMBI` • `XEROX` • `SHARP`
-i	--ip	MFD IP address	
-a	--apikey	API key	API key obtained from your SAFEQ Cloud account.
-m	--server-domain	Server Domain	The domain of the server to which the Cloud Terminal will connect. It can be either domain of a cloud primary server or the domain of a local gateway. Example: • customer.ap.ysoft.cloud • 10.22.56.21
-u	--username	MFD admin username	
-p	--password	MFD admin password	

Optional parameters

Short parameter	Long parameter	Description	Note
-tap	--terminal-admin-password	Custom password for accessing terminal application settings on MFD. If not provided, default value of "Sharp123" is used.	Sharp Terminal only Needs to be specified in case terminal was installed with a custom terminal admin password value.
-cre	--card-reader-enabled	Enables or disables card reader on MFD. If not provided, default value is true (enabled).	Sharp Terminal only If specified, card reader can be enabled or disabled on MFD using this parameter (value true/false).

Optional URL override parameters

Paths to all the needed services are resolved automatically from the `--server-domain` parameter. In case of non-standard deployment, individual paths can be overridden using the following parameters:

Short parameter	Long parameter	Description	Note
-s	--sqts	Cloud Terminal API URL	Xerox terminal is not supported. Example: • https://customer.ap.safeq.cloud:8705
-d	--idm	Authorization Service URL	 Example: • https://customer.ap.safeq.cloud:7400/oauth/v1

Short parameter	Long parameter	Description	Note
-w	--scan	Scan server URL for document delivery	FUJIFILM BI Terminal only Example: • https://customer.ap.safeq.cloud:7400/oauth/v1

Command examples

- Ricoh

```
.\terminaldeploymenttool CONFIGURE RICOH -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- FUJIFILM BI

```
.\terminaldeploymenttool CONFIGURE FUJIFILMBI -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- Xerox

```
.\terminaldeploymenttool CONFIGURE XEROX -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- Sharp

```
.\terminaldeploymenttool CONFIGURE SHARP -i <MFD_IP_ADDRESS> -m <SERVER_DOMAIN> -a <API_KEY> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

HELP

Displays help information about the specified command.

Command example

```
.\terminaldeploymenttool HELP INSTALL
```

Advanced commands

These commands are meant for more experienced users and are not commonly used. For general issues, it is recommended to uninstall and install the Terminal again.

RESTART

Reboots the MFD.

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported (case insensitive): • `RICOH` • `FUJIFILMBI` • `XEROX (except for AltaLink devices)` • `SHARP`
-i	--ip	MFD IP address	
-p	--password	MFD admin password	
-u	--username	MFD admin username	

Command example

- Ricoh

```
.\terminaldeploymenttool RESTART RICOH -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- FUJIFILM BI

```
.\terminaldeploymenttool RESTART FUJIFILMBI -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- Xerox

```
.\terminaldeploymenttool RESTART XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

- Sharp

```
.\terminaldeploymenttool RESTART SHARP -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

Advanced commands for Ricoh

CONFIGURE-SP-OPTIONS

Set SP options of the device.

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported (case insensitive): `RICOH`
-i	--ip	MFD IP address	
-p	--password	MFD admin password	
-u	--username	MFD admin username	

Example command

```
.\terminaldeploymenttool CONFIGURE-SP-OPTIONS RICOH -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

CONFIGURE-CARD-READER

Configures card reader on the device

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported (case insensitive): `RICOH`
-i	--ip	MFD IP address	

Short parameter	Long parameter	Description	Note
	--vid	VID for card reader configuration. Skip the parameter if you wish to configure a USB Reader set in configuration properties.	Optional parameter
	--pid	PID for card reader configuration. Skip the parameter if you wish to configure a USB Reader set in configuration properties.	Optional parameter
-p	--password	MFD admin password	
-u	--username	MFD admin username	

Example command

```
.\terminaldeploymenttool CONFIGURE-CARD-READER RICOH -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

CONFIGURE-HOME-KEY

Configures home key mode on the device

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported (case insensitive): `RICOH`
-i	--ip	MFD IP address	
-p	--password	MFD admin password	

Short parameter	Long parameter	Description	Note
-u	--username	MFD admin username	
-m	--mode	Home key mode	Possible values: 'general' for General mode, 'change' for UI change mode, 'off' to disable home key configuration. Default value: 'general'

FETCH-CERTIFICATE

Configures custom authentication.

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported (case insensitive): `RICOH`
-s	--sqts	SQTS Terminal URL	Address of your SAFEQ Cloud installation with SQTS port example: *https://myserver.local:8705* When running Cloud Terminal against an on-premise solution, the value is equal to FQDN or IP address of the gateway device.
	--force-untrusted	enables download of untrusted certificate	Without this parameter, a certificate will not be downloaded unless it's being trusted by the local workstation.

Example command

```
.\terminaldeploymenttool FETCH-CERTIFICATE -s https://<SERVER_ADDRESS>:8705/ --force-untrusted
```

Advanced commands for FUJIFILM BI

CONFIGURE-FUJIFILM

Configures custom authentication.

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported (case insensitive): `FUJIFILMBI`
-i	--ip	MFD IP address	
-p	--password	MFD admin password	
-u	--username	MFD admin username	

Command example

```
.\terminaldeploymenttool CONFIGURE-FUJIFILM FUJIFILMBI -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD>
```

Advanced commands for Xerox

SET-APP-ACCESS

Allows you to change the installed application (any application regardless of origin) accessibility on the device without having to change the values manually in the device administration UI.

Parameters

Short parameter	Long parameter	Description	Note
	vendor	Vendor	Currently supported: XEROX (*case insensitive*)
-i	--ip	MFD IP address	
-p	--password	MFD admin password	
-u	--username	MFD admin username	

Short parameter	Long parameter	Description	Note
-a	--app	Application name	If the app is not found, the deployment tool will output all installed application names into the console so that you can check for spelling errors and other potential issues.
enable or disable		Determines whether the application is enabled or disabled	If not specified, the application will be enabled.

Command example

```
.\terminaldeploymenttool SET-APP-ACCESS XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -a "Fax" enable
```

```
.\terminaldeploymenttool SET-APP-ACCESS XEROX -i <MFD_IP_ADDRESS> -u <MFD_ADMIN_USERNAME> -p <MFD_ADMIN_PASSWORD> -a "Fax" disable
```

Additional configuration

You can find these options in the *configuration.properties* file inside the terminal deployment tool folder.

Configuration options

xeroxSetTerminalAsDefault

Controls whether the installed Cloud Terminal should also be set as a default application (meaning that it loads automatically after rebooting the device or waking it from sleep).

xeroxKioskAllowList

If this option is not commented out and filled with a comma-separated list, it makes the specified applications accessible even with the kiosk mode enabled.

xeroxApplicationOverrideUrl

Use this option only if your SAFEQ Cloud is hosted on OpenTelekom infrastructure.

By default, the address of Xerox Cloud Terminal points to the tenant's cloud address and is resolved to the appropriate instance of the cloud terminal. However, this automatic resolution is currently not supported for OpenTelekom clusters. Therefore, with this option. you can use Xerox Cloud Terminal also for OpenTelekom clusters.

Set to following values based on your region:

Europe
xeroxApplicationOverrideUrl=https://primary.eu-central.ysoft.cloud/xerox

North and South America
xeroxApplicationOverrideUrl=https://primary.us.ysoft.cloud/xerox

Asia and Pacific
xeroxApplicationOverrideUrl=https://primary.ap.ysoft.cloud/xerox

Bundled tools

The `< your deployment tool location>\ tools` folder contains some vendor-specific tools to be used in certain scenarios (such as advanced debugging, etc.). The following tools are included in the Terminal Deployment Tool files:

Xerox Remote Logger – This tool allows you to obtain extensive logs from a running Xerox Gen 2 Cloud Terminal. For more information see Using Xerox Remote Logger tool.

Brother Terminal

MFD Prerequisites

The default administrator password on the MFD has been set.
The MFD supports the Brother Solution Interface(BSI).
'Scan to Email' must be enabled on the MFD

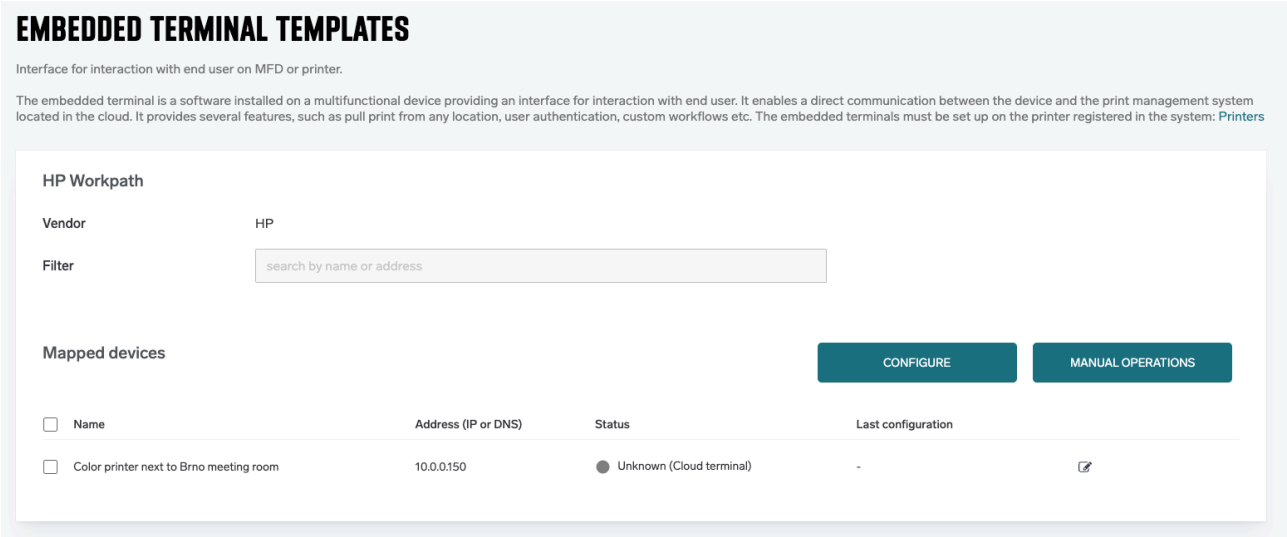
Brother Solutions Interface BSI

Supported devices list can be found in YSoft Partner Portal.

Installing

Installing Terminal Application

Once the device is properly configured, push out the Embedded configuration from embedded screen in SAFEQ Cloud. Make sure your secondary gateway is configured according to Secondary Gateway mapping.



Up until 3.27, the server address had to be a hostname that the printer could verify to make a proper secure connection. If an IP-setup was used configure the embedded client, the user would have to access the webpage of the printer and manually change it to using non-secure HTTP and port 8704 to be able to use the Brother client. *Starting from 3.27, this is now done automatically, if it is detected during installation that an IP is used.*
This means that, if an IP setup is used, for some instances of communication with SAFEQ Cloud and local communication on the printer, non-secure HTTP and port 8704 is used. For SAFEQ Cloud, this includes installation and uninstallation. Locally on the printer, this occurs whenever the Brother system initiates a redirect; on login, logout and when the embedded app is accessed through the solutions app on the printer.
To see (or change this setting), access the webpage of the printer -> login -> Administrator -> Solutions -> Solutions Application Entry -> press Login / Logout /Menu1.

Deploying CA Certificate

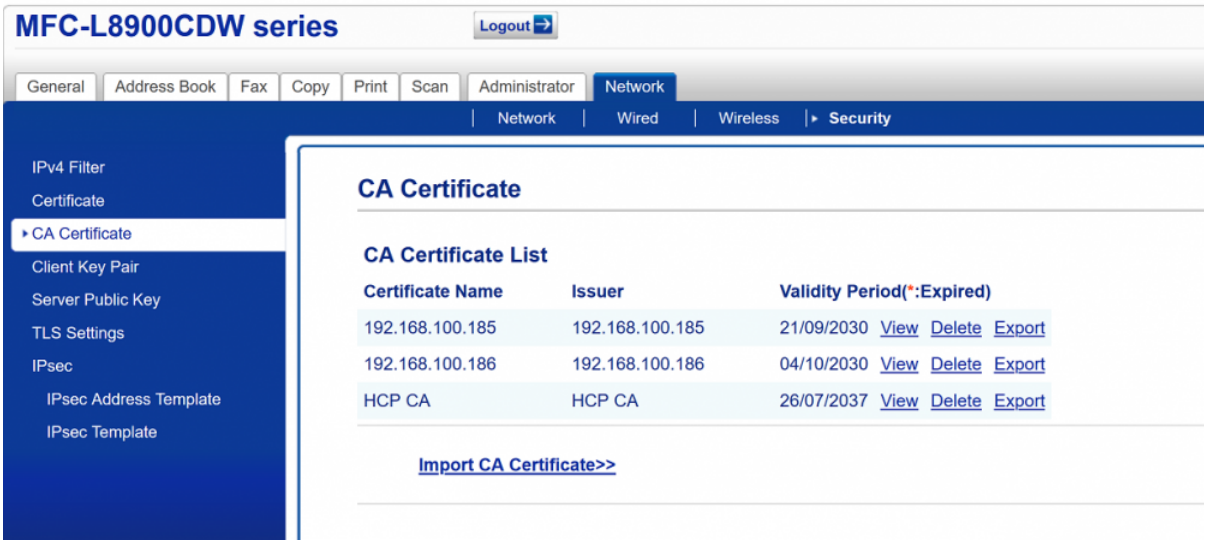
To ensure that communication can be established between the gateway and the MFD, the CA certificate used to sign the gateway certificate must be installed in the MFD.

First of all, you need the CA certificate. Here are the possible options:

1. Use your own CA certificate signed by an authority
2. Generate your own self-signed certificate if you understand and are comfortable with the security risks

In both cases, you need to import the CA certificate to

1. SQC server certificate trust store
    a. Follow this guide Certificates
2. MFD certificate trust store
    a. CA certificate has to be imported manually on the following page:



b. Some MFDs have a limit of 4 certificates, and won't be able to install new ones before old ones are deleted. This can also present a problem if multiple leaf certificates need to be installed.

Uninstalling

Uninstalling the Brother client is straight-forward (as in using the uninstall-button through SAFEQ Cloud). However, a currently running embedded instance must be exited after uninstallation, either manually or through waiting for the automatic timeout on the printer to trigger, or they will still be able to use the embedded client. Also, If a user was logged while the uninstallation took place, they must manually logout.

Troubleshoot

BSI

If BSI is missing, then you have to request access to development resources at the link below:
Enable BSI

After BSI is enabled there should now be a 'Solutions' or 'Solutions Settings' in the web page. Select it, and set the radio button 'Solutions' to 'On'.

Customize login message

The printer has the option to customize the login message from the printer web page. Under Administrator -> Solutions you can change Login Portal Message to the message you want, the default english text is "Login Requested"

Scan to email

Verify that there is an entry 'Scan to email-server' in the scan-menu. The scan menu can be reached, on the printers display, from the main screen.

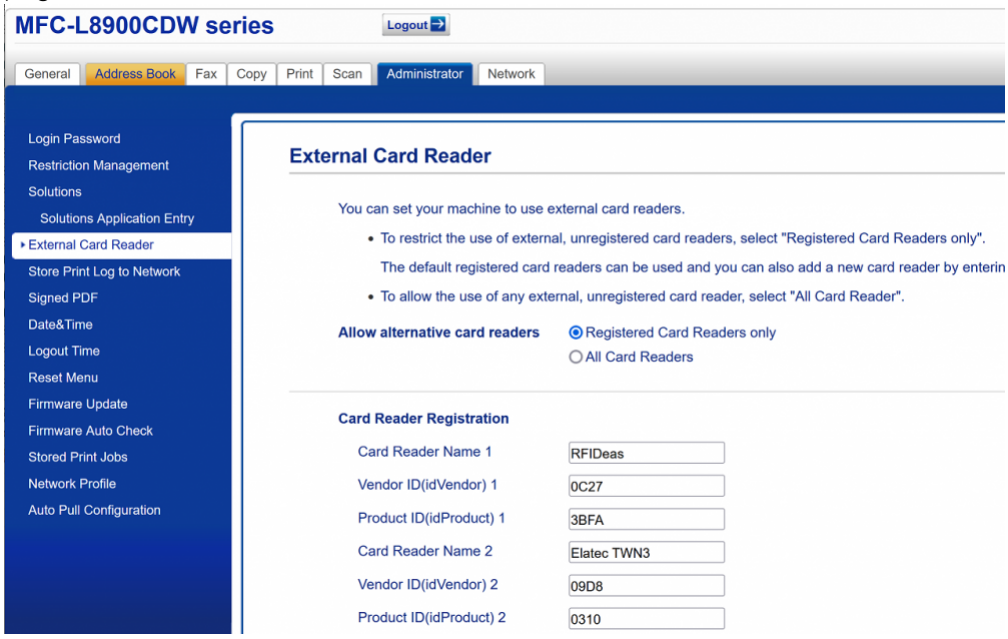
If the 'Scan to email-server' is not present, you'll need to install a firmware addition.

Card readers

As standard only a few card readers are supported on the Brother devices.

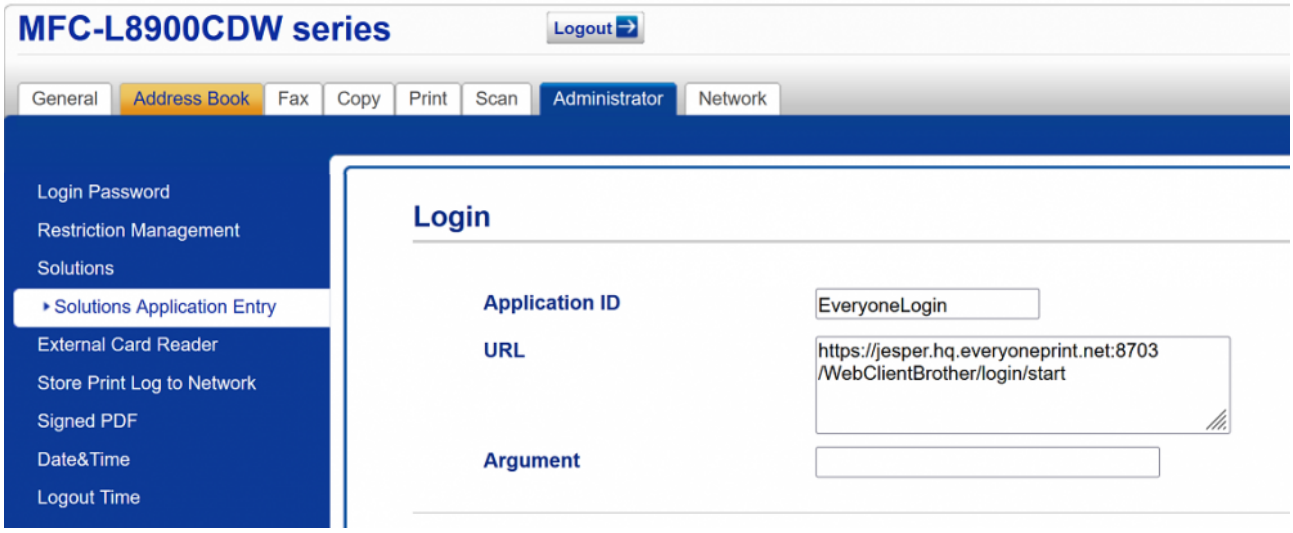
Remember to enable USB card reader support.

To add support for additional readers you have to set up External Card reader on the printer web page.



Solutions Application Entry
There needs to be 3 entries, Login, Logout and a menu.

For **login** URL should be https://[SERVER]:8703/WebClientBrother/login/start, leave arguments empty



For **Logout** URL should be https://[SERVER]:8703/WebClientBrother/main/logout

For **MenuX** URL should be https://[SERVER]:8703/WebClientBrother/login/start

Error codes

Refer to the following chart to check and solve the error code displayed on the LCD of the Brother device

Error codes

FUJIFILM BI Terminal

Prerequisites

- Make sure that you have Cloud Terminal Integration enabled. For information on how to do this, see Enable Cloud terminal integration.
- Make sure that you have a signing certificate selected. To check this, log in to SAFEQ Cloud Web UI and navigate to Security > Security options > scroll down to PKI and encryption. The Signing certificate field must not be blank.

Limitations

General

- To install, uninstall, or reinstall a device, it must be in power saver mode.
- If the device is in sleep mode, swiping a card at the card reader will not authenticate the user.
- Username information is not propagated when printing a job. This means that all print jobs printed on the MFD/SFD are printed under Local User. This behavior is consistent across the whole solution, for all vendor terminals.

Cloud Print

Finishing options:

- Booklet bind direction Left to Right is always used.
- Only Output trays 1-4 are supported.
- Supported paper sizes: A3, A4, A5, B4, B5, LEGAL, LETTER.
- Media type (type of paper) is not supported.
- Landscape page orientation is not supported.
- DPI is not supported.
- If a job is sent via a custom driver, finishing options are not supported.

Advanced finishing options:

- Only Stapling and Punching options are supported (saddle stapling is not supported).

Scan

- Scan Mixed Size Originals are not supported.
- Scan Workflows with JPEG output format will result in a TIFF output file if the color was set to Black and White or the color was Auto and the MFD detected a black and white document.
- The Merge originals feature is not supported.
- The scan file size is limited to 18 MB when using scan delivery via email. If the scan file size is larger, the email is not delivered. There is no extra notification of such an event.

Accounting

- If a scan or copy operation is still in progress when a user logs out, the terminal will only report information that has already been processed.
- If a user logs out while scanning or copying is still in progress and then logs back in before the job is finished, the job will be reported twice.
- USB print accounting is not supported.

ApeosPort devices support

Only devices with the following specifications are supported:

- XCP SDK Platform 2.0.0 or newer
- AiP7 compatible FW
- EWB v5 and newer

Signature validation is not supported on ApeosPort devices.

Custom logo

- Formats other than JPEG, JPG, PNG, and GIF are not supported.
- Images over 12 kB will be resized and compressed.
- GIF images over 12 kB will be turned into still images.

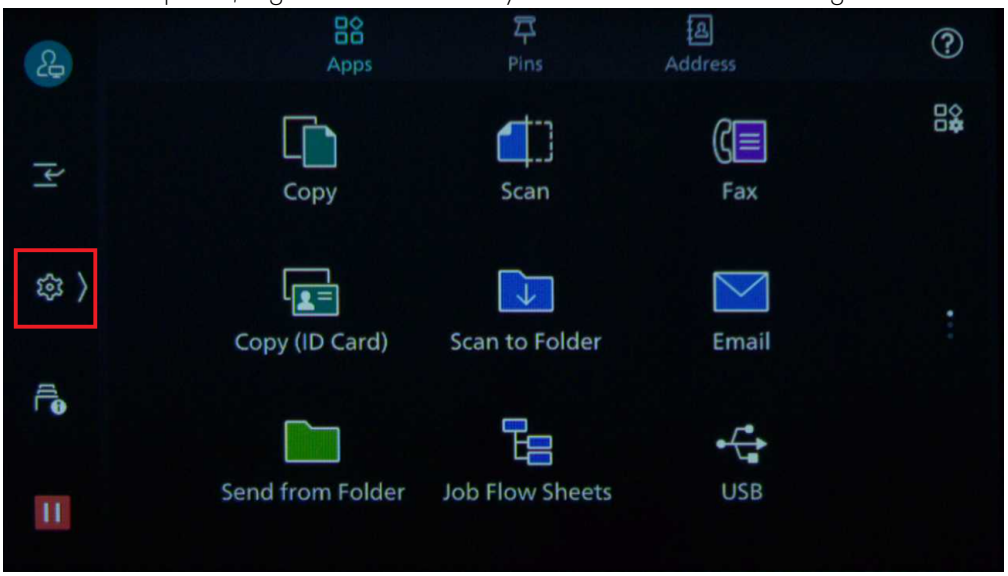
Device setup

During the configuration, MFD sometimes requires a reboot. When prompted for reboot, follow the instruction displayed either on the web browser or on the MFD operation panel.

General configuration

General settings

1. On the MFD panel, log in to MFD as a system administrator and go to the **Device settings**.



2. Go to **Device** > **System Settings** > **System Clock / Timers**.
    a. Configure date and time:
        1. Set **Time Zone**.
        2. Set **Date**.
        3. Set **Time**.

Set these options in the aforementioned order, because the Time Zone setting has an effect on the Time setting.

b. Optionally, configure NTP:

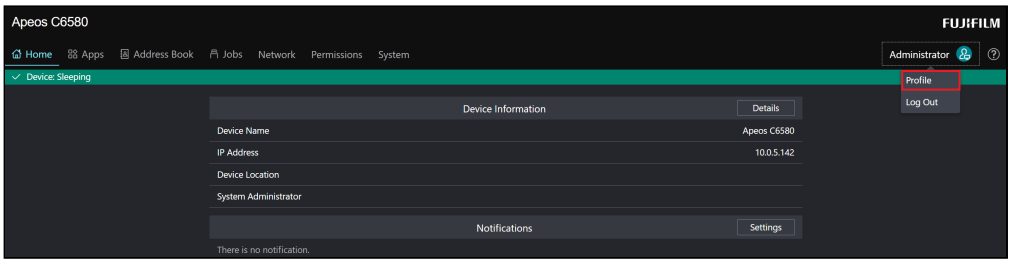
1. Set **NTP time synchronization** to **On**.
2. In **Time Server Address**, fill in your chosen NTP server address.

Security settings

Enter the IP address of the MFD in your web browser to access the MFD's web interface and log in as administrator. Configure the following:

1. Administrator user ID and password:

a. Go to **Administrator > Profile**.



b. Click **Edit**. On the edit screen, enter a new username for Administrator and click **Save**.

c. Click **Change password**, enter a new password, and click **Save**.

d. Log in to the MFD's web interface with your new admin username and password.

2. Machine digital certificate:

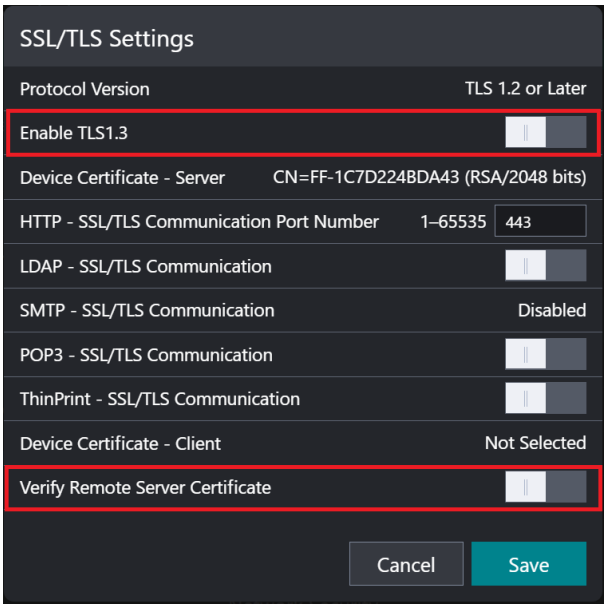
a. The certificate is installed by default. You don't need to generate a new one.

3. SSL/TLS:

a. Apeos has TLS 1.2 enabled by default.

b. Make sure that **Verify Remote Server Certificate** is disabled. Otherwise, users would get an error message when opening the SAFEQ Cloud application on the MFD panel due to an

untrusted certificate.



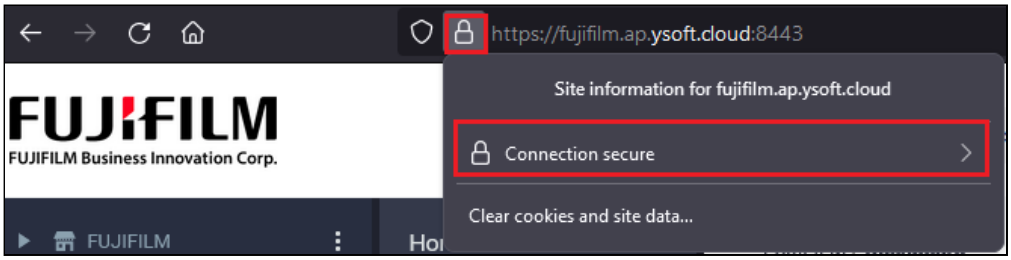
Setting up trust between the server and MFD/SFD

To secure the communication between the server and MFD/SFD by certificate validation, you must import the relevant certificate authorities into the device, and enable server certificate validation.

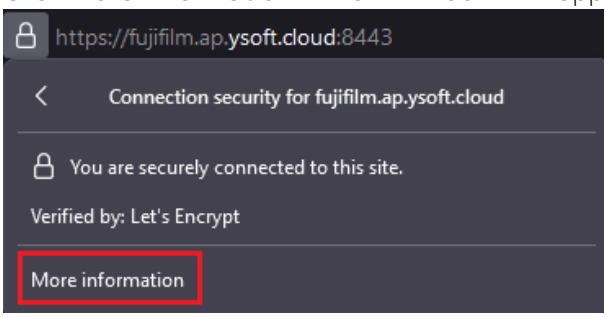
FUJIFILM BI devices come with a pre-installed list of globally trusted Certification Authorities. However Let'sEncrypt authority used as a default authority for SAFEQ Cloud servers is not included.

Obtain the relevant certificate authorities:

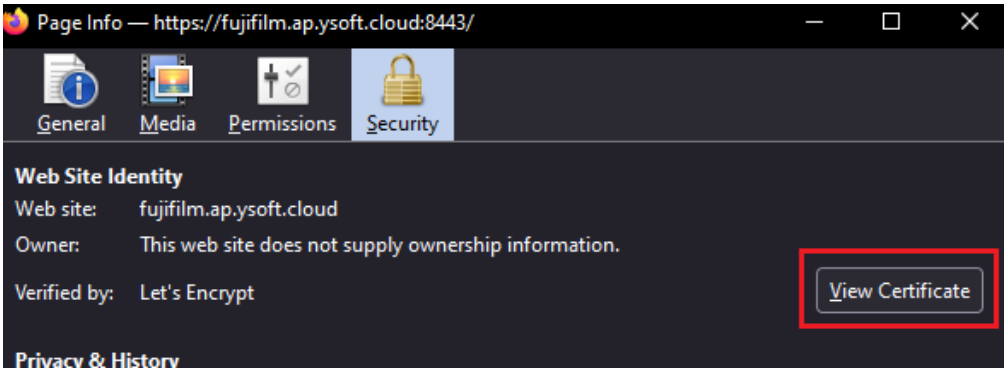
1. If you are using your own certificate and domain, you will need to get your issuing Certificate Authority in PEM format. See Certificates.
2. If you are connecting to a secondary SAFEQ Cloud server, OMNI Bridge, or to a primary server that is hosted on-premise, make sure that the destination has a valid certificate tied to a domain. See Certificates.
3. If you are using the default certificates of SAFEQ Cloud, you will need to obtain these in the following way:
   - Navigate to your SAFEQ Cloud instance and click the lock icon next to the address bar in order to view the certificate information.



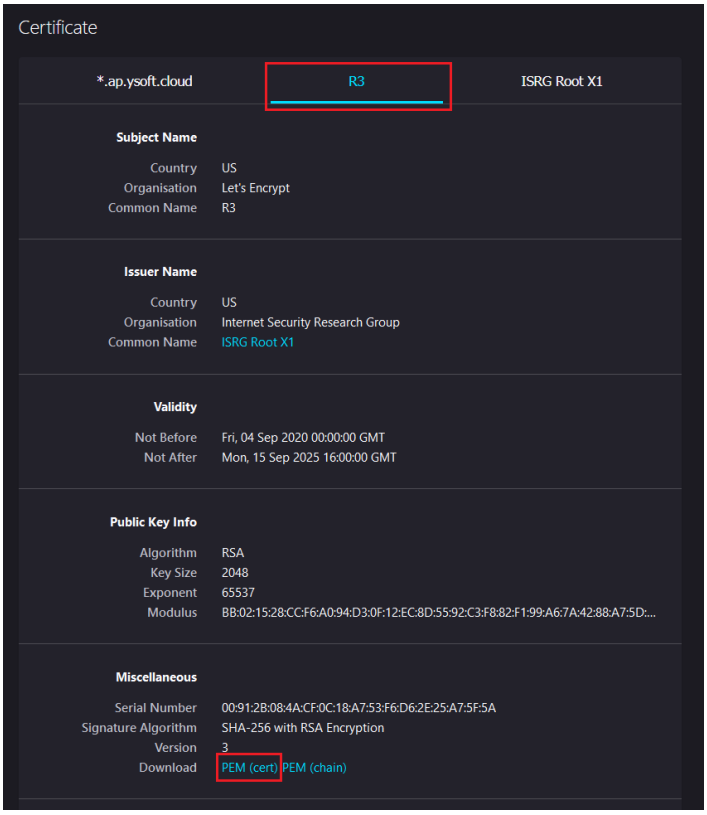
- Click **More information**. A new window will appear.

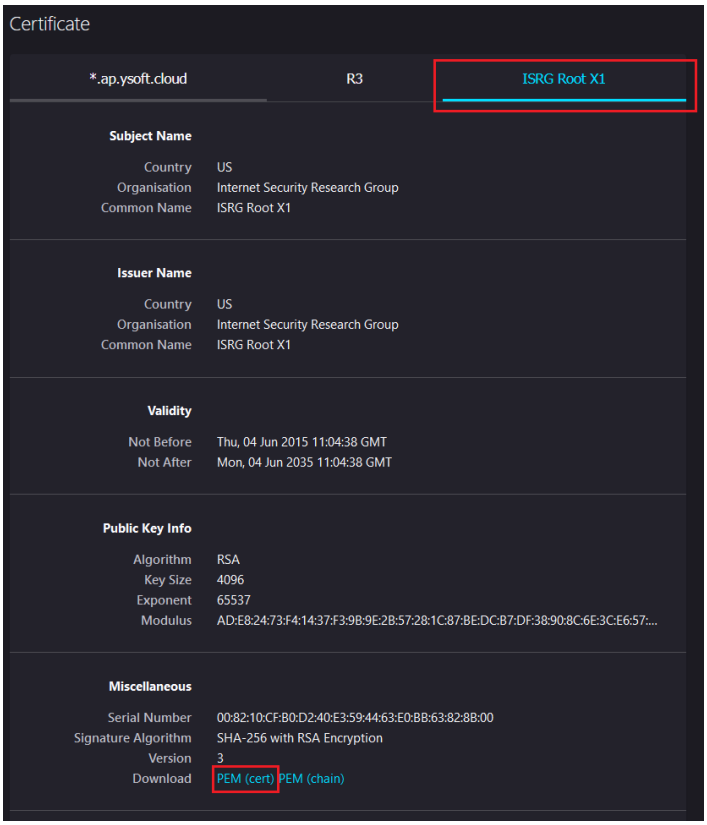


- Click **View Certificate**.



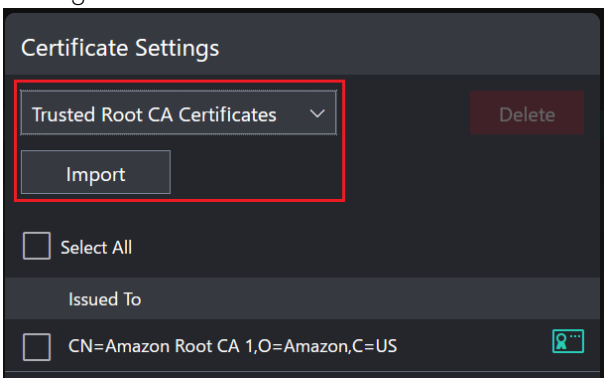
- In the new window, navigate to both tabs marked below and download the certificate in PEM format.



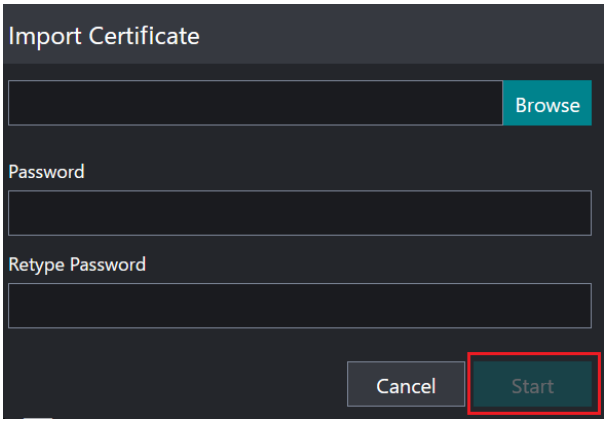


Importing certificate authorities to the MFD/SFP:

1. Log in to your MFD's web interface as an administrator.
2. Navigate to **System > Security > Certificate Settings**.
3. Change the selection to **Trusted Root CA Certificates** and click **Import**.



4. Find the obtained Certificate Authority in PEM format, fill in the admin password, and click **Start**.

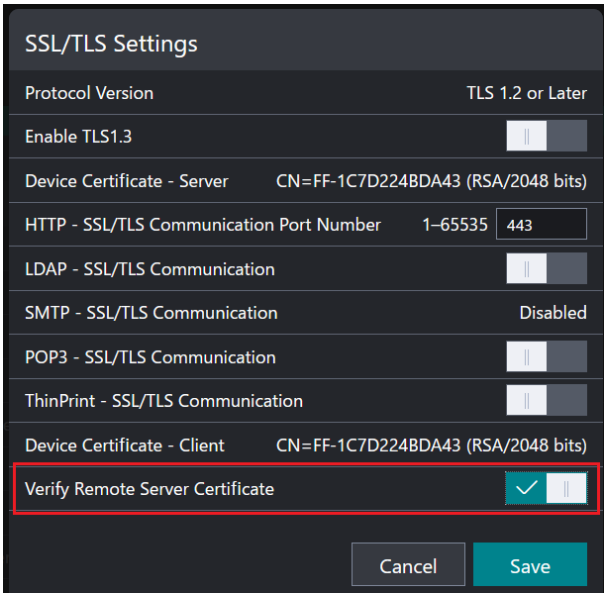


5. Repeat the process for all the Certificate Authorities in the chain (each PEM file that you obtained).

Enable server certificate validation:

> For server certificate validation to work, the server must have a certificate issued for the domain and not an IP address (or local host). Otherwise, the machine will reject such certificates even if proper Certificate Authorities were imported.

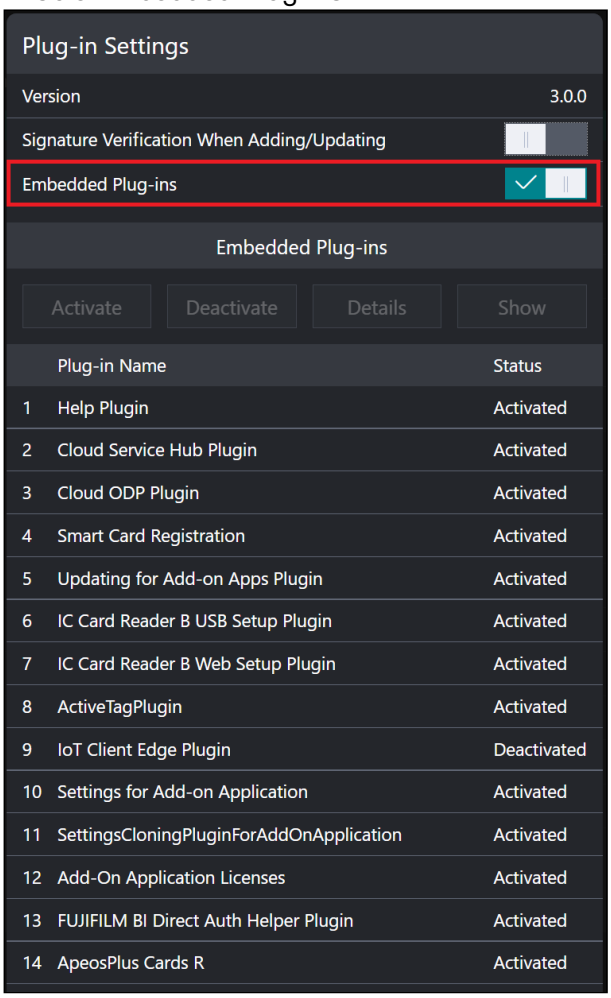
1. Log in to your MFD's web interface as an administrator.
2. Navigate to **System > Security > SSL/TLS Settings**.
3. Enable **Verify Remote Server Certificate** and click **Save**.



Plug-in settings

1. Go to **System > Plug-in Settings**.

2. Enable **Embedded Plug-ins**.

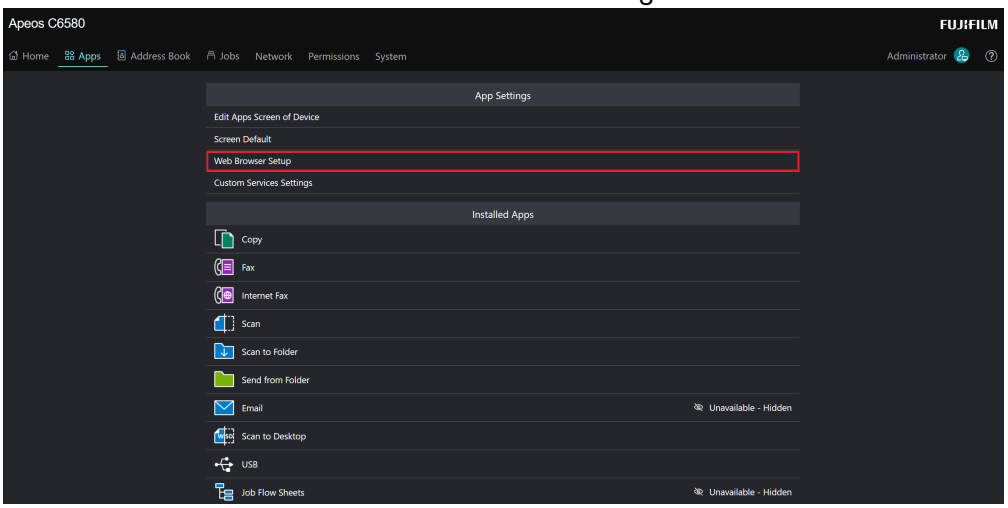


The **Signature Verification when Adding/Updating** option will not be visible on production models. You can safely ignore it.

For ApeosPort devices, the **Signature Verification when Adding/Updating** option will be visible, but it should be disabled due to limitations.

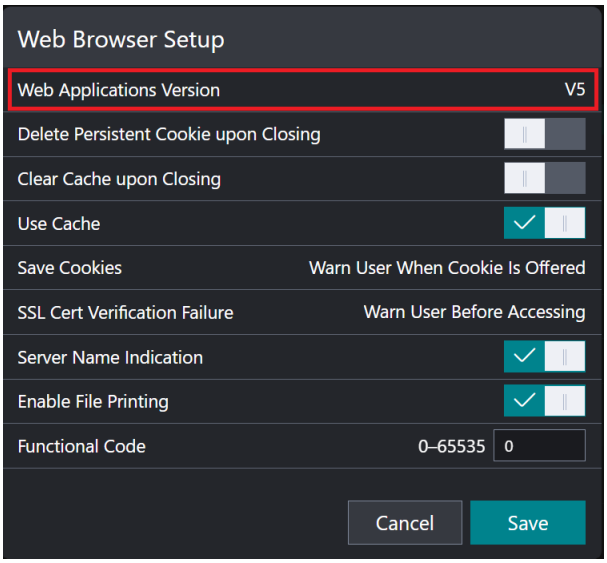
Web browser settings

1. Go to **Apps** > **App Settings** > **Web Browser Setup**. In case of **ApeosPort devices**, go to **Permissions** > **Authentication** > **Advanced Settings**.



2. Ensure that **Web Application Version** is set to **V5**.

> If the "Web Application Version" parameter is missing, "V5" should be the default value.

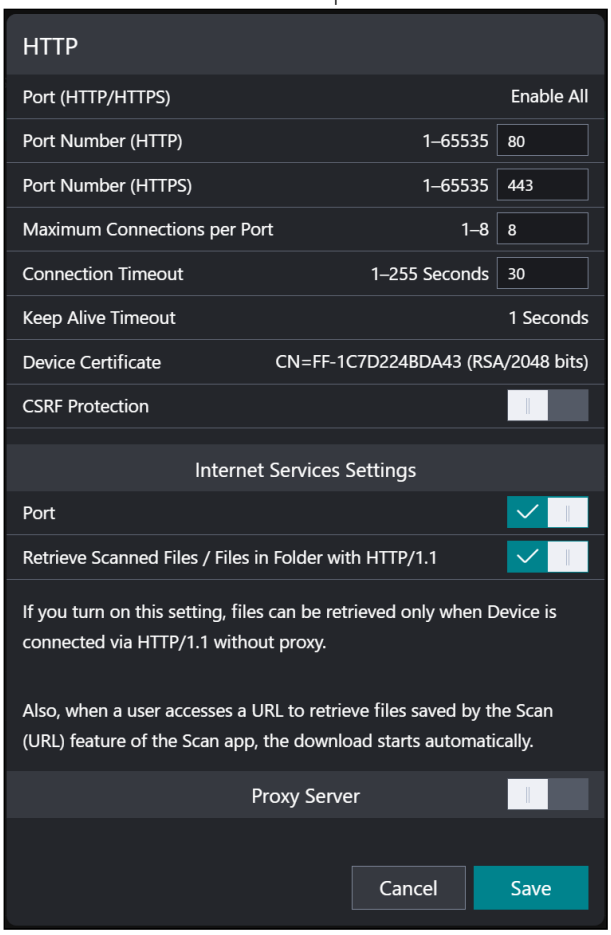


Protocol settings

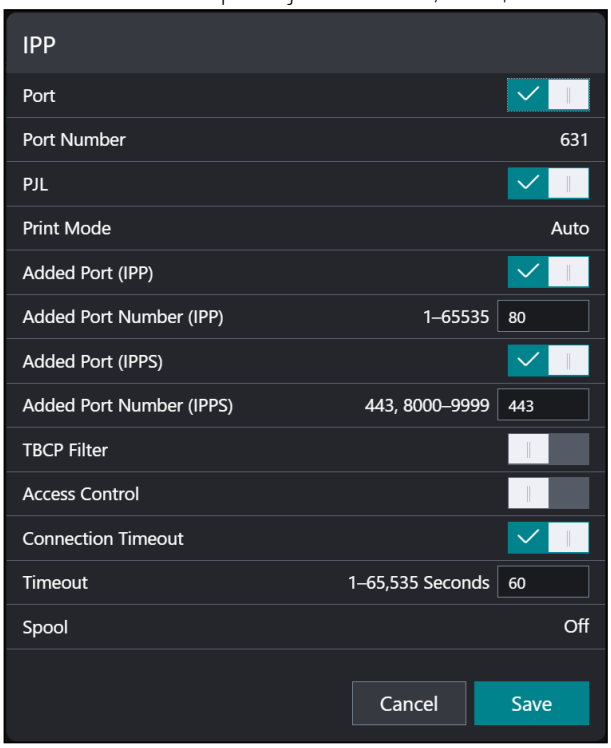
In the MFD's web interface, configure the following:

1. Go to **Network** > **Network settings** > **Protocols**.

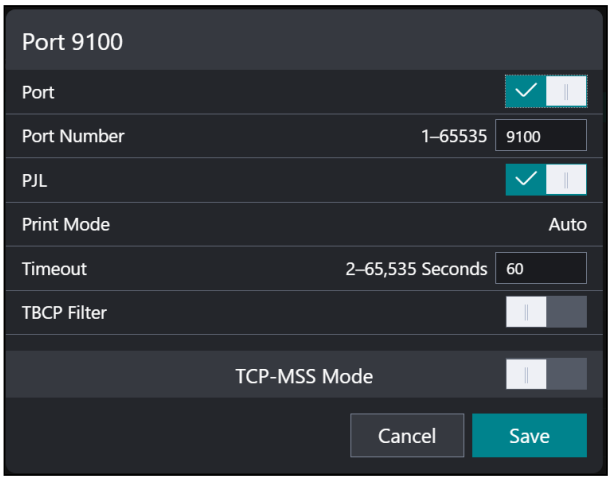
2. Check that **Port (HTTP/HTTPS)** is set to **Enable All**. You can also set it to Enable **HTTPS Only**, which disables the HTTP port.



3. **IPP** – To receive print jobs via IPP/IPPS, IPP must be enabled.



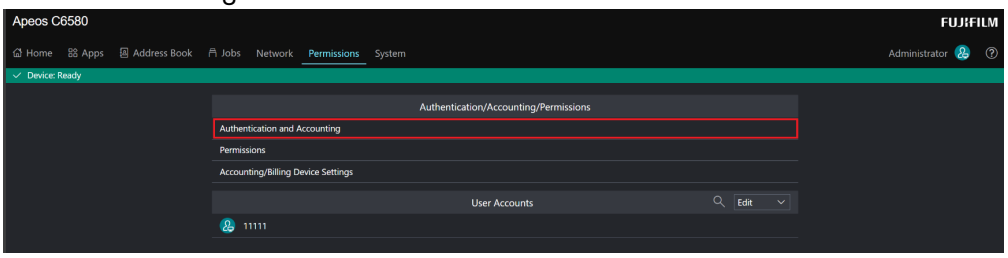
4. **Port 9100** – To receive print jobs via TCP/IP RAW, Port 9100 must be enabled.



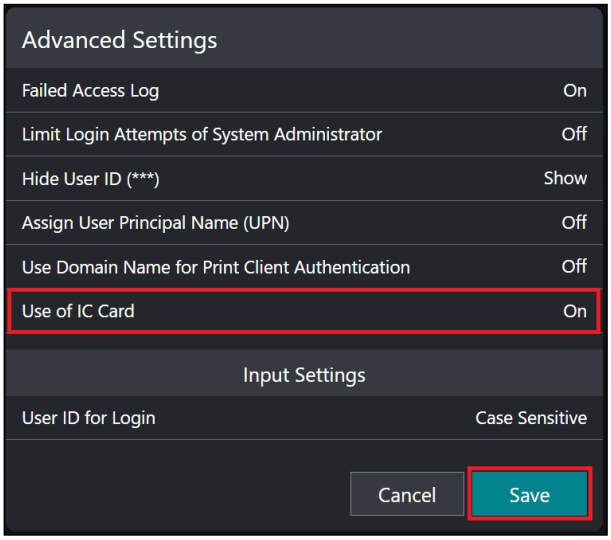
> If you keep port 9100 disabled for security reasons, be aware that you must enable it before MFD firmware upgrade.

Card reader settings

1. To enable Enable Card Reader support, go to **Permissions** > **Authentication and Accounting** > **Advanced Settings**.



2. Set **Use of IC Card** to **On**.
3. Click **Save**.
4. For ApeosPort devices, set **Use of Smart Card** to **On** and click **Save**.

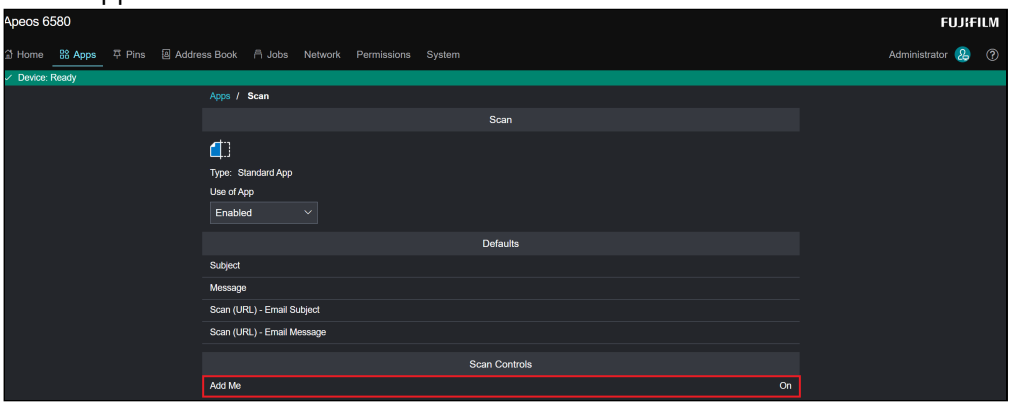


Do not enable **Use of IC Card** with no card reader connected; otherwise, you will not be able to authenticate with a card.

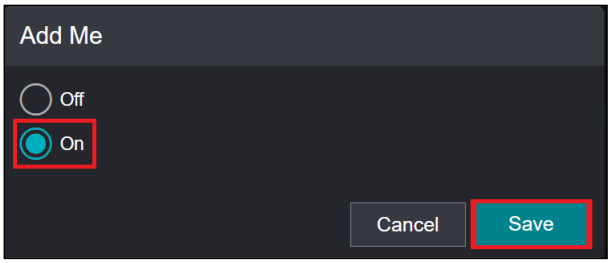
Scan related settings

To enable the auto-completion of email addresses in the native scanning application, perform the following steps:

1. Go to **Apps** > **Scan** > **Add me**.

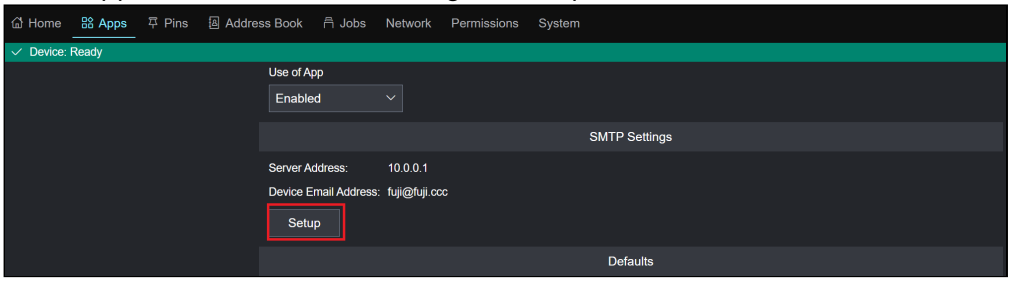


2. Switch it to **On**.

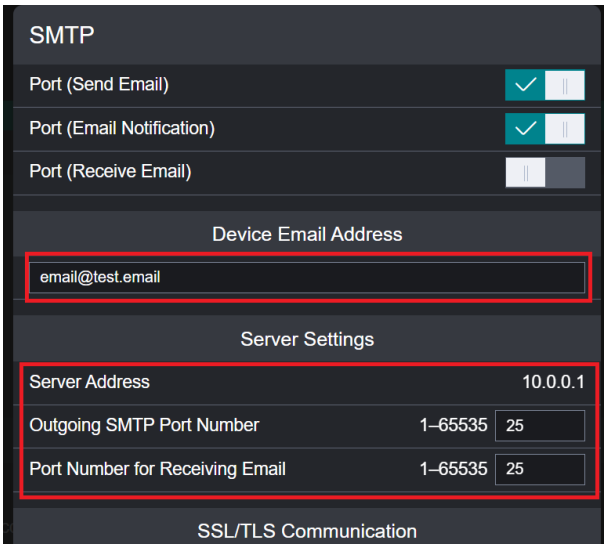


3. Click **Save**.

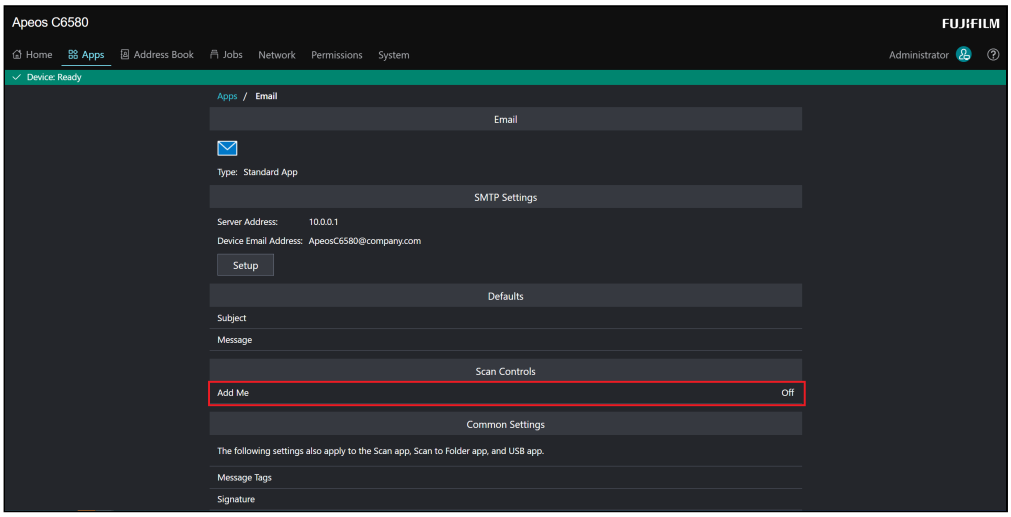
4. Go to **Apps** > **Email** > **SMTP Settings** > **Setup**.



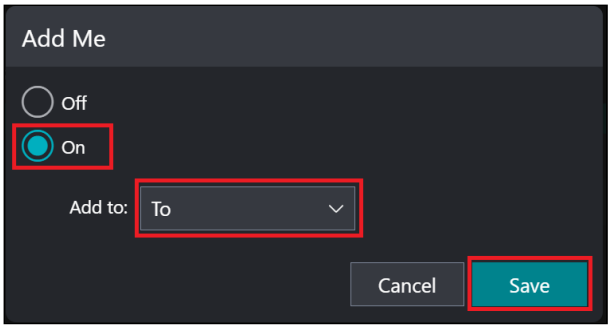
5. Set the **Device Email Address** and **Server Settings**.



6. In **Scan Controls**, click **Add Me**.



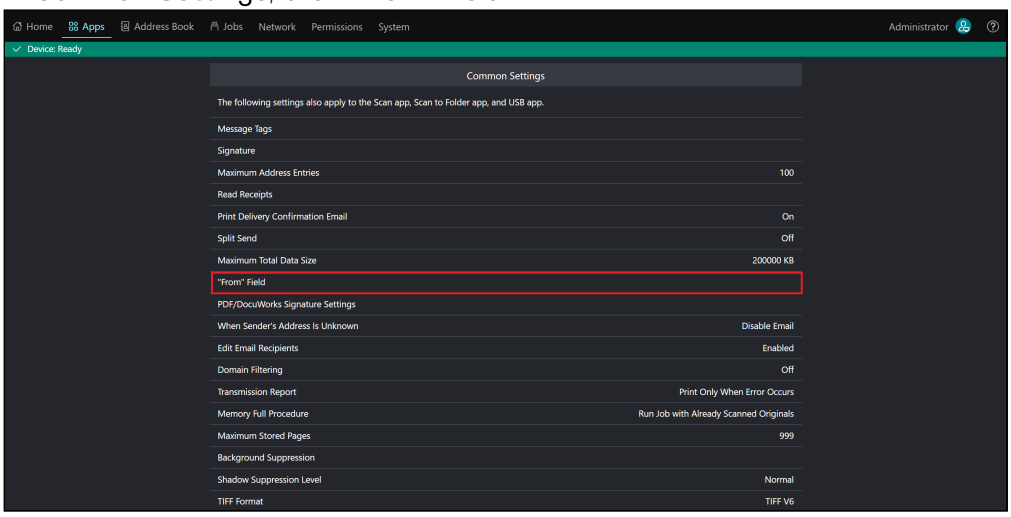
7. Select **On** and set **Add to:** to **To** or **Cc**.



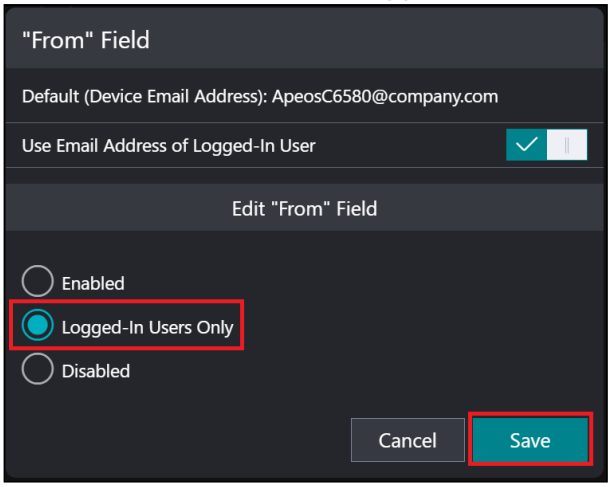
8. Click **Save**.

9. Configure the **"From" Field** (optional):

a. In **Common Settings**, click **"From" Field**.



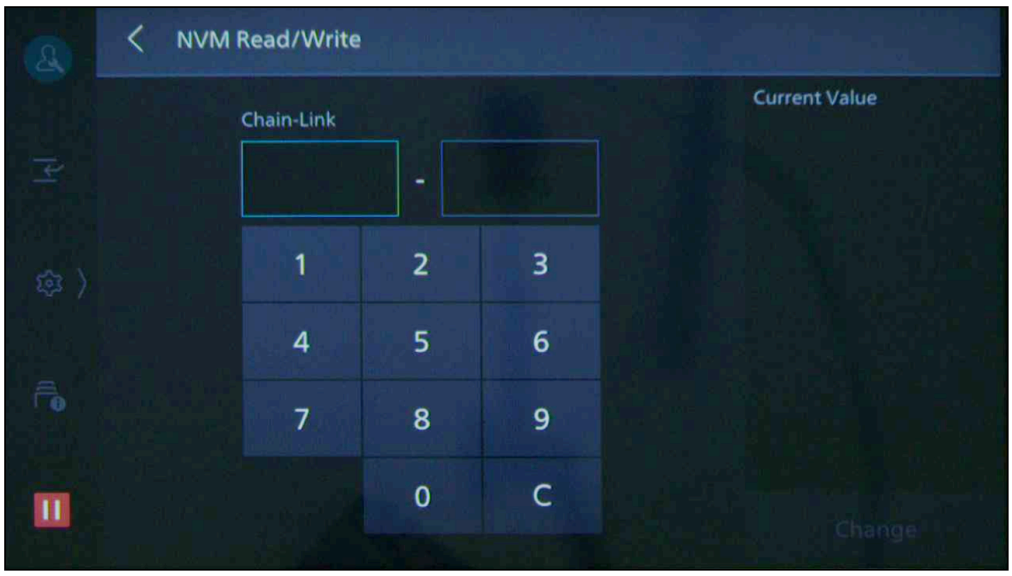
b. In **Edit "From" Field**, select **Logged-In Users Only** and click **Save**.



Device NVM setup

The NVM setup can be done only by the FUJIFILM BI partner engineer on-site. It is necessary for Apeos to report the accounting of print jobs to SAFEQ Cloud. If not done, Apeos will require authentication for print requests and store print jobs without authentication information in the internal storage.

Accounting settings: The FUJIFILM BI partner engineer has to navigate to the **NVM Read/Write** screen, enter **Chain-Link** `701-436` and set the value to `0`.



Installing and uninstalling FUJIFILM BI Cloud Terminal

When reconnecting FUJIFILM BI Cloud Terminal between servers (for example, between Cloud primary and OMNI Bridge), the terminal must be uninstalled and installed again.

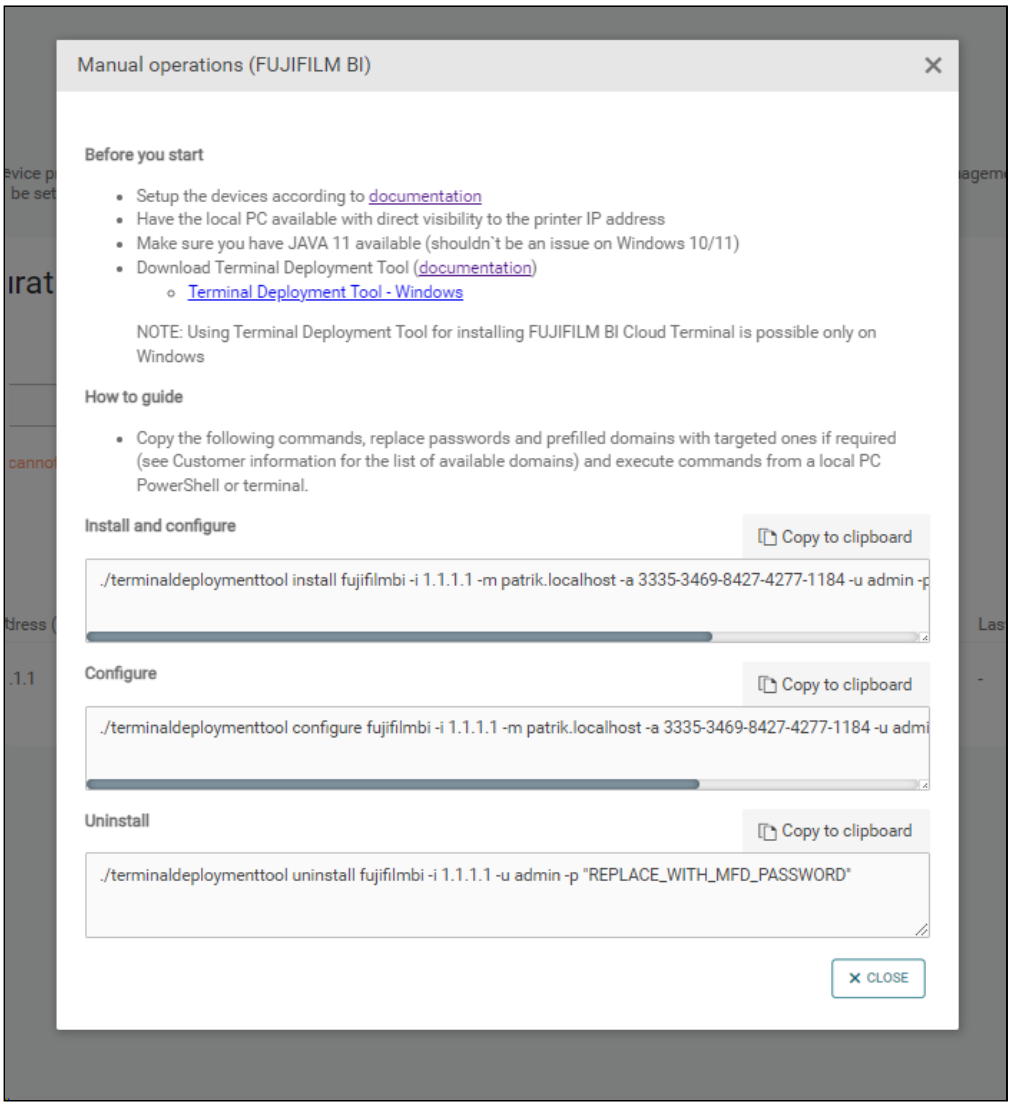
Using Terminal Deployment Tool

Using Terminal Deployment Tool for installing FUJIFILM BI Cloud Terminal is possible only with MS Windows.

1. After adding the printer and Embedded configuration (see section Adding FUJIFILM BI printer and Embedded in SAFEQ Cloud below), go to **Printers > Embedded templates** and open the newly created Embedded.
2. Click **Manual operations**.
3. Follow the instructions in the modal dialog shown below:

   The example commands are generated regardless of the operating system.

   For Windows, the full file name should be used in the command so that each command starts with `./terminaldeploymenttool.bat`

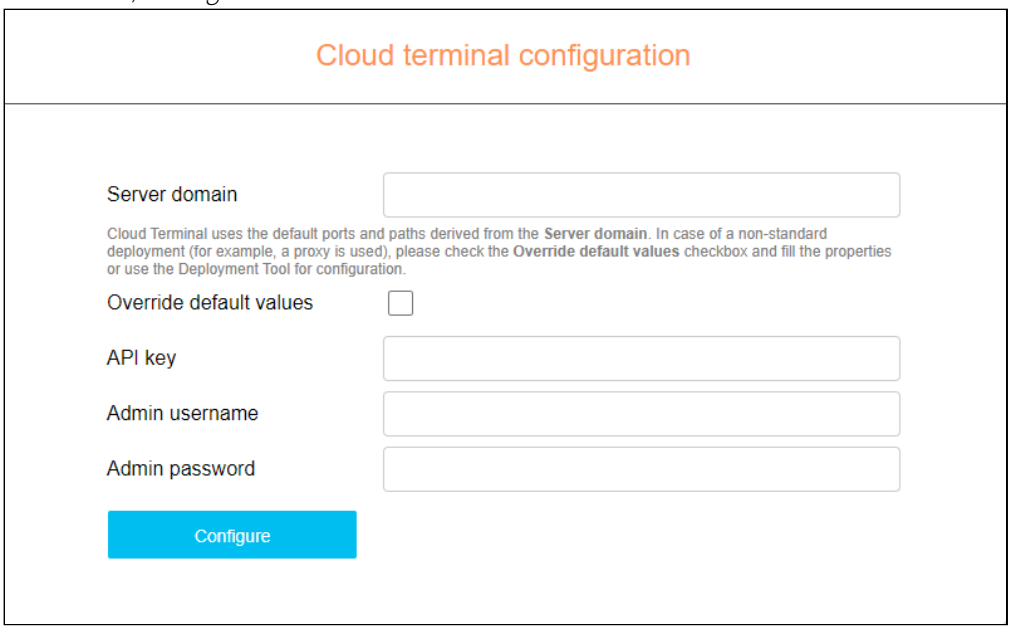


You can also use configuration web UI to configure FUJIFILM BI Cloud Terminal as described in the following section.

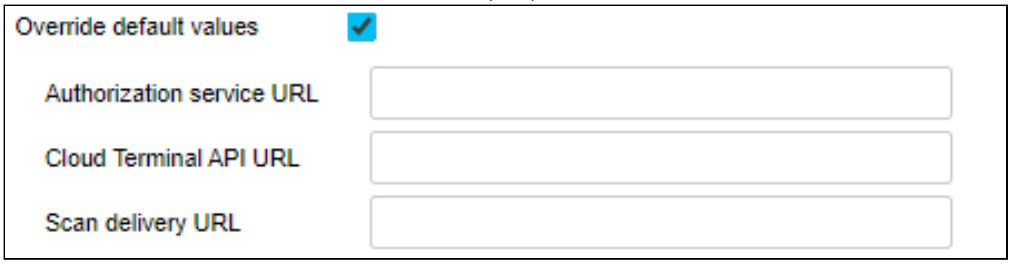
Using Configuration UI

Using Terminal Deployment Tool is the recommended way for installing and configuring FUJIFILM BI Terminal.

1. To access the configuration web UI, enter the following URL in your browser: *https://<device IP>:58070/configuration*



2. To configure the device, fill in the following fields:
   - Server URL – address of the SQTS, Idm, and scan server (for ex. https://rnd14167.rnd.local)
   - In case of a non-standard deployment (for example, a proxy is used), check the Override default values checkbox and fill in all properties.

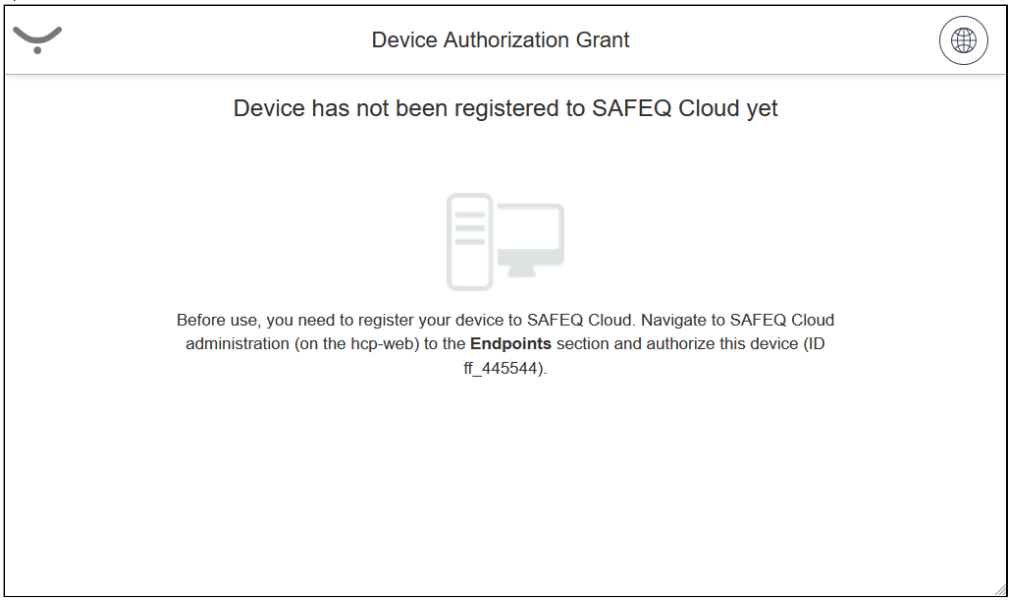


   - API key – API access key set up in SAFEQ Cloud.
   - Admin username/password – login credentials set up in the MFD.

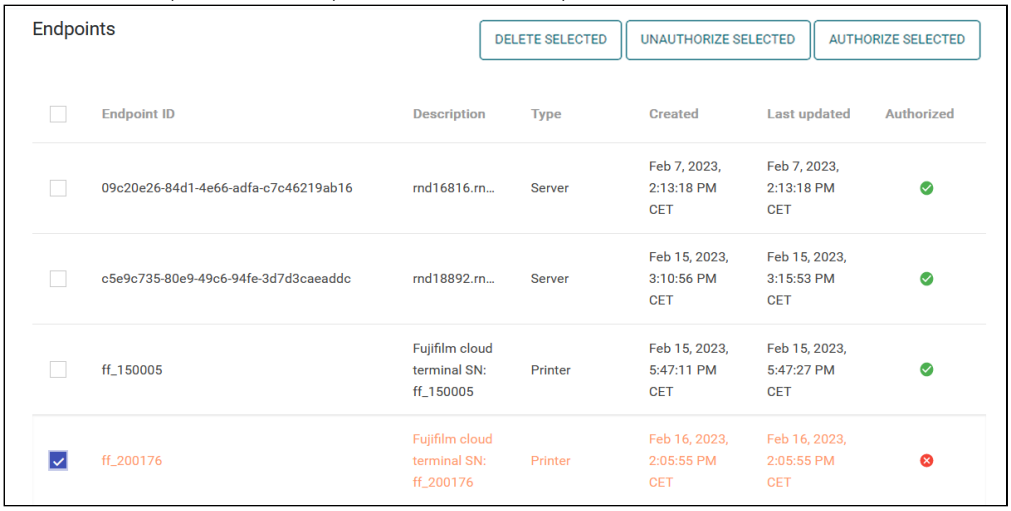
URL addresses of the SQTS, Idm, and scan server are automatically created from the Server URL by suffixing the respective ports to it. For a custom deployment (for example, with a proxy), use Terminal Deployment Tool.

Registering Cloud Terminal in the SAFEQ Cloud web interface

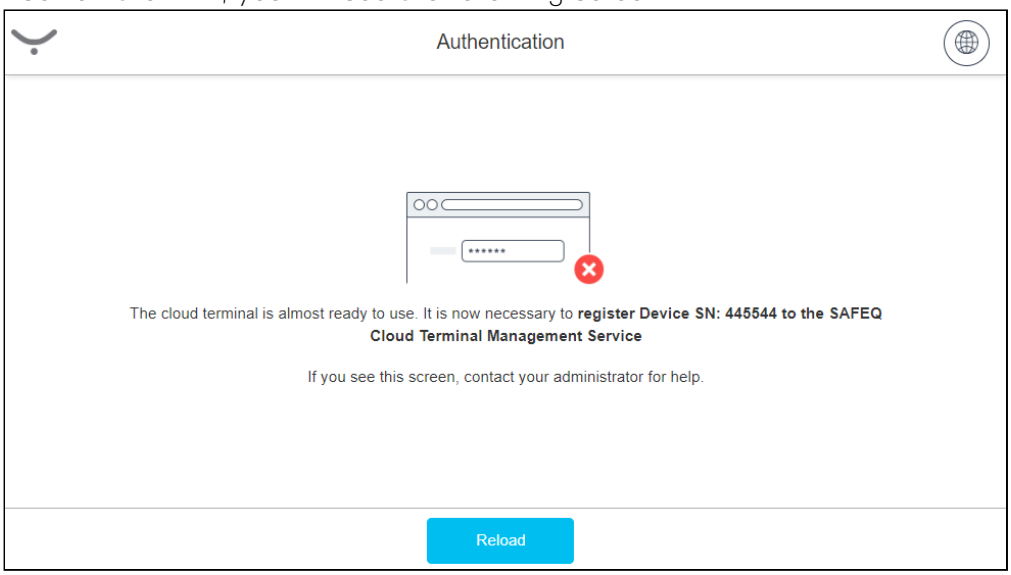
1. Upon installing the terminal on the MFD, you will see a screen with the ID of the device (prefixed with "ff_"). Note the ID number.



2. In SAFEQ Cloud web UI, go to Security > Endpoints and find the entry with ID number that you noted in the previous step. Select the entry and click Authorize selected.



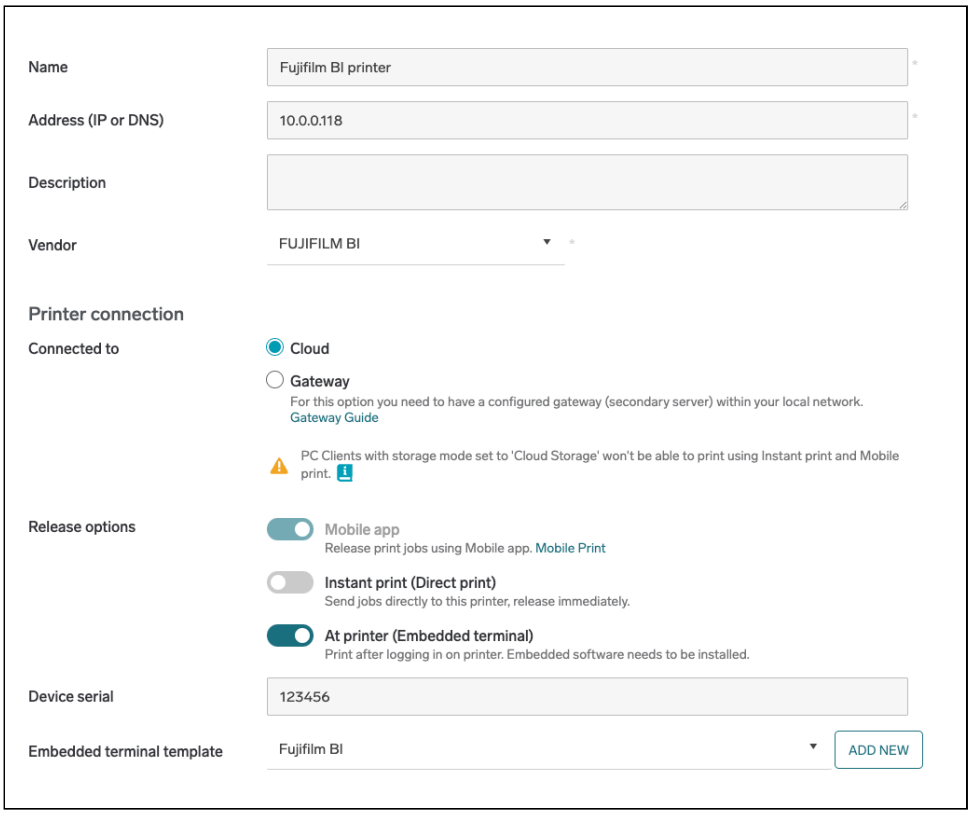
3. Back on the MFD, you will see the following screen:



Adding FUJIFILM BI printer and Embedded configuration in SAFEQ Cloud Web UI

1. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
2. If not done already, create an embedded configuration for Fujifilm BI by clicking **Add**.
3. In **Vendor**, select **Fujifilm BI**.
4. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.
5. Go to **Printers**.
6. Click **Add**.

7. In Vendor, select FUJIFILM BI.

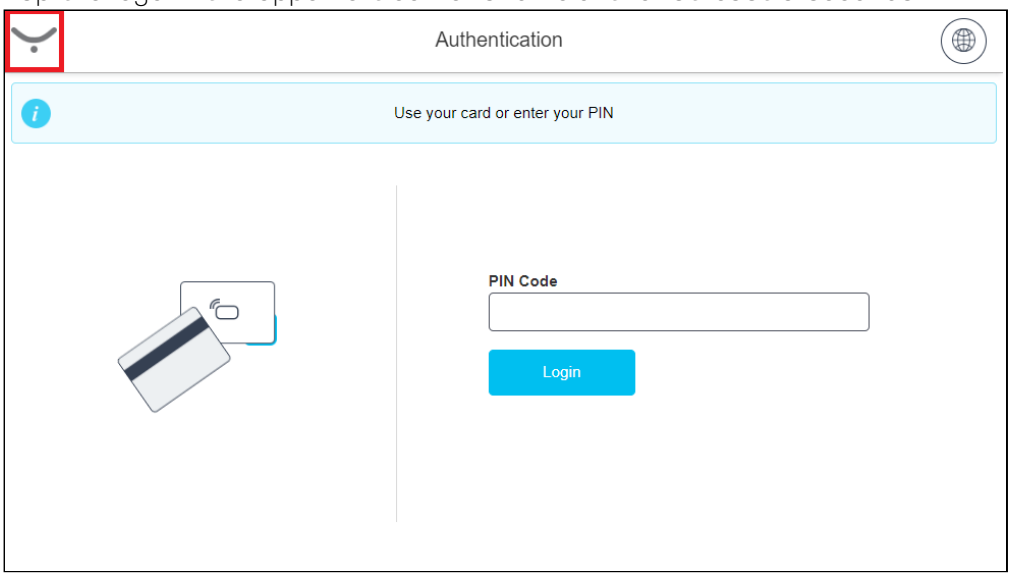


8. In Device serial, enter the serial number which was presented on the MFD and which you noted down as ID.
9. Fill in the rest of required information according to your needs.
10. In Embedded configuration, select your Fujifilm BI embedded configuration from the list.
11. Click Save.
12. The MFD will now display a login screen with your chosen authentication type.

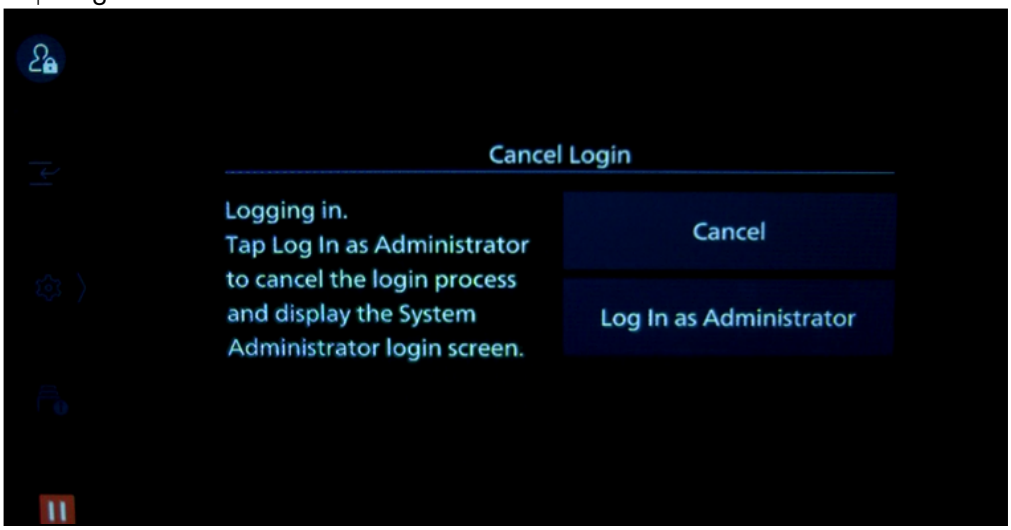
Logging in with the machine administrator account

To change settings and configure the device, you can log in as a machine administrator from the authentication screen or device code flow screen or error screens that can appear instead of the authentication screen.

1. Tap the logo in the upper left corner and hold it for at least 5 seconds.



2. Tap **Log In as Administrator** and enter the administrator credentials.



Finishing device setup after cloud terminal installation/configuration

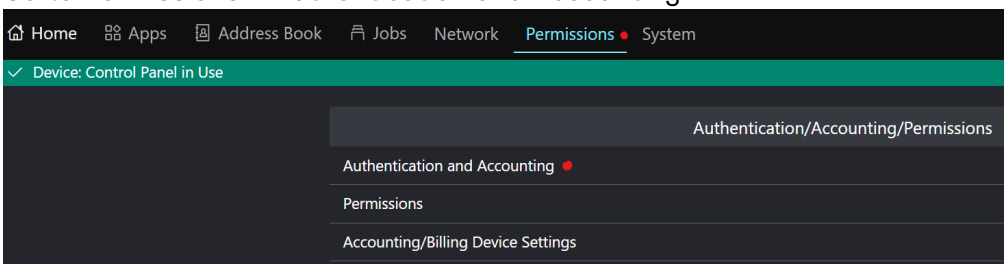
After finishing the Cloud Terminal installation, you must do additional configuration steps in the MFD's web interface.

Do the following actions in the exact order in which they are listed.

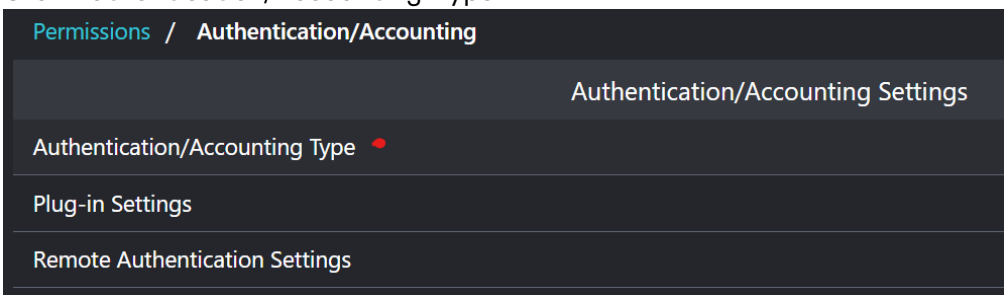
Turn on custom service authentication on the device

1. In the address bar of your web browser, type `https://<DeviceIP>.`
2. Log in as administrator.

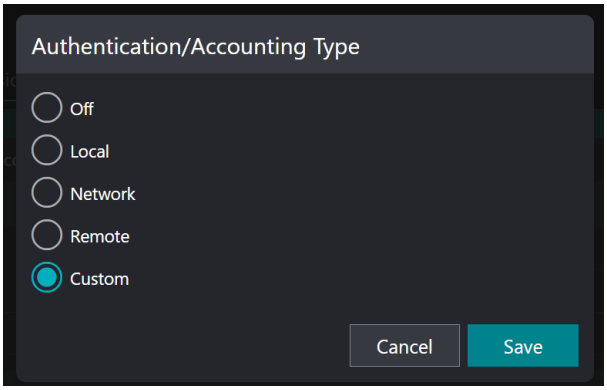
3. Go to **Permissions** > **Authentication and Accounting**.



4. Click **Authentication/Accounting Type**.



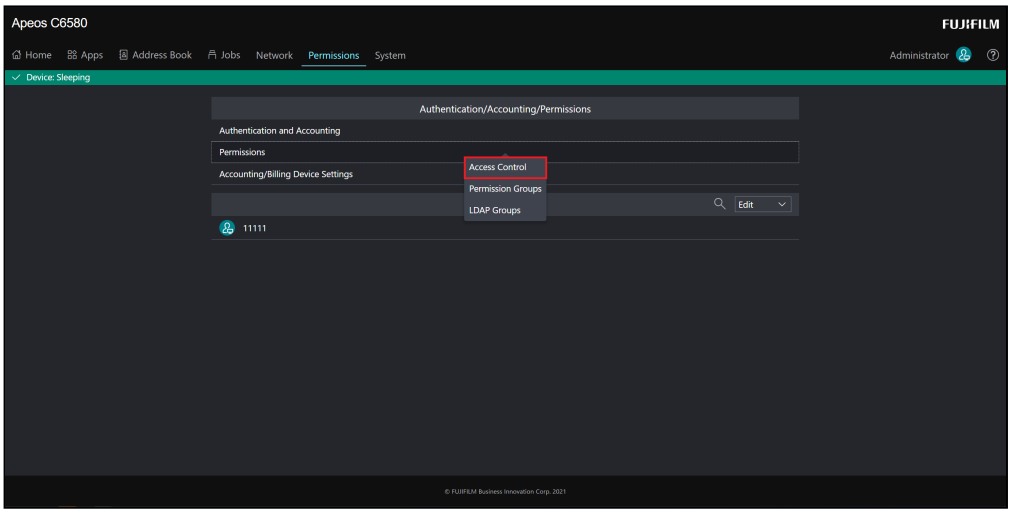
5. Select **Custom** and click **Save**.



Configure access to the device functions

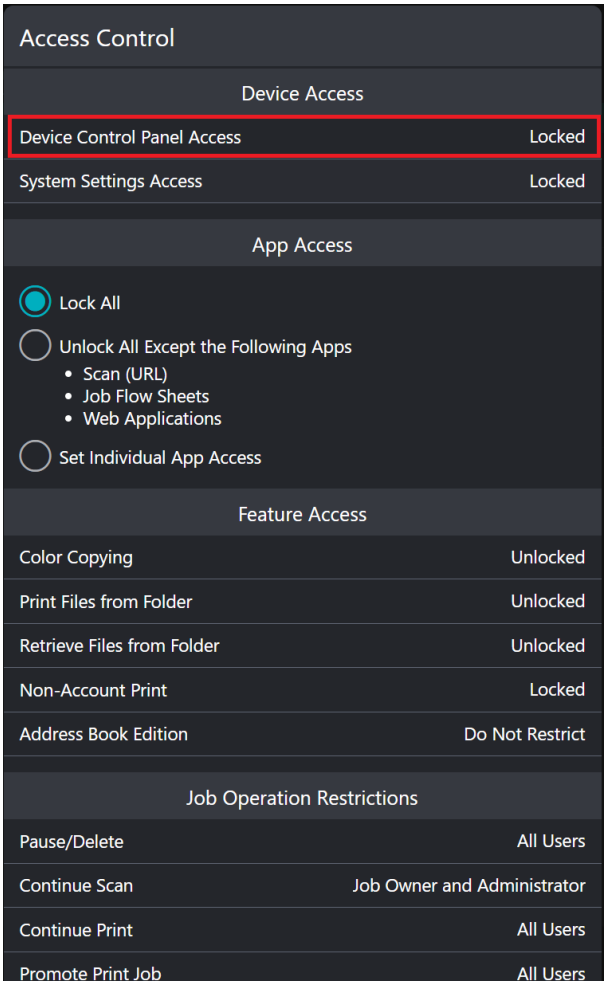
Configure the Access Control as described below to restrict access to walk-up functions by user access right setting. By doing this, the authentication screen becomes the home screen, and the users need to authenticate to access any functions.

1. Go to **Permissions** > **Permissions** > **Access Control**.



2. Set the **Device Control Panel Access** to **Locked**.

3. Click **Save**.



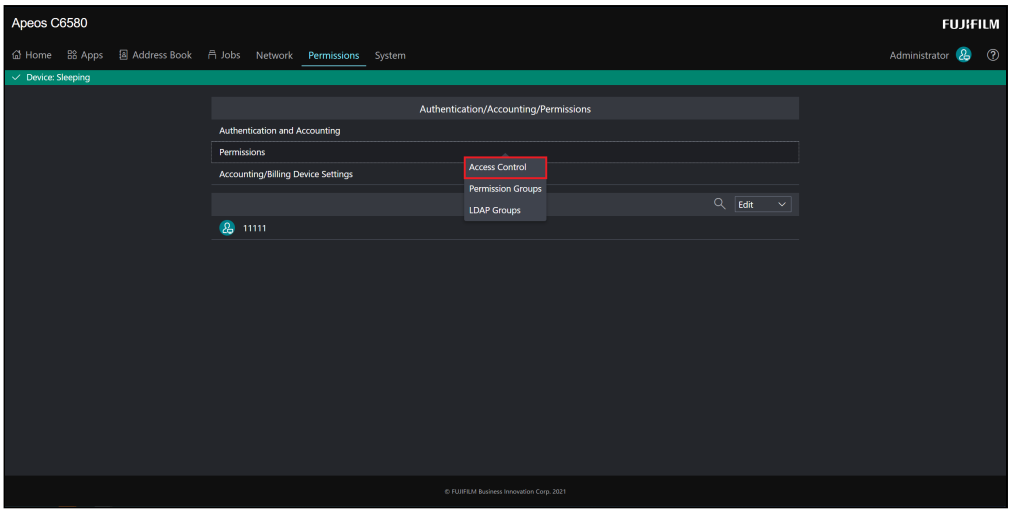
If you wish to define access to individual functions separately, set **App Access** instead of **Device Control Panel Access**.

If you uninstall the terminal from the MFD, these settings need to be set to **Unlocked** to allow access to the MFD's functions again.

Configure color copy restriction (optional)

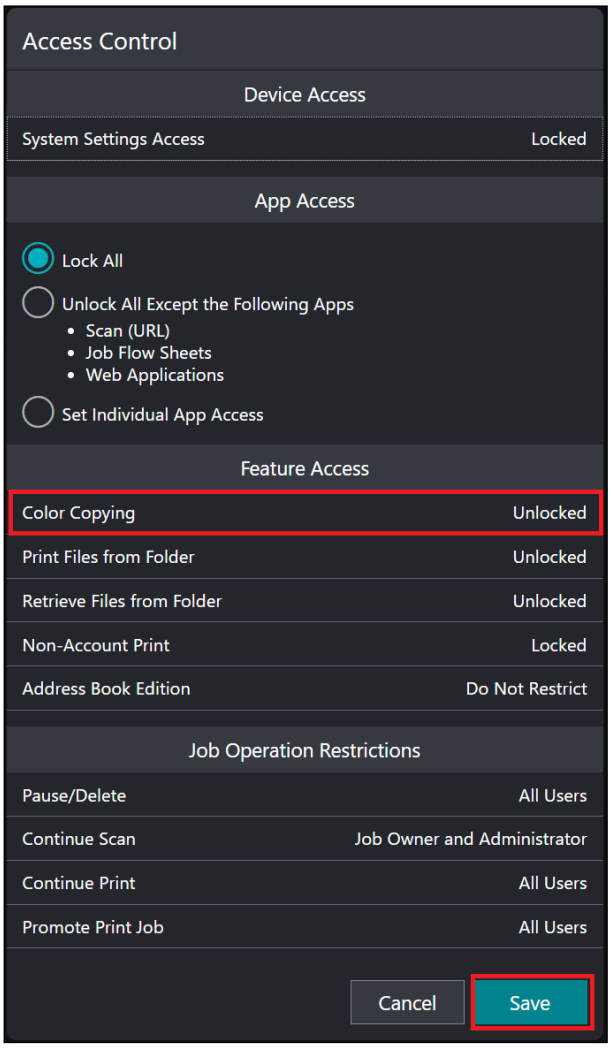
For the terminal to restrict access to Full-color copy by user access right setting, configure the Access Control in the following way:

1. Go to **Permissions** > **Permissions** > **Access Control**.



2. Set **Color Copying** to **Locked**.

3. Click **Save**.

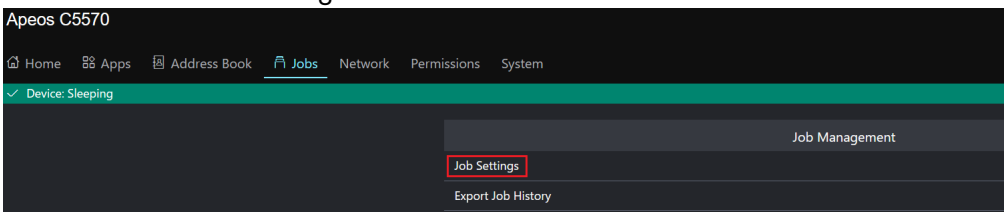


Configure access to completed jobs

> This configuration is required to report the accounting of scan and copy.

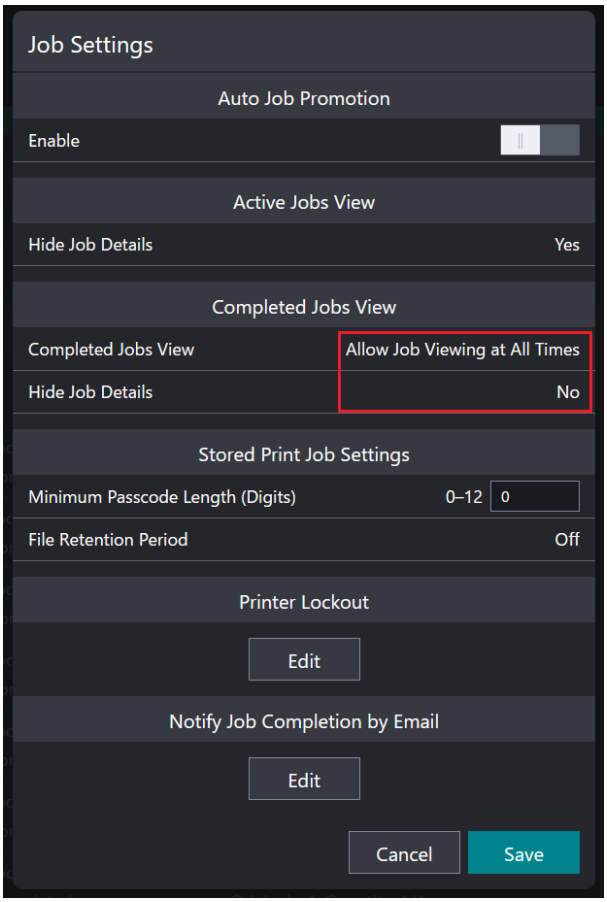
This configuration is not strictly required to use the terminal. Changing these settings enables the Cloud Terminal to track the actual failure of printing on the MFD (in addition to tracking any possible failure while processing the job, which is always done, regardless of this configuration).

1. Go to **Jobs** > **Job Settings**.



2. Change the following settings and save them
   - In **Completed Jobs View**, select **Allow Job Viewing at All Times**.

- In Hide Job Details, select No.



HP Terminals

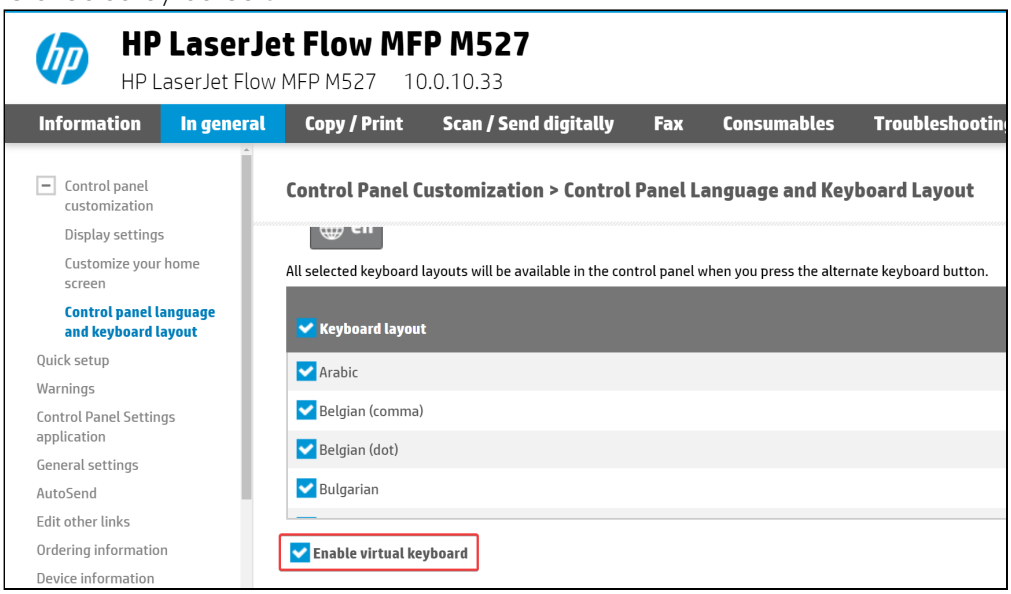
HP Workpath Gen 2 Cloud Terminal

Note that this manual is for HP Workpath Cloud Terminal which is in SAFEQ Cloud Web UI called Workpath Gen 2. This terminal connects directly to the cloud. The first generation of the HP terminal (OXPd/Workpath Gen1) can connect to the cloud only via a secondary gateway.

Prerequisites

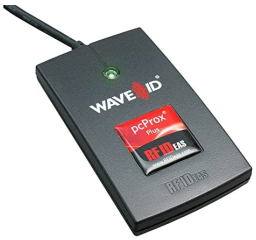
- Make sure you have Cloud Terminal Integration enabled (for information on how to do this, see Enable Cloud terminal integration guide).
- Minimum required firmware version is 5.6.0.1 or higher.
- Make sure that you have a signing certificate selected. To check this, log in to SAFEQ Cloud Web UI and navigate to Security > Security options> scroll down to PKI and encryption section. The Signing certificate field must not be blank.
- SAFEQ Cloud HP Workpath version 3.6 or later is required for Remote Configuration.
- Workpath has to be enabled on the MFD. You can enable it in HP Command Center or in the EWS interface at the MFD, on the Security tab.
- If you have a legacy Workpath terminal installed on the MFD, we recommend uninstalling it before proceeding further.

- The device must be added to your HP command center account. Navigate to the last window on the terminal, tap **HP Command Center**, and follow the wizard.
- Native keyboard must be enabled on the MFD (in some instances, it is disabled by default).
  - Log in to the EWS interface as administrator.
  - Go to **General > Control Panel Language and Keyboard Layouts**.
  - Select **Enable Virtual Keyboard**. If you don't see this checkbox, it means that the keyboard is enabled by default.



Card readers compatibility

VID	PID	Name	Note	
09D8	0310	Elatec - TWN3 Mifare USB Keyboard emulating	(untested)	
09D8	0410	Elatec - TWN4 Mifare USB	tested	

VID	PID	Name	Note	
09D8	0206	Elatec - TWN3 Mifare USB	(untested)	
04D8	FE86	SB - SBR 0993 MIX	(untested)	
0C27	3BFA	RFIDeas - pcProx Card Reader	(untested)	
03F0	0045	HP - X3D03A HP USB Universal Card Reader	tested	
076B	5428	HID - OMNIKEY 5427G2 (keyboard)	(untested)	
1FC9	80D9	Seawing - Card Reader, issue IB-3416	(untested)	

VID	PID	Name	Note	
214C	0309	YSoft Card Reader, MU03065 - configured for HP mode	tested	
0A5C	BD1F	JetDirect 3100w BLE/NFC Wireless Accessary, model 3JN69A	(untested)	

Limitations

When you change the authentication type associated with card login in the Embedded client configuration in the SAFEQ Cloud Web UI, the change won't take effect until the terminal is manually opened. For example, if you change the authentication type from **short ID** (PIN) to **short ID or card login**, the user will not be able to log in by swiping their card at the card reader until the terminal is opened. Once they open the terminal manually, the configuration change will be applied.

Cloud Print

- Color, Duplex, Number of Copies, stapling, punching, and other finishing options cannot be changed at the terminal.
- Print & hold functionality is not supported.
- Favorite print jobs are not supported.
- Only print jobs in the waiting folder can be printed/deleted. The printed tab shows historical data.

Scan

- Scanning only works when the MFD is connected to a primary server. This is a limitation of scanning and therefore applies to all terminals.

Copy

- The Cloud terminal doesn't support copying. The users must go to the native menu by tapping the home button on **My quick actions** screen and use the MFD's native copy application.

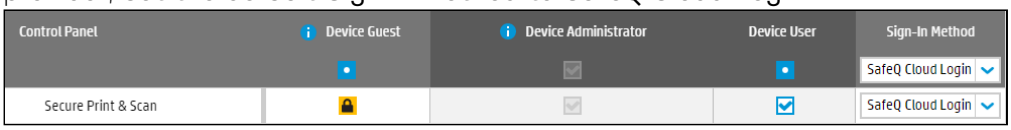
Installing the Cloud Terminal

Remote installation

1. In the HP Command Center, go to **Account** and choose the **SAFEQ Cloud Secure Print & Scan** solution.
2. Click **Manage**.
3. Click **Install** and follow the wizard.

After the installation, you must lock the MFD so that users cannot log in without authentication:

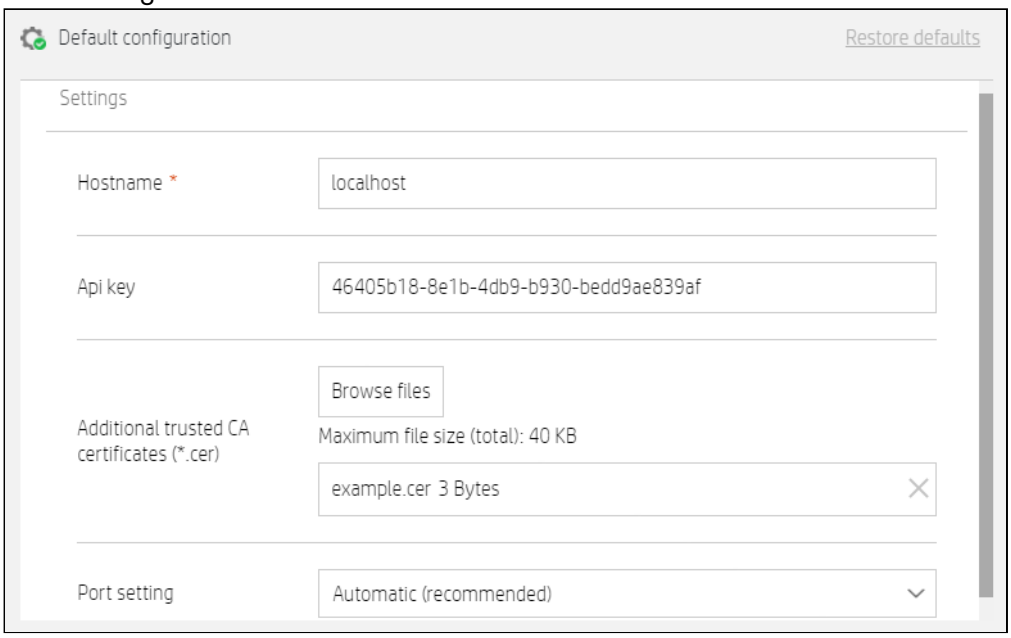
1. Log in to the EWS interface as an administrator.
2. On the **Security** tab, select **Access Control**.
3. Lock the **SAFEQ Cloud Secure Print & Scan** application, using the **SafeQ Cloud Login** authentication provider. If you wish to use **SafeQ Cloud Login** as the default authentication provider, set the default **Sign-in Method** to **SafeQ Cloud Login**.



If you skip this setting, launching the application without using the authentication provider may lead to issues with automatic logout when the MFD goes to sleep mode.

Remote configuration

1. In the HP Command Center, go to **Account** and choose the **SAFEQ Cloud Secure Print & Scan** solution.
2. Click **Manage**.
3. Click **Configure** and follow the wizard.



a. **Hostname** – Domain name of your tenant in SAFEQ Cloud. It can be a primary or a secondary server.

b. **API key** – A valid SAFEQ Cloud API Access Key. It defaults to **Default key for client and gateway**. To increase security, we recommend you to create a dedicated key. If you wish to use a dedicated key, log in to the SAFEQ Cloud Web UI and go to **Security > API access keys**. Click **Add**. Copy the key value and click **Save**. For more information see API access keys.

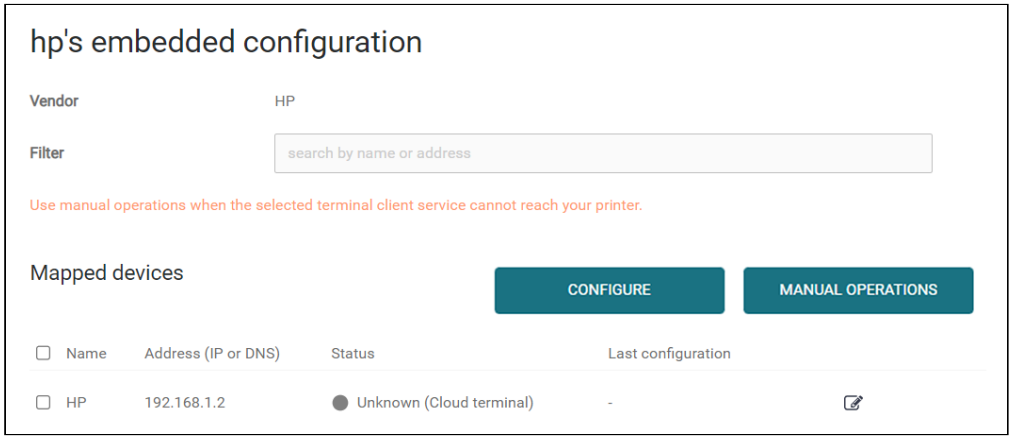
c. **Additional trusted CA certificates** – If the specified hostname does not provide a HTTPS certificate issued by a globally trusted Certification Authority, additional trusted certificates can be specified here. See the following section for details.

d. **Port setting** – Choose one of the following options. For more details about ports, see Requirements, section *Ports and protocols*.

1. **Automatic** – The recommended option. The terminal will check whether port 443 is open on the host. If it is, the terminal will use it for all communication. Otherwise, it will use legacy ports (8705 and 7400). The chosen ports will be stored after the first start of the terminal and used until the terminal is reconfigured.
2. **Use 443** – The terminal will use port 443 for all communication.
3. **Use legacy ports** – The terminal will use ports 8705 and 7400 for all communication.

Automatic local configuration

If the MFD is located in a network with a Secondary gateway and is configured to connect to SAFEQ Cloud using this gateway, you can create and deploy the Embedded configuration as described in Embedded Terminals' configuration.



Additional trusted CA certificates

The terminal uses HTTPS to connect to the server specified by a hostname securely.

The WorkPath SDK comes preinstalled with a list of globally trusted Certification Authorities, meaning that if you are connecting to a cloud server, chances are that no special configuration is needed.

If you are connecting to a secondary gateway or OmniBridge, we recommend using the Automatic local configuration described above.

Only in rare cases, you might need to configure certificates manually within HP Command Centre in the following ways:

1. Using an in-house Certification Authority.

2. Using a Certification Authority that comes bundled in SAFEQ Cloud.

> The list of CAs trusted by the WorkPath SDK is distinct from the CAs trusted by the native functions of the printer.
>
> Natively trusted CAs can be manipulated in the printer's web interface, usually in the Security section, and have effect, for example, on outbound LDAPS or SMTP connections.
>
> However, they have no effect on the Cloud Terminal or other apps that use WorkPath SDK.
>
> This counter-intuitive behavior is confirmed by HP. The only way to grant additional trust to the Cloud Terminal is described in this guide.

Prerequisites

The server you are connecting to must have a domain specified, not just an IP address.

There must be a certificate assigned to this domain in SAFEQ Cloud. See Certificates.

Certificates

You must have the root CA certificate in PEM format.

If you are using the default SAFEQ Cloud CA, you can copy is from here:

```
-----BEGIN CERTIFICATE-----
MIIDMDCCAhigAwIBAgIIKSkOK6vJeiIwDQYJKoZIhvcNAQELBQAwNjELMAkGA1UE
BhMCREsxFjAUBgNVBAoTDUV2ZXJ5b25lUHJpbnQxDzANBgNVBAMTBkhDUCBDQTAe
Fw0xNzA3MzEwNzI3MzBaFw0zNzA3MjYwNzI3MzBaMDYxCzAJBgNVBAYTAkRLMRYw
FAYDVQQKEw1FdmVyeW9uZVByaW50MQ8wDQYDVQQDEwZIQ1AgQ0EwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDextBfBlinhJfLxLzMSyATyHsJMMnfl/oY
jrEFxXnR/7p8KvvXSGwKzF2ZUvoggtvZUe0O94GIttZEwoQuyj7r6RrO7OtT5F9S
BLk2jKx6O4/JD5AlOMsORwRXdFSmhC4CNYWQ7EmPIK6DR7pEZSSkk49wPfcaT8Un
/745hya7p9Asl8NmyrADOjy3BWhLysXnM7qH8gzrYH96X9X/KfRZLSw1IgA/vUbr
+RRknYR4R/Hp7PYyW6HihDlW6eb0yLO5USWpVMHUhyEGPgV8DVU9Z5Q/8xxN5FoT
snvM//HnJnPXCz+J6voJF9DYN3dbRmpp2OiZ+lFdluruRbOT8i9VAgMBAAGjQjBA
MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRsfCK7
yUhtZmk//7xnQU5jbqqg3TANBgkqhkiG9w0BAQsFAAOCAQEAwTj0rIr6uKUpo0T7
Hx+cILl+LeIwmmlkNC8zeE6B5Ulan2k7KWP6uAeM7FkKcFUtWpd036S96yjjw2KD
auO1+xjlL2wRyQCG+Y0EZ/4JNHXVAWpxvbt25jFMqs5OFYNLu3/iRLRsfbi0/+2Z
PdfIMpyRIDK+Y7rgLniVfnwAfxGD278I6v0s+6LPAS0ax4P2lr6jjLeWxC3hM/XG
HPQEESpyqe859xWHQXpu/87SNZn0o8Ka57x+0kE7fNjQE6ksQbl948aIQgwZo5UL
TtoxV35fWsmrsRNUm5BdfIBrSLbSWqIlhy4FbOj7Hr04qTqYBO82tRlB6Hx53nTL
SXShZw==
-----END CERTIFICATE-----
```

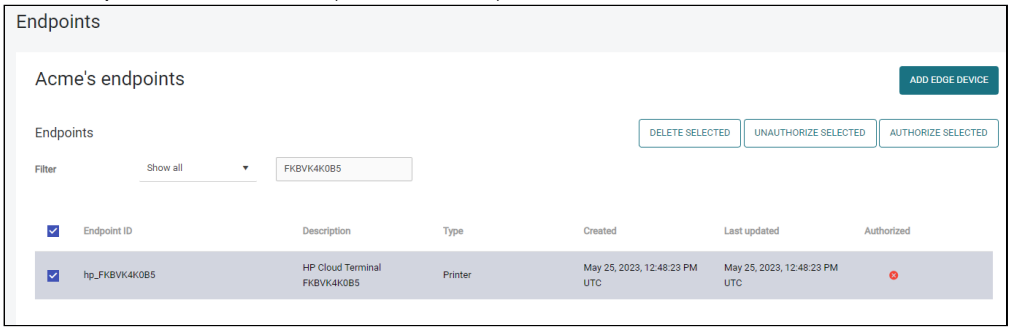
You can specify more than one trusted CA. For example, for migration purposes.

The default item in the configuration, named example.crt, does not contain a certificate and serves no practical purpose other than being a default. It is safe if you remove it but does no harm if you keep it.

Registering the Cloud Terminal in the SAFEQ Cloud Web UI

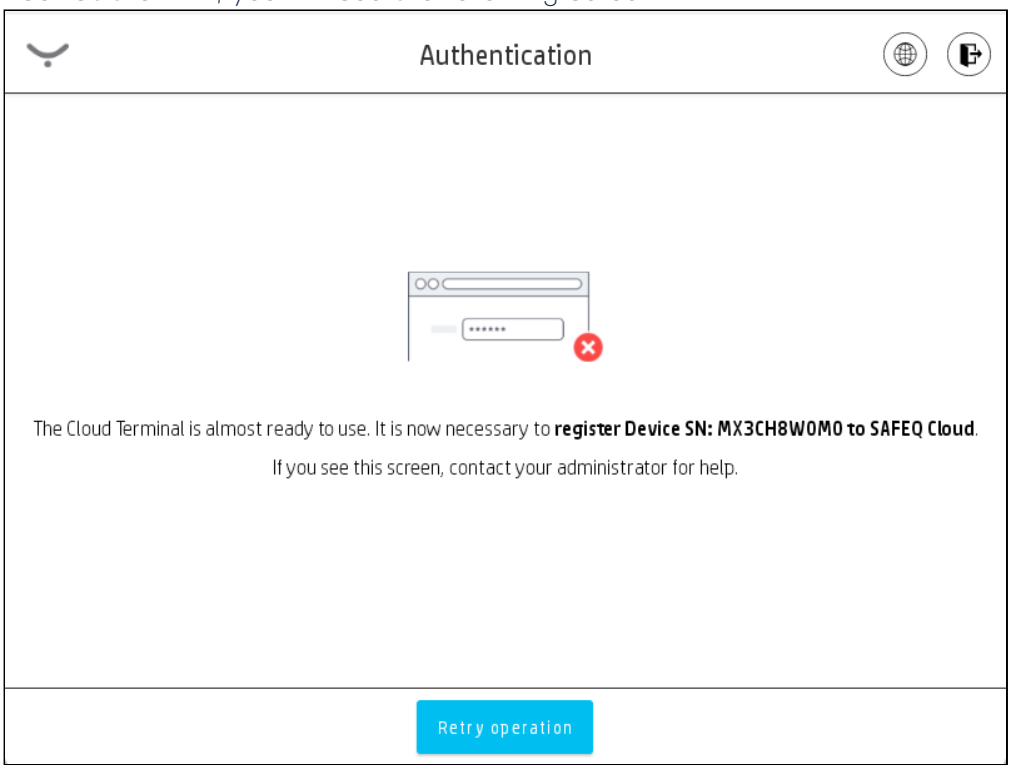
1. After the terminal installation from the HP Command Center, you will see the following screen on the MFD. Note down the endpoint ID. The endpoint ID is the MFD serial number prefixed with "hp_".

2. In SAFEQ Cloud web UI, go to **Security > Endpoints** and find the entry that contains the **endpoint ID** from the previous step.



3. Select the entry and click **Authorize selected**.

4. Back at the MFD, you will see the following screen:



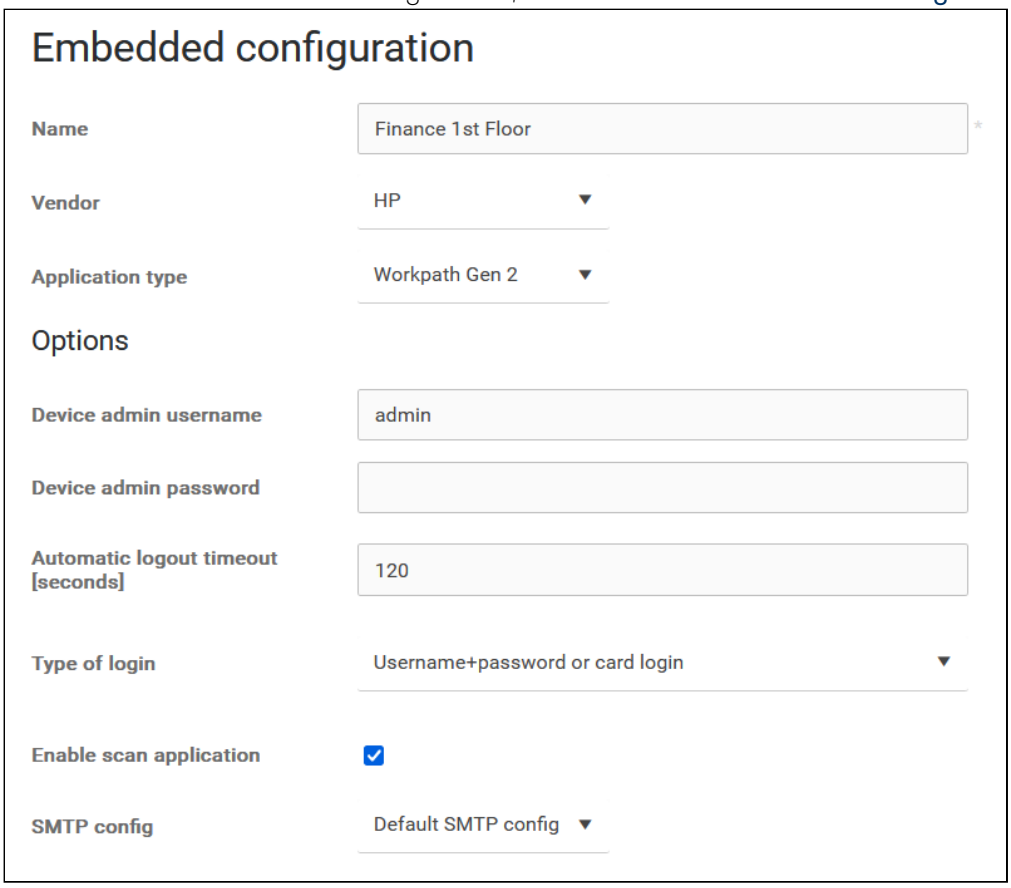
If the terminal on the MFD is reinstalled, you must delete the already authorized endpoint before it can be re-authorized.

The terminal will display instructions on how to do that.

Adding HP Workpath printer and Embedded configuration in SAFEQ Cloud Web UI

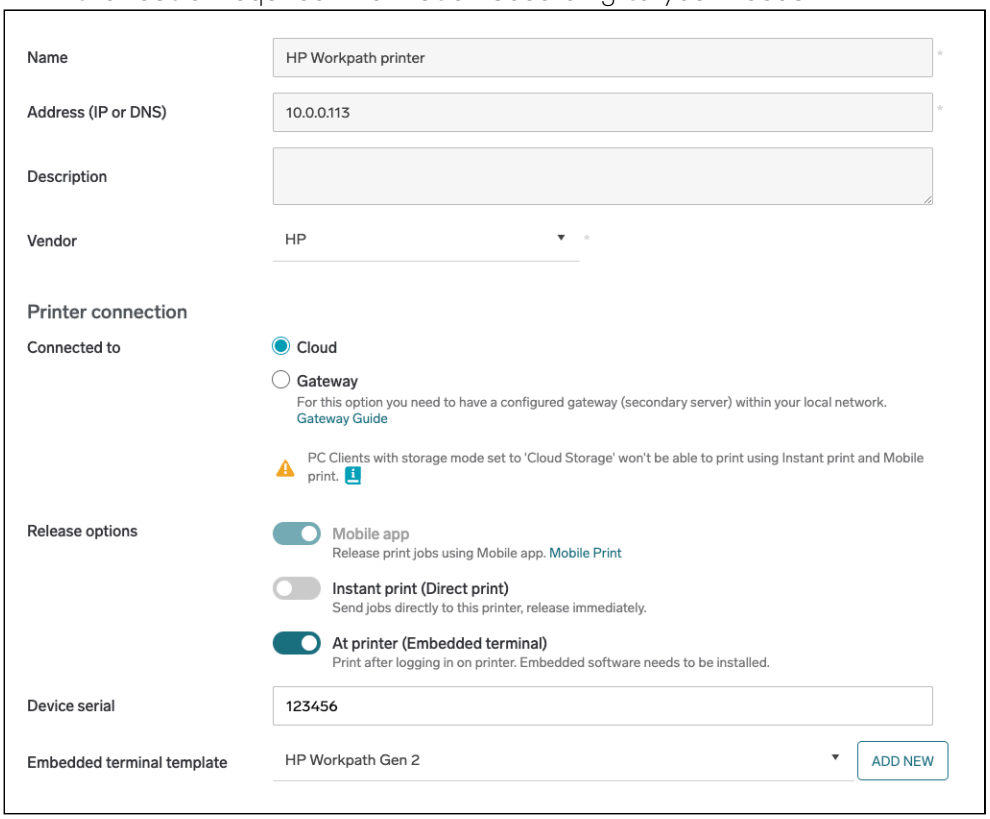
1. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
2. If not done already, create an embedded configuration for HP Workpath by clicking **Add**.
3. In **Vendor**, select **HP**.
4. In **Application type**, select **Workpath Gen 2**.

5. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.



6. Go to **Printers** and click **Add**.
7. In **Vendor**, select **HP**.
8. In **Address**, fill in the MFD IP address.
9. In **Device serial**, enter the serial number which was presented on the MFD. Leave out the **hp_** prefix.

10. Fill in the rest of required information according to your needs.



11. In **Embedded configuration**, select your HP embedded configuration from the list.
12. Click **Save**.
13. The MFD will now display a login screen with your chosen authentication type.

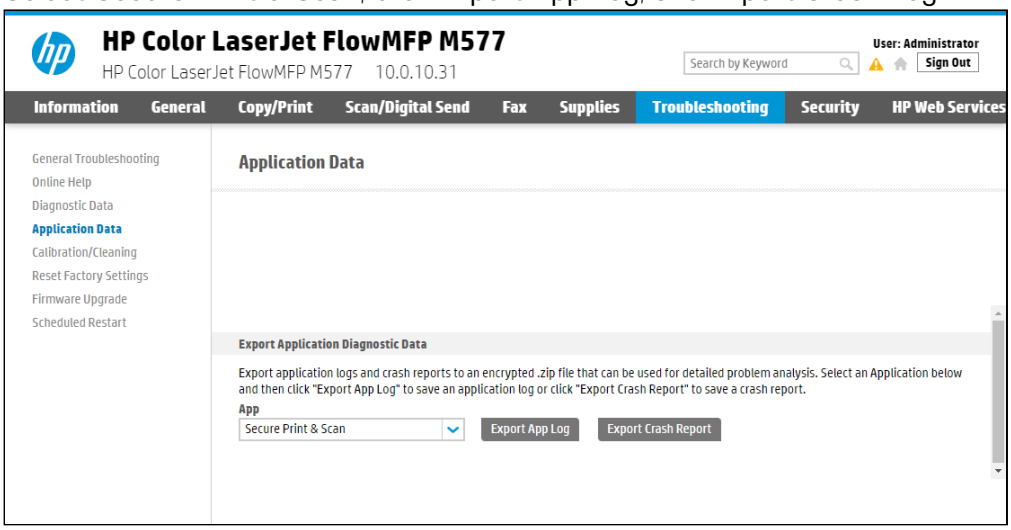
Troubleshooting

When reporting an issue with the HP Cloud Terminal to our service desk, please include logs from the MFD.

To obtain the logs:

1. Log in to MFD's web administration interface and navigate to **Troubleshooting > Application Data.**

2. Select Secure Print & Scan, click Export App Log, and Export Crash Log.



HP Workpath Gen 1 Embedded Terminal

> ⚠ This is the HP Workpath Gen 1 terminal, not the HP Workpath Gen 2 pure cloud terminal. For the pure cloud terminal, see HP Workpath Gen 2 Cloud Terminal.

This guide is to install, configure and setup the HP Workpath Application which has the following parts:

- Prerequisites
- Installation of EveryonePrint HCP Pull Print from Command Center
- SAFEQ Cloud Server Setting using Web UI
- EveryonePrint HCP Authentication application remote configuration
- HP Workpath embedded application setup

Prerequisites

- Ensure all necessary ports on SAFEQ Cloud server are open. Please refer to Ports and Protocols, section *Embedded clients to Cloud Server or Gateway*.
- If using SAFEQ Cloud Client in local storage mode, please ensure that all necessary ports on the MFD are open. Please refer to Ports and Protocols, section *SAFEQ Cloud Clients to printers – print operations*.
- On the MFD, under Network Identification, please make sure that you configured the Host Name, Domain Name and DNS.
- If you have an account on SAFEQ Cloud Cloud, please ensure that the communication between the MFD and the SAFEQ Cloud server is working.
- On the MFD, under Security -> General Security, HP JetAdvantage Link Platform setting must be enabled.
- If the mobile service does not need the SAFEQ Cloud CA, please skip this. Otherwise, you need to have a valid certificate under "Private certificate chains."
- As a precondition to establish the communication between a printer and SAFEQ Cloud server successfully, the printer has to trust the Certification Authority (CA), which issued certificates used by SAFEQ Cloud server. By default, it is the well-known CA "Let's Encrypt". The "Let's

Encrypt" root certificate "ISRG X1" can be downloaded from the web page https://letsencrypt.org/certificates/. Please note that at the Vendor or Customer level, CA certificates other than those issued by "Let's Encrypt" can be specified.

- Set up Mobile Print under the customer. Select from drop-down the mobile service and make sure that "Enable MDM Single Sign On" is unchecked.
- Set up the remote configuration from HP Command Center for EveryonePrint HCP Authentication application.
- SAFEQ Cloud API Access Key is required, the Default key for client and gateway is preconfigured. See Secondary Gateway mapping.

Installation of EveryonePrint HCP Pull Print from Command Center

The access can be exclusively provided by HP after their Verification and Validation process. HP embedded contains two applications which can be downloaded and installed from HP Command Center:

- EveryonePrint HCP Authentication
- EveryonePrint HCP Pull Print

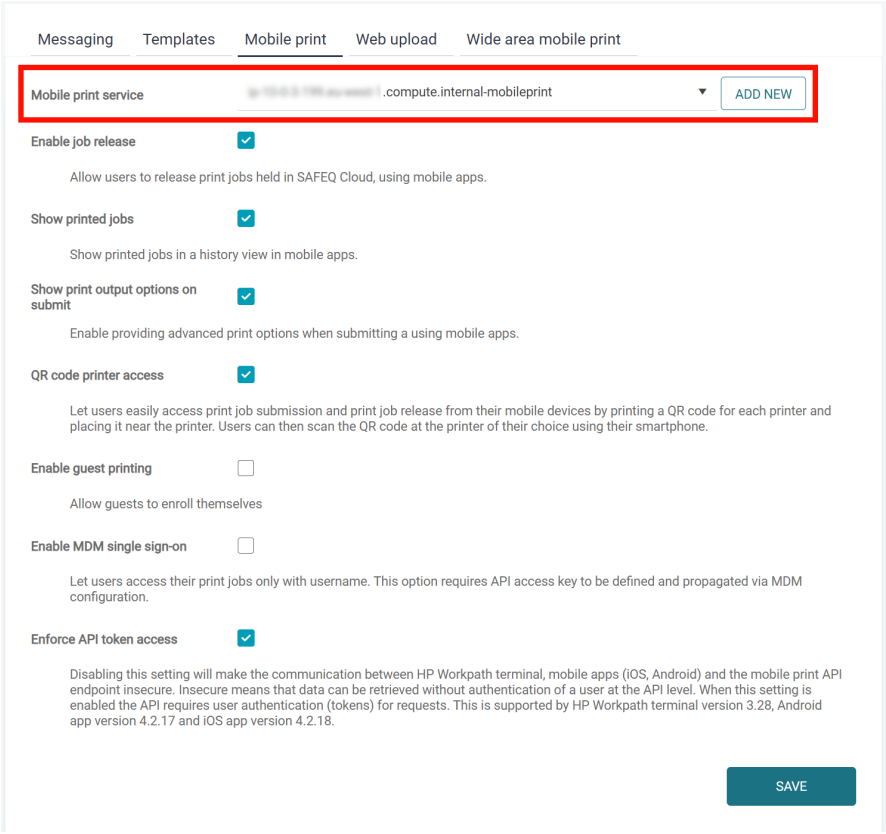
On the MFD, check the following:

- In **Security > Access Control**, EveryonePrint HCP Pull Print application should be locked, using EopAuthAgent
- In **HP Web Services**, enable the web services

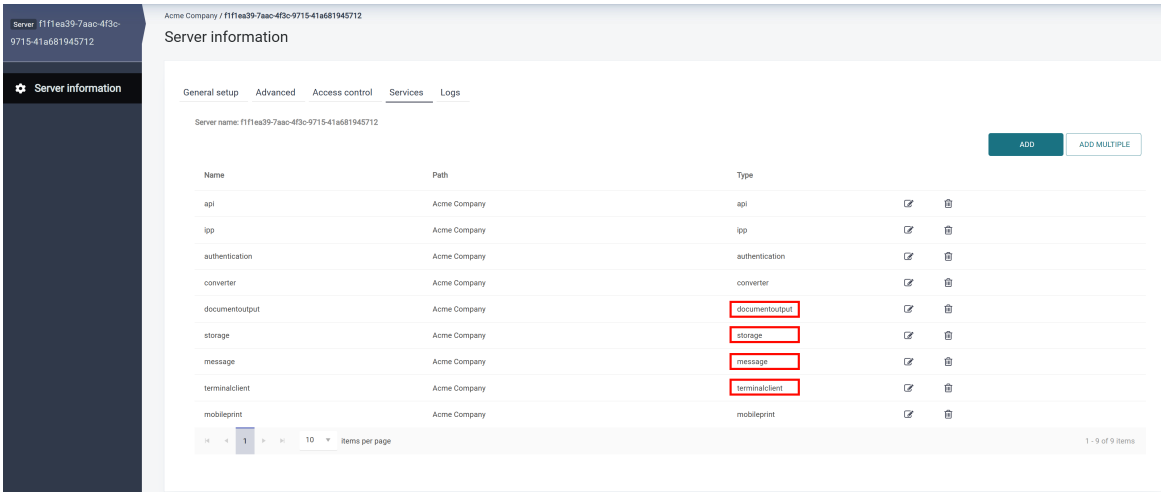
> For SAFEQ Cloud Workpath app 3.20 & above, you must install HP Firmware 5.4 as a minimum.

SAFEQ Cloud Server Setting using Web UI

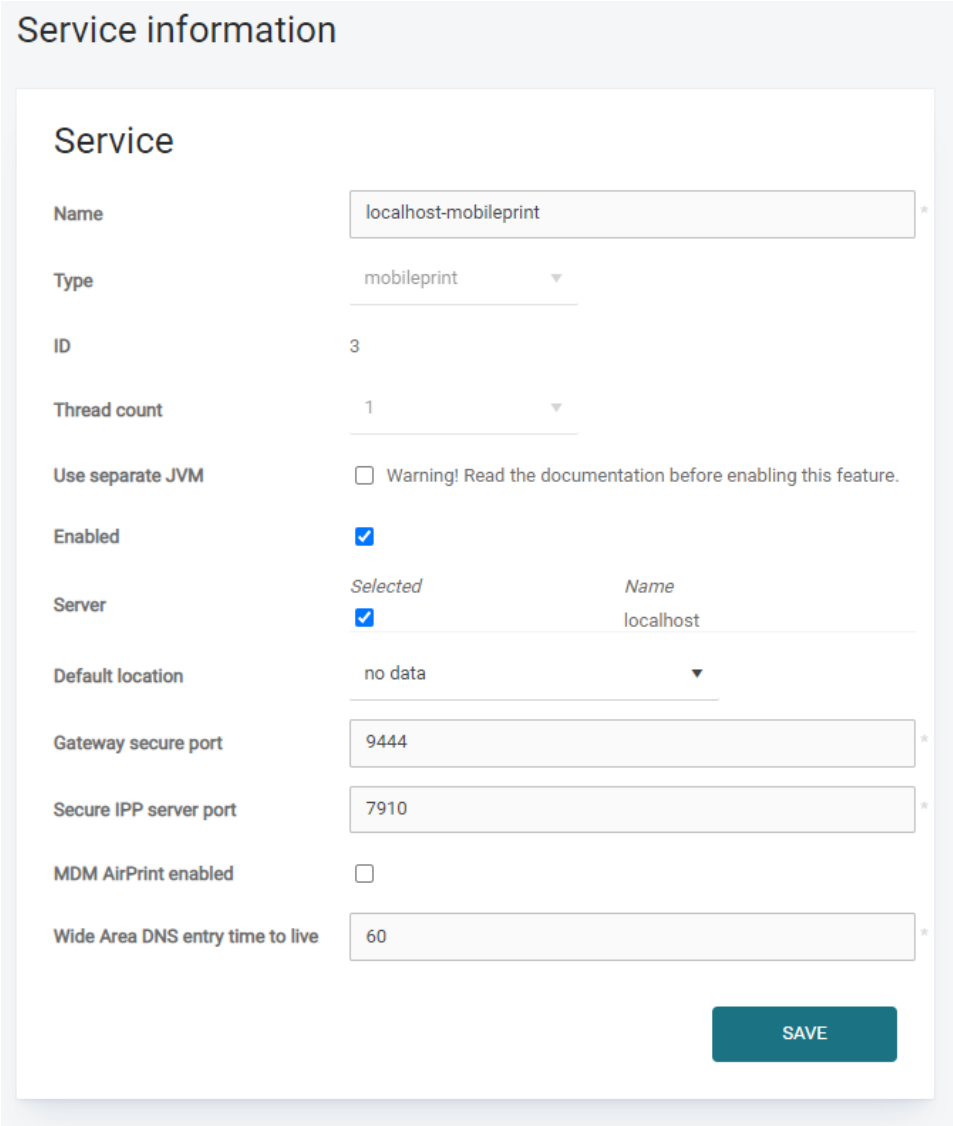
1. Log in to the SAFEQ Cloud Web UI.
2. If you are hosted on Y Soft side, make sure you have selected Primary's mobile print service in **Settings > General settings > Mobile Print** tab.



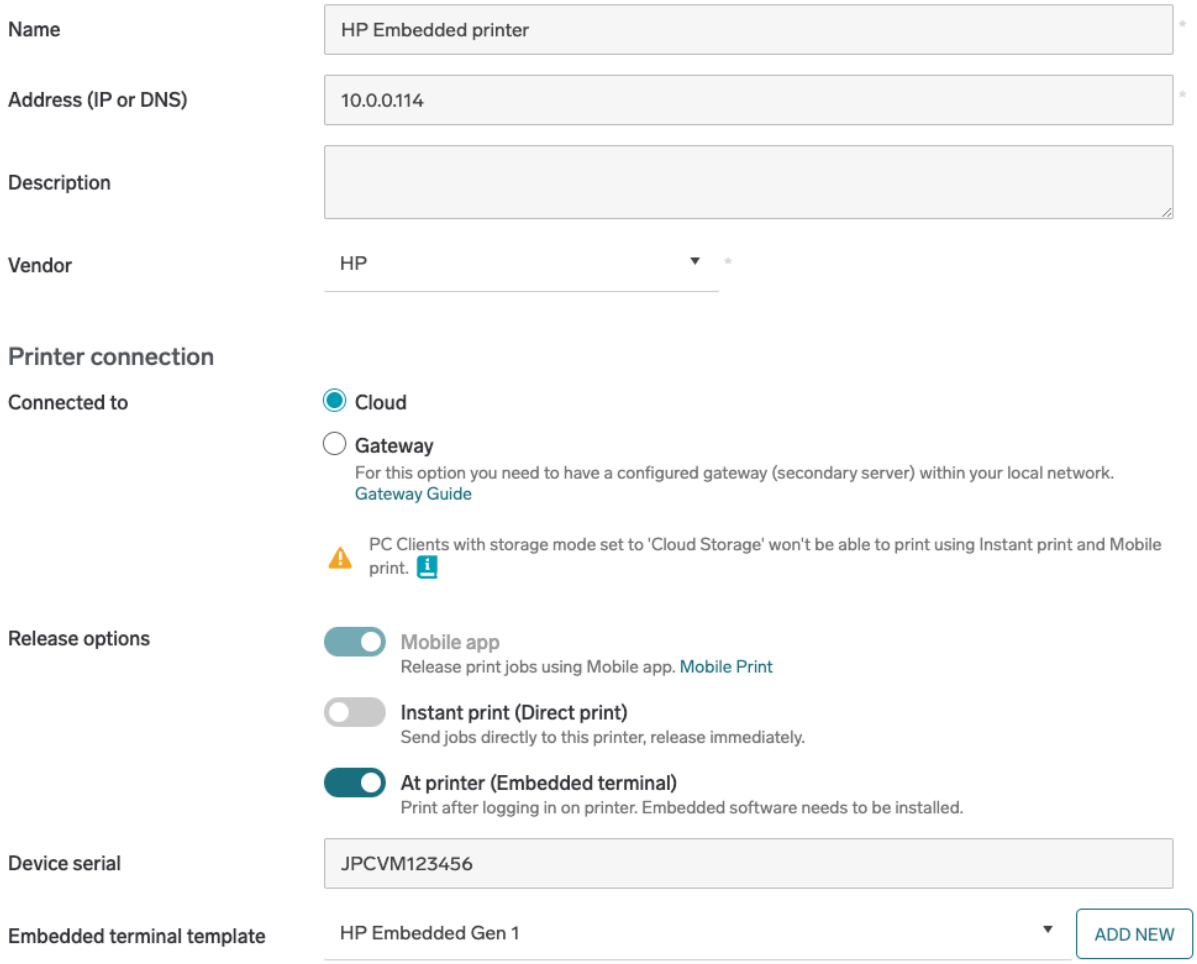
3. Otherwise, make sure that you have the following services under your hosted server (gateway): terminal, document output, mobile, and messaging.



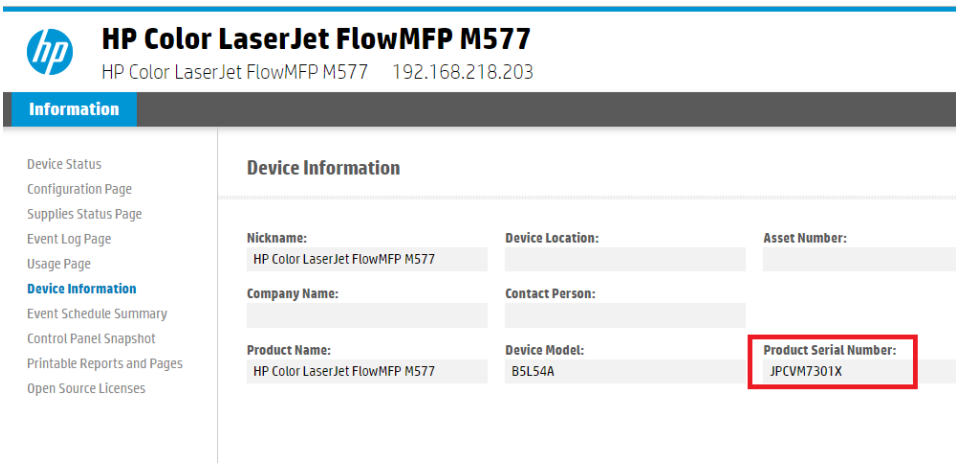
4. Set the mobile service in the following way:



5. Click Messaging and fill in all the required details.
6. Create an embedded configuration. It is required for Scan to My Email functionality (note that this feature is available in the embedded application only if "Enable scan application" is checked). Fill in the required details: Name, Vendor as HP, valid device admin username and password, USB Card Reader Vendor ID, USB Card Reader Product ID, Check Enable Scan Application, Select SMTP Configuration, Select Mapped Devices.
7. Add one Input Port under the customer. Select Port Type as Pull Queue for it.
8. Add the HP printer. The following parameters are mandatory:



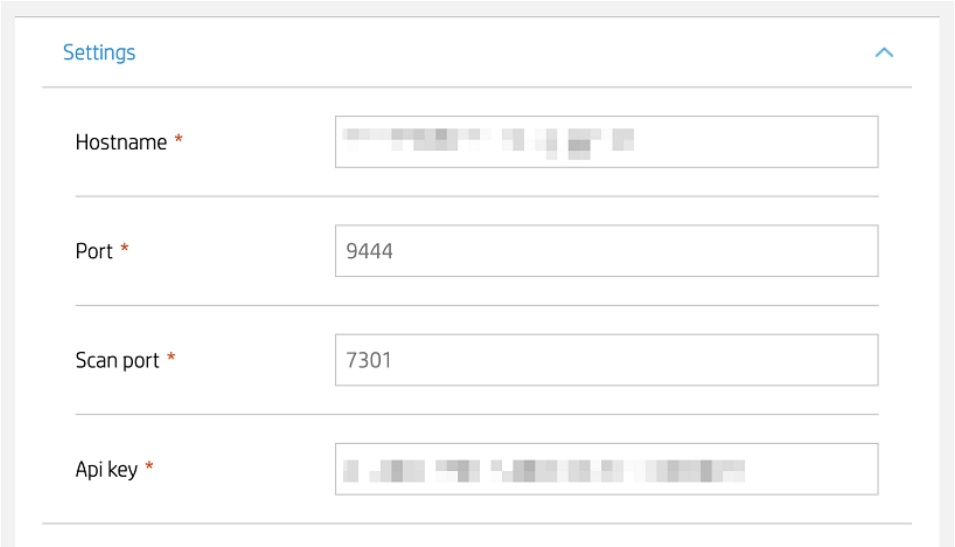
You can retrieve the device serial number from the MFD UI:



EveryonePrint HCP Authentication application remote configuration

Note – SAFEQ Cloud HP Workpath version 3.6 or later is required for Remote Configuration

The remote configuration can be done from HP Command Center by choosing the EveryonePrint HCP Authentication application, selecting the option **Configure** and following the wizard. The below settings screen is displayed:



Hostname
Domain name of the account to which the applications will be connecting.

Port
The secure (SSL) server port for the mobile service. The default value is 9444.

Scan port
The secure (SSL) server port used by the scan to my email feature. The default value is 7301.

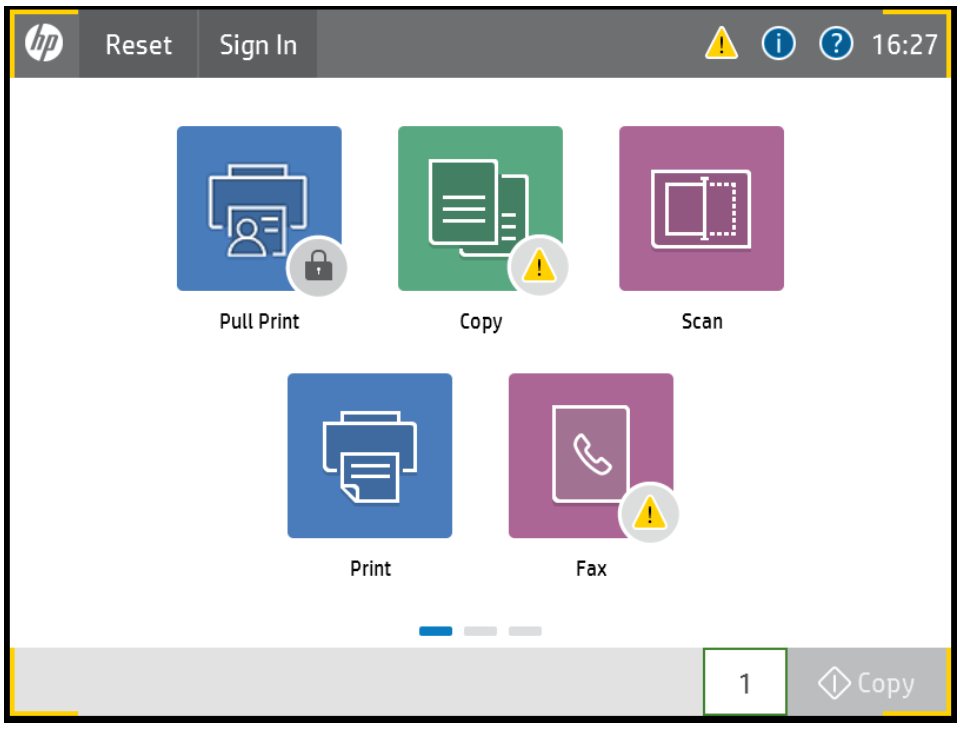
Please make sure that 7301 and 9444 ports are opened.

Api key

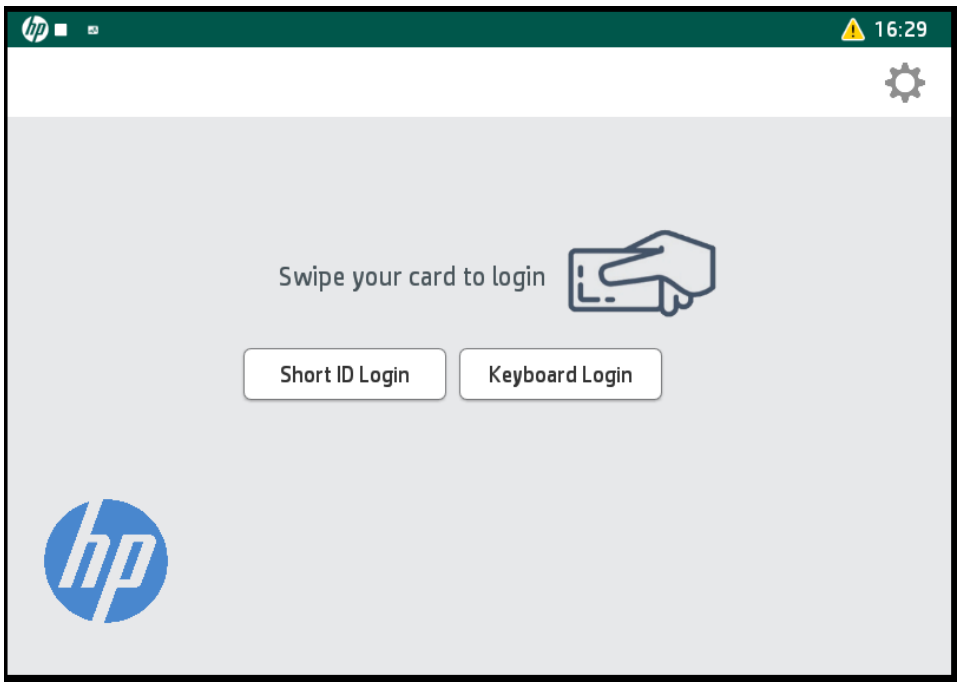
A valid SAFEQ Cloud API Access Key. If defaults to Default key for client and gateway, but customers who have disabled or changed the default key have to supply a valid alternative.

HP Workpath embedded application setup

1. Go to the MFD. The Home screen with installed applications will be displayed.

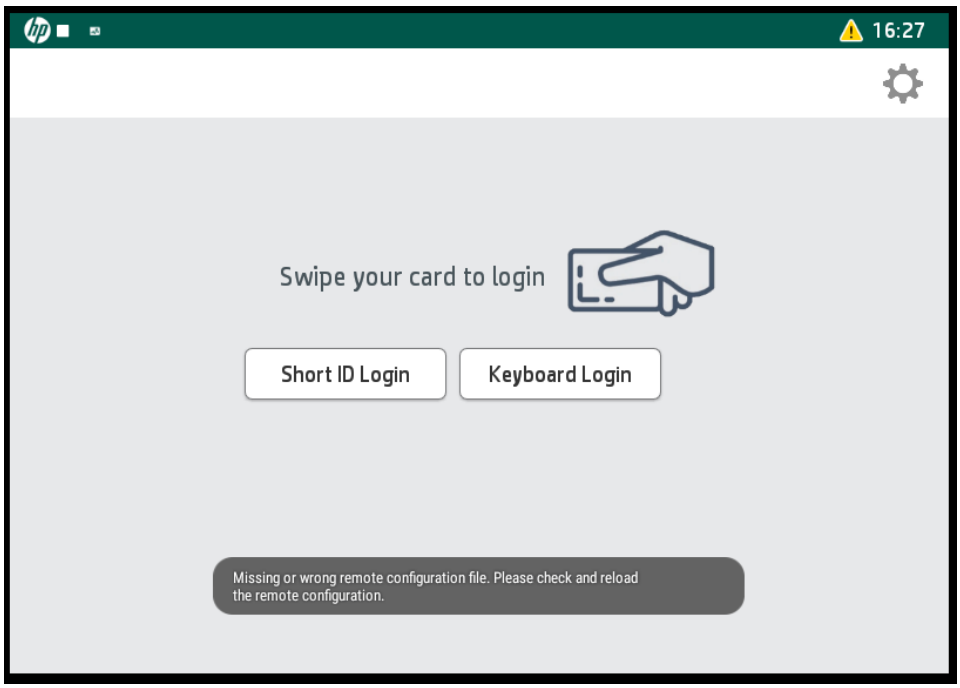


2. Click on Pull Print Icon to go to the application. The login on MFD is possible using "Short ID Login" or "Keyboard Login" or by swiping the card.

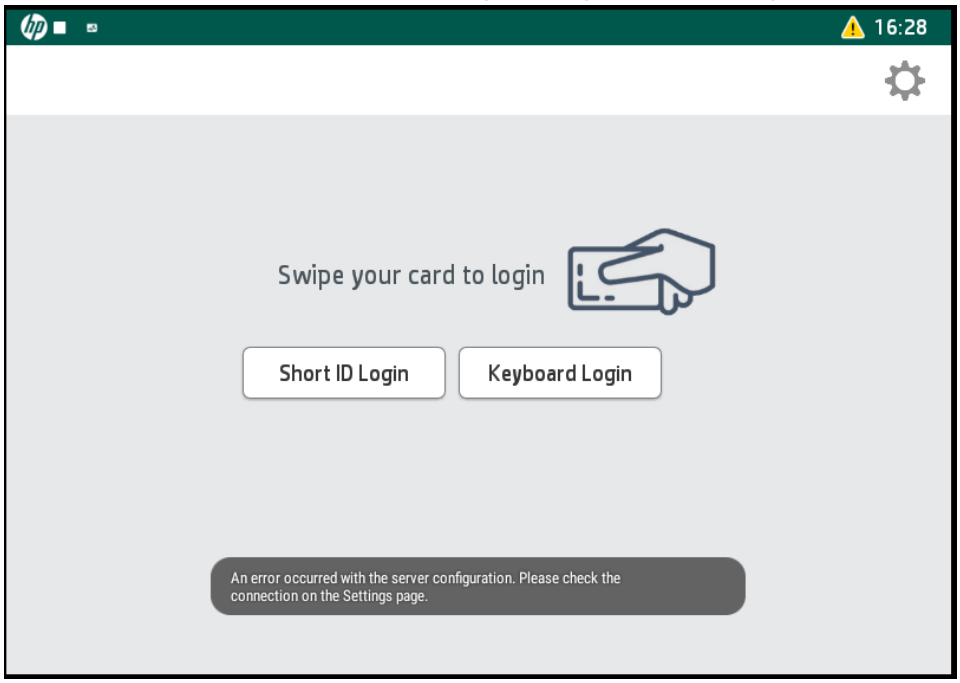


At this step the remote configuration file is loaded in the application and is checking the server configuration. Also, at this step the account logo is retrieved from the server and displayed in the main screen.

- In case the application has no remote configuration file uploaded, the error from the below image will occur:



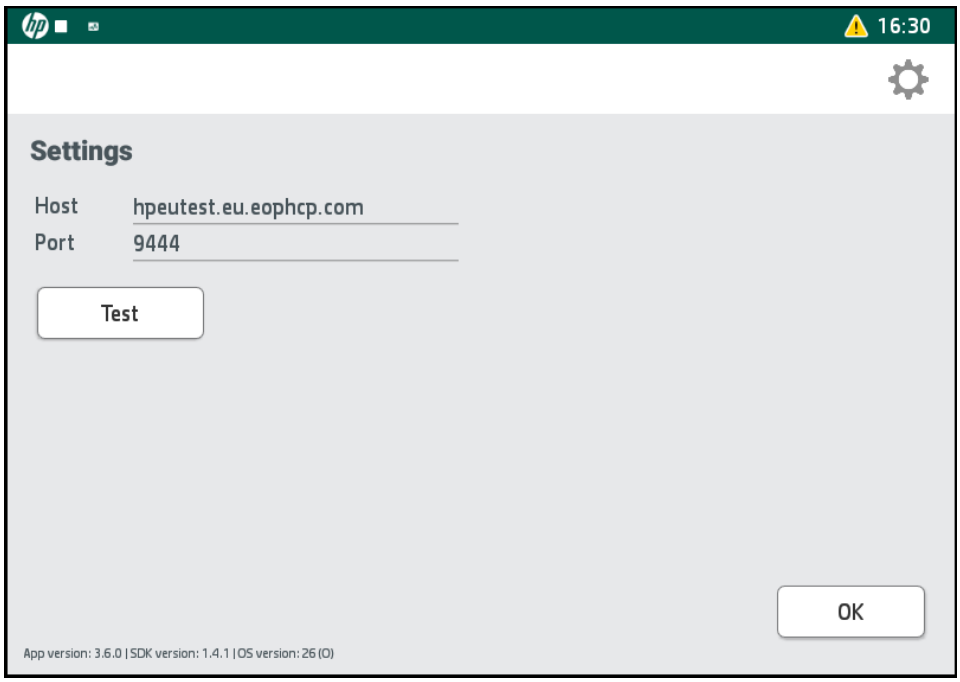
- In case the admin uploaded wrong settings in the configuration file, this error is displayed:



For the above two cases the admin should re-upload a valid configuration file from HP Command Center. If the authentication application is still opened, the new configuration settings will be automatically reloaded.

3. Go to the Settings page by clicking on the top-right icon to check the settings and SAFEQ Cloud connectivity. The host and the port fields are read-only and their values are retrieved from the remote configuration file. The "Test" button is used for testing the SAFEQ Cloud connectivity. The API Access Key is not displayed, but the key is also validated in the connectivity test. The OK

button will set up the connection to the server according to the settings for future actions. Then, the application will navigate to the main screen and the account logo will be refreshed.



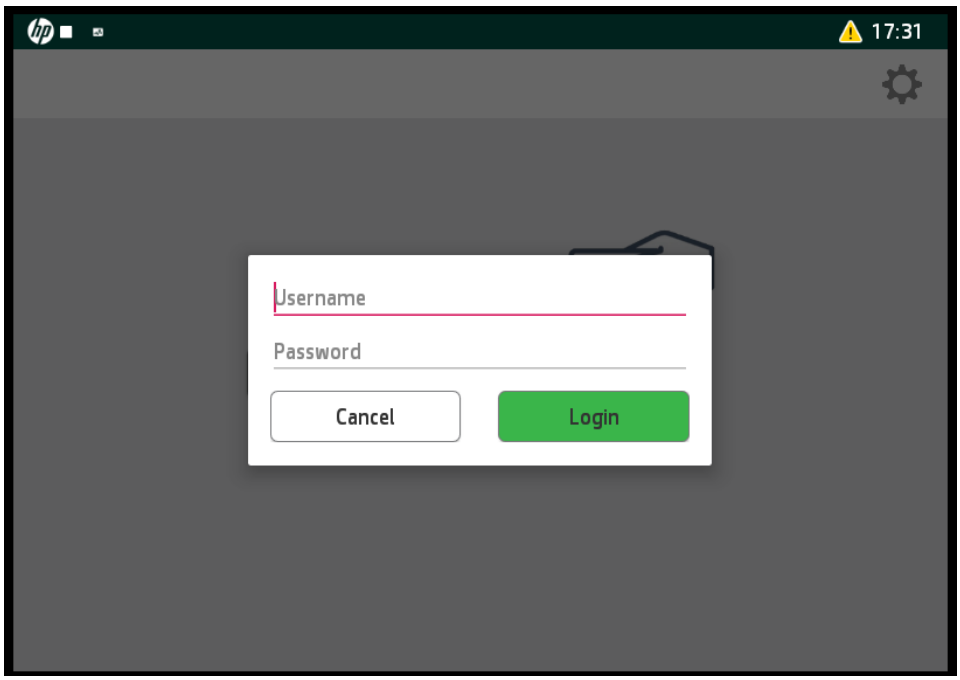
Important Remark: HP MFD should have internet connection

4. User can login to the application using one of those three methods:

- Short ID login: use the "Short ID" value from the user you want to login
- Keyboard login: use the "Username" and "Password" values from the user
- Swipe card: it is working from the application and from HP Launch screen

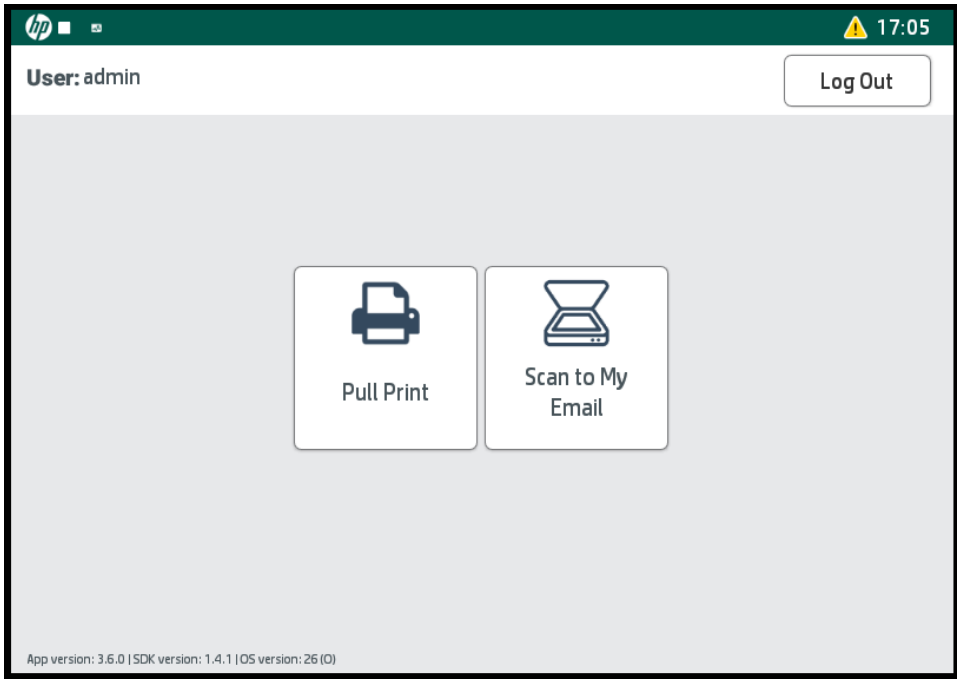
For card authentication please refer to section Supported Card Readers – VIDs and PIDs to check the supported card readers.

When user will swipe card for the first-time, application will ask for card registration process. Register the card using Username and Password.



5. After successful login using any of the three methods there are two options:

- the screen with "Pull Print" or "Scan to my email" buttons is displayed in case the setting "Enable Scan application" under the embedded configuration is checked. By pressing one of them, the user will be redirected to the corresponded page.

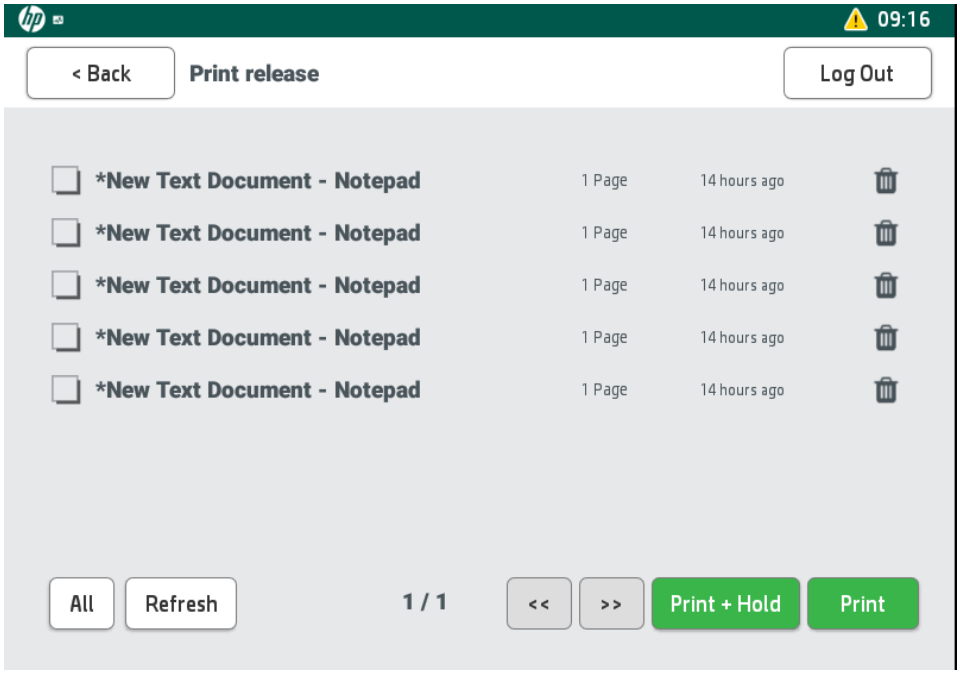


- if the "Enable scan application" setting is unchecked then the Pull print page is displayed after launching the application.

6. Pull Print

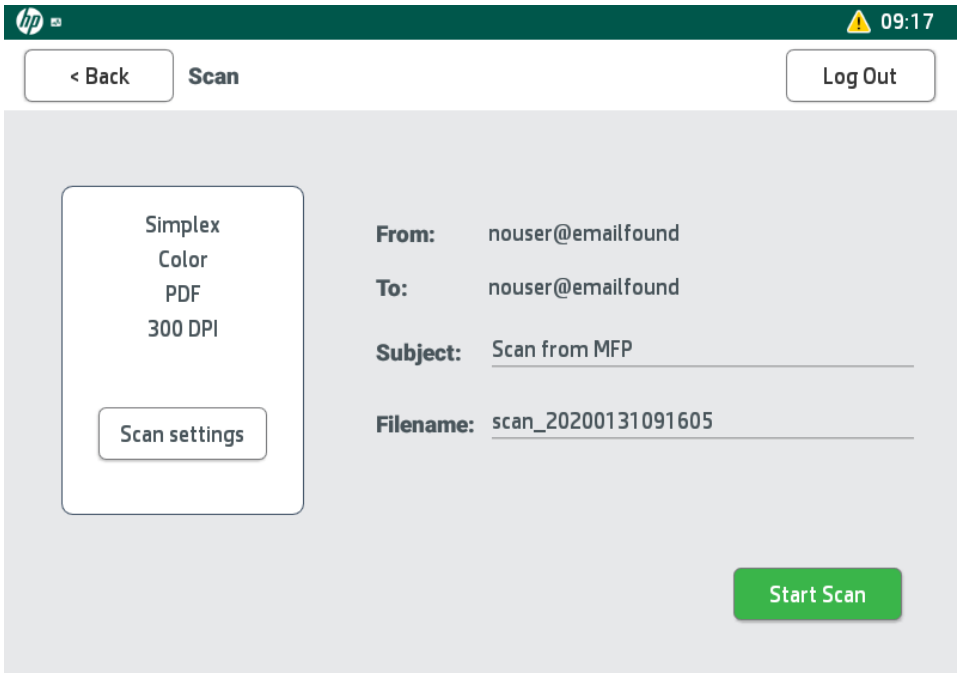
- All – select all jobs from all pages
- Refresh – refresh the job list, retrieve the job from the server
- Navigation buttons

- Print – will print the selected documents on MFD
- Print + Hold – will print the selected documents on MFD. The printed files will remain stored in MFD and will be available for another jobs
- Delete button on the right on every row will remove the job from the server

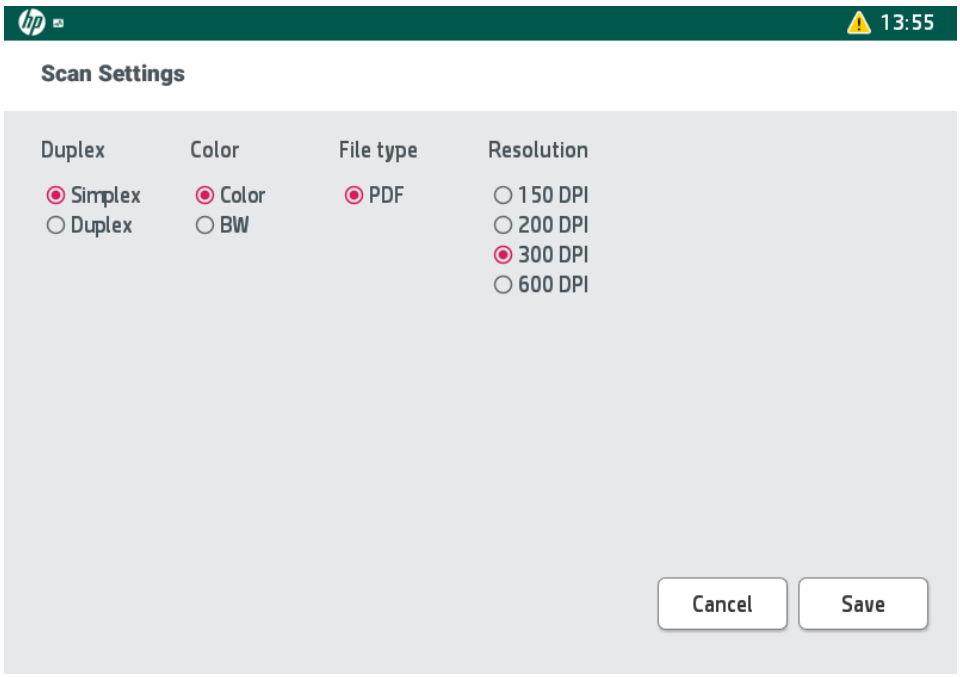


7. Scan to My Email
"Start Scan" button will begin the scan process.

If your gateway use the standard certificate, you will have to install the SAFEQ Cloud CA, certificate in the printer for scan jobs to send successfully.



By pressing the button "Scan settings" user can select settings for scan operation.



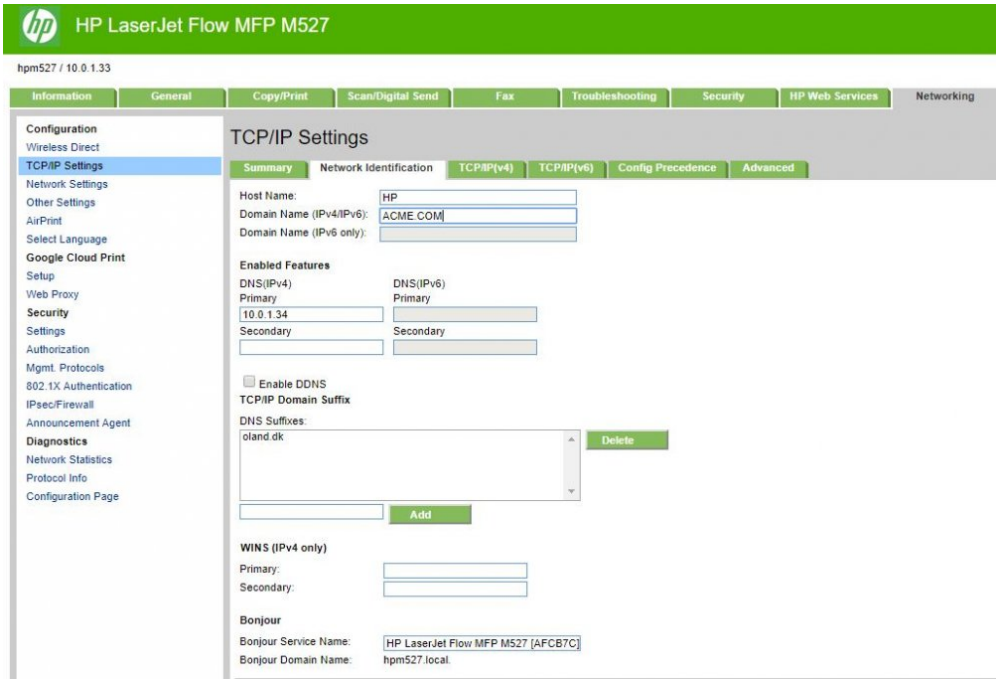
HP OXPd embedded

Configuring your secondary gateway

Before you begin, you must configure your secondary gateway. See Secondary Gateway mapping.

MFD preparation

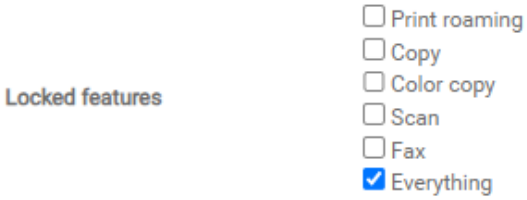
1. Log in as administrator and change the admin password.
2. Verify that your MFD has proper DNS configured, so that when the MFD connects to *berlin.acme.com*, it can resolve that DNS record to the correct IP.



After the Printer is restarted, push the Embedded configuration from the embedded screen in SAFEQ Cloud. Remember PID/VID if Cardreader is used.

Lock/Unlock third-party applications

You can lock/unlock other third-party applications like Autostore when using SAFEQ Cloud embedded client for compatible HP devices.
While setting up **Embedded Configuration** in the SAFEQ Cloud Web UI, select **Everything** in **Locked features** section.



Konica Minolta Terminals

Konica Minolta IWS Gen 2 Cloud Terminal

Prerequisites

- Make sure that you have Cloud Terminal Integration enabled (for information on how to do this, see the Enable Cloud terminal integration guide).
- Make sure that you have a signing certificate selected. To check this, log in to SAFEQ Cloud Web UI and navigate to **Security** > **Security options** >scroll down to **PKI and encryption** section. The **Signing certificate** field must not be blank.
- Konica Minolta MarketPlace is installed on the MFD.

Limitations

Card readers

- Keyboard Wedge: In order to use Card Readers with Keyboard Wedge, the MFDs must have a correct Loadable Device Driver installed.
- When the card reader is in keyboard mode, you must select the US keyboard layout.
- If you use a card reader in the Keyboard mode, the users won't be able to swipe their cards when the input field is focused.
- Other Card Readers: See the manufacturer's documentation for installation and setup.

Cloud print

- Toner save (economy printing) is not supported.
- Printing 2 or more pages per sheet is not supported.

Copying

- The **Zoom** function depends on MFD's ability to autorotate the original. If this function is restricted or not supported, zooming may not work as expected. Autorotate restriction is configurable in device administration: **Utility** > **Administrator Settings** > **System Settings** > **Restrict User Access** > **Restrict Operation**.
- The **Zoom** function depends on MFD's detection of paper tray's paper sizes. For some devices, you may need to configure the paper sizes in paper trays manually.

Scanning

- Automatic paper size detection depends on the MFD's capabilities. A3 models generally have good detection, but smaller A4 devices do not.
  - The device cannot recognize papers with mixed sizes of mixed formats (AB and inch formats. For example, A3 and Legal sized papers). Therefore, the output will be cropped to the nearest format device is set to
  - If the MFD units are set to inches, it will expect inch-sized originals. Otherwise, it will expect AB-sized originals.
  - You can change the units in device settings > Utility > System Settings > Measurement Unit Settings.
  - Scanning with an open scanner cover may result in the wrong paper size detection.
- When scanning mixed paper sizes, the paper size of the document is set to the largest paper in the tray, and smaller pages have blank spaces.

Accounting

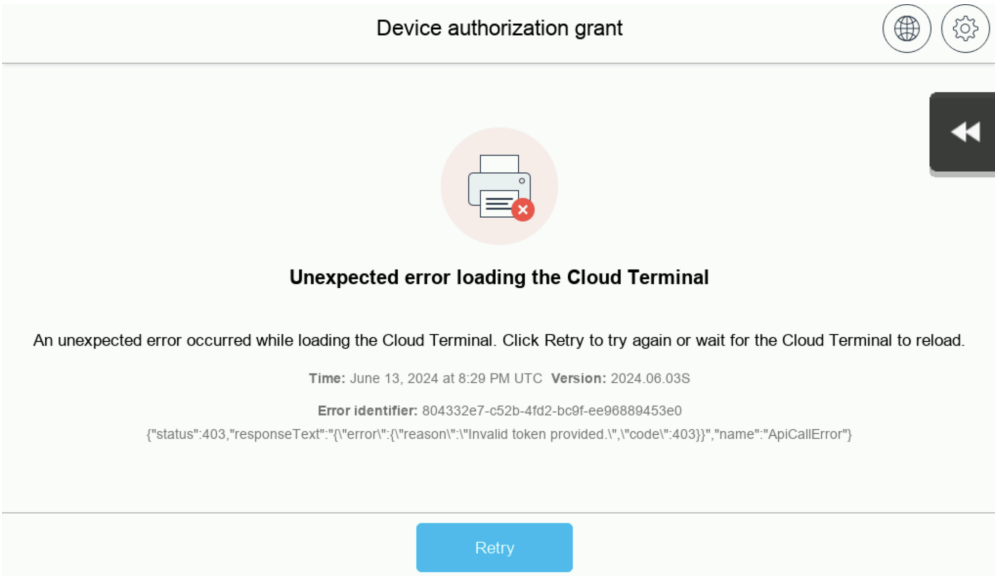
- Accounting is not supported when using Native copy or Advanced (native) scan functionality.

Cloud Terminal registration in SAFEQ Cloud Web UI

If you see "Device has not been registered to SAFEQ Cloud yet" message too often on your MFDs, this will be resolved after the update of SAFEQ Cloud to version 3.45 and the update of the Cloud Terminal to version 2024.06.02. Once you register your MFDs with the Cloud Terminal in SAFEQ Cloud again (see the *Registering the Cloud Terminal in the SAFEQ Cloud Web UI* section of this document), the terminals will be able to automatically re-register themselves in SAFEQ Cloud.

Port switching

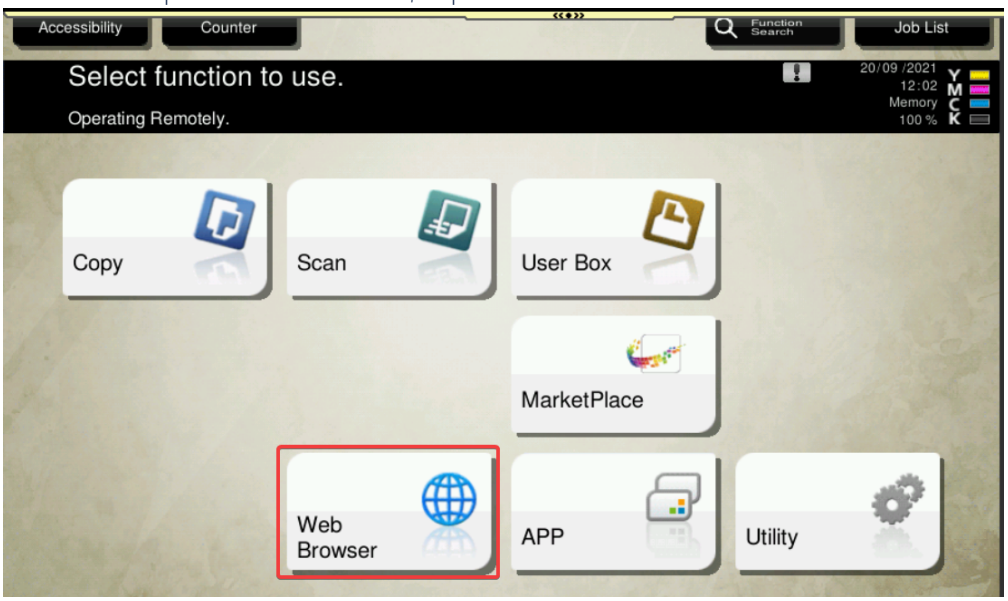
The 2024.06.02 terminal version supports port switching on server port 443. This change has introduced a limitation to the terminal when switching from the SAFEQ Cloud primary server to the SAFEQ Cloud secondary server. In this situation, an error may occur, accompanied by an error message that mentions "invalid token provided" in the details. To resolve this, you must reinstall the terminal.



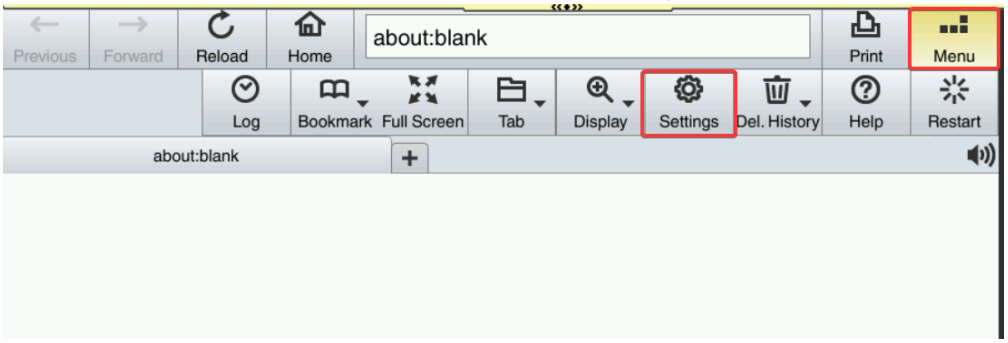
Proxy settings

If your MFD needs to access the public Internet via a dedicated (non-local) gateway, such as a VPN with a proxy server, you must perform the following steps in the MFD settings of the browser.

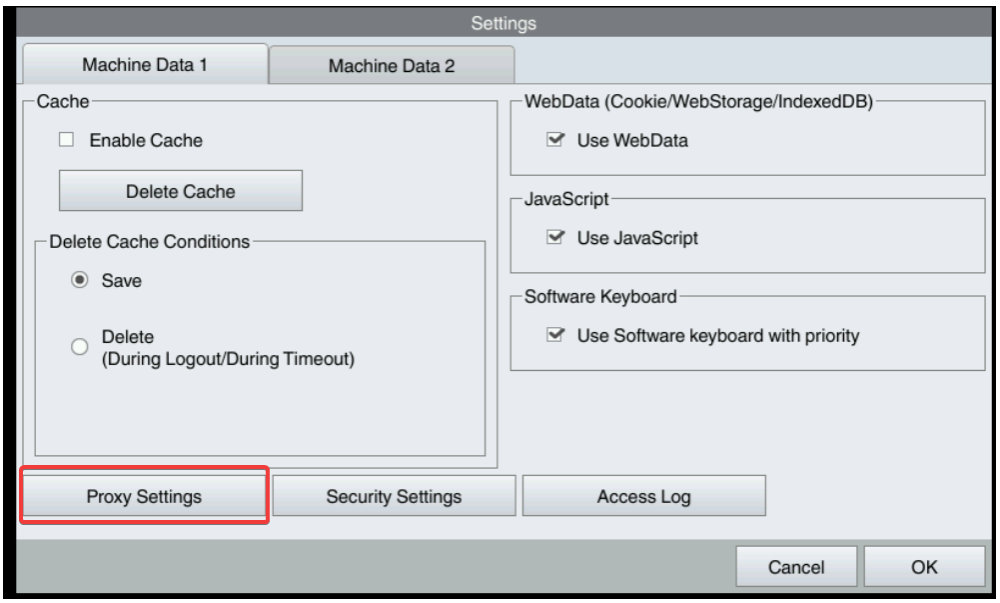
1. On the MFD panel home screen, tap **Web Browser**.



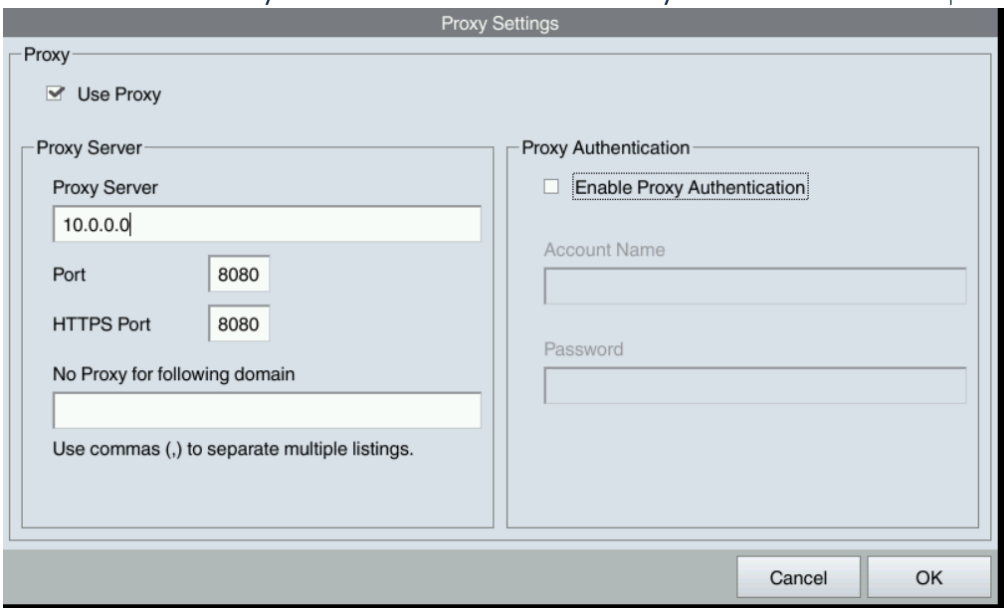
2. In the Web Browser, tap **Menu** and then tap **Settings**.



3. Authenticate with the Administrator password.
4. Tap **Proxy Setting**.



5. Check the Use Proxy checkbox and enter the Proxy Server address and ports.

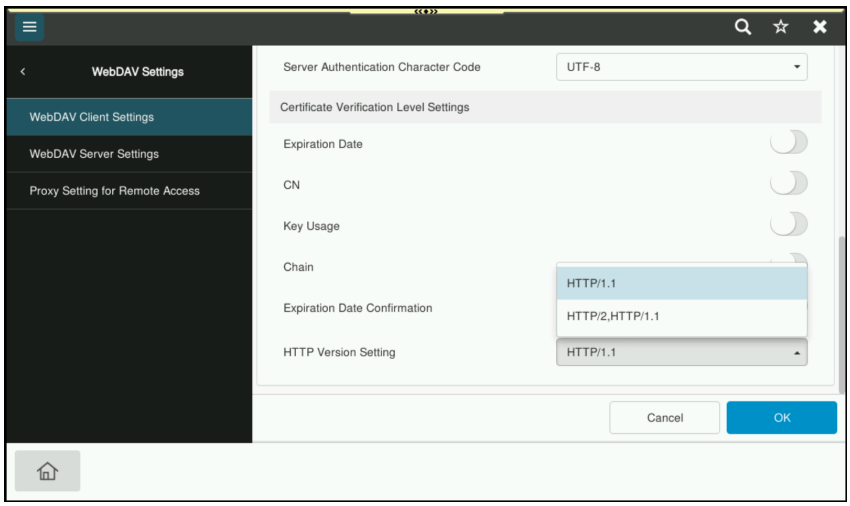


6. If the Proxy server needs authentication, check also Enable Proxy Authentication checkbox and fill Account Name and Password in Proxy Authentication settings.

7. Tap OK to save the proxy settings.

Webdav settings

Select HTTP Version Setting to HTTP/2,HTTP/1.1 to allow scanning on the terminal



Installing the Konica Minolta Cloud Terminal

Install the terminal from Konica Minolta MarketPlace.

The name of the application in MarketPlace is SAFEQ Cloud Secure Print & Scan.

For remote installation, see https://help.konicaminoltamarketplace.com/nib/en/installing/manage-licenses/.

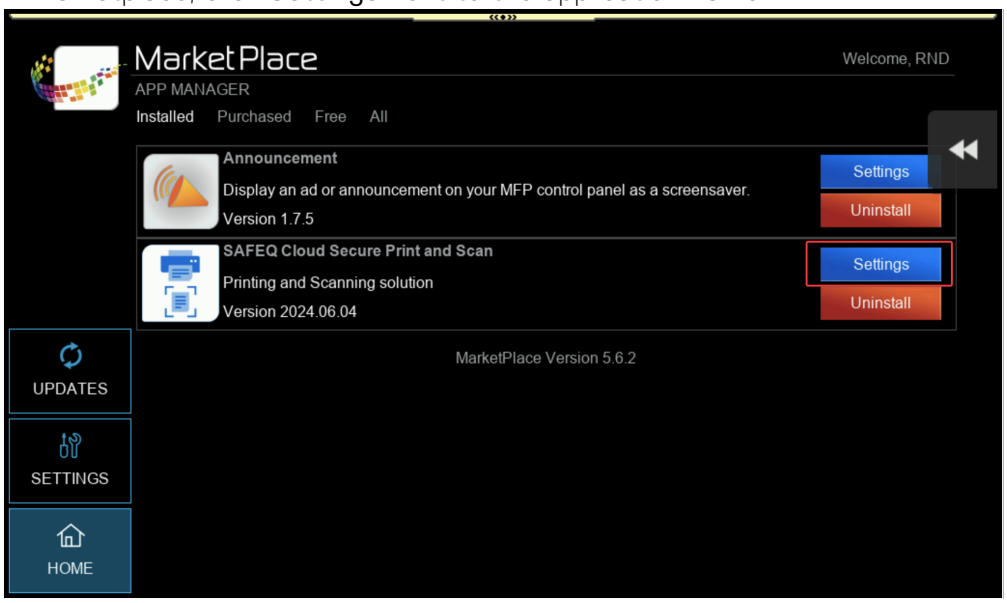
For installation at the MFD, see https://help.konicaminoltamarketplace.com/nib/en/installing/using-at-mfp/.

The Konica Minolta Cloud Terminal supports copying app settings. See https://help.konicaminoltamarketplace.com/nib/en/installing/manage-licenses/#copying-app-settings.

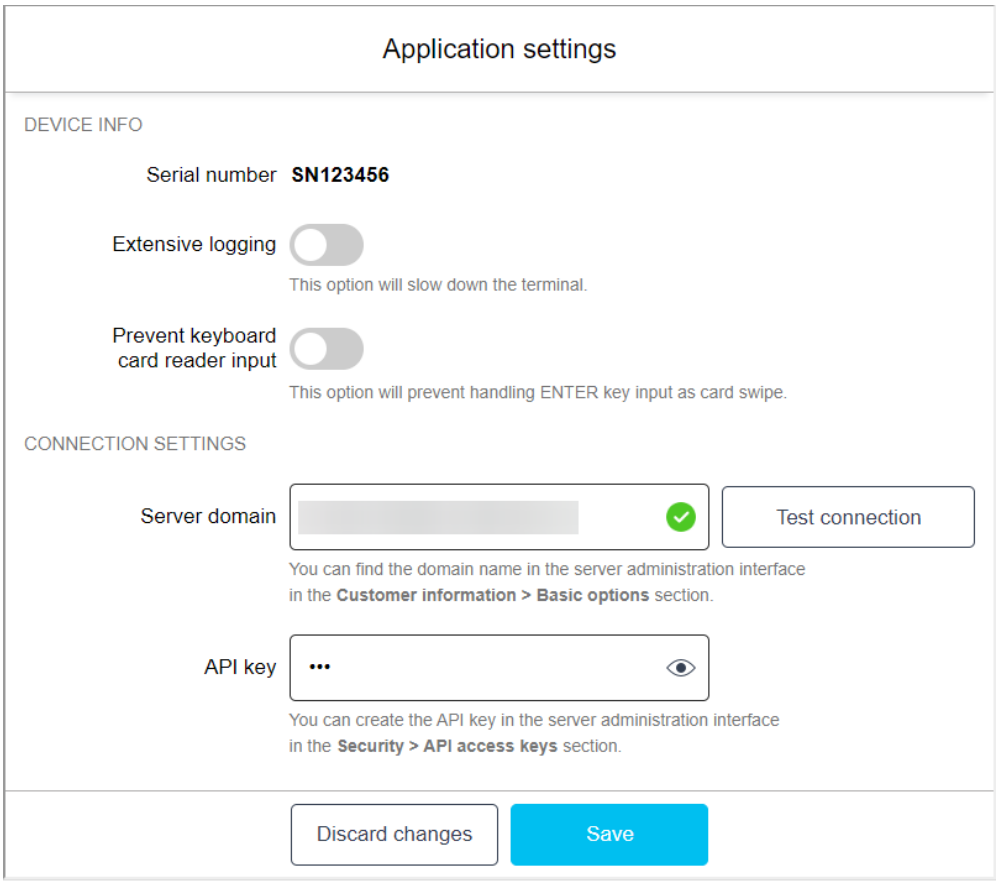
To copy the settings, log in to Marketplace at the MFD or set up periodical sync in the Marketplace app at the MFD. Note that the screensaver on the MFD must be enabled.

Configuring the terminal

1. In Marketplace, click **Settings** next to the application name.



2. On the **Application settings** screen, fill in your domain and your API key.



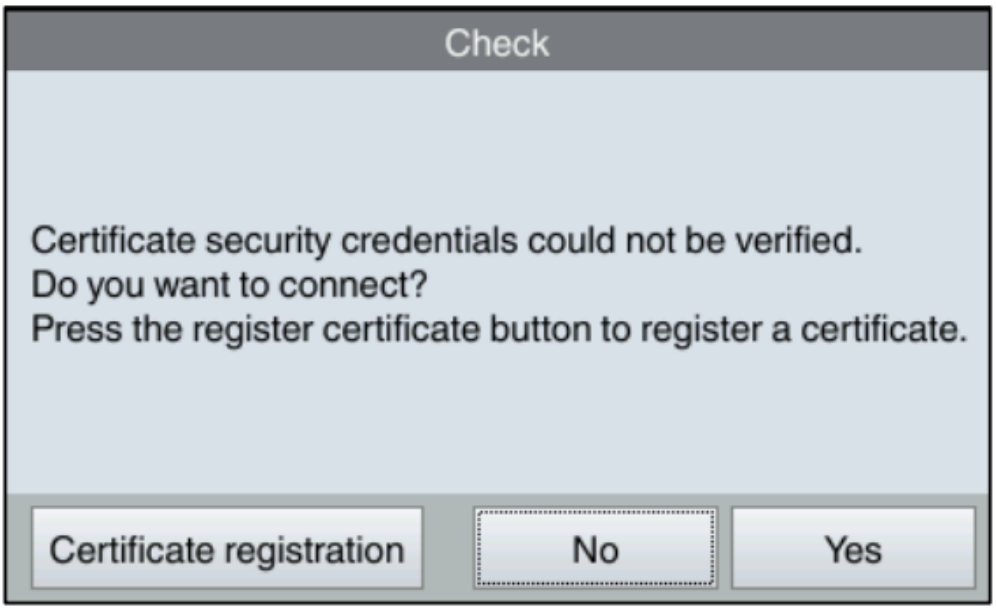
3. You can also enable extensive logging. This option allows outputting all log levels from terminal into a log file. This might be useful for troubleshooting purposes. However, be aware that this option will slow down the terminal.

> You can find the logs here:

- https://<MFD-IP>:8091/IWS/log/script.log
- https://<MFD-IP>:8091/IWS/log/system.log

You will need your machine administrator credentials to access them.

4. When you tap **Test connection** or when you attempt to save the configuration, the following window may appear on older MFDs that do not recognize the Let's Encrypt certification authority. Tap **Certificate Registration** to save the server certificate in the MFD.



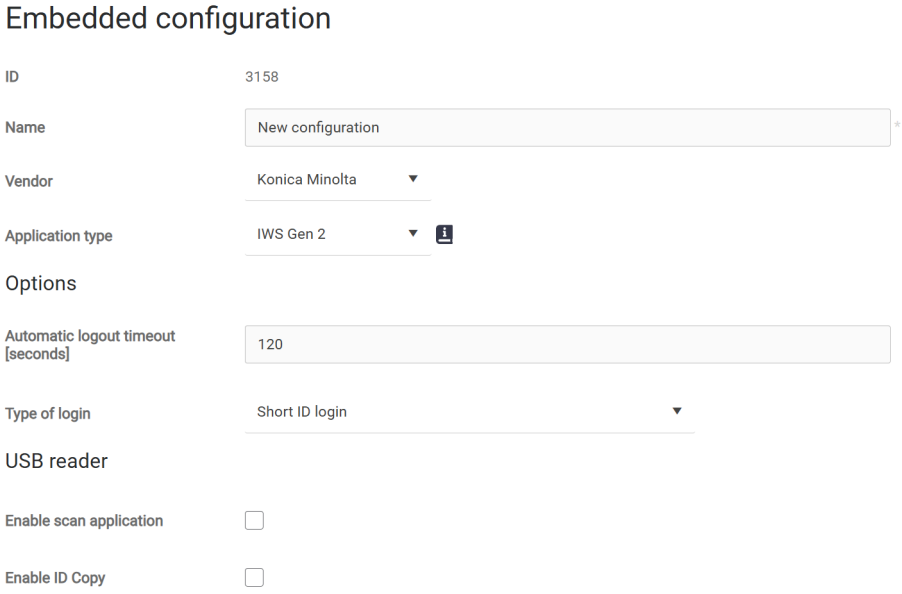
5. Tap **Save** and log out.

Adding Konica Minolta printer and Embedded configuration in SAFEQ Cloud Web UI

These steps are optional and if not performed, the Konica Minolta printer will be added automatically after the endpoint is authorised, see *Registering the Cloud Terminal in the SAFEQ Cloud Web UI* section of this page.

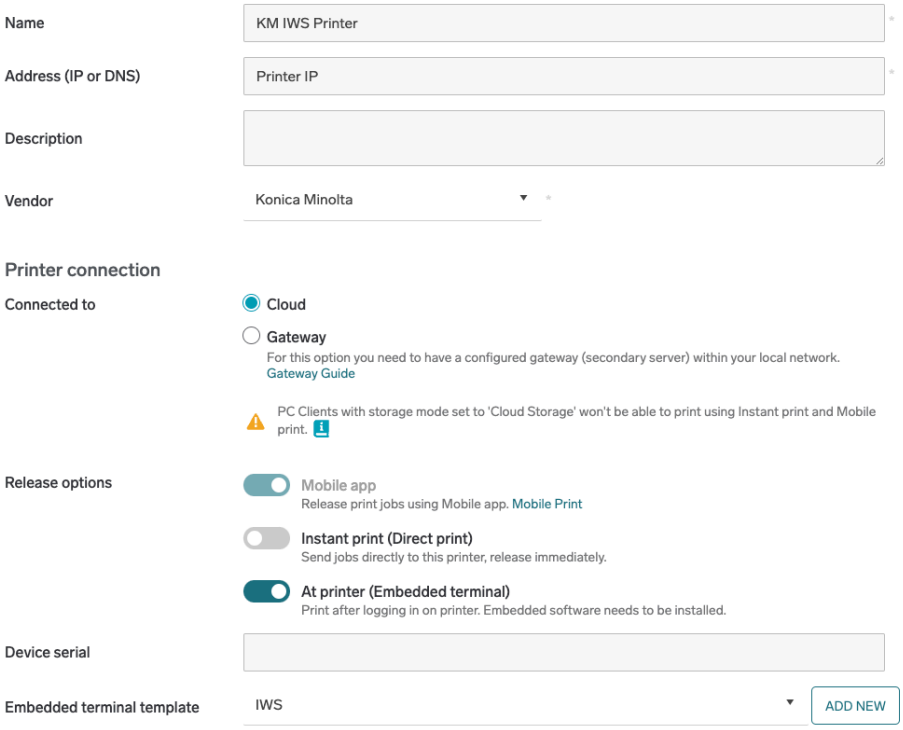
1. Have the MFD's serial number and IP address at hand.
2. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
3. If not done already, create an embedded configuration for Konica Minolta by clicking **Add**.
4. In **Vendor**, select **Konica Minolta** .
5. In **Application Type**, select **IWS Gen 2**.

6. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.



- **Enable ID Copy** adds the ID Copy quick action to **My quick actions** screen on the MFD. This instant action allows users to copy both sides of their ID/IC card and print them out on one sheet of paper.

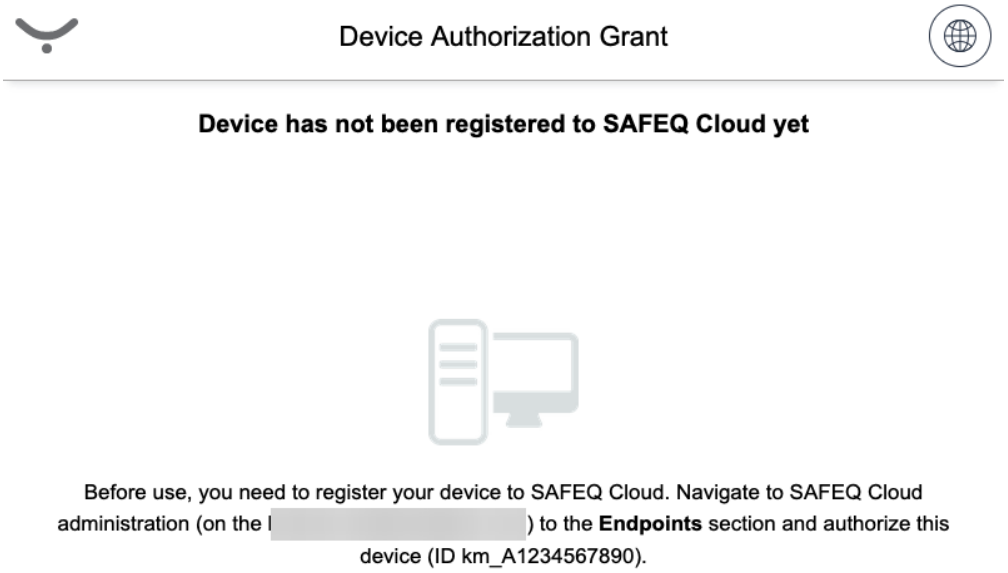
7. Go to **Printers (Output Ports)**.
8. Click **Add**.
9. In **Vendor**, select **Konica Minolta**.



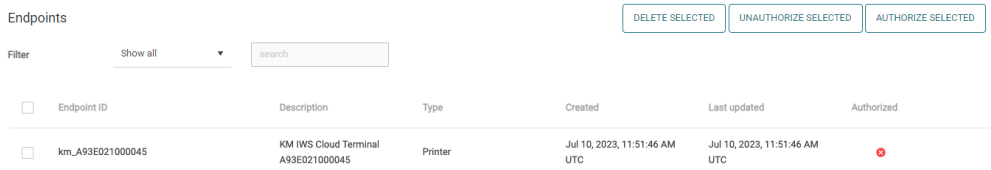
10. In **Device serial**, enter the serial number.
11. Fill in the rest of the required information according to your needs.
12. In **Embedded configuration**, select your Konica Minolta embedded configuration from the list.
13. Click **Save**.
14. The MFD will now display a login screen with your chosen authentication type. If not, tap **Reload**.

Registering the Cloud Terminal in the SAFEQ Cloud Web UI

1. After the terminal installation and configuration, you will see the following screen. Note down the endpoint ID.

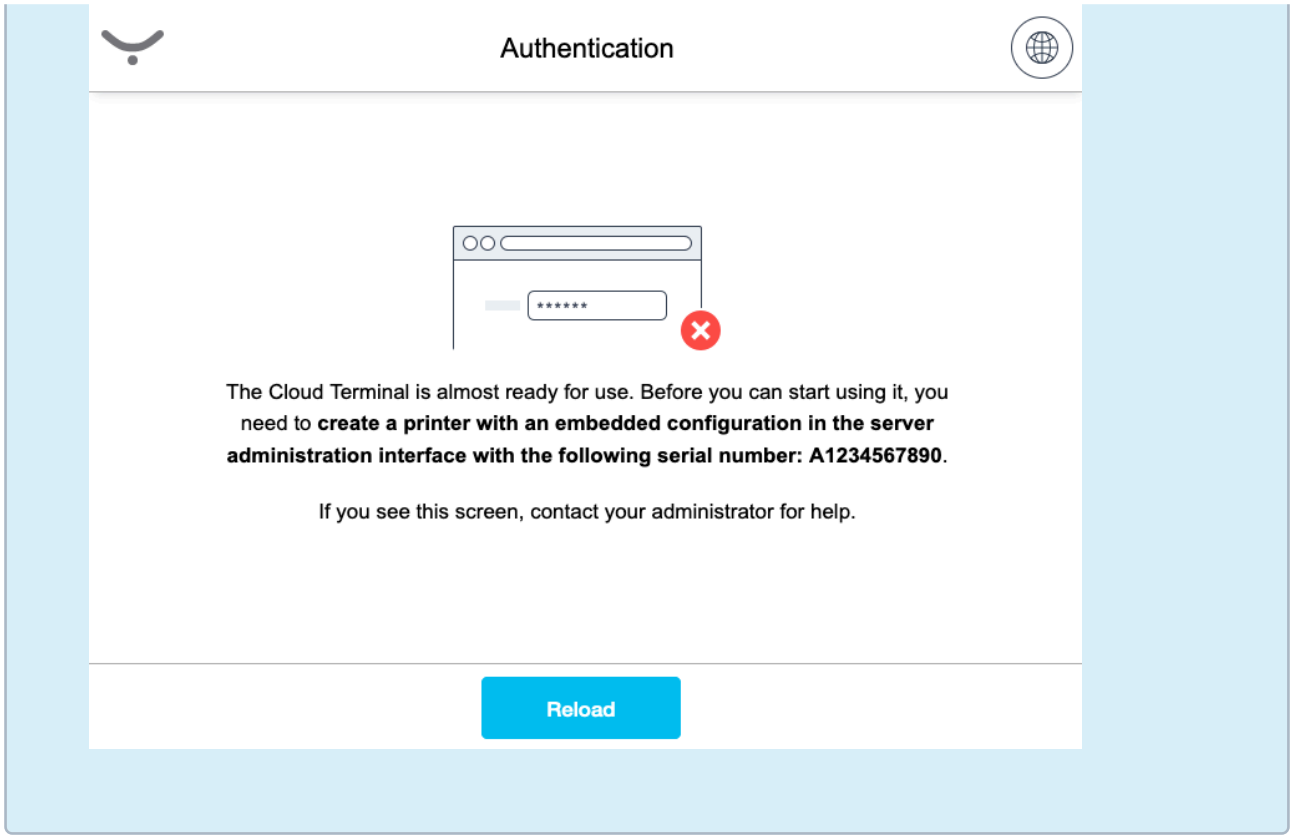


2. In SAFEQ Cloud web UI, go to **Security** > **Endpoints** and find the entry that contains the endpoint ID from the previous step.



3. Select the entry and click **Authorize selected**.

If you see the following screen on the MFD, it means that you haven't added the MFD in SAFEQ Cloud Web UI. See section *Adding Konica Minolta printer and Embedded configuration in SAFEQ Cloud Web UI* of this page.



Konica Minolta IWS Cloud Terminal

Contents

- Hardware requirements and prerequisites
- Konica Minolta printer setup
- SAFEQ Cloud Configuration for IWS
- How to install using the IWS Install Tool
- KM IWS Application overview

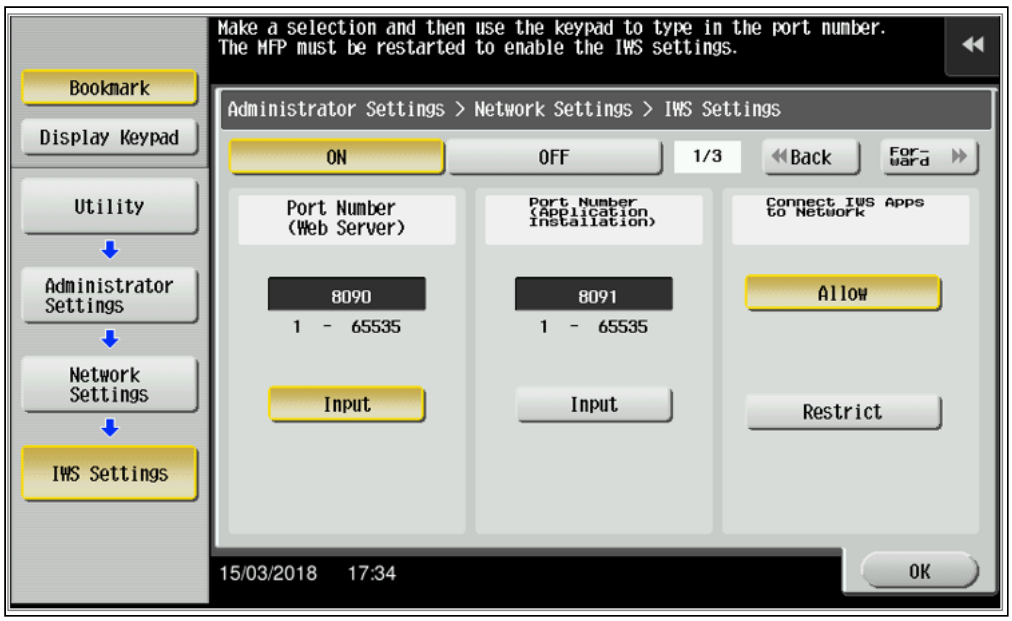
KM printer hardware requirements

- 5th generation or higher for the printer
- Extended memory module
- Chromium browser
- Function version 4.2 or higher
- IWS version 2.5.6 or higher

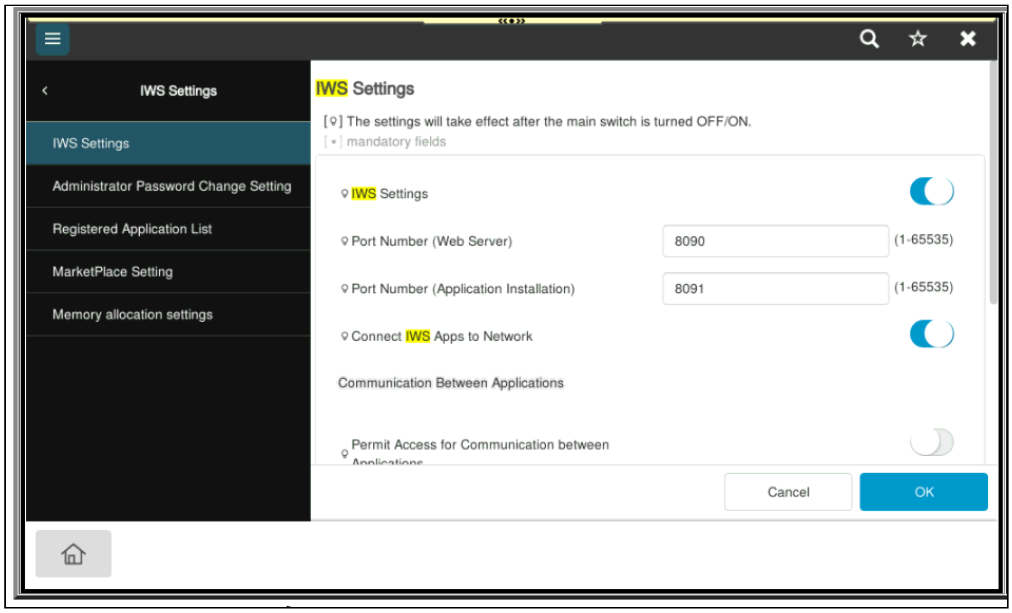
Prerequisites

- Ports 7301 and 9444 are open. See Ports and Protocols for more information.
- You have configured your secondary gateway. See Secondary Gateway mapping.

KM printer setup
1. The IWS setting must be turned ON:
Utility → Administrator Settings → Network Settings → IWS Settings → ON

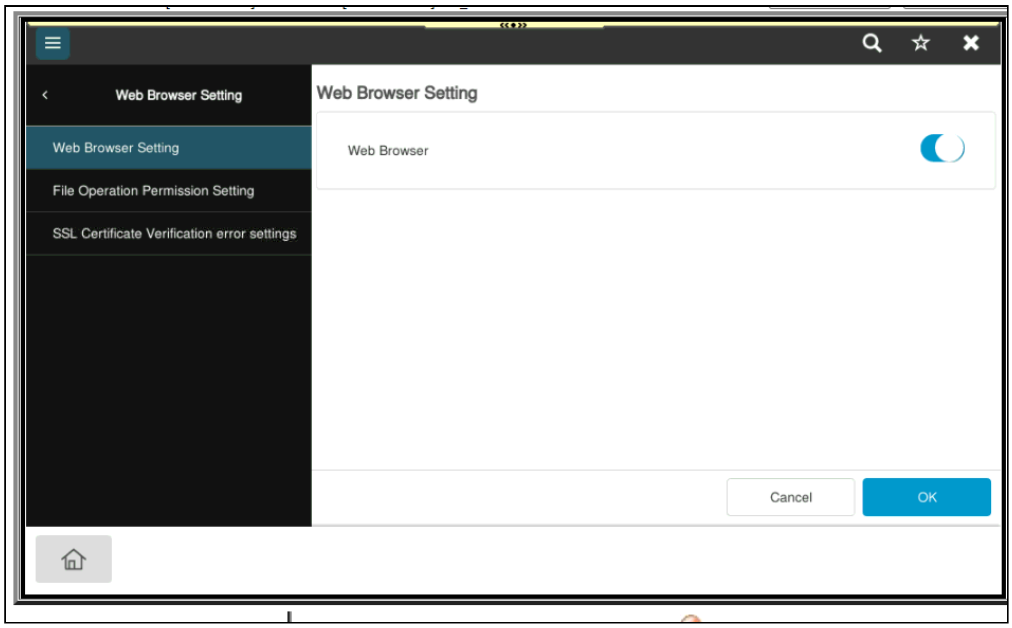


This is the screen for the newer models:

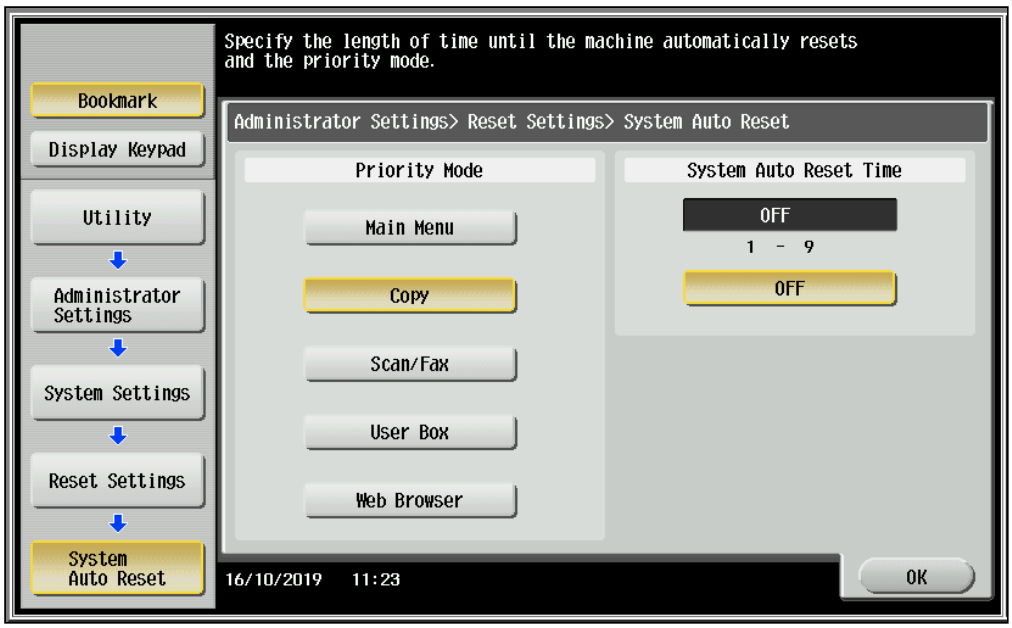


2. The Web browser must be turned ON:
Utility → Administrator Settings → Network Settings → Web Browser Setting → Web Browser Usage Settings → ON

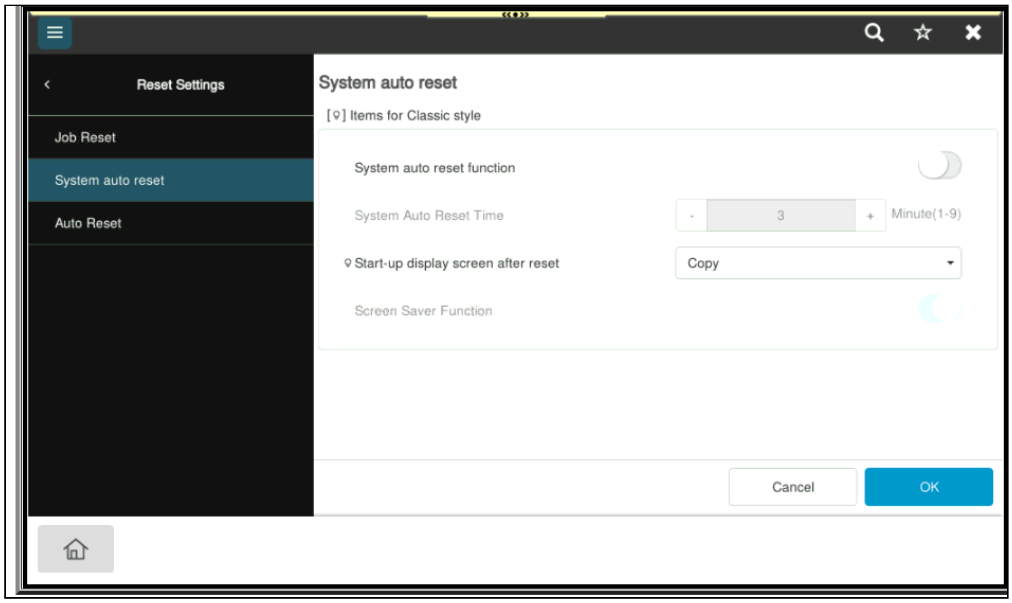
This is the screen for the newer models:



3. Disable System Auto Reset:
Utility → Administrator Settings → System Settings → Reset Settings → System Auto Reset → OFF



This is the screen for the newer models:



4. The Slider Menu should be turned OFF:
Utility → Administrator Settings → System Settings → Custom Display Settings → Slider Menu Settings

Next steps SAFEQ Cloud Configuration for IWS

IWS Cloud Terminal Configuration

Contents

- Required services
- Creating a printer for IWS
- Creating an Embedded configuration for IWS
- Certificates

- API Access keys

Prerequisites

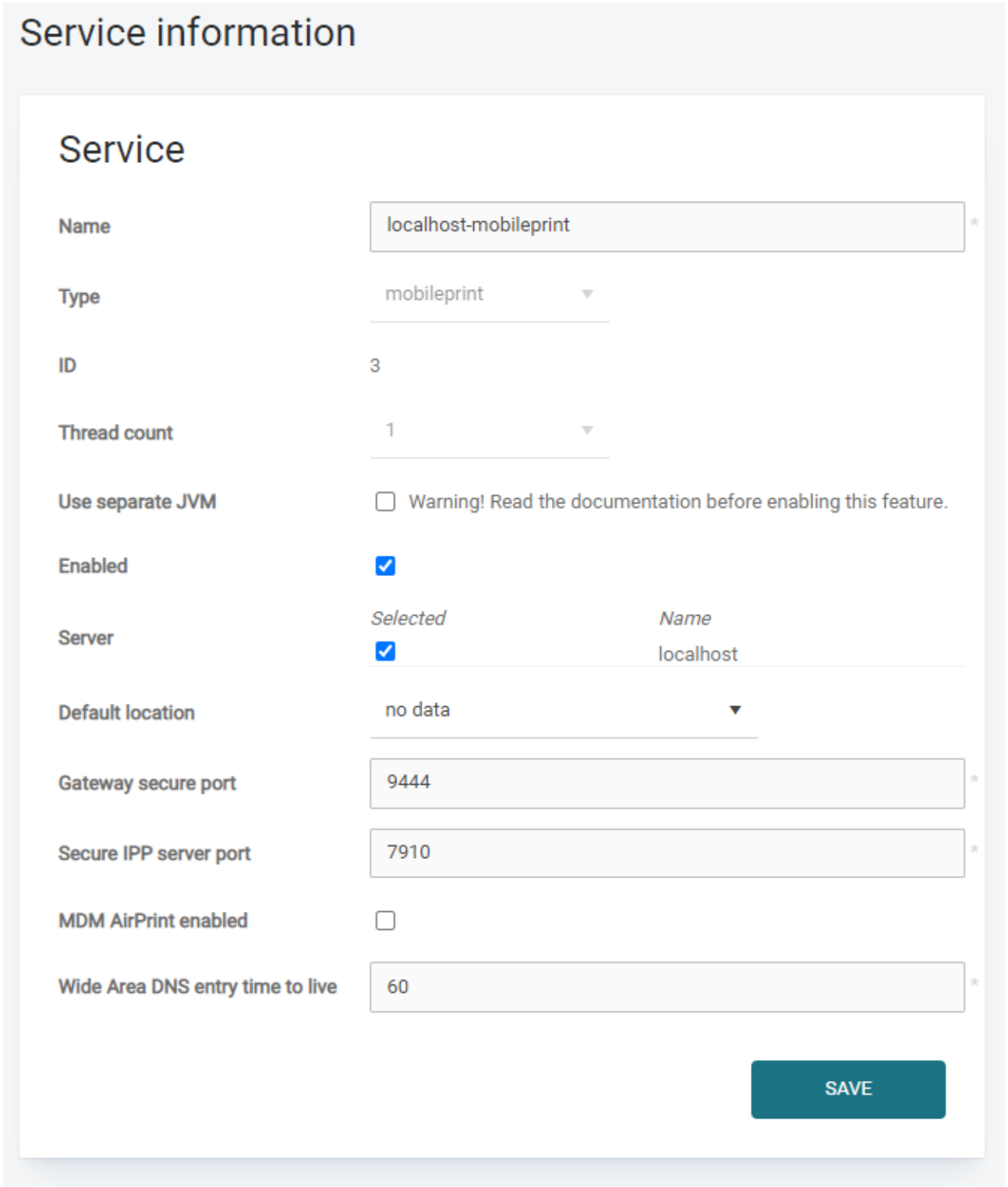
- Konica Minolta IWS Cloud Terminal has to be completed beforehand

1. Open SAFEQ Cloud Web UI `https://<domain_name>:8443`

2. Enter the required credentials in order to login into SAFEQ Cloud.

3. Make sure that you have the following services under the server:

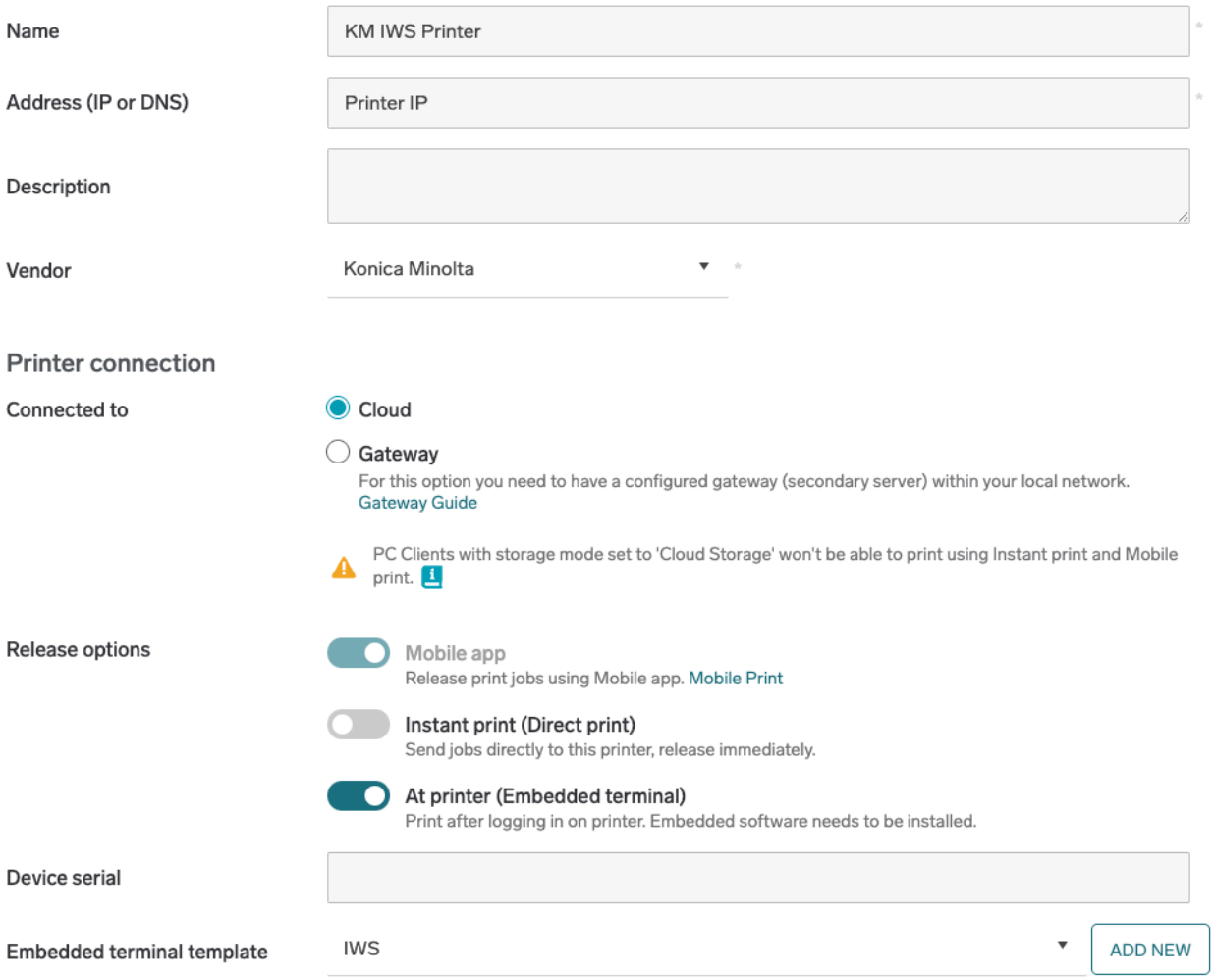
- terminal client
- document output
- messaging
- mobile – The mobile service should have the below ports set correctly:



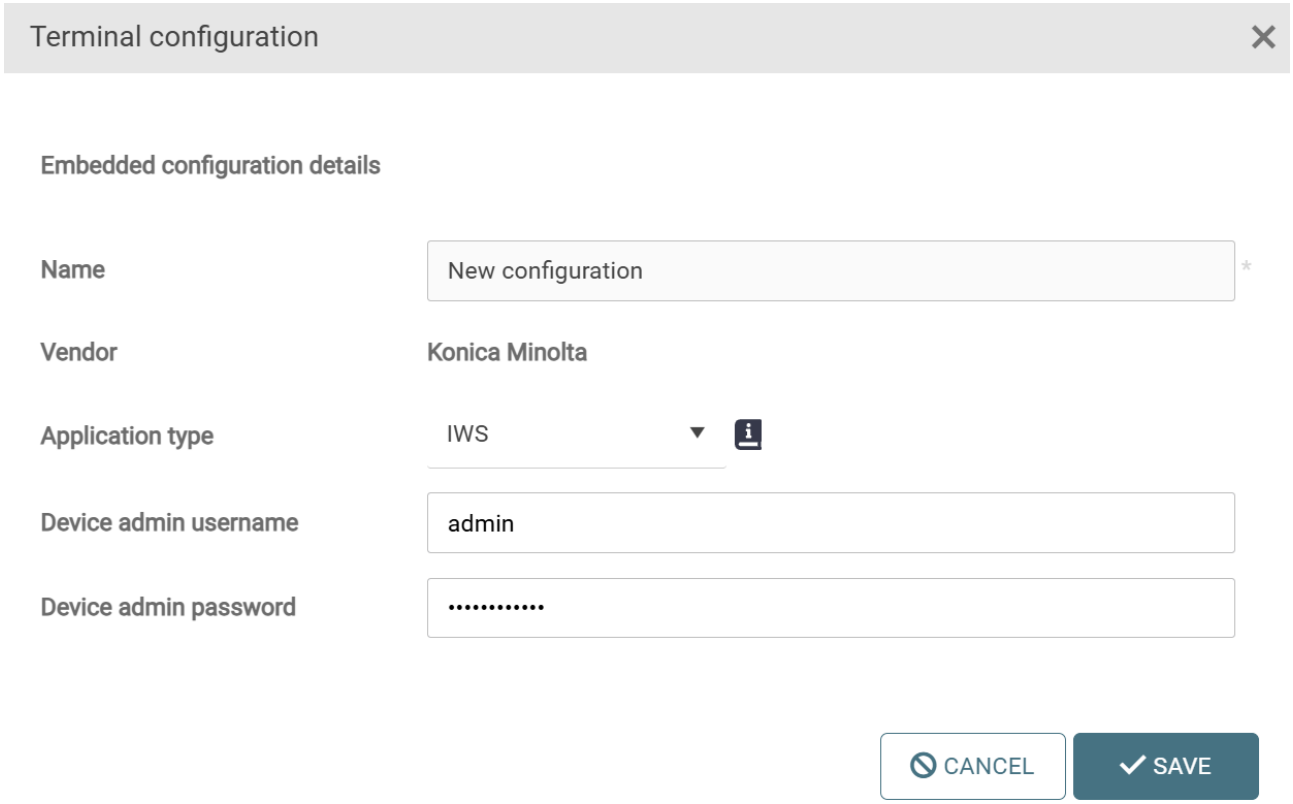
The login should not be enabled since this is handled by the SAFEQ Cloud server.

For Y Soft hosted Accounts the Primary services are already configured accordingly and ready to be used.

4. Create the Konica Minolta printer under the customer and add information in the fields:

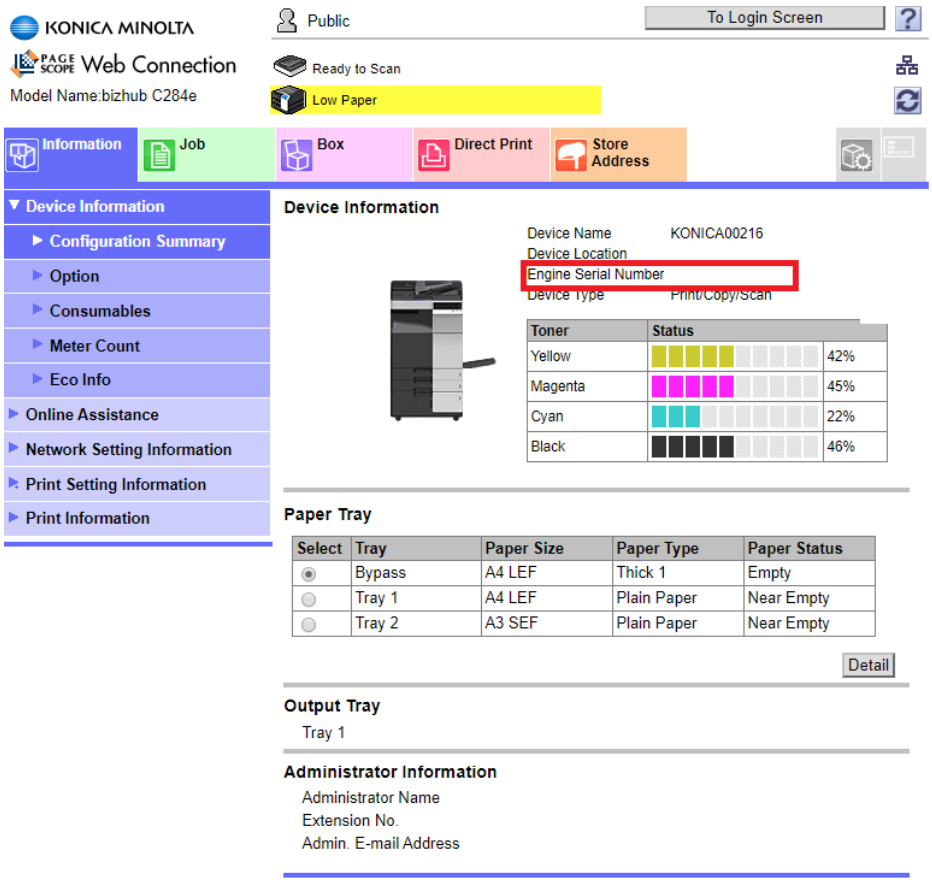


4.1. An *Embedded Configuration* needs to be created by clicking ADD:



The Embedded Configuration will be later edited (step 6.) in this documentation.

4.2. Device serial number from the printer can be retrieved from here:
Device Information → Configuration Summary → Engine Serial Number



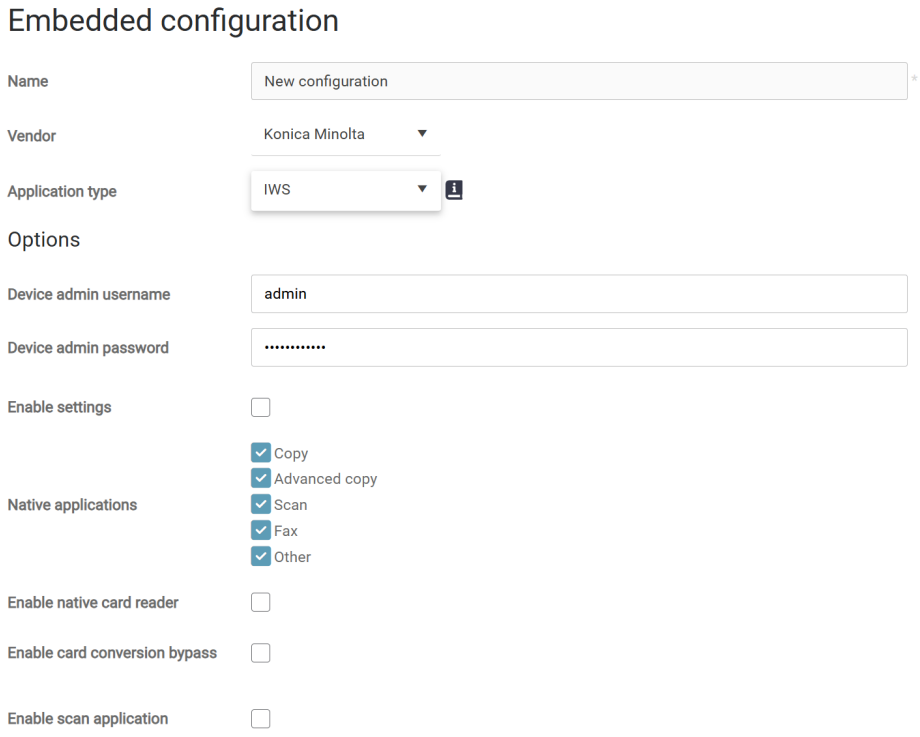
5. In the tree, go to **Settings > General settings > Messaging** and add a SMTP configuration. Fill in all the required details.

6. Edit the *Embedded configuration* created previously under the customer. In addition to the mandatory fields (Name, Vendor, valid device admin username and password), fill in:

- For *Application Type* select IWS
- Uncheck *Enable settings*
- Check *Enable Scan Application*
- Select the *SMTP Configuration*
- Select the printer in *Mapped Devices* (should be already selected from step 4.1.)

If *Enable settings* is checked, then the user will have the possibility to change the settings for the IWS application.
If it remains unchecked, then the user will not be able to modify the settings within the App. In this case only an Administrator that has access to the Marketplace will be able to configure the settings.

The native applications (Advanced Copy, Scan, Fax, Other Installed Applications) can be enabled/disabled from the embedded configuration.



7. Add one *Input Port* under the customer. Select Port Type as Pull Queue for it.

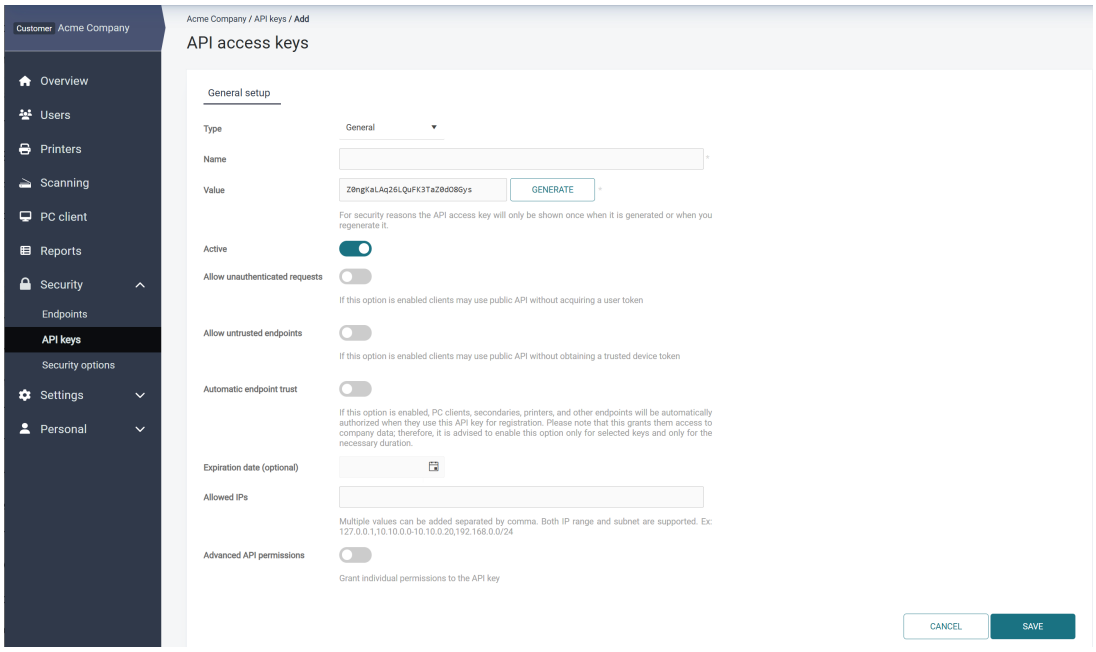
8. Adding a *Certificate* for IWS:

- For Accounts that are hosted in the Y Soft Cloud (EU, US, UK, AP), there is no need to create a new certificate for IWS.
- For on-premises Accounts that have a Self-Signed Certificate, it is required to have a Certificate under "Private Certificate chains":
  - Click Create
  - Select from the drop-down the Account domain name
  - Click Generate
  - In the Application settings (described at step 6.) uncheck "Verify SSL". Verifying the SSL connection here means that the IWS application will validate the server certificate. This will only be possible when connecting the IWS app to the Y Soft Cloud servers (as stated above) and using their deployed certificates. When using a self-signed certificate for an on-prem installation, or when deploying your own ca certificate in the cloud the IWS application is not able to verify the validity of the server certificate and so this checkbox should be unchecked in this case.

Imported Self-Signed Certificates will not work in this case.

9. In the **Settings > General settings >** ***Mobile Print*** section under the account, select from the drop-down the mobile service and make sure that "Enable MDM Single Sign On" is unchecked.

10. Add an *API access key*.



Allow untrusted endpoints must be checked and the other checkboxes must be unchecked for the key to work properly.

The default API access key can be used, however the same set up as in the above image must be made for it.

Other options availble on the embedded page:

- *Enable native card reader* – the native/non-native setting will only determine how the card is read/handled on the device side: "native" means that the full card number length is used, "non-native" means that the card number is truncated.
- *Enable card conversion bypass* – IWS applies a conversion of the card number passed from the Loadable Device Driver. When opted out of the conversion, the card number stored in SAFEQ Cloud should be the raw card number passed by the Loadable Device Driver to IWS.

Installation from the Marketplace

Prerequisites

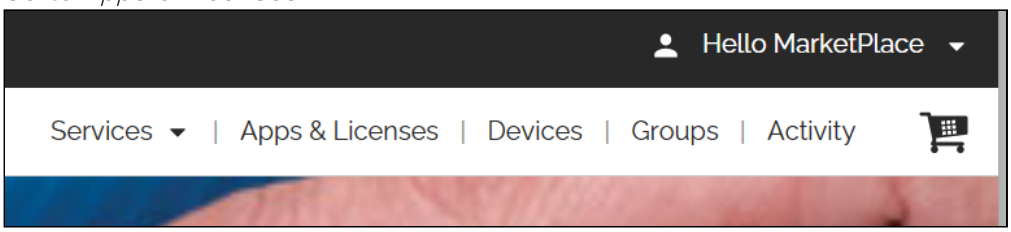
- Section IWS Cloud Terminal Configuration needs to be completed before this section

For this step, you would require to have a KM Marketplace valid account and have the Marketplace application installed on the printer.

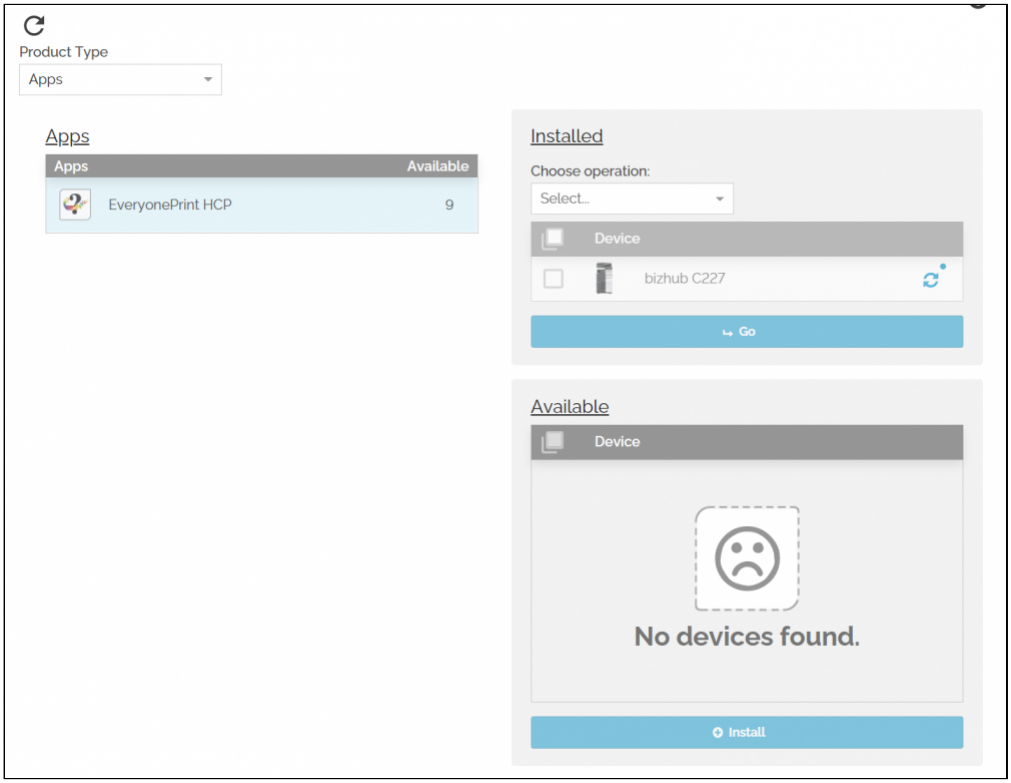
In case the “Enable settings” flag is disabled in the embedded configuration in SAFEQ Cloud the settings can be changed only from the Marketplace.

Install

1. Login on the *KM Marketplace* portal.
2. Go to *Apps & Licenses.*



3. Select the *Y Soft* application from the list.

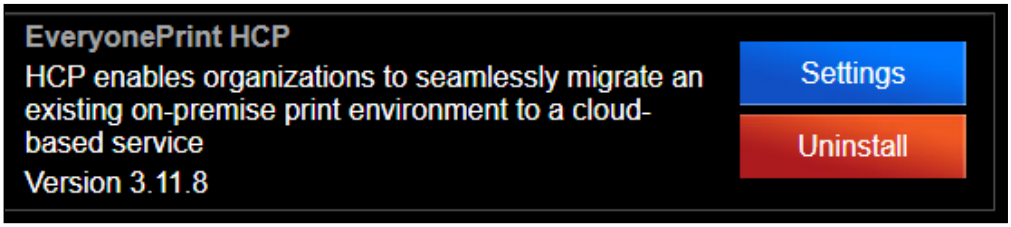


4. In the *Available* section, select the printers where the application should be installed and click *Install*.
5. After the operation is finished the application can be accessed on the printer via the Marketplace.

The application can also be installed from the printer using the KM Marketplace application. On the home page go to *All* tab and select the Y Soft application.

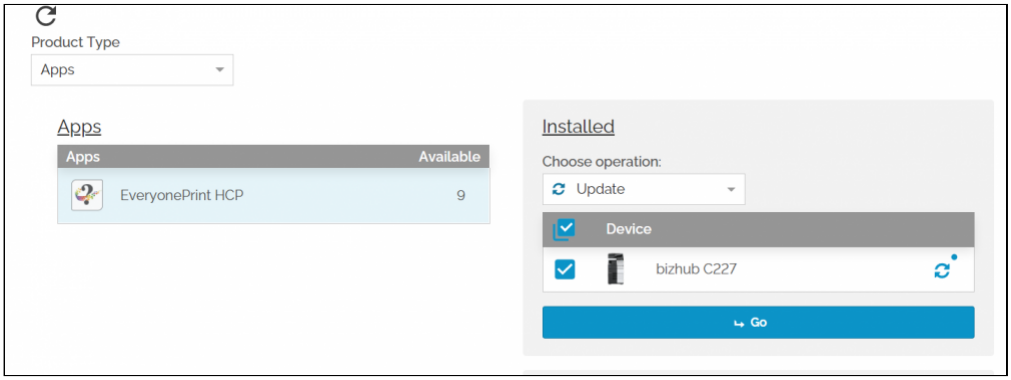
Configure the application using the Marketplace on the printer

1. Go to the printer and open the Marketplace application.
2. Click on *App Manager* and login using your KM Marketplace credentials.
3. Click on *Settings* on the Y Soft application.
4. Edit the fields and click *Save* (more info available in section IWS Cloud Terminal usage point 2).



Update

1. Login on KM Marketplace portal.
2. Go to *Apps & Licenses.*
3. Select the *Y Soft* application from the list.
4. From Chose operation select *Update.*
5. Select the desired printers and click on *Go.*



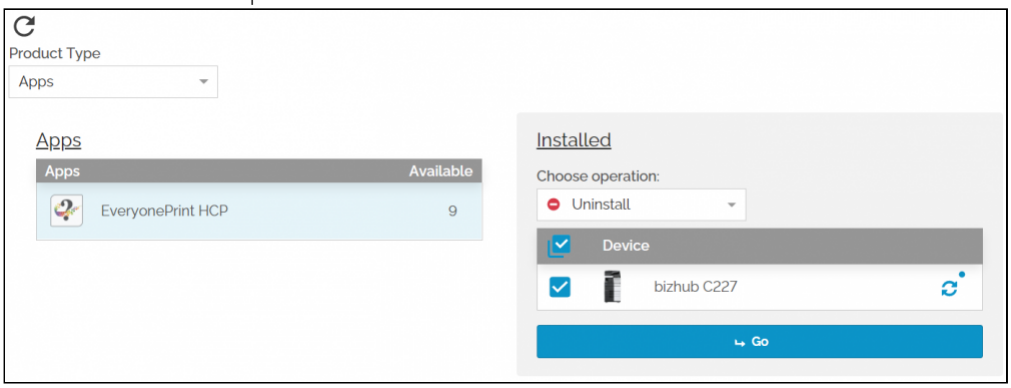
The application can also be updated from the printer using the KM Marketplace application

Uninstall

1. Login on KM Marketplace portal.
2. Go to *Apps & Licenses.*
3. Select the *Y Soft* application from the list.

4. From Chose operation select *Uninstall.*

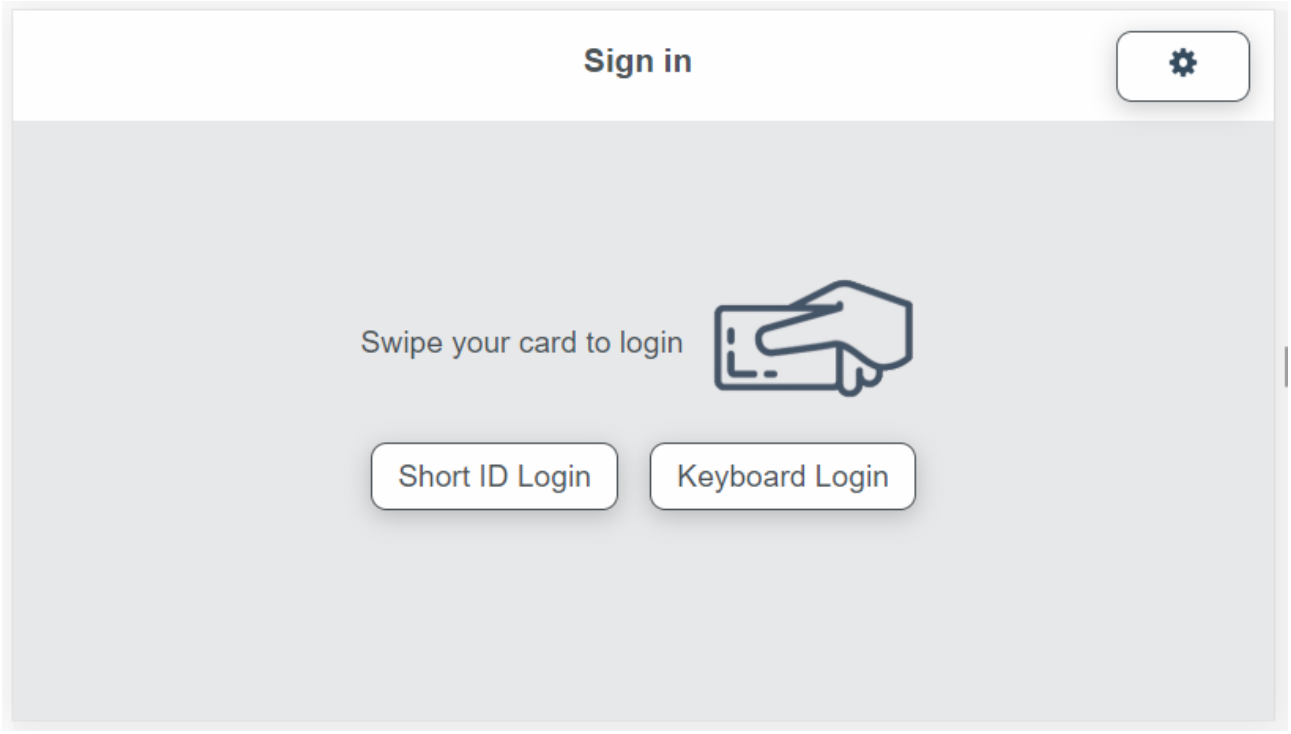
5. Select the desired printers and click on *Go.*



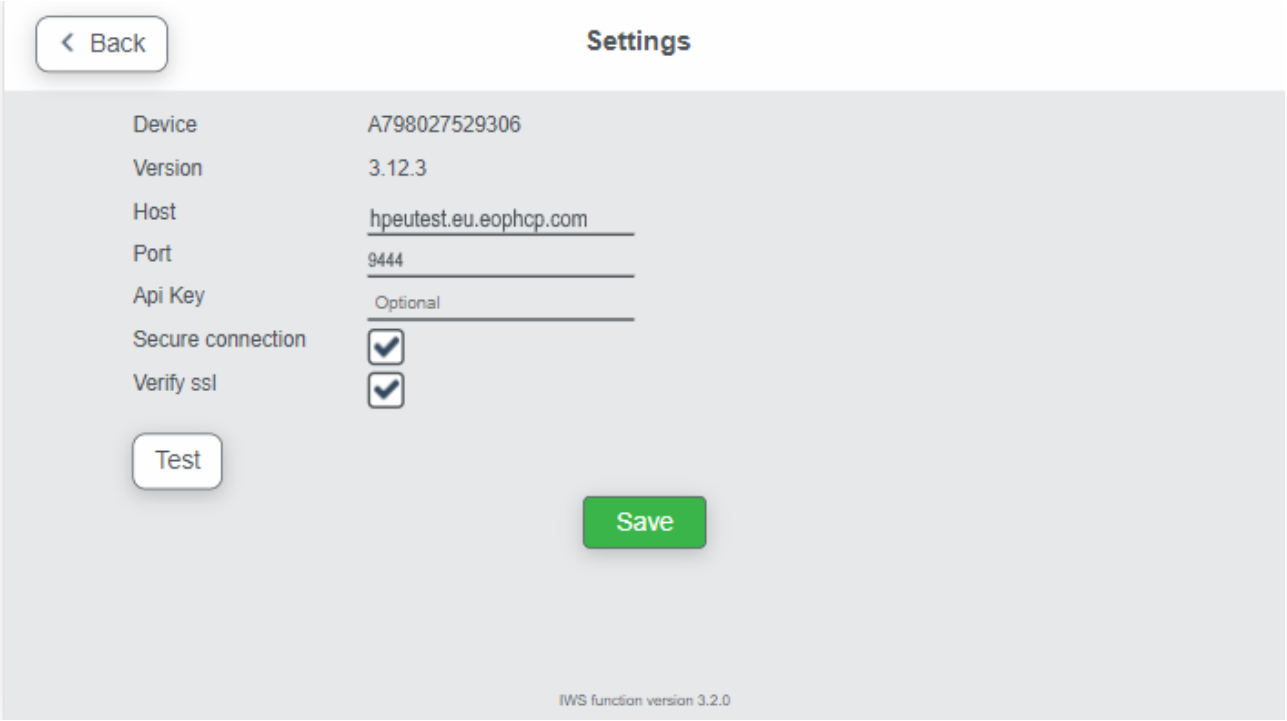
IWS Cloud Terminal usage

KM IWS application

1. Login page:



2. Go to the Settings page by clicking the top-right icon to set the SAFEQ Cloud connection parameters:



Host
Domain name of the account to which the applications will be connecting.

Port
The secure (SSL) server port for the mobile service. The default value is 9444.

> In case no API Key is provided the default server key will be used.

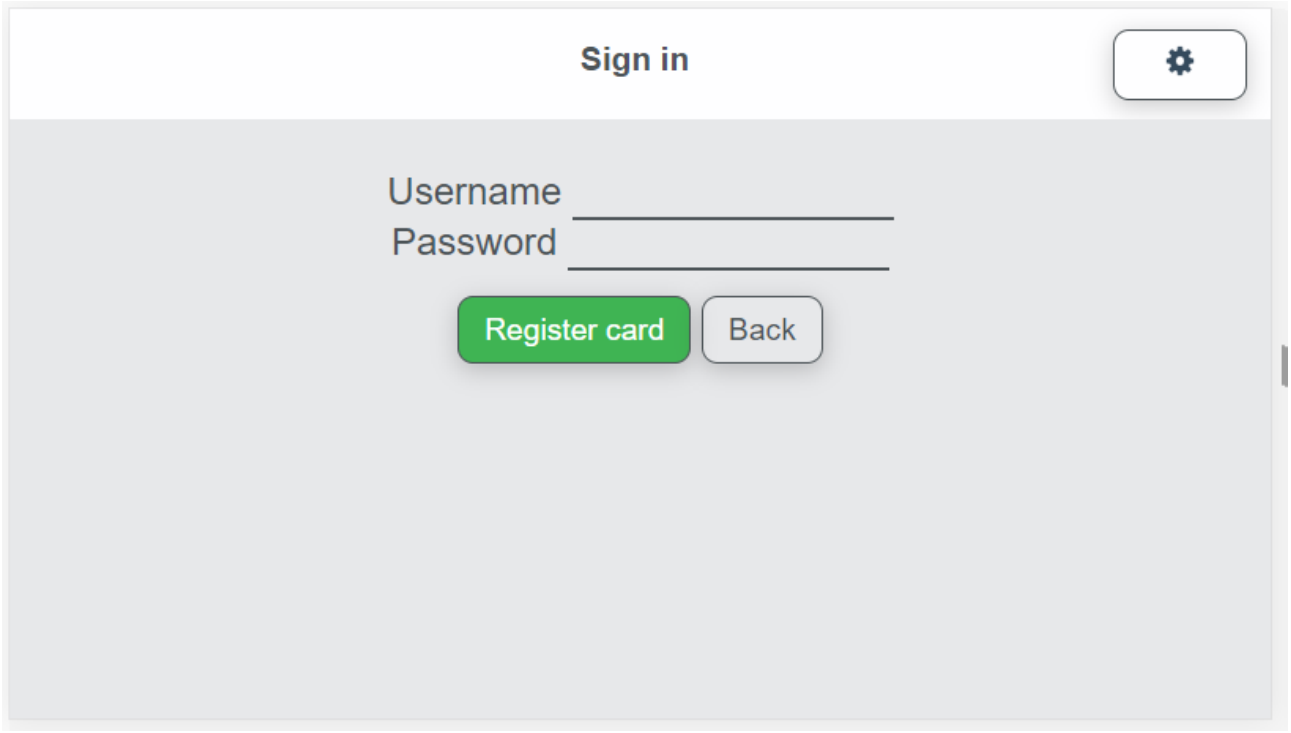
3. Click Test to test the connection

4. Click Save to save the settings

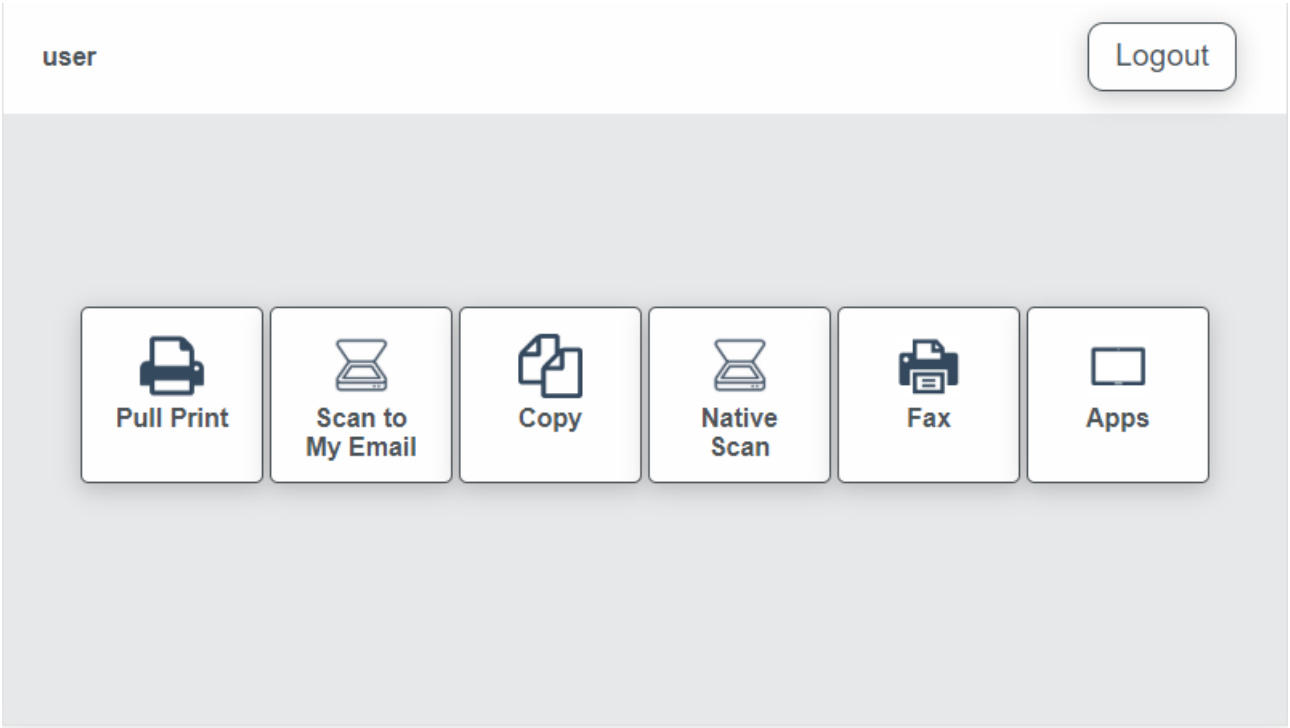
5. Users can login to the application using the following methods

- Short ID login
- Username and Password login
- Swipe card login

6. When the user will swipe their card for the first-time, the application will ask for card registration. Register the Card using Username & Password.



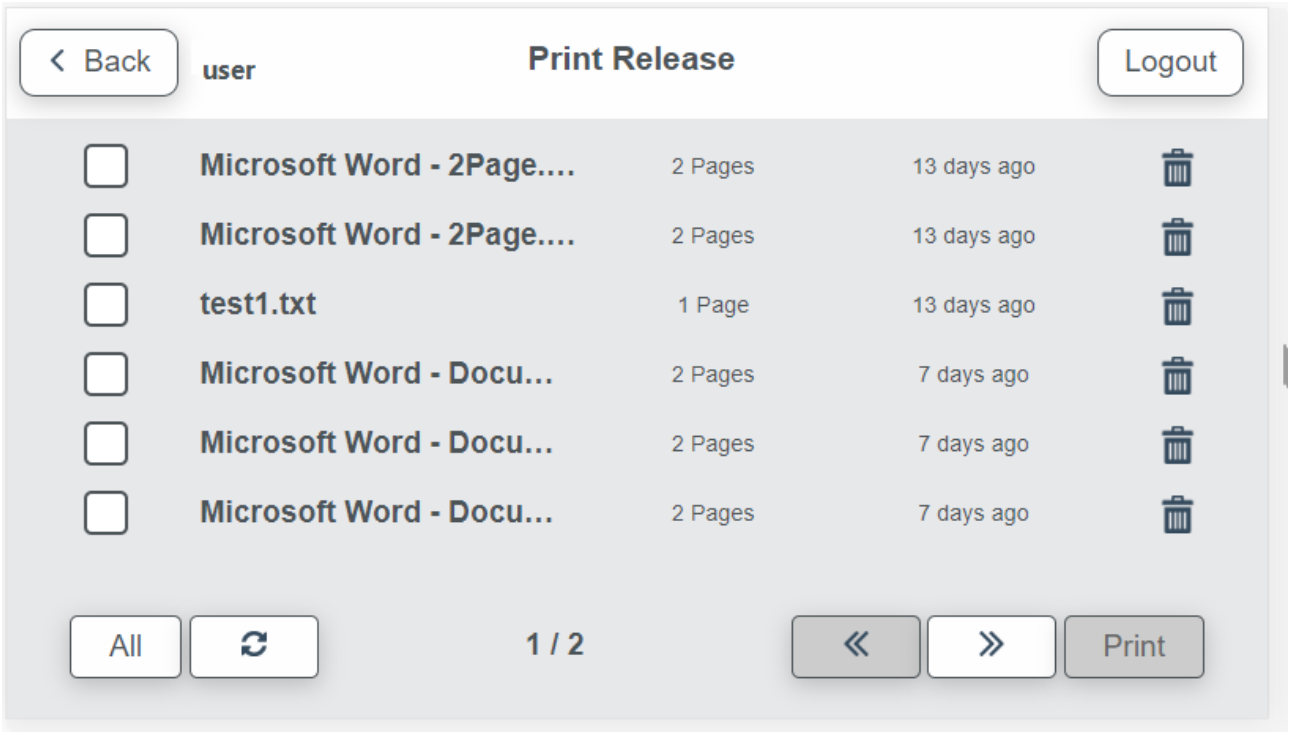
7. Menu page



8. Pull Print

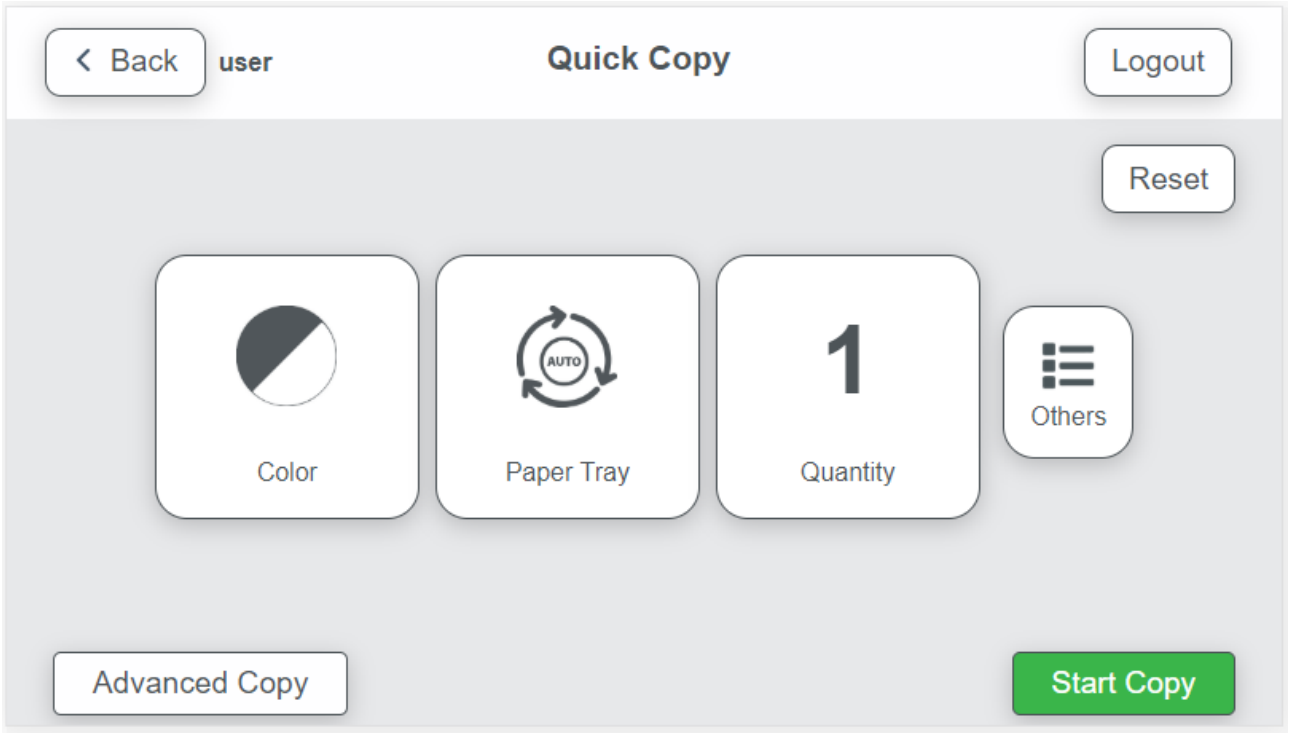
- All – select all jobs from all pages
- Refresh – refresh job list
- Navigation – navigate through the job list pages
- Print – print selected jobs

- Delete – delete the job



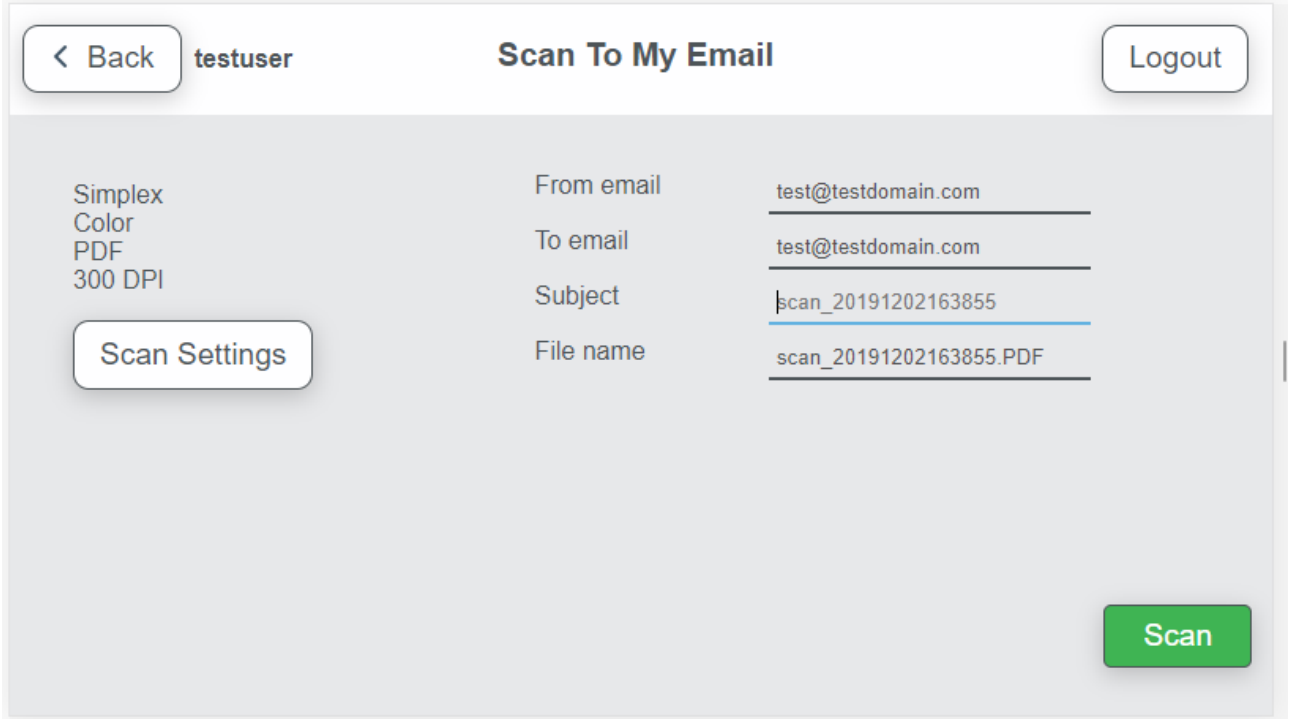
9. Copy

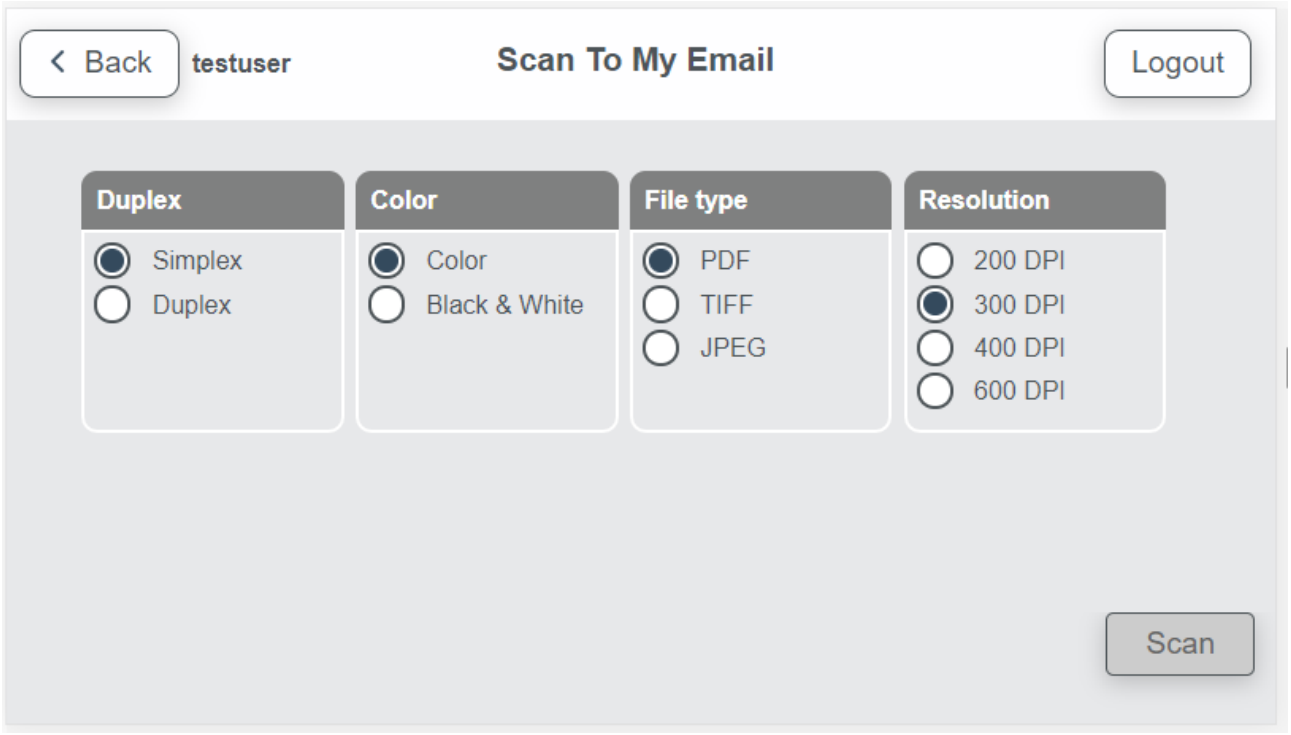
- Color – set color option
- Paper Tray – set paper tray
- Copies – set number of copies
- Other – set other options
- Copy – start to copy
- Advanced Copy – start printer native copy



10. Scan to My Email

- Start Scan – will begin the scan process
- Scan Settings – the user can select settings for the scan operation





11. Native Scan

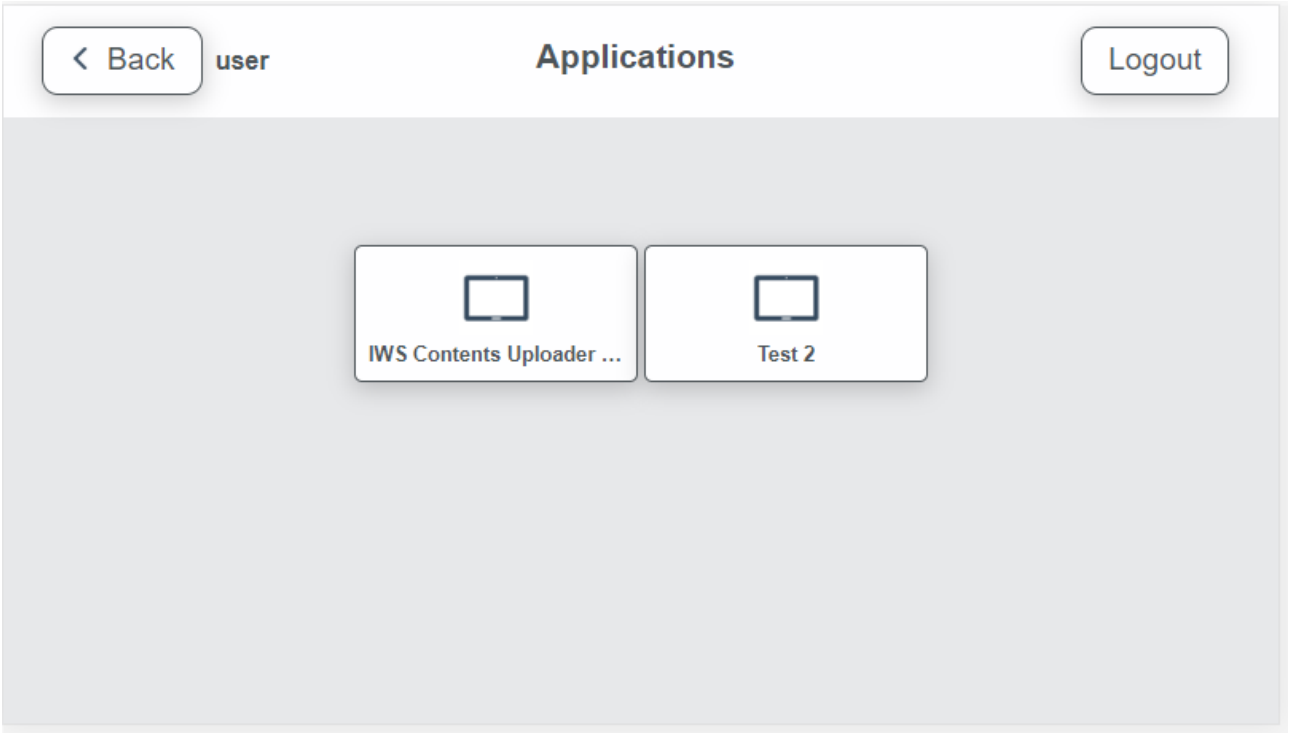
- The native scan screen of the printer

12. Native Fax

- The native fax screen of the printer

13. Other installed applications

- List with all installed applications on the printer



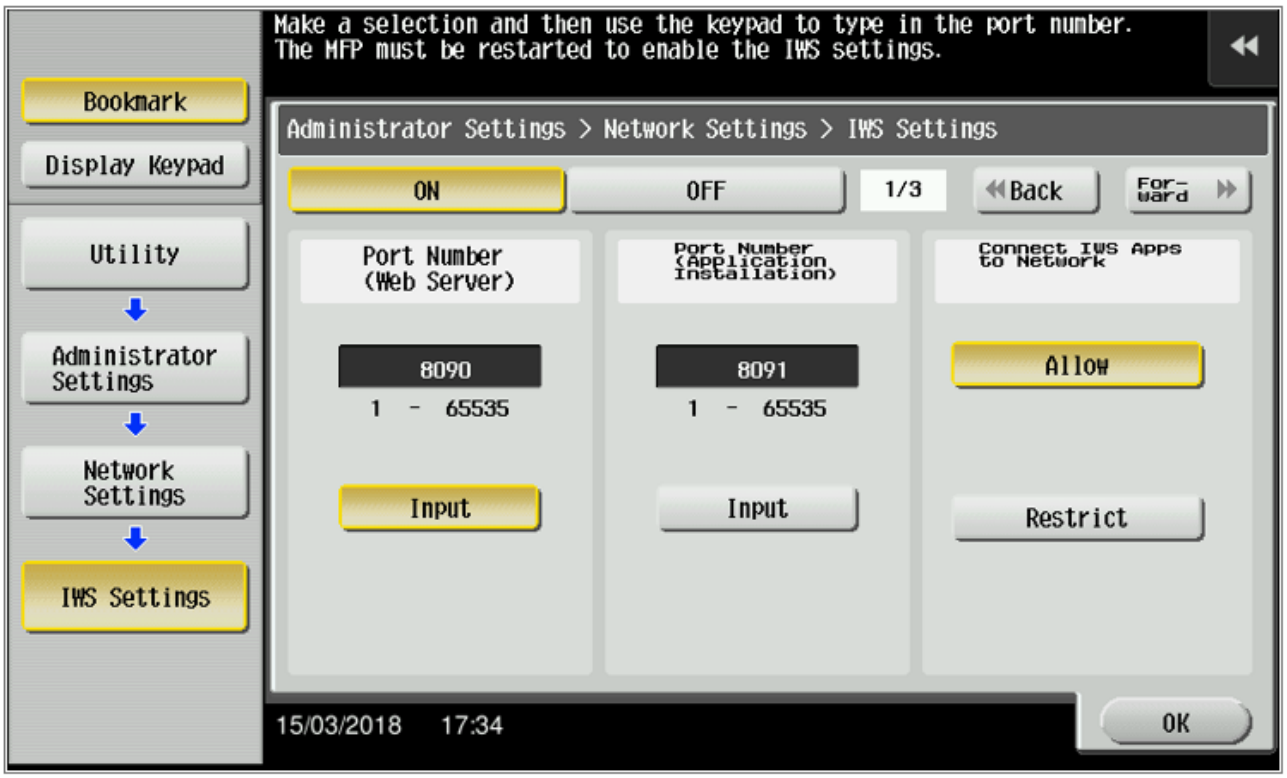
Installation using the IWS Install Tool

Prerequisites

- Section IWS Dispatcher Paragon Cloud Configuration needs to be completed before this section.

> For this step, you would require to use Konica Minolta's **IWS Install Tool**. If you do not have this tool, contact us at support@ysoft.com.
>
> This functionality is not needed in the U.S. or Canada because MarketPlace is available in the U.S. and Canada.

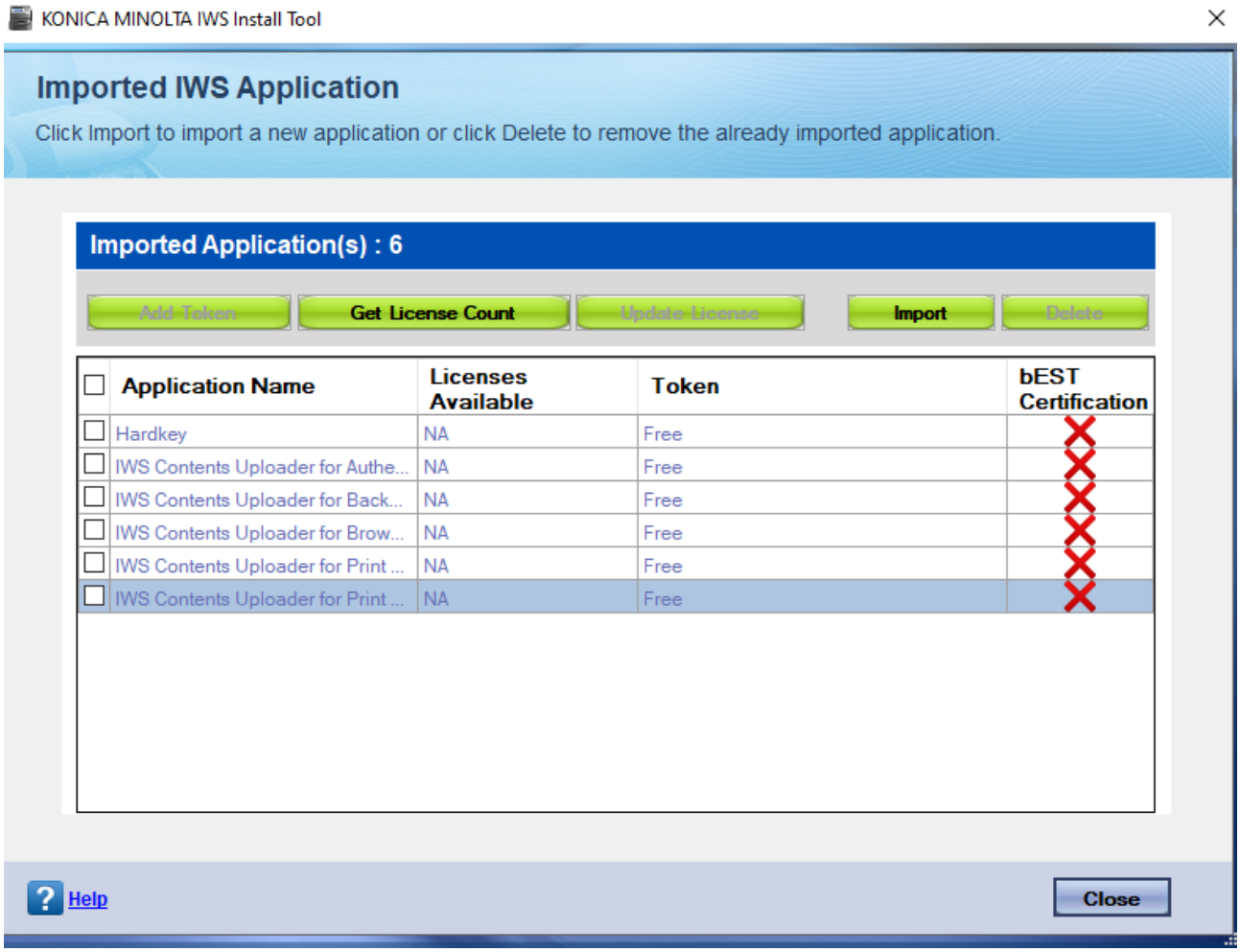
1. Make sure that the port for installing the IWS is open between the machine and the printer (default value 8091). This port can be checked on the printer:
Utility -> Administrator Settings -> Network Settings -> IWS Settings



2. Install the *IWS Install Tool*

3. Open the *IWS Install Tool*

4. Click on *Application List*



5. Click *Import*.

> In case the application Y Soft is already in the list, check the application and click on Delete.

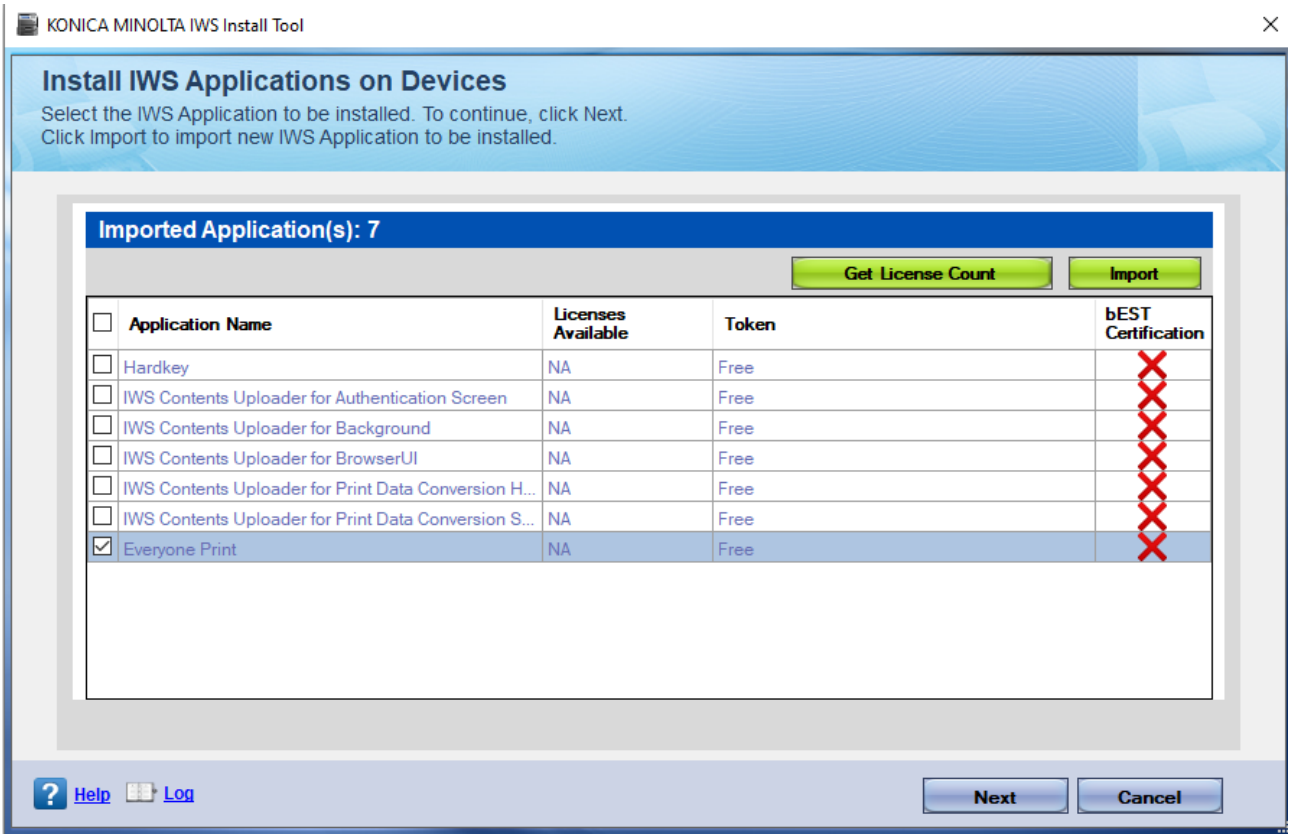
6. Select the Y Soft release file with the extension '.iws'

7. Click *Next*, agree with the license and click *Import*

8. Go back to the main screen by clicking *Close*

9. Click *Install Applications*

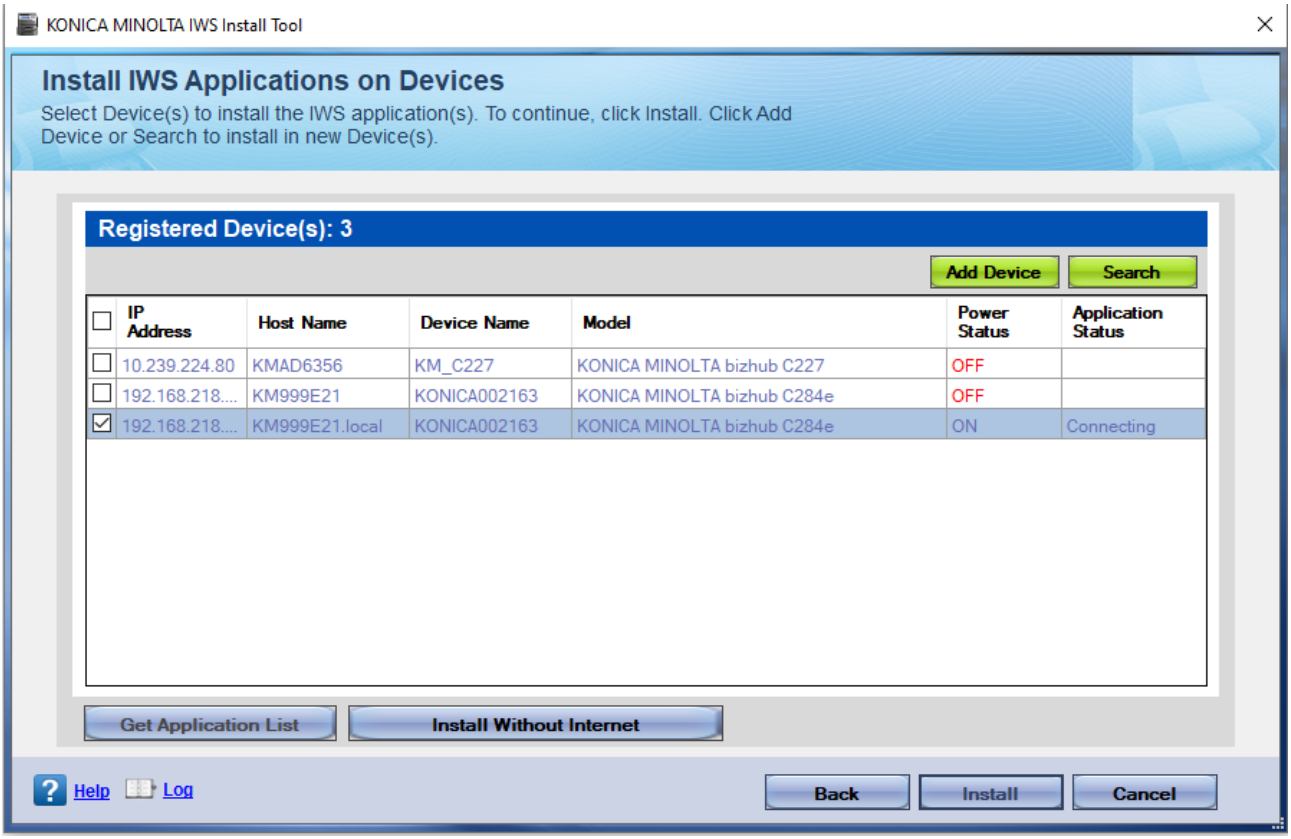
10. Check the *Everyone Print* application and click *Next*



11. Check the printer from the list and click *Install*.

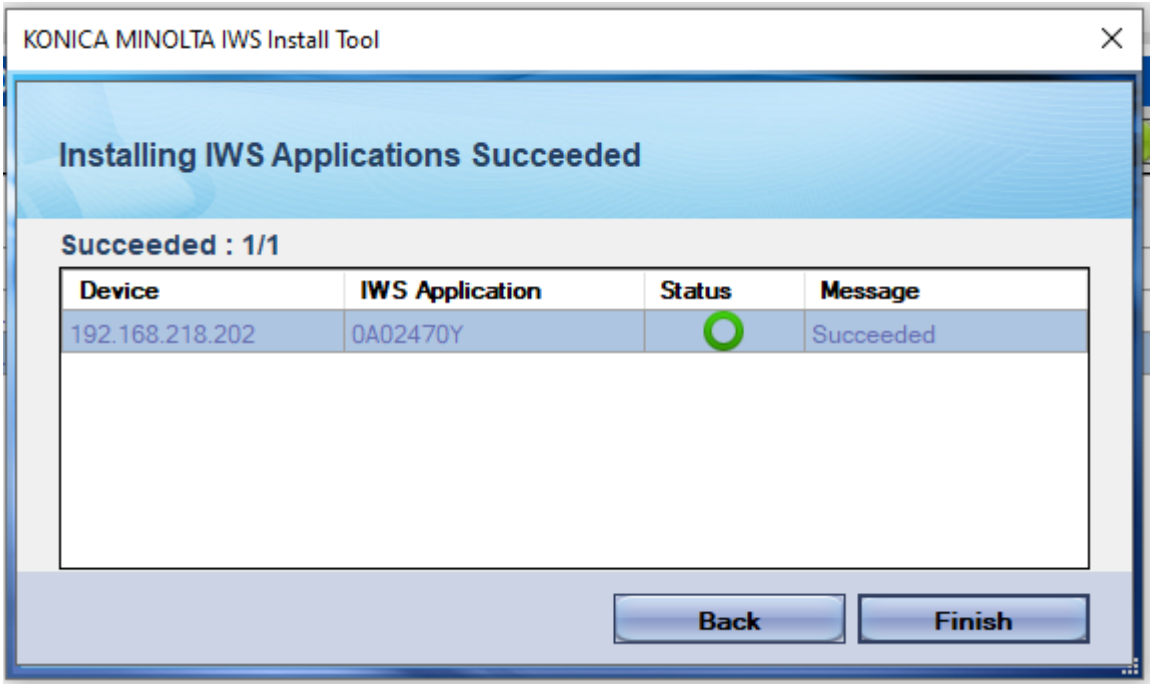
In case the printer is not available in the list click *Add Device*, it is required to have administrator rights.

In case the printer is not responding remove the printer from sleep mode by pressing the wake button.



12. Click *Finish*.

> In case the installation fails, first try to uninstall the application and then install it again.

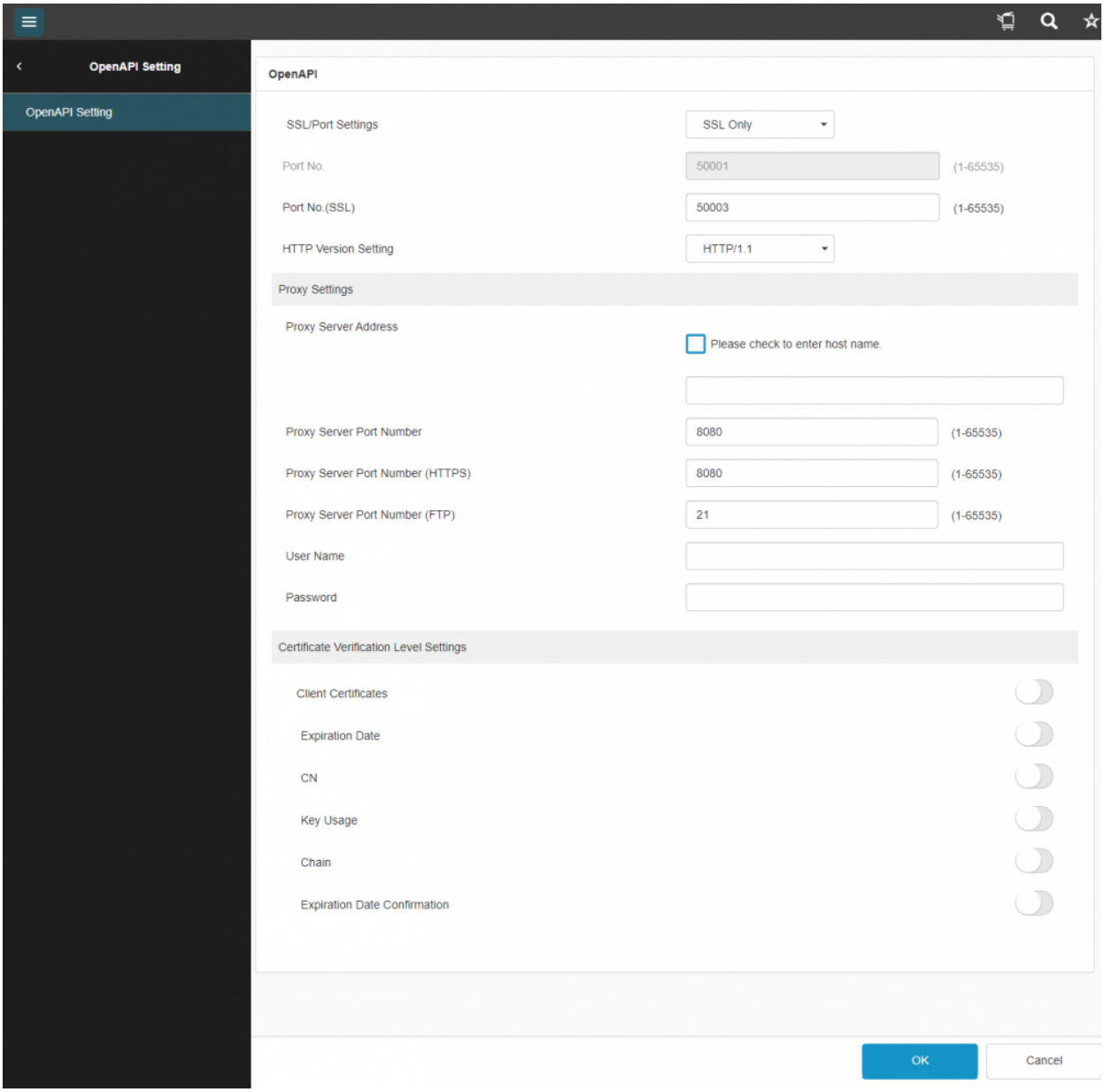


Check the overview of the Konica Minolta IWS application.

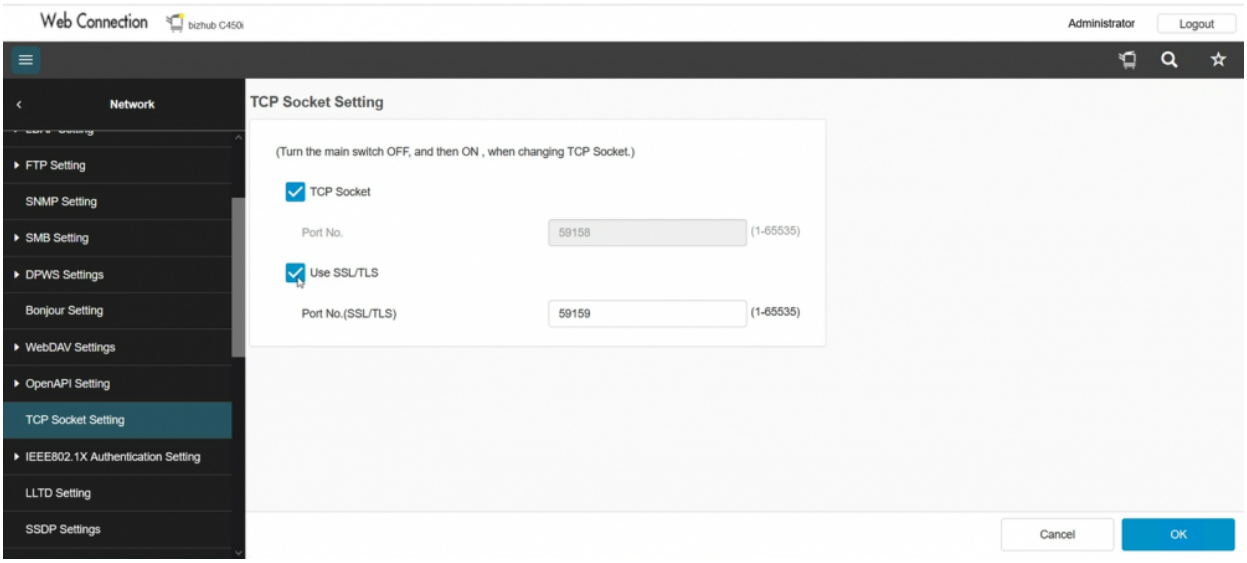
Konica Minolta OpenAPI Terminal

Prior to deploying the embedded configuration to a Konica Minolta MFD, ensure that you have configured your secondary gateway according to Secondary Gateway mapping and that the following settings are enabled and configured on the MFD:

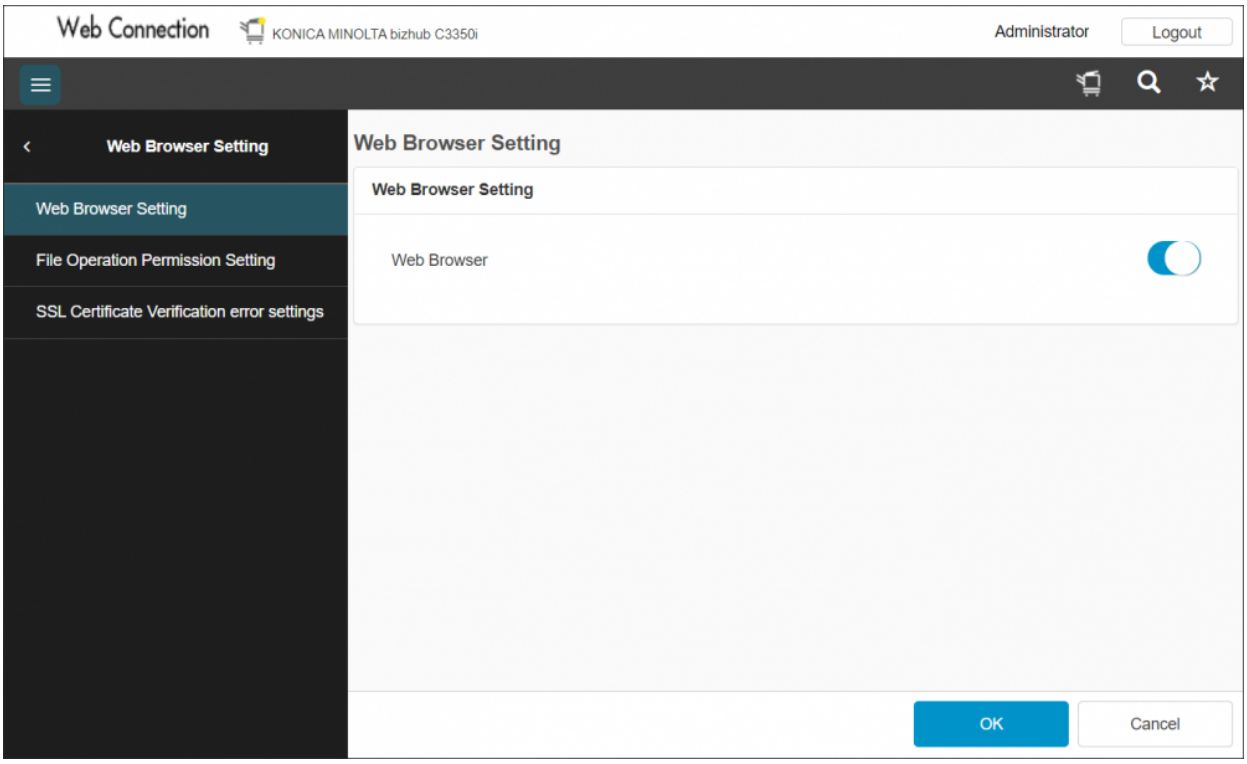
- SSL is configured on the device



- OpenAPI is installed and configured for SSL on port 50003
- TCP Socket Setting must have the setting 'Use SSL/TLS' enabled

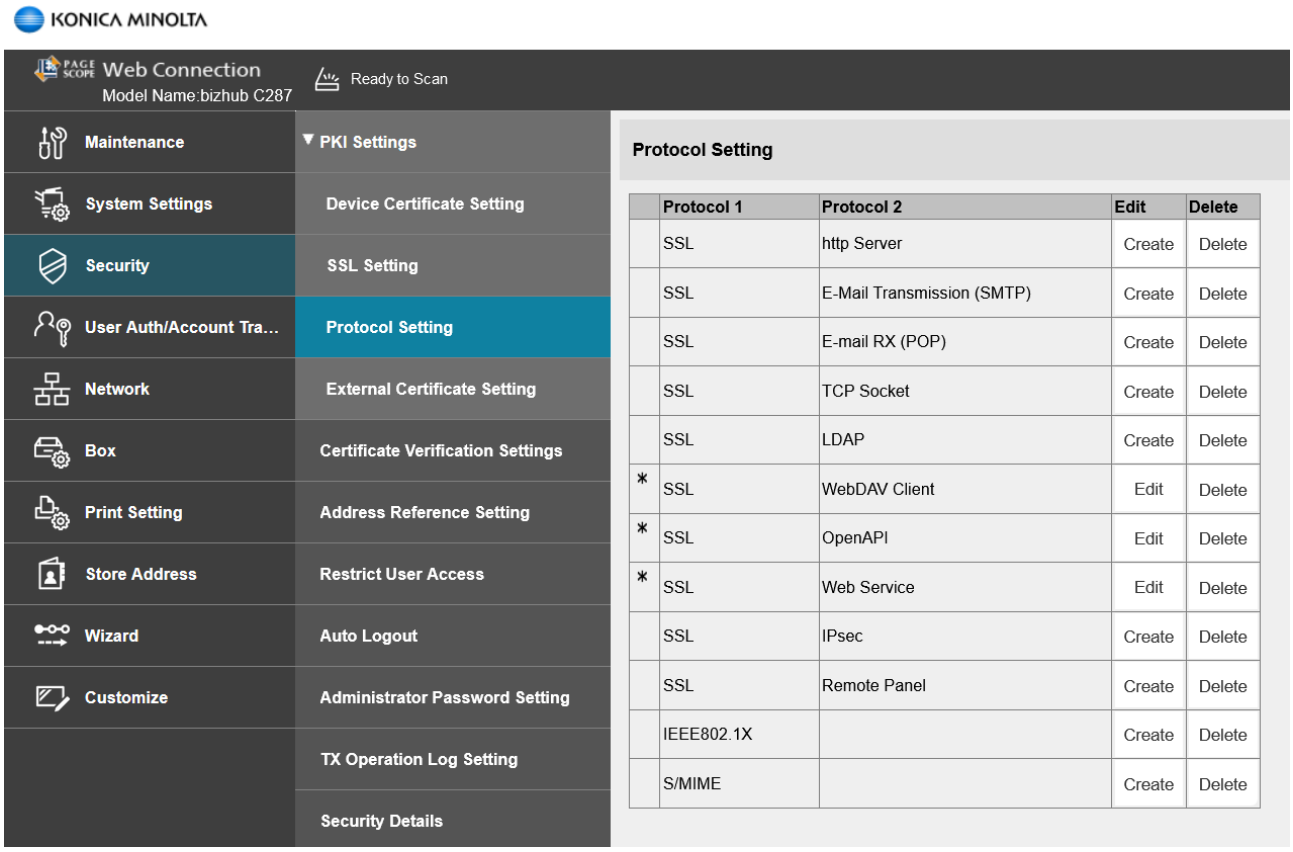


- Web Browser is Enabled on the device



- Cookies MUST be enabled for the Web Browser if not already enabled
- No other Authentication Service is currently configured on the Konica Minolta MFD

Press *Create* in *WebDAV Client*, *OpenAPI* and *Web Service*



The default configuration for the SAFEQ Cloud Terminal Client service is to support only TLS 1.2. Ensure the device is either configured for TLS 1.2, or if not possible, enable support for TLS 1.0 and 1.1 in the Terminal Client service.

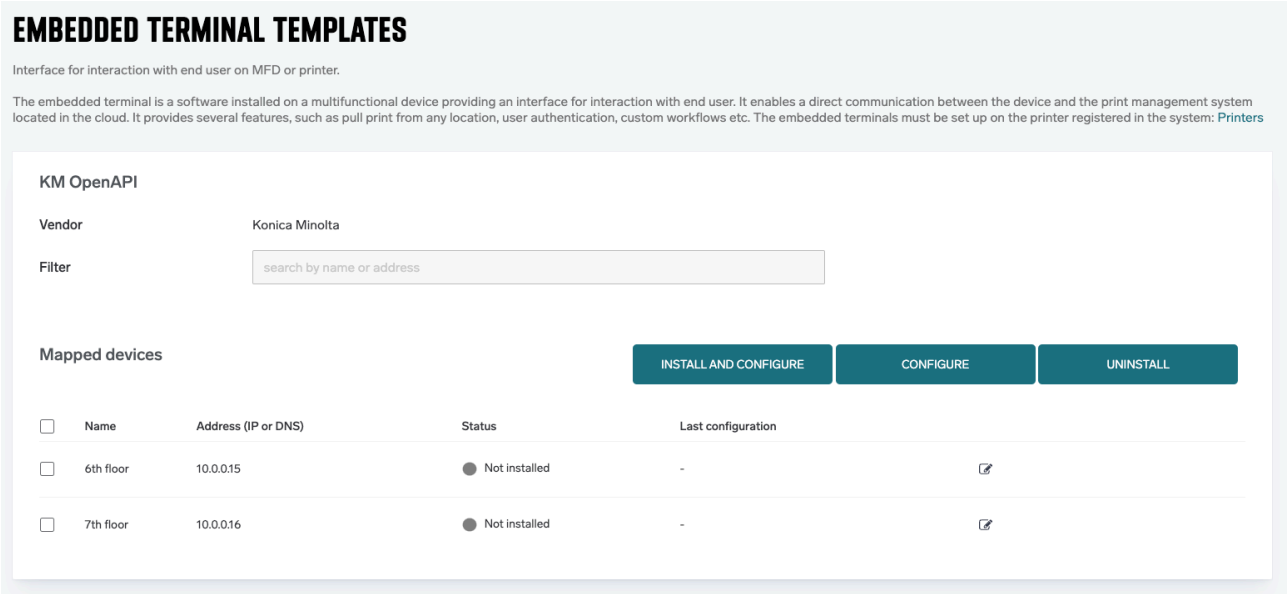
If The TCP Socket Setting does not have SSL enabled, a false-successful installation will proceed which will place the PullPrint application on the MFD but will NOT enable the authentication layer. If this occurs, enable this setting (Located in the Web panel of the device under Network > TCP Socket Setting) and redeploy.

If Public user is configured on the MFD, users will be unable to use Pull Print and Scan to My Email applications, unless they authenticate on the MFD using their SAFEQ Cloud credentials.

The application type must be set to OpenAPI.

Ensure that the 'Print Without Authentication' option is set to allow Color on the MFD settings (User Auth > Print without Authentication) otherwise all print traffic will print as Black and White.

Once the device is properly configured, push out the Embedded configuration from embedded screen in SAFEQ Cloud.



If using the default certificate loaded on the SAFEQ Cloud server, ensure that Certificate Verification is disabled on the MFD to avoid device errors concerning the new certificate.

Konica Minolta IWS Gen 2 Cloud Terminal with device locking (IWS Service Platform integration)

The feature is under KmIwsServicePlatformEmbedded feature flag and under a beta program. If interested, please register at https://www.ysoft.com/safeq/beta-testing.

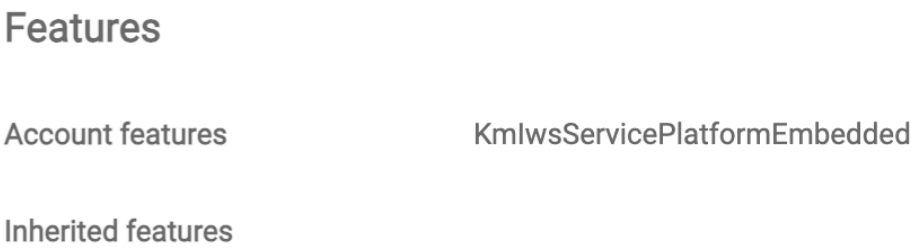
Card login is fully supported when the terminal is set as a default app. Refer to "Card reader" section below for more details.

Prerequisites

- MFD Network Configuration:

Settings	Value
Network → TCP/IP Setting → Quick IP Filtering	No Filtering
Network → IWS Settings	Enable IWS Settings
Network → OpenAPI Setting → OpenAPI Setting → SSL Port Settings	SSL Only
Network → TCP Socket Setting → TCP Socket Setting	Enable Use SSL/TLS
Network → WebDav Server Settings → SSL Settings	SSL/Non-SSL

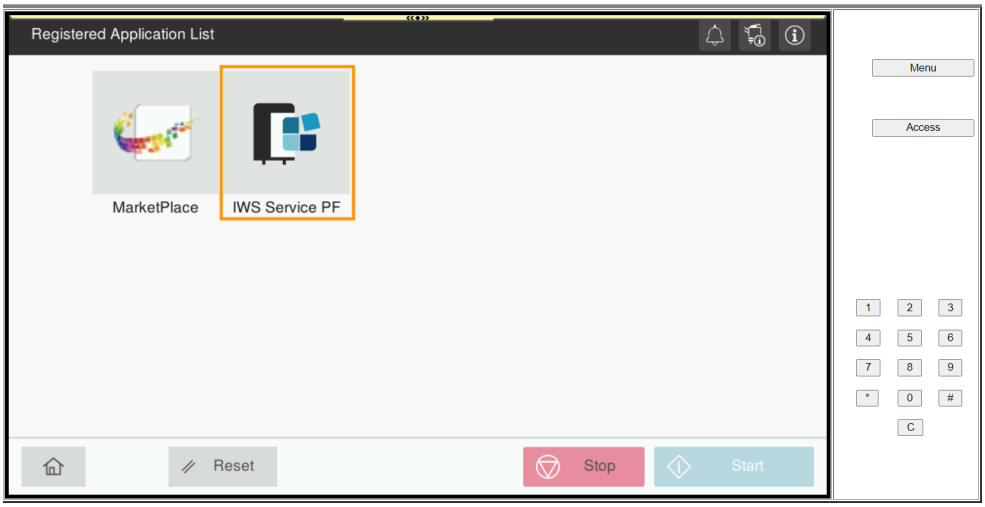
- License with a "KmIwsServicePlatformEmbedded" feature flag
  You can check if the feature is enabled by scrolling down on the Overview page. It must be present under the Account or Inherited features.



- IWS Service platform application is installed on the MFD (usually installed using KM Marketplace on MFD, valid KM Marketplace account needed)
- KM Cloud terminal installed (minimal version 2025.03.02, a guide is available here: Konica Minolta IWS Gen 2 Cloud Terminal)
- Network visibility from MFD to cloud servers

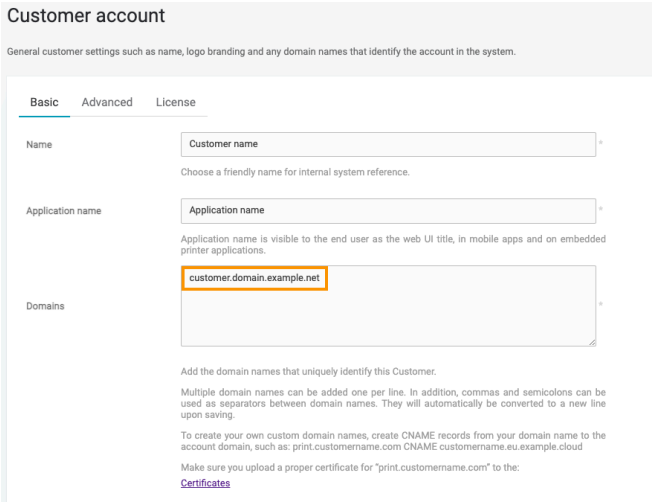
Setup

1. Open IWS Service PF application on the MFD



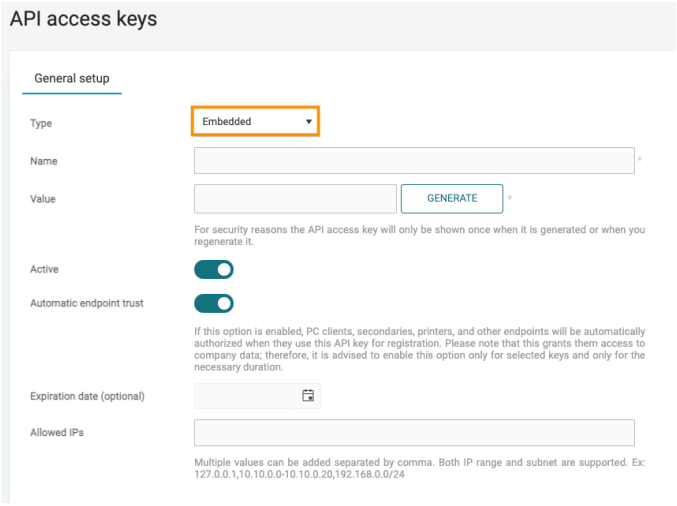
2. Prepare configuration values for the next step to avoid machine logout timeout.
   You will have to enter the tenant domain three times, the API key of embedded type twice and change "Authorization Server Parameter".

   <customer-domain>: Go to ***Settings > Customer account*** and obtain a domain from the **Domains** list

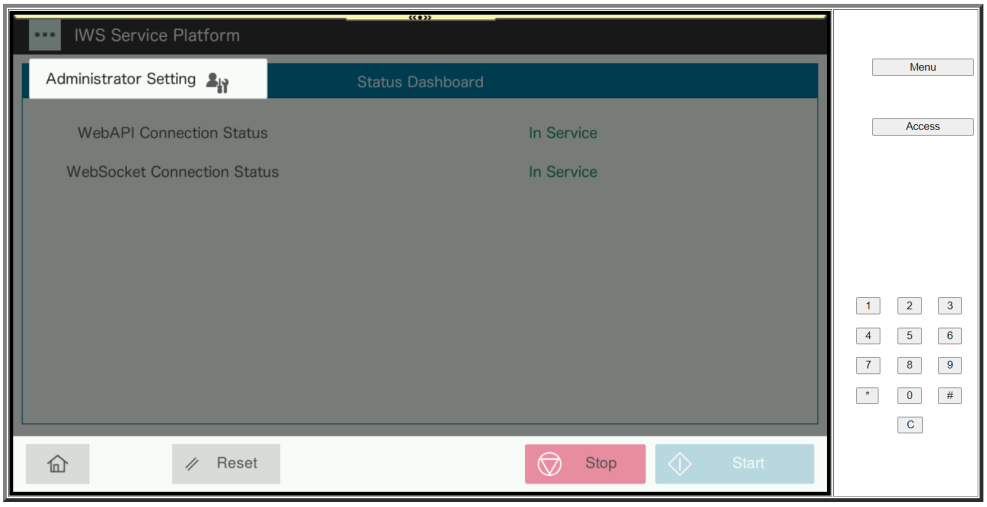


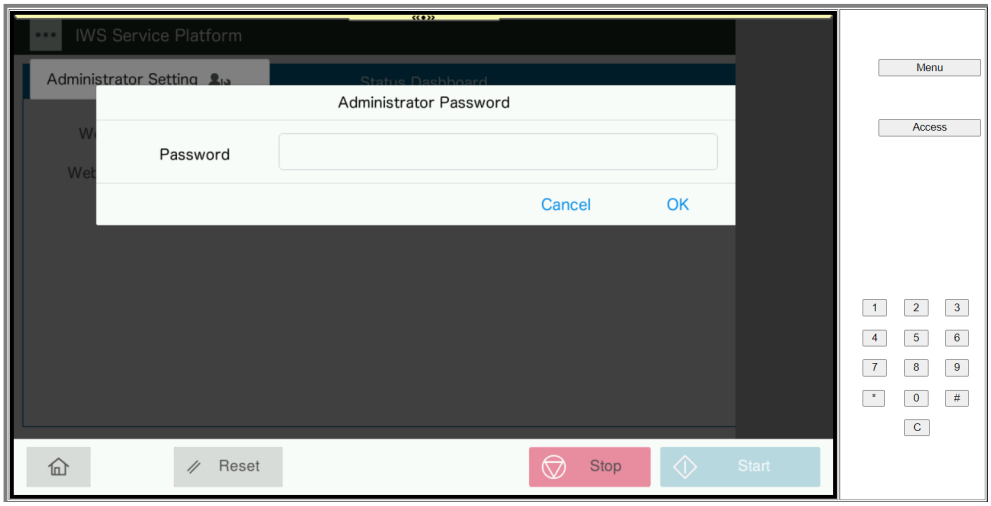
   <embedded type API KEY>: Create a new API key under ***Security > API keys > Add***, select

Embedded type and note the API key value.



3. Click on three dots in the upper left corner, open Administrator Setting, and Login by Administrator Password
   (use the admin MFD password).

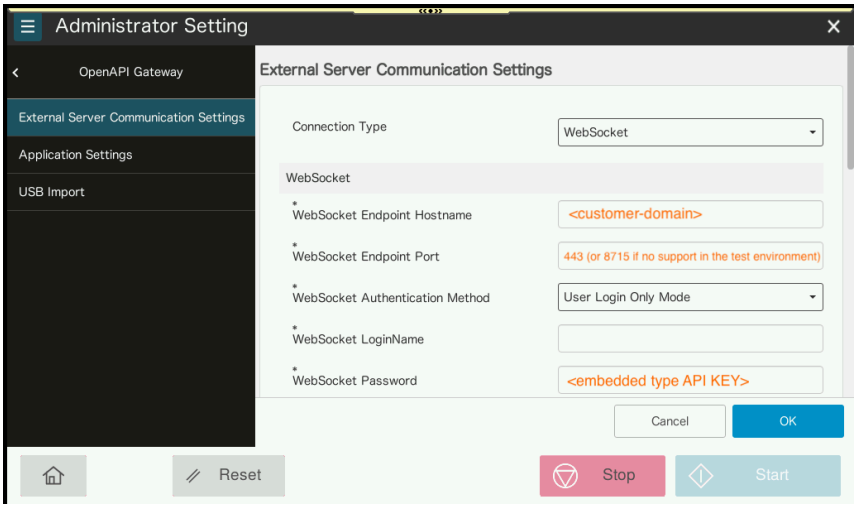


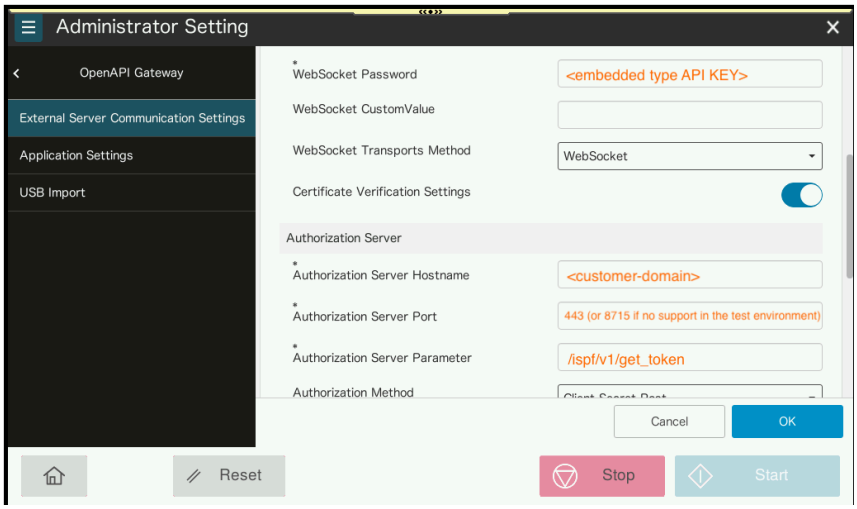


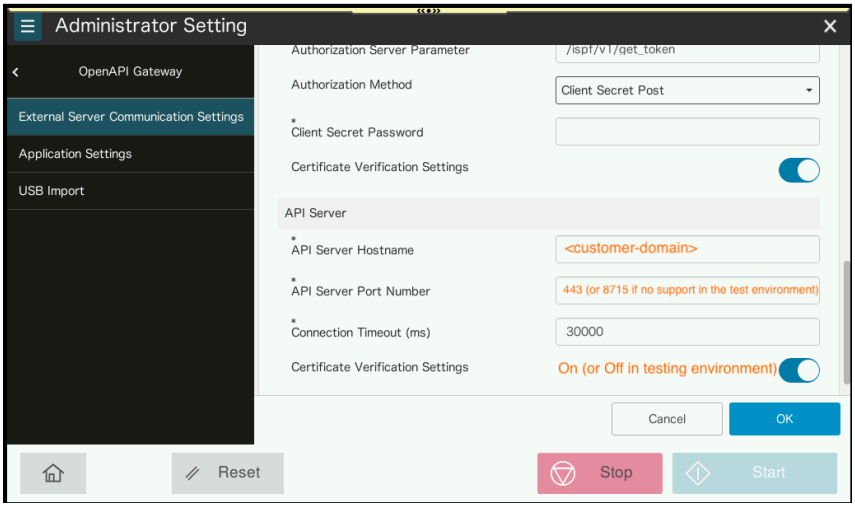
4. Go to **OpenAPI Gateway > External Server Communication Settings**

5. Fill in the following fields and click save:
   WebSocket Endpoint URL: *<customer-domain>*

WebSocket Endpoint Port: 443 (or 8715 if test environment does not support 443)
WebSocket LoginName: fill with any character, such as "t". The value is mandatory but not used.
WebSocket Password: *<embedded type API KEY>*
Authorization Server Hostname: *<customer-domain>*
Authorization Server Parameter: /ispf/v1/get_token
Authorization Server Endpoint Port: 443 (or 8705 if test environment does not support 443)
API Server Hostname: *<customer-domain>*
API Server Port Number: 443 (or 8705 if test environment does not support 443)
Client Secret Password: *<embedded type API KEY>*
Certificate Verification Settings: leave on True (or set False in a testing environment)

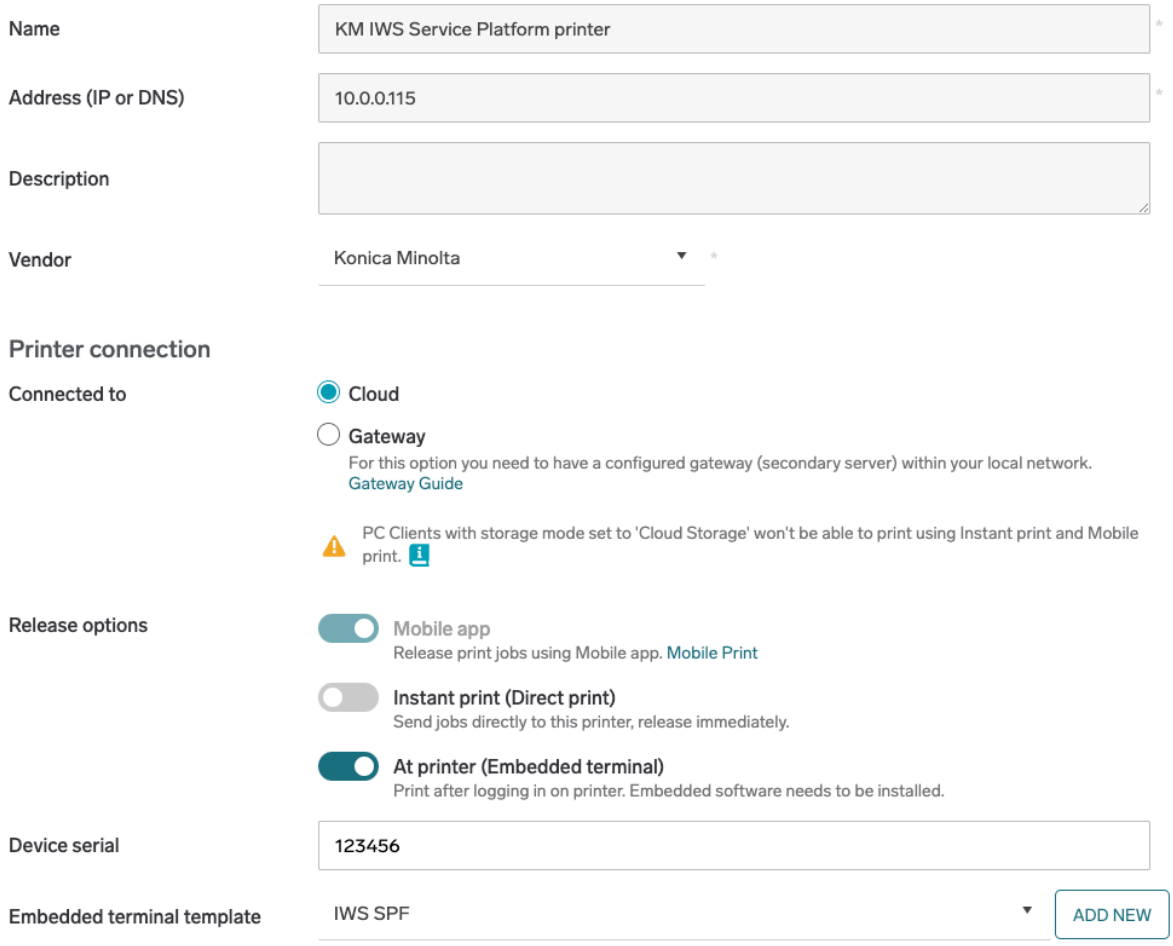






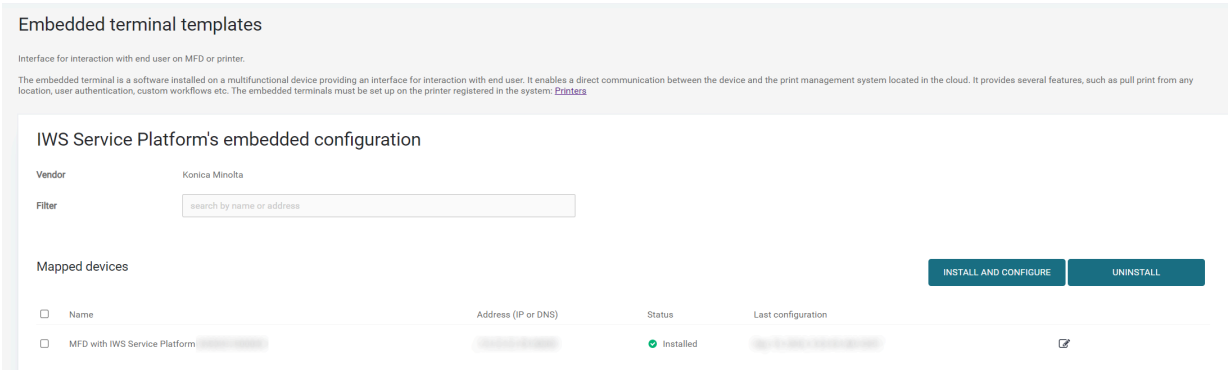
6. Login as an administrator to a web UI and check the Printers tab.

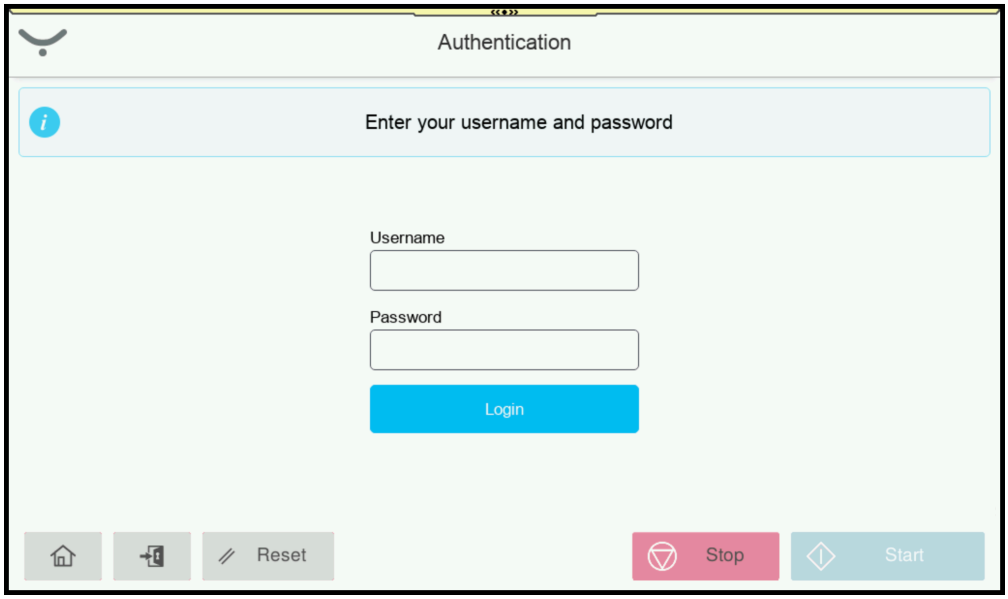
   There should be a printer with name MFD with IWS Service Platform *<mfd-serial-number>* which has assigned IWS Service Platform Embedded configuration.



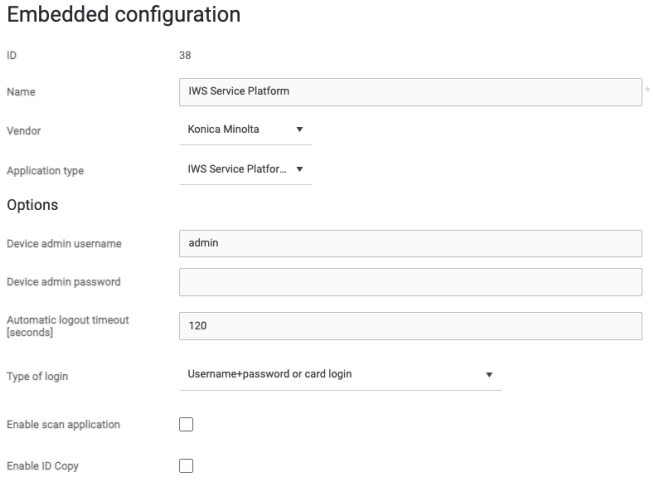
7. Go to the Embedded clients and select **Deployment actions** for **IWS Service Platform**

a. If the printer has the same machine admin password as default the Embedded is automatically installed and the MFD is locked.



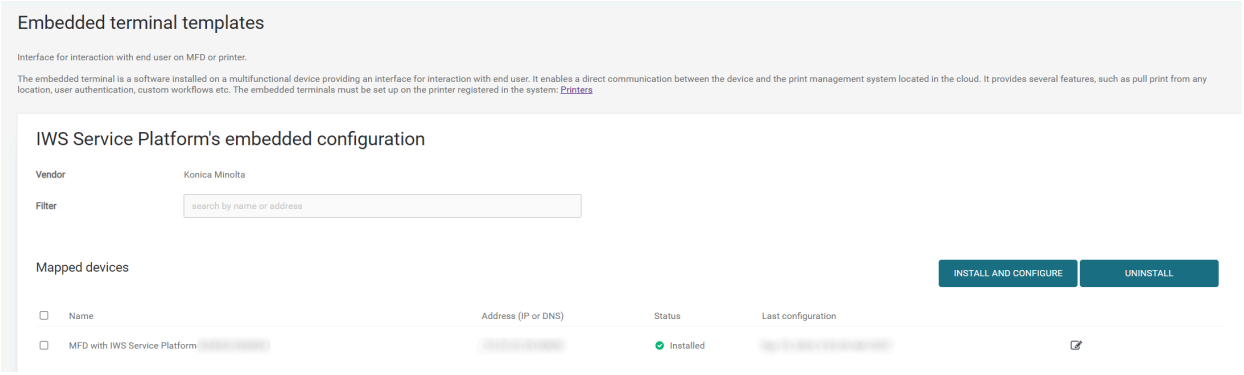


b. If the password differs the automatic installation fails and you need to change the Device admin password to the correct value in **Embedded configuration** > **Device admin password**



c. You can configure "Type of login" here (Credentials or PIN).

8. If the Device admin password is set correctly and automatic installation failed, the MFD can be Locked by the **Install and configure** button and also Unlocked by the **Uninstall** button.



Card reader in CCID mode or in Keyboard wedge mode using loadable driver

In order for a card reader to work in CCID mode or Keyboard wedge mode using loadable driver, you need to ensure following:

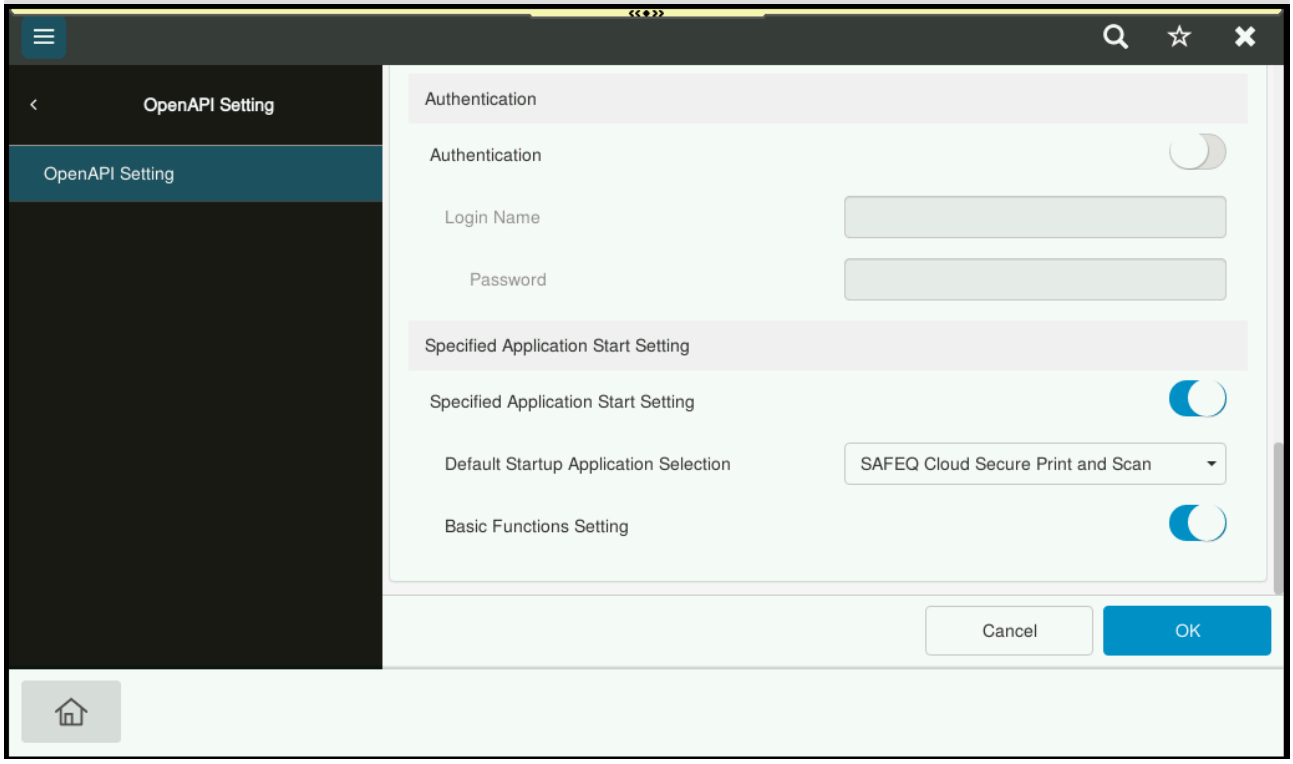
- Loadable driver is installed. You may verify it in administrator settings under Firmware Version

- "Authentification Device 2" dip switch ("Management Function Choice" on some models) is set to "Card"
- MFD is in a Kiosk mode with default startup application configured (restrict to use only default app is not required- Basic Functions Setting option can be enabled)

Setting up kiosk mode using MFD Admin settings

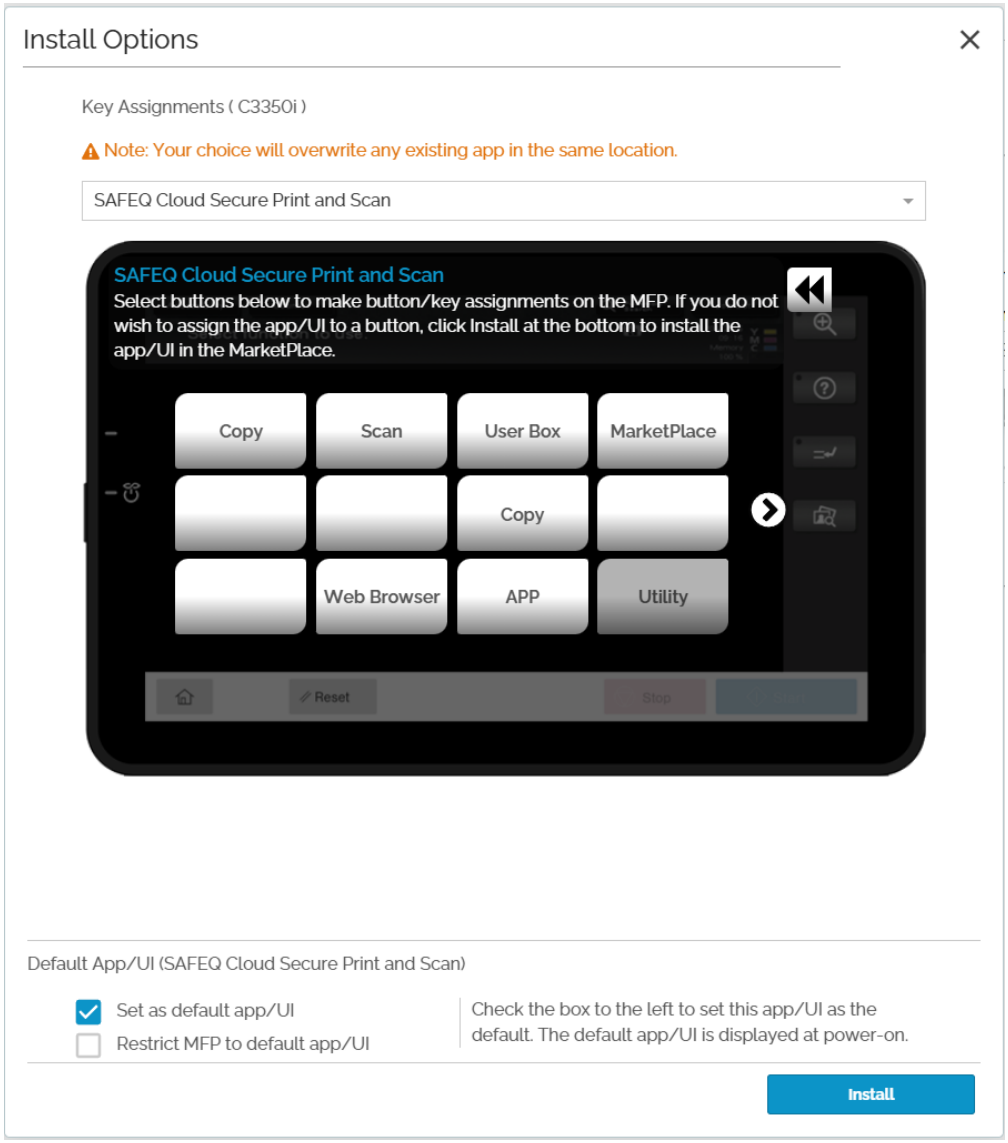
- Network → OpenAPI Setting → Specified Application Start Setting

Settings	Value
Network → OpenAPI Setting → Specified Application Start Setting → Specified Application Start Setting	On
Network → OpenAPI Setting → Specified Application Start Setting → Default Startup Application Selection	Terminal application selected
Network → OpenAPI Setting → Specified Application Start Setting → Basic Functions Settings	On = enable access to other MFD applications Off = disable access to other MFD applications (not recommended)



Setting up kiosk mode using Marketplace

Settings	Value
Set as default app/UI	On
Restrict MFD to default app/UI	On = enable access to other MFD applications Off = disable access to other MFD applications (not recommended)



Troubleshooting

If these steps don't help, please contact support.

- Printer is not created automatically - possible causes:
  - Printer with the same serial number already exists (for example from a previous Cloud terminal deployment):
    - Either change its embedded configuration to IWS Service Platform and trigger the installation under **Deployment actions** of the embedded template (icon)
    - Or delete the existing printer and restart the MFD to trigger automatic creation again
  - Wrong domain in the configuration - check if it was entered correctly
  - Wrong API key in the configuration - check if it was entered correctly
  - IWS Service PF application was previously configured to a different environment - please restart the MFD after the configuration.

- Printer is created, but cannot be installed:
  - Please see the exact message under **Printers > Embedded templates > Deployment actions of the IWS Service Platform** embedded template (icon), follow the instructions and manually trigger the installation from deployment actions again.

Supported Firmware Versions

Model	Required Version
bizhub C750i	GC4-RB or G00-RF or later
bizhub C650i, C550i, C450i	GC4-RB or G00-RF or later
bizhub C360i, C300i, C250i	GC4-RB or G00-RF or later
bizhub C287i, C257i, C227i	GC4-RB or G00-RF or later
bizhub 950i, 850i	GC4-RB or G00-RF or later
bizhub 750i	GC4-RB or G00-RF or later
bizhub 650i, 550i, 450i	GC4-RB or G00-RF or later
bizhub 360i, 300i	GC4-RB or G00-RF or later
bizhub C4050i, C3350i	GC4-RB or G00-RF or later
bizhub C4000i	GC4-RB or G00-RF or later
bizhub 4750i, 4050i	GC4-RB or G00-RF or later
bizhub 4700i	GC4-RB or G00-RF or later
bizhub C751i	GC4-RB or G00-RF or later
bizhub C651i, C551i, C451i	GC4-RB or G00-RF or later

Model	Required Version
bizhub C361i, C301i, C251i	GC4-RB or G00-RF or later
bizhub 751i	GC4-RB or G00-RF or later
bizhub 651i, 551i, 451i	GC4-RB or G00-RF or later
bizhub 361i, 301i	GC4-RB or G00-RF or later
bizhub C4051i, C3351i	GC4-RB or G00-RF or later
bizhub C4001i	GC4-RB or G00-RF or later
bizhub 4751i, 4051i	GC4-RB or G00-RF or later
bizhub 4701i	GC4-RB or G00-RF or later

Limitations

General

- Configuration to the secondary gateway server is not supported.
- Features that are not documented may not be supported.
- The software logout button is not present. Logout is done only when the user clicks the HW logout button.

Authentication

- Card authentication is active regardless of the chosen login method. It can be disabled by unplugging the card reader or turning it off in the MFD settings.
- Card authentication registration is supported in keyboard mode. CCID Mode (also known as Loadable Driver Mode) is also supported, but only when the terminal is in kiosk mode.
- Logging out with a card is not available.

Accounting

- If you are using Cloud Terminal version 2024.11.01 or older with SQC server version 2024.11.14 or newer, the Copy job accounting from Cloud Terminal will be doubled in Reports.
- If you are using Cloud Terminal version 2025.03.02 or older with SQC server version 2025.03.20 or newer, the Print job accounting from Cloud Terminal will be doubled in Reports.
- External direct print is not accounted (may change in future releases)

Printing

- USB printing is not restricted by USB print permission. Instead, it inherits the release job and color print permissions for black-and-white and color printing, respectively

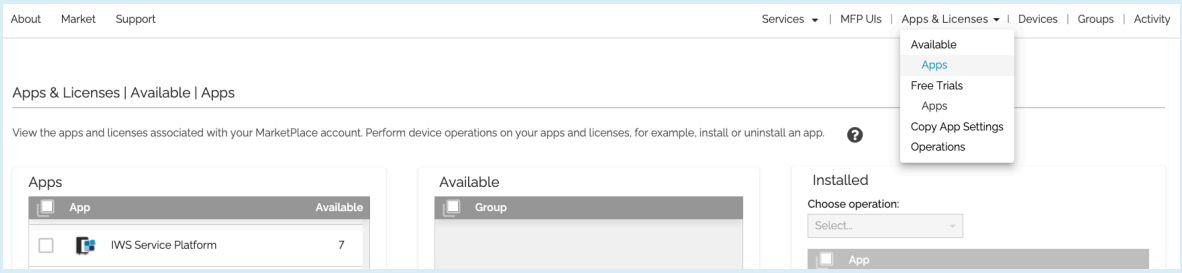
3rd party limitations

KM IWS Service Platform

- USB import - Currently not implemented feature.

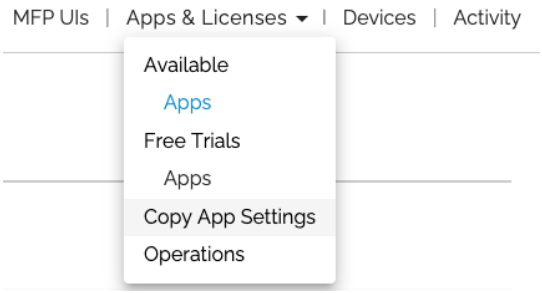
Application configuration copy through Marketplace

If the app is not present under Copy App Settings, check Available Apps and click on the app in the Apps list in the left.



To copy an app's settings from one device to other devices, do the following:

1. Install the app on a device and configure it using the App Manager.
2. Install the app on all devices that you want to copy the app's configuration settings to.
3. Click on **Apps & Licenses** on the MarketPlace menu bar. The Apps & Licenses drop-down menu appears.
4. From the drop-down menu, select Copy App Settings.



The Copy App Settings page appears displaying the following panels:

- Select App - Lists the apps for which the Copy App Settings feature is available.
- From: Reference Device - Lists the devices (if any) on which the selected app is currently installed and has been configured. Devices in this panel are organized by device group.
- To: Target Device - Lists the devices (if any) on which the selected app is currently installed, organized by device group.

5. In the Apps panel, select the app whose settings you want to copy. The From and To panels populate with the devices on which the selected app is currently installed, restricted to devices for which you are an **administrator**.
6. In the From panel, select the reference device (that is, the device containing the app settings you want to copy). The To panel activates.
7. In the To panel, select the target devices (that is, the devices to which you want to copy the app's settings). The **Copy App Settings** button activates.
8. Click on the **Copy App Settings** button. The copy process begins and the **Operations page** updates with the copy status for each of the selected devices.
   - If the copy process was successfully initiated for all devices, the following occurs on the Copy App Settings page:
     - A green banner appears briefly on the screen.
     - A green check mark appears next to each selected device.
     - The **Close** button appears. To end the current operation, click on this button.
   - If the copy process was not successful for one or more devices, the following occurs on the Copy App Settings page:
     - A red banner appears on the screen.
     - A red icon appears next to the unsuccessful devices and **Select devices with an error and try again** appears in red.
     - To retry the copy process, select one or more failed devices and click on the **Copy App Settings** button.

Notes:

- The Copy App Settings feature overwrites all of an app's configuration settings on the target devices.
- The "Last Synced" timestamp indicates the last time the selected app's configuration settings on the selected device were synced with MarketPlace. If you updated an app's settings in the last few minutes and you want to include the changes when using the Copy App Settings feature, be sure to check the Last Synced timestamp to confirm the changes have been synced with MarketPlace.
- The "No Configurations" label appears in the To panel for any devices on which the selected app's configuration settings have never been changed from the default settings and then synced with MarketPlace.

Kyocera Terminal

This guide is to install, configure and setup the Kyocera Embedded Terminal consists of the following parts:

- Kyocera devices hardware requirements
- Kyocera printer setup
- Install Kyocera application
- SAFEQ Cloud Server Setting using SAFEQ Cloud Web UI
- Kyocera application

Before you begin, make sure that your secondary gateway is configured according to Secondary Gateway mapping.

Requirements

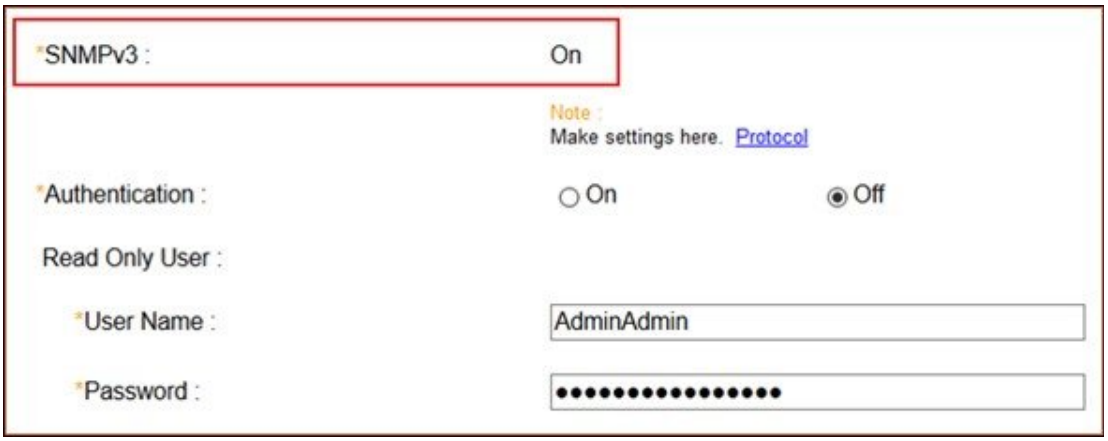
The MFD must support the HyPAS applications.

Some devices require additional memory and an additional SD-Card

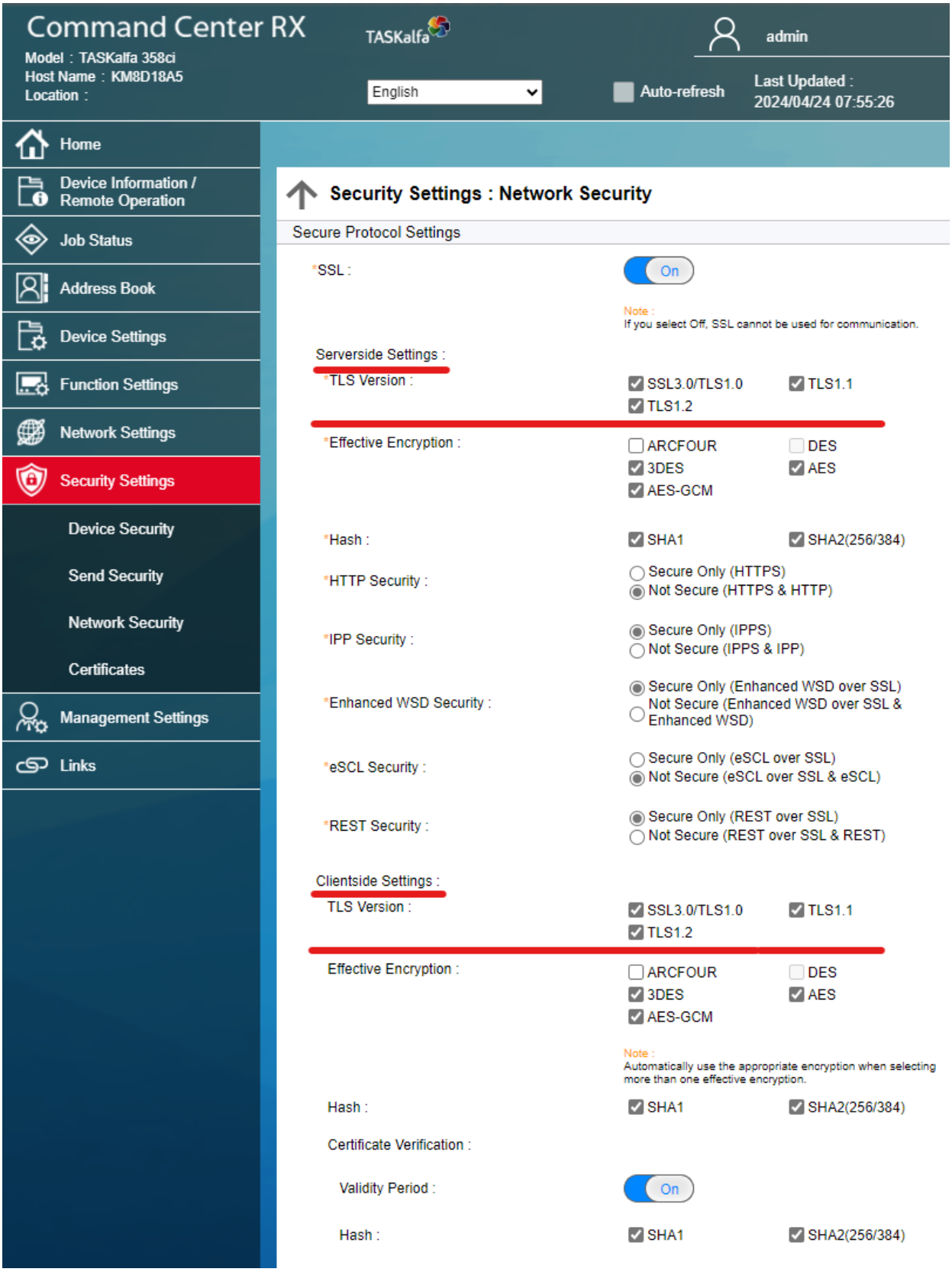
For a list of supported devices, go to SAFEQ Cloud Partnerzone (https://www.ysoft.com/safeq/hardware-compatibility-list/ysoft#cloud)

MFD setup

1. Enable SNMPv3 on the device.



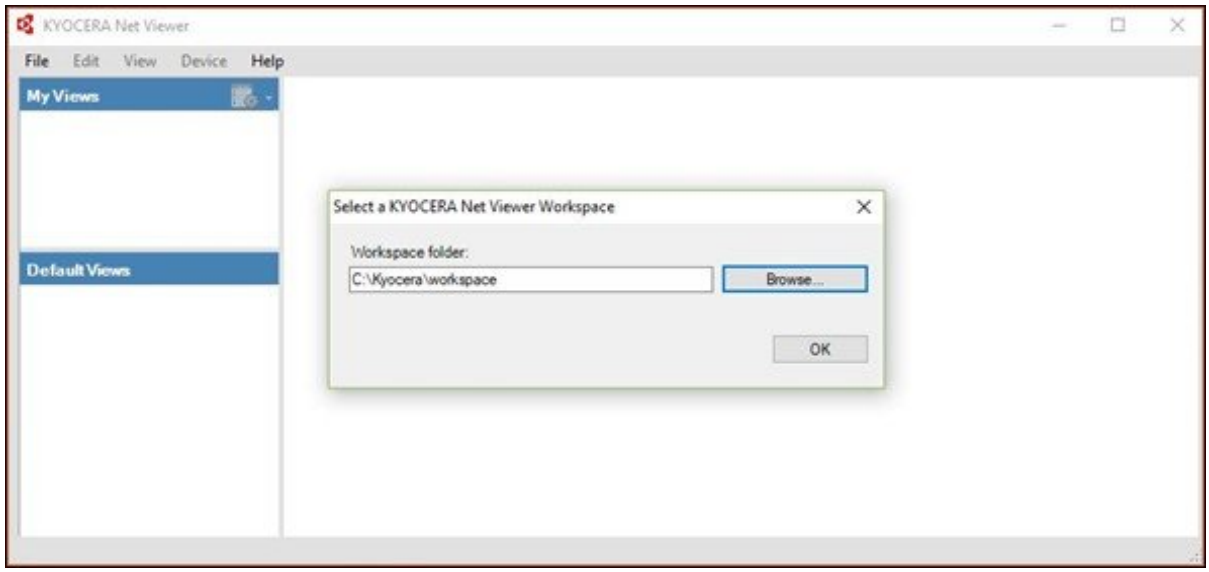
2. If you want to change the MFD's admin password on the newer models, select all TLS versions in the Serverside Settings and Clientside Settings and save the settings before changing the password.



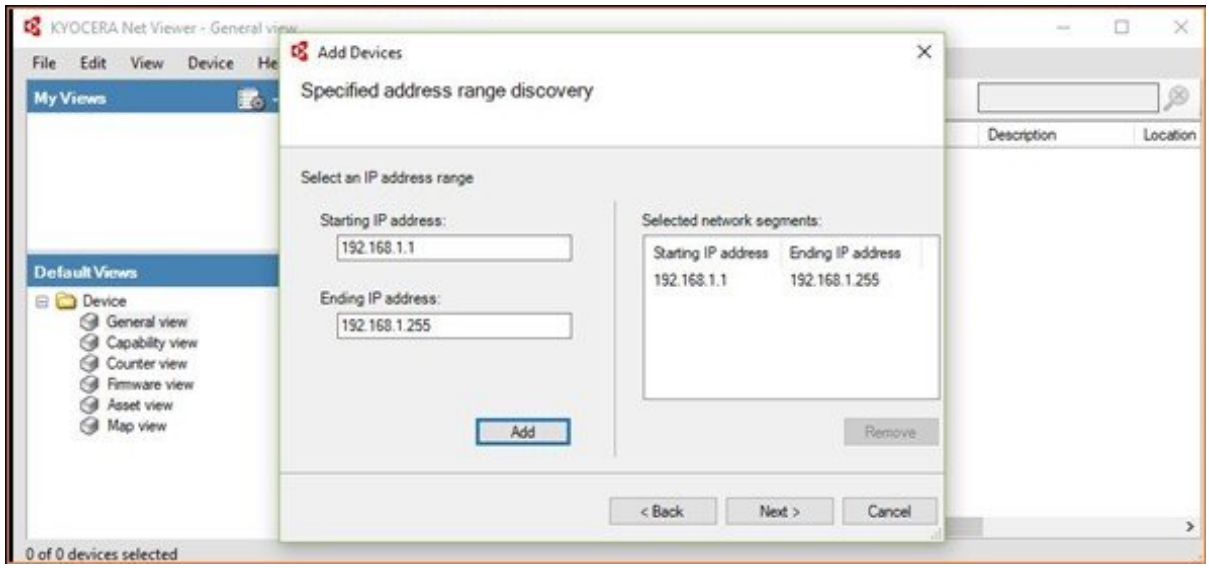
3. Download the installation package (a pkg file) from the Y Soft Partnerzone. Go to the Library and search for *Kyocera Embedded Client*.

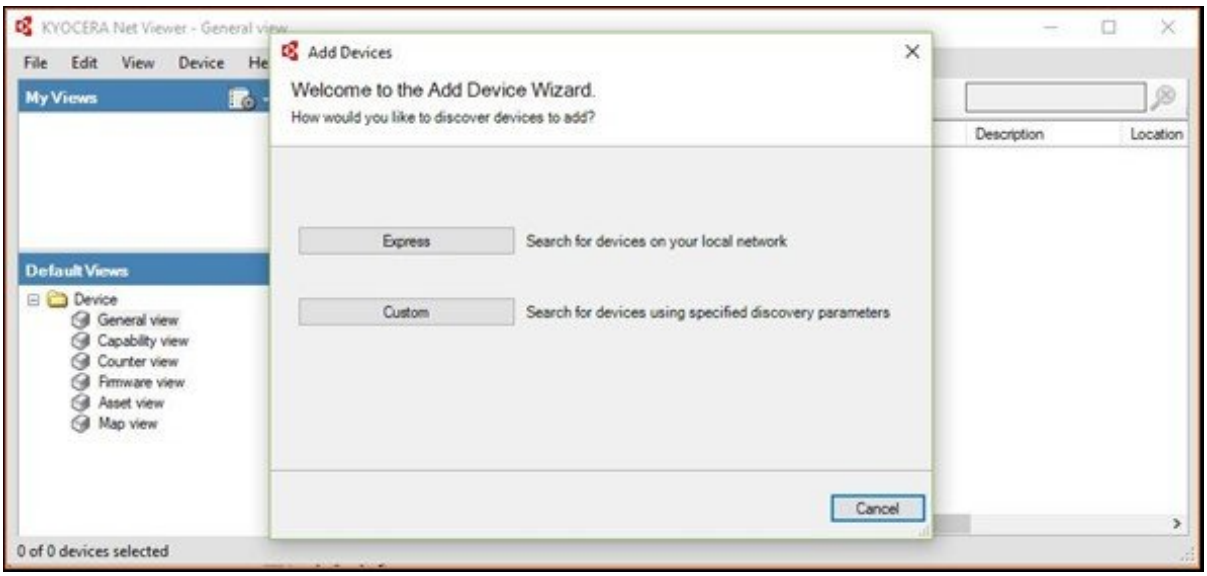
Installing the Kyocera Embedded Terminal via KYOCERA Net Viewer

1. To install the terminal, download and install KYOCERA Net Viewer.
2. Run KmInstall.exe.
3. Search for devices:
   a. Create a folder and select it as the workspace folder.



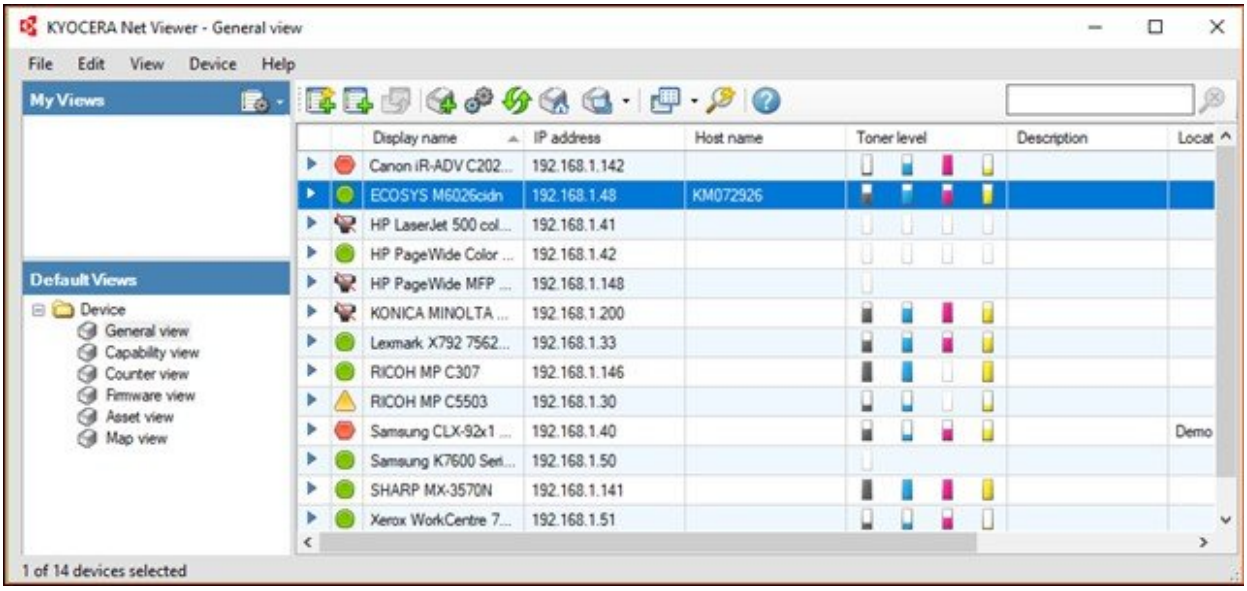
   b. Search for devices in your network.



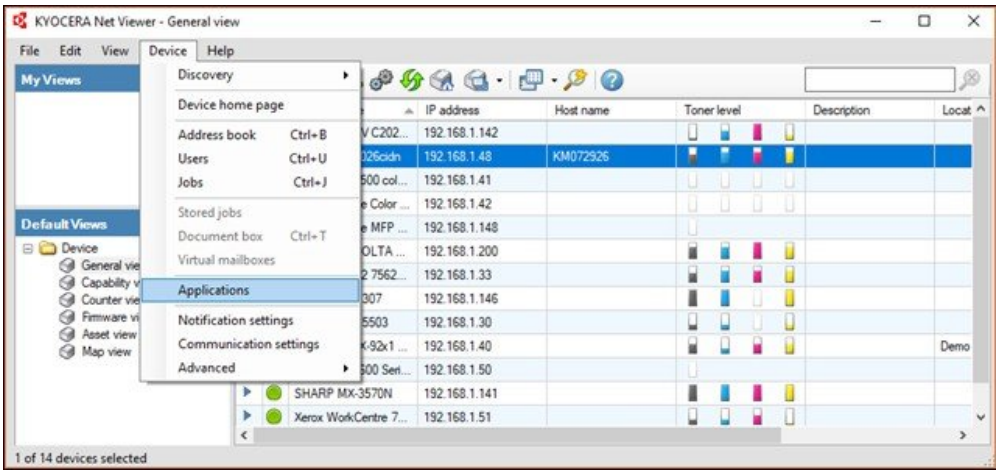


c. Set SNMPv3 Username and password.

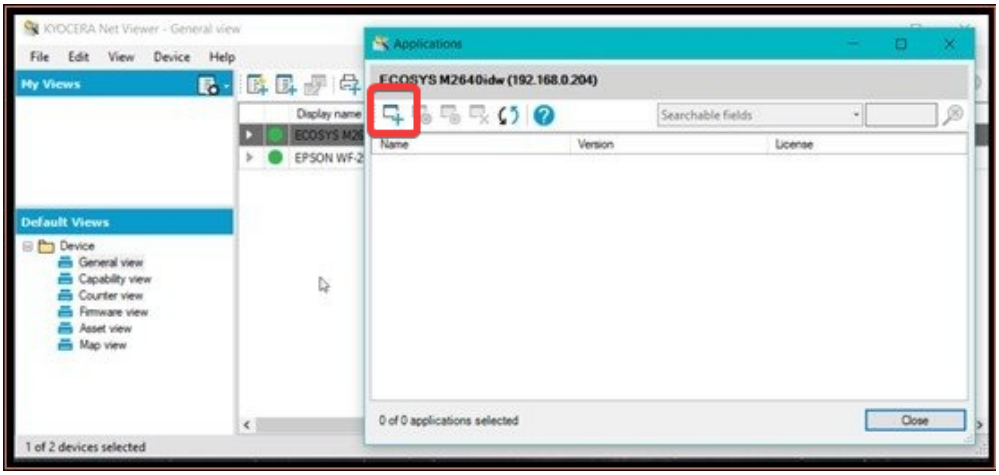
4. To install the terminal, select the device(s) where you wish to install it.



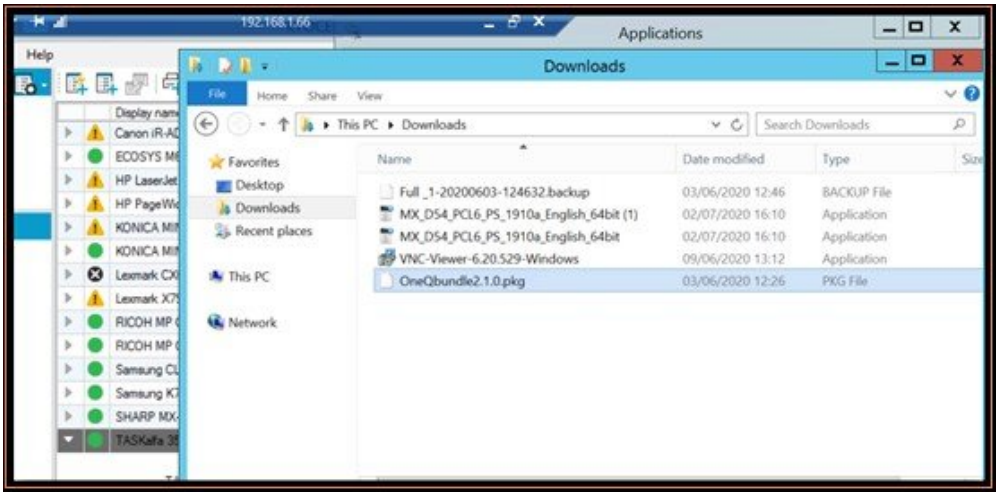
5. Click **Device** > **Applications**.



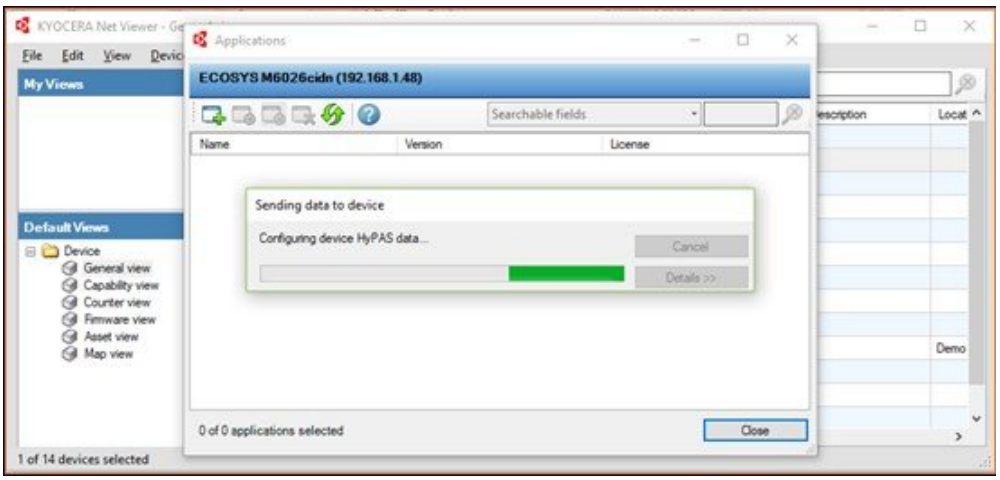
6. Click the **Install new** button.



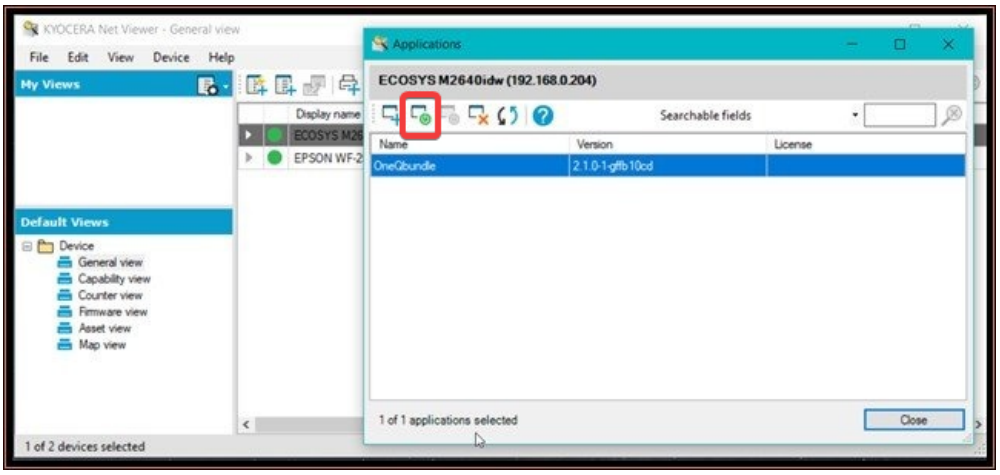
7. Browse to where you have saved the pkg file and select it.



8. Run the installer.



9. Click the activation icon and activate the application without a license key.



Default Screen setting

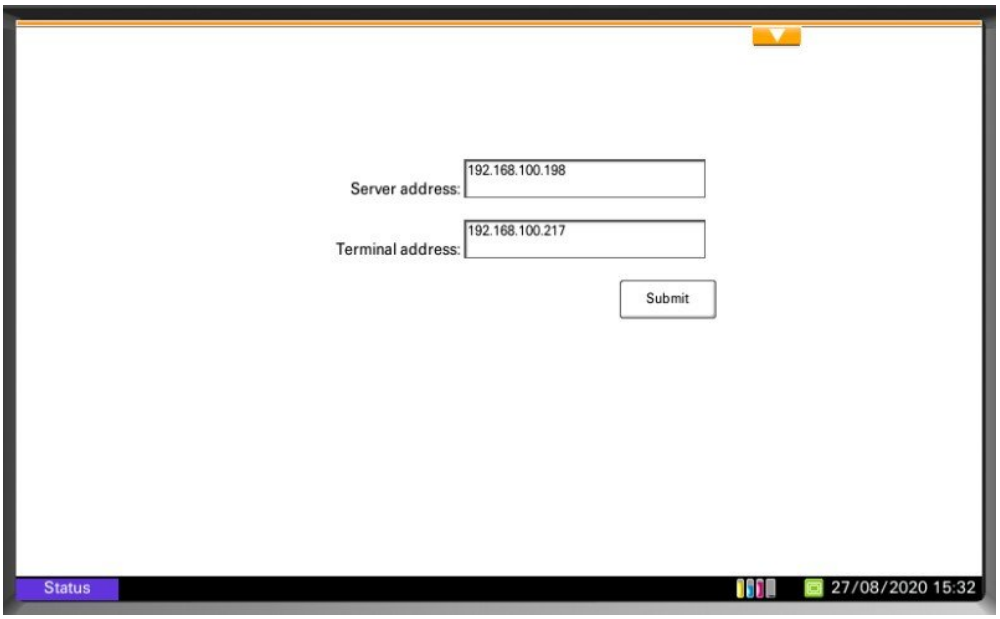
1. Change this setting if you want the user's job list to be displayed after they are logged in. You can also set the initial screen after login to be one of the native MFD's functions.
2. Go to the printer's home screen.
3. Log in as the machine administrator.
4. Go to **Device Settings** > **System**.
5. Set **Default Screen** to **Favorites/Application**.
6. Set the Default Screen (Favorites/Application) to the One Q application.
7. Reboot the MFD.

Using Kyocera Fleet Service (KFS)

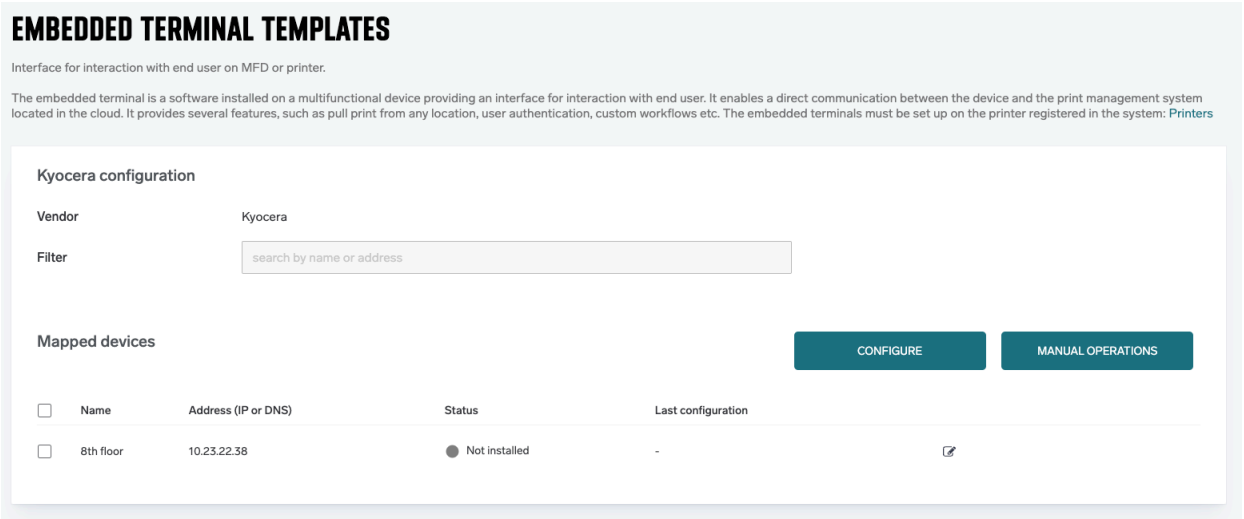
You can also install the Kyocera Embedded Terminal via the Kyocera Fleet Service.
For more information on using Kyocera Fleet Service please contact your Kyocera vendor.

Configuring the terminal

1. After you have installed the terminal, tap the terminal's icon on the MFD.
2. In the **Server address** field, enter the secondary gateway address.
3. The **Terminal address** field should already contain the MFD's IP address. If not, enter it.

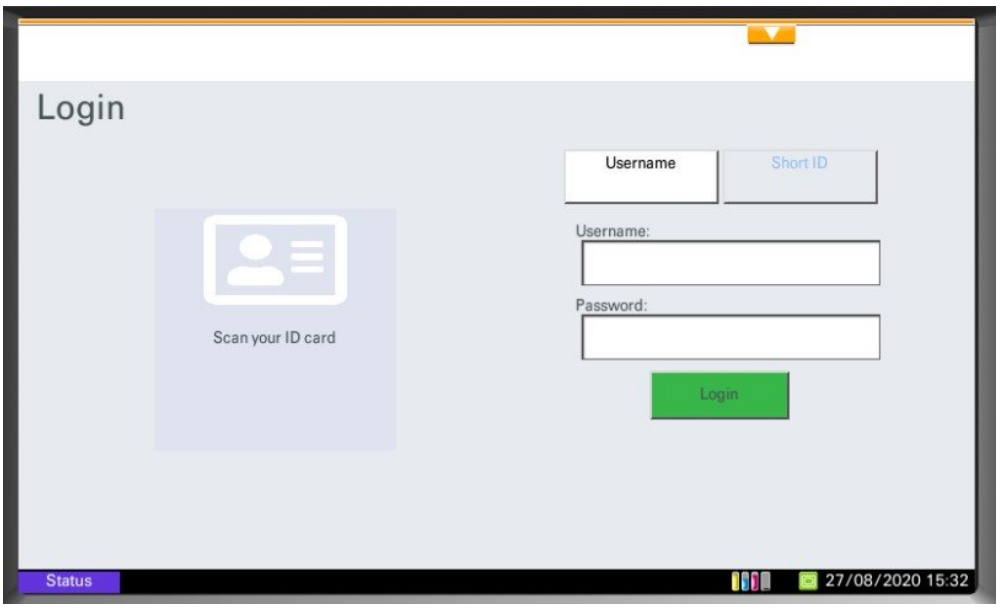


4. Tap **Submit**.
5. Log in to SAFEQ Cloud Web UI and create the embedded configuration for Kyocera, if not done already. See Embedded Terminals' configuration.
6. Select the MFD from the list and click **Configure** to push the configuration to the MFD.

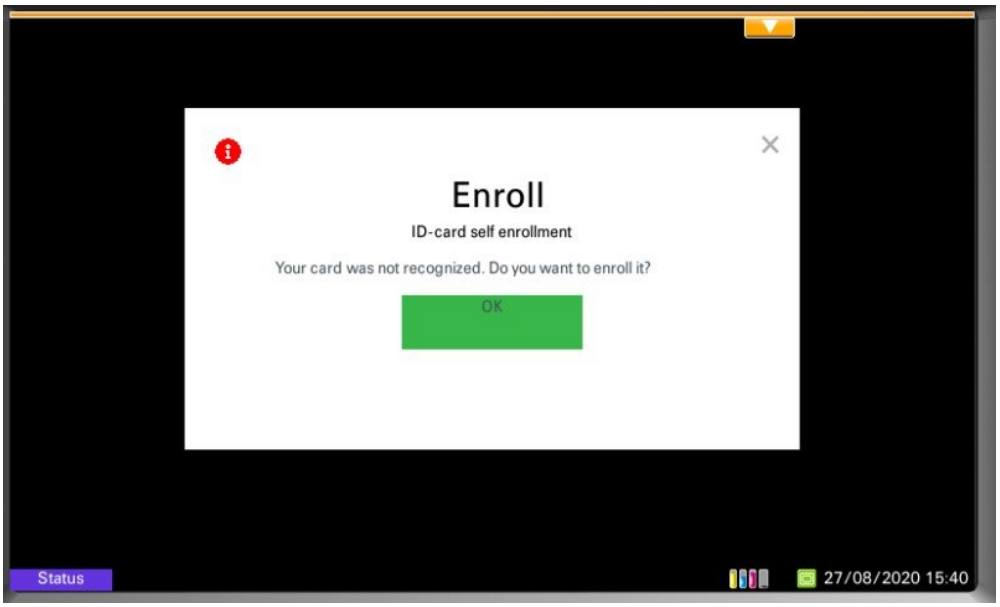


Using the terminal

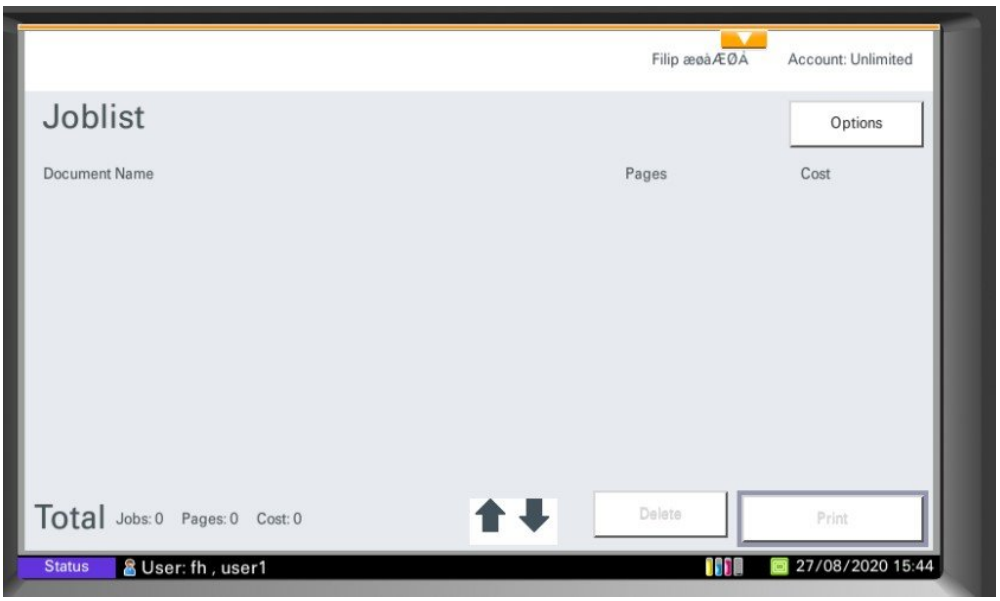
- Login screen



- Card enrollment



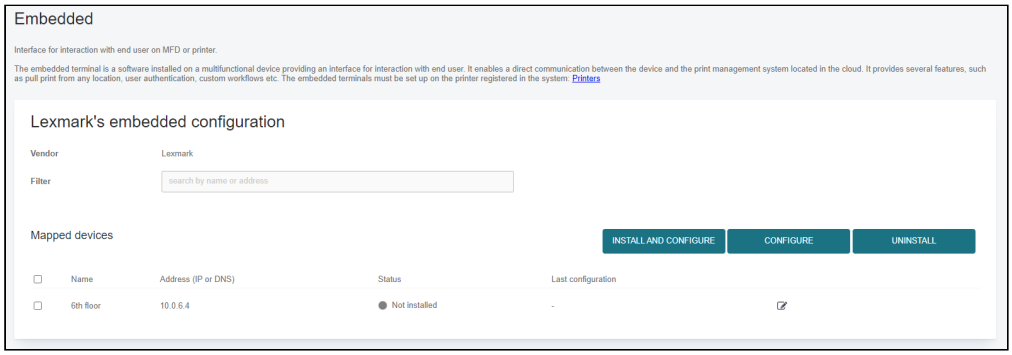
- Job list



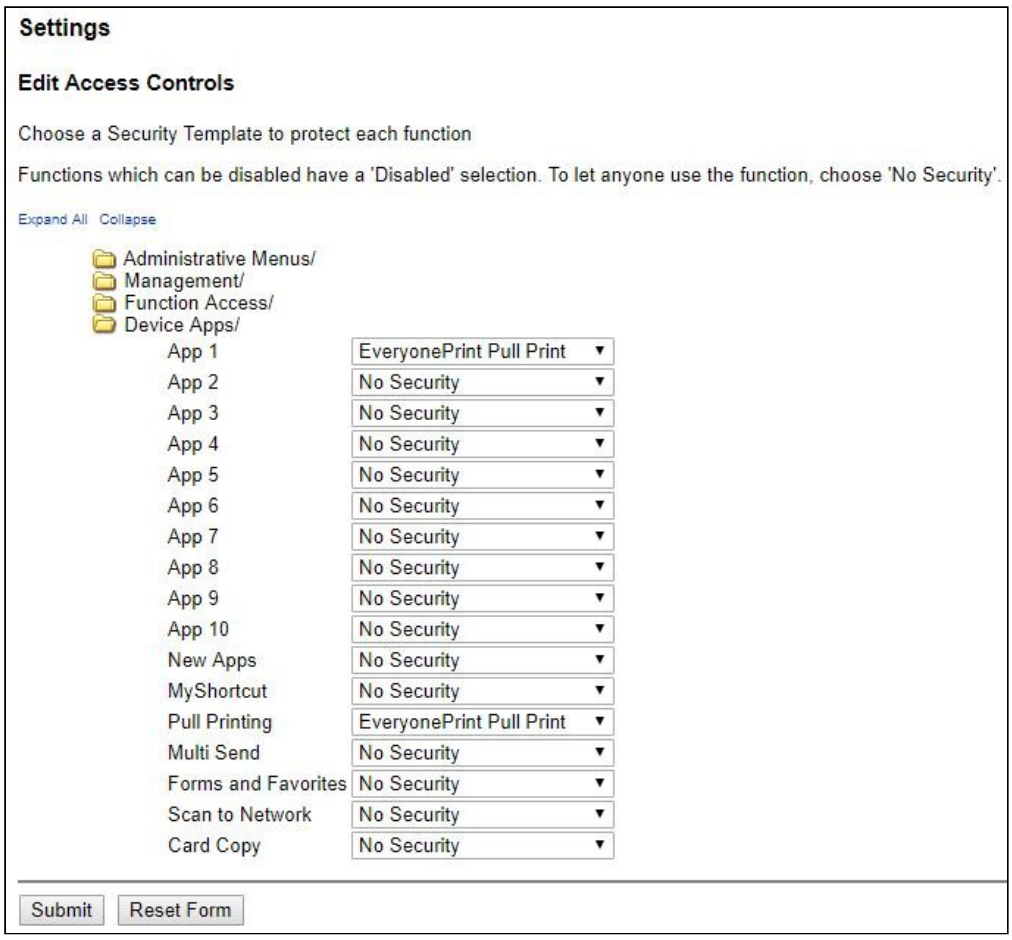
Lexmark Terminal

Before you begin, make sure that your gateway is configured according to Secondary Gateway mapping.

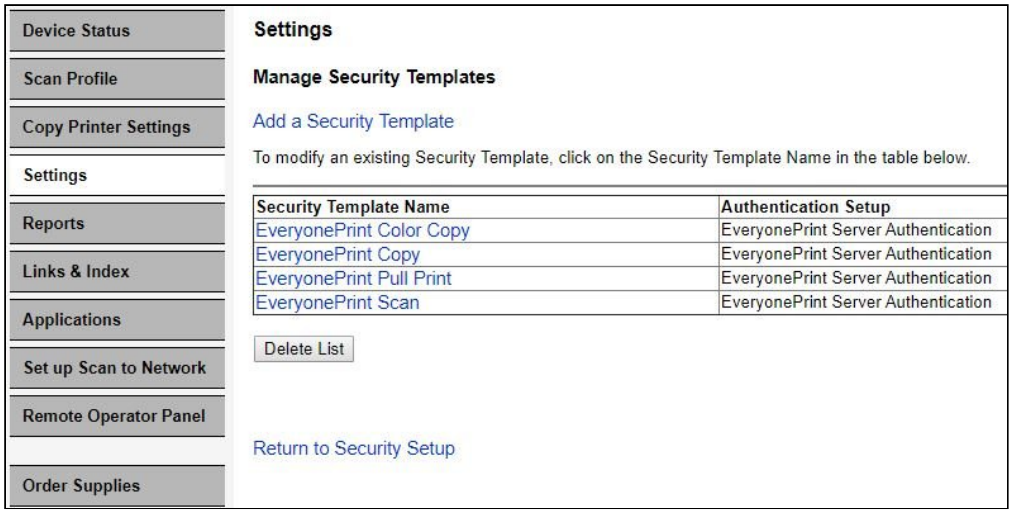
After setting up the printer on the network and configuring in SAFEQ Cloud, push out the Embedded configuration from embedded screen found in SAFEQ Cloud Web UI **Printers** > **Embedded templates** tab and clicking deployment action icon.



On some models you need to do a change in "Access Control" for setting the security on the MFD right.
Open MFD´s Web-interface in a browser and navigate through "Settings", "Security", "Security Setup", "Access Controls".
Expand "Device Apps" and set "Pull Printing" to "Y Soft Pull Print" and hit "Submit".



On some models you need to do a change in "Security Templates" for setting the security on the MFD right.
Open MFD´s Web-interface in a browser and navigate through "Settings", "Security", "Security Setup" and "Security Template".
Choose "Add a Security Template" and follow the guide to make all four Templates below.

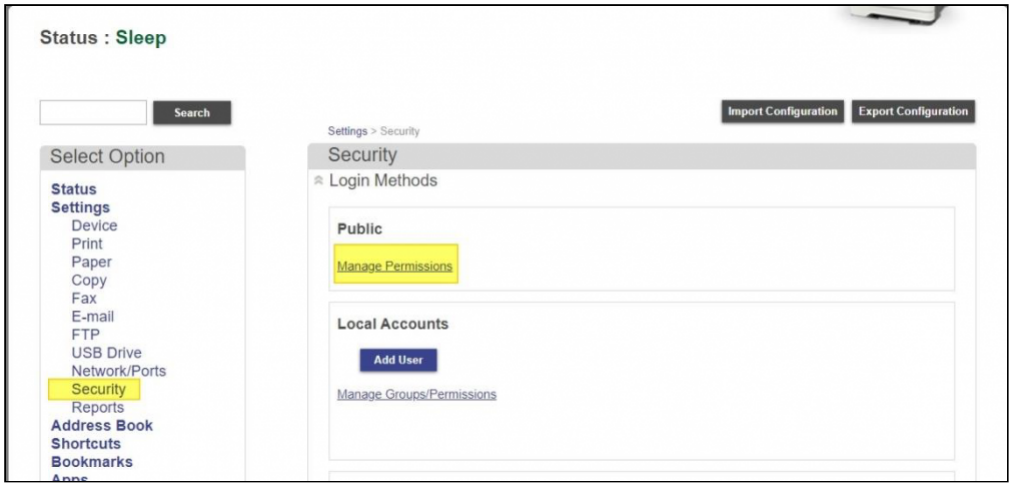


Here you see the configuration for the four Templates.

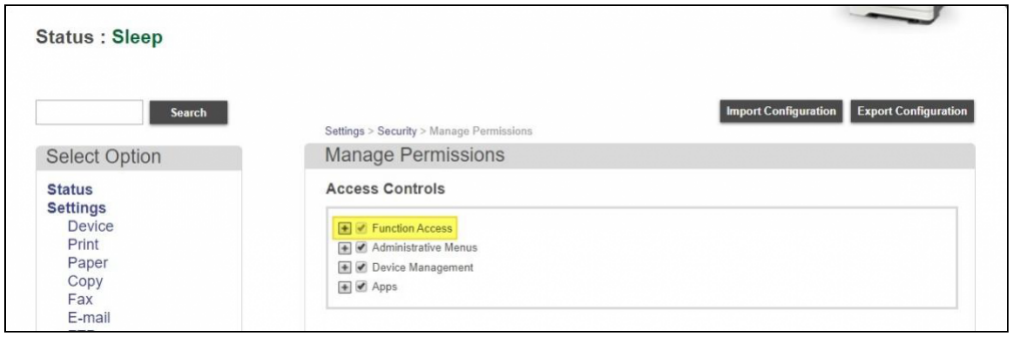
Security Template Name	Authentication Setup	Authorization Setup	Group authorization selection
EveryonePrint Color Copy	EveryonePrint Server Authentication	EveryonePrint Server Authentication	Color Copy
EveryonePrint Copy	EveryonePrint Server Authentication	EveryonePrint Server Authentication	Copy
EveryonePrint Pull Print	EveryonePrint Server Authentication	EveryonePrint Server Authentication	Print
EveryonePrint Scan	EveryonePrint Server Authentication	EveryonePrint Server Authentication	Scan

Security and Access Control on eFS6 models

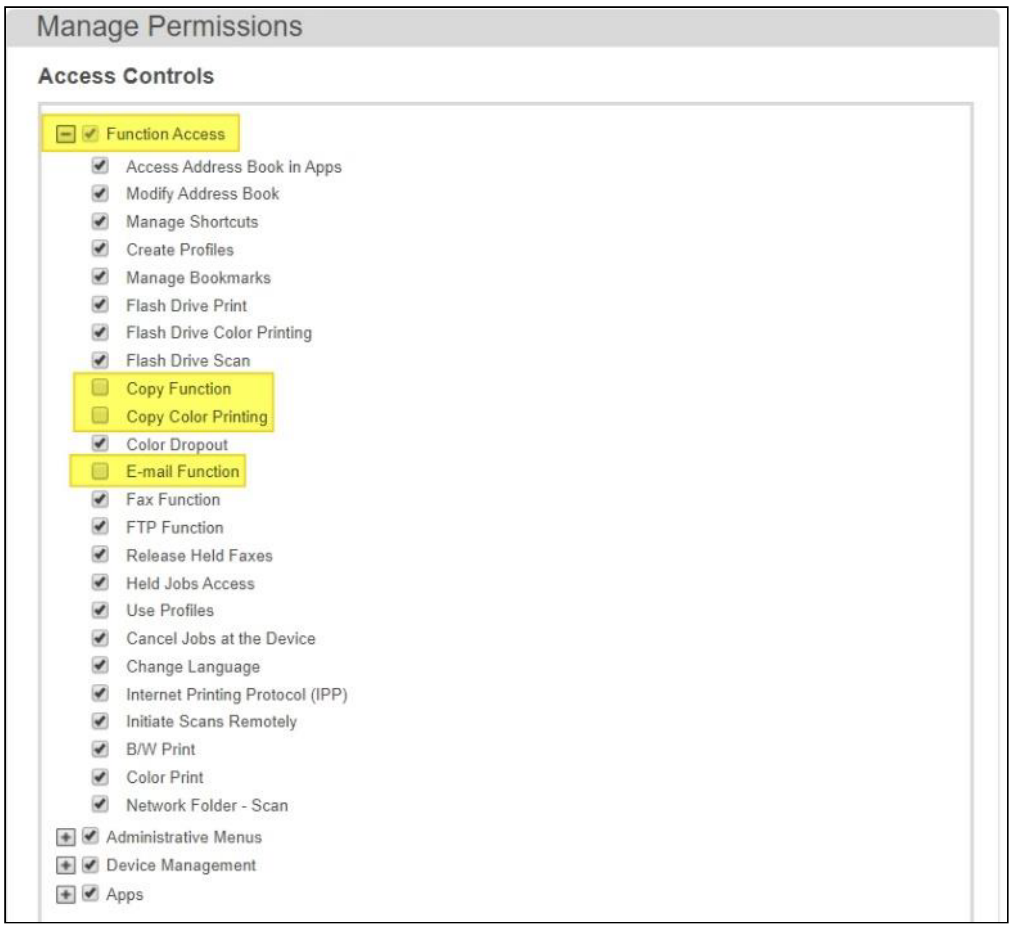
Logon to the device and select Security and Manage Permissions



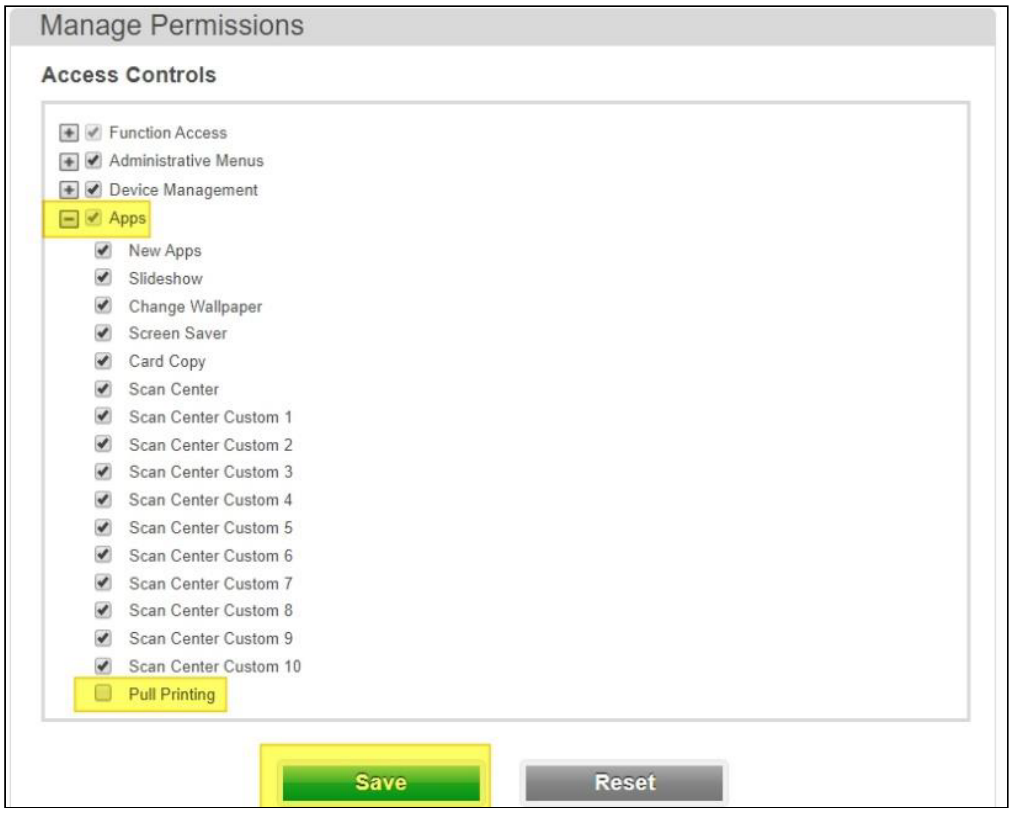
Select Function Access



Deselect Copy Functions, Color Copier Printing and E-mail functions.

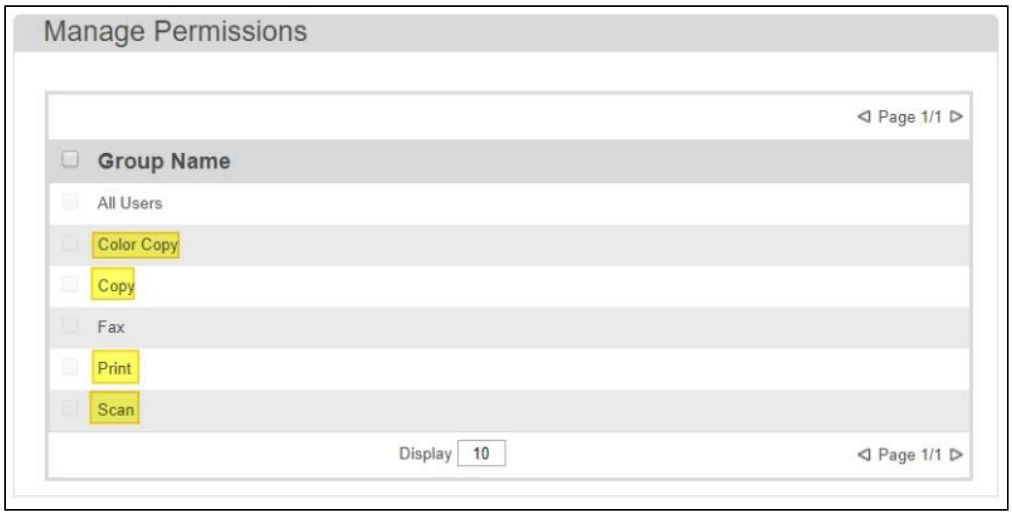


In Apps deselect Pull Printing

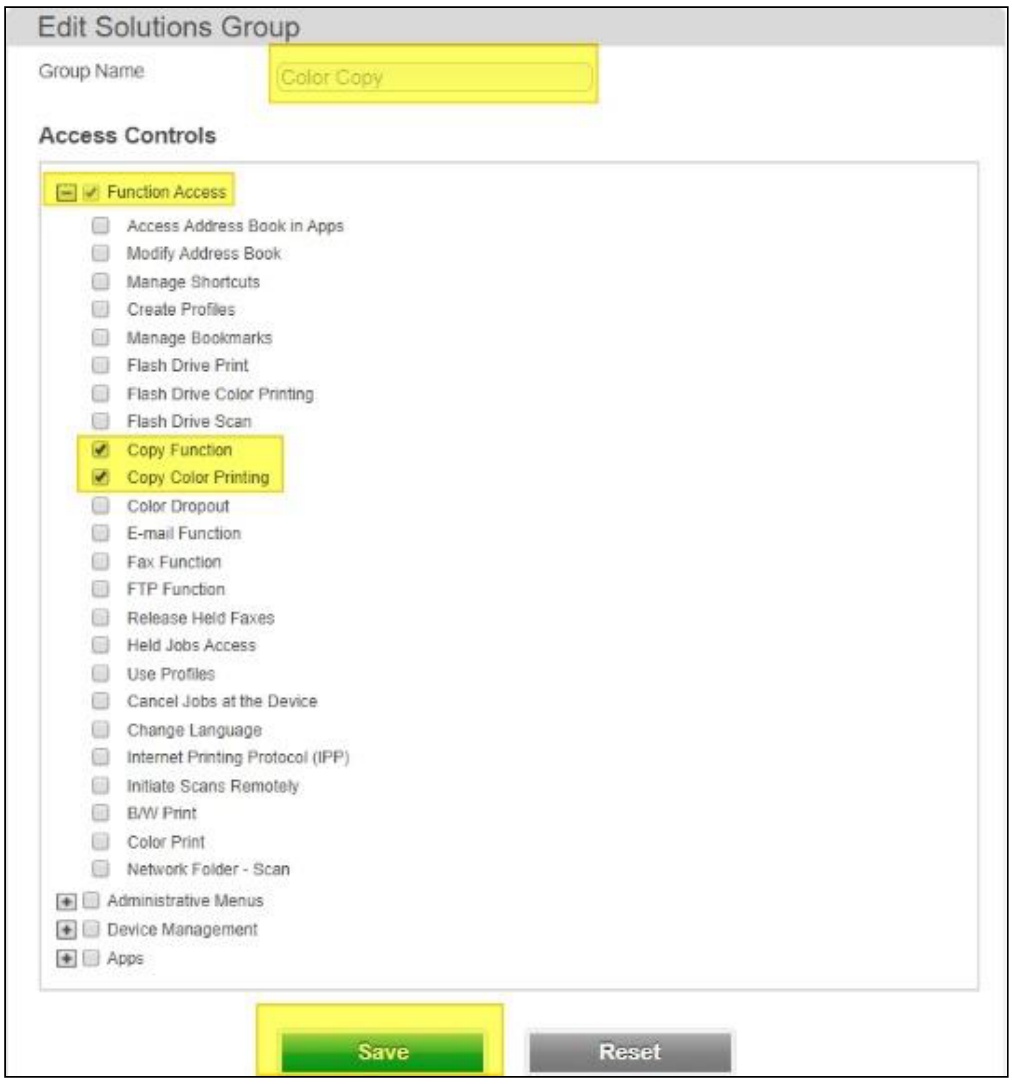


After selecting Save then go to Security and select Manage Permission, located right of the Y Soft Server Authentication

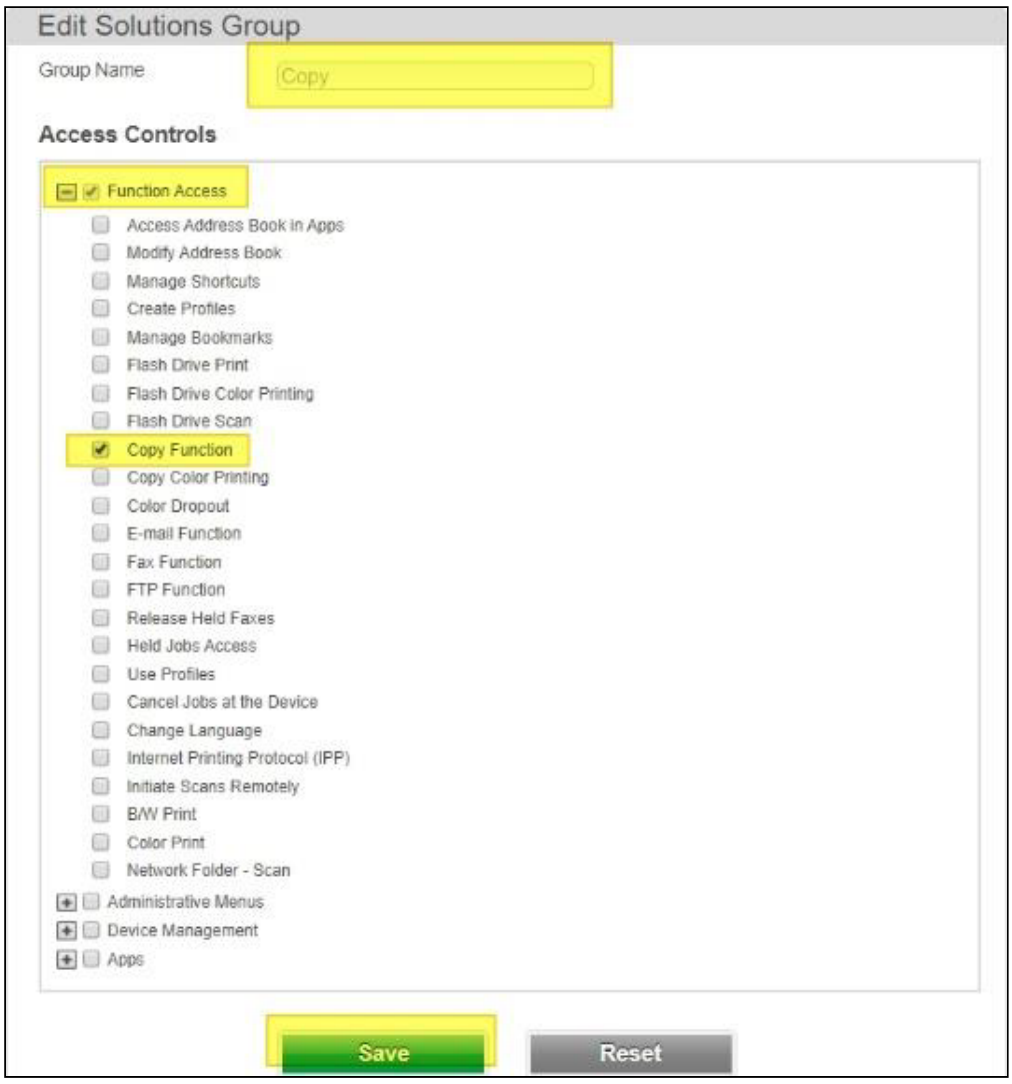
Here you need to modify, if required, the authentication for: Color Copy, Copy, Print and Scan



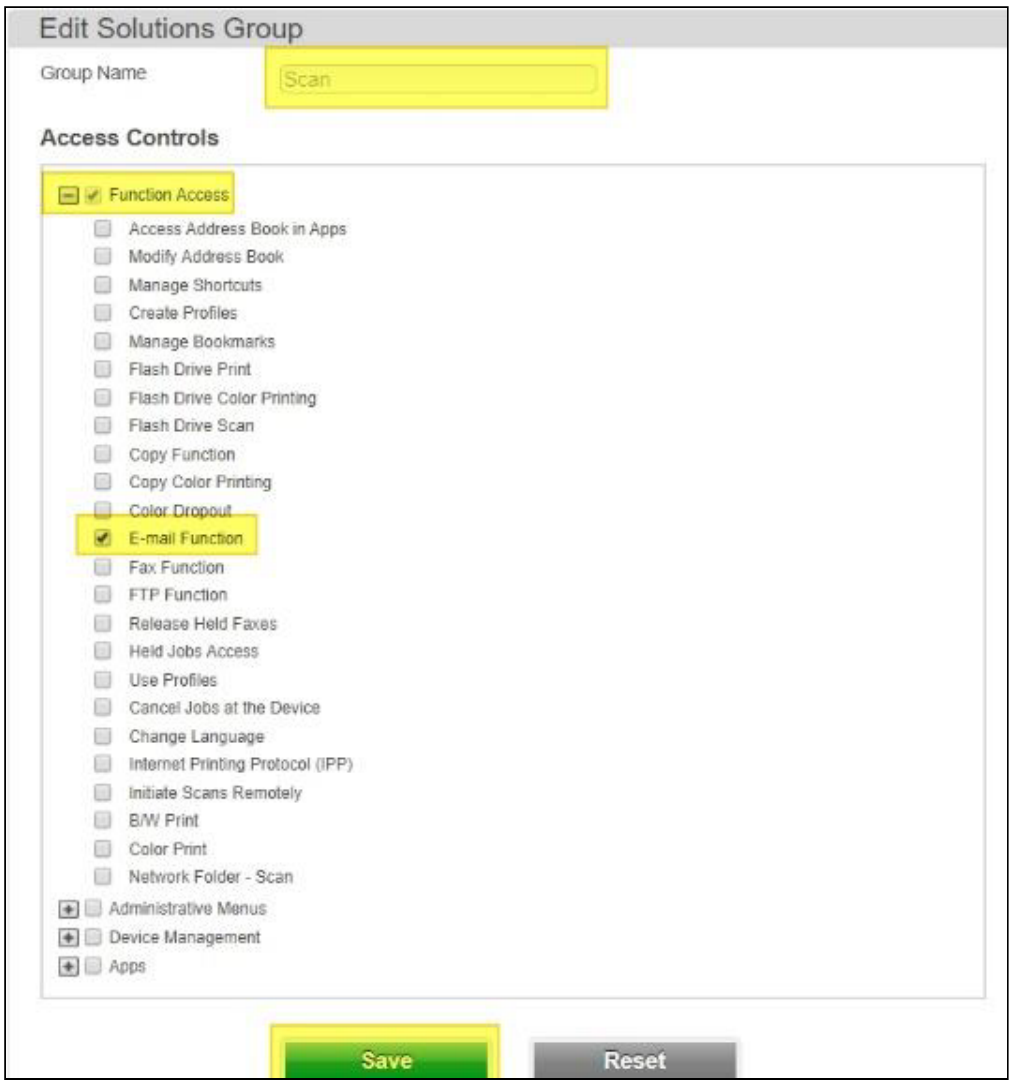
For the Color Copy, select Copy Function and Color copy Printing under Function Access and select Save



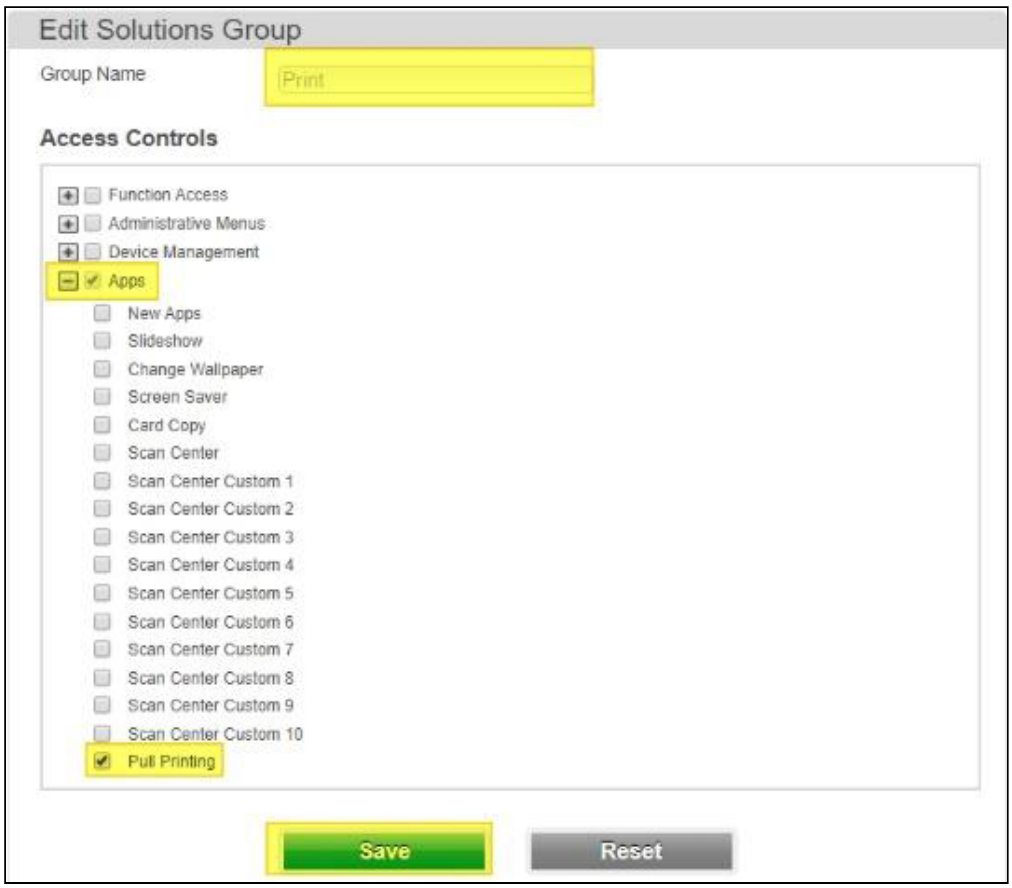
For the Copy, select Copy Function under Function Access and select Save



For the Scan, select E-mail Function under Function Access and select Save



For the Print, select Pull printing under Apps and select Save



Ricoh Terminals

Ricoh Standard Gen 2 Cloud Terminal

Note that this manual is for Ricoh Cloud Terminal which is in SAFEQ Cloud Web UI called Standard Gen 2. This terminal connects directly to the cloud. The first generation of Ricoh terminal can connect to the cloud only via a secondary gateway.

The following pages describe all the setup and installation steps. Perform them in the order in which they are listed.

1. Go through the requirements and limitations.
2. At the MFD, do the initial device setup.
3. In the SAFEQ Cloud Web UI, add Embedded configuration and Ricoh MFD.
4. Install the cloud terminal itself via one of the three available methods: Cloud Terminal installation. From these methods, only the installation from Ricoh App Store requires your presence at the MFD.
5. In the SAFEQ Cloud Web UI, register the Cloud Terminal.
6. In some cases, you must perform manual device configuration. For details, see Post-installation device setup.

Requirements and limitations

Requirements

- Make sure that you have Cloud Terminal Integration enabled (for information on how to do this please follow Enable Cloud terminal integration guide).
- Make sure that you have a signing certificate selected. To check this, log in to SAFEQ Cloud Web UI and navigate to Security > Security options > PKI and encryption. The Signing certificate field must not be blank.
- The server needs to use a certificate trusted by the MFD. If the server is not using a certificate signed by a publicly trusted authority, this means the Certificate Authority needs to be added to the trust store of the MFD. The deployment tool can be used for the import (see fetch-certificate command for import from SAFEQ Cloud in Terminal Deployment Tool, or see the CustomCA-README file located in <your deployment tool location>\certificates for custom CA creation and import).

  A certificate issued for an IP address will not be accepted by the MFD. The server must use a certificate issued for a domain name.
- Ports 8705 and 7400 must be opened for terminal communication.

Limitations

Authentication

- In WIM, if you change settings that require reboot or after you click Reset the machine, you must restart the MFD manually or via the Terminal Deployment Tool. Otherwise, functional problems with the device may occur, and while authentication at the MFD may not stop working immediately, it will eventually fail for end users.

Cloud print

- Only the following finishing options are supported: Color, Sides, Copies, Collation, Staple, Punch, Booklet, Input tray, and Output tray. This limitation applies to both the terminal and the triggers. Only Color, Sides and Copies can be modified on the terminal.
- If matching size is not available, printer prints job on available paper. This will result in job not being printed properly.
- Optimized print delivery is used to release print jobs locally without transferring them through the cloud, if allowed by network visibility. Optimized print delivery has the following limitations:
  - Print progress during an optimized print delivery is not supported.
  - If a problem with the MFD occurs during an optimized delivery, such as paper jam, no print error message will be visible.
- When a user submits a duplex job with landscape orientation from the Mobile app or legacy mobile print, the short-edge / long-edge setting is reversed.
- If the MFD goes offline while a print job is waiting, it will display a notification regarding the print job status within a 20-minute window.
- Username and filename are not filled in on the native Job History screen.
- When a custom print driver is used, finishing options selected on the terminal do not have to be applied.
- Processing large PDF documents may not be possible on devices without sufficient memory. Devices may become stuck while downloading the job, and a PDL error can occur after an extended period. Workarounds:
  - Print via a secondary server that has network visibility to the MFD.

- Print via a SAFEQ Cloud Client with network visibility to the MFD, using local storage mode.
- Print via the Mobile app.
- Submit the print job from a Mac workstation.
- Submit the print job as an image (e.g., using Adobe Reader).

Scan

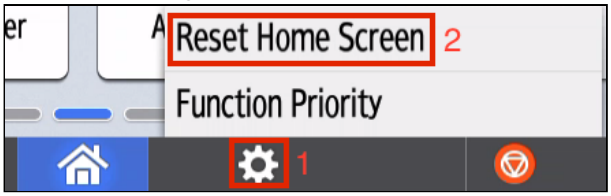
- Scan Workflows with **JPEG** output format will result in a **TIFF** output file if the color was set to **Black and White** or the color was **Auto** and the MFD detected a black and white document.
- **Email** method scan file size is limited to 18MB. If the scan file size is over, the email is not delivered. There is no extra notification of such an event.
- The scanned document is lost if the device is powered off before scan delivery completion.
- If you modify a scan workflow that is currently being used by a user at the MFD, the scan workflow will be started with the original settings. To apply the new settings, the user must close and open the Scan application or log out and log in again.
- If the MFD's HDD is full, an error message or "Upload unsuccessful" message may not appear.
- Date picker dialog: An incorrect month/year may sometimes be displayed above the calendar view in the dialog window when the default is not a valid date.

Accounting

- G2 scan and copy jobs are accounted for in batch. Reports include one job for every started scan with 0 pages and one additional job with all pages done during a user session.
- At the latest, G2 scan and copy jobs are accounted for during the user's next login.
- Precise print job accounting, eg. when a job is canceled by the user and only printed pages are accounted for, is not supported on G2 devices (all devices with SmartSDK version older than 3).
- Precise direct print may currently be accounted twice, precise direct and push print may be accounted under the last authenticated user (this will be removed in a near future)
- USB Print accounting is not supported on G2 devices (all devices with SmartSDK version older than 3).

Shortcuts

- Application shortcuts are not automatically recreated once you have manually deleted them. Reset the user-specific home screen to display them again. You might want to prevent changes to shortcuts by setting **Device Management** > **Configuration** > **Screen** > **Screen Device Settings** > **User's Own Customization** to **Prohibit** in WIM.



Localisation

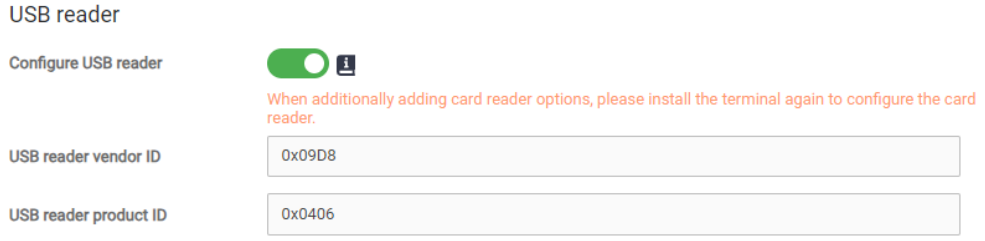
- Right-to-left (RtL) languages are not fully supported.

Adding Embedded configuration and Ricoh MFD in SAFEQ Cloud Web UI

Before you begin, prepare the serial number of the MFD that you wish to add.

Creating the Embedded configuration

1. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
2. If not done already, create an embedded configuration for Ricoh by clicking **Add**.
3. In **Vendor**, select **Ricoh**.
4. In **Application Type**, select **Standard Gen 2**.
5. Optionally, enable **Configure USB reader** to set up the card reader and perform the following steps (set to disable to leave the card reader configuration untouched for future installations):

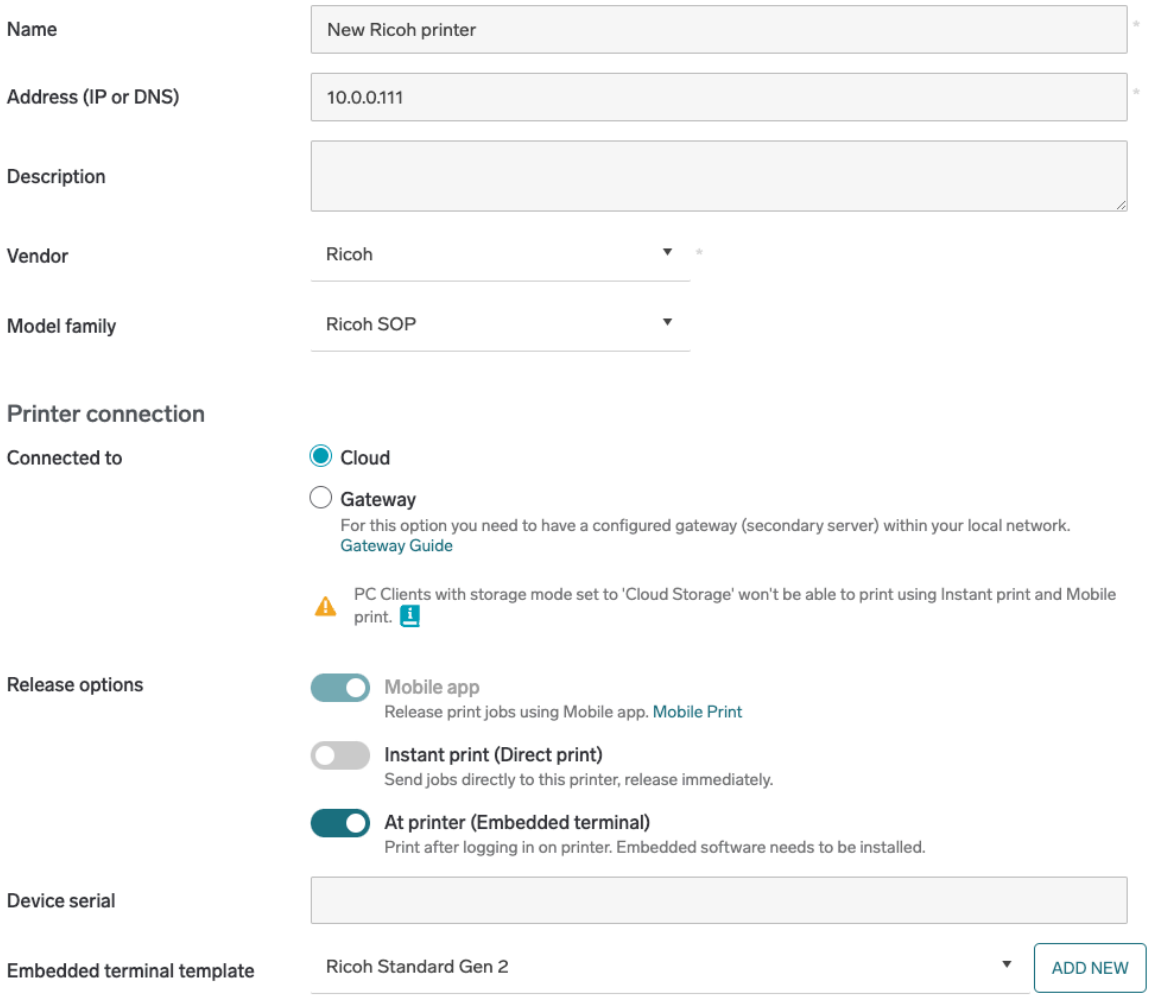


   a. Enter its VID and PID in the configuration, in HEX format, with or without the 0x prefix.
      1. Please see Compatible Card Readers for the values.
   b. Click **Install and Configure** in the embedded menu (if applicable due to network visibility).
   c. Or Click **Manual operations** in the embedded menu.
      1. Make sure the VID and PID values are explicitly specified in the respective command parameters
   d. Beware that until the terminal is installed or reinstalled, changes are not propagated.
   e. If you reinstall, there is no priority for the installation options - the card reader configuration specified last will be applied.
   f. When installing the terminal by other means (directly through Web Image Monitor), the USB reader must be configured manually.

6. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.

Adding the MFD

1. Go to **Printers** tab.
2. Click **Add**.
3. In **Vendor**, select **Ricoh**.
4. In **Model family**, select **Ricoh SOP**.



5. Fill in all required information.
6. Click **Save**.
7. Proceed to Cloud Terminal installation. You will have a choice of three installation methods.

Cloud Terminal installation

You can install the terminal in the following ways:

- From SAFEQ Cloud Web UI
- From Ricoh Application Site
- Manually via the Terminal Deployment Tool

Installing the terminal from SAFEQ Cloud Web UI

Prerequisites

- This installation method requires you to have SAFEQ Cloud secondary server (Gateway) in your network. The terminal can only be installed from the secondary gateway because of network visibility to the MFD.

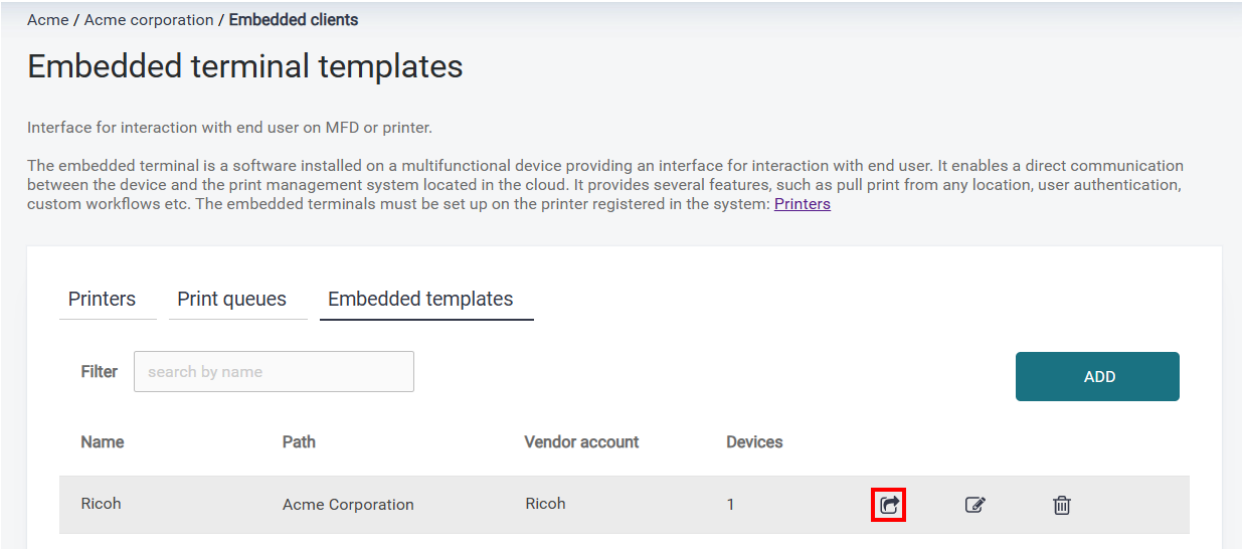
- Your secondary server has the Terminal client service created, and the service has Cloud terminal integration enabled.
- You have already created Ricoh embedded configuration and added your Ricoh MFD according to Adding Embedded configuration and Ricoh MFD in SAFEQ Cloud Web UI. When adding the MFD, in the **Client Terminal Services** and **Service** drop-down menus, you must select services running on your secondary server.
- In your embedded configuration, the **API key for installation** field must not be empty.

Limitations

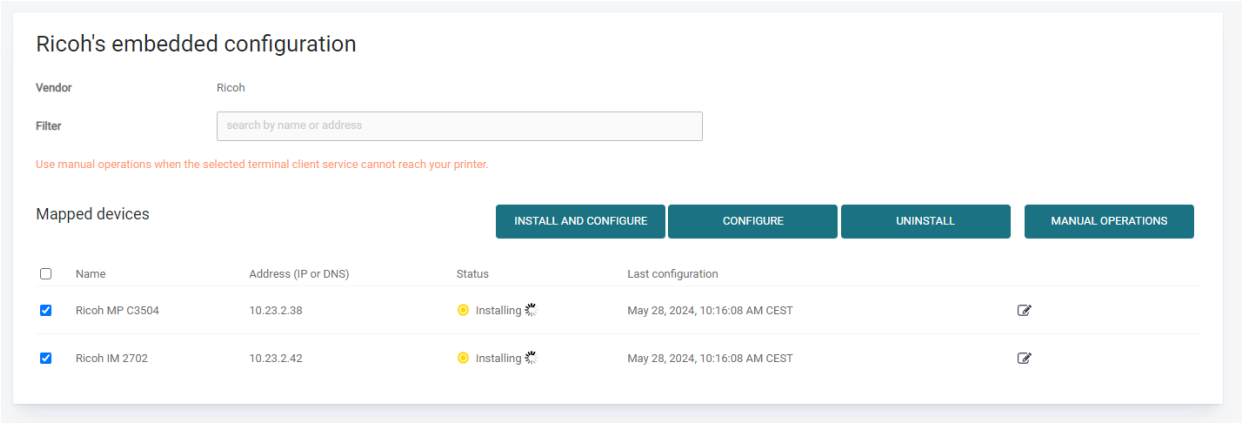
- Terminal installation status messages are not localized
- If the terminal configuration fails, you must click **Configure** to run it again.
- The installation implicitly trusts any device specified in the printer address field. Make sure you are installing only in case you are aware of what device is on that IP address. To prevent MFD admin credentials and API Key leakage, make sure that you know which device is on the specified IP address before you run the installation.
- If you want to upgrade to the Ricoh Cloud Terminal from the Ricoh Embedded with Application Type Standard, or any other kind of Ricoh terminal, you must first uninstall the old terminal so that you can run a clean installation of the Cloud Terminal.

Installation

1. Go to **Printers > Embedded templates** and click the icon next to your Ricoh embedded configuration to open the configuration.



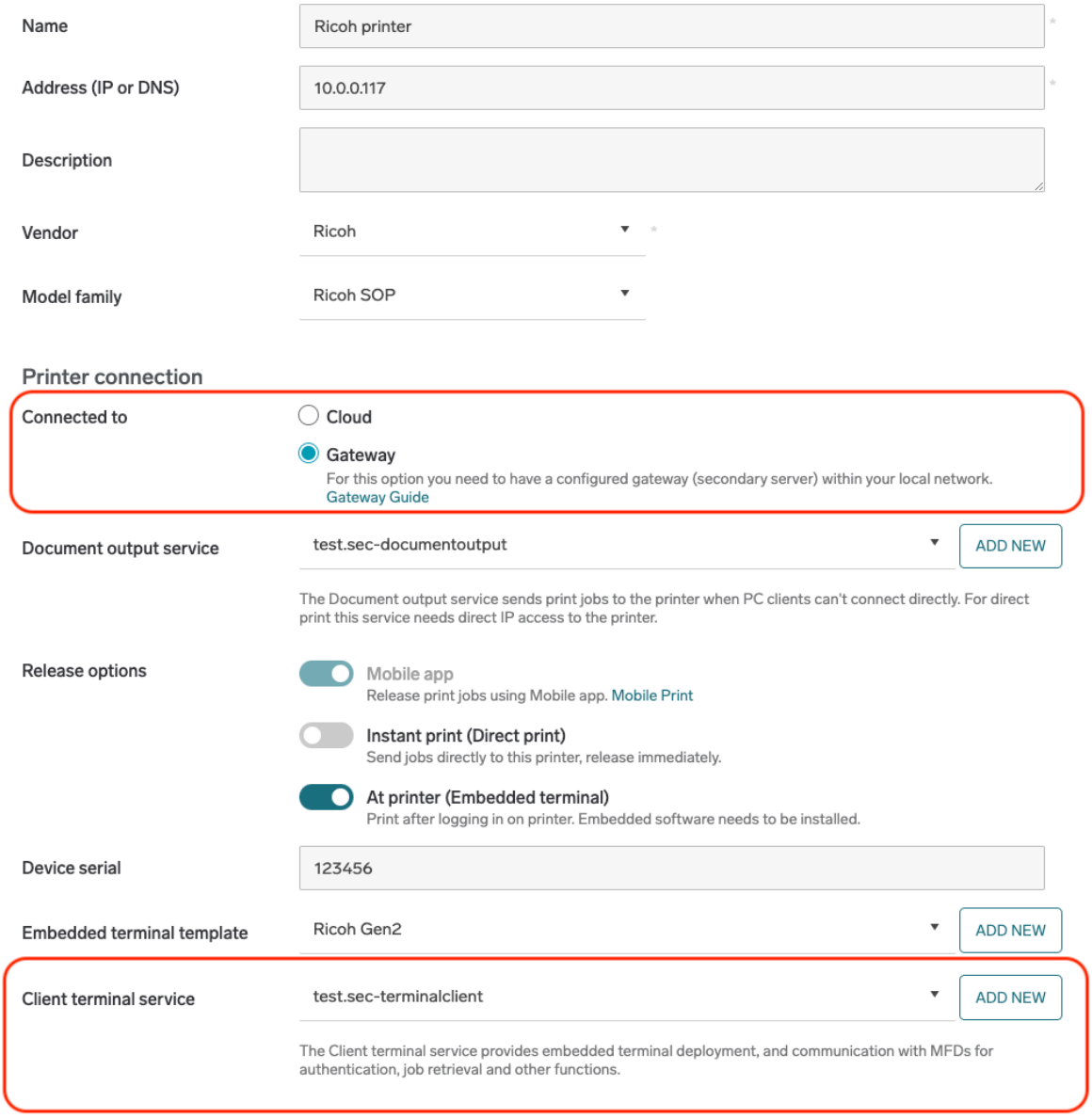
2. Select all MFDs where you want to install the Cloud Terminal.
3. Click **Install and configure**. The status will change to *Installing*.



4. When the installation finishes, the status will change to *Installed*.
5. If you see the error message "Failed to configure SP options" or "Failed to configure card reader. Please refer to documentation for manual configuration," you must configure the MFD manually. See Post-installation device setup.

Terminal-to-server communication

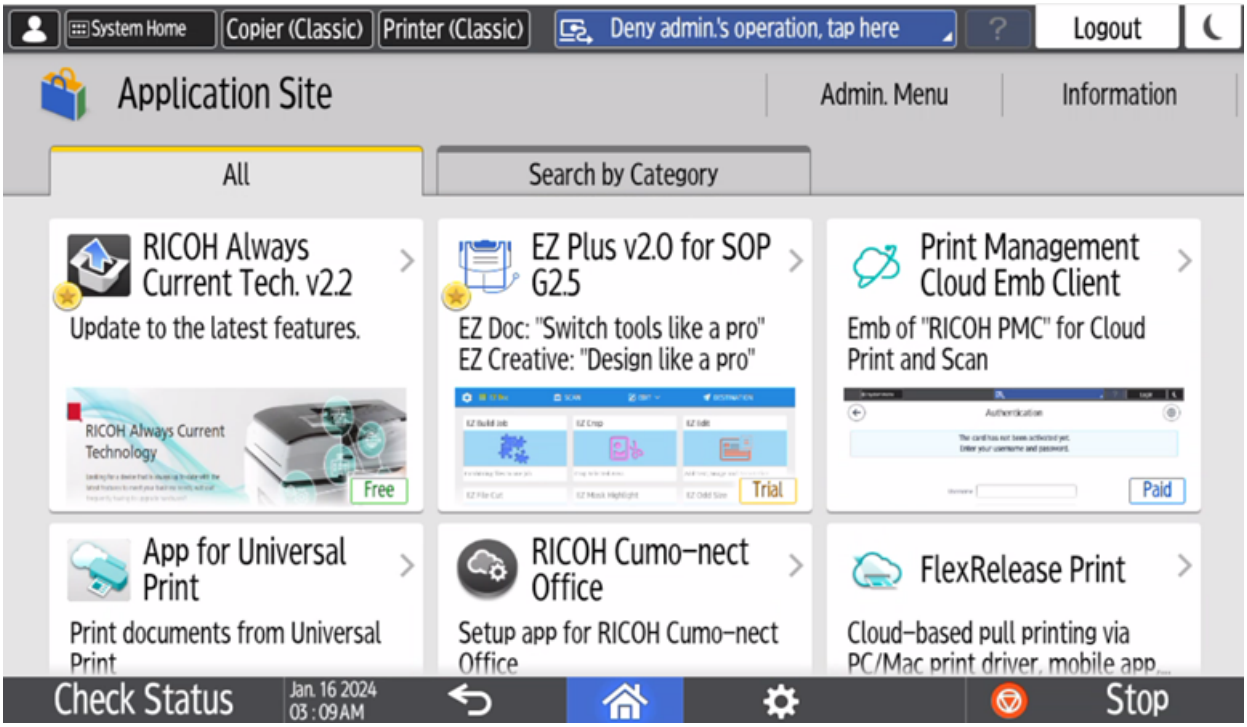
By default, the installed Cloud terminal communicates with the server specified in the Client Terminal Services field. To configure this, go to the **Printers** page > **Printers** tab, edit a printer, and navigate to the **General setup** tab in the SAFEQ Cloud Web UI.



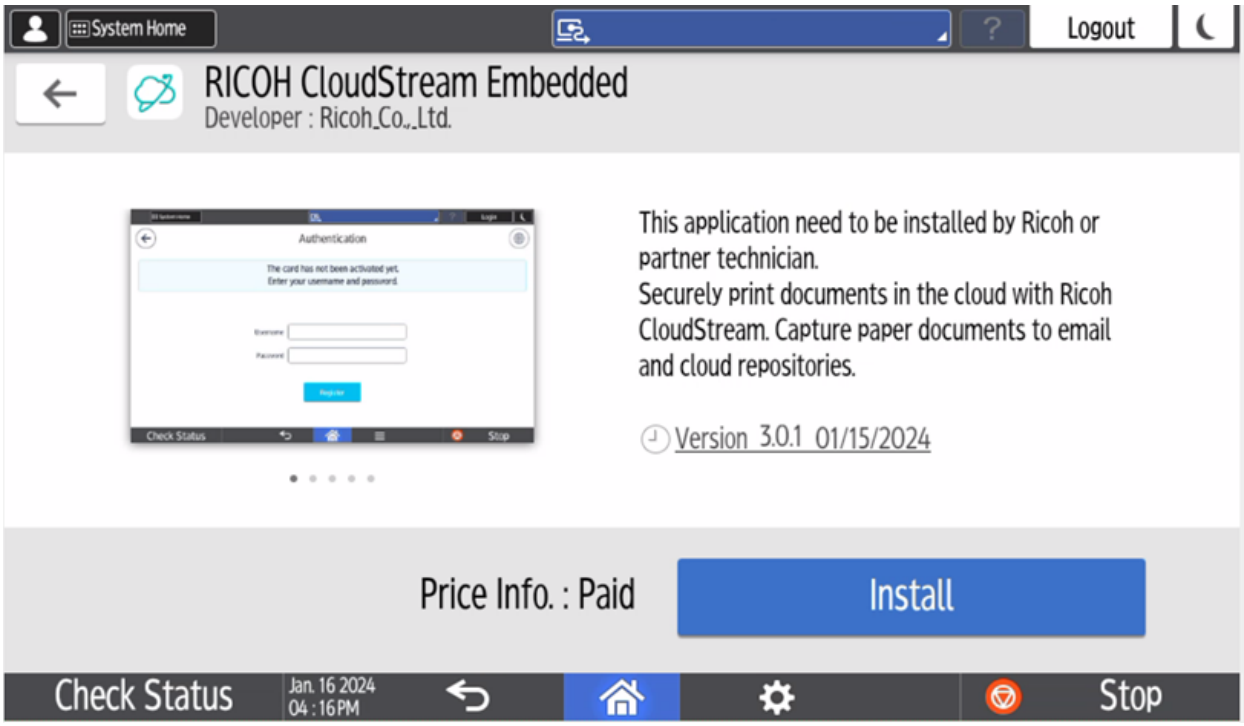
Installing Ricoh Cloud Terminal from Ricoh Application Site

Please note that this application needs to be installed by Ricoh or a partner technician.

1. At the MFD, navigate to the **Ricoh Application Site**.
2. Select **Ricoh Print Management Cloud** application.

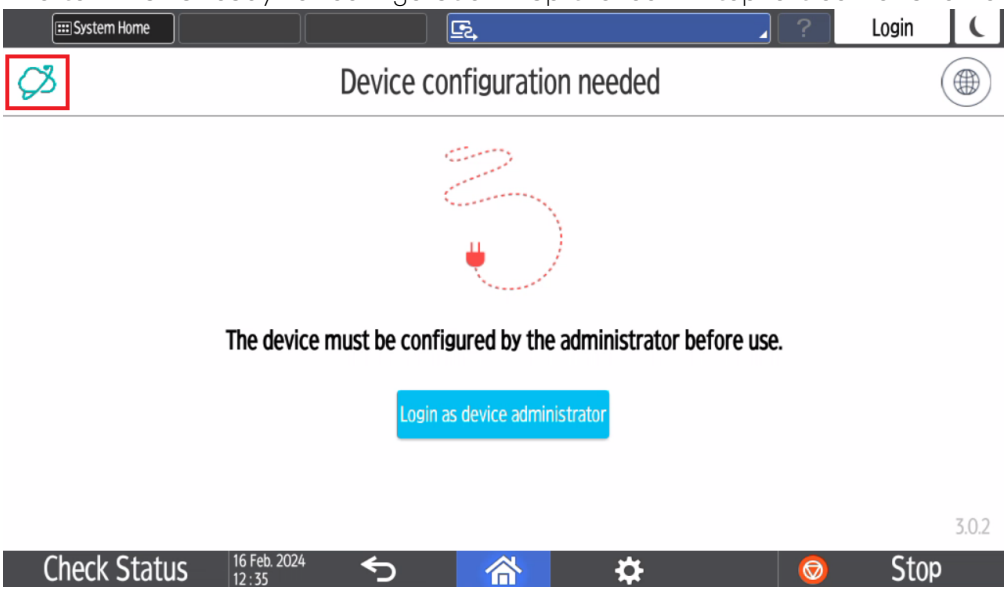


3. Tap **Install**.

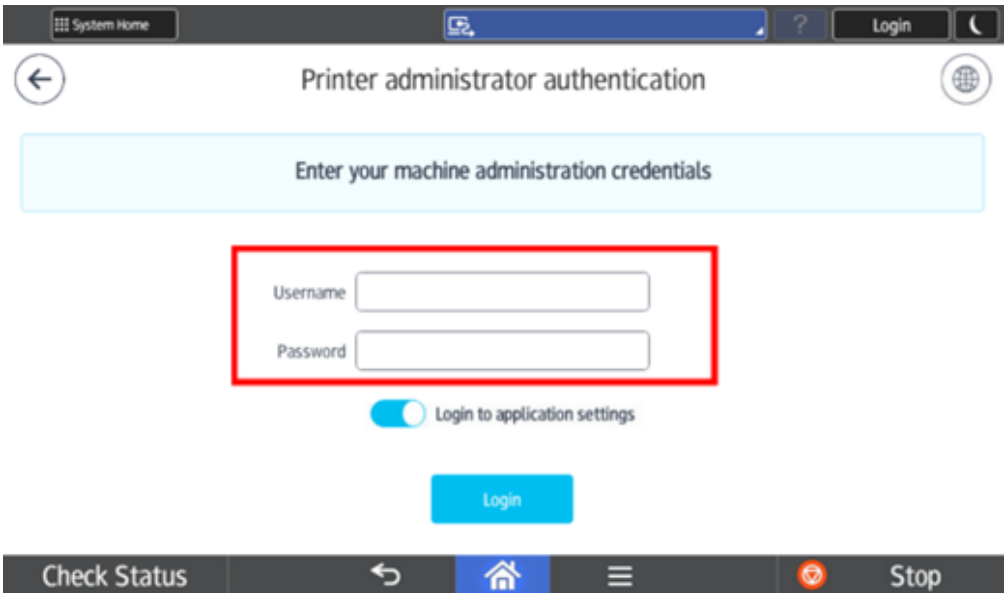


4. After the installation, please make sure device settings are set according to the Initial device setup.

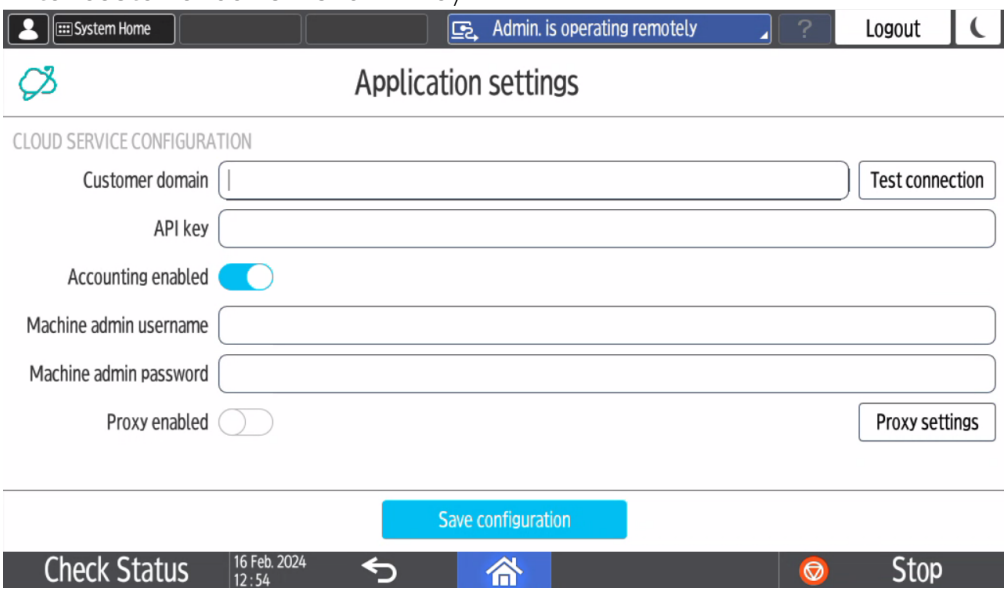
5. The terminal is ready for configuration. Tap the icon in top left corner and hold for 5 seconds.



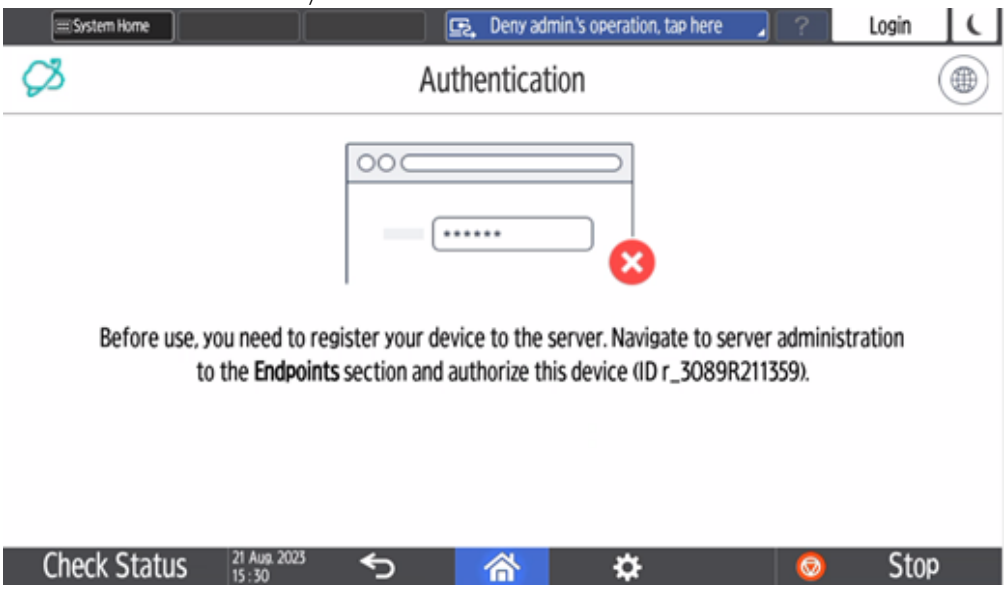
6. Enter the device administrator credentials.



7. Enter customer domain and API key.



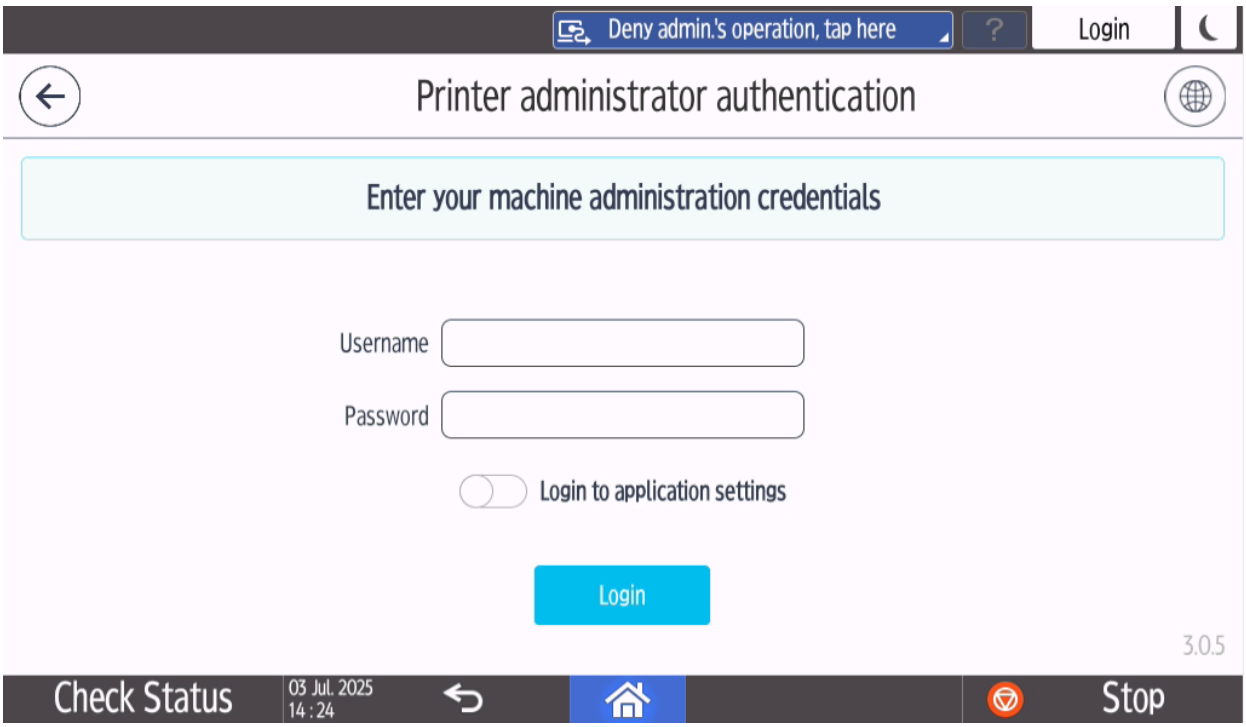
8. The device is now ready to be authorized.



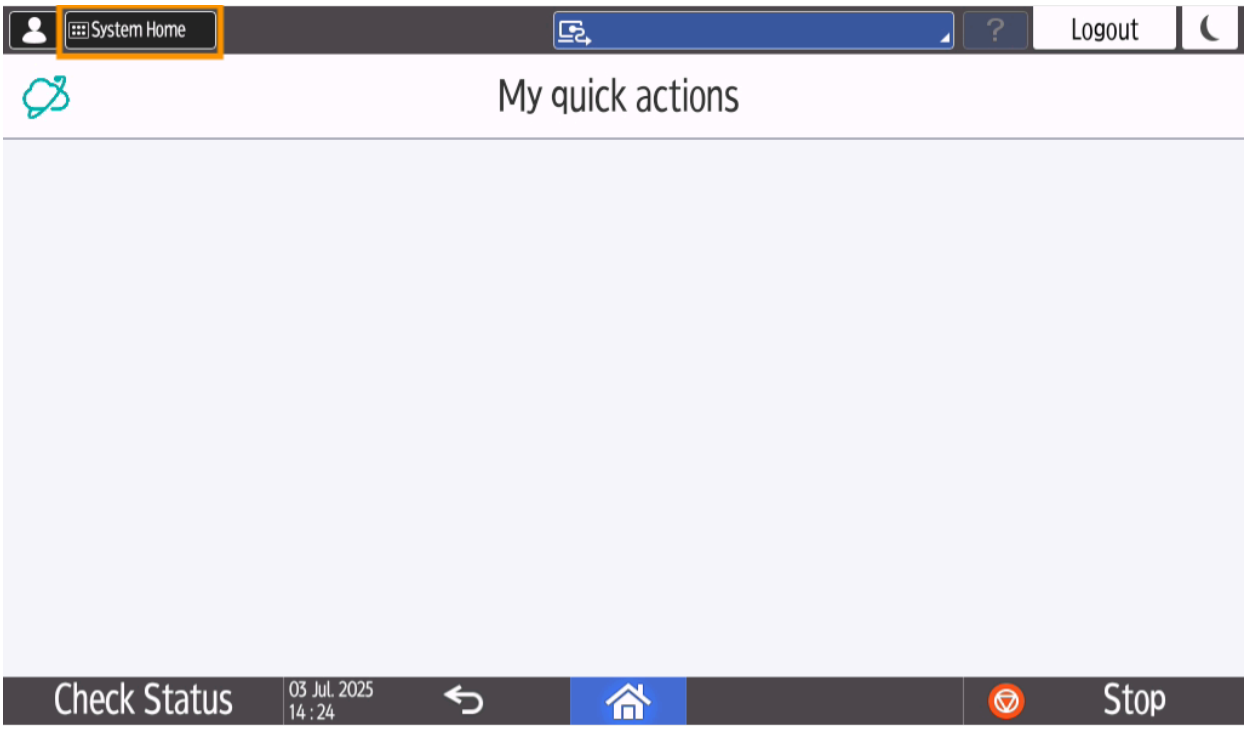
9. Proceed to registering the Cloud Terminal in the SAFEQ Cloud Web UI. This is described on the Registering the Cloud Terminal in the SAFEQ Cloud Web UI page.

Configuring auto update in Ricoh Application Site

1. Hold down logo in the upper left corner for 5 seconds.
2. Login as machine administrator.

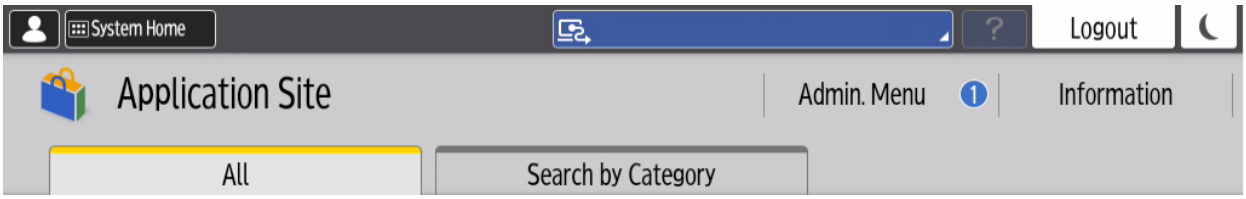


3. Go to the system Home screen.

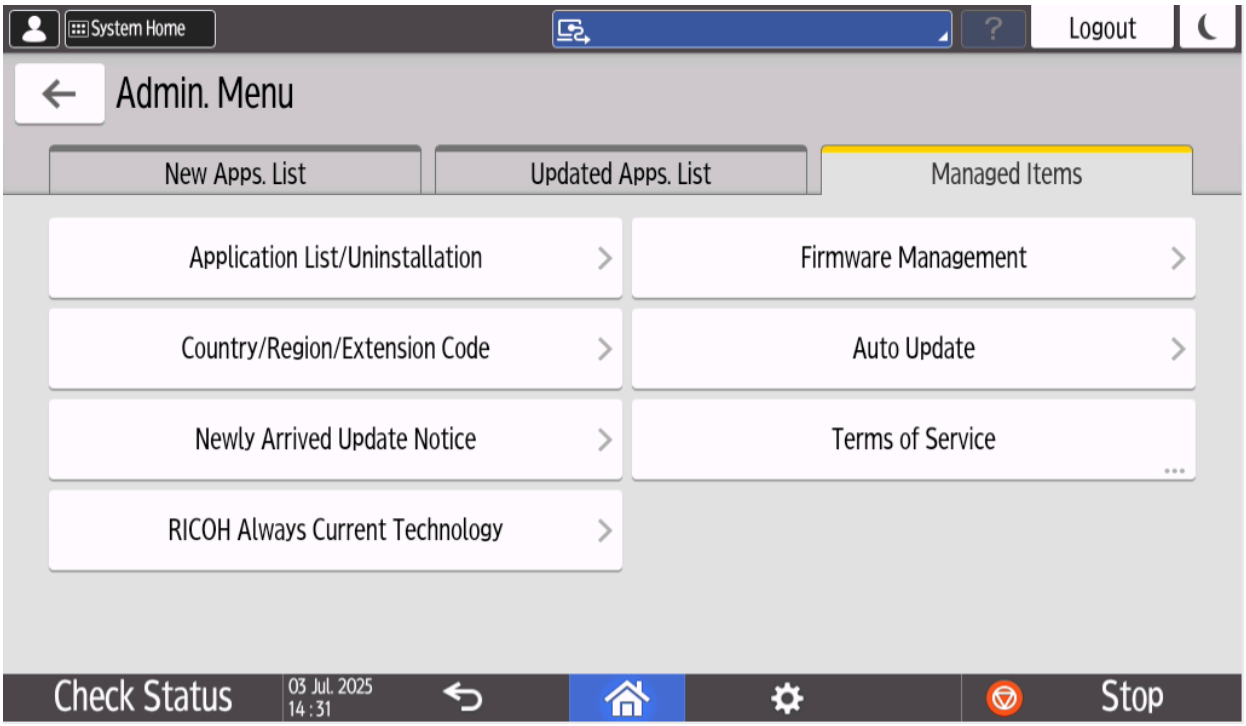


4. Open Application Site.

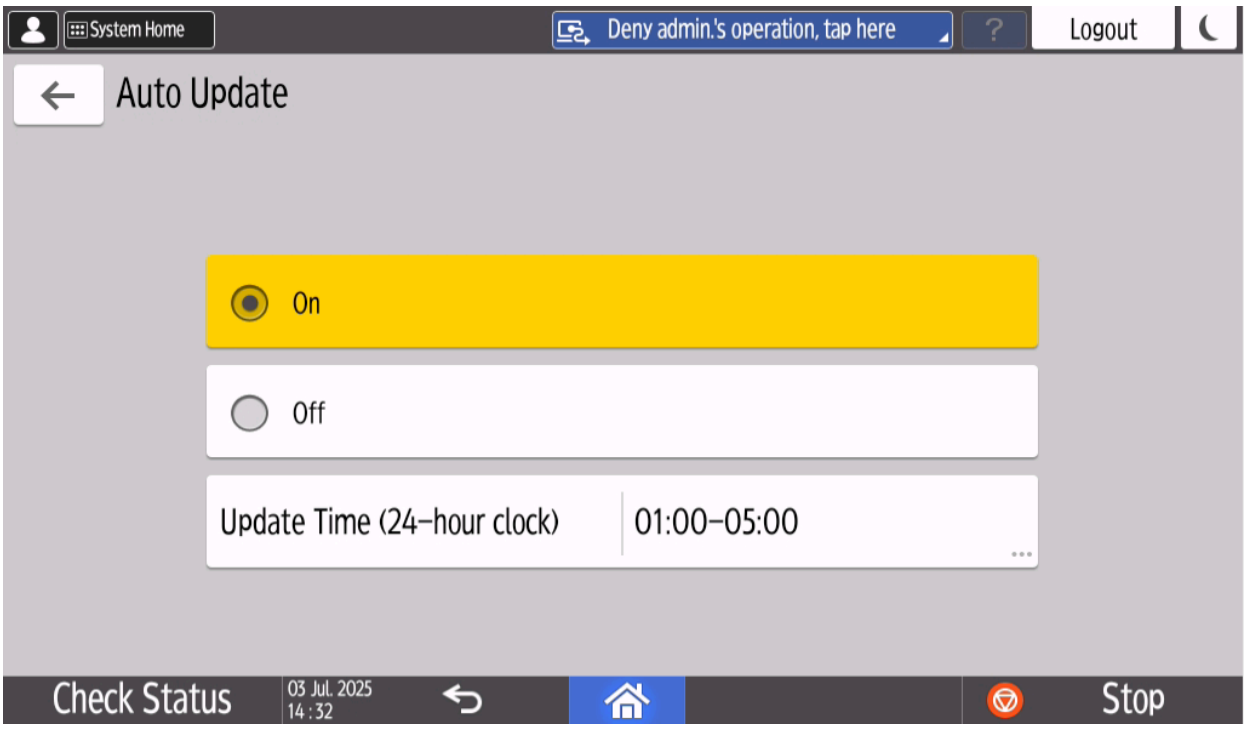
5. Open **Admin. Menu**.



6. Go to **Managed Items** tab and select **Auto Update**.

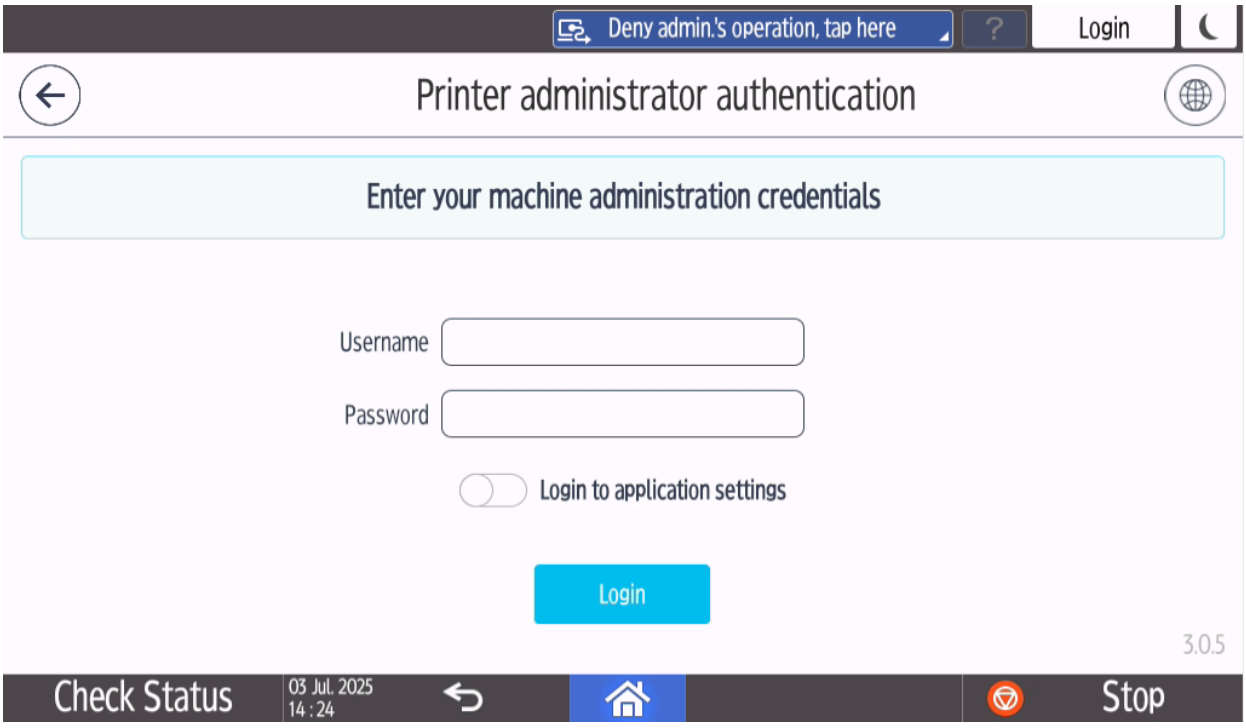


7. Configure the Auto Update according to your needs.

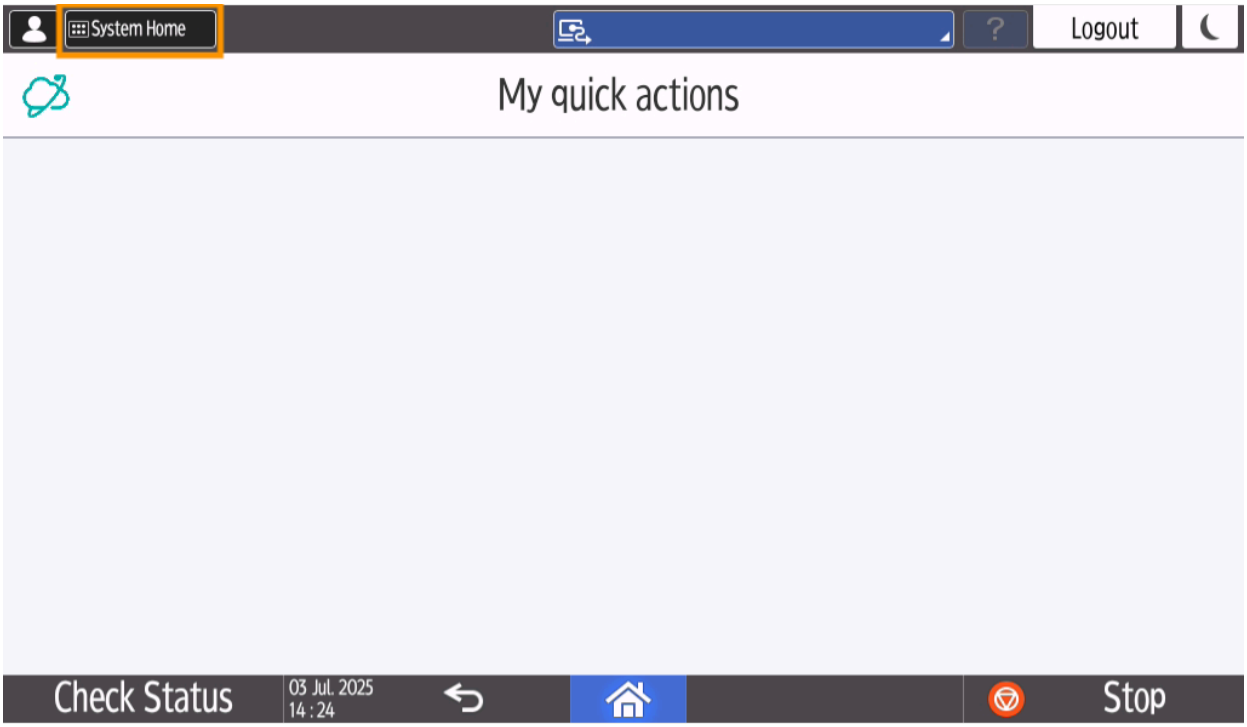


Updating Ricoh Cloud Terminal through Ricoh Application Site manually

1. Hold down logo in the upper left corner for 5 seconds.
2. Login as machine administrator.

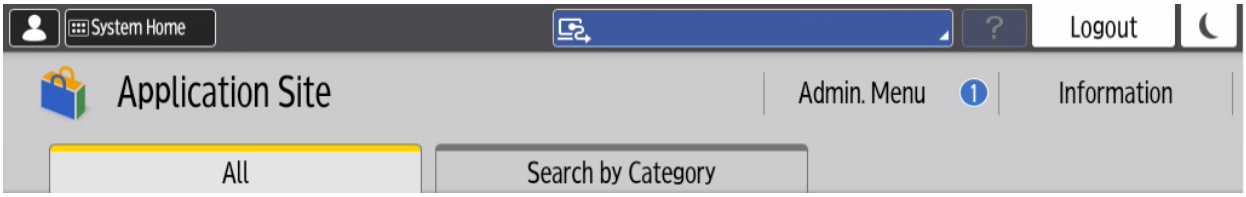


3. Go to the system Home screen.

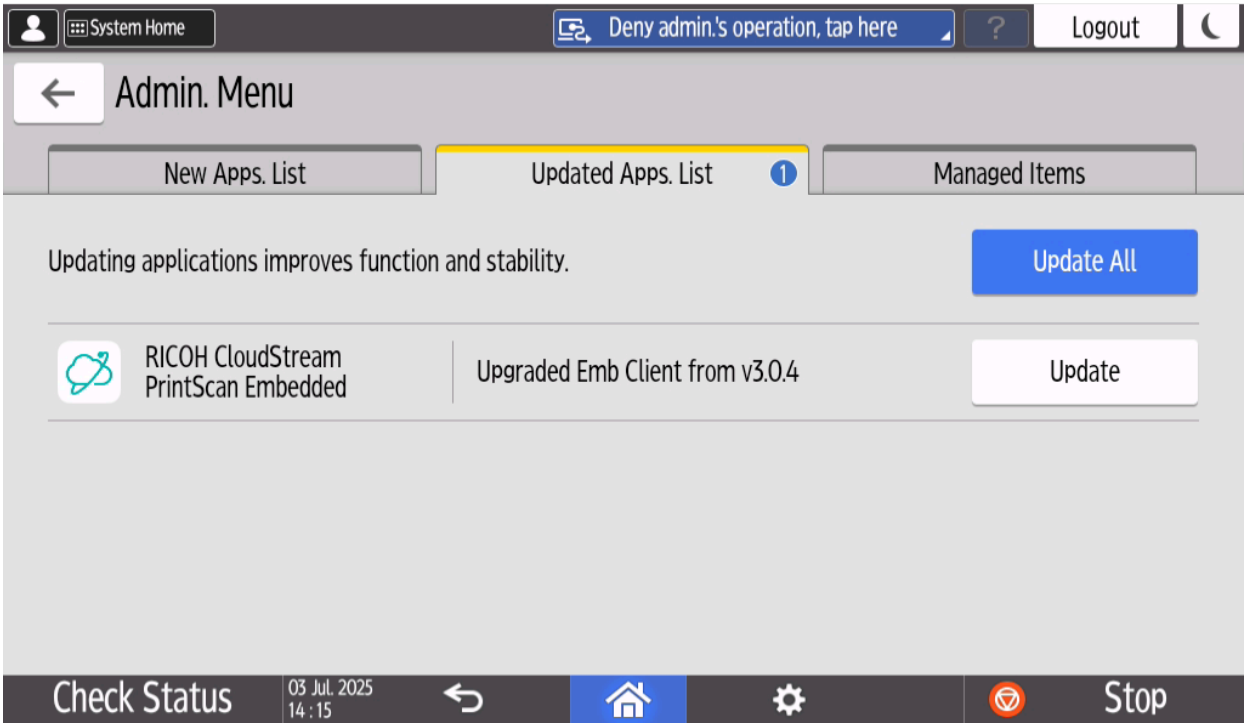


4. Open Application Site.

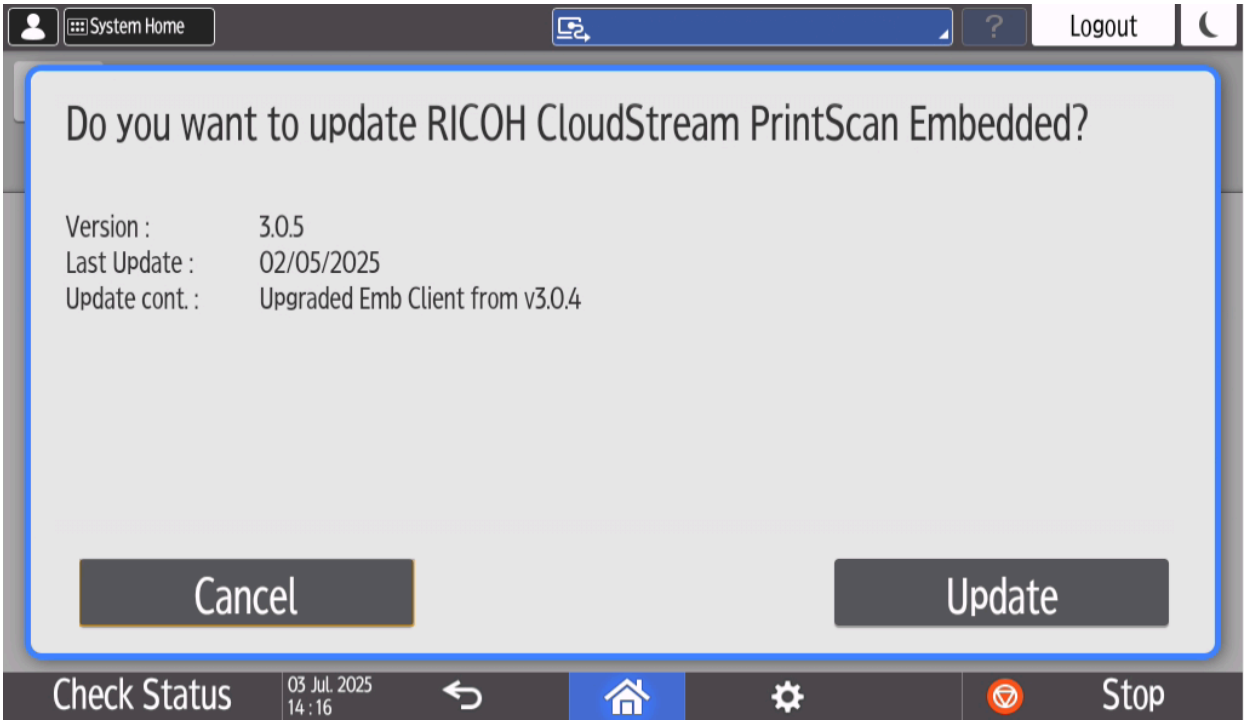
5. Open Admin. Menu



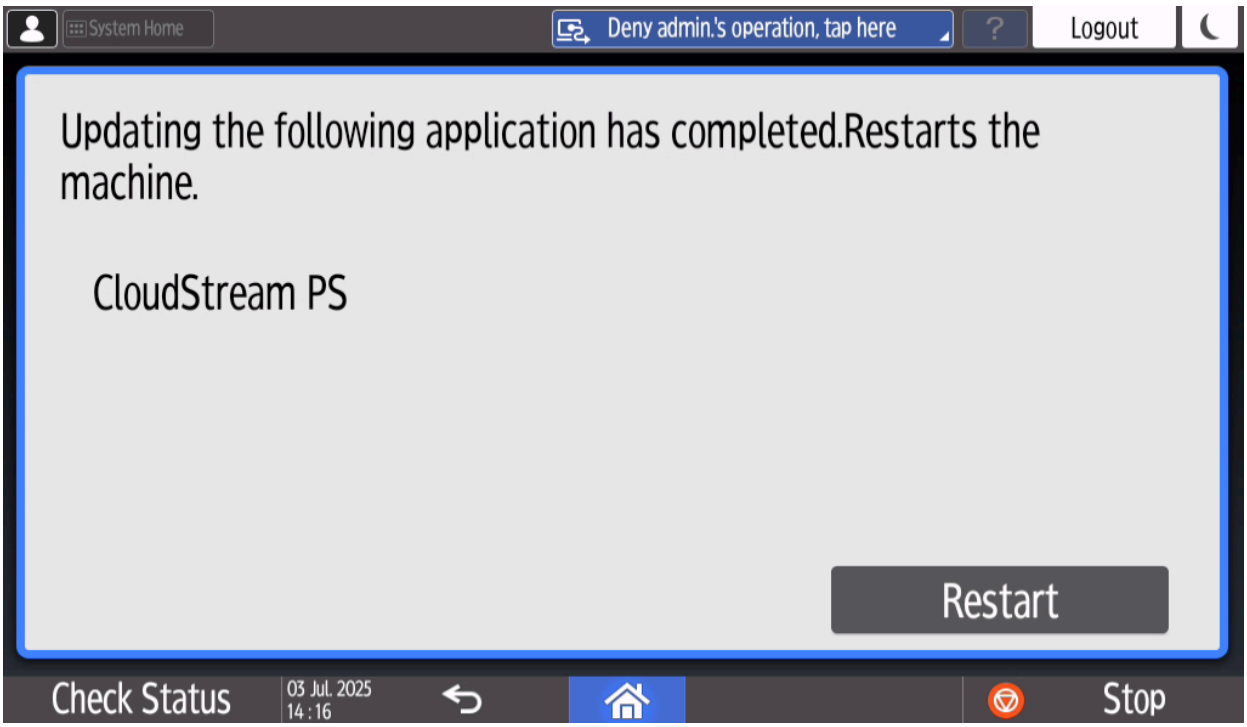
6. Select update



7. Confirm the update



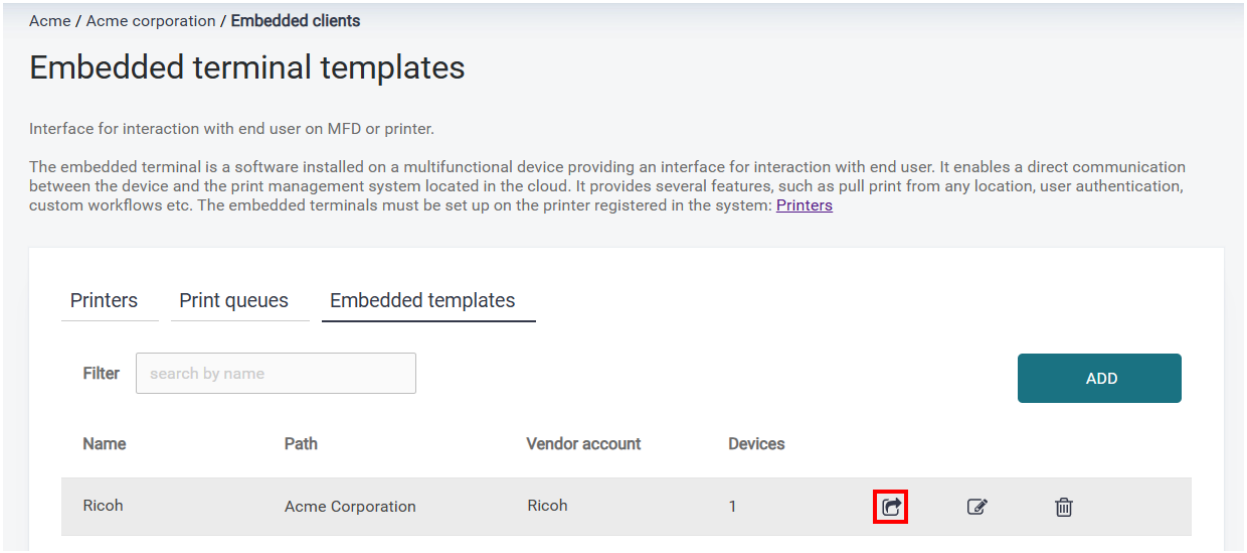
8. Confirm the restart



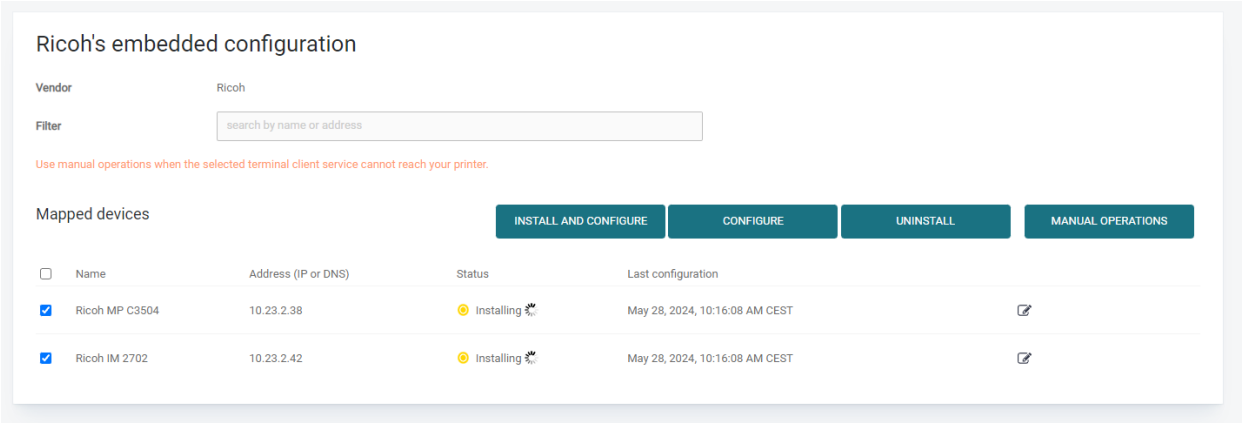
Manual installation via the Terminal Deployment Tool

Following these steps will give you the option to download the Terminal Deployment Tool from SAFEQ Cloud Web UI and it will generate the installation command for you.

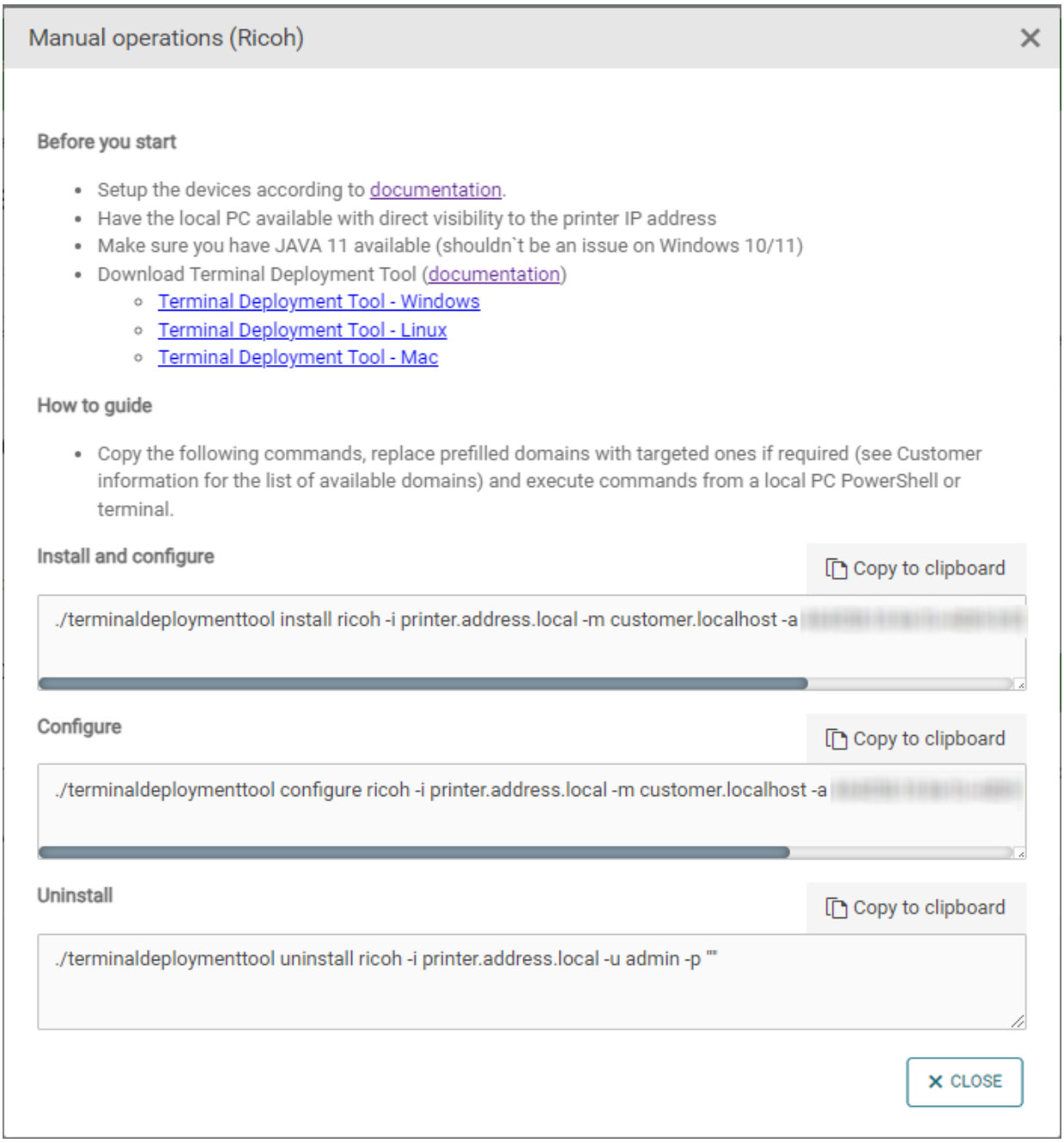
1. Go to SAFEQ Cloud Web UI. Create your Ricoh Embedded configuration and add your Ricoh MFD according to page Adding Embedded configuration and Ricoh MFD in SAFEQ Cloud Web UI.
2. Go to **Printers > Embedded templates** and click the icon next to your Ricoh embedded configuration to open the configuration.



3. Click **Manual operations**.



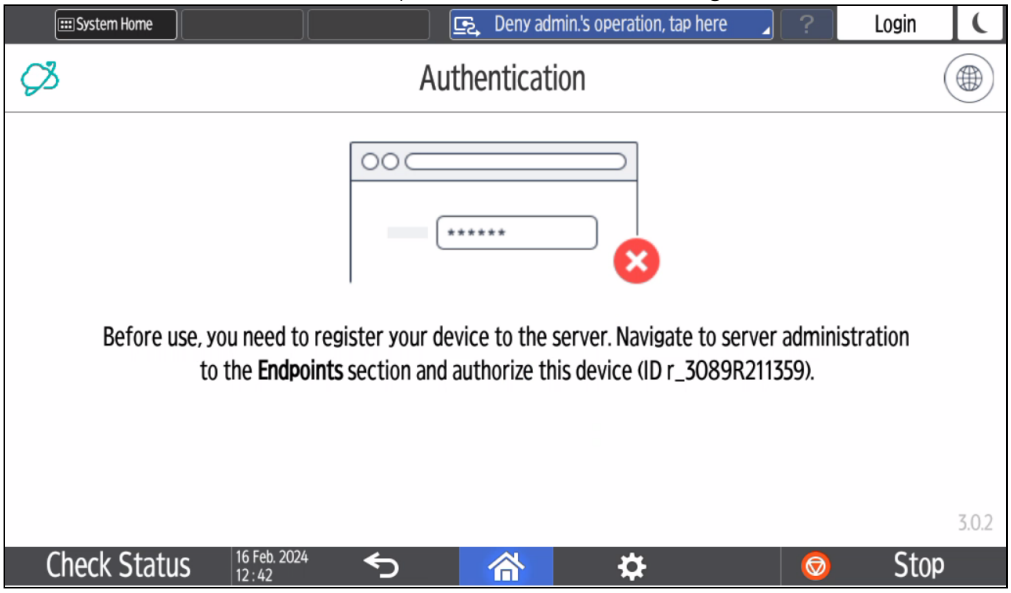
4. A new modal window will appear. Follow the instructions.



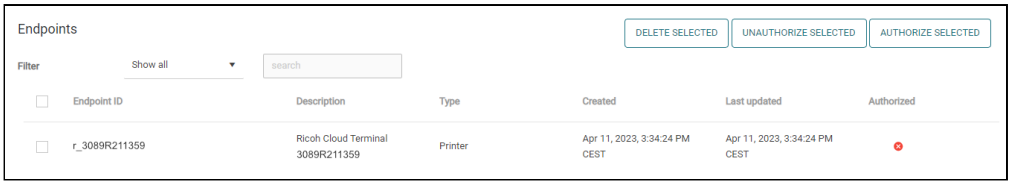
5. After the installation, proceed to registering the Cloud Terminal in the SAFEQ Cloud Web UI. This is described on the Registering the Cloud Terminal in the SAFEQ Cloud Web UI page.

Registering the Cloud Terminal in the SAFEQ Cloud Web UI

1. After the terminal installation, you will see the following screen. Note down the endpoint ID.

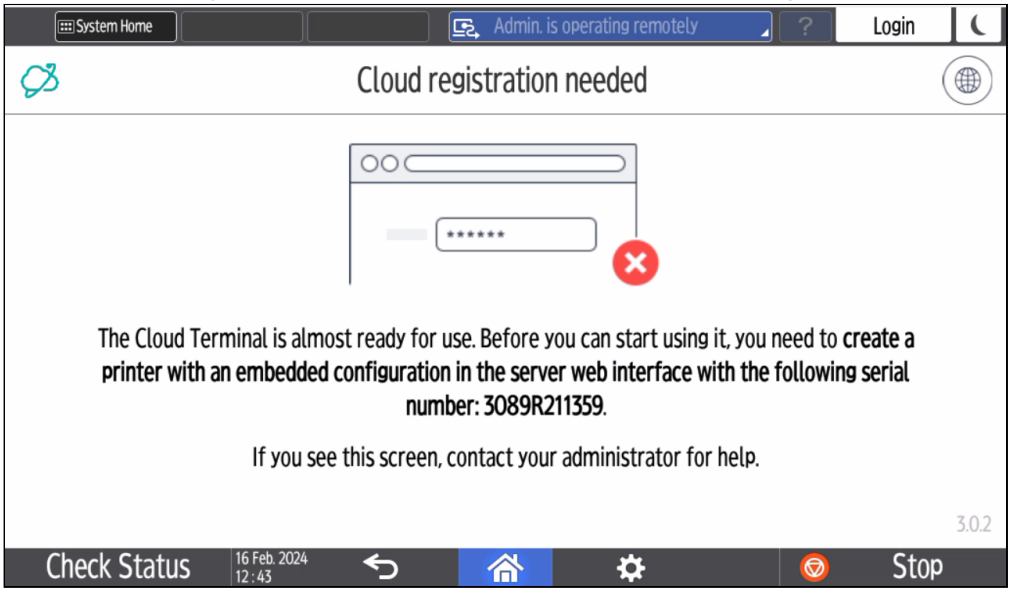


2. In SAFEQ Cloud web UI, go to **Endpoints** and find the entry that contains the endpoint ID from the previous step.



3. Select the entry and click **Authorize selected**.

4. If you haven't created an embedded configuration and added your Ricoh printer in SAFEQ Cloud Web UI, including the serial number, you will see the following screen on the MFD.



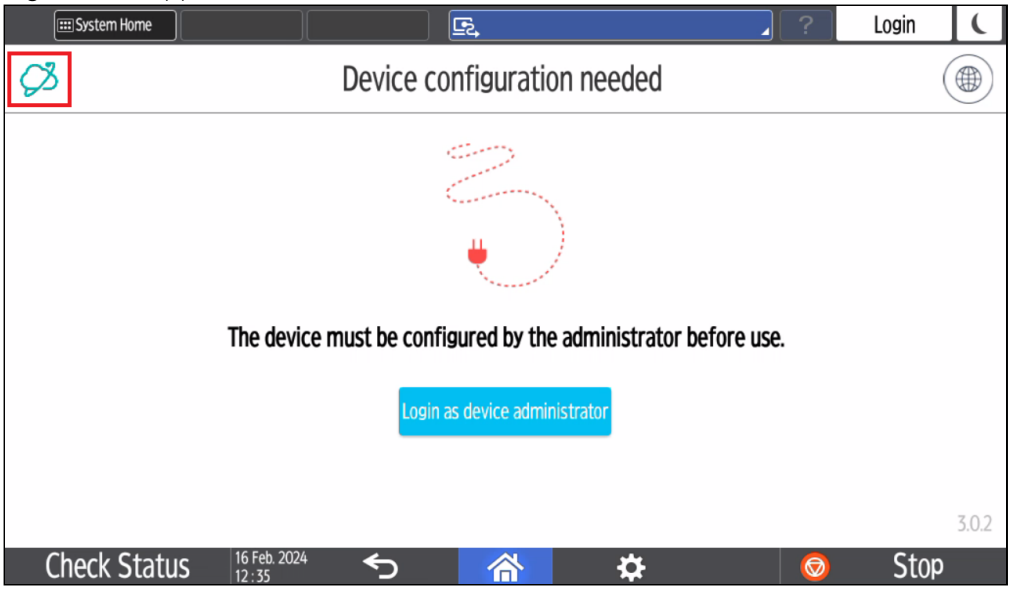
5. If you installed the Cloud Terminal from Ricoh Application Site, proceed to Post-installation device setup, section *Manual device configuration*.

Post-installation device setup

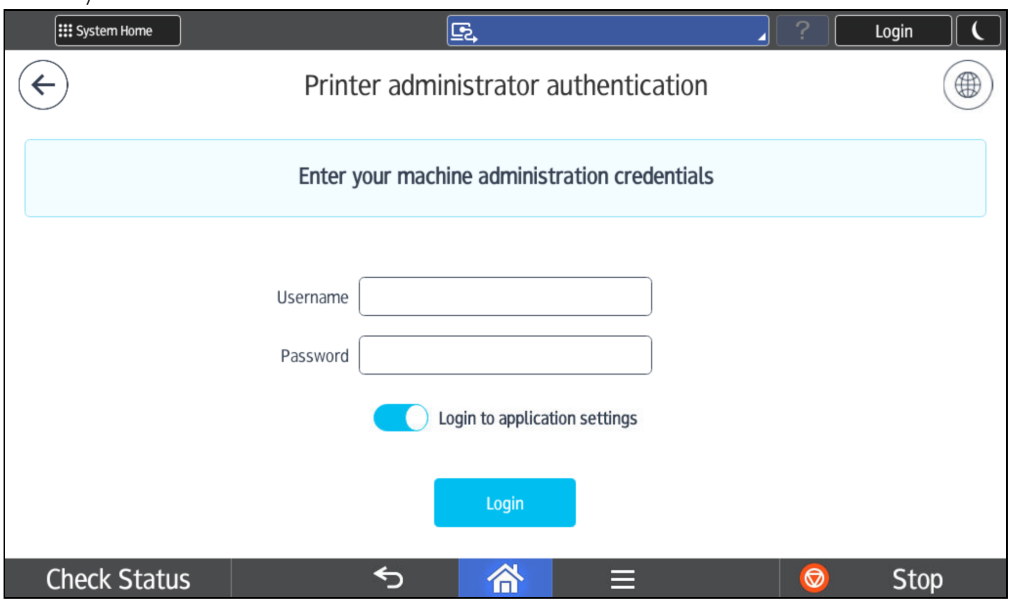
Logging in as machine administrator

After the terminal installation, if you need to log in at the MFD as machine administrator, perform the following steps:

1. On the Authentication screen or device code flow screen or an error screen, tap and hold the logo in the upper left corner for at least 5 seconds.



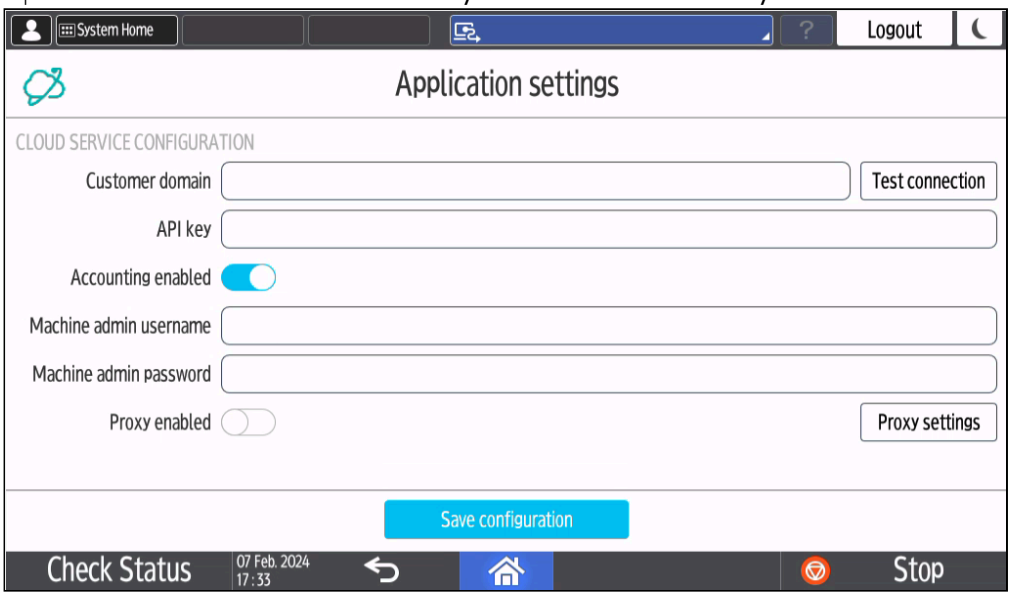
2. Enter your admin credentials.



Manual application configuration

You need to configure the terminal manually only if you haven't set the **Customer domain** and **API key** via the Terminal Deployment Tool or by configuring the terminal from the SAFEQ Cloud Web UI.

1. Login as machine administrator to application settings (see section *Logging in as machine administrator* above).
2. Update **Customer domain** or **API key**. Note that the **API key** field cannot be saved empty.



How to obtain the API key: Log in to the SAFEQ Cloud Web UI and go to **Security** > **API keys**. Click **Add**. Copy the key value and click **Save**. For more information, see API access keys.

3. Tap **Test connection**.
4. If needed, enable accounting.
   a. Fill in the machine administrator username and password. It will be used for accounting based on the device counters and for address book management. Without it, accounting will not work and the address book will display entries from previously logged users.

5. If you wish to use proxy, tap **Proxy settings**.

6. Fill and save the proxy settings.
7. Back in the main menu, enable proxy.
8. Tap **Save configuration**.
9. The identity management URL will be updated after the Customer domain change automatically.
10. Log out.

Manual device configuration

The following steps are done automatically during the installation.

Manual configuration is needed:

- If you installed the Cloud Terminal from Ricoh Application Site.
- On G2 machines without Java enabled (the administrator is informed about this during the installation).
- If the remote configuration fails due to an unexpected error (the administrator is notified about this situation during the installation).

Configuring USB Card Reader

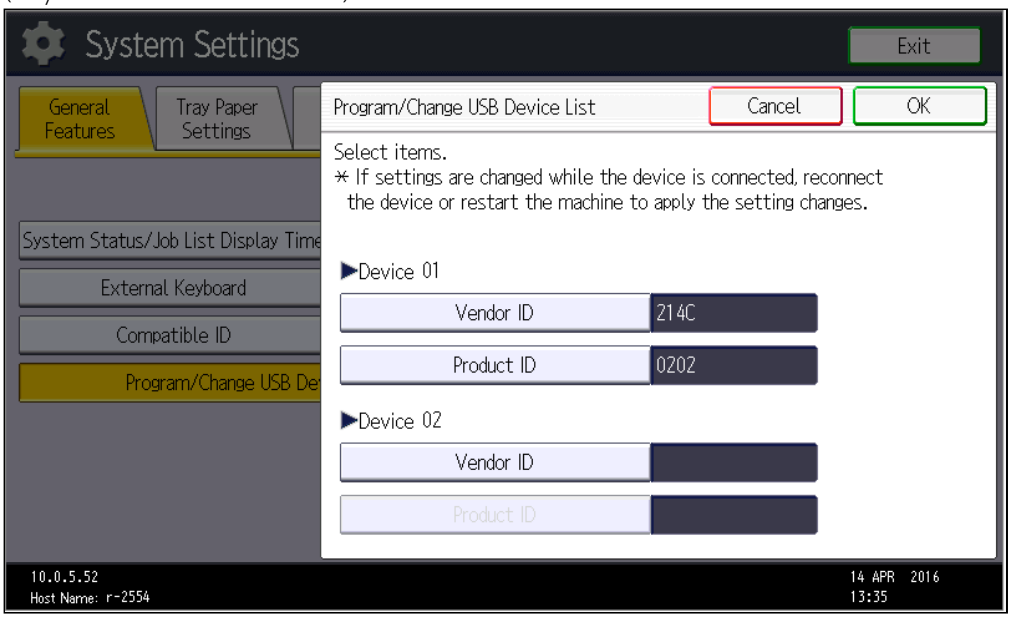
Manual configuration is needed for card readers other than Y Soft card readers.

Configure the card reader in System Settings

1. Navigate to **System Settings** > **General Features** > **Program/Change USB Device List**.

2. Under **Device 01**:

   a. If you have a YSoft card reader, enter values for **Vendor ID**: 214C and **Product ID**: 0202 (keyboard emulation mode).

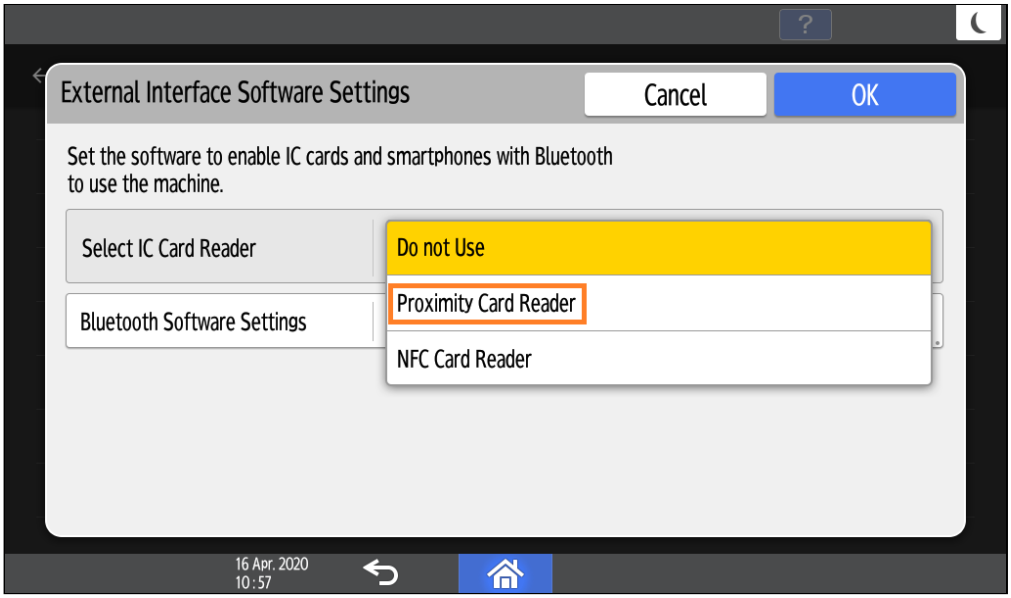


   b. If you have a card reader from another manufacturer, you can find the Vendor ID and Product ID in Compatible Card Readers.

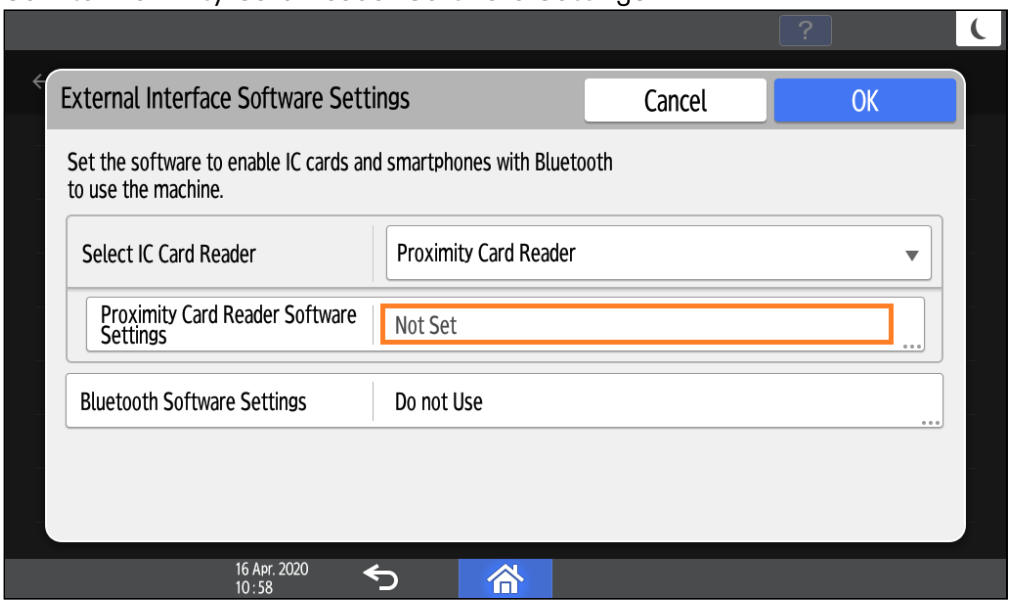
Set up card reader in Smart Operational Panel

1. Navigate to **User Tools / Settings** > **Screen Features** > **Screen Device Settings** > **IC Card Bluetooth Software Settings / External Interface Software Settings** > **Select IC Card Reader**.

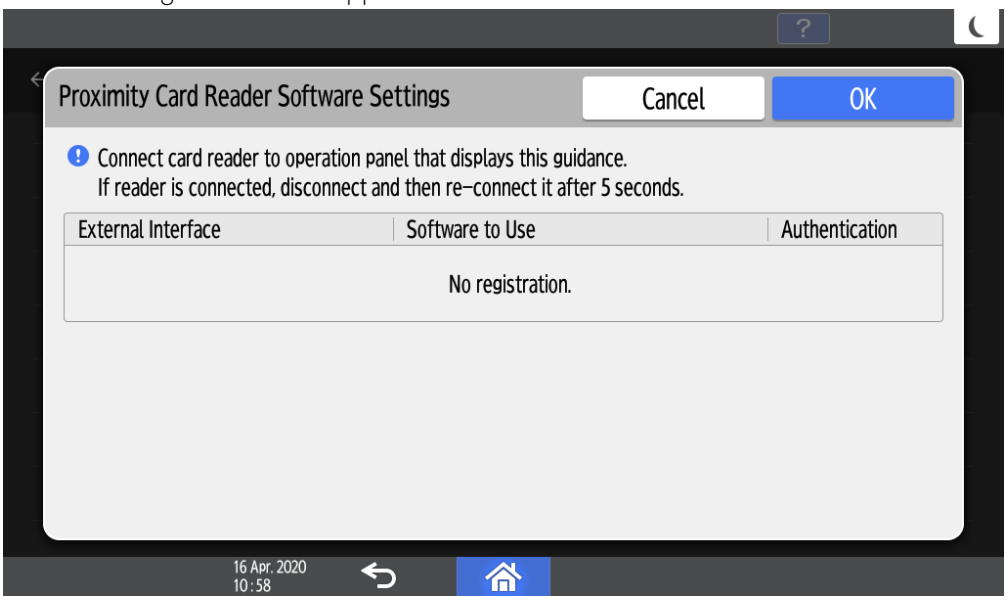
2. Select **Proximity Card Reader**.



3. Go into **Proximity Card Reader Software Settings**.



4. The following screen will appear:



5. Connect or reconnect a card reader to USB on the Smart Operational Panel.

> ⚠ You can use only Smart Operational Panel USB – either a visible one or a hidden micro-USB through an adapter. The card reader will not work with MFD ports (on the back or on the side of the device).

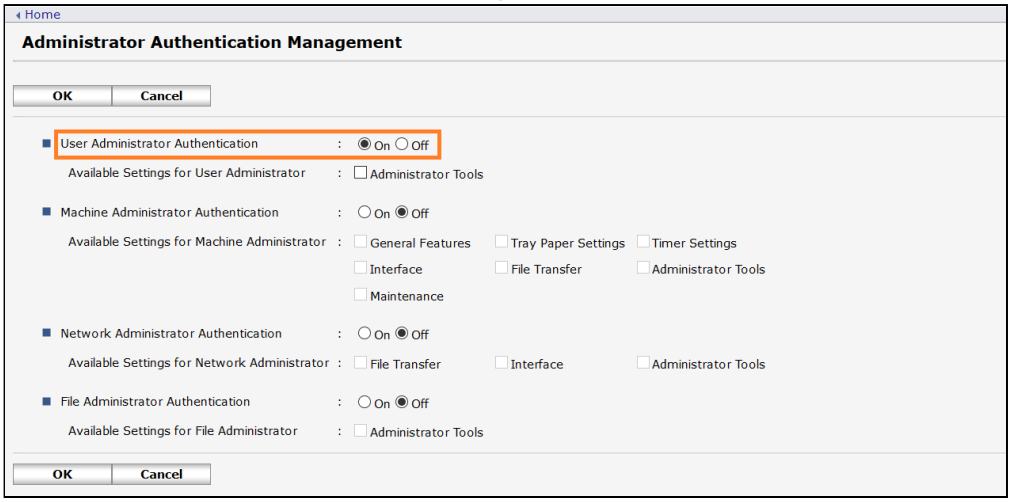
6. Check the settings, confirm the change, and restart the MFD.

Service menu settings

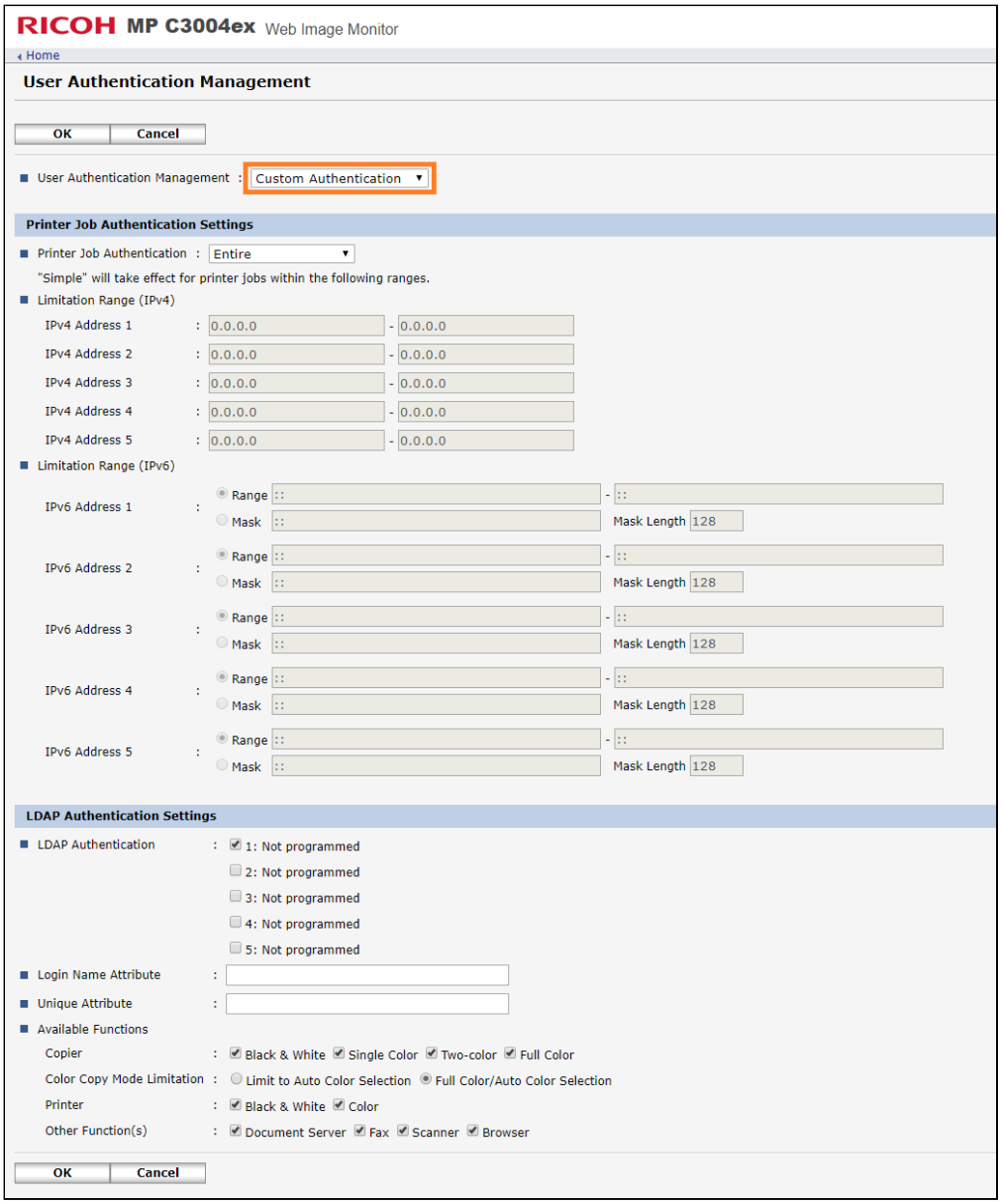
> ⚠ The firmware update should be updated to the latest version. Ask your Ricoh technician to configure the settings for the terminal application for you.

Authentication settings in Web Image Monitor

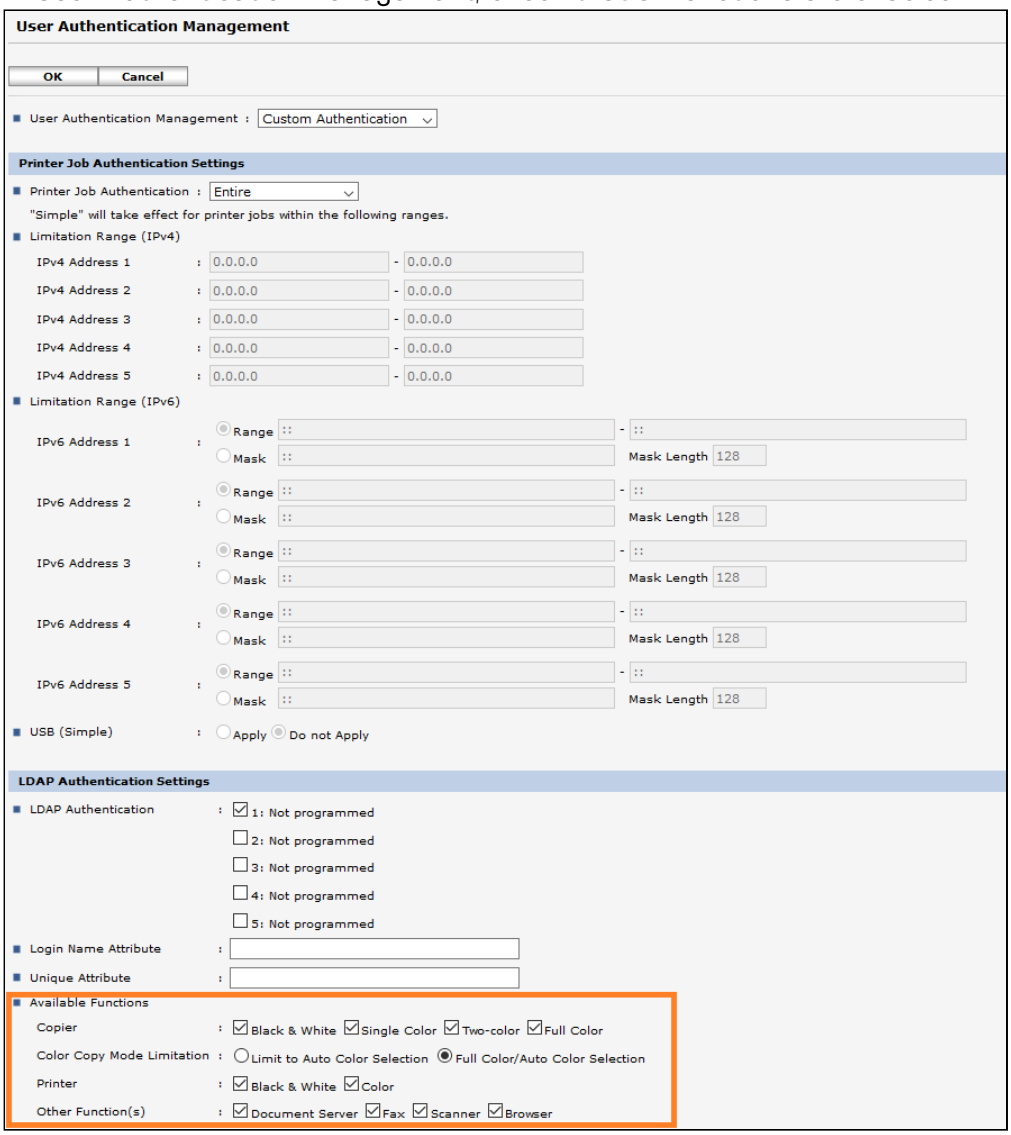
1. Go to the Ricoh MFD web interface (Web Image Monitor).
2. Log in as an administrator.
3. Under **Device Management** > **Configuration**, change the following settings so the authentication application will be displayed:
   a. In **Administrator Authentication Management**, set **User Administrator Authentication** to **On**.



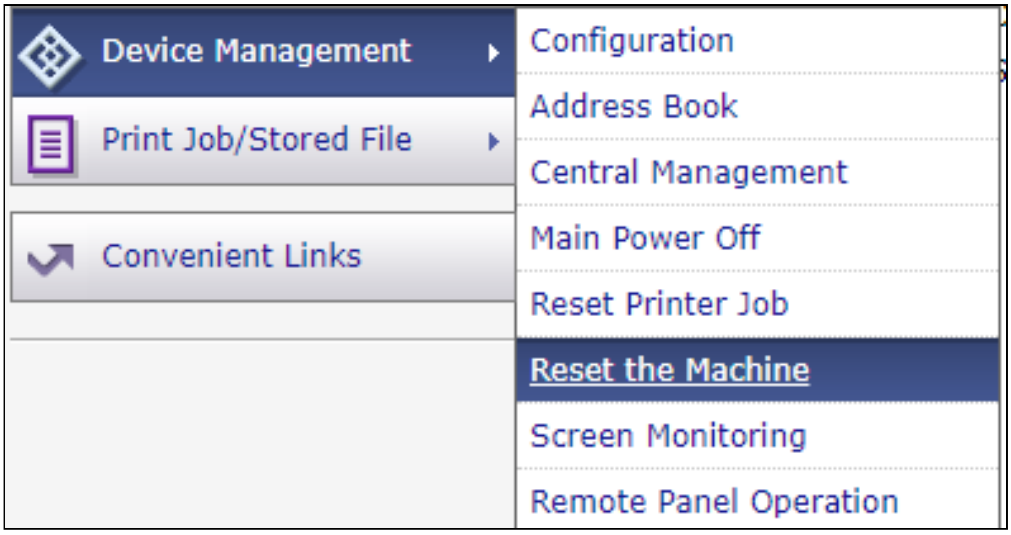
b. In User Authentication Management, set User Authentication Management to Custom Authentication.



c. In **User Authentication Management**, check that all functions are enabled.



4. Restart the device. You may use **Reset the Machine** in WIM.

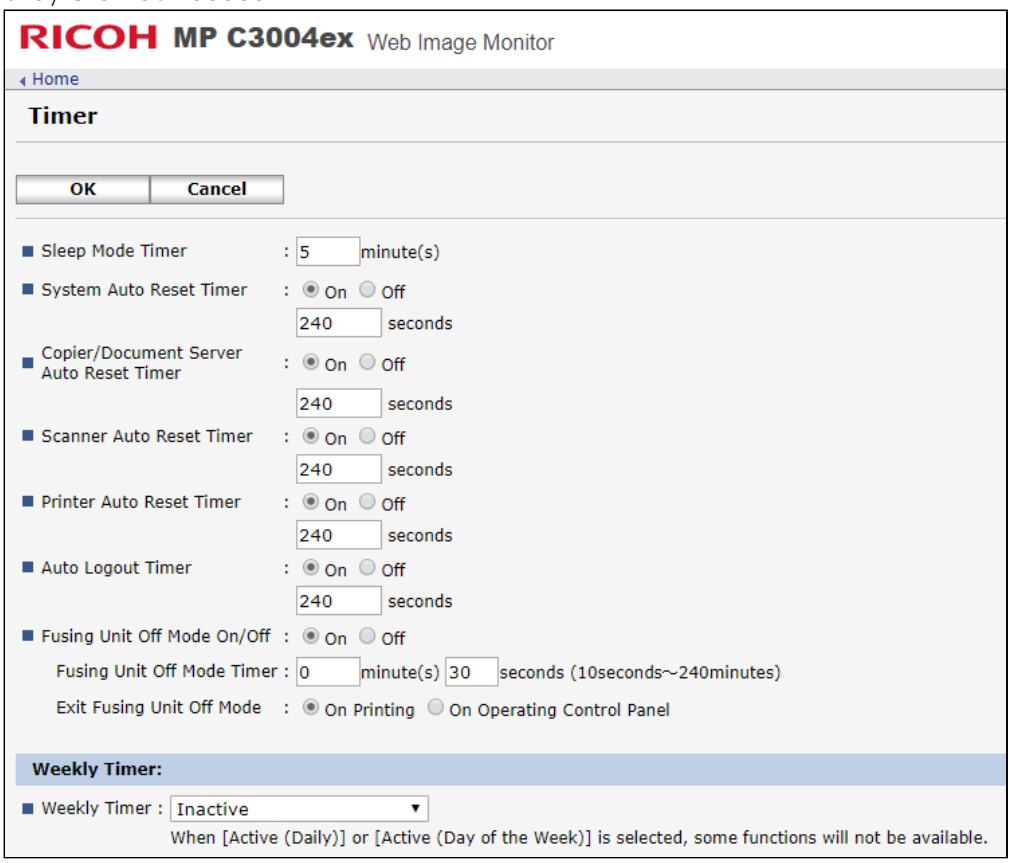


Set appropriate timers

Terminal inactivity timeout is a value for the user's automatic logout. It is defined for Cost centers and can be specified per user. This feature is currently not supported by Ricoh SOP.

The default value on MFD is automatically set to more than 3 minutes. It can be manually changed after installation.

1. Login to WIM (Web Image Monitor) as machine administrator.
2. Under **Device Settings**, navigate to **Device Management** > **Configuration** > **Timer**.
3. As default set all timers higher than Terminal inactivity timeout (so for default Terminal inactivity value, set all values to more than 3 minutes). Most of the timers can be turned off if they are not needed.

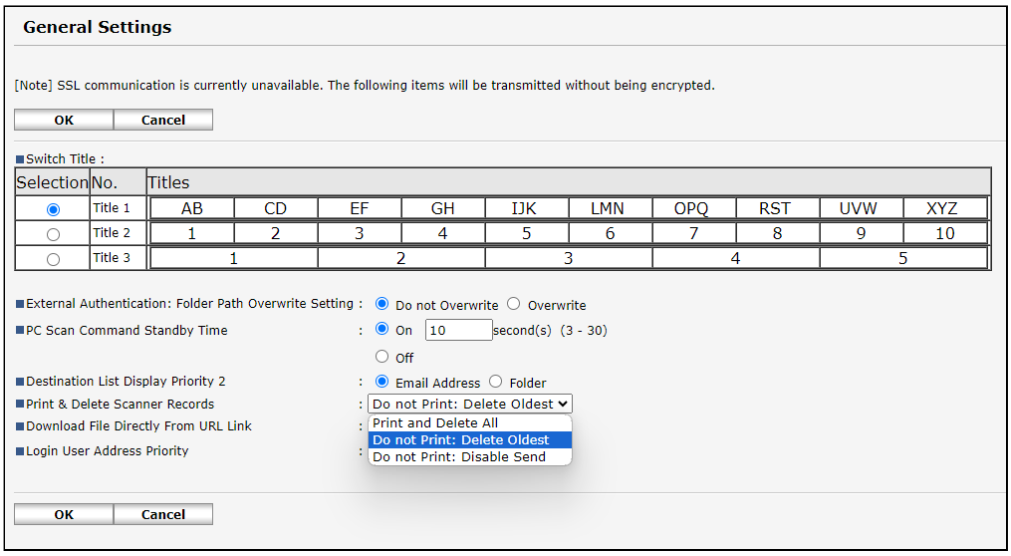


Scan journal settings

For the users to always be able to scan, we recommend you setting the following scan journal deletion strategy:

1. Log in to WIM (Web Image Monitor) as machine administrator.
2. Go to **Device Management** > **Configuration** > **Scanner** > **General Settings**.

3. Set **Print & Delete Scanner Records** to **Do not Print: Delete Oldest**.



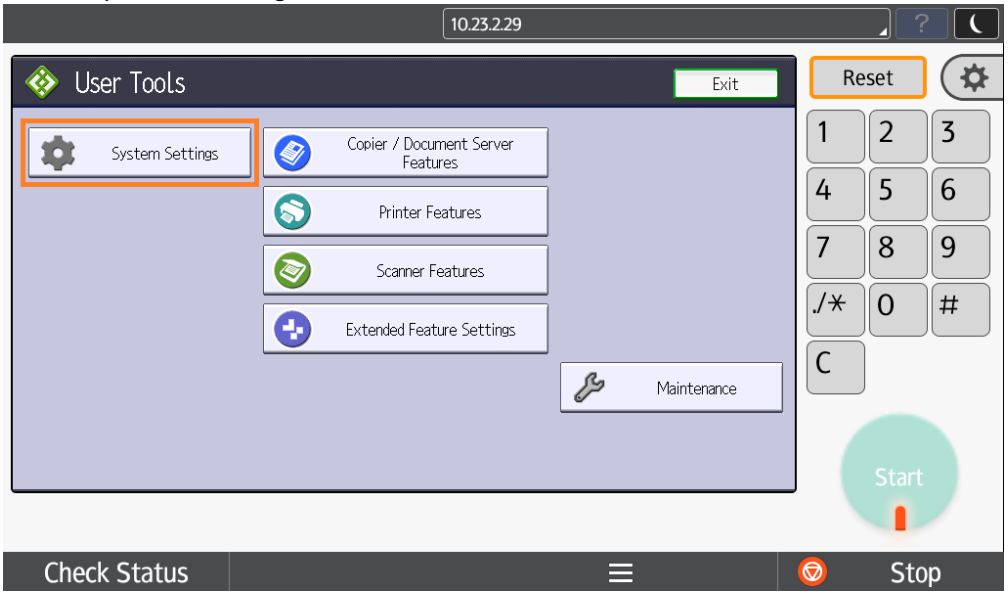
4. Alternatively, you can change this by setting **SCAN_SETTINGS__PRINT_DELETE_SCANNER_JOURNAL SP** option to **1**.

Key Counter Management settings on the MFD

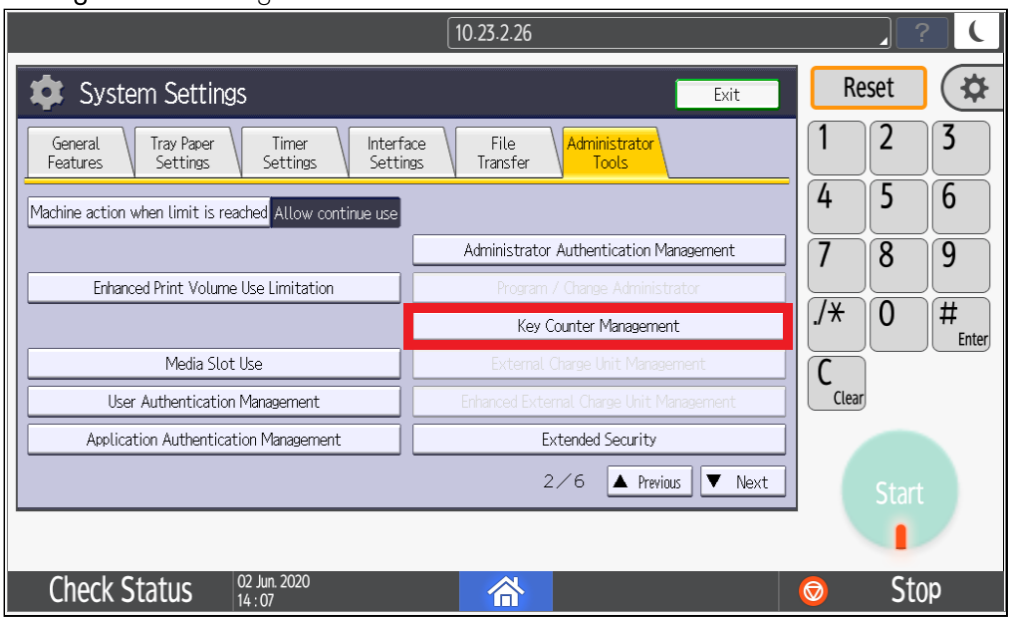
1. Go to **User Tools** on MFD.

2. Select **Machine Features**.

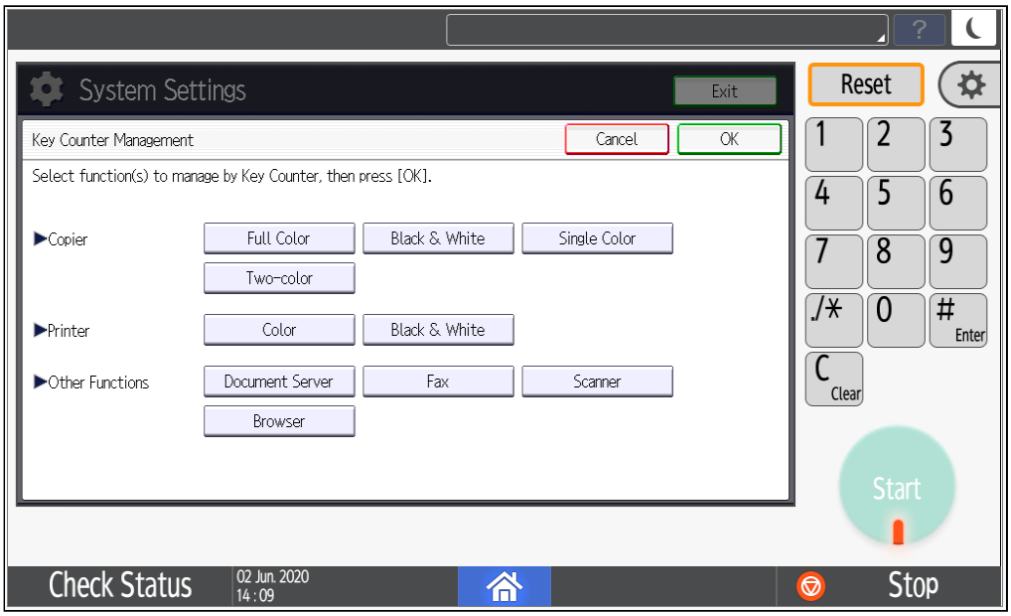
3. Go to **System Settings**.



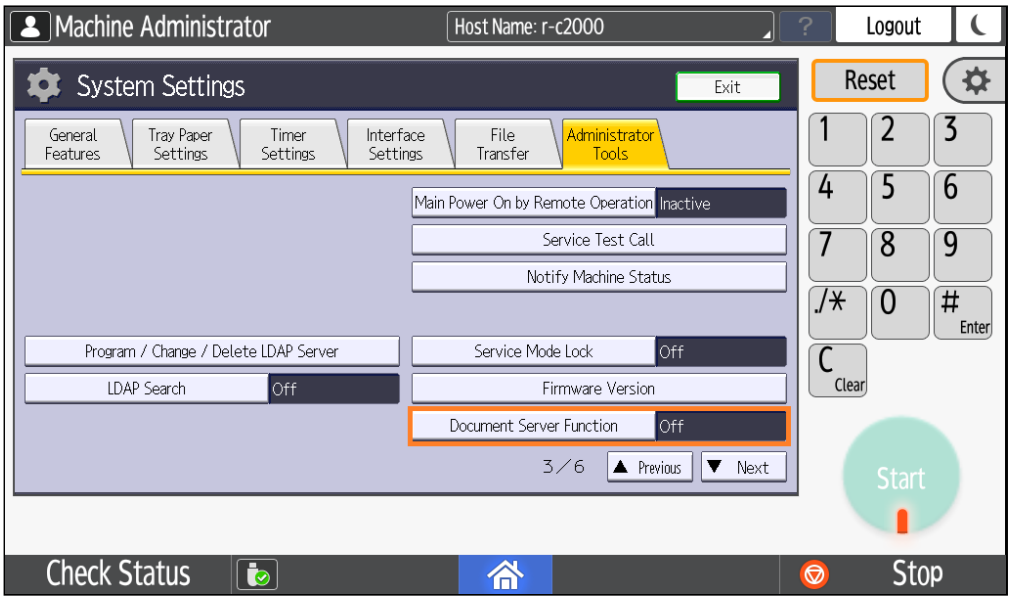
4. Go to **Administrator Tools**. Use **the Previous** or **Next** buttons to locate the **Key Counter Management** setting.



5. Unblock all functions.



6. Set **Document Server Feature** to **Off**.



Initial device setup

Setup for all types of cloud terminal installation

The following setup is necessary for all types of installation method.

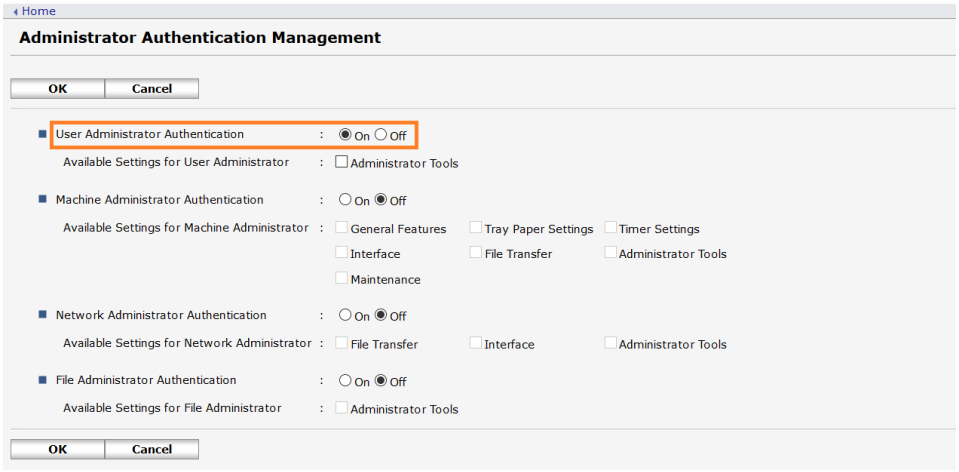
1. Log in to the web interface of your Ricoh MFD (Web Image Monitor - WIM) as Machine Administrator.
2. Navigate to **Device Management** > **Configuration** > **Date/Time** and set the time on MFD to match your regional settings or specify automatic time configuration via the NTP server.
3. Navigate to **Device Management** > **Configuration** > **Device Settings** > **Paper**.
4. Set **Apply Auto Paper Select** to **Yes** for all trays.
5. Optional: Set card reader to be available from sleep mode:
   a. Log in as Machine administrator.
   b. Go to **Settings** > **Screen Features**.
   c. Navigate to **Screen Device Settings**.
   d. Set **Screen device always-connection Setting** to **true**.

Setup for installation from Ricoh Application Site

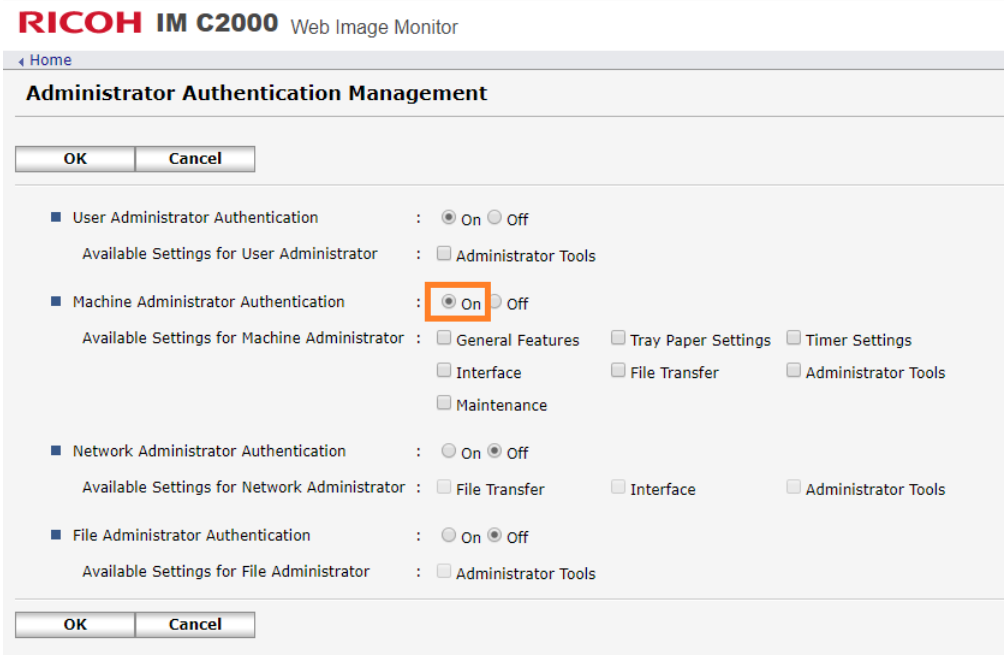
Please note that this application needs to be installed by Ricoh or a partner technician.

The following setup is necessary only if you plan to install the terminal from Ricoh Application Site.

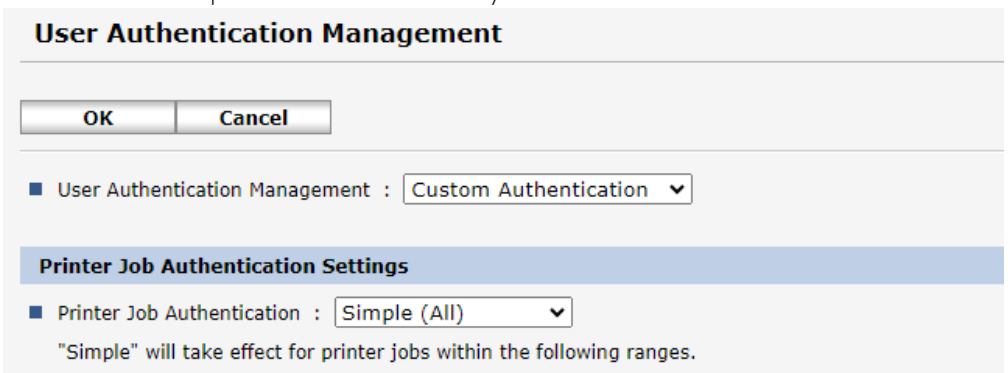
1. Go to **Device Management** > **Configuration**.
2. In **Administrator Authentication Management**, set the **User Administrator Authentication** to **On**.



3. In Administrator Authentication Management, set Machine Administrator Authentication to On.



4. In User Authentication Management, set User Authentication Management to Custom Authentication, and set Printer Job Authentication to Simple.
Note that this option is conditioned by a SP mode.



Ricoh Standard Embedded Terminal

This terminal was formerly called Ricoh Embedded Android (SOP). In the Embedded clients configuration in SAFEQ Cloud Web UI, it is called Ricoh Standard.

Pre-Embedded Deployment setup

This guide describes the prerequisites and implementation steps to successfully deploy an Android (SOP) embedded client on the Ricoh IMC device. The guide also describes how to configure the MFD to change the Login path of the user to the `PullPrint` app to lock the device from unauthorized use.

You must change the Y Soft local admin account to use a different username when compared to the Machine username / Embedded settings in the SAFEQ Cloud Portal, or the local machine admin will not be able to log in at the MFD. Go to **Users**, select the **Local Provider**, and change the admin username to something else.

Before you begin, make sure your secondary gateway is configured according to Secondary Gateway mapping.

Enable Custom Authentication

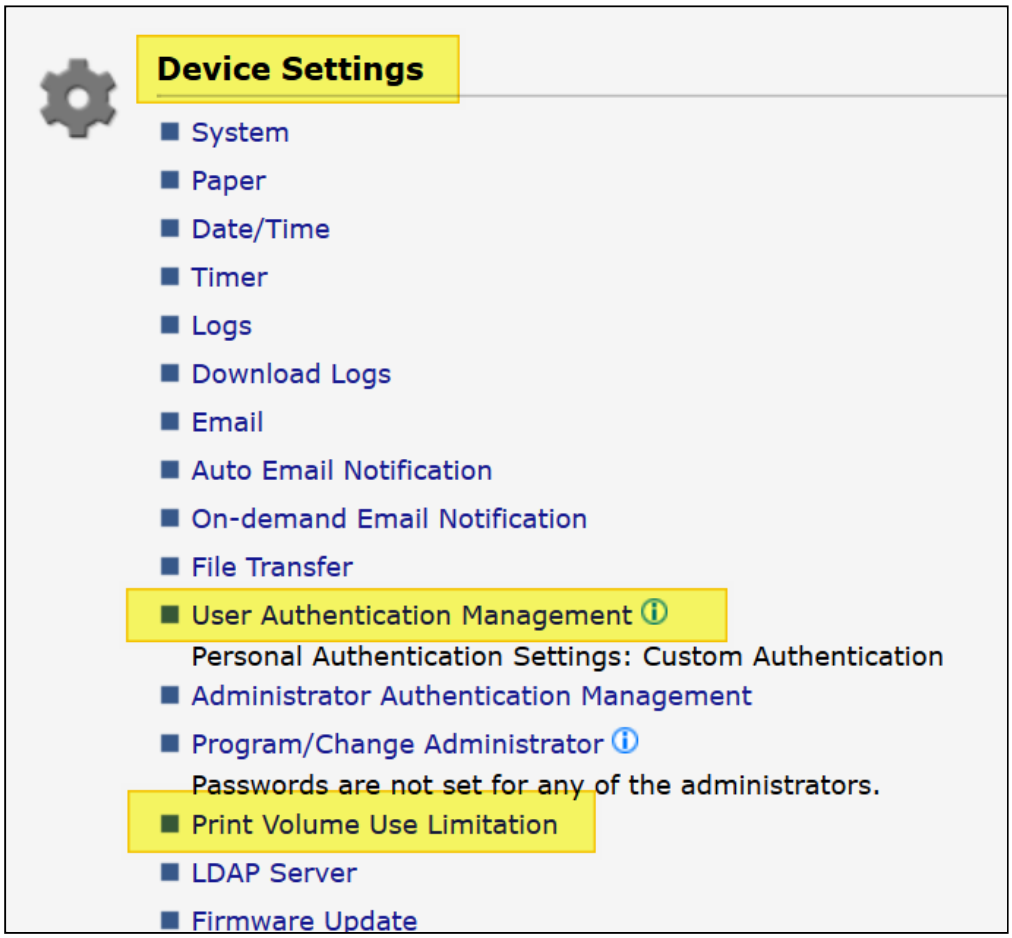
Custom Authentication must be enabled on the device as a prerequisite for the SAFEQ Cloud `Pull Print` App to function.
As of version 3.14, these settings will be applied during deployment of the Ricoh SOP Embedded (Pull Print) client. Ensure the Secondary Gateway server is updated see Remote Update of Secondary Gateways.

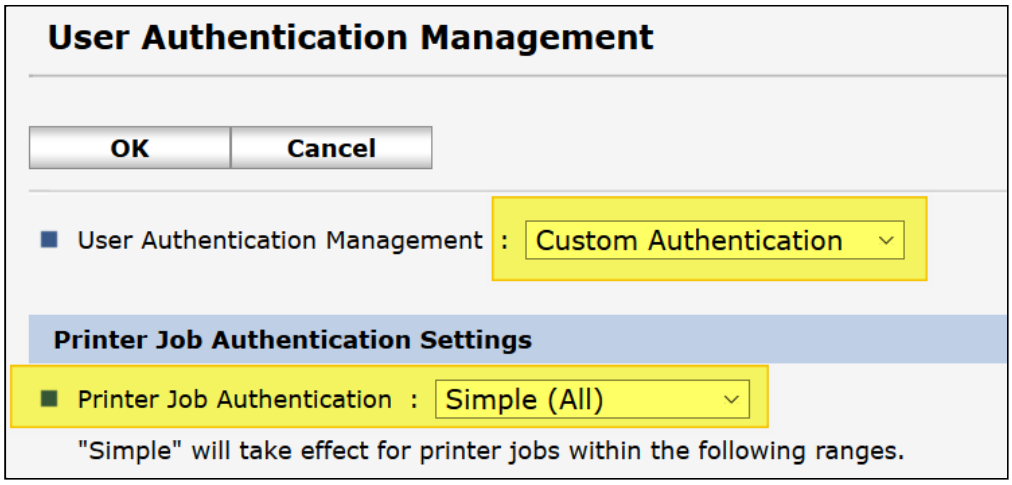
If preferred, you can change these settings manually from the device service menu, please contact your local Ricoh service contact to access the device service menu.

User Authentication Management, UAM

The SAFEQ Cloud Pull Print APP requires the device User Authentication Management (UAM) to be enabled.
Step one on the device Web Image Monitor (access WIM via the device IP from your web browser), log in as admin and navigate to >Configuration >Device Settings User Authentication Management.

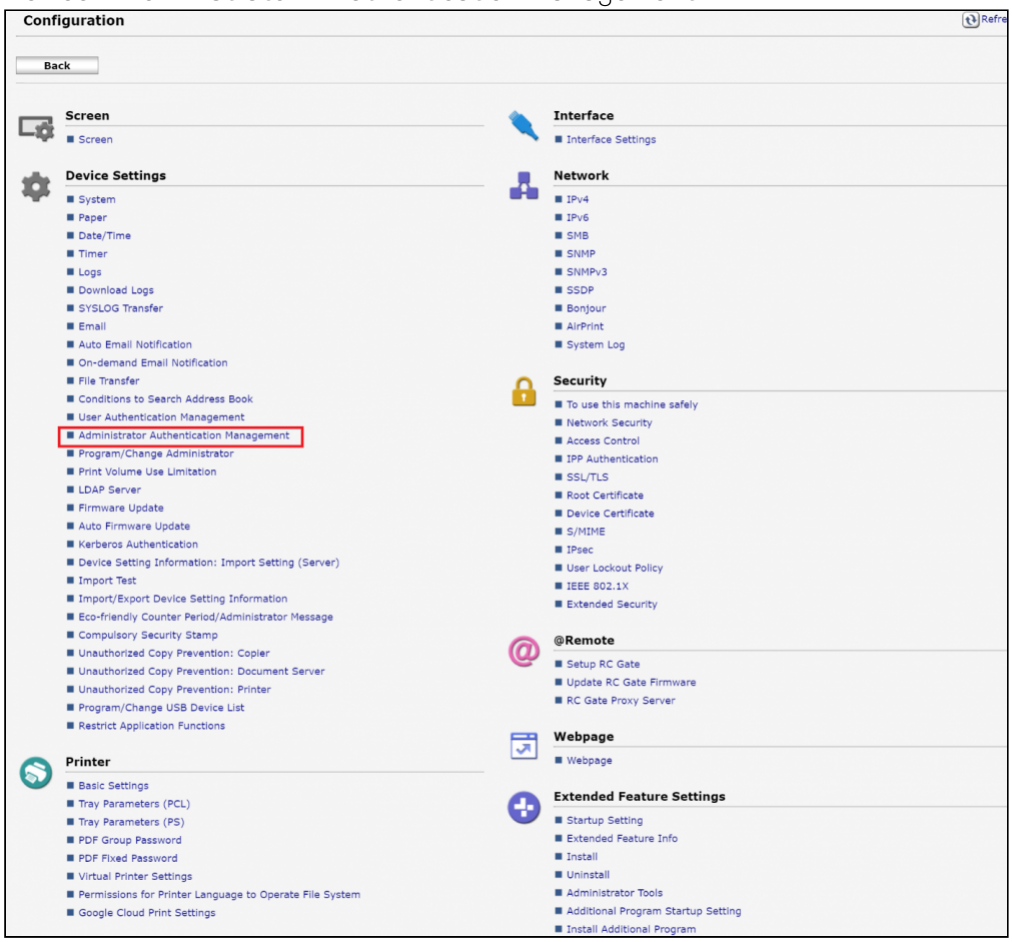
See below.



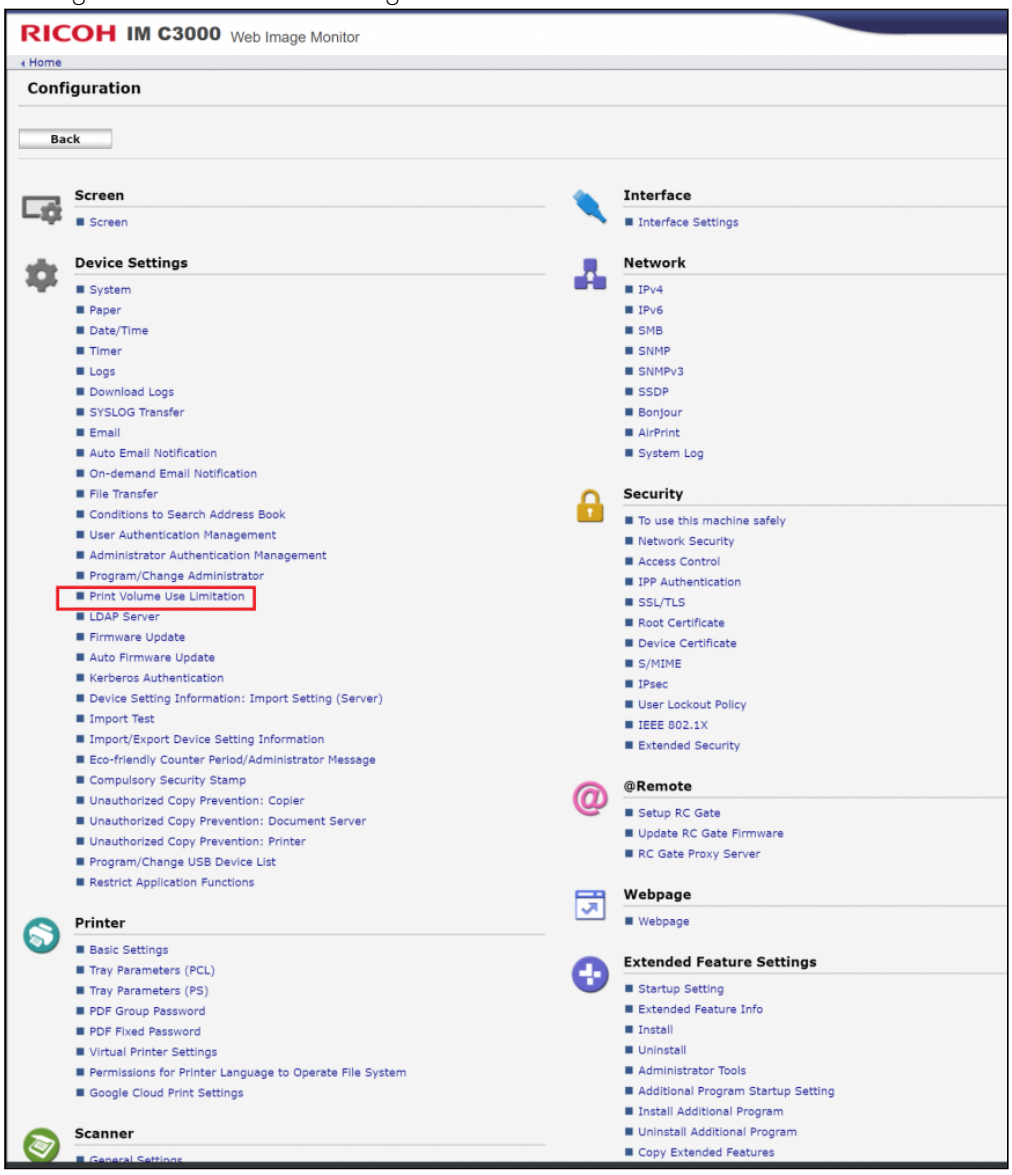


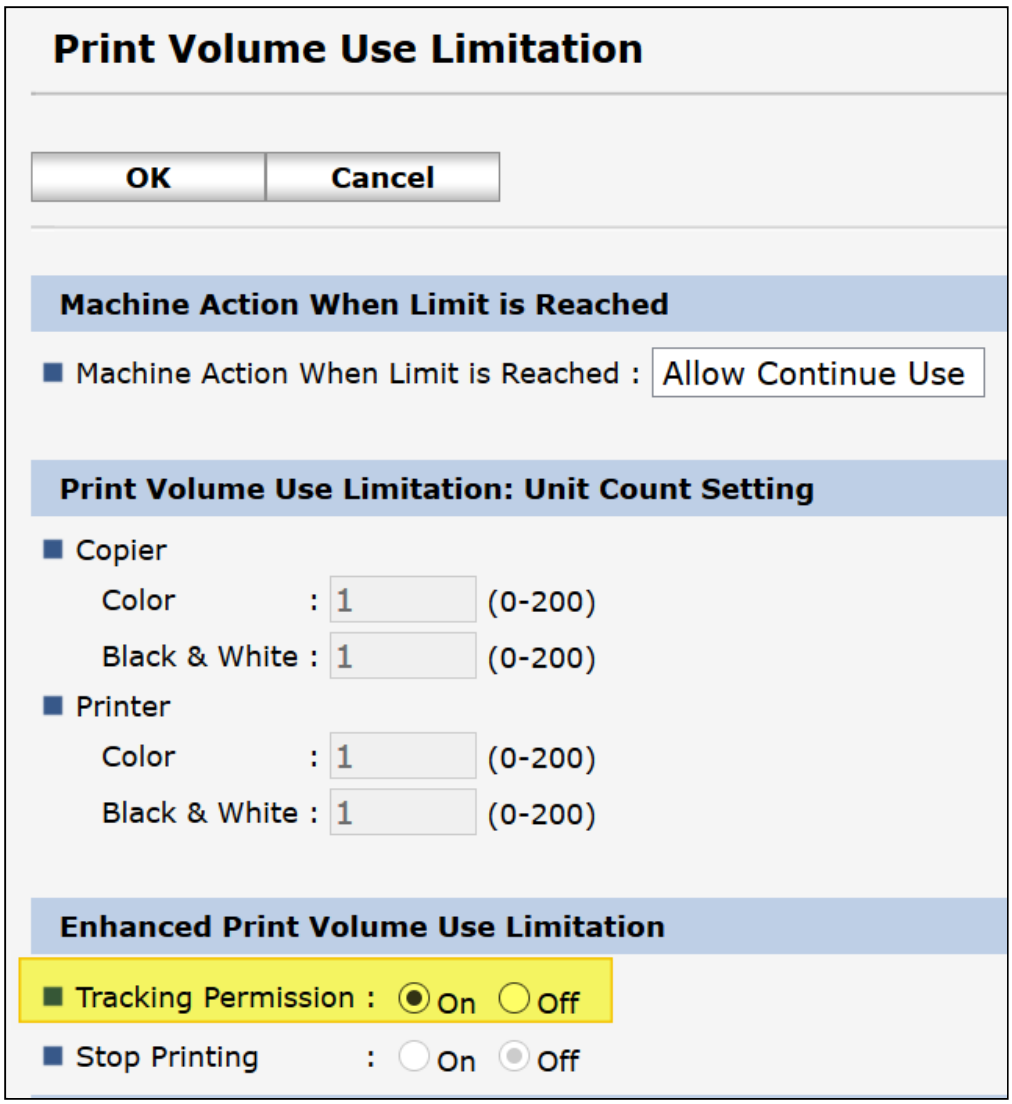
Select Custom Authentication in the dropdown. If not selected, it will not be possible to print and the job will spool and disappear from the Pull Print app without being printed. If the above setting in not visible for selection, please enable below.

Device > Administrator > Authentication Management



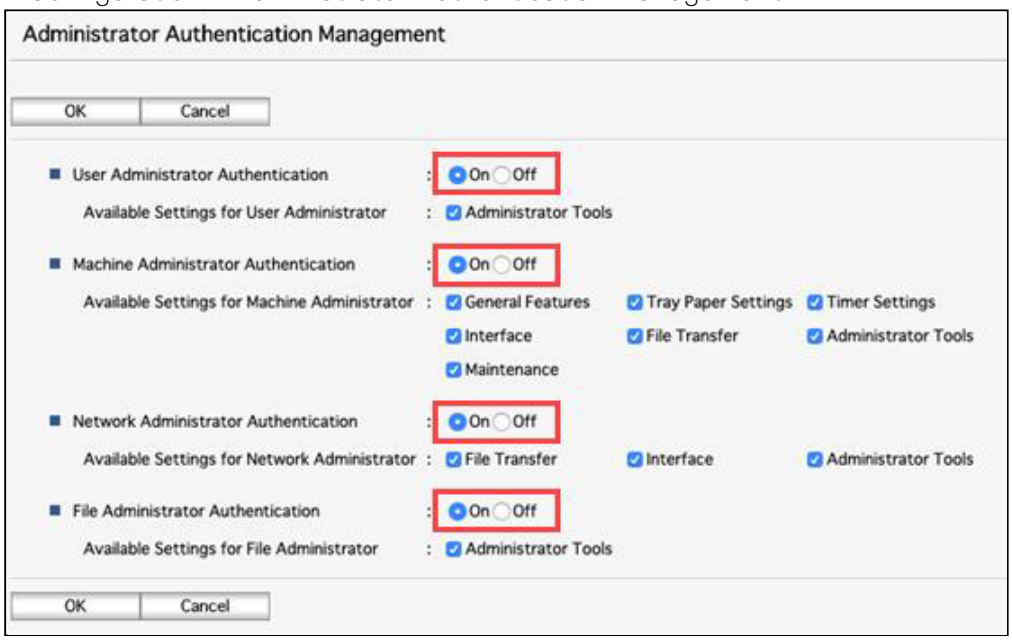
Tracking Permission needs to be set for Copy/scan Accounting
Configuration > Device Settings > Print Volume Use Limitation





To maximize the device's security and prevent users logging in via SAFEQ Cloud Embedded App accessing Administrator's functions, login to the device's web page and go to Device Management

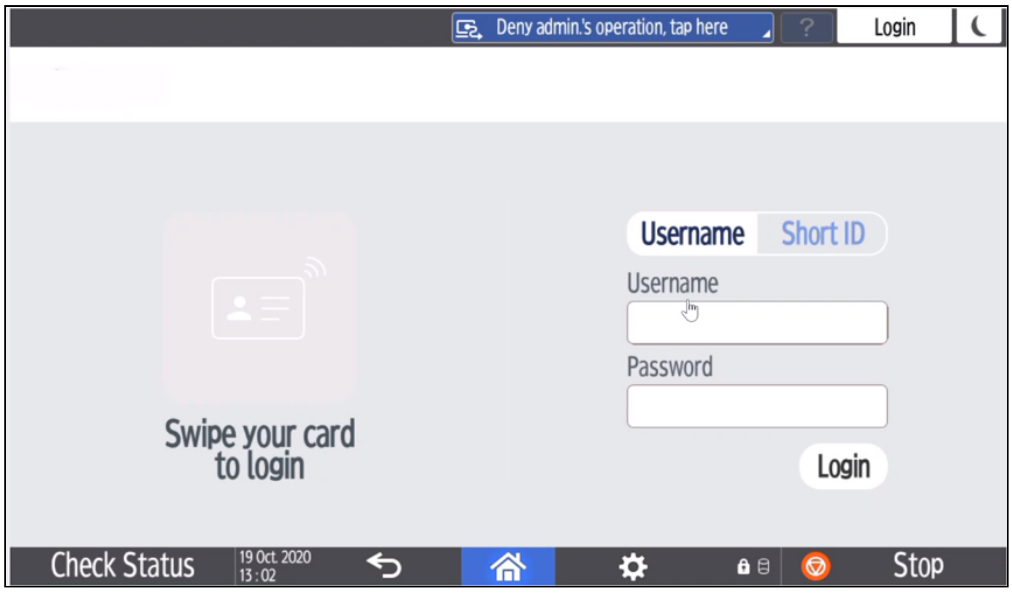
> Configuration > Administrator Authentication Management



Click OK to save the settings.
Your Ricoh device is now configured and ready for use with the SAFEQ Cloud solution.

Android, login

You can login to the device using the username/password or Short ID:

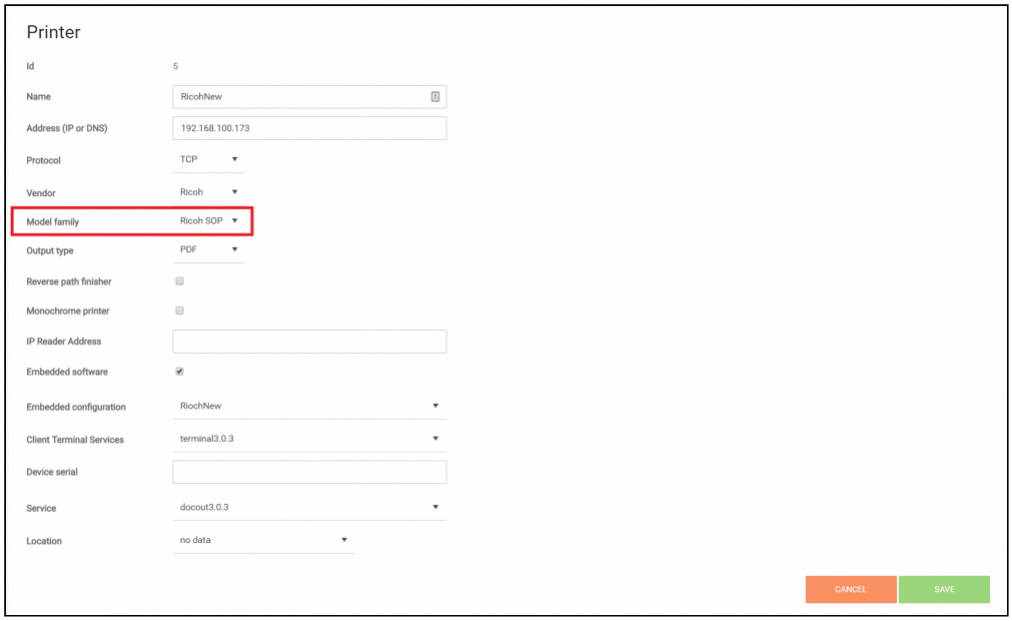


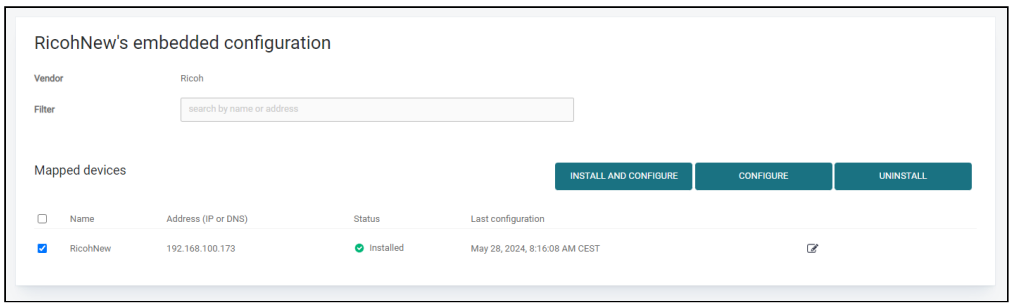
Installing the Embedded-on Ricoh Machine (SAFEQ Cloud Console)

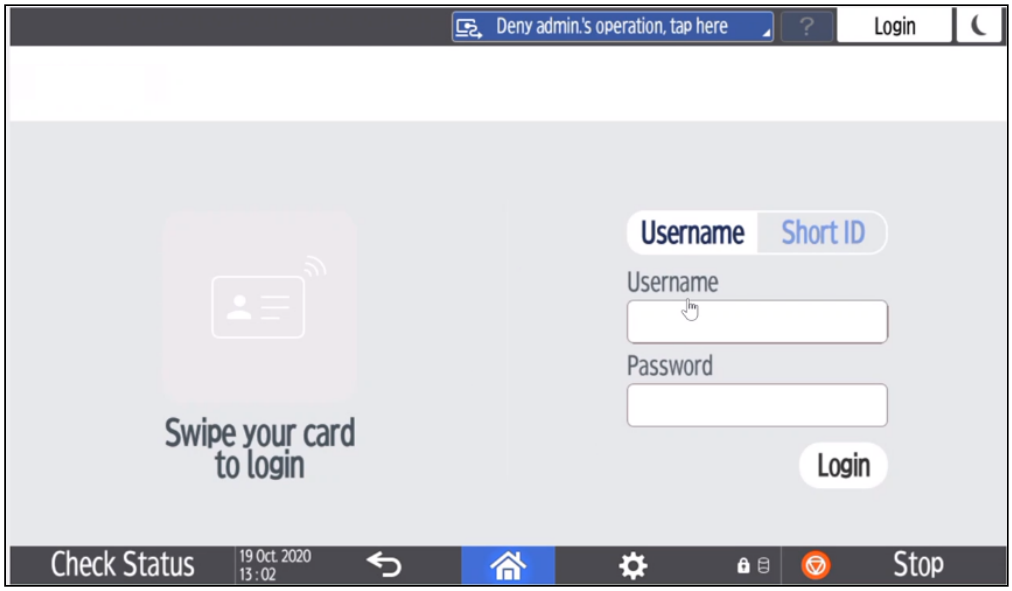
Please be aware that all changes made during the application install, including the ones mentioned in the “Pre-Embedded Deployment setup” section, will not be reverted to their previous state / values after uninstallation. Following uninstall of the Ricoh SOP application, a factory reset must be done to revert to default settings.

Login into your SAFEQ Cloud Console and Setup the Printer and Embedded settings. Once you follow the below 2 steps Status on your Mapped Device must indicate "Installed".

In order to have a successful deployment of the embedded it is required to have a non-empty password for the printer.



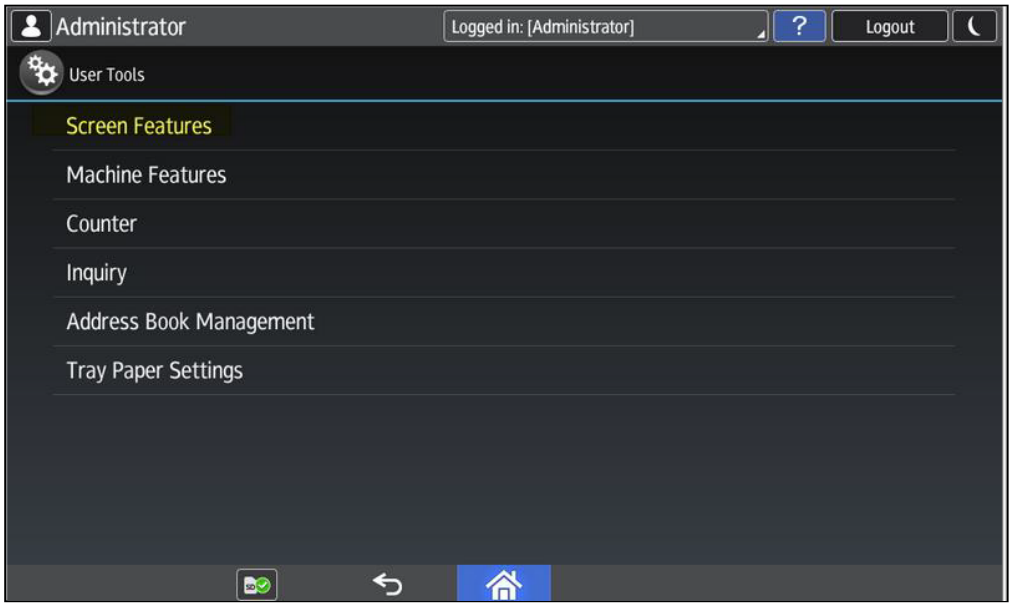




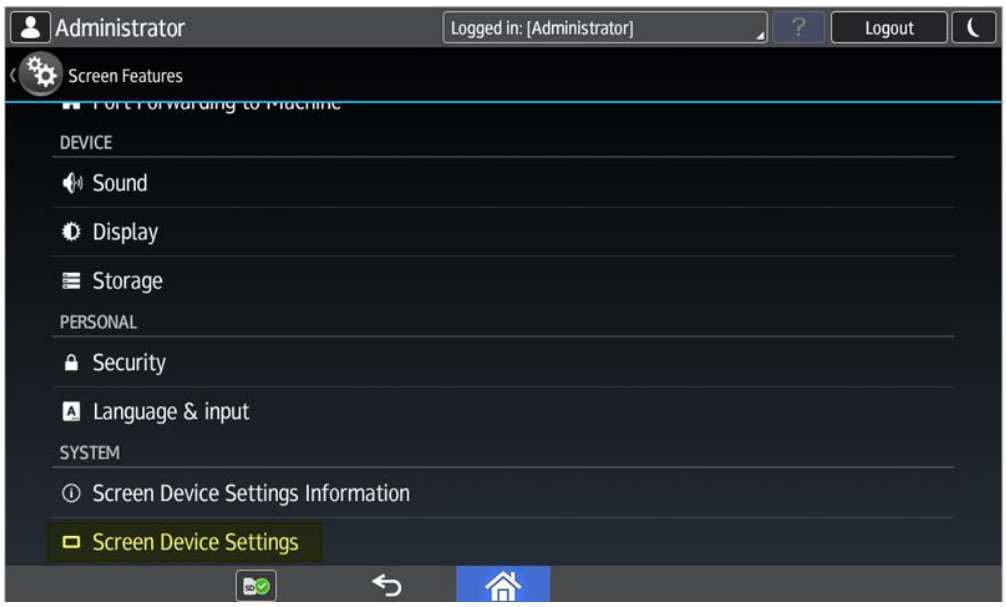
(Note – Please don't use username "admin" as it might conflict with Native username "admin" set in the printer console)

Changing the login path to Pull

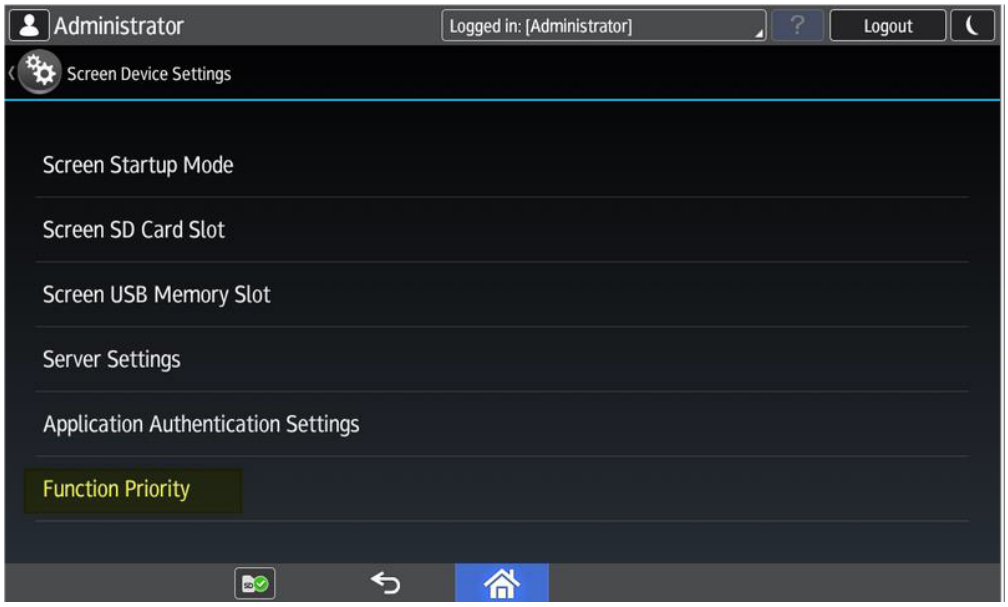
Login at the device and select User Tools > Screen Features



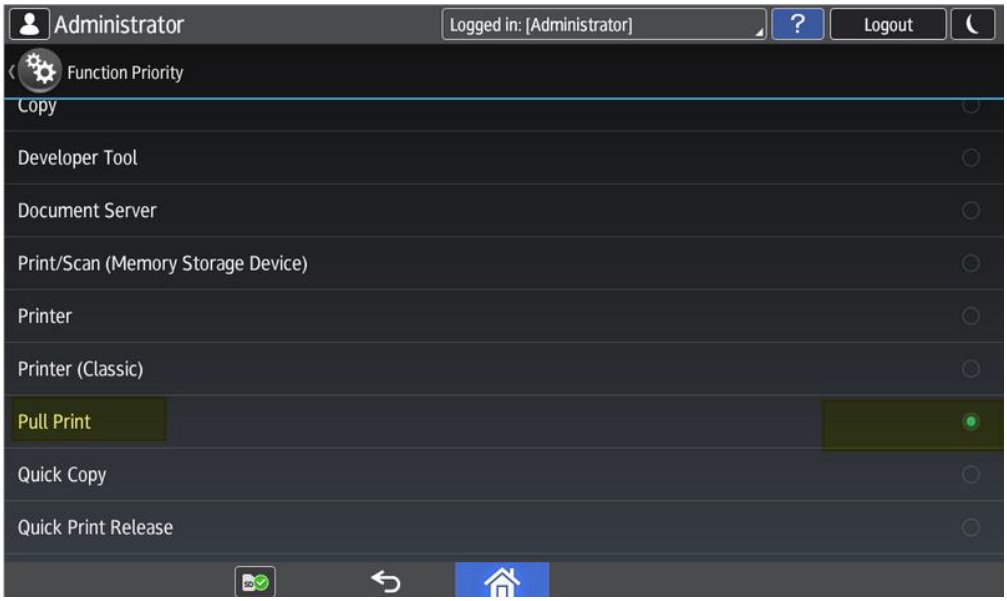
Select Screen Device Settings



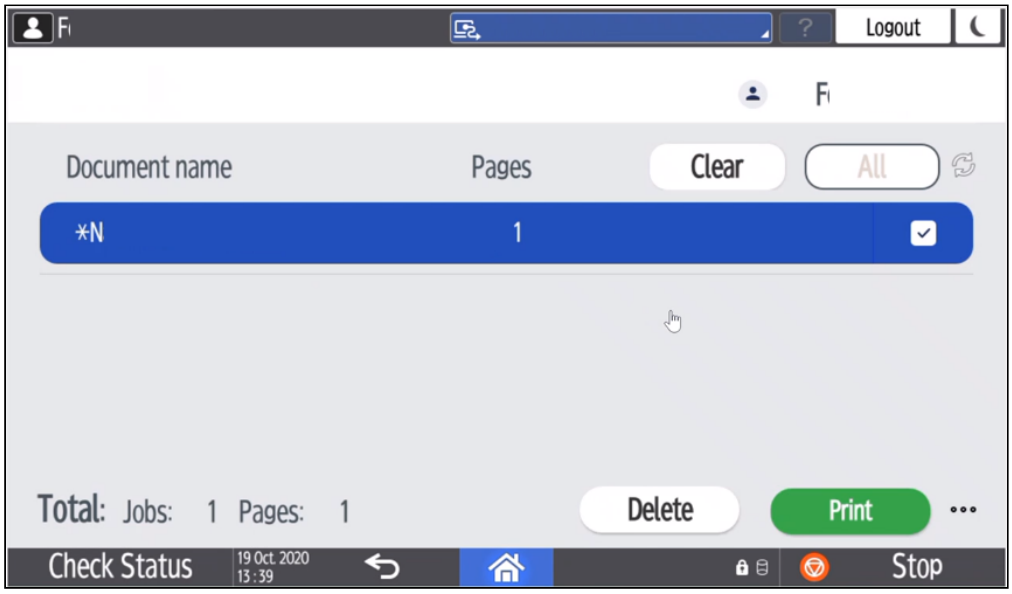
Select Function Priority



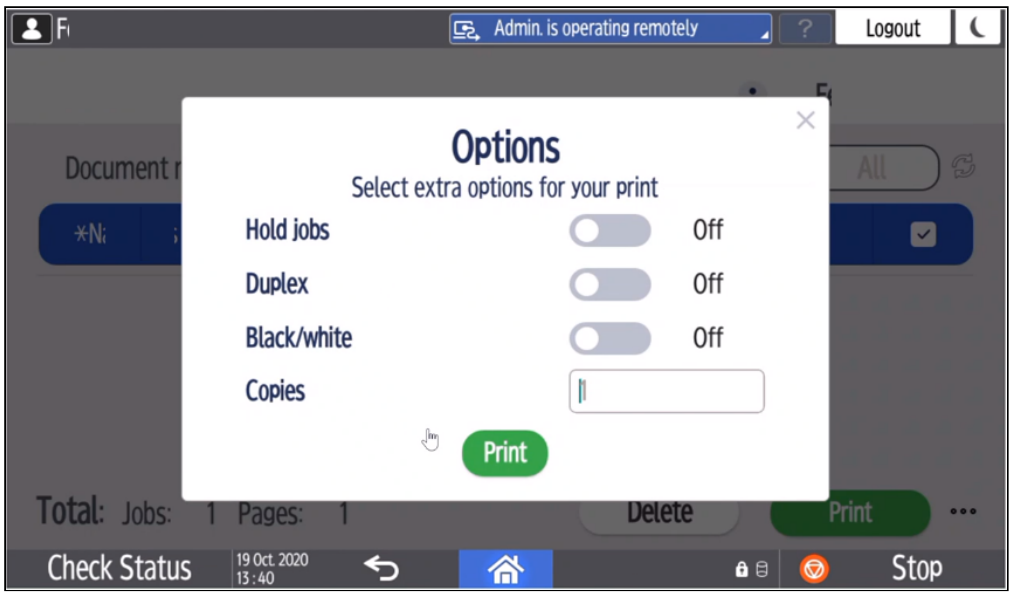
Select the function you would like to be presented after login



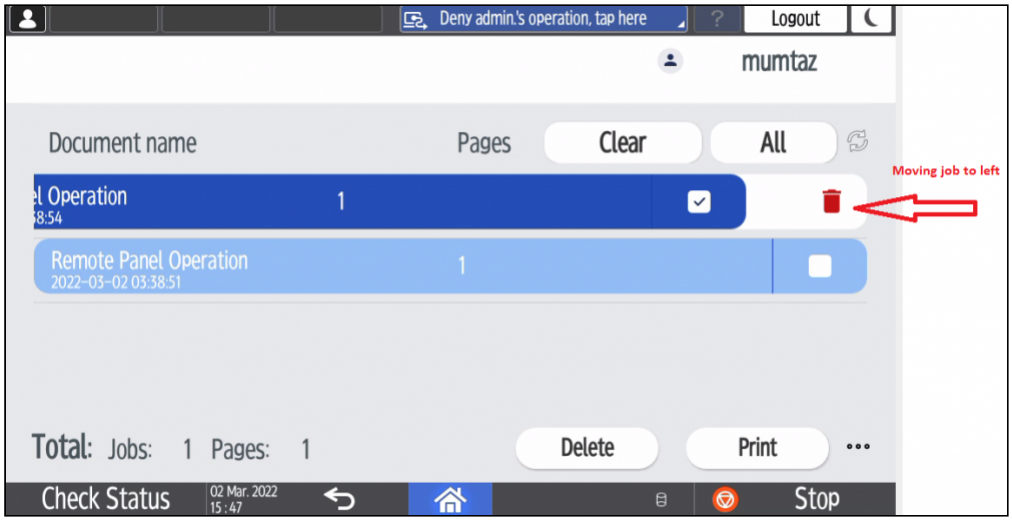
Next time the user Logs in he will be presented with the direct-pull print queue .



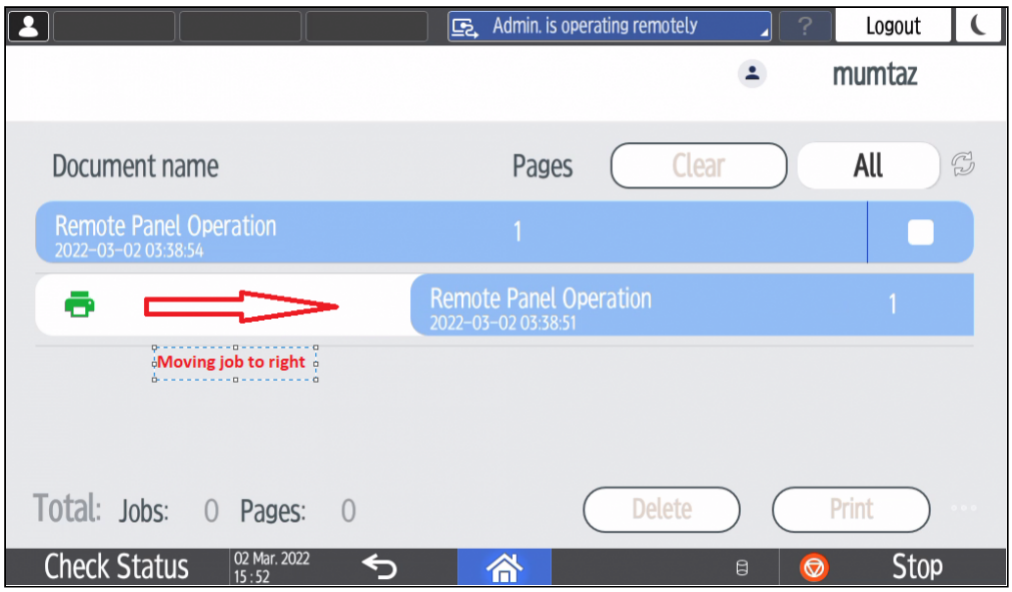
Print options can be changed by pressing ellipsis in the right bottom corner



To delete or print a document, the corresponding buttons can be pressed. To delete the documents in the joblist, they can be flung left:



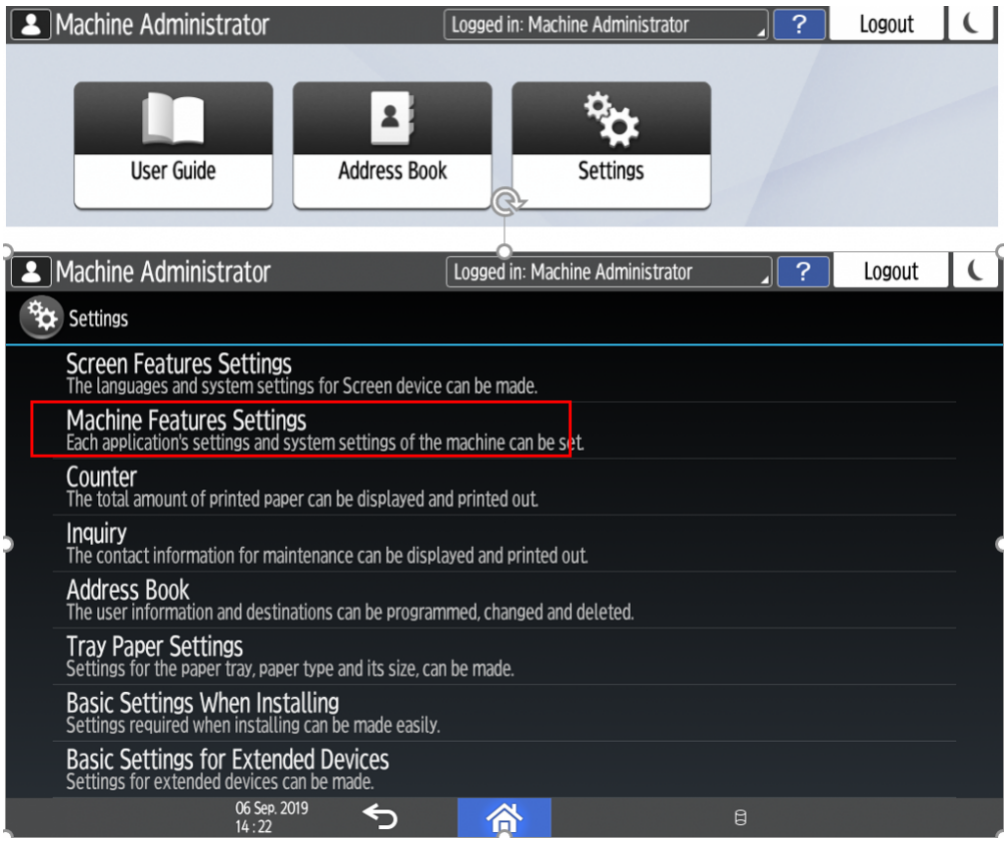
To print, they can be flung right:

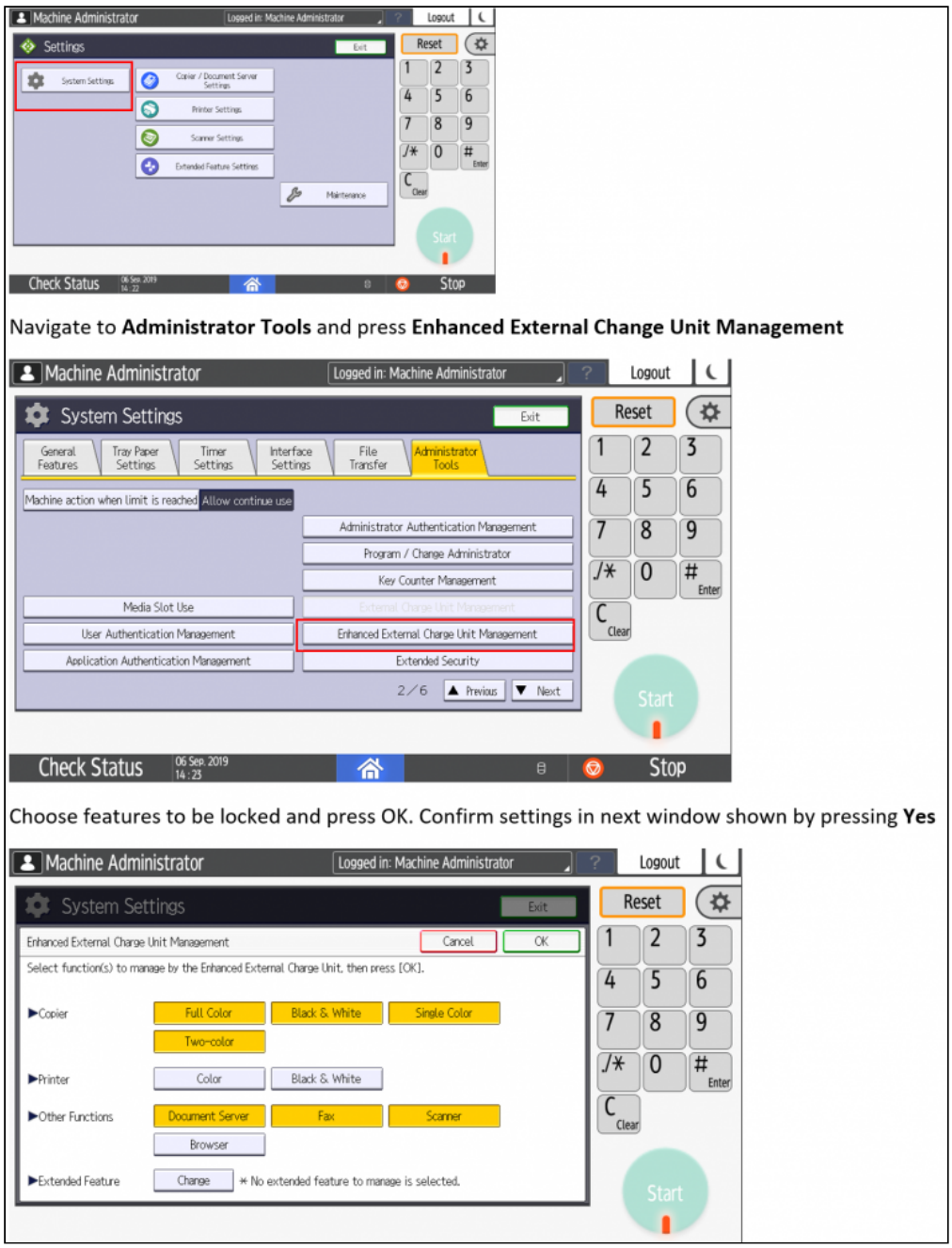


To Lock The SOP Client

If you are using windows print servers with the Ricoh driver and bi-directional feedback on, then printing will stop after the service setting has been applied due to the MFD wanting a user value passed in the print stream

Login as machine administrator. Go to Settings > Machine Features Settings





Note – Make sure though that you do not lock the print functions because the server will not be allowed to print. Also, Java should not be locked since that will prevent the users from unlocking the device

Card Reader Functionality

From the 3.14 version of SAFEQ Cloud the Ricoh Embedded has seen some changes to the cardreader. These changes both affect current installations and new installation.
The cardreader now has to be recognized as a *Proximity Card Reader*.
How to do this is explained here:

> For existing installation these changes will take place when an install and configure is done from the SAFEQ Cloud Web UI.

For a more extensive manual please see this Knowledge-base Article

On SOP G2 devices

- When the Y Soft Ricoh SOP application is installed and configured log ins as device admin.
- Select 'User Tools'
- Enter 'Screen Device Settings Information'
- Select 'External Interface Software Settings'
- Select 'IC card Software Settings' and select 'Proximity Card Reader' Go back and select 'Proximity Card Reader Settings'
- Reboot the Ricoh device

On SOP G2.5 devices

- When the Y Soft Ricoh SOP application is installed and configured log ins as device admin.
- Select 'User Tools'
- Select 'System Settings'
- Select 'Network Interface' on Left and then Scroll Down to 'External Interface Software Settings'
- Select 'Proximity card reader'
- Plug Card Reader In and Select Ok
- Reboot the Ricoh device

Ricoh Embedded (JavaSDK/J) Terminal

Support for this terminal will end on 1st January 2025.

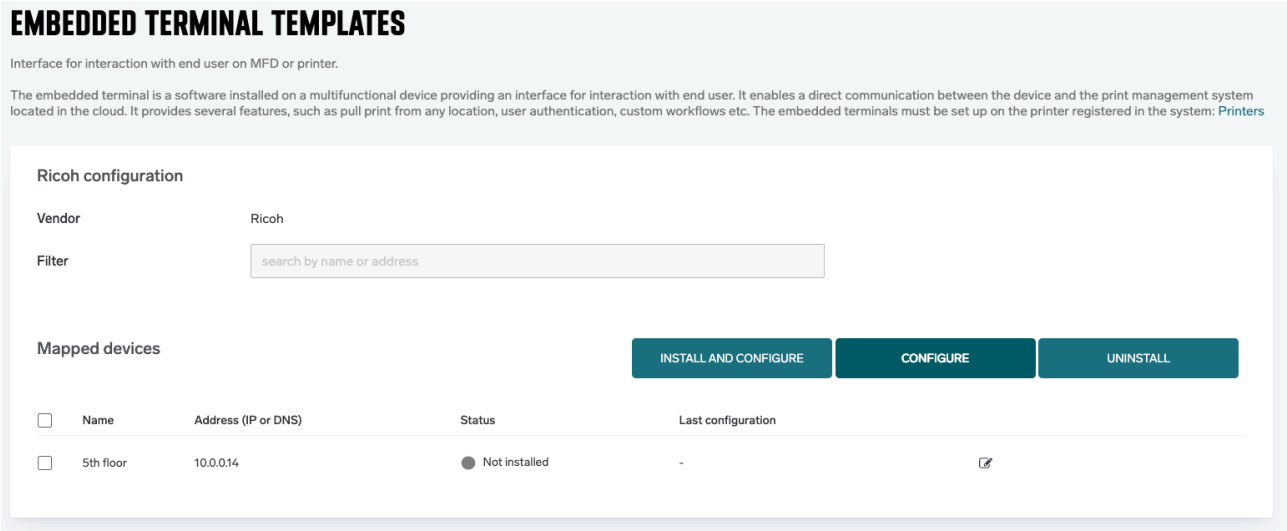
With SAFEQ Cloud version 3.1 onwards, we have updated Ricoh's rxop libararies which requires that SSL is enabled on Ricoh devices prior to installing the embedded client

Ricoh Java SDK/J based embedded client can be installed from SAFEQ Cloud directly to the device where Java SDK/J is available on device by default. Follow steps in section *Install Embedded on Ricoh devices from SAFEQ Cloud*.
For IMC devices, where Java SDK/J is not present by default, additional installation of SD card with Java SDK/J is required. For installation in this scenario, follow steps in section *Sideload Java Embedded on Ricoh IMC Device*.

Before you begin, make sure your secondary gateway is configured according to Secondary Gateway mapping.

Install Embedded on Ricoh devices from SAFEQ Cloud

After setting up the printer on the network and configuring in SAFEQ Cloud, push out the Embedded configuration from the embedded screen in SAFEQ Cloud.



Sideload Java Embedded on Ricoh IMC Device

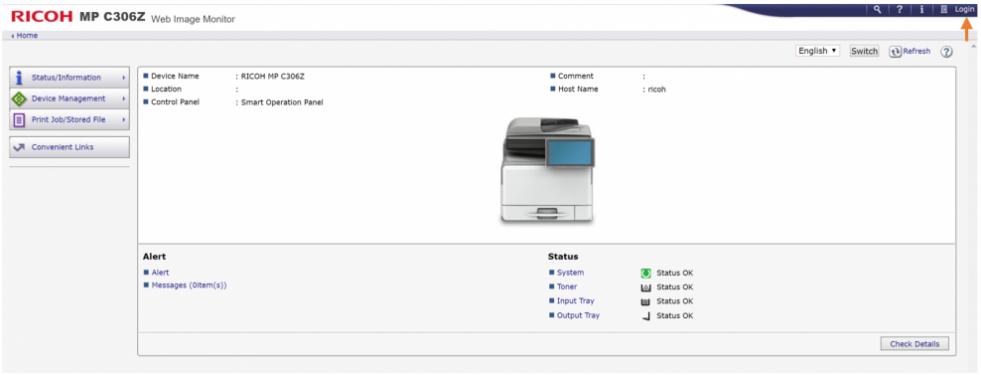
Prerequisites

Get java embedded client bundle (Xlet) with support for SDK 10.xx and forward for supported Ricoh devices:

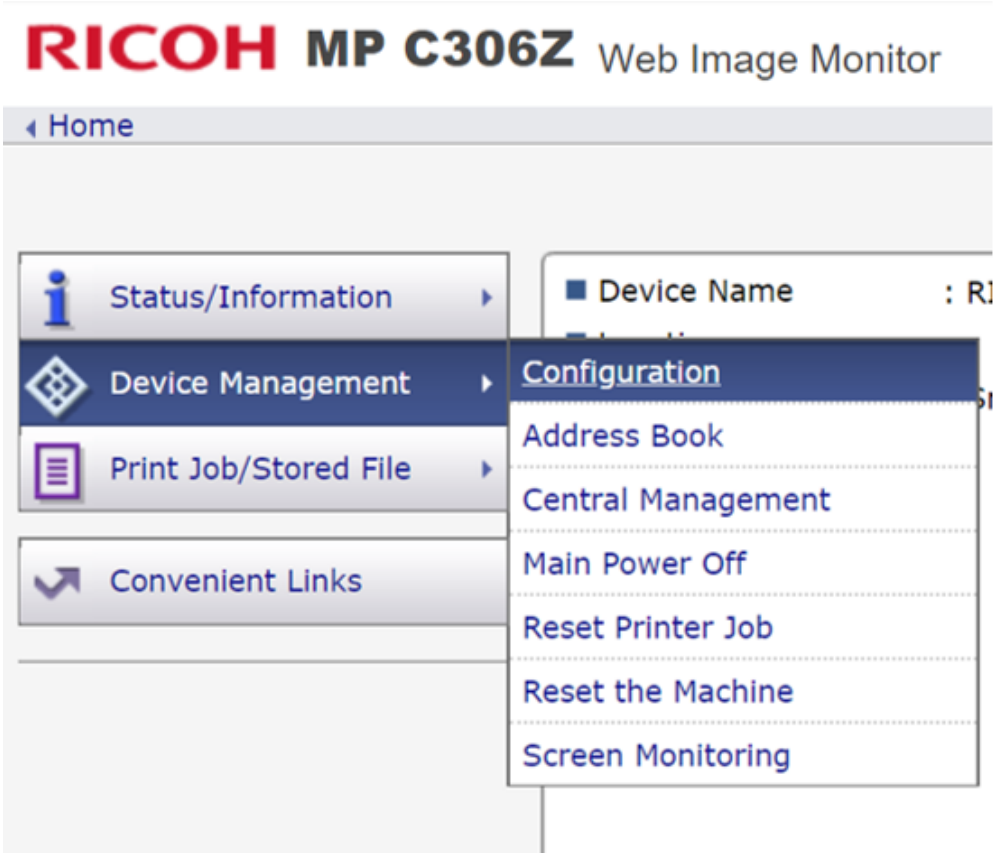
The java embedded client bundle is available on the gateway. The file is located in `/opt/safeqcloud/clients` folder, the command for listing the folder is: `ls -al /opt/safeqcloud/clients/*xlet*`. If you don't have access to an SAFEQ Cloud gateway, contact support@ysoft.com.
For list of supported devices, please visit https://www.ysoft.com/safeq/hardware-compatibility-list/ysoft#cloud.Once logged in, go to SAFEQ Cloud > Technical Documents > Embedded client device support and open pdf file corresponding to the Ricoh device.

Verify if SDK/J is on the Ricoh device:

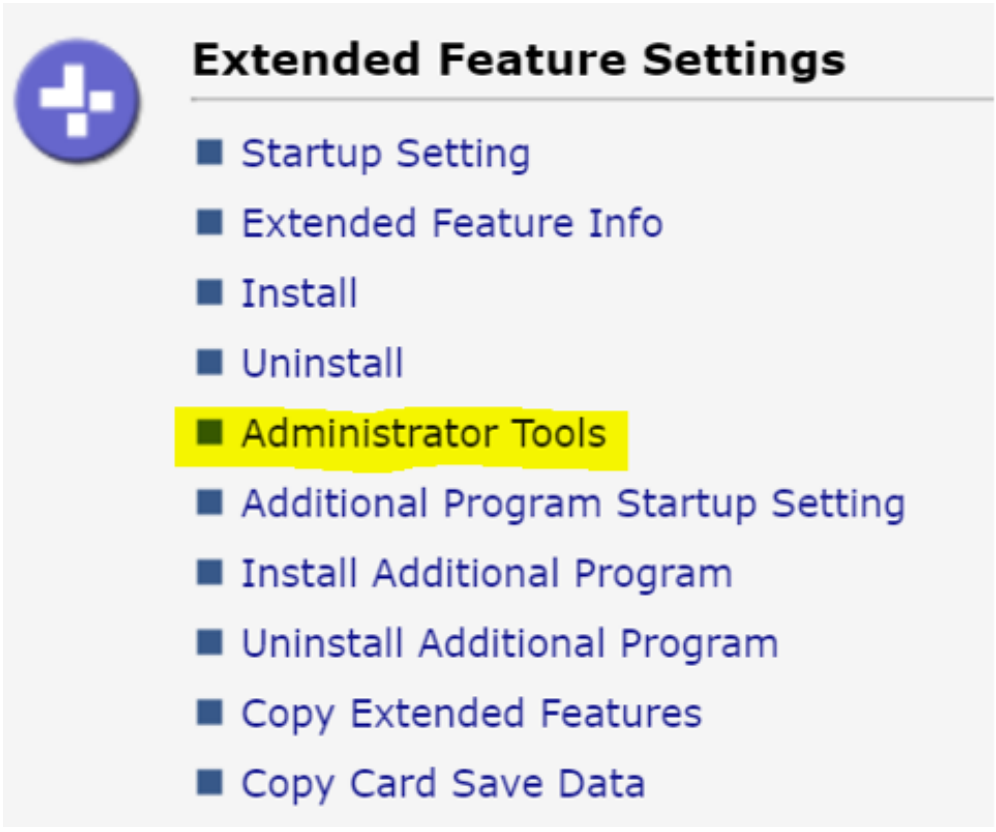
- Go to Ricoh Web Image Monitor (type IP address of Ricoh device in browser)



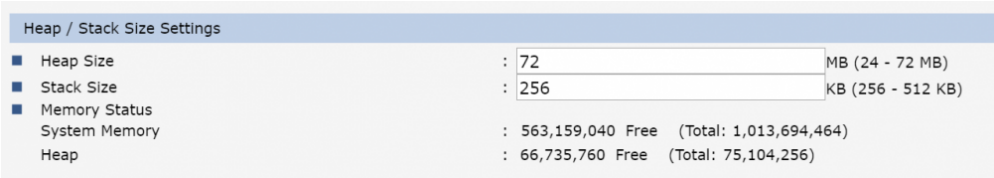
- Login as admin and go to Device Management > Configurations (Some models have direct link to Configuration)



- Navigate to Extended Features Settings > Administrator tools



- Confirm there are memory settings in Heap/Stack Size Settings section in the Heap Size and Stack Size fields. For example, it would look similar to as shown below which says "72" as Heap Size and shows heap in use etc. You can set Stack Size to 512.



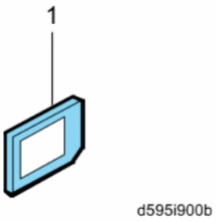
If SDK/J is not running, the fields would be there, but there would be no entries.
NOTE – If SDK/J not running, check that SD card is in the device in the right slot. See section on Installation of SD card below. Otherwise, if SDK/J is present and running, follow steps in section Preparation

Installation of SD card and SDK/J

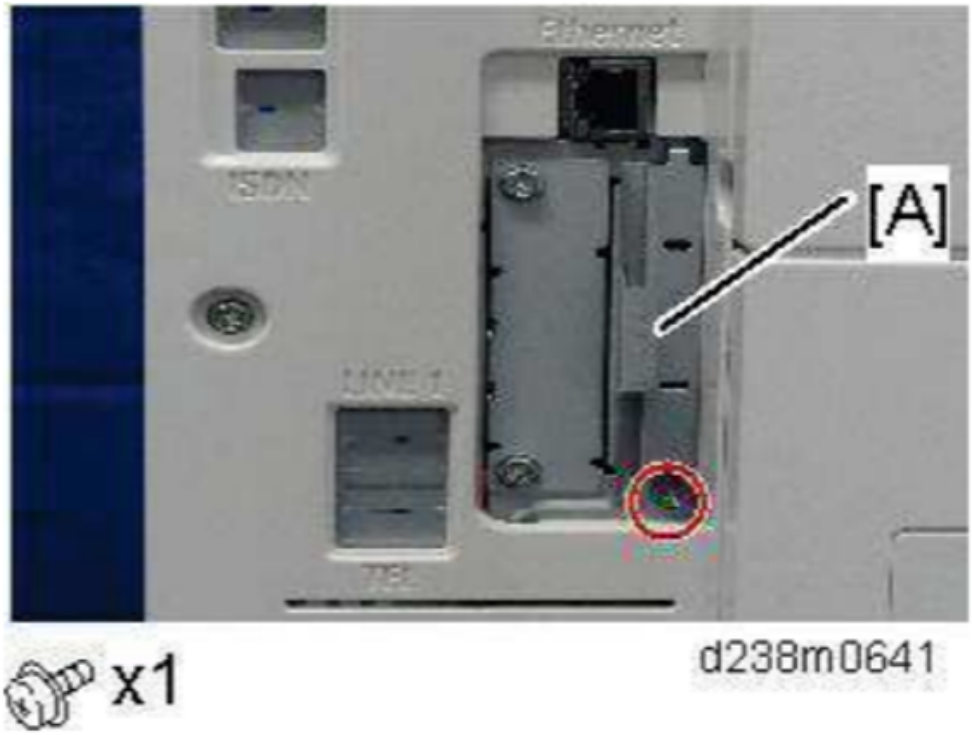
VM CARD Type M37 (D3GF-32)

Component Check

No.	Description	Q'ty
1	SD Card	1



1. Installing the SD card – Turn OFF the device and remove SD card slot cover [A]



2. Install the VM Card in SD card slot2 [A: Lower Slot]

3. Reattach the SD card slot cover and turn ON device

Installing the Java Platform

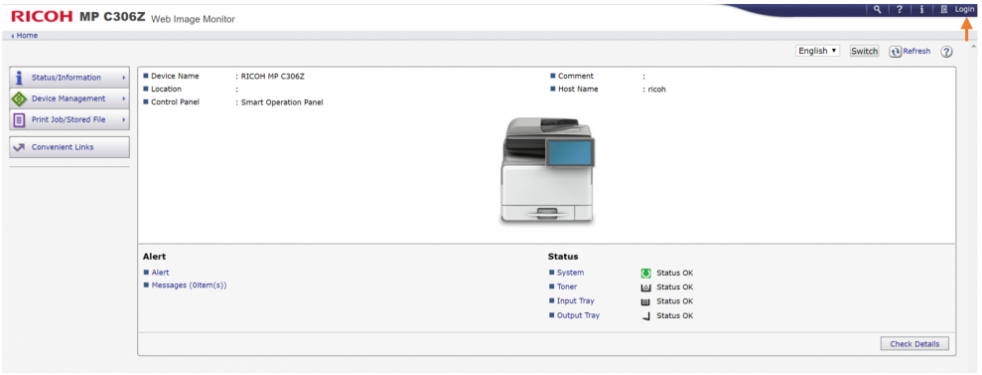
Insert the SD card and turn the main power on as described in section above, then the Java platform is automatically installed. Automatic installation takes around 1-2 minutes.
NOTE – If you turn the power off during installation, the VM card may be damaged.

Preparation

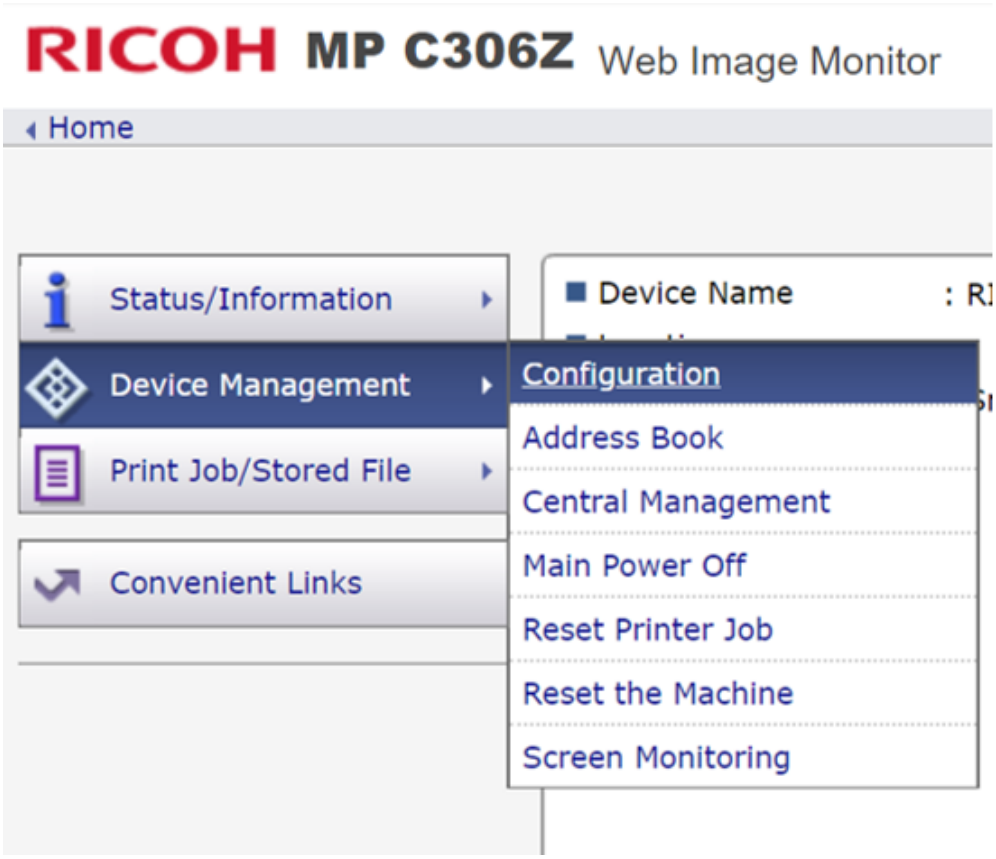
For every Ricoh device, push the configuration with the Embedded Configuration action. For configuring the Embedded Configuration follow this link and see the section `Setting the Embedded Configuration`.

Installation Steps

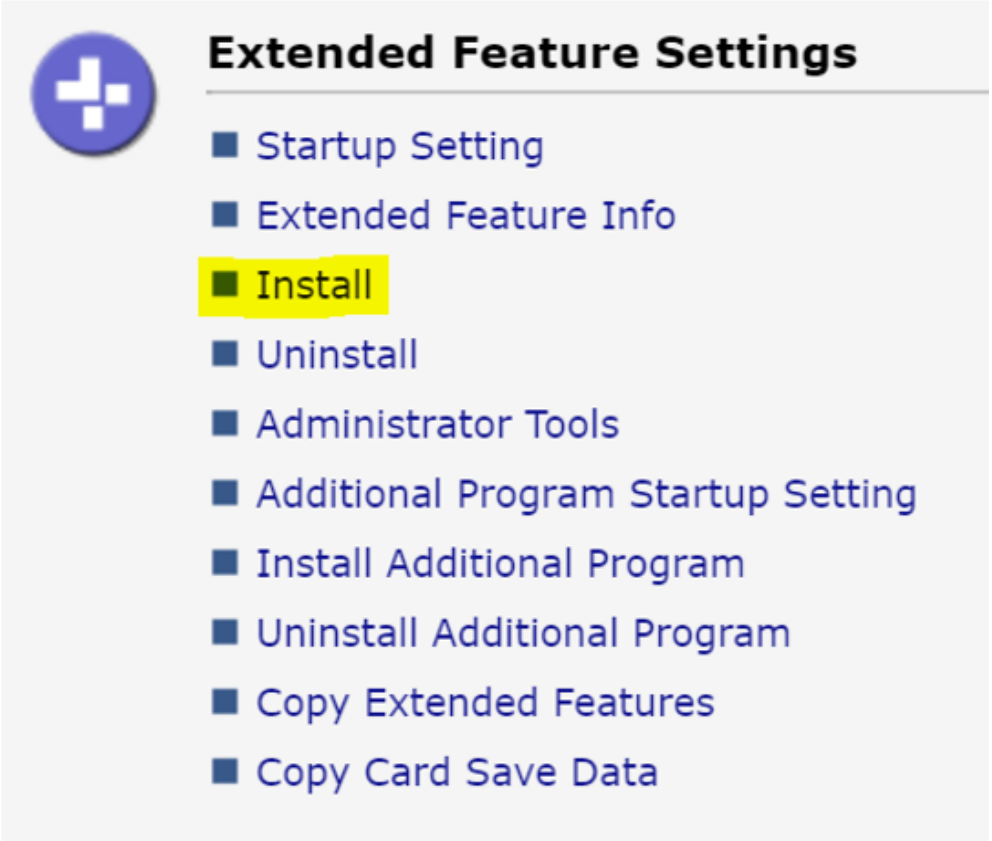
1. Login to Ricoh Web Image Monitor (type IP address of Ricoh device in browser) as administrator



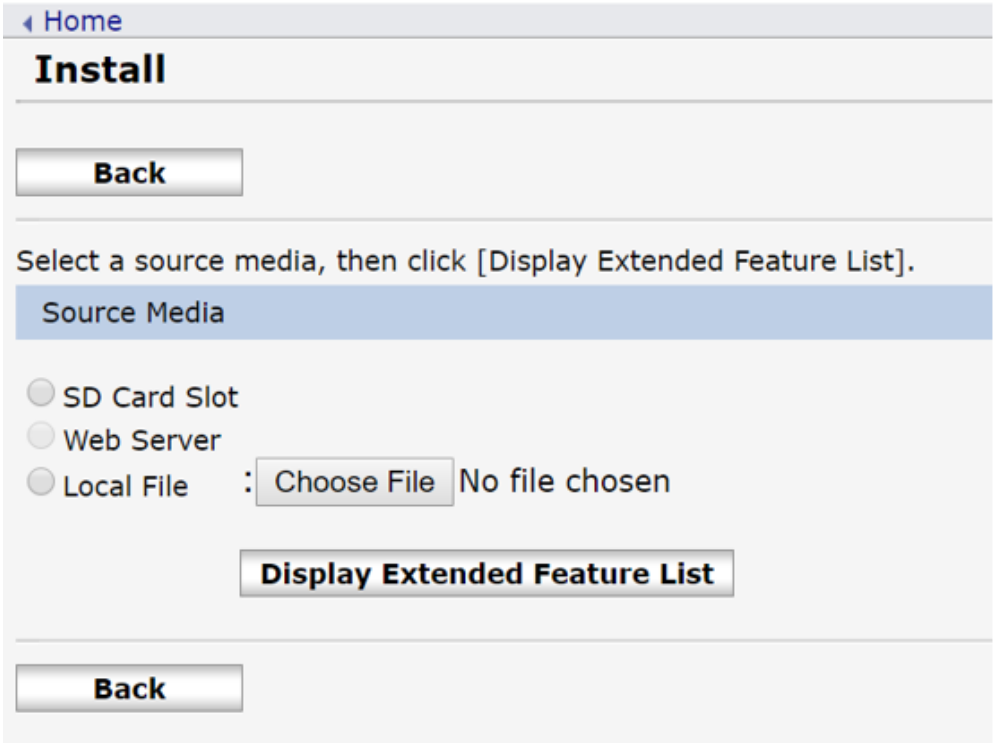
2. Go to Device Management > Configurations (Some models have direct link to Configuration)



3. Navigate to Extended Feature Settings and press Install. It will open a new page

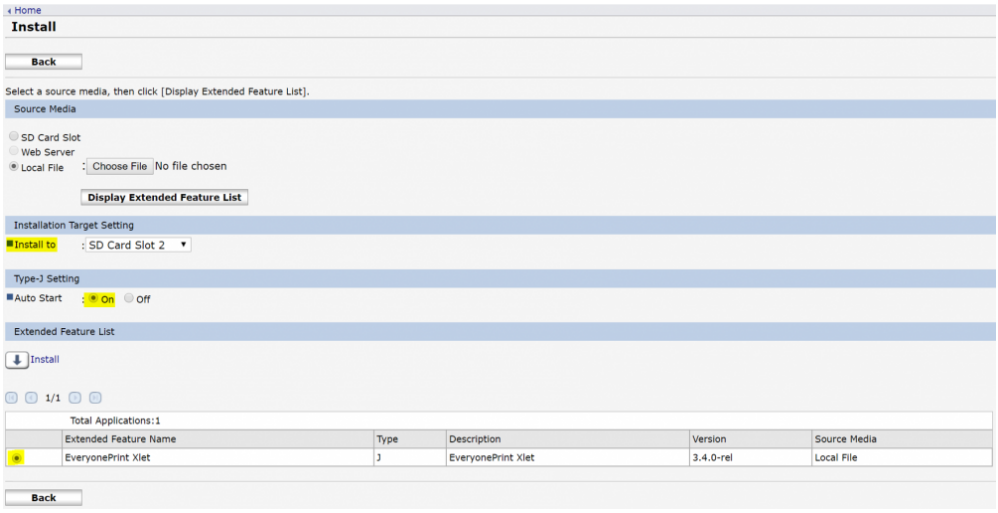


4. Choose Local File and press 'Choose File' button

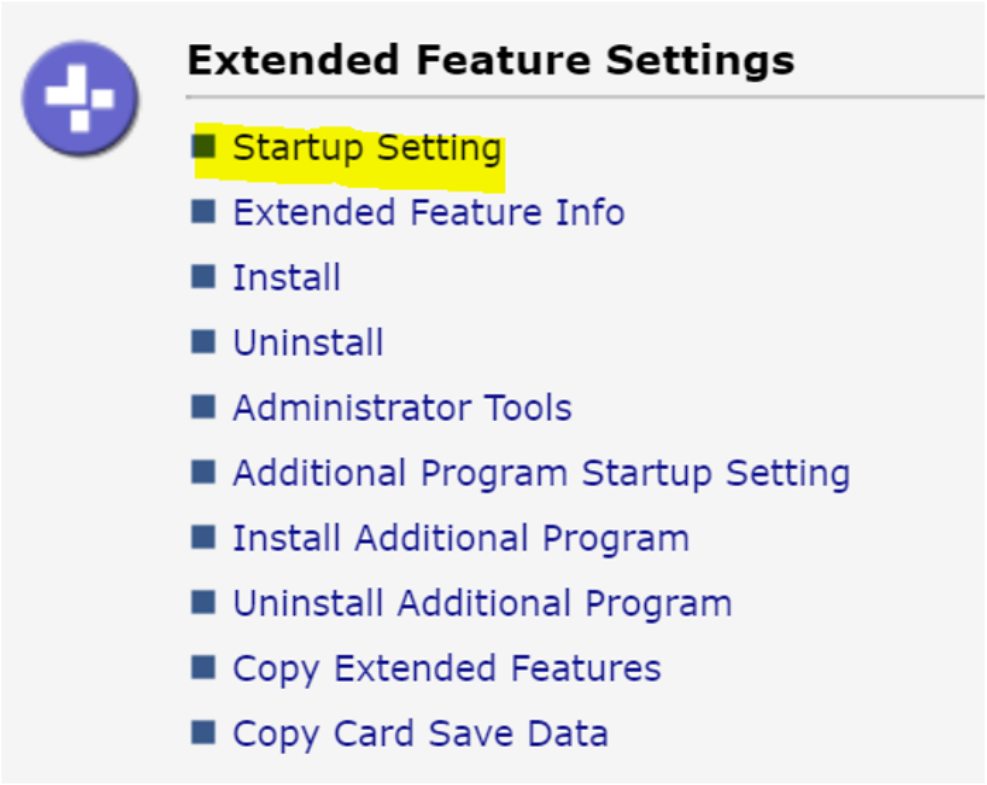


5. Browse the embedded client prepared from section **Preparation** above and press Open
6. Press Display Extended Feature List and wait until the new page loads
   Note – Only press the button ONCE!!
7. On the new page –

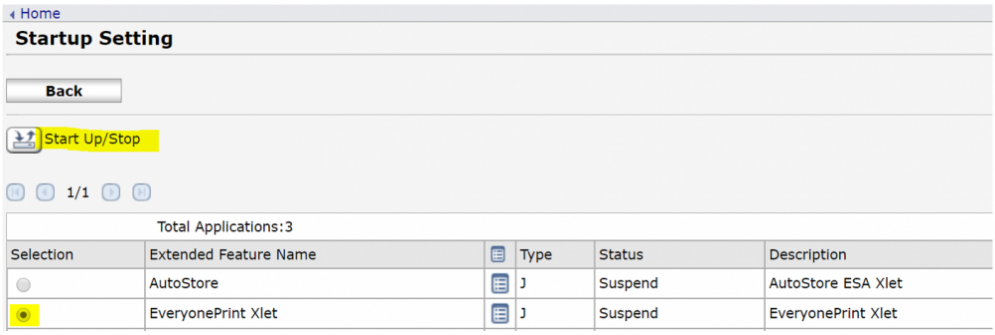
- in Installation Target Settings, select the location where SDK/J was installed in section **Installation of SD card and SDK/J**
- Enable Auto Start
- Select Y Soft Xlet
- Press Install and confirm installation when asked



- Once the installation procedure is completed press **Back** and go to **Startup settings**



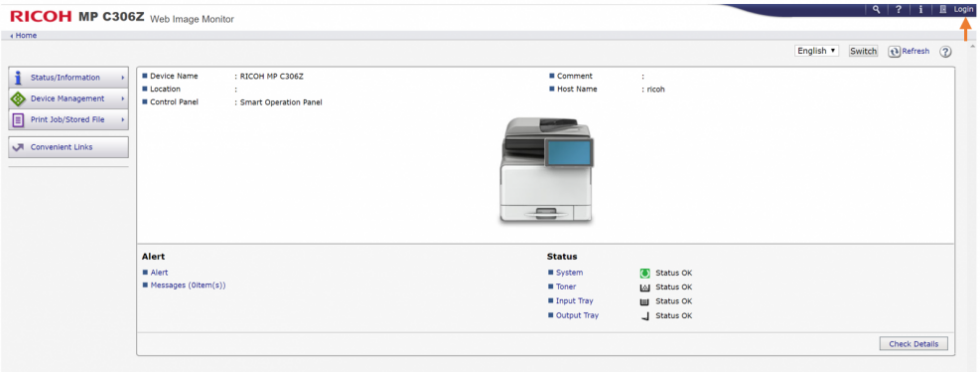
- Select **Y Soft Xlet** and press **Start Up/Stop**



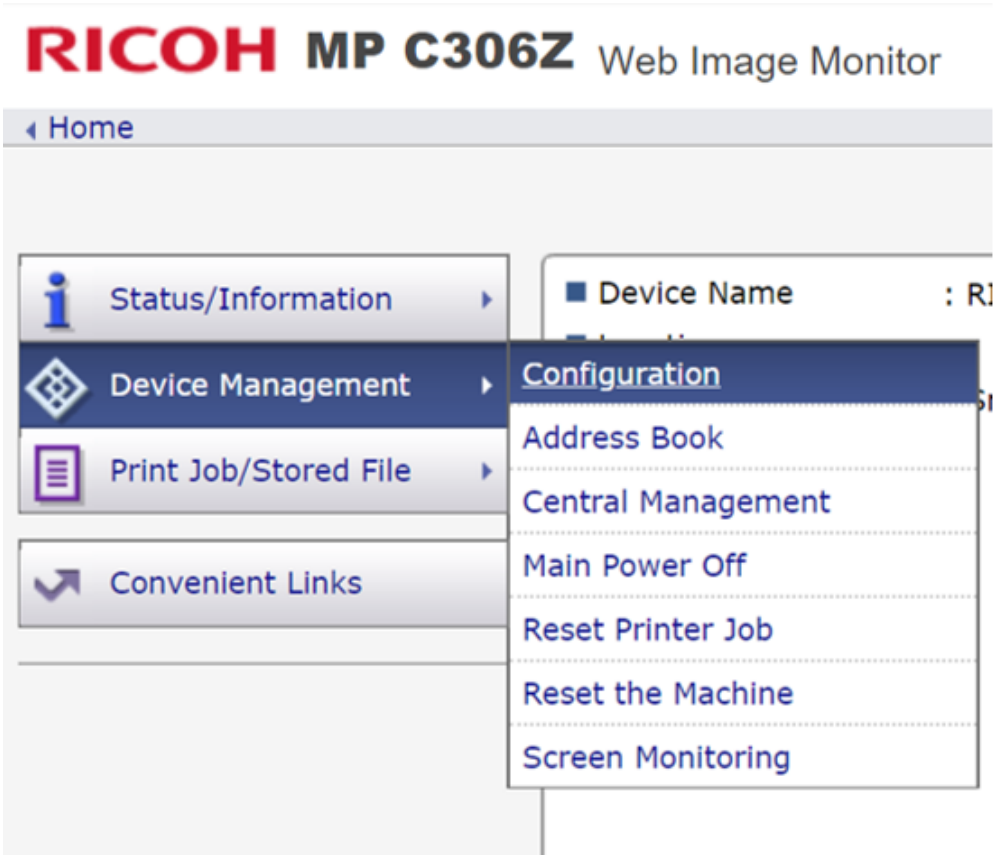
Locking the device

1. On Web Monitor

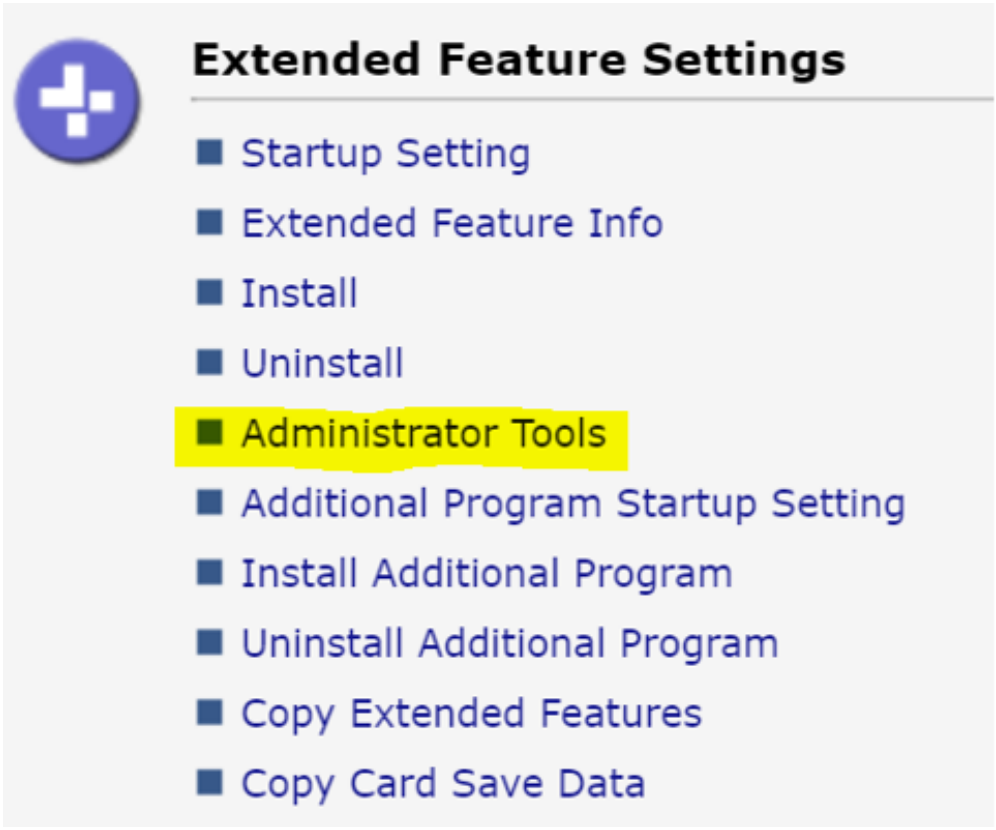
- On Ricoh Web Image Monitor (type IP address of Ricoh device in browser) login as administrator



- Go to Device Management > Configurations (Some models have direct link to Configuration)



- Navigate to **Extended Feature Settings** and press **Administrator Tools**. It will open a new page

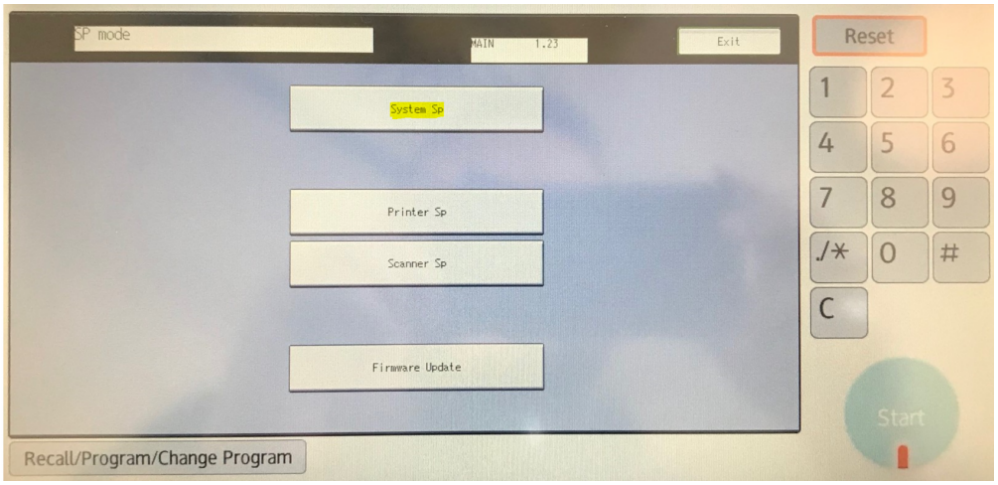


- Under **Select Available Functions** section, make **"PanelService API"** as **"Active"**

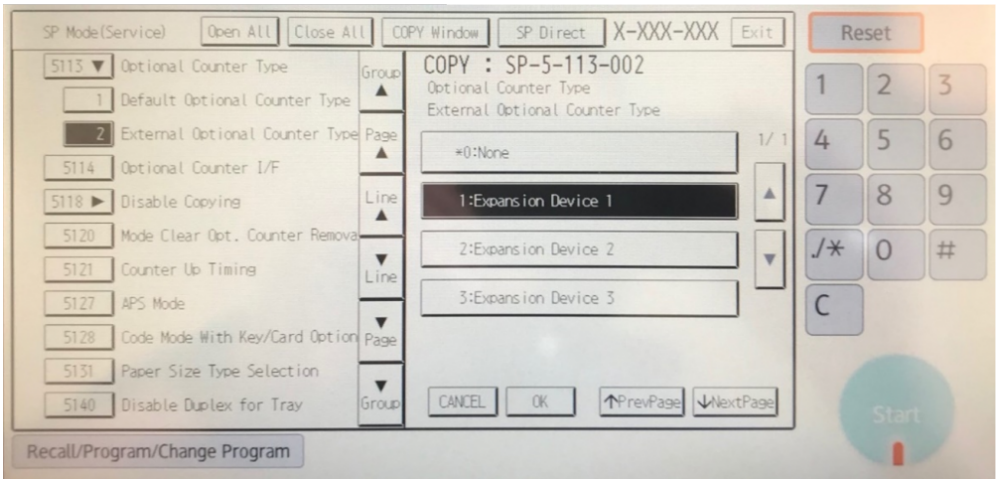
- Press **Apply** and **Back**

1. On Ricoh Device

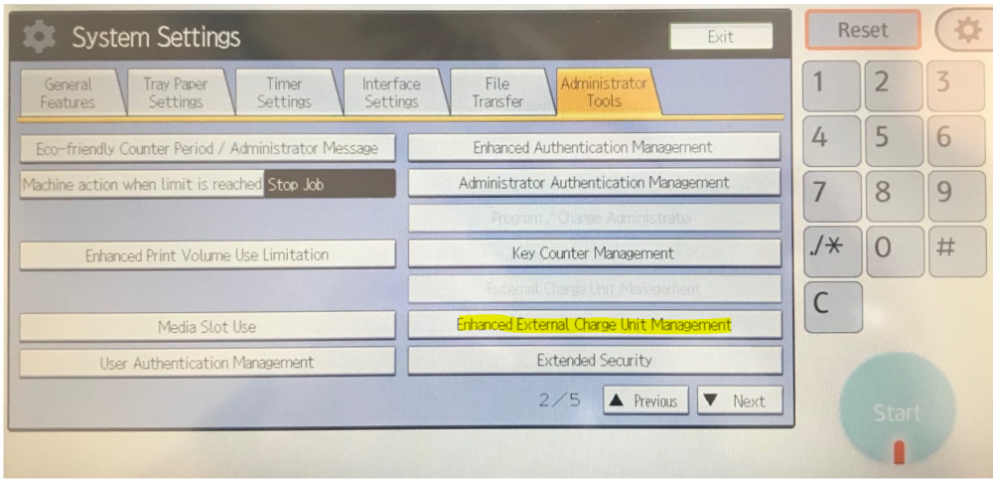
- On Ricoh device, go to **Service Menu** to enable lock. To go to Service Menu on your device follow instructions given by Ricoh. Ensure that all prerequisites stated in section 2.1 above are met.
- In Service Menu, press **System Sp**



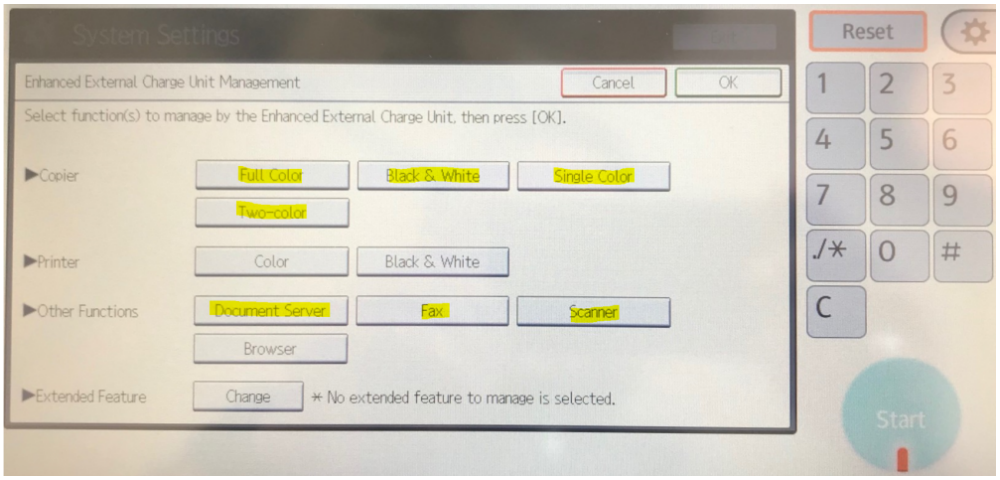
- Then go to menu **5113 – Optional Counter Type** and choose 2 – External optional Counter Type and then 1 – Expansion Device 1



- Press **OK** and **Exit** to exit service menu
- Now, go to **System Settings** in Administrative interface on device. Navigate to **Administrator Tools** and press **Enhanced External Change Unit Management**



- Then select the features that you wish to be locked without authentication.



Note – Make sure though that you do not lock the print functions because the server will not be allowed to print. Also Java should not be locked since that will prevent the users from unlocking the device.

Sharp Terminals

Sharp Gen 1 Terminal

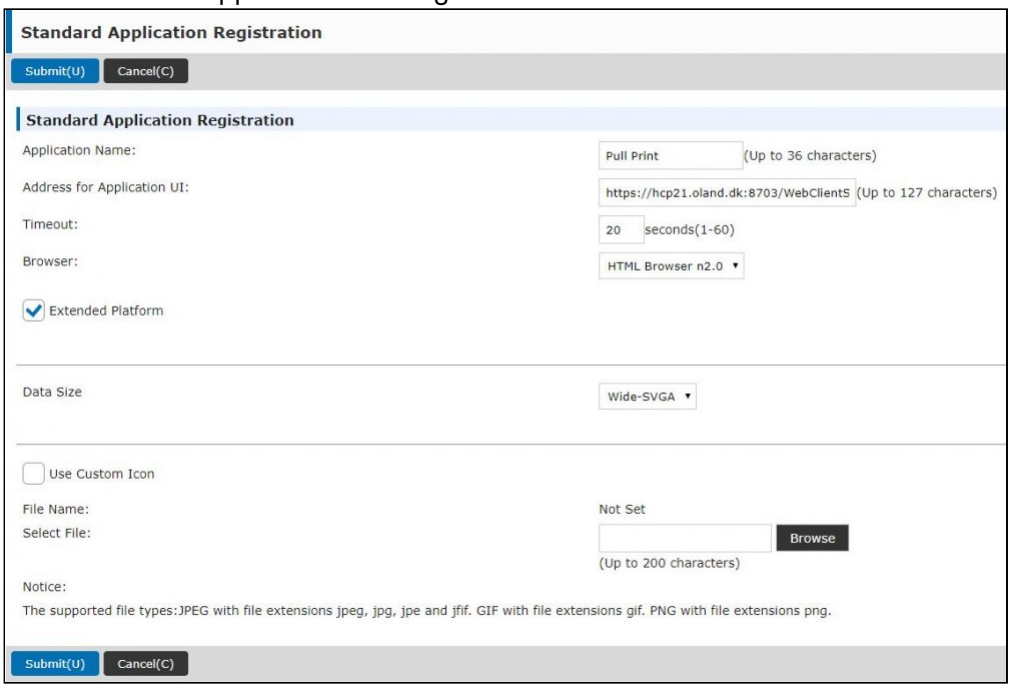
Prerequisites

- Your secondary gateway is configured according to Secondary Gateway mapping.
- Terminal Client service is created with the SAFEQ Cloud embedded terminal integration.
- Document output service is created.
- The sharp Embedded client is created. See Embedded Terminals' configuration.
- A Printer is created (using above mentioned Terminal Client service, Document output service, and created Sharp Embedded Client). See Printers.

Installing and configuring the terminal

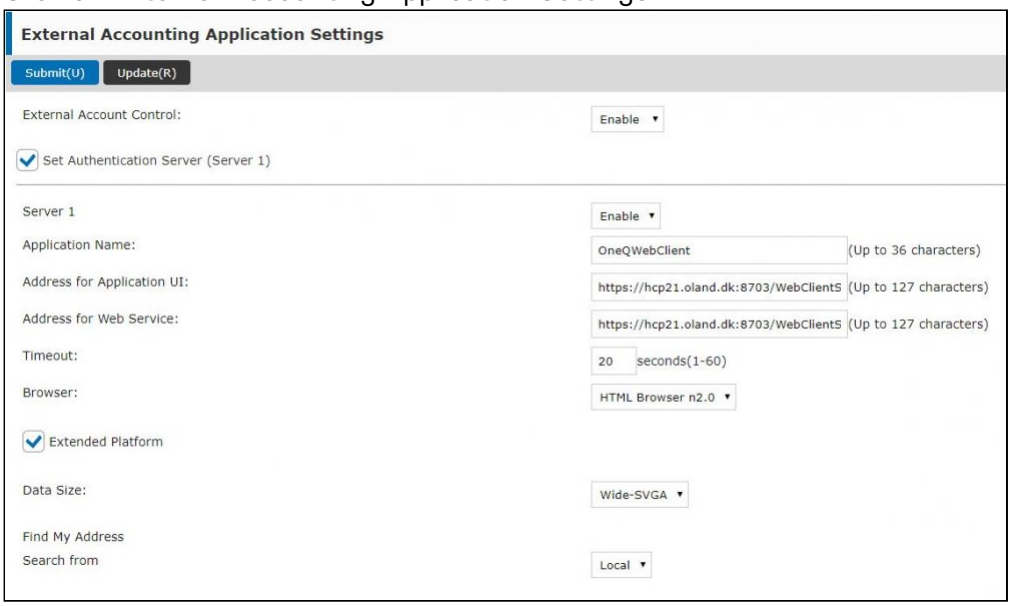
1. Log in as an administrator to the MFD web interface.
2. Go to **System settings**.

3. Click **Sharp OSA settings.**
4. Click **Standard Application Settings** and click **Add**.



5. Enter a desired application name.
6. Enter the address for application UI as `https://'server name':8703/WebClientSharp/HomeAdapterServlet?addr=<MFD_adress>`. Example: `https://print.acme.com:8703/WebClientSharp/HomeAdapterServlet?addr=192.168.100.101` .
   - server name - The fully qualified domain name of the SAFEQ Cloud Gateway.
   - MFD_address - The IP address or hostname of the MFD.
   - addr - If the MFD is configured in SAFEQ Cloud Web UI using the IP address, this parameter is optional. If it's configured using the hostname, this parameter is mandatory.
7. Select **Extended Platform**.
8. Click **Submit**.

9. Click on External Accounting Application Settings.

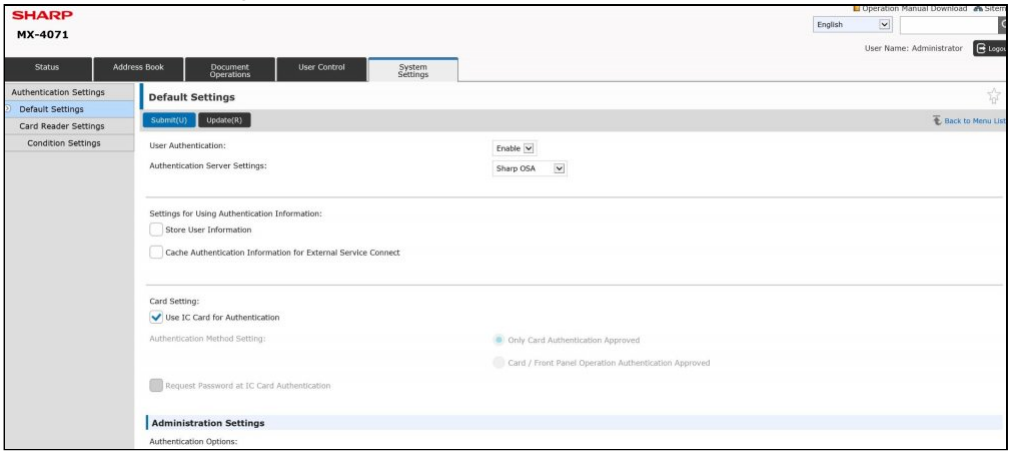


10. Enable External Account Control.
11. Select Set Authentication Server (Server 1).
12. Enable Server 1.
13. In Application Name, enter *OneQWebClient*.
14. Enter the address for application UI in the following format: `https://'server name':8703/WebClientSharp/LoginAdapterServlet?addr=<MFD_adress>`. Example: `https://print.acme.com:8703/WebClientSharp/LoginAdapterServlet?addr=192.168.100.101`.
15. Enter the address for Web Service in the following format: `https://'server name':8703/WebClientSharp/ws?addr=<MFD_adress>`. Example: `https://print.acme.com:8703/WebClientSharp/ws?addr=192.168.100.101`.
    - server name - The fully qualified domain name of the SAFEQ Cloud Gateway.
    - MFD_address - The IP address or hostname of the MFD.
    - addr - If the MFD is configured in SAFEQ Cloud Web UI using the IP address, this parameter is optional. If it's configured using the hostname, this parameter is mandatory.
16. Select Extended Platform.
17. Change Find My Address to Local.
18. Click Submit.
19. Restart the MFD.
20. If you haven't done so already, create the Printer and the Embedded configuration in SAFEQ Cloud Web UI. See Printers and Embedded Terminals' configuration. These settings are all that

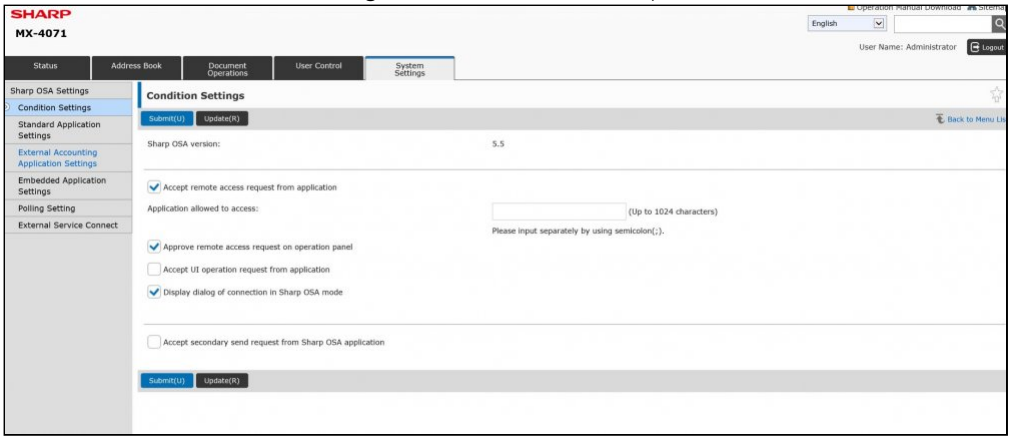
is needed to install and configure the terminal. You don't need to click **Install and Configure** from the SAFEQ Cloud Embedded Configuration.

To deploy on newer Sharp devices like MX-4061 and MX-4071, configure also the following settings:

1. Go to **Authentication settings** > **Default Settings**.
2. Enable **User Authentication**.
3. Set **Authentication Server Settings** to **Sharp OSA**.
4. In the **Card Settings** section, enable **Use IC Card for Authentication**.



5. Go to the **Conditions Settings** and select all the options as shown in the screenshot.



6. If you wish to use a custom logo on the terminal, name the file with the logo *logo.png* and place it in `/opt/safeqcloud/conf/sharp.`

Sharp Gen 2 Cloud Terminal

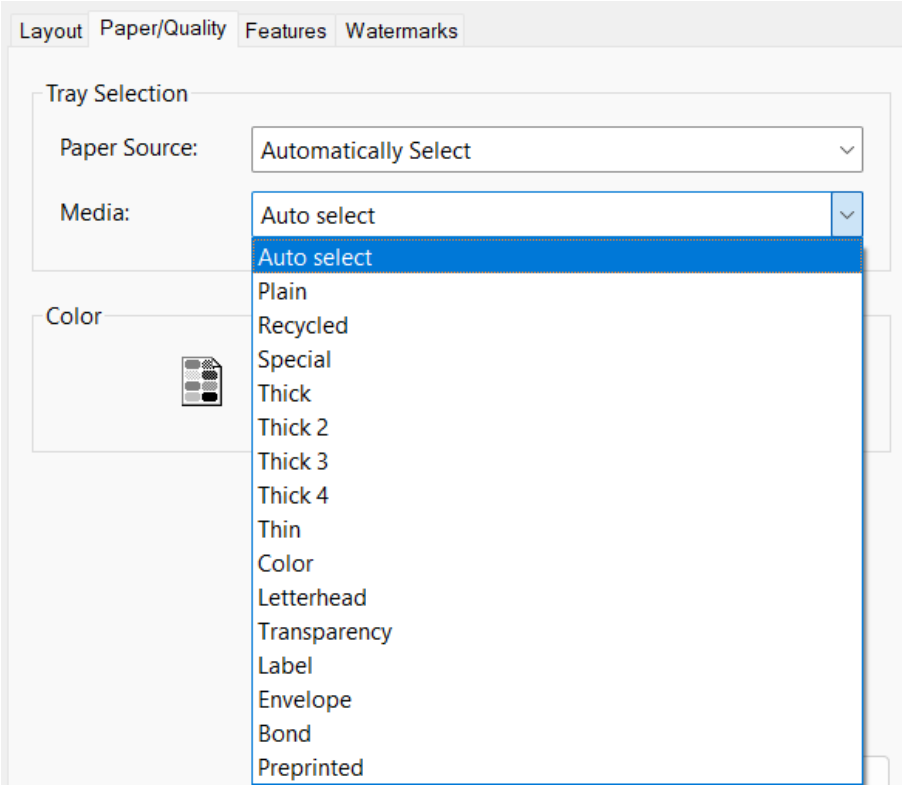
Prerequisites

- The MFD must have OSA 5.5 or higher.
- Make sure that you have Cloud Terminal Integration enabled. For information on how to do this, see Enable Cloud terminal integration.

Limitations

Cloud print

- If a finishing option is not available in print API, it will be omitted.
- Media type selection is not supported.



- Toner saving (economy printing) is not supported.
- Specific paper size is supported only for the following formats: A3, A4, A5, A6, B4, B5, Executive, Legal, Letter, Ledger, Tabloid
- Tray 6 input type is not supported.
- Borderless print is not supported.
- The stapling and punching functionality can vary based on the type of finisher, paper size, and paper orientation, which may result in outcomes that differ from expectations.
- The UpperRight stapling option is not supported.

Authentication

- Users cannot log out via their cards
- Authentication can fail at printers that do not support TLSv1.3. For how to configure these printers properly, see the *Troubleshooting* section of this page.

Scan

- When scanning from the glass, a prompt to place a new original appears every time, regardless of whether the Merging Originals function is used.

Uninstallation

- When uninstalling the terminal using Terminal Deployment Tool during an ongoing user session at the MFD, the action will fail and uninstallation needs to be performed manually afterwards.

Installing the cloud terminal

Manual installation

The terminal can be installed manually, using installation packages and the MFD's web interface.

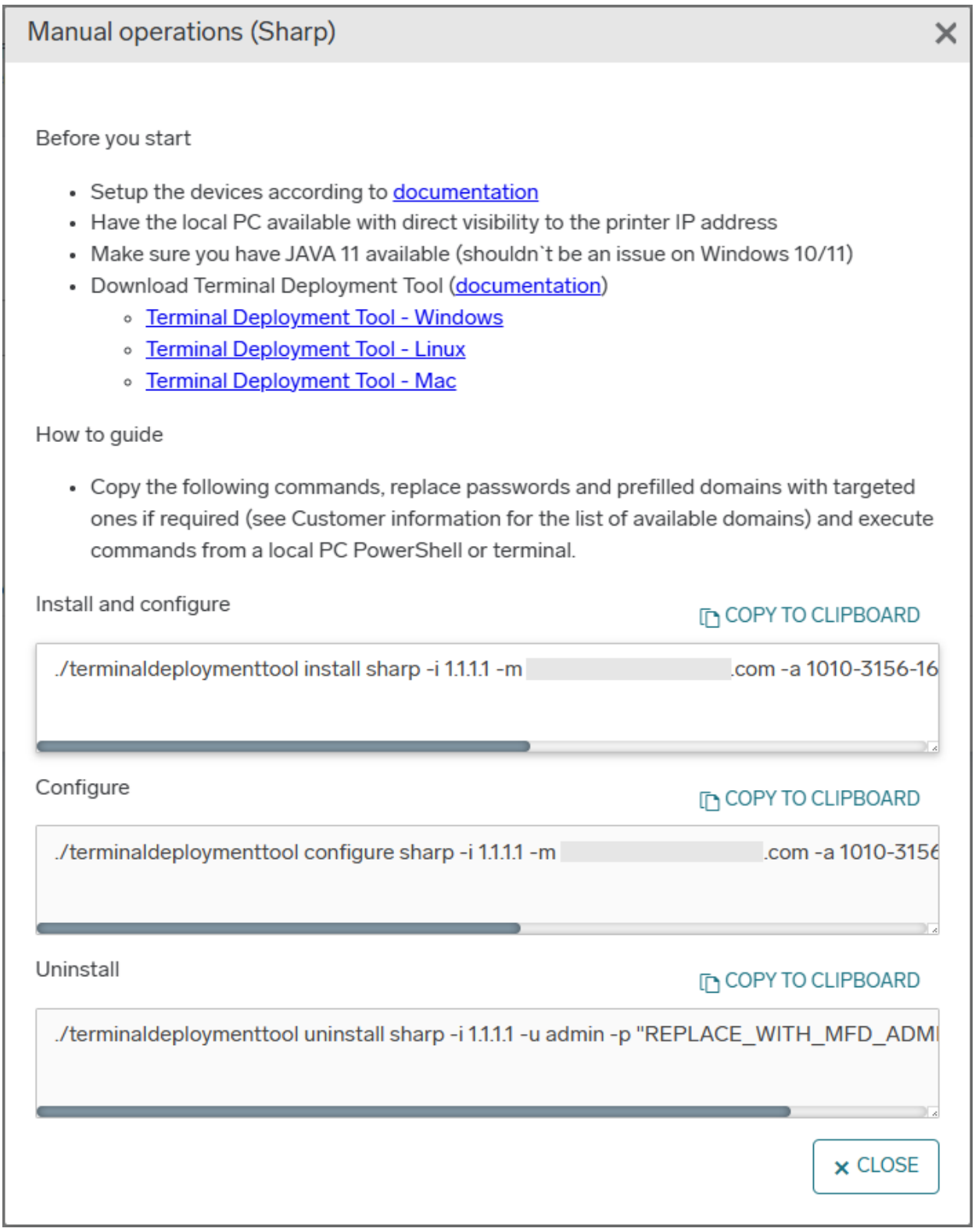
Follow the procedure described in section Manual installation.

Installing using Terminal Deployment Tool

> Please note that Sharp Cloud Terminal installation via TDT is currently in beta phase.

The terminal can be installed using the Terminal Deployment Tool.

1. Start with adding your Sharp MFD and creating the embedded configuration in SAFEQ Cloud Web UI. See section *Adding the Sharp printer and Embedded configuration in SAFEQ Cloud Web UI* of this guide.
2. Go to **Printers** > **Embedded templates** and open the newly created embedded configuration.
3. Click **Manual operations**.
4. Follow the instructions in the dialogue window.



Examples:

Install
.\terminaldeploymenttool.bat install sharp -m <DOMAIN> -a <API_KEY> -i <MFD_IP> -u <MFD_ADMIN_USER> -p <MFD_ADMIN_PASS>

Configure

.\terminaldeploymenttool.bat configure sharp -m <DOMAIN> -a <API_KEY> -i <MFD_IP> -u <MFD_ADMIN_USER> -p <MFD_ADMIN_PASS>

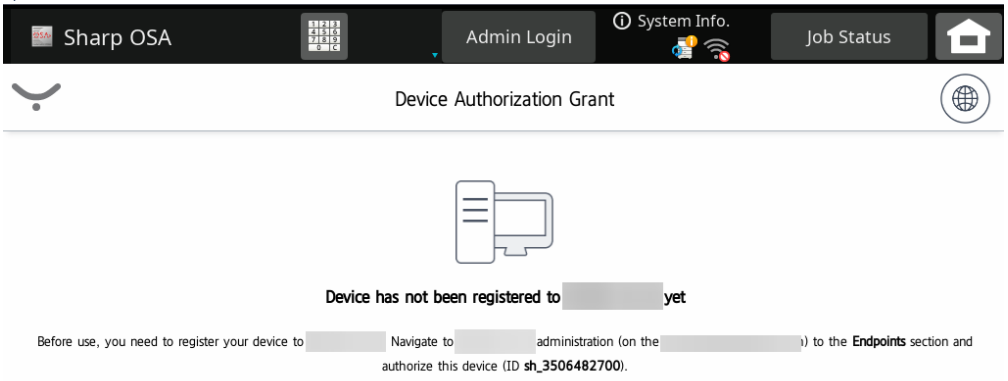
Uninstall
.\terminaldeploymenttool.bat uninstall sharp -i <MFD_IP> -u <MFD_ADMIN_USER> -p <MFD_ADMIN_PASS>

The example commands are generated regardless of the operating system.

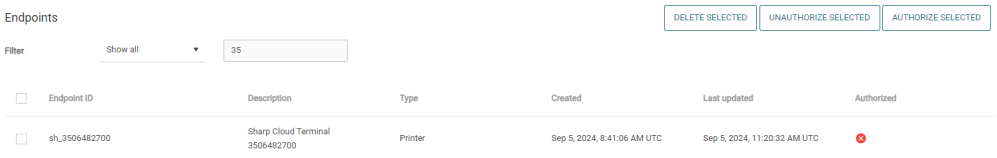
For Windows, the full file name should be used in the command so that each command starts with `./terminaldeploymenttool.bat`

Registering the cloud terminal in SAFEQ Cloud Web UI

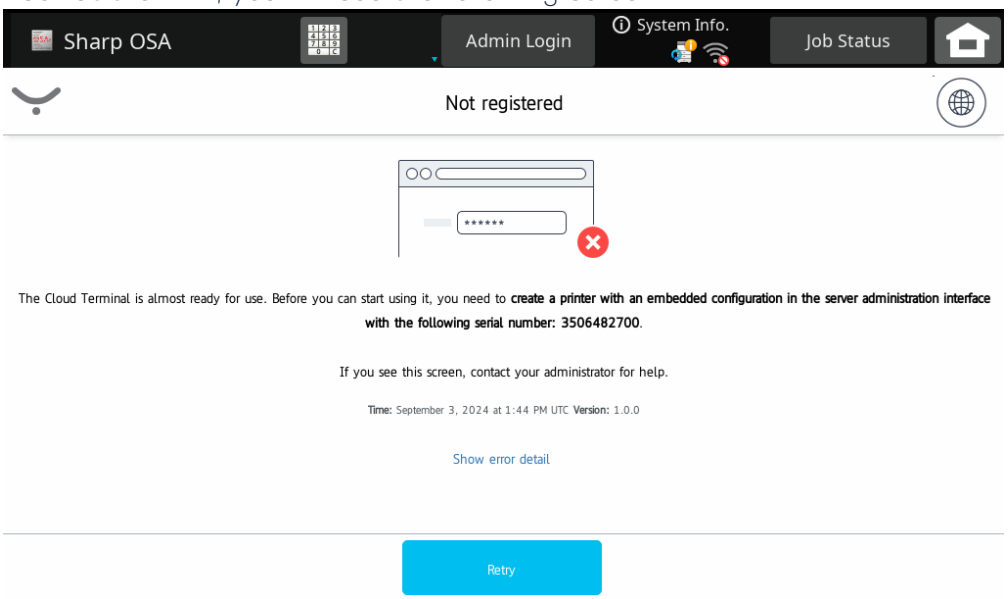
1. Upon installing the terminal, you will see a screen with the **Serial Number** of the device (prefixed with **sh_**). Note down the ID number.



2. In SAFEQ Cloud web UI, go to **Security > Endpoints** and find the entry with ID number that you noted in the previous step. Select the entry and click **Authorize selected**.



3. Back at the MFD, you will see the following screen:

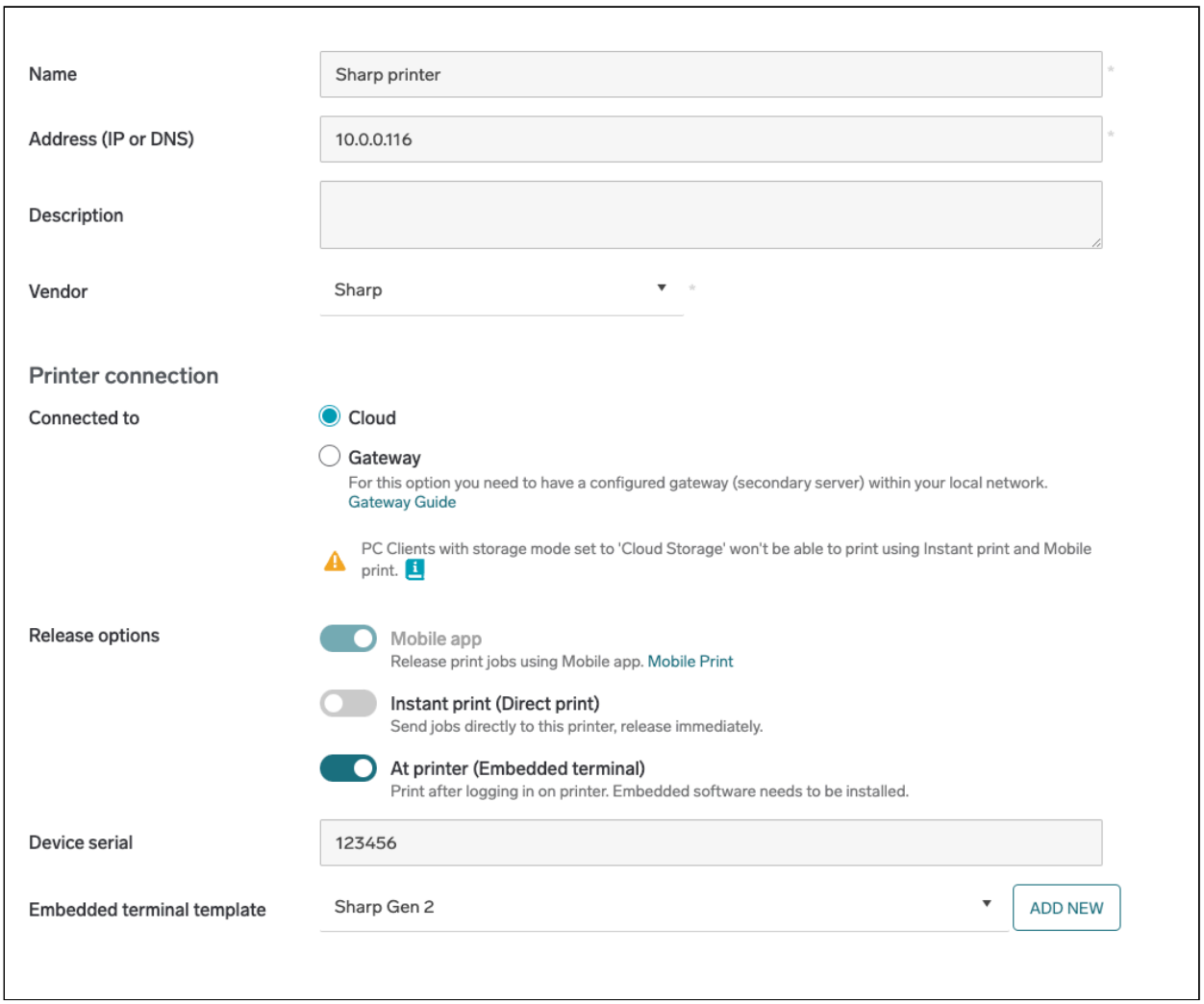


Adding the Sharp printer and Embedded configuration in SAFEQ Cloud Web UI

These steps are optional and if not performed, the Sharp printer will be added automatically after the endpoint is authorised, see *Registering the cloud terminal in the SAFEQ Cloud Web UI* section of this page.

If you want to connect the MFD that is already connected and registered to a different SAFEQ Cloud account, you must remove the Embedded applications in the Sharp OSA settings and add them again (see the *Installing the cloud terminal* section of this guide).

1. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
2. If not done already, create an embedded configuration for your Sharp MFD(s) by clicking **Add**.
3. In **Vendor**, select **Sharp**.
4. In **Application type**, select **Sharp Gen 2**.
5. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.
6. Go to **Printers**.
7. Click **Add**.
8. In **Vendor**, select **Sharp**.

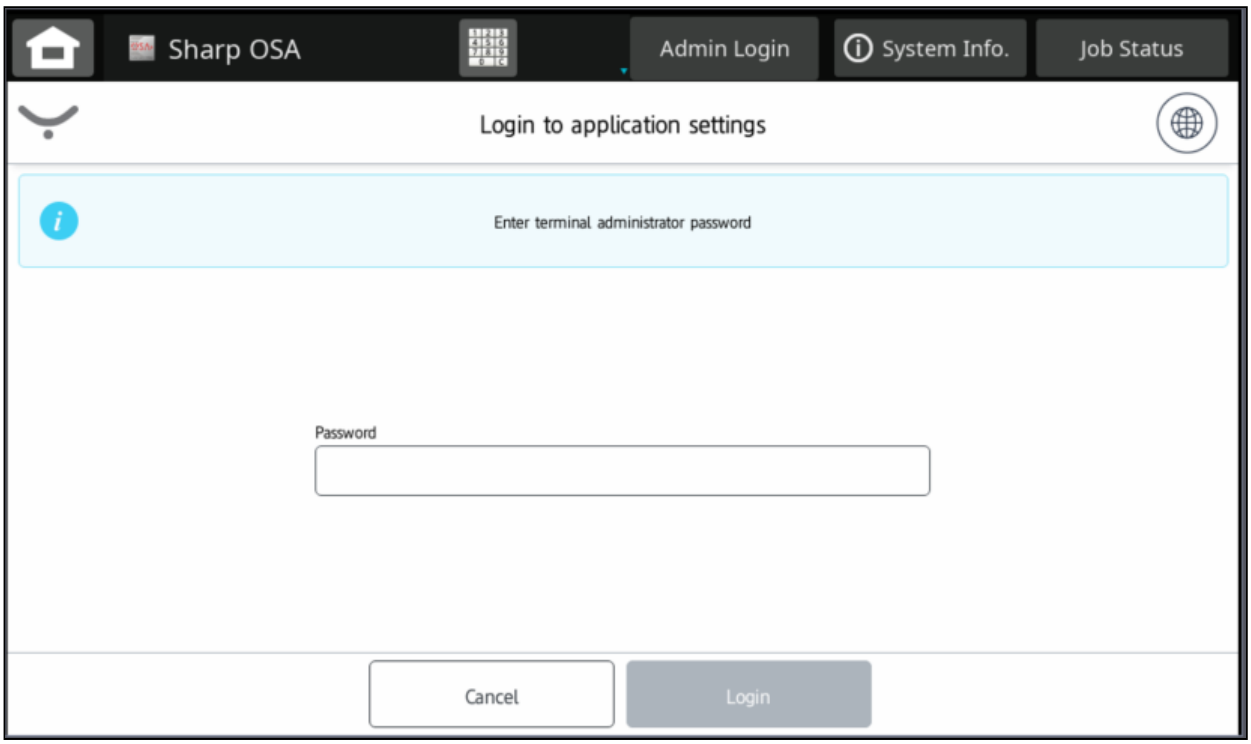


9. In Serial number, enter the serial number that the MFD displayed on the screen in the previous steps.
10. Fill in all the other required information.
11. In Embedded configuration, select your Sharp embedded configuration from the list.
12. Click Save.

Accessing terminal application settings

On certain screens (*Authentication* screen, *Device Authorization Grant* screen), while there is no explicit button to access settings, the administrator can access the terminal application settings by holding the terminal logo pressed for 5 seconds.

1. Admin login screen appears. Terminal admin default password is 'Sharp123'.



Accessing terminal application logs

Application logs can be found under the following URL:

```
https://<MFD_IP>:10443/apps/O2L000021/SafeqCloudAuth/Log.ejs
```

To access this URL, please use the following credentials: user name '**admin**' and the specified '**Terminal admin password**' (if set, otherwise use the default password '**Sharp123**'). By default, this retrieves log file for the current day - if all stored logs should be retrieved from MFD, append the following query parameter to the URL: "**?allFiles=true**".

Security recommendations

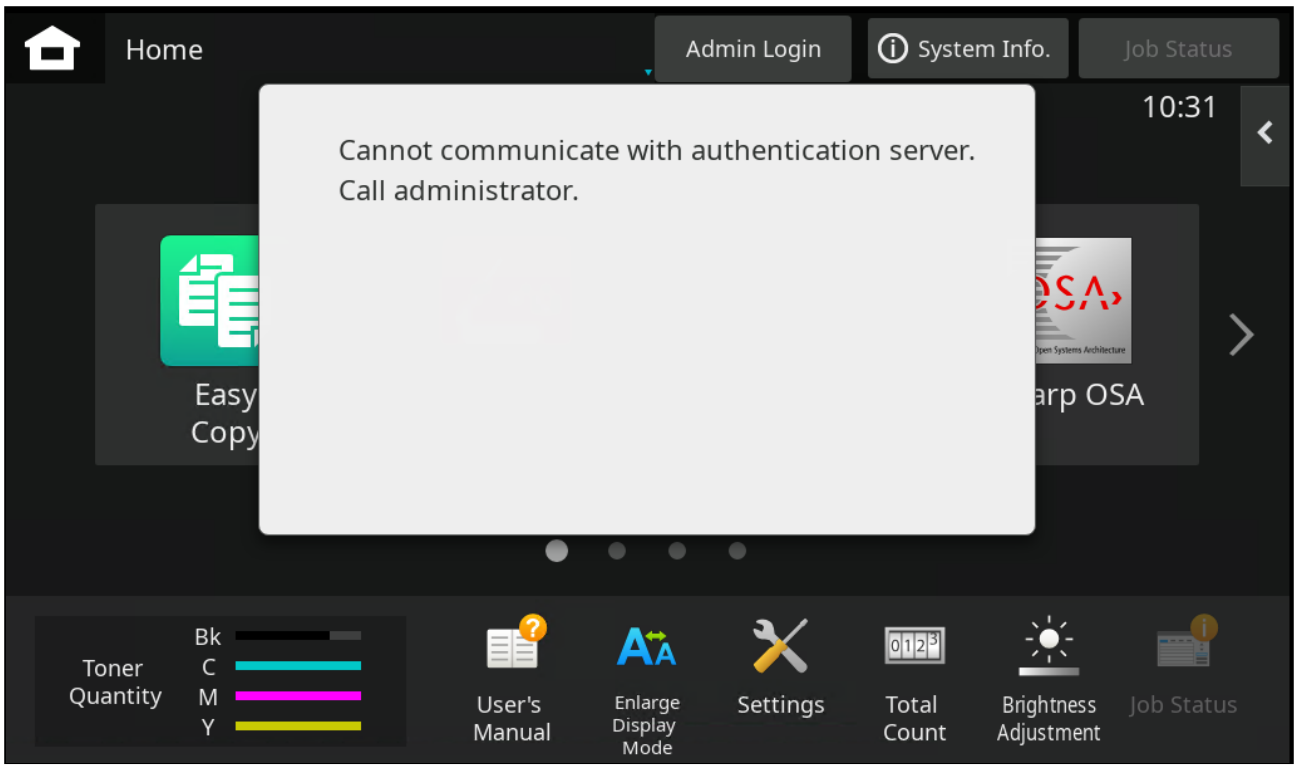
Following can be done to improve MFD security on local network:

- For customers that do not require installation via Terminal Deployment Tool and do not need terminal log access, it is possible to disable the Sharp OSA ports (10080, 10443) in MFD settings to prevent local access to application endpoints.
- Because Sharp Cloud Terminal cannot use device admin password to authenticate settings screen access, customers should change the default terminal admin password value to a custom one, to decrease risk of configuration tampering (local access to MFD only).

Troubleshooting

Error message "Cannot communicate with authentication server. Call administrator"

Problem description: When trying to use the MFD, you get an error message:



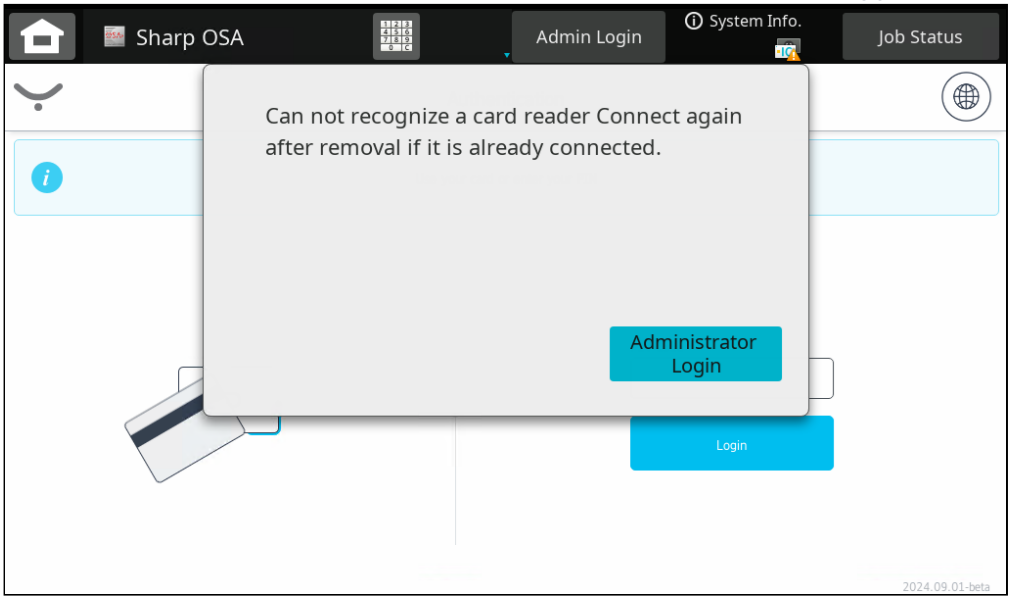
Solution: A possible cause of this is that Sharp OSA is configured for authentication; however, Offline authentication is enabled (possibly from the previous state of the MFD). You must disable it. See the *Device setup* section of this guide.

The card reader is not working

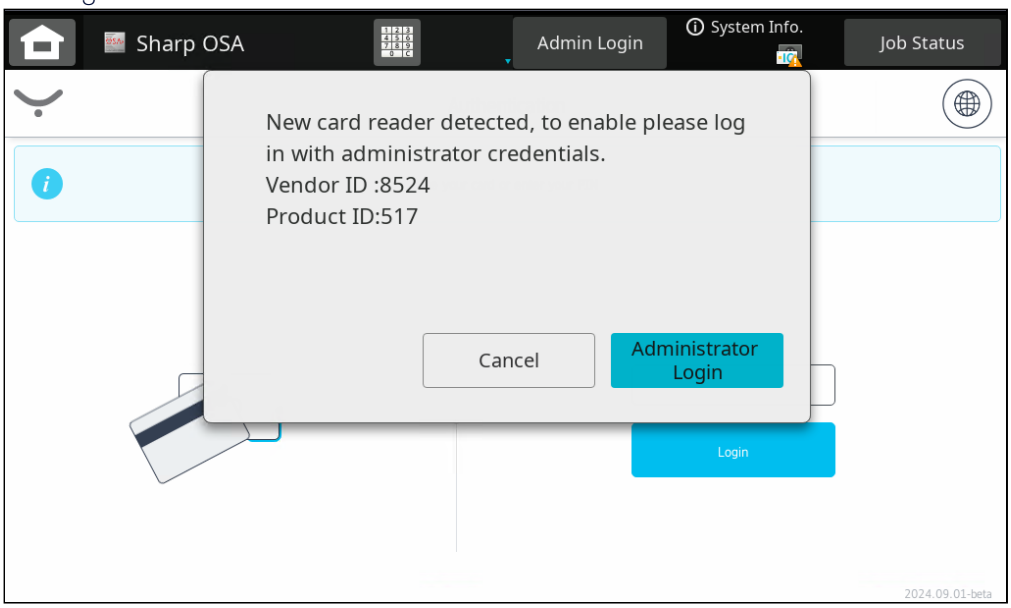
Problem: The card reader is not recognized.

Solution:

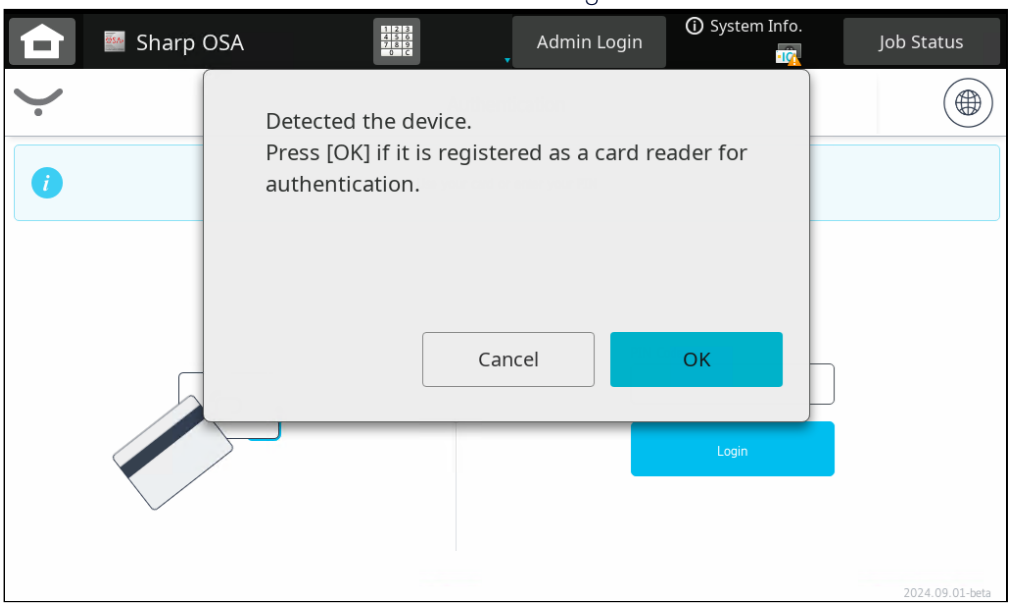
1. A possible cause is that the reader is not enabled after it was plugged in.



2. Connect the card reader to the MFD. A prompt to enable it will appear. Tap **Administrator Login** and log in as machine administrator.



3. Enable the card reader. You will see a message "Detected the device."



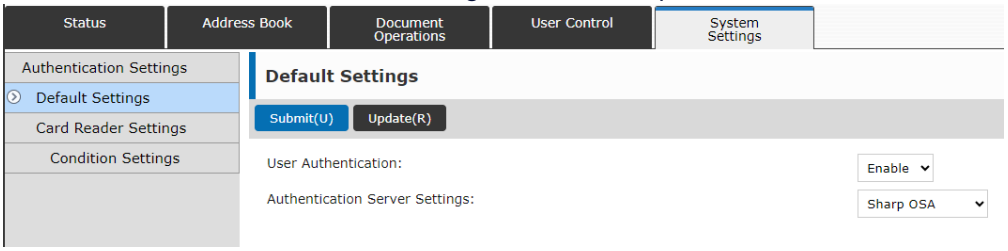
4. Note that if you disconnect and then reconnect the reader, you might be required to enable it again.

Manual installation

Device setup

1. If you plan to use a card reader, connect it to the MFD.
2. Log in to the MFD UI and go to **System Settings** > **Authentication settings**.
3. Enable **User Authentication**.

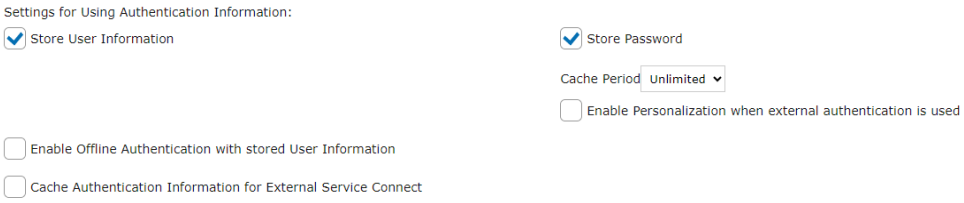
4. In the **Authentication Server Settings**, select **Sharp OSA**.



5. Make sure that **Offline Authentication** is disabled.

   a. Select Store User Information

   b. Deselect **Enable Offline Authentication with stored User Information**.



   c. Deselect **Store User information** again.

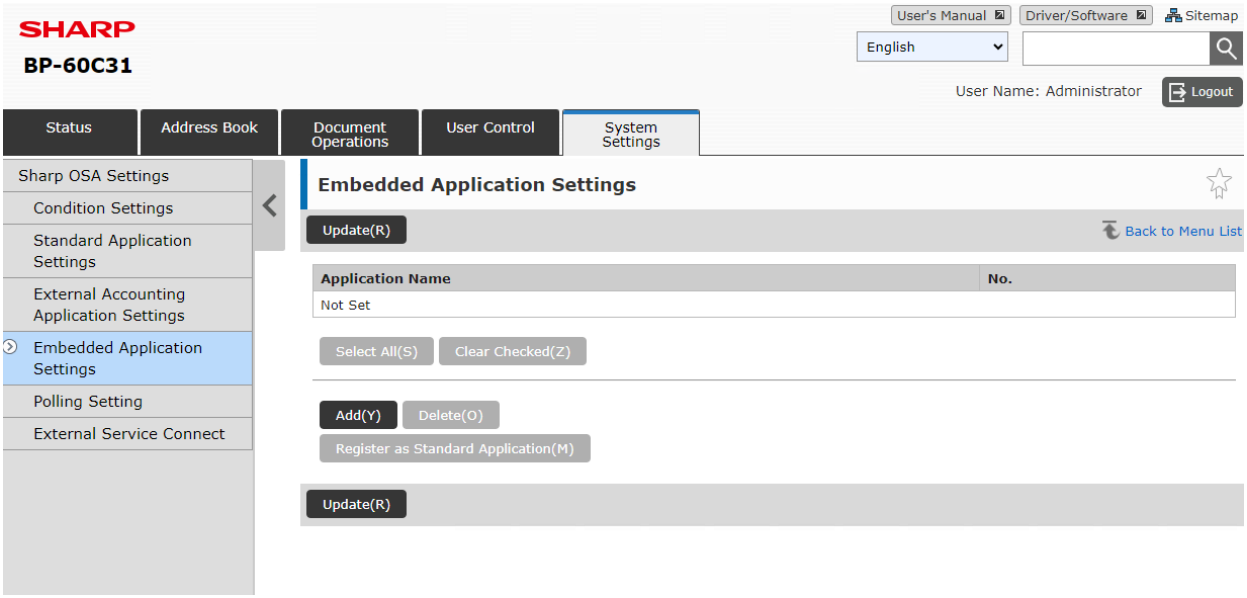
6. Select **Use IC Card for Authentication**.

Installing the cloud terminal

The terminal can only be installed manually via installation packages. Installation packages are available in the SAFEQ Cloud Web UI in the **Installation files** section.

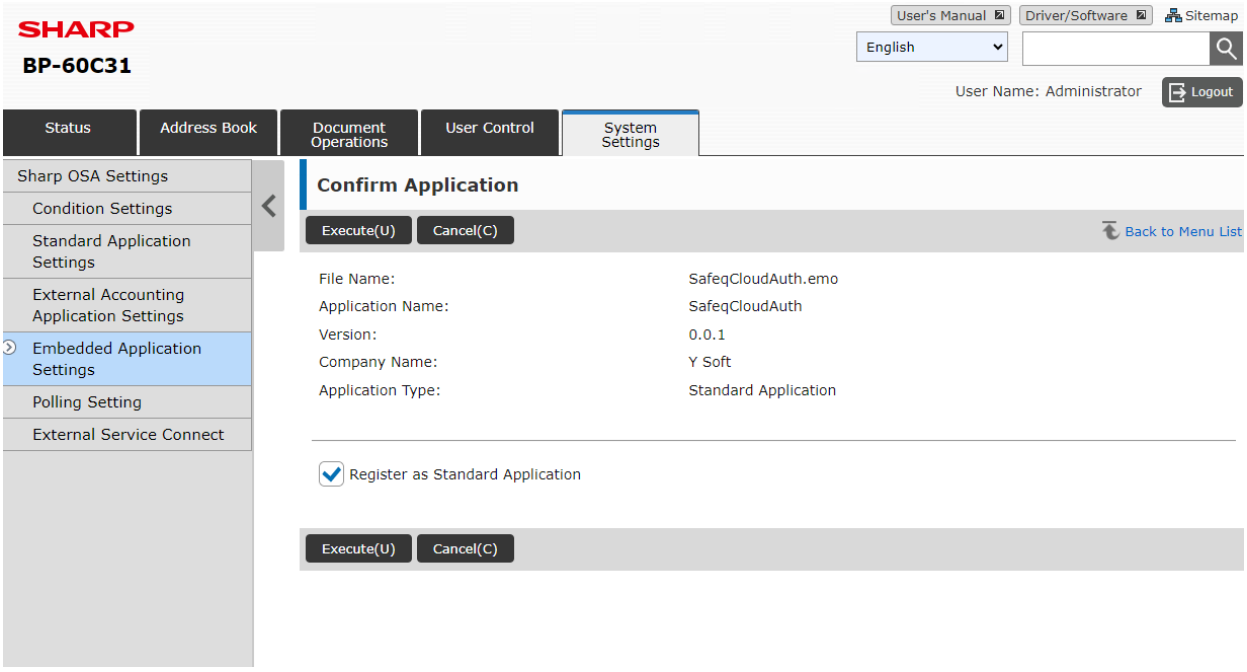
To install the terminal, perform the following steps:

1. Log into the MFD UI and go to **System Settings** > **Sharp OSA Settings**.
2. In **Embedded Application Settings**, tap **Add**.

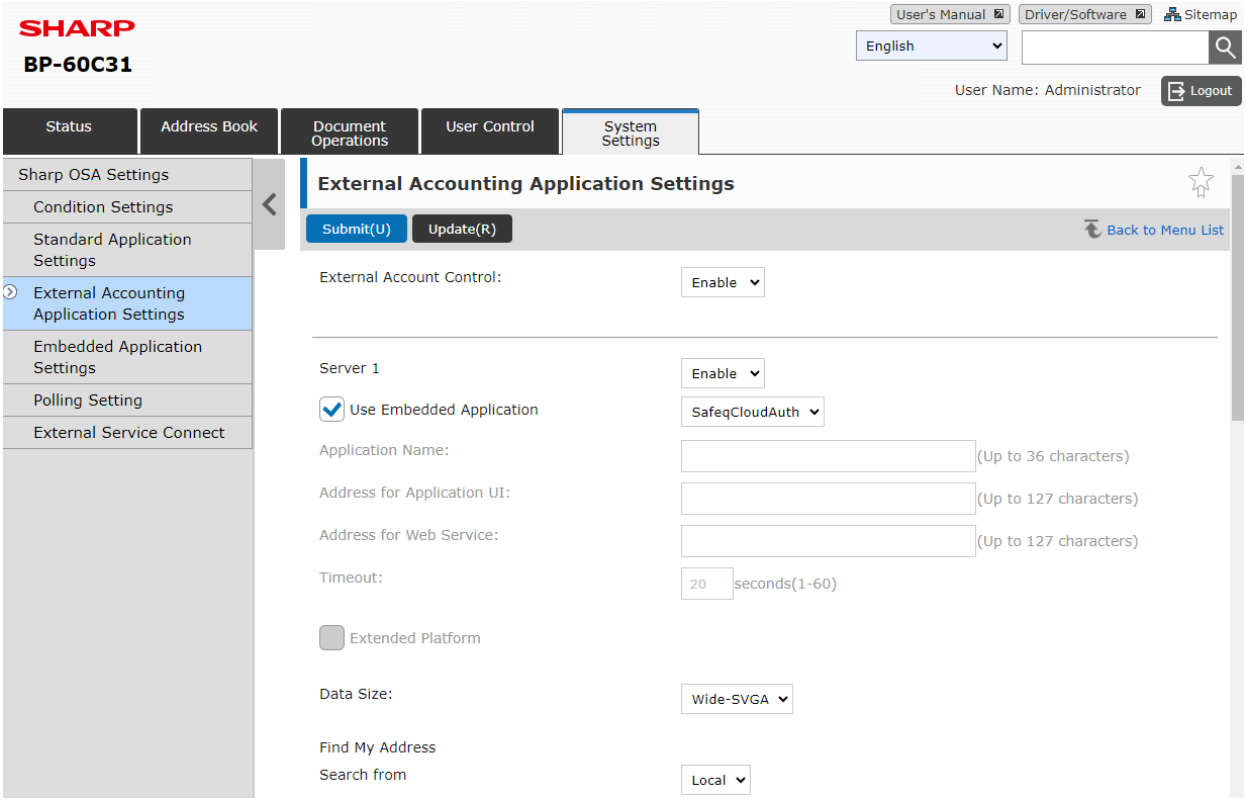


3. Tap **Browse** and select the SafeqCloudAuth.emo package and SafeqCloudTerminal.emo.

4. Tap **Execute**.



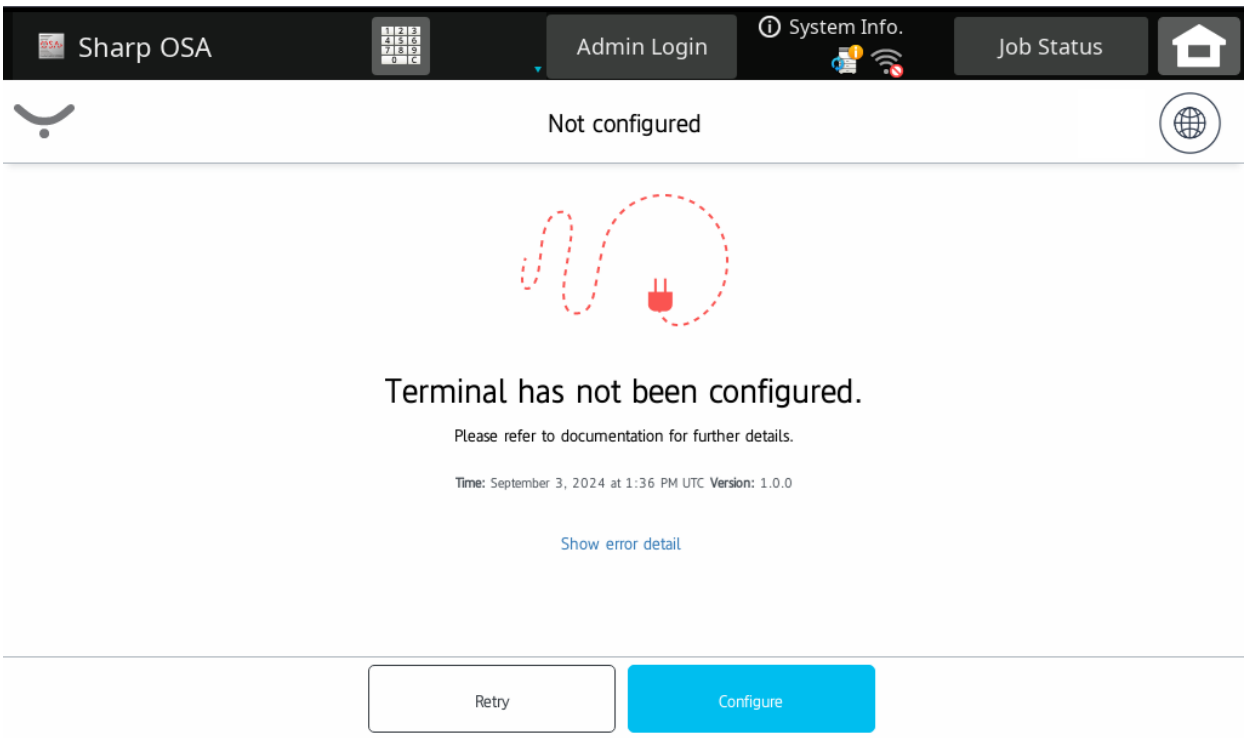
5. In **External Accounting Application Settings**, select **Enable** and assign the SafeqCloudAuth embedded application as Server 1. Disable servers 2-4.



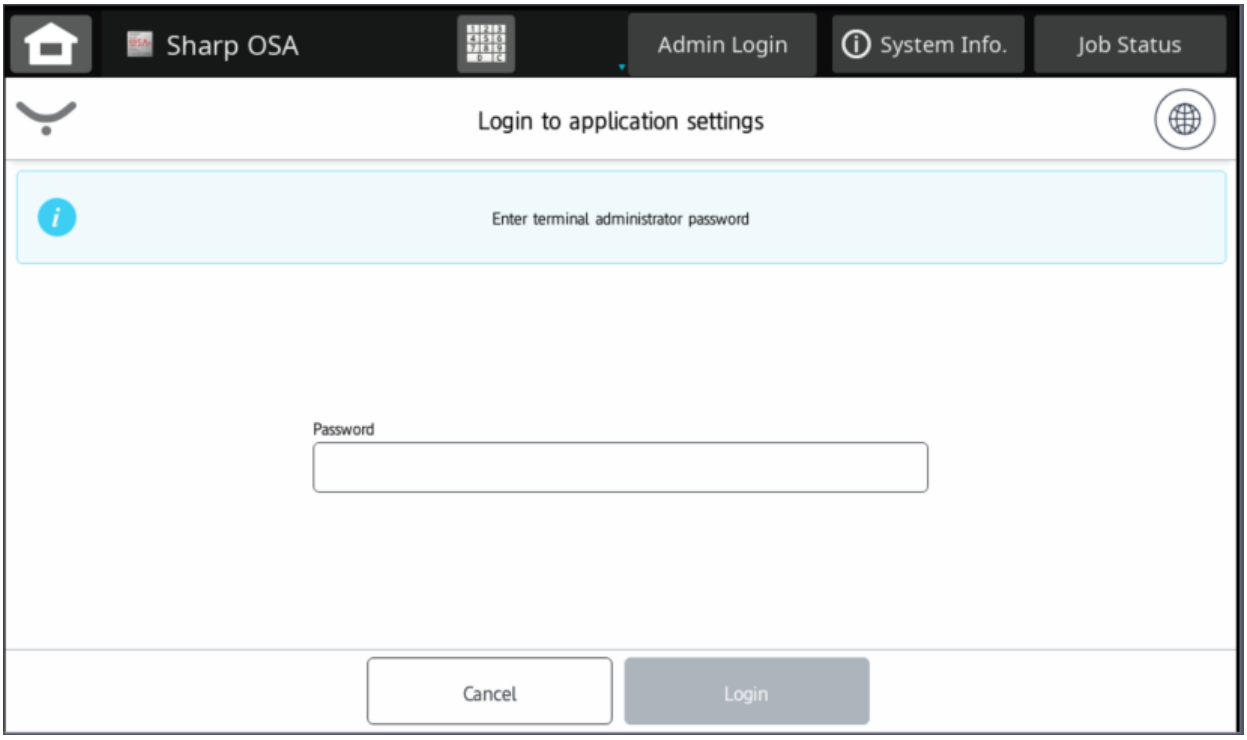
6. Tap **Submit**.
7. Reboot the MFD.

Configuring the Terminal settings

1. Have your SAFEQ Cloud domain at hand. You can find it in SAFEQ Cloud Web UI in the **Customer information** section.
2. If you haven't done so already, create an API key of the Embedded type. See API access keys.
3. After rebooting the MFD, you will be presented with the **Not configured** screen. Tap **Configure**.

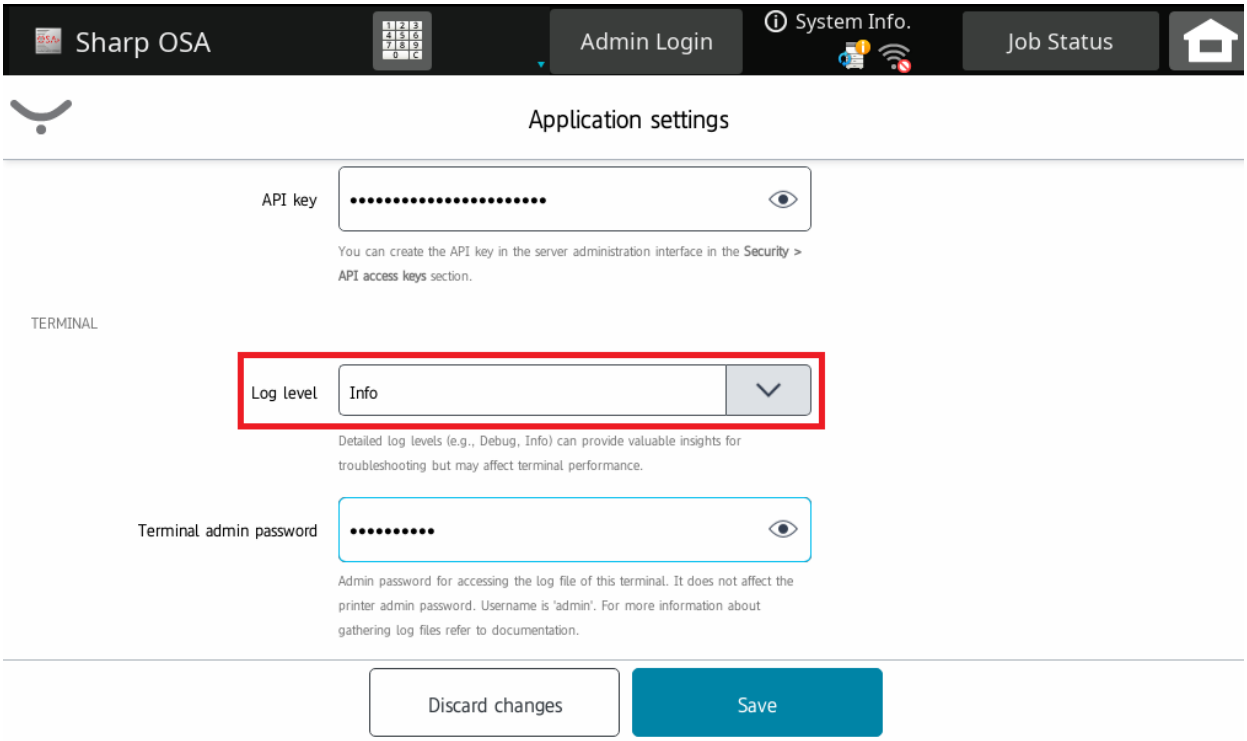


4. Admin login screen appears. Terminal admin default password is 'Sharp123'.

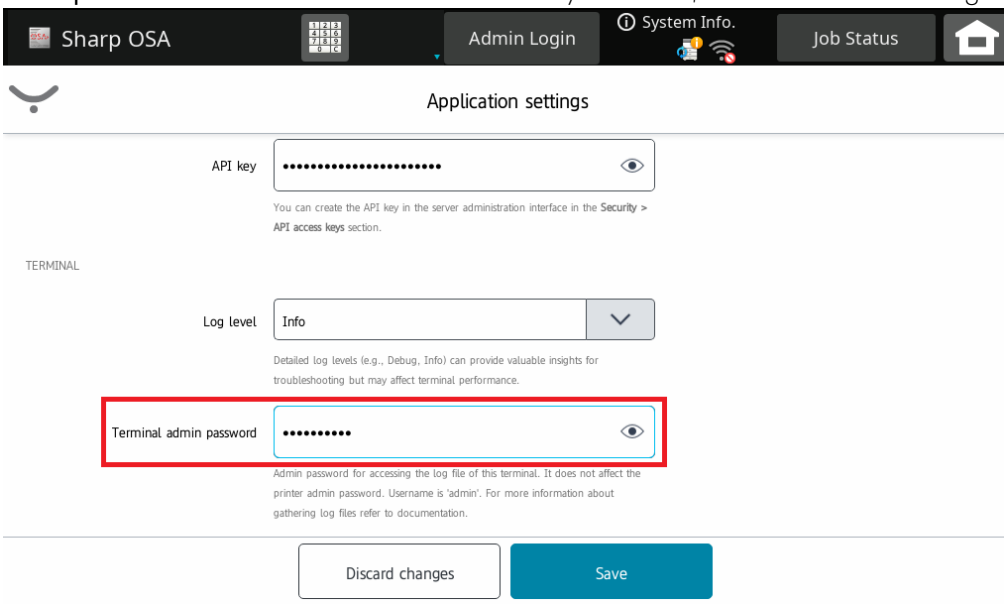


5. Enter your SAFEQ Cloud domain and API key. You can verify the domain by tapping **Test connection**.

6. In **Log level**, you can choose four levels of log details (Debug, Info, Warning, Error). We recommend the default level - **Info**. The Debug level will give Y Soft more information for troubleshooting but may slow down the terminal.



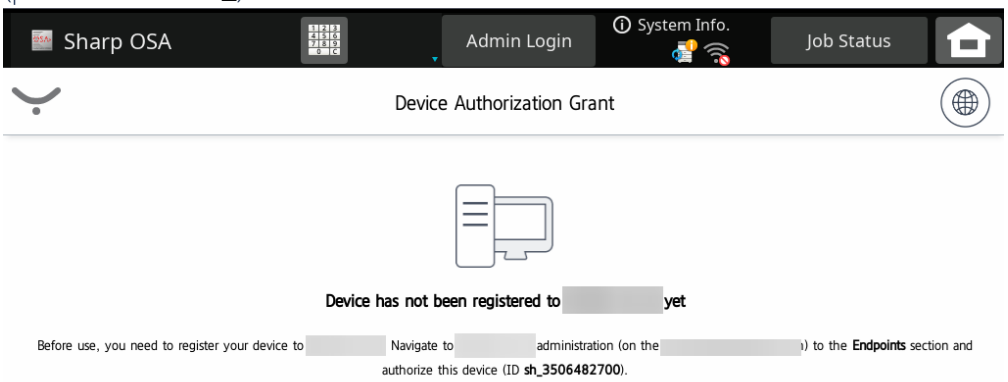
7. In the **Terminal admin password** field, you can set the password that will be used when accessing device logs and the application settings . If left empty, the default password "Sharp123" will be used instead. For security reasons, we recommend filling in the field.



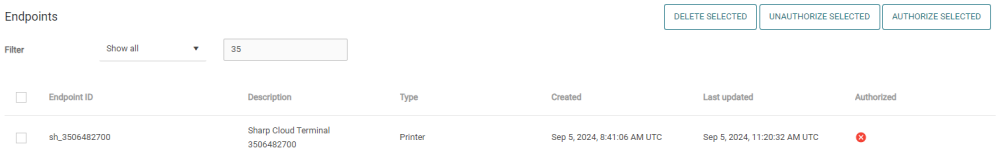
8. Tap **Save**.

Registering the cloud terminal in SAFEQ Cloud Web UI

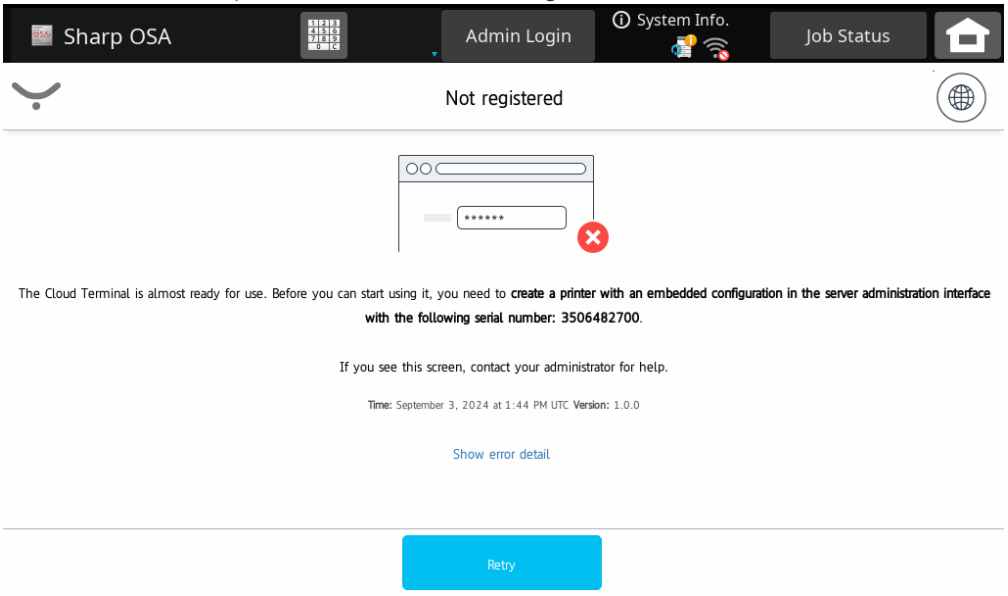
1. Upon installing the terminal, you will see a screen with the **Serial Number** of the device (prefixed with **sh_**). Note down the ID number.



2. In SAFEQ Cloud web UI, go to **Security > Endpoints** and find the entry with ID number that you noted in the previous step. Select the entry and click **Authorize selected**.



3. Back at the MFD, you will see the following screen:

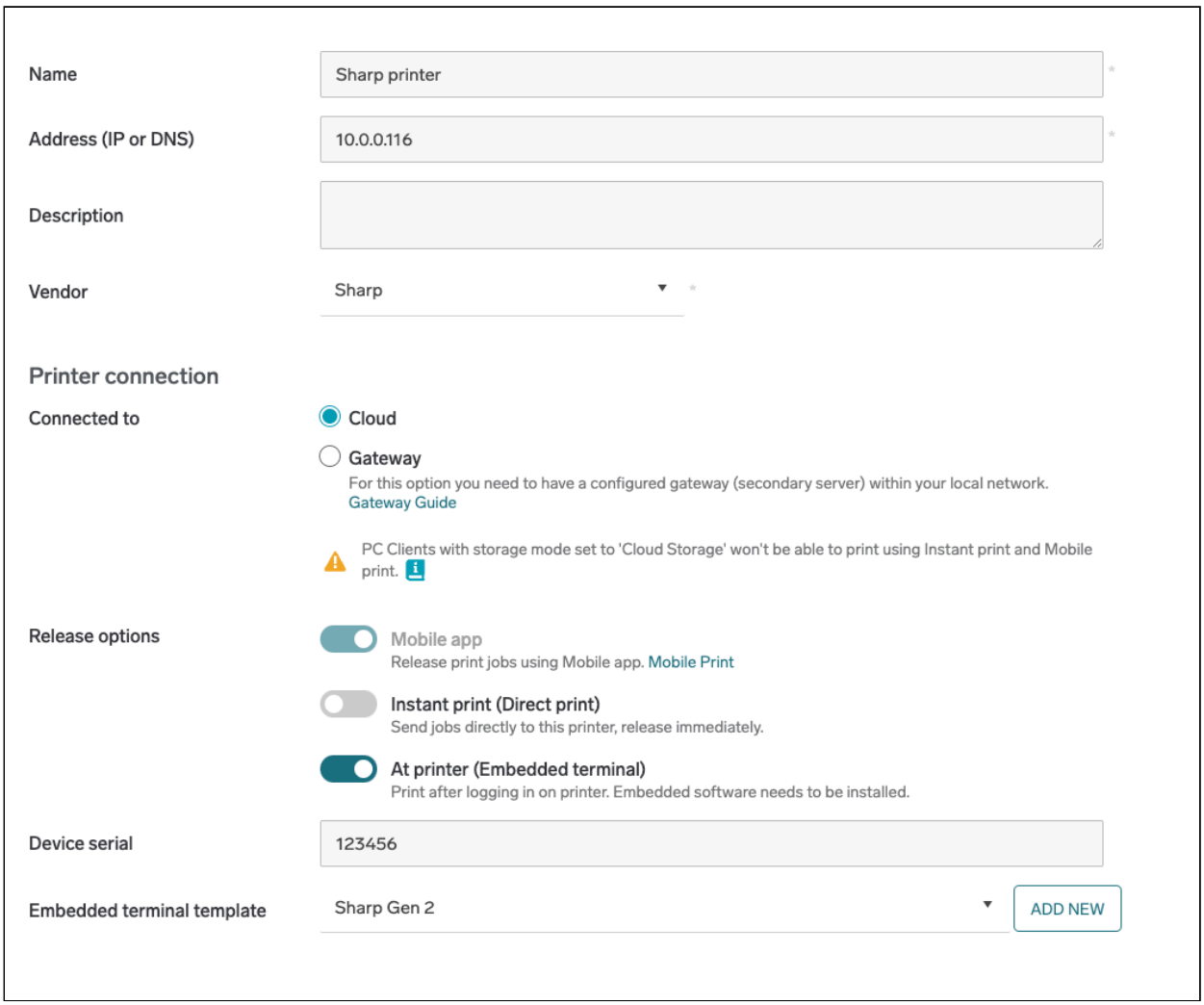


Adding the Sharp printer and Embedded configuration in SAFEQ Cloud Web UI

These steps are optional and if not performed, the Sharp printer will be added automatically after the endpoint is authorised, see *Registering the cloud terminal in the SAFEQ Cloud Web UI* section of this page.

If you want to connect the MFD that is already connected and registered to a different SAFEQ Cloud account, you must remove the Embedded applications in the Sharp OSA settings and add them again (see the *Installing the cloud terminal* section of this guide).

1. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
2. If not done already, create an embedded configuration for your Sharp MFD(s) by clicking **Add**.
3. In **Vendor**, select **Sharp**.
4. In **Application type**, select **Sharp Gen 2**.
5. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.
6. Go to **Printers**.
7. Click **Add**.
8. In **Vendor**, select **Sharp**.



9. In Serial number, enter the serial number that the MFD displayed on the screen in the previous steps.
10. Fill in all the other required information.
11. In Embedded configuration, select your Sharp embedded configuration from the list.
12. Click Save.
13. Return to MFD, if you see the screen from the end of the previous section tap Reload. The MFD will now display a login screen with your chosen authentication type.

Xerox Terminals

Xerox Gen 2 Cloud Terminal

Prerequisites

- Make sure that you have Cloud Terminal Integration enabled. For information on how to do this, see Enable Cloud terminal integration.
- Make sure that HTTPS (and TLS 1.2 or above) is enabled on the MFD, see Enabling HTTPS section.

Limitations

Printing

Finishing options

- Booklet bind direction Left to Right is always used.
- Booklet is always folded per-page instead of folding the whole stack of papers at once when printing using other method than a local storage method.
- When a simplex or duplex short-edge job is changed to a duplex long-edge job in basic finishing options, it will be printed as a simplex job. The duplex long-edge job sent to the queue will be printed as a duplex long-edge job. For a workaround, see the section *Changing default printing value on AltaLink devices*.
- A combination of two or more advanced finishing options (stapling, punching or booklet folding) is not possible when printing using other method than a local storage method.

Scanning

The impact of color setting on resulting file format

Depending on what color setting (Auto, Full color, Greyscale, etc.) you or the user chooses, the MFD will deliver different formats:

- When scanning on VersaLink models with color mode set to **Auto**, the device will produce a PDF file regardless of the configured file format.
- If you select **JPG** file format in combination with **Black and white**, **One color**, or **Two color**, VersaLink devices will produce a TIFF file.
- If you select **JPG** file format in combination with **Full color** or **Greyscale**, the device will produce a JPEG file.

Merging originals

- Merging originals for **multipage TIFF** works only with **Black and white**, **One color,** and **Two color** color settings.

Duplex scan from glass

For AltaLink devices only: A simplex scan is performed when a duplex scan with merging originals set to "off" is started while the feeder is empty. This is due to vendor limitations that prevent us from altering scan behavior based on the scan source.

Copying

- Advanced finishing options (Stapling, Punching, and Folding) are not supported.
- PrimeLink devices do not support accounting for copy functions and are restricted to single-sided copying. Double-sided (duplex) copying is not available.

Language switching

- If you set the language on the MFD, the selected language becomes the default application language. If a user changes the language from the application's language selection menu, the new language will be used for the current user session and will reset to the default device language once the user logs out.
- Languages with limited support
  - Thai, Chinese (Simplified), Japanese, Korean
  - Languages are limited to devices that are capable of displaying them – they must have the respective browser fonts embedded.

- These languages are only available when set as the device language (not via the application language selection menu).

Accounting

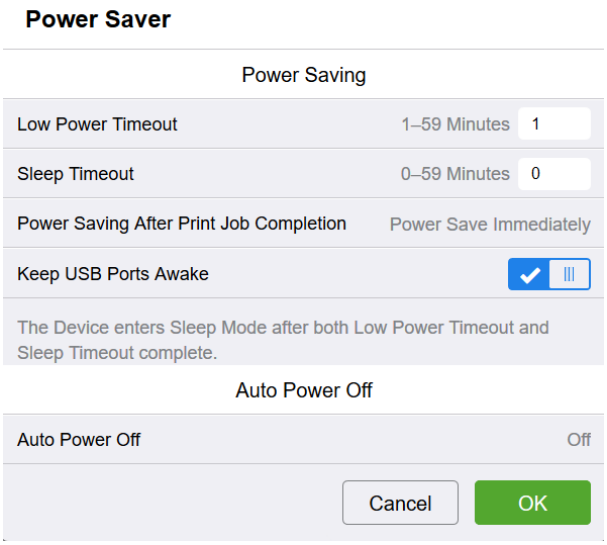
Accounting for native applications like Copy, USB print, and Fax is not supported. If you set the device to the kiosk mode, the users will not be able to use these applications and you will not miss any accounting information.

Scanning

- If the terminal loses connection before finishing the scan job, the scan job will be accounted for even if it was not delivered to the user.

Card Readers

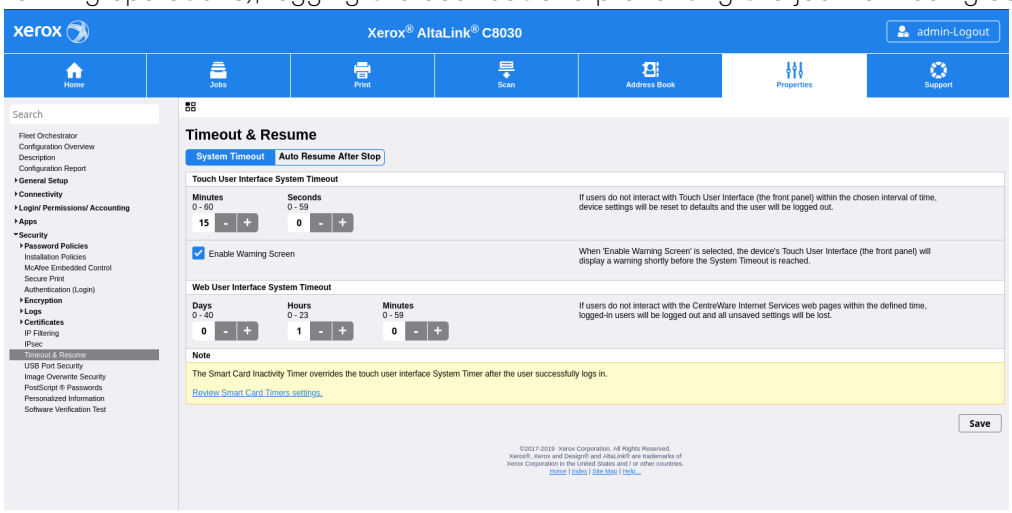
- The user is not able to logout by card swipe.
- On VersaLink MFDs, the **Keep USB Ports Awake** option in the **Power Saver** settings must be **enabled.** Otherwise, when the MFD wakes up from a deep sleep, card authentication will not work until you reset the Cloud terminal by tapping the **Reset** button on the MFD home screen (the button reloads all application).



Automatic logout timeout

In order for automatic user logout to function correctly, the system timeout on the device must be set to a larger value than the Automatic logout timeout (120 seconds by default), ideally 15 minutes which is the maximum value on most Xerox devices. Using a lower system timeout increases the likelihood of the device locking the user session during a print job (or other long

running operations), logging the user out and preventing the job from being accounted.

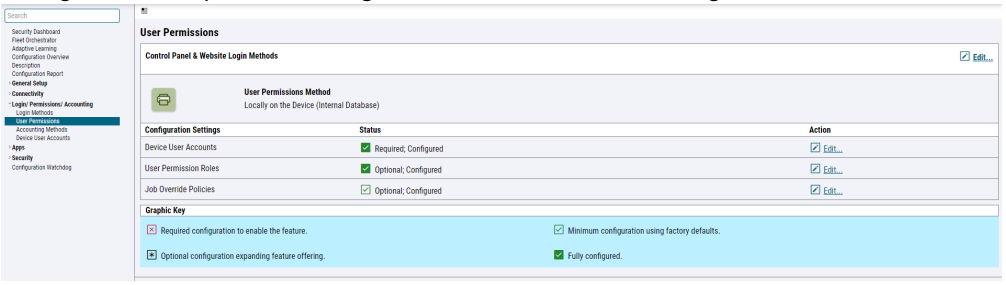


Device setup

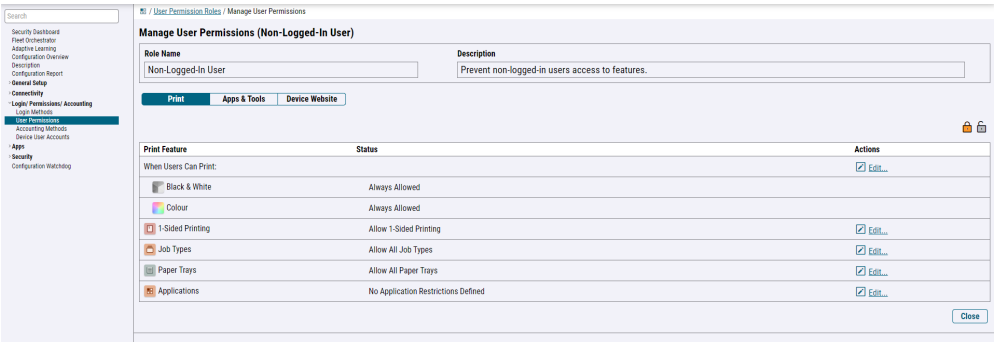
Enabling Printing on AltaLink Devices

To set user permissions for printing on AltaLink devices:

1. Log in to the MFD as an administrator.
2. Navigate to **Properties** > **Login/Permissions/Accounting** > **User Permissions**.



3. Click **Edit** in the **User Permission Roles** section.
4. Select **Edit** under **Non-Logged-In User**.
5. Set the desired permissions for Non-Logged-In user.



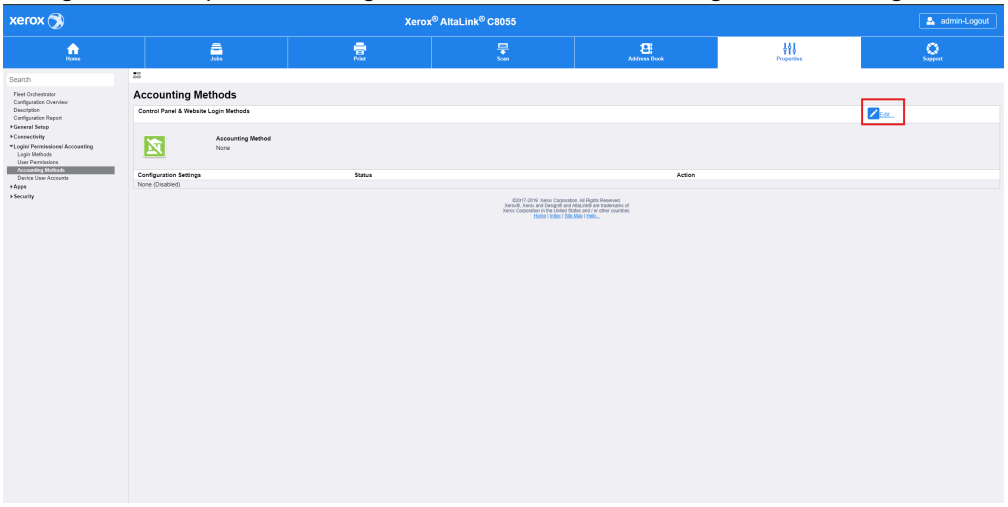
Enabling Accounting (Reporting) on AltaLink and VersaLink Devices

This section is fully automated in the Terminal Deployment tool.

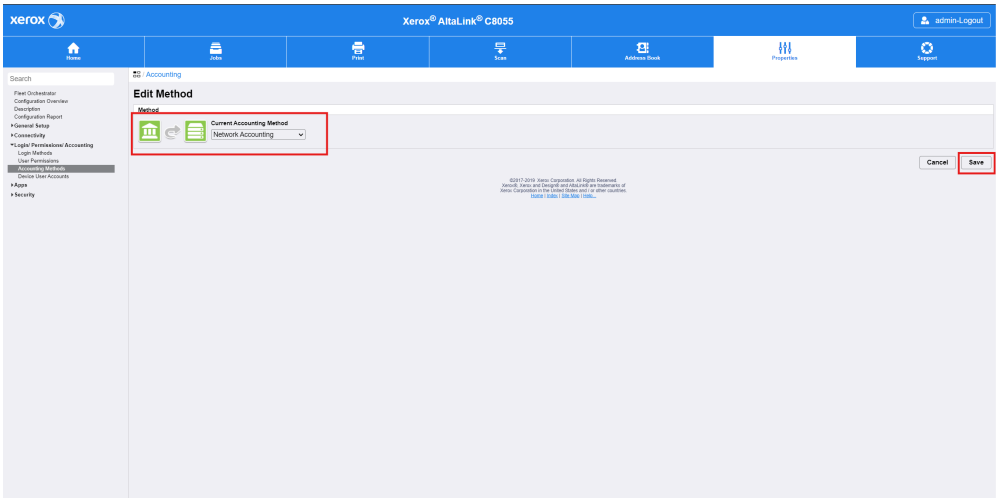
AltaLink

To enable accounting on AltaLink devices, perform the following steps:

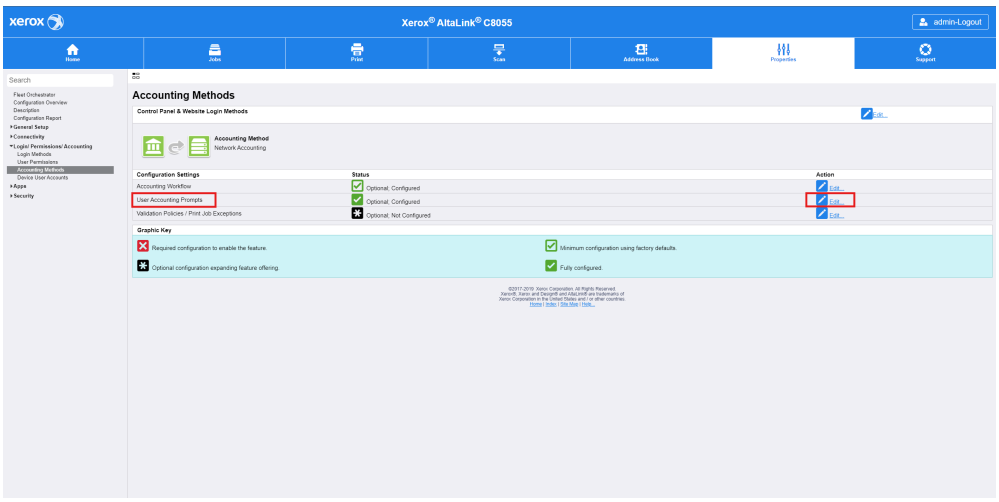
1. Log in to the MFD as an administrator.
2. Navigate to **Properties** > **Login/Permissions/Accounting** > **Accounting Methods** and click **Edit**.



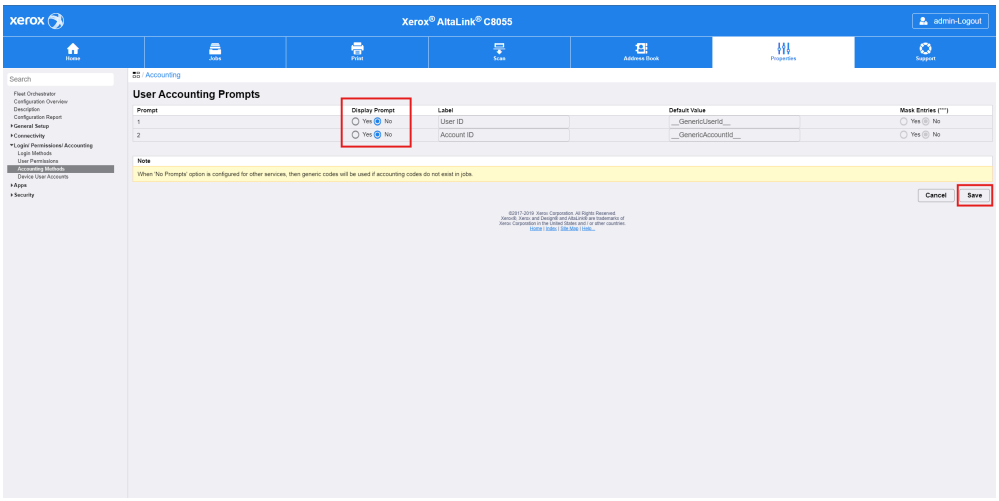
3. Select **Network Accounting** in **Current Accounting Method** selection box. Click **Save**.



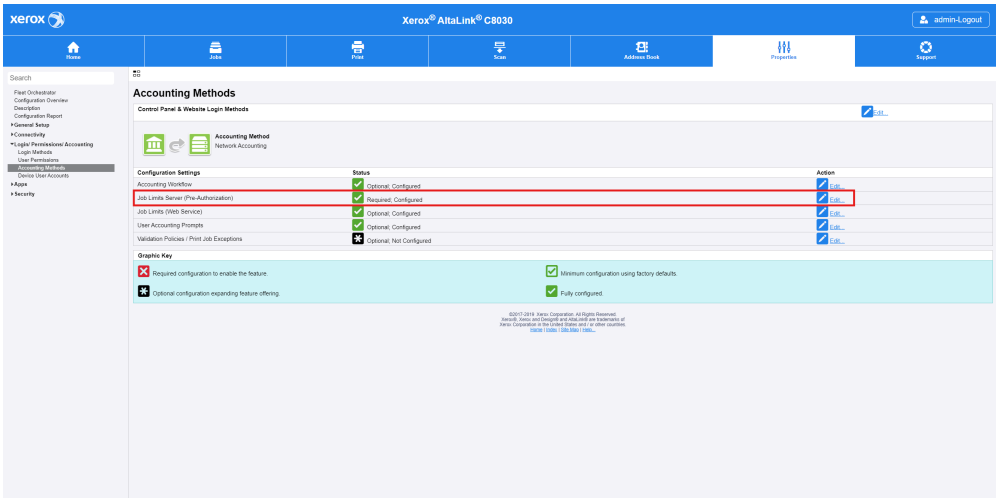
4. Click **Edit** in the **User Accounting Prompts** section.



5. Disable prompts **User ID** and **Account ID** by selecting **No** in **Display Prompt** column. Click **Save**.



6. If the **Job Limits Server (Pre Authorization)** is in **Configuration Settings** list on **Accounting Methods** screen click **Edit** and set the **Server URL** to *https://127.0.0.1*.



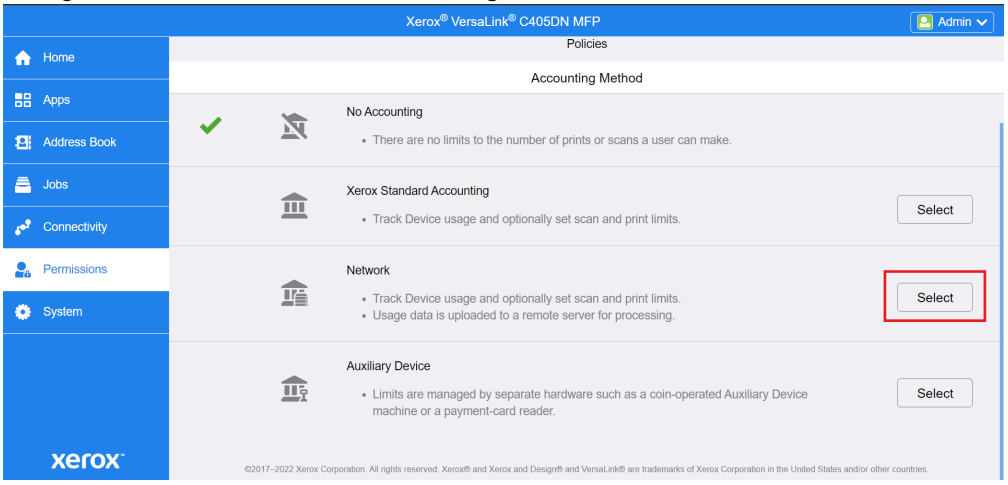
7. Click **Save**.

8. Restart the MFD to apply the new Accounting setting.

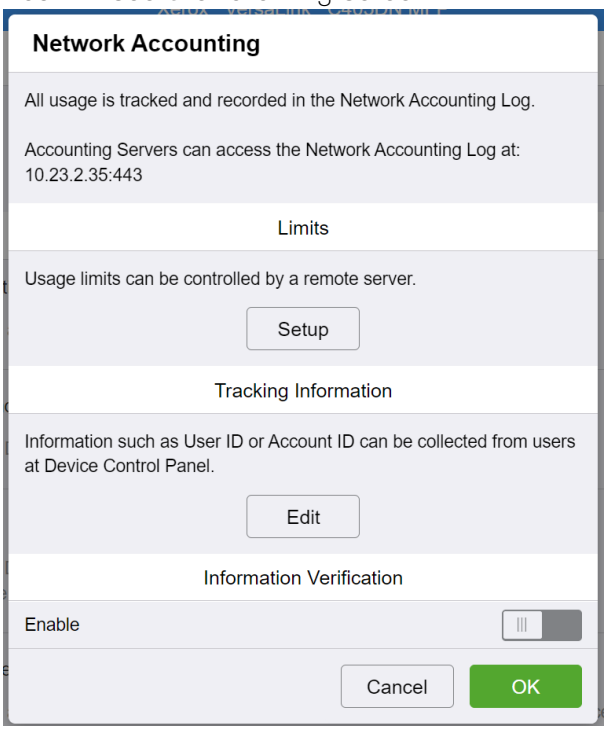
VersaLink

To enable accounting on VersaLink devices, perform the following steps:

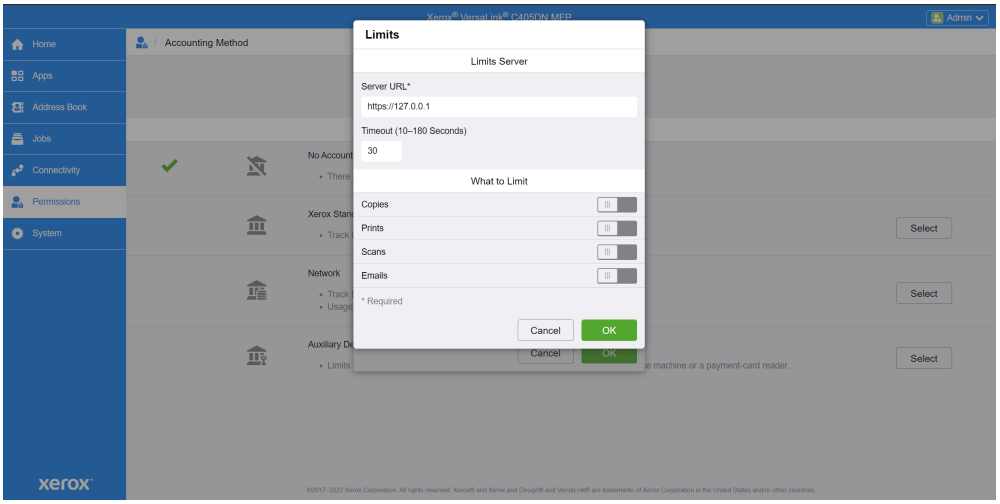
1. Log in to the MFD as an administrator.
2. Navigate to **Permissions > Accounting Method**. Click Select in the **Network** section.



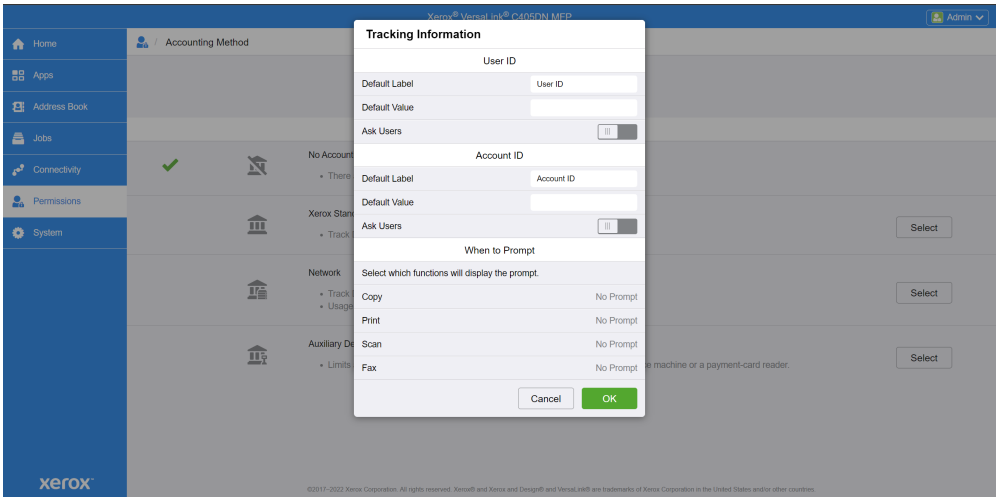
3. You will see the following screen.



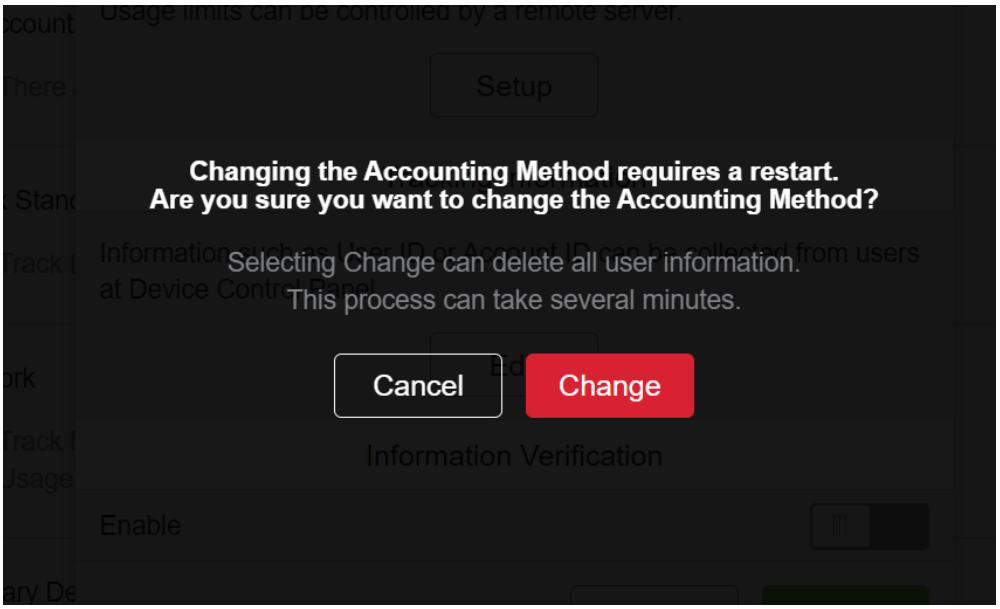
4. Click **Setup** in the **Limits** section. Set **Server URL** to *https://127.0.0.1*. Disable all items (Copies, Prints, Scans, Emails) in **What to Limit** section, and click **OK**.



5. Open **Tracking Information** settings by clicking **Edit**. Disable **Ask Users** option for **User ID** and **Account ID**. Select **No Prompt** for Copy, Print, Scan and Fax in **When to Prompt** section. Click **OK**.



6. Click **OK** on the **Network Accounting** screen. Restart the device by clicking **Change**.

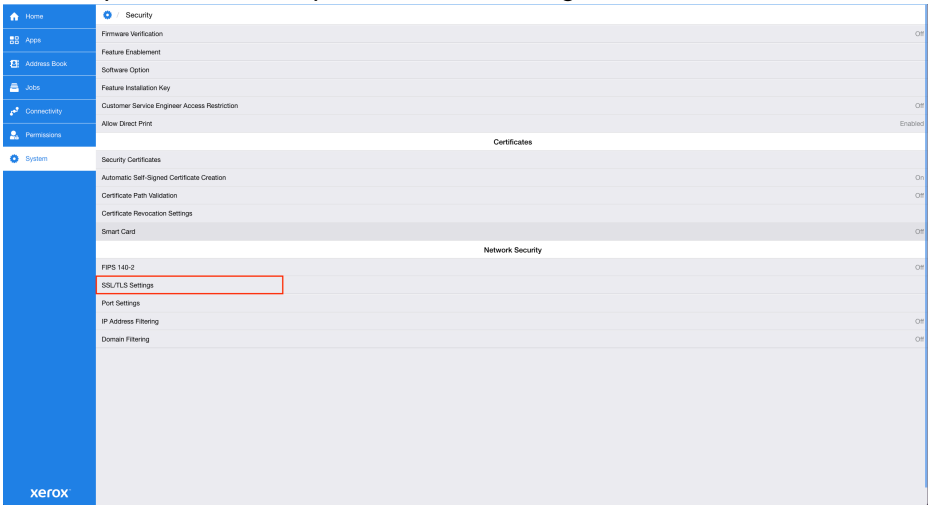


Enabling HTTPS

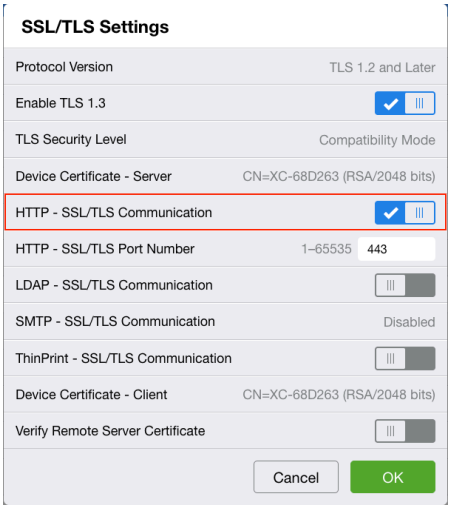
VersaLink

Enabling HTTPS and TLS 1.2 or higher on VersaLink devices is required to proper functioning of a device.

1. Log in to the MFD as an administrator.
2. Go to **System** > **Security** > **SSL/TLS Settings**.



3. Enable **HTTP - SSL/TLS Communication**.

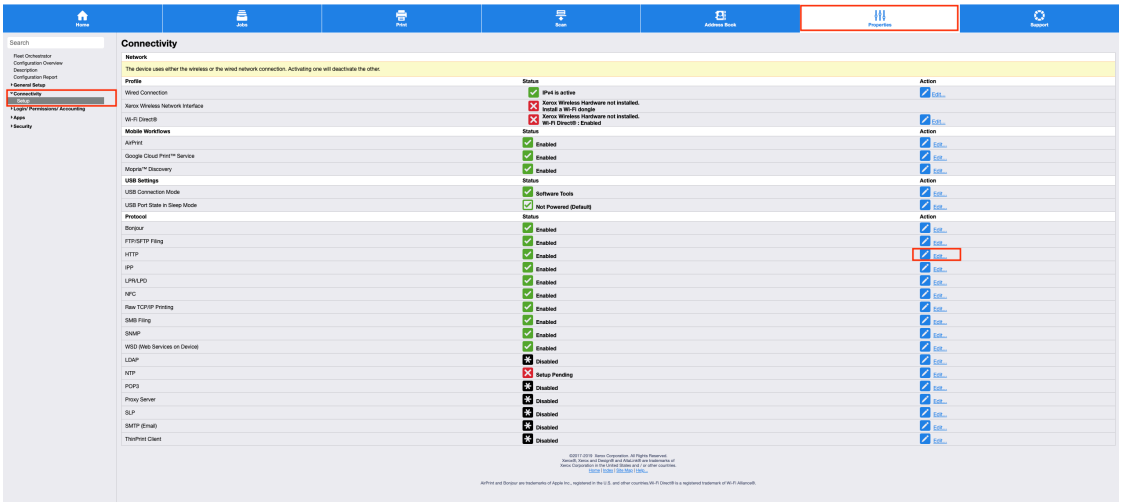


4. Click **Ok** to save changes.

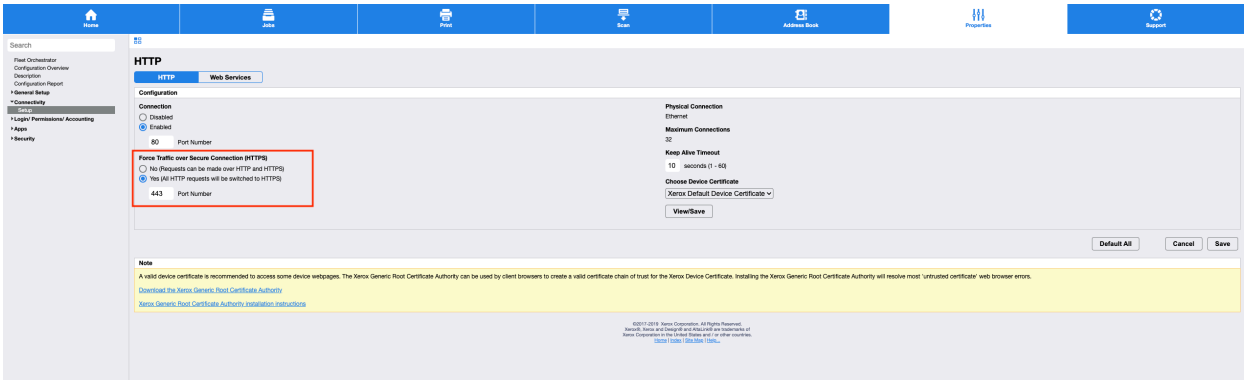
AltaLink

Enabling HTTPS and TLS 1.2 or higher on AltaLink devices is required to proper functioning of a device.

1. Log in to the MFD as an administrator.
2. Go to **Properties** > **Connectivity** > **Setup**
3. Locate **HTTP** and click **Edit** on the right side in the same row.



4. Enable **Force Traffic over Secure Connection (HTTPS)**



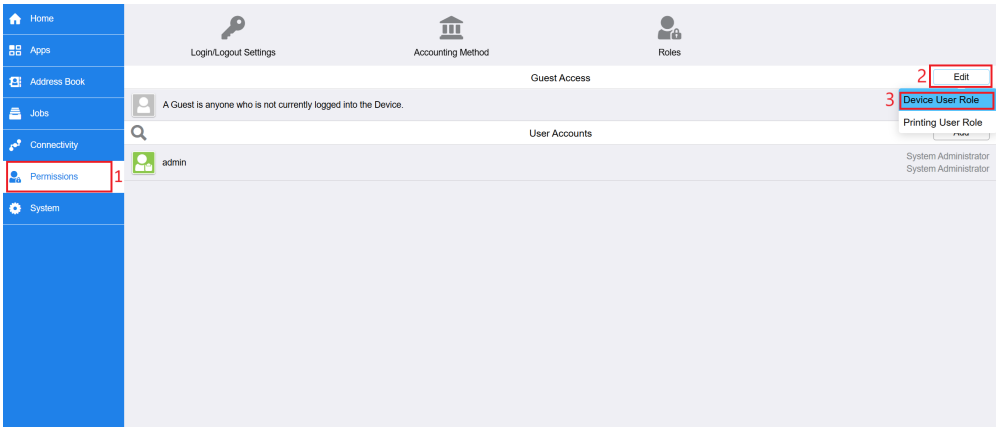
5. Click **Save** to save changes.

Enabling Copy on VersaLink Devices

To enable the copy function and avoid permissions problem (Internal error 500 when the user tries to copy without permissions) enable Guest Access for copy application below.

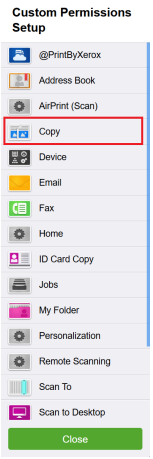
1. Log in to the MFD as an administrator.

2. Go to **Permissions**. Click **Edit** in the **Guest Access** section and then **Device User Role**.



3. Select **Custom Permissions** in the **Control Panel Permissions** section and click **Setup.**

4. Click on **Copy** application.



5. Allow all available options **Access Copy**, **Make Color Copies** (relevant only for Color devices), 1-Sided Output

6. Click on **OK**→ **Close** → **OK** buttons to save changes.

Enabling ECDHE Ciphers on VersaLink Devices

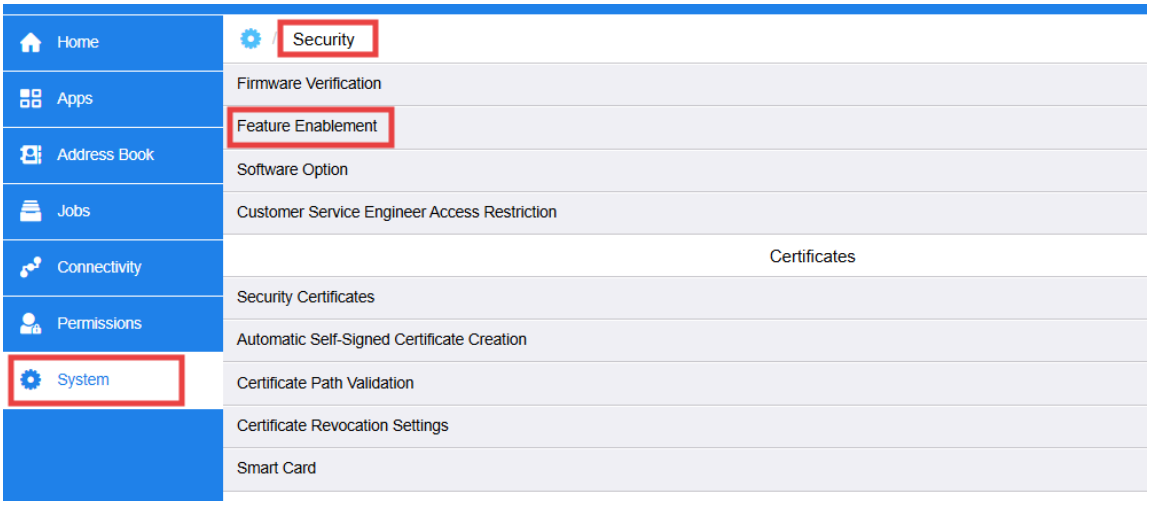
To successfully establish a secure TLS connection between a device and the cloud server, we recommend to enable ECDHE Ciphers for the TLS communication on the device.

If device FW version is xx.71.21 or higher, the ECDHE Ciphers are available by default - not further steps are needed.

If device FW version is below xx.71.21, the steps below need to be done.

The key codes below enable these ciphers. When the "Enablement Key" is applied, the ciphers are available. The "Disablement Key" will restore the default condition, i.e. ciphers are not available. Feature Key Instructions:

1. On the device's Embedded Web Server select System-> Security-> Feature Enablement



2. Enter correct enable/disable code (include the * character)

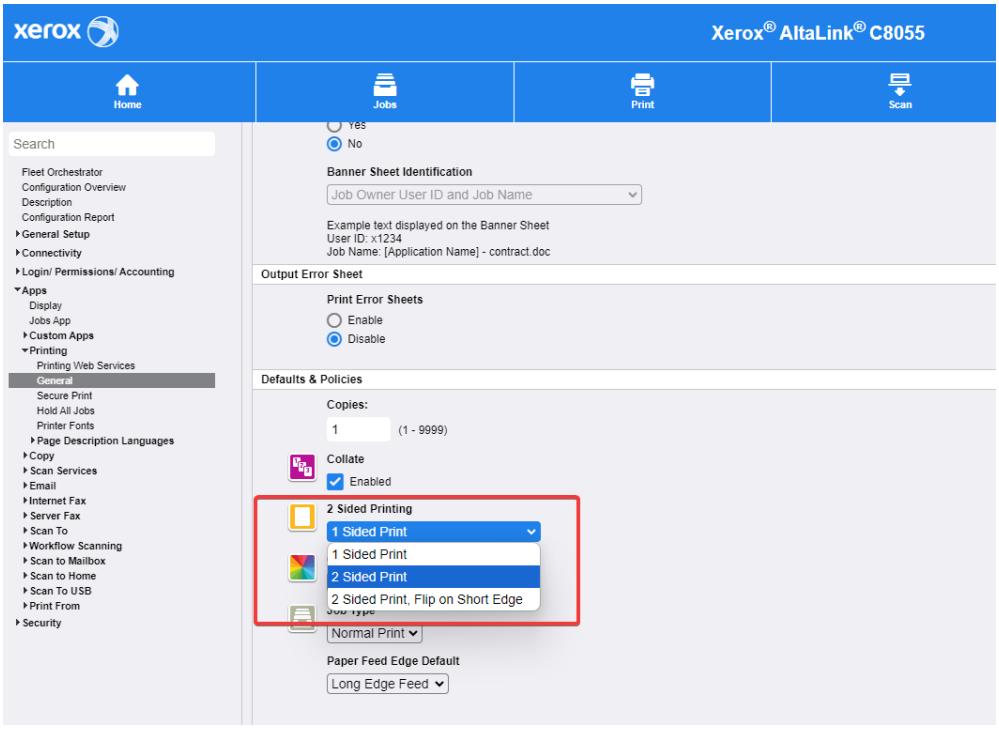
The Feature keys are as follows:

Product Model	Enablement Key	Disablement Key
Xerox® VersaLink™ C405	*3002452891	*3002452890
Xerox® VersaLink™ C400	*3006452891	*3006452890
Xerox® VersaLink™ B405	*3003452891	*3003452890
Xerox® VersaLink™ B400	*3007452891	*3007452890
Xerox® VersaLink™ C7020/C7025/C7030	*3014452891	*3014452890
Xerox® VersaLink C7000	*3015452891	*3015452890
Xerox® VersaLink C505/C605	*3016452891	*3016452890
Xerox® VersaLink C500/ C600	*3017452891	*3017452890
Xerox® VersaLink™ B605/B615	*3020452891	*3020452890
Xerox® VersaLink™ B600/B610	*3021452891	*3021452890
Xerox® WorkCentre 6515	*3005452891	*3005452890
Xerox® Phaser 6510	*3008452891	*3008452890
Xerox® VersaLink™ B7025 / B7030 / B7035	*3004452891	*3004452890
Xerox® C8000 / C9000	*3023452891	*3023452890
Xerox® C8000W	*3064452891	*3064452890

Changing default printing value on AltaLink devices

We recommend you to set up the following to prevent issues with duplex printing with basic finishing options.

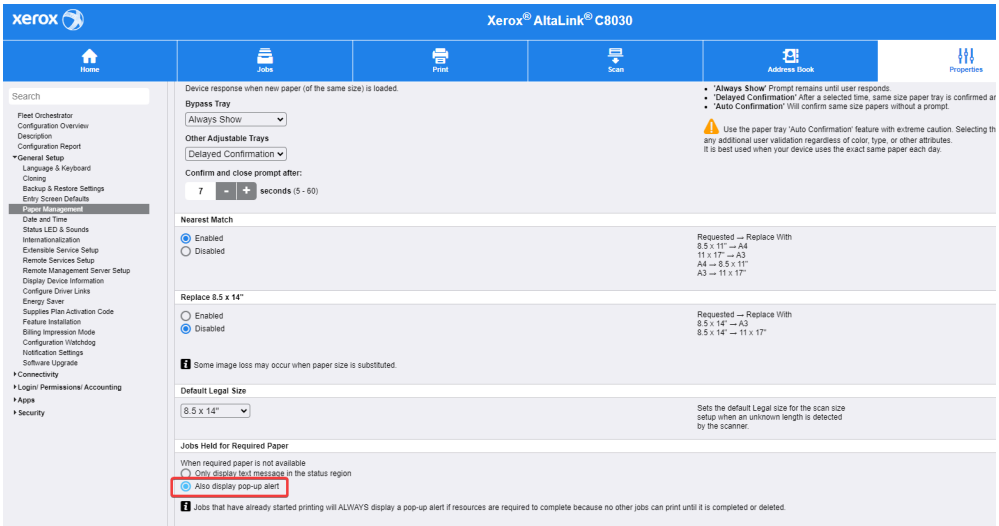
1. Log in to the MFD as an administrator.
2. Go to **Properties** > **Apps** > **Printing** > **General.**
3. In **2 Sided Printing**, select **2 Sided Print**.



4. Click **Save**.

Allowing "Resources Required" native pop-up screen on Altalink devices

1. Log in to the MFD as an administrator.
2. Go to **Properties** > **General Setup** > **Paper Management** > **Required Paper Policies**.
3. In **Jobs Held for Required Paper section**, select **Also display pop-up alert option**.



4. Click **Apply**.

Setting the default screen when originals are detected

This setting is necessary to prevent the cloud terminal from being closed and another application being opened when the user puts a document in the feeder. Also, if Kiosk mode is enabled on the MFD, the user would be prompted to enter admin credentials for the MFD.

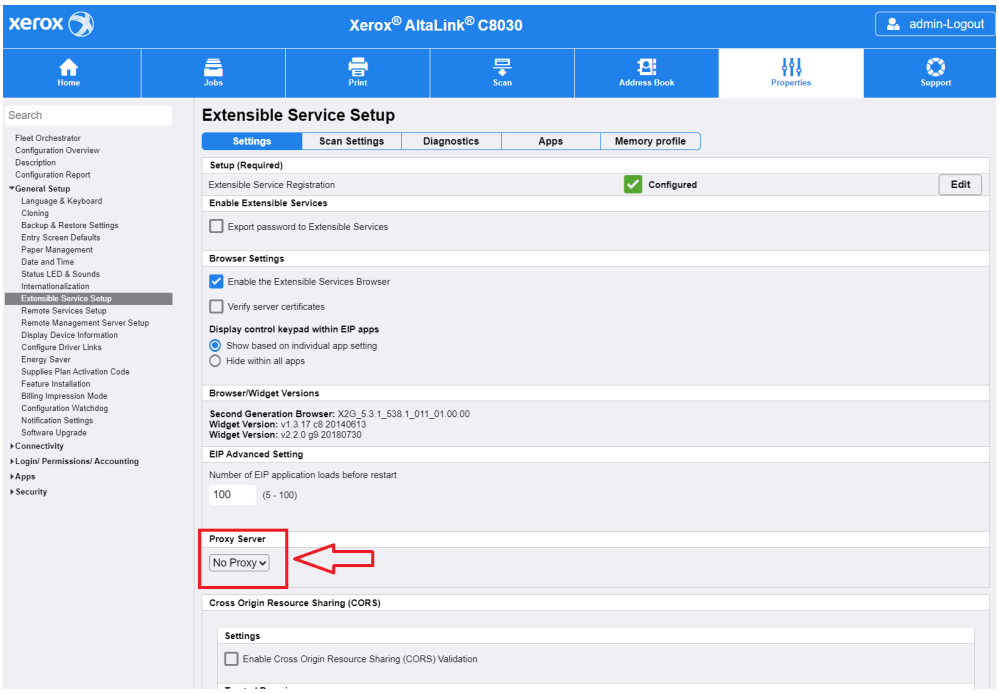
1. Log in to the MFD as an administrator.
2. Go to **Properties** > **General Setup** > **Entry Screen Defaults**.
3. In **Default Screen when Originals are Detected**, select **None (Take No Action)**.

Changing the proxy settings on AltaLink devices to prevent issues while scanning to WebDAV

This section is fully automated in the Terminal Deployment tool.

If your MFD supports WebDAV but you are receiving an error message "A connection to the server could not be established" while scanning to WebDAV, perform the following steps to bypass the proxy servers.

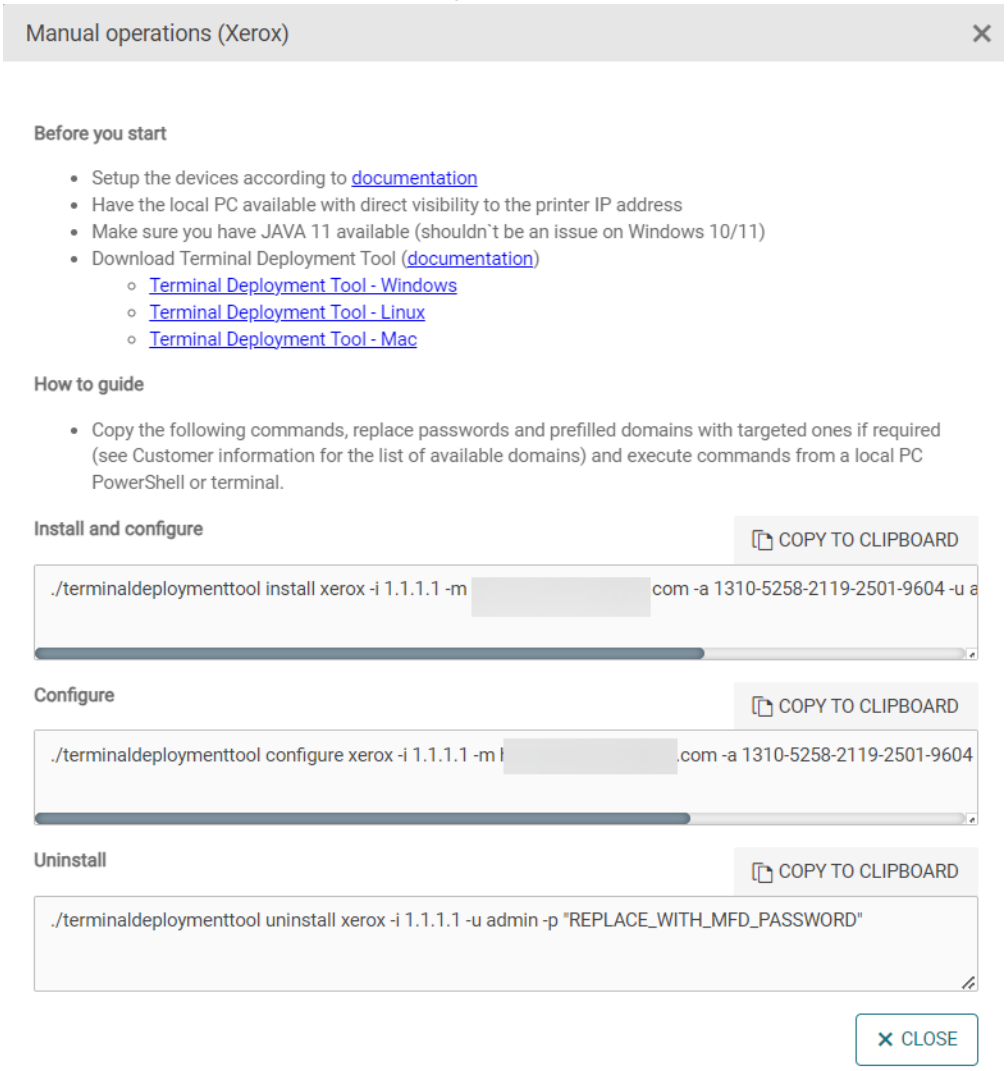
1. On the MFD's home screen, tap Properties to access the MFD's Control Panel. If you cannot access it this way, consult your the manual for your MFD's model.
2. Go to **General Setup** > **Extensive Service Setup**.
3. Locate **Proxy Server Settings**.
4. Set **Proxy** to **No Proxy**.



5. Tap **Save**.
6. The device may require a restart for the changes to take effect.

Installing the cloud terminal manually

1. Start with adding your Xerox MFD and creating the embedded configuration in SAFEQ Cloud Web UI. See section *Adding the Xerox printer and Embedded configuration in SAFEQ Cloud Web UI* of this guide.
2. Go to **Printers > Embedded templates** and open the newly created embedded configuration.
3. Click **Manual operations**.
4. Follow the instructions in the dialogue window.

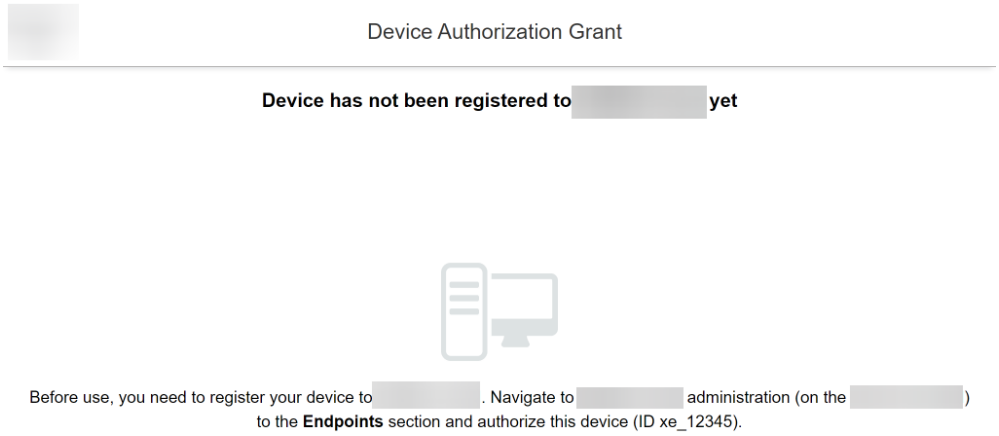


The example commands are generated regardless of the operating system.

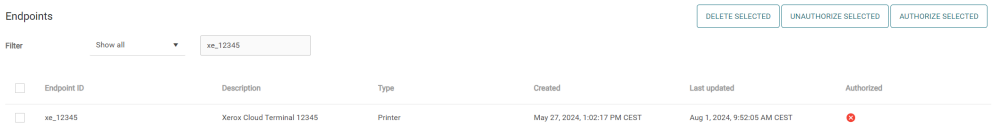
For Windows, the full file name should be used in the command so that each command starts with `./terminaldeploymenttool.bat`

Registering the cloud terminal in SAFEQ Cloud Web UI

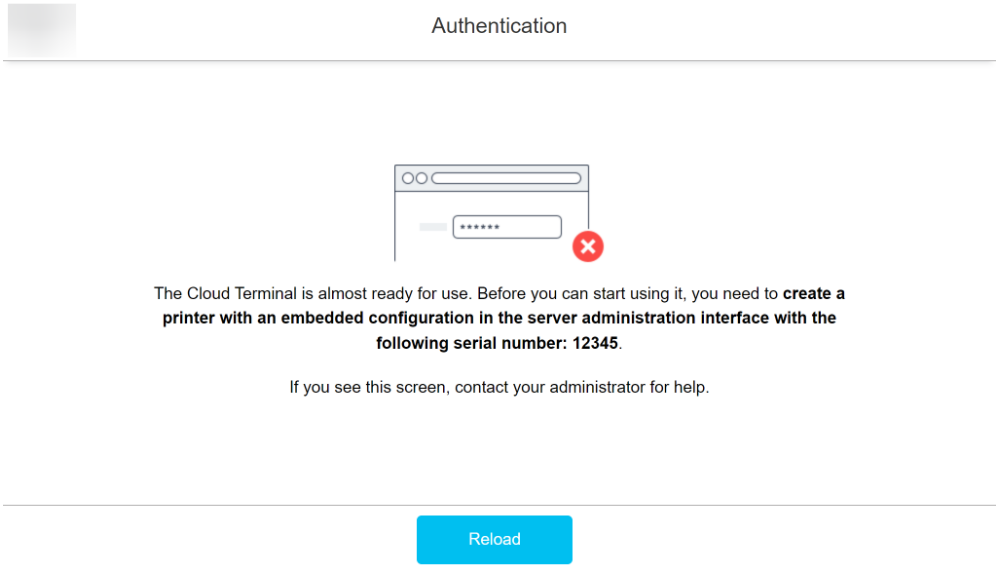
1. Upon installing the MFD, you will see a screen with the **Serial Number** of the device (prefixed with **xe_**). Note down the ID number.



2. In SAFEQ Cloud web UI, go to **Security > Endpoints** and find the entry with ID number that you noted in the previous step. Select the entry and click **Authorize selected**.



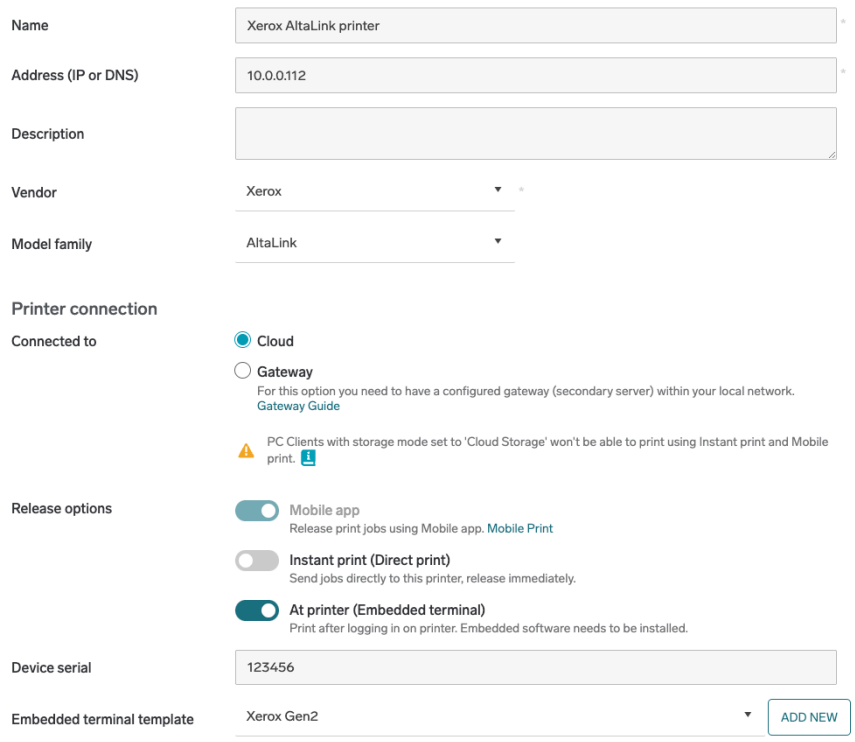
3. Back on the MFD, you will see the following screen:



Adding the Xerox printer and Embedded configuration in SAFEQ Cloud Web UI

These steps are optional and if not performed, the Xerox printer will be added automatically after the endpoint is authorised, see *Registering the cloud terminal in the SAFEQ Cloud Web UI* section of this page.

1. In the SAFEQ Cloud Web UI, go to **Printers** > **Embedded templates**.
2. If not done already, create an embedded configuration for your Xerox MFD(s) by clicking **Add**.
3. In **Vendor**, select **Xerox**.
4. In **Application type**, select **Xerox Gen 2**.
5. Fill in the rest of the configuration according to your needs and click **Save**. For more information on embedded configuration, see Embedded Terminals' configuration.
6. Go to **Printers**.
7. Click **Add**.
8. In **Vendor**, select **Xerox**.



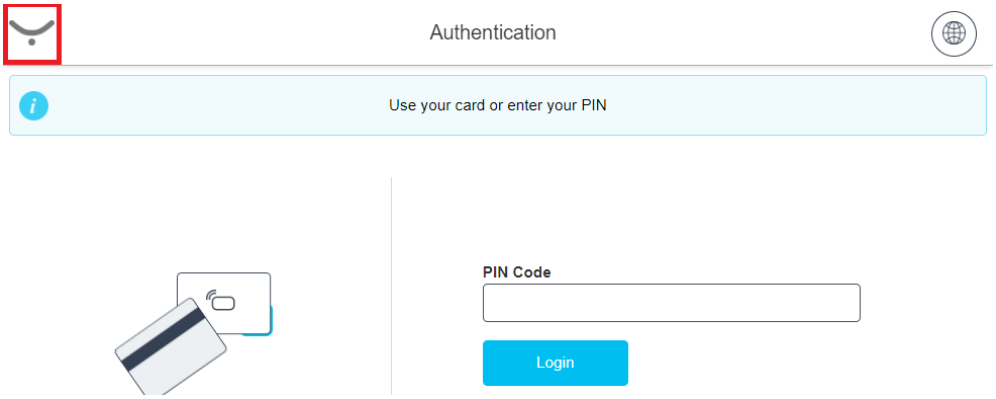
9. Fill in all required information.
10. Select the **At printer (Embedded terminal)** release option**.** This will display additional fields related to embedded configuration.
11. In **Embedded configuration**, select your Xerox embedded configuration from the list.
12. Click **Save**.

13. Return to MFD, if you see the screen from the end of the previous section tap **Reload**. The MFD will now display a login screen with your chosen authentication type.

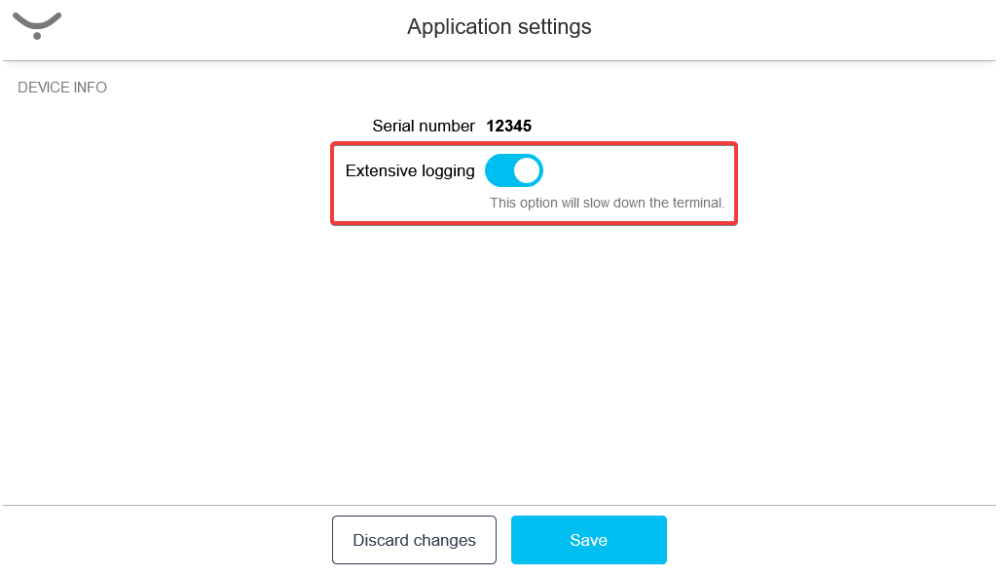
Extensive logging

In case of problems, we might ask you to enable detailed logs from the terminal. This is done in the **Application settings** menu. Note that this option may significantly slow down the terminal.

1. At the MFD, go to the **Authentication** or **My quick actions** screen.
2. Tap and hold the logo in the top-left corner for at least 5 seconds (note that the logo will be different if you have set up a custom logo in the SAFEQ Cloud Web UI).



3. Enable **Extensive logging**.



4. Tap **Save**.

How to use YSoft MFX and TWN4 card readers with older VersaLink devices

The older Xerox VersaLink devices use plugins for card authentication. This section describes how to use the TWN4 readers and the YSoft MFX readers with these devices

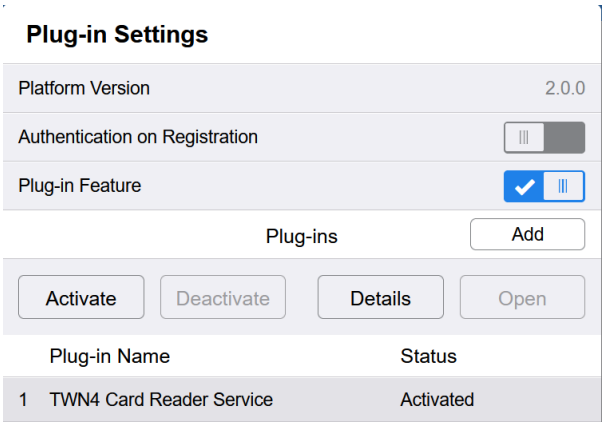
The screenshots were taken on Xerox VersaLink B605 and Xerox VersaLink C405DN. The UI may look different on other models.

TWN4 card readers

To use the TWN4 card reader, connect it to the MFD. The cloud terminal will detect the connected card reader, and card authentication will work out of the box.

In case of problems, check if the TWN4 card reader service plugin is active:

1. Log in to the MFD's admin interface.
2. Go to **System > Plug-in settings**.
3. Check if the **Plug-in Feature** is enabled. If not, activate the TWN4 Card reader service.



4. Restart the MFD.

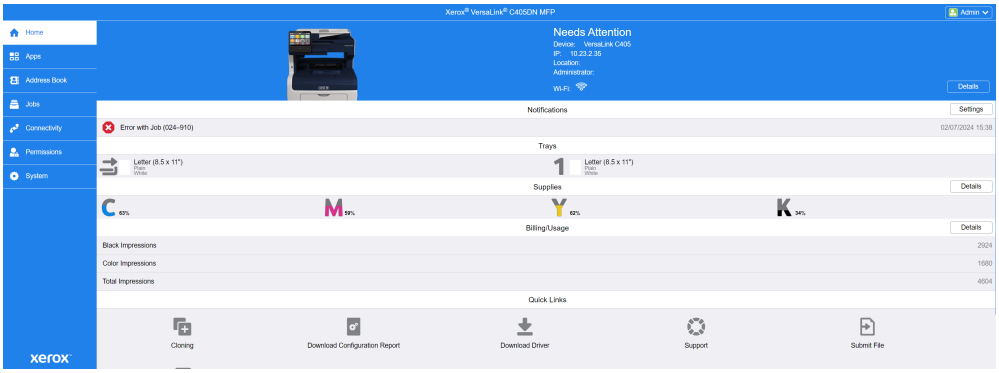
YSoft MFX card readers

> ⚠ This step is done automatically during installation via the Terminal Deployment Tool. Use the following guide in case of the plugin setup failing consistently during the installation.

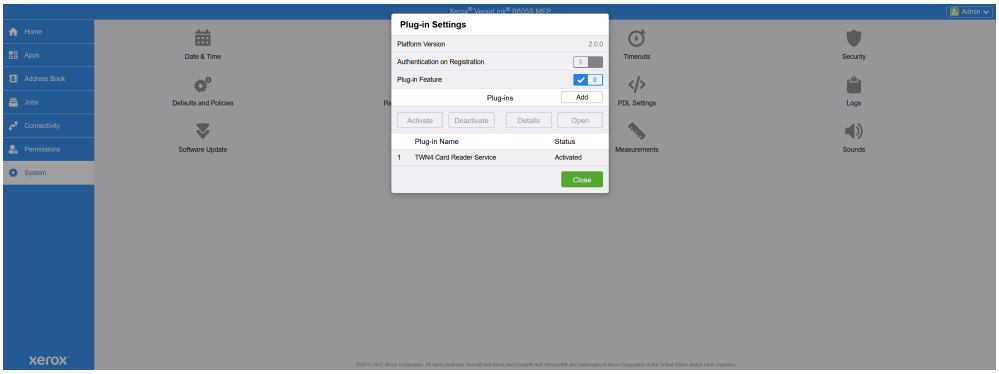
For the YSoft MFX reader, you must install two plugins (CardPlugin and CardService) manually. They are part of the terminal deployment tool and they can be found in `terminaldeploymenttool/packages/xerox/.`

To install the plugins, perform the following steps:

1. Log in to the MFD's UI as an administrator.

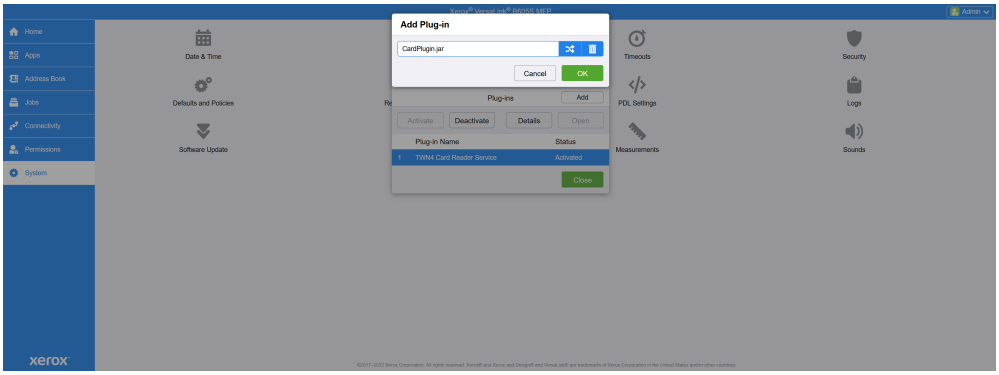


2. Go to the system settings and enable the **Plug-in feature**.



3. Notice that the TWN4 card reader service is enabled. You must deactivate it (it cannot be deleted).

4. Add both plugins from the terminal deployment tool and activate them.



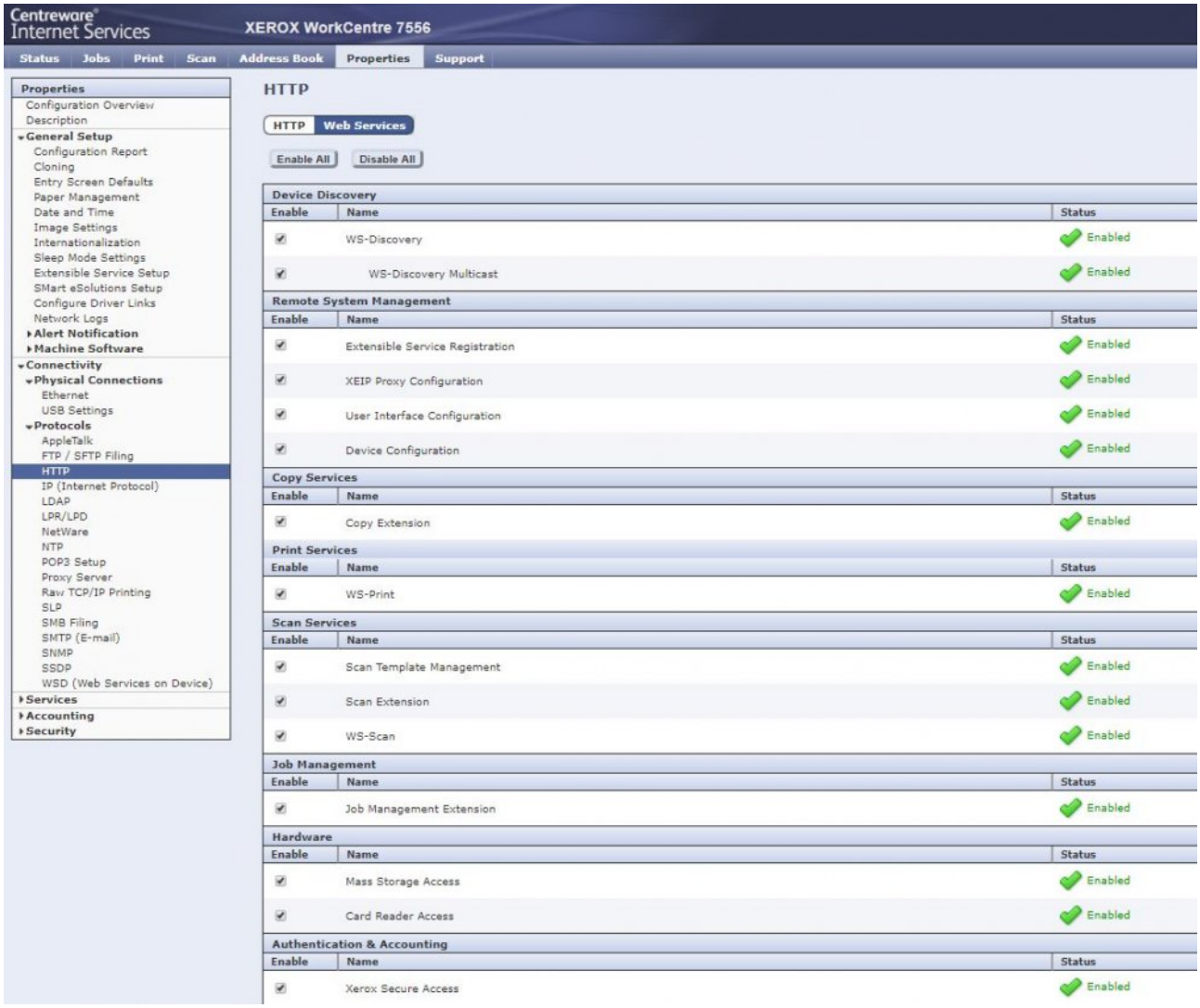
5. Restart the device in order to deactivate TWN4 and activate the new plugins.

Xerox Gen 1 Terminal

To configure SAFEQ Cloud on Xerox devices

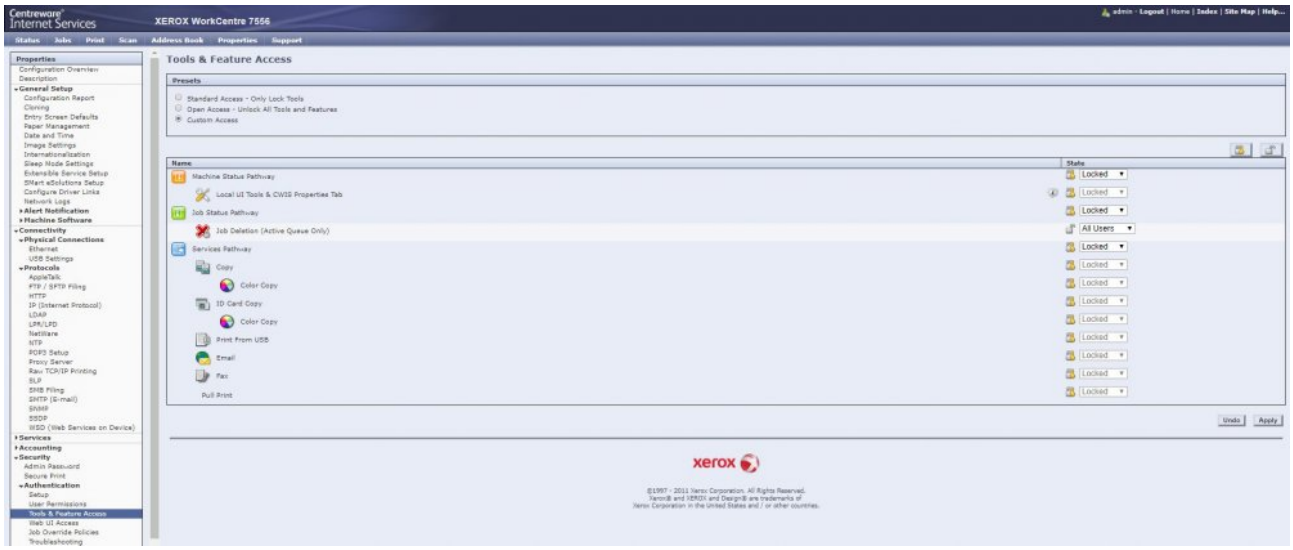
- Open the webinterface of the device in a browser
- Log in to the device (Default username and password is *admin* and *1111*)
- Locate the "HTTP"-settings and enable the HTTPS

Afterwards push the "Web Services" and activate "Xerox Secure Access"
(Location of "Xerox Secure Access" depends on model)



Restart the printer and push the Embedded configuration from embedded screen in SAFEQ Cloud. Make sure your secondary gateway is configured according to Secondary Gateway mapping.

If you want to lock down all functions, set them all to "Locked" in "Authentication" and "Tools & Feature Access". (Location of these menus can vary depending on model)

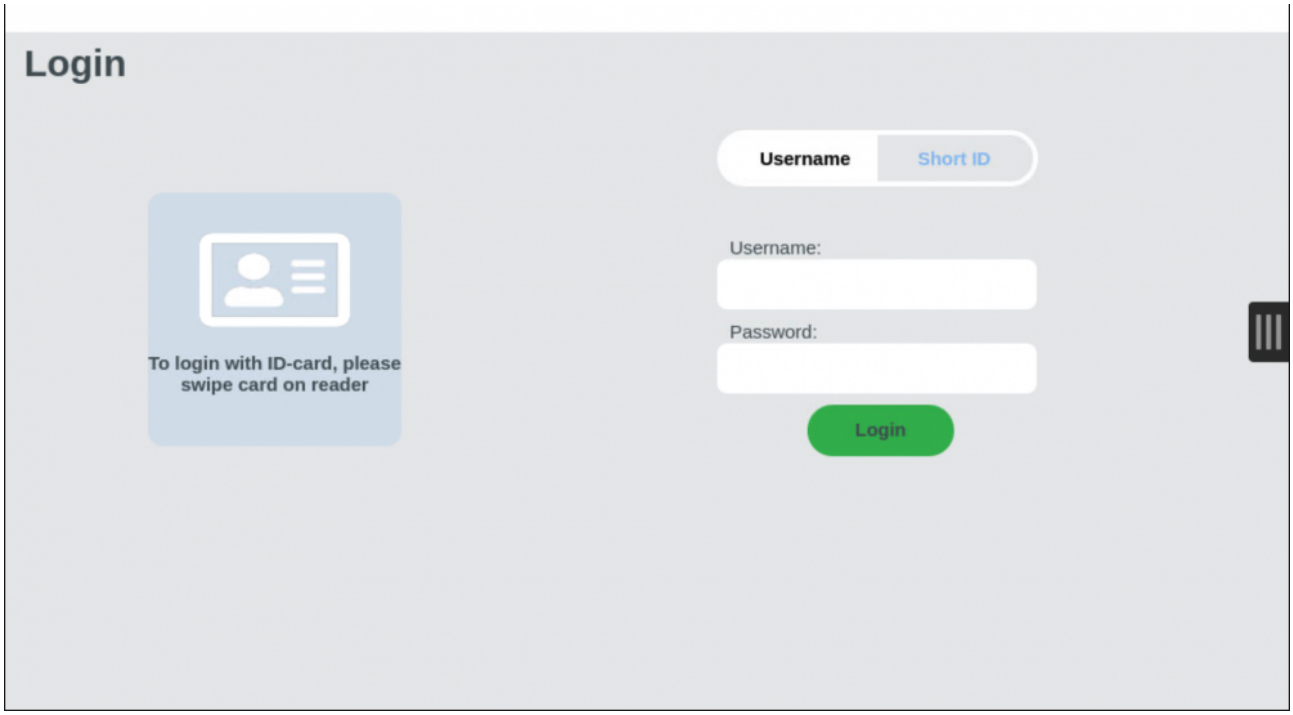


Embedded UI

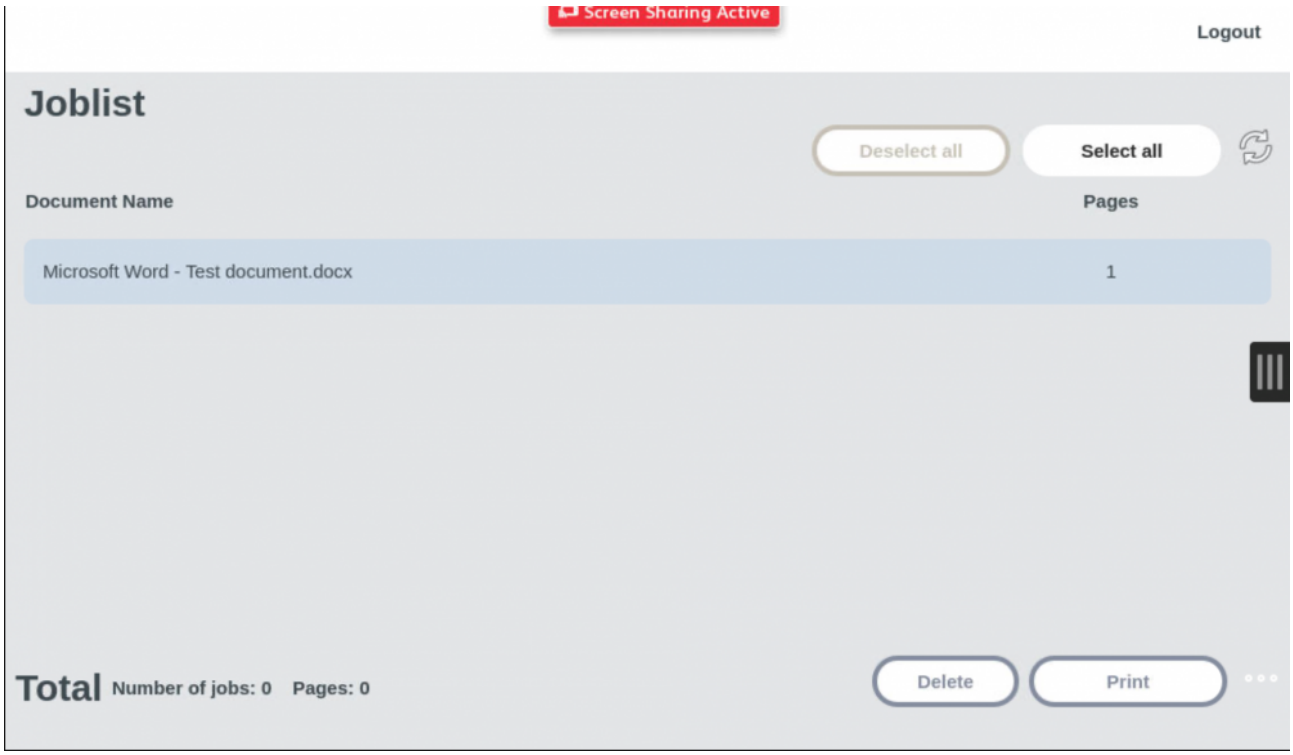
The Xerox Embedded has two different UI's dependent on the screen functionality of the printer. The Xerox embedded will automatically check the screen functionality and deploy the appropriate UI.

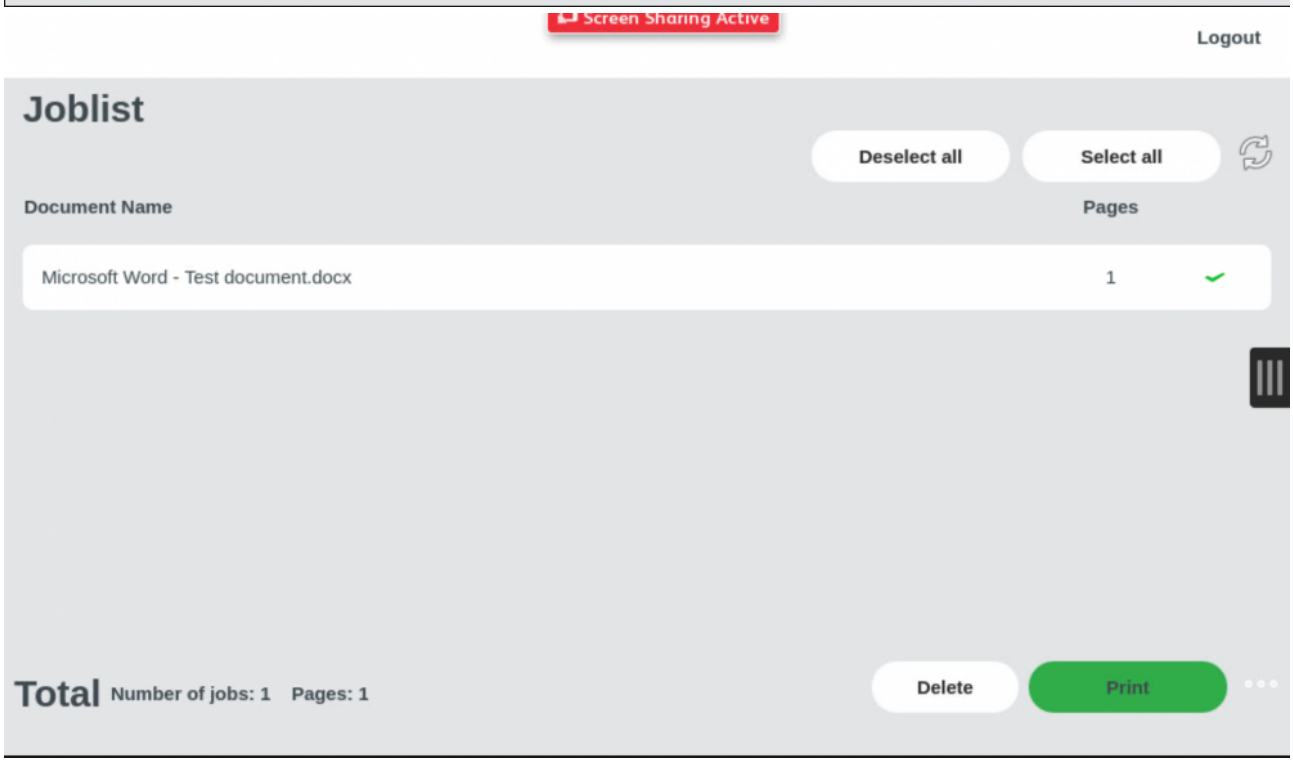
On new devices the UI will be as presented below:

Login with Username/Password or Short ID:

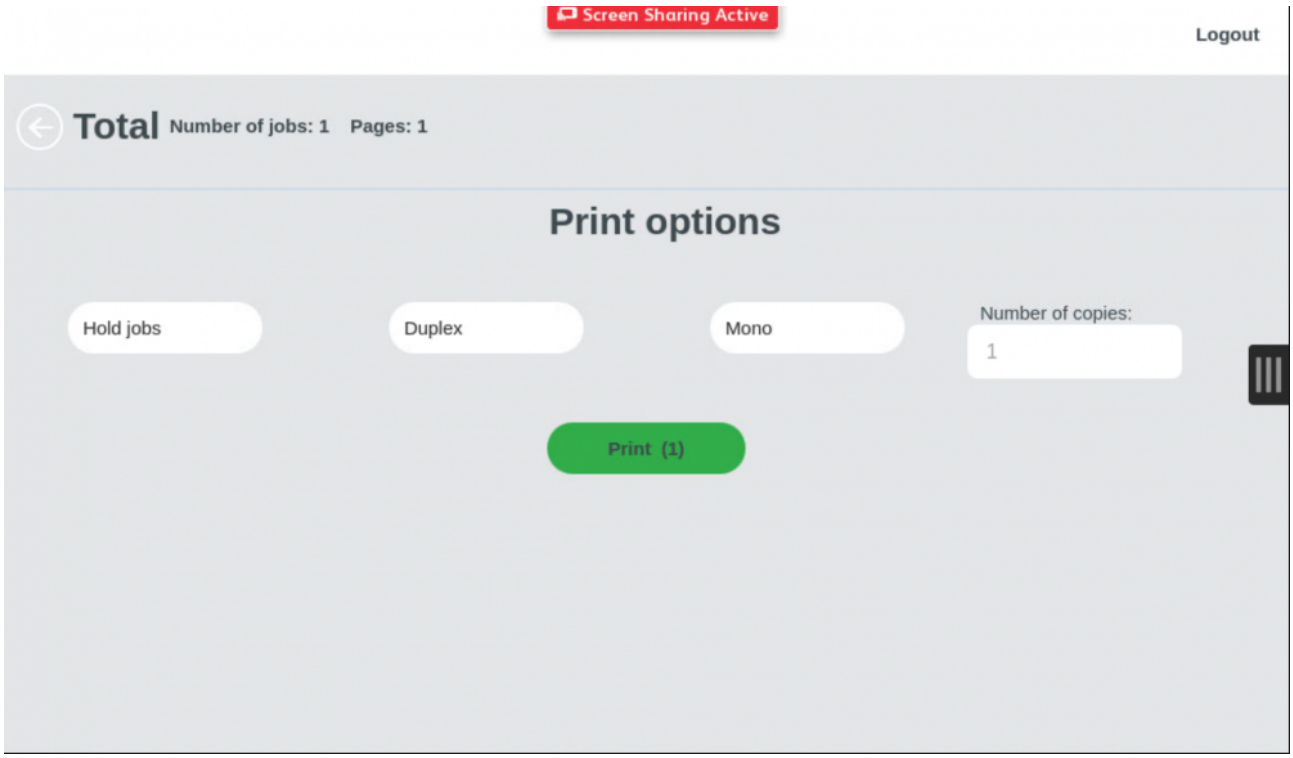


Joblist:





With the Xerox embedded it is possible to change settings of the print job on the printer:



Xerox WorkCentre 71xx

Enable extensible services browser

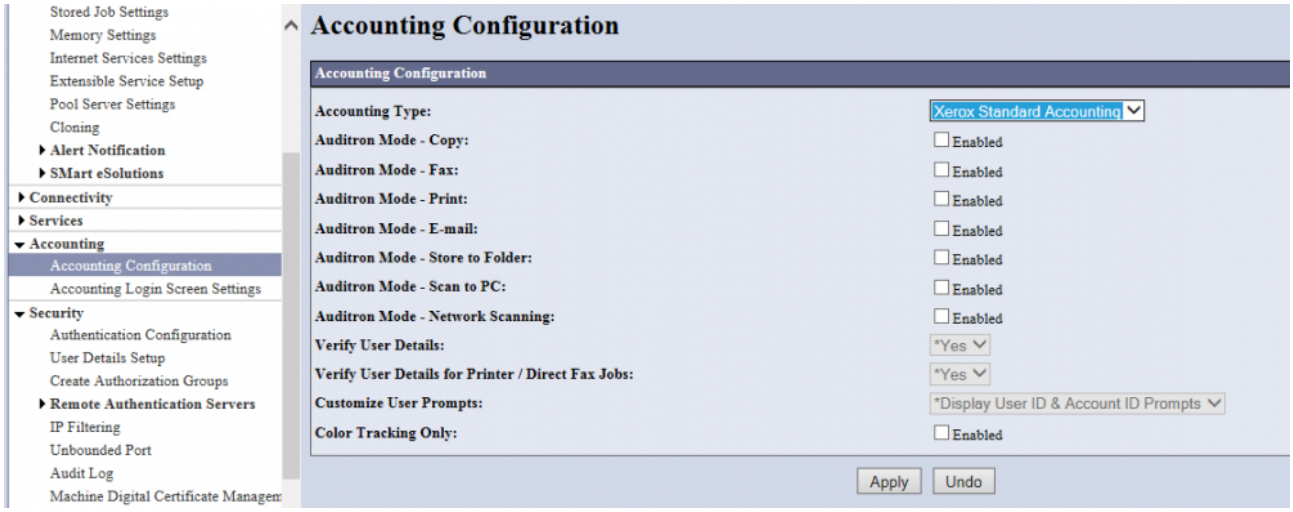
Enable the **Extensible Services Browser**; otherwise, it is not possible to choose pull print at the printer.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. Under **Browser Settings** check the **Enable the Extensible Services Browser**, and click **Apply**.

Enable Accounting on the printer

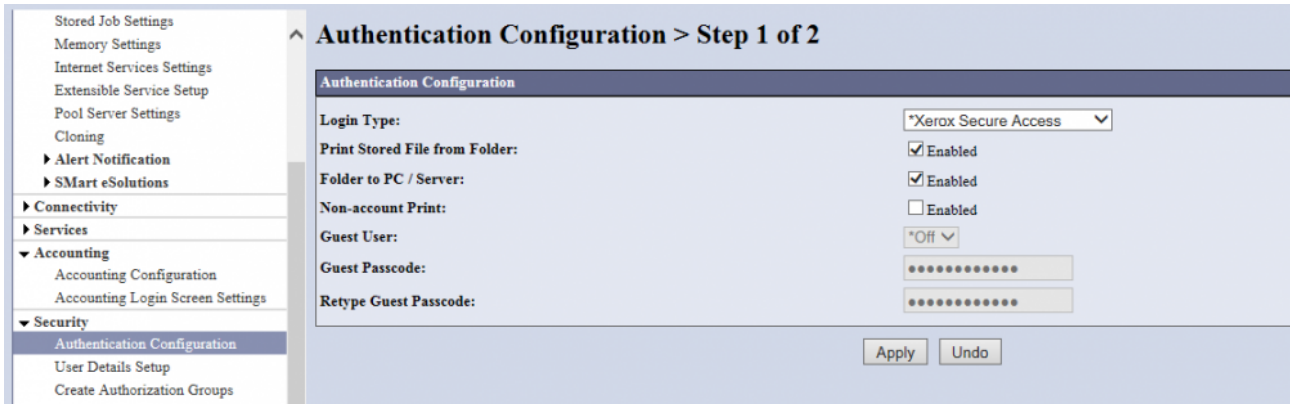
1. Open the printer's web page and click on the **Properties** tab.

2. Select Accounting
3. Click Accounting Configuration
4. On the Accounting Configuration select the Xerox Standard Accounting
5. Click Apply. Click OK.

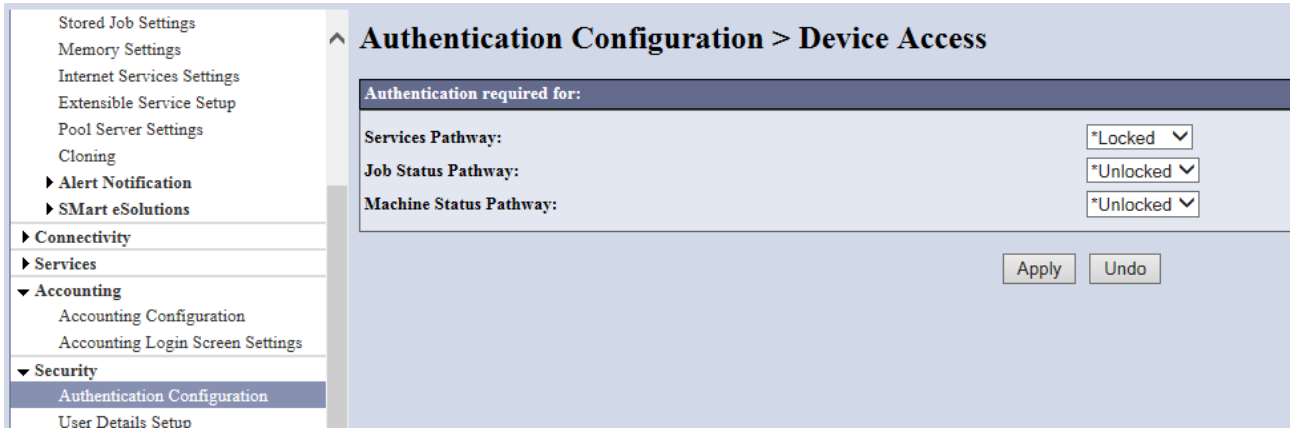


Enable Authentication on the printer

1. Open the printer's web page and click on the Properties tab.
2. Select Security.
3. Click Authentication Configuration.
4. On the Accounting Configuration select the Xerox Secure Access.

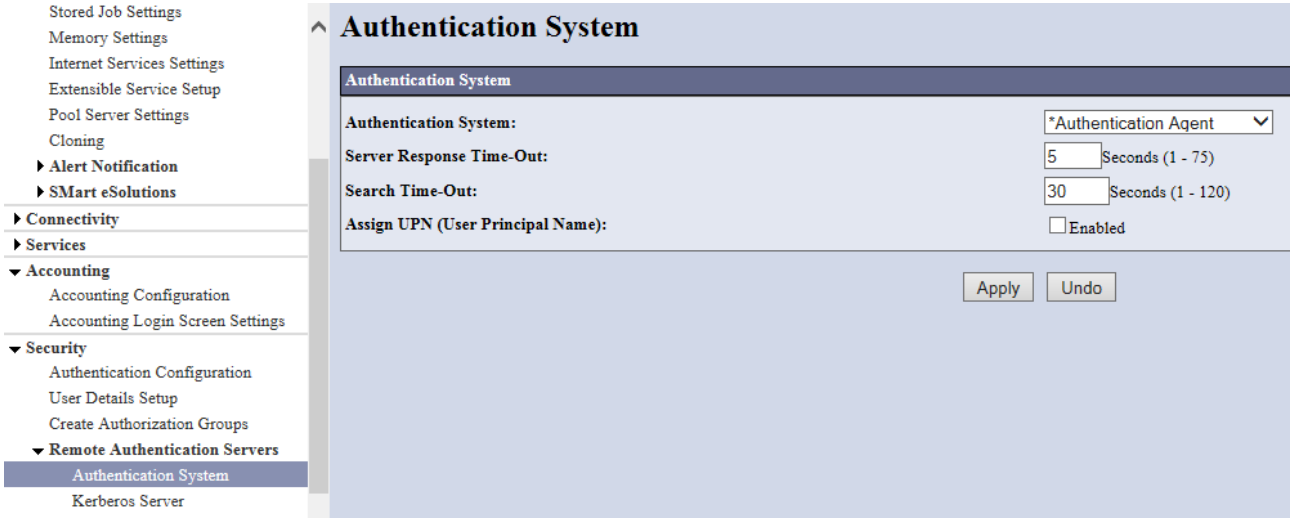


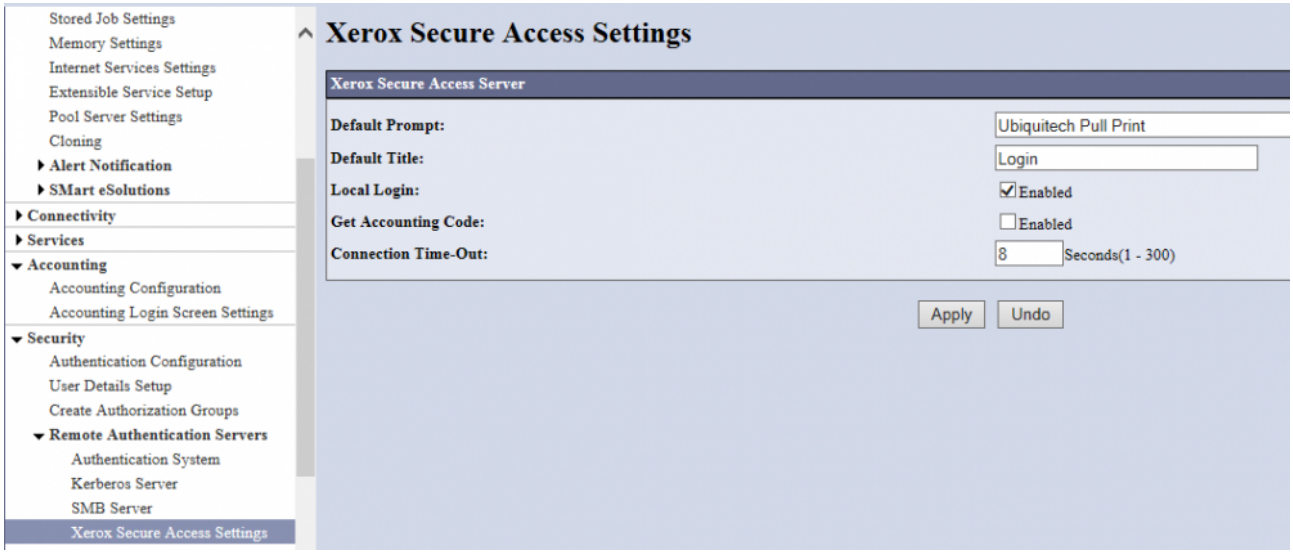
1. Click Apply. Click OK.
2. Configure the Device and/or the Service access according to the customer setup for blocking access to device.


Stored Job Settings
Memory Settings
Internet Services Settings
Extensible Service Setup
Pool Server Settings
Cloning
Alert Notification
SMart eSolutions
Connectivity
Services
Accounting
Accounting Configuration
Accounting Login Screen Settings
Security
Authentication Configuration
User Details Setup
Authentication Configuration > Device Access
Authentication required for:
Services Pathway:
*Locked
Job Status Pathway:
*Unlocked
Machine Status Pathway:
*Unlocked
Apply
Undo

Stored Job Settings
Memory Settings
Internet Services Settings
Extensible Service Setup
Pool Server Settings
Cloning
Alert Notification
SMart eSolutions
Connectivity
Services
Accounting
Accounting Configuration
Accounting Login Screen Settings
Security
Authentication Configuration
User Details Setup
Create Authorization Groups
Remote Authentication Servers
IP Filtering
Unbounded Port
Audit Log
Machine Digital Certificate Managem
Authentication Configuration > Service Access
Authentication required for:
Installed Services
Lock All
Unlock All
Copy:
*Locked (Show Icon)
Fax:
*Unlocked
E-mail:
*Unlocked
Store to Folder:
*Unlocked
Scan to PC:
*Unlocked
Send from Folder :
*Locked (Show Icon)
Network Scanning:
*Unlocked
Job Flow Sheets:
*Locked (Show Icon)
Print:
*Locked
Pull Print:
*Locked (Show Icon)
Apply
Undo

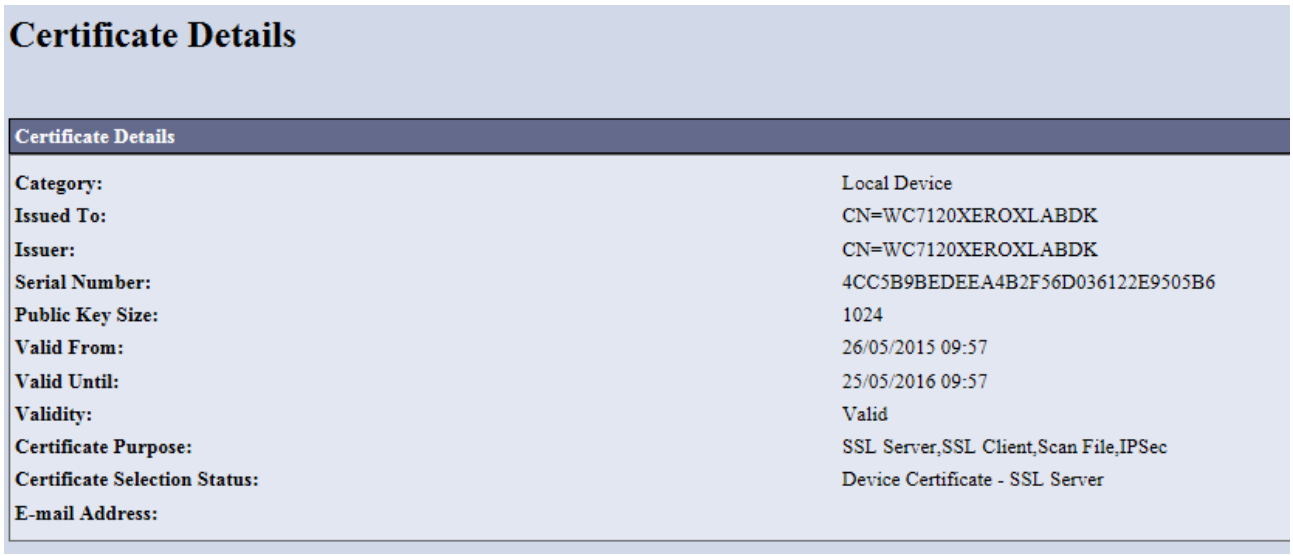
Stored Job Settings
Memory Settings
Internet Services Settings
Extensible Service Setup
Pool Server Settings
Cloning
Alert Notification
SMart eSolutions
Connectivity
Services
Accounting
Accounting Configuration
Accounting Login Screen Settings
Security
Authentication Configuration
User Details Setup
Create Authorization Groups
Remote Authentication Servers
IP Filtering
Unbounded Port
Audit Log
Machine Digital Certificate Managem
Authentication Configuration > Step 2 of 2
Authentication - (Required)
Authentication System:
Configure...
Kerberos Server:
Configure...
SMB Server:
Configure...
LDAP Server:
Configure...
LDAP User Mappings:
Configure...
LDAP Authentication:
Configure...
LDAP Authorization Access:
Configure...
Custom Filters:
Configure...
Device Default State Configuration
Device Access:
Configure...
Service Access:
Configure...





Create certificate on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Certificate Management**.
3. Click **Add**.
4. Select **Create Xerox Device Certificate**.
5. Click **Continue**.
6. Complete the form with the requested information (Use Printers hostname for CN).
7. Click **Finish**.



Embedded Plug-ins

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then select **Plug-in settings**.
3. Click **Plug-in Settings**.

4. Upload the plugin needed for the reader.
5. Click **Finish**.

Xerox WorkCentre 52xx, 72xx, 73xx and 74xx

Some devices might not have the Network Accounting software/kit install. This can be ordered from Xerox.

Enable certificate on the printer

When you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

After creating the certificate, check the date *and* time for when the certificate becomes valid on the device web page by clicking the certificate in the address field.

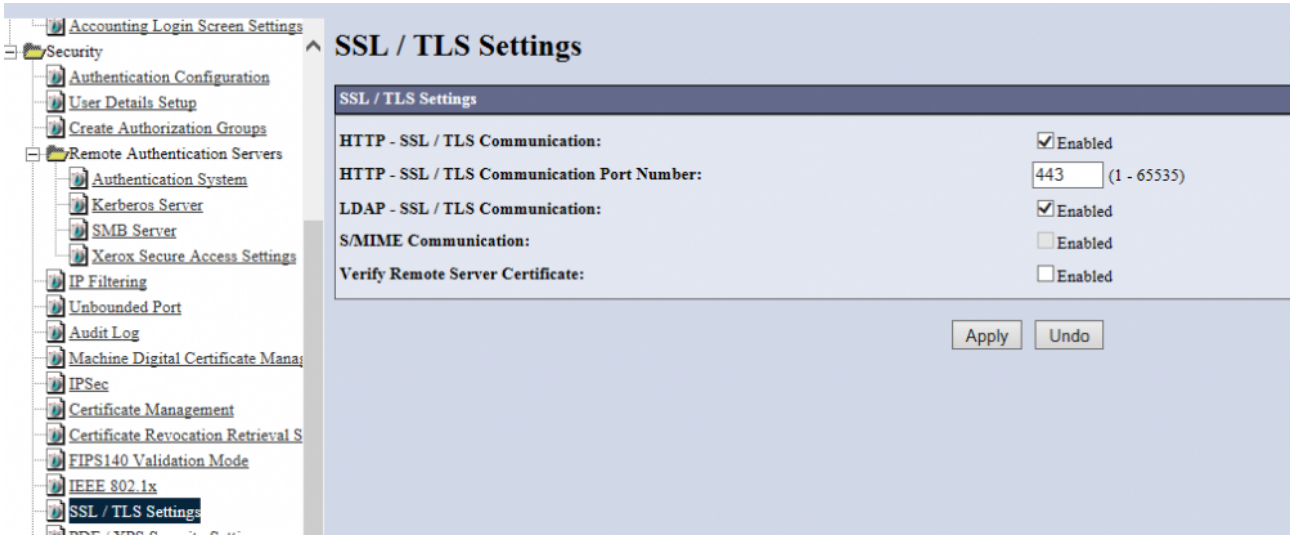
Click **View certificates**, then the **Details** tab and make a note of the **Valid from** and **Valid to** dates *and* times.

Create a certificate

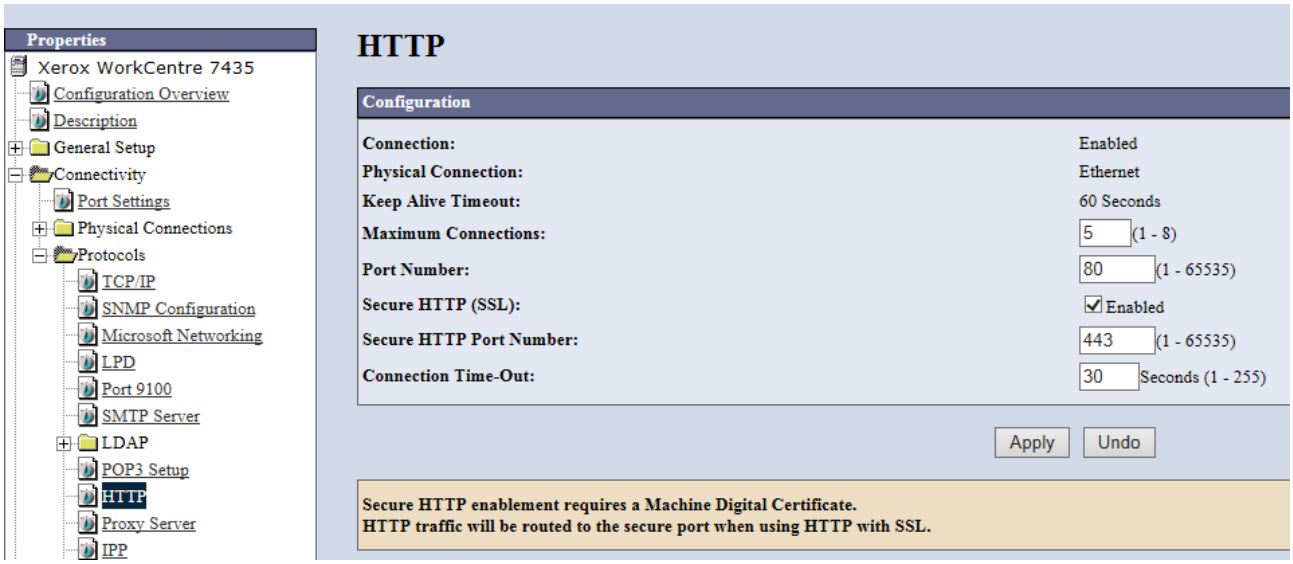
1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management**. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to the next section
3. Click **Create new certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field. Please note that the **maximum** number of days allowed is **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits) even though higher numbers can be entered!
6. Click **Apply**.

Enable HTTPS

1. Click **Security** and then **SSL / TLS Settings** in the menu and confirm that **HTTP – SSL / TLS Communication** is enabled.



2. Click **Connectivity**, **Protocols** and then **HTTP** and check that **Secure HTTP (SSL)** is enabled on port **443**.



3. Click **OK**.
4. Reboot the device.

Enable Custom Services

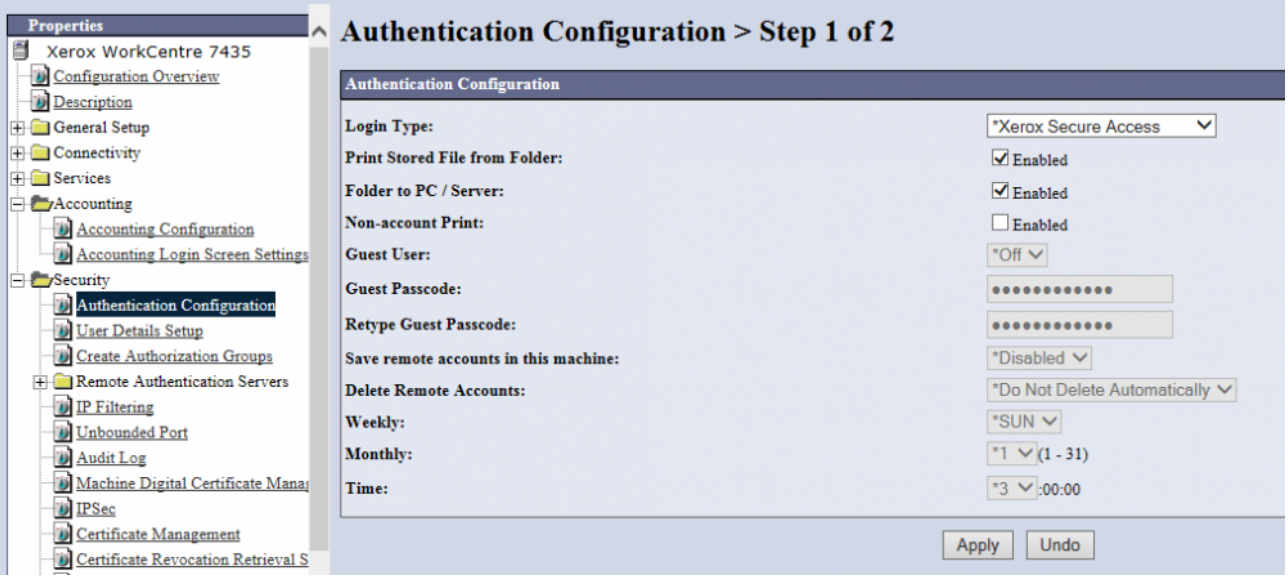
1. Open the printer's web page and select the **Properties** tab.
2. Click **Services**, **Custom Services** and then **Custom Services** on the menu.
3. Select **Enabled** in the **Enabled** area and then click **Apply**.
4. The **Custom Services** button should now be present on the touch screen of the printer when All Services are selected. If not, you may have to power cycle the printer.

Enable ports

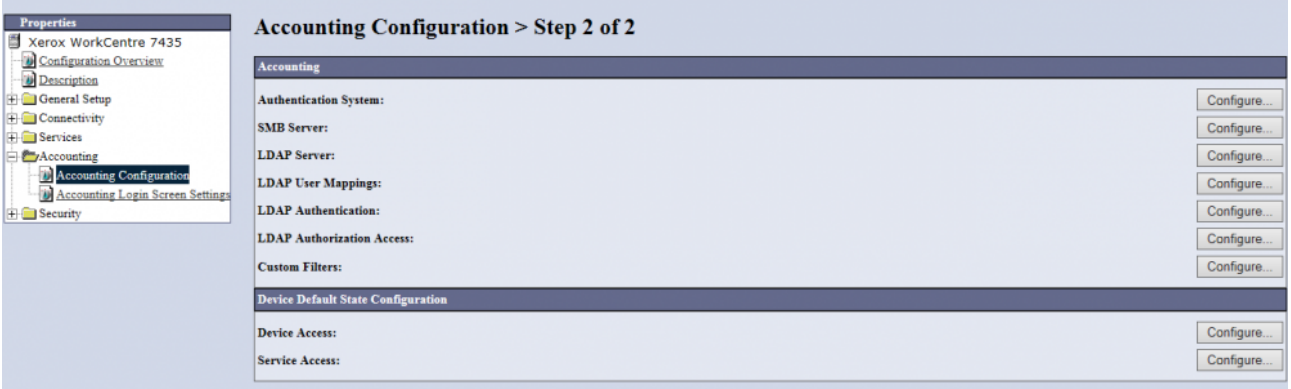
1. Open the printer's web page and click on the **Properties** tab.
2. Click the **Connectivity** and then **Port Settings**.
3. Check **SNMP**, **SMB**, **FTP Client** and **SOAP**.

Configure authentication and access control on the printer

1. Open the printer's web page and select the Properties tab.
2. Click **Security** and then click **Authentication Configuration** in the menu
3. Ensure that **Xerox Secure Access** is selected in the **Login Type** box

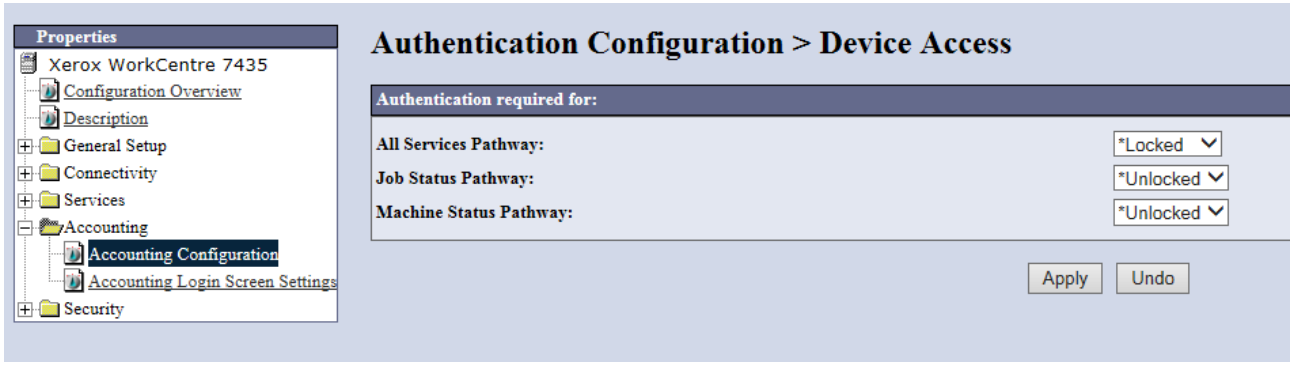


4. Click **Apply**.
5. Click **Reboot Machine**. Click **OK** to reboot. This reboot MUST occur otherwise the subsequent steps cannot be performed. After the reboot, continue with the remaining steps.
6. Open the printer's web page and click on the **Properties** tab.
7. Click **Security** and then click **Authentication Configuration** in the menu.
8. Click **Next**.
9. From the **Device Default State Configuration** area, you can configure either:



- **Device Access** By locking the Service Pathway (recommended) the users would be requested to authenticate to access all available services: Copy, E-mail, Custom Services, etc.
  A. Under **Device Default State Configuration**, next to **Device Access**, click **Configure**.

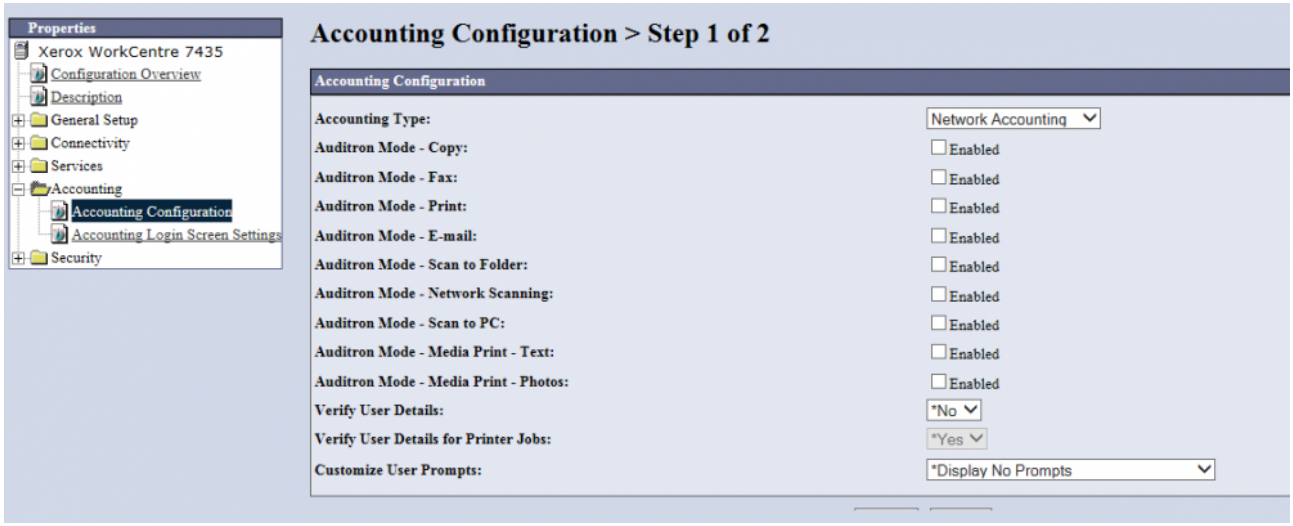
B. Select **Locked** for **Services Pathway** to require authentication for all services at the control panel. If is recommended to leave the **Job Status Pathway** and **Machine Status Pathway** unlocked. They control the access to the Job status and the Machine Status button.

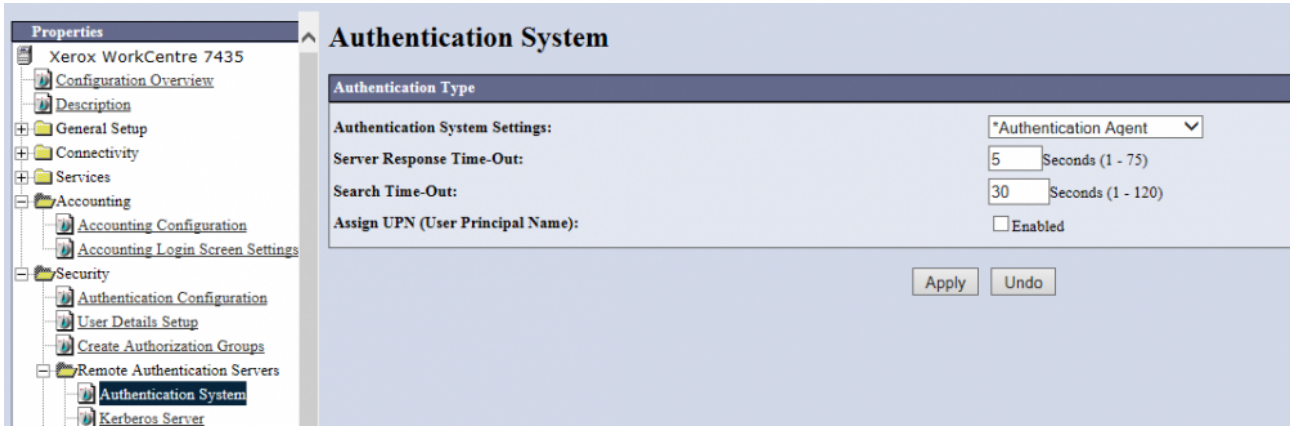


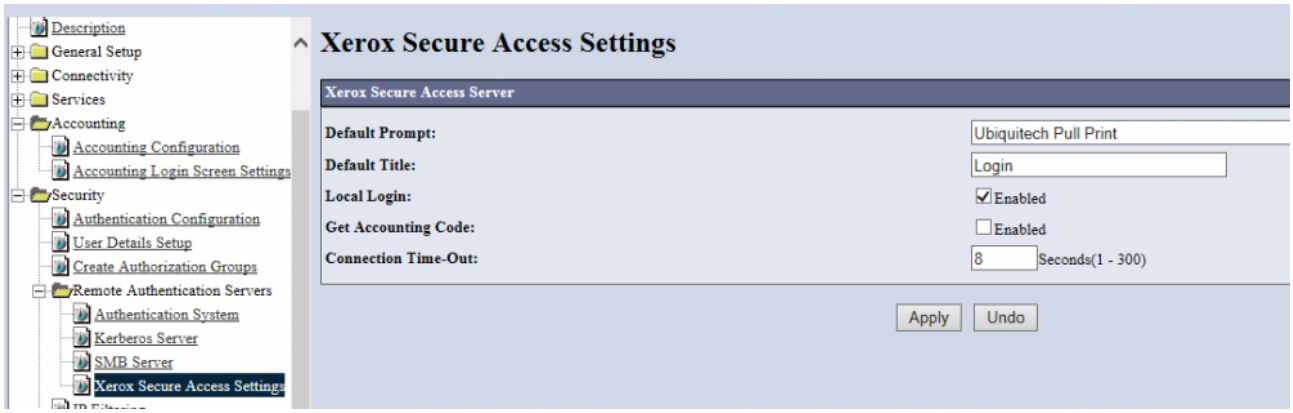
C. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

- **Service Access** Instead of device access, it is possible to control access on a per-service basis. However, Custom Services must always be locked, because otherwise the One Q solution does not know who the user is.
  A. Under **Device Default State Configuration**, next to **Service Access**, click **Configure**.
  B. Select **Locked (Show Icon)** for **Custom Services** so users must authenticate to access the Pull Print icon on the control panel. Select **Locked** to require authentication for any additional services.

C. Click **Apply** to accept the changes or **Undo** to retain the previous settings.







Xerox WorkCentre 75xx

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might not be valid until the following day.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Security Certificates**.
3. Click **Add**.

4. Select Create Xerox Device Certificate.
5. Click Continue.
6. Complete the form with the requested information (Use Printers hostname for CN).
7. Click Finish.

Enable HTTPS on the printer

1. Open the printer's web page and click on the Properties tab.
2. Click Connectivity, Protocols and then HTTP and check that Secure HTTPS is Enabled on port 443.
3. Click Apply.
4. Click OK to restart the device's web server.
5. Click Reboot Machine. Click OK to reboot.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the Properties tab.
2. Click Connectivity Protocols and then HTTP in the menu.
3. Click Web Services at the top of the page. Select Enable next to Extensible Service Registration.
4. Click Apply. Click OK.

Enable extensible services browser

Enable the Extensible Services Browser; otherwise, it is not possible to choose pull print at the printer.

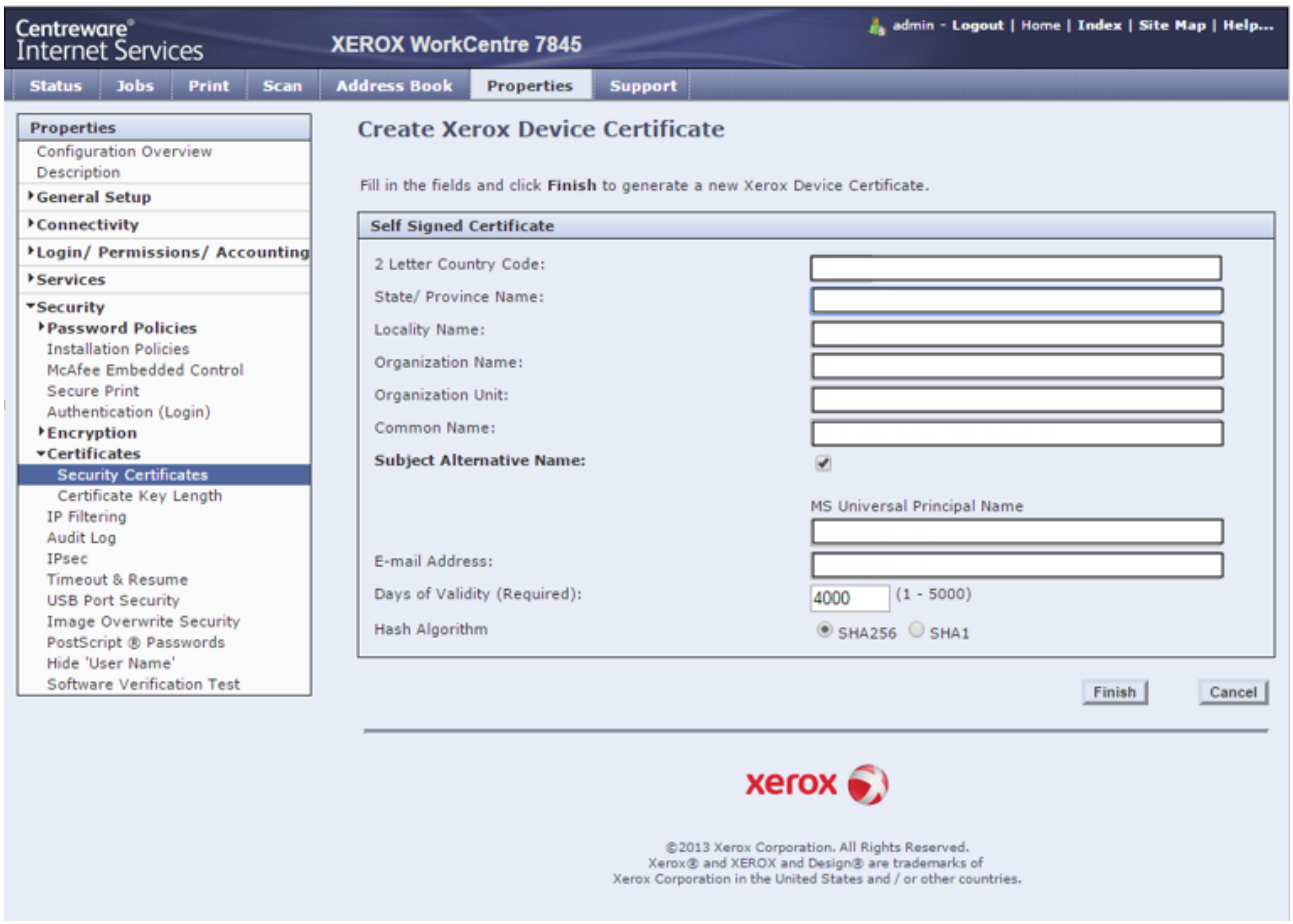
1. Open the printer's web page and click on the Properties tab.
2. Click General Setup and then Extensible Service Setup.
3. Under Browser Settings check the Enable the Extensible Services Browser, and click Apply.

Xerox WorkCentre 78xx

Create a certificate

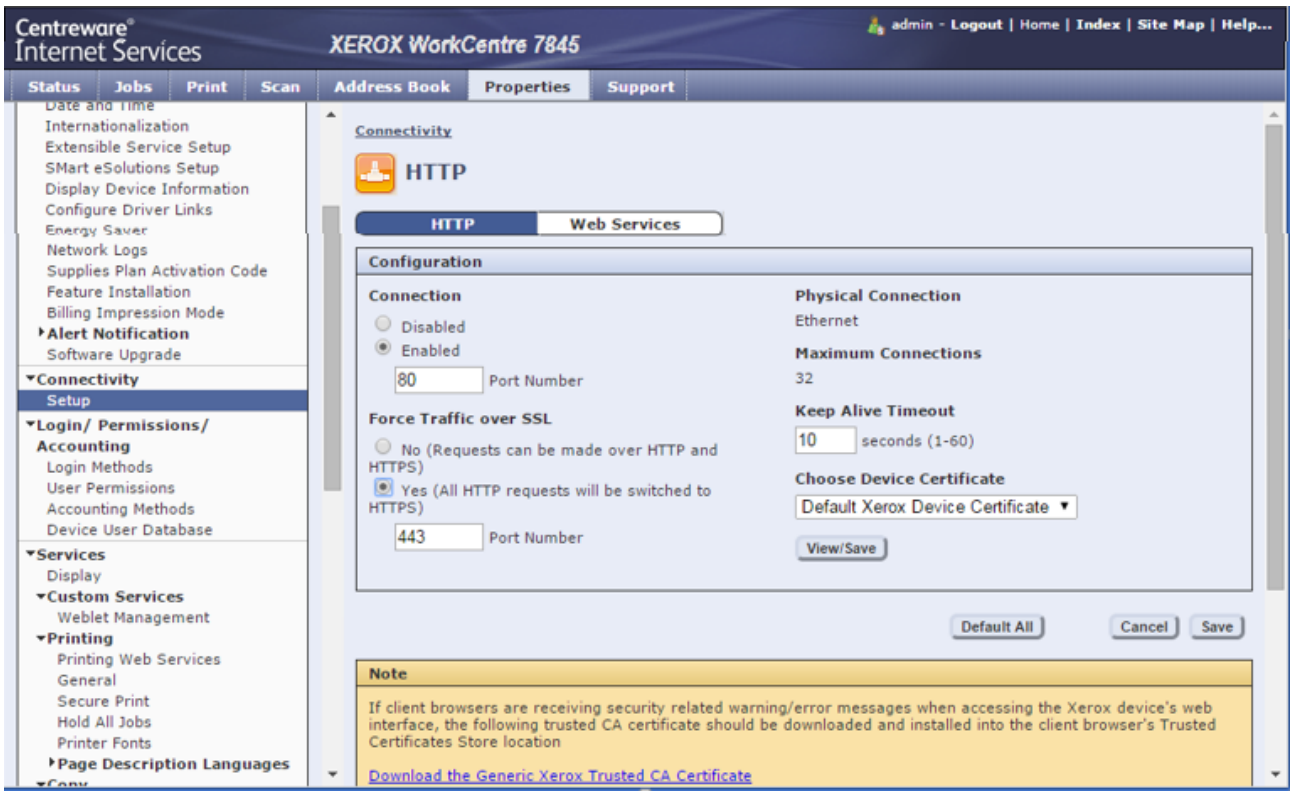
1. Open the printer's web page and click on the Properties tab.
2. Click Security and then Security Certificates.
3. Click Add.
4. Select Create Xerox Device Certificate.
5. Click Continue.
6. Complete the form with the requested information.

7. Click **Finish**.



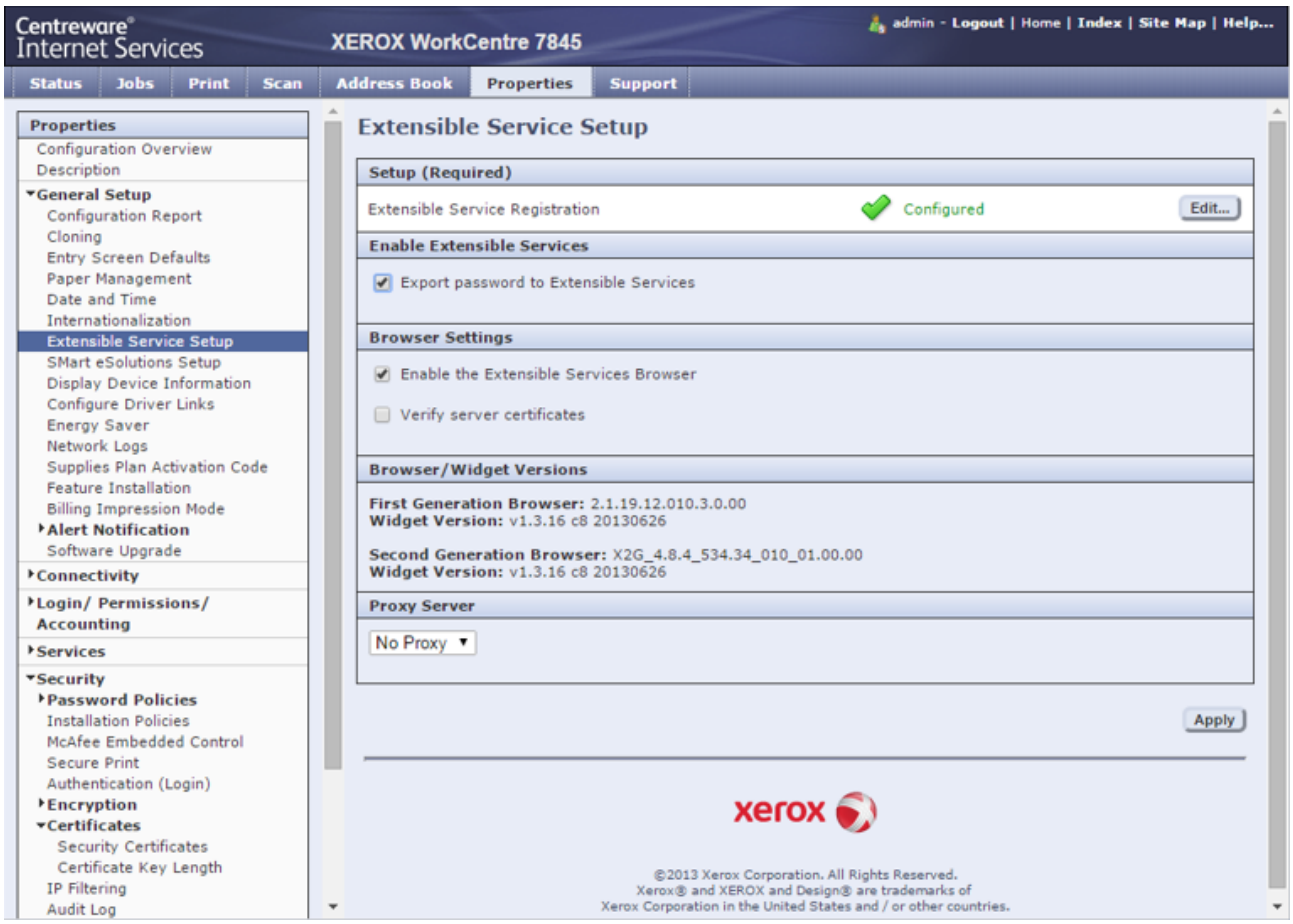
Enable HTTPS on the printer

1. Open the printer's web page and select the **Properties** tab.
2. Click **Connectivity**, **Setup**.
3. On the **Connectivity** page click **Edit** next to **HTTP**.
4. In **Force Traffic over SSL select Yes** (All HTTP requests will be switched to HTTPS) radio button and set **Port Number** to **443**. **Save** and **OK** to restart the device's web server.
5. Reboot MFD.



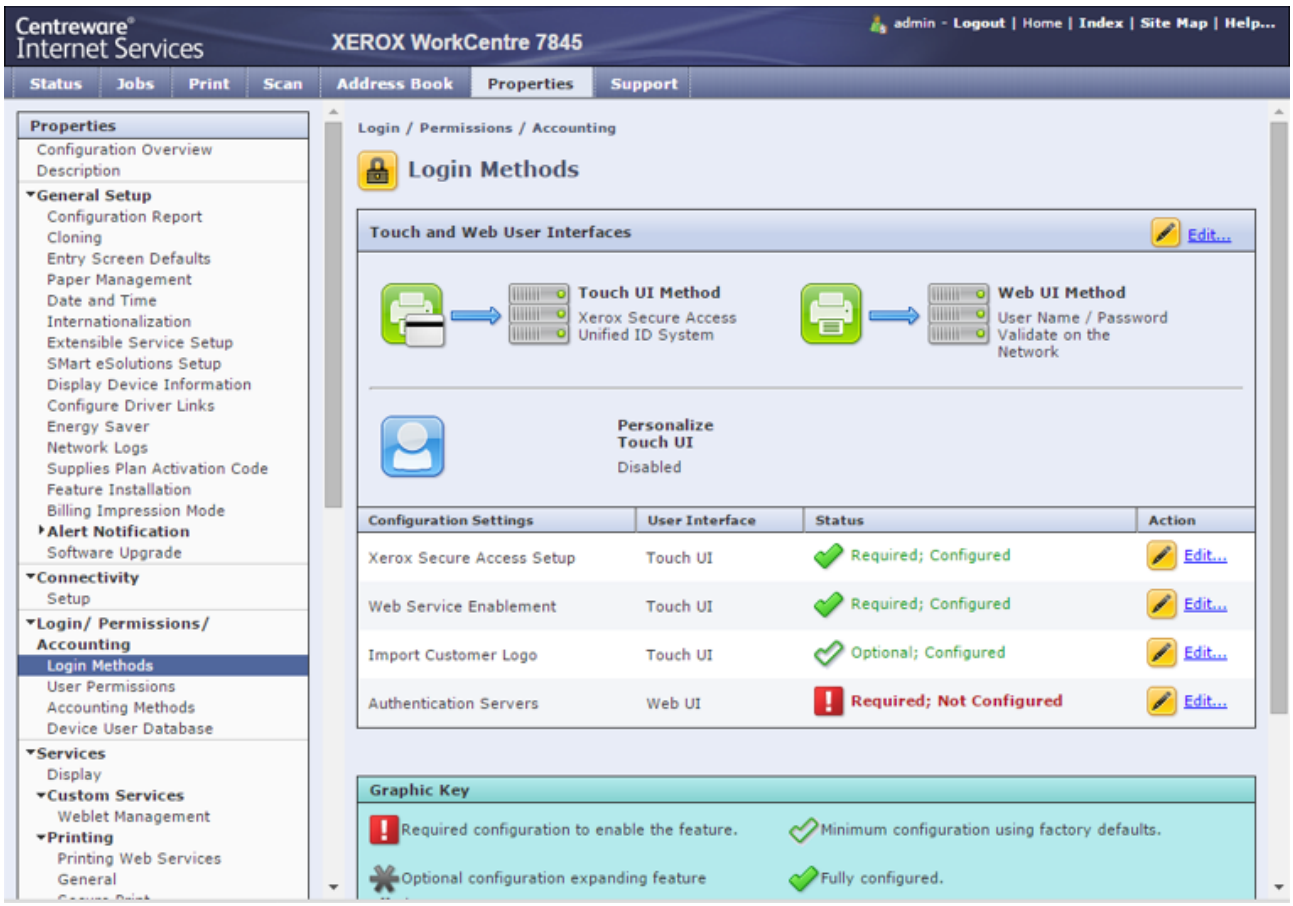
Enable Extensible Service Registration on the printer

1. Open the printer's web page and select the **Properties** tab.
2. Click **General Setup**, **Extensible Service Setup**.
3. Select **Enable** next to **Extensible Service Registration**. Click Apply and OK.

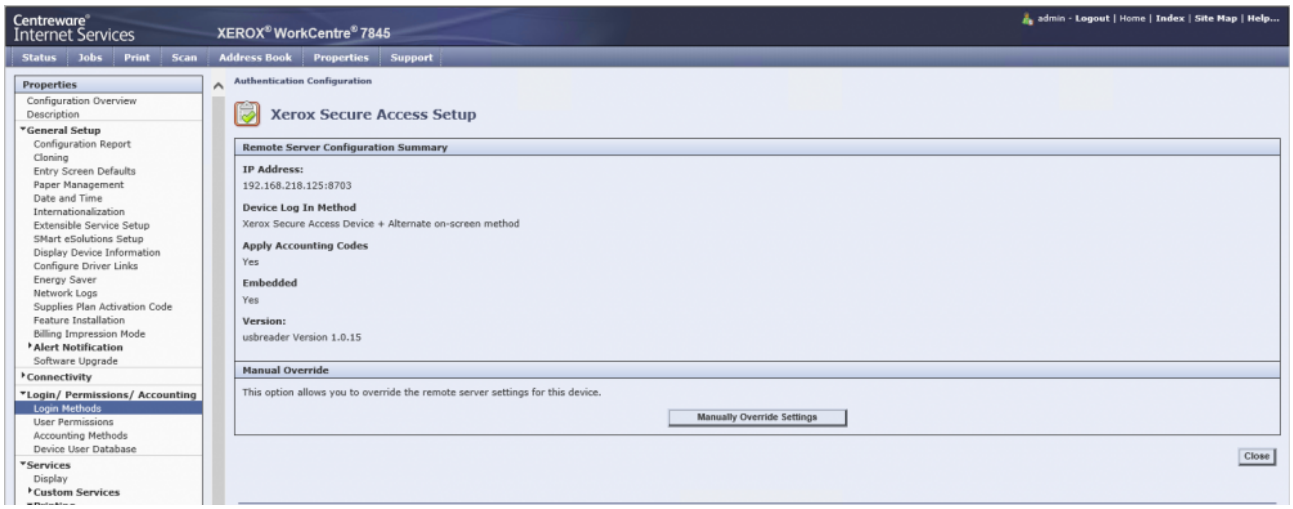


Configure authentication and access control on the printer

1. Open the printer's web page and select the Properties tab.
2. Expand Login / Permissions / Accounting and click Login Methods.



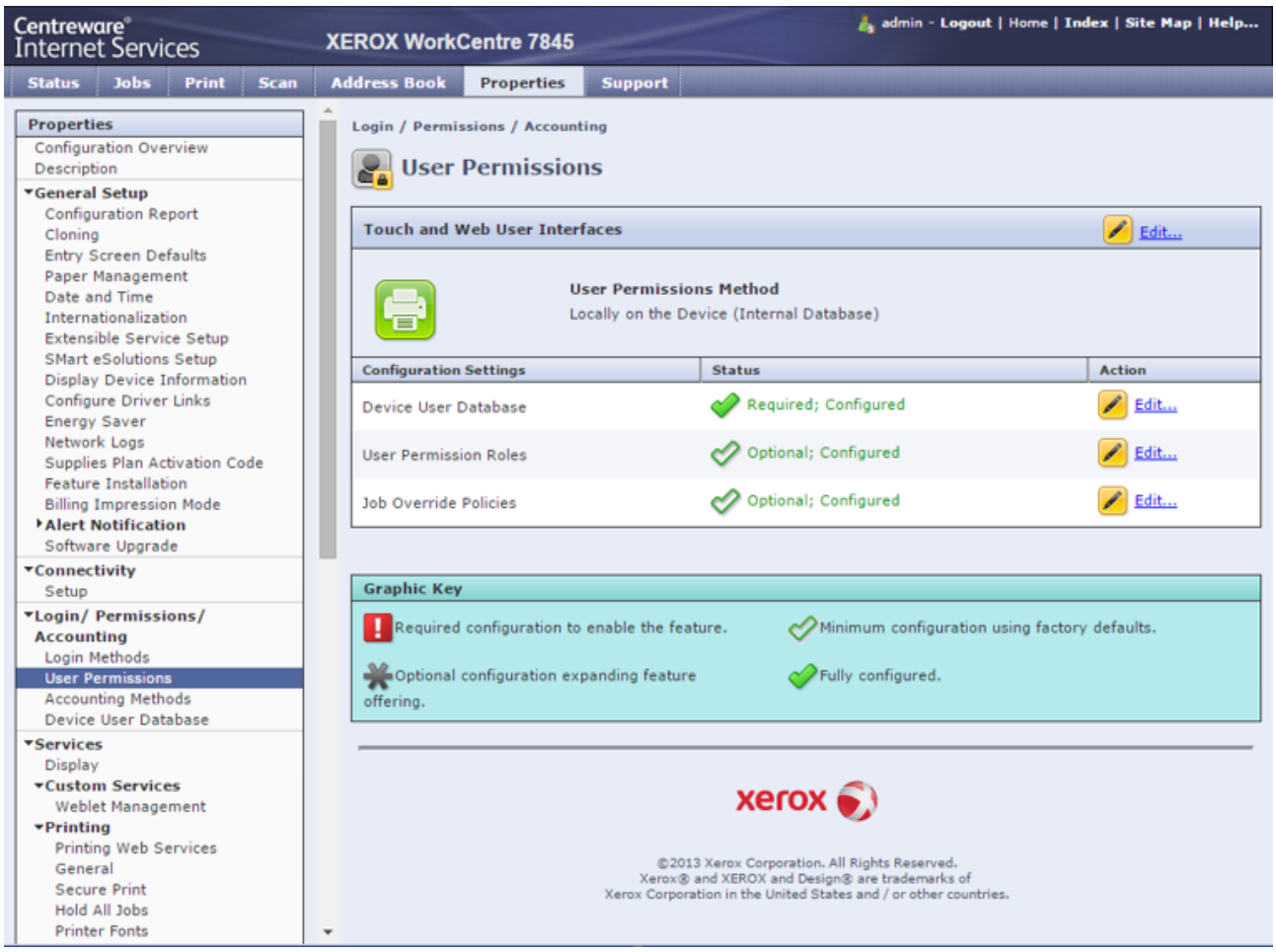
3. On the **Manual Override** page, in the **Device Login Methods** section select the **Xerox Secure Access Device + alternate on-screen authentication** method button.



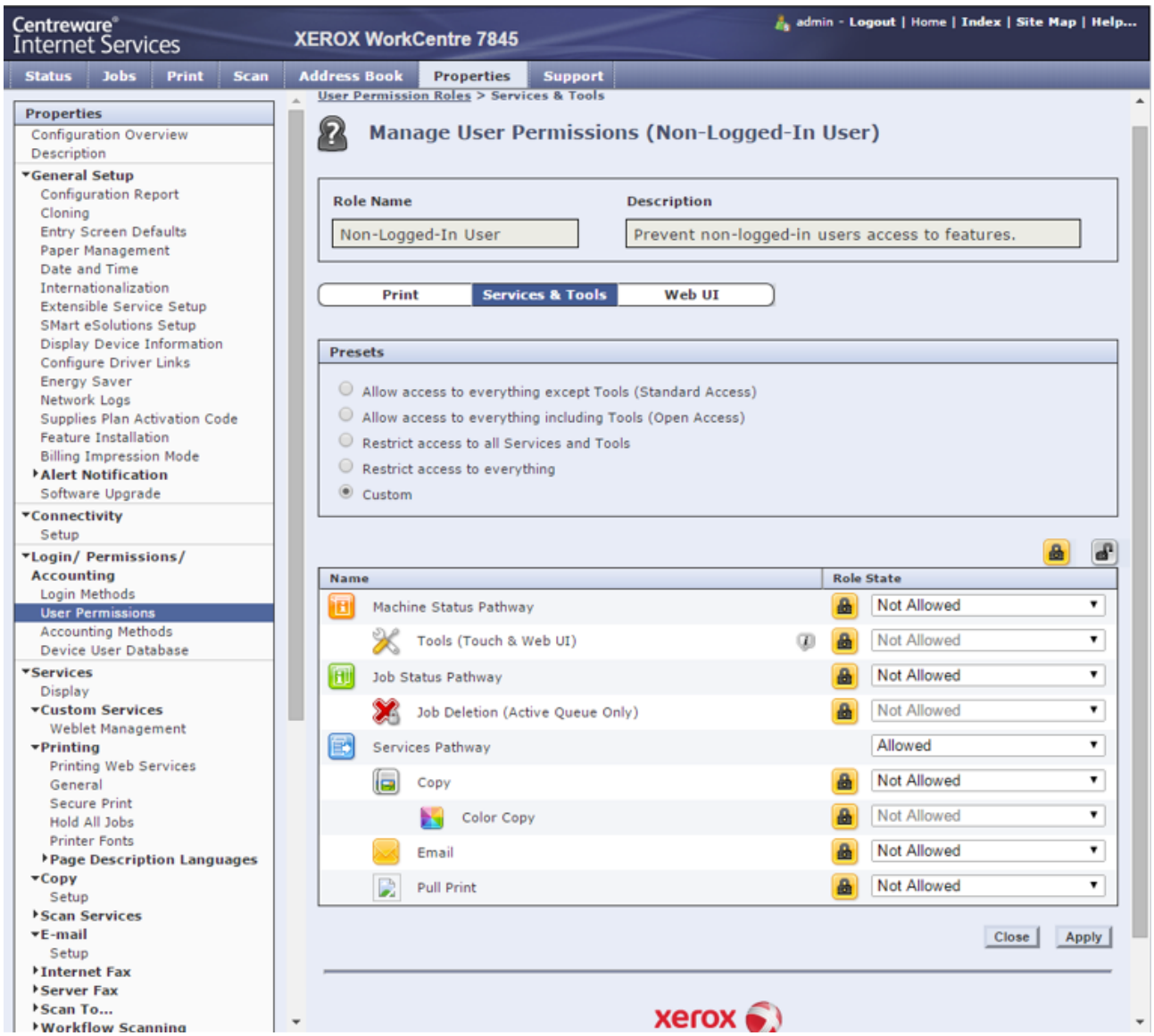
> **Important!** On some Xerox WorkCentre 78xx if 'Embedded' option is checked card readers will NOT work properly. Uncheck 'Embeded' option if is the case.

4. Click **Save**.

5. In the **Properties** menu to the left click **User Permissions** and **User Permissions Roles**.



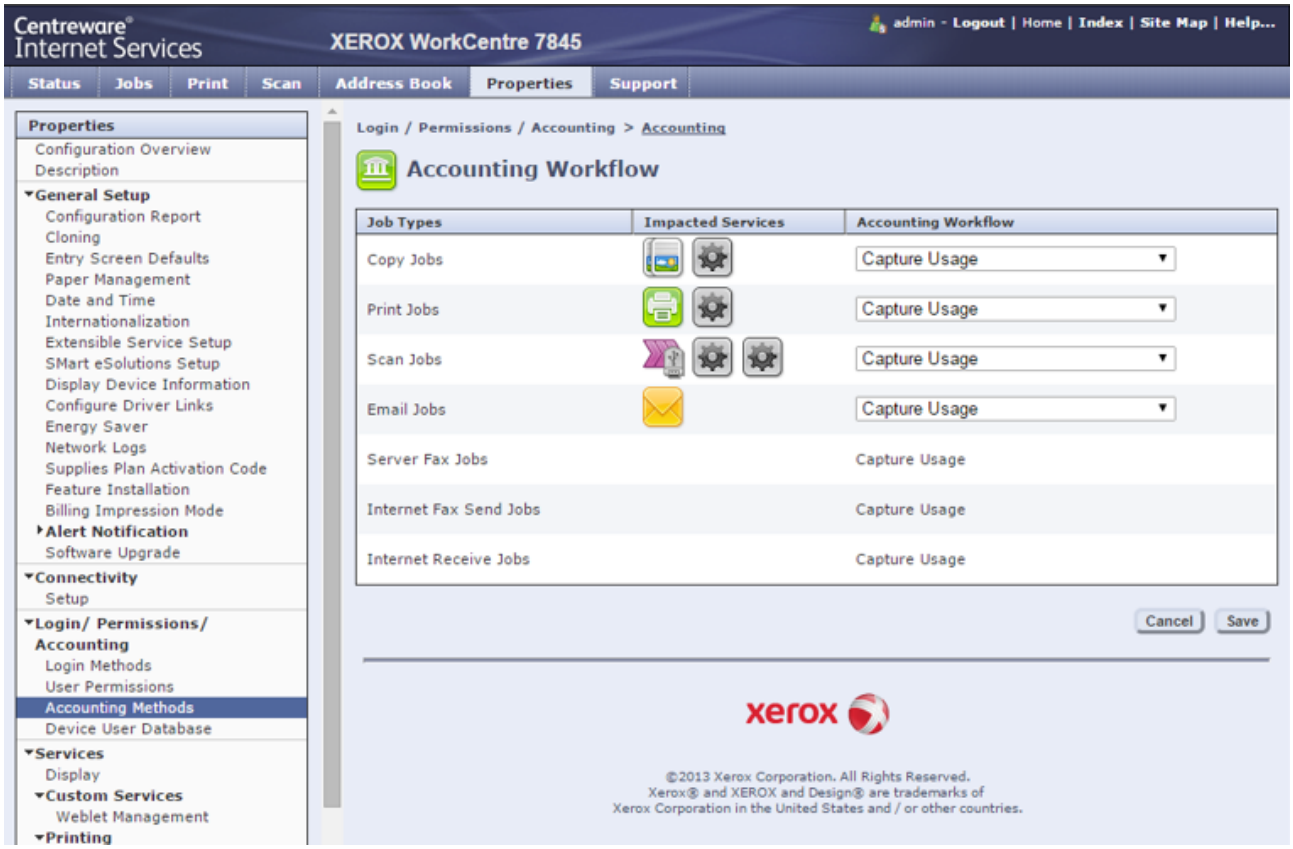
6. On the Manage User Permissions (Non-Logged-in User) page, in the Presets section select the Restrict access to all Services and Tools radio button. Alternatively, select Custom to set individual permissions. Click Apply



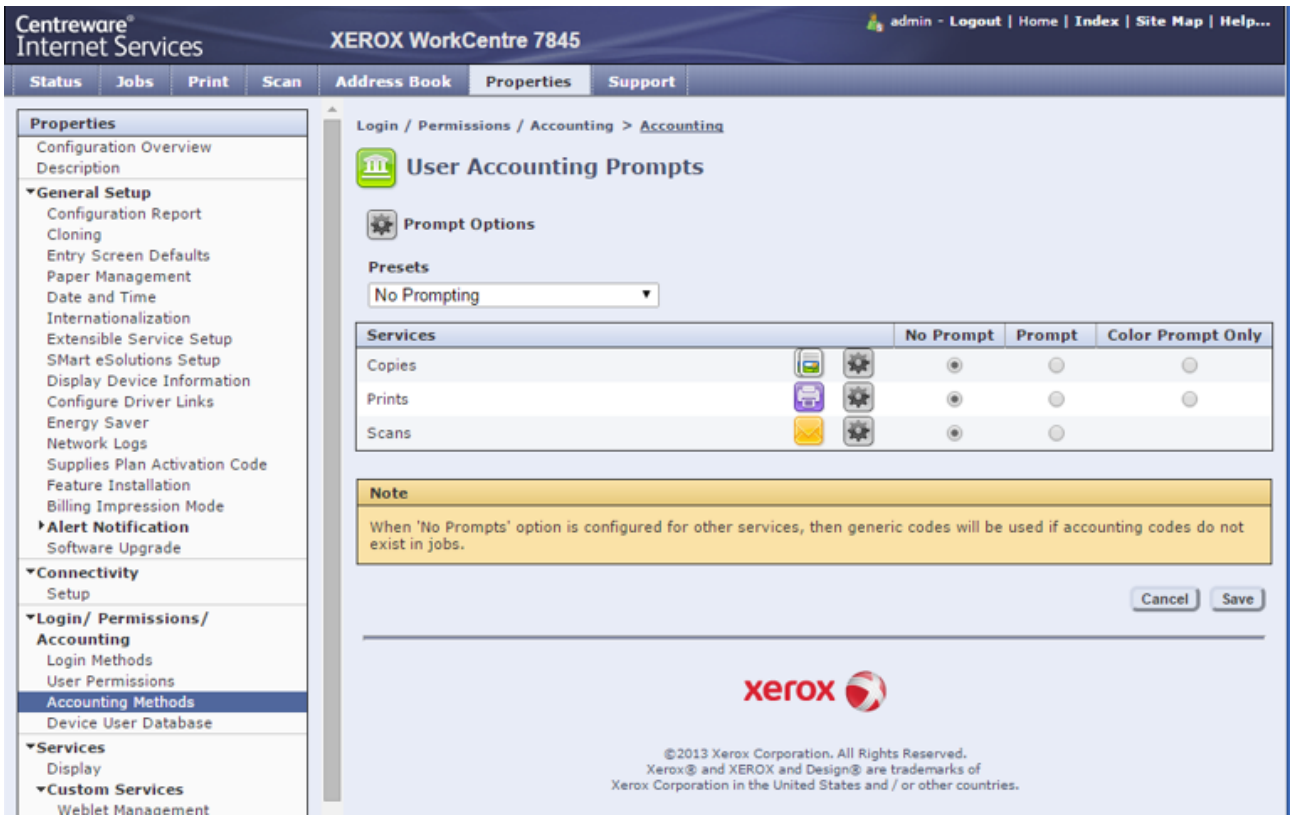
Enable Network accounting

1. Open the printer's web page and select the **Properties** tab.
2. Go to **Login / Permissions / Accounting**, **Accounting Methods**
3. Select **Network Accounting** and **Save**

4. From Accounting Workflow press Edit and make sure all options are set to Capture Usage

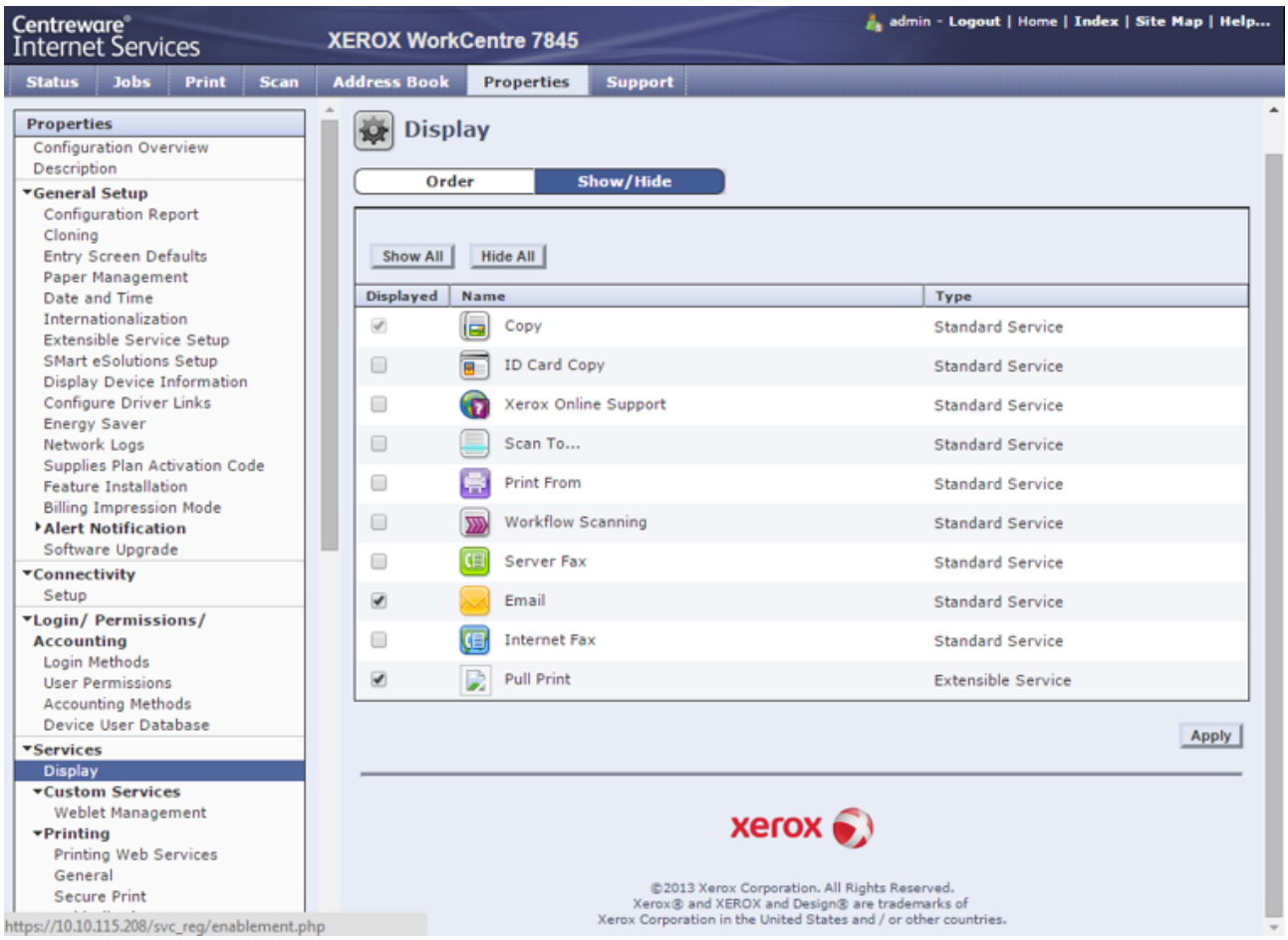


5. From User Accounting Prompts select the radio button No Prompt for all options and press Save



Display – Service

1. Open the printer's web page and select the **Properties** tab.
2. Go to **Services**, **Display**
3. Select **Copy**, **Email** and **Pull Print**



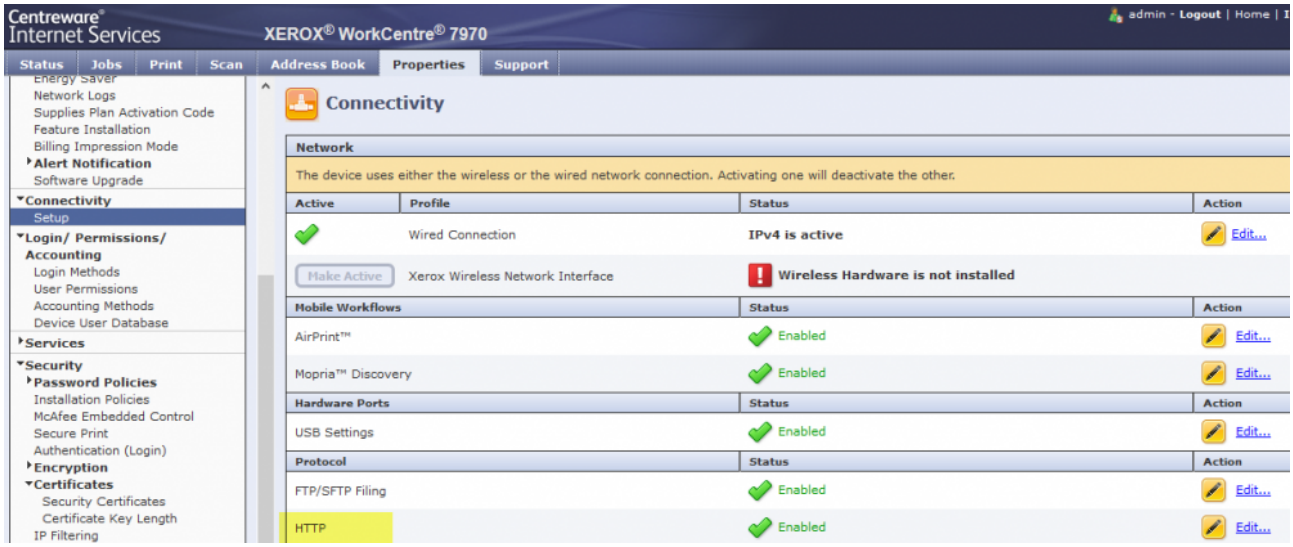
Xerox WorkCentre 79xx

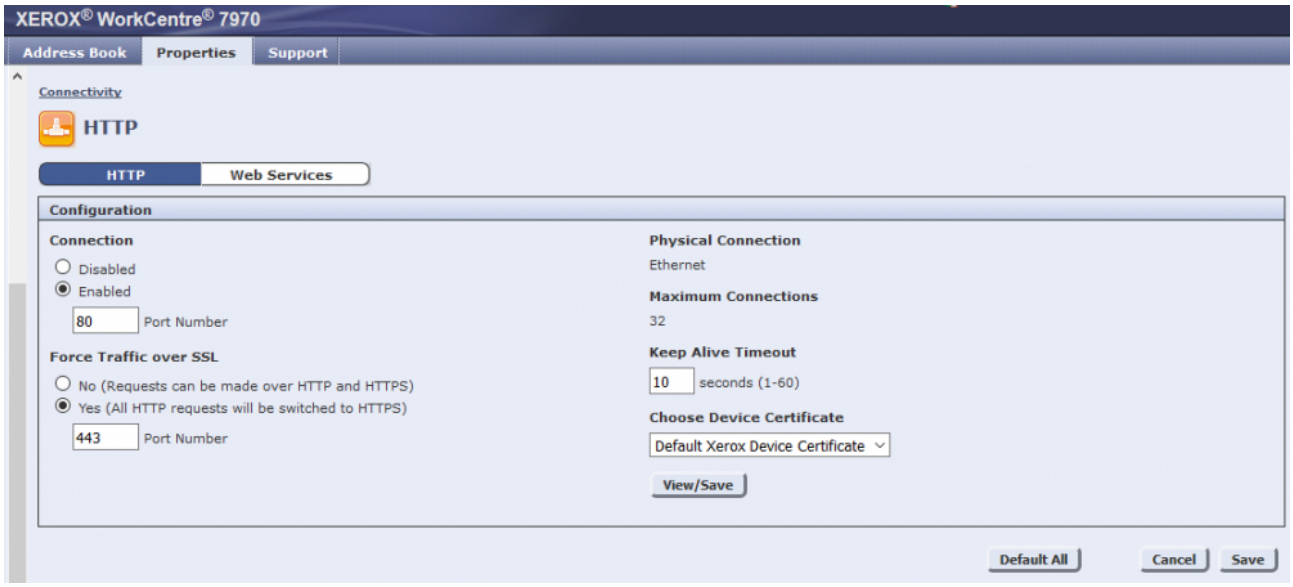
Create a certificate

On the Connect key it is not needed, please use the device certificate.

Enable HTTPS on the printer

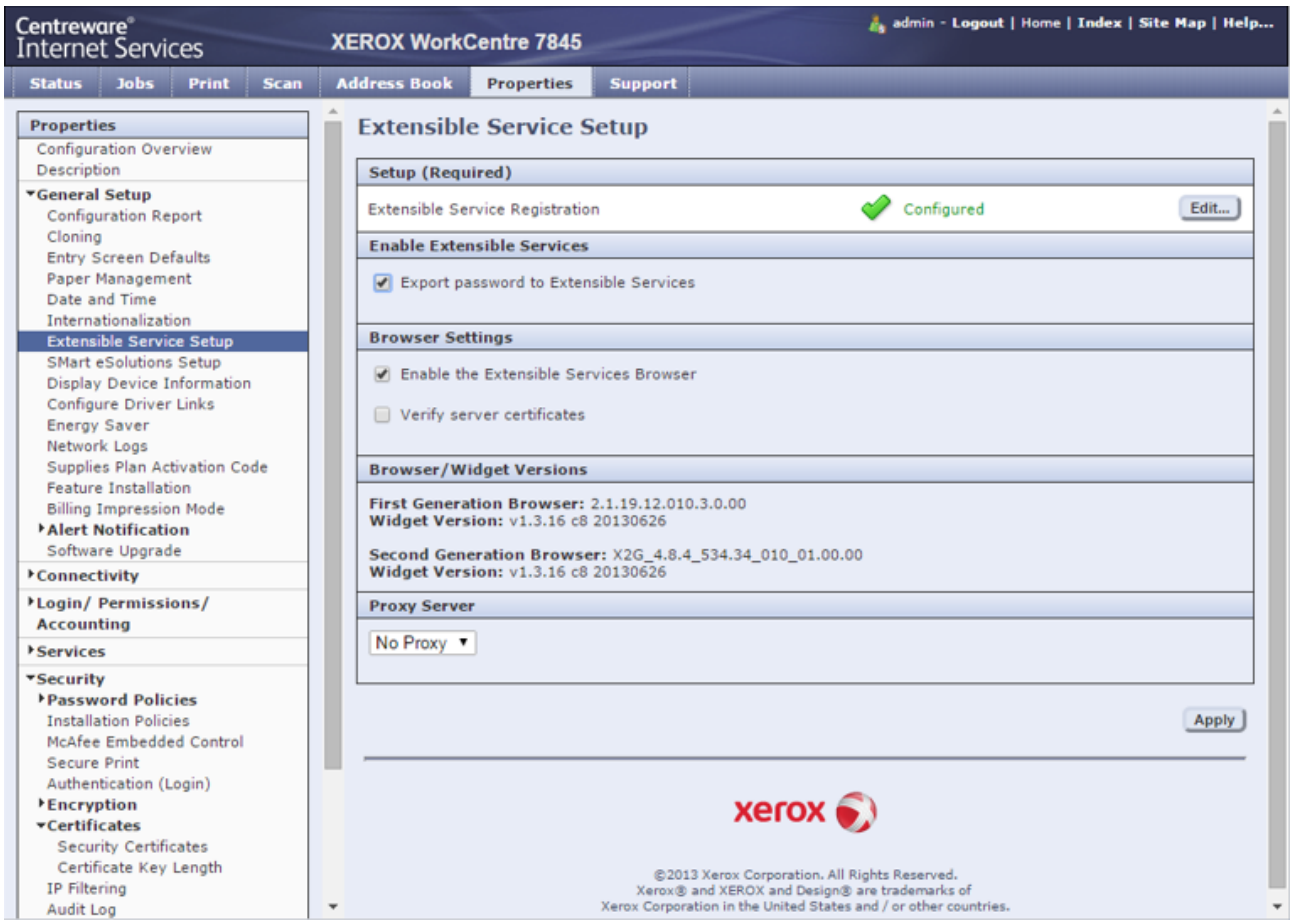
1. Open the printer's web page and select the **Properties** tab.
2. Click **Connectivity**, **Setup**.
3. On the **Connectivity** page click **Edit** next to **HTTP**.
4. In **Force Traffic over SSL** select **Yes** (All HTTP requests will be switched to HTTPS) radio button and set Port Number to **443**. **Save** and **OK** to restart the device's web server.
5. Reboot MFD.

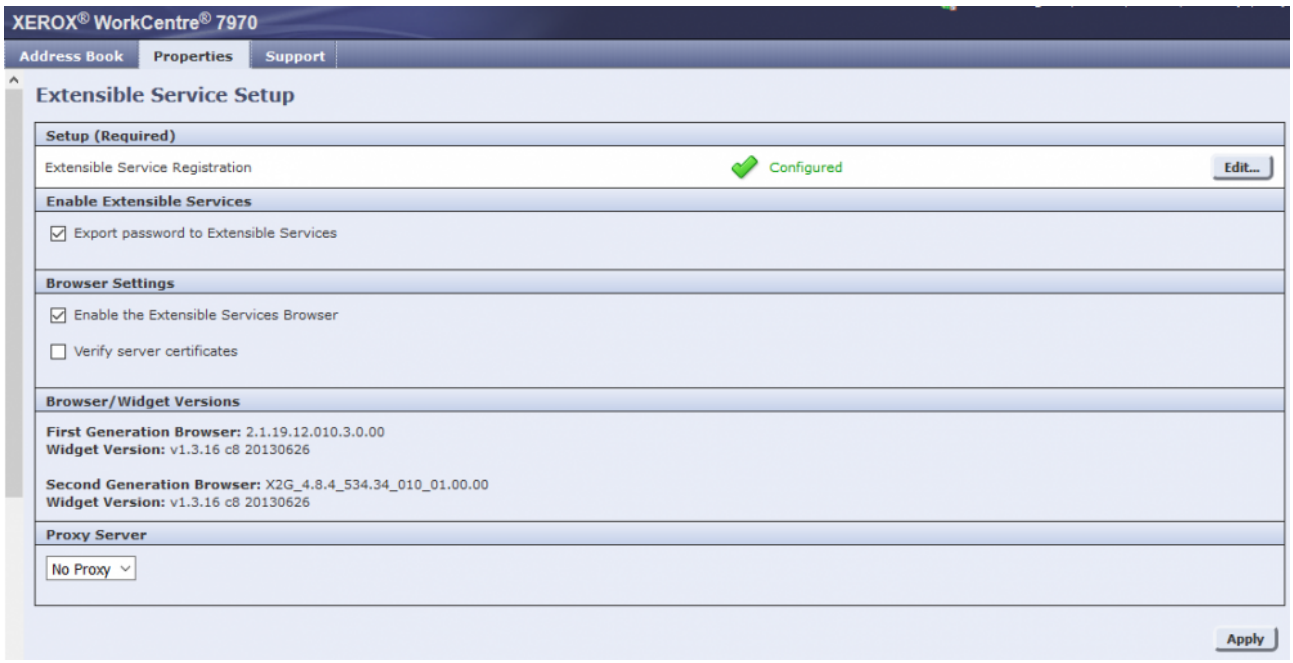




Enable Extensible Service Registration on the printer

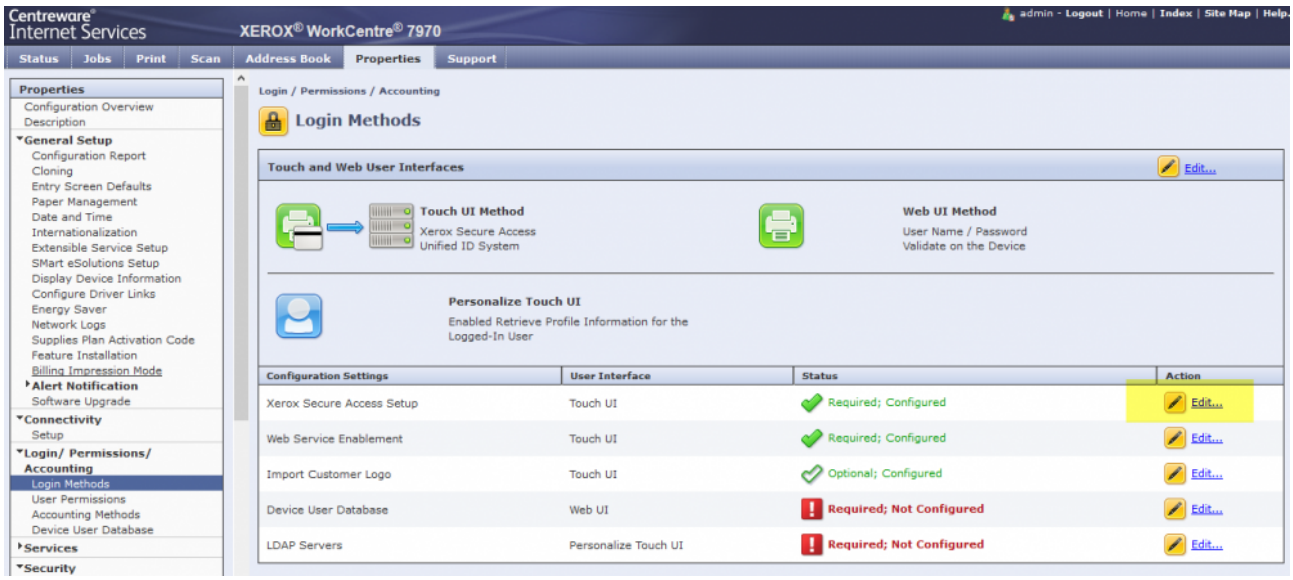
1. Open the printer's web page and select the **Properties** tab.
2. Click **Connectivity**, **Setup**.
3. On the **Connectivity** page, click **Edit** next to **HTTP**.
4. Click **Web Services** at the top of the page.
5. Select **Enable** next to **Extensible Service Registration**. Click **Apply** and **OK**.



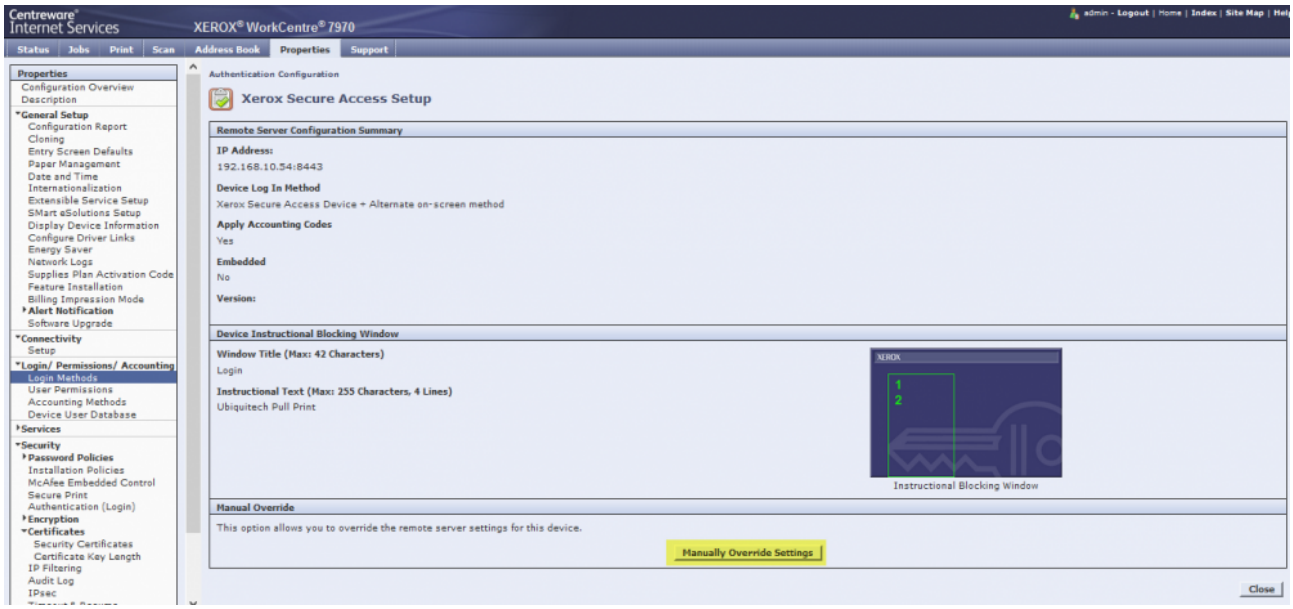


Configure authentication and access control on the printer

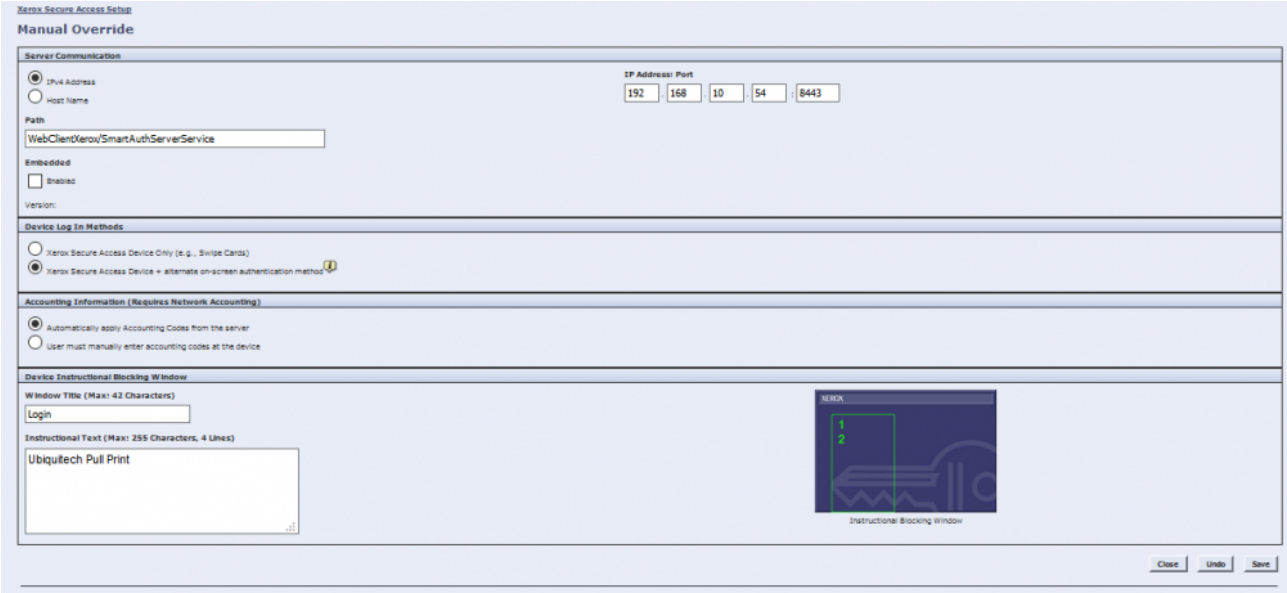
1. Open the printer's web page and select the **Properties** tab.
2. Expand **Login/ Permissions/ Accounting** and click **Login Methods**.



3. Open **Manual Override** page



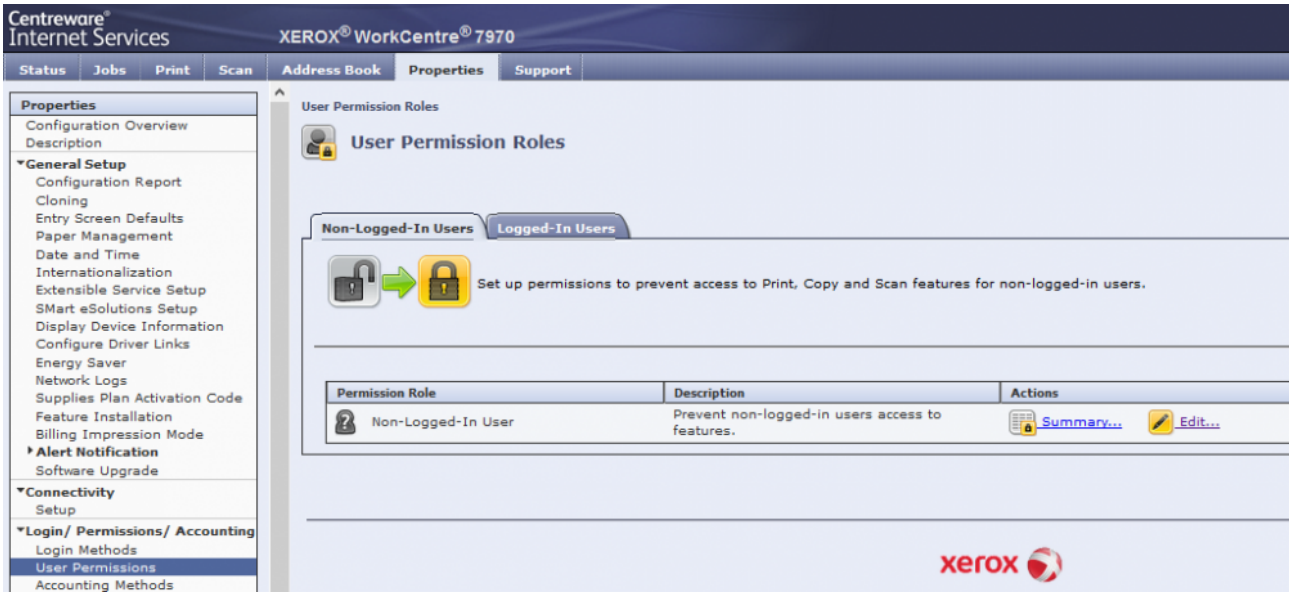
4. In the **Device Log In Methods** section select the **Xerox Secure Access Device + alternate on-screen** authentication method button.



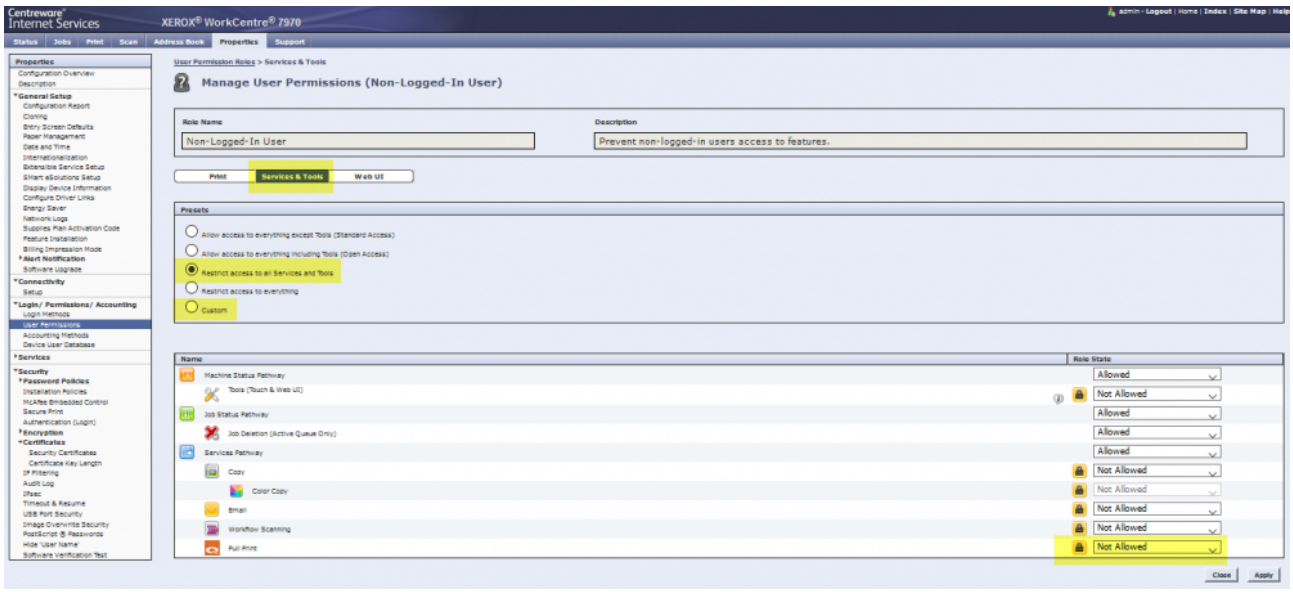
5. Click **Save**.

User Permissions

1. In the **Properties** menu to the left click **User Permissions**.

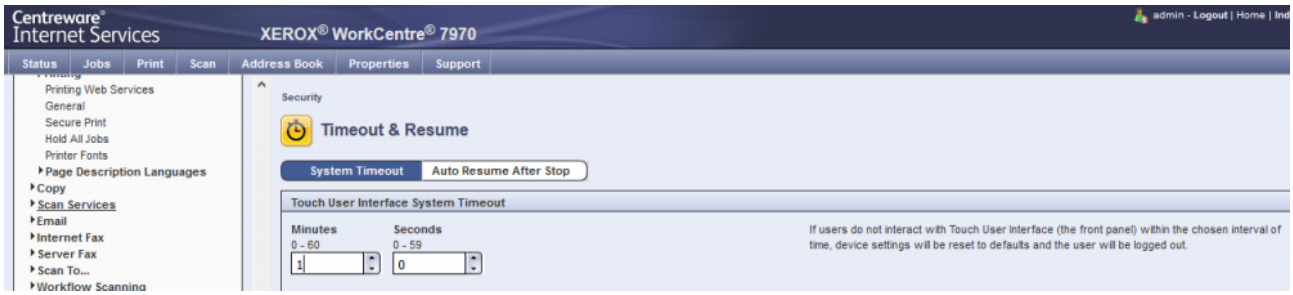


2. On the **User Permissions Role, Non-Logged-in User** page, in the **Presets** section select the **Restrict access to all Services and Tools** radio button. Alternatively, select **Custom** to set individual permissions. Click **Apply**.



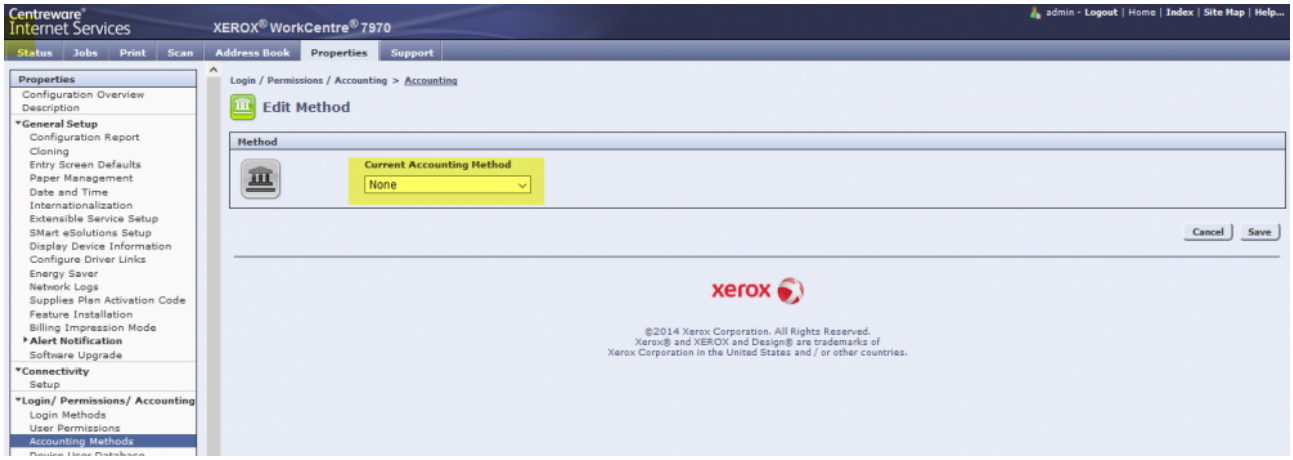
Device Timeout

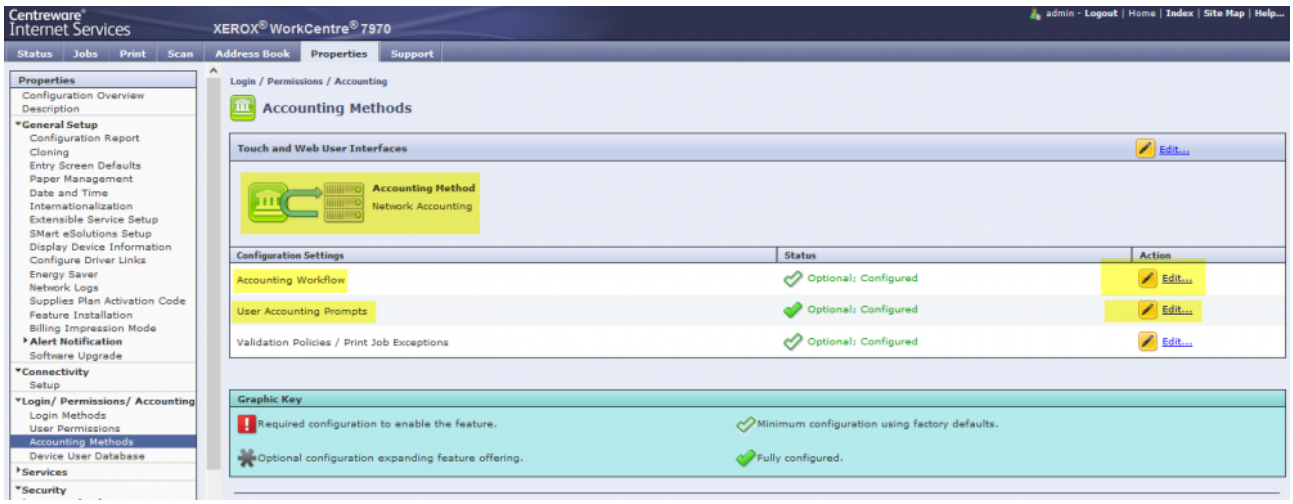
Under **Security**, **Timeout & Resume**, the device timeout can be set.



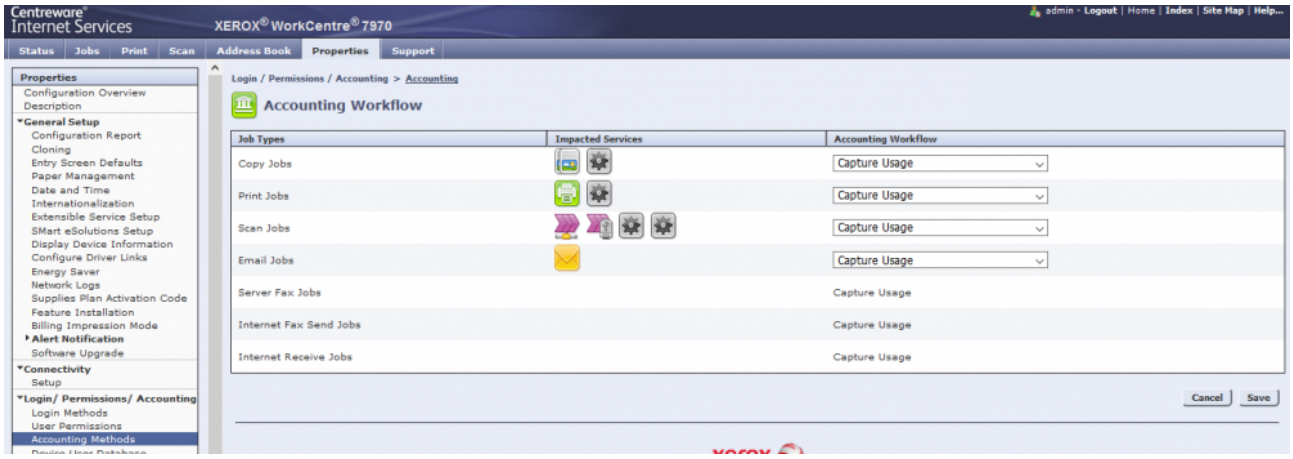
Enable Network accounting

1. Open the printer's web page and select the **Properties** tab.
2. Go to **Login / Permissions / Accounting**, **Accounting Methods**.
3. Select **Network Accounting**.

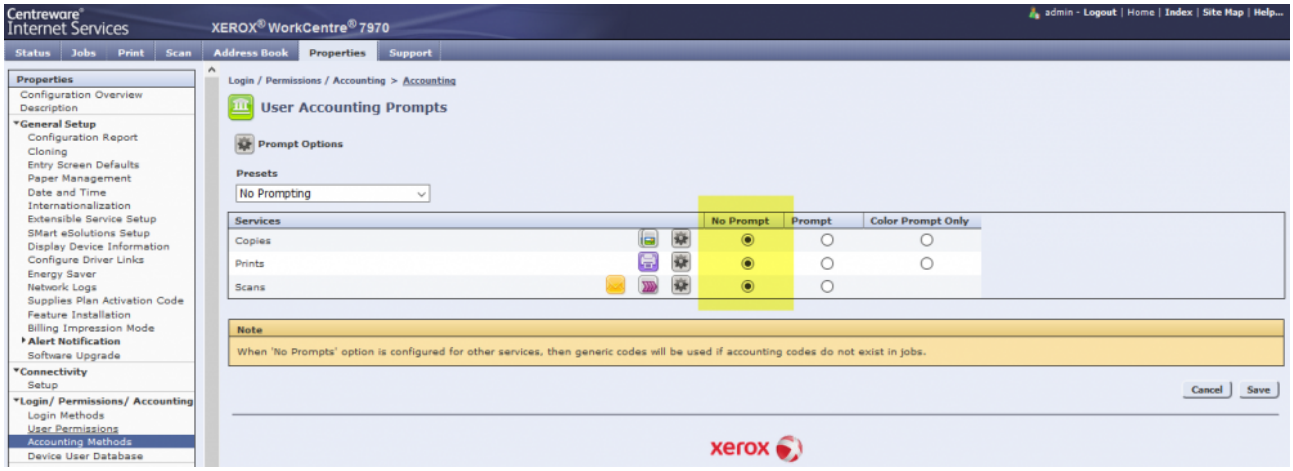




4. From **Accounting workflow** press **Edit** and make sure all options are set to **Capture Usage**.

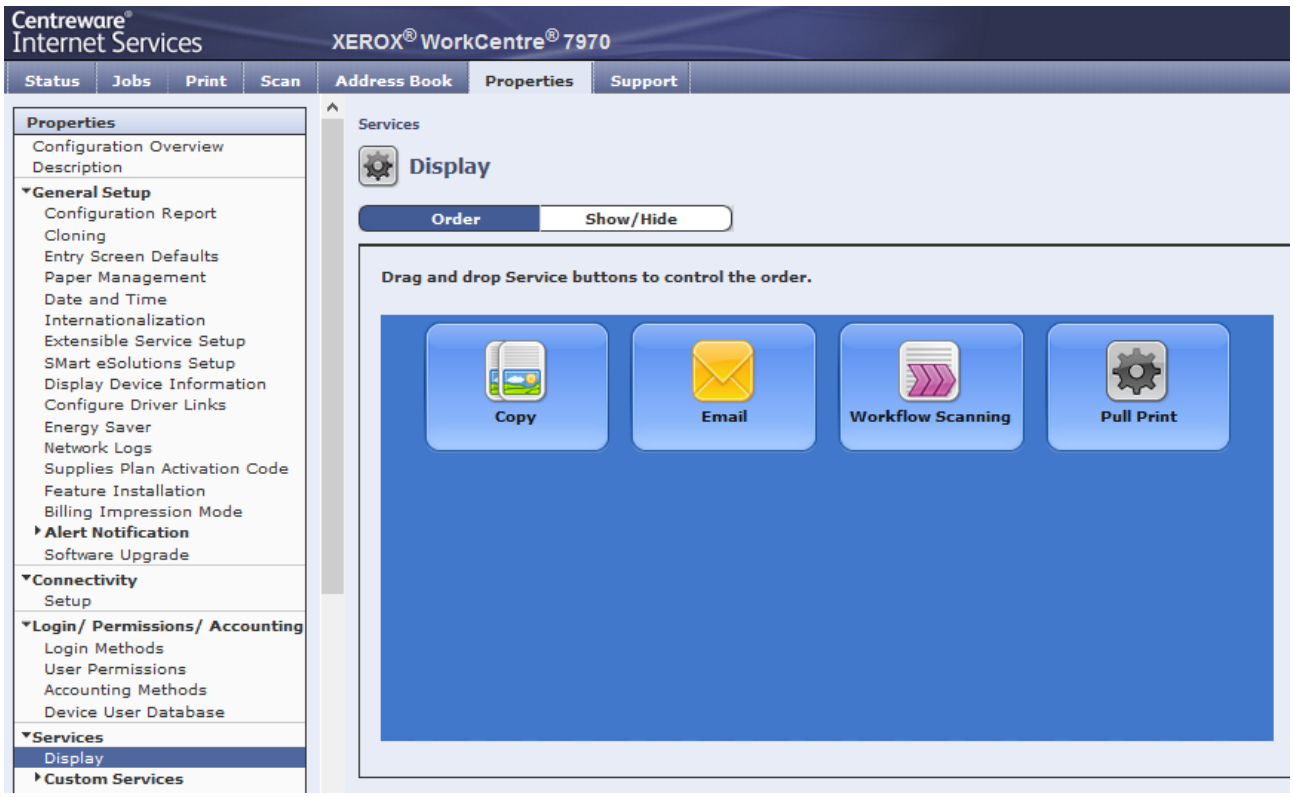


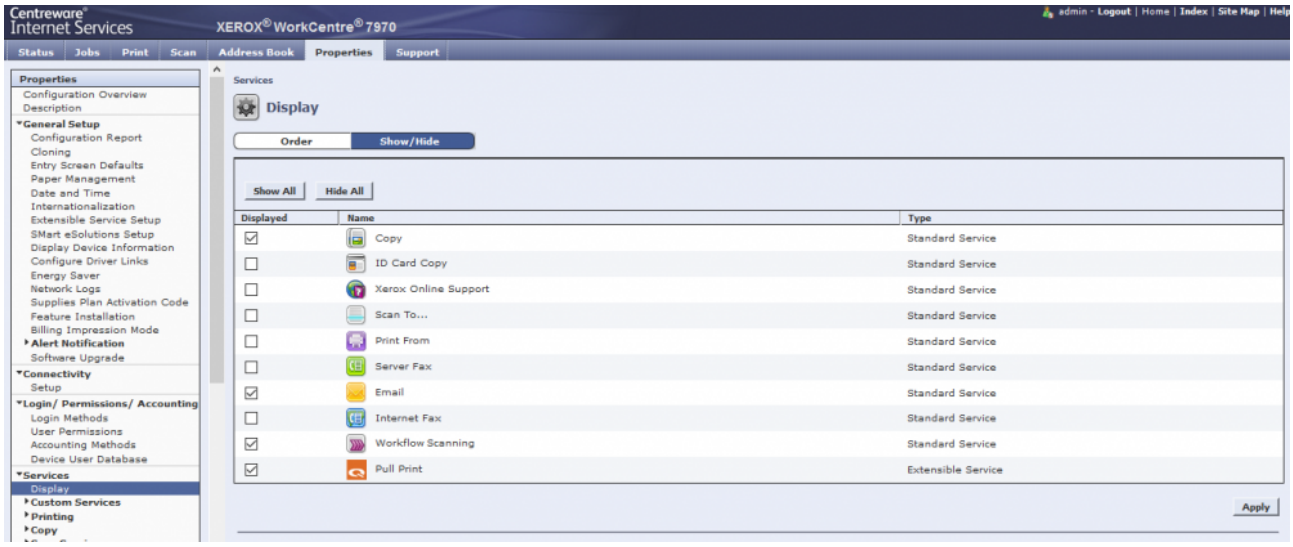
5. From **User Accounting Prompts** select the radio button **No Prompt** for all options and press **Save**



Display – Service

1. Open the printer's web page and select the **Properties** tab.
2. Go to **Services**, **Display**.
3. Select **Copy**, **Email** and **Pull Print**.

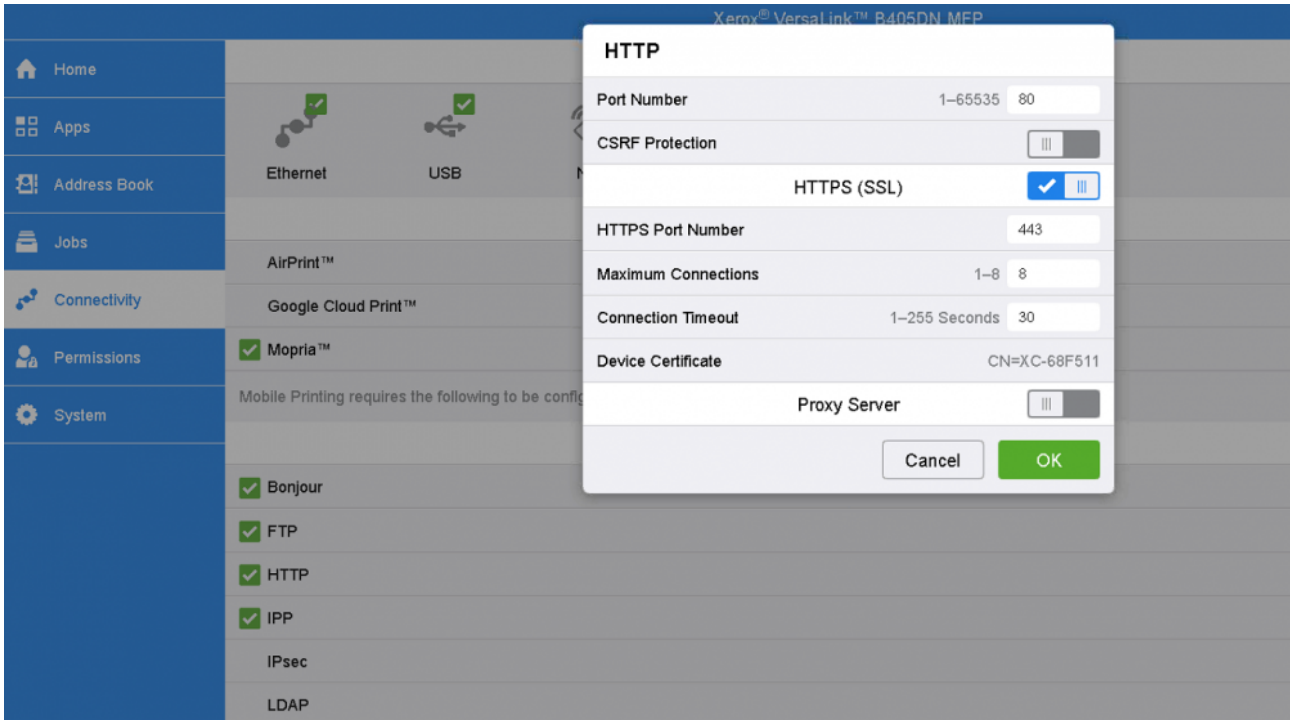




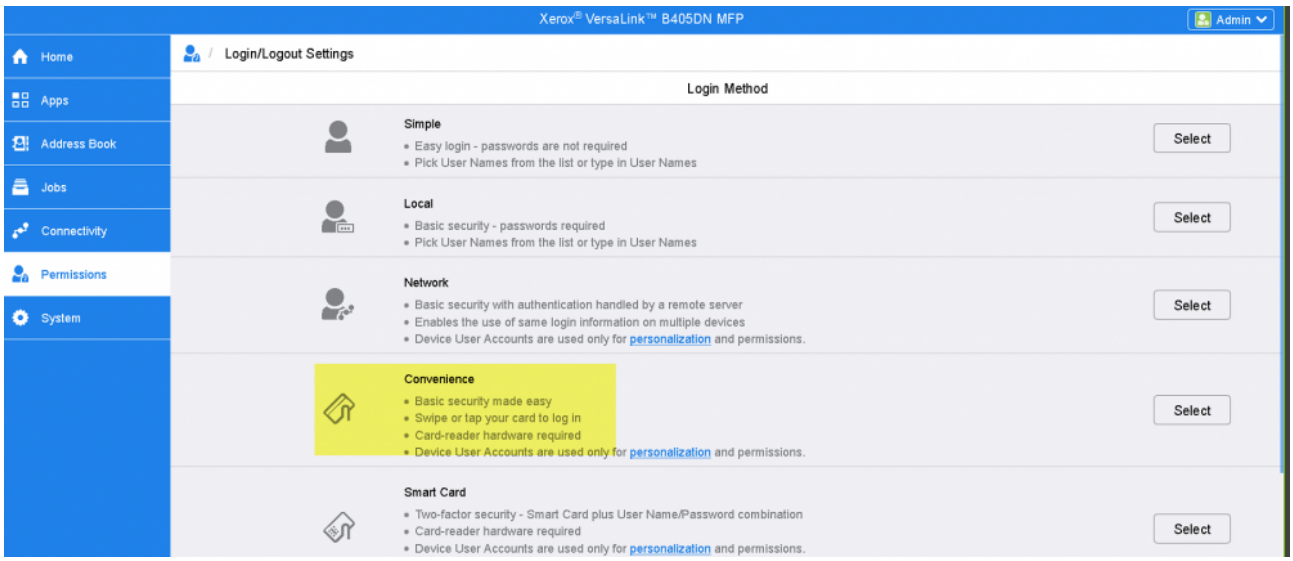
Xerox Versalink

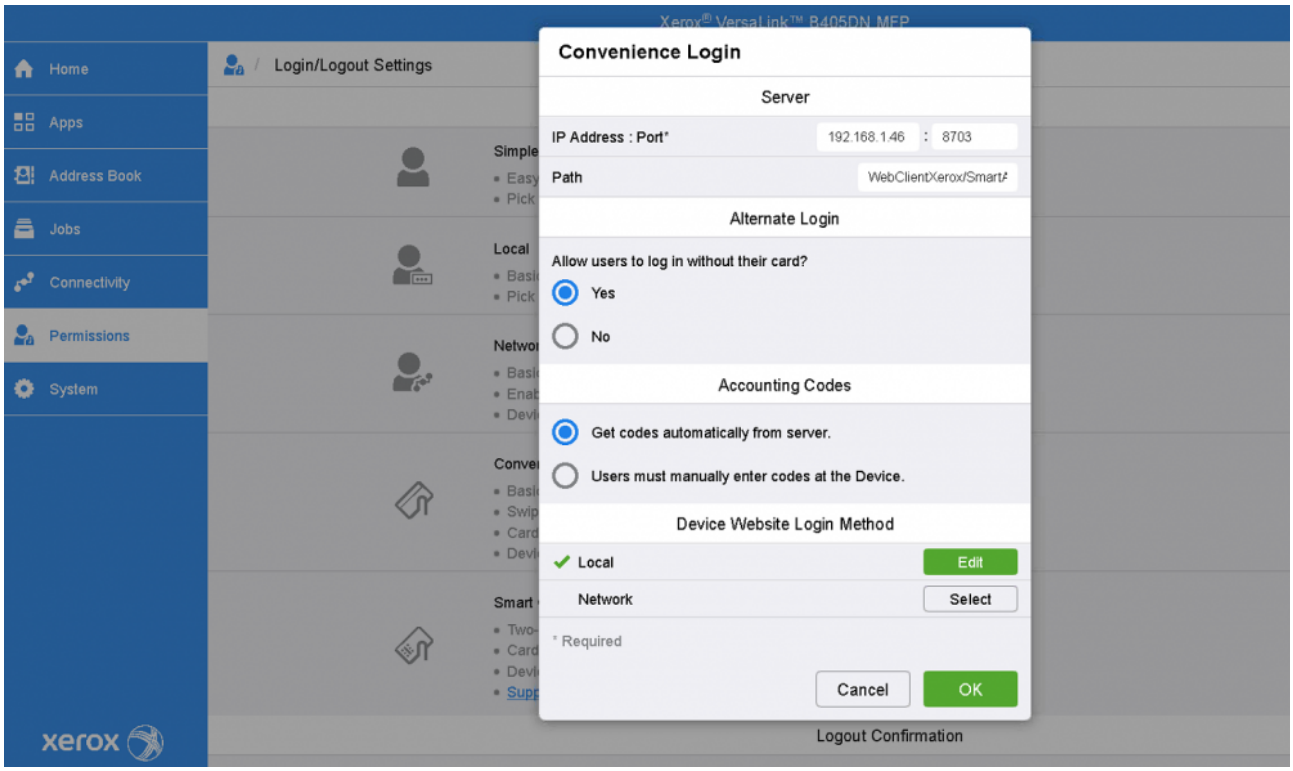
*Login at the device as admin

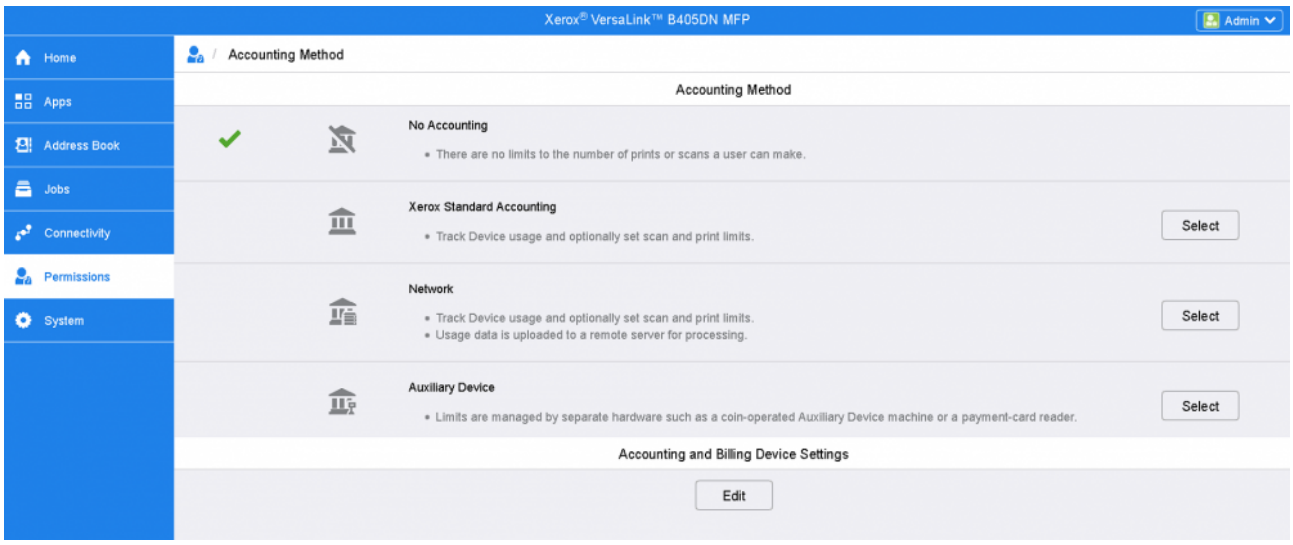
Go to **Connectivity** and setup **SSL** with settings as below picture.



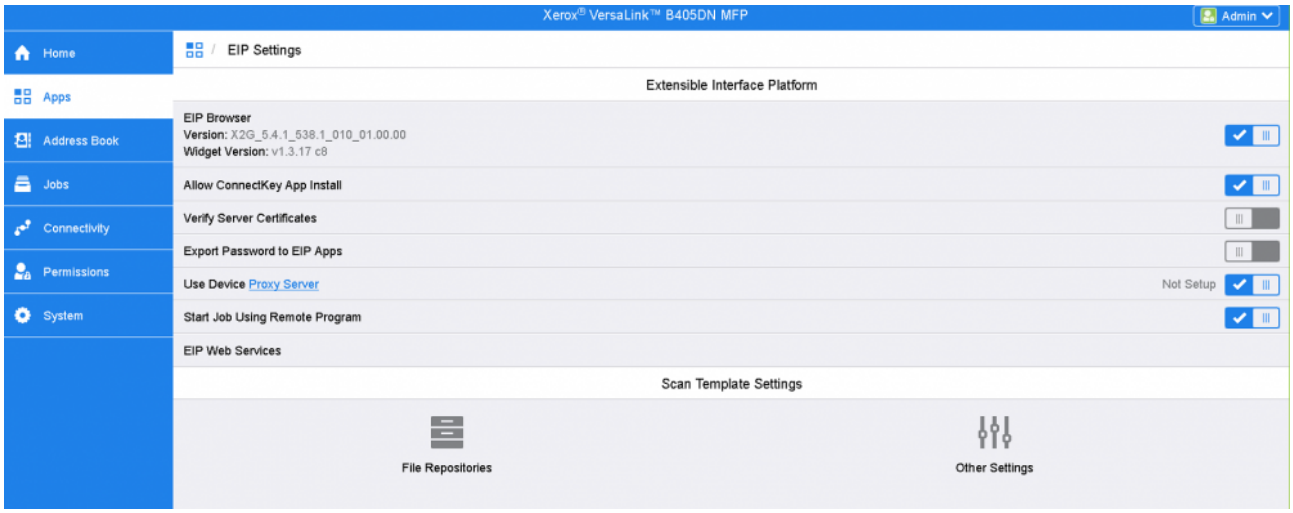
Go to **Permissions**, **Convenience** and setup device as described in the next few pictures.

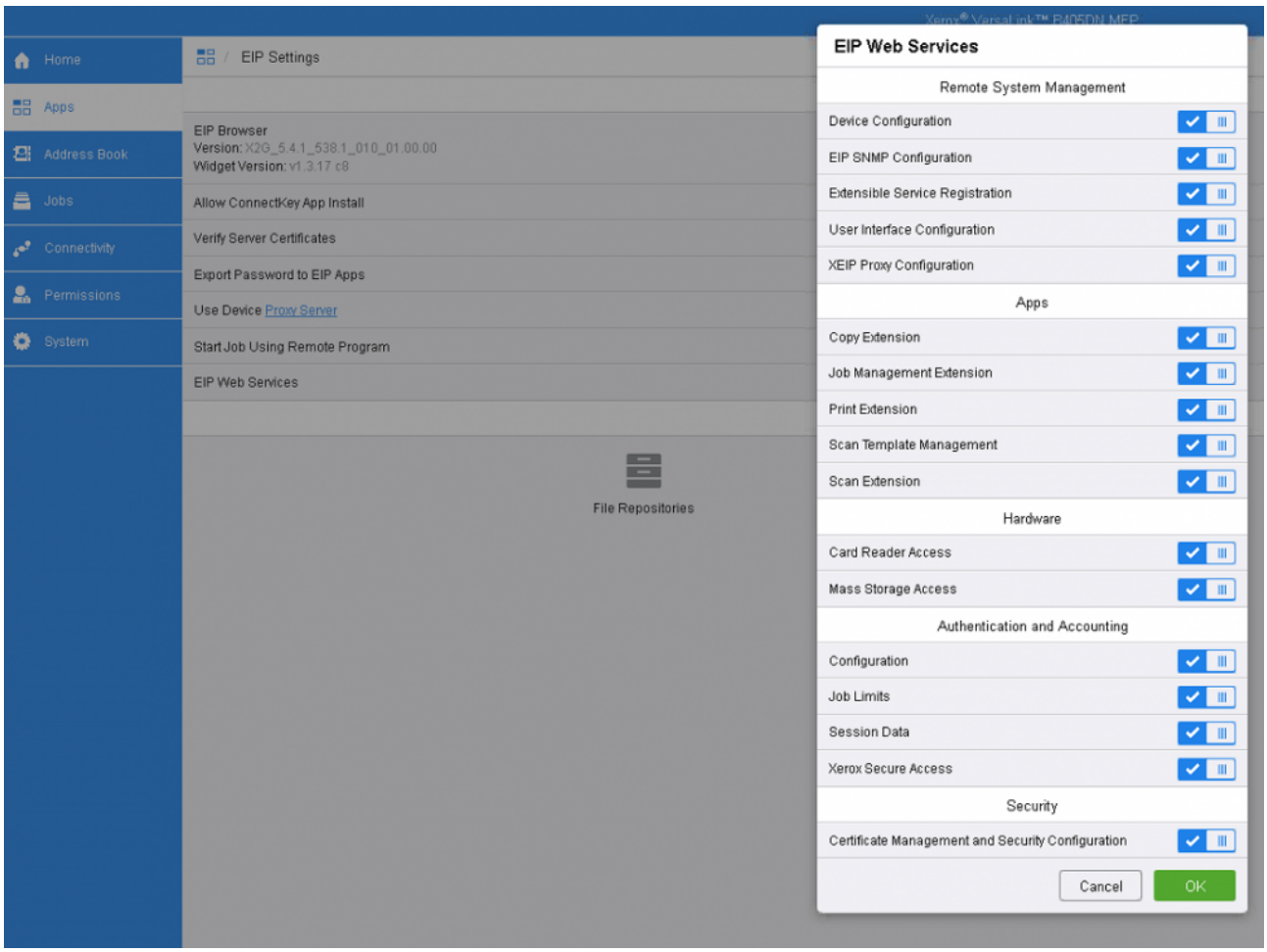

Xerox® VersaLink™ B405DN MFP
Admin
Home
Apps
Address Book
Jobs
Connectivity
Permissions
System
Login/Logout Settings
Login Method
Simple
• Easy login - passwords are not required
• Pick User Names from the list or type in User Names
Select
Local
• Basic security - passwords required
• Pick User Names from the list or type in User Names
Select
Network
• Basic security with authentication handled by a remote server
• Enables the use of same login information on multiple devices
• Device User Accounts are used only for personalization and permissions.
Select
Convenience
• Basic security made easy
• Swipe or tap your card to log in
• Card-reader hardware required
• Device User Accounts are used only for personalization and permissions.
Select
Smart Card
• Two-factor security - Smart Card plus User Name/Password combination
• Card-reader hardware required
• Device User Accounts are used only for personalization and permissions.
Select


Xerox® VersaLink™ B405DN MFP
Home
Apps
Address Book
Jobs
Connectivity
Permissions
System
Login/Logout Settings
Convenience Login
Server
IP Address : Port*
192.168.1.46
8703
Path
WebClientXerox/SmartA
Alternate Login
Allow users to log in without their card?
Yes
No
Accounting Codes
Get codes automatically from server.
Users must manually enter codes at the Device.
Device Website Login Method
Local
Edit
Network
Select
* Required
Cancel
OK
Logout Confirmation
xerox

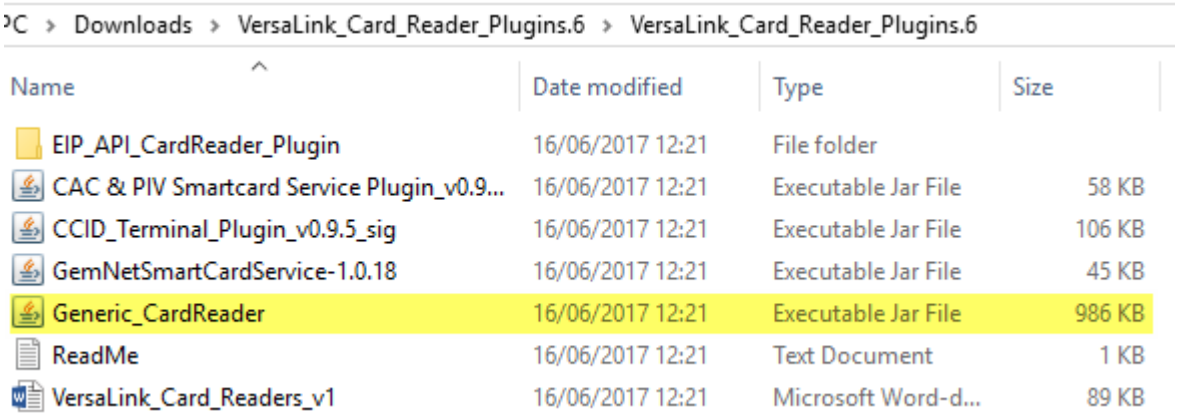


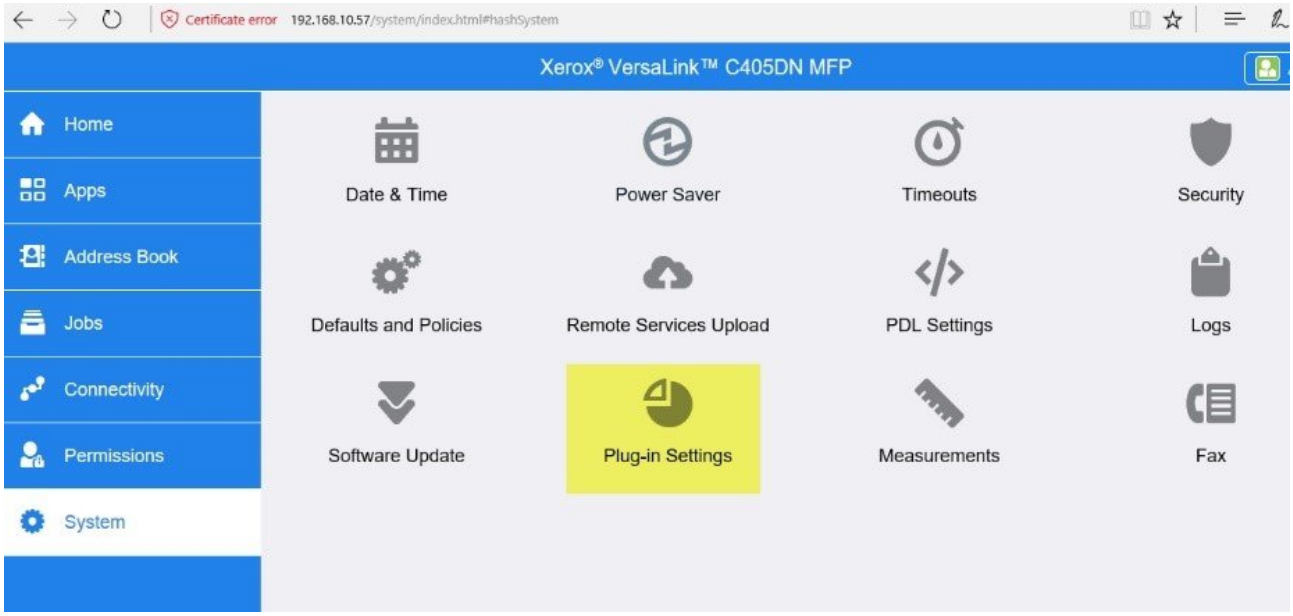
Under **Apps**, setup the **EIP settings**



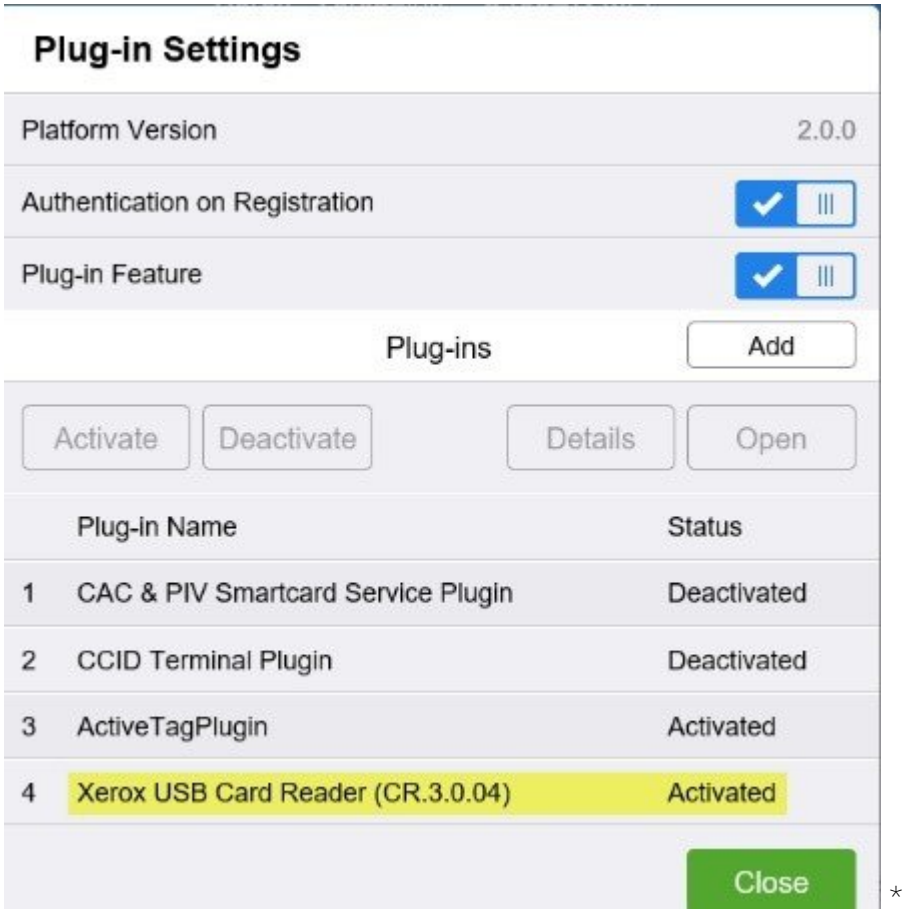


To setup a card reader on the Xerox Versalink, it is necessary to download and install the Versalink card reader plugin, to be downloaded from Xerox web





Select Xerox USB Card reader



*

Using Xerox Remote Logger tool

The Xerox Remote Logger tool can be found bundled as part of Terminal Deployment Tool in the `< your deployment tool location>\ tools` folder. Its primary purpose is to supplement

missing device logs on Xerox devices in cases where debugging is needed to determine the root cause.

Gathering logs

Direct network visibility must exist between the computer running the Xerox Remote Logger tool and the device on which Xerox Gen 2 Cloud Terminal is running. Port 5079 is used for communication.

1. Set up Remote Logger Tool

> ⚠ Depending on your OS and settings, you might need to adjust the binary's execution rights using the `chmod +x` command.

Run the remote-logger-tool binary (e.g., by running `./xerox-remote-logger-osx`). If the tool starts correctly, you will see the list of IP addresses on which it can accept incoming communication:

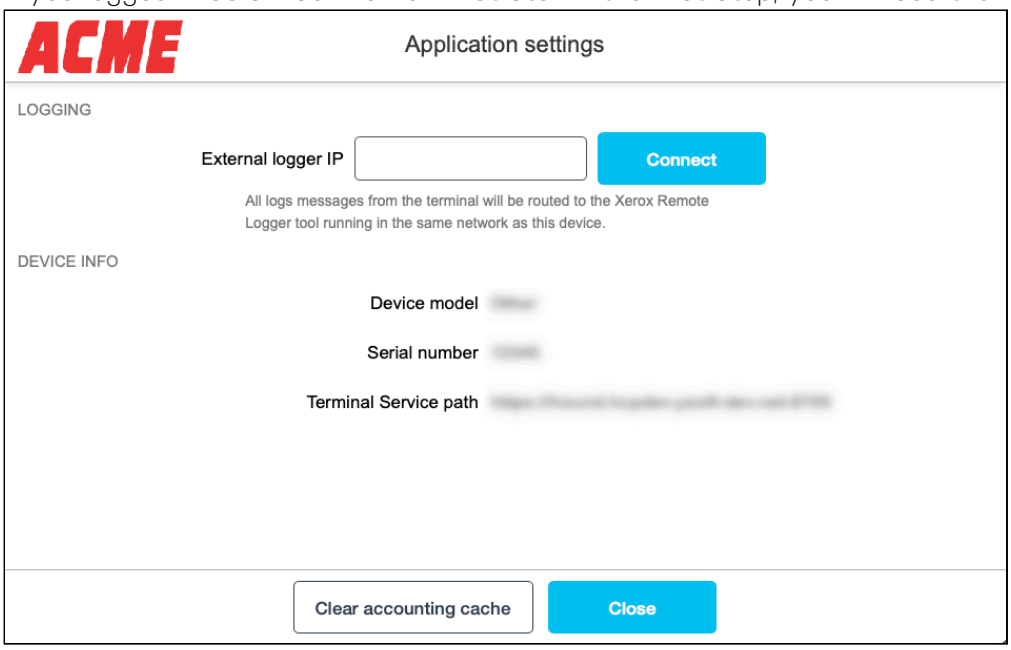
For further steps, use the IP address visible from the MFD.

2. Set up the device running Cloud Terminal

> ⚠ The following settings are persisted, meaning that once set, they will remain set even after restarting the device, etc. As there is a slight performance impact on the terminal, disable the remote logging once finished.

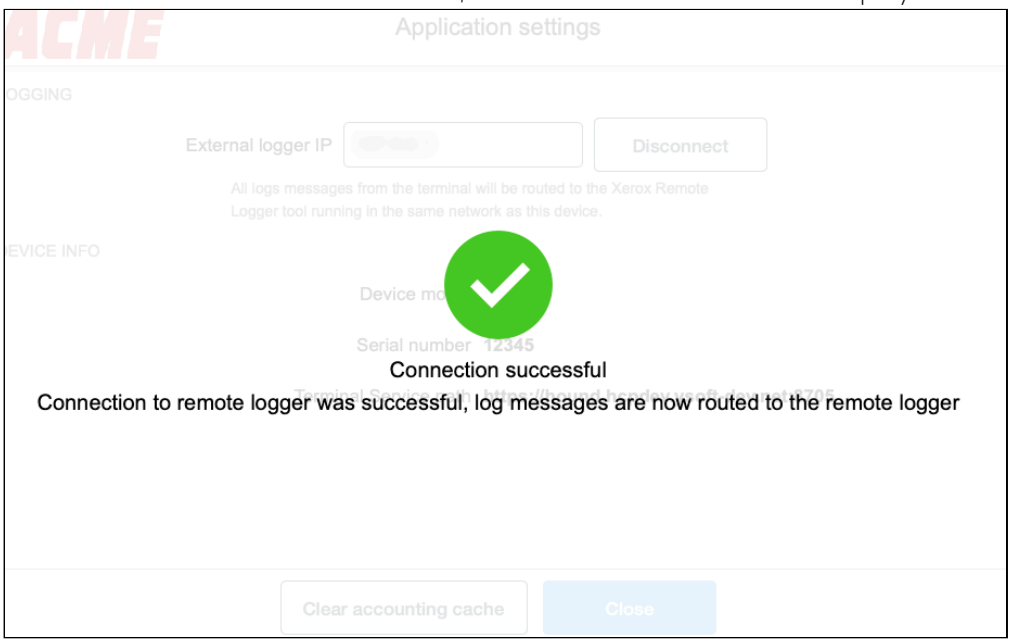
1. On the MFD, use the native login menu to log in as a Machine Administrator, and press **Reset All Apps**.
2. Open Cloud Terminal.
3. Hold your finger on the logo in the upper left corner of the screen for about 5 seconds.

4. If you logged in as a Machine Administrator in the first step, you will see the following screen:



5. Fill in the IP address on which your Xerox Remote Logger tool is running and press **Connect**.

6. After the connection is established, the confirmation screen is displayed:



3. Gather logs

All logs should now be routed to your Xerox Remote Logger instance. You will be able to see the log messages as they come.

All logs are also stored in the `< your deployment tool location>\ tools\machine-log.log` file. Share this output with our support when raising an incident.

Canon Terminal

Limitations

Canon Terminal can be installed only on MFDs in Europe. Other regions are not approved by Canon yet.

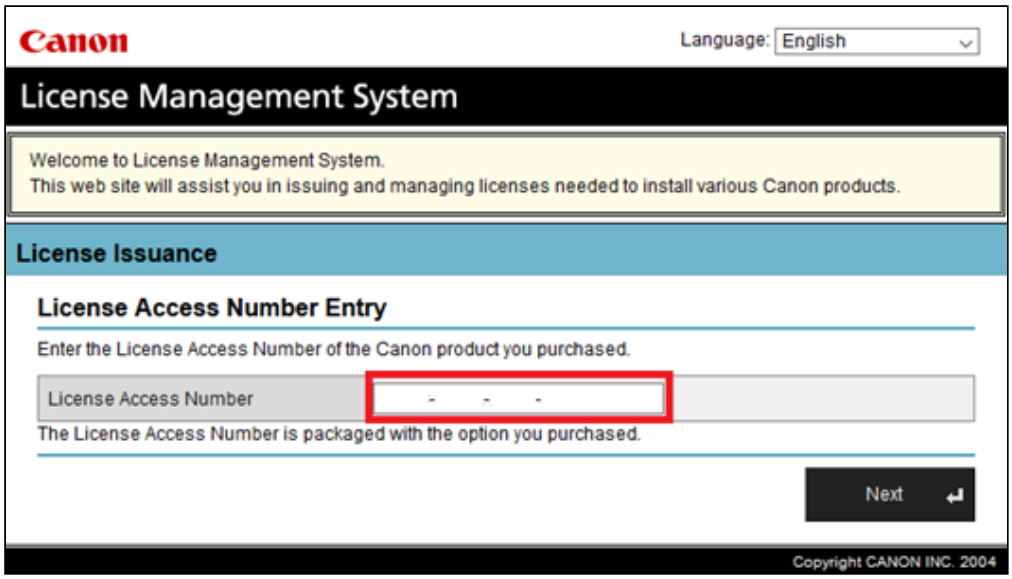
Prerequisites

- A custom login application will be installed on the MFD. This requires obtaining the necessary files from the SAFEQ Cloud folder: */opt/safeqcloud/conf/canon*
  Required files are:
  - a Java package file (YSoft SAFEQ Embedded Terminal_1.6.0.jar)
  - an accompanying text file (A1_YSoftSAFEQEmbe_160_20230905085252_0001.txt). The text file contains a License Access Number that will be used to generate the license file (.lic).
- The "Web Access" browser/software must be installed on the Canon MFD.
  When this web browser is installed on the MFD, it can be verified on the printer homepage (RUI) under Status Monitor/Cancel: Device Features – Other.
- You have configured your secondary gateway according to Secondary Gateway mapping.

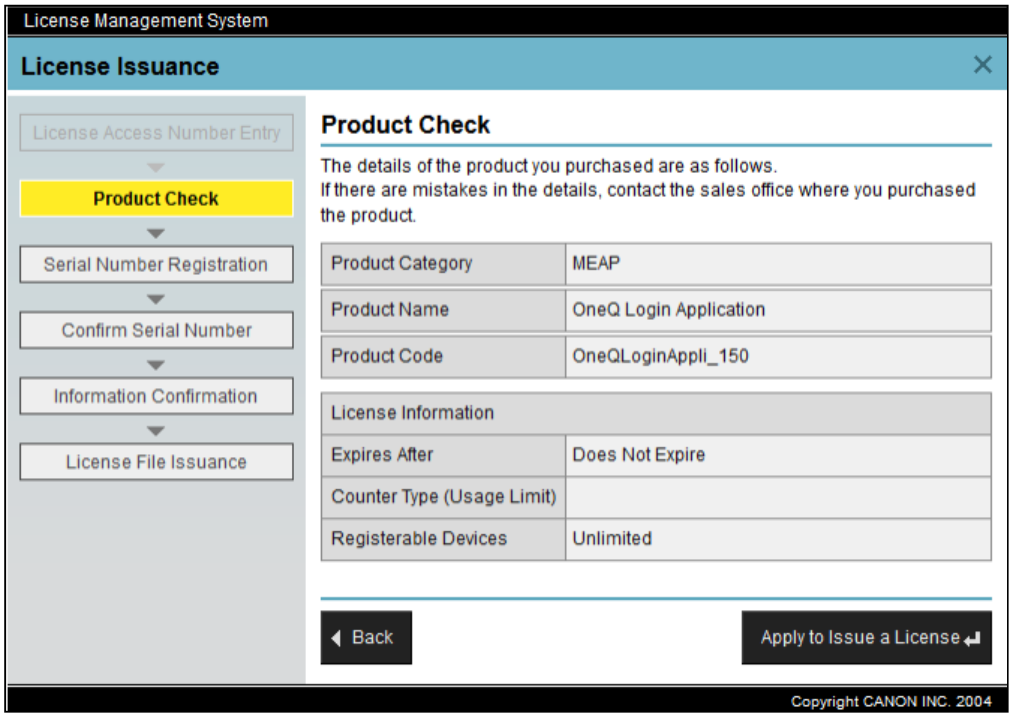
License file generation

Beforehand, it is recommended that you gather the Device Serial Number for all the MFDs you need to install the application on.
To generate the license file, we need to follow the steps and instructions available on the Canon website for the License Management System.

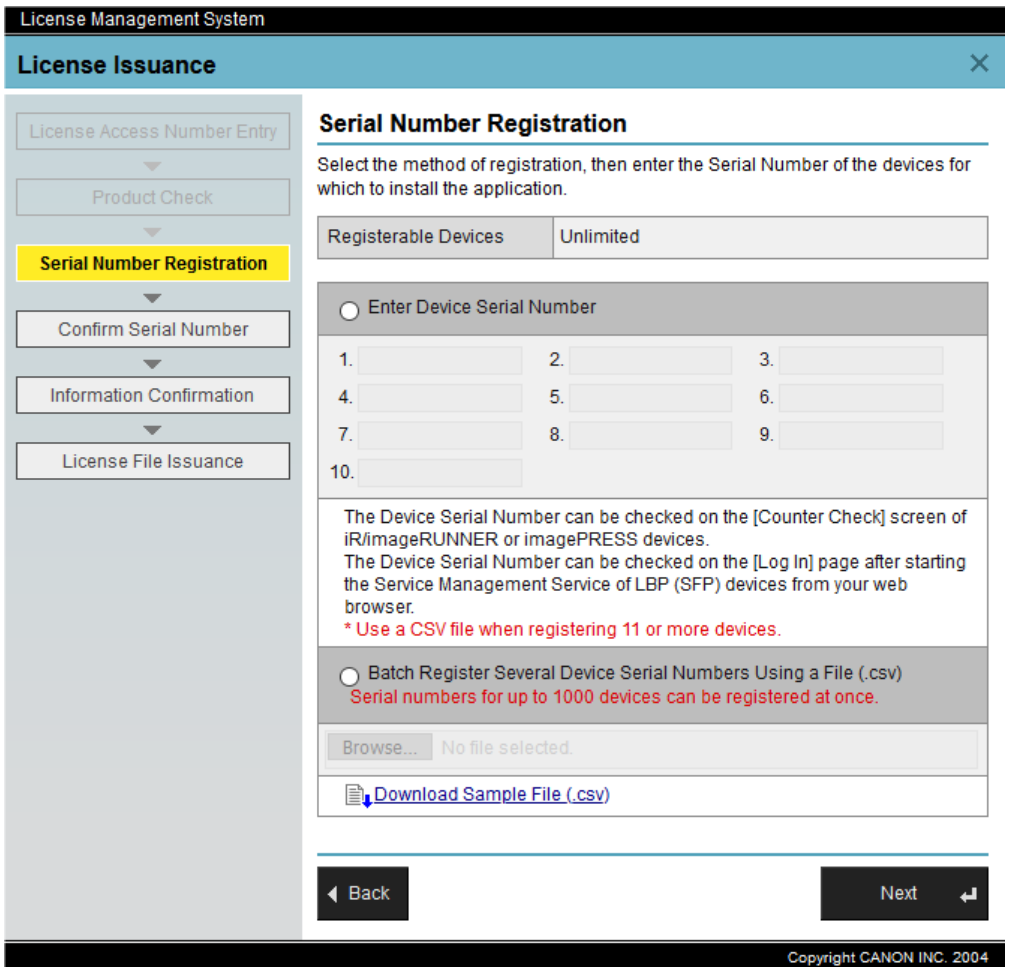
- Open this a web browser and go to this address: https://asd-pub-an18.srv.ygles.com/web/licenses
- Enter the License Access Number provided in the downloaded text file, then press 'Next':



- Review the information on the Product Check page, then press 'Apply to Issue a License':



- On the 'Serial Number Registration' page enter the Device Serial Number(s) for the impacted MFDs:



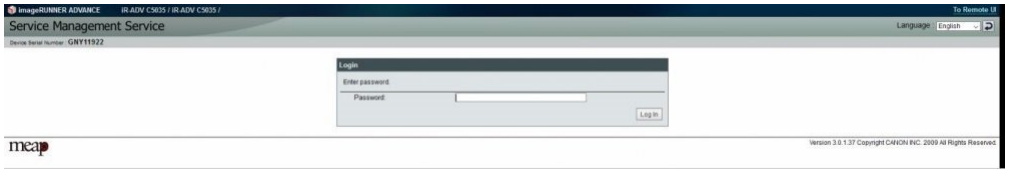
- On the following pages confirm the information provided and retrieve the issued license file.

Install Login application

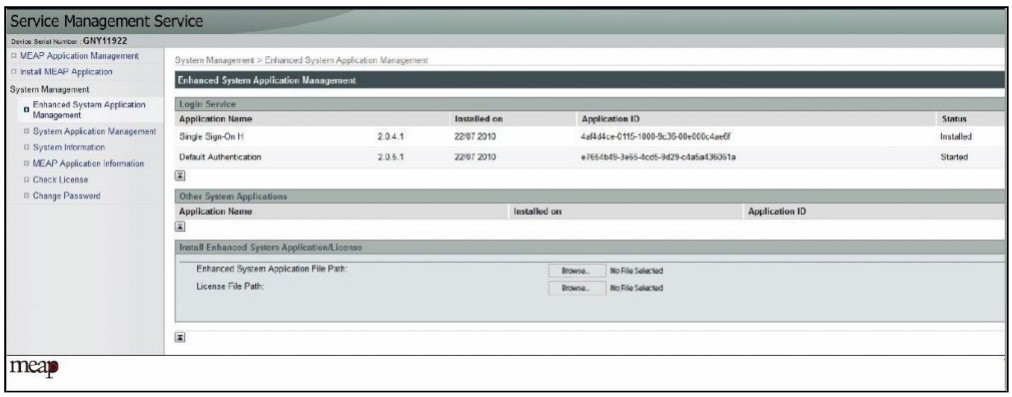
On a Canon device, an embedded login application must be installed in order to make the Browser client work.

To install the Login app, follow these steps:

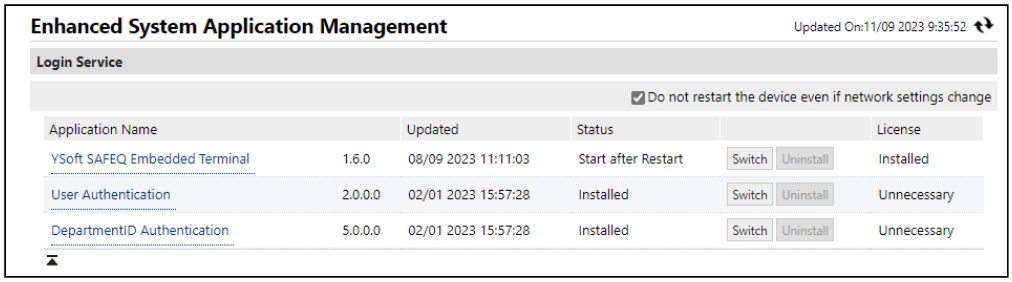
- Open the following page in a web browser and enter the MEAP admin password to login. The default password is '*MeapSmsLogin*'
  http://[PrinterIpAddress]:8000/sms/



- Click on 'Enhanced System Application Management', and then inside the 'Install Enhanced System Application/License' section:
  - For the 'Enhanced System Application File Path' select 'Browse...' and point to the downloaded .jar file
  - For the 'License File Path' select 'Browse...' and point to the downloaded .lic file



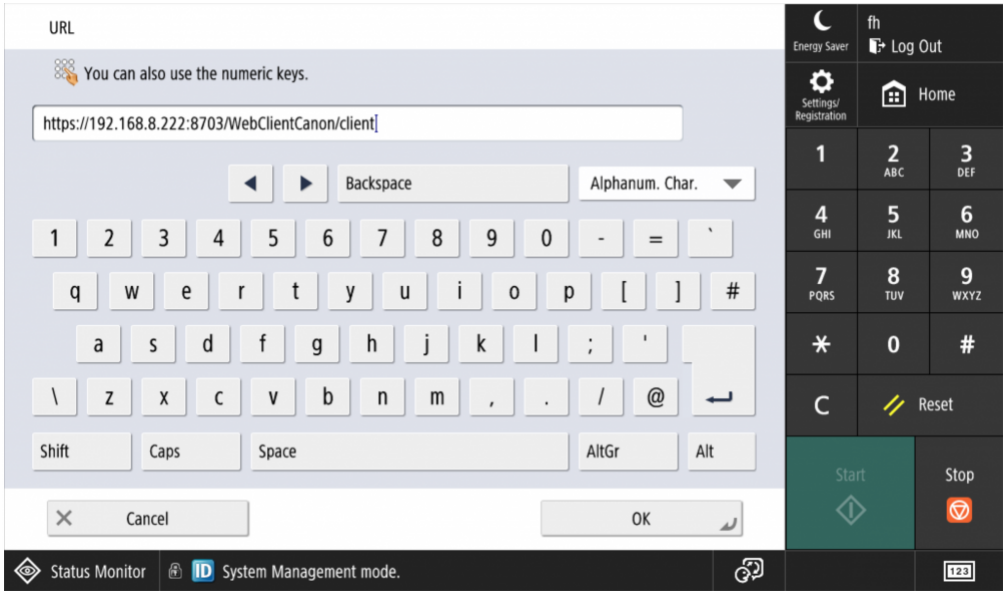
- Click 'Install'
- Click 'Yes' if a confirmation page is displayed.
- In the list of Login Service applications, the page should look like this:



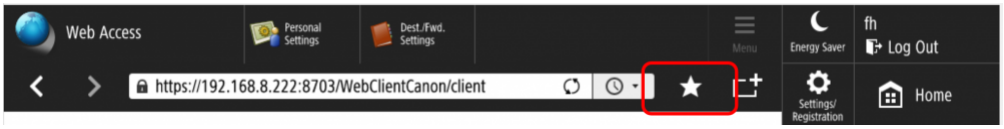
- Reboot the device to complete the installation (Reboot can be done remotely by pushing "To portal" and then "Restart Device" under "Settings/Registration")
- After the Printer is restarted push the Embedded configuration from embedded screen in SAFEQ Cloud

Setup browser

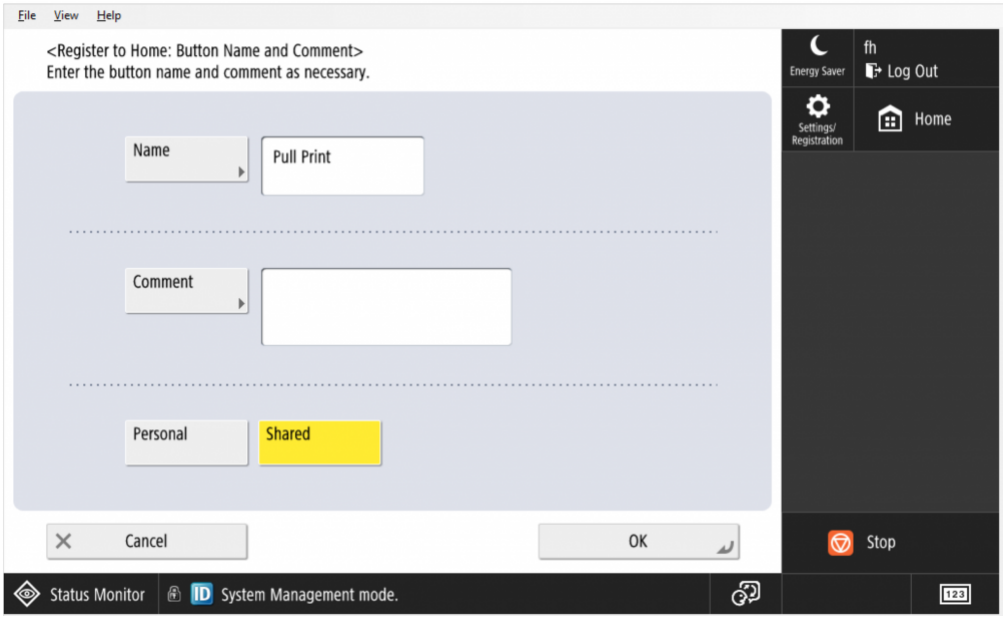
- On the device, open "Web Access" browser and enter the following address (take care as it is case sensitive), and afterwards click "OK": https://[SERVER-ADDRESS]:8703/WebClientCanon/client or https://[SERVER-ADDRESS]:8703/WebClientCanon/client?addr=hostname for the DNS setup



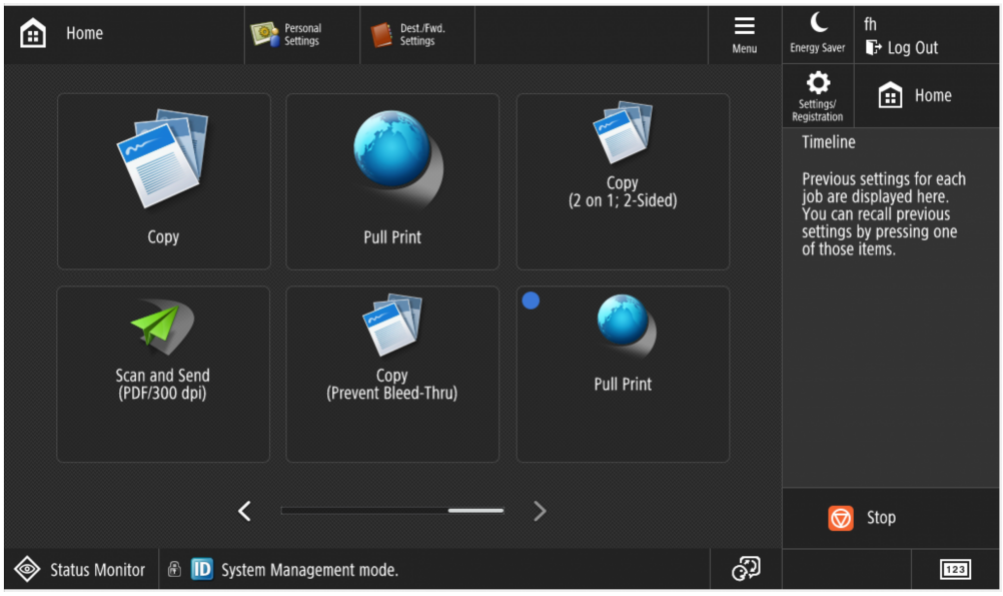
- After the web page is loaded, hit the "Favorite" button ( ), then select "Register to Quick Menu" and choose the first "Not Registered" slot.



- Give the button a name and choose "OK"



- Now the button is added in "Shared" functions in the "Quick Menu"



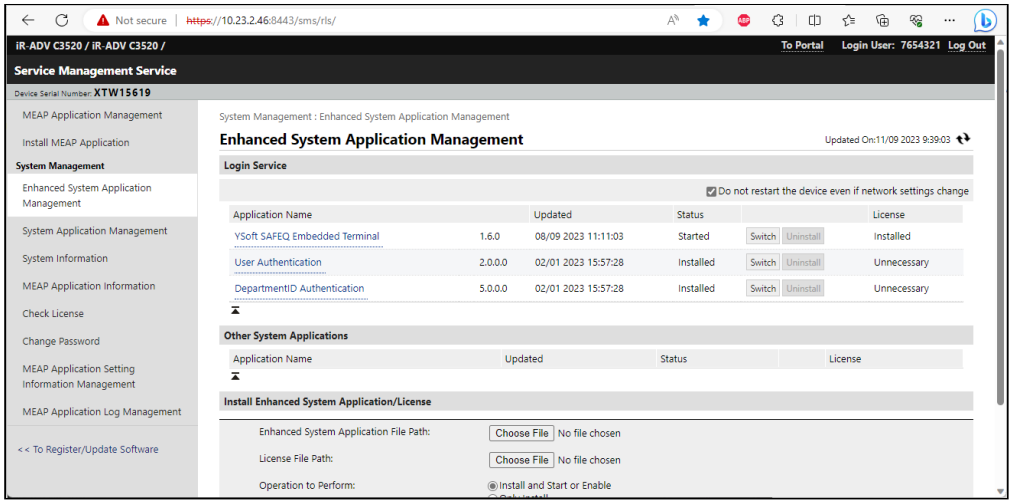
Notes:

- For changing the default menus and buttons, refer to the Canon manual

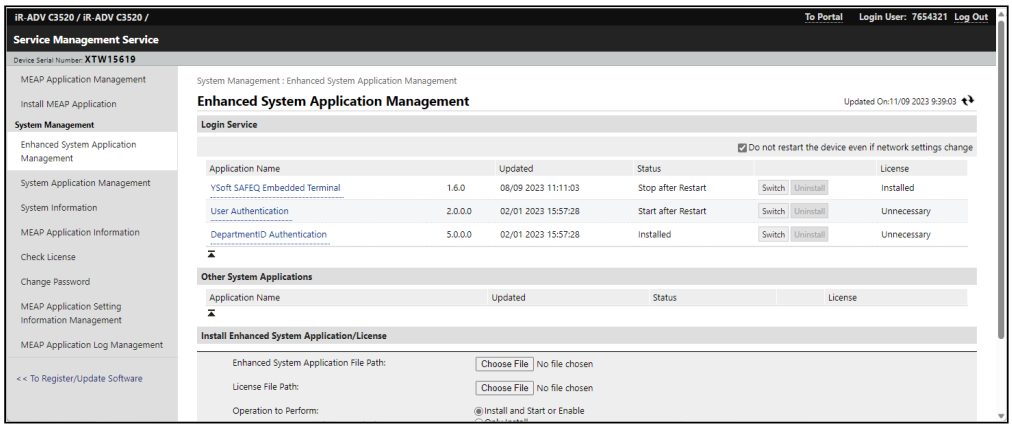
- To use a card reader on the device, you need to enable the card reader within the menu of the Canon device. Go to: "Settings" – "Preferences" – "External Interface" – "USB Settings", and then change "Use MEAP Driver for USB Device" to "On". Remember that the card reader needs to be configured as Keyboard emulated.

Uninstall login application

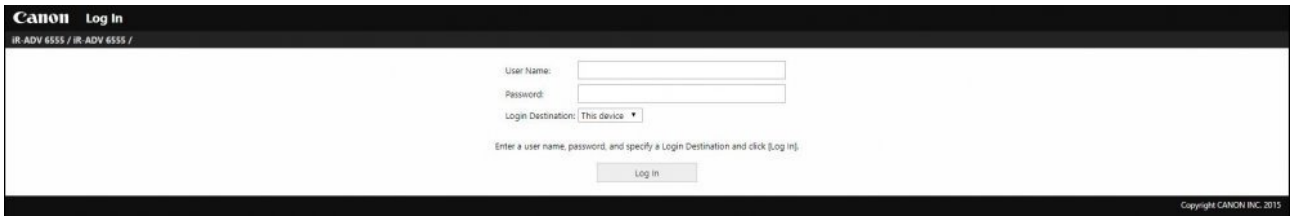
- Open the following page in a web browser. The default setting for both the System Manager ID and System PIN is '*7654321*: https://[PrinterIpAddress]:8443/sms/rls
- Push the "Switch" beside the "User authentication."



- Then the screen should look like this:

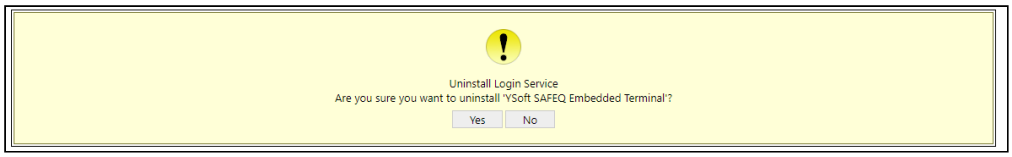


- Reboot the device
- After reboot, log in by using the administrator's username and password for the Canon Device. The default user name for the administrator is "*Administrator*" and the default password is "*7654321*"



- Browse to "Service Management Service"

- Push the "Uninstall" beside the "YSoft SAFEQ Embedded Terminal." If the uninstall button is disabled, you may have to disable and delete the license file.
- Push "Yes" to uninstall YSoft SAFEQ Embedded Terminal.

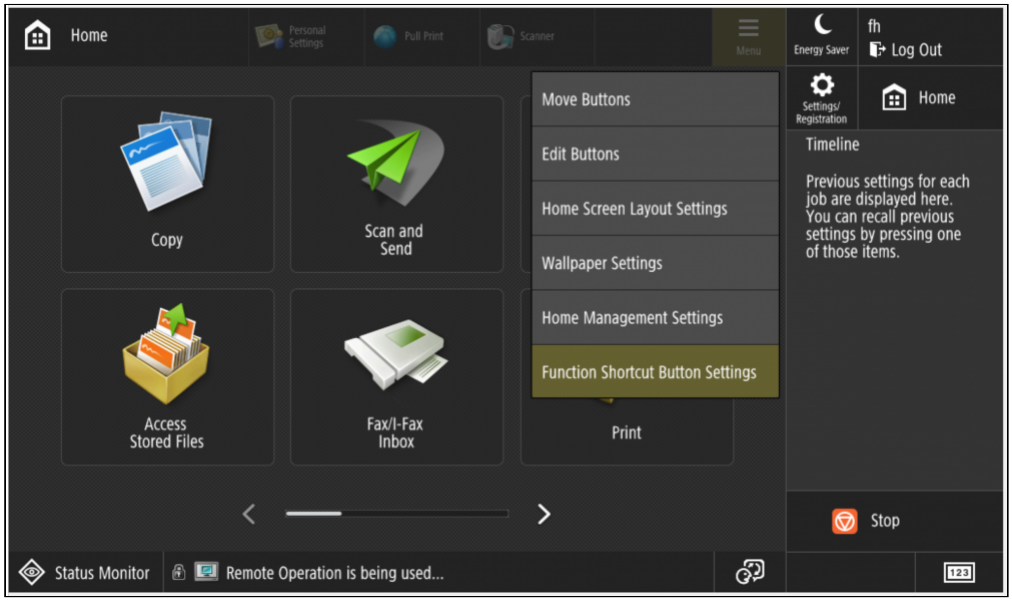


- Reboot device, and then the uninstall of the "YSoft SAFEQ Embedded Terminal" should be finalized.

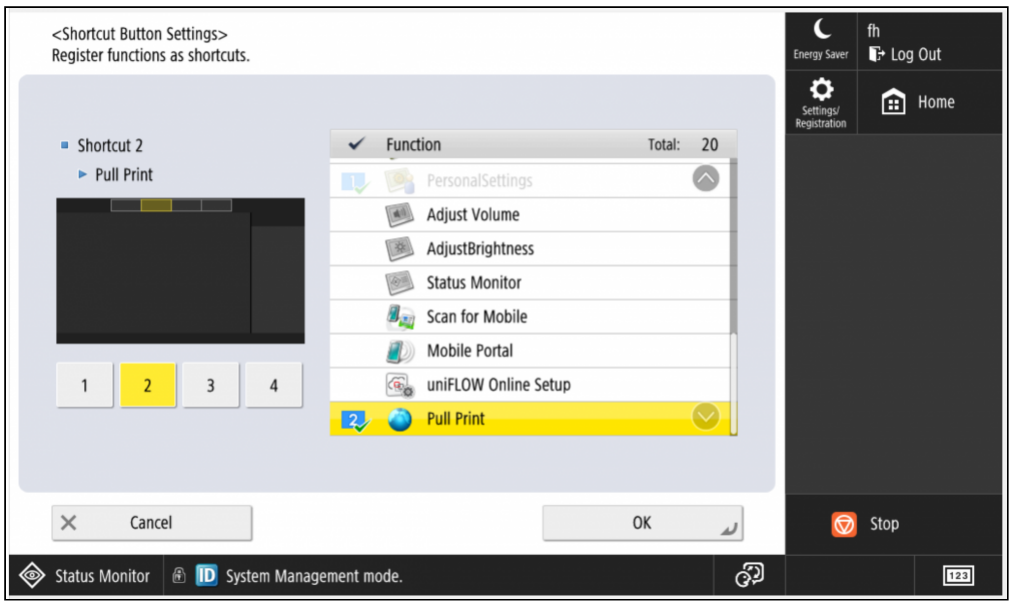
Customize UI

Shortcuts

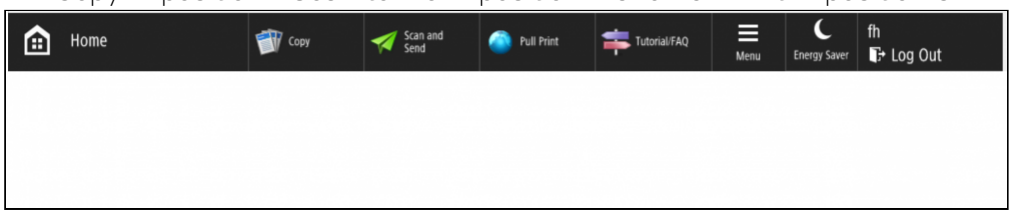
It is possible to link features as shortcuts, in the top of the screen.
From the menu, select Function Shortcut Button Settings



Select the shortcut position on the left and link it with the feature on the right

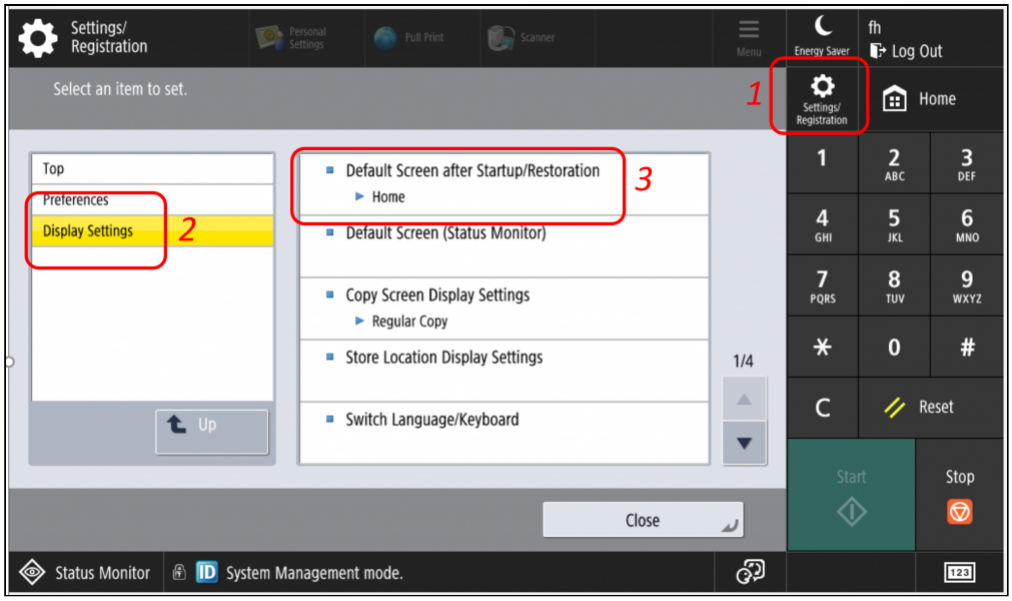


Ex.: Copy in position 1 Scan to me in position 2 and Pull Print in position 3

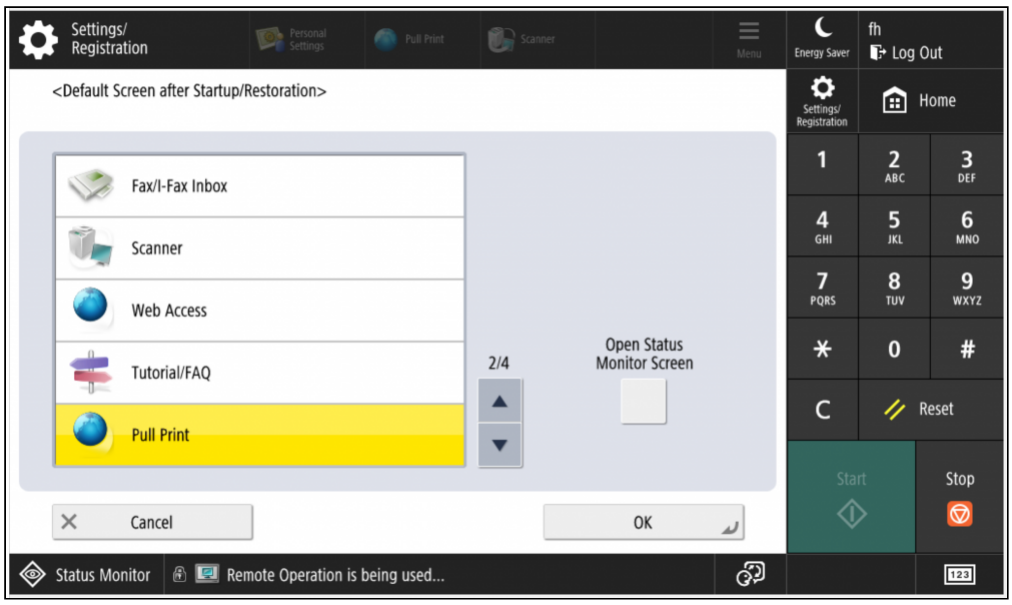


Start screen

To configure the start screen that is shown after login go to Settings / Registration (1), find Display Settings (2) and select Default Screen (3)



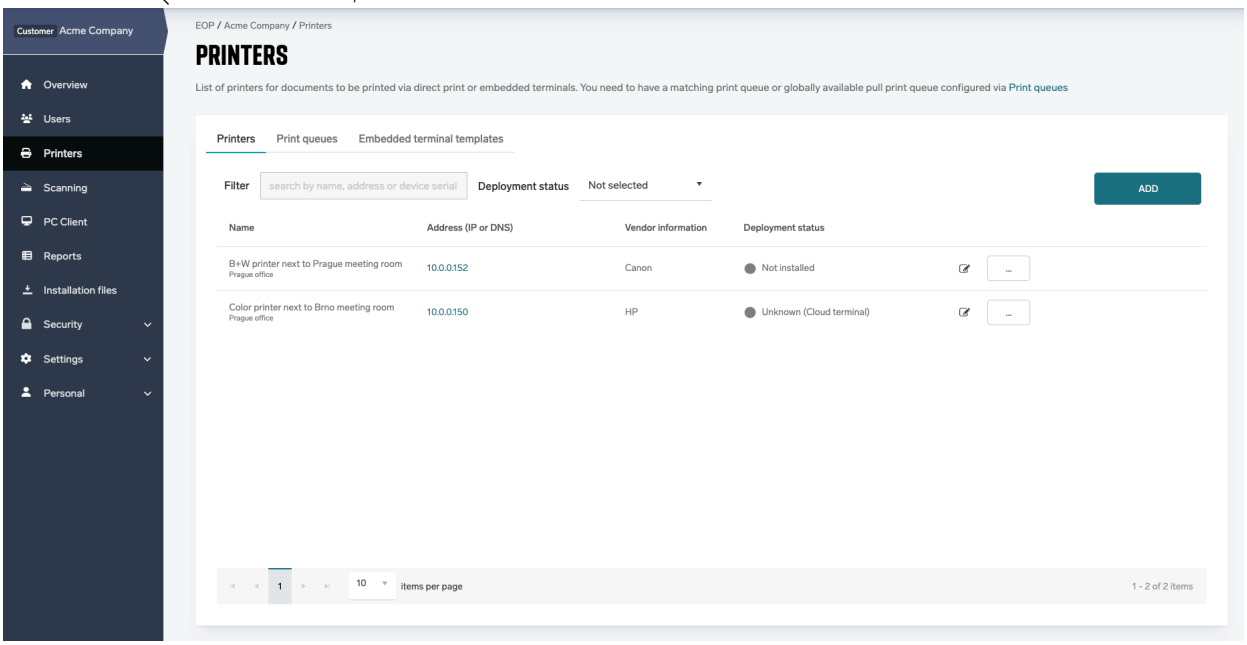
Browse to the feature you want to start in



Printers

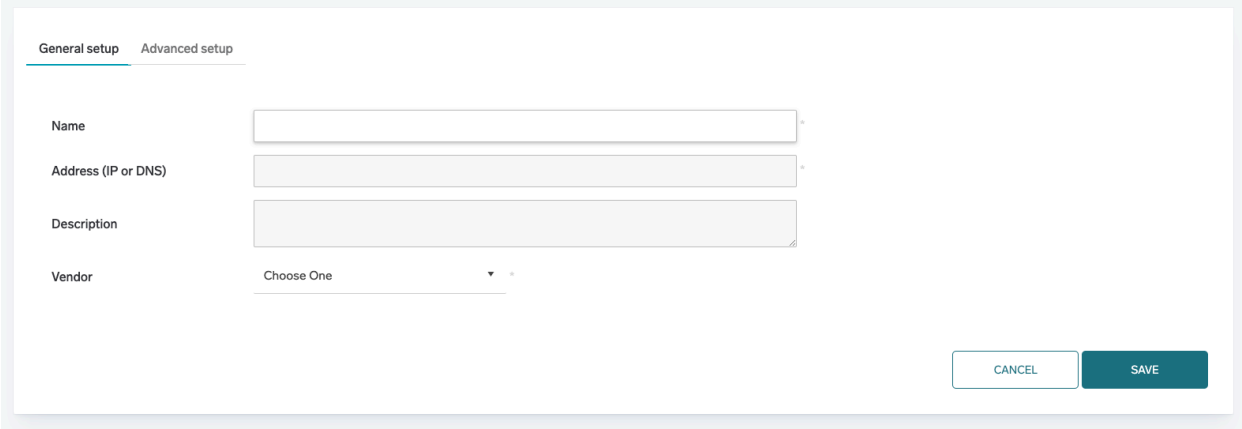
Adding a printer

1. In the SAFEQ Cloud Web UI, click **Printers**.



2. The **Printers** list shows basic information for the MFDs configured for this account.
3. Click **Add** to add a new MFD. A dialog window will be displayed.

4. On the **General setup** tab, configure the following:



a. **Name** – A user-friendly name of the printer within the account.

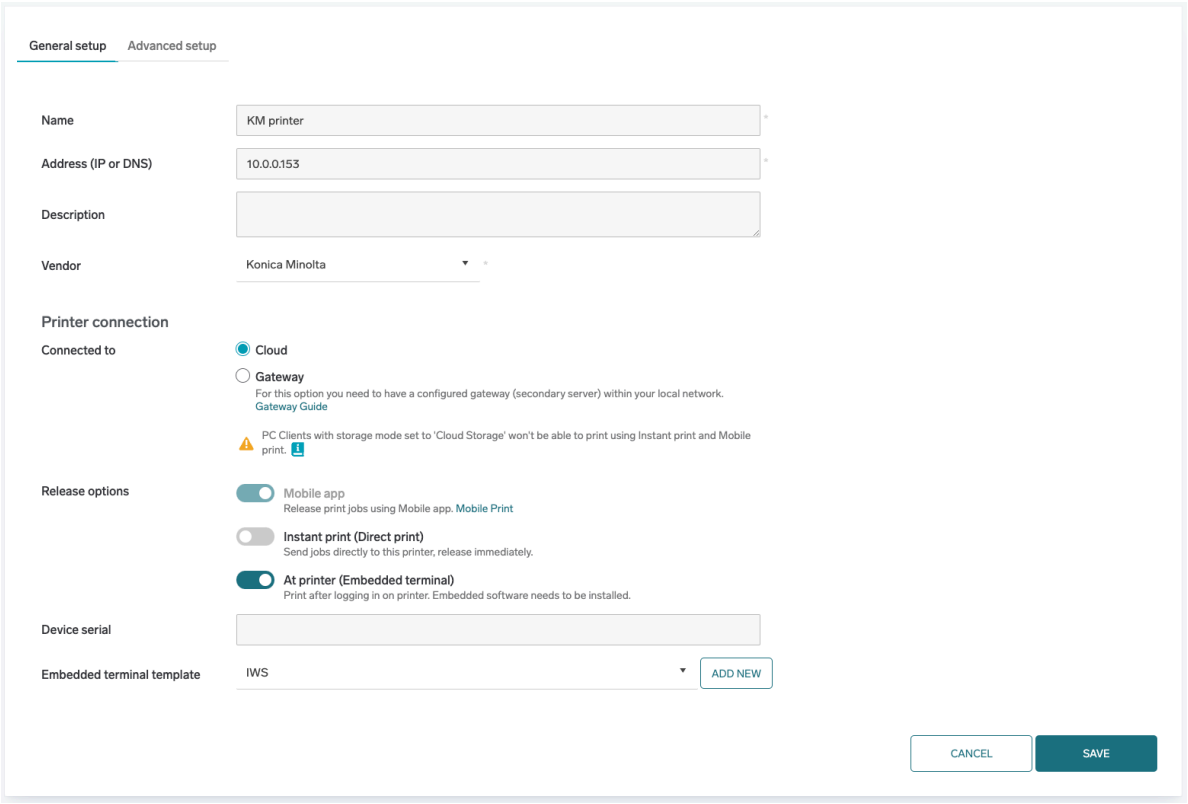
b. **Address** (IP or DNS) – The IP address or hostname of the MFD in your network.

c. **Description** – Additional information about the MFD.

d. **Vendor** – Select the MFD vendor from the drop-down list.

> SAFEQ Cloud uses the vendor type to determine how the print data stream should be translated from the Universal Driver.
> If you don't want SAFEQ Cloud to optimize print jobs, or if you want to use a third-party driver, choose the option **Other vendor**; then the **Print language** property will be set to **Raw** and the job data will be passed to the printer unmodified.

5. Once a vendor is selected, new configuration fields are displayed:



a. **Connected to** - Defines how the device is connected

1. **Cloud** - device is connected directly to the cloud

> PC Clients with storage mode set to 'Cloud Storage' won't be able to print using Instant print and Mobile print when the Cloud option is selected. For details on the service setup, see SAFEQ Cloud Client configuration.

2. **Gateway** - For this option you need to have a configured gateway (secondary server) within your local network. If there is no gateway detected, this option is disabled.

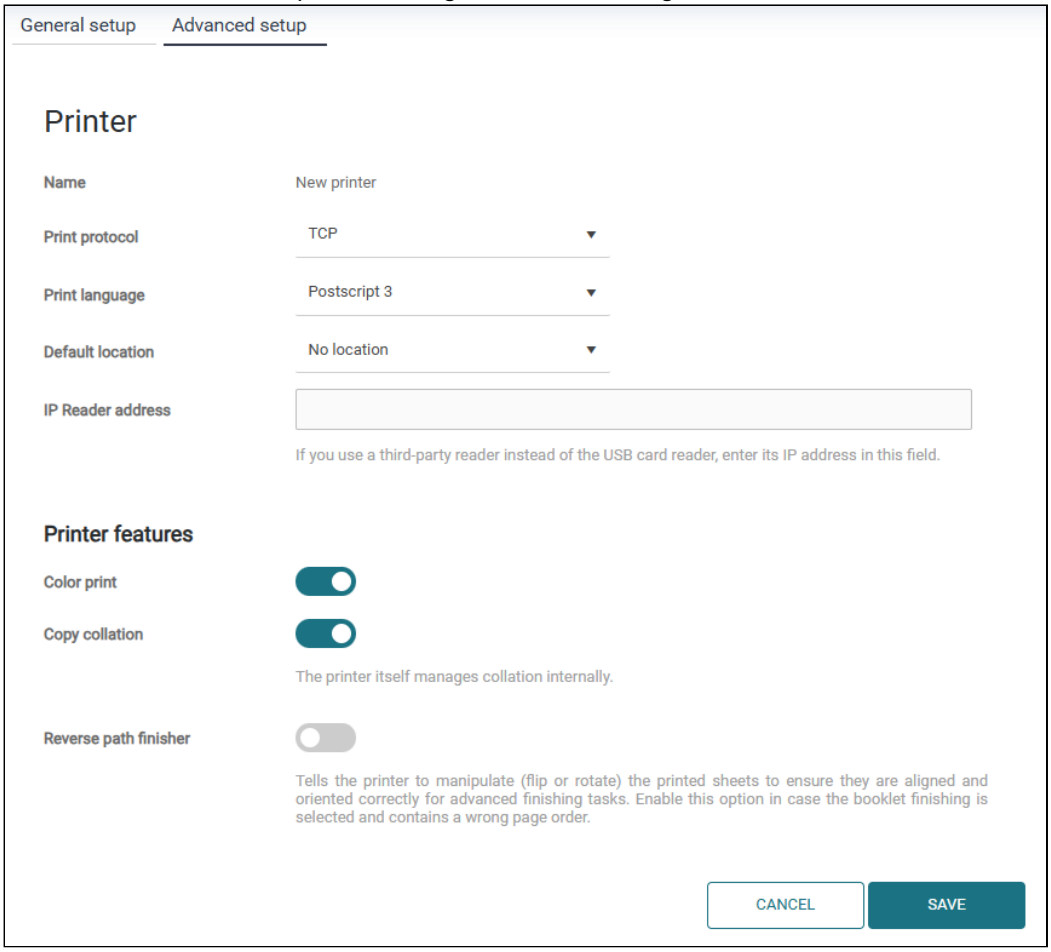
    1. **Document output service** (Available when the 'Gateway' option is selected under 'Connected to'. For the 'Cloud' option, this service is selected automatically.) – Select the Document output service from the drop-down list. If no service exists, you can add it by clicking **Add**. The Document output service is responsible for delivering print job data to the MFD if there is no direct IP visibility from the PC clients to the MFD. Note that for direct print queues, this service must have direct IP visibility to the printer. For Print Roaming, the service can be the same as for terminal services, and the print job is always delivered in the most efficient way – either directly from the SAFEQ Cloud Client in case of visibility to the MFD, or downloaded from the selected service.

b. **Release options** - Defines how print jobs are released from the MFD.

1. **Mobile app** - Allows users to release documents from Mobile app. This option is always enabled.

2. **Instant print (Direct print)** – This option will automatically create a matching Print queue for the MFD. The default settings for this Print queue are: a name identical with the MFD, Direct (Push) Print queue type, linked to the Printer, available by default.
3. **At printer (Embedded terminal)** - This option allows you to configure the embedded terminal on the MFD, enabling users to release documents after logging in. Embedded software must be installed. The option is disabled (cannot be enabled) for vendors that do not support an embedded terminal.
   Following configuration is available when this option (At printer) is selected:
   1. **Embedded terminal template** – Select the embedded configuration from the drop-down list. If no embedded configuration exists, you can add it by clicking **Add**. In that case, a new dialog window will appear. For details on the available settings, see Embedded Terminals' configuration.
   2. **Client terminal service** (Available when the 'Gateway' option is selected under 'Connected to'. For the 'Cloud' option, this service is selected automatically.) - Select the Client terminal service from the drop-down list. If no service exists, you can add it by clicking **Add**. Client terminal service deploys embedded terminal clients running on MFDs, and the service with which MFDs communicate for authentication, retrieving job lists, and other purposes. The MFD will communicate to the selected service that may be deployed in the cloud or hosted locally on an edge device.

6. On the **Advanced setup** tab, configure the following:

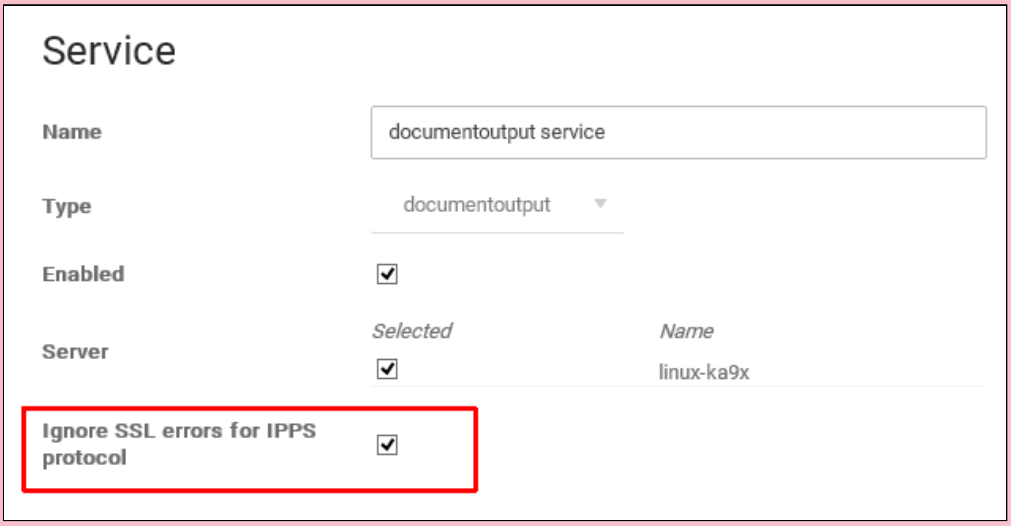


a. **Print protocol** – Select the communication protocol to the MFD according to the following table:

Protocol	Usage	Notes
TCP (default)	Direct delivery to printer via TCP port 9100	SAFEQ Cloud has control over print process, show errors in the log
IPP	Direct delivery to printer via IPP protocol	SAFEQ Cloud controls delivery, supports both IPP and IPPS printing

b. **IPP** – If you wish to use IPP printing, enter the Printer IPP URL for the destination printer:

If printing via IPPS/HTTPS to the printer, and the device uses a self-signed certificate or other non-trusted certificates, go to the relevant Document Output service and enable **Ignore SSL errors for IPPS protocol.**



If you wish to send the username together with the print job, enable the **Publish username** option (available only for IPP). Note that in such case all jobs printed on this MFD will contain the user's username. If you leave it in the default state (disabled), all jobs will be shown as printed by an anonymous user.

> ⚠ If you enable **Publish username**, make sure that access to the printed jobs at the MFD is restricted, so that sensitive data, such as who printed what, is not disclosed.

c. **Print language** – Select the output type for the print job data. The languages listed are based on the vendor you selected and correspond to those supported by SAFEQ Cloud. Only select the **Raw** output type if you use a third-party print driver instead of the SAFEQ Cloud universal driver. In this case, the job data will be passed to the MFD unmodified. Select the other languages (Postscript2, Postscript3, PCL6, or PDF, depending on availability) when using the universal driver for printing.

d. **Default location** – Select the MFD location. If no location is set, SAFEQ Cloud will retrieve and display the inherited location of the parent node.

e. **IP Reader address** – If you use a third-party IP card reader instead of the USB card reader, enter its IP address in this field (for specific cases MAC address is also acceptable).

f. **Color print** – Enabled by default. This option affects only reporting – if disabled, reports will not contain any information regarding color pages. If you want to control how a job is printed, use Rules - triggers and automation.

g. **Copy collation** – Enabled by default. When enabled, copy collation is handled by the MFD. When disabled, it is handled by the print driver. If your MFD doesn't support this function, disable it here. Note that this will make the advanced finishing options unavailable (for example, stapling and booklet) and increase the job size.

h. **Reverse Path Finisher** – Disabled by default. Instructs the MFD to manipulate (flip or rotate) the printed sheets to ensure they are aligned and oriented correctly for advanced finishing tasks. Enable this option if booklet finishing is selected and the pages are in a wrong order.

7. Click **SAVE**.

Other Printer actions

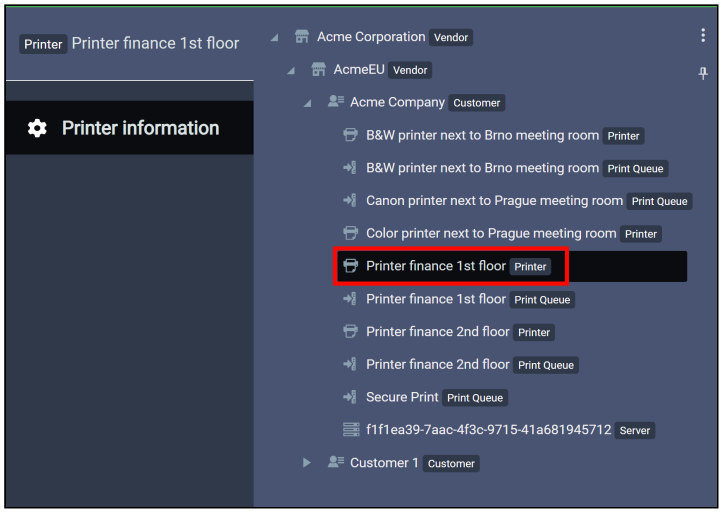
In the Printers list, click the edit icon or the three-dots button to access the following actions from the pop-up menu:

	Edit Printer settings	If you don't have the edit permission, settings are read-only.
	Show QR code	Opens a pop-up to display the QR code for Mobileprint scanning (verify browser settings do not block pop-up)
	Duplicate	Creates a duplicate of an existing printer configuration, where all settings are pre-populated to match the original. The only fields left blank or needing modification are the IP address (blank) and the printer name, which will automatically include a "Copy" suffix to differentiate it from the original.

	Delete	Deletes a printer after the user confirms by clicking "OK" in a pop-up prompt.
	Deployment actions	Navigates to the Embedded Configuration Deployment page, where deployment actions are available for a printer. This option is available only when an embedded configuration is assigned to a printer.

Printer details

MFDs appear in the SAFEQ Cloud system tree as sub-nodes of the account. Selecting the MFD in the tree displays the sub-menu.



The details page consists of the following tabs:

- General setup – Click this tab to edit printer settings, or delete the printer.
- Advanced setup – Contains the settings described in the *Adding a printer* section.
- Access control – Manage the permissions to access this MFD. For more details on Access control settings, see Access Control.
- Document history – Displays a list of jobs, the job owner (user name), status, number of pages, and date/time for each job printed on the device.

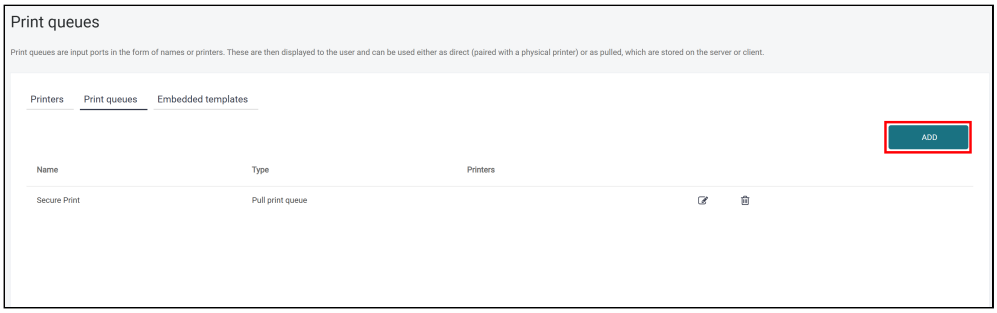
Print queues

Print queues are created at an Account level within the SAFEQ Cloud system tree and define how users can send documents into the SAFEQ Cloud system for Direct print, Pull print, Storage, etc.

Adding a Print Queue

1. In the SAFEQ Cloud Web UI, click Printers > Print queues.

2. The **Print queues** list shows the name and type of the Print queues configured for the Account. Click **Add.**



3. Fill in the following:

   a. **Name** – The name of the Print queue as it appears in the SAFEQ Cloud system tree.

   > The name of the Print queue is specified as part of the URL used to configure the Client devices that send jobs to SAFEQ Cloud. We recommend you to keep the Print queue name short and descriptive.

   b. **Queue type** – Select between a Direct print queue and a Pull print queue. Direct queue sends the job directly to the output printer. Pull queue sends the job to the Storage Service, where it will be retained and released when a user visits a configured MFD (Roaming Printing).

   c. **Printer** (Direct print only) – Select the MFD that will print the print jobs sent to the Direct queue.

   d. **Available by default** – When this option is set, the Print queue will appear for users with access on workstation PC's, mobile Apps, etc. This option is enabled by default, and it can be changed by the user in their own profile in the **My Printers** section.

   > **My Printers**
   >
   > For customers who have many direct queues, this section of SAFEQ Cloud Web UI provides their end users with the ability to choose their own favorite queues out of all the queues they have access to, apart from the default queues assigned to them by an admin. To see this section, the users must have the `ViewUserInputPorts` permission.

   > **Default print queue in Microsoft Windows**
   >
   > Default print queue is set only on the first PC client synchronization when there are no SAFEQ Cloud print queues present yet. If multiple pull queues are available for the user, the default queue will be the one with the lowest ID (found in the Cloud interface under Printers > Print queues > Print queue details > ID). After the initial synchronization:
   >
   > - SAFEQ Cloud client printer queues are dynamic, meaning they are automatically added or removed based on the user's login status.

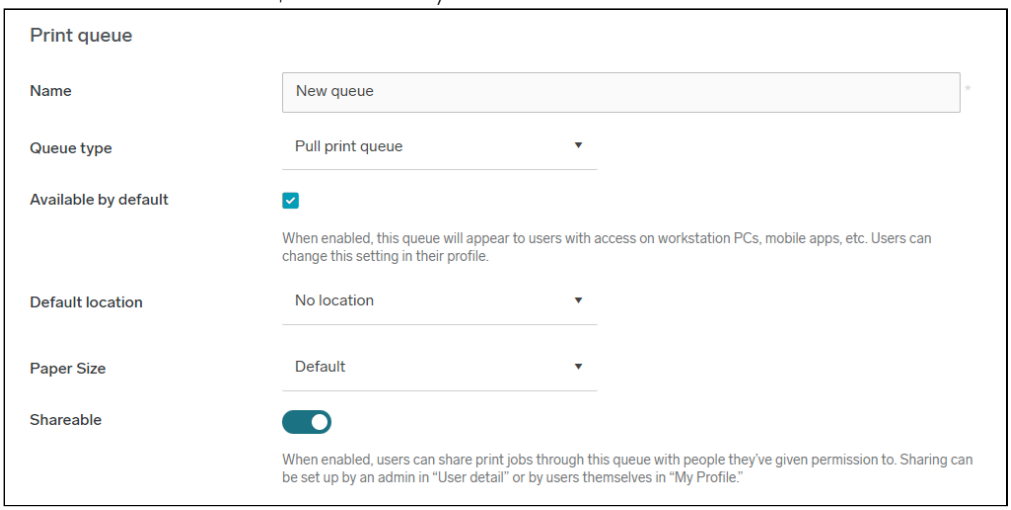
- SAFEQ Cloud client does not manage or retain control over the default print queue, allowing users to manually change the default print queue if needed - user changes to the default are preserved.

To ensure that newly added printer queues do not override the existing default, you can set KEEPDEFAULTPRINTER=true during installation. This setting also allows Group Policy Objects (GPOs) to enforce and maintain the configured default print queue settings consistently across clients.

e. **Location** – Select a location. If no location is set on the Print queue, it will retrieve and display the inherited location of the parent node.

f. **Paper size** – Select the paper size that will be used for printing with this queue. If you select **Not set**, the default paper size value from the terminal settings will be used. Note that some applications, such as MS Word, can override this selection.

g. **Shareable** (Pull print only) – When this option is enabled (the default), users that other users share their jobs with via the Sharing feature will be able to see those jobs when they are spooled into this queue. If this option is disabled, jobs spooled to this queue will not be visible to other users, even if they are shared.



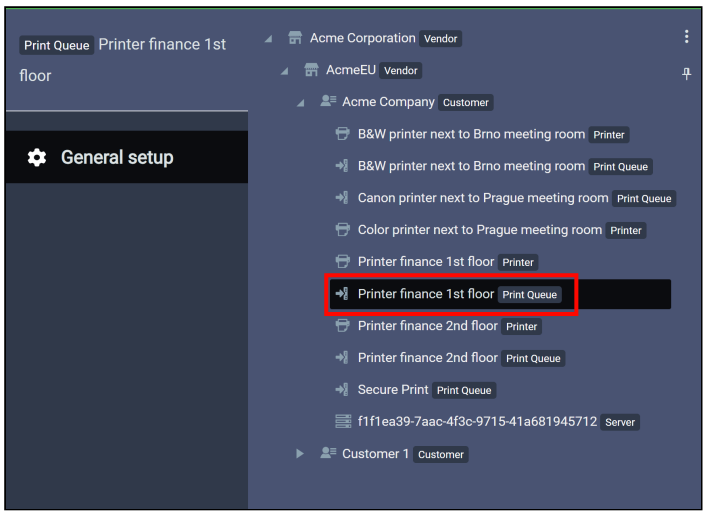
4. Click **Save**.

Editing and deleting Print queues

To edit an existing Print queue, open the Print queues list and click the edit icon. To delete a Print queue, click the delete icon and confirm your action.

General setup, Pending jobs, and Access control

Print queues appear in the SAFEQ Cloud system tree as sub-nodes of the Account. Selecting a Print queue in the navigation tree displays the sub-menu with **General setup**, **Pending jobs**, and **Access control**.



General setup

In this section, you can edit the queue name, Default location, and paper size.

Pending jobs

This section displays a list of jobs and the job owner (user name). If the Print queue is a Pull queue, this list will remain static until the jobs are released by users at the MFD. If the Print queue is a Direct queue, the pending list will show jobs in progress as they are sent to the printer via the Document Output service.

If you have the DeleteJob permission, you can delete jobs being held in a Pull queue by clicking the delete icon in the pending job list.

Access control

This section allows you to manage who has access to the Print queue. For more information about the roles and access controls configuration, see Access Control.

8.1.4 SCAN WORKFLOWS

The Scan workflows feature (scan to email, SharePoint, and OneDrive) is available only in the Y Soft-hosted cloud environment and only with pure cloud terminals (FUJIFILM BI, HP Workpath, Konica Minolta, Ricoh, Sharp, Xerox).

Scan workflows create digital content from paper documents consistently and accurately. Configure scan workflows in the Scan Workflows section of SAFEQ Cloud Web UI. Creating a workflow consists of three steps:

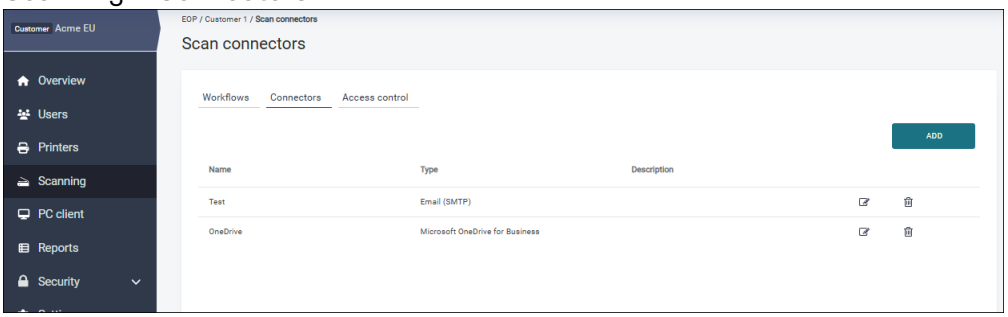
1. Create a connector – A connection to the final destination for the documents scanned via scan workflows. The final destinations are external systems such as Microsoft OneDrive. Each connector supports different settings during workflow creation.
2. Create a workflow – specify the name and description and select the connector (the destination). Optionally, you can enable document processing and use variables.

3. Set up access rules (access rights) – allow or deny access to selected users or groups of users.

Connectors

Creating and editing a connector

1. To create a connector or edit an existing connector, log in to SAFEQ Cloud Web UI and go to Scanning > Connectors.

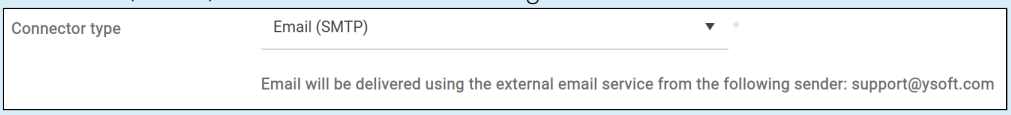


> Because connectors are required to be able to create workflows, they are available behind the same permission set.
>
> The user doing this configuration must have the "ViewScanWorkflow" permission to access the section. Additionally, permissions "CreateScanWorkflow", "ModifyScanWorkflow", and "DeleteScanWorkflow" are required for their respective actions to be enabled.

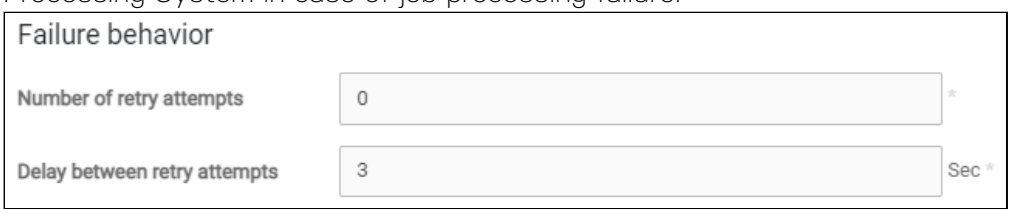
2. To add a connector, click **Add**. To modify a connector, click the edit icon. The form is the same for adding and editing a connector.

3. Fill in the name and description of the connector.

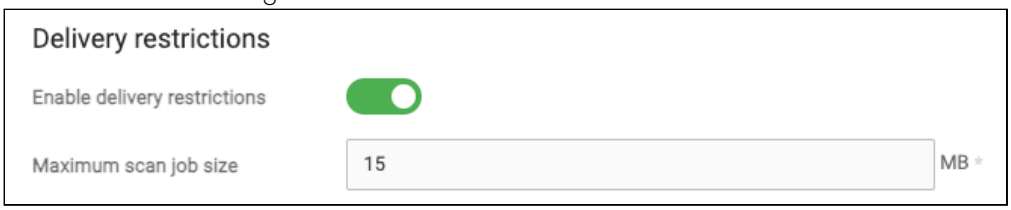
4. In **Connector type**, select the type. Further configuration fields specific to your selected connector type will be displayed.

> The Email(SMTP) connector has no configurable fields.
>
> 
>

5. Fill in the Failure behavior fields. These fields that control the behavior of the Workflow Processing System in case of job processing failure.



6. (Optional) Enable delivery restrictions and define the maximum size of a scan job that can be delivered when using the connector.



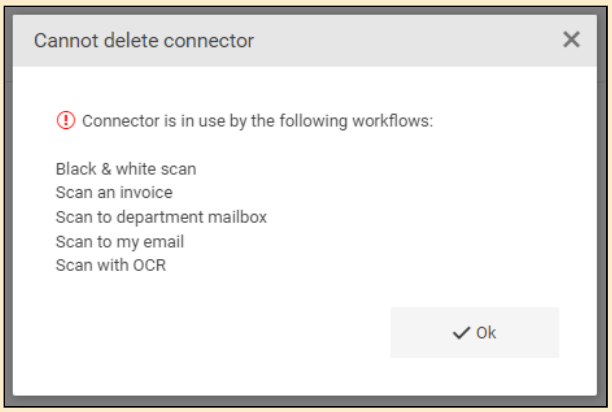
If you wish to set up a failure notification email, do so in the **Triggers** section. See Rules - triggers and automation.

Deleting a connector

You can delete a connector by clicking the delete icon next to the connector by clicking **Delete** in the connector detail.

To do this, you must have the *DeleteScanWorkflow* permission.

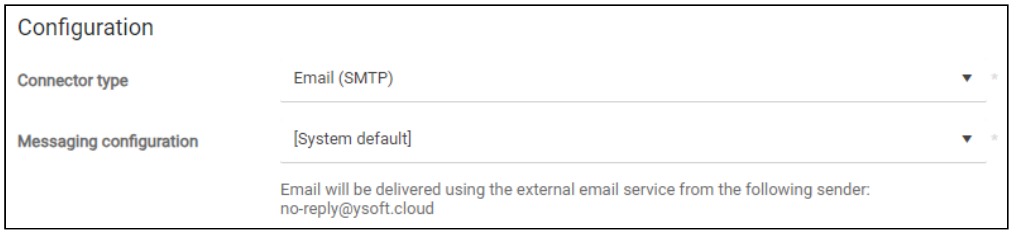
You cannot delete a connector that is used by one or more workflows. You will see an error message. The message displays a maximum of 10 workflows.



Email (SMTP) connector

The email connector sends scanned documents using the system SMTP configuration. The default system SMTP configuration is done by your SAFEQ Cloud provider.

Connector configuration



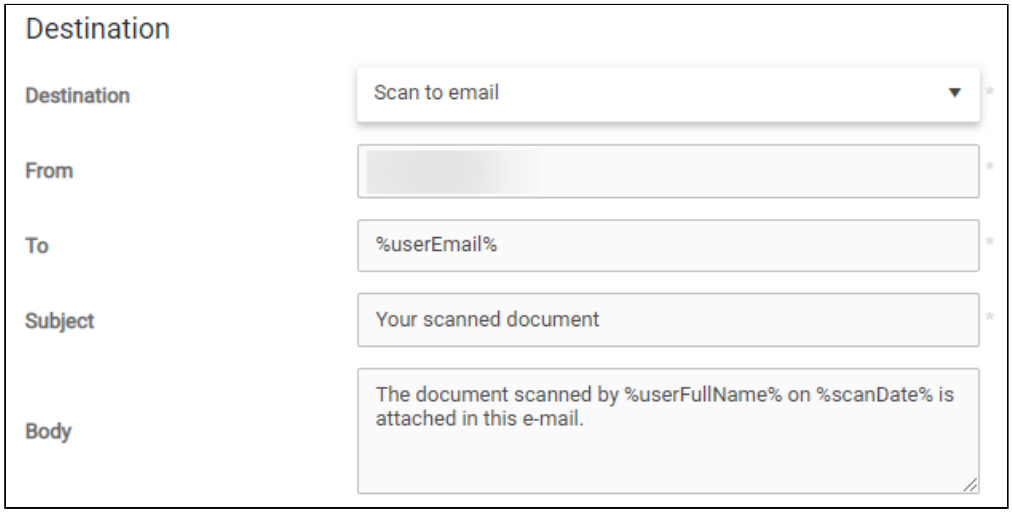
1. In **Connector type**, select **Email (SMTP)**.

2. In **Messaging configuration**, select **[System default]**. This option uses our globally available SMTP messaging service to deliver the scanned documents from SAFEQ Cloud to the SMTP server. If you wish to create a custom SMTP Messaging configuration, see Messaging.

   > The Message service as listed in Services is not used for delivery of scan documents to SMTP server. Emails are always delivered by SAFEQ Cloud to SMTP server specified in the email connector messaging configuration.

3. We recommend you to make sure that the SMTP server is accessible from SAFEQ Cloud by executing an SMTP Scan workflow from an MFD.

Workflow configuration



In this instance, the fields **From**, **To**, **Subject,** and **Body** are taken over from the selected email connector and represent its customizable parameters. You can also use various dynamic placeholders. See Workflow variables. The **From** field is read-only because it is set in your SAFEQ Cloud tenant's SMTP configuration. If your tenant is hosted by Y Soft and you have selected the **System default** messaging configuration, the emails are delivered by the SendGrid service.

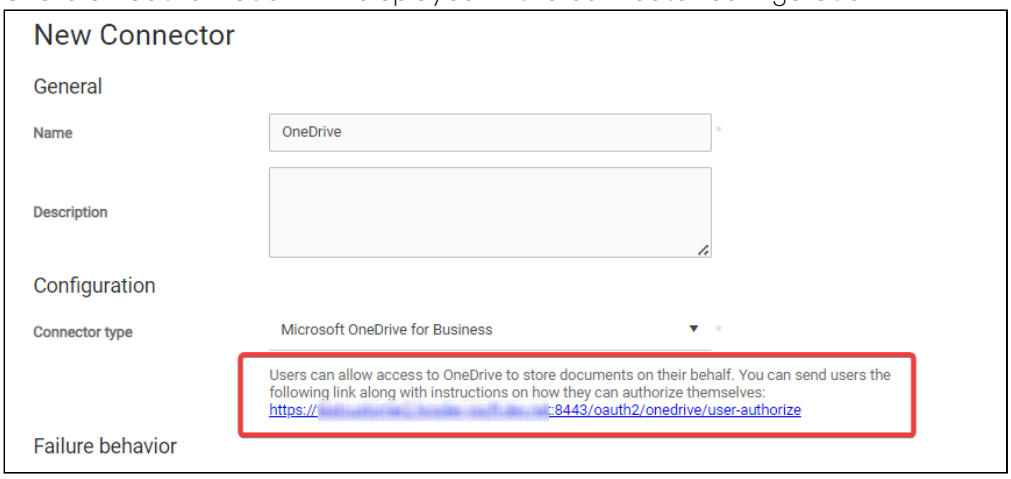
The **Body** field is optional and can contain HTML tags such as <br> or <a>.

Microsoft OneDrive for Business connector

Use the Microsoft OneDrive for Business (OAuth 2.0 with user-based access) type connector to deliver scanned files to a location in a selected Microsoft OneDrive for Business library with user-based authorization.

If you wish the users to authorize in advance (before going to the terminal), you can:

- Share an authorization link displayed in the connector configuration.



- Advise the users to use the **Authorizations** tab in **My profile** section of SAFEQ Cloud Web UI.

Integration is done using **Graph API**. Access is granted on per-user basis using **OAuth2 Authorization Code Flow** and the authorization is secured via **Proof Key for Code Exchange (PKCE)**.

The following permissions (scopes) are needed:

Scope	Description	Reason
Files.ReadWrite	Have full access to user files. Allows the app to read, create, update, and delete the signed-in user's files.	To be able to upload and modify (create folders, append into files) content on the user's behalf.
offline_access	Maintain access to data you have given it access to. Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	To keep access working even after one hour.

Connector configuration

There are no additional configurable fields.

Workflow configuration

Target OneDrive relative path – The directory where the workflow delivers scanned files, relative to the root of the user's drive.

Microsoft SharePoint Online connector

Use the Microsoft SharePoint Online (OAuth 2.0 with user-based access) type connector to deliver scanned files to a location in a selected Microsoft SharePoint Online document library with user-based authorization.

If you wish the users to authorize in advance (before going to the terminal), you can:

- Share an authorization link displayed in the connector configuration.
- Advise the users to use the **Authorizations** tab in **Personal** > My profile section of SAFEQ Cloud Web UI.

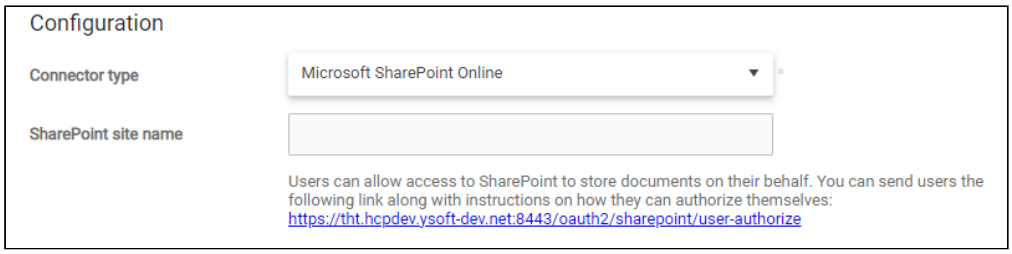
Integration is done using Graph API. Access is granted on per user basis using OAuth2 Authorization Code Flow, authorization is secured via Proof Key for Code Exchange (PKCE).

The following permissions (scopes) are needed:

Scope	Description	Reason
Sites.ReadWrite.All	Allow the application to edit or delete documents and list items in all site collections on your behalf.	To be able to upload and modify (create folders, append into files) content on the user's behalf.
offline_access	Maintain access to data you have given it access to. Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	To keep access working even after one hour.

Connector configuration

You can find the link for users to initiate authorization of the connector in this section.



SharePoint site name – Define the site names you want your scans to be delivered to (marked below in green).

- If you use a custom site, the address will have this form: `https://myCompanyName.sharepoint.com/sites/<mySite>/<myOptionalSubsite>/<myDocumentLibrary>/Forms/AllItems.asp`
  - Open your SharePoint site in your web browser. The part of the address that you need to enter in **SharePoint site name** is `sites/<mySite>/<myOptionalSubsite>`

    Example: If the address of your SharePoint site is `https://acme.sharepoint.com/sites/HR/hiring/templates/Forms/AllItems.asp`, the **SharePoint site name** will be `sites/HR/hiring`.

- If you use the default SharePoint site, the address will have this form: `https://myCompanyName.sharepoint.com/<myOptionalSubsite>/<myDocumentLibrary>/Forms/AllItems.asp.`
  - Open your SharePoint site in your web browser. The part of the address that you need to enter in SharePoint site name is `<myOptionalSubsite>`

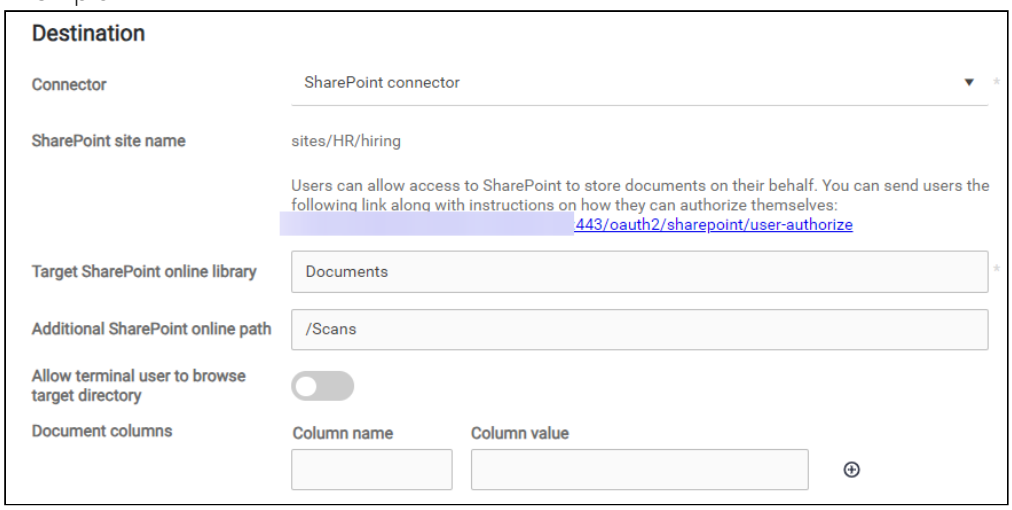
    > Example: If the address of your SharePoint site is `https://acme.sharepoint.com/legal/templates/Forms/AllItems.asp`, the SharePoint site name will be `legal`.

- Leave empty in case you wish to use the default site.

There are no additional configurable fields.

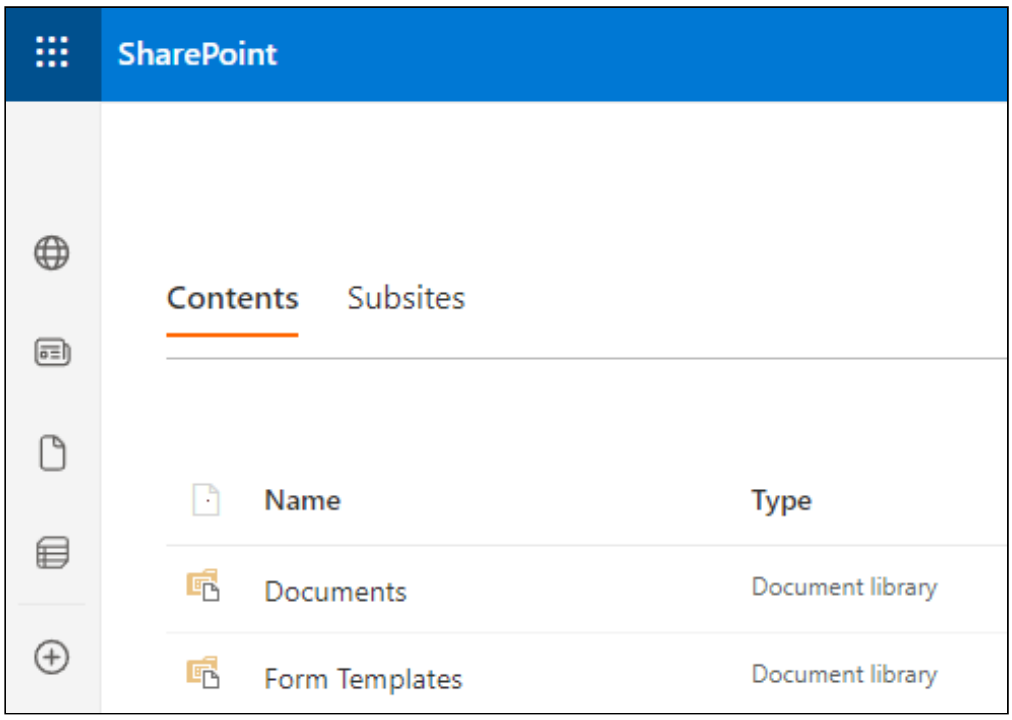
Workflow configuration

Example:

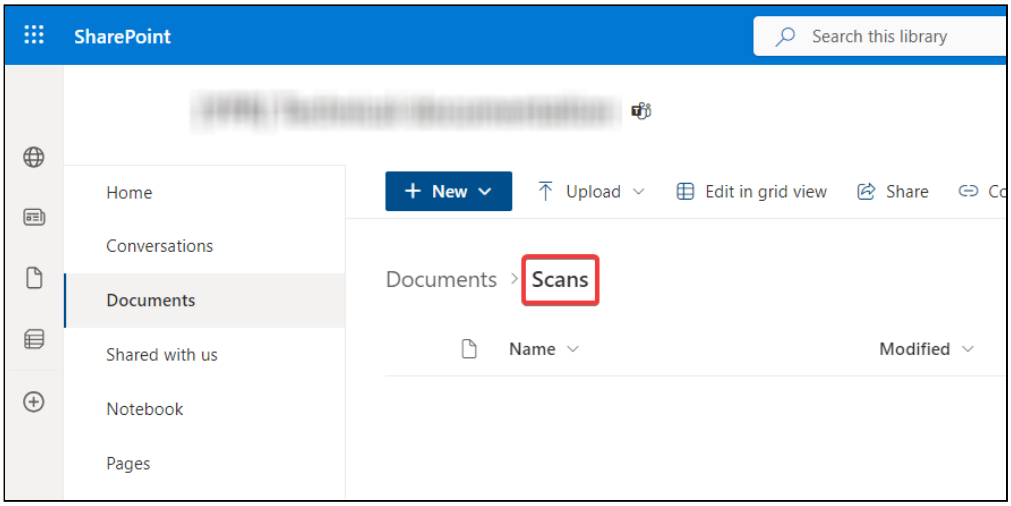


1. In Connector, select your SharePoint connector.
2. The SharePoint site name is taken automatically from the connector configuration.
3. In Target SharePoint Online Library, enter name of the public SharePoint library. Be aware that the SharePoint library name is case-sensitive. Usually, at least the library "Documents" exists by default, so you can make an initial test using this library. The library name is taken from the Document Library, which the user can see on their SharePoint page.

   > The library name in the SharePoint URL and in the SharePoint UI may differ from the real name of the library. This may happen, for example, when your SharePoint is installed in languages other than English or when someone renamed the library. You can obtain the real name via Graph API.See the section *Obtaining the real name of the SharePoint library* below.



4. In Additional Sharepoint Online path, enter the directory where the workflow delivers scanned files, relative to the connector's document library. You can use Capture variables. Keep in mind the limitations of characters that are allowed to be in paths. Optionally, you can specify a path to a subfolder.



5. In Document columns, you can add an administrator-predefined document column to the corresponding SharePoint document metadata. The document column value must be a string in the format expected by the SharePoint column. Otherwise, the column value will not be saved. You can use variables in column values. Duplicate column names are not allowed.

Obtaining the real name of the SharePoint library

1. Go to https://developer.microsoft.com/en-us/graph/graph-explorer.
2. Log in with an account that has access to the library.
3. Search for the site using the following query:

```
https://graph.microsoft.com/v1.0/sites?search=<site>
```

Example:

```
https://graph.microsoft.com/v1.0/sites?search=acme
```

4. Locate your site and copy the site ID.
   Example:

```
acme.sharepoint.com,779cddfd-cef6-4d5a-b361-387183042c00,b9423f0d-e151-4e78-897d-5f2271751d39)
```

5. List the document libraries using the following query:

```
https://graph.microsoft.com/v1.0/sites/<library id>/drives
```

Example:

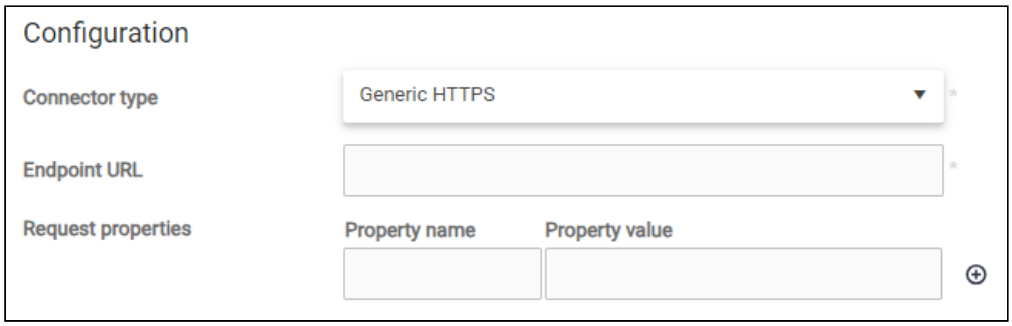
```
https://graph.microsoft.com/v1.0/sites/acme.sharepoint.com,779cddfd-cef6-4d5a-
b361-387183042c00,b9423f0d-e151-4e78-897d-5f2271751d39/drives
```

6. Locate the document library in the response and use the "name" as the library name in the **Target SharePoint Online Library** field in SAFEQ Cloud.

Generic HTTPS connector

Use the Generic HTTPS connector to deliver scanned files to a specific HTTPS endpoint for custom post-processing. The endpoint must be able to handle the predefined request format.

Connector configuration



- **Endpoint URL** – HTTPS endpoint URL where the scanned documents should be sent (for example, Azure function URL).
- **Request properties** (optional) – properties in the name-value pair propagated to the Endpoint URL.

Each custom request property will be sent to the endpoint URL as a separate part in a single multipart/form-data request. The property name is automatically prepended with "custom_" prefix to avoid collisions with existing properties. For example, "MyProperty=1234" will be sent as "custom_MyProperty=1234" parameter.

Request

The scanned job files are sent all together in a single multipart/form-data request. The request also includes all scan parameters, which are added dynamically.

API documentation that your endpoint should implement

```
openapi: 3.0.0
info:
description: This is an API for uploading scan jobs
version: "1.0.0"
title: API scan connector

paths:
  /api/scan:
    post:
      summary: Uploads and process scan job
      description: |
        Upload scan job (both data and metadata),
      responses:
        '200':
          description: scan job processed successfully
        '400':
          description: 'error'
      requestBody:
        content:
          multipart/form-data:
            schema:
              type: object
              properties:
                username:
                  type: string
                  # all other connector-specified and user-defined variables goes here
                  # in the same way as username
                  # e.g:
                  # mailTo:
                  # type: string
                  # mailFrom:
                  # type: string
                filename:
                  # default is application/octet-stream, need to declare the type
                  # e.g. application/pdf or image/jpg
                  type: array
                  items:
                    type: string
                    format: binary
              encoding:
                filename:
                  contentType: image/jpeg, image/tiff, applicaton/pdf
                  style: form
                  explode: true
```

Example request

A request with one variable *%userEmail%* and one document. In a production environment, the request would contain all the scan metadata, all available user inputs, and all files. The boundary is randomly generated with each request.

```
POST / HTTP/1.1
Connection: keep-alive
Content-Type: multipart/form-data; boundary=--------------------------123456789
Content-Length: 554

----------------------------123456789
Content-Disposition: form-data; name="userEmail"

john.doe@company.com
----------------------------123456789
Content-Disposition: form-data; name="file1"; filename="document.pdf"
Content-Type: text/plain

Content of document.pdf.

----------------------------123456789
```

Example parameters that are added to the multipart/form-data request

Example of paramaters sent in the request

```
scanTime: 15-57-20-003,
workflowID: 3,
scanJobID: 89905361-d77c-45ae-a2d1-6179283dddb5,
userDepartment: ,
scanDate: 2023-10-17,
deviceDescription: Printer,
safeqHome: \opt,
userEmail: user@mail.com,
deviceID: 1,
userHome: ,
workflowName: My workflow,
userUsername: user@2,
userFullName:
```

In addition, any custom input variables set in the workflow, such as *%faxNumber%*, will be included in the request too.

Google Drive connector

Overview

Use the Google Drive connector to deliver scanned files to a location in a selected Google Drive with user-based authorization.

The connector is configured to use non-sensitive access, as recommended by Google. This allows SAFEQ Cloud to access only those files and folders that were previously created by SAFEQ Cloud. While this method is safer than granting SAFEQ Cloud access to the entire disk, it means that users cannot browse folders they have created in their disks or replace/modify existing files.

SAFEQ Cloud communicates with Google Drive via the Google Drive API. Access is granted on a per-user basis using OAuth 2.0 to Access Google APIs.

The following permissions (scopes) are used:

Scope	Description	Reason
https://www.googleapis.com/auth/drive.file	Create new Drive files, or modify existing files, that you created with the application.	To be able to upload and modify (create folders, append into files) content.

Limitations

Append to PDF might not work properly if two or more users are modifying the same document at the same time due to a limitation in Google Drive's ability to resolve conflicts.

User authorization

If you wish the users to authorize in advance (before going to the MFD), you can:

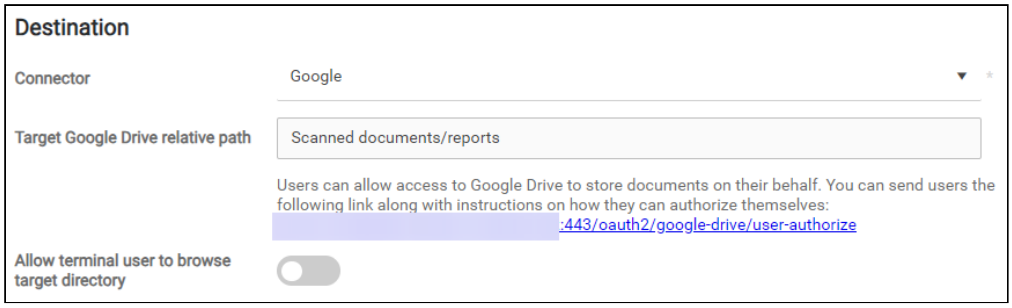
- Send them an authorization link displayed in the connector configuration.
- Advise them to authorize the Google Drive connector on the Authorizations tab in Personal > My profile section of SAFEQ Cloud Web UI.

The users can revoke the authorization at any time from their Google account: https://myaccount.google.com/connections?filters=3.

Connector configuration

This section does not contain configurable fields, only the link for users to authorize the connector.

Workflow configuration



In the Target Google Drive relative path, enter the folder where the workflow delivers scanned files, relative to the root of the user's drive. For example, *Scanned documents/reports*. If the folder doesn't exist, the connector will create it.

Scan to download (My documents) connector

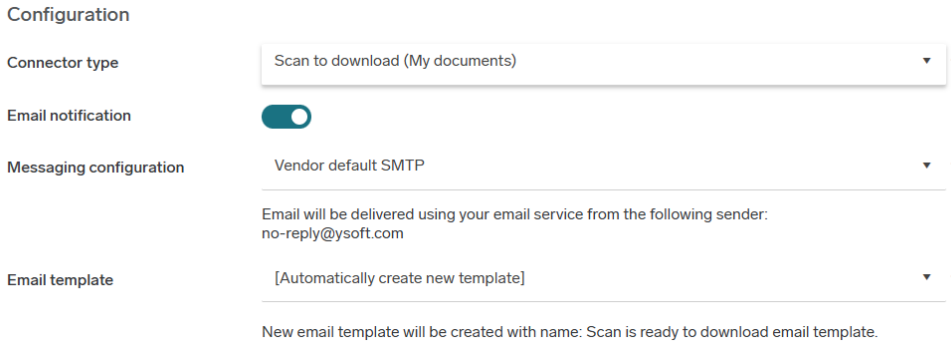
Overview

The Scan to download connector stores scanned files on the server with access restricted to the users who performed the scan. Authentication is required to access and download files from the My documents page (Scans tab) in the SAFEQ Cloud web UI.

Limitations

- Only one "Scan to Download (My Documents)" connector can be configured per account.
- This connector type does not support delivery restrictions.

Connector Configuration



1. Connector type - Select Scan to download (My documents).
2. Email notification - Once the scan is complete, the user receives an email notification containing a link to the My Documents section of the SAFEQ Cloud web UI.
   - Messaging Configuration – If a single SMTP configuration is available, it is automatically preselected. Otherwise, you can select from the available options or create a custom configuration. To set up a custom SMTP messaging configuration, see Messaging.
   - Email Template – The email template includes the notification content, along with a link to the My Documents section of the SAFEQ Cloud web UI.
     - If no template exists, one is automatically created when saving the connector. You can also create a custom template and select it here.
     - By default, this link is represented by the placeholder *{{myDocumentsLinkPlaceholder}}*.
     - The template can be customized in the SAFEQ Cloud web UI under Settings → General Settings → Templates.

When the connector is saved with Email Notification enabled, a "Scan to Download" trigger is automatically created to send notifications upon scanning; if the notification is disabled, the trigger is removed. This trigger can be found in the SAFEQ Cloud web UI under Settings → Rules → Triggers.

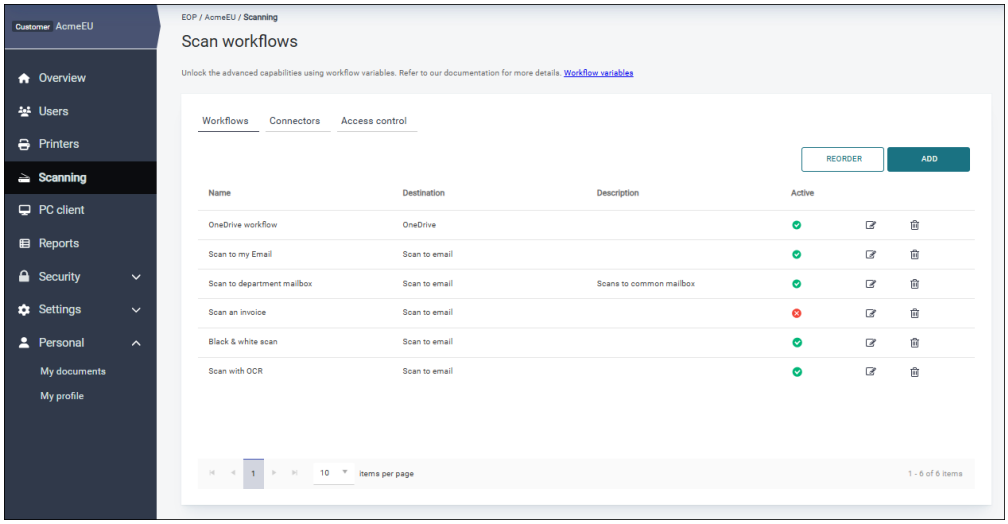
Workflows

Creating and editing a workflow

Log in to SAFEQ Cloud Web UI and go to **Scanning** > **Workflows**.

> You must have *ViewScanWorkflow* permission to access the section. Additionally, you must have the following permissions to create, edit, and delete scan workflows respectively: *CreateScanWorkflow*, *ModifyScanWorkflow*, and *DeleteScanWorkflow*.

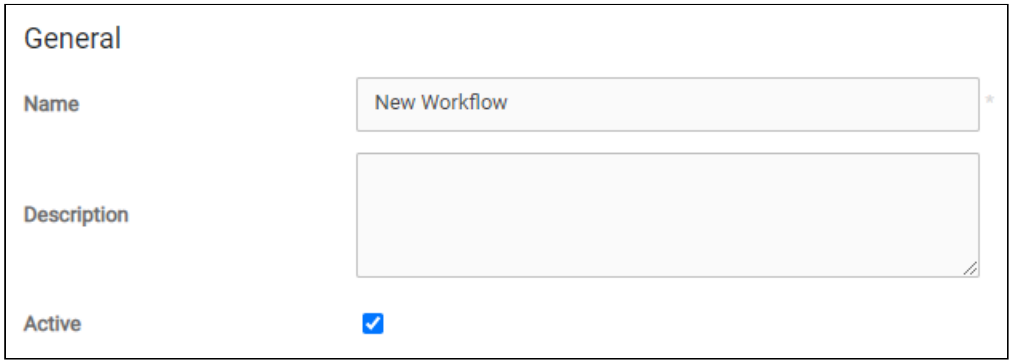
To add a workflow, click **Add**.



To modify a workflow, click the edit icon next to your selected workflow. The form is the same for adding and editing a workflow and consists of several sections with a specific set of fields.

General section

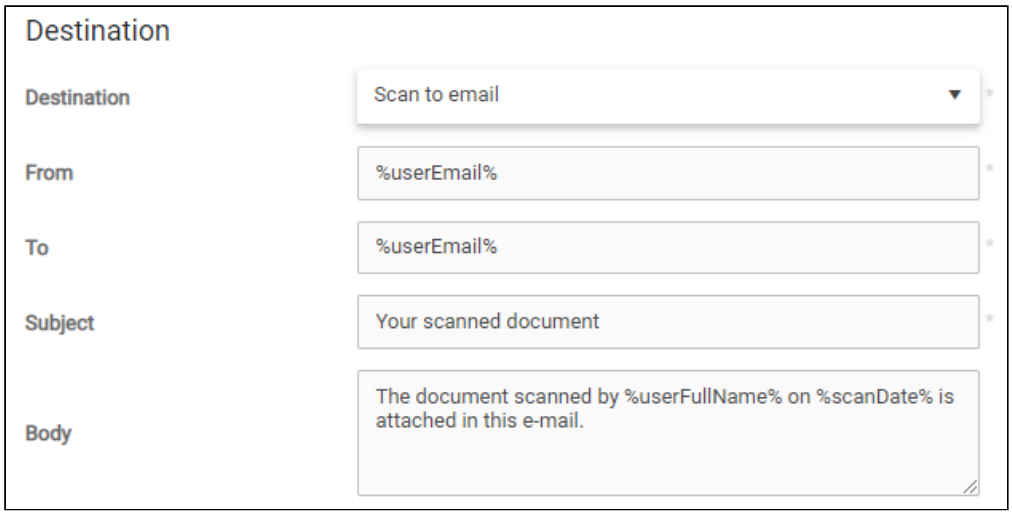
In the **General** section, enter the name and the description of your workflow.



> The **Name** and **Description** fields appear to end users on the terminal. The field "Active" determines, whether the workflow is available on the terminal at all (in addition to how you configured the access rules – see Access rules).

Destination section

In the **Destination** section, select a connector. After selecting a connector, its per-workflow customizable fields will be displayed below. Connectors are managed separately.



In this instance, the **From**, **To**, **Subject,** and **Body** fields are taken over from the selected email connector and represent its customizable parameters. You can use various dynamic placeholders, as described in Workflow variables.

Processing section

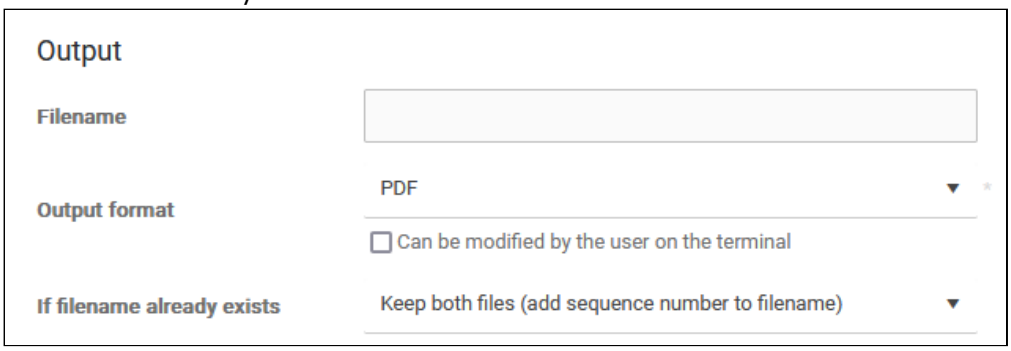
In the **Processing** section, you can enable additional workflow processing. When you enable a processing step, its configurable fields will be displayed. For more information, see Workflow processing steps.

Output section

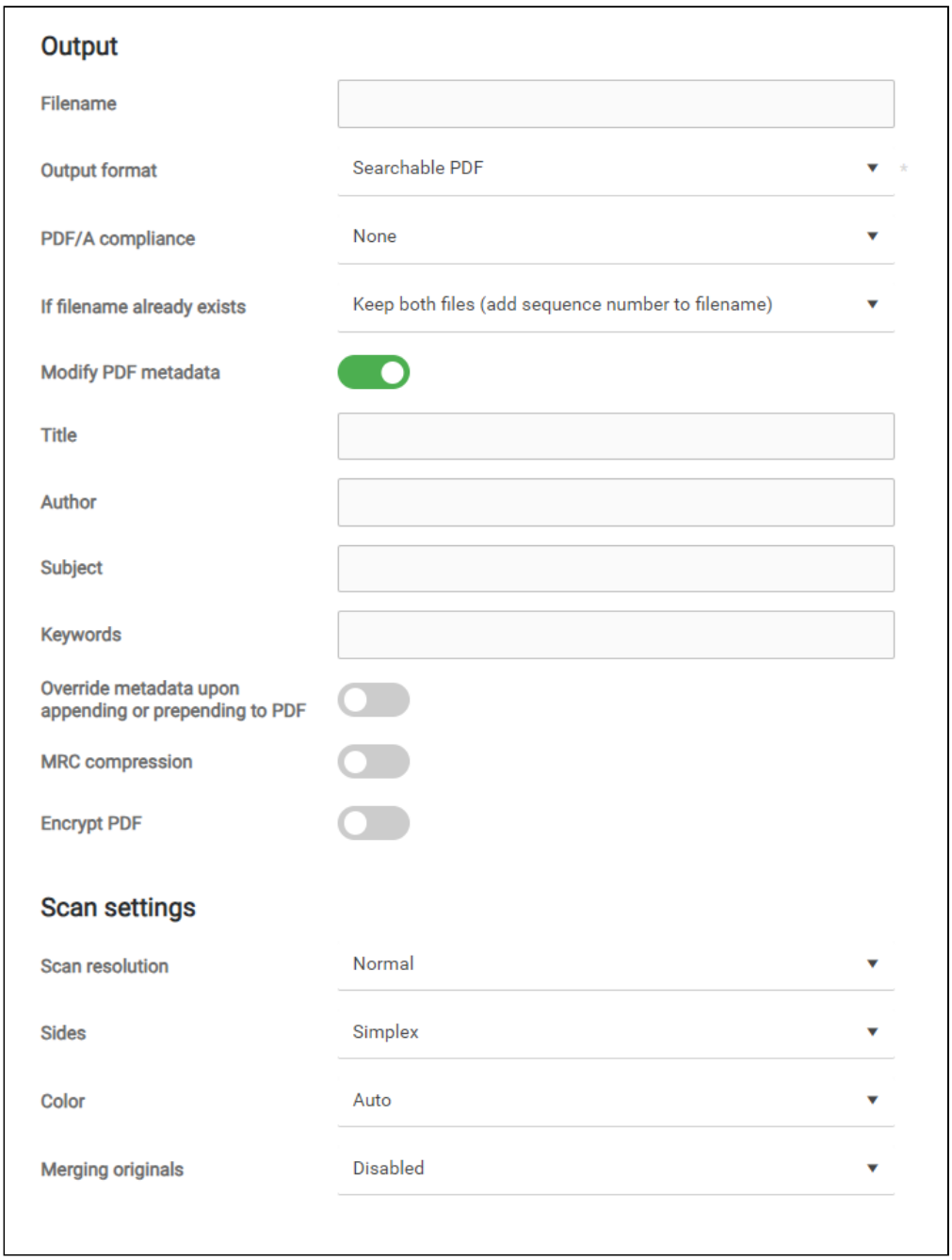
In the **Output** section:

1. Enter the **Filename**.
2. Select the output format. The available formats are:
   - PDF
   - Compact PDF
   - JPEG
   - TIFF
   - Multipage TIFF

3. If you wish to allow the users to change the output format at the MFD before scanning, select Can be modified by the user on the terminal.



4. Choose what happens if the filename already exists in the target directory:
   - Keep both files — A new file will be created with a numeric sequence in the "_#####" format. For example, "filename_00001", "filename_00002", etc. No files will be deleted.
   - Replace original file — The original file will be replaced with a new one.
   - Append to the original file (PDF only)
   - Prepend to the original file (PDF only)
5. When OCR processing is enabled in the Processing section, the available formats change to Searchable PDF, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, RTF, and TXT.
6. If you selected the Searchable PDF format, you will see additional configuration options.



- Modify PDF metadata
  - This option allows you to modify the standard PDF metadata in the searchable PDF fields. If enabled, you can specify the following metadata: **Title**, **Author**, **Subject**, **Keywords**.
  - If appending or prepending a searchable PDF file, you can choose to overwrite the metadata on each append or prepend by enabling the **Override metadata upon appending or prepending to PDF** option.
- MRC compression
  - Enables or disables the MRC compression in a searchable PDF file.

> MRC (Mixed Raster Content) is a special compression technology used to minimize the size of PDF files.

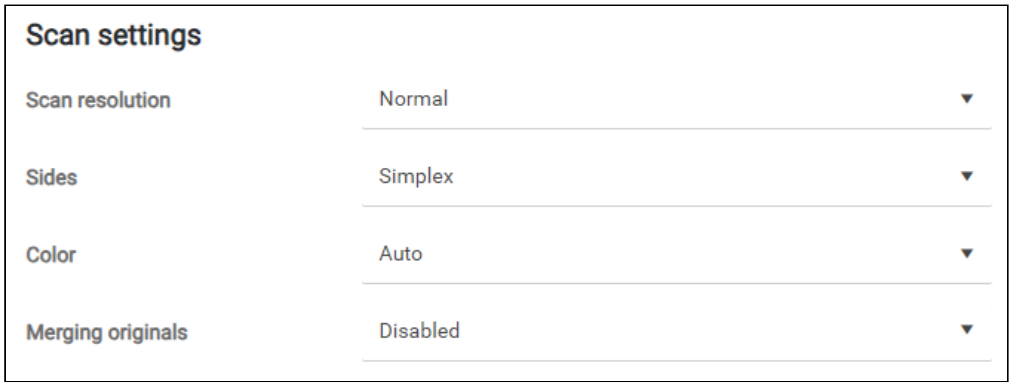
If document image files are excessively large, it's often due to the background, which may account for up to 90% of the file size. This compression technology recognizes the color background and deletes it or compresses it, leaving the text and pictures against a white background. This reduces the PDF file size. Picture objects (diagrams, graphs, logos, photos, drawings, stamps, signatures, etc.) are also slightly compressed, but only to an extent that does not lower the quality. Therefore, we recommend using this option if you don't need background in the scanned documents.

- The supported **PDF/A compliance** types are:
  - PDF/a-1a
  - PDF/a-1b
  - PDF/a-2a
  - PDF/a-2u
  - PDF/a-3a
  - PDF/a-3u

  Due to a limitation in third-party software, the options **"Append to the original file (PDF only)"** and **"Prepend to the original file (PDF only)"** do not preserve the selected PDF compliance level.
- The supported **Encryption strengths** are:
  - Low - 40 bit
  - High -128 bit
  - High - AES 128bit

Scan settings section

In the **Scan settings** section, you can configure the general scan settings.



- **Scan resolution** — Select scan resolution. The DPI values depend on the MFD vendor. See the table below.
- **Sides** — Choose whether only one side or both sides will be scanned.
- **Color** — Select the color of the scanned document.
- **Merging originals** — Choose whether the documents will be combined together.

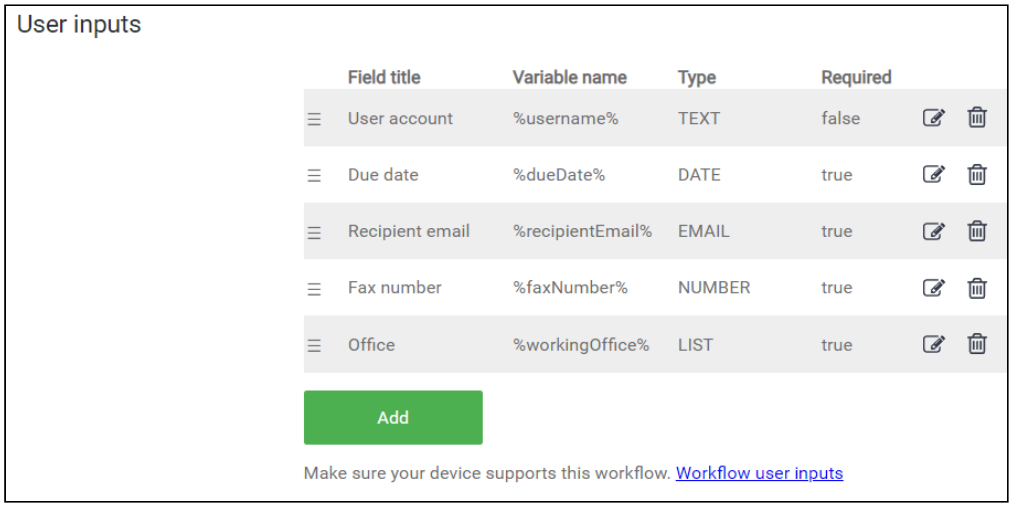
Scan resolution DPI values:

Scan resolution in Scan settings	Konica Minolta*	Ricoh*	FUJIFILM BI*	HP Workpath*	Sharp
Low	200*200	100*100	200*200	75*75	100*100
Normal	200*200	200*200	200*200	150*150	200*200
Fine	300*300	300*300	300*300	300*300	300*300
High	400*400	400*400	400*400	500*500	400*400
Super	600*600	600*600	600*600	600*600	600*600

**Pure cloud terminal*

User inputs section

In the **User inputs** section, you can define scan metadata that will be collected at the MFD's terminal in the form of user input. Input values supplied by terminal users are saved in user input workflow variables.



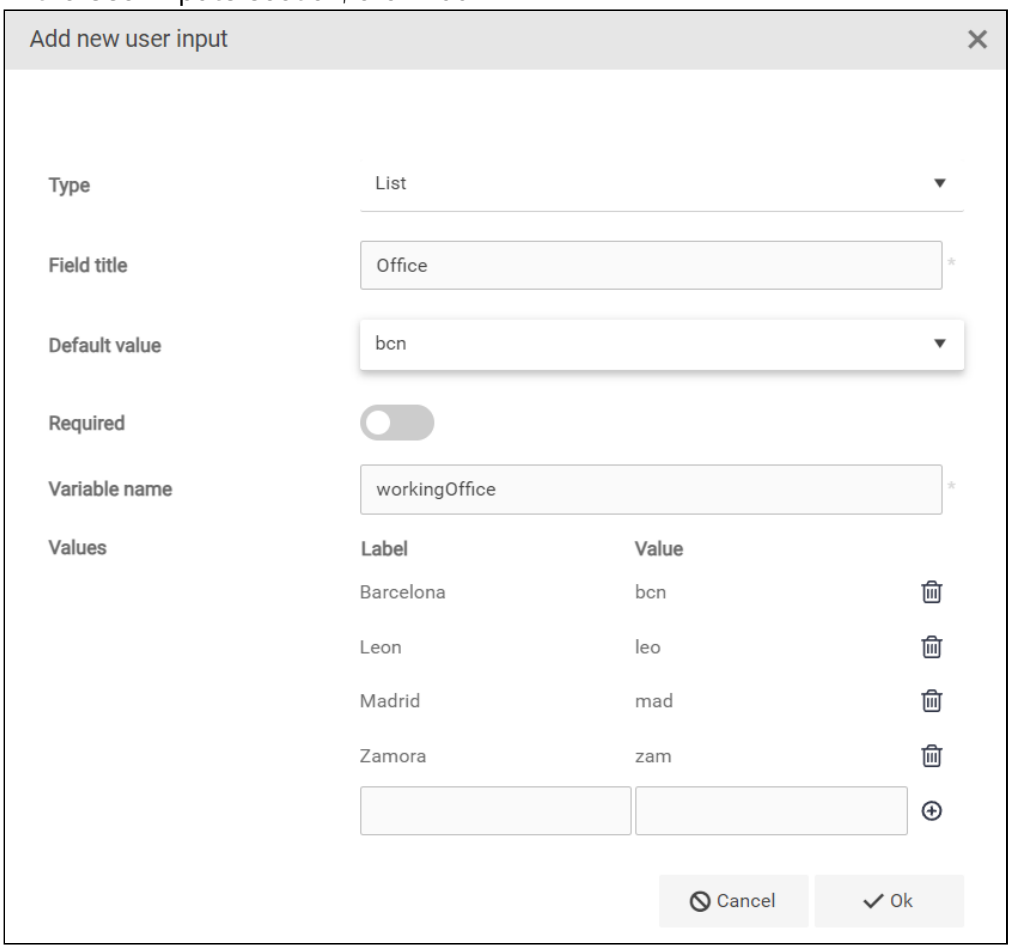
Reorder user inputs using the ≡ icons on the left side.

Remove user inputs by clicking the trash icon beside the user input.

Edit user inputs by clicking the edit icon beside the user input. The form is the same for adding and editing a user input.

Create a new user input:

1. In the **User inputs** section, click **Add**.



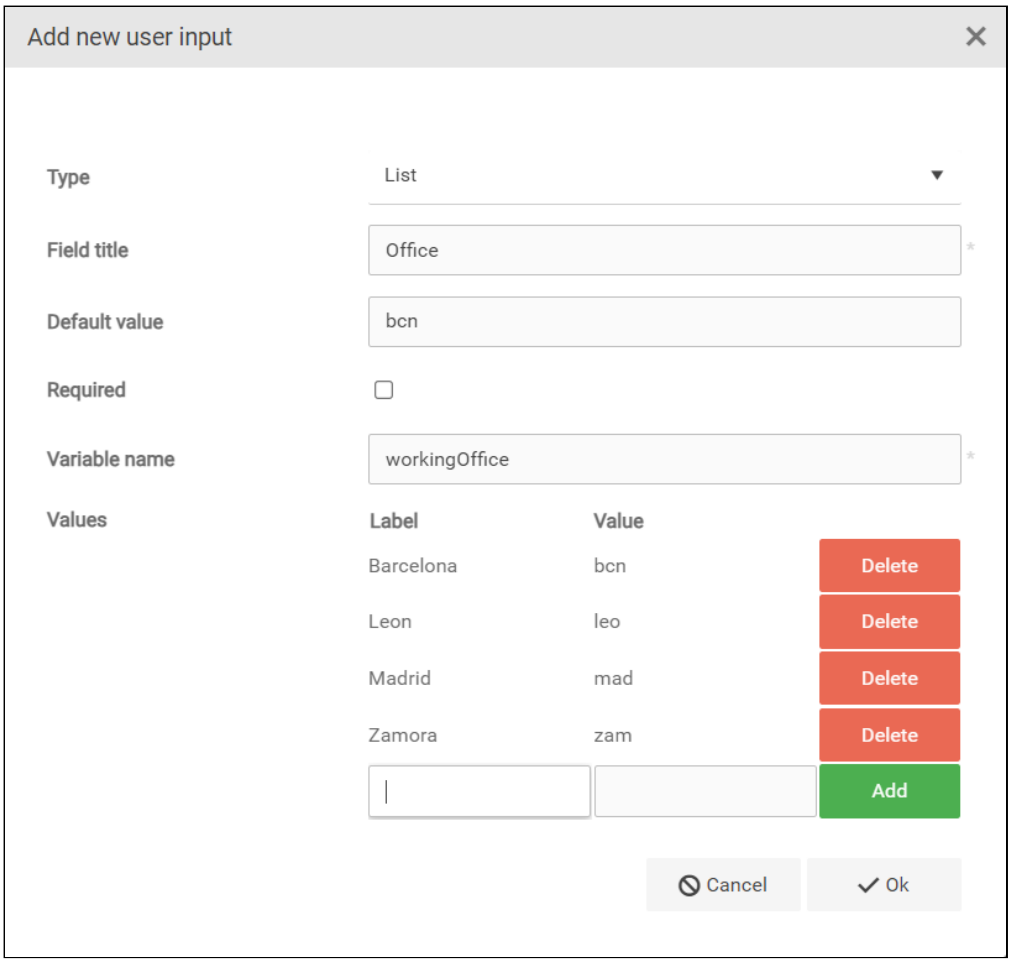
2. In the **Add new user input** popup window, select **Type** from the drop-down menu:
   - **Text** – Create a field, where users can enter any text.
   - **Number** – Create a field, where users can enter whole positive numbers.
   - **Date** – The expected format is YYYYMMDD (e.g., "20160719" for July 19, 2016)
   - **Email** – Create a field, where users can enter any text in email address format.

     The "SearchUser" permission is required in order to be able to search email addresses directly on the MFD's terminal. Without this permission, the result is empty.

     The result is limited to 40 records per authentication provider.

     Only users who have interacted with the system at some point (for example, by authenticating through the PC client) will be listed in the result.
   - **List** – Manually enter values that will be available as a list on the MDF's terminal.
3. Enter **Field title**.
4. Set **Default value**.
5. Check **Required** if the user input is necessary to start scanning.

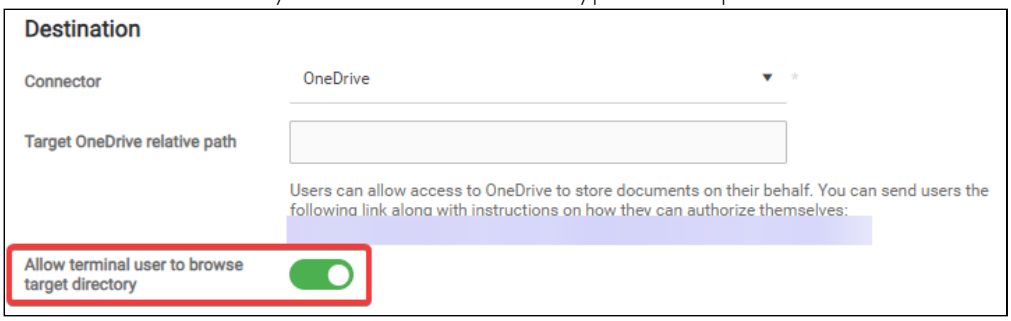
6. Set **Variable name**.
7. If you selected the **List** type, create a list of values. For each value, enter the label and the value, and then click **Add**. Click **Delete** to remove a value from the list.



8. Click **OK** to save the user input.

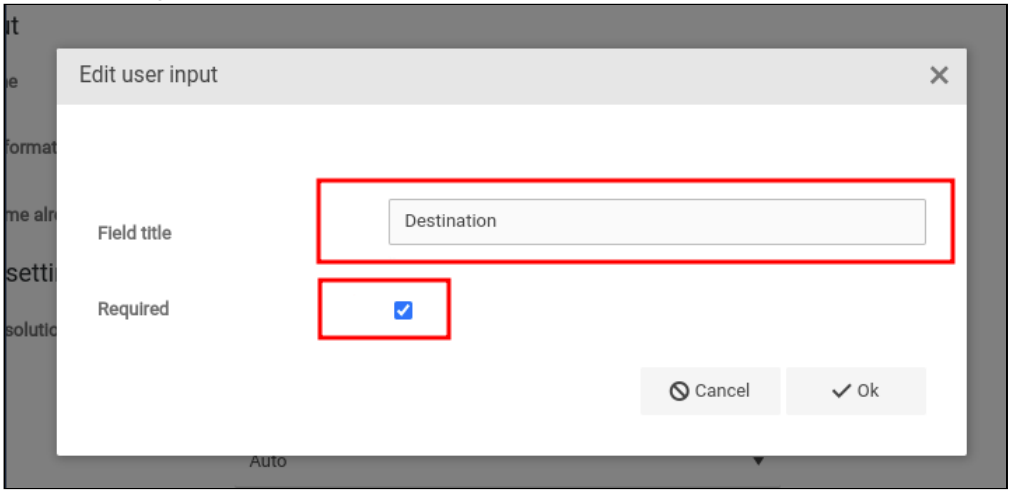
Allow terminal user to select the destination folder

1. If you wish the end users to be able to choose the destination folder in a scan workflow, select the **Allow terminal user to browse target directory** option in the **Destination** section. This will automatically create the **BROWSE** type user input field.



2. Once the **BROWSE** input field is created, you can edit or delete it like any other user input field. To edit it, click the edit icon.

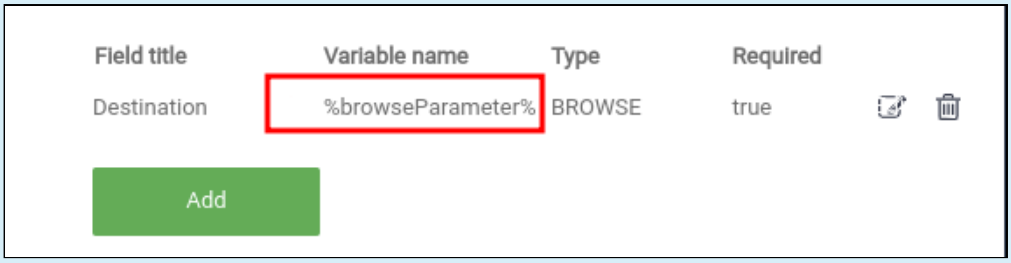
3. A new dialog window will be displayed.



- **Field title** – The title of the user input field that will appear in the workflow detail on the terminal. Capture variables may be used.
- **Required** – If selected, the user must select a destination folder before they scan a document. Before allowing destination folder selection, make sure it contains browsable subfolders. The user will not be able to select the root of the target directory.

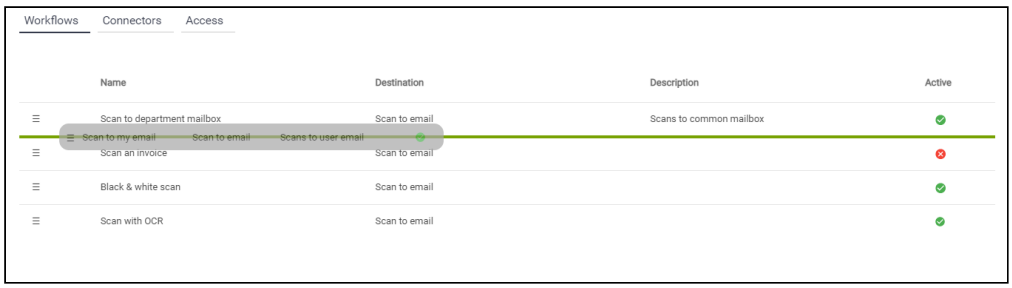
4. Click **Ok** to save changes.

For the **BROWSE** type user input field, the variable name is always %browseParameter%.



Changing the order of workflows

To alter the order in which workflows are presented on terminals and in the SAFEQ Cloud Web UI, click **Reorder** in the list of workflows. This will switch the UI to re-ordering mode, where paging is disabled and individual workflows can be dragged & dropped in the desired position.



You must have the *ModifyScanWorkflow* permission to reorder workflows.

Deleting a workflow

You can delete a workflow directly from the workflow list by clicking the delete icon, or by clicking **Delete** in the workflow detail. To do this, you must have the *DeleteScanWorkflow* permission

Deleting a workflow will also remove all access rules that were configured for it.

Workflow variables

Use variables to customize your workflows further by allowing dynamic information to be included in the workflow process. For example, if a workflow involves scanning documents and sending them via email, you can use variables such as %userEmail% and %userFullName% to automatically populate the recipient fields with the email and name of the user who initiated the scan. Similarly, you can use variables such as %deviceName% and %deviceID% to identify the device where the scan was made, which can be useful for tracking purposes.

In addition, you can use variables such as %scanDate% and %scanTime% to include the date and time of the scan in the file name or metadata of the scanned document. This can help with the organization and retrieval of scanned documents.

Variables start with the '%' character followed by a variable name (no spaces allowed) and end with the '%' character, e.g. %userEmail%, %userFullName%, etc.

Variables are case-sensitive. If the variable name does not match, the variable is not replaced by its value.

Name	Usage
%userUsername%	The username of the user who made a scan at the terminal.
%userProviderID%	The authentication provider ID of the user who made a scan at the terminal.
%userEmail%	The email of the terminal user who made a scan.

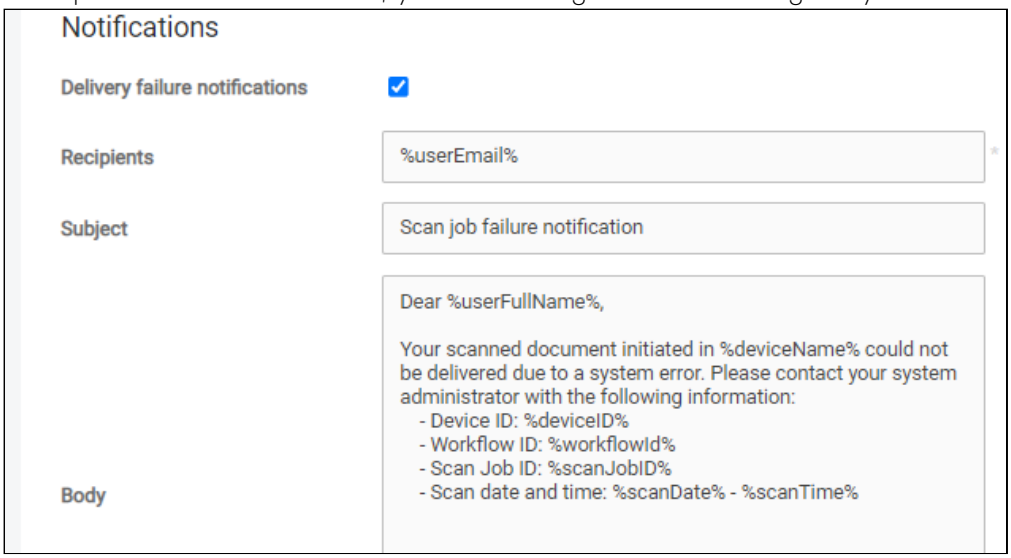
Name	Usage
%userFullName%	The full name of the terminal user who made a scan.
%userDepartment%	The department of the terminal user who made a scan.
%userHome%	The home folder of the terminal user who made a scan.
%deviceName%	The name of the device where a scan was made.
%deviceID%	The ID of the device where a scan was made.
%deviceDescription%	The description of the device where a scan was made.
%scanDate%	The local date on SAFEQ Cloud server at the time of a scan in the format yyyy-MM-dd, e.g., '2022-12-21' for December 21, 2022.
%scanTime%	The local time on SAFEQ Cloud server at the time of a scan in format *HH-mm-ss-fff*, e.g., '12-15-00-000' for quarter past twelve.
%workflowID%	The ID of the workflow used to make the scan.
%workflowName%	The name of the workflow used to make the scan.
%scanJobID%	(available only during scan workflow execution) The unique ID of the scan job instance. This identifier of the scan job is visible also in the log files.

If the information which should be replaced in the variable is not configured, it will use an empty value instead. For example, if %userFullName% is not set, the result of the string "User full name is %userFullName%" will be "User full name is ".

In general, you can use workflow variables anywhere within the workflows and connectors configuration, except for the Workflow name. For example:

- In the filename of the delivered document. Example: "*scan-%userEmail%-%scanDate%*" would result in "*john.doe@example.com-2012-12-21*")
- In the root or target paths where the document will be delivered. Example: "*acme/%userDepartment%/%workflowName%*" would result in "*acme/Human Resources/Scan a CV*")

- In the notifications sent to the user when there is a status change in the workflow processing. Example: if the workflow fails, you can configure the following body in the notification:



Workflow error codes

When a scan workflow fails, the admin will receive an email notification. The email may contain one of the following error codes:

Error code	Error message
WPS-BARCODE-9999	Barcode recognition has failed.
WPS-DOCUMENT_SEPARATION-9999	Document separation has failed.
WPS-EXTERNAL-9999	External processing step has failed.
WPS-EXTERNAL-0002	External processing step command finished with a nonzero exit code. Contact your vendor to get the API exit code from the logs.
WPS-HIGHLIGHT-9999	Recognition of highlighted text has failed.
WPS-OCR-9999	OCR processing has failed.
WPS-REDACT-9999	Text redaction has failed.

Error code	Error message
WPS-ZONAL_OCR-9999	Zonal OCR has failed.
WPS-BOX-9999	Upload of scan files to Box has failed.
WPS-DROPBOX-9999	Upload of scan files to Dropbox has failed.
WPS-EMAIL-9999	The sending of scan files to email has failed.
WPS-EMAIL-0001	The client is not authenticated to send e-mails.
WPS-EMAIL-0002	The size of the scan job exceeded the size limit of the SMTP server. Check the maximum scan job size setting in the e-mail connector.
WPS-EMAIL-0003	The user does not have an email address set in their profile.
WPS-EMAIL-0004	Connection refused. Check that the SMTP server is running and is set up correctly.
WPS-EMAIL-0005	The concurrent connections limit has been exceeded.
WPS-EXCHANGE-9999	The sending of scan files to Exchange has failed.
WPS-EXTENSION-9999	An error occurred on the extension connector.
WPS-HPRM-9999	An error occurred on the HPE Records Manager connector.
WPS-ONEDRIVE_BUSINESS-9999	The upload of scan files to OneDrive has failed.
WPS-ONEDRIVE_BUSINESS_OAUTH2-9999	The upload of scan files to OneDrive has failed.

Error code	Error message
WPS-ONEDRIVE_BUSINESS_OAUTH2-0001	The user did not authorize the OneDrive storage.
WPS-SCRIPT-9999	An error occurred on the Script connector.
WPS-SHAREPOINT_ONLINE-9999	The upload of scan files to SharePoint Online has failed.
WPS-SHAREPOINT_ONLINE_OAUTH2-9999	The upload of scan files to SharePoint Online has failed.
WPS-SHAREPOINT_ONLINE_OAUTH2-0001	The user did not authorize the SharePoint storage.
WPS-SHAREPOINT_ONLINE_OAUTH2-0003	SharePoint site was not found. Check the site name in the SharePoint connector settings.
WPS-SHAREPOINT_ONLINE_OAUTH2-0004	SharePoint library was not found. Check the library name in the scan workflow settings.
WPS-CORE-9999	The processing of scan files has failed.
WPS-RESTRICTION-0001	The scan job size limit has been reached.
SQ-WPS-9999	SAFEQ Cloud was not able to reach the WPS service.

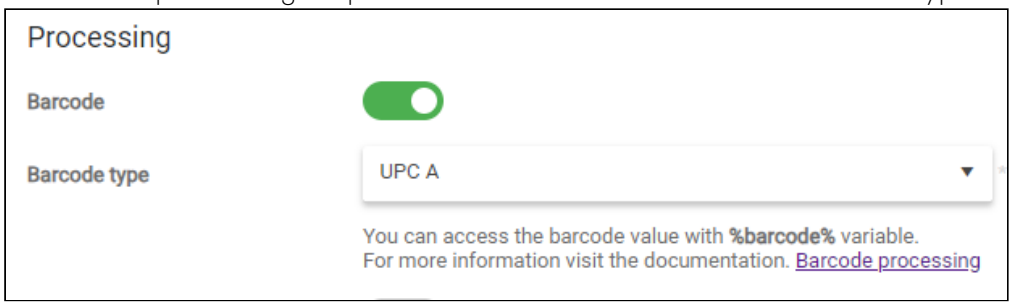
Workflow processing steps

Processing steps can transform (e.g., process images into a searchable PDF) or extract data from scanned documents into variables. Each of the processing steps can be enabled and configured independently.

You may enable or disable all the available processing steps in any workflow.

Barcode processing step

Enable this processing step to find barcodes of the selected barcode type.



Barcode type

Determines which barcode type should be identified and extracted from a document. The supported types are:

- UPC A
- UPC E
- EAN 8
- EAN 13
- Code 39
- Code 93
- Code 128
- Codabar
- ITF
- RSS 14
- RSS Expanded
- Any 1D barcode – the barcode in a document can be any of the supported (above-listed) 1D barcode types.
- Aztec
- Data Matrix
- Maxicode
- PDF 417
- QR Code

Barcode variables

First occurrence of the barcode – The barcode step reads the barcode value and saves it into the %barcode% variable. If multiple barcodes of the selected type are found, the leftmost and uppermost barcode value is used. If no barcode is found, the %barcode% variable is set to an empty string.

- Special characters "/\<>:"|?*~#%{}&" are removed to prevent unsafe user input.
- Example:
  - %barcode% = ABCD1234

Multiple barcodes – Variables %barcode<X>% contain each barcode value with X starting from 1. If multiple barcodes are found, they are sorted from upper-left to bottom-right.

- Special characters "/\<>:"|?*~#%{}&" are removed to prevent unsafe user input.
- Example:
  - %barcode1% = ABCD1234
  - %barcode2% = C--TEMP

Non-sanitized multiple barcodes – Variables %barcodeInsecure<X>% contain each unmodified barcode value with X starting from 1. If multiple barcodes are found, they are sorted from upper-left to bottom-right.

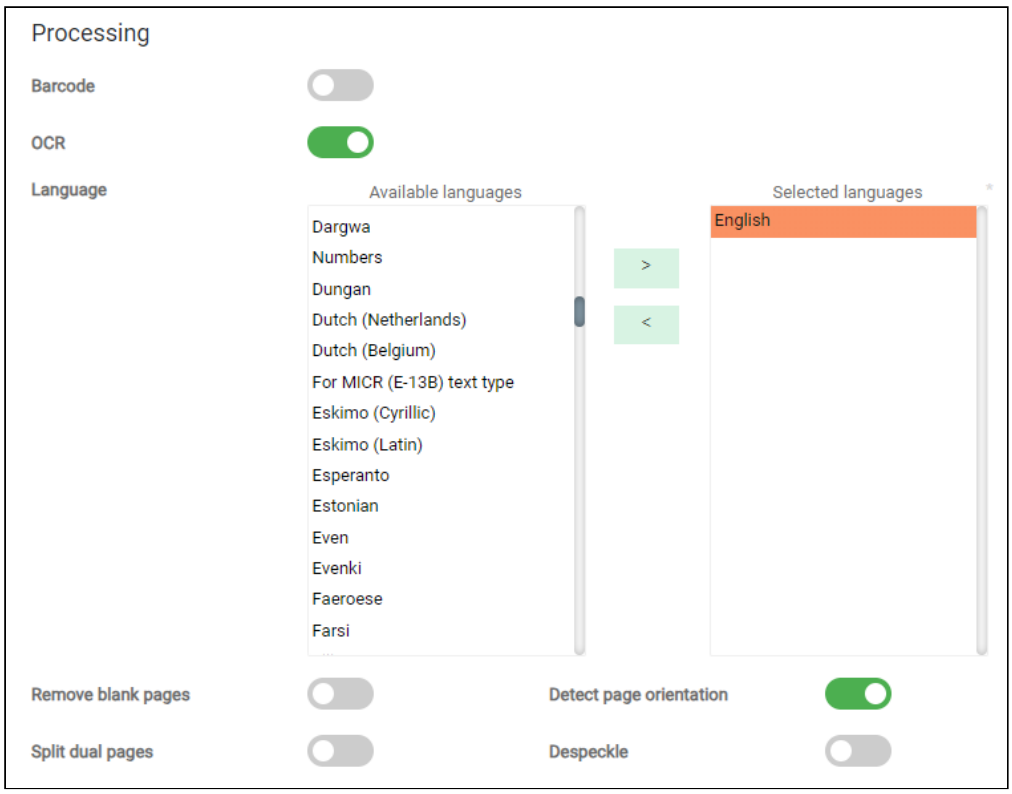
- The value may contain unsafe user input.
- Example:
  - %barcodeInsecure1% = ABCD1234
  - %barcodeInsecure2% = C:\TEMP

JSON variables – Variables %barcode_<JSON key path>% contain barcode JSON values with a key path using dot notation replaced by an underscore character.

- Special characters "/\<>:"|?*~#%{}&" are removed to prevent unsafe user input.
- Example:
  - %barcode_store_book_0_title% = My Book
  - %barcode_store_book_0_price% = $10.00

OCR processing step

Enable the OCR processing step to analyze text documents, recognize and extract document text and formatting, and save the result to a file of a selected output format. The OCR step recognizes only the common typographic type of text.



- Language – Document languages. OCR processing requires the language setting to recognize the document's text correctly. You can select multiple languages.

  See the *Supported Languages* section for the list of languages recognized by the OCR processing step.

  The accuracy of OCR depends on many factors, such as the quality of the printed document, scanner quality, and text size. Therefore, it is never 100%, even with correctly configured document language. To get the best results out of OCR, we recommend you to use the following scan resolution settings:

  - For regular texts (font size 8-10 points), use 300 dpi resolution for OCR (in most cases, represented by the "Fine" setting) as the OCR technologies are tuned for that resolution.
  - For smaller font text sizes (8 points or smaller), use 400-600 dpi resolution.
  - Low image quality (e.g., low resolution) may decrease quality and speed as uncertainty in the character picture produces more recognition variants to process.

- Remove blank pages – removes blank pages from the scanned document. The blank page detection algorithm is heuristic. Therefore, its results cannot always be accurate. There are predefined thresholds used for blank page detection. The page is not considered blank when any value of the following criteria is exceeded:
  - The maximum number of letters belonging to the recognition languages is five.
  - The maximum percentage of black areas on a page is one.
  - The maximum number of objects found on a page is 20.
  - If a page contains a barcode, it is not considered blank.

If all pages in a scan job are evaluated as blank, the job will be processed without the option to remove them. Therefore all scanned pages will be included in the resulting document.

- Detect page orientation – detects each page's orientation in the document and rotates upside-down pages to correct the orientation.
- Split dual images – splits dual pages (e.g., when scanning double pages of a book) into two pages in the resulting document.
- Despeckle – cleans the noise in the scanned document. This may impact the speed and performance of the OCR engine.

Supported languages

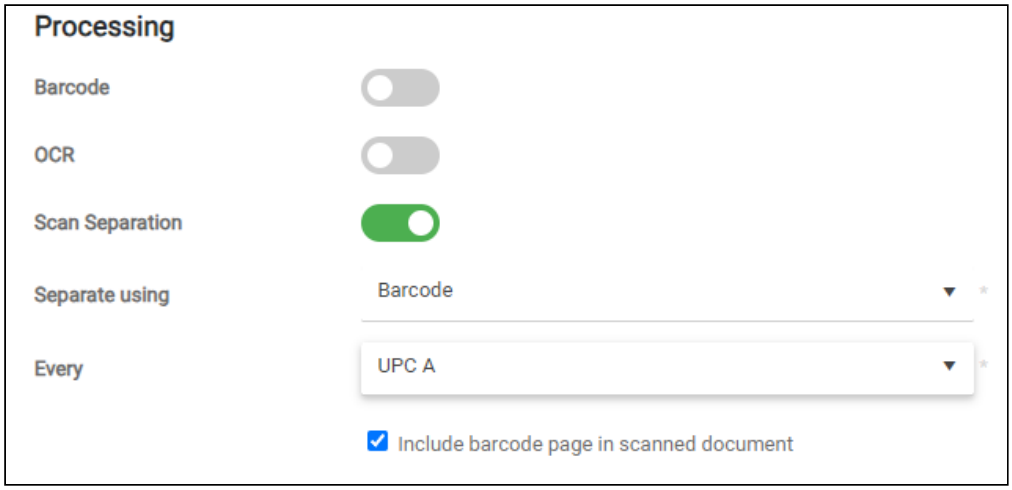
The OCR processing step supports the recognition of the following OCR languages:

- Languages with dictionary support
  - Latin, Cyrillic, Greek or Armenian characters, for which the FineReader Engine provides dictionary support: Armenian (Eastern, Western, Grabar), Bashkir, Bulgarian, Catalan, Croatian, Czech, Danish, Dutch (Netherlands and Belgium), English, Estonian, Finnish, French, German (new and old spelling), Greek, Hungarian, Italian, Indonesian, Latvian, Lithuanian, Norwegian (Nynorsk and Bokmal), Polish, Portuguese (Portugal and Brazil), Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Tatar, Turkish, and Ukrainian.
  - Japanese, Korean, and Hangul with dictionary support, Chinese (PRC and Taiwan).
  - Japanese Modern (Japanese texts which may include Latin or Greek letters)
  - Thai with dictionary support.
  - Hebrew with dictionary support, Yiddish.
  - Arabic with dictionary support, Farsi.
  - Latin, Azerbaijani (Latin), and Russian (old spelling) with dictionary support.
- Additional languages
  - Latin, Cyrillic, or Greek characters: Abkhaz, Adyghian, Afrikaans, Agul, Albanian, Altaic, Avar, Aymara, Azerbaijani (Cyrillic), Azerbaijani (Latin), Bangla, Basque, Belarusian, Bemba, Blackfoot, Breton, Bugotu, Burmese, Buryat, Cebuano, Chamorro, Chechen, Chukchee, Chuvash, Congo, Corsican, Crimean Tatar, Crow, Dakota, Dargwa, Dungan, Eskimo (Cyrillic), Eskimo (Latin), Even, Evenki, Faeroese, Fijian, Frisian, Friulian, Gagauz, Galician, Ganda, Georgian, German (Luxemburg), Guarani, Hani, Hausa, Hawaiian, Icelandic, Ingush, Irish, Jingpo, Kabardian, Kalmyk, Karachay-balkar, Karakalpak, Kasub, Kawa, Kazakh, Khakass, Khanty, Kikuyu, Kirghiz, Koryak, Kpelle, Kumyk, Kurdish, Lak, Latin, Lezgi, Luba, Macedonian, Malagasy, Malay, Malinke, Maltese, Mansy, Maori, Mari, Maya, Miao, Minangkabau, Mohawk, Moldavian, Mongol, Mordvin, Nahuatl, Nenets, Nivkh, Nogay, Nyanja, Ojibway, Ossetian, Papiamento, Provencal, Quechua, Rhaeto-Romanic, Romany, Rundi, Russian (old spelling), Rwanda, Sami (Lappish), Samoan, Scottish Gaelic, Selkup, Serbian (Cyrillic), Serbian (Latin), Shona, Somali, Sorbian, Sotho, Sunda, Swahili, Swazi, Tabasaran, Tagalog, Tahitian, Tajik, Turkmen (Latin), Tok Pisin, Tongan, Tswana, Tun, Turkmen, Tuvinian, Udmurt, Uigur (Cyrillic), Uigur (Latin), Uzbek (Cyrillic), Uzbek (Latin), Vietnamese, Welsh, Wolof, Xhosa, Yakut, Zapotec, Zulu.
- Artificial languages

    - Esperanto, Interlingua, Ido, and Occidental.
- Programming languages
    - Basic, C/C++, COBOL, Fortran, JAVA, and Pascal.
- Simple chemical formulas
- Mathematical formulas
- Digits

Scan separation processing step

Enable this processing step to split a batch scan into multiple documents.

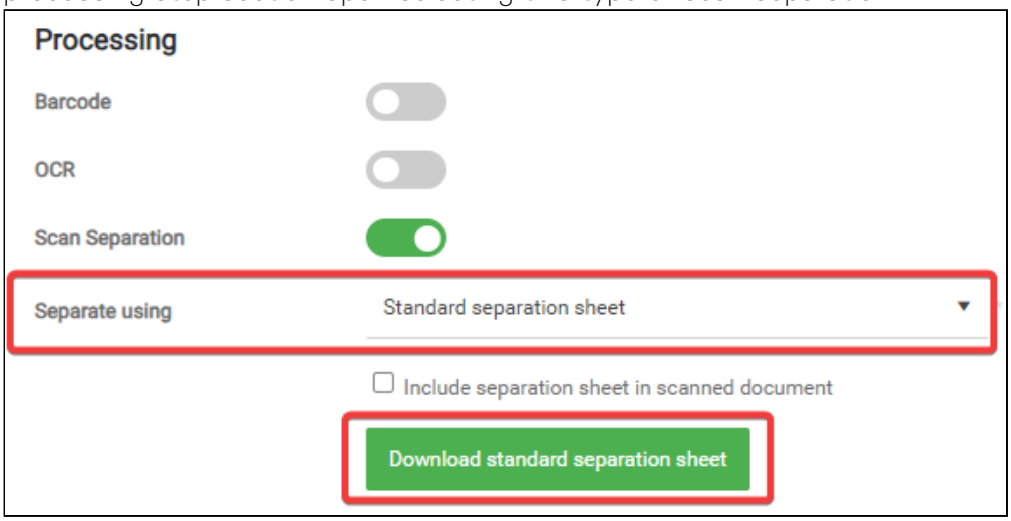


You can separate the scan using the following options:

- Page count – A new document starts after the number of specified pages. The number of specified pages can be a number or a variable.
- Barcode – A new document starts when a barcode of the specified type is detected in the scan. The value of the corresponding barcode is stored in the %separationBarcode% variable. Pages with these barcodes are included in the scan jobs by default. You can disable this by leaving the Include barcode page in scanned document option blank.
  Barcode types:
    - UPC A
    - UPC E
    - EAN 8
    - EAN 13
    - Code 39
    - Code 93
    - Code 128
    - Codabar
    - ITF
    - RSS 14
    - RSS Expanded

- Any 1D barcode
- Aztec
- Data Matrix
- Maxicode
- PDF 417
- QR Code

- Standard separation sheet – A new document starts when the standard separation sheet is detected in the scan. You can download the standard separation sheet in the Scan Separation processing step section upon selecting this type of scan separation.



By default, the standard separation sheet is not included in the scan job. You can enable this by selecting the Include separation sheet in scanned document option.

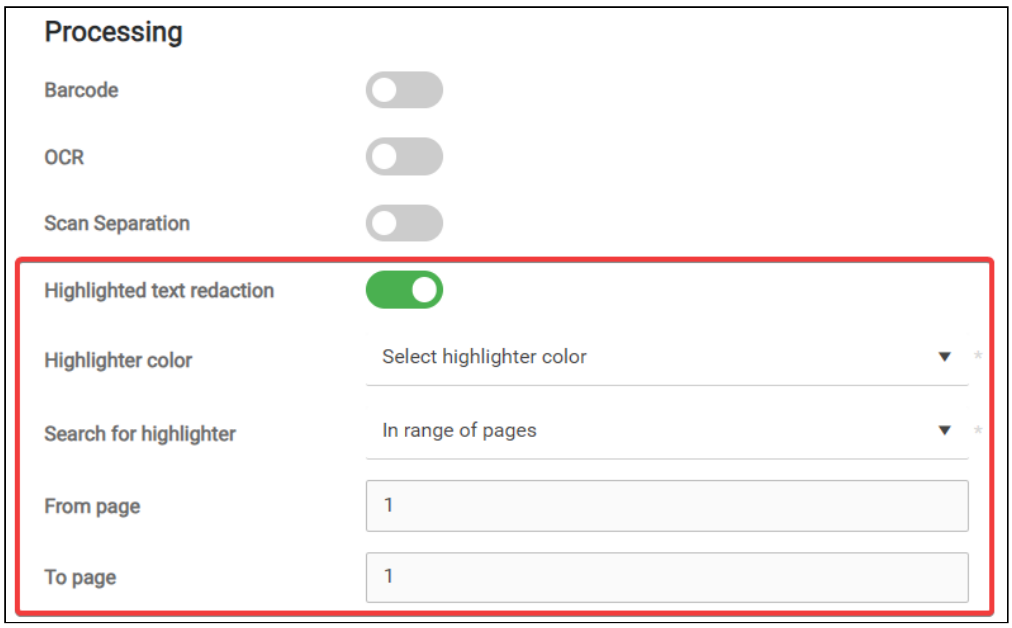
Highlighter redaction processing step

Use the highlighter redaction step to enable the end users to redact areas in a scanned document. The users only need to highlight these areas with a highlighter. In the scanned document, these will be overlaid with black.

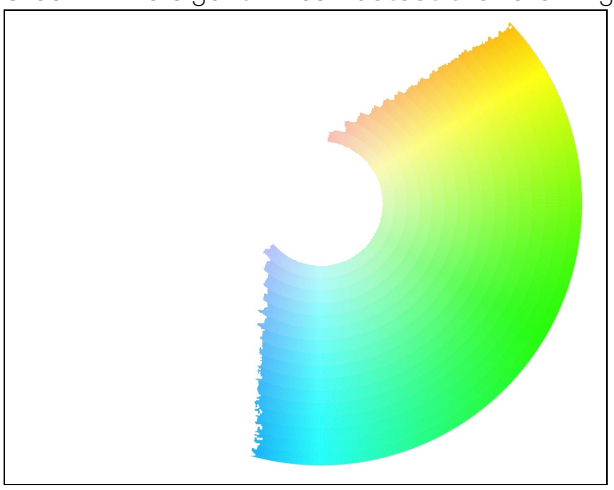
The highlighter redaction works in black and white documents only.

Do not combine multiple highlighter colors in one document.

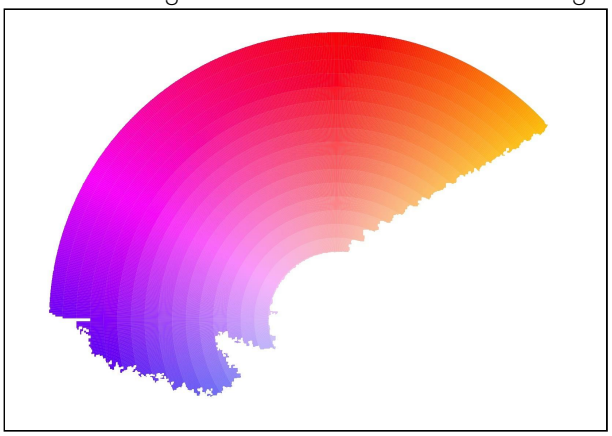
Avoid using orange highlighters.



1. Enable **Highlighted text redaction**.
2. Select the **Highlighter color**. Areas highlighted with this color will be redacted.
   a. Green – The algorithm can detect the following color range (approximately).



   b. Red – The algorithm can detect the following color range (approximately).



3. In Search for highlighter, select whether to search in the whole document or in a range of pages.
    a. From – The lower limit of the page range. If empty, the range starts on the first scanned page.
    b. To – The upper limit of the page range. If empty, the range ends on the last scanned page.

Recommendations

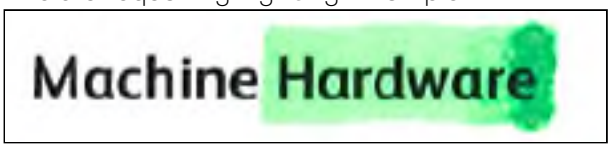
- The optimal resolution for highlighter redaction is 300 DPI. Higher DPI settings may have a negative impact on the performance.
- Use the lowest compression settings on MFD. Redaction in highly compressed files is not recommended. Make sure you adjust your MFD settings before redacting.

How to highlight the text correctly

- Avoid using an orange highlighter. It is on the border between green and red (see the above highlight ranges), therefore the algorithm is unable to process it.
- Use lighter shades of highlighter. Dark colors might make the text unrecognizable.
- Make sure that the highlight covers the whole word or region you need to redact in the text.
    - Example of correct usage:

    - Examples of incorrect usage:

- Avoid unequal highlighting. Example:



Access rules

In order for users to be able to see and execute a scan workflow on a terminal, you must configure their access. By default nobody has access.

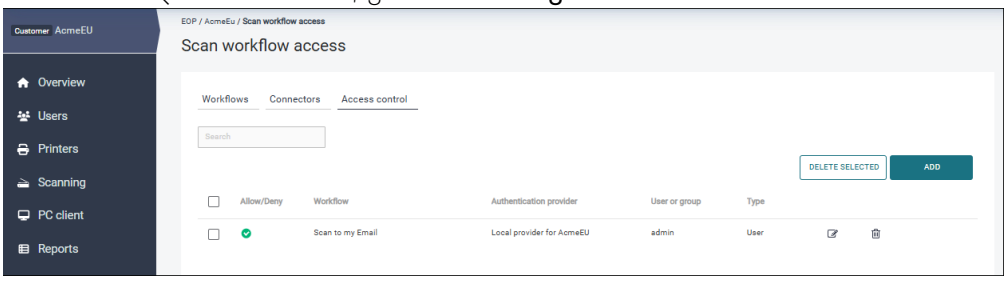
Types of access rules

Access to each individual workflow can be configured via rules on a group or user basis:

- Allow – the given user/group has access to the workflow.
- Deny – the given user/group is denied access to the workflow.

Configuring access rules

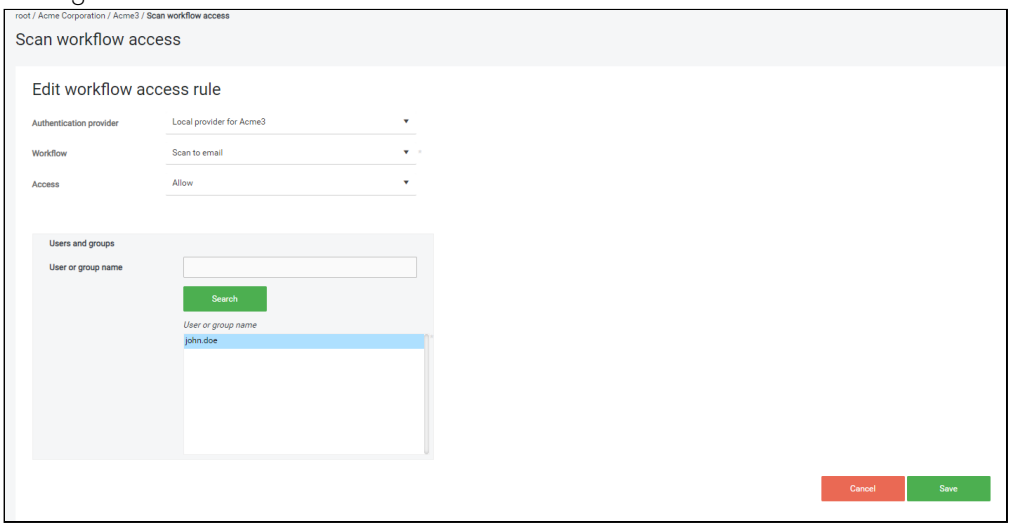
1. In the SAFEQ Cloud Web UI, go to **Scanning** > **Access control**.



2. To create a new access rule, click **Add**.

> You must have both the *ViewScanWorkflow* and *ViewScanWorkflowAccessRule* permissions to access the section, and at least *CreateScanWorkflowAccessRule* permission to create an access rule.

3. Configure the access rule:



- **Authentication provider** – choose the provider which contains the target users or groups.
- **Workflow** – scan workflow for which the access should be granted/denied.
- **Access** – choose the type of rule to create for the target users or groups.
- **User or group name** – full-text search under the given authentication provider. If you leave the search field blank, all users and groups from the selected provider will be listed.
  In the selection box, either one or multiple users & groups can be selected via standard selection methods (mouse drag, shift+click, ctrl + click).

4. Click **Save**. If you selected multiple users or groups, multiple access rules will be created after clicking **Save**.

Effective workflow access evaluation

To determine whether a user has access to a workflow (and therefore can see it on the terminal and execute it), the system is evaluating a combination of all configured rules that apply to the given workflow and target the actual user + any group, that the user is a member of.

Rules are evaluated with the following priority:

- Rules that target the user explicitly have higher priority than rules that target a group containing this user
- Rules that deny access have higher priority than rules that allow access on the same level. For example, deny rule for a group is stronger than allow rule for a group, but it can be overruled by a user-explicit allow rule.

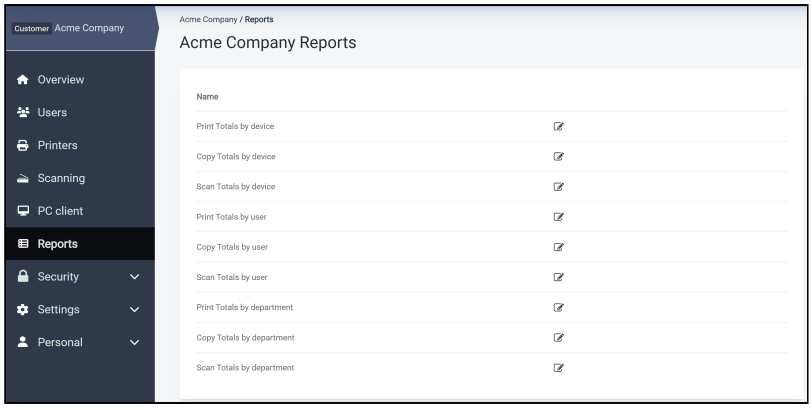
Availability of the workflow for a user is also affected by the "active status" of the workflow itself – even if a user has access to it, inactive workflows aren't shown on the terminal.

8.1.5 REPORTS

In the SAFEQ Cloud Web UI navigation menu, click **Reports**.

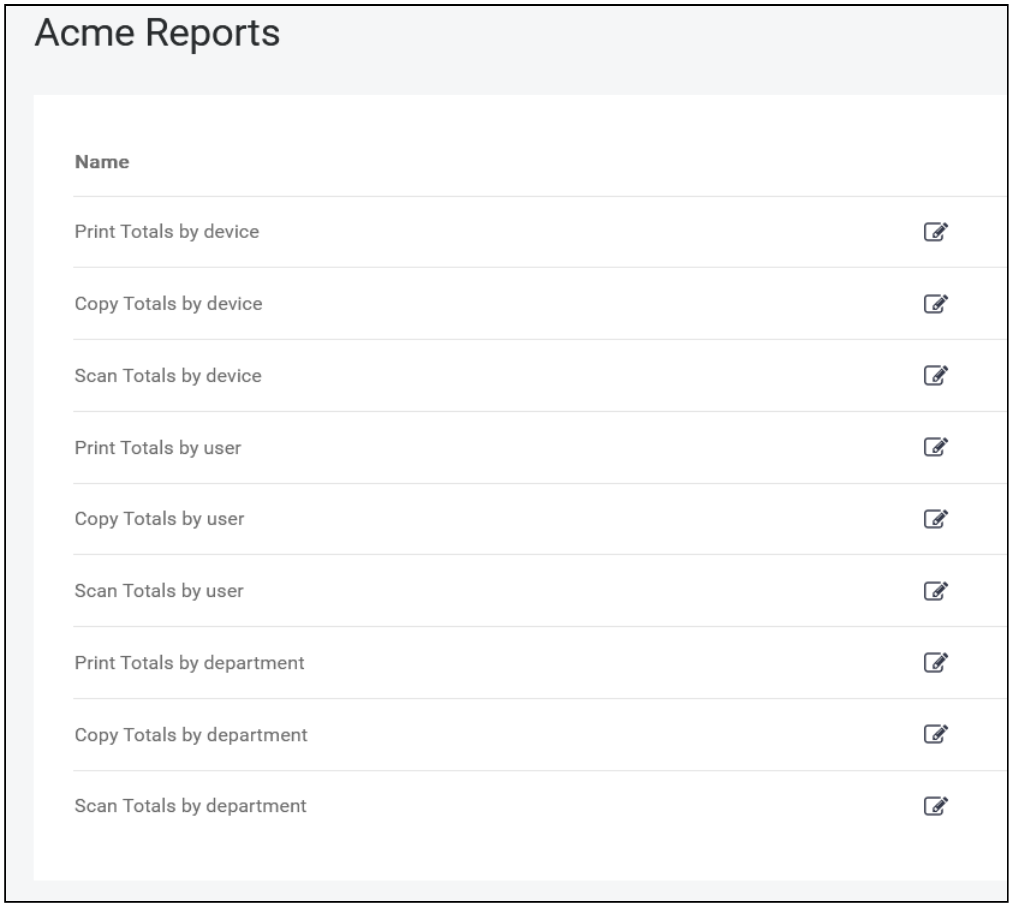
YSoft SAFEQ Cloud includes high level reports to show printed output by user, by device, or by department. You can view the reports in your browser or export them to Excel, PDF, or CSV. For department reports, you must set the **Department** attribute to a proper Entra/LDAP/Okta attribute name that contains the user's department.

SAFEQ Cloud does not act as a print accounting solution and only considers the attributes of a print job at the time of submission, whether it was overall sent as color vs mono, and the total number of pages sent to SAFEQ Cloud. Changes in attributes at print time, print errors, or mixed color/mono jobs are not accounted for.



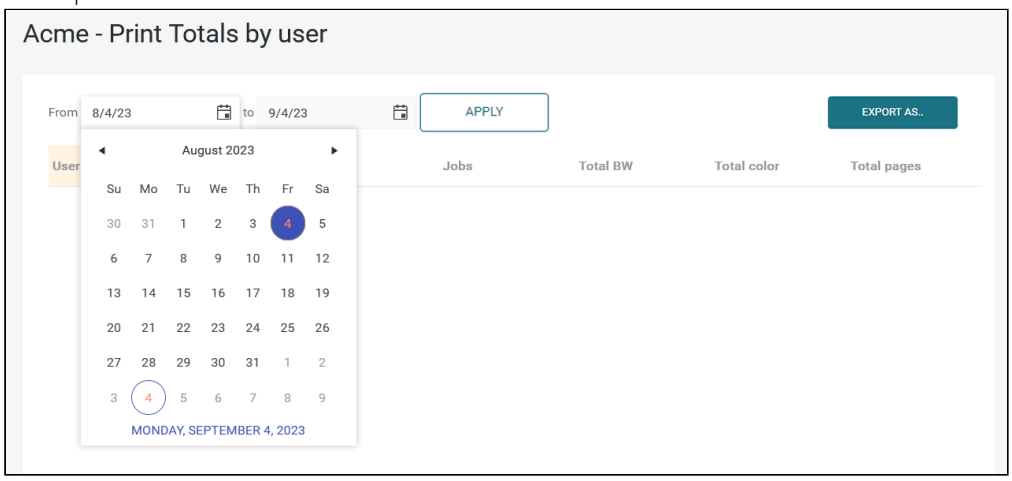
Customer account reports

For customer accounts, you can generate the following reports:



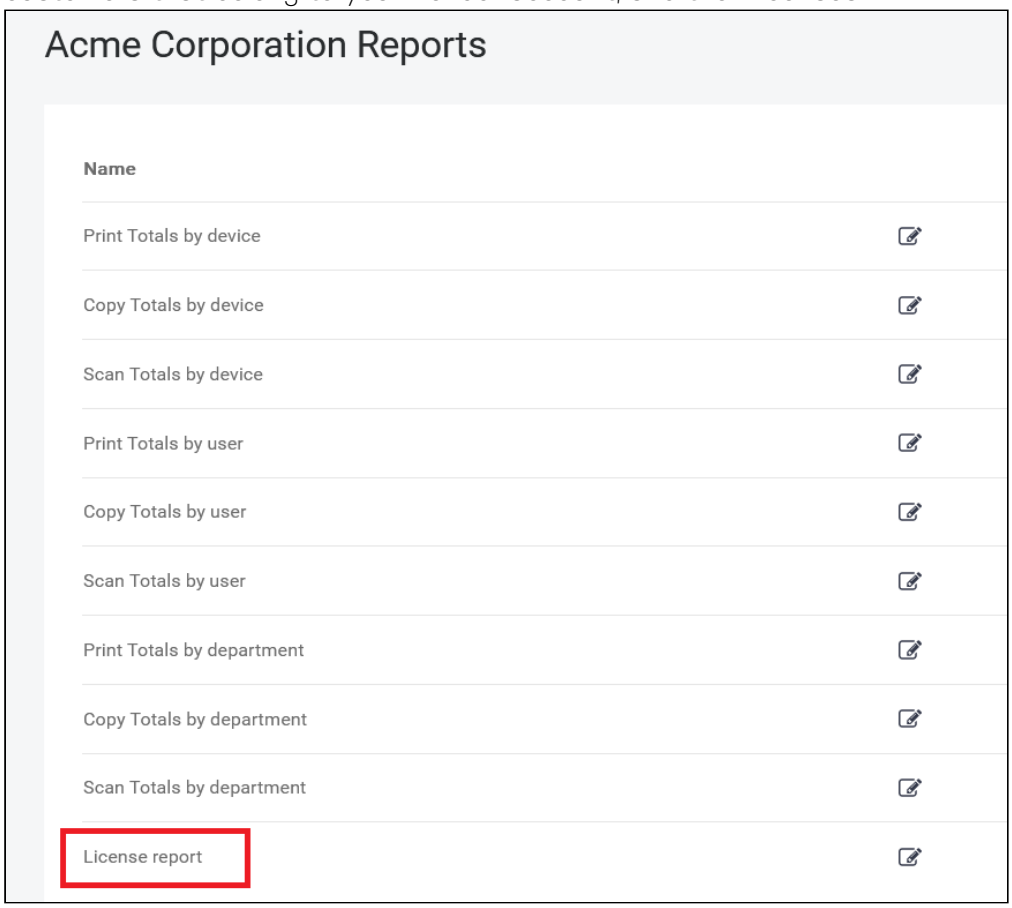
1. Click the type of report you wish to export.
2. Select the date range and click **Apply**.
3. Click **Export as** and select your preferred export format (PDF, XLSX, or CSV).

Example:

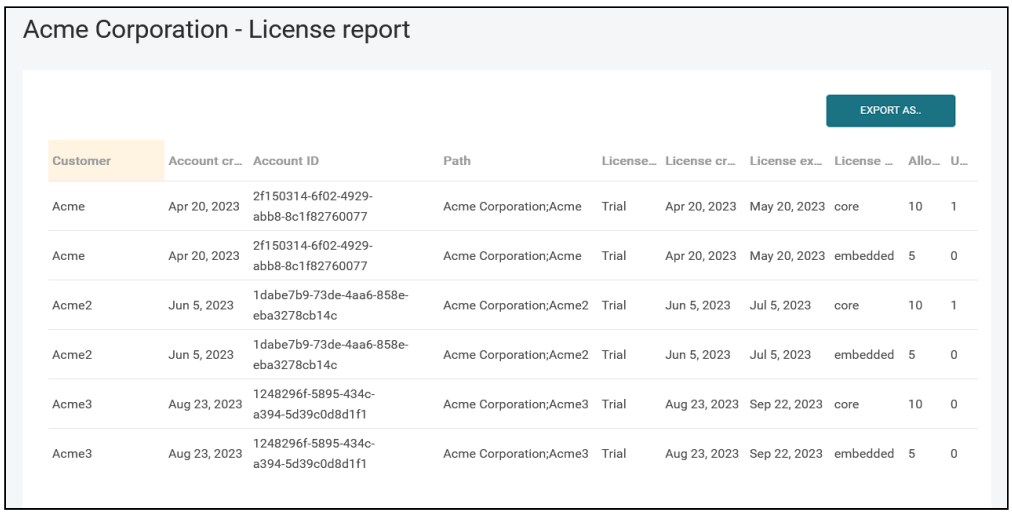


Vendor account reports

For Vendor accounts, the list also contains the **License report**. This provides an overview of all customers that belong to your Vendor account, and their licenses.

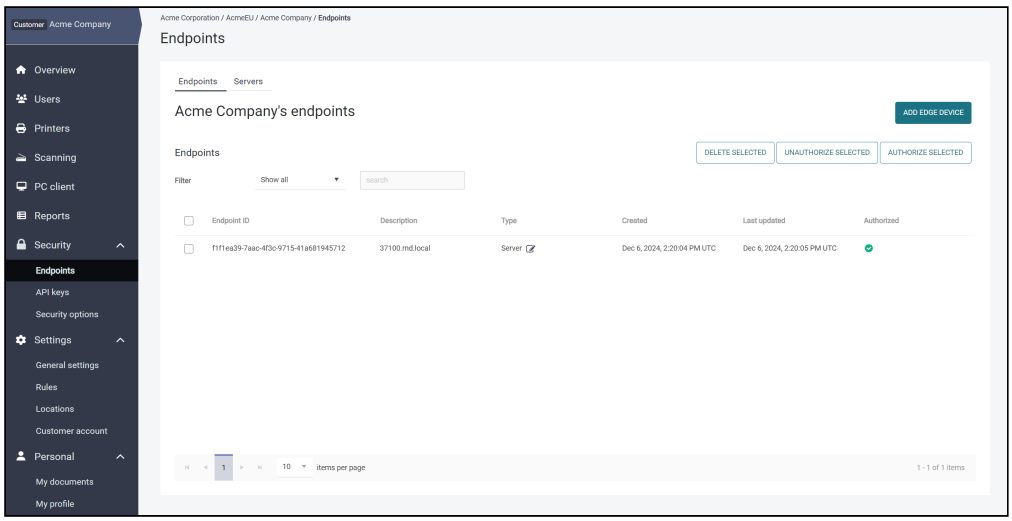


Example:



8.1.6 SECURITY SECTION

The **Security section** of the application includes pages that allow you to manage **Endpoints** with Servers, **API keys**, and various other **Security options**.

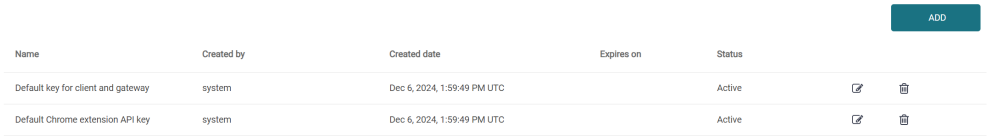


API access keys

API keys in YSoft SAFEQ Cloud server are required to access various server functions using API calls. Please refer to separate API documentation for a full description of the available API endpoints and how to use them.

By default, there are several API keys predefined for each customer account which are used by various clients connecting to SAFEQ Cloud server, for example, the SAFEQ Cloud client or a Chrome browser extension.

> For security reasons, we recommend you to use a custom API key instead of the predefined ones and disable the predefined keys. A custom API key can be specified during SAFEQ Cloud client or SAFEQ Cloud gateway installation.

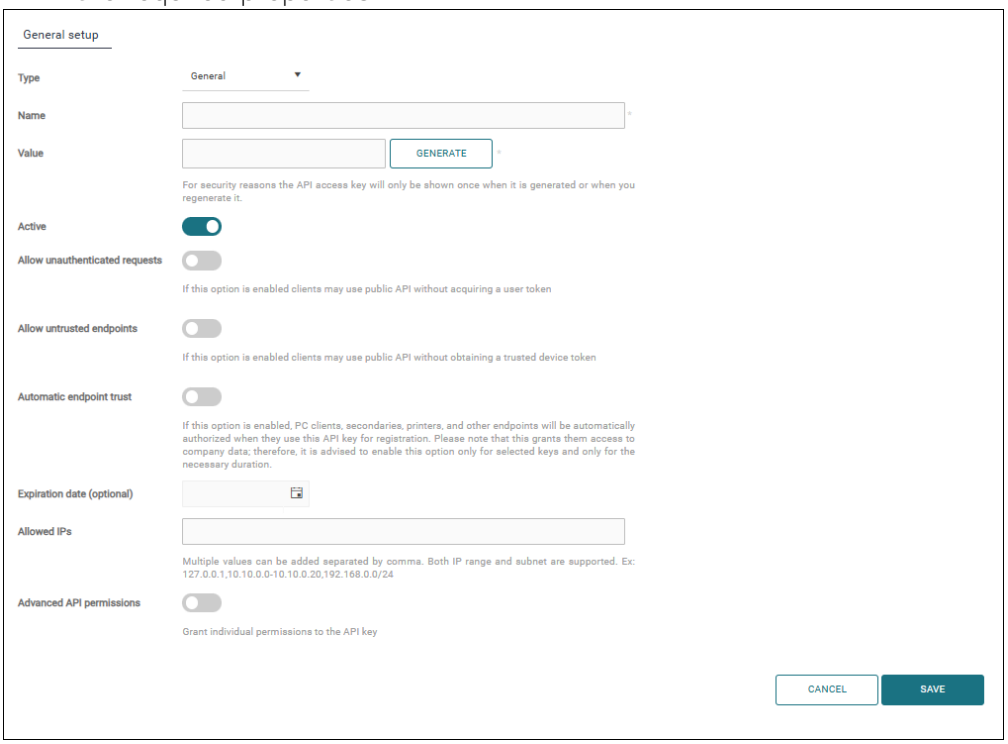


Access to the API key section in the SAFEQ Cloud Web UI is controlled by **ModifyApiKey**, **ViewApiKey**, and **DeleteApiKey** permissions set in the user roles. API keys are inherited from top-level vendor nodes. If an API key is defined on a vendor account level, it can be used to access API functions across all sub-accounts associated with that vendor.

Creating an API key

1. In the SAFEQ Cloud Web UI, click **Security** > **API keys**.
2. Click **Add**.

3. Fill in the required properties.



- Type
  - General – The default type. You can set all the permissions according to your needs.
  - Embedded – Used in Embedded configurations. Use the raw value if you wish to install a terminal via Manual operations (see Embedded Terminals' configuration and Terminal Deployment Tool).
  - Chrome – Used for Chrome extensions. If you wish to use the one that is created by default, regenerate it to see the value behind the hash.
  - Edge – Used for Edge devices such as the OMNI bridge. When you add a new edge device, a new value is added to this default Edge API key.
- Name – a descriptive name of the API key.
- Value – an automatically generated unique value associated with the API key.
- Active – a flag indicating whether this API key is active.
- Allow unauthenticated requests – if this option is enabled, it is possible to send API requests without acquiring the user token first.
- Allow untrusted endpoints – if this option is enabled, it is possible to perform login operations and acquire a user token for insecure login types without completing the device registration workflow. Insecure login types include Session user, Session user + domain, and User principal name. See the API documentation for more information.

  If both unauthenticated requests and untrusted endpoints are enabled, the API key can be used without any authentication and a leaked API key could result in unauthorized access to the system.

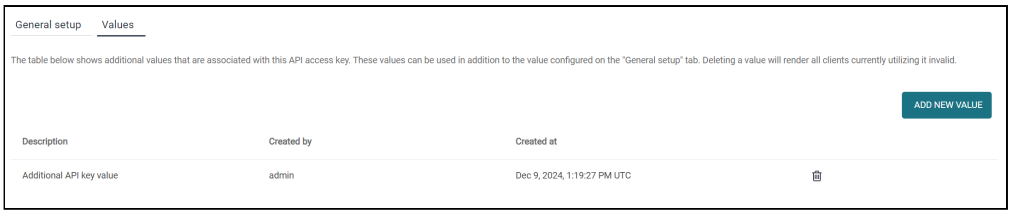
When configuring the SAFEQ Cloud Client with a custom API key, we recommend you to keep **Allow unauthenticated requests** and **Allow untrusted endpoints** turned off. If both of these options are disabled and an insecure authentication type is used, you must enable the **Enable secure login for session authentication types** option in the SAFEQ Cloud Client configuration.

- **Automatic endpoint trust** – if this option is enabled, SAFEQ Cloud Clients, secondary gateways, printers, and other endpoints will be automatically authorized when they use this API key for registration. Note that this grants them access to company data; therefore, we recommend enabling this option only for selected keys and only for the necessary duration.
- **Expiration date** – an optional field indicating the date when this API key expires. If not set, the key does not expire.
- **Allowed IPs** – a list of whitelisted IP addresses from which API requests are allowed for this key. If not specified, all IPs are allowed.
- **Advanced API permissions** – if this option is enabled, it allows you to additional special permissions required for specific API calls. See the API documentation for additional details.
- Additional values associated with the API key are present in the Values tab at the top of the configuration form.

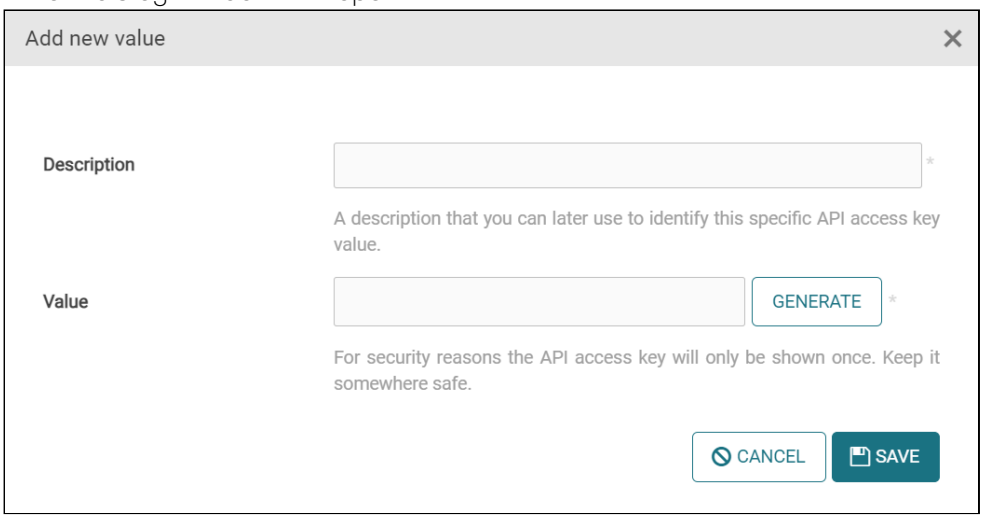
Note that for the predefined key **Default key for client and gateway** or for a custom key which is intended to be used by the SAFEQ Cloud Client or SAFEQ Cloud gateway, you must enable the **Allow unauthenticated requests** and **Allow untrusted endpoints** flags. Otherwise, you won't be able to install or use the SAFEQ Cloud Client in the local storage mode, and to install the secondary SAFEQ Cloud gateway.

Creating additional values for an API key

1. After you have created and saved your new API key, click the edit icon to edit it. Go to the **Values** tab and then click **Add new value**.



2. A new dialog window will open.



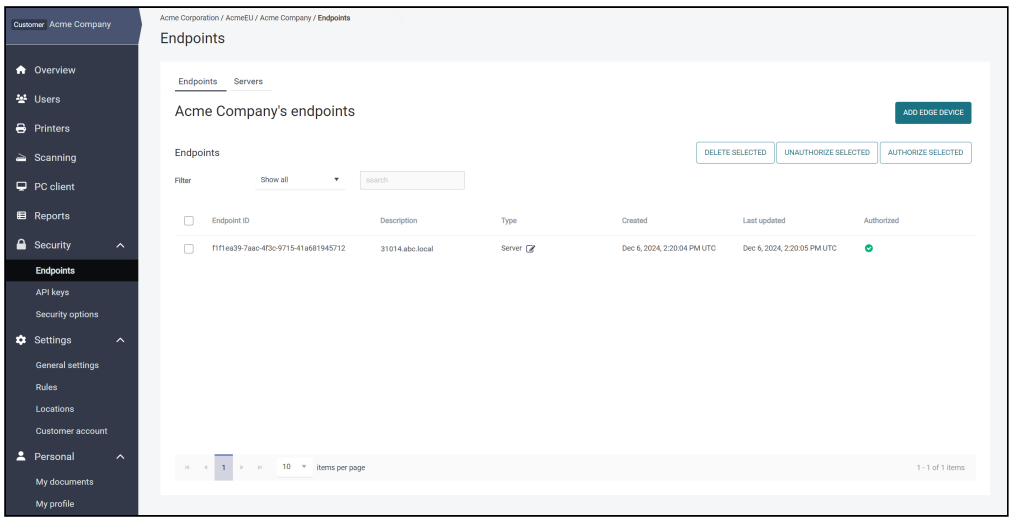
3. In the **Description** field, enter a description that you can later use to identify this specific API access key value.
4. Click **Generate** to generate a unique value associated with the API key.

> All other properties are inherited from the associated API key.

5. Click **Save**.

Endpoints menu

In the **Endpoints** menu, you can configure **Endpoints** and **Servers**.

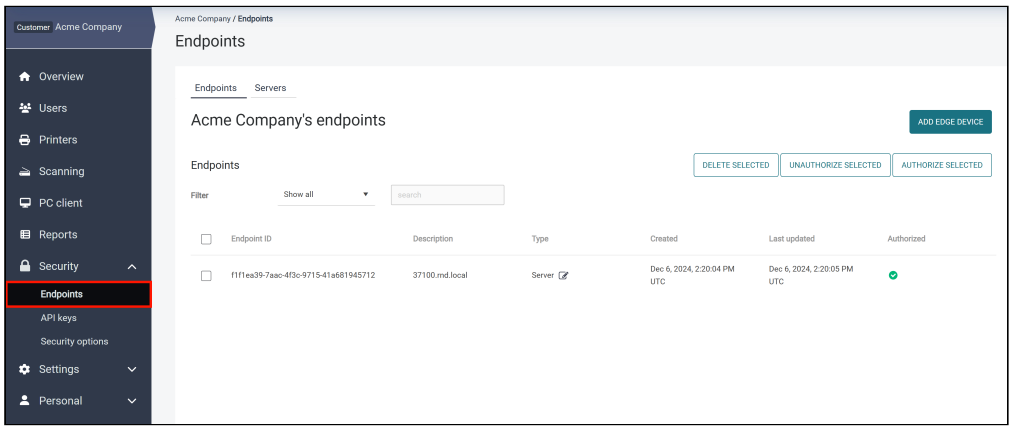


Endpoints

In the SAFEQ Cloud Web UI navigation menu, click **Security** > **Endpoints**.

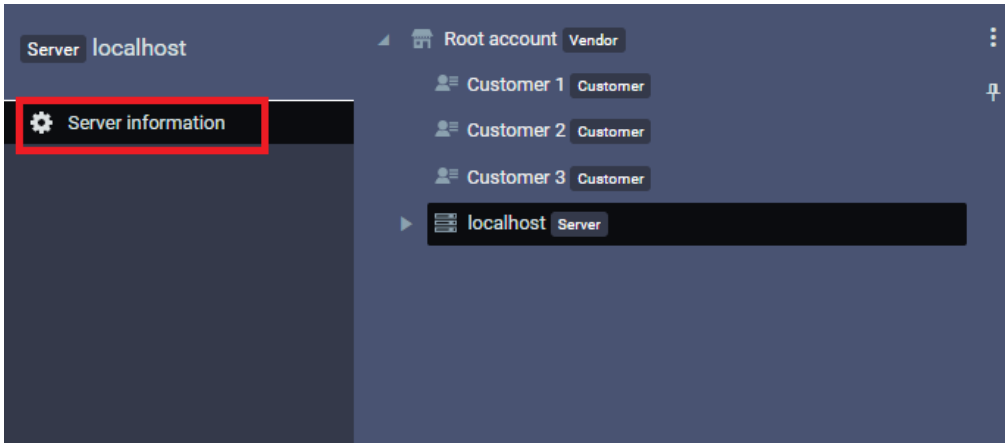
The **Endpoints** tab contains the list of all endpoints that accessed the server. You can authorize or unauthorize individual endpoints and filter them by type. YSoft SAFEQ Cloud distinguishes the following endpoint types:

- Server
- Printer
- SAFEQ Cloud client
- Browser extension



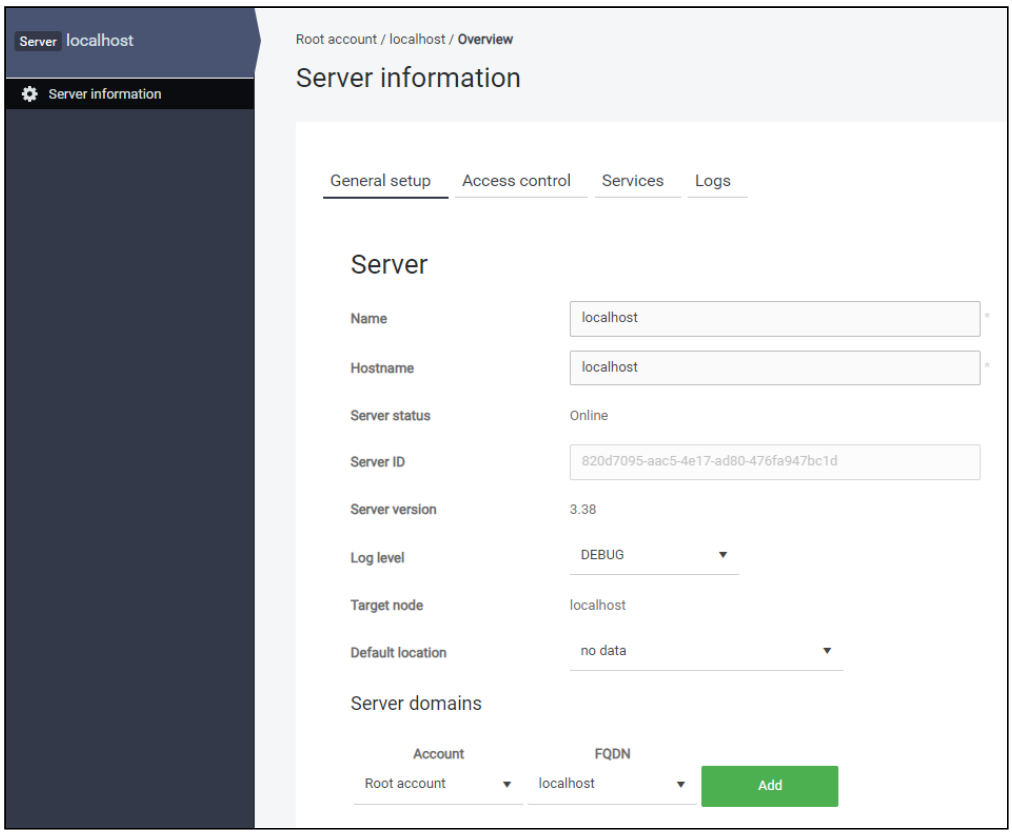
Servers

A server in SAFEQ Cloud provides the platform for running services. When you assign a service to run on a server, then that server is responsible for executing and managing the lifetime of that running service instance. In addition to running services, each server has a number of properties that identify and control the server caching features.



General setup section

Manage the server settings. If you don't have edit permissions, settings are displayed in read-only mode.



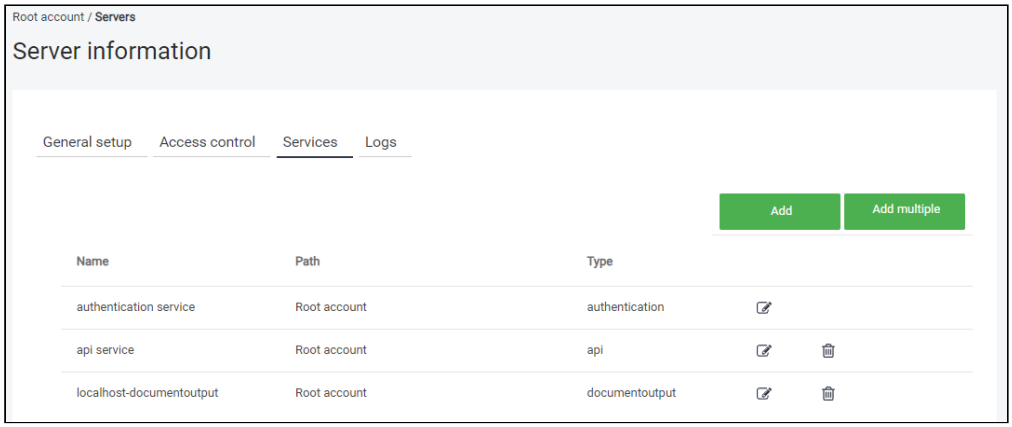
- **Name** – A user-friendly name of the server as it appears in the SAFEQ Cloud system tree.
- **Hostname** – The host name of the server that was read from the server operating system when it was added to the SAFEQ Cloud system.

  > If running multiple primary servers in a cluster, it's important that the **Hostname** is a valid hostname or DNS address that all cluster nodes can resolve, as the Hostname is used to communicate heartbeats between cluster nodes.

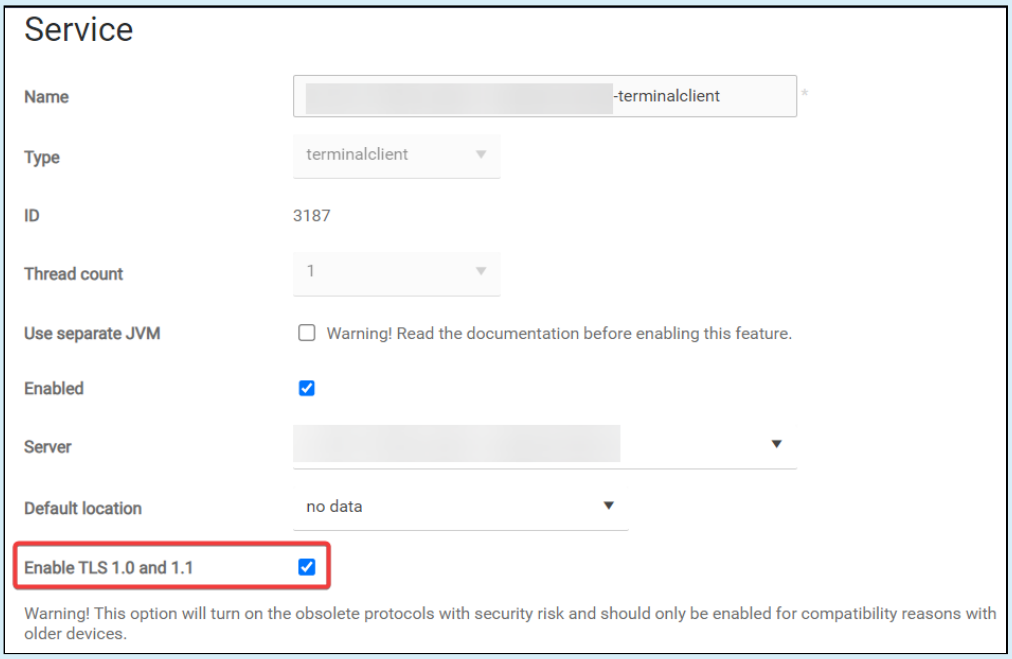
- **Server ID** – A system-generated unique identifier for the server. This value cannot be modified.
- **Log level** – The default option is **INFO**. Select **DEBUG** if you wish to have more detailed logs.
- **Enable offline cache** – Use this option to enable the offline cache function on the server. For more information on the offline cache feature in SAFEQ Cloud, see Offline Server Cache.
- **Cache Window in hours** – When offline cache is enabled, this value sets the duration of the cache. For example, a value of 24 hours means that the server will retain any activity performed on that server for 1 full day in as a rolling window.
- **Target Node** – This value is read-only and indicates the node name within the SAFEQ Cloud system where the server is placed.
- **Location** – This value indicates the Server location. If no location is set on the Server, it will retrieve and display the inherited location of the parent (Account).
- **Server Domains** – Each server can be associated with the domain name that identifies and locates the services that it hosts. You may add several domain names to the server that have been created in the SAFEQ Cloud system within the account where the server resides in the SAFEQ Cloud system tree.

Services section

The services section lists the services that are hosted by this server. On this screen, you may add multiple, add, edit, or remove services. For more details on managing services, see section Services.

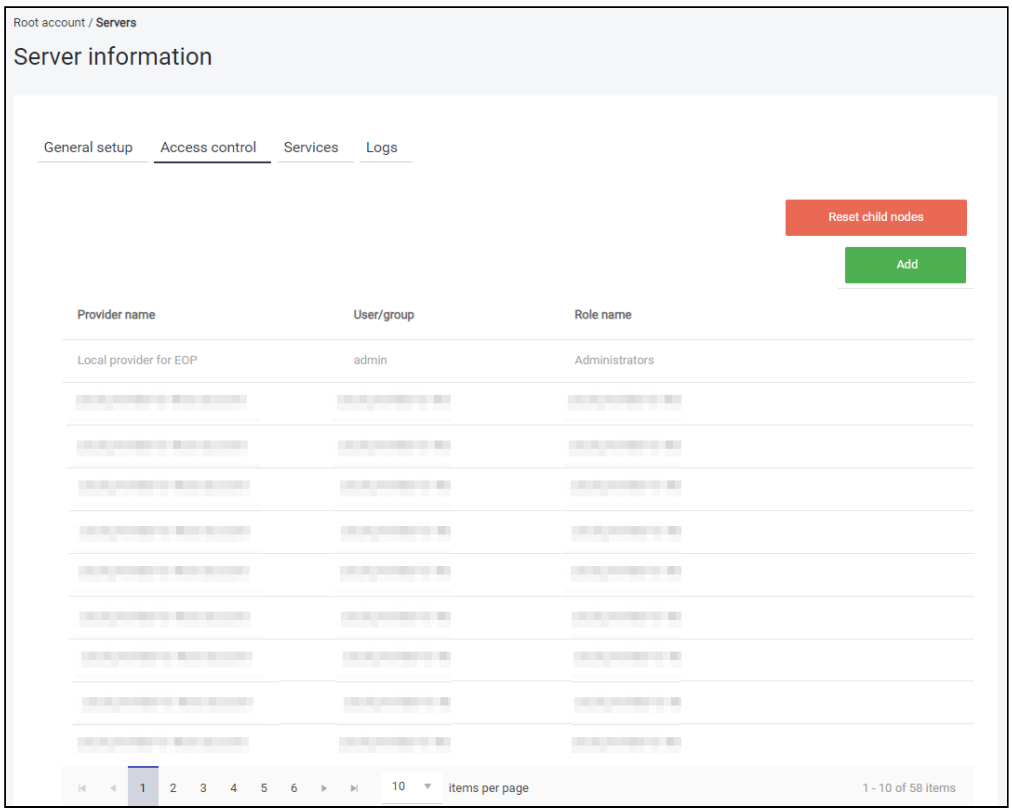


By default, SAFEQ Cloud uses TLS 1.3 for all communication. If SAFEQ Cloud can't communicate with an endpoint (such as an MFD) via TLS 1.3, it will fall back to TLS 1.2. If the endpoint doesn't support TLS 1.2 (as some older MFDs don't) and you have selected the **Enable TLS 1.0 and 1.1** option in the *terminalclient* service, SAFEQ Cloud will also try TLS 1.1, and (if required) TLS 1.0.



Access Control section

The Access control section allows you to manage permissions for accessing this server. For more details on Access control settings, see section Access Control.



Audit log

Audit log documentation

The Audit Log gives administrators the ability to see all actions made by a user during a selected period and all configurations and settings made on the system during a selected time period.

It can be used for audit and compliance purposes.

All configuration changes in SAFEQ Cloud are logged.
All higher-level operations are logged to audit log.
So it should be possible to see *what* has been done *where*, *when* and by *whom*.

Audit event log configuration

The configuration of the event log happens in **application.conf** config file.

```
event-log {
  file {
    is-enabled = false
    basename = "audit"
    directory = ${app.home}"/logs"
    retention-days = 30
  }
}
```

The sub-node(s) under `event-log` are the output writers. Currently there is only a file writer. So the settings under `file` only apply to the file writer, or generally to the node under which they are present.

Most settings are self-explanatory.

- `is-enabled` switches the audit log file writing on/off. Changing this setting requires re-start of SAFEQ Cloud.
- `basename` is the base name of the audit log file. A date is automatically appended to the `basename`.
- `directory` is the directory where the log files are created in. `${app.home}` is a variable that points to the root folder of SAFEQ Cloud.
- `retention-days` is unused

Audit log writing

File writer

The audit log file is only written on primary servers. The log file name is simply: 'audit-YYYY-MMM-DD.log'. Every day a new log file is created with events that occured on that day. The 'audit' part is the `basename` of the configuration above.

Events from secondary/gateway servers

Under normal circumstances (secondary is online/connected to primary) *entity events* are not logged at all on secondary servers. Because entities are not modified on secondary servers.

Action events and config update events are being raised on secondary servers, i.e. if a user authentication happens on an Authentication Service. So those kinds of events are being forwarded to primary servers and logged there.

Log synchronization from offline secondary servers

In case a secondary server looses connection to the primary and the offline-cache is enabled it will record any entity, action and config events locally and synchronize them to the primary when the connection is established again. The original `event-context` and `event-detail` of the event is maintained with original timestamps of when those operations did occur on the secondary server while offline.

For this to work a temporary audit log file is written on the secondary where the audit entries are written to in an encoded format.

The log structure

An audit log entry current has the following structure. It is embedded into starting `{` and ending `}` as the first character of a line. For example:


```
{
   event-context:{type:EventContext,source:test,traceId:"fabb825a-6fb6-4d25-96c2-
f6482972319d",serverId:"f4911326-eb36-41e7-8fc5-
bee01ca07ae5",datetime:"2020-05-11T15:37:24.627+02:00",request:{type:UnauthenticatedRequest,requesting-
user:{type:RequestingUser,user-id:user-not-defined},requesting-domain:}},
   event-detail:{type:DeleteEntityEvent,entity-type:Account,entity-to-delete:{type:Account,account-
type:Container,id:1,name:Foo,domains:[]},result:{type:Account,account-type:Container,id:1,name:Foo,domains:
[]}},datetime:"2020-05-11T15:37:24.630+02:00"}
```

```
}
```

There are two major parts of a log entry.
The first one is `event-context`. The `event-context` transports the *when*, *where* and *who*.
The same `event-context` may be part of multiple log entries. This happens when an operation triggered at a system boundary (i.e. API) or in the UI and consists of multiple configuration changes. Each configuration change is separately logged with the same `event-context` as they all group one operation. This is easily visible as the `traceId` value is static to multiple audit log entries.

The `event-context` has the following parameters:

- source: the source of where the event occurred. This can be i.e.: "web", or "api".
- traceId: The trace ID combines multiple events into a single action. For example, an API request to upload a document may result in multiple audit log events that change some data but are all part of this higher-level operation. The value is generated as a UUID by default. If the OpenTelemetry (OTEL) feature is enabled, the value is generated by OpenTelemetry—32 hexadecimal characters without any dash or so.
- serverId: the server ID where this event originated.
- datetime: the date and time when the event first hit an SAFEQ Cloud boundary system or was initiated otherwise.
- request: distinguishes between an *authenticated request* and an *unauthenticated request*. An *authenticated request* contains an account-id and user details. This is used when a user could be identified as part of an API request or an UI operation. An *unauthenticated request* is used when a user could not be identified, for example because the API uses an ApiKey. In this case the *unauthenticated request* contains at least the domain that is the target of the request and any ApiKey, or email address that was additionally available.

The second part is the `event-detail`. The `event-detail` is the *what*.

There are the following different types of *what*:

Domain model/entity based configuration changes

The following operations on domain model/entities are recorded:

- adding data, `AddEntityEvent`
- updating data, `UpdateEntityEvent`
- deleting data, `DeleteEntityEvent`
- deleting all of something, `DeleteAllEntityEvent`
- some custom operation on entities that cannot be easily catigorized on the above, `CustomEntityEvent`

All of the above events record changes to entities.

- `entity-type` logs the name/type of entity.

- `result` log the operation result.

Additionally each operation has special fields. I.e. `UpdateEntityEvent` logs a previous/old value and the new value as `result`.

The `result` field can also contain an error like so:
`result:{type:Error,error-code:9999,error-msg:Foo,cause:none}`

The following entities may get recorded:

```
Account, ApiKey, AuthProvider, AuthRole, Document, EncryptionKey, Group,
InputPort, KeystoreData, LicenseAllocation, Location, MessagingConfig,
MobilePrintConfig, MobilePrintWideArea, ObjectNode, OutputPort,
Server, Service, Storage, TagGroup, TemplateConfig, TerminalConfig, Trigger, User, UserDetail
```

Other configuration changes

Log type: `ConfigUpdateEvent`

Config updates are raised and written to log when configuration is changed that is stored in `application.conf` file.

Here is an example of how this looks for a change to the log-level:

```
{
   event-context:
{type:EventContext,source:web,traceId:"19d09e6c-8d10-4390-9256-1dbb7d9002ba",serverId:"1e786aa7-
d46a-473b-98e8-5c8cccb39fb5",datetime:"2020-05-26T15:06:31.055+02:00",request:
{type:AuthenticatedRequest,executing-user:...,account-id:1}},
   event-detail:{type:ConfigUpdateEvent,configType:app.logging,configData:
{"loglevel":"DEBUG"}},datetime:"2020-05-26T15:06:31.066+02:00"}
}
```

Action based operations

Log type: `IntentActionEvent`

The `IntentActionEvent` events mark high-level operations. Those include things like user authentication, document upload, push or pull-print, etc.

Those operations usually involve changes to multiple entities. To get those together the `IntentActionEvent`s mark a start and end block where multiple *entity events* may occur.

The opening block event is usually marked with an `intent` similar like this:
`event-detail:{type:IntentActionEvent,intent:{type:AddDocumentIntent...`

Where the closing block is marked with an `intent-result` similar like this: `event-detail:{type:IntentActionEvent,intent-result:{type:AddDocumentIntentResult...`

All events within this block have the same `event-context` and hence the same `traceId`.

So the `traceId` can be used to filter for higher-level operations that contains multiple entity operations.

Common to all is the `datetime` when events happened.

The following `intent` types may get logged:

AuthUserIntent, FindUsersIntent, FindGroupsIntent, TestAuthProviderIntent, PrintInputIntent, MobilePrintInputIntent, PrintOutputIntent, PrintAllIntent, CreateOutputPortIntent, UpdateOutputPortIntent, DeleteOutputPortIntent, DefaultConvertDocumentIntent, InternalConvertDocumentIntent, ScheduledConvertDocumentIntent, MoveStorageIntent, AddDocumentIntent, UpdateDocumentIntent, RetrieveDocumentIntent, UploadDocumentIntent, DownloadDocumentIntent, DeleteDocumentIntent, DeleteTemporaryDocumentIntent, GetDocumentUriIntent, AddDocumentFromServerIntent, UpdateDocumentFromServerIntent, ConfigureTerminalIntent, DeployTerminalIntent, UndeployTerminalIntent, LicenseCheckIntent, EmailMessageSendIntent, TestEmailMessageSendIntent

Offline Server Cache

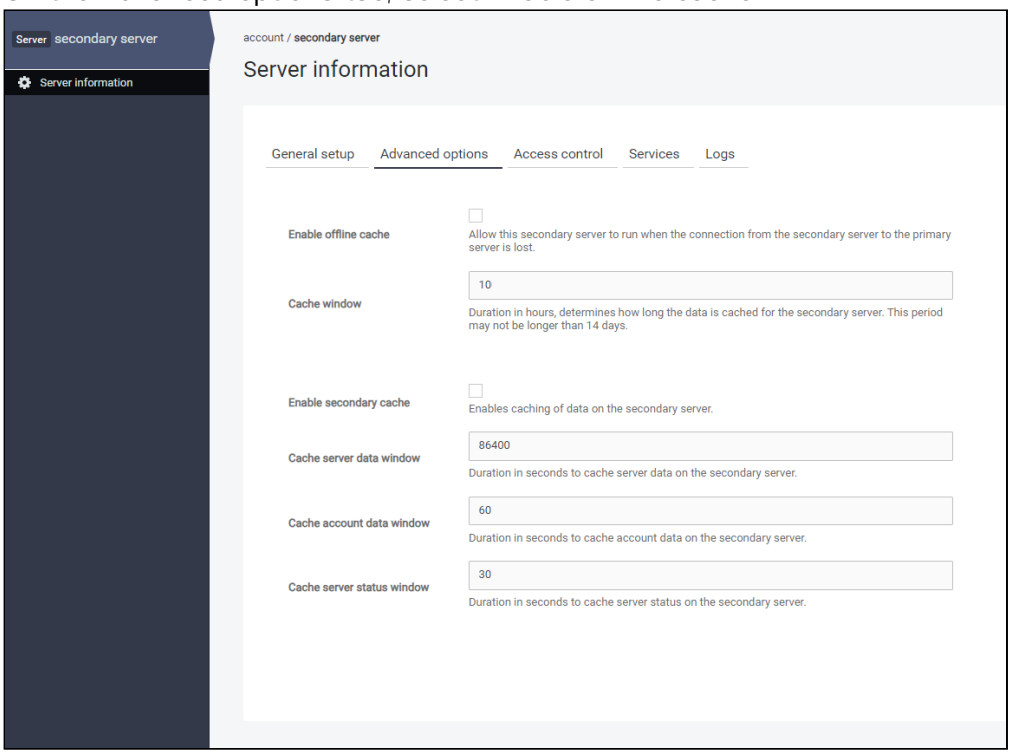
This feature is currently not working as intended and is under review. It has been added to the Known Issues and Limitations list.

Offline server cache will allow a secondary server to run when the connection from the secondary server to the primary server is lost. Enabling this option will allow a secondary server to run for 14 days while in the offline state.

Enabling Offline Server Cache

1. To enable offline server cache, select the server in the tree; this will display the server sub-menu.

2. On the **Advanced options** tab, select **Enable offline cache.**



3. Click **Save**.

Specifying cache window

The cache window determines how long the data is cached. For example, if this value is set to 2, and the secondary server loses connectivity to the primary server, then all users that authenticated in the last 2 hours since the loss of connectivity can log in. The value specified will be counted in hours. However, this period may not be longer than 14 days, as Offline server cache mode allows the secondary server to run up to 14 days in an offline state.

Secondary cache

To cache server data, account data, and server status on this secondary server, enable the **Secondary cache** option.

Cache window (in seconds) determines for how long the data is cached on this secondary server. You can specify the following:

- Cache server data window
- Cache account data window
- Cache server status window

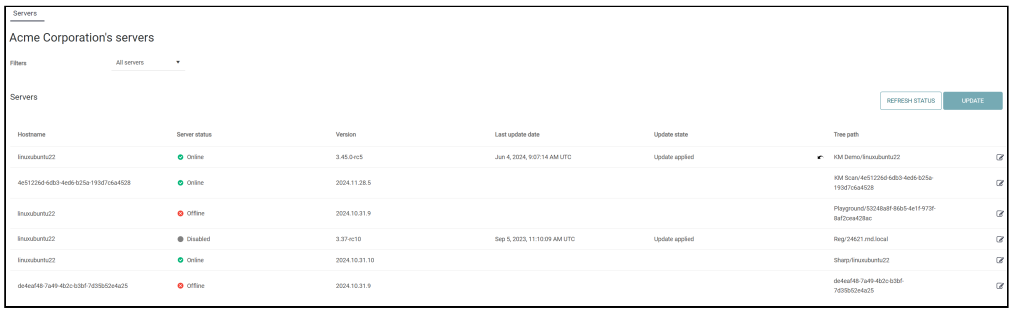
To disable one of these caches on the secondary server when the secondary cache is enabled, set the respective cache window value to 0.

Server list

Use this feature to see a list of all the account servers, their status, last update state and to perform remote server updates.

The status of the servers can be:

- green – online
- red – offline
- yellow – starting
- grey – disabled or not authorized

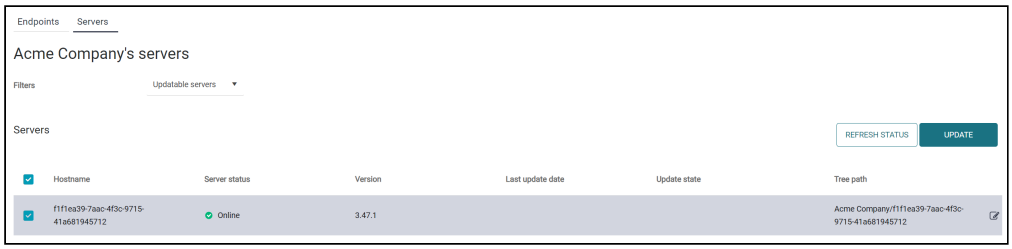


You can go to the server details by clicking the edit icon.

Remote Update of Secondary Gateways

Initiating remote updates

Since YSoft SAFEQ Cloud server version 3.9, you can update Secondary Gateways centrally using the **Servers** tab in **Endpoints** section in SAFEQ Cloud Web UI.
Secondary Gateways which can be updated are displayed when you select **Updatable servers** in **Filters**.

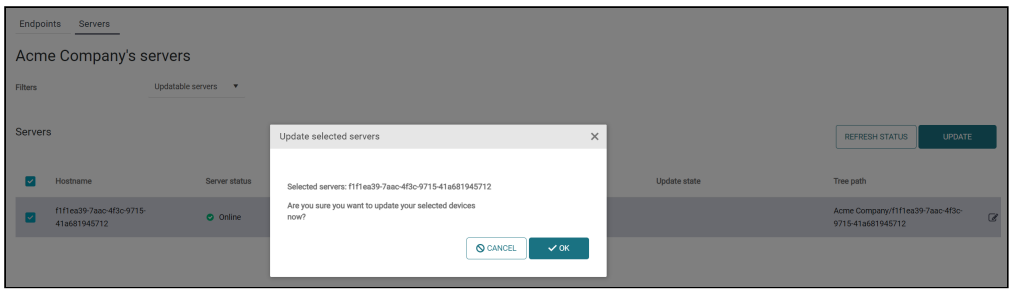


Secondary Gateways are considered updatable when the following conditions are met:

- This is a Secondary Gateway (not a primary SAFEQ Cloud server)
- The Secondary Gateway is online
- The version of the Secondary Gateway is 3.9 or higher
- There is an update available on Y Soft CDN website which is newer than the version running on this server

Note: for the on-premise installations of SAFEQ Cloud primary server, the Y Soft update site must be available: `cdn.everyoneprint.com`, port 443. If the primary server does not have access to the Internet, you can configure it for custom update site. For more information please contact technical support which will assist you in configuring primary server in this way. The gateways do not need access to the CDN website.

To perform an update, select one or more Secondary Gateways from the list, click **Update**, and confirm the action by clicking the **OK** button.



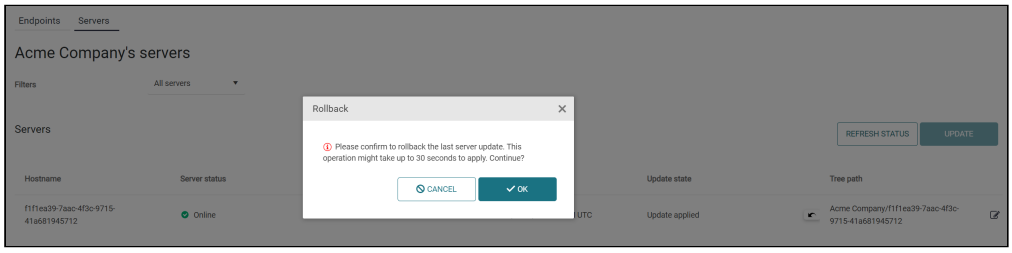
Update of the selected Secondary Gateways will start in the background. You can monitor the update status in the **Update state** column by clicking **Refresh**. It may happen that the Secondary Gateway will disappear from the list of updatable servers. In this case select **All servers** in **Filters**.

If the update was successful, the status will change to **Update applied** and an icon which allows to rollback the server update will appear.

Rolling back the update

In some cases, it is necessary to perform a rollback of the applied update, for example, if the updated software does not work as expected. SAFEQ Cloud provides a possibility to rollback the update even if the Secondary Gateway remains offline (does not connect anymore to the primary server). If the gateway stays offline after the update, the rollback is possible within 72 hours. If the gateway comes online, then the rollback is possible without a time limit.

To perform the rollback, click the rollback icon in the server status column and click **OK** in the confirmation window:



Rate limiting

Rate limiting is a technique to limit network traffic to prevent users from exhausting system resources. In this case, you can use it to prevent on-premise primary server(s) resource depletion by too many connected gateways or SAFEQ Cloud clients.

By default, rate limiting is disabled.

To configure rate limiting, edit the *operation* section of the *application.conf* config file located at `/opt/safeqcloud/conf/application.conf`.

The rate limiting uses a fixed window algorithm.

```
channel-server {
    connection-throttling-window-in-seconds=0
    allowed-connections-per-window=0
  }
```

You must set both of the following settings:

- connection-throttling-window-in-seconds – sets throttling window size in seconds.
- allowed-connections-per-window – sets the amount of allowed connections per throttling window.

An example of setting the limit to 50 connections per 1 second:

```
channel-server {
    connection-throttling-window-in-seconds=1
    allowed-connections-per-window=50
}
```

Thread Pool settings

These settings are done in the wrapper-safeq-cloud-server.conf file, which is a key configuration file used in conjunction with the application's execution wrapper. It contains various settings and parameters that govern the behavior and performance of the application. Among these settings are factors that determine the parallelism levels for different components of the application. This document explains the usage and customization of two such factors: `balanced.factor` and `remote-messaging.factor`.

Parallelism factors

Parallelism factors dictate the number of threads or concurrent processes used for specific tasks within the application. These factors are instrumental in optimizing resource utilization and improving overall performance.

balanced.factor

The `balanced.factor` property determines the parallelism factor for balanced processing tasks within the application. Balanced processing typically involves tasks where the workload is evenly distributed across available resources.

remote-messaging.factor

The `remote-messaging.factor` property determines the parallelism factor for tasks related to remote messaging functionalities. These tasks often involve communication with external systems or services over a network.

threadpools.Conversion

The `threadpools.Conversion` property determines the size of the document conversion thread pool. When there is an expectation of a high volume of documents being converted directly on the secondary server, we recommend increasing this thread pool size to ensure efficient document processing. However, the number should never overreach the CPU cores available, because too many parallel conversions may cause the whole system to be slowed down.

Conversion of big files can consume up to 1GB of memory, so you must allocate enough memory on the secondary server for each conversion. Increase the memory availability or reduce the thread pool size accordingly.

Calculations for Balanced and Remote messaging thread pool

The value is calculated based on the available processors and the configured factors. The formula used for calculation is:

```
Runtime.getRuntime.availableProcessors * factor
```

- `Runtime.getRuntime.availableProcessors` returns the number of available processors in the system.
- `factor` represents configured `balanced.factor` and `remote-messaging.factor` value from the system properties. If not explicitly set, it'll use default values.

Default values and limits

Default values are applied to the parallelism factors. These default values ensure reasonable performance and resource utilization under typical circumstances.

- `balanced.factor` : 8
- `remote-messaging.factor` : 4
- `Maximum Allowed Factor` : The parallelism-factor should be carefully chosen considering the available hardware resources and workload characteristics. The maximum allowed factor is 64, beyond which the thread pool size will not be increased.

Customization

You can customize the default parallelism factors by setting the system properties in the wrapper-safeq-cloud-server.conf file. This customization allows you to tailor the application's behavior to suit specific deployment environments and workload characteristics.

Suggested Thread pool Conversion Configuration

To ensure efficient document processing when there's a high volume of documents converted directly on the secondary server, we suggest using a thread pool size close to the CPU cores (CPU cores - 1) for document conversion:

```
wrapper.java.additional.<n>=-Dthreadpools.Conversion=7
```

Adjust the thread pool size (7 in this case for 8 CPU cores machine) based on the expected workload and system capabilities.

Property format

Property	Description
`-Dbalanced.factor=<value>`	Sets the parallelism factor for balanced processing tasks.

Property	Description
`-Dremote-messaging.factor=<value>`	Sets the parallelism factor for tasks related to remote messaging.
`-Dthreadpools.Conversion=<value>`	Sets the size of the document conversion thread pool.

Example configuration

```
# Customized parallelism factors for balanced processing and remote messaging

wrapper.java.additional.<n>=-Dbalanced.factor=<value>

wrapper.java.additional.<m>=-Dremote-messaging.factor=<value>

wrapper.java.additional.<k>=-Dthreadpools.Conversion=32
```

Replace <n>, <m> and <k> with appropriate numerical values to denote the order of additional Java options in the wrapper-safeq-cloud-server.conf file.

Replace <value> with the desired integer representing the desired parallelism factor.

JVM heap memory configuration

The JVM heap memory configuration is done in the wrapper-safeq-cloud-server.conf file. This is a is a key configuration file used in conjunction with the application's execution wrapper. It contains various settings and parameters that govern the behavior and performance of the application.

Use the `-XX:MaxRAMPercentage` parameter to specify the maximum heap size for Java Virtual Machine (JVM) processes as a percentage of total system memory.

This setting is crucial for optimizing JVM performance and ensuring efficient memory utilization. See the below recommendations for configuring this parameter based on system memory usage and requirements.

Recommendations

1. Standard Configuration:
   - Recommended Value: 70% of total system memory.
   - Use Case: Suitable for most scenarios. Provides a balance between JVM heap allocation and leaving sufficient memory for the operating system and other processes.
2. High System Memory Usage (> 90%):
   - Recommended Action: Decrease the setting to 60% or lower.

- Use Case: When the system's memory usage is consistently high, reducing the heap size percentage helps alleviate memory pressure and ensures smoother operation of the system.

3. Large System Memory (> 32GB):
   - Special Consideration: When available system memory exceeds 32GB.
   - Recommended Action: Manually limit JVM heap memory to 31GB using `-Xmx=31GB`.
   - Reason: Prevents the disabling of compressed Ordinary Object Pointers (OOPs), which occurs when the heap size exceeds 32GB. Limiting the heap size to 31GB ensures optimal performance without compromising memory efficiency.

Configuration

Admins can also configure the maximum percentage of RAM allocated to the application using the `wrapper.java.additional` property. This setting is particularly useful for ensuring optimal memory utilization and preventing excessive resource consumption.

The property format is `-XX:MaxRAMPercentage=<value>`, and it sets the maximum percentage of RAM allocated to the Java Virtual Machine (JVM). The default value is 70.

Example configuration:

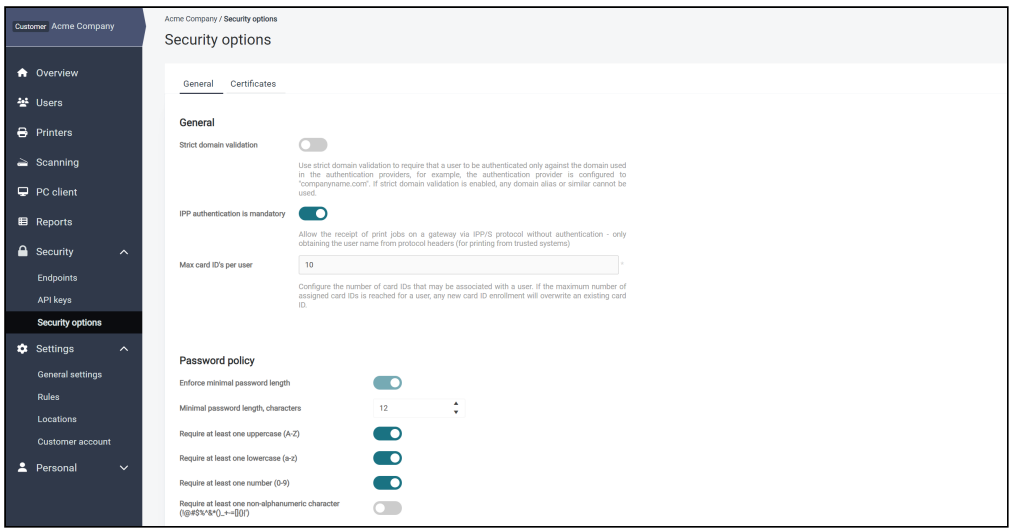
```
# Set the maximum percentage of RAM to 80%

wrapper.java.additional.<n>=-XX:MaxRAMPercentage=80
```

Replace <n> with appropriate numerical values to denote the order of additional Java options in the wrapper-safeq-cloud-server.conf file. Ensure that the numerical value (<value>) represents the desired percentage of RAM that you wish to allocate to the JVM.

- It's essential to monitor system memory usage regularly and adjust the `-XX:MaxRAMPercentage` parameter accordingly to maintain optimal performance.
- Detailed monitoring and analysis tools can help in determining the most suitable heap size configuration for specific use cases and environments.

Security options

The **Security options** menu contains settings related to security, password policy, PKI and encryption, privacy and certificates.



General

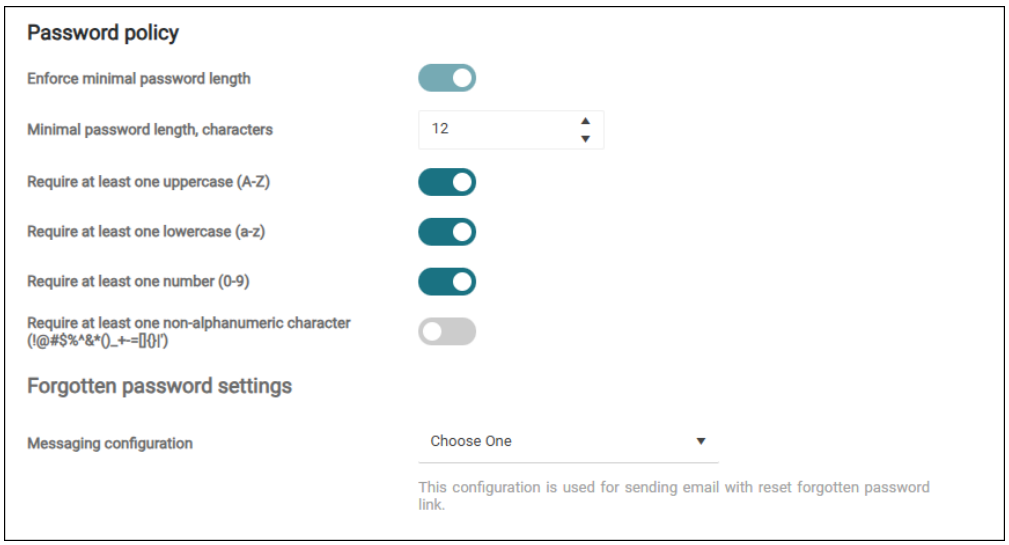
This section of the **General** tab contains several settings that are not in Vendor/Customer account. Both Vendor and Customer account types have the same options available, except for **Max card ID's per user** which is only available for Customer.

- **Strict domain validation** – If enabled, a user can be authenticated only against the domain used the authentication providers. Domain aliases cannot be used.
- **IPP authentication is mandatory** – Allow the receipt of print jobs on a gateway via IPP/S protocol without authentication, only obtaining the user name from protocol headers (for printing from trusted systems)
- **Max card ID's per user** – Configure the number of allowed card IDs associated with a user. The default value for existing or new Customer accounts is 10. If the maximum number of assigned card IDs is reached for a user, any new card ID enrollment will overwrite an already-existing card ID.

Password policy

This section can be found on the **Security Options** page under the **General** tab.

In the **Password policy** section, you can create a password policy for local users.



Note that the minimal password length policy property can not be disabled, and minimal password length can't be lesser than 6 characters.

Policy scope

The policy will start to be applicable to all operations in which passwords are created or changed:

- administrator edits the user record
- user edits their own profile
- user account is created or updated via the API

If the password doesn't meet the policy requirements, the operation will be rejected. Errors will be shown on the top of the UI form. In the case of API usage, errors will be recorded in the log file.

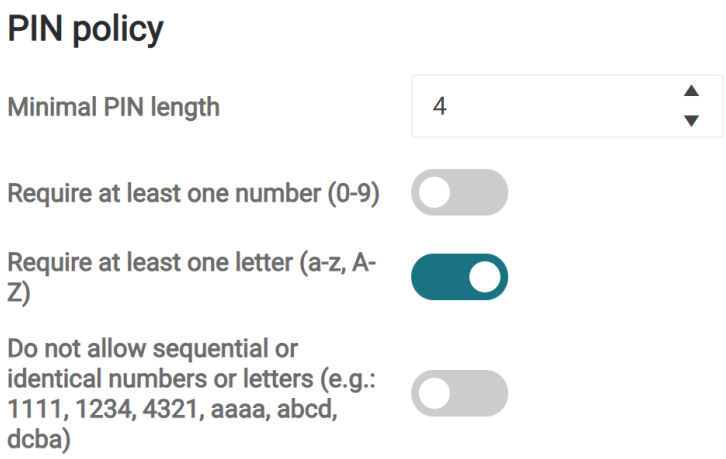
Existing users

When an administrator changes the password policy, it's not applied to existing users. Thus, even after policy edit, the database may retain users with passwords that do not correspond to the policy. The policy will be applied when the administrator or user attempts to change the password (both via UI form or API).

PIN policy

This section is located on the Security Options page under the General tab.

In the PIN policy section, you can create a PIN policy for users.



The minimal PIN length property can't be disabled, and the minimum PIN length can't be less than 4 characters.

Property Do not allow sequential PIN

If enabled, PINs consisting of sequential characters or repeated patterns, such as 1234, 4321, 1111, abcd, AAAA, or ABCD, are automatically disallowed. However, the policy does allow mixed case patterns, such as AbCd, aaAA as these are considered to be more complex and less predictable.

Scope of the policy

The policy applies to all operations where a user's PIN is created or changed:

- administrator edits the user record

- user edits their own profile
- user account is created or updated via the API
- Via a trigger rule. For example, when the user submits their first print job to SAFEQ Cloud.

If the PIN doesn't meet the policy requirements, the operation will be rejected. Errors are displayed at the top of the UI form. When using the API, errors are recorded in the log file.

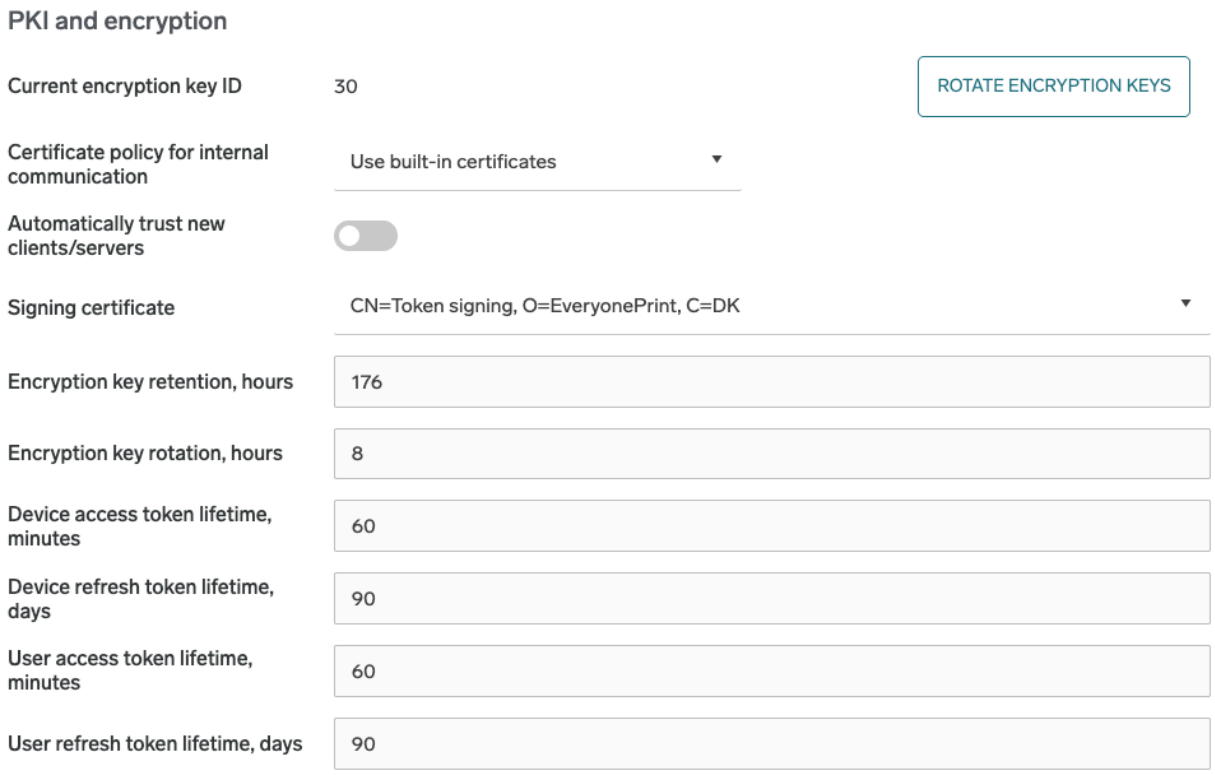
Existing users

When an administrator changes the PIN policy, it doesn't apply to the current PINs of existing users. Therefore, even after the policy has been changed, the database may still contain users with PINs that do not comply with the policy.

PKI and encryption

This section can be found on the Security Options page under the General tab.

In the PKI and encryption section, SAFEQ Cloud server provides several advanced options to configure public key infrastructure and data encryption at rest.



Public key infrastructure settings

For internal communication (the one used to send messages between servers and SAFEQ Cloud clients), SAFEQ Cloud uses either the built-in certificates or the customer-provided certificates.

> ⚠ Customer-provided trusted CA certificates are currently supported only by on-premise primary server installations.

If the *built-in certificates* (default) are used, you must authorize each server or SAFEQ Cloud client connection from the corresponding SAFEQ Cloud Web UI section. You can temporarily disable the authorization by selecting the Automatically trust new clients/servers option.

If the *trusted CA certificates* option is selected, you must configure the account for custom PKI. We assume that you are familiar with the PKI infrastructure, and it is deployed and provisioned on end-user workstations:

- Secondary servers/gateways must be installed in unattended mode with a custom keychain configured in the configuration file (see Installing SAFEQ Cloud unattended/silently for details)
- SAFEQ Cloud clients operating in local storage mode must be installed with the enabled option to use the system (Windows) certificate store.
- Root and intermediate CA certificates for the custom PKI must be uploaded to this account via the Web UI under the Security section > Security options page > Ceritificates tab > Trusted CA certificates part.

Optionally, you can enable OCSP revocation checks for the certificates and configure a custom OCSP URL if the provisioned certificates do not contain it.

You can configure the following settings:

- Certificate policy for internal communication – This option defines which certificates will be used in the internal SAFEQ Cloud communication between servers and SAFEQ Cloud clients.
- Automatically trust new clients/servers – Only applies to built-in certificate policy. When disabled, any new SAFEQ Cloud client/server connections will require manual authorization by the administrator.
- Enable OCSP revocation check – Only visible when trusted CA certificates are used. Enables certificate revocation check via OCSP protocol.
- Custom OCSP URL – Allows specifying custom URL for OCSP service if the provisioned certificates do not contain it.

Signing certificate

The signing certificate signs all device and user tokens.
If signing certificate is changed, then issued device tokens will not work anymore, users will be logged out, terminals and PC Clients in local or hybrid storage mode will be disconnected - they will have to be authorized again.

Data encryption at rest

SAFEQ Cloud server provides transparent encryption for stored documents. The documents in the persistent storage will be encrypted with the randomly generated account key. This applies to primary server, gateways, and SAFEQ Cloud clients.
Keys are rotated automatically and are expired after the specified time. Rotation means that a new key is generated after each "key rotation period" (8 hours by default), which will be used to encrypt new documents. When a particular key is expired (key retention default is 168 hours), it is not possible to decrypt or recover the document which was encrypted with it. When the document is sent to the printer it will be decrypted automatically.

Encryption keys are stored in the central database and are exchanged via the internal secure channel between the trusted servers and/or SAFEQ Cloud clients. Encryption keys are account-specific, so the documents are encrypted per Vendor or Customer account. When the document is encrypted, the account encryption key is combined with the local key specific to a server or

SAFEQ Cloud client. The document can only be decrypted on this particular server or client. **Encryption is enabled by default for all accounts, including existing ones.** The option to disable encryption at rest, which was available in the previous version, has been removed.

You can configure the following settings:

- **Encryption key retention** – the number of hours after which the key expires. The default is 168 (7 days).
- **Encryption key rotation** – the number of hours after which the new key will be generated. The default is 8.

Encryption Retention Policy

Encryption key retention period has to be greater than *Encryption key rotation* + *Scan Job Retention* periods together, in other case it may cause issues with failed scans or scans related to Scan to Download connector. Documents with a deleted encryption key cannot be recovered.

(Encryption key retention) >= (Scan job retention) + (Encryption key rotation)

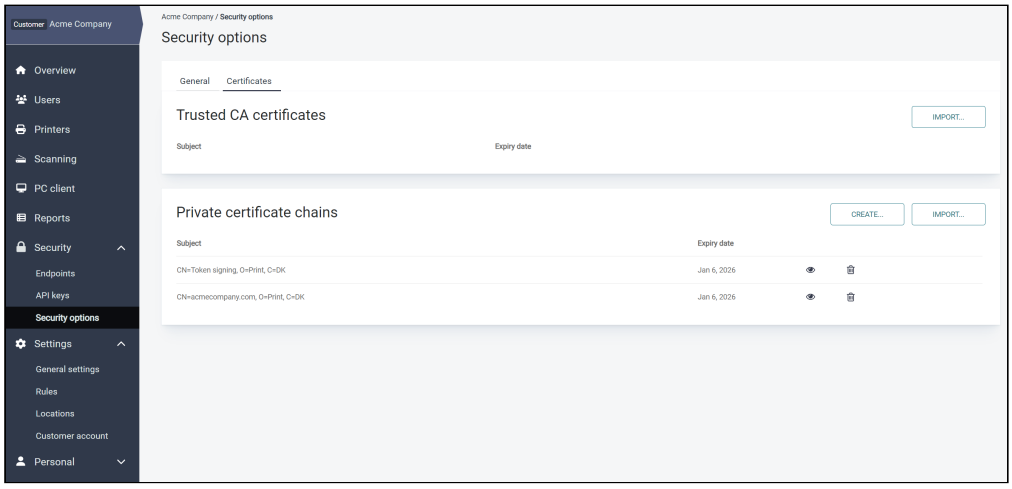
This configuration ensures that scan documents can be decrypted throughout their retention period.

Token lifetime settings

Here you can set lifetimes for device and user access and refresh tokens respectively. Note that the lifetime for access tokens is measured in minutes, while for refresh tokens it is measured in days.

Certificates

The **Certificates** tab allows you to import or create valid SSL certificates for a Vendor or Customer account for use in the various interfaces, including SAFEQ Cloud Web UI, APIs, IPP print, and embedded terminal communications.



Trusted valid SSL certificates are required for HTTPS/IPPS printing from SAFEQ Cloud Client.

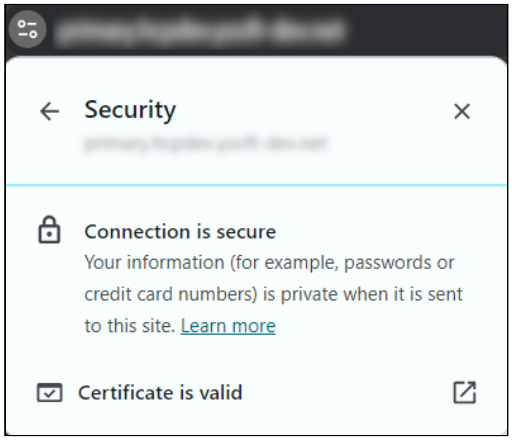
Trusted CA certificates

If the vendor or customer account are their own Certificate Authority (CA) and issue certificates for domain controllers, mail servers etc, those CA certificates can be imported to SAFEQ Cloud for LDAPS and similar.

Export the certificates from the remote server to PEM or DER format, and click **Import** to import the trusted certificate.

> ⚠ The PEM file format can contain multiple certificates in a chain. If this is the case, only the last certificate in the chain (typically the CA certificate) will be imported. During the import process, the certificate is validated to ensure it represents a valid Certificate Authority (CA). The import will fail if the certificate does not represent a CA (i.e. if it is an entity certificate).

Private certificate chains



To enable valid trusted SSL connections from SAFEQ Cloud Client to the SAFEQ Cloud server, either the SAFEQ Cloud Web UI in a Web browser, API connections, IPP printing, or in embedded terminals, import a valid SSL certificate chain in PFX or PKCS12 format.

These formats include both public and private keys required for a server to create the encrypted connection. Certificates without the private key would be ignored during import.

> ⚠ When importing Private certificate chains, both the key pair and the keystore file has to be password protected with the same password.

> ⚠ The certificate chain should contain a valid path from the server certificate to the trusted certificate on the clients.

The following criteria must be matched to be able to import the private certificate chain:

- If the SAN (Subject Alternative Names) are specified, they will be verified against the domains defined in the account.

- If SAN are empty, CN (Common Name) will be verified against the domains defined in the account.
- If both SAN and CN are empty, the certificate import will fail.
- Verification is done as follows:
  - All the DNS names specified in SAN or CN must match at least one of the domains defined in the account.
  - The DNS name may contain a wildcard "*" to allow subdomains (e.g., "SAN=*.test.com" will be valid for the account domain "test.com").
  - It is not possible to import certificates for subdomains (e.g., "SAN=my.test.com" will fail for the account domain "test.com"). However, if you plan to use this subdomain, you can define it in the account information.
  - IP addresses in the SAN are filtered out of the validation; only DNS names are being validated. If the SAN contains only IP addresses, it will be considered empty.

Generating certificate chains

Instead of importing a trusted certificate chain, you can generate it using the default SAFEQ Cloud CA certificate as an issuer. Certificates can be generated for two purposes: TLS server security and token signing. When generating a TLS certificate, select in the drop-down list the domain name to which this chain will be generated. Embedded clients will then be able to connect to this domain name without warning.

> For TLS security, creating a self-signed certificate chain is not recommended and should only be used for test purposes. For proper transport layer protection, a trusted certificate chain created by a trusted certificate authority must be imported.

Generating a certificate chain for token signing

Some external clients require an authorization token when calling SAFEQ Cloud public API functions. The token is only issued when there is a signing certificate chosen in the account's PKI settings. By default, each newly created account has a special signing certificate chain created which is also set as a default signing certificate in the PKI settings. It is possible to re-generate it manually or choose another certificate (e.g., import a trusted chain) for signing purposes.

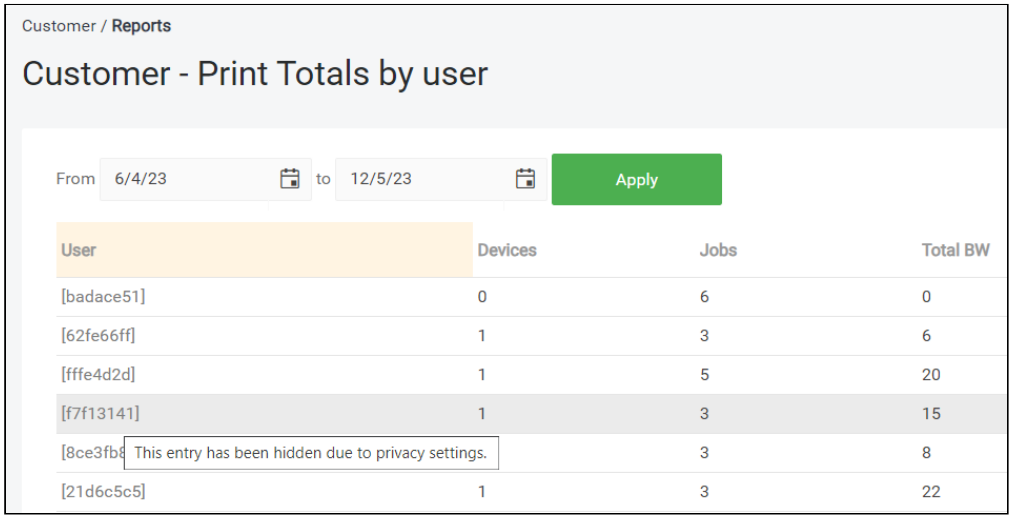
Privacy

This section can be found on the Security Options page under the General tab.

> This setting is available for Customer accounts only.

Use this setting to anonymize the usernames and document names in print reports, print queues, print history panel, top 5 users panel, and others.

When a field is anonymized, the original value is replaced by a random string in braces, and a tooltip is displayed when you hover over it.

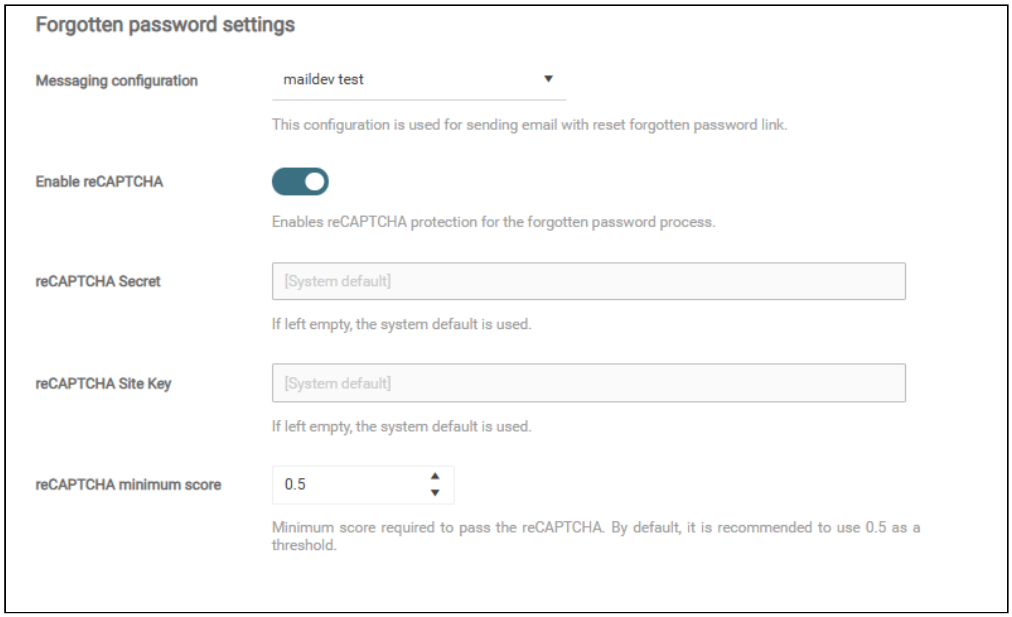


Data hiding in public API

When using public API, the anonymized data are displayed as: "********"

Forgotten password

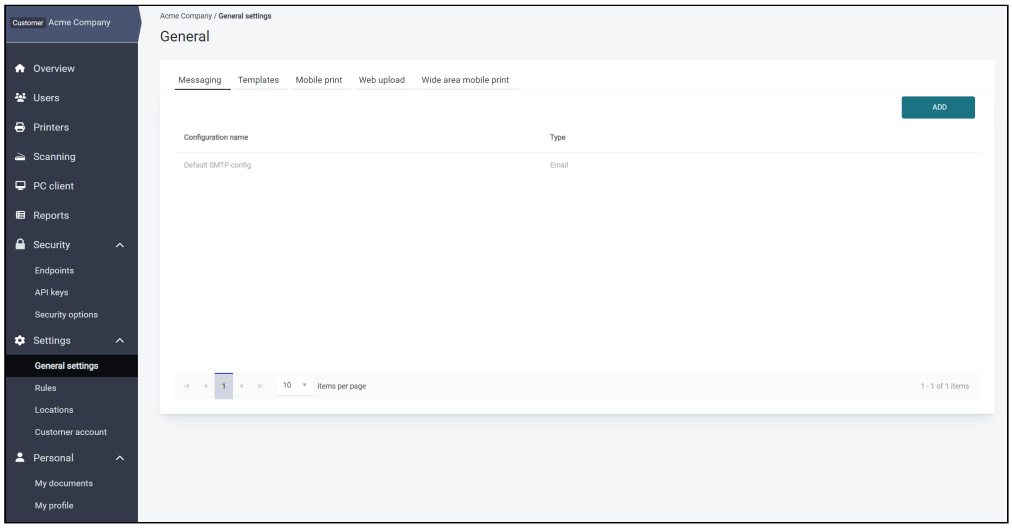
In the Forgotten password section you can setup messaging configuration and reCaptcha settings of forgotten password feature.



1. In **Messaging configuration**, select which of your messaging configurations will be used to send transaction emails to users that requested reset of forgotten password.
2. Enable the **reCAPTCHA** toggle if you wish to use reCAPTCHA protection for the reset forgotten password process. We strongly recommend keeping this option enabled.
3. In **reCAPTCHA Secret**, enter your reCAPTCHA secret if you wish to use your own reCAPTCHA account. If the field is left empty, the system default will be used.
4. In **reCAPTCHA Site Key**, enter your reCAPTCHA site key if you wish to use your own reCAPTCHA account. If the field is left empty, the system default will be used.

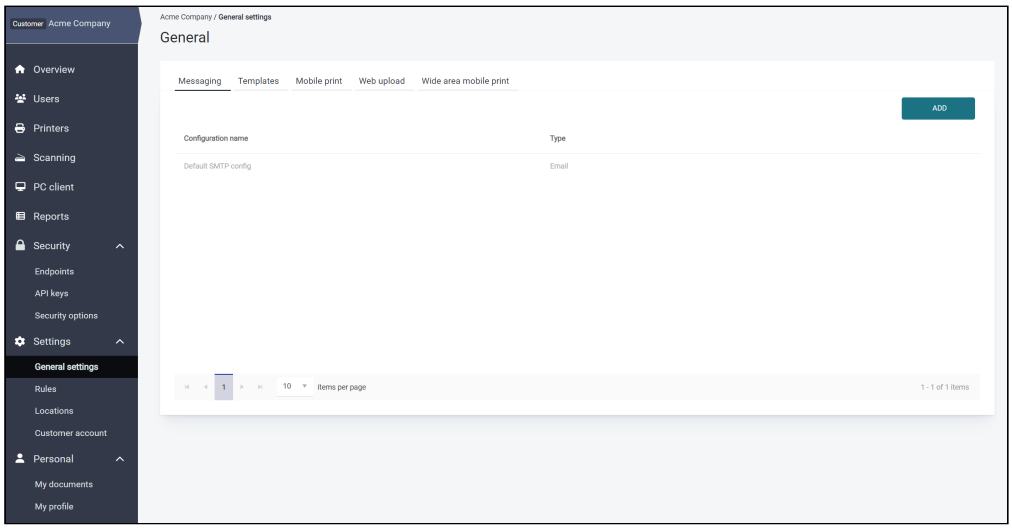
8.1.7 SETTINGS SECTION

The **Settings section** of the application includes pages that allow you to manage **General settings, Locations, Rules** (Triggers and Automations) and **Vendor/Customer account**.



General settings

The **General settings** page of the application includes tabs that allow you to manage **Messaging, Templates, Mobile print, Web upload** and **Wide area mobile print**.



Messaging

Messaging configuration enables YSoft SAFEQ Cloud to deliver messages, such as emails with scanned documents, to users.

A messaging configuration is added for each delivery mechanism, such as an email SMTP delivery. Furthermore, a messaging configuration is required for any SAFEQ Cloud feature that uses email.

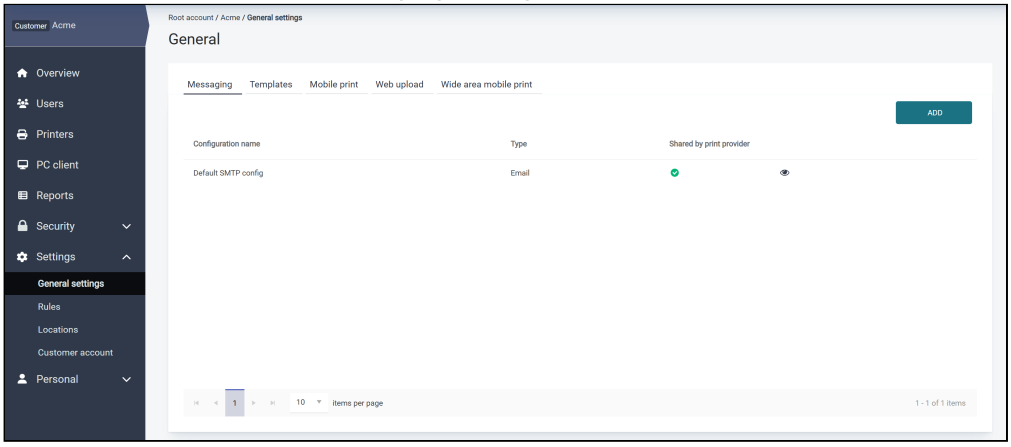
Limitations

Note that SMTP Scan Workflows with the **System default** Messaging email connector used by Pure Cloud terminals utilize the globally available Amazon Simple Email Service (SES SMTP). This service has the following limitations:

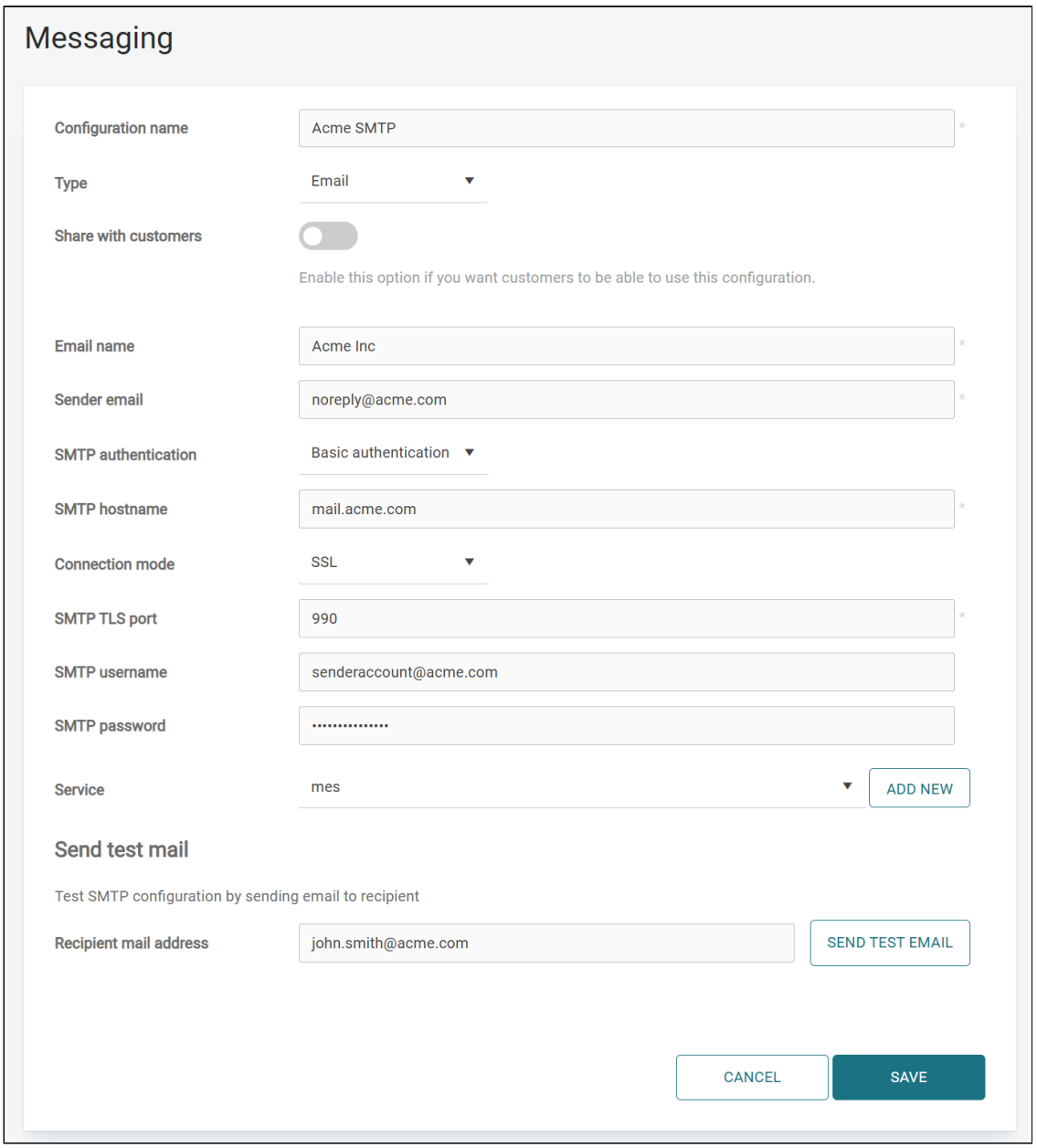
- The maximum size of the email message is 40MB (including images and other types of attachments).
- Messages larger than 10MB are subject to bandwidth throttling. Depending on your sending rate, the service may be throttled for you to as low as 40MB/s. This means that your users would be able to send a 40MB message at the rate of 1 message per second or two 20MB messages per second. Therefore, the scan jobs may not be delivered if your scan workflows generate large files. For these cases, we recommend configuring your own SMTP provider.

Adding a new Messaging configuration

1. Click **Add** to add a new Messaging configuration.



2. Enter the mail servers SMTP settings for outgoing email, including choosing relevant ports and security protocols as needed for the SMTP mail server. Any email service can be used, as long as it supports standard SMTP protocols, including Office365, Google Gmail, Exchange, etc. If a configuration is created or edited by the vendor, you can choose whether it should be shared with customers.



We strongly recommend using a secure **Connection mode**. An insecure mode may expose sensitive data such as scanned documents, usernames, and passwords to potential attackers.

3. Select the Messaging service from the drop-down list that will send the email using the SMTP configuration. If no service is already created, you can add it by clicking **Add**.

4. You can test the settings by entering an email address to receive a test email, and clicking **Send test email**. We recommend you to choose an external test email address, to confirm that SAFEQ Cloud can send emails to all users. The configured message service will deliver the test email from SAFEQ Cloud to the SMTP server, which will then forward it to the recipient.

5. If an error occurs, make sure that:
   - A Message Service has been added to a server.

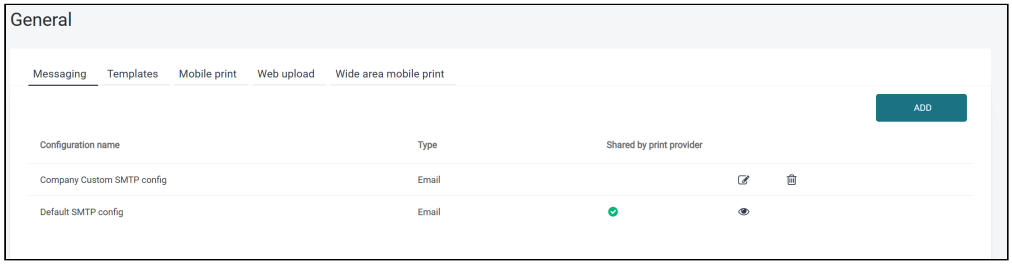
- Firewalls are open from the server hosting the message service and to the SMTP server on the ports used.

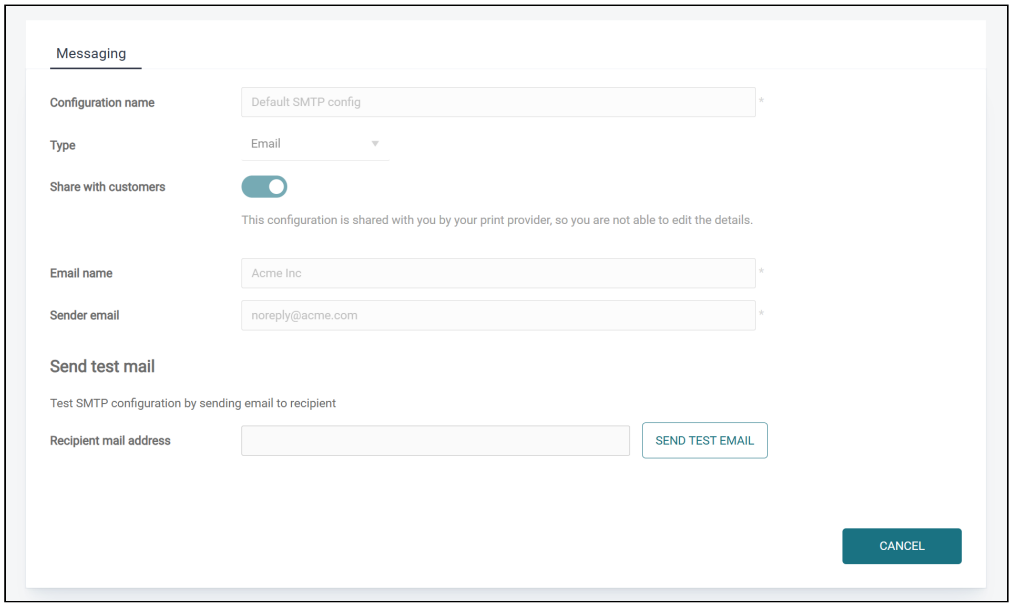
Sharing Messaging configurations with customers

Vendors have the option to share their configuration with customers below them. If a configuration is shared, it is visible and usable by those customers.

Customers cannot edit or delete shared configuration details. Customers can only view sender details and use test mail functionality of shared configuration.

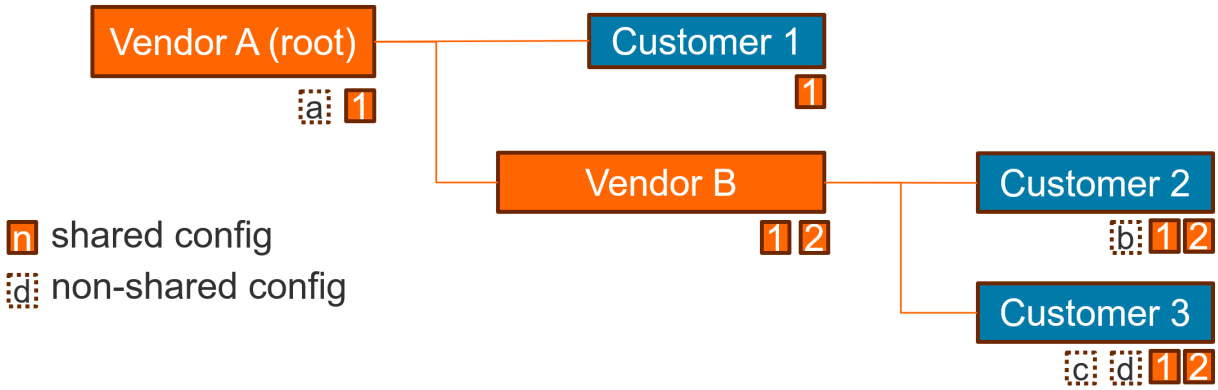
Emails sent by customers using a vendor's messaging configuration will display sender details based on the shared configuration settings.





Customers have access to all shared messaging configurations from the vendors above them. If there is more than one, the configuration closest to the customer is used as the default.

For example, in the diagram below, a new customer under Vendor A will use Configuration 1 as the default, and a new customer under Vendor B will use Configuration 2 as the default.



Vendors should be cautious when disabling sharing for a configuration that was previously shared, as this may require reconfiguring the customers' use of the configuration.

Additionally, the customer may need to create their own configuration if they do not already have a custom one and no shared configuration from the vendor is available.

If the customer has no configuration available, a health check alert will be shown to notify them.

Office365 authentication option

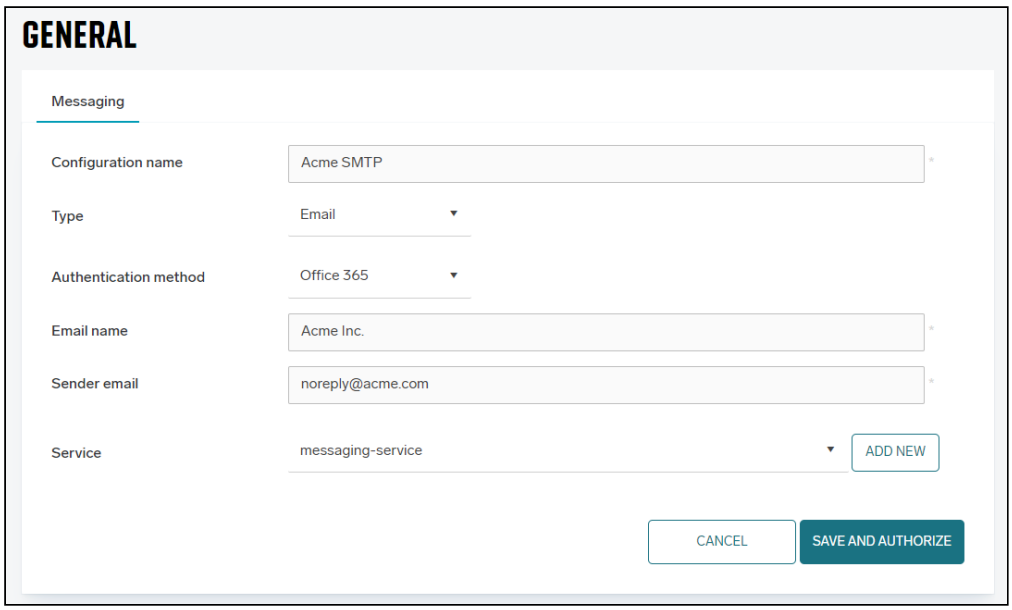
Office365 is one of the available authentication options under the **authentication method** dropdown. It uses OAuth 2.0 as the authorization protocol, and during authorization, you will be redirected to the Microsoft authorization flow (when saving a new Office365 messaging configuration or after pressing the Authorize/Reauthorize button when editing an already created Office365 configuration).

The **Username** field is not visible (or editable when editing) as it obtains the username from the OAuth 2.0 authorization process after it is finished. The fields for hostname, connection mode, and port are static for this option, so they are not shown.

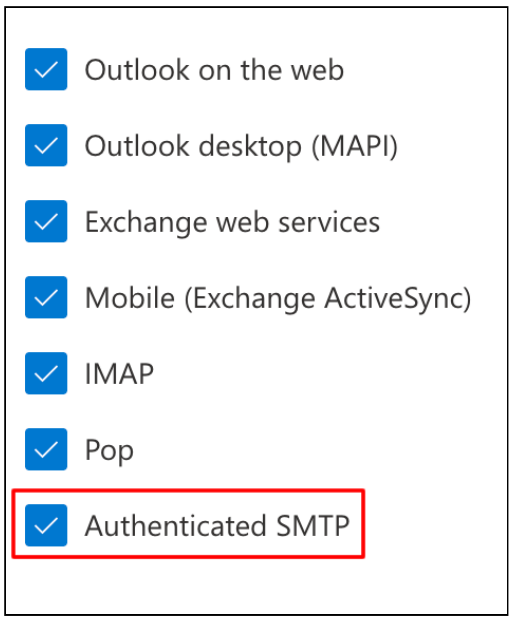
When Office365 is not yet authorized, the **Sending test mail** section is not visible, as it would be able to send emails.

Sender email

Please note: The **Sender email** field is *case sensitive*. If your email is displayed in Entra ID as for example Printing.Notices@myDomain.com it must be entered here in the same format.



For the correct behavior of sending emails, the user who authorizes the configuration through the Microsoft authorization flow has to have enabled the Authenticated SMTP setting in the Microsoft 365 admin center; otherwise, the sending of emails will not work even if the configuration is authorized.



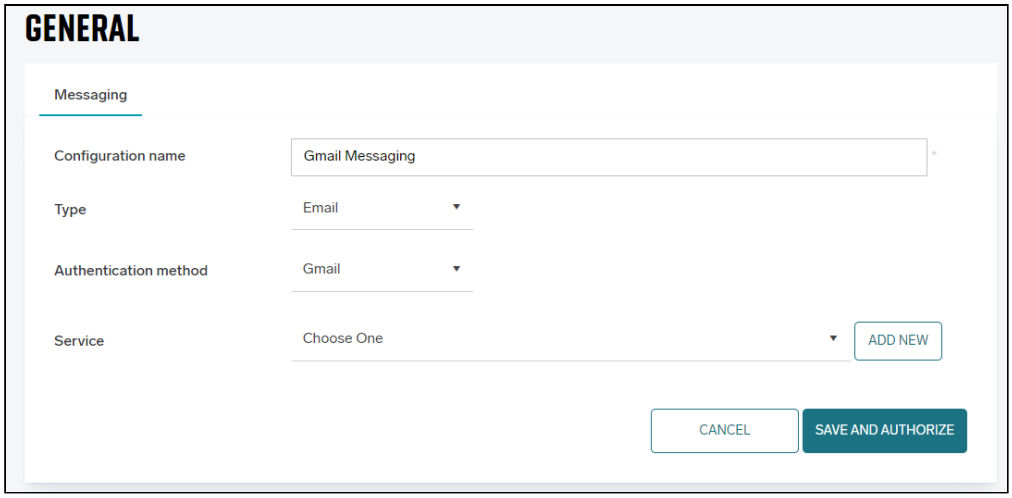
Gmail authentication option

Gmail is one of the available authentication options under the **authentication method** dropdown. It uses OAuth 2.0 as the authorization protocol, and during authorization, you will be redirected to

the Google authorization flow (when saving a new Gmail messaging configuration or after pressing the Authorize/Reauthorize button when editing an already created Gmail configuration).

The **Username** field is not visible (or editable when editing) as it obtains the username from the OAuth 2.0 authorization process after it is finished. The fields for hostname, connection mode, sender email, email name and port are static or obtained from the authorization process for this option, so they are not shown.

When Gmail is not yet authorized, the **Sending test mail** section is not visible, as it would be able to send emails.



Mobile print

Mobile print enables the submission and release of print jobs from Apple iOS and Android devices.

The steps involved in preparing mobile print are:

- Configure Mobile Print (mandatory)
- Wide area mobile print to support Apple devices
- Create QR codes to support release by QR scan (only if using QR codes)

You can also enable upload of documents for print under the Web upload tab.

Configure Mobile Print

Adding the mobileprint service

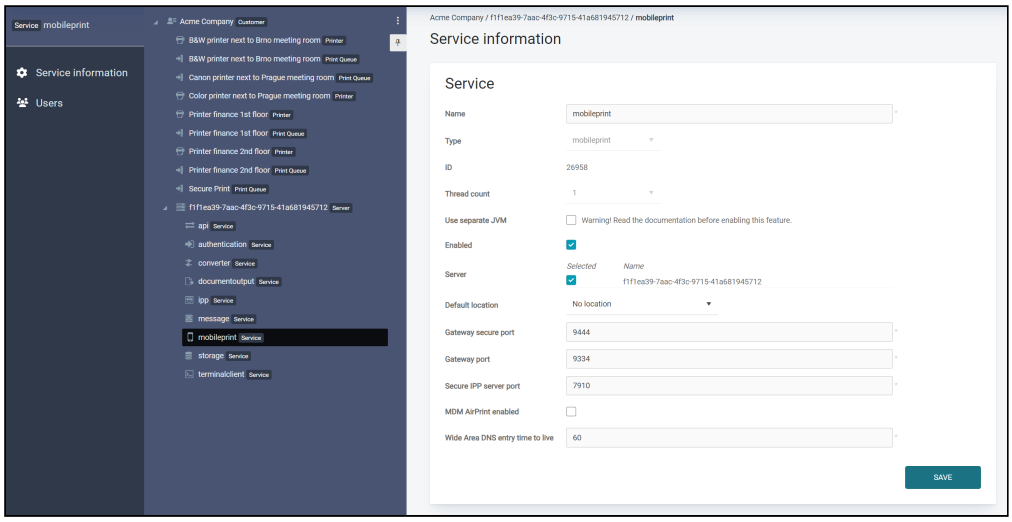
The mobileprint service is added in the Administrator Interface as any other service, as described in this section. The mobileprint service is used to establish the connection between mobile devices and SAFEQ Cloud.

The Mobile Print service depends on:

- Storage Service

- Conversion Service

In the mobileprint service settings, you can edit the following. All default ports are listed in the Ports and Protocols section.



Name
The name is used to identify the mobileprint service in the SAFEQ Cloud Web UI.

Enabled
Enable or disable the service

Gateway secure port
The secure (SSL) port of the SAFEQ Cloud server encrypts all communication.

Secure IPP server port
The secure (SSL) IPP server port encrypts all communication. IPP server is a component of SAFEQ Cloud.

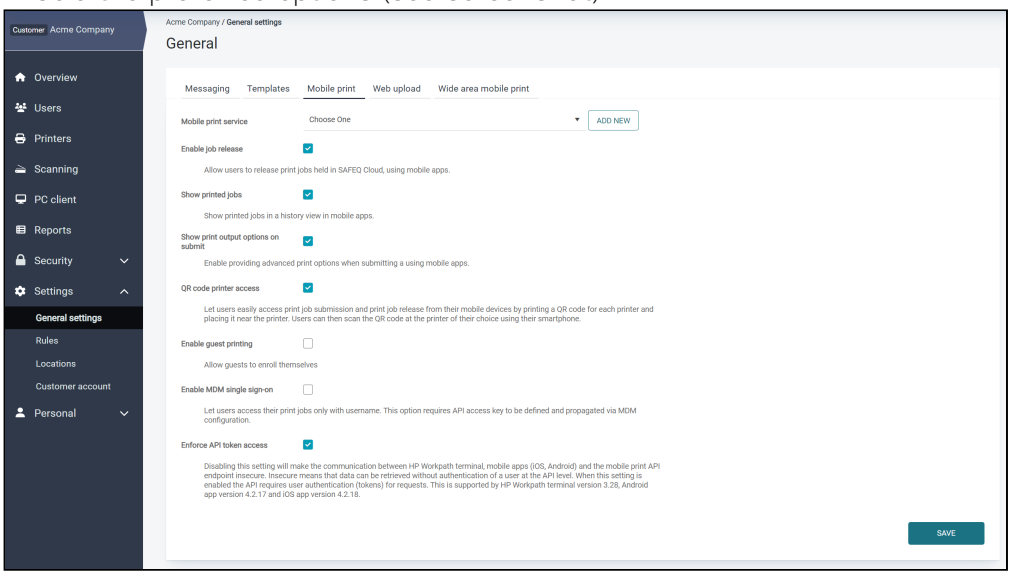
MDM Airprint enabled
This option allows the gateway to support AirPrint printers deployed via MDM (Mobile Device Management) providers. This requires the gateway to occupy port 443 as the encrypted endpoint for IPP communication. Hence, port 443 must not be taken already on the host system. Restart the gateway after toggling this setting.

Wide Area DNS entry time to live
This option allows you to change the TTL value that is used for printer announcements made via DNS-SD. The default value is 60 seconds. This setting will be picked up on the next refresh of the DNS zones, which happens every 2 minutes.

Configure Mobile Print

1. Go to the **Settings** > **General settings** and tab **Mobile print**.
2. Choose a predefined mobile print service to be used. If no service is created, it can be added using the **ADD NEW** button.

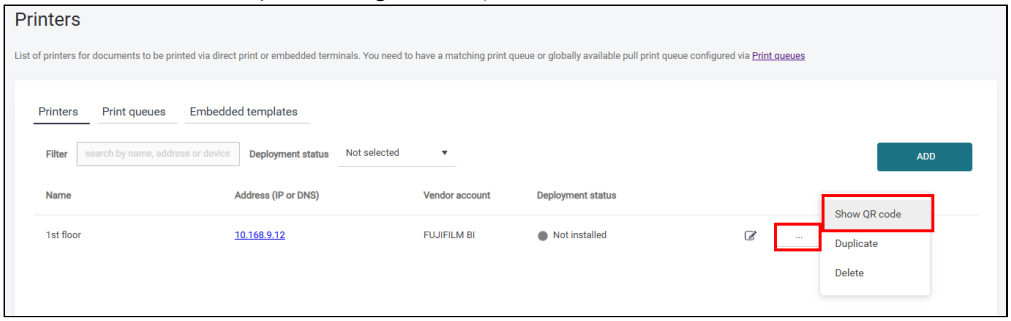
3. Enable the preferred options (see screenshot).



Creating QR-codes

Place the QR codes on your MFDs so that users can release their print jobs submitted via the Mobile app.

1. Go to **Settings** > **Customer account**. Click the **Advanced** tab.
2. Write your text in the **Mobile release printer QR code text** field. The text will appear in combination with the printer name when a QR code is scanned.
3. Go to the **Printers** menu and locate the printer(s) that will support QR-code release.
4. Click the **QR-code** button to see the code specific to that printer (every printer you add to the list will automatically be assigned a QR code).



5. Print the QR code, for example, as a sticker, and place it on the printer.

Limitations for releasing a print job using mobile app:

- only works for MFDs that are accessible from a primary or secondary (gateway) server.

Mobile apps: configure DNS-SD for _discovermobile

YSoft SAFEQ Cloud Mobile Apps for iOS and Android are able to discover the Gateway address automatically using a specific DNS-SD service entry named "_discovermobile"

Configure Windows DNS

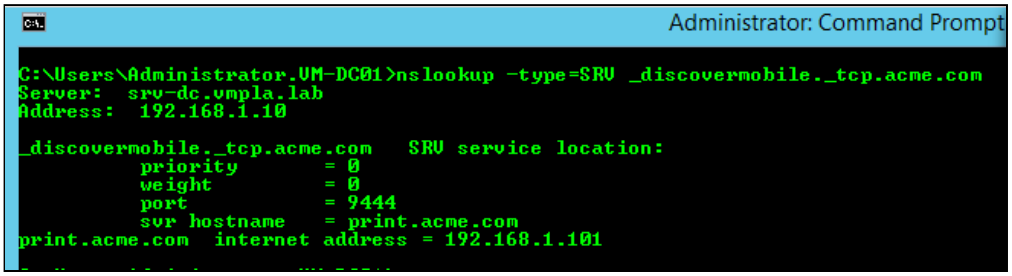
1. Right click the domain and select "Other New Records..."
2. In the "Resource Record Type" window, scroll down, select "Service Location (SRV)" and click "Create Record..."
3. Enter values:
   a. Service: _discovermobile
   b. Protocol: _tcp
   c. Leave Priority and Weight to default: 0

d. Port number: 9444

e. Host offering the service: gateway-name.domain.ext

Verify DNS-SD

1. On Windows:
   - Open a CMD
   - Type: nslookup -type=SRV _discovermobile._tcp.domain.ext



2. On the SAFEQ Cloud Gateway
   - Launch the following script: $ discovermobile.sh

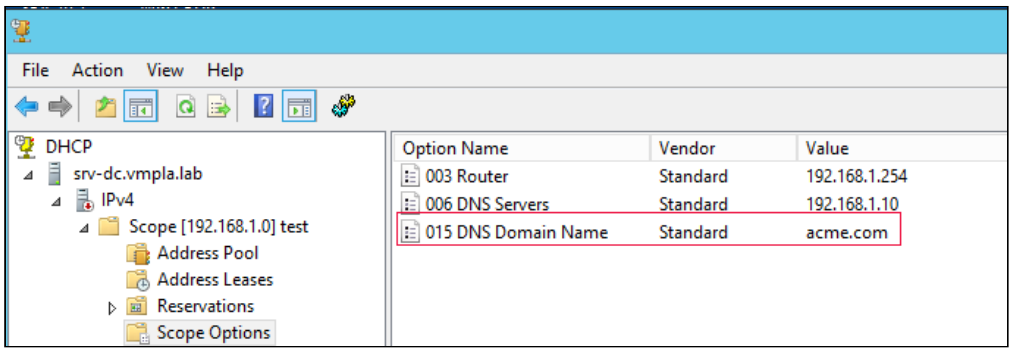
- Enter the domain name : domain.ext

```
    Discovermobile announcement

----------------------------------------
    Domain name ?
----------------------------------------

Enter value:acme.com
Server:         192.168.1.10
Address:        192.168.1.10#53

_discovermobile._tcp.acme.com   service = 0 0 9444 print.acme.com.
```

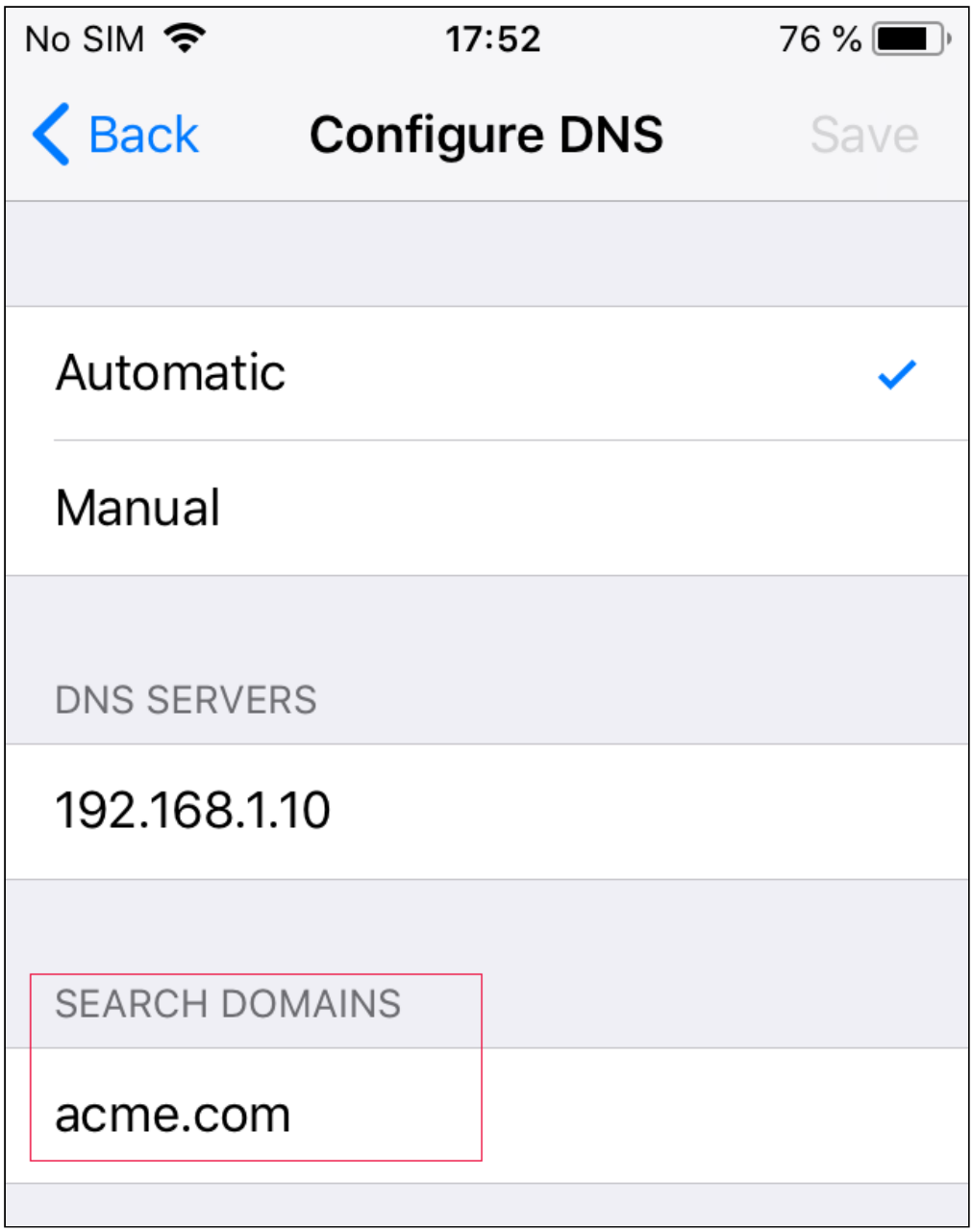
Pre-requisites for successful discovery

iOS devices:

The iOS WiFi settings need to be set up with the proper "search domain"; this is auto-configured by the DHCP server, using Scope Option 015.

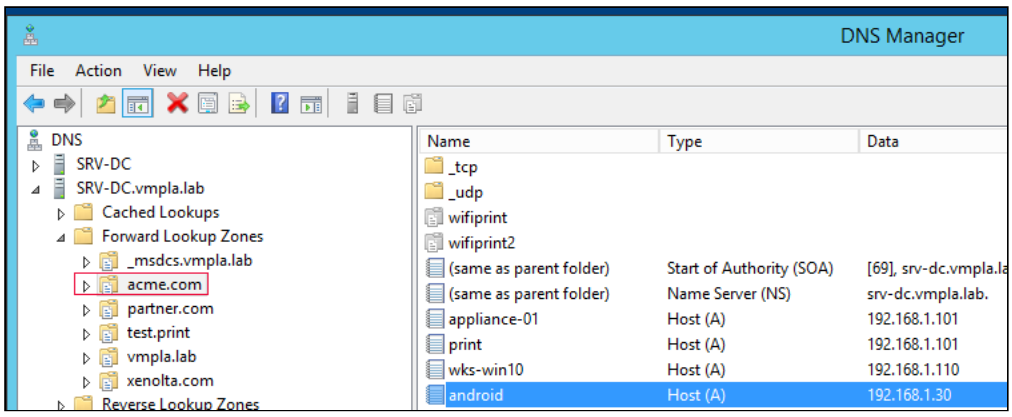


You can verify this is working fine in the iOS WiFi settings: select the WiFi connection, tap the (i) then -> DNS.



Android devices:

Android devices are not implementing the 'Search Domain' settings; for the _discovermobile SRV retrieval to work, the Android devices must be registered within the correct domain in the DNS server.



Configure the Mobile Apps with the Mobile Device Management

Mobile Device Management, hereafter abbreviated as MDM, can help you with the following tasks:

- Deploying mobile apps on devices
- Managing the deployed mobile apps
- Configuring the mobile app options

Prerequisites

- Configured MDM solution
- Mobile device that is enrolled in the MDM

Configuration

Use the following apps' IDs to start managing the mobile apps.

- Android: com.ysoft.ysoftsafeq
- iOS: id1617032214

Then you can use the following examples to import the configuration options into your MDM solution and replace individual options with your values or enter the wanted configuration options from the table below manually.

For Android:

Cloud environment config example

```
{
  "domain_name": "REPLACE_DOMAIN"
}
```

Alternative environment config example

```
{
  "client_id": "REPLACE_WITH_CLIENT_ID",
  "issuer": "REPLACE_WITH_ISSUER",
  "api_server": "REPLACE_WITH_API_SERVER"
```

```
}
```

For iOS:

Cloud environment config example

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>user_domain</key>
    <string>REPLACE_WITH_USER_DOMAIN</string>
</dict>
</plist>
```

Alternative environment config example

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>issuer</key>
    <string>REPLACE_WITH_IDENTITY_PROVIDER_URL</string>
    <key>api_server</key>
    <string>REPLACE_WITH_API_ENDPOINT</string>
    <key>client_id</key>
    <string>REPLACE_WITH_CLIENT_ID</string>
</dict>
</plist>
```

Available options to configure apps' values from the login form:

Managed Cloud Environment Configuration Value	Required	Data Type	Default Value	Example	Explanation
domain_name	yes	String	—	"your.domain"	Address of your cloud print management solution.

Managed Cloud Environment Configuration Value	Required	Data Type	Default Value	Example	Explanation
client_secret	optional	String	—	"XZmTxYCdMZJRNurFGzTeeZVsJql"	API key that authenticates the app.
fully_managed	optional	Bool	true	true	Disables any user interaction with the login form when set to true.

Managed Alternative Environment Configuration Value	Required	Data Type	Default Value	Example	Explanation
issuer	yes	String	—	"https://your.domain/oauth/v1"	Identity provider URL
api_server	yes	String	—	"https://your.domain"	API endpoint
client_id	yes	String	—	"mobile-client"	Client ID
client_secret	optional	String	—	"XZmTxYCdMZJRNurFGzTeeZVsJql"	API key that authenticates the app.
allow_invalid_certificates	optional	Bool	false	false	Disables validation of the server certificates when set to true.
fully_managed	optional	Bool	true	true	Disables any user interaction with the login form when set to true.

Limitations

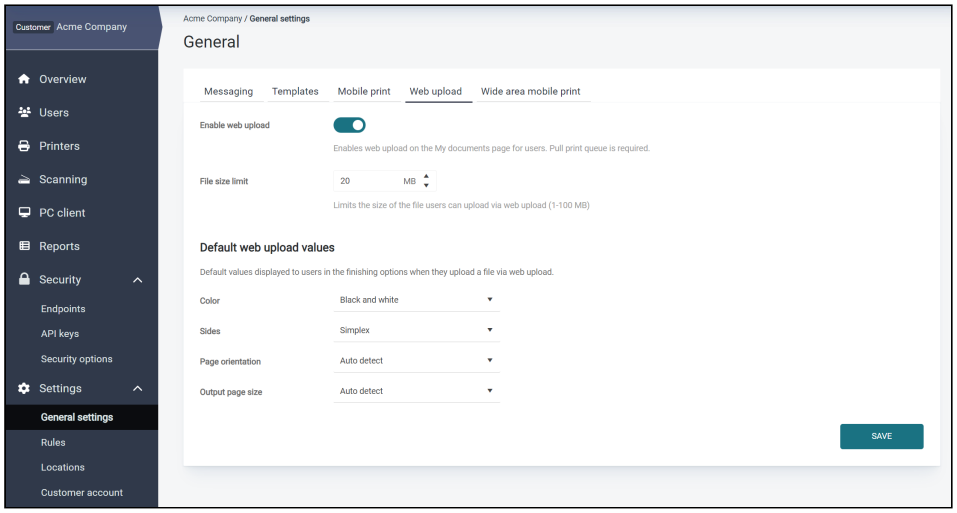
If you deploy a valid configuration for both – cloud and alternative environment – only cloud environment will be set.

If you don't deploy all the required values, managed configuration won't be used.

Deploying new configuration will log out already logged-in users and apply the newly deployed values on Android.

Web upload

On this tab in **Settings** > **General settings**, you can enable and configure the document upload functionality. Users can then use this functionality to upload documents for print at **Personal** > My documents page.



- **Enable Web upload** - If enabled, users will see the Web Upload widget on the **Personal** > **My documents** page, provided the other requirements, mentioned in My documents > **Document upload** section, are met.
- **File size limit** - Set the maximum document size that users can upload. The default value is 20MB. The maximum value is 100MB.
- **Default Web upload values** - Configure the default values for the finishing options shown to users in a modal window after they upload a document. The available options are: Color, pages, page orientation, and output page size.

Limitations for uploading the MS Office files:

- Print preview of one Microsoft Excel file can contain at most 10 thousand pages.
- The duration of conversion from MS Office files to PDF is limited to 5 minutes.

If the user exceeds any of these limitations, it will result in conversion failure.

Limitations for non-PDF/A documents:

- Only standard fonts are supported. Documents containing non-standard fonts may result in the printed document looking different from the original.

Wide area mobile print

Wide area mobile print is a highly flexible and powerful alternative to Apple's multicast DNS Bonjour method of announcing printers to Apple iOS devices.

Wide area mobile print uses Unicast DNS-SD, and announcing available printers in SAFEQ Cloud to Apple iOS devices, can be achieved with extreme ease using the Wide area mobile print feature combined with simple standard DNS records created on the DNS server. With Wide area mobile print, AirPrint can be enabled across large and complex networks.

There is a built-in DNS server which must be reachable from mobile devices if you wish to use Wide area mobile print.

The Wide area mobile print configuration involves the following overall steps, explained in the following sections:

- Create one or more Wide area mobile print sub domains in the Administrator Interface
- Configure the network DNS server
- Set search domain on mobile devices

Configure DNS server

For each created Wide area mobile print sub domain, the DNS requests for those sub domains, should be delegated to SAFEQ Cloud, so SAFEQ Cloud can respond with relevant printer details for the sub domains.
For more information about Zone Delegation, refer to the following articles:

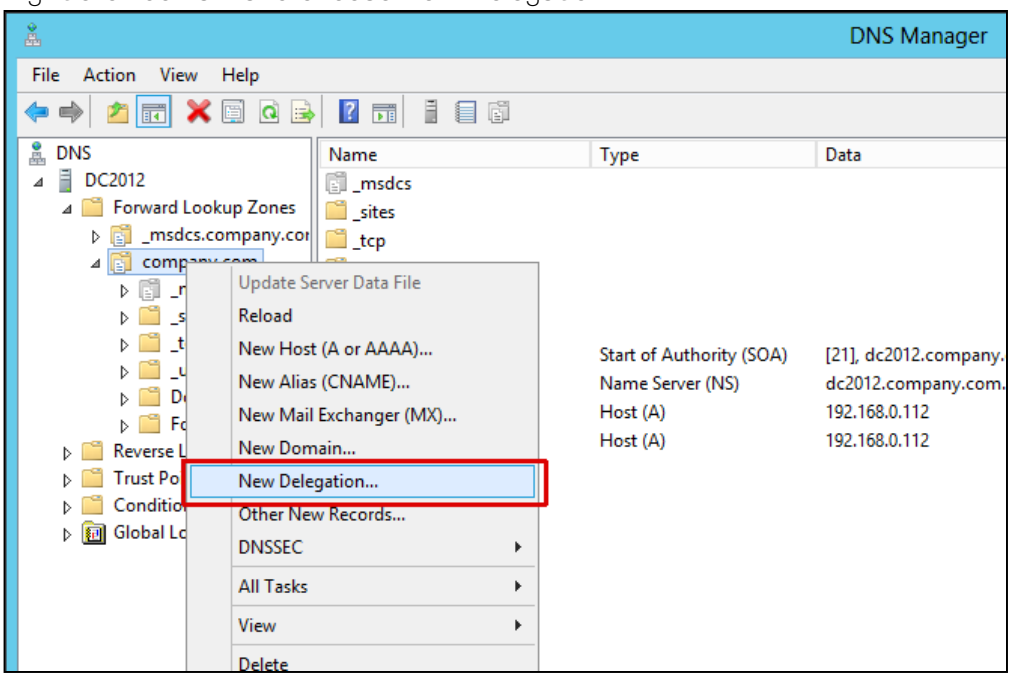
Wikipedia: DNS zone
Microsoft: Understanding zone delegation
Microsoft: Create a zone delegation

For example configurations of the zone delegation, refer to below two sections on Microsoft Windows DNS BIND (Mac OSX or Linux).

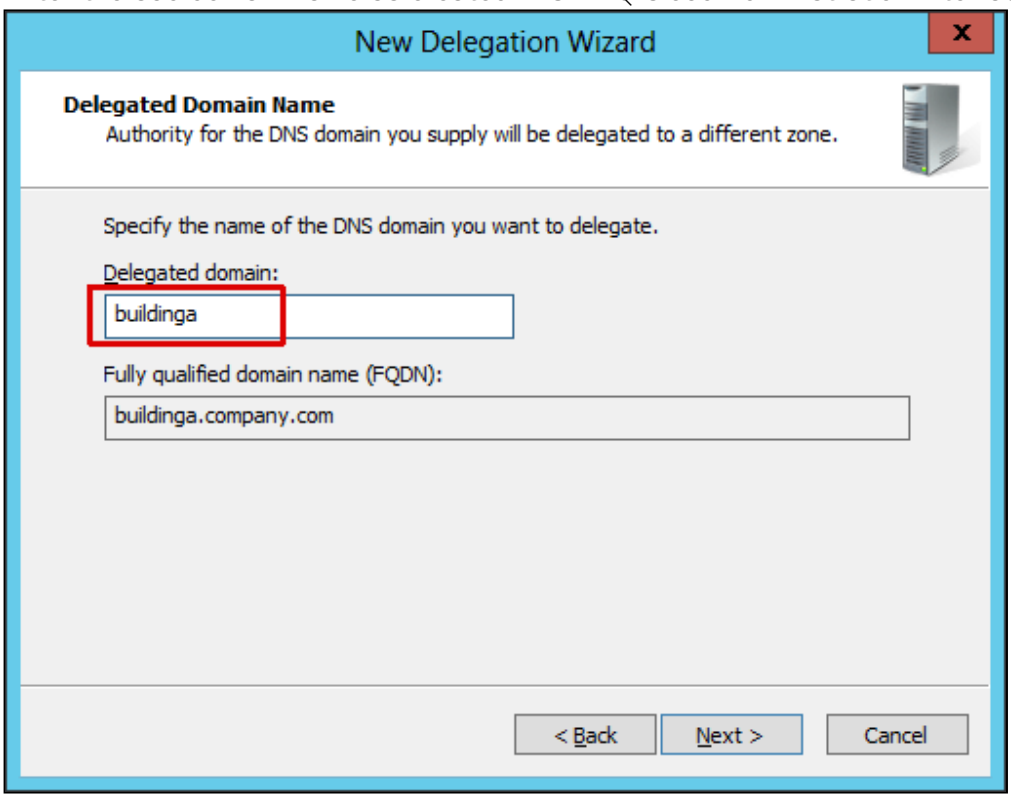
Configure Windows DNS

To configure zone delegation for the created Wide Area Mobile Print subdomains on Windows DNS, open Windows DNS on the DNS server that mobile devices use.

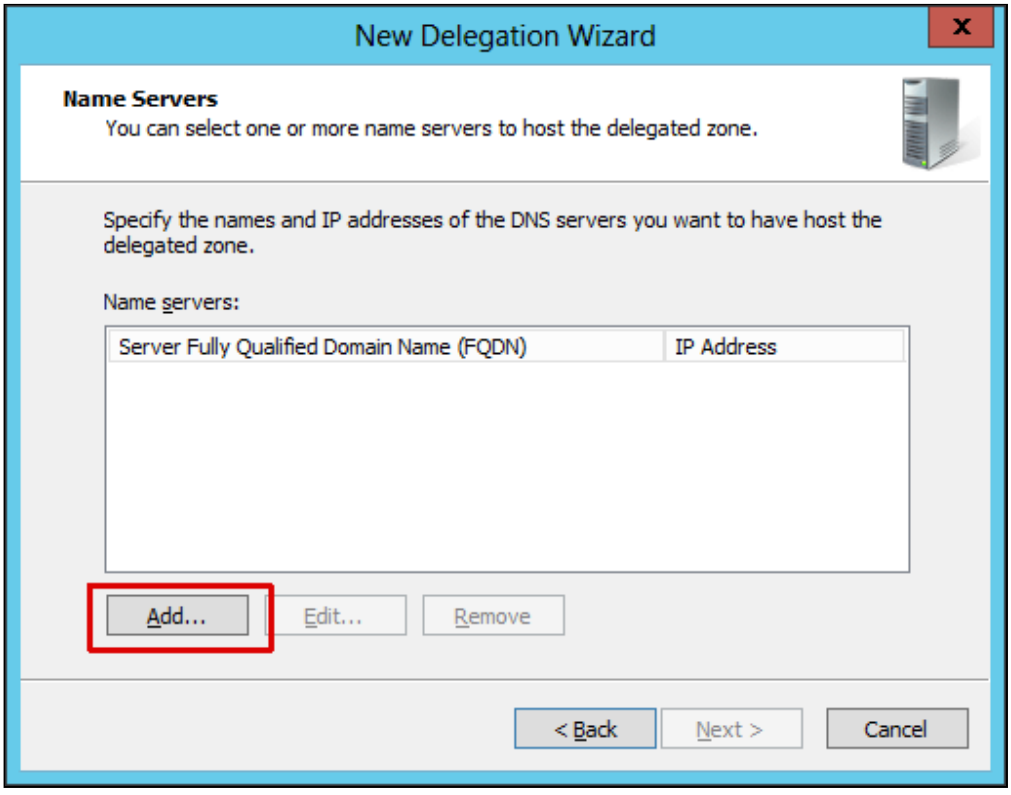
1. Right-click domain and choose New Delegation.



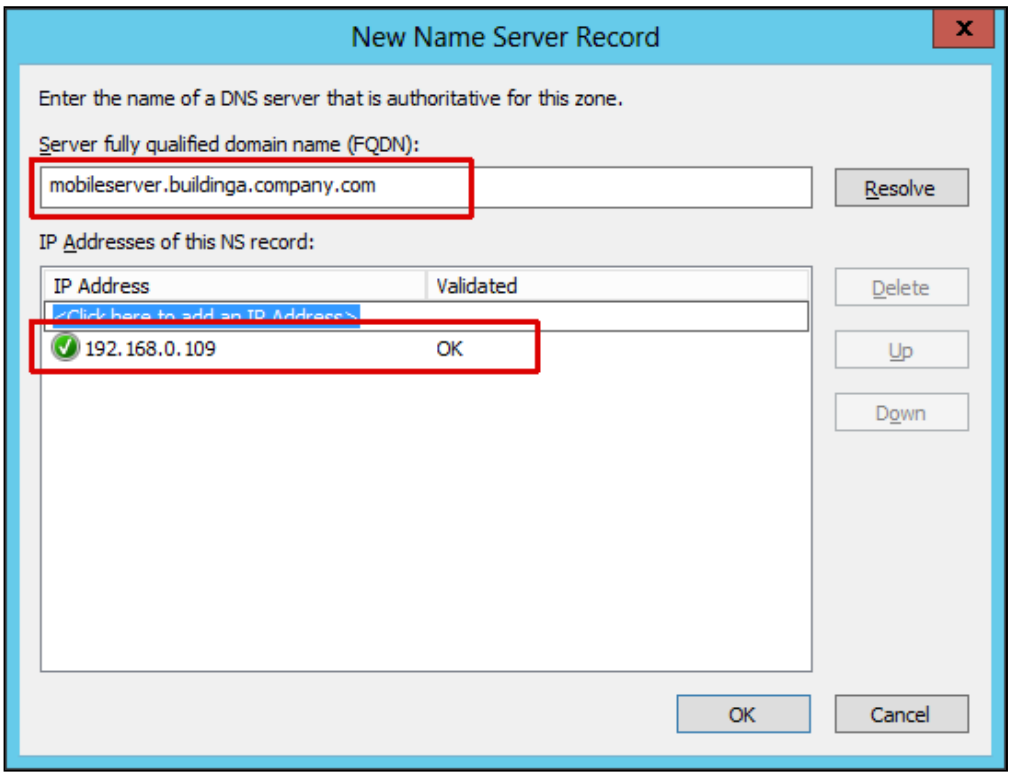
2. Enter the sub domain name as created in SAFEQ Cloud Administration Interface



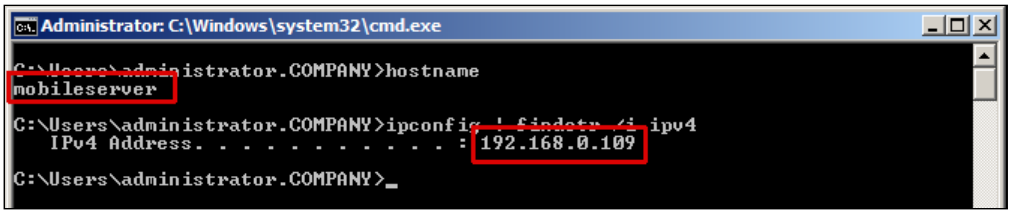
3. Choose to Add a name server



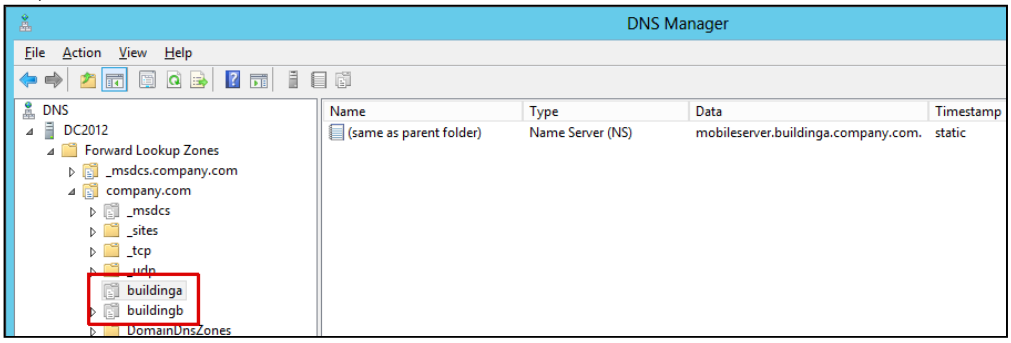
4. Enter the server **name/hostname** of the SAFEQ Cloud server/gateway where the Mobile print service is installed, followed by the Wide Area Mobile Print subdomain and Active Directory domain, and then enter the **IP address** of the SAFEQ Cloud server/gateway.



In this example, the hostname of the SAFEQ Cloud server is "mobileserver" and its IP address is 192.168.0.109



5. Repeat for each created subdomain



Configure BIND

Configure zone delegation for the created Wide Area Mobile Print subdomains on BIND running on Mac OSX or Linux, by adding the subdomains to the domains master zone file.

1. In this example, the subdomains are added to the BIND master zone file for the domain "company.com".

```
;
; Zone file for company.com
;
$TTL 360
@       IN      SOA     ns.company.com. root.company.com. (
                        201404011       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds

                NS      ns              ; Inet Address of name server
ns              A       192.168.0.139

; Delegation for Wide Area Mobile Print sub domains
$ORIGIN buildinga.company.com.
@       IN      NS      mobileserver.buildinga.company.com.
mobileserver IN      A       192.168.0.109

$ORIGIN buildingb.company.com.
@       IN      NS      mobileserver.buildingb.company.com.
mobileserver IN      A       192.168.0.109

$ORIGIN buildingc.company.com.
@       IN      NS      mobileserver.buildingc.company.com.
mobileserver IN      A       192.168.0.109
```

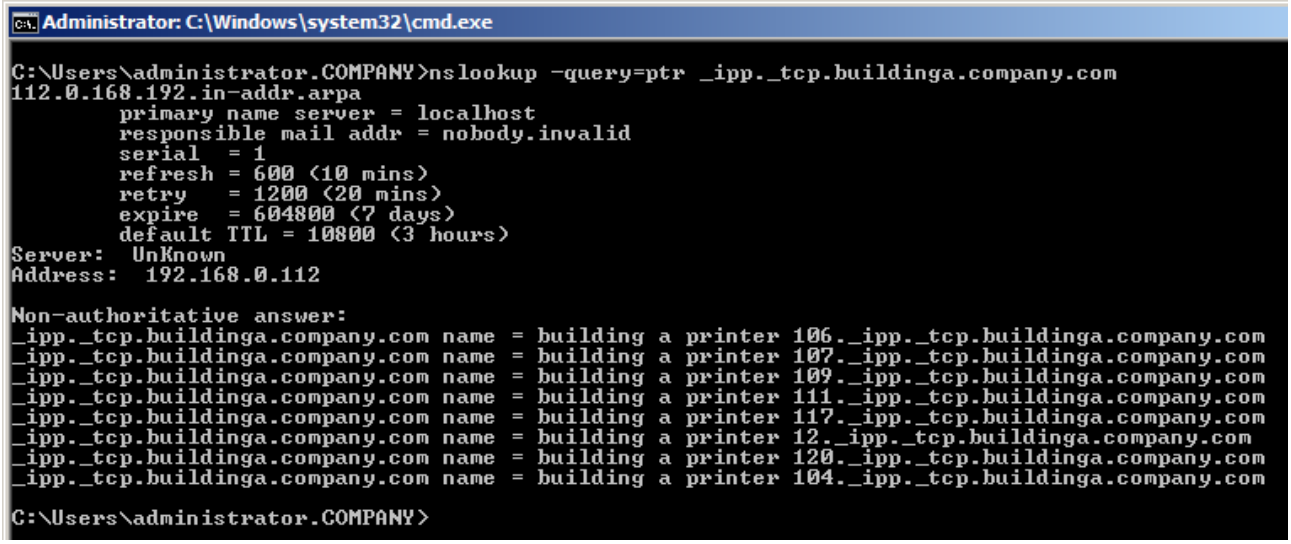
Now any DNS requests for one of the subdomains to the primary DNS server will be forwarded to SAFEQ Cloud.

Verifying DNS configuration

To confirm the proper DNS configuration with either Windows DNS or BIND on Mac OSX or Linux, run the nslookup command for each of the sub domains:

```
nslookup -query=ptr _ipps._tcp.buildinga.company.com
```

If successfully configured, this will return a list of the printers in the sub domain as configured in SAFEQ Cloud.

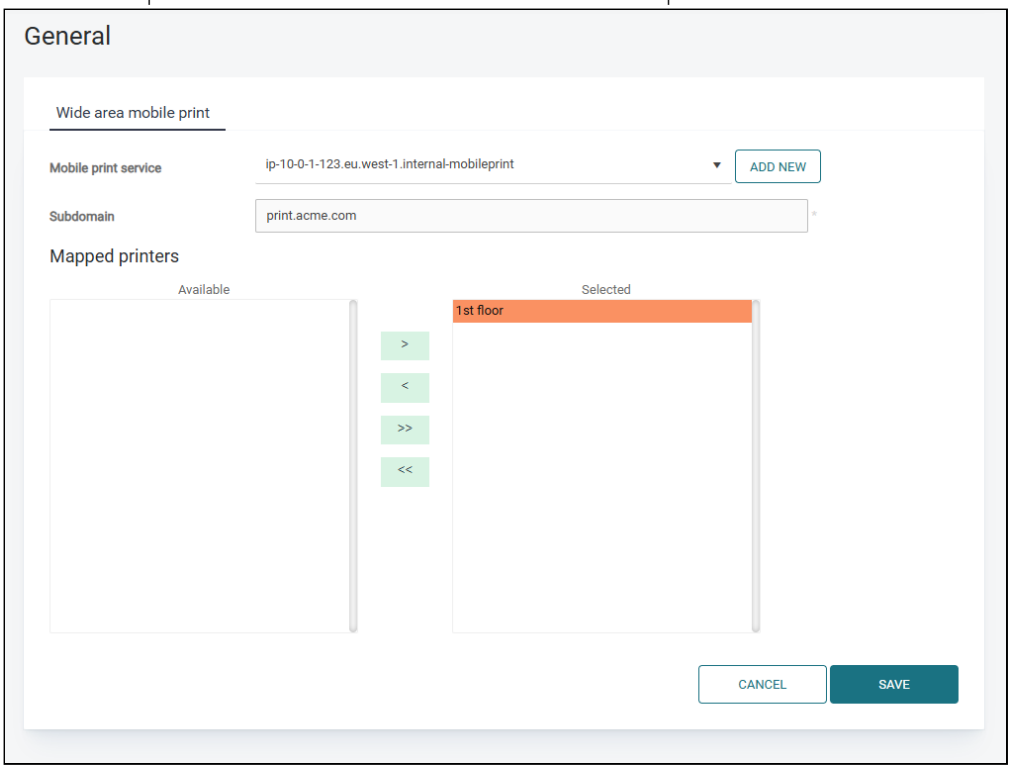


Nslookup result from Windows

Create Wide area mobile print subdomains

You can create multiple sub-domains, to separate access to printers, for example by location (one subdomain per building, campus, city, department) or by user access level (one subdomain for employees, another subdomain for guests).

1. Go to the **Settings** > **General Settings**, tab **Wide area mobile print** tab and click **Add.**
2. Select the mobile print service to be used. In case no service is already created, it can be added using the Add button.
3. Input the sub domain
4. Select the printers to be made available for mobile print



5. Click **Save**.

Set search domains on mobile devices

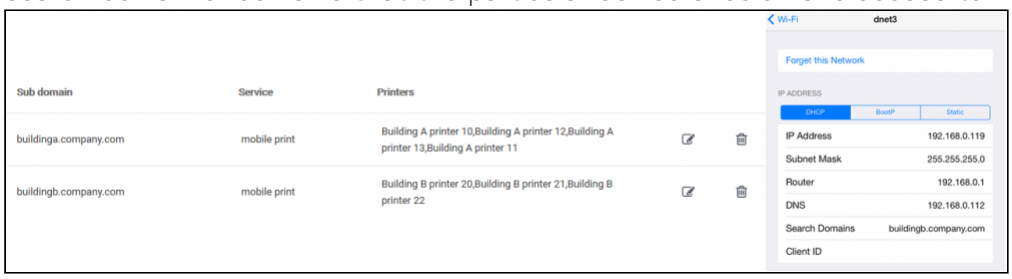
For Apple iOS mobile devices to retrieve the printers available for Wide Area Mobile Print, the iOS devices must be instructed to query the sub domains, using DNS-SD.
This can be done in one of two ways, depending on one or multiple sub domains having been created in SAFEQ Cloud.

- Configuring for One Wide Area Mobile Print sub domain
- Configuration for Multiple Wide Area Mobile Print sub domains

Multiple Wide area mobile print subdomains

If multiple Wide area mobile print subdomains have been created, access to the subdomains on Apple iOS devices is given, by populating the "search domain" on the mobile device, with the

search domain or domains that the particular device should have access to.



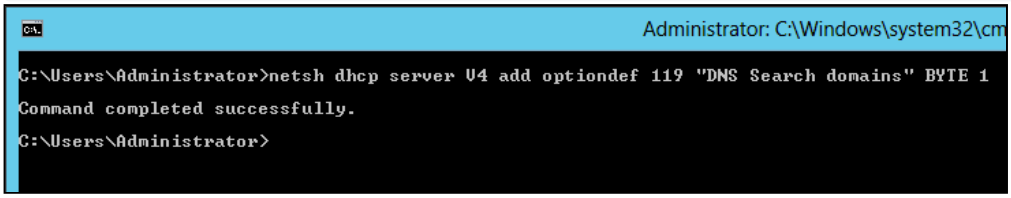
This can be done either manually, or by having the DHCP server provide this value, using what is called "DHCP option 119".
See below sections for instructions on how to populate "search domain" using Windows and Linux DHCP.

Multiple subdomains configuration on Windows DHCP

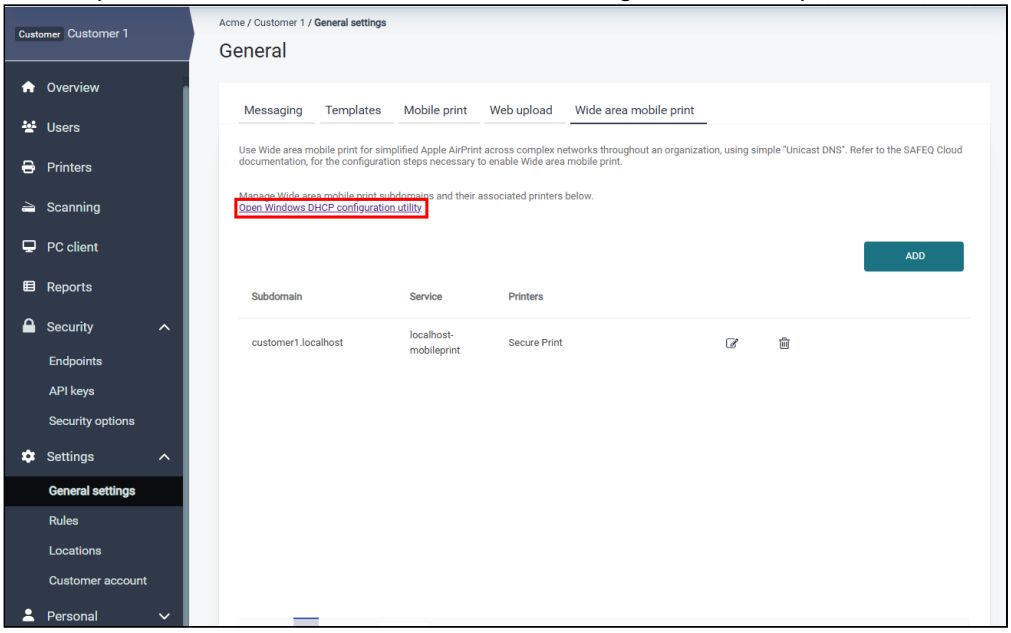
Microsoft Windows DHCP does not provide a friendly configuration interface for the DHCP option 119.
Configuration of DHCP option 119 on Windows DHCP involves the following steps:

1. If not done previously, first define the DHCP option 119 to the Windows DHCP server by running the following command on the DHCP server

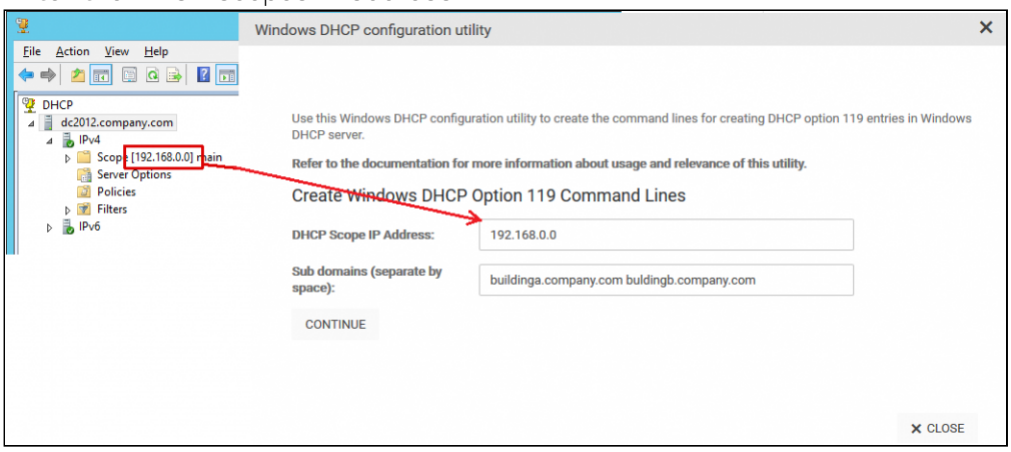
```
netsh dhcp server V4 add optiondef 119 "DNS Search domains" BYTE 1
```



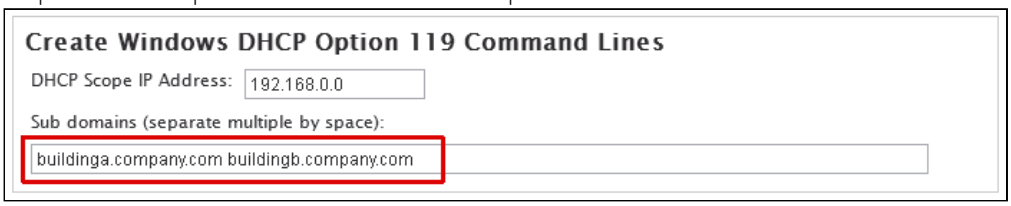
2. In the SAFEQ Cloud Administrator interface, go to **Settings** > **General settings**, tab **Wide area mobile print** and click the **Windows DHCP Configuration Utility**



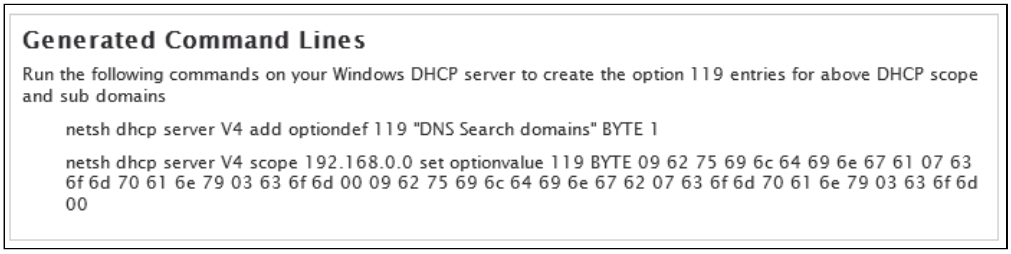
3. Enter the DHCP scopes IP address



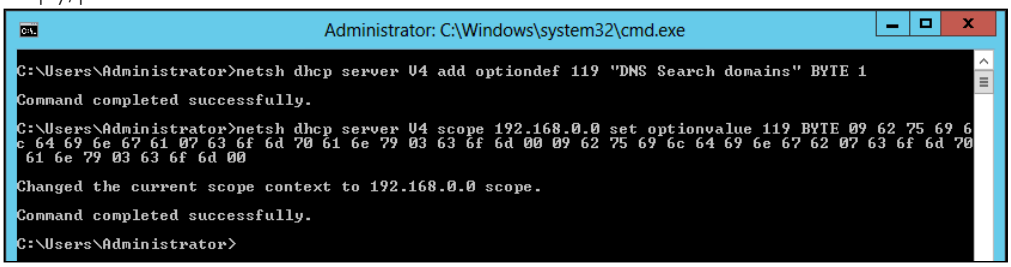
4. Enter the Wide area mobile print subdomains that should be published to this DHCP scope. Separate multiple subdomains with a space.



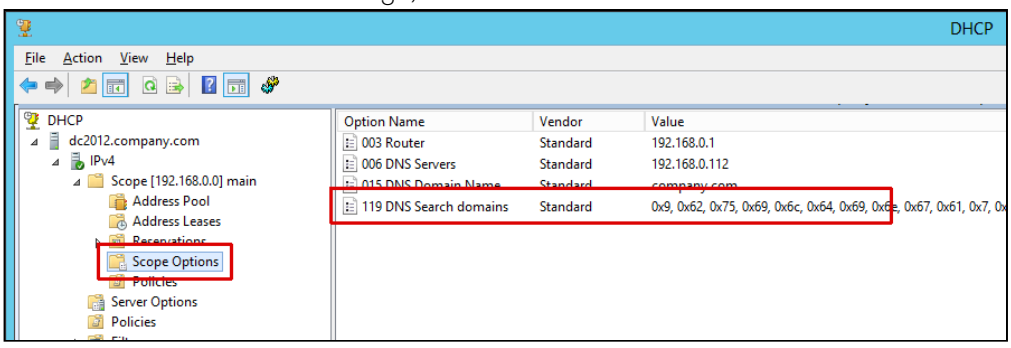
5. Click **Continue** when ready, and the needed commands are shown on screen



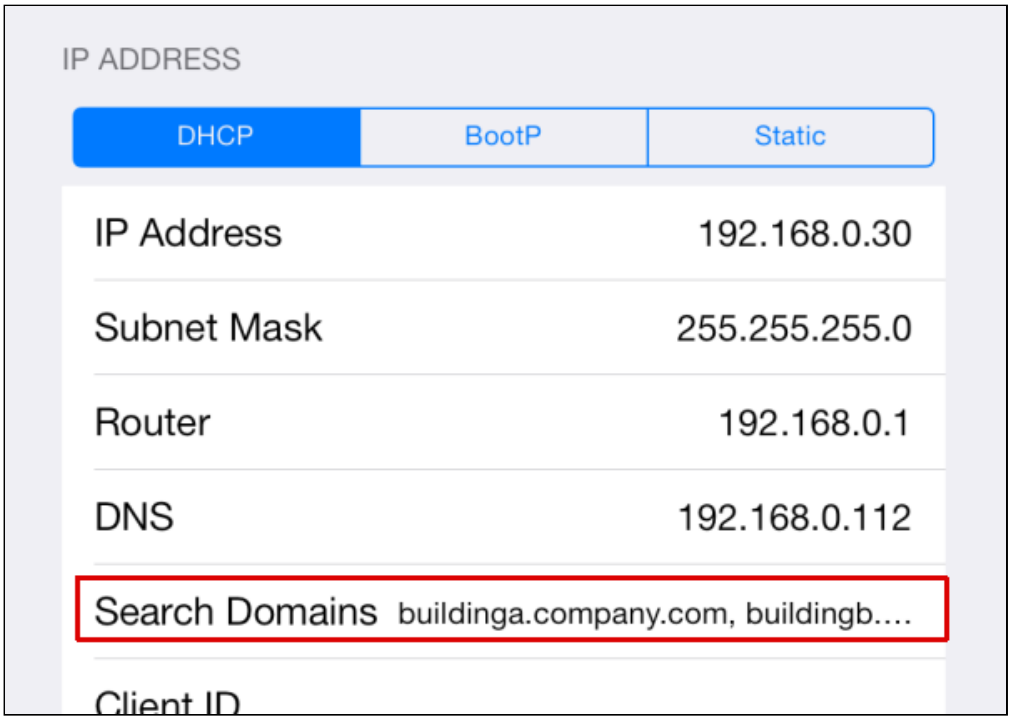
6. Copy/paste and run these commands on the DHCP server to create the DHCP entries



7. Confirm the entries appear under Scope Options in the DHCP server (refresh the DHCP server view to show the new settings).



8. Mobile devices obtaining a new lease from the DHCP should now show the correct search domains.



Multiple subdomains configuration on Linux DHCP

To specify search domains for a subnet on Linux DHCP, edit the dhcpd.conf file and insert a domain-search option with the subdomains to publish.

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.101 192.168.1.199;
    option domain-name "company.com";
    option domain-search "buildinga.company.com", "buildingb.company.com";
    option domain-name-servers 192.168.0.139;
    option routers 192.168.0.1;
}
```

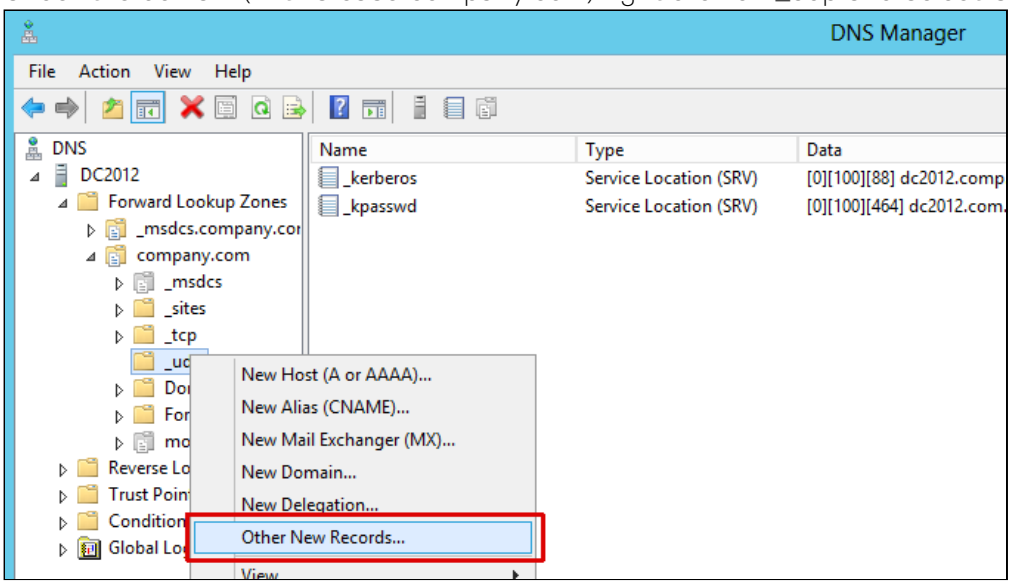
One Wide Area Mobile Print sub domain

If only one Wide Area Mobile Print subdomain has been created (recommended) the configuration needed to instruct Apple iOS devices to query the domain is simple.

Single subdomain configuration on Windows DNS

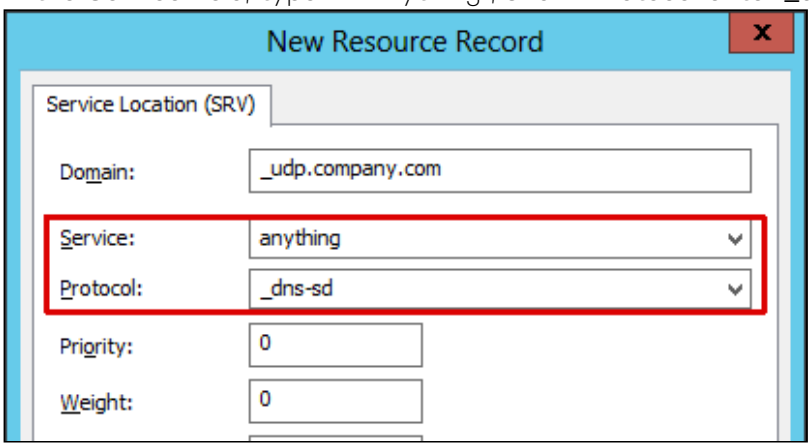
In addition to a delegation DNS record for the single "mobileprint.company.com" subdomain as outlined in the previous section, create DNS-SD discovery record in Windows DNS.

1. Under the domain (in this case company.com) right-click on _udp and select **Other new records**.

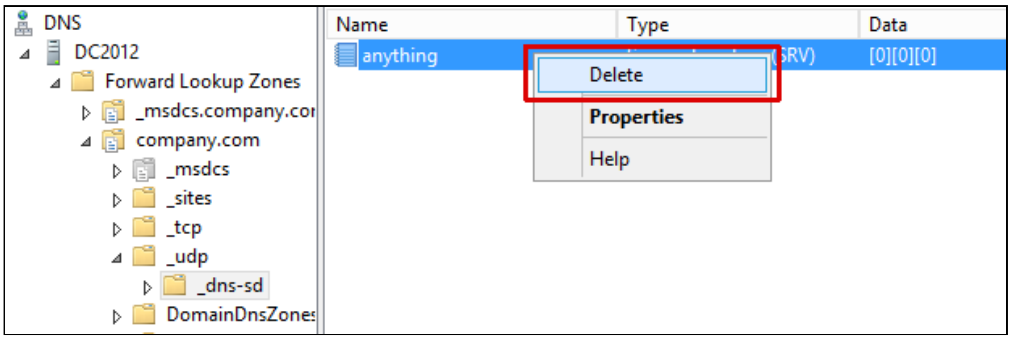


2. Select to insert a **Service Location (SRV)** record.

3. In the Service field, type in "Anything", and in Protocol enter **_dns-sd**

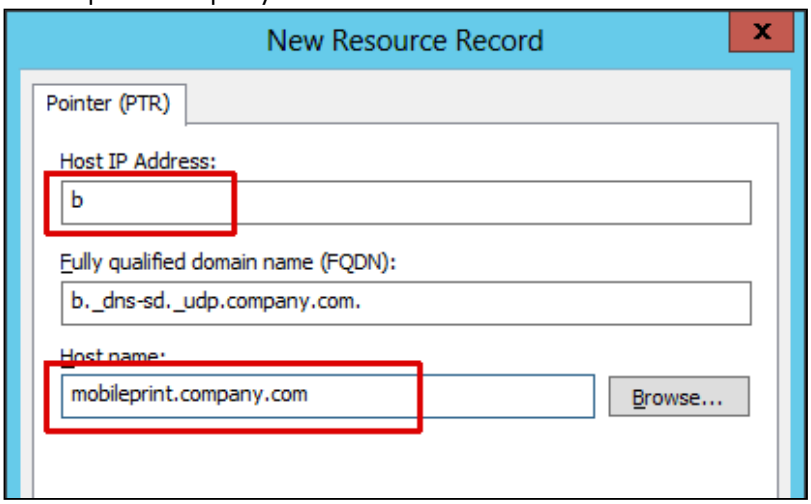


4. There should now be an _dns-sd folder under _udp. **Delete** the "Anything" SRV record from within the _dns-sd folder that was created.



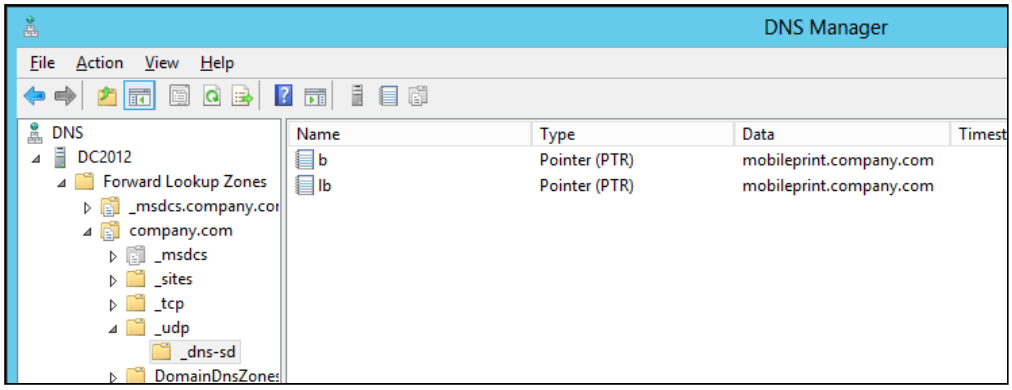
5. Right-click the _dns-sd folder and select **Other new records...** and select to insert a **Pointer (PTR)** record.

6. In Host IP Address enter the letter **b** and in Host Name enter the Wide Area subdomain such as **mobileprint.company.com**



7. Create an additional **Pointer (PTR)** record with letters **lb** also pointing to the same subdomain

The final structure should look like below.



Now any Apple iOS device with the search domain set to just "company.com", will discover the "mobileprint" subdomain and query SAFEQ Cloud for printers.

Single subdomain configuration on BIND

In addition to a delegation DNS record for the single "mobileprint.company.com" subdomain as outlined in section 3.18.4.2 Configure BIND , create DNS-SD discovery record in BIND.

In the domains master zone file, insert the following two DND-SD records:

```
b._dns-sd._udp IN PTR mobileprint.company.com.
lb._dns-sd._udp IN PTR mobileprint.company.com.
```

(replace "mobileprint.company.com." with the actual subdomain as created in SAFEQ Cloud)

```
;
; Zone file for company.com
;
$TTL 360
@       IN      SOA     ns.company.com. root.company.com. (
                        201404011       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds

                NS      ns              ; Inet Address of name server
ns              A       192.168.0.139


b._dns-sd._udp IN PTR mobileprint.company.com.
lb._dns-sd._udp IN PTR mobileprint.company.com.

; Delegation for Wide Area Mobile Print sub domains
$ORIGIN mobileprint.company.com.
@       IN      NS      mobileserver.mobileprint.company.com.
mobileserver IN      A       192.168.0.109
```

Sample BIND zone configuration file for the domain "company.com" with a single "mobileprint.company.com" Wide Area Mobile Print subdomain.

Internal copy with Scan to download trigger: Rules - triggers and automation v1

Triggers and automation rules modify document properties based on predefined conditions and actions. They can be helpful in implementing budget and security policies, and for tailoring efficient workflows.

Triggers run when a document is added or printed, and execute when a predefined set of conditions is met.

Automations run every 15 minutes and execute if conditions are met.

In this section, the triggers & automation features are explained, and these main aspects will be covered:

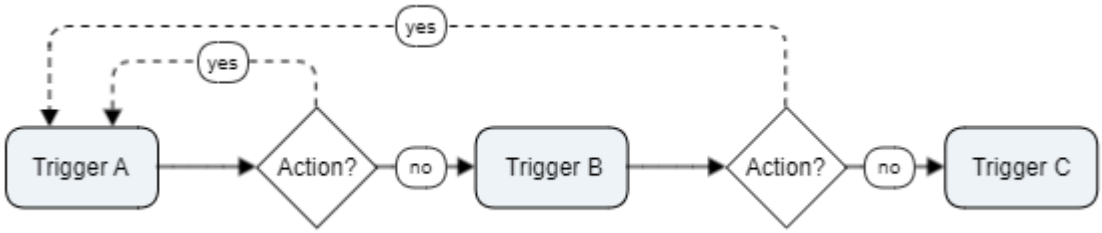
1. Building condition and action statements
2. Name triggers and automations using descriptive names
3. Reordering triggers and automations to achieve the desired outcome
4. Avoid conflicting triggers or automation

Working with triggers & automation

Triggers and Automation rules are handled in the SAFEQ Cloud Web UI under each account and office. Therefore, you can set up rules for an entire organization or a specific office within the organization.
On the Settings > Rules page, you can search for, add and reorder rules. You can also edit, clone, and deactivate/activate specific triggers/automation. Note that inactive rules are shown at the bottom of the table. Only inactive rules from the list may be deleted.

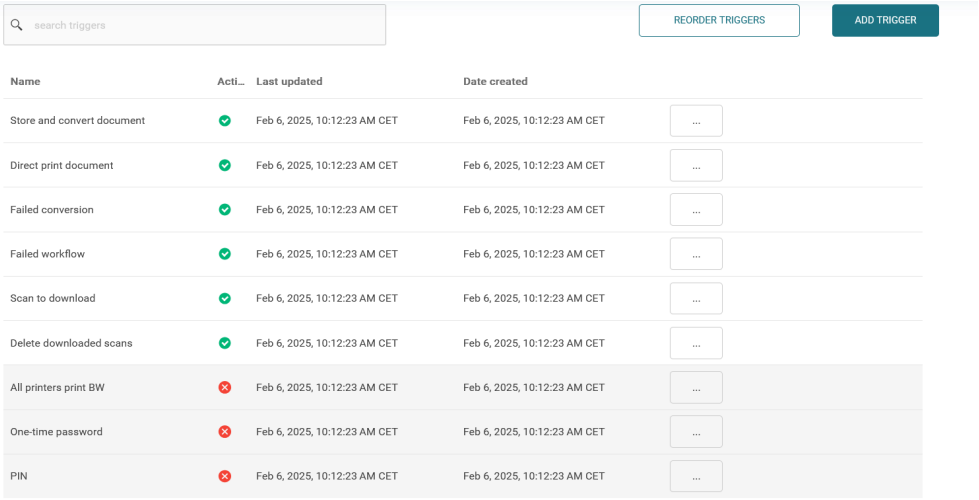
Rules are run, and possibly executed, in a sequential cycle according to the order defined in the Web UI. Whenever the conditions for a specific rule are met, and an action is executed, the cycle

restarts (see flowchart below). This cyclic flow ensures that interdependent rules execute as expected with fewer requirements for detailed ordering of rules.

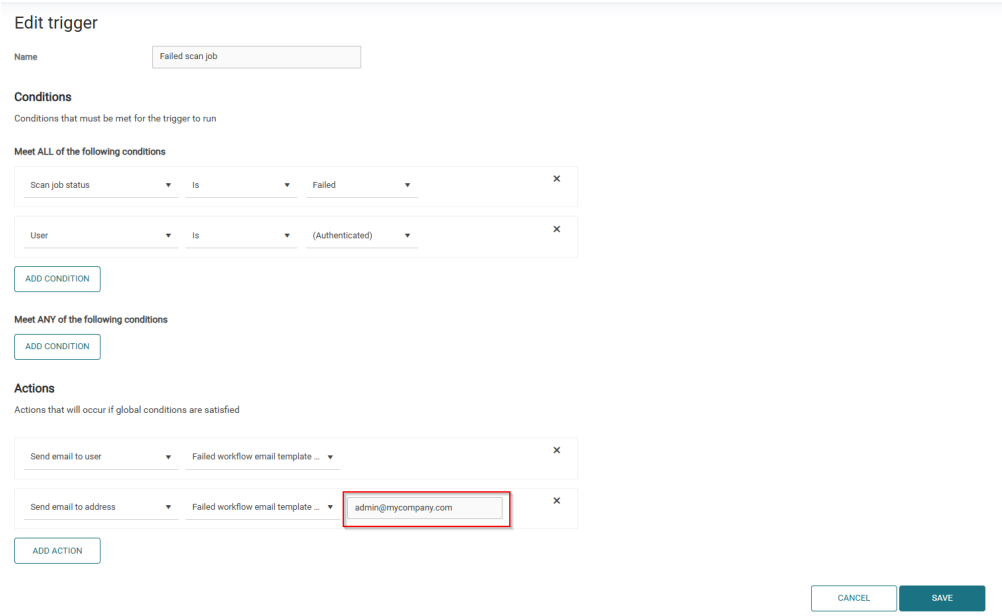


Default triggers

Certain SAFEQ Cloud functionalities are implemented as default triggers when a new tenant is created.



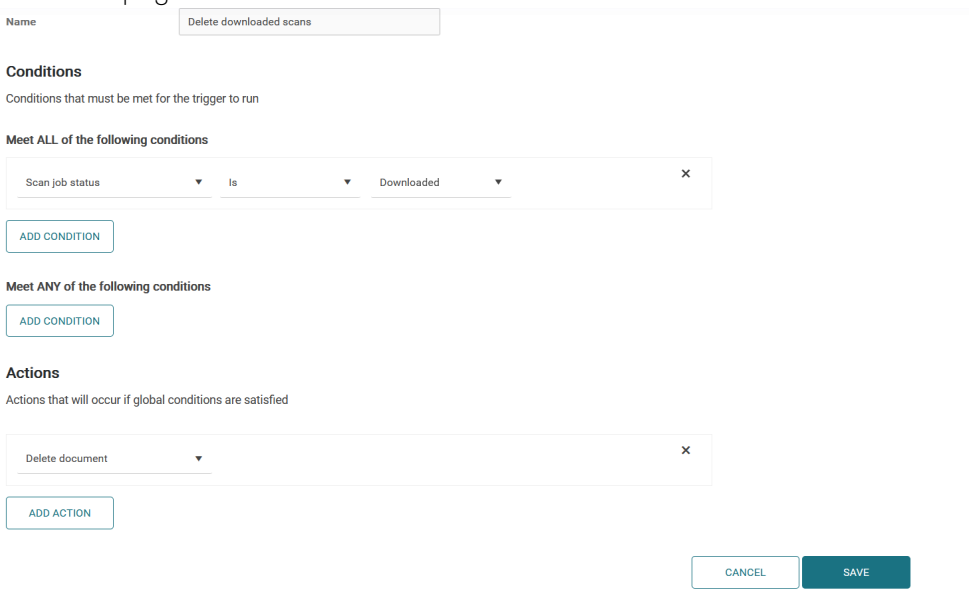
- **Failed workflow** – This trigger activates when a scan job hasn't been successfully delivered. For this trigger to function correctly, you must set the email address of the admin user in the trigger actions.



The admin will receive an email with information about the failure, the error code, and the error

message which may help the admin to resolve the problem. For the list of error codes, see Workflow error codes.

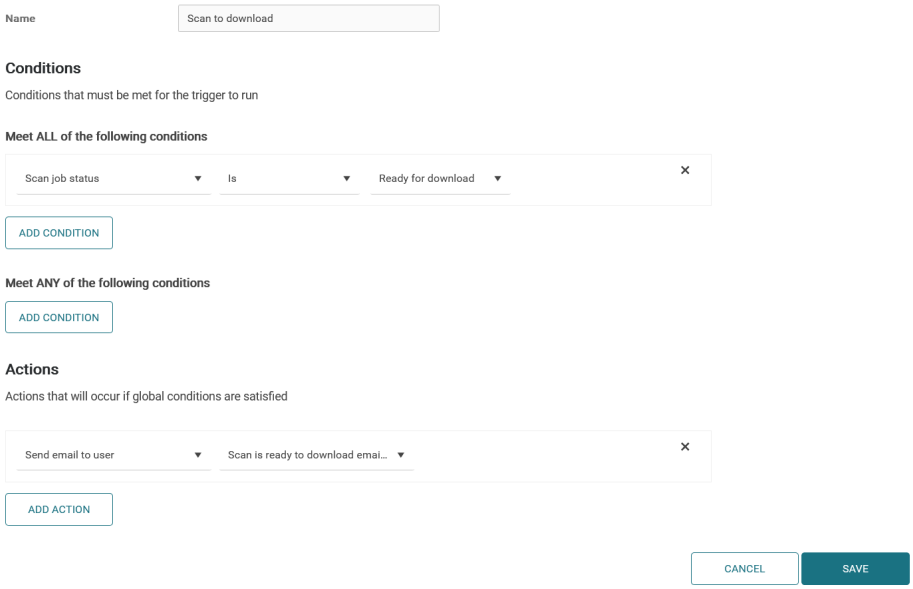
- **Delete downloaded scans** - This trigger activates when a scan job is downloaded from the My documents page.



It removes the scanned document from My Documents page.

> The document is removed even if the browser prompts the user for a download location and the user subsequently cancels the download.

- **Scan to download** - This trigger activates when a scan job using the Scan to download connector is successfully delivered and available for download on the My documents page.

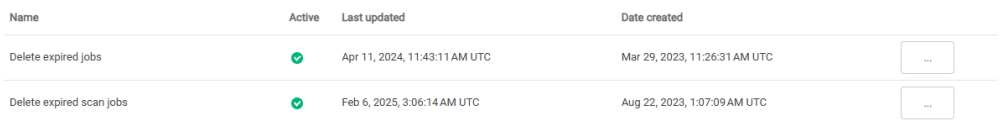


An email notification is sent to the job owner with a link to the document download page. The email content can be customized on the Settings/Templates page.

Default rules

Certain SAFEQ Cloud functionalities are implemented as default rules when a new tenant is created. For example, an automation will mark print jobs as expired after 32 hours. We recommend

you not to deactivate or delete the default rules. Be aware that some default rules, such as **Delete expired scan jobs,** do not have the **Delete** and **Edit** options.



Delete expired scan jobs

This rule controls **Retention** in **My documents**. If you wish to decrease it and have the new value displayed to the end users correctly, clone it and make sure the cloned rule contains the following conditions:

- Hours since document created
- Job type Is Scan

If you use higher value than 7 days in your cloned rule, then the default rule will take precedence.

Building condition and action statements

Both Triggers and Automation consist of condition statements and action statements.

- Condition statements consist of conditions, field operators, and condition values (these vary depending on the condition selected). Condition statements are essentially 'if' statements that return all print jobs that meet the specified criteria.
  For condition statements, the trigger will execute whenever the condition is changed. 'Changed' means any update made to the value, even if the value previously did not exist. For example, the Input Port Name trigger condition will execute even if the Output Port did not exist when a trigger was defined.
- Action statements consist of actions and action values (these vary depending on the condition selected). Some actions will be unambiguous, in which case a value does not apply – for example, the Delete Document action. Action statements define what occurs if all the condition statements are true and the trigger executes. You can think of action statements as 'then' statements – if all your conditions are true then perform these actions to update the document or print job.

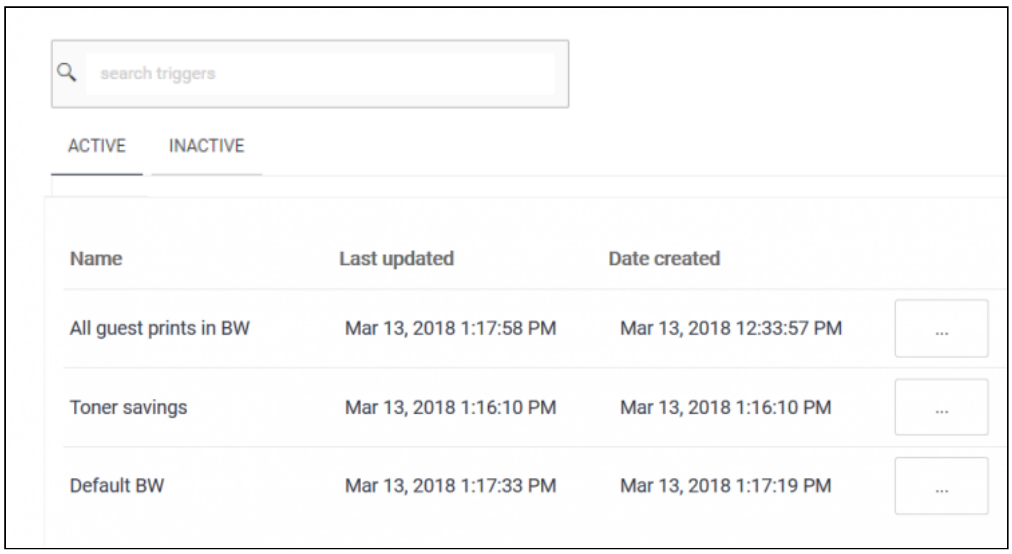
At the end of this section are reference lists with all conditions and actions, as well as field operators and values (see *Conditions and Actions Reference lists* below).

Best Practices for triggers & automation

Triggers and automation rules should be carefully designed and arranged to achieve the desired outcome. As more rules are added over time, it becomes more critical to manage the collection – therefore we recommend establishing good practices from the beginning.

Choosing a descriptive name

While triggers and automation rules can be a huge benefit, they can be tedious to maintain if not named appropriately. Choose a descriptive name that makes it easy for you (and any future admins) to remember what statements are contained in the rule, and to distinguish between different rules.
Consider these three identical triggers with different names.



They all communicate some aspect of the rule, but the first name is clearly superior for introducing what the rule does.

Reordering rules

Rules run in a sequential cycle. Certain rules will have actions that change parameters used as conditions in other rules. To achieve the expected outcome, it is therefore important to consider the order by which rules are run.

Avoiding conflicting rules

You may need to watch out for triggers that undo or modify an action contained in another trigger.
Consider an example where you want all print by guests to be in black&white. Trigger 1 determines all print jobs by guests will be set to black&white. Now consider a Trigger 2 – added for a different purpose – that sets all PowerPoint files to be printed in color. Consequently, if a guest prints a PowerPoint file, the order of triggers will determine the color attribute. One remedy for this situation is to add a condition to Trigger 2 that checks if it is a guest user, so only PowerPoint files from non-guests are set to color.

Consider if automation only runs once

Automations check every 15 minutes to see if their conditions are met. Typically, automation rules are meant to only execute once for each print job or document that satisfies the conditions.
To avoid continuous executions, an automation must include one of the following:

* an action that nullifies at least one of the conditions, or * a condition that can be true only once

If there is no nullifying action or true-only-once condition, the unmodified conditions will continue to be met, and the automation will continue to execute – possibly in an endless loop.

Conditions and Actions Reference lists

Condition	Operators	Values	Triggers	Automations
User Assign actions to either employees or guest users	Is Is not	(authenticated) User is successfully authenticated in a designated authentication provider. Non-authenticated can be used for assigning rights to a guest user	✓	✗
User name Assign actions to specific users	Is Is not Contains Does not Contain	[text input] Text is (part of) the user name	✓	✓
User group Assign actions to specific user groups	Is Is not Contains Does not contain	[text input] Text is (part of) the group name	✓	✗

Condition	Operators	Values	Triggers	Automations
Document status Assign actions to documents at a specific time during the print flow	Is Is not Changed Changed from Changed to Changed not from Changed not to	**Received** The document is added to print queue but not yet visible to users. **Ready** The document is added to a print queue and ready to be printed, meaning it is accepted, stored, and possibly converted. **Printed** The document is successfully printed. **Deleted** The document is deleted from storage, but has not necessarily been printed. **Expired** The document has been deleted from storage due to expiration of designated retention period. **Failed** The document failed to print. **Awaiting conversion** The document failed to convert and is awaiting conversion to be retried. **Converting** The document conversion is in progress. **Conversion failed** The document conversion failed and will not be retried. **Stored** The document is received and stored in the storage service. **Deleting** The document failed to be deleted. The deletion will be retried.	✓	✓

Condition	Operators	Values	Triggers	Automations
Document name Assign actions to specific documents	Is Is not Contains Does not contain	[text input] Text is (part of) the document name	✓	✓
Document type Assign actions to certain types of documents	Is Is not	Unknown The file type is not recognized and will result in a conversion error PDF PS PCLXL HTML DOCUMENT SHEET SLIDE TEXT XPS IMAGE	✓	✓
Document attribute Assign actions to a document that has certain attributes	Is Is not	Color Black & white Duplex long side Duplex short side Simplex	✓	✓
Hours since document ready Assign action within a certain time after the document state changed to "ready"	Is Is not Greater Than Not greater than Not less than	[number input] The number defines whole hours (integer)	✓	✓

Condition	Operators	Values	Triggers	Automations
Print queue Assign actions to documents sent from known or unknown print queues	Is Is not	**(Empty)** Documents sent via IPP or API can have a designated print queue that is not specified in the SAFEQ Cloud Web UI, in which case the port is empty. **(Listed input ports)** Print queues set up in the SAFEQ Cloud Web UI are individually listed.	✓	✗
Print queue name Assign actions to documents received from specific print queues.	Is Is not Contains Does not contain	**[text input]** Text is (part of) print queue name	✓	✓
Print queue type Assign actions to documents from either a push or pull queue	Is Is not	**Roaming Print Queue** Follow-me print **Direct (Push) Print queue** Direct print	✓	✗
Output port Assign actions to documents that are not associated with any output port (for example, a printer)	Is Is not	**(Empty)** Push print jobs can have a designated output port that is not specified in the SAFEQ Cloud Web UI. **(Listed output ports)** Output ports set up in the SAFEQ Cloud Web UI are individually listed.	✓	✗
Output port name Assign actions to print jobs assigned to specific output ports (for example, printers)	Is Is not Contains Does not contain	**[text input]** Text is (part of) output port (for example, printer) name.	✓	✗

Condition	Operators	Values	Triggers	Automations
Output port type Assign actions to print jobs assigned to either a physical printer or a dummy	Is Is not	**Dummy** Output port is a dummy intended for purposes other than physical printing **Printer** Output port is a physical printer **Rightfax** Output port is a virtual Rightfax destination. **Discovered Printer** Output port for the printer has been automatically discovered.	✓	✗
Output port address Assign actions to print jobs assigned to specific output ports (for example, printers)	Is Is not Contains Does not contain	**[text input]** Text is (part of) the output port address in IP-format	✓	✗
User card ID Assign actions to users with a specific card ID	Is Is not Contains Dost not contain	**[text input]** Text is (part of) the user's card ID.	✓	✗
User one-time password Assign actions to users with a specific one-time password.	Is Is not Contains Does not contain	**[text input]** Text is (part of) the user's one-time password.	✓	✗

Condition	Operators	Values	Triggers	Automations
User short ID Assign actions to users with a specific short ID	Is Is not Contains Dost not contain	[text input] Text is (part of) the user's short ID	✓	✗
Scan job status Assign actions to scan jobs in the specific status	Is	Failed The scan job has failed	✓	✗
Job type Assign actions in dependency of the job type	Is	Print Copy Scan Fax	✓	✓
Hours since document created Assign action within a certain time after the document was created	Greater Than	**[number input]** The number defines whole hours (integer).	✓	✓
Number of pages in the document Assign actions based on the total number of pages in the document (number of pages multiplied by number of copies)	Is Is not Greater Than Not greater than Not less than	**[number input]** The number defines the page count	✓	✗

Action	Values	Triggers	Automations
Output document Output the document, for example, by printing	(associated output port) The specific output port the document is already associated with (Listed output ports) Output ports that are added in the SAFEQ Cloud Web UI shown as individual entries in the list of possible values	✓	✗
Delete document Delete the document from storage	-	✓	✓
Set document attribute Set a specific document attribute	Color Black & white Duplex long side Duplex short side Simplex	✓	✓
Store document Store the document in storage	(Default storage) Default storage according to storage service settings.	✓	✓
Assign document Assign the document to the specified user	(Alias) See the Users section for this feature description. If the user has multiple aliases, this trigger assigns the document to one of them randomly because their order isn't defined. [text input] Type the target username	✓	✓
Convert document Runs the document conversion	-	✓	✓
Generate OTP for user Generates new one-time password for the user	-	✓	✗
Generate short ID for user Generates a new short ID for the user	-	✓	✗

Action	Values	Triggers	Automations
Send email to user Send an email to the logged-in user	(template - SMTP config) List of available email templates and SMTP configs.	✓	✗
Send email to address Sends an email to the specified address	(template - SMTP config) List of available email templates and SMTP configs. [text input] Recipient's email address.	✓	✓

Template parameters

Several conditions and actions may accept template parameters enclosed in double curly braces. The following parameters are currently recognized:

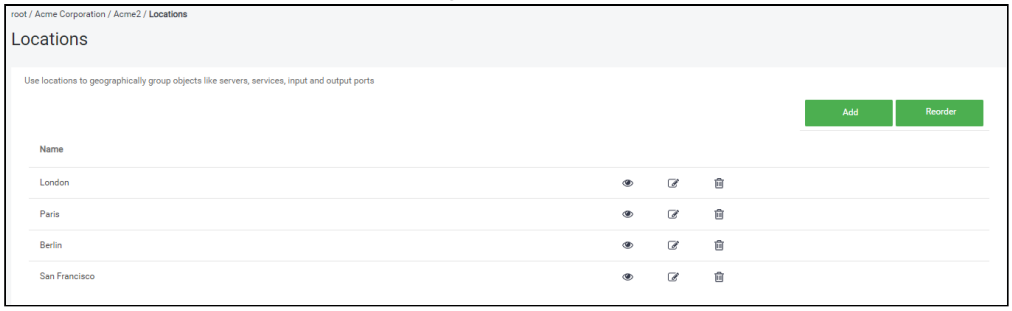
Parameter	Value
`{{username}}`	Name of the user
`{{userotp}}`	Value of one-time password of the user
`{{shortid}}`	Value of the short ID field of the user
`{{documentname}}`	Title of the document submitted to trigger chain
`{{inputportname}}`	Name of the input port through which the document was sent
`{{outputportname}}`	Name of the printer to which the document was sent for printing
`{{errorcode}}`	Value of the error code (scan workflows only)
`{{correlationid}}`	Value of the correlation ID of the failed scan job. This can help to identify the cause of the failure.

Parameter	Value
`{{errorhint}}`	Value of the hint connected to the error code, if it exists.
`{{usererrorhint}}`	Value of the hint bound to the error code for the user, if it exists.

Locations

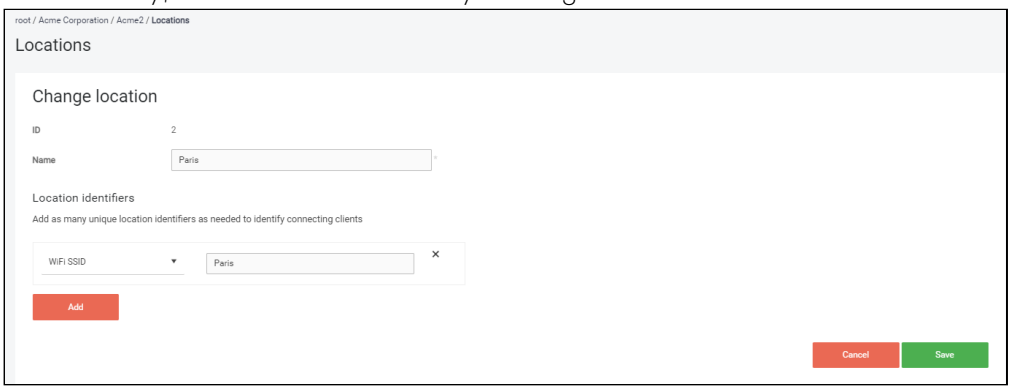
Location list

List view of all locations with navigation to reorder, add, view associated objects, edit, and delete.



Adding a new location

1. To add a new location, click **Add**.
2. Enter the location name.
3. In **Location Identifiers**, select an identifier for your new location:
   - Gateway IPv4
   - Subnet IPv4
   - IPv4 range from – to
   - WIFI-SSID
4. If necessary, add more identifiers by clicking **Add**.



5. Click **Save**.

Editing a location

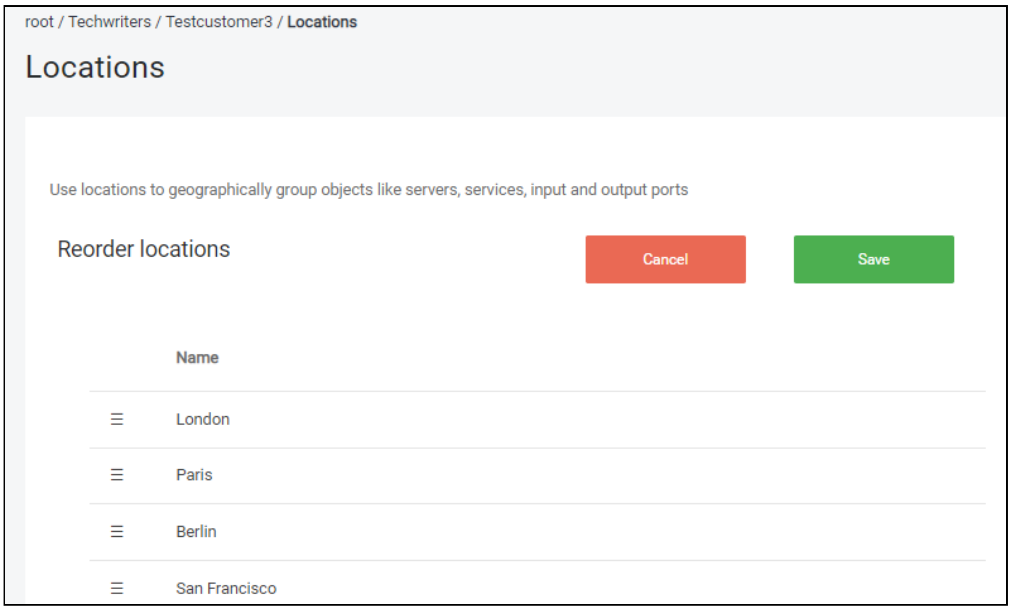
1. Click the edit icon next to the location you wish to edit.
2. Make your changes. The form is the same as for adding a location.
3. Click **Save**.

Deleting a location

1. Click the delete icon next to the location you wish to delete.
2. Confirm your action.

Reordering locations

1. Click **Reorder**.
2. A new view where you can drag and drop the locations will be loaded. Reorder the locations as needed.



3. Click **Save**.

Viewing associated objects

1. Click the eye icon next to the location for which you wish to see the associated objects.

2. You will see all associated objects in a list with search and filtering.
    - Accounts (vendors/accounts)
    - Containers
    - Servers
    - Printers
    - Connected SAFEQ Cloud Clients

    > The **associated objects** list shows only objects within the given vendor account or customer account.

Adding location to nodes

When creating the following main tree nodes, you have an option to add a location to them:

- Vendor account or customer account
- Containers
- Servers
- Services
- Input ports
- Output ports

If a node doesn't have any location information filled in, you can look up the inherited location from the settings of the parent node.

In advanced Vendor/Customer account settings you can set the Default location for all printers/queues and change the Policy for unknown location.

Rules - triggers and automation

Triggers and automation rules modify document properties based on predefined conditions and actions. They can be helpful in implementing budget and security policies, and for tailoring efficient workflows.

Triggers run when a document is added or printed, and execute when a predefined set of conditions is met.

Automations run every 15 minutes and execute if conditions are met.

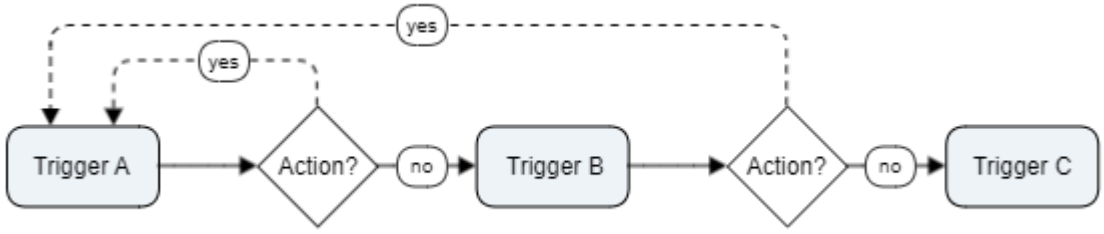
In this section, the triggers & automation features are explained, and these main aspects will be covered:

1. Building condition and action statements
2. Name triggers and automations using descriptive names
3. Reordering triggers and automations to achieve the desired outcome
4. Avoid conflicting triggers or automation

Working with triggers & automation

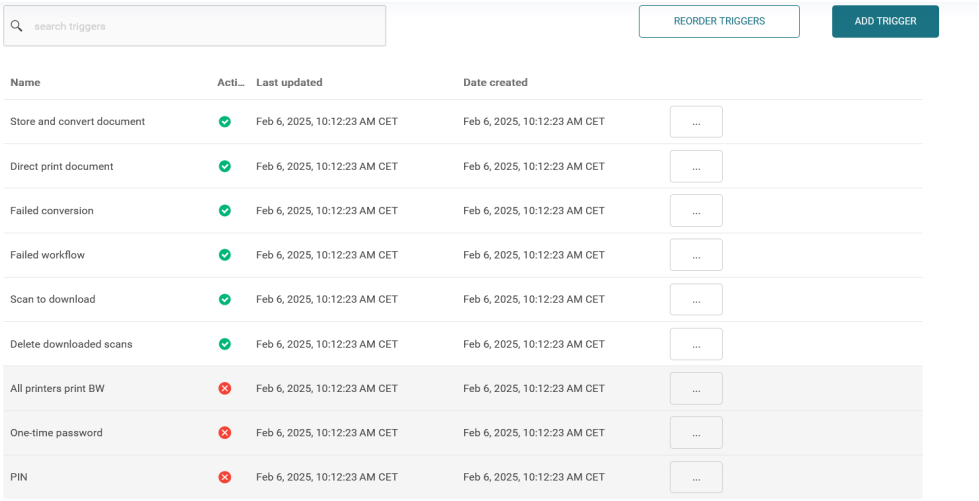
Triggers and Automation rules are handled in the SAFEQ Cloud Web UI under each account and office. Therefore, you can set up rules for an entire organization or a specific office within the organization.
On the Settings > Rules page, you can search for, add and reorder rules. You can also edit, clone, and deactivate/activate specific triggers/automation. Note that inactive rules are shown at the bottom of the table. Only inactive rules from the list may be deleted.

Rules are run, and possibly executed, in a sequential cycle according to the order defined in the Web UI. Whenever the conditions for a specific rule are met, and an action is executed, the cycle restarts (see flowchart below). This cyclic flow ensures that interdependent rules execute as expected with fewer requirements for detailed ordering of rules.

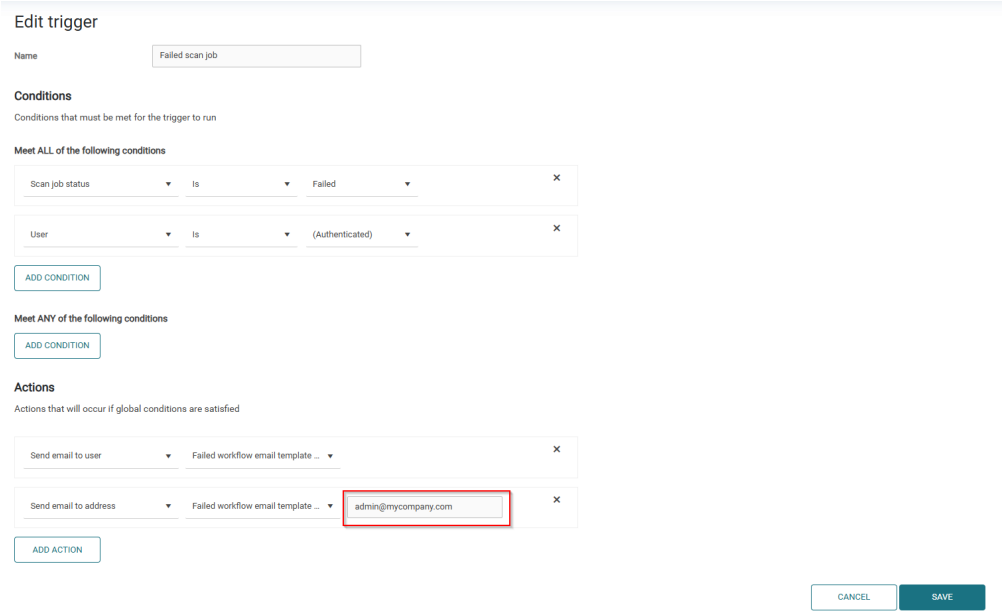


Default triggers

Certain SAFEQ Cloud functionalities are implemented as default triggers when a new tenant is created.

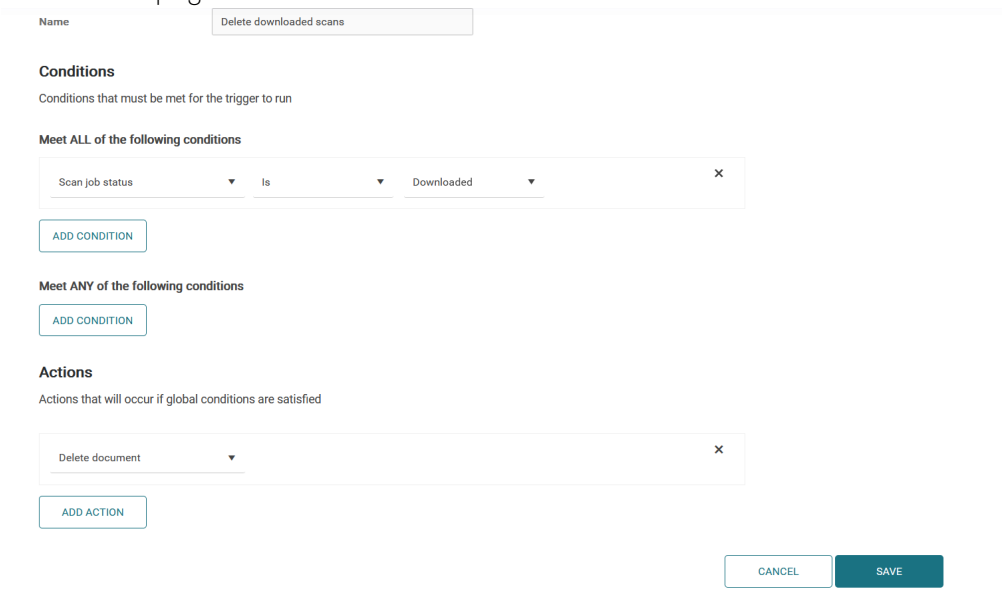


- Failed workflow – This trigger activates when a scan job hasn't been successfully delivered. For this trigger to function correctly, you must set the email address of the admin user in the trigger actions.



The admin will receive an email with information about the failure, the error code, and the error message which may help the admin to resolve the problem. For the list of error codes, see Workflow error codes.

- Delete downloaded scans - This trigger activates when a scan job is downloaded from the My documents page.



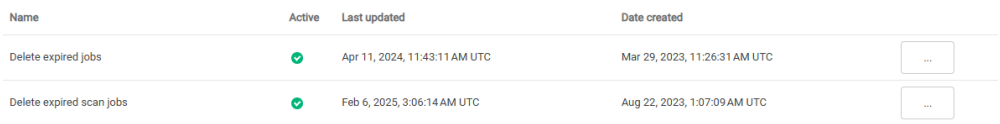
It removes the scanned document from My Documents page. If you want to keep the downloaded documents, you should deactivate this trigger.

The document is removed even if the browser prompts the user for a download location and the user subsequently cancels the download.

Default rules

Certain SAFEQ Cloud functionalities are implemented as default rules when a new tenant is created.

We recommend that you do not deactivate or delete these default rules.
Note that some default rules, such as *Delete expired scan jobs*, cannot be deleted or edited.



Delete expired jobs

Marks unprinted jobs as expired and deletes them after 32 hours.

Delete expired scan jobs

This rule sets the maximum retention period in for scan documents to 168 hours (7 days).

To decrease this retention period and ensure the correct display for end users, clone the rule and include the following conditions:

- Hours since document created
- Job type Is Scan

If your cloned rule specifies a retention period longer than 7 days, the default rule will override it.

Building condition and action statements

Both Triggers and Automation consist of condition statements and action statements.

- Condition statements consist of conditions, field operators, and condition values (these vary depending on the condition selected). Condition statements are essentially 'if' statements that return all print jobs that meet the specified criteria.
  For condition statements, the trigger will execute whenever the condition is changed.
  'Changed' means any update made to the value, even if the value previously did not exist. For example, the Input Port Name trigger condition will execute even if the Output Port did not exist when a trigger was defined.
- Action statements consist of actions and action values (these vary depending on the condition selected). Some actions will be unambiguous, in which case a value does not apply – for example, the Delete Document action. Action statements define what occurs if all the condition statements are true and the trigger executes. You can think of action statements as 'then' statements – if all your conditions are true then perform these actions to update the document or print job.

At the end of this section are reference lists with all conditions and actions, as well as field operators and values (see *Conditions and Actions Reference lists* below).

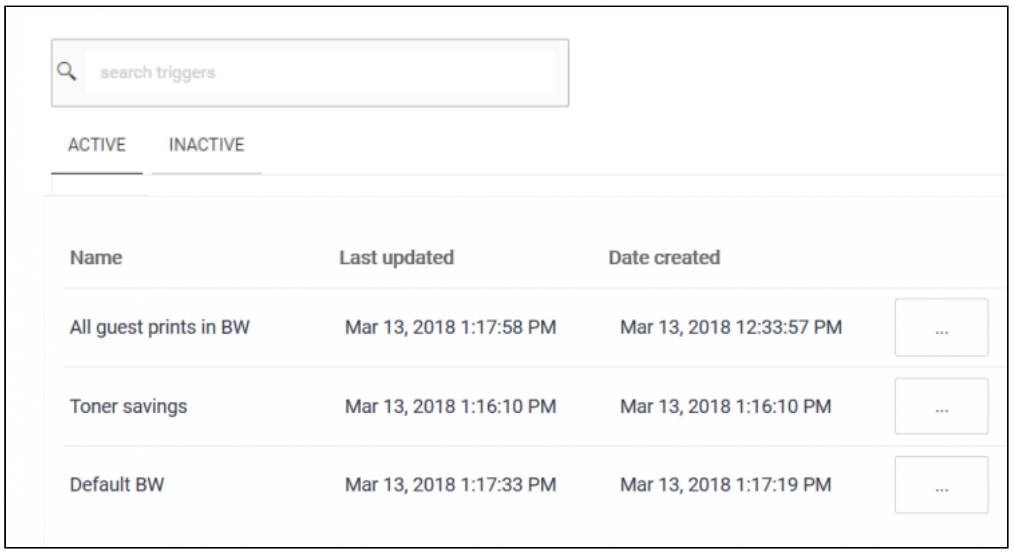
Best Practices for triggers & automation

Triggers and automation rules should be carefully designed and arranged to achieve the desired outcome. As more rules are added over time, it becomes more critical to manage the collection – therefore we recommend establishing good practices from the beginning.

Choosing a descriptive name

While triggers and automation rules can be a huge benefit, they can be tedious to maintain if not named appropriately. Choose a descriptive name that makes it easy for you (and any future

admins) to remember what statements are contained in the rule, and to distinguish between different rules.
Consider these three identical triggers with different names.



They all communicate some aspect of the rule, but the first name is clearly superior for introducing what the rule does.

Reordering rules

Rules run in a sequential cycle. Certain rules will have actions that change parameters used as conditions in other rules. To achieve the expected outcome, it is therefore important to consider the order by which rules are run.

Avoiding conflicting rules

You may need to watch out for triggers that undo or modify an action contained in another trigger.
Consider an example where you want all print by guests to be in black&white. Trigger 1 determines all print jobs by guests will be set to black&white. Now consider a Trigger 2 – added for a different purpose – that sets all PowerPoint files to be printed in color. Consequently, if a guest prints a PowerPoint file, the order of triggers will determine the color attribute. One remedy for this situation is to add a condition to Trigger 2 that checks if it is a guest user, so only PowerPoint files from non-guests are set to color.

Consider if automation only runs once

Automations check every 15 minutes to see if their conditions are met. Typically, automation rules are meant to only execute once for each print job or document that satisfies the conditions.
To avoid continuous executions, an automation must include one of the following:

* an action that nullifies at least one of the conditions, or * a condition that can be true only once

If there is no nullifying action or true-only-once condition, the unmodified conditions will continue to be met, and the automation will continue to execute – possibly in an endless loop.

Conditions and Actions Reference lists

Condition	Operators	Values	Triggers	Automations
User Assign actions to either employees or guest users	Is Is not	**(authenticated)** User is successfully authenticated in a designated authentication provider. Non-authenticated can be used for assigning rights to a guest user	✓	✗
User name Assign actions to specific users	Is Is not Contains Does not Contain	**[text input]** Text is (part of) the user name	✓	✓
User group Assign actions to specific user groups	Is Is not Contains Does not contain	**[text input]** Text is (part of) the group name	✓	✗

Condition	Operators	Values	Triggers	Automations
Document status Assign actions to documents at a specific time during the print flow	Is Is not Changed Changed from Changed to Changed not from Changed not to	**Received** The document is added to print queue but not yet visible to users. **Ready** The document is added to a print queue and ready to be printed, meaning it is accepted, stored, and possibly converted. **Printed** The document is successfully printed. **Deleted** The document is deleted from storage, but has not necessarily been printed. **Expired** The document has been deleted from storage due to expiration of designated retention period. **Failed** The document failed to print. **Awaiting conversion** The document failed to convert and is awaiting conversion to be retried. **Converting** The document conversion is in progress. **Conversion failed** The document conversion failed and will not be retried. **Stored** The document is received and stored in the storage service. **Deleting** The document failed to be deleted. The deletion will be retried.	✓	✓

Condition	Operators	Values	Triggers	Automations
Document name Assign actions to specific documents	Is Is not Contains Does not contain	[text input] Text is (part of) the document name	✓	✓
Document type Assign actions to certain types of documents	Is Is not	Unknown The file type is not recognized and will result in a conversion error PDF PS PCLXL HTML DOCUMENT SHEET SLIDE TEXT XPS IMAGE	✓	✓
Document attribute Assign actions to a document that has certain attributes	Is Is not	Color Black & white Duplex long side Duplex short side Simplex	✓	✓
Hours since document created Assign action within a certain time after the document was created	Greater Than	**[number input]** The number defines whole hours (integer).	✓	✓

Condition	Operators	Values	Triggers	Automations
Hours since document ready Assign action within a certain time after the document state changed to "ready"	Is Is not Greater Than Not greater than Not less than	[number input] The number defines whole hours (integer)	✓	✓
Print queue Assign actions to documents sent from known or unknown print queues	Is Is not	(Empty) Documents sent via IPP or API can have a designated print queue that is not specified in the SAFEQ Cloud Web UI, in which case the port is empty. (Listed input ports) Print queues set up in the SAFEQ Cloud Web UI are individually listed.	✓	✗
Print queue name Assign actions to documents received from specific print queues.	Is Is not Contains Does not contain	[text input] Text is (part of) print queue name	✓	✓
Print queue type Assign actions to documents from either a push or pull queue	Is Is not	**Roaming Print Queue** Follow-me print **Direct (Push) Print queue** Direct print	✓	✗
Output port Assign actions to documents that are not associated with any output port (for example, a printer)	Is Is not	(Empty) Push print jobs can have a designated output port that is not specified in the SAFEQ Cloud Web UI. (Listed output ports) Output ports set up in the SAFEQ Cloud Web UI are individually listed.	✓	✗

Condition	Operators	Values	Triggers	Automations
Output port name Assign actions to print jobs assigned to specific output ports (for example, printers)	Is Is not Contains Does not contain	**[text input]** Text is (part of) output port (for example, printer) name.	✓	✗
Output port type Assign actions to print jobs assigned to either a physical printer or a dummy	Is Is not	**Dummy** Output port is a dummy intended for purposes other than physical printing **Printer** Output port is a physical printer **Rightfax** Output port is a virtual Rightfax destination. **Discovered Printer** Output port for the printer has been automatically discovered.	✓	✗
Output port address Assign actions to print jobs assigned to specific output ports (for example, printers)	Is Is not Contains Does not contain	**[text input]** Text is (part of) the output port address in IP-format	✓	✗
User card ID Assign actions to users with a specific card ID	Is Is not Contains Dost not contain	**[text input]** Text is (part of) the user's card ID.	✓	✗

Condition	Operators	Values	Triggers	Automations
User one-time password Assign actions to users with a specific one-time password.	Is Is not Contains Does not contain	[text input] Text is (part of) the user's one-time password.	✓	✗
User short ID Assign actions to users with a specific short ID	Is Is not Contains Dost not contain	[text input] Text is (part of) the user's short ID	✓	✗
Scan job status Assign actions to scan jobs in the specific status	Is	Failed The scan job has failed	✓	✗
Job type Assign actions in dependency of the job type	Is	Print Copy Scan Fax	✓	✓
Number of pages in the document Assign actions based on the total number of pages in the document (number of pages multiplied by number of copies)	Is Is not Greater Than Not greater than Not less than	**[number input]** The number defines the page count	✓	✗

Action	Values	Triggers	Automations
Output document Output the document, for example, by printing	(associated output port) The specific output port the document is already associated with (Listed output ports) Output ports that are added in the SAFEQ Cloud Web UI shown as individual entries in the list of possible values	✓	✗
Delete document Delete the document from storage	-	✓	✓
Set document attribute Set a specific document attribute	Color Black & white Duplex long side Duplex short side Simplex	✓	✓
Store document Store the document in storage	(Default storage) Default storage according to storage service settings.	✓	✓
Assign document Assign the document to the specified user	(Alias) See the Users section for this feature description. If the user has multiple aliases, this trigger assigns the document to one of them randomly because their order isn't defined. [text input] Type the target username	✓	✓
Convert document Runs the document conversion	-	✓	✓
Generate OTP for user Generates new one-time password for the user	-	✓	✗
Generate short ID for user Generates a new short ID for the user	-	✓	✗

Action	Values	Triggers	Automations
Send email to user Send an email to the logged-in user	(template - SMTP config) List of available email templates and SMTP configs.	✓	✗
Send email to address Sends an email to the specified address	(template - SMTP config) List of available email templates and SMTP configs. [text input] Recipient's email address.	✓	✓

Template parameters

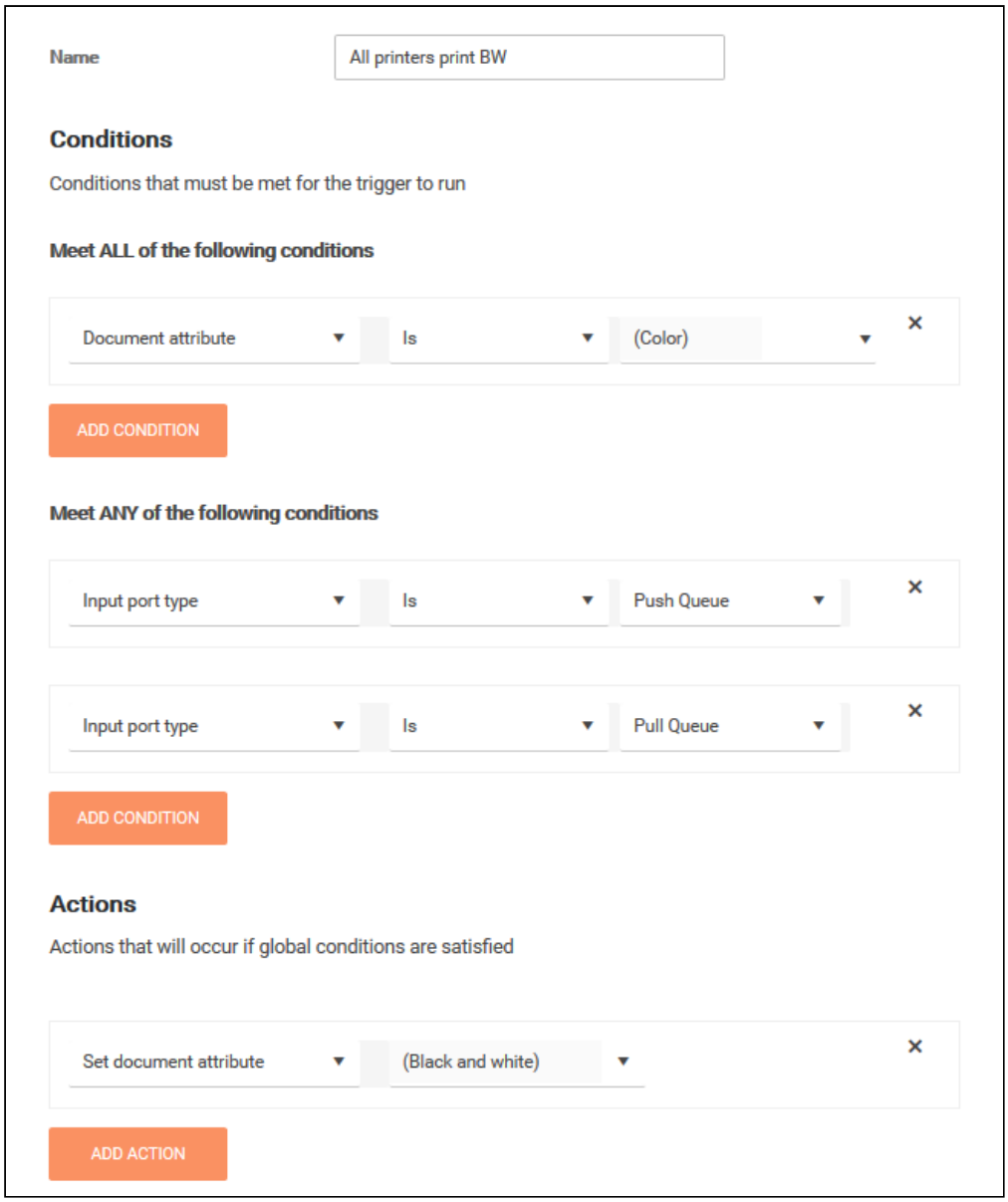
Several conditions and actions may accept template parameters enclosed in double curly braces. The following parameters are currently recognized:

Parameter	Value
`{{username}}`	Name of the user
`{{userotp}}`	Value of one-time password of the user
`{{shortid}}`	Value of the short ID field of the user
`{{documentname}}`	Title of the document submitted to trigger chain
`{{inputportname}}`	Name of the input port through which the document was sent
`{{outputportname}}`	Name of the printer to which the document was sent for printing
`{{errorcode}}`	Value of the error code (scan workflows only)
`{{correlationid}}`	Value of the correlation ID of the failed scan job. This can help to identify the cause of the failure.

Parameter	Value
`{{errorhint}}`	Value of the hint connected to the error code, if it exists.
`{{usererrorhint}}`	Value of the hint bound to the error code for the user, if it exists.

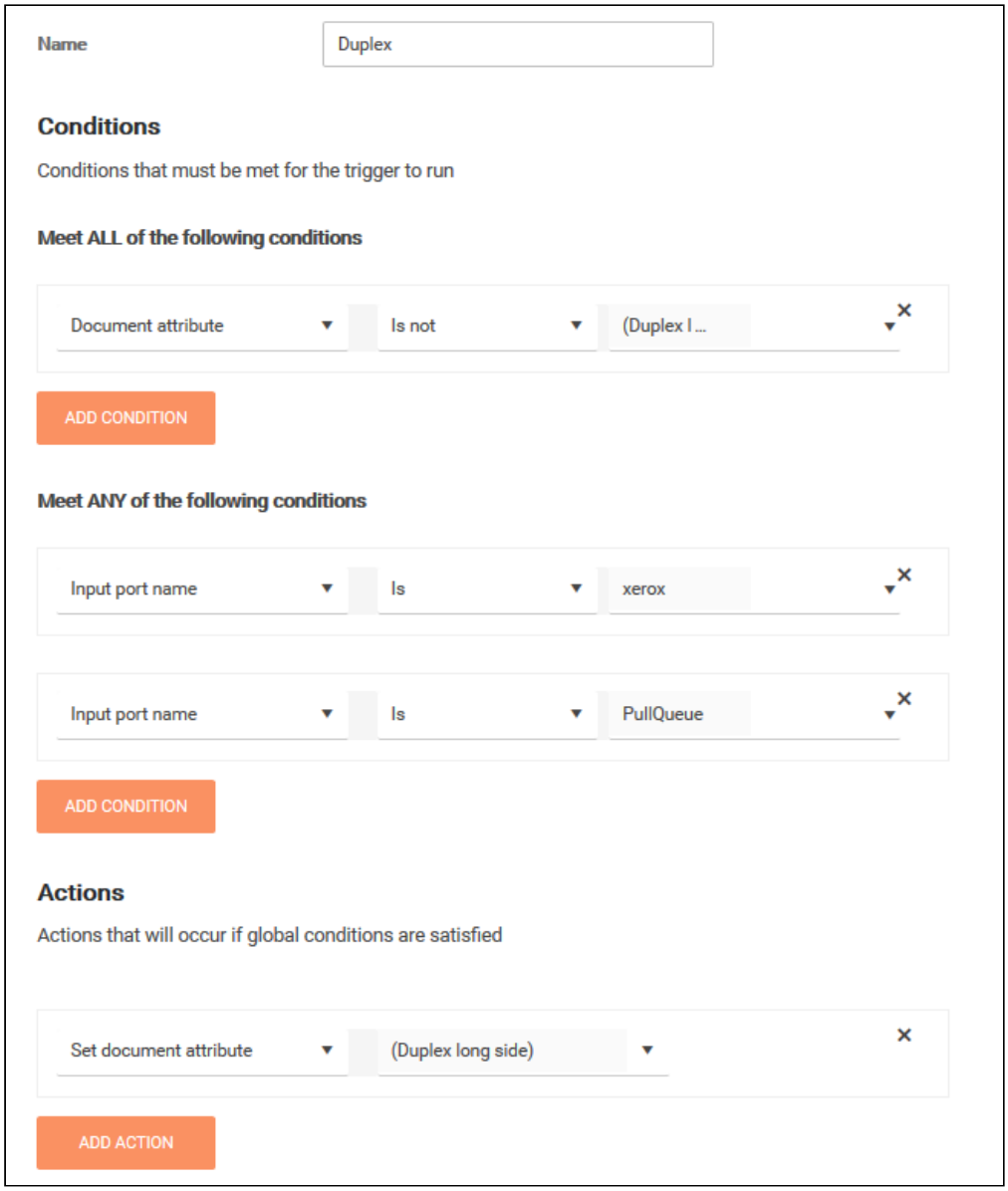
Trigger examples

Example of a trigger that sets all jobs to be printed in black and white for every type of queue:

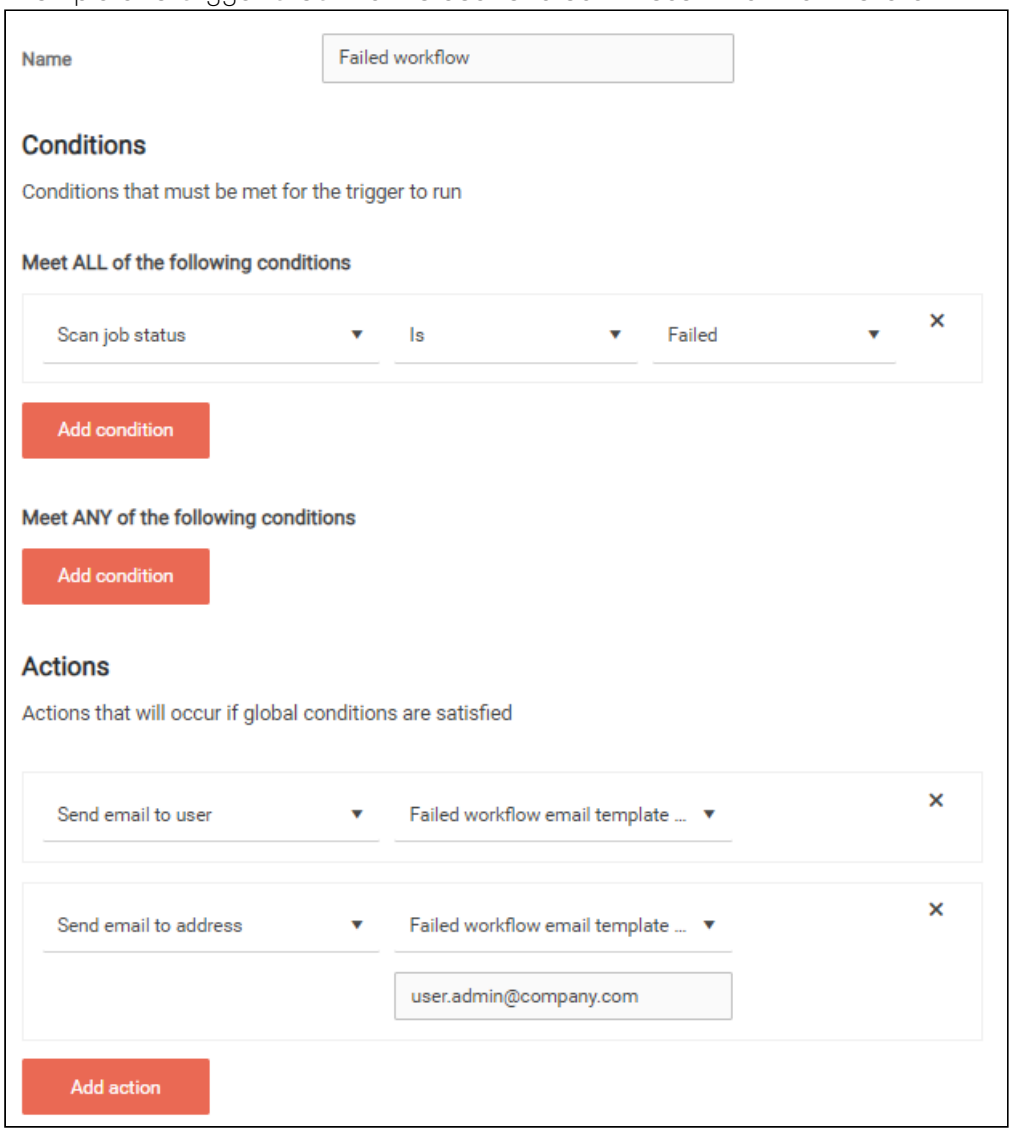


From version 3.48, this BW trigger is one of the default triggers and is created (as inactive) for all new customers.

Example of trigger that sets all jobs pull and xerox printer to be printed duplex:

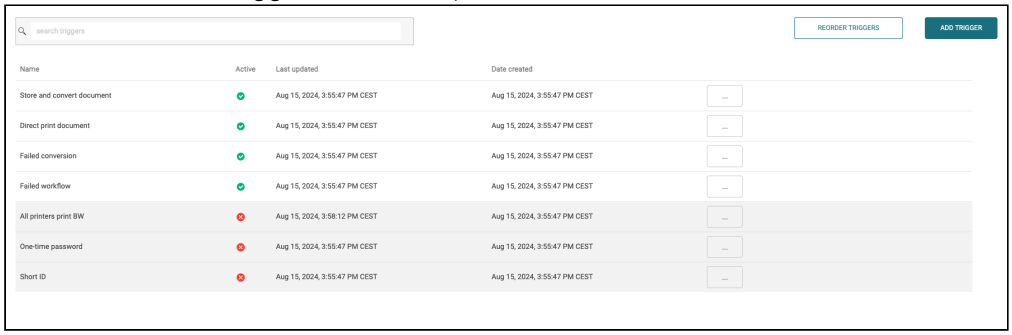


Example of a trigger that informs user and admin scan workflow failure



You must set up the administrator's email address in the trigger configuration manually as there is no guaranteed way of fetching the admininistrator's email form the system.

The order of the triggers is also important:



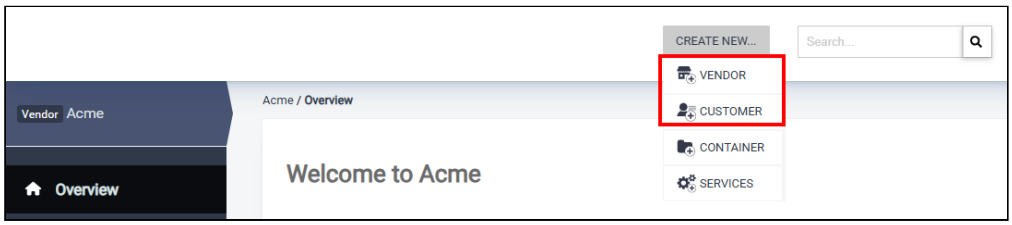
Rules run in a sequential cycle. Certain rules will have actions that change parameters used as conditions in other rules. To achieve the expected outcome, it is therefore important to consider the order by which rules are run. Inactive triggers are always displayed at the bottom of the table, where their order doesn't matter. Only the order of the active triggers is taken into account.

Vendor/Customer account

Each Vendor primary account, Customer primary account, or standard Account in the YSoft SAFEQ Cloud system tree has a **Settings** > **Vendor account** or **Customer account** menu item. It holds the general settings for the entity in the system, such as Name, logo branding, and any domain names that identify their system in the SAFEQ Cloud.

Adding Vendor accounts and Customer accounts

1. Select a parent node within the SAFEQ Cloud system tree.
2. If you wish to add a Vendor account, click **Create new** and select **Vendor**.
3. If you wish to add a Customer account, click **Create new** and select **Customer.**

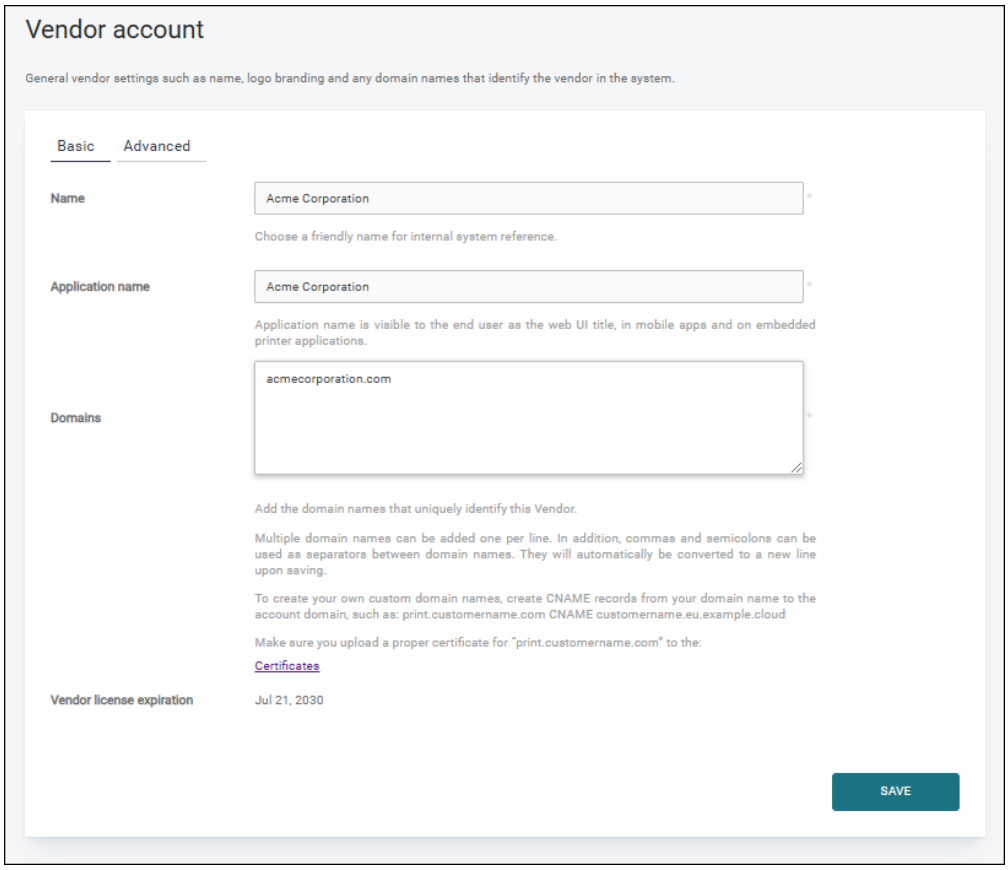


> Vendor accounts and Customer accounts can only be added to Primary nodes or Vendor nodes, not to Customer account nodes.

General setup

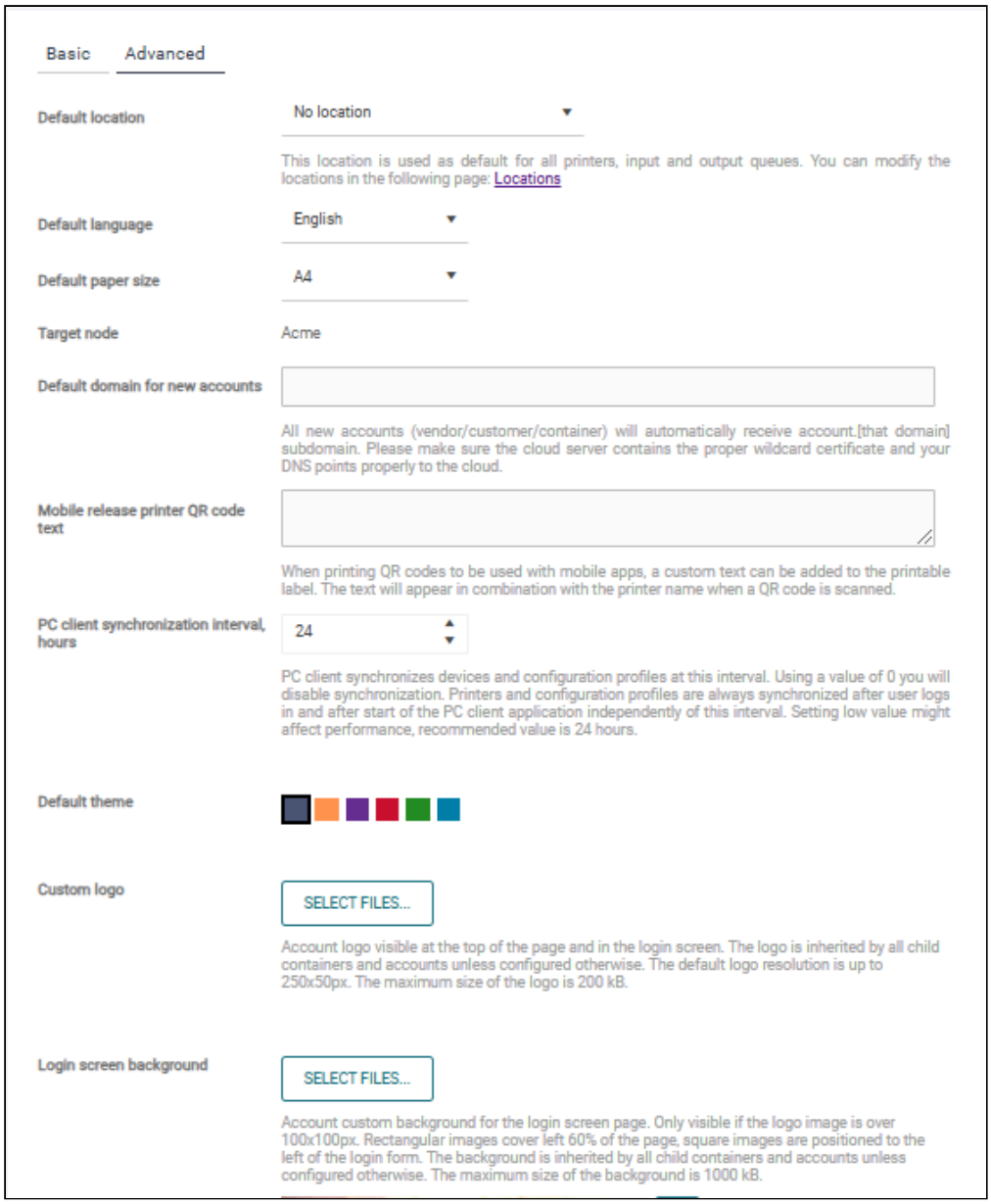
Configure the Vendor account or Customer account settings. Most options are the same for both types of accounts.

Basic



- Name – Enter a user-friendly name of the Vendor or Customer within the SAFEQ Cloud system.
- Application Name – The application name is automatically copied from the Name field when creating the account but you can modify it. Note that the Application name is primarily for display purposes.
- Domains – Add the domain names that uniquely identify this Vendor or Customer. You can add multiple domain names, one per line. You can use commas and semicolons as separators between domain names. They will automatically be converted to a new line upon saving. When creating the account, the first domain name will be automatically copied from the Name field. During the copying, it will be converted to a valid domain name format. If any parent Vendor account of this new Vendor or Customer account has the "Default domain for new accounts" set, then this value from the closest Vendor will be used as a suffix to your domain name. See the above screenshot where the ".eu.example.cloud" part was inherited from a parent Vendor.
- Application Name – Add an application name for the Vendor or Customer. This is primarily for display purposes only.
- OEM Logo – Upload a logo image file that will be displayed both in the top right side of the SAFEQ Cloud Web UI and on the login screen for this Vendor or Customer.

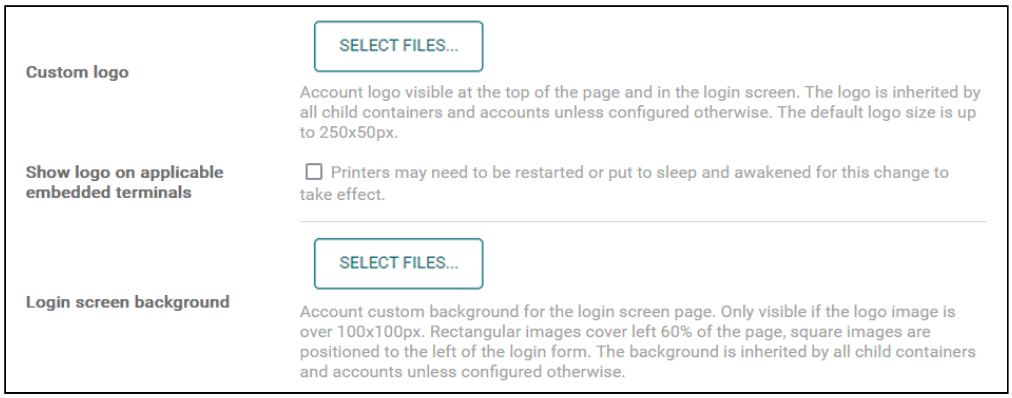
Advanced



- Default location – This value indicates the Vendor or Customer location. If no location is set on the Vendor or Customer, the no data value will automatically be assigned to the Location parameter.
- Default language – The default language of the account.
- Default paper size – The default paper size of the account.
- Default duplex mode – Duplex mode for default Configuration profile. Note: This setting serves only for creating default profile during customer creation and will not be visible once customer has been created.
- Default color mode – Color mode for default Configuration profile. Note: This setting serves only for creating default profile during customer creation and will not be visible once customer has been created.
- Target Node – This read-only value displays the parent node where the Vendor or Customer will be placed.

- Default domain for new accounts – Available only for Vendor accounts. The subdomain that all new Vendor or Customer accounts created under this new Vendor account will receive. The format is <account>.<Default domain for new accounts>. Make sure that the cloud server contains a correct wildcard certificate and that your DNS points correctly to the cloud.
- Mobile release printer QR code text – The text displayed under QR codes used to release print jobs via the Mobile application
- Policy for unknown location – This policy determines which print queues are available to the SAFEQ Cloud Client if it does not belong to any known location.
- Default theme – Allows you to change the visual style of the SAFEQ Cloud Web UI.
- Custom logo – Upload a logo image file that is displayed in the upper left corner of the SAFEQ Cloud Web UI and on the login screen for this vendor/customer account. The maximum size of the logo is 200 kB.
- Login screen background – Upload an image file that is displayed on the login screen of the SAFEQ Cloud Web UI. The maximum size of the background is 1000 kB.

Some options are specific only for customer accounts:

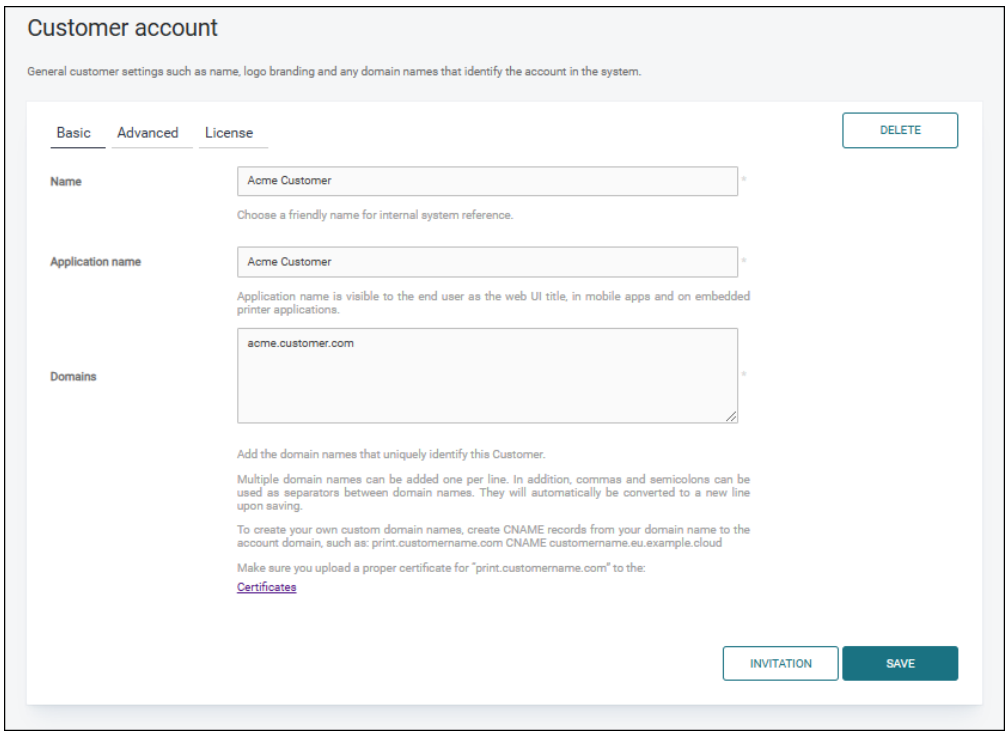


- Show logo on applicable embedded terminals – Check the checkbox so the image uploaded in Custom logo appears also in the upper left corner of an installed Embedded Terminal.

Click SAVE to create the Vendor or Customer entity within the SAFEQ Cloud system.

Editing the settings

Select the appropriate node in the SAFEQ Cloud system tree. This will open the navigation sub-menu. In the sub-menu, click Customer account.



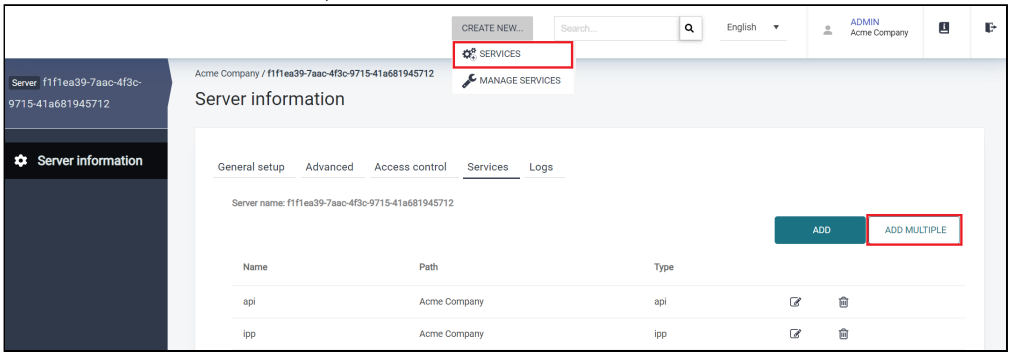
8.1.8 SERVICES

Services are software agents in YSoft SAFEQ Cloud that manage the workflow of the document process, for example, authentication, printing, or document storage.

Adding and removing multiple services to/from a server

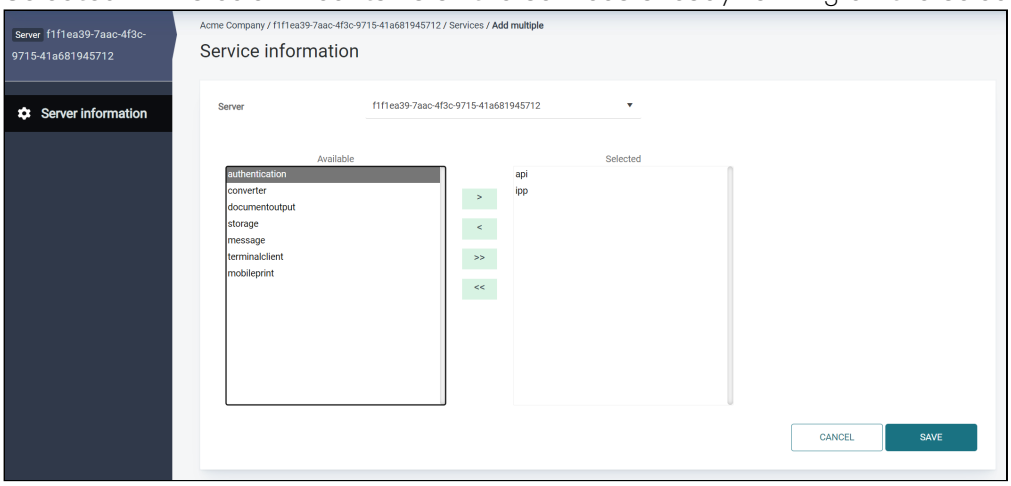
You can add or remove multiple services from the SAFEQ Cloud system under a server node in the system tree. When a service is placed under a server node in the tree, it is owned by that parent node and will inherit any security and access control permissions granted to the parent.

1. To add and remove multiple services, click **Create new > Services** or click **Add multiple**.



2. The Service information screen will be displayed. It contains the following elements:
   a. **Server** – The server where you are adding services or removing them.
   b. **Available** – This column contains all the services not yet running on the selected server.

c. **Selected** – This column contains all the services already running on the selected server.



3. Click **SAVE** to save your changes.

> A service can also be added directly to a server in the **Server** > **Services** group, see Settings section.

Service information settings

When adding a service, specify the following, to determine the service role, the host server, and other settings:

1. **Name** – User-friendly name of the service as it appears in the SAFEQ Cloud navigation tree.
2. **Type** – Choose service type. See the table in section *List of available services in SAFEQ Cloud* for the available types.
3. **Use Separate JVM** – Select this option to run the service within its own JVM on the target server. Running the service within its own JVM instance eliminates potential Java class or system resource conflicts and ensures that the service does not affect any existing services or the main application. It can be useful if you need:
   - to constrain the resources (CPU and memory) consumed by a service
   - to monitor the behavior of each service instance

Be aware that enabling separate JVM mode has higher requirements on the hardware; in particular, more RAM is typically needed.

4. **Enabled** – Controls whether the service is active or not.
5. **Location** – This value indicates the service location. If no location is set in the service, it will retrieve and display the inherited location of the parent (Account).
6. **Server** – Select the target server or servers where the service should run. The service will be hosted on the selected server(s) after it is created. Only servers that exist on the same branch within the SAFEQ Cloud system tree will be displayed.

   Some services can run only on a single server (such as Storage), while others (such as Document Output service) can run on multiple servers. This is useful for load balancing a service across multiple servers and providing redundancy for a service, so if one server goes down, the service will continue to run on the other server.

Click **SAVE** to create and run the service on the target server(s).

Note you may only host one instance of a service type on the same server.

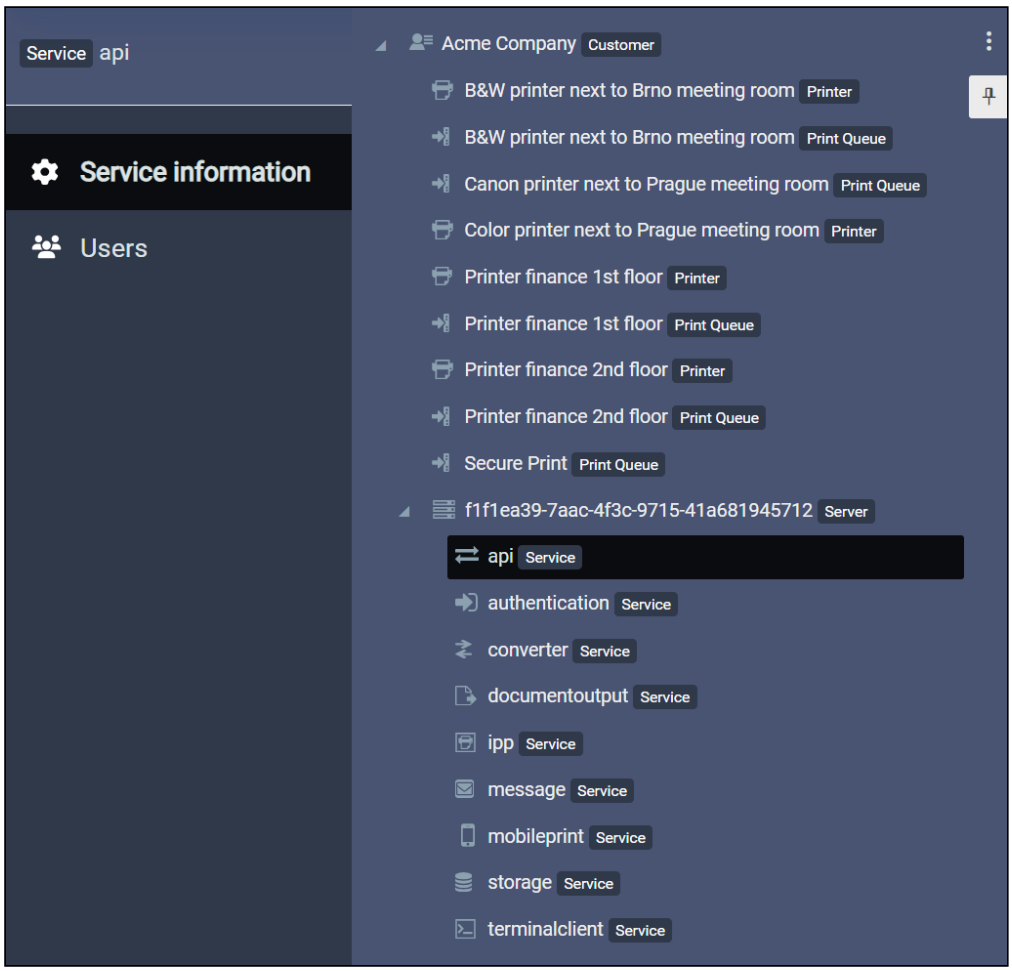
The list of available services in SAFEQ Cloud

Service type	Description
API	A service used to programmatically interact with SAFEQ Cloud, for example, from external applications, automation scripts, etc.
Authentication	A service that communicates with AD/LDAP directories, Microsoft Entra ID, and similar to authenticate users.
Conversion	A service responsible for converting or preparing documents in one format to another, for example, converting a Word document to PDF.
Document Output	A service responsible for delivering print job data to printers or MFDs.
IPP	A service that receives print job data from SAFEQ Cloud clients (Windows, Mac, and Linux).

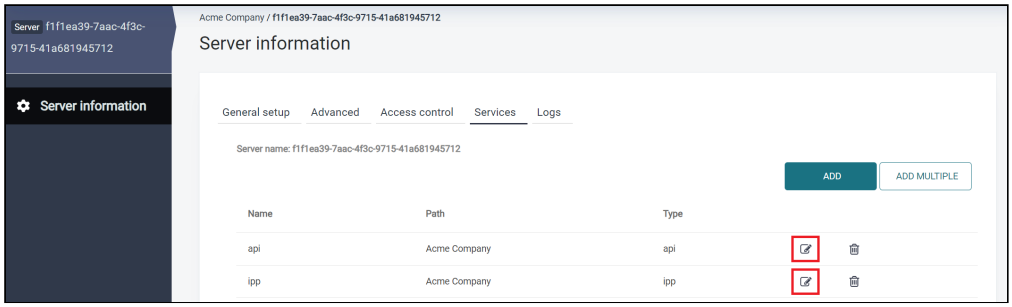
Service type	Description
Mobile	A service handling communication from Y Soft Apps, MDM solutions, Wide Area Mobile Print DNS communication, etc.
Storage	A service responsible for transferring and storing documents.
Terminal Client	A service that deploys embedded terminal clients running inside MFDs, and the service with which MFDs communicate for authentication, retrieving jobs and other purposes.
Message	A service is responsible for delivering messages, such as emails, from SAFEQ Cloud to external systems, such as email SMTP servers.

Editing a Service

Edit a Service by clicking the Service name within the SAFEQ Cloud System tree and clicking Service information.

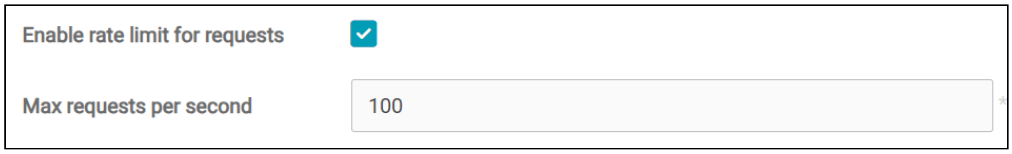


You can also manage services in the **Services** tab of the host server (either select the server from the navigation tree or under the **Security** section > **Endpoints** page > **Servers** tab and edit server). Click the edit or delete icon in the list to edit or delete the service from SAFEQ Cloud.



Limiting Request rate

To minimize the denial of service attack possibility, the API and IPP services can be configured to limit the number of requests per second from a given IP address. You can modify this in the service configuration screen:

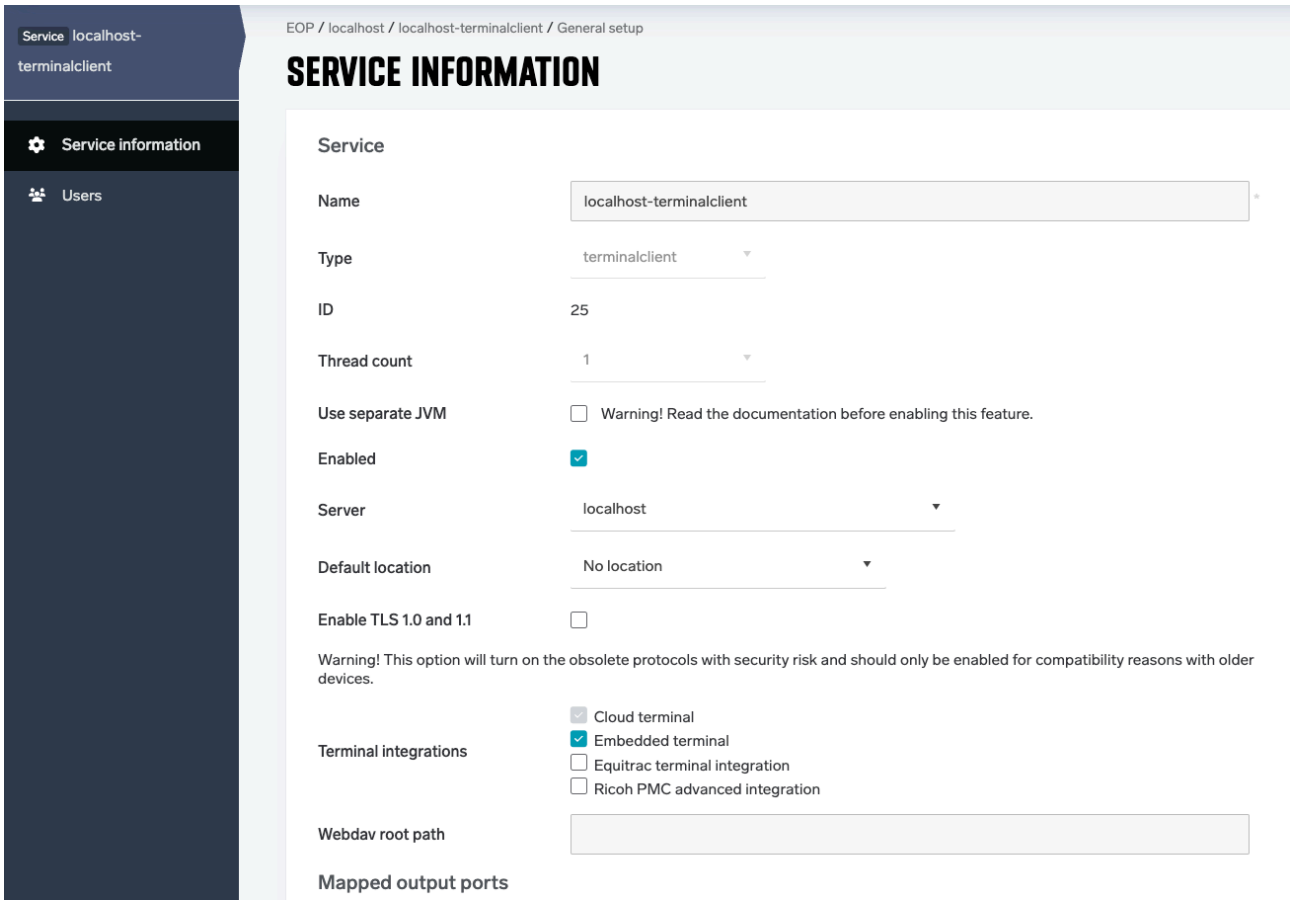


If the number of requests exceeds the given limit, the client will receive HTTP error 425.

Enable Cloud terminal integration

Prerequisites: *terminalclient* service is added, for information on how to add a new service, see section Services.

Cloud terminal integration is now enabled by default and cannot be disabled. No manual action is required.

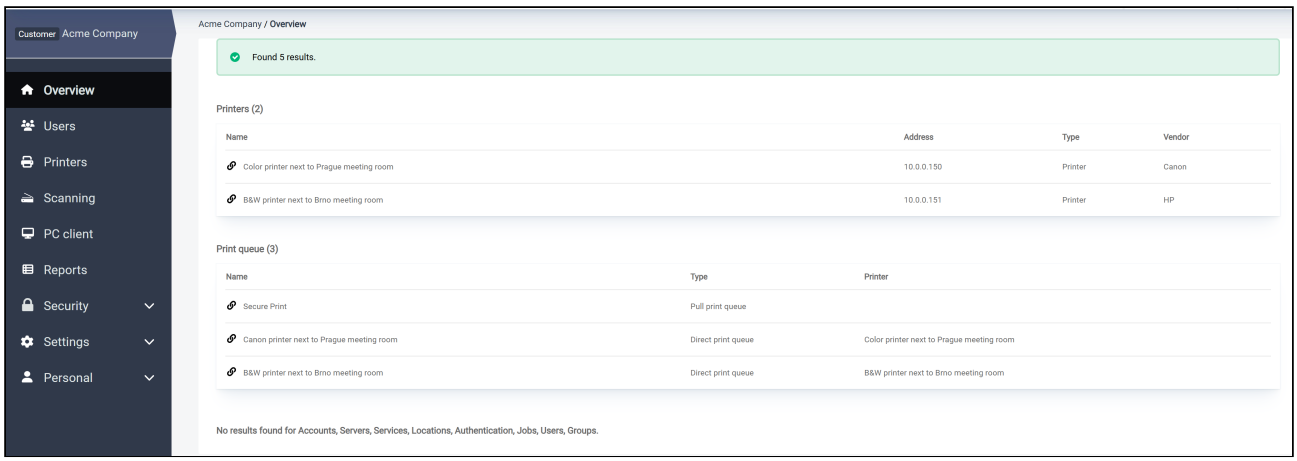


8.1.9 SEARCH FUNCTIONALITY

Use the search functionality to find information for a specific account. When you search for an element, the output will provide information that is linked to the first parent of vendor account or customer account based on the selected element from the navigation tree.

Searchable elements by selection type:

- Vendor: accounts (vendors, customers, containers), servers, services, locations
- Customer: containers, printers, input ports, servers, services, locations, authentication providers, jobs, users, groups



The limit for the results is 40 for each category. If you need more results, your search should be more specific. For users and groups, the limit is 20 entries for each authentication provider.

Some found items like accounts, printers, input ports, servers, services, locations, and authentication providers have a redirect link to go to the desired element.

The minimum number of characters needed for search functionality is 3.

See below for each search category the necessary permissions, search fields, redirection, and other information.

Accounts

Permission: SearchAccount
Search fields: Name
Redirection: Account settings

Printers

Permission: SearchOutputPort
Search fields: Name, Address
Redirection: View printer

Input ports

Permission: SearchInputPort
Search fields: Name
Redirection: View input port

Servers

Permission: SearchServer
Search fields: Name, UUID
Redirection: Server settings

Services

Permission: SearchService
Search fields: Name
Redirection: View service

Locations

Permission: SearchLocation
Search fields: Name
Redirection: View location
Information: The search for locations is works only for the selected account. It will not take into account the locations within child accounts.

Authentication providers

Permission: SearchAuthProvider
Search fields: Name, Domain, Type, Client identity provider type
Redirection: View authentication provider

Jobs

Permission: SearchJob
Search fields: Name, User, UUID
Information: Only documents with the status Ready and Printed are searched.

Users

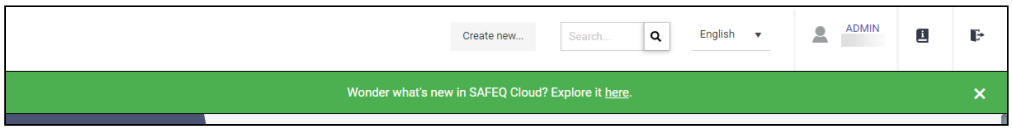
Permission: SearchUser
Search fields: Username, Full name, Email
Information: Users are searched in the local provider and all active authentication providers.

Groups

Permission: SearchUser
Search fields: Name
Information: Groups are searched in the local provider and all active authentication providers.

8.1.10 NOTIFICATIONS

Whenever SAFEQ Cloud is updated to a new version, the notification with a link to the release notes appears at the top of the SAFEQ Cloud Web UI. It will be displayed until you close it manually. You will only see these notifications if you have the ViewNewReleaseNotification permission.

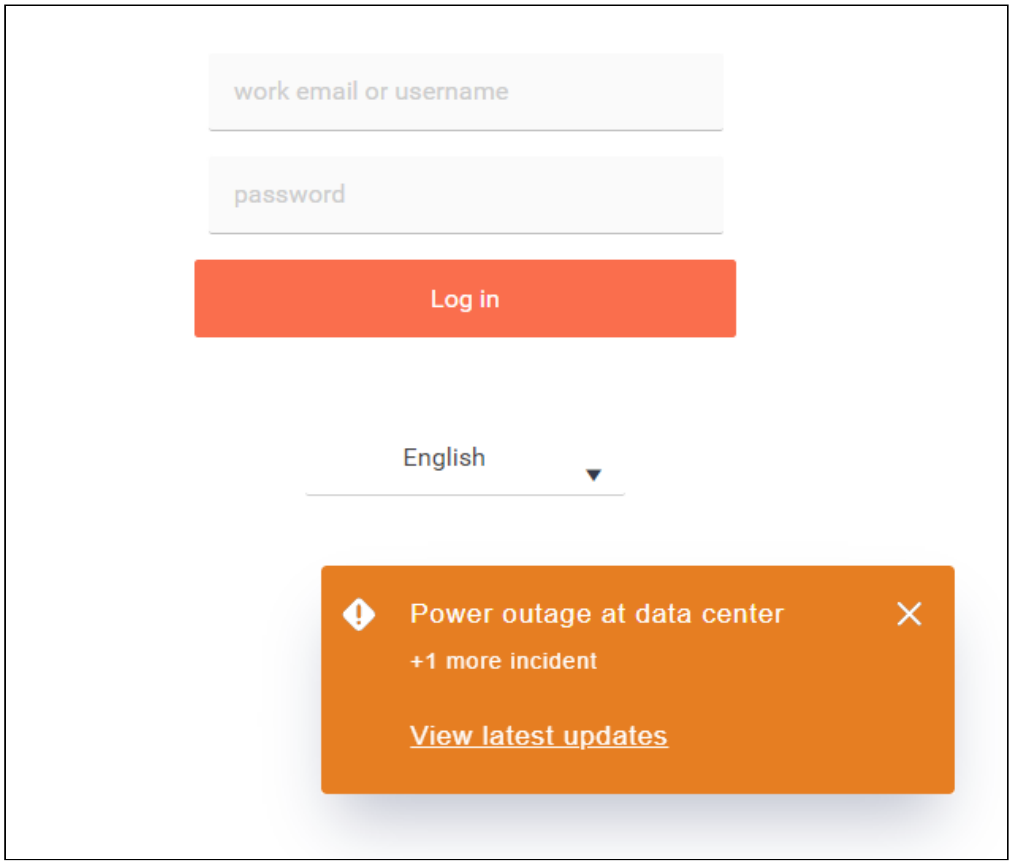


8.1.11 CREATING A CLOUD STATUS WIDGET

This guide is for creating your own cloud status & maintenance notification widget for your primary server. Whenever there is a cloud incident or a planned maintenance, the widget will be displayed to all users on SAFEQ Cloud Web UI login page and Web UI homepage.

⚠ To create the widget, you need to edit the application.conf file. Note that this setting applies to the whole production environment, so you must have admin rights for the whole environment to set it up.

The notification widget is based on statuspage.io. This is a platform that allows companies to create and maintain a public status page for their online services, displaying real-time updates about the status of their systems, such as service outages, scheduled maintenance, or performance issues.



Prerequisites

You have your own SAFEQ Cloud production environment with its own *application.conf* file.

How to

By default, the cloud status and scheduled maintenance notifications are not enabled. The process of enabling them consists of setting up your own statuspage.io account, creating a script, which will generate a frame version of the embed version of your status page, and modifying the primary server configuration to enable the notifications.

Perform the following steps:

1. Go to statuspage.io and set up your own account.
2. Create a script which will be pointing to the embed version of your status page. You can set the position and transition of the cloud status embed widget. Make this script publicly accessible. Example: *https://[address-of-status-script-page]/embed/script.js*.

```
(function(){

    var frame = document.createElement('iframe');
    frame.src = 'https://[your-status-page].statuspage.io/embed/frame';
    frame.style.position = 'fixed';
    frame.style.border = 'none';
    frame.style.boxShadow = '0 20px 32px -8px rgba(9,20,66,0.25)';
    frame.style.zIndex = '9999';
    frame.style.transition = 'left 1s ease, bottom 1s ease, right 1s ease';

    frame.title = 'YSoft SAFEQ Cloud Status';
    frame.ariaHidden = true;

    var mobile;
    if (mobile = screen.width < 450) {
      frame.src += '?mobile=true';
      frame.style.height = '20vh';
      frame.style.width = '100vw';
      frame.style.left = '-9999px';
      frame.style.bottom = '-9999px';
      frame.style.transition = 'bottom 1s ease';
    } else {
      frame.style.height = '115px';
      frame.style.width = '320px';
      frame.style.left = 'auto';
      frame.style.right = '-9999px';
      frame.style.bottom = '60px';
    }

    document.body.appendChild(frame);

    var actions = {
      showFrame: function() {
        frame.tabIndex = '0';
        if (mobile) {
          frame.style.left = '0';
          frame.style.bottom = '0';
        }
        else {
          frame.style.left = 'auto';
          frame.style.right = '60px'
        }
      },
      dismissFrame: function(){
        frame.style.left = '-9999px';
        frame.tabIndex = '-1';
      }
    }

    window.addEventListener('message', function(event){
      if (event.data.action && actions.hasOwnProperty(event.data.action)) {
        actions[event.data.action](event.data);
      }
    }, false);

    window.statusEmbedTest = actions.showFrame;
```

```
})();
```

3. Open your *application.conf* file located at */opt/safeqcloud/conf/application.conf.*
4. Edit the *cloud-status* section as follows:

```
cloud-status {
  embed-script-url="https://[address-of-status-script-page]/embed/script.js"
  custom-script-src-directive="https://[address-of-status-script-page]"
  custom-frame-src-directive="https://*.statuspage.io"
}
```

   a. embed-script-url – The URL of the status embed script. You can obtain this in the statuspage.io administration and customize it.

   b. custom-script-src-directive – The script-src directive in Content Security Policy (CSP). This specifies the valid sources from which scripts can be loaded on a web page. It should contain the server address where the script is hosted.

   c. custom-frame-src-directive – The frame-src directive in Content Security Policy (CSP). This specifies the valid sources from which frames or iframes can be embedded into a web page. It must contain the server address of the statuspage.io, where the frame will be taken from.

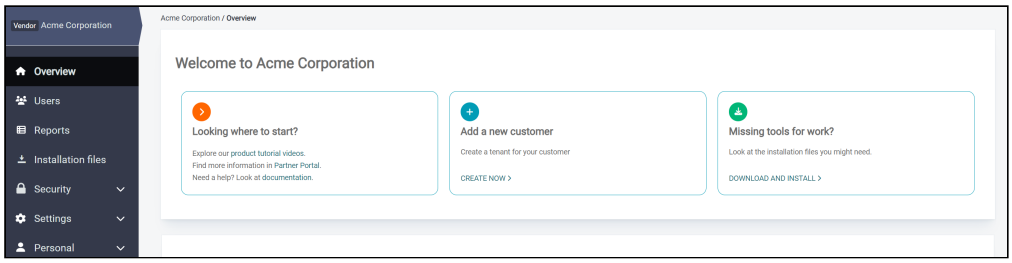
5. Save the file.

8.1.12 OVERVIEW

Each Account node in the YSoft SAFEQ Cloud system tree has an **Overview** landing page showing:

- The Quick start steps (customers only)
- Statistics and charts for Account health (customers only): Print activity, Top 5 Users, and Top 5 Devices.

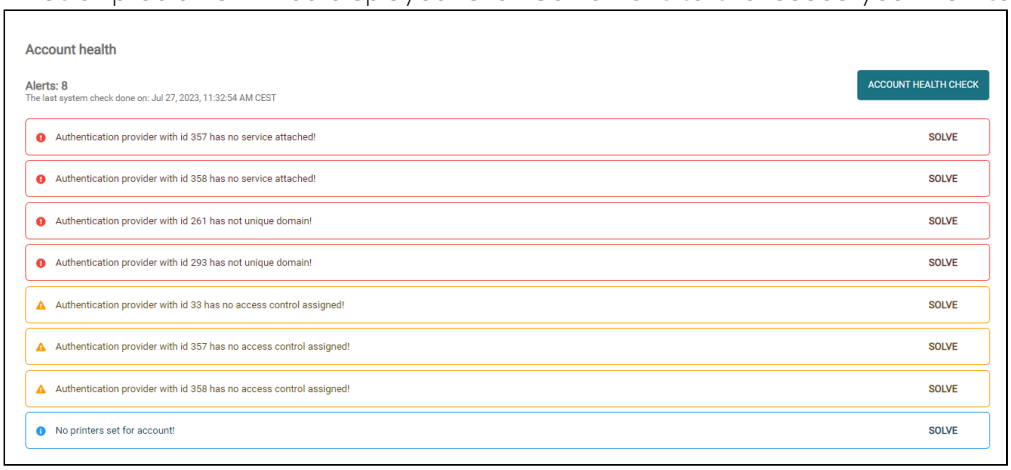
Where there are multiple levels and sub-accounts, the **Overview** page will reflect the aggregate total of activity taking place at that level in the tree.



Account health

1. Click **Account health check**.
2. SAFEQ Cloud will validate the current configuration of the account.

3. A list of problems will be displayed. Click **Solve** next to the issues you wish to resolve.



4. Once an alert is solved, it will not be visible when you click **Account health check** next time.

Available check alerts:

1. License validity
2. License validity in 30 days
3. Test authentication providers
4. Check for Input ports without a valid output port
5. Authentication providers without any authentication service
6. No authentication providers set
7. Printers without a document output service
8. No output ports (printers) defined for account
9. Embedded printers with no embedded configuration
10. Embedded printers with no terminal service attached
11. Authentication provider has no access control assigned
12. Active authentication providers share the same domain
13. Secondary servers that host used by printers services are offline
14. No messaging configurations available

Alert Severity:

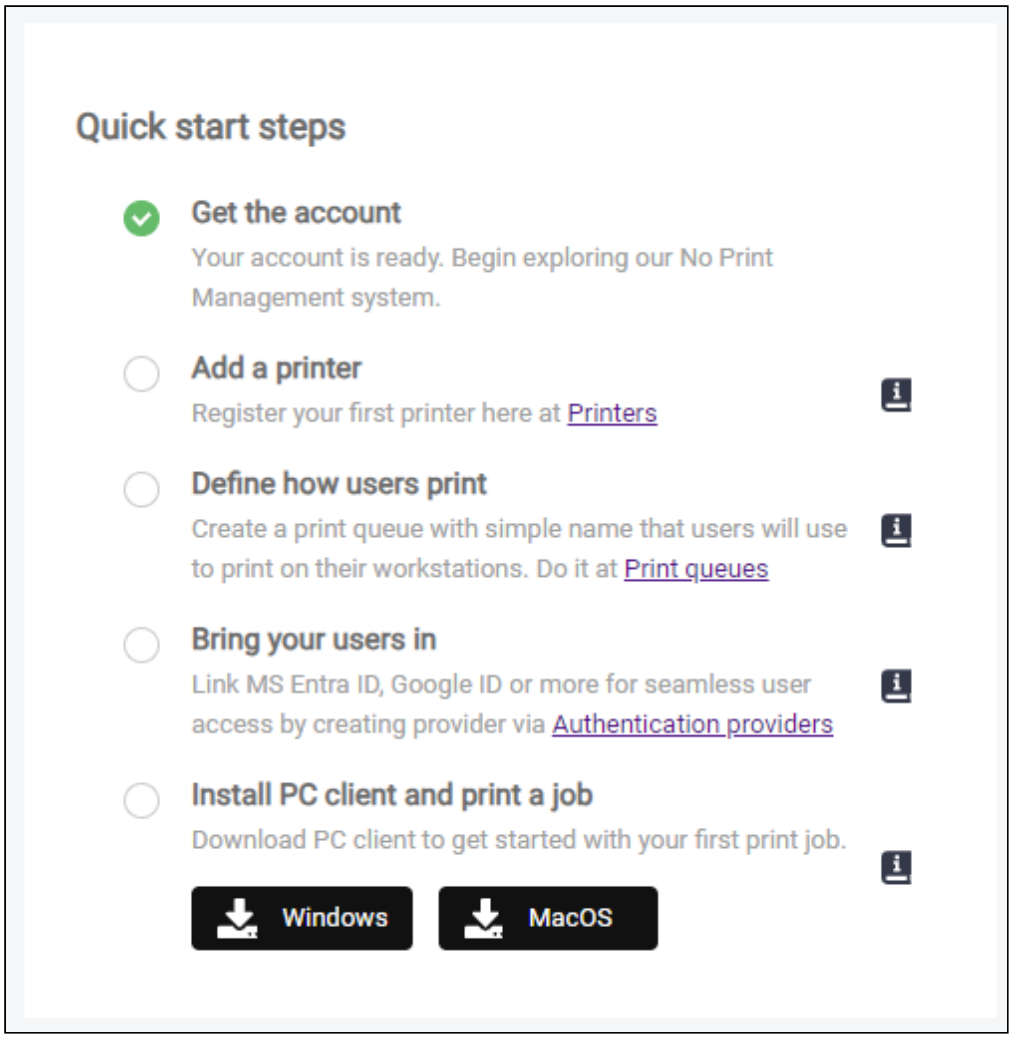
- **error** – The corresponding functionality will not work properly unless the problem is solved.
- **warning** – The corresponding functionality may not work properly in the future.
- **info** – The corresponding functionality has not been set yet.

Quick start steps

After account creation, each customer account will display a panel with several steps that you must complete before you can start printing.

When you complete a step, it will automatically be displayed as completed. Each step (except for the first one) contains a link to the documentation.

After completing all the steps, the panel will no longer be shown.



Conditions for completing the Quick start steps

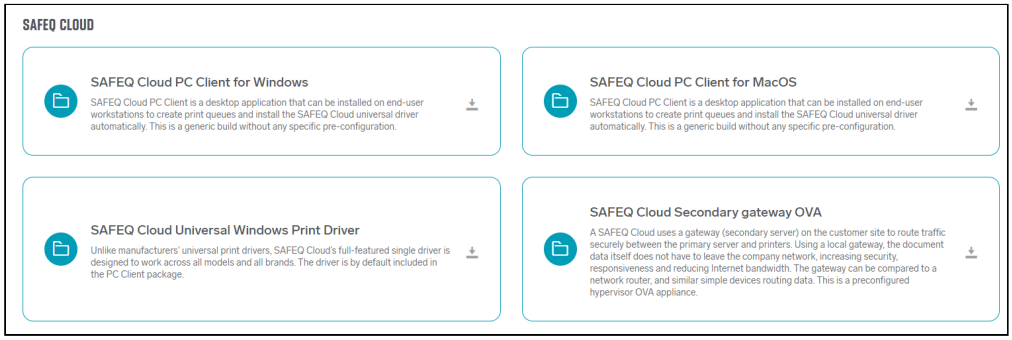
1. Get the account – Your SAFEQ Cloud account is already created, therefore this step always shows as completed.
2. Add a printer – Add at least one printer on the Printers page.
3. Bring your users in – Add at least one non-local authentication provider on the Users page under Authentication providers tab. Alternatively, add at least five local user accounts other than the default ones on the Users page under Users tab.
4. Install PC Client and print a job – Print at least one print job.

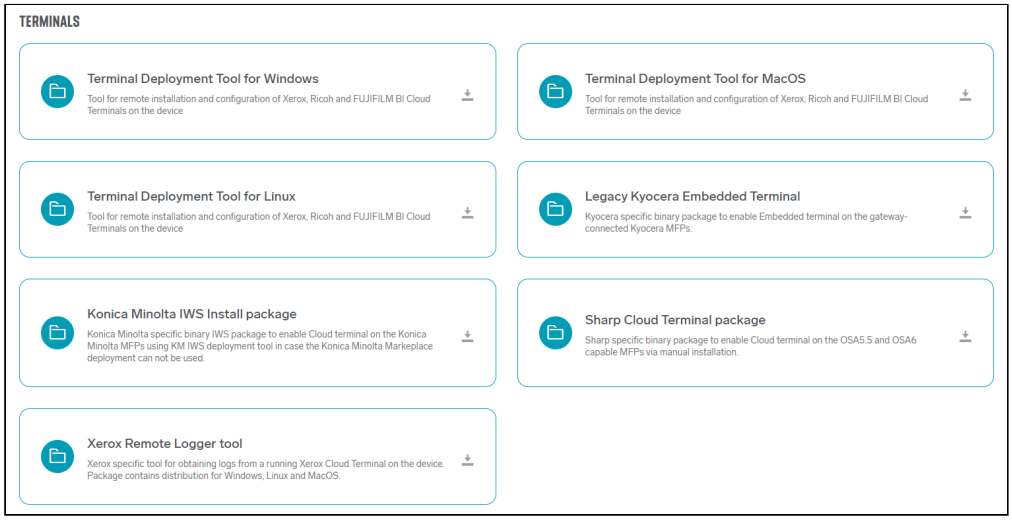
> Users will only see the download links if you assign them the ViewClientAndMobileDownload permission.

8.1.13 INSTALLATION FILES

In **Installation files** you can find download links for multiple products related to SAFEQ Cloud and terminals like PC client, driver, Terminal deployment tools, embedded terminals, etc.

The **ViewInstallationFiles** permission is required to display the page in the menu.





8.2 SAFEQ CLOUD CLIENT

SAFEQ Cloud Client is a desktop application that can be installed on end user workstations to automatically create print queues and install drivers based on the SAFEQ Cloud server configuration for a given account.

SAFEQ Cloud Client also provides the following features:

- Serverless direct printing to local printers.
- Serverless pull printing from embedded clients.
- Authentication using custom SAFEQ Cloud login, OpenID Connect workflow, or via session user name.
- Direct offline printing: automatically create direct queues in offline mode for the last used printers.
  - Direct offline printing only compatible with Local and Hybrid storage modes.
- Customized synchronization period.

- Location-based printer synchronization.
- Secure TLS channel to SAFEQ Cloud server with optional use of system certificates and possibility to authorize a specific Client from the SAFEQ Cloud Web UI.

8.2.1 SAFEQ CLOUD CLIENT OVERVIEW

SAFEQ Cloud Client consists of the background service and the frontend application. The service module is responsible for managing print queues, connectivity with SAFEQ Cloud server, printing and storage operations; the frontend part contains user interface for configuration operations.

There are three modes of operation:

1. The local storage mode. SAFEQ Cloud Client connects to the primary server via the persistent channel and performs all print and job storage operations locally. It is also possible to temporarily switch to gateway job delivery using system tray menu, which can be useful in the pull printing scenario when SAFEQ Cloud must be powered off. Local storage mode requires SAFEQ Cloud Client endpoint authorization in the SAFEQ Cloud server. For more details about endpoints, see Endpoints. When user prints, the jobs are stored on the PC. In the case of Citrix or other VDI, it depends on where the SAFEQ Cloud Client is running, specifically the underlying SAFEQ Cloud Client service "SAFEQ Cloud Client Core" runs. Jobs are stored on the Citrix server (where client core service runs) and they will remain there when the thin session is terminated, assuming they have session retention etc configured in their VDI environment.
2. The gateway mode, in which SAFEQ Cloud Client sends all print jobs to the SAFEQ Cloud server, and has no persistent connection to the server. When a user prints, the jobs are delivered from the PC to an SAFEQ Cloud server, either primary or secondary gateway, depending on configuration. Jobs are delivered to printer using a "Document Output" service.
3. The hybrid mode essentially switches modes based on print type. In the case of direct print, SAFEQ Cloud Client will store and deliver jobs locally and in the case of pull (secure print) it will deliver the job via the cloud. This mode requires registration and authorization in the SAFEQ Cloud server (same as local storage mode).

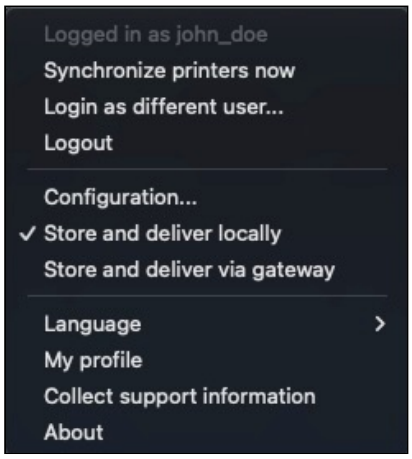
Jobs are delivered from the SAFEQ Cloud Client to the printer directly if the SAFEQ Cloud Client can reach the printer. If the SAFEQ Cloud Client cannot reach the printer, the job will automatically be routed via primary SAFEQ Cloud server to the appropriate "Document Output" service which will then deliver to the printer.

The mode of operation is chosen during installation and can be later changed by using `Service setup` configuration dialog as explained in section 7.5.1.

Which operation mode to choose depends on the customer solution configuration. If serverless operations are required and there is no primary or secondary SAFEQ Cloud server available on the local network then the SAFEQ Cloud Client should be configured with either local storage and delivery option or hybrid mode. In this case it will connect to the cloud SAFEQ Cloud server for authentication and job reporting purposes. If a local server is available, the SAFEQ Cloud Client may use it in the gateway mode.

In local delivery mode, the computer on which the SAFEQ Cloud Client is running must have a direct connection to the printer, to be able to deliver print jobs to the printer.

Service module is installed as a Windows service on Windows or launched daemon on macOS and runs under a privileged account. The frontend part shows a notification icon in the system tray and provides a default menu:



- Synchronize printers now – Perform manual printer synchronization.
- Login as different user... – Perform user authentication against the SAFEQ Cloud server (only visible if the SAFEQ Cloud Client is configured with a custom login authentication type).
- Logout – Perform user logout from SAFEQ Cloud server and delete synchronized printers.
- Configuration... – opens a configuration dialog.
- Store and deliver locally – Switch to local job delivery (only visible if local storage is enabled during installation).
- Store and deliver via gateway – Switch to gateway job delivery (only visible if local storage is enabled during installation).
- Language – Submenu to select the UI language from the list of supported languages.
- My profile – opens a new browser window with My profile.
- Collect support information – opens a dialog with options to collect logs (useful for troubleshooting).
- About – shows version and copyright information.

The taskbar icon indicates the current operational state of the SAFEQ Cloud Client:

- – idle state, connected to SAFEQ Cloud server
- – error state, no connection to background service (it is stopped or not functioning correctly)
- – synchronization is currently in progress
- – offline operation, no connection to SAFEQ Cloud server

SAFEQ Cloud Client will perform printer synchronization automatically based on the synchronization internal option. It is also possible to trigger manual synchronization by right-clicking the taskbar icon and choosing Synchronize printers now menu item.

New printers will appear automatically in the system, matching input ports configured on the server side and can be used immediately for pull or push printing depending on the input port configuration. When running in local storage mode, print jobs will be delivered directly to the printer

via TCP or IPP protocol, depending on the printer configuration in the SAFEQ Cloud Web UI. When gateway mode is enabled, the job will be sent to TCP port 7300 of SAFEQ Cloud server (via TLS secure channel). Make sure this port is opened on the server side.

8.2.2 SYSTEM REQUIREMENTS

SAFEQ Cloud Client is available for Windows 10 or later, Windows Server 2012 or later, and macOS 11 or later.

There are different requirements for SAFEQ Cloud Client depending on which operation mode is chosen in the installer.

1. For local storage and delivery mode:

- SAFEQ Cloud Client can only connect to SAFEQ Cloud primary server
- API service must be configured on the server
- Workstation must be able to communicate with primary SAFEQ Cloud server (see Ports and Protocols for port details)
- Workstation must be able to communicate with printers for printer status and print job delivery (see Ports and Protocols for port details)

2. For gateway mode:

- SAFEQ Cloud Client can connect to both SAFEQ Cloud primary and secondary gateway server. For the secondary gateway server, you must do secondary gateway mapping and create or import an SSL certificate (private certificate chain) with the correct CN corresponding to the domain mapped to the secondary server. See Secondary Gateway mapping.
- API service must be configured on the destination SAFEQ Cloud server or gateway
- Workstation must be able to communicate with SAFEQ Cloud server (see Ports and Protocols for port details)

Installation requires administrator privileges. The application itself does not require any privileges and will work under any user account.

For Citrix thin clients or Windows Terminal Services clients, user or location specific printers are not supported. Print queues created by the SAFEQ Cloud Client on Windows thin clients are all created as shared among all sessions on the Citrix or Terminal Services host. When SAFEQ Cloud Client detects the session is running in a Terminal Services session, it will not delete printers on custom logout.

8.2.3 INSTALLING SAFEQ CLOUD CLIENT ON MACOS

SAFEQ Cloud Client installer can be downloaded from SAFEQ Cloud Web UI.

SAFEQ Cloud Client can be installed in two ways:

- Quick installation – preconfigured installation without the possibility to change configuration after installation
- Advanced installation – installation with the possibility to change the configuration after installation

For general requirements and prerequisites, see System requirements.

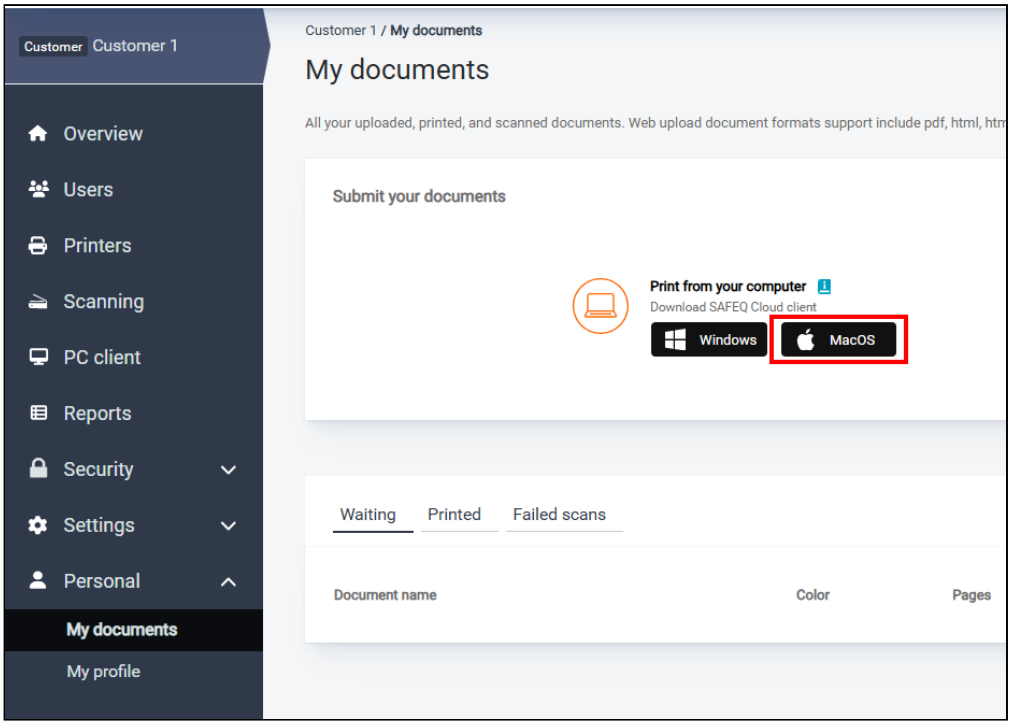
Quick installation

Limitations

- The client can not be installed in local storage mode.
- The Client is installed with the SAFEQ Cloud OAuth2 login authentication type.
- Once the Client is installed, the Configuration option is removed from the menu.

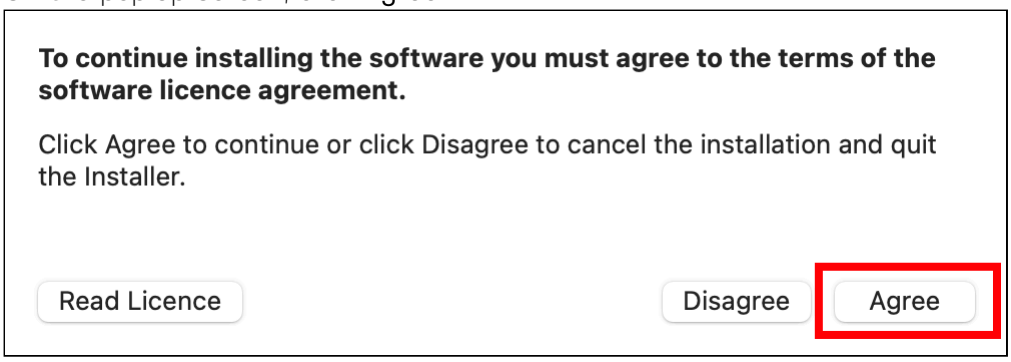
Do the following to install SAFEQ Cloud Client using the quick installation type:

1. Log in to your Web UI, navigate to **Personal** > **My documents**, and click **MacOS**.

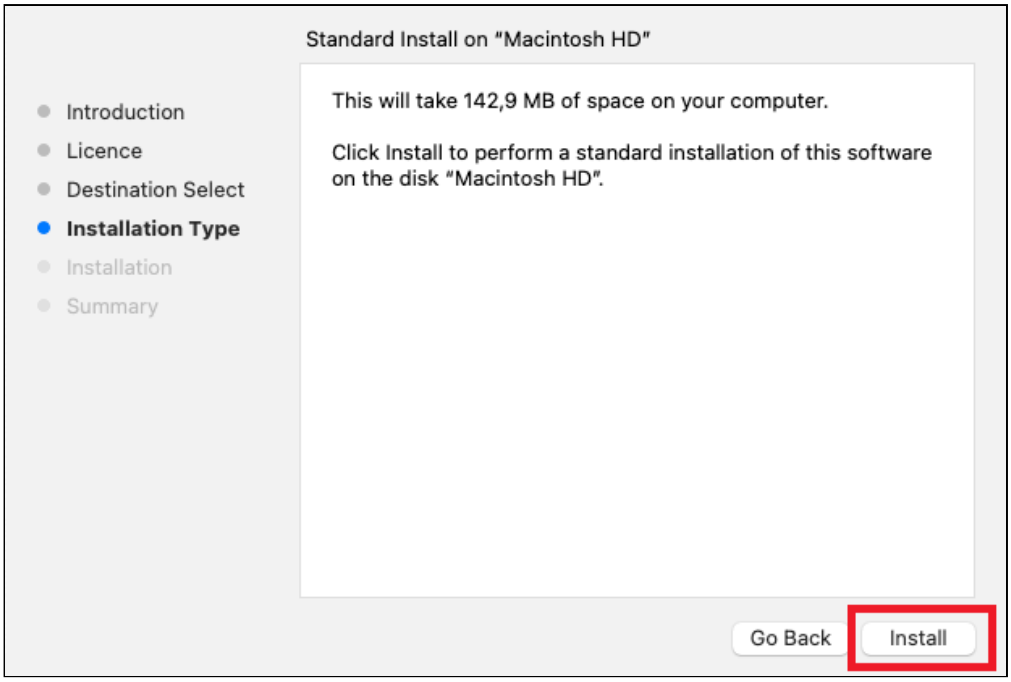


2. Run the installation file.
3. On the welcome screen, click **Continue**.

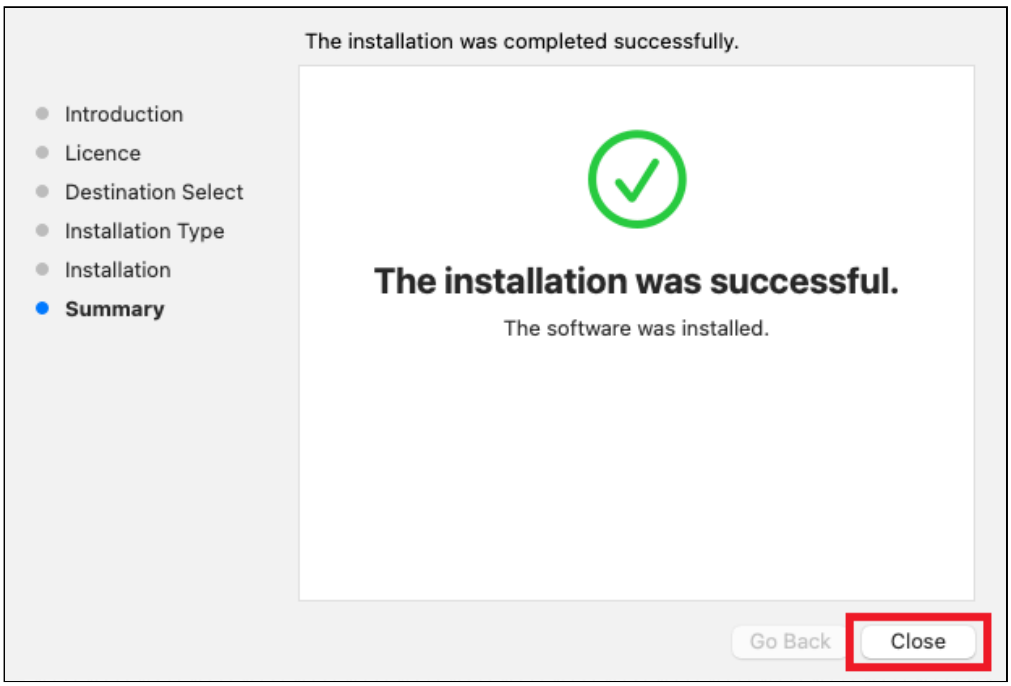
4. On the next screen, read the license agreement and click **Continue**. A pop-up screen will appear.
5. On the pop-up screen, click **Agree**.



6. On the **Installation Type** screen, click **Install**.



7. Authorize the installation, wait until the SAFEQ Cloud Client is installed, and then click **Close**.

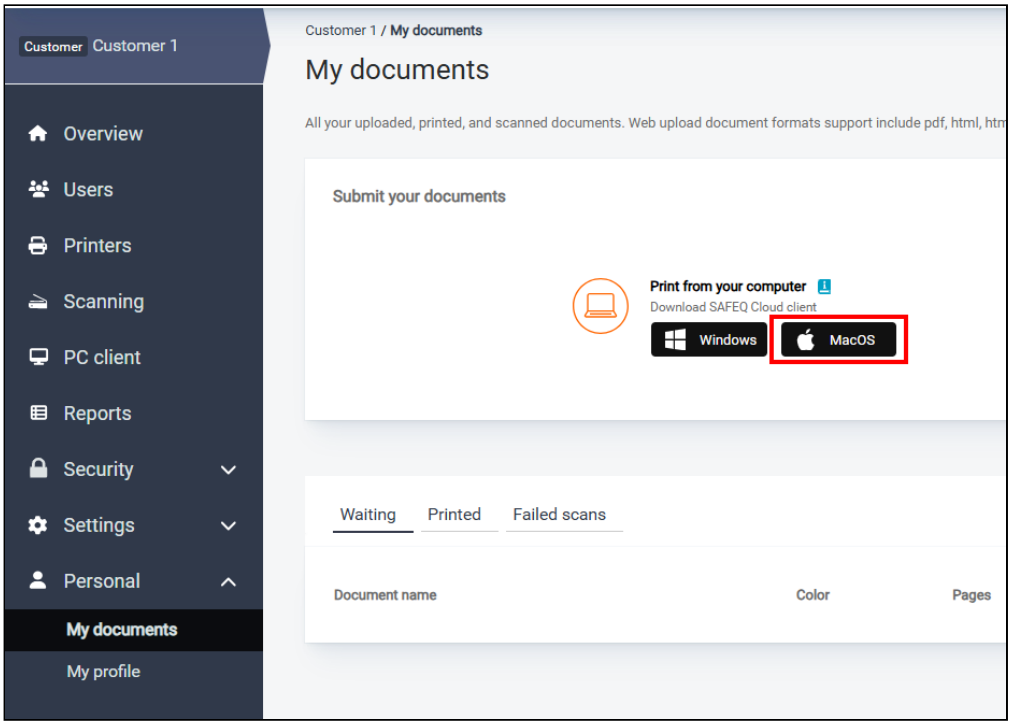


8. Log in on the login screen opened in your web browser.
9. The application starts automatically.

Advanced installation

Do the following to install SAFEQ Cloud Client using the advanced installation type:

1. Log in to your Web UI, navigate to **Personal** > **My documents**, and click **MacOS**.

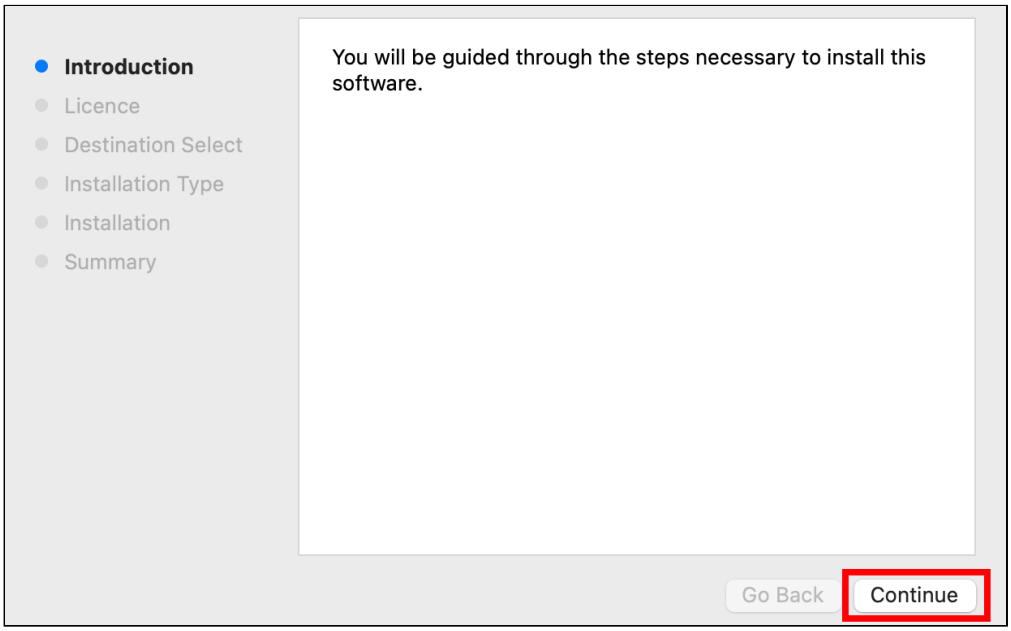


2. Modify the installer name so it does not contain your domain name in square brackets.
   Example: `safeq-cloud-client-x.x.x-setup[acme.eu.ysoft.cloud].pkg` -> `safeq-cloud-client-x.x.x-setup.pkg`

   > ⚠ If you keep the square brackets in the name of the installer, the installer will default to quick installation and you will not be able to configure the SAFEQ Cloud Client after installation.

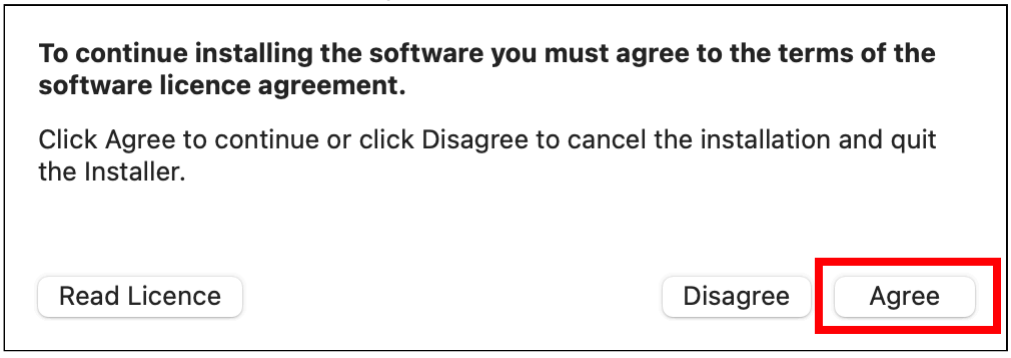
3. Run the renamed installation file.

4. On the welcome screen, click **Continue**.

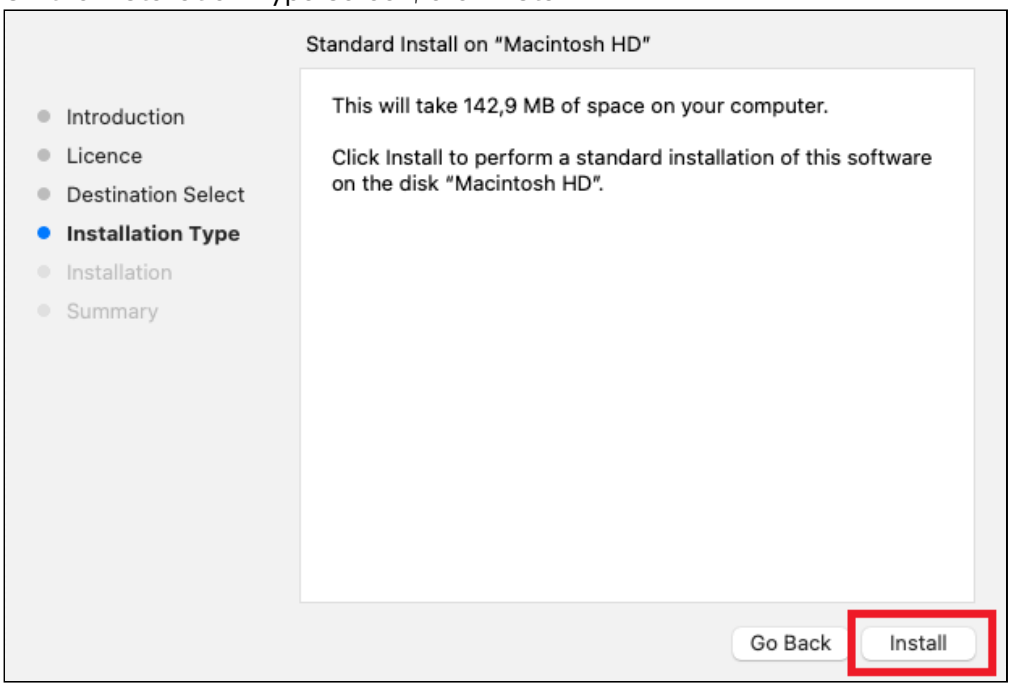


5. On the next screen, read the license agreement and click **Continue**. A pop-up screen will appear.

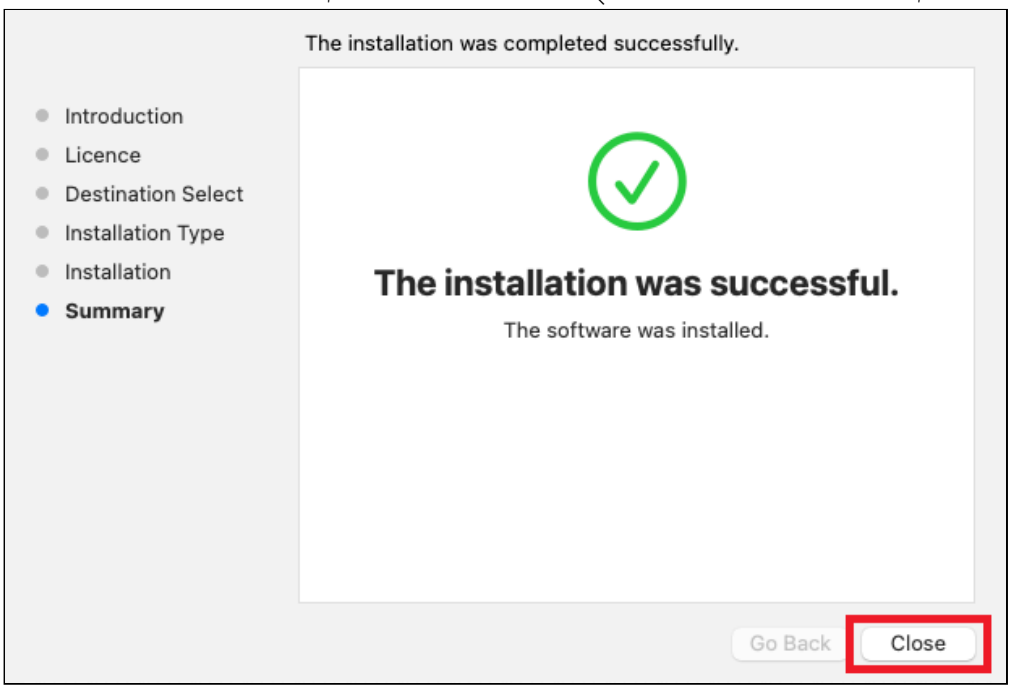
6. On the pop-up screen, click **Agree**.



7. On the **Installation Type** screen, click **Install**.

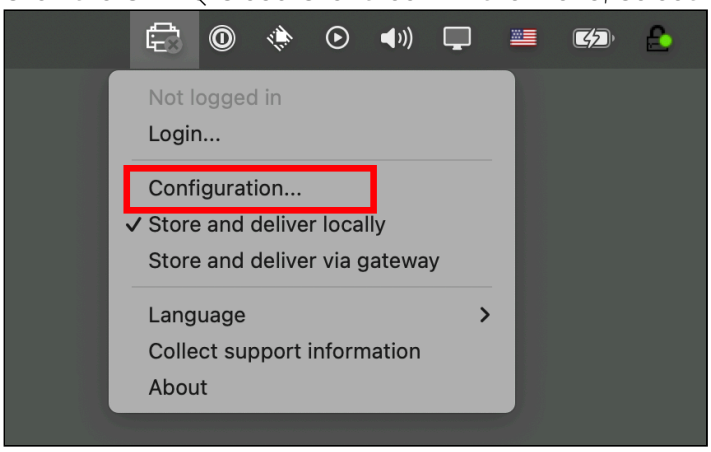


8. Authorize the installation, wait until the SAFEQ Cloud Client is installed, and then click **Close**.

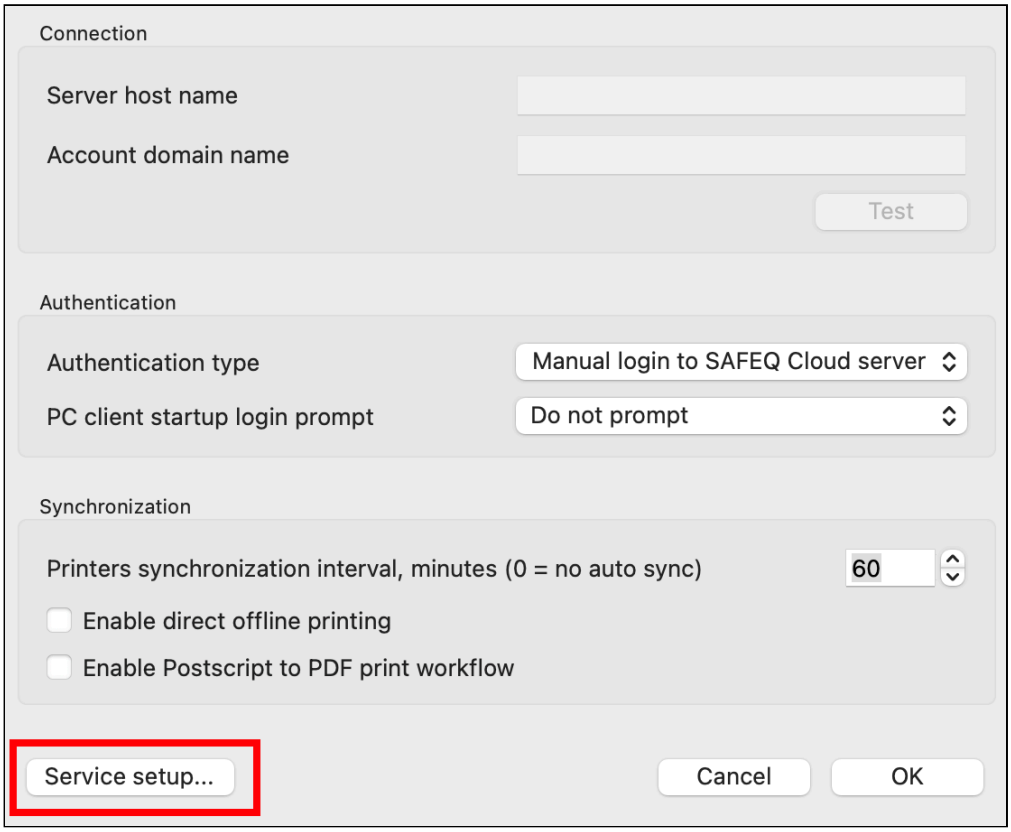


9. The application will start automatically.

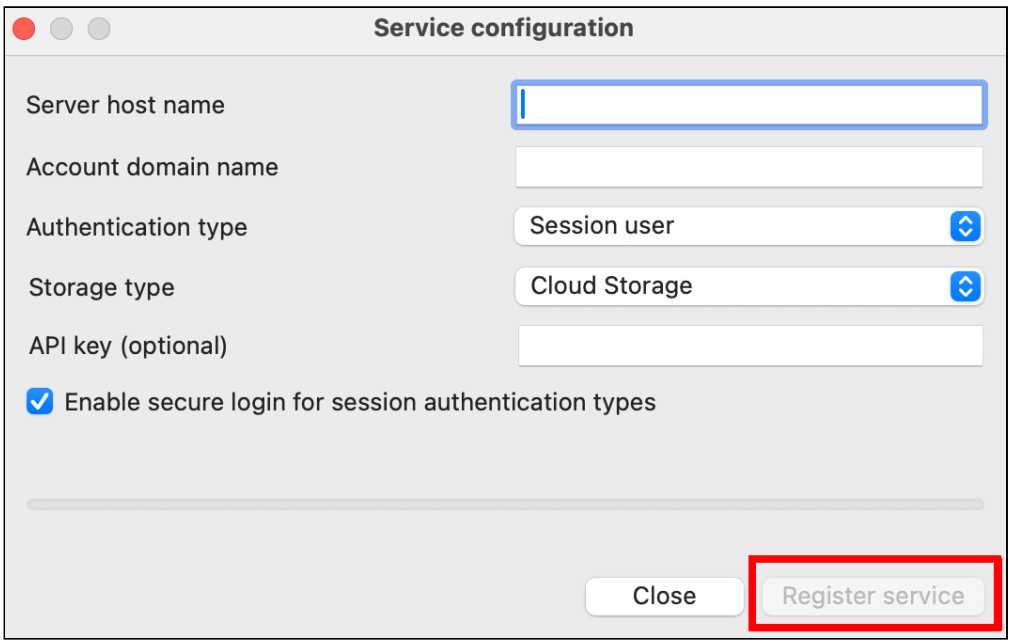
10. Click the SAFEQ Cloud Client icon. In the menu, select **Configuration**.



11. On the configuration screen, click **Service setup** and enter your password for the privilege elevation.



12. On the **Service configuration** screen, set your custom configuration, and then click **Register service**.



- Server host name – address or host name of the SAFEQ Cloud server to connect to. For "Local storage mode" the address should be the DNS of the SAFEQ Cloud primary server.
- Account domain name – domain name of the target account. It can be found in SAFEQ Cloud Web UI on the Customer information tab.
- Authentication type – select user authentication type.
- Storage type– select where SAFEQ Cloud Client stores the data: Cloud storage, Local storage, and Hybrid (direct print locally, secure print to cloud).
- API key – API key from the account settings. If omitted the default (restricted) API key will be used. Default API key will be removed in the future product versions.
- Enable secure login for session authentication types – see *secureSessionLogin* option below for details.

13. After the configuration, users can log in.

Unattended installation

> You can also use this guide to push the SAFEQ Cloud Client to Mac devices using tools like **jamf** or **Workspace ONE**.
> For further information, you can refer to these Jamf guides:
> - Jamf – deploying custom configuration profiles
> - Jamf – installing packages

.plist `com.ysoft.safeqclient.plist`

Below is a description of each of the parameters:

- `accountDomain` – account domain name.
- `allowConfiguration` – true = enable configuration menu item, false = disable configuration menu item. The default value is `true` (`false` for QuickInstall).
- `allowRememberLogin` – true = show the "Remember login" option when showing a prompt to enter a custom username and password, false = do not show this option. The default value is `true`.
- `apiKey` – custom API key to use instead of the default one.
- `authType` – User authentication type: 0 = session user, 1 = custom login, 2 = Microsoft Entra OAuth2, 5 = OpenID Connect, 6=SAFEQ Cloud OAuth2 login. The default value is `6`.
- `directOfflinePrint` – true = enable direct offline printing. The default value is `false`.
- `gatewayAddress` – SAFEQ Cloud gateway address.
- `loginPopupType` – specify the type of the login popup: 0=no popup, 1=informational bubble, 2=dialog. The default value is `0` (`2` for QuickInstall).
- `offline` – if set to true, it will install the SAFEQ Cloud Client in offline mode, without registration or server connectivity check. See this section for details. The default value is `false`.
- `refreshPeriod` – an automatic synchronization period in minutes. The default value is `60`.
- `rememberLogin` – turn on or off the login remembering option. The default value is `false`.
- `secureSessionLogin` – this option is applicable only when authType is set to 0 (Session user), 1 (Session user + domain name), or 3 (User principal name), which are considered insecure login types. This parameter is ignored during updates. The default value is true, meaning the SAFEQ Cloud Client registers an endpoint, requiring administrator authorization. When set to false, no endpoint is created, and the SAFEQ Cloud Client will only function if both Allow unauthenticated requests and Allow untrusted endpoints are enabled in the API key settings.
- `serverCheck` – This option is deprecated in favor of the `offline` option. The default value is `true`.
- `storageType` – specify the type of storage: 0 = cloud, 1 = local storage, 2 = hybrid (direct print locally, secure print to cloud). The default value is `0`.

Example of a `.plist` file:

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>accountDomain</key>
    <string>
acme.local</string>
    <key>authType</key>
```

```
    <integer>1</integer>
    <key>gatewayAddress</key>
    <string>server.acme.local</string>
    <key>loginPopupType</key>
    <integer>2</integer>
    <key>refreshPeriod</key>
    <integer>60</integer>
    <key>storageType</key>
    <integer>0</integer>
    <key>offline</key>
    <true/>
</dict>
</plist>
```

Jamf best practices

For Jamf deployment, it is recommended to use a script that runs before the pkg file is installed and copies the `.plist` file to the proper location.

SAFEQ Cloud Client supports two locations for the `.plist` file: `/Library/Preferences` and `/Library/Managed Preferences`. The latter can be used by Jamf deployment tool to deploy the preferences automatically without the custom script.

Script example:

```
#!/bin/bash
PLIST=/Library/Preferences/com.ysoft.safeqclient.plist
cat << EOF >$PLIST
[xml plist content]
EOF
defaults read $PLIST
```

Replace `[xml plist context]` with the actual `.plist` file.

Steps for silent installation

> You can also copy the .plist file to `/Library/Preferences` if the configuration is to be shared by all users. This requires a restart of Mac devices or running the `defaults read /Library/Preferences/com.ysoft.safeqclient.plist` command.

1. Copy the updated `.plist` file at `/Users/[username]/Library/Preferences` on Mac device

```
sudo cp <from path> /Library/Preferences
```

2. Install SAFEQ Cloud Client

```
sudo installer -pkg safeq-cloud-client-2025.02.06.2-setup.pkg -target /
```

3. Uninstall SAFEQ Cloud Client

```
sudo /Applications/safeqclient.app/Contents/MacOS/uninstall
```

Download this sample file to update it with the desired SAFEQ Cloud Client configuration parameters. Make sure the file is named as

8.2.4 INSTALLING SAFEQ CLOUD CLIENT IN OFFLINE MODE

In some situations, it is desirable to install SAFEQ Cloud Client offline, i.e. without server connectivity. For example, when the IT department prepares target workstation images to be rolled out on the user PCs.
The installer allows this with an additional installation option, **Enable offline installation** in the installer UI or with `/OFFLINE=true` unattended command line parameter.

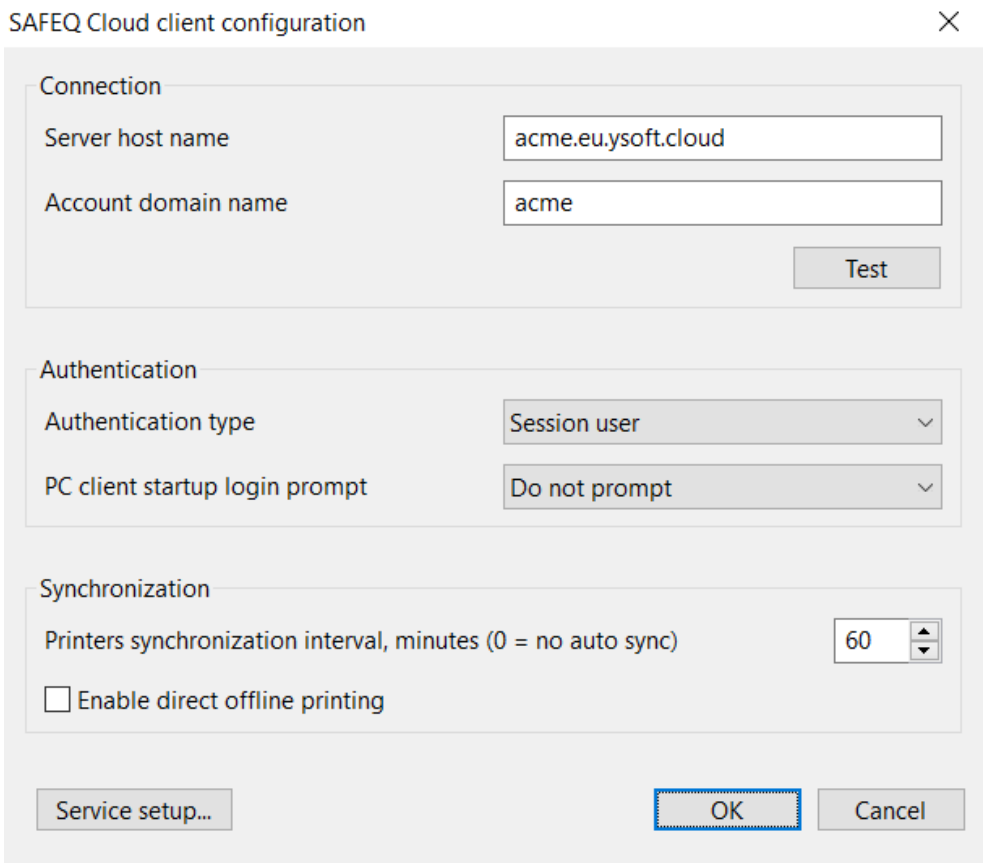
When this option is enabled, the SAFEQ Cloud Client will not attempt to communicate with the server or register itself as an endpoint on the server side. Also, the client won't start automatically after installation, so a PC reboot is required. Additionally, SAFEQ Cloud Client will use a machine GUID identifier acquired from the operating system instead of generating a random UUID during installation, for compatibility purposes with cloned PC images.

When the SAFEQ Cloud Client core service starts, it will automatically attempt to register itself against the SAFEQ Cloud server if registration is not done yet. In case it's not possible (e.g. due to network error), the re-registration will be attempted every 30 seconds.
After registration succeeds SAFEQ Cloud Client will transition to normal operation.

8.2.5 SAFEQ CLOUD CLIENT CONFIGURATION

⚠ This configuration is not enabled on SAFEQ Cloud Client installed using the quick installation scenario.

Users can modify several client settings using the configuration dialog:



Server host name – host name of the SAFEQ Cloud server or gateway to which the client will connect. If SAFEQ Cloud Client is running in local storage mode this option can only be changed via `Service setup` button.

Account domain name – domain name of the customer account configured on SAFEQ Cloud server. If not specified it will be inferred from the gateway address setting. If SAFEQ Cloud Client is running in local storage mode this option can only be changed via the Service setup button.

Test – the user is informed about the connection (SAFEQ Cloud gateway address and the account domain name should be accessible in order for the connection to be successful)

Authentication type – currently following authentication types are supported:

- Session user – username from the current OS session is used for authentication and job sending.
- Session user + domain – username@ad-domain from the current OS session is used for authentication and job sending. This matches server setting 'strict domain validation'.
- Session user principal name – UPN is used for authentication and job sending (whatever UPN configured in user profile, it can be the same as username@ad-domain for simple AD setups).
- Manual login to SAFEQ Cloud server – The user will be prompted to enter user name and password which will be validated in the SAFEQ Cloud server.

- Microsoft Azure login (deprecated) – Online authentication is performed against Microsoft Entra ID using OAuth2 workflow. This option is deprecated in favor of "SAFEQ Cloud OAuth2 login".
- OpenID Connect login – Perform online authentication against OIDC-compliant identity provider by opening a browser window with OAuth2 workflow. This authentication type supports MFA and requires SAFEQ Cloud server to have at least one authentication provider defined with the type `Client`. If a single client-based authentication provider is defined for a given account the user will be redirected to that identity platform. If multiple client-based authentication providers are defined a generic OpenID connect window will be shown prompting the user to enter his or her username. Based on the domain part of the user name the browser will be redirected to the matching identity platform. The following identity platforms are currently supported: Microsoft Entra ID, Google GSuite, Ping Identity.
- SAFEQ Cloud OAuth2 login – Uses a new server login screen with configurable providers for user login.

  For this authentication option to work properly, HSTS needs to be disabled for the localhost domain in your browser.

SAFEQ Cloud Client startup login prompt – currently following options are supported after the user restarts the Windows machine:

- Don't show – no notification will be shown by the SAFEQ Cloud client
- Informational popup – the user is asked to login into SAFEQ Cloud Client, "Please login to synchronize printers"
- Login dialog – the login to print popup appears on the screen, the user is asked to introduce his credentials in order to login into SAFEQ Cloud Client

Automatic refresh period – how often to perform automatic synchronization of the printers, in minutes. When set to 0 automatic refresh will be completely disabled.

Enable direct offline printing – only applies when SAFEQ Cloud Client is running in either Local or Hybrid storage modes.

If SAFEQ Cloud Client loses cloud or primary server connectivity for 10 consecutive minutes it will switch to offline mode. In offline mode SAFEQ Cloud Client will delete any mapped pull queues and instead map direct push print queues to the five most recently used pull printers by SAFEQ Cloud Client logged-in user. When cloud or primary server connection is re-established these offline queues are deleted and any pull queues restored.

Further information:

- SAFEQ Cloud Client must be running in either Local or Hybrid storage mode, this feature is not compatible with SAFEQ Cloud Client operating in Cloud or Gateway storage modes
- User's five recently used devices are cached by the client for three days. If a user has not printed for longer than three days prior to offline mode activation, no direct push queues will be mapped
- As queues are direct push queues, traffic routing from SAFEQ Cloud Client to the printer over standard printing protocols (TCP9100, IPP) is necessary
- If the user has any direct push queues mapped prior to entering offline mode, these queues are retained in offline mode

- All printing performed in offline mode is cached and accounted for following reconnection to the cloud or primary server

Service setup – Perform SAFEQ Cloud Client service configuration which requires administrator privileges. This includes: changing between local job storage mode and gateway mode and changing the SAFEQ Cloud server address and domain name in local job storage mode. When pressing this button the user will be prompted with an elevation request.

Options are taken from the system-wide configuration provided during installation. When modified they are stored per user, so it is possible to have multiple user accounts on one PC with different settings.

Note on OKTA and Microsoft Entra ID authentication when using the SAFEQ Cloud Client

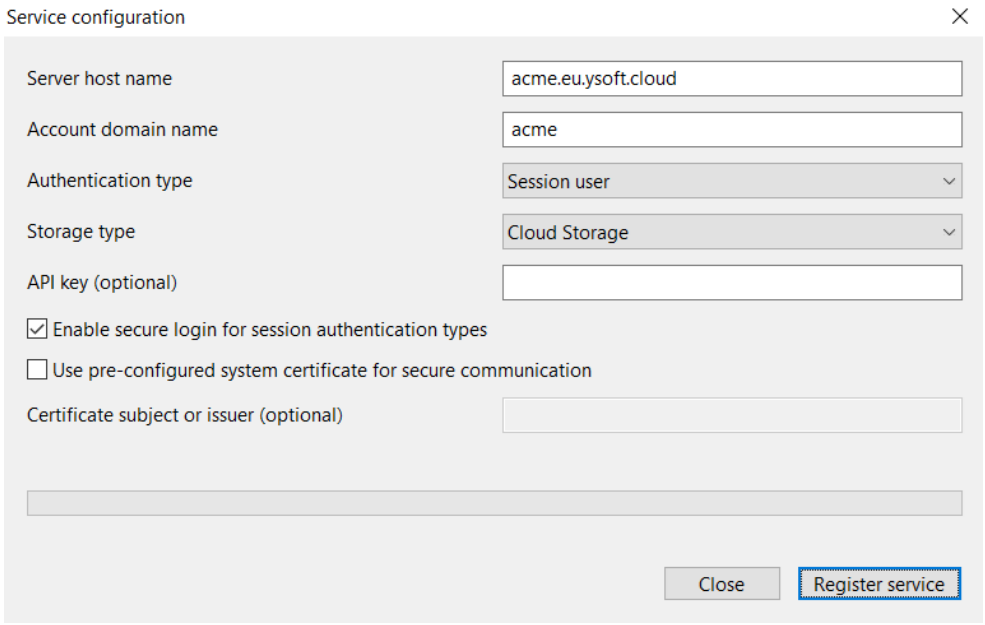
For both OKTA and Entra ID authentication providers the supported authentication types are currently "Session + domain name", "User Principal Name" or "Custom login".
When custom login is used the user name must be a fully qualified name with "@domain" part which should match the "Domain name" setting in the authentication provider.

Note on client-based authentication with MFA

It is possible to use MFA-enabled authentication against OpenID Connect-compliant identity providers. When this type of authentication is chosen in the configuration a browser window will be opened which will allow to perform online authentication. When authentication is successful the user ID token will be sent to SAFEQ Cloud server. SAFEQ Cloud server should have at least one authentication provider configured with the type `Client`. The user will then be registered on the server side with an expiration time set according to the token expiration policy configured in the authentication provider.
SAFEQ Cloud Client will attempt to refresh the token periodically and notify the server. When the refresh token expires the user will be logged out. A typical refresh token expiration time is 3 months and usually can be customized in the identity provider settings.

Service setup

Certain SAFEQ Cloud Client settings require service reconfiguration. This can only be done by PC administrator. Reconfiguration is possible either by reinstalling SAFEQ Cloud Client and choosing the relevant settings in the installation dialog or by entering the Service setup from the SAFEQ Cloud Client configuration screen.
Note that pressing this button will show a privilege elevation prompt.



Server host name – host name of SAFEQ Cloud primary server or gateway.

Account domain name – domain name of the account to which this SAFEQ Cloud Client will be connecting. If the account has multiple domains any of them can be specified in this field.

Authentication type – currently following authentication types are supported:

- Session user – username from the current OS session is used for authentication and job sending (default)
- Session user + domain – username@ad-domain from the current OS session is used for authentication and job sending. This matches server setting 'strict domain validation'.
- Session user principal name – UPN is used for authentication and job sending (whatever UPN configured in user profile, it can be the same as username@ad-domain for simple AD setups).
- Manual login to SAFEQ Cloud server – The user will be prompted to enter user name and password which will be validated in the SAFEQ Cloud server.
- Microsoft Azure login (deprecated) – Online authentication is performed against Microsoft Entra ID using OAuth2 workflow. This option is deprecated in favor of "OpenID Connect login".
- OpenID Connect login – Perform online authentication against OIDC-compliant identity provider by opening a browser window with OAuth2 workflow. This authentication type supports MFA and requires SAFEQ Cloud server to have at least one authentication provider defined with the type `Client`. If a single client-based authentication provider is defined for a given account the user will be redirected to that identity platform. If multiple client-based authentication providers are defined a generic OpenID connect window will be shown prompting the user to enter his or her username. Based on the domain part of the user name the browser will be redirected to the matching identity platform. The following identity platforms are currently supported: Microsoft Entra ID, Google GSuite, Ping Identity.

Storage type – select where SAFEQ Cloud Client stores the data: Cloud storage, Local storage, and Hybrid (direct print locally, secure print to cloud).

API key – API key used to communicate with SAFEQ Cloud server. If this option is not specified the default restricted key will be used. Note that the restricted key may be removed by the server administrator, in this case, a dedicated key must be specified.

Enable secure login for session authentication types – If this option is enabled SAFEQ Cloud Client will be registered as an endpoint and must be authorized by the administrator to use insecure login types (such as Session User or User Principal Name).

Use pre-configured system certificate for secure communication (Windows only) – this option will use the client certificate and key chain from the Windows certificate store when establishing a connection to SAFEQ Cloud server instead of the standard SAFEQ Cloud certificate.

This option is deprecated and will be removed in future versions.

Certificate subject or issuer – an optional field to specify a search pattern for the pre-configured certificate. Only relevant when the **Use pre-configured system certificates** option is also enabled. A certificate with a matching X.509 subject or issuer will be selected. It is possible to only specify a partial match here, for example, "acme" will select a certificate with "company.acme.com" in a subject or issuer line. If this option is left empty the first available certificate with a private key will be picked up.

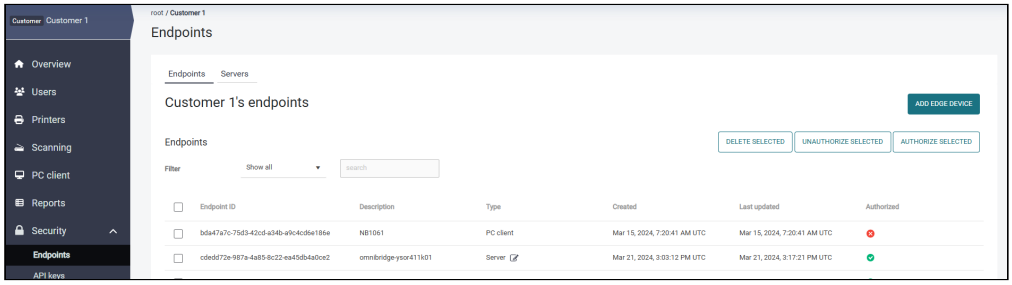
Pressing the **Register service** button will start the registration and configuration process which will be displayed as a progress bar.

Using pre-configured system certificates requires a PKI infrastructure in place and a dedicated SAFEQ Cloud server configuration as described in this section.

8.2.6 SAFEQ CLOUD CLIENT AUTHORIZATION

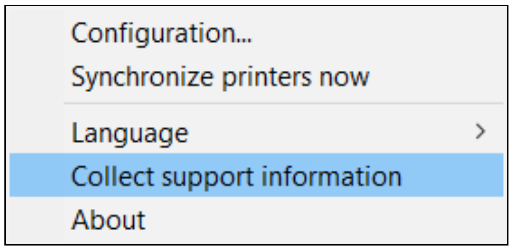
If the SAFEQ Cloud Client is installed in local storage mode and connects to the primary SAFEQ Cloud server, it is necessary to authorize it before the server can accept the connection, unless the account is configured to preauthorize all SAFEQ Cloud Clients in the account PKI configuration. Please refer to the SAFEQ Cloud user manual for details.

SAFEQ Cloud Client authorization is done from the **Security** section > **Endpoints** section:

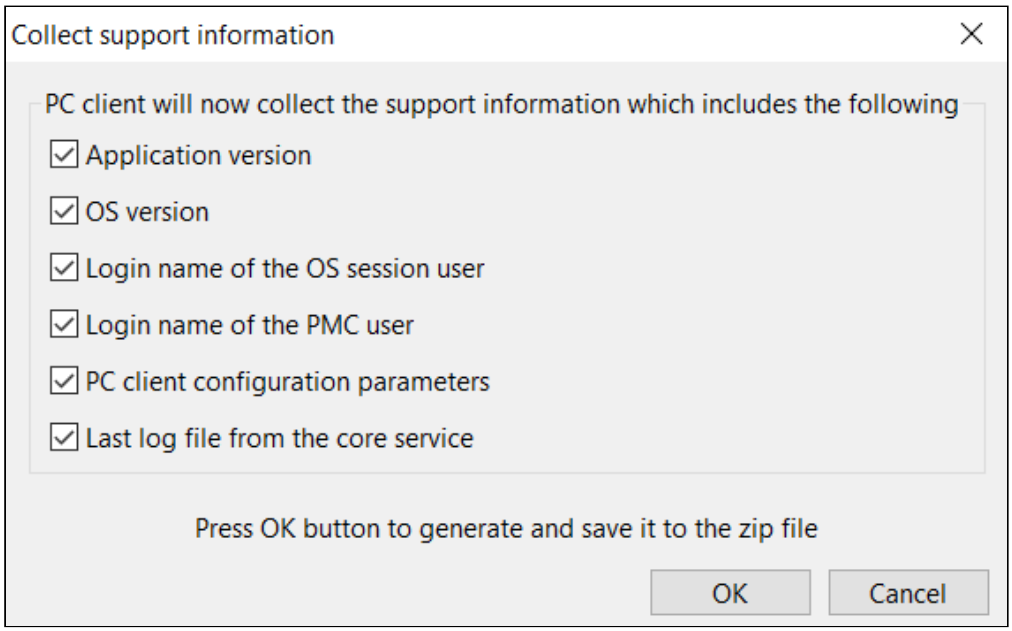


8.2.7 SAFEQ CLOUD CLIENT LOG DOWNLOAD

You can retrieve the current SAFEQ Cloud Client log & configuration from the SAFEQ Cloud Client application by selecting **Collect support information**:



This will display a pop-up from which you can select which information you wish to select:



Click **OK**. You will be prompted to select a location for the download. The download contains a zip archive with files for the selected options.

If the UI is unavailable (e.g. SAFEQ Cloud Client was not installed successfully), you can extract install logs for debugging here:

- Windows: `C:\ProgramData\safeqclientcore\install_logs`
- macOS: `/Library/safeqclientcore/install_logs`

In addition on the Windows operating system, some important events (e.g. updates, installation, security checks, etc.) are logged into the Windows Event log.

8.2.8 SAFEQ CLOUD CLIENT AUTO UPDATE

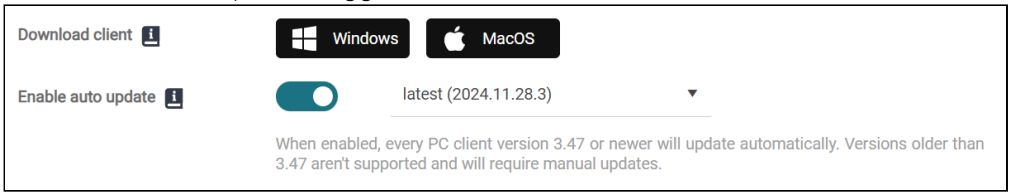
Prerequisites

- To use the auto update feature you must first manually update your existing Clients to version that supports auto update (3.47).
- The SAFEQ Cloud Client must be able to access `cdn.everyoneprint.com`.

Enabling the auto update

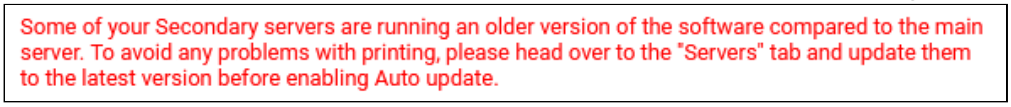
To enable SAFEQ Cloud Client auto update function, perform the following steps:

1. Log in to SAFEQ Cloud Web UI and go to **PC Client** > **Auto update**.
2. Enable the auto update toggle.



> When auto update is enabled, the Client will always try to update itself to version specified on this page. If you use other tools to keep your Clients updated to a specific version (GPO, SCCM, etc), we recommend you to keep the auto update function in SAFEQ Cloud Web UI disabled to avoid conflicts.

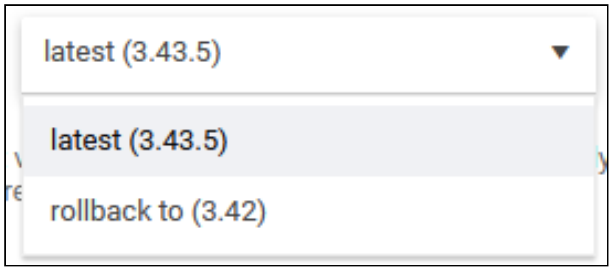
3. In order for Auto update to work properly, we recommend you to have all the secondary gateway servers on the same version as the Primary server. If that is not the case, you will see a warning when enabling auto update. This warning will not prevent you from enabling auto update, just be aware that inconsistencies in server versions might lead to issues.



4. Optionally, set the **Auto update delay** in case you don't want to update your Clients immediately after the new server version is rolled out.
5. Click **Save**.

Rollback

If you encounter issues with the latest Client version, you can use the version selection drop-down menu to roll back to the minor version that was previously installed.

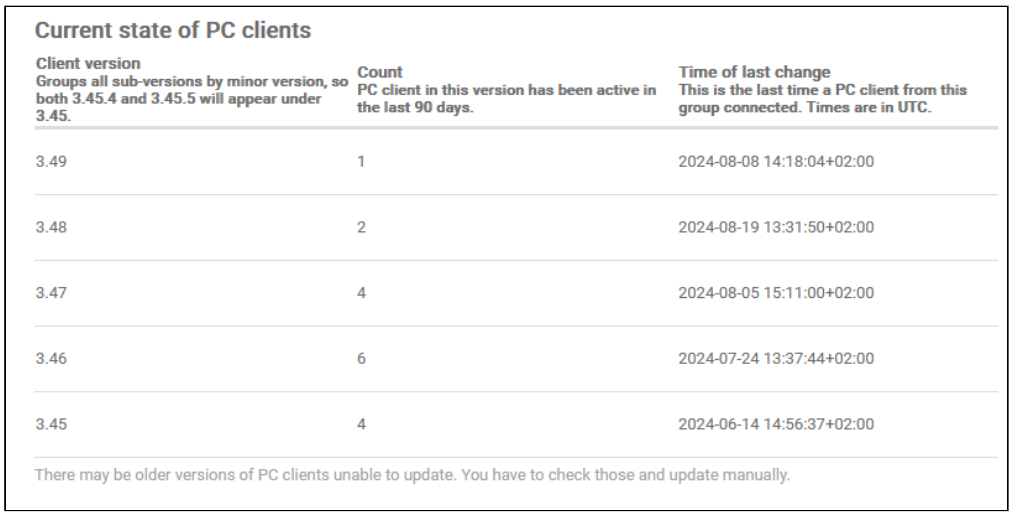


This will still function as if auto update was enabled – all applicable Clients with different versions will still try to update to the rollback version) but will prevent any further auto updates to later versions.

Overview of the current state of SAFEQ Cloud Clients

This section provides information on the number of Clients installed for particular versions and the last time any Client from this version group connected.

The table with versions may not contain all the older Client versions, as older Clients installed in cloud storage mode cannot report their versions.



Current state of PC clients

Client version Groups all sub-versions by minor version, so both 3.45.4 and 3.45.5 will appear under 3.45.	Count PC client in this version has been active in the last 90 days.	Time of last change This is the last time a PC client from this group connected. Times are in UTC.
3.49	1	2024-08-08 14:18:04+02:00
3.48	2	2024-08-19 13:31:50+02:00
3.47	4	2024-08-05 15:11:00+02:00
3.46	6	2024-07-24 13:37:44+02:00
3.45	4	2024-06-14 14:56:37+02:00

There may be older versions of PC clients unable to update. You have to check those and update manually.

Failed updates

If there are any failed client updates, this view will show you how many clients failed to update. You can also generate a CSV report with causes of those failures.

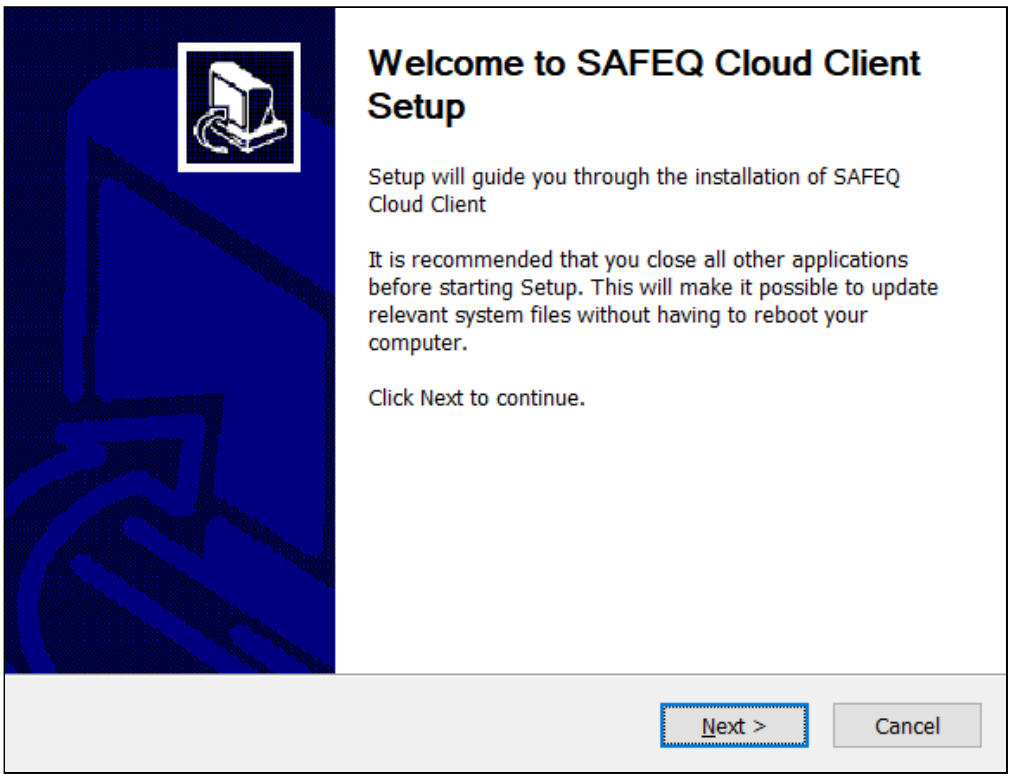
8.2.9 SAFEQ CLOUD CLIENT UPGRADE

Upgrading SAFEQ Cloud Client on Windows

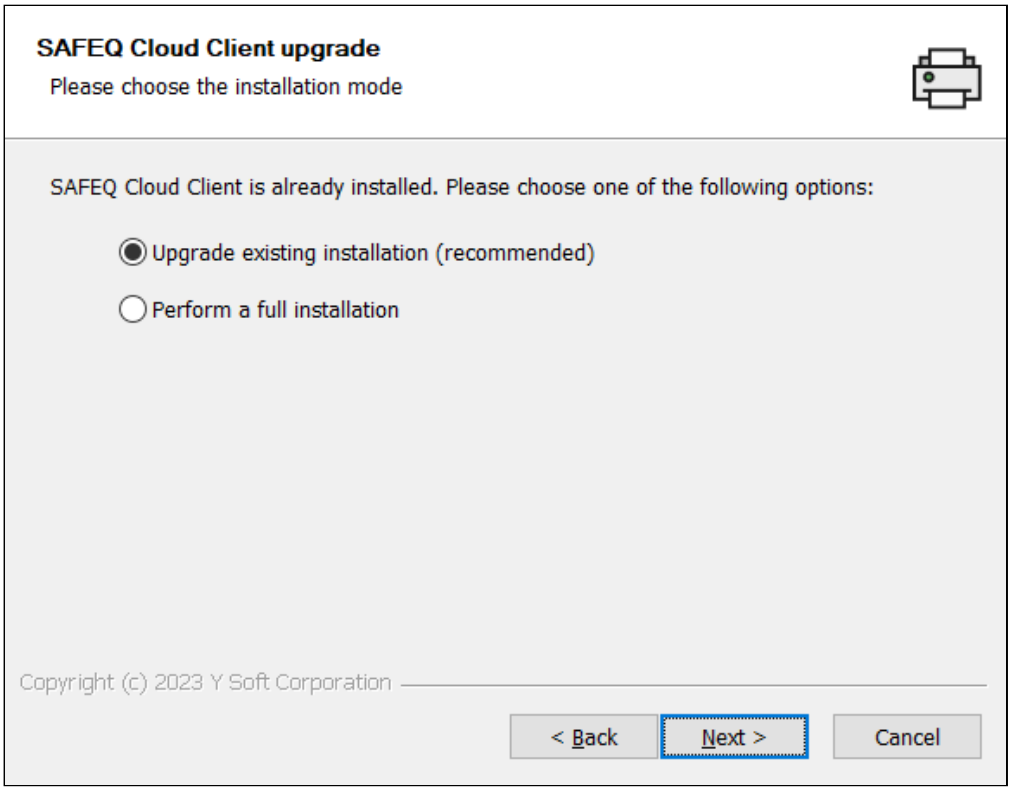
Manual upgrade process

Follow these steps to upgrade the existing installation of SAFEQ Cloud Client in the Windows environment:

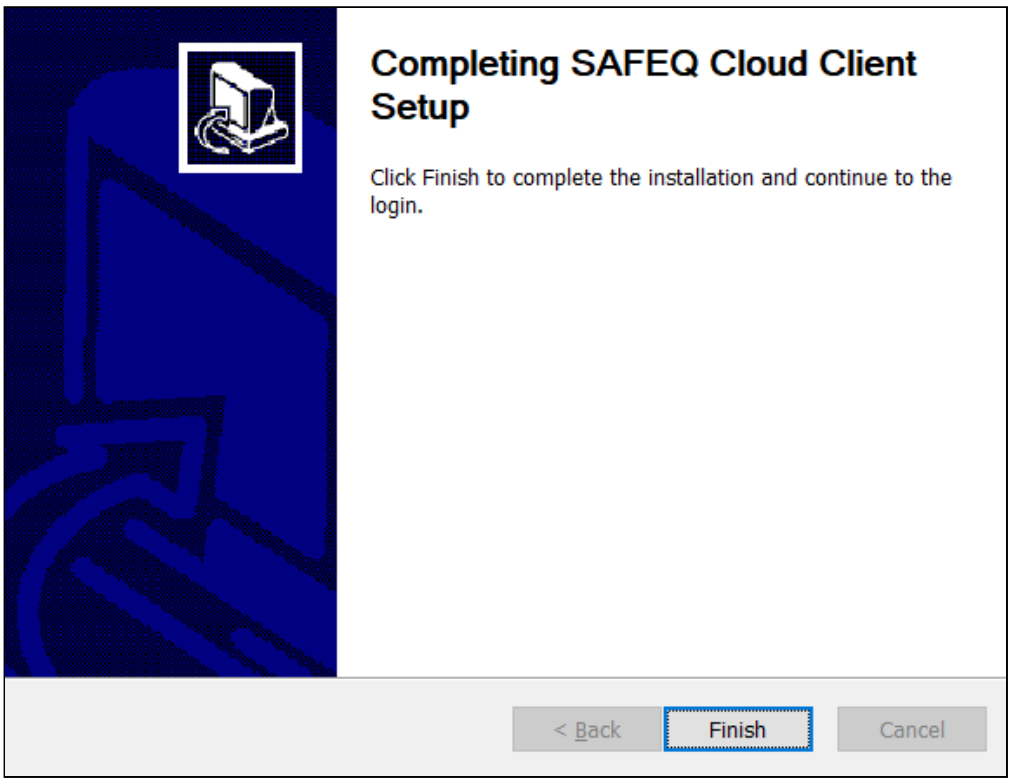
1. Run the SAFEQ Cloud Client executable file.
2. Click **Next**.



3. Select the **Upgrade existing installation (recommended)** option and then click **Next**.



4. Wait while the SAFEQ Cloud Client is being updated and then click **Finish**.



Upgrade via Windows command line

This is similar to the unattended installation. Open a Command Prompt and go to the location of the SAFEQ Cloud Client installer. Run the following command:

```
safeq-cloud-client-3.x.y-release-setup.exe /S /GATEWAYADDRESS=<IP or DNS> /ACCOUNTDOMAIN=<accountDomainName>
```

Windows installer also accepts several command-line parameters for unattended installation that can be found in section Installing SAFEQ Cloud client on Windows.

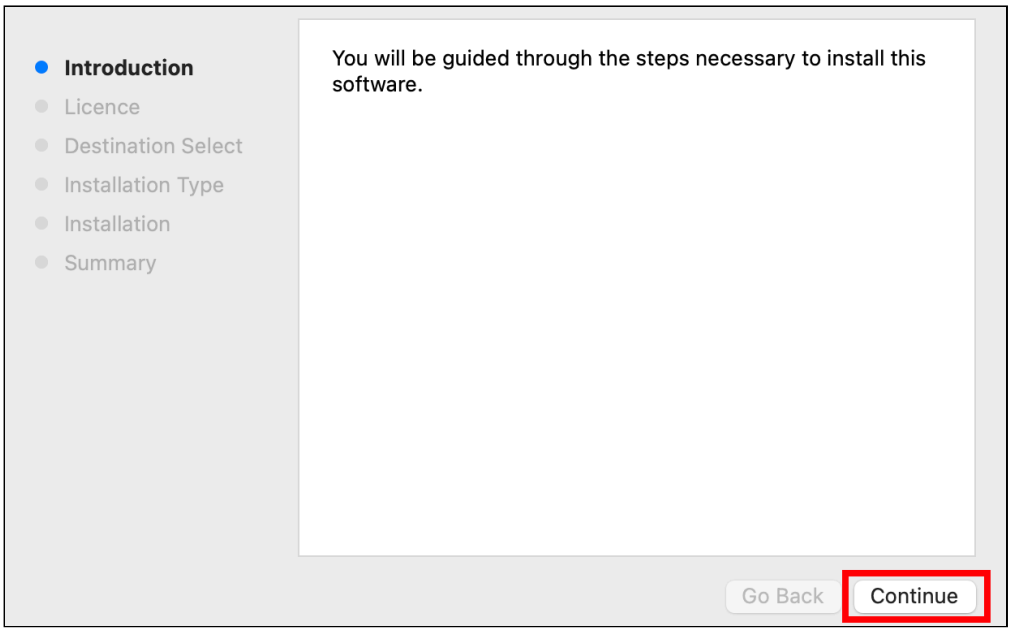
Upgrading SAFEQ Cloud Client on macOS

Manual upgrade process

Follow these steps to upgrade the existing installation of SAFEQ Cloud Client in the macOS environment:

1. Run the SAFEQ Cloud Client .pkg file.

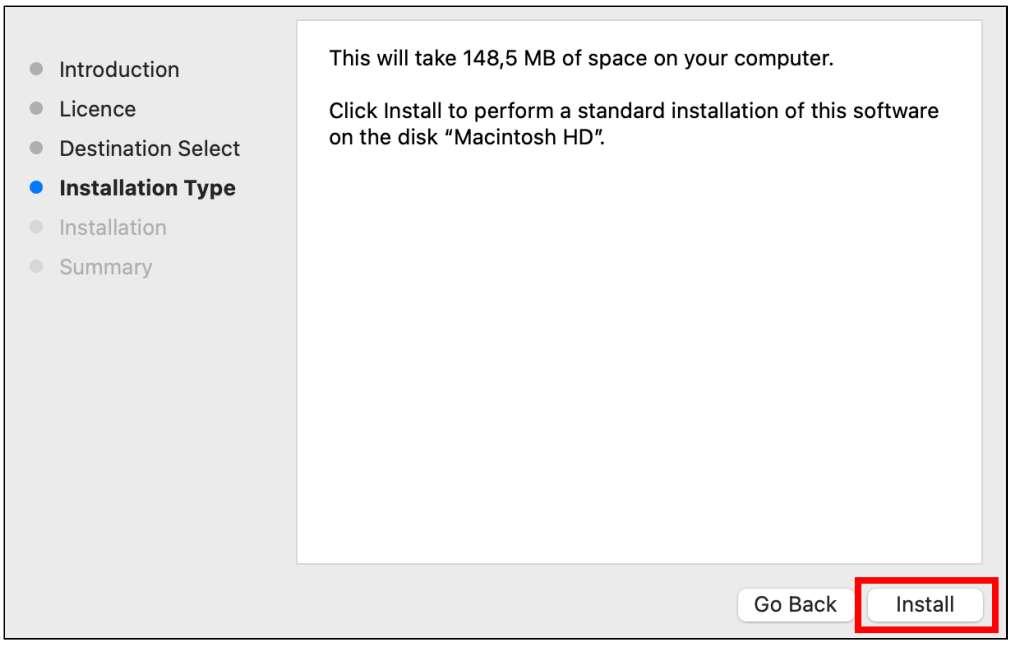
2. Click **Continue**.



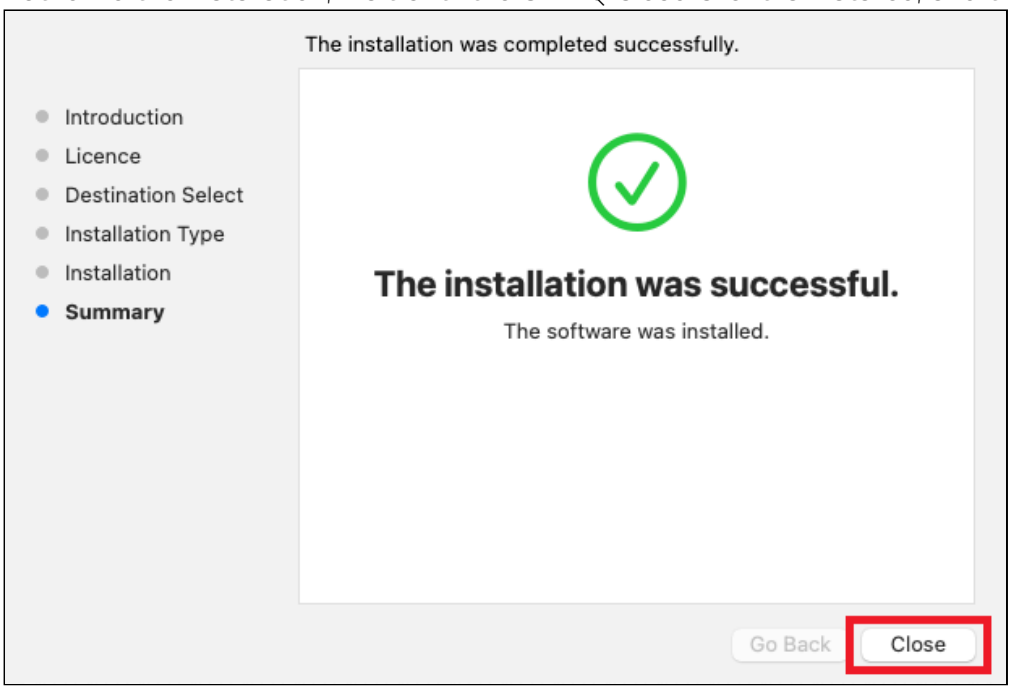
3. On the next screen, read the license agreement and click **Continue**. A pop-up screen will appear.

4. On the pop-up screen, click **Agree**.

5. Click **Install** and then click **OK**.



6. Authorize the installation, wait until the SAFEQ Cloud Client is installed, and then click **Close**.



Unattended upgrade process on macOS

The same steps outlined in section Installing SAFEQ Cloud client on macOS can be followed for upgrading.

Post-upgrade checks

- The SAFEQ Cloud Client icon is displayed normally in the System Tray area.
- The upgraded app version is correct in the **About** window.
- The previously set configuration options are unchanged in the **Configuration...** window.

8.2.10 SAFEQ CLOUD CLIENT TROUBLESHOOTING

SAFEQ Cloud Client cannot connect to a server

Problem description

- When you right-click the client icon in the system tray, select **Login**, enter your credentials, and click **OK**, the client displays the error message "Cannot connect to server!".
- When you right-click the client icon in the system tray, select Configure, fill in the **host name** and **domain name**, and click **Test**, the client displays the error message "Cannot connect to server!".

Troubleshooting

1. Make sure that the Server address/host name information is correct.

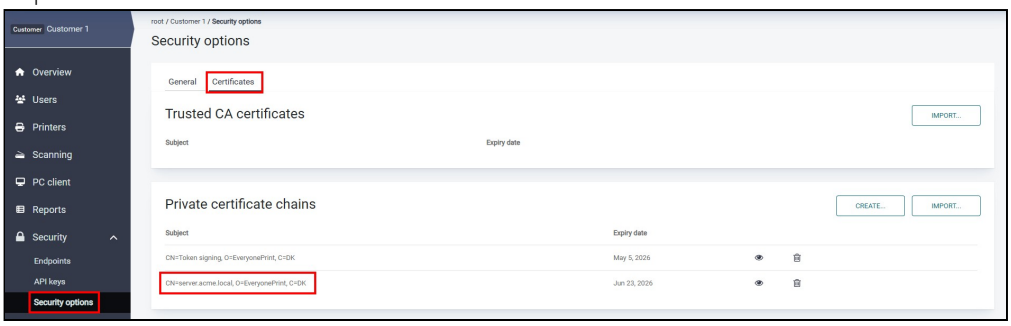
> ⚠ You must use the domain name. The IP address will not work.

2. Check whether you see the same issue in the Client's `safeqclinetcore` log file:
`[ERROR] YYYY-MM-DD HH:MM:SS.sss {xxxx } SAFEQ Cloudapi::connector - error sending request for url (https://server.acme.local:7300/api/v1/account?domainname=acme.local): error trying to connect: The certificate's CN name does not match the passed value.`

3. If you can see the above error log, a likely cause of the problem is a missing private certificate chain in the SAFEQ Cloud Web UI.

4. Log in to the SAFEQ Cloud Web UI. Go to **Security** > **Security Options** and select tab **Certificates**.

5. Verify that for the server your SAFEQ Cloud Client is connecting to, a private certificate chain is present.



6. If not, create a new one by clicking **Create**, selecting the server host name and then clicking **Generate**.

7. Wait 1 - 2 minutes for the certificate to propagate to your SAFEQ Cloud Client.

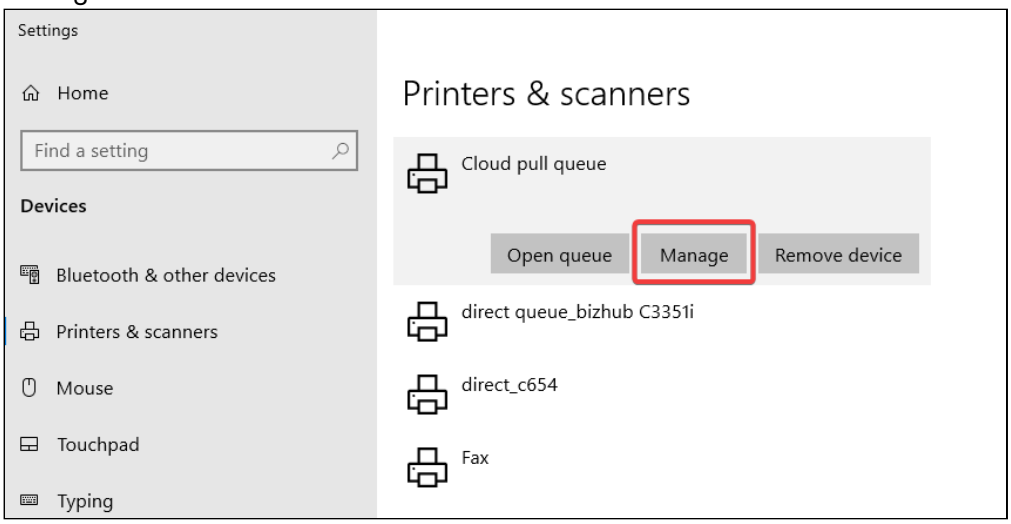
8.2.11 UNIVERSAL DRIVER SETTINGS

When using the Universal driver provided by SAFEQ Cloud Client, you can change the default settings of how the documents will be sent to the printer.

Windows

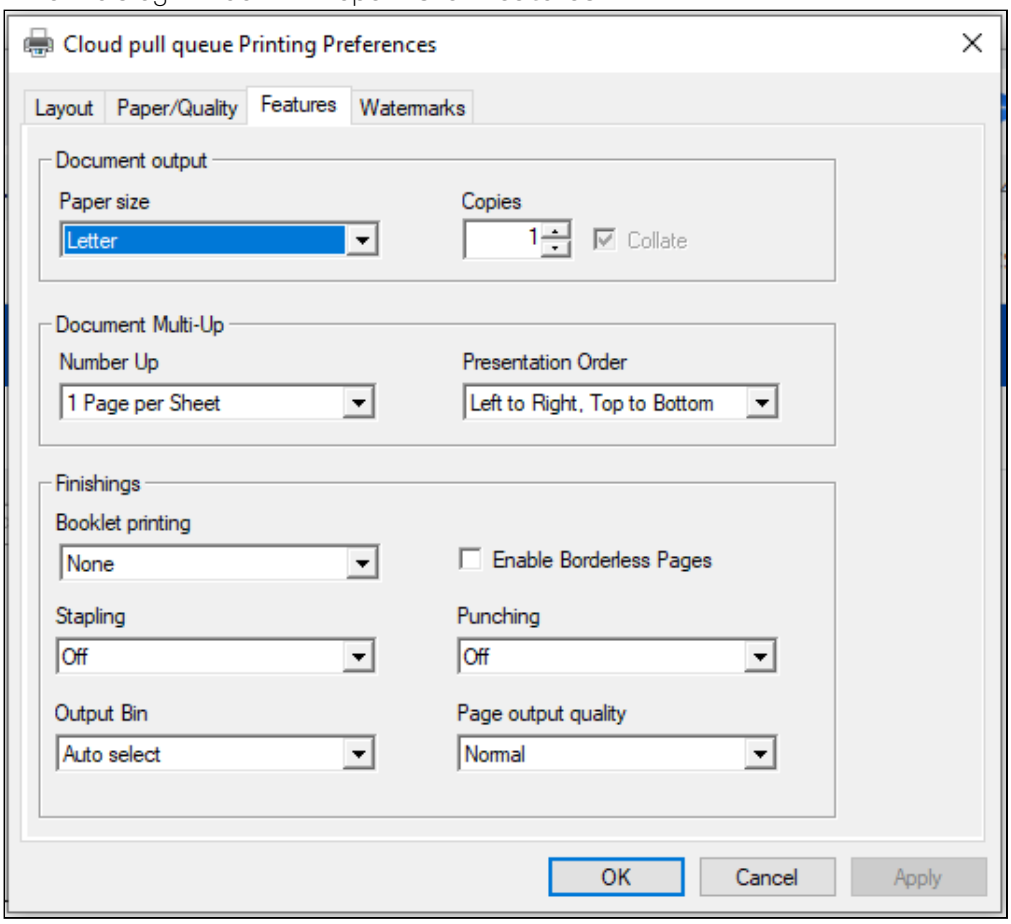
1. Go to **Printers & scanners**.

2. Click one of the printers (print queues) created by the SAFEQ Cloud client and then click **Manage**.



3. Click **Printing preferences**.

4. A new dialog window will open. Click **Features**.



5. Change the following properties according to your needs:
   - **Number up** – Set the number of document pages per printed page
   - **Presentation Order** – Set how the multiple pages will be sorted on the printed page
   - **Booklet printing**

- Stapling – Add staples to the printed document (if available)
- Output bin
- Enable borderless pages – By default, the Universal Print driver scales the document page to 96%. Enabling borderless pages disables scaling and allows you to configure your own borders when printing the document.
- Punching
- Page output quality

6. Click OK.

8.2.12 SAFEQ CLOUD CLIENT PROXY SUPPORT

SAFEQ Cloud Client supports the following proxy configurations taken from the operating system settings:

- Plain proxies without authentication
- Proxies with Kerberos authentication. The authentication token is acquired automatically from the user session.

Which system proxy configurations are supported depends on the target platform and may change in the future. Note that in order for the local storage or hybrid mode to work correctly via proxy, the proxy service must allow idle TCP connections for extended periods of time, so that the persistent connection to SAFEQ Cloud is not terminated.

Windows

The following system proxy configurations are supported:

- Manual configuration with address and port.
- Automatic configuration with auto-discovery URL (PAC).

Windows provides per-user proxy settings. In multi-user environments like Terminal Services or Citrix, proxy settings or authentication token of any logged-in user may be used for communication.

MacOS

Only Manual proxy configuration for HTTPS proxy access is supported.

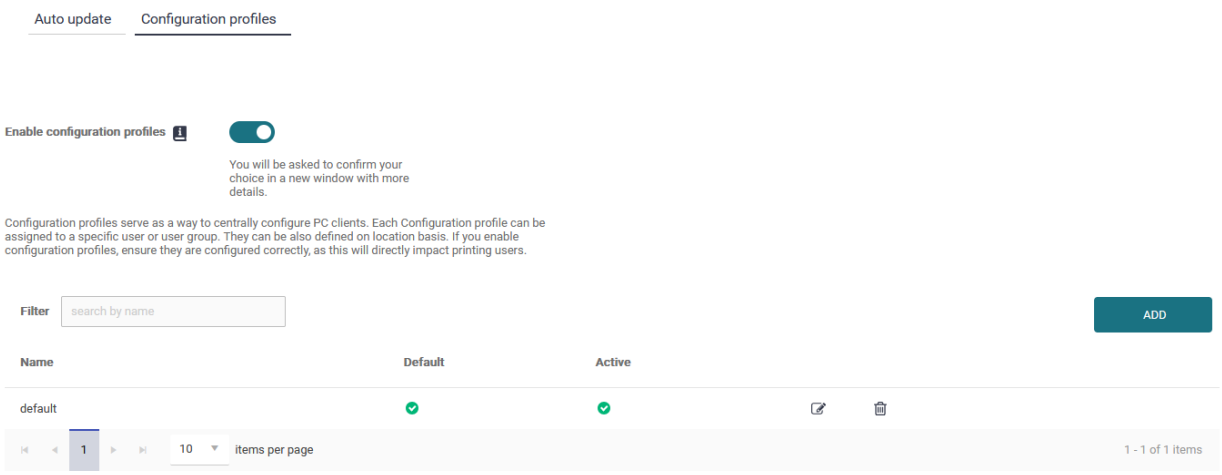
HTTP proxy settings are deprecated.

8.2.13 SAFEQ CLOUD CLIENT CONFIGURATION PROFILES

Configuration profiles section contains list of profiles used for remote configuration of SAFEQ Cloud Client. It can be found in PC Client → Configuration profiles

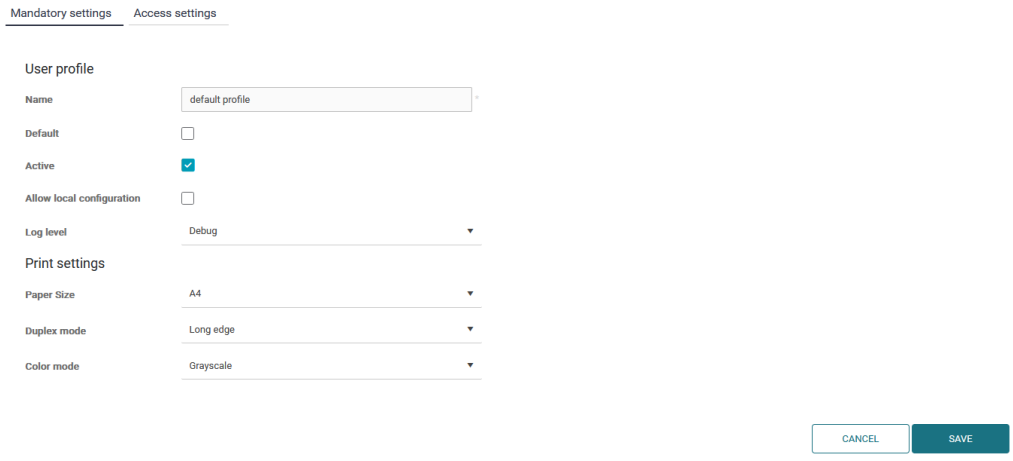
Default profile will be created automatically for each new customer. Existing customers will not have any configuration profiles created for them and if they wish to use this feature, they need to create the profiles manually.

On the initial screen you can see a list of current profiles and whether the profile is active and marked as default. You can also edit/delete profiles and enable/disable configuration profiles altogether. Enabling/Disabling configuration profiles requires confirmation in the form of a pop-up window.



After clicking on **"Add"** or editing an existing profile. You are taken to the profile page. There are two tabs:

Mandatory Settings:



where you set up basic configuration options:

Name: Profile name

Default: Whether the profile is set as default (only one profile can be default at a time)

Active: Whether the profile is going to be used when applicable (Setting a profile as default will automatically make it active)

Allow local configuration: Enables or disables capability of SAFEQ Cloud Client being locally configured through their context menu.

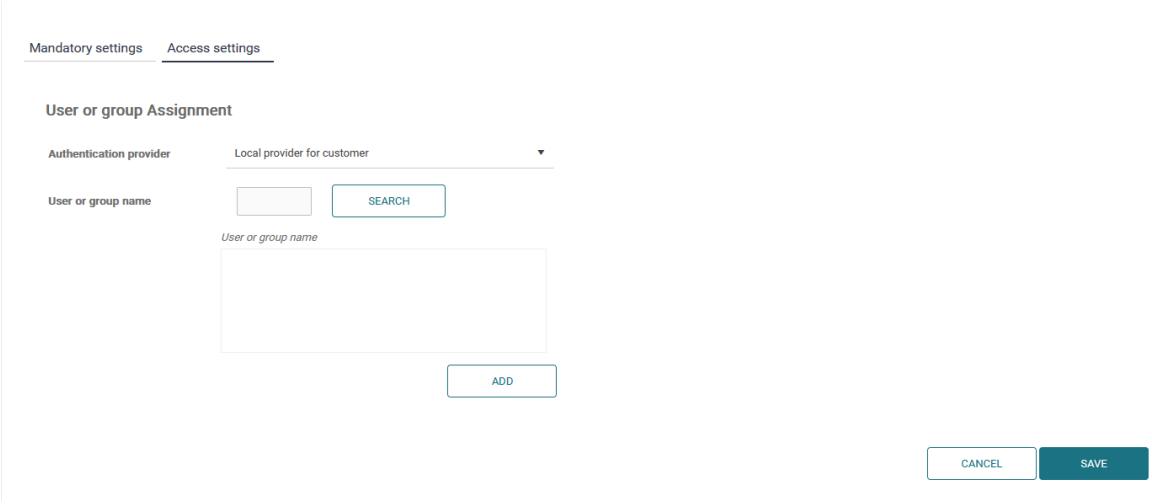
Log level: Sets logging level for SAFEQ Cloud Client

Color mode: Toggle between Color and B/W

Duplex mode: Simplex/Duplex selection

Paper size: Paper size selection

and
Access settings:

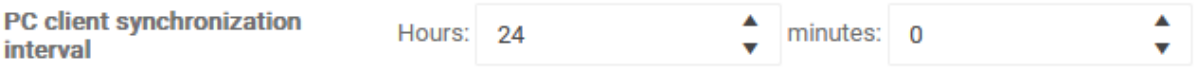


Where you can assign the filter to particular user(s) or user group(s).

Profiles will always be applied in following order:
Profiles assigned to specific user. If those do not exist then profiles assigned to a group user is in. And lastly if no profile is found for either user or group default profile will be applied.

> Only the highest possible hierarchy is considered when applying profiles. (E.G. If there is a profile assigned directly to a specific user, profiles assigned for his/her group will not be considered)

There is also an option for setting up client synchronization interval in which SAFEQ Cloud Client will synchronize printers and user profiles. This can however be only done on vendor level as setting up this interval incorrectly can affect performance. You can find this setting in: **Settings → Vendor account → Advanced options** menu section.



Merging profiles:

If a user is assigned two or more profiles SAFEQ Cloud Client resolves potential conflict by profile merging in the following way:

- Log level: The highest level in order (from lowest to highest): Off, Error, Warn, Info, Debug, Trace
- Color mode: If at least one assigned profile is color then color, otherwise B/W
- Duplex: The highest priority in order (from lowest to highest): Long edge, Short edge, Simplex
- Paper size: The highest priority in order (from lowest to highest): Letter, A3, A4, A5

8.2.14 WINDOWS PROTECTED PRINT MODE

About

Windows Protected Print Mode provides additional print security benefits by leveraging Windows modern print stack that solely relies on Internet Printing Protocol (IPP) and Microsoft IPP Class Print Driver.

Enabling Windows Protected Print Mode

Please follow official Microsoft documentation.

- Enable Windows Protected Print mode for individual PC
- Enable Windows Protected Print mode as group policy

Enabling of Windows Protected Print mode deletes already installed queues.

SAFEQ Cloud Client installation and deployment

You don't need to do any additional setup. Once the Windows Protected print mode is enabled, SAFEQ Cloud Client will recreate print queues on the next printer synchronization which is triggered:

- Every time the SAFEQ Cloud Client service is started.
- Periodically in set intervals (default is one hour).
- Manually by the user via tray menu "Synchronize printers".

Enabling Windows protected Print mode on a PC with already installed SAFEQ Cloud Client is supported as well as installation of SAFEQ Cloud Client to PC with enabled Windows Protected Print mode.

Enablement of Windows Protected Print mode in organizations

It is recommended to enable Windows Protected Print mode first for several individuals or small group of people via group policy and check compatibility with your printers. Older printers don't have to be compatible with PDF generated by Microsoft IPP Class Print Driver and may require document conversion.

Mopria certified printers are supposed to work without any issues or document conversions.

The output type of the Microsoft IPP Class driver is PDF. Therefore, it is pre-requisite that all the printers support the PDF generated by the Microsoft IPP Class driver.

Supported Finishing Options

The SAFEQ Cloud Client supports the following finishing options:

- Color modes
  - Color
  - Monochrome
- Duplex modes
  - Simplex
  - Duplex - flip on long edge
  - Duplex - flip on short edge
- Number of copies
  - Collated copies
  - Uncollated copies
- Various paper sizes
  - Particular paper size must also be supported by the printer where the job is released.
- Page range
- Input tray
- Output bin
- Stapling
- Punching
- Upload File Size Limitation

The following table compares the available finishing options when using the SAFEQ Cloud Client with WPP, the Universal driver or printing with a vendor driver via IPP:

Finishing Option	WPP	Universal Print Driver	IPP with vendor driver
Color modes	✔	✔	✔
Duplex modes	✔	✔	✔
Number of copies	✔	✔	✔
Page sizes	✔	✔	?
Page range	✔	✔	✔

Finishing Option	WPP	Universal Print Driver	IPP with vendor driver
Input tray	✓	✓	?
Output bin	✓	✓	?
Stapling	✓	✓	?
Punching	✓	✓	?
Watermark	✗	✓	?
Booklet	✗	✓	?
Media type	✗	✓	?
Upload File Size Limitation	1 GB (max)	1 GB (max)	1 GB (max)

? The availability of these finishing options depends on the capabilities of each vendor driver. They are not recorded by our server, may not be editable on the terminal, and will only function with the vendor's printers.

Links to Additional Information

For additional information about specific cloud terminals and their limitations see:

- Ricoh Standard Gen 2 Cloud Terminal - Requirements and limitations
- FUJIFILM BI Terminal
- HP Workpath Gen 2 Cloud Terminal
- Konica Minolta IWS Gen 2 Cloud Terminal

8.2.15 INSTALLING SAFEQ CLOUD CLIENT ON WINDOWS

SAFEQ Cloud Client installer can be downloaded from SAFEQ Cloud Web UI.

SAFEQ Cloud Client can be installed in two ways:

- Quick installation – preconfigured installation without advanced options
- Advanced installation – advanced options are enabled during the installation

SAFEQ Cloud Client can be installed by any type of user defined on the Windows machine. After installation of SAFEQ Cloud Client, it should be visible in Apps and features for all the users. If another user was logged in during SAFEQ Cloud Client installation, the icon corresponding to SAFEQ Cloud Client will appear only after a re-login.

For general requirements and prerequisites, see System requirements.

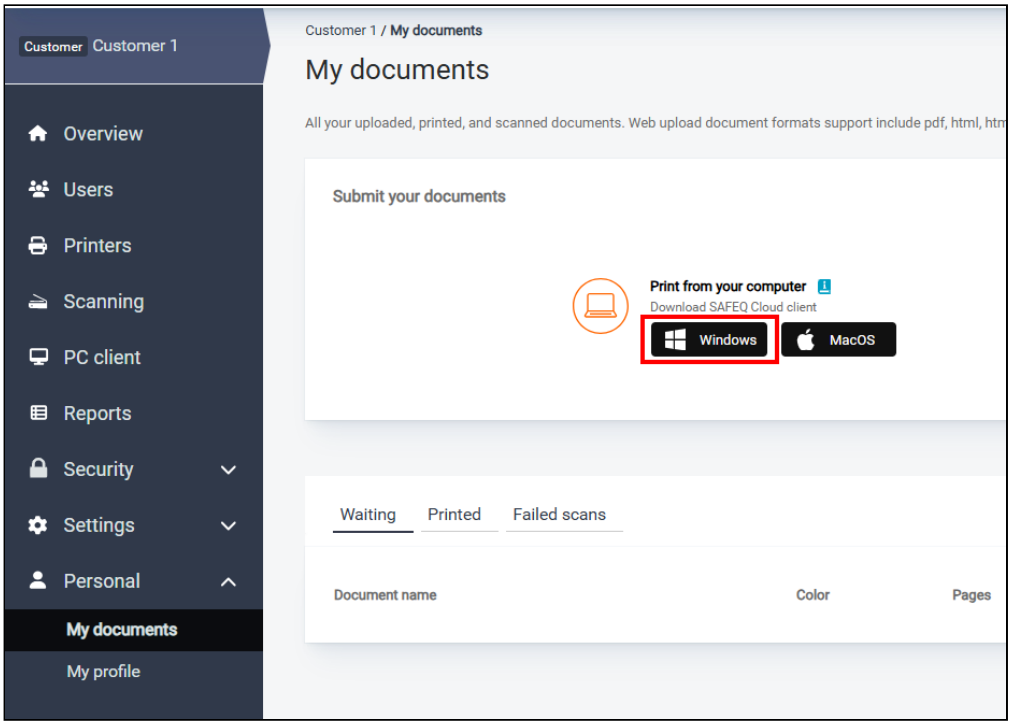
Quick installation

Limitations

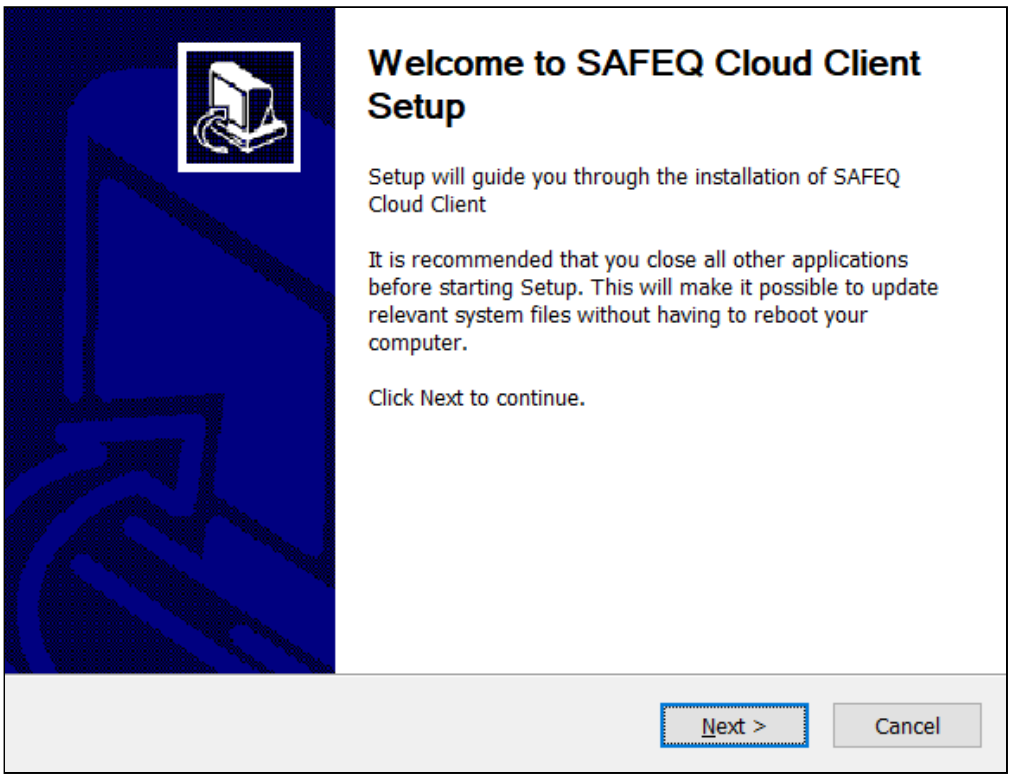
- The client can not be installed in local storage mode.
- The Client can only be installed in the default folder.
- Ghostscript will not be installed.
- The Client is installed with the SAFEQ Cloud OAuth2 login authentication type.
- Once the Client is installed, the Configuration option is removed from the menu.

Do the following to install SAFEQ Cloud Client using the quick installation type:

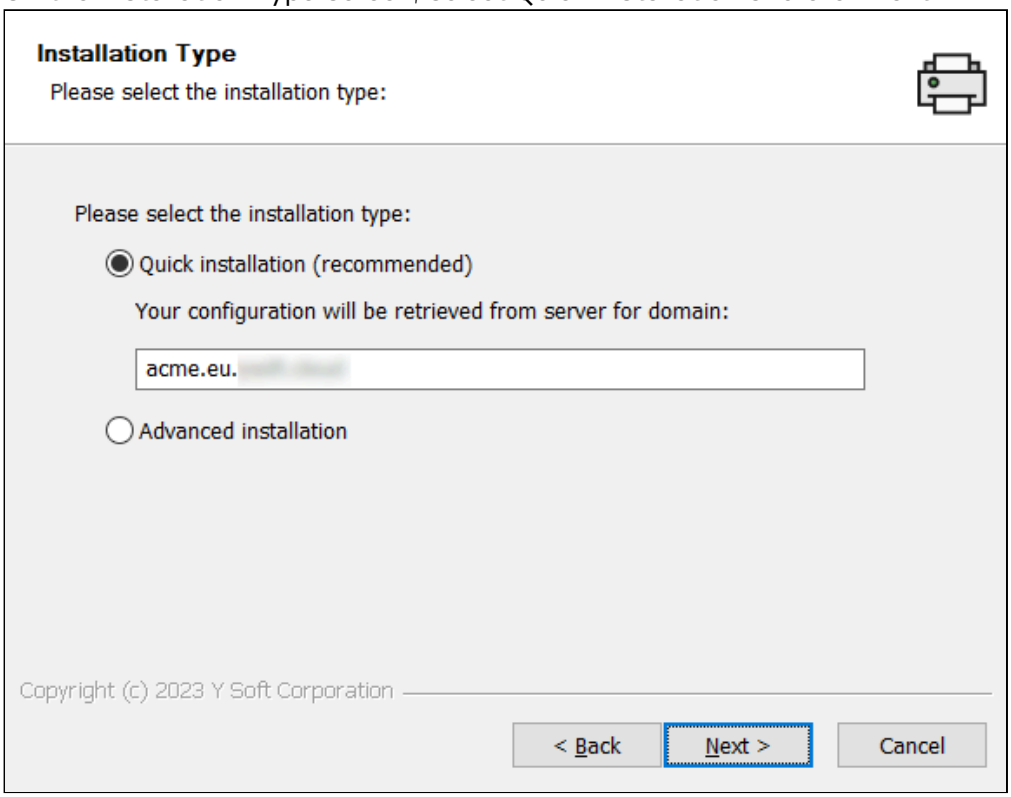
1. Log in to your Web UI, navigate to **Personal > My documents**, and select **Windows**.



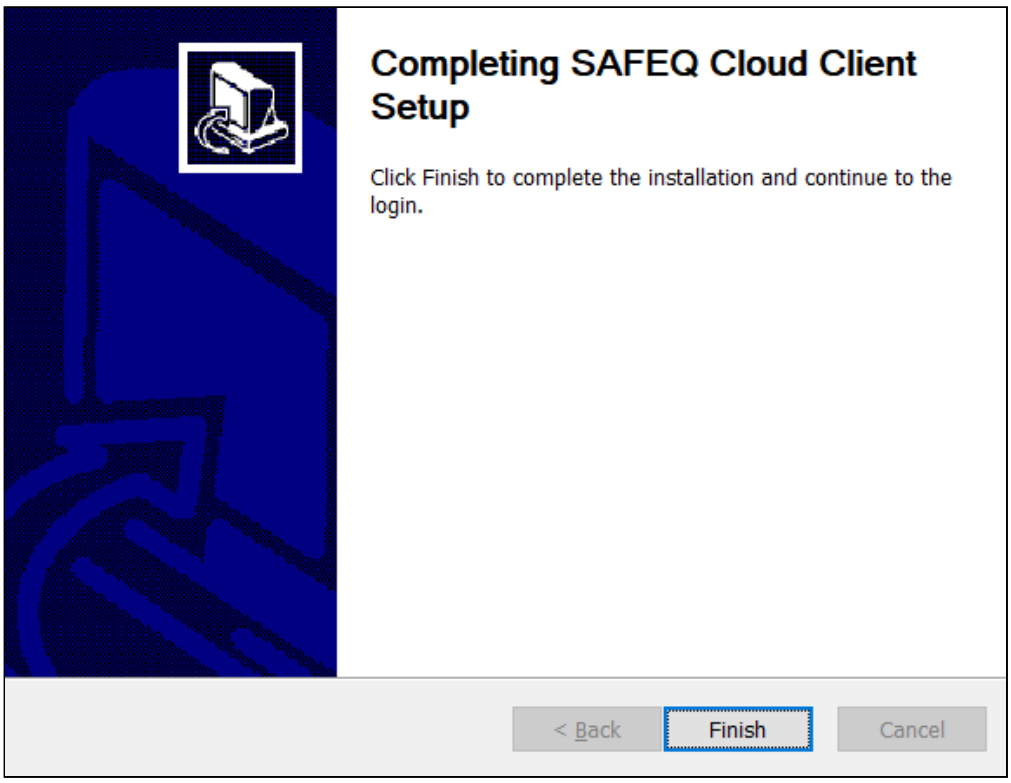
2. Run the downloaded installation file.
3. On the welcome screen, click **Next**.



4. On the next screen, read the license agreement and consent by clicking I Agree.
5. On the Installation Type screen, select Quick installation and click Next.



6. Wait until the SAFEQ Cloud Client is installed, and then click Finish.

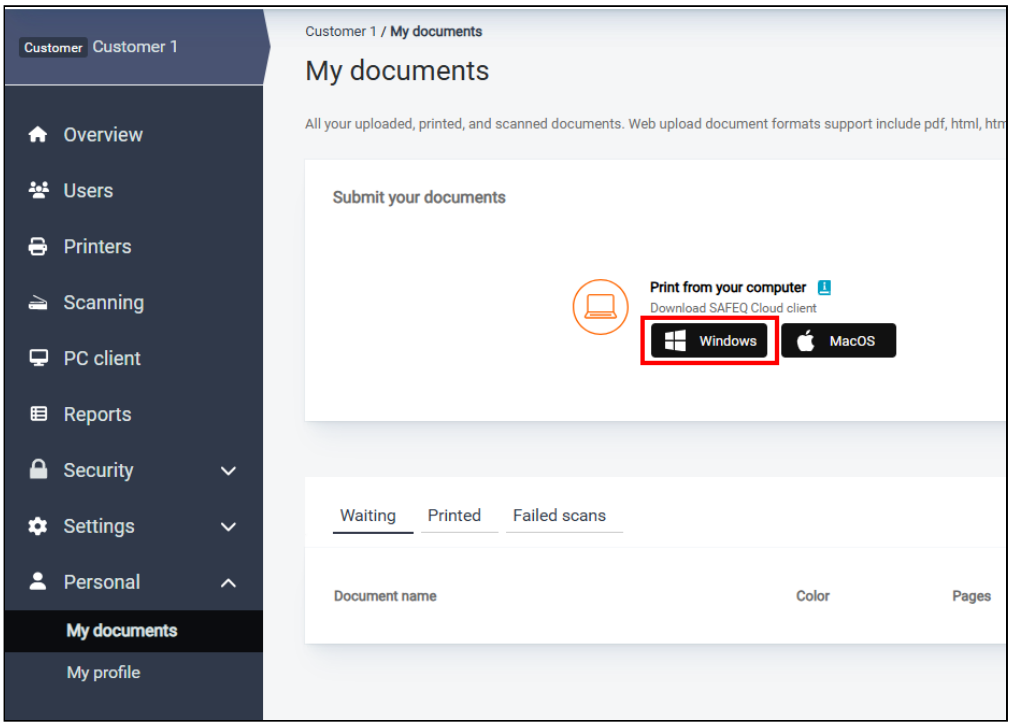


7. Log in on the login screen opened in your web browser.
8. The application starts automatically.

Advanced installation

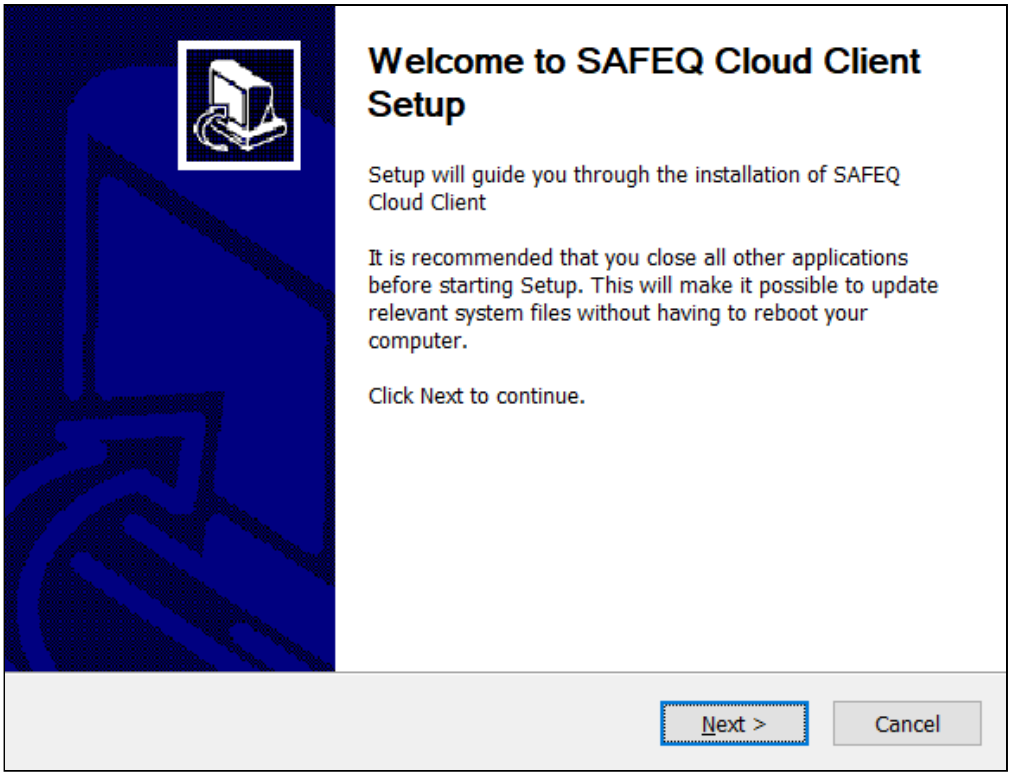
Do the following to install SAFEQ Cloud Client using the advanced installation type:

1. Log in to your Web UI, navigate to **Personal > My documents**, and select **Windows**.



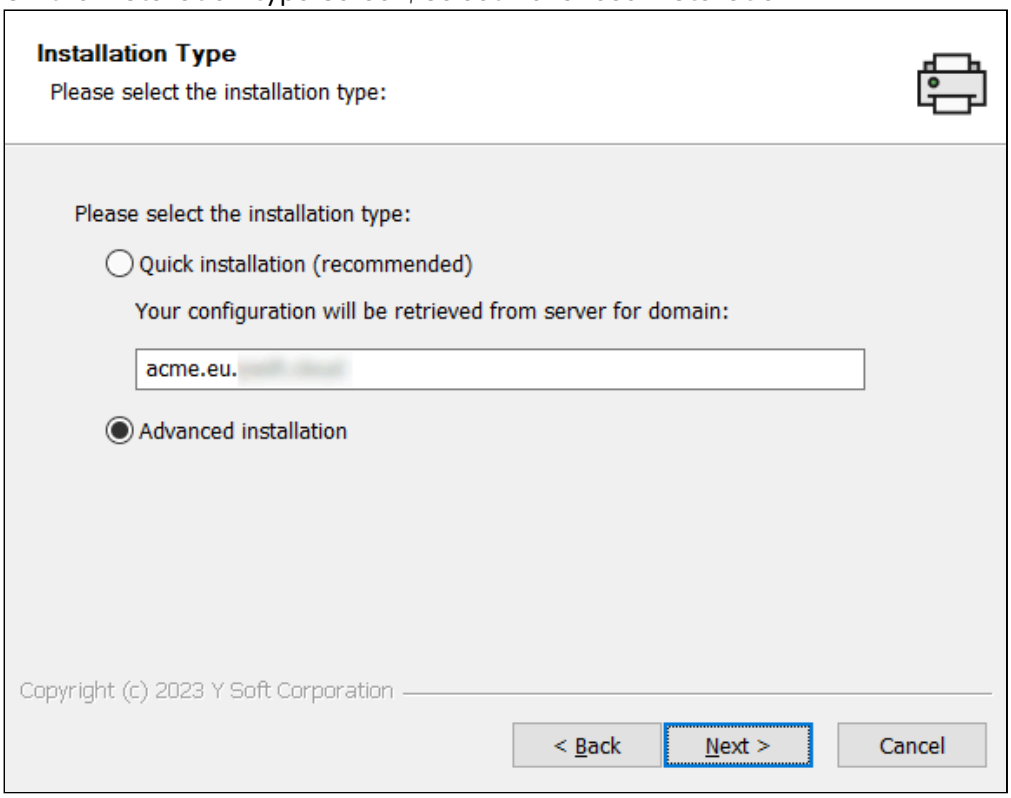
2. Run the downloaded installation file.

3. On the welcome screen, click **Next**.

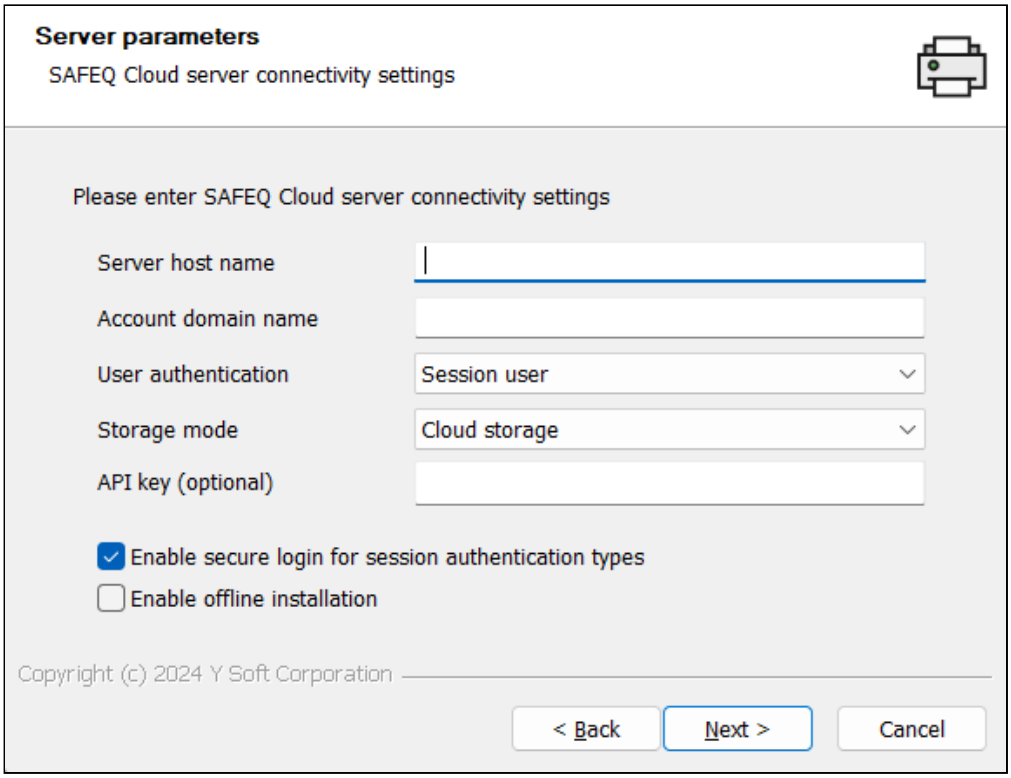


4. On the next screen, read the license agreement and consent by clicking **I Agree**.

5. On the Installation type screen, select Advanced installation.



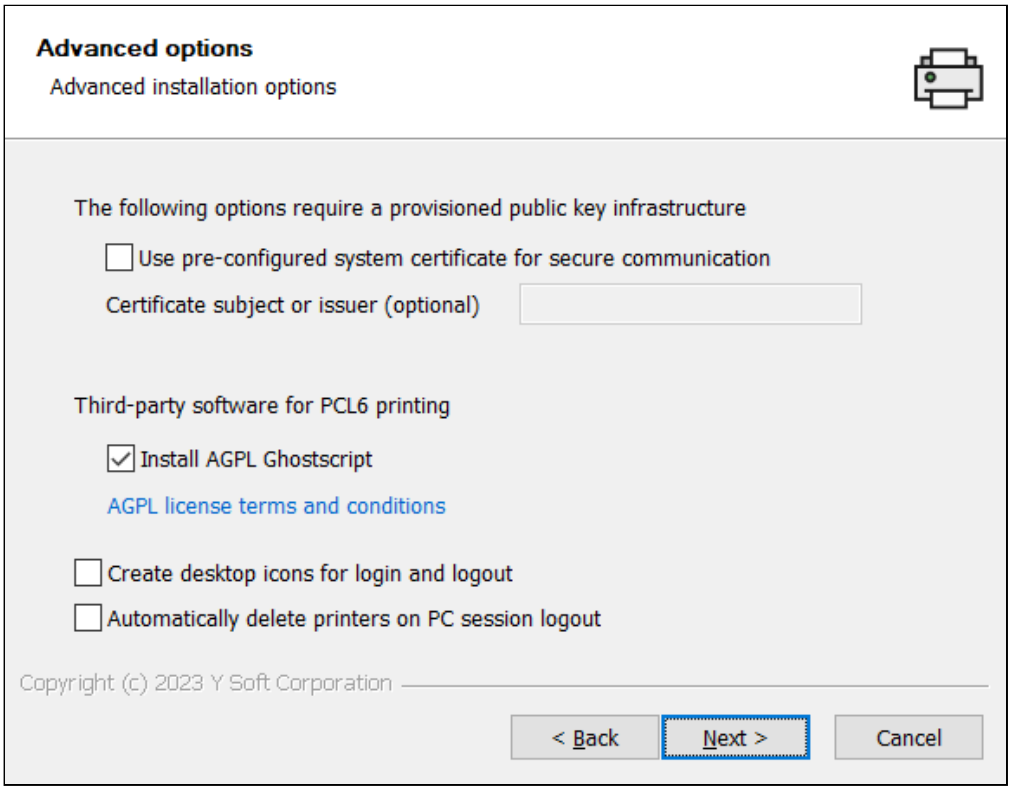
6. Fill in the server connectivity parameters.



- Server host name – address or host name of the SAFEQ Cloud server to connect to. For "Local storage mode" the address should be the account DNS of the SAFEQ Cloud primary server, usually the same as Account domain name.

- Account domain name – domain name of the target account. It can be found in SAFEQ Cloud Web UI on the Customer information tab.
- User authentication – select user authentication type.
- Storage mode – select where SAFEQ Cloud Client stores the data: Cloud storage, Local storage, and Hybrid (direct print locally, secure print to cloud).
- API key – API key from the account settings. If omitted the default (restricted) API key will be used. Default API key will be removed in the future product versions.
- Enable secure login for session authentication types – enable SAFEQ Cloud Client registration as an endpoint which must be authorized by the administrator to use insecure login types (such as Session User or User Principal Name).
- Enable offline installation – install SAFEQ Cloud Client without registering or checking server connectivity. Please see this section for details.

7. Modify the advanced options

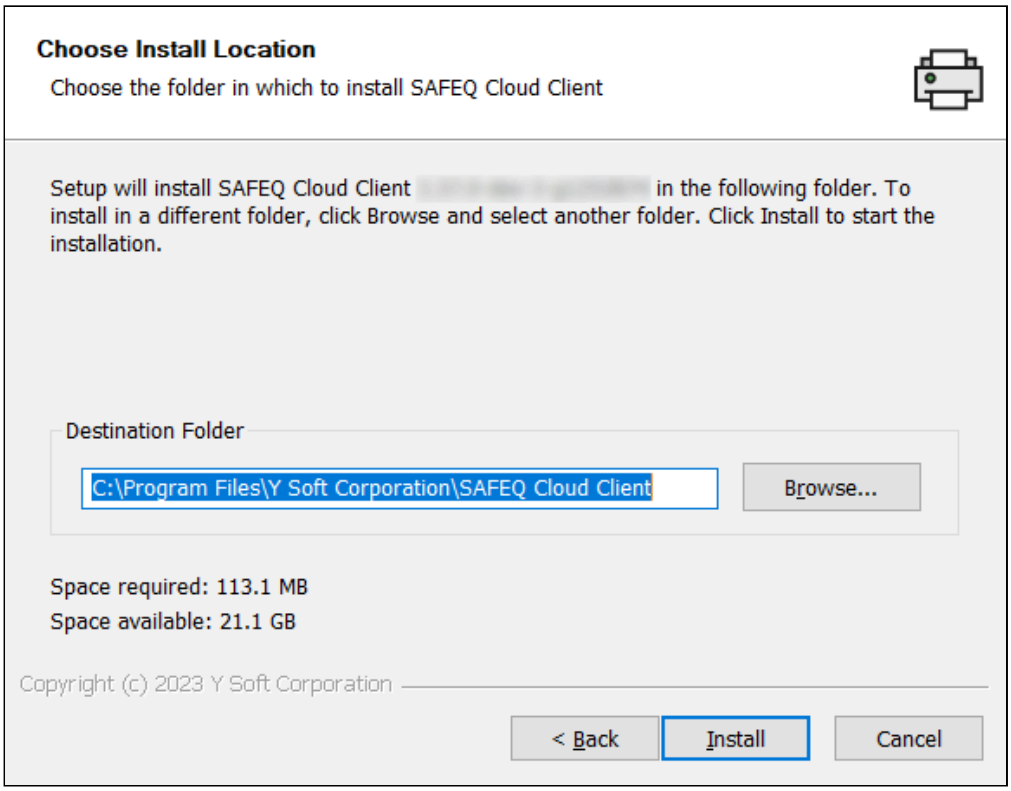


- Use pre-configured system certificate for secure communication – for TLS connectivity use the default certificate from the PC certificate store. NOTE: This option requires a managed public key infrastructure environment or a manually configured private key chain in the certificate store.
- Certificate subject or issuer – search pattern to choose for a client certificate from the Windows certificate store.
- Install AGPL Ghostscript – install AGPL Ghostscript software which is necessary for PCL6 printing.
- Create desktop icons for login and logout – create login and logout icons on the desktop. Clicking on login icon will prompt the user to login to SAFEQ Cloud Client (if custom login

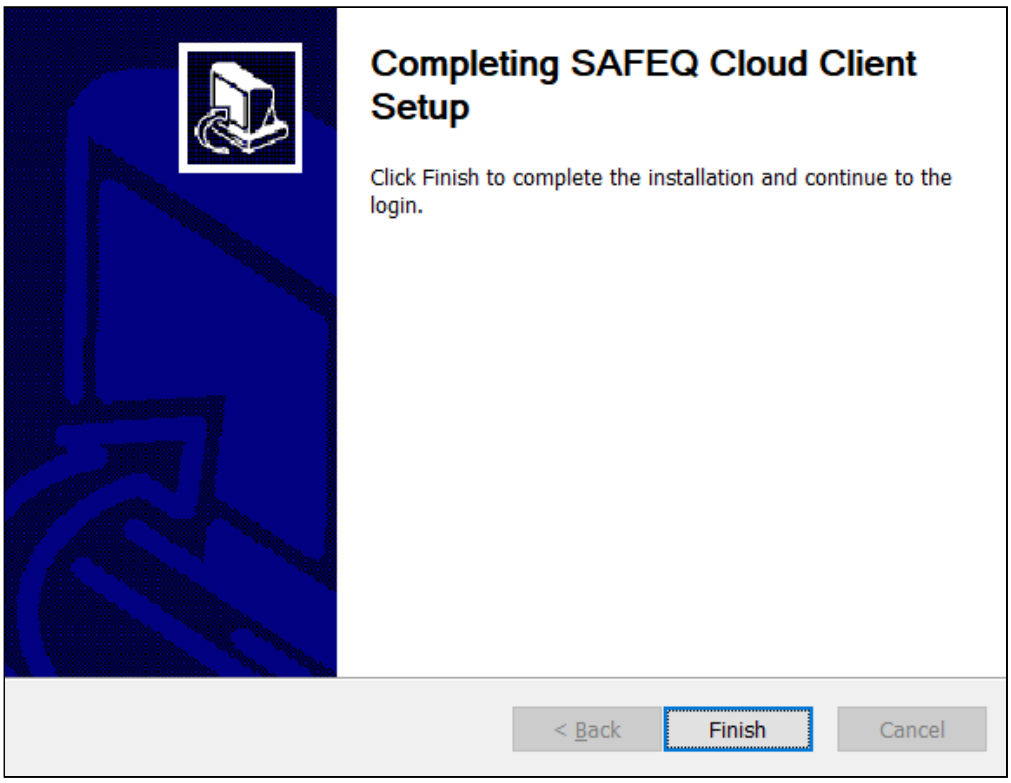
type is activated). Clicking on logout button will perform SAFEQ Cloud Client logout and delete the printers.

- **Automatically delete printers on PC session logout** – when user logs out from the operating system or shuts down PC the printers will be removed.

8. Select the target directory and click **Install**.



9. Wait while the SAFEQ Cloud Client is being installed and then click **Finish**.



10. After installation, the application will start automatically.

Unattended installation

> ⚠ Parameters `/GATEWAYADDRESS` and `/ACCOUNTDOMAIN` are mandatory when installing SAFEQ Cloud Client in unattended mode.

Windows installer accepts several command-line parameters for unattended installation:

- `/ACCOUNTDOMAIN=yyy` – chooses account domain name.
- `/AGPLGHOSTSCRIPT=true|false` – Accept the AGPL license and install Ghostscript software which is needed for PCL6 printing. The default value is `false`.
- `/ALLOWCONFIGURATION=true|false` – enable or disable the ability for the end-user to configure the SAFEQ Cloud Client after installation. The default value is `true`.
- `/ALLOWREMEMBERLOGIN=true|false` – enable or disable the ability for the end-user to remember custom login information. The default value is `true`.
- `/APIKEY=xxx` – Specify a custom API key. The default is to use the built-in restricted API key.
- `/AUTHTYPE=0|1|2|3|4|5 |6` – User authentication type: 0=Session user (default), 1=Session user + domain name, 2=Custom login, 3=User principal name, 4=Microsoft Entra OAuth2, 5=OpenID Connect, 6=SAFEQ Cloud OAuth2 login

- `/CERTSTORE=true|false` – enable or disable using a TLS certificate from the system certificate store. The default value is `false`.
- `/CERTSUBJECT=xxx` – choose a system certificate with X.509 subject or issuer matching xxx (partial string match can be used). Only relevant with `/CERTSTORE=true` option.
- `/COLOR=true|false` – set default value to color (true) or BW (false). The default value is `false`.
- `/CUSTOMDRIVER="Driver name" - will use Windows V3 Print Driver, instead of SAFEQ Cloud universal print driver.`

  Windows V3 drivers ONLY. The print driver must be already installed/available at the workstation. If not found, it will default to SAFEQ Cloud universal print driver.

  Number of features may not be available, depending on the print driver used, including possibility to change finishing options or use conversion triggers. YSoft also does not guarantee nor supports in any way that the document produced by the custom driver will be properly printed by the target printer. Ensuring compatibility between a print driver and the printer is solely in the responsibility of the vendor and / or the customer.

  Advanced only: driver can be changed in the C:\ProgramData\safeqclientcore\safeqclientcore.conf, the custom-driver="xxx" parameter. If run from powershell, triple quotes needs to be used as it seems PowerShell has problem escaping spaces otherwise on newer W11/W10 builds. From command line use single quotes. /CUSTOMDRIVER="""PCL6 Driver for Universal Print 2"
- `/D=fullpath` – install the application to an alternate path (e.g. `/D=d:\SAFEQ Cloud`). The default is `C:\Program Files\ Y Soft Corporation\SAFEQ Cloud Client`
- `/DELETEPRINTERSONLOGOUT=true|false` – enable or disable printer deletion on PC session logout (e.g. user logout from Windows). The default is false. Manual logout from the SAFEQ Cloud Client application will still remove the printers.
- `/DESKTOPICONS=true|false` – the installer will create Windows desktop login and logout buttons for Custom Login (authtype=2). The default is `false`.
- `/DIRECTOFFLINEPRINT=true|false` – enable direct offline printing functionality. The default is `false`.
- `/DUPLEX=true|false` – set default value to duplex (true) or simplex (false). The default value is `true`.
- `/GATEWAYADDRESS=xxx` – chooses SAFEQ Cloud gateway address.
- `/KEEPDEFAULTPRINTER=true|false` – if set to `true`, the default print queue is not changed by SAFEQ Cloud Client.

- `/LOGINPOPUPTYPE=0|1|2` – specify the type of the login popup: 0=no popup, 1=informational bubble, 2=dialog. The default value is `0`.
- `/OFFLINE=true|false` – the installer will skip connection to SAFEQ Cloud during the installation. Please see this section for details. This option is the opposite of `/SERVERCHECK`. The default value is `false`.
- `/PAPER=A3|A4|A5|Letter` – choose the default paper format for the driver (if different from the Windows system locale).
- `/PDFA=none/2u` – choose whether to disable PDF/A-2U document conversion in the driver. It is enabled by default.
- `/REMEMBERLOGIN=true|false` – turn on or off the login remembering option. The default value is `false`.
- `/S` – Run the installer in unattended mode.
- `/SECURESESSIONLOGIN=true|false` – enable secure session login for session authentication types. This option is applicable only when AUTHTYPE is set to 0 (Session user), 1 (Session user + domain name), or 3 (User principal name), which are considered insecure login types. This parameter is ignored during updates. The default value is true, meaning the SAFEQ Cloud Client registers an endpoint, requiring administrator authorization. When set to false, no endpoint is created, and the SAFEQ Cloud Client will only function if both Allow unauthenticated requests and Allow untrusted endpoints are enabled in the API key settings.
- `/SERVERCHECK=true|false` – the installer will skip connection to SAFEQ Cloud during the installation. Please see this section for details. This option is deprecated in favor of the `/OFFLINE` option.
- `/STORAGETYPE=0|1|2` – specify the type of storage: 0 = cloud, 1 = local storage, 2 = hybrid (direct print locally, secure print to cloud). The default value is `0`.
- `/SYNCPERIOD=nn` – automatic synchronization period, in minutes. The default period is 60 minutes.
- `/UPGRADE=true|false` – perform a full clean installation discarding the previous configuration (`false`) or upgrade the existing installation and keep the previous configuration (`true`). The default value is `false` for new clean installations and `true` if a previous installation was detected.
- `/USESERVICEACCOUNT= true|false` – controls whether the SAFEQ Cloud Client runs under a restricted virtual service account instead of the default Local System account. Default value is `false`, meaning the SAFEQ Cloud Client is installed to run with administrative privileges under the built-in Local System account. When set to `true`, `t` he SAFEQ Cloud Client is installed to run without administrative privileges. A virtual NT SERVICE account is automatically created during installation and granted the necessary permissions to add and remove printers.

When / `USESERVICEACCOUNT` is set to `true` the Auto-update feature and custom print drivers cannot be used, as both require administrative privileges.

- `/RESETCONFIG=true|false` – When used with /UPGRADE=false, it wipes out configuration files and creates new ones, effectively performing a clean installation. If not provided, it defaults to false.

Examples of SAFEQ Cloud Client usage:

- Unattended installation of SAFEQ Cloud Client to `D:\Programs\SAFEQCloudClient` directory: `safeq-cloud-client-2025.02.06.2-setup.exe /S /GATEWAYADDRESS=x.x.x.x /ACCOUNTDOMAIN=acc1 /D=D:\Programs\SAFEQCloudClient`
- Installation of SAFEQ Cloud Client with Trusted certificate: `safeq-cloud-client-2025.02.06.2-setup.exe /S /GATEWAYADDRESS=x.x.x.x /ACCOUNTDOMAIN=acc1 /SYNCPERIOD=60 /SYNCDRIVER=true /AUTHTYPE=0 /ALLOWCONFIGURATION=true /ALLOWREMEMBERLOGIN=true /REMEMBERLOGIN=false /LOGINPOPUPTYPE=0 /STORAGETYPE=1 /CERTSTORE=true /DUPLEX=true /COLOR=true`

8.3 GATEWAY GUIDE

SAFEQ Cloud uses a gateway (secondary server) on the customer site to route traffic securely between the primary server and printers. Using a local gateway, the document data itself does not have to leave the company network, increasing security, responsiveness and reducing Internet bandwidth. The gateway can be compared to a network router, and similar simple devices routing data.

The Gateway is simply installed on a prepared hardware or software appliance using the SAFEQ Cloud installer.
This Gateway Guide contains all information needed to have a fully working gateway, including hardware recommendations, appliance preparations and installation guidelines.

After the installation, perform Secondary Gateway mapping.

8.3.1 DIFFERENT GATEWAY OPTIONS

The gateway can be installed on a hardware appliance, a software appliance or on existing server infrastructure. You can also choose to use only the SAFEQ Cloud Client as a Gateway.

- **Hardware Appliance** — A hardware appliance can be a new dedicated appliance for routing print traffic, comparable to an internet router. For YSoft OMNI Bridge device, see Setting up OMNI Bridge.

- **Software Appliance** — The virtual software appliance is a pre-configured virtual machine image, ready to run on a hypervisor such as VMWare ESX, Xen or Hyper-V or similar Infrastructure-as-a-Service solutions.
- Existing Server Infrastructure — The gateway can run in a virtual environment on existing server infrastructure.

In preparation of the installation, the following pre-requisites have to be verified:
- No Firewall is blocking outbound communication on defined TCP ports to the Primary server in the Cloud. See the Ports and Protocols section *Server to Server*.
- No Proxy server filtering outbound communication to the Primary server in the Cloud. The gateway needs a direct connection to the Primary server as it creates a secure channel (TLS 1.2) that a proxy cannot handle

8.3.2 SECONDARY GATEWAYS METRICS COLLECTION

Understanding what data is collected from secondary gateways, why this information is gathered, and how telemetry can be managed is important for maintaining transparency and control. This overview details the specific metrics monitored to ensure optimal system performance, explains the purpose behind collecting this data, and outlines the available options to configure telemetry settings according to your preferences.

Please note that this feature is currently available only in certain regions, and may not be accessible everywhere at this time. Availability varies depending on your deployment region.

Data Collected

The following metrics are retrieved from each secondary gateway to monitor system health and performance:

- Customer domain
- Secondary gateway version
- Uptime duration
- Gateway name
- Authentication success and failure rates
- Authentication process duration
- Print success and failure rates
- Printing process duration
- JVM memory (RAM) usage
- JVM CPU utilization
- Storage requests per minute (covering storing, deleting, and retrieving documents)

Configuration

You can control whether telemetry data is sent by accessing the **Server information** page for the selected secondary gateway. The available options are:

- **None:** Telemetry is completely disabled, and no data is collected or transmitted.
- **Logs:** Metrics are stored locally on the gateway, with no external transmission.
- **Live:** Data is transmitted continuously to the endpoint for live monitoring.

The collected data is automatically transmitted to a secure endpoint at https://pushprox.prod.eu-west-2.ysoft-stats.com/ only if the telemetry option is set to **Live**. When this setting is enabled, data is sent continuously and in real time, allowing for immediate monitoring and analysis of gateway performance across regions. This facilitates quick detection of issues, trend analysis, and proactive management.

We want to assure you that **no private or personally identifiable information** is collected through this process. This means usernames, document names, document contents, or any other sensitive data are not included. The data collected is solely focused on system performance metrics, ensuring transparency while prioritizing your privacy and data security.

8.3.3 YSOFT OMNI BRIDGE

Setting up OMNI Bridge

Target audience: Vendors.

This step is necessary only in the edge printing scenario.

In the edge printing scenario, perform the following steps to set up an OMNI Bridge for your customer:

1. Infrastructure preparation

YSoft Partner Portal account

You will need a Partner Portal account to authorize your YSoft OMNI Bridge during the setup process. If you don't have an account, you can obtain it in the following ways:

1. If someone in your organization already has access to Partner Portal and has permission to create accounts, ask this person to create an account for you.
2. Ask the YSoft Regional Sales Manager (RSM) responsible for your organization to create an account for you.

3. Request access from YSoft Partner Portal team – send the request to partner.portal@ysoft.com.

The YSoft OMNI Bridge address has to be reserved.

You can do the following:

- Reserve an IP address for the YSoft OMNI Bridge MAC address.

  > After your OMNI Bridge receives an IP address from DHCP, reserve this IP address in your DHCP server/router for the MAC2 address of your OMNI Bridge. You can find the MAC2 address on the sticker at the back of the OMNI Bridge and also on its packaging box.

- Assign a domain name for YSoft OMNI Bridge in the local DNS.
- Configure the network manually on the device (YSoft OMNI Bridge).

> During the initial setup, the IP address of the OMNI Bridge is set to DHCP. If you want to change the IP address to static, you must run the initial setup again until the device verification code is displayed. Changing the IP address during the initial setup of the OMNI Bridge may cause problems with the device. The IP address should be changed after the initial setup is completed.

For information on how to configure the network manually on the device, see OMNI Bridge operation manual section *Network*.

NTP server must be available for the YSoft OMNI Bridge device.

- If you have your own NTP server or have a specific NTP server already allowed in your firewall, allow traffic from YSoft OMNI Bridge to your NTP server. Make sure your NTP server is properly specified in your local DHCP server.
- If the NTP address is not obtained via DHCP, YSoft OMNI Bridge defaults to Google NTP servers. Create a firewall rule to allow UDP traffic on port 123 to these servers: time1.google.com, time2.google.com, time3.google.com, and time4.google.com.
- Change the NTP server manually on the device (YSoft OMNI Bridge).

To configure the NTP server manually on the device, do the following:

1. Press **0** to enter the service menu.
2. Enter PIN and press .
3. Select **Time settings** and press **0**.
4. Select **Set NTP servers** and press **0**.
5. Select **Add new NTP server** and press **0**.
6. Enter your NTP server and press .
7. Press to save your changes.

Network connectivity

IoT Hub

The following connectivity to IoT Hub is required:

- Connectivity to IoT Hub Device Provisioning Service (DPS) - worldwide endpoint. DPS is a helper service for IoT Hub that is used to configure zero-touch device provisioning to a specified IoT Hub.
  Reference: https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-glossary?toc=/azure/iot-dps/toc.json&bc=/azure/iot-dps/breadcrumb/toc.json#device-provisioning-service
- Connectivity to IoT Hub where DPS assigns the device to. When the OMNI Bridge is receiving configuration from IoT Hub, it uses port TCP 443 to connect.
  Reference: https://www.cloudelicious.net/azure-region-and-datacenter-find-your-best-match/
- Connectivity to Azure Container Registry (ACR) - The OMNI bridge will download the latest updates/containers from ACR.
  Reference: https://docs.microsoft.com/en-us/azure/container-registry/container-registry-intr

Firewall rules

The following external domains and their communication ports must be allowed in your network firewall for the edge devices to function correctly.

`mcr.microsoft.com`	443	Microsoft Container Registry
`*.data.mcr.microsoft.com`	443	Data endpoint providing content delivery
`*.cdn.azcr.io`	443	Deploy modules from the Marketplace to devices
`global.azure-devices-provisioning.net`	443	Device Provisioning Service access (optional)
`*.azurecr.io`	443	Personal and third-party container registries
`*.blob.core.windows.net`	443	Download Azure Container Registry image deltas from blob storage
`*.azure-devices.net`	5671, 8883, 4431	IoT Hub access

`*.docker.io`	443	Docker Hub access (optional)
`*.ysoft.cloud`	443	Partner Portal
`*.ysoft.cloud`	443	SAFEQ Cloud Primary
`*.google.com`	UDP 123	NTP server (time{1-12}.google.com) or any chosen NTP server
`ports.ubuntu.com`	80	Official Ubuntu package repository for non-x86 architectures
`cdn.everyoneprint.com`	443	SAFEQ Cloud Secondary Installation Files

Use of HTTP (Port 80) for APT Traffic to `ports.ubuntu.com`

The `ports.ubuntu.com` repository serves Ubuntu packages for non-x86 architectures and primarily uses HTTP over port 80 for package distribution. Although HTTP is unencrypted, APT ensures the security and integrity of all downloaded packages and metadata through robust GPG signature verification. This cryptographic validation guarantees that any tampering or unauthorized modification of packages is detected and rejected before installation.

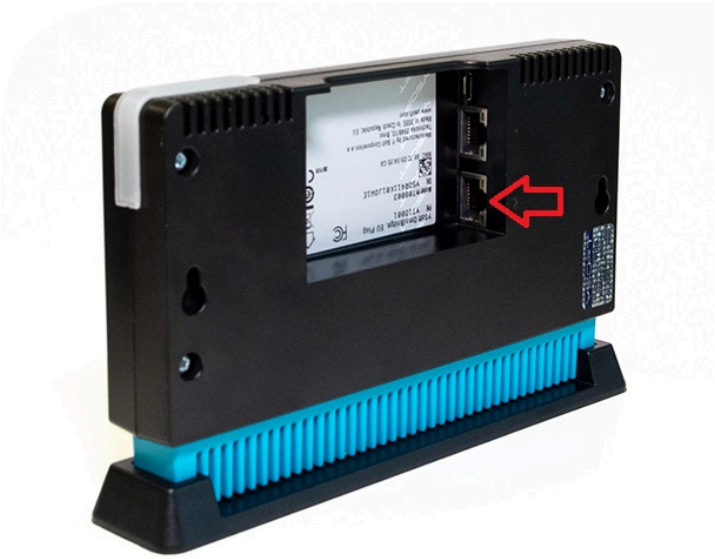
As a result, the use of HTTP on port 80 is considered secure and is the standard method employed by official Ubuntu repositories, including `ports.ubuntu.com`. Therefore, allowing outbound traffic on port 80 to this endpoint is necessary and generally poses no undue security risk within the APT package management context.

2. OMNI Bridge Preparation

1. Ensure your **partner portal account** is set up.

   For more information, see section Setting up OMNI Bridge above..

2. **Plug an Ethernet cable** into network port 2 and note down its MAC address.



3. Make sure you have **reserved an IP address** for the MAC address of your YSoft OMNI Bridge. For more information, see section Setting up OMNI Bridge above.

> Do not change the assigned IP address! If the address changes, the device must be reconfigured.

4. Make sure your YSoft OMNI Bridge has access to an **NTP server**. For more information, see section Setting up OMNI Bridge above.

5. **Attach the power supply.** YSoft OMNI Bridge will start to initialize. This process usually takes several minutes, but it can take a longer time for the device to download the necessary modules and configure itself.

> Do not turn the power during the initialization process off.

6. When the OMNI Bridge is ready, it will show an **eight-letter device verification code** and its LED light will be orange.

> If the device code is too small for you to read:
>
> a. On the **Device status screen**, press two times.
>
>
>
>
> b. This will take you to the **Module status screen**. Press **0** and .

c. You will see the device code displayed in bigger letters.

When the OMNI Bridge is ready, it will show an eight-letter device verification code and its LED light will be orange.

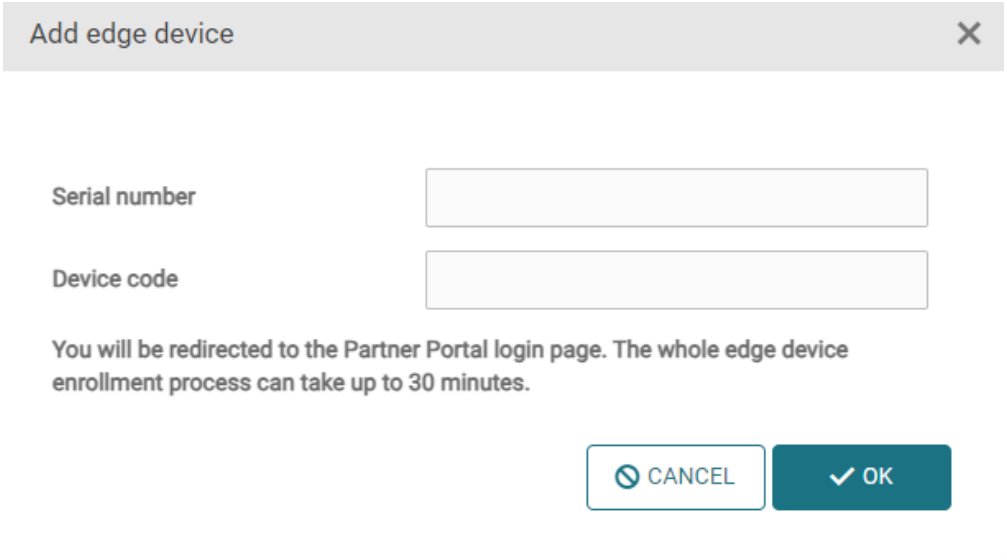
The code expires after 10 minutes and a new code is generated.

3. Adding the device in SAFEQ Cloud Web UI

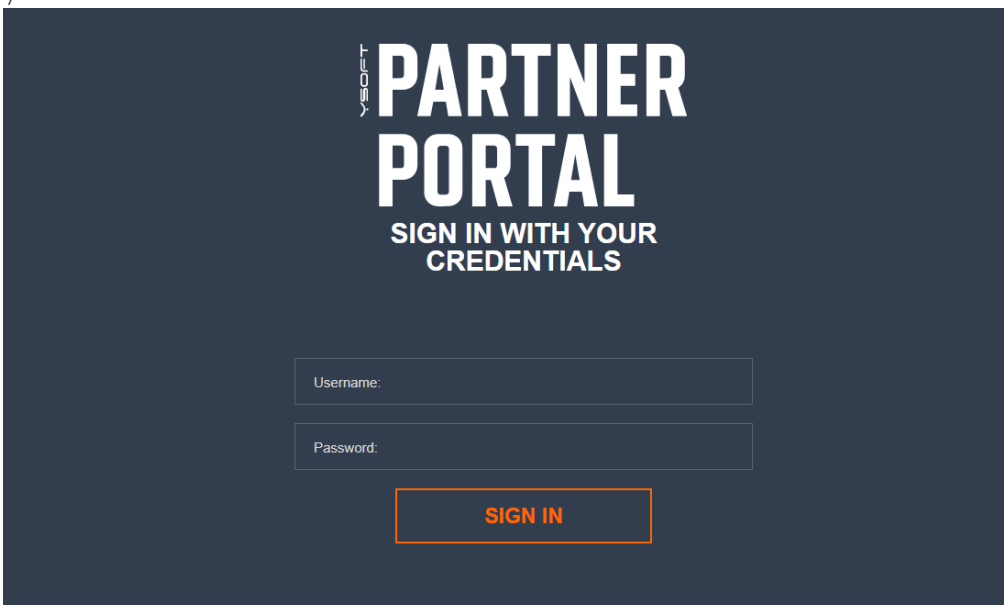
1. Log in to SAFEQ Cloud Web UI.

Only Chrome, Firefox and Edge browsers are supported.

2. Go to Security > Endpoints.
3. Click Add edge device.
4. Fill in the following:
   - Serial number – You can find it on the sticker at the back of the device.
   - Device code – The eight-letter device verification code which your OMNI Bridge displays after the initialization phase.

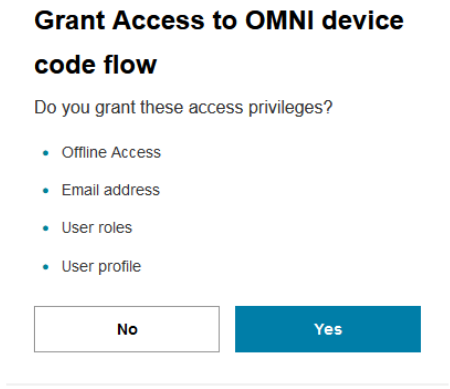


5. To authorize the device, a new tab with **Partner Portal login** will open in your browser. Enter your Partner Portal credentials.



6. Grant the requested permissions by clicking **Yes**.

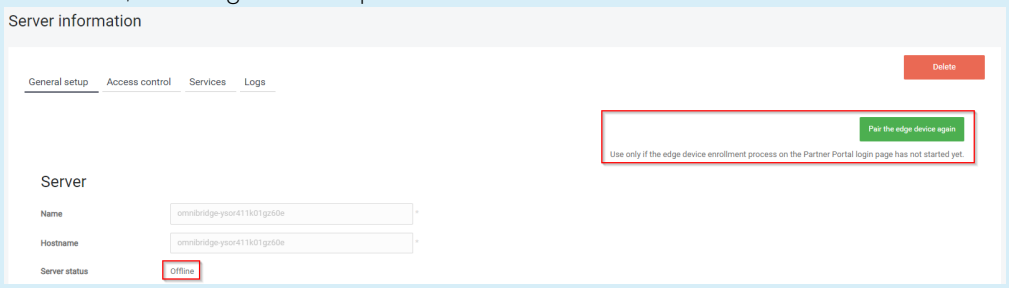
Do not close the Partner Portal tab until the device is authorized in the next step!



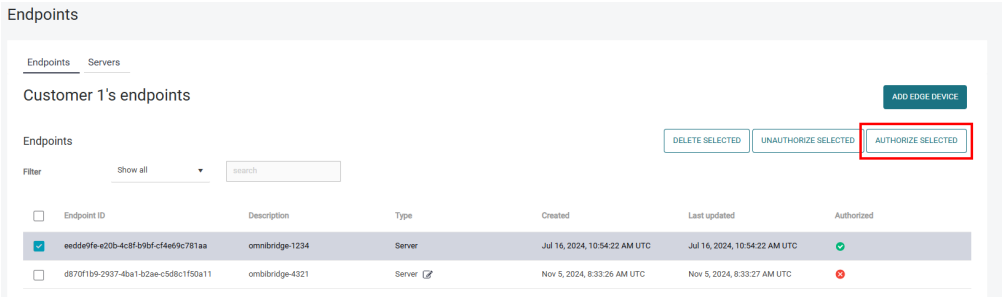
If you accidentally closed the Partner Portal page before you could grant access to the OMNI bridge device, or if you want to start the enrollment process for a device added some time ago, you can do it from its server detail page in SAFEQ Cloud Web UI.

1. The option is only available for devices that are authorized and offline. To successfully finish the enrollment process, the device must still be set up according to the *Setup* section of this document.

2. On the **Server information** page, click **Pair the edge device again**. Don't do this while the enrollment process is in progress. The process may take several minutes; therefore, starting another process will not work.



7. You will see the newly added device in **Endpoints**. **Select it and click Authorize selected**.



> You can see the device details by clicking the link icon next to **server**. You can authorize the device from the details view as well.

8. **The device will continue downloading and installing modules**. The process may take up to 10 minutes. When finished, the LED will turn blue.

> Startup of the necessary services can take more than 10 minutes, depending on which services were configured. The service state is not visible in the Web UI. You can only monitor it in server siteapp.log. Note that service startup also happens after each reboot or software update of the OMNI Bridge.
>
> The embedded terminals connected to your OMNI Bridge may be slower to respond during your first interaction (such as logging in at the MFD) as the components may still be loading.

9. When you add a new OMNI bridge device, a **new value is automatically added to the default Edge API key**. See **API access keys**.

4. Performing secondary gateway mapping

After all the modules are downloaded, perform the secondary gateway mapping as described in **Secondary Gateway mapping**.

5. Adding services to your OMNI Bridge

As a minimum, add the following services to your OMNI Bridge so that it can function as a gateway:

- Converter
- Storage
- Documentoutput

For how to do that, see Services.

Optional services:

- Add *Api* if you plan to use Gateway storage rather than Local storage or Cloud.
- Add *Authentication* if you need the edge device to connect to Active Directory or Microsoft Entra ID directly. Otherwise, the cloud instance of the Authentication service will be used.
- Add *Terminalclient* if you plan to use the legacy embedded terminals.
- Add other services according to your needs.

6. Security

Physical security

We recommend you to keep your OMNI Bridge in a physically secure area to prevent unauthorized access or theft. The OMNI Bridge has strong overall security, but its internal storage which contains print data and meta data (including user information) is not encrypted on HW level.

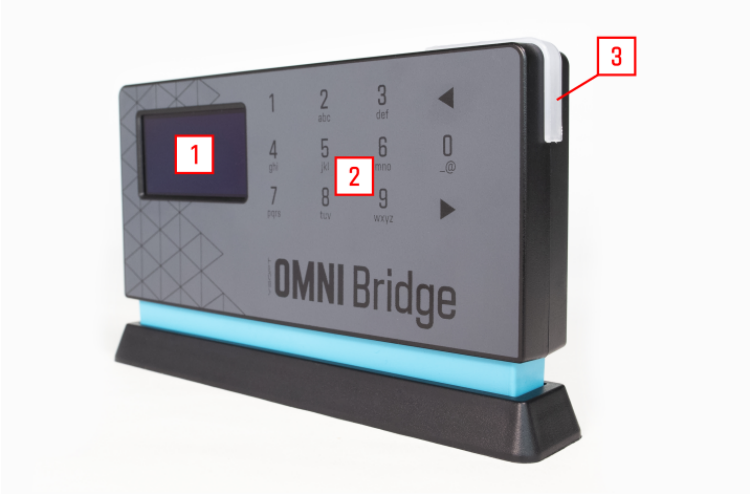
Changing the manager password

If you wish to change the manager password for your OMNI Bridge, see OMNI Bridge operation manual section *Change manager password*. We strongly recommend changing the password only after the enrollment of the device in your SAFEQ Cloud is complete.

OMNI Bridge operation manual

About YSoft OMNI Bridge

YSoft OMNI Bridge is a small device (about a size of a router), that can connect any networked printer to the cloud. This piece of hardware is manufactured by Y Soft.



1. Display
2. Keyboard
3. Device status LED

Safety instructions

Use only the AC power adapter provided with your YSoft OMNI Bridge. The voltage must be the same as stated on the adapter.

Do not expose the device to water.

Do not expose the device to fire.

Clean only with a dry cloth.

Keep unprotected cords out of the path of foot traffic to prevent tripping. Do not leave cords dangling in places where they can be pulled down and tripped over.

Regulatory information

Only for indoor use

CE (Europe)

WEEE (Europe)

The product conforms with Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment (WEEE) and Directive 2003/108/EC of the European Parliament and of the Council of 8 December 2003 amending Directive 2002/96/EC on waste electrical and electronic equipment (WEEE).

FCC (USA)

FCC Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

- this device may not cause harmful interference
- this device must accept any interference received, including interference that may cause undesired operation

ISED (Canada)

CAN ICES-003(B)/NMB-003(B)

ISED statement

This Class B digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la class B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

EAC (Eurasian Customs Union)

ACMA (Australia/New Zealand)

China RoHS

Y Soft Corporation, a.s. Technology Park, Technická 2948/13 616 00 Brno Czech Republic P: +420 533 031 500; email: info@ysoft.com

Y Soft North America, Inc., 1452 Hughes Road, Suite 110, Grapevine, TX 76051, USA; P:+1 888-761-9977; email: info.na@ysoft.com

Y Soft Japan Ltd. 〒658-0032　兵庫県神戸市東灘区向洋町中６－９神戸ファッションマート１０階; email: info.jp@ysoft.com

https://www.ysoft.com

Technical specifications

Parameter	Description
Size	178 mm H / 103 mm W / 33 mm D
Weight	400 g
Operating System	Linux
Status indicators	RGB LED
User interfaces	White OLED Display, 12-pad capacitive touch keyboard
Power source	External 12V (DC jack 2.1 mm)
Network connectivity	2 10/100/1000 Ethernet
CPU	NXP i.MX 6DualLite Cortex-A9 @1 GHz
RAM	4GB RAM
Storage	64GB eMMC

Operating conditions

Operating condition	Value
Working temperature	+5°C to +35°C
Storage temperature	0°C to +50°C
Working air humidity	20% to 85% without condensation
Storage air humidity	8% to 85% without condensation

LED statuses

The LED indicator on YSoft OMNI Bridge displays the following colors based on device status:

- No light – Early device startup.
- Yellow – A module (or the device) is starting or processing.
- Blue – All modules are operational.
- Orange – User input is required.
- Red – Error or alert state.

During normal routine operation after the device has been powered on, the LED color transitions from no light to yellow and then to light blue.

During an update, the components need to be restarted. This will briefly turn the device status indicator yellow, indicating that some component is starting or restarting.

Based on the installed modules, other colors may be displayed. For information on the meaning of these colors, consult the specific module documentation.

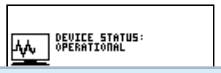
Operating System updates

The version of the Operating System is automatically updated after your device is connected to the Internet.

Main menu

The YSoft OMNI Bridge main menu consists of the following screens:

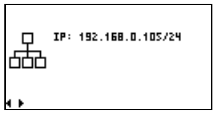
Device status screen – Current device status summary.



If your YSoft OMNI Bridge displays a device verification code on the device status screen and the code is too small for you to read, do the following:

1. On the **Device status screen**, press two times.
2. This will take you to the **Module status screen**. Press **0**.
3. You will see the device code displayed in bigger letters.

Network status screen – The current network address as received from DHCP. Should the device receive an IPv6 address other than link-local, it will also be displayed here.



Module status screen – If there are any modules running on your OMNI Bridge, you can see their individual statuses here. Press **0** to display details.

Device info screen

Press 0 to display to access the following information about the device:

- Serial number
- Default PIN
- Default manager password
- Main MAC address
- Auxiliary MAC address
- Current OS version

Press or to navigate through the screens.

Service menu screen – For more information, see the section *Service menu*.

Press or to navigate through the screens.

Service menu

The Service menu is accessible from any main menu screen:

1. Press 0.
2. Enter PIN and press . The default PIN is located on a sticker on the back of the device.
3. The Service menu is displayed.

In the Service menu, you can find the following settings:

Logout – Log out from the Service menu.

Network – Network configuration menus.

IMS address – Adding an IMS server address.

Use IMS pairing key – Pairing the device with the IMS.

Time settings – Set NTP time servers.

Change PIN – Change the PIN to access the Service menu.

Factory reset – Perform a device factory reset.

All settings are described in detail below.

Logout

1. In the Service menu, use or to select Logout.

2. Press 0.
3. You are logged out of the Service menu.

Network

IPv4

By default, the network is configured by DHCP.

Disabling the DHCP and configuring the IP address manually

To enable manual configuration, turn off the DHCP and then proceed with the configuration:

1. In the Service menu, use or to select Network.
2. Press 0.
3. Select IPv4: DHCP and press 0.
4. Select DHCP: On and press 0.
5. Select Disable DHCP and press 0.
6. The Manual config screen appears for a short period of time.
7. Enter the IP address and press .
8. Enter the network mask and press .
9. Enter the gateway address and press .
10. Enter the DNS address and press to save all changes.

After the IPv4 has been set to a static address, you can use the Network setting wizard to edit all subsequent settings in one flow or set the IPv4 address, IPv4 Network mask, IPv4 Gateway, and DNS individually. For individual settings, select a setting, enter a value and press to save changes.

Enabling the DHCP

1. In the Service menu, use or to select Network.
2. Press 0.
3. Select IPv4: Static and press 0.
4. Select DHCP: Off and press 0.
5. Select Enable DHCP and press 0.
6. The DHCP is enabled.

Disabling the IPv4 stack

1. In the Service menu, use or to select Network.
2. Press 0.

3. Select **IPv4: DHCP** and press **0**.
4. Select **Disable IPv4** and press **0**.

Enabling the IPv4 stack

1. In the Service menu, use or to select **Network**.
2. Press **0**.
3. Select **IPv4: Disabled** and press **0**.
4. Select **DHCP: Off** and press **0**.
5. Select **Enable DHCP** and press **0**.

IPv6

By default, the network is configured by DHCP.

Disabling the DHCPv6 and configuring the IP address manually

To enable manual configuration, turn off the DHCPv6 and then proceed with the configuration:

1. In the Service menu, use or to select **Network**.
2. Press **0**.
3. Select **IPv6: DHCP** and press **0**.
4. Select **DHCPv6: On** and press **0**.
5. Select **Disable DHCPv6** and press **0**.
6. The **Manual config** screen appears for a short period of time.
7. Enter the IP address and press .
8. Enter the network mask and press .
9. Enter the gateway address and press .
10. Enter the DNS address and press to save all changes.

After the IPv6 has been set to a static address, you can use the **Network setting wizard** to edit all subsequent settings in one flow or set the **IPv6 address**, **IPv6 Network mask**, **IPv6 Gateway**, and **DNS** individually. For individual settings, select a setting, enter a value and press to save changes.

Enabling the DHCPv6

1. In the Service menu, use or to select **Network**.
2. Press **0**.
3. Select **IPv6: Static** and press **0**.
4. Select **DHCP: Off** and press **0**.

5. Select **Enable DHCPv6** and press **0**.
6. The DHCPv6 is enabled.

Disabling the IPv6 stack

1. In the Service menu, use or to select **Network**.
2. Press **0**.
3. Select **IPv6: DHCP** and press **0**.
4. Select **Disable IPv6** and press **0**.

Enabling the IPv6 stack

1. In the Service menu, use or to select **Network**.
2. Press **0**.
3. Select **IPv6: Disabled** and press **0**.
4. Select **DHCPv6: Off** and press **0**.
5. Select **Enable DHCPv6** and press **0**.

Ethernet separation

By default, the two network interfaces on the device are bridged together. The device can be connected to the network using either of them.

For some applications, it is possible to strictly separate the interfaces.
Once separation has been enabled, the network interfaces are no longer equal and must be used as follows:

- Interface 1 – Isolated network
- Interface 2 – Internet connection

There is no need to separate the interfaces for YSoft OMNI UP365.

To enable or disable Ethernet separation, do the following:

1. In the Service menu, use or to select **Network**.
2. Press **0**.
3. Select **Eth. sep.: Disabled / Enabled** and press **0**.
4. Select **Enable / Disable eth. sep.** and press **0**.
5. Confirm by pressing .
6. Press **0** to return to the **Network** menu.

IMS address

IMS is obsolete.

Adding a new IMS address

1. In the Service menu, use or to select **IMS address**.
2. Press **0**.
3. Select **Add new IMS address** and press **0**.
4. Enter a new IMS address and press .
5. Press to save changes.

All IMS addresses in the list will be tested and the first to respond will be used.

Editing an IMS address

1. In the Service menu, use or to select **IMS address**.
2. Press **0**.
3. Use or to select an IMS address and press **0**.
4. Select **Edit** and press **0**.
5. Edit the IMS address and press .
6. Press to save the changes.

Deleting an IMS address

1. In the Service menu, use or to select **IMS address**.
2. Press **0**.
3. Use or to select an IMS address and press **0**.
4. Select **Delete this server** and press **0**.
5. Confirm by pressing .

Use IMS pairing key

IMS is obsolete.

1. In the Service menu, use or to select **Use IMS pairing key**.
2. Press **0**.
3. Press to confirm.

4. Enter the pairing ID and press .
5. Enter the pairing key and press .
6. Press again to use the IMS pairing key.

Time settings

Setting NTP server

Google time servers are used by default.

> YSoft OMNI Bridge will try to connect to the NTP servers in the same order as they are listed, and will use the first reachable NTP server.

Adding new NTP server

1. In the Service menu, use or to select **Time settings**.
2. Press **0**.
3. Select **Set NTP servers** and press **0**.
4. Use or to select **Add new NTP server** and then press **0**.
5. Enter a new NTP server address and press .
6. Press to save changes.

Editing an NTP server

1. In the Service menu, use or to select **Time settings**.
2. Press **0**.
3. Select **Set NTP servers** and press **0**.
4. Use or to select a server you want to delete and then press **0**.
5. Select **Edit** and press **0**.
6. Edit the NTP server address and press .
7. Press to save changes.

Deleting an NTP server

1. In the Service menu, use or to select **Time settings**.
2. Press **0**.
3. Select **Set NTP servers** and press **0**.
4. Use or to select a server you want to delete and then press **0**.
5. Select **Delete this server** and press **0**.

6. Confirm by pressing .

Change PIN

1. In the Service menu, use or to select **Change PIN**.
2. Press **0**.
3. Enter the current PIN and press .
4. Enter a new PIN and press .
5. Enter the new PIN once again for confirmation and press to save changes.

Change the manager password

1. Log into the management shell using the following command:

   ```
   ssh manager@<IP address of your OMNI Bridge>
   ```

2. To set a new password, type:

   ```
   password set manager
   ```

3. Enter a new password.
4. Confirm the new password by entering it again.

Factory reset

The device may need further configuration after a factory reset has been performed. You will therefore need to call our service desk to bring the device back online.

1. In the Service menu, use or to select **Factory reset**.
2. Press **0**.
3. Press to continue.
4. Confirm by pressing .
5. If you press **1**, the reset will proceed only if the device is not busy (for example, printing is in progress).
6. If you press **7**, the reset will proceed immediately, regardless of the device status.

In case of an emergency, you can perform a factory reset even without knowing the service menu pin.

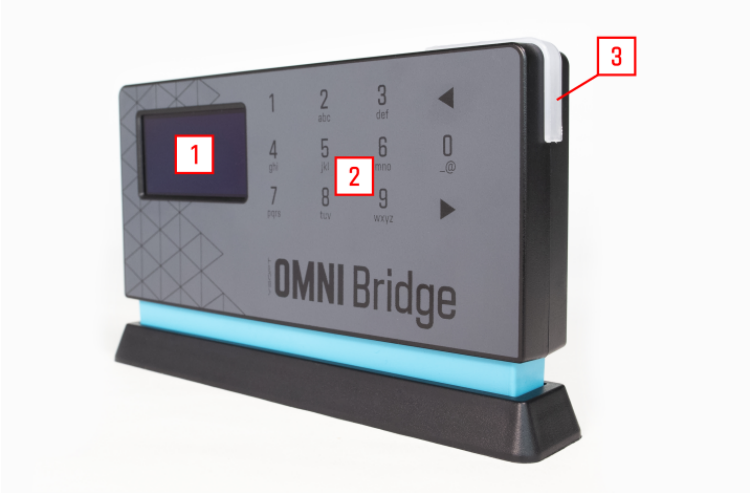
You can enter the word "factoryreset" (which corresponds to numerical pin "322867973738") on the keypad instead of the Service menu PIN. This will take you directly to the factory reset wizard.

This feature cannot be turned off.

OMNI Bridge gateway installation and troubleshooting

About YSoft OMNI Bridge

YSoft OMNI Bridge is a small device (about the size of a router), that works as a print server.



1. Display
2. Keyboard
3. Device status LED

The LED indicator on YSoft OMNI Bridge displays the following colors based on device status:

- No light – Early device startup.
- Yellow – A module (or the device) is starting or processing.
- Blue – All modules are operational.
- Orange – User input is required.
- Red – Error or alert state.

For more information on YSoft OMNI Bridge, see OMNI Bridge operation manual.

About YSoft OMNI Bridge Site Server

The YSoft OMNI Bridge gateway is a YSoft OMNI Bridge configured to provide local site services as an Edge device.

A new YSoft OMNI Bridge is delivered without any software or configuration, except for basic utilities. Upon starting for the first time, the device will try to obtain the latest software images and a valid configuration from the Azure portal, specifically the Azure IoT Hub Device Provisioning Service (DPS).

The whole installation process may take approximately 30 minutes, depending on network throughput. If the installation process takes more than 120 minutes, please contact service desk.

Basic prerequisites

- Power supply
- Internet connection

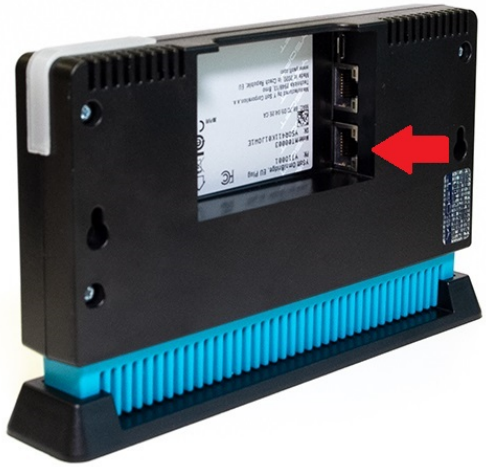
For the complete list of prerequisites see Setting up OMNI Bridge.

Installation

The installation process consists of the following steps:

Power on

1. Unpack the YSoft OMNI Bridge device.
2. Plug a network cable into the second network port and connect YSoft OMNI Bridge to the Internet (see the picture below).



3. Plug the power cable into the power port and then connect the power adapter to a power outlet. The YSoft OMNI Bridge will start to initialize. The display will show DEVICE STATUS: STARTING, and the LED light will turn yellow.

Hardware enrollment

The hardware enrollment phase of installation is fully automated. During this phase, the *Azure runtime* module tries to connect to the Azure DPS. At the beginning of this phase, the display shows DEVICE STATUS: DPS CONFIGURATION > PROCESSING. If any error occurs during the hardware enrollment phase, see section *Troubleshooting – Azure runtime connectivity errors*.

After a successful connection, the display will show DEVICE STATUS: OPERATIONAL, and the LED light will turn blue.

Module download

The Module download phase is fully automated. It begins after the successful completion of the "HW enrollment phase". Azure runtime will download all modules based on Azure deployment. At the start of the downloading process, the display shows DEVICE STATUS: DOWNLOADING MODULES > INITIALIZING.

> This screen is optional. If all download requirements have already been met, the downloading progress is displayed instead.

Once all download requirements have been met, the display will show the downloading progress e.g., DEVICE STATUS: DOWNLOADING MODULES > MODULE X OF Y. The progress speed is based on network throughput.

> Azure runtime periodically checks if there has been any change in Azure deployment. If change is detected, then the progress is displayed.
>
> The downloading progress may also be displayed after the restart of the device. Azure runtime checks that modules are downloaded and started according to the current Azure deployment.

Once all modules have been downloaded (started), the display will show DEVICE STATUS: PLEASE VERIFY DEVICE CODE and the LED light will turn orange.

Device code flow

Perform the device code flow as described in Setting up OMNI Bridge.

Device configuration

Add the device in SAFEQ Cloud Web UI, perform the secondary gateway mapping and add services to the OMNI Bridge as described in Setting up OMNI Bridge.

After a successful configuration, the display will show DEVICE STATUS: OPERATIONAL, and the LED light will turn blue.

Troubleshooting

DEVICE STATUS: DOWNLOADING MODULES

Description: The YSoft OMNI Bridge may display the DEVICE STATUS: DOWNLOADING MODULES message after it is restarted even if it has been fully configured and functional.

Resolution: Wait for the download to finish.

Azure runtime connectivity errors

AZ-RUN-0001

Description: DPS availability error.

Resolution: The OMNI Bridge does not have a connection to the Azure IoT Hub Device Provisioning Service (DPS). This problem can occur when the connection to the Internet has been lost for any reason. This error code is displayed for information purposes only.

Next steps: Check that YSoft OMNI Bridge has access to the Internet and Azure DPS service is available. Check if the AZ-RUN-0002 error appears.

AZ-RUN-0002

Description: DPS connection error.

Resolution: Connection to the Azure IoT Hub Device Provisioning Service (DPS) failed. This problem can happen when the Azure DPS service is out of order or the Internet connection has been lost. The device uses a cycle that repeats requests to the DPS. If a response is successfully obtained during the cycle, the error code disappears and the enrollment process continues.

Next steps: Check that the Azure DPS service is available or the OMNI Bridge has not lost access to the Internet. If the problem persists, contact your service representative.

8.3.4 ADD A SECONDARY GATEWAY SERVER

Install a secondary gateway when you need to add a new server to the existing deployment, where either a vendor or a customer primary server already exists. This page is applicable to Gateway on Software Appliance and Gateway on Hardware Appliance.

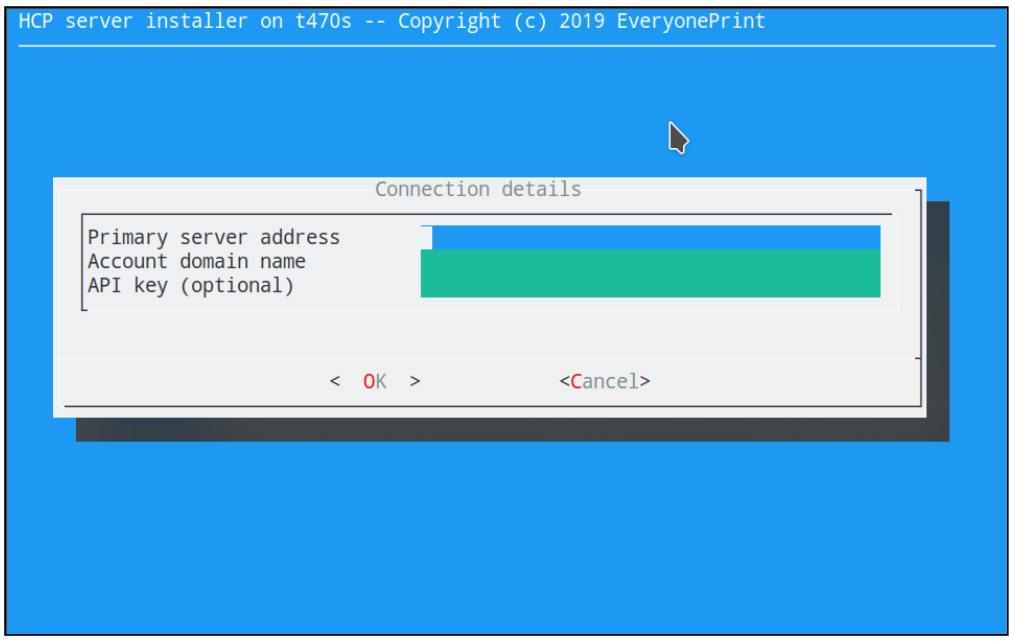
This is often necessary in the following cases:

- Scalability, when some load should be distributed across multiple servers
- Access to the private network, for example for authentication or embedded terminal deployments. Because primary server doesn't normally has access to the customer's internal networks an additional server is required which will connect to internal authentication services (LDAP) or to printers on the Intranet.

If you want to send print jobs or use embedded terminal clients from a secondary gateway server, make sure you create a DNS entry for the server.

For a complete guide to setting up an appliance and installing the gateway, see the Gateway Guide section.

To install secondary server the following options should be provided:

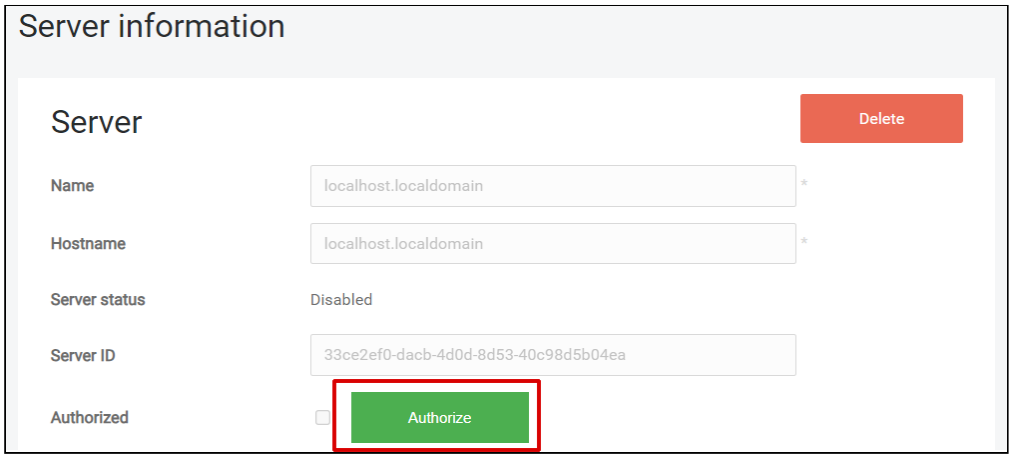


- Primary server address – this is the IP address or domain name of the primary server. It does not have to match any DNS names of the accounts.
- Account domain name – this field should be filled with the DNS name of the account to which this server will be attached to.
- API key – optional API key from the account settings, used for server registration. If left blank the default restricted API key will be used.

The installer will try to connect to the primary server and validate the entered information. If there is no connection or the specified account domain name is wrong the error message will be printed. If the entered details are valid installation will proceed.

After the secondary server starts it will attach itself to the specified account. It will be possible to see it under the tree on the left side of the web UI.

By default, secondary servers are "not trusted" by a primary server. So after adding the secondary server, go to the server's Server information and click Authorize to allow the secondary server to establish a secure connection to the primary server.



8.3.5 GATEWAY ON HARDWARE APPLIANCE

A Gateway hardware appliance can be installed on Customer site to route traffic securely between the primary server and printers.

After the hardware appliance is prepared, you can simply install by following the Server Installation section.

For YSoft OMNI Bridge device, see Setting up OMNI Bridge.

Use cases

The choice of specific Gateway hardware is simply based on the number of printers installed, from 1 to 500. In case more than 500 printers are installed, it is just a matter of installing extra gateways.
The customer can choose to have extra Gateways installed as redundancy in case of network or power outage. For sizing, see Server Requirements, section *Recommended server sizing*.

Recommended hardware

These are recommendations for specific hardware. NUC kits from Intel have been selected due to small physical form-factor, high quality standards and availability. Appliances with similar specifications will work equally well. Y Soft is not affiliated with any suppliers of hardware appliances.

	GW Small (R3)	Large (R5)
Model name	AMD LLM1r3RK	AMD LLM1r5RK
CPU	AMD	AMD
Memory	8GB	16GB
Hard Disk	128GB M2 SSD	256GB M2 SSD

8.3.6 GATEWAY ON SOFTWARE APPLIANCE

A SAFEQ Cloud Gateway can be installed as a software appliance using the approach described on page Rocky Linux 9 Software Appliance.
The software appliance can be a Virtual Machine (VM) running at any Infrastructure as a Service (IaaS) provider, e.g. Amazon EC2 or Microsoft Azure. For this guide we will explain the detailed steps of installing SAFEQ Cloud Gateway using VMware.

Using virtual appliances allows for extremely rapid provisioning of SAFEQ Cloud primary or secondary gateway servers, and cleanly decouples the operator from the consumer by encapsulating all knowledge of the application within the virtual appliance.

The choice of specific Gateway virtual hardware specifications is simply based on the number of users and printers installed. Additional gateways can be configured for scalability or availability.

Rocky Linux 9 Software Appliance

This document outlines the specifics of a virtual appliance designed to operate on VMware with Hardware Version 17. It is compatible with ESXi 7.0 and later versions.

Y Soft offers a comprehensive Virtual Software Appliance that includes Rocky Linux 9 and the latest version of SAFEQ Cloud. For detailed package specifications, see the *Complementary Information* section of this page.

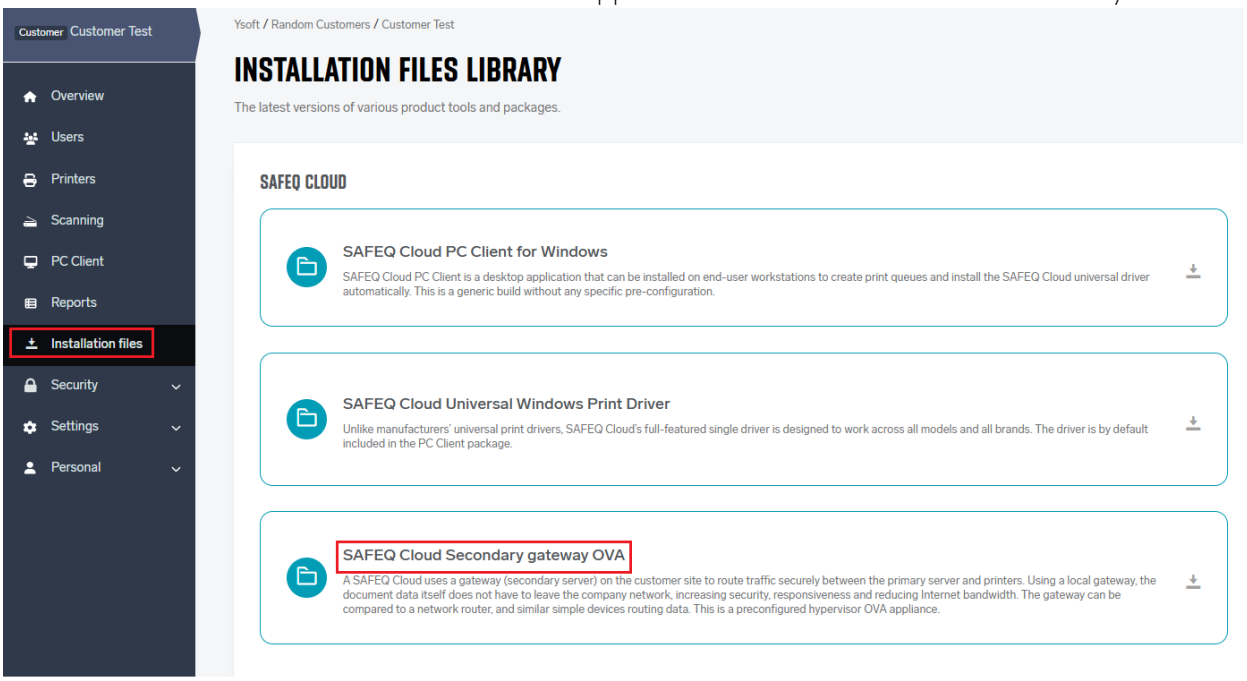
This guide is applicable to virtual machines using OVA/OVF images.

Prerequisites

A functioning virtual machine (VM) environment. If you are not sure how to set up a VM, ask your IaaS provider for assistance.

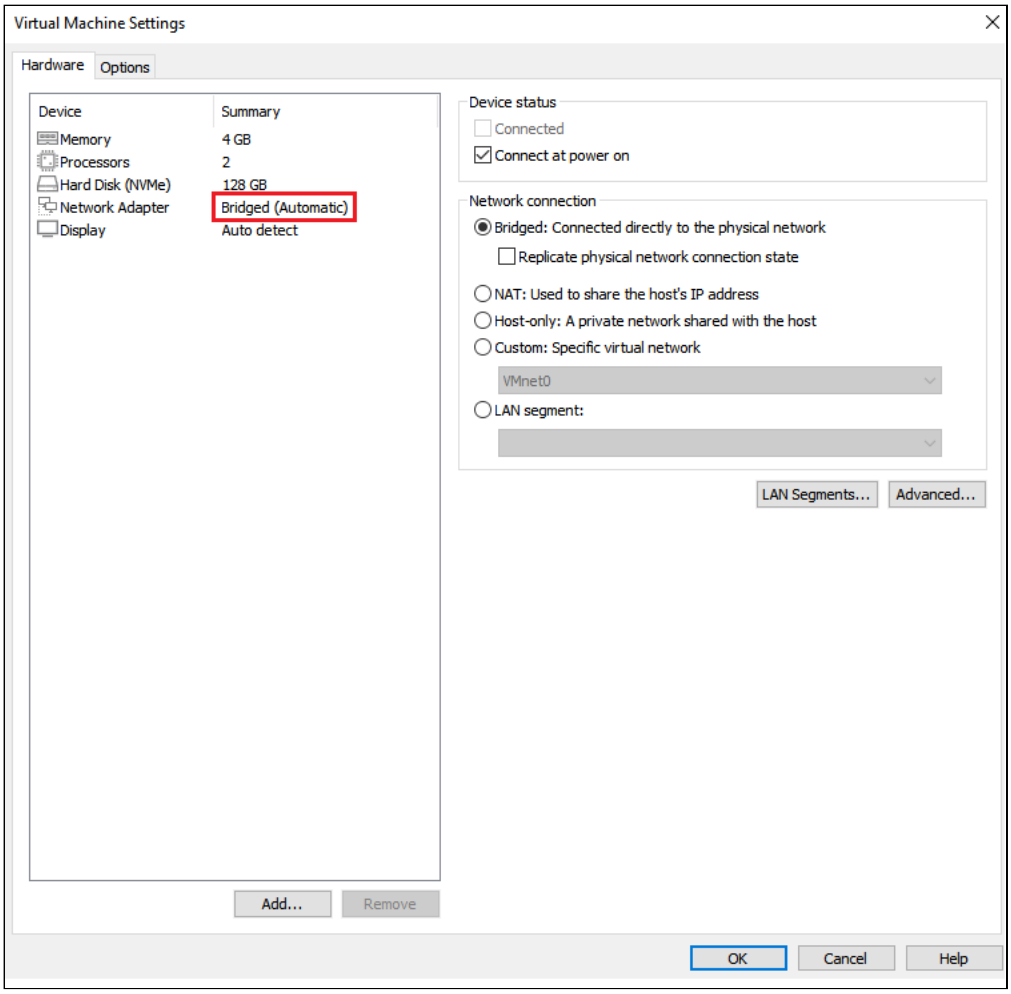
Installing the Virtual Software Appliance

1. Download the most recent Virtual Software Appliance from the **Installation files** library.



2. Open the package in your VM manager. If you are using VMware, select **File** > **Open**, then navigate to the Virtual Software Appliance and follow the on-screen guided instructions.
3. Once the Virtual Software Appliance is imported, verify and adjust the VM settings:
   a. **Memory size** – The default is 4 GB.
   b. **Processor** – We recommend 1 processor/2 cores.
   c. **Options** > **VMware Tools** – Verify the **Synchronize guest time with host** option. Disable automatic updates as the appliance uses *open-vm-tools* updated with Rocky Linux 9.

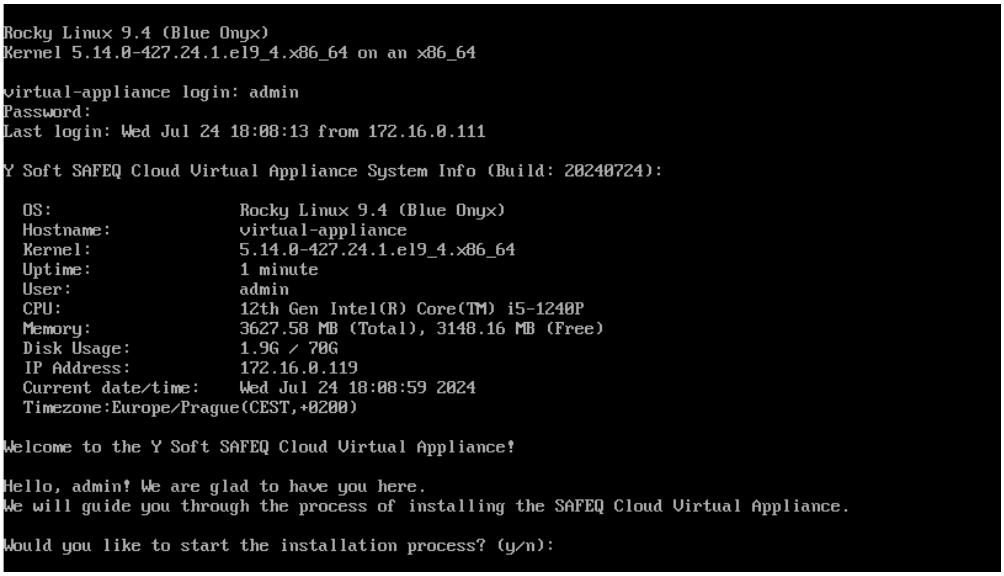
d. **Network** – Make sure the network adapter is set to **Bridged Mode** to ensure the appliance has direct access to the network.



4. Start the VM.
5. At the login prompt, enter **admin** as the username and **va** as the password.
6. After your first login, you will be prompted to change your password. If you are connected via SSH, you will be disconnected after changing the password. Log in again to continue.

> ⚠ By default, the appliance is set up to use the US keyboard mapping.

7. The Appliance Welcome screen provides a comprehensive view of the setup. Note these values, as you will be customizing them later on.



From here, you can continue the installation in your VM manager or remotely connect to the appliance using an SSH client such as MobaXterm or PuTTY (see the *Complementary Information* section) with the username **admin** and your new password.

Installing SAFEQ Cloud

1. When prompted to start the installation process, press **y**.
2. Enter your password to start the wizard with elevated privileges. Follow the instructions in the wizard. During the installation, you will be asked to:
   a. Change the keyboard layout.
   b. Customize the complete hostname in **FQDN** form (e.g., `appliance-01.acme.com`).
   c. Customize the network settings. For example, change to a static IP address.

      ⚠ Do not change the network profile name.

   d. Customize the Time Zone.
3. When the SAFEQ Cloud installer opens:
   - Read and accept the license agreement.
   - Accept the installation directory.
   - Select the role of the server – in this case **Extra secondary server for existing vendor or customer installation**.
4. When prompted for **Connection details**, provide the required information for the primary server address and account name.

You can see these in **Customer information** in SAFEQ Cloud Web UI.

5. Accept to autostart all services and complete the installation.

Firewall ports will be updated automatically.

At the end of the installation, you will be presented with instructions on how to use the **Cockpit** admin tool.

Optional recommended post-installation tasks

Connect to the appliance via an SSH client with the username **admin** and your password.

If you did not set a static IP address during installation, change the network settings as follows:

```
$ sudo nmtui
```

To change the keyboard layout:

1. To list all available keymaps:

   ```
   $ sudo localectl list-keymaps
   ```

2. To temporarily change the system's keymap, for example, to 'English UK keyboard':

   ```
   $ sudo loadkeys uk
   ```

3. To permanently change the system's keymap, for example, to 'English UK keyboard':

   ```
   $ sudo localectl set-keymap uk
   ```

Complementary Information

Automatic Updates with DNF Automatic

This virtual appliance uses DNF Automatic to apply the latest security patches and package updates on a daily basis.

Understanding Mirrors and the Impact of Blocking Them

Rocky Linux uses a network of **mirrors** to distribute packages and updates efficiently. When you run a command like `dnf update`, your system fetches packages from one of these mirrors—public servers that host copies of the Rocky Linux repositories.

Mirrors are geographically distributed servers that host identical copies of official Rocky Linux repositories: https://mirrors.rockylinux.org/mirrormanager/mirrors

DNF automatically selects a mirror (usually the fastest or nearest).
This system improves download speeds, reduces load on individual servers, and provides redundancy.

If your system cannot reach the mirrors (e.g. due to firewall rules, proxy restrictions, or DNS blocks), you may experience:

- Failed package installations or updates
- DNF timeouts or errors like `Cannot find a valid baseurl`
- DNF automatic failing silently or logging update errors
- Delays while DNF retries alternative mirrors

This affects both manual package management (`dnf install`, `dnf update`) and automated updates via DNF Automatic.

External URL Requirement for Installation

During installation, the virtual appliance connects to the following URL to download the SAFEQ Cloud installation binary:

https://cdn.everyoneprint.com/updatecatalog.json

This URL hosts the update catalog, which provides metadata and download links for the latest version of the SAFEQ Cloud. The installation wizard retrieves this catalog to:

- Determine the latest available version
- Download the correct installer file
- Ensure compatibility and integrity before proceeding

Web-Based Management with Cockpit

This virtual appliance includes Cockpit, a modern web-based interface for managing Linux systems. It is enabled by default for easy system monitoring and administration.

Accessing Cockpit

Once the appliance is powered on and connected to the network, you can access Cockpit by navigating to:

`https://<appliance-ip>:9090`

- Replace `<appliance-ip>` with the actual IP address of the appliance.
- You'll need to log in using a valid system user account (typically `root` or an admin user).
- The connection is secured via HTTPS.

Features of Cockpit

Cockpit provides access to:

- System logs and journal

- Storage and disk usage
- Networking status
- Running services and systemd units
- Terminal access
- Software updates

Disabling Cockpit

If you prefer to manage the system only via SSH or other methods, you can disable Cockpit with the following command:

```
systemctl disable --now cockpit.socket
```

To re-enable it later:

```
systemctl enable --now cockpit.socket
```

Installation log

During the setup process, all actions performed by the installation script are logged for transparency and troubleshooting purposes.

The log file is automatically created at:

```
/home/admin/install_script_<date>.log
```

SSH clients

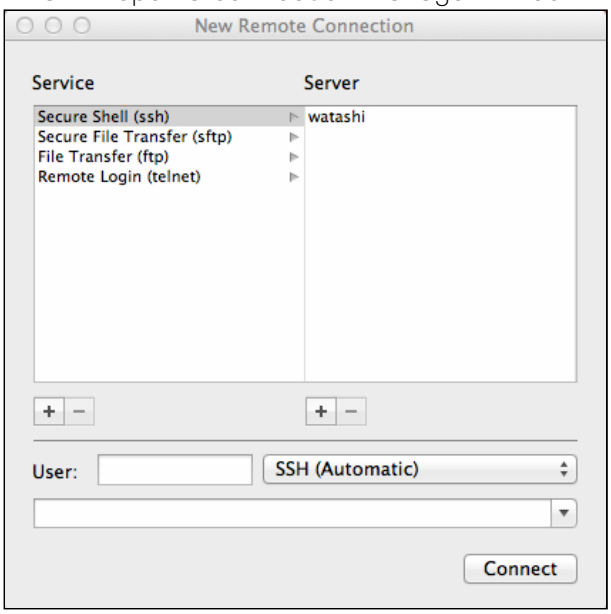
Windows:

- PuTTY: Download PuTTY
- MobaXterm: Download MobaXterm

macOS:

1. Launch the Terminal app.
2. From the menu, select Shell > New Remote Connection.

3. This will open a connection manager window.

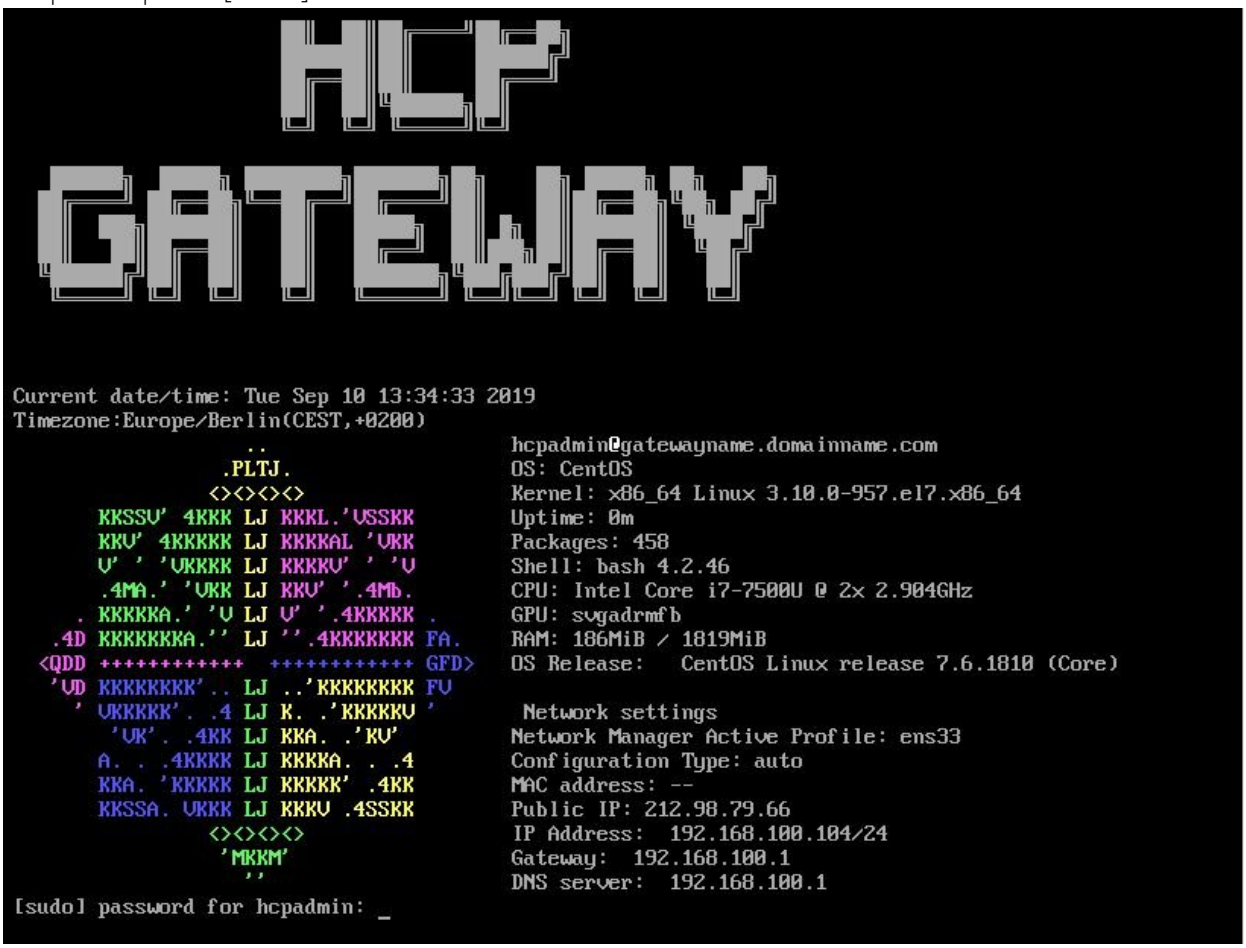


8.3.7 CONFIGURING A PRE-CONFIGURED GATEWAY

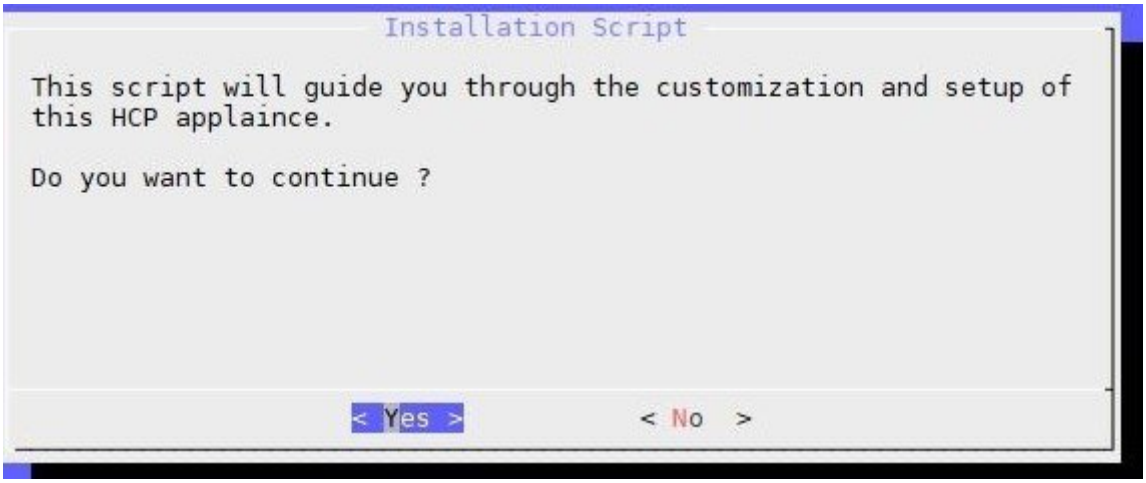
Instructions for installing and configuring a preconfigured gateway bought from Y Soft.

- Connect Ethernet, Power, Keyboard, Mouse (optional) and Screen to the gateway and turn it on.
- Log in using *hcpadmin* / *eop* as login / password.

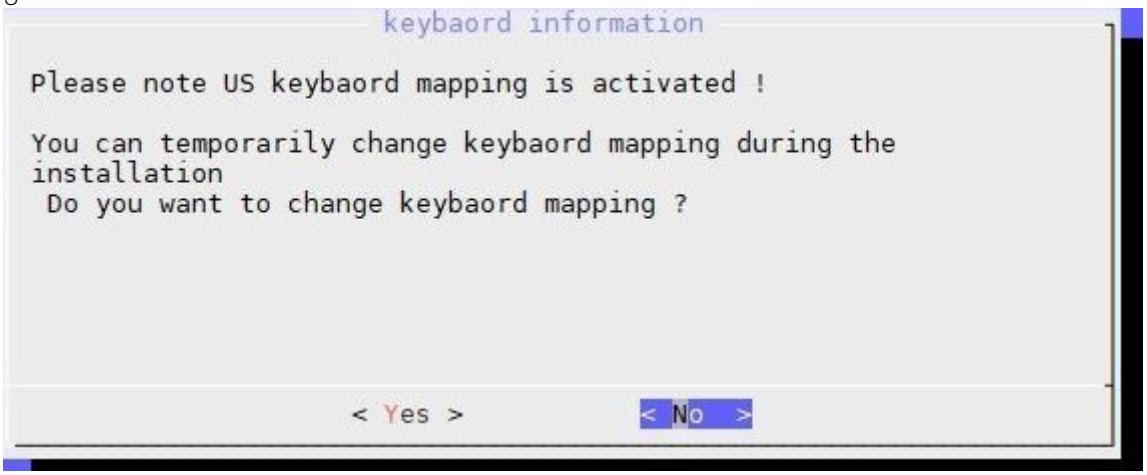
- Enter *eop* password again at the prompt to elevate privileges (sudo) for the guided install script and press [Enter] to launch it.



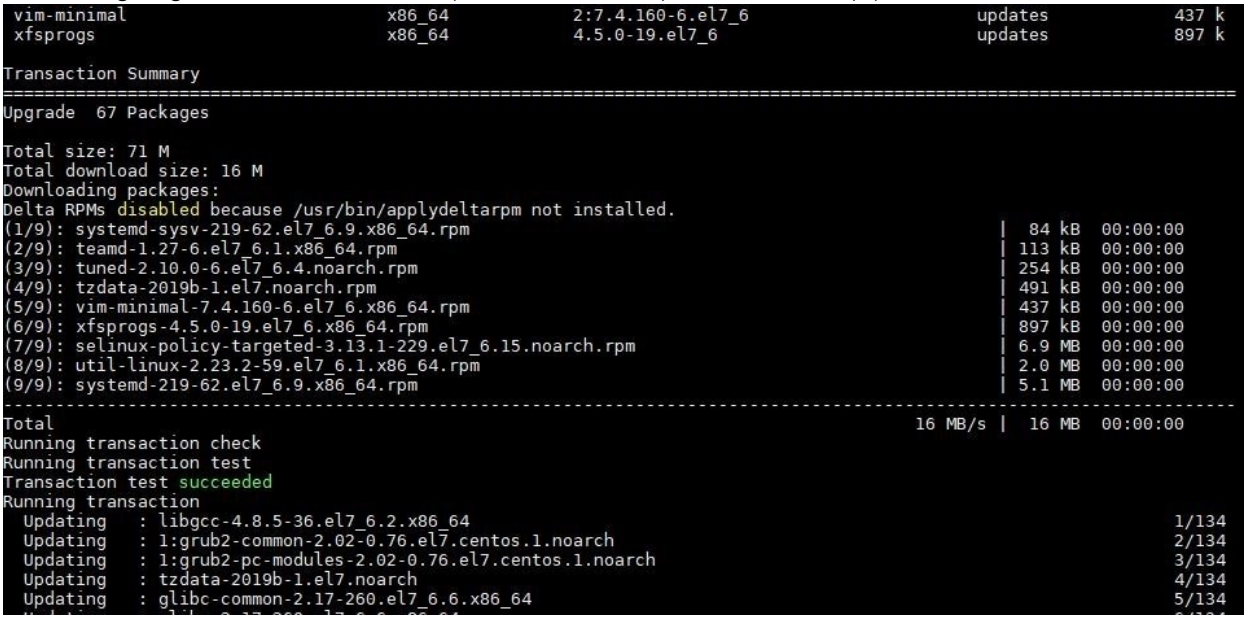
- Click "Yes" to start the installer-script.



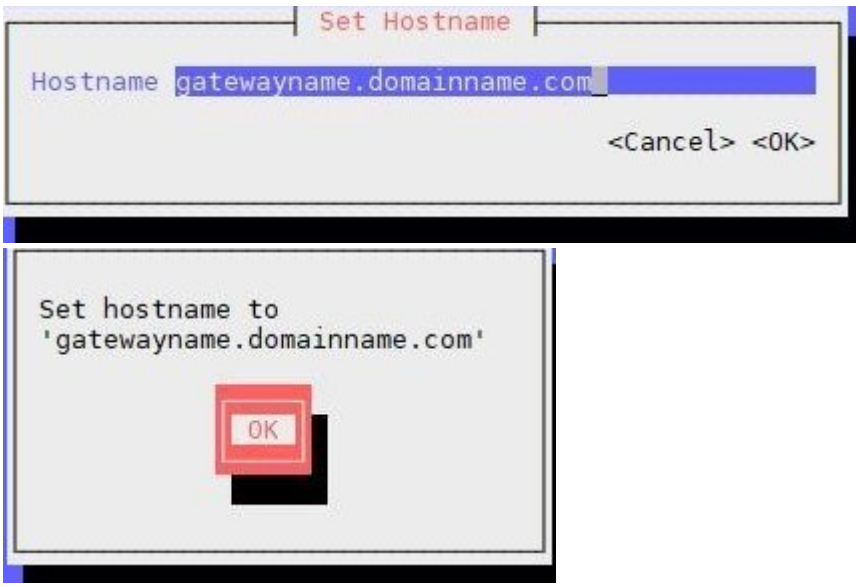
- Click "No" to keep the default keyboard layout, otherwise click "Yes" and follow the steps guided.



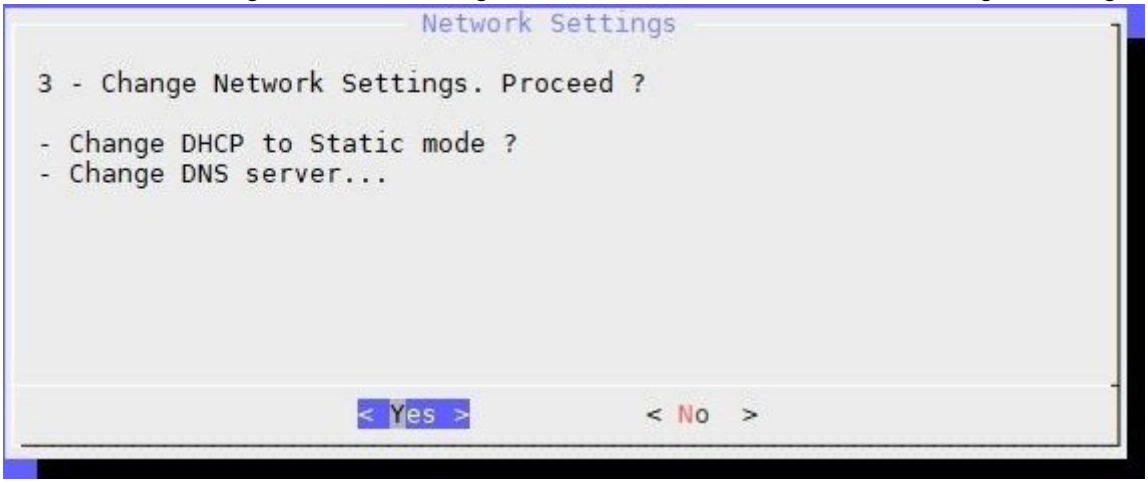
- CentOS is updated with all the latest patches and updates. This will make sure that SAFEQ Cloud is going to be installed on top of latest Rocky Linux security patches and kernel fixes.



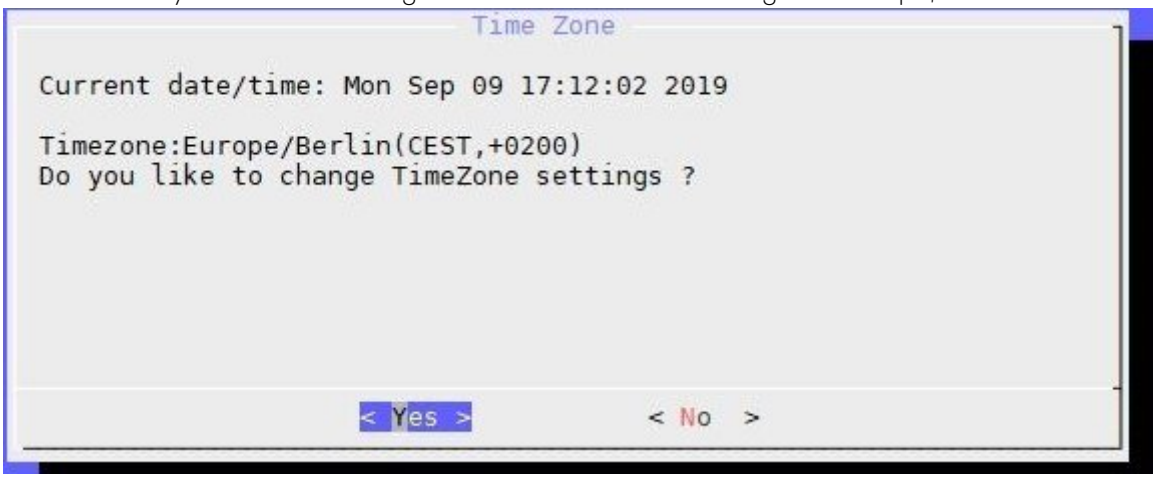
- Click "Ok" to customize the Hostname of the Gateway, please use FQDN provided by customer when DNS-setup is used.



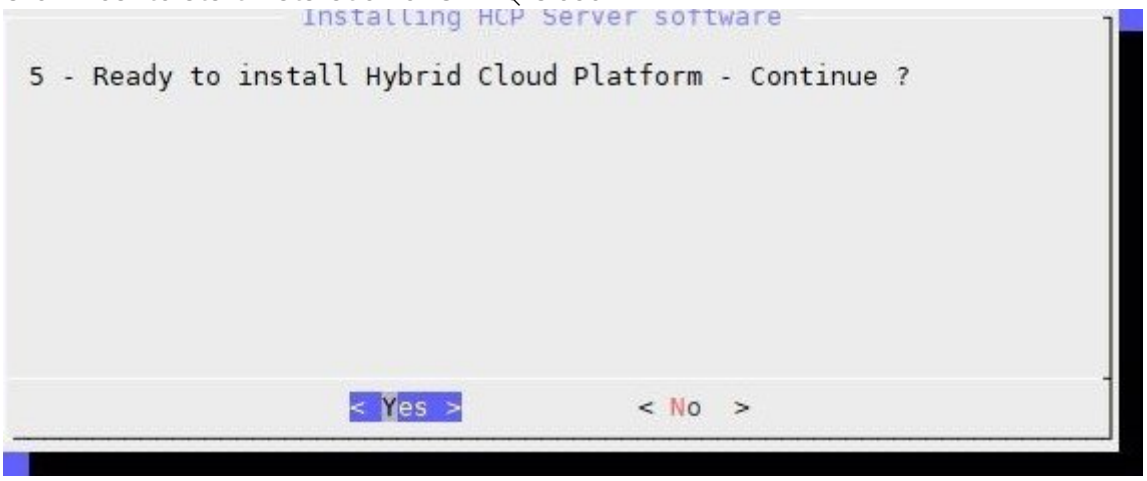
- Click "Yes" to change network-settings (Static IP, DNS etc.) or "No" if nothing to change.



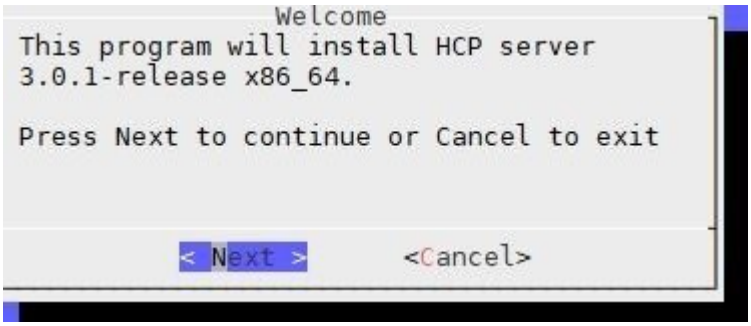
- Click "Yes" if you want to change timezone and follow the guided steps, otherwise click "No".



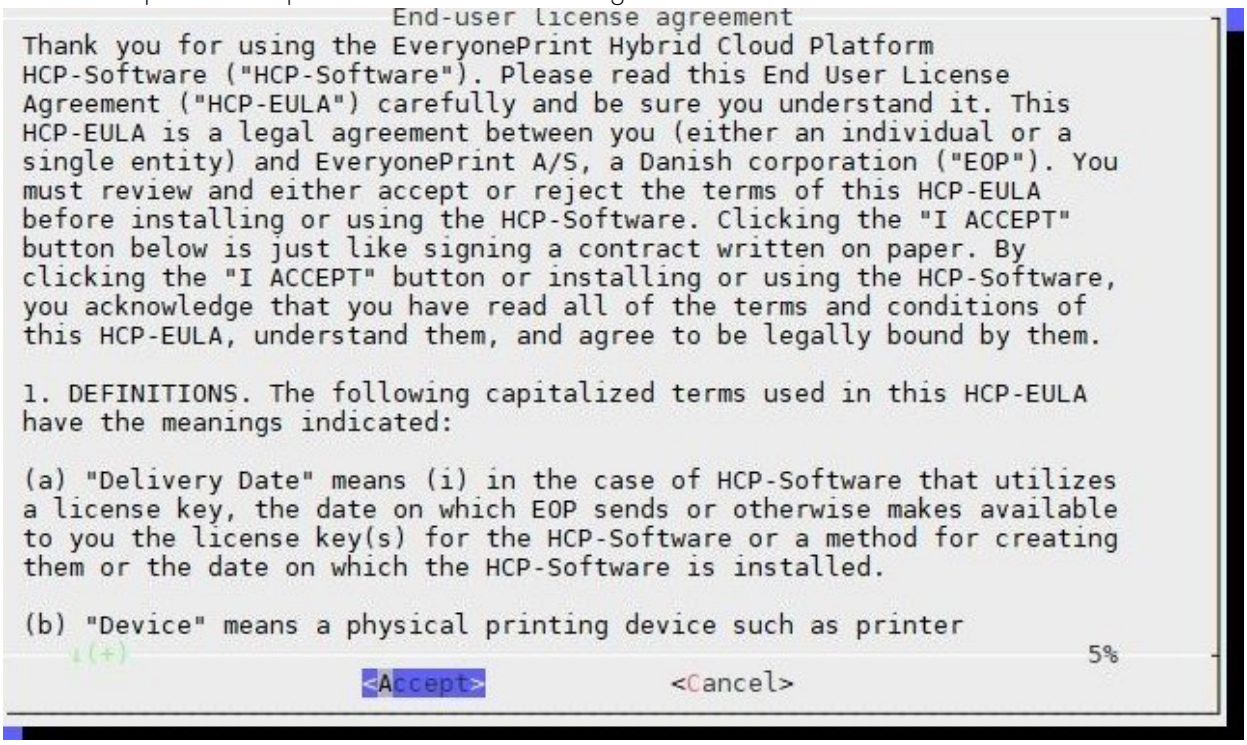
- Click "Yes" to start installation of SAFEQ Cloud.



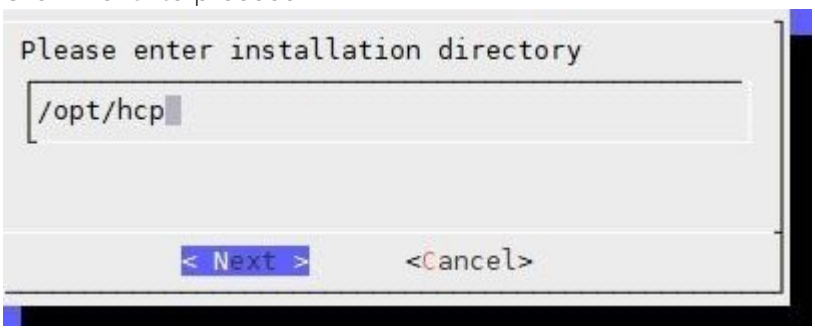
- Click "Next" to continue.



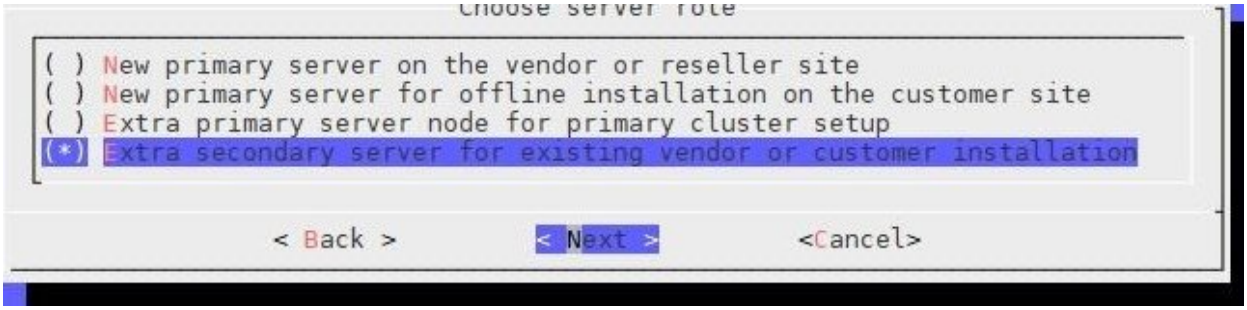
- Click "Accept" to accept the End-user license agreement.



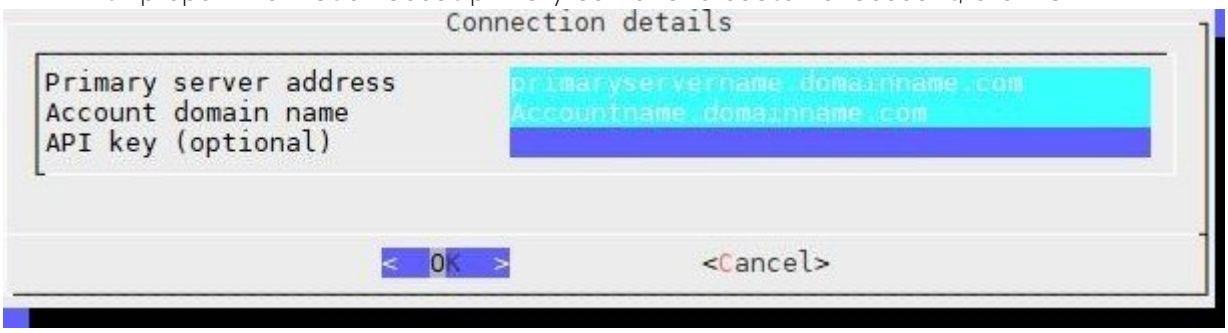
- Click "Next" to proceed.



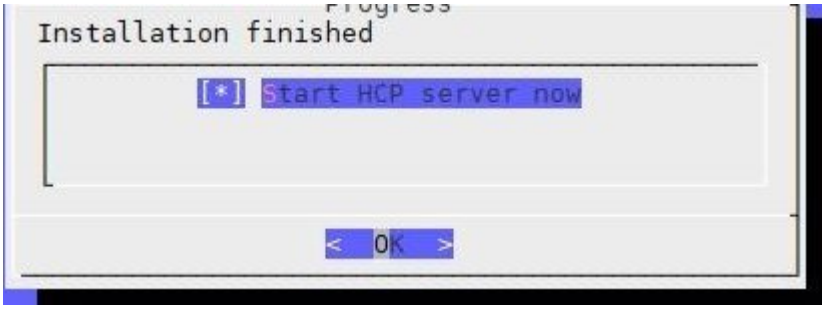
- Select "Extra secondary server for existing vendor or customer installation" by marking the line, hit "Space" (make sure the * is moved to the selection) and then click "Next".



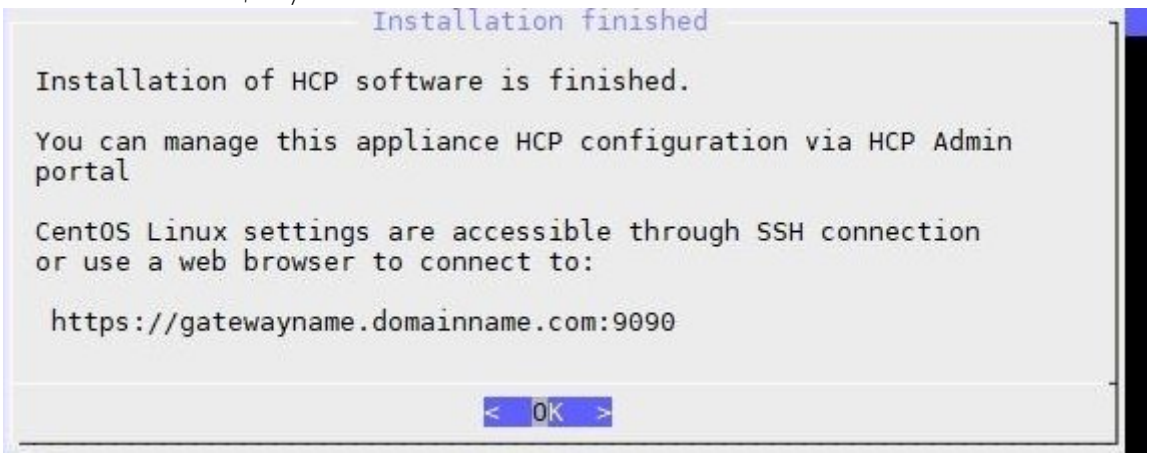
- Fill in with proper information about primary server and customer-account, click "Ok".



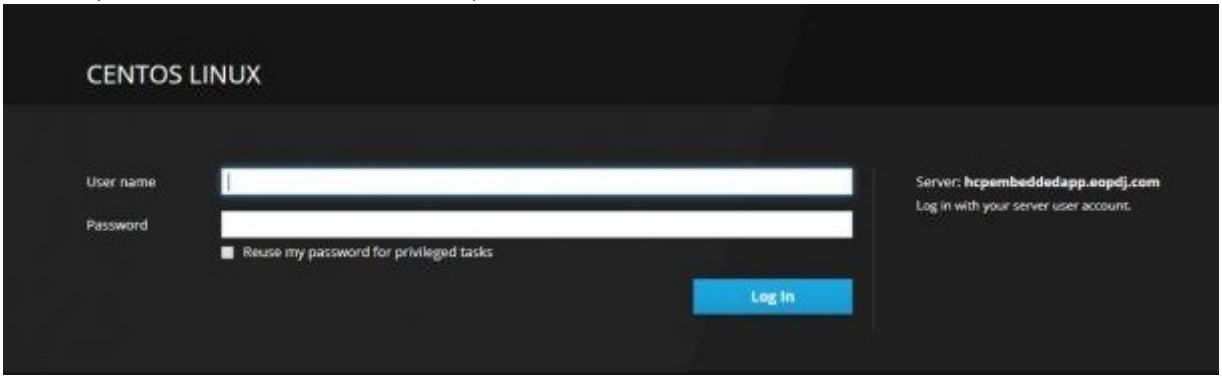
- Click "Ok" to start SAFEQ Cloud-Service. Firewall-rules will now be updated and the Gateway will start up.



- When Installation is finished, click "Ok" ; then type 'exit' at the prompt to logout, then you can disconnect screen, keyboard and mouse.



- The link provided in the last picture will give you access to *Cockpit*, a graphical web dashboard, where you can control CentOS setup and health status.



Please remember to update the gateway to the latest version of SAFEQ Cloud prior to authorizing, mapping and adding services to the gateway to the Account in the Portal.

- The gateway is scheduled to run an automatic update to ensure all security fixes are applied on a monthly basis.
- New kernel updates to the underlying OS are not updated. These need to be managed directly as some will require a the gateway to be rebooted.

- Please ensure hardware gateways are added into standard change management processes to ensure updates required by the end-user are applied.

8.4 SAFEQ CLOUD CHROME EXTENSION

READY FOR REVIEW

8.4.1 OVERVIEW

SAFEQ Cloud Chrome Extension is an extension that can be installed on Chromebook devices or in the Chrome browser.

It has the following features:

- Authentication using Chromebook user email address with the SAFEQ Cloud server.
- Sync with the SAFEQ Cloud printers
- Ability to send print jobs to Direct print queues and to Pull print queues

8.4.2 SYSTEM REQUIREMENTS

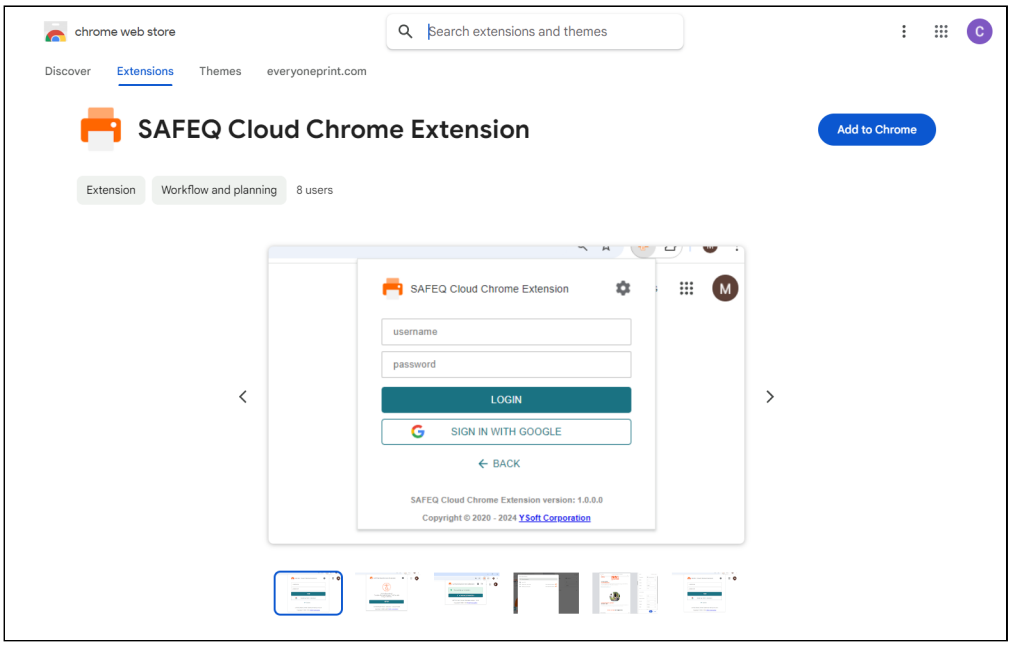
- Chrome version 44 and higher.
- Users must be logged in Chrome Browser and have Sync ON.
- A valid certificate must be installed on the SAFEQ Cloud server.

8.4.3 INSTALLATION

From Chrome Web Store

1. Go to Chrome Web Store using this link.
2. Search for SAFEQ Cloud Chrome Extension.

3. Click Add to Chrome.



From Google Admin Console

Google Admin Console could be used for centralized distribution inside organization and preconfiguration of settings. See section *Configuring the extension remotely in Google Admin Console* of this guide.

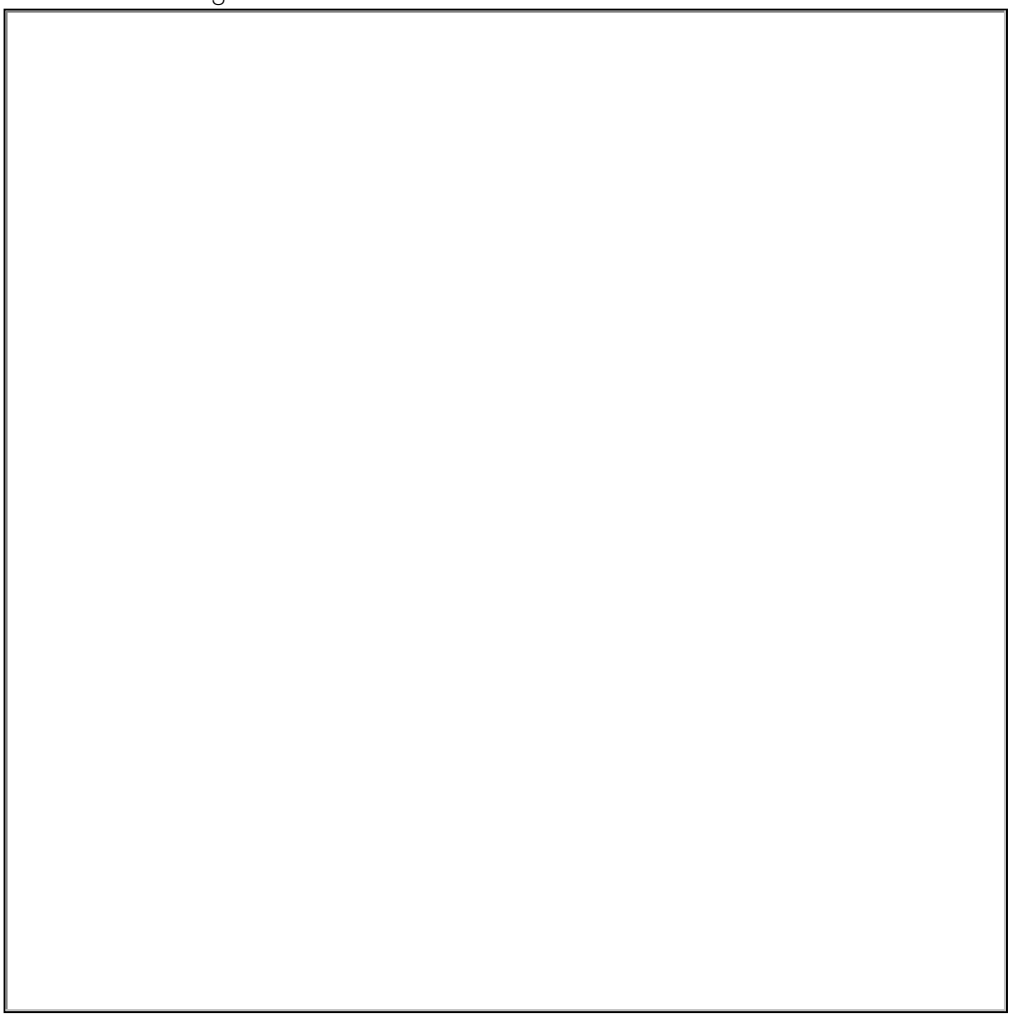
8.4.4 CONFIGURATION

To use the extension, you must configure a signing certificate in SAFEQ Cloud Web UI. After that you, you can configure the extension individually in Chrome, or remotely in Google Admin Console in order to apply the settings to all users in your organization.

Configuring the signing certificate in SAFEQ Cloud Web UI

1. Log in to SAFEQ Cloud Web UI.
2. Go to Security > Security options, tab General and section PKI and encryption.

3. In Signing certificate, select the token signing certificate. Note that it may take a few minutes before the change takes effect.

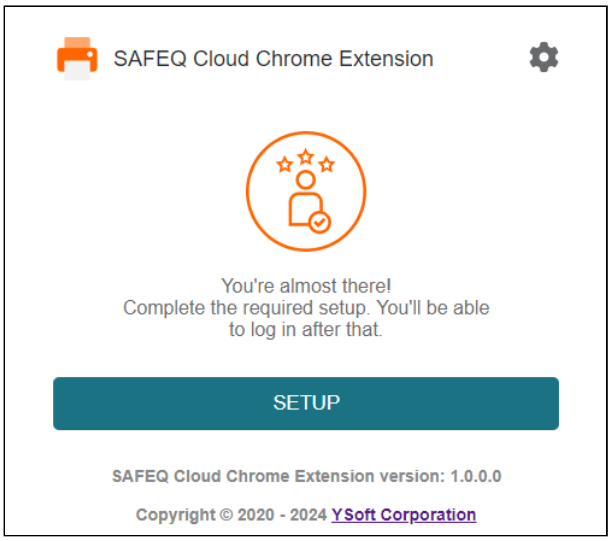


4. Click Save.

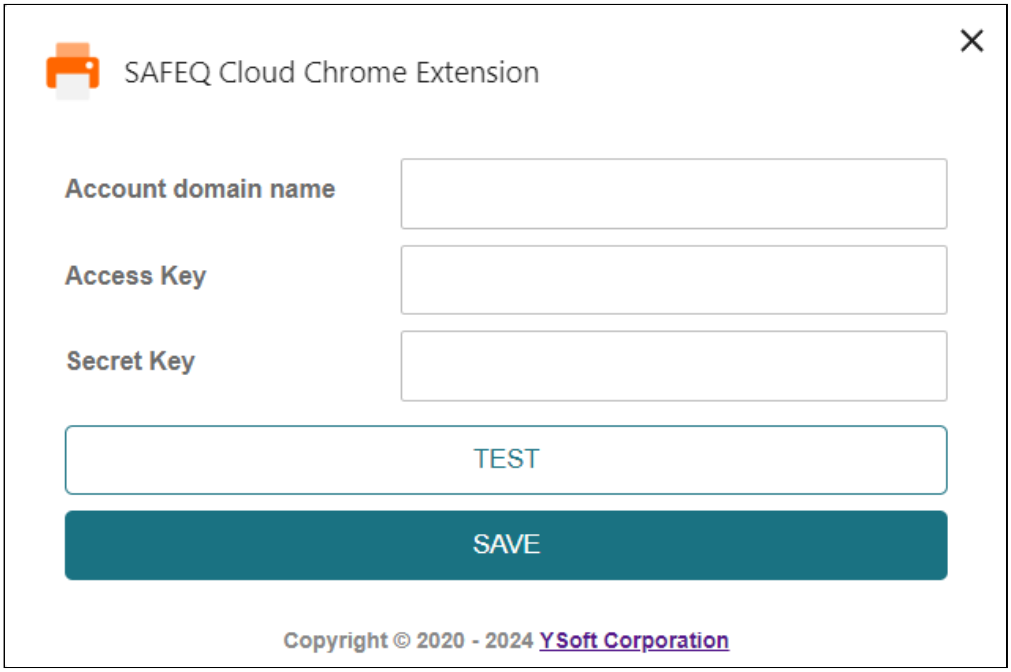
Configuring the extension in Chrome

1. Have your SAFEQ Cloud domain at hand. You can find the domain name in Settings > Customer account in the SAFEQ Cloud Web UI.
2. If you haven't generated an API access key for the Chrome extension yet, follow the instructions in API access keys and choose the Chrome extension type of key when creating it.

3. Left-click the extension button and then click the cogwheel icon to open the settings.



4. On the following screen, enter your SAFEQ Cloud account domain name. Note that this URL must be accessible for you from the browser (you may need to accept the certificate for it).



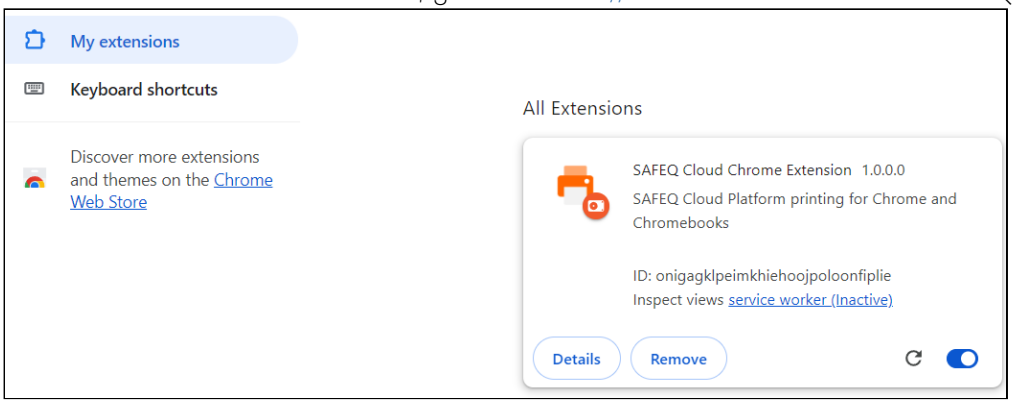
5. In **Access Key**, fill in your API access key for the Chrome extension.
6. If authentication is disabled, fill in the secret key from the G Suite OAuth2 identity provider (if set).
7. Check the connection by clicking **Test**.
8. If successful, click **Save**.
9. If unsuccessful, check whether you have entered the correct domain and API key, then click **Test** again.

Logging in

See Using the SAFEQ Cloud extension for Chrome.

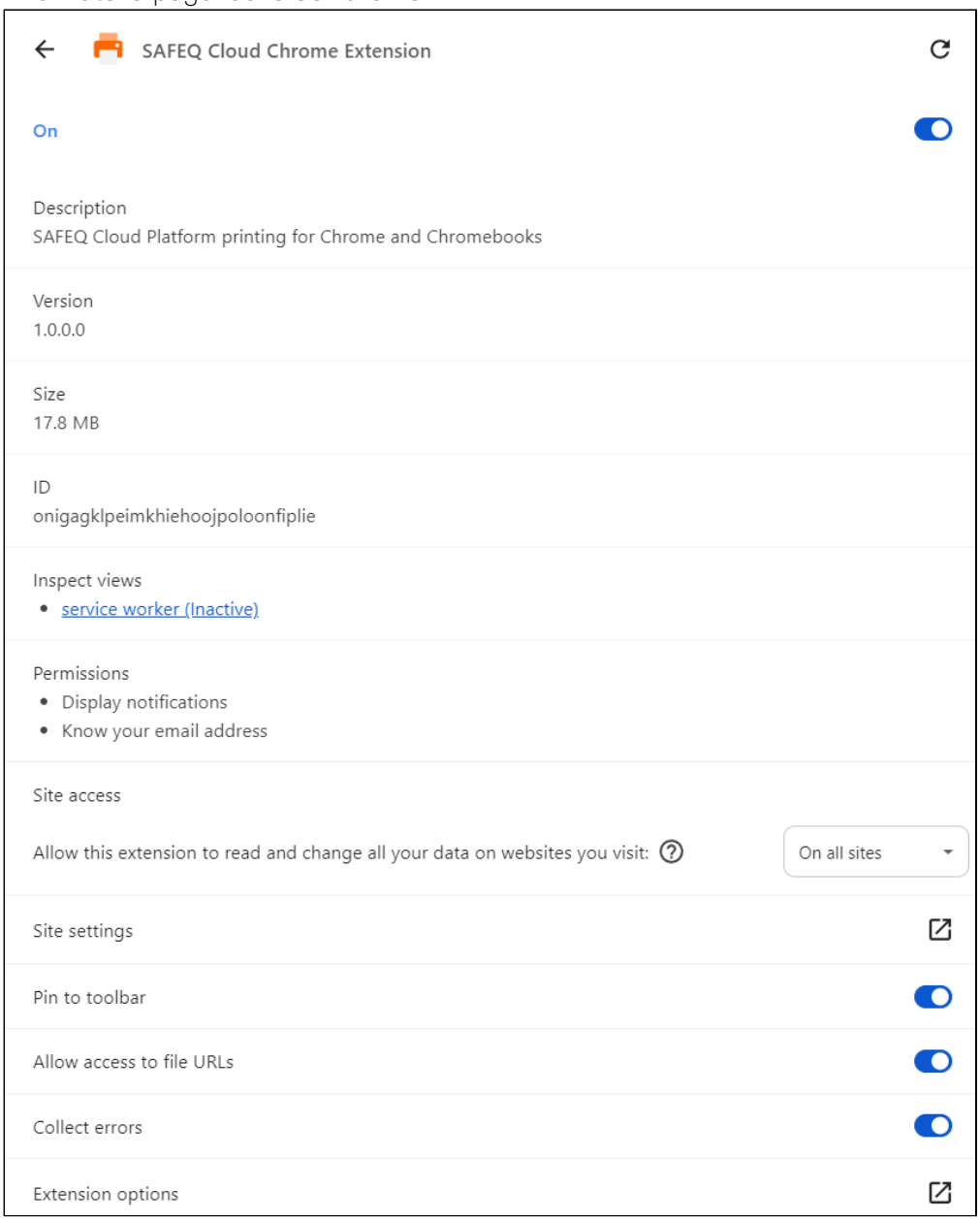
Details about the extension in Chrome

1. To see info about the extension, go to chrome://extension and find the SAFEQ Cloud extension.

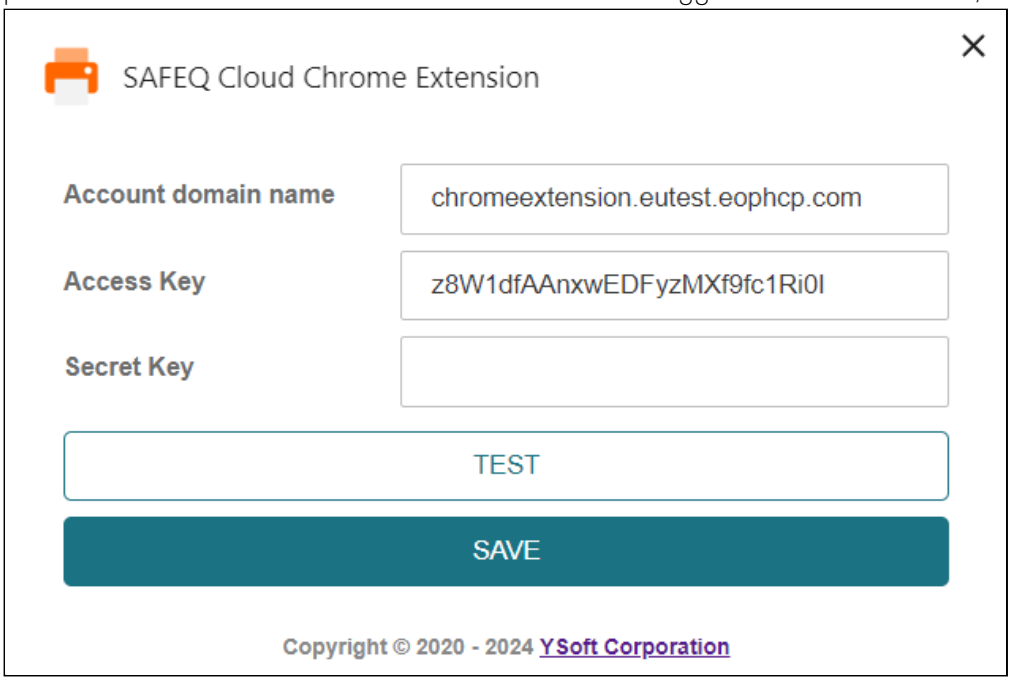


- **Details** - Opens a page with information about the extension.
- **Remove** - Removes the extension from Chrome browser.
- The toggle enables/disables the extension.
- The refresh icon updates the extension to a new version (if there is any).

2. The Details page looks as follows:



3. Click **Extension options** to open the Extension options page. Note that this extension asks for permission to know the email address of the user logged in to Chromebook/Chrome browser.



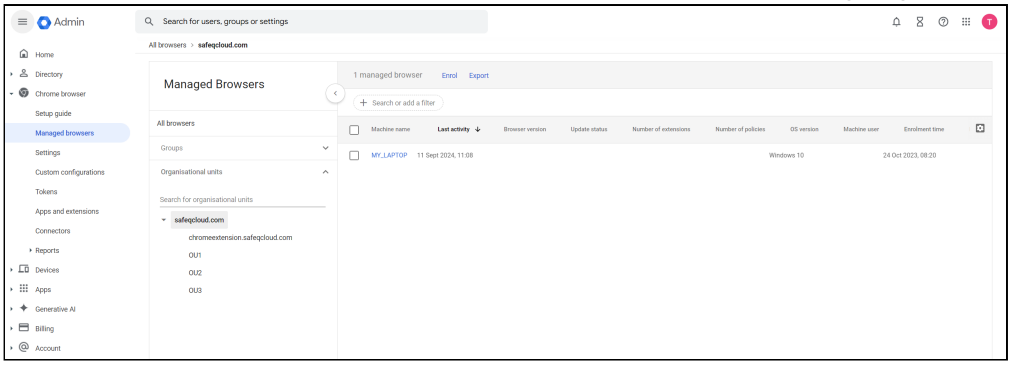
- **Account domain name** - The domain name of your SAFEQ Cloud account.
- **Access Key** - The API key used in the communication with the SAFEQ Cloud server.
- **Test** - Tests the connection to the SAFEQ Cloud server.
- **Save** - Saves the settings.

4. For using the extension, see Using the SAFEQ Cloud Chrome Extension.

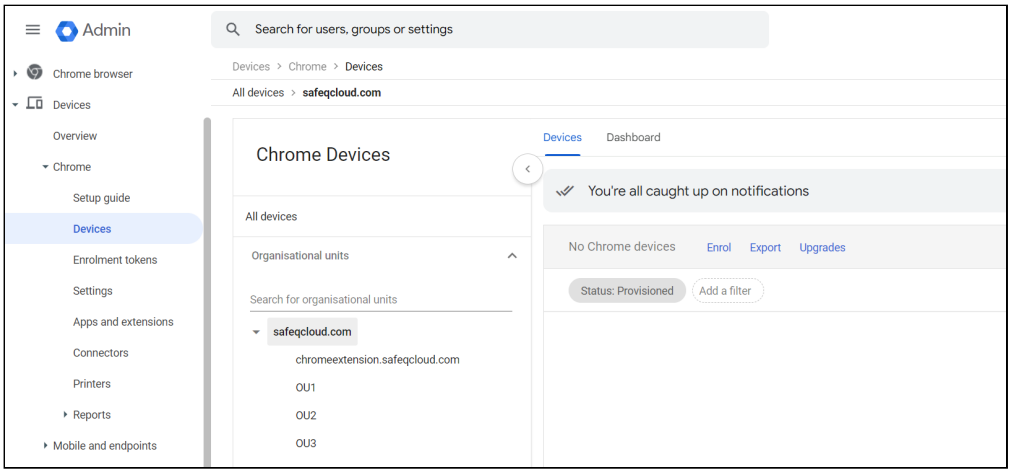
Configuring the extension remotely in Google Admin Console

If you wish to configure and distribute the extension across the devices in your organization remotely, perform the following steps:

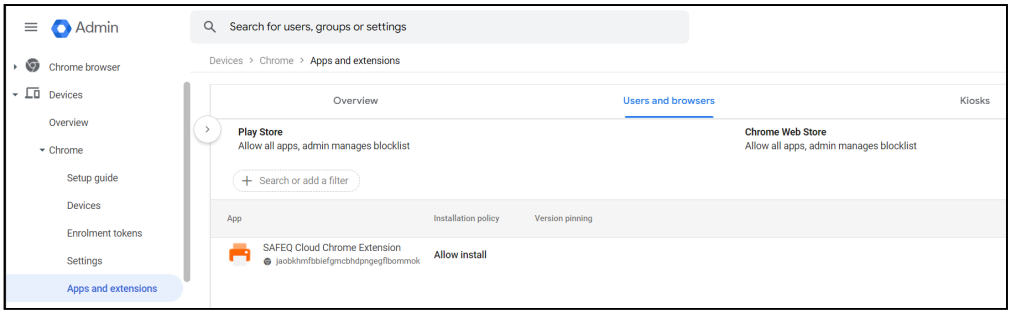
1. Log in to Google Admin Console.
2. Go to **Managed browsers** and check that all needed user browsers are enrolled and listed in the table. If not, enroll the required browsers in the corresponding Organizational Unit.



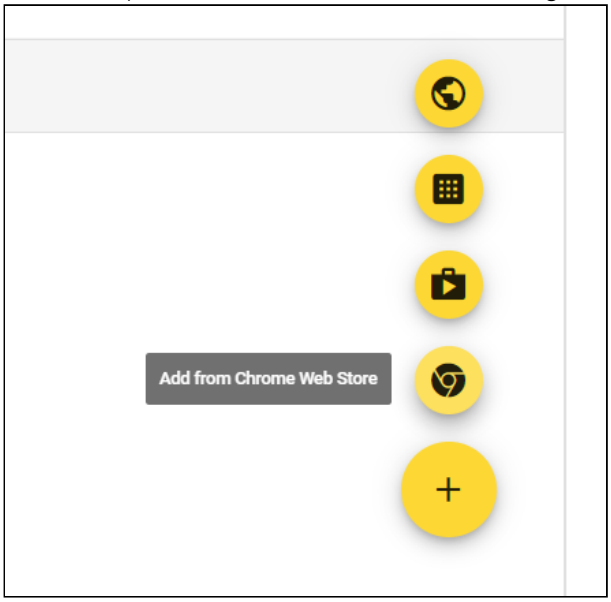
3. Go to the **Devices** and check that all required Chromebook devices are enrolled and in **Provisioned** status.



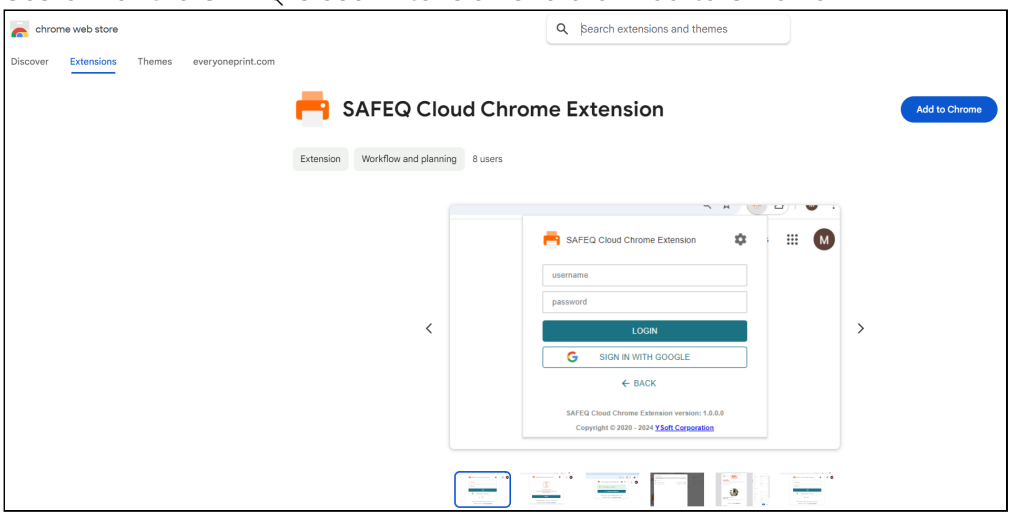
4. Go to **Apps & extensions** and click the **Users and browsers** tab.



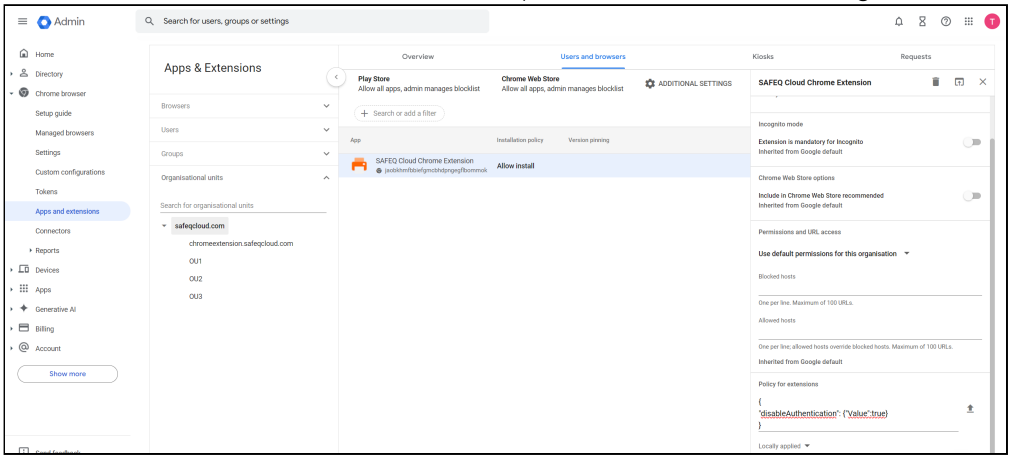
5. Click the yellow **+** button on the bottom right corner and select **Add from Chrome Web Store**.



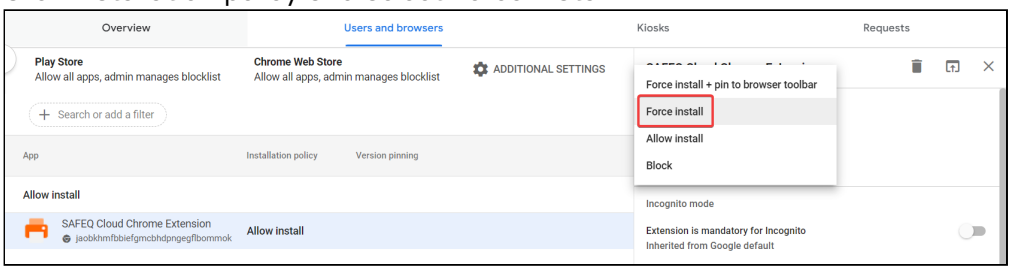
6. Search for the SAFEQ Cloud Extension and click **Add to Chrome**.



7. Click the extension in the list. This will open a new menu on the right side of the screen.



8. Click **Installation policy** and select **Force install**.



9. Scroll down and click **Policy for extensions**.

10. Enter configuration JSON with correct values in this form:

```
{
"hostname": {"Value":"accountdomainname"},
"port": {"Value":"port"},
"apikey": {"Value":"apikeyvalue"},
"disableAuthentication": {"Value":false|true},
"secret": {"Value": "secretkeyvalue"}
}
```

- `hostname` – Your SAFEQ Cloud account domain name.
- `port` – Not required. Note: If port value is null, enter "". Otherwise, enter the value without quotation marks.
- `apikey` – The API key value for the default Google Chrome API key in SAFEQ Cloud (Note: this can be set to a custom string if required). For EveryonePrint Mobile Print, this is not required.
- `disableAuthentication` – If set to `False`, the extension will require the user to log in. If set to `True`, the extension will be set to bypass the login and authenticate the user by email only.

  If "disableAuthentication" is set to true, the default Chrome Extension API key permissions must have "Allow untrusted endpoints" set. This means that the API key could be used to submit jobs on behalf of other users. If so, we also recommend setting the "secret" to enhance security. Only set this flag to true if this risk is acceptable.
- `secret` – G Suite OAuth2 identity provider secret key (if set).

9 END USER GUIDE

This section contains:

- various ways of Submitting a print job into YSoft SAFEQ Cloud. What is available to you depends on how your administrator configured SAFEQ Cloud.
- how to use SAFEQ Cloud cloud terminals for several MFD brands. See Using an MFD.

9.1 SUBMITTING A PRINT JOB

This section describes the various ways in which you can send a print job to SAFEQ Cloud:

Via the SAFEQ Cloud Client.
Via the Mobile app.
Via the Chrome extension.
Via adding an IPP queue in Windows or Mac.

If you wish to print from SAP, you have two options:

1. Add an IPPS queue to your SAP server. See Adding IPP print queue manually in Windows.
2. Print from an SAP client installed on your PC. This way, the client will be able to print to any print queue available on your PC, such as the print queue(s) created by the SAFEQ Cloud Client.

9.1.1 USING THE SAFEQ CLOUD CLIENT

Overview

SAFEQ Cloud Client is a desktop application that can be installed on end-user workstations to automatically create print queues and install drivers based on the SAFEQ Cloud server configuration for your company.

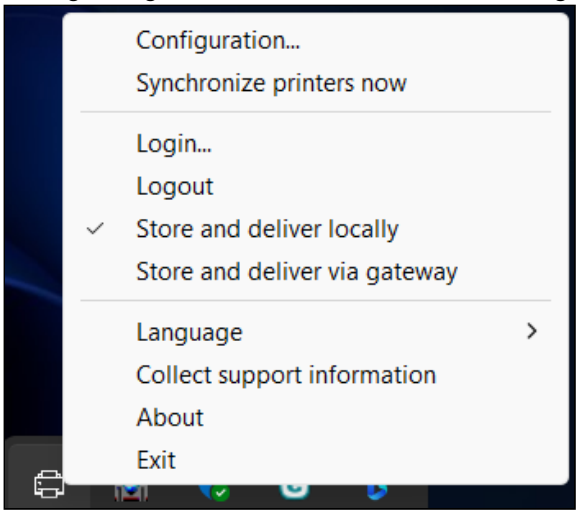
The installation can be done remotely by your administrator. When the Client is installed on your PC, you will see its icon in your system tray. The icon indicates its current operational state:

- – idle state, connected to SAFEQ Cloud server
- – error state, no connection to background service (it is stopped or not functioning correctly)
- – SAFEQ Cloud Client is not logged in
- – synchronization is currently in progress
- – offline operation, no connection to SAFEQ Cloud Server

SAFEQ Cloud Client will perform printer synchronization automatically based on its synchronization settings. You can also trigger manual synchronization by right-clicking the taskbar icon and choosing Synchronize printers now menu item.

Logging in

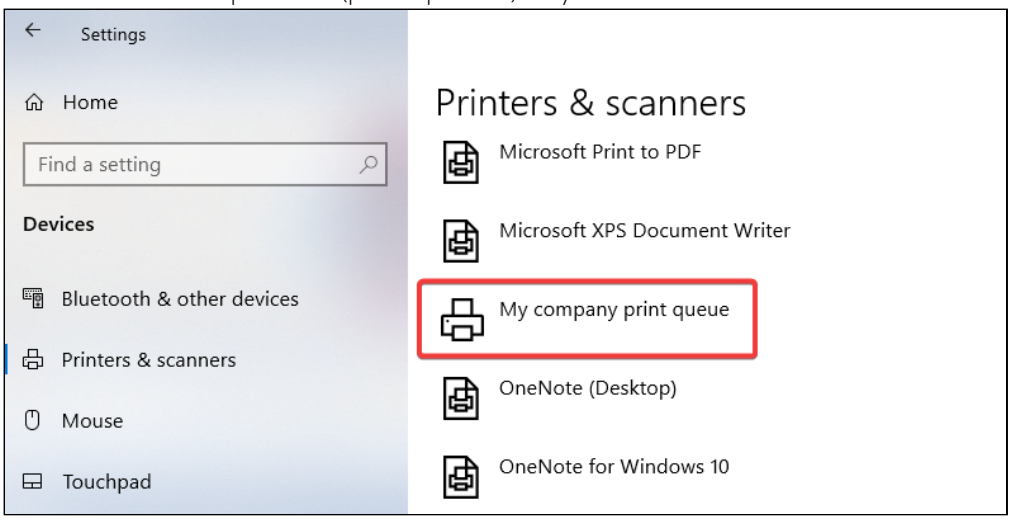
1. To log in, right-click the icon, and select Login.



2. Depending on how your administrator has set up the Client, you will either be prompted to enter your credentials in the Client itself, or you will be directed to a login page in your browser where you will be asked to log in with your external identity provider account, such Microsoft, Google, or Ping.

3. You will see a pop-up window with a login success message.

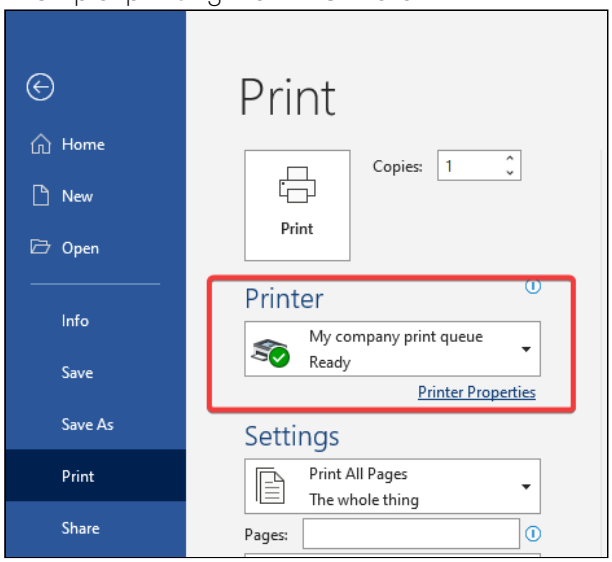
4. You will see new printers (print queues) in your Windows or Mac OS.



Submitting print jobs

You will see all print queues (printers) that your administrator made available to you in your operating system. Select one of the queues in the print dialogue when printing a document from your chosen application.

Example: printing from MS Word:



If you choose a finishing option, e.g. stapling, that is not supported on the MFD where you will release the print job, the print job will be printed without that option.

9.1.2 USING THE MOBILE APP

With the SAFEQ Cloud mobile app you can submit documents for print. Upload documents directly from the app or via a share extension and share menu on iOS and Android respectively. Also you can select the desired finishing options before job submission.

Limitations

- You can use the app to release print jobs only at MFDs that are accessible from a primary or secondary (gateway) server.
- Scanning via the app is not supported.
- Bulk operations on the uploaded documents (except deletion) are not supported.
- Only PDF files are supported. You can submit PNG or JPG files, but be aware that these file formats are converted to A4-sized PDF pages. You can modify the page size later on in the finishing options. However, this won't scale the image from scratch, the app will use the pre-rendered A4 page.
- The app does not store page range as a preferred finishing option - the page range is initially set to all pages after you submit a file via the app.

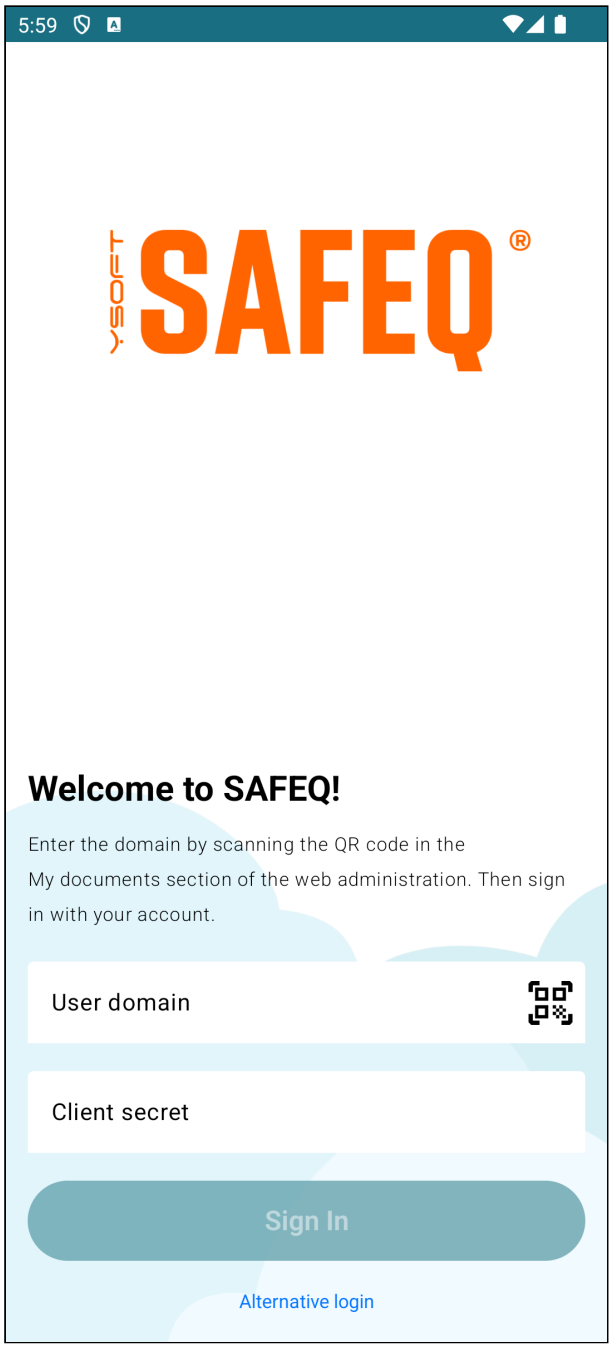
Using the Android Mobile app

Download the application from Google Play Store.

Logging in

1. After you start the application for the first time, you will see the login screen .
2. Enter the **User Domain**. You can enter it manually or by scanning the configuration QR code that you can find in SAFEQ Cloud Web UI.
3. Tap **Sign in** and enter your SAFEQ Cloud username and password or use other login methods, for example via your Microsoft or Google account. The available login methods depend on how your administrator configured the app.

Alternatively, tap Alternative Login if your company uses, for example, a custom identity provider.

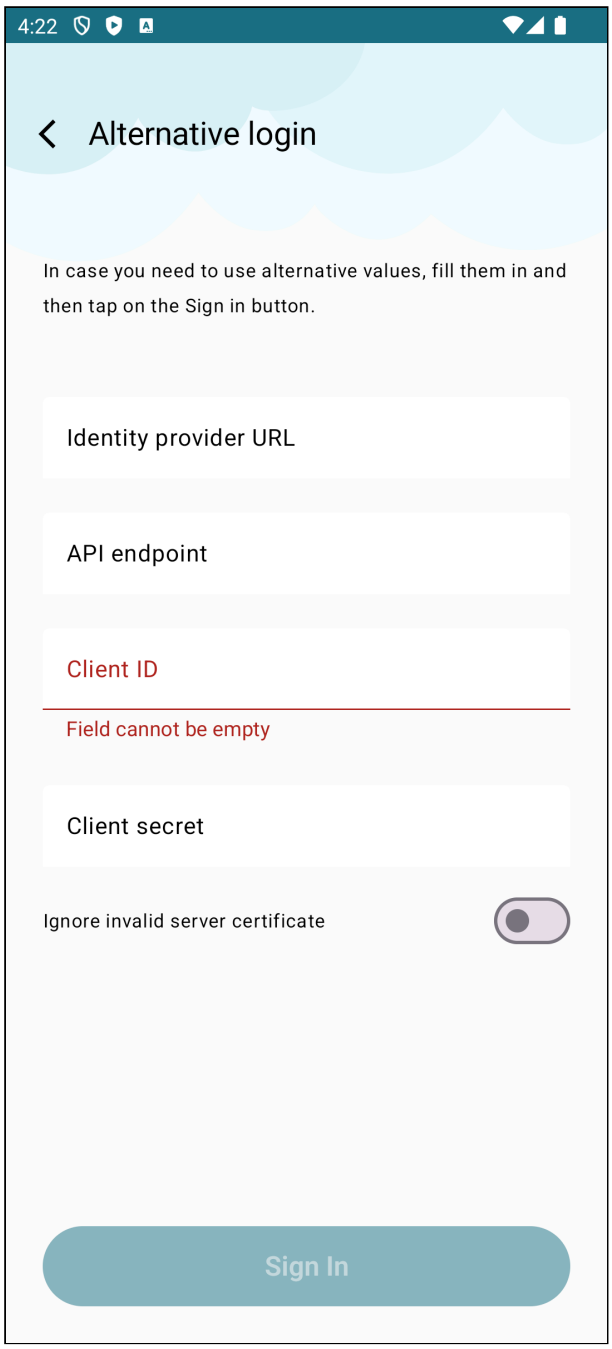


Alternate login

On the Alternate Login screen, enter the following:

- Identity provider URL – If a custom identity provider is deployed, provide the custom identity provider's URL. For a default deployment, enter the address and port of Job Service. For example, if the Job Service is deployed on a machine with hostname example.com, then the value is https://example.com:5000/.
- API endpoint – Use the address and the HTTPS port of Spooler, e.g. https://example.com:5002 .
- Client ID – Use the ClientId value specified in the identity provider. For a default deployment using Job Service as an identity provider, use *ClientId of Additional Clients* located in Job Service's local.json configuration file. The default value is mobile-application.
- Client Secret – Optional value of the API Key that authenticates the app.

You can enable communication that is not secured by TLS by using the toggle button.



Job list

After a successful login, you will see all of your documents.

Submitting print jobs

Supported formats

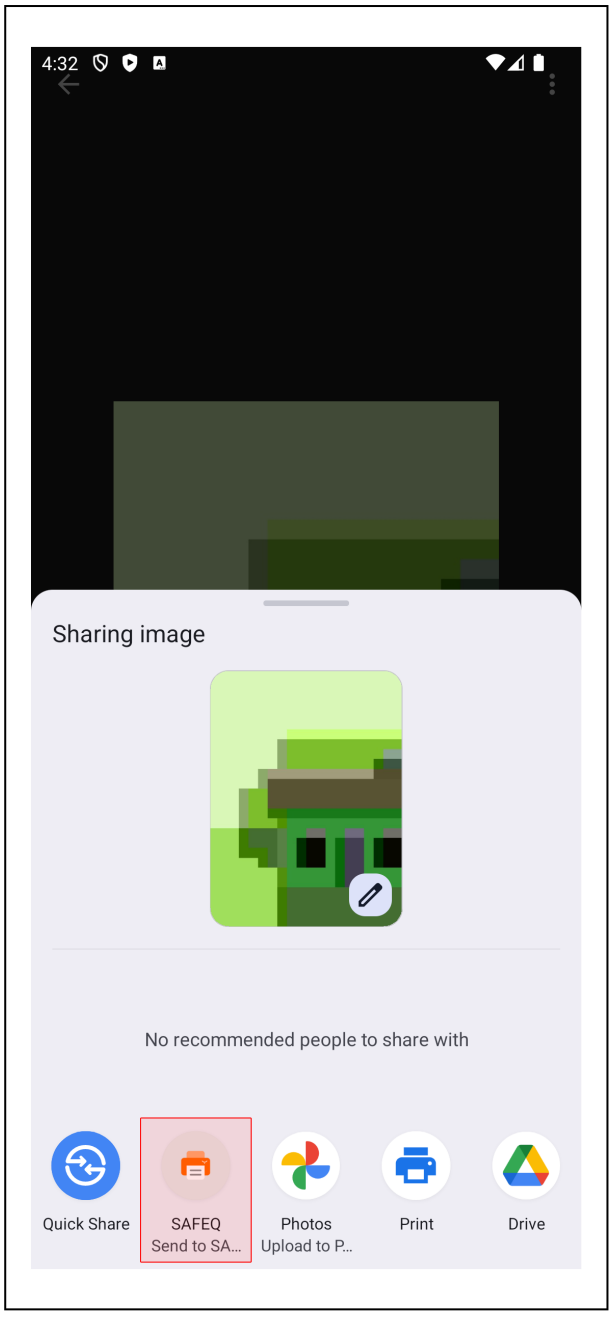
- BMP
- GIF
- HEIF
- JPEG
- PDF
- PNG
- WebP
- HTML

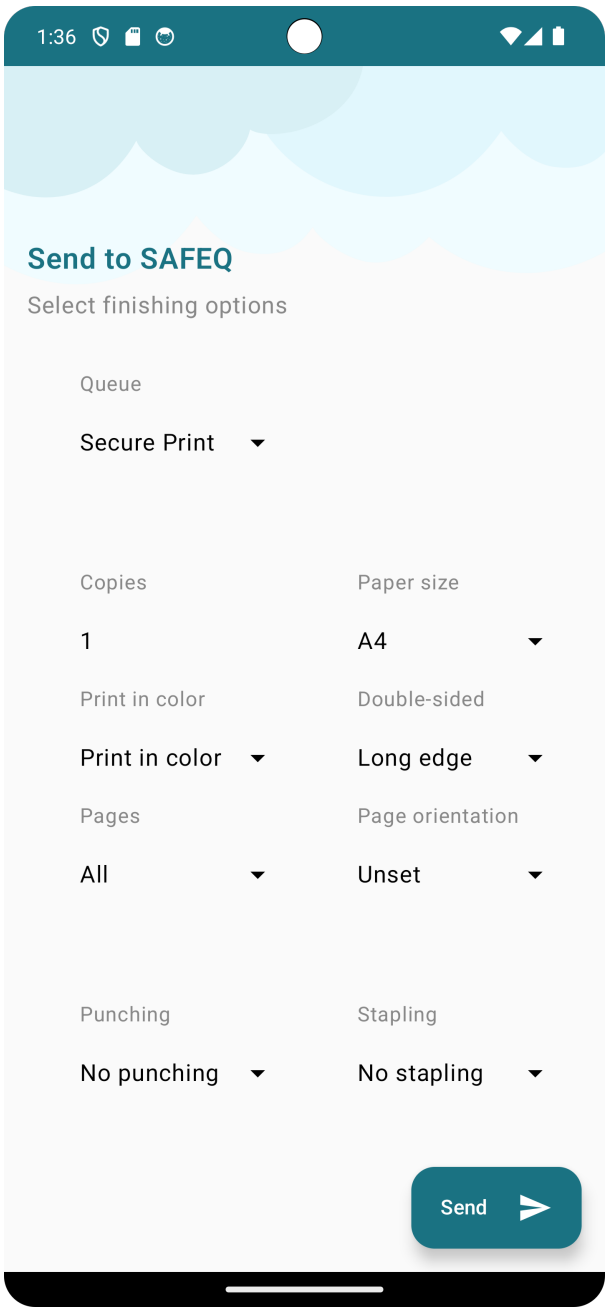
- Various forms of plain text

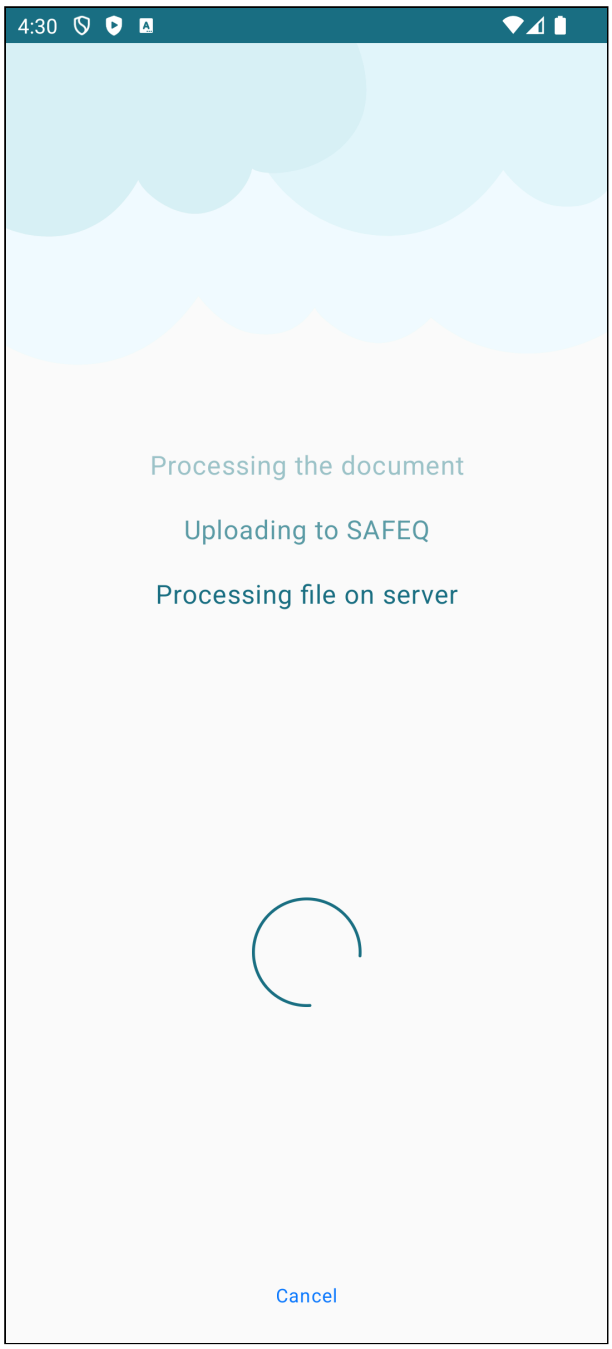
Submitting print jobs from the apps via the share menu

This method works with any application that supports printing.

1. Tap the share menu in the app from which you wish to print.
2. Tap the SAFEQ Cloud icon.
3. Modify the finishing options according to your needs. If the chosen file is protected by a password, a dialog box will prompt you to enter the password.
4. Tap **Send**.



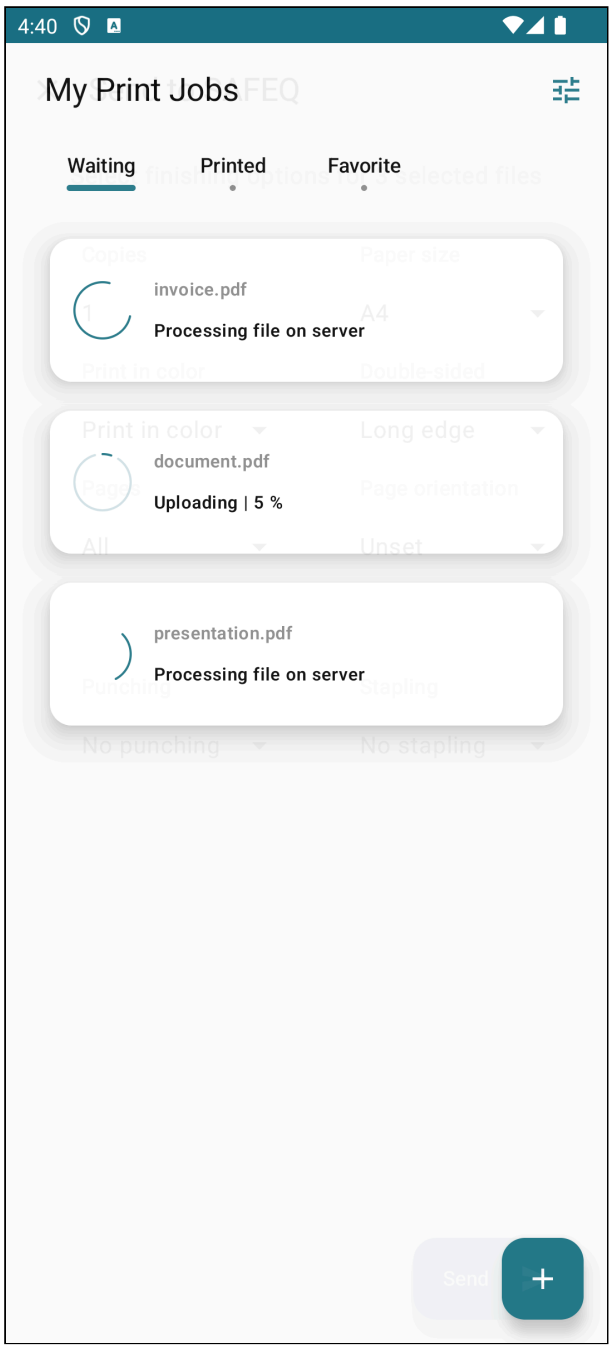

1:36
Send to SAFEQ
Select finishing options
Queue
Secure Print
Copies
1
Paper size
A4
Print in color
Print in color
Double-sided
Long edge
Pages
All
Page orientation
Unset
Punching
No punching
Stapling
No stapling
Send

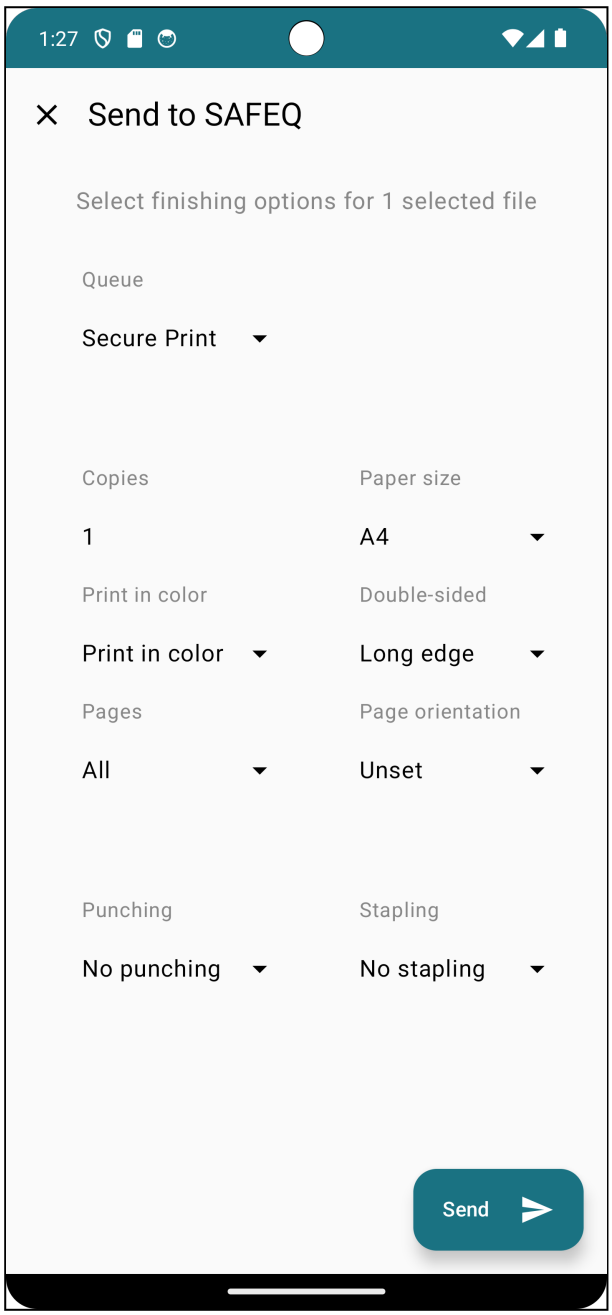


Note: Devices running Android 14 may not render the shadow in the file unlocking dialog.

Submitting print jobs directly from the app

1. To submit a new document, tap the plus button at the bottom of the Job List screen. This will open the standard system file picker.
2. Select one or more files. If any of the chosen files are password-protected, a dialog will appear prompting you to enter the password. You will have the option to skip those files you do not wish to unlock.
3. On the next screen, customize the finishing options (print queue, number of copies, color, page size, page orientation, and sides) according to your needs.
4. Tap **Send**.


4:40
My Print Jobs
Waiting
Printed
Favorite
invoice.pdf
Processing file on server
document.pdf
Uploading | 5 %
presentation.pdf
Processing file on server



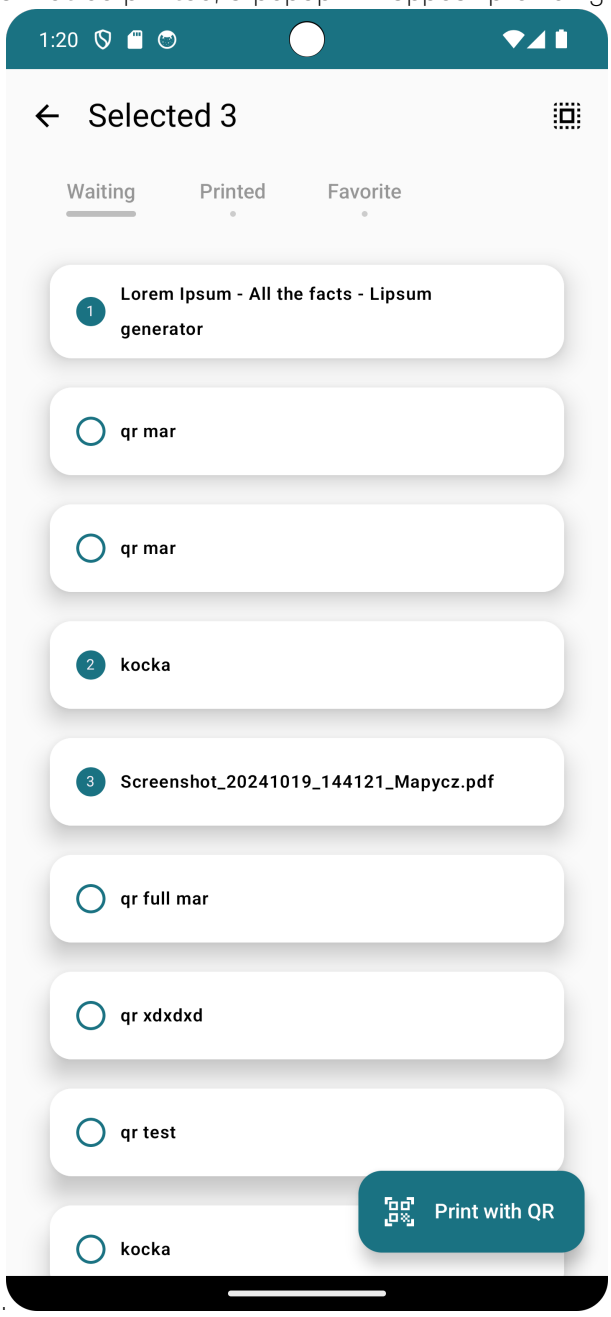
Deleting print jobs

To delete a print job, swipe it to the left.

Job release with QR code

Users can select multiple files in a specific order. After tapping the Print with QR button, they can scan a QR code to release the jobs to the corresponding printer in the previously selected order. If

any jobs cannot be printed, a popup will appear providing information about why they could not be processed.



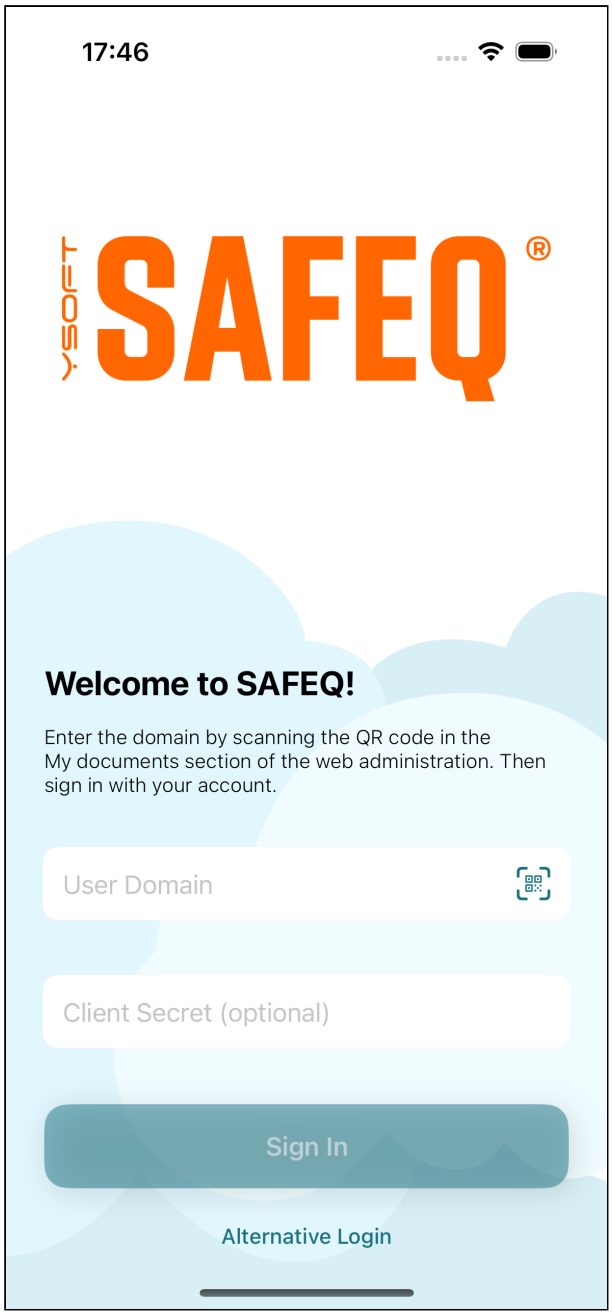
Using the iOS Mobile app

Download the application from the App Store.

Logging in

1. After you start the application for the first time, you will see the login screen.
2. Enter the **User Domain**. You can enter it manually or by scanning the configuration QR code that you can find in SAFEQ Cloud Web UI.
3. Tap **Sign in** and enter your SAFEQ Cloud username and password or use other login methods, for example via your Microsoft or Google account. The available login methods depend on how your administrator configured the app.

Alternatively, tap **Alternative Login** if your company uses, for example, a custom identity provider



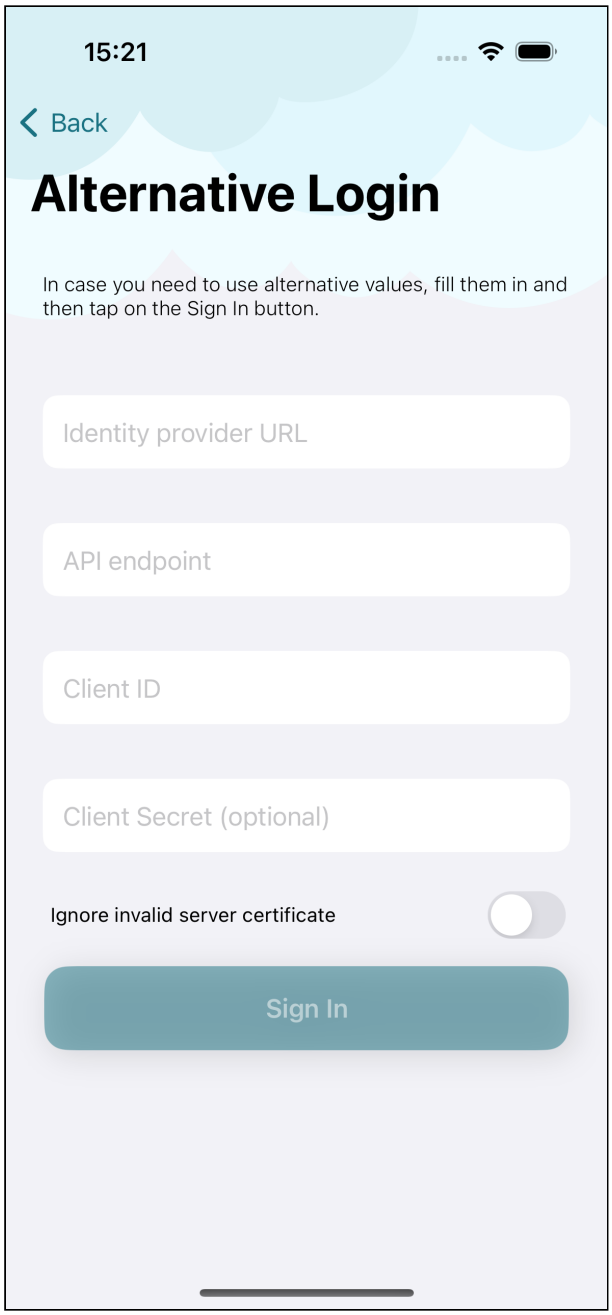
Alternate login

On the **Alternate Login** screen, enter the following:

- **Identity provider URL** – If a custom identity provider is deployed, provide the custom identity provider's URL. For a default deployment, enter the address and port of Job Service. For example, if the Job Service is deployed on a machine with hostname *example.com* , then the value is *https://example.com:5000/* .
- **API endpoint** – Use the address and the HTTPS port of Spooler, e.g. *https://example.com:5002* .

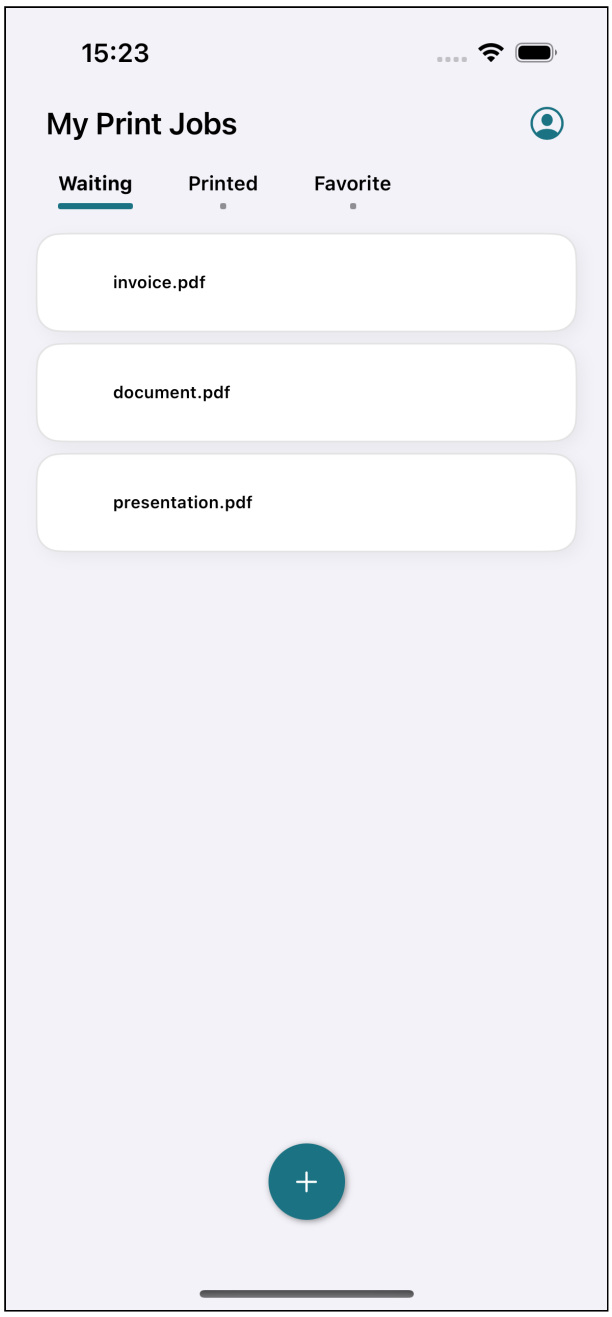
- Client ID – Use the ClientId value specified in the identity provider. For a default deployment using Job Service as an identity provider, use *ClientId of Additional Clients* located in Job Service's local.json configuration file. The default value is mobile-application.
- Client Secret – Optional value of the API Key that authenticates the app.

You can enable communication that is not secured by TLS by using the toggle button.



Job list

After a successful login, you will see all of your documents.



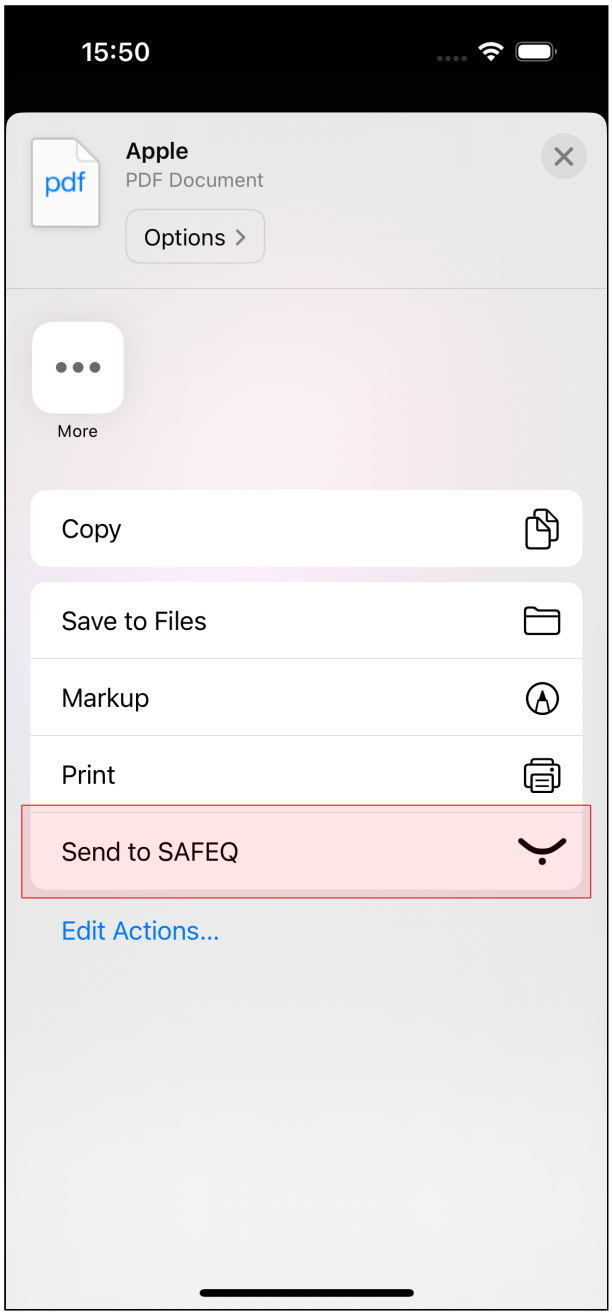
Submitting print jobs

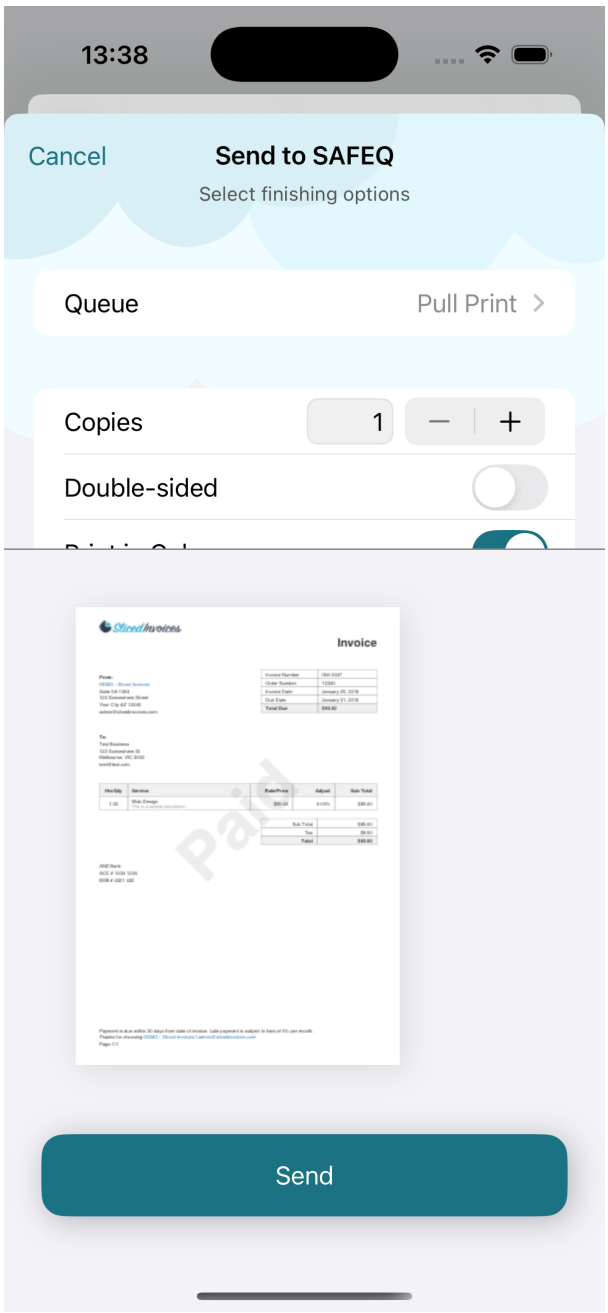
Supported formats

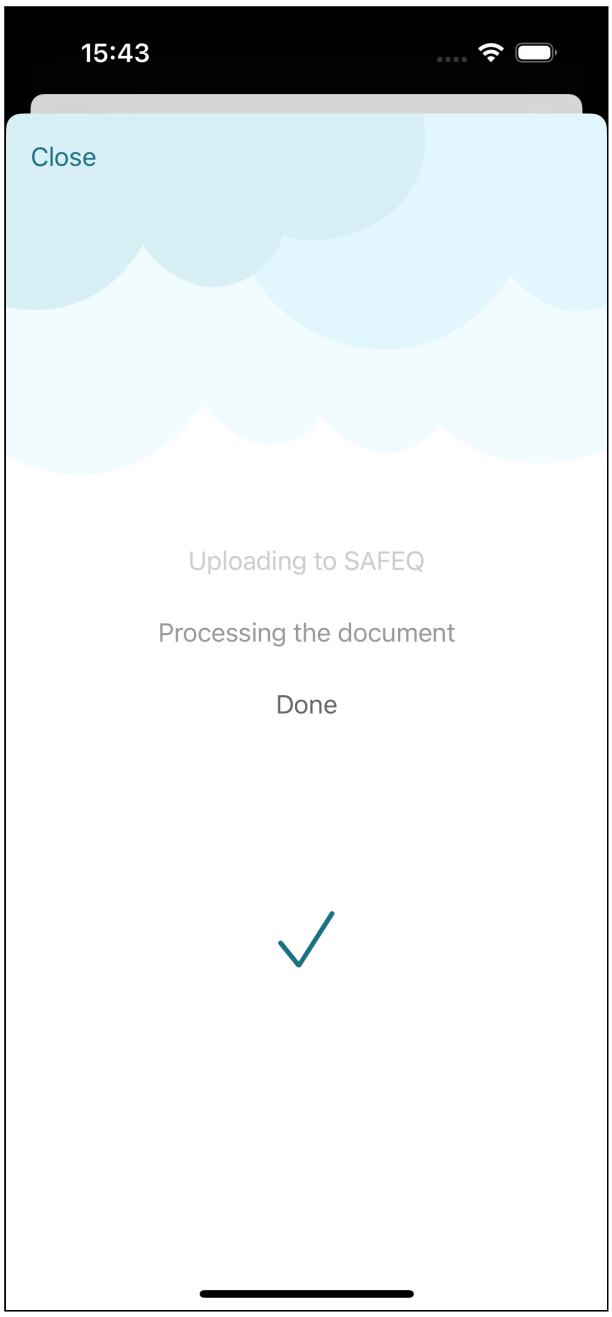
- BMP
- JPEG
- PDF
- PNG
- rawImage
- SVG
- TIFF
- WebP

Submitting print jobs from the apps via the share menu

This can be done from any app that supports printing. Select SAFEQ Cloud from the share extension in the iOS share menu.

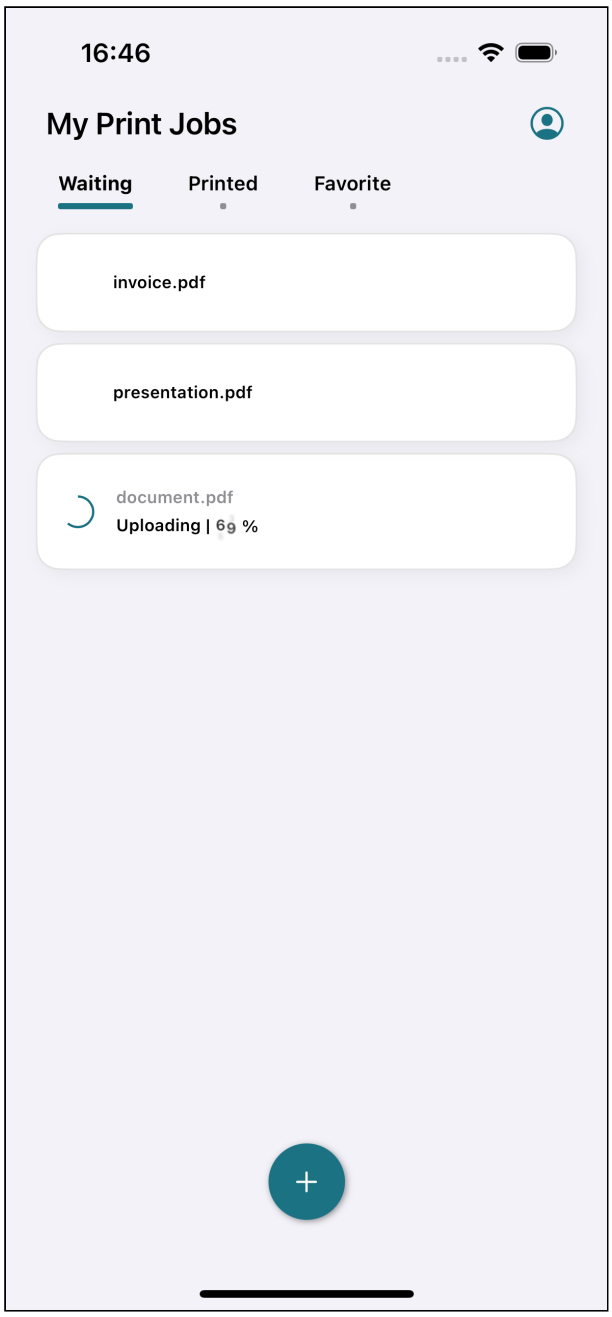


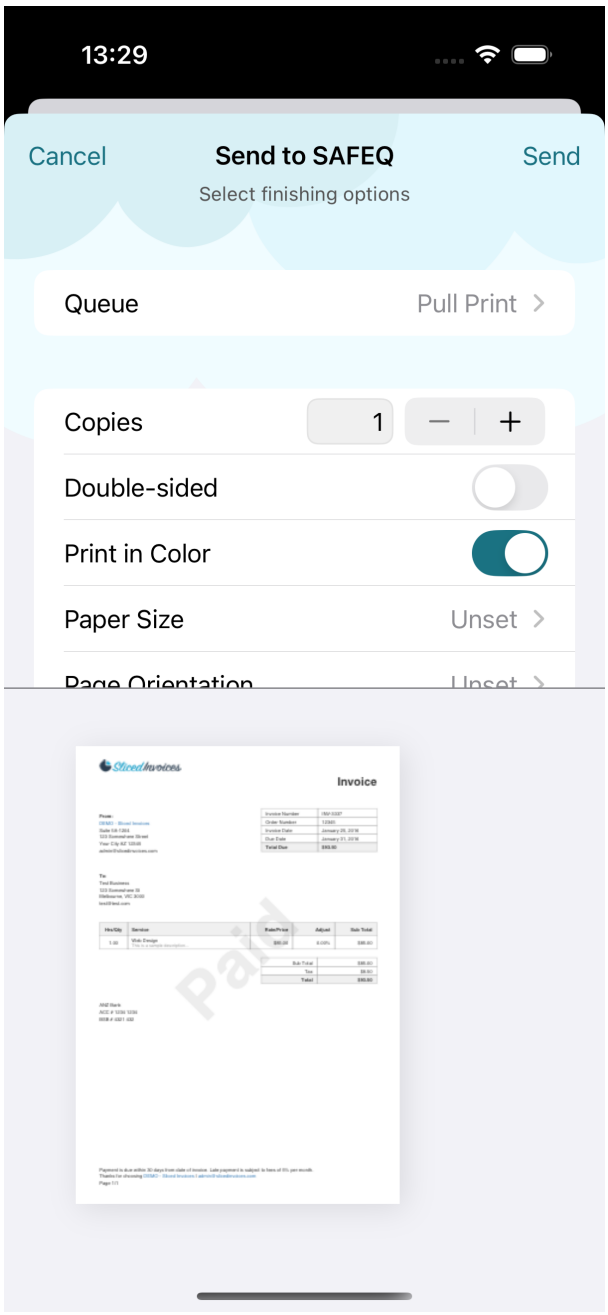

13:38
Cancel
Send to SAFEQ
Select finishing options
Queue
Pull Print
Copies
1
Double-sided
Invoice
Paid
Send



Submitting print jobs directly from the app

1. To submit a new document, tap the plus button at the bottom of the Job List screen. This will open the standard system file picker.
2. Select one or more files. If any of the chosen files are password-protected, a dialog will appear prompting you to enter the password. You will have the option to skip those files you do not wish to unlock.
3. On the next screen, customize the finishing options (print queue, number of copies, color, page size, page orientation, and sides) according to your needs.
4. Tap **Send**.


16:46
My Print Jobs
Waiting
Printed
Favorite
invoice.pdf
presentation.pdf
document.pdf
Uploading | 69 %



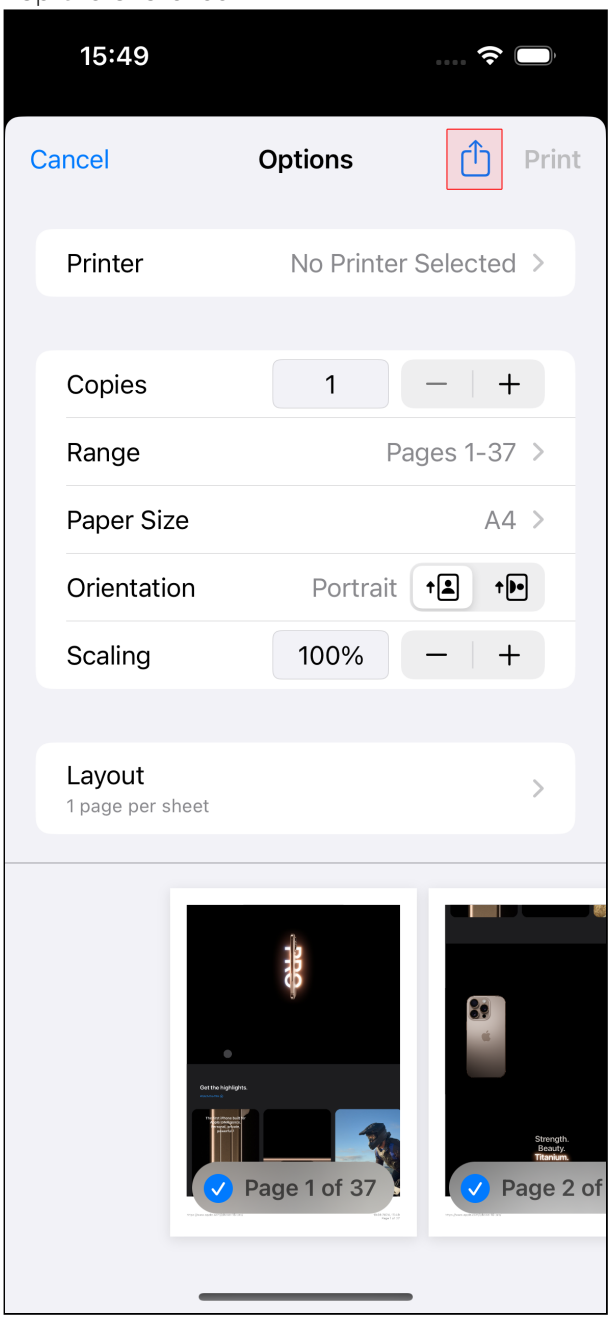
Printing unsupported file formats

If the printable document is not in supported format, you can use the standard system print dialog and share the output into the SAFEQ Cloud mobile app instead of selecting the AirPrint printer. You can do this in any app that supports system print.

iOS 16 or higher

1. Open the system print dialog and use the system print finishing options.

2. Tap the share icon.



3. Continue as described in the *Submitting print jobs* section above.

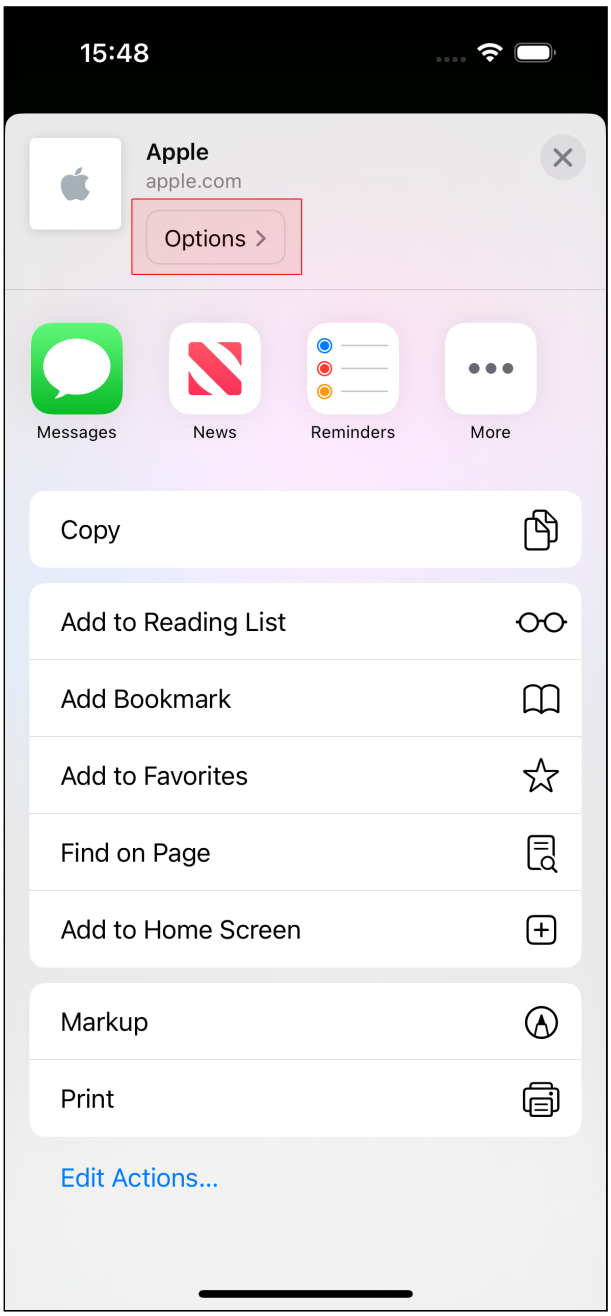
iOS 15 or lower

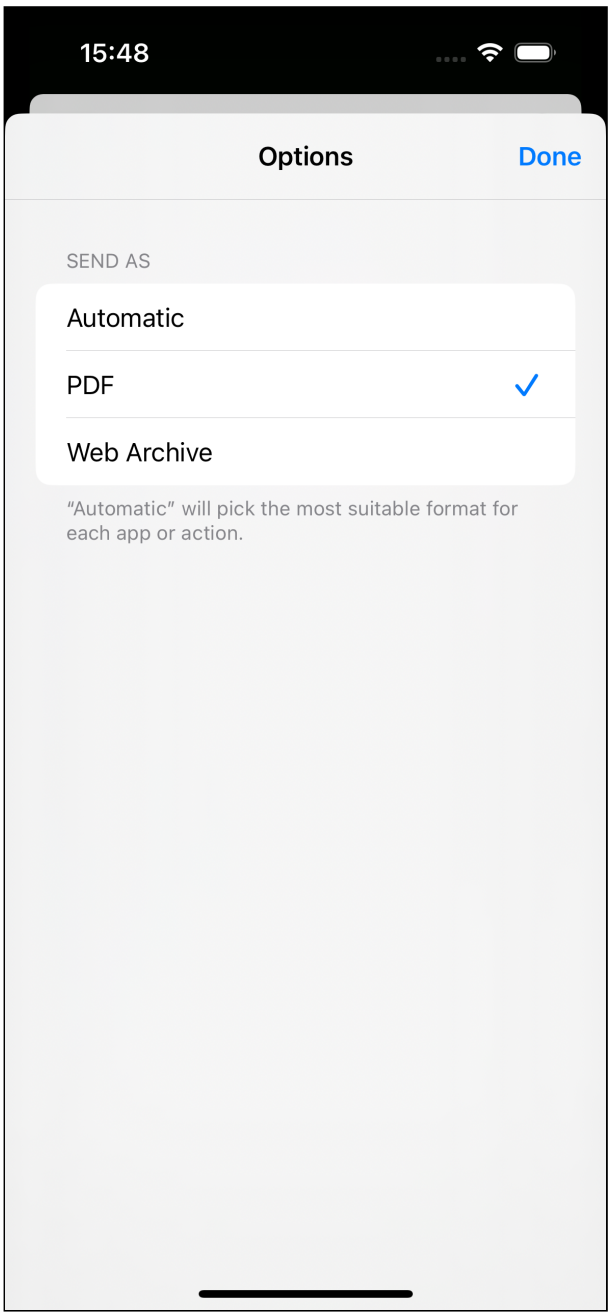
1. Open the system print dialog and pinch to zoom with two fingers on the preview of the document.
2. This will open the preview of the document in PDF format.
3. On this preview, tap the share button.
4. Continue as described in the *Submitting print jobs* section.

Printing a web page from Safari

1. Go to the iOS share menu.

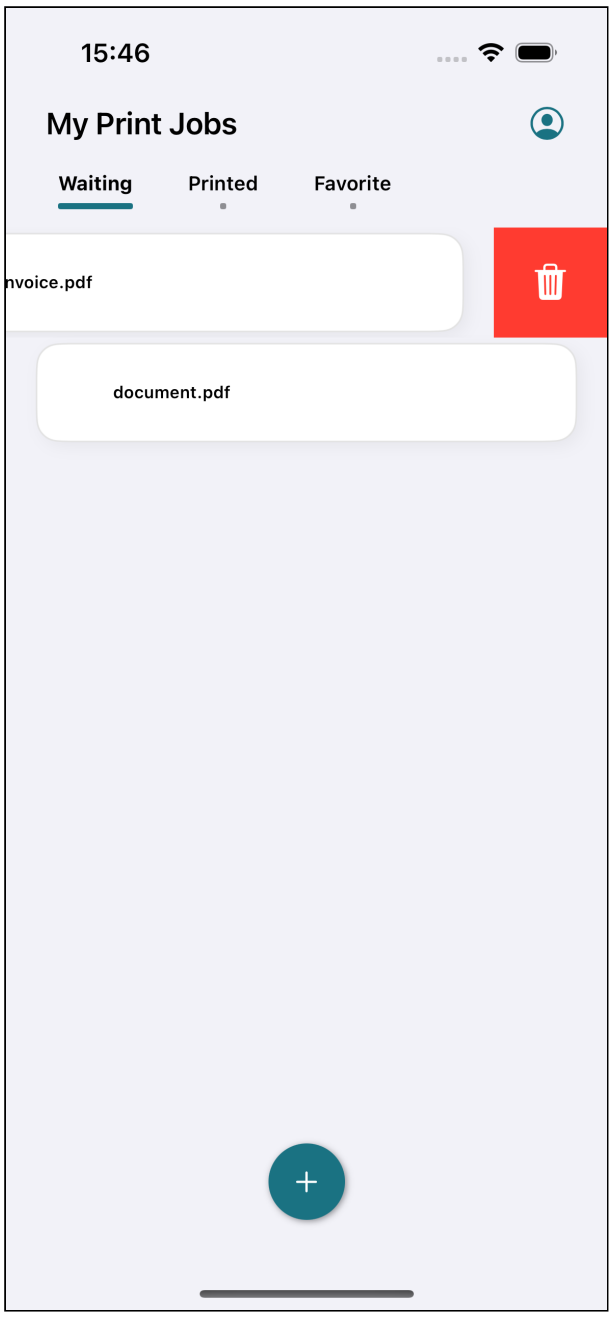
2. Tap **Options**. Make sure that the PDF option is selected so that the SAFEQ Cloud share extension is visible in the share menu.


15:48
Apple
apple.com
Options
Messages
News
Reminders
More
Copy
Add to Reading List
Add Bookmark
Add to Favorites
Find on Page
Add to Home Screen
Markup
Print
Edit Actions...



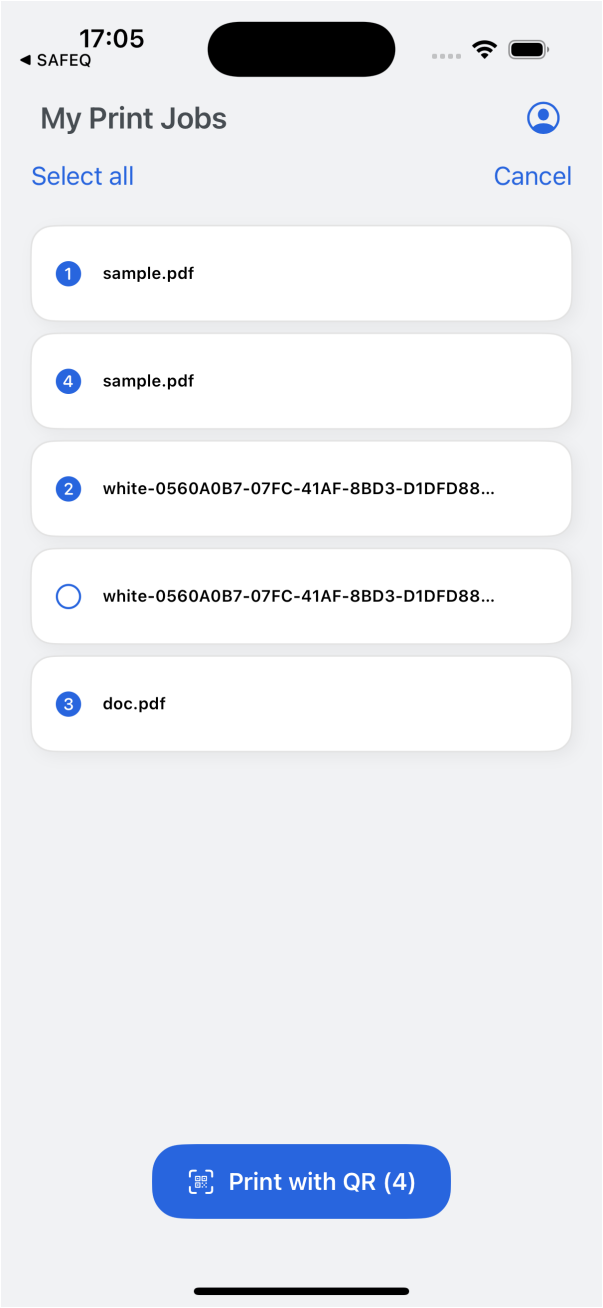
Deleting print jobs

To delete a print job, swipe it to the left.



Job release with QR code

Users can select multiple files in a specific order. After tapping the Print with QR button, they can scan a QR code to release the jobs to the corresponding printer in the previously selected order. If any jobs cannot be printed, a popup will appear providing information about why they could not be processed.



9.1.3 USING THE LEGACY MOBILE APP

Downloading the app

Download the YSoft SAFEQ Cloud Mobile app for Apple iOS from the link below or search for SAFEQ Cloud in App Store:
https://itunes.apple.com/us/app/everyoneprint/id565311817

Download the YSoft SAFEQ Cloud Mobile app for Android from the link below or search for SAFEQ Cloud in Google Play Store:
https://play.google.com/store/apps/details?id=com.nps.everyoneprint

Mobile Apps are available for the following MDM providers as well:

- AirWatch

- MobileIron

Supported devices

- Android 10.0 or higher
- iOS 12.0 or higher

Logging in

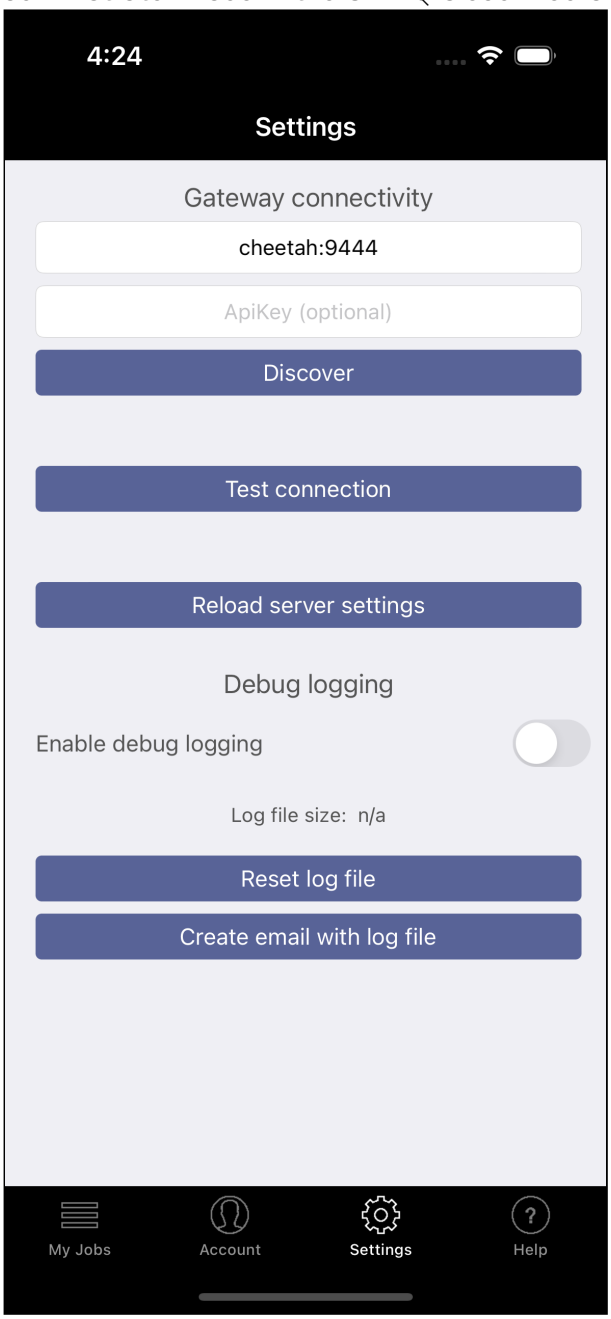
When using the YSoft SAFEQ Cloud app for the first time, the app will need to connect to the mobile gateway host – the SAFEQ Cloud server where the mobileprint service is installed.
The configuration is similar on iOS and Android, with only slight UI differences.

1. Tap the Settings tab in the app.
   a. Tap Discover. The discovery process will try to find the mobile print service announcement via DNS-SD. Once it is found, the domain name and port number of the mobile gateway host are automatically inserted in the text field.
   b. If the gateway was not found, enter the domain and port manually,

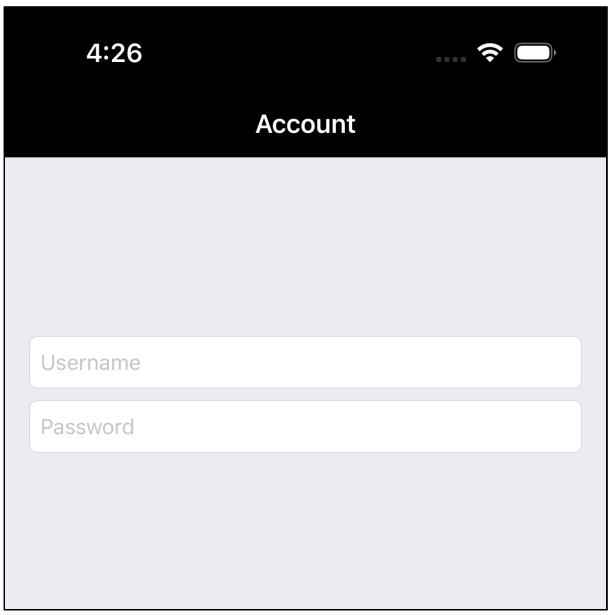
      e.g. "acme.eu.ysoft.cloud:9444".

      Contact your administrator to provide you with these values.
2. Tap Test connection to validate the connection to the mobile gateway.
3. After a successful test, the Save button will appear. Tap it to save the settings. This process will also retrieve the server settings to update the app according to the configuration your

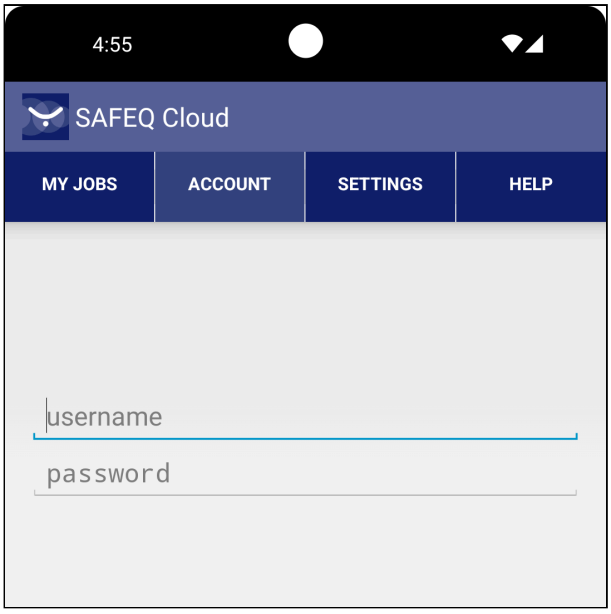
administrator made in the SAFEQ Cloud Web UI.



4. To log into the mobile app, tap **Account** and enter your SAFEQ Cloud credentials.
iOS:

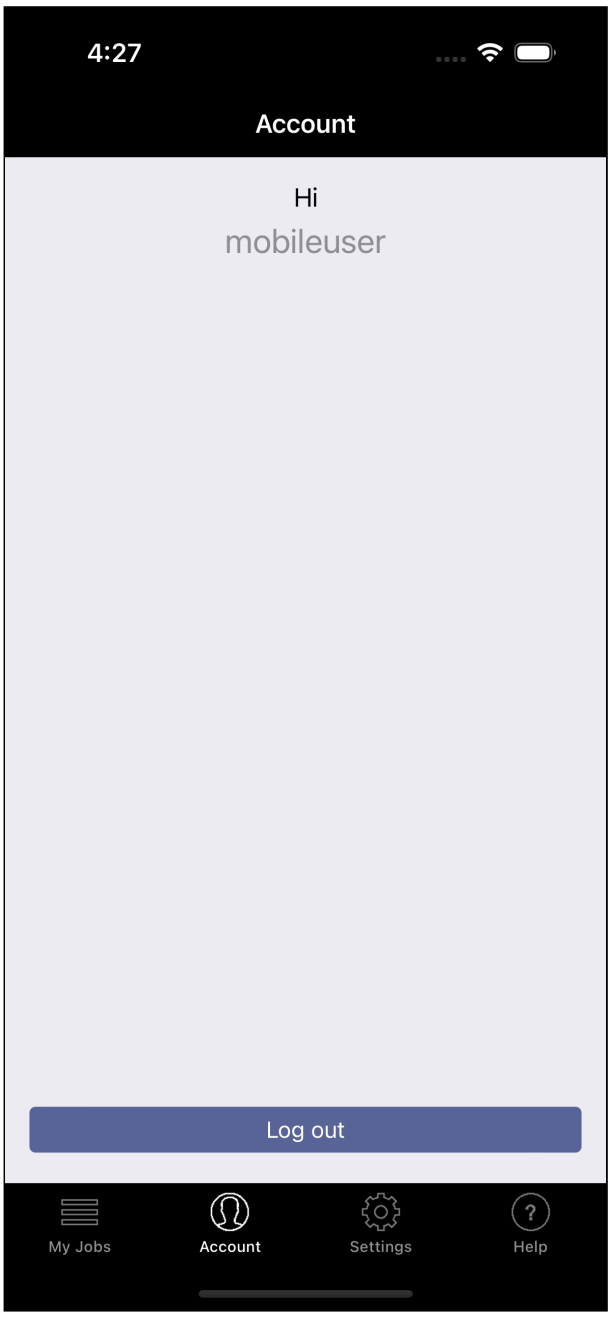


Android:

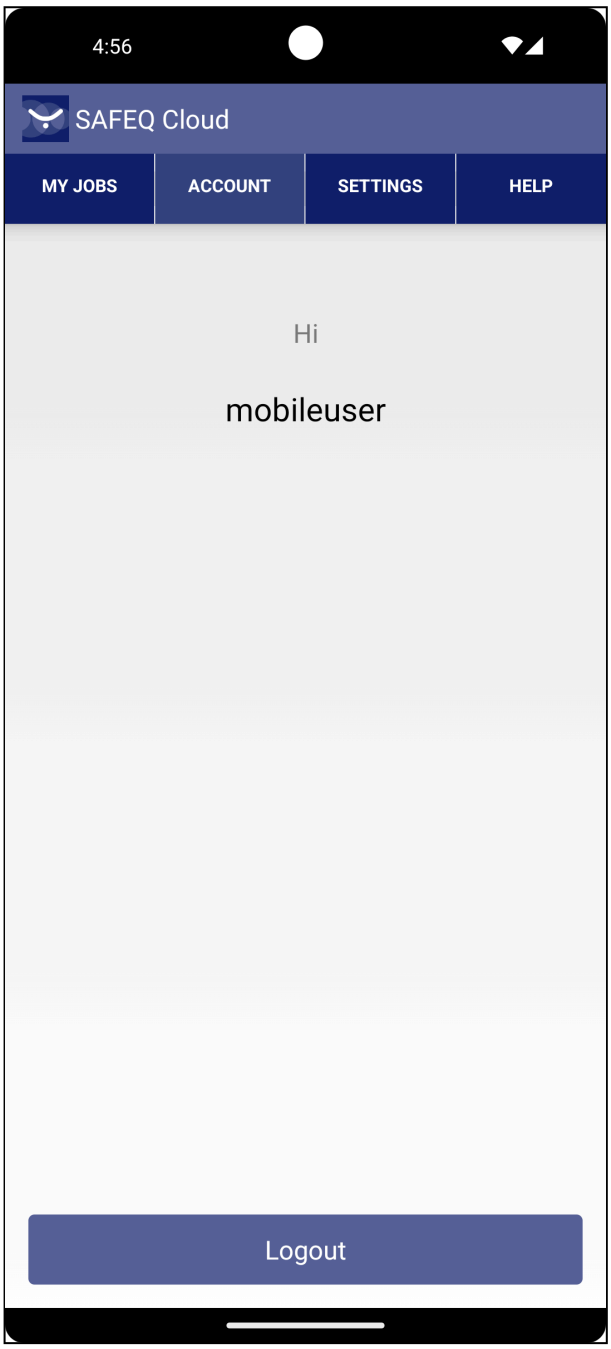


Printing

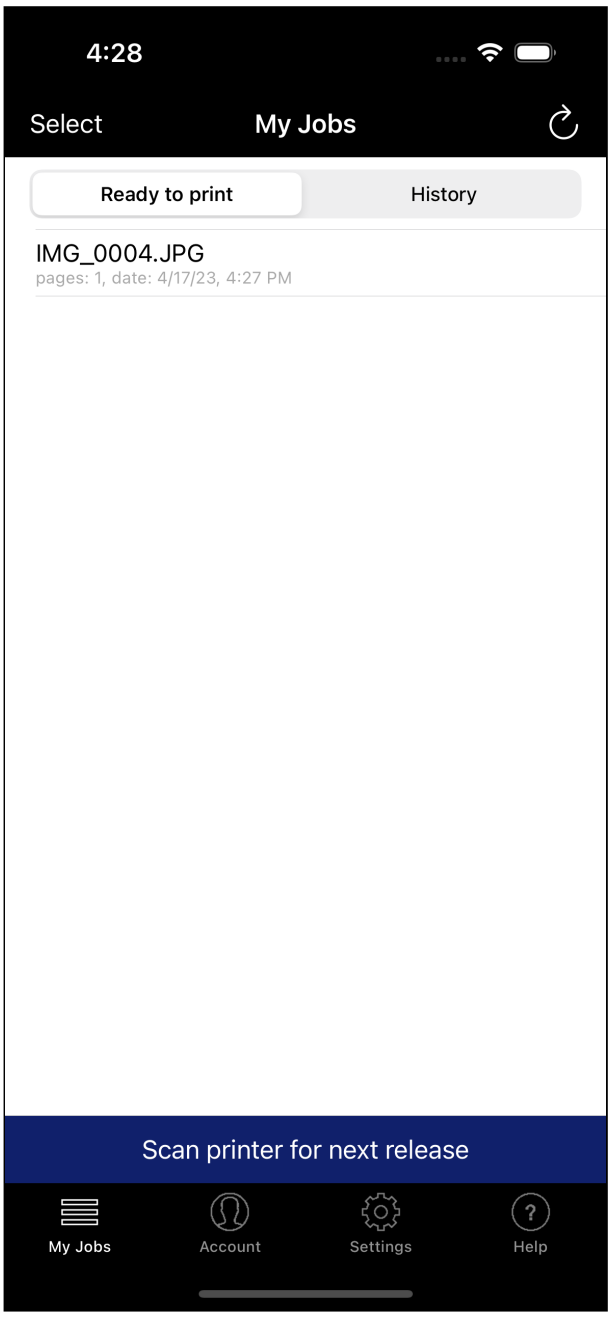
1. After logging in, you will see the welcome screen.
   iOS:


4:27
Account
Hi
mobileuser
Log out
My Jobs
Account
Settings
Help

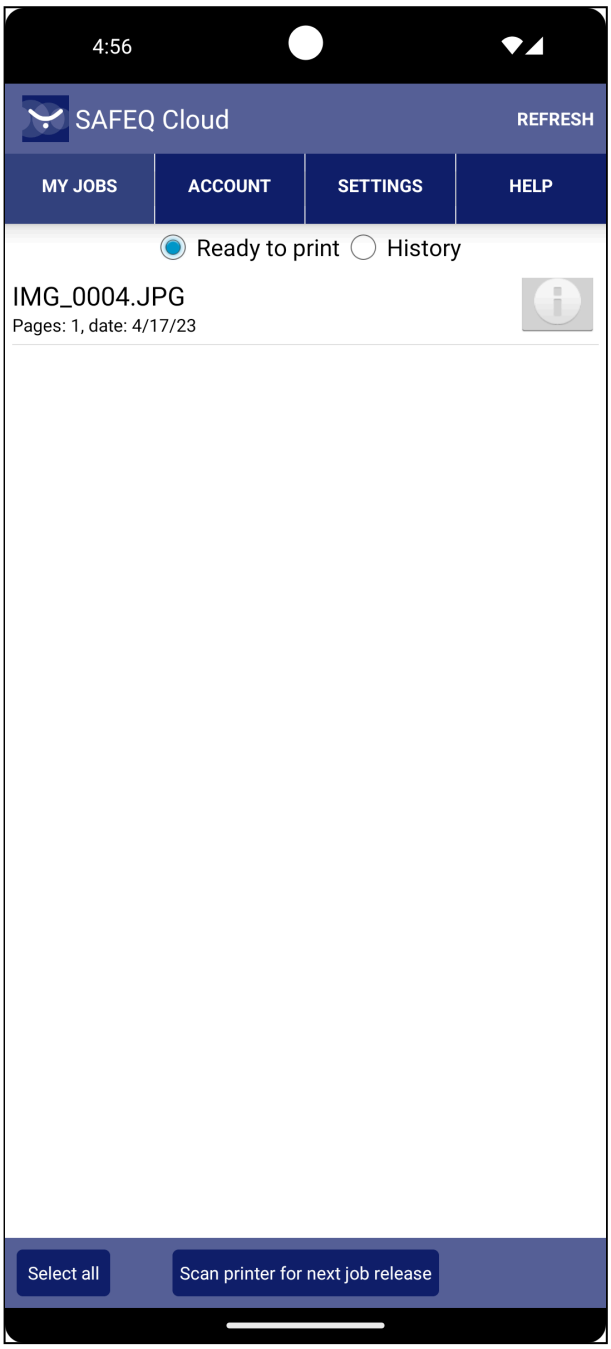
Android:



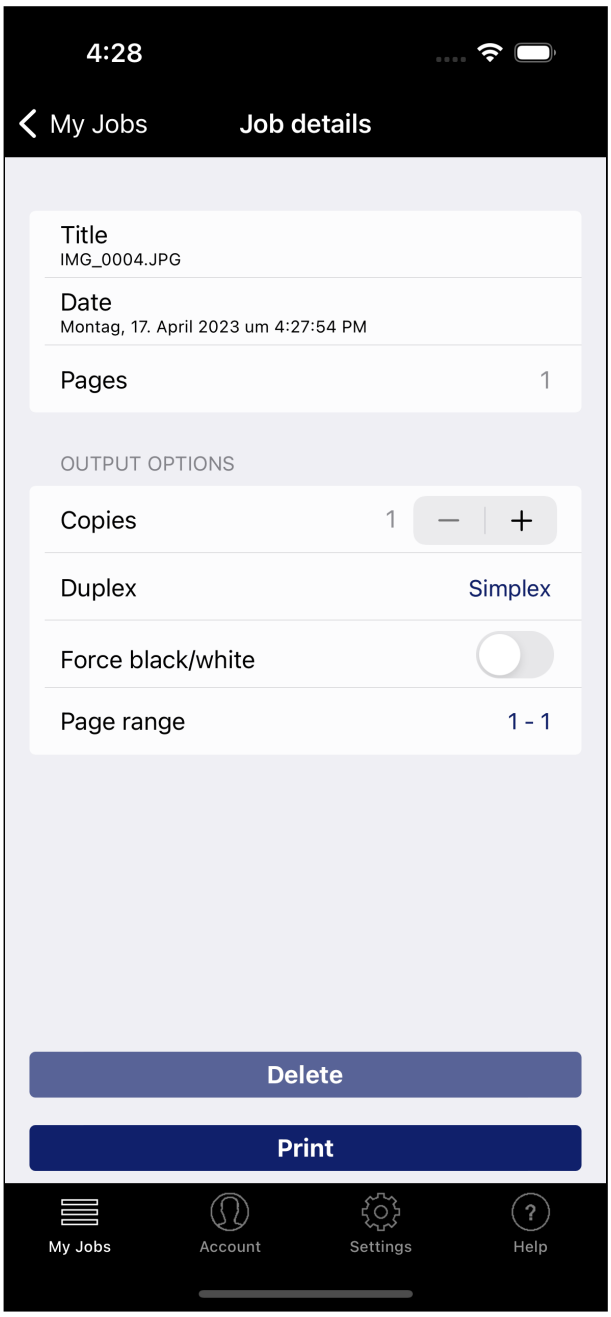
2. Go to the **My Jobs** tab. You will see the list of your waiting print jobs and printed print jobs.
iOS:


4:28
Select
My Jobs
Ready to print
History
IMG_0004.JPG
pages: 1, date: 4/17/23, 4:27 PM
Scan printer for next release
My Jobs
Account
Settings
Help

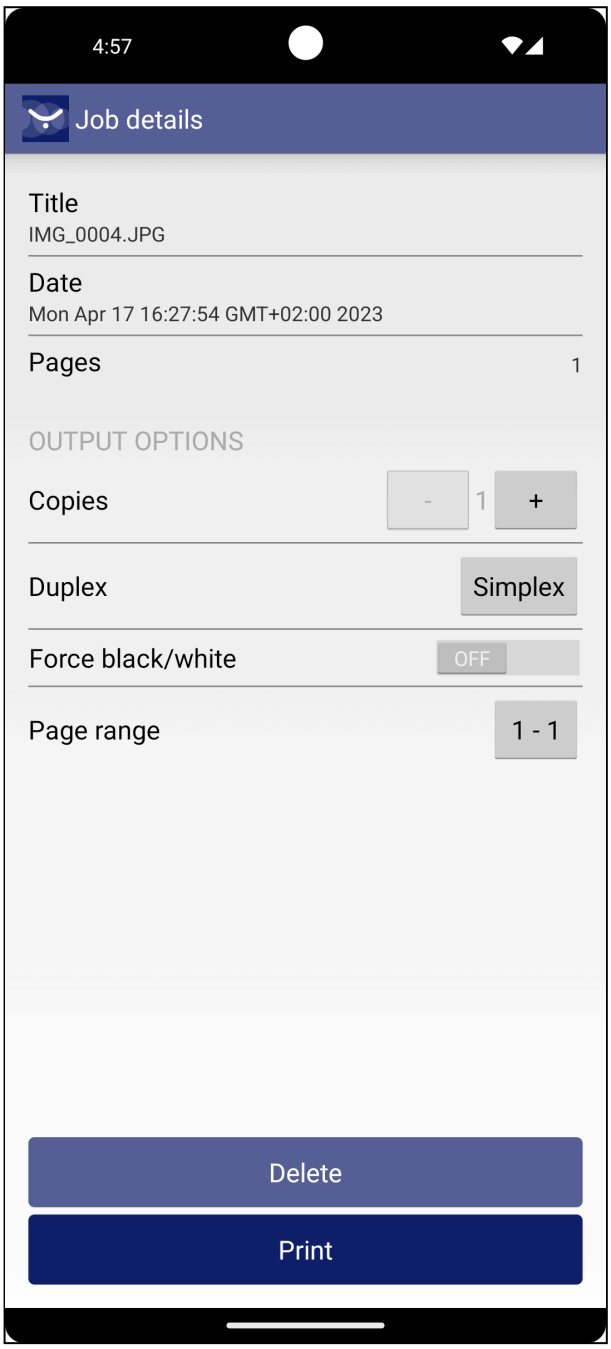
Android:



3. Tap the document you wish to print. The job details will be displayed. Tap **Print**.
iOS:


4:28
My Jobs
Job details
Title
IMG_0004.JPG
Date
Montag, 17. April 2023 um 4:27:54 PM
Pages
1
OUTPUT OPTIONS
Copies
1
Duplex
Simplex
Force black/white
Page range
1 - 1
Delete
Print
My Jobs
Account
Settings
Help

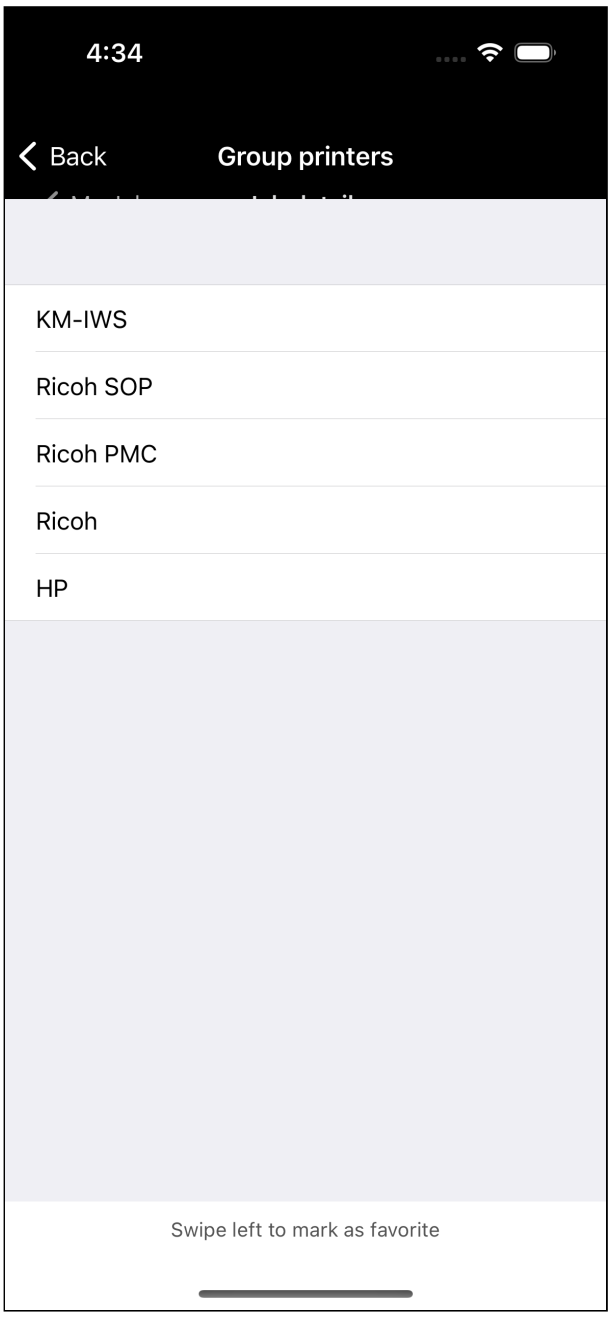
Android:

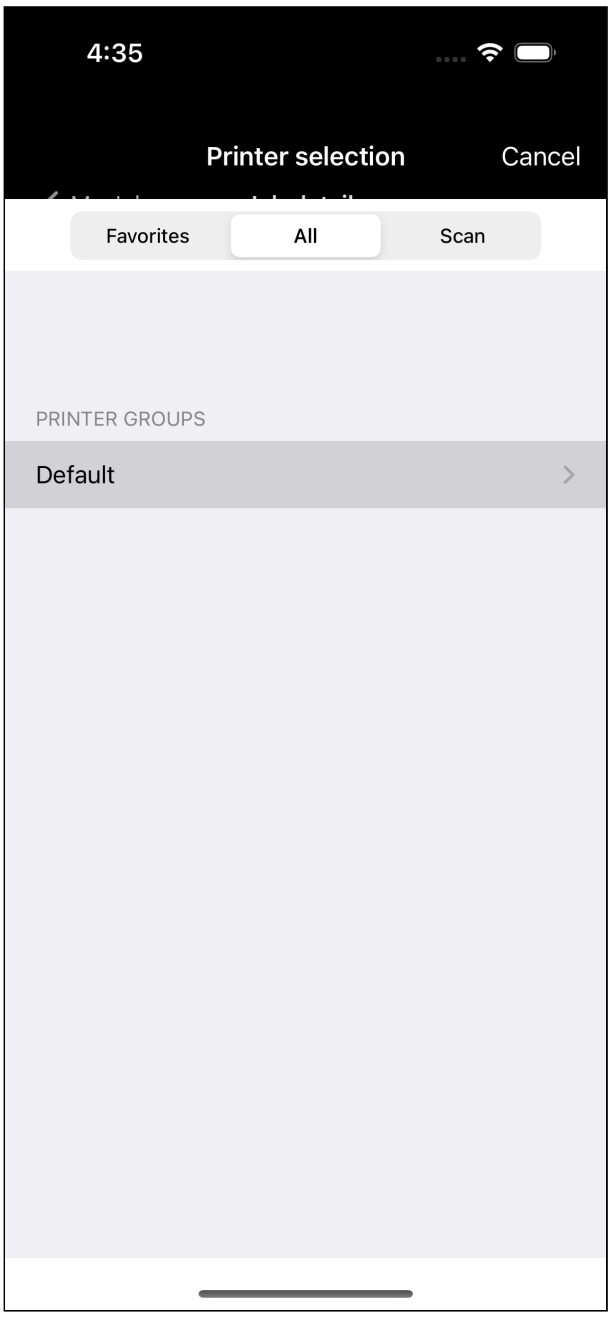


4. You can release your print job in the following two ways:

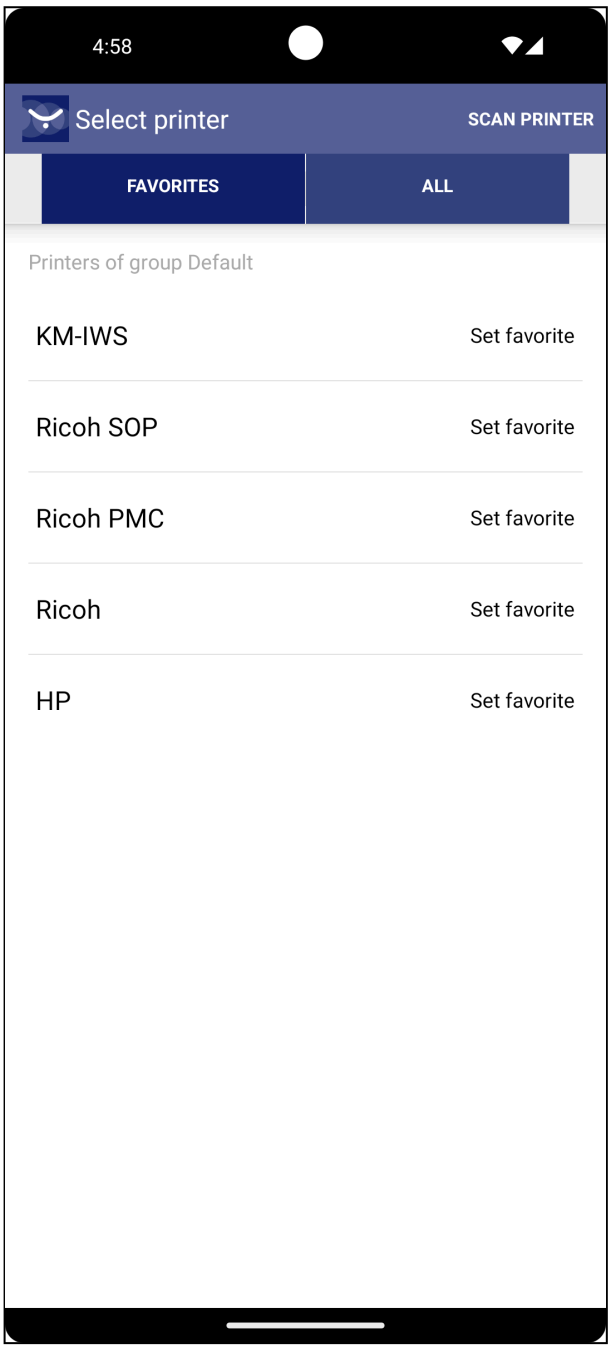
   a. After tapping **Print**, the app will display a list of printers. Tap the selected MFD where you wish to release the job.

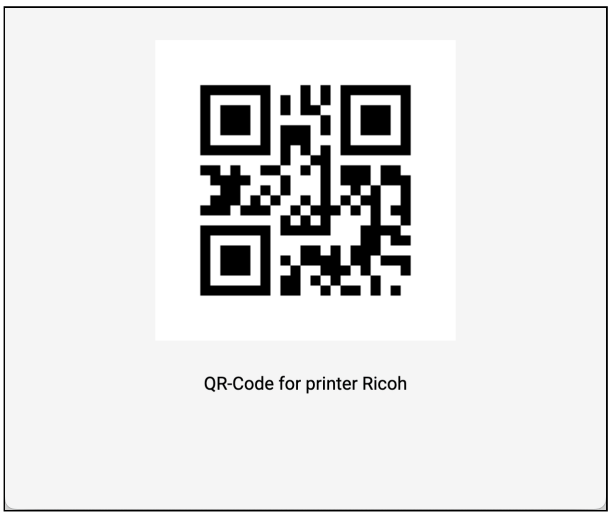
   b. Go to an MFD and scan its QR code. If using the iOS app, tap **Back** and select the **Scan** tab. If using the Android App, tap **SCAN PRINTER** in the top-right corner.
   iOS:


4:34
Back
Group printers
KM-IWS
Ricoh SOP
Ricoh PMC
Ricoh
HP
Swipe left to mark as favorite


4:35
Printer selection
Cancel
Favorites
All
Scan
PRINTER GROUPS
Default

Android:


4:58
Select printer
SCAN PRINTER
FAVORITES
ALL
Printers of group Default
KM-IWS
Set favorite
Ricoh SOP
Set favorite
Ricoh PMC
Set favorite
Ricoh
Set favorite
HP
Set favorite



Native print on Android

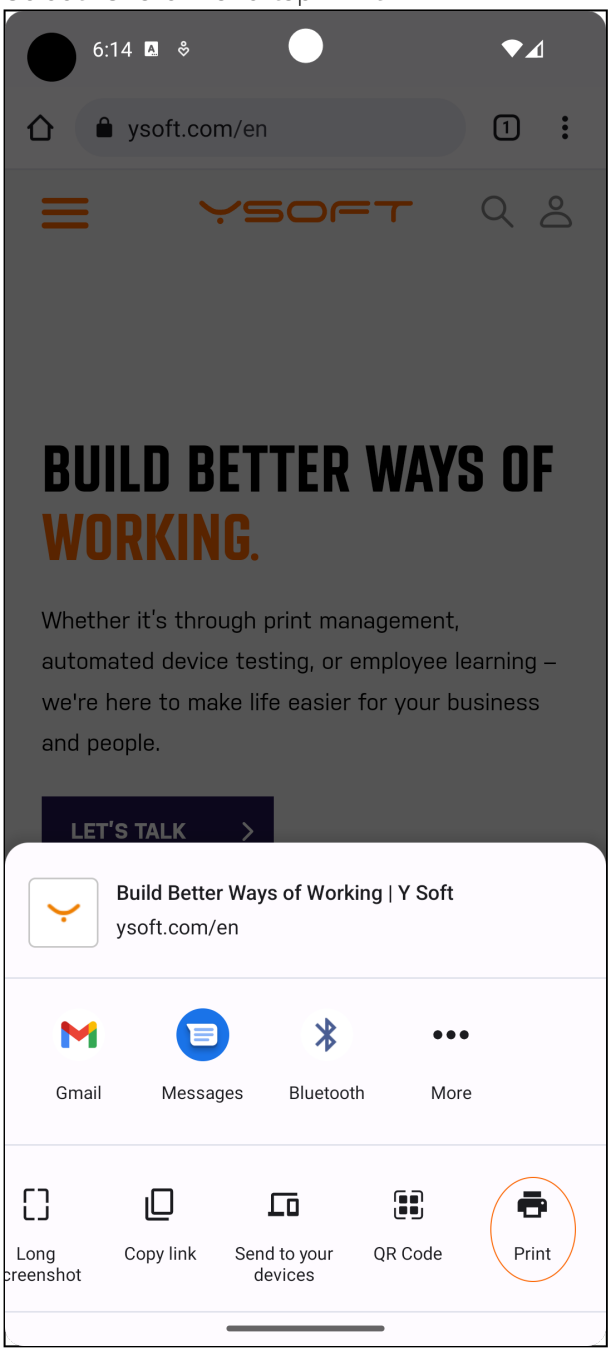
The Android app supports the native print functionality of Android OS. This is only available from Android version 5.0.
The following list of apps is known to work with native printing on Android 5 and later:

- Google Chrome
- Firefox
- Google Gmail
- Google Docs
- Google Photos
- Adobe Acrobat
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

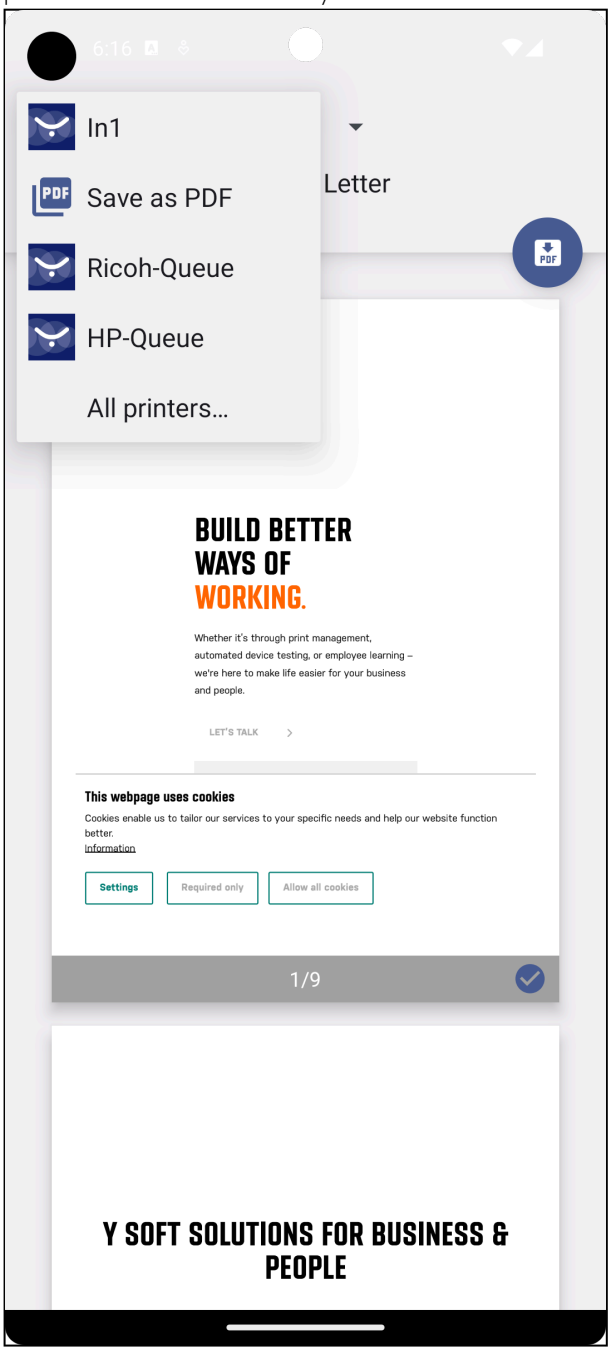
Enabling native print on Android

1. Open the Mobile app and log in.
2. Open Chrome or any other app that supports Android native print

3. Select "Share..." and tap **Print**.



4. The print queues that your administrator configured in SAFEQ Cloud will be available to you as printers. Select the one you wish to use.



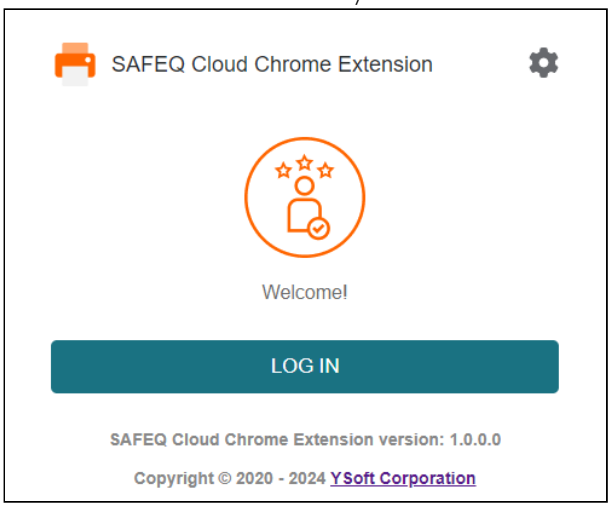
9.1.4 USING THE SAFEQ CLOUD CHROME EXTENSION

Prerequisites

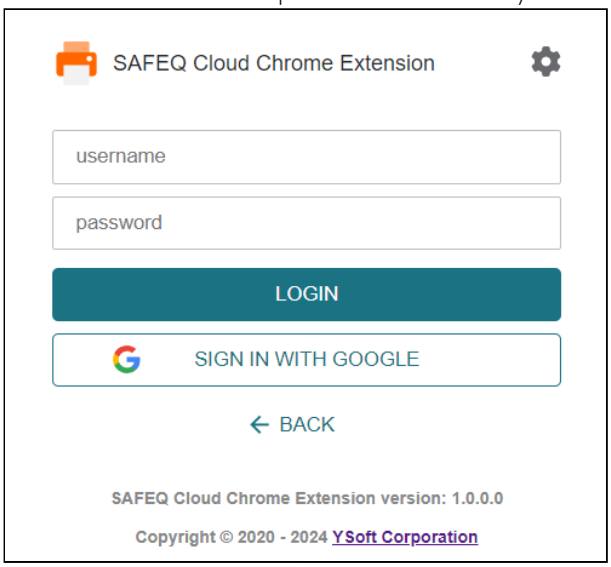
- Your administrator has installed and configured the extension for you.
- To use SAFEQ Cloud Chrome extension, you must enable account synchronization in Chrome (see section *Enabling account synchronization in Chrome* of this page).

Logging in

1. Click the extension icon in your browser.



2. Click **Log in**. A login dialogue window will open. You will have a choice to log in with SAFEQ Cloud username and password or with your Google account.

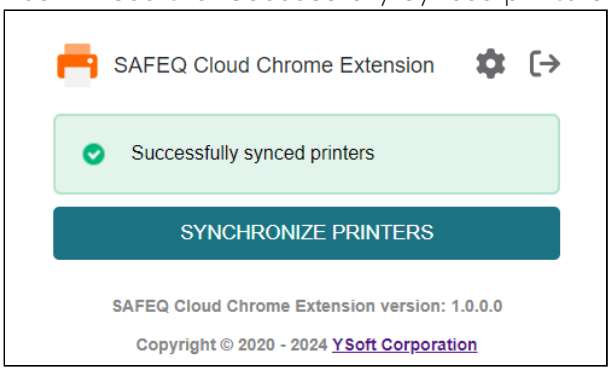


3. Enter your username and password for SAFEQ Cloud and click **Login**.
4. Alternatively, click **Sign in with Google** and enter your Google credentials.

Synchronizing printers

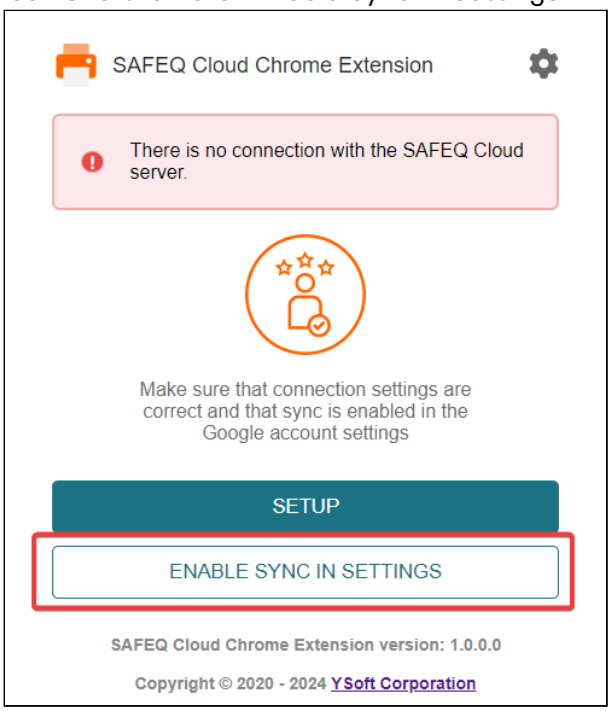
1. Open the extension icon in your browser. A dialog window will appear.
2. Printers are automatically synchronized by opening the extension popup window. To trigger the synchronization manually, click **Synchronize printers**.

3. You will see the "Successfully synced printers" message.

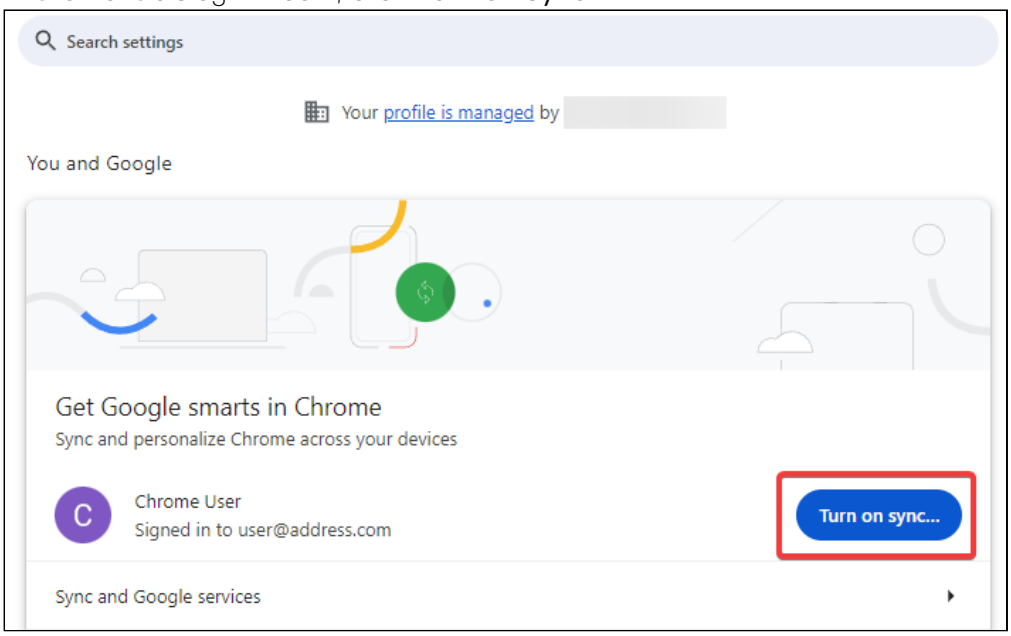


Enabling account synchronization in Chrome

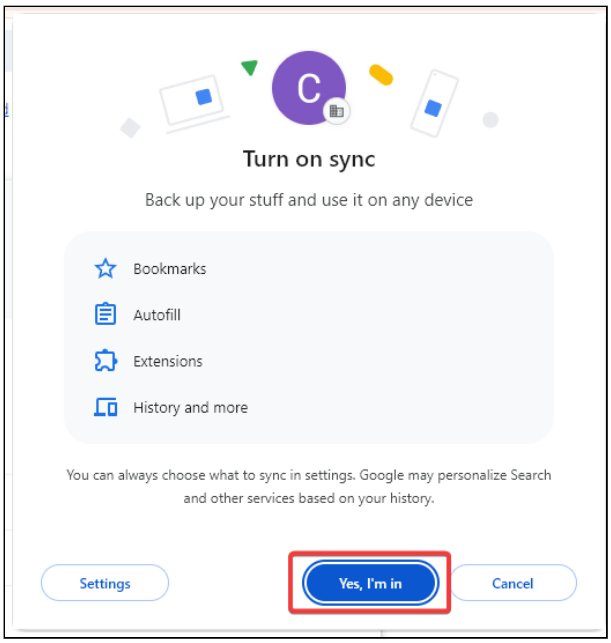
1. In your Chrome browser, go to chrome://settings/people or click the SAFEQ Cloud extension icon and then click Enable sync in settings.



2. In the next dialog window, click **Turn on sync...**



3. Click **Yes, I'm in**.

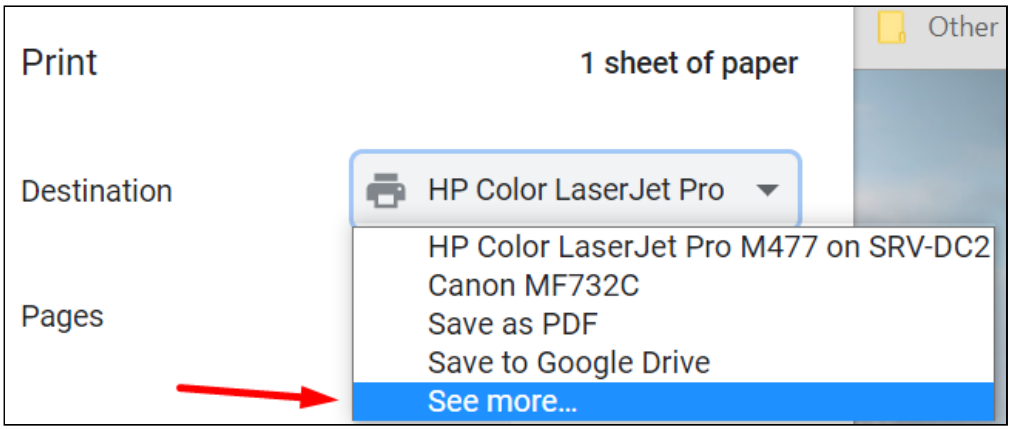


4. After successful login, verify your configuration by clicking the extension icon. You should see the "Successfully synced printers" message.

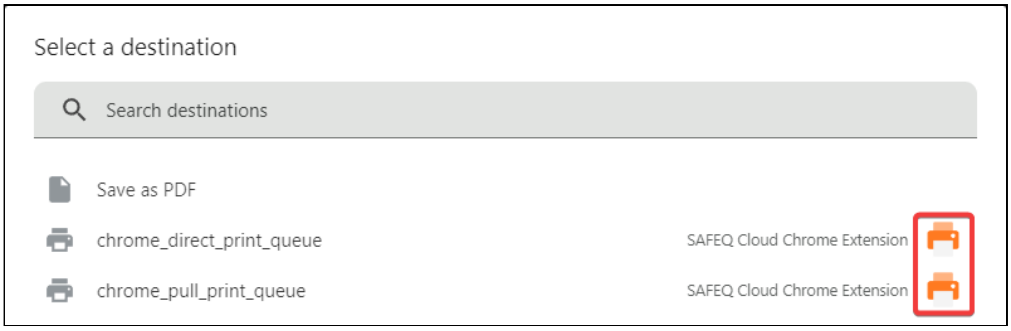
Submitting a print job

1. Select a document for print.
2. Open the **Print** dialogue in your Chrome browser.

3. In **Destination**, click **See more**.



4. Select a printer with the SAFEQ Cloud Chrome extension icon.



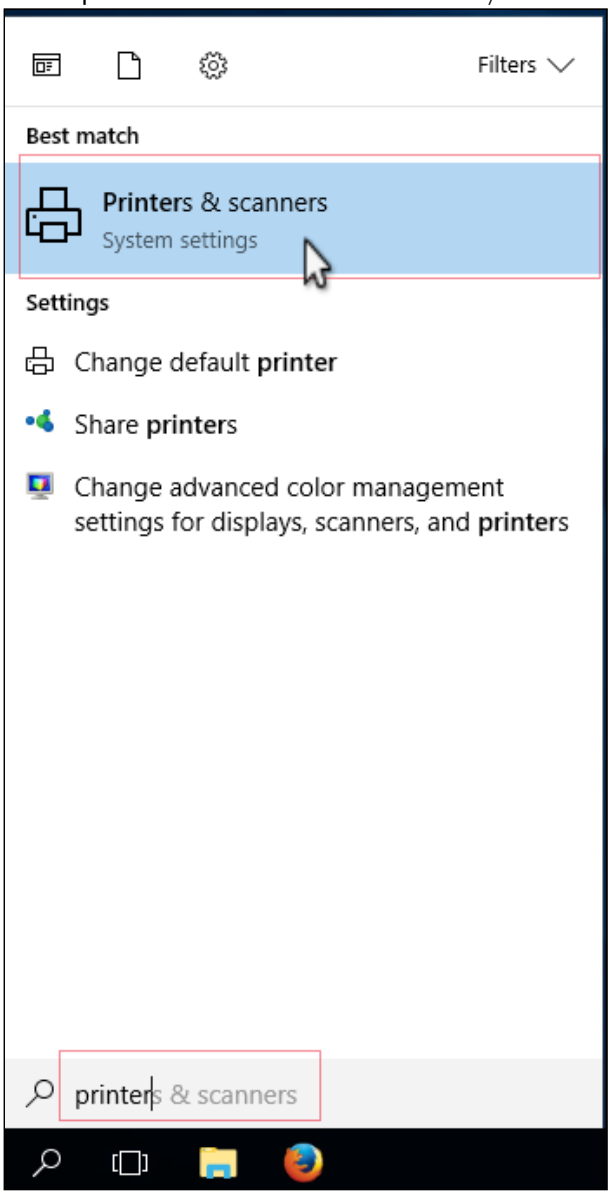
5. Click **Print**.

9.1.5 ADDING IPP PRINT QUEUE MANUALLY IN WINDOWS

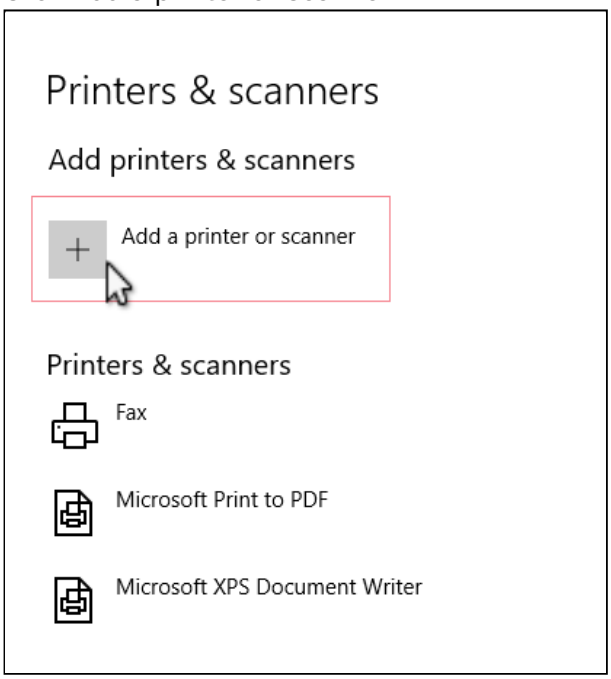
If you are not using the SAFEQ Cloud Client for Windows, you can print directly from the programs on your computer, by adding an IPP print queue manually. Your administrator must provide you with the print queue address and with information on which print driver to use. When you have this information, perform the following steps:

Windows 10

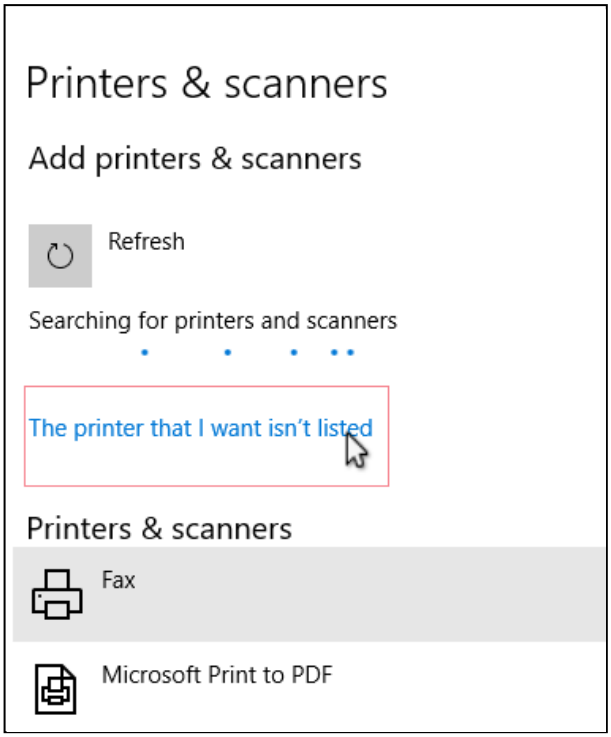
1. Enter **printer** in the Search field in in your task bar. Click **Printers & Scanners**.



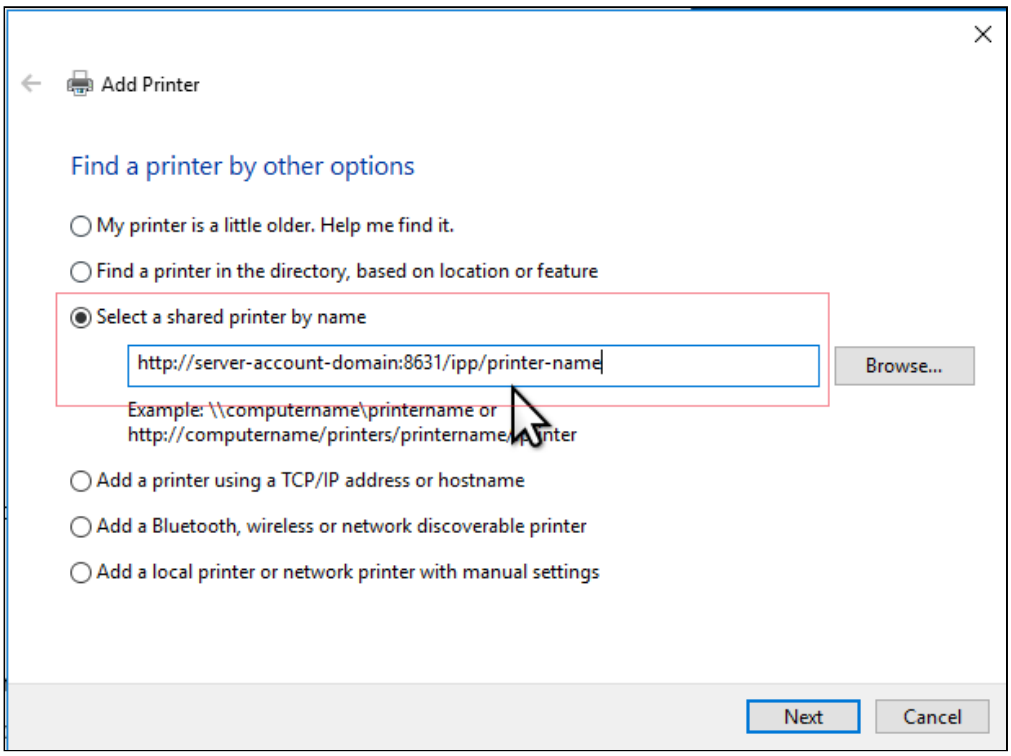
2. Click **Add a printer or scanner**.



3. Wait until you see **The printer that I want isn't listed**, and click the link.



4. Select **Select a shared printer by name** and enter the address of the IPP print queue that you received from your administrator.



Information for administrators regarding the print queue URL customization:

SSL (requires a valid certificate for the domain):

https://<server-fqdn>:9631/ipp/<printer-name>/accountdomain=<account-domain-fqdn>/username=<user-name>/providerid=<auth-provider-ID>

Non-SSL:

http://<server-fqdn>:8631/ipp/<printer-name>/accountdomain=<account-domain-fqdn>/username=<user-name>/providerid=<auth-provider-ID>

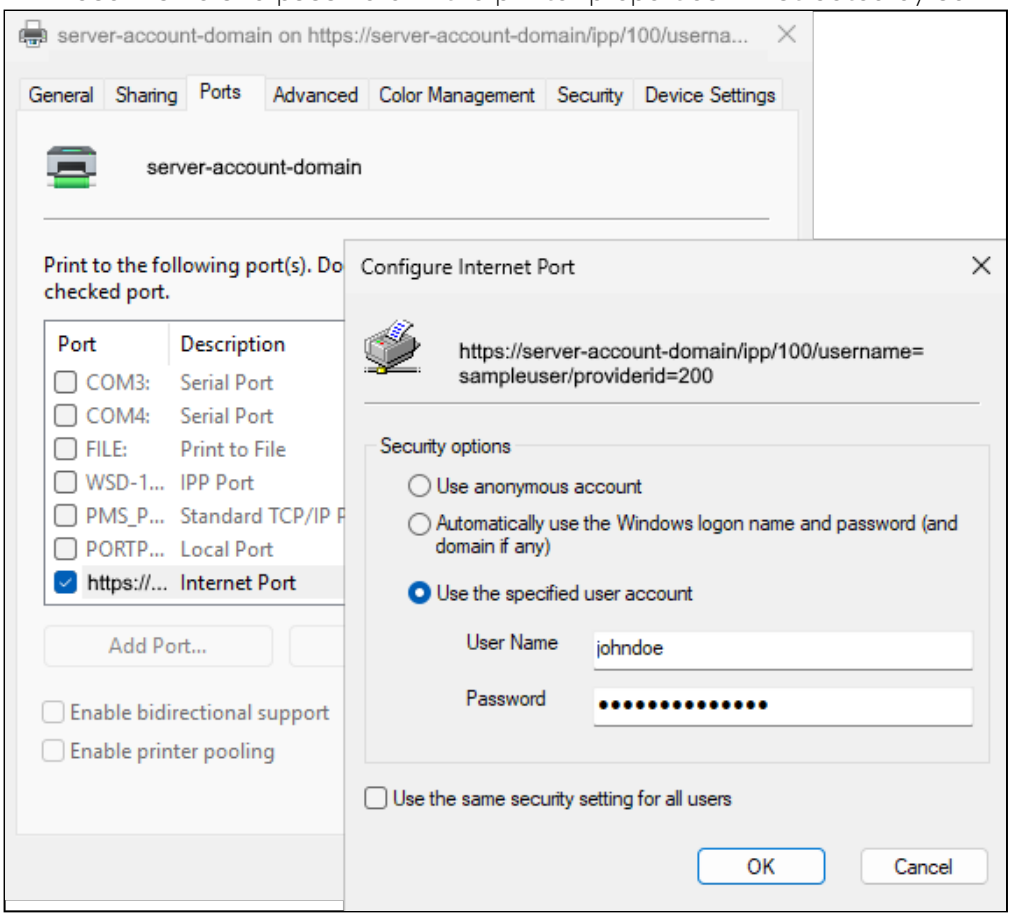
For both types:

- Replace **<server-fqdn>** with the domain name of the server that hosts the IPP service.
- Replace **<printer-name>** with the print queue name or ID as created in the **Print queues** section in SAFEQ Cloud Web UI. We recommend using the ID of the printer in the IPP URL, so that any potential queue renaming doesn't break any existing client configurations. You can leave out the port and use the default HTTPS port (443) in environments with standard port 443 support.
- Replace **<user-name>** with the user name.
- Replace **<account-domain-fqdn>** with your SAFEQ Cloud domain name.

- Replace **<auth-provider-ID>** with your authentication provider ID as created in the **Authentication** section in SAFEQ Cloud Web UI. This can be useful if your users have the same usernames in different providers.

5. When prompted for the Printer Driver, select the one specified by your administrator, or the SAFEQ Cloud Universal Driver depending on your installation.

6. Fill in user name and password in the printer properties if instructed by administrator.

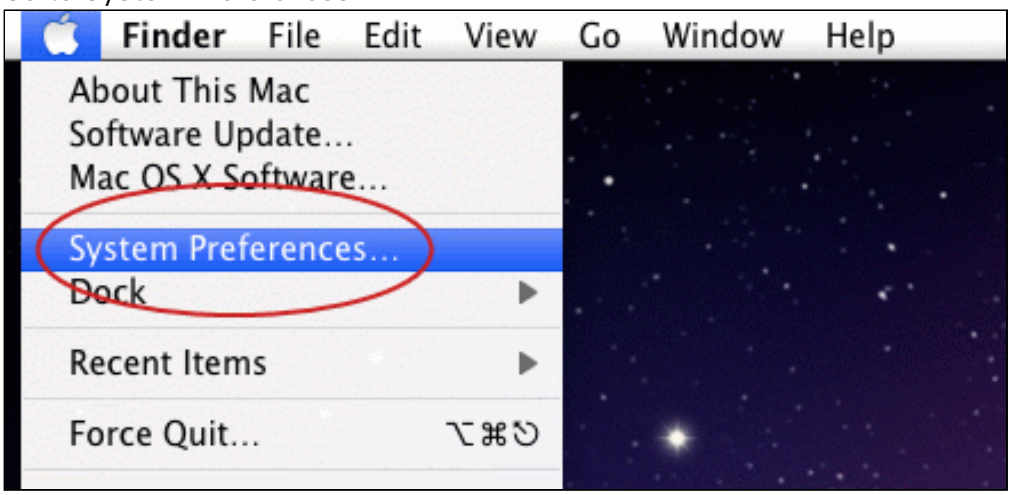


This is essential when the "IPP authentication is mandatory" is enabled in Security options; otherwise, the job will not appear in the print queue.

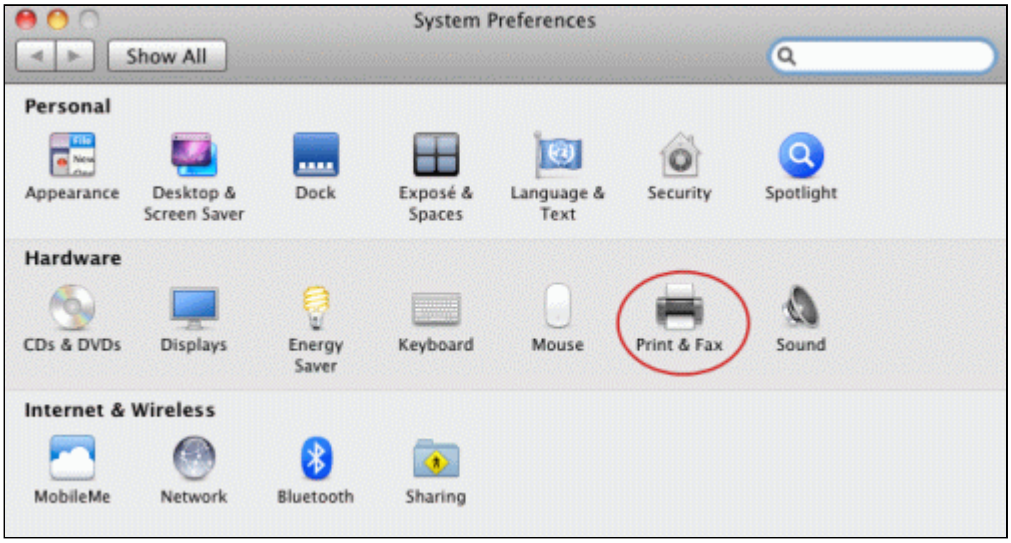
9.1.6 ADDING IPP PRINT QUEUE MANUALLY IN MAC OS

If you are not using the SAFEQ Cloud Client for MacOSX, you can print directly from the programs on your computer, by adding an IPP print queue manually. Your administrator must provide you with the print queue address and with information on which print driver to use. When you have this information, perform the following steps:

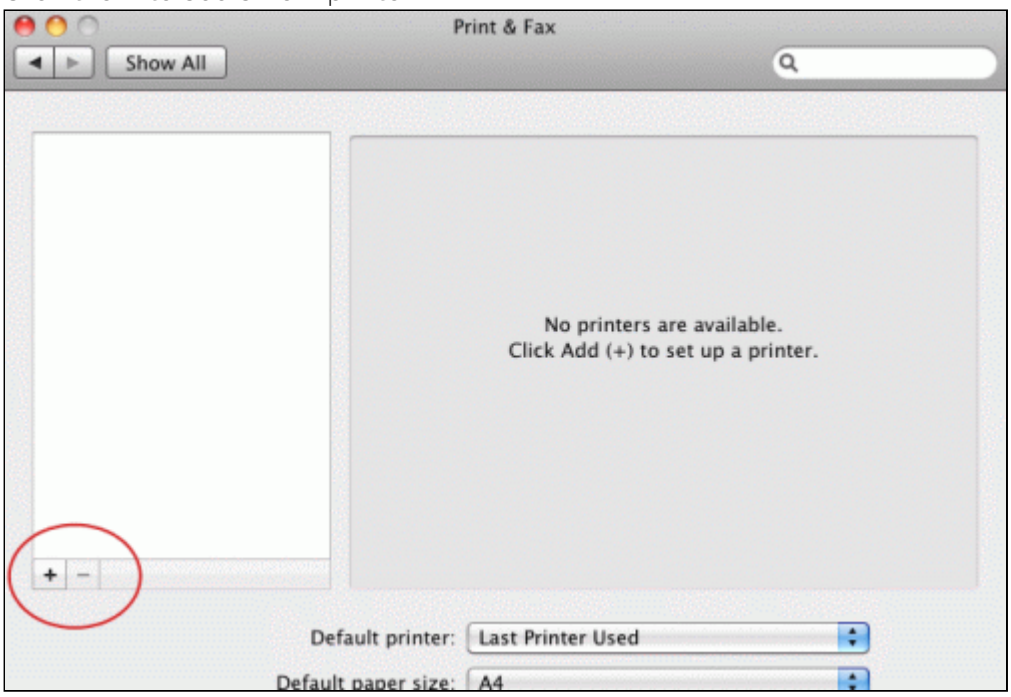
1. Go to System Preferences.



2. Click the Print & Fax icon.

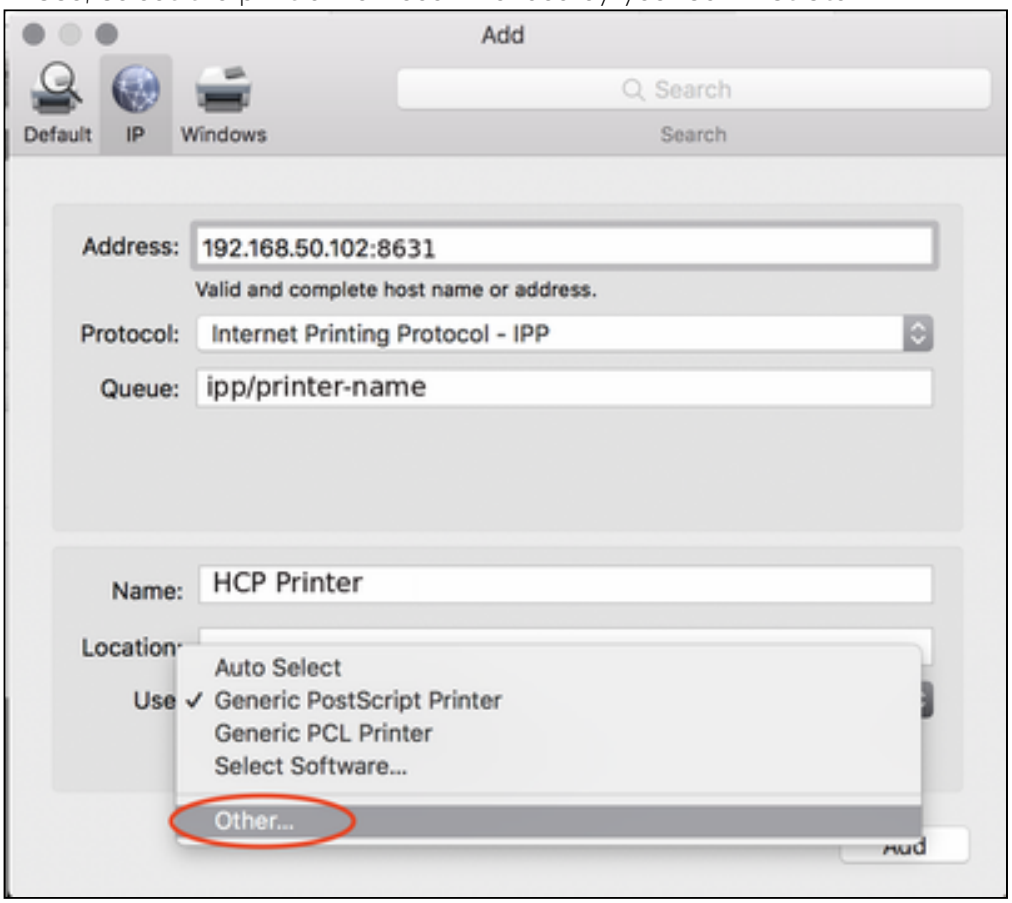


3. Click the + to add a new printer.



4. The Add dialogue window will be displayed. Enter the following:
   a. In Address, enter the print queue address that you received from your administrator.
   b. In Protocol, select Internet Printing Protocol – IPP.
   c. In Queue, enter the queue name that you received from your administrator
   d. In Name, enter a user-friendly name. This name will be visible only to you.

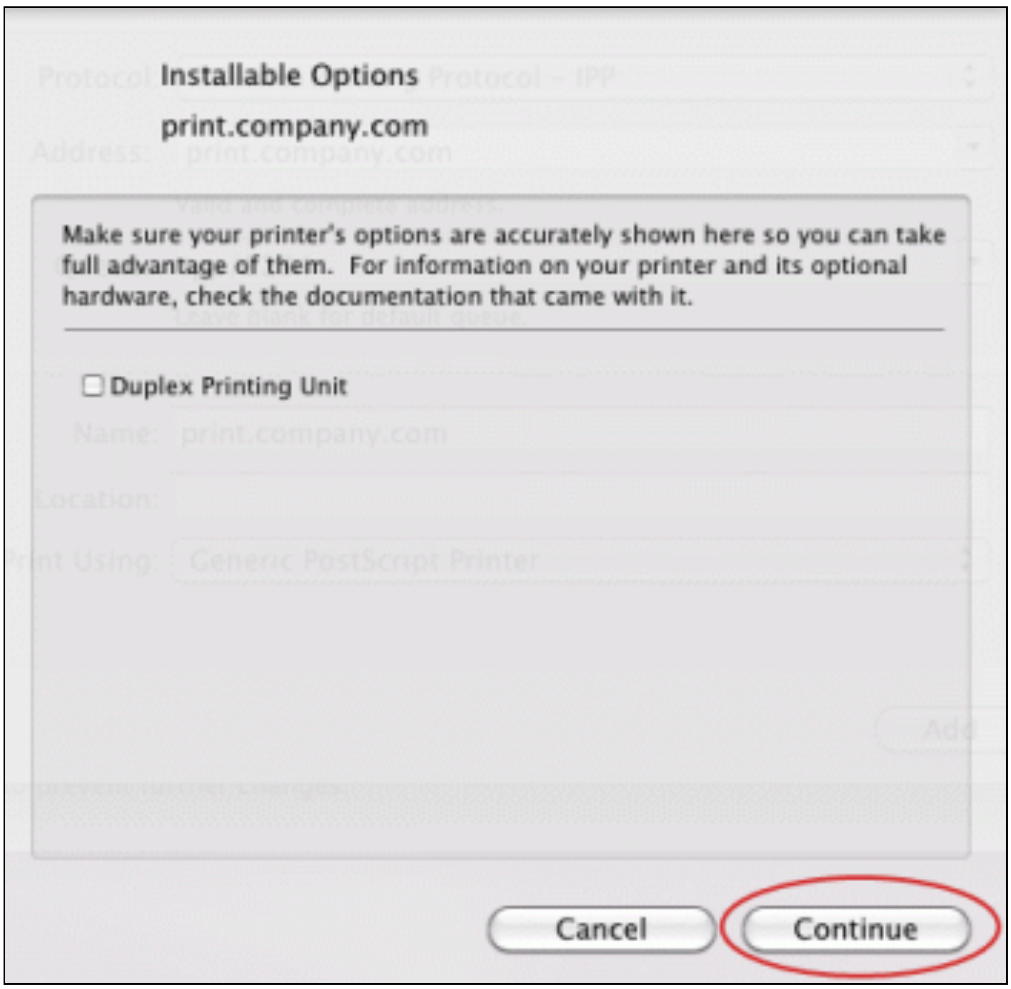
e. In **Use**, select the print driver recommended by your administrator.



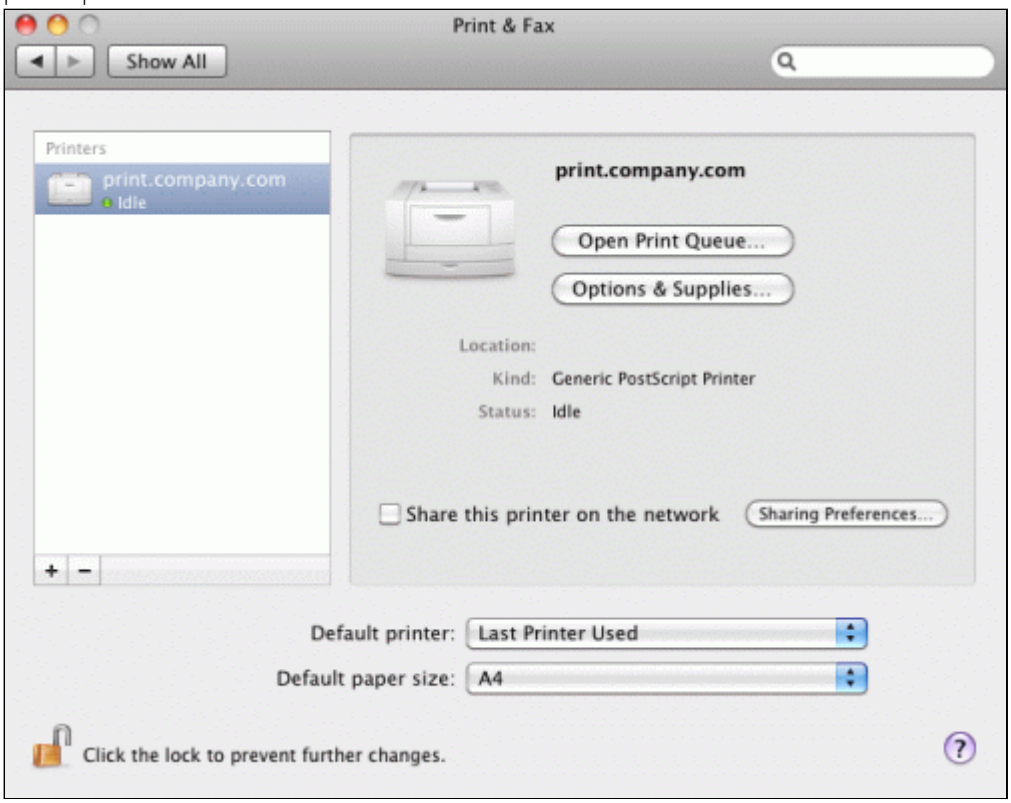
Information for administrators:

- Address: *SAFEQ Cloud-gateway:8631* (or 9631 for HTTPS)
- Queue: *ipp/input-port-name*

5. If a window opens asking about options, click **Continue**.


Installable Options
print.company.com
Make sure your printer's options are accurately shown here so you can take full advantage of them. For information on your printer and its optional hardware, check the documentation that came with it.
Duplex Printing Unit
Cancel
Continue

6. Now you can print from the programs you use. In the **Print** dialogue, select your newly created print queue.



9.1.7 PRINTING FROM SAP

If you wish to print from SAP, you have two options:

1. Add an IPPS queue to your SAP server. See Adding IPP print queue manually in Windows.
2. Print from an SAP client installed on your PC. This way, the client will be able to print to any print queue available on your PC, such as the print queue(s) created by the SAFEQ Cloud Client.

9.2 USING AN MFD

If your company uses card authentication at the MFD, start with Card registration at the MFD.

Each MFD brand and its SAFEQ Cloud terminal is slightly different. Read the manual for the MFD brand you wish to use:

- Using FUJIFILM BI Cloud Terminal
- Using Ricoh Standard Gen 2 Cloud Terminal
- Using HP Workpath Gen 2 Cloud Terminal
- Using Konica Minolta IWS Gen 2 Cloud Terminal

Difference between push printing and pull printing

- Push printing – The print job is released immediately. You are not required to authenticate at the MFD. When you are submitting your document, you must select the MFD where you wish it to be printed. This is done by selecting the Push queue which belongs to the respective MFD.
- Pull printing – You must authenticate at the MFD to make sure you are authorized to release the print job. When submitting the print job, you are sending it to a pull queue and then choosing where to release it by going to any compatible MFD connected to SAFEQ Cloud. The pull queue is not tied to any specific printer. Depending on how your administrator has set up the MFD, you can authenticate via card, PIN/short ID, one-time password, or username/password.

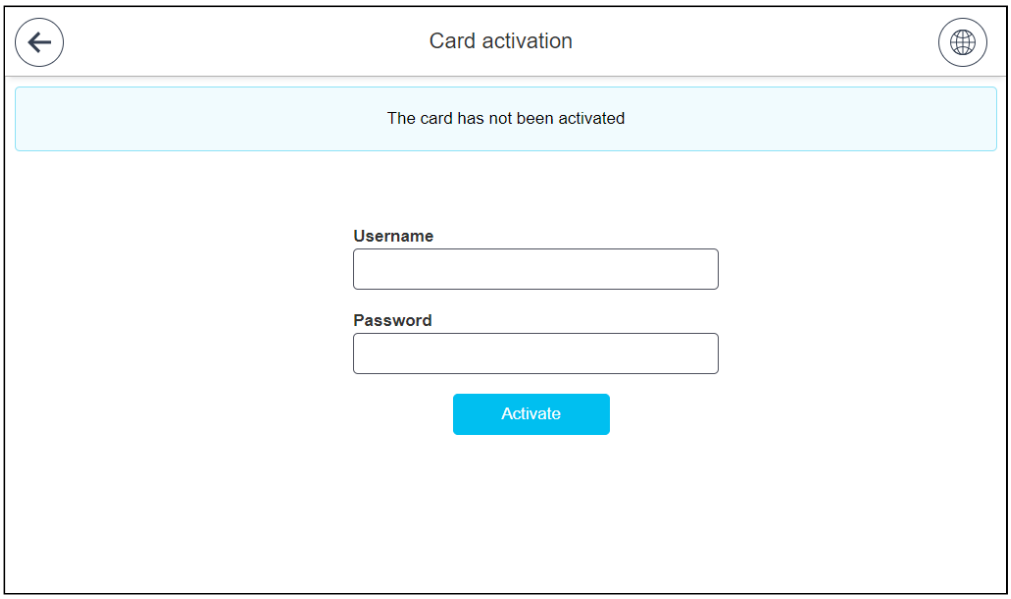
9.2.1 CARD REGISTRATION AT THE MFD

If you are a new user of SAFEQ Cloud and you want to register your card, perform the following steps. If you are an already-existing user who needs to register a new card, follow the same process.

Note that the look of card activation screens may slightly differ, depending on the MFD brand.

1. Go to the MFD of your choice and place your card on the card reader. The terminal will recognize an unassigned card and prompt you to enter your username and password.

   If you don't have a password assigned to your user account, your administrator can generate a one-time-password for you.



2. Tap **Activate**.
3. You will be logged into the device and the new card will be assigned to your user account.

If you have assigned to yourself more cards than the allowed amount, the oldest assigned card will be replaced with a new one.

9.2.2 USING FUJIFILM BI CLOUD TERMINAL

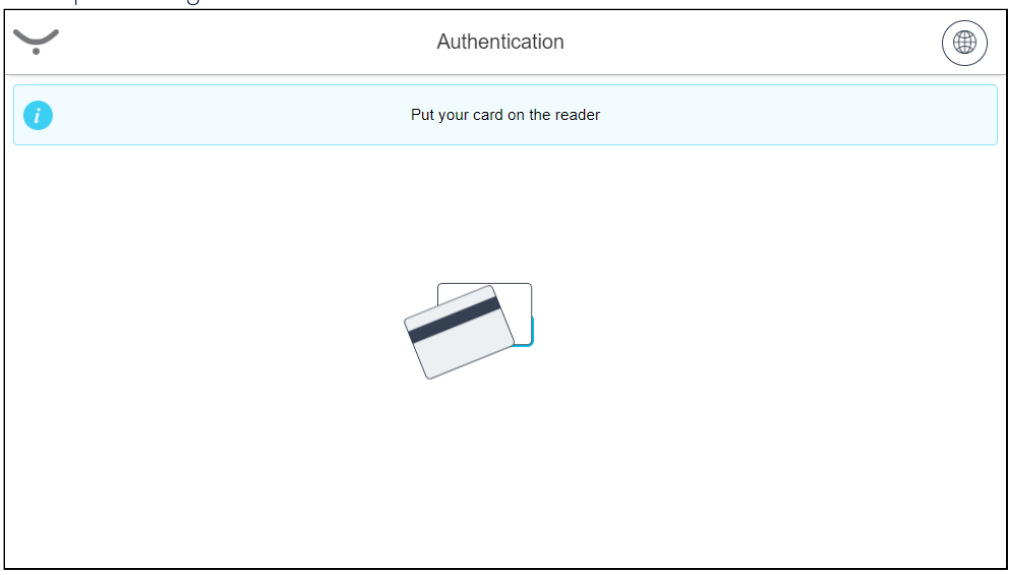
Registering your card

See Card registration at the MFD.

Logging in and out

Logging in

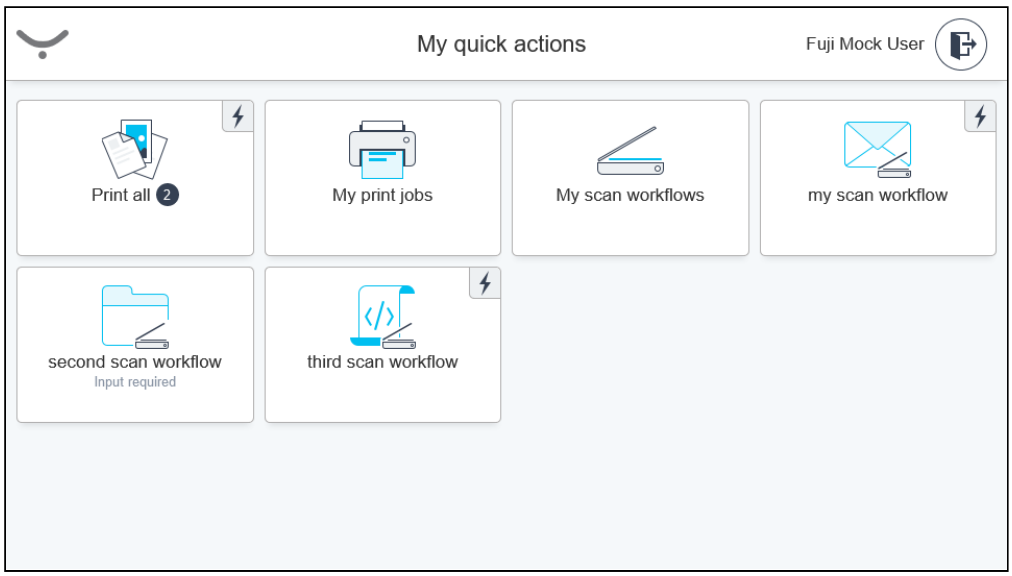
1. The authentication method depends on how your administrator configured the terminal. You can log in via card, PIN (Short ID), username/password, or their combinations. Follow the instructions on the screen.
   Example for login via card:



2. You will see the Cloud Terminal home screen – My quick actions application.
3. If the authentication fails, you will see an error message saying "You have placed unknown or damaged card."
4. If your card is not registered, you will see a message "Your card has not been activated yet." You must register your card. See Card registration at the MFD.

My quick actions application

My quick actions application enables you to access frequently used functions, such as print all jobs or use a scan workflow immediately after login. The quick action buttons are displayed according to your rights and scan workflows assigned to you.

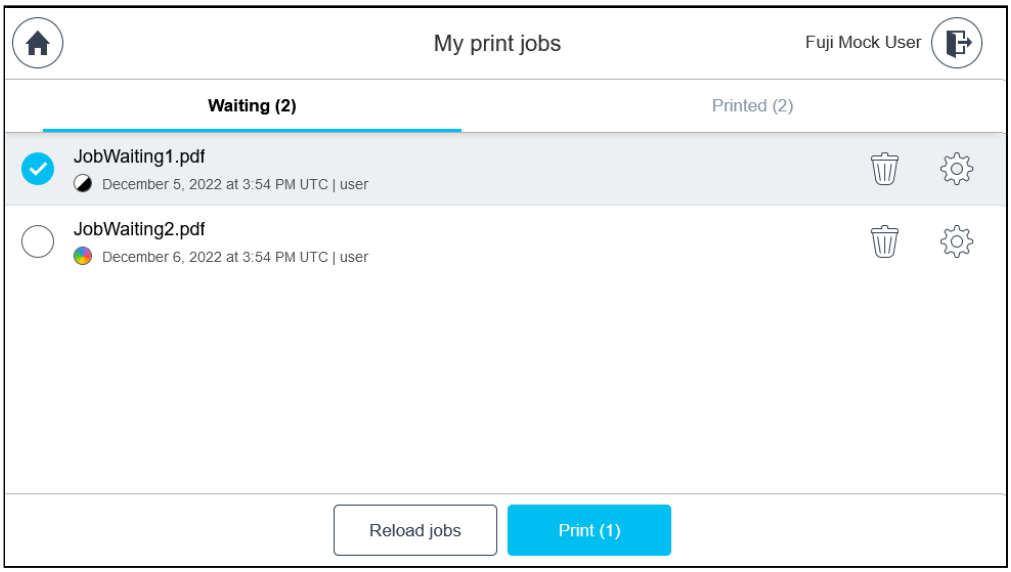


Printing and managing jobs

1. Log in to the Cloud Terminal. You will see **My quick actions** screen.
2. If you wish to release all of your print jobs, tap **Print all**.

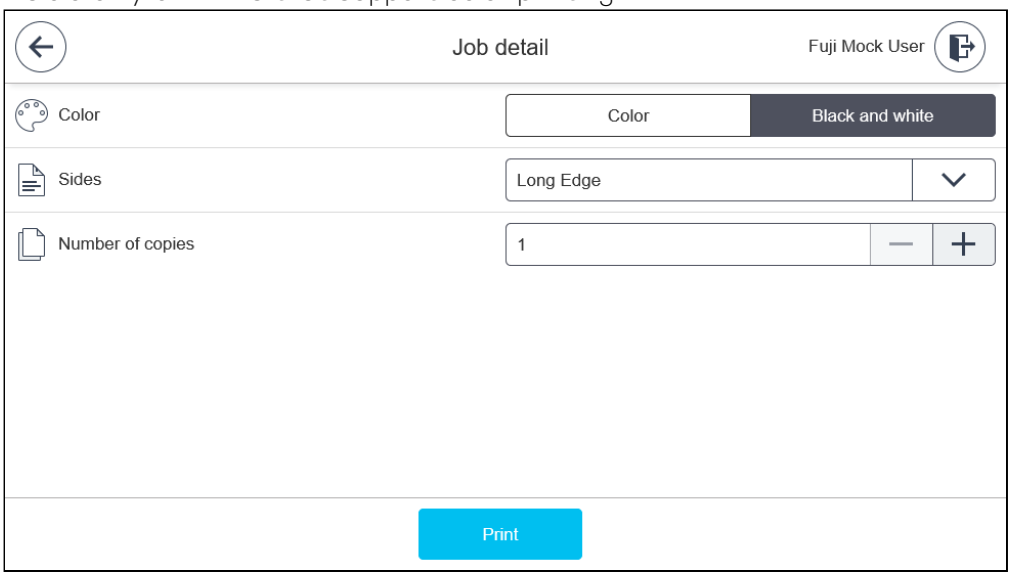
   If there are no jobs to be printed, the **Print all** quick action is greyed out.

3. If you wish to release only specific print job, tap **My print jobs**.
4. Tap the print job.



5. If you wish to modify the finishing options, tap the gear icon next to the job. Modify the **Color**, **Slides**, and **Number of copies** options according to your needs. Note that the Color option is

visible only on MFDs that support color printing.



6. Tap **Print**.
7. If new jobs are sent during your current MFD session, you can load them by tapping **Reload jobs** on **My print jobs screen**.
8. If you wish to delete a print job, tap the trash bin icon next to it.
9. After tapping **Print**, you will see an overlay showing the overall progress and the status of the currently processed job. The status can show one of the following values:
   - **Waiting** – The job is yet to be processed.
   - **Printing** - SAFEQ Cloud tries to print the document from any location that has network visibility to the printer. Without network visibility, the print method will change to Downloaded and printing.
   - **Downloading** - the downloaded print job(s) is being downloaded by the Cloud Terminal.
10. If some of the print jobs had to be downloaded for printing or when the Cloud Terminal waits for the finalization of the print job(s) by the MFD, the following message will appear: "All jobs were sent to the printer. Waiting for printing to end."
11. After the last job has been delivered, the following success message will appear: "Your print jobs have been sent to the printer."
12. If any job fails to be printed, a screen with the following error message will appear: "X/Y jobs failed to print. Please try again or contact your administrator."

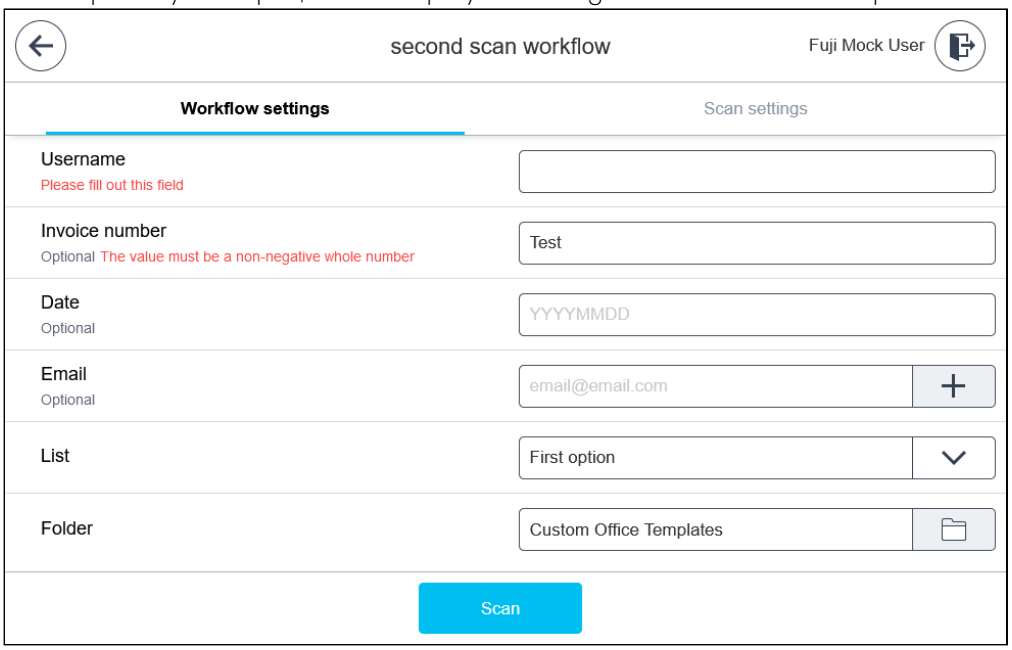
Scanning

1. You can run scan workflows from **My quick actions** screen or from **My scan workflows** screen.

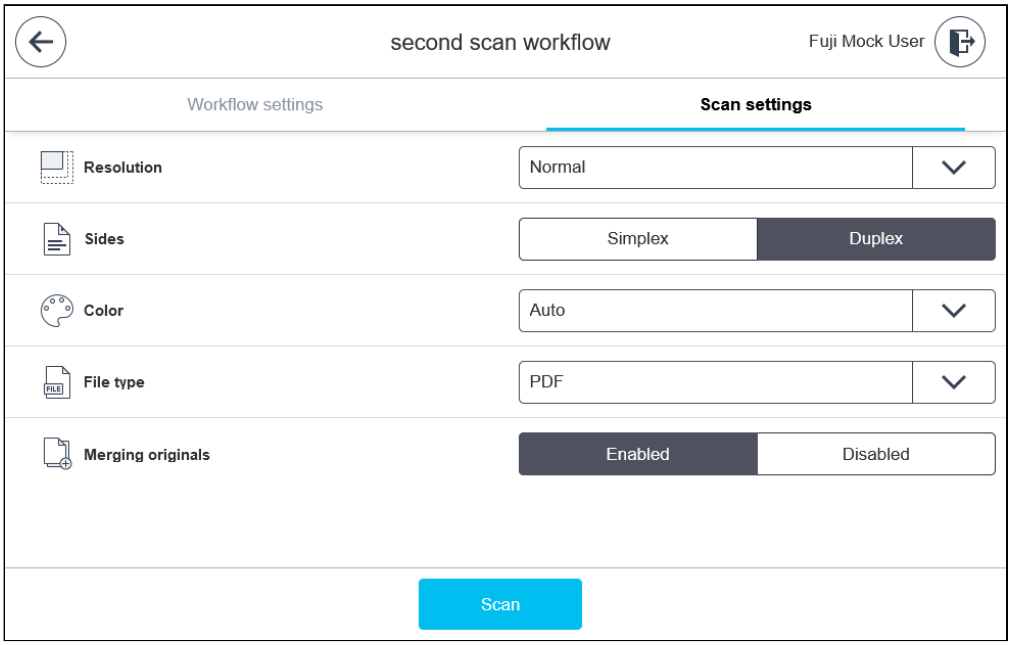
> If no scan workflows are available to you or if scanning is disabled on the device, you will see an error message: "No scanning workflows available. If the problem persists contact the administrator."

a. **My quick actions** screen displays the first three workflows from all scan workflows that your administrator made available to you. Tap the workflow you wish to execute.

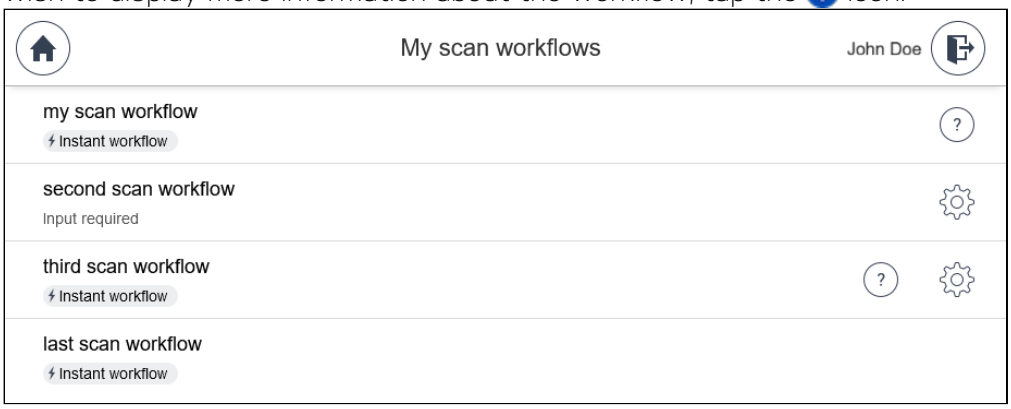
1. If it is an instant workflow, it will start immediately.
2. If it requires your input, it will display a settings menu. Fill in the required information.



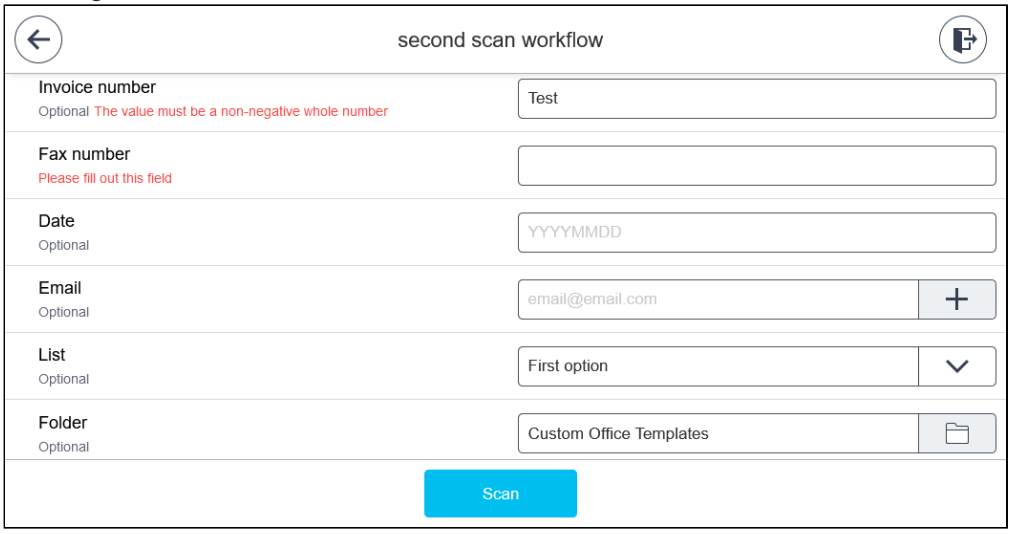
3. Tap the **Scan settings** tab to modify the can settings according to your needs. Note that you will only be able to view and modify the settings that your administrator has allowed.



b. **My scan workflows** screen displays the list of all scan workflows available to you. If you wish to display more information about the workflow, tap the ? icon.

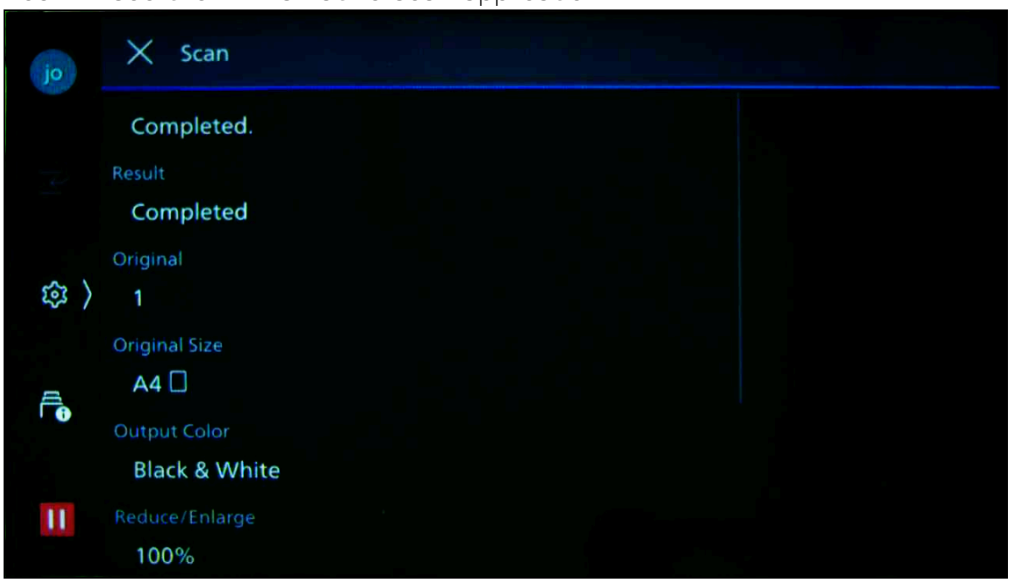


c. Tapping the workflow marked **Input required** or tapping the cog icon will open the workflow settings. Fill in the required information. For some of the parameters, a new dialog window will open, allowing you to search emails, browse folders or lists the available options. If the terminal fails to fetch emails or directory structure, you will see an "Unexpected error" error message.



d. Tap **Scan**.

2. You will see the MFD's native scan application.



3. When the physical scanning finishes, you will see once again the Cloud Terminal application displaying the progress of the document upload.

4. If your document was correctly scanned and uploaded to SAFEQ Cloud, you will see a success message. If there is a problem, you will see an error message "Your scan job failed. Please try again or contact your administrator."

9.2.3 USING HP WORKPATH GEN 2 CLOUD TERMINAL

Registering your card

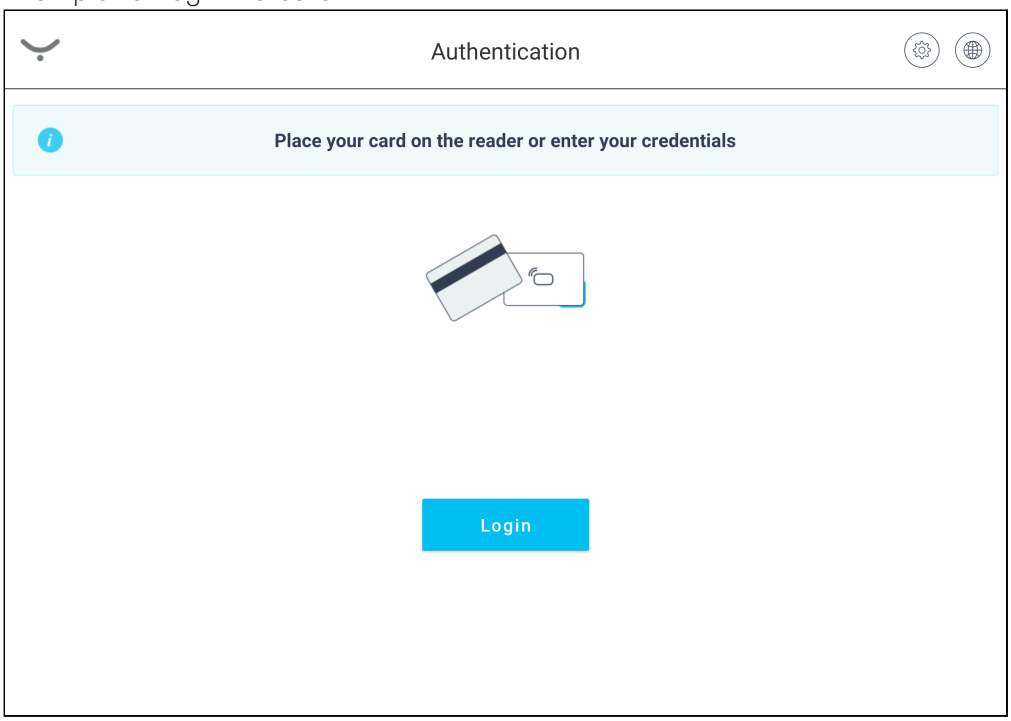
See Card registration at the MFD

Logging in and out

Logging in

1. The authentication method depends on how your administrator configured the terminal. You can log in via card, PIN (Short ID), username/password, or their combinations. Follow the instructions on the screen.

Example for login via card:



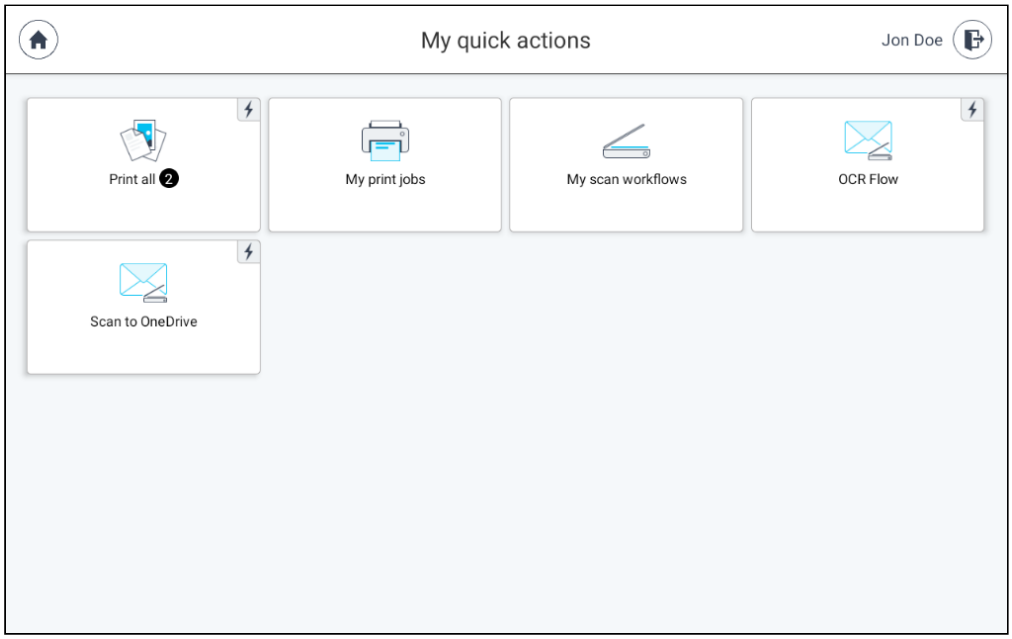
2. You will see the Cloud Terminal home screen – My quick actions application.

Logging out

Tap the logout button in the top-right corner of the screen.

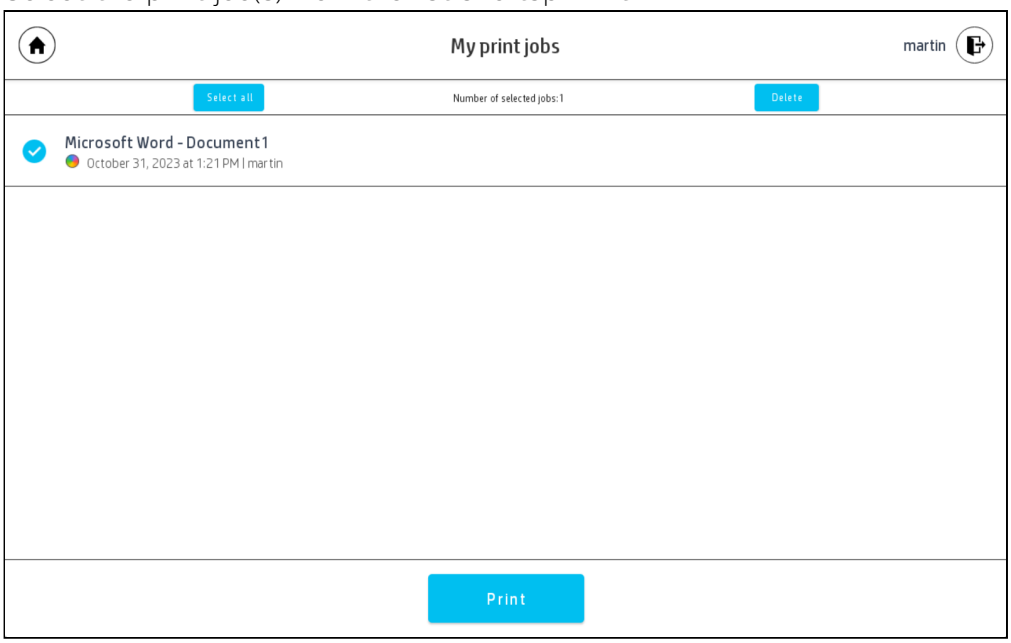
My quick actions application

My quick actions application enables you to access frequently used functions, such as print all jobs or use a scan workflow immediately after login. The quick action buttons are displayed according to your rights and scan workflows assigned to you.



Printing and managing jobs

1. Log in to the Cloud Terminal. You will see **My quick actions** screen.
2. If you wish to release all of your print jobs, tap **Print all**.
3. If you wish to release only specific print job, tap **My print jobs**.
4. Select the print job(s) from the list and tap **Print**.



> Jobs that you have insufficient rights to print or jobs that cannot be printed on your selected MFD will be marked as **Unavailable**.

5. If you wish to modify the finishing options such as color, sides and the number of copies, tap the gear icon next to your selected print job.

> Modifying finishing options on terminal is only possible with jobs sent via one of the SAFEQ Cloud supported methods (e.g., using a PC client / SAFEQ Cloud Universal print driver, Chrome extension, SAFEQ Cloud mobile app, or web upload).

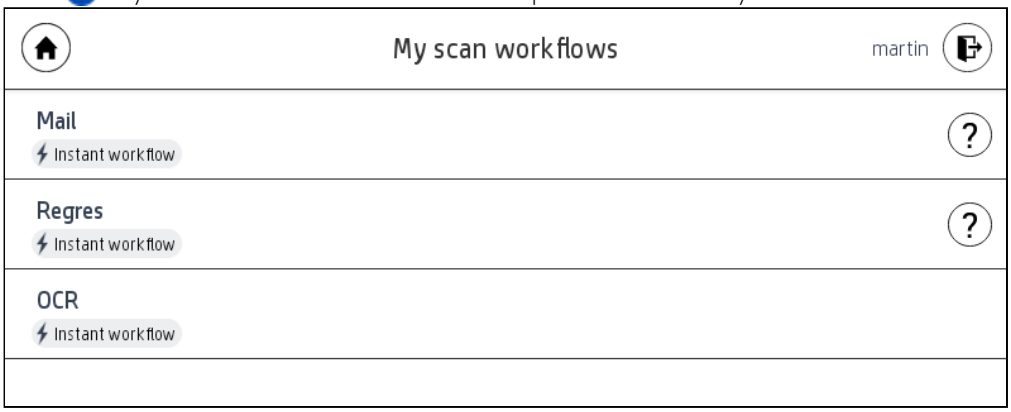
6. After tapping **Print**, you will see an overlay showing the overall progress and the status of the currently processed job. The status can show one of the following values:
   - **Printing** - SAFEQ Cloud tries to print the document from any location that has network visibility to the printer. Without network visibility, the print method will change to **Downloaded and printing**.
   - **Downloading and printing** - the downloaded print job(s) is being printed by the Cloud Terminal.
7. When the printing is finished, you will see a success message.

8. If a problem occurs, the **Could not retrieve job data from the server** error message is displayed.

Scanning

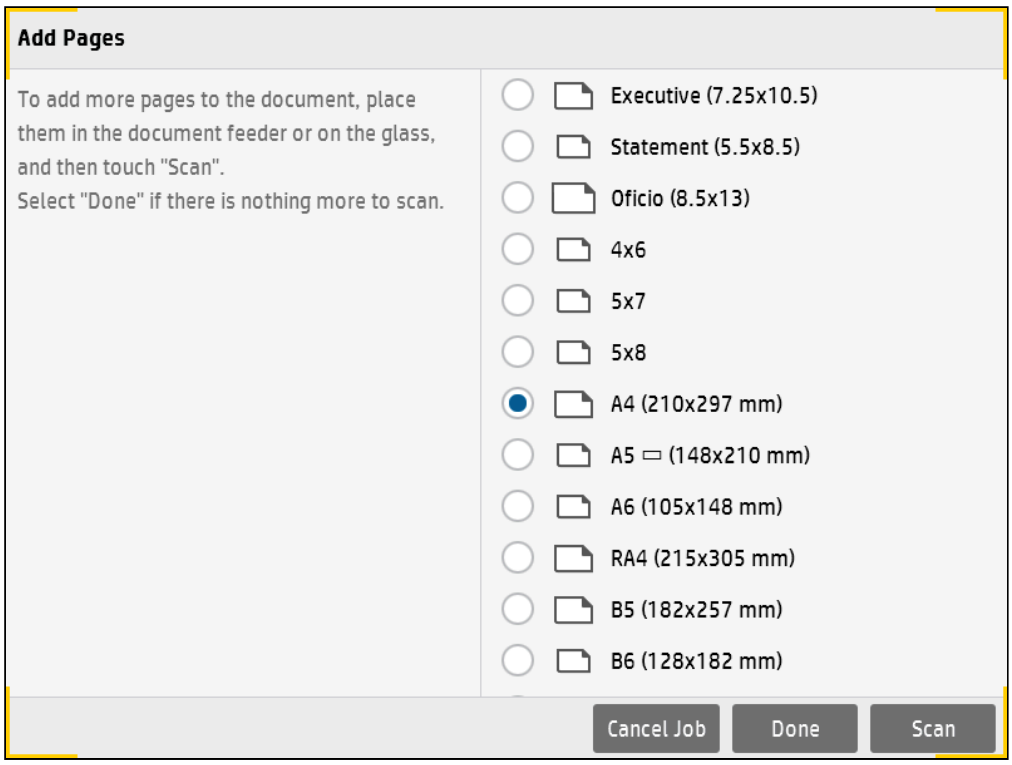
> Workflows that require user input aren't currently supported. Such workflows will appear as grayed out.

1. You can run scan workflows from **My quick actions** screen or from **My scan workflows** screen.
2. **My quick actions** screen displays the first three workflows from all scan workflows that your administrator made available to you. Tap the workflow you wish to execute. The workflow will start immediately.
3. **My scan workflows** screen displays the list of all scan workflows available to you. Tap the info icon if you wish to see the details. Tap the workflow you wish to execute.



4. You will see the scan progress screen. Tap **Stop** if you wish to cancel the scanning.
5. If no problem occurs, you will see a success message.

If the merging originals feature is enabled in the scan workflows settings, you will be prompted to add more pages and choose the size of the pages:



If the sides are set to duplex in the scan workflows settings, you will be prompted to turn the page over to scan the back side:

9.2.4 USING KONICA MINOLTA IWS GEN 2 CLOUD TERMINAL

Registering your card

See Card registration at the MFD.

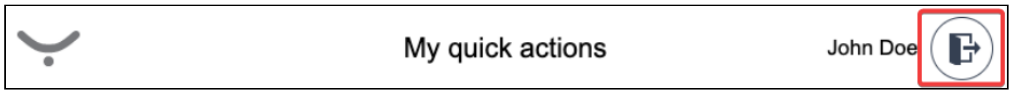
Logging in and out

Logging in

The authentication method depends on how your administrator configured the terminal. You can log in via card, PIN (Short ID), username/password, or their combinations. Follow the instructions on the login screen.

Logging out

Tap the logout button in the top right-hand corner of the screen.

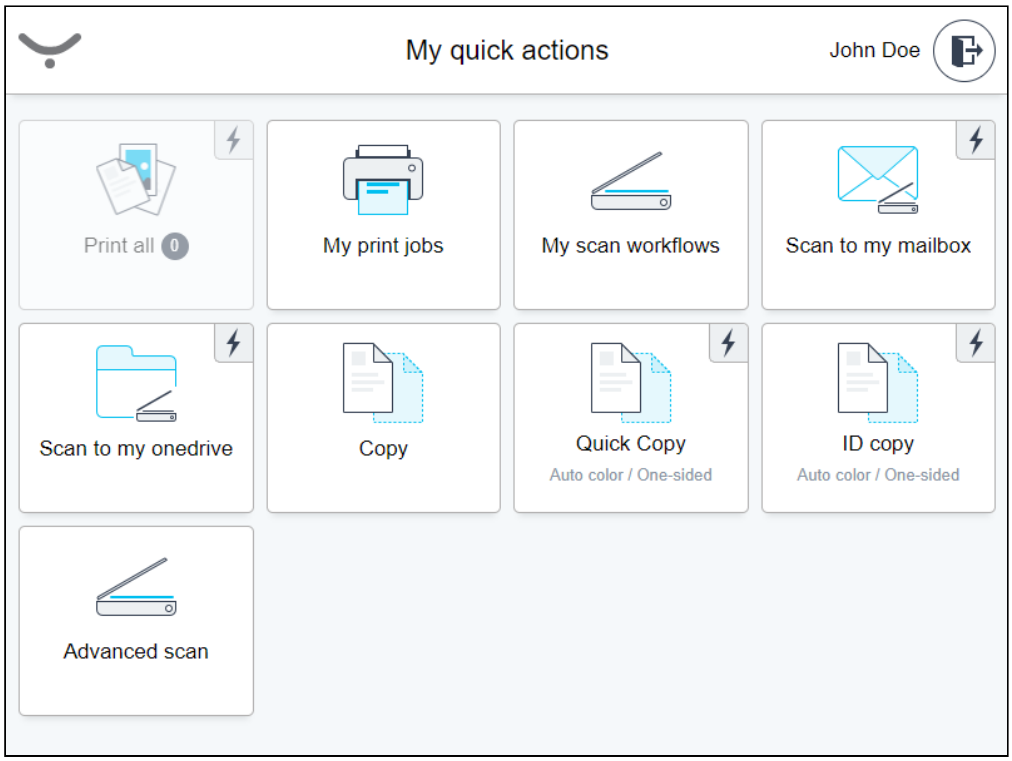


If the terminal is configured to use authentication by card, you can also log out by placing your card on the card reader.

My quick actions application

My quick actions application enables you to access frequently used functions, such as print all jobs or use a scan workflow immediately after logging in. The quick action buttons are displayed according to your rights and scan workflows assigned to you.

If a button has a small flash icon in the top-right corner, it means that the action will be executed immediately after you tap the button. No other screen or confirmation action will be displayed.



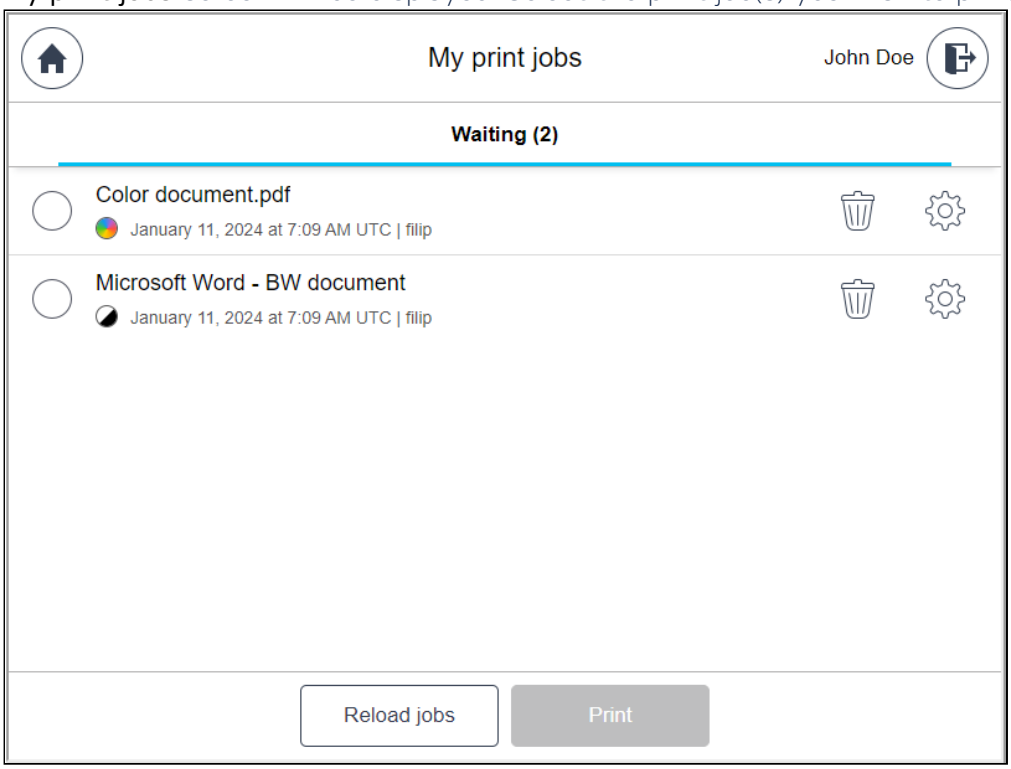
Printing and managing jobs

1. Log in to the SAFEQ Cloud Cloud Terminal. You will see **My quick actions** screen.
2. If you wish to release all of your print jobs, tap **Print all**.

   If you have no jobs to be printed, this button is greyed out.

3. If you wish to release only specific print jobs, tap **My print jobs**.

4. **My print jobs** screen will be displayed. Select the print job(s) you wish to print from the list.



5. If you wish to modify the finishing options such as color, sides and the number of copies, tap the gear icon next to your selected print job.

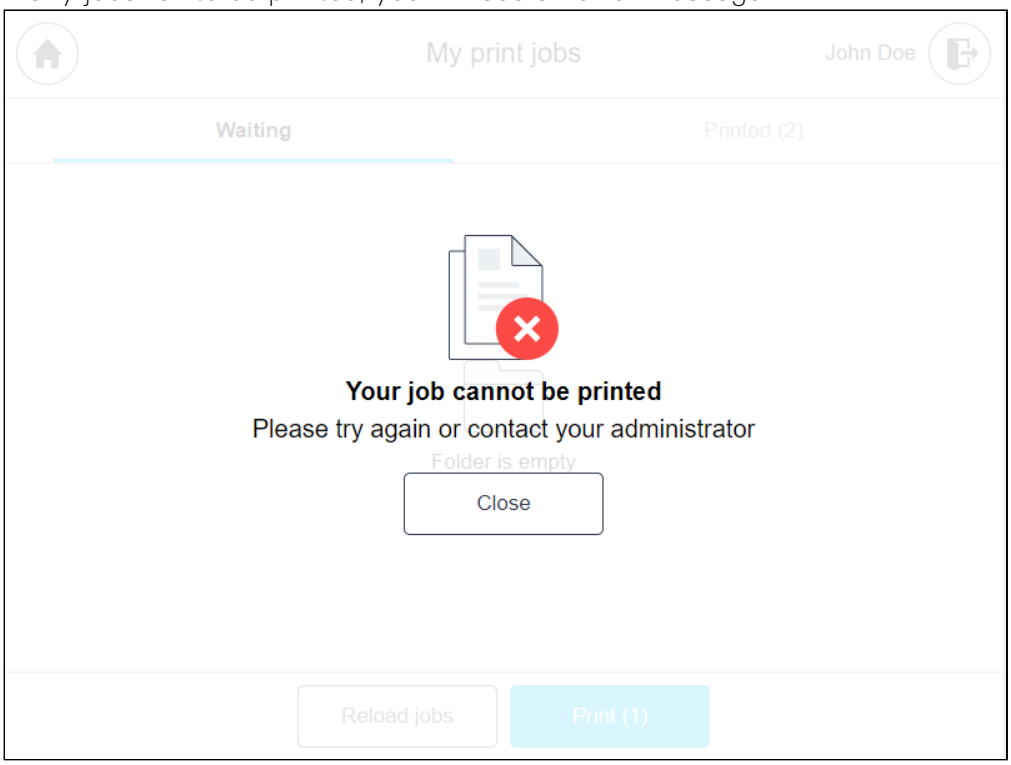
> Modifying finishing options on terminal is only possible with jobs sent via one of the SAFEQ Cloud supported methods (e.g., using a PC client / SAFEQ Cloud Universal print driver, Chrome extension, SAFEQ Cloud mobile app, or web upload).

6. Tap **Print**.

> Print jobs that the MFD cannot print or that you do not have rights to print will be marked as **Unavailable**.

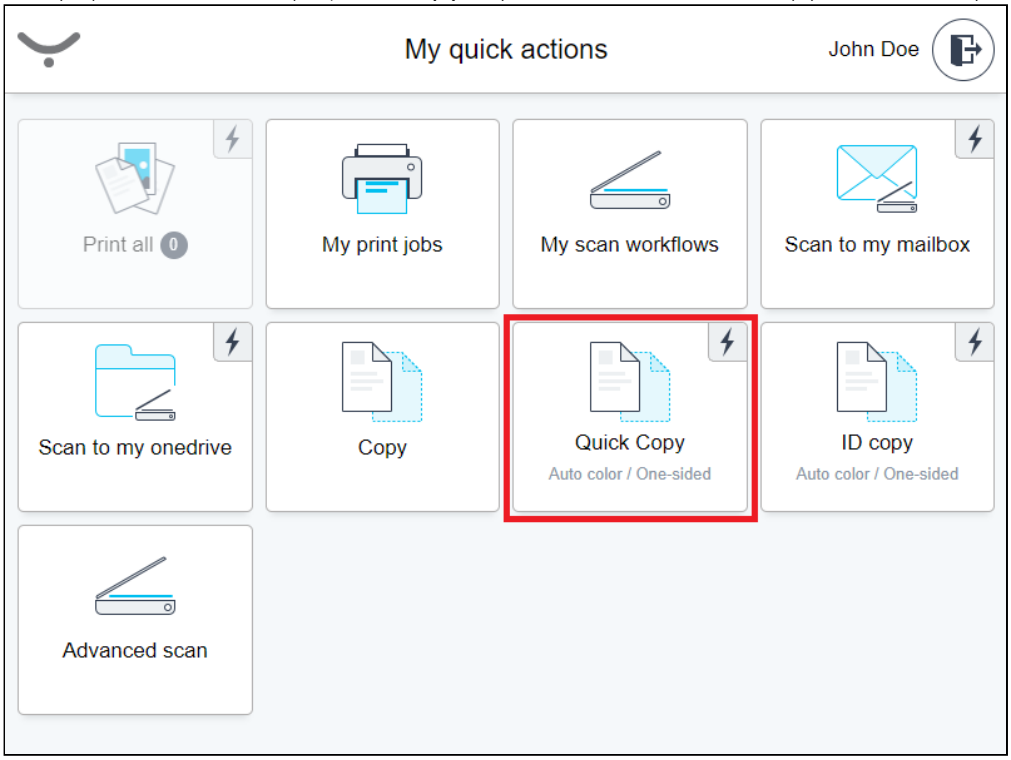
7. If you have sent new print jobs during your current session at the MFD, tap **Reload jobs**.
8. After tapping **Print**, you will see a status screen with progress.
9. When the printer downloads the last print job, you will see a message "Job sent for print."

10. If any jobs fail to be printed, you will see an error message.



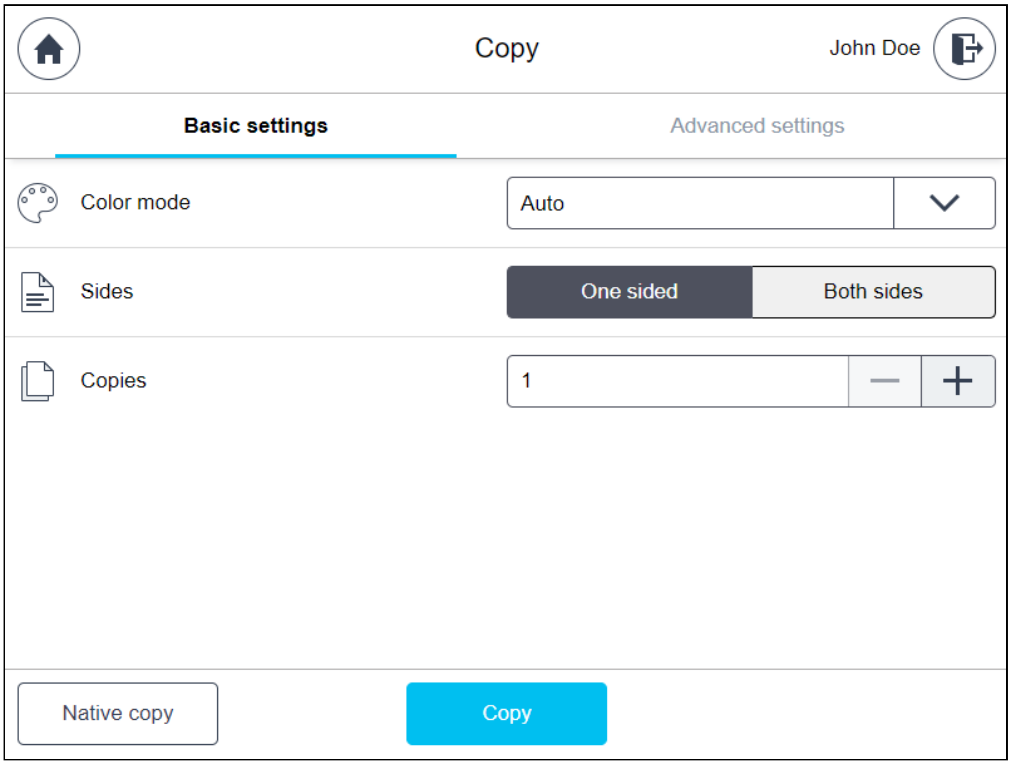
Copying

1. In My quick actions, tap **Quick Copy** if you wish to make a copy without any settings.



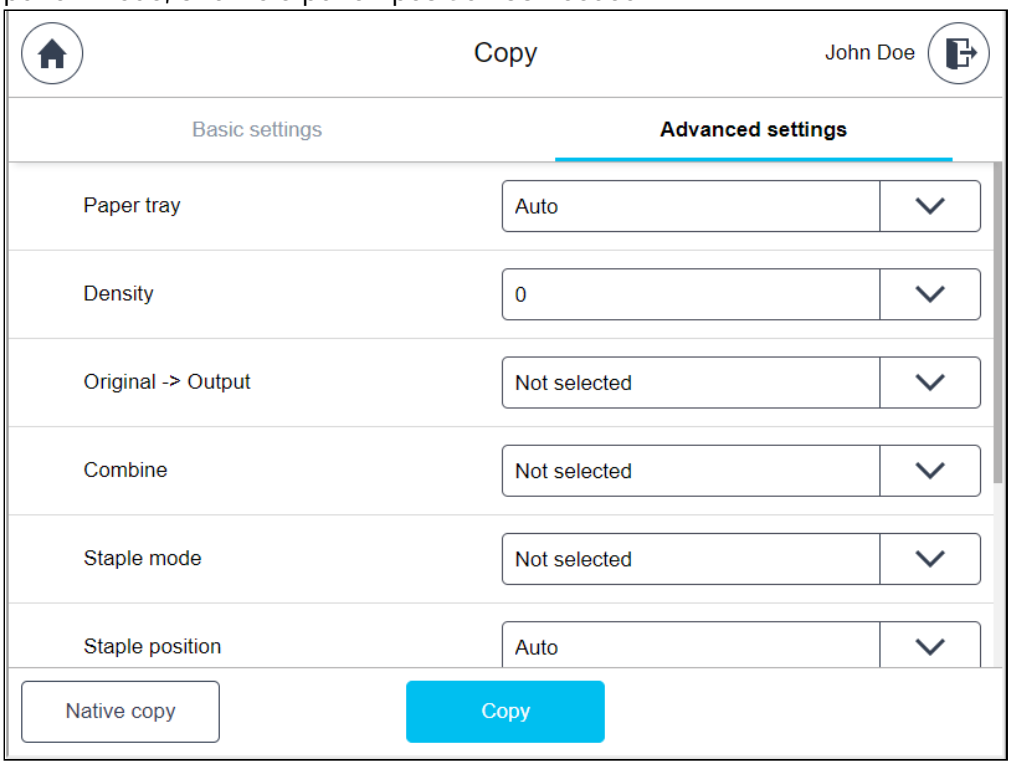
2. If you wish to modify the copy settings, tap **Copy**.
3. Adjust the **Color mode**, **Sides,** and **Number of copies** as needed.

The default **Color mode** value is **Auto**. It automatically detects the color of an original, chooses the proper color, and accounts copied pages accordingly. If the device is not capable of color copying, the BW option is automatically preselected and the user can not see the **Color** mode option.



4. If you need more settings, tap the **Advanced settings** tab and adjust **Paper tray**, **Paper size**, **Density**, **Original -> Output**, **Combine**, **Staple mode**, **Staple position**, **Staple angle**, **Zoom**, **Hole**

punch mode, and Hole punch position as needed.



Only settings supported by the MFD will be displayed.

5. Tap **Copy**.

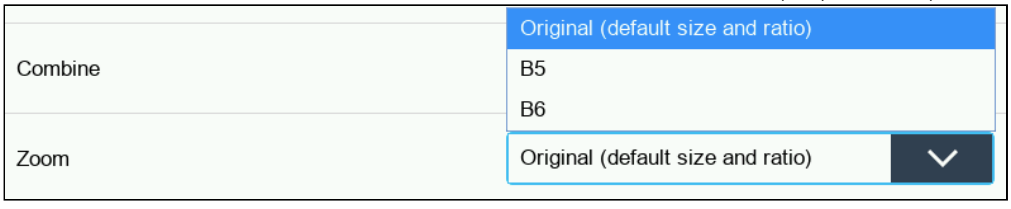
Your administrator may have also configured the **ID Copy** quick action. This instant action allows you to copy both sides of your ID/IC card and print them out on one sheet of paper.

Zoom

The **Combine** and **Zoom** functions cannot be used at the same time.

The **Zoom** function employs automatic zooming based on MFD available paper trays and your selected **Paper tray**. **Zoom** options are displayed depending on the selected **Paper tray** options:

- If **Paper tray** is set to **Auto** (the default option) the **Zoom** options are determined by the paper tray sizes available at the MFD. This means that if the device has paper trays with different size formats, such as A3, A4, and B5, those sizes will be displayed as options for Zoom.



- If **Paper tray** is set to a specific tray, then the **Zoom** option will be limited to the selected tray's paper size.

- If **Paper tray** is set to **Manual** (meaning the manual override paper tray is selected as the input paper tray), then the **Zoom** behavior will be dependent on the selection of the **Paper size** option:
  - if **Paper size** is set to **Auto**, the **Zoom** option will also contain the **Auto** option.
  - If **Paper size** is set to a specific paper size, the **Zoom** option will also contain that selected paper size.

By selecting any **Zoom** option, the original document will be auto-rotated (if the MFD supports that), and the copy will be printed on the selected paper size and zoomed to match its dimensions.

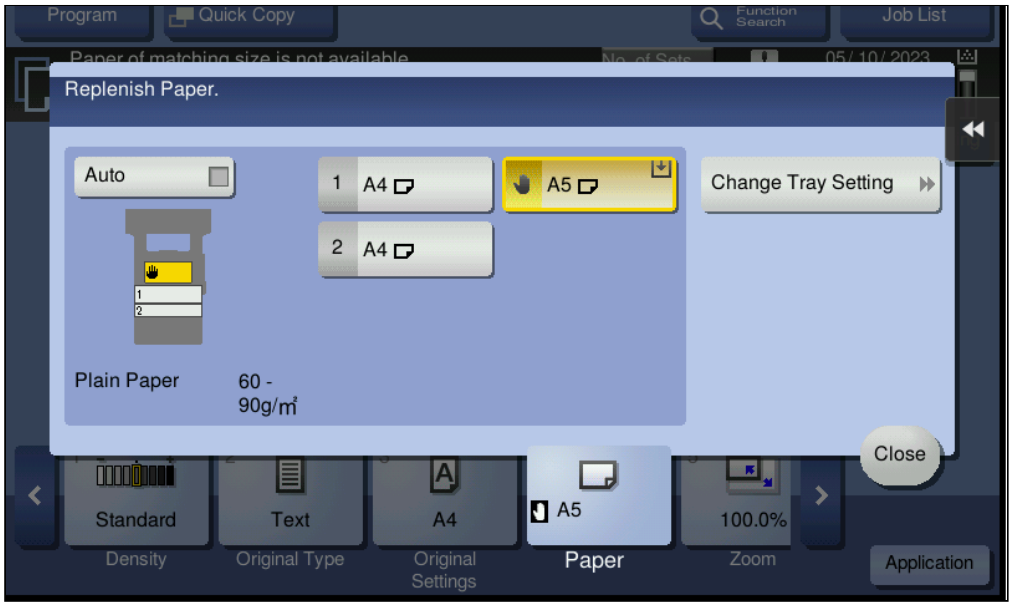
The **Zoom** function supports the following paper sizes: A0, A1, A2, A3, A4, A5, A6, B0, B1, B2, B3, B4, B5, B6, LETTER, LEGAL, EXECTIVE, LEDGER.

Example:

- If the detected original document size is **A4**, the selected **Paper tray** is **Auto**, and the selected **Zoom** is **A3**, the copy will be zoomed to **A3.**
- if the detected original document size is **A3**, the selected **Paper tray** is **Auto**, and the selected **Zoom** is **B6**, the copy will be scaled down to **B6.**
- if the detected original document size is **A4**, the selected **Paper tray** is **Manual**, the selected **Paper size** is **Auto**, the user loaded *A5* into the manual feeder/tray override, and the selected **Zoom** is **Auto**, the copy will be scaled down to **A5**.

Note that for some MFDs, you must set the paper tray sizes manually in the Native copy application before you can use them in the Cloud Terminal.

Navigate to **Copy** > **Paper** > **Change Tray Setting**, and configure the paper sizes before first use.

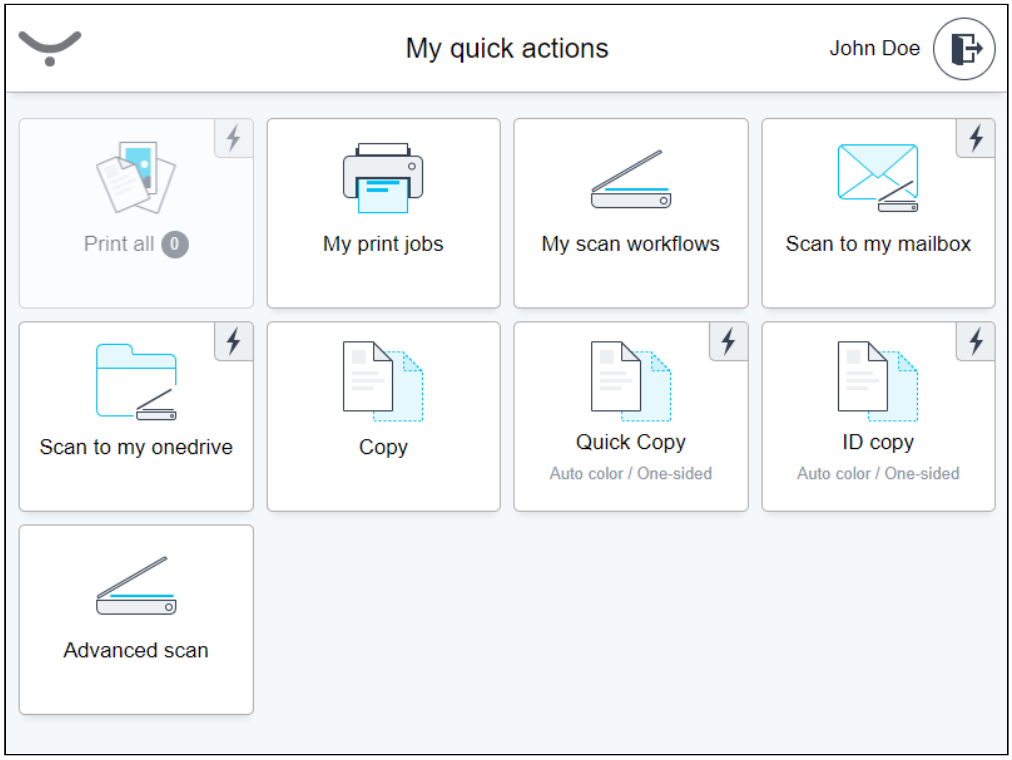


For the **Zoom** function to work correctly, the auto-rotate feature must be supported by the MFD and should not be restricted for use by users. Administrators can check this at the MFD in **Utility** > **Administrator Settings** > **System Settings** > **Restrict User Access** > **Restrict Operation**.

Scanning

Using quick scan workflows

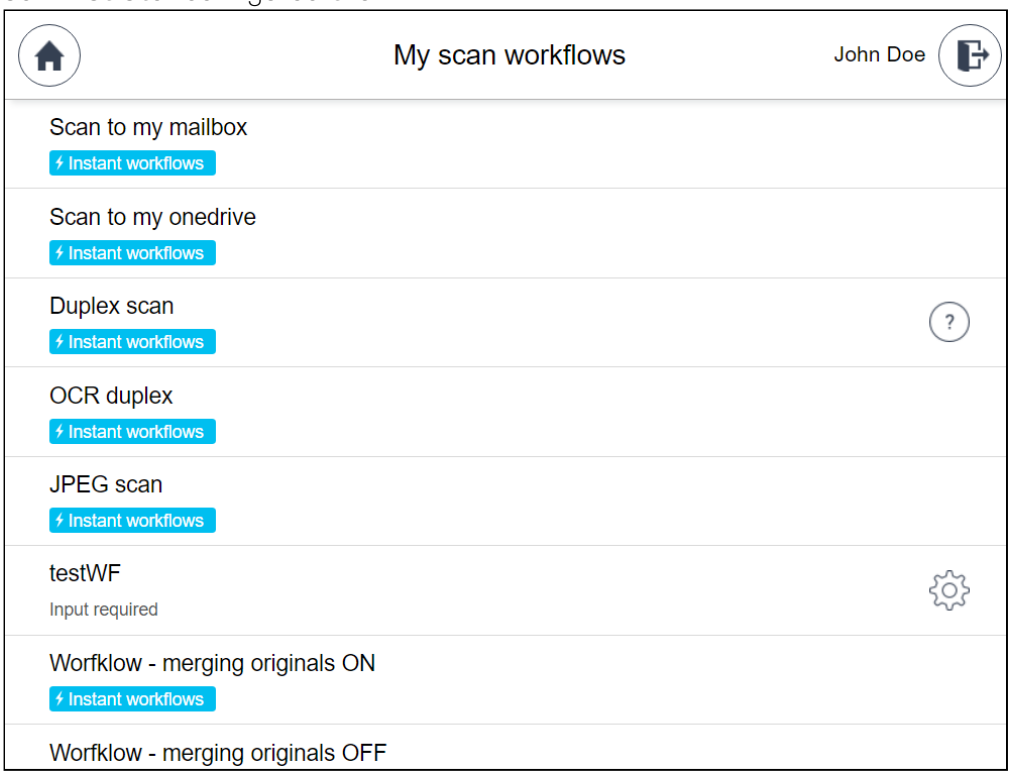
Log in to the terminal and tap any of the available quick scan workflows (tiles between **My scan workflows** and **Copy**).



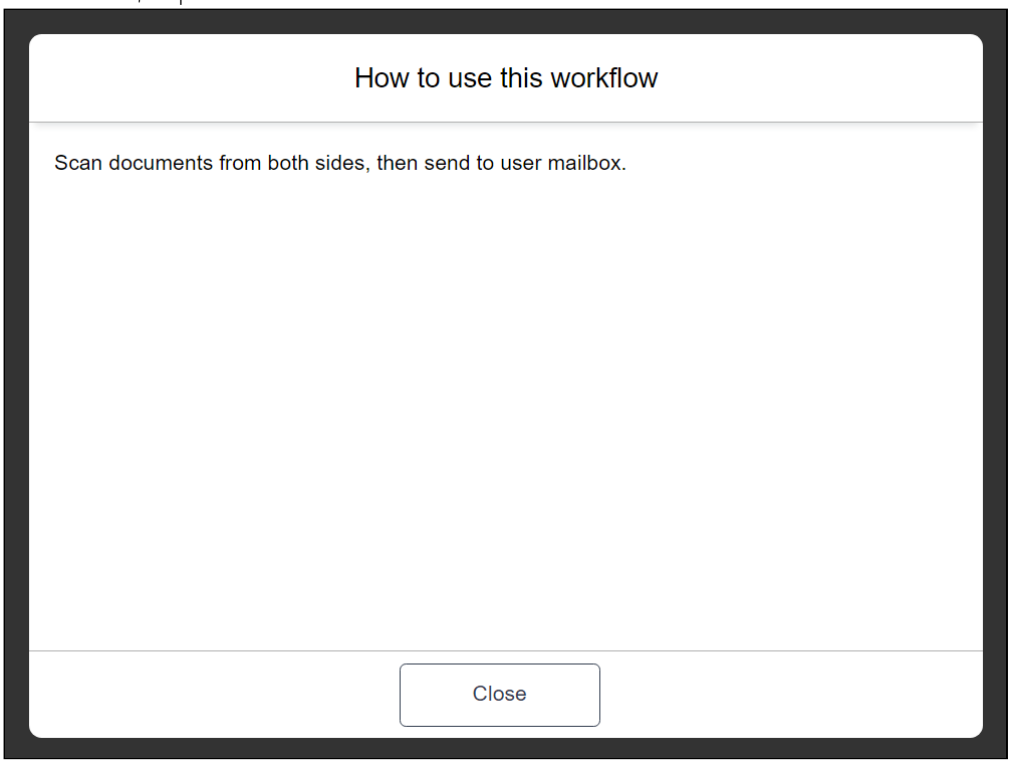
Using all available scan workflows

1. Log in to the terminal and tap **My scan workflows**. The list of all available scan workflows will be displayed. Note that some workflows may have only **Workflow settings** available, some may have only the **Scan settings** available, and some may have both. This depends on how your

administrator configured them.

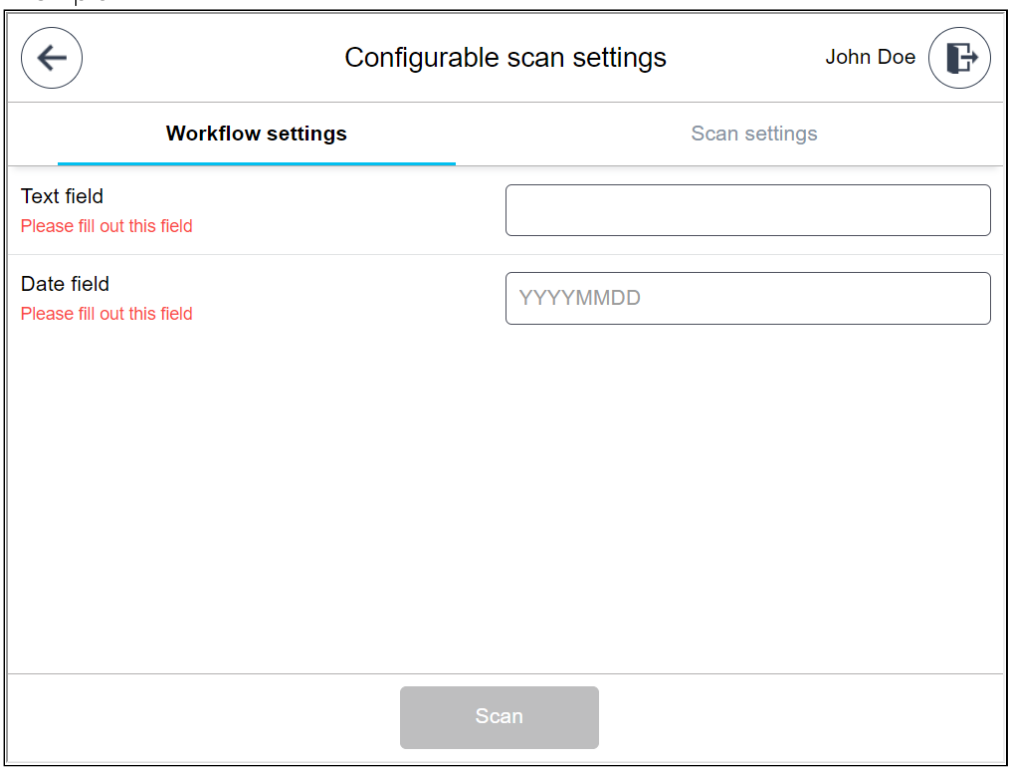


2. The question mark icon on the right side of a scan workflow shows there is more information about the workflow. Tap the icon to display the information. To get back to the list of scan workflows, tap the **Close** button.



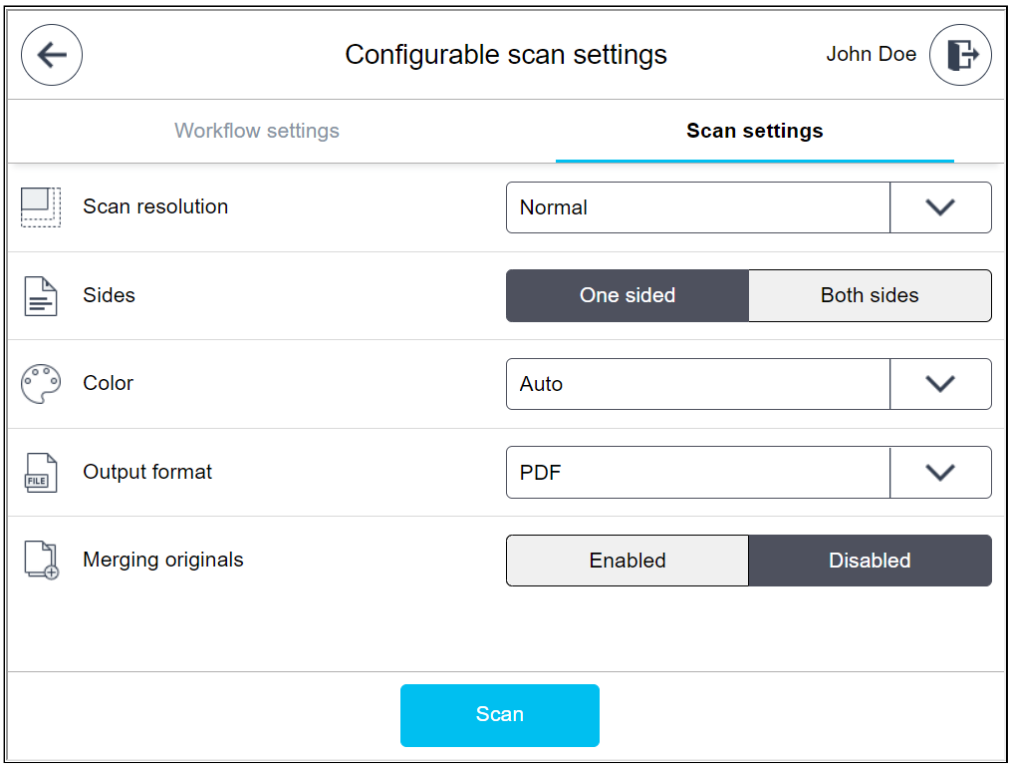
3. To use a specific workflow, tap anywhere in the row with the desired scan workflow. If some input is required for a specific scan workflow, you will see a screen with **Workflow settings**.

Example:



4. If your administrator configured the workflow to allow you to change the scan settings, you will see the **Scan settings** tab. Tap it to modify the settings.

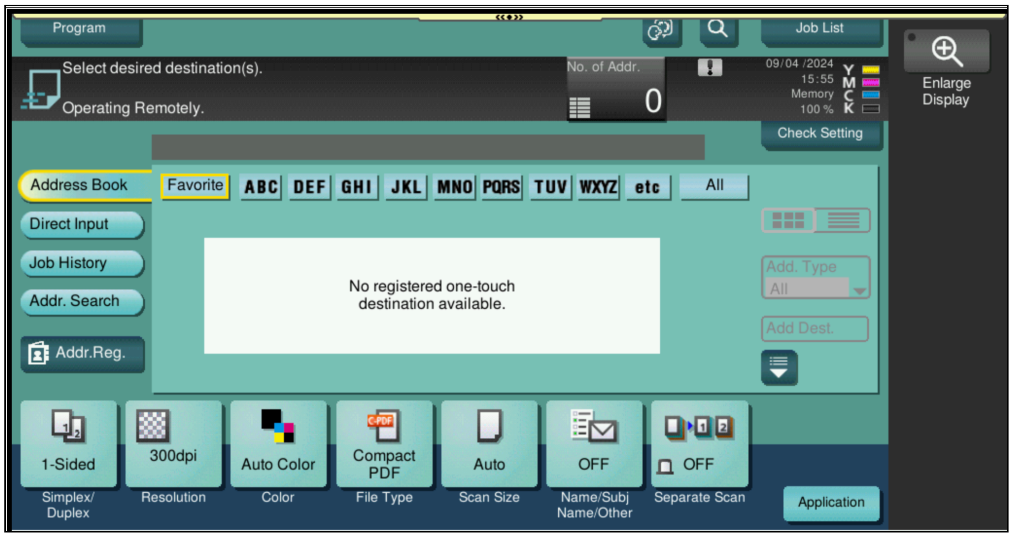
> If you tap **Scan settings** before filling in the workflow settings, you will see a warning message that the workflow settings must be configured.



5. Tap **Scan**.

Advanced (native) scan functionality

If you wish to use the MFD's native scan functionality, tap **Advanced scan** on **My quick actions** screen.



Note that if you want to return to the Cloud Terminal after using this functionality, you must open it and log in again.

9.2.5 USING RICOH STANDARD GEN 2 CLOUD TERMINAL

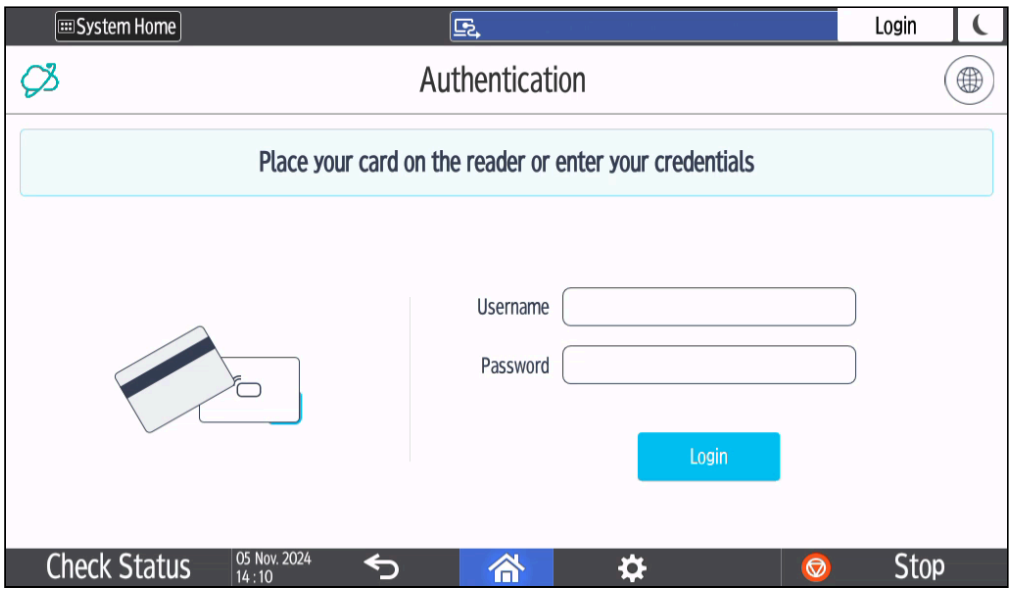
Registering your card

See Card registration at the MFD.

Logging in and out

Logging in

The authentication method depends on how your administrator configured the terminal. You can log in via card, PIN (Short ID), username/password, or their combinations. Follow the instructions on the screen.



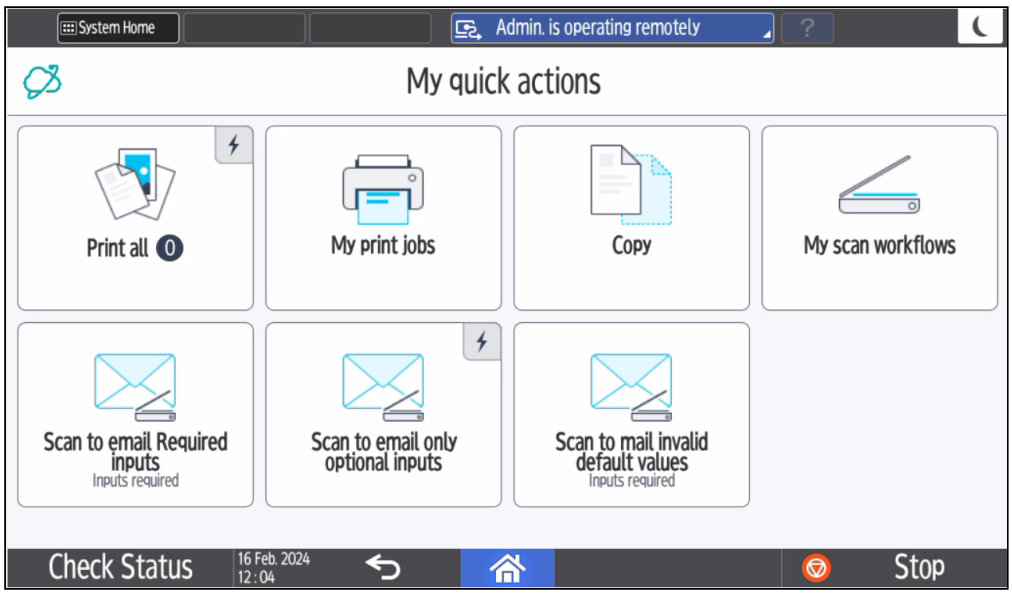
Logging out

Tap the logout button in the right-hand top corner of the screen.

If the terminal is configured to use authentication by card, you can also log out by placing your card on the card reader.

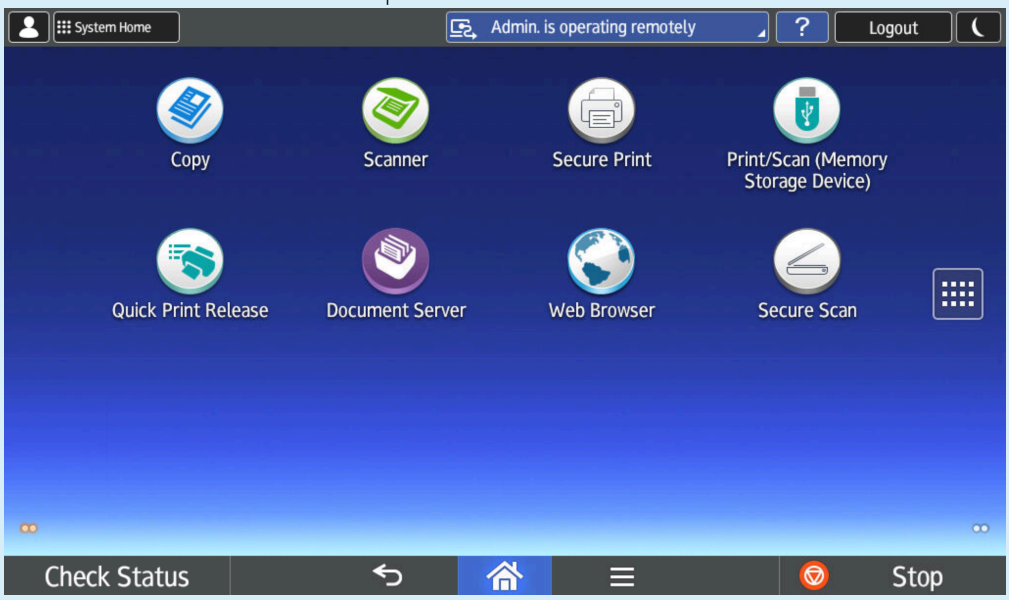
My quick actions application

My quick actions application enables you to access frequently used functions, such as print all jobs or use a scan workflow immediately after login. The quick action buttons are displayed according to your rights and scan workflows assigned to you.

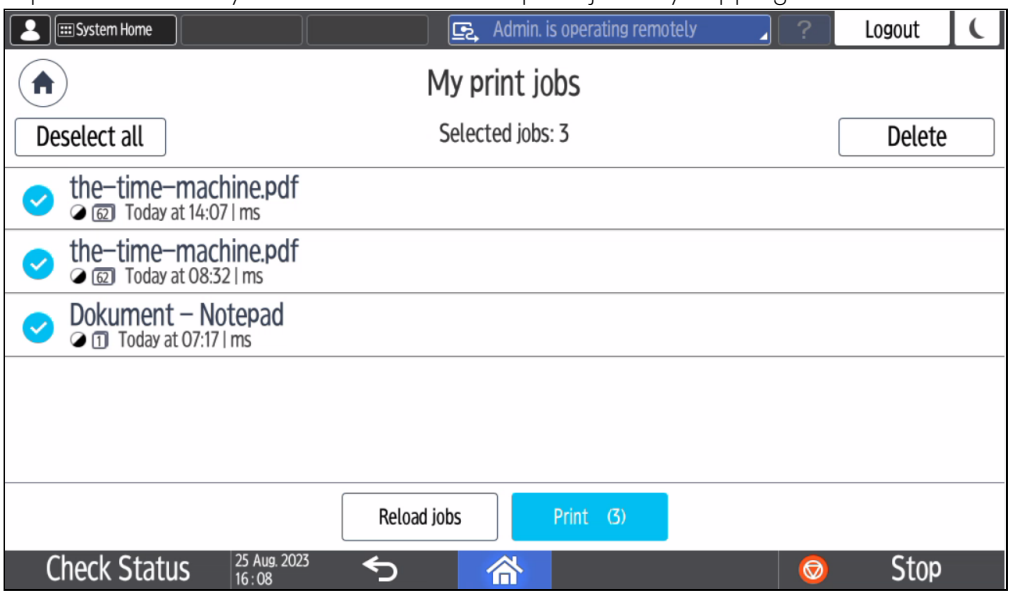


Printing and managing jobs

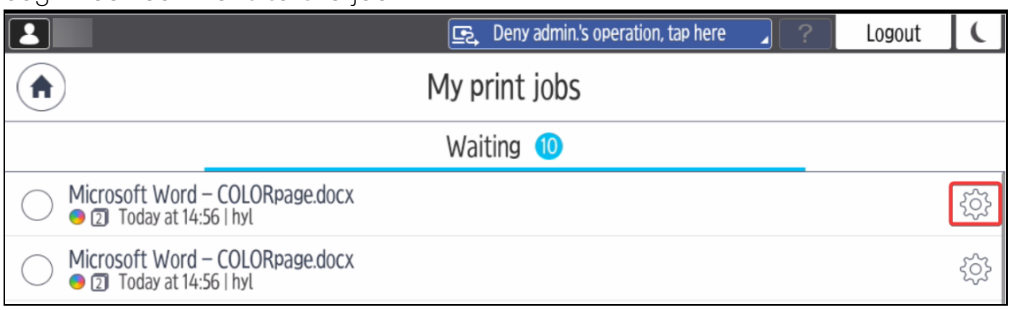
1. Log in to the Cloud Terminal. You will see **My quick actions** screen.
2. If you wish to release all of your print jobs, tap **Print all**.
3. If you wish to release only a specific print job or jobs, tap **My print jobs**.

> If you are in another application than **My print jobs**, tap the **Home** button to access the home screen and then tap **Secure Print**.
>
> 
>

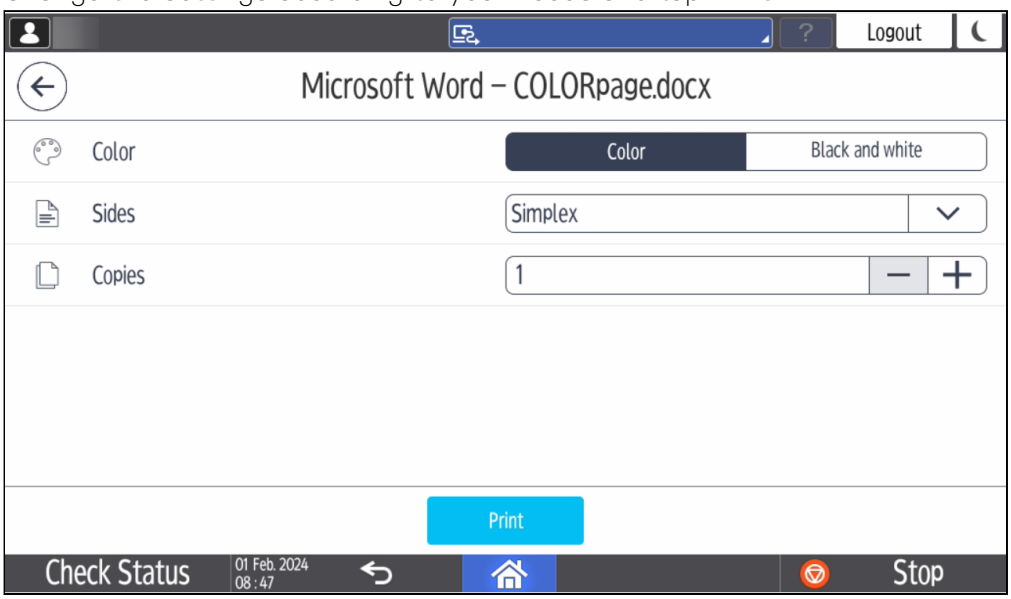
4. **My print jobs** screen will be displayed. Select the print job(s) you wish to print from the list and tap **Print**. You may also delete selected print jobs by tapping **Delete**.



5. To modify the finishing options (Color, Sides, and Number of copies) before printing, tap the cogwheel icon next to the job.



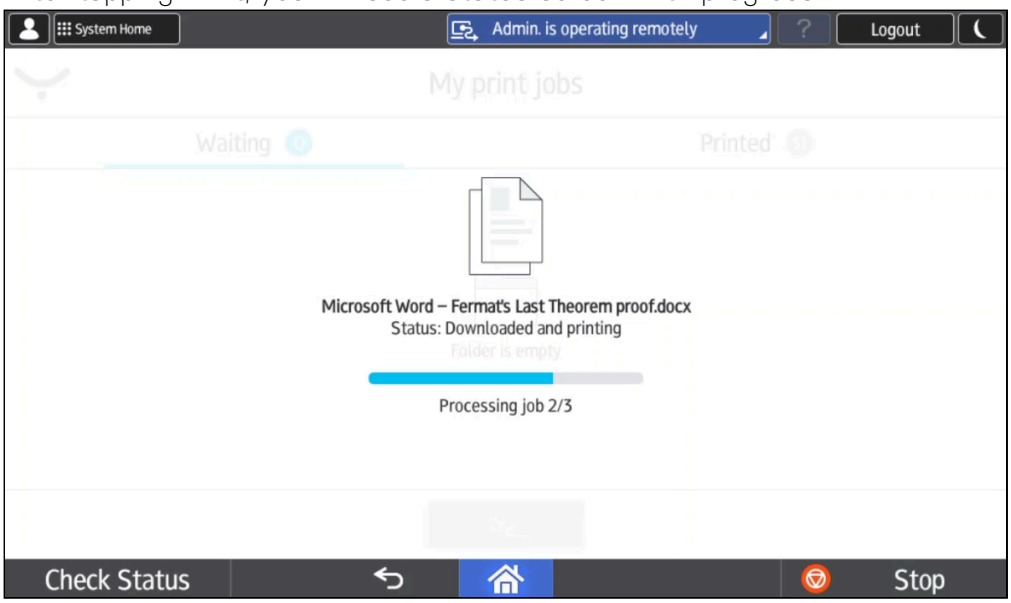
6. Change the settings according to your needs and tap **Print**.



- The **Color** option is greyed out on MFDs that don't support color printing.
- In **Sides**, you can select between **Simplex**, **Duplex (Flip on Long Edge)**, and **Duplex (Flip on Short Edge)**.

- The range for the number of copies is between 1 and 1000. You can modify the number by tapping the plus and minus buttons or by entering it directly into the text field.

7. After tapping **Print**, you will see a status screen with progress.



Above the overall progress, the status of the currently processed job is displayed with one of the following values:

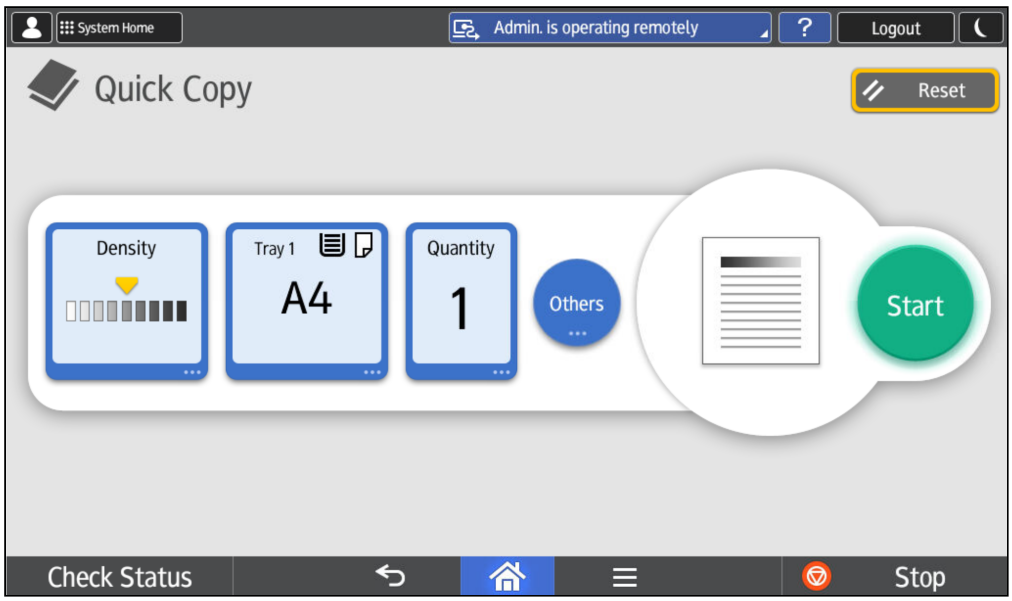
- **Waiting** – The job is yet to be processed.
- **Printing** – The server tries to print the document from any location with network visibility to the printer (called "optimized print."). Without network visibility, the print method will change to **Downloaded and printing**.
- **Downloading** – The job is being downloaded for print by the Cloud Terminal.
- **Downloaded and printing** – The downloaded job is being printed by Cloud Terminal.

8. After the last job has been delivered, a success message will appear.
9. If any job fails to be printed, the following error message with the number of failed jobs will appear: "X/Y jobs failed to print. Please try again or contact your administrator."

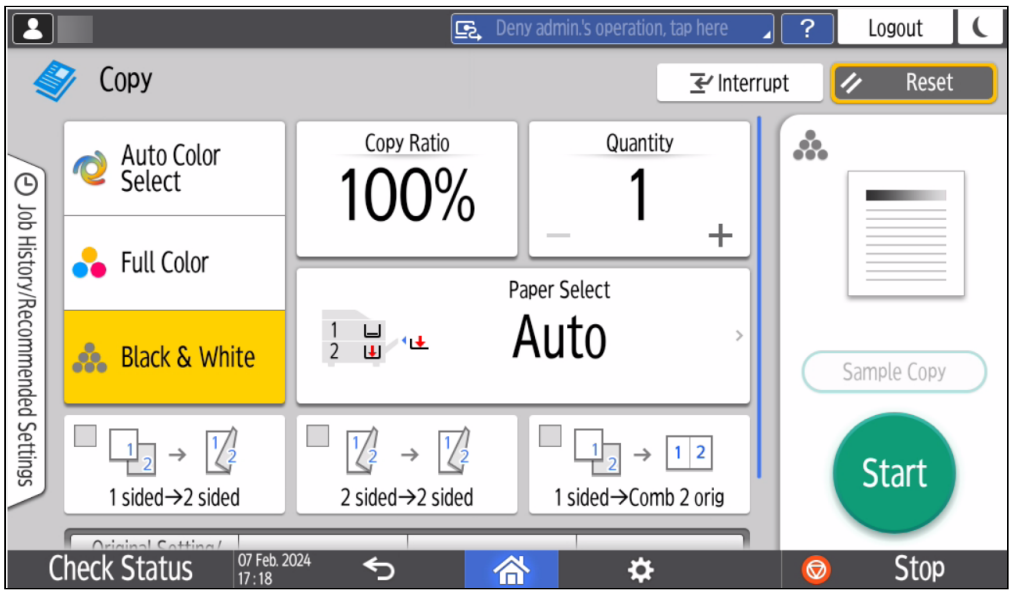
Copying

If you have copy permissions in SAFEQ Cloud and your MFD has the native Copy and/or Quick Copy applications installed, you will see a **Copy** button in **My quick actions**. Tapping it will take you to Quick Copy or Copy application, depending on which of them is installed. If both of them are installed, the Copy button will take you to Quick Copy application.

In Quick Copy, you can modify basic copy options. Tap **Start** to start copying.



The Copy application offers you more options, depending on the capabilities of your MFD. Tap **Start** to start copying.

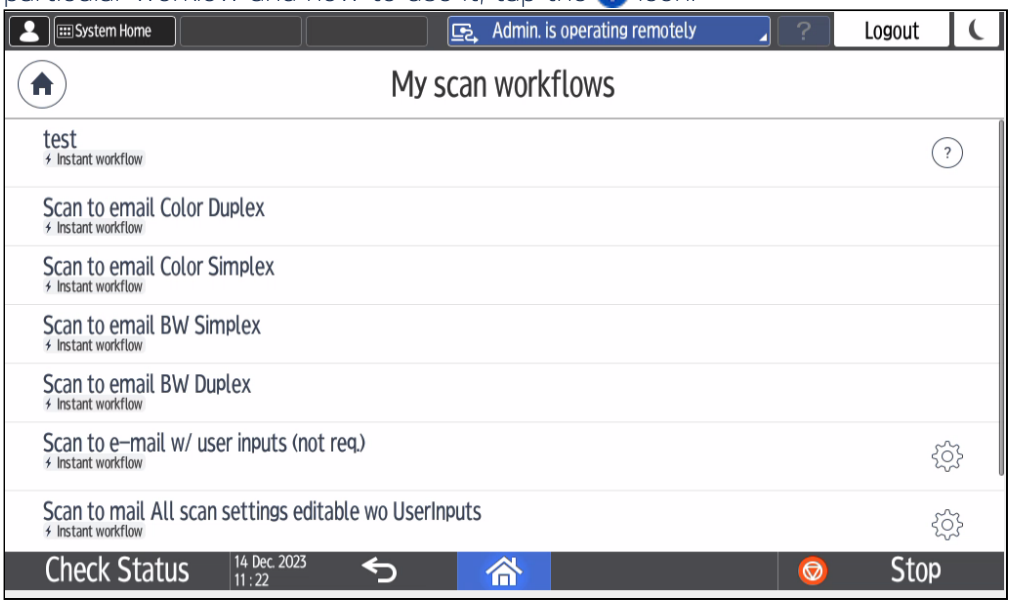


Scanning

1. Log in to the terminal. You will see **My quick actions screen**.
2. You can run scan workflows from **My quick actions** screen or from **My scan workflows** screen.
3. **My quick actions** screen displays the first three workflows from all scan workflows that your administrator made available to you. Tap the workflow you wish to execute. The workflow will start immediately.
4. **My scan workflows** screen displays the list of all scan workflows available to you.

If you are in another application than **My scan workflows**, tap the home button and then tap **Secure Scan**.

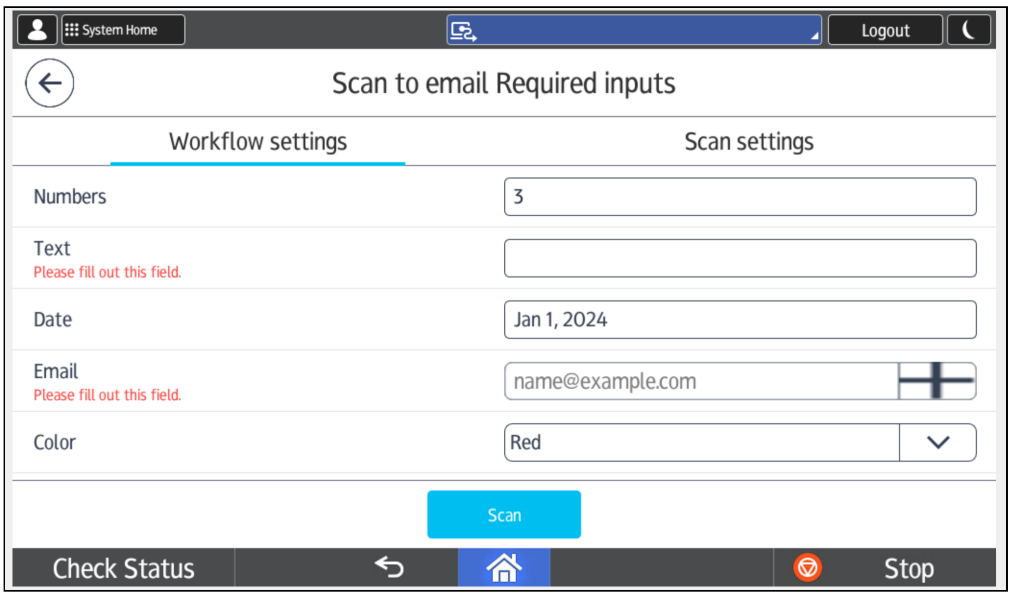
5. Tap the workflow you wish to execute. The workflows that do not require any user input are called instant workflow and are marked with a flash icon. If you need more information on a particular worklow and how to use it, tap the ? icon.



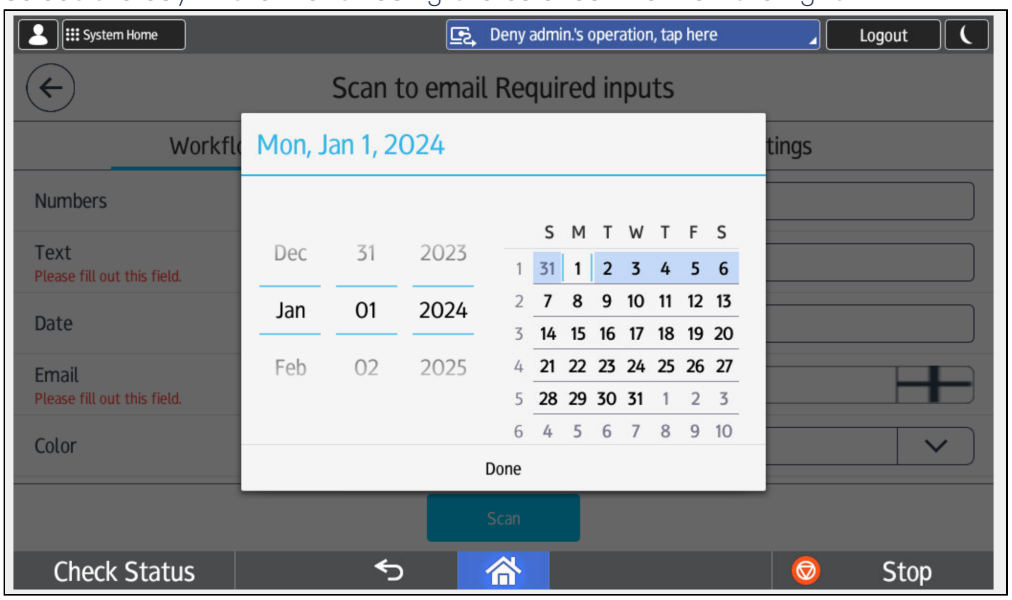
6. If a workflow is marked with **Input required**, tapping it will take you to **Workflow settings** and/or **Scan settings**. Note that the available settings depend on how your administrator configured the workflow. Alternatively, you can access these settings by tapping the gear icon.

   a. The **Workflow settings** tab is displayed only if the workflow has at least one user input. Fill in the required information (marked in red). You can leave the other fields empty if you do not wish to modify them.

   If the format of your input does not pass validation, you will see an error message. If the date field value is incorrect, the date picker will try to adjust it automatically, but the error will still be displayed.

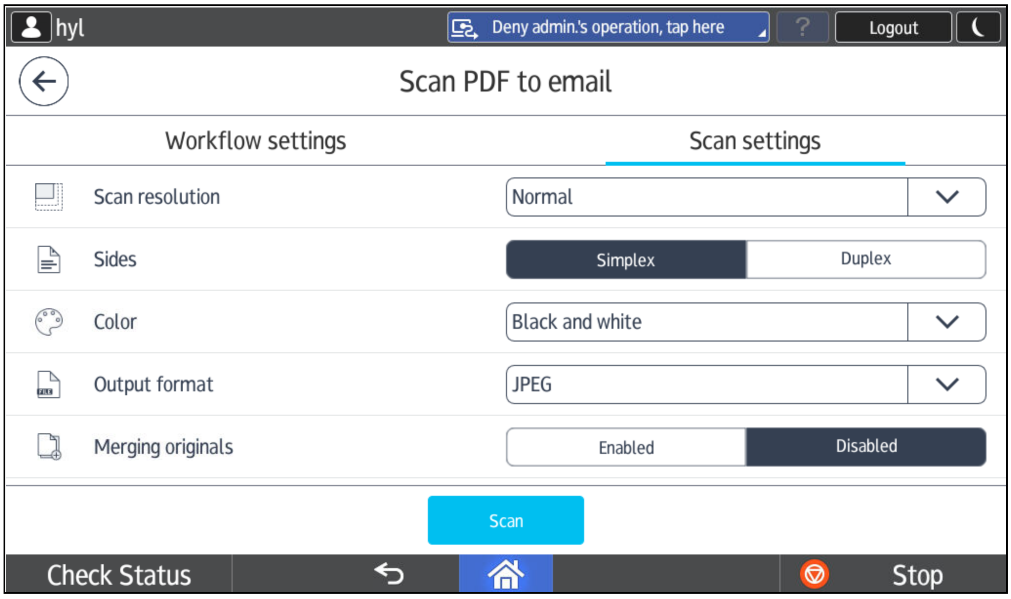


- To enter the date, tap the date field and scroll through the dates on the left side, or select the day in the month using the calendar view on the right.



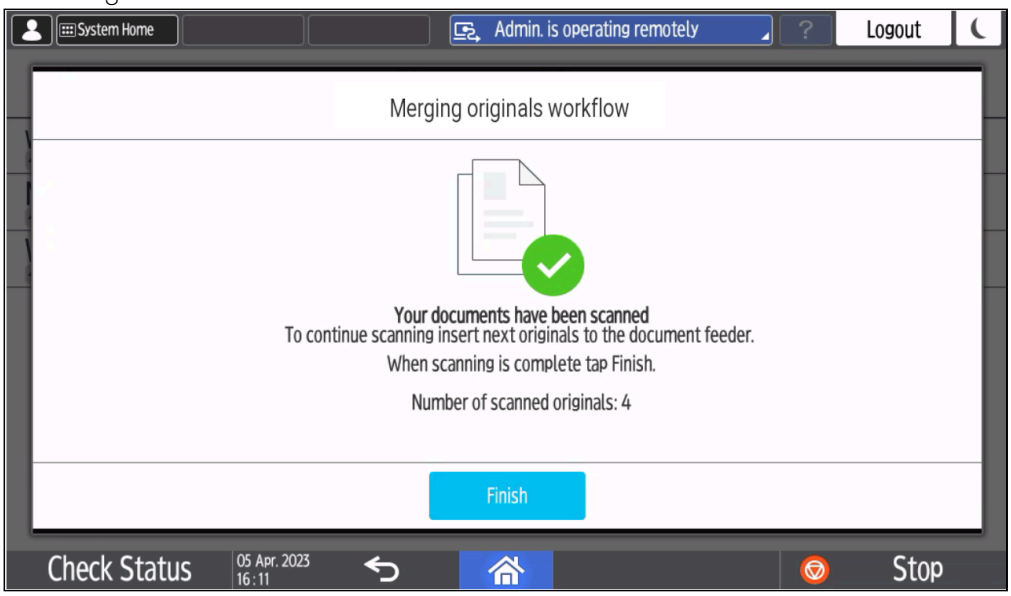
- You can input an email address manually, or tap the + icon next to the email field to open the search dialogue and select an existing email address. You can input multiple email addresses.

b. The **Scan settings** tab is displayed only if the workflow has at least one scan setting. Select the options according to your needs.



c. Tap **Scan**.

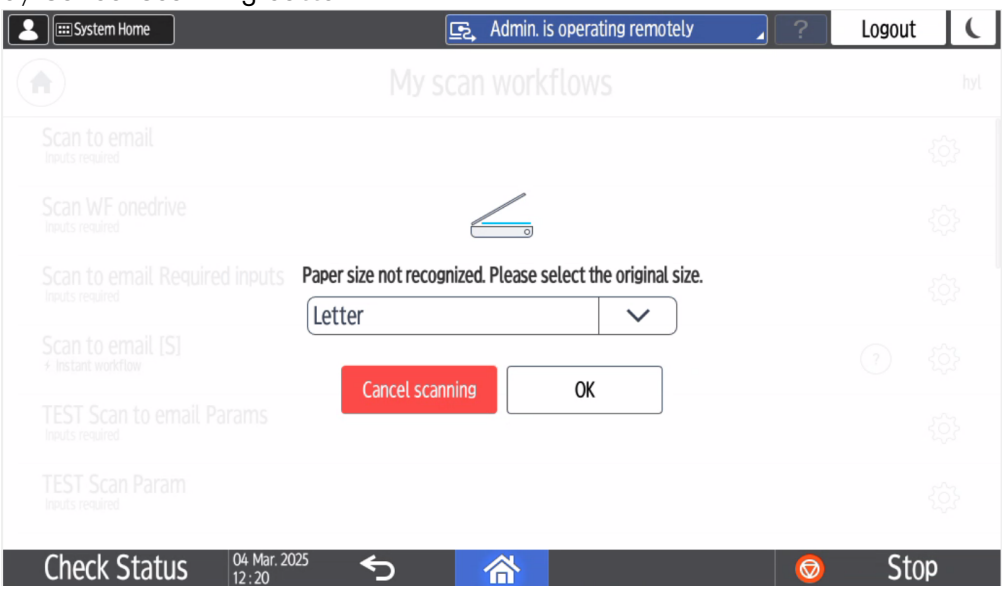
7. While scanning, you will see the **Scanning workflow in progress** screen. When scanning from glass or having **Merging originals** enabled, the following screen will be displayed when the scanning is finished.



8. If you want to continue scanning, insert more documents into the document feeder. Otherwise, tap **Finish**.

9. If the size of the paper on the glass is not recognized, you will see the option to select it manually. Tap **OK** to continue scanning. There is also possibility to cancel the scan job

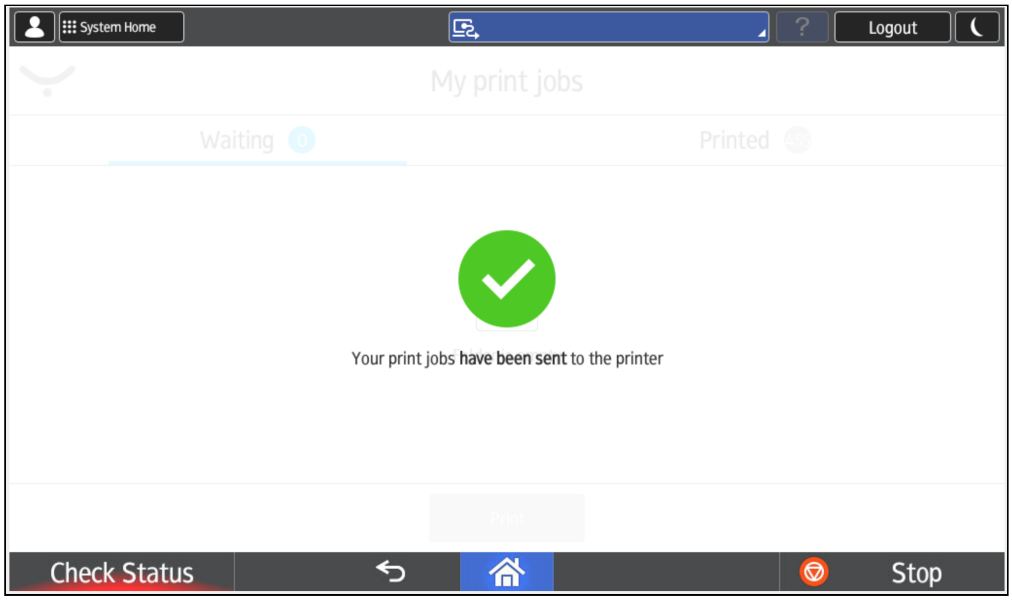
by Cancel scanning button.



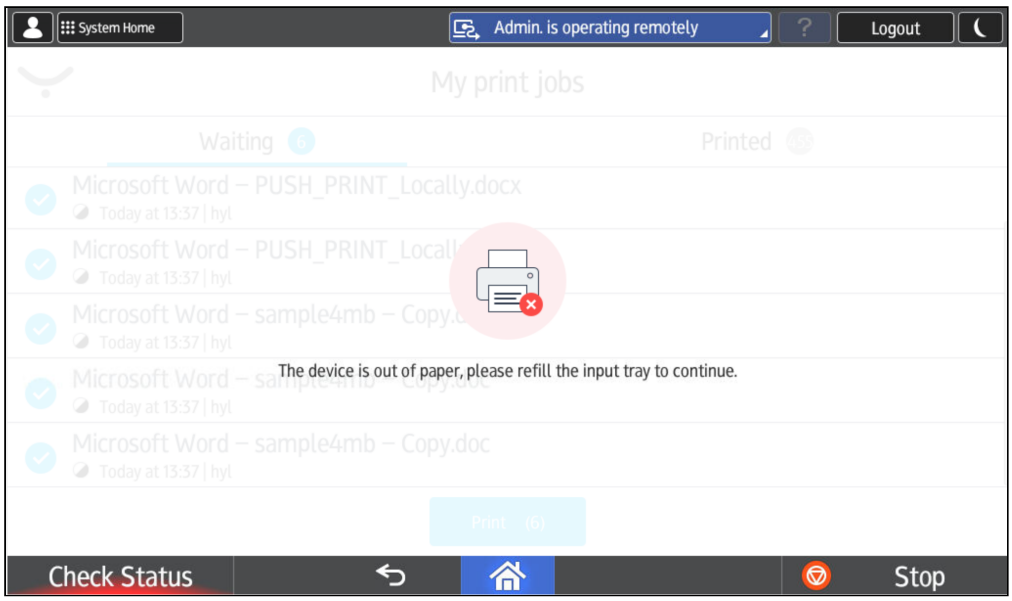
Troubleshooting

Printer issues during printing

If there is an issue with the printer during the Printing phase, the Check Status button at the bottom will have a red illumination.

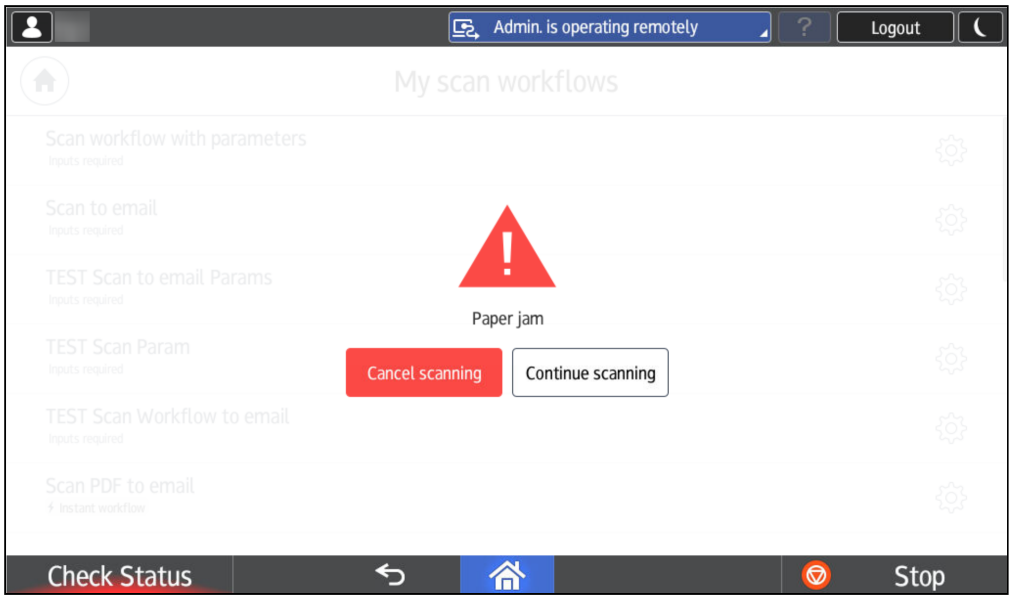


If there is an issue with the printer during the Downloading or Downloaded and printing phase, the Check Status button on the bottom will have a red illumination and the following message will appear:



Paper jam during scanning

If a paper jam occurs during scanning, you will see the Scanning error screen.



After removing the jammed paper, you can cancel the scan job by tapping Cancel scanning or continue the scanning by tapping Continue scanning.

Empty screen in My scan workflows

If your screen with workflows is empty, it means that no scan workflows have been assigned to you by your administrator. Contact your administrator.

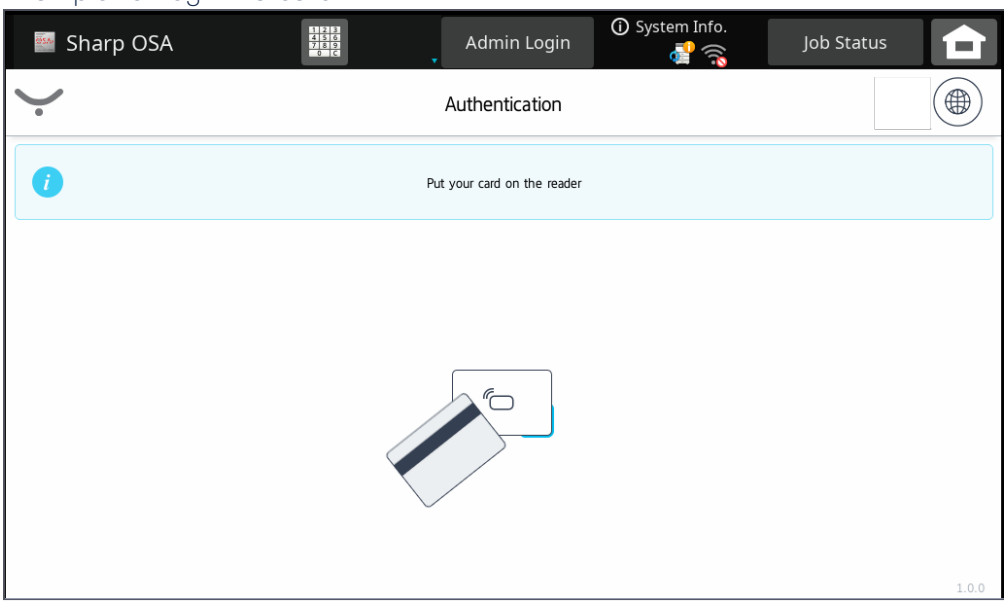
9.2.6 USING SHARP GEN 2 CLOUD TERMINAL

Registering your card

See Card registration at the MFD.

Logging in

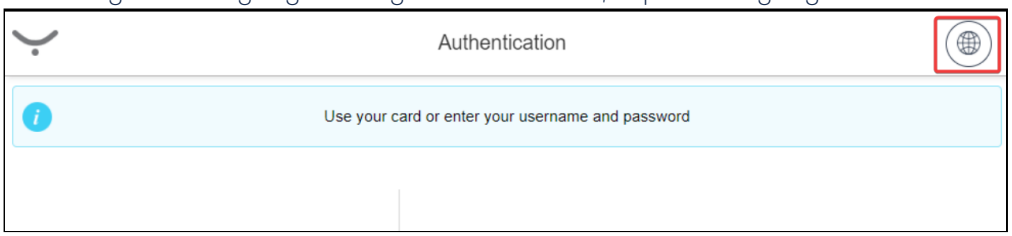
1. The authentication method depends on how your administrator configured the terminal. You can log in via card, PIN (Short ID), username/password, or their combinations. Follow the instructions on the screen.
   Example for login via card:



2. If the authentication fails, you will see an error message saying "You have placed unknown or damaged card."

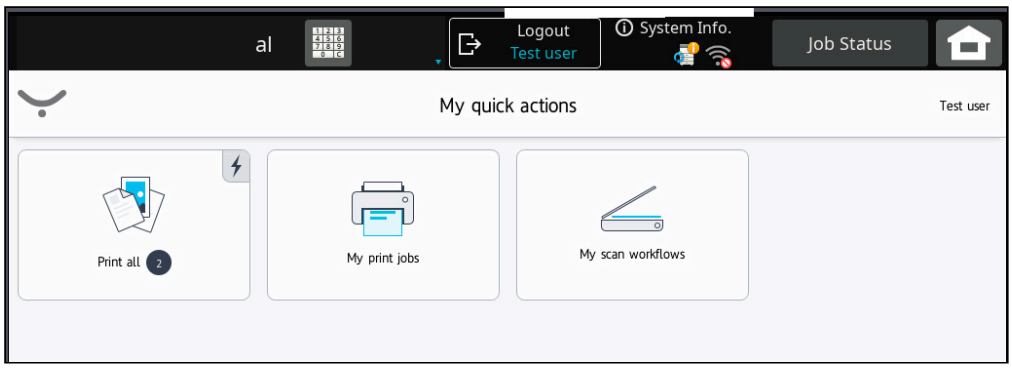
3. If your card is not registered, you will see a message "Your card has not been activated yet." You must register your card. See Card registration at the MFD.

4. To change the language during authentication, tap the language icon in the top-right corner.



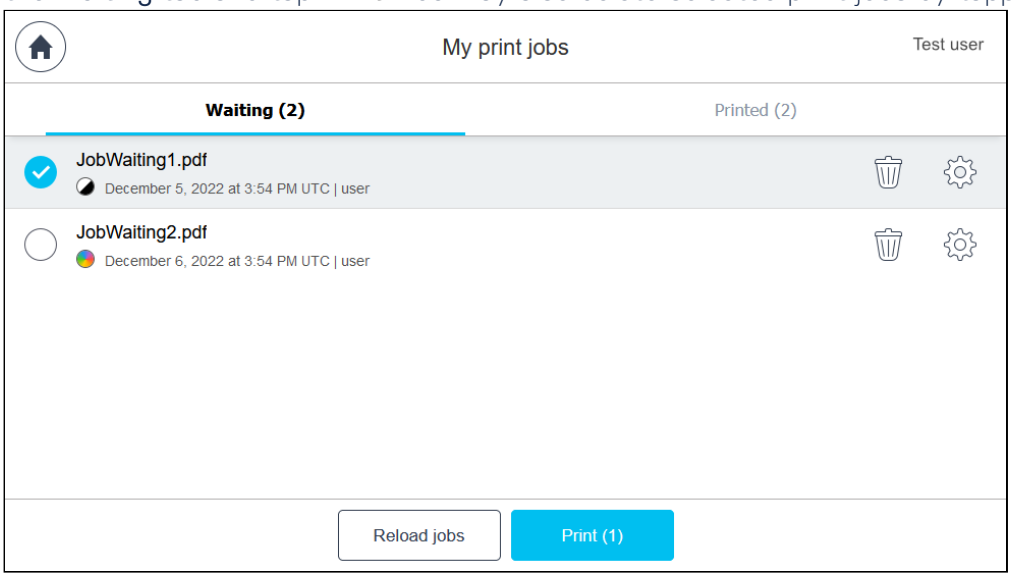
My quick actions applications

My quick actions application allows you to access frequently used functions, such as print all jobs or use a scan workflow immediately after login. The quick action buttons are displayed according to your rights and scan workflows assigned to you.



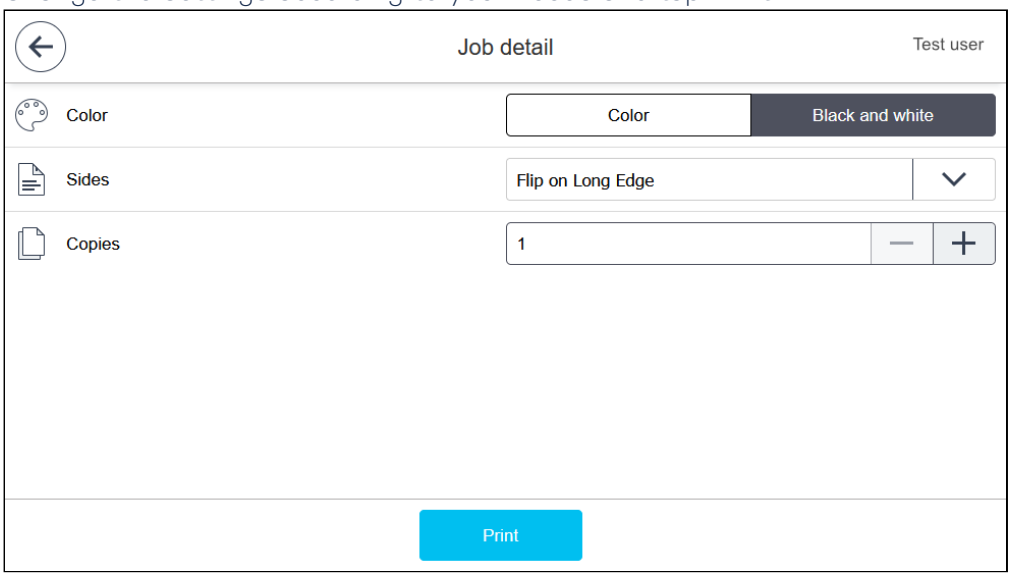
Printing and managing jobs

1. Log in to the Cloud Terminal. You will see the **My quick actions** screen.
2. If you wish to release all of your print jobs, tap **Print all**. Note that if you have no print jobs to release, the button will be greyed out.
3. If you wish to release only a specific print job or jobs, tap **My print jobs**.
4. **My print jobs** screen will be displayed. Select the print job(s) you wish to print from the list on the **Waiting** tab and tap **Print**. You may also delete selected print jobs by tapping the bin icon.



5. If you've sent an additional print job while logged in at the MFD, tap **Reload jobs**.
6. To modify the finishing options (Color, Sides, and the number of copies) before printing, tap the cogwheel icon next to the job.

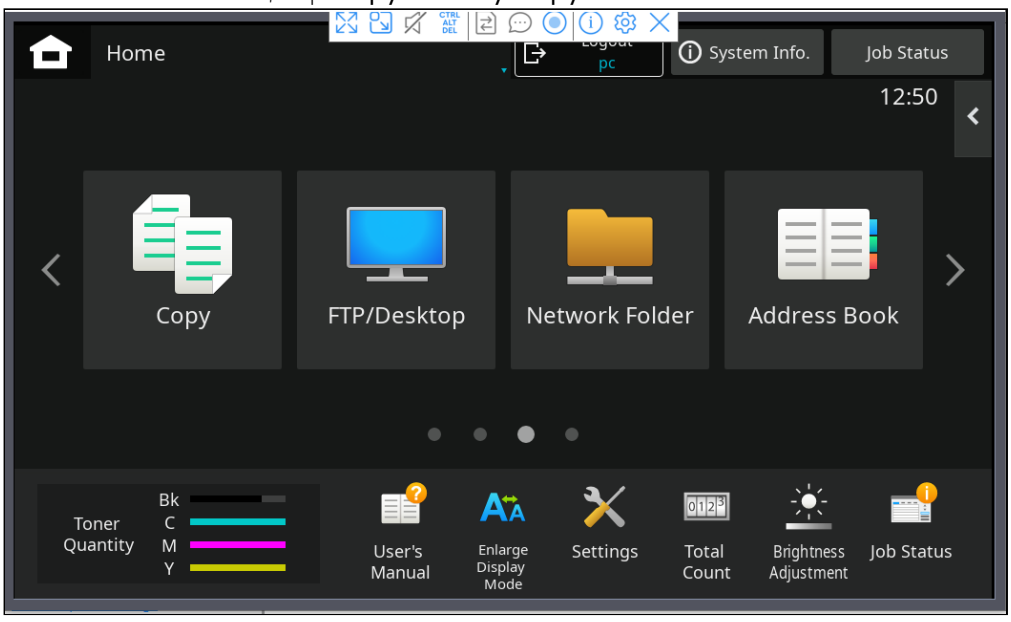
7. Change the settings according to your needs and tap **Print**.



8. After tapping **Print**, you will see a status screen with progress.
9. After the last job has been delivered to the MFD and printed, a success message will appear.
10. If any job fails to be printed, the following error message with the number of failed jobs will appear: "Print job failed. Please try again or contact your administrator."

Copying

1. If you are logged to the SAFEQ Cloud cloud terminal, tap the home icon in the upper bar to access the home screen of the MFD.
2. On the home screen, tap **Copy** or **Easy Copy**.

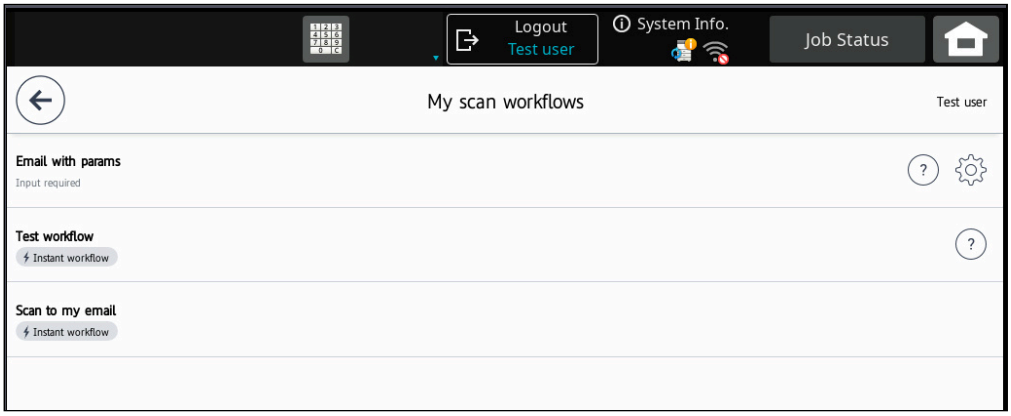


3. This will take you to the native copy application of the device.

Info for administrators: copy jobs done in the native copy applications are also accounted for in SAFEQ Cloud.

Scanning

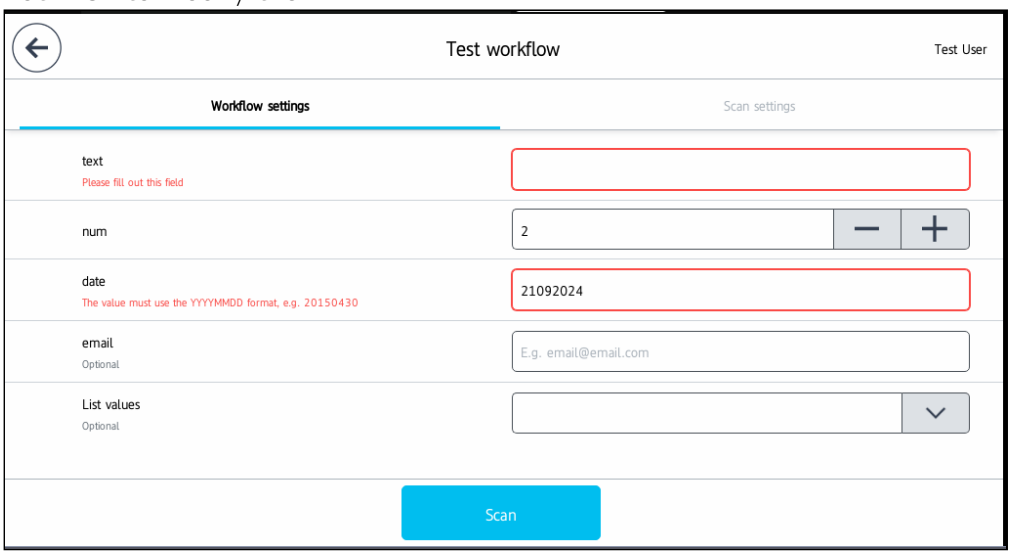
1. Log in to the terminal. You will see **My quick actions** screen.
2. You can run scan workflows from **My quick actions** screen or from **My scan workflows** screen.
3. **My quick actions** screen displays the first three workflows from all scan workflows that your administrator made available to you. Tap the workflow you wish to execute. The workflow will start immediately. Feeder takes precedence over glass.
4. **My scan workflows** screen displays the list of all scan workflows available to you.



If none are available, you will see a "No scanning workflows available" message.

5. Tap the workflow you wish to execute. The workflows that do not require any user input are called instant workflow and are marked with a flash icon. If you need more information on a particular worklow and how to use it, tap the ? icon.
6. If a workflow is marked with **Input required**, tapping it will take you to **Workflow settings** and/or **Scan settings**. Note that the available settings depend on how your administrator configured the workflow. Alternatively, you can access these settings by tapping the gear icon.
   a. The **Workflow settings** tab is displayed only if the workflow has at least one user input. Fill in the required information (marked in red). You can leave the other fields empty if you do

not wish to modify them.

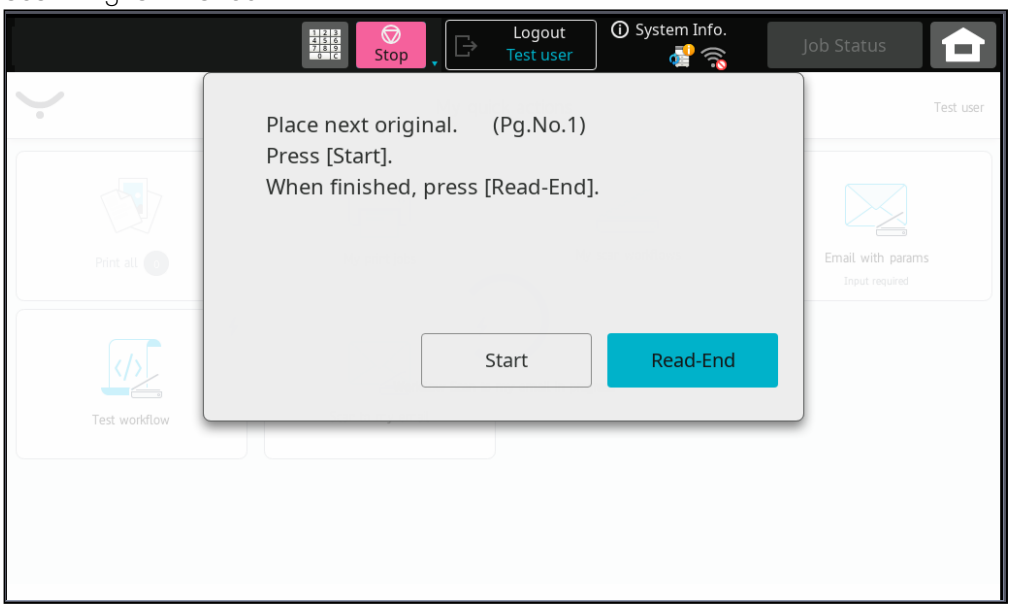


b. The **Scan settings** tab is displayed only if the workflow has at least one scan setting. Configure the options according to your needs.

c. Tap **Scan**.

7. While scanning, you will see the **Scanning workflow in progress** screen. When scanning from glass or having **Merging originals** enabled, the following screen will be displayed when the

scanning is finished.



a. If you want to continue scanning, insert more documents into the document feeder or on the glass and tap **Start**. Otherwise, tap **Read-end** to finish scanning.

8. If the workflow was successful, you will see a message "Your scan has been completed." If there was a problem or if you canceled the workflow, you will see a message "Your scan job failed" with the details of the problem.

9. If you want to continue scanning, insert more documents into the document feeder. Otherwise, tap **Finish**.

9.2.7 USING XEROX GEN 2 CLOUD TERMINAL

Registering your card

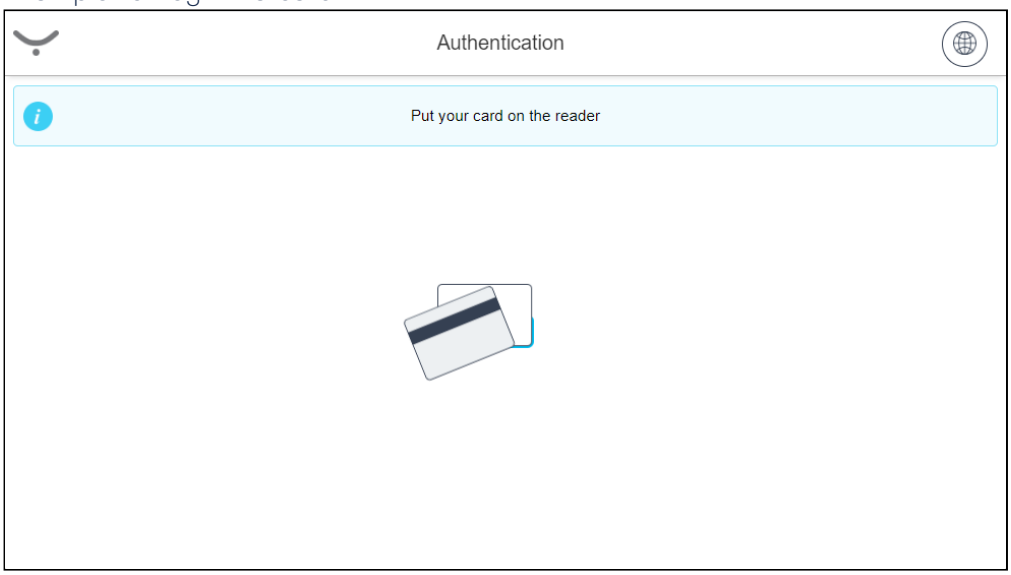
See Card registration at the MFD.

Logging in and out

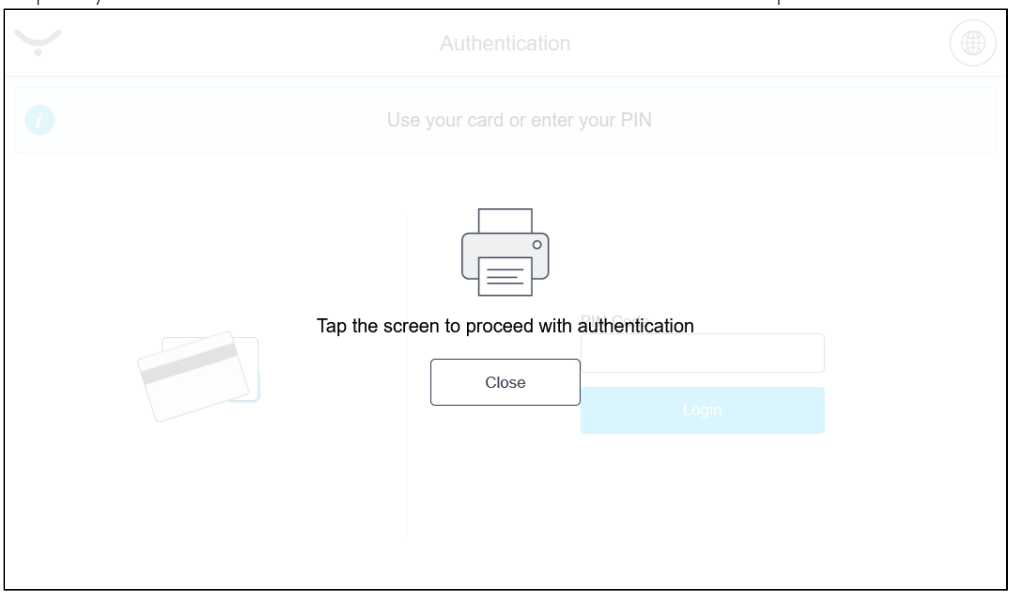
Logging in

1. The authentication method depends on how your administrator configured the terminal. You can log in via card, PIN (Short ID), username/password, or their combinations. Follow the instructions on the screen.

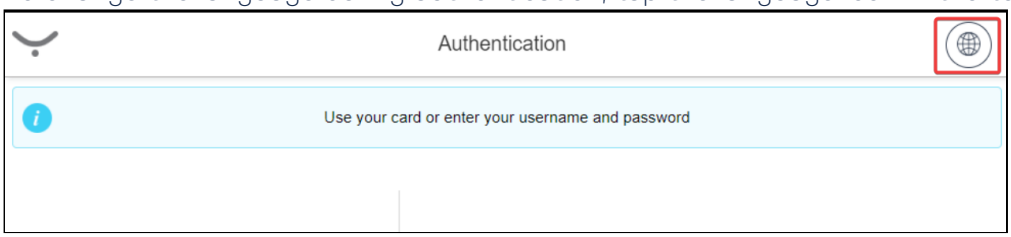
Example for login via card:



2. You will see the Cloud Terminal home screen – **My quick actions** application.
3. If the authentication fails, you will see an error message saying "You have placed unknown or damaged card."
4. If your card is not registered, you will see a message "Your card has not been activated yet." You must register your card. See Card registration at the MFD.
5. If the authentication screen is kept awake for too long and the device has a long enough timeout, the following screen appears and card authentication becomes temporarily disabled. Tap anywhere on the screen to resume the authentication process.

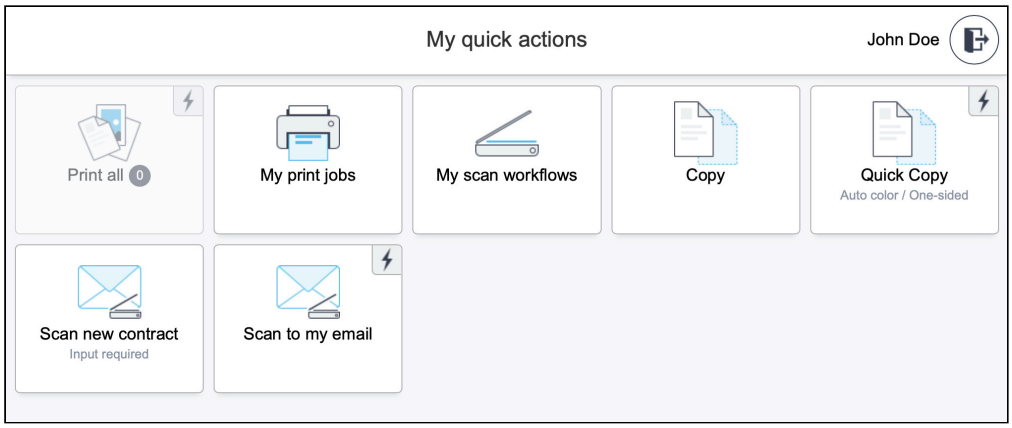


6. To change the language during authentication, tap the language icon in the top-right corner.



My quick actions applications

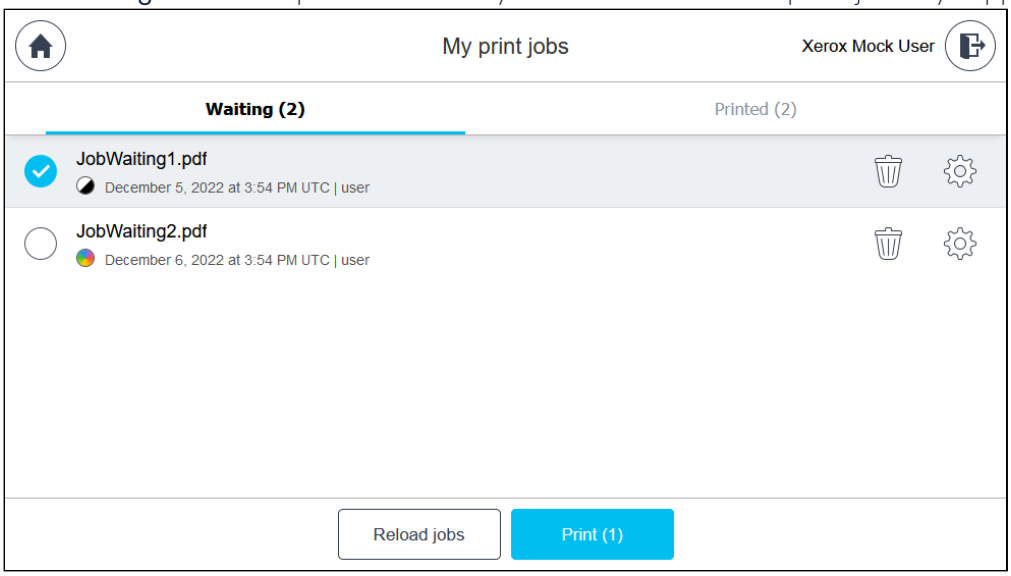
My quick actions application allows you to access frequently used functions, such as print all jobs or use a scan workflow immediately after login. The quick action buttons are displayed according to your rights and scan workflows assigned to you.



Printing and managing jobs

1. Log in to the Cloud Terminal. You will see My quick actions screen.
2. If you wish to release all of your print jobs, tap Print all.
3. If you wish to release only a specific print job or jobs, tap My print jobs.

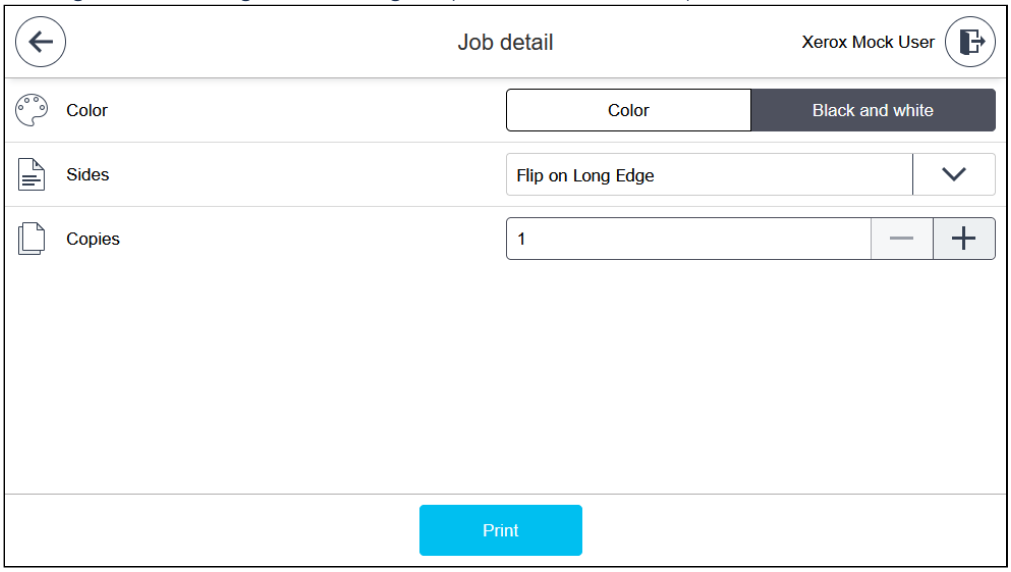
4. **My print jobs** screen will be displayed. Select the print job(s) you wish to print from the list on the **Waiting** tab and tap **Print**. You may also delete selected print jobs by tapping **Delete**.



5. If you've sent an additional print job while logged in at the MFD, tap **Reload jobs** on the MFD.

6. To modify the finishing options (Color, Sides, and the number of copies) before printing, tap the cogwheel icon next to the job.

7. Change the settings according to your needs and tap **Print**.



> The Color option is greyed out on MFDs that don't support color printing.

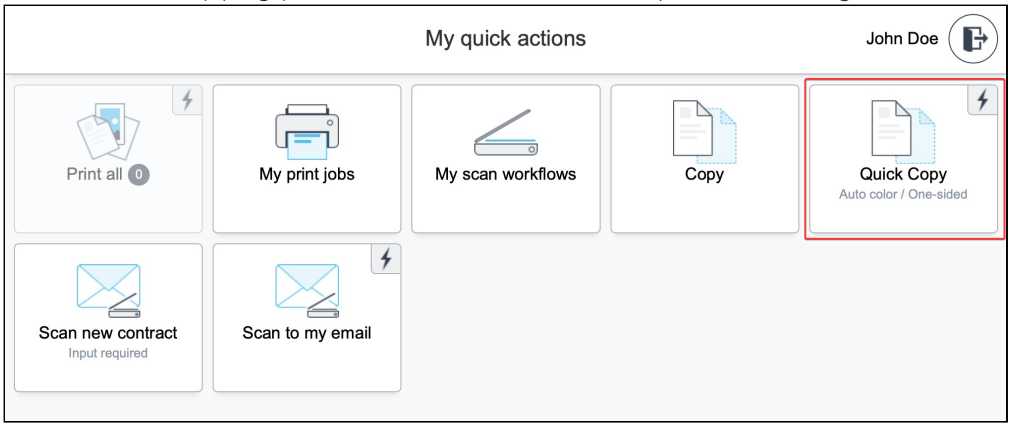
8. After tapping **Print**, you will see a status screen with progress.

9. After the last job has been delivered to the MFD and printed, a success message will appear.

10. If any job fails to be printed, the following error message with the number of failed jobs will appear: "X/Y jobs failed to print. Please try again or contact your administrator."

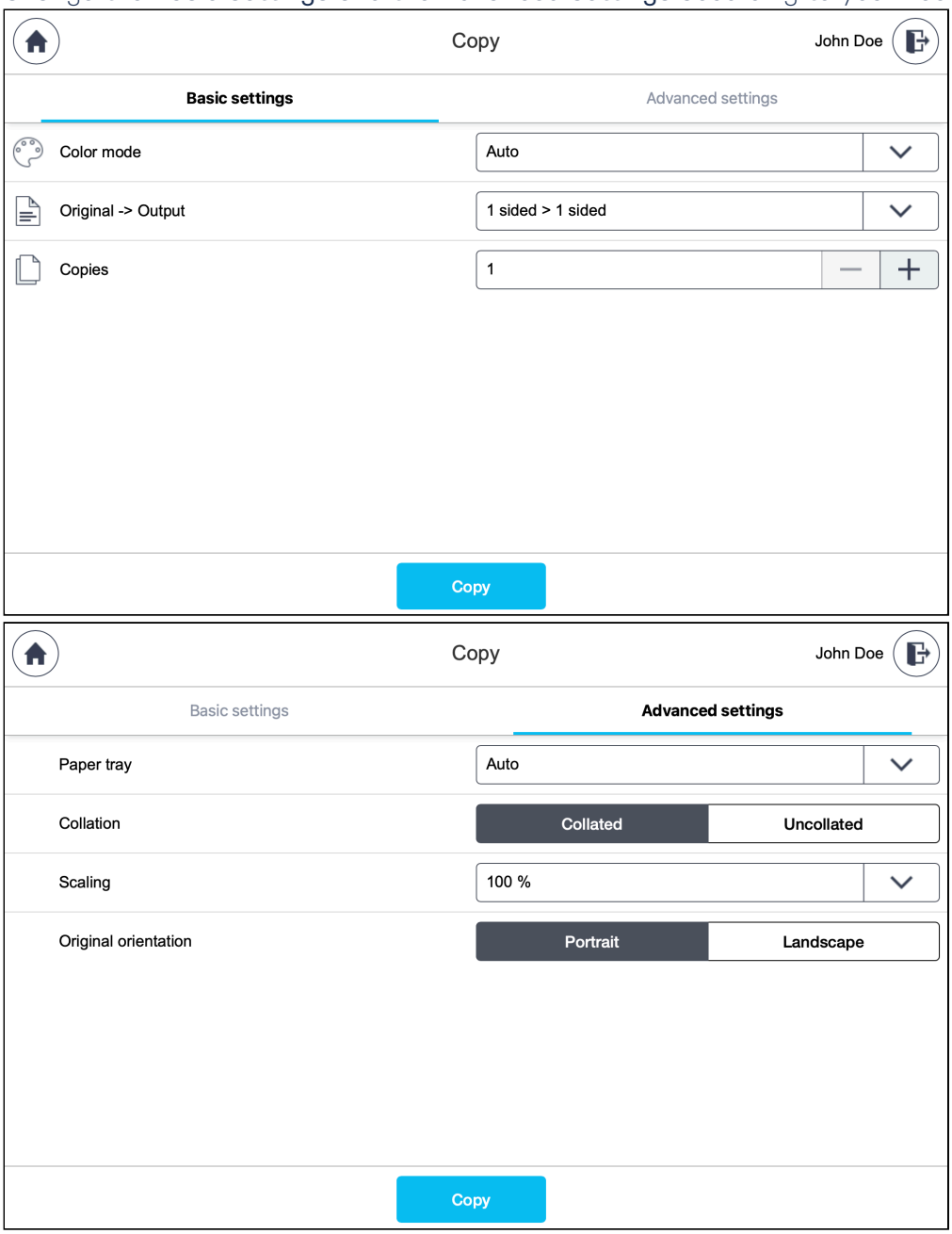
Copying

1. To make a quick one-sided copy with automatic color selection, tap **Quick Copy** in **My quick actions**. The copying process will start without any further dialogue windows.



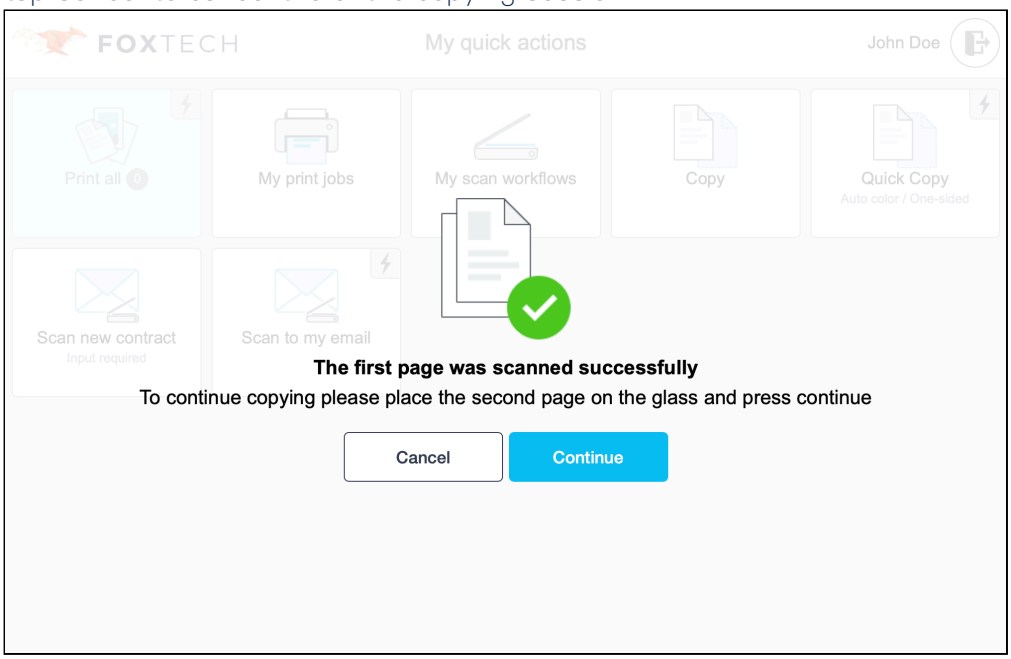
2. To modify settings before copying, tap **Copy** in **My quick actions**.

3. Change the **Basic settings** and the **Advanced settings** according to your needs and tap **Copy**.



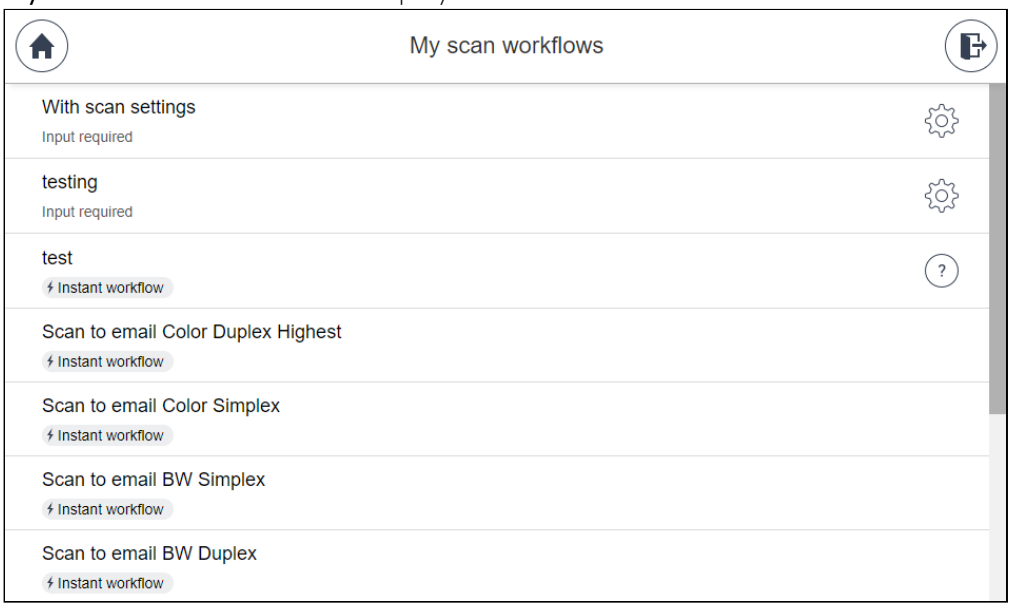
4. If you are copying multiple batches of documents, or if the document should be rotated during the scanning phase, you will see the following screen. Tap **Continue** to copy another page, or

tap **Cancel** to cancel the entire copying session.



Scanning

1. Log in to the terminal. You will see **My quick actions screen**.
2. You can run scan workflows from **My quick actions** screen or from **My scan workflows** screen.
3. **My quick actions** screen displays the first three workflows from all scan workflows that your administrator made available to you. Tap the workflow you wish to execute. The workflow will start immediately.
4. **My scan workflows** screen displays the list of all scan workflows available to you.

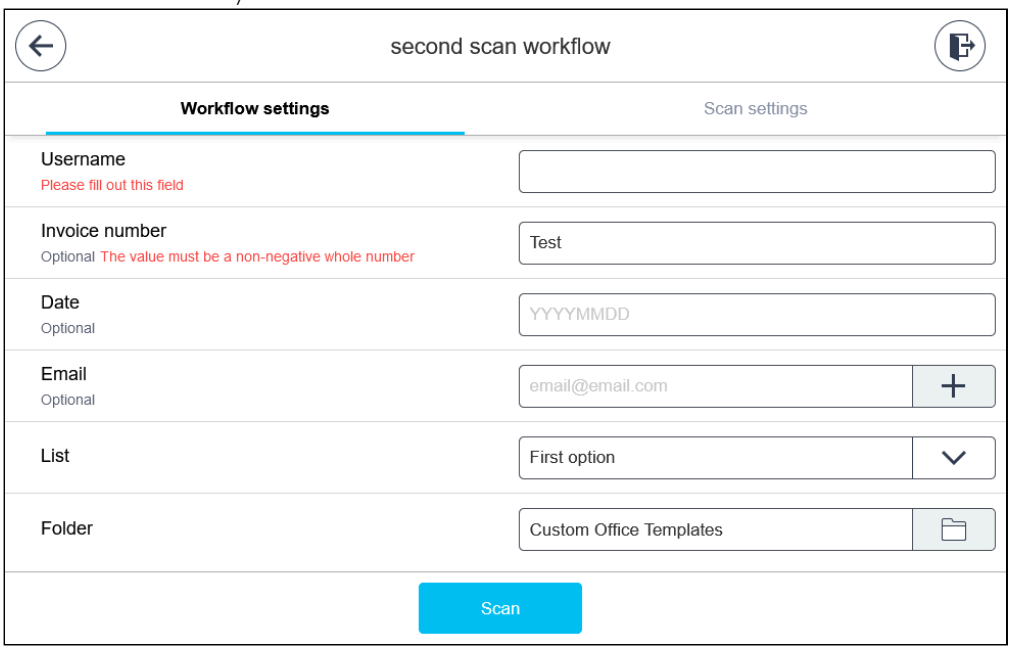


If none are available, you will see a "No scanning workflows available" message.

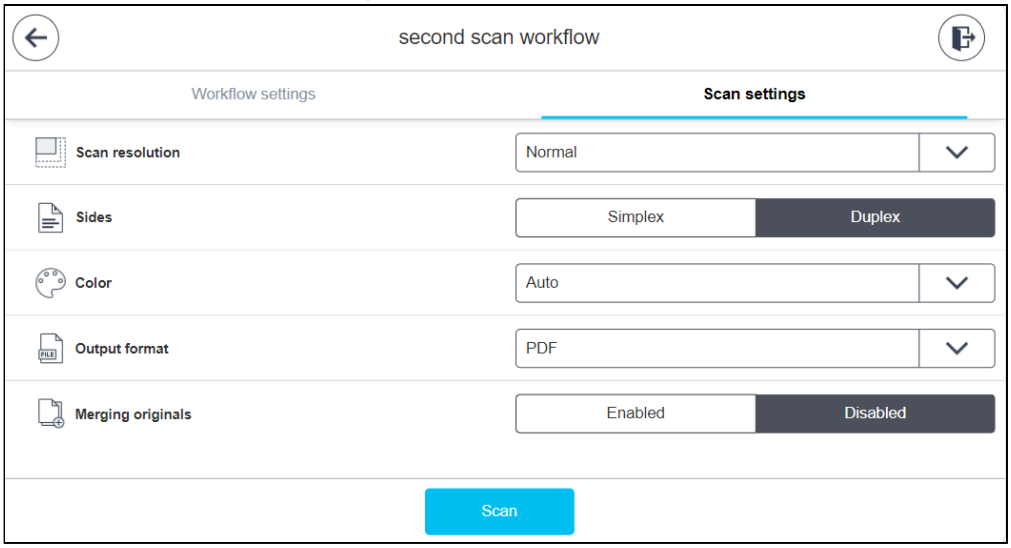
5. Tap the workflow you wish to execute. The workflows that do not require any user input are called instant workflow and are marked with a flash icon. If you need more information on a particular worklow and how to use it, tap the ? icon.

6. If a workflow is marked with **Input required**, tapping it will take you to **Workflow settings** and/or **Scan settings**. Note that the available settings depend on how your administrator configured the workflow. Alternatively, you can access these settings by tapping the gear icon.

   a. The **Workflow settings** tab is displayed only if the workflow has at least one user input. Fill in the required information (marked in red). You can leave the other fields empty if you do not wish to modify them.



   b. The **Scan settings** tab is displayed only if the workflow has at least one scan setting. Select the options according to your needs.



   c. Tap **Scan**.

7. While scanning, you will see the **Scanning workflow in progress** screen. When scanning from glass or having **Merging originals** enabled, the following screen will be displayed when the scanning is finished.

8. If the workflow was successful, you will see a message "Your scan has been completed." If there was a problem or if you canceled the workflow, you will see a message "Your scan job failed" with the details of the problem.

9. If you want to continue scanning, insert more documents into the document feeder. Otherwise, tap Finish.

9.3 SAFEQ CLOUD WEB UI FOR END USERS

SAFEQ Cloud Web UI is generally used by administrators. Depending on your access permissions, the following sections may be available to you as an end user:

- My profile
- My documents

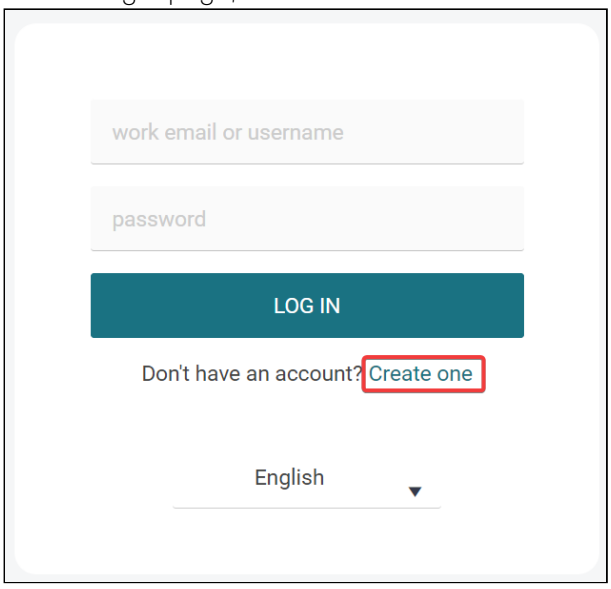
The Web UI address differs for each company. Ask your administrator to provide you with a link.

9.3.1 REGISTERING AS A STANDARD USER

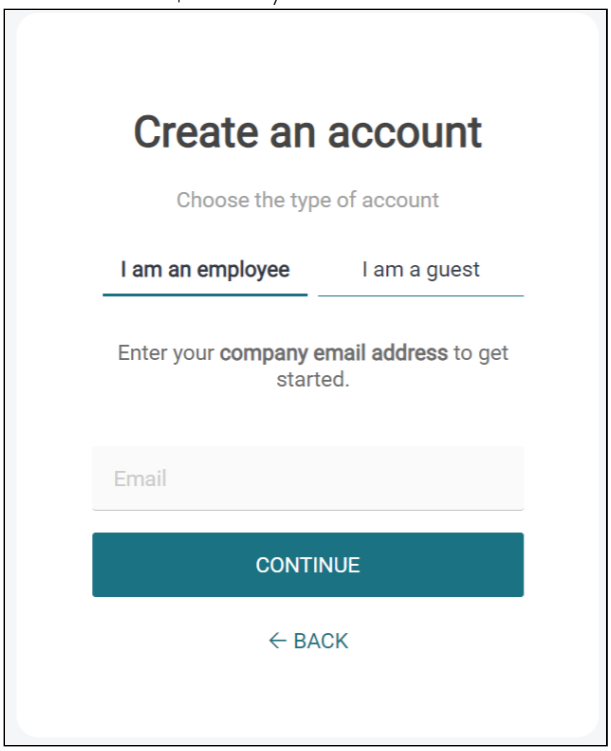
If your administrator enabled this option, you can register in SAFEQ Cloud yourself.

1. Open the SAFEQ Cloud Web UI address provided by your administrator.

2. On the login page, click Create one.

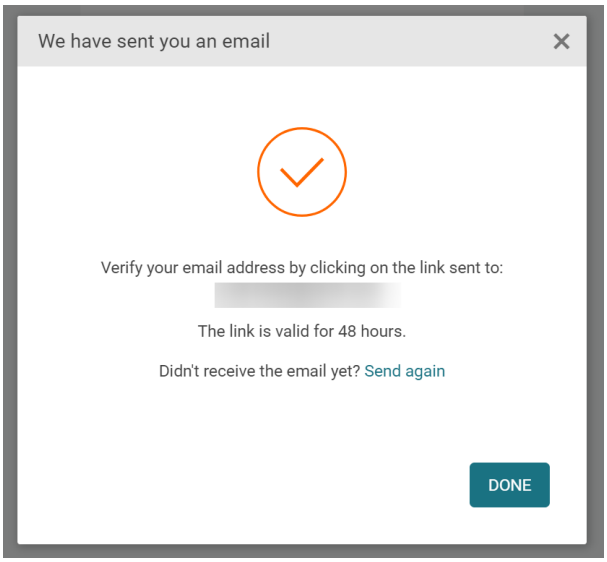


3. On the following screen (**Create an account**), enter your company email address. If the screen has two tabs, enter your email address on the **I am an employee** tab.



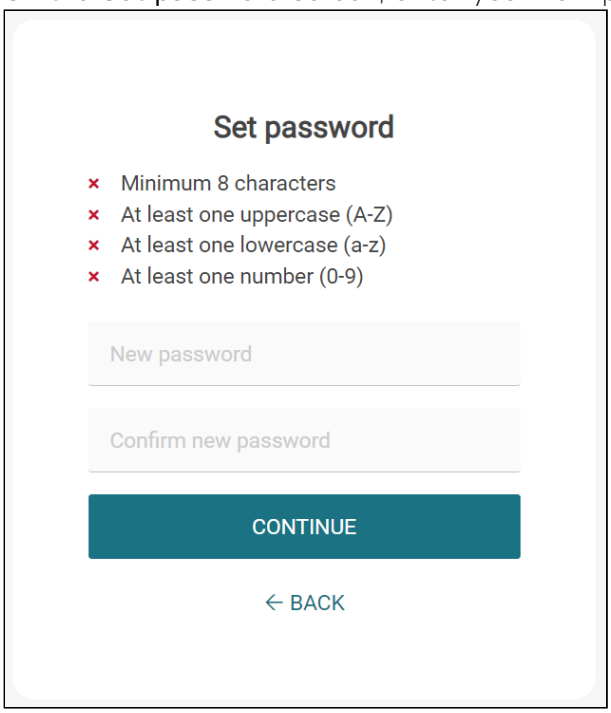
4. Click **Continue**.

5. You will receive an email with the verification link. If the email doesn't arrive, click **Send again**.

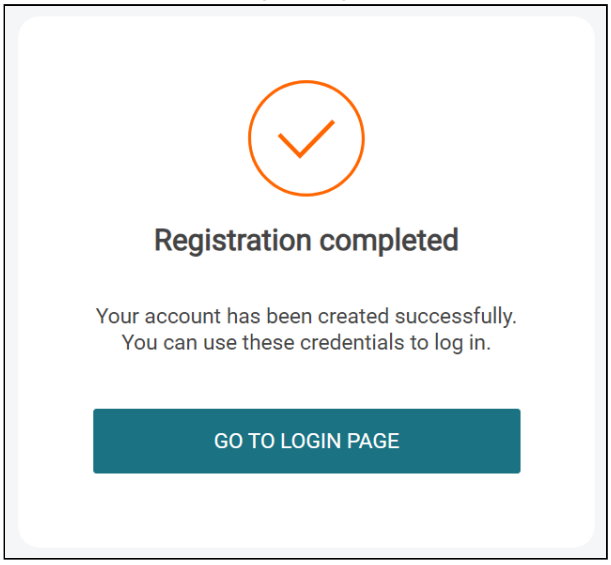


6. In the activation email, click **Activate your account**.

7. On the **Set password** screen, enter your new password for SAFEQ Cloud.



8. You will see a message that your registration is completed. If you wish to log in to SAFEQ Cloud, click **Go to login page**.

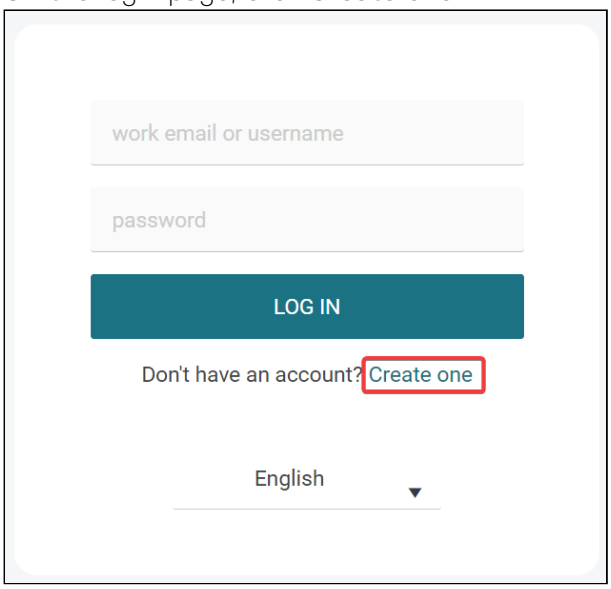


9.3.2 REGISTERING AS A GUEST

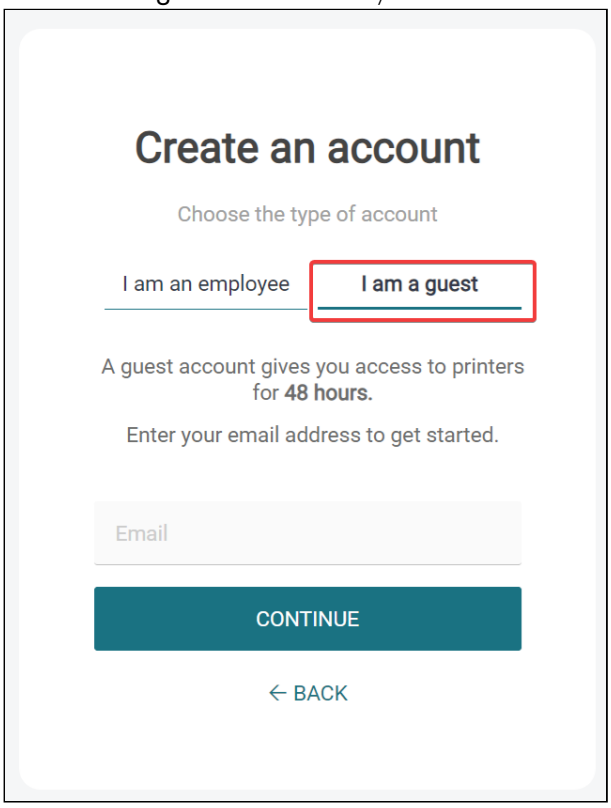
To register in SAFEQ Cloud as a guest, perform the below steps. A guest account in SAFEQ Cloud is meant for visitors, temporary employees, etc. It is a temporary account with more limited privileges than those of a standard user. The privileges and the expiration period depend on the settings done by the SAFEQ Cloud administrator.

1. Open the SAFEQ Cloud Web UI address provided by the SAFEQ Cloud administrator.

2. On the login page, click **Create one**.

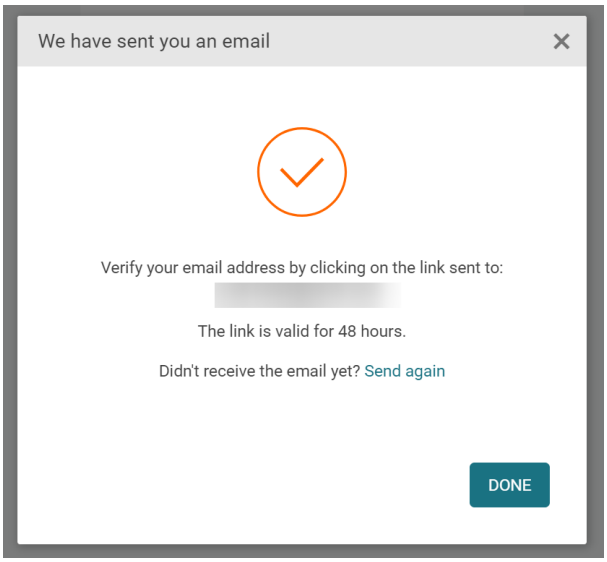


3. On the following screen (**Create an account**), enter your email address. If you see two tabs, click **I am a guest** and enter your email address there.



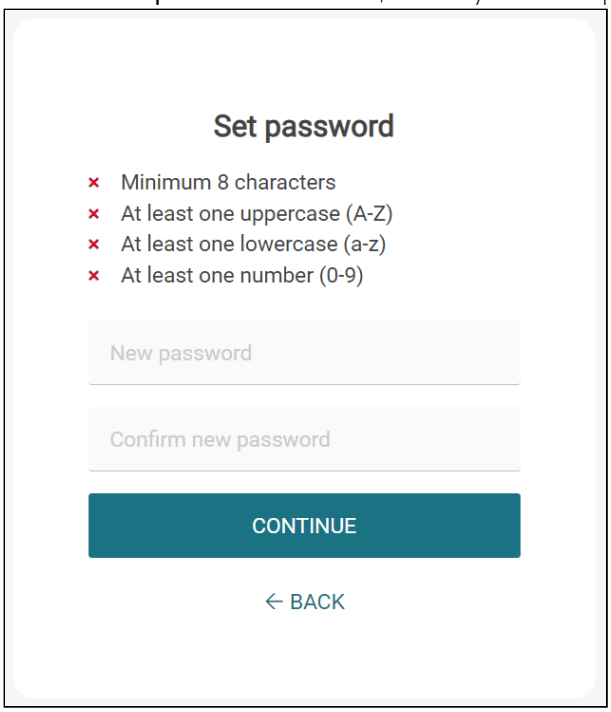
4. Click **Continue**.

5. You will receive an email with the verification link. If the email doesn't arrive, click **Send again**.

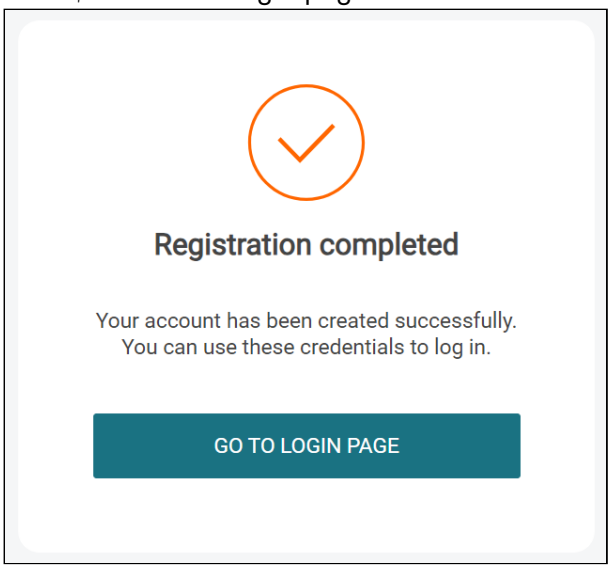


6. In the activation email, click **Activate your account**.

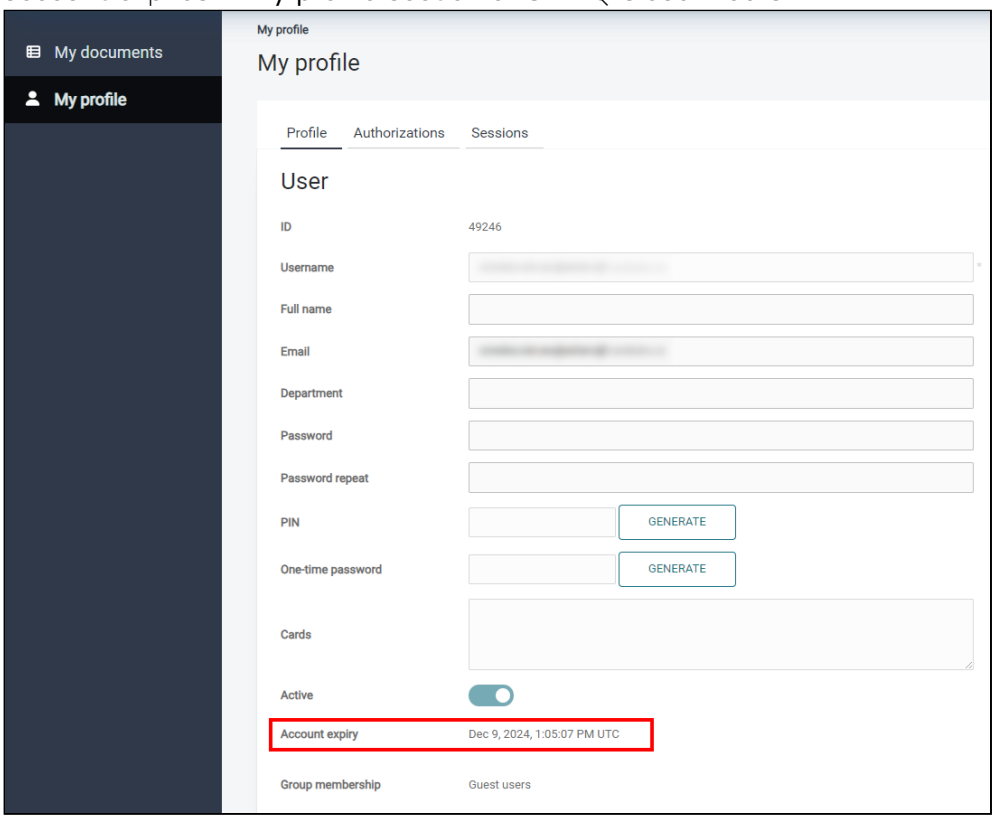
7. On the **Set password** screen, enter your new password for SAFEQ Cloud.



8. You will see a message that your registration is completed. If you wish to log in to SAFEQ Cloud, click **Go to login page**.

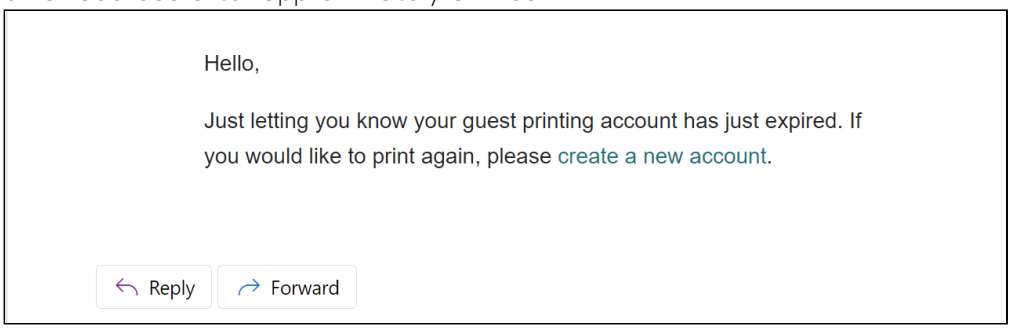


9. If the SAFEQ Cloud administrator set an expiration period, you will be able to see when your account expires in **My profile** section of SAFEQ Cloud Web UI.



10. After your account expires, you will receive an email notification. Expiration means that you won't be able to log in and your account will be deleted. You may register again using the same

email address after approximately an hour.



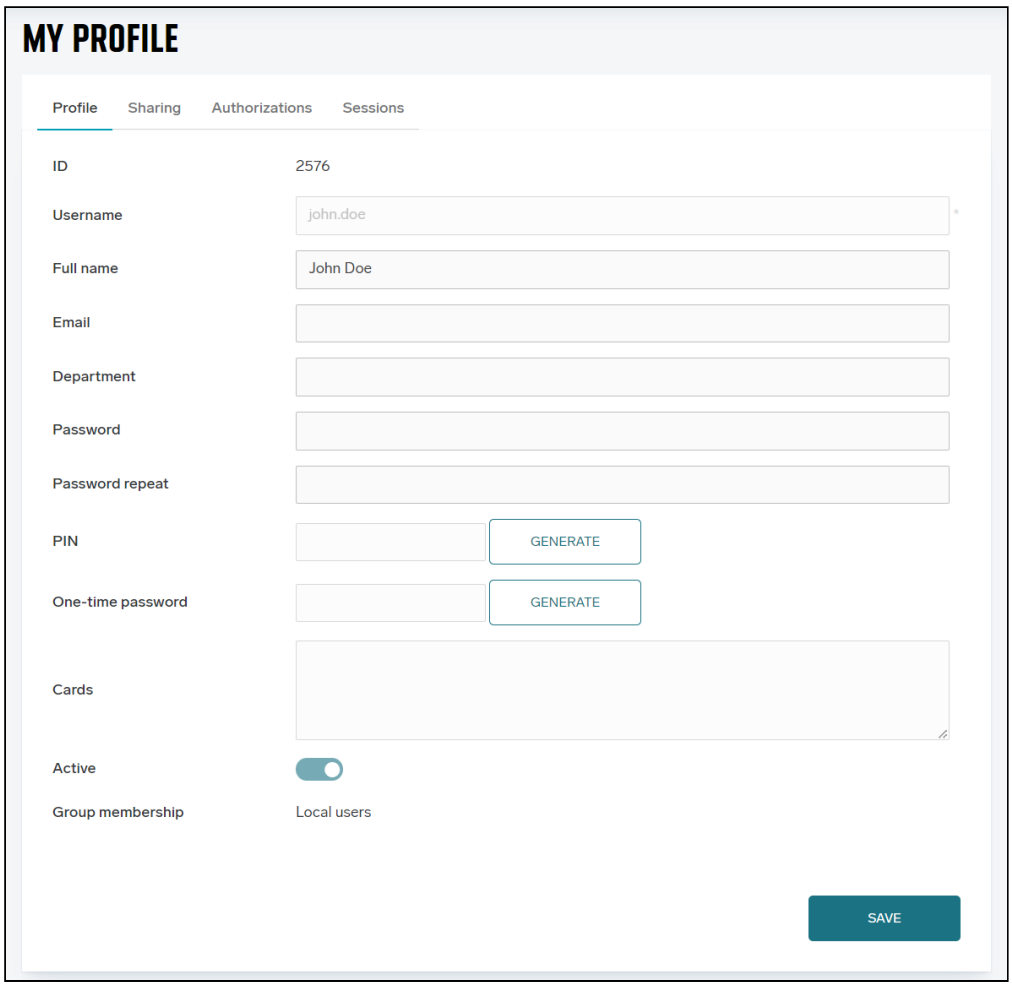
9.3.3 MY PROFILE

In the My profile section of the SAFEQ Cloud Web UI, you can find the following tabs:

- Profile – display or modify your profile information, generate a Short ID or a one-time password.
- Sharing – share your documents with other users.
- Printers – select your favorite queues from your available Print queues.
- Authorizations – display your authorizations for specific Scan workflow connector types.
- Sessions – display a list of OAuth sessions typically created by SAFEQ Cloud Clients or mobile applications.

Profile

You can modify your profile information directly using the Profile tab.



Depending on your access permissions, you can view and/or modify your profile.

If your account is a 'local user' account, you can:

- modify your full name, email address, and password.
- generate one-time passwords (see section *One-time passwords*).
- generate short IDs (PINs).

If your account is a 'directory account' (for example, LDAP or Microsoft Entra ID), you can:

- generate one-time passwords
- generate short IDs.

All other information is provided by the remote directory and cannot be changed.

For both types of accounts, some fields can only be changed by the administrator, for example, card ID or document release rights.

What you can do with your profile depends on the following permissions:

- ViewMyProfile – allows the user to view their profile
- ModifyMyProfile – allows the user to edit their profile
- GenerateOTP – allows the user to generate a one-time password

- **GenerateShortID** – allows the user to generate a short ID

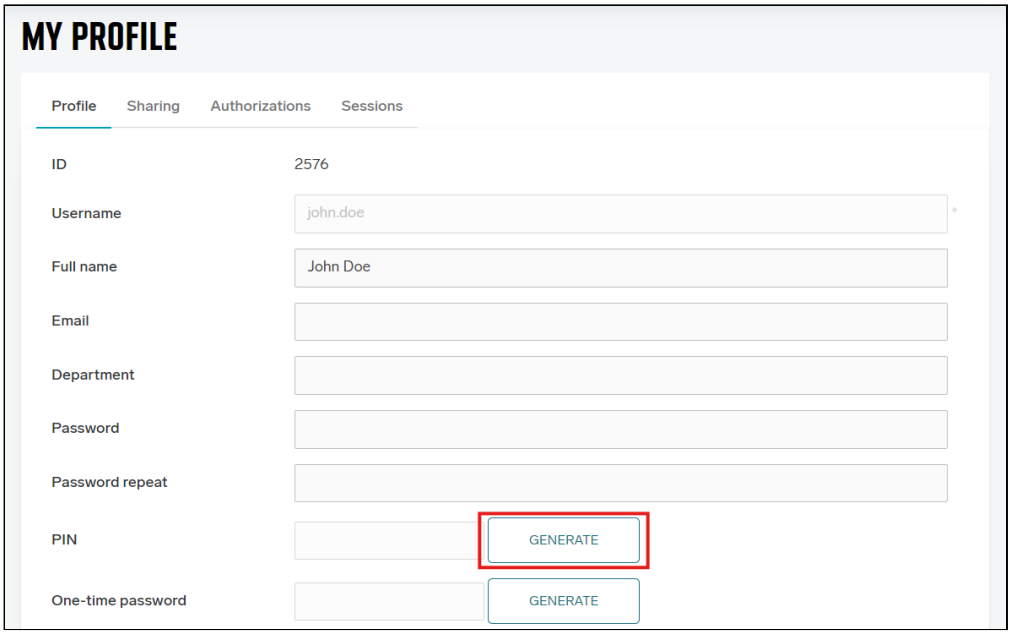
Short IDs

Short IDs can be used as one of the authentication methods at SAFEQ Cloud Embedded Terminals. The ways to generate a Short ID:

- You can generate/view a Short ID code yourself
- Administrators can set up an email with a Short ID to be sent to users automatically.

> To generate a Short ID, you must have the **EditMyProfile** and **GenerateShortID** permissions.

1. Log in to SAFEQ Cloud Web UI.
2. Navigate to **My profile** > **Profile**.
3. Click **Generate** beside **Short ID.**



4. Click **Save**.

One-time passwords

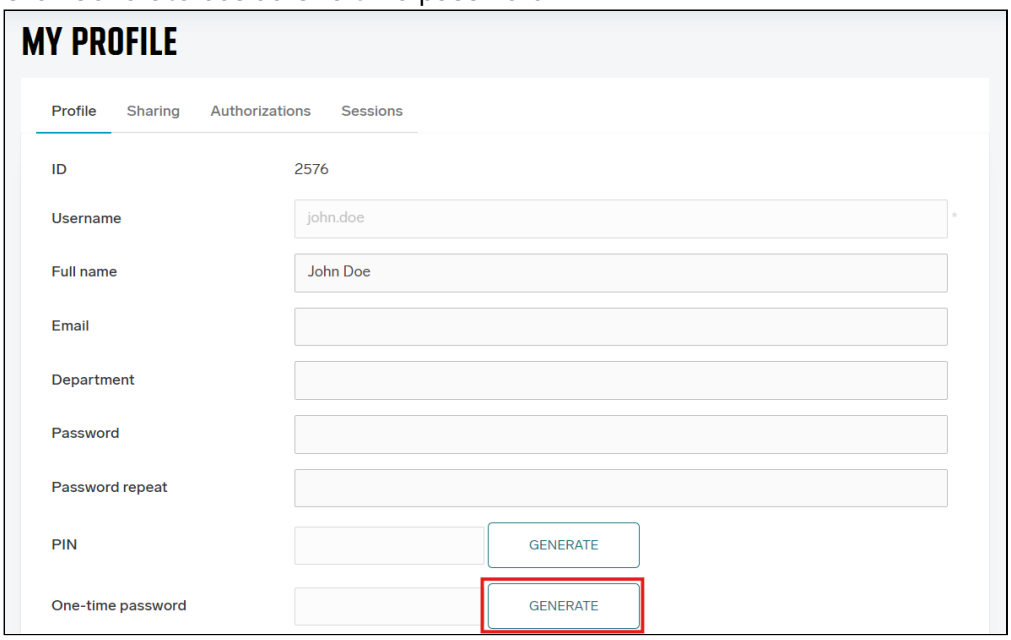
A one-time password (or OTP) is an authentication method where the generated password can only be used once. After you successfully authenticate with it, it is removed from your profile.

OTPs are useful in the following cases:

- You can generate/view an OTP and use it to register your card at an MFD.
- Administrators can set up an email with OTP to be sent to all users in the company who don't have a card associated with their account upon their first submission of a print job to a pull queue.

To generate an OTP, you must have the **EditMyProfile** and **GenerateOTP** permissions.

1. Log in to SAFEQ Cloud Web UI.
2. Navigate to **My profile** > **Profile**.
3. Click **Generate** beside **One-time password**.

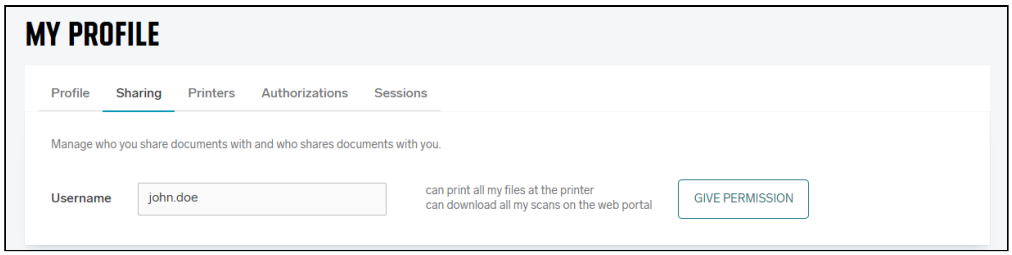


4. Click **Save**.

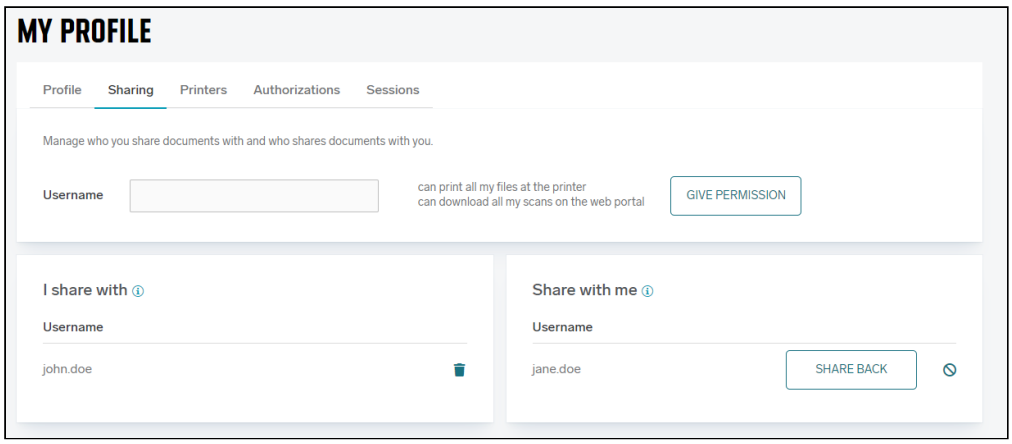
Sharing

In the **Sharing** tab you can add sharing permission to other users, so they can see and print/ download your documents/scans.

You can add users with whom you want to share your documents by typing their username and clicking on **Give permission** button.



In the bottom part of the page you have two lists which show with whom you are currently sharing your documents and who is sharing theirs with you.



You can remove these sharing permissions by clicking the **delete/deny** buttons. You can also use **Share back** button to quickly share your documents with that user.

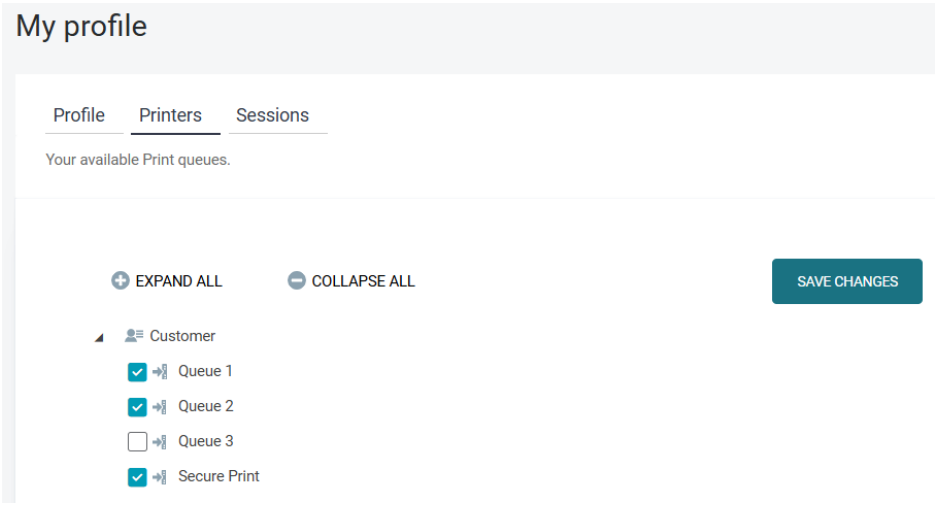
To see this panel you must have the **ViewUserSharingDocuments** permission and to add or remove sharing permission you must have **ModifyUserSharingDocuments** permission.

Printers

If your company has many direct queues in SAFEQ Cloud, you can go to the **Printers** tab and select your favorite queues out of all the queues you have access to (apart from the default queues assigned to you by your admin).

To see this section, you must have the **ViewUserInputPorts** permission.

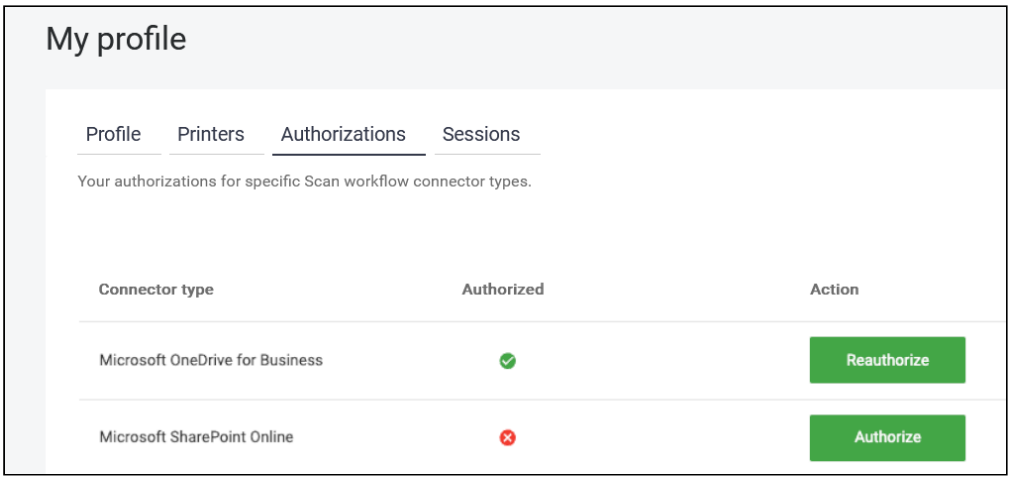
1. Log in to SAFEQ Cloud Web UI.
2. Click **My profile** and select the **Printers** tab.
3. You will see all available Print queues in an expandable tree based on the object tree structure (containers, etc) with the first level expanded. You can expand all or collapse the tree view items using the **Expand all** and **Collapse all** buttons.
4. Each print queue has a checkbox next to it. If the Print queue has the option **Available by default** enabled, it appears selected. This setting can be changed according to your selection, but it applies only to your account.
5. Click **Save changes** to save your selections.



Authorizations

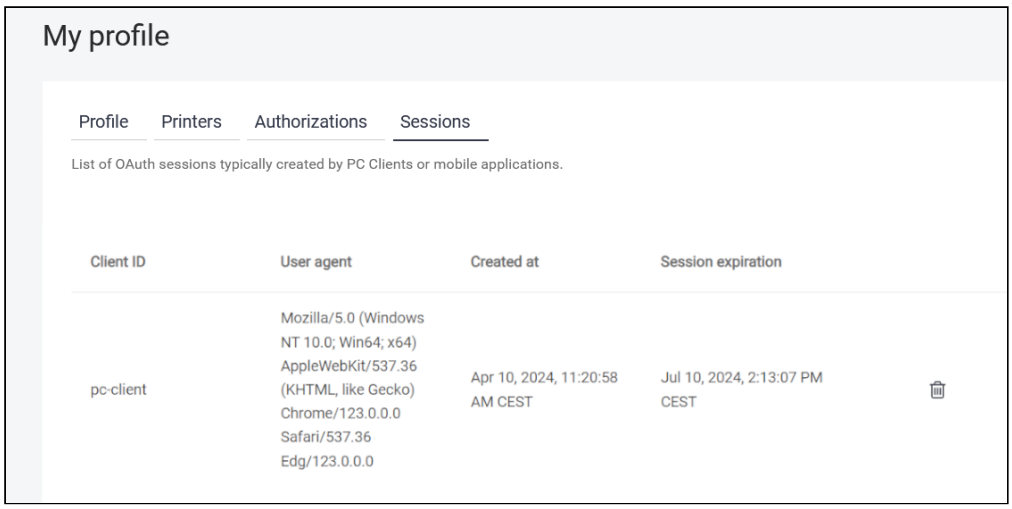
On the **Authorizations** tab, you can view the status of your authorizations for specific Scan workflow connector types. You will only see the connector types related to the Scan workflows for which you have access permissions. Authorization is required when you wish to use these Scan workflows.

Click **Authorize** to start the authorization process.



Sessions

The **Sessions** tab shows your sessions created typically by logging in via the mobile application or SAFEQ Cloud Client. Each session contains information about the client ID, the user agent used for authentication, the date and time of session creation, and the session expiration. The expiration can be extended by refreshing a refresh token, typically done automatically by the clients.



You can delete a session if you have permission to modify your account.

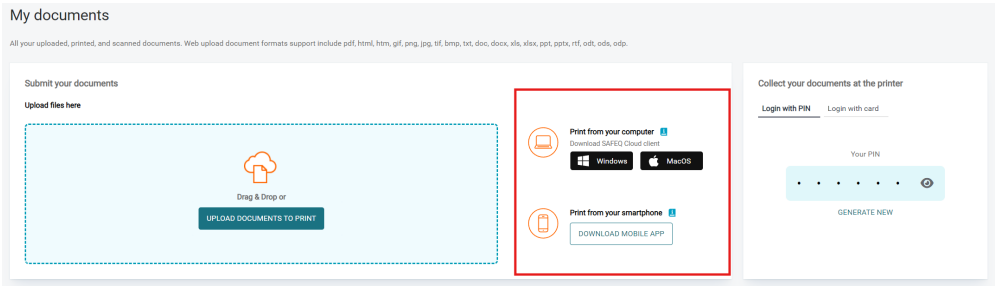
9.3.4 MY DOCUMENTS

In the My documents section of the SAFEQ Cloud Web UI, you can:

- Download the SAFEQ Cloud Client application (if you have the ViewClientAndMobileDownload permission).
- Download the mobile application (if you have the ViewClientAndMobileDownload permission).
- Upload documents for print.
- See your waiting print jobs, printed print jobs, and failed scan jobs.
- See your PIN and one-time password, and generate new ones (if you have GenerateShortID and GenerateOTP permissions respectively)
- Download your scanned documents.

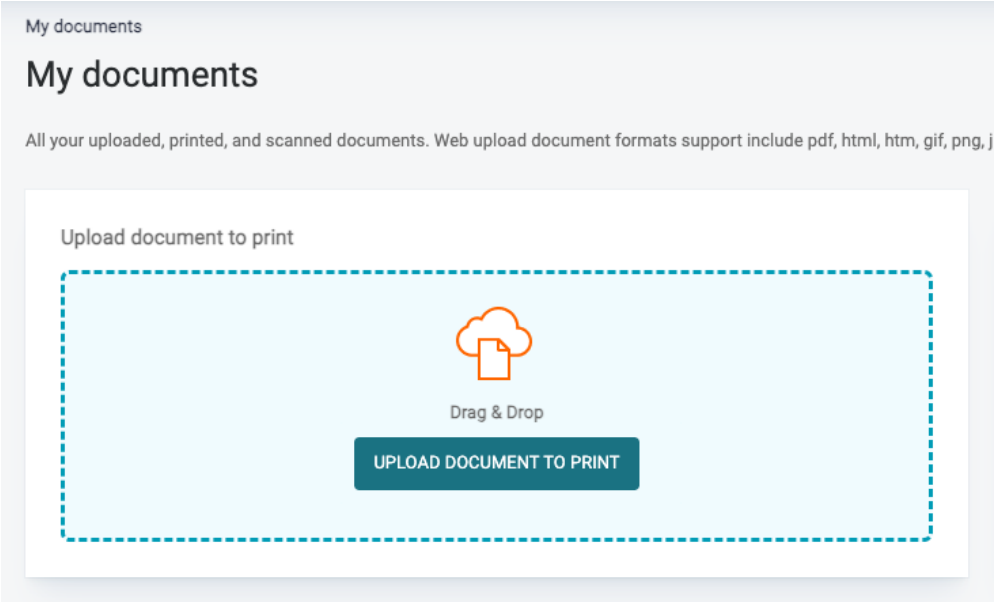
Downloading the SAFEQ Cloud Client and the mobile app

To download the SAFEQ Cloud Client, click the button with your operating system. To download the mobile app, click on the Download Mobile App button to display a pop-up window with installation and configuration QR codes for your mobile operating system.



Document upload

In this area, you can upload documents that you wish to print.

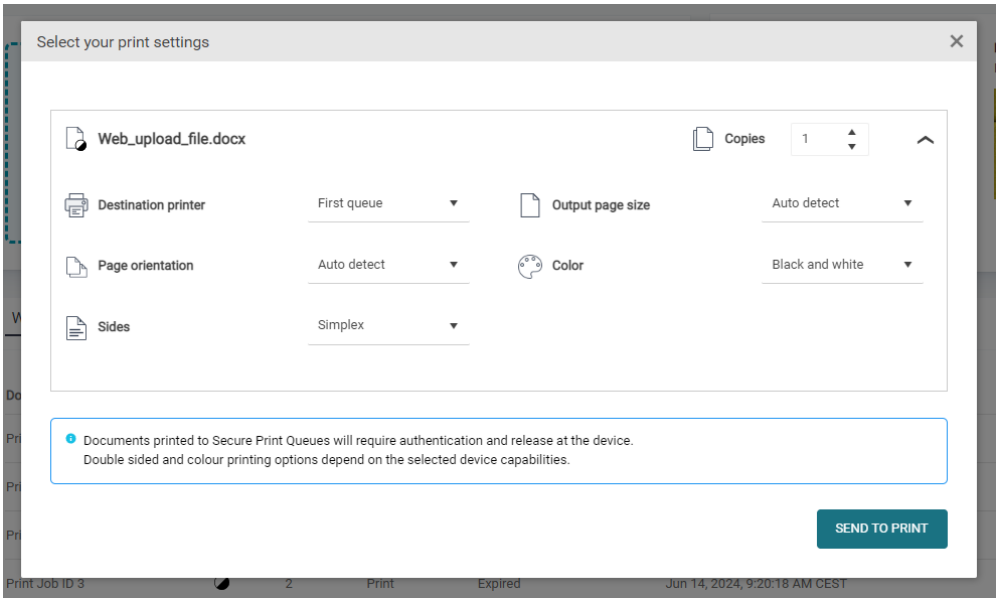


You will see this option only if the following conditions are fulfilled:

- Your administrator enabled it in **Settings > General settings > Web upload**.
- Your administrator granted you the **WebUploadDocument** and **AllowPullPrint** permissions.
- Your administrator has created at least one pull print queue in SAFEQ Cloud.

To upload a document:

1. Click **Upload document to print** or drag&drop one or more files into the area.
2. After the file(s) are uploaded, you will see a dialog window with finishing options. Modify the settings according to your needs.



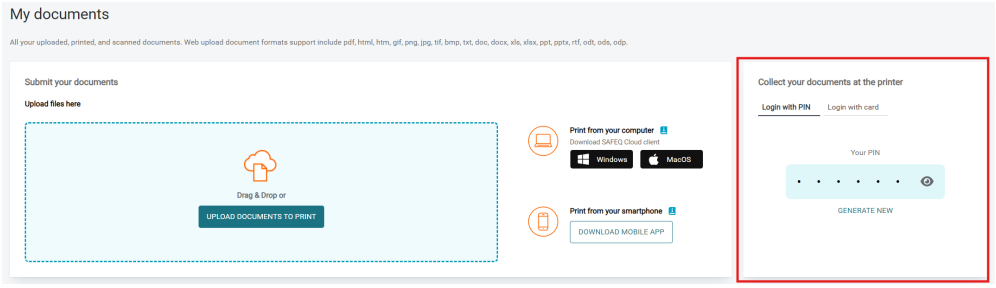
3. Click **Send to print**.
4. The print job(s) will appear on the tab with waiting print jobs.

Viewing and generating PIN and OTP

In this area you can see and generate new PIN and one-time password (OTP) in two tabs, one for PIN and one for OTP (often used for card registration).

You will be able to see and use them under these conditions:

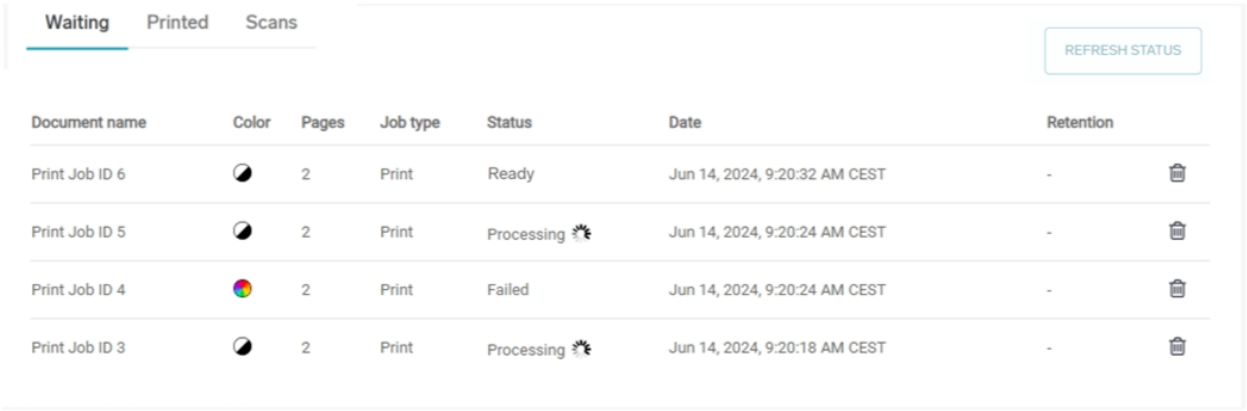
- Printer with set PIN authentication exists within your account (set up by administrator). This shows **Login with PIN** tab.
- Printer with set Card authentication exists within your account (set up by administrator). This shows **Login with card** tab.
- **GenerateShortID** and **GenerateOTP** permissions for generating PIN and OTP respectively



Managing print jobs and scan jobs

Waiting jobs

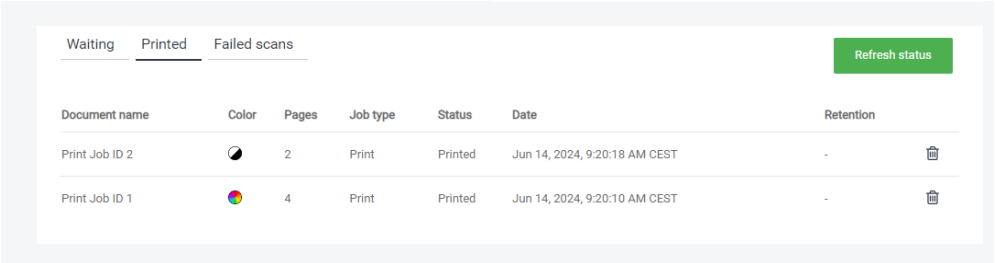
On the **Waiting** tab, you can display and delete your documents that are ready to print.



To delete a document, click the delete icon in the respective row. Note that you must have permission to delete jobs assigned to you.

Printed jobs

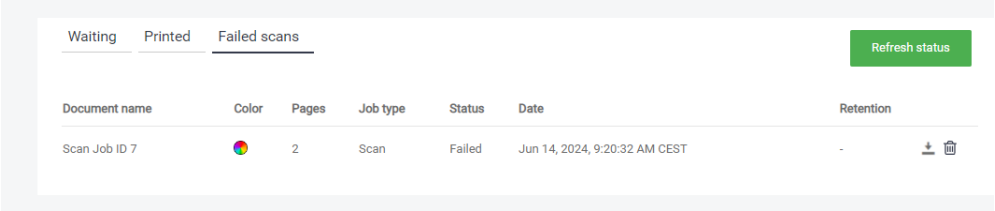
Display and delete your documents that were already printed.



To delete a document, click the delete icon in the respective row. Note that you must have permission to delete jobs assigned to you.

Scan jobs

Display, download, or delete your scanned documents that are still being processed, already processed or their scan workflow failed.



To delete a document, click the delete icon in the respective row. Note that you must have permission to delete jobs assigned to you. To download a scanned document, click the download icon.

The **Retention** column indicates the remaining time (in days) until the document is automatically deleted. The default value is 7 days but can be changed by your administrator.

The number of pages may not be provided for the scanned documents because they are not fully processed.

The document name consists of the scan workflow name and the time stamp. If SAFEQ Cloud is unable to obtain the workflow name, the document name is generated randomly.

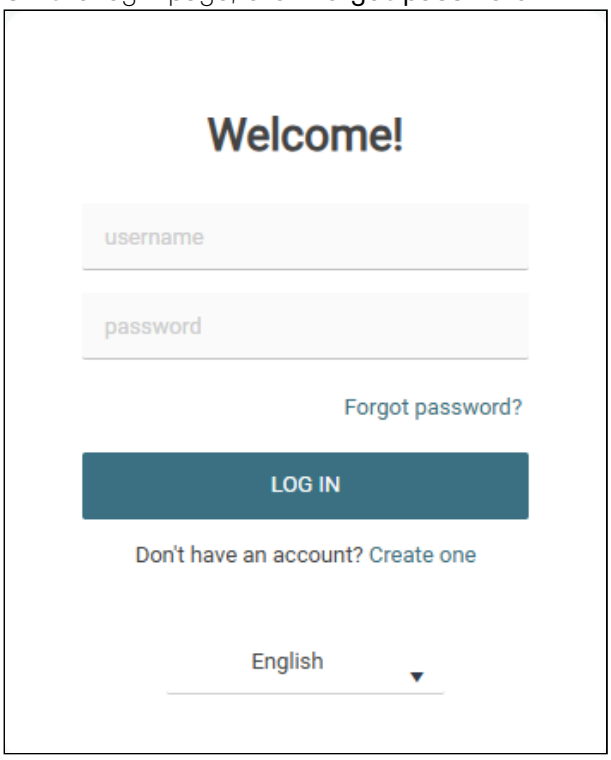
For documents in the Ready to download state there is triggered delete action when document is downloaded. Look at the Rules - triggers and automation for more details.

9.3.5 RESETING FORGOTTEN PASSWORD

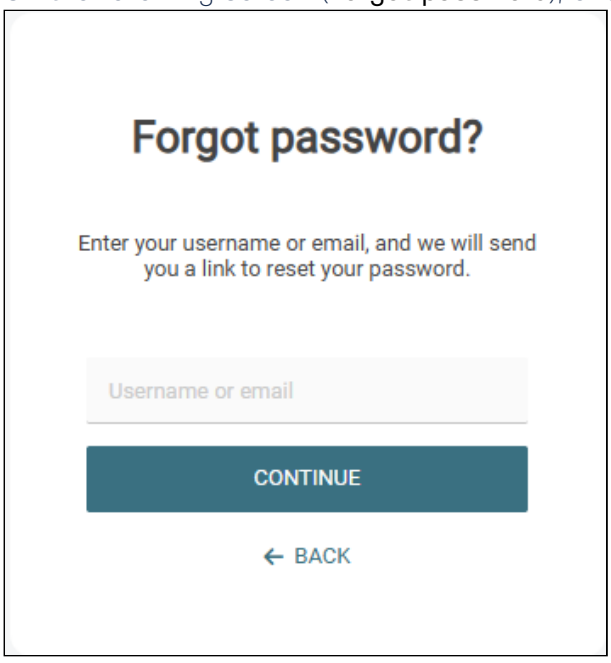
To reset forgotten password in SAFEQ Cloud, perform the below steps.

1. Open the SAFEQ Cloud Web UI address.

2. On the login page, click **Forgot password?**

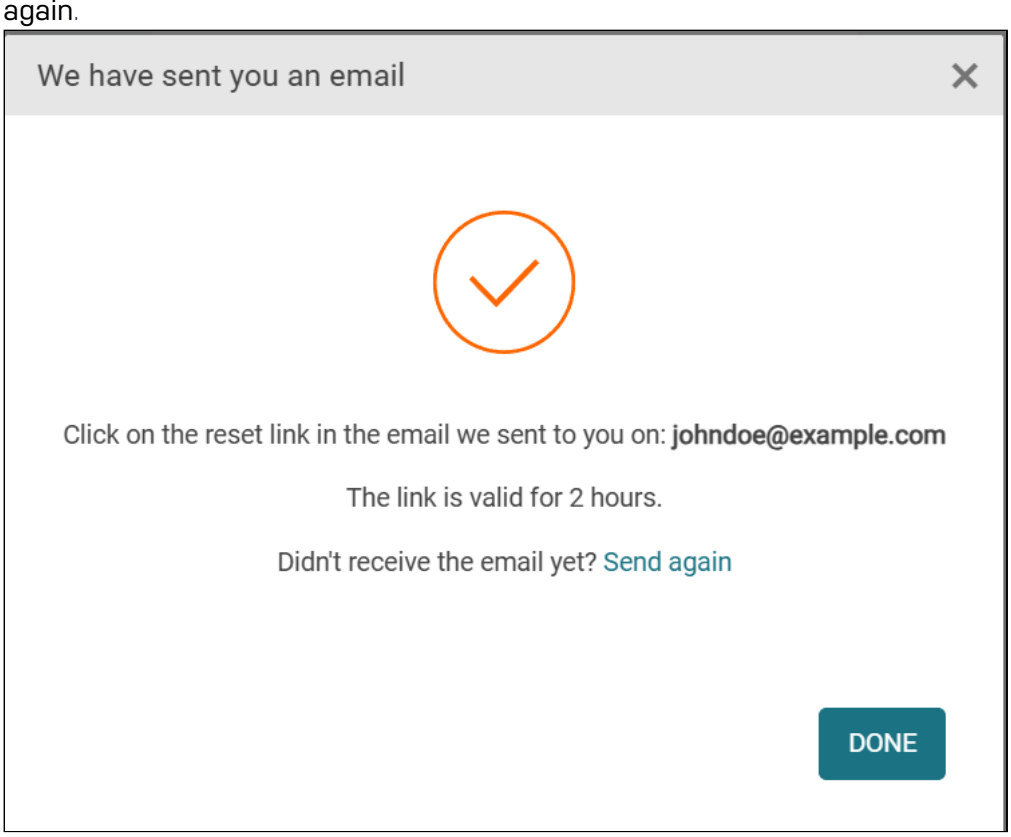


3. On the following screen (**Forgot password**), enter your username.

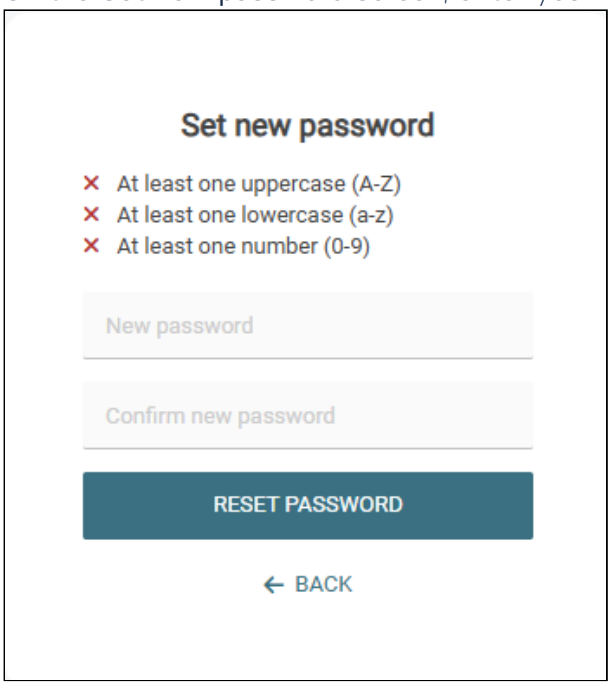


4. Click **Continue**.

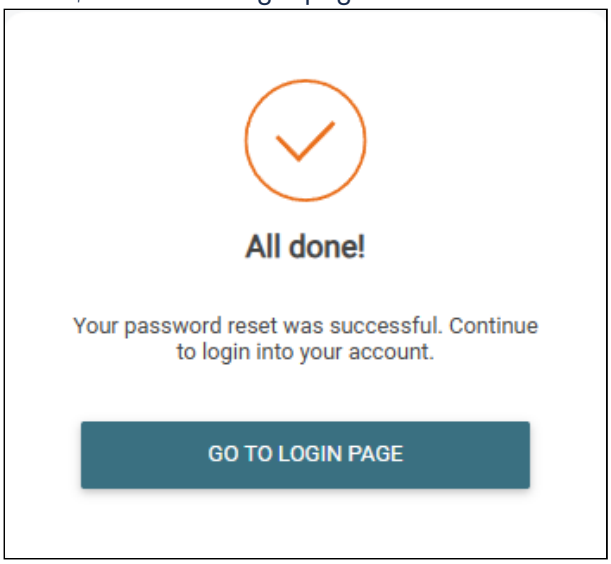
5. You will receive an email with the reset password link. If the email doesn't arrive, click Send again.



6. In the activation email, click Reset your password.
7. On the Set new password screen, enter your new password for SAFEQ Cloud.



8. You will see a message that your password reset is completed. If you wish to log in to SAFEQ Cloud, click **Go to login page**.



10 REFERENCE DOCUMENTS

This section contains in-depth materials about YSoft SAFEQ Cloud.

10.1 ASIAN FONTS SUPPORT FOR DIRECT PRINT

This article explains how to fix documents that are unreadable after printing due to missing fonts (particularly Asian fonts). This may happen if a PDF is uploaded to SAFEQ Cloud via public API. This solution is not applicable to the situation where a user submits the PDF document via the SAFEQ Cloud Client and the document is flattened and converted to PDF/A.

Background information

Once a print job is submitted via public API, the Primary or Secondary servers convert it. The goal is to convert any print job to PDF format. If the submitted job is a PDF already, the conversion process will leave it as is and the file will be spooled in the original format. When the job is released using direct print, another service converts it to the Postscript format. Sometimes, the printed document lacks certain fonts. Typically if the original contains Asian languages. You can solve this issue by adding the fonts into the operating system for your Primary or Secondary server and providing a configuration file for the Xpdf converter.

10.1.1 SOLUTION FOR CENTOS (RHEL)

Due to many languages and distributions, we only provide support for the most used platform - CentOS (RHEL). Packages and configuration can also be customized based on the customer's needs.

1. Check whether the CMap package is installed by running the following command:

```
rpm -q poppler-data
```

2. If it isn't, install it.

```
sudo yum install poppler-data
```

3. Install the required fonts, for example, Google Noto fonts. Note that the Xpdf converter does not support ttc (true type collections) such as google-noto-cjk. Use only otf or ttf format. Example:

```
sudo yum install google-noto-sans-japanese-fonts
```

```
sudo yum install google-noto-sans-korean-fonts

sudo yum install google-noto-sans-traditional-chinese-fonts

sudo yum install google-noto-sans-simplified-chinese-fonts
```

4. Prepare the xpdfrc configuration file for Xpdf converter. This file must have the following structure:

```
#----- begin Japanese support package
cidToUnicode    Adobe-Japan1    /usr/share/poppler/cidToUnicode/Adobe-Japan1
unicodeMap      ISO-2022-JP     /usr/share/poppler/unicodeMap/ISO-2022-JP
unicodeMap      EUC-JP          /usr/share/poppler/unicodeMap/EUC-JP
unicodeMap      Shift-JIS       /usr/share/poppler/unicodeMap/Shift-JIS
cMapDir         Adobe-Japan1    /usr/share/poppler/cMap/Adobe-Japan1
toUnicodeDir                    /usr/share/poppler/cMap/Adobe-Japan1
fontFileCC      Adobe-Japan1    /usr/share/fonts/google-noto/NotoSansJP-Regular.otf
#----- end Japanese support package
```

   - You can download the file here.
   - Or from Y Soft CDN using the following command:

     ```
     sudo wget https://cdn.everyoneprint.com/conversion/xpdfrc
     ```

     In this case, we use mapping to the poppler-data resources. As conversion fonts, we use installed NotoSans regular otf versions.

5. Place the xpdfrc file in the /etc/ folder.

6. Set the permissions for the file to 644 at minimum.

```
sudo chmod 644 xpdfrc
```

For Xpdf configuration in general, see https://www.xpdfreader.com/xpdfrc-man.html.

For Xpdf language support, see https://www.xpdfreader.com/download.html.

10.2 ASIAN FONTS SUPPORT FOR MS OFFICE DOCUMENTS CONVERTED TO PDF

This article explains how to fix documents that are unreadable after printing due to missing fonts (particularly Asian fonts). This may happen if an MS Office document is uploaded to SAFEQ Cloud via public API. The solution is not applicable to the situation when a user submits the MS Office document via the SAFEQ Cloud Client and the document is converted to PDF/A before the print job is uploaded to SAFEQ Cloud.

Background information

Once a print job is submitted via public API, the Primary or Secondary servers convert it. The goal is to convert any MS Office document to PDF format. Sometimes, the printed document lacks certain fonts. Typically if the original contains Asian languages. You can solve this issue by adding the fonts into the operating system for your Primary or Secondary server.

10.2.1 SOLUTION FOR CENTOS (RHEL)

Due to many languages and distributions, we only provide support for the most used platform - CentOS (RHEL). The list of installed fonts can be customized based on the customer's needs.

1. Install the required fonts in your Primary or Secondary server. We can recommend Google Noto fonts. If you wish to increase the success rate, install the MS core fonts as well. The converter works with common true type font formats such as ttf, otf and collection ttc. For basic Asian support, you can install the CJK (Chinese, Japanese, Korean) set:

   ```
   sudo yum install google-noto-cjk-fonts
   ```

2. Check whether the fontconfig library is already installed in your server by using the following command:

   ```
   rpm -q fontconfig
   ```

3. If it isn't, install it.

   ```
   sudo yum install fontconfig
   ```

4. Rebuild the font cache to include the newly installed fonts.

   ```
   sudo fc-cache -r -v
   ```

10.3 MIGRATION OF AUTHENTICATION PROVIDERS AND SSO TO PORT 443

This guide outlines the steps required to migrate your Single Sign-On (SSO) and authentication provider configurations to port 443. Alternatively, you can set it up in a way to keep port 8443 working.

- If you need the authentication working via both the 8443 port and the 443 port, do not update your existing Redirect URLs. Just add a new HTTPS URL without the port specified to the list of Redirect URLs for your authentication provider. The result will be that in the values for the Redirect URL, you will have two records for each callback - one with the old port e.g.:

`https://<domain>:8443/<callback>` and one without port number: `https://<domain>/<callback>`.

- If you wish to only use port 443, update your existing Redirect URLs by removing port 8443.

We do not recommend using Redirect URLs with an explicitly specified port 443, as some authentication providers may check for the presence of this port, and most web browsers omit this standard HTTPS port after accessing a web address.

10.3.1 MICROSOFT ENTRA ID

OAuth 2.0 and OIDC configuration

The general process for migrating Microsoft Entra ID configurations for OAuth 2.0 and OpenID Connect (OIDC), as well as the creation of applications in Azure, is similar, as both protocols are built on the same foundation. For more details, see Add a custom app in Microsoft Entra ID and Microsoft Entra authentication.

1. Log in to Microsoft Entra Admin Center as an administrator.
2. Navigate to **App registrations**. Find and select the application you wish to update.
3. Click **Authentication Settings**. In your app registration overview, click **Authentication** in the left menu.
4. In the **Redirect URIs** section, scroll down to **Redirect URIs**.
5. Update the **Redirect URI**. You'll see a list of current Redirect URIs that are configured to handle authentication responses.
   - Locate URIs that reference port 8443 and depending on your use case, either remove the 8443 port, or add a new URI record as follows: `https://<domain>/<callback>`.
   - The domain should be the same as the one of the SAFEQ Cloud Web UI URL. For example, if your SAFEQ Cloud Web UI URL is `https://print.acme.com:8443/some/callback`, the new value should be: `https://print.acme.com/some/callback`
6. Save and test your changes.

SAML configuration

To migrate SAML Single Sign-On configuration in Microsoft Entra ID, perform the following steps. For more details about Microsoft Entra, see Microsoft Entra Single Sign-On.

1. Log in to Microsoft Entra Admin Center as an administrator.
2. Go to **Enterprise applications** > **All applications**. Find and select the application you wish to update. You can use the search bar to find and select the application for which you need to update the SAML SSO settings.
3. Go to the **Single Sign-On Settings**. Within your selected application, click **Single sign-on** in the left menu. This will open the SAML-based SSO configuration page.

4. Update the Identifier (Entity ID): https://<domain_name_that_has_saml_configured>/. Change SSO issuer ID optional parameter in Single sign-on authentication settings in your account to match this value if it is filled in.

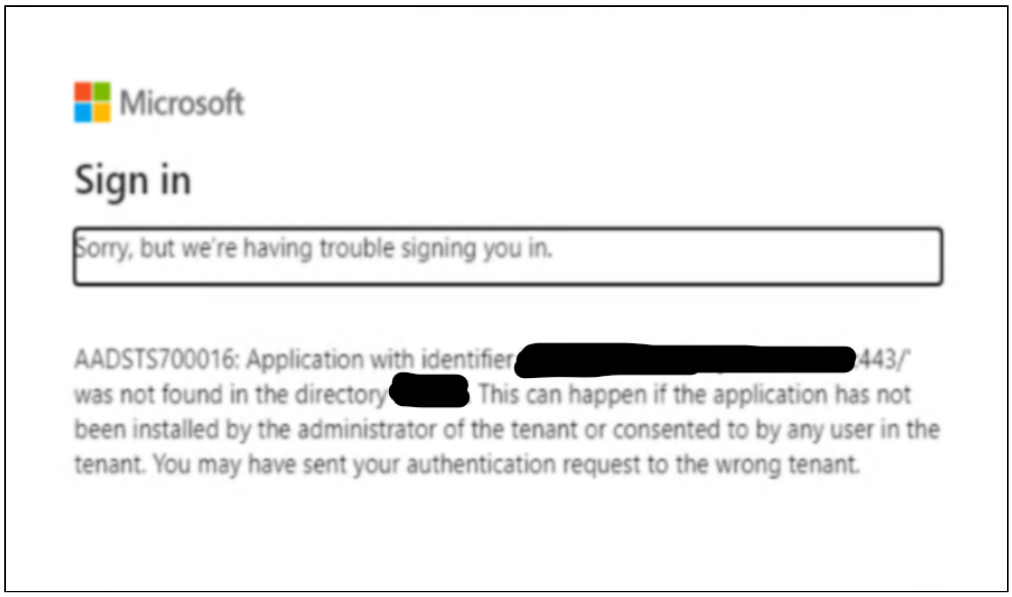
   > ⚠ SAFEQ Cloud Client with OAuth2 login will use a port based on connection to SAFEQ Cloud, i.e. either 8443 or standard HTTPS port 443. To make both ports work, you can either:
   >
   > - have two URIs in Entity ID, one without the port, i.e. `https://<domain_name_that_has_saml_configured>` and one with port specified, i.e. `https://<domain_name_that_has_saml_configured>:8443/`
   > - or specify the SSO issuer ID optional parameter in the Single sign-on authentication settings in your account to match the URI specified in Entity ID, e.g. `https://<domain_name_that_has_saml_configured>/`

5. Update the Sign-On URL: `https://<domain_name_that_has_saml_configured>/assertion/saml`
6. Update the Reply URL : `https://<domain_name_that_has_saml_configured>/assertion/saml`
7. Save and test your changes.

Troubleshooting

OAuth2 authentication stops working in SAFEQ Cloud Client when used with Single sign-on: "Sorry, but we're having trouble signing you in."

You get the following message from Microsoft, saying "Application with identifier 'https://[domain_name]:443/' was not found in the directory...":



This can be caused by SAFEQ Cloud Client opening an authentication page with a different port than expected by the Microsoft Entra ID application for SAML SSO.

To fix this, you can either:

update Microsoft Entra ID application for SAML SSO:

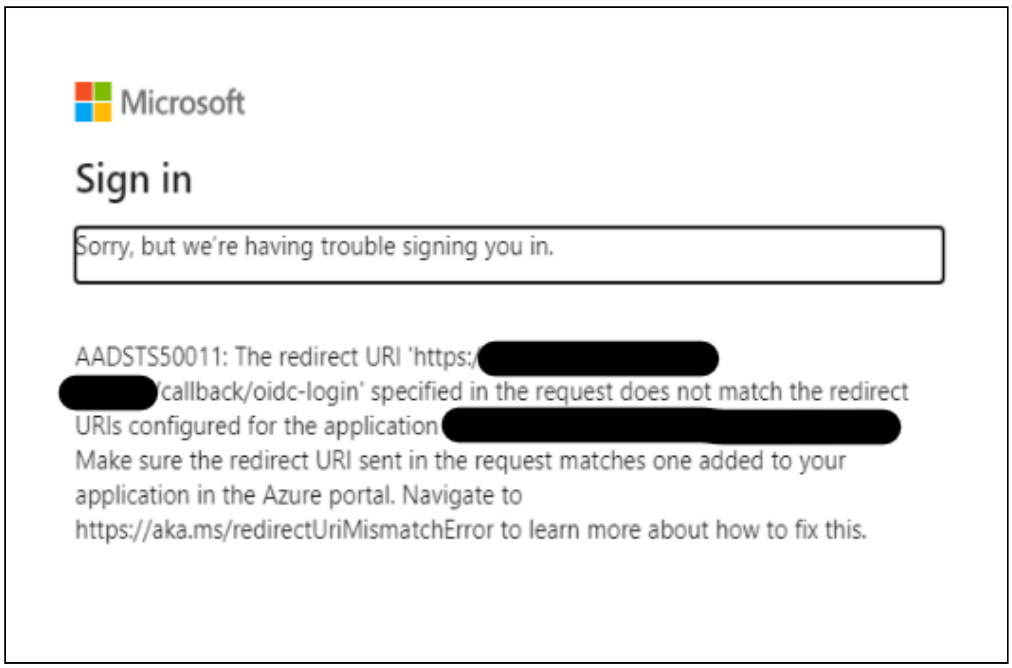
1. Navigate to Microsoft Entra Admin Center in your web browser and sign in with your administrator credentials.
2. Select Enterprise applications and then select All applications. Find and select the application you wish to update. You can use the search bar to find and select the application for which you need to update the SAML SSO settings.
3. Access Single Sign-On Settings. Within your selected application, click on Single sign-on in the left-hand menu. This will open the SAML-based SSO configuration page.
4. In Identifier (Entity ID), depending on your use case, either remove port 8443 from the URI, or add a new record as follows: `https://<domain_name_that_has_saml_configured>/`.
5. If you added a record, you will now have two URIs in Entity ID – one without the port specified (i.e. `https://<domain_name_that_has_saml_configured>/` and one with port specified, i.e, `https://<domain_name_that_has_saml_configured>:8443/)`.
6. Save and test your changes.

or update Single sign-on authentication settings in your account:

1. Log in to SAFEQ Cloud Web UI.
2. Navigate to Authentication > Single sign-on.
3. Specify the optional parameter SSO issuer ID to match the URI specified in Entity ID in your Microsoft Entra ID application for SAML SSO (e.g. `https://<domain_name_that_has_saml_configured>/`).
4. Save and test your changes.

OAuth2 authentication stops working in SAFEQ Cloud Client when used with Microsoft Entra ID Customizable authentication: "Sorry, but we're having trouble signing you in."

You get the following message from Microsoft, saying "The redirect URI 'https://[domain_name]/callback/oidc-login' specified in the request does not match the redirect URIs configured for the application...":



This can be caused by SAFEQ Cloud Client opening the authentication page with a different port than the Microsoft Entra ID application for OIDC expects.

To fix this, update the Microsoft Entra ID application for OIDC:

1. Navigate to Microsoft Entra Admin Center in your web browser and sign in with your administrator credentials.
2. Navigate to **App registrations**. Find and select the application you use for OIDC in your authentication provider. You can search for it by name if needed.
3. Access **Authentication Settings**. In your app registration overview, click on "Authentication" in the left-hand menu.
4. Locate the **Redirect URIs Section**. Scroll down to the **Redirect URIs** section.
5. In **Redirect URI**, you'll see a list of current Redirect URIs that are configured to handle authentication responses.
6. Depending on your use case, either remove the 8443 port from the URIs, or add new records as follows: `https://<account-domain>/callback/oidc-login` and `https://<account-domain>/callback/acl` (replace `<account-domain>` with other addresses you have configured for port 8443).
7. If you added new records, you will now have 4 addresses in total (two with port 8443 and two without port specified).
8. Save and test your changes.

10.3.2 OKTA

OIDC configuration

To migrate OIDC Okta to port 443, perform the following steps. For more details about Okta, see OKTA Authentication.

1. Log in to the Okta Admin Console as administrator.
2. Navigate to Applications. Find and select the application for which you need to update the redirect URLs.
3. In the application settings, go to the General tab and click Edit.
4. In the Sign-in redirect URIs section, depending on your use case, either remove the 8443 port number from the existing records, or add new URI records as follows: `https://<domain>/callback/oidc-login` and `https://<domain>/callback/acl`.
5. Save and test your changes

SAML configuration

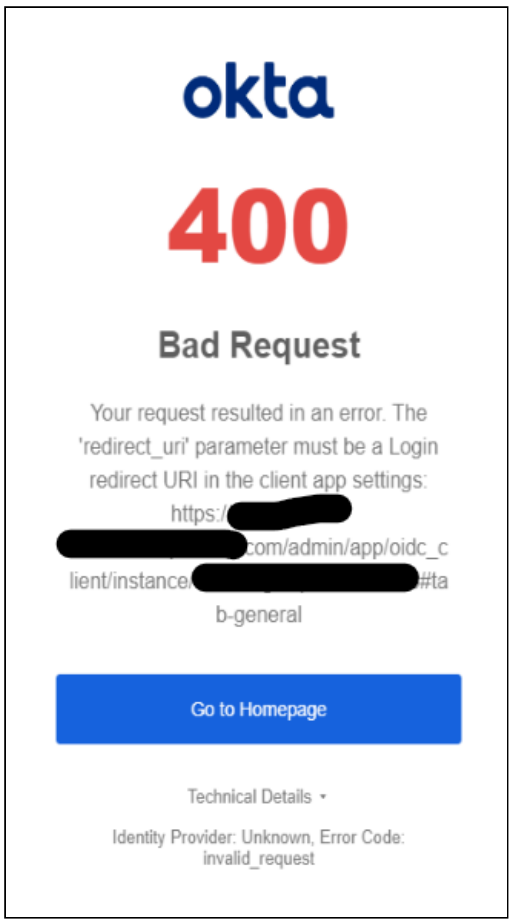
To migrate SAML Single Sign-On in Okta to port 443, perform the following steps. For more details about Okta, see Okta Single Sign-On / Logout.

1. Log in to the Okta Admin Console as administrator.
2. Navigate to Applications. Find and select the application for which you need to update the SAML SSO settings.
3. Locate the Single Sign-On URL and depending on your use case, either remove the 8443 port number from the existing URL or add a new URI value as follows: `https://<account-domain>/assertion/saml`.
4. Update the Audience URI (SP Entity ID). Change the SSO issuer ID optional parameter in Single sign-on authentication settings in your account to match this value if it is filled in.
5. Review and update any additional URLs, such as Logout URL, in case they contain port 8443.
6. Save and test your changes.

Troubleshooting

OAuth2 authentication stops working in SAFEQ Cloud Client when used with Okta Customizable OIDC authentication

You get the following message from Okta saying: "The 'redirect_uri' parameter must be a Login redirect URI in the client app settings...":



This can be caused by SAFEQ Cloud Client opening the authentication page with a different port than the Okta application for OIDC expects.

To fix this, update Okta application for OIDC:

1. Access the Okta Admin Console and log in with your administrator credentials.
2. Navigate to **Applications**, find and select the application for which you need to update the redirect URLs.
3. In the application settings, go to the **General** tab and click **Edit**.
4. In the **Sign-in redirect URIs**, add `https://<account-domain>/callback/oidc-login` and `https://<account-domain>/callback/acl` (replace `<account-domain>` with other addresses you have configured for port 8443)
5. You should now have 4 addresses in total (two with port 8443 and two without port number specified).
6. You can add more addresses in **Configure SAML settings** > **SAML Settings** > **show Advanced Settings** > **Other Requestable SSO URLs**.
7. Save and test your changes.

10.3.3 PINGID

OAuth 2.0 configuration

To migrate OAuth 2.0 PingId Single Sign-On to port 443, perform the following steps. For more details about PingId, see PingID Single Sign-On and Add a custom app in the Ping identity platform.

1. Log in to the PingID Admin Console as administrator.
2. In the main menu, click Applications.
3. Select the OAuth2 Worker that you need to update.
4. In the OAuth2 Worker settings, go to Redirect URIs.
5. Locate the URI that reference port 8443 and depending on your use case, either remove the 8443 port number from the existing URIs, or add new one as follows: `https://<account-domain>/callback/ping`.
6. Save your changes

SAML configuration

To migrate SAML PingId Single Sign-On to port 443, perform the following steps. For more details about PingId, see PingID Single Sign-On.

1. Log in to the PingID Admin Console as administrator.
2. In the main menu, click Applications.
3. Select the specific application for which you need to update the SAML SSO settings.
4. In the selected application, go to Configuration settings.
5. In the Assertion Consumer Service (ACS) URL, either remove the 8443 port or add a new record as follows: `https://<account-domain>/assertion/saml`.
6. Update Entity ID - change the SSO issuer ID optional parameter in Single sign-on authentication settings in your account to match this value if it is filled in.
7. Update any other relevant URLs (e.g., Single Logout URL) - if they include the port number, remove it.
8. Save your changes

10.4 INSTALL KM CLOUD TERMINAL WITHOUT MARKETPLACE

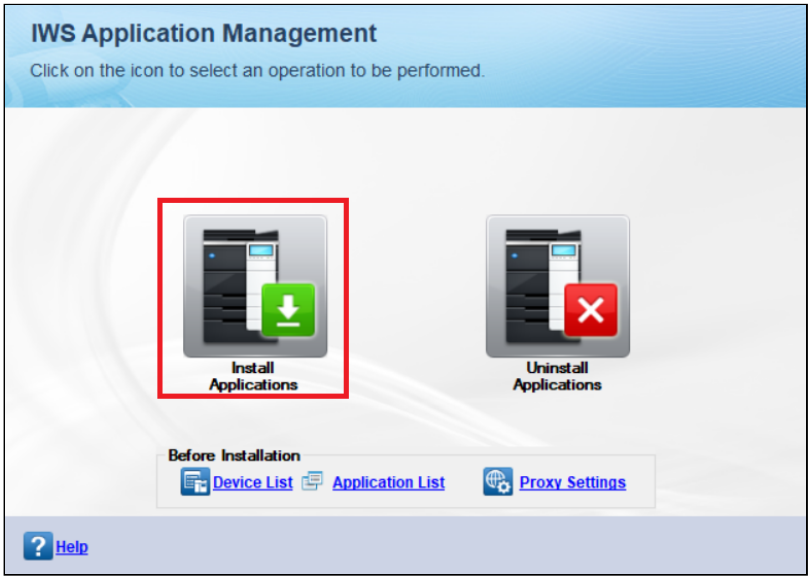
IWS Install Tool is provided by Konica Minolta.

The screenshots in this guide may look different than your version of the IWS Install tool.

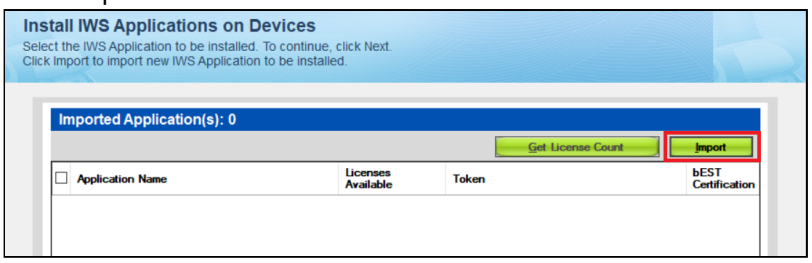
This feature is not available in the US or Canada.

If you have no access to MarketPlace in your region, you can side-load the KM Cloud Terminal.

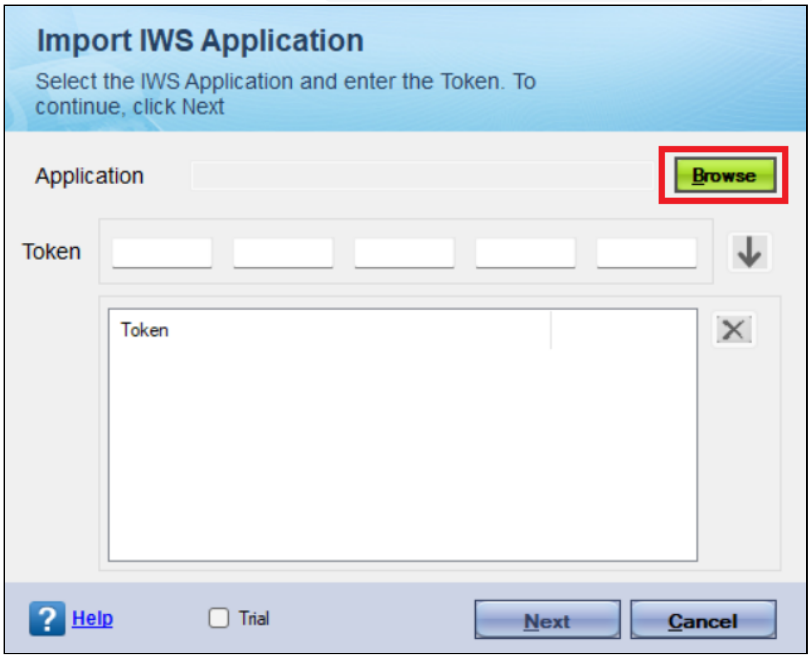
1. Obtain the IWS Install Tool from Konica Minolta.
2. Install the tool on your PC.
3. Request the KM Cloud Terminal application (the `SAFEQ Cloud Terminal.iws` file) from Y Soft support.
4. Run IWS Install Tool.
5. Import the file with the terminal:
   a. Select **Install Applications**.



   b. Click **Import**.



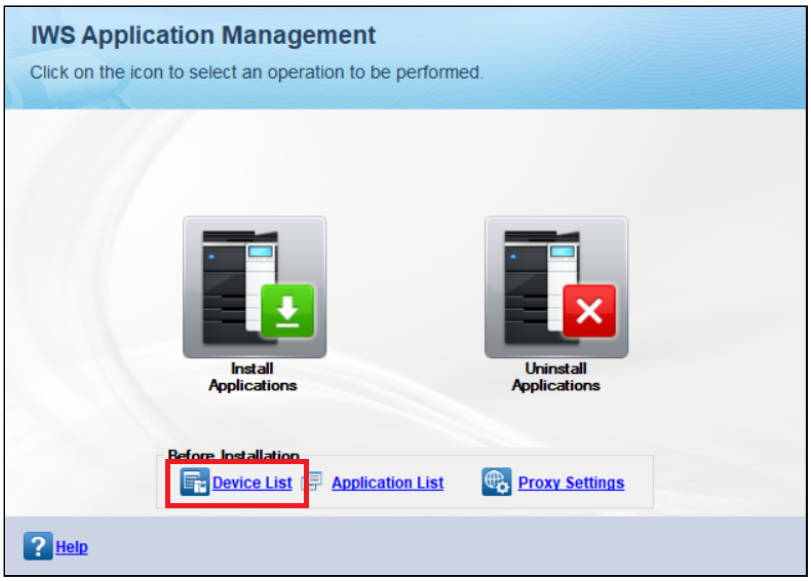
c. Click **Browse**, select the `SAFEQ Cloud Terminal.iws` file and then click **Next**.



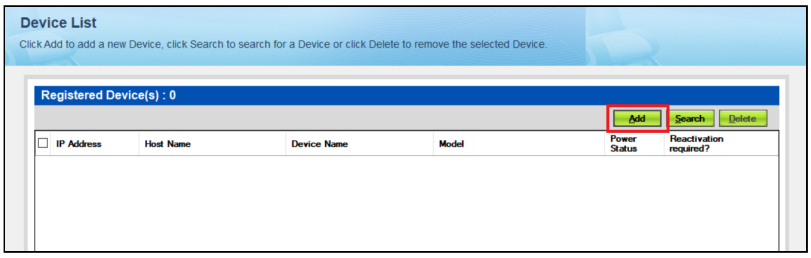
d. Agree with the license and click **Import**.

6. Add your MFD(s):

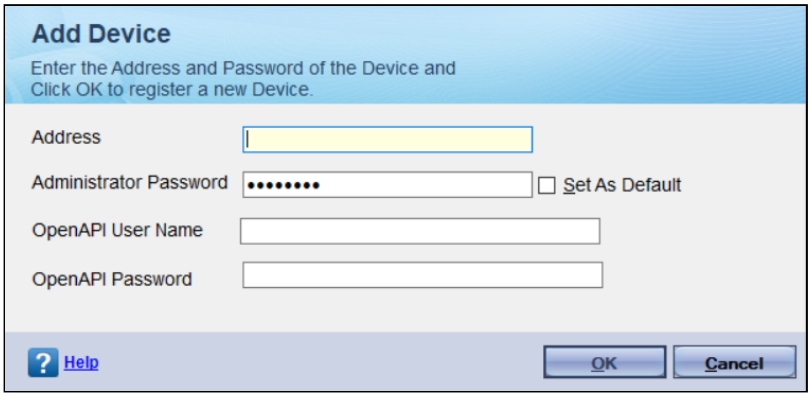
a. Back on the home screen, click **Device List**.



b. Click **Add**.

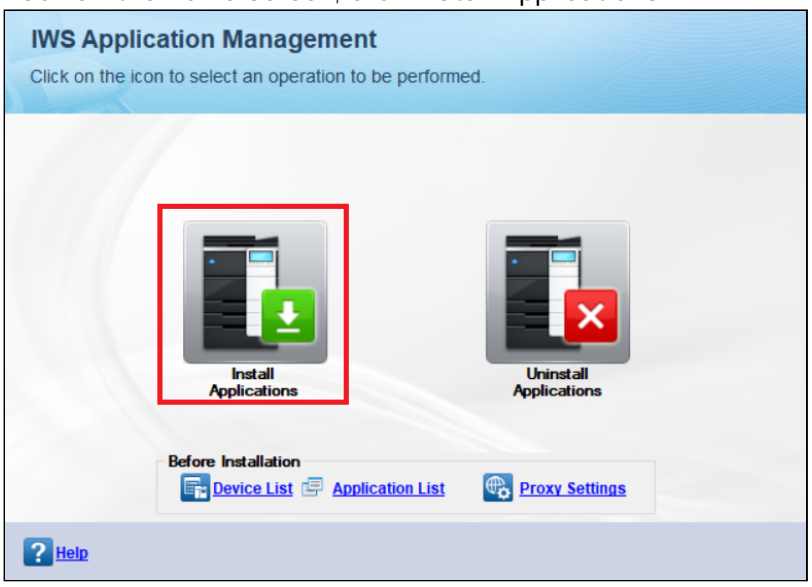


c. Fill in the IP address of the MFD and the administrator password. Click **OK**.

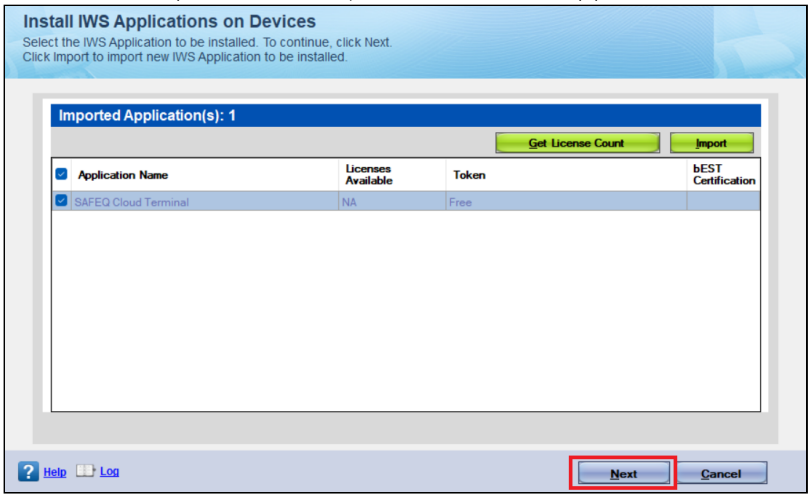


7. Install the terminal:

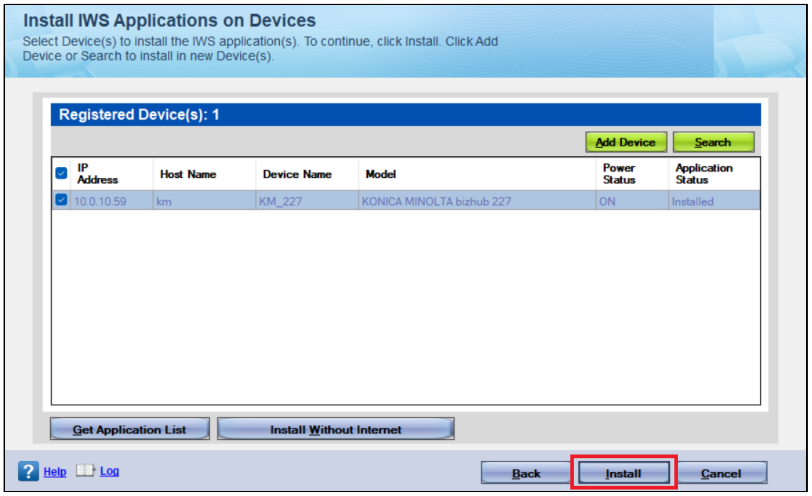
a. Back on the home screen, click **Install Applications**.



b. Select the imported SAFEQ Cloud Terminal application and click **Next**.



c. Check the correctness of information about your newly added MFD and then click **Install**.



d. After successful installation, click **Finish**.

11 LEGACY DOCUMENTATION

The Legacy section contains documents that are still valid but haven't yet been reworked to fit our new standards for documentation.

11.1 TECHNICAL INTRODUCTION

YSoft SAFEQ Cloud is a distributed document platform.

- Send documents from any number of sources; PC workstations, mobile devices, Host and mainframe systems, thin clients, ERP systems, from backend systems via API's and much more.
- Store documents securely or push the documents directly to an output device, such as a multi-function printer or single function printer.
- Use the mobile Apps, embedded MFD client software or swipe card readers to release documents on the selected printer.

11.1.1 THE CONCEPT OF SERVICES

SAFEQ Cloud is made up of modular services which can run anywhere, allowing for extremely flexible deployments, to meet virtually any customer infrastructure requirement.

A service performs a specific action. For example, the **Authentication Service** is responsible for communicating with the customers authentication system to authenticate users, whether it's Active Directory/LDAP, Microsoft Entra ID or similar. The **Document Output** service is responsible for delivering print job data from SAFEQ Cloud to a printer or MFD.

In f SAFEQ Cloud, the following services exists:

Service type	Description
API	For programmatically interacting with SAFEQ Cloud, for example from external applications, automation scripts or similar
Authentication	The Authentication Service is the service which communicates with AD/LDAP directories, Microsoft Entra ID and similar to authenticate users
Conversion	The conversion service is responsible for converting or preparing documents in one format to another, for example, converting a Word document to PDF

Service type	Description
Document Output	Responsible for delivering print job data to printers or MFD's
IPP	The IPP service receives print job data from SAFEQ Cloud Clients (Windows, Mac and Linux)
Mobile	The Mobile Print service is a service handling communication from Y Soft Apps, MDM solutions, Wide Area Mobile Print DNS communication and similar
Storage	The Storage Service is responsible for transferring and storing documents
Terminal Client	The service which deploys embedded software release terminal clients running inside MFD's, and the service to which MFD's communicate back for authentication, retrieving jobs etc
Messaging	Messaging configuration is used to enable YSoft SAFEQ Cloud to deliver messages, such as email, to users. The emails delivered by YSoft SAFEQ Cloud could be emails with files from "Scan to email" actions on an MFD or similar.

Let's take an example: A user sends a push print job from a workstation through SAFEQ Cloud for printing directly on a printer:

1. The user sends the jobs from the workstation client and the **IPP Service** receives the job
2. The **Authentication Service** authenticates the user against customer's LDAP
3. The **Storage Service** transfers the document internally in SAFEQ Cloud and stores the document data
4. The **Conversion Service** prepares the document for processing, converting if needed
5. The **Document Output Service** transforms and delivers the print job to the destination printer

The services could effectively be located anywhere, the IPP Service on a server in London, the Authentication Service on a server in New York and the Document Output Service in Singapore.

11.1.2 SERVERS

Services can be configured to run on any server, either a server running in a remotely hosted environment, or locally within the customers environment, either on-premise, or in the customers own private cloud, such as Amazon Web Services or Microsoft Azure.

When installing SAFEQ Cloud, you have the choice for installing:

Primary server – the primary server runs Web UI's for configuration and management, handles core communication and connection to backend databases and similar master roles

Secondary gateway server – the secondary servers are additional server gateways which can run services.

Some important points:

- A "server" can take any form, it can be either a hardware or software appliance, or it can be implemented on existing server infrastructure, virtual or physical.
- A "server" can run anywhere, in the public cloud, private cloud, completely disconnected on-premise, or on-premise connected to a primary in the cloud for central management
- A "server" no matter if it's primary or secondary, can run a single service or all services, depends on the features needed for that particular node.
- A single service can be used by many different customers
- There can be any number of primary and secondary gateway servers, from just single individual servers, to tens of thousands of servers in a very large distributed configuration, without a single point of failure.

More information on information about gateways and possible configurations can be found in the section Gateway Guide with recommended configurations.

11.1.3 ACCOUNT TYPES

There are 2 types of accounts that can be created:

Vendor – Vendor accounts are reseller or partner accounts, for example, a reseller or a subsidiary of a partner. Vendor accounts can have its own authentication, users and permissions. Vendors can have servers hosting services, but Vendors themselves cannot have printers or other document functionality. There is no licensing on the Vendor level.

Account – Customer accounts are for end-customers and can have full document functionality, with printers, ports, authentication, users, permissions etc. Accounts can have their own servers associated with them, running their own services. Accounts must have licensing, and have a trial license by default on account creation.

NFR or demo accounts for Vendors themselves are created as the Account type.

11.1.4 DOMAIN NAMES

DNS names are essential in how vendor and customer accounts are identified by the system, and how different accounts are identified.

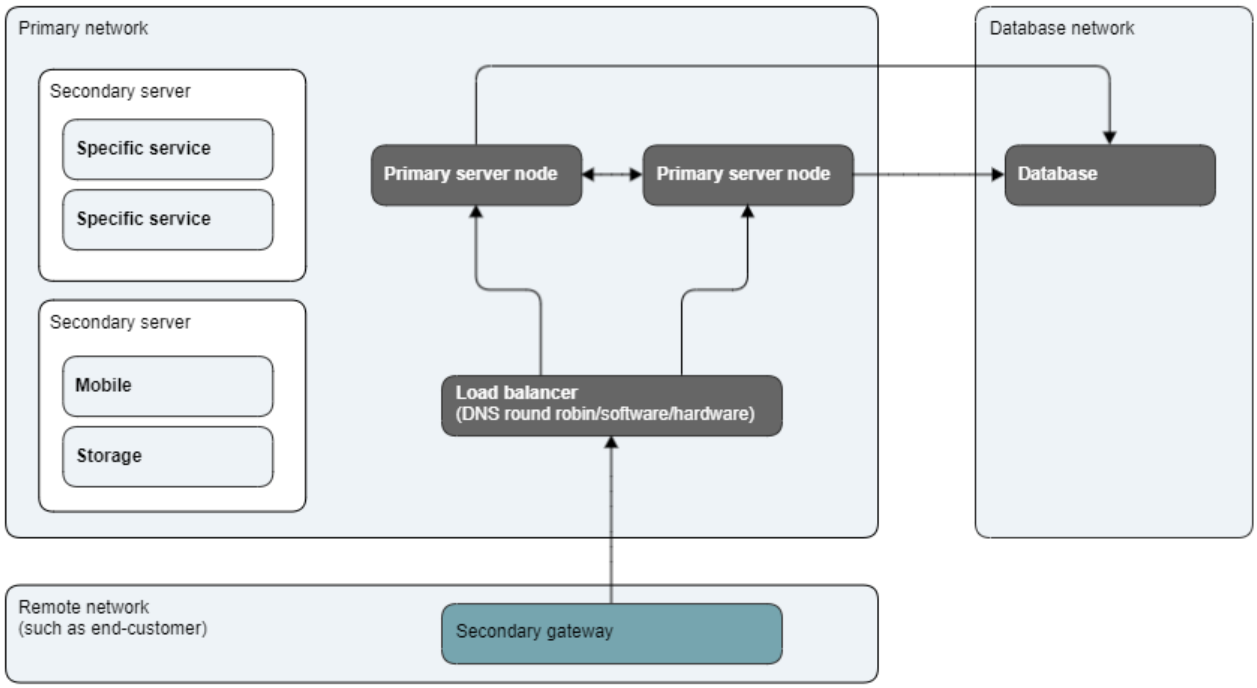
For example, the primary server runs the Web UI, and depending on which domain is accessing this server, a different account is shown. For example:

The DNS "print.partner.com" points to the primary SAFEQ Cloud server, and when the Web UI is accessed in a browser using this "print.partner.com" the SAFEQ Cloud server knows that it's a user for the partner viewing the Web UI
The DNS "print.customer.com" points to the same primary SAFEQ Cloud server, and when this is loaded, it's the customers Web UI which loads

11.2 HOW TO..

11.2.1 CONFIGURE A PRIMARY SERVER CLUSTER

The following is a quick step-by-step guide for installing and configuring SAFEQ Cloud in a high-availability cluster environment.



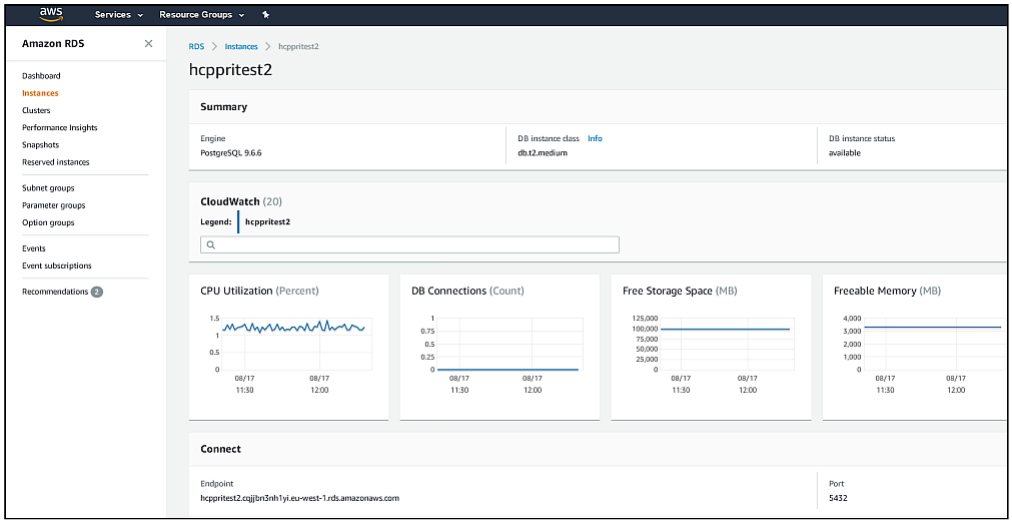
Designing solutions for high availability is a complex and often difficult task, as the cluster is only as strong as the weakest link, and it can be extremely hard to find the balance between uptime requirements, cost and complexity.

This guide will not cover design principles for high availability, configuration of load balancers or database clusters, but will assume those are in place already.

In this example we are using an Amazon RDS Postgresql for our database cluster and Amazon Network Load Balancer to distribute the load across 2 primary server cluster nodes. This is a simple example with just 2 nodes behind a single load balancer, but the entire setup could be expanded with redundancy everywhere and effectively zero point of failure, and any number of primary servers for scalability and availability.

Configure external database

The first step is to ensure a database is available to all primary cluster nodes.



In this example we have configured a Postgresql database cluster in Amazon's RDS service. Any database service, such as Microsoft's Azure Database for PostgreSQL or a manually configured external database could be used.

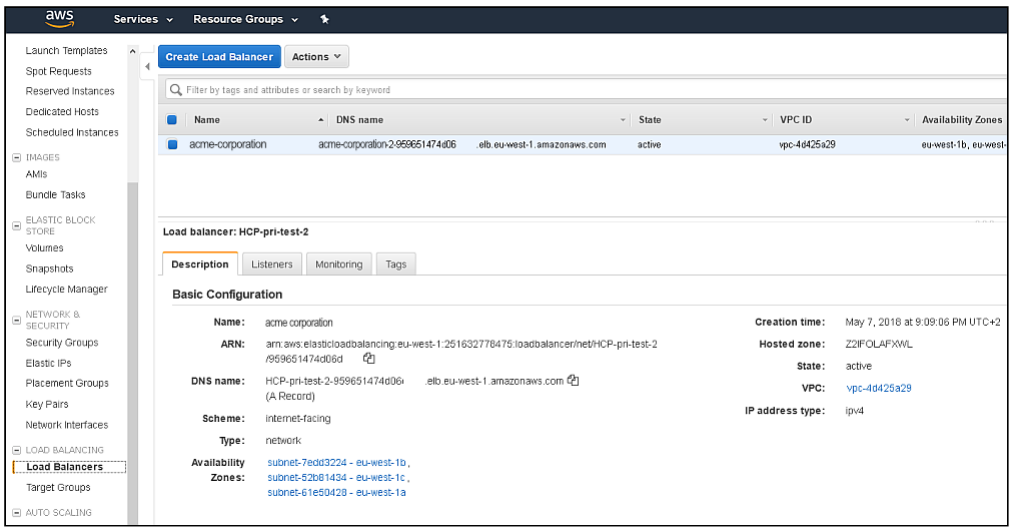
Configure load balancing

Second step is to configure the load balancer which will receive requests and distribute load across the primary server nodes in the cluster.

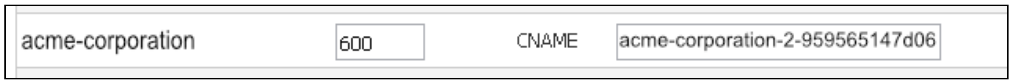
There are numerous ways to load balance, the most simple and most cost effective being simply round-robin DNS. This is a method of load balancing, which does not require a dedicated software or hardware node. In this technique, multiple IP addresses are associated with a single domain name, and then clients are given an IP in round robin fashion, simply assigned to clients on a time based method, evenly distributing load. Some DNS services, such as Amazon Route53, are sophisticated and can check for the destination IP being healthy before giving the IP to the client.

Generally we would always recommend dedicated software or hardware load balancers for environments with high uptime requirements.

> The only real important thing about load balancer, is to use a load balancer which supports persistent connections.



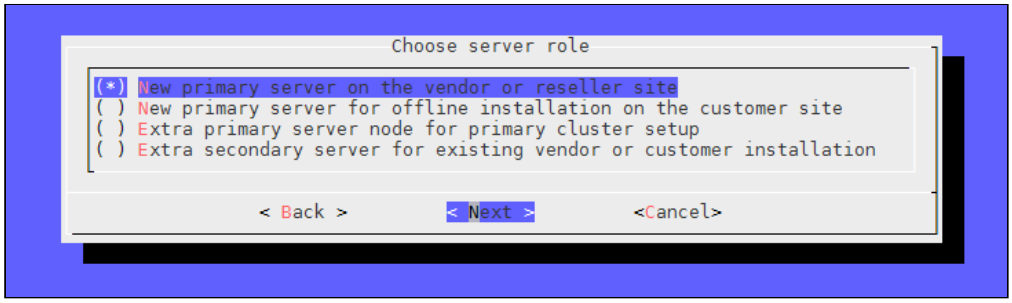
In this example we have configured an Amazon Network Load Balancer but similar services could be Azure Load Balancer.



We have further created a shorter and more pretty DNS CNAME record for our primary server cluster, so we don't use the long load balancer URL provided by Amazon.

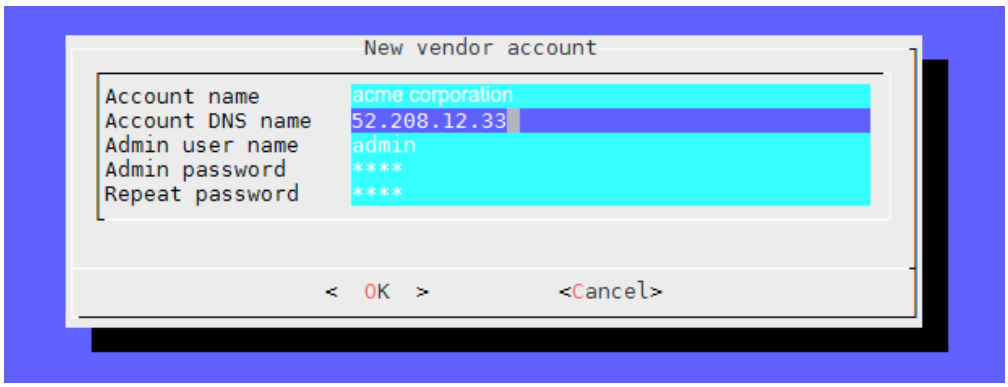
Install the first primary

On the first primary server, run the installer as normal and choose a "New primary.." type of role for the server. This can be either a **new primary for vendor or reseller site**, or a **new primary for an offline customer**, depending on the desired final installation type. See Server Installation in custom deployment scenario for more information.



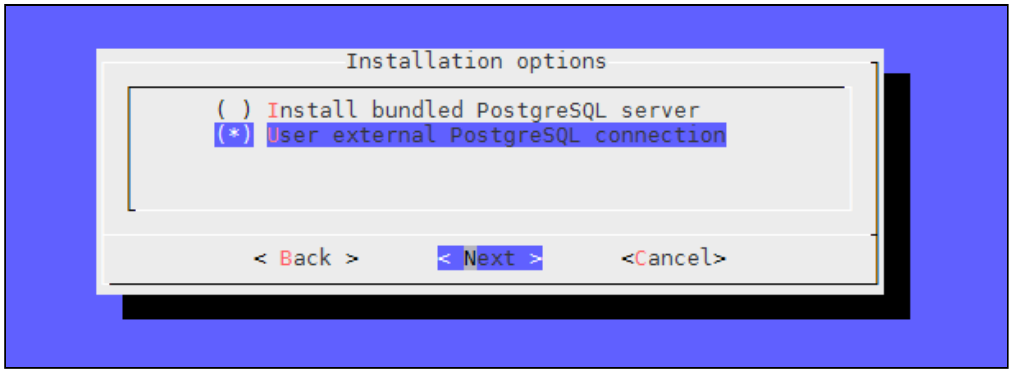
In this example, we will host many customers in the multi-tenant configuration, so we'll choose the **New primary server on the vendor site**.

Next adding the Vendor information, we choose as the account domain, to use the IP address of the first primary server.

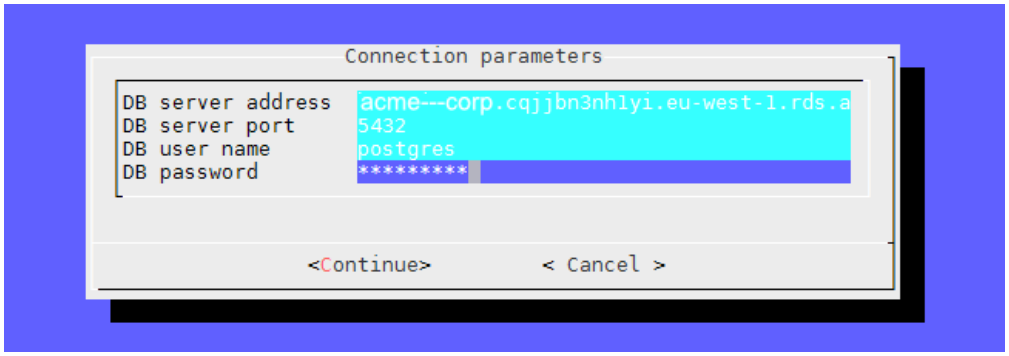


This way we don't rely on the load balancer to function in order to be able to access the first primary server. This is not required, but just a helpful step, when first configuring the cluster. The IP address can always be removed later in the Web admin interface, from account domains under root account settings.

Next, choose to use an external database.

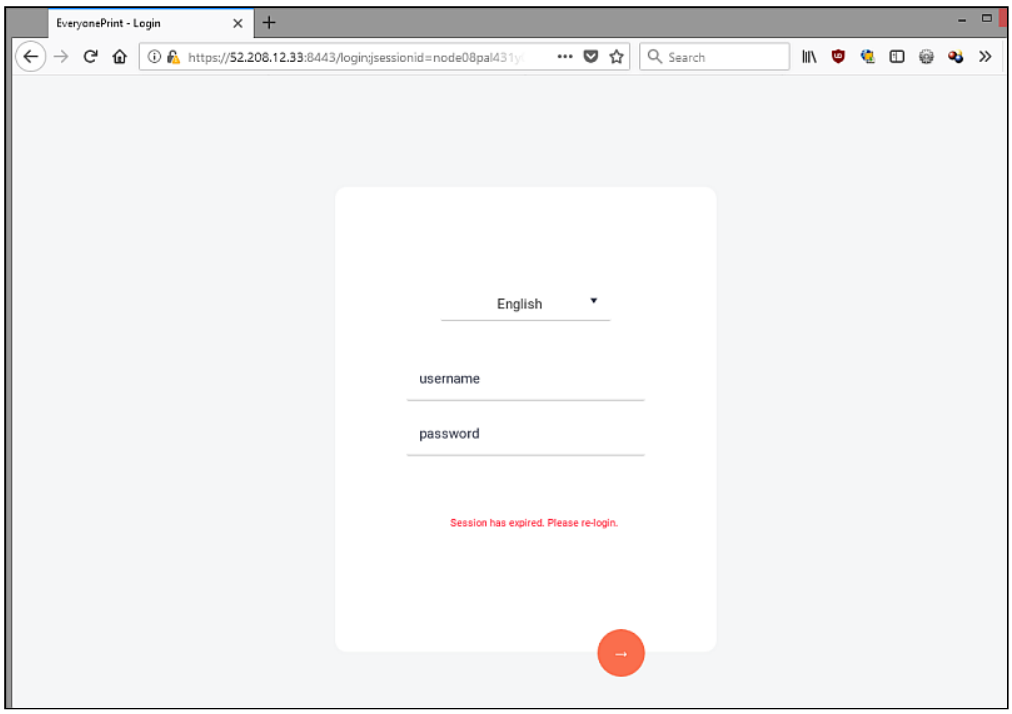


Enter the details of the externally hosted database cluster.



The installer will connect to the database and create any databases and database tables needed.

With SAFEQ Cloud installer finished, open up the SAFEQ Cloud Web interface on the entered IP address to confirm access.

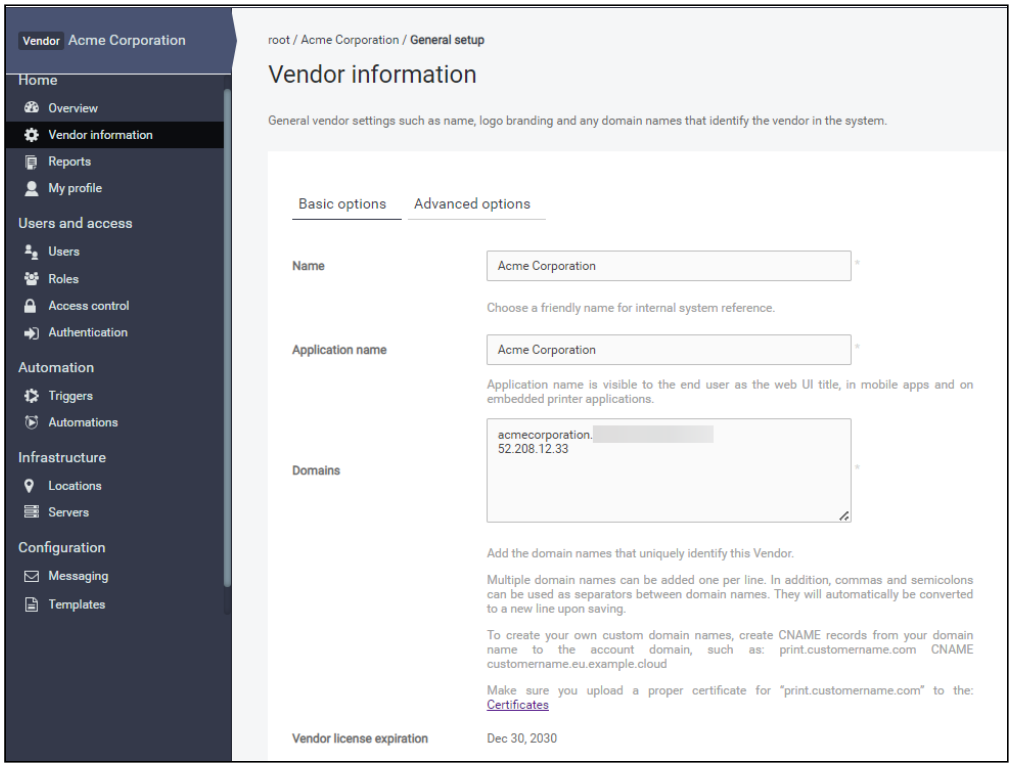


This means that we can access the primary server directly via its IP address.

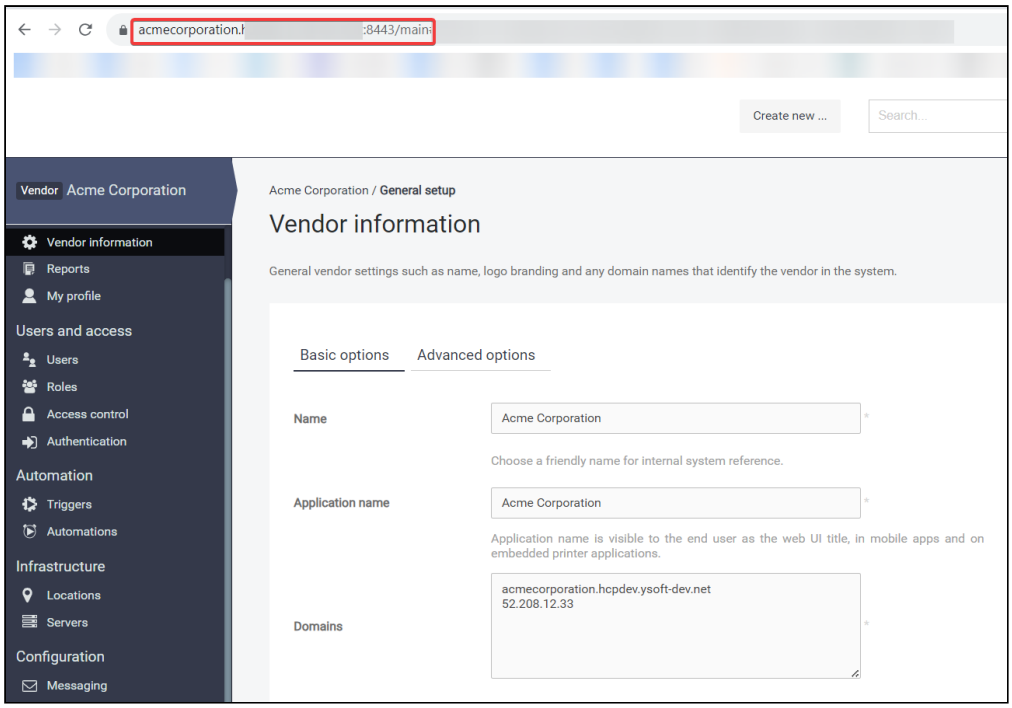
Add the load balancer DNS to root account

Next we want to add the load balancer DNS to the root account's account domains, so we can also access the root account using the load balancer DNS record, and not just directly via IP.

Log on to the root account, go to **Vendor information** and add the load balancer DNS as the first domain record, above the IP address of the first primary.



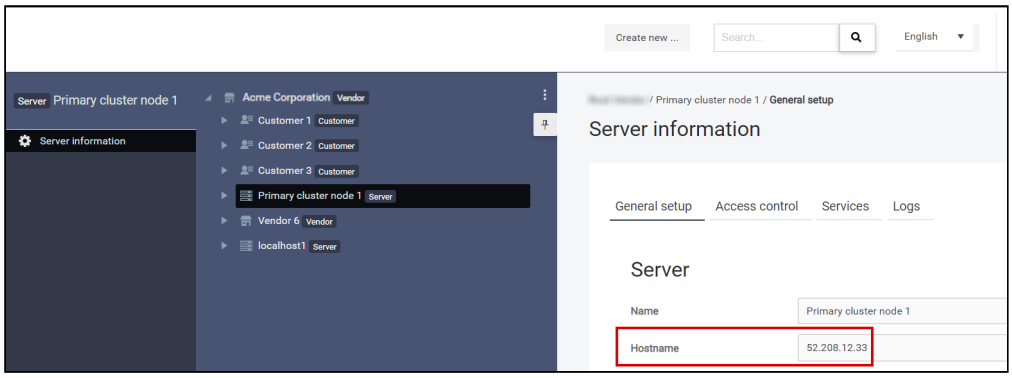
Now try the same through the load balancer.



The Web UI loads when we access the primary server via the load balancer DNS, and we can log in, which confirms the load balancer successfully routed the traffic to our first primary and we added the load balancer DNS correctly to root account.

Confirm the primary servers internal address

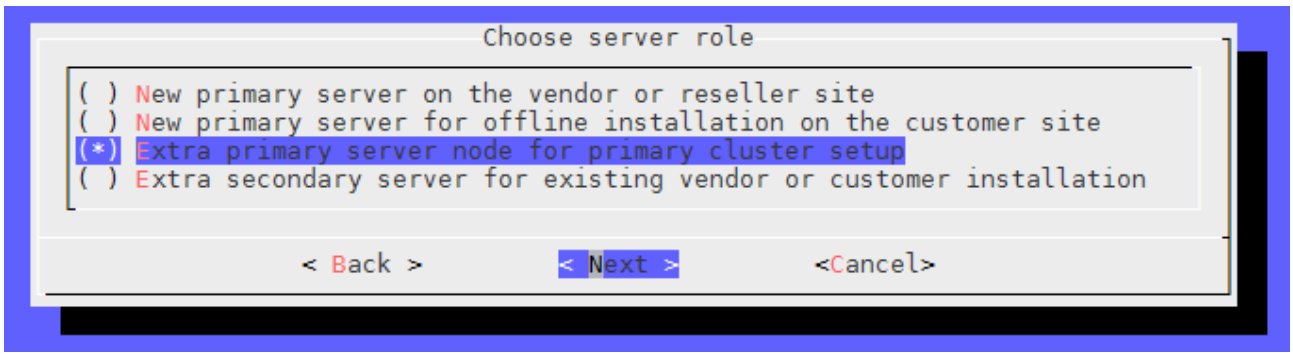
All primary servers in a cluster communicate internally for heartbeats, to check if they're alive, load levels and similar. This communication is done via the **Hostname** found under the servers Settings and TCP port 2552.



If the hostname is changed for a running SAFEQ Cloud server, the affected server must be restarted, so the cluster system can start up with the correct hostname settings.

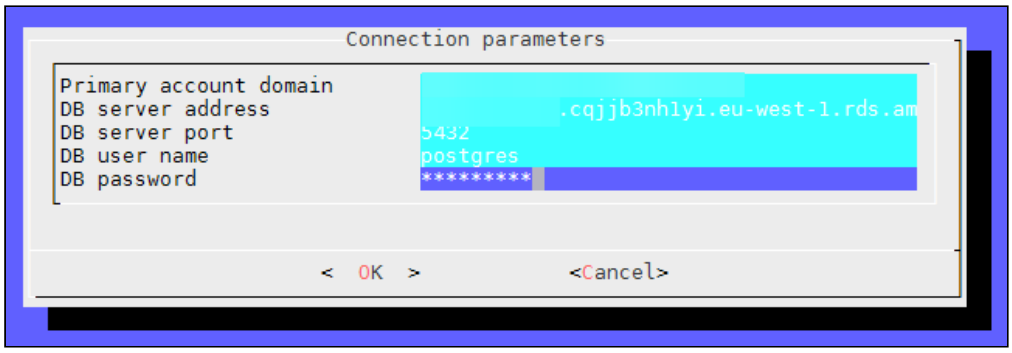
Add additional primary server nodes to the cluster

To add additional server nodes to the primary cluster, run the SAFEQ Cloud installer on a new server, and choose the option **Extra primary server node for primary cluster setup**



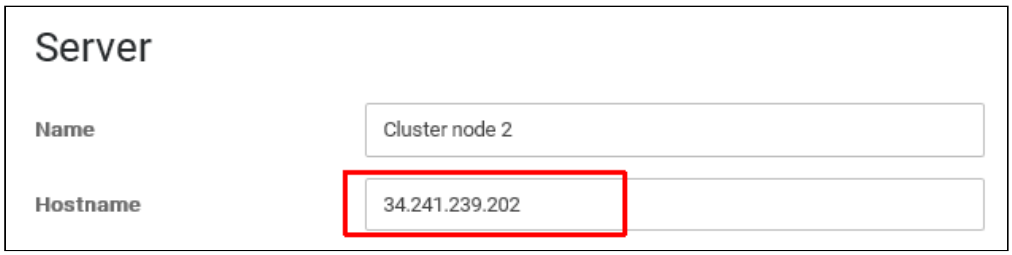
If the primary root account is of type **primary vendor** then the hcp.license file **must** be present in the directory where installer is run.

Next enter the account domain name of the root primary account. In this example, we use the load balancer DNS that was previously added as the accounts first domain.



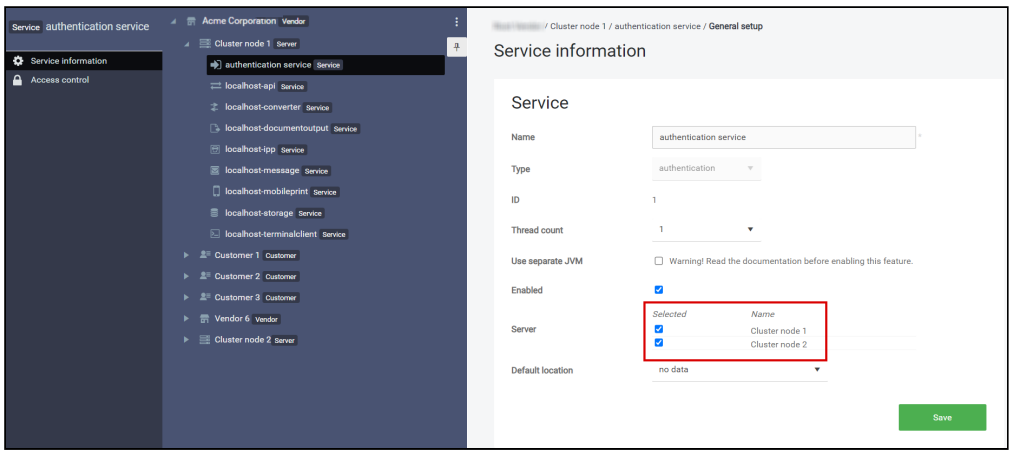
Confirm the Hostname of the primary server in settings

Go to the added primary cluster node settings, that the Hostname is a valid reachable address by all other primary cluster nodes.



Enable services to run on multiple nodes

When going from a single primary server to multiple, it's important to enable services to run on multiple servers. For example the Authentication Service used by an authentication provider, should be selected to run on all primary nodes, so if a primary node goes down, the authentication request is routed to an available server.



Common issues:

Server hostname

The most common issue in primary cluster configurations is an invalid server Hostname, as required for the inter communication between primary nodes.

11.2.2 INTEGRATE MOBILE PRINT FOR SAFEQ CLOUD

In SAFEQ Cloud 3.0, some features are served by the standard EveryonePrint Mobile Print product. Ultimately all major features from the EveryonePrint Mobile Print will be integrated into SAFEQ Cloud directly, but until then, this section outlines the configuration necessary to integrate the "legacy" Y Soft into SAFEQ Cloud.

Added Features

Combining SAFEQ Cloud with EveryonePrint Mobile Print for SAFEQ Cloud include the following additional features:

1. Printing from mobile devices via Web upload and Email print
2. Create guest users in SAFEQ Cloud from within the Y Soft Web interface
    a. Y Soft creates a unique numeric username and password for the guest
    b. User accounts are created as internal YSoft SAFEQ Cloud users
    c. Users email address set in YSoft SAFEQ Cloud
    d. Login credentials optionally emailed to user
3. Automatically create guest user in SAFEQ Cloud when user sends email print job
    a. Y Soft creates a unique numeric username and password for the guest
    b. User accounts are created as internal YSoft SAFEQ Cloud users
    c. Users email address set in YSoft SAFEQ Cloud
    d. Login credentials emailed to user
4. Ability to automatically delete created guest user accounts in SAFEQ Cloud after a pre-defined time period

Prerequisites and Requirements

- YSoft SAFEQ Cloud must be minimum version 2.1 and EveryonePrint Mobile Print for SAFEQ Cloud must be minimum version 4.2.6.
- EveryonePrint Mobile Print can run either on Windows or on Linux.
- An EveryonePrint Mobile Print installation is required for each account in SAFEQ Cloud (EveryonePrint Mobile Print is not multi-tenant)
- Root access for installation
- The following libraries/tools are required:
  - CUPS
  - CURL
  - Fontconfig
  - FreeType
  - rsync

**bzip2

- Relevant firewall ports should be opened. See Ports and Protocols, section *Web Administration UI.*
- An API key with full API access needs to be generated in SAFEQ Cloud to use in Y Soft Mobile for SAFEQ Cloud > User Authentication

Install EveryonePrint Mobile Print for SAFEQ Cloud

Install dependencies

Prior to installing Y Soft, install the required dependencies using either yum or zypper, ie

```
yum install cups curl fontconfig freetype rsync bzip2
```

Install Y Soft

Download EveryonePrint Mobile Print for SAFEQ Cloud from the YSoft Partner Portal, and upload to the secondary server where it should be installed, or download directly on the secondary server:

xxxxx is the version number for the latest Y Soft Mobile for SAFEQ Cloud

```
wget https://cdn.everyoneprint.com/everyoneprint-for-SAFEQ Cloud-xxxxxxx.tar.bz2
```

Next extract the compressed file.

```
tar -xjf everyoneprint-for-SAFEQ Cloud-xxxxxx.tar.bz2
```

Next, change to the Y Soft directory and run the install script.

```
cd everyoneprint/
./install.sh
```

The installer script will check for dependencies, create a user and copy files to /opt/everyoneprint. During the installer script, the license agreement is shown. Enter "yes" to accept and continue.

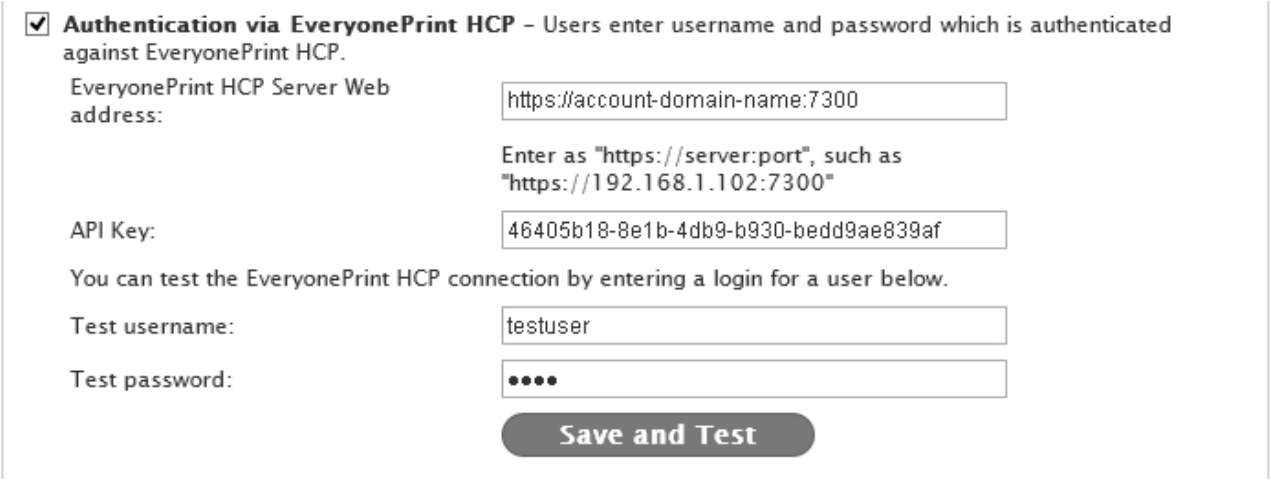
Configuring YSoft SAFEQ Cloud features in Y Soft

The following section covers the configuration screens in Y Soft Admin.

http://server-address:7290/admin

Configure Authentication

First, configure User Authentication against YSoft SAFEQ Cloud:



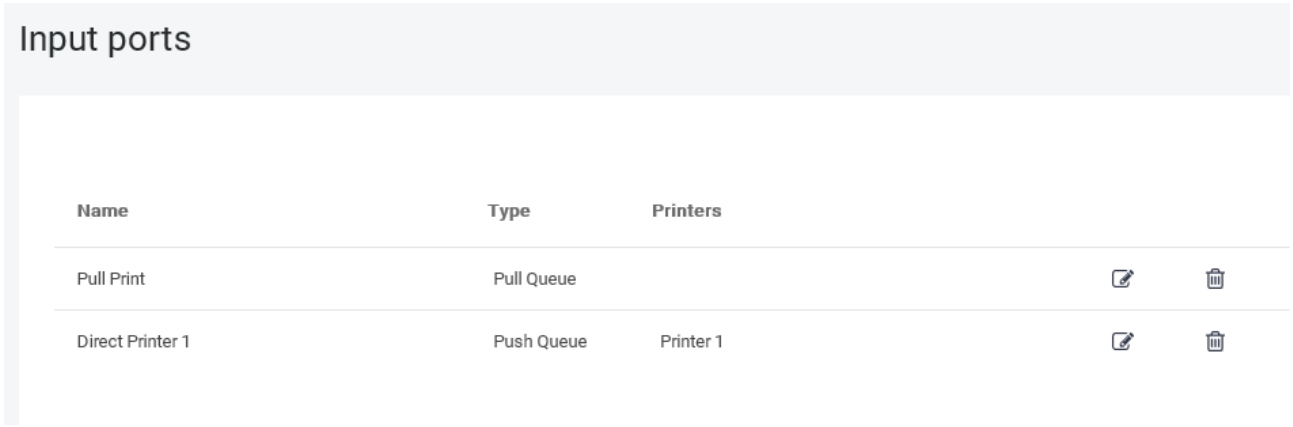
1. Replace *account-server-domain* with the account domain name of the SAFEQ Cloud account to which this Y Soft should be connected.
2. Generate an API key with full API access in SAFEQ Cloud for use with EveryonePrint Mobile Print for SAFEQ Cloud
3. Report the API key in "User Authentication" > "Authentication via YSoft SAFEQ Cloud" >"API key"
4. Verify the authentication to YSoft SAFEQ Cloud using a username or password of a test user created in YSoft SAFEQ Cloud.

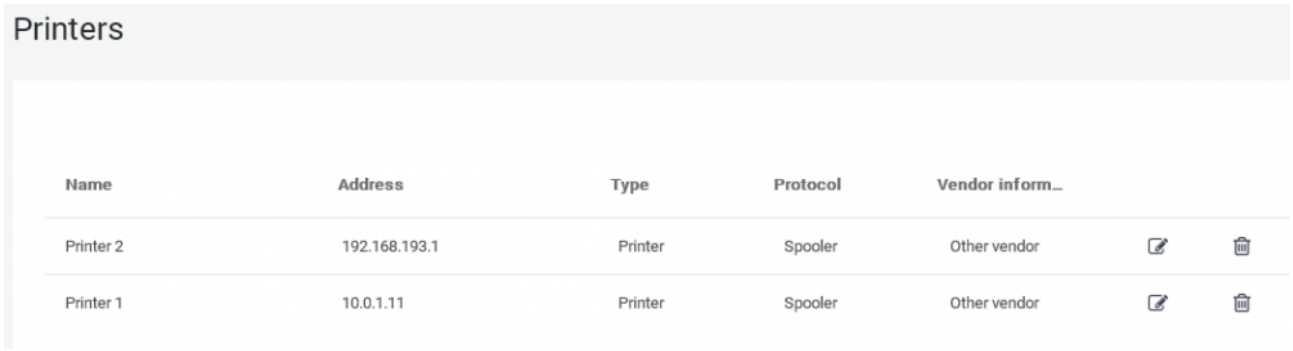
If test authentication fails, an error message will be shown, and error details written to the Y Soft log files.

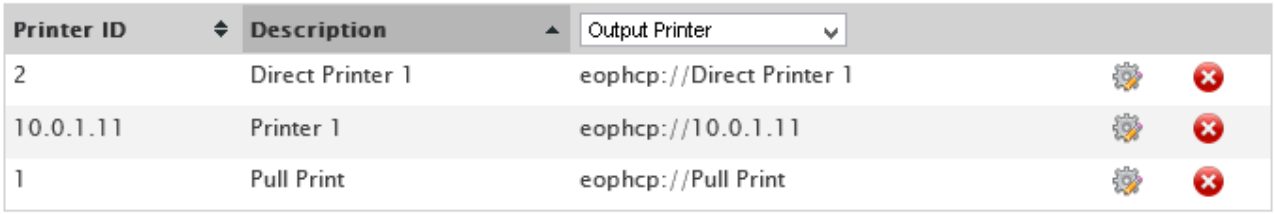
Add Devices

Go to Admin -> Devices and add the print queues.

Queues in the list starting with eophcp:// are the input and output ports of the SAFEQ Cloud account. Add the input ports for sending jobs from Y Soft legacy to SAFEQ Cloud, and add output ports for releasing jobs using the Y Soft Apps with or without QR codes.

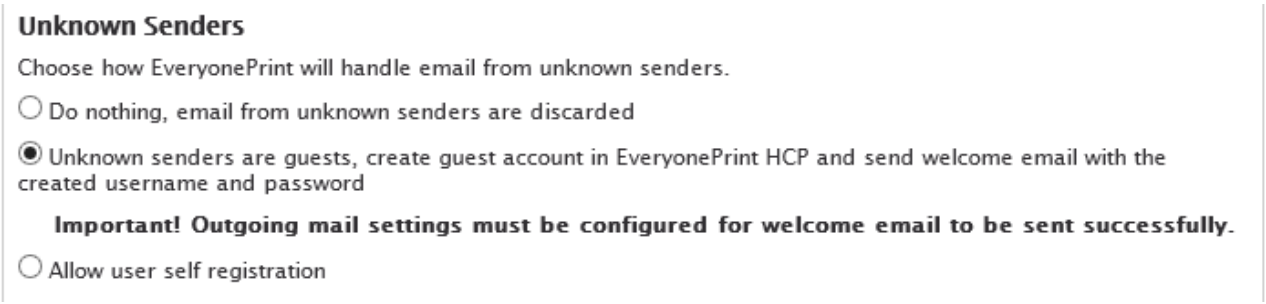






Automatically create accounts for email print

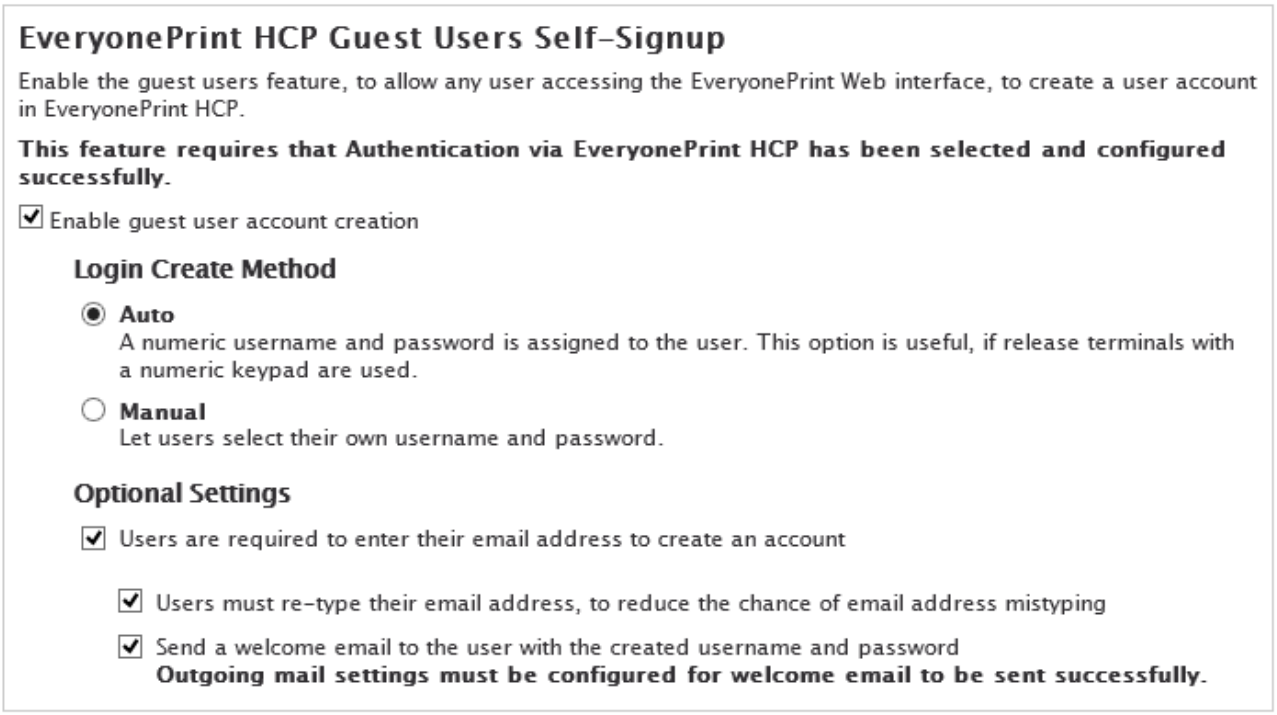
Under Email Authentication, choose how email from unknown senders should be handled, whether unknown senders are guests, and accounts should be created in YSoft SAFEQ Cloud automatically for guests.



In this configuration an account is created in YSoft SAFEQ Cloud for unknown users.

YSoft SAFEQ Cloud Guest User self-sign up via the Web

If Y Soft is installed in an environment where guests should be able to create guest accounts using a Web interface, enable the YSoft SAFEQ Cloud Guest Users Self-Signup feature.



Users created via the Web portal are created in the internal YSoft SAFEQ Cloud users database. If an Active Directory exists, both LDAP and YSoft SAFEQ Cloud users can authenticate.

Automatically delete created guest user accounts

To automatically delete created guest user accounts, specify under User Authentication the time period in minutes after which accounts are deleted. Set to 0 to never automatically delete guest user accounts.

Troubleshooting tips

Create a test accounts using Web form

Even if the feature is not needed, it's recommended to test the account creation in YSoft SAFEQ Cloud, using the Web based self-sign-up feature, outlined in section 4.2.2, as errors will appear and be written to log immediately.

Once accounts can be created successfully using the Web form, they can also be created from email.

11.2.3 SCAN TO MAIL

SAFEQ Cloud can use the built in scan-functionality of the MFD.

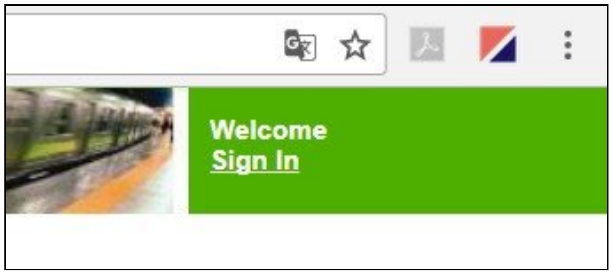
SAFEQ Cloud can handle Scan To Mail by putting in the email address of the logged in user into the "To"-Field.

SAFEQ Cloud can also put in the logged in users email address into the "From"-Field.

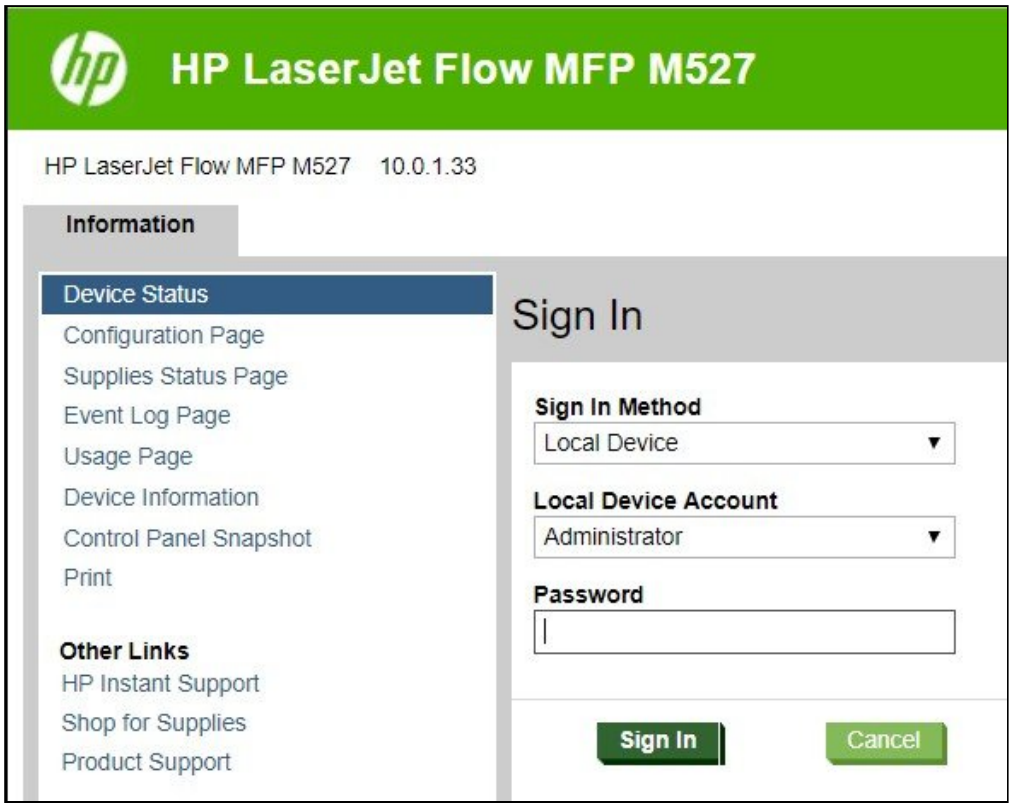
Both options depends on Vendor.

HP MFDs

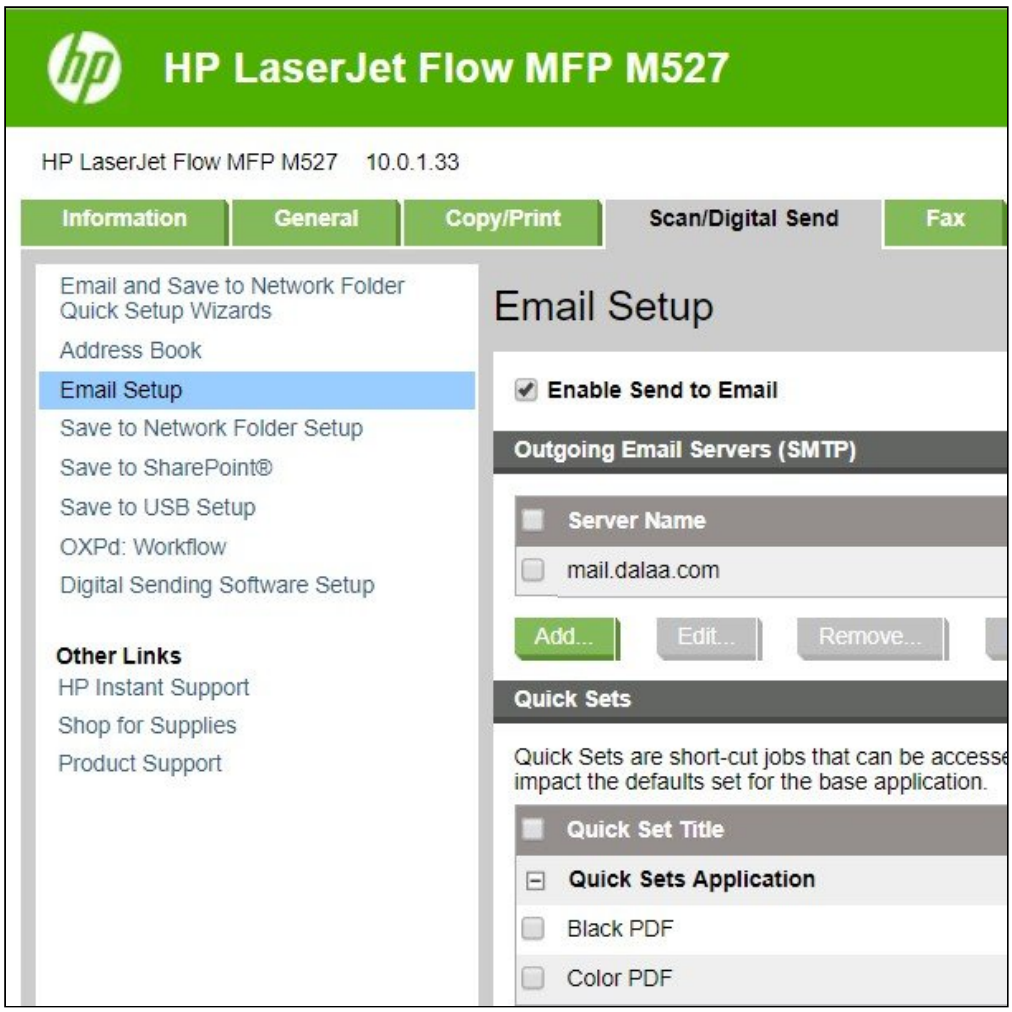
Open printers Webinterface in a browser and choose "Sign in" at the upper right corner.



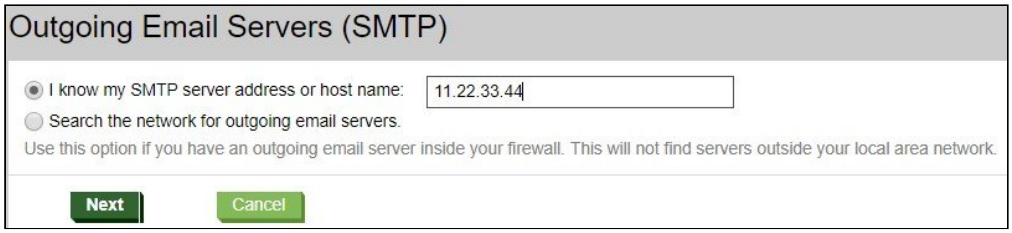
Write "admin" under "Password" and choose "Sign in".

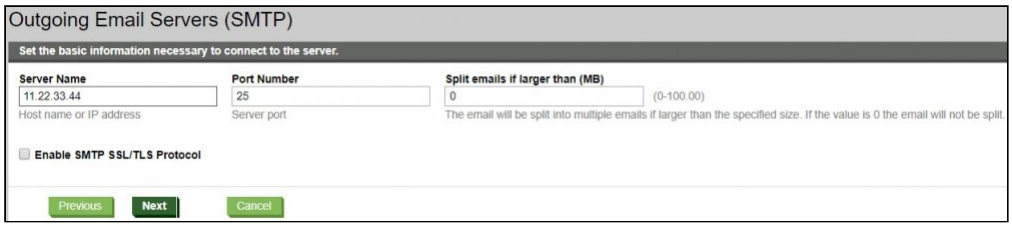


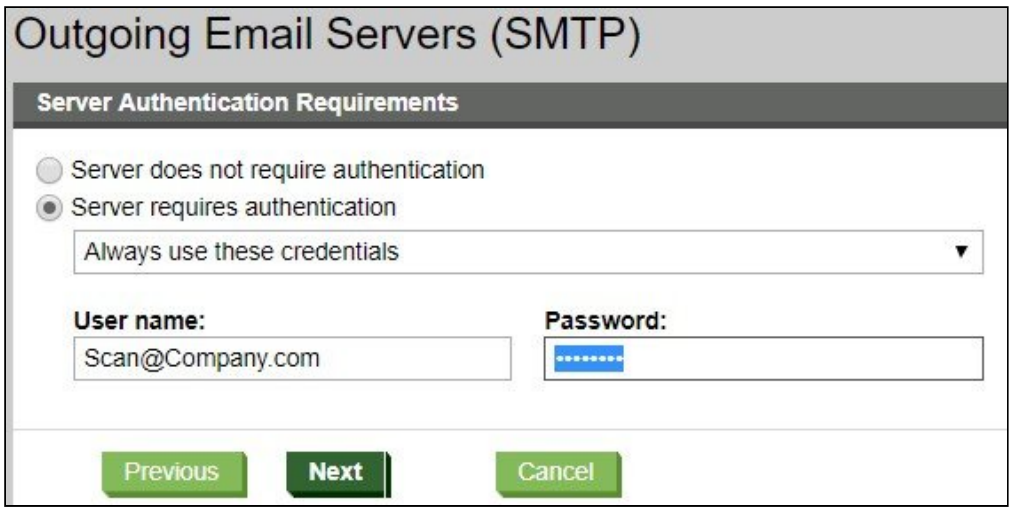
Under "Scan/Digital Send" choose "Email Setup" and choose "Add" under "outgoing Email Servers (SMTP).



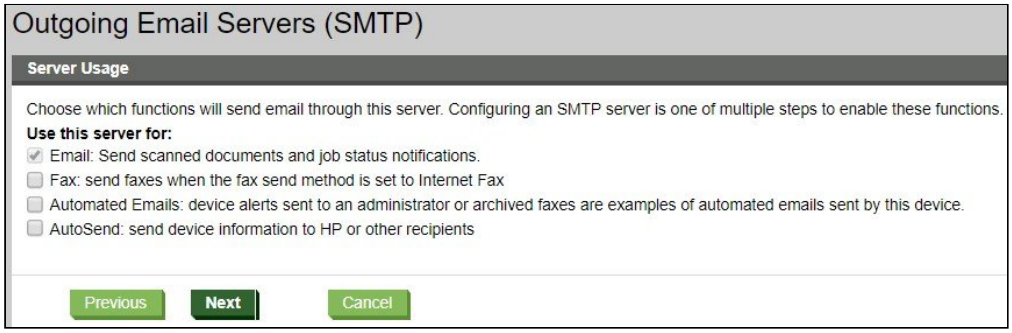
Follow the guide to set up Scan To Mail with proper information.





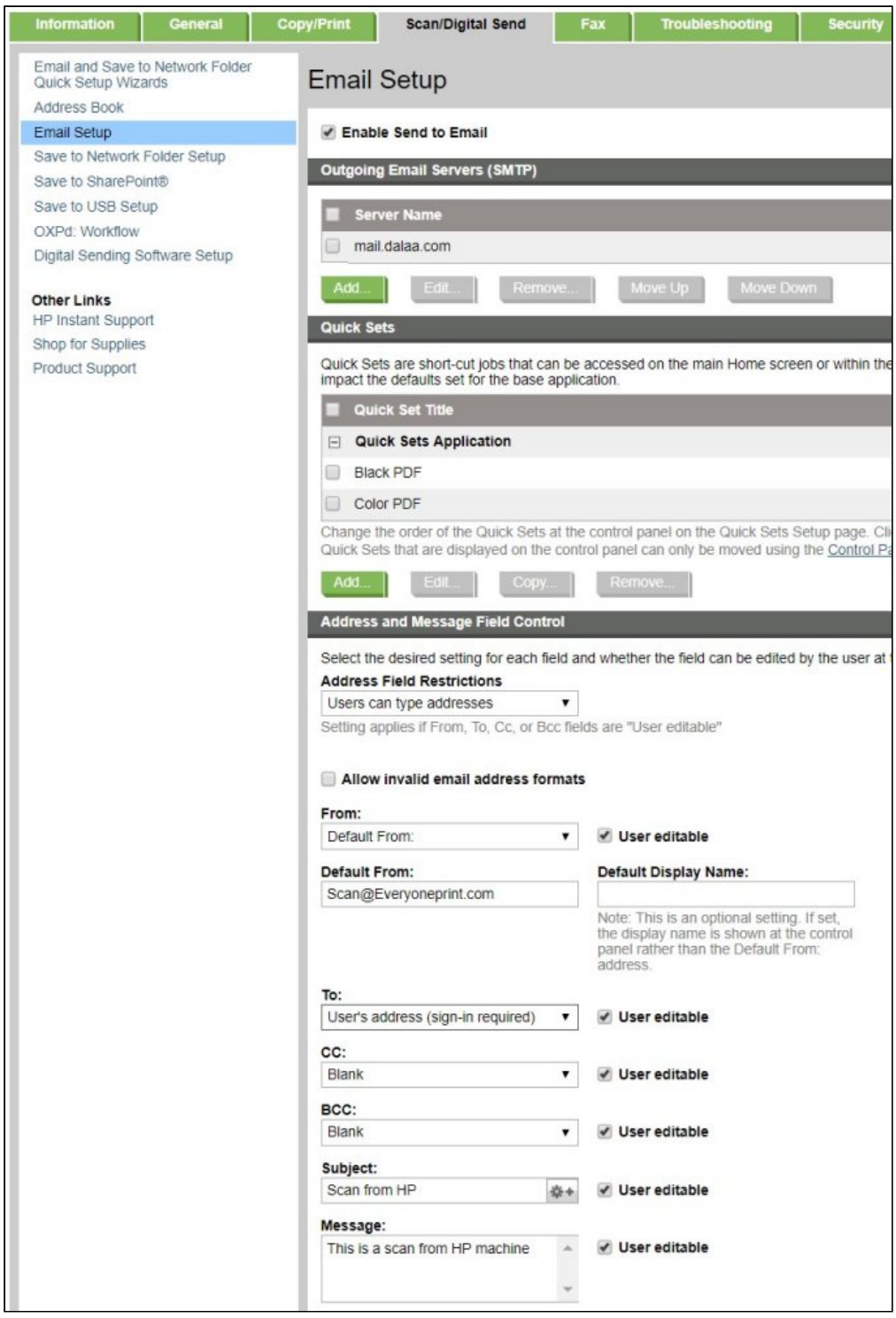


Be sure to remove the lower three markings.



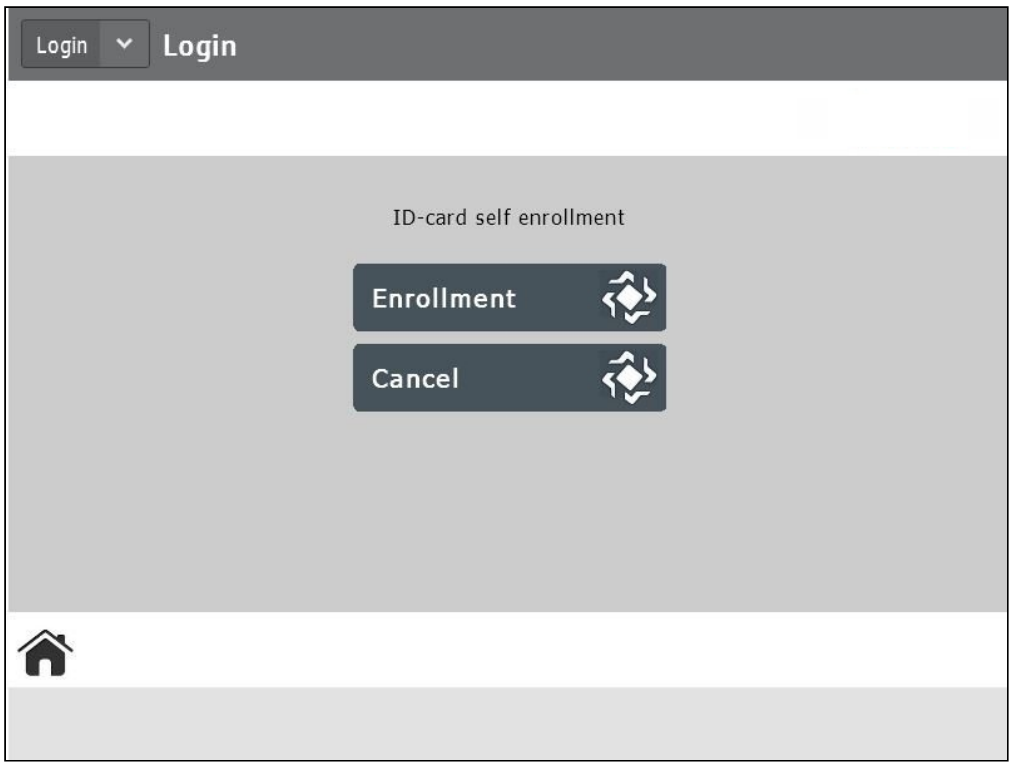
Here you can send a testmail.

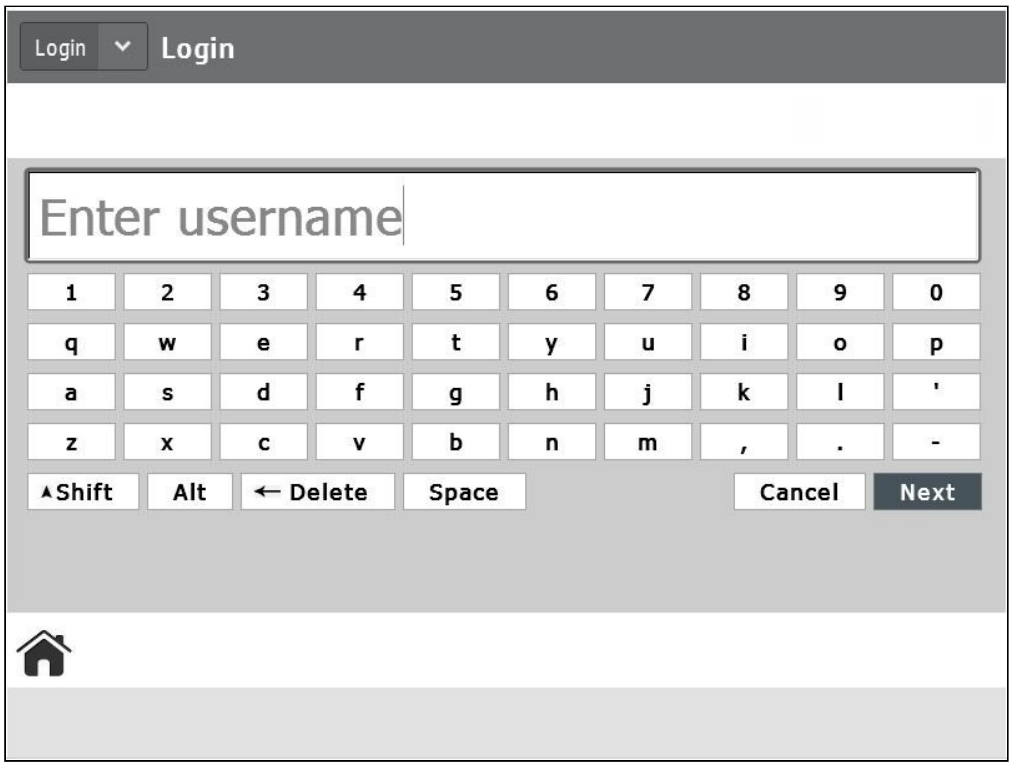
Under "Scan/Digital Send", "Email Setup", "Address and Message Field Control" you can choose wether the logged in user is set in as the default receiver of the scan, who should be in the "From"-field and which functions should be editable by logged in user.

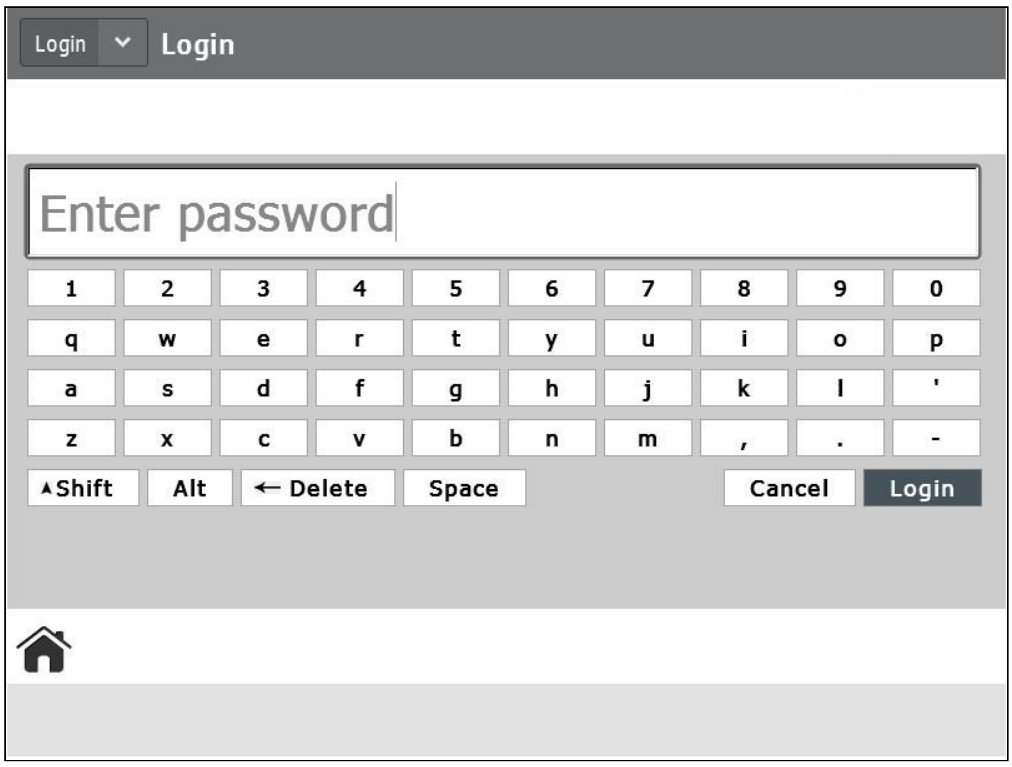


Card Self enrollment on the MFD:

Swipe your card and follow the guide for Self Enrollment.


Login
Login
ID-card self enrollment
Enrollment
Cancel

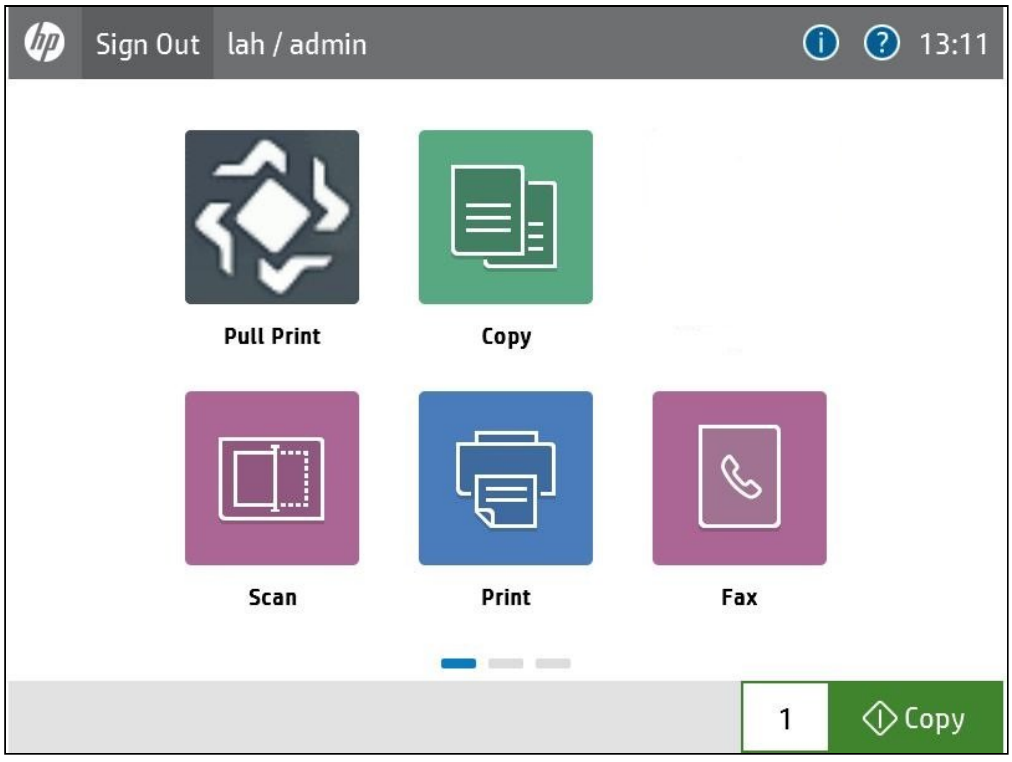

Login
Login
Enter username
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l '
z x c v b n m , . -
Shift
Alt
Delete
Space
Cancel
Next



Now your card are enrolled with your user and you can just swipe your card from now on.

Log in to the machine by card:

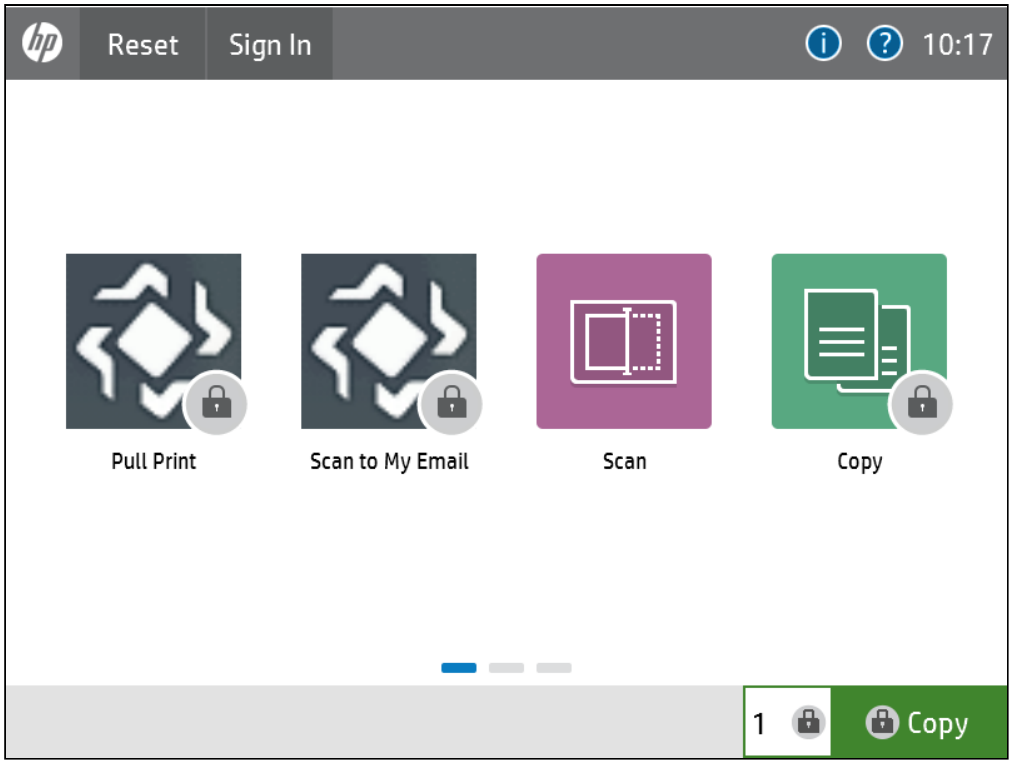
Just swipe the card and hit the function you want to use.



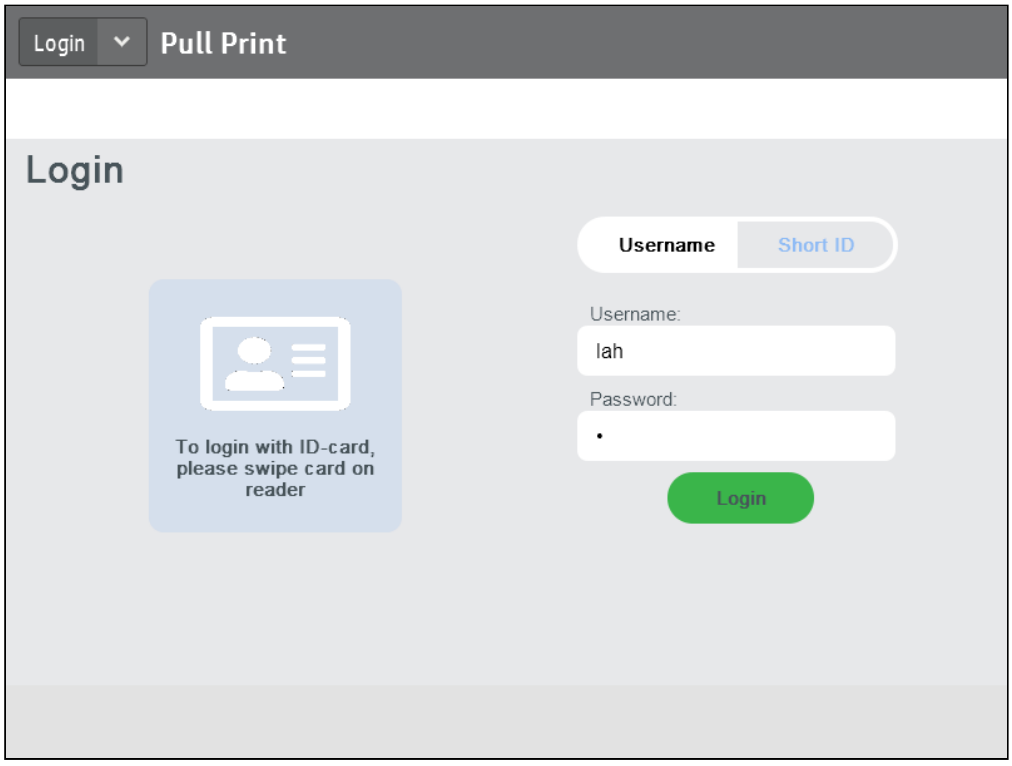
Swipe your card again to log out.

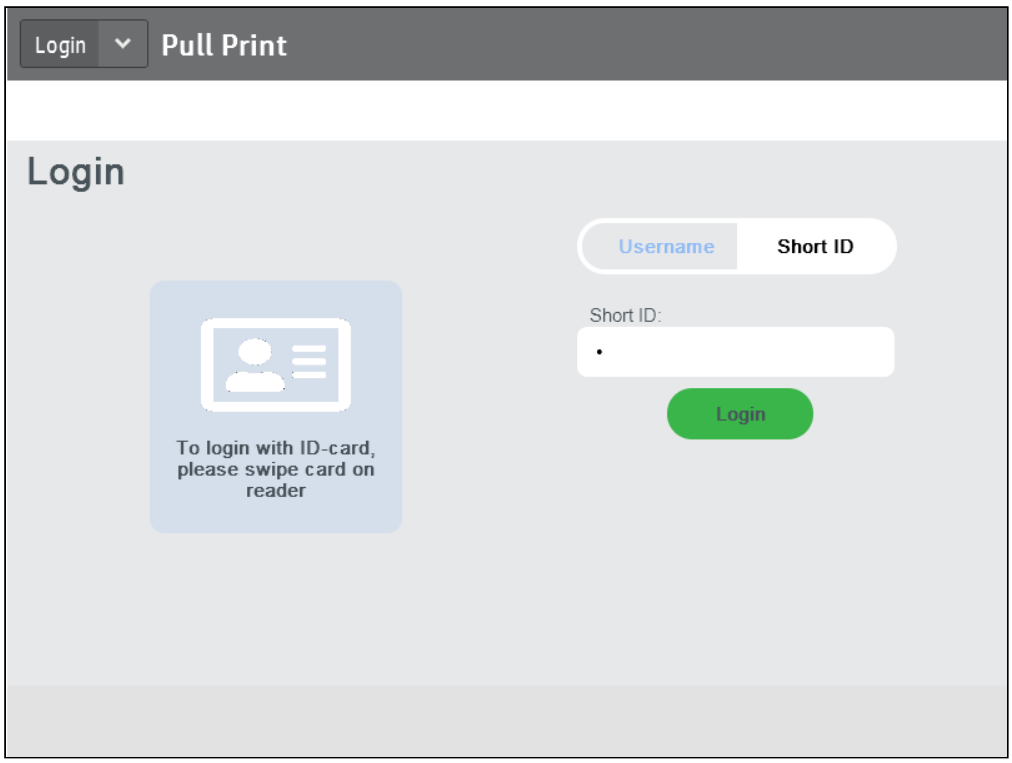
Manual login on the mfp:

Hit the "Sign in"-icon

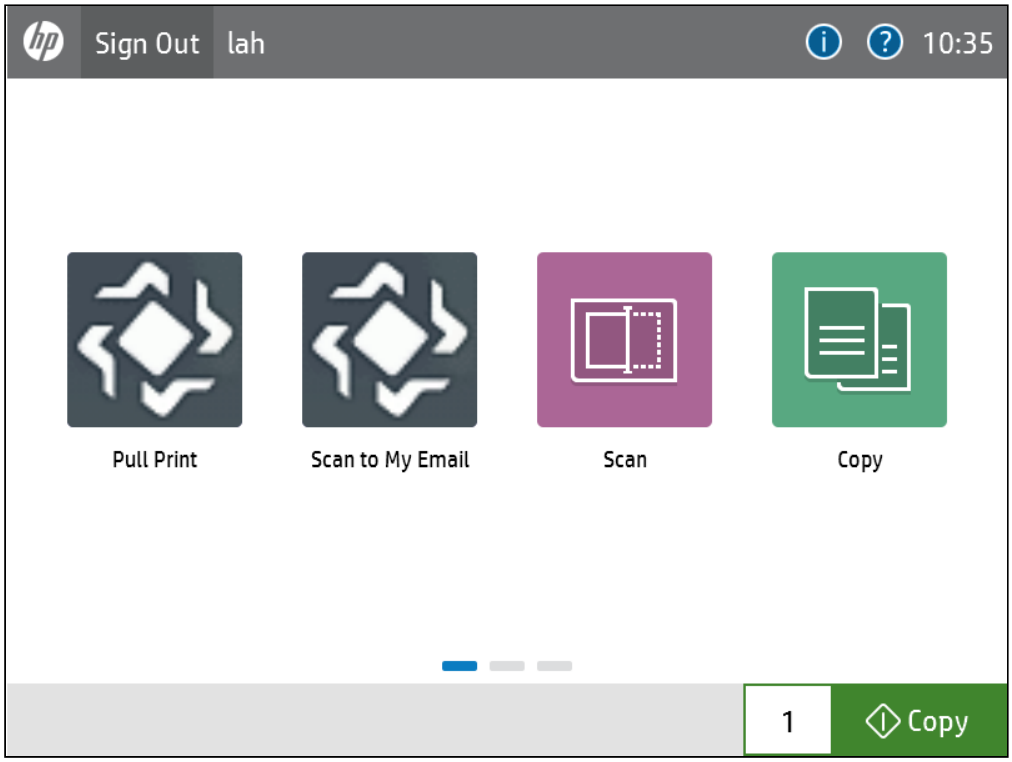


Authenticate using Username/Password or Short ID



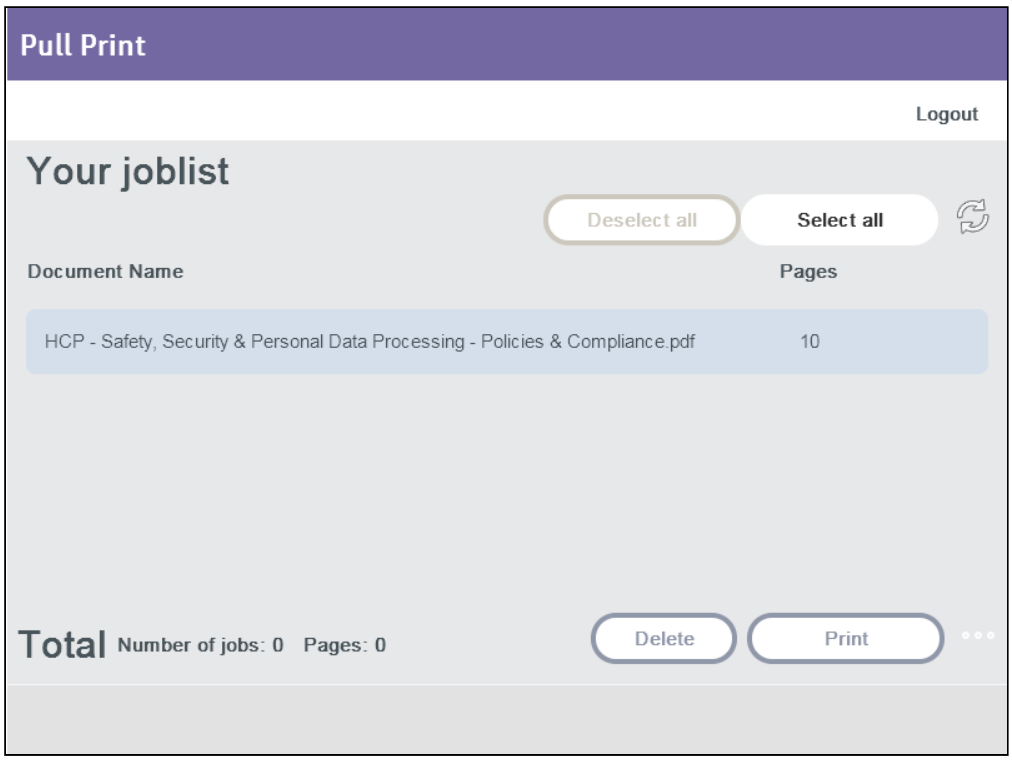


You can now choose the function you want to use.

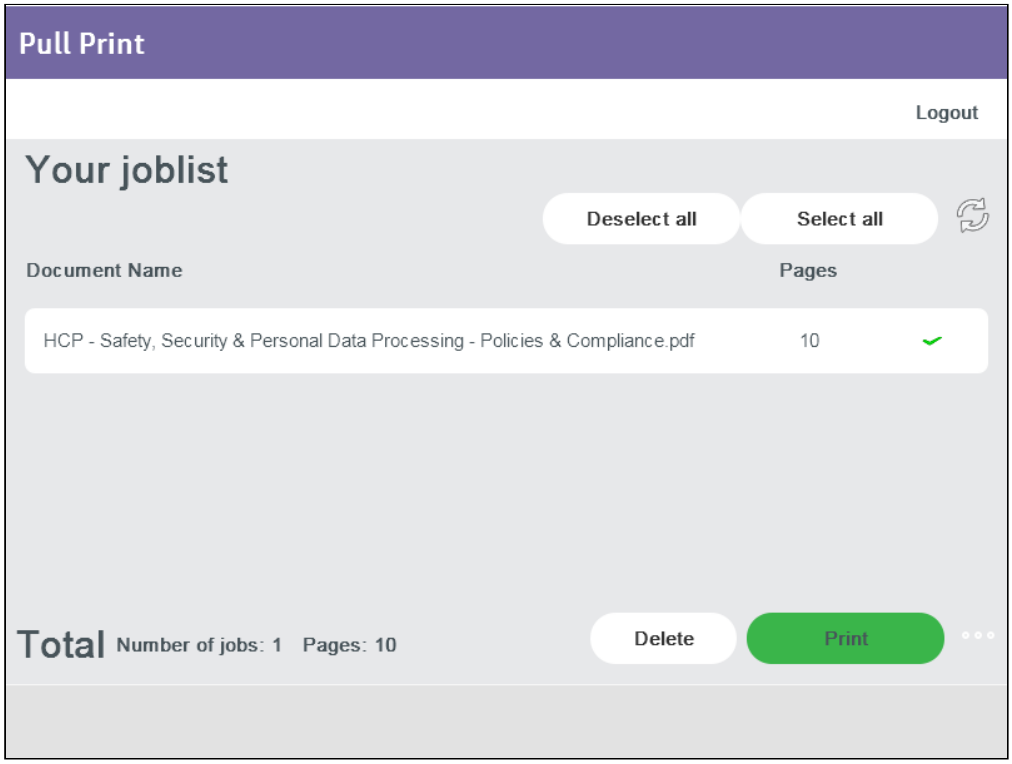


Releasing printjobs:

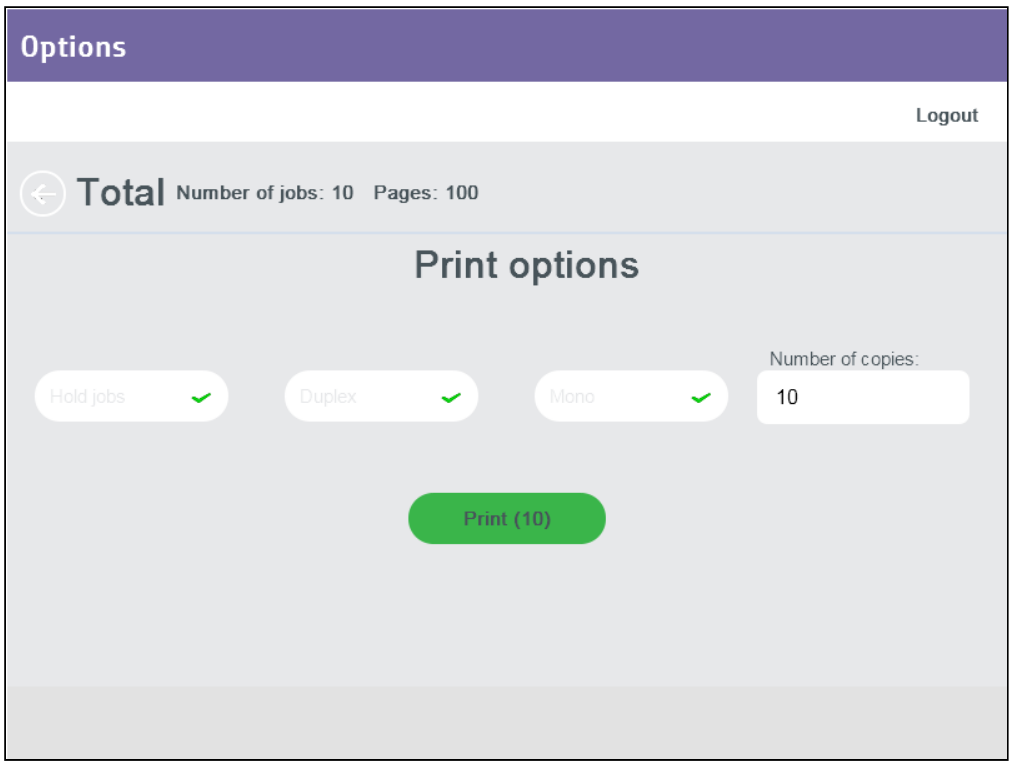
Log in on the mfp and choose "Pull Print" for releasing your printjobs.



Select job(s) you want to release by touching the each job or using Select/Deselect all buttons

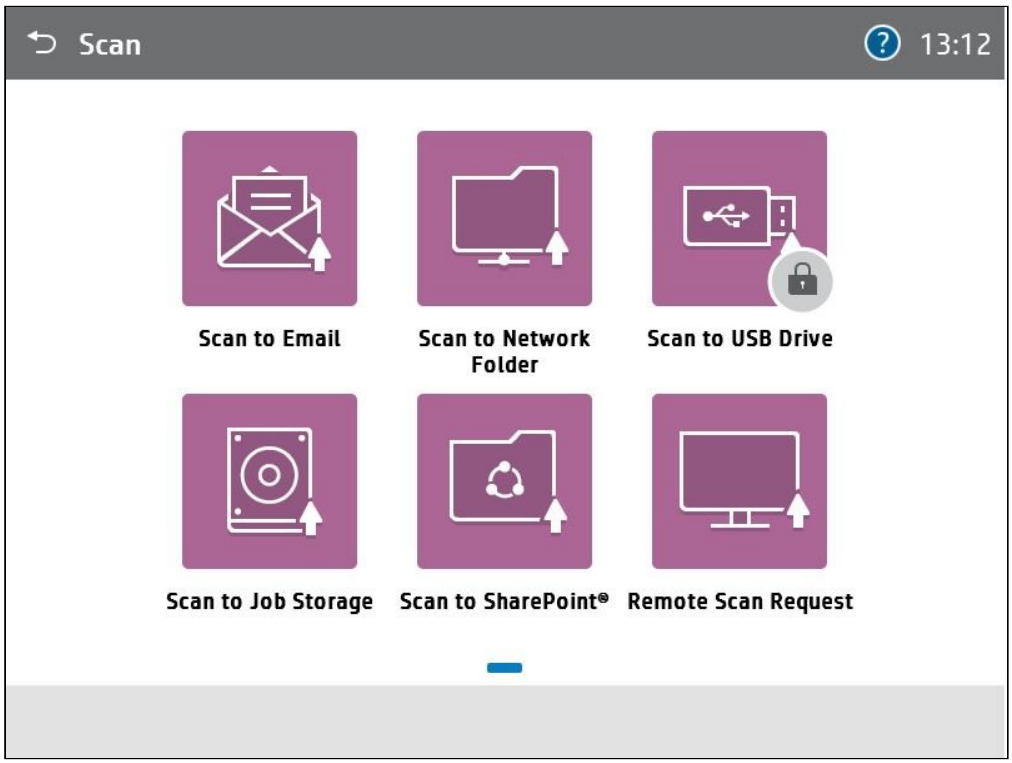


You can change options for your printjob by hitting the ellipsis in the bottom right corner.

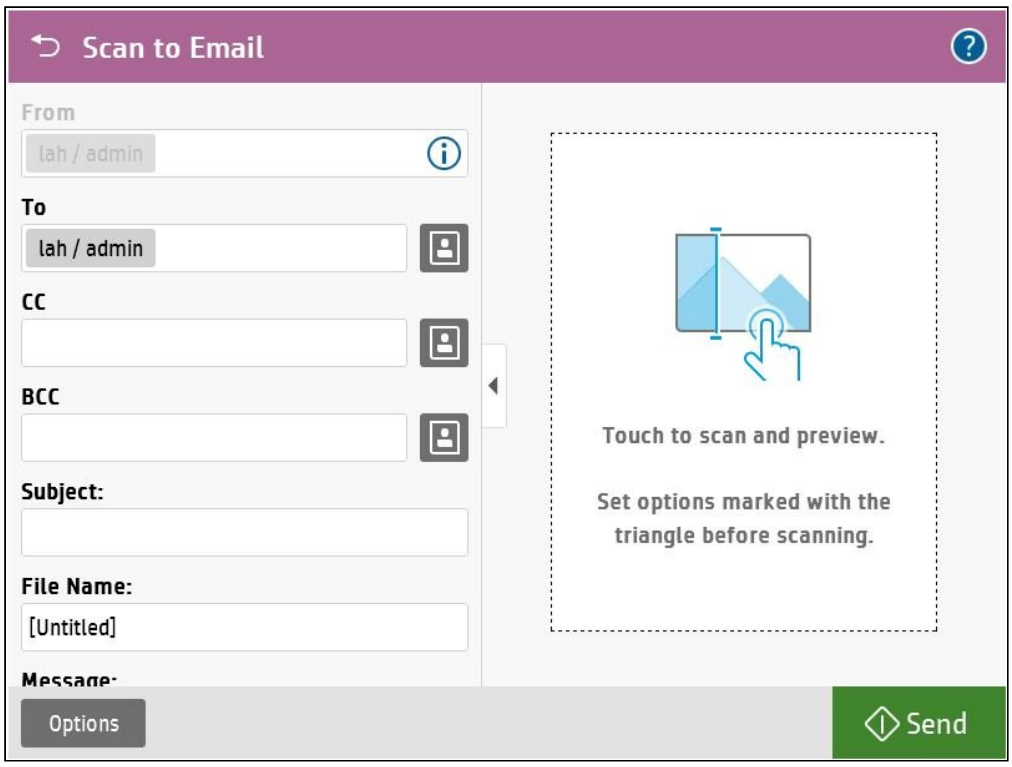


Using the native Scan-function:

Log in on the mfp and choose "Scan" in the mainscreen and then "Scan to Email".

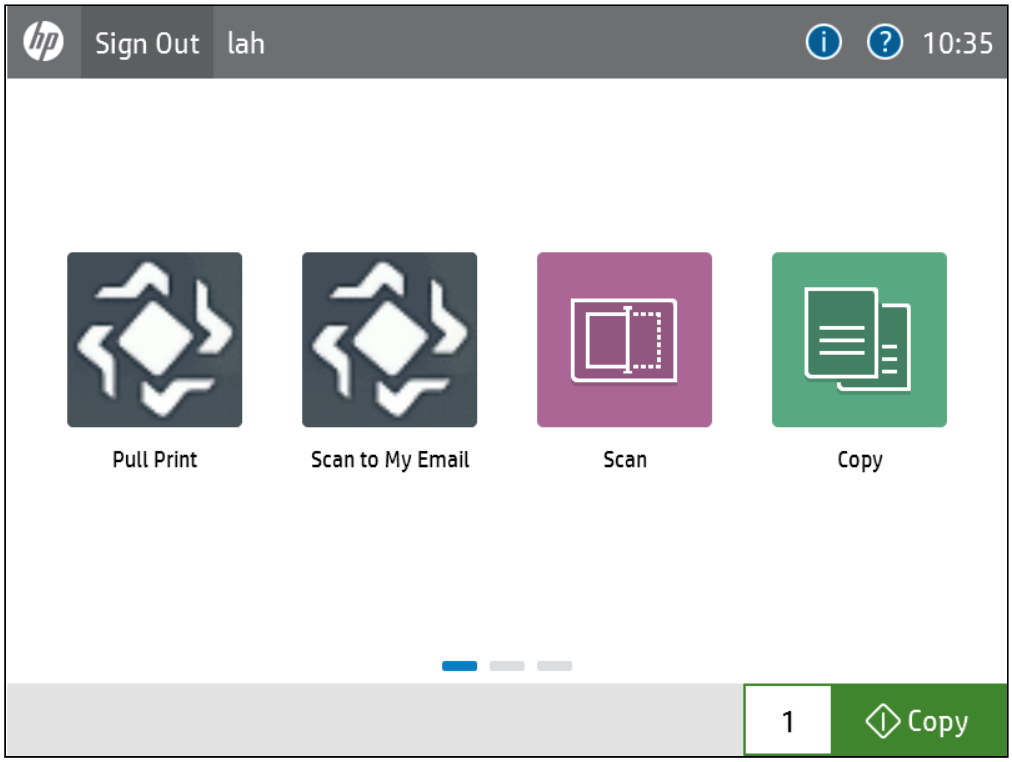


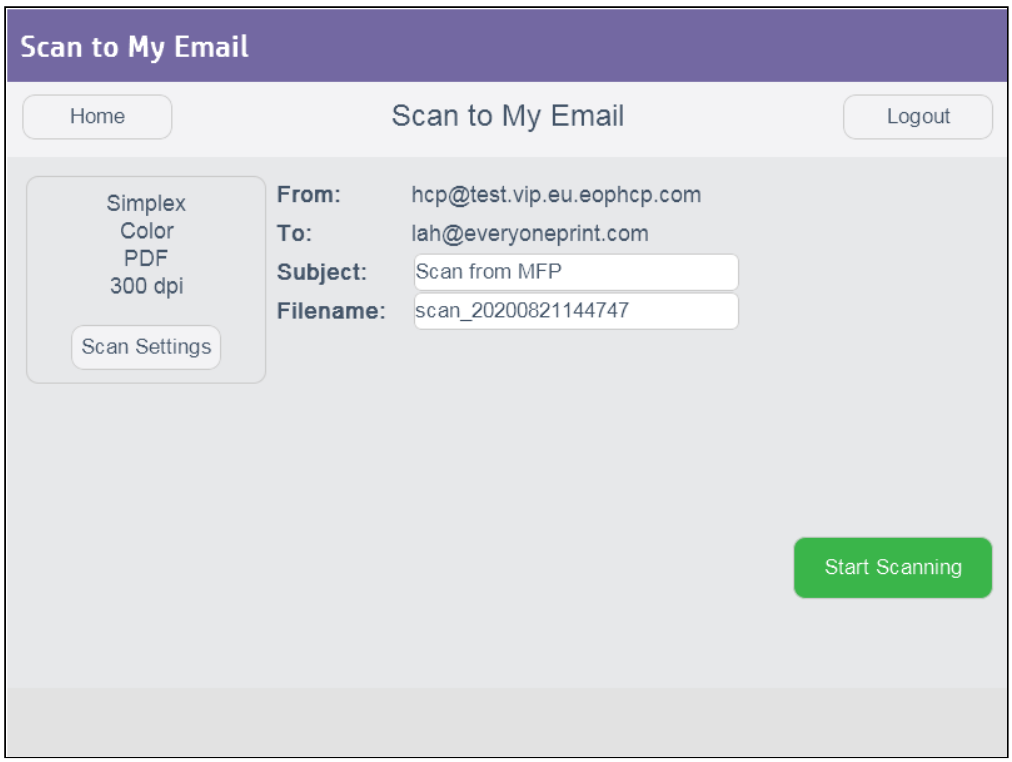
Choose "Options" for changing the options for your scan or just make your scan.



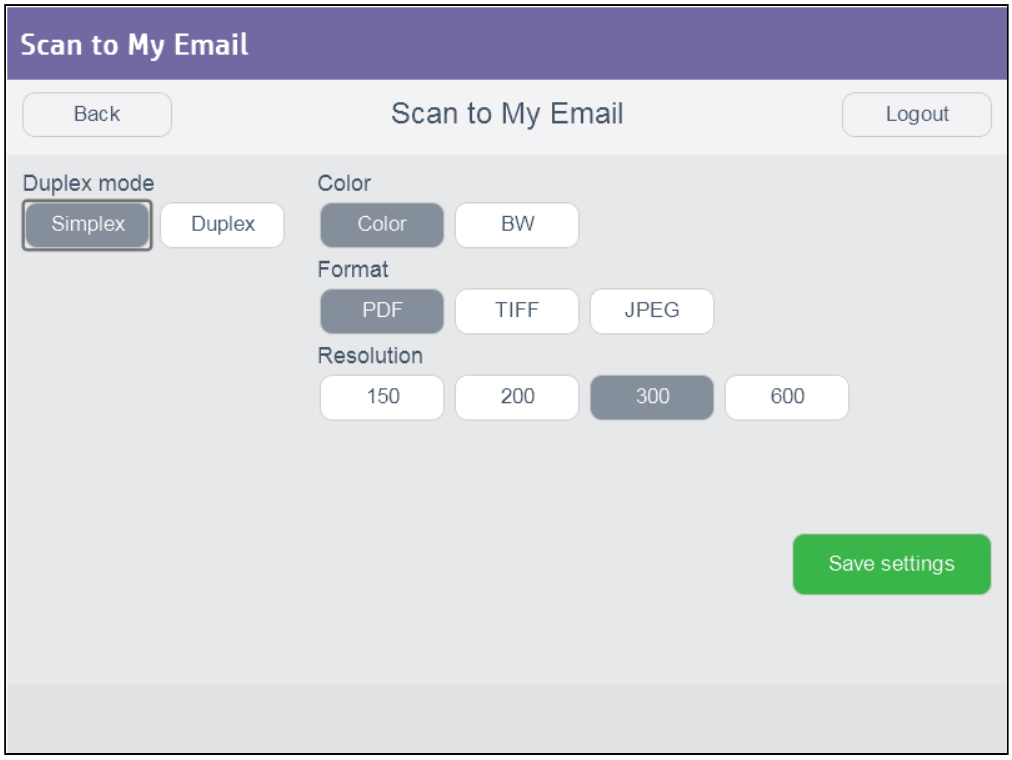
Using the Scan to My Email function:

Log in on the mfp and choose "Scan" in the mainscreen and then "Scan to My Email".

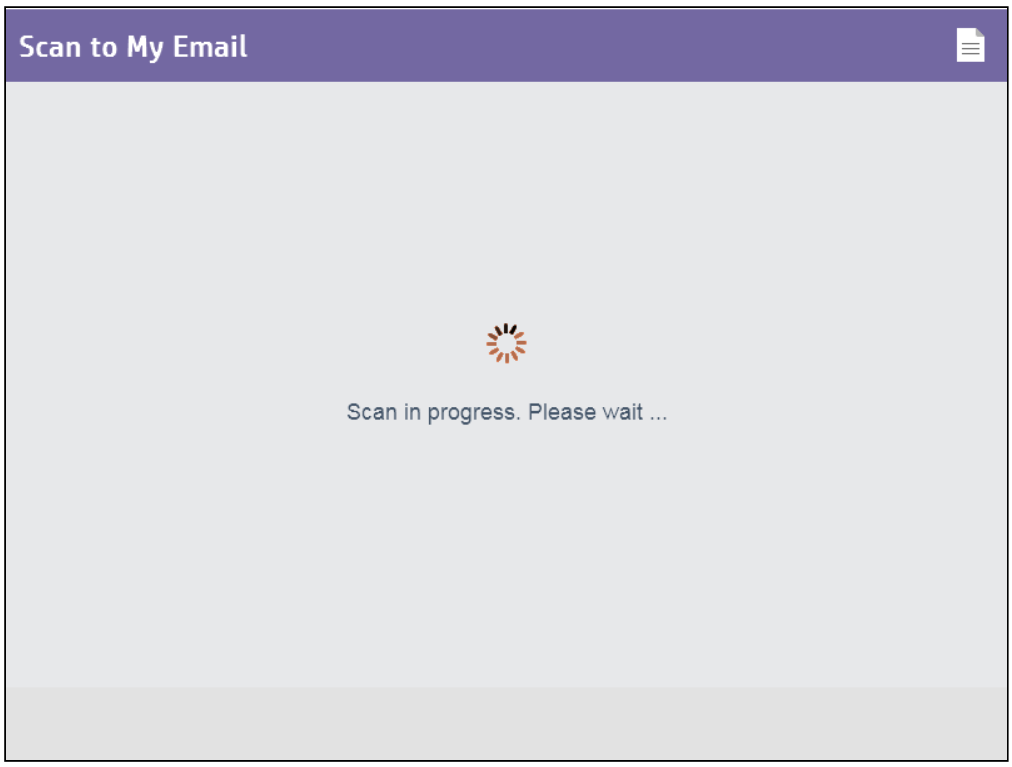




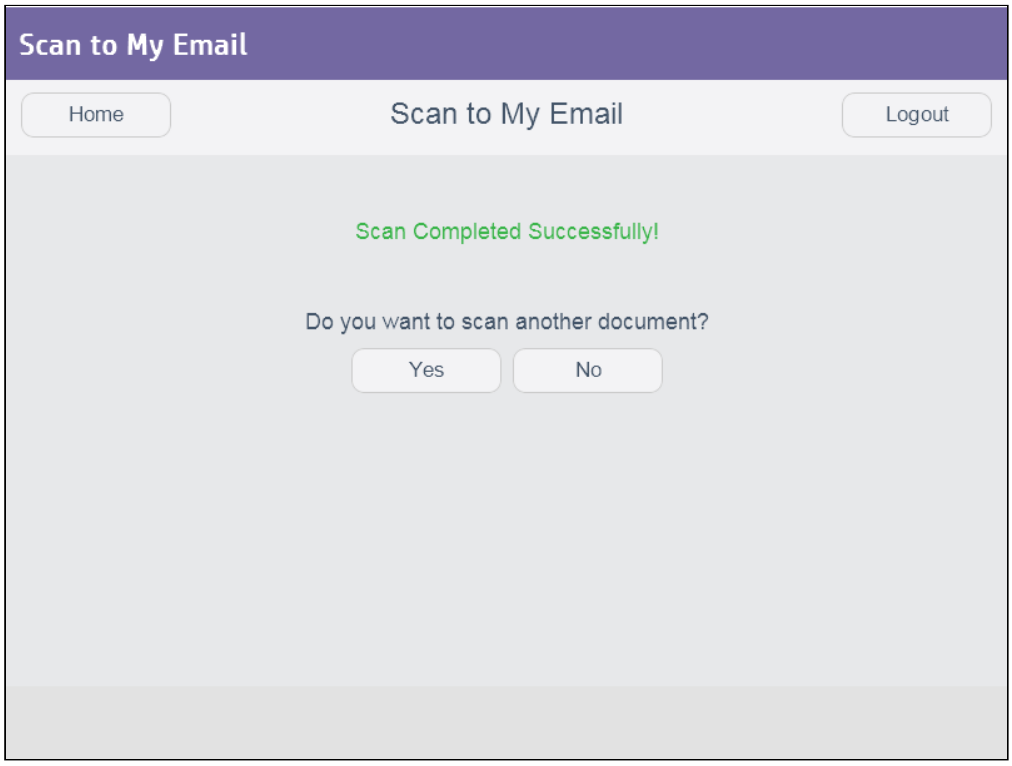
You can change Scan Settings



Start Scanning

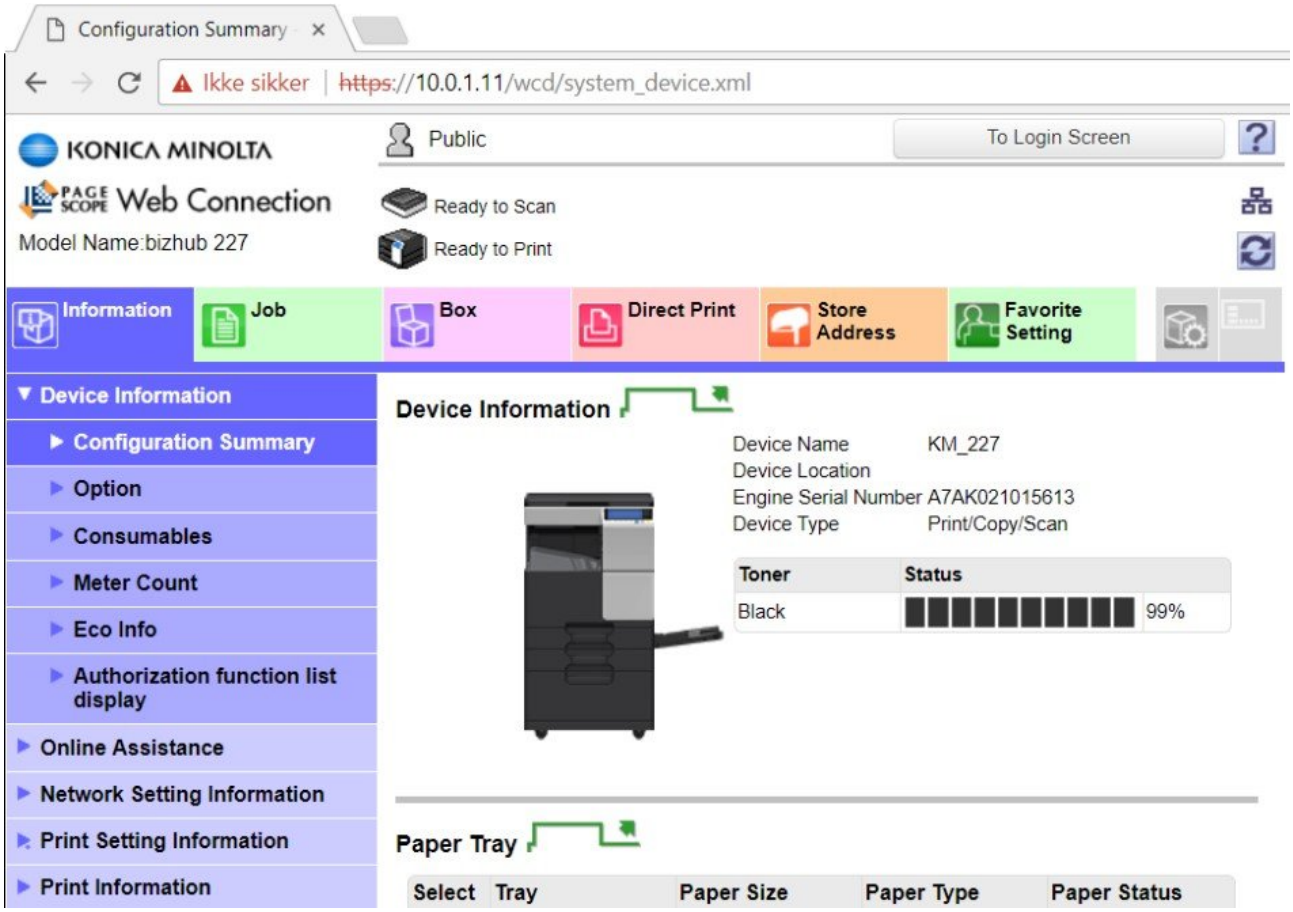


You can scan another document at the end

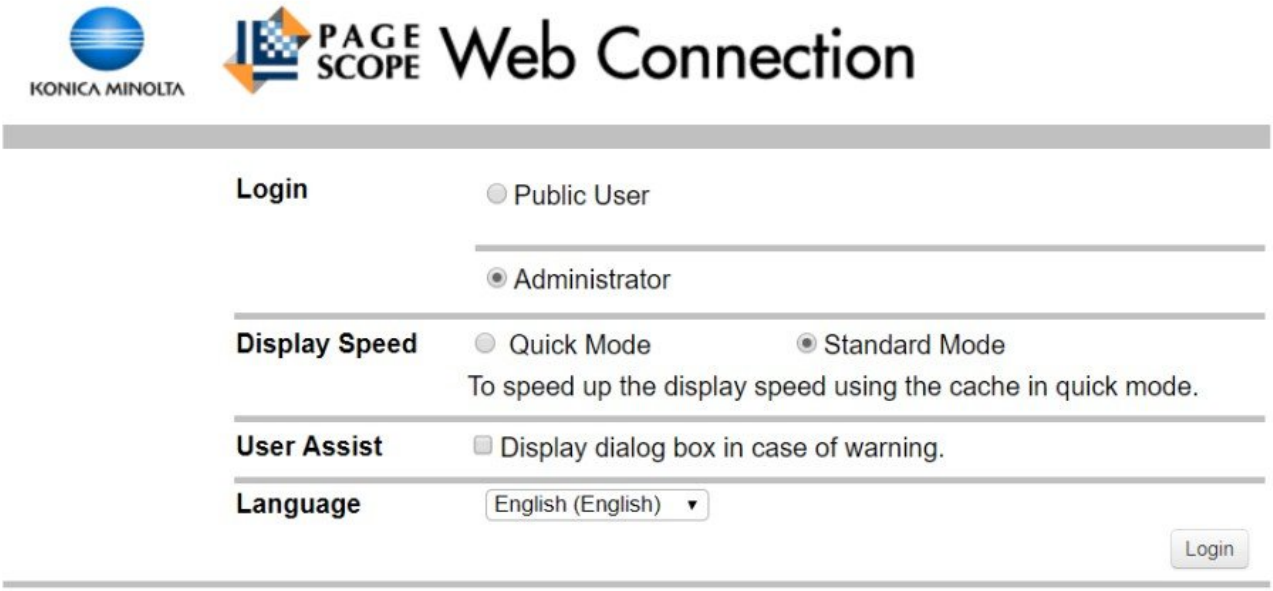


Konica Minolta MFDs

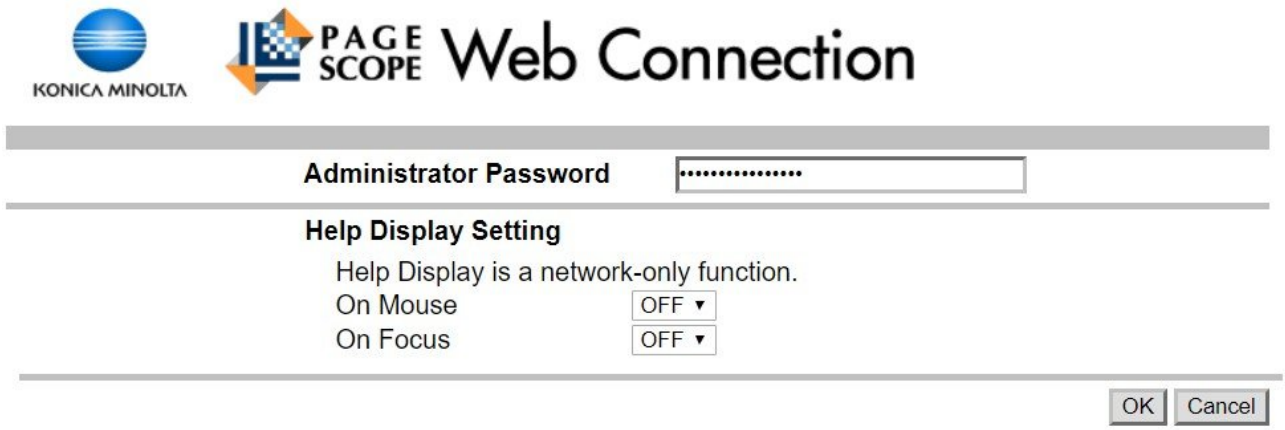
Open printers Webinterface in a browser and choose "To Login Screen" and choose "Ok" when asked if you are sure to logout Public User.



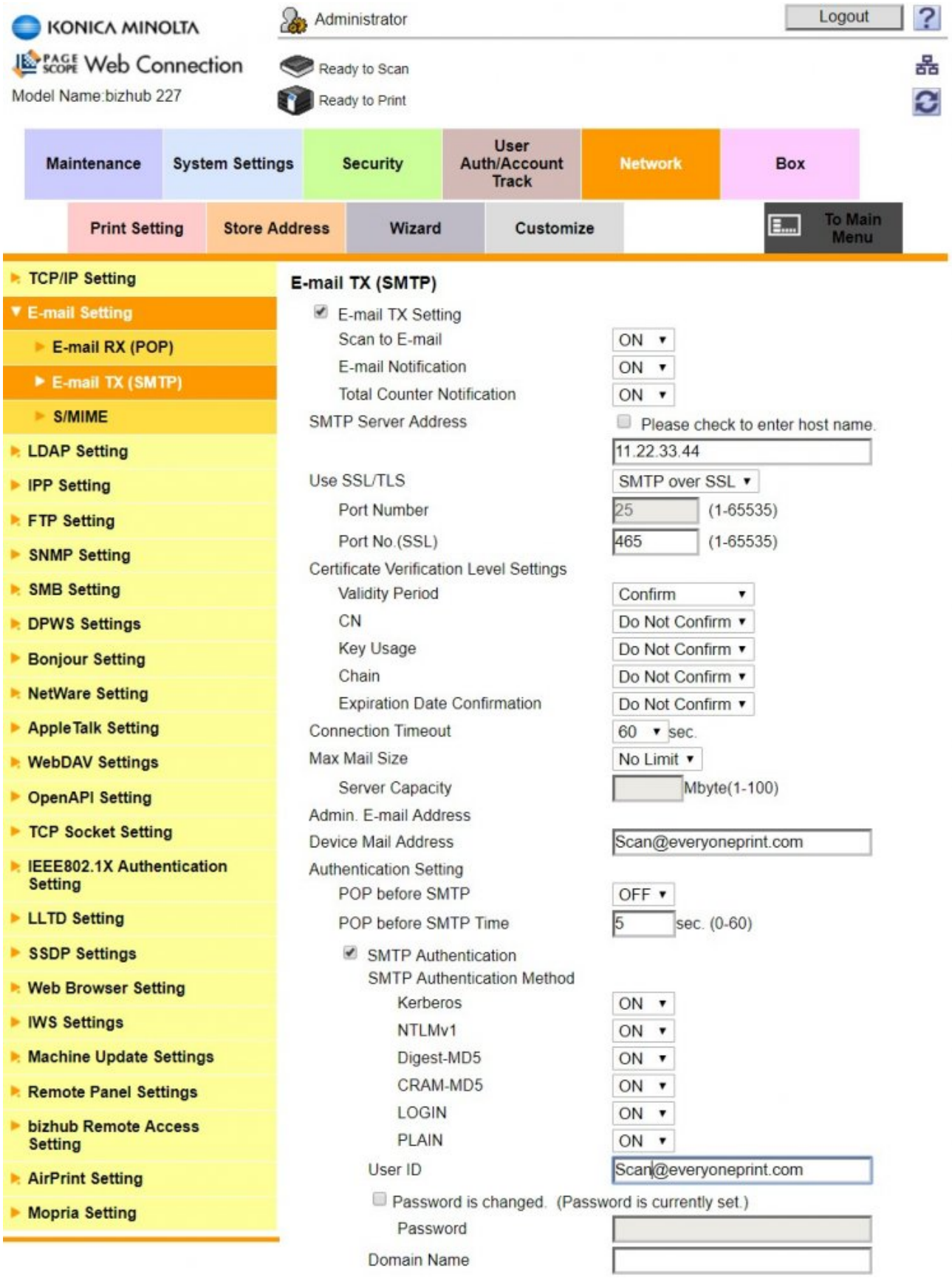
Choose "Administrator" and choose "Login".



Enter the administrator password and choose "OK".

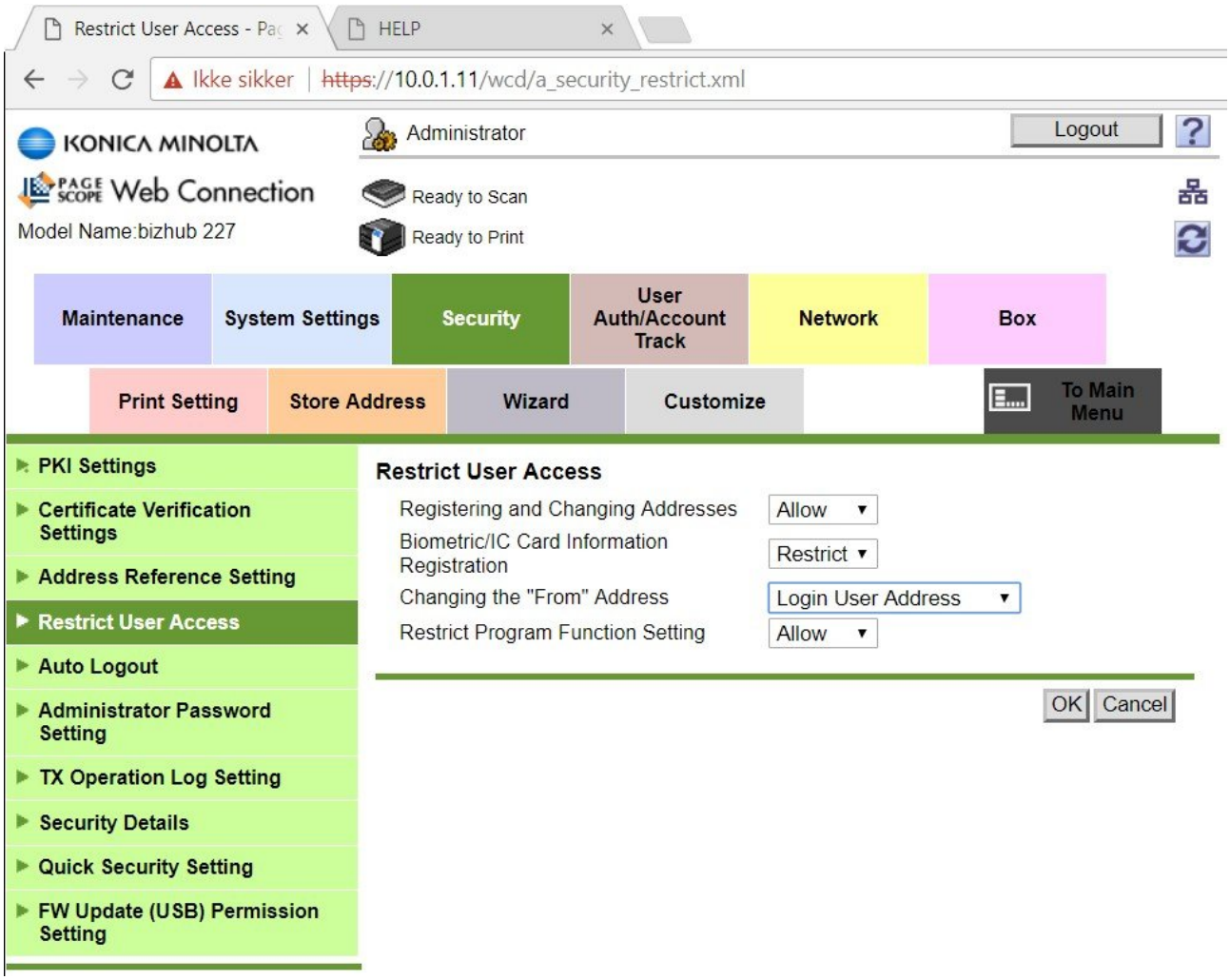


Choose "Network", "E-mail Settings" and "E-mail TX (SMTP)".
Fill out with proper information for setting up Scan To Email and choose "Ok" at the bottom of the page.



The are three options in the "From"-field in the E-mails going out as Scan To E-mail.
It is changeable under "Security" and "Restrict User Access", "Changing the "From" Address", also

here you are able to block users from adding email-addresses into the printers Addressebook by changing "Registering and changing Addresses".



The "From"-Field can be set to:

Allow:	Allows the user to change the "From"-field to any E-mail.
Login User Address:	Uses the logged in users E-mail address.
Admin. E-mail Address:	Uses the E-mail Address set under "Admin E-mail Address" in SMTP-settings.

If any of the last two options is set the user cannot change the field.
Remember that "Admin. E-mail Address" is set under "System Settings" and "Machine Settings".

Kyocera MFDs

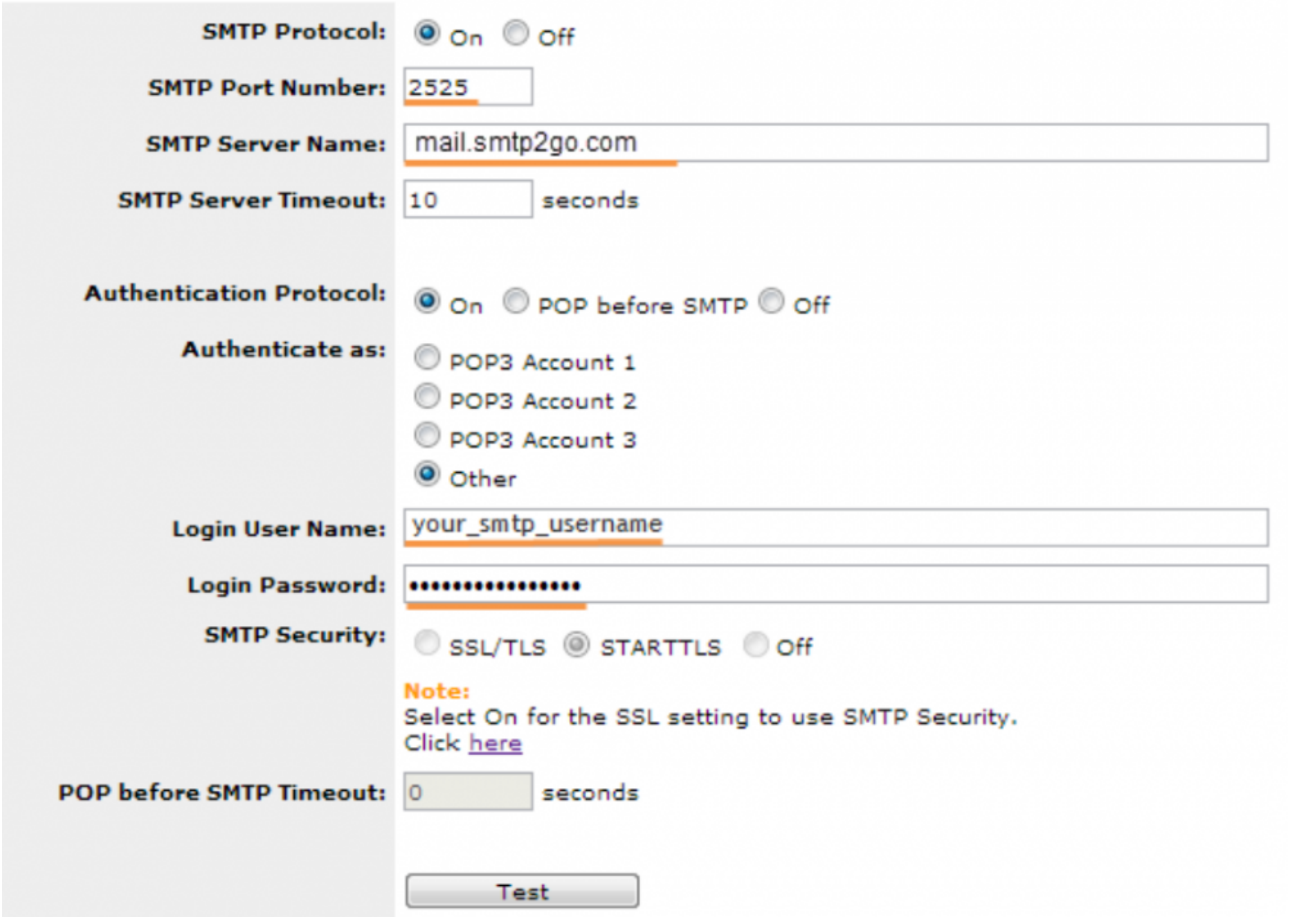
For Kyocera devices, native scan to email functionality will be used.

Please follow the below steps by opening the printer Web interface in a browser to do SMTP configuration:

1. Go to device homepage

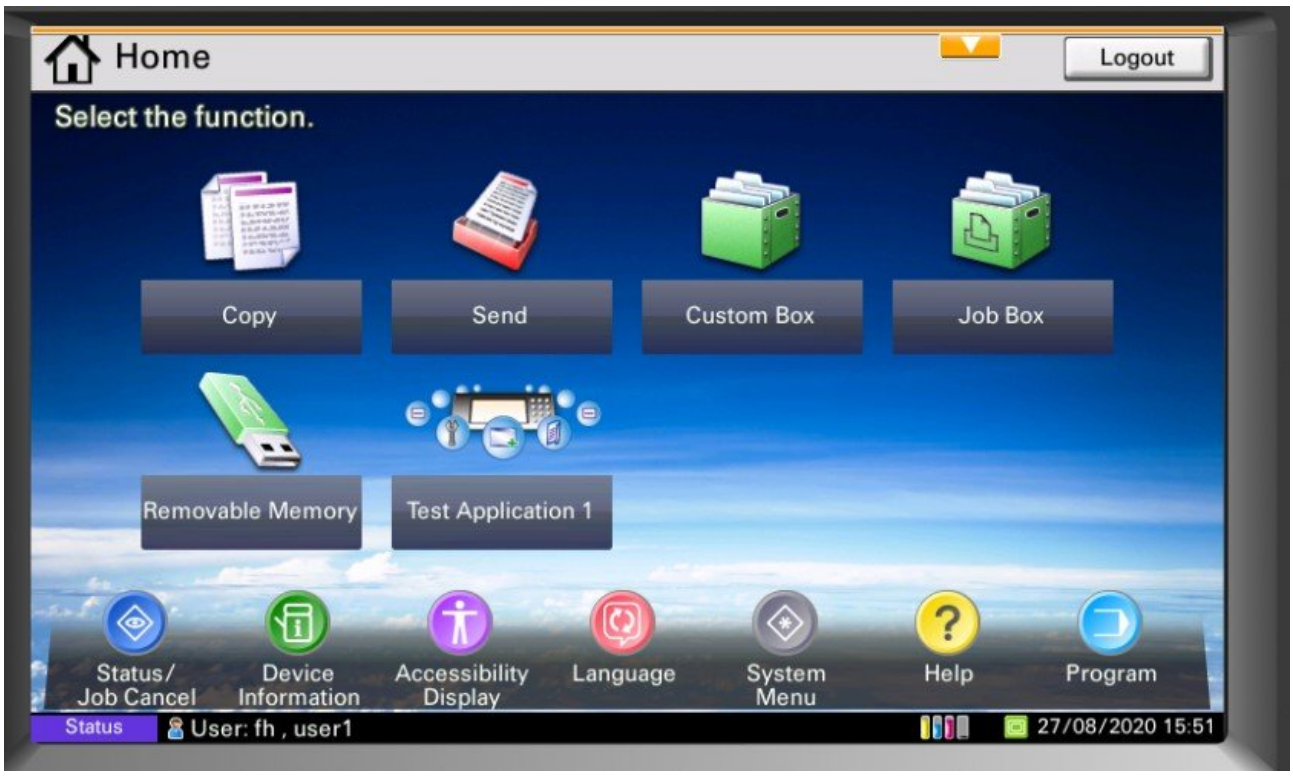
2. Login using valid credentials

3. Go to Advanced > E-mail > SMTP > General and add a SMTP configuration as applicable

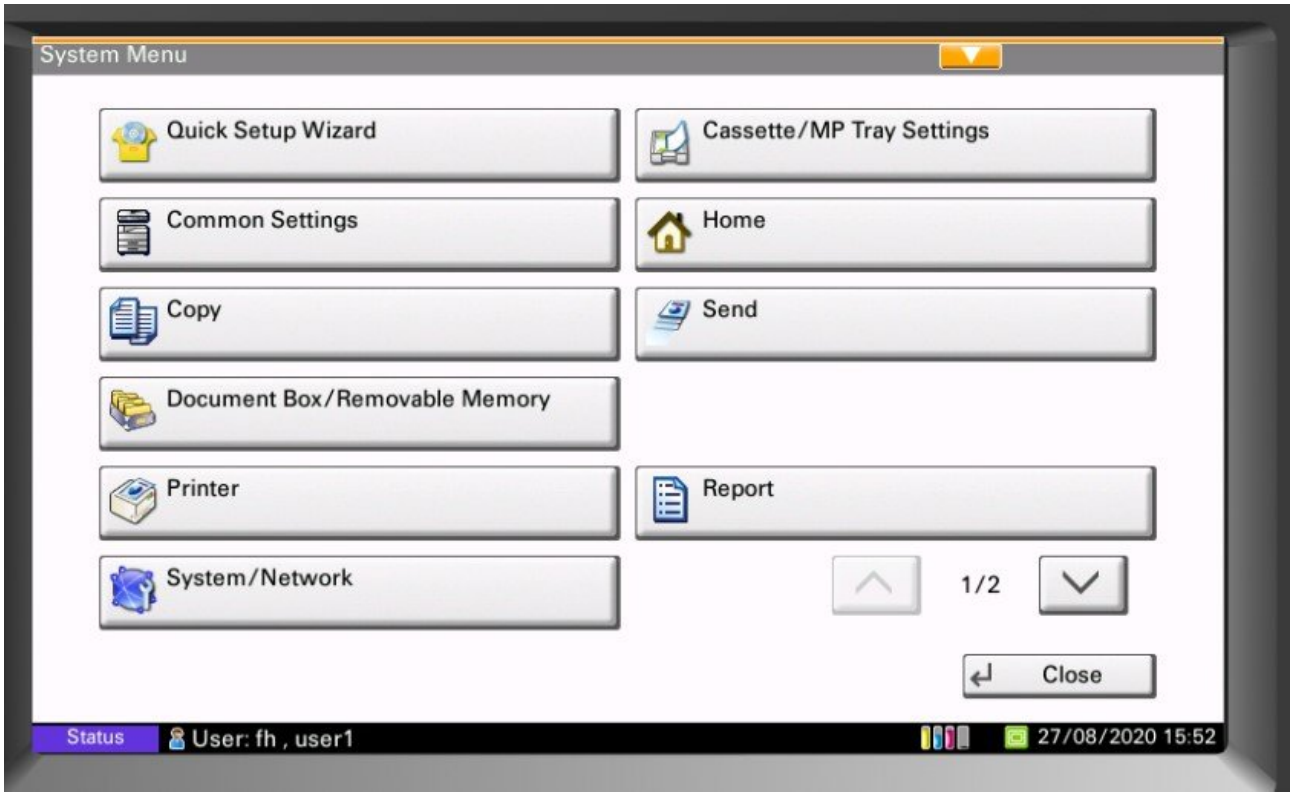


Please follow the below steps on the device for configuring scan to email functionality:

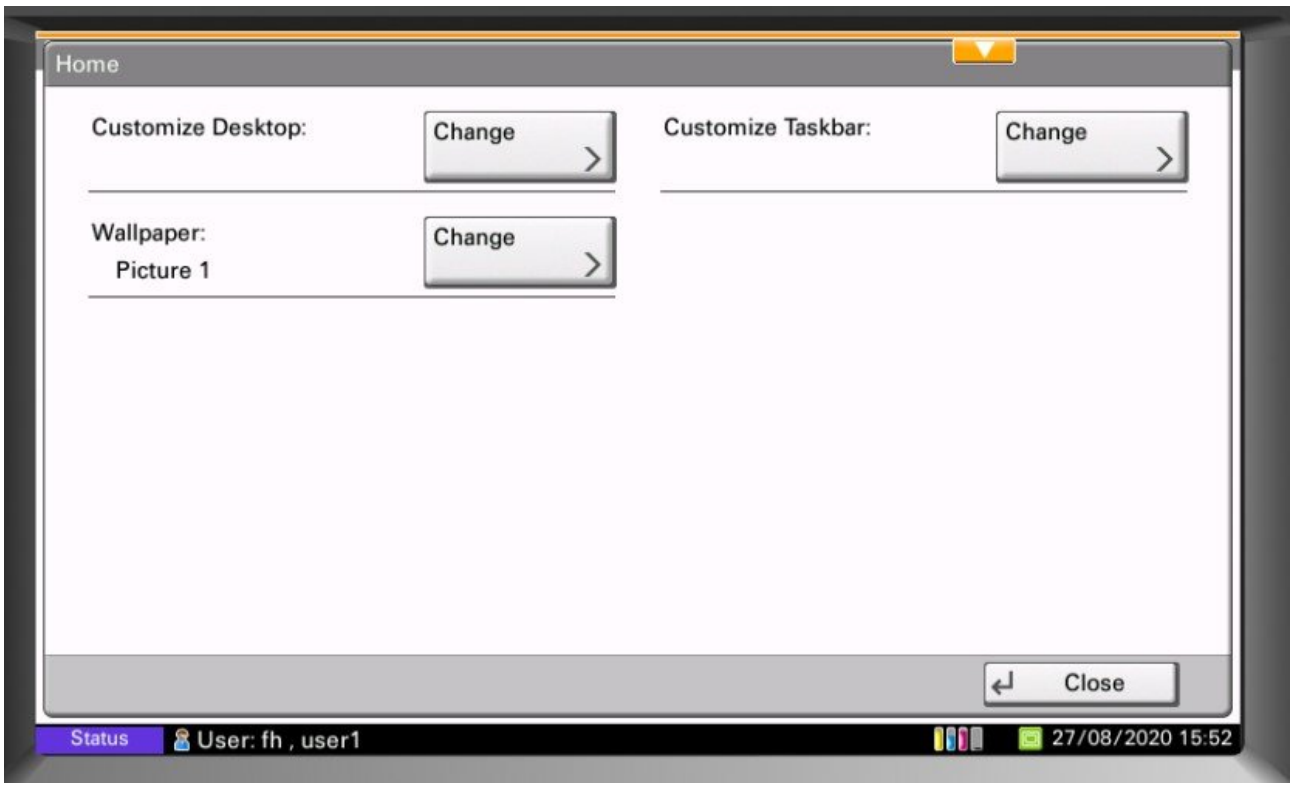
1. From Home screen, please select "System Menu"



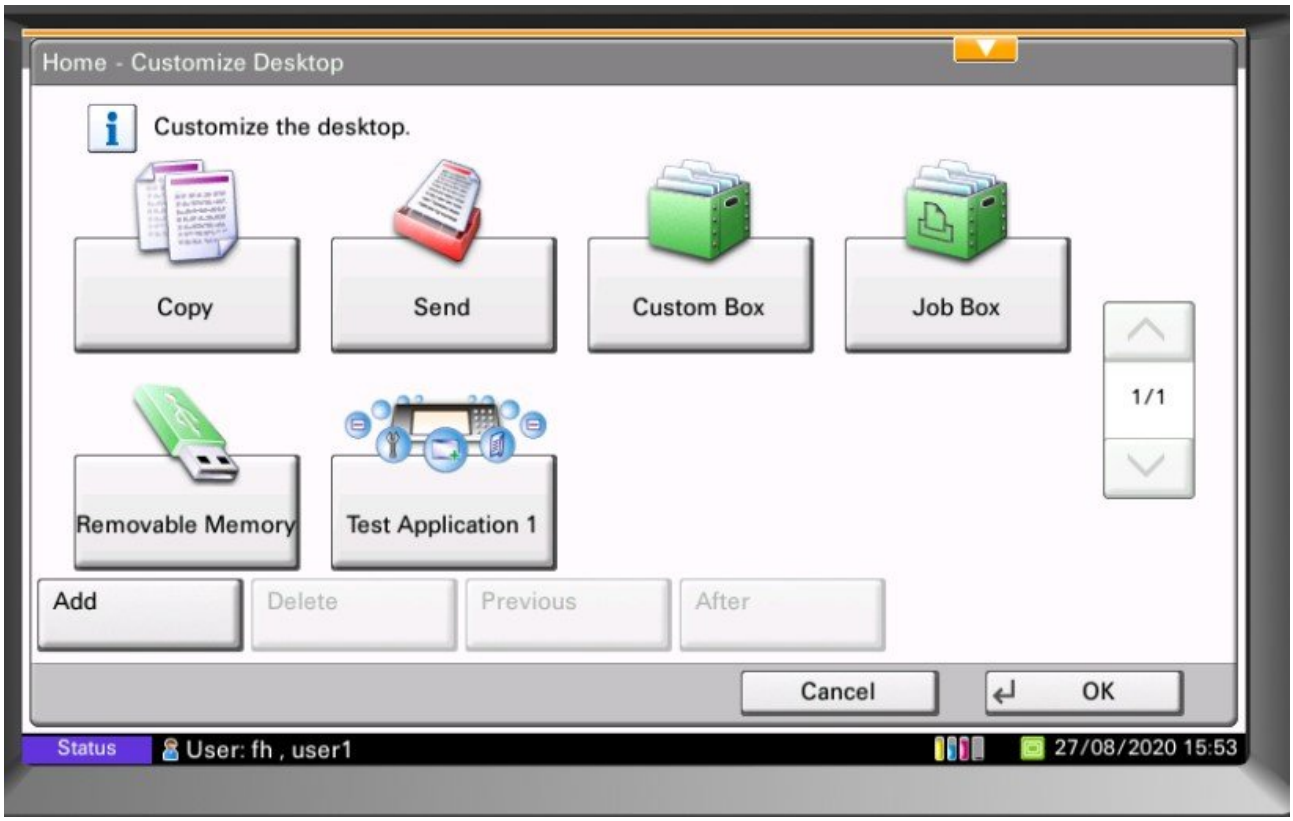
2. From "System Menu", please select "Home"



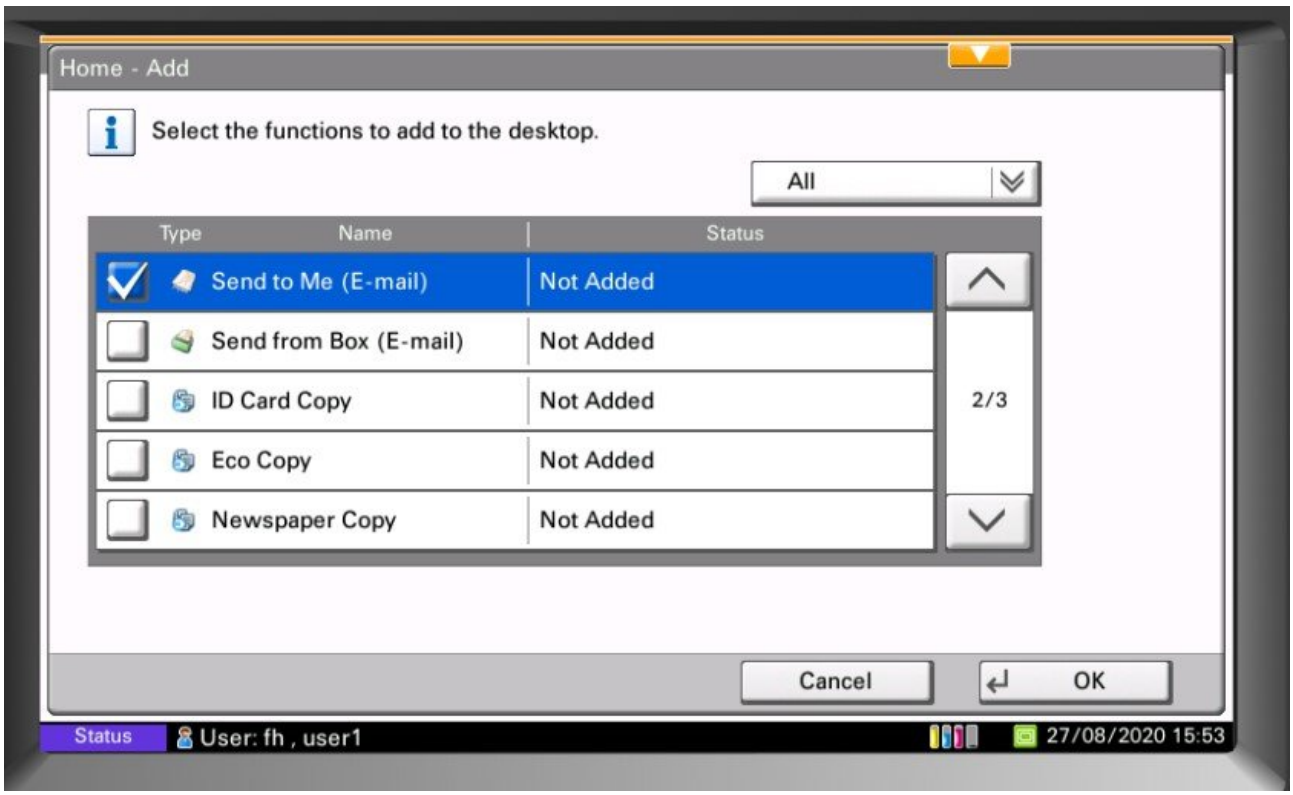
3. From "Home", please select "Customize Desktop" and press "Change" button



4. From "Customize Desktop", please press "Add" button



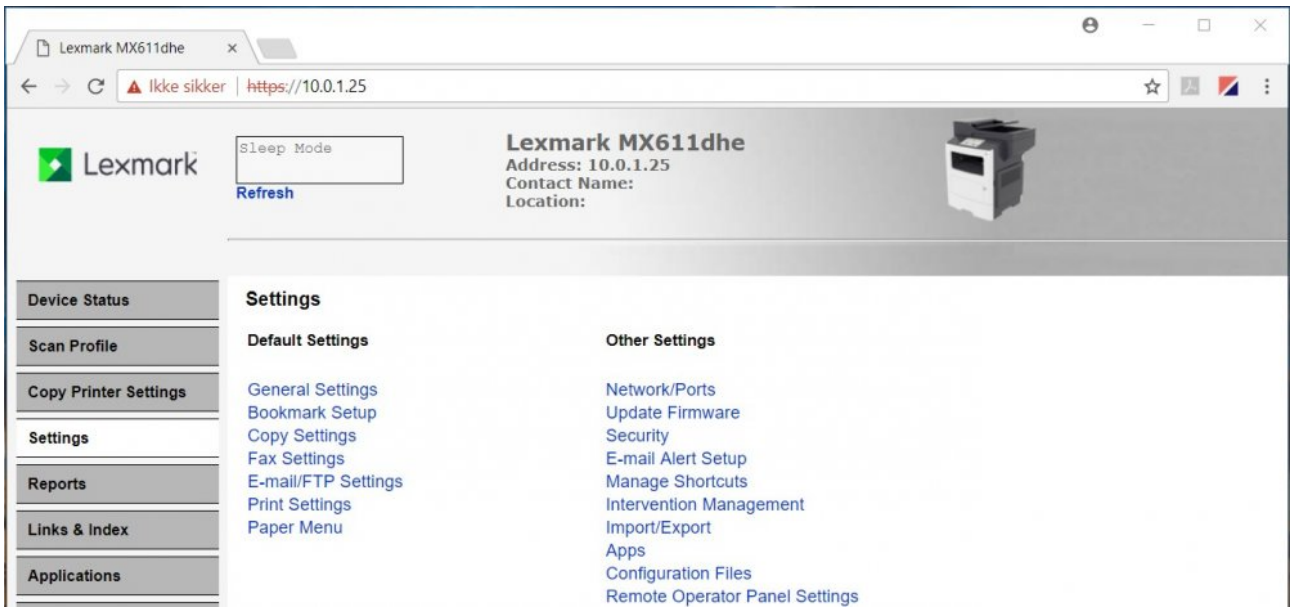
5. From the new screen, scroll down and select "Send to ME (E-Mail)" and press OK all the way to the HOME screen



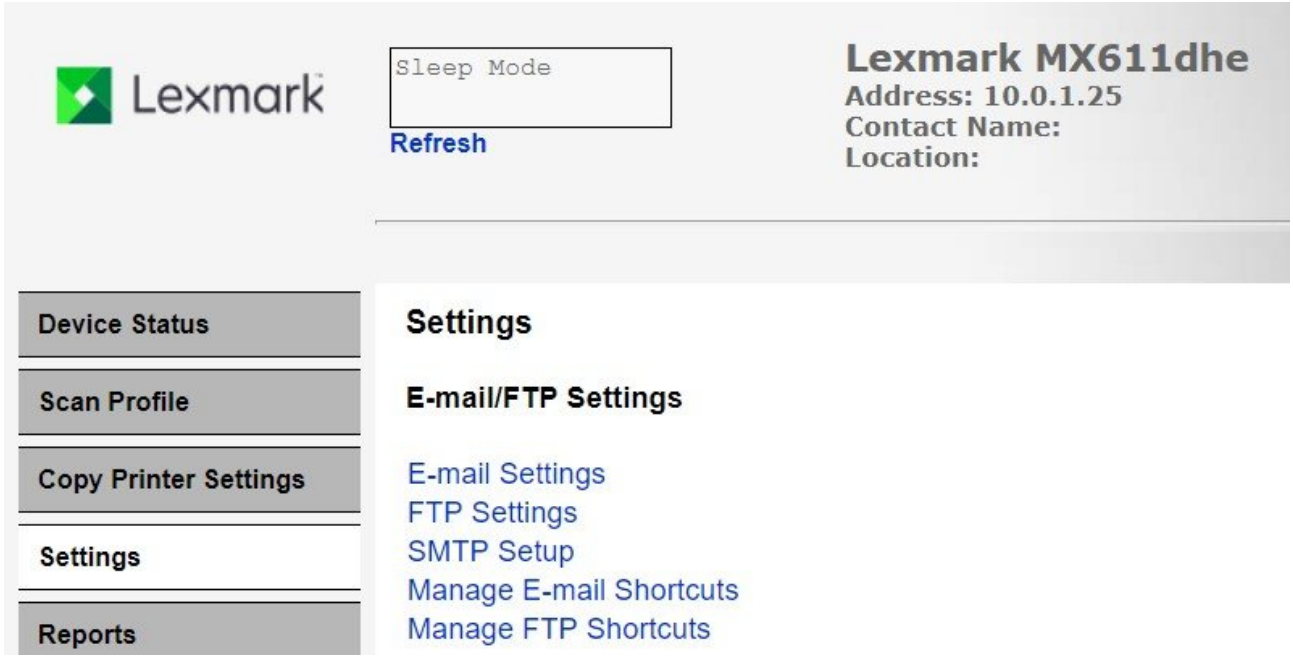
6. On the "Home" screen, "Send to ME (E-Mail)" should be available

Lexmark MFDs

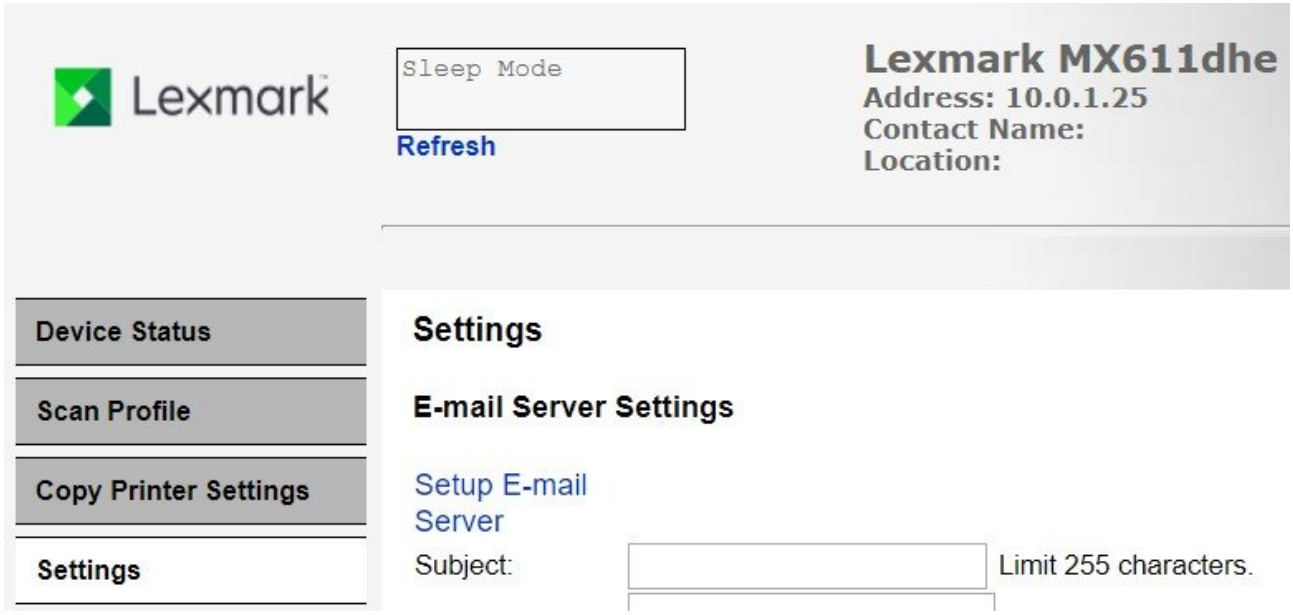
Open printers Webinterface in a browser and choose "Settings" in the left pane and then "E-mail/ FTP Settings".



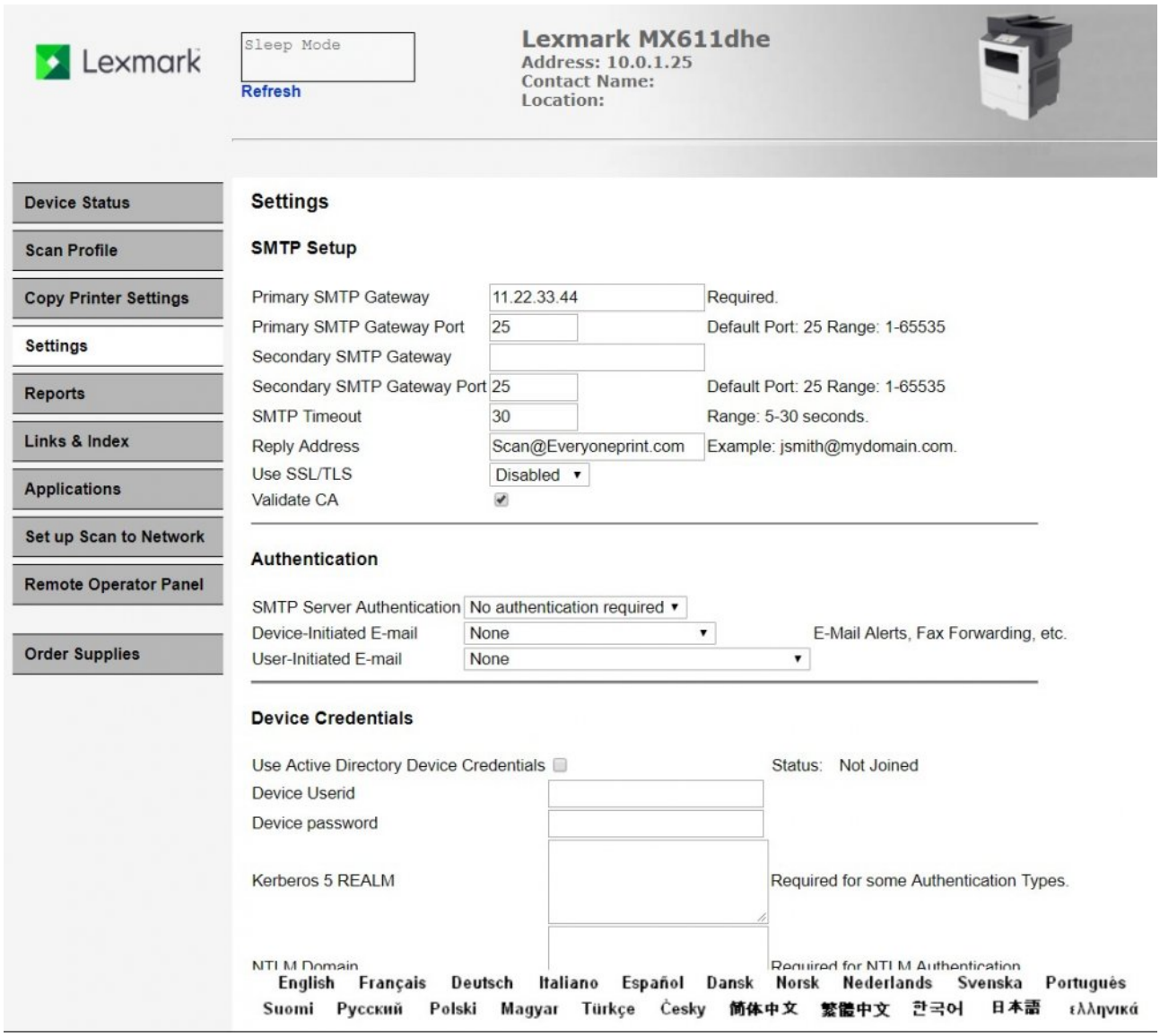
Choose "E-mail Settings".



Choose "Setup E-mail Server".

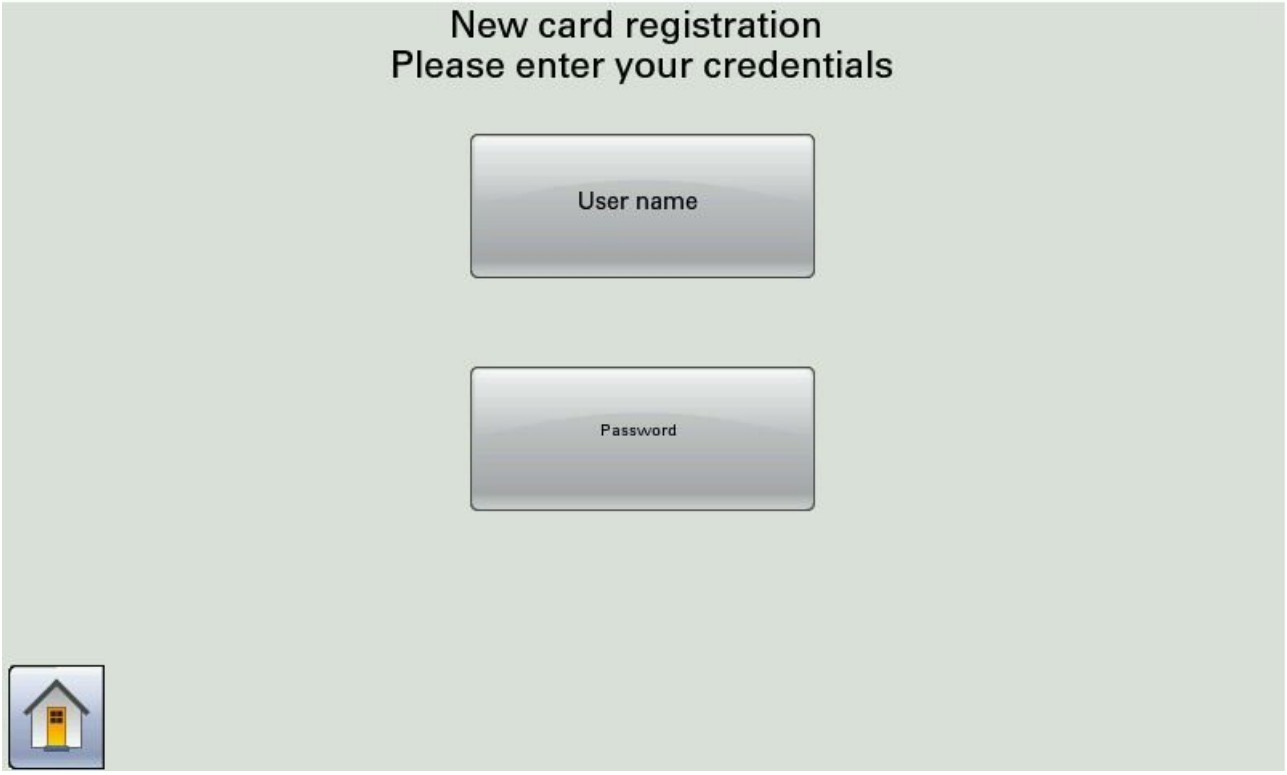


Set up with proper information and choose "Submit".



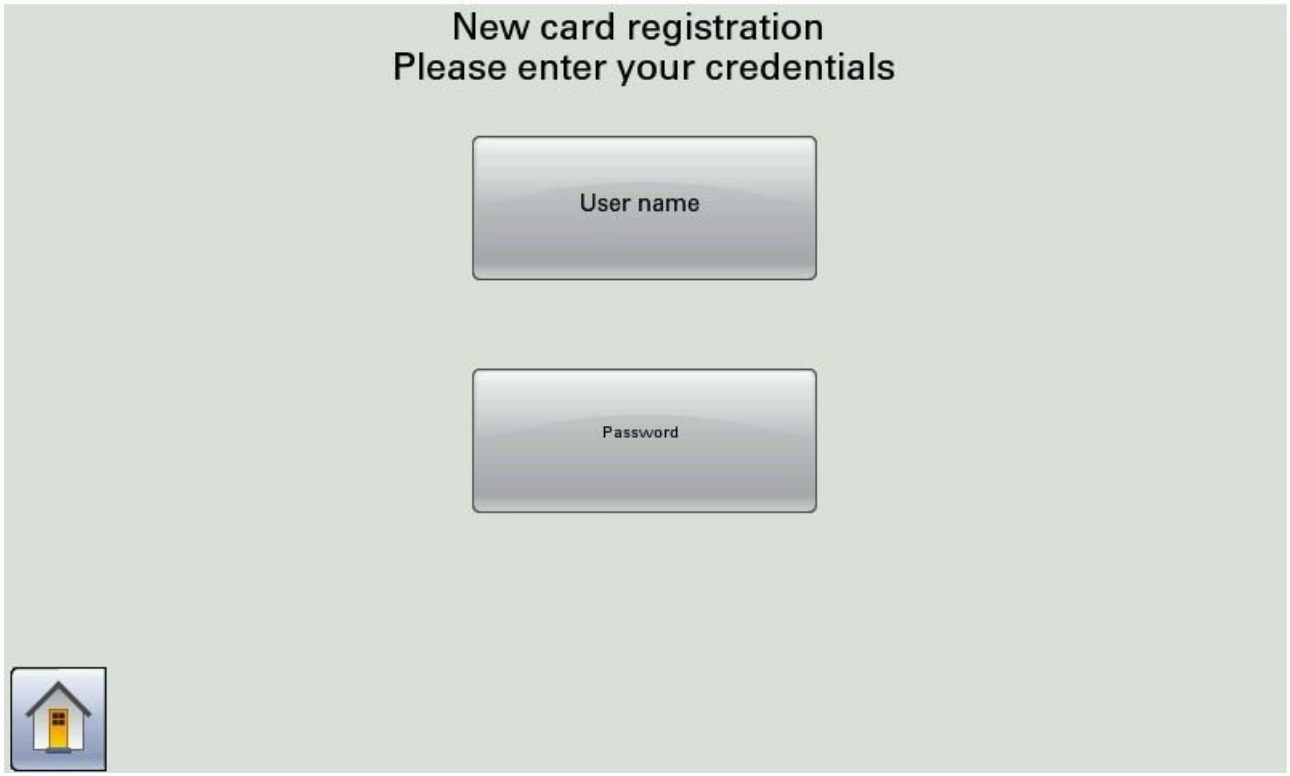
Card Self Enrollment:

Swipe your card over the cardreader.

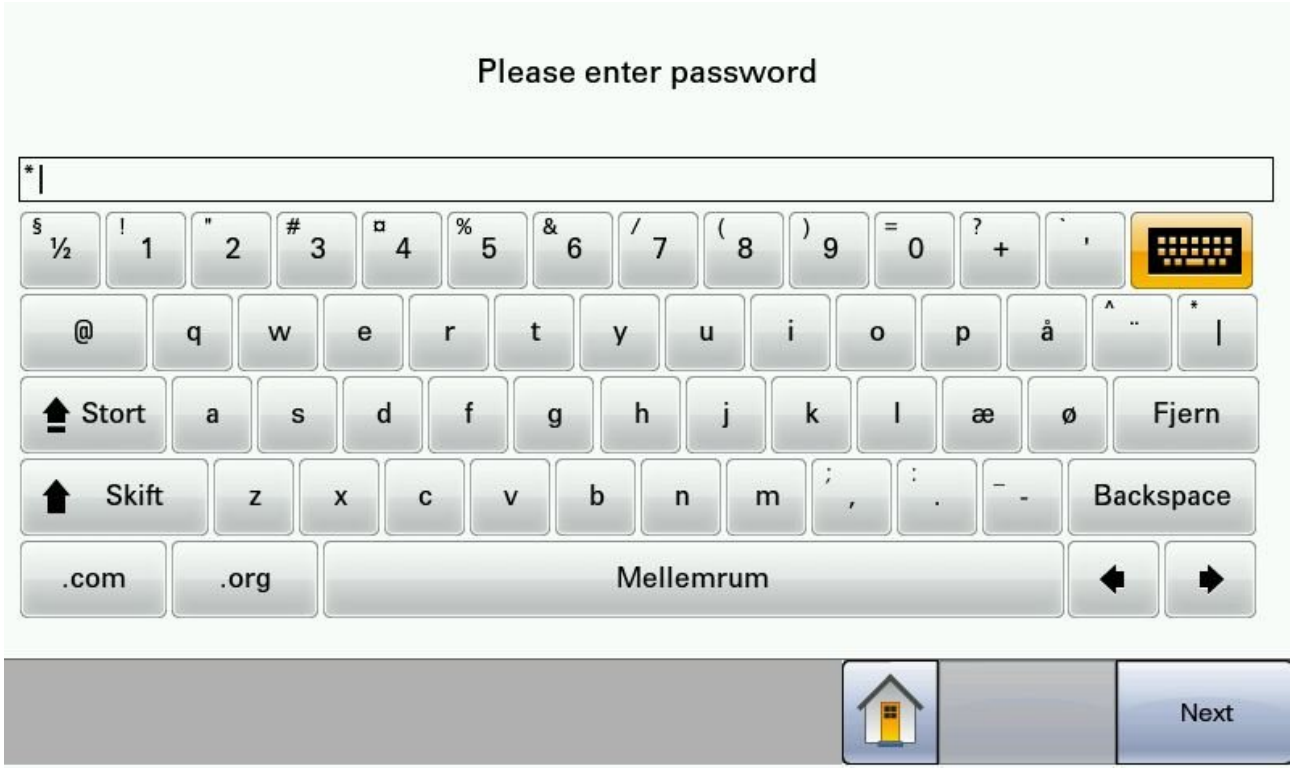


Choose "User name" and fill out with your proper Username.

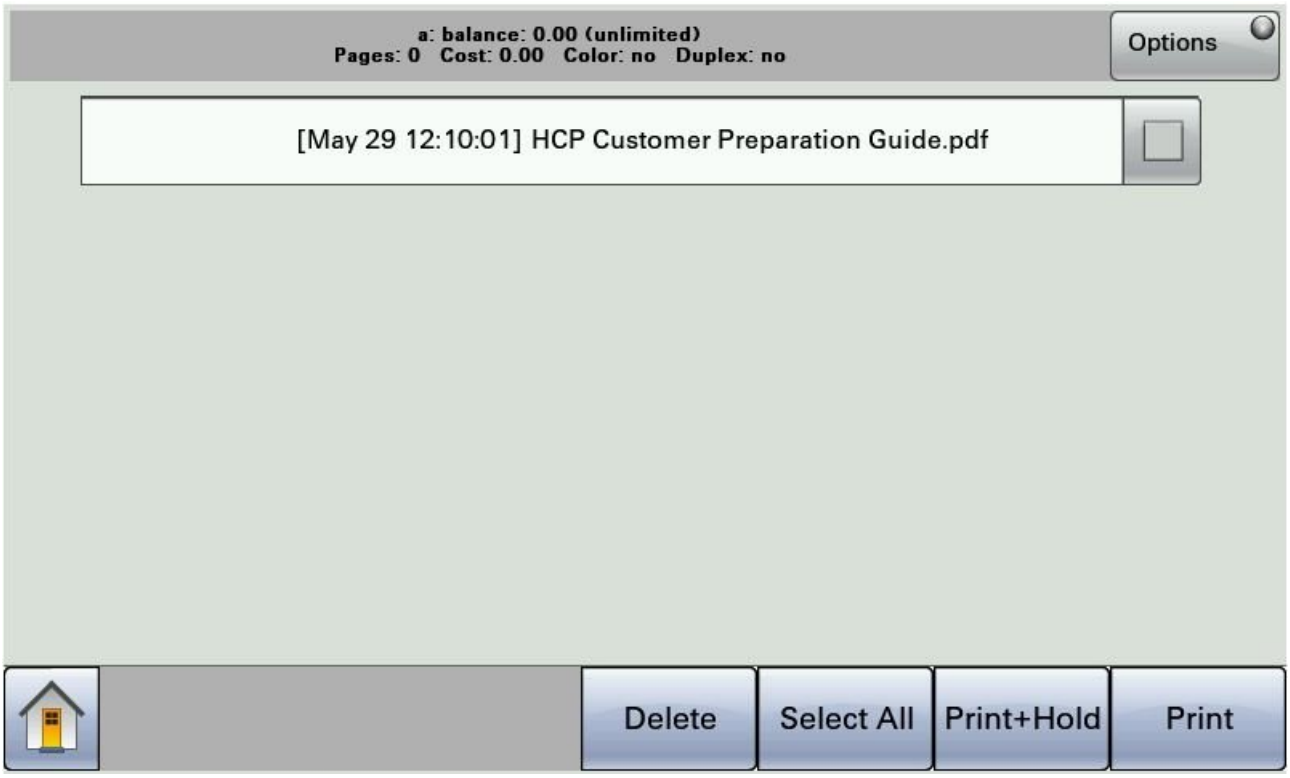
Choose "Password".



Fill out with your proper password.

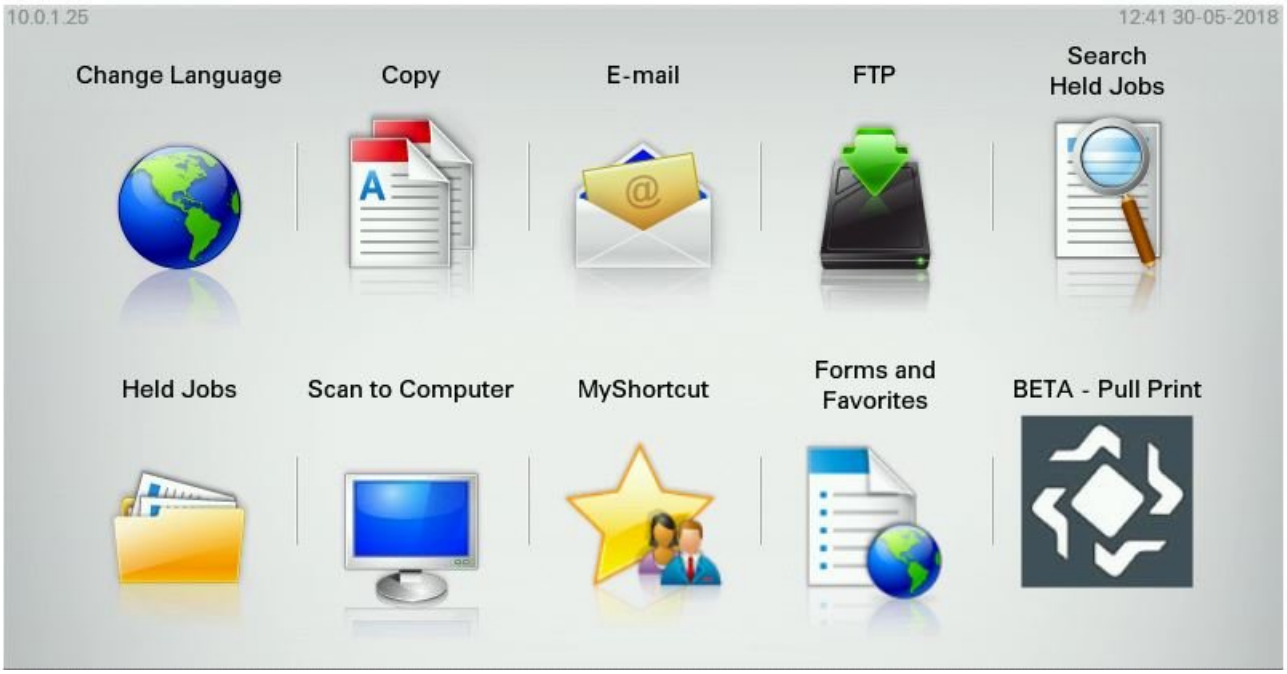


Now you have enrolled your card to your user and you are able to login using the cardreader for releasing printjobs or using other functions at the MFD.

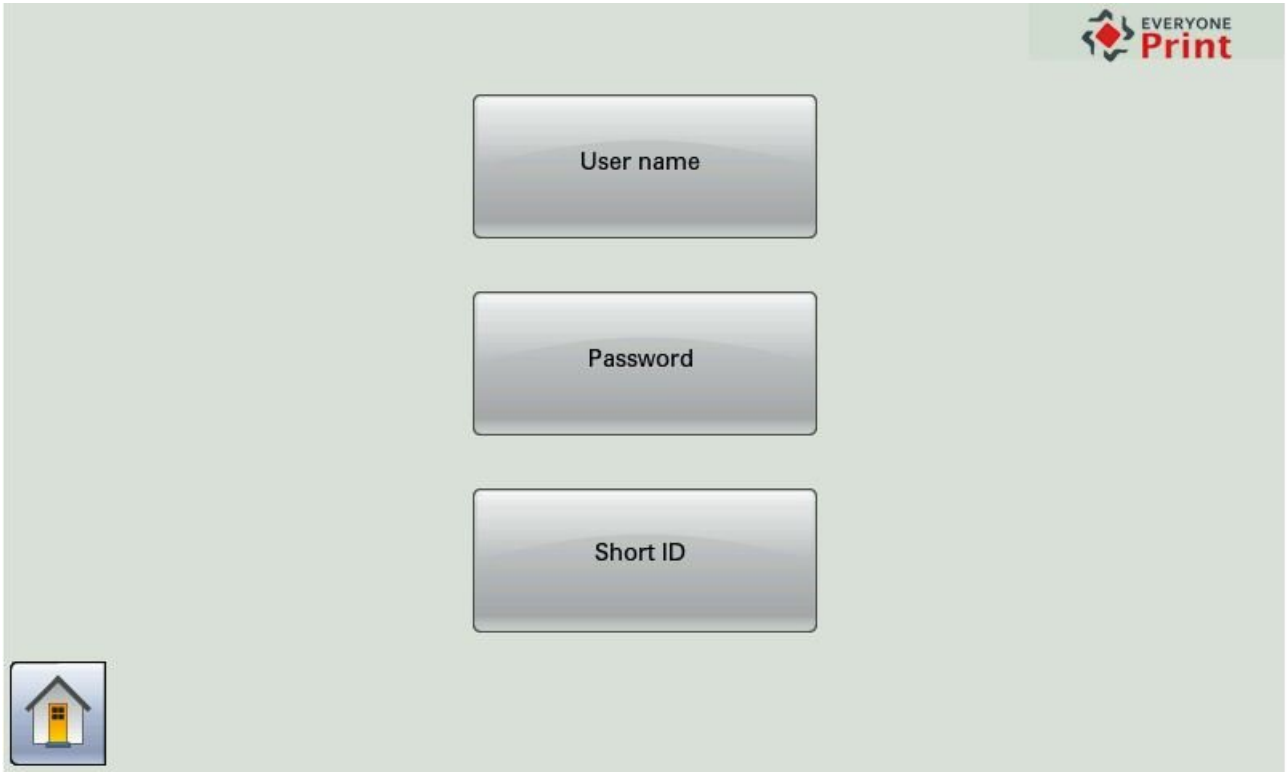


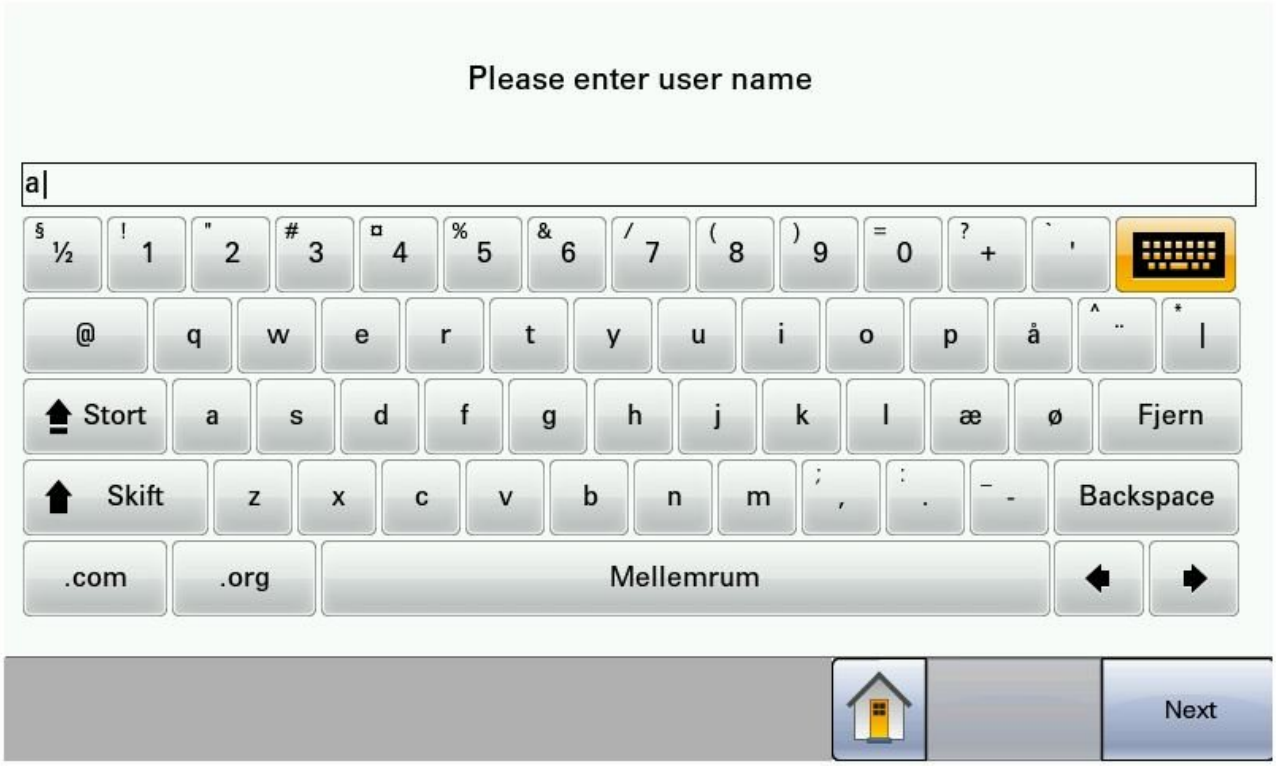
Manual login on the printer:

Choose the "Pull Print"-button on the display.

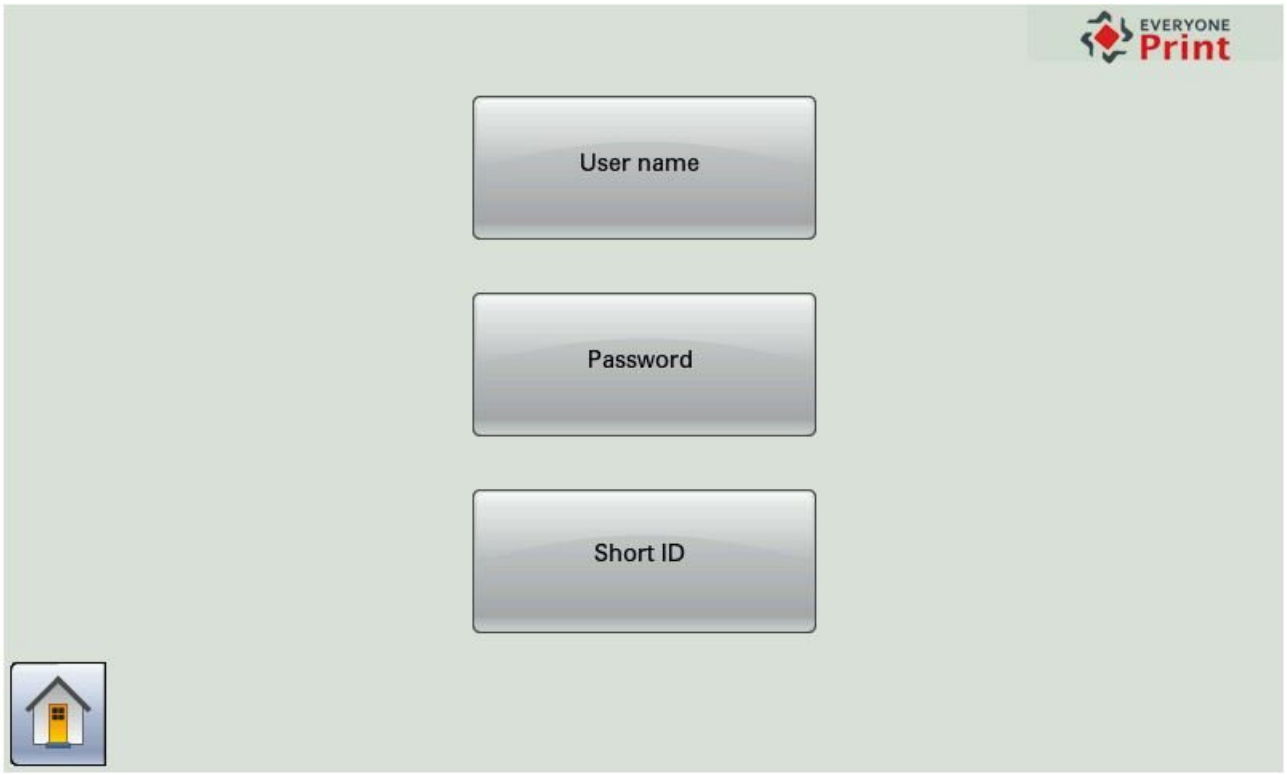


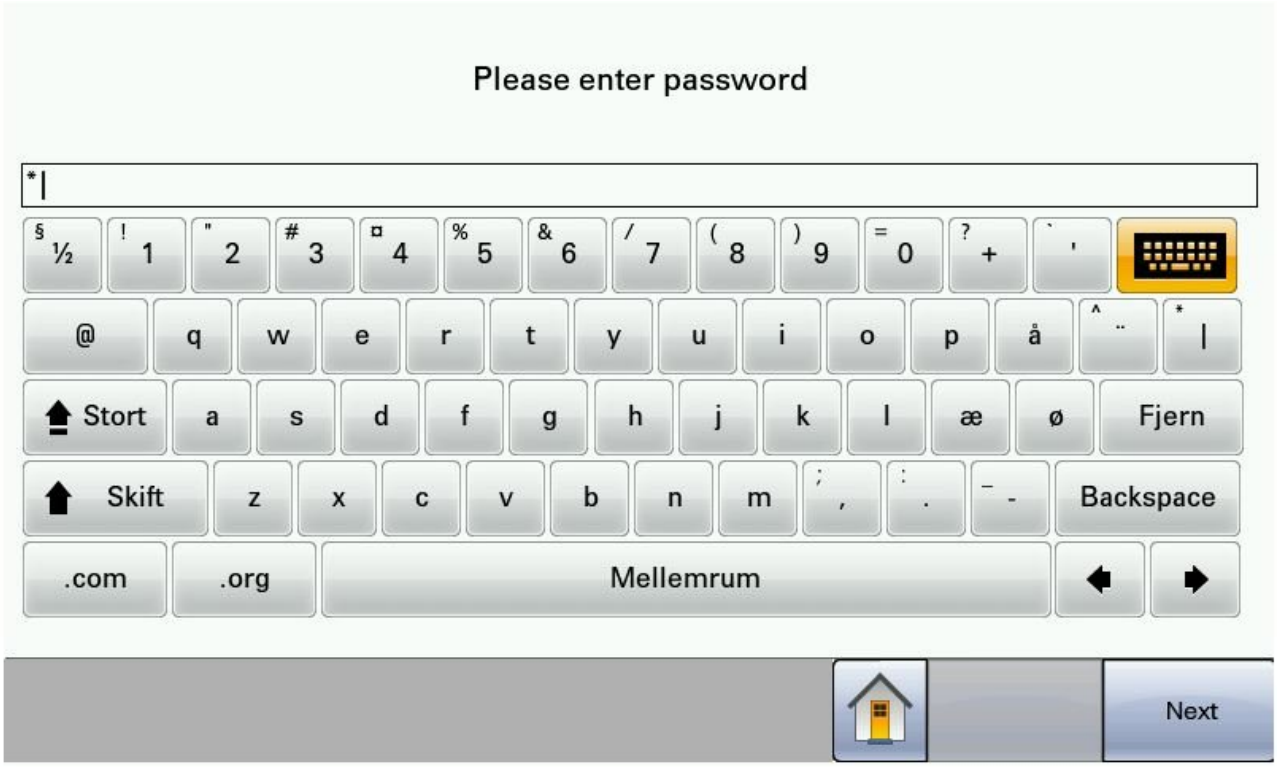
Choose the "User name"-button and enter your username.



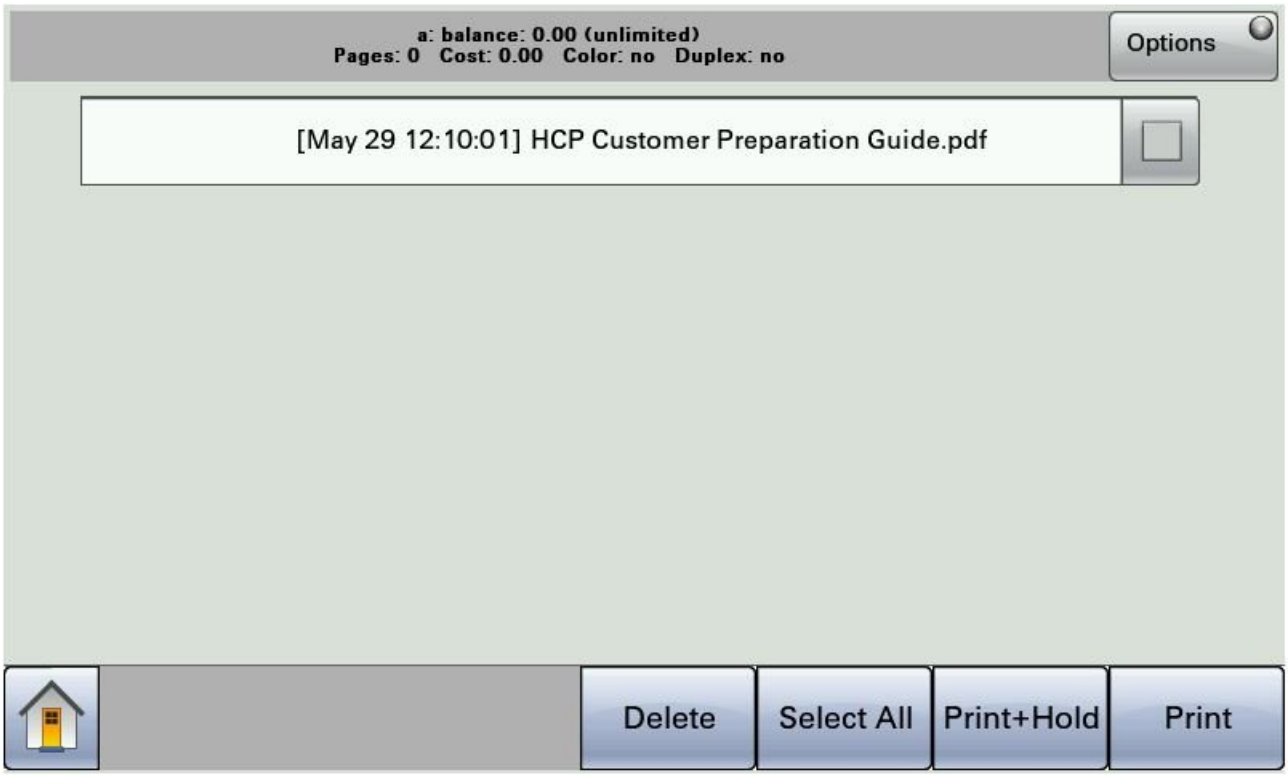


Choose the "Password"-button and enter your password.



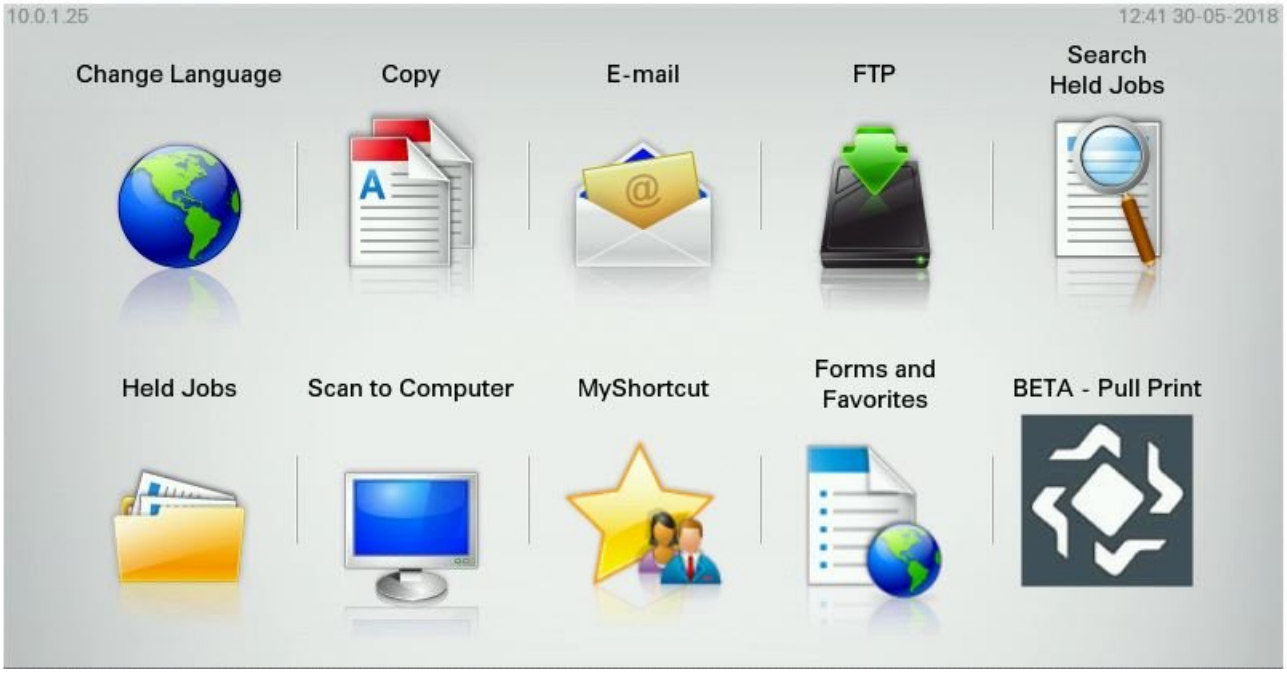


Now you can release your printjobs or push the "Home"-button for Scan, copier etc.



Using the Scan to E-mail function:

Choose the "E-mail"-button.



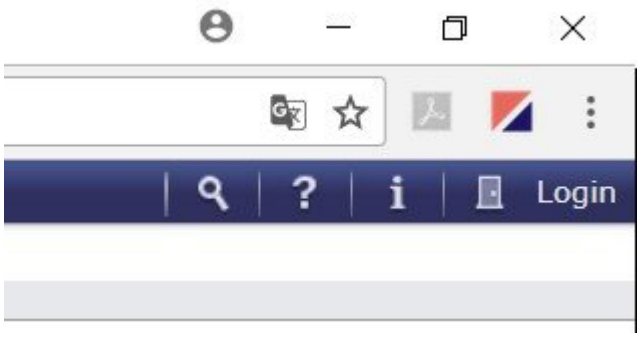
Touch the keyboard besides the "Recipient (S)"-button and fill in your E-mail.

Now you are ready to Scan, just touch the "Scan it"-button.

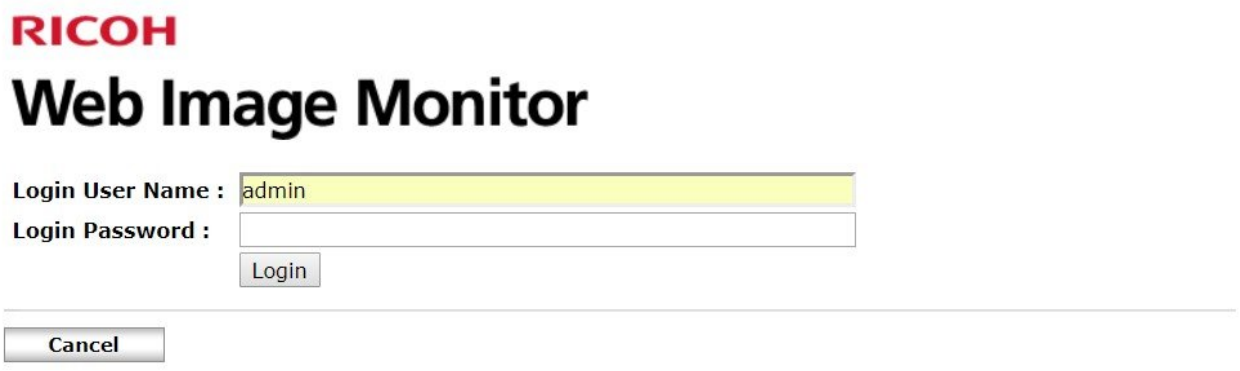
Ricoh MFDs

Setting up Scan2Mail

Open printers Webinterface in a browser and choose "Login" at the upper right corner.

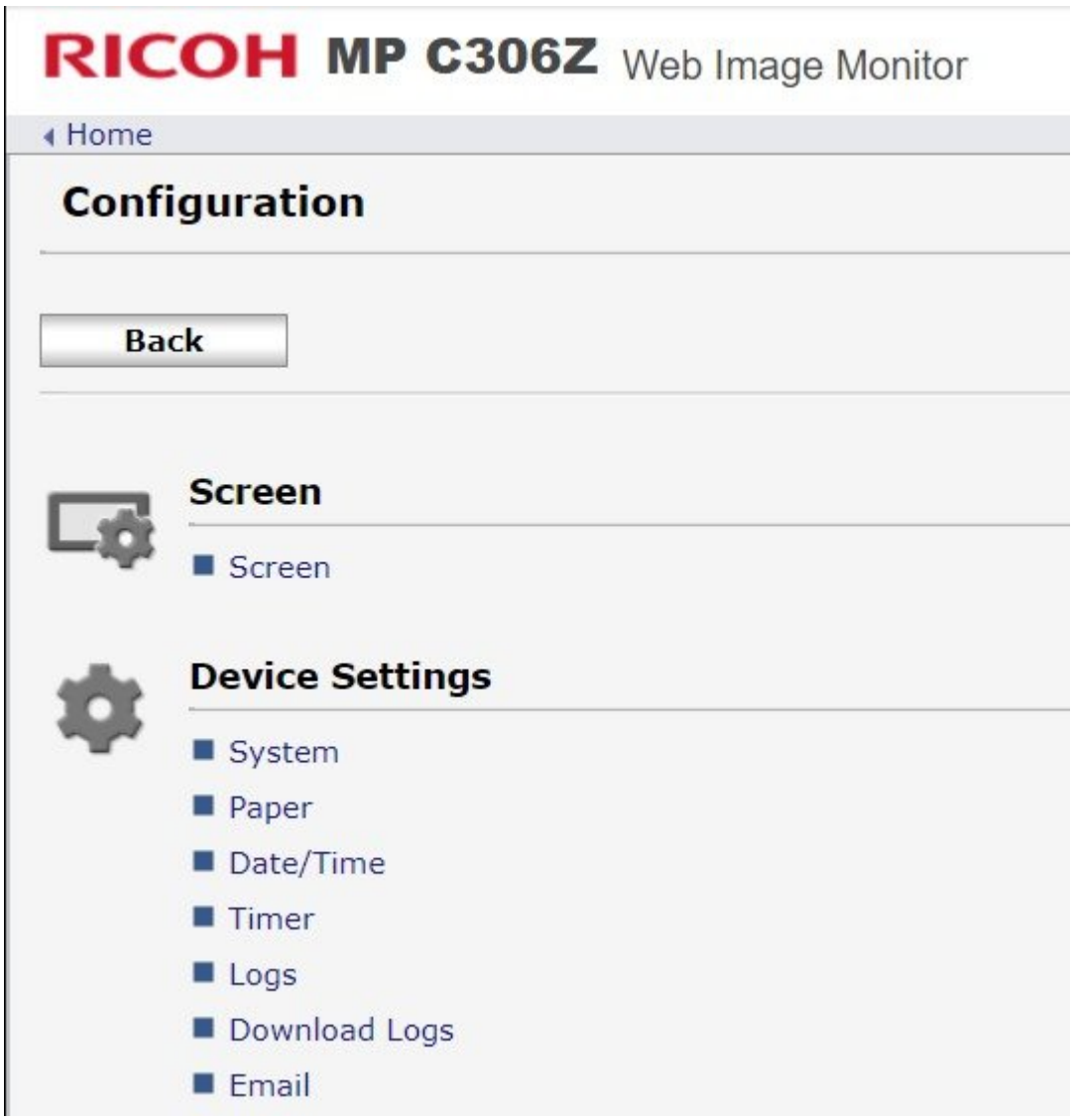


Write "Admin" under "Login User Name" and don't write a password if you have not changed it. Choose "Login".

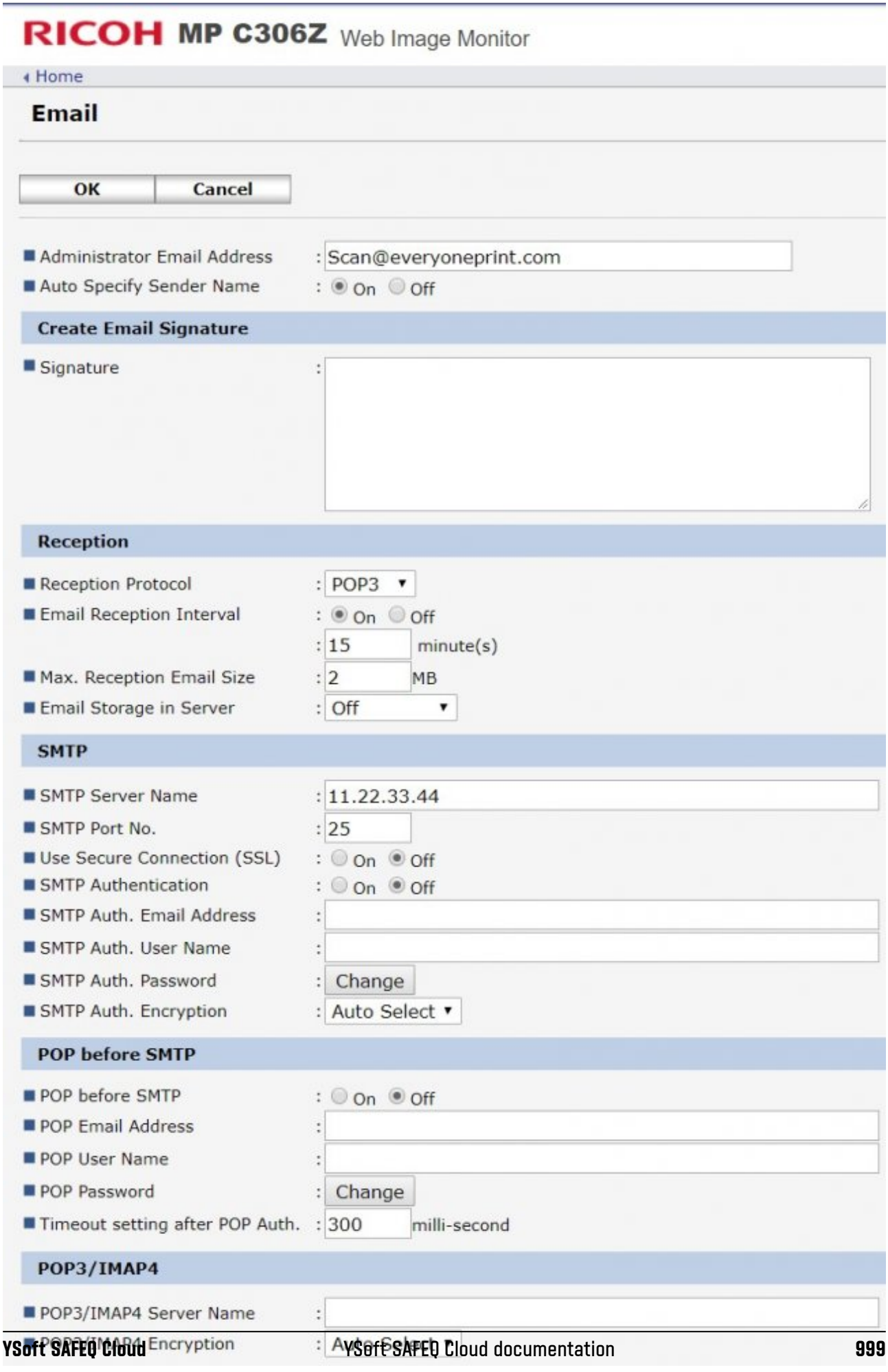


Under "Device Management" choose "Configuration".

Choose "Email" under "Device settings".



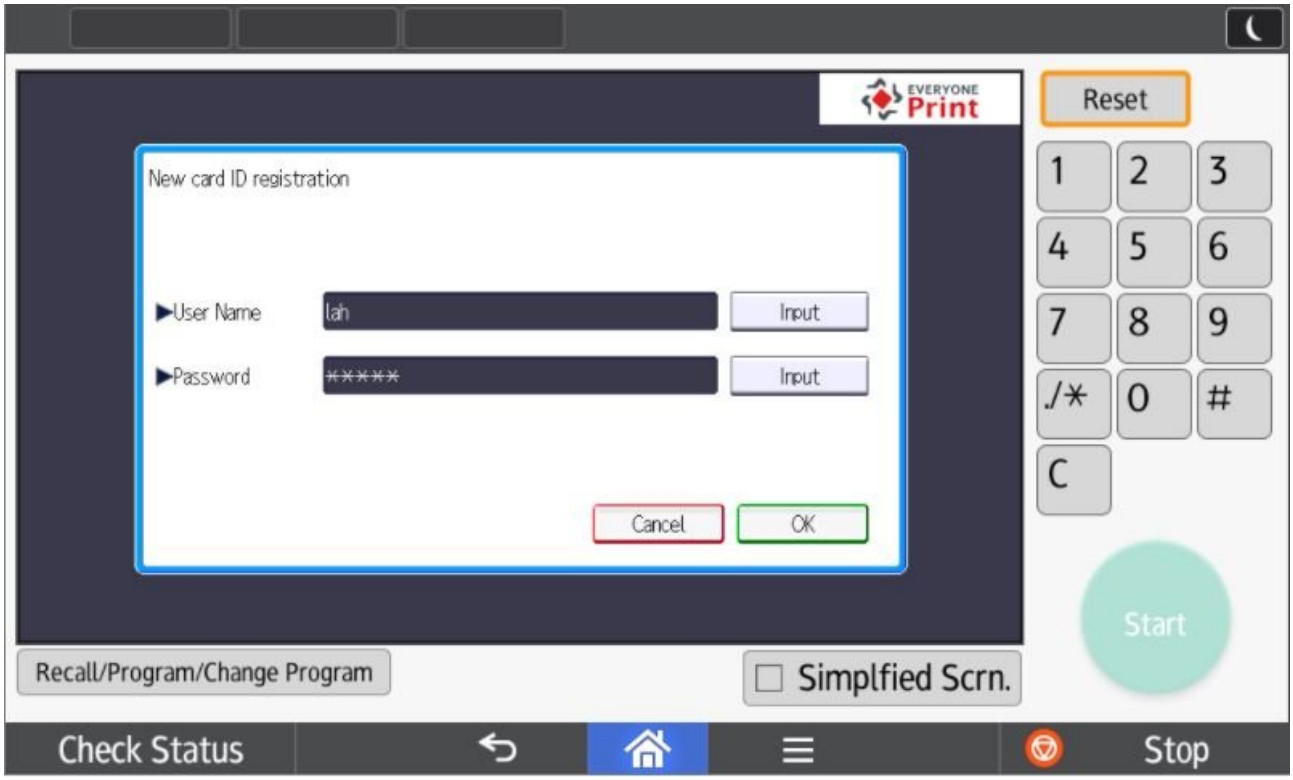
Fill out with proper information for setting up Scan To Email and choose "Ok" at the bottom of the page.


RICOH MP C306Z Web Image Monitor
Home
Email
OK
Cancel
Administrator Email Address : Scan@everyoneprint.com
Auto Specify Sender Name : On Off
Create Email Signature
Signature :
Reception
Reception Protocol : POP3
Email Reception Interval : On Off
: 15 minute(s)
Max. Reception Email Size : 2 MB
Email Storage in Server : Off
SMTP
SMTP Server Name : 11.22.33.44
SMTP Port No. : 25
Use Secure Connection (SSL) : On Off
SMTP Authentication : On Off
SMTP Auth. Email Address :
SMTP Auth. User Name :
SMTP Auth. Password : Change
SMTP Auth. Encryption : Auto Select
POP before SMTP
POP before SMTP : On Off
POP Email Address :
POP User Name :
POP Password : Change
Timeout setting after POP Auth. : 300 milli-second
POP3/IMAP4
POP3/IMAP4 Server Name :

If "Auto Specify Sender Name" is set to "On" the Administrator Email Address will be set as the default sender at Scan To Email.
If "Auto Specify Sender Name" is set to "Off" the logged in users email address is set as the sender at Scan To Email. (Depends on model of MFD)

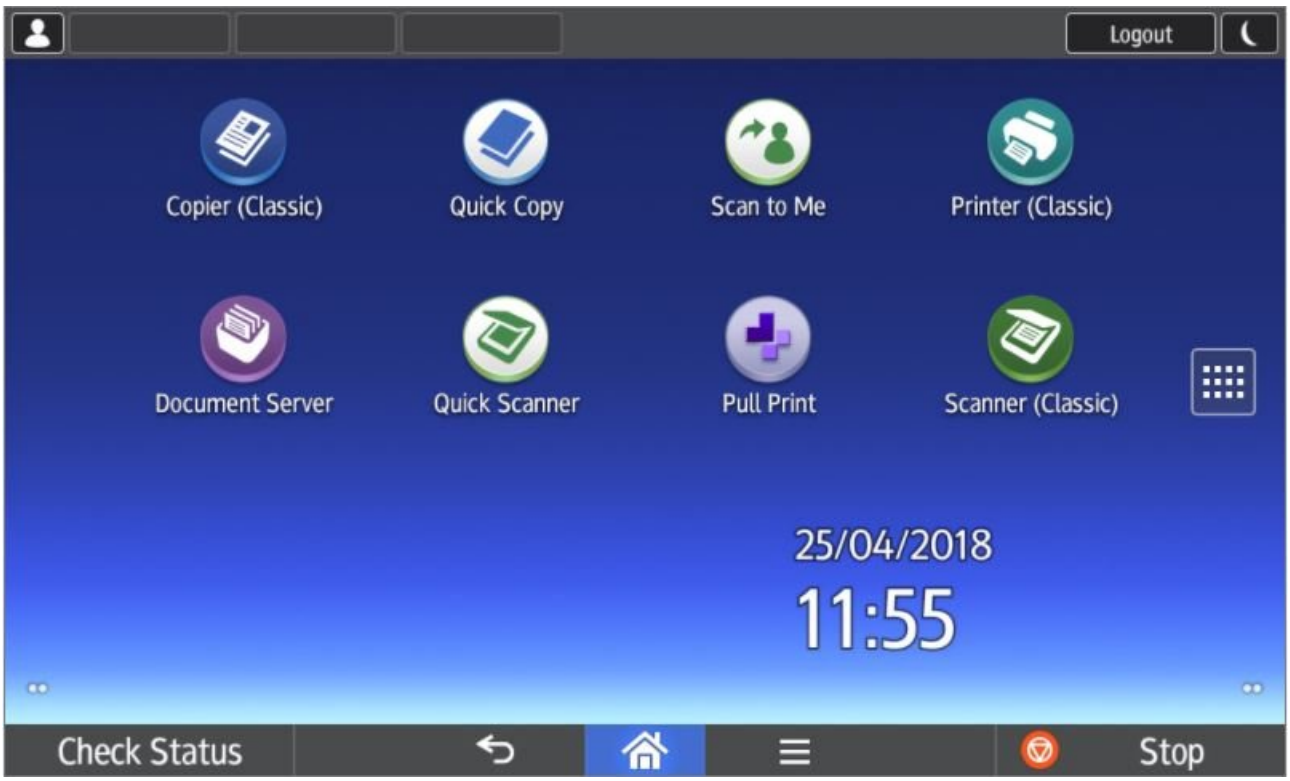
Card Self enrollment on the MFD:

Push the "Pull Print"-icon on the display. Swipe your card over the cardreader, enter your username and password when asked for it and then "Ok". Now your card is enrolled to your user.



Log in to the machine by card:

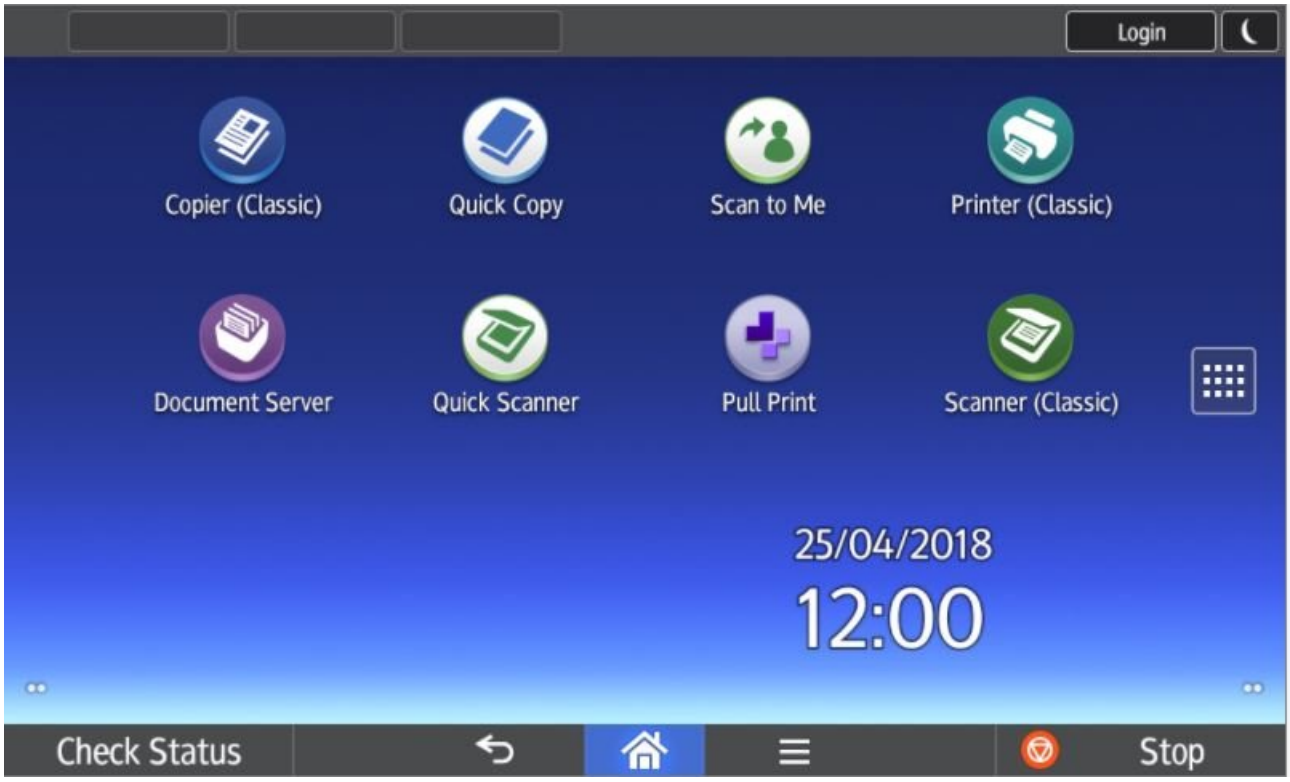
Just swipe your card and choose the function you want to use.



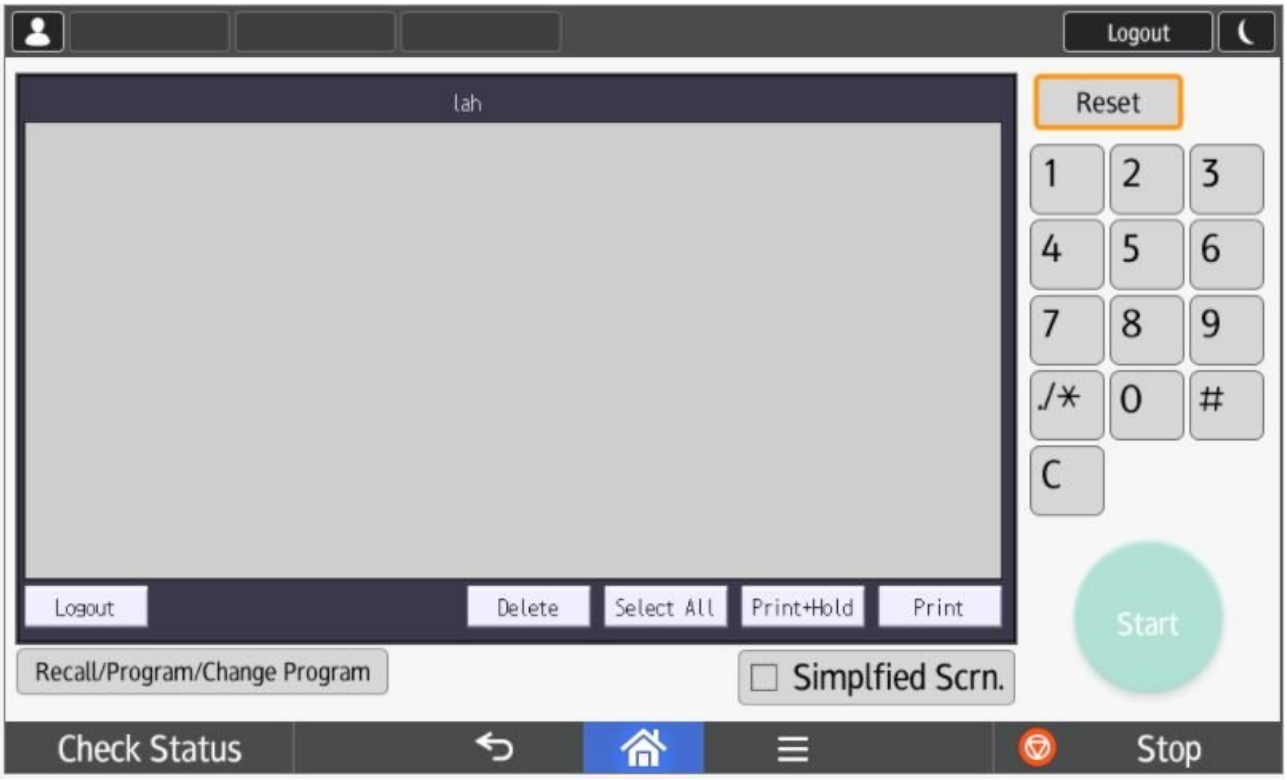
Swipe you card again to log out.

Manual login on the mfp:

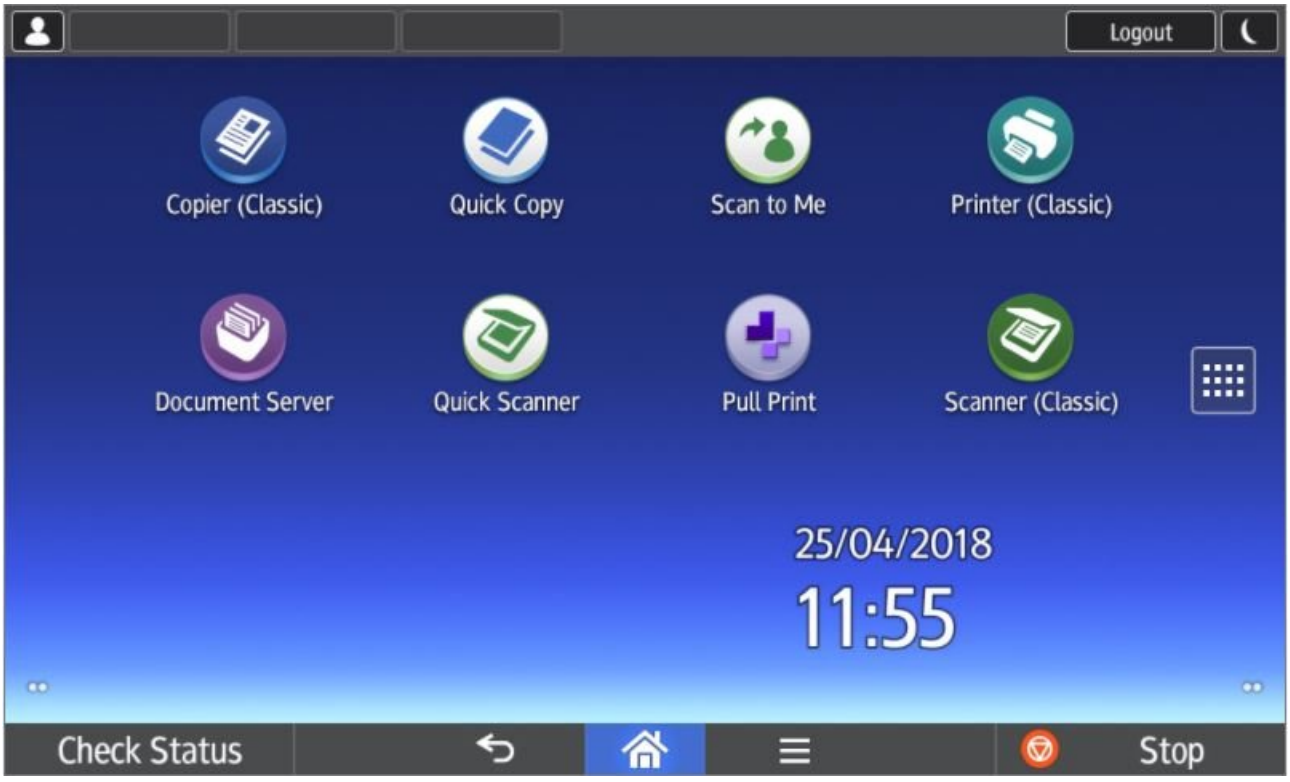
Choose the "Pull Print"-icon and enter your username and password, push "Ok".



Now you can release your printjobs or push the "Home"-button in the bottom for Scan, Copier etc.

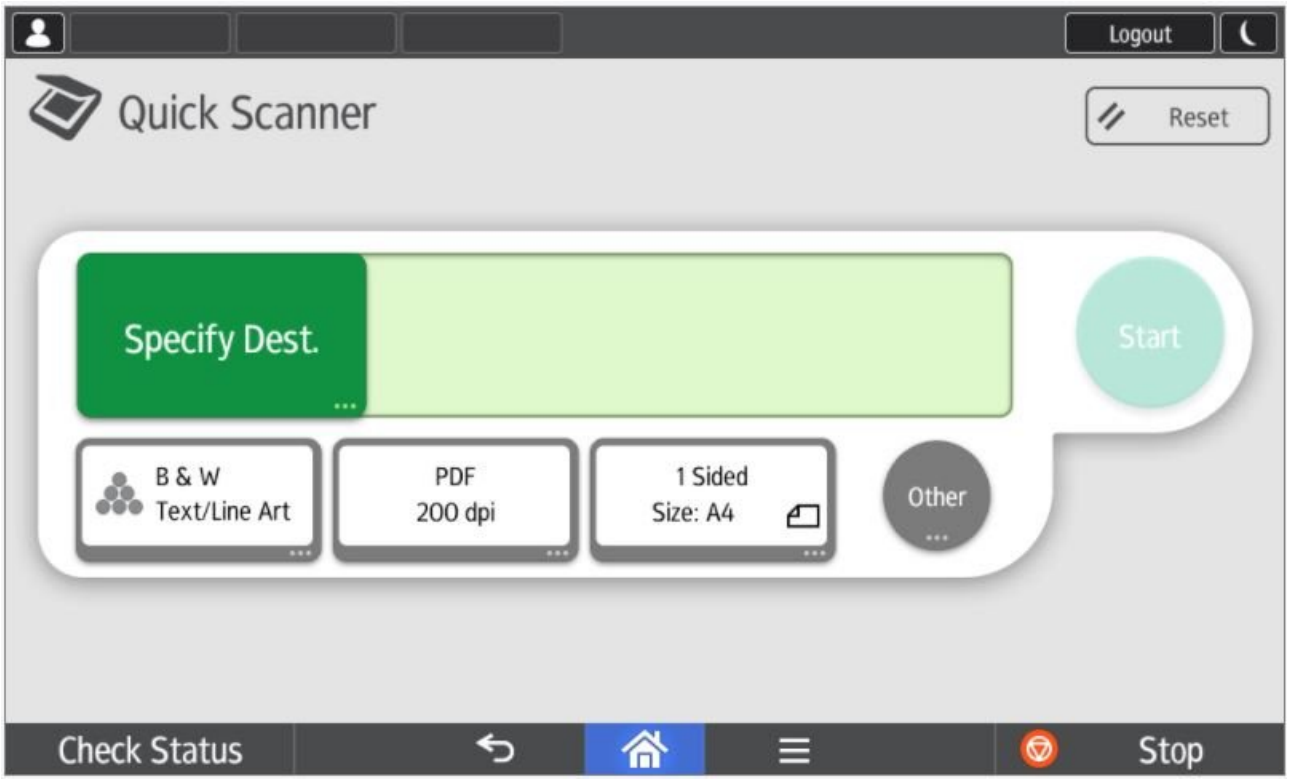


After "Home"-button is pushed you are able to choose the functions you want to use.

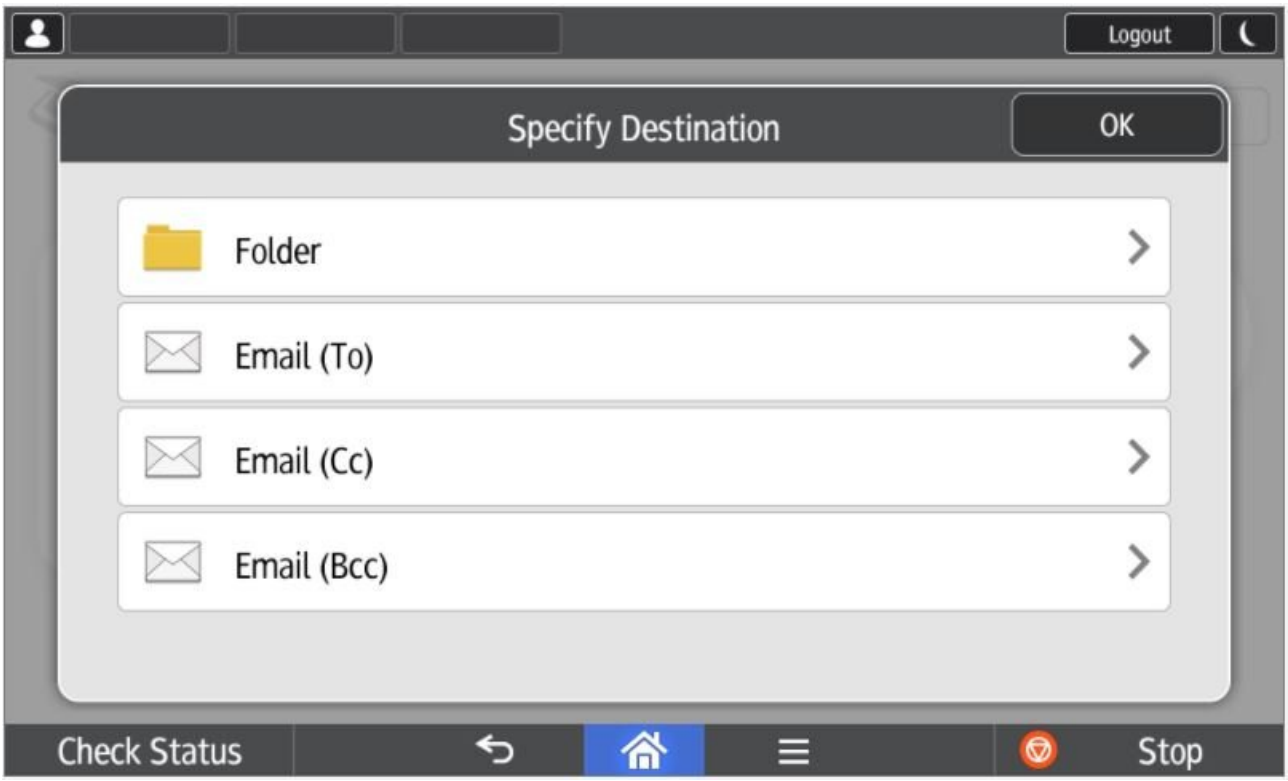


Using the Quick Scanner:

After logging in to the mfp push the "Quick Scanner".

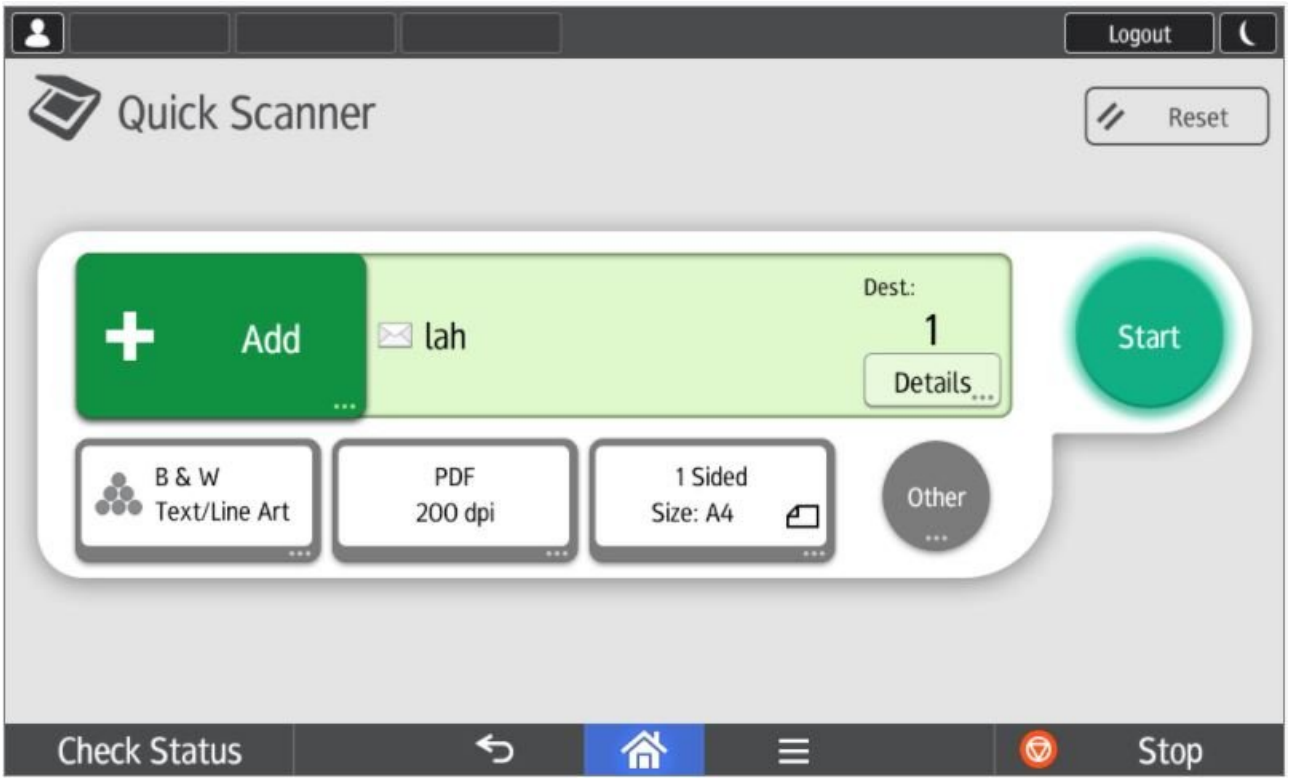


Hit the "Specify dest."-button and choose "Email (To)" in the next view



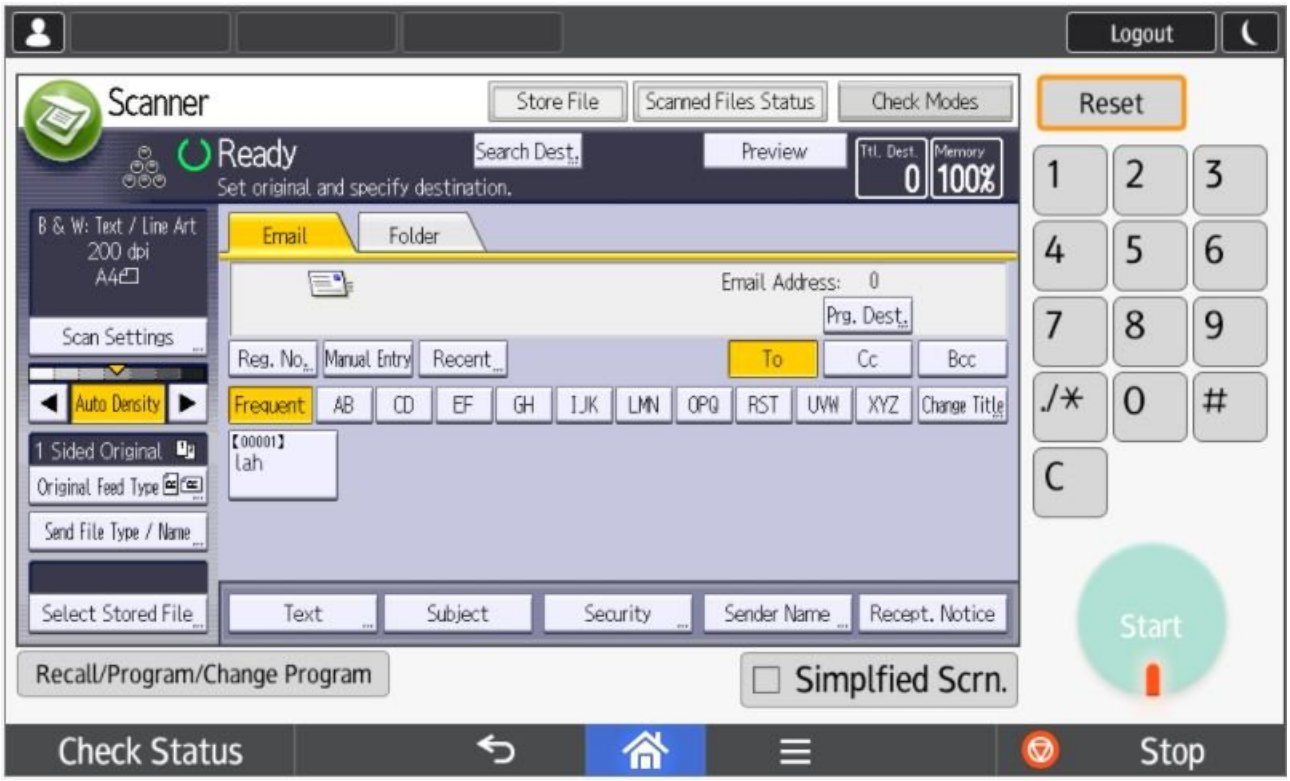
Mark you user/email and push "Previous Scr."

Hit "Ok" and make you scan

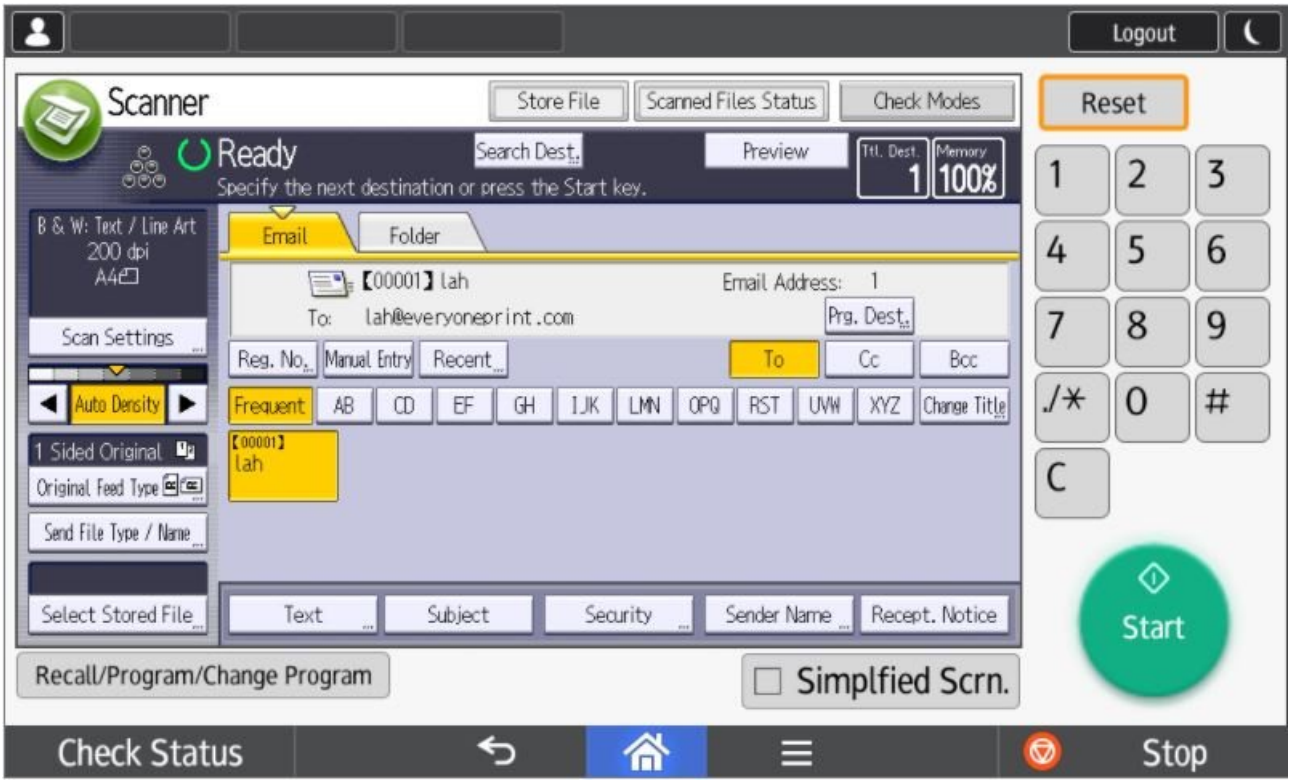


Using the Scanner (Classic):

After logging in to the mfp push the "Scanner (Classic).

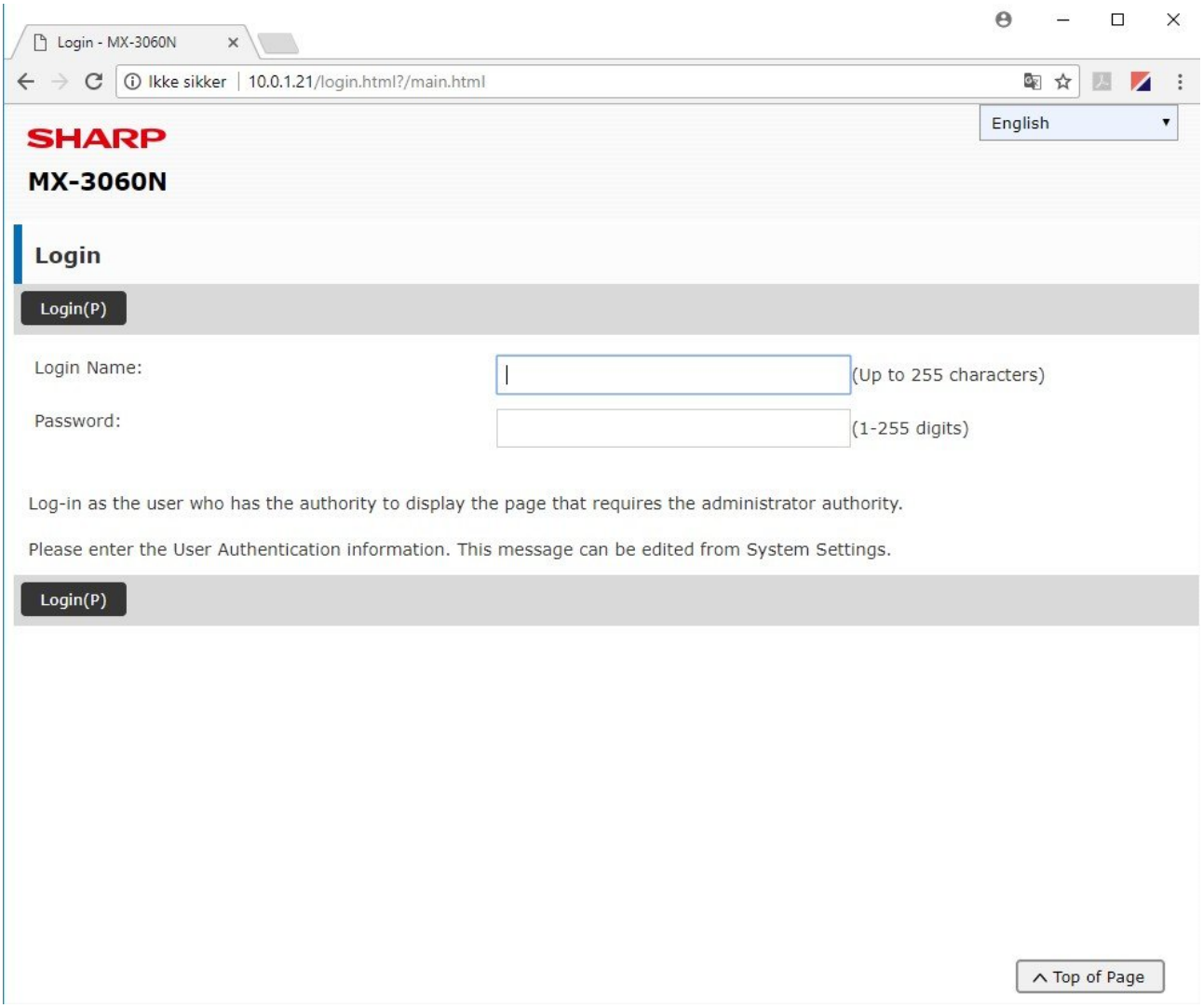


Choose your username and start scanning.

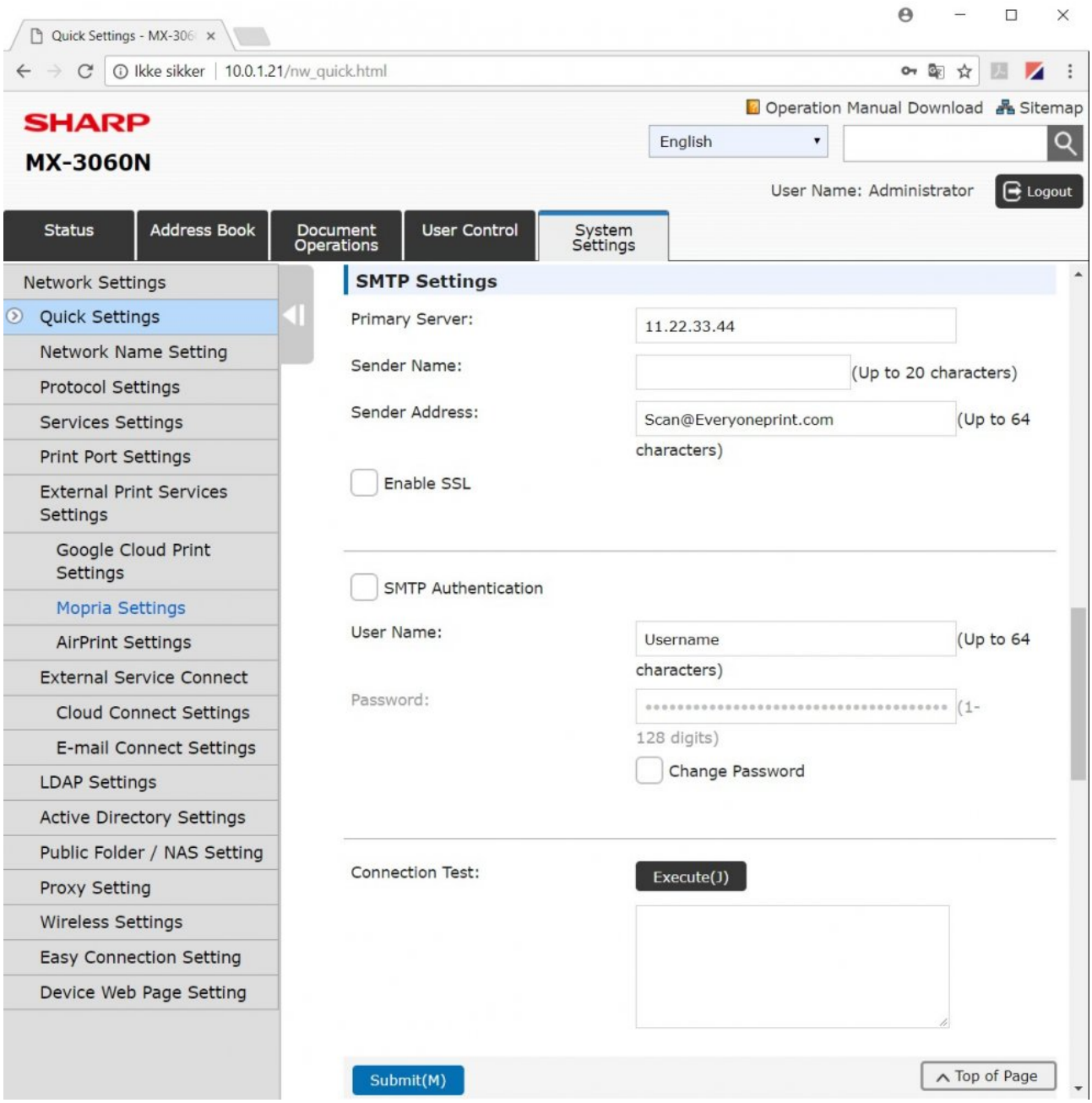


Sharp MFDs

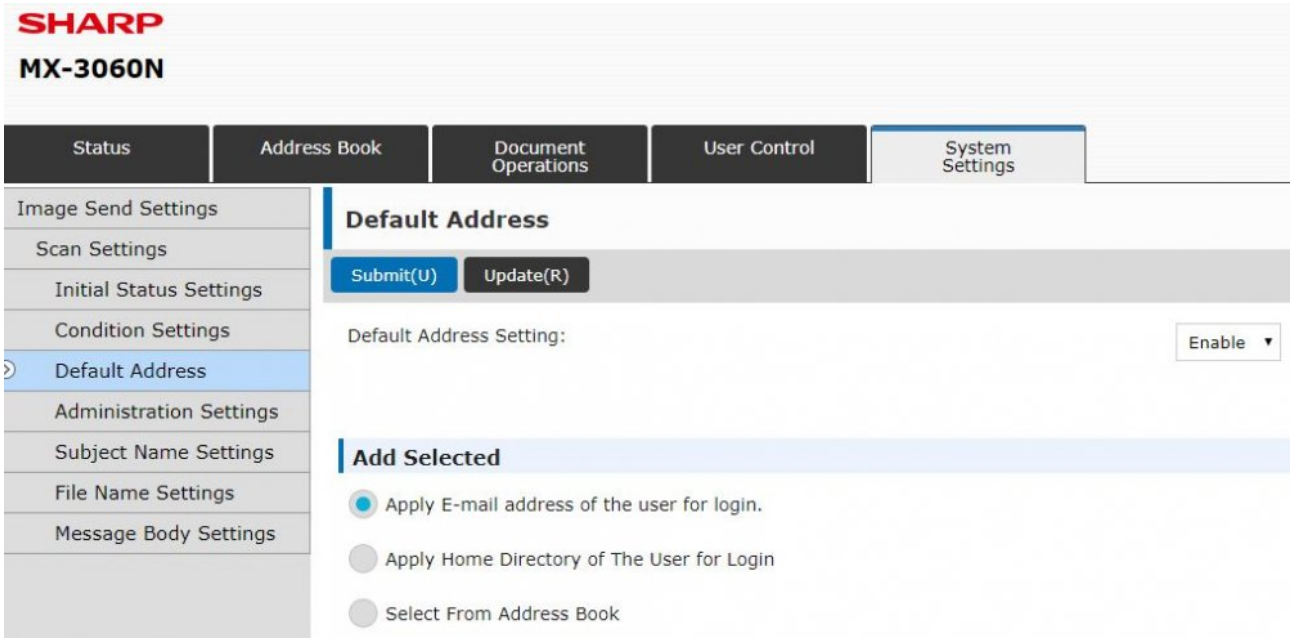
Open printers Webinterface in a browser, type admin as login name and admin as password, if you haven't changed it.



Choose "System Settings" and "Network Settings", and scroll down to "SMTP Settings".
Fill in proper information and choose "Submit".



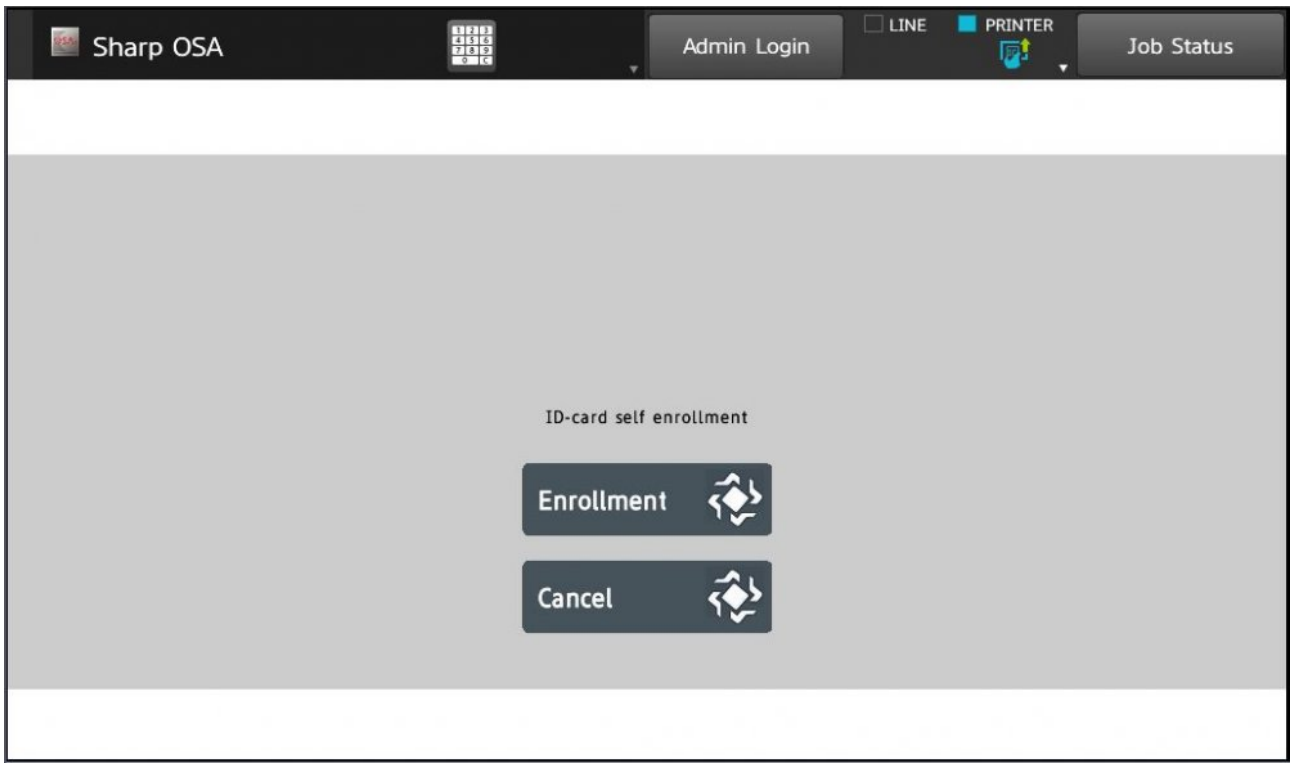
To set in default reciever of the email to the logged in user choose "System Settings", "Image Send Settings", "Scan Settings", "Default Address", enable the function and set a mark in "Apply E-mail address of the user for login" and choose "Submit".



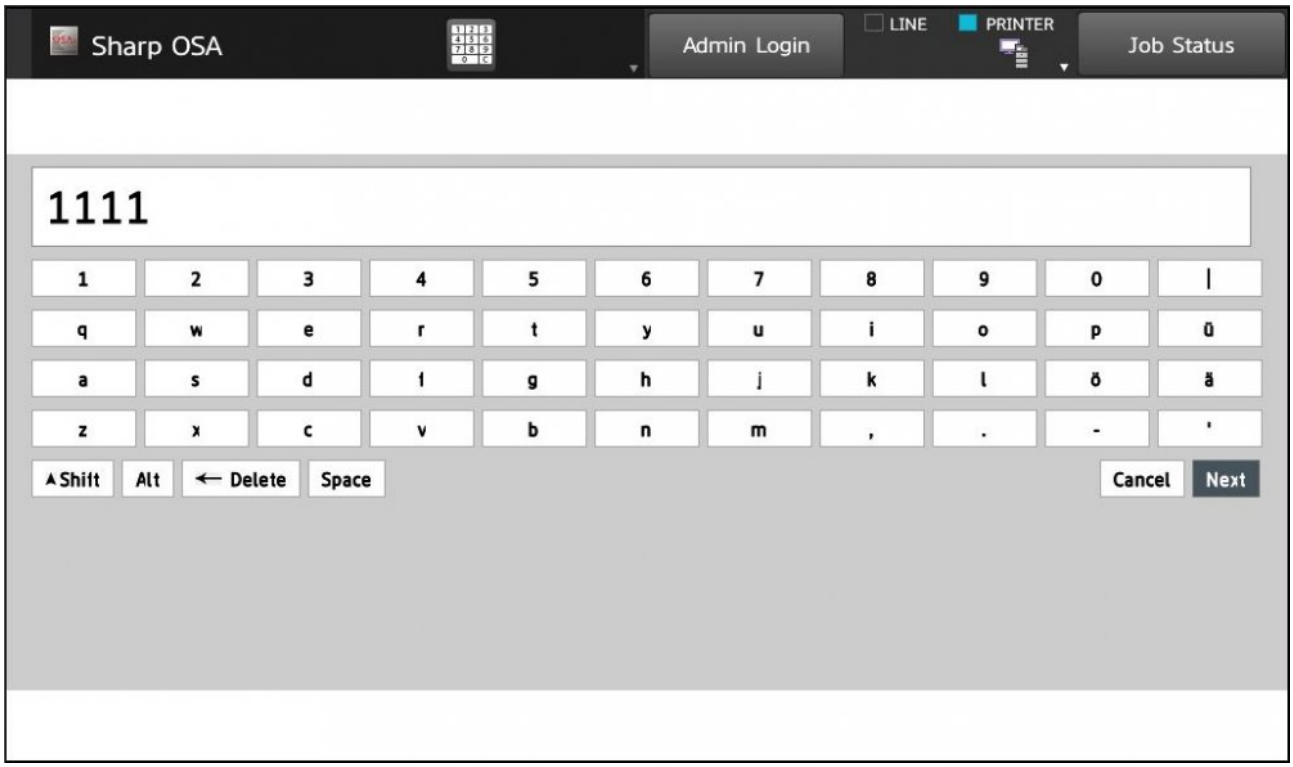
Card Self Enrollment:

Swipe your card over the cardreader.

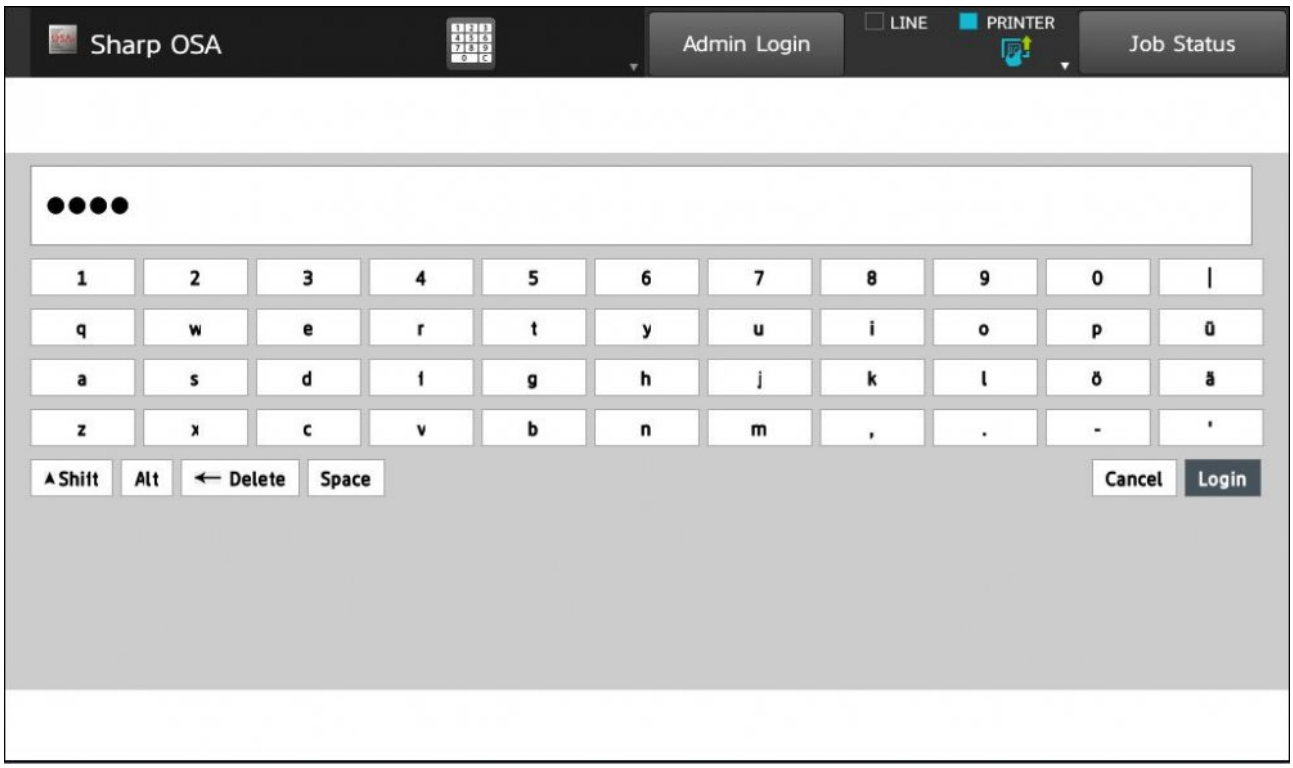
Choose "Enrollment".



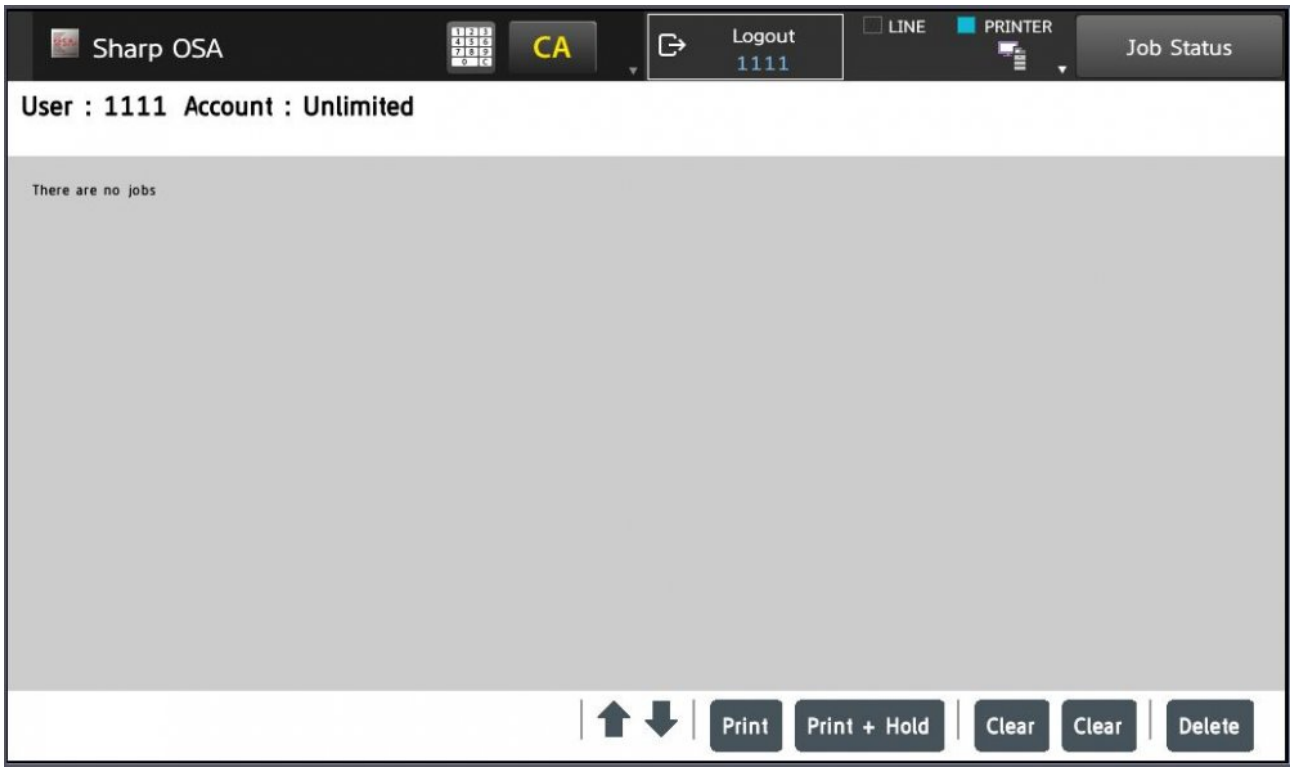
Enter your username.



Enter your password.

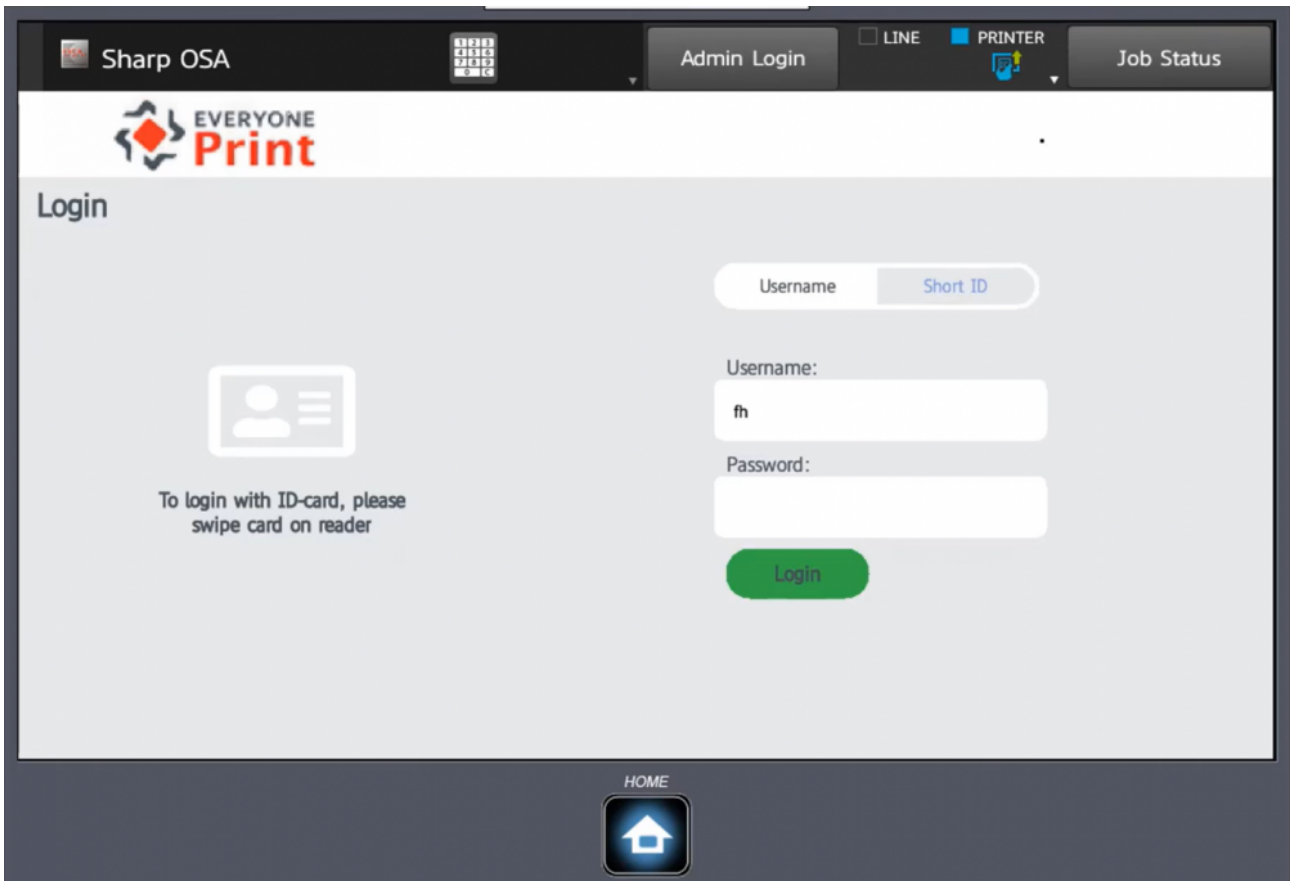


Now you have enrolled your card to your user and you are able to login using the cardreader for releasing printjobs or using other functions at the MFD.

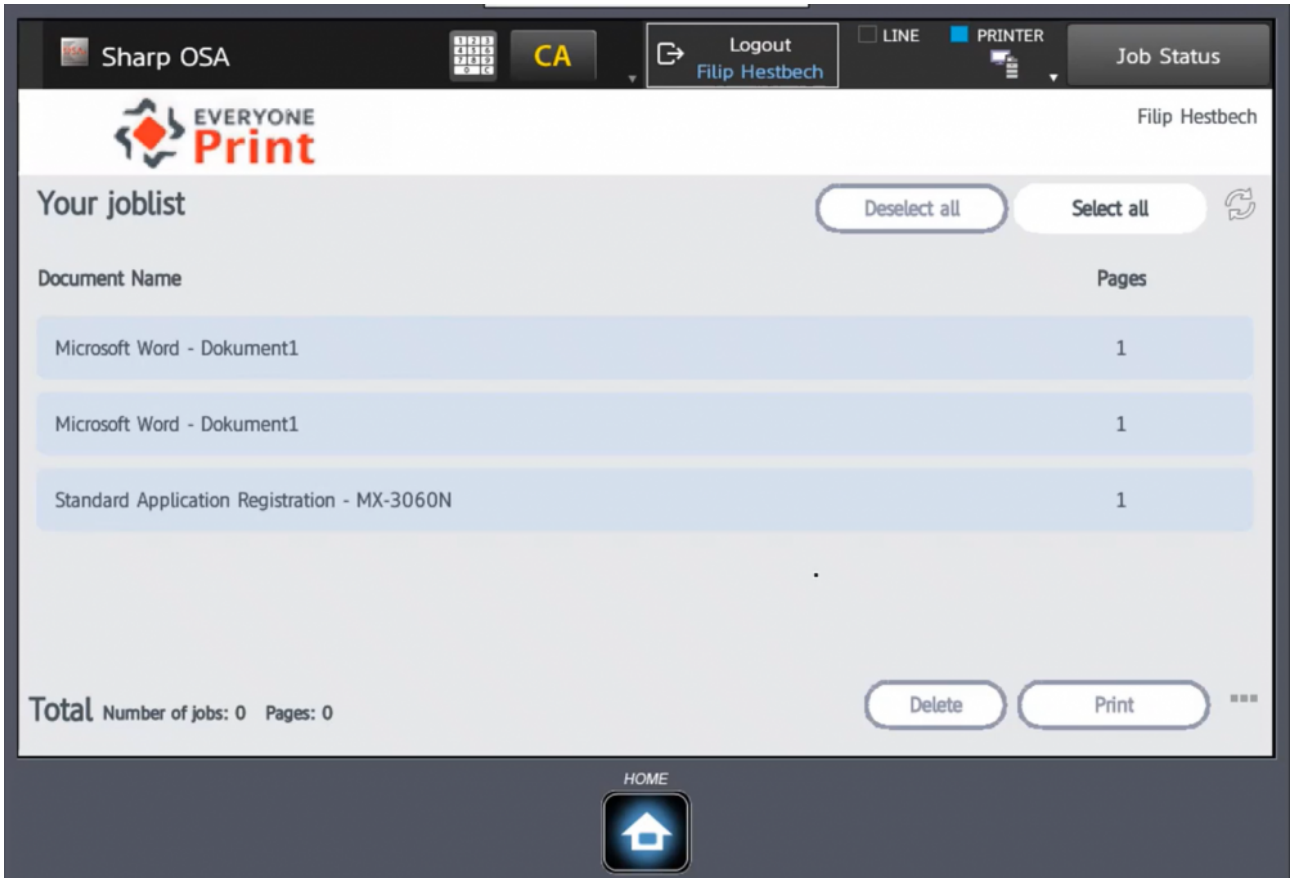


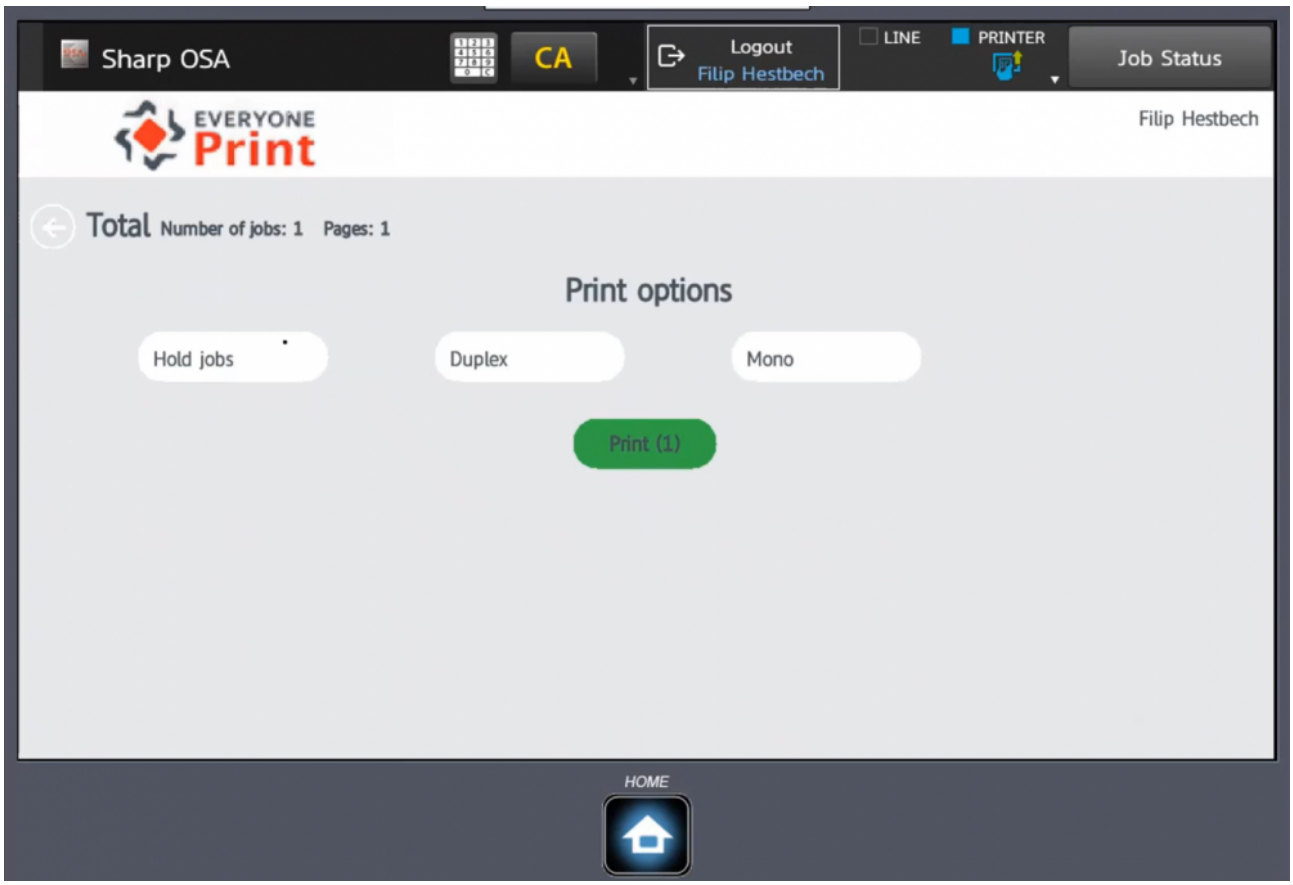
Manual login on the mfp:

Choose the "Short ID"-button or enter your username and password.



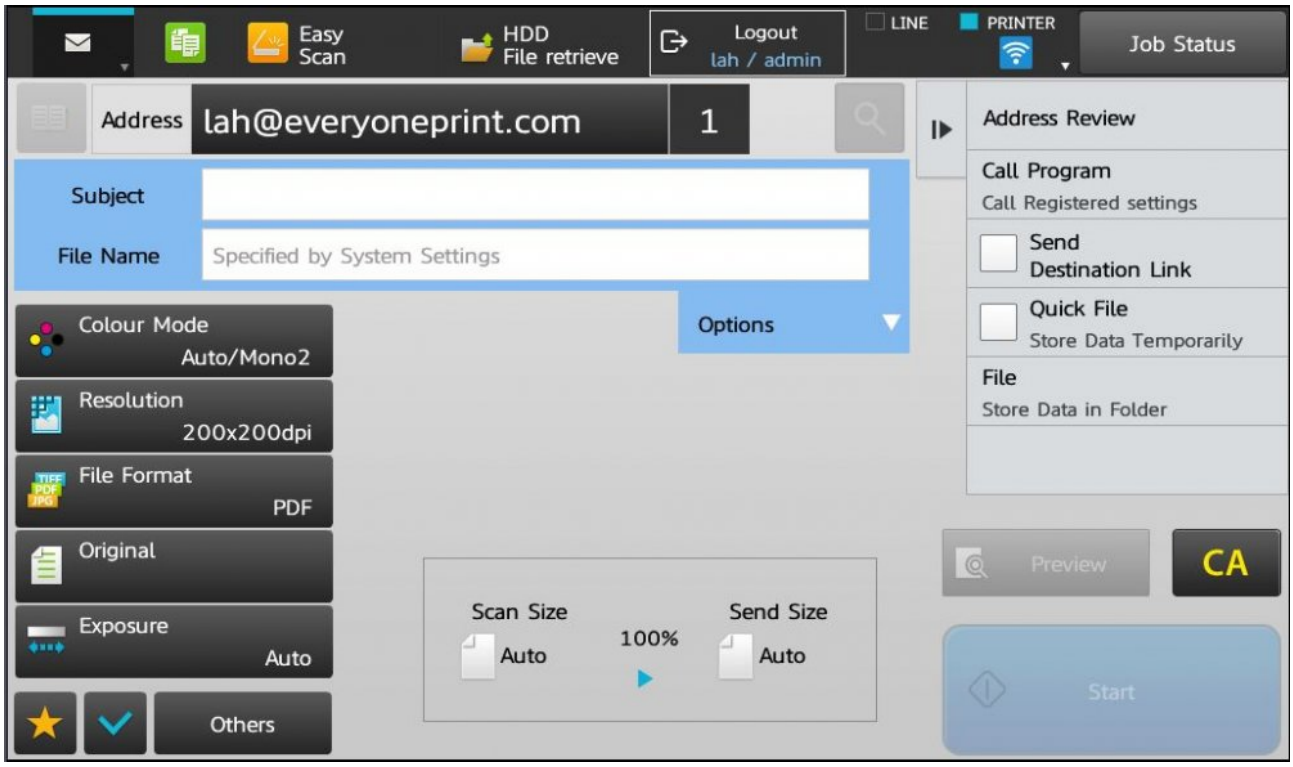
Now you can release your printjobs or adjust the print settings via the three dot menu.





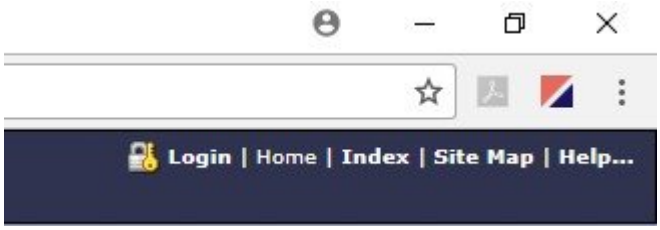
Using the Scan to E-mail function

"Push the "Sharp OSA"-button and choose "E-Mail", sender and recipient is automatilcaly set if above instructions is followed.

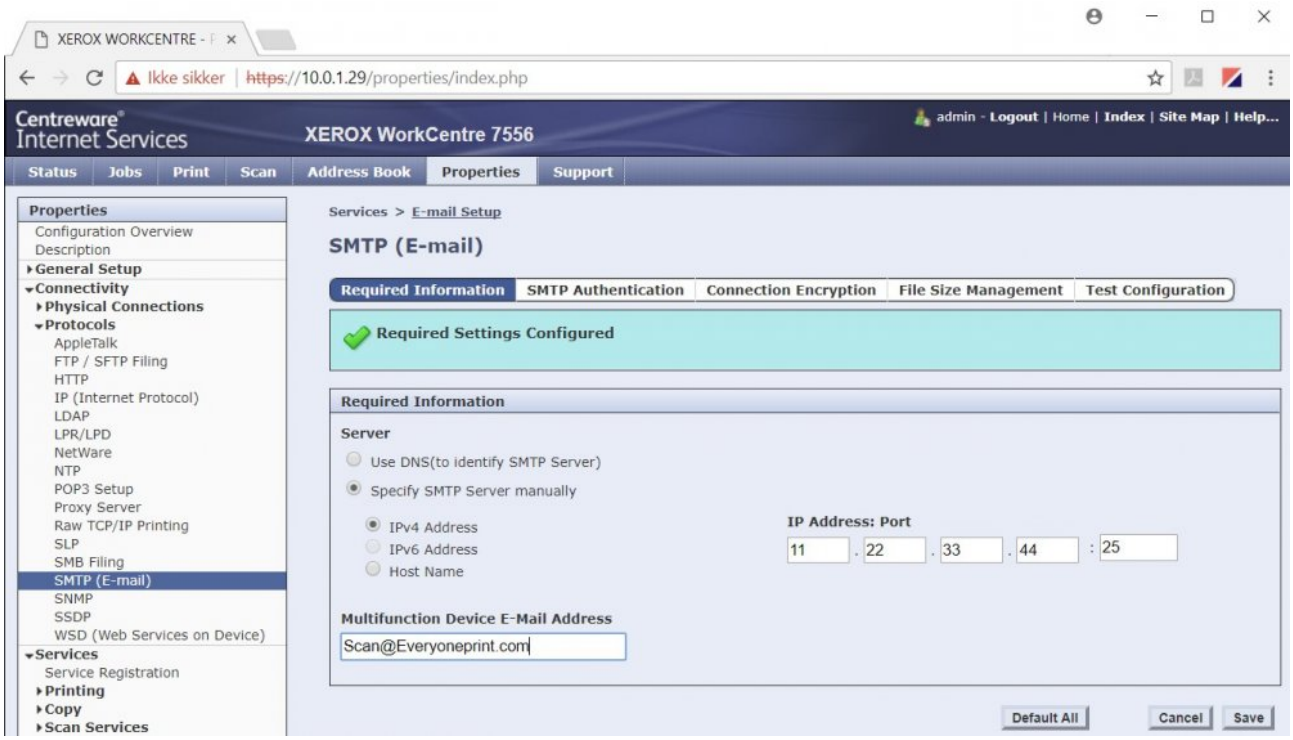


Xerox MFDs

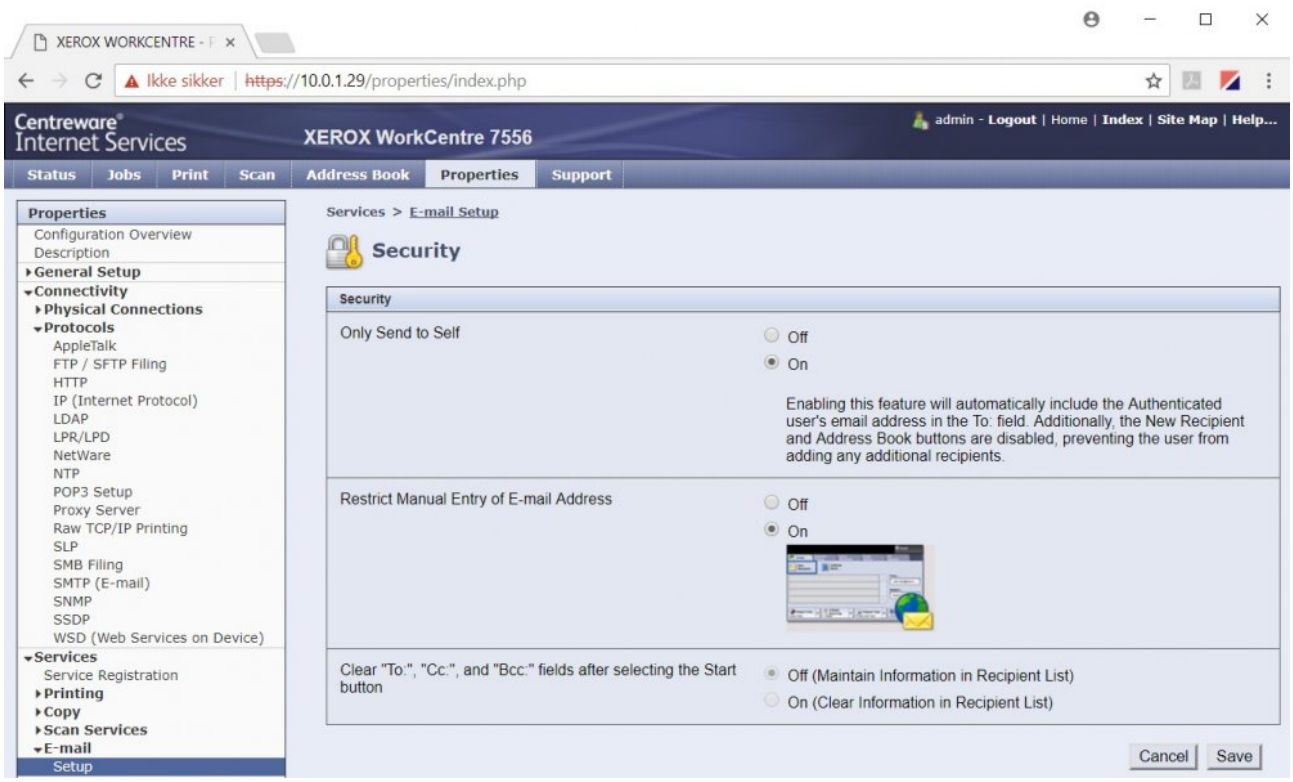
Open printers Webinterface in a browser and choose "Login" at the upper right corner.



Choose "Properties", "Connectivity", "Protocols" and "SMTP (E-mail).
Fill out with proper information and choose "Save"

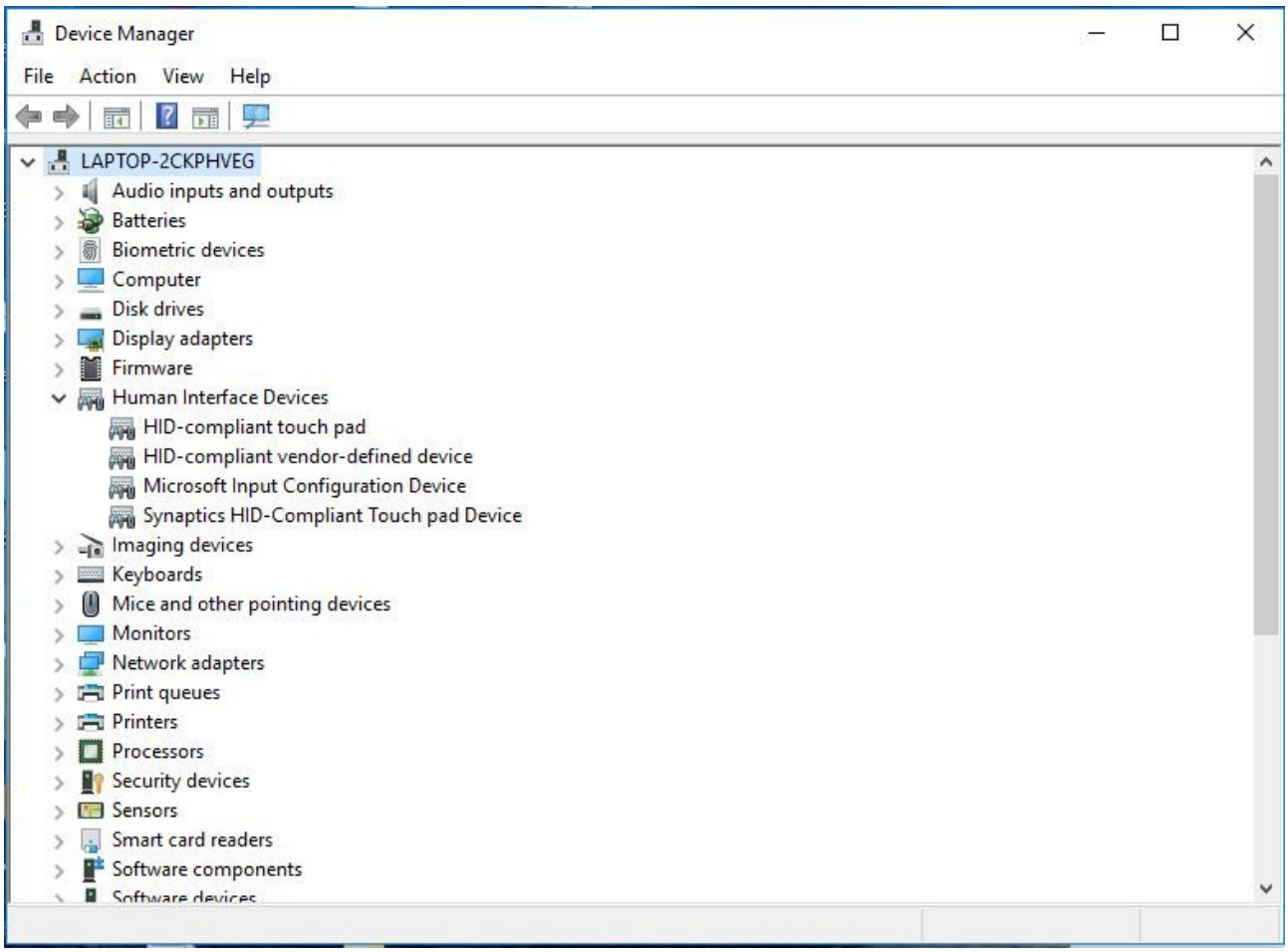


Under "Properties", "Services", "E-mail", Setup" and "Security you can set the logged in users E-mail as default receiver of the scanned document and restrict users access to add other E-mailaddresses.



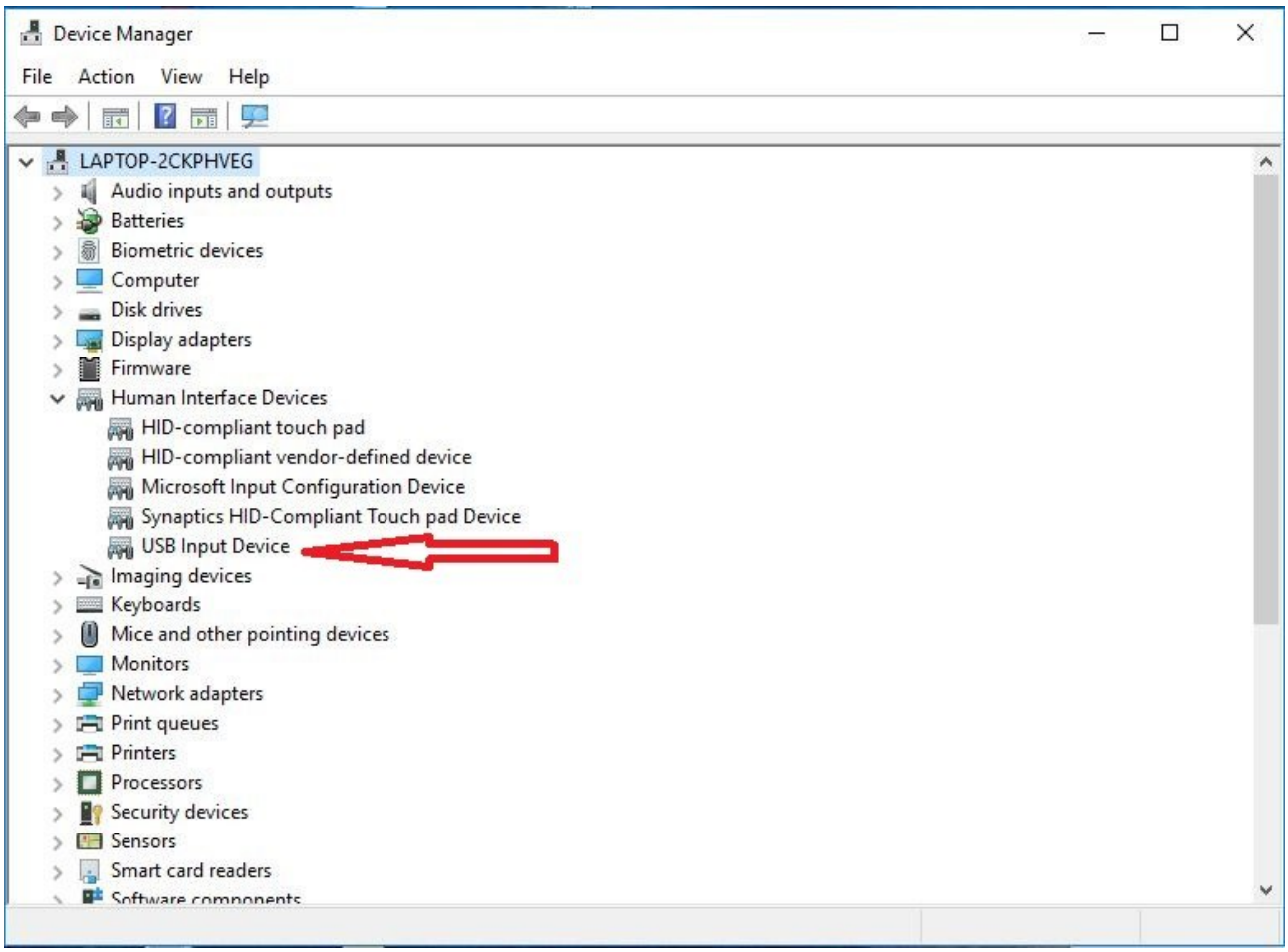
11.2.4 HOW TO CHECK VID AND PID ON CARDREADER

Open up your "Device manager" on your computer and expand "Human Interface Devices".

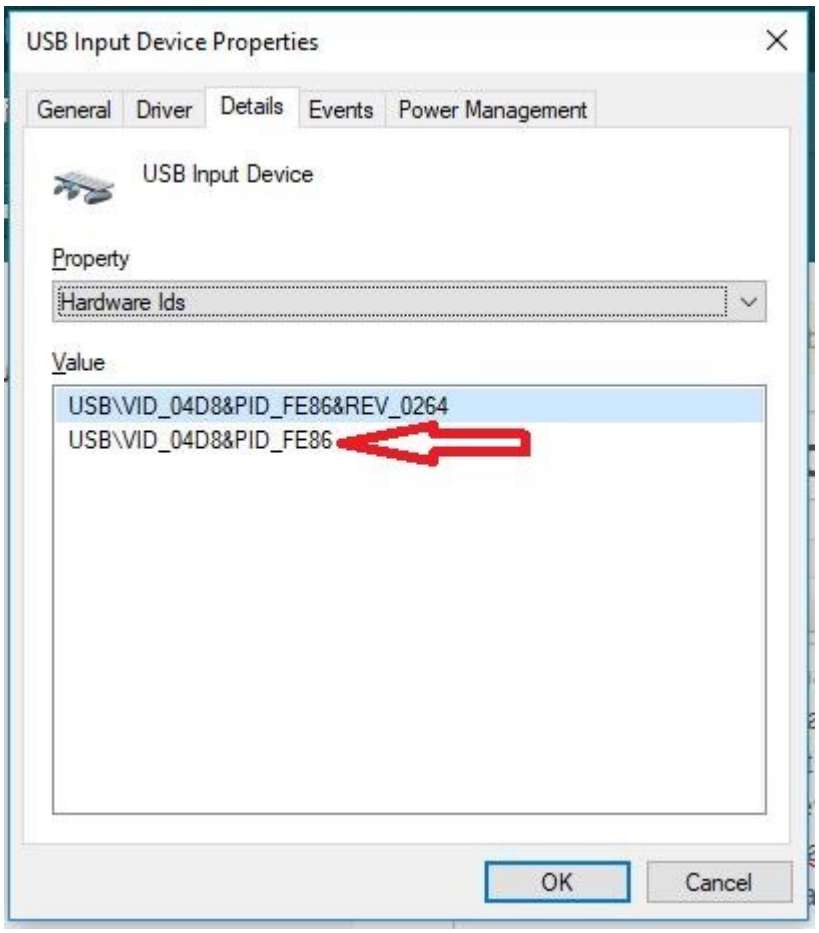


Note which devices are in there and plug the USB-cardreader into a free USB-port on your computer.

Now there will be a new device under "Human Interface Devices", rightclick that device and choose "Properties".



Now choose "Details"-tab and "Hardware ID´s" in the dropdown-menu.

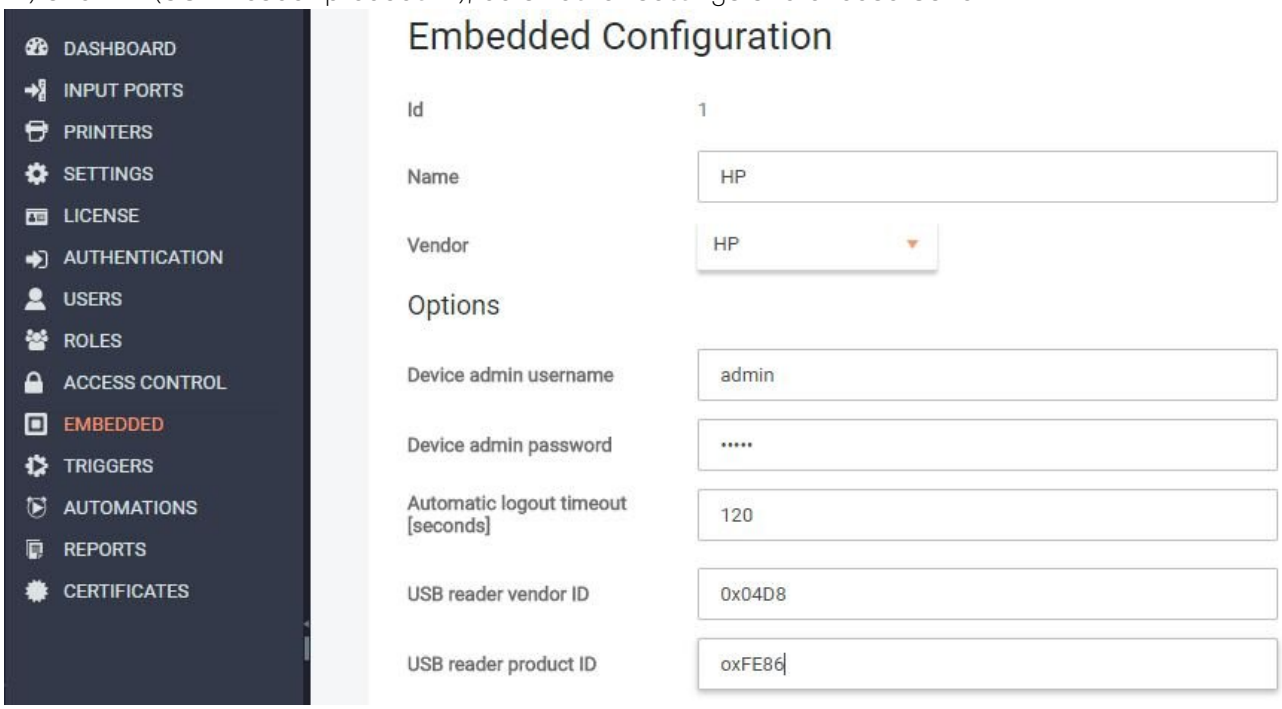


Now you see the VID and the PID, which here are: VID: 04D8 and PID: FE86. Remember when putting in VID and PID to use 0x in front of the value.

Put in VID and PID on HP Embedded

For HP it is necessary to put in VID and PID for the connected Card-Reader when adding the embedded configuiration to the printer. Remember to add 0x in front of the VID and PID
Add or edit an Embedded configuration for HP in SAFEQ Cloud and put in VID (USB Reader vendor

ID) and PID (USB Reader product ID), do all other settings and choose Save.



11.2.5 USE EQUITRAC EMBEDDED CLIENTS WITH SAFEQ CLOUD

For customers with Nuance Equitrac already deployed, or where customers wish to utilize the Equitrac embedded client front-ends for pull print and integration to advanced scanning solutions (such as Nuance AutoStore or eCopy ShareScan), but wish to move their print infrastructure away from Windows print servers.

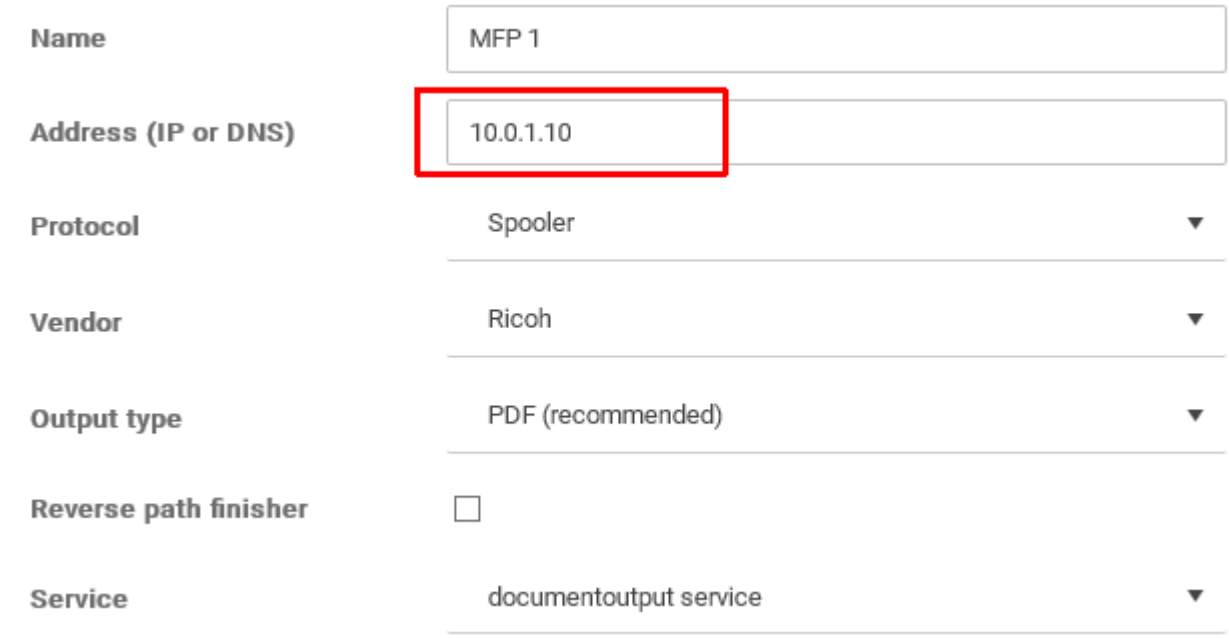
Connect Equitrac to YSoft SAFEQ Cloud, for Equitrac embedded front end clients to retrieve, display and release jobs stored for a user in SAFEQ Cloud.

Prerequisites:

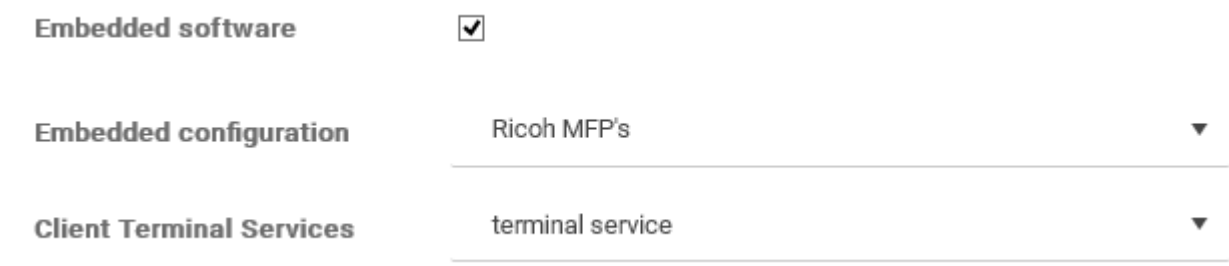
- Uses Equitrac's External Print Queue functionality (configuration takes ~2 minutes per device)
- Requires an Equitrac External Data Connector license on all Equitrac servers where functionality is needed
  - Nuance part number: EQ5DC001-3PB
  - Description EO5/EE5: External Data Connector 3Y
- An YSoft SAFEQ Cloud output port configured with Embedded checked (and valid license) for each device in Equitrac

Configure SAFEQ Cloud

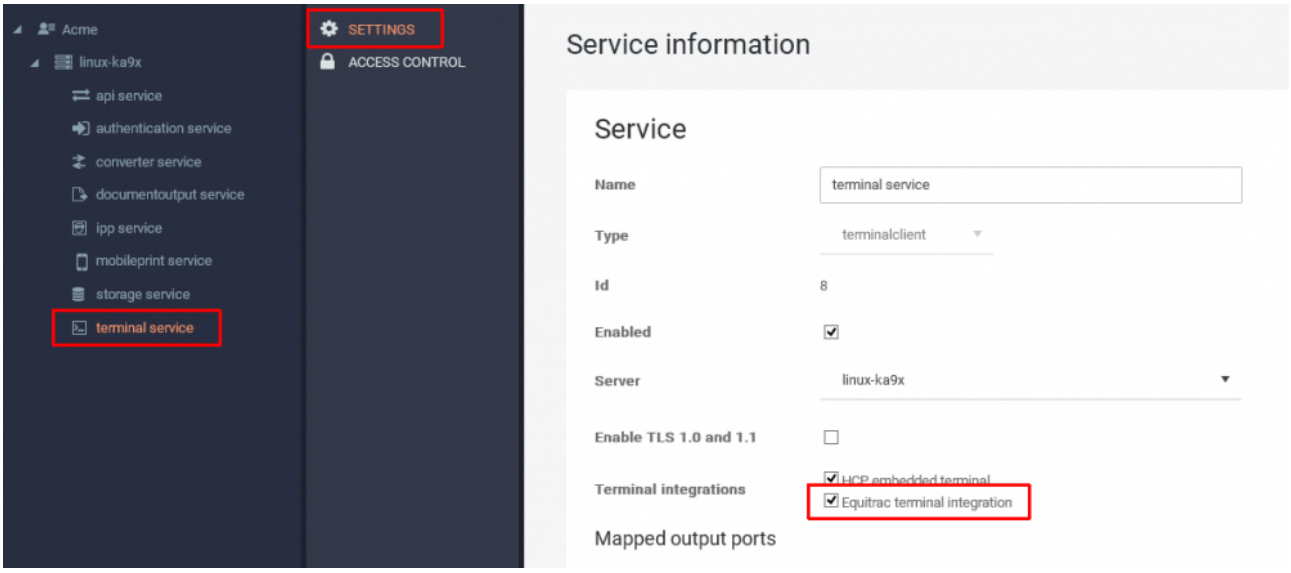
Configure an output port in SAFEQ Cloud with the hostname, DNS or IP address of the printer, matching the hostname, DNS or IP address used in Equitrac



Make sure Embedded is checked, and the output port has a valid Embedded configuration and terminal service selected.



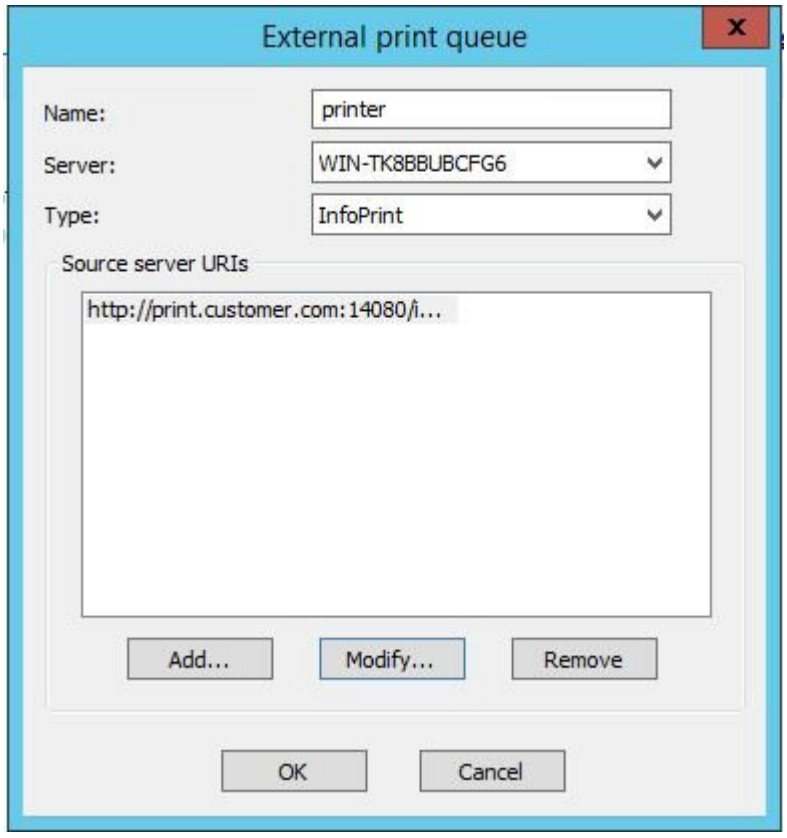
Go to the Terminal Service to which the Equitrac server(s) will communicate and enable the Equitrac embedded integration



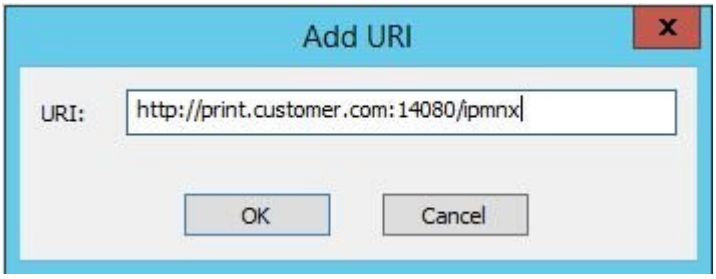
Configure Equitrac

For each print device in Equitrac, enable the External Print Queue, by right-click on the print queue and choose Add external print queue device.

Enter a name, just an internal identifier, choose the Equitrac server where this device is active, and choose the type InfoPrint.



In *Source server URI's* add the URL to the SAFEQ Cloud server gateway running the terminal service, in the format http(s):// `SAFEQ Cloud-account-domain-name` : `port` /ipmnx



`SAFEQ Cloud-account-domain-name` is a valid DNS pointing to the SAFEQ Cloud server where terminal service is running and a domain added to the accounts domains under Settings

`port` is either 14080 for https (SSL) or 14081 for https (non-SSL)

11.2.6 CONTAINERS AND ACCESS CONTROLS

Containers were introduced in SAFEQ Cloud version 2.4 to facilitate the separation of views depending on the customer requirements.

There are multiple ways of using grouping in a container. The following two examples describe the most common implementation of containers in customer setups.

Example 1 :
The customer needs two gateways installed under two different accounts separated from each other. To fulfill this need, you can create two containers, each containing an account and its gateway, therefore, operating separately without any gateway interfering with the other.

Example 2 :

The customer has:

- a single gateway
- two different departments in two different locations
- a need for multiple users to access the view from different authentication providers while using strict domain validation (the users must be allowed to login only against the domain name)

Access control does not apply to gateways and their mapped services. For example, in the Terminal Client service's details, you can map it to any printer from any container or account root's node, regardless of the defined access control.

- Create containers
- Example 1
- Example 2

Creating containers

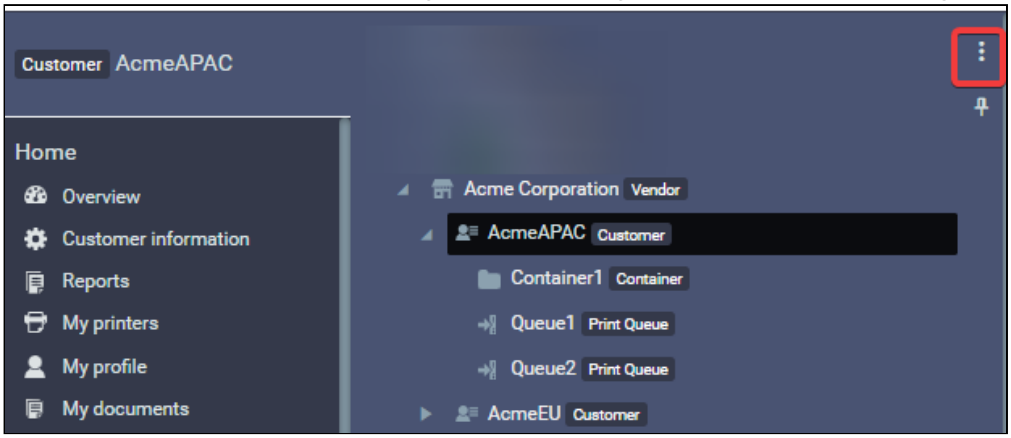
To create a new container, perform the following steps:

1. Click **Create new...** at the top of the SAFEQ Cloud Web UI.
2. From the drop-down menu, select **Container**.
3. Enter the following information:
   a. Name: Visible name of the container
   b. Domain: A DNS name by which this container can be accessed (Optional). The domain name can contain letters, numbers, hyphens, and periods. Any part of the domain name (separated by a period) should begin and end with a letter or a number.
   c. Default location: This location is used as default for all printers and print queues.

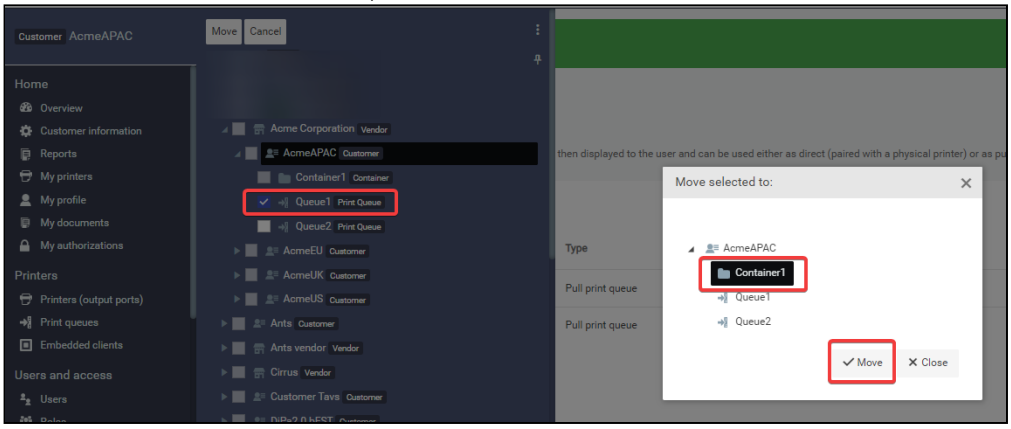
4. Click **Save**.

Moving existing configuration items into containers

1. Click the three dots at the top-right of the navigation tree. Then click **Organize tree**.



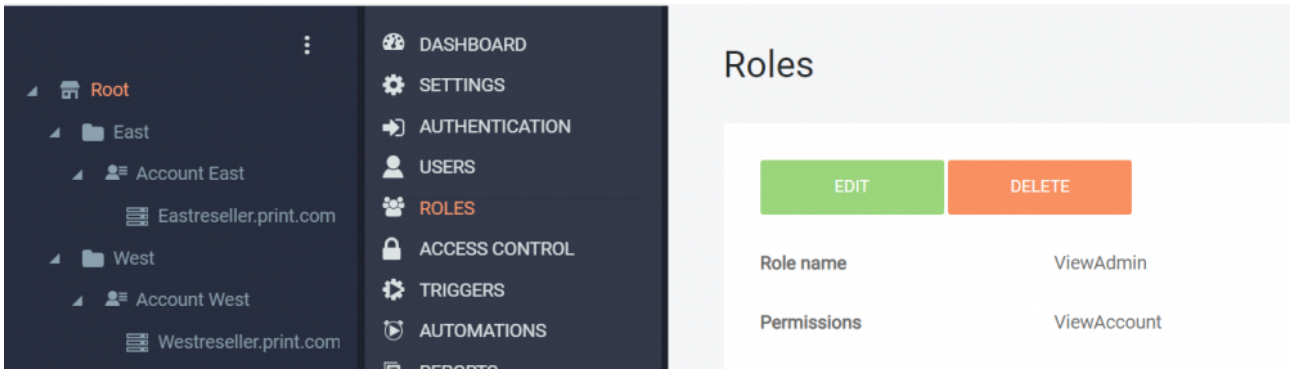
2. Select the item that you wish to move.
3. Select the container where you want to move it. Click **Move**.



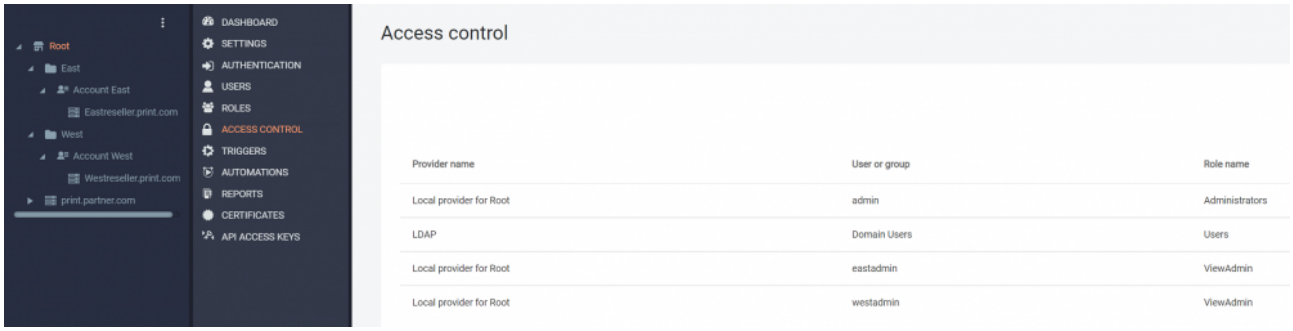
Permissions on Containers – Example 1

In this example each container has an active account under it (Account East & Account West)

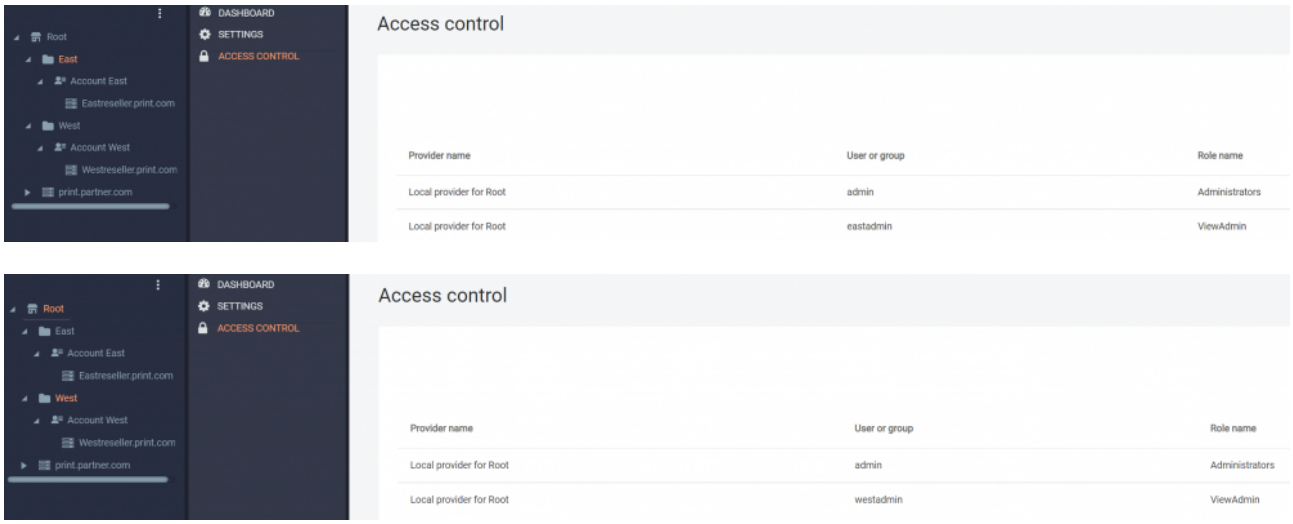
Create a new role in the "Roles" section, add all the permissions required by the user on the containers. Existing roles namely, admin, users, reporting, support can also be reused. (How to create/modify roles has been explained in section Roles)



On the root node, make an access control entry for each of the users/groups for each container. Make sure to delete all the access controls that are not required, as the containers may have all the inherited permissions from the root under which they were created. (Remember : If you delete the access control entry for the local provider for root's admin user on a container, that container will not be visible under the root tree for the admin user, as the admin rights will have been taken away)



Go to the container and hit "Access controls". Add the access control entry required for this container



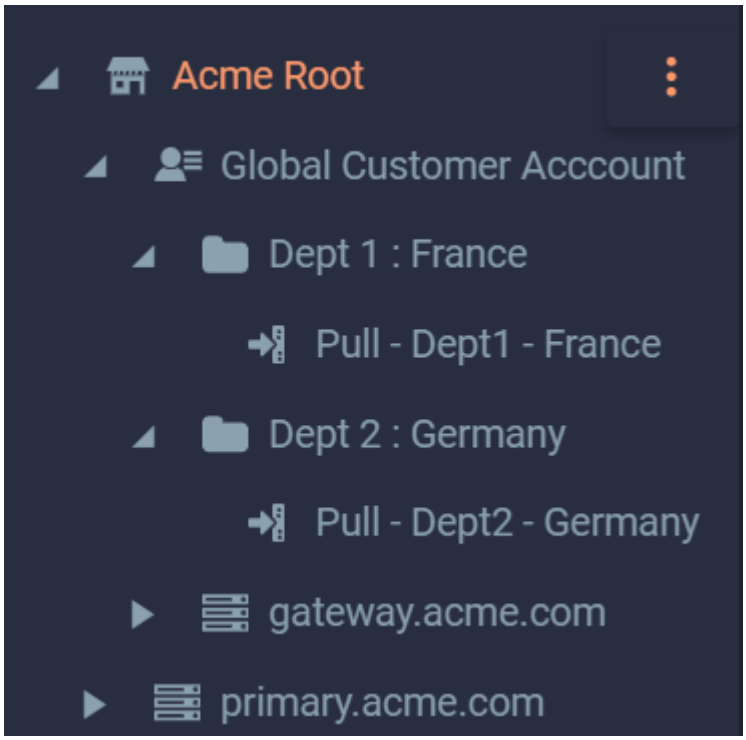
Now, go to the domain of the container, in this case Westreseller.print.com/Eastreseller.print.com. Login into the UI with the required users, only the right users have the access to the containers. Example : "eastadmin" will only be able to see the contents of the container "East" and "westadmin" will only see the contents of the container "West"

Permissions on Containers – Example 2

In this example, we will consider having an account with a gateway installed on it, when the customer requires a user to be authenticated only against the domain used for authentication provider (Strict domain validation) and also a separation of view pertaining to showing of different containers and its content to different users

Below is what the hierarchy looks like, there can exist a configuration similar to this,

Account name – "Global Customer Account" and strict domain validation is enabled (Go to the Account —> Settings —> Edit —> Strict domain validation enable)
Gateway domain name – "gateway.acme.com"
Container 1 – "Dept 1 : France" , domain name – "france.dept1.acme.com"
Container 2 – "Dept 2 : Germany", domain name – "germany.dept2.acme.com"



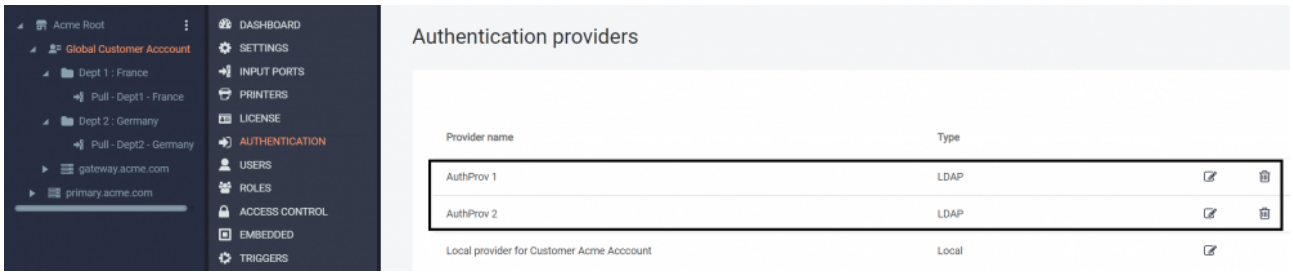
Each department can use its own authentication provider
Example
1. Name – "AuthProv 1", domain name – "dept1.acme.com", used by "Dept 1 : France"
2. Name – "AuthProv 2", domain name – "dept2.acme.com", used by "Dept 2 : Germany"

The goals to be achieved,
1. Users must be able to login into the gateway
Example :
a. The user "test1@dept1.acme.com" should be able to see only the content of container "Dept 1 : France" with the Account as the root.
b. The user "test1@dept2.acme.com" should be able to see only the content of container "Dept 2 : Germany" with the Account as the root.
2. A user "test1@dept1.acme.com" must be able to login into the container "Dept 1 : France" and see the content of the container with Container as the root
3. A user "test1@dept2.acme.com" must be able to login into the container "Dept 2 : Germany" and see the content of the container with Container as the root

The following steps should be followed to achieve the goals above,

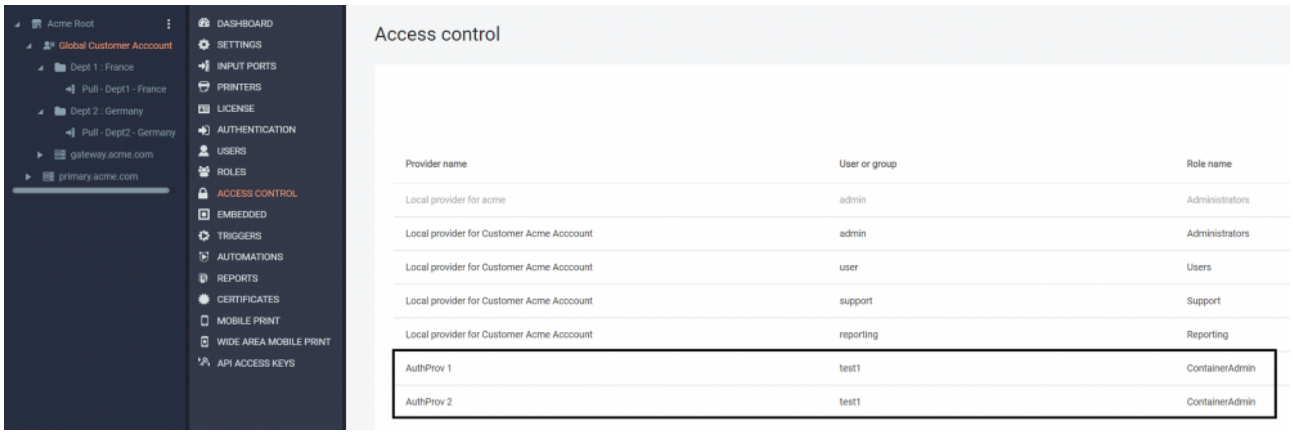
1. Login into the SAFEQ Cloud web UI as an admin user

2. Go to Account (Global Customer Account) —> Authentication —> Add Authentication Provider
Make 2 new authentication providers which will be used on both the containers
Example : AuthProv 1 —> dept1.acme.com & AuthProv 2 —> dept2.acme.com

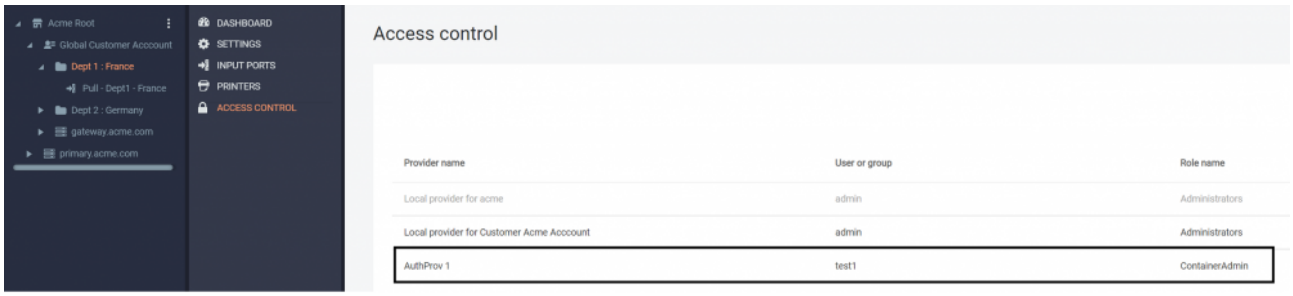


> Please note a new role “ContainerAdmin” was created on the Account to grant the users appropriate permissions. Existing “Roles” can also be reused. Refer to Roles and Access Controls to know more

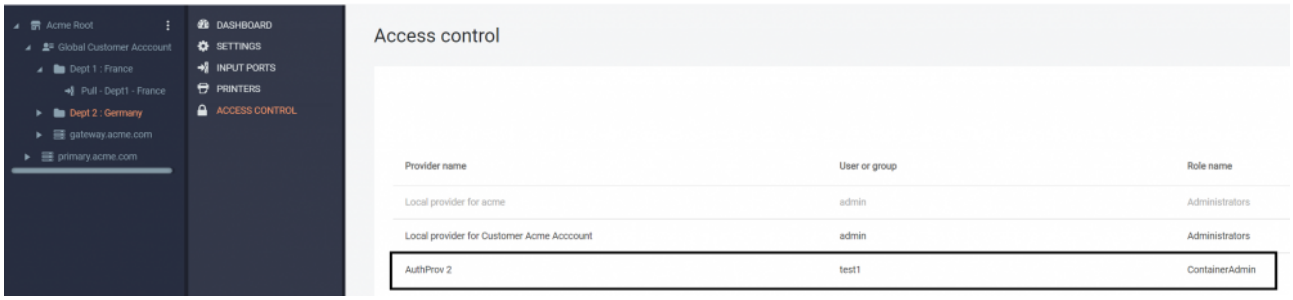
3. Go to Account —> Access Controls —> Add
Add access control for the authentication providers on the Account (Global Customer Account)



3. Go to the Container "Dept 1 : France" —> Access Controls —> Add
Add access control for one authentication provider which is required (dept1.acme.com). The unwanted access controls could be deleted but only after a new entry is added



4. Go to the Container "Dept 2 : Germany" —> Access Controls —> Add
Add access control for one authentication provider which is required (dept2.acme.com)

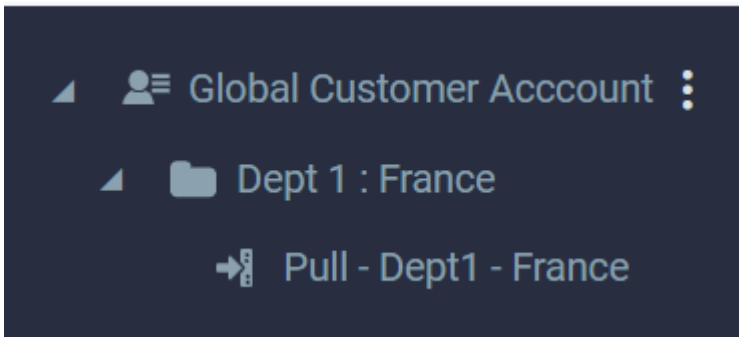


All the settings have been been set into place. It's time to see it in action.

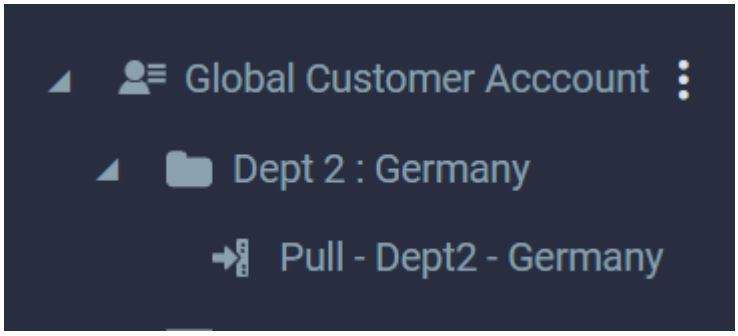
> **Logging in using only the username as “test1” and the password will fail as strict domain validation is enabled**

1. Logging in onto the Account (gateway.acme.com)

Try to login with "test1@dept1.acme.com". The user should be able to see only the contents under the "Dept 1 : France" container



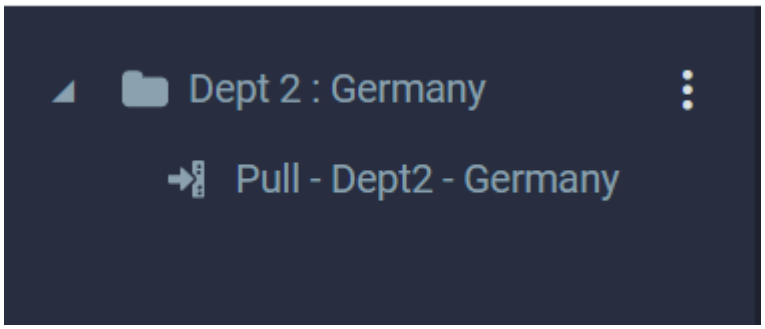
Similarly, if the user "test1@dept2.acme.com" tries to login onto the gateway it should be able to see the contents under the container "Dept 2 : Germany"



2. Logging in onto the Containers

Try to login onto the container "Dept 1 : France" (france.dept1.acme.com) using test1@dept1.acme.com (Only the content of the container will be shown)

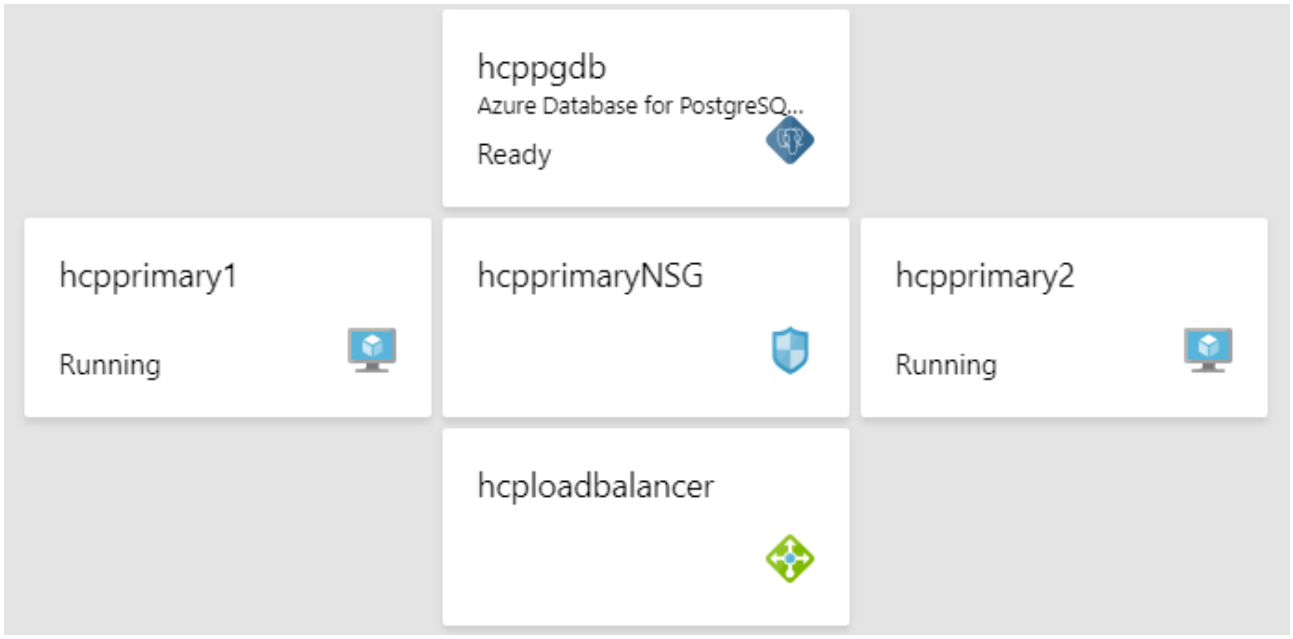
3. Try to login onto the container "Dept 2 : Germany" (germany.dept2.acme.com) using test1@dept2.acme.com



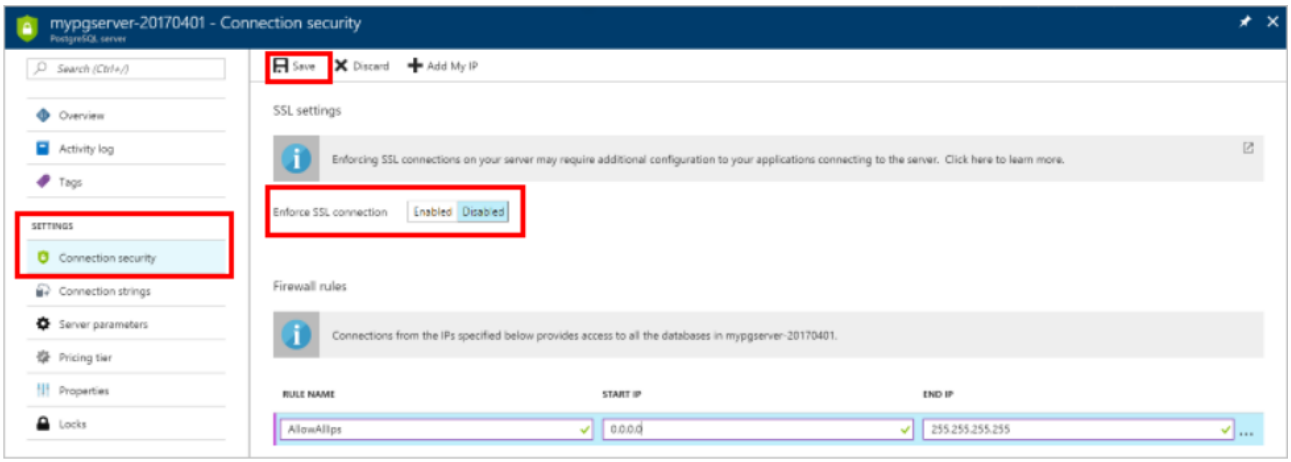
11.2.7 CONNECT TO AZURE SSL ENABLED POSTGRESQL DATABASE

Setting up SAFEQ Cloud solution within Azure cloud needs some security. By default, Azure SAFEQ Cloud servers need to connect to external Azure PostgreSQL (ver. 10.0) database. Azure PostgreSQL server can run as IaaS or PaaS mode and enabling SSL in the database would require some small steps to follow. Below are the steps to follow:

1. Consider the clustered architecture for SAFEQ Cloud where 2 SAFEQ Cloud application servers are running behind an Azure load balancer and connecting to an Azure PostgreSQL PaaS database. The entire environment is been secured via Azure Network Security Group



2. Enable SSL Enabled option in Azure PostgreSQL database from Azure Portal



3. Download the certificate file from the Certificate Authority (CA). For Azure, you can download from here: https://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt

If Customer has their own CA, download the certificate from their verified Certificate Authority.

4. Place the certificate file within primary SAFEQ Cloud application server. It needs to be compiled using OpenSSL libraries which will create the Root certificate at the very end. Remember to put this root certificate within all SAFEQ Cloud application servers across the SAFEQ Cloud application server cluster.

5. Go to primary SAFEQ Cloud server. Create a temporary folder named 'cert' within /opt/safeqcloud/conf:

```
[user@server]$ cd /opt/safeqcloud/conf
[user@server]$ sudo mkdir cert
```

6. Download OpenSSL in the cert directory. In general, it is by default been installed in the OS. If not, you can download it by the following command:

```
sudo yum install openssl
```

7. To confirm that you've successfully installed OpenSSL on your system, run the following command and check to make sure you get the same output:

```
[user@server]$ /opt/safeqcloud/conf/cert/openssl version
OpenSSL 1.0.2k-fips  26 Jan 2017
```

8. The downloaded Root CA file is in encrypted format. Use OpenSSL to decode the certificate file. To do so, run this OpenSSL command (Remember to put the BalitimoreCyberTrustRoot.crt file in the same directory):

```
openssl x509 -inform DER -in BaltimoreCyberTrustRoot.crt -text -out root.crt
```

This will create a root.crt file within the same location.

9. Use the root.crt file created and the sslmode=verify-ca or sslmode=verify-full option. Go to pgsql directory within primary SAFEQ Cloud server and run the below command:

```
./psql "sslmode=verify-ca sslrootcert=/opt/safeqcloud/conf/cert/root.crt
host=hcppgdb.postgres.database.azure.com dbname=eopng_config user=hcpadmin@hcppgdb"
```

Remember to change database host, dbname and username in the above line matching your own environment.
If everything is alright, this will connect to the database with psql prompt

```
psql.bin (9.6.9, server 10.5)
WARNING: psql.bin major version 9.6, server major version 10.
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-SHA384, bits: 256, compression: off)
Type "help" for help.
eopng_config=>
```

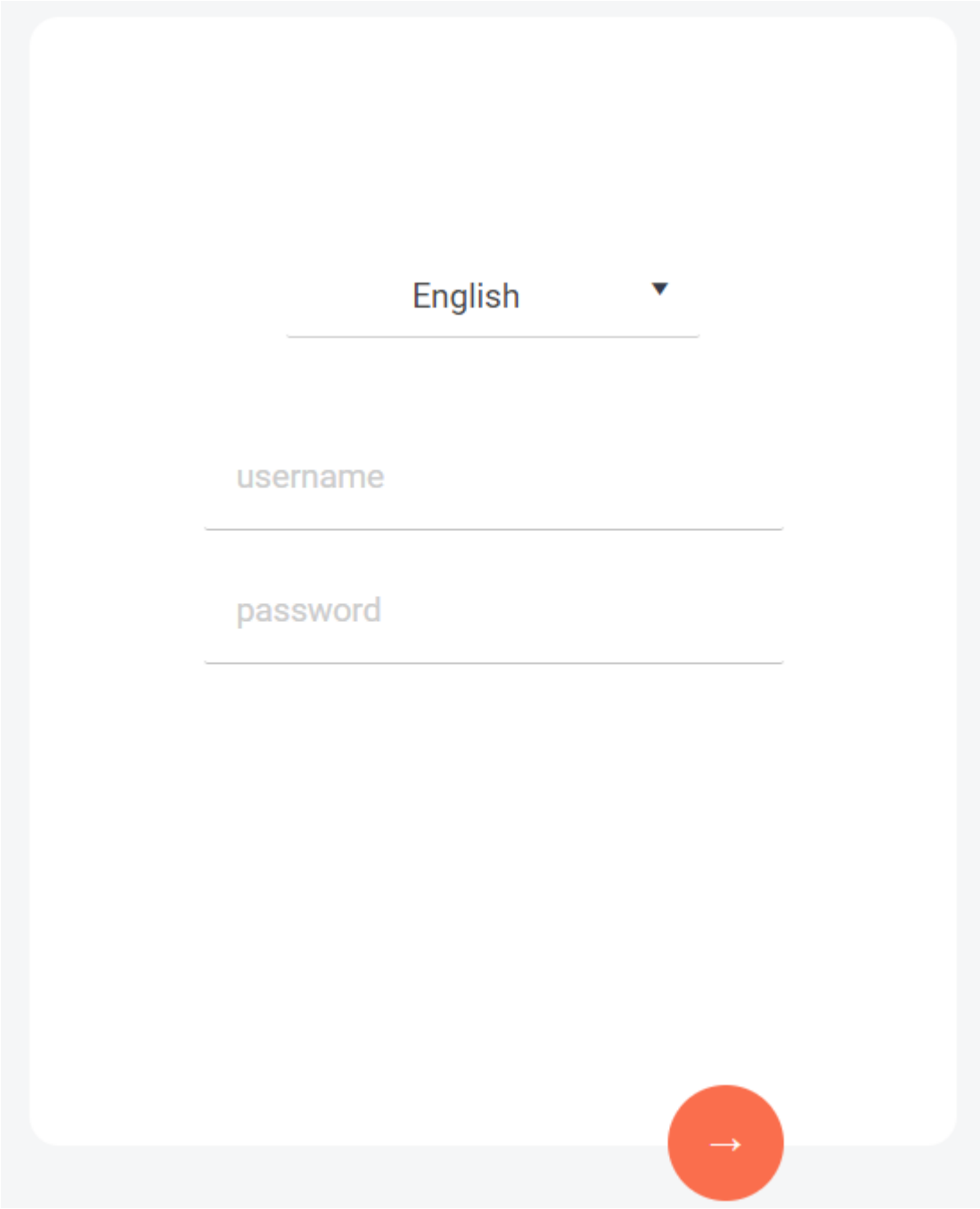
10. Now stop the SAFEQ Cloud server by /opt/safeqcloud/bin/safeq-cloud-server stop command and take a backup of the following configuration file /opt/safeqcloud/conf/application.conf

```
cp -p application.conf  application.conf.backup
```

11. Open the application.conf in any linux editor and add the following lines:

```
schema {

        config {
           password="ENC:f84Qf3Ba5BZbEbTXA4b5Xw"
           poolsize=20
           timeout=30000

         url="jdbc:postgresql://hcppgdb.postgres.database.azure.com:5432/eopng_config?sslmode=verify
         -ca&sslrootcert=/opt/hcp/conf/cert/root.crt"
           username="hcpadmin@hcppgdb"
        }


documents {
           password="ENC:f84Qf3Ba5BZbEbTXA4b5Xw"
           poolsize=20
           timeout=30000

         url="jdbc:postgresql://hcppgdb.postgres.database.azure.com:5432/eopng_documents?sslmode=
         verify-ca&sslrootcert=/opt/hcp/conf/cert/root.crt"
                   username="hcpadmin@hcppgdb"
                }
```

12. Save the application.conf. Distribute the root.crt file in all the SAFEQ Cloud servers and change all the application.conf file in the corresponding servers. Finally start all the SAFEQ Cloud servers. Now it should connect to the Azure PostgreSQL external database with SSL enabled tunneling. You can securely login to your SAFEQ Cloud portal



Reference: https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security

11.2.8 DEPLOY SAFEQ CLOUD CLIENT USING MICROSOFT INTUNE

This guide describes how to silently deploy SAFEQ Cloud Client software on Windows 10/11 user devices being managed using Microsoft Intune.

Pre-requisites/requirements for customer

- Microsoft Intune & Active Directory Premium subscriptions
- Windows 10/11 on user devices
- Microsoft Entra Joined, Windows 10/11 user devices, or Intune Company Portal for manual installation.

- Latest version of the SAFEQ Cloud Client software that you download from SAFEQ Cloud Web UI.

Configuration and deployment steps

Configuration and deployment of SAFEQ Cloud Client software to end user devices (Windows 10/11) using Microsoft Intune is a 3-steps process.

1. Package the .exe to a .intunewin file
2. Upload and create the Intune deployment
3. Assign it to profiles/user groups

Intune will silently deploy SAFEQ Cloud Client software on all workstations when the next sync happens.
Now refer below guidelines to configure and deploy SAFEQ Cloud Client software.

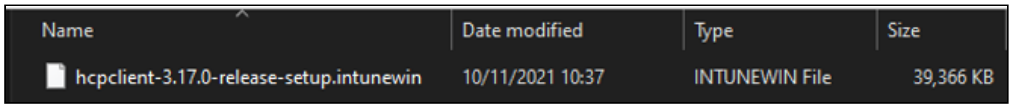
Create .intunewin file

Package the SAFEQ Cloud Client for MS Intune using the Microsoft-Win32-Content-Prep-Tool. This can be downloaded from GitHub – https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool

This command line tool guides you through the process. Ensure the SAFEQ Cloud Client is located in a folder with no other files present.

Example:

```
Please specify the source folder: C:\Users\%username%\Documents\Client
Please specify the setup file: safeqclient-3.17.0-release-setup.exe
Please specify the output folder: C:\Users\%username%\Documents\Output
Do you want to specify catalog folder (Y/N)? N
```



Ensure there are no other files in the folder, or the intunewin creation tool will attempt to package everything and the subsequent install will fail.

Upload and create the Intune deployment

1. Log into the Intune Portal – https://aka.ms/intuneportal
2. Navigate to All Apps, and + Add
3. Select App Type – Windows App (Win32) – Select
4. Follow the Intune Portal to upload the created .intunewin file.

5. Name and Describe the File accordingly, and add Y Soft as the publisher.

6. The Program section requires:

   a. Install Command, this is if you were running the installer as a command line, and all the install flags can be found in the SAFEQ Cloud documentation. At a minimum you would need primary/gateway and account domain address, however, setting login type, and denying access to config is recommended. Further information regarding silent installation can be found in the SAFEQ Cloud Client section of the documentation. Example:
   `safeqclient-3.XX.Y-release-setup.exe /S /GATEWAYADDRESS=[GATEWAYADDRESS] /ACCOUNTDOMAIN=[DOMAIN]`

   b. Uninstall command – `"C:\Program Files\Y Soft Corporation\SAFEQ Cloud Client\latest\uninstall.exe" /S`

   c. Behavior:
      - User – the installer has the same privileges as the logged-in user. If the user has the administrative permissions necessary for adding a driver and a system service, the installation finishes and the user can see the SAFEQ Cloud Client tray icon. If the user does not have the necessary permissions and cannot grant administrative consent, the installation will abort.
      - System – the installer has privileges of the local system account, so the installation finishes. The logged-in user will not see the SAFEQ Cloud Client tray icon right after the installation because the installation was not running under the user account. The icon will be visible after the next login or restart of the computer.

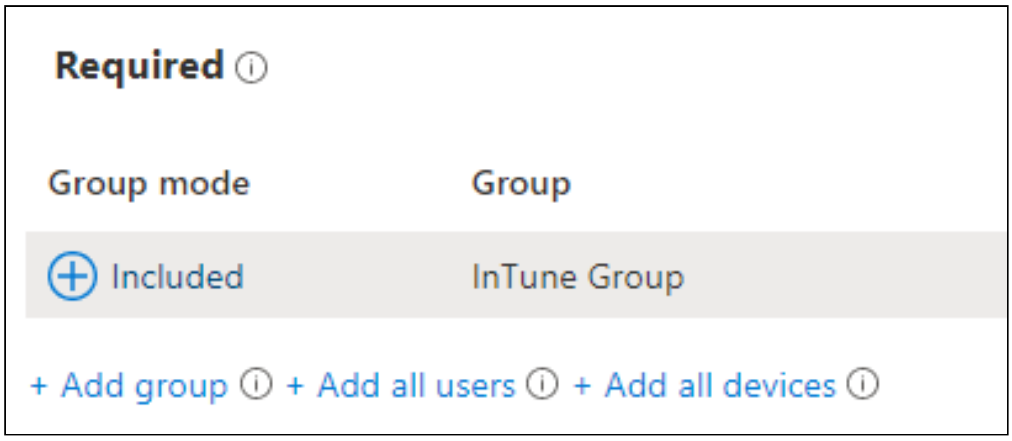
   d. Device Restart Behavior – None.

7. Requirements
   - OS Architecture – 64-bit & 32-bit
   - Minimum OS – Win 10 1607

8. Detection Rules – we can detect the version of the SAFEQ Cloud Client by looking for a Registry entry. This enables different versions to be created to install over the top or use the supersedence feature in Intune.
   - Registry = Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SAFEQ Cloud Client
   - Value name = DisplayVersion
   - Detection method = Version Comparison
   - Operator = Greater than or equal to
   - Value = 3.XX.X or YYYY.MM.DD.X

     Note that the value depends on which client version is being installed.
     It can be in the format 3.XX.X (semantic version) or YYYY.MM.DD.X (calendar version), where 'X' denotes the version of the SAFEQ Cloud Client being installed."

Assign the App to the required groups



11.2.9 CONFIGURE MDM AIRPRINT INTEGRATION ON MICROSOFT INTUNE

This guide describes how to configure Microsoft Intune MDM Airprint integration of Apple devices with SAFEQ Cloud.

Pre-requisites/requirements for customer:

- Azure Intune & Active Directory Premium subscriptions
- iOS/macOS BYOD/corporate user devices enrolled on Microsoft Intune

Configuration and deployment steps

Please follow below step -
i. Setup and assign Airprint profiles for iOS and macOS devices in Microsoft Intune
ii. Verify configuration on Apple user devices

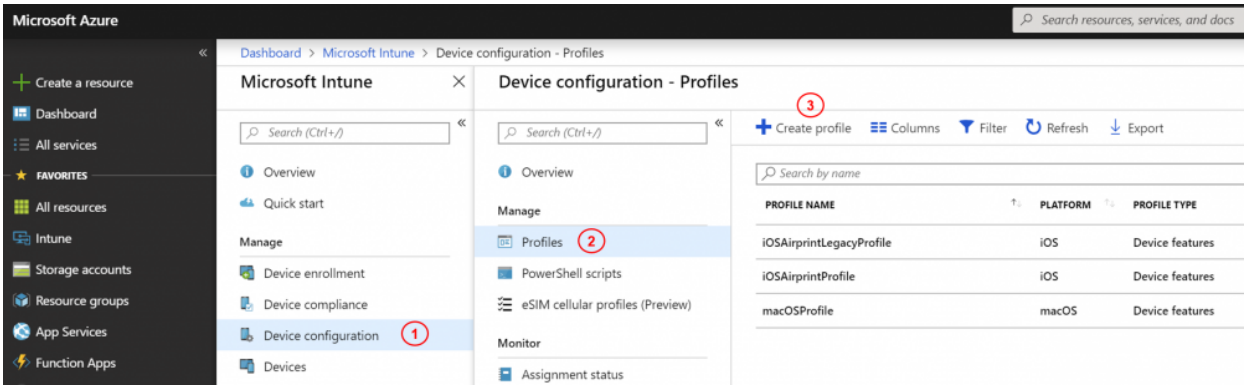
Intune will silently configure SAFEQ Cloud Client software on all workstations when the next sync happens.
Now refer below guidelines to configure and deploy SAFEQ Cloud Client software.

Setup and assign Airprint profiles for iOS and macOS devices in Microsoft Intune

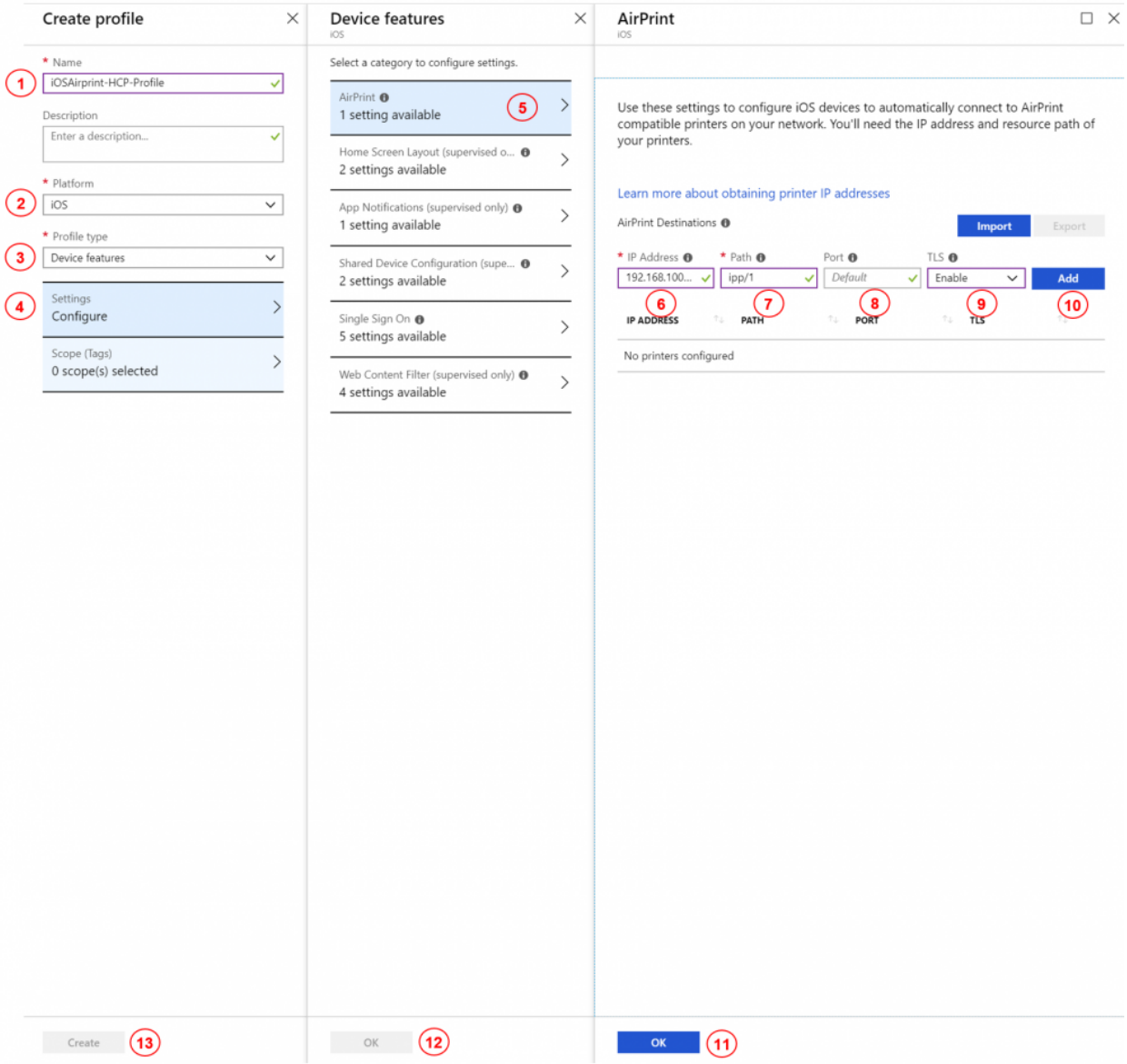
Before you setup Airprint profile in Microsoft Intune, ensure that your Apple BYOD/corporate user devices are already enrolled on Microsoft Intune.
Refer to these documentation on how to enroll Apple devices on Microsoft Intune –
*Get an Apple MDM push certificate for Microsoft Intune enrollment
*Enroll iOS devices in Intune
*Enroll macOS devices in Intune

- Login to Azure portal

- Go to Device Configuration > Profiles page in Intune to create separate profiles for iOS and macOS devices

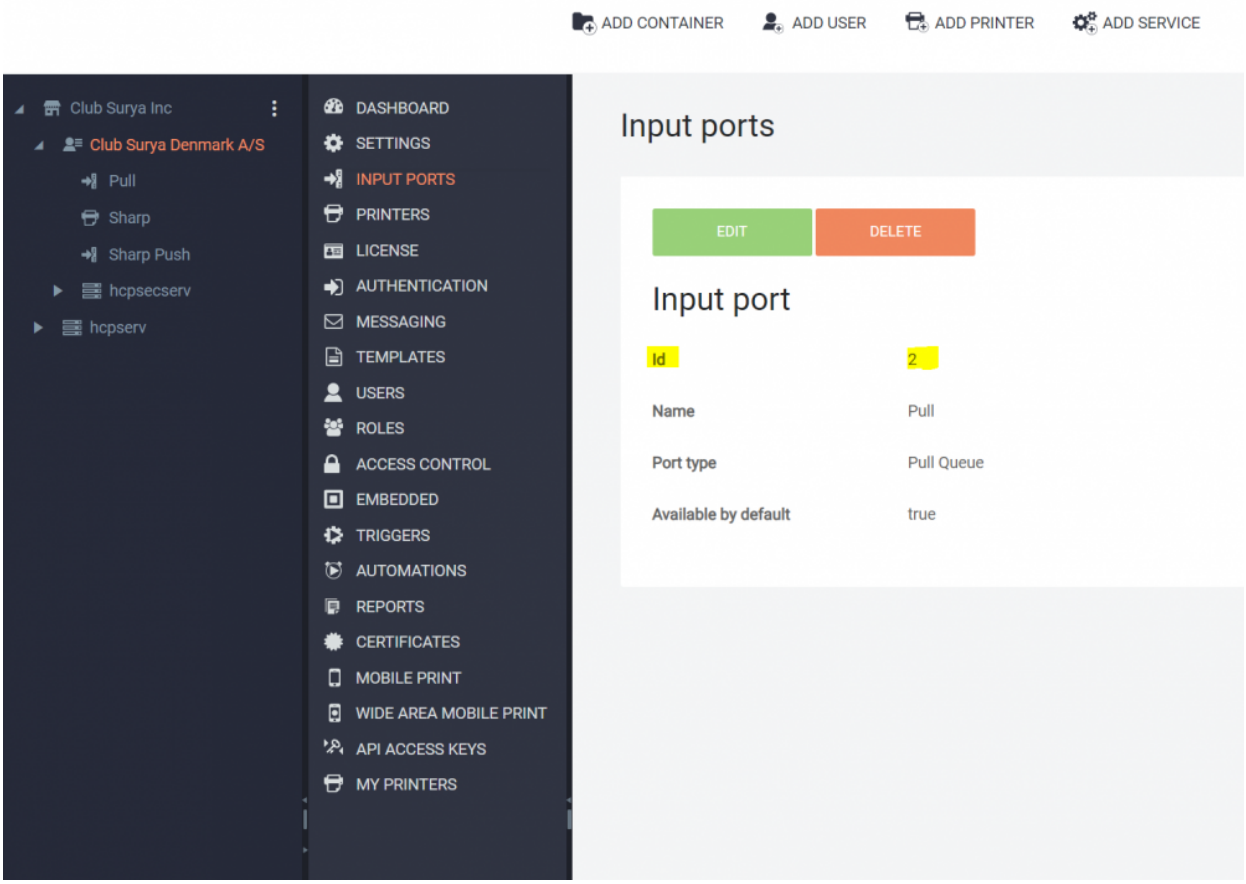


- Create profile separately for iOS and macOS devices as required



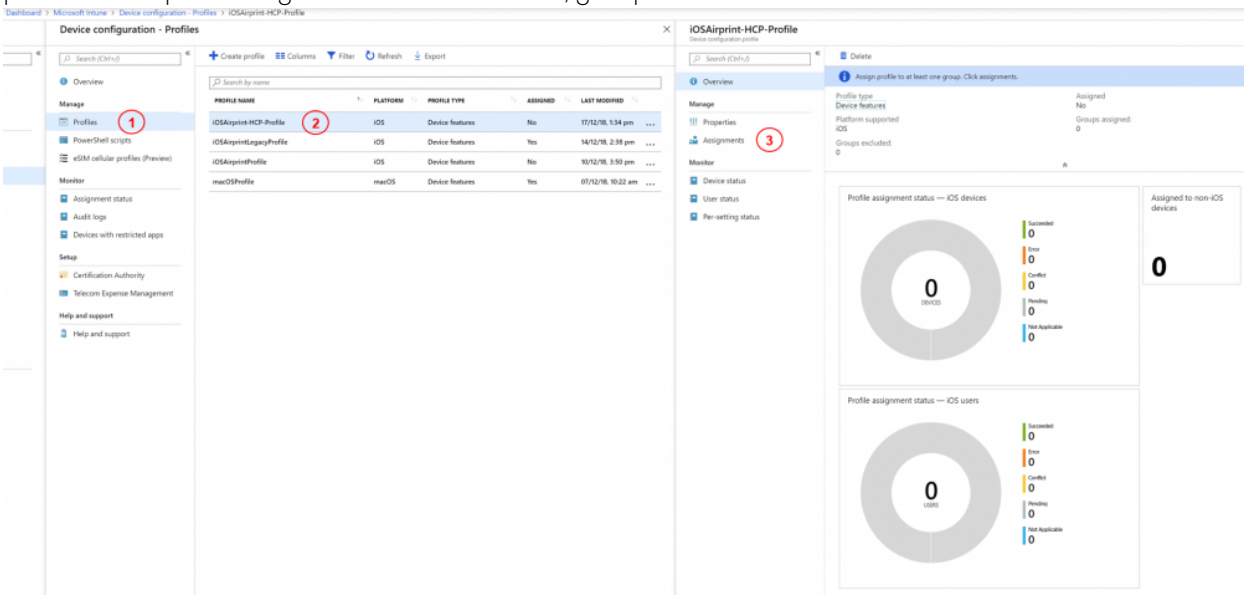
1 – Type in suitable profile name
2 – Choose iOS or macOS from drop-down
3 – Choose '**Device Feature**' as profile type
4 – Hit '**Configure**' settings

5 – Hit '**Airprint**' settings
6 – Add SAFEQ Cloud mobile gateway host IP address
7 – Add resource path to relevant printer in the following format – **ipp/#** where **#** is port number as shown on SAFEQ Cloud web UI **Input Ports** section for the configured ports.

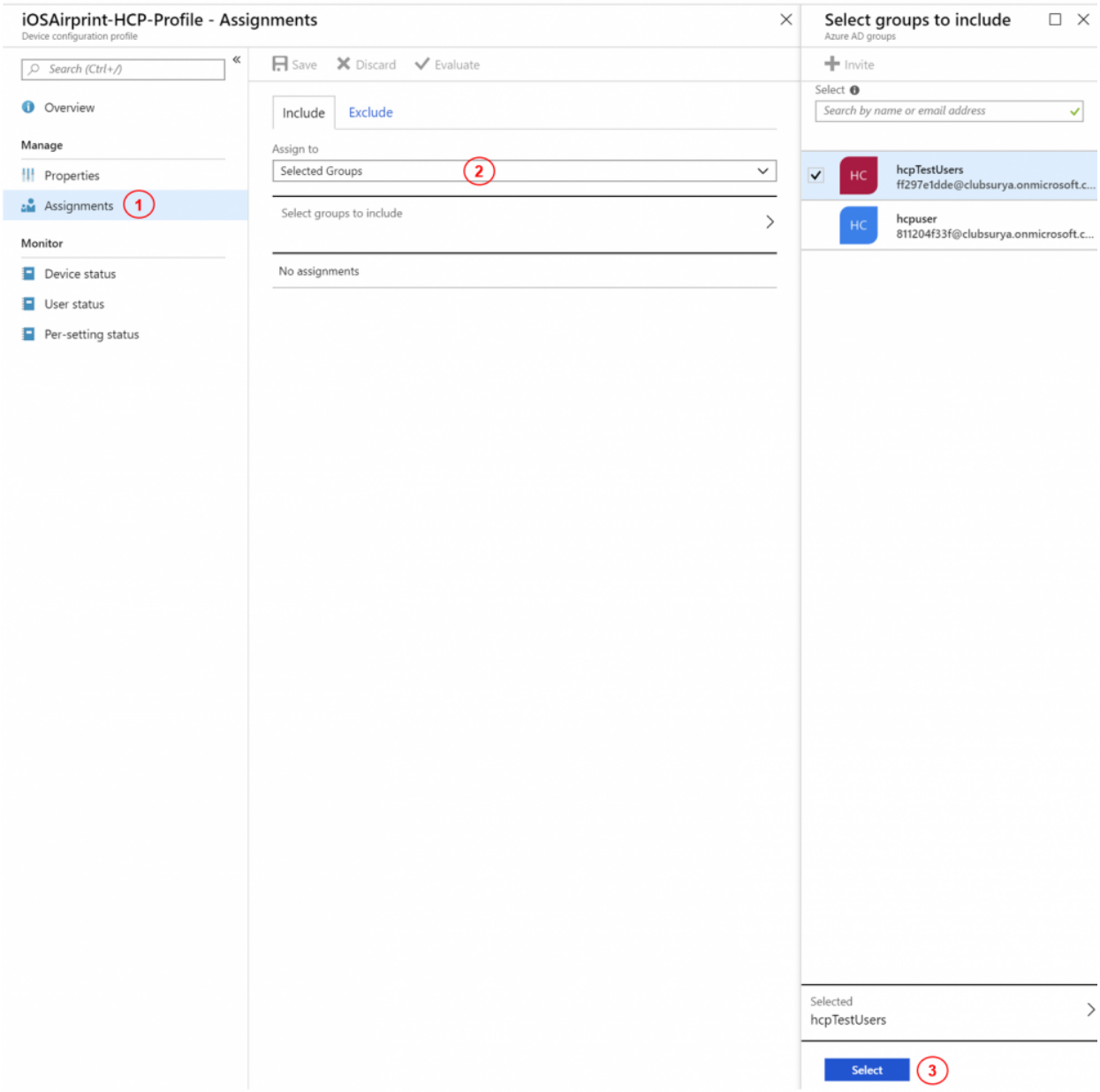


8 – Leave it as 'Default'
9 – Choose 'Enable' from dropdown
10 – Click on 'Add' button
11, 12, 13 – Click on 'OK', 'OK' and 'Create' buttons respectively to create new profile

- Go to Device Configuration > Profiles page in Intune and choose newly created profile from previous step to assign it to relevant users/groups



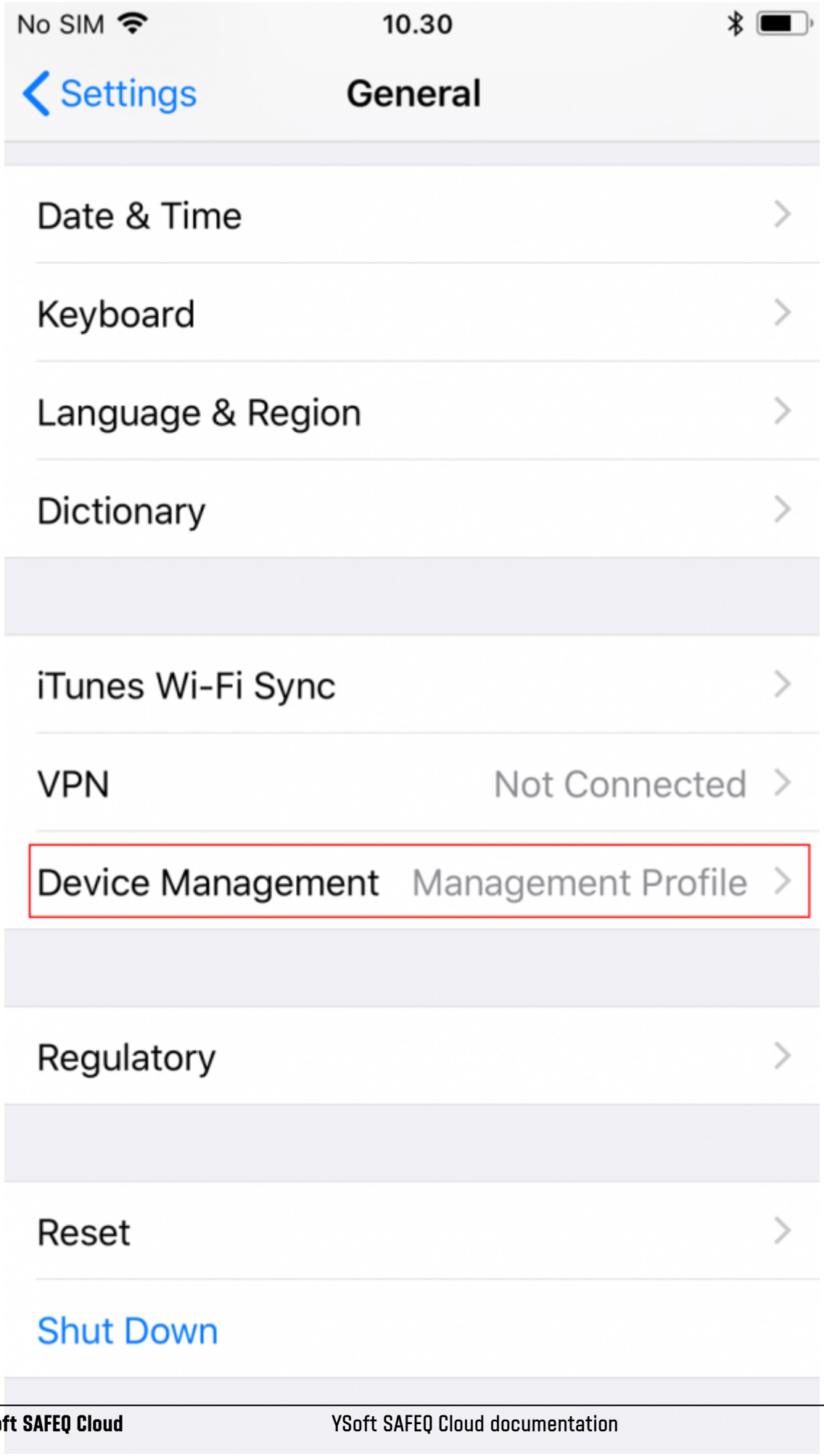
- Choose 'Selected Groups' from 'Assign to' dropdown and select relevant groups for assignment. Other options available are – 'All Users and All Devices', 'All Devices' and 'All Users'



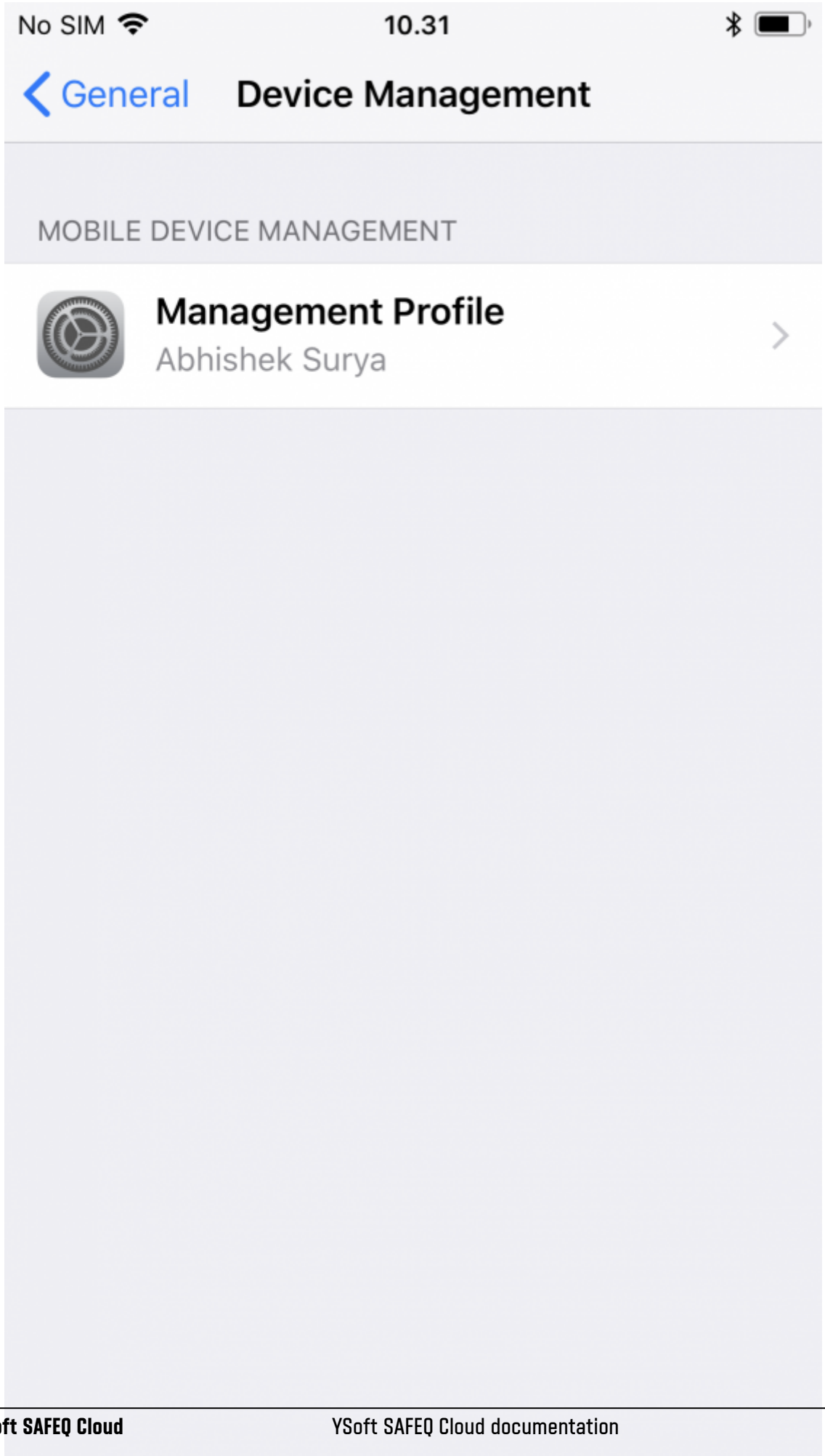
Verify Airprint profile is available onto pushed user iOS device

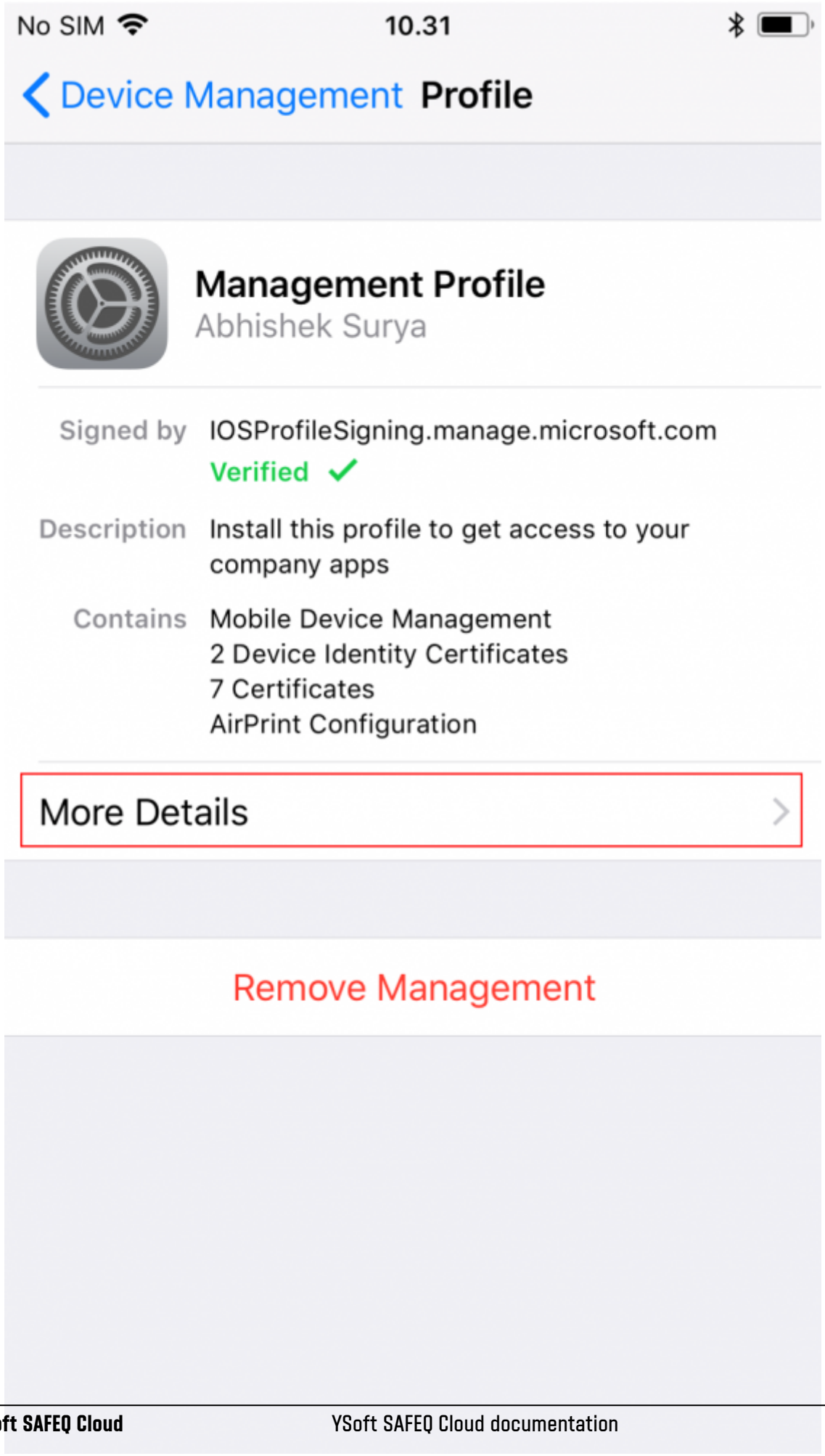
The configured Airprint profile will be synced automatically to all applicable enrolled devices. Read about Intune policy sync FAQs here. If needed, you can also manually sync a device, read this How-to

- In your iOS device go to Settings > General > Device Management

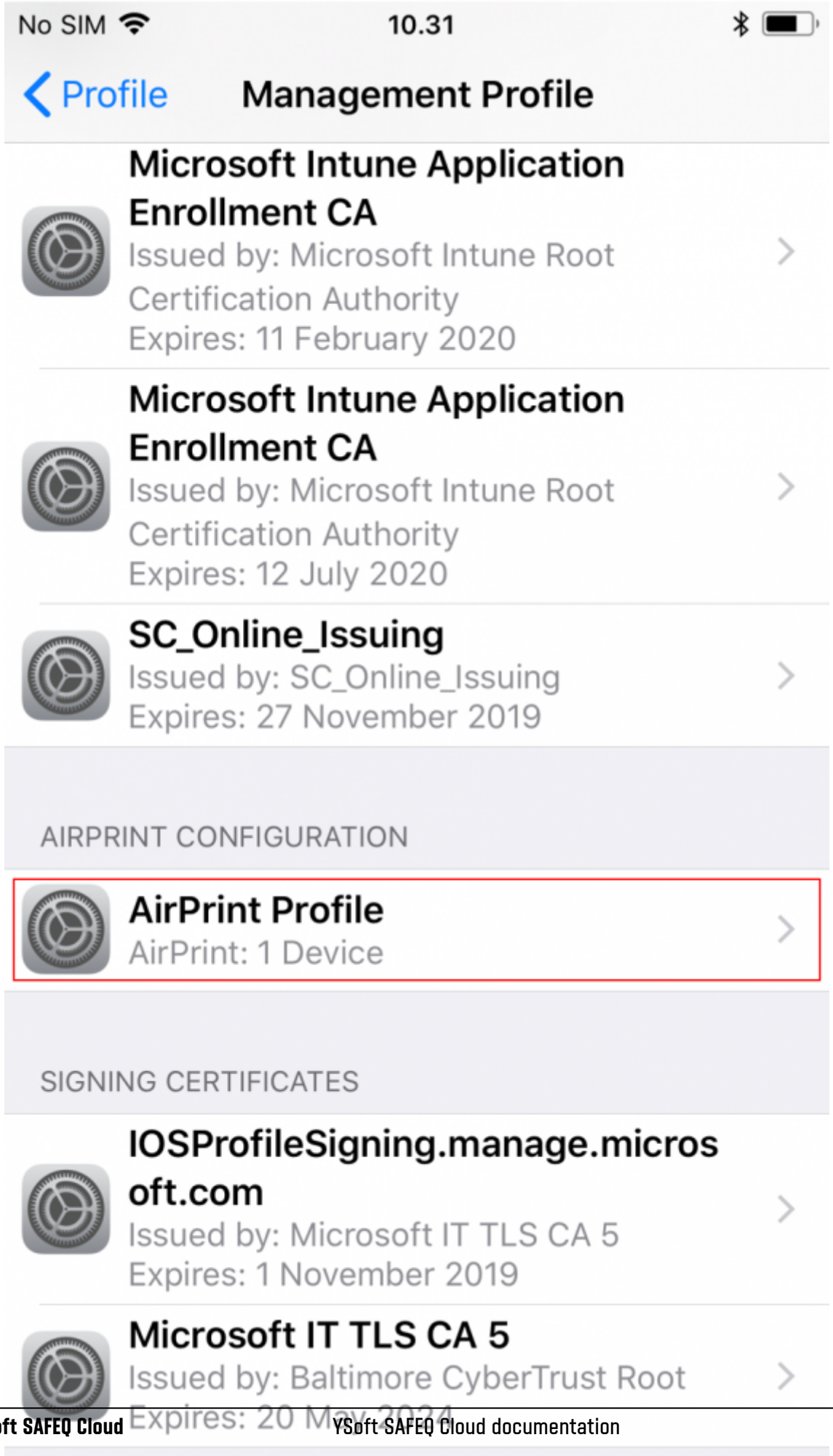

No SIM
10.30
Settings
General
Date & Time
Keyboard
Language & Region
Dictionary
iTunes Wi-Fi Sync
VPN
Not Connected
Device Management
Management Profile
Regulatory
Reset
Shut Down

- Open Management Profile of the user and go to More Details page


No SIM
10.31
General
Device Management
MOBILE DEVICE MANAGEMENT
Management Profile
Abhishek Surya


No SIM
10.31
Device Management
Profile
Management Profile
Abhishek Surya
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Mobile Device Management
2 Device Identity Certificates
7 Certificates
AirPrint Configuration
More Details
Remove Management

- Scroll down and open Airprint profile and verify that the pushed configurations are as per profile setup done in Step 2.1


No SIM
10.31
Profile
Management Profile
Microsoft Intune Application Enrollment CA
Issued by: Microsoft Intune Root Certification Authority
Expires: 11 February 2020
Microsoft Intune Application Enrollment CA
Issued by: Microsoft Intune Root Certification Authority
Expires: 12 July 2020
SC_Online_Issuing
Issued by: SC_Online_Issuing
Expires: 27 November 2019
AIRPRINT CONFIGURATION
AirPrint Profile
AirPrint: 1 Device
SIGNING CERTIFICATES
IOSProfileSigning.manage.microsoft.com
Issued by: Microsoft IT TLS CA 5
Expires: 1 November 2019
Microsoft IT TLS CA 5
Issued by: Baltimore CyberTrust Root
Expires: 20 May 2024

No SIM
15.45
Management Profile
AirPrint Profile
AIRPRINT PATHS
ipps://192.168.100.178/ipp/1
ipps://192.168.100.178/ipp/2

- Once everything is in place, you should be able to access available printers from the configured SAFEQ Cloud Mobile Gateway

11.2.10 DISASTER RECOVERY PROCEDURE FOR PRIMARY SERVER

The primary objective of the disaster recovery procedure is to ensure stability and orderly recovery after a failed primary server to enable minimal disruption in the use of SAFEQ Cloud.

The following outlines the steps to backup and restore a SAFEQ Cloud primary server.

Backup a primary server

1. To take a backup of all the runtime configurations, truststore, log4j config files and the license

Go to the folder /opt/safeqcloud

```
cd /opt/safeqcloud
```

Take a backup of the conf folder

```
tar -cvzf conf.tar.gz conf
```

where conf.tar.gz – name of the backup
conf – name of the folder that is backed up

2. To take a backup of the runtime information, server-ids and the local database
Go to the folder /var/lib

```
cd /var/lib
```

Take a backup of the eopng folder

```
tar -cvzf eopng.tar.gz eopng
```

3. If you are using an external postgres DB then take a backup of the database as well

```
pg_dump -f primarydbdump -b -c -C -h <DBHOST> -U postgres -p <DBPORT> eopng_config
```

Where DBHOST and DBPORT are the database cluster address and port number.

Restore a primary server

In case the server fails, the below steps can be taken on a clean system

4. Run the SAFEQ Cloud installer

```
./safeq-cloud-server-*-release-setup-linux-x86_64.bin [-f]
```

The optional `-f` switch can be specified to force the full installation instead of upgrade.

5. Fill out all the details in the installer (All the details in the installer will only be used to get through the wizard and setup all the binaries we do not need to backup)
6. **Opt out** of starting SAFEQ Cloud in the final installer step (uncheck the "Start SAFEQ Cloud server" checkbox). Or stop it afterwards with `systemctl stop safeq-cloud-server` command.
7. Stop the database (only if bundled postgresql was used and not the external database)

```
systemctl stop SAFEQ Cloud-database
```

8. Replace the new /opt/safeqcloud/conf with the backup taken in step 1

```
cd /opt/safeqcloud
tar -xvzfp /path/to/backedup/conf.tar.gz
```

9. Replace the new /var/lib/eopng with the backup taken in steps 2

```
cd var/lib
tar -xvzfp /path/to/backedup/eopng.tar.gz
```

10. Start the database (only if bundled postgresql was used and not the external database)

```
systemctl start SAFEQ Cloud-database
```

10. Start the SAFEQ Cloud services again

```
systemctl start safeq-cloud-server
```

While restoring the folders please make sure that the permissions on the folders backed up are retained

11.2.11 CONFIGURE SCAN TO MY EMAIL

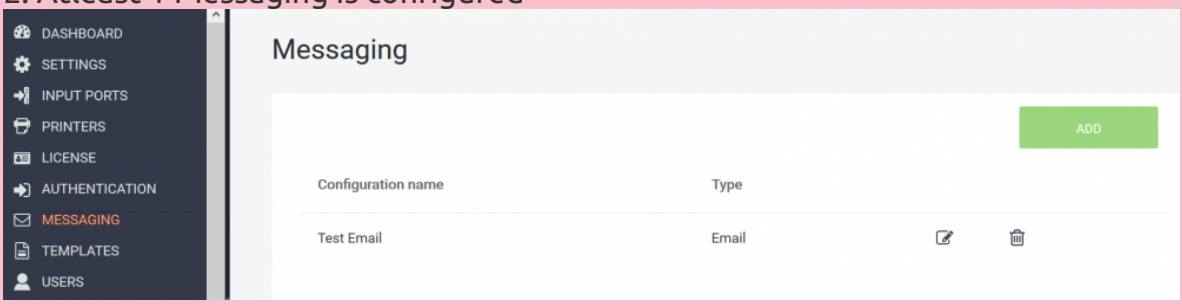
YSoft SAFEQ Cloud 2.5 introduced "Scan to My Email" feature on HP and Konica Minolta embedded applications.

With 'Scan to My Email' enabled, users can scan documents on MFD and send it to their email -

Authentication	Precondition
Local user	add email address of the user in SAFEQ Cloud web console

Authentication	Precondition
LDAP authenticated user	email address of the user exists in LDAP user profile
Microsoft Entra authenticated user	email address of the user exists in Microsoft Entra user profile
okta authenticated user	email address of the user exists in okta user profile

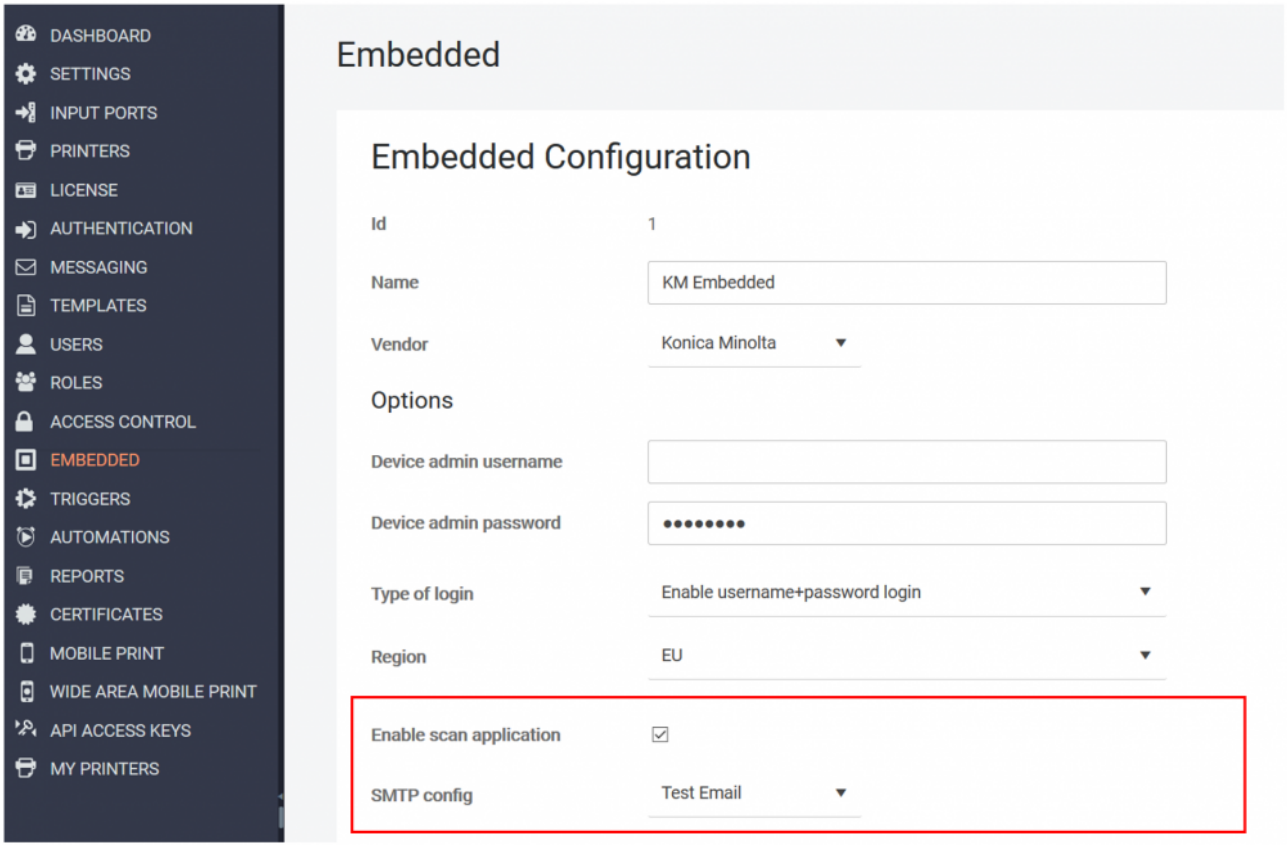
Before you can use this feature, ensure that -
1. Message service is running on desired SAFEQ Cloud server – see SAFEQ Cloud Services
2. Atleast 1 Messaging is configured



Embedded Setup

Enable 'Scan to My Email' feature while setting up embedded application
1. *Enable scan application* – tick to enable

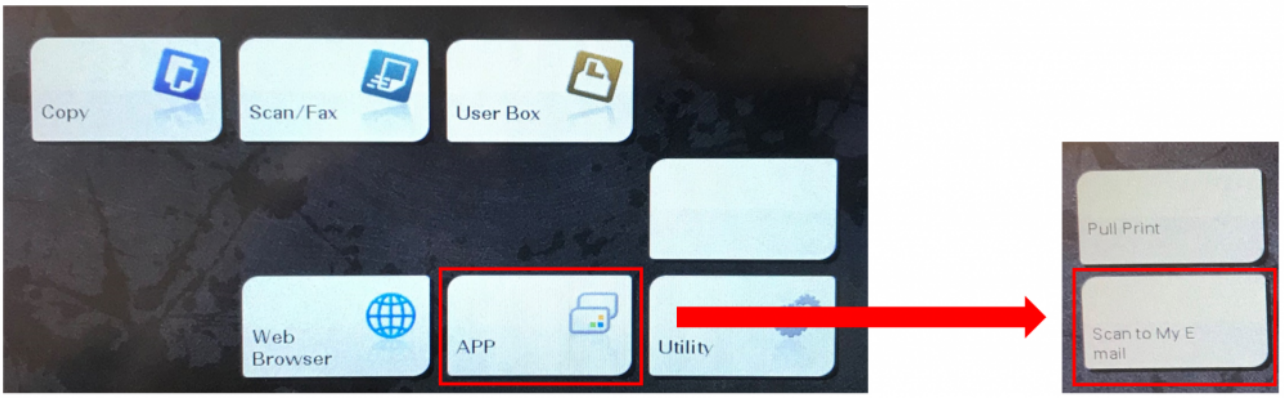
2. *SMTP config* – Choose from available messaging



To know how to deploy embedded application on HP or Konika Minolta devices see – Deploy HP embedded | Deploy Konica Minolta embedded

Using 'Scan to My Email'

After the embedded application has been successfully deployed, login to the embedded application and find 'Scan to my email' application.
for example, on Konika Minolta device, you can find it under App folder from main menu



11.2.12 USE NETWORK CONNECTED CARD READERS

YSoft SAFEQ Cloud 3.0 introduced support for Network/IP connected card readers, so users can release all print jobs to the printer when swiping their card.

Please refer to below documentation on IP Card Readers

IP Card Reader Options	Link
Security Engineering – Switchbridge	guide link
RFIdeas – 241 Controller	guide link

If your preferred brand of network card reader is not mentioned above, please contact support (support@ysoft.com)

RFIdeas – Ethernet 241 configuration & setup with SAFEQ Cloud

This guide is to configure and setup RFIdeas Ethernet 241 controller for IP card reader solution to be used with SAFEQ Cloud.
The controller is a two-port switch that connects between a network device, such as a printer, and its network. Included USB and serial ports provide an interface to a wide variety of RFIDeas card readers. The controller can send badge data to the SAFEQ Cloud server which will use the badge data information to control the dispatching of jobs to the printer.
You can read more about the product please see – Ethernet 241 Controller
This how-to guide has 3 parts –

- Prerequisites
- Ethernet 241 Configuration
- SAFEQ Cloud Configuration

Prerequisites

> Get MAC address printed on the back of Ethernet 241. Use it to get IP address of controller from DHCP server in the network.

- RFIDeas Ethernet 241 requires a RFIDeas pcProx card reader with part numbers ending in AK5
- SAFEQ Cloud server version – 3.1 onward is installed and licensed
- Verify Ethernet 241 controller is plugged-in to power supply and is connected to the network and is reachable on browser at `http://<ip address of Ethernet 241 controller>/index.htm`
- Ethernet 241 controller is located next to printer/MFD where it will be used to release print jobs.
- Verify compatible card reader is connected to the switchbridge on USB port and a test has been performed to ensure the reader is able to read the utilized ID cards. Confirmation that cards are read properly can be obtained from the Log tab available through the controller configuration web page. A successful card recognition entry will look similar to:
  `0.01:48:39.7 DEBUG Reader 1 Card Presented: Dec Id=33459, Hex Id=7082B3, Bits=24`

Ethernet 241 controller configuration

You might have to logon to the controller if an admin password was configured previously

MAC Address – Take note of MAC Address of Card Reader. This will be used to configure Card Reader in SAFEQ Cloud. The MAC address is on the back of the Ethernet 241 controller and it also shown under the **'Status'** tab of the Web UI

Open Ethernet 241 controller's web page `http://<ip address of controller>/index.htm`

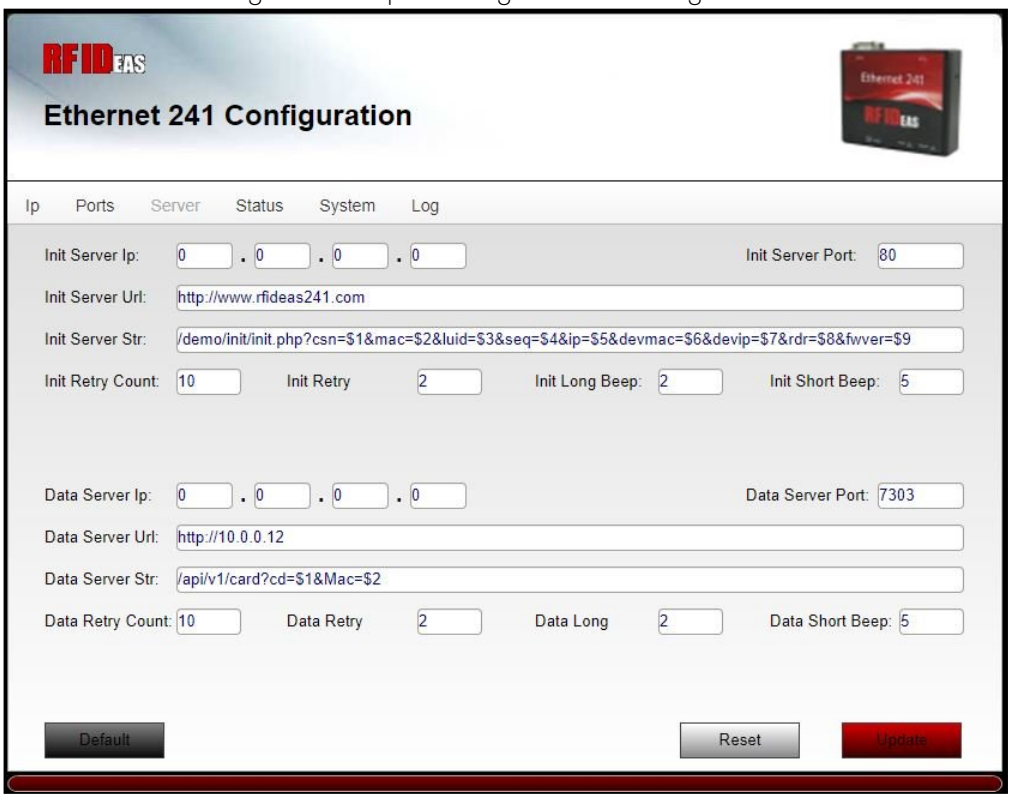
Go to **Server** tab to add following detail –

- All settings that start with Init are not used and can be ignored.
- Data Server Ip – this setting is not used. Leave it as default 0.0.0.0
- Data Server Url – Add IP address of SAFEQ Cloud server as applicable in following format `https://<server-address>` In case the communications should be non-encrypted replace the https prefix with http.
- Data Server Port – Port `7300` can be used in case the communication between the controller and the server must be encrypted using HTTPs. For non-encrypted communication, port `7303` can be used

Please note: Not every RFIdeas 241 Card Reader may be HTTPs compatible. Please check with the manufacturer guidelines before setting up the data server ports.

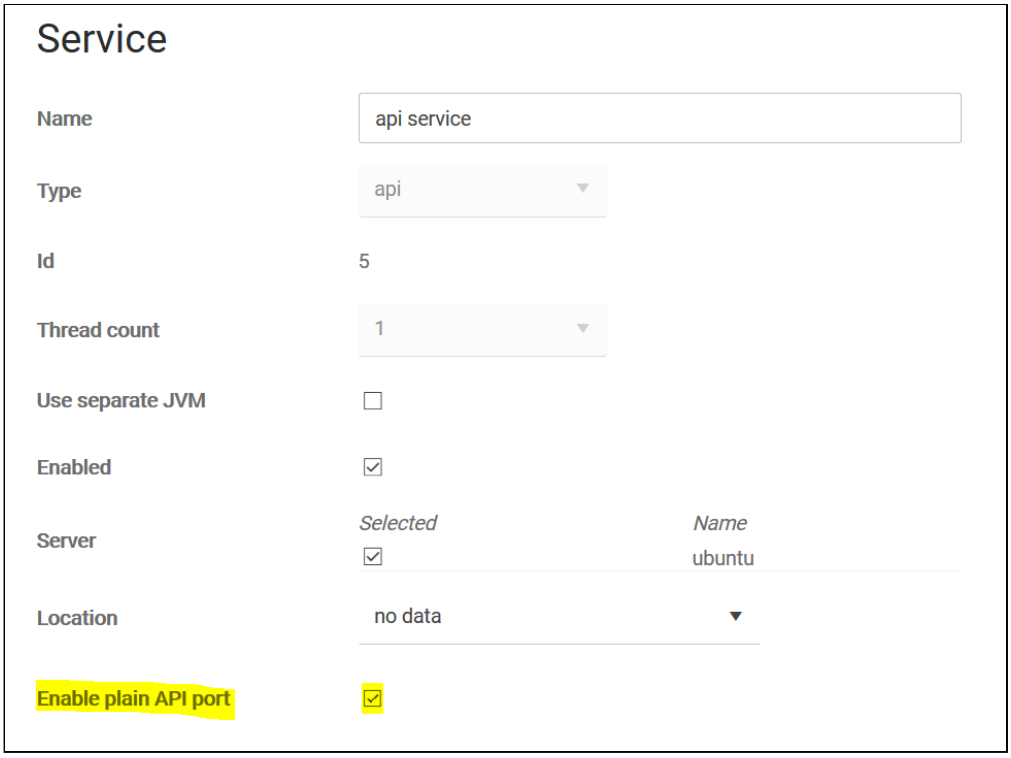
- Data Server Str – Add SAFEQ Cloud API path `/api/v1/card?cd=$1&Mac=$2`
  Note: no spaces should be added before, after or in this string or the reader will not be able to communicate with the server.
- The other four remaining settings can be ignored.

- Select **Update** to save settings
  Refer to below image for sample configuration settings

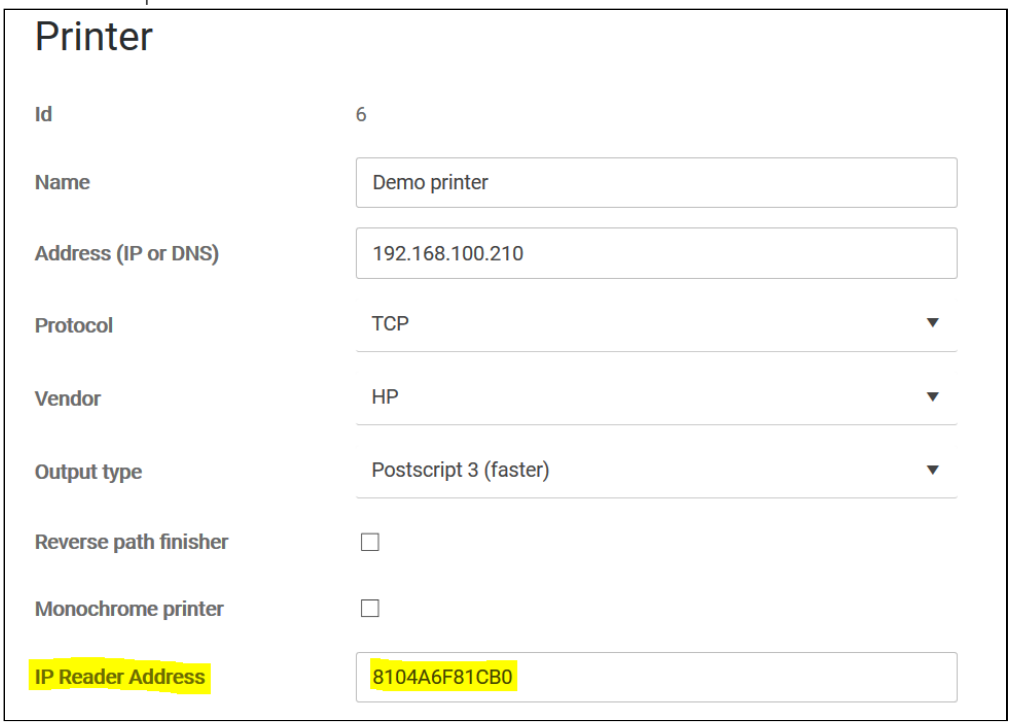


SAFEQ Cloud Configuration

- Edit SAFEQ Cloud API Service on primary/gateway as applicable to 'Enable plain API port' (optional – needed only if you want to use plain port)



- Edit Printer Settings in SAFEQ Cloud to add MAC ID of Ethernet 241 controller on Printer/MFD where 'swipe-and-release' feature has to be used



- Enroll cards on available MFD to use that card with IP card reader solution. If its not a possibility, add Card ID to the user in SAFEQ Cloud using SAFEQ Cloud public API. Link to API documentation is here. Please note that you will need to read Card ID from the Reader if not already known. One way to do so is to open notepad application on computer and plug the reader into its USB port. Card ID of the reader will be printed on the notepad.

Security Engineering – Switchbridge configuration & setup with SAFEQ Cloud

This solution is no longer supported as Security Engineering has started using new hardware that is no longer compatible with the below firmware.

This guide is to configure and setup Security engineering's Switchbridge for IP card reader solution to be used with SAFEQ Cloud.
Security Engineering's Switchbridge is a dual port Ethernet interface. A USB card reader connects to the SwitchBridge™ via the USB Host port and Ethernet connection from the central network and the local printer is connected to the on board Ethernet switch. The switchbridge can send badge data to the SAFEQ Cloud server which will use the badge data information to control the dispatching of jobs to the printer.
You can read more about Switchbridge here – Switchbridge datasheet
This how-to guide has 3 parts –

- Prerequisites
- Switchbridge Configuration
- SAFEQ Cloud Configuration

Prerequisites

> Get MAC address printed on the back of Switchbridge. Use it to get IP address of switchbridge from DHCP server in the network. Alternatively, you can use Security Engineering's tool `sendu.exe` to locate Switchbridge in network and get its MAC address.
> You can download `sendu.exe` tool from Security Engineering site – link (On the webpage, click on **IP Device Package** to download tool package in zip file. When you unzip it, `sendu.exe` is located at path `90_ipdevicepack-4.zip/Tools`

- Switchbridge firmware version – `sbr1022app_5_02_07` (Contact Y Soft support@ysoft.com to get the latest firmware.)
- SAFEQ Cloud server version – 3.0 onward is installed and licensed
- Verify Switchbridge is plugged-in to power supply and is connected to the network and is reachable on browser at `http://<ip address of switchbridge>/index.htm`
- Switchbridge is located next to printer/MFD where it will be used to release print jobs.
- Verify suitable card reader is connected to the switchbridge on USB port and a test has been performed to ensure the reader is able to read the utilized ID cards.

Switchbridge Configuration

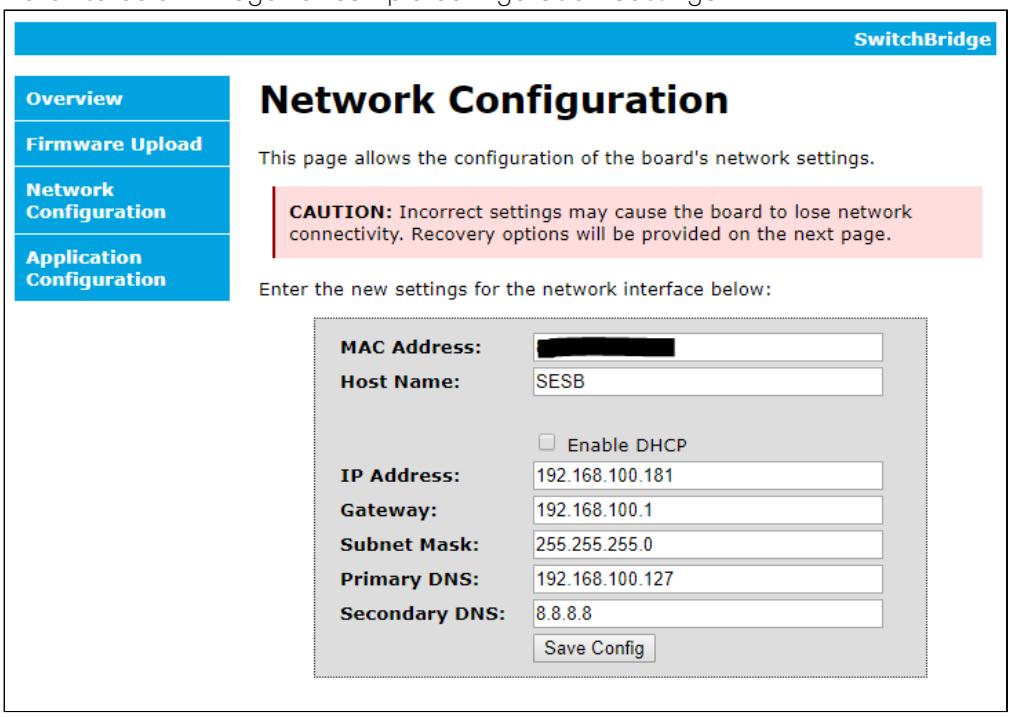
> Use username: "admin" and password: "seceng" to login when prompted on IP card reader's webpage

Open Switchbridge's web page `http://<ip address of switchbridge>/index.htm`

Go to Network Configuration page to add following detail –

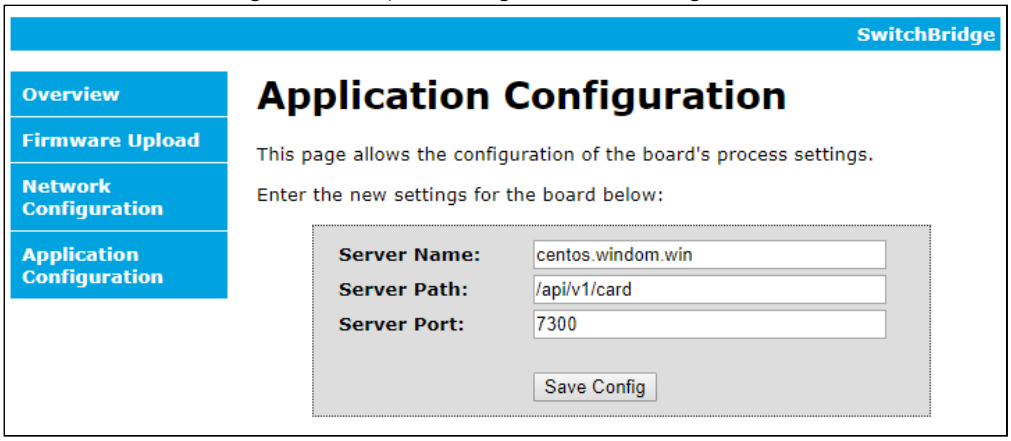
- MAC Address – Take note of MAC Address of Switchbridge. This will be used to configure it in SAFEQ Cloud
- Host name – Change it to a desired name or to IP address of Switchbridge. If you are using DNS Server, make sure there is a CNAME entry for the Switchbridge on it.
- DHCP – If you are using DHCP, select Enable DHCP option
- DNS settings – Update values of Gateway, Subnet Mask, Primary DNS and Secondary DNS as applicable and based on your network settings

Refer to below image for sample configuration settings



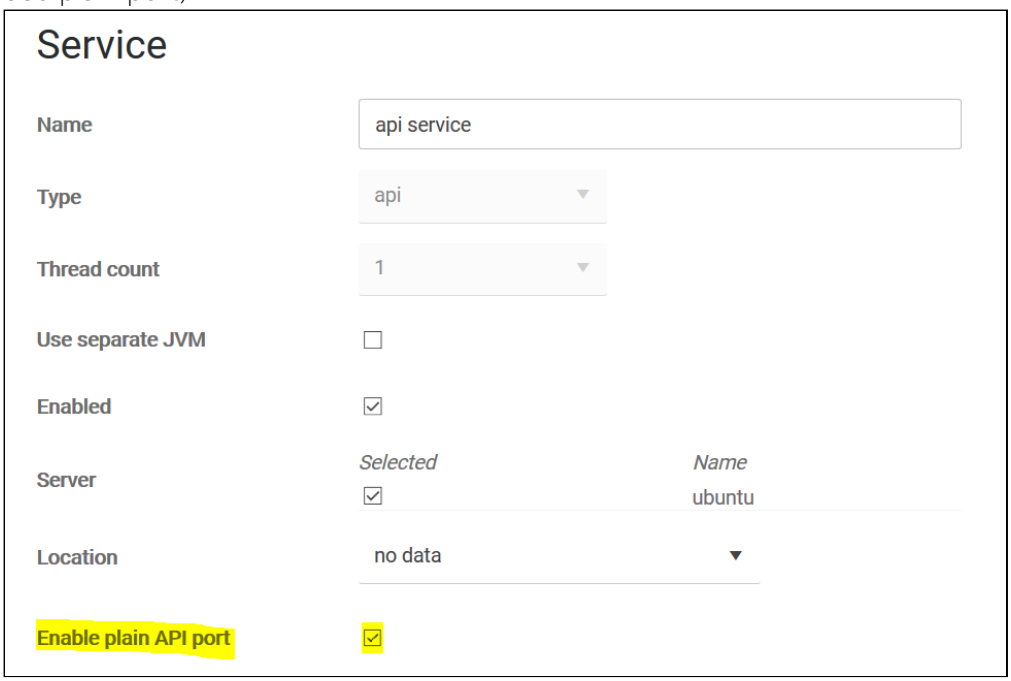
Go to Application configuration page to add following details for communication with SAFEQ Cloud –

- Server name – Add FQDN or IP address of SAFEQ Cloud server as applicable
- Path to be set on IP Card reader – Add SAFEQ Cloud API path `/api/v1/card/`
  Note: no spaces should be added before, after or in this string or the reader will not be able to communicate with the server.
- Port number – Port `7300` can be used in case the communication between the controller and the server must be encrypted using HTTPs. For non-encrypted communication, port `7303` can be used
  Refer to below image for sample configuration settings

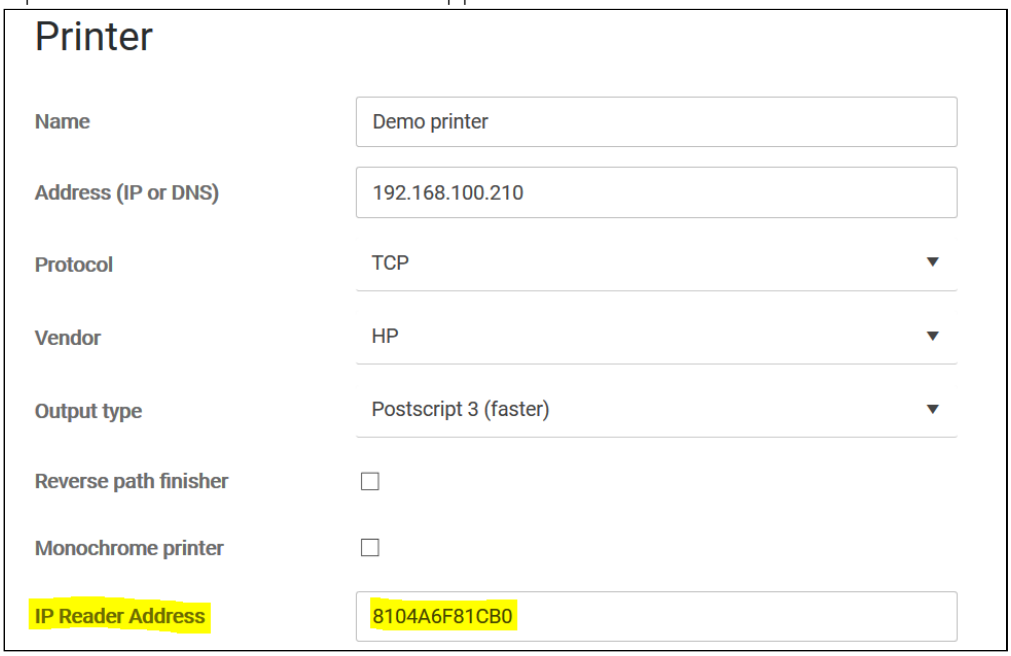


SAFEQ Cloud Configuration

- Edit SAFEQ Cloud API Service to 'Enable plain API port' (optional – needed only if you want to use plain port)



- Edit Printer Settings in SAFEQ Cloud to add MAC address of Swithcbridge in IP Reader Address field on Printer where 'swipe-and-release' feature has to be used. Note – Please ensure all alphabets in MAC address are in upper case



- Enroll cards on available MFD to use that card with IP card reader solution. If its not a possibility, add Card ID to the user in SAFEQ Cloud using SAFEQ Cloud public API. Link to API documentation is here. Please note that you will need to read Card ID from the Reader if not already known. One way to do so is to open notepad application on computer and plug the reader into its USB port. Card ID of the reader will be printed on the notepad.

11.2.13 CREATE PRINT QUEUES WITH SPECIFIC OUTPUT OPTIONS

There may be cases where a customer would like to provide specific Print queues for their users, which force specific print output settings, for example, "Roaming Print Duplex Letterhead" which should force Duplex printing and set the output tray to tray3, because that paper tray always contains the company letterhead.

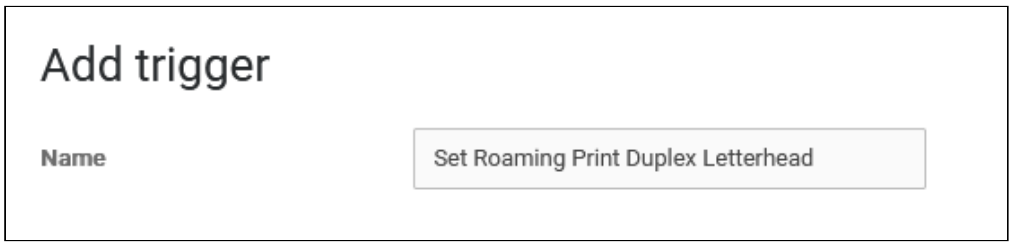
This is easily achieved with the YSoft SAFEQ Cloud Triggers system, which works simply on conditions "if this is true then do that".

Below is an example of how you could configure a Print queue and a Trigger to force any print job coming to this Print queue, to always be Tray3 and Duplex. This can be customized for virtually all print output attributes, such as booklet, color/bw, hole punching, and stapling.

Create a Print queue with a name such as "Roaming Print Duplex Letterhead". It doesn't matter if this is a Pull or a Push queue.

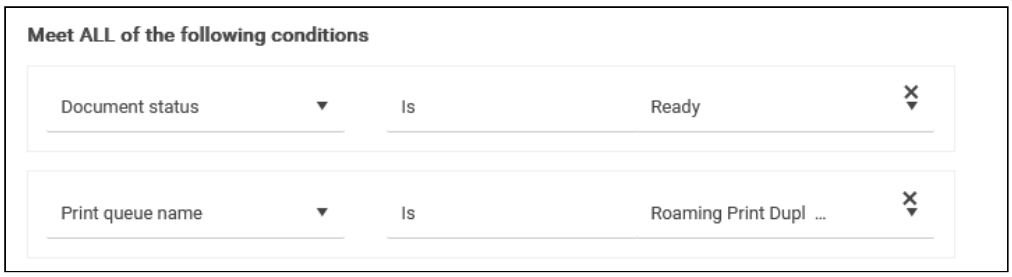
Remember, this could work on an existing Pull print queue or a Direct print queue as well, but triggered on a user group membership or similar. There are numerous ways a trigger can be configured. Ask support for help if you need it!

Next, go to Triggers and create a new Trigger. Name it something recognizable, such as "Set Roaming Print Duplex Letterhead".



Set the first conditions so we fire this trigger only when a job has been received successfully (no point in spending time on triggers if it's a failed job), and when the Print queue name matches the queue name we created.

```
Document status is Ready
Print queue name is Set Roaming Print Duplex Letterhead
```



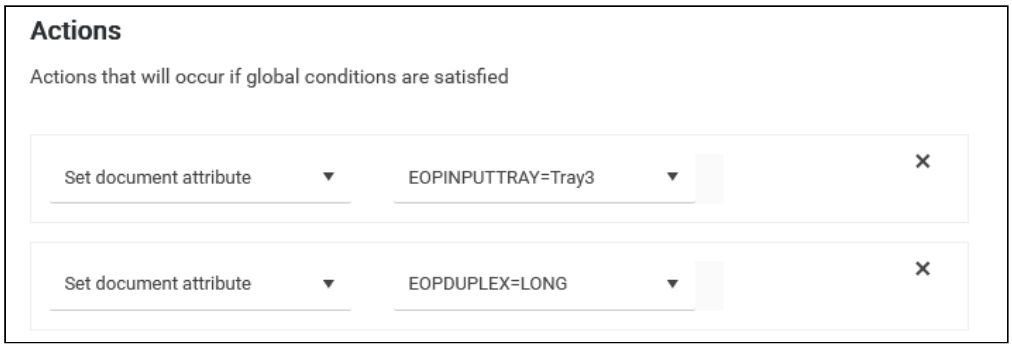
These two conditions should always be true.

Next, we create conditions that ensure we only run the trigger once (without these, the trigger would fire indefinitely):

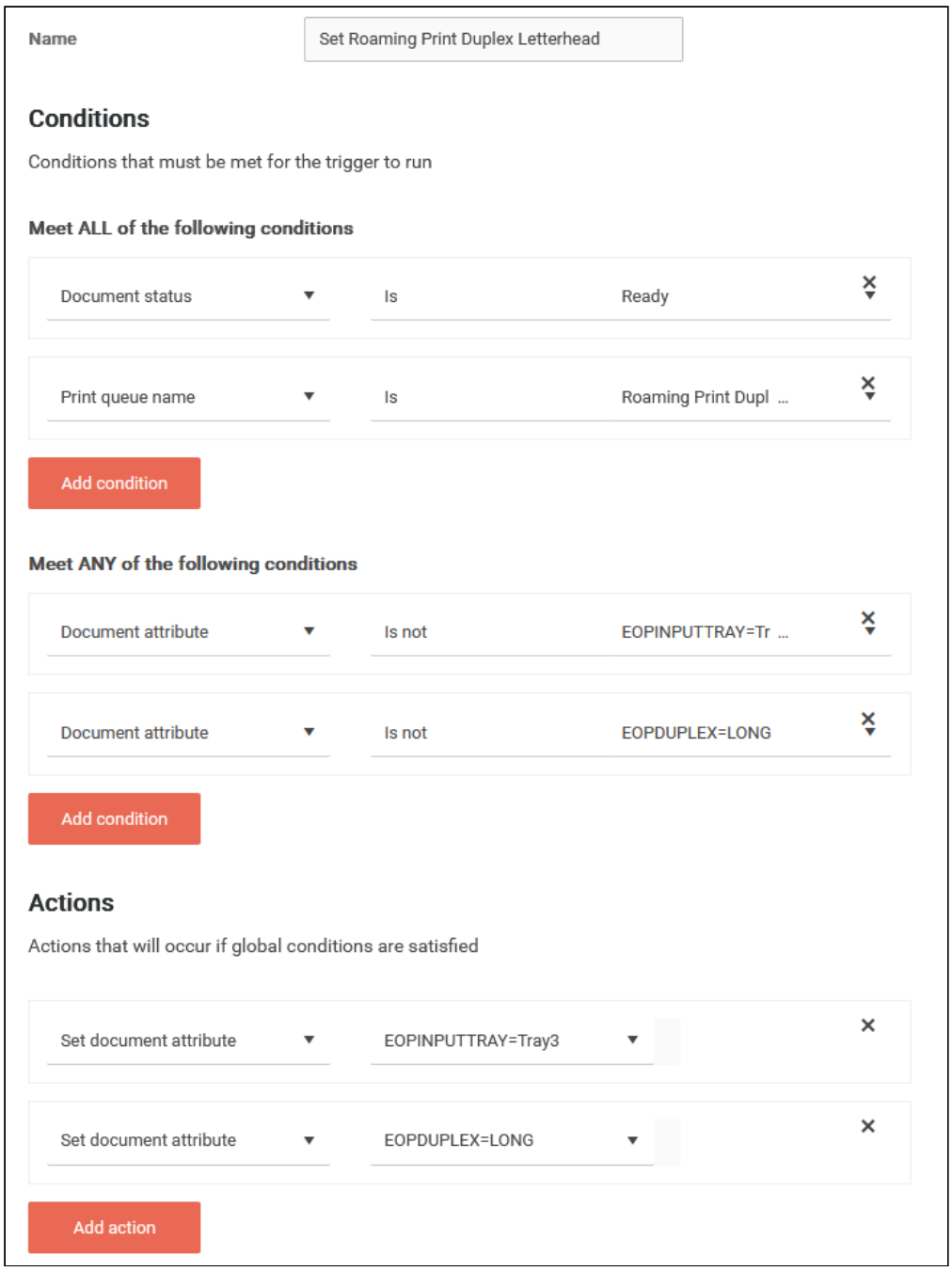
Document attribute is not EOPINPUTTRAY=Tray3
Document attribute is not EOPDUPLEX=LONG

If any of these are true, it means at least one of these things is not set on the job, so create the actions to set these document attributes:

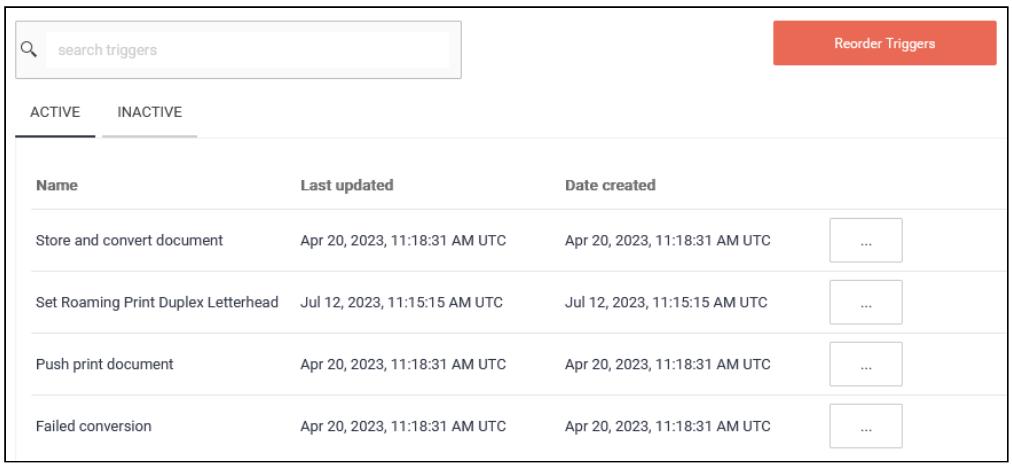
Set document attribute EOPINPUTTRAY=Tray3
Set document attribute EOPDUPLEX=LONG



Now our trigger is complete:



Save this trigger and move it after the **Store and convert document** trigger but before the **Push print document** trigger, so it doesn't fire unnecessarily before the job is actually received and before the job is sent to a Pull print queue (if the Print queue was a Pull print queue).



Remember that we created our trigger above so it fired based on the Print queue name, but this could have been configured to trigger based on group membership if other attributes or conditions are set, etc. The possibilities are endless, reach out to support, if you need help configuring this.

11.2.14 MIGRATE SAFEQ CLOUD BUNDLED POSTGRESQL DATABASE TO EXTERNAL POSTGRESQL DATABASE

This guide can also be useful when you are migrating SAFEQ Cloud from single primary server to high-availability cluster of primary servers which can be reliably utilized with minimum downtime duration and to avoid single point of failure..

> Apart from database migration, if you also require to migrate from SAFEQ Cloud single server to cluster server setup, please go through the article on how-to – Configure a primary server cluster

All steps from the section *Migrate database from existing SAFEQ Cloud server to external database* onward need to be performed in one go. It is recommended that you allocate a migration window during non-business hours to perform these tasks. For migration of the database, the recommendation is to have a standard 4 hours migration window.

Prerequisites/requirements for migration:

Before getting started, ensure that the below prerequisites are met -

- PostgreSQL database configured on the database server which will be used as an external database server. The following database details are needed for SAFEQ Cloud server:
  - Database host name or IP address
  - Database port,
  - Database username
  - Database password
- Make sure that all necessary ports are open for communication between SAFEQ Cloud and external database. Refer to Ports and Protocols section.
- Take full snapshot backup of existing SAFEQ Cloud server before proceeding with migration or take a complete backup of /opt/safeqcloud
- Have a Rollback plan in place in-case any issue comes up during migration.

Migrate database from existing SAFEQ Cloud server to external database

In this step we will describe how to migrate bundled PostgreSQL database from existing SAFEQ Cloud server to an external PostgreSQL database server.

> Before starting this step, ensure that communication to existing SAFEQ Cloud is stopped in order to avoid any data loss.
> One way to do this is to SSH into SAFEQ Cloud server and stop SAFEQ Cloud service by typing in following command – `sudo systemctl stop eopng-server.service`

> Contact Y Soft (support@ysoft.com) to get default db password if you do not know already

SSH into SAFEQ Cloud server and follow below steps to perform database migration -

1. Take backup of "eopng_config" database from the SAFEQ Cloud server using "pg_dump" utility. Run this command from terminal -

```
PGPASSWORD="<db_password>" /opt/safeqcloud/pgsql/bin/pg_dump -f /tmp/eopng_config_backup.dump -v -F t -b -c -C -h localhost -U postgres -p 7295 eopng_config
```

This will create backup file `eopng_config_backup.dump` in `/tmp` folder.

2. Take backup of "eopng_documents" database from the SAFEQ Cloud server. Run this command from terminal -

```
PGPASSWORD="<db_password>" /opt/safeqcloud/pgsql/bin/pg_dump -f /tmp/eopng_documents_backup.dump -v -F t -b -c -C -h localhost -U postgres -p 7295 eopng_documents
```

This will create backup file `eopng_documents_backup.dump` in `/tmp` folder.

3. Restore "eopng_config" database on external database server using "pg_restore" utility. Run this command from terminal –

```
PGPASSWORD="external_db_password" /opt/safeqcloud/pgsql/bin/pg_restore -C -v /tmp/eopng_config_backup.dump -h <external database server IP> -U postgres -p 5432 -d postgres
```

This will create database `eopng_config` on external PostgreSQL database server and migrate all data to it from dump file `eopng_config_backup.dump`.

**Note – you can use `-n public` switch in restore command if you want to restore only public schema (where SAFEQ Cloud data is)

4. Restore "eopng_documents" database on external database server using "pg_restore" utility. Run this command from terminal –

`PGPASSWORD="external_db_password" /opt/safeqcloud/pgsql/bin/pg_restore -C -v /tmp/eopng_documents_backup.dump -h <external database server IP> -U postgres -p 5432 -d postgres`

This will create database `eopng_documents` on external PostgreSQL database server and migrate all data to it from dump file `eopng_documents_backup.dump`.

**Note – you can use `-n public` switch in restore command if you want to restore only public schema (where SAFEQ Cloud data is)

5. Verify both databases have been migrated successfully.
Note – You can connect to external DB tools like DB Visualizer or Tableplus to verify contents of database

Change SAFEQ Cloud configuration to point to migrated external database

Before starting this step, ensure that full backup of SAFEQ Cloud folders **/opt/safeqcloud/conf** and **var/lib/eopng** has been taken.

1. In `applications.conf` file at location `/opt/safeqcloud/conf` change following JDBC settings for database schema config and documents to use migrated external database. Also update username and password as applicable.
You can specify password in plain text (for example: password = "mypass"). It will be re-encrypted after SAFEQ Cloud server restart.

```
url="jdbc:postgresql://<external_db_address>:5432/eopng_config"
url="jdbc:postgresql://<external_db_address>:5432/eopng_documents"
```

Below shown is example of database schema when connecting to external database –

```
config {
            password="<db_user_password>"
             poolsize=10
             timeout=30000
             url="jdbc:postgresql://<external_db_address>:5432/eopng_config"
             username=<db_user>
          }
documents {
             password="<db_user_password>"
             poolsize=10
             timeout=30000
             url="jdbc:postgresql://<external_db_address>:5432/eopng_documents"
             username=<db_user>
          }
```

2. Restart SAFEQ Cloud service. Type in following command – `sudo systemctl restart eopng-server.service`

3. Login to SAFEQ Cloud web UI and perform sanity checks to verify systems and health-checks are working as expected. Once you are satisfied with migration

Verification

After migration, perform sanity checks to verify systems and health-checks are working as expected. Recommendation is to -
1. Perform CRUD (create, read, update and delete) operations from SAFEQ Cloud Web UI to verify operations with external database is working as expected
2. Verify as applicable that the connections from SAFEQ Cloud gateways, SAFEQ Cloud Clients, embedded clients, Y Soft Mobile App are operational after migration

Rollback

If because of any reason the migration is not successful or if you encounter issues which needs troubleshoot time beyond migration window, rollback to use existing SAFEQ Cloud.

p(banner tip).If you have taken the snapshot backup of SAFEQ Cloud server before starting the migration procedures ,then please revert it so that you dont have to follow the below steps

1. Restore "application.conf" file from the backup taken before performing tasks in section 3
2. Restart SAFEQ Cloud service. Use command `sudo systemctl restart eopng-server.service`
3. Verify SAFEQ Cloud works as expected

When root cause analysis has been done for the issue encountered during migration and sufficient mitigation steps have been taken, try again from section 3

11.2.15 CARD ENROLLMENT / SELF-REGISTRATION

Prerequisites

To proceed with card enrollment, make sure that the embedded application is properly configured and installed on the MFD, and that the card reader is supported and set up correctly.

> For additional details please refer to the links provided in the 'Related information' paragraph at the end of this section.

Enrolling cards

Here are the steps to follow to enroll a new card:

1. When a new or unassigned card is swiped on the card reader, there will be displayed a new window that is confirming the start of the enrollment process (see picture examples below).
    a. If available, click the 'Enrollment' button.
2. Next, the user credentials will need to be provided
    a. In the 'Username' field enter the user ID for which you want the card to be assigned

b. In the 'Password' field enter the correct password for that user ID, or the One-Time Password (OTP) that was received by email or was manually set/generated within the SAFEQ Cloud portal (in the 'User' section or 'My Profile' section).

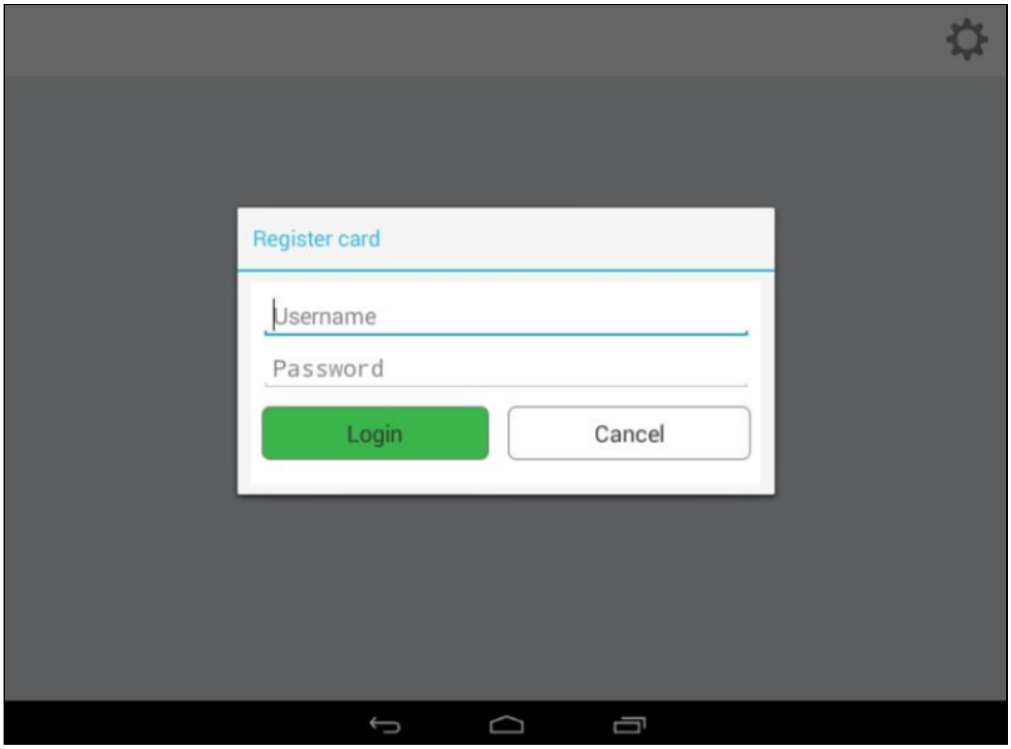
c. When Client Authentication is used, user has to be logged in via the SAFEQ Cloud Client first and obtain One-Time Password. Then use username/OTP to authenticate and complete the enrollment process.

3. Press 'Login'/'Register card'

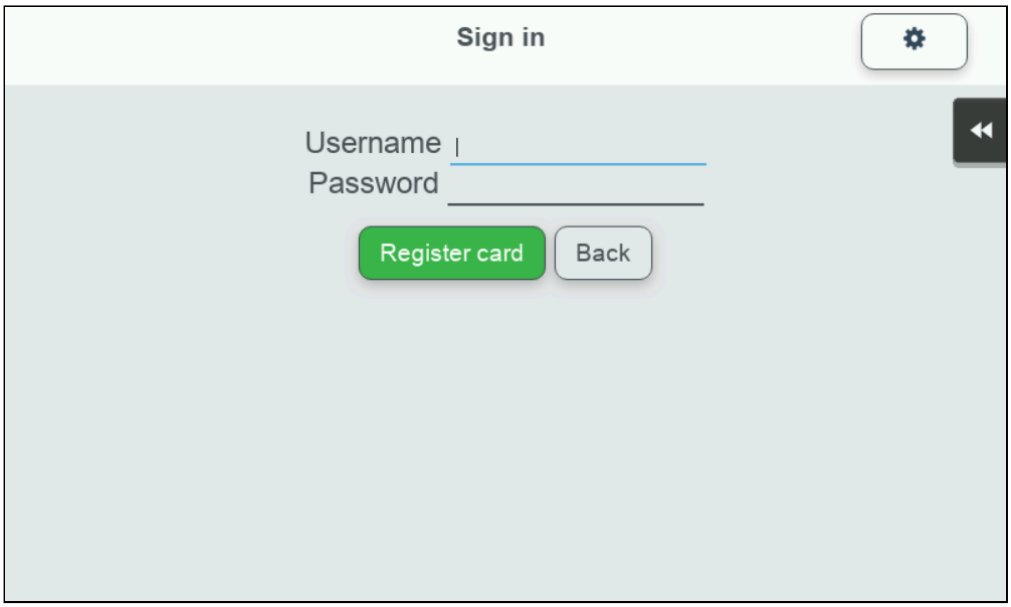
4. If the provided credentials are correct, the user should now appear as logged in and the card ID should be registered to this user.

Here are a few examples from embedded applications:

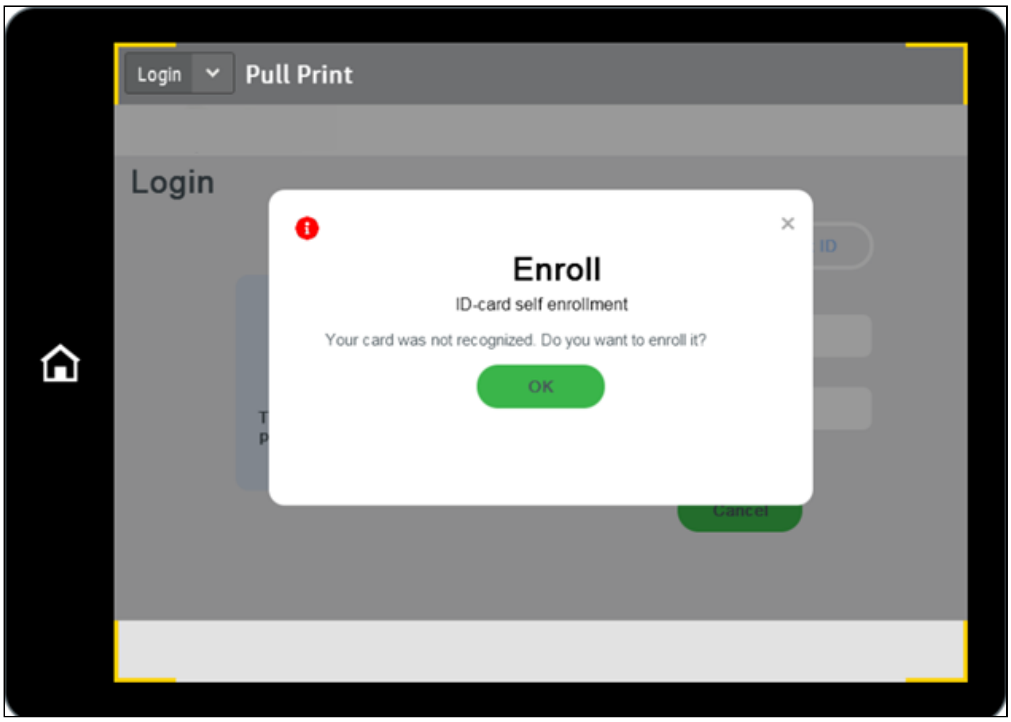
- HP Workpath:

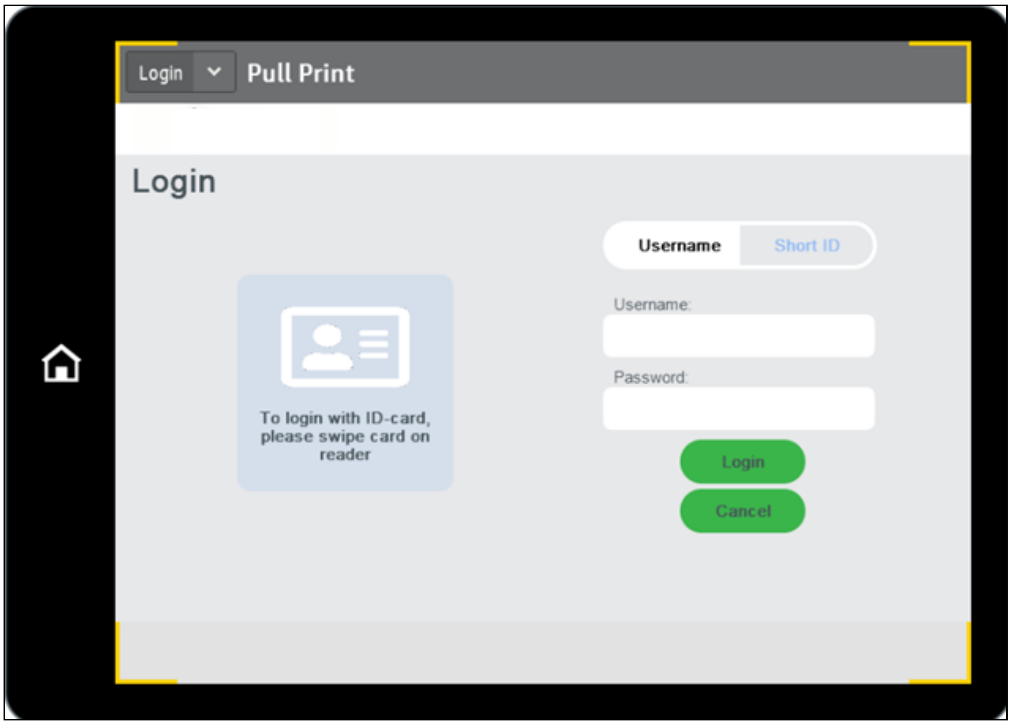


- KM IWS:



- HP Webclient:





Checking the assigned Card IDs for a user

To check the assigned card IDs:

- If the impacted user has the `EditMyProfile` permission, he can go to the SAFEQ Cloud portal, select the 'My Profile' section, then press 'Edit', and check the values inside the 'Cards' field.

- An administrator can go to the SAFEQ Cloud portal, find and 'Edit' the impacted user within the corresponding 'Users' section, and check the values inside the 'Cards' field.

Note: If you set the authentication provider to provide the Card Id via the custom attributes, you still can register your cards in the system. However, card numbers will be stored internally in SAFEQ Cloud and won't be synchronized with the data source.

Related information:

- Embedded configuration
- Supported card readers
- My profile

11.2.16 USE YOUR OWN DOMAIN NAMES FOR SAFEQ CLOUD HOSTED ACCOUNTS

Customers or partners hosting with Y Soft, in the YSoft SAFEQ Cloud clouds in any of our regions, are automatically given a domain name such as "customername.eu.ysoft.cloud".

To create your own custom domain names, create CNAME records from your domain name to the account domain, such as:

```
print.customername.com CNAME customername.eu.ysoft.cloud
```

Make sure you upload a proper certificate for "print.customername.com" to the SAFEQ Cloud Web admin portal -> Certificates.

11.2.17 CONFIGURE SAFEQ CLOUD ENVIRONMENT WITH TRUSTED CERTIFICATES

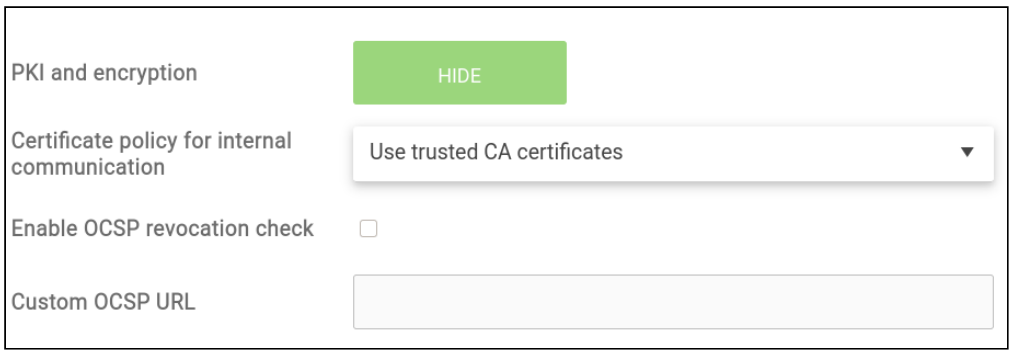
Certificates overview

The internal communication between the secondary gateways and the primary server and also between the SAFEQ Cloud Clients in local storage mode and the primary server is protected with TLS encryption.

By default the built-in SAFEQ Cloud certificates are used for that and the user must explicitly authorize each of the gateway or SAFEQ Cloud Client before it can connect to the primary server. SAFEQ Cloud uses mutual TLS authentication, meaning that the primary server checks the certificates of the connecting clients and every client also checks the server certificate to which it connects. This is different from the common web browser behavior and requires an elaborated setup which is explained in this chapter.

> When trusted certificate policy is enabled the endpoint authorization mechanism is no longer used and it is not necessary to authorize each Client manually.

Trusted certificate policy can be set on the account level under account settings, PKI and encryption section:



Two OCSP settings are related to the certificate revocation protocol. They should be used in the way instructed by the corporate PKI administrator.

Setup preparation

In this example we assume the following setup: one on-premise primary server, one gateway, one SAFEQ Cloud Client. For each of them a separate certificate chain must be prepared which might look like this:

```
Acme-CA-Root
    Acme-CA-Intermediate
        primary-host
```

```
Acme-CA-Root
    Acme-CA-Intermediate
        gateway-host
```

```
Acme-CA-Root
    Acme-CA-Intermediate
        pcclient-host
```

Here we have three certificate chains, for the primary server, for the gateway and a SAFEQ Cloud Client. Each certificate chain consists of two CA certificates (root and intermediate) and an entity certificate which corresponds to it's usage. In the production environment it is possible that multiple intermediate certificates are used or no intermediate certificates at all.

If the cloud primary server is used the first setup step can be skipped, in this case the certificate chain for the primary server is not needed.

For server and gateway the chains must be exported to a PFX (PKCS12) file. For SAFEQ Cloud Client running on Windows the chain should be placed into Windows certificate store.

Primary server setup

This step is only needed if primary server is hosted in the customer's network. We assume that the certificate chain from the above example is exported to "primary-host.pfx" file and the password for it is "changeit".

Configuration steps:

- Copy the primary-host.pfx file to the primary server, under `/opt/safeqcloud/conf` directory (for example by using any of SSH/SFTP utilities)
- Make sure this file is readable, e.g. has `-rw-r--r--` permissions
- Open the `/opt/safeqcloud/conf/application.conf` file in the editor (please don't use standard notepad application as it might corrupt the file), locate and change the following two settings:
  - `default-keystore-file = "/opt/safeqcloud/conf/primary-host.pfx"`
  - `default-keystore-password = "changeit"`
- Restart primary server with `systemctl restart safeq-cloud-server`
- Validate that the certificate is used correctly with openssl command: `openssl s_client -servername primary-host -connect localhost:2560`, where primary-host should match the hostname from the certificate. The command should dump the correct server certificate on the console. If it returns a fallback "localhost" instead please check the above two settings are correct, the pfx file is readable and the password matches.

If the root CA certificate is not issued by the global certificate authority it must be added also to standard Java cacerts keystore with the following command:

```
sudo /opt/safeqcloud/jre/bin/keytool -importcert -file cacert.crt -keystore /opt/safeqcloud/jre/lib/security/cacerts
```

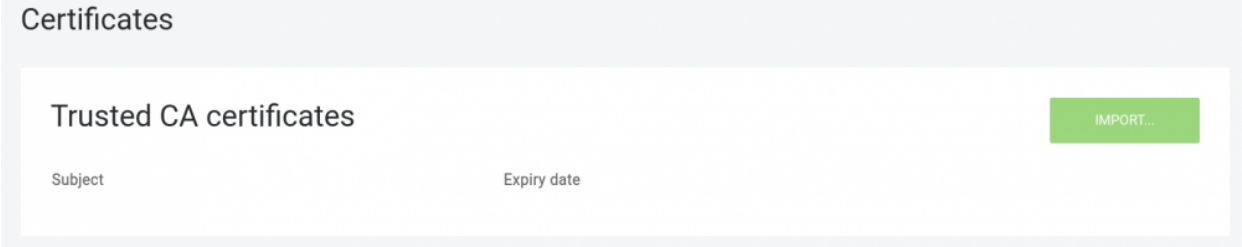
Where cacert.crt contains a root certificate (Acme-CA-Root). The password for the cacerts file is "changeit". When prompted whether to trust the added certificate please type "yes" and press enter.

Account setup in the SAFEQ Cloud web portal

The `Certificate policy for internal communication` option should be set to `Use trusted CA certificates`, as shown on the above picture.

If the CA certificates are not issued by the global certificate authority but by the corporate PKI they must be marked as "trusted" in the SAFEQ Cloud server:

1. Export all CA certificates from the certificate chain into separate .cer or .der files. So the Acme-CA-Root and Acme-CA-Intermediate must be exported to separate files in X.509 encoded format (could be also base64).
2. Under CERTIFICATES section in the account settings import those CA certificates under "Trusted CA certificates" panel:



If CA certificates are the global ones (e.g. Digicert, Globalsign, etc) there is no need to import them as they are part of the standard trusted CA bundle.

Primary server is now ready to accept connections from trusted clients.

Setting up gateway in unattended mode

If the root CA certificate of the primary server is not issued by the global certificate authority it must be added to a truststore and this truststore must be specified in the unattended installation file, so that the gateway will trust the primary certificate to which it connects. The truststore is a PKCS12 file which can be created using Java keytool command: `keytool -importcert -file acme-ca.cer -alias acme-ca -storetype PKCS12 -keystore acme-ca.pfx`. This command will produce acme.ca.pfx file which can be specified as a truststore for the gateway installation.

In the unattended configuration file please specify the following options:

```
HCP_DEFAULT_KEYSTORE="/full/path/to/gateway-host.pfx"
HCP_DEFAULT_KEYSTORE_PASSWORD="gateway-pfx-password"
HCP_DEFAULT_TRUSTSTORE="/full/path/to/acme-ca.pfx"
HCP_DEFAULT_TRUSTSTORE_PASSWORD="acme-ca-pfx-password"
```

Setting up SAFEQ Cloud Client for trusted connection

Before installing or configuring the SAFEQ Cloud Client make sure the Windows certificate store contains the correct certificate chain. See the first paragraph for an example of the chain. Refer to Installing SAFEQ Cloud Client on Windows chapter for details. When installing SAFEQ Cloud Client enable the local storage mode and `Use pre-configured system certificate for secure communication` option and specify the subject of the entity certificate or of it's issuer (CA certificate). This can be a substring. SAFEQ Cloud Client will use this certificate for communication with the server.

> If local storage mode is not used in the SAFEQ Cloud Client the trusted certificate setup is not needed.

If the SAFEQ Cloud Client can connect to the server the notification icon will have an idle gray color. If it is yellow it means there is a network issue or the certificate setup is not correct. Please check the SAFEQ Cloud Client log file under `C:\ProgramData\safeqclientcore\logs\safeqclientcore.log`. Make sure all root and intermediate CA certificates are imported into SAFEQ Cloud as previously described.

11.2.18 CONFIGURE DENIAL OF SERVICE FILTERING FOR WEB UI

Introduction

SAFEQ Cloud server has a possibility to enable denial of service (DoS) filtering to prevent the system from being overloaded by excessive amounts of requests. DoS filter can be enabled for

on-premise primary server by editing the configuration file: `/opt/safeqcloud/conf/application.conf`.

DoS filter configuration

Multiple DoS filters can be defined under `app.dos-filters` section in the application configuration file. By default there is one filter defined called `default`:

```
dos-filters {
    default {
        delay-ms=100
        ip-whitelist=[]
        max-idle-tracker-ms=30000
        max-request-ms=30000
        max-requests-per-sec=25
        max-wait-ms=50
        remote-port=false
        throttle-ms=30000
        throttled-requests=5
        track-sessions=true
    }
}
```

To activate the particular DoS filter it must be specified in the `dos-filter` parameter under `web` section:

```
    web {
        # dos-filter = ${app.dos-filters.default}
        dos-filter=""
        port=8080
        ssl {
            enable-protocols=[
                "TLSv1.2",
                "TLSv1.3"
            ]
            exclude-cipher-suites=[
                "SSL_RSA_WITH_RC4_128_MD5",
                "SSL_RSA_WITH_RC4_128_SHA",
                "TLS_ECDHE_RSA_WITH_RC4_128_SHA",
                "TLS_DHE_RSA_WITH_AES_128_CBC_SHA",
                "TLS_DHE_RSA_WITH_AES_128_CBC_SHA256",
                "SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA"
            ]
            port=8443
        }
    }
}
```

Comment out the `dos-filter = ""` line (add the # sign) and uncomment the `dos-filter = ${app.dos-filters.default}` (remove the # sign).

Save the file and restart the server with `systemctl restart safeq-cloud-server` command.

DoS filter parameters

The following parameters control the behavior of the filter:

- `max-requests-per-sec` – Maximum number of requests from a connection per second. Requests in excess of this are first delayed, then throttled. Default is 25.
- `delay-ms` – Delay imposed on all requests over the rate limit, before they are considered at all: 100 (ms) = Default, -1 = Reject request, 0 = No delay
- `max-wait-ms` – Length of time, in ms, to blocking wait for the throttle semaphore. Default is 50 ms.
- `throttled-requests` – Number of requests over the rate limit able to be considered at once. Default is 5.
- `throttle-ms` – Length of time, in ms, to async wait for semaphore. Default is 30000.
- `max-request-ms` – Length of time, in ms, to allow the request to run. Default is 30000.

- `max-idle-tracker-ms` – Length of time, in ms, to keep track of request rates for a connection, before deciding that the user has gone away, and discarding it. Default is 30000.
- `track-sessions` – If true, usage rate is tracked by session if a session exists. Defaults to true.
- `remote-port` – If true and session tracking is not used, then rate is tracked by IP and port (effectively connection). Defaults to false.
- `ip-whitelist` – A comma-separated list of IP addresses that will not be rate limited.