KONICA MINOLTA

Dispatcher Paragon Cloud

Dispatcher Paragon Cloud documentation

Giving Shape to Ideas

CONTENT

Welcome to Dispatcher Paragon Cloud documentation. The documentation is divided into four sections for the four types of target audiences:

Partner admins: Go to the Deployment guide section. It contains information on registering a new customer in Dispatcher Paragon Cloud.

Customer admins: Go to the Configuration and administration guide section. It contains steps to take after your company was registered in Dispatcher Paragon Cloud, i.e. after receiving the *Welcome to Dispatcher Paragon Cloud* email.

End users: Go to the End user guide section.

Solution architects: Go to the Architecture and solution design section.

1 DEPLOYMENT GUIDE

This Deployment guide is intended only for Partner admins. If you are a customer admin, go to Configuration and administration guide.

1.1 DOCUMENTATION CHANGELOG - RELEASE 2023.01.26

What's new	Where
Added that Client v3 installation package for Mac can be created in Quick Print.	Creating Dispatcher Paragon Client v3 installation packages, section *Installation options*.

1.2 GENERAL INFORMATION

1.2.1 ABOUT THIS GUIDE

This guide contains information on the deployment of Dispatcher Paragon Cloud – see the Deployment process.

If you need some pieces of information intended for customer admins and end users, you can find them in Configuration and administration guide and End user guide respectively.

How to read this guide

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.

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.

Terms and definitions

Term	Description
Dispatcher Paragon Cloud	A cloud-based print management service.
Dispatcher Paragon Cloud Terminal	An application provided by the Konica Minolta MarketPlace. This application enables communication between an MFD and the cloud.
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 Dispatcher Paragon Cloud.
YSoft OMNI Bridge	YSoft OMNI Bridge is a piece of hardware manufactured by Y Soft.
YSoft OMNI Bridge Site Server	YSoft OMNI Bridge configured to serve as an Edge device providing local site services.

Term	Description
Pure Cloud printing	A service with architecture (printing method) based on MFDs that support the Dispatcher Paragon Cloud Terminal. 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 Dispatcher Paragon Cloud).
MFD	Multi-function device (a copier).
SFD	Single-function device (a printer).
Reporting-only devices	MFDs or SFDs where the customer wants to capture the number of printed pages (and related statistics) but does not need any other capability such as Embedded Terminal or Cloud Terminal or print roaming, and so on.
Card Activation Code Provider page (CACP)	A web service allowing users to assign cards to their Dispatcher Paragon Cloud accounts using their Azure Active Directory accounts.
IPP Gateway	IPPS server for print job submission by users to their personal secure queues in Dispatcher Paragon Cloud.
Dispatcher Paragon Cloud management interface	A web interface used by administrators to manage their product instance centrally, and by end users to manage their accounts. It displays information and functions as per the role of the individual logged in. The Management interface runs via the Management service.

Term	Description
Dispatcher Paragon Portal	A web portal for Partners allowing them to manage their partner structure and download documentation. https://paragon.konicaminolta.com
Dispatcher Paragon Cloud Portal	A web interface for partner admins to register new Customers. To log in to Dispatcher Paragon Cloud Portal, you need a Dispatcher Paragon Portal user account with specific privileges. Customer admins have access to Dispatcher Paragon Cloud Portal if they have a specific role in their Azure AD. They have a different view in the Cloud Portal than partner admins. https://dipa.cloud
Konica Minolta MarketPlace	Konica Minolta's service for browsing, purchasing and downloading applications to MFDs.

Personas and roles

Persona	Description	Which role(s) in Dispatcher Paragon Cloud management interface can this person have?
Managed Service Provider (MSP)	The role with the highest set of privileges in the Dispatcher Paragon Cloud service, responsible for service availability and maintenance. Has access to all customer settings. Is responsible for Dispatcher Paragon Cloud Portal maintenance, monitoring, deployment of updates etc.	System admin
Partner	A partner of MSP. It can also be a reseller (a partner of a partner).	see *partner admin*

Persona	Description	Which role(s) in Dispatcher Paragon Cloud management interface can this person have?
Customer	The customer of a partner and, at the same time, a representation of the customer in the Dispatcher Paragon Cloud Portal. This representation is sometimes called Tenant. Each Customer has its own admin. This can be the partner admin or the customer admin. See the *Personas and roles* section below.	see *customer admin*
Partner admin	An administrator in the Dispatcher Paragon Cloud management interface who can (if agreed with the customer) manage devices, users, and some of the system settings.	Customer admin system role is the highest-level role this person can have.
Customer admin	An administrator on the customer side with rights to manage settings in Dispatcher Paragon Cloud management interface.	Customer admin system role is the highest-level role this person can have. Other than that, any kind of role is available, depending on the agreement between the Partner and the Customer.
End user	A persona within a Customer's Dispatcher Paragon Cloud instance that is permitted to print/copy/scan.	Any role that the administrator assigns to them.

1.2.2 ABOUT DISPATCHER PARAGON CLOUD

Dispatcher Paragon Cloud is a full-featured print management solution on a shared and hosted infrastructure for small and medium-size businesses. With compatible MFDs, Dispatcher Paragon Cloud can be used as a pure cloud solution. With incompatible MFDs, it can couple an on-site Edge serverless device with a secure shared application in the public cloud, where print system metadata is stored and analyzed.For more information see Basic scenarios.

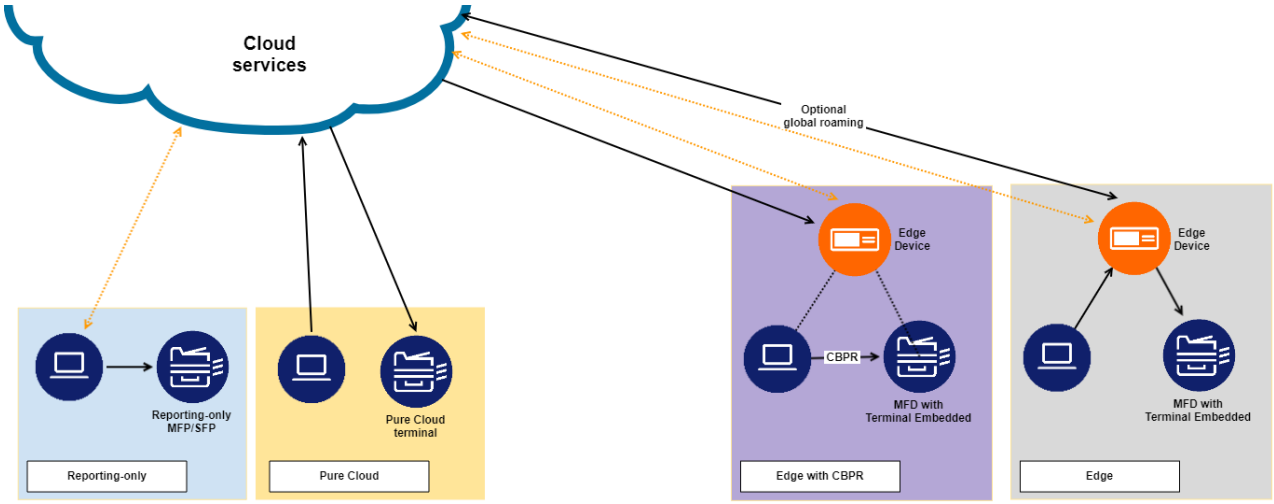
1.2.3 ABOUT YSOFT OMNI BRIDGE

Edge and pure cloud printing are options for Dispatcher Paragon Cloud. Choose Edge if your customers need higher availability and compliance with local data residency preferences/ regulations, as the print job data remain on the edge device and are not transferred to the cloud. Furthermore, print job speed is unaffected by the cloud connection or latency of the connection. In order for customers to take advantage of the full feature set of Dispatcher Paragon Cloud, they will need YSoft OMNI Bridge edge device(s) to make their on-site terminals cloud-enabled.

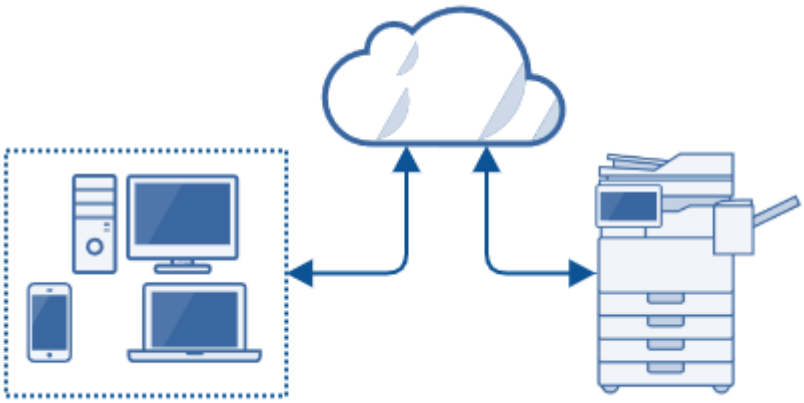
For details on how to work with the device, see YSoft OMNI Bridge operation manual.

1.3 BASIC SCENARIOS

Customers can choose from the following scenarios how to deploy Dispatcher Paragon Cloud in their locations, or they can mix them, as all of these scenarios can co-exist in one environment. For more details, see Architecture and solution design.



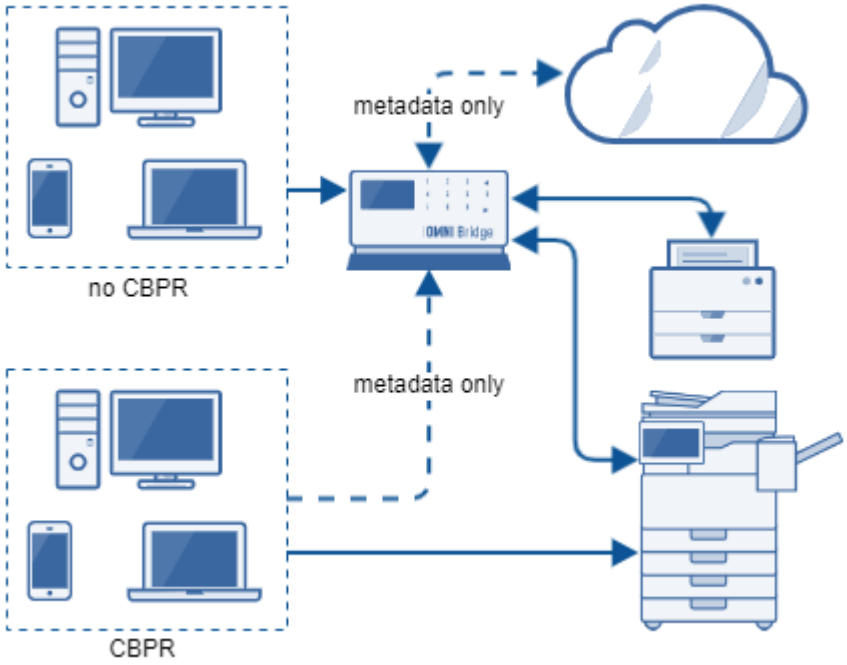
1.3.1 PURE CLOUD PRINTING



Pure Cloud printing characteristics:

- No VPN required
- No on-premise infrastructure needed
- Complies with zero trust network security principles
- No client SW required on workstations (but optionally, it is available)
- Platform-independent (Windows, Linux, Mac)
- For requirements, see Requirements.

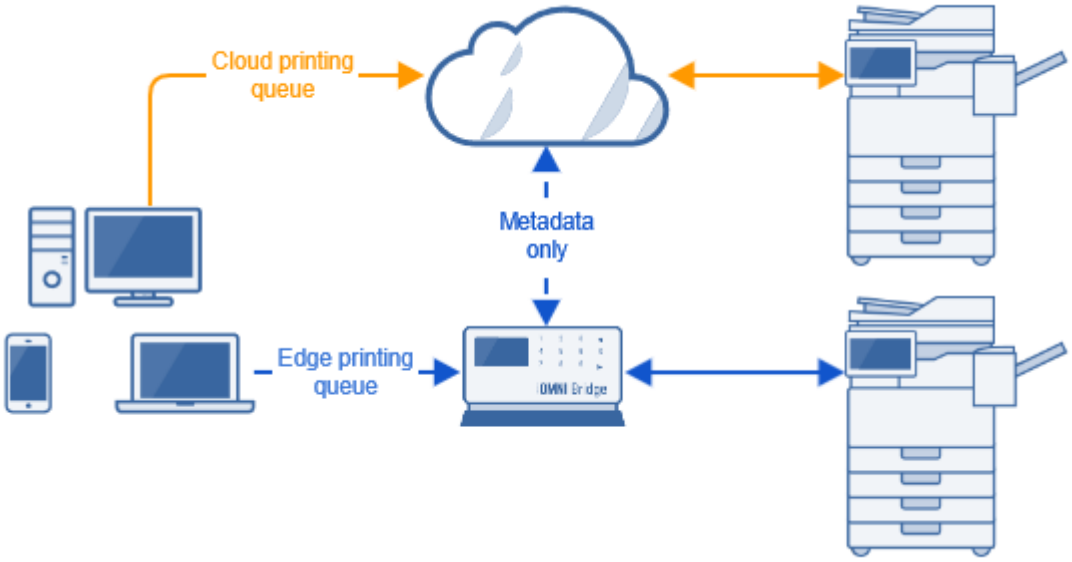
1.3.2 EDGE PRINTING



Edge printing characteristics:

- Print jobs do not leave the customer's network
- A higher number of supported Konica Minolta MFD types
- Lower network bandwidth consumption – print jobs are not transferred to the cloud and back
- Emergency printing when Client-based print roaming (CBPR) is used – users can keep printing even if an edge device is down

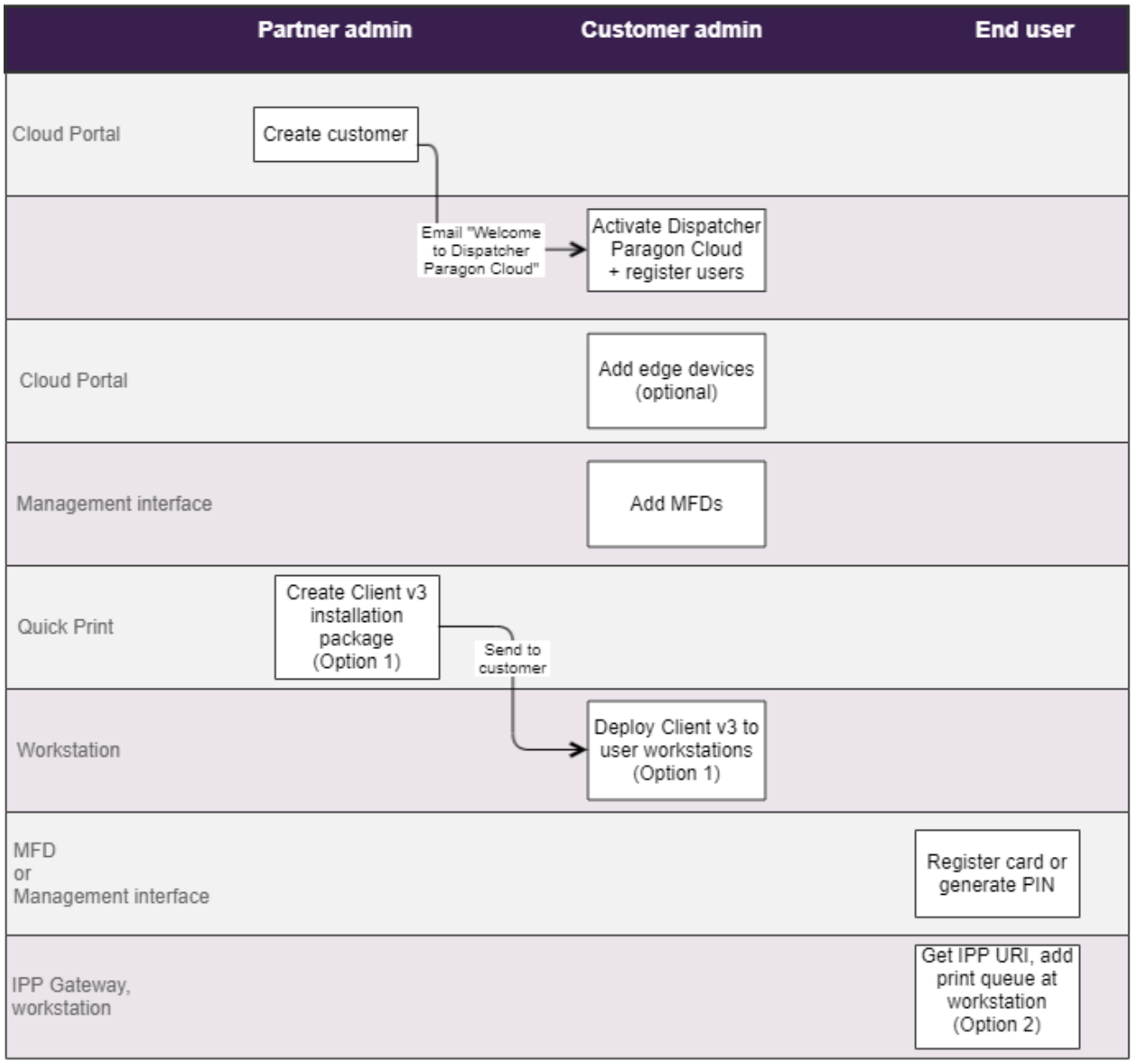
1.3.3 HYBRID PRINTING



1.4 DEPLOYMENT PROCESS

This chapter a high-level overview of the standard deployment process. Follow the links to the respective chapters in the documentation to see the complete set of instructions for each of the steps in this overview.

A diagram of the most common deployment scenario (customer manages Dispatcher Paragon Cloud themselves, has Externally managed users, registers them all at once). For other scenarios and options, see the steps and links listed below.



Option 1 = usage of Client v3

Option 2 = usage of manually added print queues

1.4.1 STEPS FOR PARTNER ADMIN

1. Register your customer at the Dispatcher Paragon Cloud Portal. See Registering a new customer.
2. During the registration process, you will have an option to grant access to customer's Dispatcher Paragon Cloud Management interface to partner technical contact, so that they can help the customer with setup. In this case, the partner technical contact should follow

Activating your admin account as partner admin and Accessing Dispatcher Paragon Cloud management interface as partner admin.

3. If the customer will be using Dispatcher Paragon Client v3, create the installation package(s) and send them to the customer. See Creating Dispatcher Paragon Client v3 installation packages.

4. If you wish to test the Edge printing scenario for yourself, or to demonstrate it to a customer, you must import CA certificate for IPP Gateway into your workstation. See How to import CA certificate for Edge printing to your workstation.

1.4.2 STEPS FOR CUSTOMER ADMIN

1. Activate your Dispatcher Paragon Cloud. See Activating your Dispatcher Paragon Cloud.

2. Set up your access to Dispatcher Paragon Cloud Portal. Use the **Manage account** button in your *Welcome to Dispatcher Paragon Cloud* email.

   a. Externally managed users: see Dispatcher Paragon Cloud Portal guide and Tenant admin role for accessing Dispatcher Paragon Cloud Portal.

   b. Internally managed users: you will be able to access the Dispatcher Paragon Cloud Portal immediately after activating your Dispatcher Paragon Cloud.

3. For Pure Cloud printing scenario:

   - Prepare your MFDs for installation of the Dispatcher Paragon Cloud Terminal. See Configuring Konica Minolta MFDs for Dispatcher Paragon Cloud Terminal.
   - Install the Cloud Terminal from the Dispatcher Paragon Cloud management interface. See Managing devices.

4. For Edge printing scenario:

   a. Prepare your YSoft OMNI Bridge. See Preparing your YSoft OMNI Bridge.

   b. Configure the YSoft OMNI Bridge as a site server. See Managing Edge devices.

   c. Install the Embedded Terminal on the MFDs connected to your YSoft OMNI Bridge. See Managing devices.

   d. Download the CA certificate and deploy it to user workstations. See Managing Edge devices, section *Downloading CA certificate*.

5. Manage print queues:

   a. Client v3: if you agreed with your service representative that your company will be using Dispatcher Paragon Client v3, deploy the Client v3 to users' workstations.

   b. Manually created print queues: if you won't be using Client v3, provide the end users with the following:

1. The link to IPP gateway.
2. How to configure the print queues, see Configuring IPP print queues.
3. Which print drivers to use when configuring their print queues. For best compatibility, we recommend PCL5.

6. Manage users:
   a. If your company's users are going to be Internally managed users, invite them from Dispatcher Paragon Cloud Portal. See Internally managed users. They will need to register themselves. See the *End user guide*, chapter Registering yourself in Dispatcher Paragon Cloud.
   b. If your company's users are Externally managed users, they were all registered during Dispatcher Paragon Cloud activation.
   c. To be able to log in at MFDs and release their print jobs, both types of users must either register their cards at MFDs (see the End user guide, chapter Card registration at the MFD terminal) or generate a PIN (see the End user guide, chapter Management interface guide, section *Generating a PIN*).
7. Send the End user guide to the end users.

1.5 REQUIREMENTS

1.5.1 GENERAL PREREQUISITES FOR PURE CLOUD PRINTING

- Customer's MFDs are compatible with Dispatcher Paragon Cloud.
- MFD firmware is updated to the specific version which supports Dispatcher Paragon Cloud.
- The MFDs have a loadable device driver installed.
- The customer has Konica Minolta MarketPlace account.

1.5.2 NETWORK REQUIREMENTS FOR PURE CLOUD PRINTING AND EDGE PRINTING

This section provides information about ports and protocols that must be enabled on firewalls and other related security aspects to ensure safe usage of the solution.

Bandwidth and Latency

Bandwidth and latency must be considered for each implementation:

- Latency is important to be kept under 100ms for metadata synchronization in Site Server cluster locations and for user experience on all browser-based terminals (i.e. between where the MFD is and its respective Terminal Server).

- The bandwidth required is vastly dependent on print job data size. Print job metadata traveling among components averages around 40–60 kB per print job.

Network communication overview

The following tables provide a complete list of the ports and protocols that must be enabled on firewalls in order to ensure system functionality.

⚠ YSoft OMNI Bridge cannot be set up in a proxy environment.

ⓘ The customer network is expected to allow access to the below-mentioned services over the Internet, including name resolution (DNS).

Cloud Environment

All below services are hosted on *.dipa.cloud domain.

Client side	Server side	Unsecured server side port	Secured server side port	Application protocols	Network protocols	Transferred data
User	Management	n/a	443	HTTPS	TCP	User credentials, settings, user data
User	Cloud Portal	n/a	443	HTTPS	TCP	User credentials, cloud provisioning
User	Status page	n/a	443	HTTPS	TCP	Cloud health check data
User	Card Activation Code Provider	n/a	443	HTTPS	TCP	User credentials, card data

Client side	Server side	Unsecured server side port	Secured server side port	Application protocols	Network protocols	Transferred data
User	IPP Gateway	n/a	443	HTTPS	TCP	User credentials, user print queue information

Cloud terminals

Dispatcher Paragon Cloud Terminal

Client side	Server side	Unsecured server side port	Secured server side port	Application protocols	Network protocols	Transferred data
MFD	Cloud Site Server (Terminal Server)	n/a	443	WebDAVS	TCP	Scanned document
MFD	Cloud Site Server (Terminal Server)	n/a	443	HTTPS	TCP	User credentials (card number), Configuration change, remote control commands, print job data
MFD	KM Marketplace	n/a	443	HTTPS	TCP	User credentials, App data
USB card reader	MFD/PC	n/a	n/a	Proprietary		User credentials (card number), Configuration change, remote control commands, firmware update

Cloud Site Server (Workflow Processing System)	Mail Server	n/a	n/a	SMTP/ SMTPS	TCP	Scanned data
System spooler (Windows)	Cloud Site Server (Spooler)	n/a	443	IPPS	TCP	Job data
System spooler (MacOS)	Cloud Site Server (Spooler)	n/a	443	IPPS	TCP	Job data

Edge Terminals

Client side	Server side	Unsecured server side port	Secured server side port	Application protocols	Network protocols	Transferred data
Edge Device	Management interface	n/a	443	HTTPS	TCP	Metadata synchronization, reports,
Embedded terminal for Konica Minolta, Develop, Olivetti	Edge Device (Terminal Server)	5021	5014, 5015, 5016, 5017, 5018, 5019, 5022	SOAP/ HTTPS	TCP	All device communication data, e.g. user credentials
MFD	Edge Device (Terminal Server)	20, 21, 1024-65535	n/a	FTP	TCP	Scanned document
MFD	Edge Device (Terminal Server)	User-defined	User-defined	WebDAV/ WebDAVS	TCP	Scanned document

User/LPD Windows Spooler	Client spooling/ Edge Device spooling	515	n/a	LPR	TCP	Job data
Other app (e.g. SAP) LPR printing	FlexiSpooler server spooling/Edge Device spooling	515	n/a	LPR	TCP	Job data
Client v3	Server spooling/Edge Device spooling	9100	n/a	TCP/IP raw/jet direct	TCP	Username and domain, job data
Edge Device (Terminal Server)	MFD (Konica Minolta)	50001	50003	HTTP/ HTTPS	TCP	Terminal installation process
Edge Device (Terminal Server)	MFD (Konica Minolta)	User-defined	User-defined	SNMP		Device control (e.g. job deletion)
Edge Device	IoT Hub Device Provisioning Service (DPS) worldwide endpoint	n/a	443	HTTPS	TCP	Edge Device provisioning
Edge Device	IoT Hub Using IoT Hub in the West Europe region only	n/a	443	HTTPS	TCP	Edge Device provisioning

Edge Device	Azure Central Registry (ACR) Using ACR in the West Europe region only	n/a	443	HTTPS	TCP	Edge Device provisioning
Edge Device	DNS	53		DNS	UDP	Domain Name Resolution
YSoft OMNI Bridge	Google NTP servers (or custom defined)	n/a	123	NTP	UDP	Edge Device provisioning
Edge Device (Spooler Controller)	MFD (Konica Minolta)	80	443	IPP/ IPPSSL	TCP	Device status information
USB card reader	MFD/PC	n/a	n/a	Proprietary		User credentials (card number), Configuration change, remote control commands, firmware update
Edge Device/ Client when client spooling	MFD	515/9100/ 80	443/631	LPR/ RAW/ IPP/ IPPS	TCP	Job data
Spooler	MFD	User-defined	User-defined	JetDirect, IPP, IPPS	TCP	Job data

Edge Device (Workflow Processing System)	Mail Server (Sendgrid cloud service)	n/a	n/a	SMTP/ SMTPS	TCP	Scanned data
System spooler (Windows)	Edge Device (Spooler)	515/631	632	LPR, IPP, IPPS	TCP	Job data
System spooler (MacOS)	Edge Device (Spooler)	5515/5631	5632	LPR, IPP, IPPS	TCP	Job data
edge-config-application	edge-remote-site-server-config		HTTPS + AMQP		TCP	Configuration + CSR and certificates
User	IPP Gateway	n/a	443	HTTPS	TCP	Configuration + CSR and certificates
Edge Device (Spooler & Print Job Storage)	Keycloak	n/a	443	HTTPS	TCP	Access token and refresh token requests and responses for service accounts. Authentication is based on client certificates.
Edge Device (Print Job Storage)	Print Job Storage	n/a	443	HTTPS	TCP	Job data

External domains

The following external domains and their communication ports must be allowed in the customer's network firewall for the edge devices to function correctly.

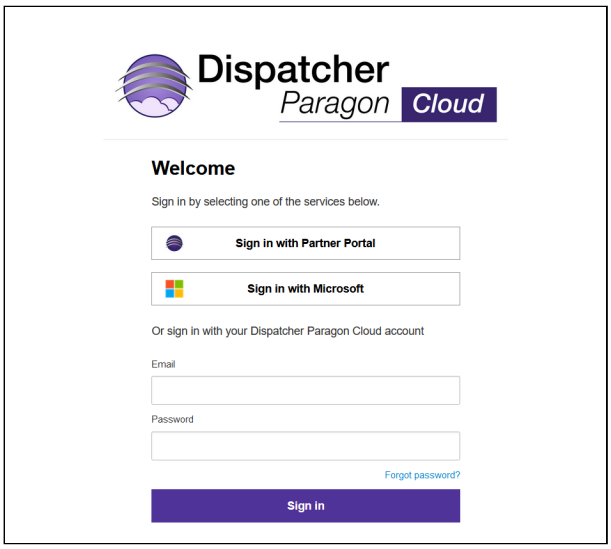
FQDN (* = wildcard)	Outbound TCP Ports	Used for
mcr.microsoft.com	443	Microsoft Container Registry
*.data.mcr.microsoft.com	443	Data endpoint providing content delivery
*.cdn.azcr.io	443	Deploy modules from the Marketplace to devices
global.azure-devices-provisioning.net	443	Device Provisioning Service 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, 443	IoT Hub access
*.docker.io	443	Docker Hub access (optional)
*.dipa.cloud	443	Dispatcher Paragon Cloud Services
*.ysoft.cloud	443	Dispatcher Paragon CodeFlow
*.google.com	UDP 123	NTP server (time{1-12}.google.com) or any chosen NTP server

1.6 REGISTERING A NEW CUSTOMER

To register a new customer in Dispatcher Paragon Cloud Portal, perform the following steps:

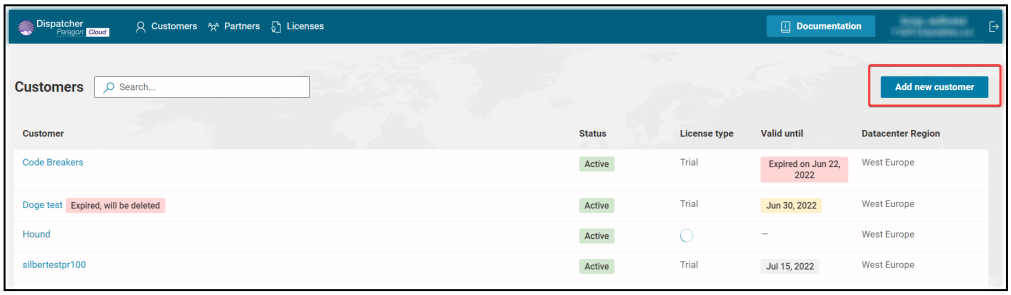
1. Go to https://dipa.cloud.

2. Click **Sign in with Partner Portal**. This will take you to Dispatcher Paragon Portal login screen.



3. Enter your credentials for Dispatcher Paragon Portal and click **Sign in**.

4. Navigate to the **Customers** tab and click **Add new customer**.



5. Enter the customer information:

   a. **Customer name**

   b. **URL prefix** – All customer's service addresses and URLs in Dispatcher Paragon Cloud will be prefixed with this. For example, if you use "example" as a URL prefix, the MFD and workstation endpoints will be in the form *https://example-tenant.eu1.dipa.cloud* or *https://management.eu1.dipa.cloud/login/example*. The prefix has to be unique for the customer across all cloud infrastructure and all regions.

   > ⚠ Note that all non-ASCII characters in your domain will be converted to hyphens (-) and hyphen characters will be doubled. For example, *test-123* will be changed into *test--123*, and t*est.123* will be changed into *test-123*.

   c. **Customer reference** – this field is optional. You can enter your own reference number (such as the **Sold To** code from your ERP) here.

6. In **License type** section:

- Select Demo license if the customer wishes to try Dispatcher Paragon Cloud and just wants to see how the solution works. Be aware that there is no possibility to convert this type of license into a commercial license. The demo will be deployed in the Sandbox environment, not in the production environment.

  > Select the checkbox **Delete this customer after <number> of days** if you are creating the tenant just for testing or demo purposes for a defined period of time.

- Select **Trial license** if the customer wishes to try Dispatcher Paragon Cloud and possibly continue with a commercial license after the trial period ends.

  > If a customer under trial decides to convert to a fully paid service, the Partner must send a purchase order to Y Soft. Y Soft will process the order and the active license will automatically be applied to the customer. Alternatively, the Partner admin can assign the license to the customer from the list of available licenses.

- Select **Commercial license** for all other cases. Click **Select license** to display the list of your purchased licenses. Select a license from the list and click **Assign**.

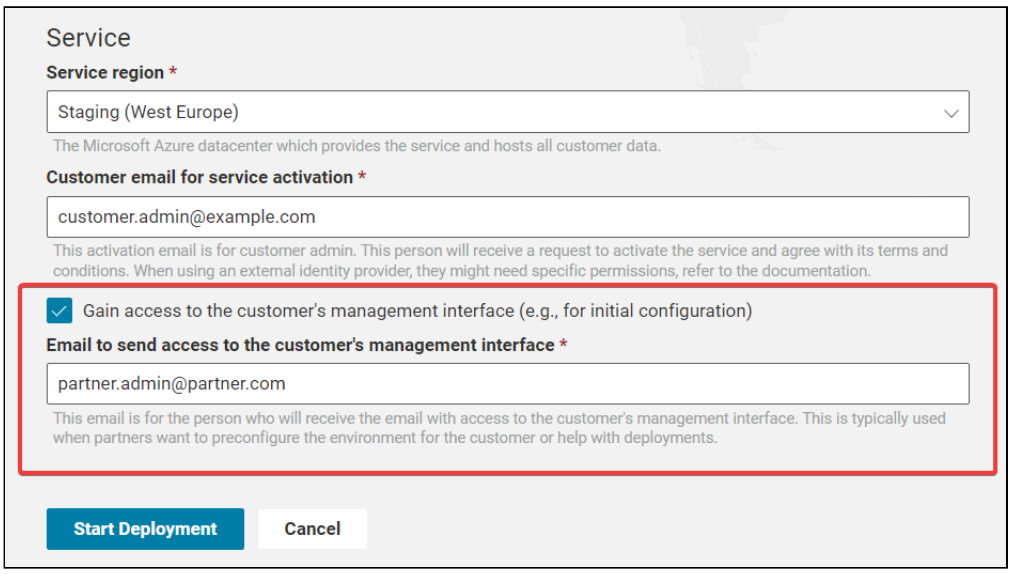
7. In the **Service** section:

   a. Select the **Service region** to host the customer's data. For more information about the regions, see https://azure.microsoft.com/en-us/global-infrastructure/data-residency/.

   b. In the **Customer email for service activation** field, enter the customer admin's email address. The customer admin will receive the invitation email ("Welcome to Dispatcher Paragon Cloud") and will gain the Customer admin system role in Dispatcher Paragon Cloud management interface.

   > The customer admin will have the possibility to synchronize their admin account with their external Identity Provider (e.g., Azure Active Directory), or to create an Internally managed user account for themselves. For more information about Internally managed users and synchronization with external Identity Providers, see Configuration and Administration guide, chapter User management and Externally managed users respectively. For the details on the activation process, see chapter Activating your Dispatcher Paragon Cloud.

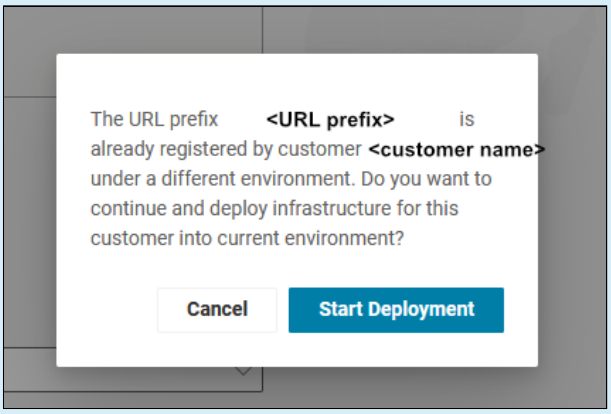
   c. If the partner technical contact is going to perform the initial configuration or to manage the Dispatcher Paragon Cloud for the customer, select the **Gain access to customer's Management Interface** checkbox. Enter the partner technical contact (partner admin) email address. The partner admin will receive the invitation email to create an admin account and will gain the Customer admin system role in the Management interface.



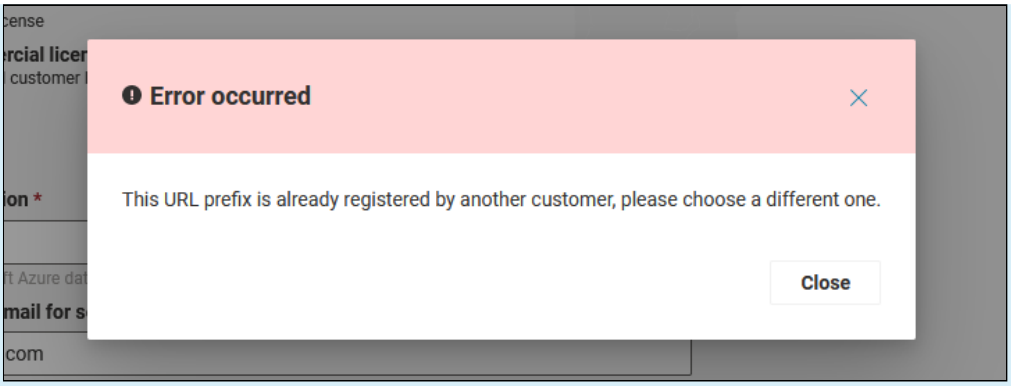
8. Click **Start deployment**.

If the customer is already registered with the same URL prefix in the same environment but in a different service group, two situations may occur:

a. The URL prefix is already registered by you. In this case, you will be able to create the customer in the current environment.



b. The URL prefix is already registered by another partner. In this case, you will not be able to create the customer with your chosen URL prefix in the current environment.



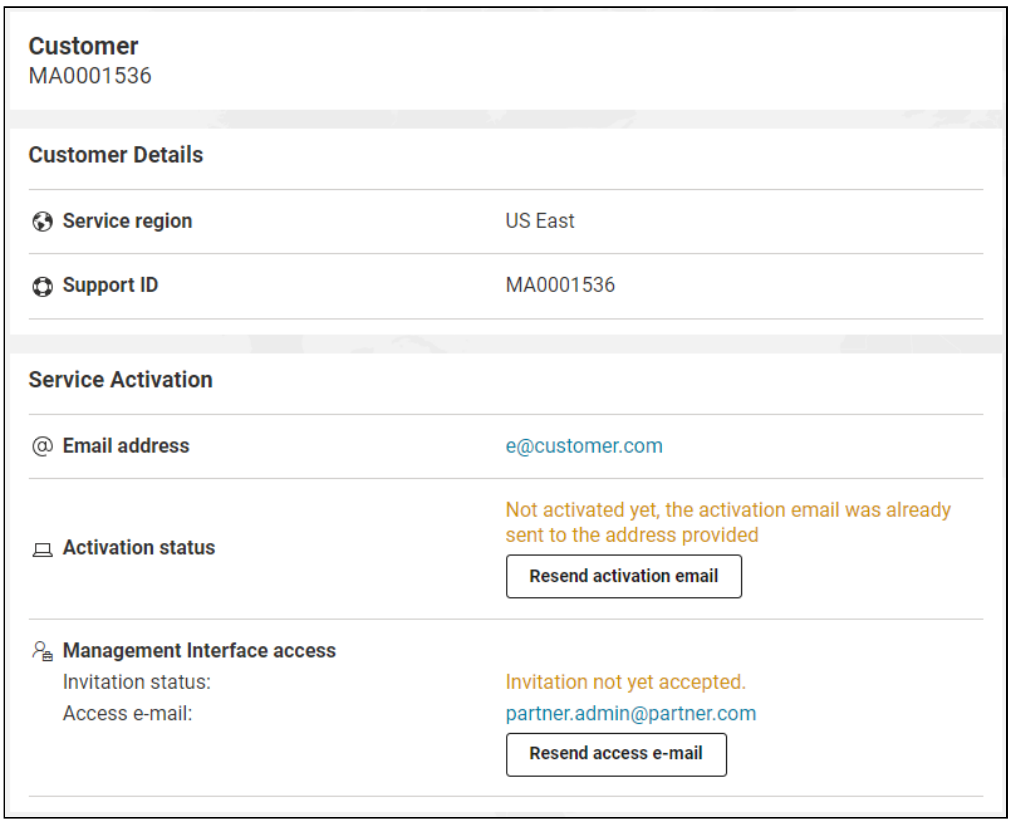
9. You can find your new customer on the **Customers** tab, showing the **Deploying** status in the **Status** column. The deployment usually takes less than 10 minutes.
10. After a few minutes, the customer receives the invitation e-mail, and the status changes to **Pending invitation**. The license type will be visible in the **License type** column.
11. After the customer successfully activates the account the status will change to **Active**.

> If the user fails to activate the account until the date noted in the e-mail, the status will change to **Invitation link expired**.

12. Click your new customer to see the details.

1.6.1 TROUBLESHOOTING

1. If the customer or partner admin missed the email to activate the admin account or the link expired, click the name of your customer in the Dispatcher Paragon Cloud Portal, and click **Resend activation email** or **Resend access email**.



1.7 CREATING DISPATCHER PARAGON CLIENT V3 INSTALLATION PACKAGES

1.7.1 ABOUT DISPATCHER PARAGON CLIENT V3

Dispatcher Paragon Client v3 is a desktop application for end users through which they can:

- Submit their print jobs to the cloud, or in case of Edge printing scenario, to local Edge devices.
- See the list of waiting print jobs and printed print jobs
- Delete print jobs
- Mark print jobs as favorite
- Manually select a site server

For the features and limitations of Client v3, see the Configuration and Administration guide, section Dispatcher Paragon Client v3.

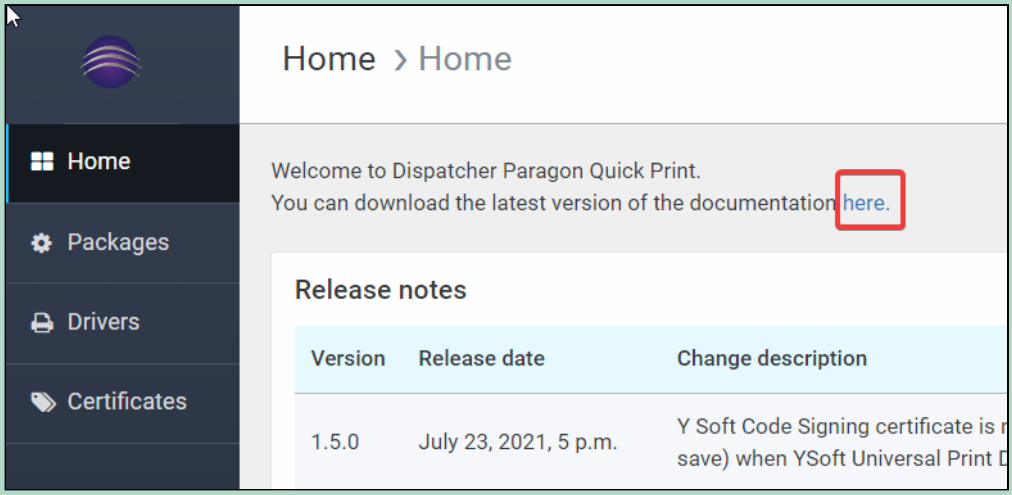
1.7.2 INSTALLATION OPTIONS

Operating system	Quick Print	Script
Windows	✓	✓
MacOS	✓	✓
Linux	✗	✗

Creating Client v3 installation packages in Quick Print

Perform the following steps at the Quick Print website to create Client v3 installation packages:

✓ For detailed information on creating installation packages, download the documentation in pdf from the Quick Print homepage:



1. Gather the following information from the customer:
   a. Driver name of the driver that the customer intends to use for direct print queues.
   b. IP addresses and aliases of all the site servers (edge devices) – this is necessary to create a list of site servers for user roaming when the Global print roaming option is disabled.
      - Gather also the default site server for each location. You will need to create a separate Client v3 installation package for each location with a default site server. This ensures that the users who do not travel between different locations can connect to the correct site server without having to select it manually.

2. Log into the Quick Print web page with your Partner Portal credentials: https://quickprint.dipa.cloud/.
3. For Windows, click **+ CLOUD CLIENT MSI**. For Mac, click **+ NEW VERSION 3 CLIENT DMG PACKAGE**.
4. Enter the configuration parameters into the **Configuration file** field. Example:

configuration/local.json

```
{
   ...
   "SpoolerOptions": {
      "Mode": "ClientNonSpooling" or "ClientSpooling",
      "DriverName": "<driver name>"
   },
   "SiteServerOptions": {
      "DisableCertificateValidation": <bool>,
      "EnableManualSiteServerSelection": <bool>,
      "SiteServerSources": <list of site server sources>,
      "SelectedSiteServerAlias": "<selected alias>"
      "SiteServers": [
         {
            "Host": "<device gateway address>",
            "Alias": "<device gateway alias>",
            "Scheme": "https",
            "JobServicePort": <port number>,
            "ServerSpoolerPort": <port number>
         }
      ]
   },
   ...
}
```

- Spooler Options Mode – enter "ClientSpooling" or "ClientNonSpooling" depending on the Dispatcher Paragon Cloud architecture that the customer will be using.
- Spooler Options DriverName – enter a driver name only if the customer will be using direct print queues.
- SiteServerOptions
  - EnableManualSiteServerSelection – set it to "true" if the customer needs traveling users to be able to select site servers (locations) manually. For more information, see the section *User roaming: manual site server selection*.
  - SiteServerSources – the list of sources from which Client v3 loads the site servers. The available options are:
    - Local - Client v3 includes site servers from its local configuration file into its site server selection pool. This is the default option when SiteServerSources parameter is not present in the configuration file.

- RESSC - Client v3 includes site servers from the cloud (currently Azure) into its site server selection pool. If you wish to use this option, you must use it together with "Local."

```
"SiteServerOptions": {
  "SiteServerSources": ["local", "ressc"]
  }
```

  - SelectedSiteServerAlias – enter the alias of the default site server (print location) for this installation package.
- SiteServers
  - Host – enter the device gateway address.
    - Pure Cloud printing: cloud spooler
    - Edge printing: customer's edge device
  - Alias – a user-friendly name for this device gateway. End users will see this name when selecting a site server manually in Client v3.
- JobServicePort
  - Pure Cloud printing: port 443
  - Edge printing: port 5000
- ServerSpoolerPort
  - Pure Cloud printing: port 443
  - Edge printing: port 5002

5. (MSI package only) If the customer requires a direct print queue, fill in the direct print queue section:

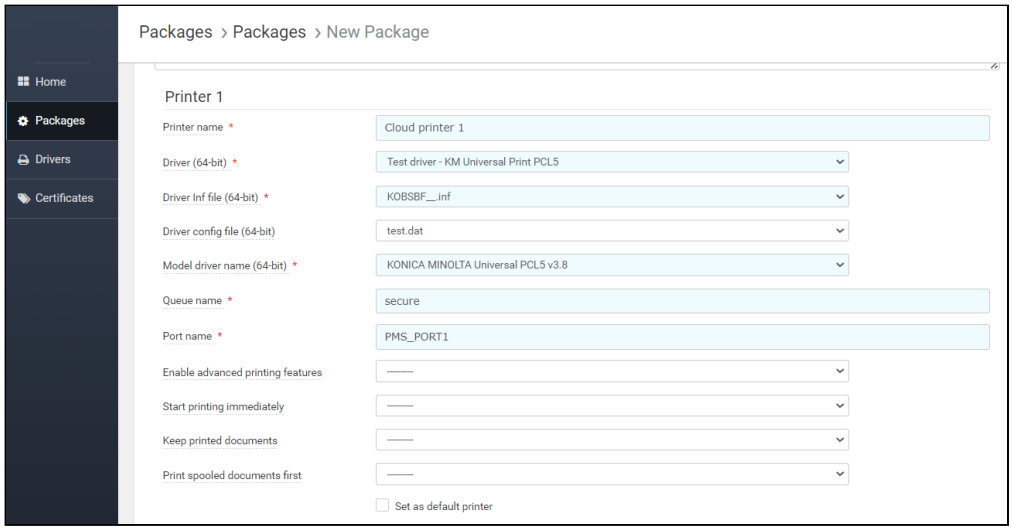
6. (DMG package only) Fill in pre and post installation scripts.
   a. Example of pre-installation script when using the Generic PS driver:

```
sudo /usr/libexec/cups/daemon/cups-driverd cat drv:///sample.drv/generic.ppd > /Library/Printers/PPDs/Contents/Resources/generic_ps_model.ppd 2> /dev/null
```

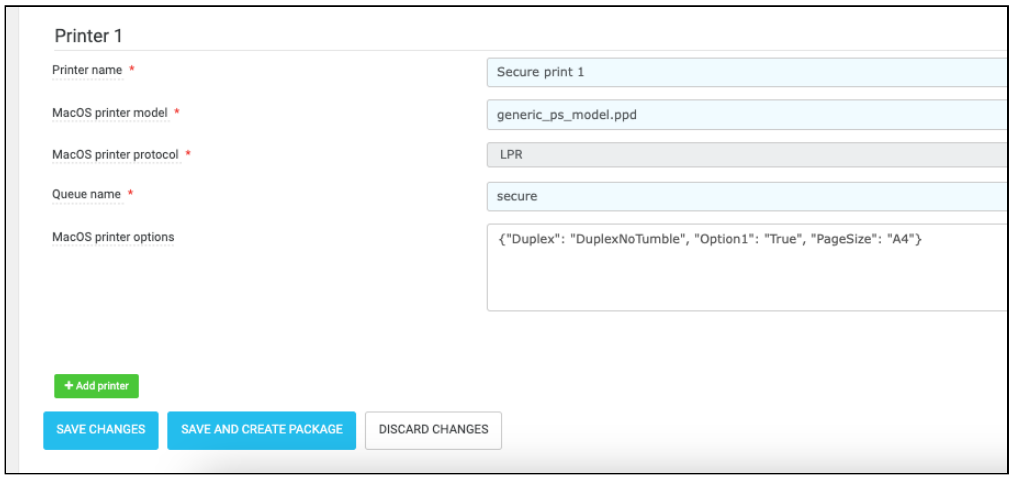
b. Example of post-installation script when using the Generic PS driver:

```
sudo rm /Library/Printers/PPDs/Contents/Resources/generic_ps_model.ppd
```

7. Fill in **Printer 1** section. This will deploy a print queue on user workstations together with Client v3.
   MSI:



   DMG:



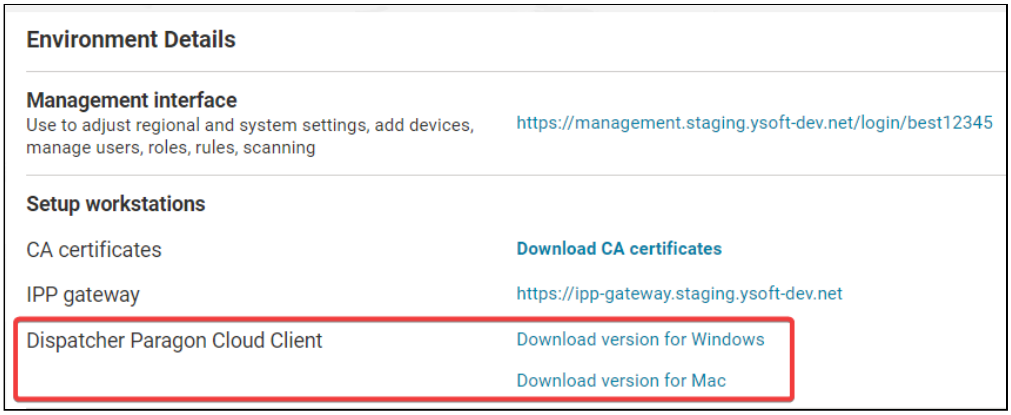
8. Fill in the rest of the fields according to the Quick Print documentation and create the package.

9. Repeat the process if you wish to create more installation packages, for example, with another default location in the configuration file.

10. Send the package(s) to the customer.

Installing Client v3 via an installation script

1. Instruct the customer to download the installation package from the Dispatcher Paragon Cloud Portal.



2. Instruct the customer to run the installation script with the following parameters:

Windows	Mac
-ServerSpoolerPorts <port numbers>	--serverspooler-ports <port numbers>
-JobServicePorts <port numbers>	--jobservice-ports <port numbers>
-SpoolerMode <mode>	--spooler-mode <mode>
-SiteServerSources <list of sources>	--siteserver-sources <list of sources>
-SiteServerHosts <device gateway addresses>	--siteserver-hosts <device gateway addresses>
-SiteServerAliases <aliases of gateway addresses>	--siteserver-aliases <aliases of gateway addresses>

For the description of the configuration parameters, see the section *Creating Client v3 installation packages in Quick Print*.

User roaming: manual site server selection

If the customer will be using Edge printing with Global print roaming disabled, Client v3 must be configured for traveling users in the following way:

Configuration parameter *EnableManualSiteServerSelection* must be set to "true" so that end users can access the manual Site Server selection settings in the **Client settings** section of Client v3.

If *EnableManualSiteServerSelection* is set to "false", or not specified at all, the site server selection option is hidden in the **Client settings**.

For more information on User roaming and Print roaming, see the Edge architecture.

⚠ Manual site server selection works only for queues deployed via the Client v3 installation package, not for queues that the user has added manually via the IPP URI generated at the IPP Gateway (*End user guide*, chapter Configuring IPP print queues).

Site server (print location) list

If you wish to use SiteServerSources with "Local" value, enter the list of site servers into the **Configuration file** field in Quick Print when creating the installation package, so that the list is present in the resulting **local.json** configuration file. The customer can change the **local.json** later on, if, for example, they need to add more site servers. Each site server must have an **Alias** defined, so that the end users see the site server names (aliases) in their Clients v3 in the **Print location** field, instead of IP addresses.

If you wish to use SiteServerSources with "Local" and "RESSC" values, it is enough if you enter the default site server for the given location into the **Configuration file** field. The rest of site servers will be loaded from the cloud.

⚠ Be aware that:

- the *SelectedSiteServerAlias* configuration property must be present in the configuration file. This is the site server the Client v3 will connect to for the first time.
- if the customer admin deploys a correctly configured installation package to users, the users don't need to select the print location manually, unless they are traveling.
- traveling users must select a print location each time they change locations, regardless of whether they are traveling from their usual location or whether they are returning to it.

Example of local.json file with two site servers

```
{
  "SpoolerOptions": {
    "Mode": "ClientNonSpooling",
```

```
    "Branding": <branding>
  },
  "SiteServerOptions": {
    "EnableManualSiteServerSelection": true,
    "SiteServerSources": ["local", "ressc"],
    "SelectedSiteServerAlias": "London",
    "SiteServers": [
      {
        "JobServicePort": 5000,
        "Host": "10.0.5.144",
        "ServerSpoolerPort": 5002,
        "Scheme": "https",
        "Alias": "London"
      },
      {
        "JobServicePort": 5000,
        "Host": "10.0.5.120",
        "ServerSpoolerPort": 5002,
        "Scheme": "https",
        "Alias": "Paris"
      }
    ]
  },
  "JobReceivingOptions": {},
  "HttpServerOptions": {
    "Port": 5002,
    "Scheme": "https",
    "CertificateOptions": {}
  },
  "JobStoreOptions": {
    "Path": "C:\\\\<install_dir>\\\\Spooler\\JobStore"
  },
  "DhcpDiscoveryOptions": {
    "Enabled": false
  }
}
```

Configuration parameters

Group	Key	Type	Default value	Description
SpoolerOptions	DriverName	string		Name of the print driver used if a user deploys a direct queue. (Available only on Windows)

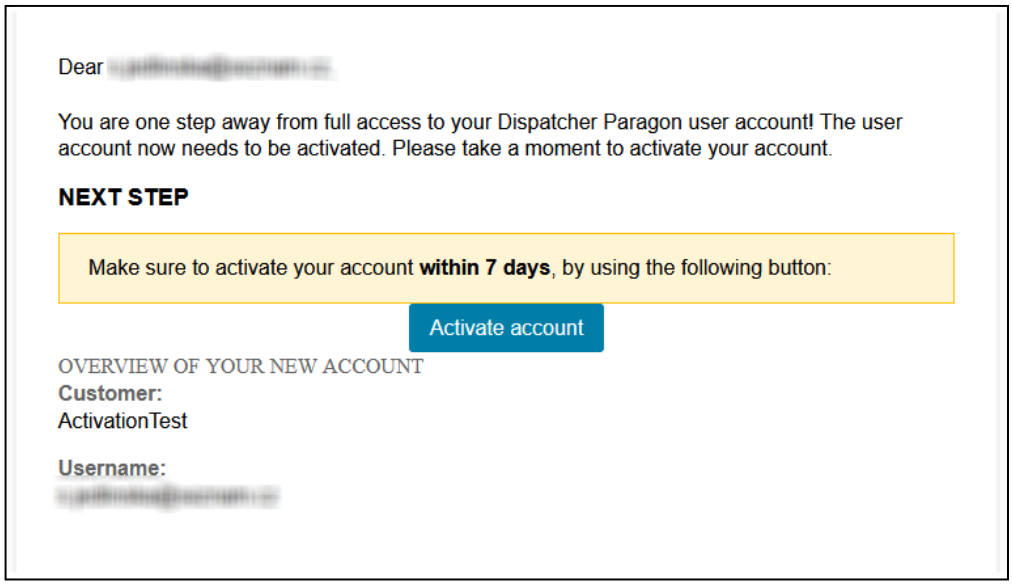
Group	Key	Type	Default value	Description
	Mode	string		The mode in which the Client v3 will be running. The possibilities are "ClientSpooling" for a client with spooling and "ClientNonSpooling" for a client without spooling.
SiteServerOptions	DisableCertificateValidation	string	false	A switch that disables Client v3's validation of HTTPS certificates. Using this switch will severely lower security since the client will be communicating with a server which does not have a valid certificate.
	EnableManualSiteServerSelection	bool	false	If set to "true", enables the users to select a site server manually.
	SiteServerSources	list	"Local"	List of sources from which Client v3 loads the site servers (print locations).
	SelectedSiteServerAlias	string		The alias of the default site server for the given installation package
SiteServerOptions.SiteServers	Alias	string		Site server alias.

1.8 ADDITIONAL MATERIALS

1.8.1 ACTIVATING YOUR ADMIN ACCOUNT AS PARTNER ADMIN

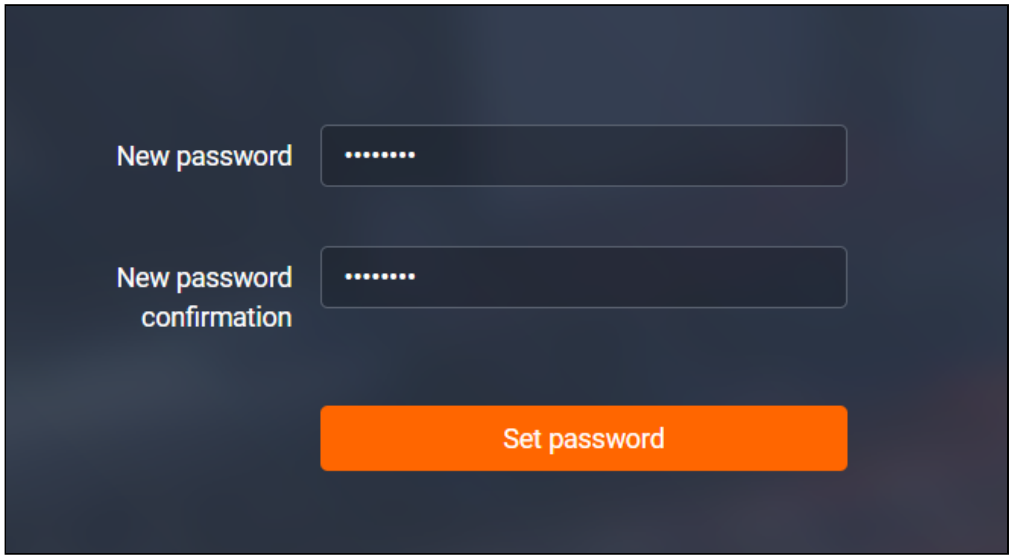
Perform these steps only if the person registering the customer granted you access to customer's Dispatcher Paragon Cloud Management interface. In that case, activating the admin account will create a *Local user* account with Customer admin role system role in the Management interface.

1. When the deployment of customer's Dispatcher Paragon Cloud has finished, you will receive an email with subject *New password activation for Dispatcher Paragon*.



2. Click **Activate account**.

3. Enter a password for your account and click **Set password**.



4. The username for this account is the email address where you received the email. For accessing the Management interface, see Accessing Dispatcher Paragon Cloud management interface as partner admin.

5. If you missed this email or the link expired, you can resend it from the Dispatcher Paragon Cloud Portal.

1.8.2 ACCESSING DISPATCHER PARAGON CLOUD MANAGEMENT INTERFACE AS PARTNER ADMIN

To access the Dispatcher Paragon Cloud management interface, do the following:

1. Go to https://dipa.cloud.
2. Log in using your Dispatcher Paragon Portal credentials.
3. Navigate to your customer and click the link in the **Management interface** section. The login screen of the Dispatcher Paragon Cloud management interface will be displayed.

   Alternatively, you can type the address into the address bar of your browser:

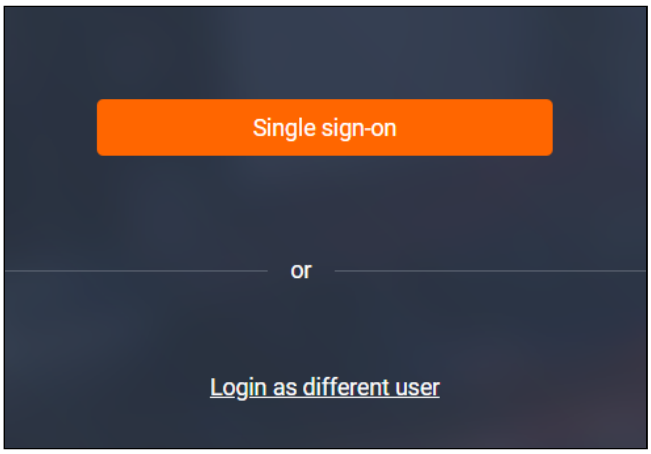
   a. Open your web browser.

   b. Type https://management.<region>.dipa.cloud/login/<modified_domain> in the address bar, where:

      1. `<region>` – Where the customer's service is deployed. The available regions are EU1, APAC1, AU1, and US1.
      2. `<modified_domain>` – Created from the customer domain by replacing dots with dashes and replacing dashes with double dashes. E.g. "my-example.com" is modified to "my--example-com".

   c. Press ENTER. The login screen of the Dispatcher Paragon Cloud management interface is displayed.

4. Click **Login as different user**.



5. In the **Username** and **Password** fields, enter the credentials that you created during Activating your admin account as partner admin.

6. Click **Login**.

1.8.3 HOW TO IMPORT CA CERTIFICATE FOR EDGE PRINTING TO YOUR WORKSTATION

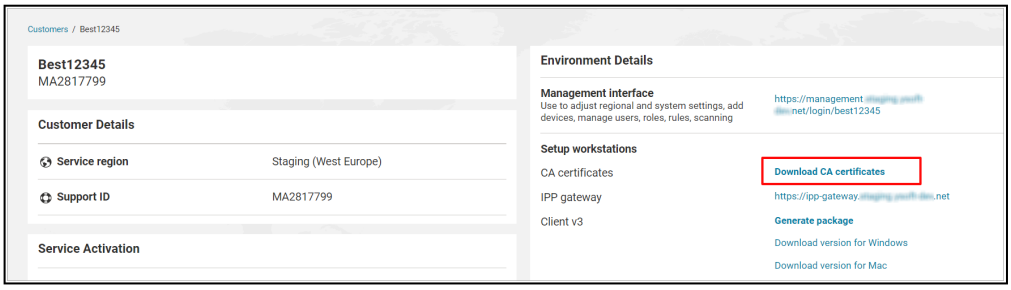
> ⚠ This is a guide for individuals who wish to test Edge printing or to demonstrate it to customers. In such cases, you must import CA certificate to your workstation yourself. In BAU scenarios, the customer admin would usually deploy it to the end user workstations, as described in the Configuration and administration guide, chapter Managing Edge devices.

When YSoft OMNI Bridge Site Server is first configured, the IPP Gateway module automatically receives a certificate signed by the MSP-provided cloud Certificate Authority (CA). In order to establish trust between your workstation and the YSoft OMNI Bridge Site Server, you must either use your own certificate, or trust on your workstation the CA available at the Dispatcher Paragon Cloud Portal.If you wish to use your own certificate, contact service desk. If you decide to use the provided CA, perform the following steps:

1. Log into the Dispatcher Paragon Cloud Portal.

2. Click the name of your customer. This will take you to the dashboard.

3. Click **Download CA certificates**.



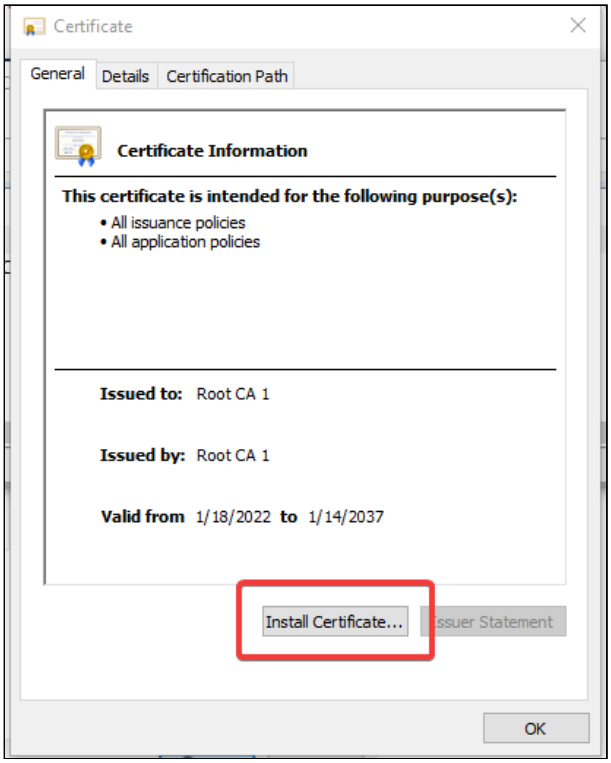
4. A file called **Root-CA-1.crt** will be downloaded to your workstation automatically.

5. Continue to the next steps for Windows, Mac, or Linux, depending on your operating system.

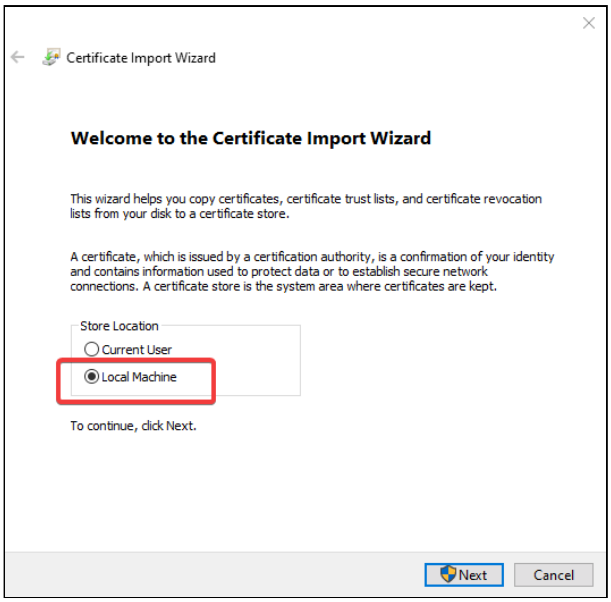
Windows workstation

1. Open the **Root-CA-1.crt** file by double-clicking it.

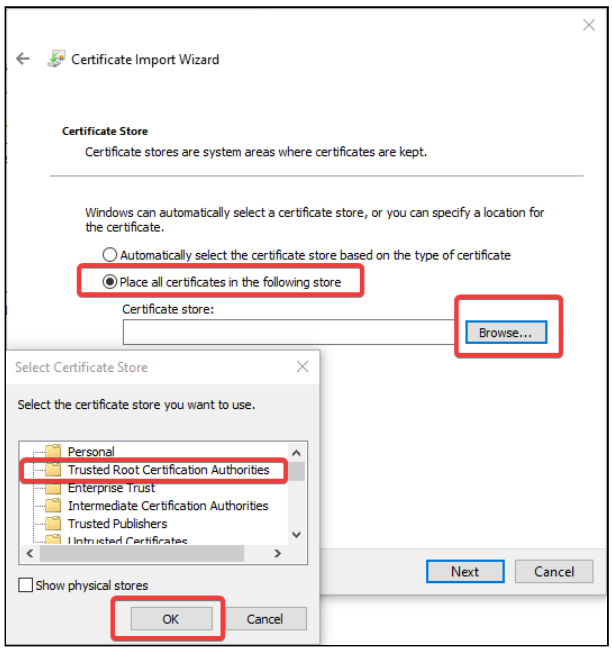
2. A new dialog window will be displayed. Click **Install certificate**.



3. A **Certificate Import Wizard** will open. In Store Location, select **Local machine** and click **Next.**



4. In the next step, select **Place all certificates in the following store**. Click **Browse** and select **Trusted Root Certification Authorities**. Click **OK**.



5. Click **Next** and then click **Finish.**

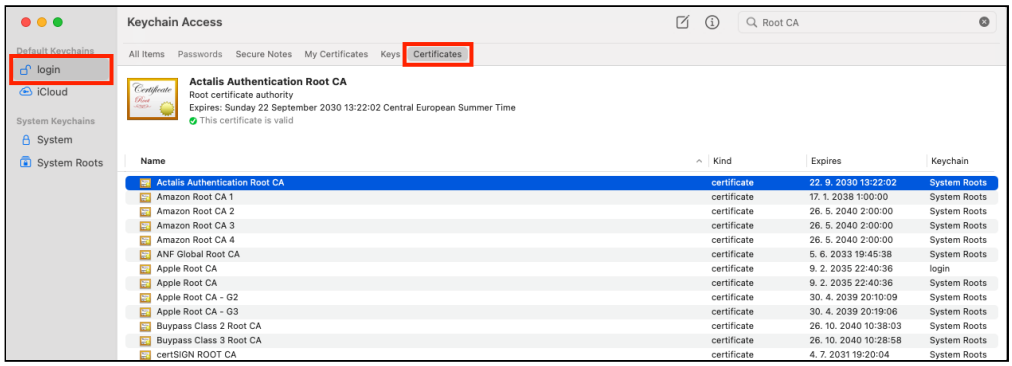
6. If you use Microsoft Edge or Google Chrome browsers, no further action is required, as these browsers use the Windows Certificate Store. If you use Mozilla Firefox, you must either import the certificates into it, or configure it to use the Windows Certificate Store. See https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox.

7. Restart your workstation.

Mac Workstation

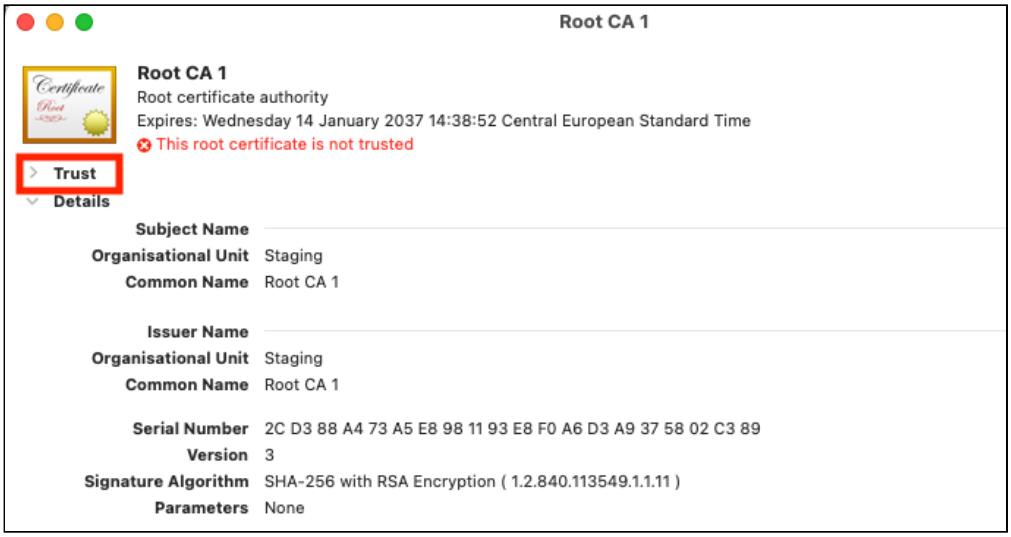
1. Open the **Root-CA-1.crt** file by double-clicking it.

2. The **Keychain Access** application will pop up. Navigate to the **Login** > **Certificates** tab.

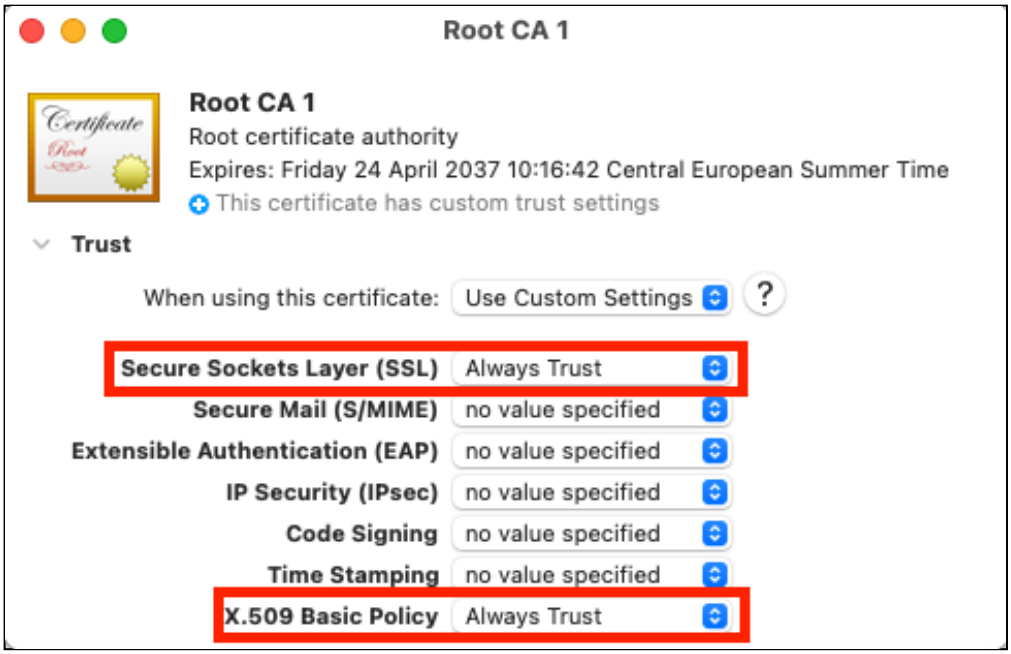


3. Find **Root CA 1** and double-click it.

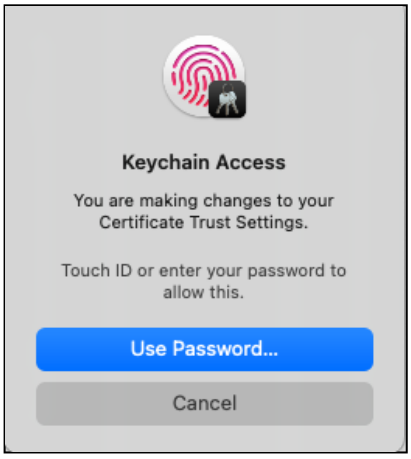
4. A new dialog window will be displayed. Expand the **Trust** section.



5. Select **Always Trust** in the **Secure Sockets Layer (SSL)** and **X.509 Basic Policy** fields.



6. Close the dialog and confirm the changes by entering your credentials or using Touch ID.



Linux workstation

> ⚠ The procedure may vary according to your Linux distribution. The following example is for Ubuntu.

1. Open Terminal by opening Terminal app or Ctrl+Shift+T shortcut.
2. Use the following command to install the **ca-certificates** package.

```
sudo apt-get install -y ca-certificates
```

3. Navigate to the folder where the **Root-CA-1.crt** file was downloaded. Use the following command to copy the downloaded file to ca-certificates.

```
sudo cp Root-CA-1.crt /usr/local/share/ca-certificates
```

4. Use the following command to update the certificate store.

```
sudo update-ca-certificates
```

1.8.4 HOW TO CREATE AZURE ENVIRONMENT FOR DISPATCHER PARAGON CLOUD

If your customer doesn't have Azure Active Directory, you can use this guide to set up a free Azure account with them. The free account has Azure Active Directory by default. If your customer has an

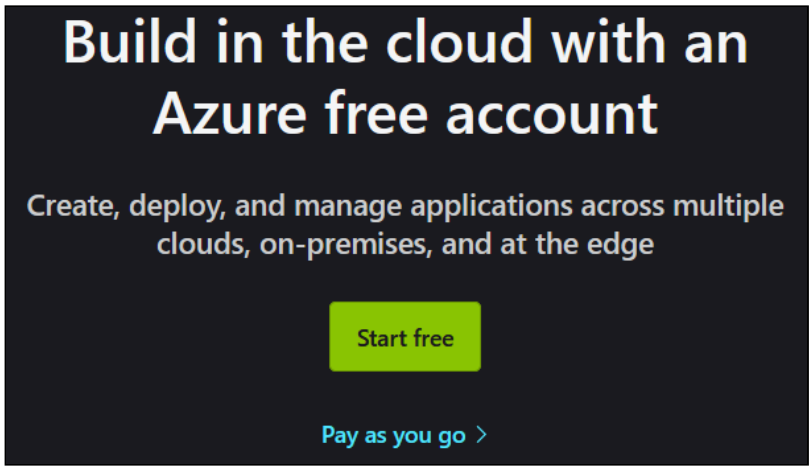
on-premise Active Directory, they can synchronize it with the newly created Azure Active Directory via Azure AD Connect.

Steps for customer admin

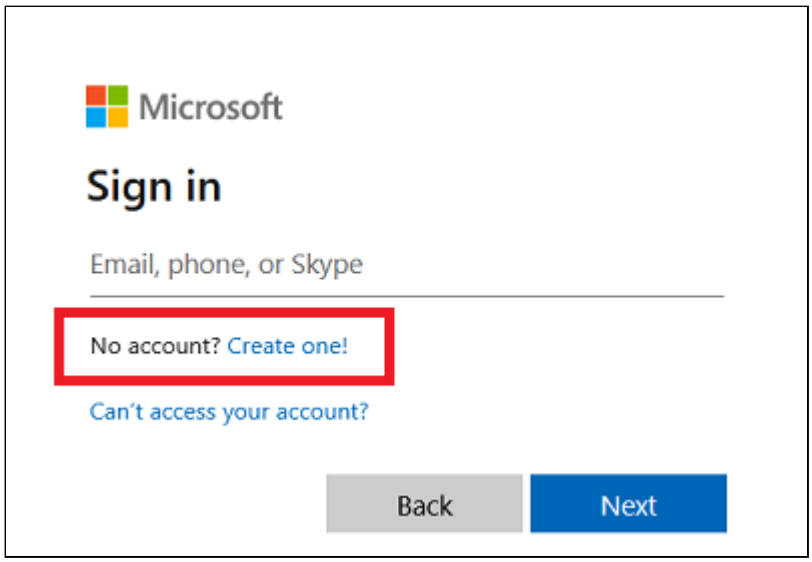
Create a free Azure account and Azure Active Directory

To create a new Azure account, do the following:

1. Navigate to https://azure.microsoft.com/en-us/free/ and click **Start Free**.

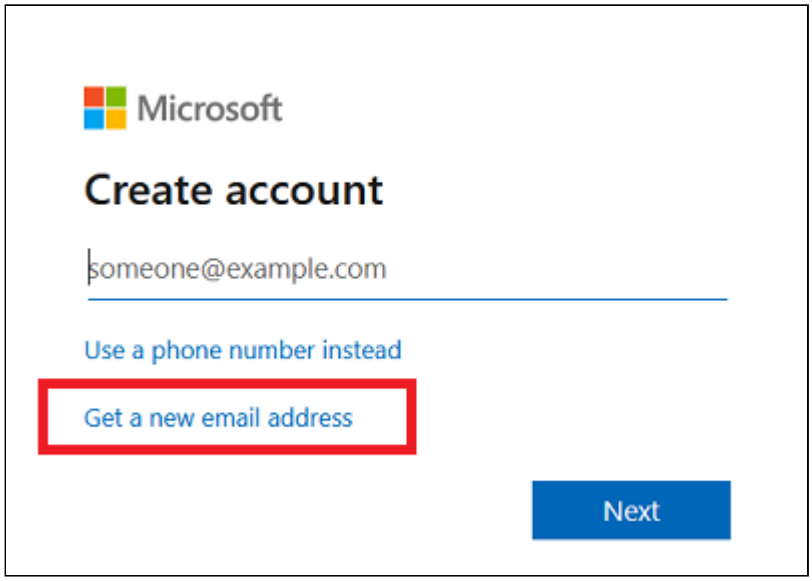


2. In the wizard, sign up with a Microsoft account. You can use an existing Microsoft account or create a new one by clicking **Use another account** and then **Create one!**.

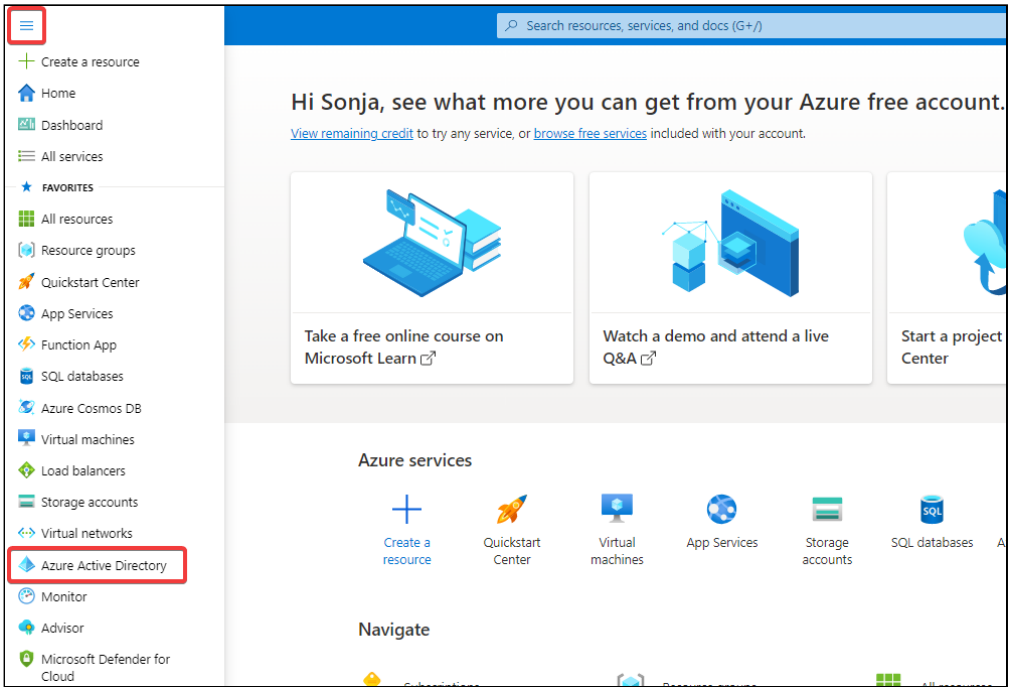


While creating a new Microsoft account, you can enter an existing email address or create a

new one by clicking **Get a new email address**.



3. You will be redirected to your profile creation page.
4. On the **Create your Azure free account** page, fill in all the mandatory information and verify your identity with your phone number and credit card. No charges will be made to the card provided unless you choose to make a purchase. After creating your profile, you will be redirected to the Azure Portal home page.
5. On the Azure Portal home page, select **Azure Active Directory** from the left sidebar menu.



Here you can add users and groups and manage tenants.

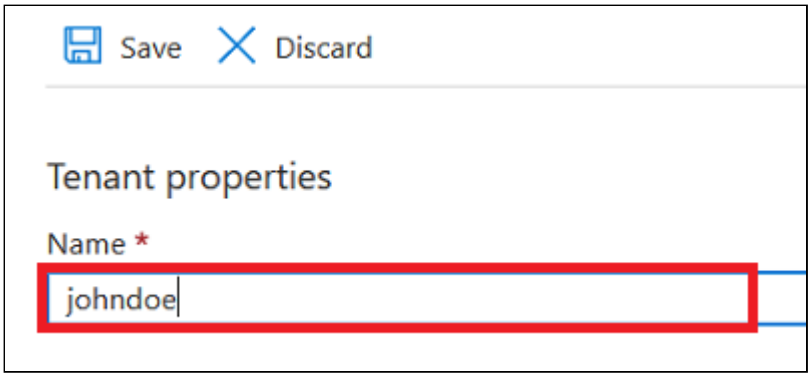
6. If you need another tenant than the default one, you can create one following this process: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant

Register a custom domain

Microsoft will add the ".onmicrosoft.com" domain extension to your freshly created Azure domain by default. If you want to create users with usernames that reflect your preferred domain name, you can register one or multiple domains in your Azure Active Directory.

Before registering a domain, you may also check the tenant's name. If the name was not set before, the prefix of the email used to create the account will be applied automatically. To check and edit your tenant name, do the following:

1. Go to https://portal.azure.com. Open the left sidebar menu and navigate to **Azure Active Directory** > **Properties**.
2. Under **Tenant properties**, you can check the name of your tenant. You may edit the name and click **Save**.



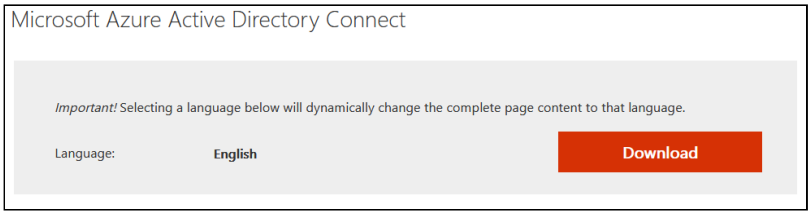
With the desired tenant name, proceed with the registration of a domain. To register a domain in Azure Active Directory, follow this process: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain

Azure AD Connect

You can use Azure AD Connect to synchronize your Azure Active Directory with an existing on-prem Active Directory domain.

Installation and setup

1. Download the installation file. You can open the left sidebar menu and navigate to **Azure Active Directory** > **Azure AD Connect**. On the **Download Center** page, click **Download**.



2. Run the downloaded MSI file to start a configuration wizard

> Run the installation file preferably on a domain controller, but definitely within the customer's on-premise Active Directory domain.
>
> As it installs a service that is used for synchronization, we advise installing it on an always-on server or workstation.

3. Follow this process: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express

Setting Password writeback

To enable password writeback in Azure AD Connect, follow this process: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr-writeback#enable-password-writeback-in-azure-ad-connect

Azure Command Line Interface

To check the status of the synchronization service and to manually initiate a synchronization for testing or troubleshooting purposes, Microsoft Azure Command Line Interface (Azure CLI) can be used on the server running Azure AD Connect.

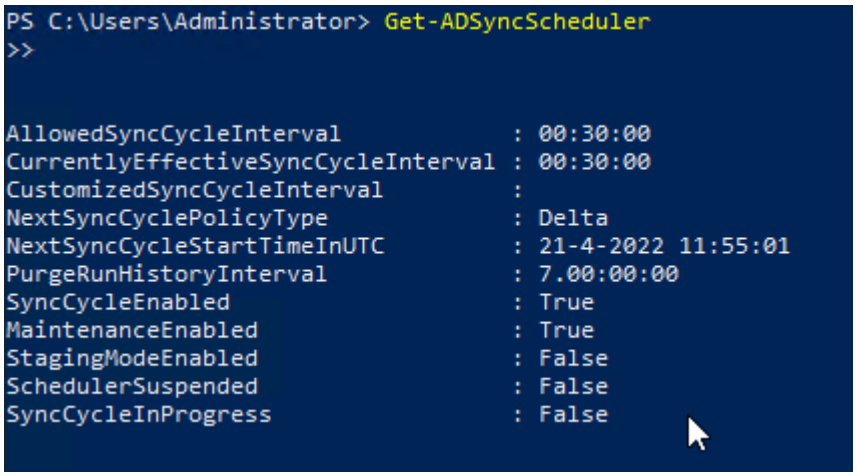
1. Use this link https://aka.ms/installazurecliwindows to download Azure CLI.
2. Run the downloaded MSI file.
3. After the installation, use Powershell to connect to your Azure tenant by typing `az login`. A web browser opens, prompting you to log in with your Azure AD credentials (use the Global administrator account created earlier).

```
PS C:\Users\Administrator> az login
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue the login
in the web browser. If no web browser is available or if the web browser fails to open, use device code flow with `az login --use-
device-code`.
```

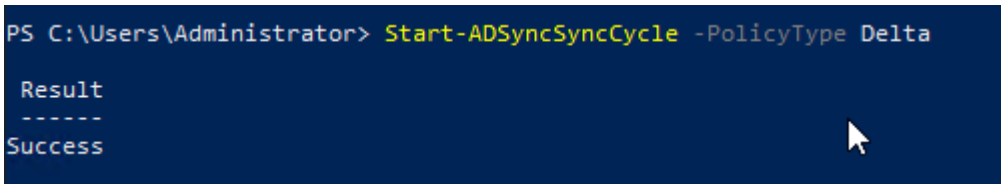
4. After successful login, type `Import-Module ADSync`.

```
PS C:\Users\Administrator> Import-Module ADSync
```

5. To verify the current synchronization status and interval, type `Get-ADSyncScheduler`.



6. To start a manual synchronization, type `Start-ADSyncSyncCycle -PolicyType Delta`. Depending on the number of objects to synchronize, this may take a few moments.



> The `Success` indicates the successful execution of the command to initiate the synchronization, not the synchronization itself.

For a detailed description of the Azure CLI ADSync Module capabilities, see https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-scheduler.

Step for partner admin

Create a Dispatcher Paragon Cloud tenant

With a working Azure Active Directory and, if applicable, synchronization with a corresponding on-premises Active Directory domain, you can create a Dispatcher Paragon Cloud tenant for your customer and use the newly created Azure domain for user authentication.

Follow this process: Registering a new customer.

The customer must use a user account with the **Global admin** role (created earlier) for the activation of the new tenant. This prevents the consent form from popping up for each user. For more information see Activating your Dispatcher Paragon Cloud.

After successful activation of the tenant, Single sign-on can be used for the IPP Gateway and Management interface of your tenant.

1.8.5 HOW TO ASSIGN YSOFT OMNI BRIDGE FROM ONE CUSTOMER TO ANOTHER

If you wish to assign YSoft OMNI Bridge from one customer to another, let's say in your testing or demo scenarios, perform the following steps:

1. Prepare the OMNI Bridge serial number and the name of the customer (tenant in the Dispatcher Paragon Cloud Portal) from which you need to remove the OMNI Bridge.

   The serial number of your OMNI Bridge can be found either on the package, on the sticker on the rear side of your device, or in the device"s main menu under **DEVICE INFO** > **SERIAL NUMBER**.

2. Perform a factory reset on the OMNI Bridge. For details, see the Configuration and administration guide, chapter YSoft OMNI Bridge operation manual.

3. Contact the MSP through service desk. The MSP needs to take manual steps to make the reassignment possible.

4. After service desk lets you know that they have finished, you can assign the OMNI Bridge to the new customer. Follow the steps described in the Configuration and administration guide: Preparing your YSoft OMNI Bridge and Managing Edge devices

If a customer admin wishes to perform a factory reset while keeping the OMNI Bridge for themselves, they should follow YSoft OMNI Bridge Site Server maintenance, section *Recovery after factory reset*.

1.8.6 HOW TO HANDLE YSOFT OMNI BRIDGE RECOVERY AFTER DISASTER

If a customer's OMNI Bridge has to be replaced and the customer wishes to use the same IP address for the new OMNI Bridge, the MSP must first remove the old device from the customer's environment.

1. Prepare the OMNI Bridge serial number and the name of the customer (tenant in the Dispatcher Paragon Cloud Portal).

2. The customer admin must delete the Embedded Terminals installed under the old device, and the Spooler controller. This is described in the Configuration and administration guide, chapter YSoft OMNI Bridge Site Server maintenance, section *Recovery after disaster*.

3. Contact the MSP through service desk and request removal of the old device from the customer's environment.

4. After the removal is done, inform the customer admin that they can proceed with configuring the new device.

2 CONFIGURATION AND ADMINISTRATION GUIDE

This documentation is intended for Customer admins.

2.1 DOCUMENTATION CHANGELOG - RELEASE 2023.01.26

What's new	Where
Added that previously created invitations for the same Internally managed user will be deleted if a new invitation is created.	Internally managed users, section *Adding new users*.
Updated the Service Health Dashboard page: • Changed the URL to https://dipa.statuspage.io/. • Changed the description of the functionalities of the page. • Changed the screenshots.	Dispatcher Paragon Cloud Service Health Dashboard

2.2 GENERAL INFORMATION

2.2.1 ABOUT THE CONFIGURATION AND ADMINISTRATION GUIDE

This guide is intended for customer admins. It contains information on:

- What configuration steps to take after Konica Minolta deployed your Dispatcher Paragon Cloud. See Configuration process.
- How to manage your Dispatcher Paragon Cloud. See Dispatcher Paragon Cloud management interface guide and Dispatcher Paragon Cloud Portal guide.
- How the print queues work in Dispatcher Paragon Cloud. See Managing print queues.
- Where to check service availability in your region if you think there is an outage. See Dispatcher Paragon Cloud Service Health Dashboard.

If you encounter any problems, contact your service representative.

2.2.2 ABOUT DISPATCHER PARAGON CLOUD

Dispatcher Paragon Cloud is a full-featured print management solution on a shared and hosted infrastructure for small and medium-size businesses. With compatible MFDs, Dispatcher Paragon Cloud can be used as a pure cloud solution. With incompatible MFDs, it can couple an on-site Edge serverless device with a secure shared application in the public cloud, where print system metadata is stored and analyzed.

2.2.3 HOW TO READ THIS GUIDE

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.

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.

2.2.4 TERMS AND DEFINITIONS

Term	Description
Dispatcher Paragon Cloud	A cloud-based print management service.
Dispatcher Paragon Cloud Terminal	An application provided by the Konica Minolta MarketPlace. This application enables communication between an MFD and the cloud.
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 Dispatcher Paragon Cloud.
YSoft OMNI Bridge	YSoft OMNI Bridge is a piece of hardware manufactured by Y Soft.
YSoft OMNI Bridge Site Server	YSoft OMNI Bridge configured to serve as an Edge device providing local site services.
Pure Cloud printing	A service with architecture (printing method) based on MFDs that support Pure Cloud Terminal. 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 Dispatcher Paragon Cloud).
MFD	Multi-function device (a copier).
SFD	Single-function device (a printer).

Term	Description
Reporting-only device	MFDs or SFDs where you want to capture the number of printed pages (and related statistics) but do not need any other capabilities such as Embedded Terminal or Cloud Terminal or print roaming.
Card Activation Code Provider page (CACP)	A web service allowing users to assign cards to their Dispatcher Paragon Cloud accounts using their Azure Active Directory accounts.
IPP Gateway	IPPS server for print job submission by users to their personal secure queues in Dispatcher Paragon Cloud.
Dispatcher Paragon Cloud management interface	A web interface used by administrators to manage their product instance centrally, and by end users to manage their accounts. It displays information and functions as per the role of the individual logged in. The Management interface runs via the Management service.
Dispatcher Paragon Cloud Portal	A web interface for: • partner admins to register new Customers. • for customer admins to configure edge devices and manage the Internally managed users.
Konica Minolta MarketPlace	Konica Minolta's service for browsing, purchasing and downloading applications to MFDs.

2.2.5 PERSONAS AND ROLES

Persona	Description	Which role(s) in Dispatcher Paragon Cloud management interface can this person have?
Managed Service Provider (MSP)	The role with the highest set of privileges in the Dispatcher Paragon Cloud service, responsible for service availability and maintenance. Is responsible for Dispatcher Paragon Cloud Portal maintenance, monitoring, deployment of updates etc.	System admin
Partner	A partner of MSP. It can also be a reseller (a partner of a partner).	see *Partner admin*
Customer	The customer of a partner and, at the same time, a representation of the customer in the Dispatcher Paragon Cloud Portal. In a more technical context, this representation is called Tenant. Each Customer has its own admin.	see *Customer admin*
Partner admin	An administrator in the Dispatcher Paragon Cloud management interface who (if agreed with the customer) can manage devices, users, and some of the systems settings. From the point of view of you as the customer admin, this is your service representative.	Customer admin system role is the highest-level role this person can have.
Customer admin	An administrator on the customer side with admin rights in the Dispatcher Paragon Cloud management interface.	Customer admin system role is the highest-level role this person can have.
End user	A persona within a customer's Dispatcher Paragon Cloud instance that is permitted to print/copy/scan.	Any role that the administrator assigns to them.

2.3 CONFIGURATION PROCESS

2.3.1 PREREQUISITES

Before you start to perform the steps in this guide, make sure that the following prerequisites are met:

Pure Cloud printing:

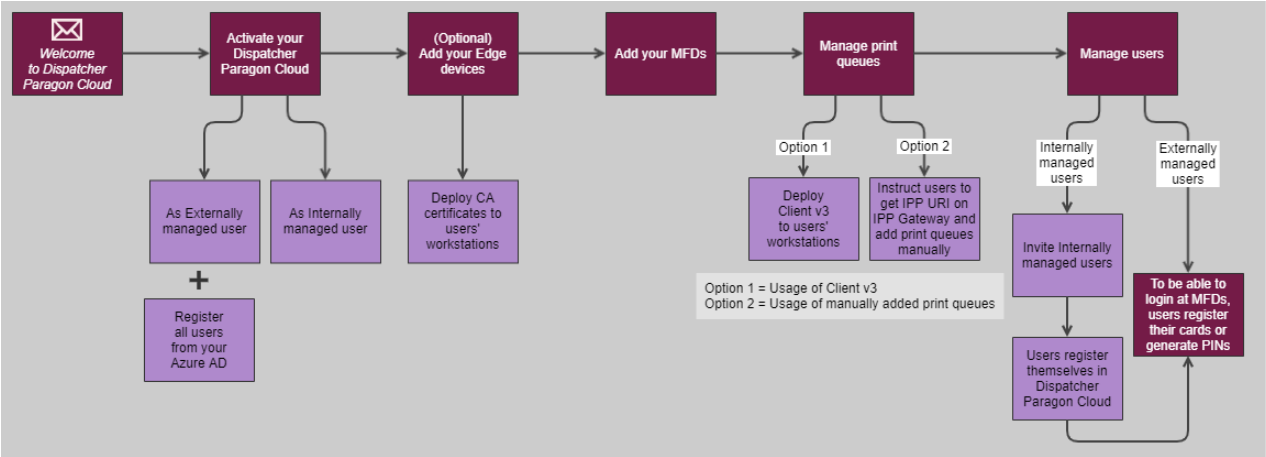
- You have received an email with subject *Welcome to Dispatcher Paragon Cloud*.
- Your service representative installed and activated Konica Minolta MarketPlace on your MFDs, updated the firmware of your MFDs, and installed the loadable device driver for the card readers. The card reader models must be supported by your MFDs.
- You have Konica Minolta MarketPlace account. If not, create an account at https://konicaminoltamarketplace.com/.
- You have received an email with subject *Welcome to Dispatcher Paragon Cloud.*

Edge printing:

- Your service representative installed the loadable device driver for the card readers. The card reader models must be supported by your MFDs.
- You have received an email with subject *Welcome to Dispatcher Paragon Cloud*.

2.3.2 THE CONFIGURATION PROCESS

This is a high-level overview of the configuration process. Follow the links to the respective chapters in the documentation to see the complete set of instructions for each step in this overview.



1. Activate your Dispatcher Paragon Cloud. See Activating your Dispatcher Paragon Cloud.

2. Set up your access to Dispatcher Paragon Cloud Portal. Use the **Manage account** button in your *Welcome to Dispatcher Paragon Cloud* email.
    a. Externally managed users: see Dispatcher Paragon Cloud Portal guide and Tenant admin role for accessing Dispatcher Paragon Cloud Portal.
    b. Internally managed users: you will be able to access the Dispatcher Paragon Cloud Portal immediately after activating your Dispatcher Paragon Cloud.
3. For Pure Cloud printing scenario:
    - Prepare your MFDs for installation of the Dispatcher Paragon Cloud Terminal. See Configuring Konica Minolta MFDs for Dispatcher Paragon Cloud Terminal.
    - Install the Cloud Terminal from the Dispatcher Paragon Cloud management interface. See Managing devices.
4. For Edge printing scenario:
    a. Prepare your YSoft OMNI Bridge. See Preparing your YSoft OMNI Bridge.
    b. Configure the YSoft OMNI Bridge as a site server. See Managing Edge devices.
    c. Install the Embedded Terminal on the MFDs connected to your YSoft OMNI Bridge. See Managing devices.
    d. Download the CA certificate and deploy it to user workstations. See Managing Edge devices, section *Downloading CA certificate*.
5. Manage print queues:
    a. Client v3: if you agreed with your service representative that your company will be using Dispatcher Paragon Client v3, deploy the Client v3 to users' workstations.
    b. Manually created print queues: if you won't be using Client v3, provide the end users with the following:
        1. The link to IPP gateway.
        2. How to configure the print queues, see Configuring IPP print queues.
        3. Which print drivers to use when configuring their print queues. For best compatibility, we recommend PCL5.
6. Manage users:
    a. If your company's users are going to be Internally managed users, invite them from Dispatcher Paragon Cloud Portal. See Internally managed users. They will need to register themselves. See the *End user guide*, chapter Registering yourself in Dispatcher Paragon Cloud.
    b. If your company's users are Externally managed users, they were all registered during Dispatcher Paragon Cloud activation.

c. To be able to log in at MFDs and release their print jobs, both types of users must either register their cards at MFDs (see the End user guide, chapter Card registration at the MFD terminal) or generate a PIN (see the End user guide, chapter Management interface guide, section *Generating a PIN*).

7. Send the End user guide to the end users.

2.3.3 ACTIVATING YOUR DISPATCHER PARAGON CLOUD

After the deployment of your Dispatcher Paragon Cloud has finished, you will receive an email with subject *Welcome to Dispatcher Paragon Cloud*. You will have two possibilities how to activate your Dispatcher Paragon Cloud:

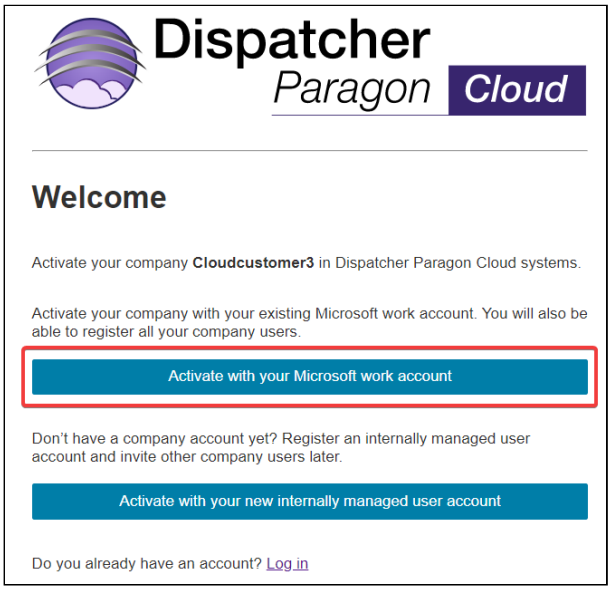
- If your company uses an external Identity Provider such as Azure AD, and you wish to synchronize your Dispatcher Paragon Cloud account with your external Identity Provider, proceed to section *Activating your Dispatcher Paragon Cloud as Externally managed user*.
- If your company doesn't have an external Identity Provider or if you don't want to synchronize your Dispatcher Paragon Cloud account with it, you can register a Dispatcher Paragon Cloud account manually. Proceed to section *Activating your Dispatcher Paragon Cloud as Internally managed user*.

Activating your Dispatcher Paragon Cloud as an Externally managed user

⚠ During the activation process, you will be asked to give admin consent for the Dispatcher Paragon Cloud Azure app. If you prefer, skip this step and give the consent manually in Azure portal. For more information about the admin consent see Giving admin consent for the Dispatcher Paragon Cloud Azure app.

1. Click **Activate account** in the *Welcome email*.

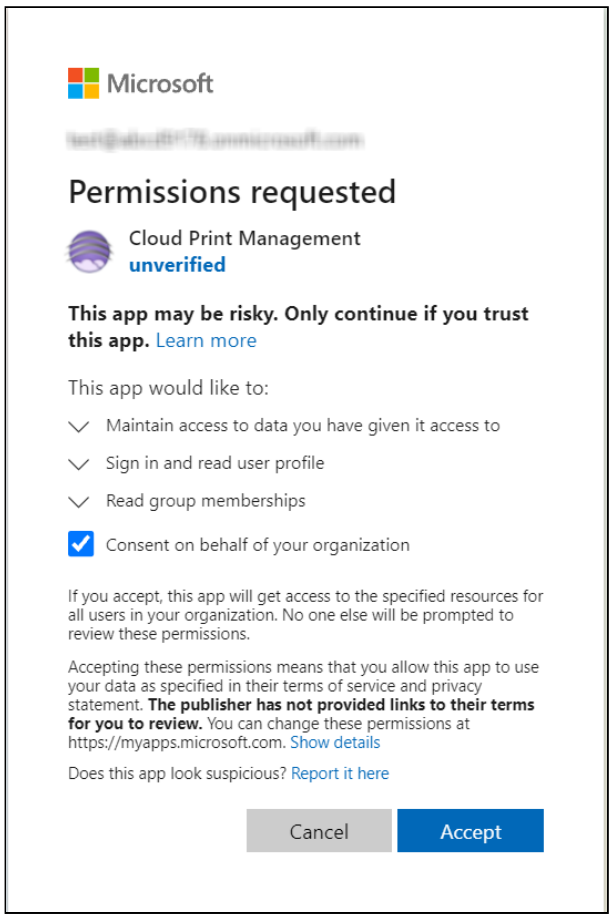
2. On the welcome screen, click **Activate with your Microsoft work account**.



3. On the next screen, click **Log in with Microsoft**.

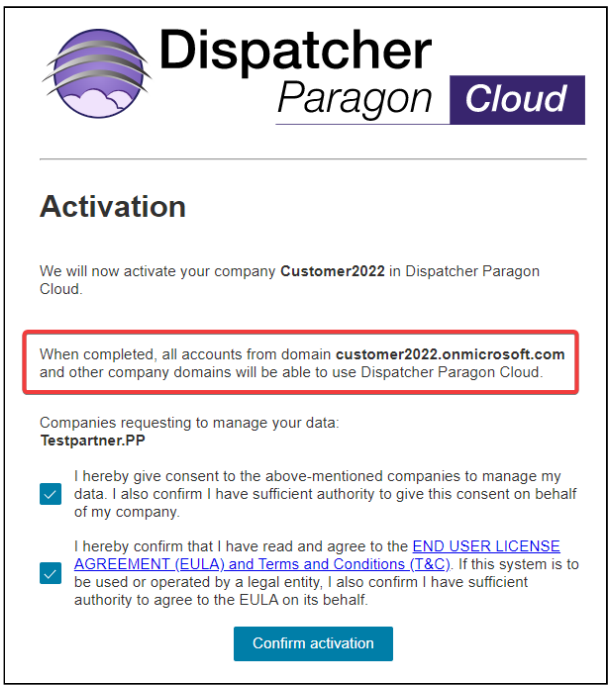
4. A dialog window will appear. Check the **Consent on behalf of your organization** checkbox. Give consent by clicking **Accept**.

> ⚠ To do this, you must have **Global administrator** role in your Azure AD.



If you don't check the **Consent on behalf of your organization** checkbox while accepting, you will need to give the consent manually in Azure portal, because this dialog window will not appear again. See Giving admin consent for the Dispatcher Paragon Cloud Azure app.

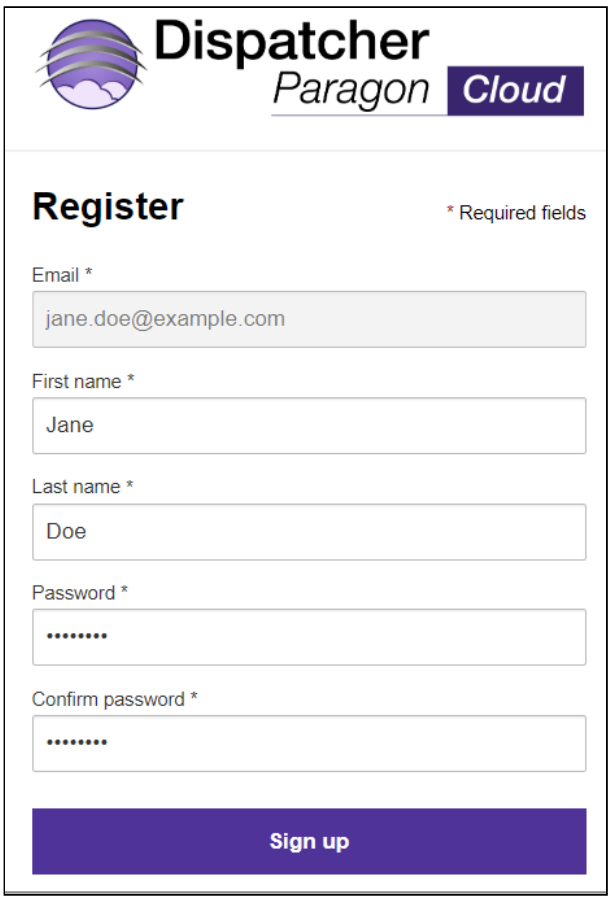
5. All users from the Azure Active Directory that you logged in with will be registered in Dispatcher Paragon Cloud.



6. Give consent to the companies requesting to manage your data by selecting the checkbox **I hereby give consent to...**
7. Agree to the End User License Agreement (EULA) linked on the page by checking the EULA checkbox. Then, click **Confirm activation**.
8. You will see a message that the activation is complete and that all company accounts are able to use Dispatcher Paragon Cloud. After that, you can close the window.

Activating your Dispatcher Paragon Cloud as an Internally managed user

1. Click the activation link in the *Welcome* email.
2. On the Dispatcher Paragon Cloud welcome screen, click **Activate with your new internally managed user account**.
3. Fill in your **First name**, **Last name**, and **Password**. **Email** is already pre-filled with the email address where you received the invitation and cannot be changed.



4. Click **Sign up**.
5. Agree to the End User License Agreement (EULA) linked on the page by checking the checkbox. Then, click **Confirm activation**.

6. You will see a message that the activation is complete. After that, you can close the window.
7. You now have an Internally managed user account. For details on account types in Dispatcher Paragon Cloud, see User management.

2.3.4 GIVING ADMIN CONSENT FOR THE DISPATCHER PARAGON CLOUD AZURE APP

> ⚠ If you are not using Azure AD, skip this step.

The Dispatcher Paragon Cloud application (called *Cloud Print Management* application) in Azure needs the following permissions to be able load groups from your Azure Active Directory and synchronize them with roles in Dispatcher Paragon Cloud:

- Microsoft Graph: Sign-in and read user profile
- Microsoft Graph: Read group memberships

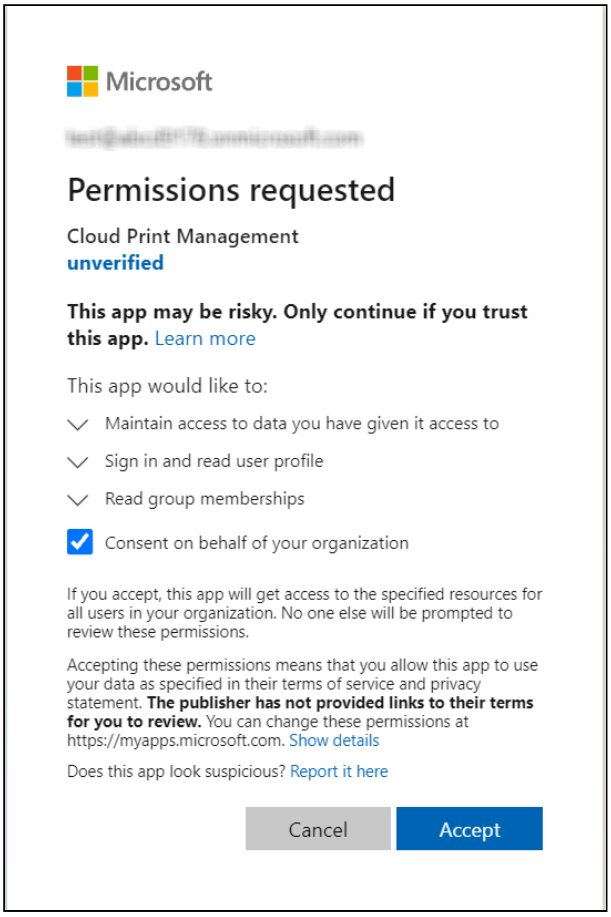
You must give consent to the application before the end users can log in to Dispatcher Paragon Cloud.

In order to give consent, you must have the Global administrator role in your Azure AD.

You can choose between two ways of giving consent:

Giving consent while using Dispatcher Paragon Cloud as an admin

You will be asked for admin consent either while Activating your Dispatcher Paragon Cloud or while logging in Dispatcher Paragon Cloud management interface via Single sign-on for the first time (depending on which of these actions you do first). In both cases, after clicking **Log in with Microsoft**, a dialog window with **Permissions requested** will appear. Check the **Consent on behalf of your organization** checkbox. Give consent by clicking **Accept**.

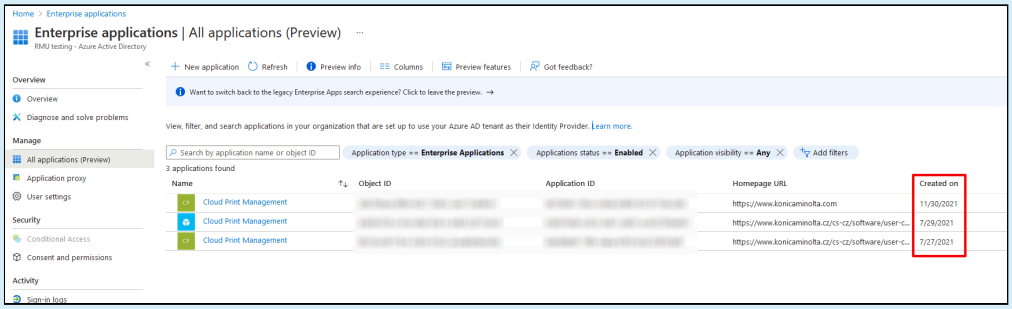


If you don't check the **Consent on behalf of your organization** checkbox while accepting, you will need to give the consent manually because this dialog window will not appear again.

Giving consent manually in Azure portal

1. Log in to https://portal.azure.com with your admin account.
2. Go to **Azure Active Directory > Enterprise Applications**.
3. Locate the **Cloud Print Management** application. If you don't see any applications, select **All applications** instead of **Enterprise Applications**.

   If there are multiple **Cloud Print Management** applications, choose the latest one. To identify the latest one, add the **Created on** column if you don't see it in your list.

4. Click the **Cloud Print Management** application.
5. In the left sidebar menu, click **Permissions**.
6. Click **Grant admin consent for <your company name>**. For more information on admin consent, see Microsoft documentation.

2.3.5 PREPARING YOUR YSOFT OMNI BRIDGE

Requirements

Tenant Admin role in Azure AD

The role is necessary only for Externally managed users synchronized from Azure AD.

To configure the YSoft OMNI Bridge, you will need to access the Dispatcher Paragon Cloud Portal. Before accessing the portal for the first time, you must assign to yourself a **Tenant admin** role for the **Cloud Print Management** application in your Azure AD. See Tenant admin role for accessing Dispatcher Paragon Cloud Portal.

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 YSoft 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.

  The IoT Hub is currently available in the West Europe region only.

  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.

  This registry currently has replicas in West Europe, Australia East, and East US regions.

  Reference: https://docs.microsoft.com/en-us/azure/container-registry/container-registry-intro
- Connectivity to Dispatcher Paragon Management Service is required - Apart from connecting to DPS, port TCP 443 is also used to connect to Management Services in the region set during the deployment of the customer in the Dispatcher Paragon Cloud Portal. Therefore, port 443 must be open in the firewall for YSoft OMNI Bridge.

  Note that even though the Site server on YSoft OMNI Bridge must connect to DPS and ACR in West Europe region, this doesn't mean that you can only use it for Customers in West Europe region. You can use YSoft OMNI Bridge with Customers from all regions available in Dispatcher Paragon Cloud Portal.

The OMNI Bridge uses 172.17.x.x and 172.18.x.x subnets as host networks for internal communication. If installed in any of those subnets at the customer site, the OMNI Bridge will not function properly.

Firewall rules

The following external domains and their communication ports must be allowed in your network firewall for the edge devices to function correctly.

FQDN (* = wildcard)	Outbound TCP Ports	Used for
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, 443	IoT Hub access
*.docker.io	443	Docker Hub access (optional)
*.dipa.cloud	443	Dispatcher Paragon Cloud Services
*.ysoft.cloud	443	Dispatcher Paragon CodeFlow
*.google.com	UDP 123	NTP server (time{1-12}.google.com) or any chosen NTP server

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. For details, see Security and privacy, section *YSoft OMNI Bridge security > OMNI Bridge application storage*.

Changing the manager password

If you wish to change the manager password for your OMNI Bridge, see YSoft OMNI Bridge operation manual, section *Change manager password*. We strongly recommend changing the password only after the enrollment of the device in your Dispatcher Paragon Cloud is complete.

Setup

> For more information about the installation of YSoft OMNI Bridge Site Server see YSoft OMNI Bridge Site Server installation and troubleshooting.

To set up YSoft OMNI Bridge, do the following:

1. Unpack the YSoft OMNI Bridge device.
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 *Requirements* above.

Do not change the assigned IP address! If the address changes, the device must be reconfigured, see YSoft OMNI Bridge Site Server maintenance, section *Recovery after factory reset*.

4. Make sure your YSoft OMNI Bridge has access to an NTP server. For more information, see section *Requirements* 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.

   The code expires after 10 minutes and a new code is generated.

   If the device code is too small for you to read:

   a. On the **Device status screen**, press ▶ two times.

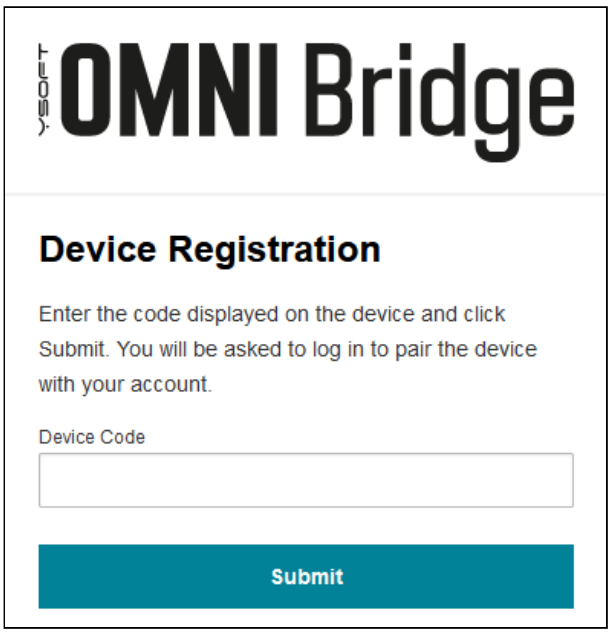
   b. This will take you to the **Module status screen**. Press **0**.

c. You will see the device code displayed in bigger letters.

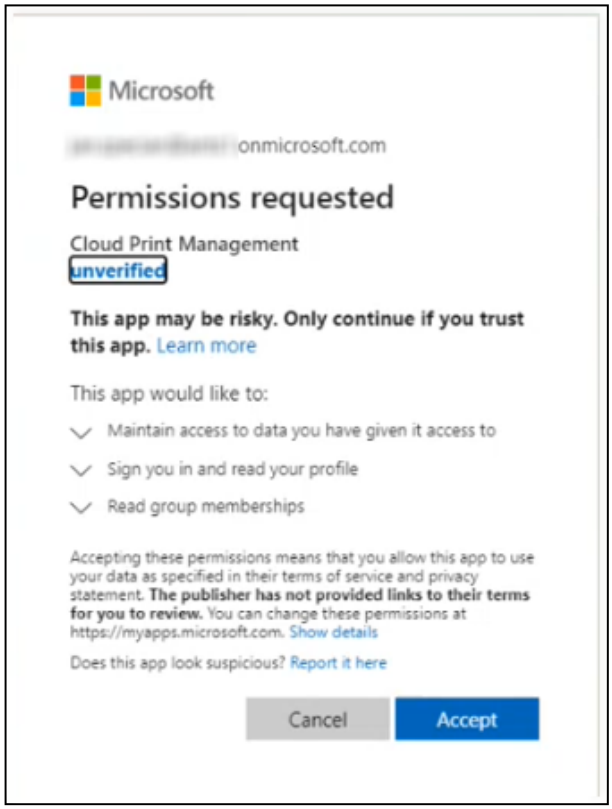
7. Go to https://sso.dipa.cloud/and enter the code displayed on the OMNI Bridge (you don't need to include the dash sign). Click **Submit**.

> If you entered the code incorrectly, you don't have to wait for a new one. Enter the code again. It is valid until it expires.



8. If you are not already logged into your account in your browser, a login screen will be displayed. If you are an Externally managed user, click **Sign in with Microsoft** and enter your Microsoft credentials. If you are an Internally managed user, enter your Dispatcher Paragon Cloud credentials.

9. If you are an Externally managed user synchronized from Azure AD, grant the requested permissions by clicking **Accept**.



> Granting permissions is necessary only when registering your first OMNI Bridge.
>
> Note that this is a different Cloud Print Management application than the one for which you granted permissions during Dispatcher Paragon Cloud activation.

10. Your OMNI Bridge device will be linked to your Dispatcher Paragon Cloud.
11. Continue to chapter Managing Edge devices as the next steps are performed in Dispatcher Paragon Cloud Portal.

2.3.6 CONFIGURING MFDS FOR PURE CLOUD TERMINALS

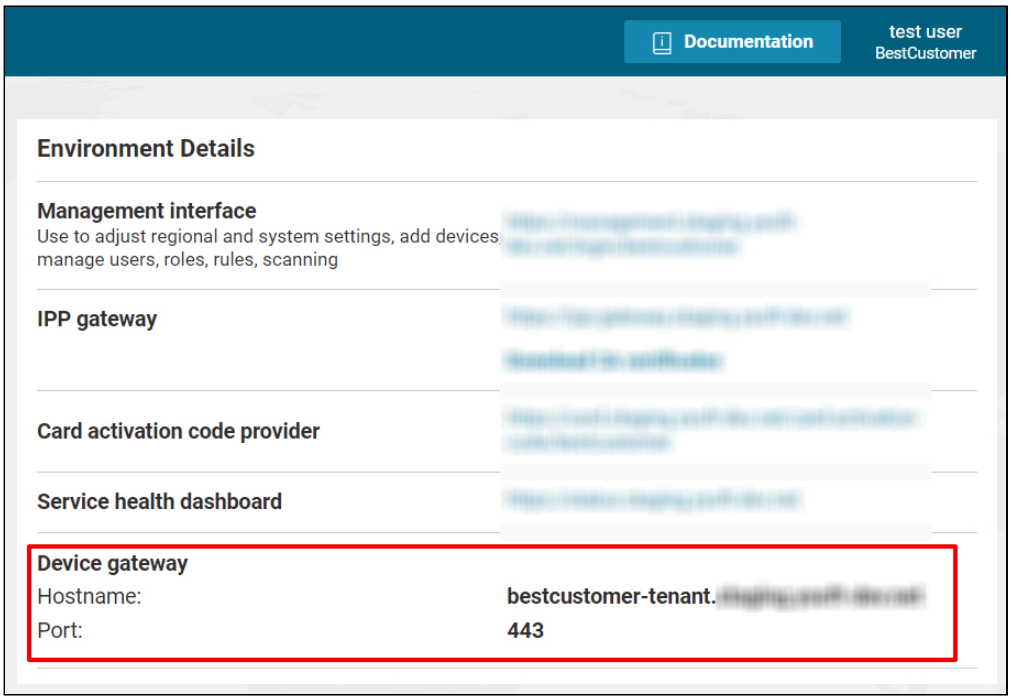
Configuring Konica Minolta MFDs for Dispatcher Paragon Cloud Terminal

This section describes the prerequisites, the installation, and configuration of the Dispatcher Paragon Cloud Terminal.

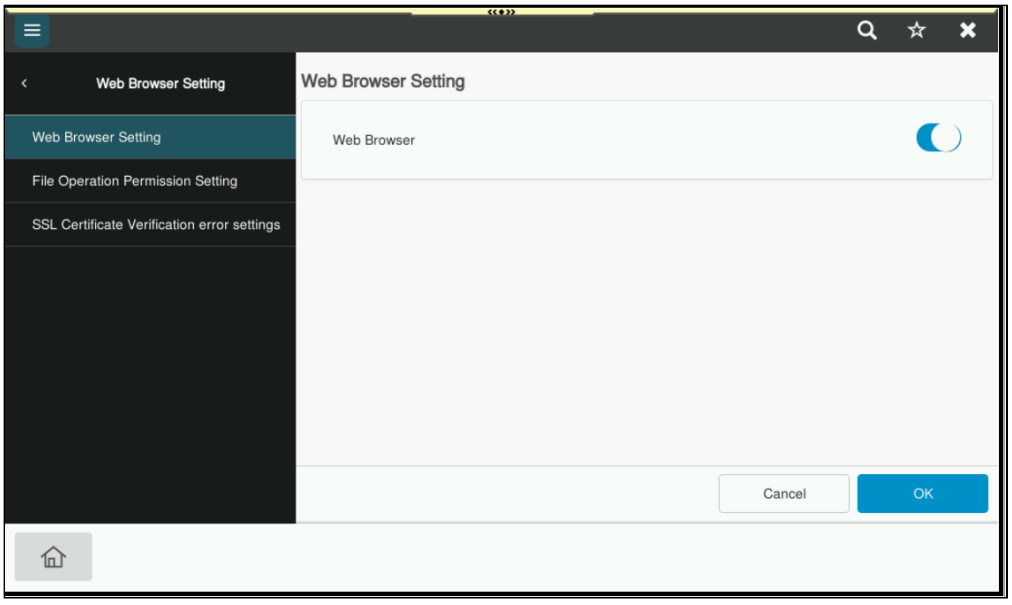
Prior to installation

1. Prepare your Konica Minolta MarketPlace credentials.

2. Prepare the **Device gateway** for your Dispatcher Paragon Cloud. You can find it in the dashboard of Dispatcher Paragon Cloud Portal. For more information on the Cloud Portal, see Dispatcher Paragon Cloud Portal guide.



3. Enable the web browser on your MFD. The procedure might differ slightly depending on your MFD model. In case of discrepancies, see the manual for your MFD model.
   a. At the MFD panel home screen, tap **Utility > Administrator**.
   b. Enter the Administrator password and tap **OK**.
   c. Tap **Network > Web Browser Setting > Web Browser Setting**.
   d. Enable the web browser and tap **OK**.

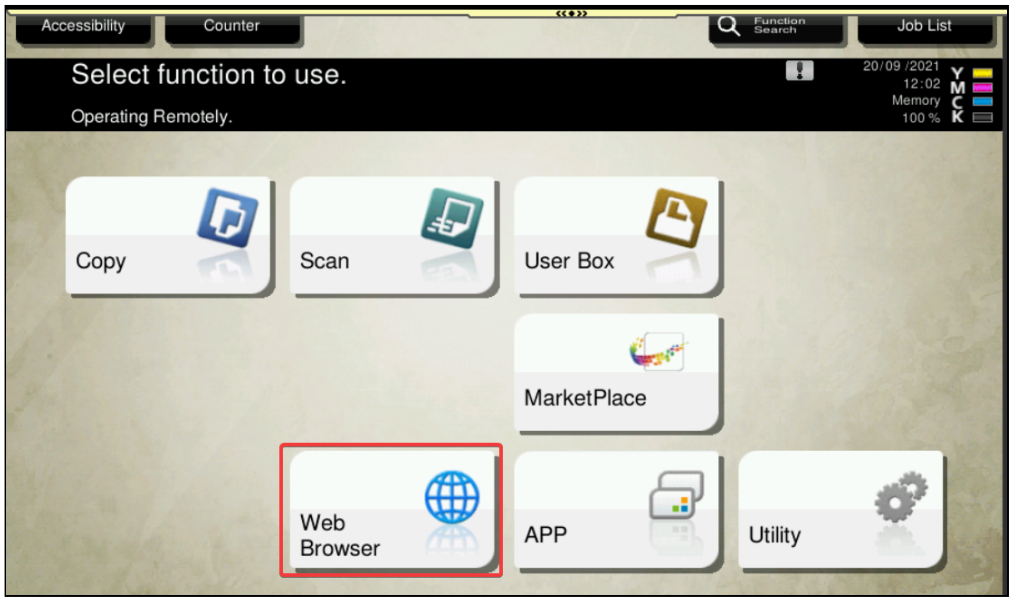


Proxy settings

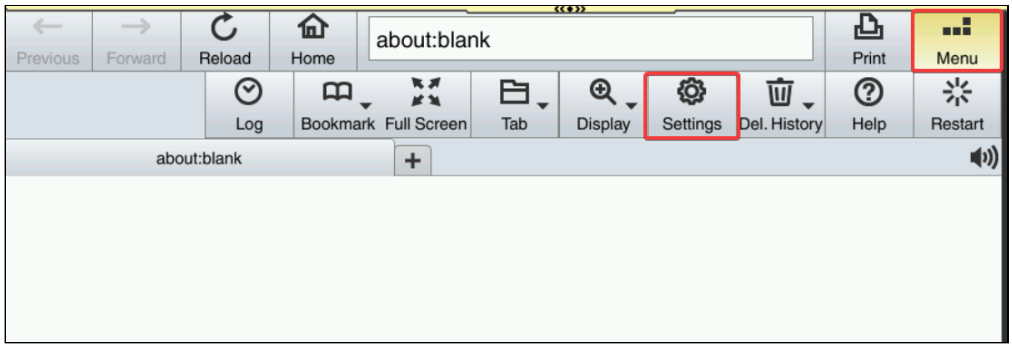
If your MFD needs to access the public Internet via a dedicated (non-local) gateway, such as a VPN with a proxy server, the Dispatcher Paragon Cloud Terminal supports this, but you must perform the following steps in the MFD settings of the browser and the WebDav Client.

Configuring the browser

1. On the MFD panel home screen, tap **Web Browser**.

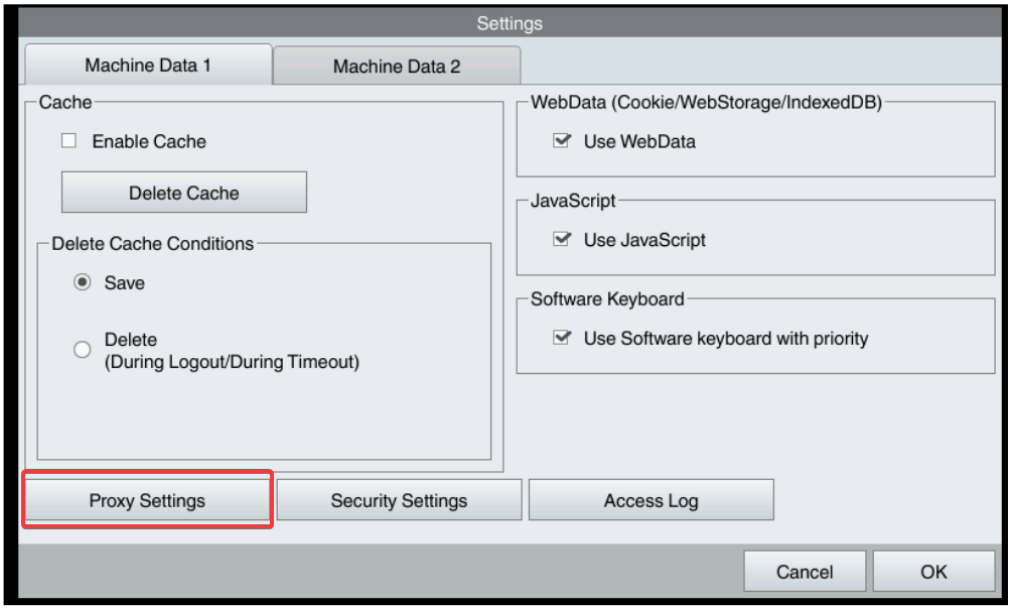


2. In the Web Browser, tap **Menu** and then tap **Settings**.

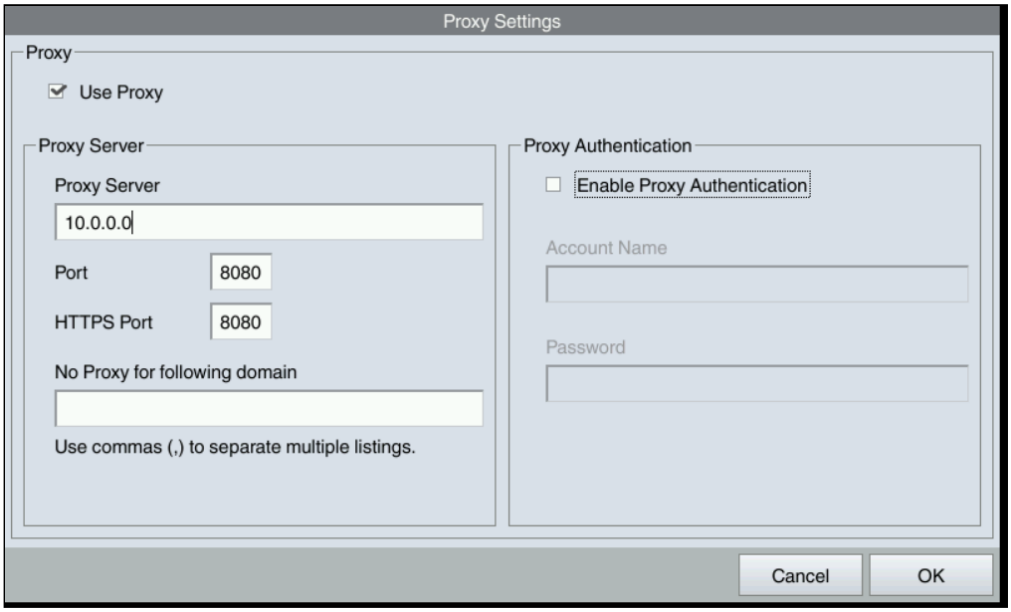


3. Authenticate with the Administrator password.

4. Tap **Proxy Setting**.



5. Check the **Use Proxy** checkbox and enter the **Proxy Server** address and ports.



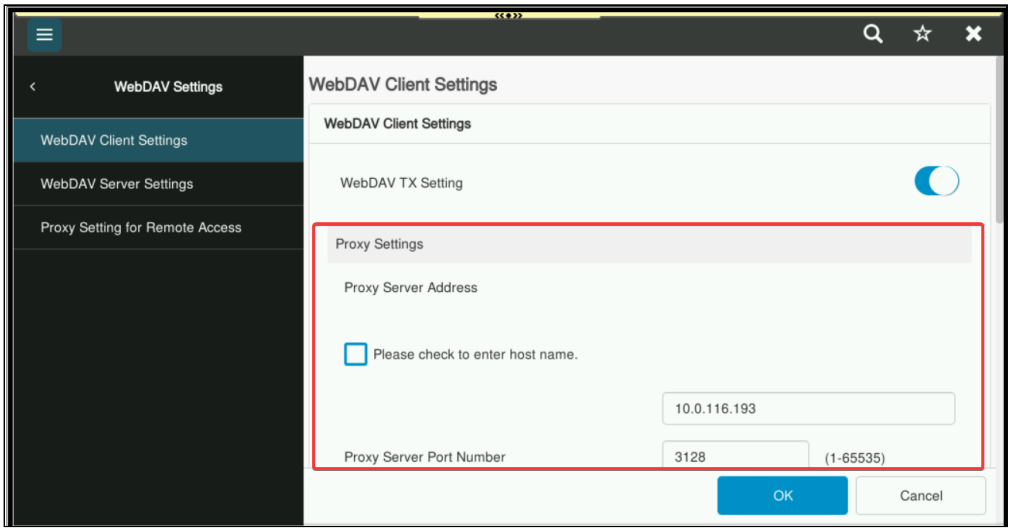
6. If the Proxy server needs authentication, check also **Enable Proxy Authentication** checkbox and fill Account Name and Password in **Proxy Authentication settings**.

7. Tap **OK** to save the proxy settings.

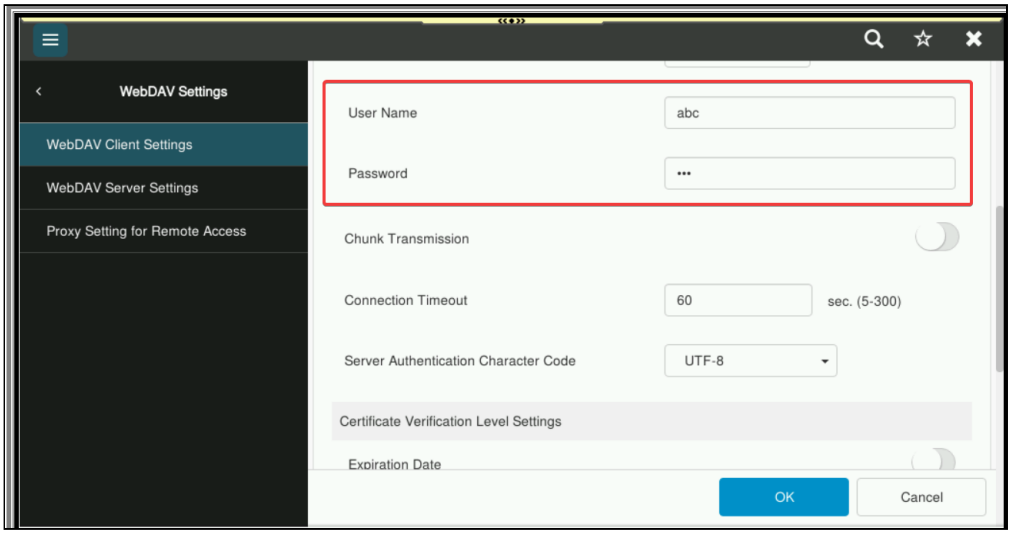
Configuring the WebDav client

1. At the MFD terminal, log in as Administrator and go to the **Administrator Settings > Network > WebDAV Settings > WebDAV Client Settings**.

2. Enter the **Proxy Server Address** and **Proxy Server Port Number**.



3. If the Proxy server needs authentication, enter the User Name and Password.



4. Tap **OK**.

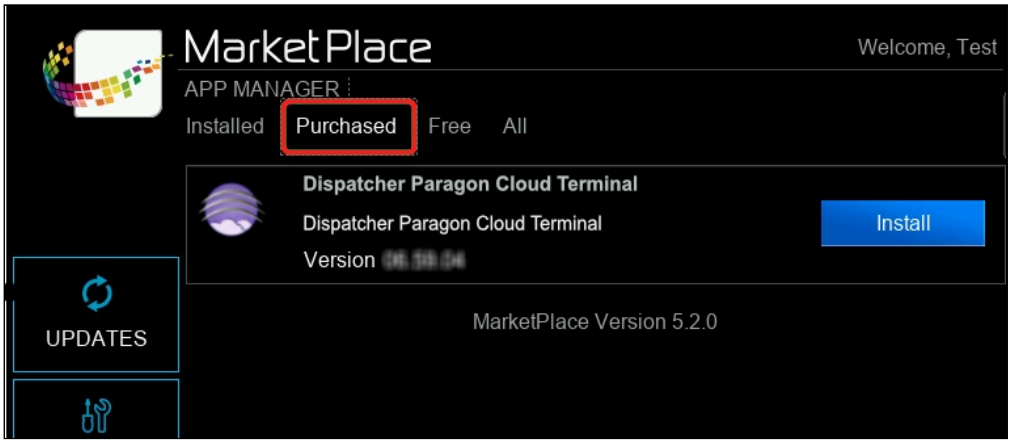
Installation on premise

In some cases the installation can be performed remotely via Remote Panel. For details on using Remote Panel, contact your service representative.

1. On the MFD terminal, tap the **MarketPlace** icon. Then tap the **App Manager** icon in the bottom left corner. You will be prompted to log in.
2. Enter your Konica Minolta MarketPlace credentials and tap **Login**.

When you log in for the first time, you will be prompted to enter both the administrator password for the MFD and the MarketPlace credentials.

3. Tap the **Purchased** list to see the applications for which you have a license.



4. Tap **Install** next to the **Dispatcher Paragon Cloud Terminal** application. The application will start installing immediately.

5. After installation, you will see the **Dispatcher Paragon Cloud Terminal** application in the **Installed** list, together with the **Settings** and **Uninstall** options.

Installation from Konica Minolta MarketPlace

Alternatively, you can perform the installation from Konica Minolta MarketPlace.

Prerequisites:

Your MFD(s) must be listed in the **Available devices** in your account at https://konicaminoltamarketplace.com/. To achieve this, you must log in to MarketPlace on the MFD panel at least once:

1. On the MFD terminal, tap the **MarketPlace** icon. Then tap the **App Manager** icon in the bottom left corner. You will be prompted to log in.

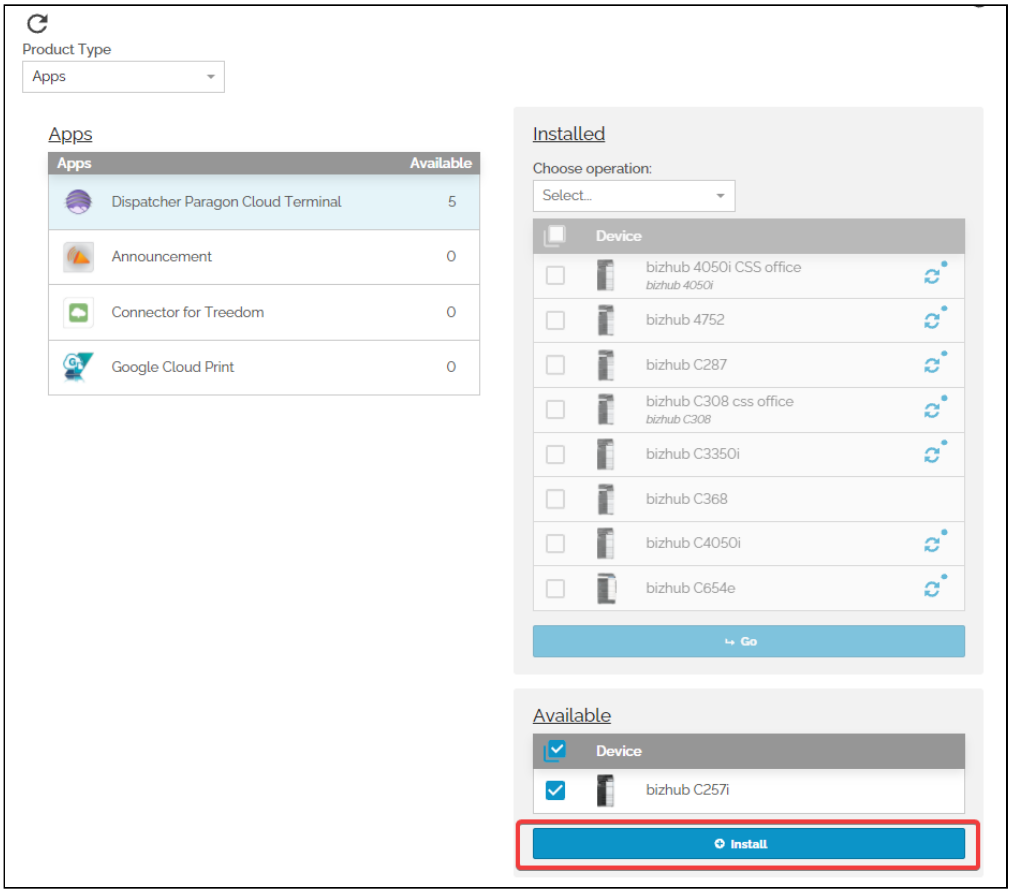
2. Enter your Konica Minolta MarketPlace credentials and tap **Login**.

To install Dispatcher Paragon Cloud Terminal from MarketPlace, perform the following steps:

1. Log in to https://konicaminoltamarketplace.com/.

2. Click **Apps & Licenses** in the navigation menu.

3. In **Apps**, click **Dispatcher Paragon Cloud Terminal**.

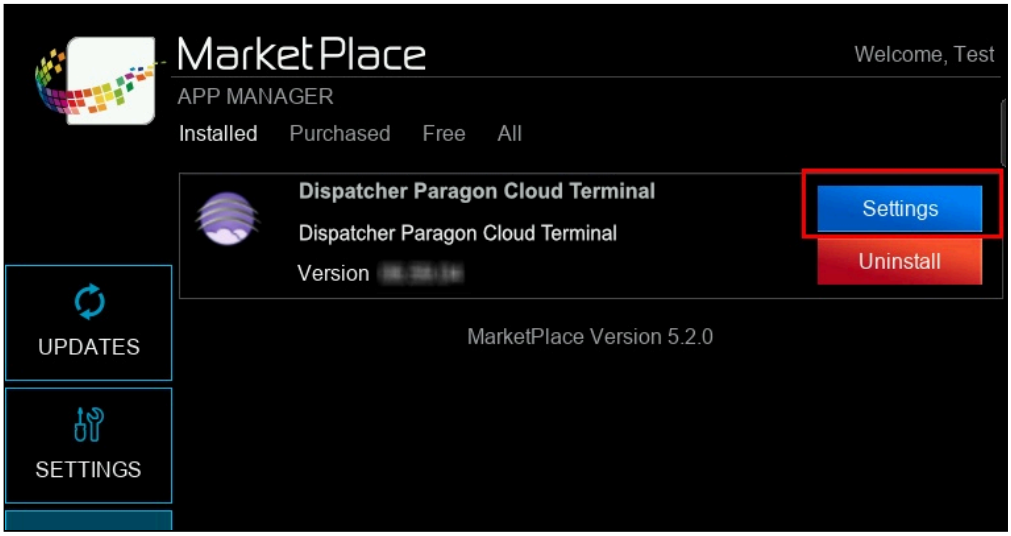


4. Select the MFD and click **Install**.

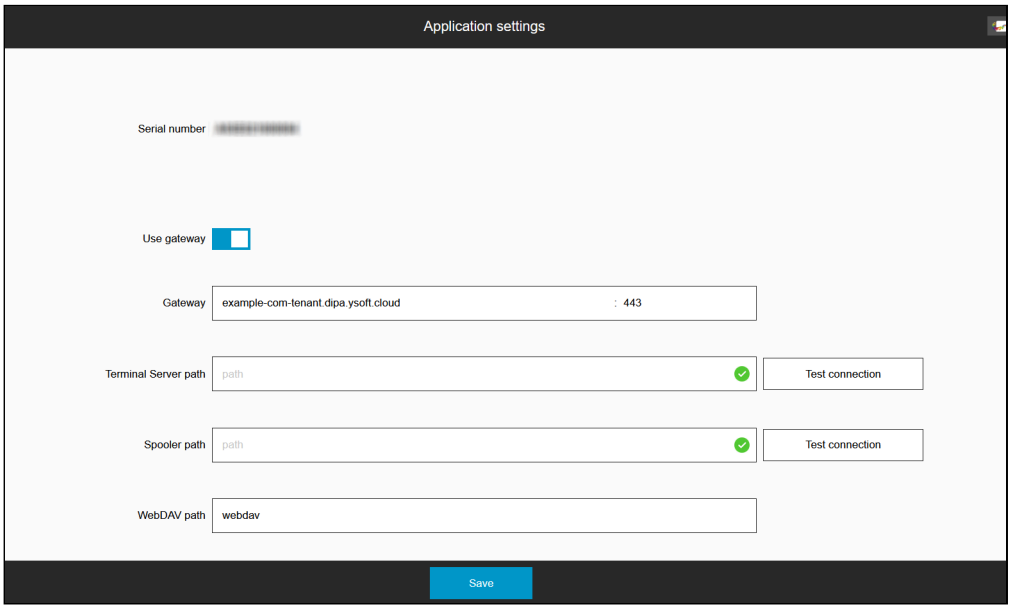
5. When finished, go back to the MFD panel to configure the Dispatcher Paragon Cloud Terminal.

Configuration

1. After logging in to the MarketPlace at the MFD panel, tap the **Settings** option.



2. In Gateway, enter the **Device gateway**. The exact URI is environment and customer-specific. Use port 443.



The device gateway is composed as `<modified-domain>-tenant.<region>.dipa.cloud`

where:

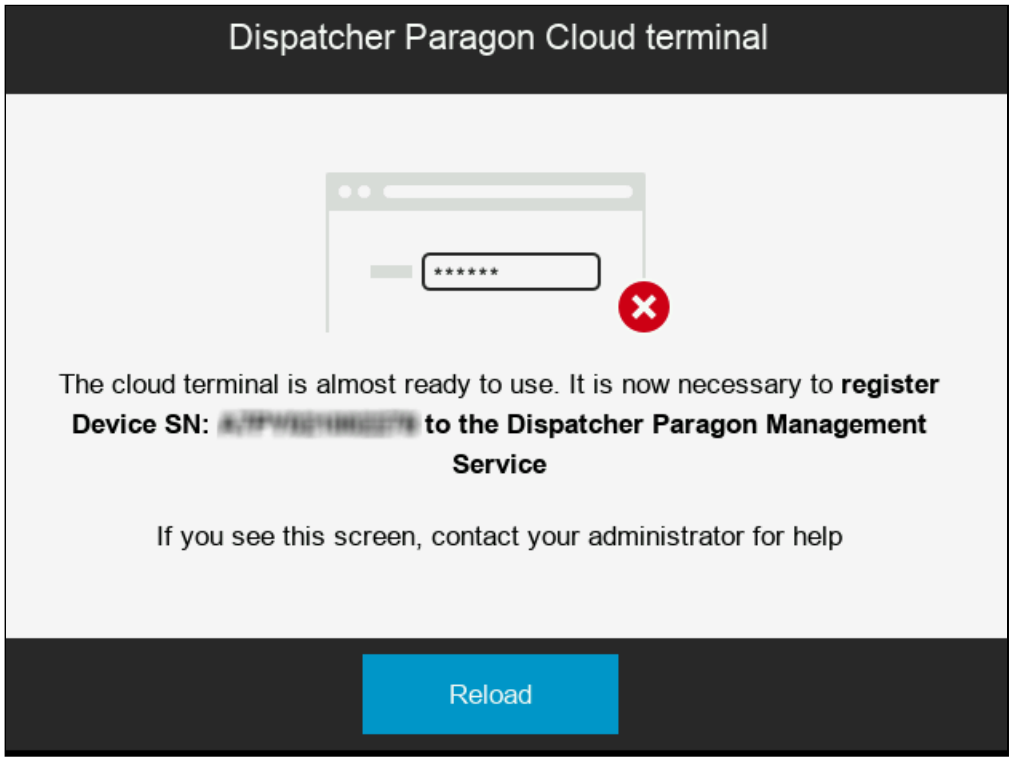
- `<modified-domain>` is automatically created from the customer domain by:
  1. replacing dots with dashes
  2. replacing dashes with double dashes. E.g. domain "nice-example.com" is transformed into "nice--example-com"
- `<region>` is where your service is deployed. You can find it in your *Welcome to Dispatcher Paragon Cloud* email. The available regions are: `EU1`, `APAC1`, `AU1` and `US1`.

Examples:

A device gateway for a customer with domain best-company.com in region APAC1 would be: `best--company-com-tenant.APAC1.dipa.cloud`

A device gateway for a customer with domain *bestcompany* in region EU1 would be: `bestcompany-tenant.EU1.dipa.cloud`

3. Leave the **Terminal Server path** and the **Spooler path** fields blank.
4. Test the connection by tapping both **Test connection** buttons to validate that you have entered the correct gateway.
5. Tap **Save** to finish the configuration.
6. A message will appear, requiring you to register the MFD in the Dispatcher Paragon Management Service. To do this, continue to Managing devices.

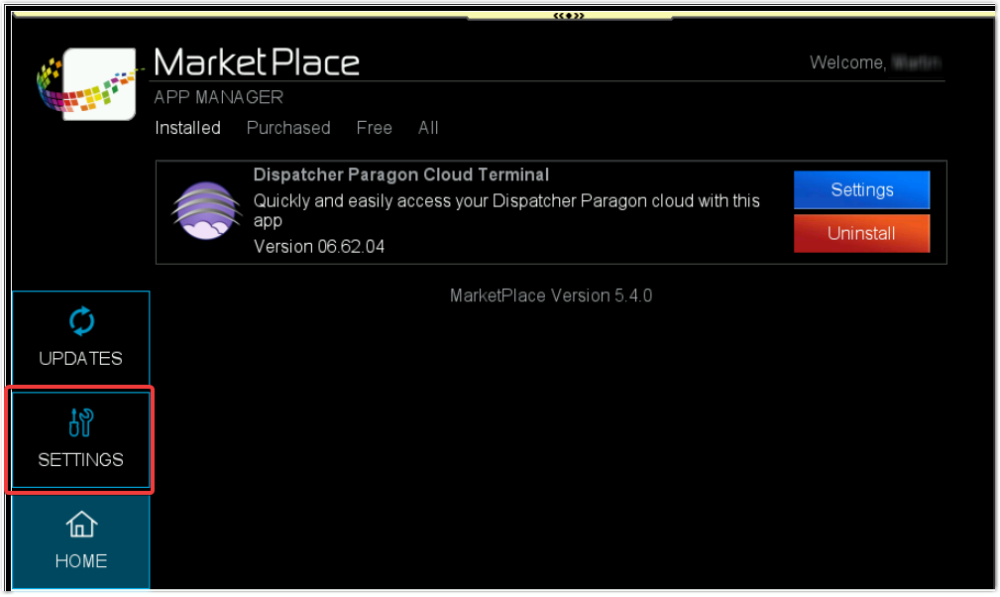


Dispatcher Paragon Cloud Terminal shortcut

The shortcut at the MFD panel is created automatically during the installation process. If it wasn't created, you can add it manually by performing the following steps:

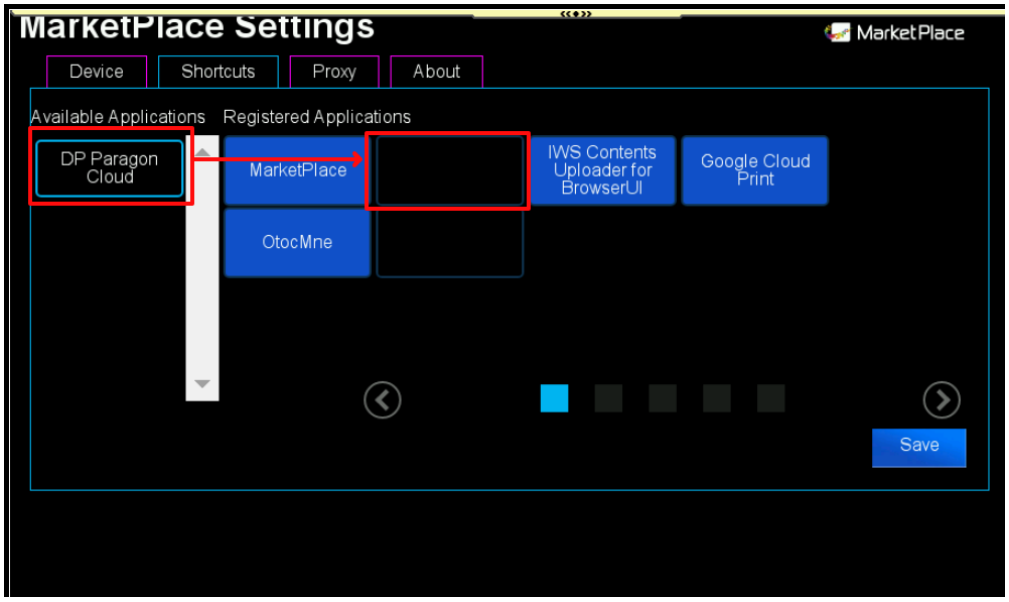
1. At the MFD panel, return to the MarketPlace main screen.

2. Tap **Settings** in the left-hand menu.



3. Tap **Shortcuts**.

4. Move **DP Paragon Cloud** to the Registered applications.

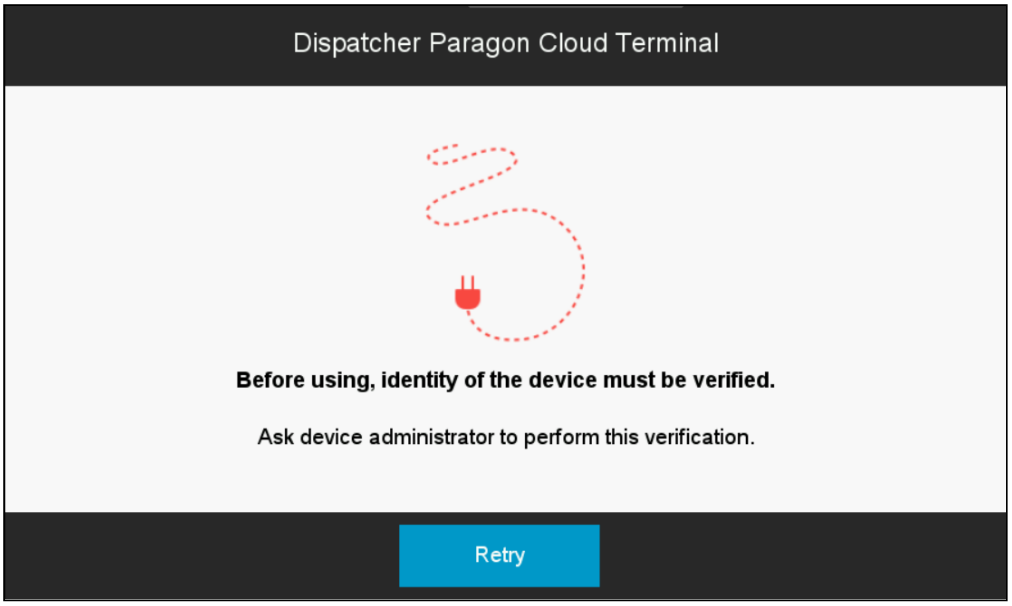


5. Click **Save**.

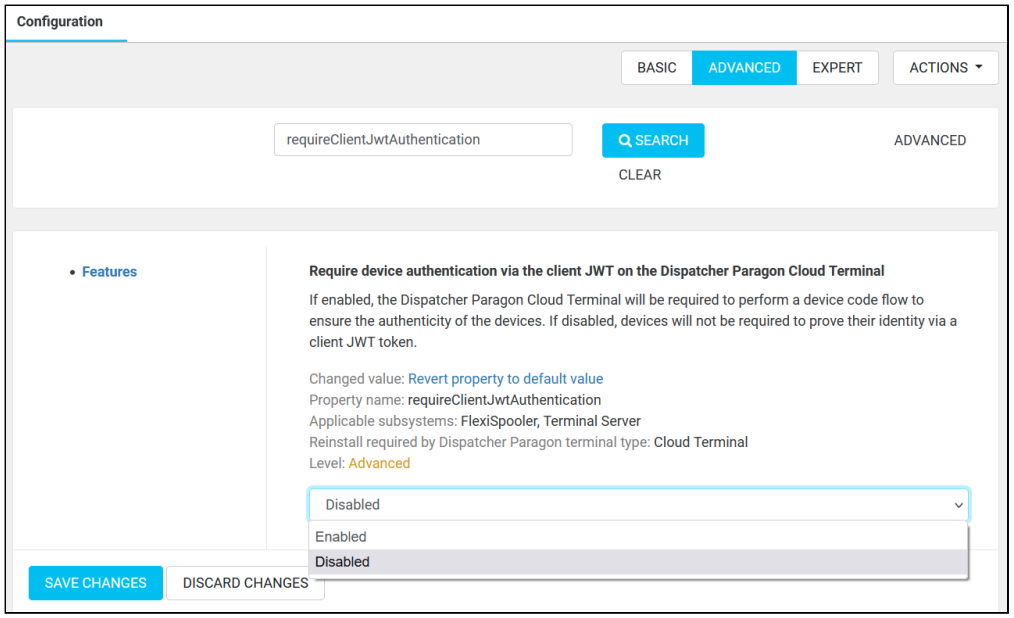
Device authorization grant

If you want users to be able to authenticate with PIN, you need to perform the device authorization grant on MFD. Without performing the device authorization grant, the terminal will display the following screen.

To perform the grant, you must have the Customer administrator role in Dispatcher Paragon Cloud Portal. See Dispatcher Paragon Cloud Portal guide.

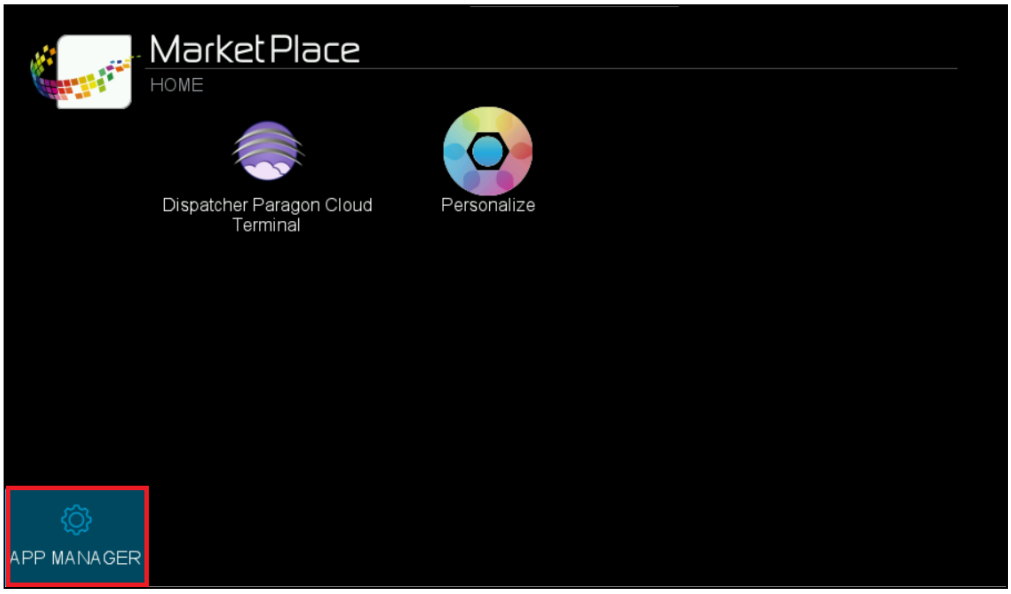


1. Log in to the management interface with your administrator account. Navigate to **System** > **Configuration**. Select **Advanced** or **Expert** settings. Search for *requireClientJwtAuthentication*. Select **Enabled** from the drop-down menu and click **SAVE CHANGES**.

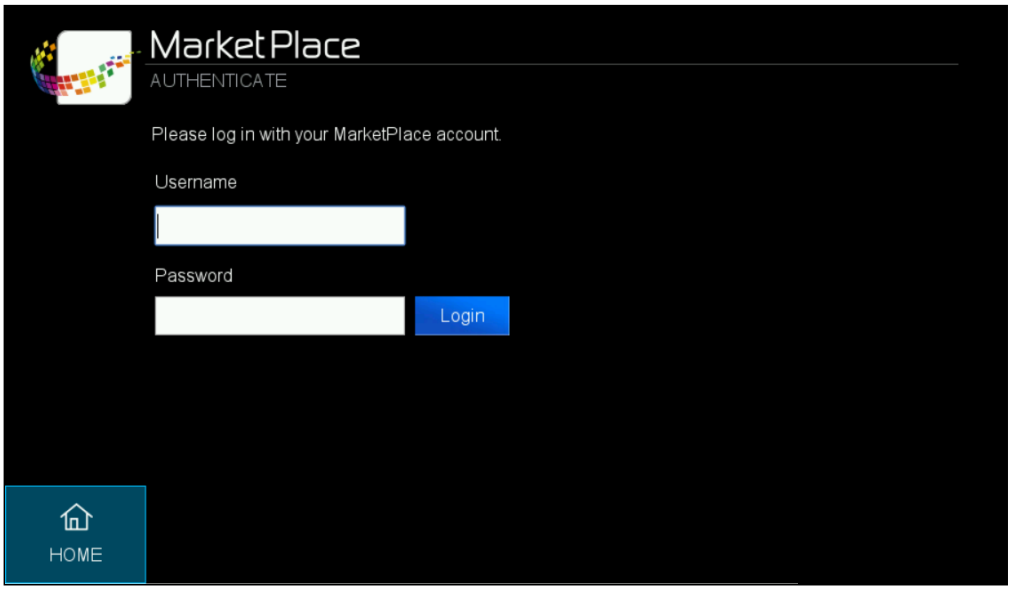


2. Confirm your changes by clicking the **SAVE CHANGES** button.

3. At the MFD panel, navigate to MarketPlace and tap APP MANAGER.

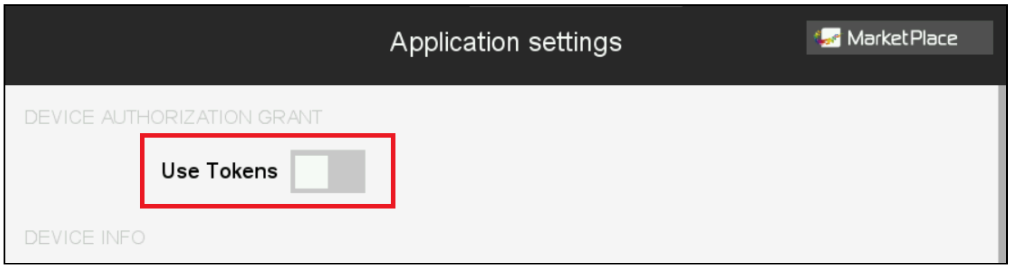


4. Enter your MarketPlace credentials and tap **Login**.

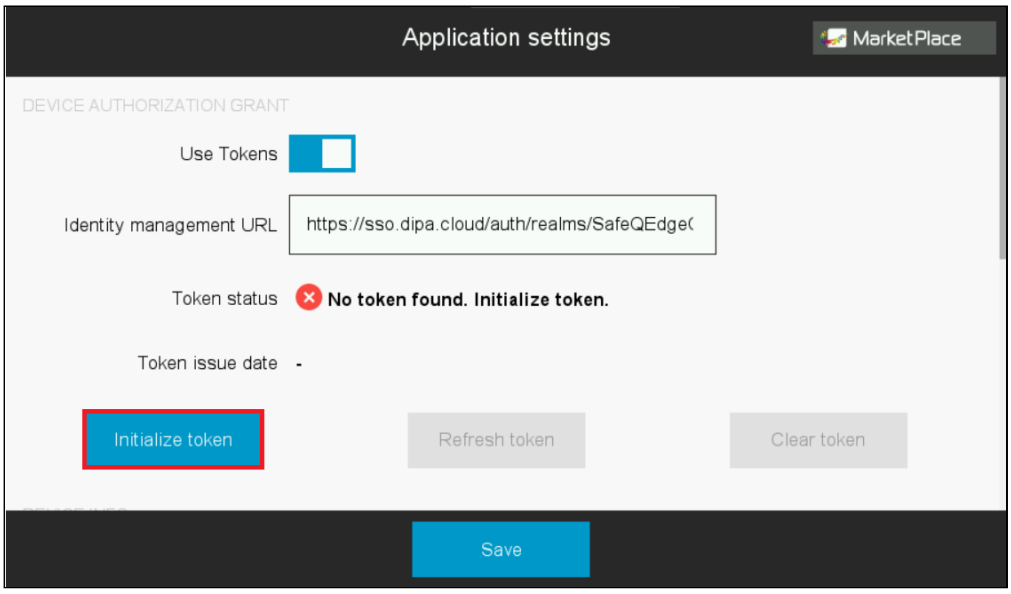


5. Tap **Settings** next to Dispatcher Paragon Cloud Terminal.

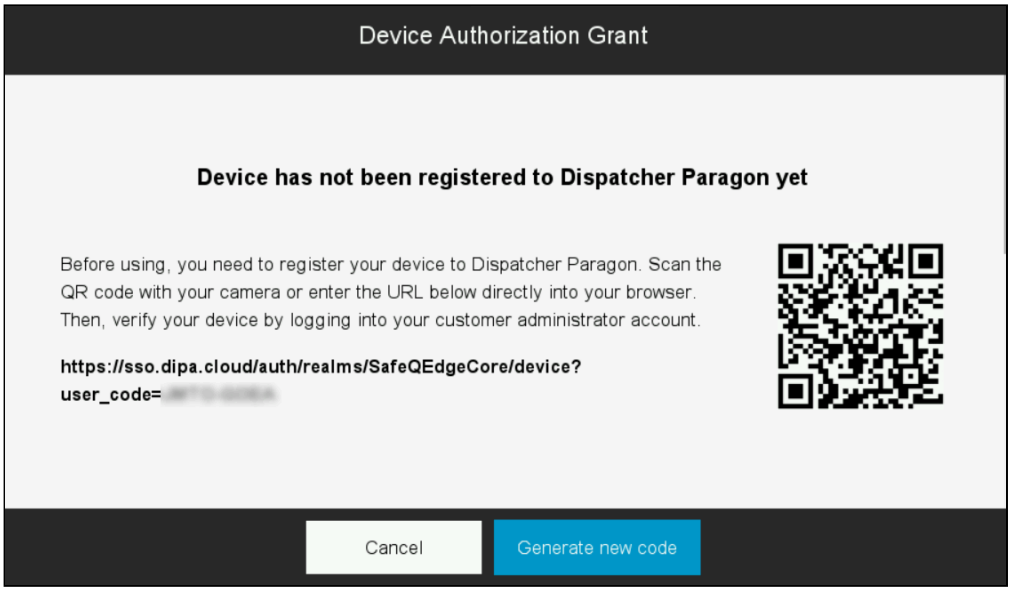
6. On the **Application settings** screen, enable the **Use Tokens** toggle switch.



7. Use the pre-filled (default) Identity management URL and tap **Initialize token**. The default URL is https://sso.dipa.cloud/auth/realms/SafeQEdgeCore/.

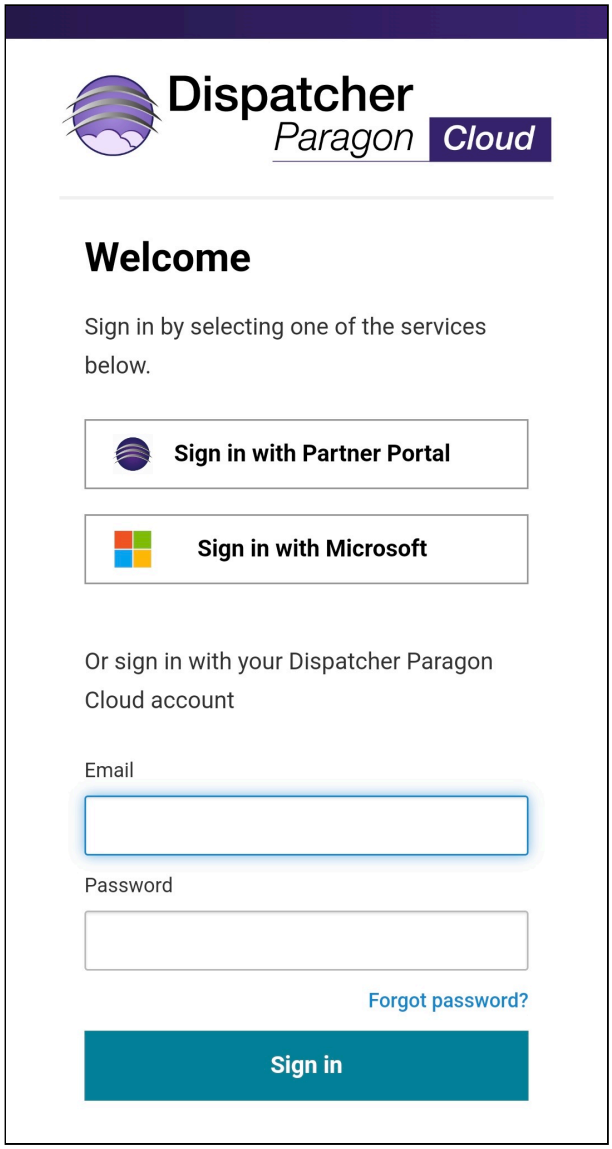


8. A screen with a QR code and URL address is displayed. Use a Smartphone or web browser to open the URL.

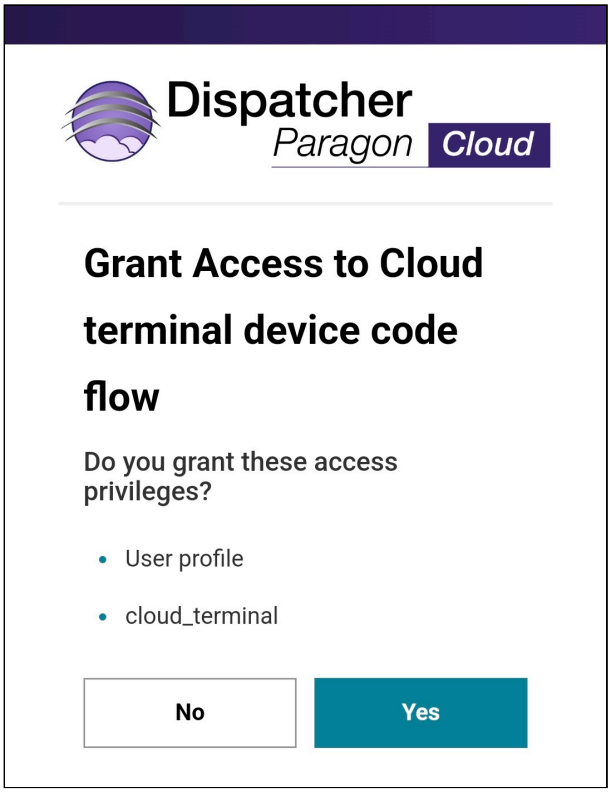


9. If you are an Externally managed user, click **Sign in with Microsoft** and enter your Microsoft credentials. If you are an Internally managed user, enter your Dispatcher Paragon

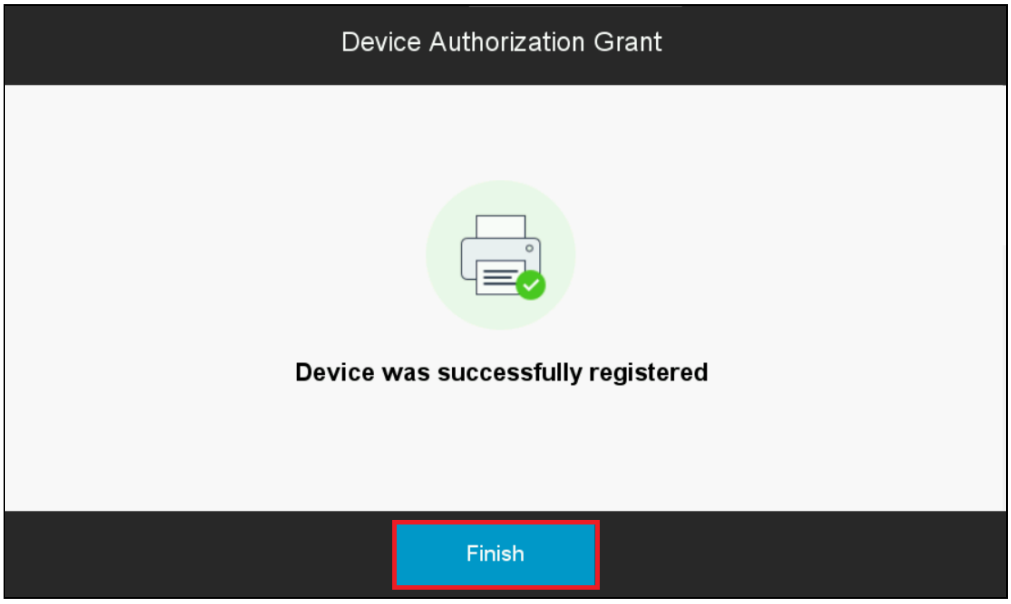
Cloud credentials and click **Sign in**.



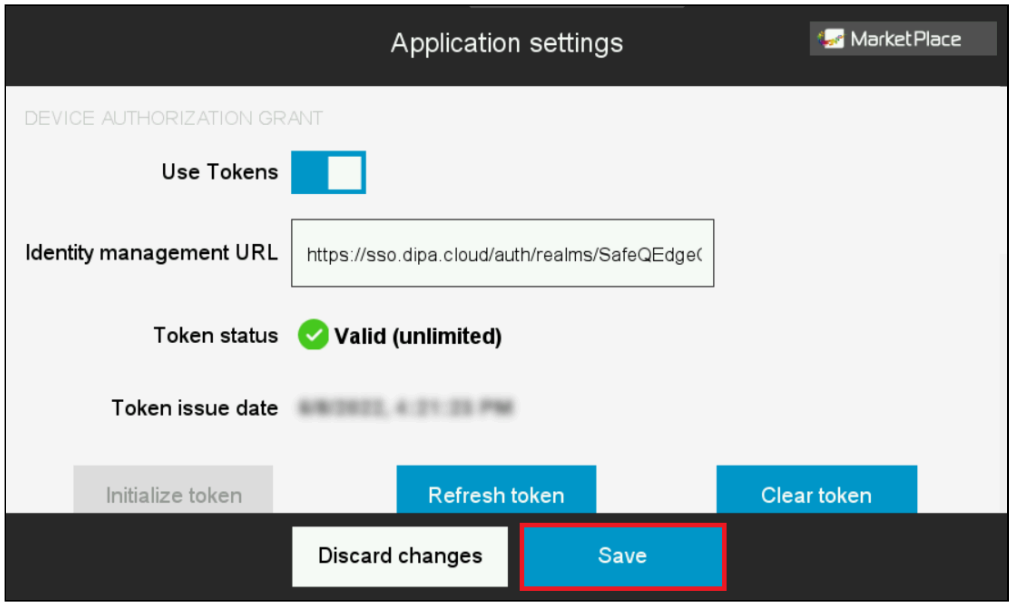
10. Grant access privileges by clicking **Yes**.



11. Back on the MFD panel, tap **Finish**.



12. The **Application settings** screen will display details about the token status and token issue date. Tap **Save**.



Error message "Device is not registered yet" when initializing the token

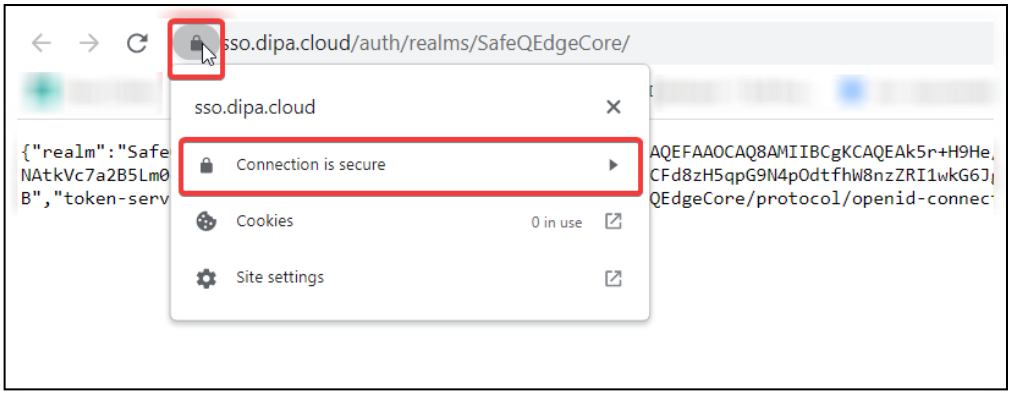
If you receive an error message "Device is not registered yet" after tapping the **Initialize token** button on the MFD panel, import the root certification authority of Identity management into the printer. For security reasons, identity management requires server certificate validation. In some cases, the printer may not have the latest certificates installed. If your environment setup is configured with proxy which is using a custom certificate, you will also need to import the certificate provided by your company.

To obtain a certificate from Identity management:

1. In your browser, open the Identity management URL: https://sso.dipa.cloud/auth/realms/SafeQEdgeCore/ (or simply https://sso.dipa.cloud).

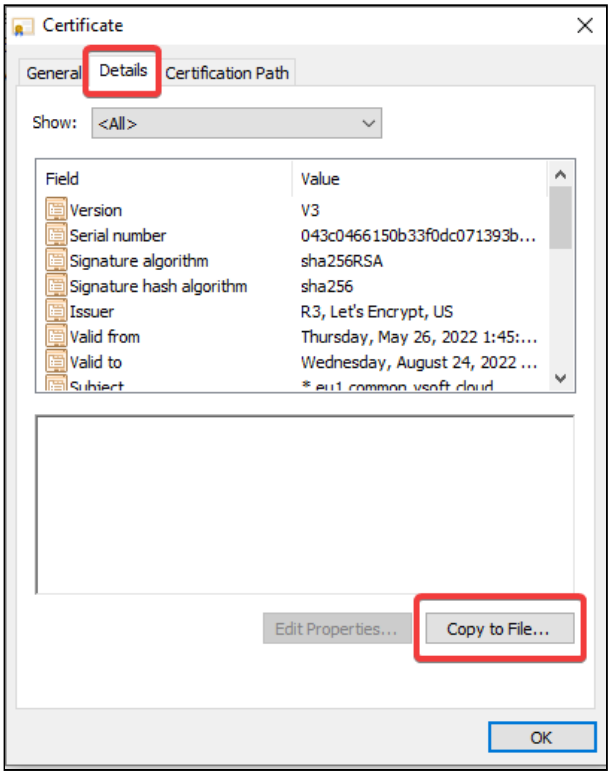
2. Export the website certificate from your browser and save it to your workstation. Make sure that the certificate format is supported by your printer. The .CER format usually is.

   a. In Google Chrome, click the lock icon next to the URL. Then click **Connection is secure**.



   b. In the next dialog window, click **Certificate is valid**.

c. The certificate will now be displayed. Click the **Details** tab and then click **Copy to file**.



d. A **Certificate export wizard** where you can choose the export format will be displayed. Go through the wizard.

To import the certificate into the MFD, perform the following steps:

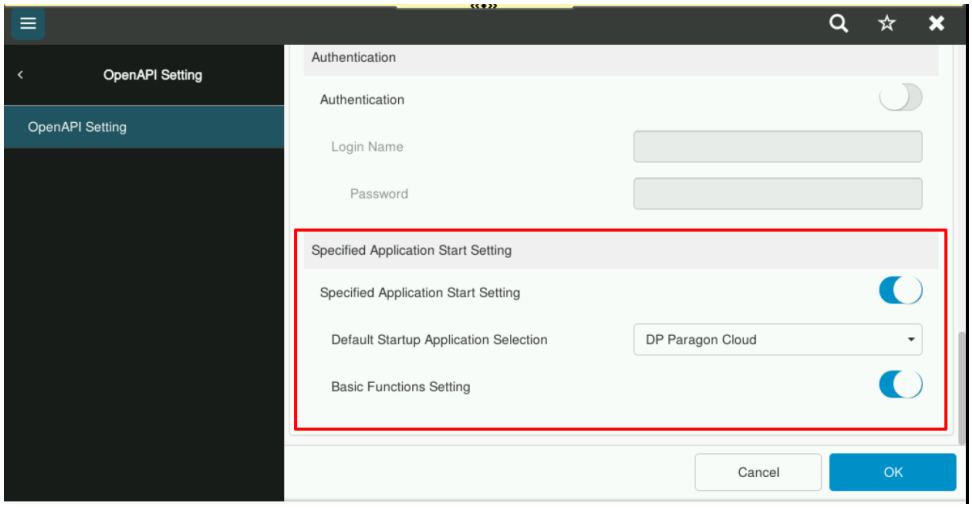
1. Import the certificate to your printer via remote connection. Go to **Administration > Security > PKI Settings > External Certificate Settings > Trusted CA Root Certificates > New Registration**. The exact procedure may vary according to your printer model. Refer to the guide for your printer model.
2. If this doesn't help, ask your service representative to update the printer firmware.

Kiosk mode

If you want the Dispatcher Paragon Cloud Terminal to be the default application that appears after the MFD starts or wakes up from sleep mode, perform the following steps on the MFD terminal:

1. Go to **Utility** > **Administrator**. Enter the administrator password.
2. Go to **Network** > **OpenAPI setting** > **OpenAPI setting**.
3. Enable the **Specified Application Start Setting** toggle switch.
4. Select **Dispatcher Paragon Cloud Terminal / DP Paragon Cloud** from the **Default Startup Application Selection** field.

5. Enable the **Basic Functions Setting** toggle switch.



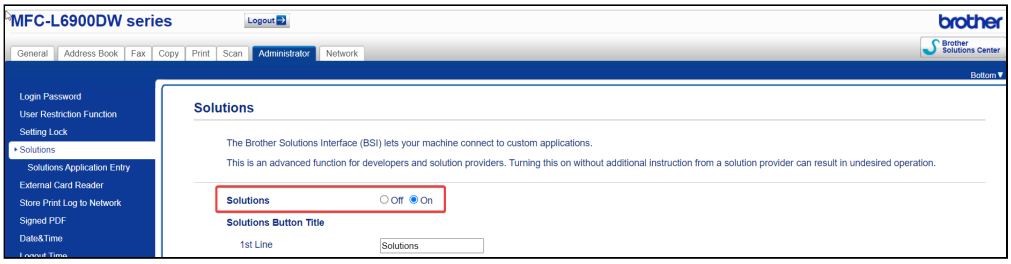
6. Tap **OK**.

2.3.7 CONFIGURING MFDS FOR EMBEDDED TERMINALS

Configuring Brother MFDs

Requirements

1. Brother Solutions Interface is enabled.
   a. Log in to the MFD's web interface.
   b. Go to **Administrator > Solutions**.
   c. Set the **Solutions** to **On**.



2. The firmware is updated to the latest version.
3. No error messages must be displayed on the device display before you start installing the embedded terminal.

> ⚠ If the device displays the "Unusable device" error message, close it before installation. If you cannot close it, unplug the card reader before installation and plug it back when finished.

4. SNTP server is specified.
    a. Log in to the MFD's web interface.
    b. Go to **Network > Protocol > SNTP > Advanced settings**.
    c. Fill in the **Primary SNTP Server Address** field.
5. Before the embedded terminal installation, there must be no CA certificates uploaded to the MFD. During the installation of the embedded terminal, one CA certificate will be uploaded to the MFD.
    a. To check that, log in to the MFD's web interface.
    b. Go to **Network > Security > CA certificate > CA certificate list**.
    c. If there are any certificates listed, delete them.
6. If you plan to install the embedded terminal with an authentication method that includes card authentication you must configure the Card reader first.
    a. In YSoft Card Reader Tool, configure your Card reader and set the following values:
        1. In **USB mode**, select **USB keyboard emulation**.
        2. In **Keyboard layout**, select **1 - US**.

Limitations

- Logout by card is not supported.
- It is not possible to copy or scan during printing. The Dispatcher Print and Dispatcher Scan applications are not available during printing.
- Print job preview is not supported.
- Print job finishing options are not supported.
- The Address book doesn't support multiple choice and free text input.
- Billing code selection at the terminal is not supported.

Configuring Epson MFDs

Requirements

Devices based on **Epson Open Platform Version 1.0+** are supported. No special settings are needed.

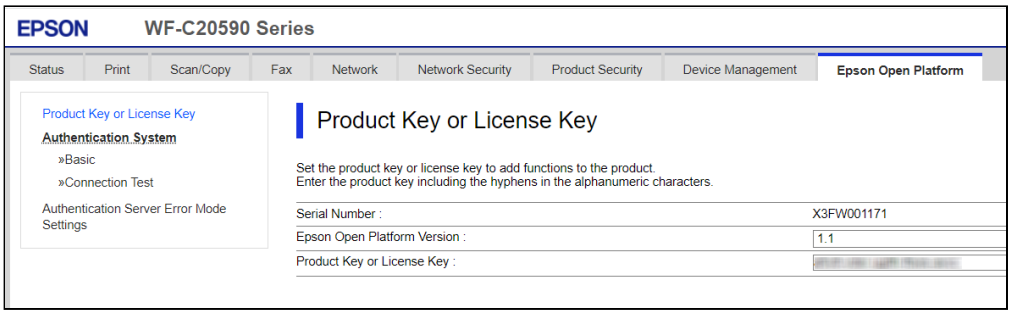
Limitations

- Scanned files can be delivered only via FTP.
- Scan settings combination must be supported by the MFD. If an invalid combination is selected, the scan will fail. Please refer to the documentation for your MFD model. For example, on some devices, only Black and white is supported for a multipage TIFF file

format or Black and white works only for PDF / Compact PDF. With image file formats the output is in greyscale.

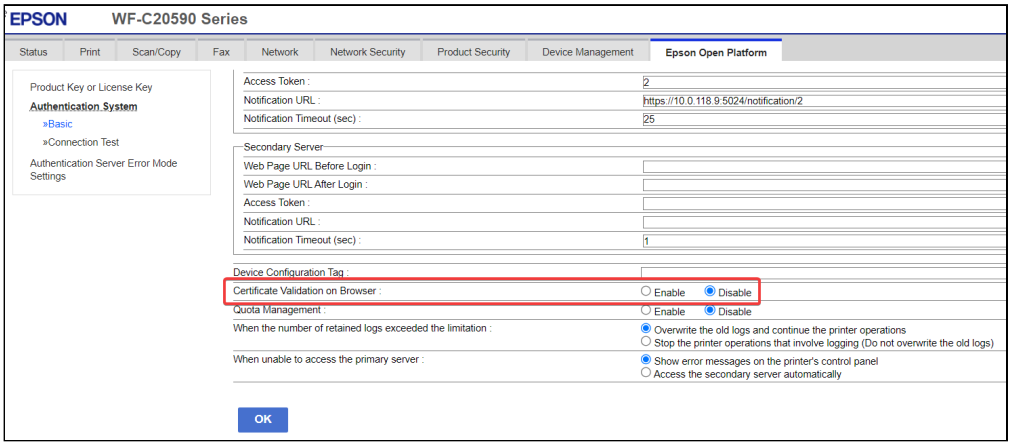
MFD configuration

1. Enable the Epson Open Platform:
   a. In your web browser, enter the IP address of the MFD. Your workstation must have network visibility to the MFD.
   b. You will see the Webconfig page of the MFD. Go to **Epson Open Platform Settings > Product key**.



   c. Enter the product key and click **OK**.

2. Disable the **Certificate validation on browser**:
   a. Go to **Epson Open Platform > Authentication System > Basic**.
   b. Set the **Certificate Validation on Browser** to **Disable**.



   c. Click **OK**.

Card reader configuration

1. In **YSoft Card Reader Tool**, configure your Card reader, and set values as follows:
   a. Set the **USB mode** to **USB keyboard emulation**.
   b. Set the **Keyboard layout** set to **1 - US**.

2. Connect the USB reader to Service USB port of the device.

- On A4 devices the Service USB port is usually located at the back of the device and covered by a sticker.
- On A3 devices the Service USB port is usually located inside the Card reader slot near the display.

3. Optionally, set the VID/PID of the USB reader via the web interface of the device.
   a. Log in as administrator, and navigate to **Card Reader settings**.
   b. Set Vendor ID to 0000 and Product ID to 0000 to disable whitelisting of USB readers. This is the default configuration.
   c. Set Vendor ID to 214C and Product ID to 0202 to accept only YSoft USB readers.

Configuring FUJIFILM BI MFDs

In order to install, uninstall, reinstall or delete the Embedded terminal, the MFD must be in power saver mode.

During configuration, the MFD sometimes requires a reboot. When prompted for reboot, follow the instruction displayed either in the web interface or on the MFD panel.

Requirements

If you plan to use Elatec TWN4 reader, make sure the reader has **Keyboard standard** firmware.

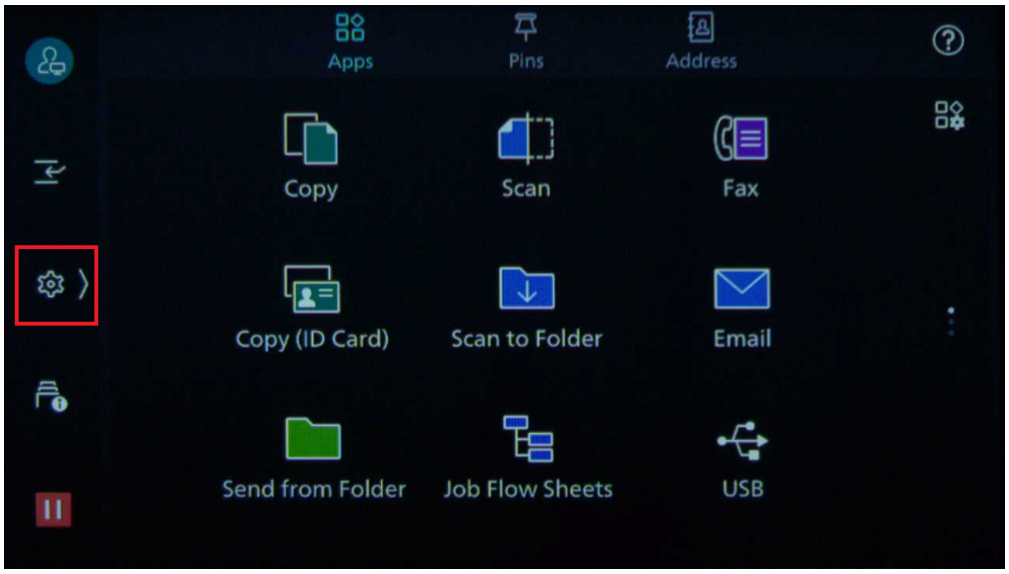
Limitations

- Fujifilm BI Embedded terminal does not work on MFDs which support only **Web Application Version** V5. The terminal requires V4.
- **Scan** Mixed Size Originals are not supported.
- When swiping a card at the card reader while the MFD is in sleep mode, the user is not authenticated.
- EPA card readers are not supported.
- Scan Workflows with Compact PDF are limited based on the possibilities of the MFD:
  - MFD must be capable of **MRC Compression**.
  - The color mode must be either **Grayscale** or **Full Color**.
  - The resolution must be **Low**, **Normal,** or **Fine**.
- Scan workflows with JPEG output 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 paper.
- If you set **System Settings > Common Service Settings > Screen/Button Settings > Screen Default** to value **Custom Service 4 – Dispatcher Paragon Authentication** on the MFD, users are redirected to Dispatcher Paragon Authentication screen after language change even if they are already authenticated.

General configuration

General settings

1. On the MFD panel, log in to MFD as a system administrator and go to the **Device settings**.



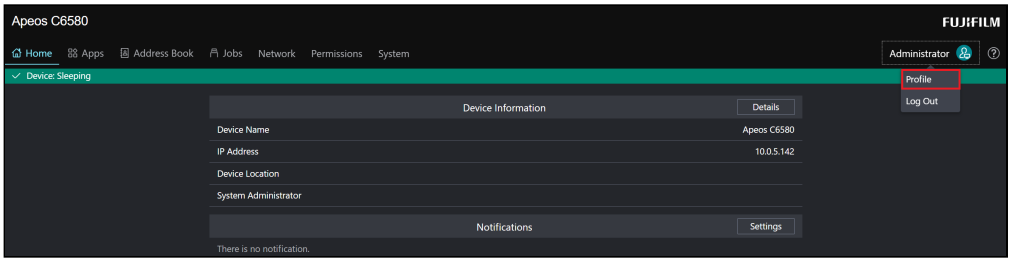
2. Go to **Device > System Settings > System Clock / Timers**.
    a. Configure date and time:
        1. Go to
        2. Set **Time Zone**.
        3. Set **Date**.
        4. Set **Time**.
    b. Optionally, configure NTP:
        1. Set **NTP time synchronization** to **On**.
        2. In **Time Server Address**, fill in your chosen NTP server address.
    c. Configure waiting time to release the print job:
        1. In **Specify Auto Print Time**, select **1 seconds**.

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.

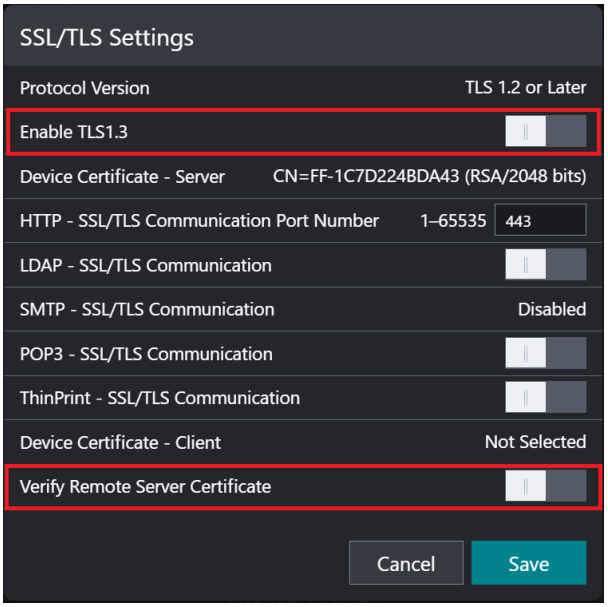
2. Machine digital certificate:

   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. You can enable TLS 1.3 as Dispatcher Paragon Cloud supports it.

   b. Make sure that **Verify Remote Server Certificate** is disabled. Otherwise, users would get an error message when opening the Dispatcher Paragon application on the MFD panel due to an untrusted certificate.

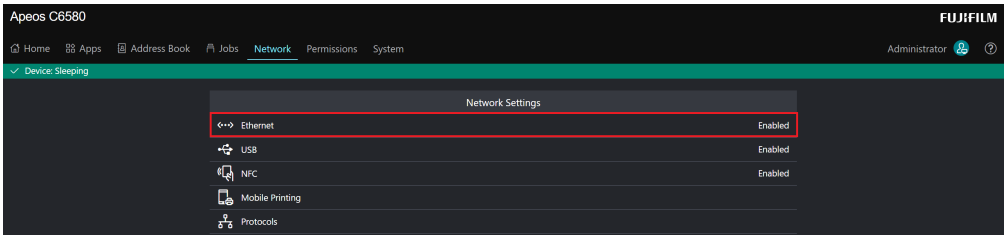


Network settings

In the MFD's web interface, configure the following:

1. Static IPv4 address:

a. Go to **Network > Ethernet**.



b. In **IPv4** section, click **Edit**.

c. Set **IP Address Resolution** to **STATIC**.

d. Fill in the **IP address**, the **Subnet Mask**, and the **Gateway Address** according to your network.

e. Click **Save**.

2. Protocols:

a. Go to **Network > Protocols**.

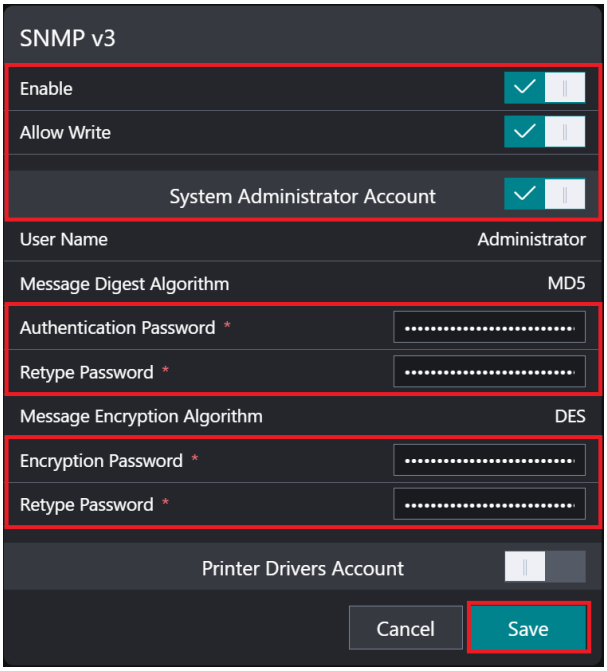
b. Verify that the following protocols are enabled:

1. **HTTP/S** – Check that **Port (HTTP/HTTPS)** is set to **Enable All**. You can also set it to Enable **HTTPS Only** which disables the HTTP port.
2. **FTP**
3. **LPD** – To receive print jobs via LPR (for example when using Client v3 in client-spooling mode), LPD must be enabled.
4. **IPP** – To receive print jobs via IPP/IPPS, IPP must be enabled.
5. **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 need to enable it before MFD firmware upgrade.

6. **SNMP (v3)** – Set **SNMP v3** to **Enable**. Set **Allow Write** to **Enable**. Enable System Administrator Account and enter the **Authentication Password** and **Encryption**

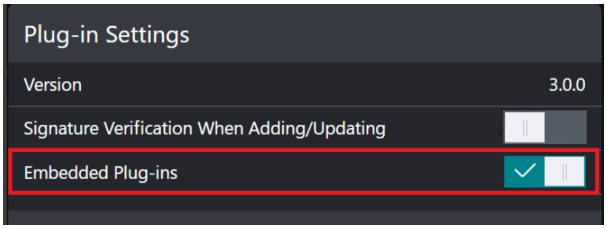
password used in your organization. Click **Save**.



> Enter the same **Authentication Password** and **Encryption password** in the **SNMP** section when installing the embedded terminal from Dispatcher Paragon Cloud Management interface.

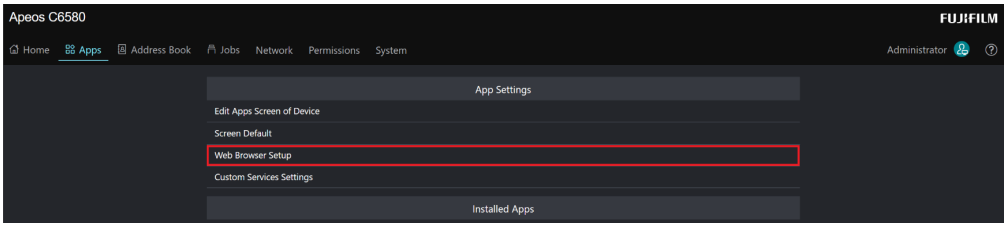
Plug-in settings

1. Go to **System > Plug-in Settings**.
2. Enable **Embedded Plug-ins**.

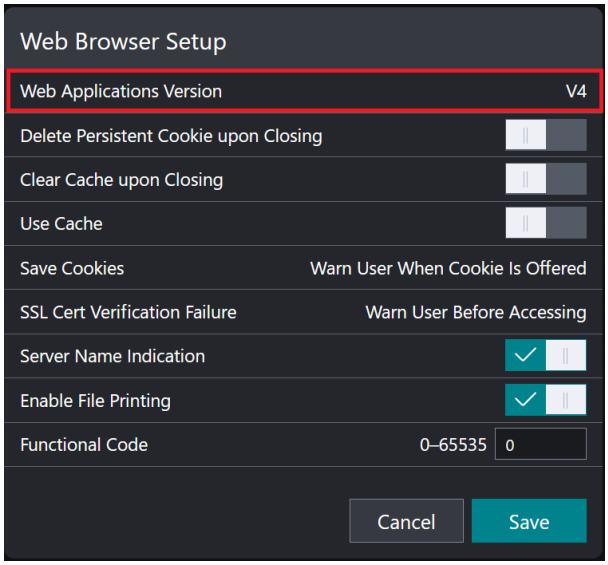


Web browser settings

1. Go to **Apps > Web Browser Setup**.



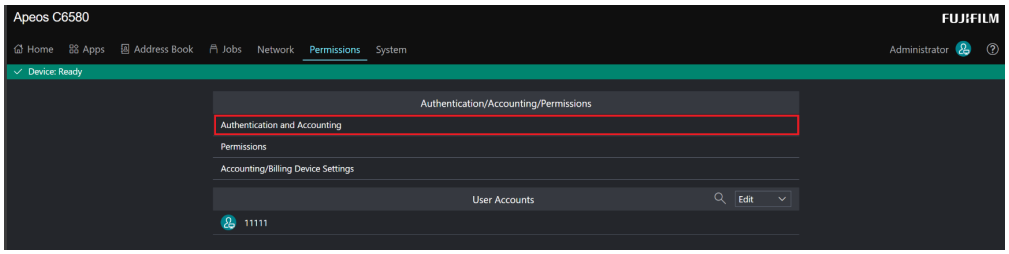
2. Make sure that in **Web Application Version** the selected value is **V4**.



Worldwide models do not have the **Web Application Version** option, as they only support V5. FUJIFILM BI Embedded terminal 1.0.0 does not support version V5.

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**.

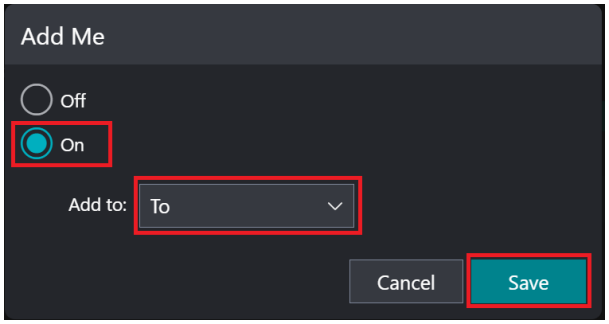
Do not enable Use of IC Card when Card Reader is not connected or you will not be using authentication with the card.

Scan-related settings

To enable the auto-completion of email addresses in the native scanning application, perform the following steps:

1. Go to **Apps > Email**.

2. Set the **Add Me** to **On** and set **Add to** to **To** or **Cc**.

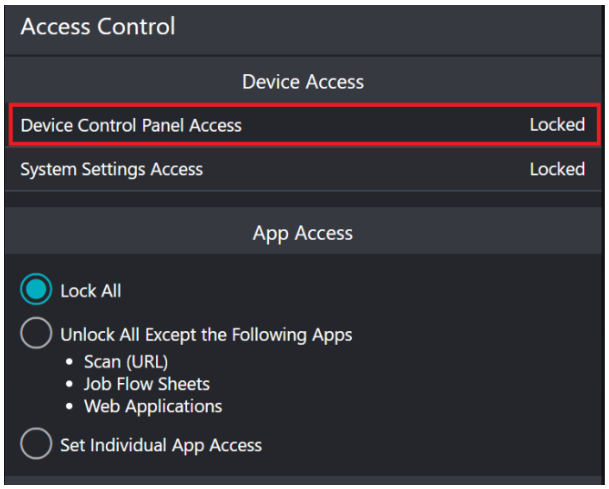


After installation of the Embedded terminal

Configure access to MFD functions

If you wish the users to authenticate to access any of the MFD functions, perform the following steps:

1. In the MFD's web interface, go to **Permissions > Permissions > Access Control**.
2. Set **Device Control Panel Access** to **Locked**.



> If you wish to define access to individual functions separately, configure the **App Access** instead of **Device Control Panel Access**.

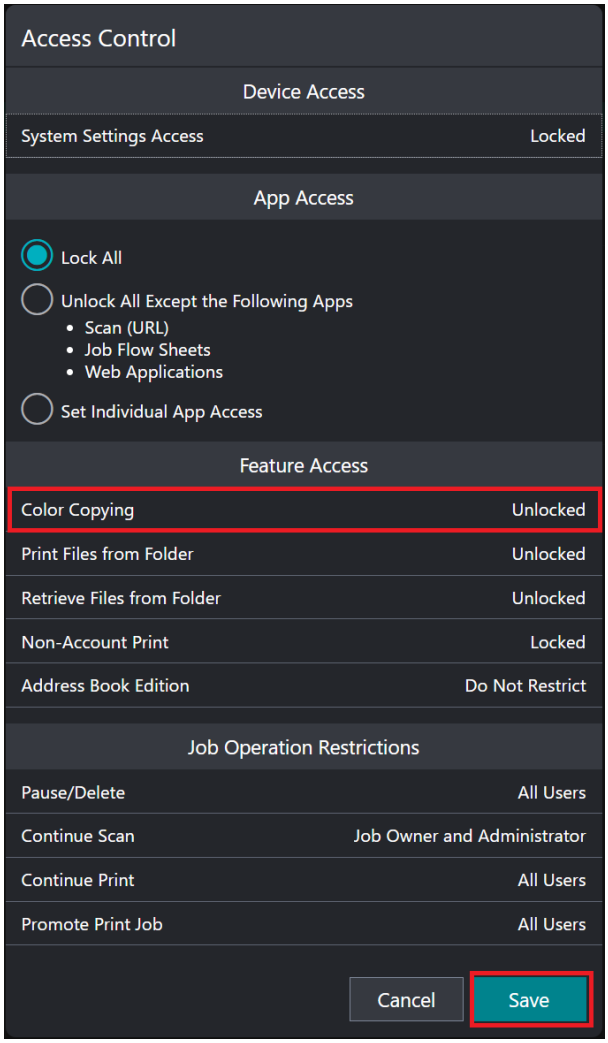
3. The Dispatcher Paragon authentication screen will become the home screen of the MFD. If you uninstall the Dispatcher Paragon Cloud Embedded Terminal from the MFD, you must set these settings to **Unlocked** in order to allow access to the MFD's functions again.

Configure color copy restriction

To restrict access to full-color copy according to Dispatcher Paragon Cloud user access right setting, perform the following steps:

1. In the MFD's web interface, go to **Permissions > Permissions > Access Control**.

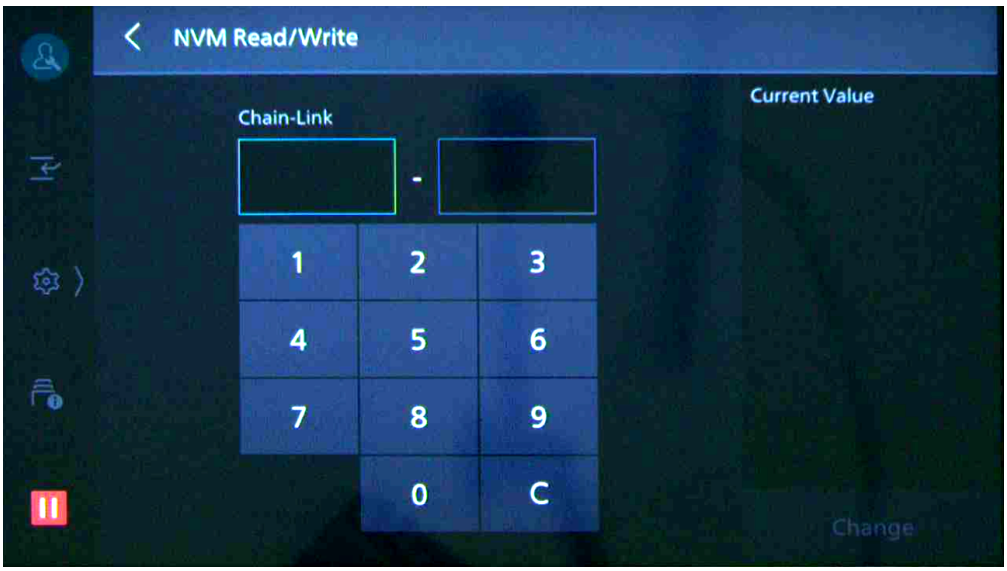
2. Set Color Copying to **Locked** and click **Save**.



Device NVM setup

The NVM setup can be done only by FUJIFILM BI Partner Engineer. It is necessary for Apeos to report accounting of print jobs to Dispatcher Paragon Cloud. If not done, Apeos will require authentication for print requests and store print jobs without authentication information in the internal storage.

Input in Chain-Link and corresponding value as **701-436=0**.



Configuring Konica Minolta MFDs

Requirements

- Correct firmware is installed on MFD (for more details see HCL – Konica Minolta)
- **MFD is OpenAPI 3.5 or higher** if embedded accounting / application shortcuts / web browser terminal functionality is required. Models that support OpenAPI 3.5 or higher may need HDD and/or additional memory installed (for more details see HCL – Konica Minolta)

At Glance

1. Configure and enable SSL
2. Enable OpenAPI on a device
3. Configure SSL for OpenAPI and TCP Socket communication
4. Disable all other authentications (User Account Track, ID & Print, key counter, Vender2 cable etc.)
5. Add domain DNS suffix in Network settings - Default DNS domain name (in case a host name for SPOC is used)
6. Configure the Windows print driver
7. Install loadable driver (if Card authentication is required)
8. Configure USB card reader settings (if authentication by CARD is required)

Configure and enable SSL

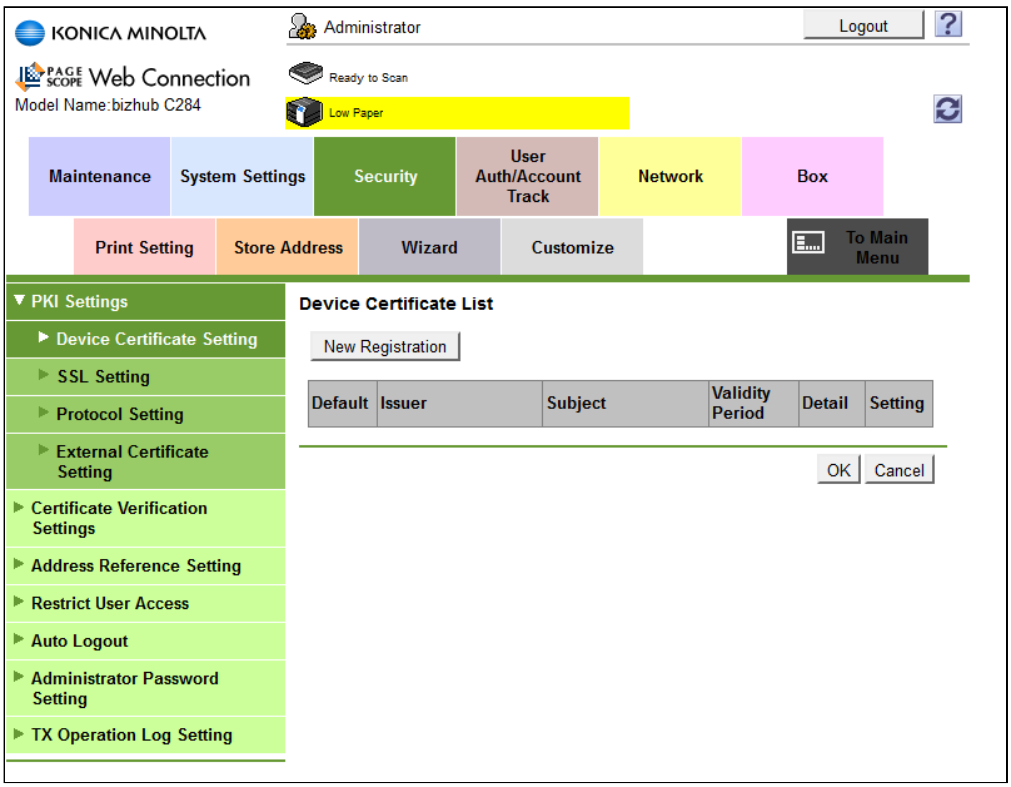
⚠ Perform these steps only if your MFD does not support Konica Minolta MarketPlace.

1. Open your Web browser and enter the MFD's IP address. The MFD Web interface,"PageScope®," opens.
2. On the PageScope Web Connection Login screen, select **Administrator**; then click **Login**. (If you are automatically logged in as a guest, log out and then log in again using the administrator account).

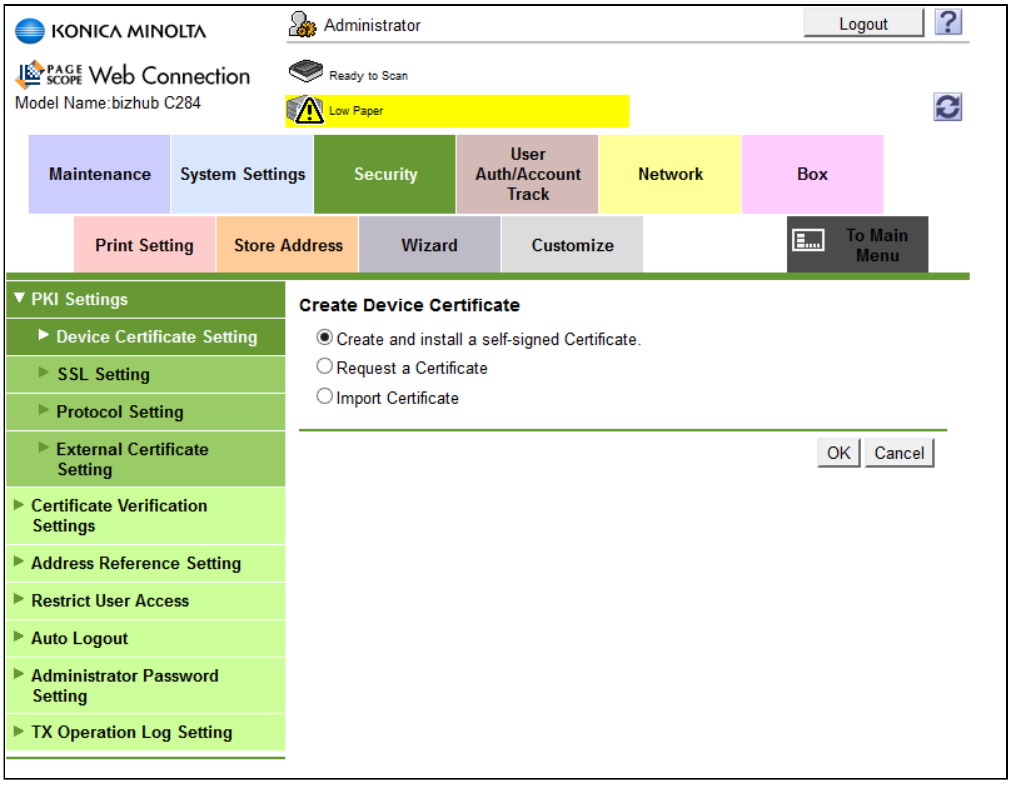
> ⚠ The Page Scope Web interface varies according to the specific MFD.

3. Enter the Administrator password for the MFD; then click **OK**.
4. Select the **Security** tab; then select **Device Certificate Setting**; Continue with selecting **New registration.**

> ⚠ If the device already has a factory default settings certificate, delete it first and then create a new one.

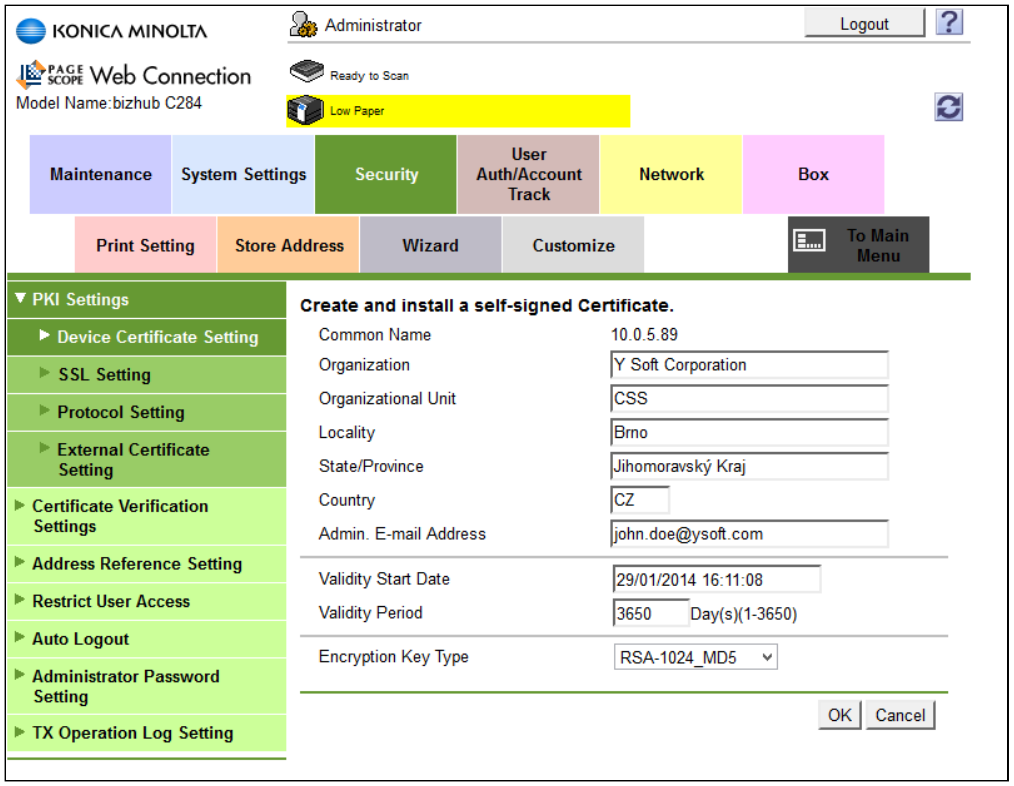


5. Select **Create and install a self-signed Certificate** and click **OK**.



6. Enter information for the SSL certificate; then click **OK**.

The information you enter does not have to be valid (for example, the **Admin E-mail Address** does not have to be valid), except the **Validity Period** , recommend is **3650** days. The **Mode using SSL/TLS** setting applies only to PageScope Web Connection; you can set it to **None** without affecting OpenAPI's SSL capabilities.



We recommend select some RSA based Encryption Key Type (e.g. RSA-2048_SHA-256).

7. When the message "Certificate has been successfully created" appears, click **OK**.
8. Log out of PageScope® Web Connection. If a message appears saying that it is necessary to reboot, reboot the MFD.

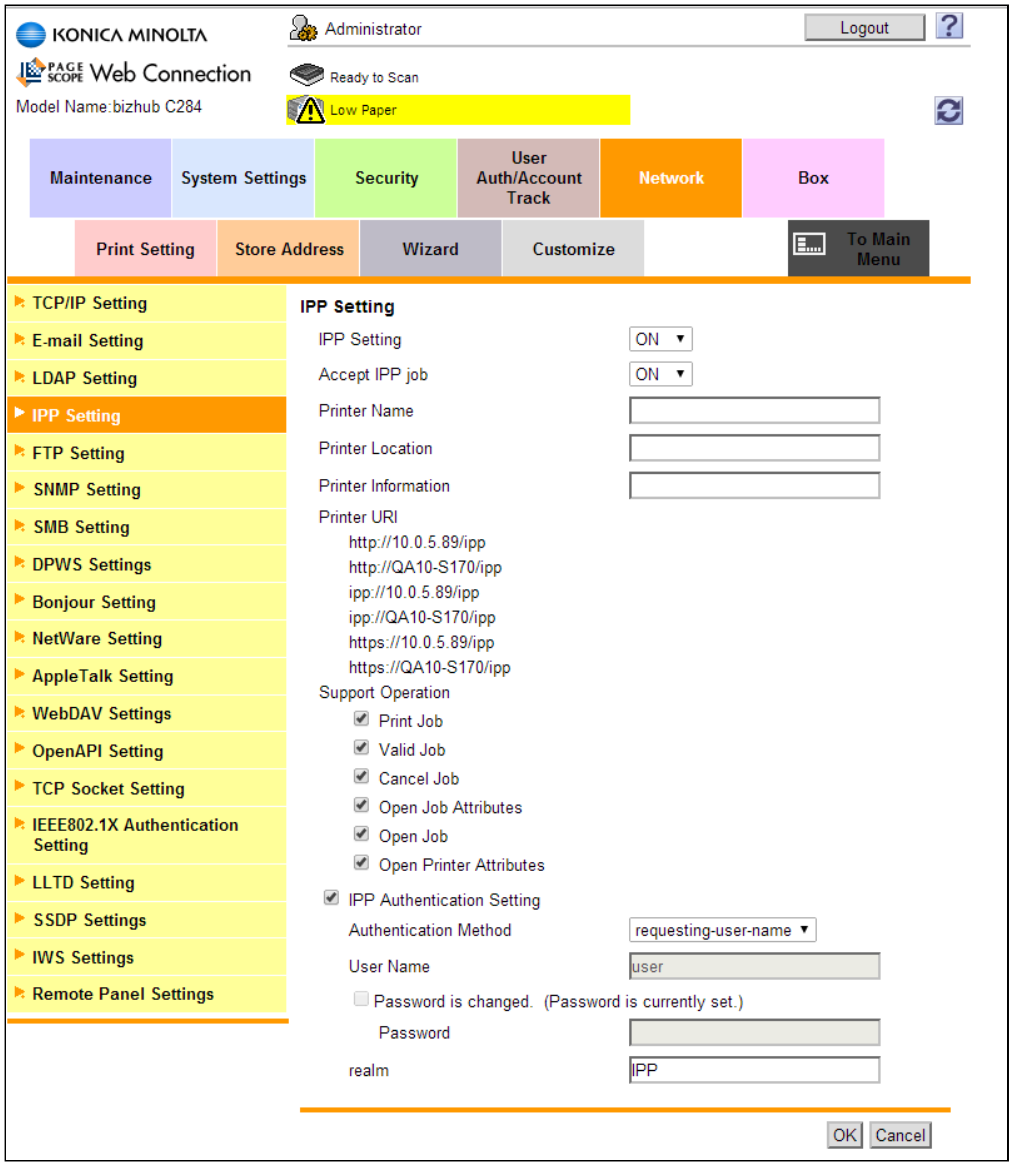
If the MFD does not request a reboot, you must log out of the Web interface before continuing the terminal installation.

Configure IPP and IPPSSL

Configuration of IPP and IPPSSL

This configuration is required for using IPP and IPPSSL.

1. Login MFD's web interface as administrator
2. Navigate to the **Network** tab
3. Continue to **IPP Setting**
4. Change the settings as shown below:



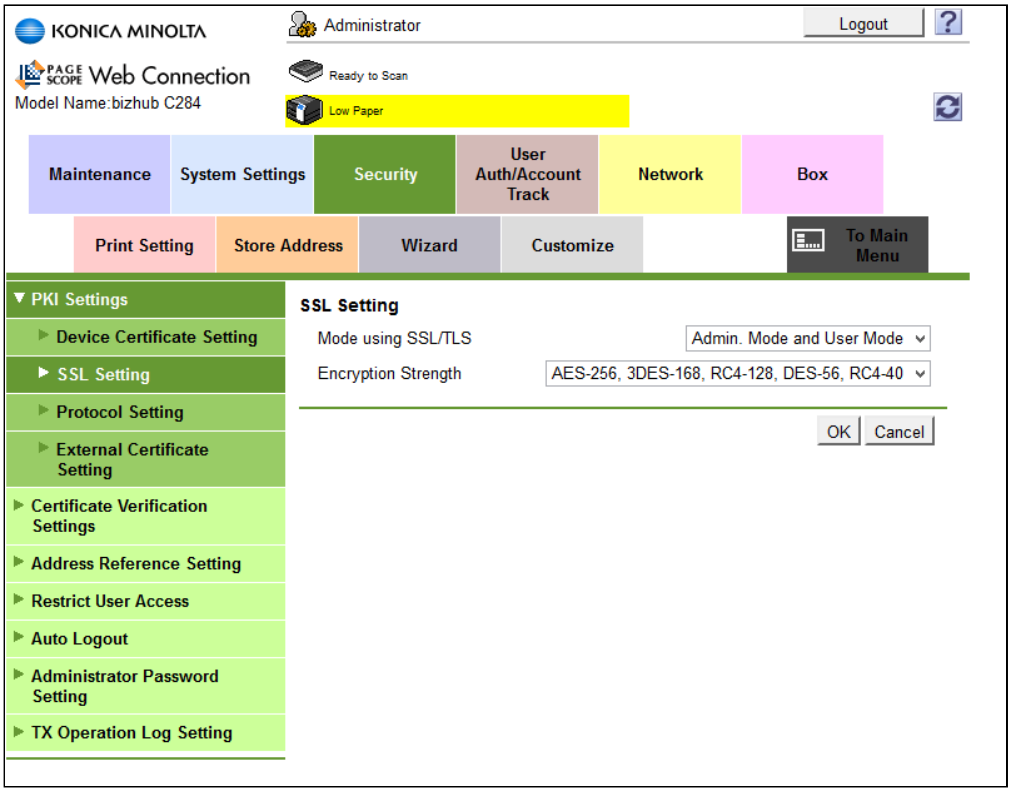
5. Enable **IPP Setting** option
6. Enable **Accept IPP job** option

Configuration of IPP over SSL

This configuration is required for using IPPSSL.

1. Navigate to the **Security** tab
2. Continue to **PKI Settings** > **Device Certificate Setting**
3. Use the **New Registration** button
4. Select the **Request a Certificate** option > **OK**
5. Insert details of your organization > **OK**
6. A message: Certificate Request was successful is displayed > **OK**
7. Copy or Save a Certificate Signing Request Data and submit them to your certification authority
8. Create a certificate with your certification authority
9. Continue on **Security** tab > **PKI Settings** > **Device Certificate Setting**
10. Select your **Requesting Certificate** and press the **Setting** button
11. Use **Install a Certificate** option > **OK**
12. Add certificate from your certification authority (the certificate you have created in step 8) > Press the **Install** button
13. A message with the result of installation will be displayed
14. Continue to **PKI Settings** > **SSL Setting**
15. Set **Mode using SSL/TLS** to **Admin. Mode and User Mode**

16. Set **Encryption Strength** to encryption which you use (if you are not sure which encryption use, set attribute to **AES-256, 3DES-168, RC4-128, DES-56, RC4-40**)



Configure SSL for OpenAPI and TCP Socket communication

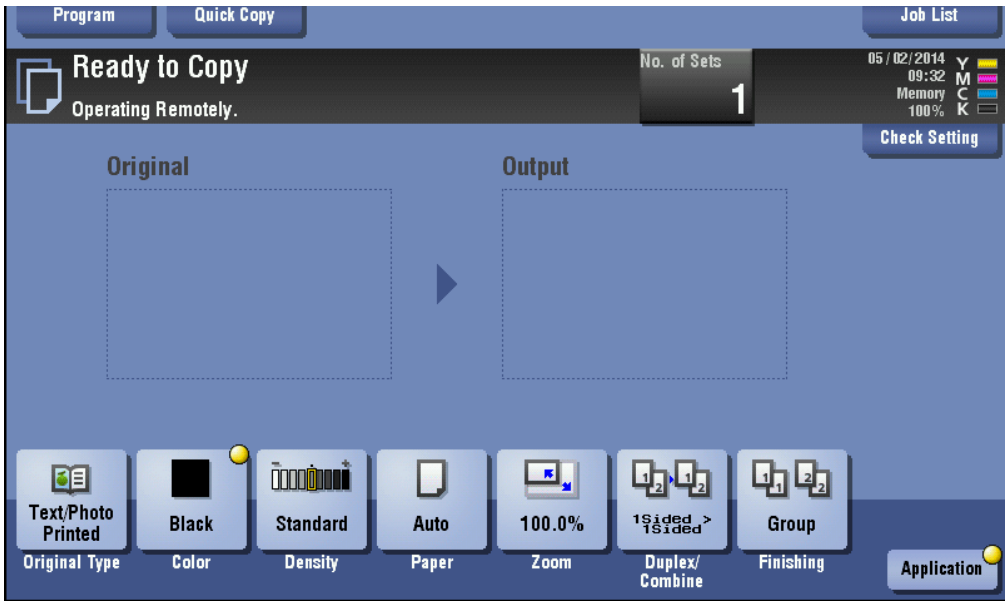
Configure additional required SSL settings as described here.

You can configure the settings by using either the MFD's Web interface or the MFD panel.

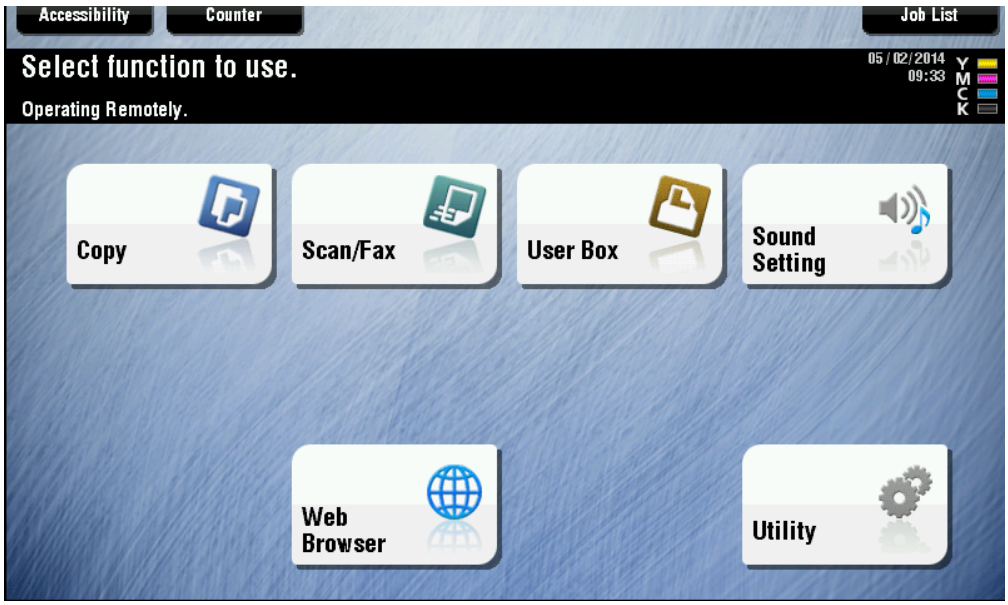
Configure SSL via MFD panel

If you did not set OpenAPI and TCP Socket settings via the MFD's Web interface, use the MFD's panel to set them as follows:

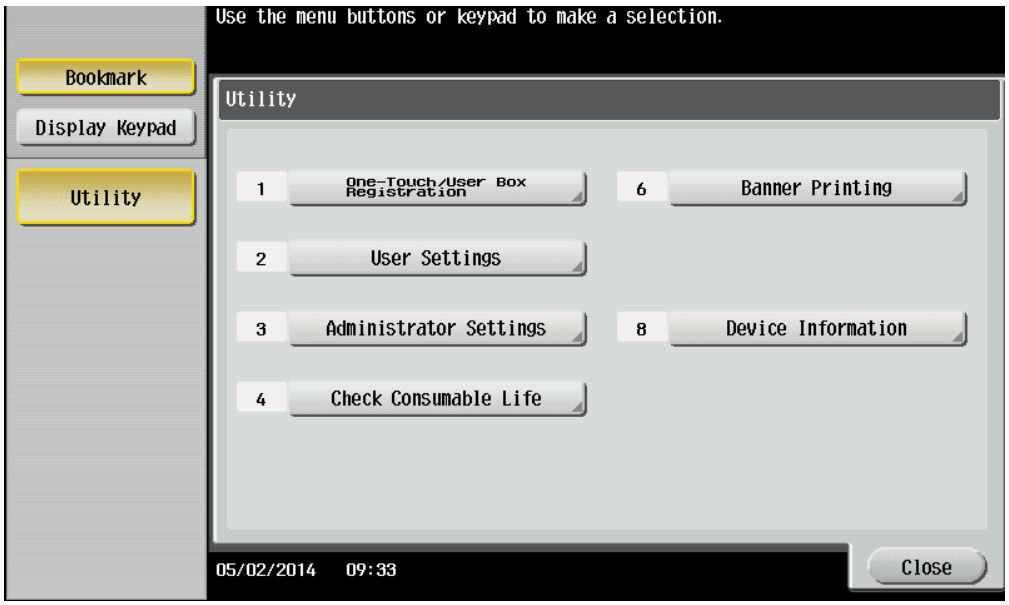
1. Make sure the MFD is idle — not copying, printing, scanning, or otherwise busy.



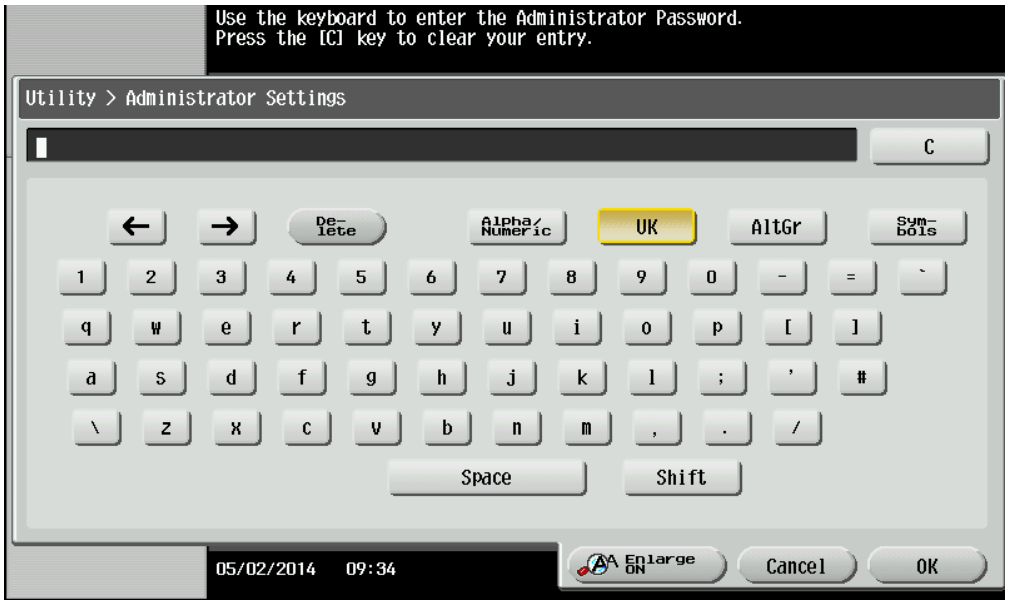
2. Open the **Utility** menu.



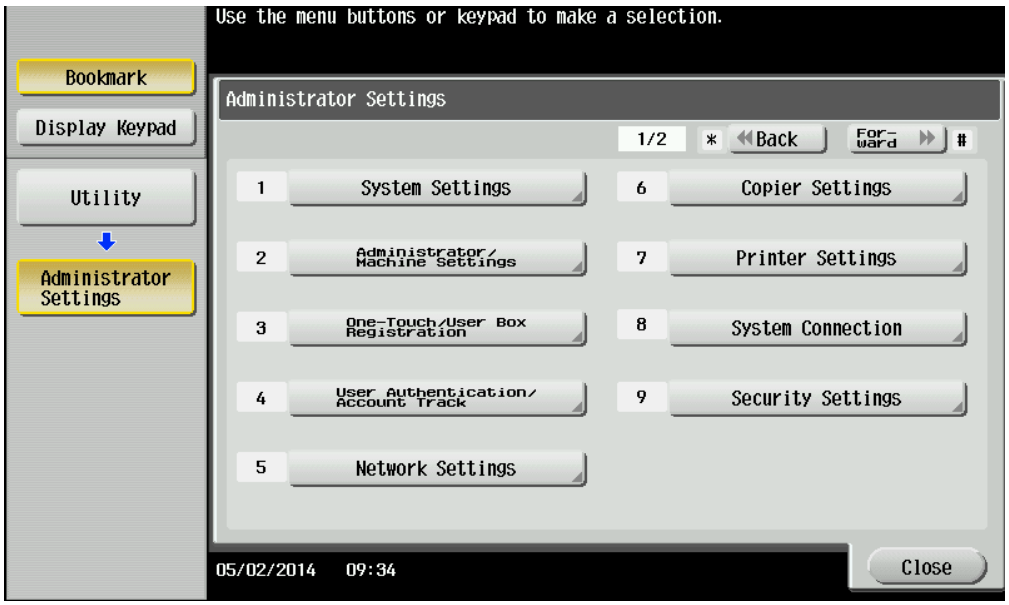
3. Tap **Administrator Settings**.



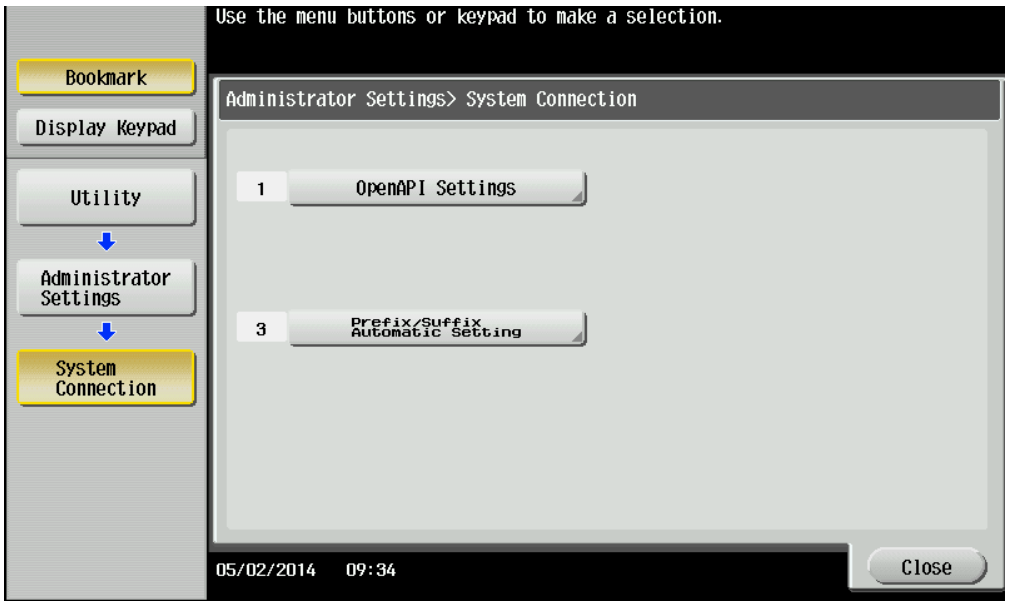
4. Enter the Administrator password for the MFD; then tap **OK**.



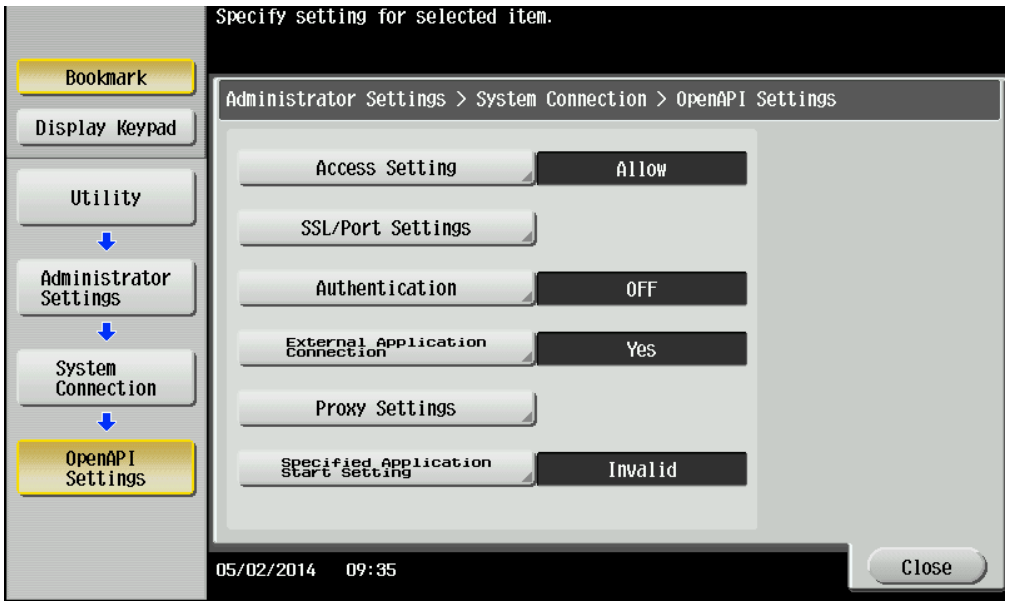
5. Tap **SystemConnection**.



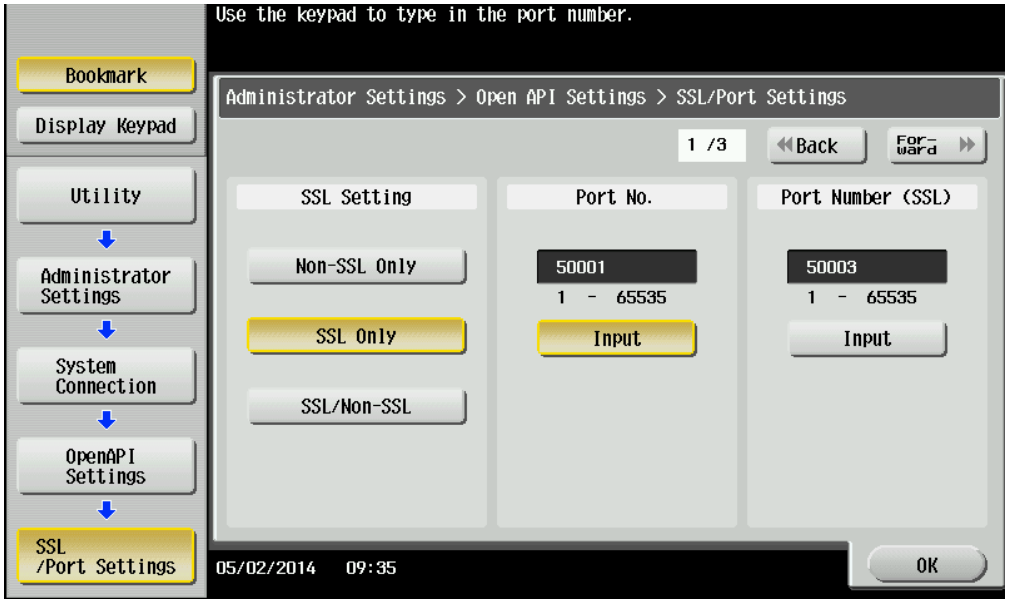
6. Tap **OpenAPI Settings**.



7. Tap **SSL/Port Settings**.



8. Select settings as shown below; then tap **OK**.



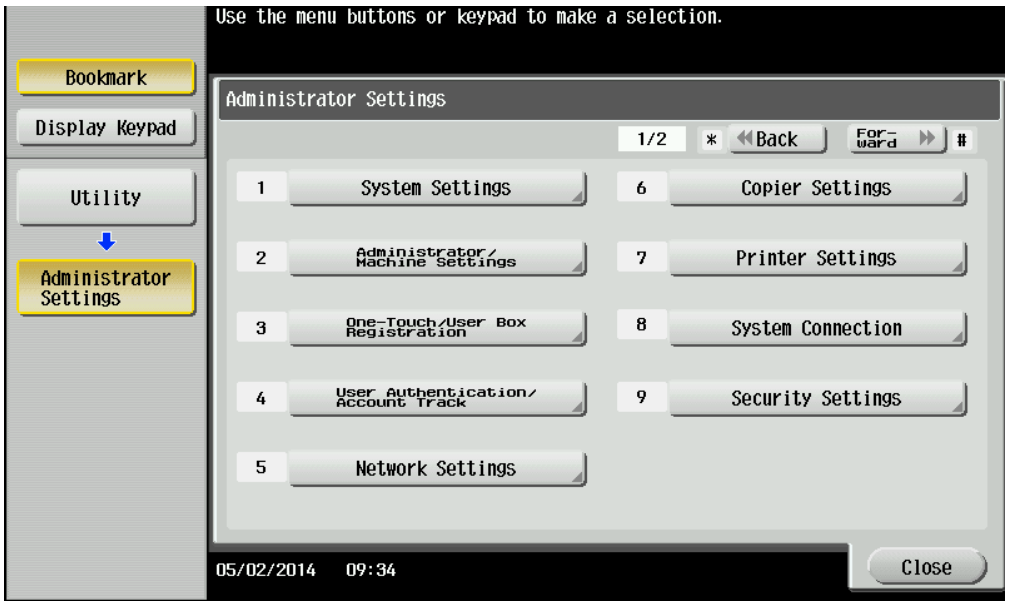
SSL Setting – SSL Only

Port No. – 50001

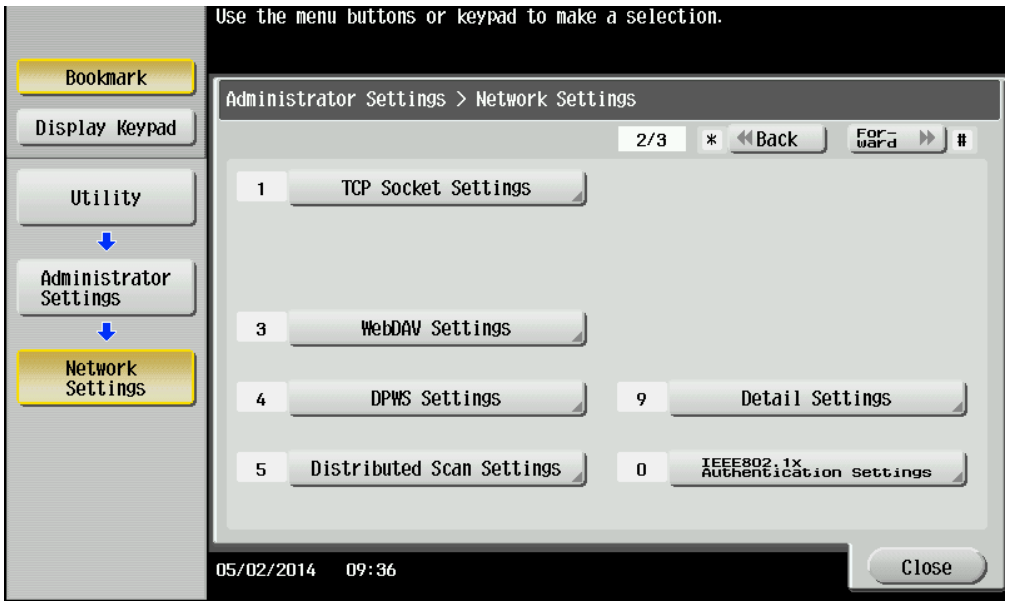
Port Number (SSL) – 50003

9. Return to Administrator Settings as follows: Tap **Close** twice or select **Administrator Settings** from the menu on the left.

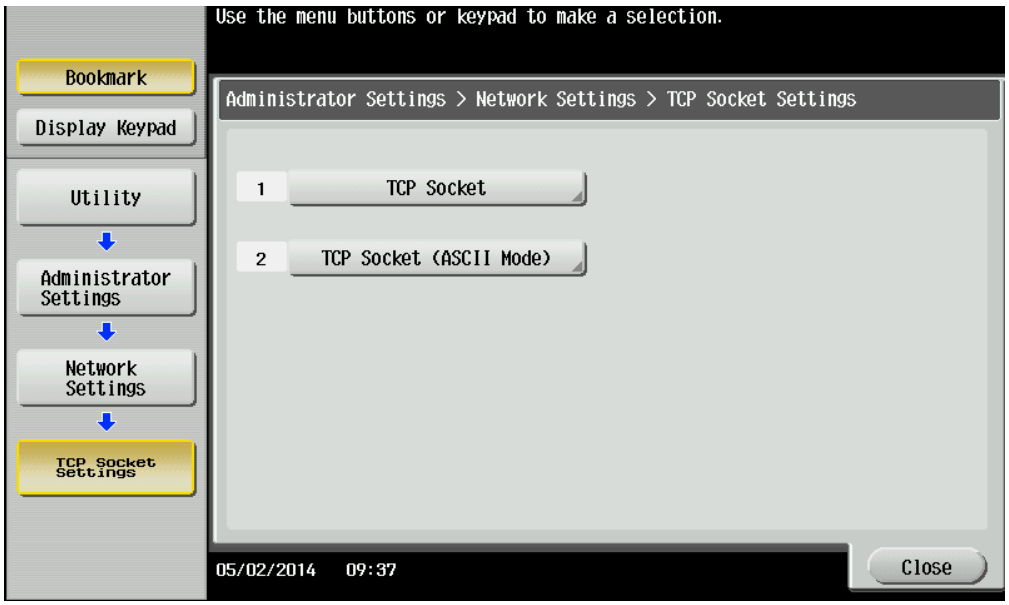
10. Tap **Network Settings**.



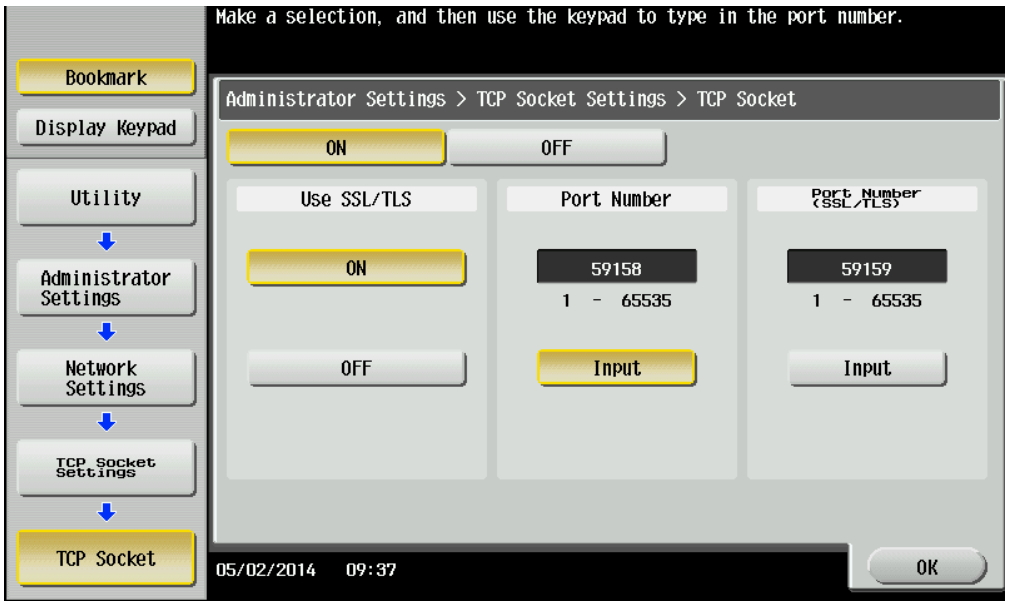
11. Tap **TCP Socket Settings** (on second page of the Network Settings menu).



12. Tap **TCP Socket**.



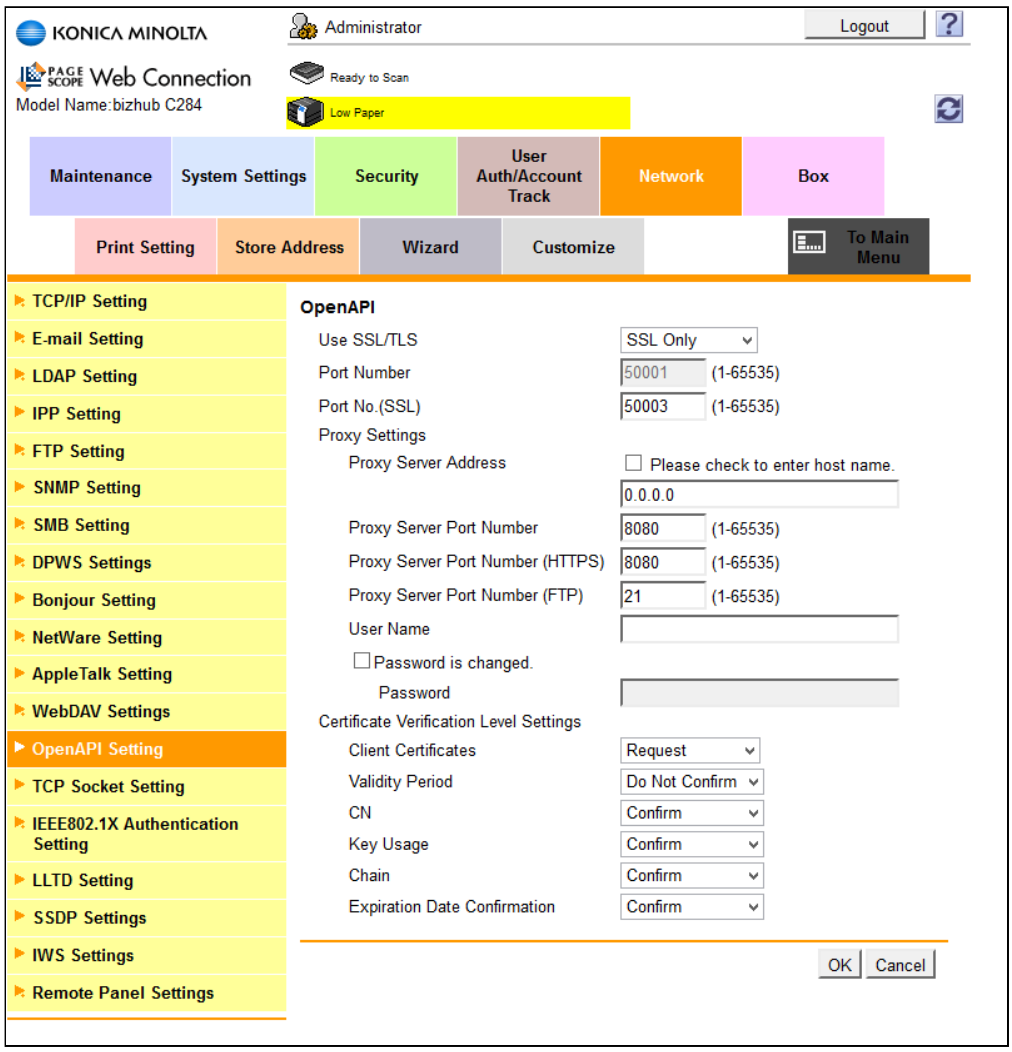
13. Change the settings for Use **SSL/TLS** to **ON**; then tap **OK**.



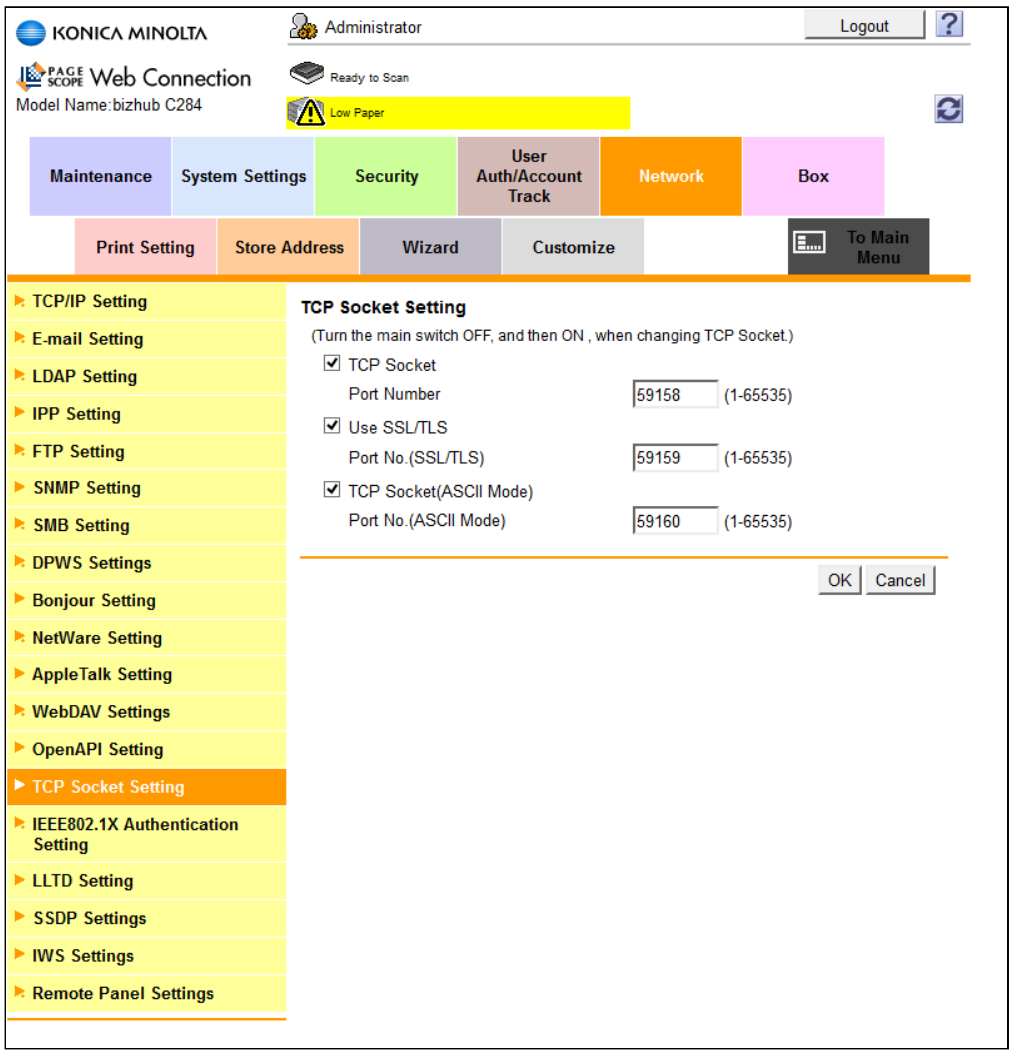
Configure SSL via MFD Web

The following settings can also be done on the MFD panel. This might be necessary if OpenAPI was disabled manually (for example if Terminal Professional was used before on the MFD).
See the Configure SSL via MFD panel article for details on the manual procedure.

1. Log In the MFD's Web interface as administrator.
2. Select the **Network** tab, then select **OpenAPI Setting** and choose the **SSL Only** option; Then Click **OK**.



3. With the **Network** tab still selected, from the menu, select **TCP Socket Setting** and check the **Use SSL/TLS** check box. Then Click **OK**.



4. Turn the main switch OFF and then ON again to apply changes to TCP Socket settings.

For remote reset use the web interface of the MFD, menu **Maintenance** > **Reset** > **Reset**.

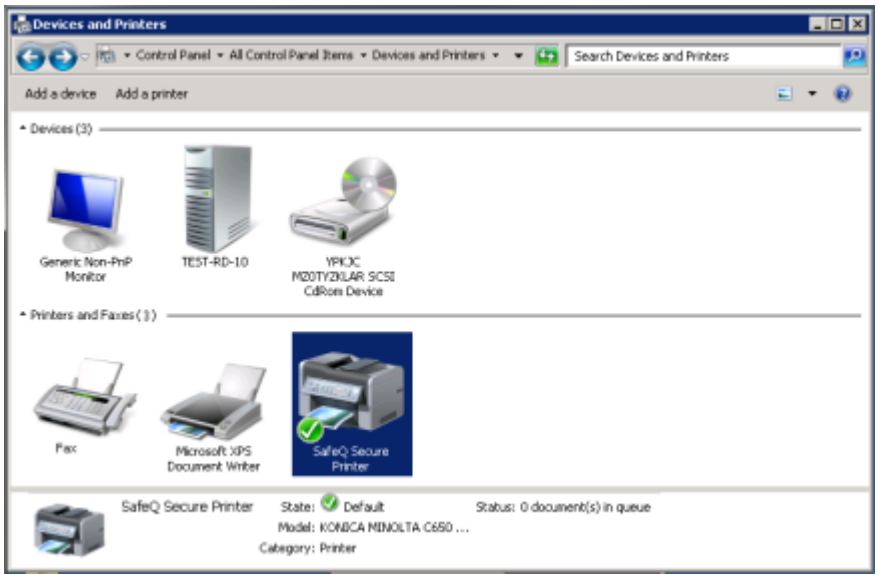
Configure USB card reader settings

Follow these steps to implement authentication via USB card reader. If a card reader will not be used, skip these steps.

> ⚠ A Konica Minolta field service engineer should configure "**Authentication Device2 > Card**" and "**ID Card Type > Card**" on the MFP

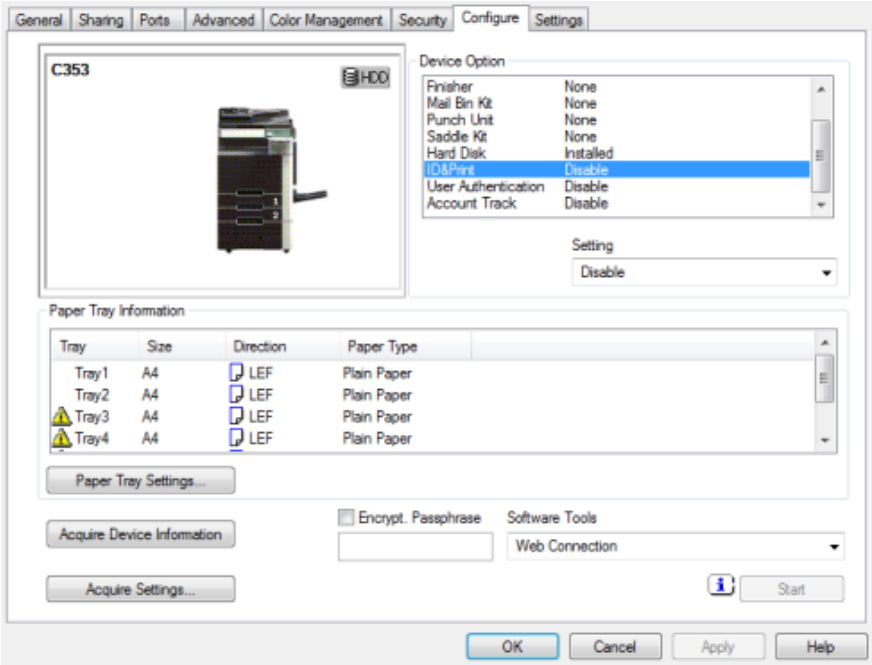
Configure User Authentication and Account Track

1. Right-click the Konica Minolta MFD driver; then select **Printer properties** > **Configure**.

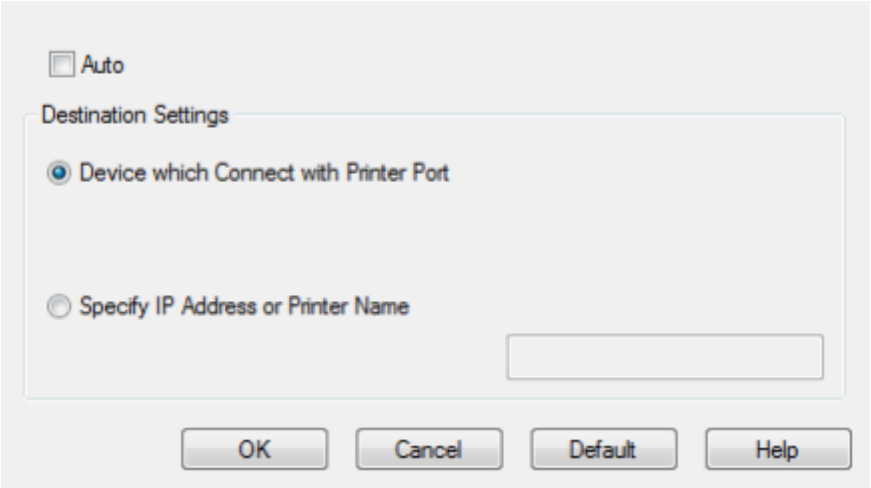


2. On the **Configure** tab, click **Acquire Settings** or **Obtain settings**.

> ⚠ Depends on your printers driver.



3. Uncheck **Auto** checkbox.
4. Click **OK**.

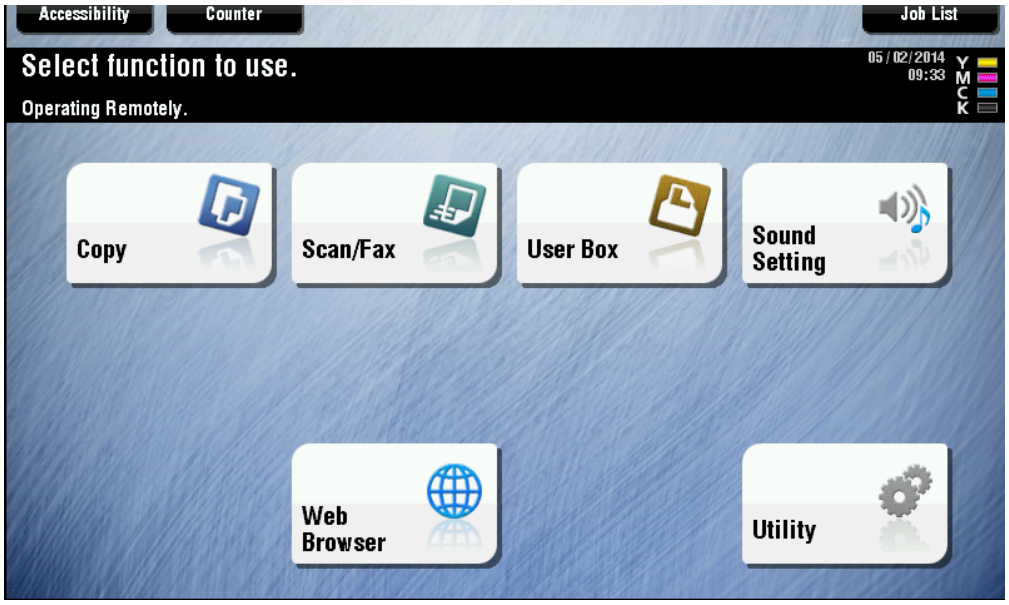


5. Back on the Configure tab, set **ID&Print, User Authentication** and **Account Track** to **disable**.
6. Click **OK**.

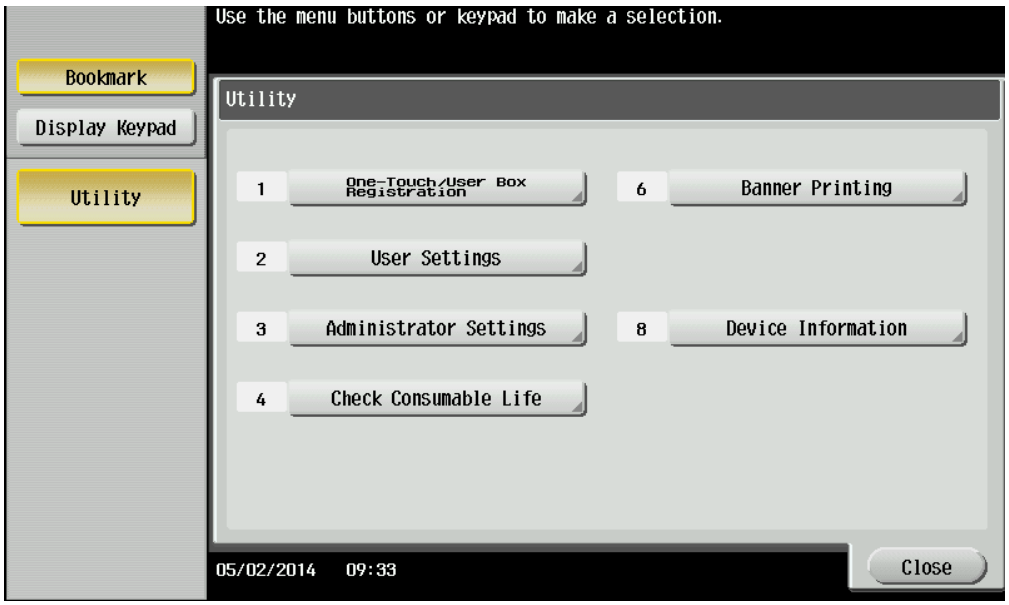
Disable the ID and print option on the MFD

At the MFD, disable the **ID & Print** option as follows:

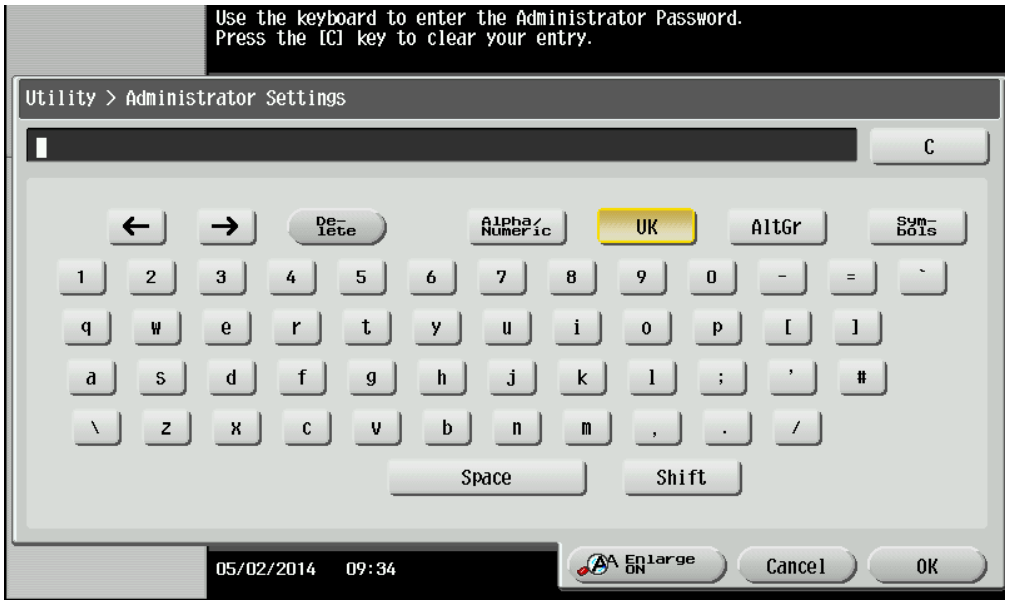
1. Open the **Utility** menu.



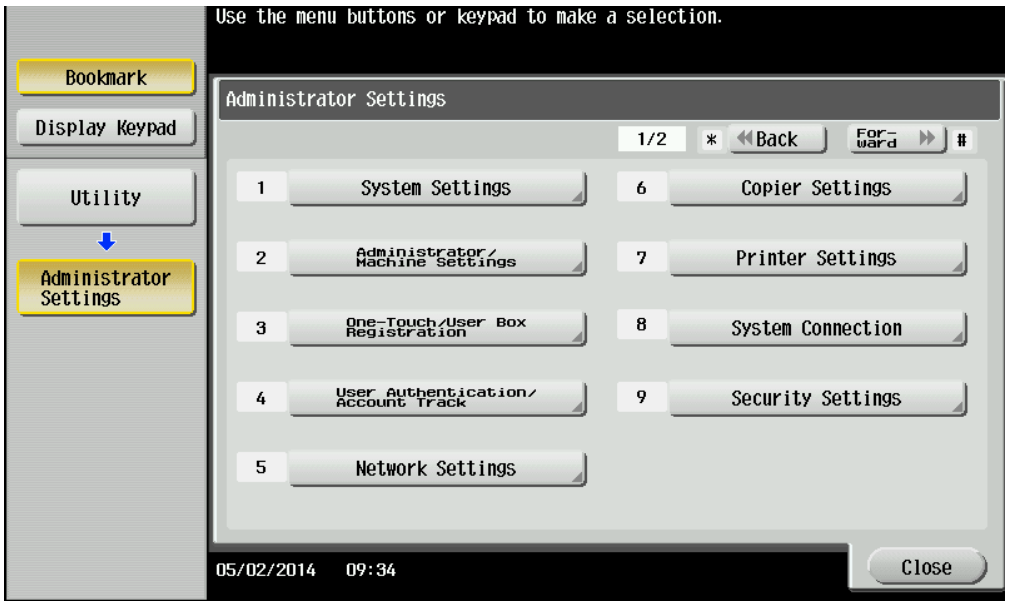
2. Tap **Administrator Settings**.



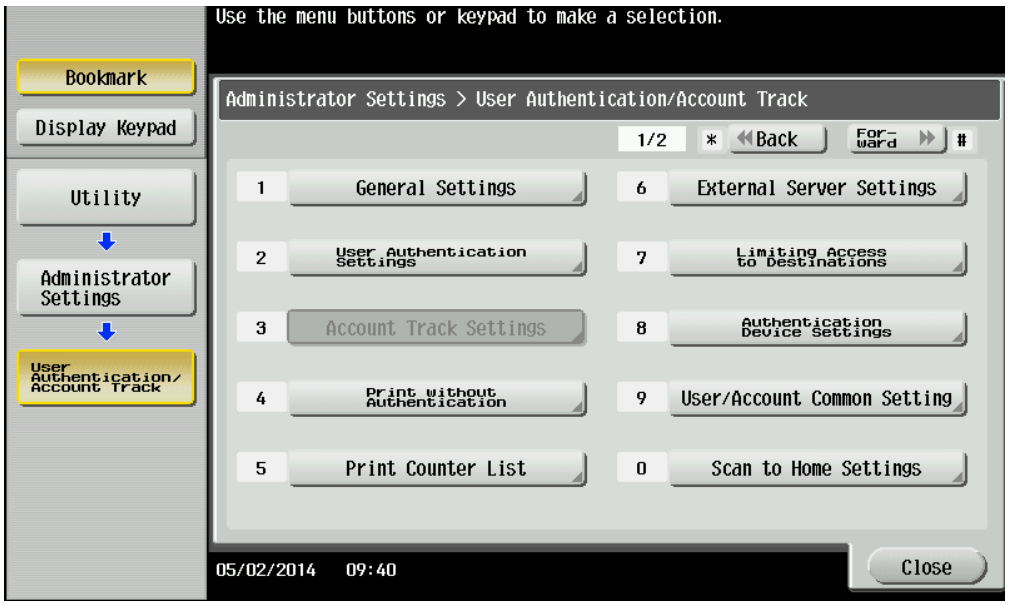
3. Enter the Administrator password for the MFD; then tap **OK**.



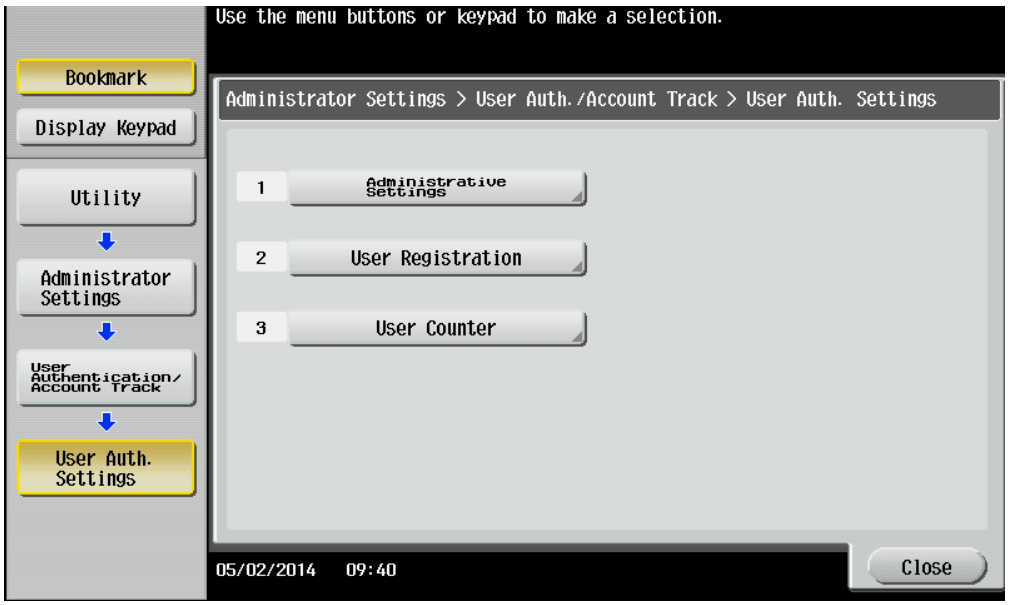
4. Tap **User Authentication/Account Track**.



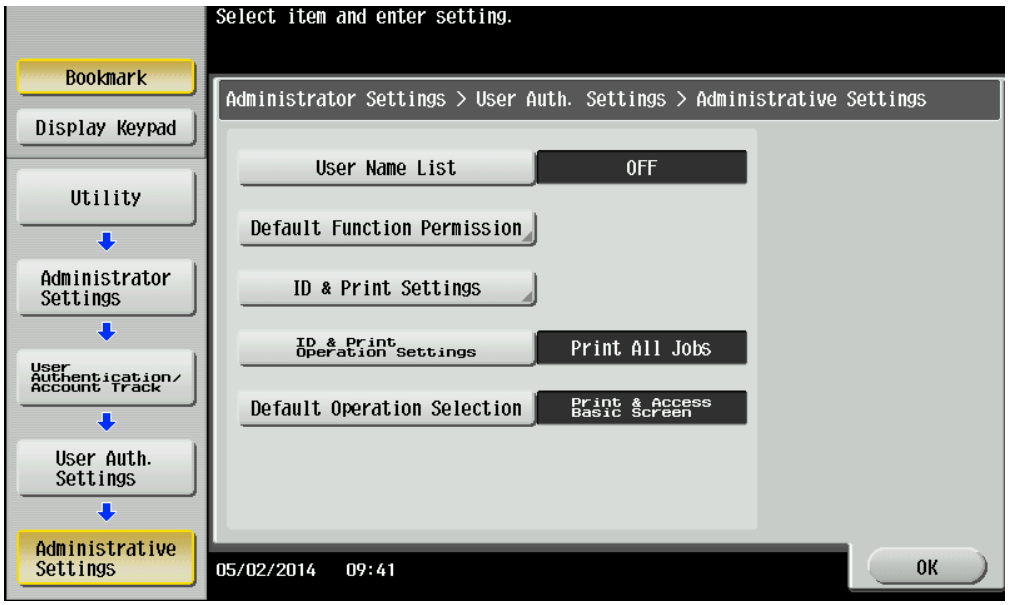
5. Tap option **User Authentication Settings**.



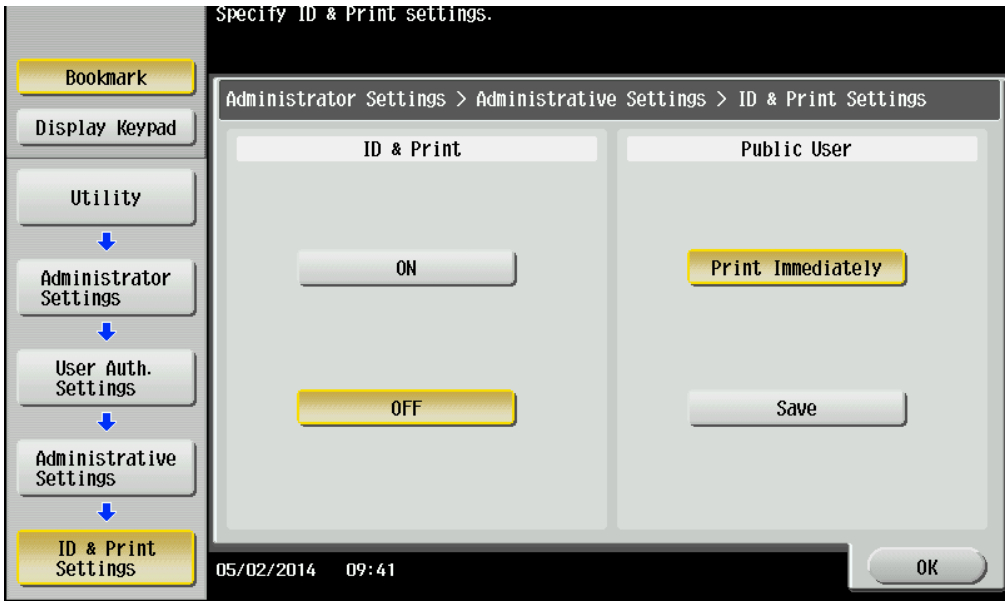
6. Tap **Administrative Settings**.



7. Tap **ID & Print Settings**.



8. Select options as shown below; then tap **OK**.



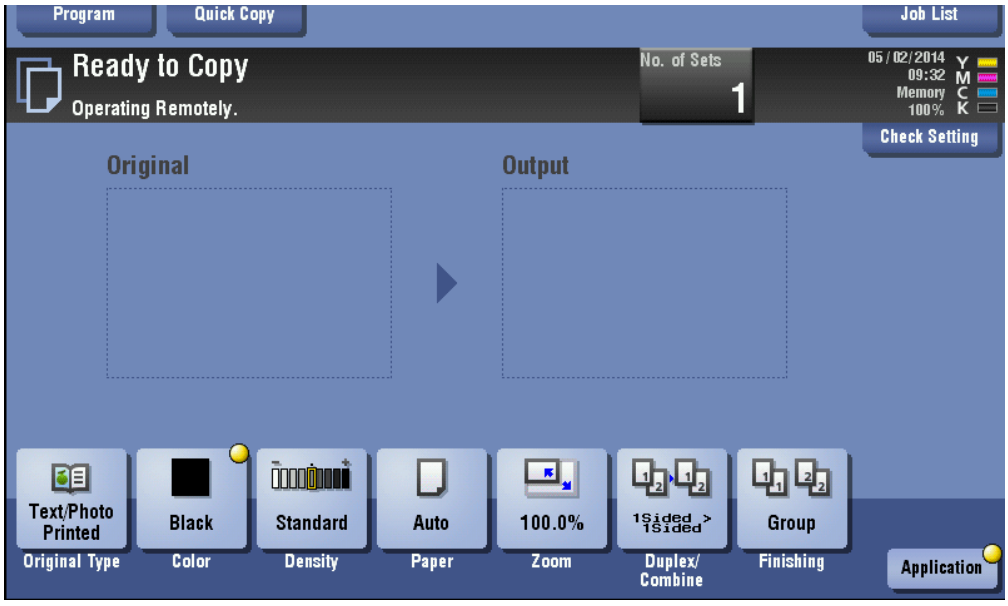
ID & Print – OFF

Public User – Print Immediately.

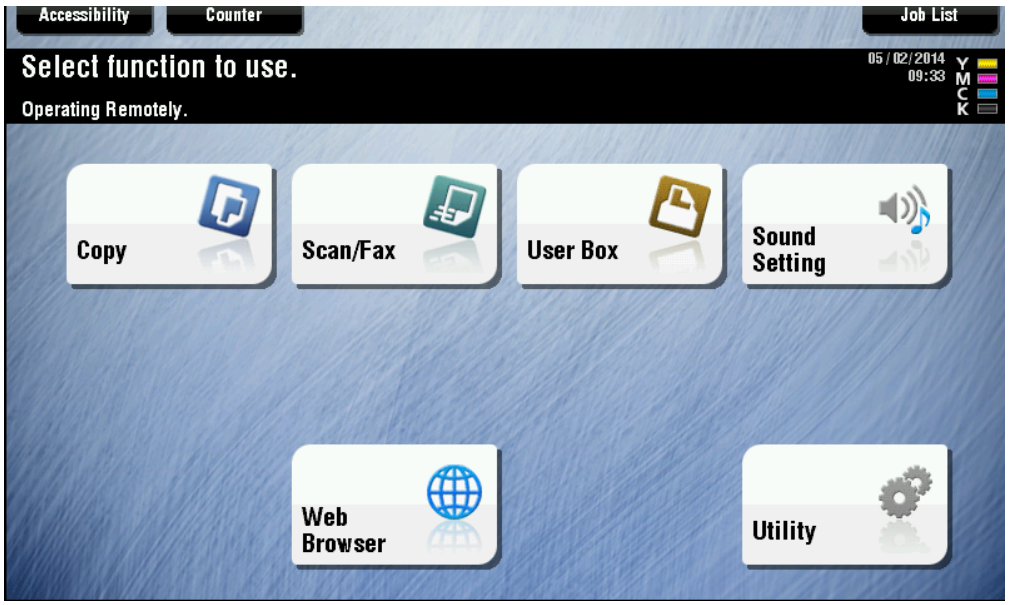
Enable OpenAPI on a device

Enable OpenAPI function at the MFD panel as follows:

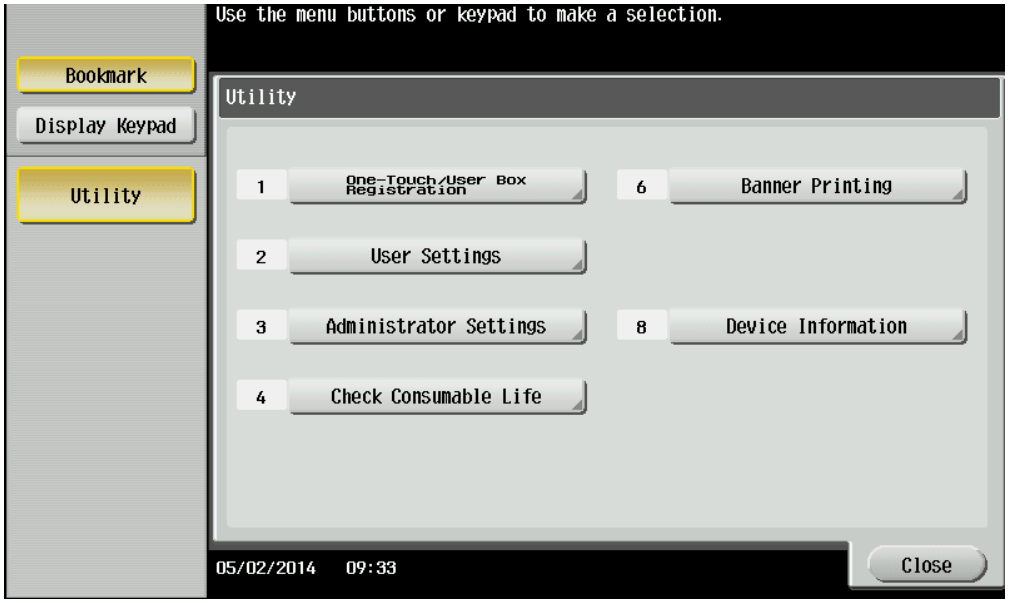
1. Make sure the MFD is idle — not copying, printing, scanning, or otherwise busy.



2. Open the **Utility** menu.

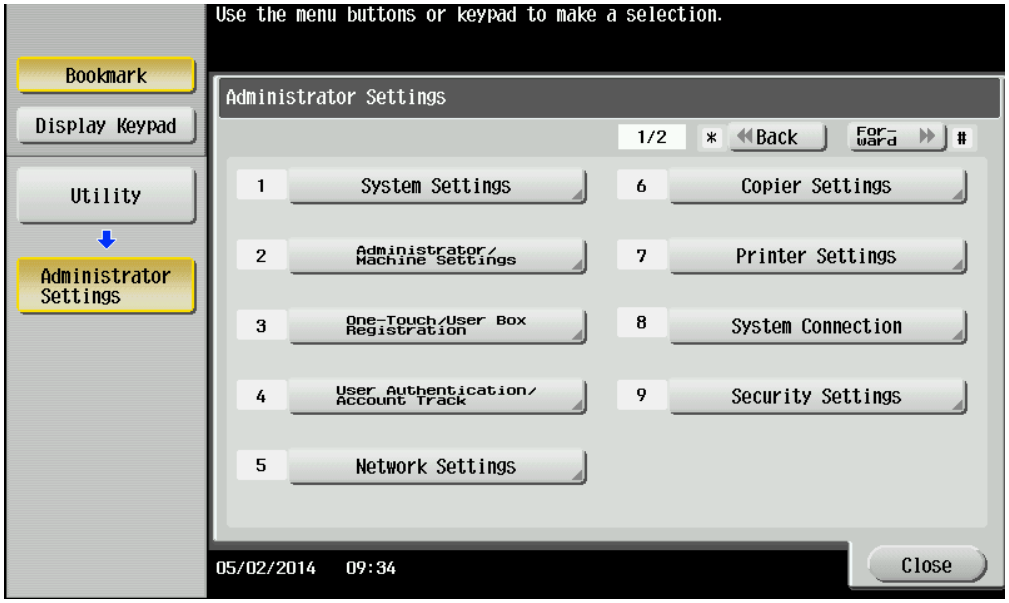


3. Tap **Administrator Settings**.

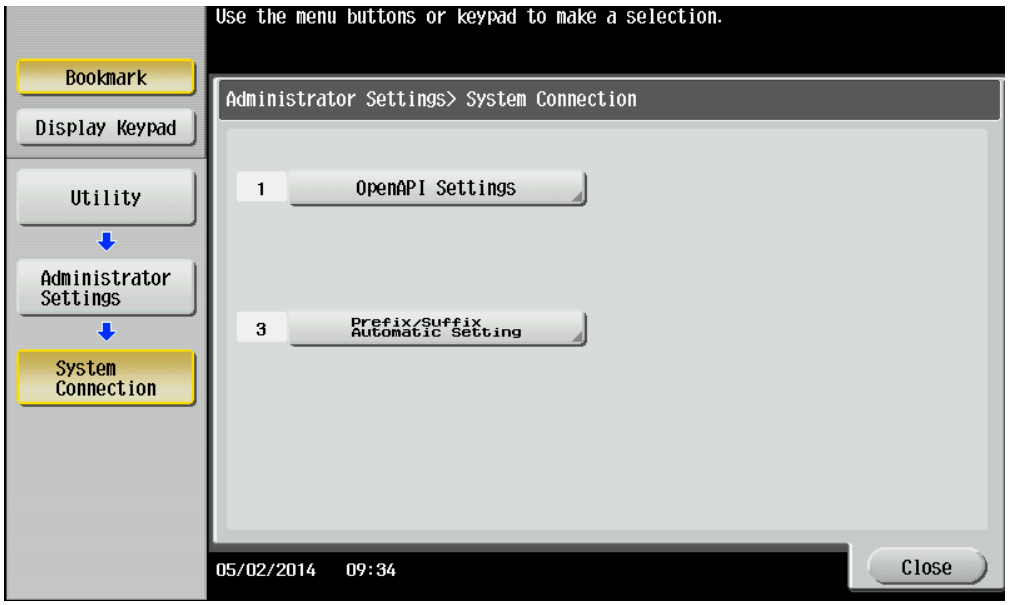


4. Enter the Administrator password for the MFD; then tap **OK**.

5. Tap **System Connection**.

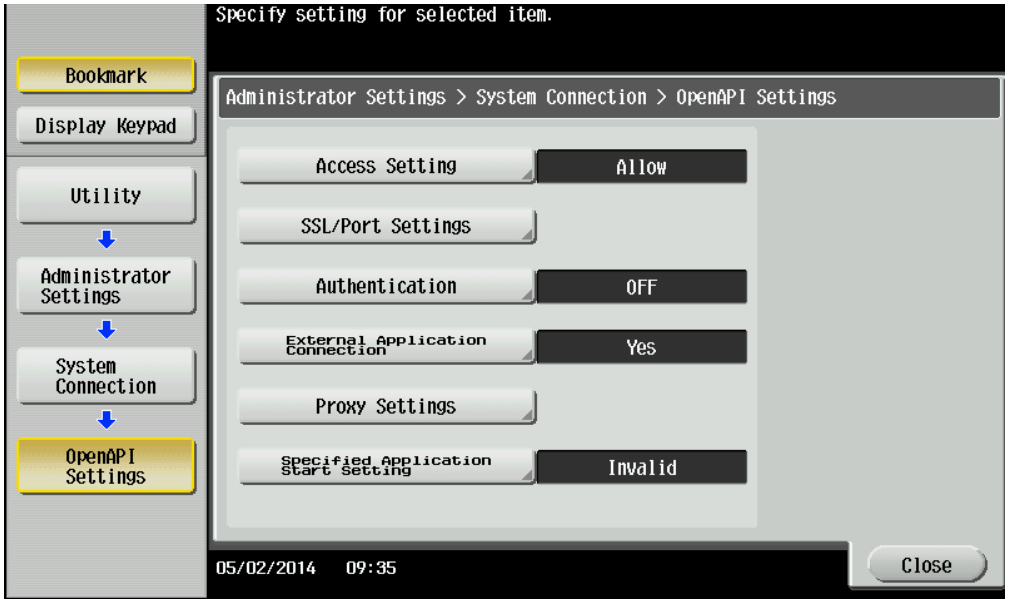


6. Tap option **OpenAPI Settings**.



If SSL and port number options appear, continue to chapter Configure SSL via MFD panel.

7. Tap **Access Setting**; then set it to **Allow**.



Install/uninstall loadable driver

This operation should be done by an authorized Konica Minolta field service engineer.

Configure Print without authentication option

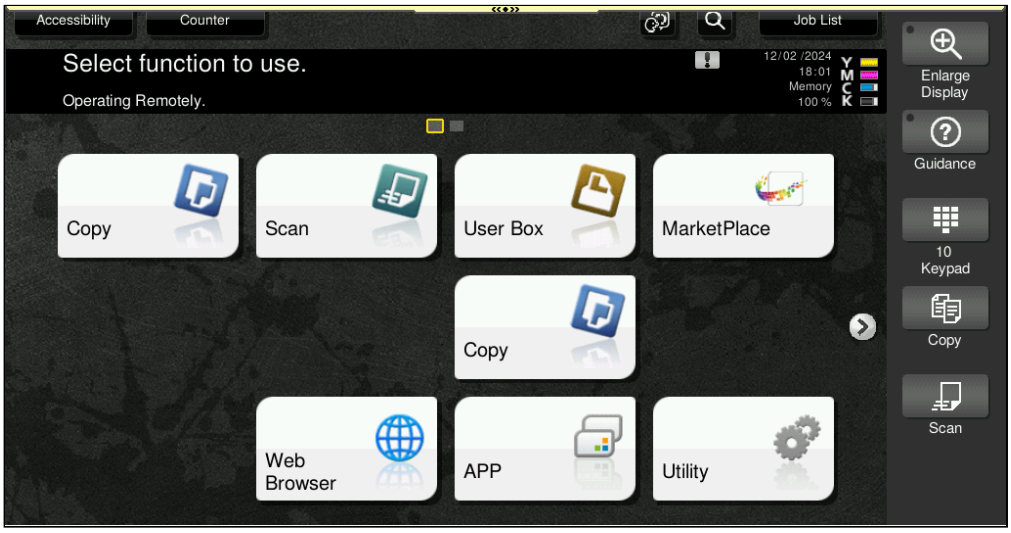
Print without authentication option allows printing of documents, that are sent directly to the MFD's IP address.

This function needs to be allowed for the Public users to be able to print.

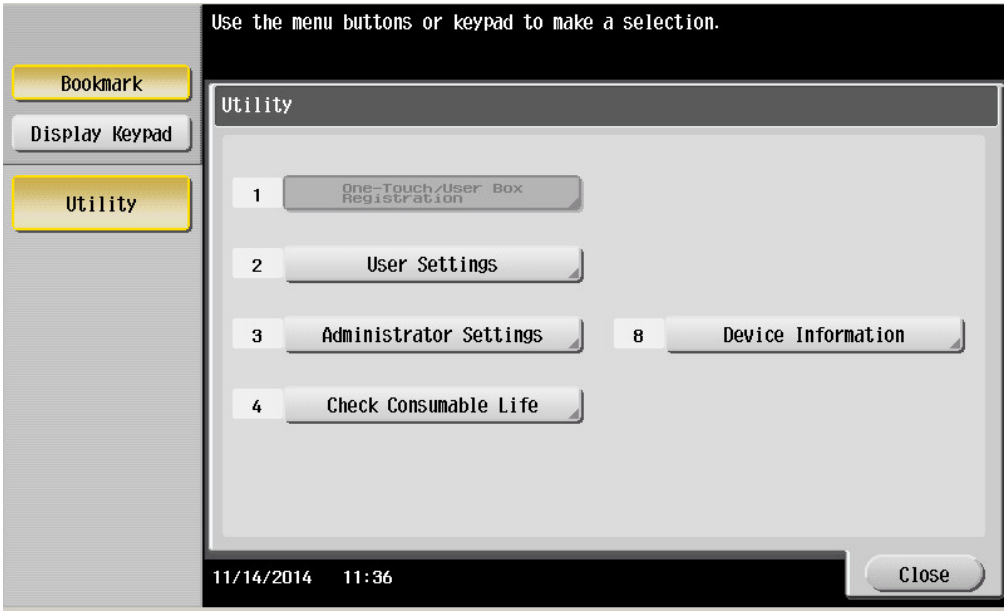
Terminal Embedded reinstallation resets the configuration back to **restricted**.

Follow these steps to set the MFD's **Print without authentication** option:

1. Tap the hardware **Home** button on MFD.
2. Tap **Utility**.

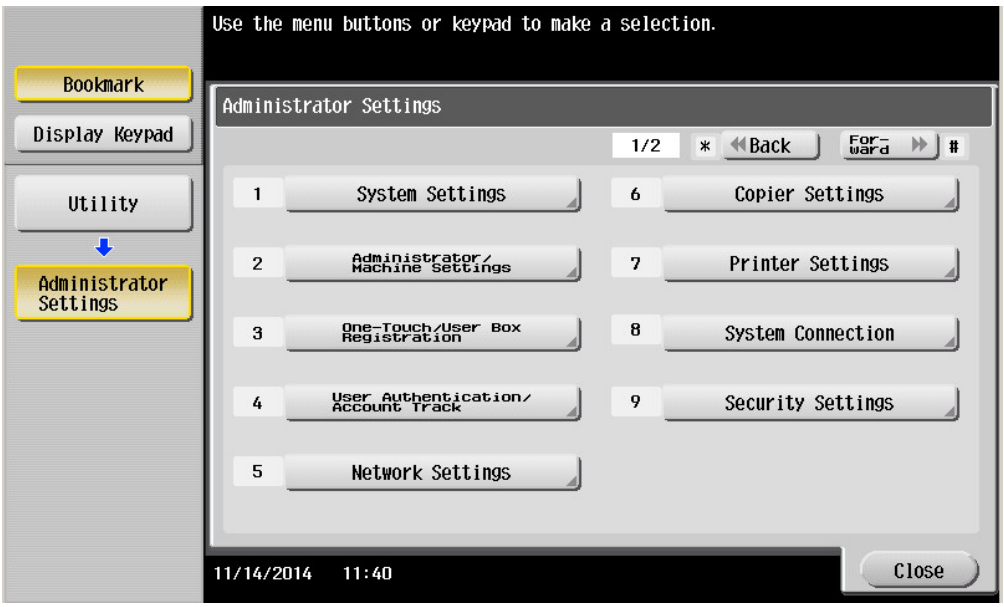


3. Tap option 3 - **Administrator Settings**.

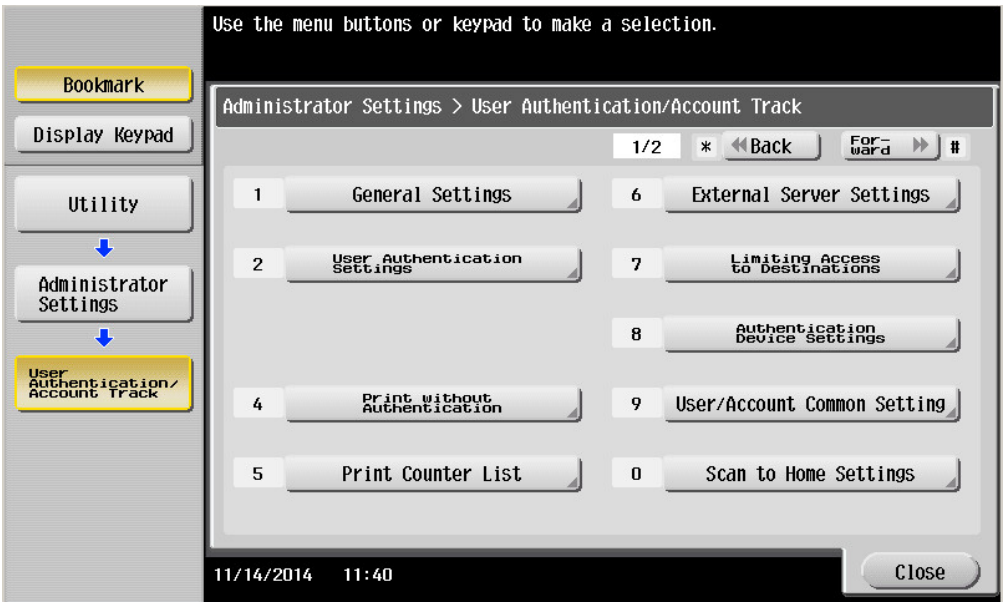


4. Enter the Administrator password for the MFD; then tap **OK**.

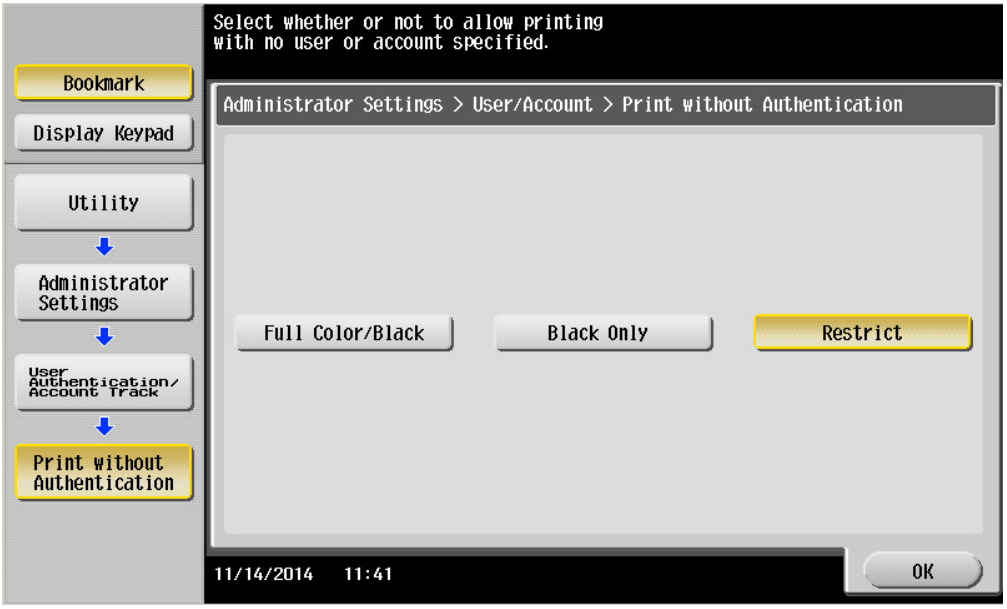
5. Tap option 4 - **User Authentication/Account Track**.



6. Tap option 4 - **Print without Authentication**.



7. Set this option to **Full Color/Black** or **Black Only** to enable printing of the documents sent directly to the MFD's IP address. To disable the printing, set the option to **Restrict**. Tap **OK** to confirm the setting.



Be sure to have your print driver configured correctly according to Configure User Authentication and Account Track.

Configure inactivity timeout

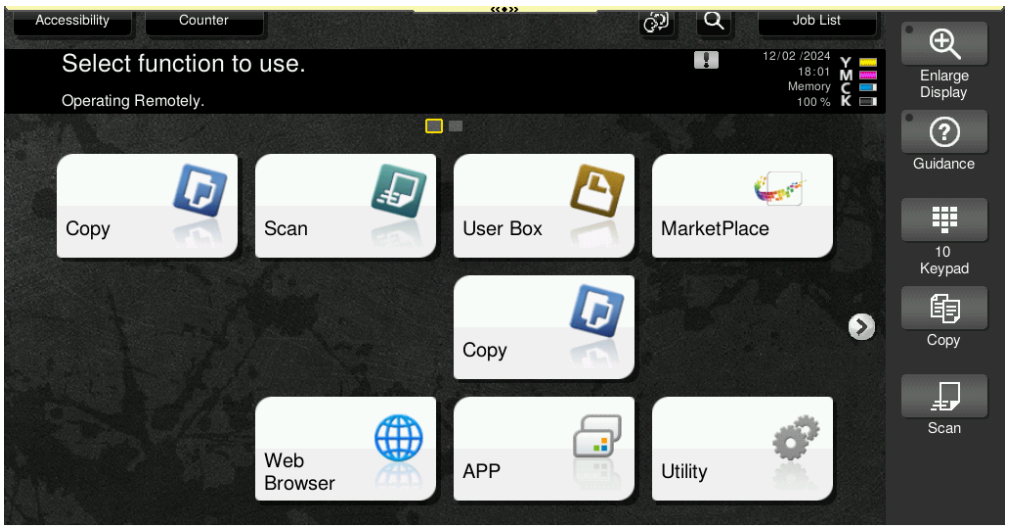
The timeout is set directly on the machine.

DIspatcher Paragon Embedded Terminal for Konica Minolta – 2nd Gen supports also the terminal inactivity timeout setting in the user's additional configuration. The priorities between MFD and Dispatcher Paragon timeouts are as follows:

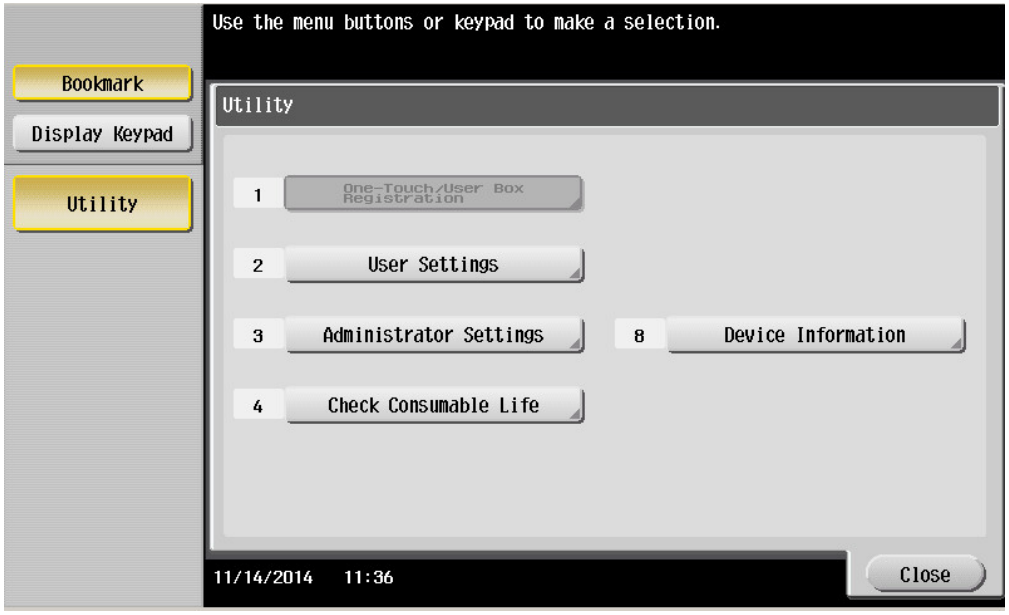
- Dispatcher Print - both timeouts are applied
- Dispatcher Scan - only Dispatcher Paragon timeout is applied
- other screens (i.e. native Copy) - only device timeout is applied

Follow these steps to set the terminal inactivity timeout:

1. Press the hardware **Home** button on the MFD.
2. Tap **Utility**.

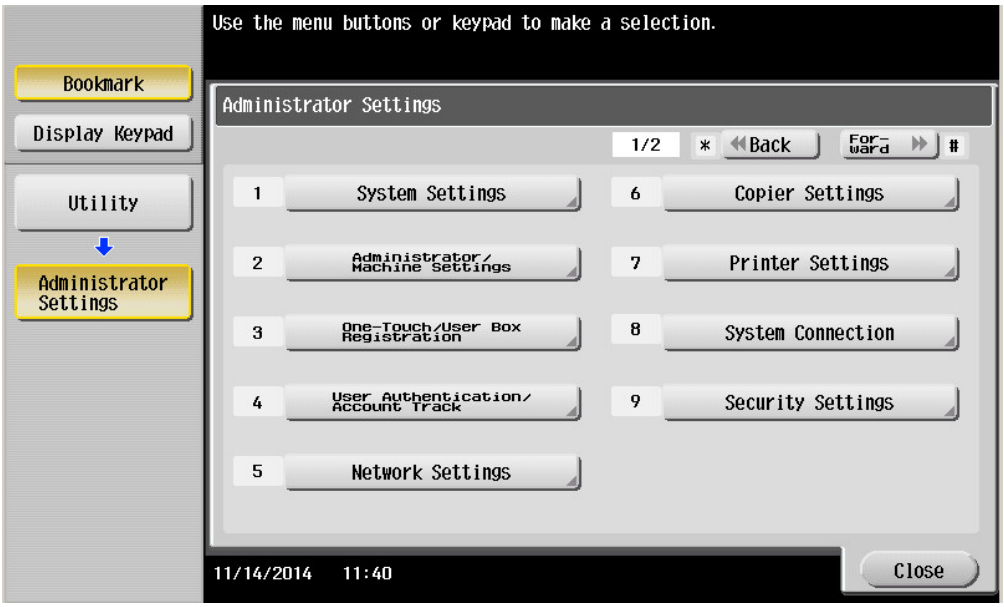


3. Tap **Administrator Settings**.

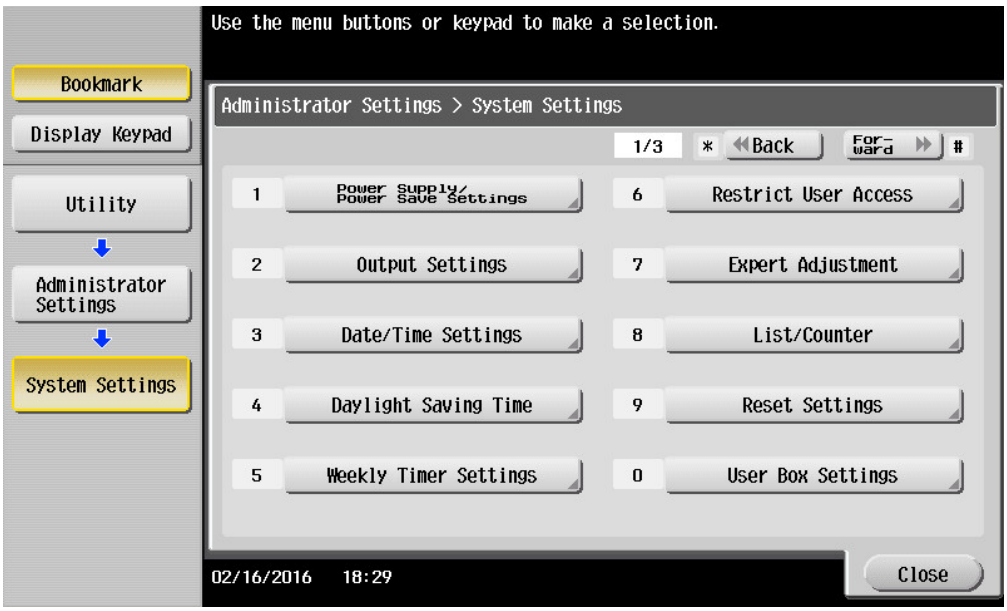


4. Enter the Administrator password for the MFD, and then tap **OK**.

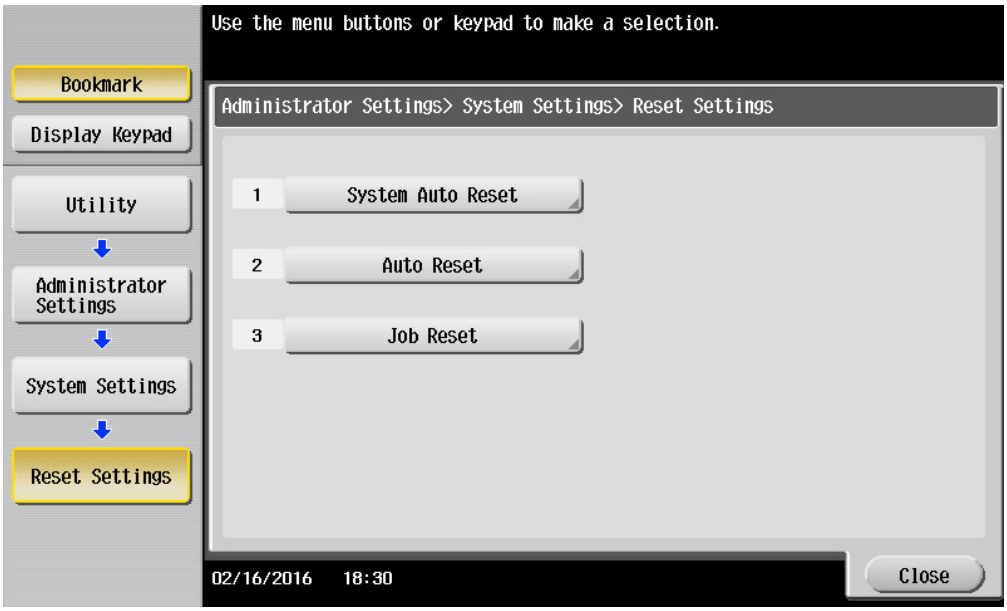
5. Tap **System Settings**.



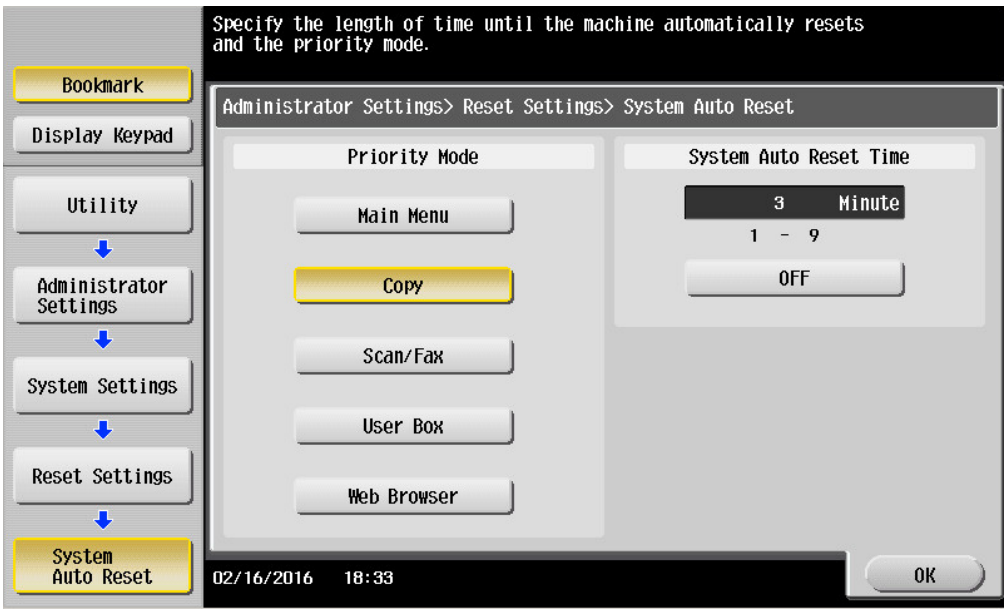
6. Tap **Reset settings**.



7. Tap **System Auto Reset**.



8. Press **C** on the keyboard and then press the number according to your preferred timeout in minutes. Confirm changes by tapping **OK**.



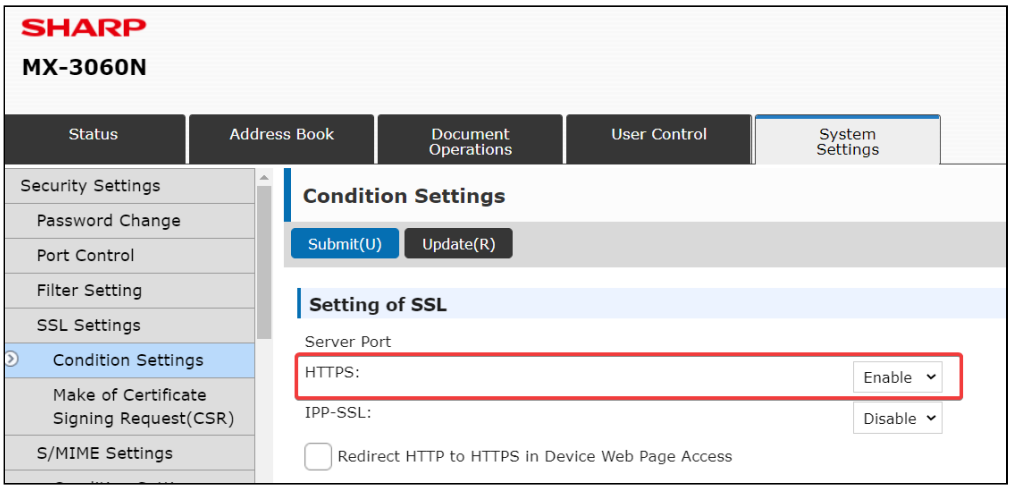
9. Change timeouts in **Auto Reset** screen (see point 7) in a similar way.

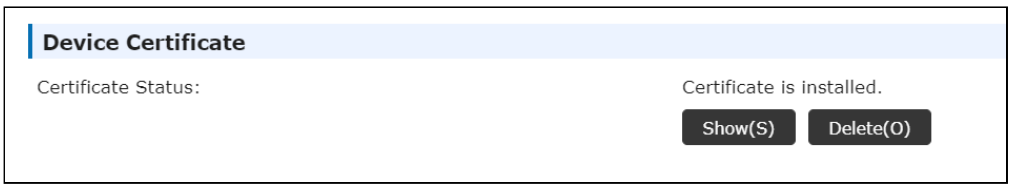
Configuring Sharp MFDs

Requirements

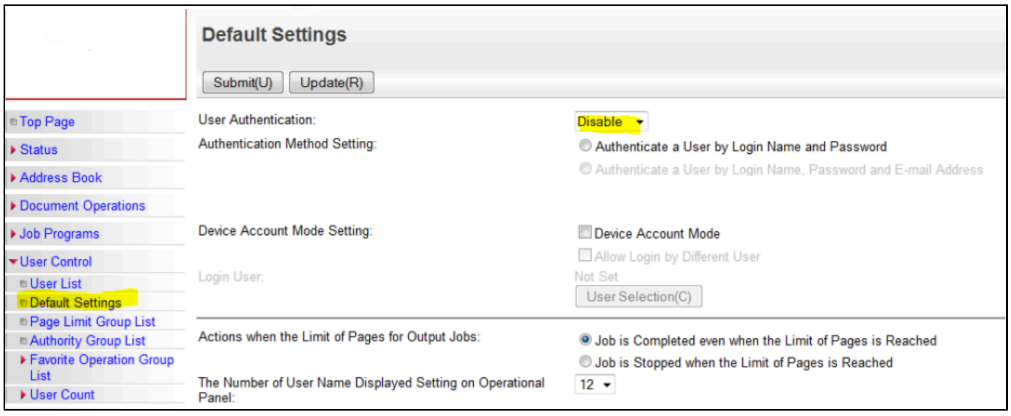
1. For the 1st gen Embedded terminal, the device must support OSA 3.5 and have MX-AMX2 and MX-AMX3 modules installed. For 2nd gen Embedded terminal, the device must support OSA 5.

2. The MFD must be configured to communicate via the SSL protocol and the associated certificate must be already created. Example for Sharp MX-3060N:





3. Sharp OSA5 devices: if **User Authentication** setting is present in **User Control > Default Settings**, set it to **Disable**.



Limitations

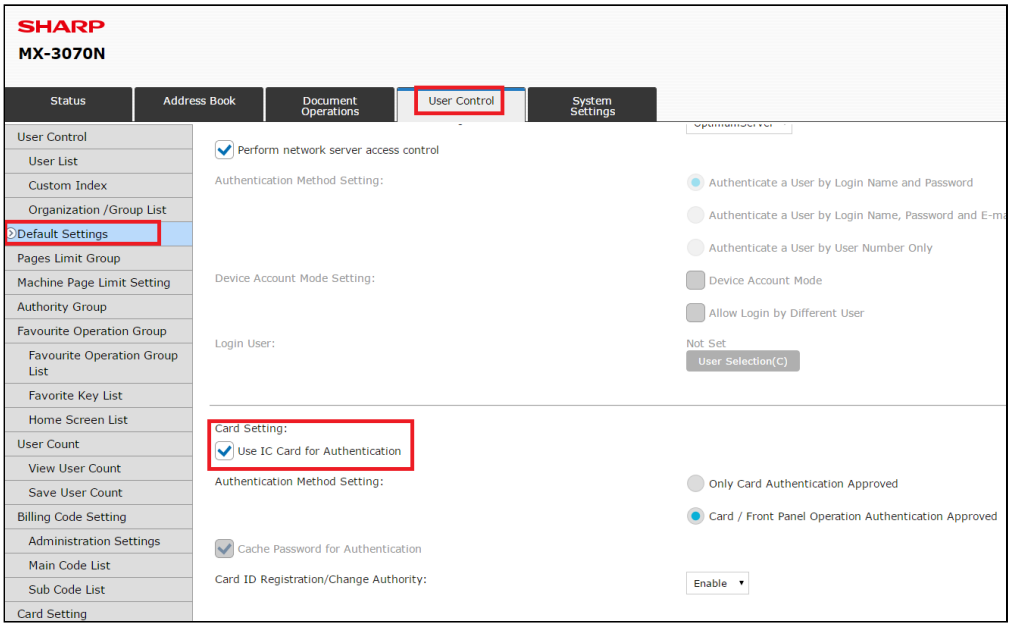
- Logout with a card is not possible if the card reader is in keyboard mode.
- Logout with a card is not possible when the device is not fully unlocked (the user did not enter the copy or scan applications after logging in).
- The *initial-screen* property is only supported on devices with OSA 4 and higher.
- If the MFD device is in sleep mode, the user must start the device manually before placing their card at the USB card reader.
- Print is not supported for users with username "admin", "blankuser", "service", "users", "other", "other2", "system", "invalid", "vendor", "vendor2" and "servicefss" as these are internally reserved words.
- In case of changing AMX2/3 license keys, Terminal Server must be restarted before installation of ET.
- If **IC Card Mode** is enabled on the device and the **Sharp mode** is set on the USB card reader, swiping the card causes occasional blinking of the display.
- The Authentication feature must be installed with the mode set to **To device** when both AMX2 and AMX3 licenses are enabled.

USB Card Reader configuration

To be able to use a card reader, you must set the IC Card mode manually.

1. Log in to the MFD's web interface
2. Go to **User Control > Default settings**.

3. Enable **Use IC card for Authentication**.



Configuring Xerox MFDs

Requirements

- The Embedded Terminal requires licensed and configured Xerox EIP Platform and Xerox XSA/CA at the device (EIP 1.5 and higher).
- Xerox Network Accounting (JBA, Job Limits) kit is required for accounting.

Limitations

- If a user changes their billing code while copying, the copy job will be assigned to the new billing code.
- When scanning on VersaLink models with color mode set to **Auto**, the device always produces a PDF file regardless of the configured file format.
- Correct functionality of Advanced Finishing options is guaranteed only with YSoft Universal Print Driver.
- Page Range setting is not supported.
- Not all Finishing options are supported on every device.

MFD configuration

The available settings, their naming, and their location in the MFD web interface can vary significantly among Xerox models. In case of doubt, refer to your MFD manual.

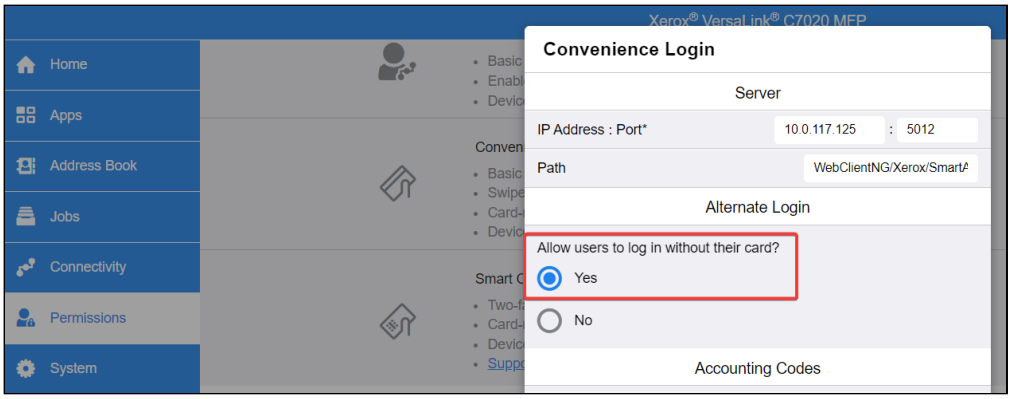
You can also find more information in the Dispatcher Paragon on-prem documentation.

Enter the MFD IP address in your web browser to log in to the MFD web interface. Perform the following steps:

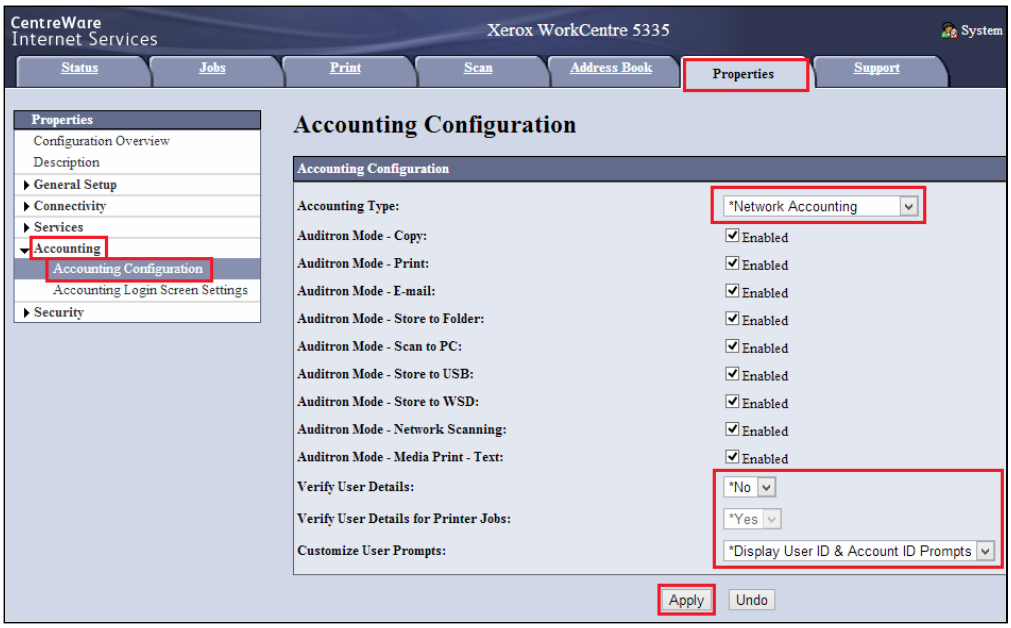
1. Time settings – These can be usually found in **Properties > General Setup > Date and Time**. Set the time and the time zone manually, or enter an NTP/SNTP server for the time to be updated automatically.

2. Protocols – These can be usually found in **Properties > Connectivity > Protocols**. Make sure that **HTTP/S**, **IPP/S**, and **SNMP** are enabled. If you need to use other protocols, enable them as well.

3. PIN-only authentication on Xerox VersaLink and AltaLink – If you plan to use PIN-only authentication, you must enable the **Allow users to log in without their card setting**. This can be usually found in **Permissions > Login/logout settings > Convenience**. Its function is to determine whether a USB card reader needs to be plugged in for authentication to take place. For example, if this is set to yes and there is no USB Card Reader attached, you can not use PIN-only authentication.



4. Network accounting (JBA) – Enable **Network Accounting** (formerly called JBA) technology if you are using device-dependent accounting instead of SNMP or job analysis accounting. This can usually be found in **Properties > Accounting > Accounting Configuration**. Example:



5. Scan Template Management – If your MFD has the **Scan Template management** setting, enable it to be able to use Dispatcher Paragon Cloud Scan workflows. Example:

6. SNMP – The settings can usually be found in **Properties > Connectivity > Protocols > SNMP selection**.

   a. If your MFD supports only SNMP v2, enable it and fill in the **Read-only community** name and **Read-write community** name. Fill in the same values in Dispatcher Paragon Cloud management interface when installing the Embedded terminal.

   b. If your MFD supports SNMP v3:

      1. Select **Enable SNMP v3 Protocol** and save the change.
      2. Click **Edit SNMP v3 Properties**.
      3. Select **Account Enabled**.
      4. Fill in the **Authentication Password**.
      5. Fill in the **Privacy Password**.
      6. Save the settings.
      7. Fill in the same values in Dispatcher Paragon Cloud management interface when installing the Embedded terminal.

2.4 DISPATCHER PARAGON CLOUD PORTAL GUIDE

2.4.1 OVERVIEW

The Dispatcher Paragon Cloud Portal is a web interface to allow:

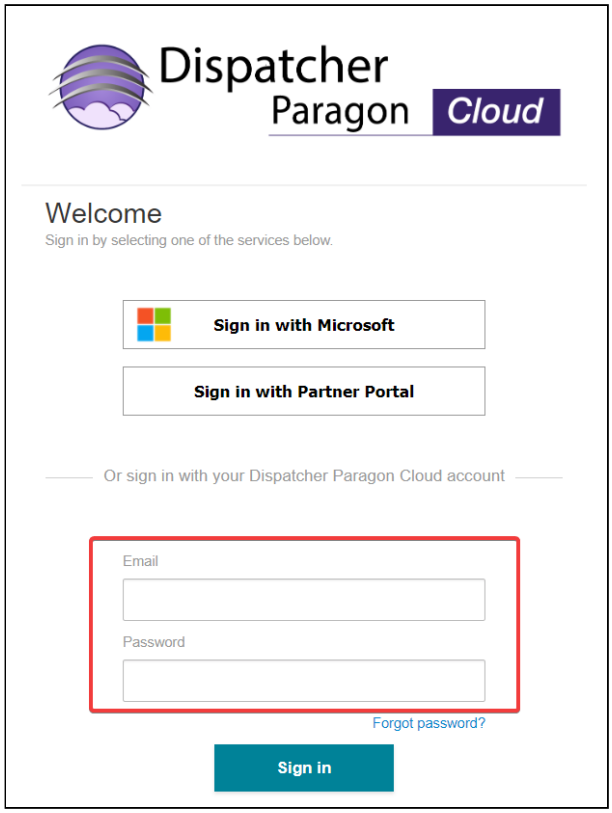
- Partner admins to register new Customers (i.e. companies).
- Customer admins to configure Edge devices and manage the Internally managed users.

If you are an Externally managed user: to access the Dispatcher Paragon Cloud Portal as a customer admin, you must assign to yourself (or to delegated users) a **Tenant admin** role for the **Cloud Print Management** application in Azure AD. Before accessing the Dispatcher Paragon

Cloud Portal for the first time, assign the role to yourself according to Tenant admin role for accessing Dispatcher Paragon Cloud Portal.

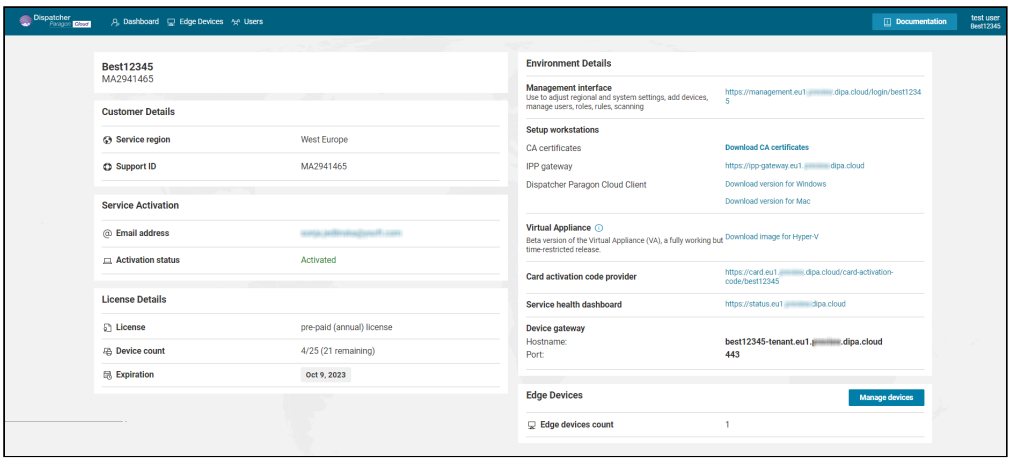
2.4.2 ACCESSING THE DISPATCHER PARAGON CLOUD PORTAL

1. Go to https://dipa.cloud/.
2. If you are an Externally managed user, click **Sign in with Microsoft** and enter your Microsoft credentials.
3. If you are an Internally managed user, enter your Dispatcher Paragon Cloud credentials and click **Sign in**.



2.4.3 DASHBOARD

After logging in, you will see the home screen of the Dispatcher Paragon Cloud Portal – the dashboard.



The dashboard allows you to see:

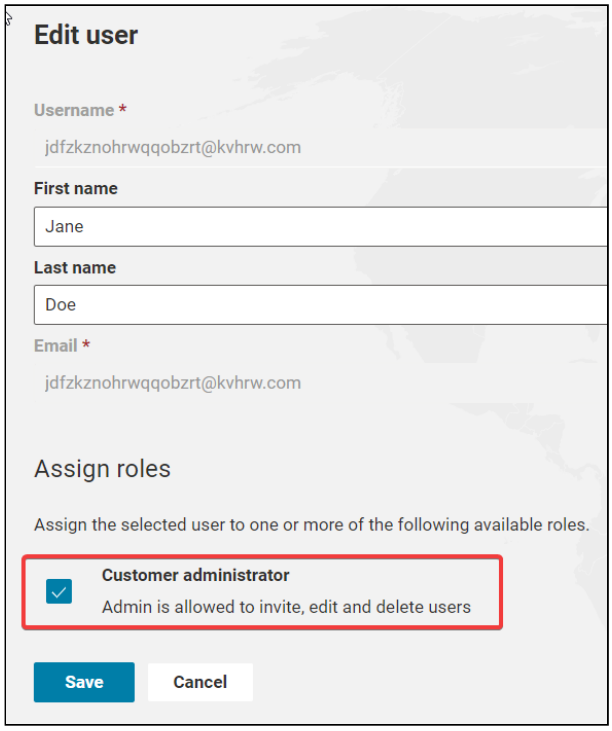
- Your Support ID
- Your license type and the number of your devices
- The links to:
  - Documentation
  - Dispatcher Paragon Cloud Management interface
  - Download the CA certificates
  - IPP Gateway
  - Download Client v3 package for Windows
  - Download Client v3 package for Mac
  - Download the VA image
  - Ricoh deployment tool
  - Card activation code provider (CACP)
  - Service health dashboard
- Device gateway
  - This section displays the address of your Cloud spooler.
- The number of your edge devices

2.4.4 GRANTING ACCESS TO CLOUD PORTAL TO AN INTERNALLY MANAGED USER

To grant access to the Dispatcher Paragon Cloud Portal to an Internally managed user, perform the following steps:

1. Invite the user to Dispatcher Paragon Cloud. See Internally managed users, section *Adding new users*.

2. Once the user accepts the invitation, you will see them on the Users tab in the Dispatcher Paragon Cloud Portal.
3. Click the edit icon next to the user.
4. In the **Assign roles** section, assign the **Customer administrator** role to the user.



5. Click **Save**.

> ⚠ Do not use the Management interface to grant the Customer administrator role to an Internally managed user. Such user would not be able to access Dispatcher Paragon Cloud Portal, because roles are synchronized from the Cloud Portal to the Management interface, but not vice versa.

2.4.5 REMOVING ACCESS TO CLOUD PORTAL FROM AN INTERNALLY MANAGED USER

1. In the Dispatcher Paragon Cloud Portal, click **Users**.
2. Click the edit icon next to the user whose access you wish to remove.
3. In the **Assign roles** section, clear the **Customer administrator** checkbox.
4. Click **Save**.

Do not use the Management interface to remove the Customer administrator role from an Internally managed user. Roles are synchronized from the Cloud Portal to the Management interface, but not vice versa. Therefore, such user would still be able to access the Cloud Portal.

2.4.6 MANAGING EDGE DEVICES

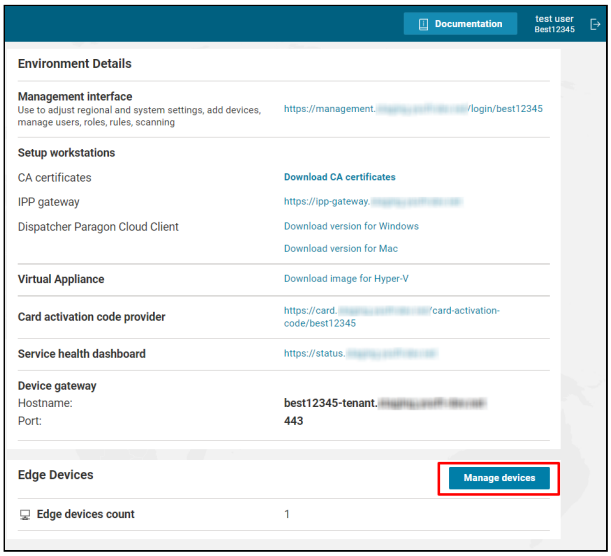
Configuring a newly added YSoft OMNI Bridge as a site server

Prerequisite: You have successfully completed the device code flow (device verification via code) as described in Preparing your YSoft OMNI Bridge.

Perform the following steps to configure your newly added YSoft OMNI Bridge as a site server.

Configuring an already configured edge device will cause problems described in YSoft OMNI Bridge Site Server maintenance.

1. Log in to Dispatcher Paragon Cloud Portal at https://dipa.cloud/.
2. You will see a Dashboard with detailed information and links. Click **Manage devices**.

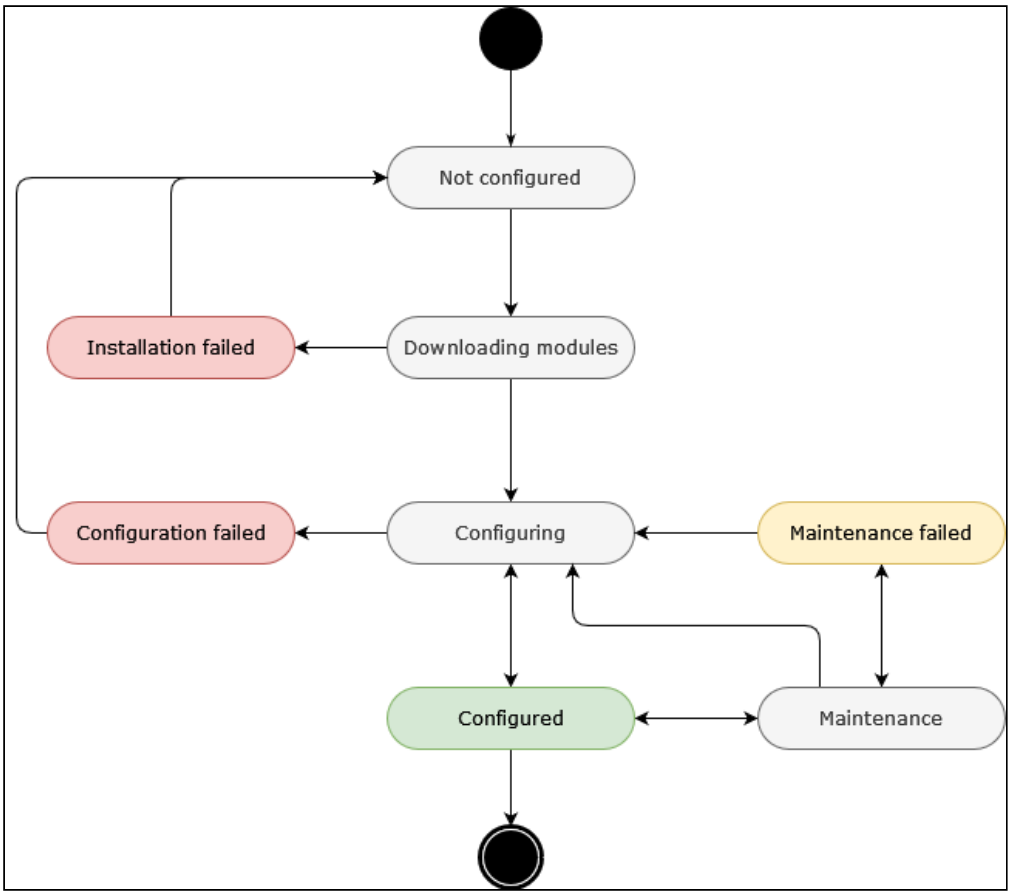


3. You will see a list of all of your Edge devices. Click the cogwheel icon next to the device you wish to configure.

4. A dialog window will open:
    a. Enter the device name. This is the name that will be visible in the IPP Gateway and in Client v3 in the **Print location** field (if you enable manual location selection). Therefore we recommend naming the device according to its location. The choice of name is especially important if your company has many locations.
        1. The name must be unique among all your devices.
        2. The name must be 1-64 characters long.
        3. The name cannot be the same as your Tenant ID (your domain with all non-ASCII characters replaced with hyphens ('-' character)).
        4. If necessary, you will be able to rename the device later on (as soon as the device state is **Configured**).
    b. Select the **Maintenance window** and the **Timezone**. The Maintenance window specifies during which hour of the day the device checks if any maintenance is needed. If yes, the device starts the maintenance process. Currently, the only maintenance operation is certificate renewal before expiration. The timezone should match the location of the configured device. It is used for calculating the maintenance time correctly with respect to the local time of the device.
5. Click **Configure**. The automatic configuration process will start. Your OMNI Bridge device will download the modules required for it to function as a site server.
6. Once the configuration process finishes, this dialog will close and you can view the state of your device in the device list. Also, the LED light on the OMNI Bridge LED will turn blue.
7. Optionally, you can log in to the Dispatcher Paragon Cloud management interface and navigate to **Devices** > **Spooler Controller groups.** You should see your OMNI Bridge there as a new Spooler Controller.

OMNI Bridge configuration states

The OMNI Bridge can have the following states:



State	Description
Not configured	You have claimed the device for your company via the device code flow. The OMNI Site Server has not been configured yet, but the device is ready to be configured.
Downloading modules	The device is currently downloading the OMNI Site Server modules. After the download is completed, the configuration process will begin automatically.
Configuring	The configuration process is now in progress and will take up to 15 minutes.

State	Description
Configured	The device is configured as OMNI Site Server and connected to cloud services. Once the device is visible in the Dispatcher Paragon Cloud management interface, you can start using it.
Installation failed	Installation of the OMNI Site Server application on the Edge device has failed. Try to configure the device again. If the problem persists, contact your service representative.
Configuration failed	The configuration has failed, please refer to the device display for more details. Try to configure the device again. If the problem persists, contact your service representative.
Maintenance	The maintenance process is now in progress on the device (for example, renewal of security certificates). This can take approximately 10 minutes. During this time the device may be unreachable.
Maintenance failed	An error occurred during the last maintenance. The device should remain operational. However, we recommend you to investigate why the maintenance process failed and resolve the problem.

Changing the device name

You can change the device name at any time in YSoft Cloud Portal.

1. Click the pencil icon next to the device.

2. Enter a new name.
3. Click **Rename**.

Be aware that:

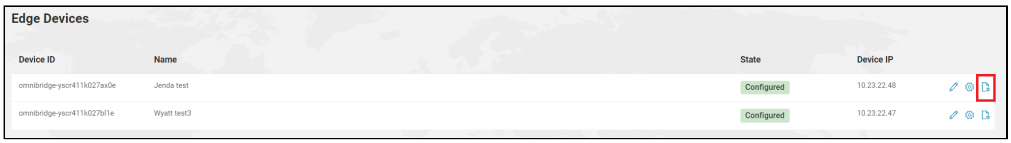
- the IPP URI on the IPP Gateway will not be available for a few minutes after the renaming.
- the name of the already-added printers on a user workstations will not change automatically. Mac users can edit the name manually. Windows users must remove and add the printer again.
- if manual Print location selection is enabled in Client v3, the users may have selected it by its name (stored in the local configuration). Renaming the device doesn't change the location name in Client v3. All affected users must change their Print location in the Client Settings to the new location (new device name). They will be prompted to change it when they try to send a print job.

Renewing device certificates

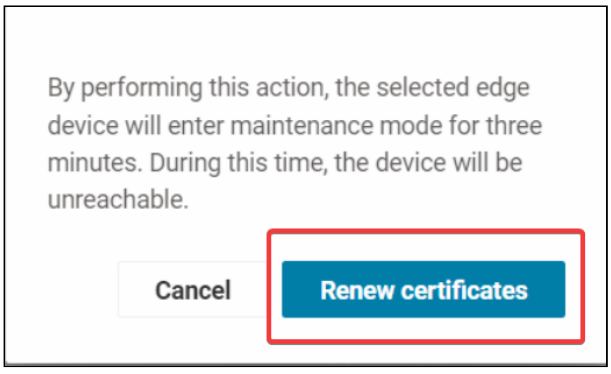
The device certificates are renewed automatically every 9 months. During the renewal, the device becomes unreachable for a few minutes. If you wish to renew them manually at a time that is convenient for you, perform the following steps.

The certificates are valid for 12 months, but they are automatically renewed 3 months before their validity ends.

1. Click the renew certificates icon next to the selected device.



2. A dialog window will open. Click **Renew certificates**.



3. The renewal will take a few minutes during which the device will be in **Maintenance** state and thus unreachable.

4. After successful renewal, the device will enter the **Configured** state again.

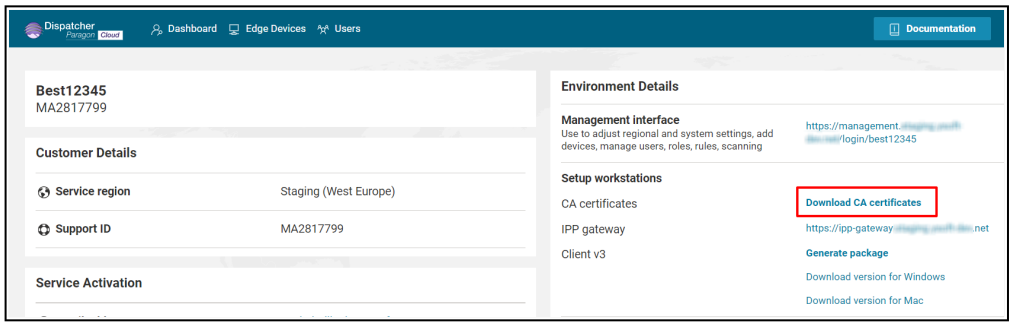
Downloading CA certificate

When YSoft OMNI Bridge Site Server is first configured, IPP Gateway module automatically receives a certificate signed by the MSP-provided cloud Certificate Authority (CA). You can:

- use your own certificate to establish trust between user workstations and YSoft OMNI Bridge Site Server. In that case, contact your service representative because manual steps need to be taken by the MSP.
- use the MSP-provided CA to establish trust between user workstations and YSoft OMNI Bridge Site Server.

If you decide to use the MSP-provided CA, perform the following steps:

1. Download the CA from the link in the dashboard of the Dispatcher Paragon Cloud Portal.



2. A file called **Root-CA-1.crt** will be downloaded to your workstation automatically.
3. Deploy this CA to user workstations. It needs to be placed in the **Trusted Root Certification Authorities** store (Windows), or the equivalent trust store for the users' operating system.
   - If you cannot deploy the CA to user workstations via means such as Active Directory, you can download it from the Cloud Portal and send it to the users by email together with instructions on how to import it. See Importing CA certificate for Edge printing manually.
4. If the users are using Microsoft Edge or Google Chrome browsers, no further action is needed, as these browsers use the OS Certificate Store. If the users use Mozilla Firefox, you must configure it to use the OS Certificate Store. See https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox.

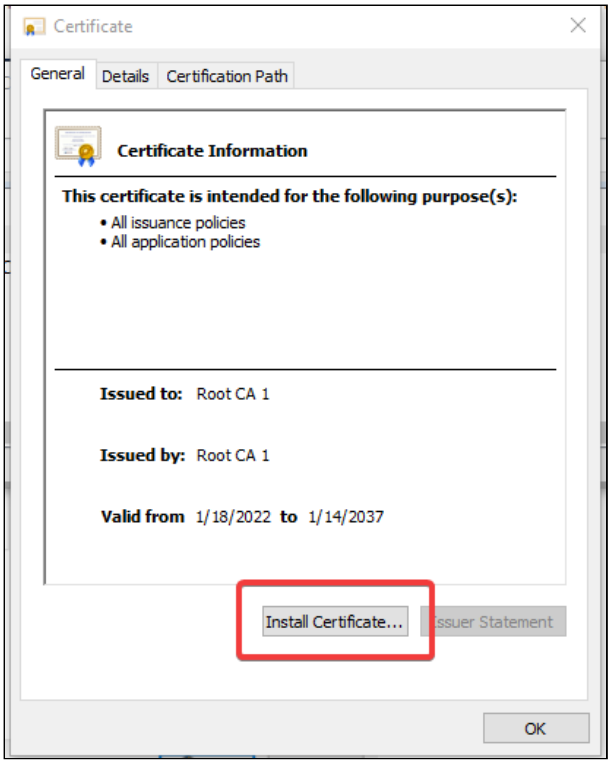
⚠ Users who don't have the CA at their workstations cannot:

- Generate IPP URI at the IPP Gateway because all YSoft OMNI Bridge devices appear as unreachable to them.
- Send print jobs to YSoft OMNI Bridge Site Server.

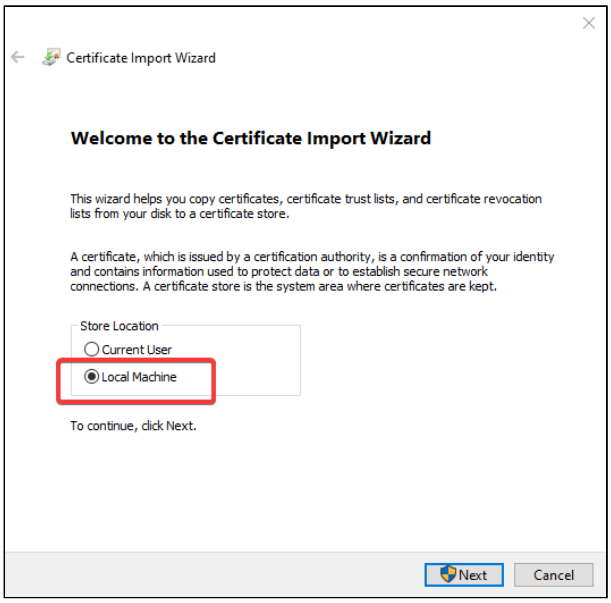
Importing CA certificate for Edge printing manually

Windows workstation

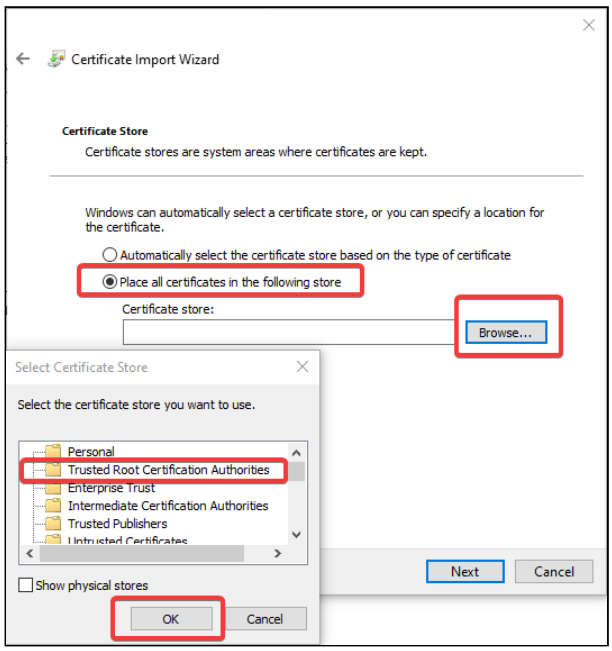
1. Open the **Root-CA-1.crt** file by double-clicking it.
2. A new dialog window will be displayed. Click **Install certificate**.



3. A **Certificate Import Wizard** will open. In Store Location, select **Local machine** and click **Next.**



4. In the next step, select **Place all certificates in the following store**. Click **Browse** and select **Trusted Root Certification Authorities**. Click **OK**.



5. Click **Next** and then click **Finish.**

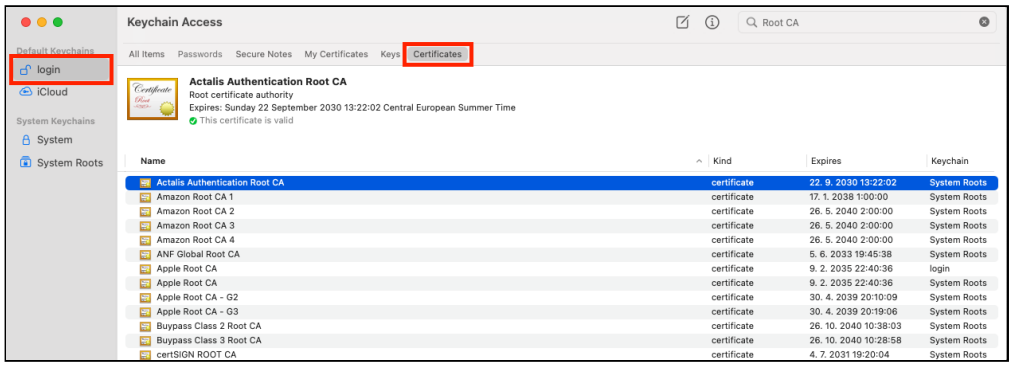
6. If you use Microsoft Edge or Google Chrome browsers, no further action is required, as these browsers use the Windows Certificate Store. If you use Mozilla Firefox, you must either import the certificates into it, or configure it to use the Windows Certificate Store. See https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox.

7. Restart your workstation.

Mac Workstation

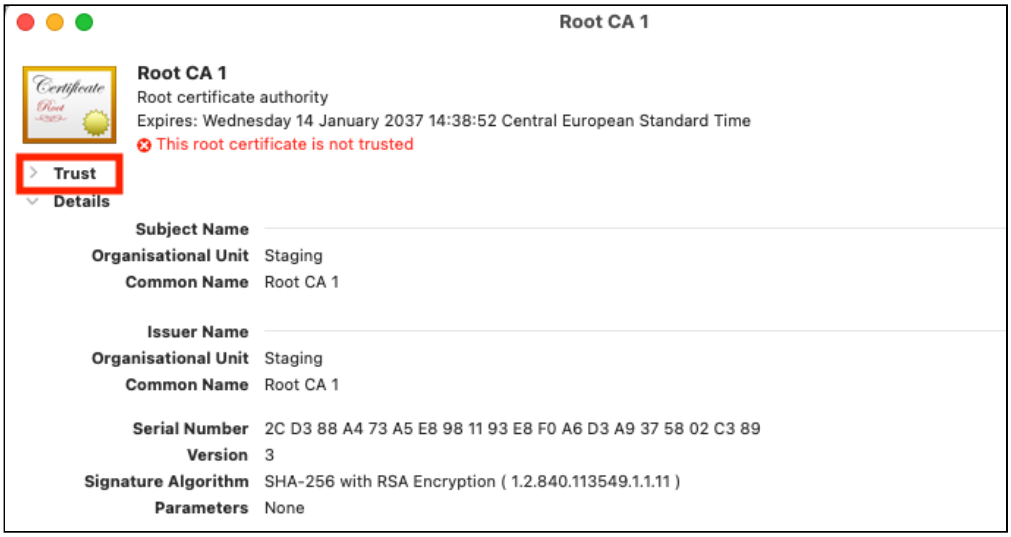
1. Open the **Root-CA-1.crt** file by double-clicking it.

2. The **Keychain Access** application will pop up. Navigate to the **Login** > **Certificates** tab.

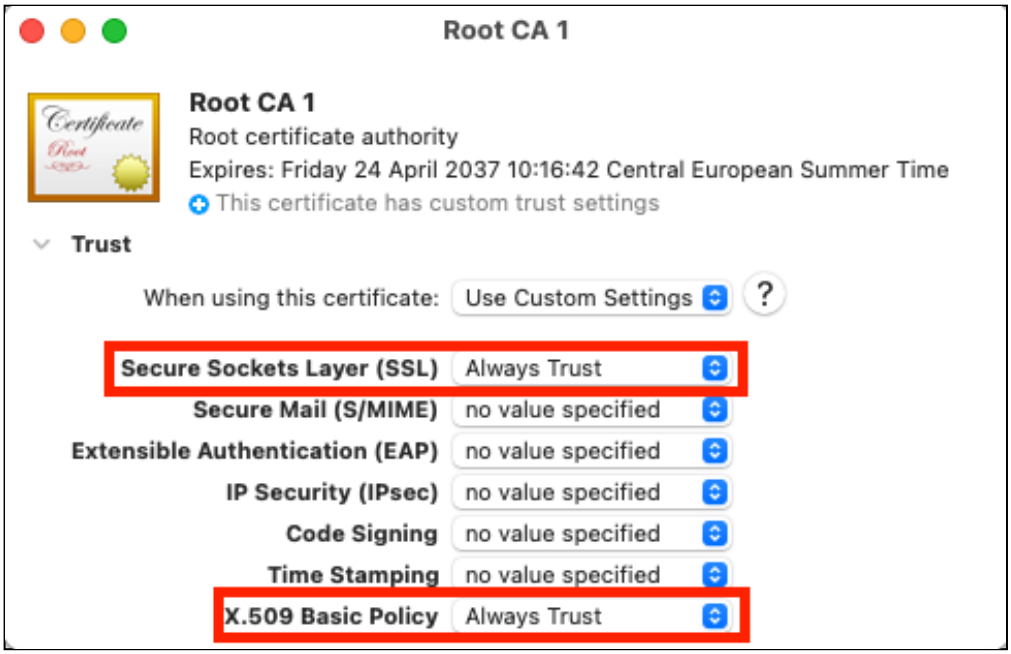


3. Find **Root CA 1** and double-click it.

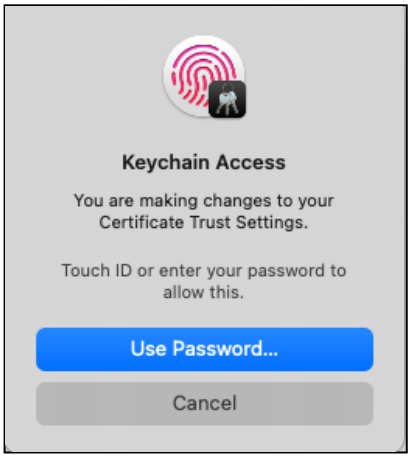
4. A new dialog window will be displayed. Expand the **Trust** section.



5. Select **Always Trust** in the **Secure Sockets Layer (SSL)** and **X.509 Basic Policy** fields.



6. Close the dialog and confirm the changes by entering your credentials or using Touch ID.



Linux workstation

> ⚠ The procedure may vary according to your Linux distribution. The following example is for Ubuntu.

1. Open Terminal by opening Terminal app or Ctrl+Shift+T shortcut.
2. Use the following command to install the **ca-certificates** package.

```
sudo apt-get install -y ca-certificates
```

3. Navigate to the folder where the **Root-CA-1.crt** file was downloaded. Use the following command to copy the downloaded file to ca-certificates.

```
sudo cp Root-CA-1.crt /usr/local/share/ca-certificates
```

4. Use the following command to update the certificate store.

```
sudo update-ca-certificates
```

2.5 USER MANAGEMENT

This chapter describes the types of user account in Dispatcher Paragon Cloud and the differences between them. For details on each type, see the subchapters:

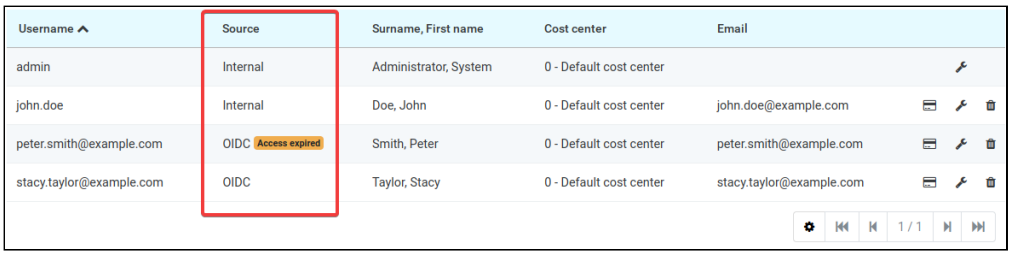
- Internally managed users
- Externally managed users

- Local users

2.5.1 THREE TYPES OF USER ACCOUNT

In Dispatcher Paragon Cloud, there are three types of user account:

- Internally managed users
  - User accounts created and managed in the Dispatcher Paragon Cloud Portal. They use OpenID connect Integration with external Identity Providers via OpenID Connect, but these accounts are NOT from an external Identity Provider.
  - This type of user account is intended for customers who have not yet migrated their identity platform to the cloud or have concerns over giving Dispatcher Paragon Cloud the permissions necessary to access their external Identity Provider platform.
  - These accounts can coexist with Externally managed users.
- Externally managed users – user accounts that are synchronized from an external Identity Provider, such as Azure Active Directory, via the OpenID Connect (OIDC) protocol. These users are not editable in the Dispatcher Paragon Cloud management interface. You can identify them by the OIDC badge in the Source column in the **Users** section. For detailed information on the integration, see Externally managed users.



- Local users – user accounts created and managed by the Dispatcher Paragon Cloud Management interface.

> ⚠ You can only edit the Local user accounts created by Dispatcher Paragon Cloud itself but you cannot create new Local user accounts.

Where to manage the three user types

> ⚠ Be aware that Externally managed users and Internally managed users are visible in the Dispatcher Paragon Cloud management interface only after performing card registration or logging into the Management interface (for example, to generate a PIN).

Actions (by admin)	Local users	Internally managed users	Externally managed users
Create user	Not possible	n/a Users register themselves after receiving an invitation.	your external Identity Provider • the user account is synchronized with Dispatcher Paragon Cloud when the user performs self-registration at the MFD terminal
Invite user to Dispatcher Paragon Cloud	n/a	Dispatcher Paragon Cloud Portal	n/a
Delete user	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud Portal	your external Identity Provider
Reset password	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud Portal	your external Identity Provider
Edit username	Dispatcher Paragon Cloud management interface	Not possible	your external Identity Provider
Edit first name and last name	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud Portal	your external Identity Provider
Edit email	Dispatcher Paragon Cloud management interface	Not possible	your external Identity Provider
Add role	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface

Actions (by admin)	Local users	Internally managed users	Externally managed users
Add alias	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface
Add billing code	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface
Assign/generate PIN	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface
Assign card	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface

Which actions can the three types of user perform

Actions (by end users)	Terminal type	Local users	Internally managed users	Externally managed users
Generate card activation code	Both	Dispatcher Paragon Cloud management interface	CACP	CACP
Generate PIN	Both	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface	Dispatcher Paragon Cloud management interface
Log in with Dispatcher Paragon Cloud username and password	Dispatcher Paragon Cloud Terminal	✅	❌	❌

Actions (by end users)	Terminal type	Local users	Internally managed users	Externally managed users
	Embedded terminals	✓	✗	✗
Log in with card at an MFD	Dispatcher Paragon Cloud Terminal	✗ Local users cannot log into CACP to generate a card activation code. A code generated in the Management interface will not work at a Cloud Terminal	✓	✓
	Embedded Terminals	✓	✓	✓
Log in with PIN at an MFD	Dispatcher Paragon Cloud Terminal	✓	✓	✓
	Embedded Terminals	✓	✓	✓
Log in to Dispatcher Paragon Client v3	n/a	✗	✓	✓

Logging in at the MFD terminal

In the Pure Cloud printing scenario, users can log in at the Dispatcher Paragon Cloud terminal in the following ways:

- Local users can authenticate via PIN or Dispatcher Paragon Cloud username and password.
- Internally managed and Externally managed users can authenticate via card or PIN. The username and password method is not supported.

In the Edge printing scenario, users can log in at the Embedded Terminal in the following ways:

- Local users can authenticate via card, PIN, or Dispatcher Paragon Cloud username and password, or combinations of those.
- Internally managed and Externally managed users can authenticate via card or PIN, or combinations of those. The username and password method is not supported.

2.5.2 INTERNALLY MANAGED USERS

Adding new users

In order to add Internally managed users to your Dispatcher Paragon Cloud, you must invite them, using a similar process to your own invitation. This is for security reasons - as any user can be invited this way, it is the user who must explicitly agree to become a user of Dispatcher Paragon Cloud. That means giving you the permission to manage their account for them - reset passwords, change role membership, and so on.

To invite a new user, perform the following steps:

1. Log in to Dispatcher Paragon Cloud Portal.
2. At the top of the page, click **Users**.
3. Click **Invite new users**.
4. Fill in the email address. You can enter multiple email addresses separated by a comma (,) or semicolon (;).

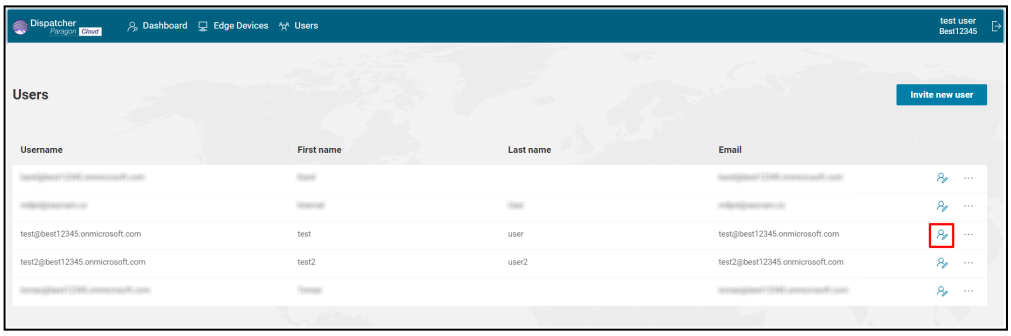
   Example of valid email formats:
   - name@company.com, secondname@company.com
   - Name Surname <name@company.com>; Name Surname<secondname@company.com>
5. Click **Submit**.
6. The user will receive an email with a unique, time-limited link. Once the user clicks the link, they are taken to the registration screen where they fill in their first name, last name, and password.
7. When the user accepts the invitation, their account appears in the list of users.

Only one invitation per user is allowed. Previously created invitations for the same user will be deleted when a new invitation is created.

Editing users

When editing a user, the editable fields are **First name** and **Last name**. **Username** and **Email** are not editable.

1. Click the user icon next to the user you wish to edit.



2. Edit the first name or the last name.
3. Click **Save**.

> While editing a user, you can assign a role to them. Currently, the only assignable role is **Customer admin**. This role allows the user to access the Dispatcher Paragon Cloud Portal and to manage users and edge devices there. See Dispatcher Paragon Cloud Portal guide.

Be aware that if you edit a user in Cloud Portal, the change will be reflected in the user list in Management interface only when:

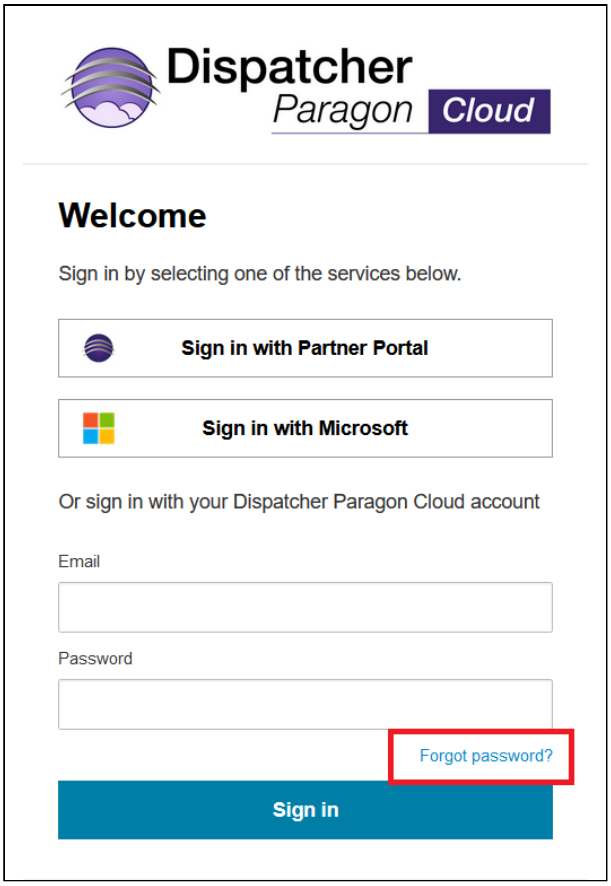
- the user logs in to the Management interface.
- the user attempts to log in at the MFD terminal. If the user information is cached in the spooler controller, the synchronization triggered by login at the MFD panel will not happen until the cache expires and the user logs in after the expiration. The expiration time is currently one hour.

Deleting users

1. Click the three-dots icon next to the user you wish to delete.
2. Click **Delete user**.
3. Confirm your action.

Resetting a password

Users must reset their passwords themselves by clicking the **Forgot password** link on the login screen of IPP Gateway/CACP/Client v3 and filling in their email address.



Pending invitations

Click **Pending invitations** to see the list of invitations and their status.

The invitations become visible in the **Pending invitations** list after you create the invitation. Once users accept the invitations and register themselves, they appear in the **Users** list.

To revoke an invitation, click the trash bin icon in the **Pending invitations** list next to the user whose invitation you wish to delete.

2.5.3 EXTERNALLY MANAGED USERS

Secure management of user identities is business-critical. Therefore, you can integrate your existing Identity Provider with Dispatcher Paragon Cloud so that your end users can authenticate to Dispatcher Paragon Cloud using accounts from an external Identity Provider.

> ⚠ Some user management tasks are done in Dispatcher Paragon Cloud management interface and some in Dispatcher Paragon Cloud Portal. For an overview where to do which task, see the table on page User management.

Adding new users

Prerequisites:

- you have already created the user accounts in your external Identity Provider.
- the users have their email addresses filled in at your external Identity Provider.

All users from your Azure AD are registered automatically during the Dispatcher Paragon Cloud activation process. If you add new users to your Azure AD, they can start using Dispatcher Paragon Cloud without any action on your side.

If you wish to create Internally managed users, you can invite them from Dispatcher Paragon Cloud Portal, and they will coexist with the Externally managed users. See Internally managed users.

Editing users

Editing username, first name, last name, email

You cannot edit the account properties which are synchronized from your external IdP (username, first name, last name, email). You can only edit them at the source, i.e., in the IdP. If you make any changes there, they are propagated to Dispatcher Paragon Cloud.

Adding role or alias or billing code

You can role, alias, or a billing code to Externally managed users in Dispatcher Paragon Cloud management interface.

⚠ If you want Dispatcher Paragon Cloud roles to be synchronized with groups in your Azure AD, the roles and groups need to meet specific conditions, see section *Group to role synchronization*.

1. Log in to Dispatcher Paragon Cloud management interface.
2. Go to **Users** > **Users**.
3. Click the edit icon next to the user you wish to edit.
4. Click **Add role** or **Add alias** or **Assign billing code**.
5. Select the role or billing code from the list. If you are adding an alias, type it into the input field and click **Add**.
6. The changes to the user profile will be saved automatically.

Deleting users

Deleting a user from Dispatcher Paragon Cloud management interface does not have any effect. You must delete the user account from your external Identity Provider.

Technical details about integration with external Identity Providers

⚠ Among the three possible types of user accounts in Dispatcher Paragon Cloud, only the Externally managed users are synchronized.

Supported Identity Providers (IdPs)

Azure Active Directory

Security

Dispatcher Paragon Cloud does not store passwords, only refresh tokens. For more information on refresh tokens, see Microsoft documentation: https://docs.microsoft.com/en-us/azure/active-directory-b2c/tokens-overview.

If a user account is disabled or deleted in an IdP, the change is propagated into Dispatcher Paragon Cloud (after the user does one of the actions that trigger user synchronization).

User synchronization

When does a user from an external IdP appear in Dispatcher Paragon Cloud management interface?

After the user performs card activation at the MFD terminal, or logs in to the Management interface to generate a PIN, you will be able to see them in the Management interface.

The new user is marked as an external IdP user in the database. From then on, you cannot edit the synchronized properties of the user account in the Dispatcher Paragon Cloud management interface. You can only edit them at the source, i.e., in the IdP. If you make any changes there, they are propagated to Dispatcher Paragon Cloud.

The **User Principal Name** (in most cases the e-mail address) from the external IdP serves as the login name of the new user in Dispatcher Paragon Cloud management interface.

What is synchronized

Only users who exist in external IdPs are synchronized. The sole entity that is updated is the user profile – specifically the first name, last name, email, and roles.

Local users and Internally managed users are unaffected by coexistence with Externally managed users.

When does synchronization occur

Once user accounts have been created in Dispatcher Paragon Cloud and their refresh tokens stored, those accounts need to be kept up to date and in sync with the IdP. User accounts are synchronized every time one of the below events occurs:

1. The user submits a print job.
2. The user attempts to log in at the MFD terminal.
3. The user logs in successfully to the Dispatcher Paragon Cloud management interface.

All three events are equivalent and the account update procedure is the same for all of them.

If an account synchronization fails when the user attempts to log in, the user remains unauthorized since Dispatcher Paragon Cloud was unable to verify if the user account in the external Identity Provider was still active and valid. See the *Delays* section below for more details.

Delays in synchronization

Following successful user synchronization, information from the last synchronization is cached. Synchronization of the same account is repeated only once the cache expires. Therefore, changes of user accounts in an external IdP may not immediately be visible everywhere due to the caching of multiple pieces of information on multiple levels. Change propagation may take up to 65 minutes at the most.

For this reason, if a user account is disabled or deleted from an external IdP, the user may still be able to use Dispatcher Paragon Cloud for up to 65 minutes.

In the Edge printing scenario, the delays are the same. However, in this scenario, the users are able to print even if the connection to the Dispatcher Paragon Cloud service is temporarily disrupted.

Disabling users in an Identity Provider

When a user account is disabled in an external IdP, this change is also reflected in Dispatcher Paragon Cloud – the user account is marked as expired. There are three ways of disabling user access to Dispatcher Paragon Cloud:

- Revoking user rights in the external IdP.
- Disabling the user in the external IdP.
- Deleting the user in the external IdP.

Any of these actions causes the user to be prompted to activate their account again using the card activation flow when they try to log in at an MFD terminal.

The user may still be cached in the system and may still be able to log into their account for up to 65 minutes after being disabled in the external IdP.

If you want to assign the card of the expired user to another user, wait for 65 minutes after disabling/deleting the user in your external IdP, then hand over the card to the new user and instruct them to perform self-registration. Or, you can remove the card manually from the expired user in Dispatcher Paragon Cloud management interface, and assign it to the new user.

User expiration

Access to Dispatcher Paragon Cloud can expire for Externally managed users. Access expiration means that the last synchronization from the external IdP has failed. The failure can be caused by:

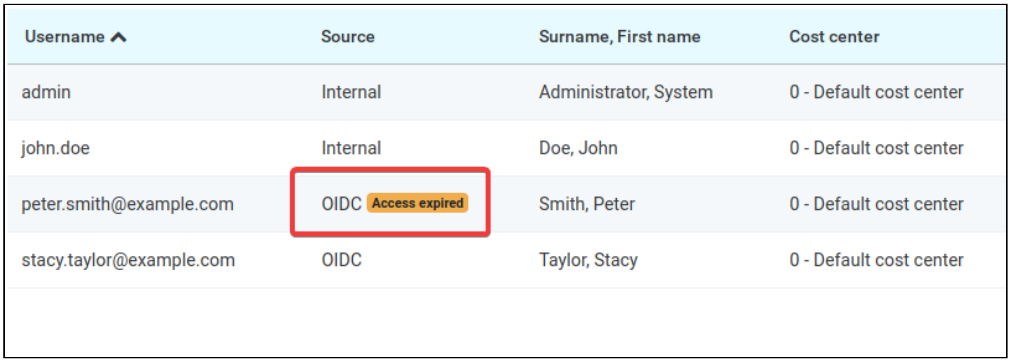
1. The user hasn't logged in to the system for more than 90 days, thus the link between the Dispatcher Paragon Cloud management interface and the external IdP expired. The user can reactivate their access by one of the following methods:
   - Logging in to the Dispatcher Paragon Cloud management interface.
   - Registering their card again via the Card activation code provider page, as described in the *End user guide*, chapter Card registration at the MFD terminal.
2. An admin revokes the user's session in the external IdP. For example, in Azure AD, by revoking the user's Azure AD refresh tokens. For more details, see https://learn.microsoft.com/en-us/azure/active-directory/develop/access-tokens#token-revocation. The user can reactivate their access by one of the following options:
   - Logging in to the Dispatcher Paragon Cloud management interface.
   - Registering their card again via the Card activation code provider page, as described in the *End user guide*, Card registration at the MFD terminal.

3. An admin disables or deletes the user account in the external IdP.

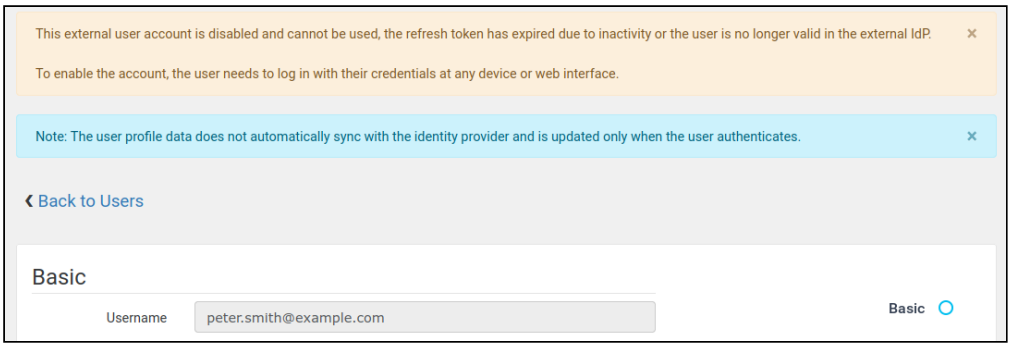
> ⚠ Users with expired access are not allowed to authenticate on MFD terminals until they reactivate their access. If a user with expired access swipes their card on a reader, the card activation screen is displayed.

During card self-assignment on the terminal, Dispatcher Paragon Cloud considers the cards owned by expired users as free cards. Therefore, any other user can assign such a card to themselves.

Admins can see that an account is expired in **Users** section in the Dispatcher Paragon Cloud management interface:



and in the user detail:



> ⚠ Note that synchronization happens only if a user tries to access Dispatcher Paragon Cloud, therefore more users can actually be expired than are detected by Dispatcher Paragon Cloud. For the same reason, what is displayed about users in Dispatcher Paragon Cloud may not be as up to date as the external IdP.

Group to role synchronization

Dispatcher Paragon Cloud synchronizes groups from external IdP starting that start with prefix "Cloud Print: " and maps them to Dispatcher Paragon Cloud roles.

What is synchronized

Only roles that already exist in Dispatcher Paragon Cloud are synchronized from IdP, therefore a group without a counterpart among the roles will be ignored. The synchronization is one-way only – if you make changes in role membership in Dispatcher Paragon Cloud, the changes will not be reflected in the external IdP.

Examples:

Role name in Dispatcher Paragon Cloud management interface	Group name in external IdP	Will the synchronization happen?
cash desk operators	Cloud Print: cash desk operators	Yes, this is a correctly named group.
forcedduplexprint	forcedduplexprint	No, the group name in external IdP doesn't contain a prefix.
none	Cloud Print: headquarters employees	No, the group in external IdP doesn't have a corresponding role in Dispatcher Paragon Cloud.
system admins	Cloud Print: system admins	No, the system **admins** and **system subadmins** roles are restricted from being synchronized with external IdP.

How to enable synchronization

To enable synchronization of your roles in Dispatcher Paragon Cloud with your groups in external IdP, perform the following steps:

1. Create or edit a group in the external IdP. The name must contain prefix "Cloud Print: " (including the whitespace).

2. Create or edit the corresponding role in Dispatcher Paragon Cloud management interface.

> ⚠ The name of the role must adhere exactly to the name of the group in external IdP without prefix, while being case sensitive.

When does synchronization occur

The group to role synchronization is triggered by the same actions as user synchronization (see *User synchronization > When does synchronization occur*). Therefore, until a user performs any of those actions, the changes in their role membership are not updated and visible in Dispatcher Paragon Cloud management interface.

2.5.4 LOCAL USERS

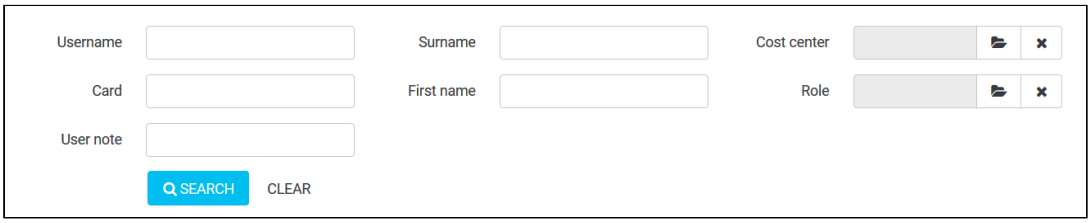
> ⚠ The main limitation of Local users is that they do not have an option to send a print job to Dispatcher Paragon Cloud under their Local user account because they cannot log in to IPP Gateway or to Dispatcher Paragon Client v3. Therefore, creating new Local user accounts is disabled. You can only edit the Local user accounts created by Dispatcher Paragon Cloud itself (e.g. the admin account created during Activating your Dispatcher Paragon Cloud).

Accessing the User management

1. Log into the Dispatcher Paragon Cloud management interface with your admin account.
2. In the main menu on the left side of the screen, select **Users**. The **Users** tab will be displayed.

Searching the user list

To find a specific user or users, use the search pane in the upper part of the **Users** tab.



The following filters can be used to search the user list:

- **Username** – Enter a number of initial characters (from the first character up to the whole username).

- **Surname** – Enter a number of initial characters (from the first character up to the whole surname).
- **First name** – Enter a number of initial characters (from the first character up to the whole first name).
- **Card** – Enter the exact card number.
- **User note** – Enter a number of initial characters - from the first character up to the whole user note.
- **Cost center** – Select a cost center from the list by clicking the **Choose a cost center from the list** icon . You can remove this filter by clicking the **Cancel this filter** icon .
- **Role** – Select a role from the list by clicking the **Choose a role from the list** icon . You can remove this filter by clicking the **Cancel this filter** icon .

Click **SEARCH** to apply filters, click **CLEAR** to reset filters.

Editing users

To edit an existing user, take the following steps:

1. On the **Users** tab, find the user you want to edit. For more information on searching users, see section *Searching the list of users* above.
2. Click the **Edit user** icon .
3. You can now change or add all the settings described in the section *Adding user manually*.
4. Click **SAVE CHANGES** in the lower left corner of the tab.
5. A notice regarding user changes appears in the upper part of the tab.
6. Click **Back to Users** in the upper left corner of the tab.

Deleting users

> In Dispatcher Paragon Cloud management interface, you can only delete Local users. If you delete an Externally managed user, the account will disappear only until the user performs some of the actions that trigger the synchronization with external IdP. You must delete such users in your external IdP. See Externally managed users.

To delete a user, do the following:

1. On the **Users** tab, find the user you want to delete. For more information on searching for users, see section *Searching the list of users* above.
2. Click the **Delete user** icon . The confirmation window opens.
3. In the window, click **Yes**.

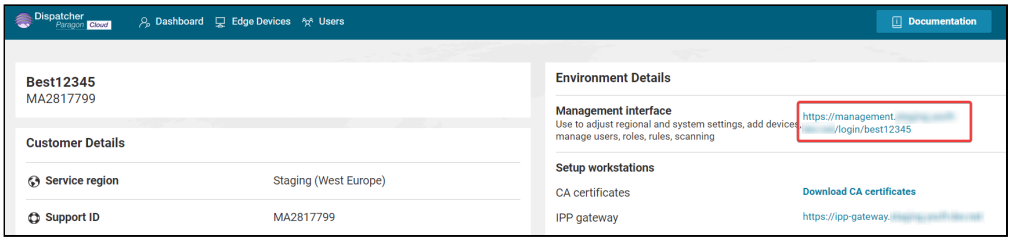
4. Notification **The user has been deleted** appears at the top of the tab. The user disappears from the list of active users and can be found in the list of deleted users.

2.6 DISPATCHER PARAGON CLOUD MANAGEMENT INTERFACE GUIDE

2.6.1 ACCESSING THE DISPATCHER PARAGON CLOUD MANAGEMENT INTERFACE

To access the Dispatcher Paragon Cloud management interface for the first time, do the following:

1. Open the email with subject *Welcome to Dispatcher Paragon Cloud* which you received after your company was registered in Dispatcher Paragon Cloud.
2. Click **Manage account**. This will take you to Dispatcher Paragon Cloud Portal.
3. Log in to Dispatcher Paragon Cloud Portal. For more information see Dispatcher Paragon Cloud Portal guide.
4. On the dashboard of Dispatcher Paragon Cloud Portal, click the link in the **Management interface** section.

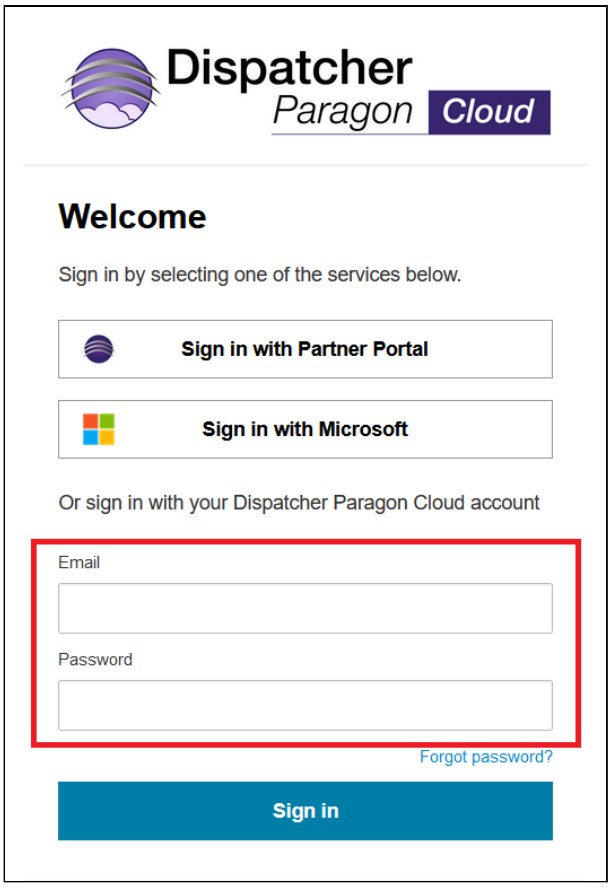


5. You will see the Dispatcher Paragon Cloud management interface login screen.

> You can change the language of the Dispatcher Paragon Cloud management interface before you log in:
>
> a. Click the flag icon  in the upper right-hand corner of the screen. A dropdown menu is displayed.
>
> b. In the menu, select the desired language. The language of the Dispatcher Paragon Cloud management interface changes.

6. Click **Single sign-on.**

7. On the next page:
   a. If you are an Externally managed user, click **Log in with Microsoft** and enter your company credentials.
   b. If you created your user account manually in Dispatcher Paragon Cloud (Internally managed user), enter your Dispatcher Paragon Cloud credentials directly on the login screen.



2.6.2 SUPPORTED LANGUAGES

- Basque
- Brazilian Portuguese
- Chinese Simplified
- Czech
- Danish
- Dutch
- French
- German
- Hungarian
- Italian
- Japanese
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish
- Turkish

2.6.3 MANAGING DEVICES

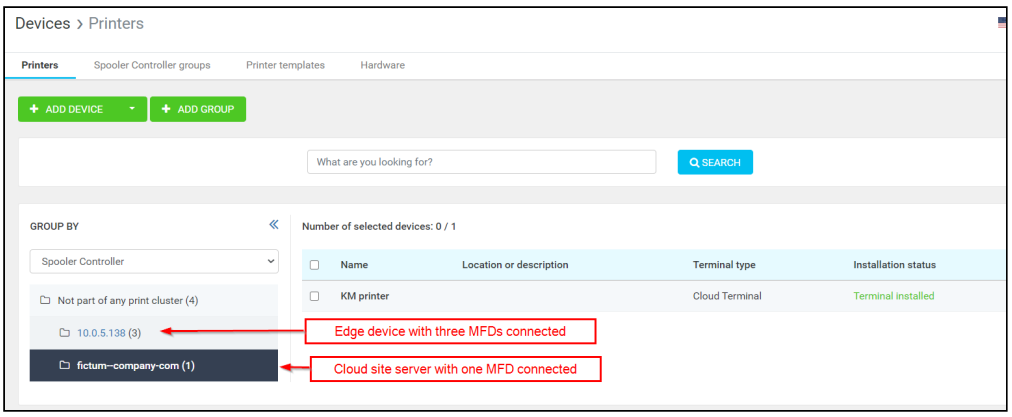
If you are using Pure Cloud printing, install the Dispatcher Paragon Cloud Terminal on your MFDs. You will then have the MFD(s) under your Cloud site server.

If you are using an edge device (e.g. YSoft OMNI Bridge), install the Dispatcher Paragon embedded terminal on the MFD(s).

You will then have the MFD(s) under your OMNI Site Server (your edge device).

> You can change the OMNI Bridge name in Dispatcher Paragon Cloud Portal, see Managing Edge devices.

Example:



Pure Cloud printing: installing the Dispatcher Paragon Cloud Terminal

Prerequisites

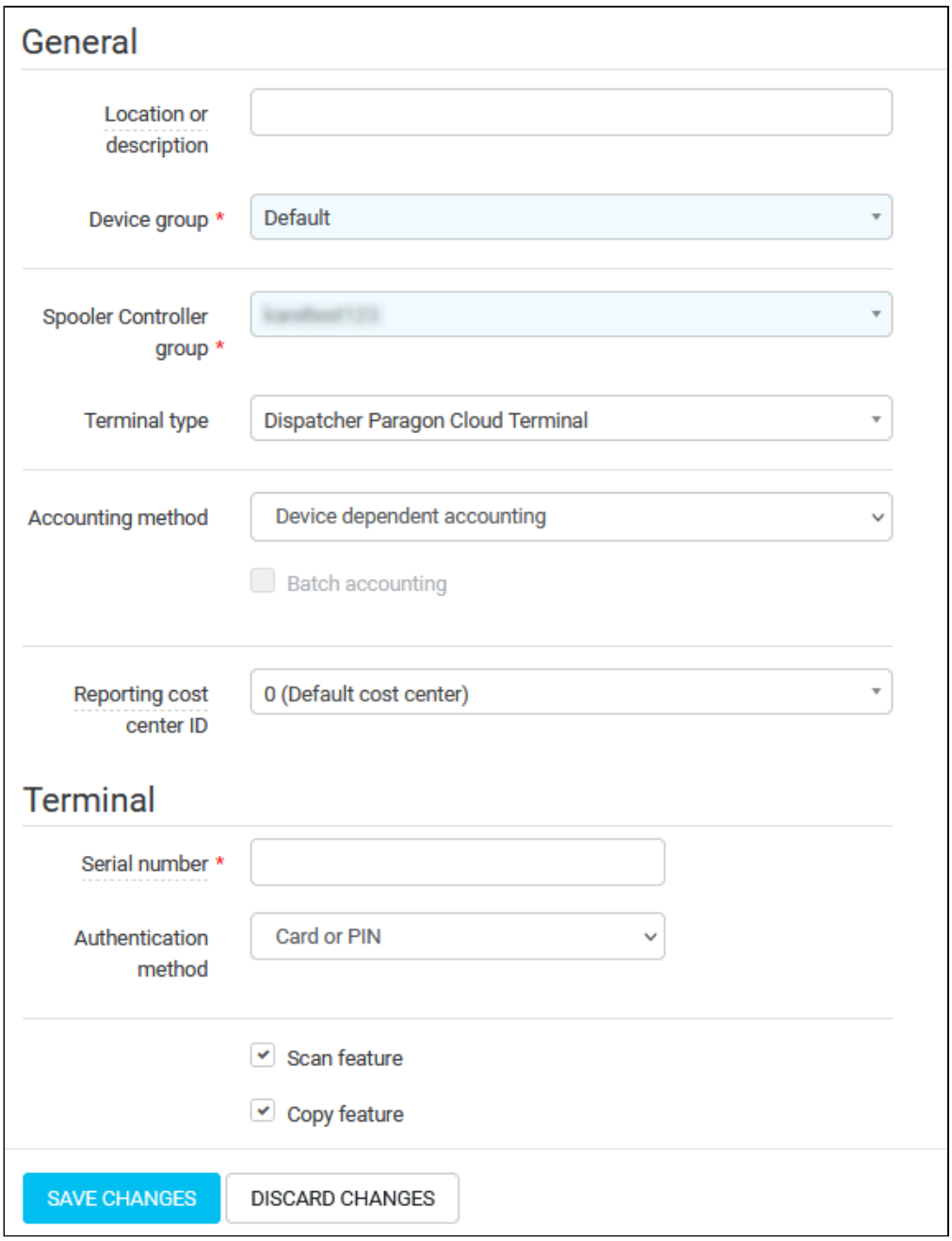
1. You have completed the configuration steps at the MFD, see Configuring Konica Minolta MFDs for Dispatcher Paragon Cloud Terminal.
2. You have the MFD serial number at hand.

Installation

To install the Cloud Terminal on an MFD, perform the following steps:

1. Log in to the Dispatcher Paragon Cloud management interface with your admin account.
2. Go to **Devices.** The **Printers** tab is displayed.
3. On the tab, click **Add Device**.
4. Select Terminal type **Dispatcher Paragon Cloud Terminal**.
5. In **Spooler Controller group**, select your **Cloud site server**.
6. In **Accounting method**, select the accounting method. For more information, see Accounting.
7. Whether you need to select a price list for the MFD depends on your configuration of cost centers. For more information see Price lists.
8. Enter the MFD serial number in the **Serial number** field. Ensure it matches the serial number in the Dispatcher Paragon Cloud Terminal, and in the MarketPlace info.

   You can find the serial number also at the MFD panel. Tap **Utility > Device information**.

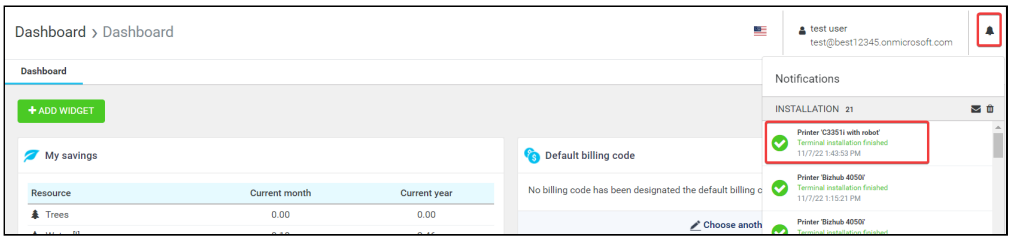


9. In the **Authentication method**, select **PIN** or **Card** or **Card or PIN**.

> ⚠ Username/password authentication is available only for *Local users*, and only at MFDs with Embedded Terminals.

10. Click **Save changes**.
11. The installation will start. A new window with the installation progress will appear.

12. If the installation was successful, you will see a success message in the window with installation progress. If you closed the window, you can access the message by clicking the notifications icon.



13. When tapping **MarketPlace** > **Dispatcher Paragon Cloud Terminal** on the MFD, you should now see a login screen.

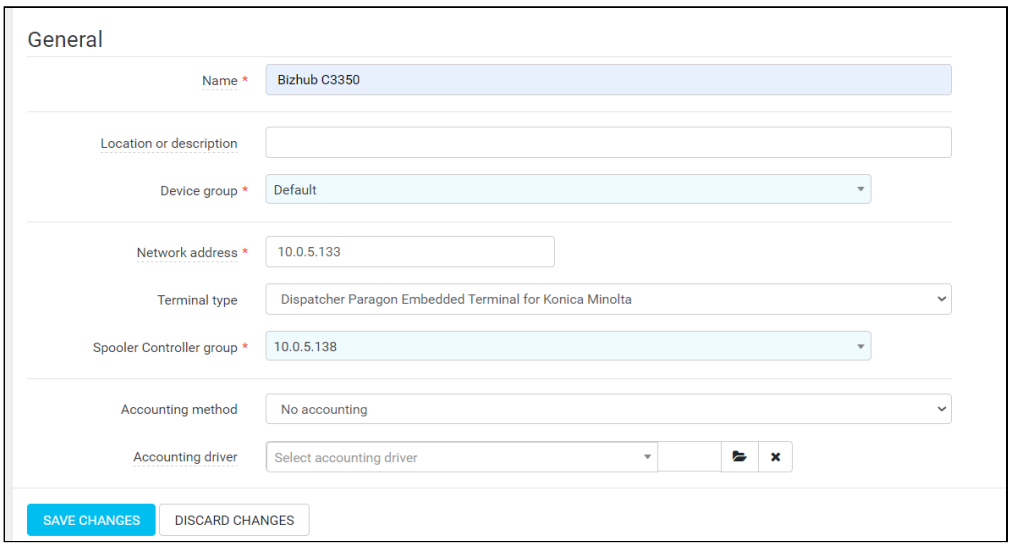
Edge printing: installing the Dispatcher Paragon Embedded Terminal

To install one of the Dispatcher Paragon Embedded Terminals on an MFD, perform the following steps:

1. Log in to the Dispatcher Paragon Cloud management interface with an admin account.
2. Go to **Devices.**
3. Click **Add Device**.
4. In **Network address**, enter the IP address of the printer.
5. In **Spooler Controller group**, select your YSoft OMNI Bridge.
6. In **Terminal type**, select **Dispatcher Paragon Embedded Terminal for <vendor name>**. The available vendors are Brother, Epson, Fujifilm BI, Konica Minolta, Sharp, and Xerox.

   > The list of available terminals is populated according to your selected Spooler controller group.

7. In **Accounting method**, select the accounting method. If you selected anything else than *No accounting*, select also an *Accounting driver* in the **Accounting driver** dropdown menu. For more information, see Accounting.



8. Whether you need to select a price list for the MFD depends on your configuration of cost centers. For more information see Price lists.

9. In the **Terminal mode**, select **Dispatcher Paragon Terminal Application - 2nd Gen**.

10. In the **Authentication method**, select **Card** or **Card and PIN** or **Card or PIN**.

    Username/password authentication is available only for *Local users*, and only at MFDs with Embedded Terminals.

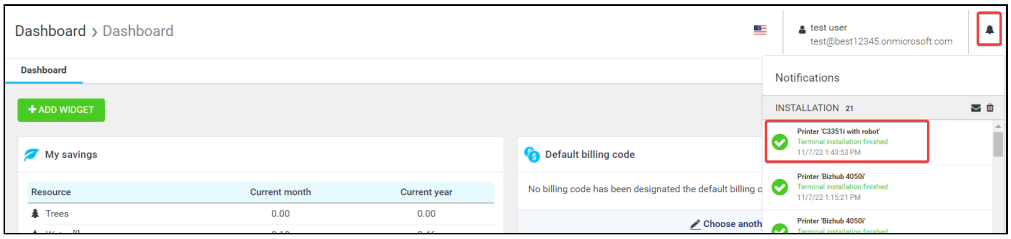
11. Fill in the Admin username and password for the MFD.

12. Click **SAVE CHANGES.**

13. The installation will start. A new window with the installation progress will appear.

    The TLS 1.0 protocol must be enabled on the MFD, otherwise, the installation might fail.

14. If the installation was successful, you will see a success message in the window with installation progress. If you closed the window, you can access the message by clicking the notifications icon.



Adding reporting-only devices (terminal type: none)

Reporting-only devices are MFDs or SFDs where you want to capture the number of printed pages (and related statistics) but do not need any other capability such as Embedded Terminal or Cloud Terminal or print roaming.

You can set up reporting-only devices in both Pure Cloud printing scenario and Edge printing scenario. In both cases, the end users will need Dispatcher Paragon Client v3 to add direct print queues to their workstation.

If the device is connected to cloud spooler (Pure Cloud printing), Client v3 must be configured in client spooling mode.

To add a reporting-only device, perform the following steps:

1. Log in to the Dispatcher Paragon Cloud management interface with your admin account.
2. Go to **Devices.**
3. Click **Add Device**.
4. In **Network address**, enter the IP address of the printer.
5. In **Terminal type**, select **None**.
6. In **Direct queue**, enter the name of the direct queue for the device. This name will be visible to the end users.
7. In **Accounting method**, select either **Offline accounting** or **No accounting.**
8. Click **SAVE CHANGES**.

Accounting

Accounting collects information from which Dispatcher Paragon Cloud creates usage and cost reports:

- Information on each job, device and user.
- Detailed information on each job:
  - The number of pages per paper size (in two sizes: large and normal)
  - The number of color/middle color (if supported by the device)/monochrome pages
  - Duplex usage
  - Job title
  - Workstation of origin

- Coverage information for each job:
  - The coverage percentage of the page (non-white area/total page area)
  - Estimated usage of CMYK toner cartridges

> Coverage information is only provided by Offline accounting.

Not all information may be available for every print job or deployment scenario. Dispatcher Paragon Cloud is typically able to trace about 95 to 98% of pages to individual users or departments. This is most commonly caused by various maintenance print jobs, system status print jobs, direct IP printing, server reboots and the limitations of page meter tracking (vendor-specific limitations).

Accounting methods

	Offline accounting		Device dependent accounting	
	Print	**Copy and scan**	**Print**	**Copy and scan**
Pure Cloud printing	✅ Only print jobs done via Dispatcher Paragon Cloud Terminal are accounted for based on job analysis done by the job parser.	❌	✅ Print jobs done via Dispatcher Paragon Cloud Terminal are accounted for in the same way as Offline accounting (job analysis done by the job parser). Therefore, it has the same behavior and limitations as Offline accounting.	✅ Copy and scan jobs done via Dispatcher Paragon Cloud Terminal are accounted for based on the information provided by MFD.*
Edge printing	✅	❌	✅	✅

* Copy and scan jobs done at the native device interface are not accounted for due to IWS platform limitations. This applies even if the native interface is accessed using Quick actions.

- OMNI Bridge spooler limitation: A print job will not be accounted if a user sends it to an OMNI Bridge spooler and releases it at an MFD with Dispatcher Paragon Cloud Terminal and the job analysis on the OMNI Bridge took more than 3 minutes. This applies both to Device dependent accounting and Offline accounting at the Dispatcher Paragon Cloud Terminal.
  The maximum document size depends on the complexity of the document and the current load on the OMNI Bridge. In general, the document size at which this problem may occur is in the range of thousands of pages.
  To make sure that a large print job is accounted, we recommend releasing it at an MFD with Embedded terminal where the accounting method is Device dependent accounting.
- Cloud spooler limitation: A print job will not be accepted and accounted if a user sends it to the cloud spooler and it fails to be parsed there because parsing took more than 5 minutes. This feature prevents print jobs that cannot be accounted from being printed.

For more information, see Offline accounting and Device dependent accounting.

Enabling accounting

Prerequisites:

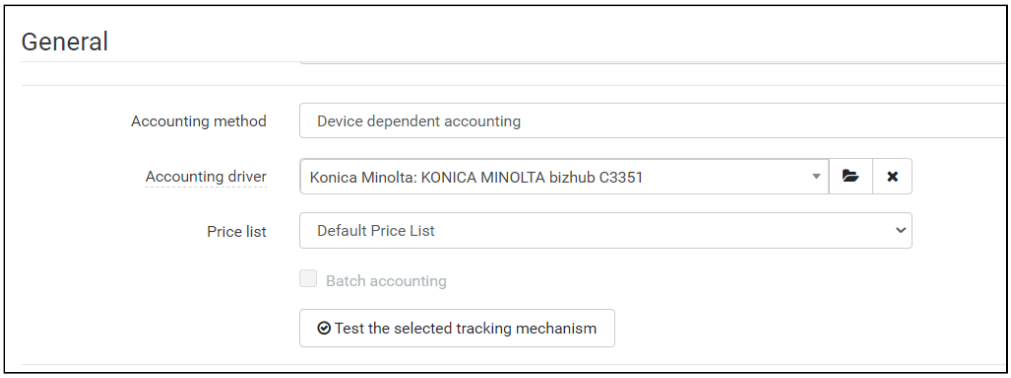
- You have either filled in the Default price list or you have created your own price list. See Price lists.
- If you don't wish to assign price list(s) to individual MFDs, assign the list(s) to individual users or cost centers. See Price lists.
- You have chosen which accounting method to use.

To enable accounting, perform the following steps:

1. Log in to the Dispatcher Paragon Cloud management interface.
2. Go to **Devices > Printers**. When adding a new MFD or editing an existing one, go to the **General** section. For more information on adding new devices, see Managing devices.
3. In **Accounting method**, select your chosen accounting method.
4. The **Accounting driver** selection:
   a. If you plan to use Counter reports in the Reports section of the Dispatcher Paragon Cloud management interface, select the corresponding accounting driver for your MFD.
   b. If you don't plan to use Counter reports, leave this field blank. Neither Offline accounting nor Device dependent accounting themselves need an Accounting driver in order for them to operate.

The **Accounting driver** field is only visible if you select **Embedded terminal** in **Terminal type** (Edge printing scenario).

5. In **Price list**, select the price list that you wish to assign to the MFD. If you have decided to assign price lists to individual cost centers or users, leave the Default price list in this field.



6. Click **SAVE CHANGES**.

Device dependent accounting

Device dependent accounting is completely dependent on MFDs. Dispatcher Paragon Cloud communicates with devices to obtain the accounting logs directly from them. Tracked information varies according to vendor and device, but may include the total number of impressions, the total number of BW/color impressions (three tiers, where supported), the total number of small (A5/A4/letter/legal) and large (A3/11 × 17/tabloid/ledger) pages and duplex usage. An impression is a copy, scan, or fax.

Unlike offline accounting, device dependent accounting tracks the number of pages that have actually been printed by an MFD, so if a user cancels a print job halfway through printing, or an MFD runs out of paper, the unprinted pages are not accounted for.

Limitations

Supported drivers:

- YSoft Universal Print Driver
- Vendor-provided PCL5
- Vendor-provided PCL6
- Vendor-provided PostScript

Offline accounting

When Offline accounting is enabled, the internal job parser in Dispatcher Paragon Cloud job parses each print job before printing. It tracks the number of A4/letter BW/color pages, A3/legal/tabloid BW/color pages, and duplex usage for all print jobs. It also tracks the per page print area coverage and estimated usage of CMYK toner cartridges.

Limitations

- The output from Offline accounting may differ slightly from the current output and information accounted by an MFD, since MFDs may use different processing algorithms. Each print job is always accounted for as a whole, even when only part of it has been printed (for example, if the user aborts printing on the MFD panel).
- Cannot provide a fully accurate report on all printed pages due to technology limitations. It doesn't take into account the status of the device and its actual output. Example: A color page printed on a BW printer is printed as BW but accounted for as a color page.
- The only supported driver is Vendor-provided PCL5.

2.6.4 MANAGING REPORTS

On the **Reports** tab, you can access the following:

- Job list – A list and audit log of all print, 3D print, copy and scan jobs tracked by Dispatcher Paragon Cloud.
- Web reports – A centralized interface for accessing cost and usage reports. See Web Reports.
- Counter reports – An interface for accessing reports from MFD counters (page meters). See Counter reports.
- Scheduled reports – An interface for scheduling regular delivery of reports by email. See Scheduled Reports.
- Terminal access – An audit log of all access attempts from Dispatcher Paragon Embedded Terminals (applicable only for Edge printing).

Management reports are disabled by default. If you need to enable them, please contact our customer support.

Web reports

Overview

The **Web reports** page is the main reporting engine for all statistical data processed in the Dispatcher Paragon Cloud environment. Here you can generate a variety of default reports and save them as custom reports.

> ⚠ Billing code reports are available only for MFDs connected to an edge device (Edge printing).

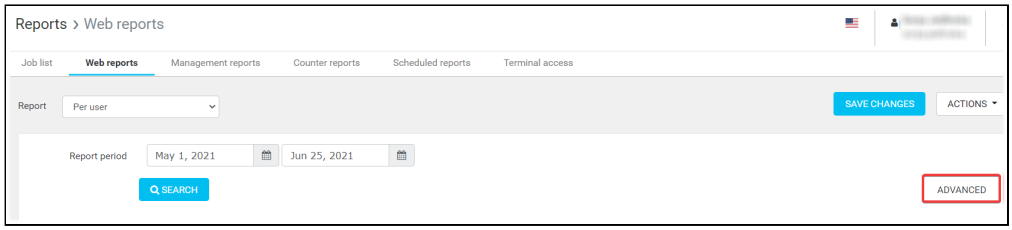
An end user can only access data for their own account. An administrator can see and modify data from all users.

Web reports consist of two kinds of statistical data:

- Basic statistics – these are created from detailed statistics by grouping similar jobs at one-hour intervals. Basic statistics preserve their general metadata (print/copy/scan, username, cost center, device and billing codes) but omit job-specific ones (job title, job origin, exact time).
- Detailed statistics – these contain details on each job accounted for by Dispatcher Paragon Cloud.

Accessing Web reports

1. Log in to the Dispatcher Paragon Cloud management interface.
2. Go to **Reports** > **Web reports**.
3. In the **Report** drop-down menu, select the type of report you wish to see.
   - **Standard** reports display summary data grouped by selected columns.
   - **Weekly averages** reports display averages for each hour of the day in a selected period.
4. In **Report period**, enter the start and end date of the report.
5. If you wish to include or exclude particular types of information from the report, click **Advanced** in the top right-hand corner of the screen. For more details, see the *Advanced filters* chapter in this document.



6. Click **Search** to display the report.

Working with reports

The report displays by default the total numbers for all counter types (**Total**, **B/W print**, **B/W copy**, **Color pages** and others). If you wish to see the numbers only for a particular counter type, click the tab with your required counter type at the top of the report.

Click **Actions** to perform the following actions:

- **Include latest processed data** – The report will be recalculated to include the latest processed data (data that has been saved in the database for more than one hour but has not been added to the report by the hourly executed statistics generator task).
- **Delete current custom filter** – Resets any filter options that you have selected.

For scheduling reports, see Scheduled reports.

Exporting reports

1. To export a report, click **Actions**.
2. Select the file format. The available formats are CSV, XLSX, PDF, HTML and XML.
3. The export starts immediately after clicking **Export to file <your selected file format>**.

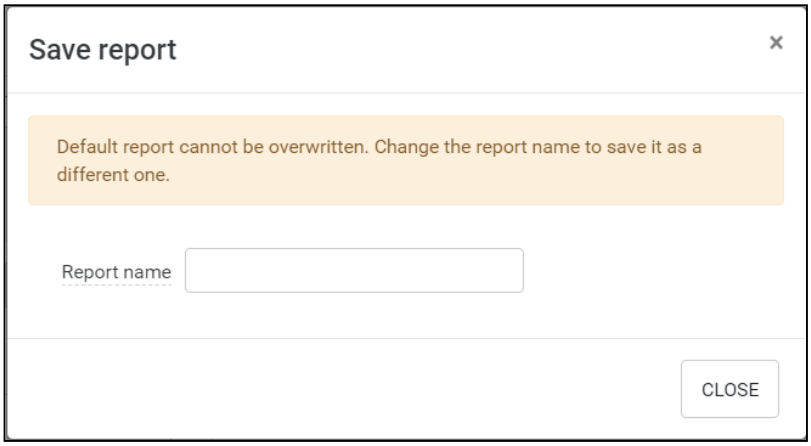
> You can set a limit for the number of exported rows in **System > Configuration > Reports**. Change the value of property **Export report maximum row count threshold**. There is no default limit.

Saving reports as custom reports

To save all the changes made in a web report (visible columns, the order of columns etc.), perform the following steps:

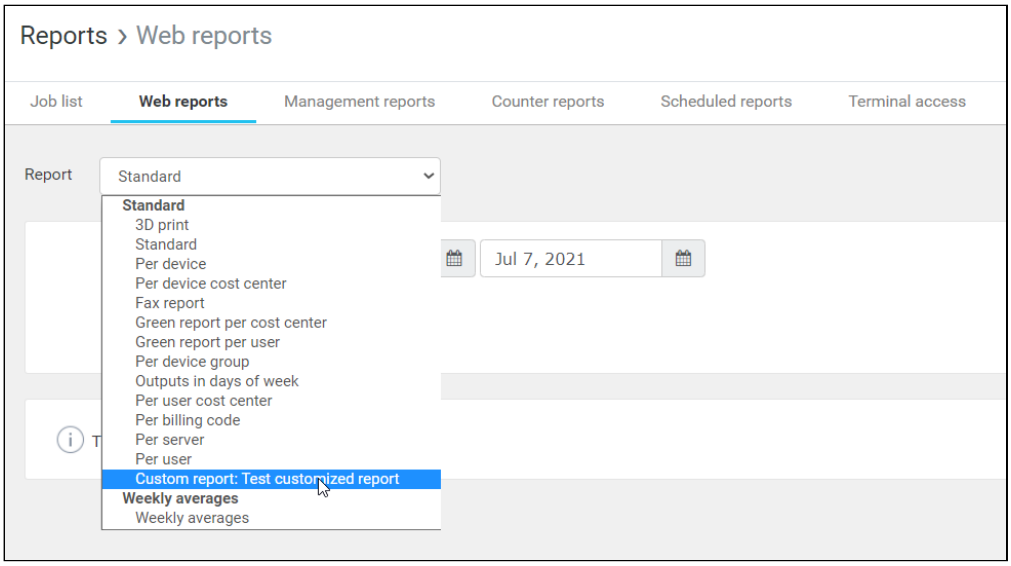
1. Click **Save changes** at the top of the page.

2. Enter a name for the new custom report.



3. Click **Save new report**.

4. From now on, the report will be listed in the **Report** drop-down menu.



Advanced filters

You can use three types of filter: **Limits**, **Columns** and **Counters**.

Limits

- **Limit to users** – Includes only data for the selected users.
- **Limit to user cost centers** – Includes only data for the selected users' cost centers.
- **Limit to device cost centers** – Includes only data for the selected devices' cost centers.
- **Limit to device** – Includes only data for the selected devices.
- **Limit to device group** – Includes only data for the selected device group.
- **Limit to billing code** – Includes only data for the selected billing codes.

The maximum number of entities that you can use in each filter type is 50.

Columns

1. Click **+Add column** to specify which columns should be present in the generated report.
2. Find the column name in the list and click it to add it to the report.
3. Click **Close** to close the dialog window.

- The following four columns with prefix *Costs* are present by default in *Green reports. Green reports* show the impact of printing on the environment. You can also however add these columns to any other report:
  - Costs – CO2 [kg]
  - Costs – energy [kWh]
  - Costs – trees
  - Costs – water [l]
- *Average coverage* is available only for jobs accounted under Offline accounting.

Counters

In the **Counters** list, select the counters that you wish to include in your report.

The report will also include a counters overview. To change the order of counters in this overview, use the associated arrow icons.

Special counters

- *Purge print* counters show the number of pages that were sent to Dispatcher Paragon Cloud but were not printed, e.g. deleted at the terminal, in the Dispatcher Paragon Cloud management interface or automatically by the system.
- Counters in italics are summary counters that display the sum of several other counters. For example, the *B/W pages* counter represents the sum of all counters for specific types of black and white pages (print, copy, both page sizes).
- *ABS [mm]* and *PLA [mm]* counters relate to 3D printing. They are used to report how much of the aforementioned material has been used during the reporting period. The value of these counters is reported in millimeters of used material length.

Counter reports

This part of documentation applies to Edge printing only.

You can configure Dispatcher Paragon Cloud to monitor MFD counters (also known as page meters). The counter reports are intended for admins who want to verify that Dispatcher Paragon Cloud accounting works correctly in comparison to device counters.

- Counter reports are available only for devices that have an Accounting driver assigned. For more information, see Accounting.
- Dispatcher Paragon Cloud keeps counters in the main database only for a given period of time – 30 days by default.

Accessing counter reports

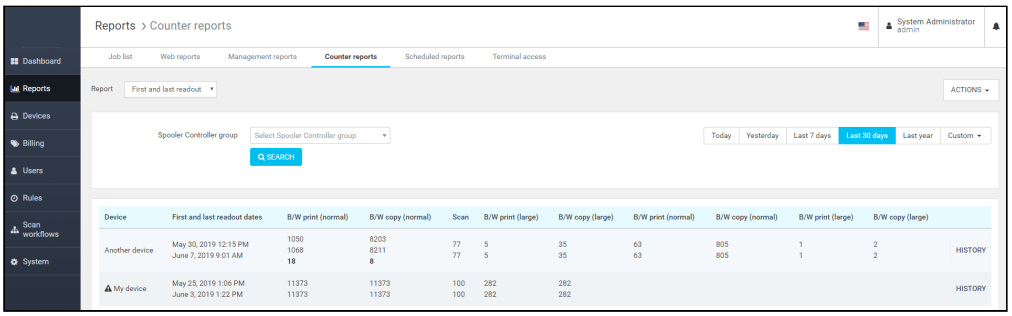
1. Log in to the Dispatcher Paragon Cloud management interface.
2. Go to **Reports** > **Counter reports**.
3. In the **Report** drop-down menu, select the type of report you wish to see.
4. If you wish to see only the reports for a particular Spooler Controller group, select the group in the **Spooler Controller group** drop-down menu.
5. Select the time period.
6. Click **Search**.

Counter report types

First and last readout report

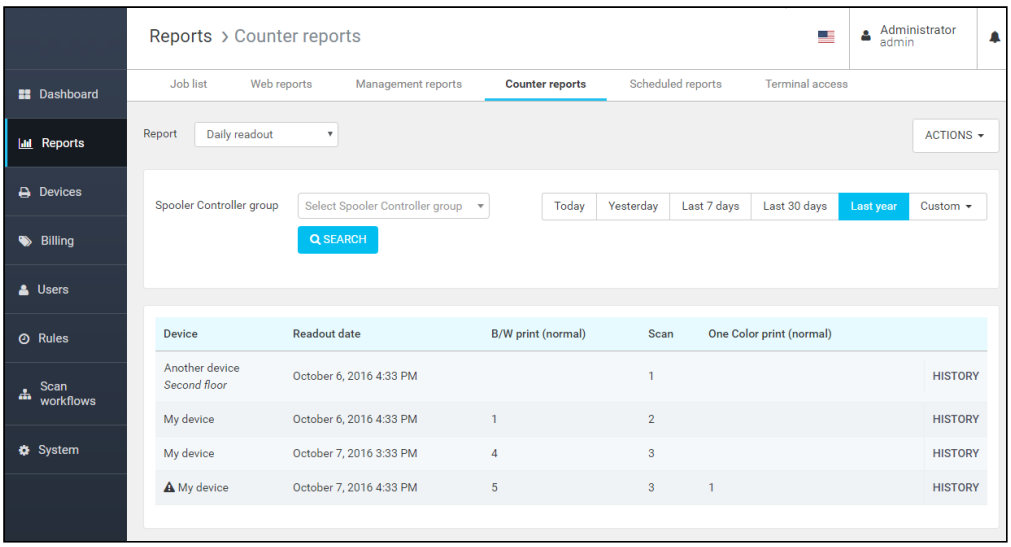
The First and last readout report displays the counter information for each device for the first and the last readout in the given time period, and the difference between the two readouts. The difference is written in bold.

The report is sorted by device name and shows one record for each monitored device in the selected period. You can find the exact times of the readouts in the **Readout date** column.



Daily readout report

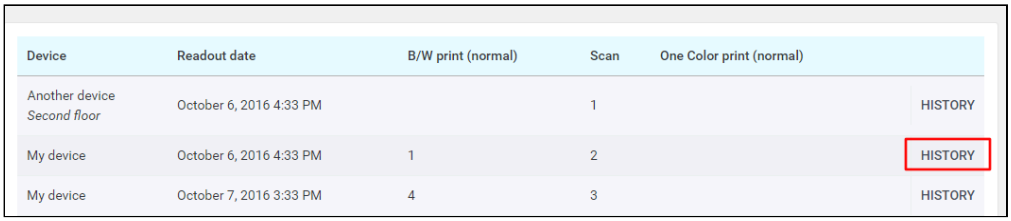
The daily readout report displays the readouts for each device for each day in the given time period.



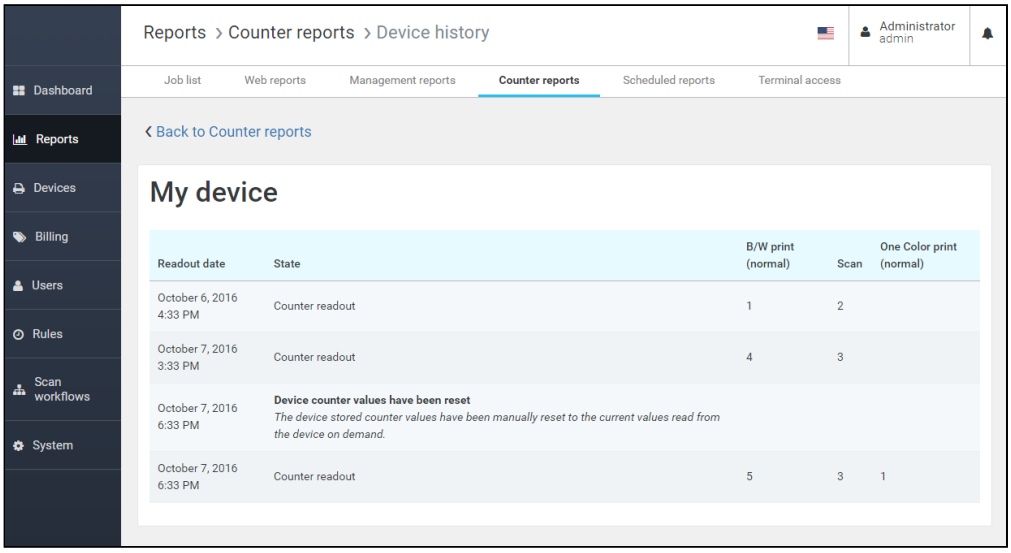
Device history

You can access the device history from both types of reports. Device history displays all the readouts for a given device stored in the main database, information about the accounting setting changes, and information about counter value resets.

1. To see the device history, click **HISTORY** next to the device.



2. The resulting report looks like this:



Exporting counter reports

1. To export your selected counter report, click **Actions**.
2. In the drop-down menu, choose a format and click **Export report to file (<your selected format>)**. The available formats are HTML, XML, XLSX, CSV and PDF.

Scheduled reports

In the **Scheduled reports** section, you can create **Web reports** and **Counter reports** to be delivered by email at regular intervals.

Scheduling Web reports to an email

To schedule a new Web report, perform the following steps:

1. In Dispatcher Paragon Cloud management interface, go to **Reports > Scheduled reports**.
2. Click **+ SCHEDULE NEW REPORT**.
3. Select **Schedule a Web report to an email** from the drop-down menu.
4. Enter the report name.
5. Select the format. The available formats are CSV, HTML, PDF, XLSX, XML.
6. Select the interval. The interval determines how often and for which period the report will be exported:
   - Previous day – The report will be created daily. The report will include data for the previous day.
   - Previous 7 days – The report will be created weekly. The report will include data for the previous 7 days.
   - Calendar month – The report will be created monthly on a selected day of the month. The report will include data starting from the selected day of the previous month until (but not including) the same day of the current month.
   - Monthly – The report will be created monthly on a selected day of the month. The report will include data from the first to the last day (included) of the previous month.
7. In the **Exported reports** section, click **+ Add report** to select the type of report you wish to include in your scheduled report. If you need more than one type of report, repeat this step. For more information on report types, see Web reports.
8. In the **Recipients** section, click **+ Add recipient**. Enter the recipient's email address. If you need to add more than one recipient, repeat this step.
9. Click **SAVE CHANGES**.

Scheduling Counter reports to an email

> ⚠ Counter reports are available only for devices that are configured for the Edge printing scenario and have an Accounting driver assigned. For more information, see Accounting.

To schedule a new Counter report, perform the following steps:

1. In Dispatcher Paragon Cloud management interface, go to **Reports > Scheduled reports**.
2. Click **+ SCHEDULE NEW REPORT**.
3. Select **Schedule a Counter report to an email address** from the drop-down menu.
4. In **Schedule name**, enter the new report name.
5. Select the report format. The available formats are CSV, HTML, PDF, XLSX, and XML.
6. Select the **Sending interval**. This is an interval that determines how often and for which period the report will be exported:
   - Previous week – The report will be created weekly. The report will include data for the previous (entire) week and will be sent on the first day of the next week immediately after midnight. The first day of the week is determined based on the server locale.
   - Previous month – The report will be created monthly. The report will include data for the previous (entire) month and will be sent on the first day of the next month immediately after midnight.
7. Select the **Report type**. The available values are the **Daily readout,** and **First and last readout**.

   > ⓘ The **Daily readout** report displays the readouts for each device for each day in the given time period.
   >
   > The **First and last day readout** report displays the counter information for each device for the first and the last readout in the given time period, and the difference between the two readouts.
8. Alternatively, you can limit the report to a particular Spooler Controller group.
9. In the **Recipients** section, enter the recipient's email address. When you start typing, an input field for another recipient will appear below the first one.
10. Click **SAVE CHANGES**.

Editing and deleting scheduled reports.

Go to **Reports > Scheduled reports** to see the list of all the reports you have created.

To delete a report, click the trash bin icon in the report row and confirm your action.

To edit a report, click the settings icon in the report row.

2.6.5 MANAGING BILLING CODES

> In the Pure Cloud printing scenario, users cannot select billing codes at the terminal since this is not supported by the Dispatcher Paragon Cloud Terminal.
>
> In the Edge printing scenario, users can select billing codes at the terminal (see Dispatcher Paragon Embedded Terminal for Konica Minolta).

About billing codes

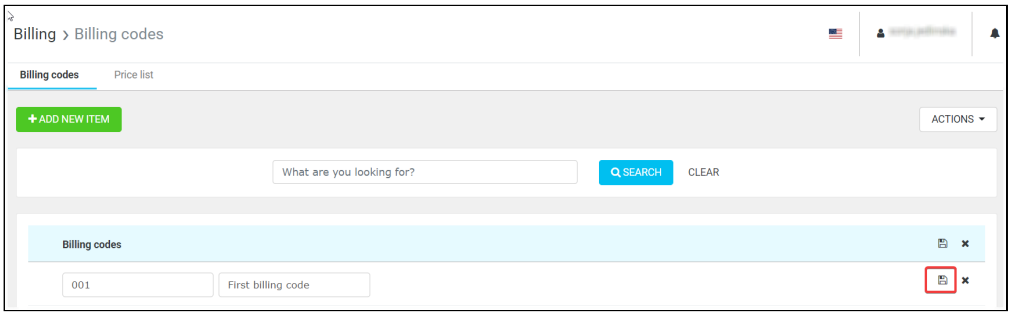
In this section of the Dispatcher Paragon Cloud management interface, you can manage billing codes (also called project codes), their structure and their assignment to individual users, roles or cost centers.

Accessing billing codes

1. Log into the Dispatcher Paragon Cloud management interface with an account that has the Customer admin system role.
2. In the main menu on the left-hand side of the screen, select **Billing**. The **Billing** section will be displayed.

Adding new billing codes

1. To add a new billing code, click the **+ADD NEW ITEM**.
2. Enter the code of the new billing code.
3. Enter the description of the new billing code.
4. Click the save icon.



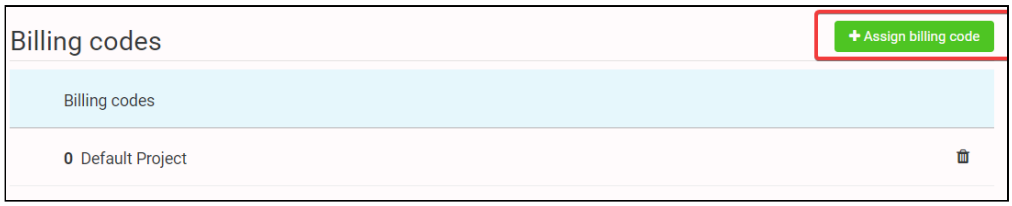
Assigning billing codes

You can assign billing codes to users, roles or cost centers. Users inherit billing codes from roles and cost centers. If you do not assign a specific billing code to a user, the user inherits the default billing code from a role or cost center.

If a user only has one billing code assigned or inherited, this billing code is automatically the default code. In this case, the device does not display a billing code selection, but automatically uses the default billing code (regardless of whether it's the Pure Cloud printing scenario or Edge printing scenario).

Assigning billing codes to users

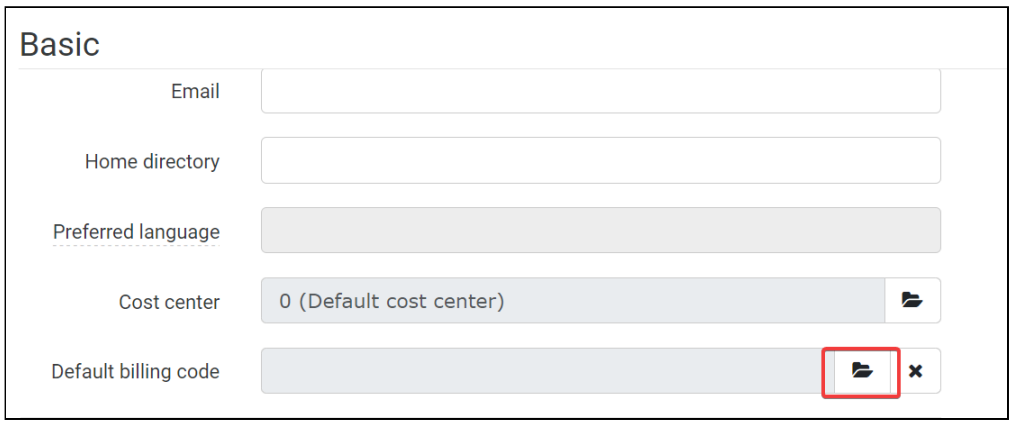
1. Log into the Dispatcher Paragon Cloud management interface with an account that has the Customer admin system role.
2. In the main menu on the left-hand side of the screen, select **Users**. The **Users** tab will be displayed.
3. Click the **Edit user** icon  next to the user whom you wish to edit.
4. In the Billing codes section, click **+Assign billing code**.



5. Find the billing code in the list of available billing codes and click it.
6. Close the dialog window.
7. Click **SAVE CHANGES** to save the changes that you made in the user detail.

Assigning default billing codes to users

1. When editing a user, click the folder icon in the **Default billing code** field to display the list of billing codes available to the user.



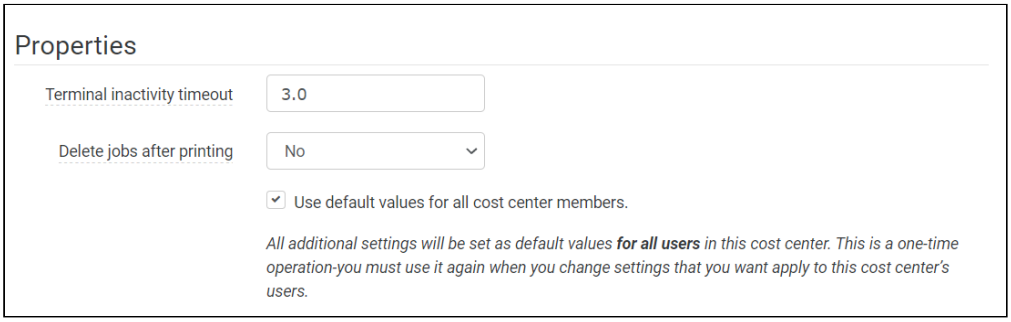
2. Find the billing code in the list of billing codes and click it.

> This list includes billing codes assigned to users, cost centers and roles. Once you have selected a **specific** default billing code for the user, that billing code overrides the cost center's default billing code.

3. Click **SAVE CHANGES** to save the changes that you made in the user detail.

Assigning a cost center's default billing code to all members of the cost center:

When you change the cost center's default billing code, check the option **Use default values for all cost center members**. This causes specific default billing codes set for users to be deleted from user settings and the users' default billing codes to be inherited from the current cost center.



Assigning billing codes to cost centers

1. Log into the Dispatcher Paragon Cloud management interface with an account that has the Customer admin system role.
2. In the main menu on the left-hand side of the screen, select **Users**.
3. Click the **Cost centers** tab.
4. Click the edit icon next to your selected cost center.

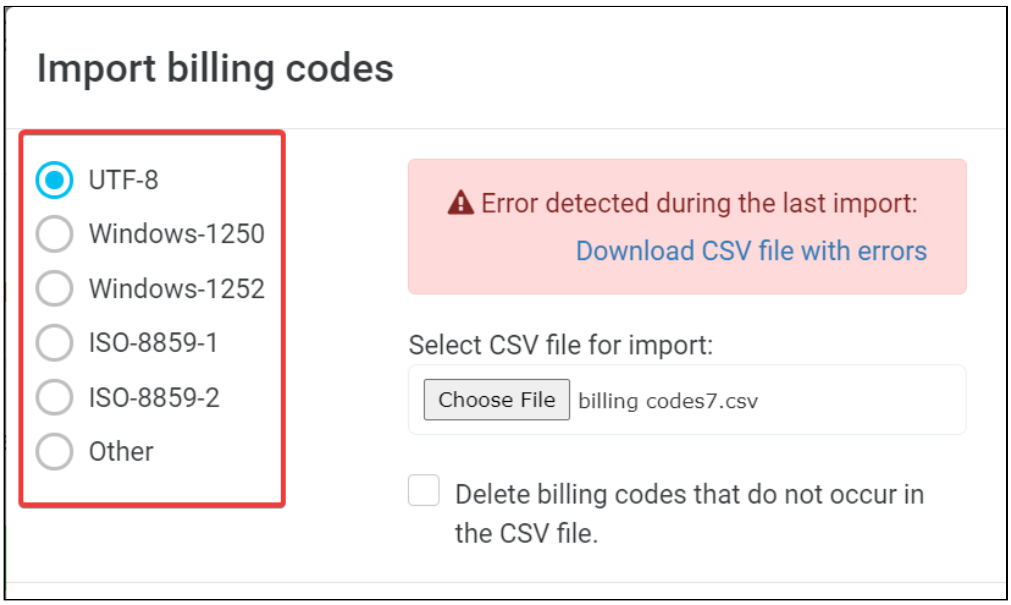
5. In the Billing codes section, click **+Assign billing code**.
6. Find the billing code in the list of available billing codes and click it.
7. Close the dialog window.

Importing billing codes from a CSV file

1. Prepare a file according to Billing codes import - CSV format specifications
2. In the Dispatcher Paragon Cloud management interface, go to **Billing > Billing codes**.
3. Click **Actions > Import billing codes**.
4. Select the format.
5. Select the CSV file for import.
6. As an option, check the **Delete codes that do not occur in the CSV file** checkbox.
7. Click **IMPORT DATA**.
8. When the import begins, you will see a progress bar. When the import is complete, you will see a confirmation message.

Troubleshooting an import from a CSV file

1. If a problem has occurred during import, you will see a message **Error detected during the last import**. To download a CSV file that includes descriptions of the errors, click **Download CSV file with errors**.
2. Make sure that the encoding of your file is the same as the encoding that you selected in the import dialog window:



3. Make sure that there are no hidden special characters in your csv file.

Billing codes import - CSV format specifications

The Dispatcher Paragon Cloud management interface supports the batch import of billing codes from a CSV file. The file must fulfill the requirements described on this page.

We recommend using a maximum of 1 000 billing codes per one level (without technical limitations on the number of nested levels).

CSV Format

Billing codes must be stored in a CSV file.

Delimiter: semicolon **;**

Quote character (if necessary): double quote **"**

Importer configuration

You can modify the behavior of the importer by configuring the first row.

Format selection

You can use two formats for importing. The format must be specified in the first line of the first column.

Available formats: *prefix*, *parent*

Format specification string: *format:parent*

Level delimiter

When you use the prefix format, you can change the default level delimiter from default '.' to another single character.

Delimiter specification string: *levelDelimiter:/*

The default prefix importer will read *1.2.3.* When you change *leverlDelimiter* to `/,` it will read the data in the format *1/2/3*.

Supported Formats

Format:prefix

1. Billing code in the tree format – mandatory; String – e.g.: 1.2.14 – the parent is, in this case, 1.2 and the billing code for this item is 14.
2. Billing code description – mandatory; String – e.g.: Primary code.

3. Extension string. From the third position, you can specify extension strings. Each column must contain only one extension. Extensions are applied from the first record, from left to right.

Format:parent

The record contains the following columns:

1. Billing code – mandatory; String – e.g.: 100, 200, 1.1.1.
2. Billing code description – mandatory; String – e.g.: Primary code.
3. Parent billing code (first-level billing code) – optional; String – e.g.: 100, can be empty.
4. Extension string. From the fourth position, you can specify extension strings. Each column must contain only one extension. Extensions are applied from the first record, from left to right.

A parent billing code (first-level billing code) is optional. When unspecified, the billing code is considered to come directly under the root element.

The uniqueness of a billing code is defined by its path. The same billing codes can appear under different parents.

Extension string

Format: *extension_name:value*

Permitted extensions: *user, center, role, action*

The extension string is case insensitive.

Extension *user*

This extension contains a user login name. The billing code, with its entire subtree, will be assigned to the specified user. The user must already exist in the management interface, or else the billing codes will be imported without being assigned to the specified user.

If a user account with the specified name does not exist, the system tries instead to find a role with the name.

Example: *user:george*

Extension *center*

This extension contains a cost center number. The billing code, with its entire subtree, will be assigned to the specified cost center. The cost center must already exist in the management interface, or else the billing codes will be imported without being assigned to the specified cost center.

Example: *center:118999881*

Extension *role*

This extension contains a role name. The billing code, with its entire subtree, will be assigned to the specified role. The role must already exist in the management interface, or else the billing codes will be imported without being assigned to the specified role.

Example: *role:everyone*

Extension *action*

Available actions:

- *remove* – deletes the billing code and its entire subtree
- *resetACL* – deletes the user, cost center, and role assignments (i.e., the Access Control List) of the billing code

Example: *action:remove*

Removing assignments

To remove a billing code assignment from a specific user, cost center, or role, prefix the username, cost center number, or role name with a minus sign.

Example: *user:-george;center:-1234;role:-everyone;user:newuser*

Alternatively, you can remove all existing assignments and add new ones:

Example: *action:resetACL;user:newuser*

Note that if a username, cost center number, or role name starts with a minus sign or a plus sign and you need to assign a billing code to it, you must prefix it with a plus sign.

An example of adding assignments to a user "*-minususer*", cost center "*-1*" and role "*-minusrole*":

user:+-minususer;center:+-1;role:+-minusrole

An example of removing assignments from user "*-minususer*", cost center "*-1*" and role "*-minusrole*":

user:--minususer;center:--1;role:--minusrole

Guidelines for working with a large volume of billing codes

If you need to process a large volume of billing codes, follow these guidelines:

1. To assign a large volume of billing codes, group them under one parent and assign this parent only.
2. To assign the same set of billing codes to a large number of users, create a role and assign billing codes to the role according to guideline 1.
3. Perform as few deletions as possible. Billing codes still remain in the database even after deletion.
4. Do not create more than 1 000 children at the first level of a billing code tree. Divide billing codes into groups.

Sample CSV data

Format:prefix

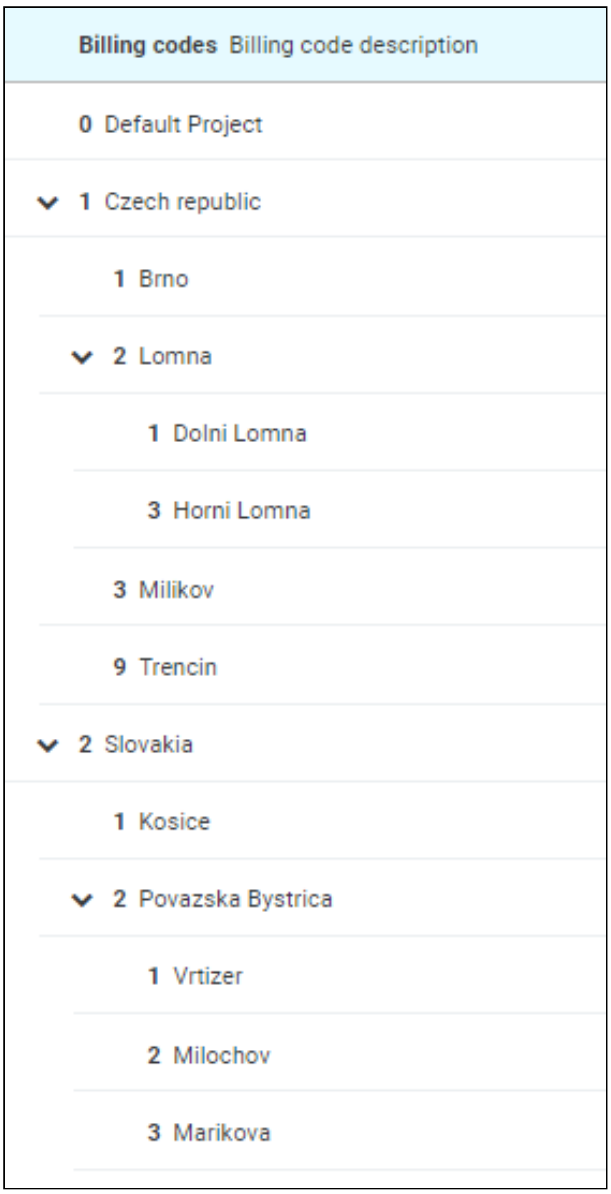
Contents of the CSV file:

```
format:prefix
1;Czech republic;user:barbora;user:richard;
1.1;Brno;
1.2;Lomna;
1.2.1;Dolni Lomna;
1.2.3;Horni Lomna;
1.3;Milikov;
2;Slovakia;center:118999881;
2.1;Kosice;
2.2;Povazska Bystrica;
2.2.1;Vrtizer;
2.2.2;Milochov;
1.9;Trencin;
2.2.3;Marikova;
```

Sample in MS Excel:

	A	B	C	D
1	format:prefix			
2	1	Czech republic	user:barbora	user:richard
3	1.1	Brno		
4	1.2	Lomna		
5	1.2.1	Dolni Lomna		
6	1.2.3	Horni Lomna		
7	1.3	Milikov		
8	2	Slovakia	center:118999881	
9	2.1	Kosice		
10	2.2	Povazska Bystrica		
11	2.2.1	Vrtizer		
12	2.2.2	Milochov		
13	1.9	Trencin		
14	2.2.3	Marikova		

The result in the Dispatcher Paragon Cloud management interface:



Format:prefix with level delimiter /

Contents of the CSV file:

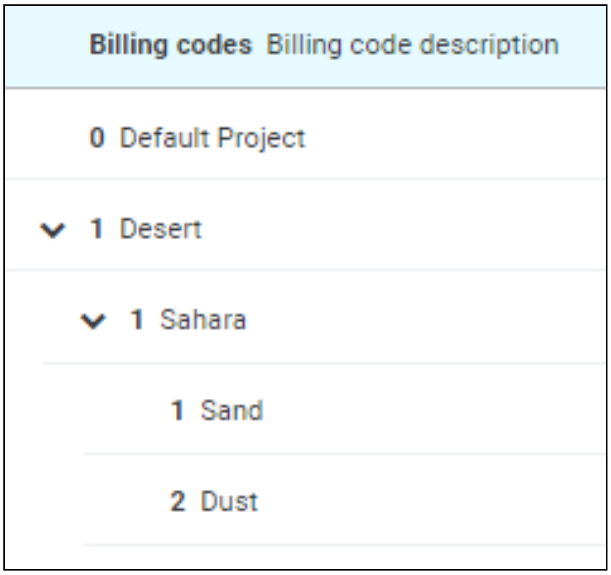
```
format:prefix;levelDelimiter:/
1;Czech republic;user:barbora;user:richard;
1/1;Brno;
1/2;Lomna;
1/2/1;Dolni Lomna;
1/2/3;Horni Lomna;
1/3;Milikov;
```

Remove and insert new

Contents of the CSV file:

```
format:prefix
1;Large forest;;action:remove;
1;Desert;;
1.1;Sahara;;user:georgik;118999881;user:arnost;
1.1.1;Sand;
1.1.2;Dust;
```

The result in the Dispatcher Paragon Cloud management interface:



Format:parent

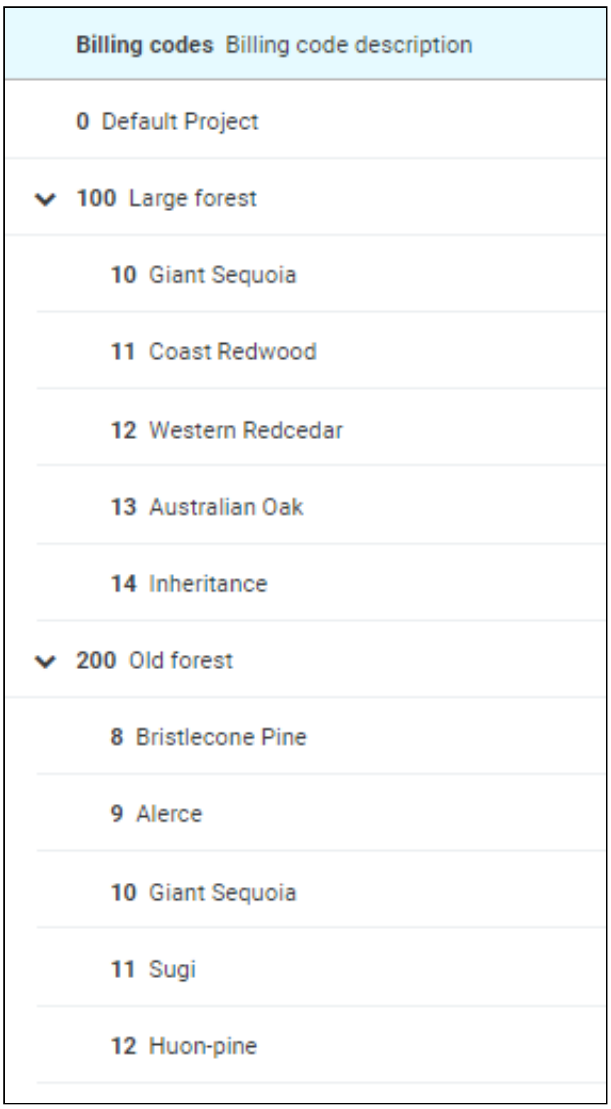
Contents of the CSV file:

```
format:parent
100;Large forest;;center:118999881;
10;Giant Sequoia;100;user:mary;user:james;
11;Coast Redwood;100;
12;Western Redcedar;100;
13;Australian Oak;100;
14;Inheritance;100;center:118999881;
200;Old forest;
8;Bristlecone Pine;200;
9;Alerce;200;
10;Giant Sequoia;200;
11;Sugi;200;
12;Huon-pine;200;
```

Sample in MS Excel:

	A	B	C	D	E
1	format:parent				
2	100	Large forest		center:118999881	
3	10	Giant Sequoia	100	user:mary	user:james
4	11	Coast Redwood	100		
5	12	Western Redcedar	100		
6	13	Australian Oak	100		
7	14	Inheritance	100	center:118999881	
8	200	Old forest			
9	8	Bristlecone Pine	200		
10	9	Alerce	200		
11	10	Giant Sequoia	200		
12	11	Sugi	200		
13	12	Huon-pine	200		

The result in the Dispatcher Paragon Cloud management interface:



Special characters

You can use LibreOffice Calc to generate a proper CSV file in UTF-8 from an Excel table. Use a semicolon as the field delimiter and no character as the text delimiter.

Contents of the CSV file:

```
format:prefix;levelDelimiter:*
1;Tiskárna;
1*1;Принтер;
1*1*1;プリンター;
2;打印机;
2*1;პრინტერი;
2*2;tölvufræði;
```

Sample in MS Excel:

1	format:prefix	levelDelimiter:*
2	1	Tiskárna
3	1*1	Принтер
4	1*1*1	プリンター
5	2	打印机
6	2*1	პრინტერი
7	2*2	tölvufræði

The result in the Dispatcher Paragon Cloud management interface:

Recommendations

- Use a maximum of 1 000 sub-levels per first-level.
- Use a maximum of 100 000 lines per CSV file.

Limitations

- The maximum for one import procedure: 1 000 sub-levels per first-level.
- CSV file size: maximum of 3MB.
- Restricted characters: `?&'"<>`
- If you need to enter the backslash character ' `\` ' you must escape it. Type ' `\\` '.

Price lists

In Dispatcher Paragon Cloud, you can define the price of various operations. You can create multiple price lists and assign them to individual users, cost centers or devices. A single price list can be assigned to multiple users, cost centers or devices. Therefore, in a homogeneous environment, where all devices run at the same cost, you can create only one price list and assign it easily to all devices, users or cost centers.

Price lists assigned to individual users have the highest priority. If no price list is defined for a user, the cost center price list is used. If no price list is defined for a cost center, the device price list is used.

> ⚠ If you enable accounting for a device and you do not specify any other price list for the device, the device configuration will be saved with the default price list.

Creating a price list

1. Log in to the Dispatcher Paragon Cloud management interface.
2. Go to **Billing** > **Price list**.
3. Click **+NEW PRICE LIST**.
4. Enter values for all the operations for which you wish to define a price.

   > ⚠ If the entered value has more than two decimal places, you won't be able to save the price list.

5. Click **SAVE CHANGES**.

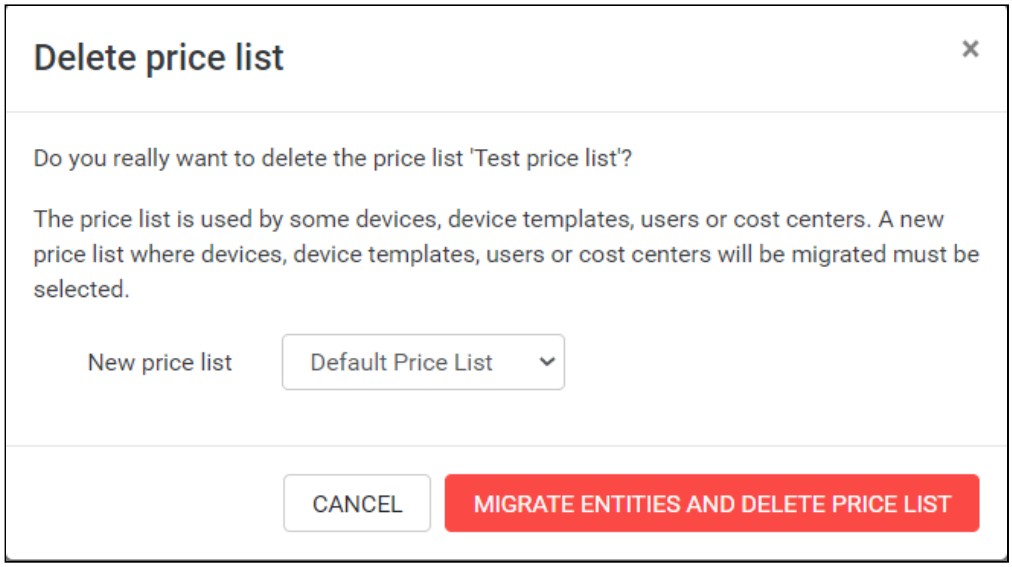
Editing a price list

1. In the Dispatcher Paragon Cloud management interface, go to **Billing** > **Price list**.
2. Click **EDIT** next to the price list you wish to modify.
3. Make your changes.
4. Click **SAVE CHANGES**.

Deleting a price list

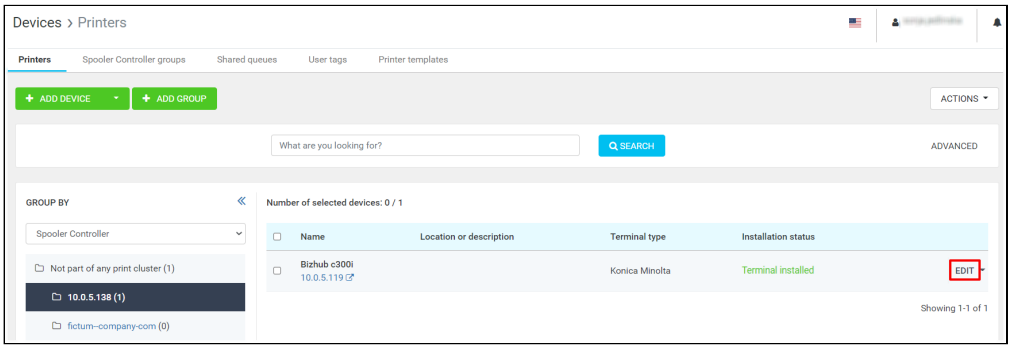
1. In the Dispatcher Paragon Cloud management interface, go to **Billing** > **Price list**.
2. To delete a price list, open the dropdown menu for the respective price list and click **Delete**.

3. If the price list is assigned to any user, cost center or device, the system will ask you to choose a new price list.

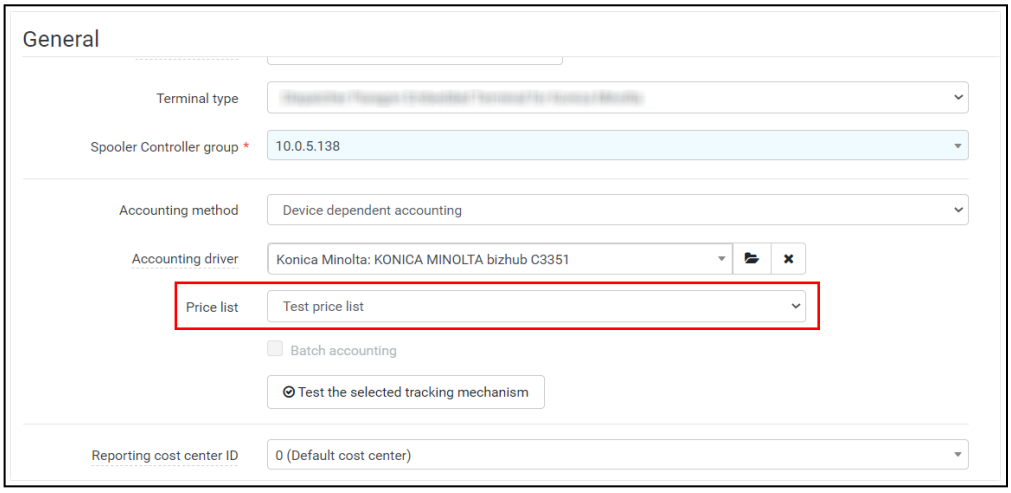


Assigning a price list to a device

1. If not done already, create your price list as described in the *Creating a price lis*t section of this document.
2. If you wish to assign the price list during the process of adding a new MFD, follow the steps in Managing devices.
3. If the MFD is already registered/installed in Dispatcher Paragon Cloud, assign the price list by editing the device:
   a. In the Dispatcher Paragon Cloud management interface, go to **Devices** and click **EDIT** next to the respective device.



b. Select the price list.

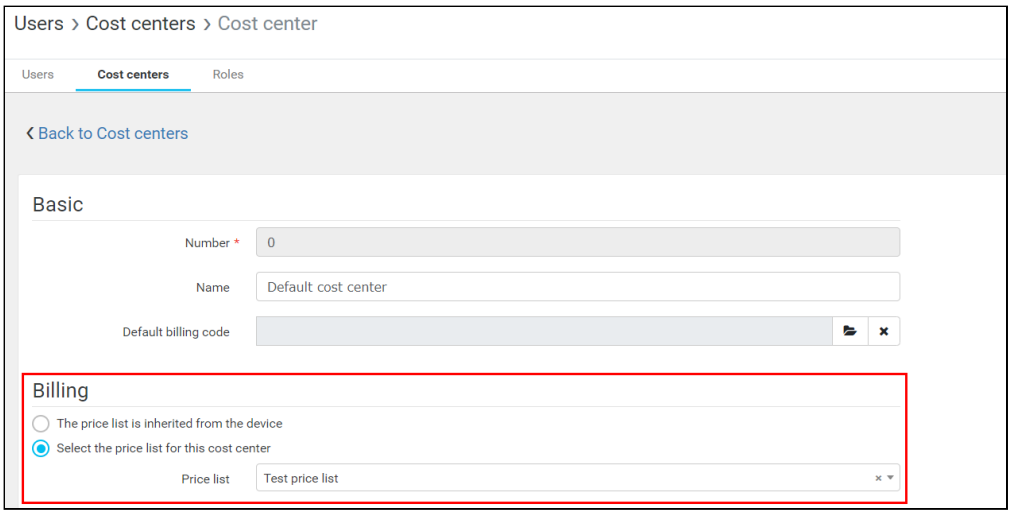


c. Click **SAVE CHANGES**.

Assigning a price list to a cost center

By default, price lists are inherited from device settings. If you wish to assign a price list to the entire cost center, perform the following steps:

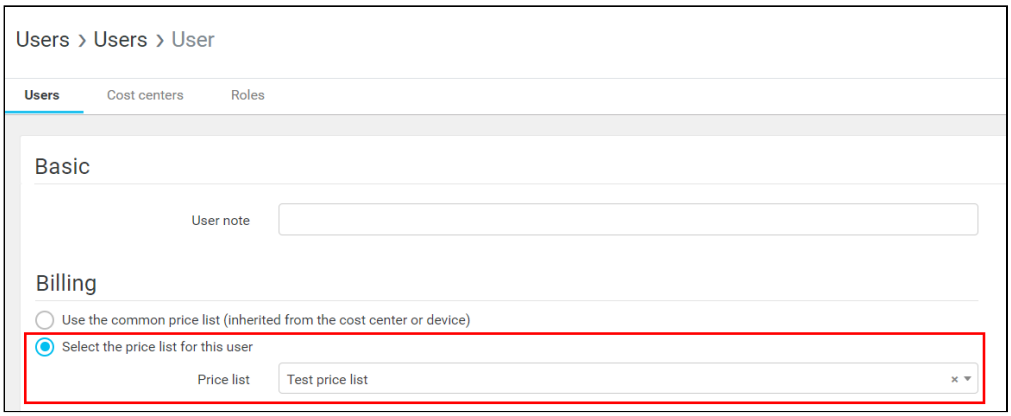
1. If not done already, create your price list as described in the *Creating a price lis*t section of this document.
2. In the Dispatcher Paragon Cloud management interface, go to **Users** > **Cost centers**.
3. Click the edit icon next to the cost center where you wish to add the price list.
4. In the **Billing** section, select **Select the price list for this cost center**.
5. Select the price list in the dropdown menu.



6. Click **SAVE CHANGES**.

Assigning a price list to a user

1. If not done already, create your price list as described in the *Creating a price lis*t section of this document.
2. In the Dispatcher Paragon Cloud management interface, go to **Users** > **Users**.
3. Click the edit icon next to the user to whom you wish to assign the price list.
4. In the **Billing** section, select **Select the price list for this user**.
5. Select the price list in the dropdown menu.



6. Click **SAVE CHANGES**.

Price calculations

The total prices are calculated based on these formulas:

Operation	Price
Scanning	Scan cost × number of scanned pages
Copying and printing	(Cost per click × number of printed pages) + (paper cost × number of used papers) + (page cost × number of printed pages)
Incoming fax	(Cost per click × number of printed pages) + (paper cost × number of used papers) + (fax page cost × number of printed pages)
Outgoing fax	Outgoing fax cost

Price calculation examples

Operation	Price
Print of 1 × A4 page in BW simplex mode	(Cost per click × 1 page) + (paper cost × 1 paper) + (BW page cost × 1 page)
Print of 2 × A4 page in color duplex mode	(Cost per click × 2 pages) + (paper cost × 1 paper) + (color page cost × 2 pages)
Copy of 1 × A4 page in BW simplex mode	(Cost per click × 1 page) + (paper cost × 1 paper) + (BW page cost × 1 page)
Copy of 1 × A4 page in color duplex mode	(Cost per click × 2 pages) + (paper cost × 1 paper) + (color page cost × 2 pages)
Scan of 2 × A4 page in BW simplex mode	Scan cost × 2 pages

2.6.6 MANAGING RULES AND ACCESS DEFINITIONS

In the **Rules** section of Dispatcher Paragon Cloud management interface, you can access the following:

- Rules – create various conditions for processing of your company's print jobs.
- Access definitions – define which user roles can perform which operations (for example, printing) on which devices.

Rules

Rule-Based Engine overview

The Rule-Based Engine maximizes the efficiency of MFDs and other networked printers and helps reduce costs and the workload of administrators and IT staff.

The efficiency of your organization’s print environment depends on three factors:

- Printers – Rule-based printing gives you, for example, the ability to automatically convert specific print jobs to B/W or duplex printing, or to automatically redirect large color print jobs to more efficient MFDs.
- People – From the end user‘s perspective, print jobs can be automatically redirected to, for example, a smaller printer closer to the user's desk. Rules also make it possible for end users to receive notifications about their print jobs.

- Processes – Rules allow administrators to automatically control access to printer functions and to align print environment operations with an organization's processes and financial strategy. For example, administrators can prevent large jobs from being printed or redirect them to the most cost-efficient printer.

How rules work

Each rule consists of three main components: trigger, condition, and action. A rule may also include a fourth (optional) component: notification.

1. Trigger – The point in the print process that triggers the rule evaluation.

   Triggers available for Pure Cloud printing:
   - On reception of job by Dispatcher Paragon server
   - On job status change.

   Triggers available for Edge printing:
   - On reception of job by Dispatcher Paragon server
   - Before job is released to the printer
   - On job's delivery to the printer
   - On user login at terminal
   - On user's logout at terminal
   - On job status change

2. Condition – Once the rule is triggered, all conditions are evaluated to determine whether the action should be performed or not. When multiple conditions are defined for a specific rule, all of them must be met for the action to be performed. When conditions are combined as OR and not as AND, more rules can be set and these are evaluated according to their order.

   Types of conditions:
   - User management conditions – You can set rules for specific users, groups, departments, or roles.
   - Printers – In case of Edge printing, Dispatcher Paragon Cloud can execute a rule if a job is sent to a specific printer or type of printer.
   - Print job specifics – Typically, the administrator sets a rule for specific job titles using regular expressions. This condition can apply to jobs printed from a specific application or to specific file formats (by defining the suffix, such as TIFF image files). Rules can also be applied to jobs based on queue name or queue type. Furthermore, you can use as conditions: tags, size of the job, status,

number of pages, size of pages, or total number of pages printed within a specified timeframe.

- Time of printing – Dispatcher Paragon Cloud can execute rules based on time or day. For example, you can create a rule that restricts printing on weekends or after normal working hours.

3. Action – Action is the part of a rule that defines what Dispatcher Paragon Cloud does after the rule is triggered and the condition is met.

   The action that has the biggest impact on cost savings is forced double-sided printing. Based on a rule's conditions, you can specify which documents must be printed double-sided by default. Another action that results in cost savings is a conversion of color prints to grayscale.

   Furthermore, you can use rules to automatically add a watermark to confidential documents, or print a predefined set of copies for specific types of jobs, thus saving employees' time, or to automatically delete a print job if a prohibited action is detected – for example, if a print job contains a file in a specific format.

4. Notification – For each rule, you can set a notification to be sent to the print job's owner and/or others. Notifications inform the users about the status of their print jobs and how the application of a rule may have affected their print jobs.

Creating and editing rules

On the **Rules** tab, you can see the list of existing rules in the system.

Each rule displays the following information:

- Name – The name of the rule.
- Trigger – The action that will trigger the rule.
- Conditions – The conditions print jobs must meet in order for Dispatcher Paragon Cloud to apply the rule.
- Action – The action that will be applied if conditions are met.

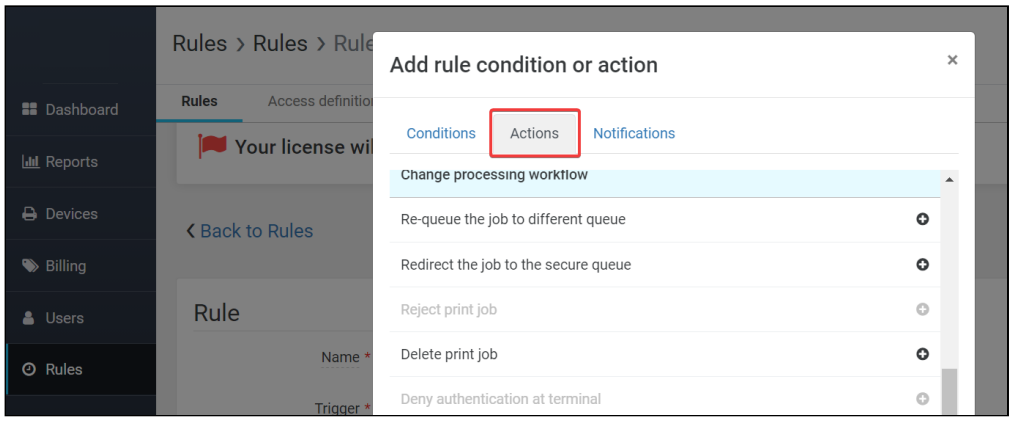
For each rule, you can perform the following actions:

- Enable/disable the rule
- Move the rule up or down in the list
- Edit the rule definition
- Delete the rule

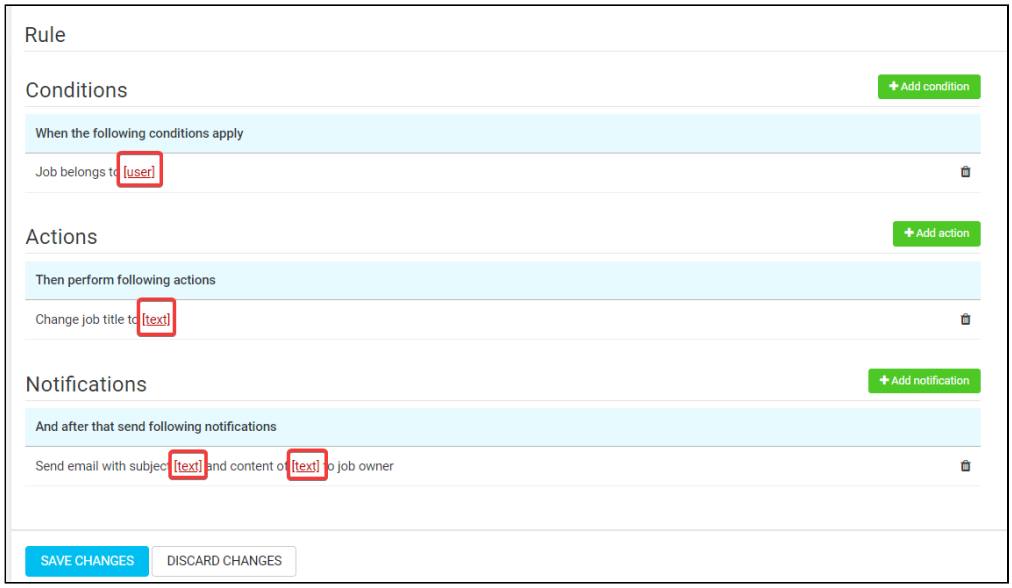
Creating a new rule

1. To create a new rule, click **+ ADD NEW ITEM.**

2. Enter the rule name.
3. In the **Trigger** drop-down menu, select the trigger.
4. Click **+ Add condition** to specify the job conditions.
5. Click the **+** icon next to the condition you wish to add.
6. Click the **Actions** tab.



7. On the **Actions** tab, click the **+** icon next to the action you wish to add.
8. If you wish to add notifications, click the **Notifications** tab.
9. On the **Notifications** tab, click the **+** icon next to the notification you wish to add.
10. Click **CLOSE** to close the dialog window.
11. Define the content of each of your conditions, actions, and notifications by clicking the variables marked in red. Example:



12. Click **SAVE CHANGES** to save your new rule.

13. The rule will become active automatically.

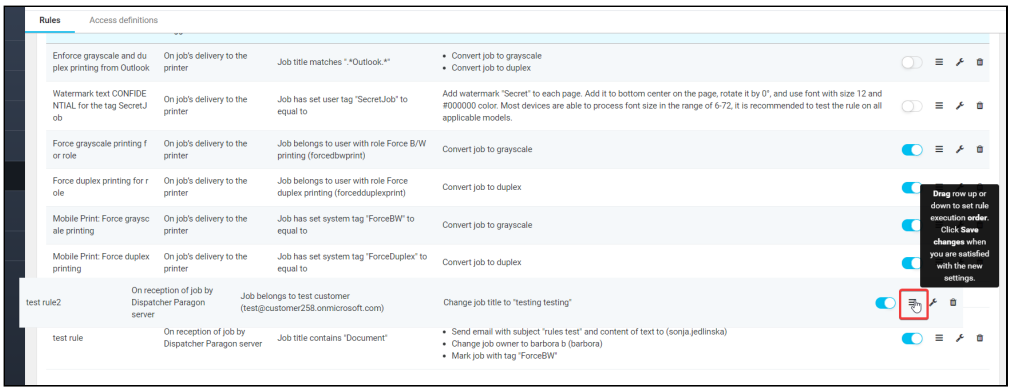
Editing a rule

1. Click the edit icon next to the rule you wish to edit.
2. You can edit the whole content of the rule - the name, the trigger, the conditions, the actions, and the notifications.
3. Click **SAVE CHANGES**. Note that if you make some conflicting changes in the rule, you will not be able to save it and will receive an error message.

Moving a rule

The rules are processed from the top to the bottom of the list. If you need to change the order of the rules execution, perform the following steps:

1. Click the hamburger menu icon next to the rule you wish to move.
2. Drag and drop the rule to a new position.



3. Click **SAVE CHANGES** to save the new order of rules.

Deleting a rule

Click the trash bin icon next to the rule you wish to delete.

List of rule definitions

This page contains a list of all triggers, conditions, actions, and notifications.

> ⚠ If a condition, action, notification or variable is not listed here even though you see it in the management interface, it means that it's available neither for Pure cloud printing, nor for Edge printing.

Triggers

Trigger	Description
On reception of job by Dispatcher Paragon server	Print job reception. This is where you can affect how the job will be processed by the system, e.g., redirect the job to a different queue.
Before job is released to the printer	Before print job is released to a device managed by Dispatcher Paragon Cloud. This is where you can set rejection of the job. ⚠ You can use this trigger only in the Edge printing scenario.
On job's delivery to the printer	Print job delivery to a device managed by Dispatcher Paragon Cloud. This is where you can apply changes to the job, such as conversion to black&white. ⚠ You can use this trigger only in the Edge printing scenario.
On user's login at terminal	When a user logs in at the MFD terminal. ⚠ You can use this trigger only in the Edge printing scenario.
On user's logout at terminal	When a user logs out at the MFD terminal. ⚠ Rules containing this trigger cannot have any actions, only notifications. ⚠ You can use this trigger only in the Edge printing scenario.

Trigger	Description
On job status change	When the status of the user print job has changed. Rule containing this trigger cannot have any actions, only notifications.

Conditions

Job Conditions	Supported triggers	Notes
Job belongs to <user>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	
Job owner's username <is / is not / contains / does not contain / matches / does not match / starts with / ends with> <text>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	

✅ Job belongs to user with <role>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's login at terminal • On user's logout at terminal • On job status change	
✅ Job belongs to user from <cost center>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	
✅ Job owner's cost center number <equal to / not equal to / greater than / lesser than / greater or equal to / lesser than or equal to> <number>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	

Job is printed on <device>	Triggers: • Before job is released to the printer • On job's delivery to the printer • On user's login at terminal • On user's logout at terminal • On job status change	
Job is printed on device with name <is / is not / contains / does not contain / matches / does not match / starts with / ends with> <text>	Triggers: • Before job is released to the printer • On job's delivery to the printer • On user's login at terminal • On user's logout at terminal • On job status change	
Job title <is / is not / contains / does not contain / matches / does not match / starts with / ends with> <text>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	Text can be in the form of a regular expression.

Job has been sent to named queue <is / is not / contains / does not contain / matches / does not match / starts with / ends with> <queue_name>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	Text can be in the form of a regular expression.
Job has been sent to queue type <direct / secured / shared>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	You can use this condition only in the Edge printing scenario.
Job <has / does not have> a <system tag>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	Setting a system tag (using the *Mark job with tag* action) in one rule doesn't affect other rules because all conditions are evaluated at the beginning.

✅ Job <has / does not have> a <user tag>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	⚠ Setting a user tag (using the *Mark job with tag* action) in one rule doesn't affect other rules because all conditions are evaluated at the beginning.
✅ Job file size <equal to / not equal to / greater than / lesser than / greater or equal to / lesser than or equal to> <number> <B / KB / MB / GB / TB>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	
✅ Job has <status>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's logout at terminal • On job status change	⚠ Only notification can be executed as a result of this condition.
Job page conditions	**Supported triggers**	**Notes**
✅ Job contains <more than, equal to, less than, between> <x> [<all,b/w,color>] pages [of paper size <large, small>]		

User status conditions	Supported triggers	Notes
Outcome of authentication on terminal <equal to / not equal to> success	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's login at terminal • On user's logout at terminal • On job status change	
User authenticates at device group	Triggers: • On user's login at terminal	Applicable to device groups and subgroups. If you select a group, the rule will apply to all subgroups as well.
User authenticates at Spooler Controller group	Triggers: • On user's login at terminal	Applicable to Spooler Controller groups. The rule will apply to all belonging SPOCs.
User is not a member of the role	Triggers: • On user's login at terminal	Rule-based engine requires an exact match (AND operator) between a user's list of roles and those selected in the rule to fulfill the condition.
Time conditions	**Supported triggers**	**Notes**

✅ Current <day of week / day of month> is <equal to / not equal to / greater than / lesser than / greater or equal to / lesser than or equal to> <day in week / day in month>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's login at terminal • On user's logout at terminal • On job status change	
✅ Current time is <equal to / not equal to / greater than / lesser than / greater or equal to / lesser than or equal to> <time>	Triggers: • On reception of job by Dispatcher Paragon server • Before job is released to the printer • On job's delivery to the printer • On user's login at terminal • On user's logout at terminal • On job status change	

Actions

Transform Job Operations	Supported Triggers	Notes

✅ Add watermark <text> to each page. Add it to <position> of the page, rotate it by <number>° and use font with <size> and <color>	Triggers: • On job's delivery to the printer	⚠ Watermarking feature is available for PCL and PostScript jobs only. Only ISO Latin-1 and Latin-2 character set is supported. ⓘ Variables can be used, see below for their definition.
✅ Find <text> in PJL header and replace it with <text> (<Append/Do not append> the text when searched text is not found)	Triggers: • On job's delivery to the printer	⚠ When a match is found, the whole line is replaced. Be sure to specify the pattern and the new value in the following format: *@PJL SET <HEADER>=<VALUE>*
✅ <Convert / Do not convert> job to grayscale	Triggers: • On job's delivery to the printer	
✅ <Convert / Do not convert> job to duplex	Triggers: • On job's delivery to the printer	
✅ <Convert / Do not convert> job to simplex	Triggers: • On job's delivery to the printer	
✅ Print job <number> times	Triggers: • On job's delivery to the printer	

✅ Mark job with <tag>	Triggers: • On reception of job by Dispatcher Paragon server	⚠ This action will not affect the evaluation of tag conditions in subsequent rules because all conditions are evaluated before any rules are executed.
Change processing workflow	**Supported triggers**	**Notes**
✅ Re-queue the job to <queue>	Triggers: • On reception of job by Dispatcher Paragon server	A direct queue can be selected from a list of existing direct queues. Alternatively, a direct or shared queue name can be typed manually. In that case, variables can be used in the queue name (see below).
✅ Redirect the job to the secure queue	Triggers: • On reception of job by Dispatcher Paragon server	Used for redirecting the job from a direct (or shared) queue to the secure queue, so that it is held by the server and not printed immediately.
✅ Reject print job	Triggers: • Before job is released to the printer	
✅ Delete print job	Triggers: • On reception of job by Dispatcher Paragon server	
✅ Deny authentication on terminal	Triggers: • On user's login at terminal	User authentication is denied (after successful authentication).

Change job title to <text>	Triggers: • On reception of job by Dispatcher Paragon server	Variables may be used in the text (see below).
Change job owner to <user>	Triggers: • On reception of job by Dispatcher Paragon server	
Change job billing code to <billing code>	Triggers: • On reception of job by Dispatcher Paragon server	
Set job as <favorite / not favorite>	Triggers: • On reception of job by Dispatcher Paragon server	

Notifications

General Notification Information	Supported triggers	Notes
Send e-mail with <subject> and content of <text> to job owner	Triggers: • all	Variables can be used, see below for their definition.
Send e-mail with <subject> and content of <text> to <user>	Triggers: • all	Variables can be used, see below for their definition.

General Notification Information	Supported triggers	Notes

⚠ Send Dispatcher Paragon Desktop Interface notification to job owner	Triggers
	• On reception of job by Dispatcher Paragon server
		⚠ The notification will be displayed in user's Client v3 only under the following conditions:
		• Client v3 is in client-spooling mode
		• The user sent the print job to a queue that uses LPR port:
		  • Queues deployed via Client v3 installation package created in Quick Print
		  • Direct print queues deployed by the user via Client v3
		  • Direct print queues created manually by the user (see Manually creating direct print queues)

Variables

ⓘ Not all variables are available for all triggers.

Variable	Description
[DEVICE_ID]	Internal Dispatcher Paragon Cloud Management Service unique ID of the involved device (printer, mfp)
[DEVICE_IP]	IP Address of the device
[DEVICE_NAME]	Device Name as configured in Dispatcher Paragon Cloud management interface

Variable	Description
[DEVICE_DESCRIPTION]	Device Description as configured in Dispatcher Paragon Cloud management interface
[DEVICE_LOCATION]	Device Location as configured in Dispatcher Paragon Management Service
[DEVICE_EQUIPMENT_ID]	Device Equipment ID as configured in Dispatcher Paragon Cloud management interface
[DEVICE_SERVICE_AGREEMENT_ID]	Device Service Agreement ID as configured in Dispatcher Paragon Cloud management interface
[DEVICE_CONTACT_PERSON]	Device Contact Person as configured in Dispatcher Paragon Cloud management interface
[DEVICE_ZIP_CODE]	Device ZIP Code as configured in Dispatcher Paragon Cloud management interface
[DEVICE_BACKEND]	Data Delivery Method as configured in Dispatcher Paragon Management Service (e.g., TCP/IP Raw, LPR, IPP) ⚠ You can use this variable only in the Edge printing scenario.
[DEVICE_SPOC_GUID]	GUID of the Spooler Controller managing the device
[DEVICE_SPOC_NAME]	Name of the Spooler Controller managing the device
[USER]	Owner of the job in the format "Name Surname (login)"
[USER_NAME]	User's first name from the Identity Database

Variable	Description
[USER_SURNAME]	User's surname from the Identity Database
[USER_LOGIN]	User's login from the Identity Database
[USER_EMAIL]	User's email address from the Identity Database
[USER_OU_NUM]	User's cost center number from the Identity Database
[USER_ID]	Internal Dispatcher Paragon Management Service unique ID of the user from the Identity Database
[JOB_ID]	Internal Dispatcher Paragon Management Service job unique ID (not available during job reception)
[JOB_GUID]	Internal Dispatcher Paragon Management Service job GUID (part of the filename in the JobStore folder in the spooler)
[JOB_TITLE]	Job Title
[JOB_SIZE]	Size of the print job (formatted for readability)
[JOB_SIZE_RAW]	Size of the print job (plain number in bytes for machine readability)
[JOB_PROJECT_ID]	Internal ID in Dispatcher Paragon Management Service of the billing code selected for the job
[JOB_QUEUE]	Target print queue name. ⚠ You can use this variable only in the Edge printing scenario.

Variable	Description
[JOB_STATUS]	Current job status
[JOB_STATUS_NUM]	Current job status as a numeric identifier
[JOB_NOTE]	Internal note generated by system
[JOB_ORIGIN]	IP address or hostname from where the job was received
[JOB_SPOOLER_HOSTNAME]	Hostname of the spooler that received the job
[JOB_SPOOLER_GUID]	GUID of the spooler that received the job
[JOB_SPOC_GUID]	GUID of the Spooler Controller that received the metadata of the job
[JOB_PAGES_BW]	Number of black and white pages in the job
[JOB_PAGES_COL]	Number of color pages in the job
[JOB_PAGES_BW_LARGE]	Number of large-format black and white pages in the job
[JOB_PAGES_COL_LARGE]	Number of large-format color pages in the job
[JOB_PAGES_LARGE]	Number of large-format pages in the job
[OP_DATE]	Current date and time
[DATE]	Current date
[TIME]	Current time

⚠ The **Send e-mail** notification sends messages in plain text. Microsoft Outlook by default removes line breaks in plain text e-mails. If this issue occurs in your environment, disable the **Remove extra line breaks in plain text message** options in Microsoft Outlook:

Access definitions

About Access definitions

Access definitions allow you to define which user roles can perform which operations (for example, printing) on which devices.

⚠ If an MFD has Dispatcher Paragon Cloud Terminal installed, Access definitions will work only for functions inside the Cloud Terminal, not for native functions, such as Native copy.

For details on inheritance and competition among roles, see section *Inheritance and competition among roles*.

Displaying the list of Access definitions

On the **Access definitions** tab, you can see a list of existing access definitions in the system.

Each access definition is represented by the following pieces of information:

- User role – the role for which the access definition is configured.
- Spooler Controller group – the Spooler Controller group for which the access definition is configured.
- Device – the device for which the access definition is configured.

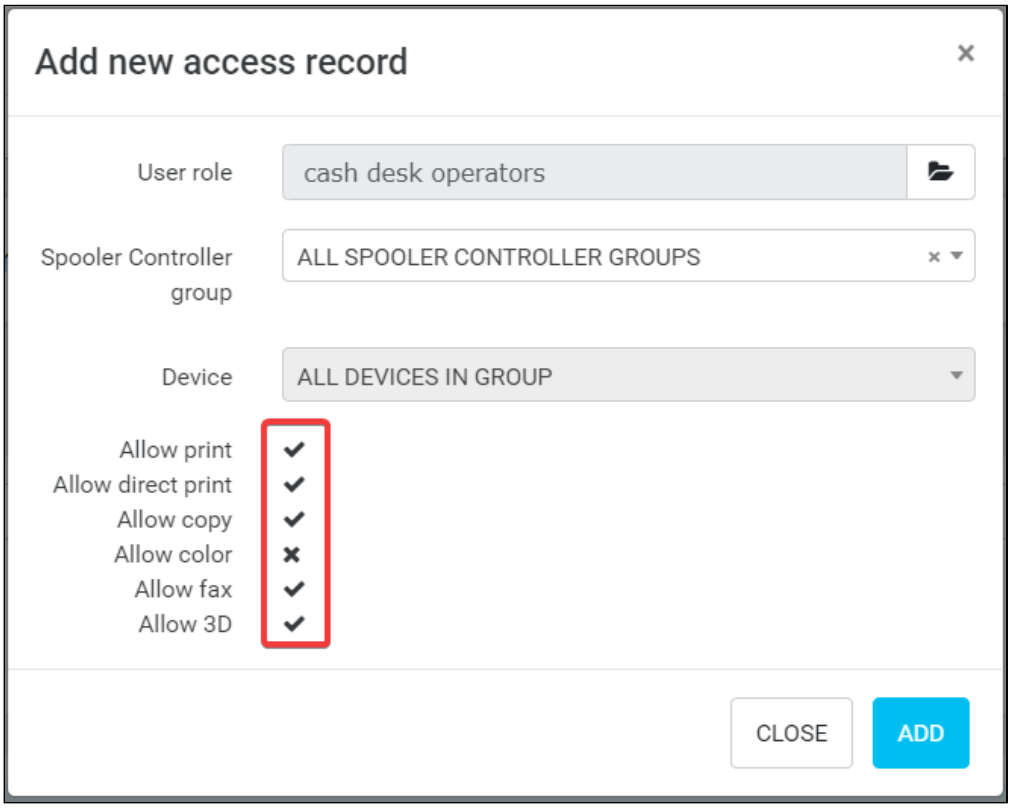
Each access definition displays whether the following actions are allowed or restricted for the given user role:

- Print – printing (when disabled, Direct print is also disabled).
- Direct print - printing on direct queues (when disabled, job delivered to direct queues will get redirected to secure queues).
- Copy – copying.
- Color – color operations (color printing/copying).
- Fax – fax operations.
- 3D – 3d printing.

Creating a new access definition

1. Click **+ ADD NEW ITEM**.

2. In the **User role** field, click the folder icon and select a role.
3. In the **Spooler Controller group** field, click the arrow icon. Select a group from the list of Spooler Controller groups.
4. In the **Device** field, click the arrow icon. Select a device from the list of devices.
5. Click the icons next to the actions that you want to restrict for the role you selected. This will change the action from its default state (allowed) to restricted. Example:



> At Dispatcher Paragon Cloud Terminal, the user will not see the buttons for restricted actions.

6. Click **ADD** to save your new access definition.

Deleting an access definition

Click the trash bin icon next to the access definition you wish to delete.

Inheritance and competition among roles

To understand rights inheritance, it is important to know how the role structure works.

Dispatcher Paragon Cloud has the *everyone* role built-in by default. This role cannot be deleted. Every Dispatcher Paragon Cloud user is a member of the *everyone* role and this cannot be changed. This role has precedence over all roles you create.

If you set access rights for the *everyone* role, these rights will be applied to all users. You can set detailed rights by defining a new role, setting its rights, and assigning it to a user. The new role inherits rights from its parent role *everyone*, but the settings made in the new role override its parent role settings.

If you set access rights for an individual device, these rights take priority over the settings of the entire device group.

If a user is a member of multiple roles of the same level, the restriction has priority.

Example: *User1* is a member of role *everyone*, *role1*, and *role2*. The *everyone* role has print access rights set for a device group named *Default*. For *role1*, the device group *Default* is restricted and for *role2*, this device group is allowed. As a result, *user1* is forbidden from printing to all devices included in the *Default* group because the permission in the *everyone* role is ignored. *User1* is also a member of other roles that are allowed to print to this *Default* device group, but the role *everyone* is subordinate to other roles and ignored – the only settings that matter for *user1* are the settings made for *role1* and *role2*. Printing is forbidden to the *Default* group for *role1* and permitted for *role2*. Because restriction has priority (see above), the restriction is applied.

Unlike function rights, assigning device access rights has one extra feature – the ability to assign default rights to a role. A role's default device rights will apply to all device groups that do not have rights explicitly set for the particular role. A role's default device rights settings have priority over the access right settings of a device group, both for the *everyone* role and for any other roles.

Example: A user is a member of the role *everyone* and *role1*. The *everyone* role has printing rights set for the device group *devices1* and *role1* has default rights set for copying. If the user accesses a device that is not part of the device group *devices1*, printing is allowed for the user because it is allowed for the *everyone* role. If a user accesses a device that is not part of the device group *devices1*, copying is allowed for the user because the default rights for copying have been set for their role in relation to all device groups that have not been explicitly set. This means that if a user in *role1* has printing rights set for the device group *devices2*, the default settings are ignored and printing is allowed for the user only according to *role1*'s device rights set explicitly for the group *devices2*.

2.6.7 MANAGING SCAN WORKFLOWS

Scan workflows allow you to create consistent digital content from paper documents.

If the screensaver is enabled on the MFD, scanning has the following limitation:

- If a user is scanning a large file, the delivery of the scan job to their email may be delayed by 5 minutes (at maximum).

Further limitations:

- Scan file size is limited to 18MB. If the scan file size is larger, the email is not delivered to the user. The system doesn't send a notification of such event.
- Email limits might block the delivery if the file is too large.

To configure scan workflows, click **Scan Workflows** in the sidebar menu of the Dispatcher Paragon Cloud management interface.

The **Scan Workflows** section contains two subsections:

- Workflows – this section serves for configuring scan workflows and making them available to the users. See Workflows.
- Connectors – this section serves for configuring connectors to external systems that serve as the destinations of the scanned documents. See Connectors.

Connectors

Before creating the first scan workflow, you must create a connector. If you already have a connector, continue to Workflows.

A connector defines the connection configuration required by scan workflows to deliver documents to external systems. Each type of external system has its specific configuration properties. You can create several connectors of the same type, each one using different credentials.

⚠ Currently, only SMTP connector and Extension connector are available.

Connectors tab

The **Connectors** tab displays all available connectors that you can use as destinations for your scan workflows. One connector can be used as the destination in multiple workflows.

Navigate to **Scan Workflows** and click the **Connectors** tab. On this tab, you can do the following:

- Create a new connector and configure its settings.
- Modify an existing connector and its settings.
- Delete a connector.

Adding an SMTP connector

To add an SMTP connector, perform the following steps:

1. On the **Connectors** tab, click **ADD CONNECTOR**.
2. Enter the connector name (maximum of 64 characters) and description (maximum of 300 characters).

3. In **Connector type**, select **Email (SMTP)**.
4. The **Primary mail server** and **Mail server account** are not editable. These are inherited from Dispatcher Paragon global mail server configuration.
5. Now you can click **SAVE CHANGES** and use the connector in a workflow, or continue with the advanced settings.

Advanced settings

To display the advanced settings, click **ADVANCED** at the upper-right corner of the **Connectors** tab. Advanced settings let you configure the **Notifications** options.

Notifications

Use connector notifications to enable email notifications. You can configure notifications for scan delivery success and scan delivery failure.

- **Delivery failure notifications** – Enables or disables notifications in case of scan delivery failure.
- **Delivery success notifications** – Enables or disables notifications in case of scan delivery success.
- **Restriction notifications** – Do not use, these settings are not available.

For each of the notifications, you can set up a recipient, subject, and body of the email. You can use HTML tags to format the body.

Adding an Extension connector for Cloud Fax

To add an Extension connector, perform the following steps.

The extension connector is visible in the list only if you have purchased one of the fax page packs, for example, *Cloud Fax Extension Additional Pages - 500 Pages*.

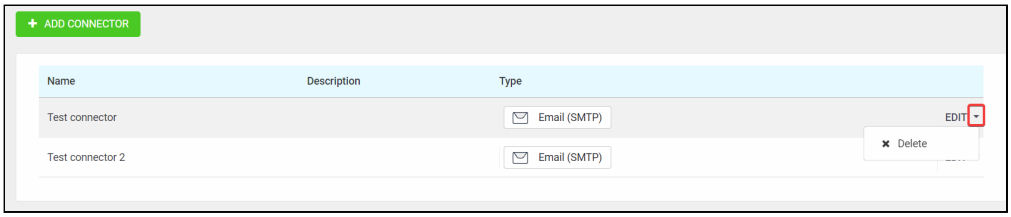
1. On the **Connectors** tab, click **ADD CONNECTOR**.
2. Enter the connector name (maximum of 64 characters) and description (maximum of 300 characters).
3. In **Connector type**, select **Extension**.
4. In the **Extension endpoint URL**, enter the URL for Cloud Fax provided by your service representative. Each customer has a unique URL. Example: https://example.azurewebsites.net/api/ScanToUplandFax.
5. Click **SAVE CHANGES**.

Editing a connector

1. On the **Connectors** tab, click **EDIT** next to the connector you wish to edit.
2. Use the **BASIC** and **ADVANCED** buttons in the upper-right corner of the tab to select the settings you want to edit. All settings and options are described in section *Adding a connector*.

Deleting a connector

1. On the **Connectors** tab, click the drop-down menu icon next to the connector you wish to delete, and click **Delete**.



2. Confirm your action by clicking **DELETE**.

> You cannot delete a connector when a workflow uses the connector as its destination. If you attempt to do so, you will see a warning message that the connector is in use.

Workflows

A scan workflow is best described as a blueprint of instructions for capturing, processing, and delivering a scanned document. A workflow's definition consists of several parts:

- General information used for workflow identification and displaying help on the MFD terminal.
- The destination – a connector that defines where and how the scanned documents are stored.
- Optional user inputs allowing users to enter additional information that will be collected alongside the scanned document.
- Scan settings (for example, scan resolution, colors).
- Access rights specifying which Dispatcher Paragon Cloud roles can use the workflow.

Workflows tab

To access the **Workflows** tab, click **Scan workflows** in the left sidebar menu.
On the **Workflows** tab, you can perform the following actions:

- Create a new workflow.

- Change the display order of workflows on the MFD terminal.
- Import a workflow definition XML file (previously exported using the **Export XML** action button).

For each workflow in the list, you can:

- Enable or disable the workflow – disabled workflows are not available to users on the MFD terminal.
- Open the connector in edit mode. See Connectors for more details.
- Edit the workflow.
- Duplicate the workflow.
- Export the workflow to XML file.
- Delete the workflow.

Adding workflows

You can add a workflow in the following ways:

- Create a new workflow
- Import a workflow from XML file

To import a previously exported workflow, click the **IMPORT XML** button in the upper-right corner of the tab. Imported workflows are disabled by default after importing. A new connector is created for each imported workflow.

For information on how to create a new workflow, see the section below.

Creating a new workflow

1. On the **Workflows** tab, click **ADD WORKFLOW**.
2. In the **General** section, enter the workflow name (maximum of 64 characters) and description (maximum of 300 characters).
3. In the **Destination** section, select the destination connector. The only currently available connector – Email (SMTP) connector – delivers scanned files by email to one or more email addresses.
4. Fill in the additional information specific to the selected connector:
   - Email connctor:
     - **From** – The email address from which the email is sent. Enter **no-reply@dipa.cloud**.Be aware that %userEmail% is currently not supported for this field.
     - **To** – The recipient's email address. You can use Process, capture, and user input variables. The default value is *%userEmail%*. You can use multiple email addresses and separate them by a comma or semicolon.

- **Subject** – The email subject. You can use Process, capture, and user input variables.
- **Body** (optional) – The email body. You can use Process, Capture, and User input variables. For the list of available variables, see Scan workflows additional information, section *Workflow Variables*. You can also use HTML tags to format the body.

5. In the **Output** section, select the output format. For more information see Scan workflows additional information, section *Supported output formats*.
6. Check **Can be modified by the user on the terminal** if you want to allow users to change the output format during their session on the MFD terminal.
7. Enter the **Filename** (optional). This is the name of the resulting scanned file (without an extension).

   ⚠ The system doesn't allow the following special characters in the file name, as they cause failure upon scanned file delivery: `* ? / \ | : < >`

   ⓘ You can use Process, Capture, and User input variables. If the scan workflow produces multiple files, the filename is appended with a numeric sequence in the "####" format, e.g., "0001", "0002", etc. If you leave the filename field blank, the system will use the filename generated by the device where the scan was made.

8. Scan settings are applied to the scanner on the MFD where the user launches the scan workflow.

   In the **Scan settings** section, configure the following settings:

   - **Scan resolution** – Determines the DPI of the scanned document. For more information see Scan workflows additional information, section *Scan resolution*.

     ⚠ Not all MFD models support all resolution levels. If you select an unsupported resolution level, scanning may not start or resolution is set to at least as good as configured or, if not possible, the best one available (this differs for each MFD vendor).

   - **Sides** – Determines whether the document will be scanned on one side (simplex) or both sides (duplex) of the sheet.

     ⚠ Some MFD models do not support forcing duplex settings and the user has to set it manually during the scan.

- **Color** – Determines the color scheme of the scan.

> ⚠ Not all MFD models support all color schemes. If you select an unsupported color scheme, scanning may not start or the color scheme is approximated to the nearest possible value (this differs for each MFD vendor).

9. If you want the users to have the ability to modify **Scan resolution**, **Sides** and **Color** at the MFD terminal, check the **Can be modified by the user on the device** checkbox under each setting. If you use this option, the value you set will be displayed as default on the MFD terminals, and the users can edit the value during their session.
10. In the Edge printing scenario, you can also use the Konica Minolta Advanced Scan Settings:
    - **Scan size**
    - **Page setting** – Use this option to split a batch scan into multiple documents.
    - **Original type** – Select an appropriate image quality level for the original, and scan at the optimal level of image quality.
    - **Background removal** – You can adjust the density of the background area for originals with colored backgrounds (newspaper, recycled paper, etc.) or originals that are so thin that text or images on the back would be scanned.
    - **Density** – Select the scan density (dark, light) of the original.
    - **Blank page removal**
    - **Resolution**
    - **Sides**
    - **Color**
    - **File type** – The following rules are applied for file formats:
        1. JPEG – **Page setting** is ignored and page separation is always set to 1.
        2. TIFF – set as single-page by default, but it can be reconfigured using the **Page setting** property.
        3. Other formats – set as multi-page by default, but they can be reconfigured using the **Page setting** property.

> ⓘ
> - If there is a conflict between Konica Minolta Advanced Scan Settings and other workflow settings, the Konica Minolta Advanced Scan Settings will have a higher priority.
> - The combinations of advanced scanning options are not validated. If the combination is invalid, it will result in a failed scan.

11. In the **User input fields** section, click **Add user input** to define and rearrange user input fields. User input fields are helpful for collecting information from the users along with the scanned document. The value of each user input field is stored in a variable and can be accessed in the workflow during the delivery. Note that the process variables cannot be used in the capture phase, meaning that the. variables defined by user input fields cannot be used in other user input fields.
12. Click **Assign access to roles** to define who will have access to the workflow. If you don't specify any role, the workflow will not be available to any users.
13. Click **SAVE CHANGES**.
14. The workflow is now available on the MFD terminals to all users in the roles to whom you provided access. We recommend testing a newly created workflow first before making it accessible to other users. Test a workflow by providing access to administrators only.

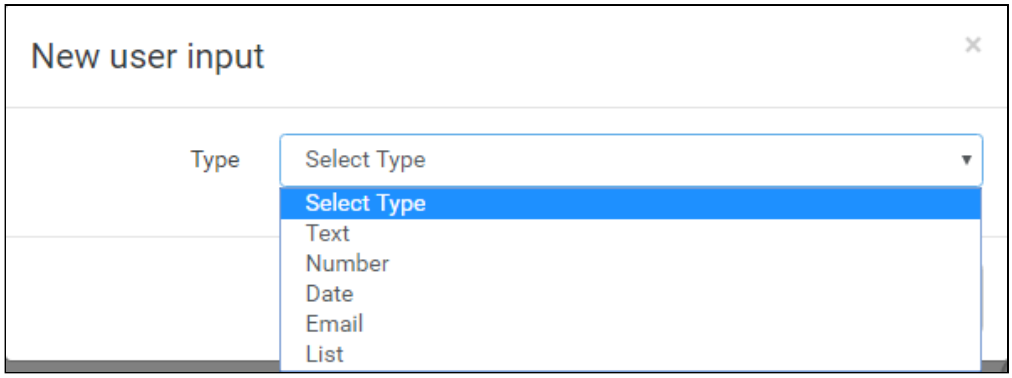
User input fields

In the **User input fields** section, you can define the scan metadata to be collected at the MFD terminal in the form of user input. User input is collected from terminal users in a scan workflow detail. The values are saved in user input workflow variables.

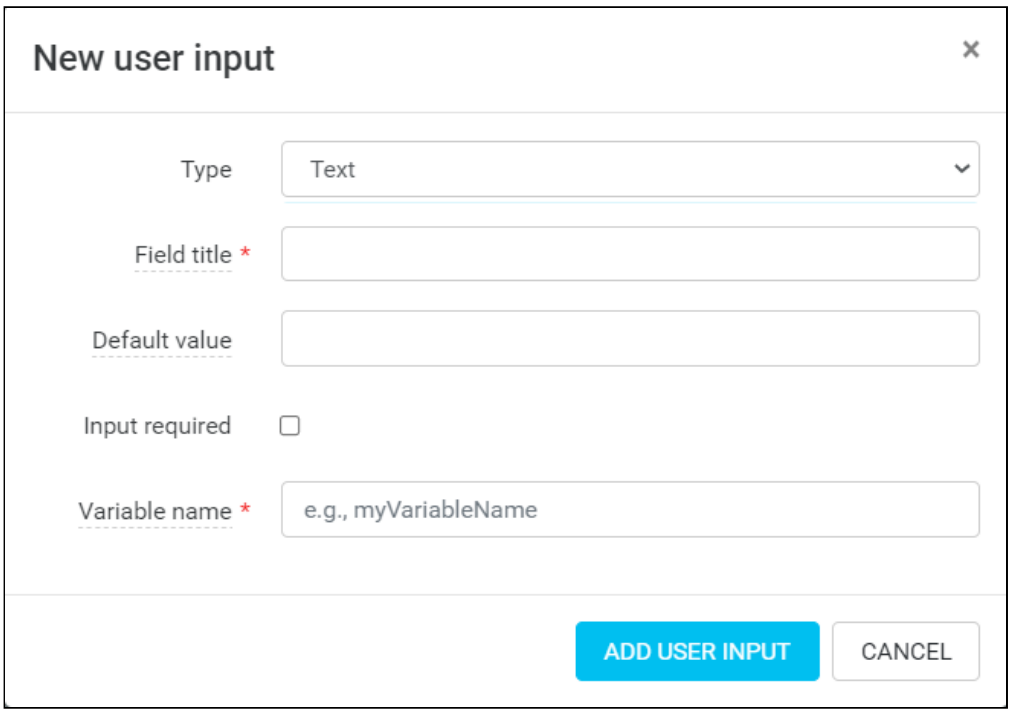
Adding User input field

To add a User input field, perform the following steps:

1. Click **ADD USER INPUT**.
2. Select the type of user input.



3. Next, additional configuration options are displayed. Some of the additional configuration options are dependent on the type of user input field selected. However, there are several options common to all types of user input fields.



a. **Field title** – The title of the user input field that will appear in the workflow detail on the MFD terminal. You can use capture variables in this field.
b. **Default value** – The default value of the user input field. You can use capture variables in this field.
c. **Input required** (optional) – If checked, user input must be filled before the user is allowed to scan a document.
d. **Variable name** – The name of the variable used to access the user input value in the workflow. NOTE: Do not use '%' characters.

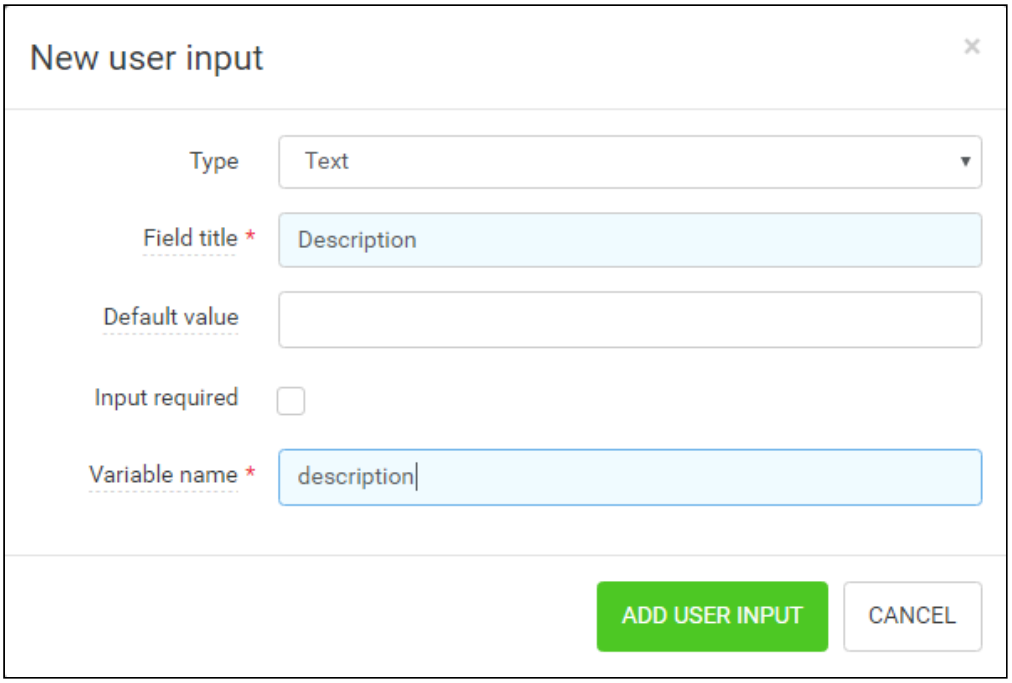
4. Click **ADD USER INPUT** to save your changes.

User input types

Text

Text type user input field lets the terminal users enter text.

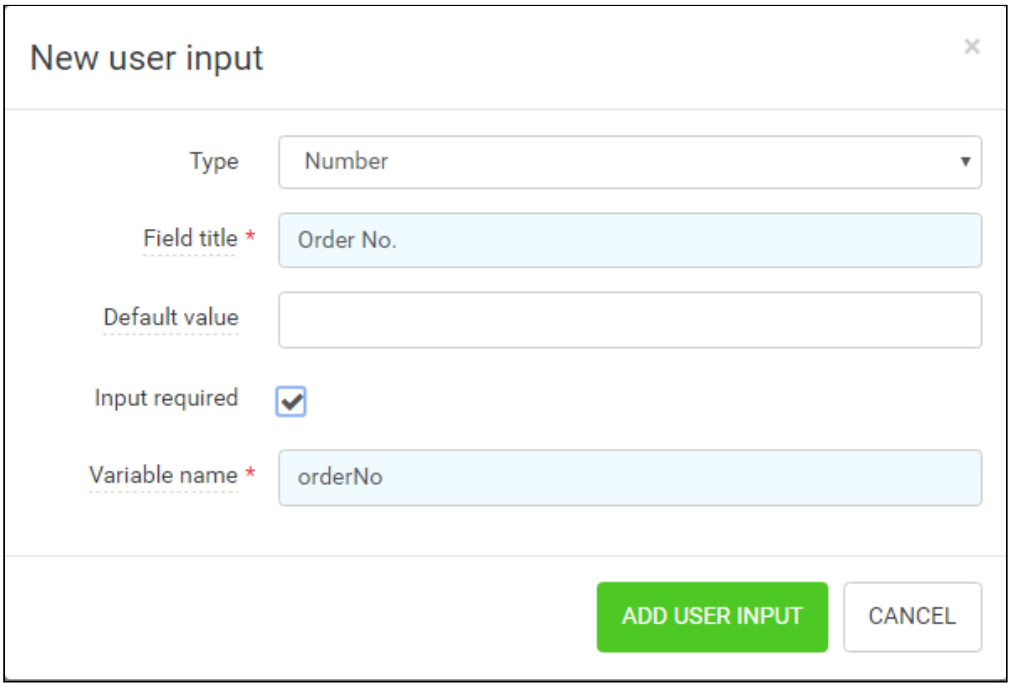
If you specify the **Default value** for text type user input fields, you can use capture variables.



Number

Number type user input field lets terminal users enter whole positive numbers.

If you specify the **Default value** for number type user input fields, you can use capture variables.

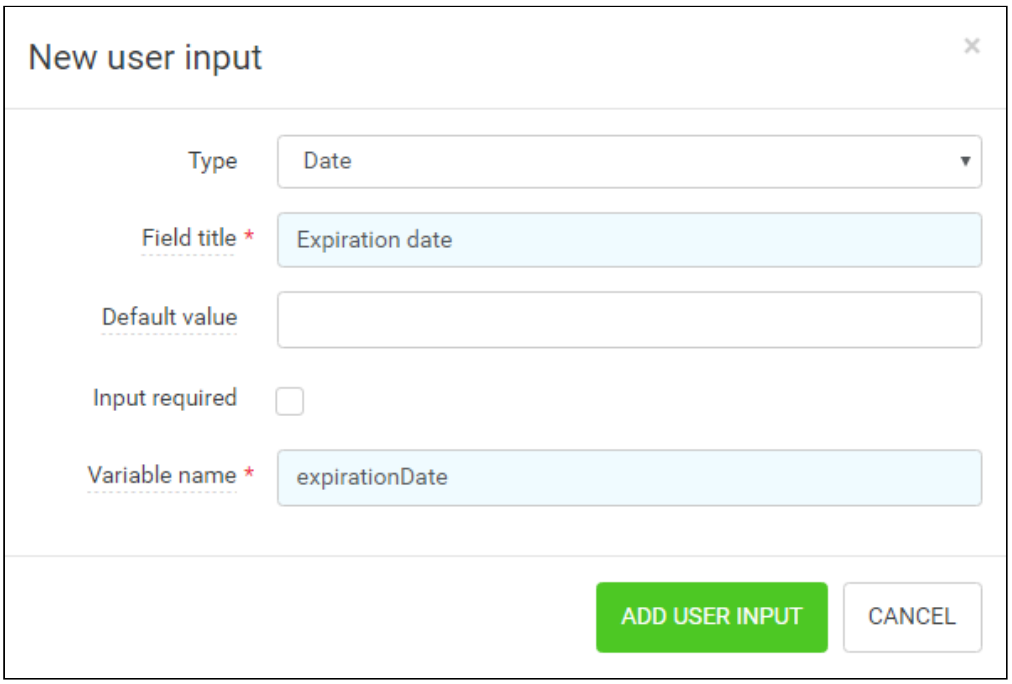


Date

Date type user input field lets terminal users enter dates.

If you specify the **Default value** for Date type user input fields, you can use capture variables.

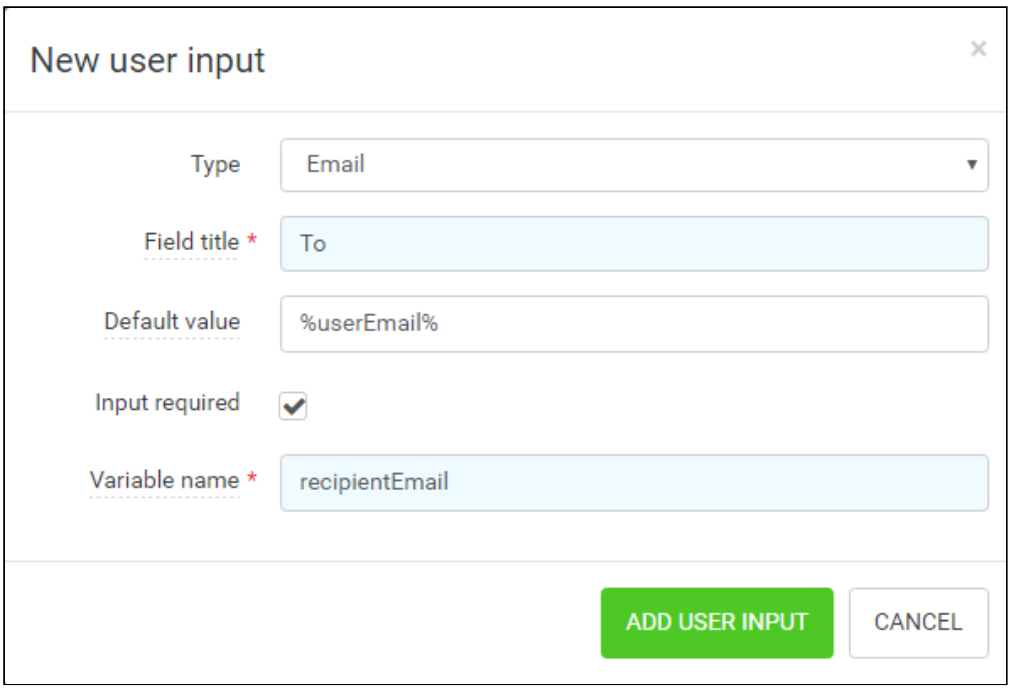
> ⚠ The only supported date format is YYYYMMDD. Do not use capture variables that do not hold values in this format.
>
> If a user tries to enter the date in another format at the terminal, they will receive an error message saying that they should use the YYYYMMDD format.



Email

Email type user input field lets terminal users enter email addresses.

If you specify the **Default value** for Email type user input fields, you can use capture variables.



List

List type user input field lets a terminal user select from a list of possible values.

If you specify the **Default value** for List type user input fields, you can use capture variables.

The supported data sources are the **Manual Input List** and **CSV List**.

Manual Input List

Manually enter list values through the Dispatcher Paragon Cloud management interface.

Fill in the following information:

1. In the **Data source** field, select **Manually input values**. These manually entered values will be available to users in a dropdown list on the MFD terminal when they run the workflow.
2. In the **List items** section is the list of values for the user input field. Click **Add row** to append a new row to the list.

   > Only rows with both **Label** and **Value** filled are considered valid and will be saved correctly in the Dispatcher Paragon Cloud management interface.

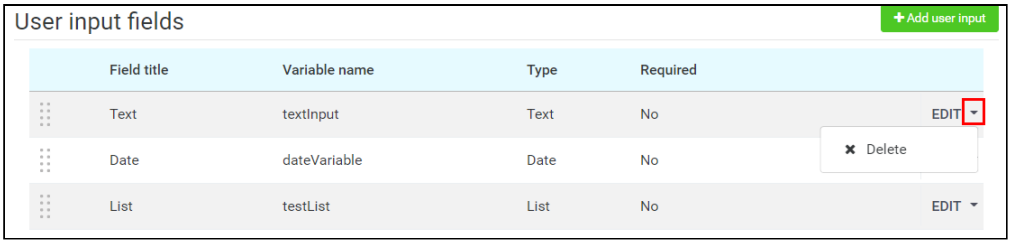
3. In the Default value dropdown list, select the default value. This is the value that will be pre-selected for the users on the Dispatcher Paragon terminal.

   > Only valid rows are listed as options in the Default Value dropdown list.

4. Click **ADD USER INPUT** to save your changes.

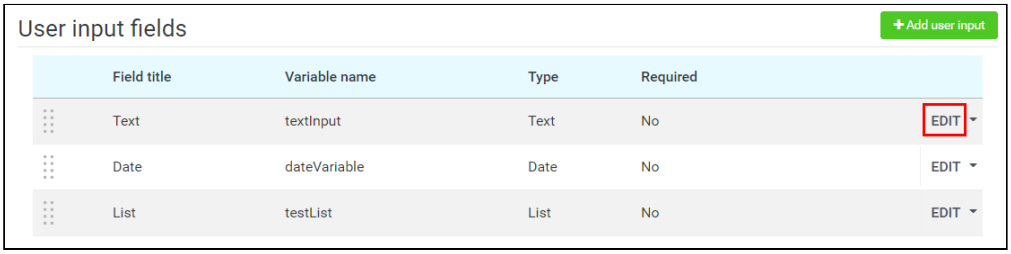
Deleting a User input field

To delete a user input field, open the dropdown menu for the user input field and click **Delete**.



Editing a User input field

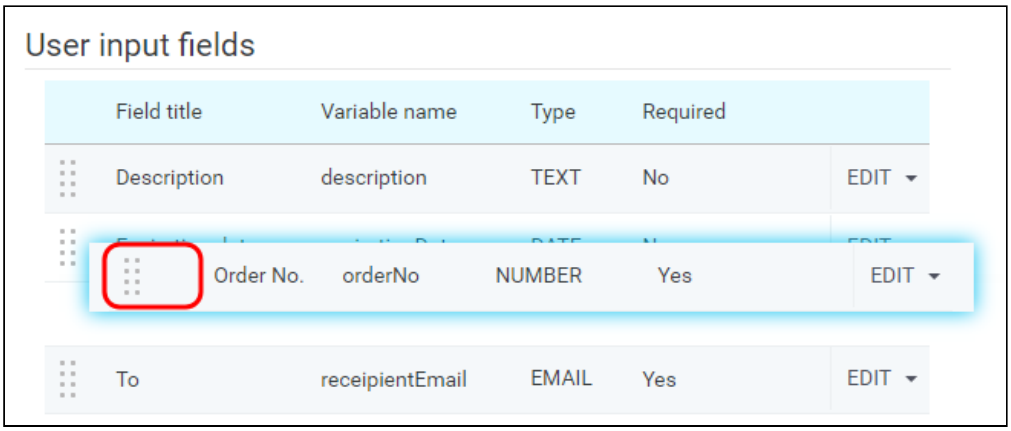
To edit a user input field, click **EDIT** next to the user input.



Reordering User input fields

User input fields are displayed in the workflow detail screen on the MFD terminal in the same order as in the workflow definition.

To change the display order of user input fields, drag and drop user input fields using the dotted area.

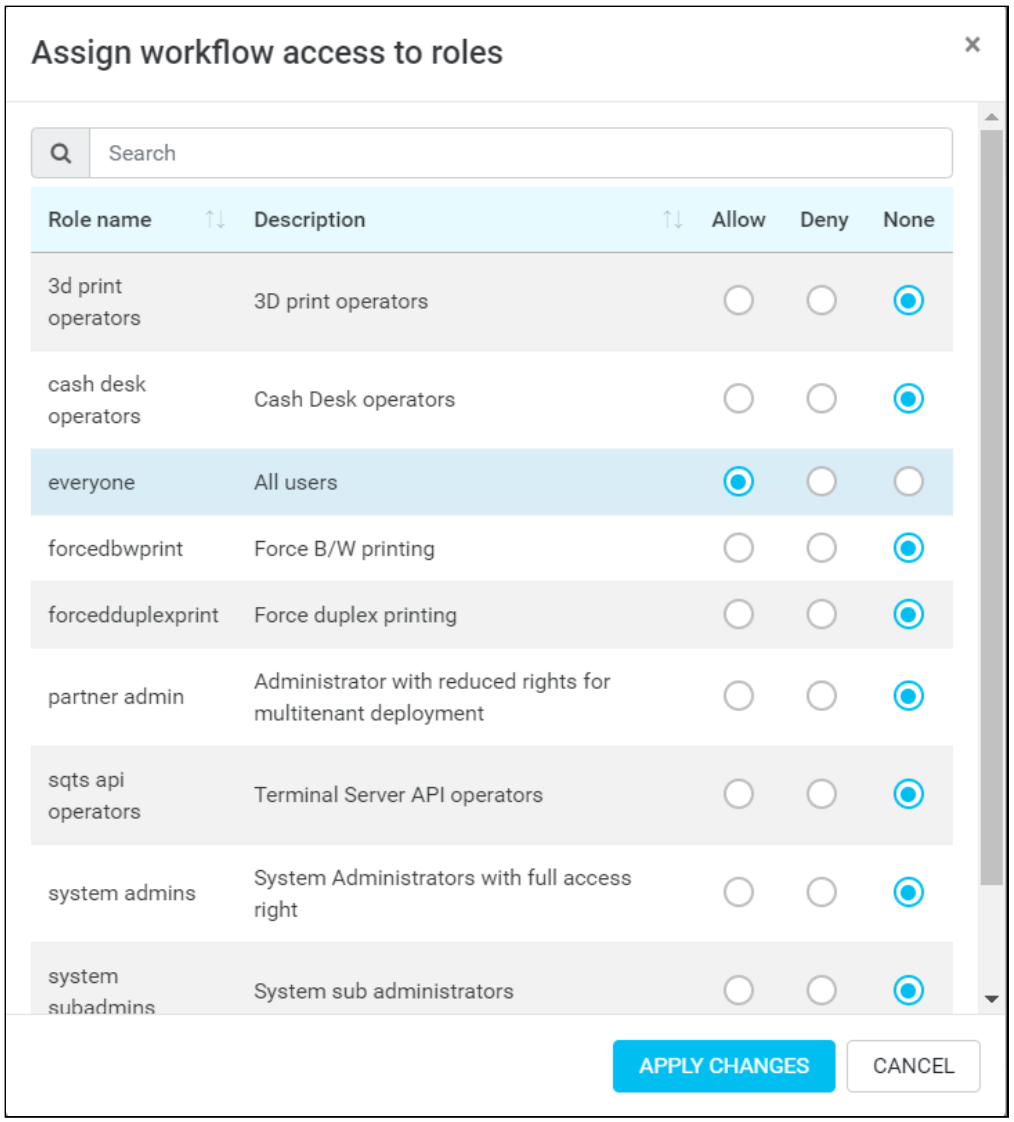


Granting access to a workflow

The **Access** section specifies which Dispatcher Paragon Cloud roles have access to the workflow.

Only users who belong to the role(s) specified in the **Access** list will be able to use the workflow.

1. Click **Assign access to roles**.
2. You will see a list of all roles. Select the radio button(s) in the **Allow** column for the roles to which you want to grant access to the workflow.



> If a user has more roles and some of them are allowed access and other roles are denied access to a workflow, then the user will not see the workflow on the MFD.
>
> **None** is the default state.

3. Click **APPLY CHANGES**.

Reordering workflows

The workflows displayed in the list of available scan workflows represent the order they are displayed to users on the MFD terminal. To change the order of listed workflows, do the following:

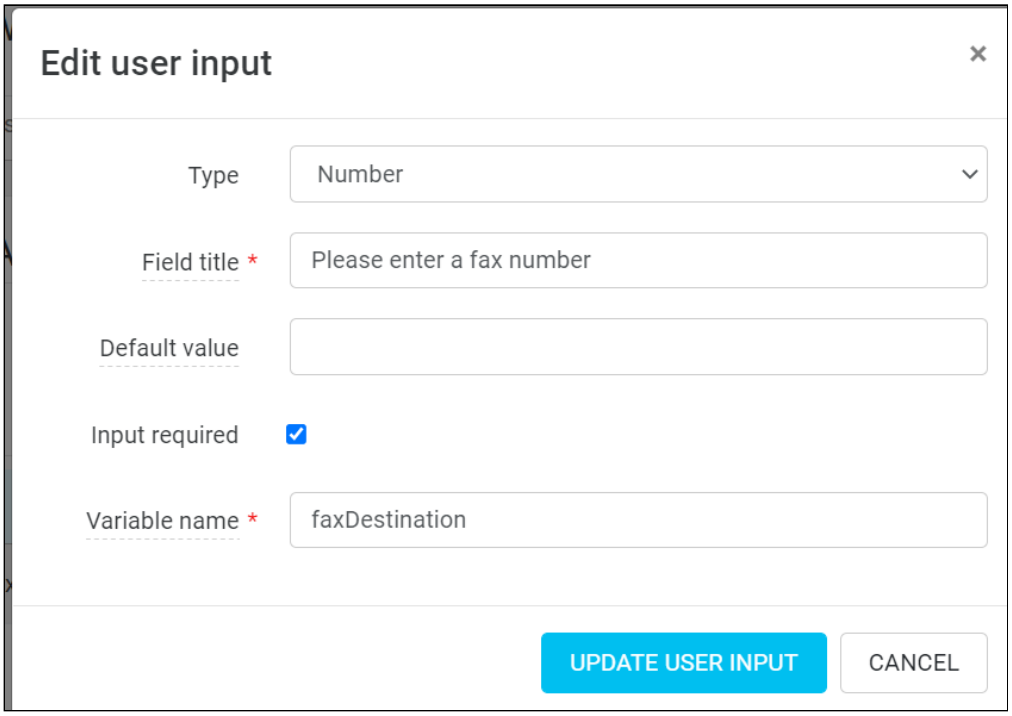
1. Click **REORDER** in the upper-right corner of the **Workflows** tab.
2. Use the dotted area on the left side of each workflow to drag and drop workflows to create the desired order of workflows.
3. Click **CONFIRM** in the upper-right corner of the tab to save the changes.

Cloud fax workflows

After configuring the Cloud fax connector (see Connectors), perform the following steps to configure a Cloud fax workflow.

1. On the **Workflows** tab, click **ADD WORKFLOW**.
2. In the **General** section, enter the workflow name (maximum of 64 characters) and description (maximum of 300 characters).
3. In the **Destination** section, select the destination connector you created for Cloud fax.
4. In the **Output format**, select **PDF**. PDF is the only supported format for Cloud Fax.
5. In **Sides**, select either **Simplex** or **Duplex**, and check the **Can be modified by the user on the terminal** checkbox.
6. In **Konica Minolta Advanced scan settings**, make sure that the **File type** is set to **PDF** as well.
7. Configure the User input fields. The users can enter fax numbers either by a phonebook entry or manual entry. If you wish both methods to be available to the users, you must create a separate workflow for each method.
    a. Configuring **Manual entry**:
        1. Click **+ Add user input**.
        2. In **Type**, select **Number**.
        3. Fill in the **Field title**. The title should make it clear to the users that they must fill in a fax number.
        4. Select the **Input required** checkbox.

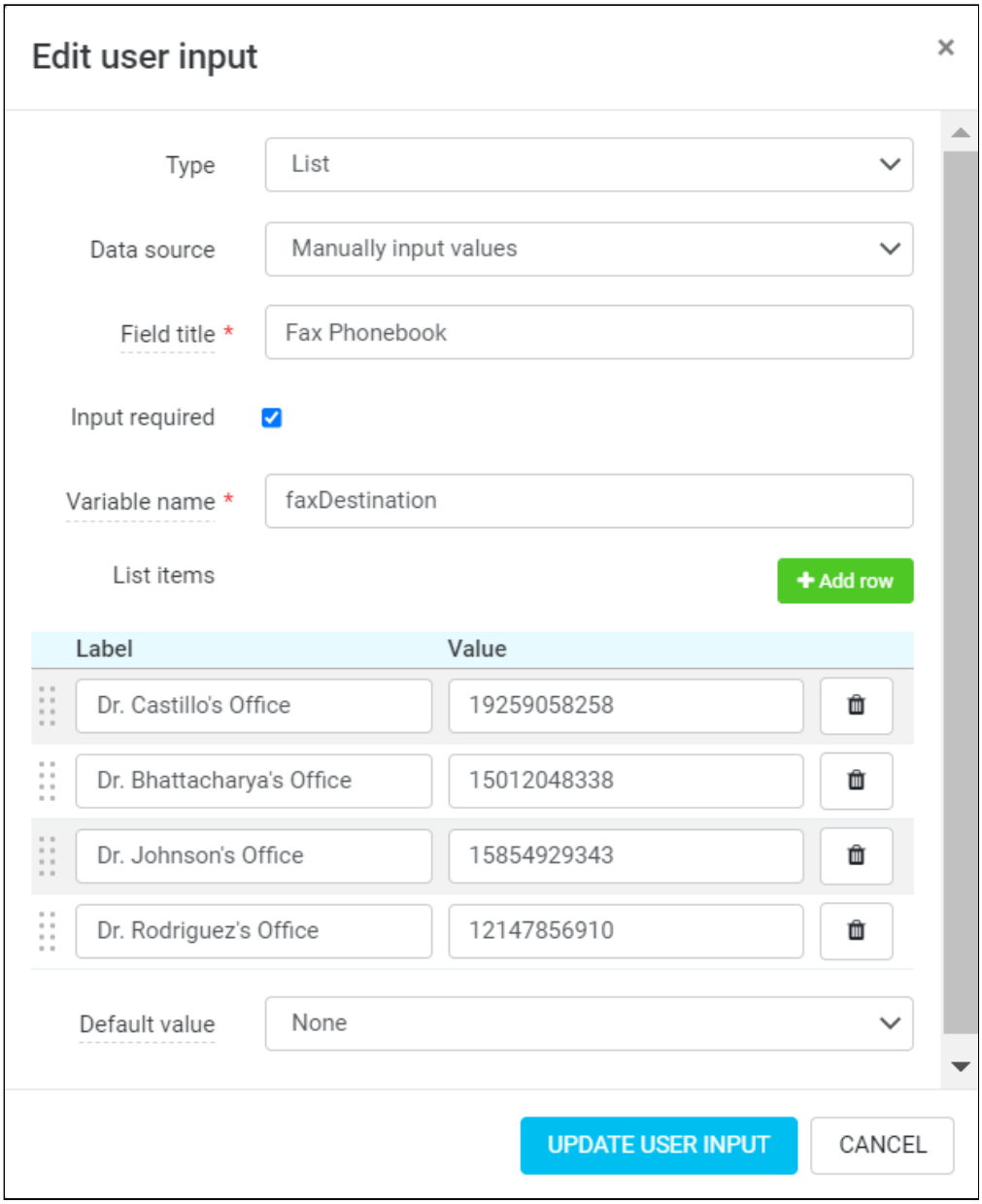
5. In **Variable name**, fill in *faxDestination*.



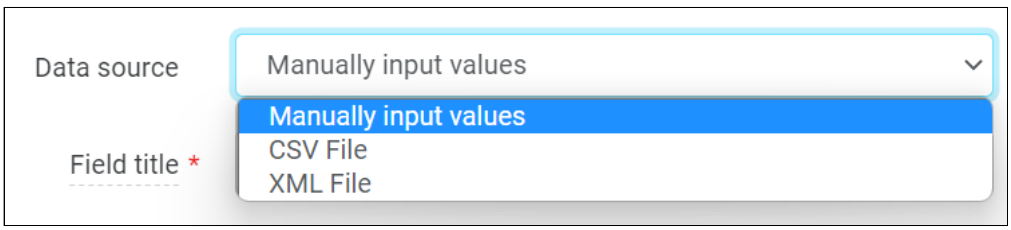
b. Configuring **Phonebook entry**:

1. Click **+ Add user input**.
2. In **Type**, select **List**.
3. Fill in the **Field title**, for example, *Fax Phonebook*.
4. Select the **Input required** checkbox.

5. In **Variable name**, fill in *faxDestination*.



6. Select the **Data source** method. You can input the values manually or upload a CSV or XML file.



8. Click **+ Assign access to roles** to define who will have access to the workflow. If you don't specify any role, the workflow will not be available to any users.

9. Click **SAVE CHANGES**.

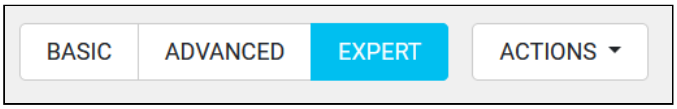
2.6.8 MANAGING SYSTEM SETTINGS

System settings overview

The system configuration settings are categorized into **Basic**, **Advanced,** and **Expert** levels. All users with Customer admin system role automatically have access to all three levels.

> ⚠ Be aware that Customer admin system role gives you the **System settings - cloud options** role, which allows you to see, export, or import ONLY the cloud-related settings from the **Basic**, **Advanced**, and **Expert** levels.

Use the buttons in the upper right corner to choose which level of system configuration settings you wish to display.



Next to the buttons, you can find the **Actions** dropdown menu. It contains the following actions:

- **Export changed configuration into the XML file**
- **Import configuration from the XML file**

Use export and import if you want to use the same configuration for multiple customers.

Editing the currency settings

1. Log into the Dispatcher Paragon Cloud management interface.
2. Navigate to **System** > **Configuration**.
3. Type *currency* into the search box and click **Search**.
4. Change the following settings according to the your needs:
   - **Currency code** – Used by embedded terminals that cannot display the currency symbol.
   - **Currency format** – Used by Dispatcher Paragon Cloud to display prices. "¤" represents the currency symbol, and "%" represents the amount, e.g., for USD use "¤ %" ($10), and for CZK use "%¤" (10 Kč).
   - **Currency symbol** – The symbol used for the currency ($ for USD, € for EUR, etc.).

Print job roaming

In case of Hybrid architecture, it is possible to share job data between pure cloud devices and edge devices. In case of Edge architecture, it is possible to share job data between multiple edge devices. This allows users to print regardless of how a job was submitted.

Global roaming is enabled by default. To opt-out of Global roaming and switch to Local roaming, perform the following steps:

1. Log into the Dispatcher Paragon Cloud management interface.
2. Navigate to **System > Configuration**.
3. Type *far roaming* into the search box and click **Search**.
4. Disable the *enableFarRoaming* setting.

   ⚠ This setting applies to all of your edge devices.

5. Click **SAVE CHANGES**.

ⓘ **Details of operation**

Global roaming – when a job is successfully spooled on an Edge device, the job data is uploaded to the cloud. When the upload is successful, the job data becomes available to all edge devices and the cloud spooler. Once the job metadata is synchronized between edge devices and the cloud (which takes less than a minute) and the job data upload is finished, the jobs can be printed at any printer.

Local roaming – when a job is successfully spooled on an Edge device, the job metadata is uploaded to the cloud for management and reporting purposes. The job data remain in the customer's network.

Switching from Local print roaming to Global print roaming

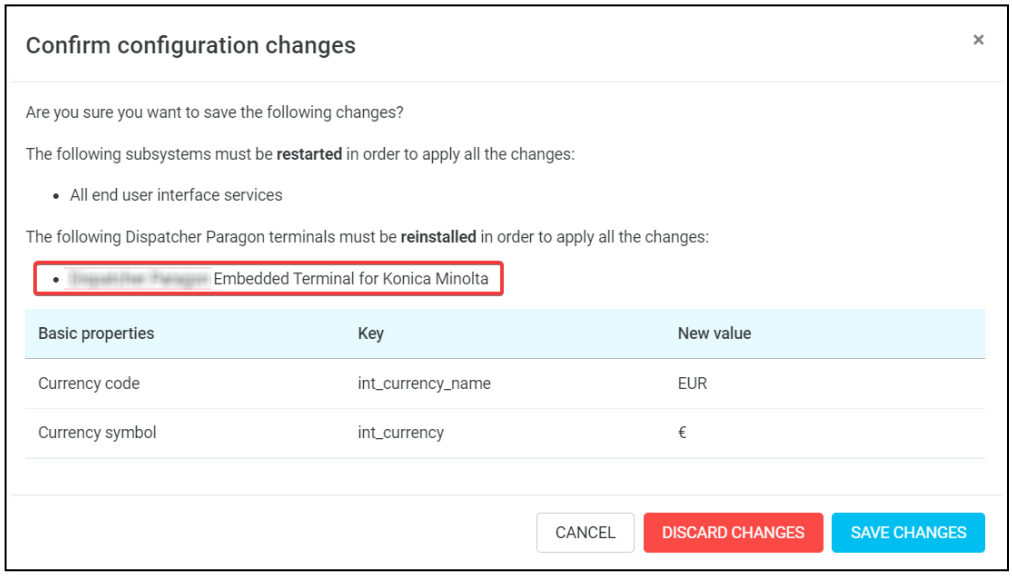
If you switch from Local print roaming to Global print roaming, the job metadata will start to synchronize to the cloud and across the site servers. Print jobs will be displayed as unavailable at MFDs not connected to the original site server where the job was spooled when Local print roaming was active. The users will not be able to release such print jobs.

Saving the system settings

After editing some of the system settings, you will need to reinstall certain types of terminals.

1. Click **SAVE CHANGES**. A confirmation window is displayed.

2. In the window, ignore the information regarding the need to restart all end user interfaces and note the type of embedded terminals to reinstall. Click **SAVE CHANGES**.



3. Navigate to **Devices** > **Printers** and select all devices with the terminal type noted in the step above.
4. Click **ACTIONS** in the upper right corner of the screen and select **Reinstall terminal** from the drop-down menu. A confirmation window is displayed.
5. In the window, click **REINSTALL TERMINALS**.

2.7 MANAGING PRINT QUEUES

There are two ways in which end users can get print queues.

2.7.1 CLIENT V3

You can deploy Dispatcher Paragon Client v3 to end user workstations together with print queues. See Dispatcher Paragon Client v3 for more details.

2.7.2 ADDING PRINT QUEUES MANUALLY

End users can configure a print queue on their workstations themselves.

1. Send the following to the end users:
   a. The link to Dispatcher Paragon IPP Gateway. If you wish to send a link to a specific edge device, see Generating IPP URI for end users for a specific edge device.
   b. Which print driver to use when adding the print queue manually.
2. End users generate an IPP URI on the IPP Gateway web page. See the *End user guide*, chapter Configuring IPP print queues.

3. End users this URI to create a printer (print queue) on their workstation. See the *End user guide*, chapter Configuring IPP print queues.

Print driver impact on job info in the Management interface

Be aware that the Management interface may display incorrect information in the print job info if one of the following conditions apply:

- An end user added the print queue without specifying a print driver, for example, when using the **Add this printer to my Mac** button on the IPP Gateway page
- An end user did not specify a print driver when adding the print queue from the command line in Mac or Linux
- An end user used a print driver that does not change job data according to print options, as described below.

The choice of print driver impacts job parsing. Some print drivers don't convert print jobs to grayscale when black & white spooling is selected on end-user workstation, but send the job as colored with additional information that it should be printed in grayscale. Such print job will be printed correctly at the MFD, but the job parser detected the job as colored, therefore the Management interface will display in the job info that it's colored. The same problem may occur with other attributes, such as duplex print.

Direct print queues

Direct print queues work both in Edge printing and Pure Cloud printing scenario.

If you wish to enable Direct printing to reporting-only devices, perform the following steps:

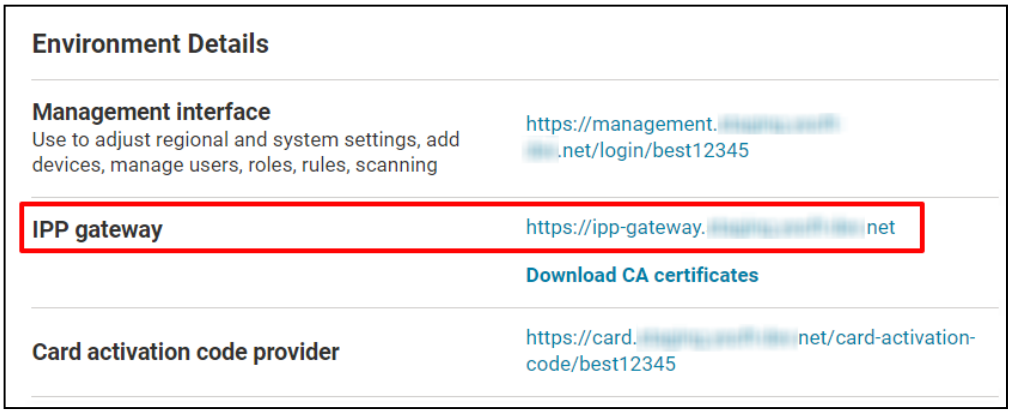
1. Add a reporting-only device with a direct queue in the Dispatcher Paragon Cloud management interface. See Managing devices, section *Adding reporting-only devices*.
2. If not done already, deploy Client v3 to end user workstations.
3. Instruct the end users to deploy the direct print queues from Client v3. See the End user guide, chapter Using Dispatcher Paragon Client v3.
4. Alternatively, the end users can create direct print queues manually, if, for example, they need to use a different print driver. See the chapter Manually creating direct print queues.

   ⚠ The users must have Dispatcher Paragon Client v3 installed even in this scenario.

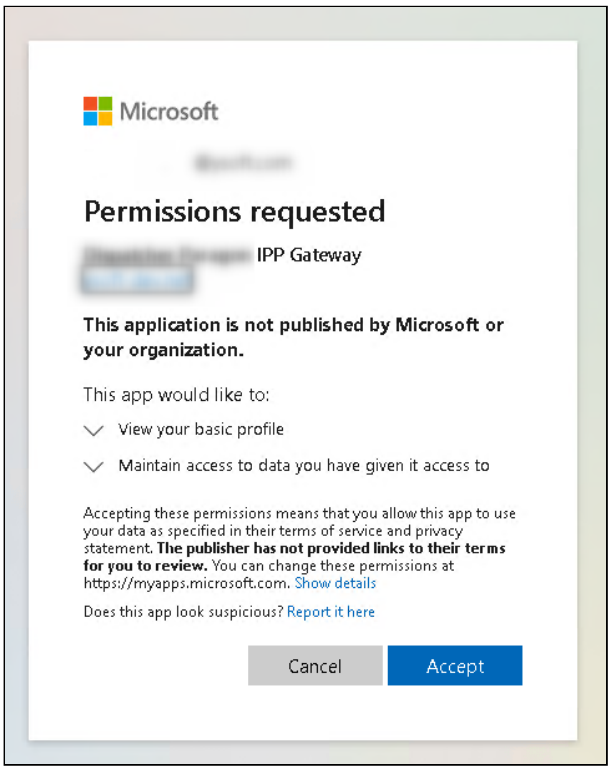
2.7.3 GENERATING IPP URI FOR END USERS FOR A SPECIFIC EDGE DEVICE

1. If not done already, deploy the CA certificate for edge printing to user workstations. See Managing Edge devices, section *Downloading CA certificates*. Make sure that the users' workstations have network visibility to the edge device.

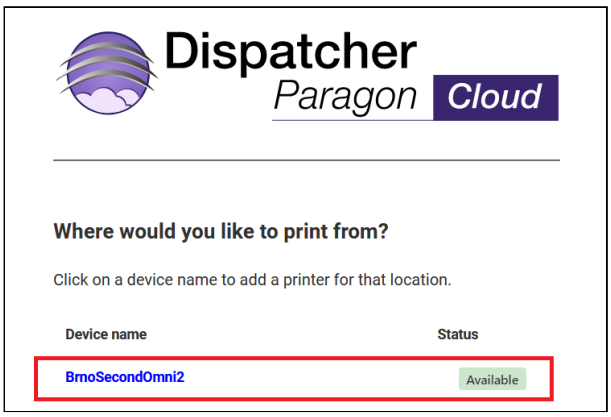
2. Log in to Dispatcher Paragon Cloud Portal. On the dashboard, click the link to IPP Gateway.



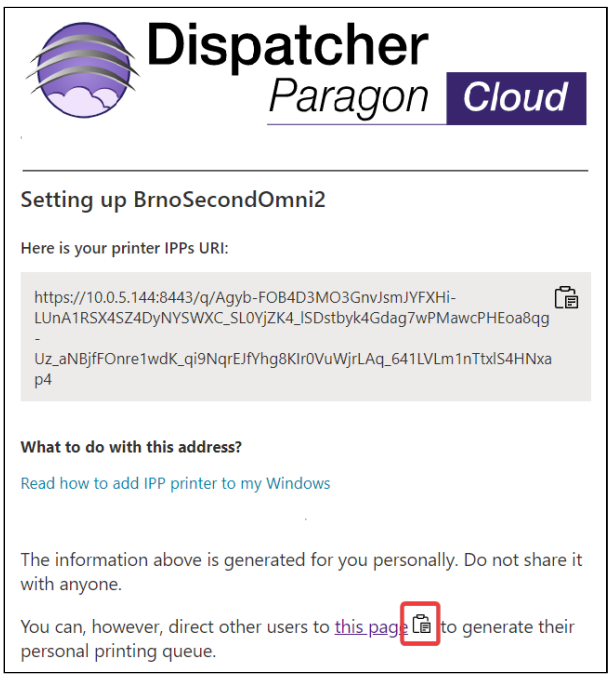
3. Authenticate with your company credentials and approve the permissions requested for IPP Gateway.



4. You will see a list of Edge devices that are connected to your Dispatcher Paragon Cloud.



5. Reachable devices are displayed in blue. Click the name of your chosen edge device. Click the clipboard icon at the bottom of the page to copy the link to IPP Gateway specific for this device.



6. You will see a message "Copied to your clipboard."
7. Distribute this link to the end users.
8. For details on how end users can use this link to add a printer (print queue), see the *End user guide*, chapter Configuring IPP print queues.

2.8 DISPATCHER PARAGON CLIENT V3

2.8.1 ABOUT DISPATCHER PARAGON CLIENT V3

Dispatcher Paragon Client v3 is a desktop application for end users, through which they can:

- Submit their print jobs to the cloud, or in case of Edge printing scenario, to local Edge devices.
- See the list of waiting print jobs and printed print jobs
- Delete print jobs
- Mark print jobs as favorite
- Add direct print queues to their workstations
- Manually select a site server

Features

Feature name	Pure cloud printing	Edge printing
Authentication	OpenID Connect	OpenID Connect
IPP authentication	Technically there's no authentication on the IPP receiver. However, when a job is submitted to the Spooler, the Spooler will request authentication (see above) from the Client.	
Job management • Mark jobs as favorite • Delete jobs • Inspect printed jobs	✅	✅
Direct queue deployment (by admin)	✅ Direct queues can be configured when creating the Client v3 installation package. Contact your service representative.	✅ Direct queues can be configured when creating the Client v3 installation package. Contact your service representative.
Direct queue deployment (by end user)	✅ The Client v3 must be in client spooling mode.	✅
Emergency Print (print to the last used MFD if server connectivity is unavailable)	❌	✅

Feature name	Pure cloud printing	Edge printing
Selecting billing codes	✗	✗
Shared print queues deployable by end users	✗	✗
Load balancing	✗	✗

Feature name	Pure cloud printing	Edge printing

Rule-Based Engine Notifications	⚠
	⚠ The notification will be displayed in user's Client v3 only under the following conditions:
	• Client v3 is in client-spooling mode
	• The user sent the print job to a queue that uses LPR port:
	  • Queues deployed via Client v3 installation package created in Quick Print
	  • Direct print queues deployed by the user via Client v3
	  • Direct print queues created manually by the user (see Manually creating direct print queues)
		⚠
		⚠ The notification will be displayed in user's Client v3 only under the following conditions:
		• Client v3 is in client-spooling mode
		• The user sent the print job to a queue that uses LPR port:
		  • Queues deployed via Client v3 installation package created in Quick Print
		  • Direct print queues deployed by the user via Client v3
		  • Direct print queues created manually by the user (see Manually creating direct print queues)

Finishing options	✅	✅

Limitations

The end user must already exist in the management interface (for example, they have performed self-registration via card). If not, they cannot manage jobs and queues in Client v3.

Supported languages

- Basque
- Brazilian Portuguese
- Chinese Simplified
- Czech
- Danish
- Dutch
- French
- German
- Hungarian
- Italian
- Japanese
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Slovenian
- Spanish
- Turkish

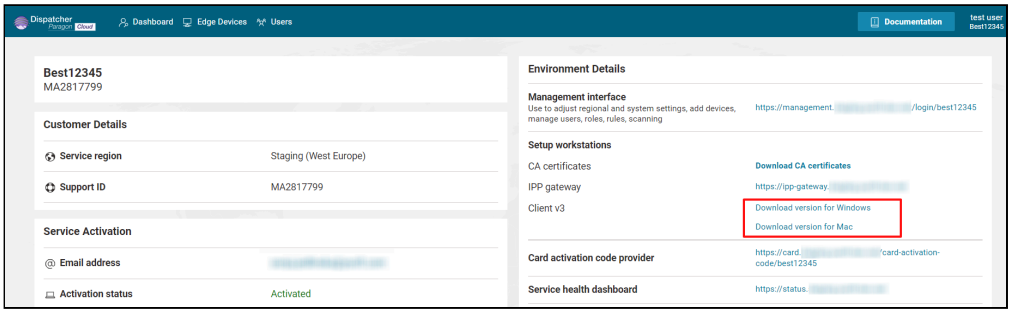
2.8.2 INSTALLATION

There are two methods of obtaining the installation package:

- Ask your service representative to create the installation package for your company. The package must be created with parameters specific to your company, such as your device gateway. After receiving the package, deploy it to the users' workstations.
- Download the installation package from the Dispatcher Paragon Cloud Portal and install it via an installation script. The package is not pre-configured for your company. You must enter the necessary configuration parameters during the installation process. We recommend this method for testing purposes only.

Installation via script

1. Log into the Dispatcher Paragon Cloud Portal.
2. Download the Client v3 package for your operating system.



3. If using Windows, unzip the package. If using Mac, open the disk image.
4. If using Windows, open PowerShell as administrator. If using MacOS, open Terminal.
5. Run the installation script with the following parameters in the directory where you unzipped the package/mounted the disk image.

Windows	Mac
-ServerSpoolerPorts <port numbers>	--serverspooler-ports <port numbers>
-JobServicePorts <port numbers>	--jobservice-ports <port numbers>
-SpoolerMode <mode>	--spooler-mode <mode>
-EnableManualSiteServerSelection	--enable-manual-siteserver-selection
-SiteServerSources <list of sources>	--siteserver-sources <list of sources>
-SiteServerHosts <device gateway addresses>	--siteserver-hosts <device gateway addresses>
-SiteServerAliases <aliases of gateway addresses>	--siteserver-aliases <aliases of gateway addresses>

Parameters:

- Spooler Options Mode – enter "ClientSpooling" or "ClientNonSpooling" depending on the Dispatcher Paragon Cloud architecture that you will be using.
- EnableManualSiteServerSelection – set it to "true" if you need traveling users to be able to select site servers (locations) manually.

- SiteServerSources – the list of sources from which Client v3 loads the site servers (print locations). The available options are:
  - Local - Client v3 includes site servers from its local configuration file into its site server selection pool. This is the default option when SiteServerSources parameter is not present in the configuration file.
  - RESSC - Client v3 includes site servers from the cloud (currently Azure) into its site server selection pool. If you wish to use this option, you must use it together with "Local."

    ```
    -SiteServerSources ["Local", "ressc"]
    ```
- SiteServers
  - Host – enter the device gateway address.
    - Pure Cloud printing: cloud spooler
    - Edge printing: the edge device to which the Client v3 will be sending print jobs
  - Alias – a user-friendly name of this device gateway. The end users will see this name when selecting a print location manually in Client v3.
- JobServicePort
  - Pure Cloud printing: port 443
  - Edge printing: port 5000
- ServerSpoolerPort
  - Pure Cloud printing: port 443
  - Edge printing: port 5002

Example for Pure Cloud printing (Windows):

```
powershell -executionpolicy unrestricted .\install.ps1 -ServerSpoolerPorts 443 -JobServicePorts 443
-SpoolerMode "ClientNonSpooling" -SiteServerHosts "cloudcustomer-tenant.eu1.dipa.cloud"
```

Example for Edge printing (Windows):

```
powershell -executionpolicy unrestricted .\install.ps1 -ServerSpoolerPorts 5002 -JobServicePorts 5000
-SpoolerMode "ClientNonSpooling" -SiteServerHosts "10.0.5.120" -EnableManualSiteServerSelection
-SiteServerSources "Local","ressc"
```

Example for Pure Cloud printing (Mac):

```
sudo ./install.rb --serverspooler-ports 443 --jobservice-ports 443 --spooler-mode ClientNonSpooling --
siteserver-hosts cloudcustomer-tenant.eu1.dipa.cloud --skip-print-queues
```

Example for Edge printing (Mac):

```
sudo ./install.rb --serverspooler-ports 5002 --jobservice-ports 5000 --spooler-mode ClientNonSpooling --siteserver-hosts 10.0.5.120 --enable-manual-siteserver-selection --siteserver-sources "Local","ressc" --skip-print-queues
```

2.8.3 UNINSTALLATION

Windows

To uninstall Client v3 installed via MSI (installation package customized for your company), perform the following steps:

1. Go to **Apps & features**.
2. Search for **Dispatcher Paragon Client**.
3. Click **Uninstall**.

To uninstall Client v3 installed via script, you can either use the above method or use the uninstallation script (*uninstall.ps1*). The script is located in the installation folder of the client application. Use the following command in PowerShell:

```
cd C:\DispatcherParagon\Spooler\
powershell -executionpolicy unrestricted .\uninstall.ps1 -Force
```

MacOS

The client application contains the uninstallation script – *uninstall.rb*. The script is located in the installation folder of the client application. Use the following command to run it.

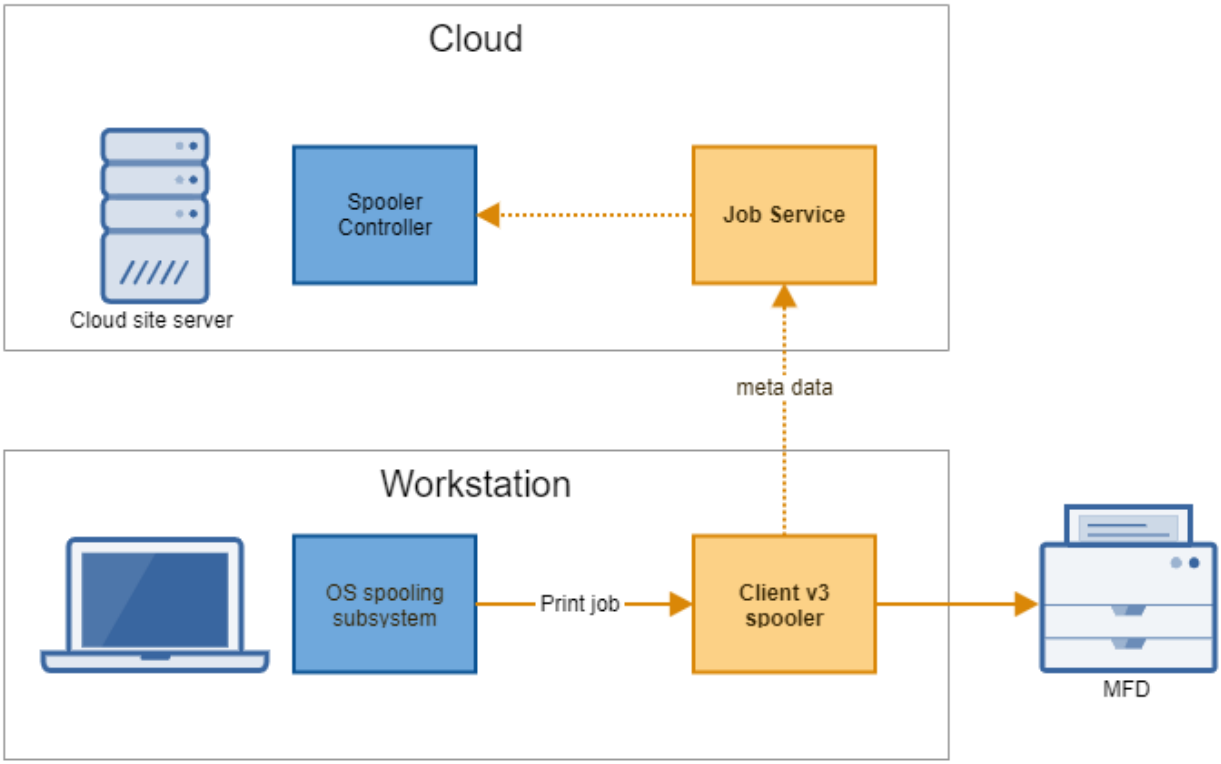
```
cd /Library/Application\ Support/YSoft.Spooler
sudo ./uninstall.rb --force
```

2.8.4 CLIENT V3 MODES

Client v3 can be configured in two modes:

- Client spooling mode – print jobs are stored locally on the workstation. Only metadata are sent to a Site Server. This mode cannot be used for IPP printing (submitting print jobs to IPP Gateway).
- Client non-spooling mode – print jobs, as well as metadata, are sent to a Site Server.

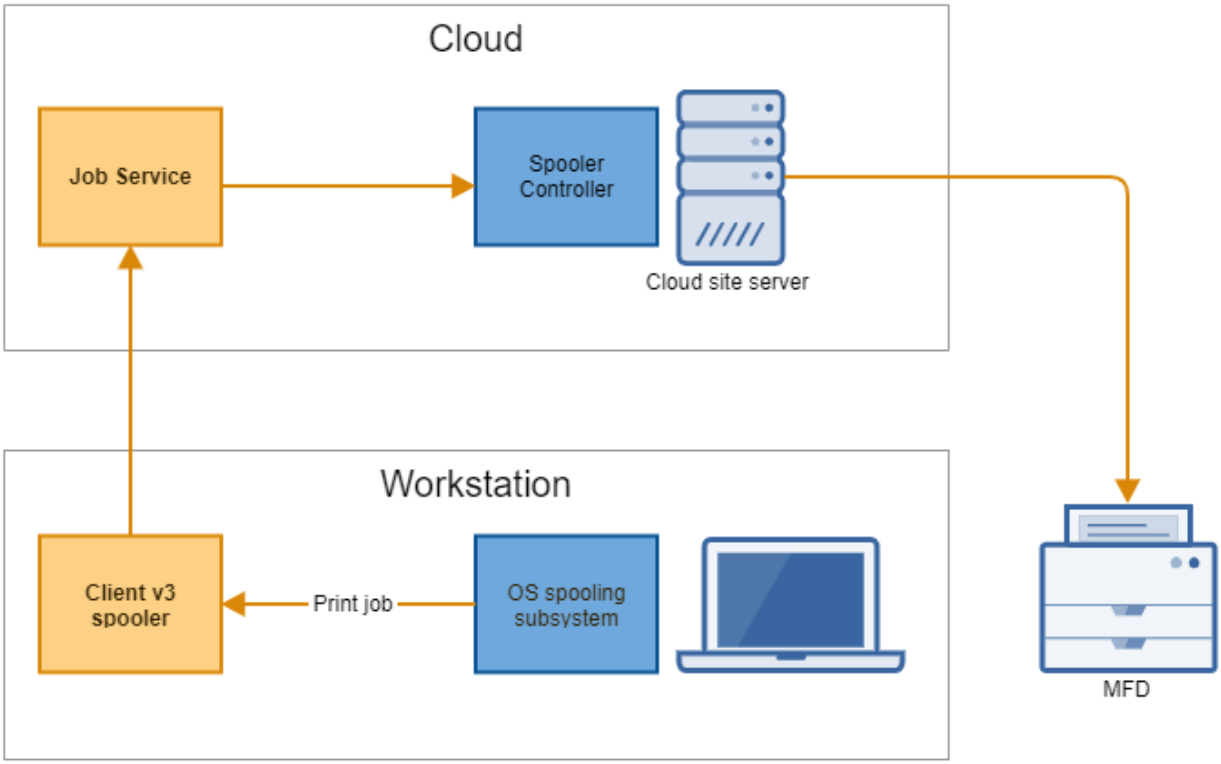
Client spooling mode



For the Pure cloud printing scenario, Client v3 must be client non-spooling mode. The only exceptions are users who are using reporting-only devices with direct print queues. In that case, Client v3 must be in client spooling mode.

In the Edge printing scenario, you can use Client v3 with reporting-only devices in both client-spooling mode and client non-spooling mode.

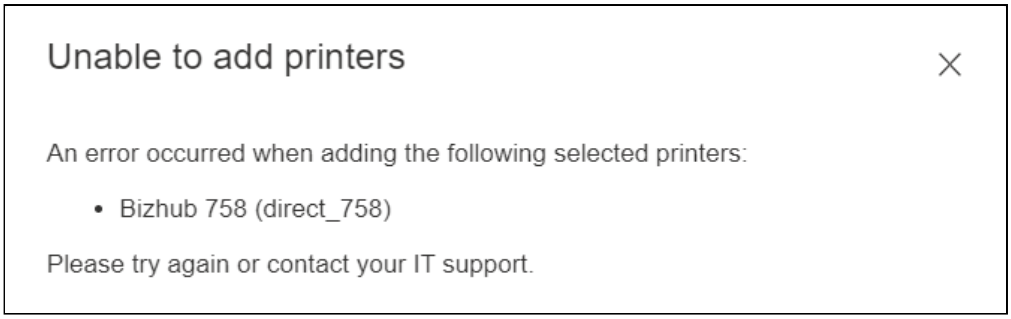
Client non spooling mode



2.8.5 DIRECT QUEUES

In both the Edge printing and Pure Cloud printing scenario, end users will be able to deploy direct queues on their workstation via Client v3 under the following conditions:

1. You have set up one or more reporting-only devices with a direct queue in the Dispatcher Paragon Cloud management interface.
2. The Client v3 must have information in its configuration file on what driver to use when deploying a printer. The driver must be installed on the workstation. Ask your service representative to add this information to the configuration file when they are creating the Client v3 installation package for your company.
   If the driver is not configured, the end user will receive the following error message when trying to deploy a direct print queue:



Users can also create a direct print queue manually, if, for example, they need to use a different print driver than the one specified in the Client v3 configuration. See the End user guide, chapter Manually creating direct print queues. Note that even in this case, they must have Client v3 installed since the direct queue uses a loopback address to send the print job to Client v3 and Client v3 then sends it to the reporting-only device.

2.8.6 EMERGENCY PRINT

Limitations

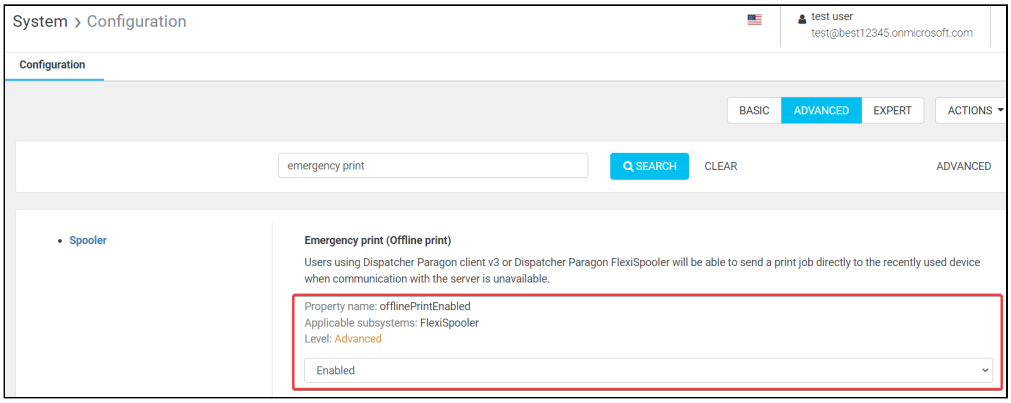
- Available only in the Edge printing scenario.
- Client v3 must be in client-spooling mode.
- MFDs must have the *Print without authentication* configuration option enabled.
- If there is IP filtering on the MFDs, it must be adjusted for communication with workstations using Client v3.
- User rights are not checked and rule-based engine rules are not applied.
- Accounting information is collected only if the MFD uses device dependent accounting.

Emergency print provides limited printing functionality while a site server is inaccessible. During an emergency print, Client v3 sends the print jobs directly to the printer, without needing to send them to the site server. The print jobs are printed immediately on the selected printer.

To enable emergency print for end users, perform the following steps:

1. Log into the Dispatcher Paragon Cloud management interface.
2. Click **System**.
3. Click **Advanced** to see all functions.
4. Enter *emergency print* into the search bar and click **Search**.

5. Set the *offlinePrintEnabled* property to enabled.



6. Click **SAVE CHANGES**.

7. Enable the print without authentication option on the MFDs. See Enabling Print without authentication option on Konica Minolta MFDs.

User roaming: manual site server (print location) selection

Ask your service representative to enable manual print location selection if the following conditions apply to your company

- You will be using Edge printing
- You have more than one location (i.e., more than one Edge device)
- Global print roaming will be disabled in your Dispatcher Paragon Cloud
- Some users in your company are traveling between locations

If the manual print location selection is enabled, the end users can access the **Print location** selection in the **Client settings** section of Client v3.

If the manual print location selection is disabled or the parameter is not specified at all, the print location selection is disabled in the **Client settings**. In this case, the print location is chosen automatically. This may cause problems in some Edge printing scenarios, therefore we recommend keeping the manual print location selection enabled.

⚠ Manual print location selection works only for queues deployed via the Client v3 installation package, not for queues that the user has added manually via the IPP URI generated at the IPP Gateway (*End user guide*, chapter Configuring IPP print queues).

Site server list

Client v3 can load the list of site servers from the Local configuration file or from the cloud.

If you wish the site servers to be loaded from Local configuration, provide the list of IP addresses and aliases of your Edge devices to your service representative so that they can enter it into the configuration of your Client v3 installation package. In this case, each site server must have an **Alias** defined, so that the end users see the site server names (aliases) in their Clients v3 in the **Print location** field, rather than IP addresses.

If you wish the site servers to be loaded from the cloud, provide the default site server (IP address, alias) for each of your locations to your service representative. The rest of your site servers will be loaded from the cloud. The users will see the same list that you can see in the Dispatcher Paragon Cloud Portal on the **Edge devices** tab.

Be aware that:

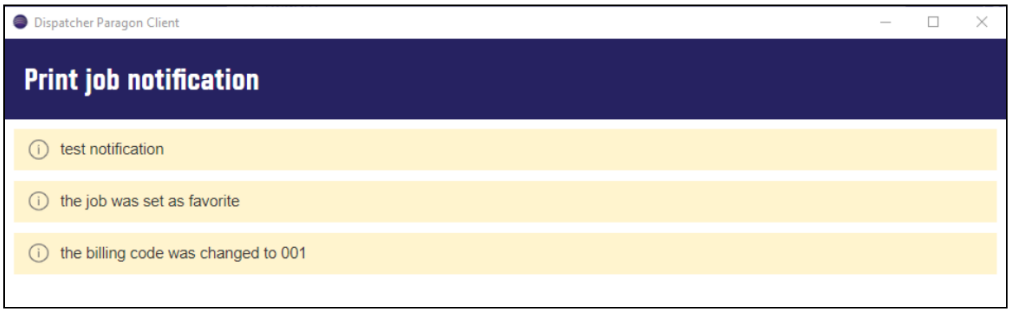
- if you deploy a correctly configured package to users in each location, they don't need to select the site server manually, unless they travel.
- traveling users must select a site server each time they change locations, regardless of whether they are traveling from their usual location or whether they are returning to it.

For the usage of manual site server selection, see the *End user guide*, chapter Using Dispatcher Paragon Client v3.

2.8.7 RULE-BASED ENGINE NOTIFICATIONS

For setting rules with notifications, see Creating and editing rules. For the list of available rules, see List of rule definitions.

The user will see the notification in a notification window until they close the window. If there are more notifications, they will be displayed in one window. Example:



2.9 DISPATCHER PARAGON CLOUD SERVICE HEALTH DASHBOARD

2.9.1 OVERVIEW

The Service Health Dashboard is a monitoring tool that performs regular checks on the availability of public cloud services. Its main purpose is to give partner admins and customer admins immediate information on possible downtime or issues in their region, without the need for contacting support.

The failure of each service may have different consequences for customers and partners. For example, **Cloud Portal** failure will prevent partner admins from creating new customers, but will not cause any problems for existing customers (unlike, for example, IPP gateway failure).

2.9.2 ACCESSING THE SERVICE HEALTH DASHBOARD

1. To access the Service Health Dashboard, click the following link:

   https://status.dipa.cloud/

2. Username and password are not required. The dashboard is publicly available.
3. You will see the Service Health Dashboard home page.
4. To display details the status of individual services, click the region where your Dispatcher Paragon Cloud is running.

   You can find the region in your *Welcome to Dispatcher Paragon Cloud* email.The link to Service Health Dashboard is also present on your dashboard in Dispatcher Paragon Cloud Portal.

2.9.3 MAIN SERVICES

After clicking your selected region, you can see the real-time status of the main services (ONLINE or OFFLINE), their history, and the calculated average uptime and response. The maximum data retention period is 90 days. Failure dates are indicated on the graph in red.

To see the failure date, hover over the red bar(s).

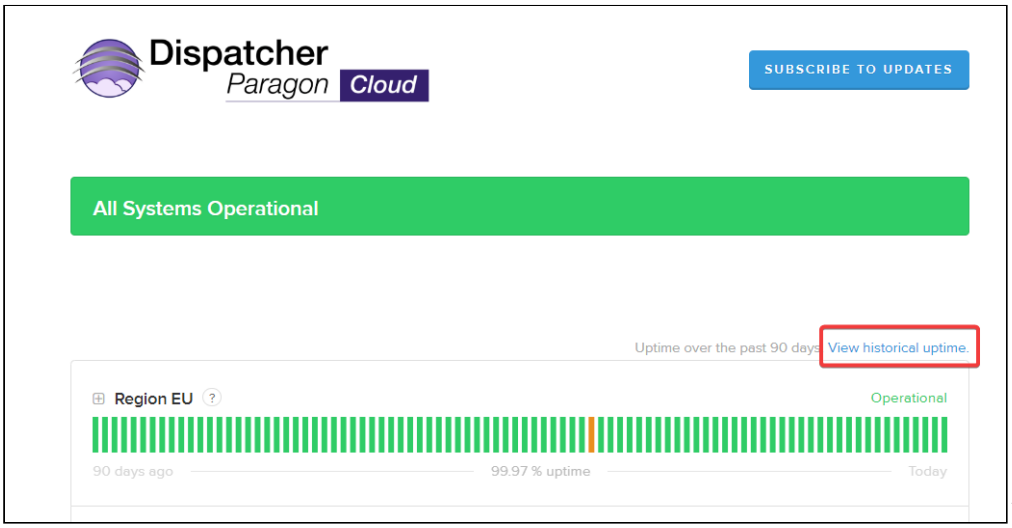
Failures

Service name	Failure consequence
Certificate Issuer	Partner admins can create new customers but certificates for a secure connection between the Site server and Management interface will not be issued. The Site server in the Management interface is offline and therefore customers will be unable to work with MFDs. Existing customers will be unaffected.
Site Server Deployer	Partner admins cannot create new customers in the Dispatcher Paragon Cloud Portal. The deployment will end in an error. Existing customers will be unaffected.

Service name	Failure consequence
Tenant Service	Partner admins cannot log into the Dispatcher Paragon Cloud Portal and create new customers there. Existing customers will most likely be affected and unable to log into the IPP gateway, Card Activation Code Provider (CACP) page, and other resources via Single sign-on (SSO).
Cloud Portal	The Dispatcher Paragon Cloud Portal is unavailable, and therefore partner admins cannot create new customers.
Identity Management	Partner admins cannot log into Cloud Portal and create new customers. Existing customers will most likely be affected and unable to log into IPP gateway, Card Activation Code Provider (CACP) page, and other resources via Single sign-on (SSO).
Card Activation Code Provider	The end users cannot generate new card activation codes or use already generated codes.
Management interface	The Management interface is unavailable. Partner admins cannot create new customers in Cloud Portal (deployment fails). For existing customers, Dispatcher Paragon Cloud may still work for some time but customer admins cannot change any of their settings until the Management service has been fully restored.
IPP Gateway	End users cannot send new print jobs to the cloud. They can only release existing ones. The IPP gateway page is unavailable and users cannot generate IPP URIs to install new printers on their PCs.

2.9.4 HISTORICAL UPTIME

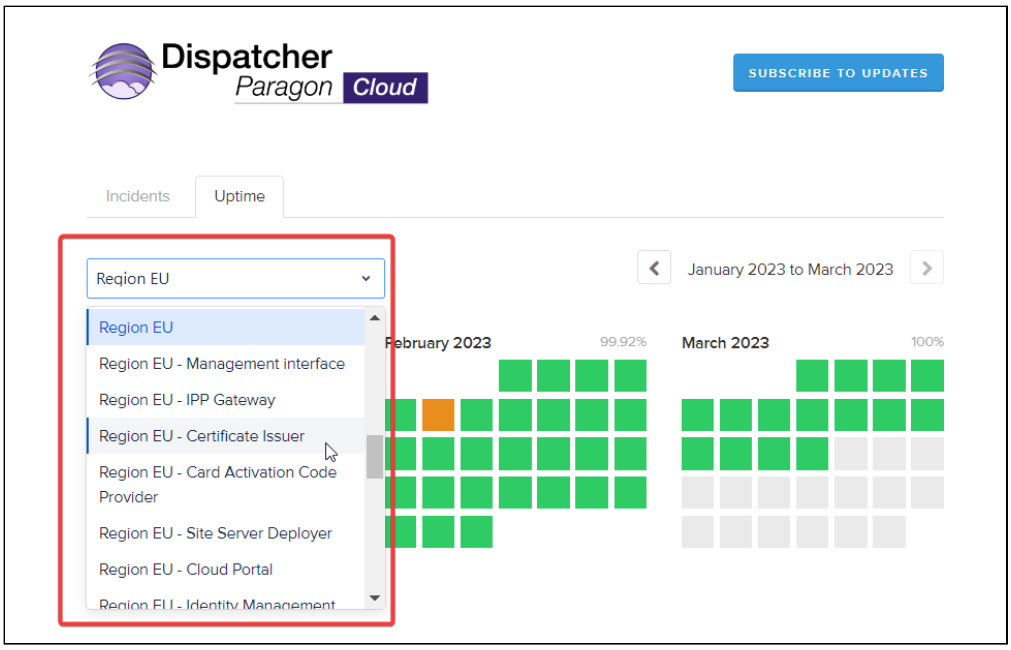
In the upper part of the Service Health Dashboard, click **View historical uptime**.



You will see the **Uptime** tab by default.

Uptime

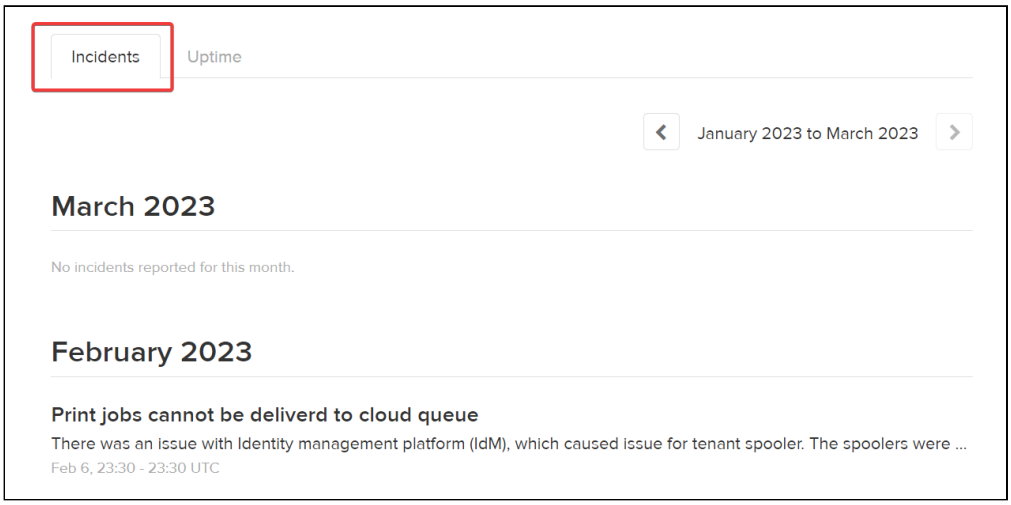
1. In the drop-down menu, you can either select whole region that you wish to see or the region and the service you wish to see.



2. Select the timeframe to display.

Incidents

1. Click the **Incidents** tab to see details regarding past incidents.



2. Select the timeframe to display.

For more information on Atlassian status page, see https://support.atlassian.com/statuspage/docs/display-historical-uptime-of-components/.

2.10 CLOUD FAX CONTROL PANEL GUIDE

2.10.1 GETTING STARTED

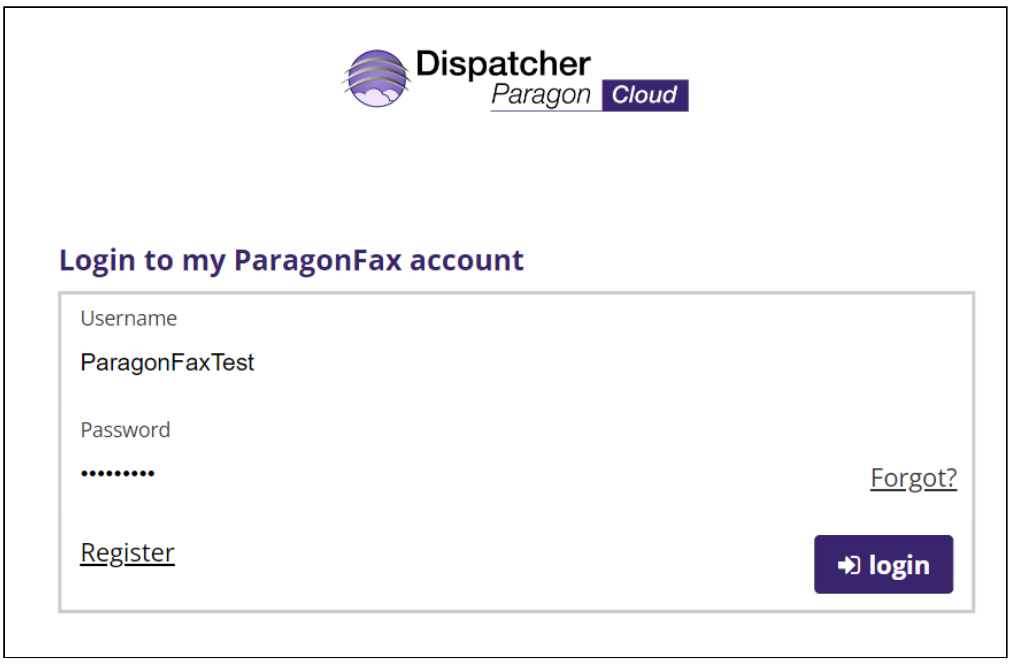
The Dispatcher Paragon Cloud Fax service is a high-capacity, reliable, and globally accessible service that enables the transmission and reception of faxes from an easy-to-use web portal or a Konica Minolta MFD. Cloud Fax is easy to install whether your business needs faxing capabilities from a single location, company campus, or multiple offices worldwide. Whether you need to allow faxing from one desktop or one thousand, Cloud Fax is designed to meet your requirements.

2.10.2 THE CLOUD FAX CONTROL PANEL

The Control Panel is a web portal that allows you to log in and access the services assigned to users, such as sending, receiving, and viewing faxes, and acting as a portal for Account Managers to amend the account and user settings.

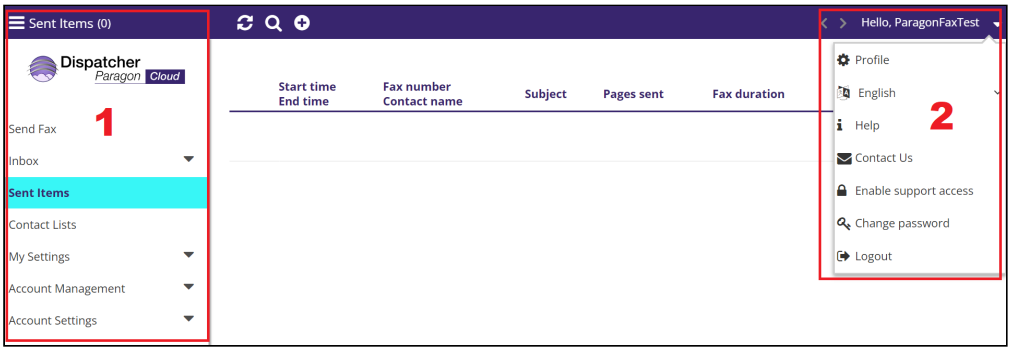
Logging in to the Control Panel

Ask your service representative/customer support to provide you with credentials for the Control Panel. Once you have them, enter your username and password to log in to Control Panel.



Navigating the Control Panel

Two main sets of menus in the Control Panel allow access to the various sections: the Navigation Menu on the left (Item 1 as shown below) and the User Menu on the right (item 2 as shown below).



The Navigation Menu

The Navigation Menu is the main menu for moving between the services available in the Control Panel. The menu can be expanded or collapsed using the 'three horizontal lines' button at the top. The following links may be found depending on your assigned services or user privileges.

- **Send Fax:** This allows users with the **Send fax** service to use the sending fax web form to submit faxes.
- **Inbox:** Gives you access to your received faxes, which you can open for viewing in the Document Viewer. Expanding the sub-menu lets you access Archived items and Trash.
- **Sent Items:** Gives you access to your sent items.
- **My Settings:** Gives you access to your user settings.
- **Account Management:** Gives Account Managers access to user management options and billing information.

- **Account Settings:** Gives Account Managers access to account information and security settings.

The User Menu

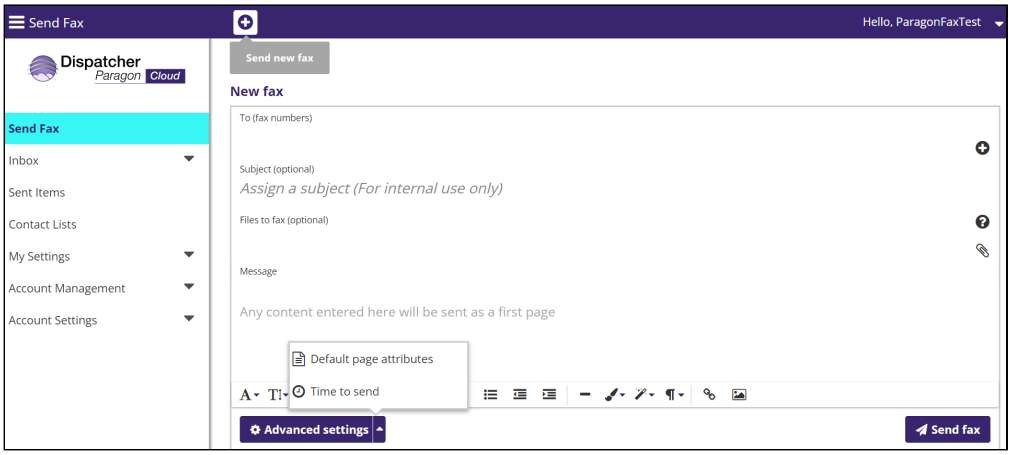
The User menu gives you quick access to commonly used links. The menu works as a drop-down, triggered by the down arrow link at the top of the page. The following links may be found:

- **Profile:** Quickly access your profile page, where you can update your details and change your password.
- **Language Selection:** Quickly change the selected display language.
- **Help Center:** Access support sections with FAQs, how-to's, and general support.
- **Contact Us:** Contact the support team in your region.
- **Change password:** Change your current password.
- **Log Out:** Log out of your current session.

Fax from the Control Panel

All users with the Send Fax service can log in to the Control Panel and send faxes quickly and easily using a simple web form. The form allows you to send faxes to multiple recipients, assign subjects for internal use, and attach files. It also provides advanced options for fax transmission. See the *Contact Lists* section if you wish to broadcast to multiple recipients.

1. In the Navigation Menu, click **Send Fax**.



2. Click the **+** icon on the right-hand side of the **To (fax numbers)** field to open the **Add new contacts to fax** window.
3. You can add the contact's name for your reference in the Contact name field.
4. Add the fax number you wish to send the fax to in the **Fax number** field, ensuring the number is formatted correctly. For more information regarding the correct formatting of fax numbers, see Fax Number Formats.
5. Click **Add** to return to the Send Fax form.

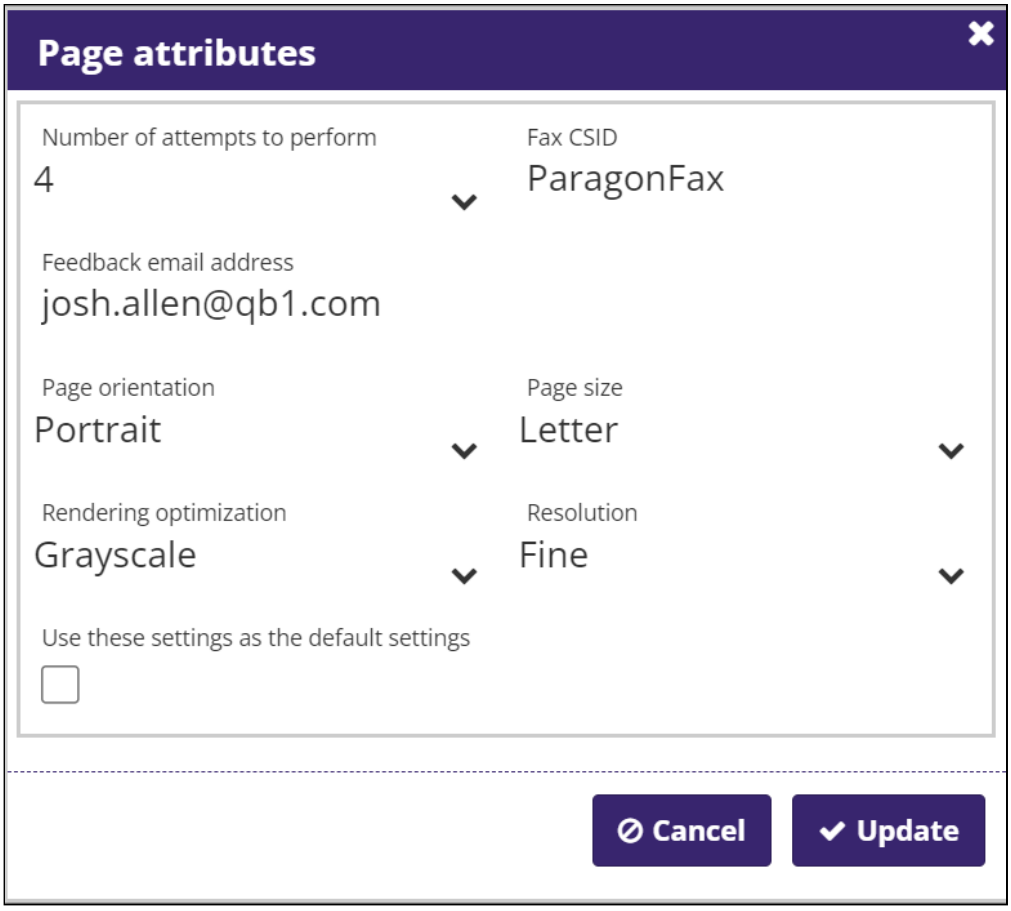
6. Select the contact list from the Recipients drop-down to send a fax to a contact list. See Contact Lists for more information.

7. To add one or more attachments to be faxed, click the **Files to fax** field to open your local file explorer, where you can locate and select the files to be attached.

8. To add a first (or cover page) to your fax, you can enter the information to be faxed in the **Message** field and use the formatting options along the bottom.

9. By default, the settings for sending a fax using the web form are taken from your user settings; however, you can tweak these options before sending a fax by clicking **Advanced Settings**. The following options are available under Advanced Settings:

   Default page attributes



The number of attempts to perform: The number of attempts to perform in cases of fax transmission failure.

Fax CSID: Your identification as seen in your outgoing fax.

Feedback email address: An optional email address to which feedback messages are sent.

Page orientation: Specify landscape or portrait page orientation for the transmission.

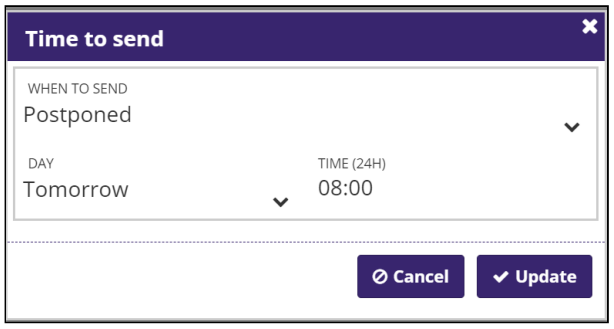
Page size: Specify the page size to be transmitted (A4, Letter, Legal, B4).

Rendering optimization: Specify whether to render documents in black and white or greyscale.

Resolution: Specify standard or fine resolution for the transmission.

Use these settings for all faxes: Select this check box to quickly update settings to save and reflect those used for this transmission.

Time to send



Time to Send allows users to specify whether to submit the fax immediately (ASAP) or to delay submission of the fax into the system for up to 14 days. Simply change the **When to send** drop-down to **Postponed**, select a future date and time for submission, then click **Update**.

10. When you are happy with the information to be faxed and the required settings, click **Send fax** to submit the fax into the cloud fax systems for sending.

    You will be prompted with a confirmation window. Click **Send new fax** to compose new fax, **Sent items** to track the status of your submissions, or click **OK** to be returned to the form you just submitted.

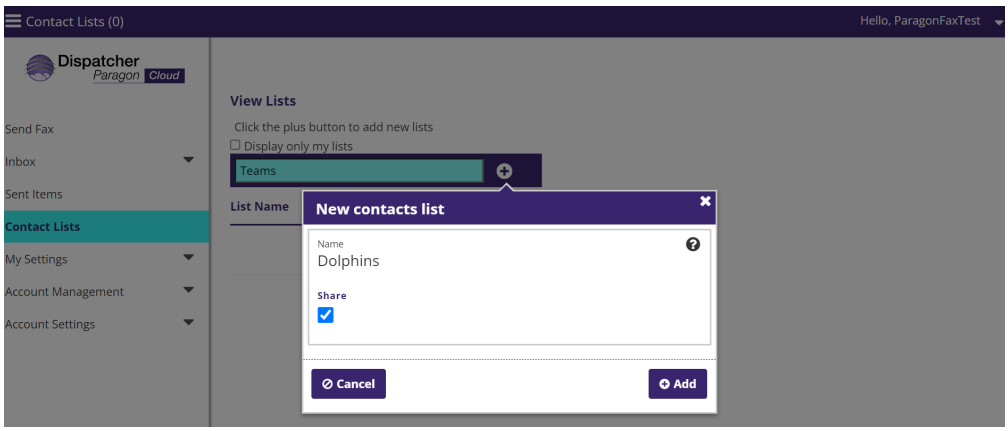
Contact Lists

Cloud Fax's contact lists management allows users to send static or dynamic faxes to lists of contacts rather than single transactions to individual contacts. Contact lists make it possible to send faxes to up to 20,000 contacts in a single transaction. In any broadcast, two items are required, the fax to be broadcast and a list of recipients. The sent fax can either be static (meaning

each recipient in the list receives the same fax) or dynamic (meaning every recipient receives personalized fax featuring merged fields).

Create a new contact list

1. In the Navigation Menu, click **Contact Lists**.
2. You will be prompted to create a new list if you have not made any lists. Otherwise, click the **Add a New list** (+) icon in the **View Lists** section.
3. In the **New contacts list** window, assign a unique name to your list and choose whether to share the list with other users under the same account.



4. Click **Add**.

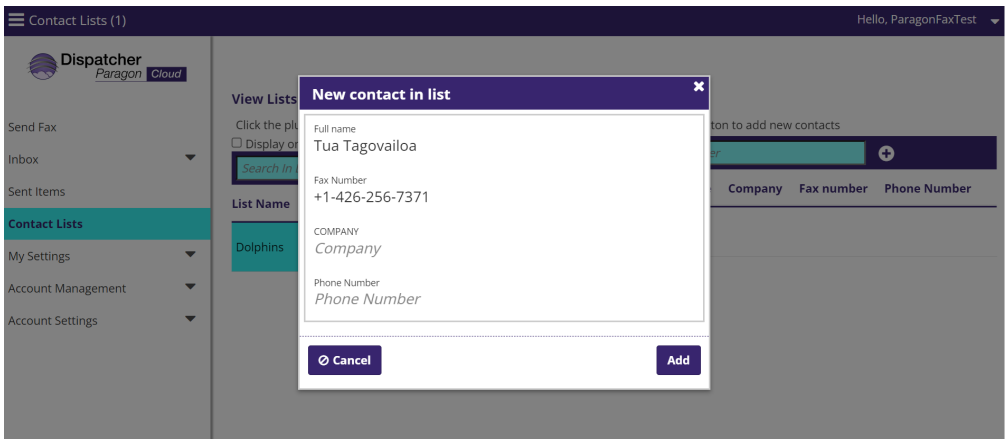
Now you can add contacts to the list you have created.

Add contacts to a list.

Once you have created a list, you will need to add contacts. You can upload a file of contacts to be imported or manually add contacts. You can simultaneously add and send up to 20,000 contacts and remove or edit contacts in existing lists.

Manually add contacts

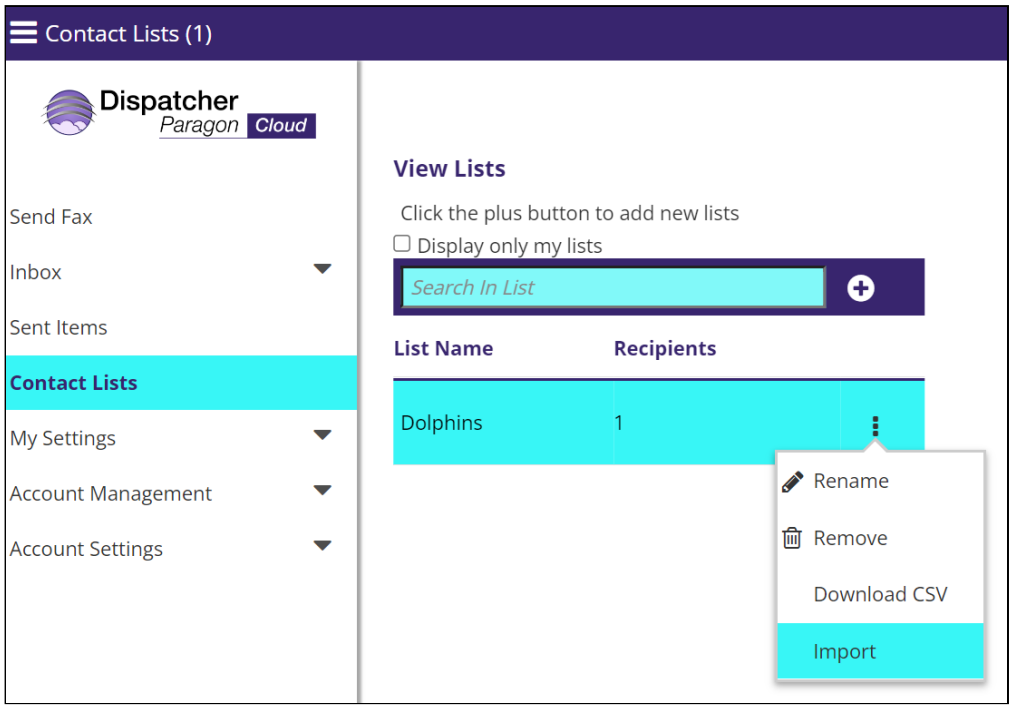
1. Select the list to which you want to add contacts in the **View Lists** section.
2. If you have not added any contacts to the list, you will be prompted to add a new contact. Otherwise, click the **Add a new contact to list** (+) icon in the **[** *List Name* **]** section.
3. In the **New contact in the list** window, enter the information for the contact.



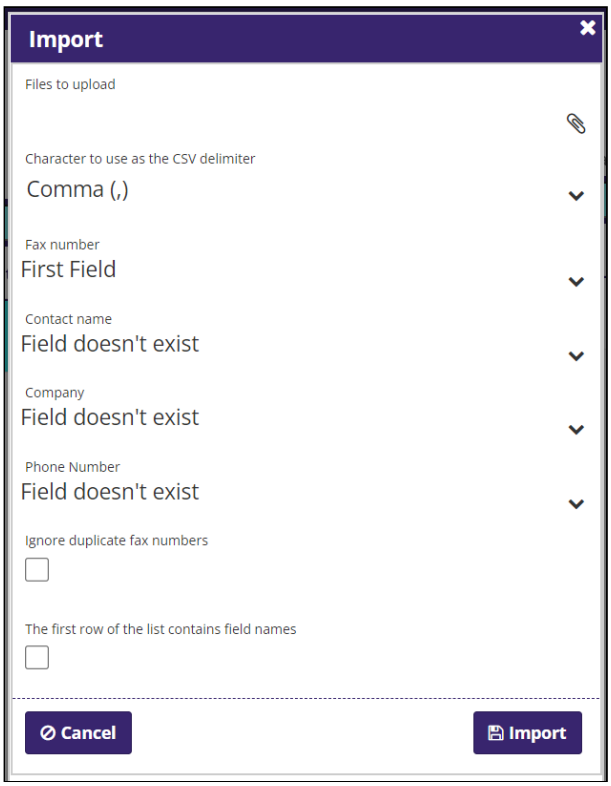
4. Click **Add**.

Import contacts from a file

1. In the **View Lists** section, click the three dots next to the list you want to import contacts to, then select **Import** from the drop-down menu.



2. In the **Import** window, select import options, then click **Import**.



Files to upload: Opens the File Explorer. Navigate to and select the file(s) you wish to import.

Character to use as the CSV delimiter: Specify whether the imported file fields are separated by comma (,) or semicolon (;).

Fax Number / Contact Name / Company / Phone Number: Define the order in which the fields appear within the file you wish to import.

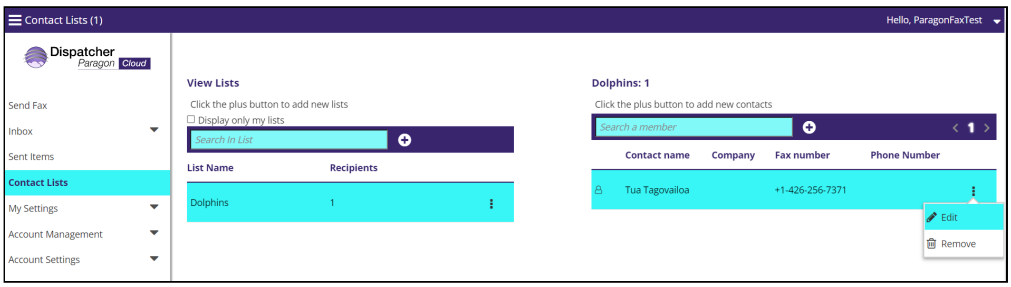
Ignore duplicate fax numbers: Select whether or not to ignore duplicate entries in the Fax Number column.

The first row of the list contains field names: Define whether or not the file contains the first row of headers.

Edit a contact

It is possible to edit the details of an existing contact within a list of contacts.

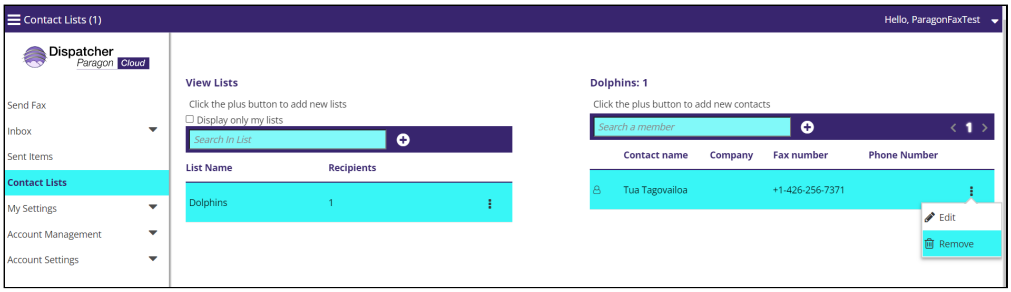
1. Select the list that contains the contact you want to edit in the **View Lists** section.
2. In the **[** *List Name* **]** section, click the three dots next to the contact you want to edit, then select **Edit** from the drop-down menu.



3. Edit contact details, then click **Update**.

Remove contacts from a list.

1. Select the list that contains the contact you want to delete in the **View Lists** section.
2. In the **[** *List Name* **]** section, click the three dots next to the contact you want to delete, then select **Delete** from the drop-down menu.



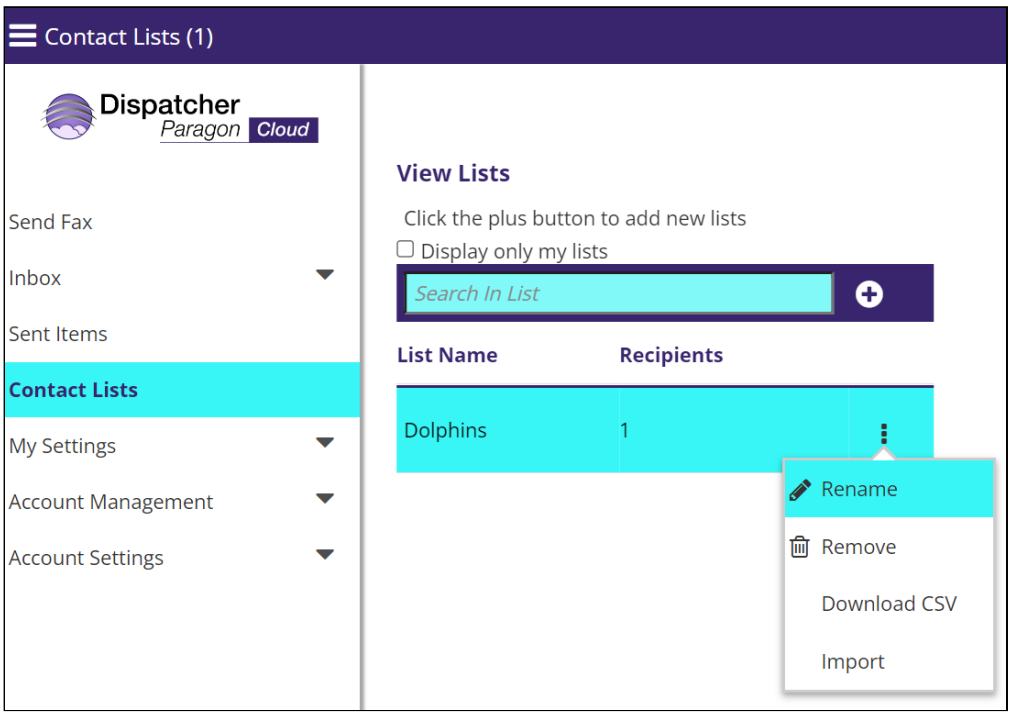
Export contacts list to file.

Exporting a list of contacts to file in CSV format is possible.

1. In the **View Lists** section, click the three dots next to the list you want to export to, then select **Download CSV** from the drop-down menu.
2. Select a local download location, then select **Save**.

Rename a list

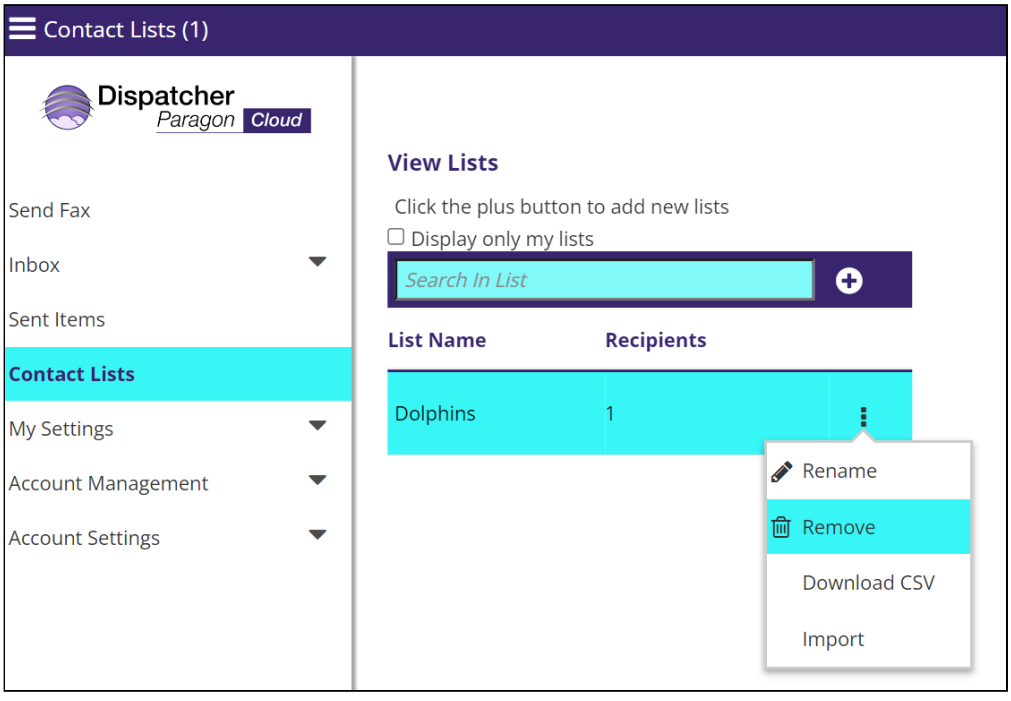
1. Click the three dots next to the list you want to rename in the View Lists section, then select **Rename** from the drop-down menu.



2. Enter a new name for the list, then click **Update**.

Delete a list

1. In the **View Lists** section, click the three dots next to the list you want to delete, then select **Remove** from the drop-down menu.



Search for a list or contact. The search boxes at the top of each section make it possible to search for specific lists or a contact within a selected list. Once you type at least two letters, suggestions will be filtered.

Fax number formats

Cloud Fax is designed to be similar to dialing a standard fax machine. The principle is to specify a fax number as if you were dialing it from a traditional telephone; however, you may add access codes (long-distance, international), country, and area codes. If no explicit access codes or prefixes are specified, Cloud Fax will automatically add them according to your user settings.

For reading convenience, a fax number may contain special characters such as hyphens, parentheses, etc. Any non-digit character is ignored, except for a plus sign (+) used as a generic International Access Code. Fax numbers that contain brackets need to be written as a quoted string.

Safest format

If you are not sure what your user settings are, simply use the following standard international access notation:

+(country code)(area code)(fax number)

For example: +1-212-9876543 or +44-208-1234567

Other international fax number examples

Example 1

(User configured to dial from New York, NY, USA)

Faxing from the USA to the UK:

Option 1: +44 161 999 8888

Option 2: 011 44 (161) 999 8888

Note: A US-based user (as defined by account) can dial the US-specific international access code 011.

Faxing to another area within the United States:

Option 1: 14089998888

Option 2: +1 (408) 999 8888

Faxing to another number within New York:

Option 1: 222 8888

Option 2: 1-212-222 8888

Option 3: “+1 (212) 222 8888”

Example 2

(User configured to dial from London, UK)

Faxing from the UK to the USA:

Option 1: +1 212 999 8888

Option 2: “001 (212) 999 8888”

Note: A UK-based user (as defined by account) can dial the UK-specific international access code 00.

Faxing to another area within the UK:

Option 1: 01619998888

Option 2: +44 (161) 999 8888

Faxing to another number within London:

Option 1: 222 8888

Option 2: 1-212-222 8888

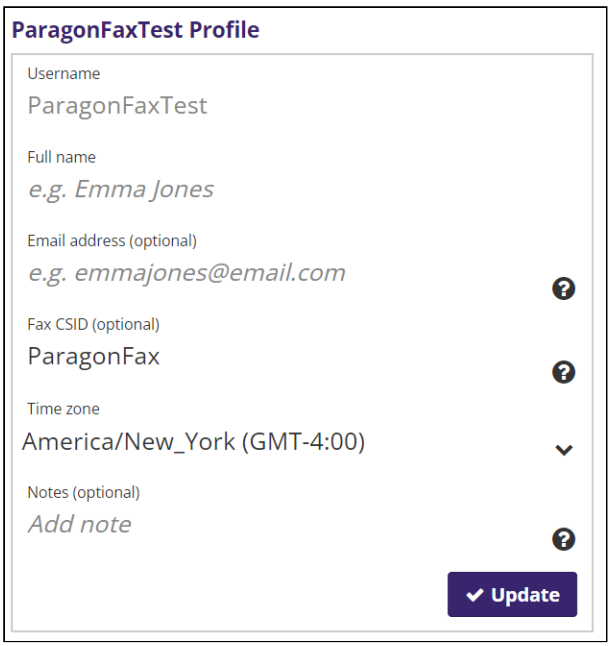
Option 3: “+1 (212) 222 8888”

My Settings

All users have a My Settings menu option, which gives you access to the options available and information about any services and the available options for those services.

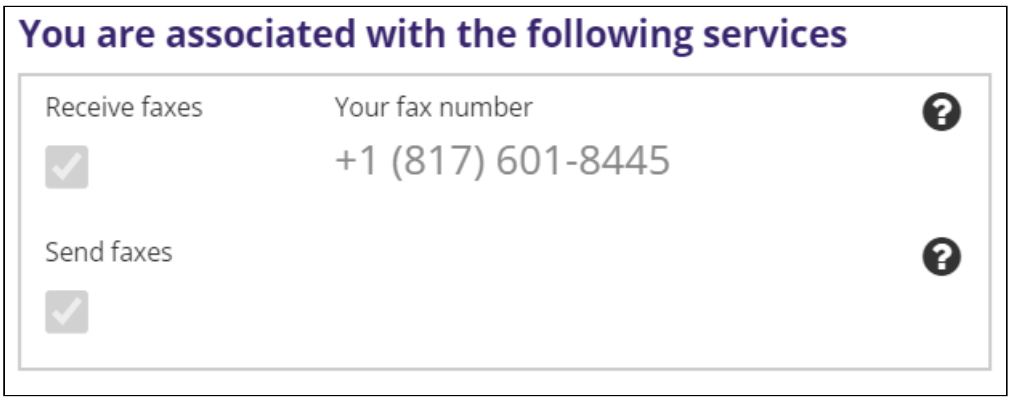
My Profile

The My Profile page lets you update your details, including name, email address for communications, a unique CSID for outgoing faxes, and select your timezone. These are user details and are separate from account-level information.



My Services

The My Services page shows the services (send or receive faxes) assigned to you. You will also find the fax number associated with your user if you have an inbound fax service.



See Services for more information.

Incoming Options

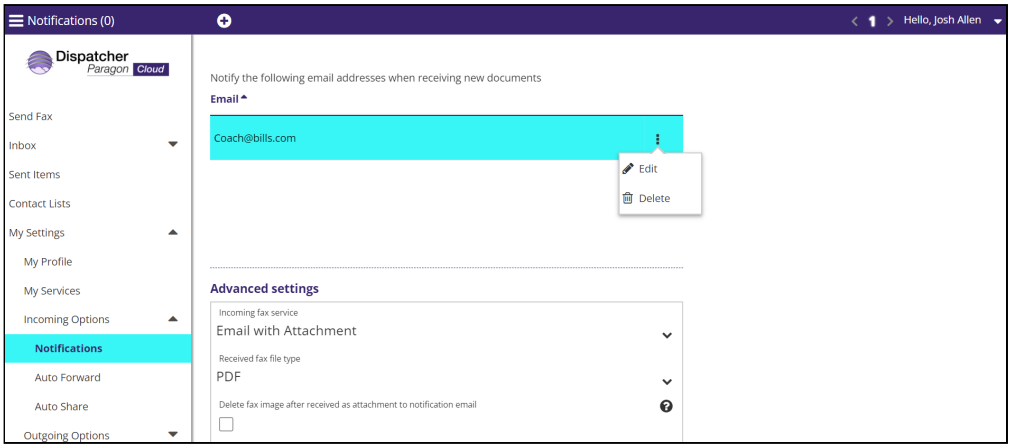
This menu item will only be available to active inbound faxing service users.

Notifications

You can receive fax to multiple email addresses simultaneously. Under Notifications, you can add and remove additional email addresses where faxes are sent.

1. Click the **Add email address** (+) icon.
2. In the **Add email address** window, enter the email address you want to add.
3. Click **Add**.

4. Once added, email addresses can then be edited or deleted via the menu on the right-hand side of the entry in the list.



Auto Share

You can use the Auto Sharing feature to automatically share received faxes with one or more users or groups of users under an account. Individual users may create and change the Auto Sharing settings, which apply only to received faxes (received items the user is the owner). Instead of sharing each fax manually, with auto-sharing, you can share all of your received faxes in just a few steps.

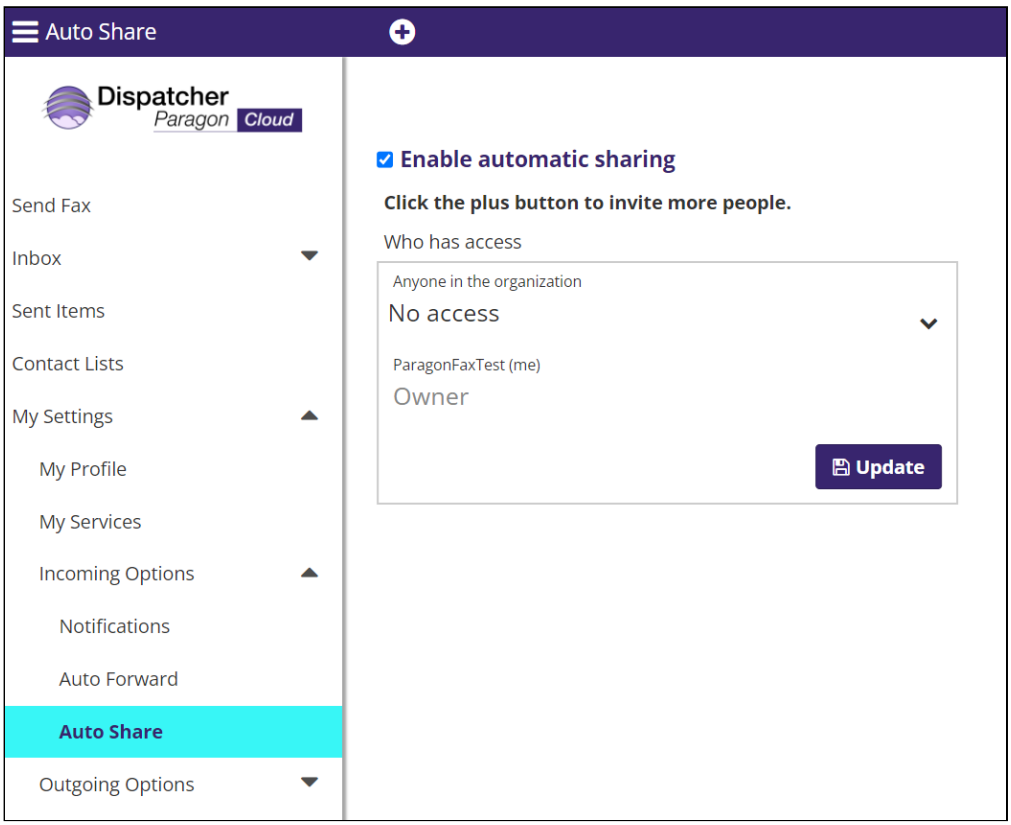
Enable auto-sharing of received documents

1. Log in to the user whose documents you would like to auto-share.

   Account Managers can log into individual users by navigating to **Account Management** / **Users**.

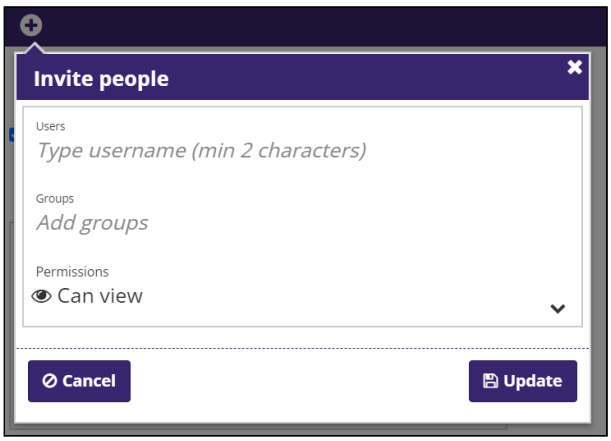
2. Click **My Settings**, **Incoming Options**, and **Auto Share in the Navigation Menu**.

3. Select the **Enable Automatic Sharing** check box.



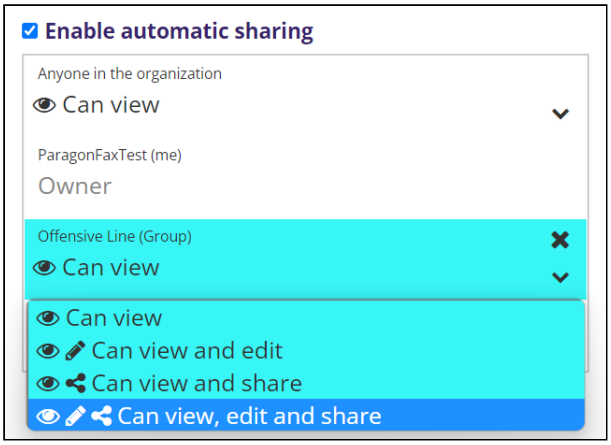
Now that automatic sharing is enabled, you can specify access to received items for all users under the account using the "Anyone in the organization" setting and add new users or groups of users to auto-share documents.

1. Click the **Invite people** (+) icon.
2. In the **Invite people** window, specify the user or group with which you want to auto-share faxes. Once you start typing, suggested users or groups will be displayed.
3. Assign the desired permission level for the user or group. The following options are available:
   - Can view
   - Can view and edit
   - Can view and share
   - Can view, edit, and share



4. Click **Update**.

Once added, you will see the new entry in the Auto Sharing list, and you can amend permissions by clicking the 'Down' arrow on the right-hand side of its entry in the list or deleted by clicking the **X** icon.



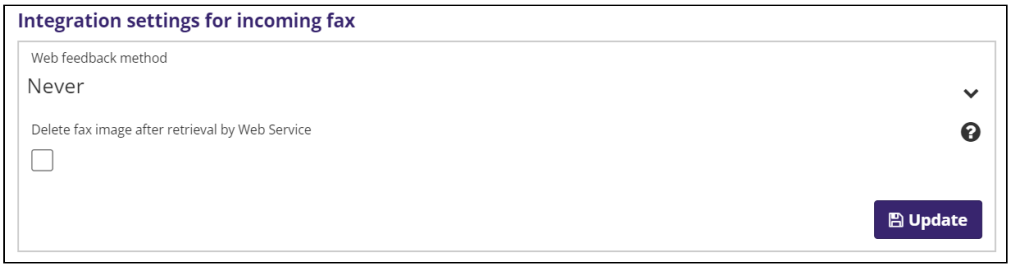
Outgoing Options

This menu item will only be available to active outbound faxing service users.

Integration Settings

Allows developers to connect through their environments to define additional inbound and outbound faxing settings.

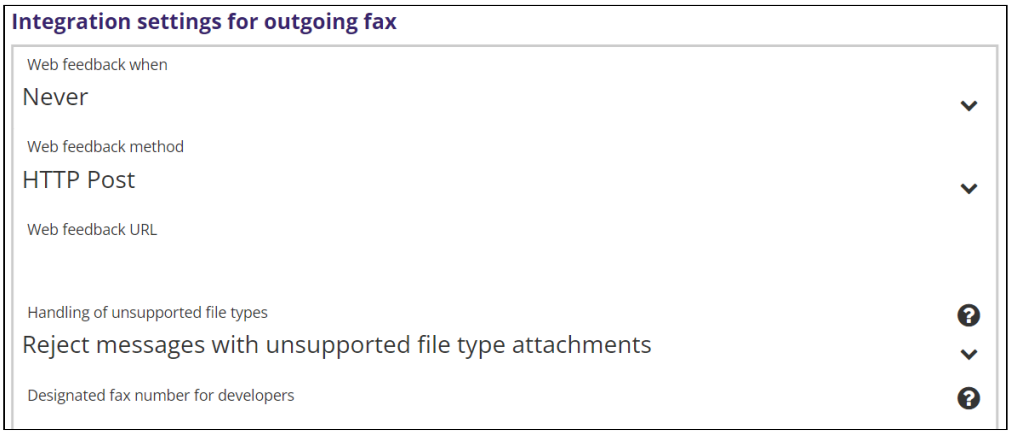
Integration settings for incoming fax



Web feedback method: You can specify a default notification method for inbound faxes. You can select to never receive notifications, receive by HTTP Post or XML web service.

Delete fax image after retrieval by Web Service: This allows you to permanently remove fax images and precursor documents from our servers after being retrieved so that any sensitive data cannot be exposed.

Integration settings for outgoing fax



Web feedback: This allows you to specify the conditions under which feedback is sent via the web service for outgoing fax transmissions. The following options are available:

- **Always:** Feedback will be provided for all fax transmissions, regardless of the transmission status.
- **Never:** No feedback will be sent regarding the status of outgoing fax transmissions.
- **On success:** Feedback will only be sent for successful fax transmissions. Feedback will not be sent for faxes that fail to transmit.
- **On failure:** Feedback will only be sent for failed fax transmissions. Feedback will not be sent for faxes that transmit successfully.

Web feedback method lets you specify what format feedback is sent in. You can select between HTTP Post and XML web service.

Web feedback URL: The URL for the web service feedback to connect to.

Handling of unsupported file types: – Allows you to specify whether or not the system should disregard unsupported file type attachments when processing outgoing fax transmissions.

Note: This option affects both web service and emails to fax services.

Services

To manage services, please contact your dealer.

2.10.3 ACCOUNT SETTINGS

AA range of options available at an Account level can be personalized to suit your needs. Only Account Managers have access to Account Settings.

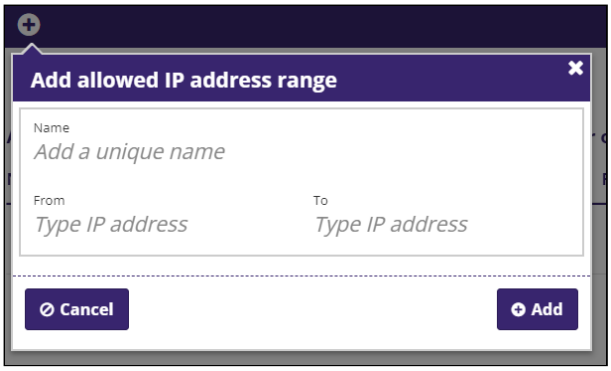
Account Information

Allows Account Managers to view and update the contact information held.

Allowed IP Addresses

Account Managers may add IP address ranges to restrict access to an account. The access restrictions also apply to the API web service. **Caution:** Make sure to allow your IP address first. Otherwise, you will lock yourself out of your account.

1. Log in as an Account Manager.
2. In the Navigation Menu, click **Account Settings and Allowed IP Addresses**. This page lists all IP addresses with access restrictions in your account.
3. Click the **Add allowed IP address range** (+) icon.

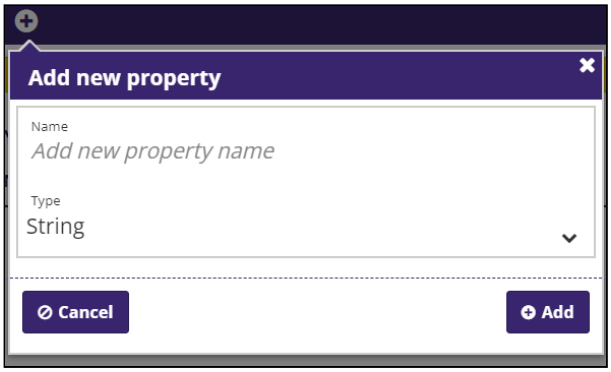


4. Give an identifier to the access restriction in the **Name** box.
5. To allow access from a single IP address, type the same IP address in the **From** and the **To** boxes. For example: From – 62.219.162.162, To – 62.219.162.162.
6. To allow access from a range of IP addresses, type the lower IP address in the **From** box and the higher IP address into the **To** box. For example: From – 62.219.62.54, To – 62.219.62.58.
7. Click **Add**.

Customized Properties

Each fax in your Inbox has several properties: time received, number of pages, shared time, and owner. Faxes can be further organized by adding tags, a unique reference, a fax name, and/or customized properties. Account Managers can define up to 10 additional customized properties for an account.

1. Log in as an Account Manager.
2. In the Navigation Menu, click **Account Settings**, then click **Customized Properties**.
3. Click the **Add new property** (+) icon.
4. In the **Add new property** window, assign a name to the new property and define the property type (string, date, or numeric).



5. Click **Add**.

   A notification will be displayed with the result of adding the property. If added successfully, you will be able to locate the property in the list and edit the property itself.

Control Features

Allows Account Managers to enable/disable features for inbound faxes. All capabilities are enabled by default.

1. Log in as an Account Manager.
2. In the Navigation Menu, click **Account Settings**, then click **Control Features**.
3. Enable or disable features as needed, then click **Update**. The following options are available:

Option	Description
Delete documents	Select this option to enable the "Delete document" option in the Inbox and Document Viewer for all users in the account.
Print received documents	Select this option to enable the "Print document" option in the Document Viewer for all users in the account.

Option	Description
Download received documents	Select this option to enable the "Download Document" option in the Document Viewer for all users in the account.
Auto forward documents	Select this option to enable the "Auto Forward" option in My Settings > Incoming Options for all users in the account.
Blackout sensitive content in documents	Select this option to enable the "Blackout" option in the Document Viewer for all users in the account.
Auto share documents	Select this option to enable the "Auto Share" option in My Settings > Incoming Options for all users in the account.
Share documents	Select this option to enable the "Share" option in the Inbox and Document Viewer for all users in the account.
Get email notifications for received documents.	Select this option to allow users to set notification emails for received faxes.
Display sender email address	Select this option to display the sender email address of received emails in the Inbox "Sender" column, the "More Details" popup, and the received email's header.
Change language	Select this option to allow users to change the user interface language.

Storage Policy

Allows Account Managers to set the fax storage period according to the fax's received time.

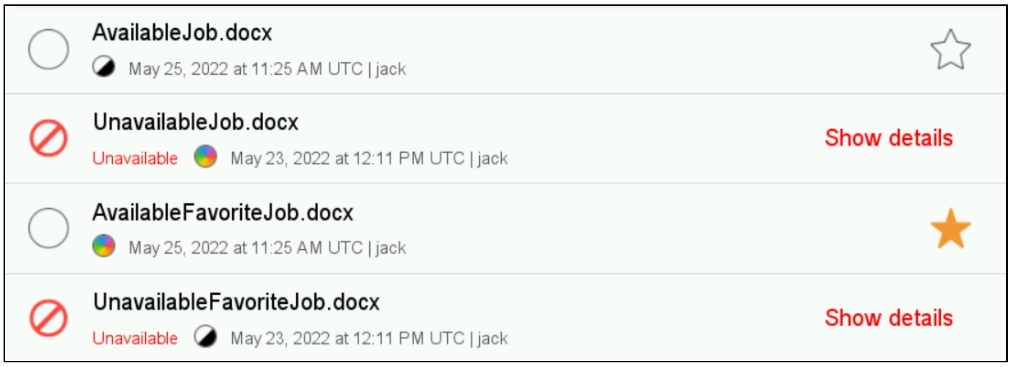
2.11 TROUBLESHOOTING

2.11.1 PRINT JOB ROAMING

Problem description: roamed print jobs cannot be printed

Possible root causes and solutions:

- The periodic job metadata synchronization hasn't yet occurred.
- The job data was not yet uploaded to the cloud, this may be because of a large job or a slow Internet connection.
- The cloud is not accessible because of a network or other failure.
- The print job was submitted via Client v3 in client spooling mode and accessed at the Cloud Terminal. In this case, the print job shows as unavailable. Solution: instruct the user to release the print job at an MFD with Embedded Terminal.

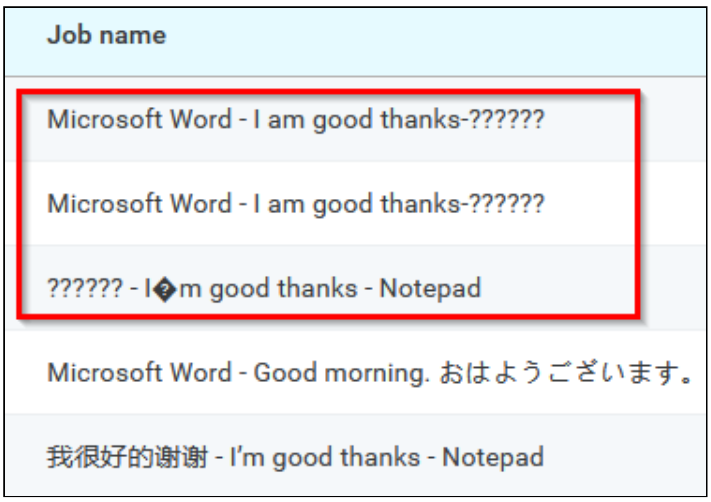


2.11.2 UNEXPECTED CHARACTERS IN JOB TITLE

Problem description: In Microsoft Windows, if a job is printed via LPR, the job title can display unexpected characters (???) in the management interface or on the terminal.

The following queues use the LPR port:

- Queues deployed via Dispatcher Paragon Client v3 installation package created in Quick Print
- Direct print queues deployed by the user via Dispatcher Paragon Client v3
- Direct print queues created manually by the user (see Manually creating direct print queues)



Possible root causes and solutions: This may be caused by different encoding in Dispatcher Paragon Cloud and in the print jobs themselves. You can use one of the following ways to unify the encoding to display the proper characters in job titles.

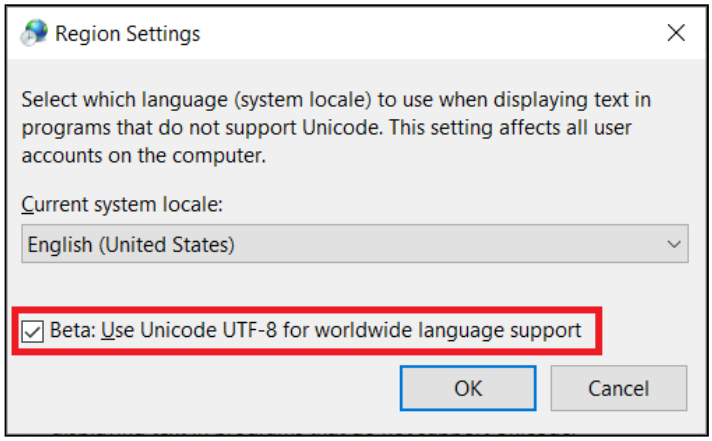
Set the *lprEncoding* property in the management interface to match users' system encoding:

1. Open PowerShell and enter `[System.Text.Encoding]::Default` to display the system encoding.
2. Log into the management interface with an admin account and navigate to **System** > **Configuration**.
3. Change the setting level to **ADVANCED** or **EXPERT**.
4. Search for "lprEncoding". Enter your system encoding displayed in PowerShell and click **SAVE CHANGES**.
5. Confirm the configuration by clicking **SAVE CHANGES**.

Instruct users to set the UTF-8 encoding for their system:

1. Leave the *lprEncoding* property unconfigured in the management interface. The UTF-8 encoding will be used by default.
2. Instruct users to set the system encoding to UTF-8:
3. Open **Control Panel** > **Region**.
4. On the **Administrative** tab, select **Change system locale**.

5. Select the checkbox and click **OK**.



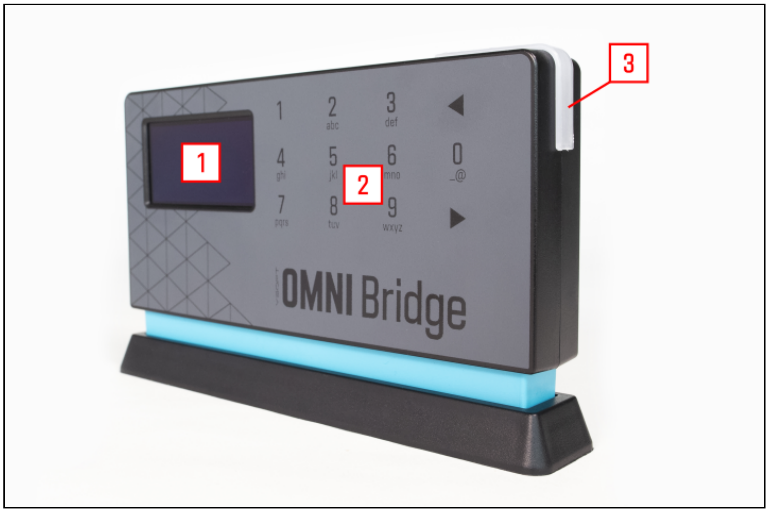
6. Restart your computer.

2.12 REFERENCE MATERIALS

2.12.1 YSOFT 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

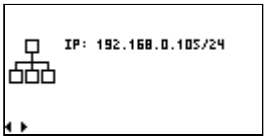
The YSoft OMNI Bridge main menu consists of the following screens:

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

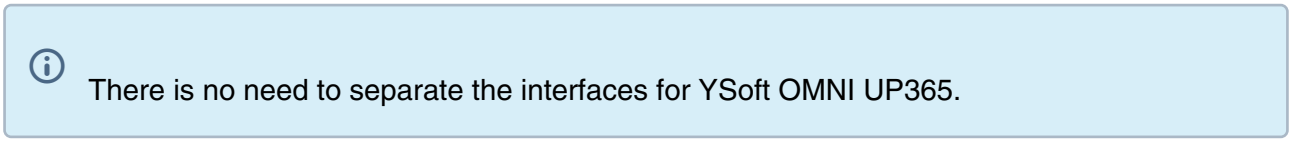
1. In the Service menu, use ▶ or ◀ to select **Network**.
2. Press **0**.
3. Select **IPv6: Disabled** and press **0**.
4. Select **DHCPv6: Off** and press **0**.
5. Select **Enable DHCPv6** and press **0**.

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**.

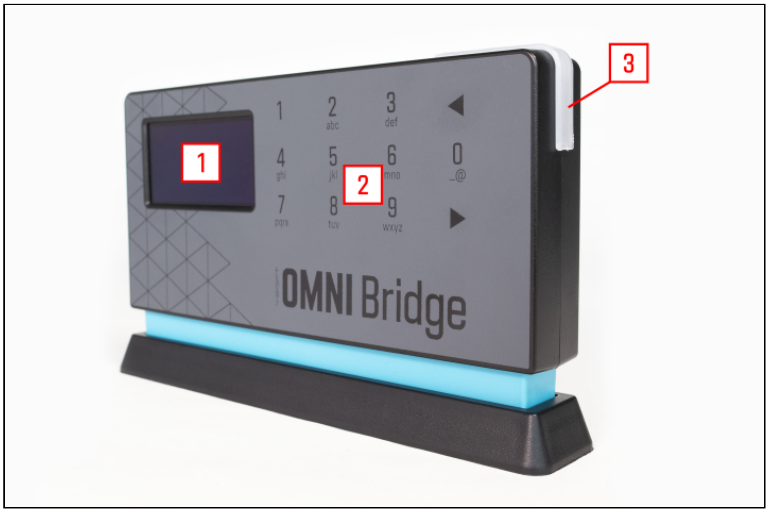
3. Press ▶ to continue.
4. Confirm by pressing ▶.
5. If you press **1**, the reset will proceed only if the device is not busy (for example, printing is in progress).
6. If you press **7**, the reset will proceed immediately, regardless of the device status.

> 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.

2.12.2 YSOFT OMNI BRIDGE SITE SERVER 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 YSoft OMNI Bridge operation manual.

About YSoft OMNI Bridge Site Server

The YSoft OMNI Bridge Site Server 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 your service representative.

Basic prerequisites

- Power supply
- Internet connection

For the complete list of prerequisites see Preparing your YSoft 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 12 OF 13**. 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 Preparing your YSoft OMNI Bridge section *Setup*.

Device configuration

Configure the device in Dispatcher Paragon Cloud Portal as described in Managing Edge devices. If any error occurs during the device configuration phase, see section *Troubleshooting – Edge-config app configuration errors*.

After a successful configuration, the display will show **DEVICE STATUS: OPERATIONAL**, and the LED light will turn blue.

The entire direct method process has defined 30 minutes timeout for successful completion of the configuration.

Device health check

The individual modules have been properly configured and should work. The *Edge-healthcheck* application periodically checks the three indicators of individual modules:

- **Port accessibility** – each of the modules uses communication ports that must be open.
- **Liveness state** – the module was successfully started. The module may not yet be ready to provide full service but is able to respond to health check requests.
- **Readiness state** – the module is able to provide a full service.

Only the health of site server modules is checked. The *Edge-healthcheck* application periodically calls the *Edge-config* application to get the status on whether monitoring should be performed or not. The *Edge-config* application is responsible for setting this status properly.

If some of the modules are unhealthy, the display will show **DEVICE STATUS: >ALERT EDGE-HEAL-0001 SOME MODULES ARE NOT OPERATIONAL. FOR MORE INFO, REFER TO THE DOCUMENTATION**.

> ⚠ It takes some time for the modules to be fully operational. During this time, an alert message is displayed as expected behavior. This state is also expected when the device is restarted.

The individual status of a module is displayed on the module's screen. Use the ▶ or ◀ buttons to navigate to the module's screen.

Each module displays its own status:

- **MODULE IS OPERATIONAL** – everything is working correctly
- **MODULE IS NOT RUNNING** – the module did not start correctly
- **MODULE IS NOT READY** – the service is not fully operational
- **SOME PORTS ARE NOT OPEN** – some of the module's ports are closed

Once all the modules are fully operational and healthy, 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.

Edge-config app configuration errors

EDGE-CONF-0001

Description: Configuration file content error.

Resolution: The incoming configuration file does not contain information about the device address within ConfigureSiteServerMethod. The actual address could not be obtained from the device. The configuration provided is incorrect or the device address is invalid.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0002

Description: Configuration file processing error.

Resolution: Device configuration failed. A problem has occurred during the processing of the configuration file within ConfigureSiteServerMethod. The JSON configuration file does not contain the expected values.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0003

Description: Direct method request error.

Resolution: An unexpected error has occurred while processing the request within ConfigureSiteServerMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0004

Description: Direct method availability error.

Resolution: Some of the direct methods have not been bound. They will be unavailable.

Next steps: Try to restart the OMNI Bridge. If the problem persists, contact your service representative.

EDGE-CONF-0005

Description: IoT HUB connection error.

Resolution: Connection to the IoT HUB has not been successfully established. Remote configuration will be unavailable. This problem can occur when the service is out of order or the Internet connection has been lost.

Next steps: Check that the Azure service is available or the OMNI Bridge still has Internet access. If the problem persists, contact your service representative.

EDGE-CONF-0006

Description: Assembly error Internal application error.

Resolution: This problem may occur when a managed assembly has been loaded from an unmanaged application. Assembly is null.

Next steps: Try to restart the OMNI Bridge. If the problem persists, contact your service representative.

EDGE-CONF-0007

Description: CSR storage error.

Resolution: The key pair was not successfully stored in the file. CSR session storage failed within GenerateCsrMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, try to restart the OMNI Bridge. If the problem still persists, contact your service representative.

EDGE-CONF-0008

Description: CSR generation error.

Resolution: CSR generation failed. An unexpected error has occurred within GenerateCsrMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, try to restart the OMNI Bridge. If the problem still persists, contact your service representative.

EDGE-CONF-0009

Description: Direct method request error.

Resolution: The tenant domain was not specified. CSR generation failed within GenerateCsrMethod. The tenant domain should be part of the initial configuration request. This problem may occur due to the provider's service outage.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0010

Description: Direct method request error.

Resolution: Invalid request, the required data was missing. The creation of the request failed within InitializeSpocTrustStoreMethod. This problem may occur due to incorrect configuration or the provider's service outage.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0011

Description: CSR session error.

Resolution: Specified CSR session ID was not found, is invalid, or the session has expired within InitializeSpocTrustStoreMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0012

Description: SPOC certificate store availability error.

Resolution: Initialization of the SPOC truststore or keystore failed within InitializeSpocTrustStoreMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0013

Description: Spooler certificate store availability error.

Resolution: Initialization of Spooler keystore failed within InitializeSpocTrustStoreMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0014

Description: Print Job Storage certificate store availability error.

Resolution: Initialization of the Print Job Storage keystore failed within InitializeSpocTrustStoreMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0015

Description: CSR processing error.

Resolution: CSR processing failed. An unexpected error has occurred within InitializeSpocTrustStoreMethod.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0016

Description: Process timeout error.

Resolution: Direct method processing has a defined timeout limit. If the timeout is reached, this error is raised.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0017

Description: Direct method request error.

Resolution: An unexpected error has occurred while processing the starting request for YSoft OMNI Bridge configuration.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0018

Description: Direct method request error.

Resolution: An unexpected error has occurred while processing the finishing request for YSoft OMNI Bridge configuration.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0019

Description: Direct method request error.

Resolution: Invalid request, the required data was missing. Request creation request itializeIppGatewayKeyStoreMethod. This problem may occur due to incorrect configuration or the provider's service outage.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0020

Description: CSR session error.

Resolution: Specified CSR session ID was not found, it is invalid, or the session has expired within *InitializeIppGatewayKeyStoreMethod*.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

EDGE-CONF-0021

Description: IPP gateway certificate store availability error.

Resolution: Initialization of IPP gateway keystore failed within I*nitializeIppGatewayKeyStoreMethod*.

Next steps: Try to repeat the configuration step again. If the problem persists, contact your service representative.

Edge-healthcheck app alerts

EDGE-HEAL-0001

Description: Module availability error.
Resolution: Some of the modules are not fully operational. The module is not running, ready or some ports are not open. Note that it takes some time for the modules to be fully operational. During this time, an alert message is displayed and it is expected behavior. This state is also expected when the device is restarted.

Next steps: Check individual module screens to determine which module is reporting the error. Try to restart the OMNI Bridge. If the problem persists, contact your service representative.

2.12.3 YSOFT OMNI BRIDGE SITE SERVER MAINTENANCE

Recovery after factory reset

> If you need to change the IP address of your OMNI Bridge, perform the factory reset procedure.

After factory reset, two steps are necessary to recover your YSoft OMNI Bridge:

1. Device code verification
2. Reconfiguring the device in the Dispatcher Paragon Cloud Portal

Once the device finishes booting, the LED turns orange or red.

If the LED turns orange, the device verification code is displayed on the screen.

- Go to https://omni.ysoft.cloud/.
- Enter the device verification code, click **Submit**, and then click **Yes**.
- Log into the Dispatcher Paragon Cloud Portal.
- Navigate to the **Edge Devices** screen (Dashboard > Manage devices), find the row with your OMNI Bridge device, and click the ⚙ icon.
- Click **Configure**.
- Wait until the LED turns blue.

If the LED turns red, an error message is displayed.

- Log into the Dispatcher Paragon Cloud Portal.
- Navigate to the **Edge Devices** screen (Dashboard > Manage devices), find the row with your OMNI Bridge device, and click the ⚙ icon.
- Click **Configure**.
- Wait until the LED turns blue.

ⓘ Factory reset of the OMNI Bridge removes all customer-related data from the OMNI Bridge, including print job data. This means that the end users will not be able to release print jobs that they submitted before the factory reset if your Dispatcher Paragon Cloud is set to Local roaming and print jobs were spooled in the OMNI Bridge. The users will only be able to release print jobs spooled at their workstations, i.e. when using Client v3 in client-spooling mode.

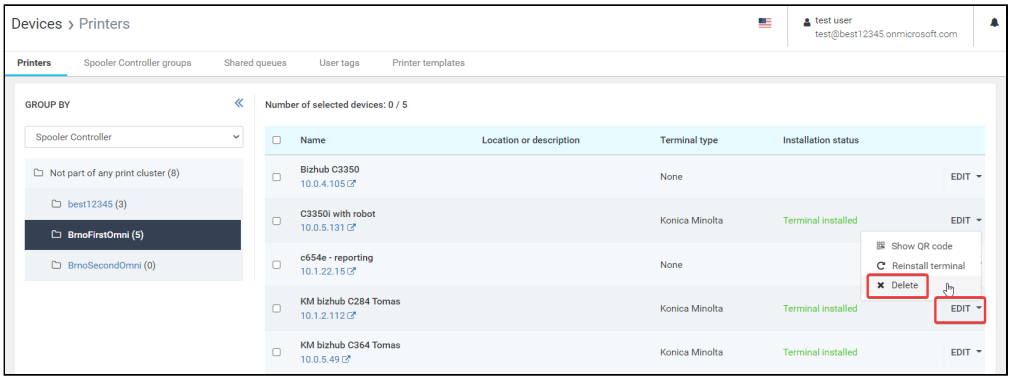
For the difference between Local and Global roaming see Edge architecture, section *Print roaming*.

Recovery after disaster

If your YSoft OMNI Bridge needs to be replaced and you want the new device to have the same IP address as the old device, perform the following steps:

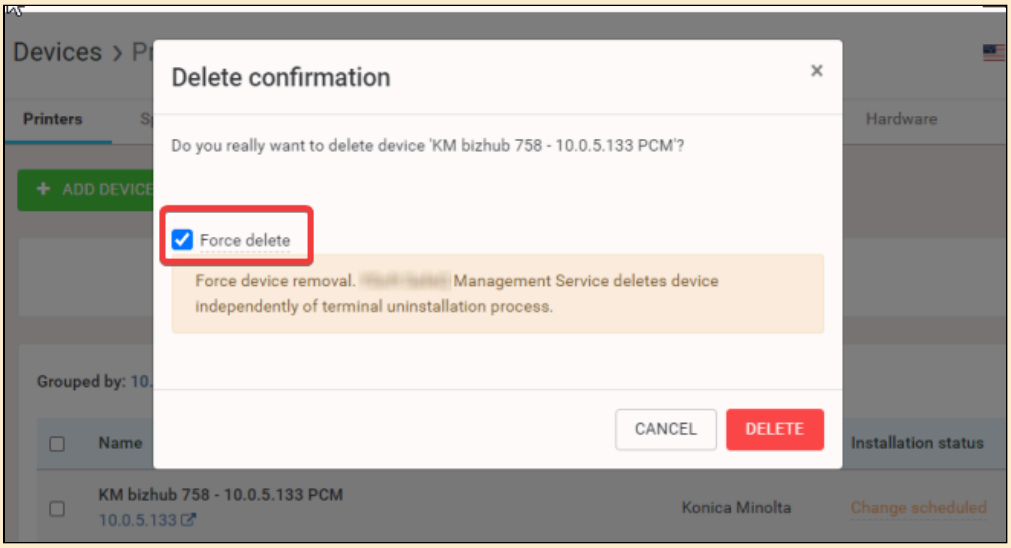
1. Log in to Dispatcher Paragon Cloud management interface.

a. Delete all Embedded Terminals installed under the respective OMNI Bridge.

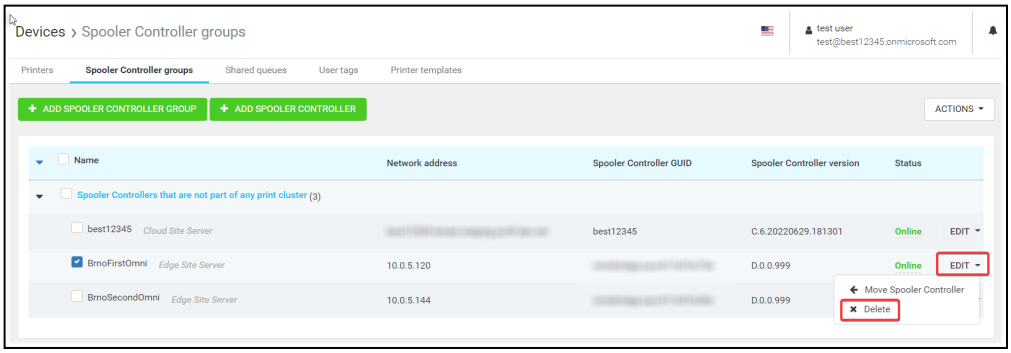


If standard deletion doesn't work, use forced deletion:

1. If the deletion hasn't worked for the first time, the **Installation status** of the terminal will change to **Change scheduled**.
2. Click **Edit > Delete** again.
3. Now you will see the **Force delete** option. Select it and click **DELETE**.



b. Delete the Spooler controller.



2. Your Service representative must arrange with the MSP a manual removal of the device serial number from your Dispatcher Paragon Cloud.
3. After you receive a new YSoft OMNI Bridge and your Service representative lets you know that you can start configuring it, follow the steps described in Preparing your YSoft OMNI Bridge and Managing Edge devices.
4. Windows printers added via IPP URI from IPP Gateway for the respective OMNI Bridge will not work. Instruct the users to generate a new IPP URI and add a new Windows printer.

2.12.4 SCAN WORKFLOWS ADDITIONAL INFORMATION

Workflow variables

If you want to customize your workflows further, use workflow variables. You can access the following types of variables:

- Capture variables – Pieces of information collected during the document capture phase. Available during the entire workflow lifecycle. For example, user and device information
- User input variables – Pieces of information that the user enters at the MFD panel. Available only during the workflow processing.
- Process variables – Outputs from document processing. Available during the workflow processing. For example, the unique ID of the scan job instance.

Variables start with the % character followed by a variable name (no spaces allowed) and end with the % character (%userEmail%, %barcode%, etc).

List of all variables

Name	Workflow Destination	Variable Type	Usage
%billingCode%	all	process	The code of the billing code used for this scan job (can be null if none is assigned).
%fileLocations%	all	process	The comma-separated file paths of all scanned files in the destination.
%deviceID%	all	capture	The ID of the device where the scan was made.

Name	Workflow Destination	Variable Type	Usage
%deviceName%	all	capture	The name of the device where the scan was made.
%deviceDescription%	all	capture	A description of the device where the scan was made.
%deviceGroupID%	all	capture	The ID of the group to which belongs the device where the scan was made.
%deviceGroupName%	all	capture	The name of the group to which belongs the device where the scan was made.
%deviceGroupIP%	all	capture	The IP address the group to which belongs the device where the scan was made.
%deviceLocation%	all	capture	The location of the device where the scan was made.
%deviceIP%	all	capture	The IP address of the device where the scan was made.
%deviceActivationDate%	all	capture	The activation date of the device where the scan was made (in the 'YYYY-MM-DD HH:MM:SS.MS' format).
%deviceEquipmentID%	all	capture	The equipment ID of the device where the scan was made.

Name	Workflow Destination	Variable Type	Usage
%deviceServiceAgreementID%	all	capture	The device service agreement ID of the device where the scan was made.
%deviceContactPerson%	all	capture	The contact person for the device where the scan was made.
%deviceCostCenterID%	all	capture	The cost center number of the device where the scan was made.
%deviceCostCenterName%	all	capture	The cost center name of the device where the scan was made.
%scanDate%	all	capture	The local date on Terminal Server at the time of the scan in the format *yyyy-MM-dd.*
%scanTime%	all	capture	The local time on Terminal Server at the time of the scan in format *HH-mm-ss-fff* (for example,12-15-00-000' for quarter past twelve).
%userCostCenterID%	all	capture	The cost center number of the terminal user who made the scan.
%userCostCenterName%	all	capture	The cost center name of the terminal user who made the scan.
%userEmail%	all	capture	The email of the terminal user who made the scan.
%userFirstName%	all	capture	The first name of the terminal user who made the scan.

Name	Workflow Destination	Variable Type	Usage
%userSurname%	all	capture	The surname of the terminal user who made the scan.
%userUsername%	all	capture	The username of the terminal user who made the scan.
%fileLocations%	all	capture	The final comma-separated list of processed files, including the path to the file. This variable is accessible in notifications only. ⚠ Not applicable for SMTP connector.
%scanJobID%	all	process	The unique ID of the scan job instance. This identifier of the scan job is visible also in the log files.
%workflowID%	all	capture	The ID of the workflow used to make the scan.
%workflowName%	all	capture	The name of the workflow used to make the scan.

Supported Output Formats

Output Format	Real Output Format									
	Konica Minolta, Develop, Olivetti, Aurora	Sharp	Sharp-eSF	Ricoh, Ricoh SOP	Fuji Xerox	Xerox	Toshiba, OKI, OKI sXP	HP	Epson	Lexmark

JPEG	JPEG	JPEG	JPEG	TIFF, JPEG*	JPEG	JPEG	JPEG	JPEG	JPEG	JPEG
TIFF	TIFF	TIFF	TIFF	TIFF, JPEG*	TIFF	TIFF	TIFF	TIFF	TIFF	TIFF
Multipage TIFF	Multipage TIFF	Multipage TIFF	Multipage TIFF	Multipage TIFF, PDF*	Multipage TIFF	Multipage TIFF	TIFF	Multipage TIFF	Multipage TIFF	Multipage TIFF
PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF
Compact PDF	Compact PDF	Compact PDF	PDF	PDF	PDF, Compact PDF**	Compact PDF	PDF	PDF	PDF	PDF

*The format depends on the selected color mode.

**Depends on the selected color mode and resolution.

Scan resolution

Scan Resolution	DPI								
	Konica Minolta, Develop, Olivetti,Aurora	**Sharp, Sharp-eSF**	**Ricoh**	**Fuji Xerox**	**Xerox**	**Toshiba, OKI, OKI sXP**	**HP**	**Epson**	**Lexmark**
Low	200*200	100*100	100*100	200*100	72*72	150*150	150*150	200*200	100*100
Normal	200*200	200*200	200*200	200*200	200*200	200*200	200*200	200*200	200*200
Fine	300*300	300*300	300*300	300*300	300*300	300*300	300*300	300*300	300*300

Scan Resolution	DPI								
	Konica Minolta, Develop, Olivetti,Aurora	Sharp, Sharp-eSF	Ricoh	Fuji Xerox	Xerox	Toshiba, OKI, OKI sXP	HP	Epson	Lexmark
High	400*400	400*400	400*400	400*400	400*400	400*400	400*400	600*600	400*400
Highest	600*600	600*600	600*600	600*600	600*600	600*600	600*600	600*600	600*600

2.12.5 ENABLING PRINT WITHOUT AUTHENTICATION OPTION ON KONICA MINOLTA MFDS

Print without authentication option allows printing of documents, that are sent directly to the MFD's IP address. This is necessary, for example, for the Emergency print feature of Dispatcher Paragon Client v3.

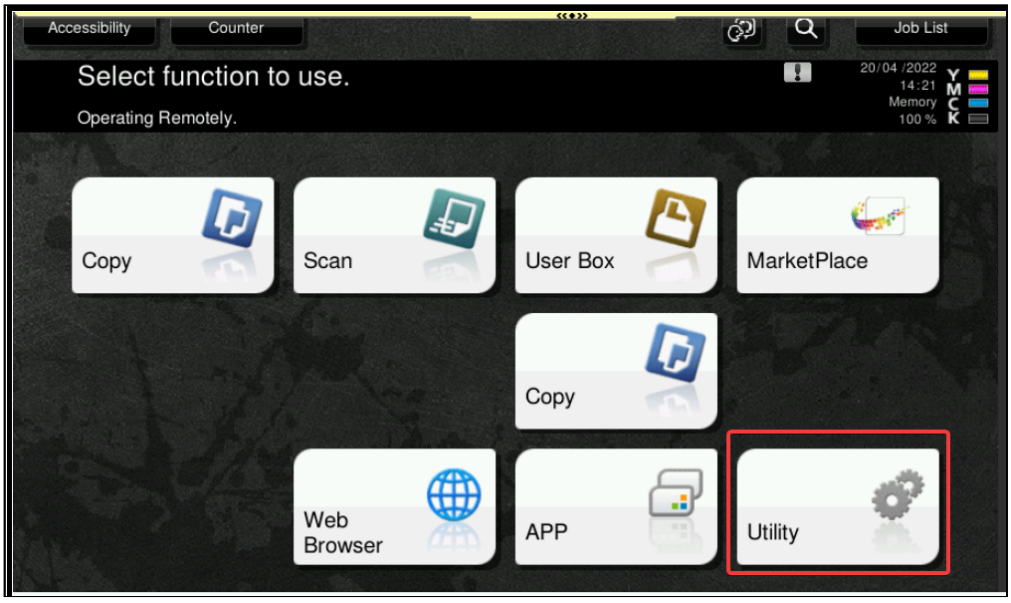
Be aware that that if you reinstall the Embedded Terminal, the configuration will be reset back to restricted.

Perform the following steps to enable the MFD's Print without authentication option:

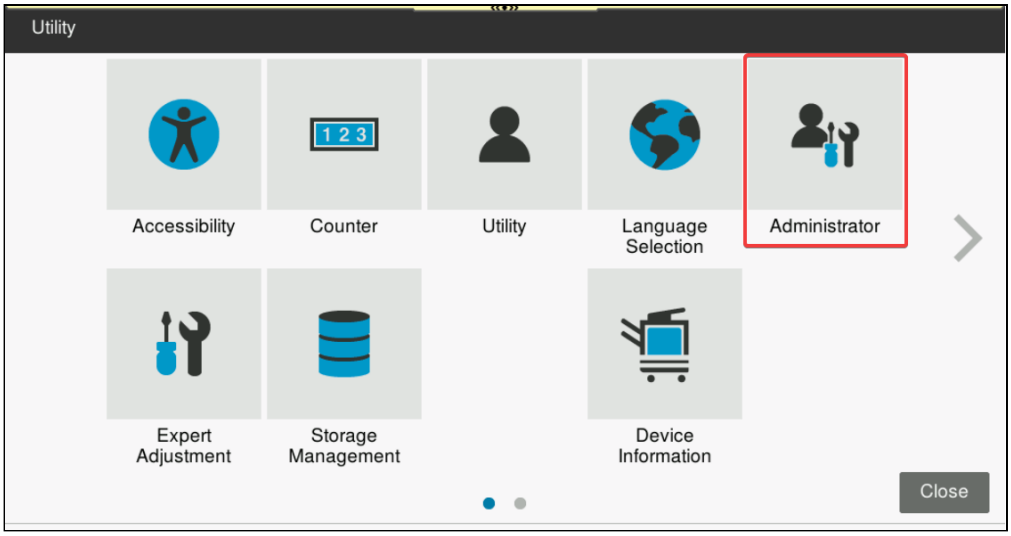
The steps may differ for your MFD. Refer to the manual for your MFD model.

1. Press the **Home** button on MFD.

2. On the MFD panel, tap **Utility**.

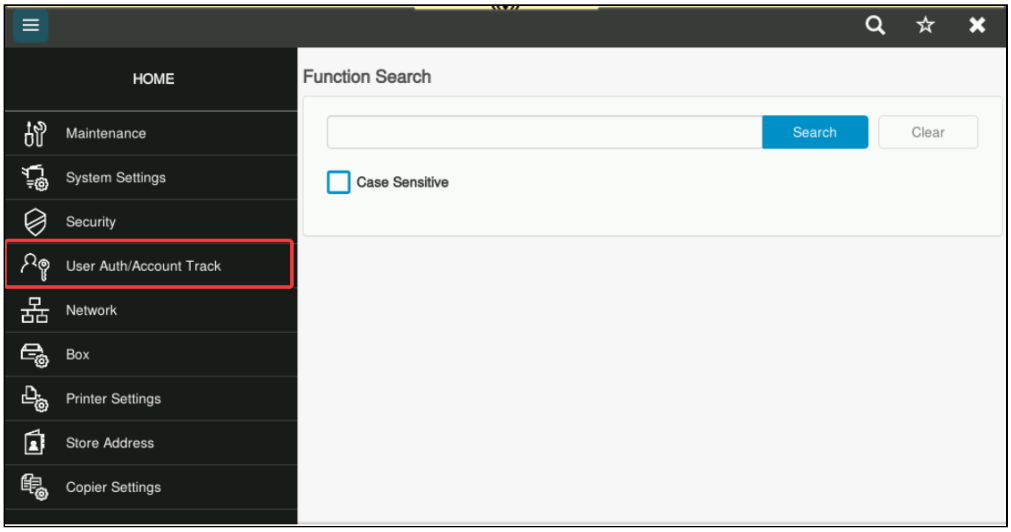


3. Tap **Administrator**.

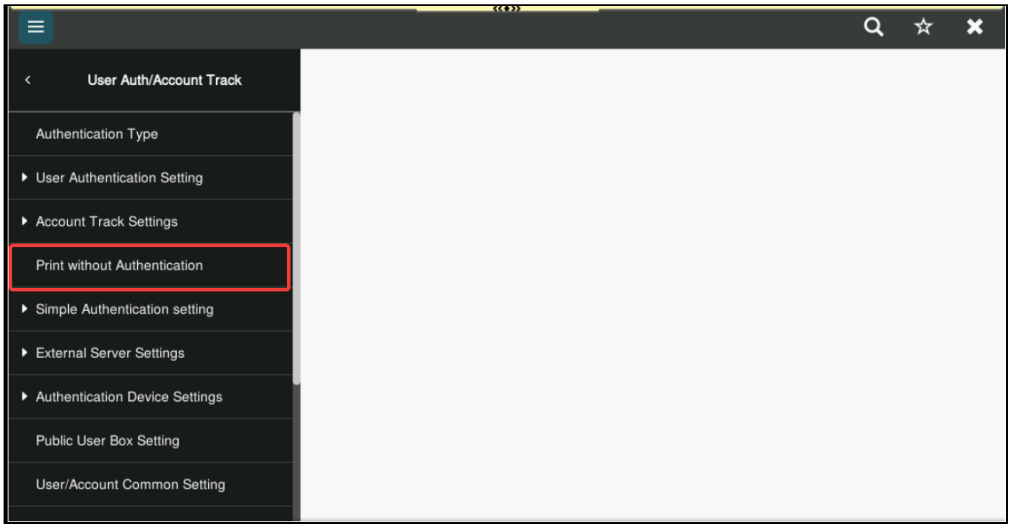


4. Enter the Administrator password for the MFD and tap **OK**.

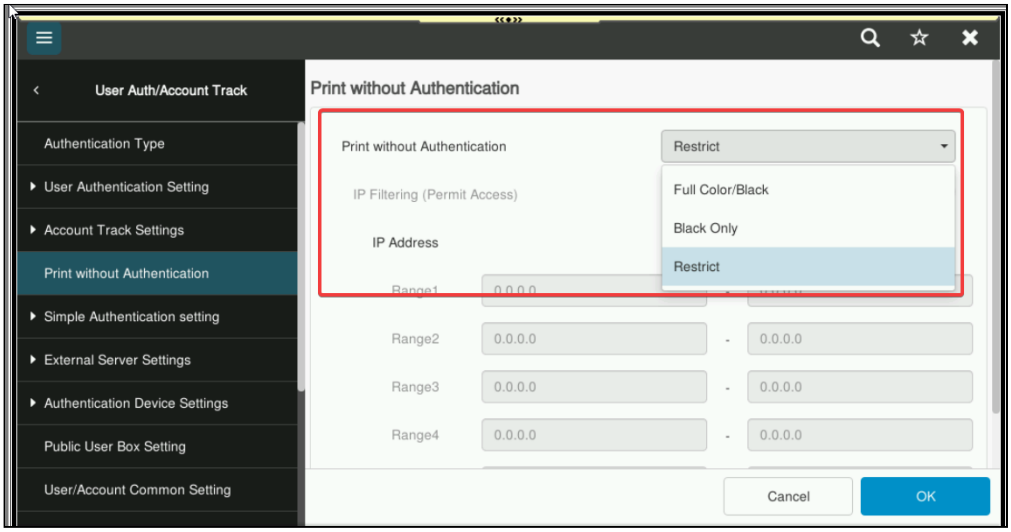
5. Tap **User Auth/Account Track**.



6. Tap **Print without Authentication**.



7. In the drop-down menu, select either **Black only** or **Full Color/Black** and tap **OK.**

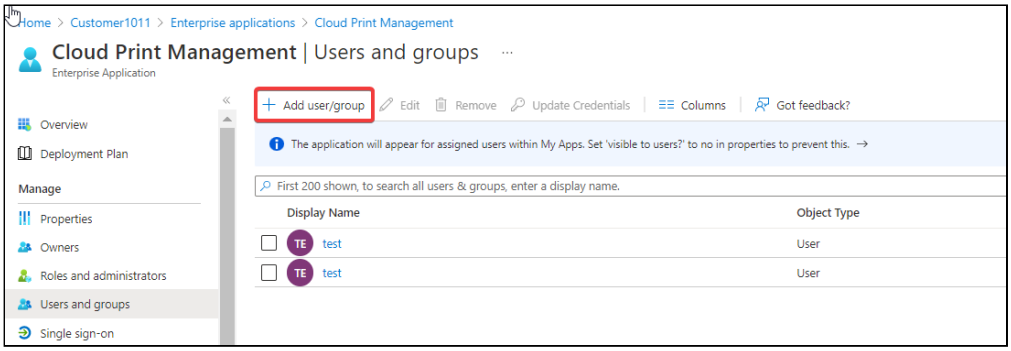


2.12.6 TENANT ADMIN ROLE FOR ACCESSING DISPATCHER PARAGON CLOUD PORTAL

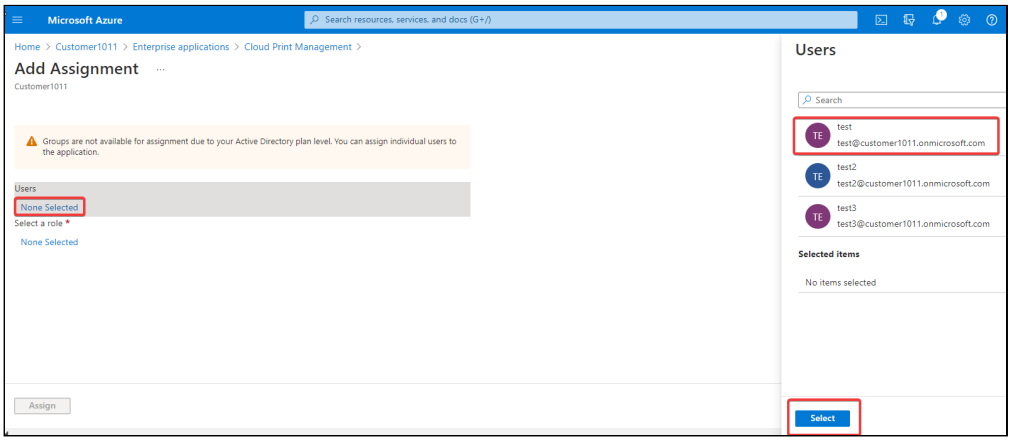
> The tenant admin role is necessary only for Externally managed users synchronised from Azure AD.

To access the Dispatcher Paragon Cloud Portal as a customer admin, you must assign yourself (or to delegate users) a **Tenant admin** role for the **Cloud Print Management** application in Azure AD.

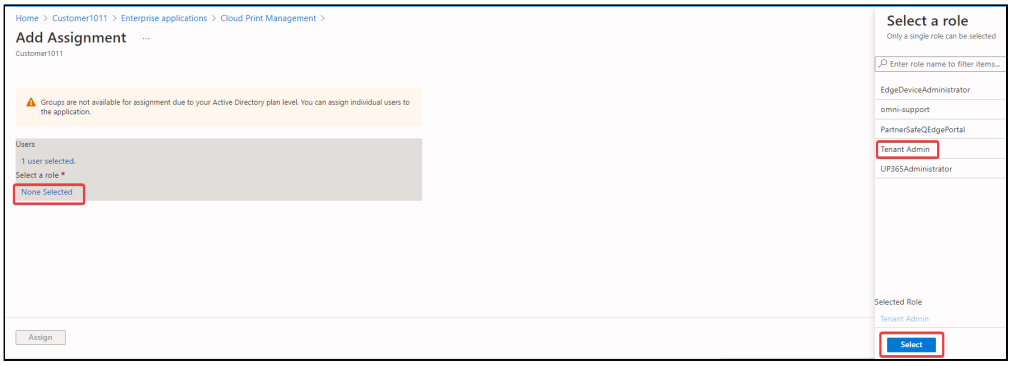
1. Log into the Microsoft Azure Portal with your administrator account.
2. Click **Manage Azure Active Directory**.
3. In the left-hand menu, click **Enterprise applications**.
4. Click the **Cloud Print Management** application.
5. In the left-hand menu, click **Users and groups**.
6. Click **+ Add user/group**.



7. In the Edit dialog, click **None selected** under **Users**, select the user from the list and click **Select**.



8. Click **None selected** under **Select a role**. In the right-hand column, click **Tenant Admin** and click **Select**.



9. Click **Assign**.

2.12.7 VIRTUAL APPLIANCES

The virtual appliance can be used in Edge printing as an alternative to YSoft OMNI Bridge. It can be deployed to customers' own VM platforms such as Microsoft Hyper-V. The following guide describes the deployment of a virtual appliance using Microsoft Hyper-V.

> ⚠ This is a beta version of the virtual appliance – a fully working but time-restricted release. Once activated, the virtual appliance will expire after 2 years and will have to be recreated. As a consequence, IPP print queues and all associated MFD terminals will have to be reinstalled. This time restriction will be removed in the final release.

Requirements

- Microsoft Hyper-V virtualization platform running on AMD x64 architecture.
- SSH Client on your desktop or server
- Allow the following external domains and their communication ports in your network firewall for the virtual appliance to function correctly:

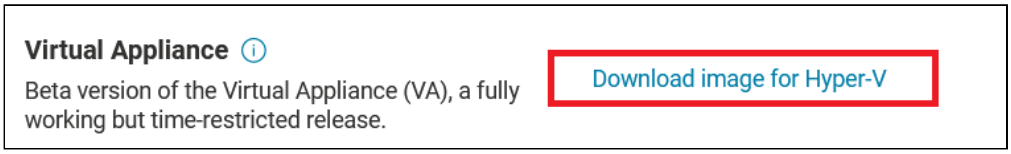
FQDN (* = wildcard)	Outbound TCP Ports	Used for
mcr.microsoft.com	443	Microsoft Container Registry
*.data.mcr.microsoft.com	443	Data endpoint providing content delivery
*.cdn.azcr.io	443	Deploy modules from the Marketplace to devices

FQDN (* = wildcard)	Outbound TCP Ports	Used for
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, 443	IoT Hub access
*.docker.io	443	Docker Hub access (optional)
*.dipa.cloud	443	Dispatcher Paragon Cloud Services
*.ysoft.cloud	443	Dispatcher Paragon CodeFlow
*.google.com	UDP 123	NTP server (time{1-12}.google.com) or any chosen NTP server

⚠ The domains and ports must be enabled in your network firewall, not in the firewall in the virtual appliance itself.

Downloading the image

1. Log into Cloud Portal.
2. On the **Dashboard** tab, use the link in the **Virtual Appliance** section.



Note the large size of the downloaded file (2GB).

Deploying the image

1. Extract files from the downloaded zip file.
2. Open the Hyper-V Manager. Go to **Action** > **Import Virtual Machine** to open the wizard.
3. Locate the extracted folder and click **Next**.
4. Select the downloaded image and click **Next**.
5. Choose one of the options and then click **Next**:
   - *Register* – Uses the files where they are stored at the time of import and retains the virtual machine's ID. If the virtual machine is already registered with Hyper-V, it needs to first be deleted.
   - *Restore* – Restores the virtual machine to a location of your choice or uses the default Hyper-V location.
   - *Copy* – Creates a copy of the virtual machine and moves the files to the default Hyper-V location.
6. On the **Connect Network** screen, select an external virtual switch. If you don't yet have an external switch, you can use the **Default Switch** option and create an external switch later. Click **Next**.
7. Click **Finish** to close the wizard.
8. In the **Virtual Machines** section, right-click on the imported machine and select **Start**.

You must always import the original downloaded image when you wish to add the first or another instance of the virtual appliance. You cannot copy an already running and registered virtual appliance.

Registering your Edge device

To register your virtual appliance as an Edge device, do the following:

1. Open the Hyper-V Manager and select the imported machine.
2. In the **Details** section, navigate to the **Networking** tab. Find the IP address of your virtual appliance.
3. Connect to the virtual appliance:

a. If you have a DHCP server in your network, you can use SSH to connect to your virtual appliance. Open Windows Command Prompt and type the following command to establish the connection.

```
ssh admin@<va-ip-address>
```

b. If you do not have a DHCP server in your network, you can use the Hyper-V Manager to connect to your virtual appliance. In Hyper-V Manager, find the **va** virtual machine and click **Connect**. If the virtual appliance cannot connect to the Internet due to not having an IP address, it will allow you to configure a static IP address. For configuring a static IP address, see the *Static IP lease / static IP address* section of this document.

c. If you are connecting for the first time, you will be prompted to enter a new admin password and you will have to log in again with the new password.

> Passwords in the virtual appliance must be a minimum of 8 characters long and contain at least one numeric character (0-9), one uppercase, and one lowercase letter (A, z). If the password contains a word that can be found in a dictionary, it must contain at least four additional characters to pass the dictionary check.

4. Copy the URL provided in the console.
5. Paste the URL into your web browser.
6. If you are an Externally managed user, click **Sign in with Microsoft** and enter your Microsoft credentials.
7. If you are an Internally managed user, enter your Dispatcher Paragon Cloud credentials and click **Sign in**.
8. Click **Yes** to grant the necessary access privileges.
9. Back in the Command Prompt console, press ENTER.
10. Enter your admin password one more time if prompted.
11. Note the ID of your virtual appliance for future use.

Network configuration

The virtual appliance must be run inside the company network in order to install terminals. This needs to be done manually after the virtual machine (VM) has been created.

First, create an external virtual switch if it does not yet exist:

1. Open the Hyper-V Manager. Go to **Action** > **Virtual Switch Manager**.
2. On the Create virtual switch pane, select **External** and click **Create Virtual Switch**.

3. On the **Virtual Switch Properties** pane. Under Connection type, select an external network of your company. Click **Apply**.

   ⚠ This will temporarily reset the network connection.

Now, reconfigure your VM to use the external virtual switch:

1. Open the Hyper-V Manager.
2. Right-click your virtual machine and select **Turn Off**.
3. Right-click your virtual machine again and select **Settings**.
4. Go to **Network Adapter** and change the switch to the external virtual switch which you previously created.
5. Click **Apply**.
6. It is recommended to set a static MAC address:
   a. Right-click your virtual machine again and select **Settings**.
   b. Under the **Network Adapter** settings, open **Advanced features**.
   c. Set the MAC address to **Static** and click **Apply**.
7. Apply settings.
8. Right-click your virtual machine and select **Start**.

The virtual appliance should now be connected to the company network. You can check the IP in the Hyper-V Manager and proceed with the configuration of the Edge device.

Static IP lease / static IP address

⚠ The virtual appliance requires a static IP lease from the DHCP server for a given MAC address in order to function correctly in the long term. It is recommended to use Static MAC address assignment. If you're moving your VM with Dynamic MAC Address to a different physical Hyper-V host machine, the MAC would be regenerated.

If you cannot use a static IP lease in the DHCP server, perform the following steps to set a static IP address directly in the virtual appliance. The virtual appliance uses Ubuntu 20.04, so you change the IP via Netplan.

1. Use the following comand to open `/etc/netplan/01-netcfg.yaml` in the nano editor:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

2. Find **eth0** and set **dhcp4** to false.
3. Under the **eth0** key, add a new block:

```
addresses:
  - <your_desired_static_ip>/<desired_mask>
gateway4: <gateway_ip_address>
```

4. Use the following command to apply the Netplan configuration:

```
sudo netplan apply
```

5. Use the following command to restart the imposter service:

```
sudo service imposter restart
```

An example of the configured `/etc/netplan/01-netcfg.yaml` file:

Netplan.cnfg

```
network:
  ethernets:
    eth0:
      dhcp-identifier: mac
      dhcp4: false
      dhcp6: false
      addresses:
        - 192.168.0.160/24
      gateway4: 192.168.0.1
      nameservers:
        addresses:
        - 4.2.2.1
        - 4.2.2.2
        - 208.67.220.220
      optional: true
  renderer: networkd
  version: 2
```

Configuring your Edge device

To configure your Edge device, follow this guide: Managing Edge devices.

Maintenance

Updating the virtual appliance

There is currently no mechanism to update the virtual appliance or its BaseOS that wouldn't require the reconfiguration of the Site Server and the reinstallation of all terminals.

This process will delete all spooled jobs.

1. Download a new image for Hyper-V from your Dashboard in Cloud Portal.
2. Deploy the virtual appliance.
3. Register the virtual appliance.
4. Configure a new Site Server on the virtual appliance.
5. Reinstall all your terminals to the new Site Server.

Factory reset

To perform a factory reset, delete the old virtual appliance, deploy and register a new one, and configure a new Site Server on this virtual appliance. You will lose all spooled jobs and have to reinstall all terminals to the new Site Server.

Troubleshooting

Device registration failed

1. Ensure you have company firewall configuration according to the requirements.
2. Close the console connection over SSH.
3. Establish a new console connection over SSH to your virtual appliance.
4. Try device registration again.

Contact Y Soft support if this doesn't resolve the issue.

3 END USER GUIDE

3.1 DOCUMENTATION CHANGELOG - RELEASE 2023.01.26

What's new	Where
Changed screenshots of Dispatcher Paragon Cloud Terminal because of its redesign.	Dispatcher Paragon Cloud Terminal for Konica Minolta
Added more supported formats to the mobile app.	Using the Dispatcher Paragon Cloud mobile app

3.2 GENERAL INFORMATION

3.2.1 ABOUT THE END USER GUIDE

This guide is intended for end users of Dispatcher Paragon Cloud. It contains information on:

- Registering yourself in Dispatcher Paragon Cloud
- Card registration at the MFD terminal
- Generating a PIN: Management interface guide, section *Generating a PIN*
- Creating print queues
- Using Dispatcher Paragon Client v3
- Using an MFD.

If you have questions or encounter problems, contact your administrator.

3.2.2 ABOUT DISPATCHER PARAGON CLOUD

Dispatcher Paragon Cloud is a print-management solution hosted in the cloud.

3.2.3 HOW TO READ THIS GUIDE

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.

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.

3.2.4 TERMS AND DEFINITIONS

Term	Description
Dispatcher Paragon Cloud	A cloud-based print management service.
Dispatcher Paragon Cloud Terminal	An application provided by the Konica Minolta MarketPlace. This application enables communication between an MFD and the cloud.
MFD	Multi-function device (a copier).
SFD	Single-function device (a printer).

Term	Description
Reporting-only device	MFD or SFD where your company wants to capture the number of printed pages (and related statistics) but does not need any other capability such as Embedded Terminal or Cloud Terminal or print roaming.
Pure Cloud printing	An architecture intended for MFDs that support Dispatcher Paragon Pure Cloud Terminal. This scenario does not require Edge devices.
Edge printing	An architecture intended for MFDs that support only the standard embedded terminal technology. These MFDs are connected to a local Edge device that provides the site server 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 Pure Cloud printing.
Card Activation Code Provider page (CACP)	A web service allowing users to assign cards to their Dispatcher Paragon Cloud accounts using their Azure Active Directory accounts.
IPP Gateway	IPPS server for print job submission by users to their personal secure queues in Dispatcher Paragon Cloud.
Dispatcher Paragon Cloud management interface	A web interface used by administrators to manage their Dispatcher Paragon Cloud centrally, and by end users to have an overview of their accounts. It displays information and functions as per the role of the person logged in.
Konica Minolta MarketPlace	Konica Minolta's service for browsing, purchasing, and downloading applications to MFDs.
Dispatcher Paragon Client v3	A desktop application for end users through which they can submit their print jobs, see the list of waiting print jobs, delete print jobs, and deploy direct print queues to their workstation.

Term	Description
Internally managed users	User accounts created and managed in Dispatcher Paragon Cloud Portal by your administrator.
Externally managed users	User accounts created and managed in an external Identity Provider (such as Azure Active Directory) by your administrator, and synchronized with Dispatcher Paragon Cloud. If your account is synchronized with Azure Active Directory, you will be using the **Sign in with Microsoft** button in IPP Gateway, Client v3, and CACP.

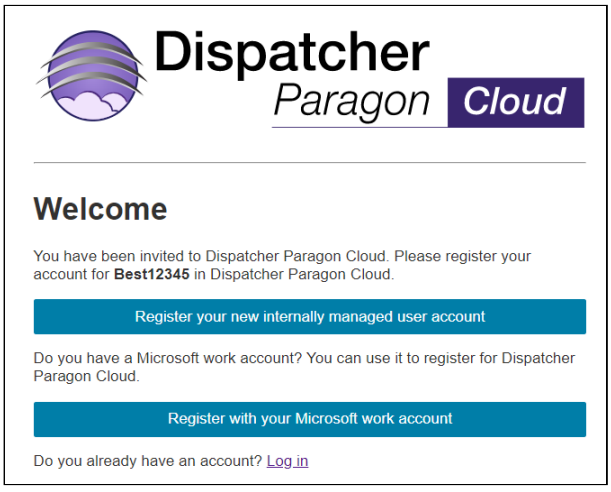
3.3 REGISTERING YOURSELF IN DISPATCHER PARAGON CLOUD

3.3.1 INTERNALLY MANAGED USERS

1. You will receive an invitation to Dispatcher Paragon Cloud via email. The subject of the email is *Welcome to Dispatcher Paragon Cloud*.This invitation must be created by your administrator.

   If the invitation email hasn't arrived, check your spam folder.

2. Click **Register your account** in the email. This will take you to the Dispatcher Paragon Cloud registration screen.



3. Click **Register your new internally managed user account**.

4. Fill in the following pieces of information:

a. Your **First name** and **Last name**.

b. **Email** – must be a valid email address. It is pre-filled with the email address where you received your invitation and cannot be changed during registration. The email also serves as a username for Dispatcher Paragon Cloud.

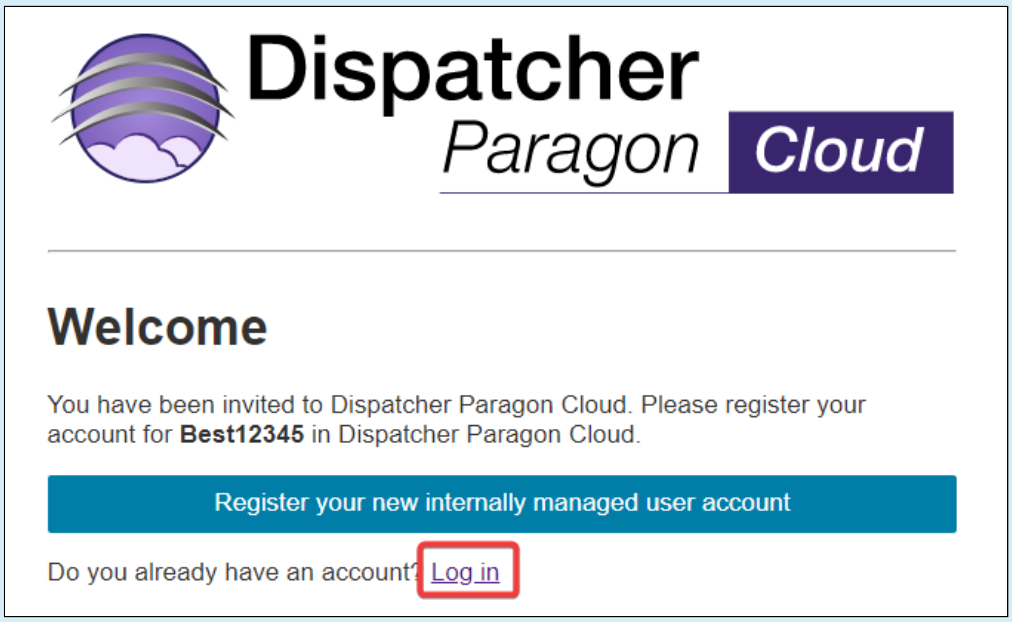
c. **Password**.

5. Click **Sign up**.

6. Select the checkbox next to the EULA agreement.

7. Click **Confirm account registration**.

If your registration was interrupted before you confirmed it, click the link in the invitation email again and then click **Log in**.



Enter the email and the password that you filled in during the registration and proceed to confirmation.

With the username and password that you have just created, proceed either to registering your card (see Card registration at the MFD terminal) or generating a PIN (see Management interface guide, section *Generating a PIN*).

The next steps after card registration are Configuring IPP print queues or Using Dispatcher Paragon Client v3 (depending on how Dispatcher Paragon Cloud has been set up for your company).

3.3.2 EXTERNALLY MANAGED USERS

No action is required from you to register in Dispatcher Paragon Cloud. Proceed straight to registering your card (see Card registration at the MFD terminal) or generating a PIN (see Management interface guide, section *Generating a PIN*).

The next steps after registering a card/generating a PIN are Configuring IPP print queues or Using Dispatcher Paragon Client v3 (depending on how Dispatcher Paragon Cloud has been set up for your company).

3.4 CREATING PRINT QUEUES

You can obtain a print queue for Dispatcher Paragon Cloud in the following two ways:

- IPP Gateway – a web-based service where you can generate an address for your own print queue (IPP URI) and use it to install a printer on your workstation. You can do this in both Pure Cloud printing scenario and Edge printing scenario. See Configuring IPP print queues.
- Dispatcher Paragon Client v3 – a desktop client for Dispatcher Paragon Cloud. During its installation, it deploys one or more printer queues (printers) on your workstation. These can be Pure Cloud print queues or Edge device print queues, or both types, depending on the scenario that your company is using. For details on Client v3, see Using Dispatcher Paragon Client v3.

3.4.1 DIRECT PRINT QUEUES

You can use direct print queues only if you have Dispatcher Paragon Client v3 installed. This applies both to Pure Cloud printing and Edge printing scenarios.

Direct queues are suitable mainly for small network printers where authentication is not required, since there is only a limited number of users who send print jobs to them. Every direct queue has a

specific name and is assigned to a specific printer (most often a reporting-only device). You cannot release the print jobs from this queue on any other MFD.

If your administrator has configured a direct print queue in Dispatcher Paragon Cloud and made it available to you through Client v3, you can send a print job to this queue in the same way as to a standard print queue. The only difference is that the print job will be printed immediately, without waiting for you to authenticate on the printer terminal and release it. For information on adding direct print queues to your workstation, see Using Dispatcher Paragon Client v3.

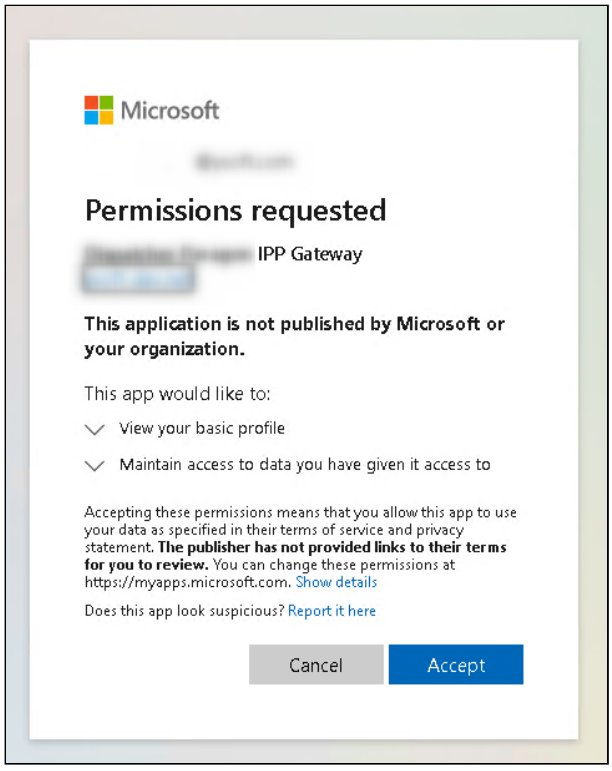
3.4.2 CONFIGURING IPP PRINT QUEUES

If your administrator decided that your company will use manual creation of print queues, follow the below steps to obtain your unique cloud print queue (IPP URI) and then configure the print queue on your workstation. At the end of this process, you will have a new printer available in your system and you can start sending your print jobs to it.

Obtaining IPP URI for Pure Cloud printing

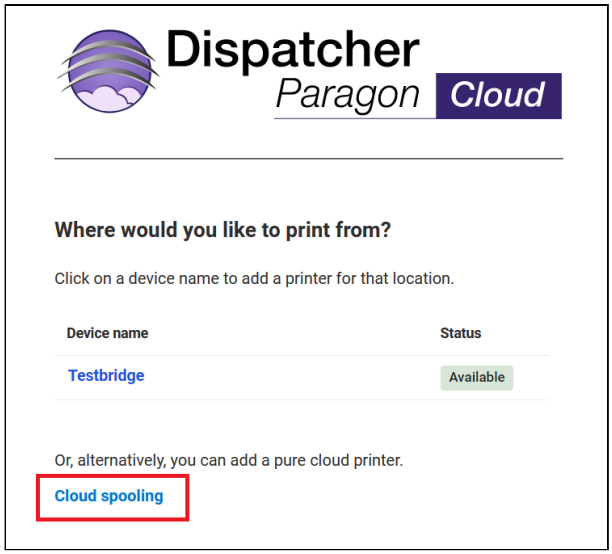
To obtain your cloud print queue, perform the following steps:

1. Open the link (provided by your administrator) to access the Dispatcher Paragon IPP Gateway page.
2. Authenticate either with your company credentials (Externally managed users) or with your Dispatcher Paragon Cloud credentials (Internally managed users).
3. If you logged in with your Microsoft account, approve the permissions requested for IPP Gateway.



4. After successful authentication, you will see your IPP URI. Click the clipboard icon to copy the link to your clipboard.

If you land after authentication on a page with more options, click **Cloud Spooling** to see your IPP URI, and then the clipboard icon to copy it.



> ⚠ The IPP URI authorizes you to send print jobs under your identity. Do not share it with anyone else!

5. Continue to the steps for adding the queue on your workstation, depending on whether it is Windows, Mac or Linux.

Obtaining IPP URI for Edge printing

If your company uses Edge printing, your administrator can send you either a link to Dispatcher Paragon IPP Gateway page with all edge devices that are configured for you or a link to an IPP Gateway page for a specific edge device.

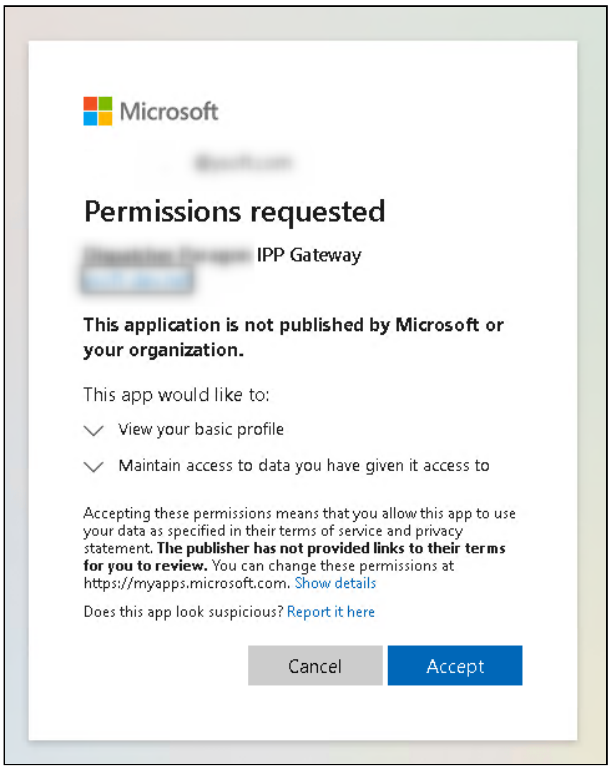
Obtaining IPP URI for Edge printing from an IPP Gateway page for a specific edge device

1. Open the link from your administrator to access the IPP Gateway page for a specific edge device.

   > This kind of link has **/device/** in its path. Example:
   >
   > https://ipp-gateway.dipa.cloud/device/MTAuMS4yLjE2Ng==/8443/dHctYnJpZGdl

2. Authenticate either with your company credentials (Externally managed users) or with your Dispatcher Paragon Cloud credentials (Internally managed users).

3. If you logged in with your Microsoft account, approve the permissions requested for IPP Gateway.

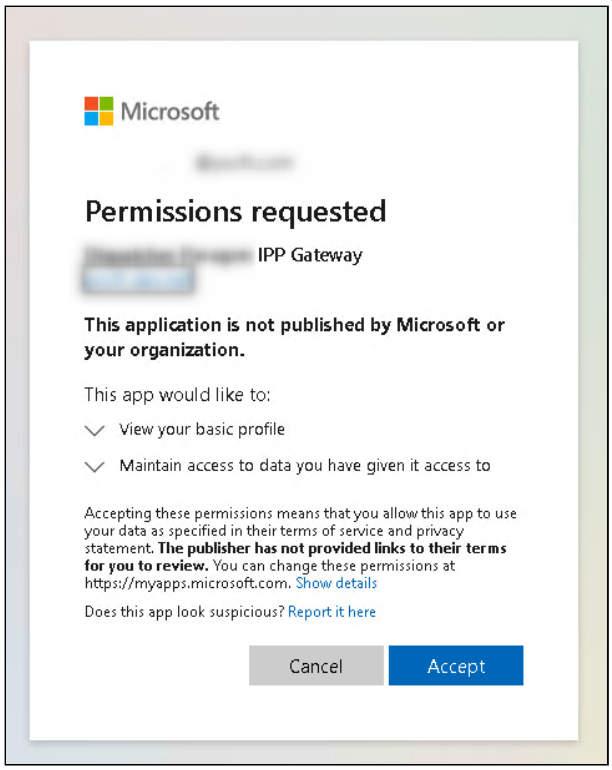


4. Click the clipboard icon to copy the link to your clipboard.

5. Continue to the steps for adding the queue on your workstation, depending on whether it is Windows, Mac, or Linux.

Obtaining IPP URI for Edge printing from an IPP Gateway page for all edge devices

1. Open the link from your administrator to access the Dispatcher Paragon IPP Gateway page with all edge devices.
2. Authenticate either with your company credentials (Externally managed users) or with your Dispatcher Paragon Cloud credentials (Internally managed users).
3. If you logged in with your Microsoft account, approve the permissions requested for IPP Gateway.



4. You will see a list of edge devices that are configured for you.

5. The reachable devices are displayed in blue color. Choose an edge device based on information from your administrator (for example, according to your location). Click the device name to see your specific IPP URI.

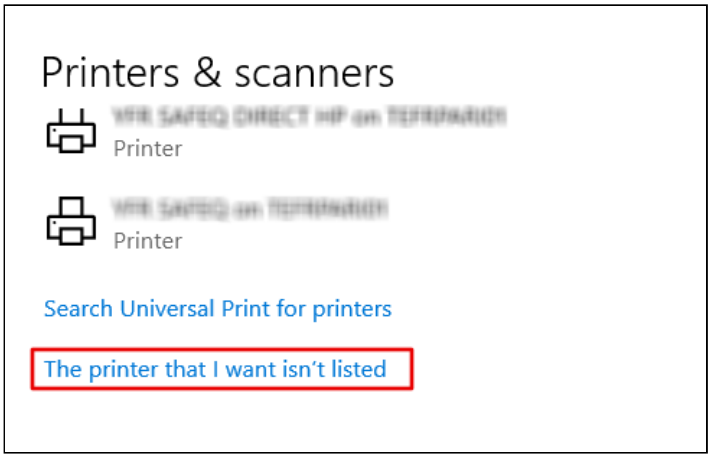
6. The page heading will change to **Setting up <your edge device name>** and the link will change to IPP URI generated specifically for you. Click the clipboard icon to copy the link to your clipboard.

7. Continue to the steps for adding the queue on your workstation, depending on whether it is Windows, Mac, or Linux.

Adding the print queue on Windows workstation

1. Add a new printer via **Add printers & scanners** dialog window. The system will search for printers in your network.

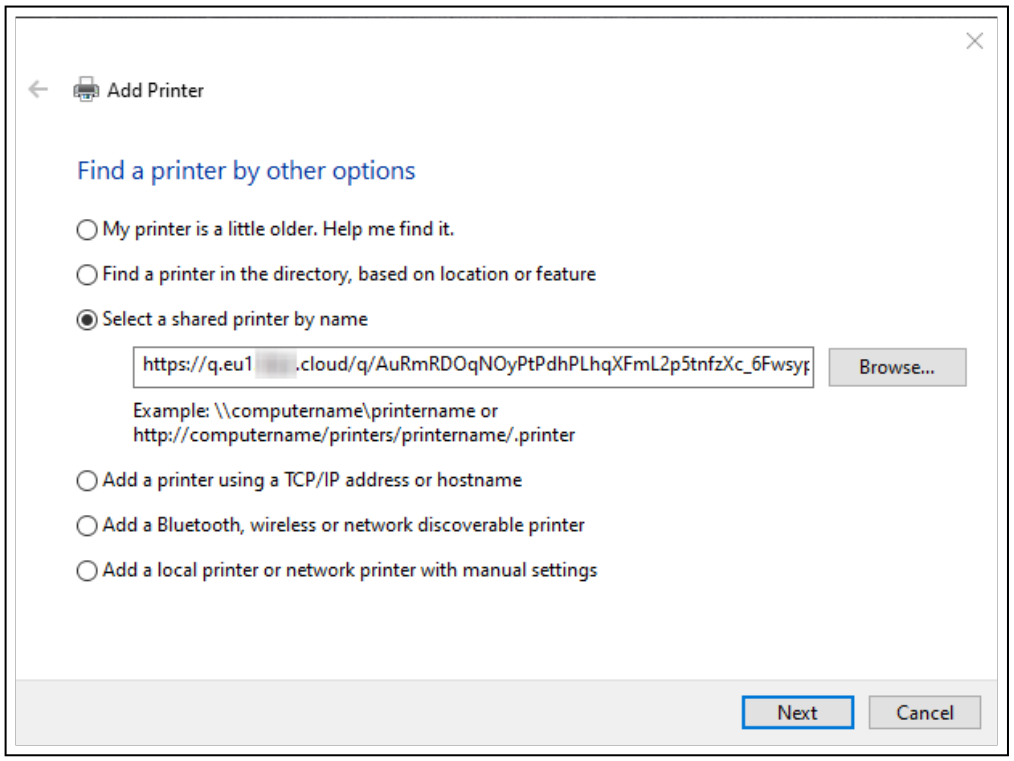
2. Click **The printer that I want isn't listed** to access the **Add Printer** dialog window.



Alternatively, you can open the **Add printer** dialog by using the following command:

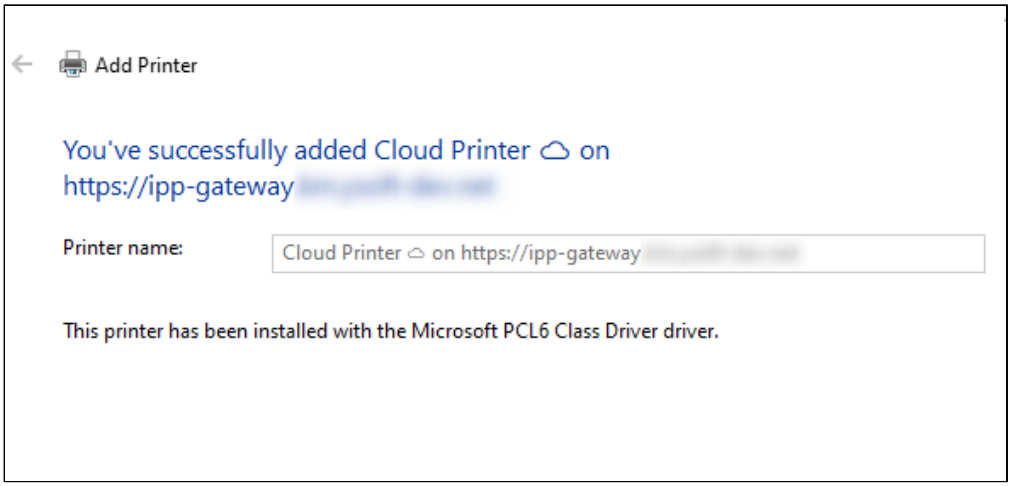
```
rundll32 printui.dll,PrintUIEntry /im
```

3. Select **Select a shared printer by name** and paste your IPP URI into the input field. Click **Next**.

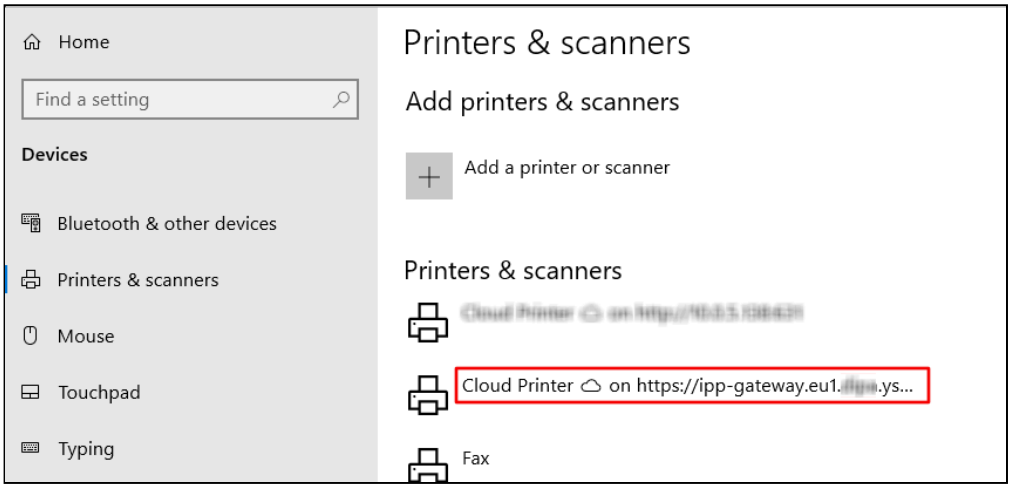


4. The **Add Printer Wizard** will guide you through the printer installation Use the print driver recommended by your administrator.

5. After adding the printer (print queue) successfully, you will see a message



6. You should also see your new printer (print queue) as **Cloud Printer** in **Printers & scanners**.

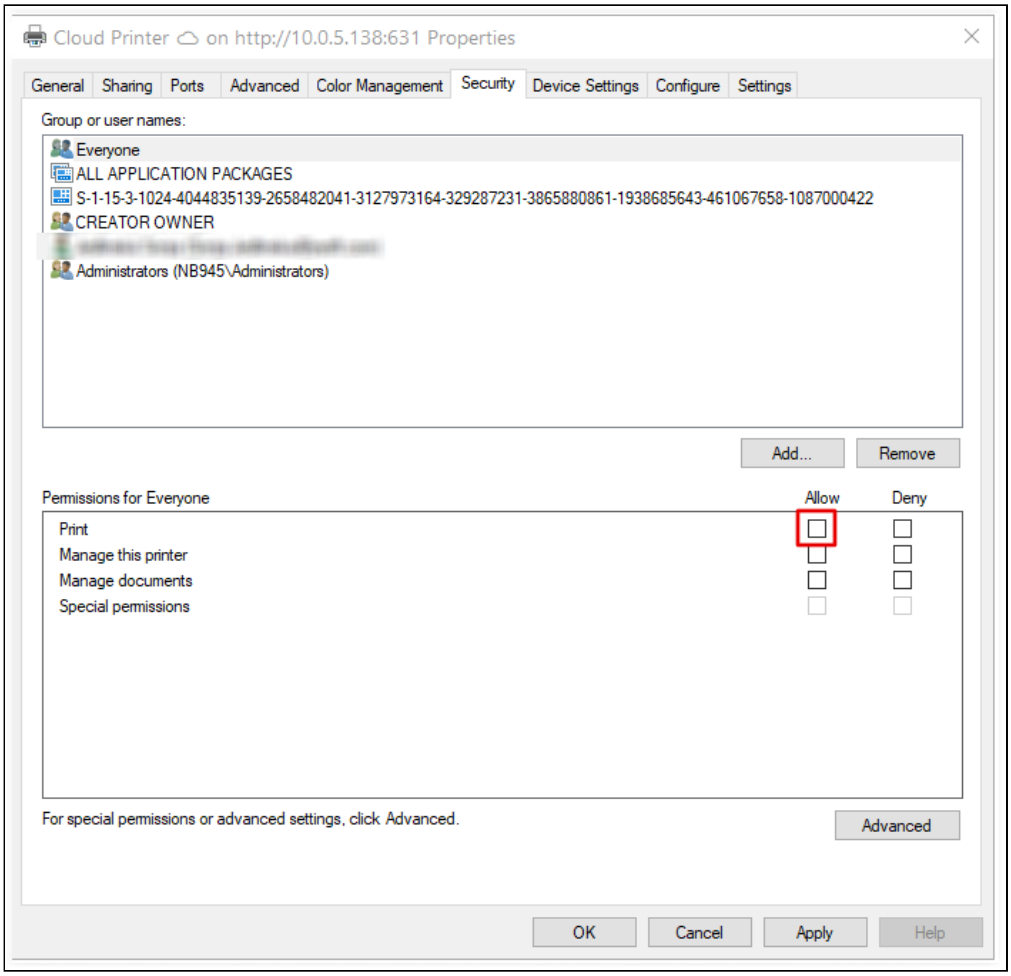


7. You can print a test page to verify that the printer was configured properly.

If you share your workstation with other users, perform the following steps to prevent the other users from being able to send print jobs to your print queue:

1. In **Printers & scanners**, click your Cloud printer.
2. Click **Manage**.
3. Click **Printer properties**.
4. Go to the **Security** tab.
5. In **Group or user names** section, click **Everyone**.

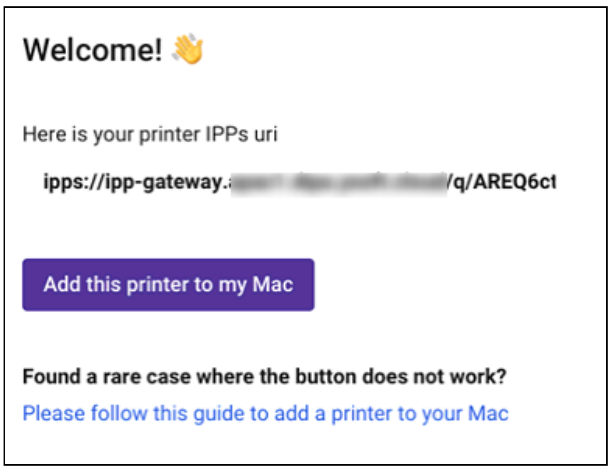
6. Uncheck **Print** in the **Allow** column.



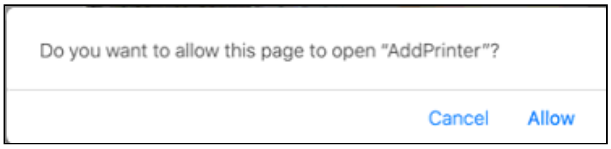
7. If there is any group in **Group or usernames** section that you want to prevent from sending print jobs to your print queue, uncheck **Print** in the **Allow** column as well.

Adding the print queue on Mac workstation

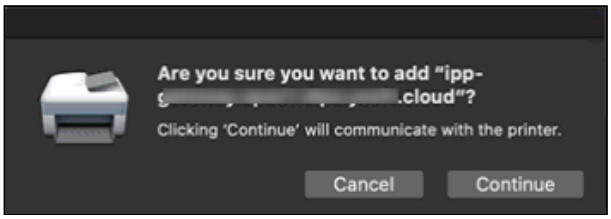
1. After logging in and obtaining the IPPs URI on the IPP Gateway page, click **Add this printer to my Mac**.



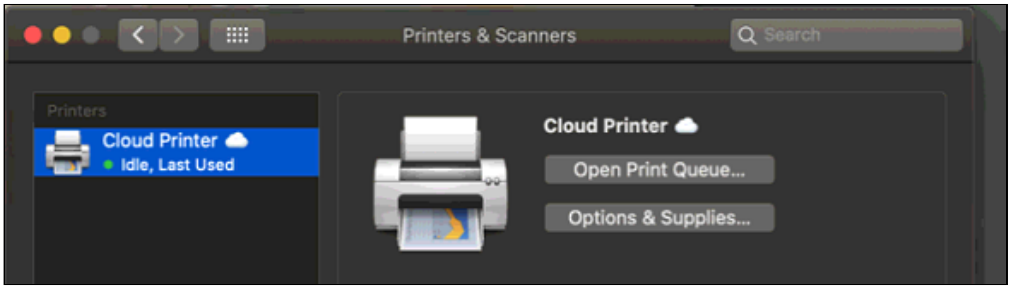
2. You will be prompted to allow the page to add a printer to your Mac. Click **Allow**.



3. Click **Continue** to add the printer.



4. The configuration is finished. You can now send print jobs to the newly created printer.

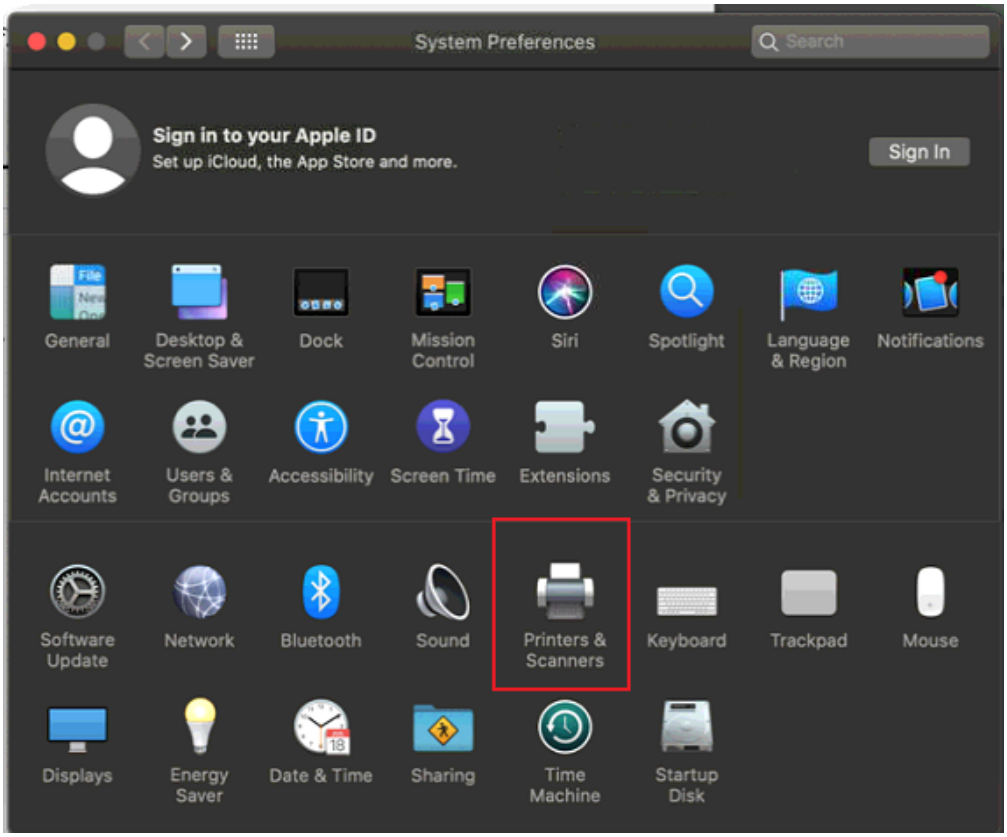


> ⚠ If you use this method of adding the printer, the Dispatcher Paragon Cloud management interface may display incorrect information about your print job. For example, that it's colored instead of black & white. However, the job will be printed correctly at the MFD.

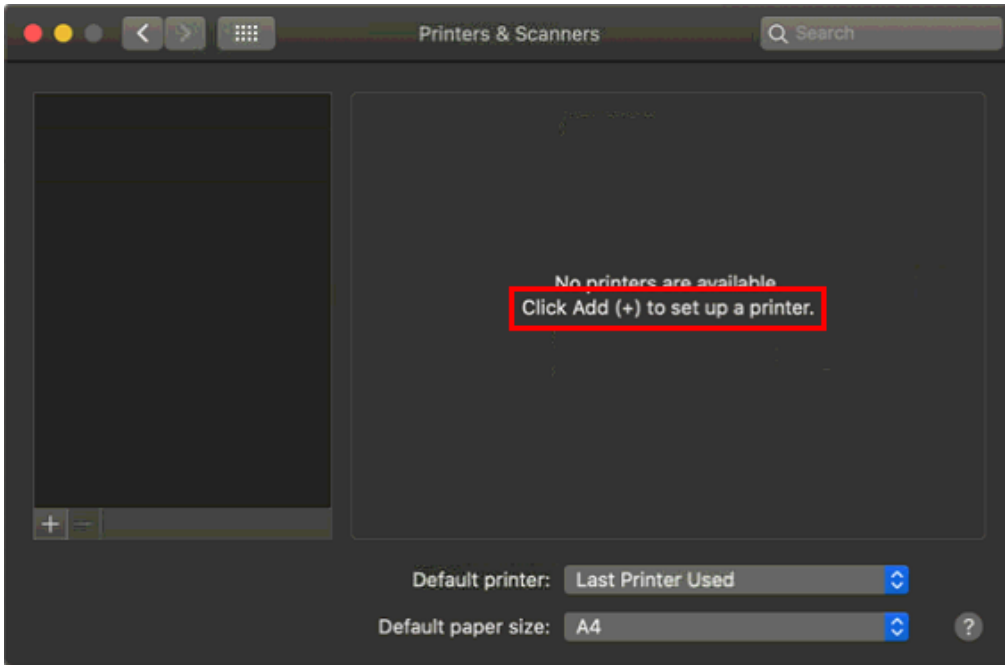
If the above procedure doesn't work, you can add the printer (print queue) manually in the graphical interface or from the command line. Be aware that the steps for adding and setting up a new printer in a macOS system may vary according to the distribution and working environment.

Adding a printer in the graphical interface

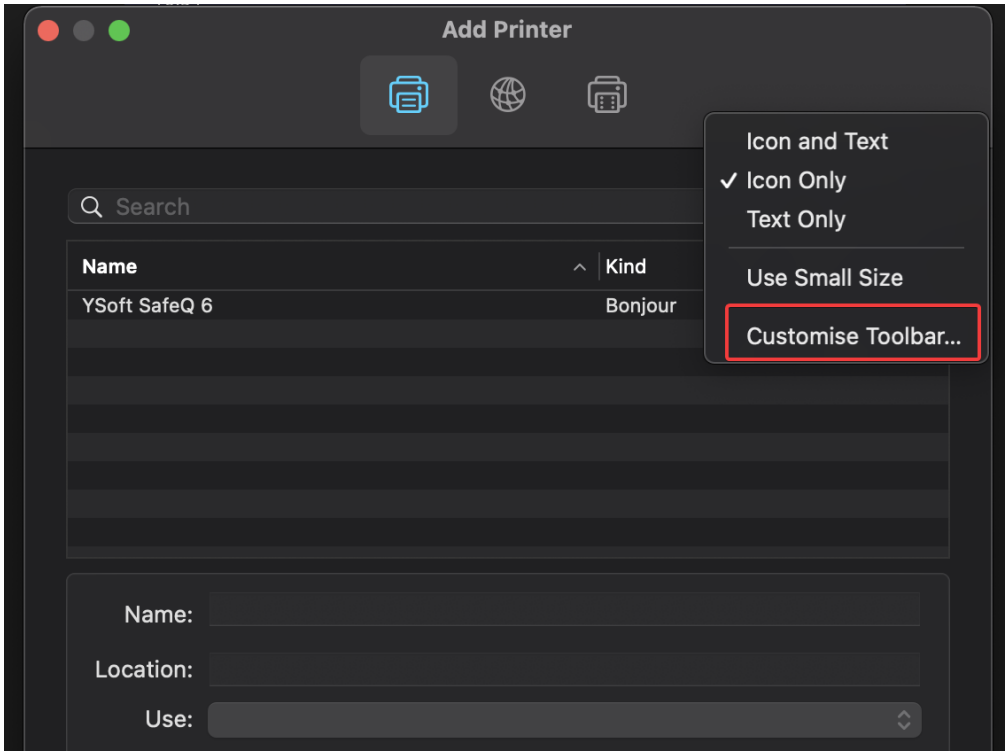
1. To add a new printer (print queue), go to **System Preferences** > **Printers & Scanners**.



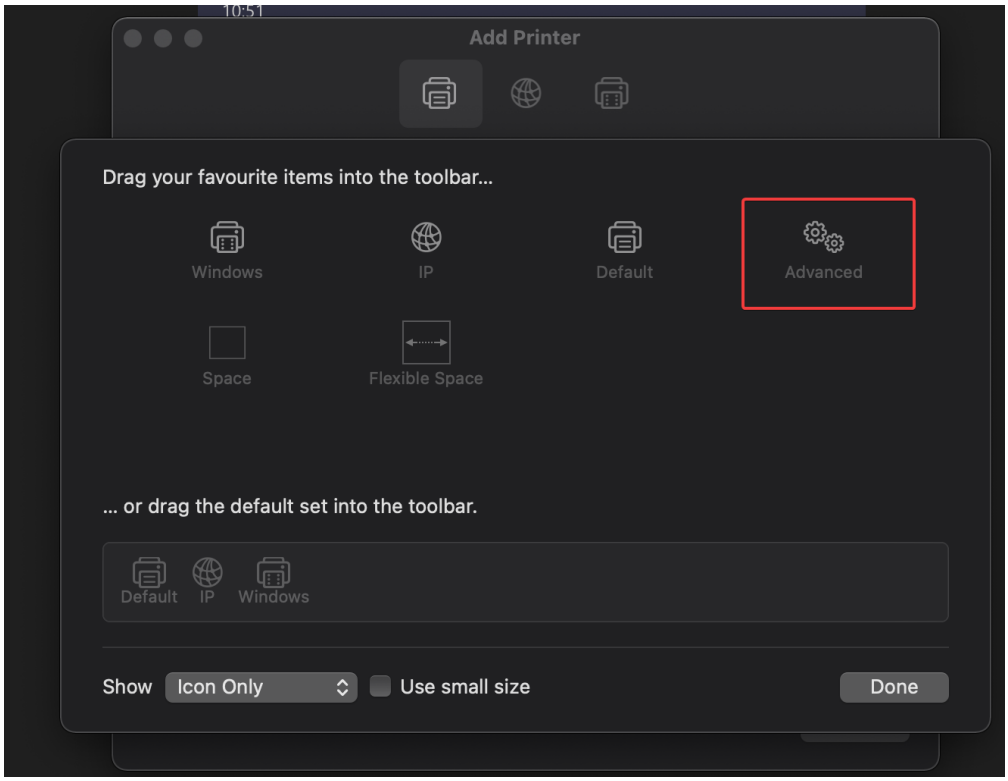
2. Click **+**.



3. Right-click the tab bar and select **Customize toolbar**.

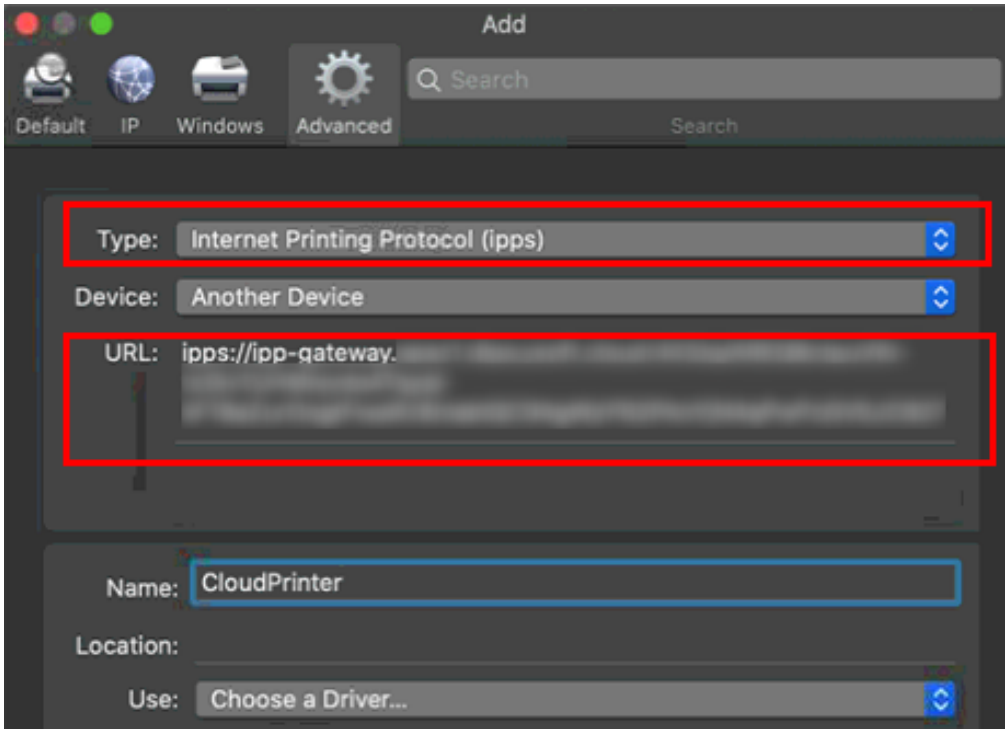


4. Drag&drop the **Advanced** tab into the menu and click **Done**.

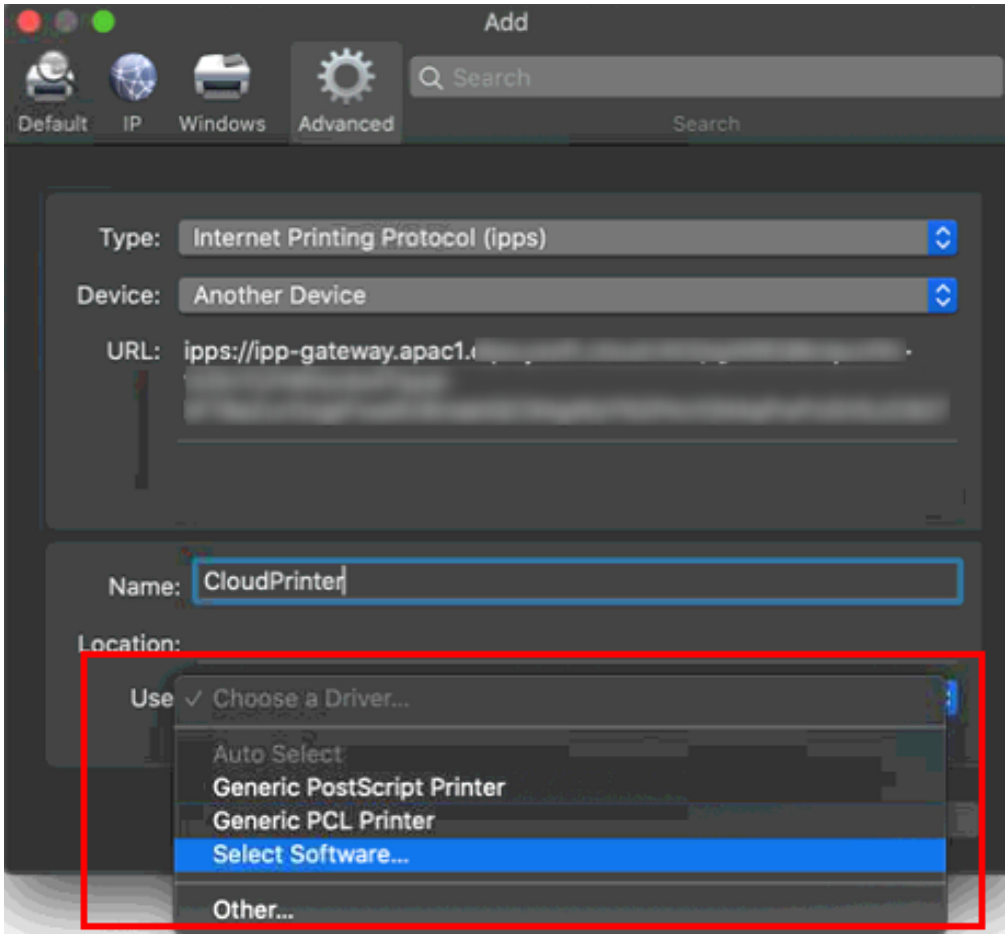


5. Click the **Advanced** tab.

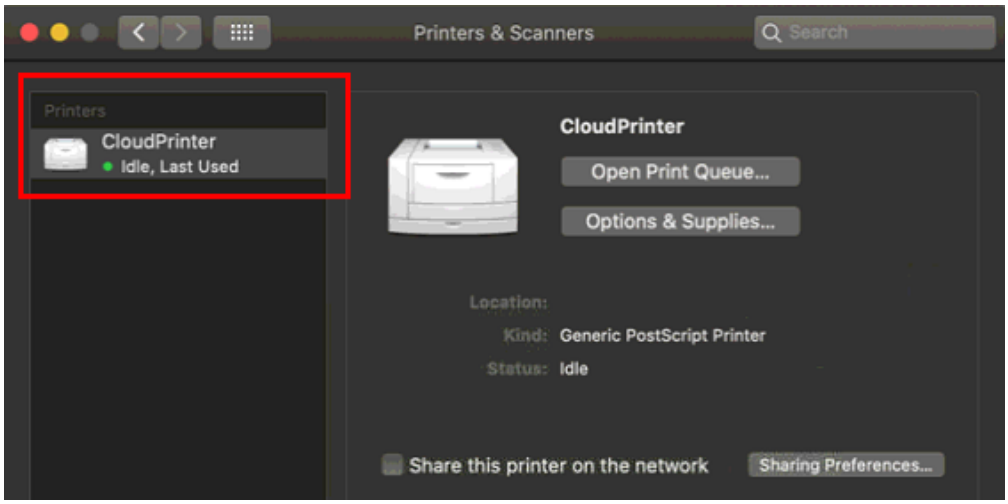
6. In **Type**, select **Internet Printing Protocol (ipps)**. Enter your IPP URI in the **URL** field.



7. In the **Use** drop-down menu, select **Select Software...** to display a list of available drivers from the database, or select **Other...** to use a PPD file.



8. Choose the driver recommended by your administrator.
9. If the configuration was successful, you will see the new printer (print queue) in the list of available printers.



Adding a printer from command line

If you prefer command line, use the following script to add a printer (print queue). Replace the IPPSURL variable with your IPP URI.

```
#!/bin/bash
PRINTER="CloudPrinter"
IPPSURL="IPPS URL address"

sudo lpadmin -E -p "${PRINTER}" -v "${IPPSURL}" \
      -m 'everywhere' \
      -o 'printer-is-shared=false' \
      -o 'auth-info-required=username,password'

sudo cupsenable "${PRINTER}" -E
sudo cupsaccept "${PRINTER}"
```

Adding the print queue on Linux workstation

You can add a printer (print queue) via command line, or in the graphical user interface, or in the CUPS interface.

Adding a printer from command line

Use this bash script to add a new printer. Replace the IPPSURL variable with your IPP URI.

```
#!/bin/bash
PRINTER= "CloudPrinter"
IPPSURL= "IPPS URL address"

sudo lpadmin -E -p
          "${PRINTER}"  -v
          "${IPPSURL}"  \
        -m
          'everywhere'  \
        -o
          'printer-is-shared=false'  \
        -o
          'auth-info-required=username,password'

sudo cupsenable
          "${PRINTER}"  -E
sudo cupsaccept
          "${PRINTER}"
```

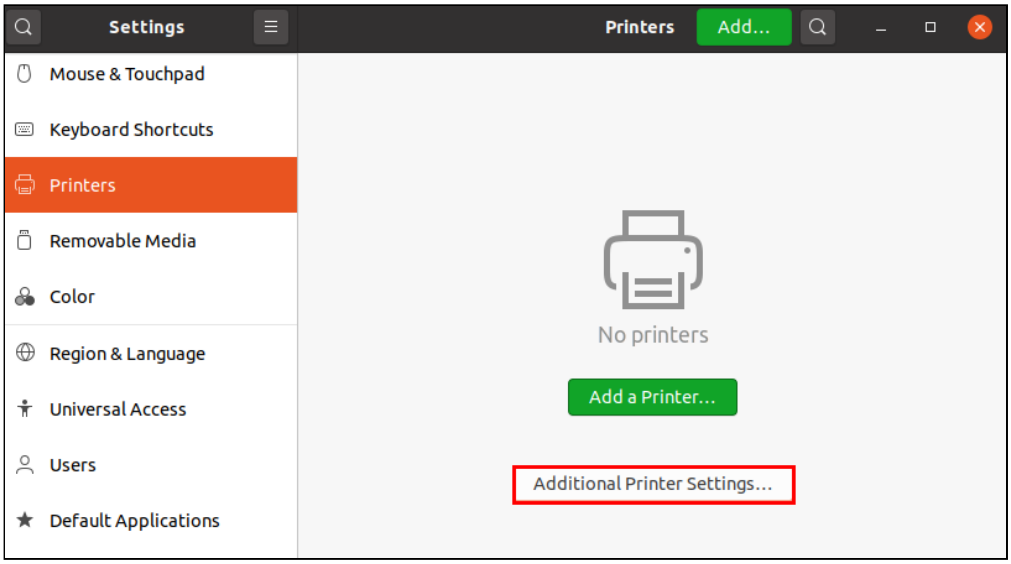
lpadmin might take about one minute to perform the configuration.

If you do not specify a print driver while adding the printer, the Dispatcher Paragon Cloud management interface may display incorrect information about your print job. For example, that it's colored instead of black & white. However, the job will be printed correctly at the MFD.

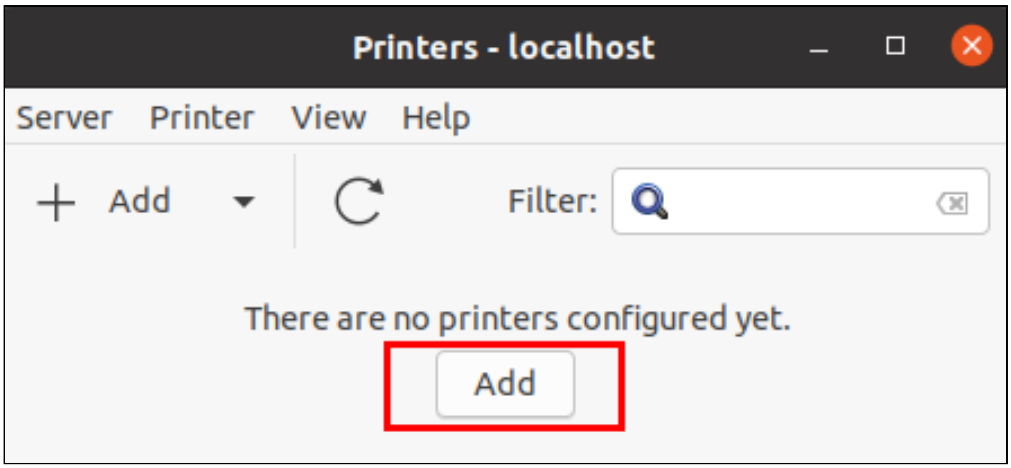
Adding a printer in the graphical user interface

The method for adding and setting up a new printer in a Linux system varies according to the distribution and working environment. The following instructions guide you through the installation process in the Gnome environment, Ubuntu distribution. For other display managers (or command line), the procedure might be slightly different.

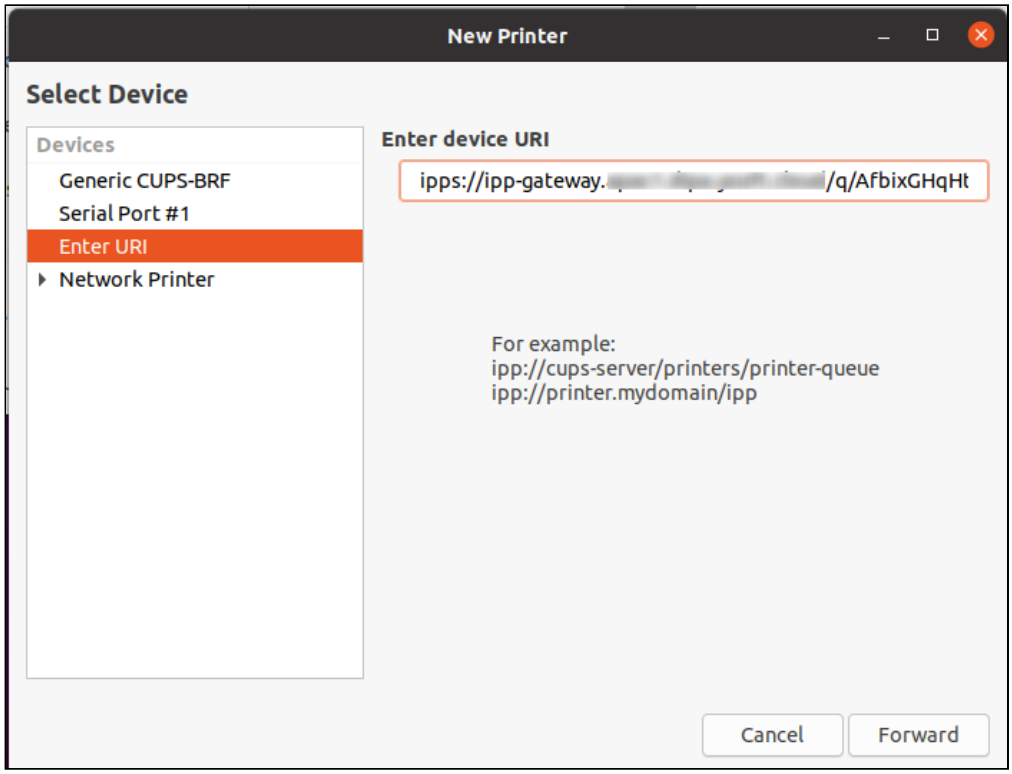
1. Go to **Settings** > **Printer** and click **Additional Printer Settings...**.



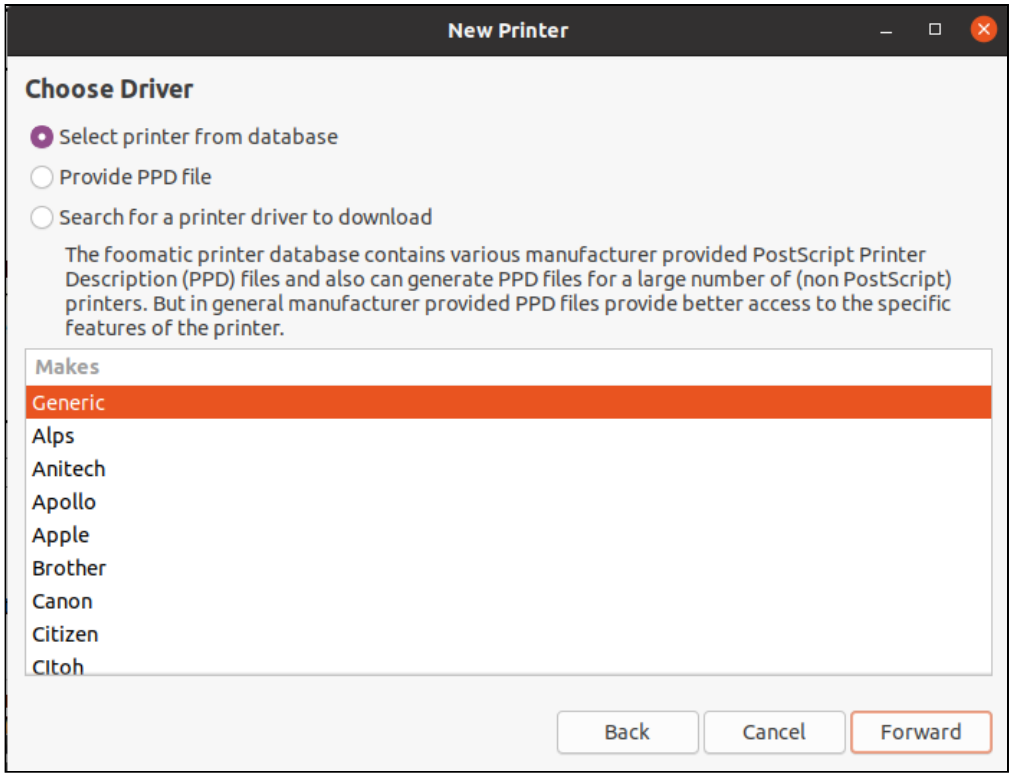
2. Click **Add** .



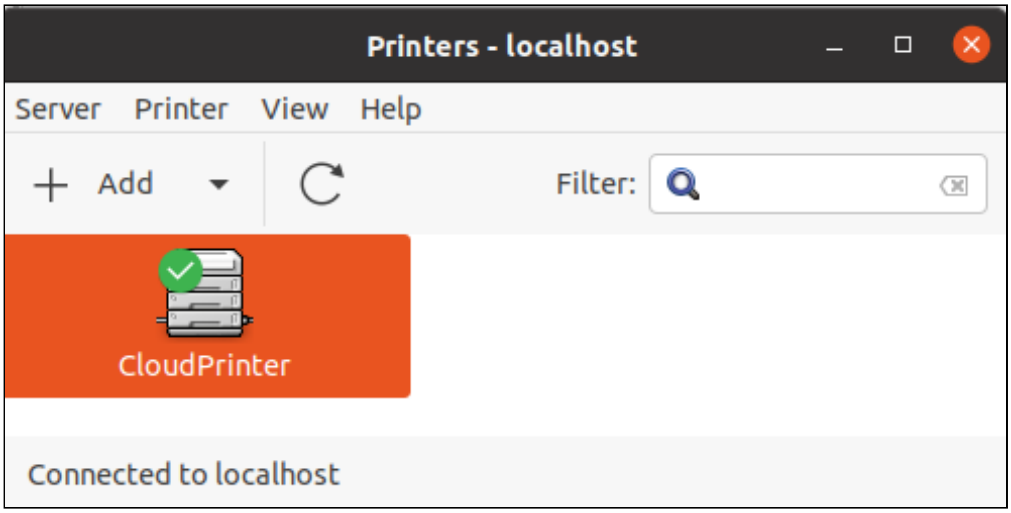
3. Enter your IPP URI in the **device URL** field. Click **Forward**



4. Select the printer driver from the database, PPD file, or download it from the Internet. Choose the driver recommended by your administrator. Click **Forward**.



5. Follow the wizard and fill in all the information according to your needs. When finished, you should see the new printer (print queue) in the list of available printers.

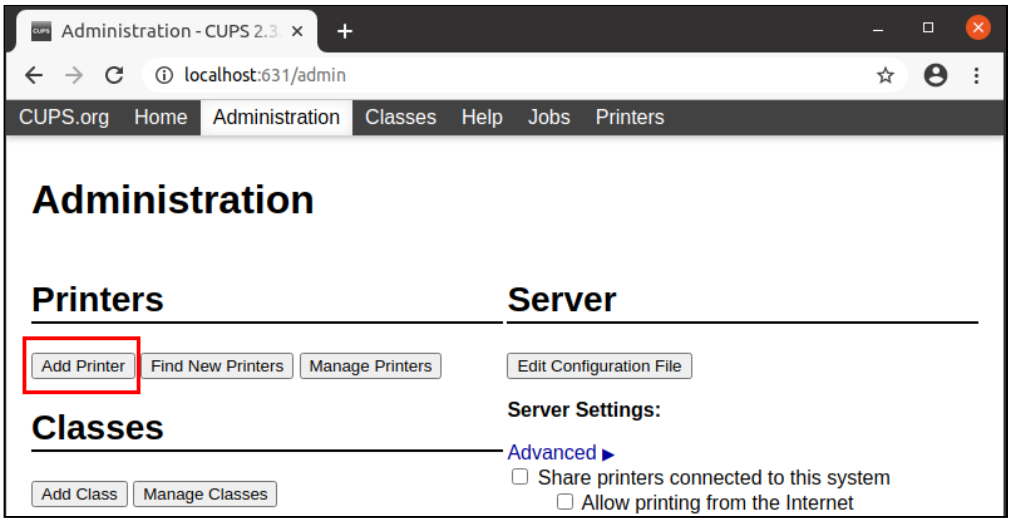


Adding a printer in the CUPS Interface

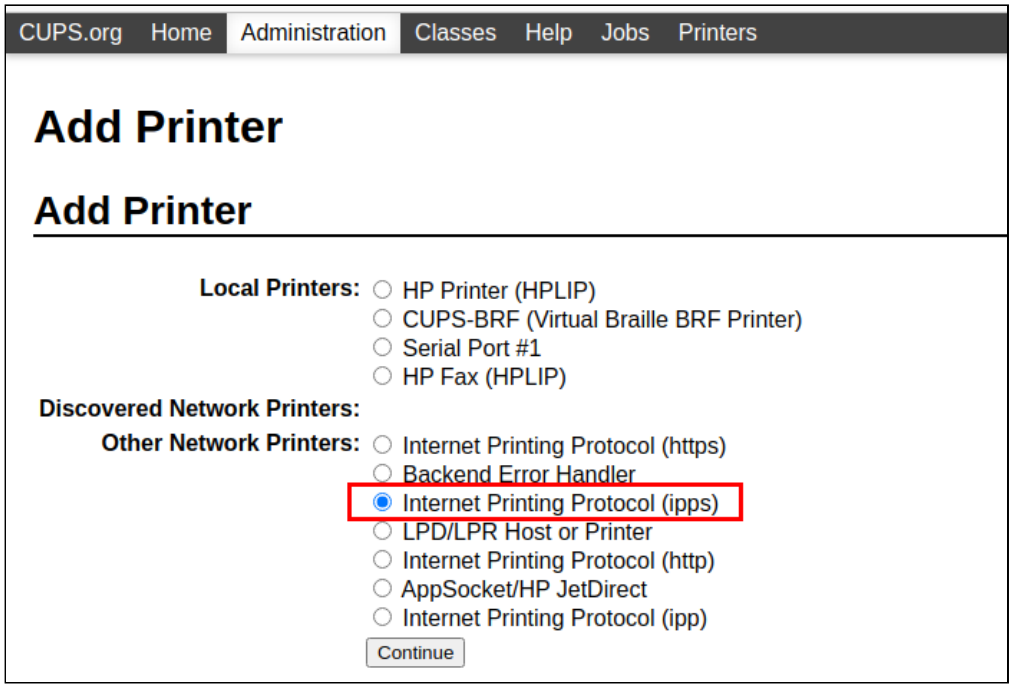
The procedure for adding and setting up a new printer in the CUPS interface is almost the same as for the graphical user interface. All you need to do is to select a hostname and queue for your printer as follows:

1. Open the CUPS interface (usually **http://<CUPS IP address>:631**) and select the **Administration** tab.

2. Click **Add Printer**. If necessary, enter the CUPS administrator credentials.



3. In the **Other Network Printers** section, select **Internet Printing Protocol (ipps)**, and click **Continue**.



4. Insert your IPP URI in the **Connection** field and click **Continue.**

5. Go through the remaining steps to set up the printer according to your needs.

If you do not specify a print driver while adding the printer, the Dispatcher Paragon Cloud management interface may display incorrect information about your print job. For example, that it's colored instead of black & white. However, the job will be printed correctly at the MFD.

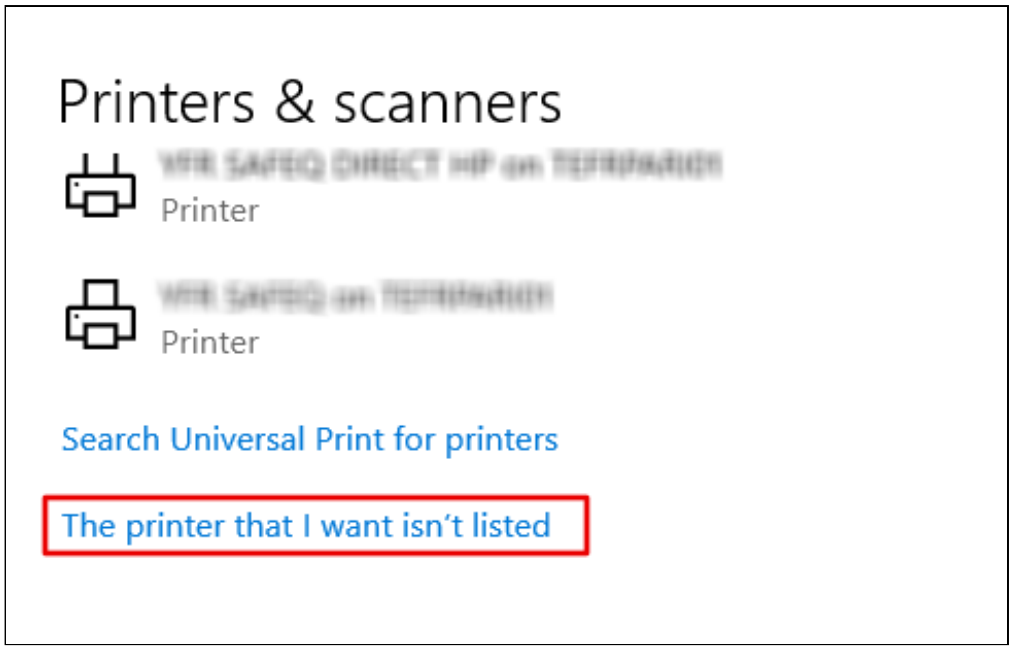
3.4.3 MANUALLY CREATING DIRECT PRINT QUEUES

Use this chapter if your administrator has instructed you to create a direct print queue manually. Otherwise, you can deploy a direct print queue from your Client v3, see Using Dispatcher Paragon Client v3.

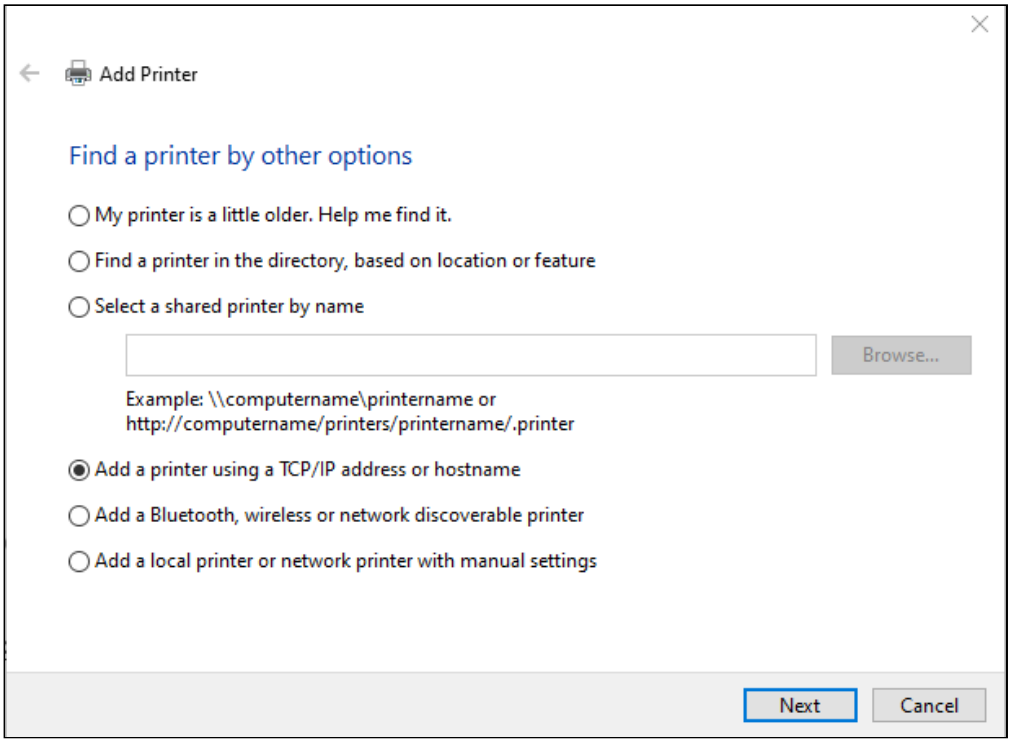
Note that even if you are creating a direct print queue manually, you must have Dispatcher Paragon Client v3 installed.

Creating a direct print queue on a Windows workstation

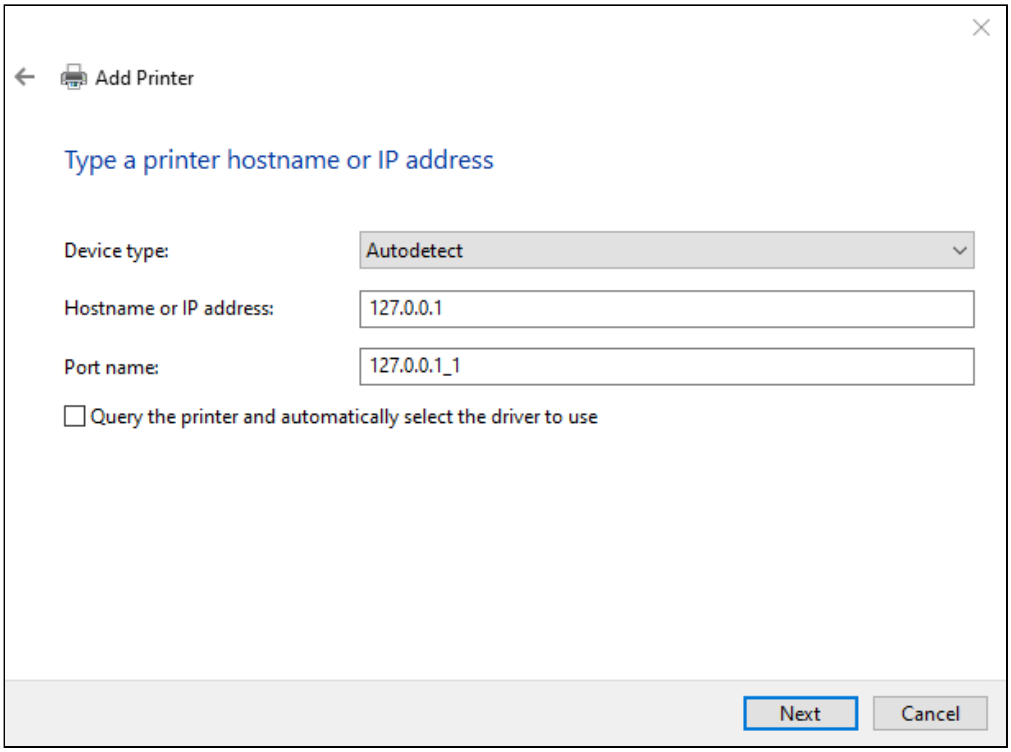
1. Every direct queue has a specific name and is assigned to a specific MFD. Ask your administrator for the queue name and driver name that you should use.
2. Go to Printers & scanners. Click **Add printer or scanner**. The system will search for printers in your network.
3. Click **The printer that I want isn't listed** to access the **Add Printer** dialog window.



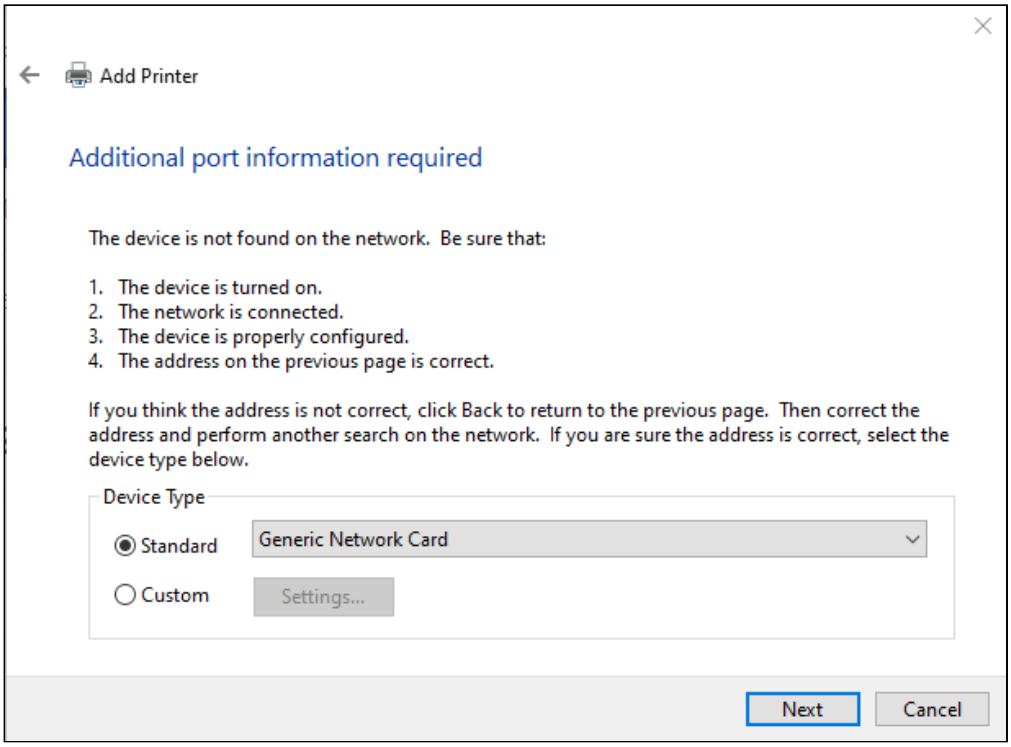
4. Select **Add a printer using a TCP/IP address or hostname**. Click **Next**.



5. In **Hostname or IP address**, enter 127.0.0.1 (loopback address). The port name is generated automatically from the IP address. Click **Next**.



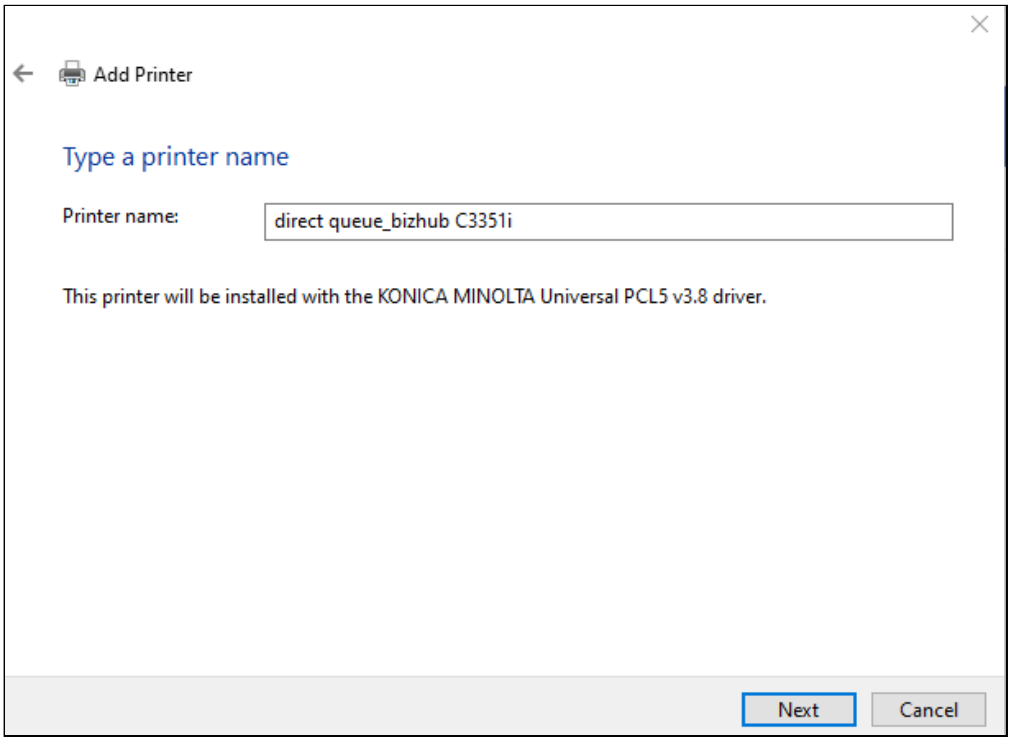
6. In **Device type**, select **Standard**. Click **Next**.



7. Select the driver that your administrator has advised you to use. Click **Next**.

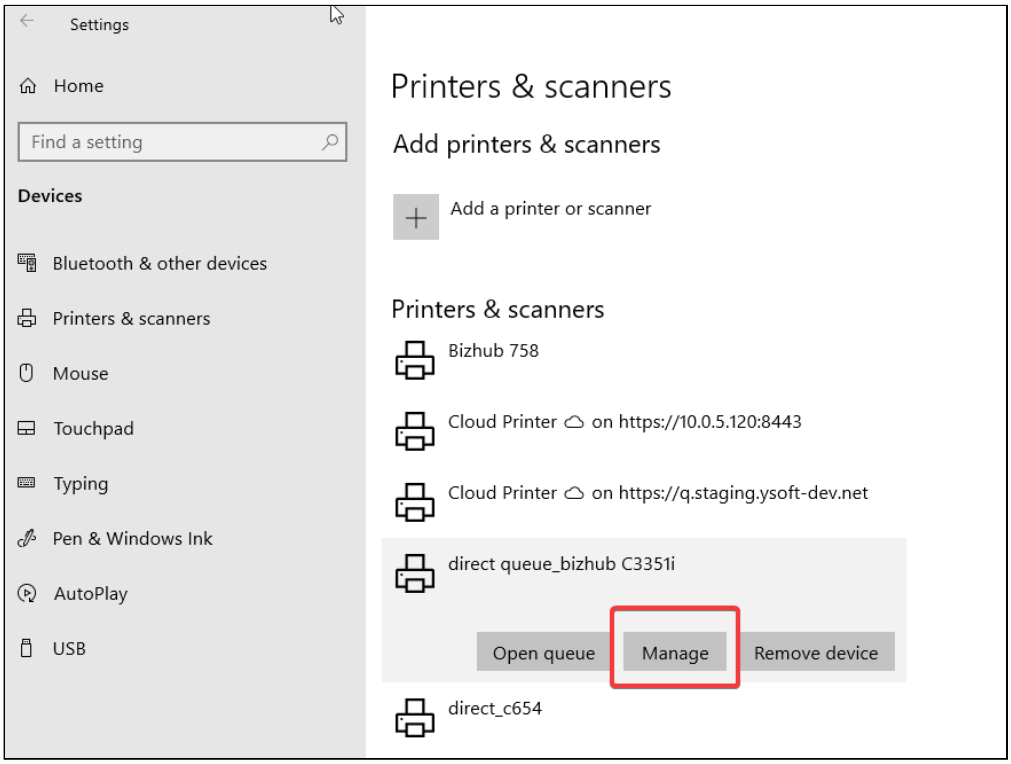
8. On the next screen, select **Use the driver that is currently installed**. Click **Next**.

9. Enter the printer name. This name will be visible to you only. Click **Next**.



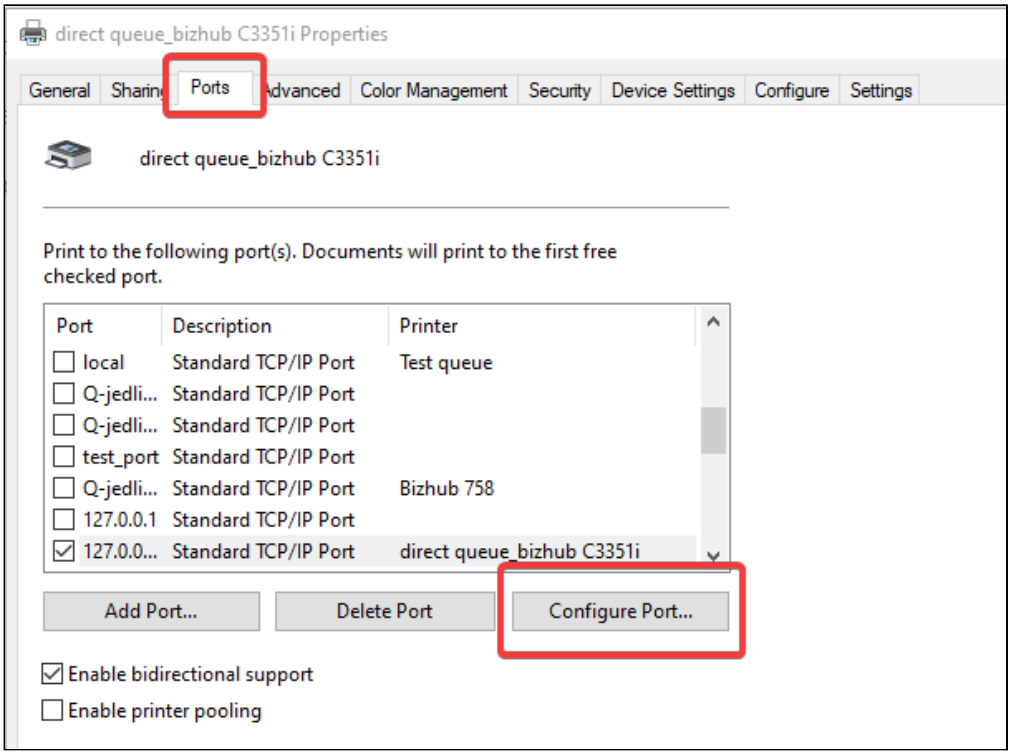
10. On the next screen, select **Do not share this printer**.

11. Click **Finish**.
12. Go to your **Printers & scanners** again and click the newly added printer.
13. Click **Manage**.

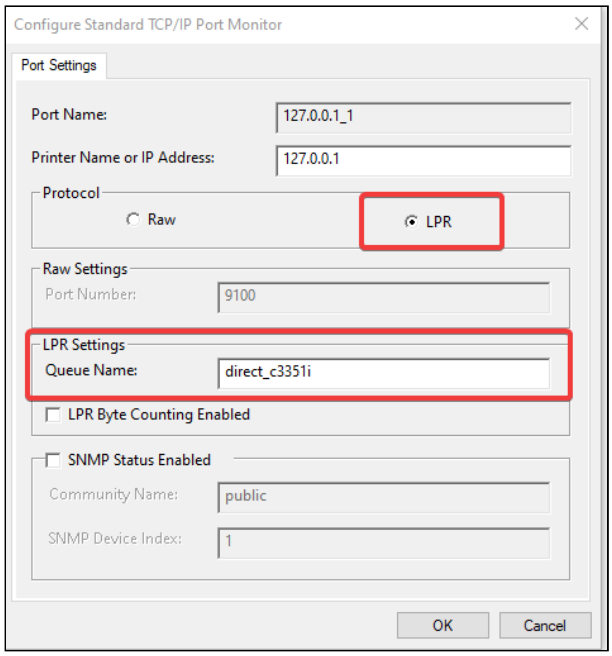


14. Click **Printer properties**.

15. Click **Ports** and then **Configure Port**.



16. In **Protocol**, select **LPR** and in the **Queue name**, enter the direct queue name provided by your administrator.



17. Click **OK** and then click **Close**.

18. Now you can start sending your print jobs to the reporting-only device. Be aware that the direct queue to this device will be visible in your Windows only, not in your Client v3.

3.5 USING DISPATCHER PARAGON CLIENT V3

3.5.1 ABOUT

Dispatcher Paragon Client v3 is a desktop application for end users, through which you can:

- Submit your print jobs to the cloud
- See the list of waiting print jobs and printed print jobs
- Delete print jobs
- Mark print jobs as favorite
- Deploy direct print queues to your workstation.
- Manually select your location – a feature for users traveling between different locations

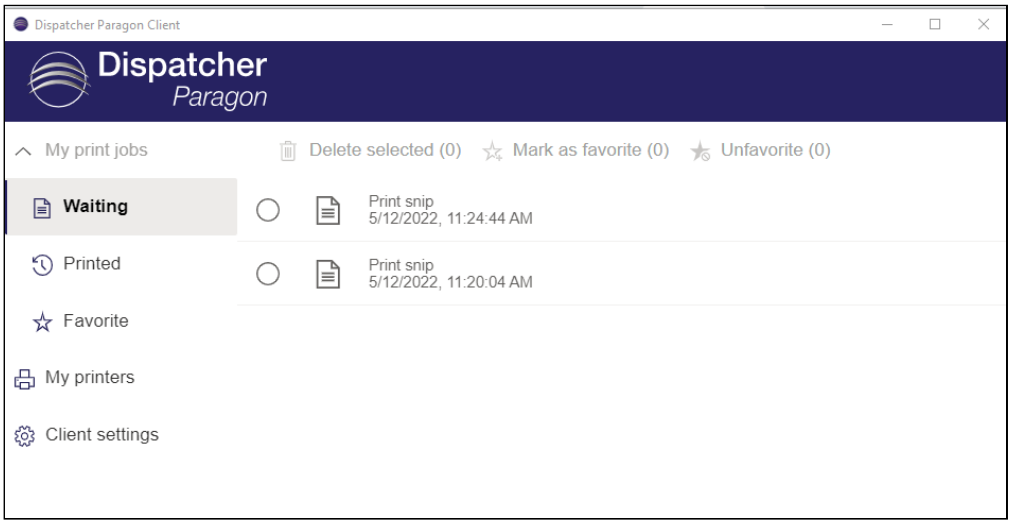
3.5.2 USING DISPATCHER PARAGON CLIENT V3

Installation

You will receive the installation file from your administrator, or the Client v3 will be deployed to your workstation automatically. The installation file will also deploy one or more printers (print queues) to your workstation. The printer names are defined by your administrator.

Logging in

1. After installation, right-click on the Client v3 icon in the system tray (Windows) or menu bar (Mac OS) and select **Open**. If you send a print job to the printer deployed by Dispatcher Paragon Client v3, this action will also open the Client v3 and you will be prompted to log in.
2. On the login screen, if you are an Externally managed user, click **Sign in with Microsoft** and enter your Microsoft credentials. If you are an Internally managed user, enter your Dispatcher Paragon Cloud credentials and click **Sign in**.
3. After successful login, you will see the Client v3 home screen.



Logging out

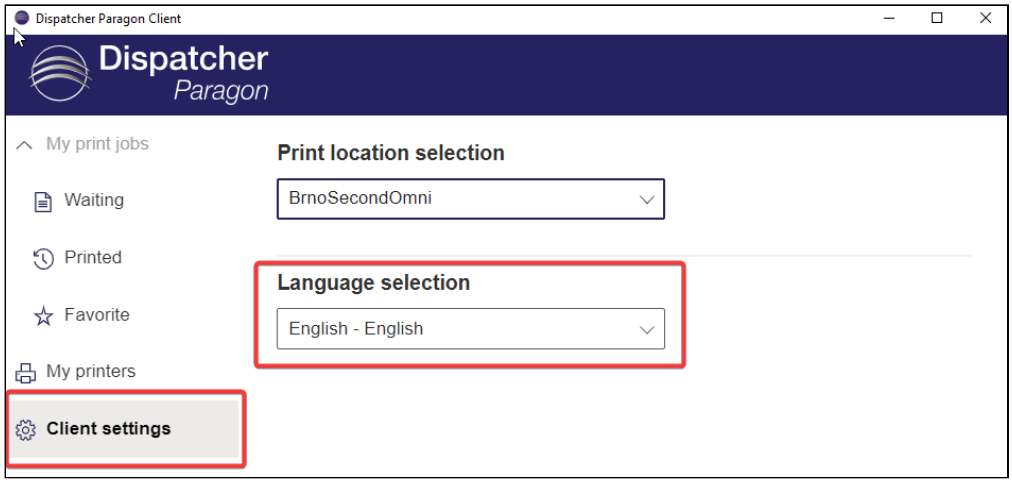
Note that there is no Logout button in the application. The application will log you out when your authentication token expires. If you need to log out without waiting for token expiration, you can remove the credentials manually in the Windows Credential Manager. Remove all credentials related to **Print Management Client**. For details on the Windows Credential Manager, see https://support.microsoft.com/en-us/windows/accessing-credential-manager-1b5c916a-6a16-889f-8581-fc16e8165ac0.

Changing language settings

To change the language settings, right-click on the Client v3 icon in the system tray (Windows) or menu bar (Mac OS) and select **Language settings**. Select your preferred language from the list.

Alternatively, you can change the language in **Client settings**:

1. Open your Client v3.
2. Click **Client settings.**
3. Select your language from the **Language selection** dropdown menu.



List of waiting, printed, and favorite print jobs

The list of waiting print jobs is the default list that you will see after logging into Client v3.

To see the list of your printed jobs, click **Printed** in the left sidebar menu.

To see the list of your favorite jobs, click **Favorite** in the left sidebar menu.

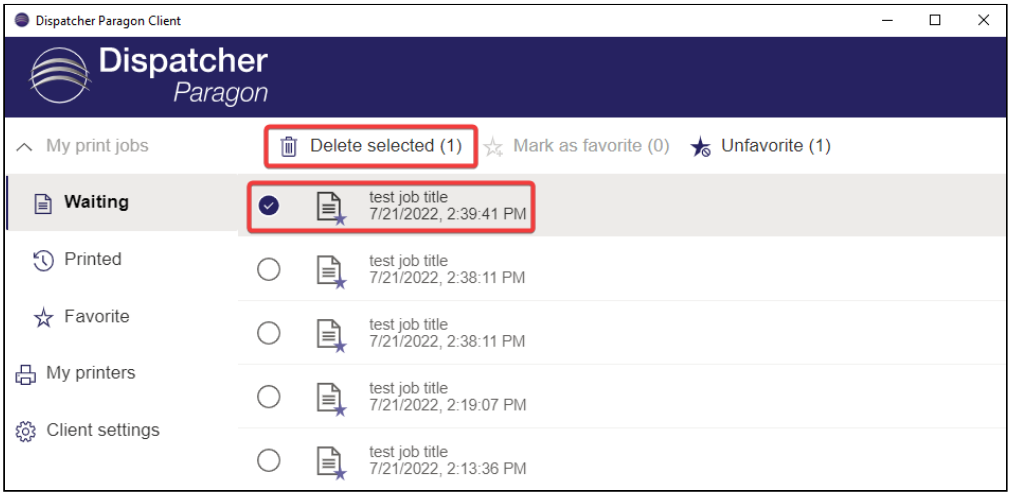
Submitting print jobs

Submit your print jobs to the printer deployed to your workstation by the Client v3 installation file. If you are not sure which one it is, contact your administrator.

If you submit a print job to a direct print queue and the target printer/MFD is not available, e.g., offline, the print job will appear on the **Waiting** list in your Client v3. If the MFD is in power save mode, your print job will be printed after it wakes up.

Deleting print jobs

To delete a waiting print job, go to the list of your waiting jobs and click the job you wish to delete. Click **Delete selected**.



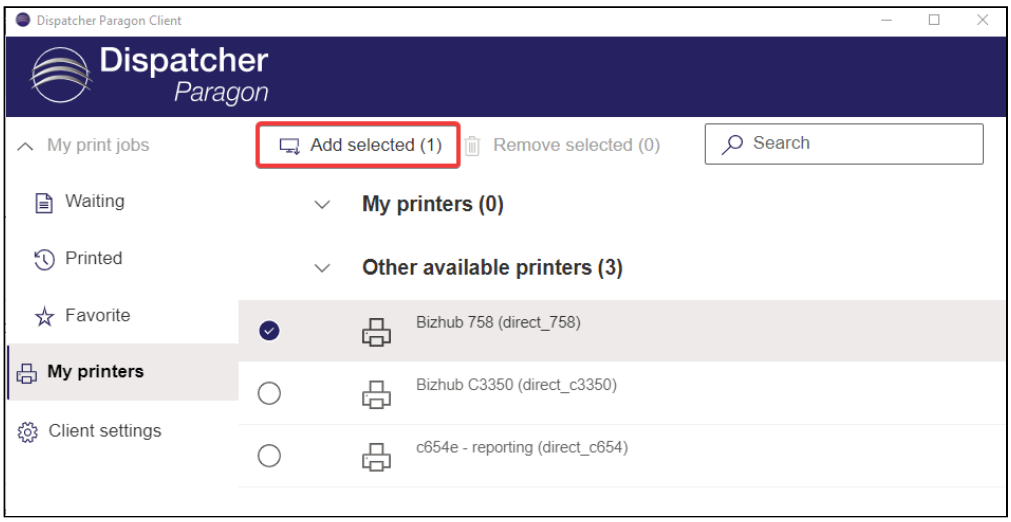
Marking print jobs as favorite

To mark a job as favorite, go to the list of your waiting or printed jobs and click the job you wish to mark. Click **Mark as favorite**. To remove the job from favorites, go to the **Favorite** list, select the job and click **Unfavorite**.

Adding direct print queues to your workstation

If your administrator has created any direct print queues in your company's Dispatcher Paragon Cloud and made them available to you, you will see them in your Client v3. You can add the direct print queues to your workstation via Client v3. Direct print queues are used most often for reporting-only devices, in case the print jobs must be printed at a particular device and do not require authentication before release.

1. Click **My printers** to see the available direct queues that your administrator has created.
2. In the **Other available printers** section, click the direct queue that you wish to deploy on your workstation.
3. Click **Add selected**.



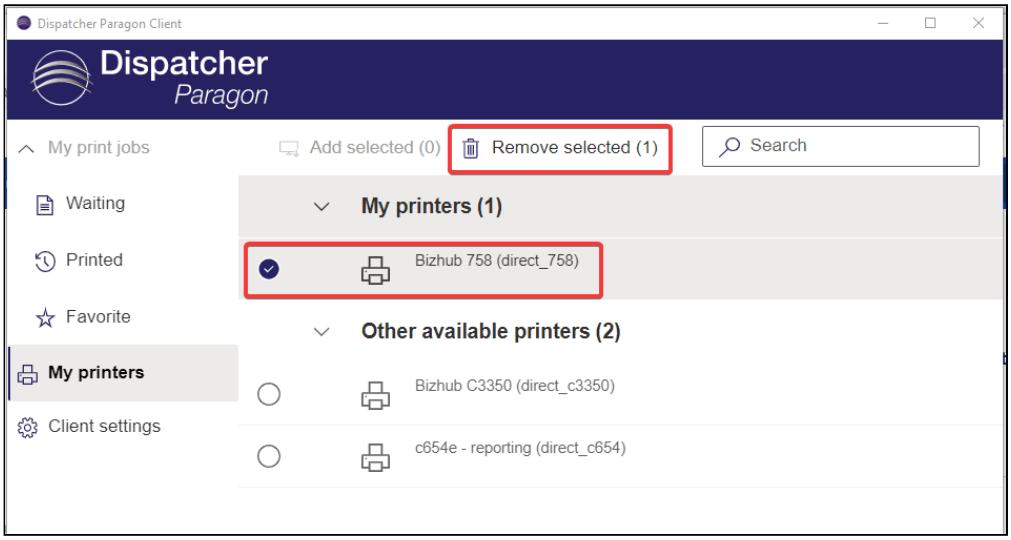
4. The queue will appear in your **My printers** section in Dispatcher Paragon Client v3 and in your **Printers and scanners** in your operating system.

Removing direct print queues from your workstation

You can remove any of the direct print queues that you have added to your workstation via Client v3.

To remove a deployed print queue, perform the following steps:

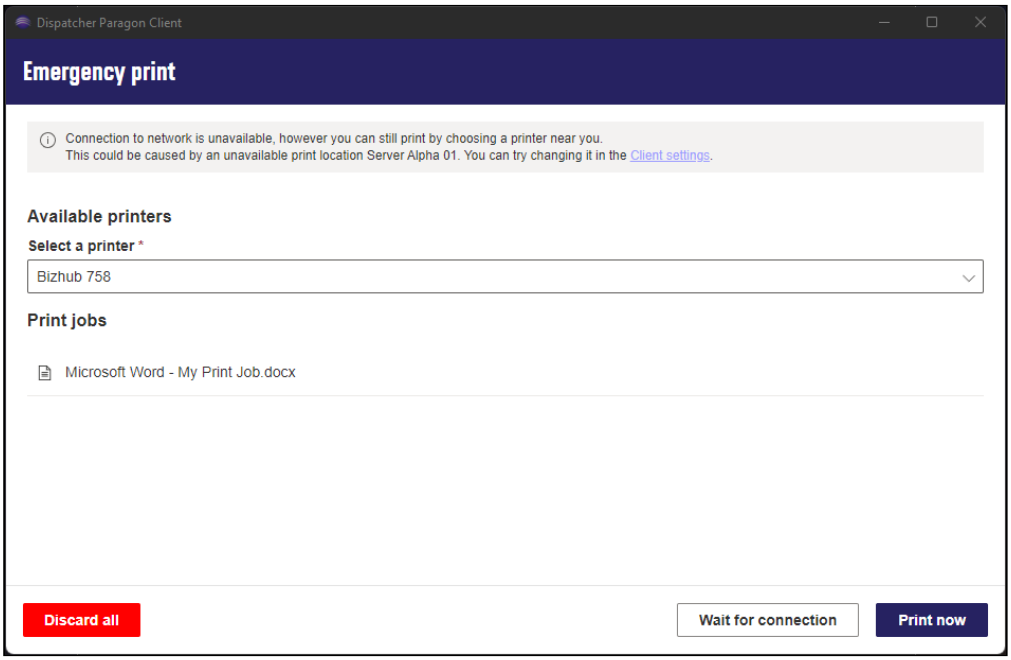
1. Click **My printers**.
2. Select the printer or printers that you wish to remove. You can use the search function to narrow down the number of printers displayed.
3. Click **Remove selected**.



Emergency print

If your administrator has enabled this feature, emergency print provides limited printing functionality while a site server is inaccessible. During an emergency print, Client v3 sends print jobs directly to the printer, without sending them to the site server. The print jobs are printed immediately on the selected printer.

If you try to print when a site server is unavailable, the Emergency print window will pop up.



If you have previously used some printers, you will have four options:

1. Select a printer from the list and click **Print now** to print the job.
2. Click **Wait for connection** to send the print job to the site server as soon as the connection is restored. Be aware that this method does not work for print jobs sent to direct print queues – those will be discarded and you will need to print them again when the connection is restored
3. Click **Discard all** to cancel the printing of all print jobs.
4. If the manual site server selection is enabled for you, click **Client settings** and change the location. Be aware that your print job will be canceled. You must send it again after changing the location. Do this only if the new location is within your reach, for example, if it's another floor of your office building.

If you haven't previously used any printer, you will have three options:

1. Click **Wait for connection**.
2. Click **Discard all**.

3. If the manual site server selection is enabled for you, click **Client settings** and change the location. Be aware that your print job will be canceled. You must send it again after changing the location. Do this only if the new location is within your reach, for example, if it's another floor of your office building.

Print location selection

If your company uses Edge printing and your administrator has enabled the option of print location selection in order to support traveling users:

- the traveling users must change print locations in their Client v3 each time that they travel between different locations
- unless instructed otherwise by their administrator, non-traveling users do not need to make any manual selection.

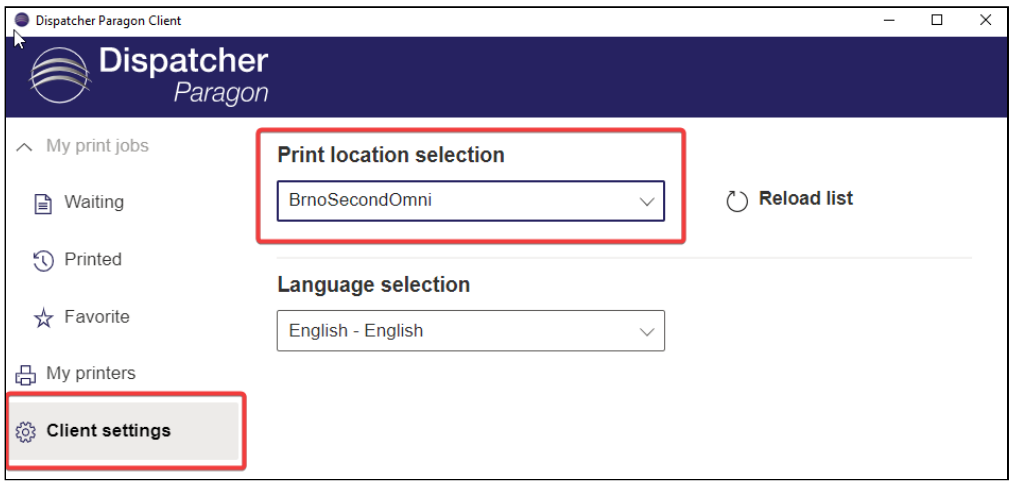
This feature ensures that:

- your print jobs will be sent to the server at the print location that you selected in Client v3.
- you can release your print jobs at MFDs at the selected print location.

If you created a print queue according to Configuring IPP print queues, print location selection in Client v3 has no effect. In this case, you must create a print queue for each location separately, and send your print jobs to the correct queue, according to your current location.

To select a site server manually, perform the following steps:

1. Open your Client v3.
2. Click **Client settings.**
3. In **Print location selection**, select a location from the drop-down menu.



If your administrator hasn't enabled Print location selection, you will be not able to change the print location. To enable it, contact your administrator.

4. Click **Reload list**.

   If you don't see this option, it means that reloading is not necessary because your Client v3 is not configured to download the list of site servers from the cloud.

5. When traveling to another location, perform the print location selection again, before you send any print jobs.

   You can also access the **Client settings** by right-clicking on the Client v3 icon in the system tray and then selecting **Client settings**.

3.6 USING AN MFD

To use an MFD, perform the following steps:

1. Register yourself in Dispatcher Paragon Cloud (see Registering yourself in Dispatcher Paragon Cloud).
2. Register your card (see Card registration at the MFD terminal) or generate a PIN (see Management interface guide, section *Generating a PIN*). The authentication method depends on how your administrator set up the MFD.

For information on how to perform operations like copying, printing, and scanning on an MFD, see:

- For MFDs with Cloud Terminal: Dispatcher Paragon Cloud Terminal for Konica Minolta

- For Konica Minolta MFDs with Embedded Terminal: Dispatcher Paragon Embedded Terminal for Konica Minolta

3.6.1 CARD REGISTRATION AT THE MFD TERMINAL

If you are a new user of Dispatcher Paragon Cloud, you must either register your card or generate a PIN to be able to log in at an MFD. The authentication method depends on the MFD setup done by your administrator.

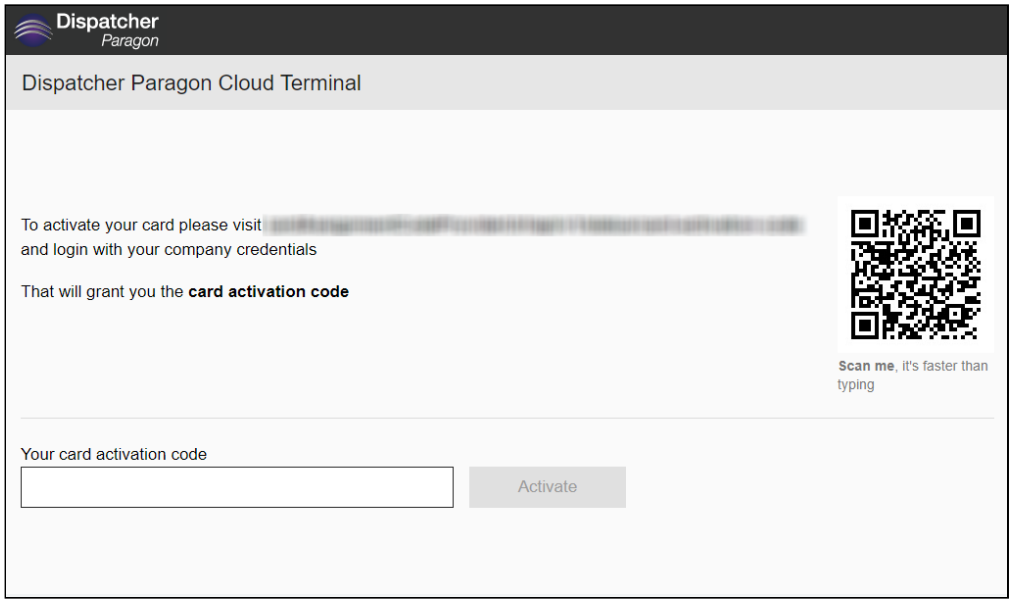
If you are an already-existing user who needs to register a new card, follow this process as well.

For generating a PIN, see Management interface guide.

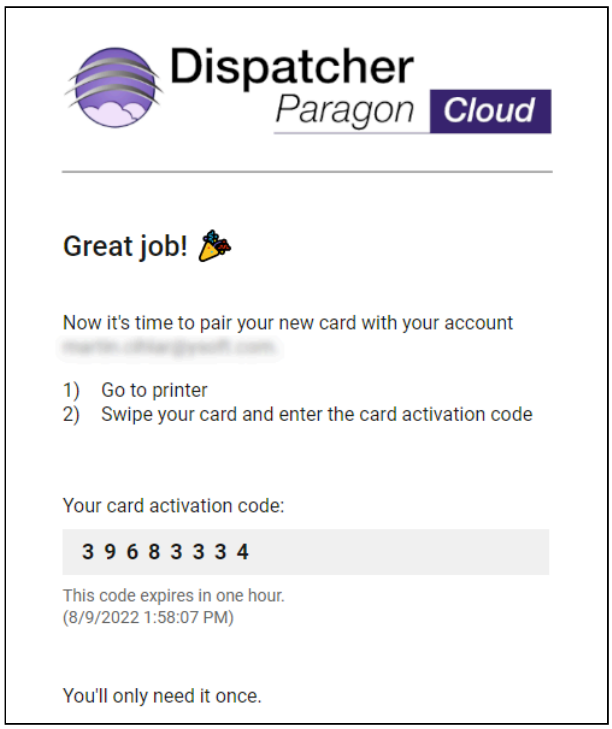
Card registration at the MFD with Dispatcher Paragon Cloud Terminal

If your company uses Pure cloud printing, perform the following steps to register your card:

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 card activation code.
2. Use your mobile phone to scan the QR code displayed at the terminal or type the address displayed there into your web browser. This will take you to the Card activation code provider page.
   Note: Do not use the QR code from this screenshot.



3. If you are an Externally managed user, log in with your company credentials. If you are an Internally managed user, log in with your Dispatcher Paragon Cloud username and password. Your card activation code will be generated.



4. Back at the MFD terminal, swipe your card again (if the login screen timed out in the meantime), enter the card activation code, and tap **Activate**.
5. The system will assign the card to you and log you in. From now on, you can use the card to log into all terminals.

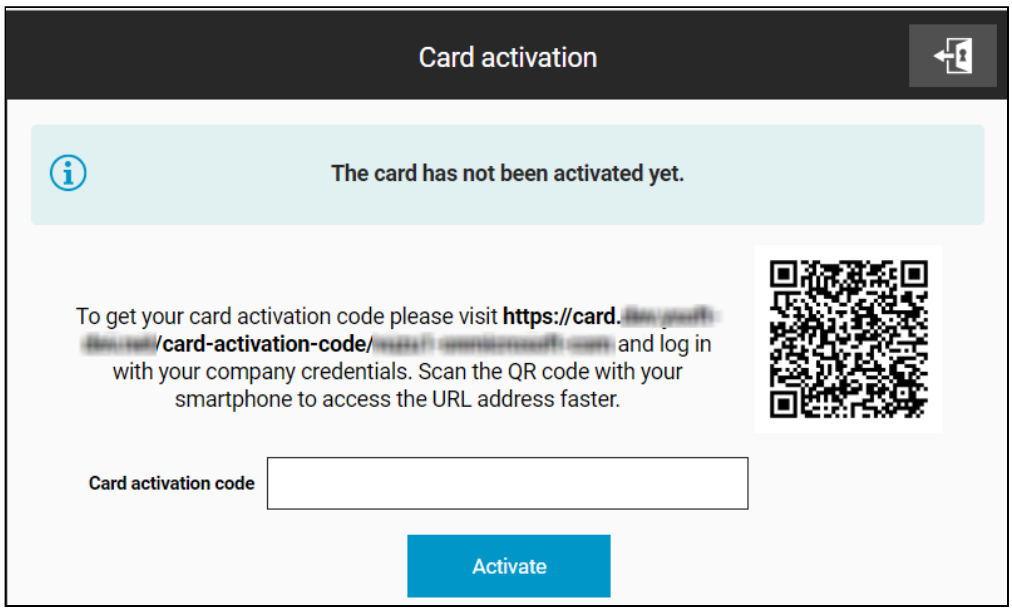
Card registration at MFD with Dispatcher Paragon Terminal Embedded

If your company uses Edge printing, perform the following steps to self-register.

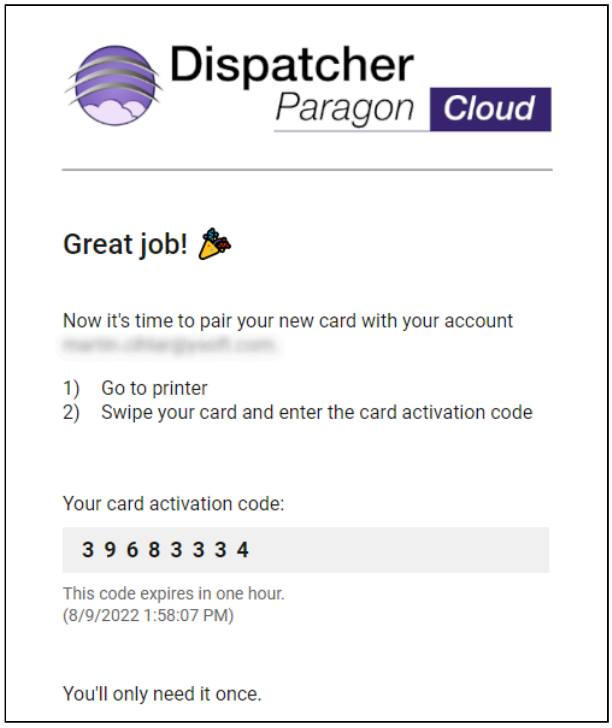
1. Go to the MFD of your choice and place your card on the card reader. The terminal will recognize an unassigned card and prompt you to enter your card activation code.

   ⚠ If you see a choice between **Activation code** and **Username and password**, you must choose **Activation code**.

2. Scan the QR code, or type the URL displayed at the terminal into your web browser. This will take you to the Card activation code provider page.



3. If you are an Externally managed user, log in with your company credentials. If you are an Internally managed user, log in with your Dispatcher Paragon Cloud username and password. Your card activation code will be generated.



4. Back at the MFD terminal, swipe your card again (if the login screen timed out in the meantime), enter the card activation code, and tap **Activate**.

5. The system will assign the card to you and log you in. From now on, you can use the card to log into all terminals.

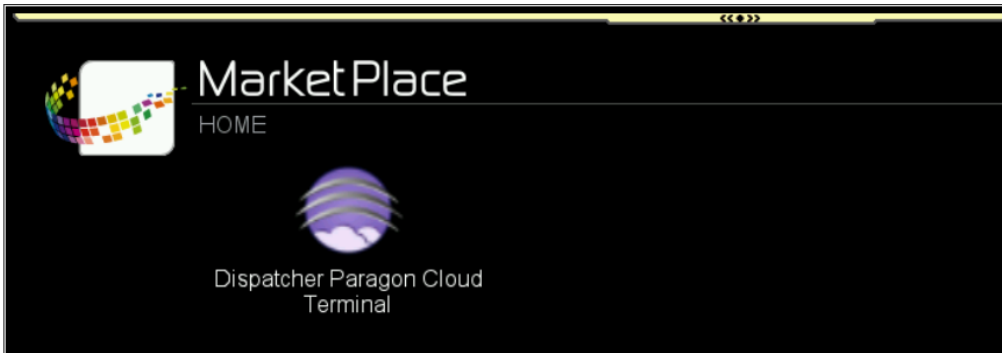
3.6.2 DISPATCHER PARAGON CLOUD TERMINAL FOR KONICA MINOLTA

Logging in and logging out

Logging in

> Authentication by card or by PIN is the only supported method. Do not use your company username and password to log in at the MFD terminal.

1. On the home screen of the MFD, tap **MarketPlace** > **Dispatcher Paragon Cloud Terminal**.



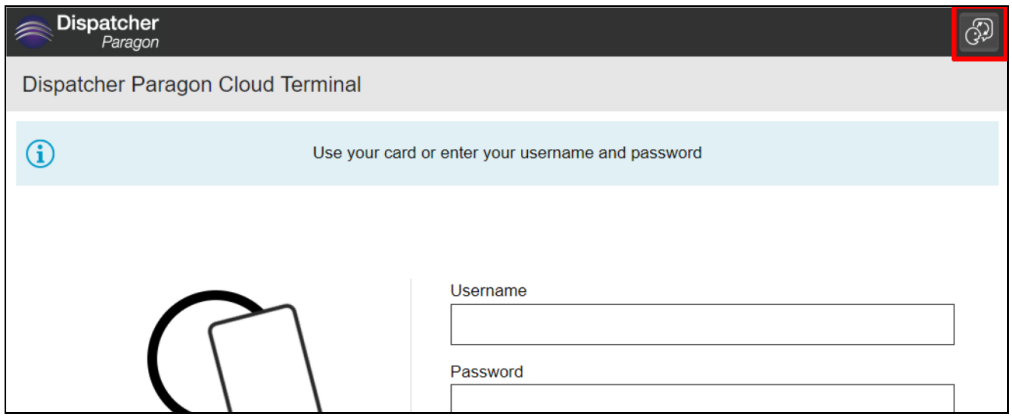
> Your administrator may have set the MFD to display the Dispatcher Paragon Cloud Terminal login screen as the home screen.

2. Enter your PIN and tap **Login** or place your card on the card reader attached to the printer. The available authentication method depends on the configuration done by your administrator.
3. You will see the Dispatcher Paragon Cloud Terminal home screen.

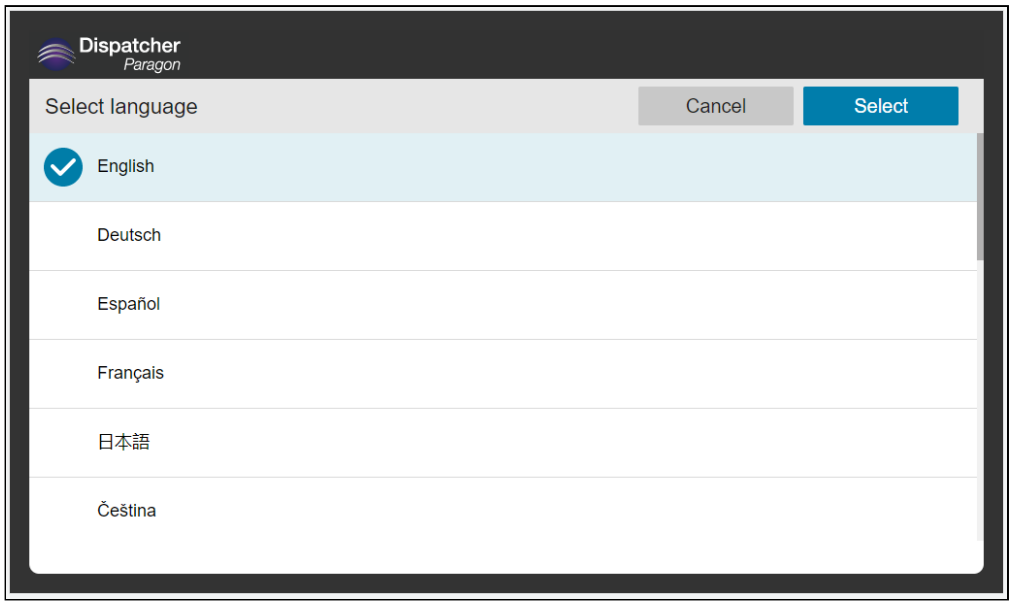
> If another user is logged in, you will log them out by placing your card on the card reader. If you want to log in, you must place your card on the card reader once again.

Selecting language

1. Tap the **language icon** to display the *Select language* dialog.



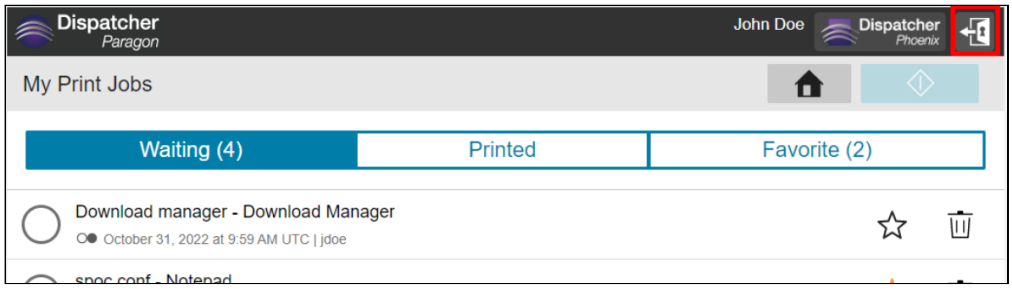
2. Select the language and tap **Select**. For the list of supported languages, see the *Supported languages* section.



Logging out

You can use two methods to log out:

1. Tap the Log out icon on the home screen of Dispatcher Paragon Cloud Terminal.



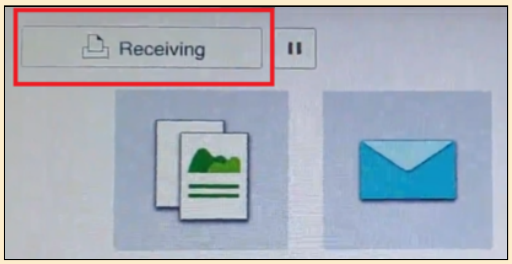
2. Place your card on the card reader attached to the printer (if the terminal uses card authentication).

Printing and managing jobs

Printing

1. **Log in** to the Dispatcher Paragon Cloud Terminal.

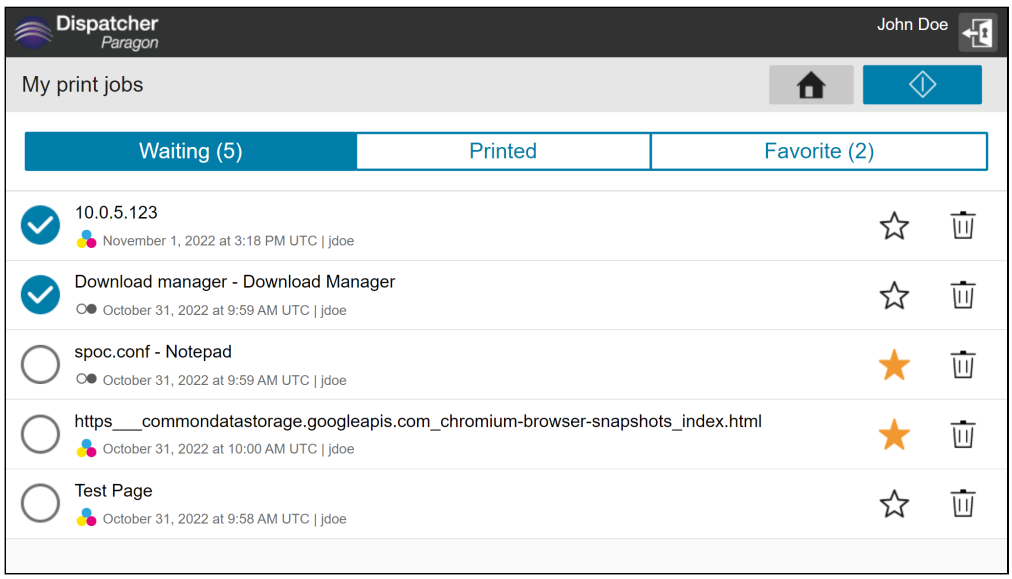
   ⚠ If the MFD is in the **Receiving** state, logging into the Dispatcher Paragon Cloud Terminal is temporarily disabled until the job has been received completely.

2. Tap **My print jobs**. You will see the list of waiting jobs.

   ⓘ If you have no jobs in the folder, you will see message *Folder is empty* instead of a job list.

3. Select at least one job and tap the **Start button** at the top of the page.



If you want to print all the waiting jobs at once, tap **Print all** on the home screen.

If printing of a large print job takes long enough for the MFD screensaver to start, the print job will stay in the "printing" status even though it was printed successfully. The status will change to "printed" only after you or another user log in to the Cloud Terminal again.

Marking a print job as favorite

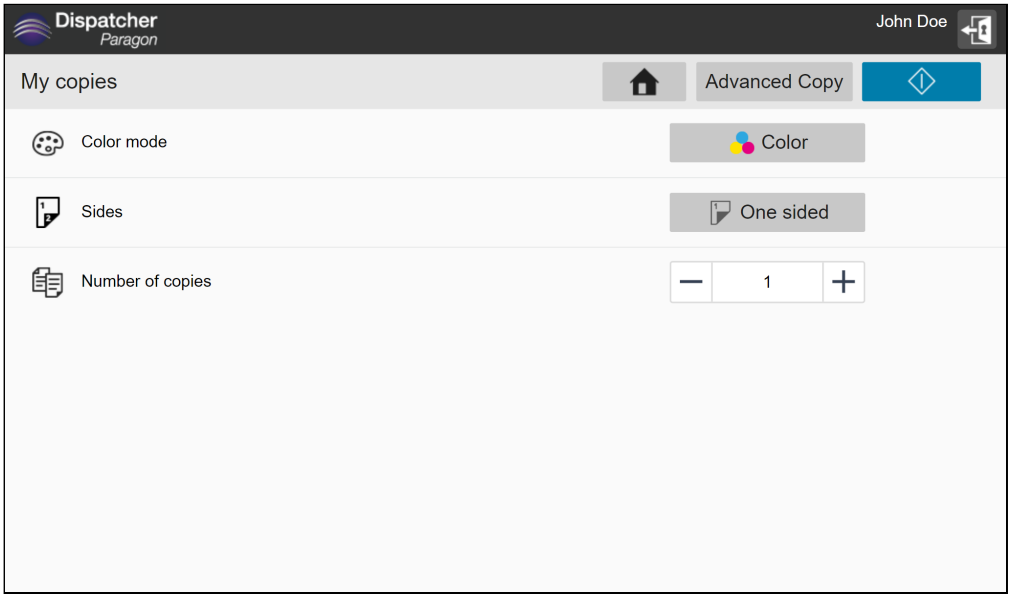
To mark a print job as a favorite, click the star icon next to the job. You can then find your favorite jobs in the **Favorite** folder.

Deleting a print job

To delete a print job, tap the trash bin icon next to the print job.

Copying

1. On the home screen of the **Dispatcher Paragon Cloud Terminal**, tap **My Copies**.
2. Set the desired parameters of your copy by tapping the available options.

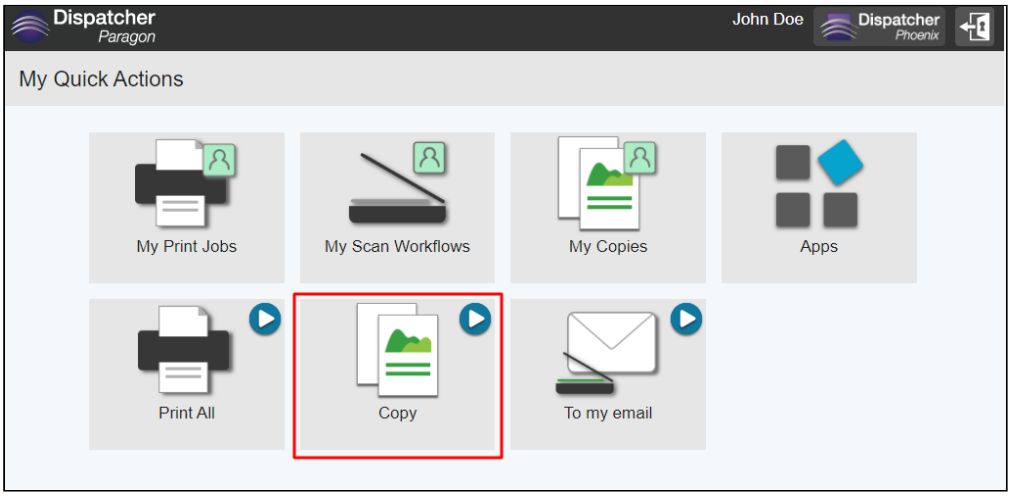


3. Tap the **Start** button at the top of the screen to start copying.

Using the native Copy application

If your administrator installed the **Dispatcher Paragon Cloud Terminal** with Copy feature and enabled copying via the native Copy application, you can open the native copy application by clicking **Advanced Copy** on the **My copies** home screen.

If your administrator didn't install the **Dispatcher Paragon Cloud Terminal** with the Copy feature, you can open the native copy application by tapping **Copy** on the home screen of **Dispatcher Paragon Cloud Terminal**.

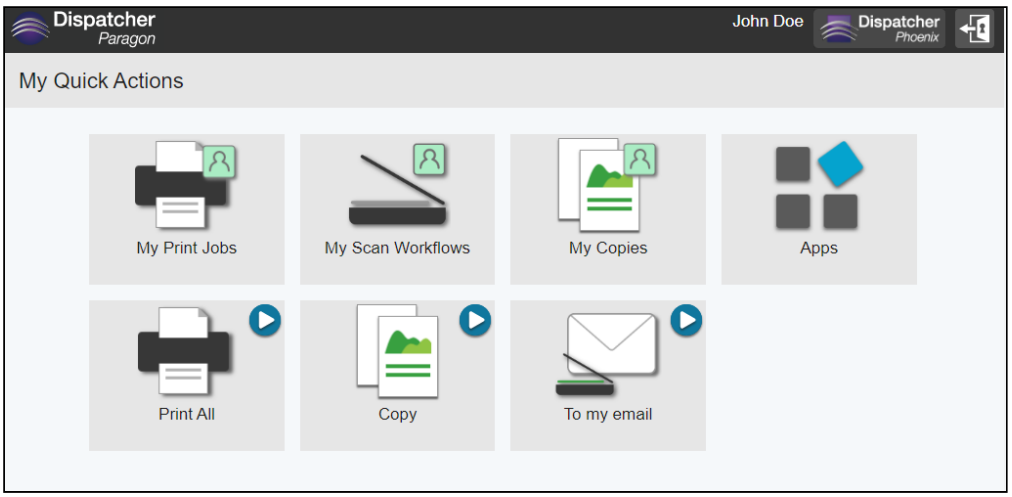


If you go to the native Copy application and want to use the functions of the **Dispatcher Paragon Cloud Terminal** again, you must reopen Dispatcher Paragon Cloud Terminal.

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.

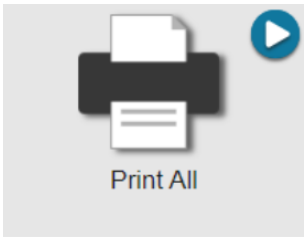
After logging in at the MFD, tap the quick action you want to execute. The actions that you can execute directly (because they don't require any input from you) are called *instant* and are marked with a *Play* icon.



Print all

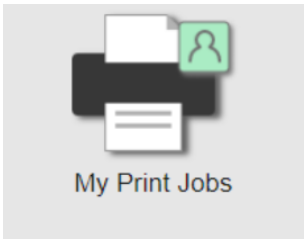
Tap **Print all** to print all jobs in your queue.

If there are no jobs, the **Print all** button is disabled.



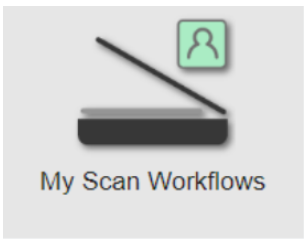
My print jobs

Tapping **My print jobs** opens the **Print** application. See the *Printing and managing* jobs section of this document.



My scan workflows

Tapping **My scan workflows** opens the **Scan** application.

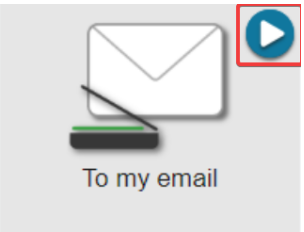


If you scan large files, internal processing may take several minutes. Logins to Dispatcher Paragon Cloud are disabled until the processing is complete.

Scan – Instant workflows

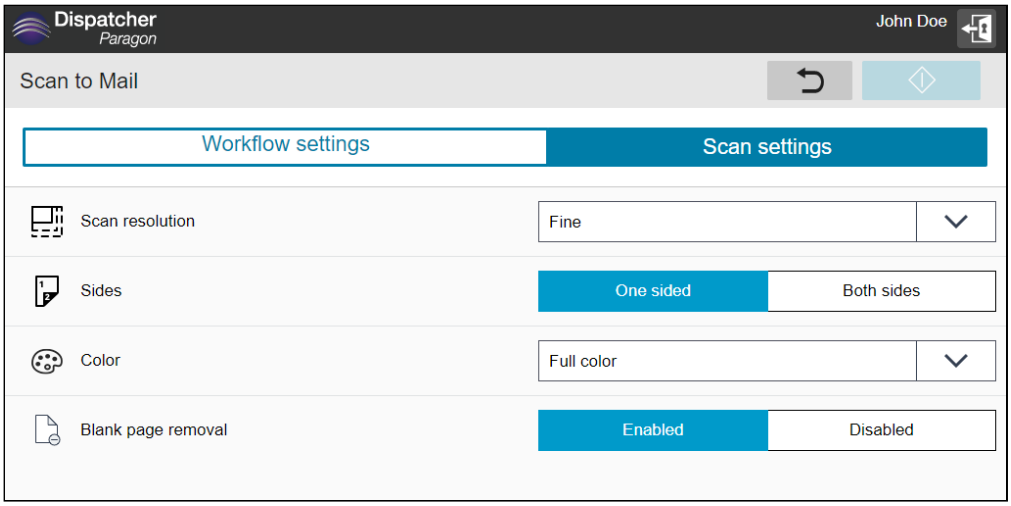
To execute an instant workflow directly from **My quick actions** application, tap the instant workflow button.

Example:



Scan – workflows with input required

1. To execute a scan workflow with mandatory user input, tap the scan workflow button with the name of your chosen workflow.
2. You will be redirected to the workflow detail screen.
3. Fill in the required information on the **Workflow settings** tab.
   Example:



4. Tap the **Scan settings** tab to modify the scan job properties.

   If the **Scan settings** tab is not visible, it means that the scan settings are not configurable by end users.

5. Tap **Scan** to start the scan job. You will be redirected back to **My quick actions** application when finished.

If the screensaver is enabled on the MFD, scanning has the following limitations:

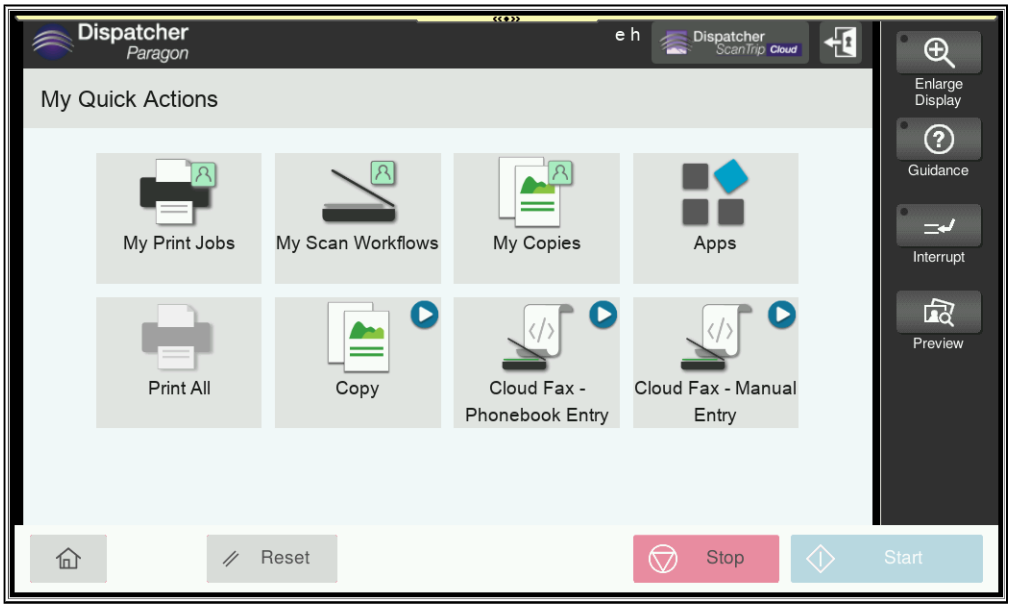
- If you are scanning a large file, the delivery of the scan job to your email may be delayed by 10 minutes (at maximum).
- If you are scanning a file with page separation enabled and another user logs in to the cloud terminal within 10 minutes after you finish scanning, your scan job will not be delivered and you will need to scan it again.

Also, be aware that email limits might block the delivery if the file is too large.

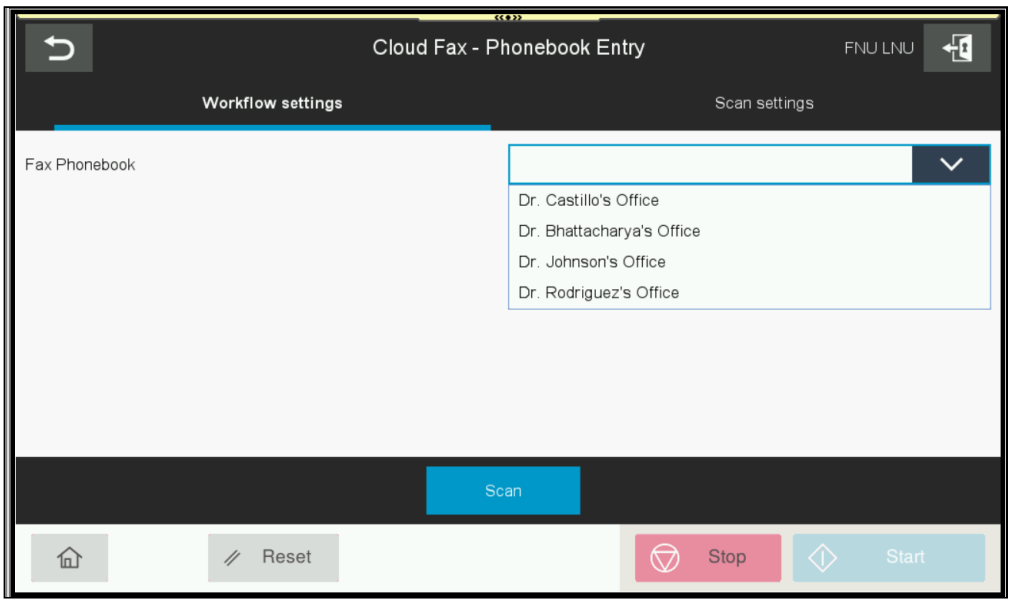
Scan - Cloud Fax workflows

The Cloud Fax service is a high-capacity, reliable, and globally accessible service that enables the transmission and reception of faxes from a web portal or a Konica Minolta MFD. If your company purchased this service, perform the following steps to send faxes from the MFD:

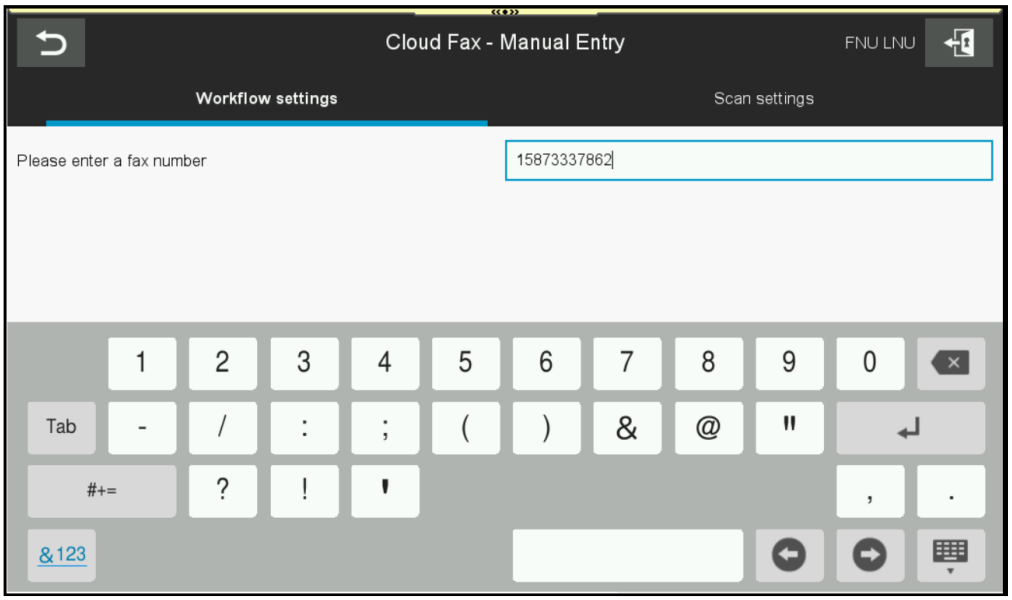
1. Select a Cloud Fax sending method. There are two methods that your Administrator may have configured: Phonebook entry and Manual entry. Your Administrator could have configured one or both methods.



   a. Phonebook entry – this method allows you to select a predefined fax number from a list of numbers. Your Administrator may list the recipient's name, fax number, or both. In this example, only the name of the recipient is shown. To update or add a new recipient, please contact your Administrator.



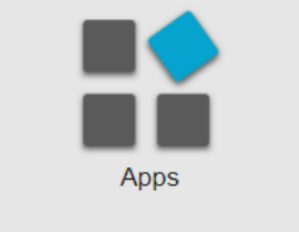
b. Manual entry – this method allows you to enter a fax number manually.



2. After selecting the recipient from the list or entering the number manually, tap **Scan**. Your document will be scanned and transferred to the cloud fax service. If your administrator configured email notifications in the system, you will receive an email notification with the status.

Apps

Tap **Apps** to see the screen with installed apps.



DP Phoenix

Tap **DP Phoenix** to enter the **Dispatcher Phoenix** application (if installed on the MFD).

Supported languages

- Brazilian Portuguese
- Chinese Simplified
- Czech
- Danish
- Dutch
- French
- German
- Hungarian
- Italian
- Japanese
- Polish
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish
- Turkish

Troubleshooting

You are prompted to register your card even though it's already registered

You have already registered your card and used it to release print jobs in the past, but now you receive a message on the MFD terminal that you need to register your card. This happens if the synchronization of your account with an external Identity Provider (such as Azure Active Directory) fails, and Dispatcher Paragon Cloud needs to verify your identity again. You can resolve this by registering your card again. See the *Registering new card at the terminal* section in this document. If it doesn't solve the problem, contact your administrator.

3.6.3 USING DISPATCHER PARAGON EMBEDDED TERMINALS

Dispatcher Paragon Embedded Terminal for Brother

Logging in and out

Logging in

1. Place your card on the card reader attached to the printer or enter your PIN and tap **Login**. The authentication method depends on how your administrator configured the terminal.
2. You will see the Dispatcher Paragon embedded terminal home screen. The content of the home screen depends on how your administrator configured the terminal. It may contain shortcuts, **My print jobs** application, or other applications.

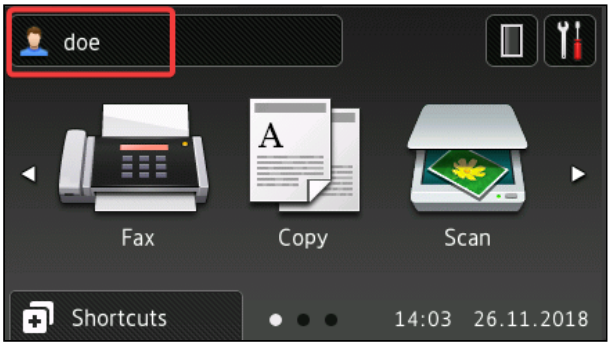
   > During logging in, you may see a prompt asking whether you wish to print all your compatible jobs after authentication.

Selecting language

Language selection is not supported.

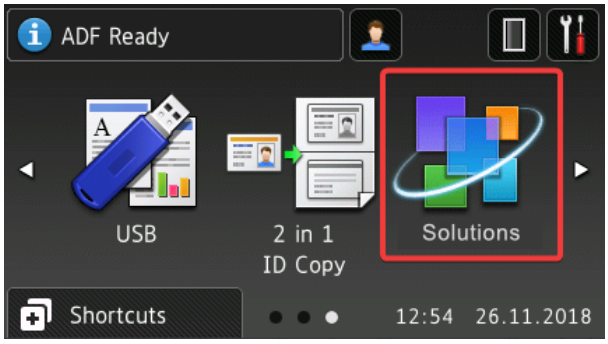
Logging out

To log out, tap your username in the top left corner of the main menu and confirm your action.

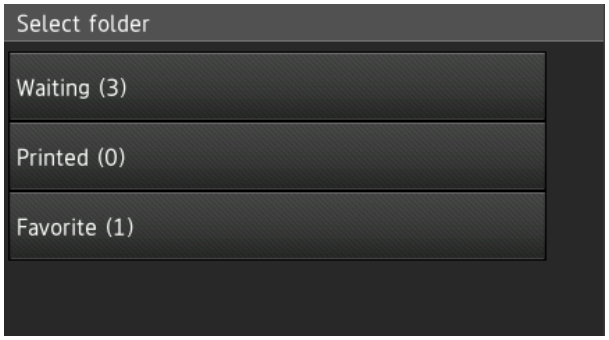


Printing and managing jobs

1. Log into the Dispatcher Paragon embedded terminal. The device main menu screen will be displayed. The content of the screen depends on the configuration done by your administrator.
2. If you are not redirected automatically to the print application, tap **Solutions** in the device main menu and then tap **Dispatcher Print**.

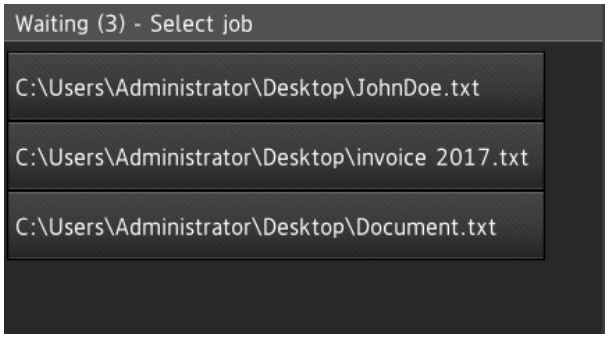


3. You will see the print application. Tap **Waiting** to display your waiting jobs.

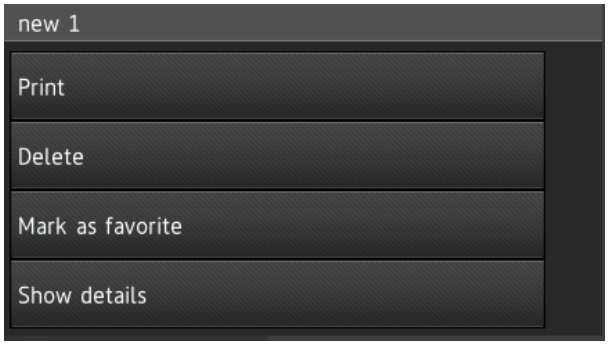


> ⚠ If there are no jobs in the respective folder, you will see zero displayed next to the folders.

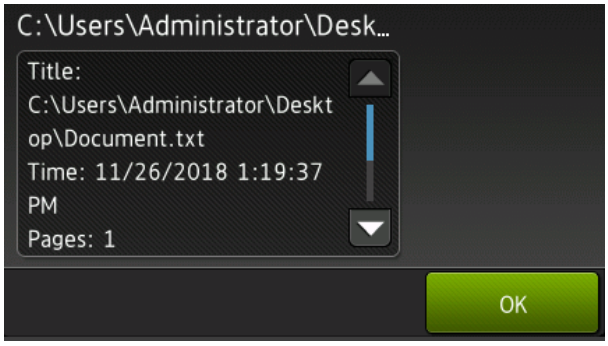
4. Tap **Waiting** to display your waiting jobs.
5. Tap the job you wish to print.



6. A list of options will be displayed. Tap **Print**.



7. You can see the details by tapping **Show details**, but you cannot modify the finishing options.



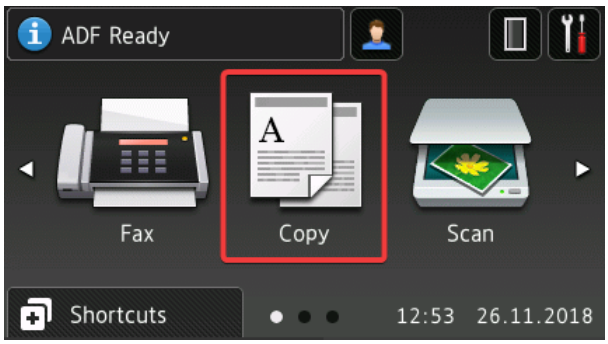
8. If you need to navigate to one of the previous screens, use the back arrow button. This will usually be a hardware button. You can also tap the home icon to return to the device main menu.

Copying

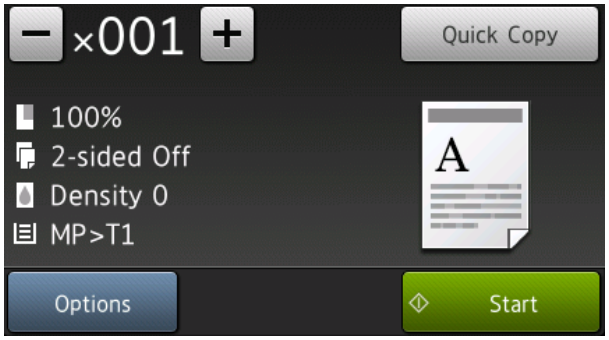
If you have permission for copying, perform the following steps:

1. Log in to the Dispatcher Paragon embedded terminal. The device main menu screen will be displayed. The content of the screen depends on the configuration done by your administrator.

2. On the main menu screen, tap **Copy**.



3. Select the number of copies by tapping the **+**and **-** buttons. Configure the copy settings by tapping **Options**.

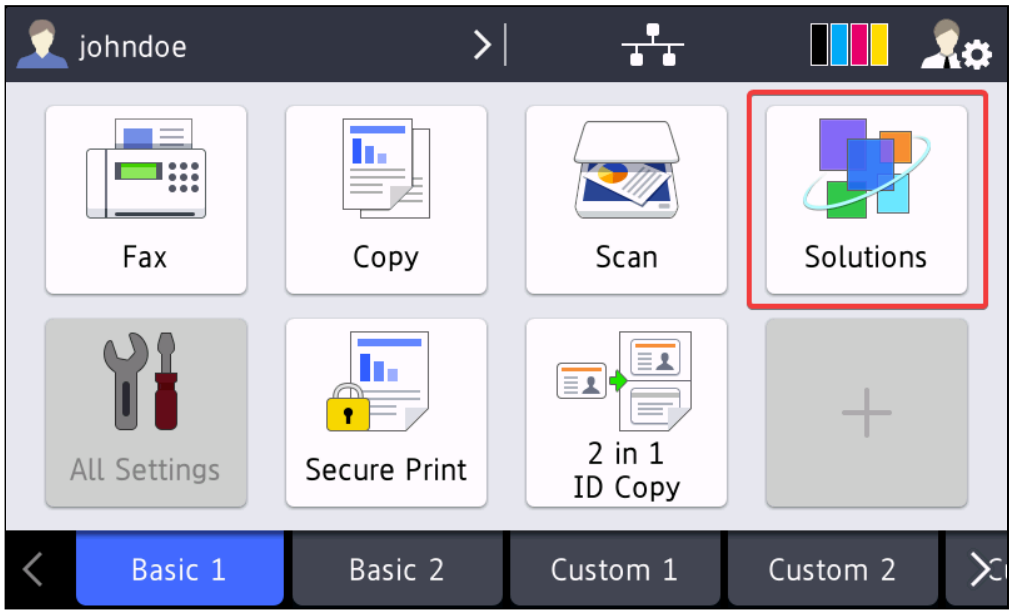


4. Tap **Start**.

Scanning

1. Log in to the Dispatcher Paragon embedded terminal. The device main menu screen will be displayed. The content of the screen depends on the configuration done by your administrator.

2. Tap **Solutions**. If you see the print application after logging in, tap the home button to go to the main menu screen and then tap **Solutions**.

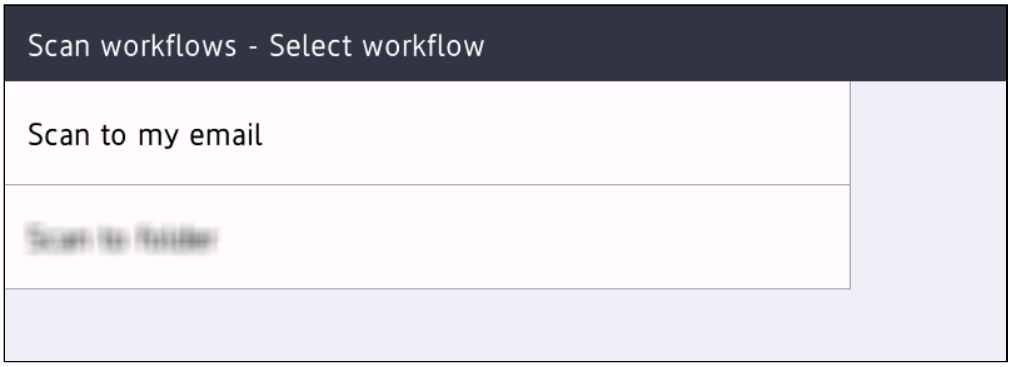


3. In the Solutions menu, tap **Dispatcher Scan**.

4. This will take you to the **Scan workflows** application.

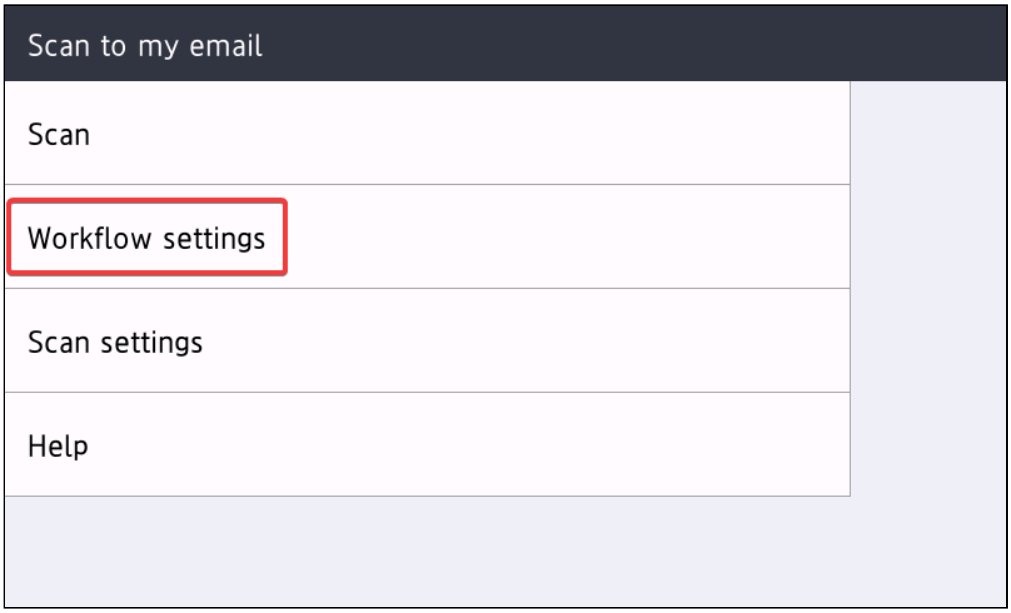
5. The **Scan workflows** application displays all scan workflows that your administrator made available to you.

6. Tap the scan workflow you wish to execute.

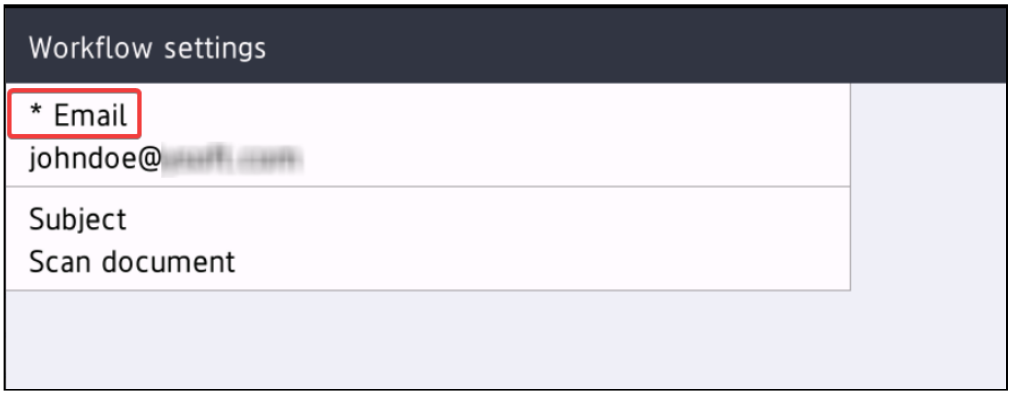


7. In the workflow detail screen, you can initialize the scan job or tap **Scan settings** to modify the settings.

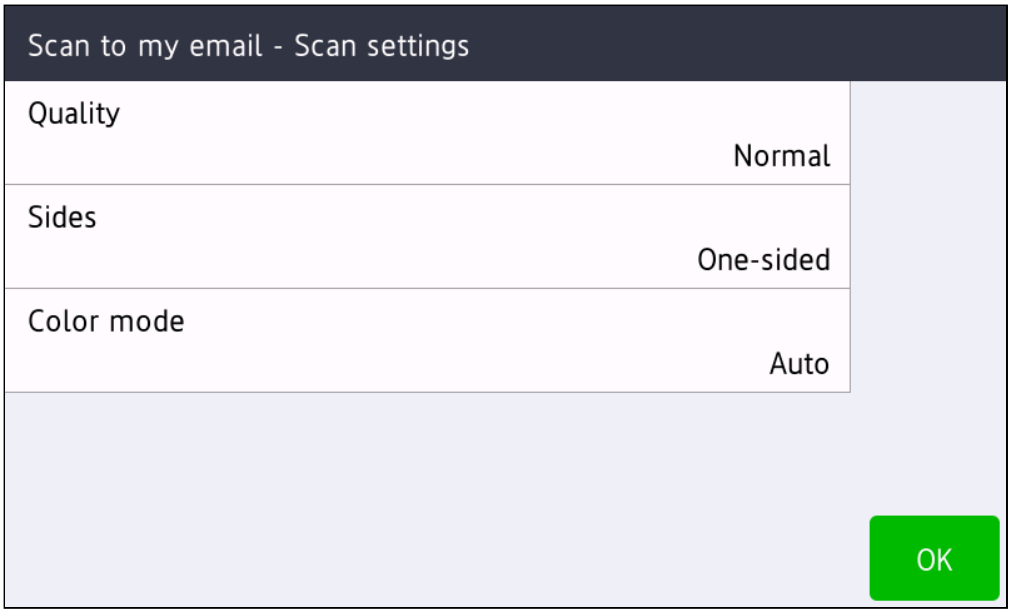
8. If the workflow has optional or mandatory user input, **Workflow settings** option will be present.



a. If there are mandatory user inputs, they will be marked with an asterisk.



9. In the **Scan settings** screen, make your changes, tap **OK** and then tap **Scan**.



By default, all scanned documents are scanned in A4 format with portrait orientation.

The device's merging originals feature is always enabled and will allow you to join more documents into a single workflow.

Dispatcher Paragon Embedded Terminal for Epson

Registering your card

See Card registration at the MFD terminal.

Logging in and out

Logging in

1. Place your card on the card reader attached to the printer or enter your PIN and tap **Login**. The authentication method depends on how your administrator configured the terminal.

2. You will see the Dispatcher Paragon embedded terminal home screen. The content of the home screen depends on how your administrator configured the terminal. It may contain shortcuts, **My print jobs** application, or other applications.

Selecting language

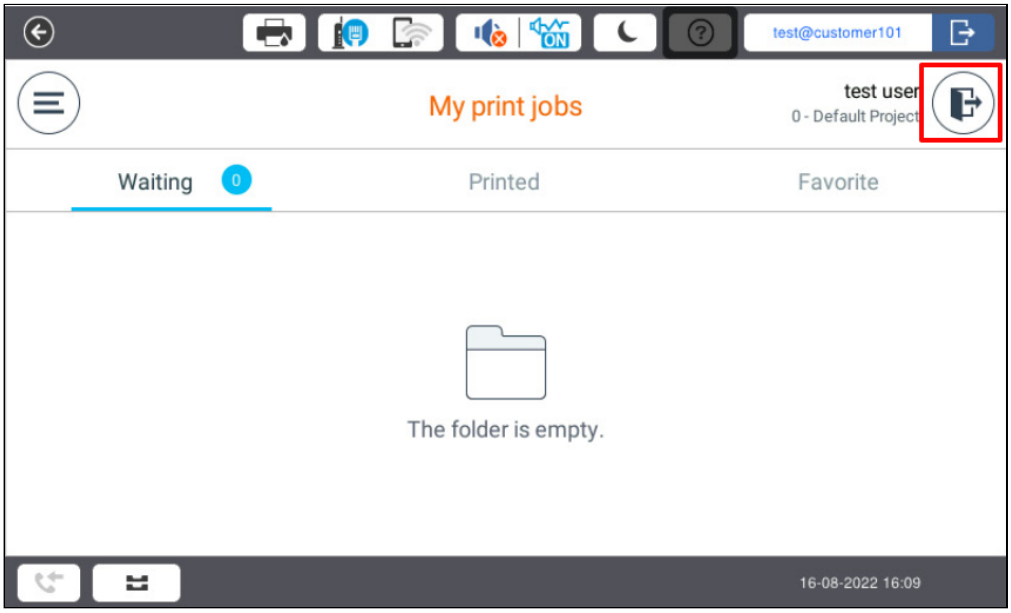
1. At the login screen, tap the language icon to display the *Select language* dialog.

2. Select the language and tap **Select**.

Logging out

You can use two methods to log out:

1. Tap the Logout icon on the home screen of Dispatcher Paragon embedded terminal.



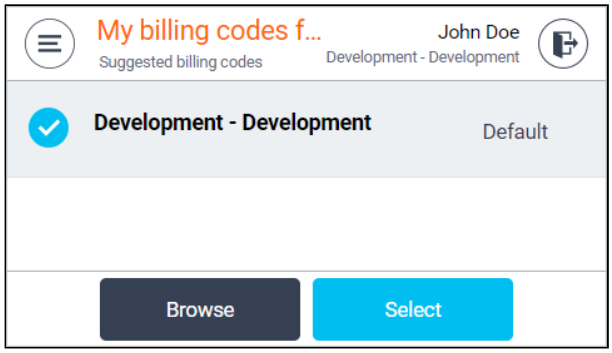
2. Place your card on the card reader attached to the printer.

Using billing codes

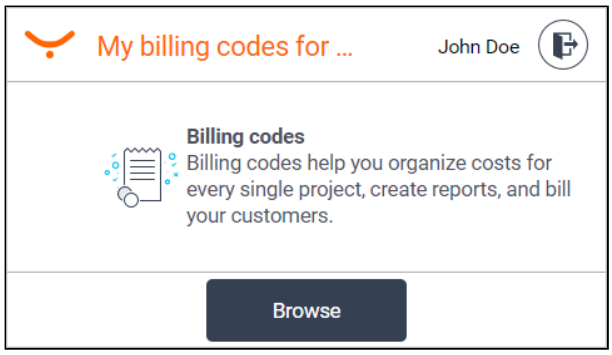
1. If your administrator enabled Billing codes selection at the terminal, you will see the **Billing codes** application after logging in at the terminal.

2. If you have a default billing code assigned, it will be automatically selected (highlighted) for you at the home screen of the Billing codes application. Tap the **Select** button to confirm the

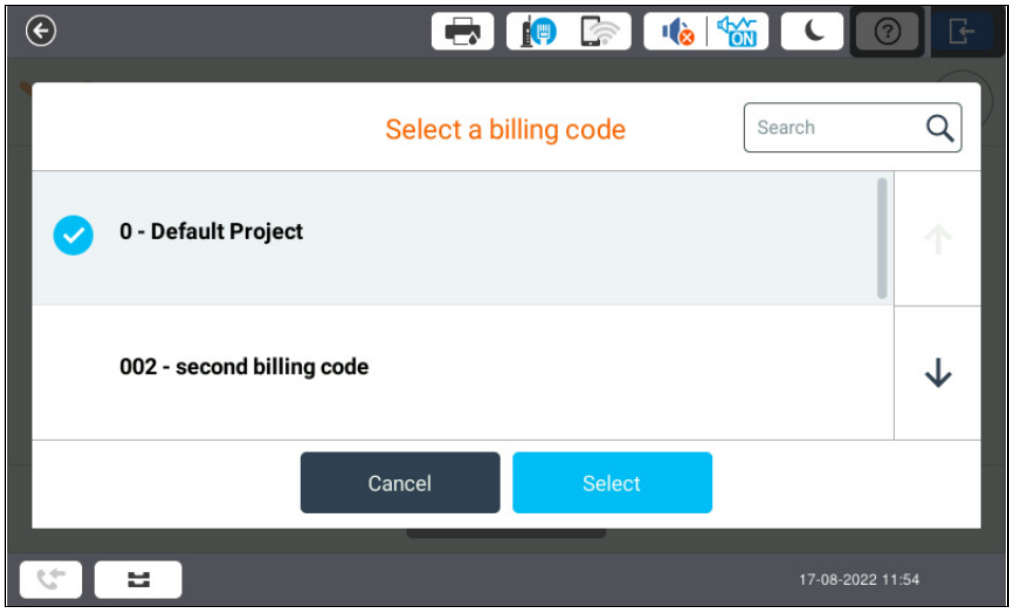
choice. If you don't want to use the default code, tap **Browse**.



3. If you don't have any default billing code, you will see the following screen. Tap **Browse** to select the code you wish to use for your session.



4. Tap the code you wish to use and then tap the **Select** button. For a more advanced search, see the Searching for billing codes section.



5. This concludes the authentication process. You will then see the home screen.

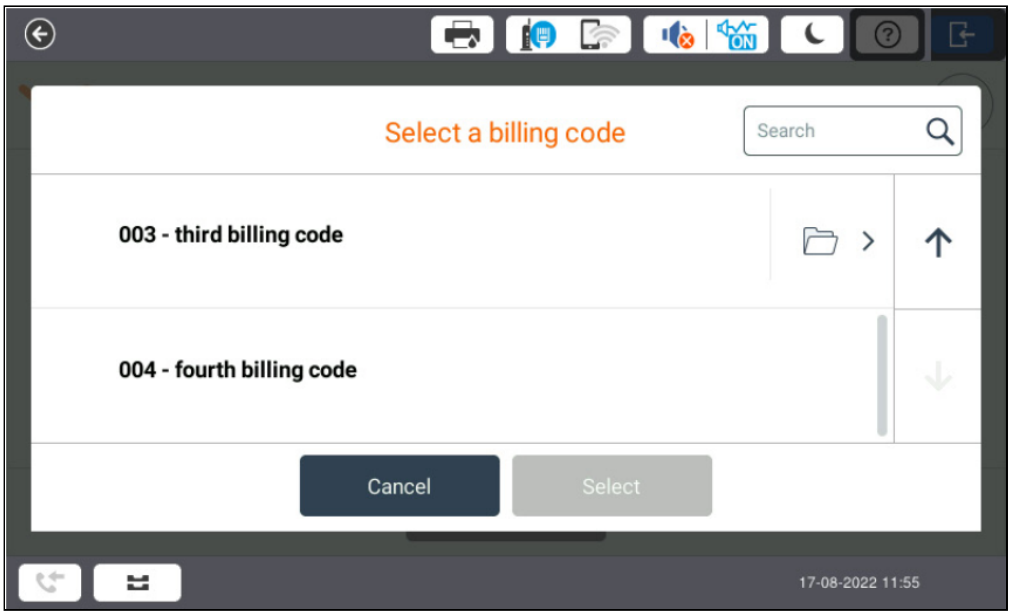
Be aware that:

- You cannot proceed with authentication unless you select a billing code.
- If you have more than one code assigned to you and you want to change the default one, you cannot do so at the terminal. The change can only be made in the Dispatcher Paragon Cloud management interface by your administrator.
- Whether the selected billing code applies to your print jobs or not, depends also on the billing codes configuration performed by your administrator.

Searching for billing codes

Browsing

1. After opening the browsing screen, you will see the root of the billing codes tree structure.
2. The billing codes which have sub-level codes have a folder icon next to them. Tap the folder icon to see the sub-level codes.



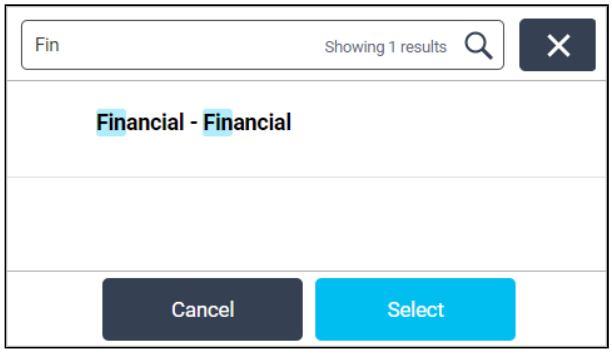
3. To go one level up in the tree structure, tap the return icon
4. When you select a billing code by tapping it, the **Select** button is enabled. Tap the button to select the code for your session.

Searching

If you cannot find the desired billing code via browsing, you can use searching via the search box on the browsing screen.

1. Tap inside the search field.
2. Enter the name or description you are searching for. The Billing codes application searches in both of these fields.
3. Tap the magnifying glass icon.

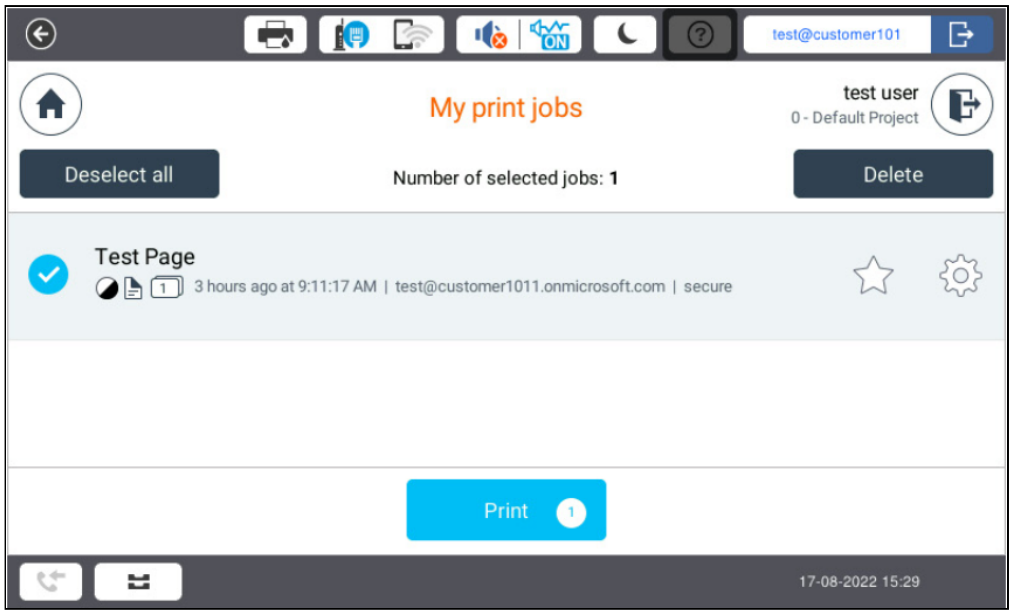
4. If you want to cancel your search and return to the browsing screen, tap the cross icon.



5. If your search returns any results, you will see a billing codes list.
6. When you select a billing code by tapping it, the **Select** button is enabled. Tap it to select the code for your session.
7. If you don't wish to select any billing codes from the list, tap **Cancel** in order to return to the Billing codes application home screen.

Printing and managing jobs

1. Log in to the Dispatcher Paragon embedded terminal.
2. You will see either the **My print jobs** application, or **My quick actions** application. If the latter is the case, tap **My print jobs**.
3. Select the print job(s) that you wish to print.

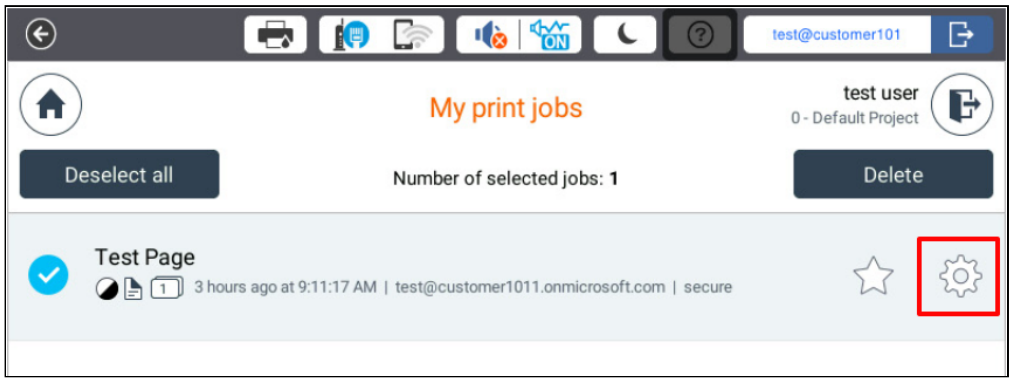


4. If needed, modify the finishing options.
5. Tap **Print**.

Finishing options

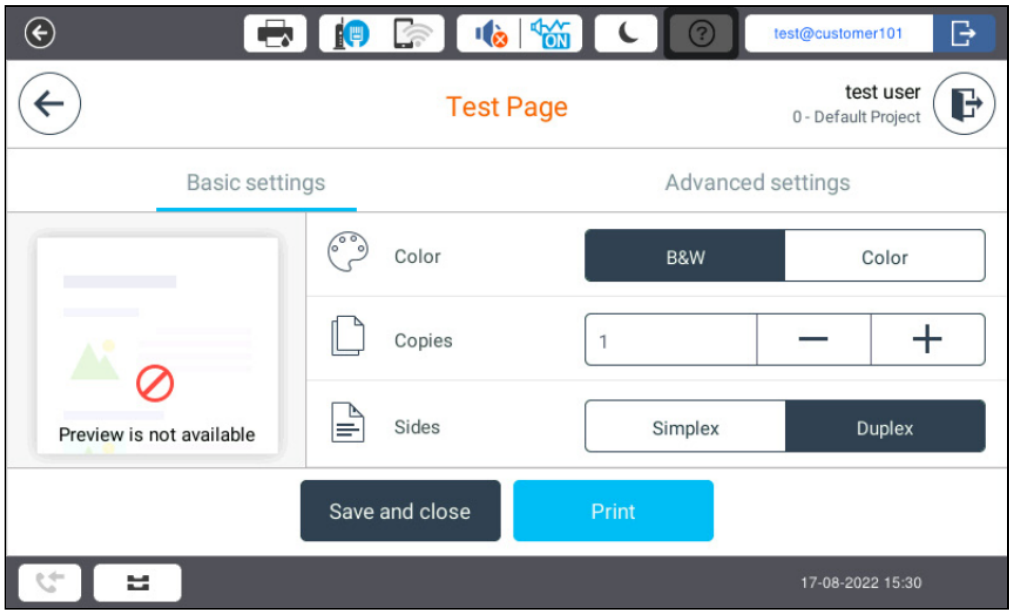
If your administrator has enabled this feature, you can modify the finishing options before printing your job.

1. To change basic finishing options (color, copies, sides) or the advanced options (stapling, punching, binding, folding), tap the settings icon.



2. You will see the job detail screen.

3. Adjust the basic finishing options as needed. Tap **Advanced settings** to adjust the advanced finishing options.



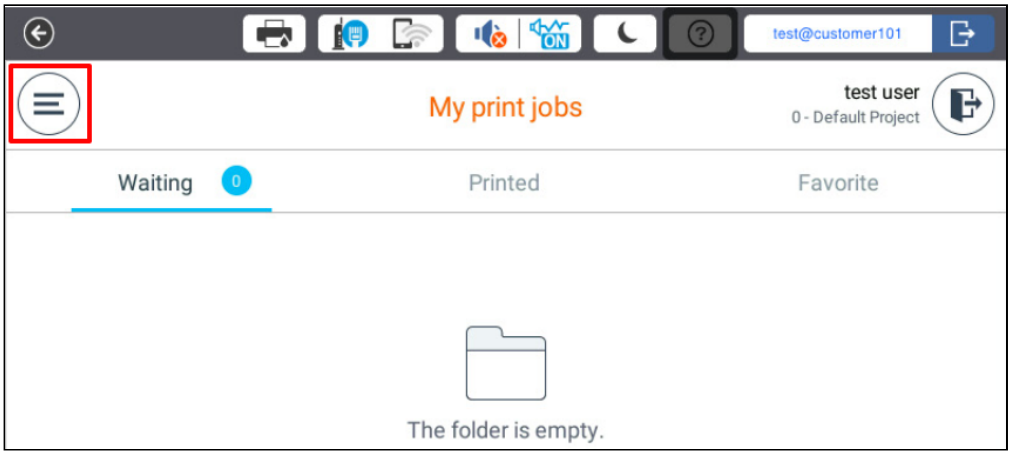
4. Tap **Print** if you wish to print the job immediately or **Save and close** if you wish to return to **My print jobs** screen.

Copying

1. Log in to the Dispatcher Paragon embedded terminal.

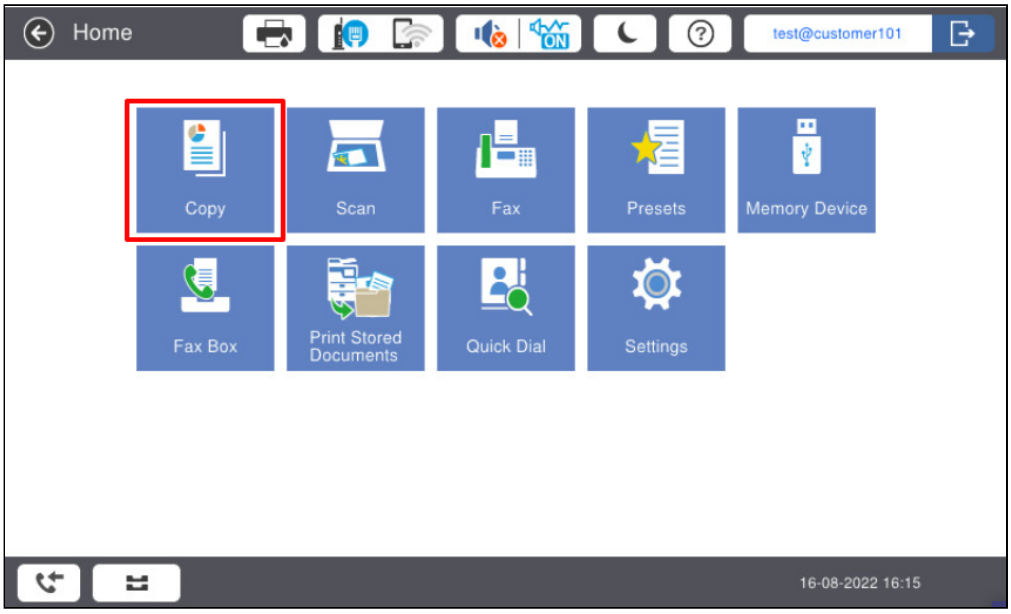
2. If the home screen of the terminal is the **My quick actions** application, tap **Copy**. This action will take you to the native copy application.

3. If the home screen of the terminal is **My print jobs** application, tap the menu button.



4. Select **Dashboard**.

5. On the dashboard, tap **Copy**.

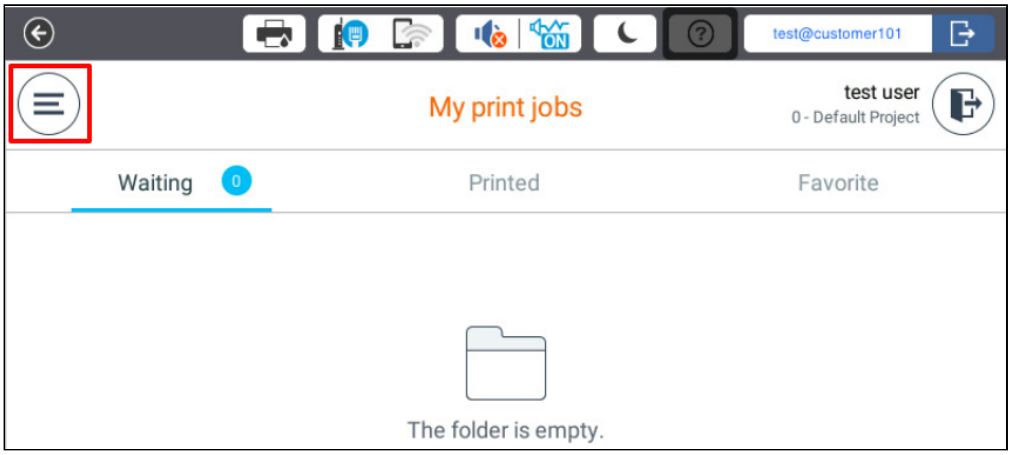


6. This action will take you to the native copy application.

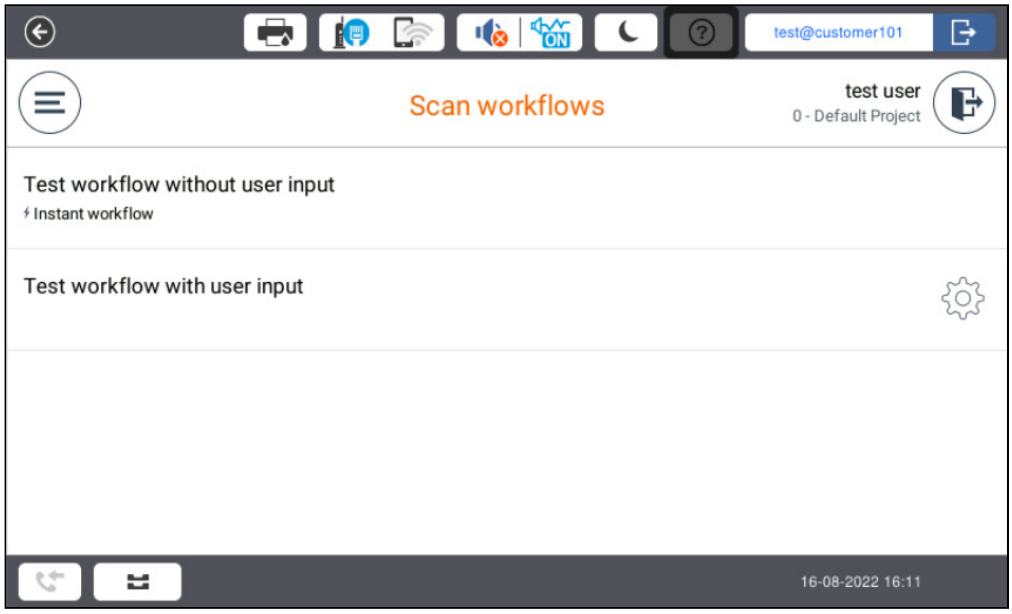
7. Select the number of copies by entering the number on the keypad.
8. Adjust the copy settings as needed by tapping the available options.
9. Tap **Copy**.

Scanning

1. Log in to the Dispatcher Paragon embedded terminal.
2. If the home screen of the terminal is the **My quick actions** application, tap **My scan workflows**. This will take you to the **Scan workflows** application
3. If the home screen of the terminal is **My print jobs** application, tap the menu button.



4. Select **Scan**. This will take you to the **Scan workflows** application.

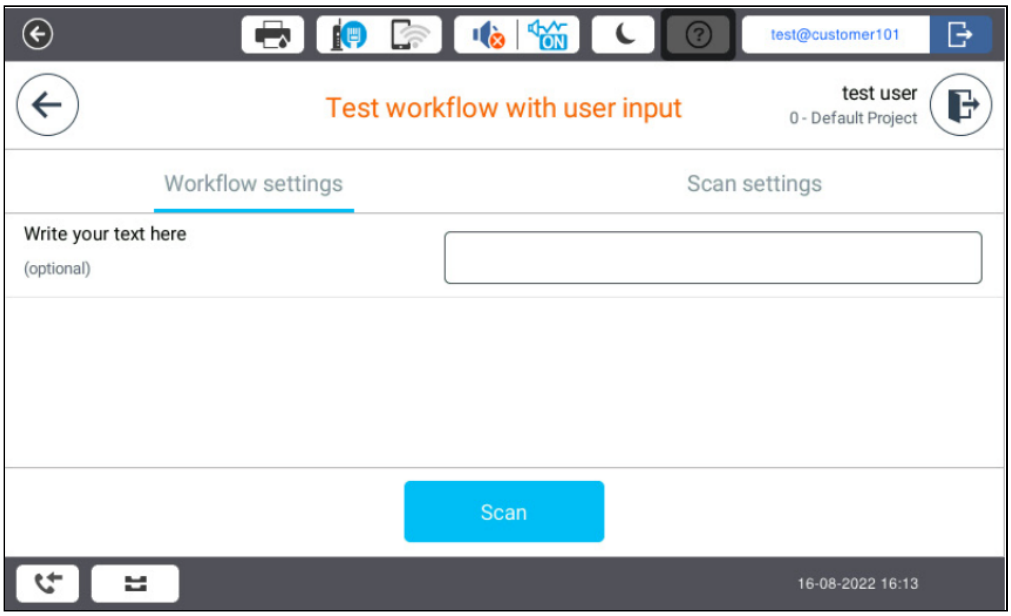


5. The Scan workflows application displays all scan workflows that your administrator made available to you.

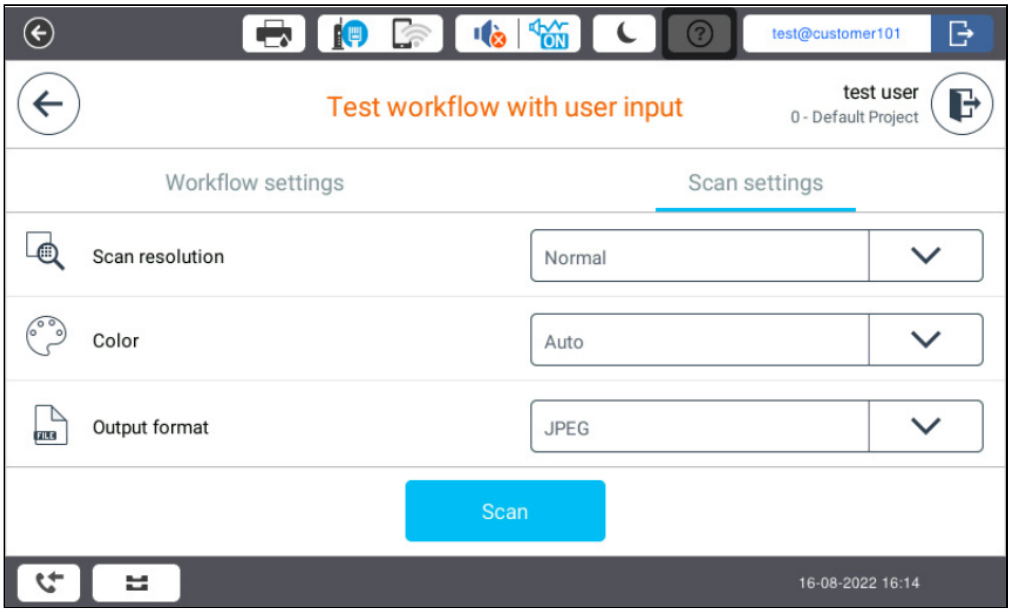
6. Tap the workflow you wish to execute.

   a. If a workflow is marked as **Instant workflow**, it will execute immediately, without any input from you.

   b. If a workflow is not marked as Instant workflow, it means that it has either mandatory user input or optional user input. Example:



   c. You can also tap the **Scan settings** tab to modify the scan job properties. This screen contains all the properties that your administrator allowed to be modified for this workflow.



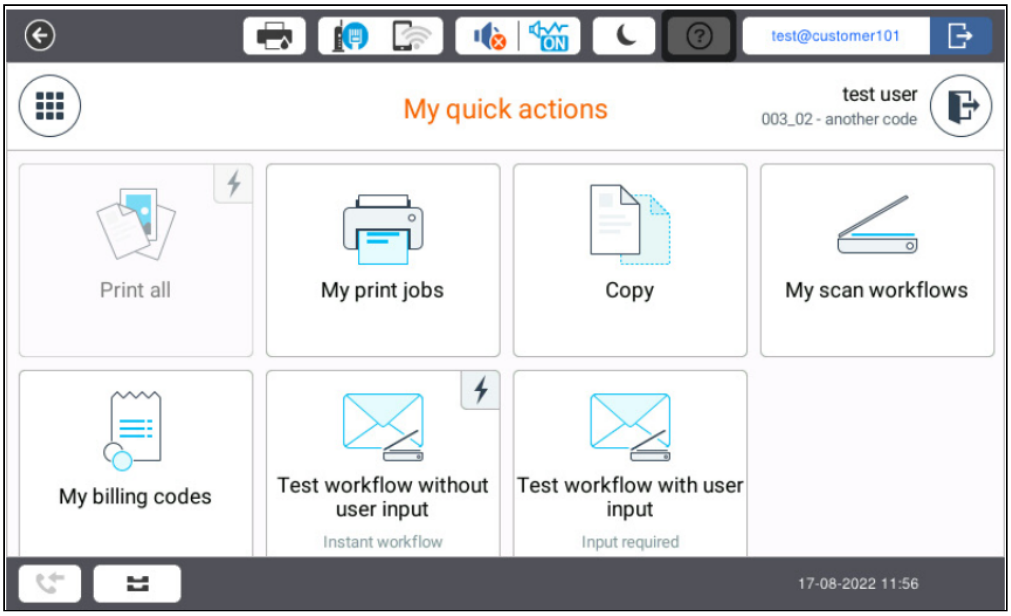
If the **Scan settings** tab is not visible, it means that the scan settings are not configurable by end users.

d. Tap **Scan**.

If **My quick actions** application is installed on your MFD, you can access scan workflows from there as well.

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. Whether this application is installed on the MFD and functions as the home screen of the terminal depends on the configuration done by your administrator.



Dispatcher Paragon Embedded Terminal for Fujifilm BI

Registering your card

See Card registration at the MFD terminal

Logging in and out

Logging in

1. Place your card on the card reader attached to the printer or enter your PIN and tap **Login**. The authentication method depends on how your administrator configured the terminal.
2. You will see the Dispatcher Paragon embedded terminal home screen. The content of the home screen depends on how your administrator configured the terminal. It may contain shortcuts, **My print jobs** application, or other applications.

⚠ If another user is logged in, you will log them out by placing your card on the card reader. If you want to log in, you must place your card on the card reader once again.

Selecting language

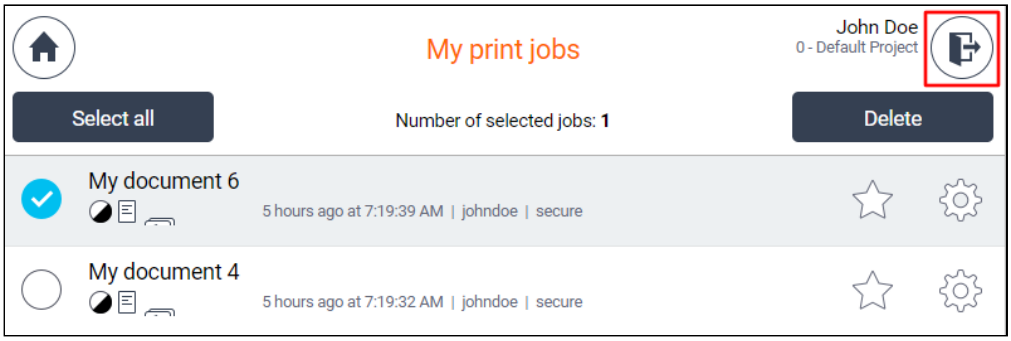
1. At the login screen, tap the language iconto display the *Select language* dialog.

2. Select the language and tap **OK**.

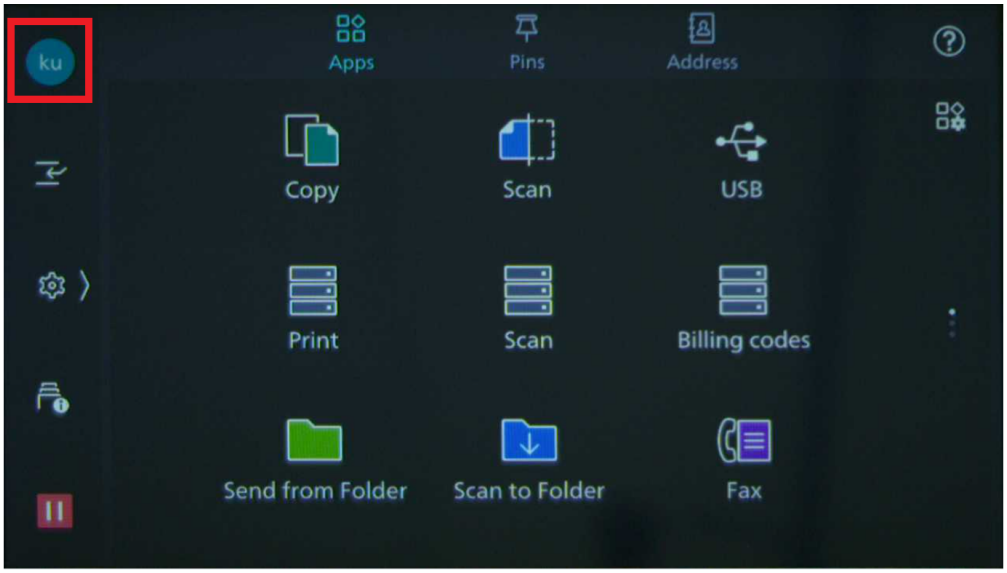
Logging out

1. Place your card on the card reader attached to the printer.

2. If you are inside one of the Dispatcher Paragon applications, such as **My print jobs**, tap the logout icon in the top right corner.



3. If you are in the main menu, tap the avatar with your username.

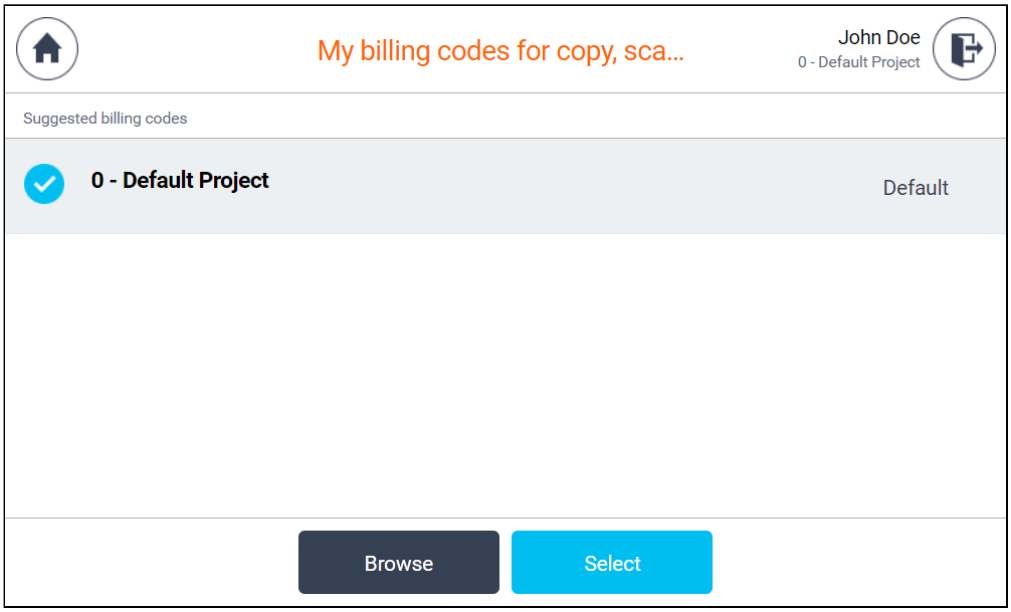


Using billing codes

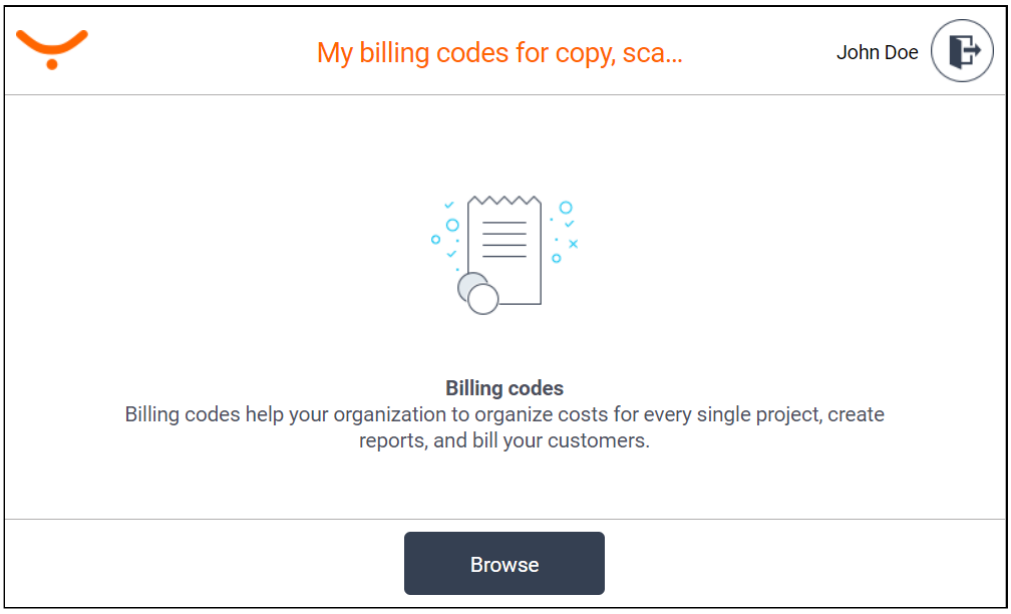
1. If your administrator enabled billing codes selection at the terminal, you will see the **Billing codes** application after logging in at the terminal.

2. If you have a default billing code assigned, it will be automatically selected (highlighted) for you at the home screen of the Billing codes application. Tap the **Select** button to confirm the

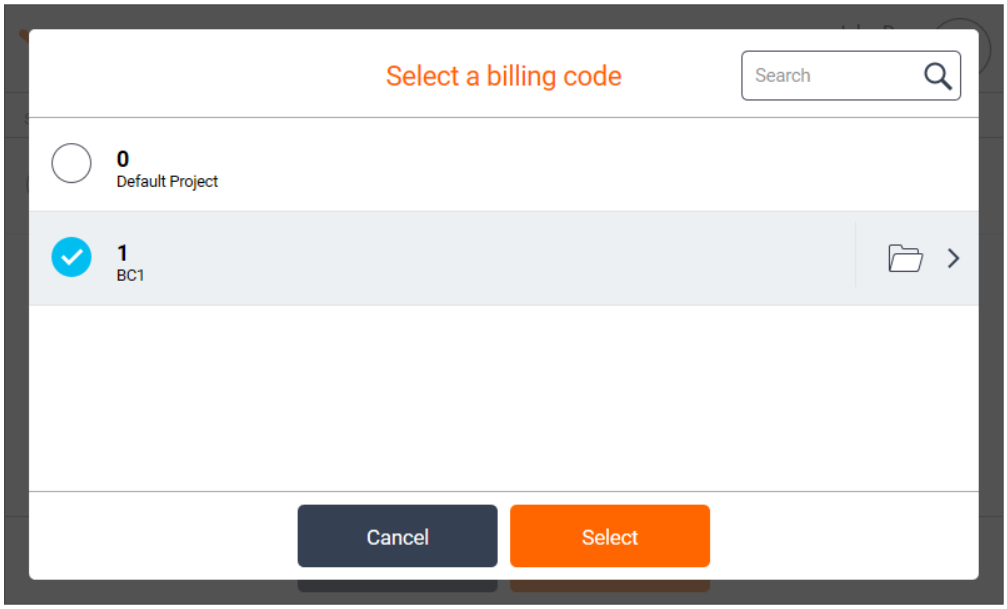
choice. If you don't want to use the default code, tap **Browse**.



3. If you don't have any default billing code, you will see the following screen. Tap **Browse** to select the code you wish to use for your session.



4. Tap the code you wish to use and then tap the **Select** button. For a more advanced search, see the Searching for billing codes section.



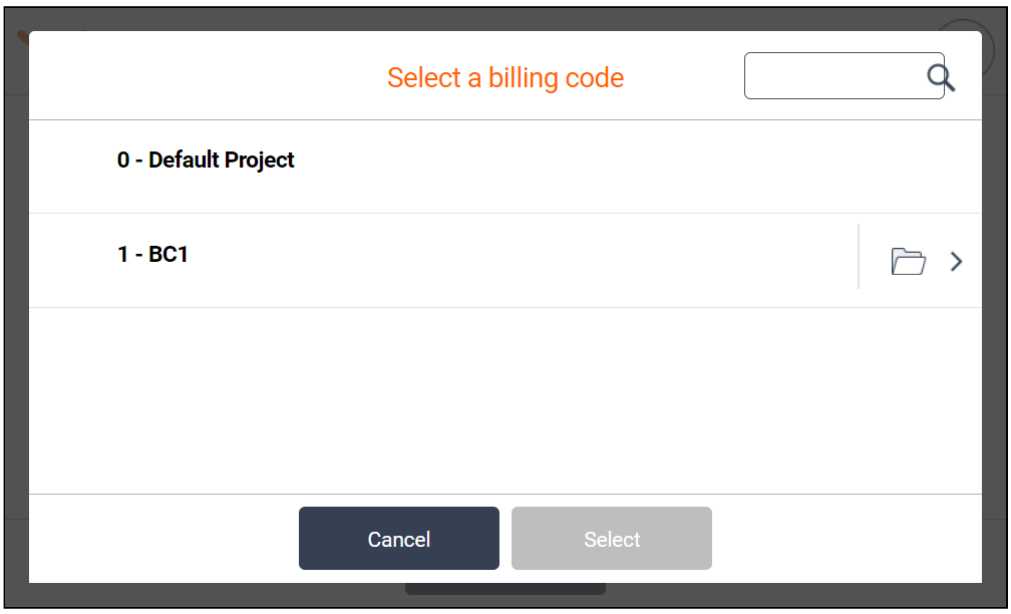
5. This concludes the authentication process. You will then see the home screen.

> ⚠ Be aware that:
>
> - You cannot proceed with authentication unless you select a billing code.
> - If you have more than one code assigned to you and you want to change the default one, you cannot do so at the terminal. The change can only be made in the Dispatcher Paragon Cloud management interface by your administrator.
> - Whether the selected billing code applies to your print jobs or not, depends also on the billing codes configuration performed by your administrator.

Searching for billing codes

Browsing

1. After opening the browsing screen, you will see the root of the billing codes tree structure.
2. The billing codes which have sub-level codes have a folder icon next to them. Tap the folder icon to see the sub-level codes.



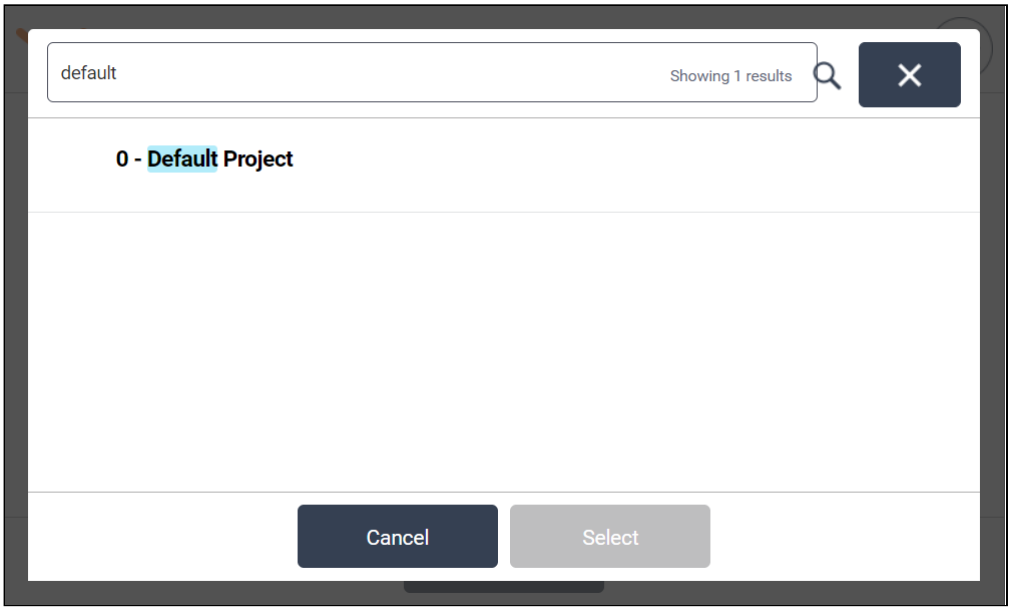
3. To go one level up in the tree structure, tap the return icon at the top of the screen.
4. When you select a billing code by tapping it, the **Select** button is enabled. Tap the button to select the code for your session.

Searching

If you cannot find the desired billing code via browsing, you can use searching via the search box on the browsing screen.

1. Tap inside the search field.
2. Enter the name or description you are searching for. The Billing codes application searches in both of these fields.
3. Tap the magnifying glass icon.

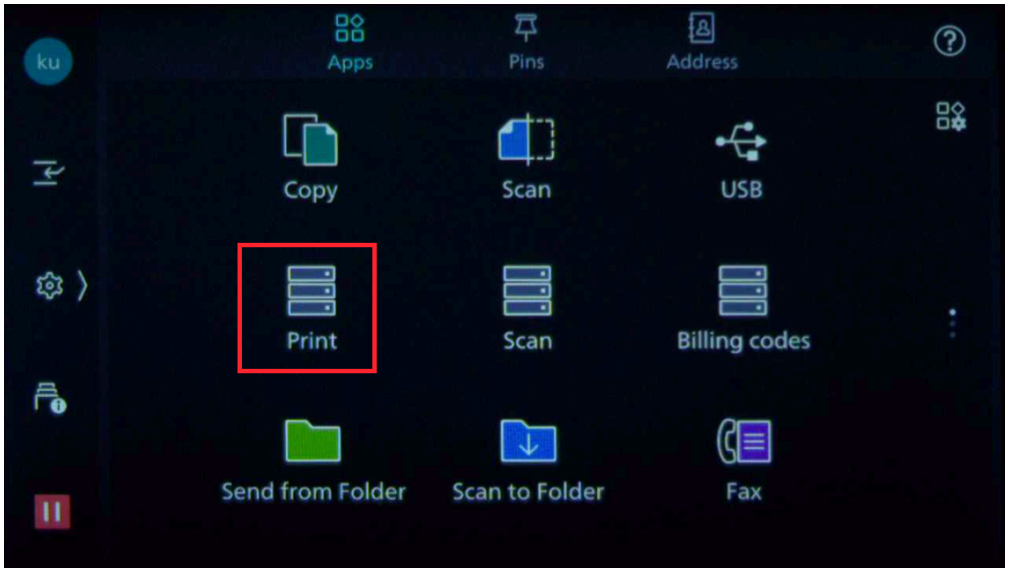
4. If you want to cancel your search and return to the browsing screen, tap the cross icon.



5. If your search returns some results, you will see a billing codes list.
6. When you select a billing code by tapping it, the **Select** button is enabled. Tap it to select the code for your session.
7. If you don't wish to select any billing codes from the list, tap **Cancel** in order to return to the Billing codes application home screen.

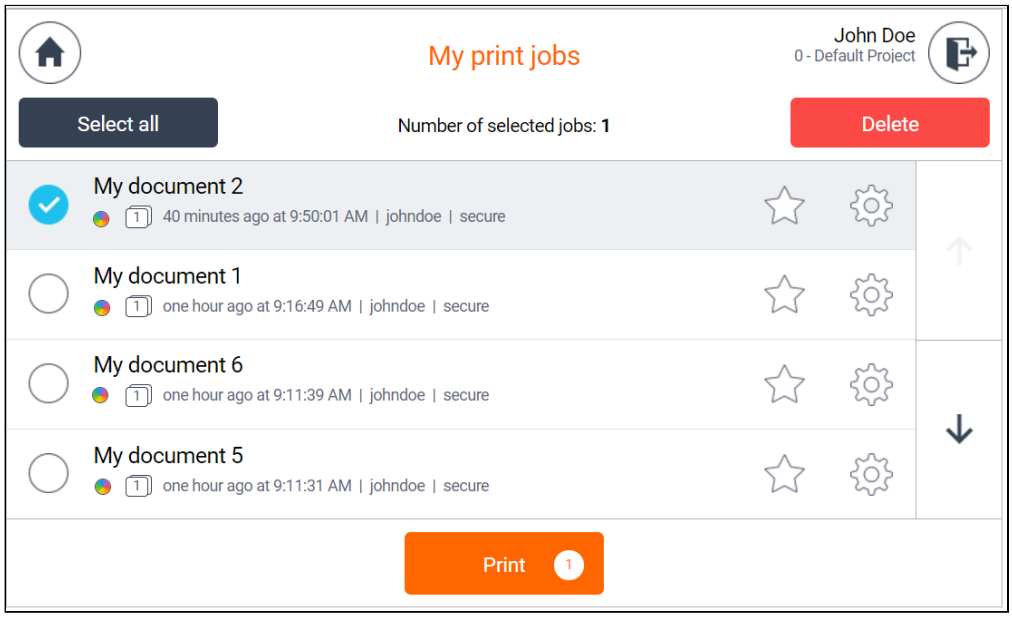
Printing and managing jobs

1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.
2. If the home screen is the main menu screen, tap **Print**.



3. If the home screen is one of the Dispatcher Paragon applications, tap the home icon to get to the main menu screen and then tap **Print**.

4. You will see the **My print jobs** application. Tap the print job you wish to print.



> If no job is selected, you can switch between the **Waiting**, **Printed**, and **Favorite** folders.

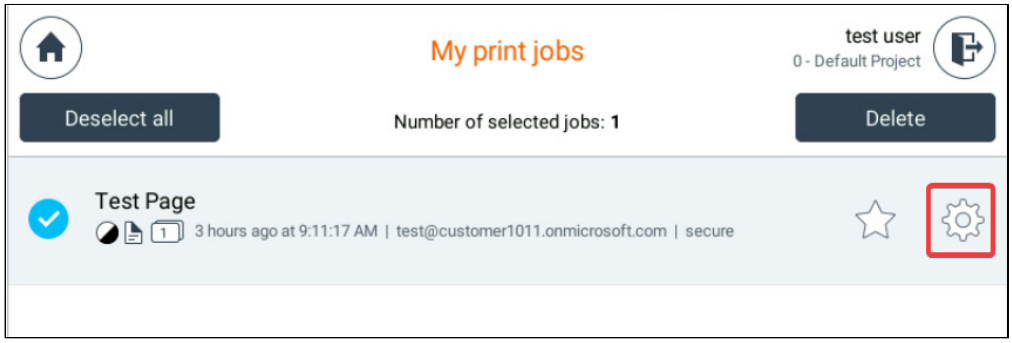
5. If needed, modify the finishing options.

6. Tap **Print**.

Finishing options

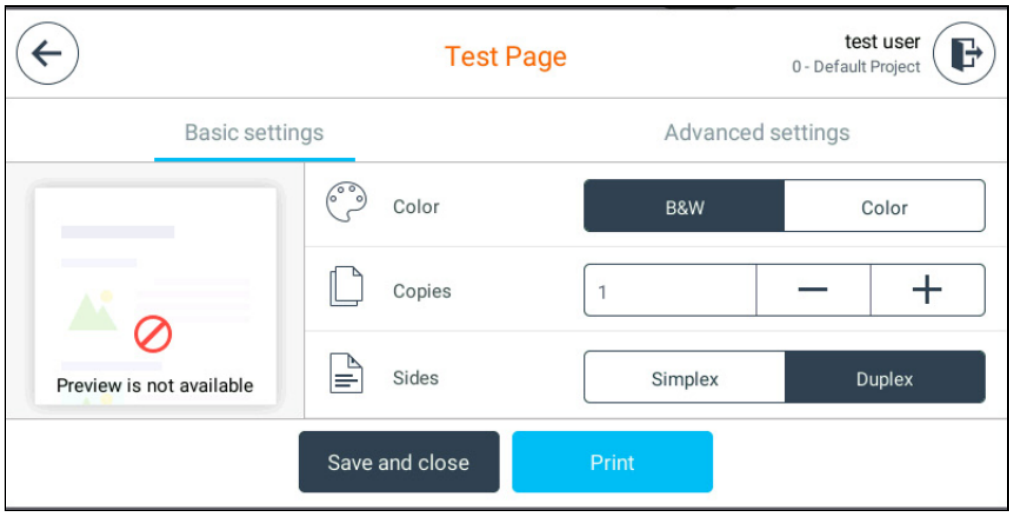
If your administrator has enabled this feature, you can modify the finishing options before printing your job.

1. To change basic finishing options (color, copies, sides) or the advanced options (stapling, punching, binding, folding), tap the settings icon.



2. You will see the job detail screen.

3. Adjust the basic finishing options as needed. Tap **Advanced settings** to adjust the advanced finishing options.

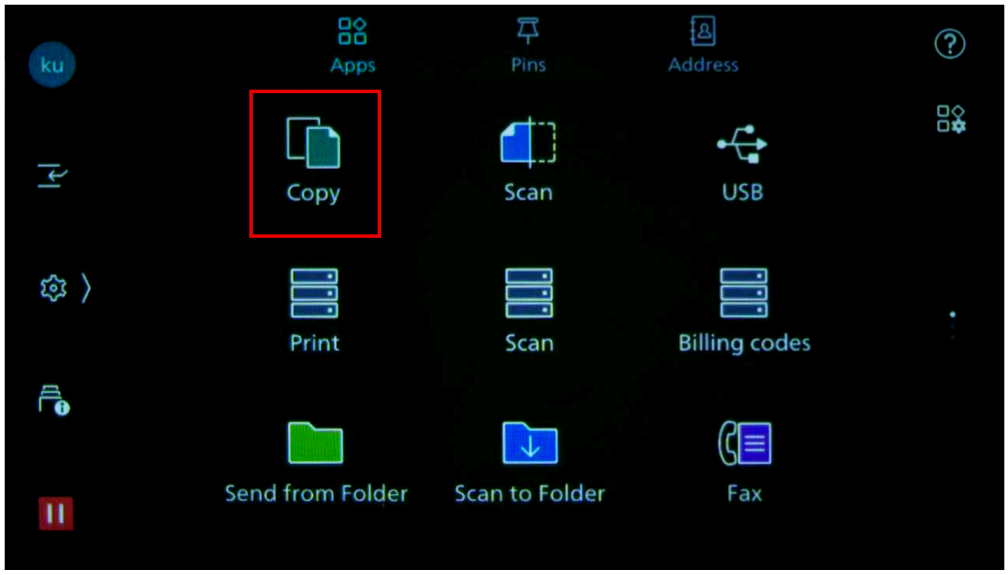


4. Tap **Print** if you wish to print the job immediately or **Save and close** if you wish to return to **My print jobs** screen.

Copying

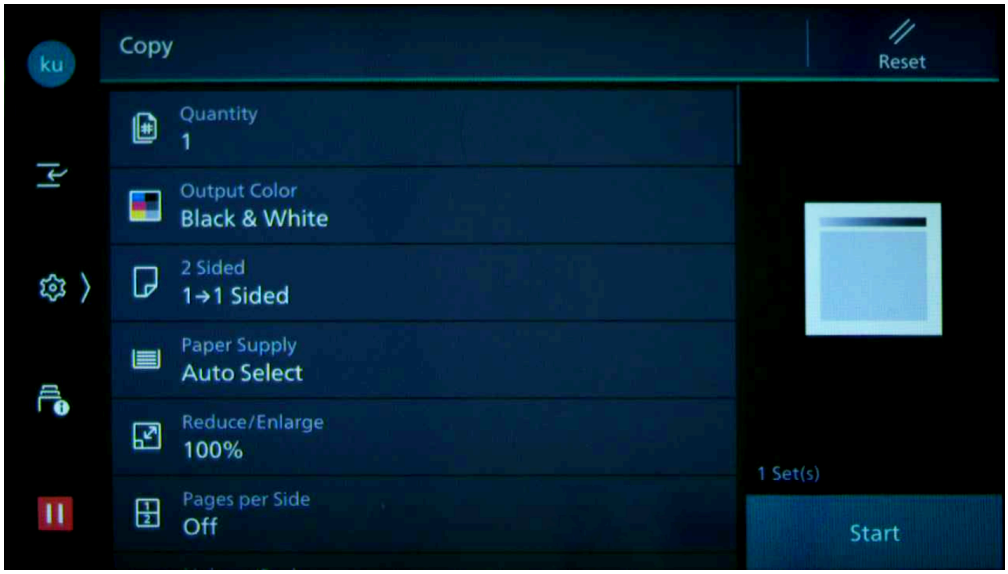
1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.

2. If the home screen is the main menu screen, tap **Copy**.



3. If the home screen is one of the Dispatcher Paragon applications, tap the home icon to get to the main menu screen and then tap **Copy**.

4. This action will take you to the native copy application. Adjust the available options (quantity, color, etc) as needed.



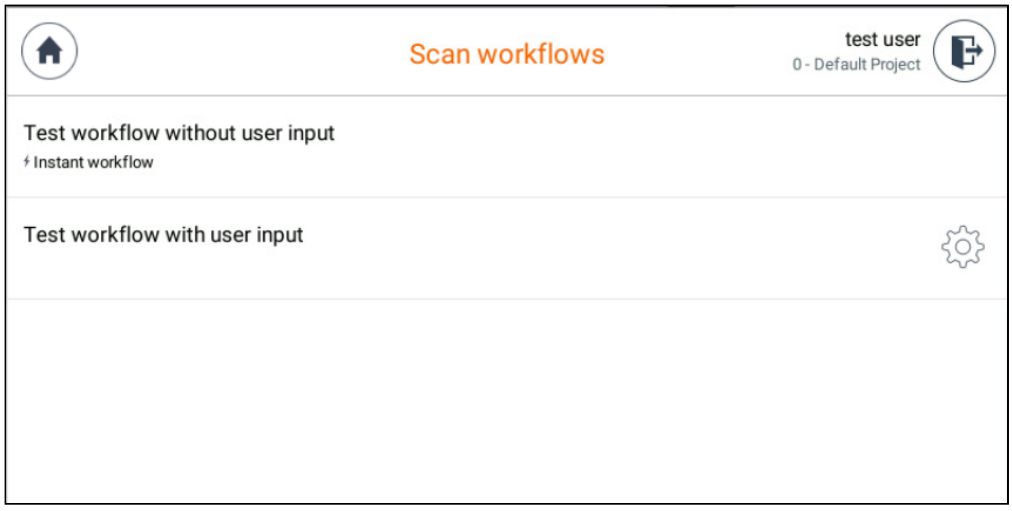
5. Tap **Start** to start copying.

Scanning

1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.

2. If the home screen is the main menu screen, tap **Scan**. If the home screen is one of the Dispatcher Paragon applications, tap the home icon ( ) to get to the main menu screen.

3. This will take you to the **Scan workflows** application.

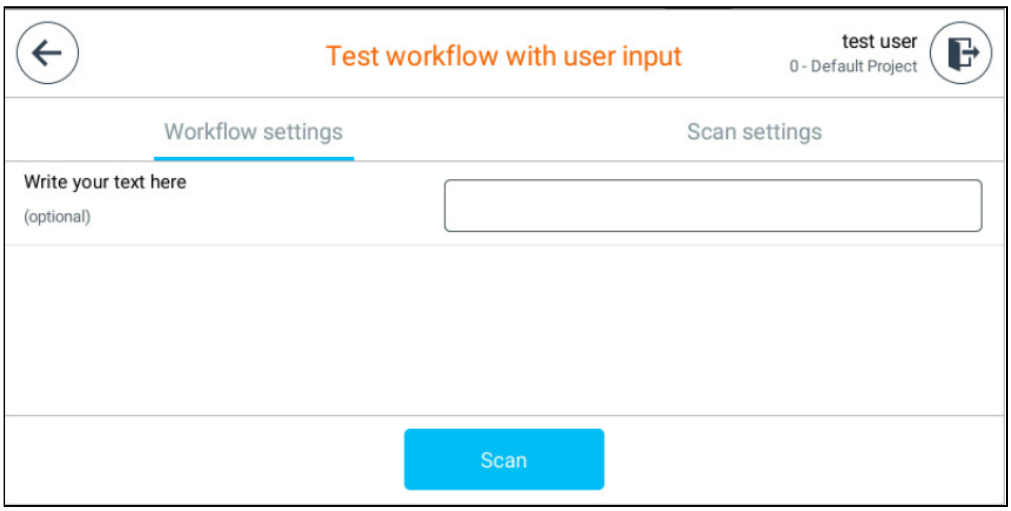


4. The Scan workflows application displays all scan workflows that your administrator made available to you.

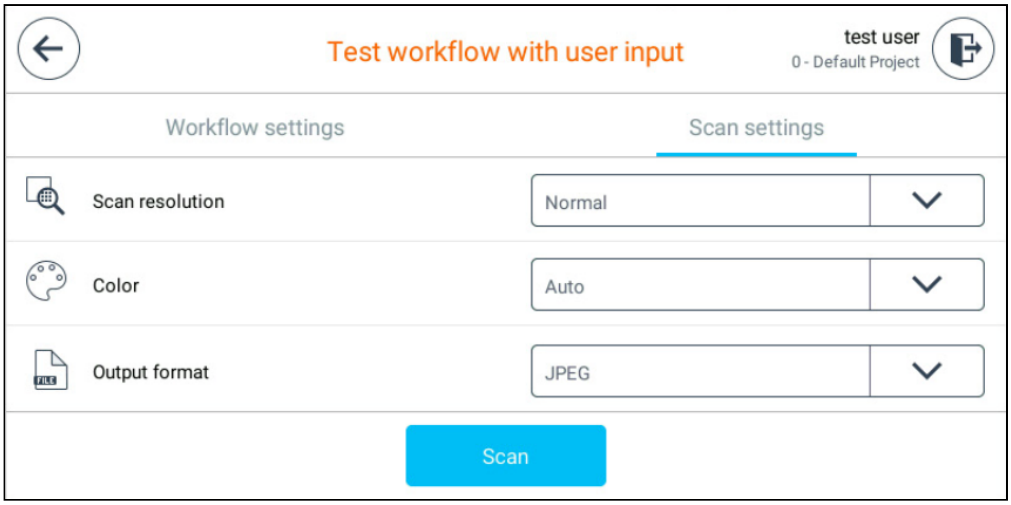
5. Tap the workflow you wish to execute.

   a. If a workflow is marked as **Instant workflow**, it will execute immediately, without any input from you.

   b. If a workflow is not marked as Instant workflow, it means that it has either mandatory user input or optional user input. Example:



c. You can also tap the **Scan settings** tab to modify the scan job properties. This screen contains all the properties that your administrator allowed to be modified for this workflow.



If the **Scan settings** tab is not visible, it means that the scan settings are not configurable by end users.

6. Tap **Scan**.

Dispatcher Paragon Embedded Terminal for Konica Minolta

Registering your card

See Card registration at the MFD terminal.

Logging in and out

Logging in

1. Place your card on the card reader attached to the printer or enter your PIN. The authentication method depends on how your administrator configured the terminal.
2. You will see the Dispatcher Paragon embedded terminal home screen. The content of the home screen depends on how your administrator configured the terminal. It may contain shortcuts, **My print jobs** application, or other applications.

> ⚠ If another user is logged in, you will log them out by placing your card on the card reader. If you want to log in, you must place your card on the card reader once again.

Selecting language

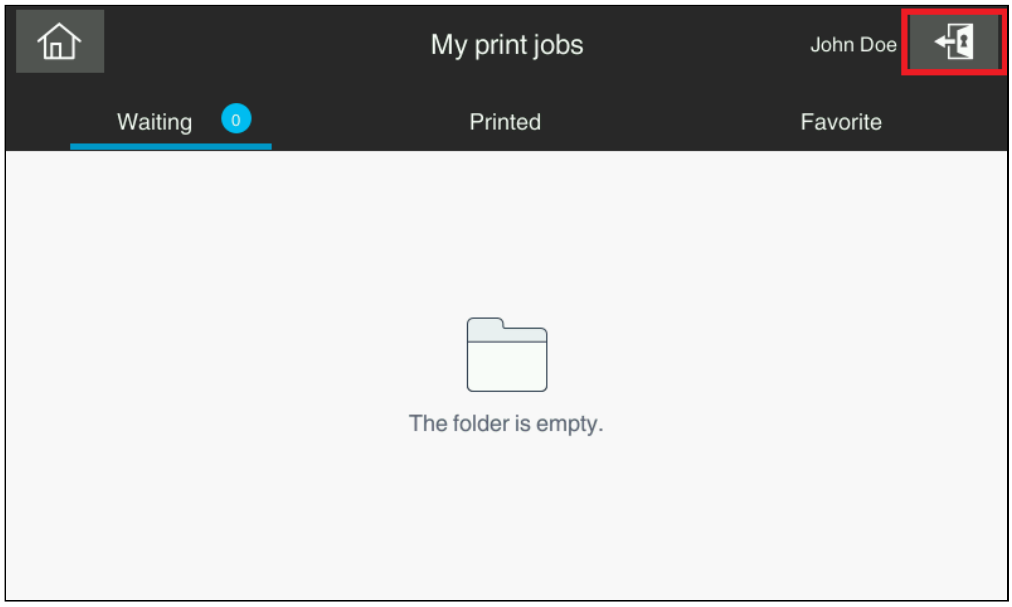
1. At the login screen, tap the language icon to display the *Select language* dialog.

2. Select the language and tap **Select**. For the list of supported languages, see the *Supported languages* section.

Logging out

You can use two methods to log out:

1. Tap the Log out icon on the home screen of Dispatcher Paragon embedded terminal.

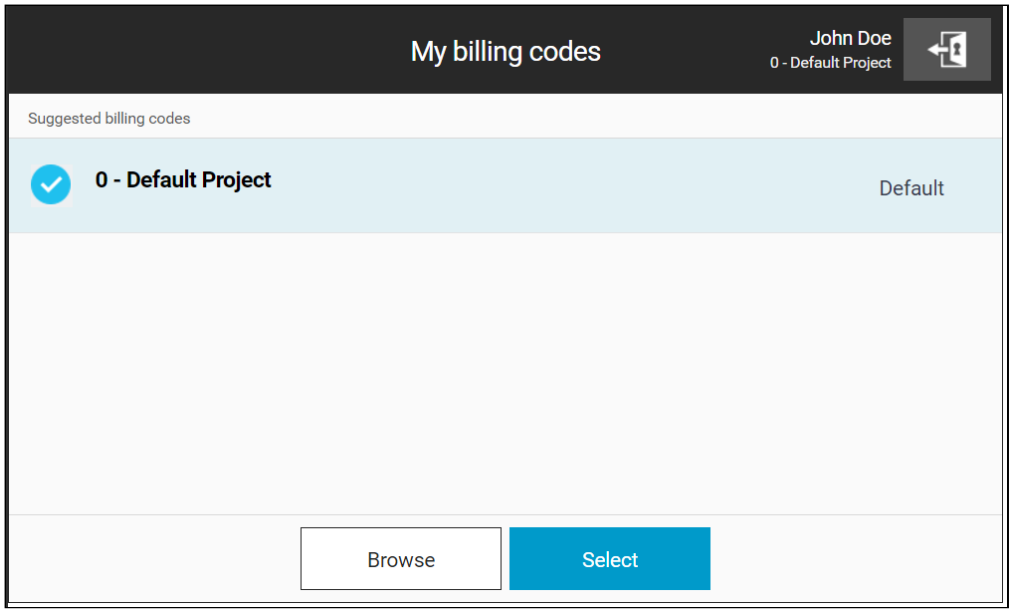


2. Place your card on the card reader attached to the printer.

Using billing codes

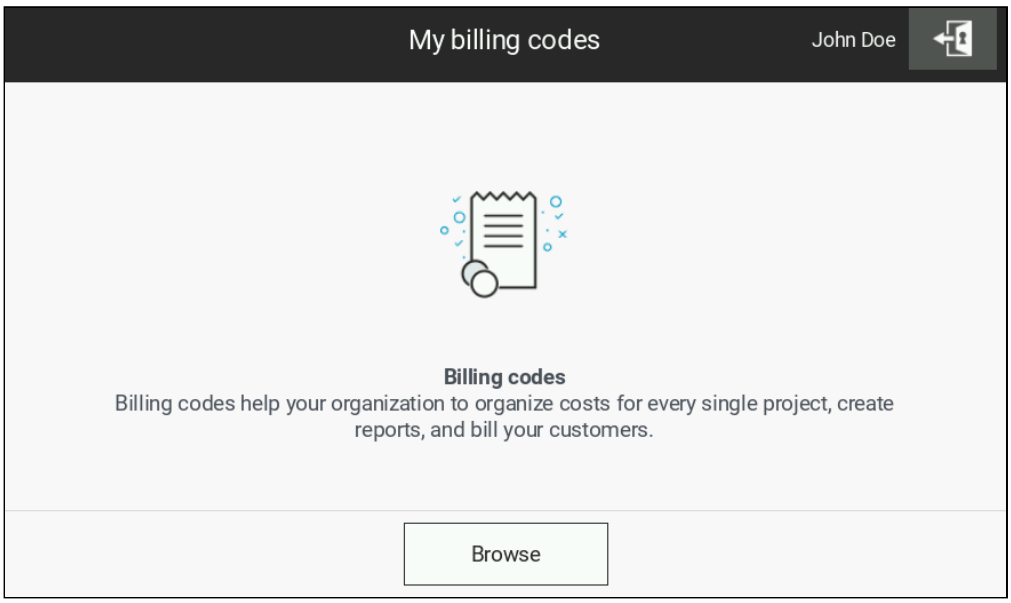
1. If your administrator enabled Billing codes selection at the terminal, you will see the Billing codes application after authentication at the terminal.

2. If you have a default billing code assigned, it will be automatically selected (highlighted) for you at the home screen of the Billing codes application. Tap the **Select** button to confirm the choice. If you don't want to use the default code, tap **Browse**.



> If you have more than one code assigned to you and you want to change the default one, you cannot do so at the terminal. The change can only be made in the Dispatcher Paragon Cloud management interface by your administrator.

3. If you have no default billing code, you will see the following screen. Tap **Browse** to select the code you wish to use for your session.



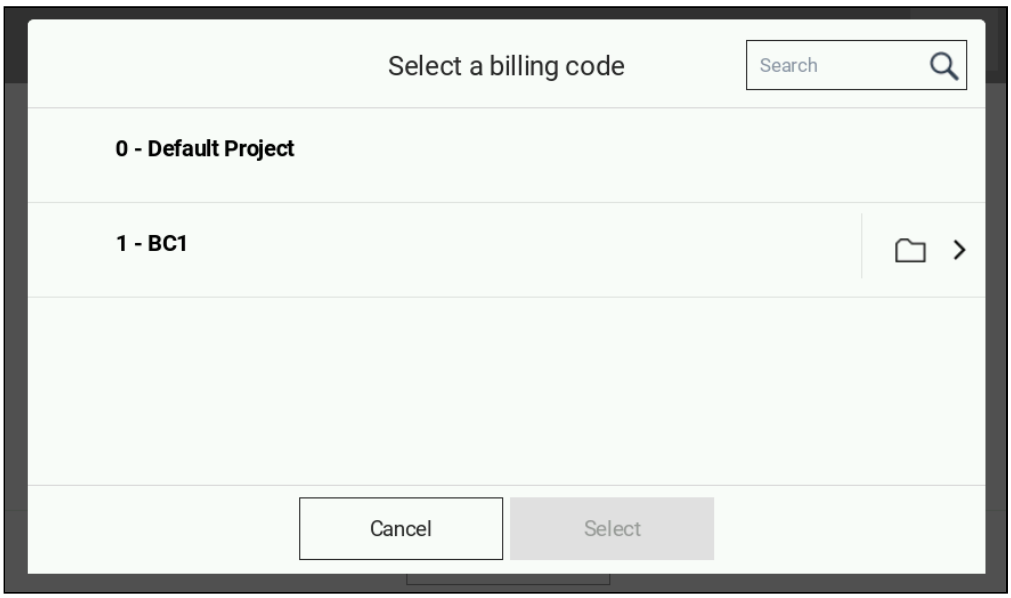
4. Tap your selected code and then tap the **Select** button. For a more advanced search, see the *Searching for billing codes* section.
5. This concludes the authentication process. You will then see the home screen.

> Be aware that:
>
> - You cannot proceed with authentication unless you select a billing code.
> - Once you select a billing code, you cannot change it during the same session.
> - Whether the selected billing code applies to your print jobs or not, depends also on the billing codes configuration performed by your administrator.

Searching for billing codes

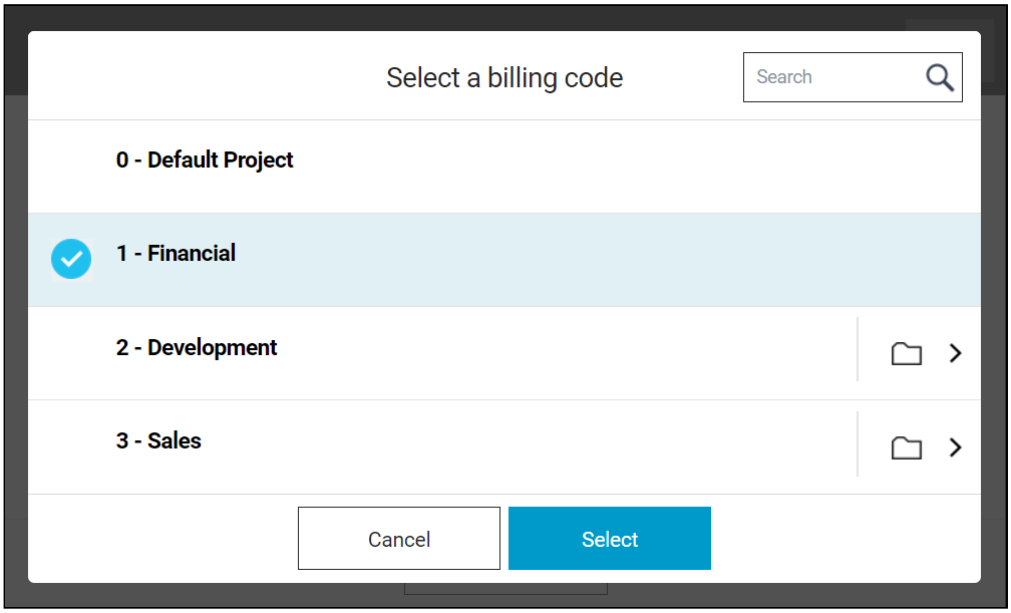
Browsing

1. After opening the browsing screen, you will see the root of the billing codes tree structure.



2. The billing codes which have sub-level codes have a folder icon next to them. Tap the folder icon to see the sub-level codes.
3. To go one level up in the tree structure, tap the return icon.

4. To go back to the root of the tree structure, tap the home icon at the top of the screen.
5. When you select a billing code by tapping it, the **Select** button is enabled. Tap it to select the code for your session.



Searching

If you cannot find the desired billing code via browsing, you can use searching via the search box on the browsing screen.

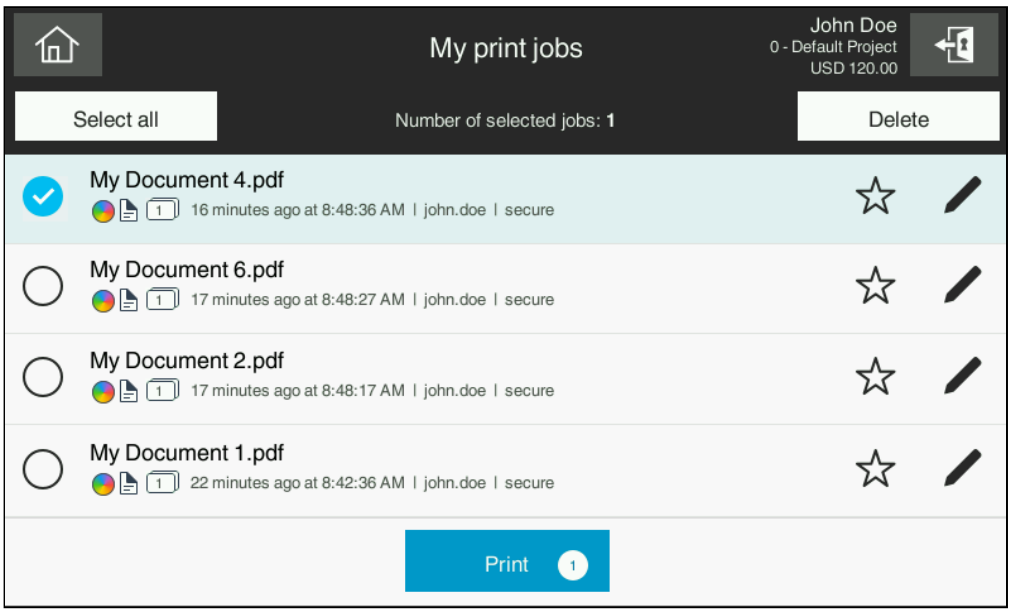
1. Tap inside the search field.
2. Enter the name or description you are searching for. The Billing codes application searches in both of these fields.
3. Tap the magnifying glass icon.
4. If you want to cancel your search and return to the browsing screen, tap the cross icon.
5. If your search returns any results, you will see a billing codes list.
6. When you select a billing code by tapping it, the **Select** button is enabled. Tap it to select the code for your session.
7. If you don't wish to select any billing codes from the list, tap **Cancel** in order to return to the Billing codes application home screen.

Printing and managing jobs

1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.
2. On the Home screen, tap **Dispatcher Print**.

   > You may be redirected automatically to the Dispatcher Print application. In that case, skip this step.

3. If the home screen is **My quick actions** application, tap **My print jobs**.
4. Tap the print job(s) you wish to print.



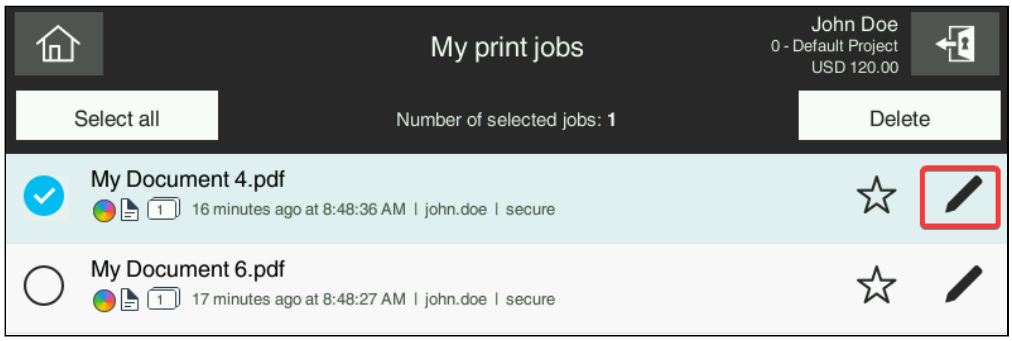
When there are no jobs in the folder, you will see the message "The folder is empty." instead of a job list.

5. If needed, modify the finishing options.
6. Tap **Print**.

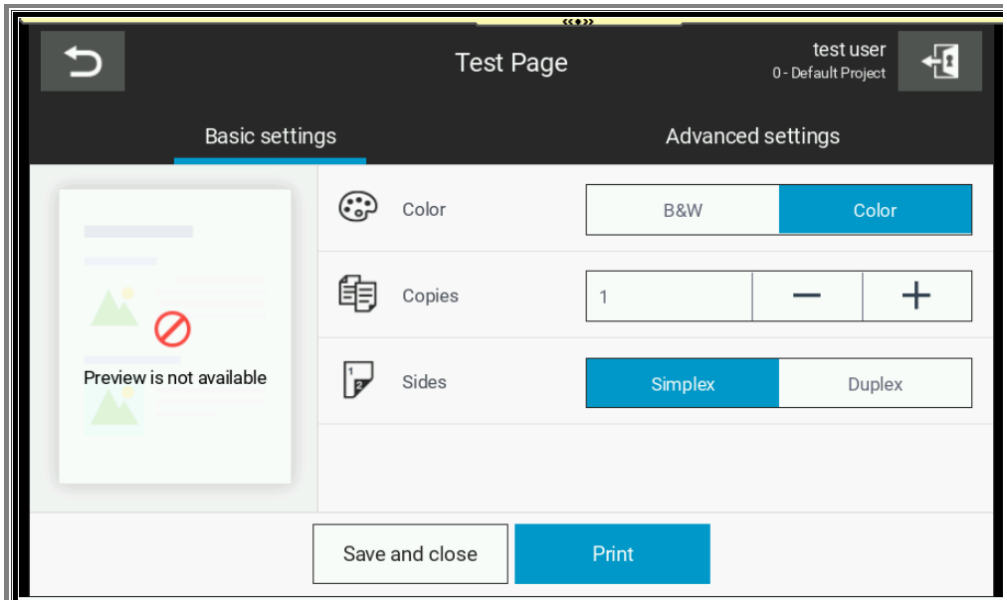
Finishing options

If your administrator has enabled this feature, you can modify the finishing options before printing your job.

1. To change basic finishing options (color, copies, sides) or the advanced options (stapling, punching, binding, folding), tap the edit icon.



2. You will see the job detail screen.



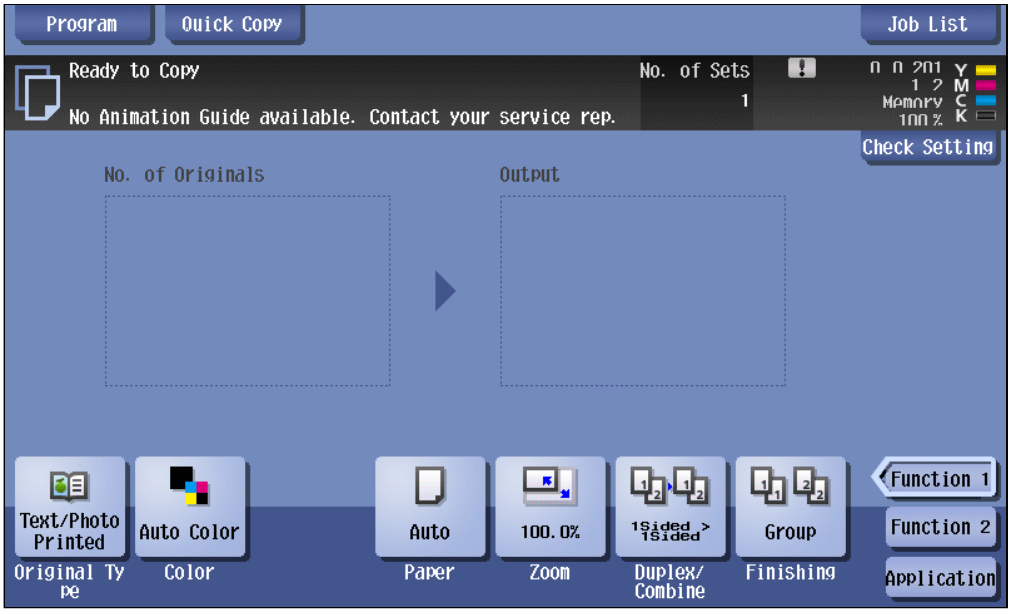
3. Adjust the basic finishing options as needed. Tap **Advanced settings** to adjust the advanced finishing options.

4. Tap **Print** if you wish to print the job immediately or **Save and close** if you wish to return to **My print jobs** screen.

Copying

1. Tap the **Copy** icon on the home screen of the terminal, or tap **Dispatcher Quick actions** > **Copy**.

2. Both of these actions will take you to the native copy application.



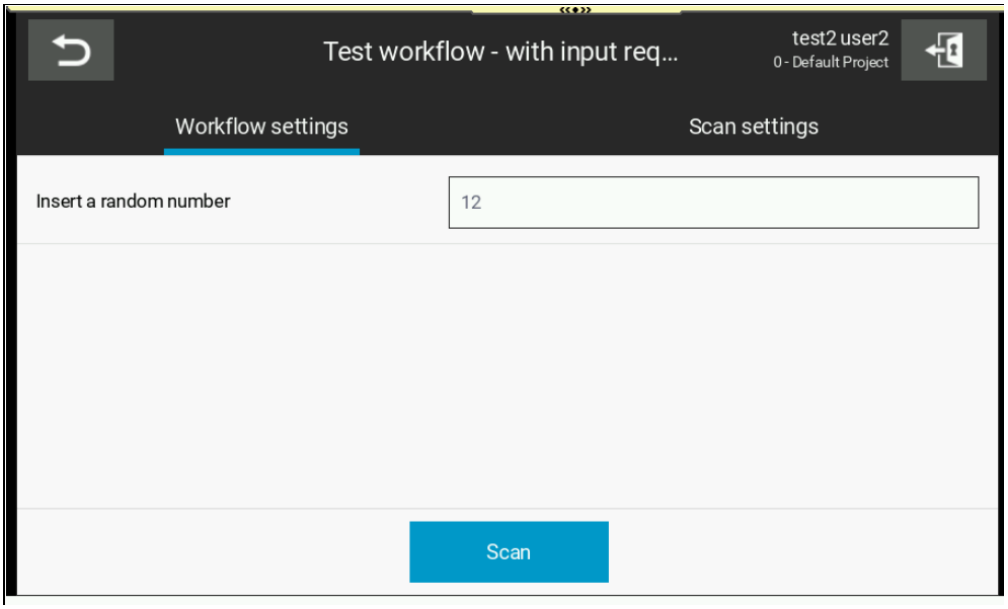
3. Select the copy settings by tapping the available options.

4. Press the **Start** button on the device panel to start copying.

Scanning

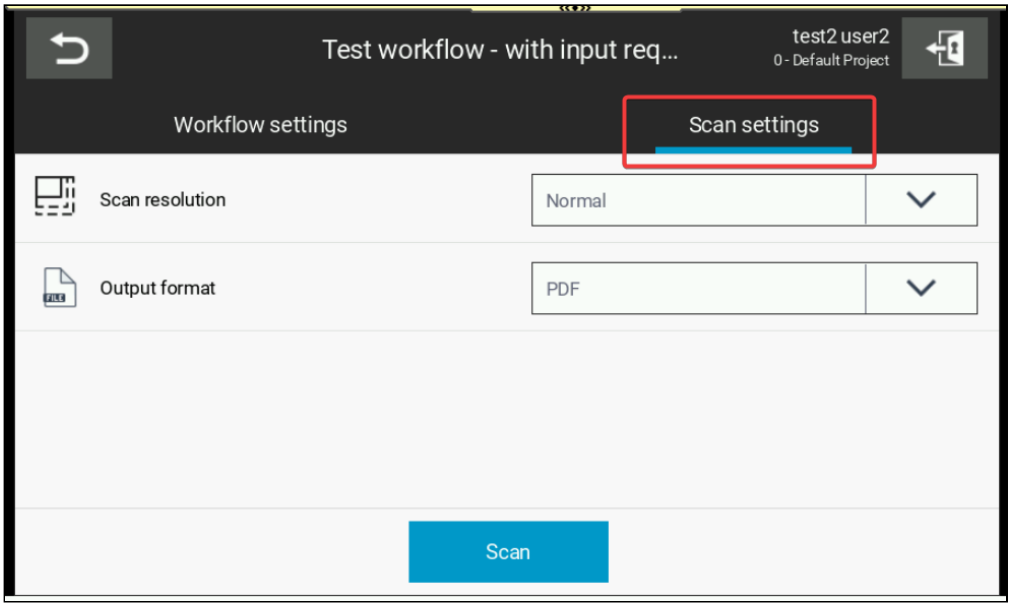
1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.
2. Tap **Dispatcher Scan**.
3. If the home screen is one of the Dispatcher Paragon applications, tap the home icon to go to the main menu and then tap **Dispatcher Scan**.

4. If the home screen is **My quick actions** applications, tap **My scan workflows**.
5. This will take you to the **Scan workflows** application.
6. The **Scan workflows** application displays all scan workflows that your administrator made available to you.
7. Tap the workflow you wish to execute.
   a. If a workflow is marked as **Instant workflow**, it will execute immediately, without any input from you.
   b. If a workflow is not marked as Instant workflow, it means that it has either mandatory user input or optional user input. Example:



   c. You can also tap the **Scan settings** tab to modify the scan job properties. This screen contains all the properties that your administrator allowed to be modified for this

workflow.



If the **Scan settings** tab is not visible, it means that the scan settings are not configurable by end users.

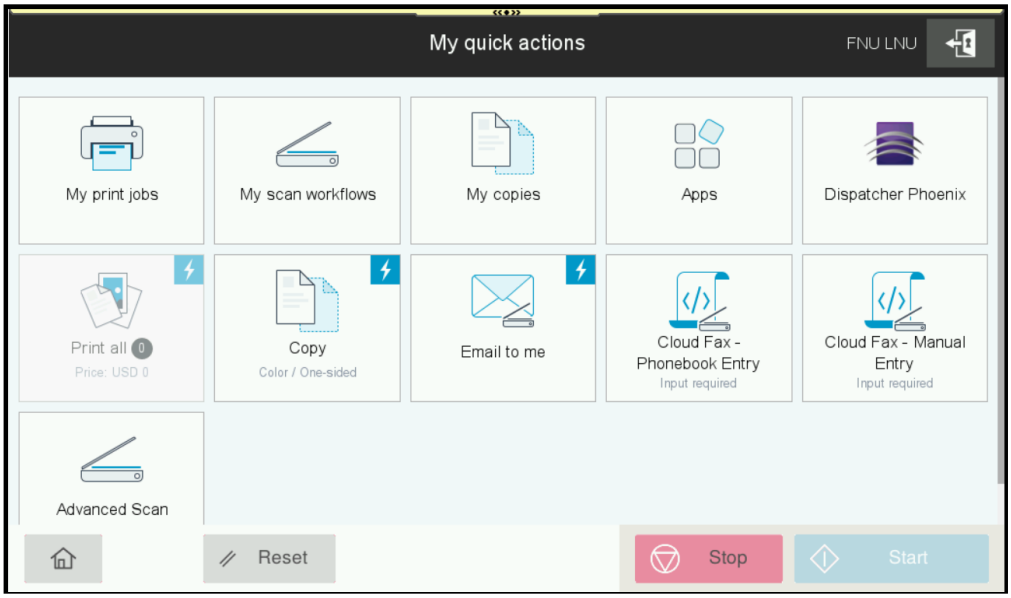
8. Tap **Scan**.

Scan - Cloud Fax workflows

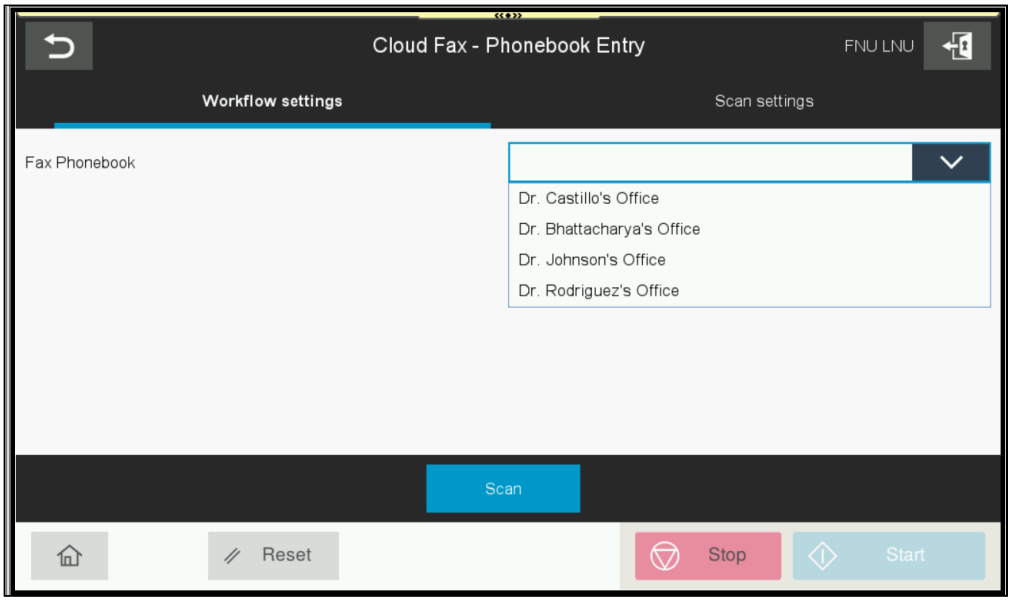
The Cloud Fax service is a high-capacity, reliable, and globally accessible service that enables the transmission and reception of faxes from a web portal or a Konica Minolta MFD. If your company purchased this service, perform the following steps to send faxes from the MFD:

1. Select a Cloud Fax sending method. There are two methods that your Administrator may have configured: Phonebook entry and Manual entry. Your Administrator could have

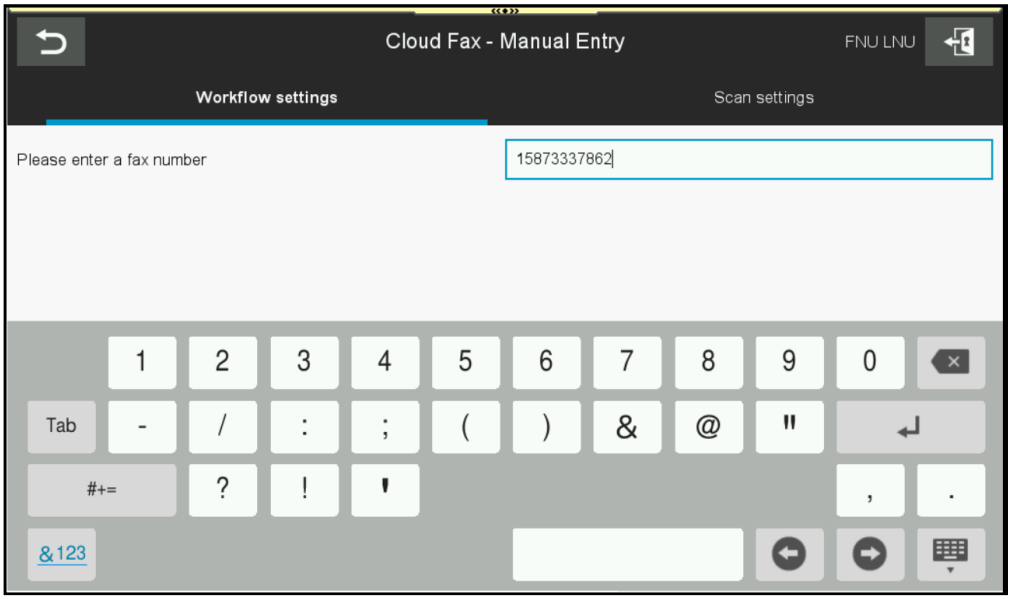
configured one or both methods.



a. Phonebook entry – this method allows you to select a predefined fax number from a list of numbers. Your Administrator may list the recipient's name, fax number, or both. In this example, only the name of the recipient is shown. To update or add a new recipient, please contact your Administrator.



b. Manual entry – this method allows you to enter a fax number manually.

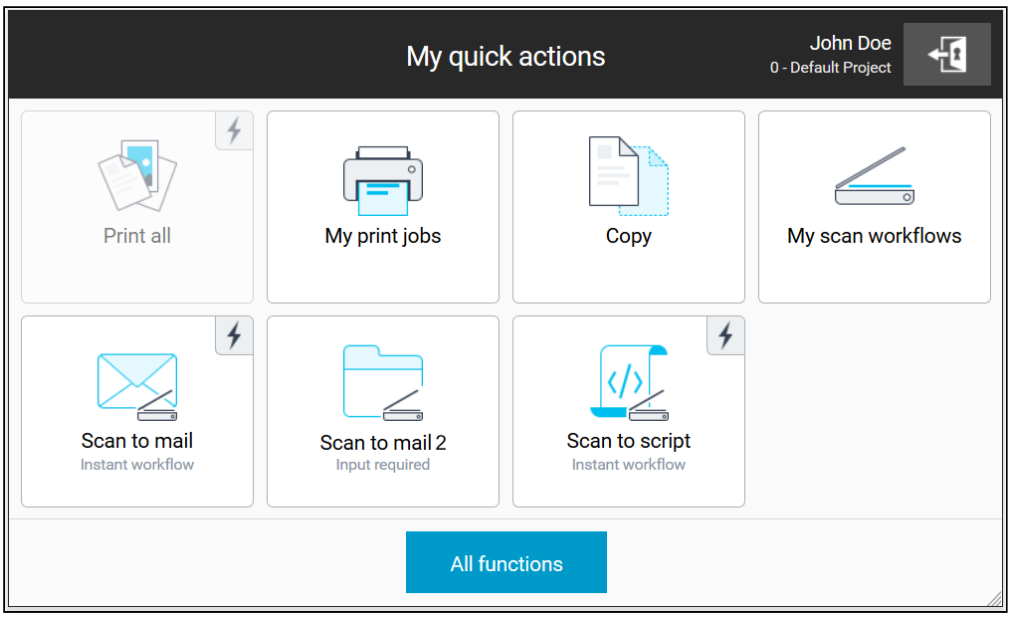


2. After selecting the recipient from the list or entering the fax number manually, tap **Scan**. Your document will be scanned and transferred to the cloud fax service. If your administrator configured email notifications in the system, you will receive an email notification with the status

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. Whether this application is installed on the MFD and functions as the home screen of the terminal depends on the configuration done by your administrator.

After logging in at the MFD, tap the **Dispatcher Quick actions** icon. Then tap the quick action you want to execute. The actions that you can execute directly (because they don't require any input from you) are called instant and are marked with a flash icon.



Supported languages

- Arabic
- Brazilian Portuguese
- Bulgarian
- Catalan
- Chinese Simplified
- Chinese Traditional
- Croatian
- Czech
- Danish
- Dutch
- Estonian
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Indonesian
- Italian
- Japanese

- Kazakh
- Korean
- Latvian
- Lithuanian
- Malaysian
- Norwegian
- Polish
- Portuguese
- Romanian
- Russian
- Serbian Cyrillic
- Serbian Latin
- Slovak
- Slovenian
- Spanish
- Swedish
- Thai
- Turkish
- Ukrainian

Dispatcher Paragon Embedded Terminal for Sharp

Registering your card

See Card registration at the MFD terminal

Logging in and out

Logging in

1. Place your card on the card reader attached to the printer or enter your PIN and tap **Login**. The authentication method depends on how your administrator configured the terminal.
2. You will see the Dispatcher Paragon embedded terminal home screen. The content of the home screen depends on how your administrator configured the terminal. It may contain shortcuts, **My print jobs** application, or other applications.

Selecting language

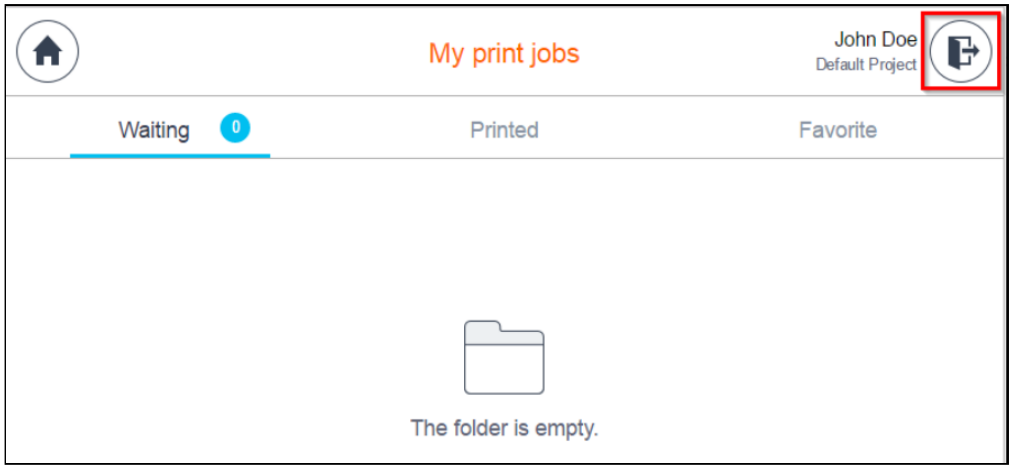
1. At the login screen, tap the language icon to display the *Select language* dialog.

2. Select the language and tap **Select**.

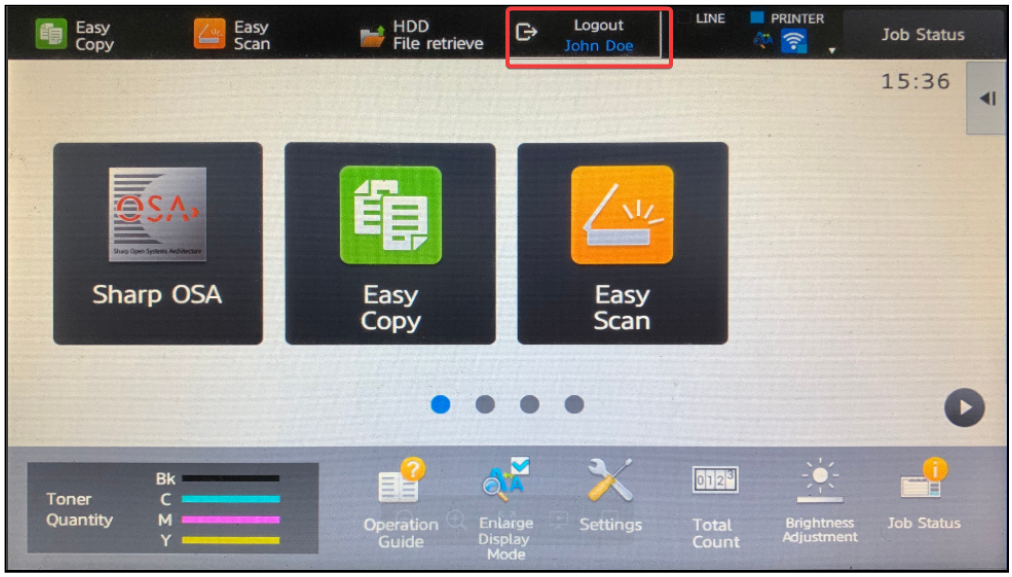
Logging out

You can use three methods to log out:

1. Tap the Logout icon on the home screen of Dispatcher Paragon embedded terminal.



2. Tap **Logout** in the device main menu.



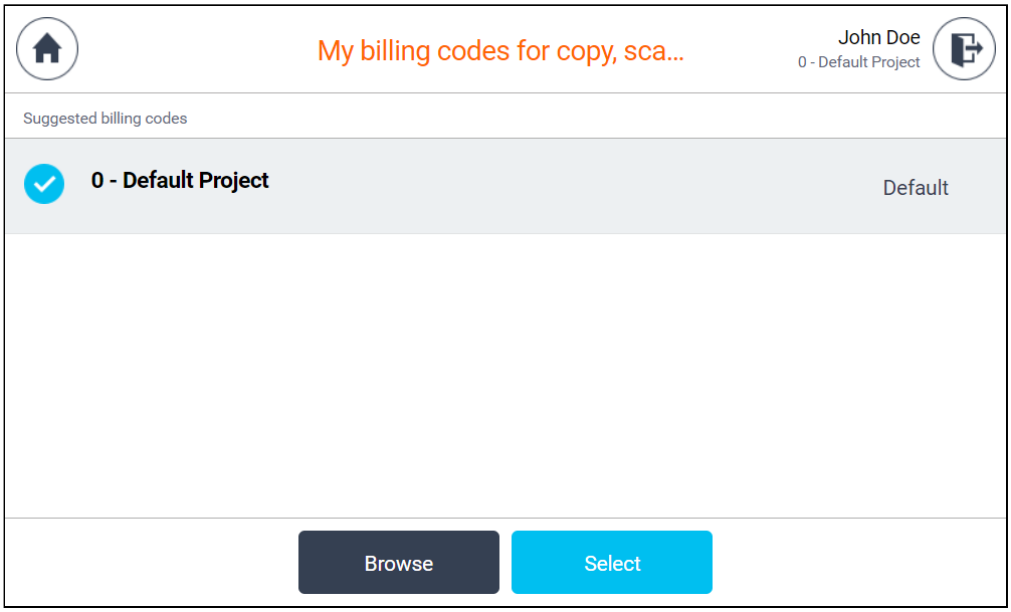
3. Place your card on the card reader attached to the printer.

Using billing codes

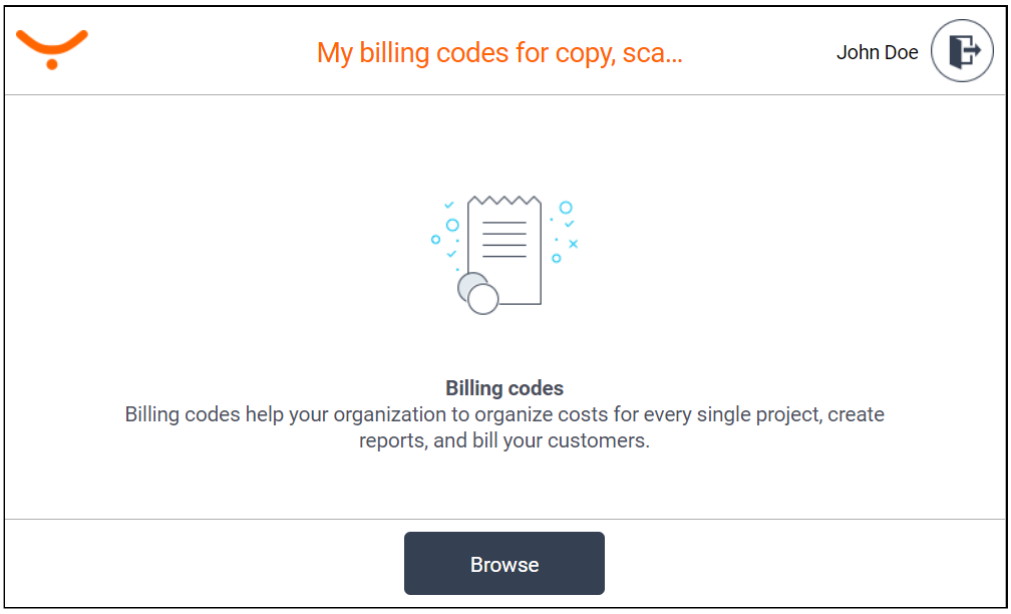
1. If your administrator enabled billing codes selection at the terminal, you will see the **Billing codes** application after logging in at the terminal.

2. If you have a default billing code assigned, it will be automatically selected (highlighted) for you at the home screen of the Billing codes application. Tap the **Select** button to confirm the

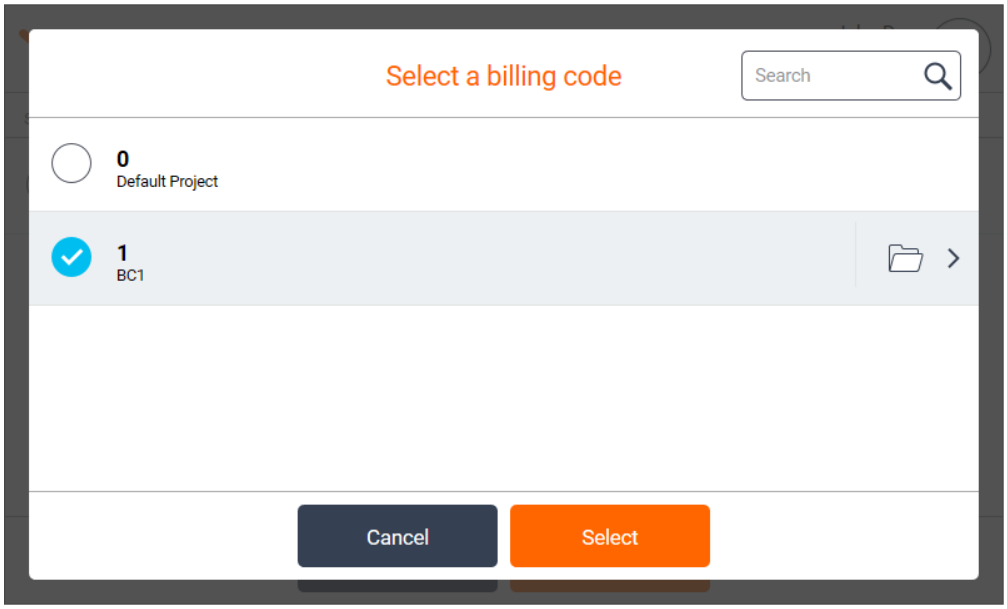
choice. If you don't want to use the default code, tap **Browse**.



3. If you don't have any default billing code, you will see the following screen. Tap **Browse** to select the code you wish to use for your session.



4. Tap the code you wish to use and then tap the **Select** button. For a more advanced search, see the Searching for billing codes section.



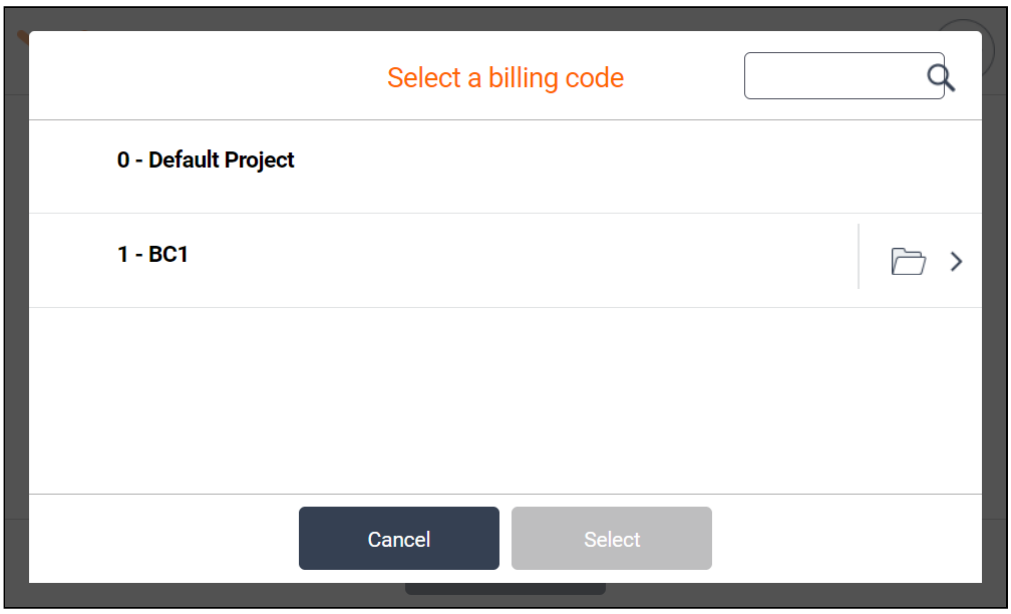
5. This concludes the authentication process. You will then see the home screen.

> Be aware that:
>
> - You cannot proceed with authentication unless you select a billing code.
> - If you have more than one code assigned to you and you want to change the default one, you cannot do so at the terminal. The change can only be made in the Dispatcher Paragon Cloud management interface by your administrator.
> - Whether the selected billing code applies to your print jobs or not, depends also on the billing codes configuration performed by your administrator.

Searching for billing codes

Browsing

1. After opening the browsing screen, you will see the root of the billing codes tree structure.
2. The billing codes which have sub-level codes have a folder icon next to them. Tap the folder icon to see the sub-level codes.



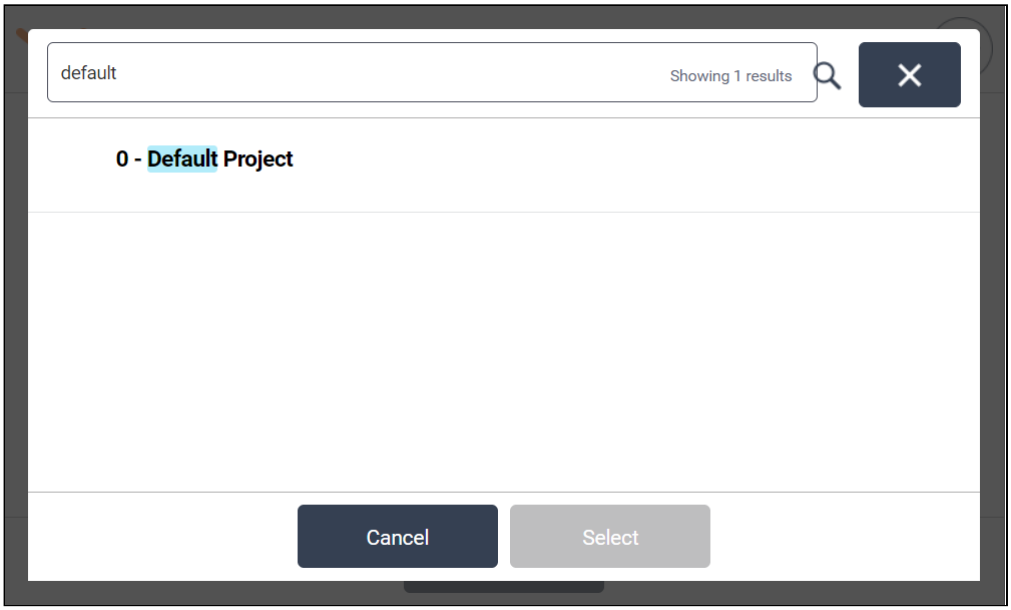
3. To go one level up in the tree structure, tap the return icon at the top of the screen.
4. When you select a billing code by tapping it, the **Select** button is enabled. Tap the button to select the code for your session.

Searching

If you cannot find the desired billing code via browsing, you can use searching via the search box on the browsing screen.

1. Tap inside the search field.
2. Enter the name or description you are searching for. The Billing codes application searches in both of these fields.
3. Tap the magnifying glass icon.

4. If you want to cancel your search and return to the browsing screen, tap the cross icon.

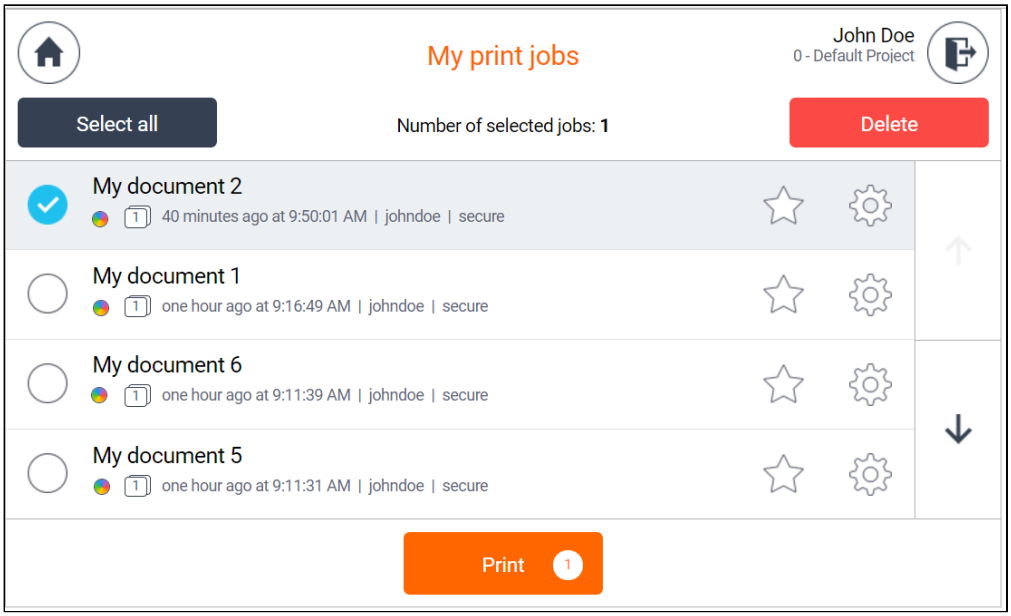


5. If your search returns some results, you will see a billing codes list.
6. When you select a billing code by tapping it, the **Select** button is enabled. Tap it to select the code for your session.
7. If you don't wish to select any billing codes from the list, tap **Cancel** in order to return to the Billing codes application home screen.

Printing and managing jobs

1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.
2. If the home screen is the main menu screen, tap **Sharp OSA** and then tap **Dispatcher Print**. If the home screen is **My quick actions** application, tap **My print jobs**.

3. You will see the **My print jobs** application. Tap the print job you wish to print.



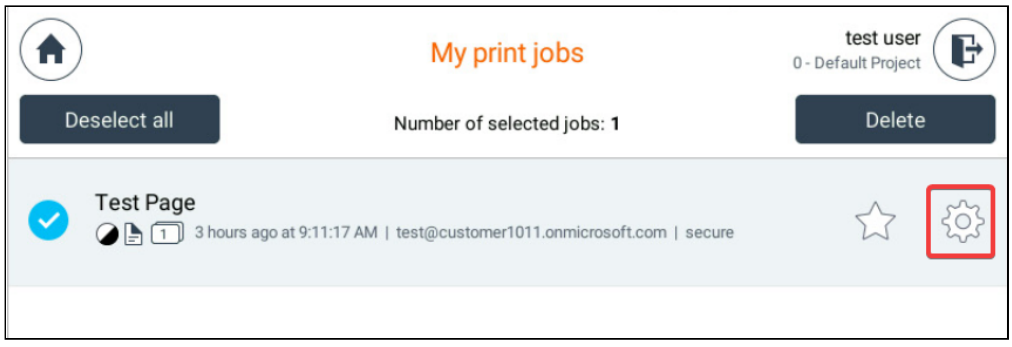
> If no job is selected, you can switch between the **Waiting**, **Printed**, and **Favorite** folders.

4. If needed, modify the finishing options.
5. Tap **Print**.

Finishing options

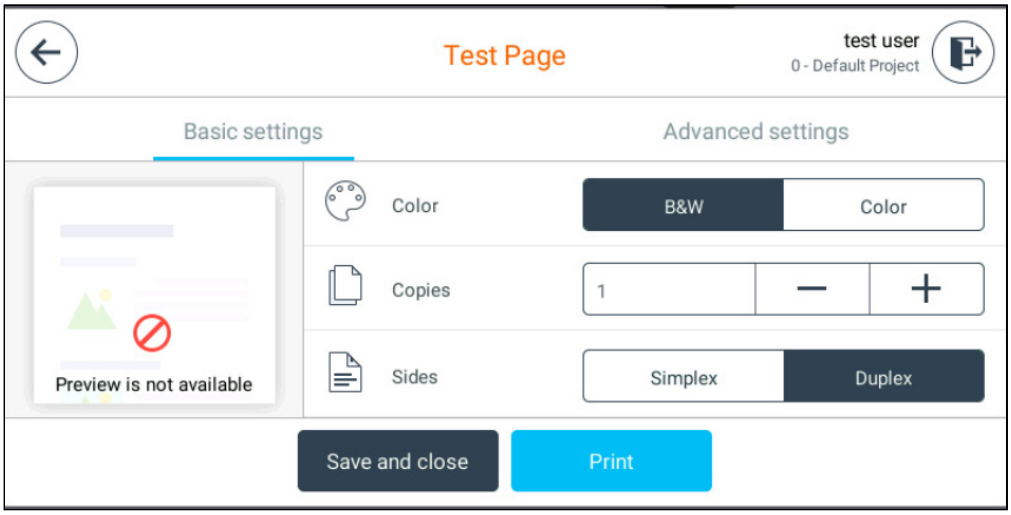
If your administrator has enabled this feature, you can modify the finishing options before printing your job.

1. To change basic finishing options (color, copies, sides) or the advanced options (stapling, punching, binding, folding), tap the settings icon.



2. You will see the job detail screen.

3. Adjust the basic finishing options as needed.



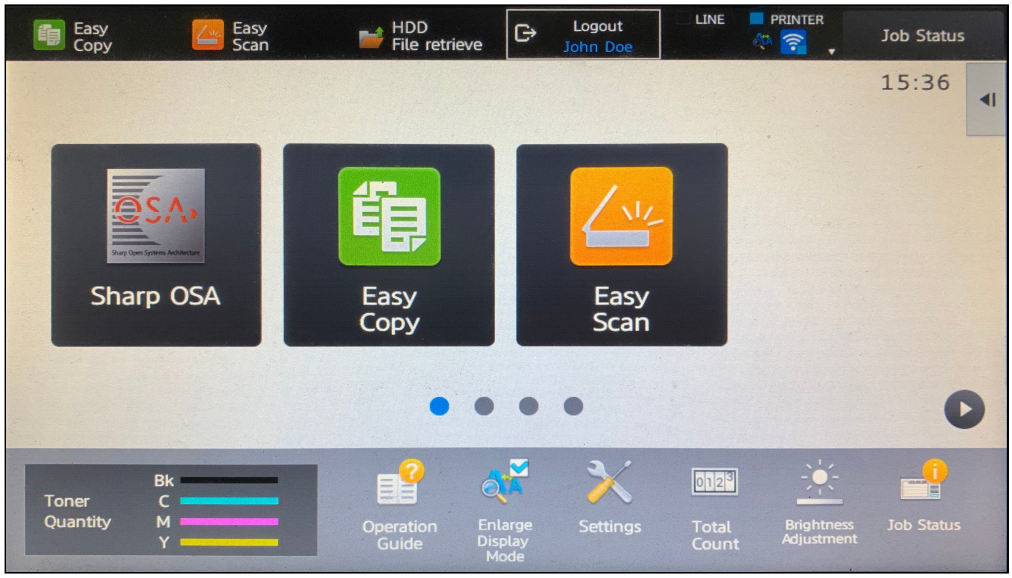
4. Tap **Advanced settings** to adjust the advanced finishing options.

5. Tap **Print** if you wish to print the job immediately or **Save and close** if you wish to return to **My print jobs** screen.

Copying

1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.

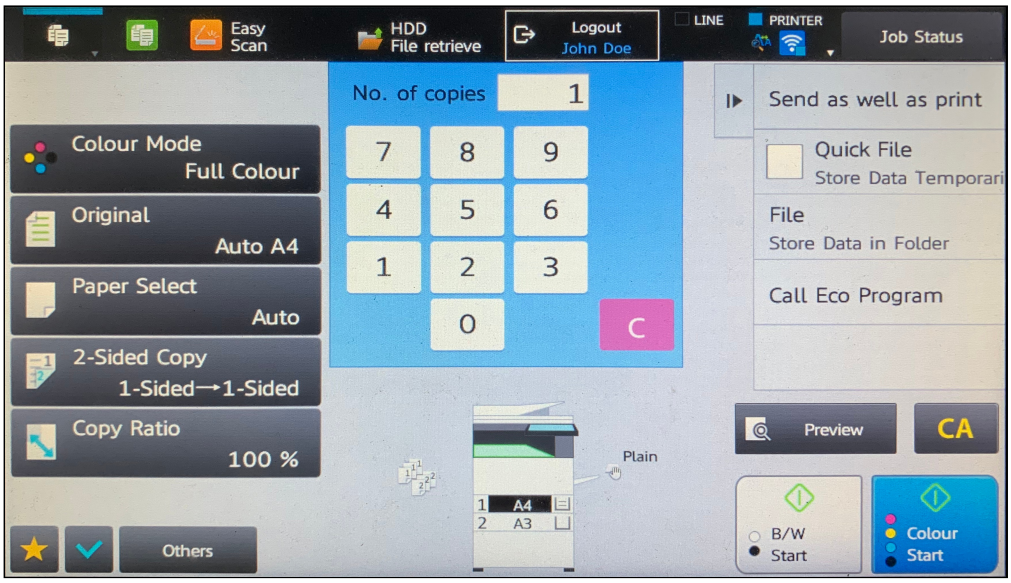
2. If the home screen is the main menu screen, tap **Easy Copy**.



> The main menu on your MFD may look slightly different.

3. If the home screen is one of the Dispatcher Paragon applications, tap the home icon to get to the main menu screen and then tap **Easy Copy**.

4. This action will take you to the native copy application. Adjust the available options (quantity, color, etc) as needed.



5. Tap **Start**.

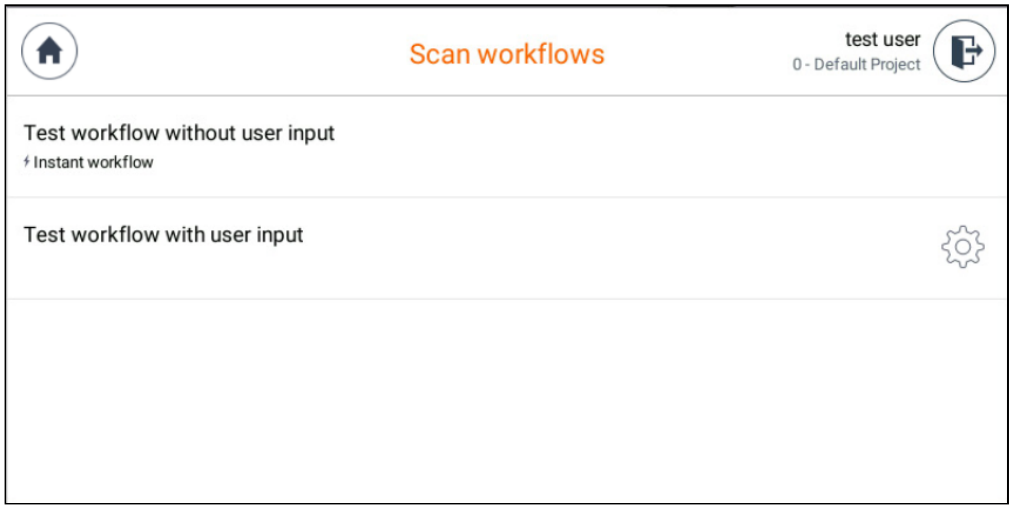
Scanning

1. Log in to the Dispatcher Paragon embedded terminal. The home screen of the terminal will be displayed. The content of the home screen depends on the configuration done by your administrator.

2. If the home screen is the main menu screen, tap **Sharp OSA > Dispatcher Scan**.

3. If the home screen is one of the Dispatcher Paragon applications, tap the home icon to go to the main menu and then tap **Sharp OSA > Dispatcher Scan**.

4. This will take you to the **Scan workflows** application.

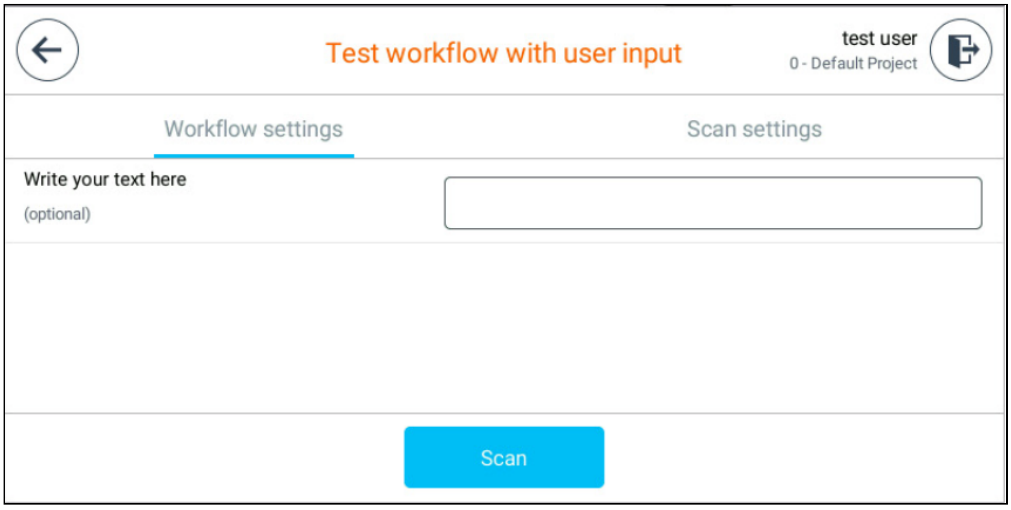


5. The Scan workflows application displays all scan workflows that your administrator made available to you.

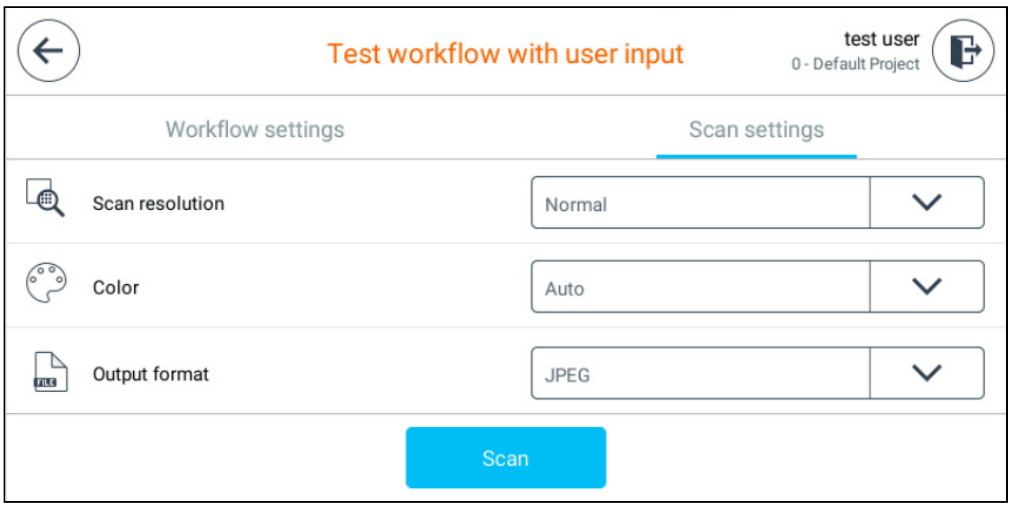
6. Tap the workflow you wish to execute.

   a. If a workflow is marked as **Instant workflow**, it will execute immediately, without any input from you.

   b. If a workflow is not marked as Instant workflow, it means that it has either mandatory user input or optional user input. Example:



   c. You can also tap the **Scan settings** tab to modify the scan job properties. This screen contains all the properties that your administrator allowed to be modified for this workflow.

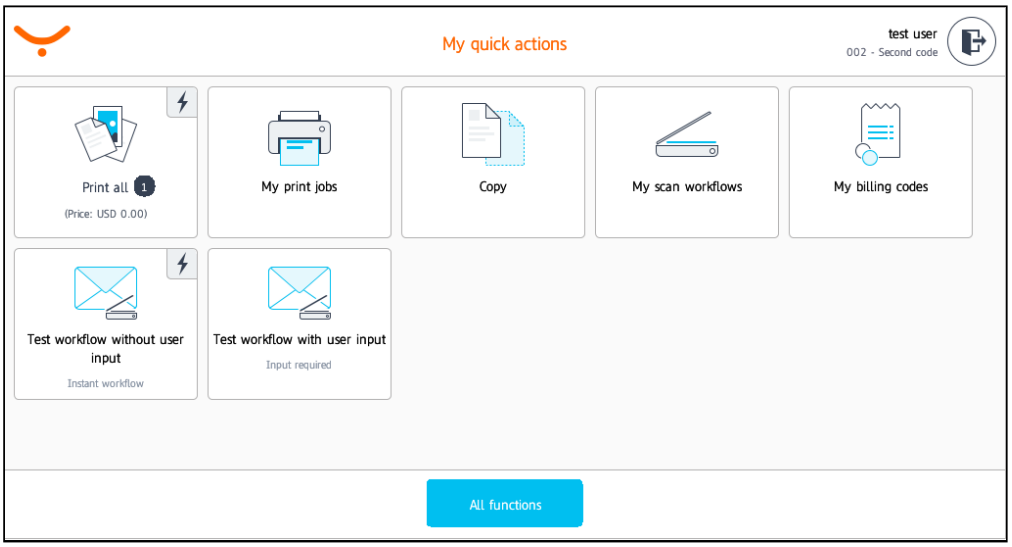


If the **Scan settings** tab is not visible, it means that the scan settings are not configurable by end users.

7. Tap **Scan**.

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. Whether this application is installed on the MFD and functions as the home screen of the terminal depends on the configuration done by your administrator.



Dispatcher Paragon Embedded Terminal for Xerox

Registering your card

See Card registration at the MFD terminal.

Logging in and out

Logging in

1. Place your card on the card reader attached to the printer or enter your PIN. The authentication method depends on how your administrator configured the terminal.
2. If this is enabled by the administrator, you will see the **Print all** screen. Tap **Yes** to release all print jobs or **No** to display the Dispatcher Paragon embedded terminal home screen. The content of the home screen depends on how your administrator configured the terminal. It may contain shortcuts, **My print jobs** application, or other applications.

Selecting language

1. Tap the language icon (or the **Language** hardware button on the older models) to display the **Language** screen.

2. Select the language and tap **OK**.

Logging out

You can use the following methods to log out:

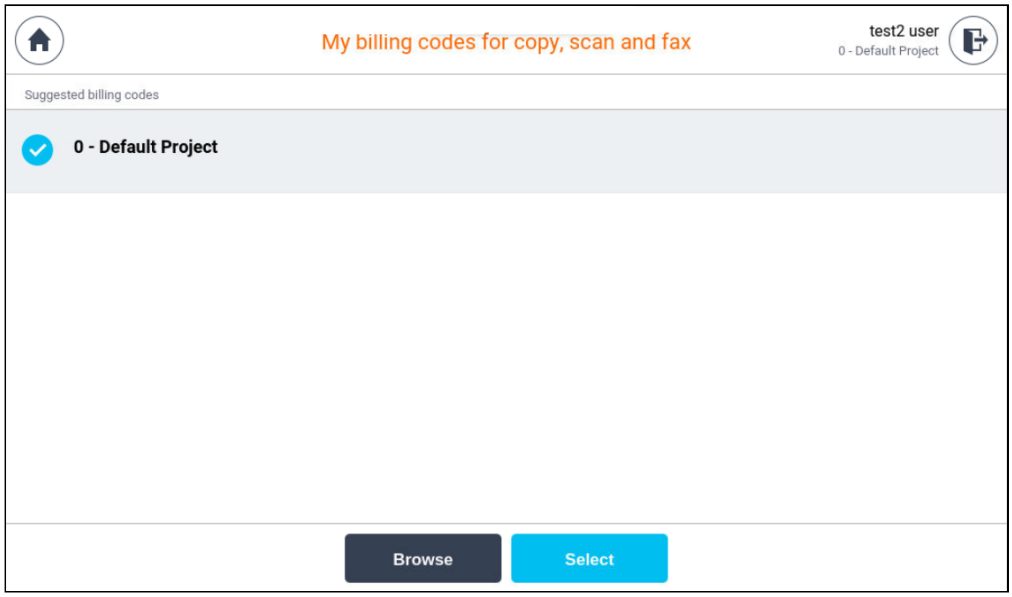
1. Tap the logout icon in the top right corner of the screen.

2. Place your card on the card reader attached to the printer.
3. After a time period set in your environment, you will be logged out automatically.

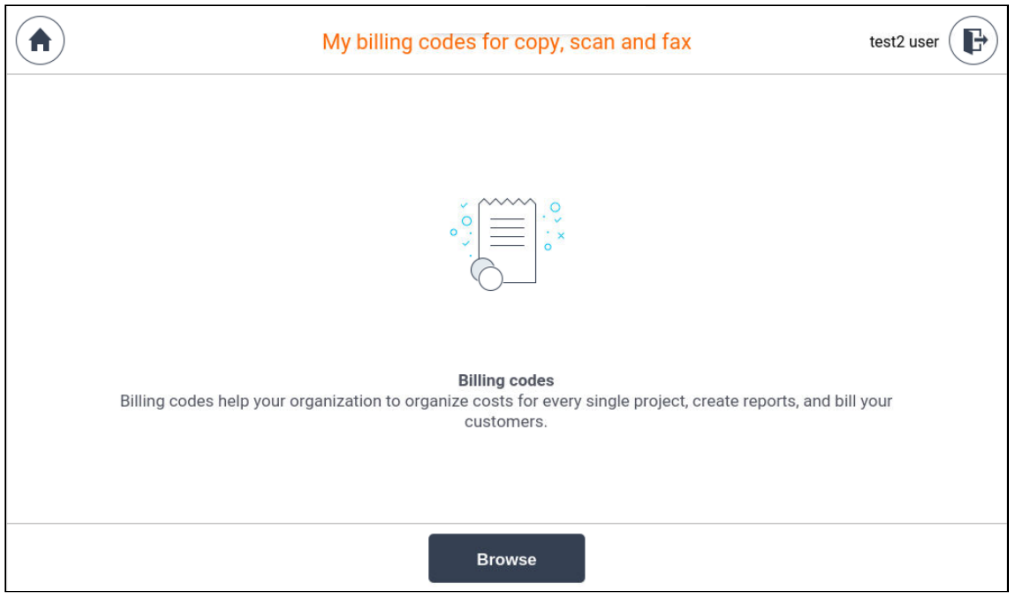
Using billing codes

1. If your administrator enabled Billing codes selection at the terminal, you will see the **Billing codes** application after logging in at the terminal.
2. If you have a default billing code assigned, it will be automatically selected (highlighted) for you at the home screen of the Billing codes application. Tap the **Select** button to confirm the

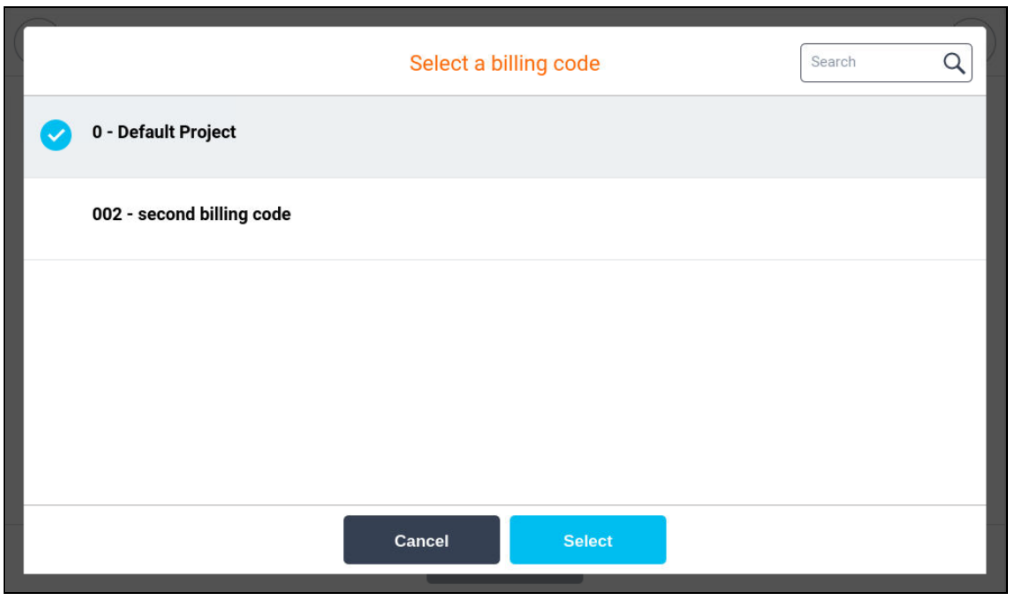
choice. If you don't want to use the default code, tap **Browse**.



3. If you don't have any default billing code, you will see the following screen. Tap **Browse** to select the code you wish to use for your session.



4. Tap the code you wish to use and then tap the **Select** button. For a more advanced search, see the Searching for billing codes section.



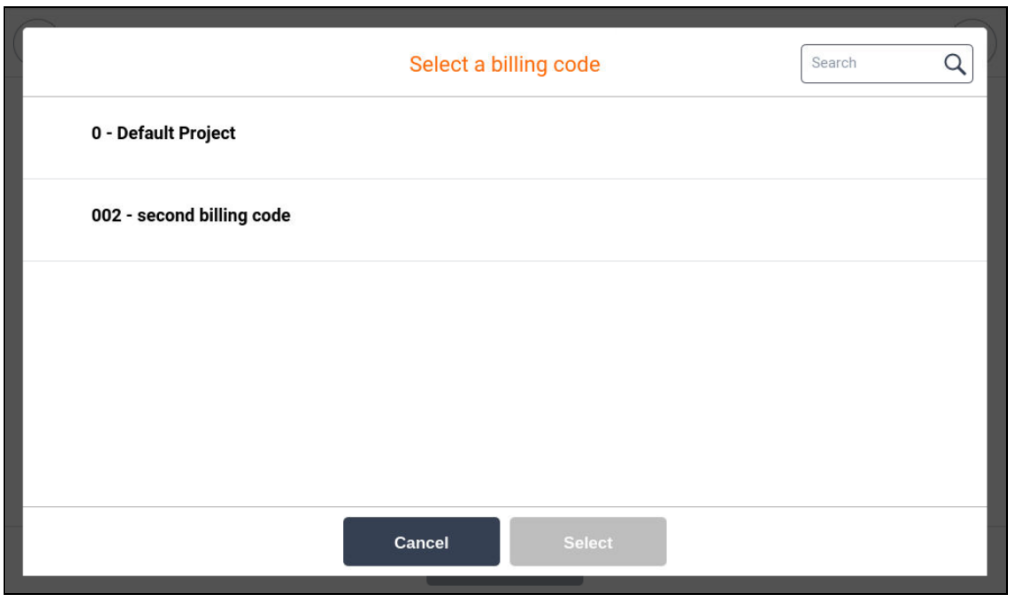
5. This concludes the authentication process. You will then see the home screen.

> Be aware that:
>
> - You cannot proceed with authentication unless you select a billing code.
> - If you have more than one code assigned to you and you want to change the default one, you cannot do so at the terminal. The change can only be made in the Dispatcher Paragon Cloud management interface by your administrator.
> - Whether the selected billing code applies to your print jobs or not, depends also on the billing codes configuration performed by your administrator.

Searching for billing codes

Browsing

1. After opening the browsing screen, you will see the root of the billing codes tree structure.
2. The billing codes which have sub-level codes have a folder icon next to them. Tap the folder icon to see the sub-level codes.



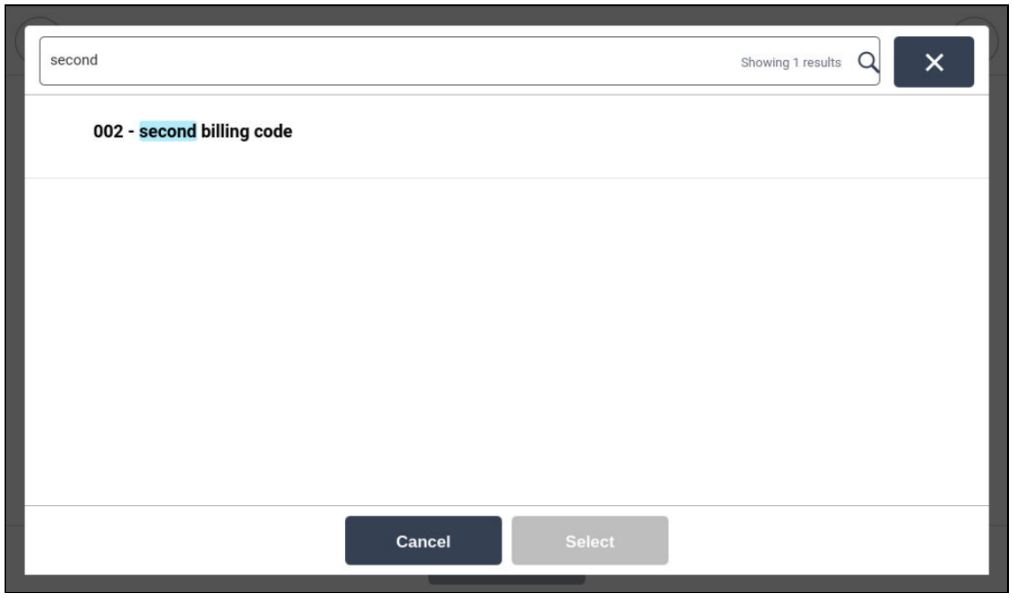
3. To go one level up in the tree structure, tap the return icon
4. When you select a billing code by tapping it, the **Select** button is enabled. Tap the button to select the code for your session.

Searching

If you cannot find the desired billing code via browsing, you can use searching via the search box on the browsing screen.

1. Tap inside the search field.
2. Enter the name or description you are searching for. The Billing codes application searches in both of these fields.
3. Tap the magnifying glass icon.

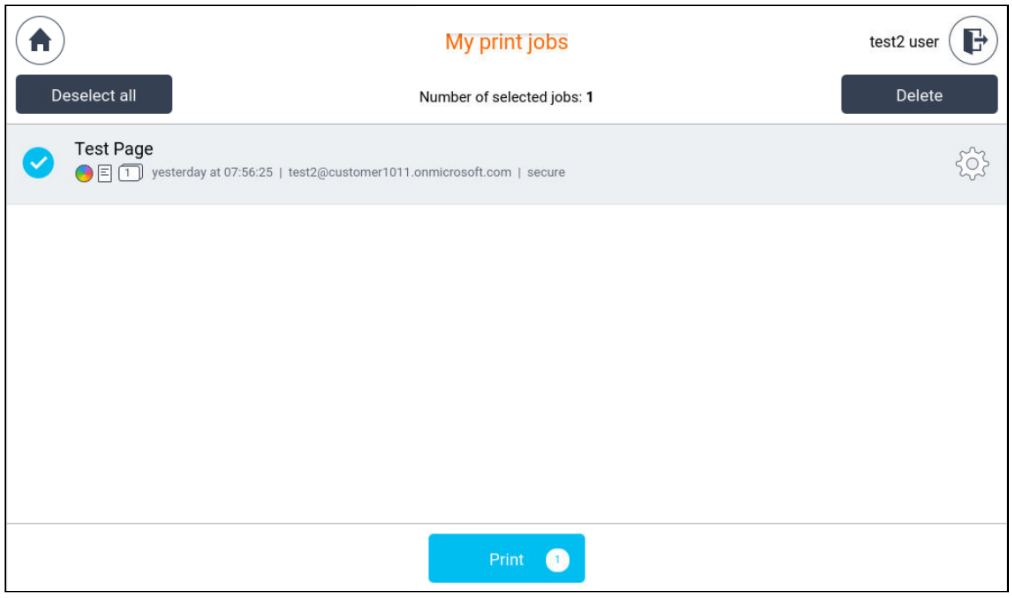
4. If you want to cancel your search and return to the browsing screen, tap the cross icon.



5. If your search returns any results, you will see a billing codes list.
6. When you select a billing code by tapping it, the **Select** button is enabled. Tap it to select the code for your session.
7. If you don't wish to select any billing codes from the list, tap **Cancel** in order to return to the Billing codes application home screen.

Printing and managing jobs

1. Log in to the Dispatcher Paragon embedded terminal.
2. On the **Home** screen, tap **SafeQ print**. This will open the **My print jobs** screen. If your home screen is **My print jobs**, skip this step.
3. On the **My print jobs** screen, select the print job(s) that you wish to print.



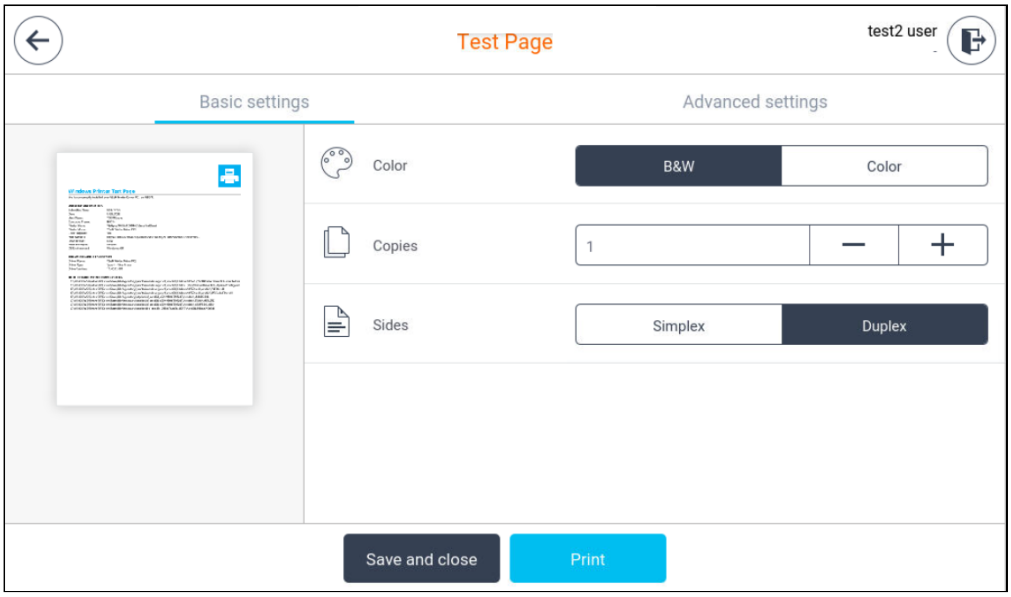
4. If needed, modify the finishing options.
5. Tap **Print**.

Finishing options

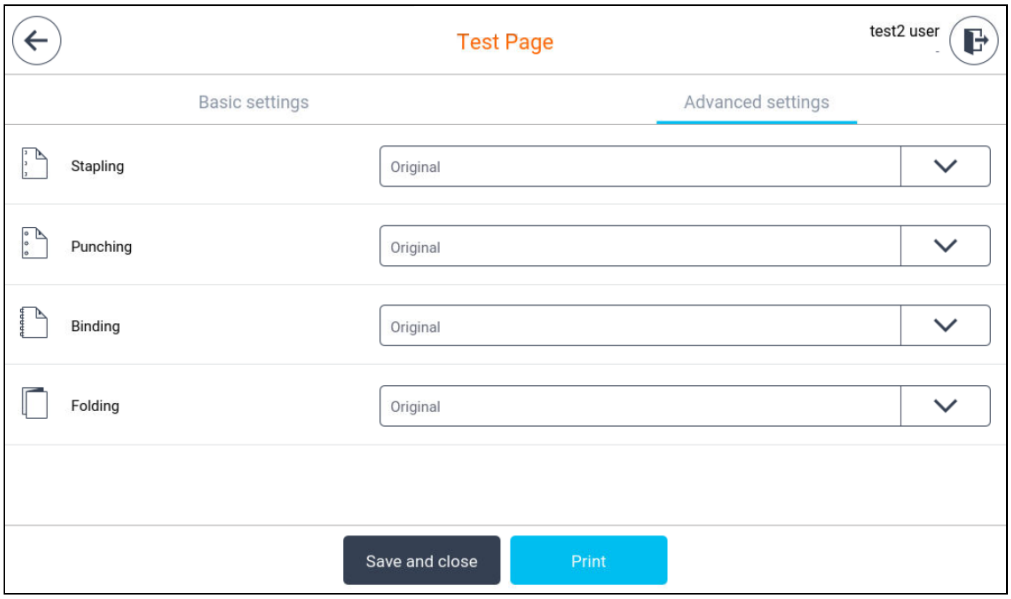
If your administrator has enabled this feature, you can modify the finishing options before printing your job.

1. To change basic finishing options (color, copies, sides) or the advanced options (stapling, punching, binding, folding), tap the settings icon.

2. You will see the job detail screen.
3. Adjust the basic finishing options as needed.



4. Tap **Advanced settings** to adjust the advanced finishing options.

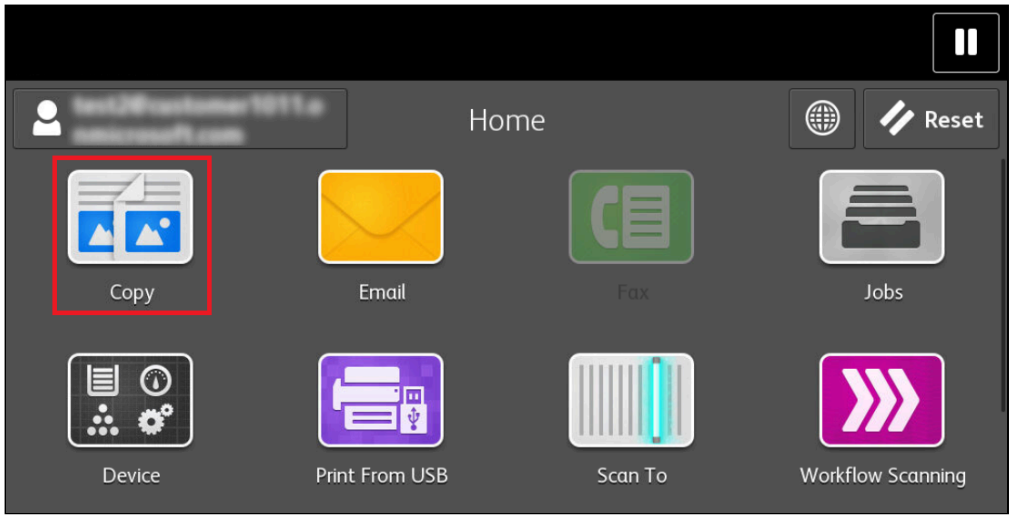


5. Tap **Print** if you wish to print the job immediately or **Save and close** if you wish to return to **My print jobs** screen.

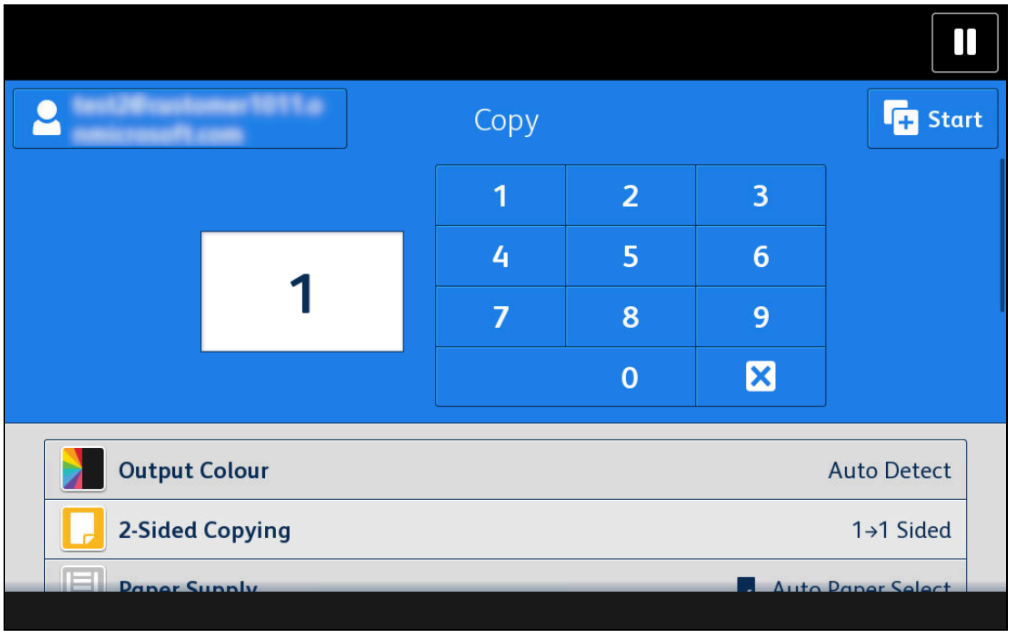
Copying

1. Log in to the Dispatcher Paragon embedded terminal.
2. On the **Home** screen, tap **Copy**. This action will take you to the native copy application.
3. If the home screen of the terminal is **My print jobs** application, tap the home button in the top left corner.

4. On the **Home** screen, tap **Copy**.



5. This action will take you to the native copy application.

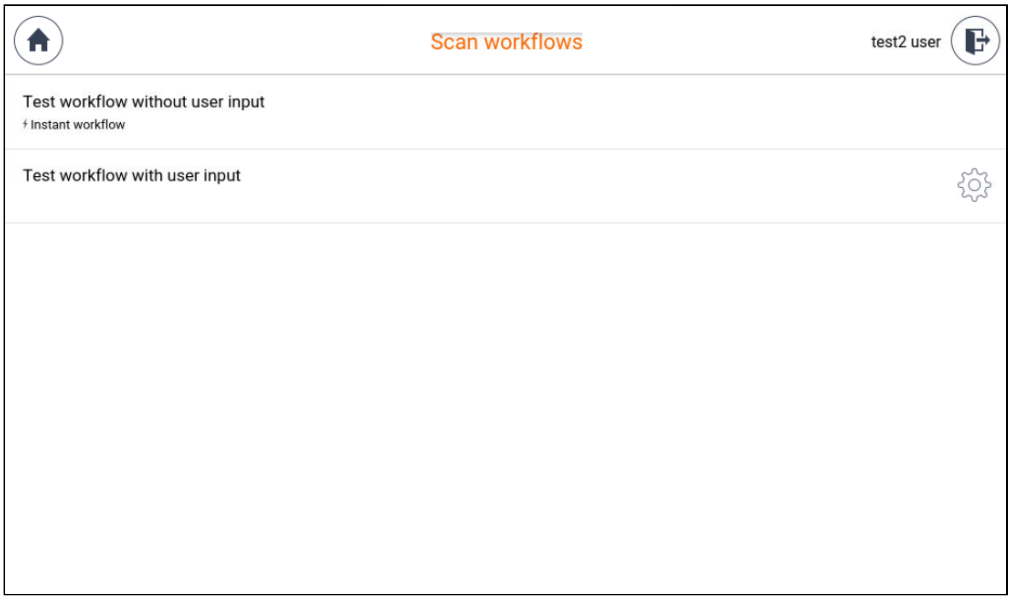


6. Select the number of copies by entering the number on the keypad.
7. Adjust the copy settings as needed by tapping the available options.
8. Tap **Start**.

Scanning

1. Log in to the Dispatcher Paragon embedded terminal.
2. On the **Home** screen, tap **SafeQ scan**. This opens the **Scan workflows** screen.
3. If the home screen of the terminal is **My print jobs** application, tap the home button in the top left corner.

4. On the **Home** screen, tap **SafeQ scan**. This opens the **Scan workflows** screen.

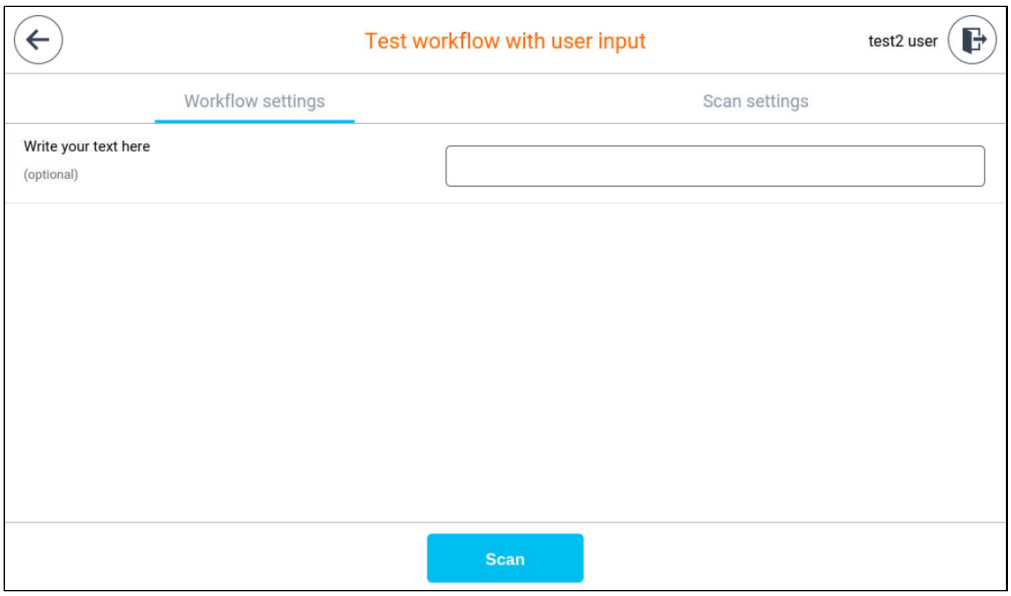


5. The Scan workflows application displays all scan workflows that your administrator made available to you.

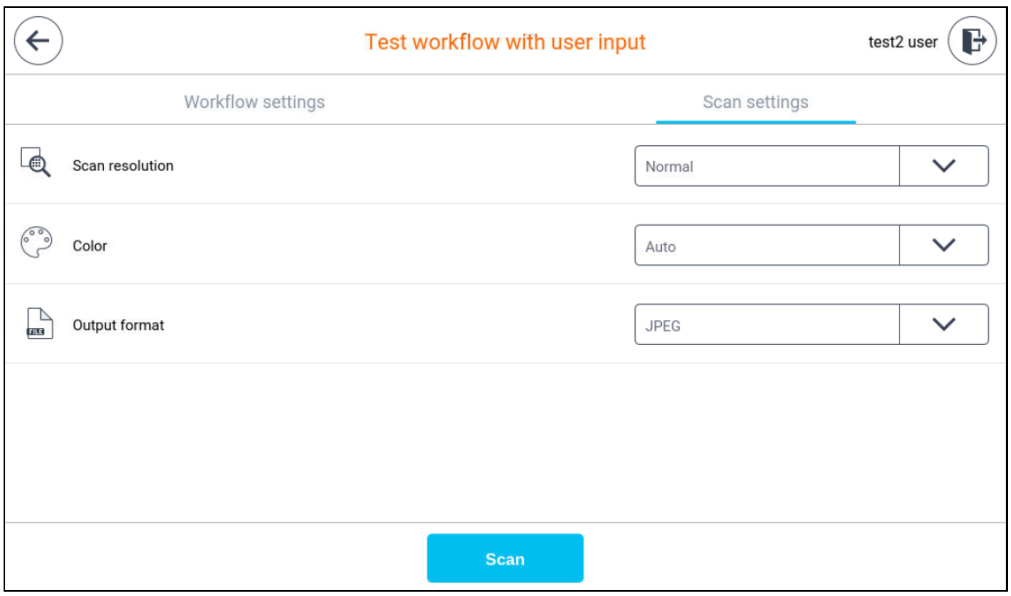
6. Tap the workflow you wish to execute.

   a. If a workflow is marked as **Instant workflow**, it will execute immediately, without any input from you.

   b. If a workflow is not marked as Instant workflow, it means that it has either mandatory user input or optional user input. Example:



   c. You can also tap the **Scan settings** tab to modify the scan job properties. This screen contains all the properties that your administrator allowed to be modified for this workflow.



If the **Scan settings** tab is not visible, it means that the scan settings are not configurable by end users.

d. Tap **Scan**.

3.7 USING THE DISPATCHER PARAGON CLOUD MOBILE APP

The Dispatcher Paragon Cloud mobile app allows you to submit documents for print. You can upload the documents directly in the app or via a share extension/share menu on iOS and Android.

Supported formats:

Format	Android	iOS
BMP	✓	✓
GIF	✓	✗
HEIF	✓	✗
JPEG	✓	✓
PDF	✓	✓

Format	Android	iOS
PNG	✓	✓
rawImage	✗	✓
SVG	✗	✓
TIFF	✗	✓
WebP	✓	✓

After submission, the mobile app converts all formats other than PDF to PDF.

Supported languages:

- English

> **Limitations**
>
> You cannot use the app to:
>
> - release print jobs on MFDs
> - scan documents
> - work with already uploaded documents (modify, delete, bulk operations, etc.)

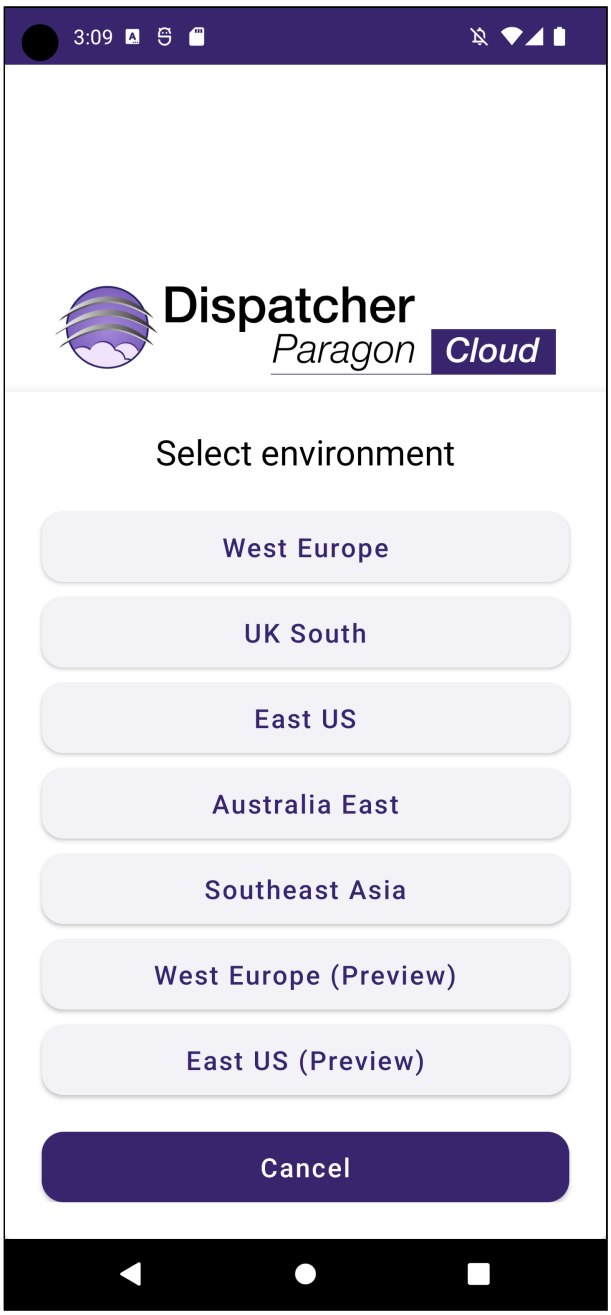
3.7.1 USING THE DISPATCHER PARAGON CLOUD APP FOR ANDROID

Downloading the app

Download the app from Google Play.

Signing in

1. Launch the app.
2. Tap **Sign in**.
3. Select the instance (environment) in which your company's Dispatcher Paragon Cloud is running. If you are unsure, contact your administrator. After that, you will see the login screen.



4. If you are an Externally managed user, tap **Sign in with Microsoft**. Enter your company credentials.
5. If you are an Internally managed user, enter your Dispatcher Paragon Cloud credentials and tap **Sign in**.
6. You will see the homepage of the mobile app – **My Print jobs**.

Alternative login to a custom solution

1. Tap **Alternative login**.

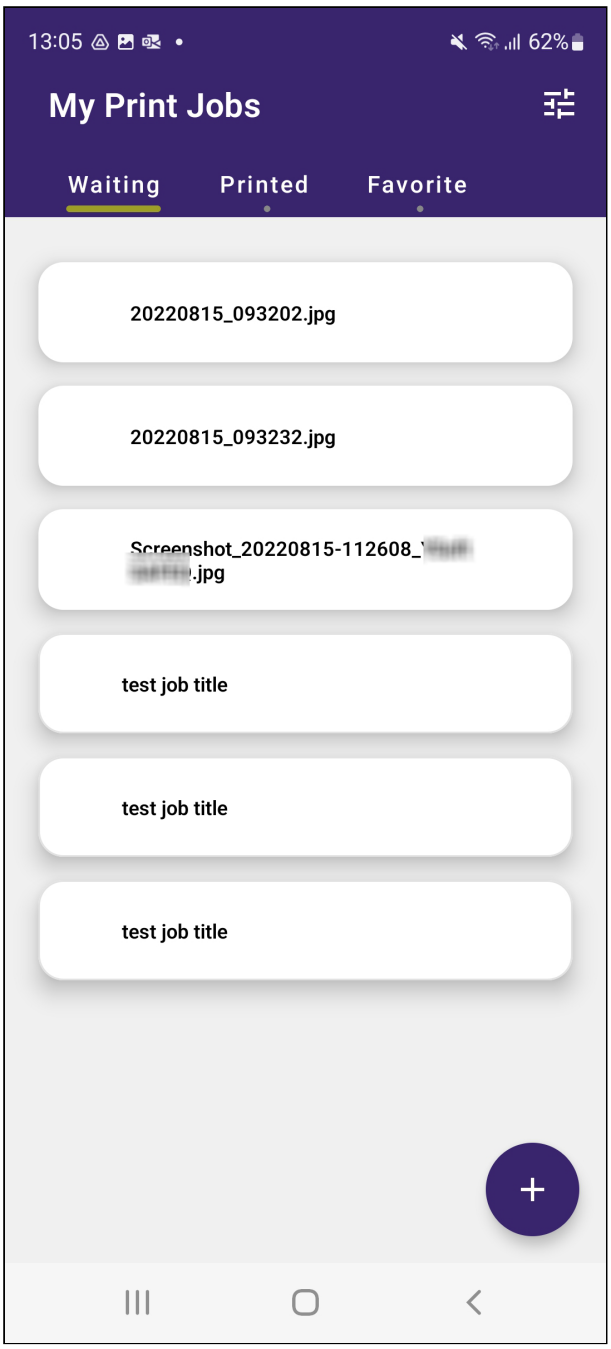
2. On the **Alternative login** screen, fill in the identity provider URL, API endpoint, and client ID.
3. If you want to allow communication that is not secured by TLS, enable **Ignore invalid server certificate**.
4. Tap **Sign in**.

My Print Jobs

The default tab of **My Print Jobs** displays all of your waiting job list.

Tap **Printed** to see the already printed print jobs.

Tap **Favorite** to see your favorite print jobs.



Submitting print jobs

To submit a print job:

1. Tap the **+** icon at the bottom of the **My Print Jobs** screen.
2. Select one or more documents you want to upload from the list.
3. Alternatively, you can submit documents to the Dispatcher Paragon Cloud application from the share menu of any mobile application that supports printing.

Signing out

1. Tap the settings icon in the top right corner.
   
2. Tap **Sign out**.

3.7.2 USING THE DISPATCHER PARAGON CLOUD APP FOR IOS

Downloading the app

Download the app from App Store.

Signing in

1. Launch the app.
2. Tap **Sign in**.
3. Select the instance (environment) in which your company's Dispatcher Paragon Cloud is running. If you are not sure, contact your administrator. After that, you will see the login screen.

4. If you are an Externally managed user, tap **Sign in with Microsoft**. Enter your company credentials.
5. If you are an Internally managed user, enter your Dispatcher Paragon Cloud credentials and tap **Sign in**.
6. You will see the homepage of the mobile app – **My Print jobs**.

Alternative login to a custom solution

1. Tap **Alternative login**.

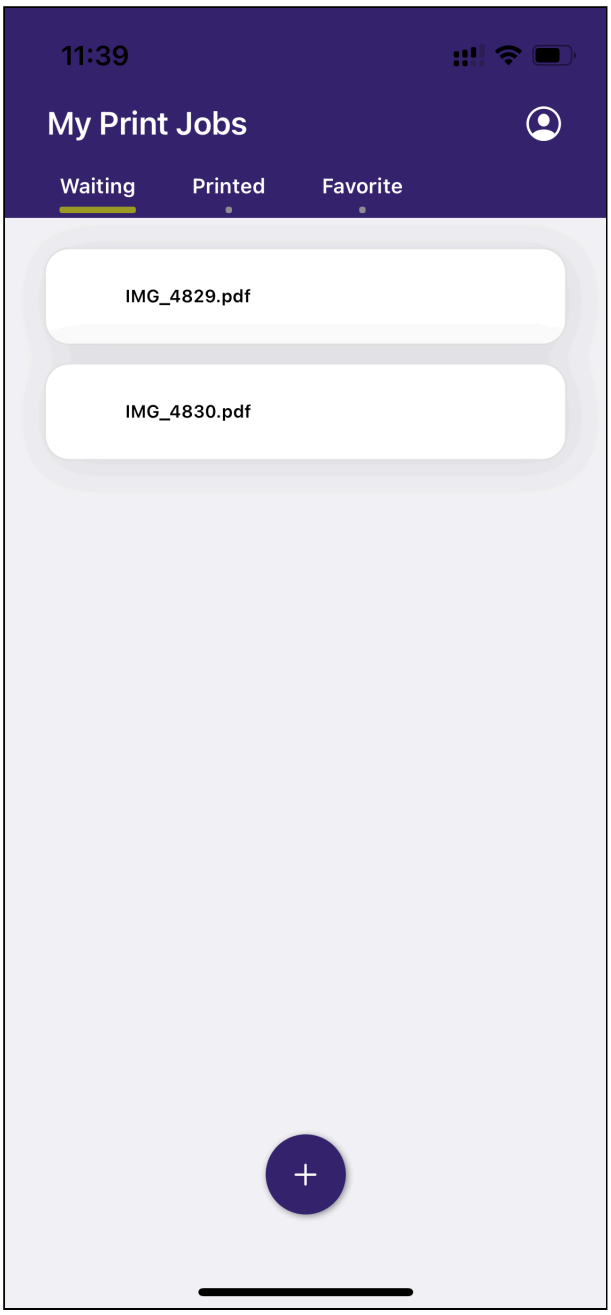
2. On the **Alternative login** screen, fill in the identity provider URL, API endpoint, and client ID.
3. If you want to allow communication that is not secured by TLS, enable **Ignore invalid server certificate**.
4. Tap **Sign in**.

My Print Jobs

The default tab **My Print Jobs** shows your waiting jobs.

Tap **Printed** to see the already printed print jobs.

Tap **Favorite** to see your favorite print jobs.



Submitting print jobs

To submit a print job:

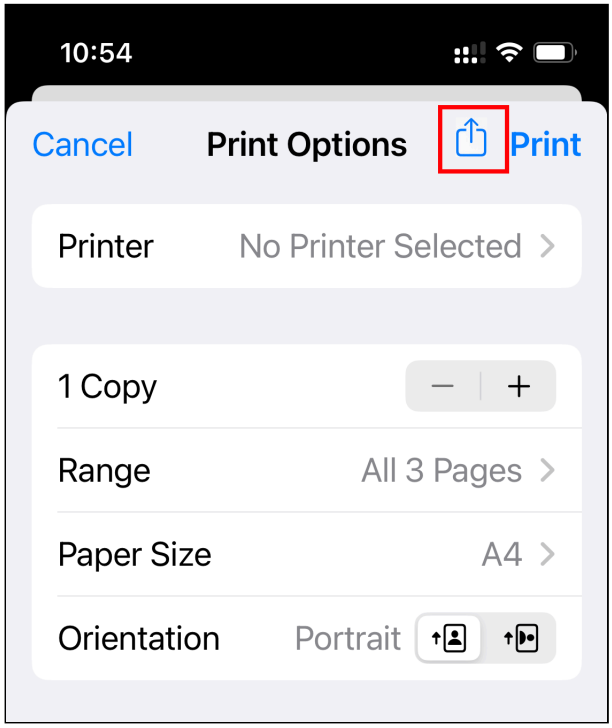
1. Tap the **+** button at the bottom of the **My Print Jobs** screen.
2. Select one or more documents you want to upload from the list.
3. Alternatively, you can submit documents to the Dispatcher Paragon Cloud application by tapping the share icon in any mobile application that supports printing. For more info, see Share photos and videos on iPhone.

Printing unsupported file formats

If you wish to print a document that is in an unsupported file format, you can use the standard system print dialog and share the output into the Dispatcher Paragon Cloud app instead of selecting the AirPrint printer. Note that you can only do this in apps that support system print.

iOS 16 or higher

1. Open the system print dialog and utilize the system print finishing options.
2. Tap on the share icon.

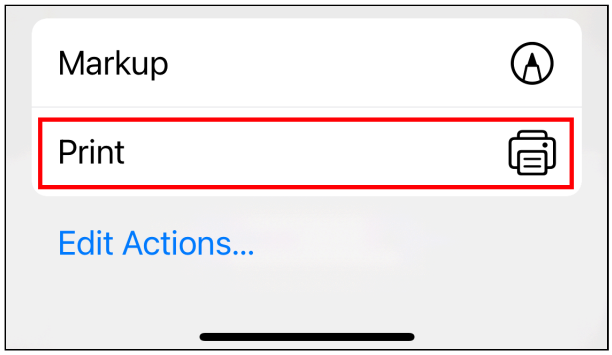


3. To submit the print job, continue as described in the *Submitting print jobs* section above.

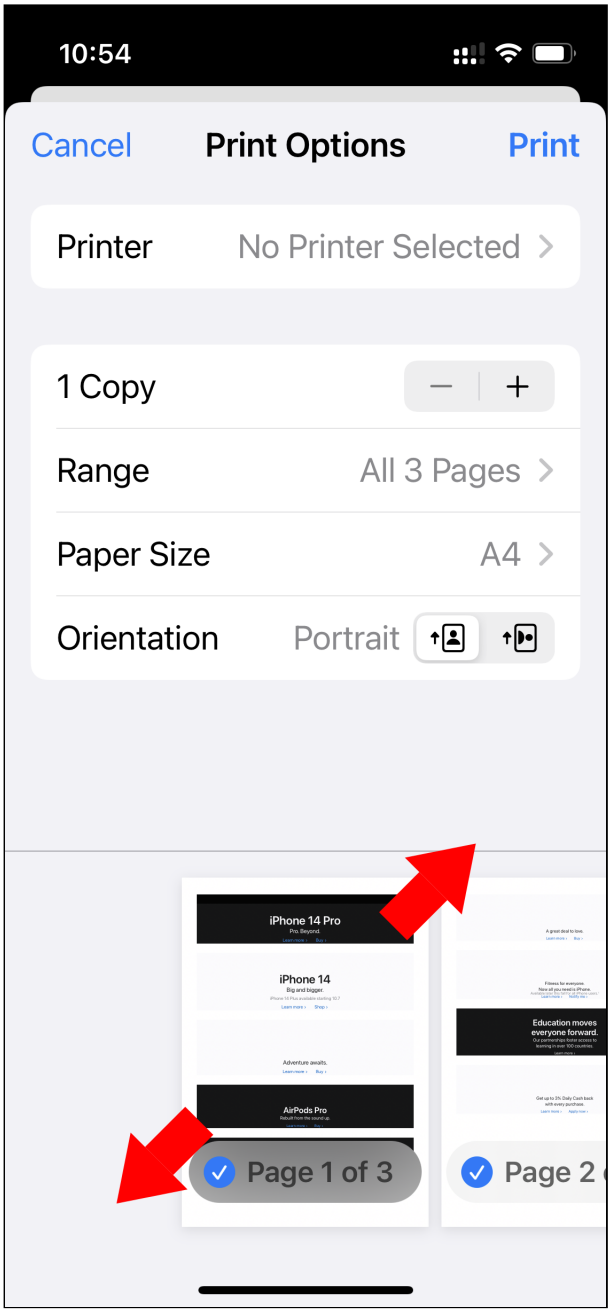
iOS 15 or lower

1. Open the app that you want to print from and tap the share icon.

2. Scroll down and tap **Print**. The **Print Options** screen opens.



3. On the **Print Options** screen, zoom by pinching with two fingers on the document preview. This will open the document preview in PDF format.



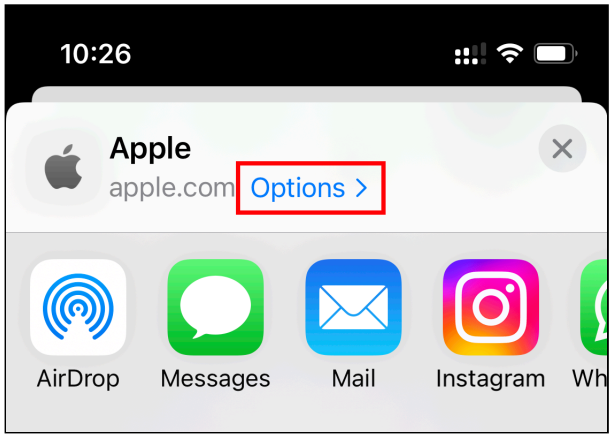
4. On the preview screen, tap on the share icon at the bottom of the screen.
5. Submit the print job as described in the *Submitting print jobs* section above.

Printing a web page from Safari

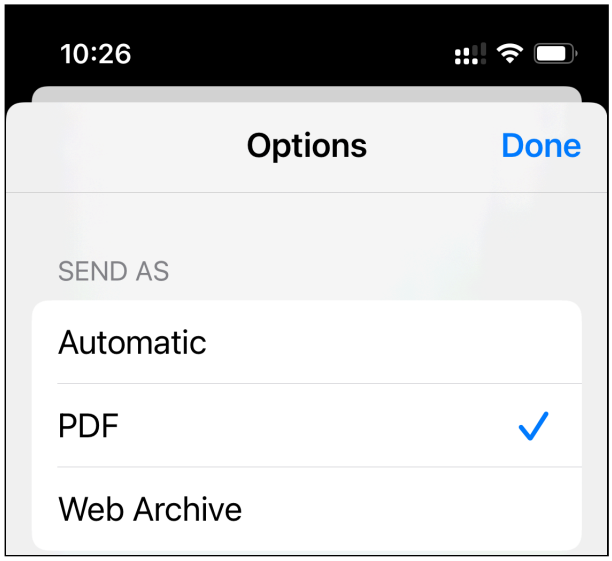
If you want to print a webpage from the Safari app, do the following:

1. Tap the share icon at the bottom of the screen.

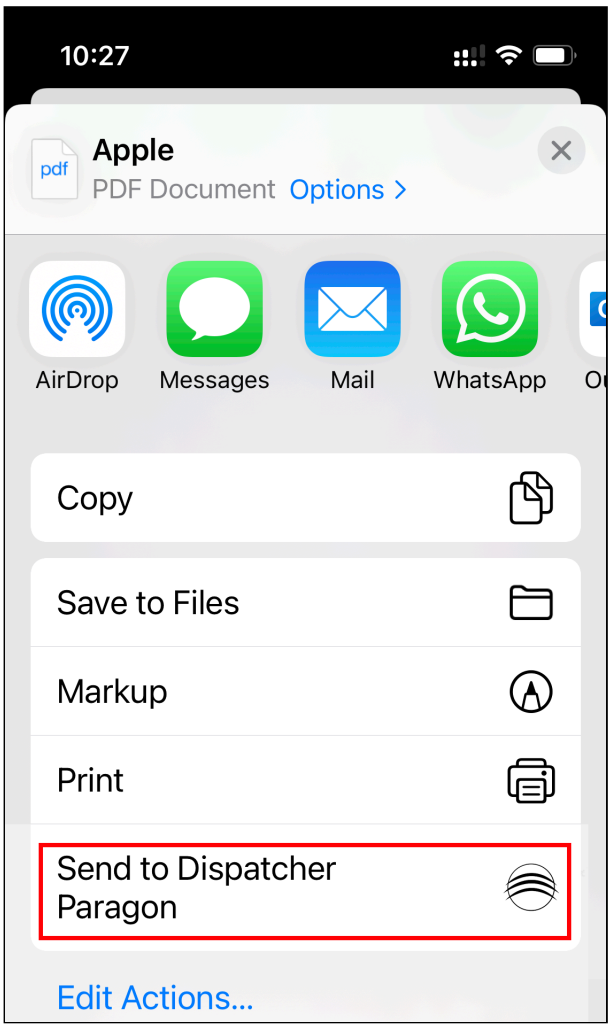
2. In the share menu, tap **Options**.



3. Make sure that the PDF option is selected and tap **Done**.



4. The **Send to Dispatcher Paragon** option is now visible in the share menu.



Logging out

1. Tap the profile icon in the top right corner.
   
2. Tap **Log out**.

3.8 MANAGEMENT INTERFACE GUIDE

The Dispatcher Paragon Cloud management interface is used by administrators to manage Dispatcher Paragon Cloud, and by end users to have an overview of their accounts. It displays information and functions according to the role of the person logged in.

3.8.1 ACCESSING THE MANAGEMENT INTERFACE

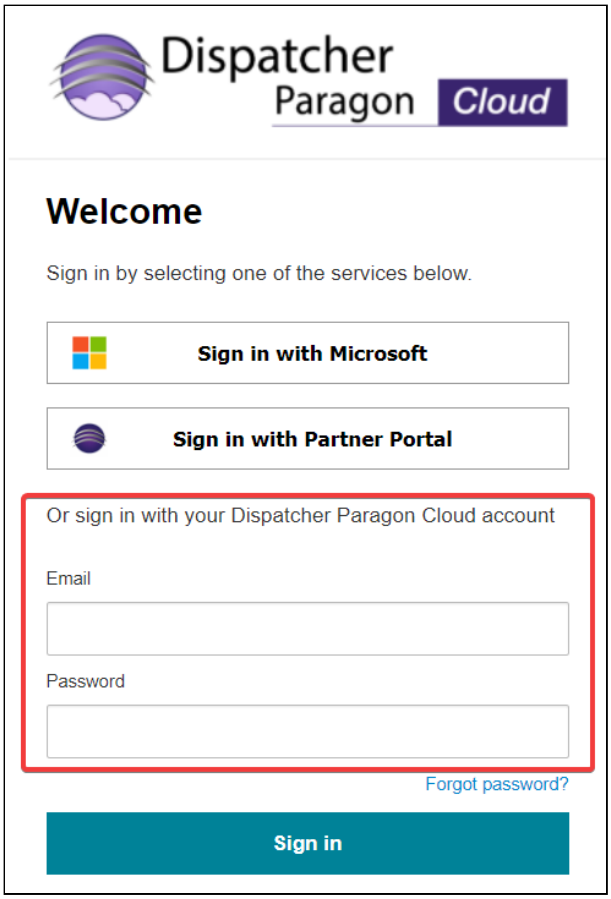
1. Open the link to Management interface provided by your administrator.

2. On the login page, click **Single sign-on**.

3. On the next page:

   a. If you are an Externally managed user, click **Sign in with Microsoft**. Enter your company credentials.

   b. If you are in Internally managed user, enter your Dispatcher Paragon Cloud credentials and click **Sign in**.

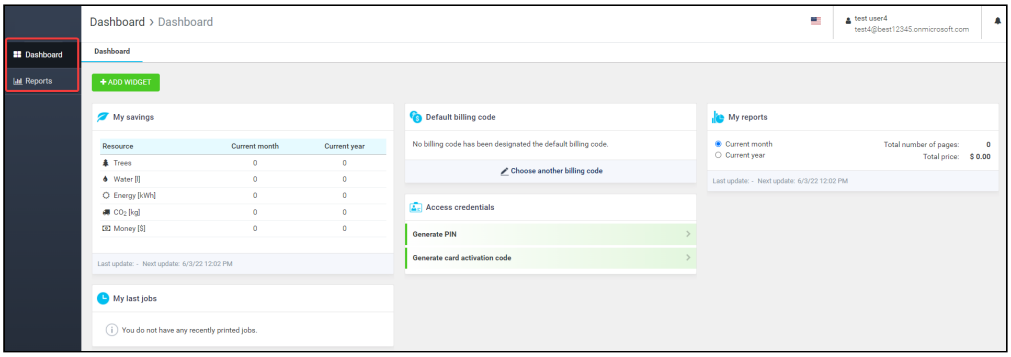


3.8.2 LOGGING OUT

To log out from the management interface, click your username in the top-right corner and then click **Log out**.

3.8.3 USING THE MANAGEMENT INTERFACE

After logging in, you have two tabs available in the navigation menu – **Dashboard** and **Reports**.



On the dashboard, you can see the following widgets by default:

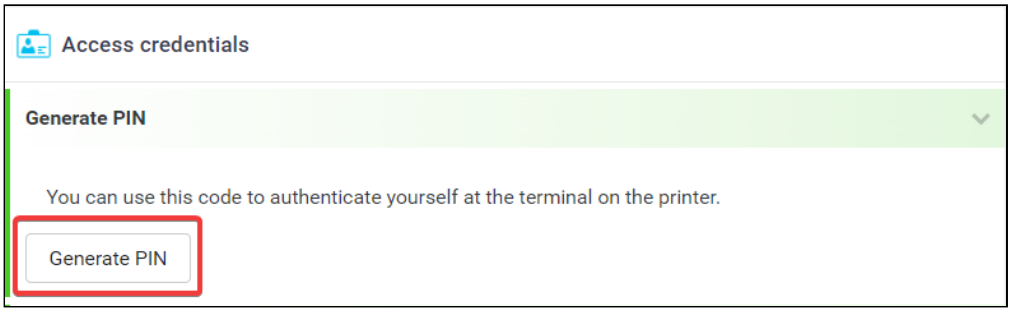
- My savings
- My last jobs
- Default billing code
- Access credentials
  - New card activation code

    > ⚠ Do not use the card activation code from this page, or try to generate a new one. Only codes from the Card activation code provider page (CACP) will work.
  - Generate PIN
- My reports

Generating a PIN

1. On the dashboard, click **Generate PIN**.

2. Click **Generate PIN** again.



3. Confirm your action.
4. You will see your new PIN in a pop-up window.

3.9 COMMON PROBLEMS

3.9.1 EDGE PRINTING: UNABLE TO GENERATE AN IPP URI ON THE IPP GATEWAY BECAUSE THE EDGE DEVICE IS IN UNREACHABLE STATUS

Problem description: when you visit the IPP Gateway to generate your print queue for an edge device, it is in unreachable status.

Possible root causes and solutions:

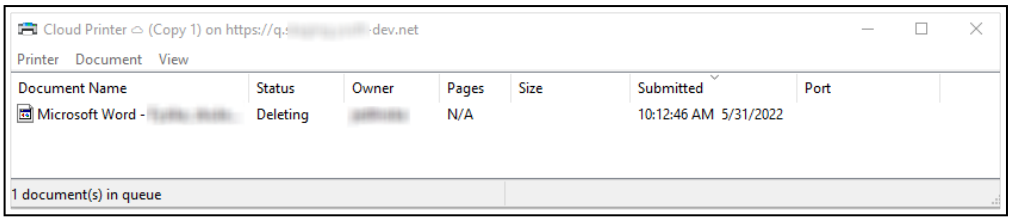
- Your workstation does not have the security certificates necessary to establish trust between your workstation and the edge device. These certificates must be distributed to the end users by the administrator. Solution: contact your administrator.
- Your workstation does not have network visibility to the edge device. Solution: contact your administrator.

- The edge device is currently being reconfigured or renamed by the administrator. Solution: wait for 10 minutes and if the problem persists, contact your administrator.

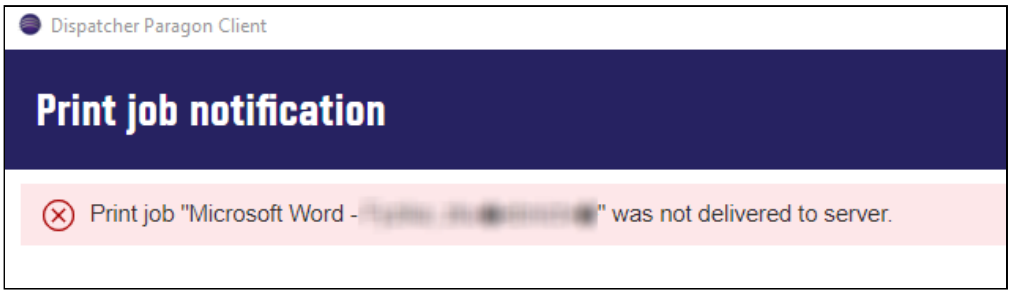
3.9.2 CANNOT PRINT A LARGE PRINT JOB

Problem description:

- Pure Cloud printing: you have sent a large print job to your print queue generated on the IPP Gateway, and the job cannot be printed. In Windows, the status of the print job is at first **Printing** and then **Deleting**.



- You have sent a large print job to your print queue deployed together with Dispatcher Paragon Client v3, and the job cannot be printed. You receive an error in Client v3 that the job was not delivered to the server.



Possible root causes and solutions:

Your print job took more than 5 minutes to parse. This is the time limit after which a print job is discarded because it cannot be accounted. Solution: contact your administrator.

4 ARCHITECTURE AND SOLUTION DESIGN

The Architecture and solution design documentation is primarily intended for solution architects. However, some of its content might be of interest also to Partner admins and Customer admins.

4.1 DOCUMENTATION CHANGELOG - RELEASE 2023.01.26

What's new	Where
No changes.	

4.2 GENERAL INFORMATION

4.2.1 TERMS AND DEFINITIONS

For terms that are not listed here, see General information.

Term	Definition
Cloud environment	All systems bound together as a working service (set of services). It includes both components dedicated to one customer and also shared components. Example: the Production (PROD) Dispatcher Paragon environment consists of three regions where each region provides one or more Cloud instances. The cloud provider is Microsoft Azure.

Term	Definition
Cloud region	Correlates with regions in Azure. Defines where the system is located and from where the service for customers is provided. Visible for partners when they order the service via the Dispatcher Paragon Cloud Portal and visible in the URL of various web apps/interfaces such as the Card Activation Code Provider page. Example: West Europe, East US.
Cloud instance	A group of subsystems providing a service to one customer. An example is Management EU1 with all of its site servers, but does not include the shared components (such as the Dispatcher Paragon Cloud Portal or the Service health dashboard).
Management Services	This is the brain of the solution. It provides, amongst other things, a web interface (Dispatcher Paragon Cloud management interface) used by administrators to manage their product instance centrally, and by end users to manage their accounts. The interface displays information and functions as per the role of the individual logged in.
Site Server	A server in Dispatcher Paragon Cloud dedicated to a customer.
Customer registration	A Partner's action at the Dispatcher Paragon Cloud Portal that results in the allocation of application and service infrastructure to a particular Customer, and invitation email for the customer admin to use the service.

Licensing

Term	Definition
Trial Period Enablement	An event of enabling the Dispatcher Paragon Cloud service for a registered customer for a limited time period (usually 30 days). All newly registered Customers start with the trial period enabled, unless the Partner has requested otherwise during customer registration.

Term	Definition
License Enablement	Provision of a subscription or term license based on a processed purchase order from the Partner. The license must be assigned to the newly created Customer or Customer in the trial period via the Dispatcher Paragon Cloud Portal. In some cases, the assignment is automatic – see *License Assignment*.For term services, the issue of an invoice occurs immediately upon processing of the Purchase order. For subscription services, the issue of an invoice occurs on the 20th day of the following calendar month from processing of the purchase order. In both cases invoicing occurs irrespective of assignment of a license to the customer.
Subscription License	A license that is valid until the Service Termination event, usually billed on a monthly basis.
Term License	A license that is pre-paid for a defined period of time (typically one year). Must be renewed on its License Anniversary Date.
License Anniversary Date	The moment a term license expires. All changes to the Term License (quantity or feature changes) must be calculated to align with the upcoming License Anniversary Date.
License Assignment	A Partner assigns an existing license (provided via License Enablement) to a registered Customer who is in the trial period. If the Trial Period license identifier matches with the License Enablement identifier (via the respective purchase order), the assignment happens automatically.
License Change	The addition or removal of licensed devices in the assigned license or the enablement of an additional service (functionality). The license change occurs automatically, based on the purchase order from the Partner.

Term	Definition
Service Termination	Termination of all services to a Customer. Based on an explicit trigger (order) for subscription licenses or after the anniversary date, if the license wasn't renewed. Automatically triggered after the trial period expires, if license assignment didn't occur.

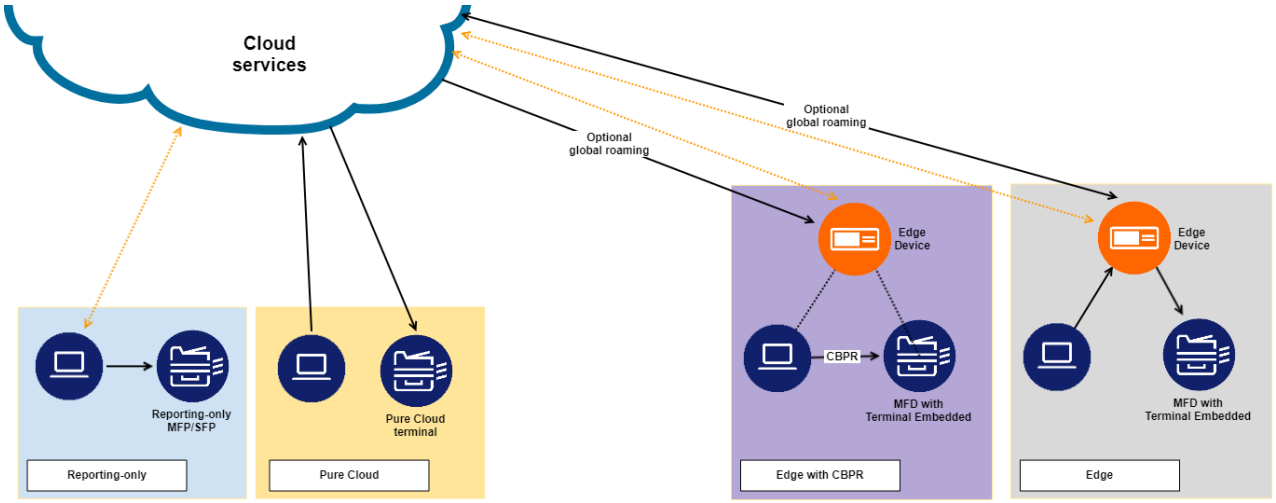
4.2.2 DISPATCHER PARAGON CLOUD

Dispatcher Paragon Cloud is an "out of the box" cloud print management and scan workflow solution for those who want a full-featured solution with little or no on-premise footprint in order to keep their IT investments to a minimum and free up their IT personnel to focus on business-critical tasks and projects. This multi-tenanted, or "shared infrastructure" service is designed to be simple for customers to install and configure. New customer accounts are faster to deploy and configure, giving access to their print and scan capabilities within minutes to hours, not weeks or months. Print devices can make a connection to the cloud directly from a cloud-enabled MFD – we call this Pure Cloud printing, where the MFD can connect directly to the cloud. Alternatively, customers can choose to use edge devices and connect their MFDs locally within their network.

Print devices can operate in a zero-trust network, enabling direct connection without any additional software or hardware.

4.2.3 ARCHITECTURE CONCEPTS

Customers can choose from the following ways of deploying Dispatcher Paragon Cloud in their locations, or they can combine them, as all of these scenarios can co-exist in one environment. See Hybrid architecture.



4.2.4 DEPLOYMENT SCENARIOS

Feature	Reporting only	Pure Cloud	Edge with CBPR	Edge
Data location: metadata are stored in the cloud (usage reports, audit trail)	✓	✓	✓	✓
Data location: print job data are stored in the cloud	✓	✓	✗	✓ opt-in, configurable
Data location: print job data are stored in the customer's LAN	✗	✗	✓	✓
Data location: all print jobs are at users' workstations (CBPR)	✗	✗	✓	✗
Does not require local HW (edge device)	✓	✓	✗	✗
Submitting print jobs: workstation Client (including unattended package deployment)	✓	✓	✓	✓
Submitting print jobs: self-service IPP gateway	✓	✓	✓	✓
MFD authentication methods	n/a	✓	✓	✓
Full Konica Minolta Terminal Embedded – native or browser	✓ offline accounting	✓ offline accounting	✓ device dependent accounting	✓ device dependent accounting

Feature	Reporting only	Pure Cloud	Edge with CBPR	Edge
Accounting – print	✓ offline accounting	✓ device dependent accoun ting	✓ device dependent accounting	✓ device dependent accounting
Accounting – copy, scan	✗	✓ device dependent accounting	✓ device dependent accounting	✓ device dependent accounting

Accounting methods

Accounting	Offline accounting	Device dependent accounting
Print - estimated	✓	✓
Print - actual	✗	✓
Copy, scan	✗	✓

⚠

- OMNI Bridge spooler limitation: A print job will not be accounted if a user sends it to an OMNI Bridge spooler and releases it at an MFD with the Cloud Terminal and the job analysis on the OMNI Bridge took more than 3 minutes. This applies both to Device dependent accounting and Offline accounting at the Cloud Terminal.The maximum document size depends on the complexity of the document and the current load on the OMNI Bridge. In general, the document size at which this problem may occur is in the range of thousands of pages.
  To make sure that a large print job is accounted, we recommend releasing it at an MFD with Embedded terminal where the accounting method is Device dependent accounting.
- Cloud spooler limitation: A print job will not be accepted and accounted if a user sends it to the cloud spooler and it fails to be parsed there because parsing took more than 5 minutes. This feature prevents print jobs that cannot be accounted from being printed.

4.2.5 USER IDENTITY MANAGEMENT

Managed users

Dispatcher Paragon Cloud is built on modern authentication methods (OAuth 2.0) and utilizes Single sign-on (SSO) provided by Identity Providers. SSO is a session and user authentication service that permits a user to use one set of login credentials to access multiple applications.

Two kinds of available identity providers:

- External – a provider already used by the customer, such as Microsoft Azure AD.
- Internal – a provider managed by the Dispatcher Paragon Cloud solution. From the customer's point of view, the users are self-registering in Dispatcher Paragon Cloud.

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

Externally Managed Users

Customers who want to use Dispatcher Paragon Cloud can use their existing 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). User credentials are safely confirmed by their external Identity Provider and never shared with the service provider (Dispatcher Paragon Cloud). The external Identity Provider provides Dispatcher Paragon Cloud only basic user details such as their first name, last name, and username.

Available external Identity Providers:

- Microsoft Azure AD
- others are planned to be added later

For more information, see the Configuration and Administration guide, chapter Externally managed users.

Internally managed users

See the Configuration and Administration guide, chapter Internally managed users.

Local users

These are standard users created and managed in Dispatcher Paragon Cloud management interface. We do not recommend their usage for anything else than testing purposes. See the Configuration and Administration guide, chapter Local users.

4.2.6 SECURITY

High security standards are one of the key features of Dispatcher Paragon Cloud. This section discusses the various security aspects that protect Customers, users, and their data.

Shared infrastructure is attractive to businesses because of its shared cost - lower, in general, compared to reserved instances. This is due, in part, to servers/infrastructure managed by the service provider and shared among multiple Customers. In addition, cloud-based applications (in this case, Dispatcher Paragon Cloud), provide services to multiple businesses, each one considered a separate *tenant*. In this multi-tenant scenario, each tenant has its own data identification, separation, and protection. Each Customer acts as a separate tenant where there is no access, communication, or data exchange between individual tenants. This approach ensures that Customer data cannot leak to other Customers.

Dispatcher Paragon Cloud obtains user details/identity from the external Identity Provider. Since these accounts may allow users to access sensitive content or resources, users must protect their credentials. Hence, some Customers require multi-factor authentication (MFA) to be enabled for all accounts. Dispatcher Paragon Cloud never asks users to enter their passwords. When a user needs to authenticate, they are redirected to the external Identity Provider (e.g. Microsoft) login page where they log in, and the login page passes the result to Dispatcher Paragon Cloud. This approach is known as Single Sign-On (SSO) – it allows users to enter their credentials at a trusted and well-known website.

4.2.7 SERVICE AVAILABILITY

Dispatcher Paragon Cloud is offered as a service with a **guaranteed uptime of 99.5%**. The MSP is fully responsible for backup, recovery, maintenance, and troubleshooting, in order to ensure high service quality. Partners and Customers can check the status of individual services online in a Service health dashboard available at https://status.<region>.dipa.cloud (depending on where their Dispatcher Paragon Cloud instance is running). The dashboard also gives information on upcoming updates and downtimes. For more information, see the Configuration and administration guide, chapter Dispatcher Paragon Cloud Service Health Dashboard.

4.2.8 UPDATES

Dispatcher Paragon Cloud is provided as a service. Therefore, MSP is responsible for its overall maintenance, including updates with new features or fixed defects. All updates occur with respect to the advertised availability and quality of the service. The update procedure also includes automated testing, aimed at detecting issues and preventing their recurrence.

4.2.9 REGIONS

Some Customers or regional regulations require sensitive data protection to meet certain criteria, such as the General Data Protection Regulation (GDPR) in the European Union. Dispatcher Paragon Cloud is GDPR compliant.

Customers can choose one of the three following data centers to ensure that their devices are as close to the server part as possible. Decreasing the distance has a positive impact on the responsiveness of the service. Dispatcher Paragon Cloud servers are available in:

- West Europe
- East US
- South UK

Reference: https://azure.microsoft.com/en-us/global-infrastructure/geographies/#geographies

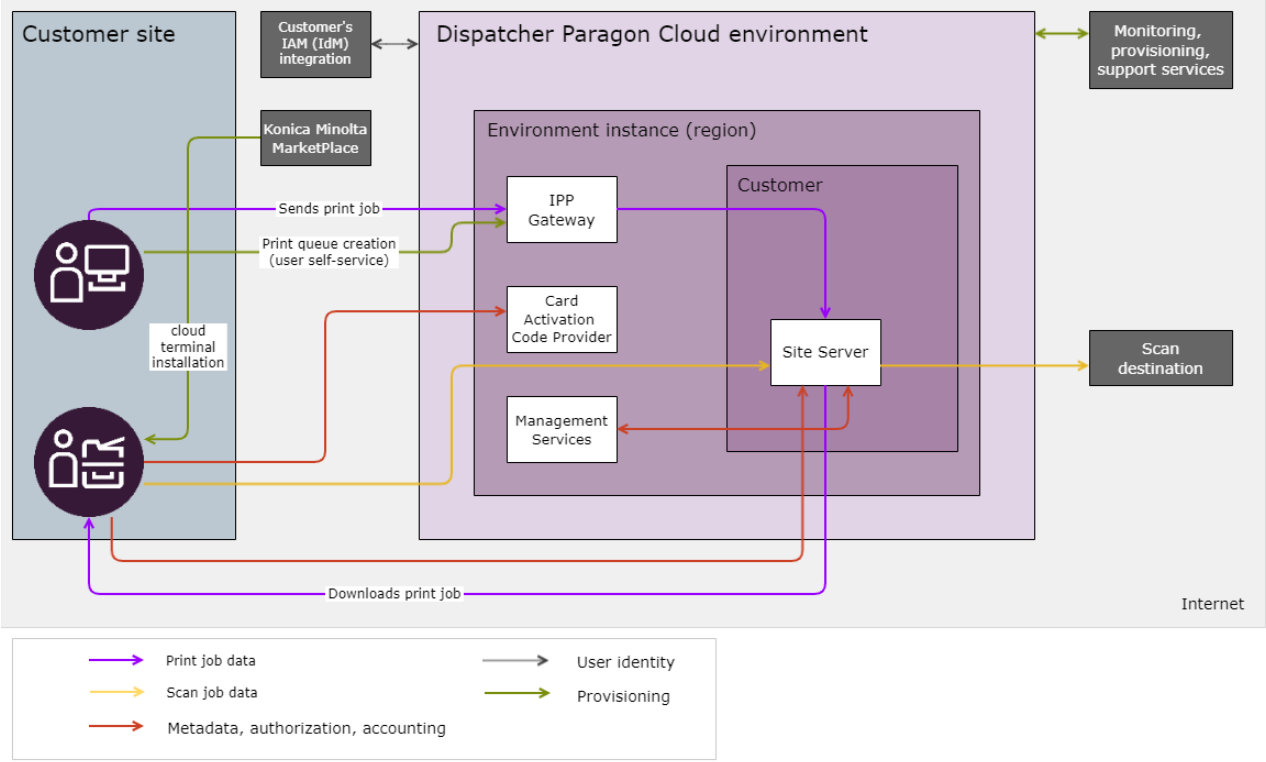
4.2.10 LICENSING

We offer three types of licenses:

- Demo – this type of license is solely for demo, testing or training purposes.
- Customer trial – a trial license that is valid for 30 days and can be converted into a commercial license. If not converted to a commercial license, at the end of the trial period, the license will expire and users will no longer be able to log into the service. 30 days after the license expiration date, the Customer and all associated print data are deleted.
- Commercial – a standard license.

4.3 PURE CLOUD ARCHITECTURE

4.3.1 ARCHITECTURE



4.3.2 SECURITY

Security is not only about authentication/authorization but also encryption. Users can interact with Dispatcher Paragon Cloud in different ways where all of them are protected using TLSv1.2 or TLSv1.3. The communication paths are as shown in the below table.

Purpose	Protocol
Account creation via an external Identity Provider	HTTPS
Interaction with MFDs	HTTPS
Print job release	HTTPS
Print job submission	IPPS

Purpose	Protocol
Scan job delivery to Dispatcher Paragon Cloud	WebDAV over HTTPS
Scan job delivery to email	SMTPS
System management	HTTPS

4.3.3 PRINT JOB SUBMISSION

Print job submission can be managed either by Client v3 or by a component called IPP Gateway over secured IPPS protocol.

Functionality	Client v3	IPP Gateway
Authenticated user (Azure AD required)	✅	✅
Authenticated user (Internally managed user)	✅	✅
Encrypted data transfer to spooler	✅	✅
Windows	✅	✅
Mac OS	✅	✅
Linux	❌	✅
Print Roaming	✅	✅
Direct print queues (release without authentication)	✅	❌

Functionality	Client v3	IPP Gateway
Emergency print	Only with edge devices	✗
User Roaming - based on DHCP	Only with edge devices	Only with edge devices
User Roaming - based on DNS	Only with edge devices	Only with edge devices
User Roaming - based on manual change of location	Only with edge devices	Only with edge devices
Deploy as MSI package (Windows)	✓	✗
Deploy as DMG package (Mac OS)	✓	✗
Billing codes selection at the workstation (before sending print job)	✗	✗
Client-based print roaming (CBPR)	✗	✗
Joblist view	✓	✗
Automated direct print queue deployment	✓	✗

Client v3

Spooling:

- All print jobs are transferred to the cloud spooler.
- Client spooling mode is not supported. Print jobs sent from Client v3 in client spooling mode will be displayed as unavailable at the Cloud Terminal. The only exception are reporting-only devices connected to the cloud spooler – in this case the user's Client v3 must be in the client spooling mode.

Deployment:

- Via Quick Print
- Via script

IPP Gateway over secure IPPS

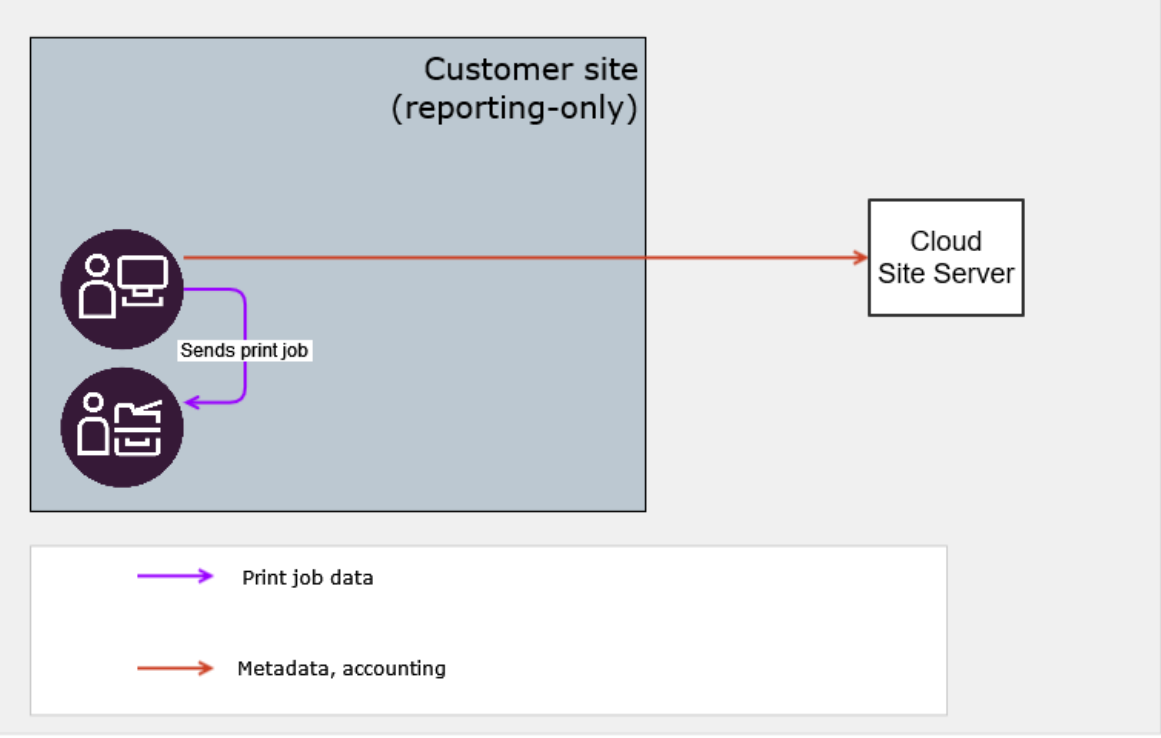
The main benefits of the IPP protocol are that it uses encryption and is supported natively on Windows, Mac, and Linux. Encryption is not only crucial when print jobs travel over the Internet, but oftentimes also in LAN environments. Or when adhering to Zero Trust concepts so that attackers are unable to read the content of network communication or to modify it. Furthermore, security certificates allow users to verify that the destination is the site server and not an attacker.

To increase security, queue deployment is fully self-service and users may only register their print queues there once they have authenticated. The IPP gateway provides a web interface where users can register their own IPP queues once their identity has been confirmed. Each printer has a unique URL that allows the IPP Gateway to identify users and their domains.

Reporting-only devices

At devices with this license type, the print jobs are immediately released. There is no authentication required at the MFD/SFD. Offline accounting is used, see Architecture and solution design, section *Accounting methods*.

Client v3 in client spooling mode is required at the workstation.



4.3.4 DEVICE MANAGEMENT

To be compatible with Dispatcher Paragon Cloud Terminal, Konica Minolta devices must have:

- Konica Minolta MarketPlace
- support for IWS technology

4.3.5 AUTHENTICATION AT THE MFD

At MFDs, the users must authenticate with their cards or with their PINs. Upon their first card authentication at the MFD, each user is asked to confirm their identity so that the card may be assigned permanently to their account. Users enter their credentials on a page they trust (e.g. Microsoft's Single Sign-on page) or on a device they trust (their smartphone/computer). For more details, see the End user guide, chapter Using an MFD.

Supported user authentication methods:

- Card assigned by Card Activation Code provider (CACP)
- PIN generated in the Management interface.

  > ⚠ PIN authentication requires the MFD to be authorized via device code flow. See the Configuration and administration guide, chapter Configuring Konica Minolta MFDs for Dispatcher Paragon Cloud Terminal, section *Device authorization grant*.

- Local users can use the username/password authentication method. See the Configuration and administration guide, chapter User management.

Method	Externally managed users	Internally managed users
Card	✓	✓
PIN	✓	✓
Card or PIN	✓	✓
Username and password	✗	✗

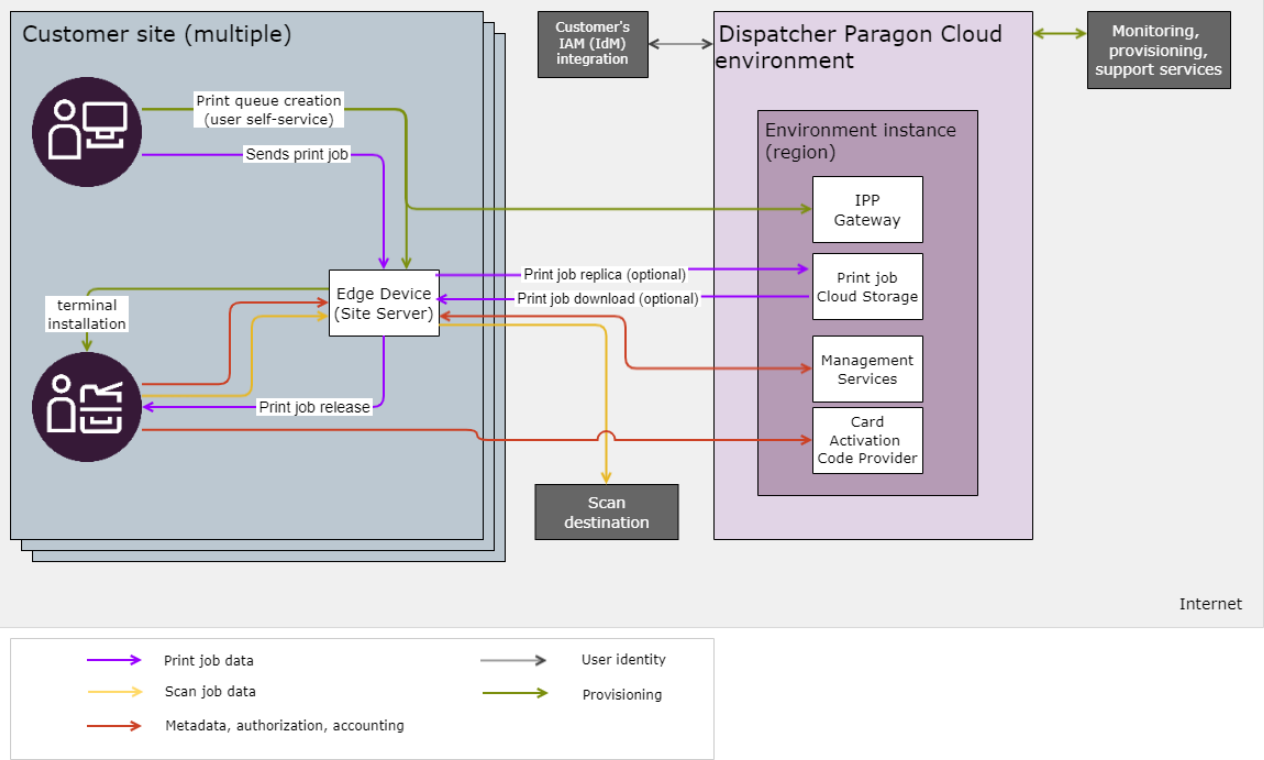
4.3.6 UPDATES

Konica Minolta MarketPlace is responsible for keeping all terminal applications up to date. Updates are pushed to devices automatically from MarketPlace's servers.

IWS tool with manual updates can be used in locations where Konica Minolta MarketPlace is not available.

4.4 EDGE ARCHITECTURE

4.4.1 ARCHITECTURE



4.4.2 TYPES OF EDGE DEVICES

You can choose between the following two options, or you can combine them per location:

- YSoft OMNI Bridge
- Virtual Appliance

Functionality	YSoft OMNI Bridge	Virtual Appliance
Level of security	✅ High	⚠️ Medium ⓘ For more details, see Security and privacy.
Capacity (using CBPR increases capacity, see section *Sizing* below)	15 devices for one OMNI Bridge	
Recovery	⚠️	✅ Self-service, customer's RTO.
Choice of hardware to run it	❌	✅
Customer self-service deployment	✅	✅

4.4.3 PRINT ROAMING

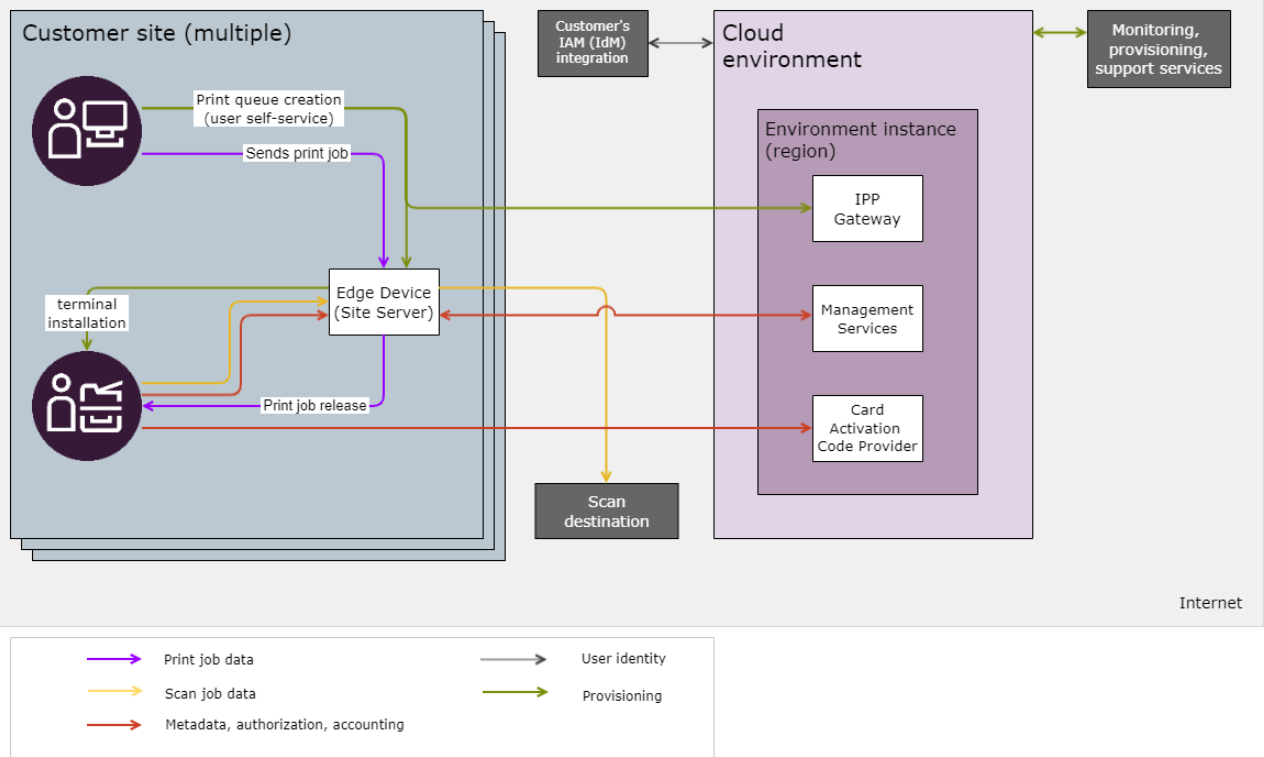
Functionality	Edge architecture with Local roaming	Edge architecture with Global roaming (default)
Print job locality: all print jobs remain local in the customer's LAN, i.e. no print jobs are stored on MSP's Cloud infrastructure.	✅	❌
Global print roaming - users can release their print jobs at any printer even without User Roaming	❌	✅

Functionality	Edge architecture with Local roaming	Edge architecture with Global roaming (default)
Client v3 usage	✅	⚠️ CBPR print jobs are not replicated

Local print roaming

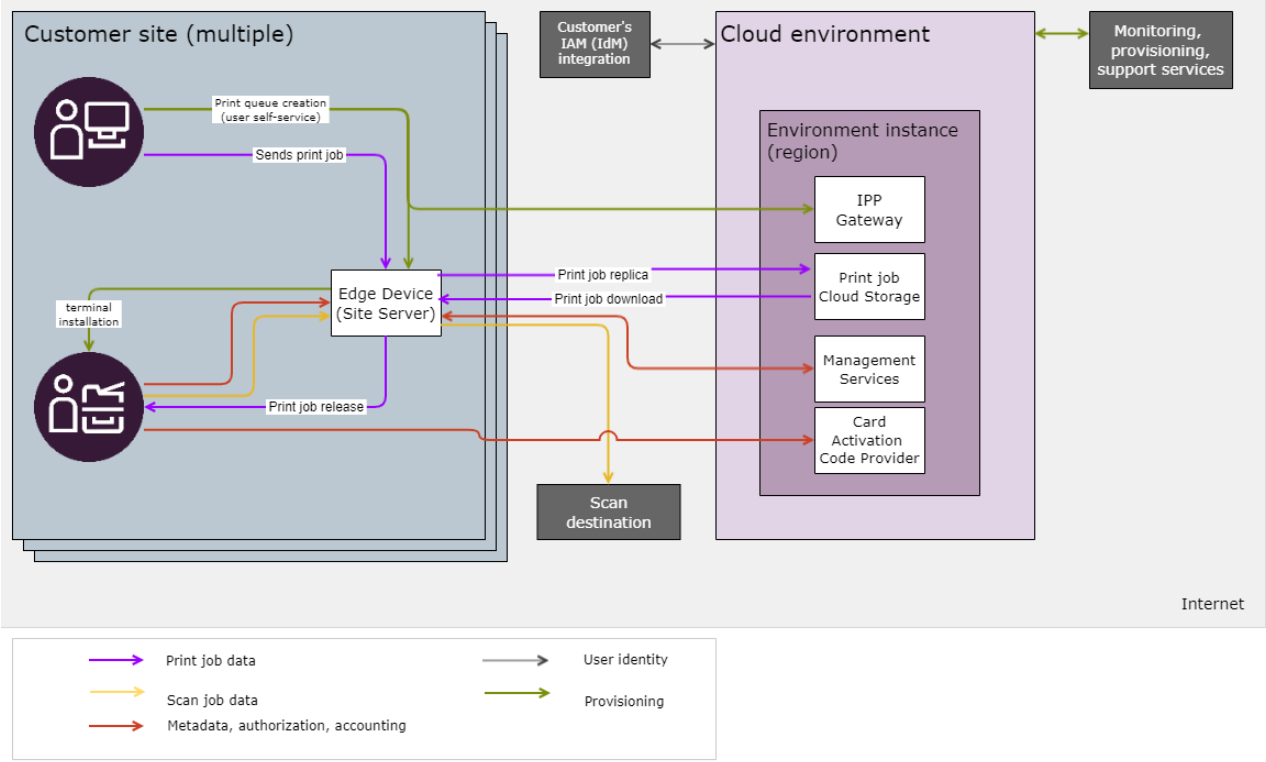
Edge devices enable document storage and processing to remain local, to ensure that document integrity and privacy are maintained. Only the print job's selected metadata are transferred to the cloud for management and reporting purposes via an encrypted channel. Document content remains secure because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

Local print roaming is disabled by default. For details on how customer admin can enable Local print roaming see the Configuration and administration guide, chapter Managing system settings. If Local print roaming is enabled, it applies to all of the customer's edge devices.



Global print roaming

When using client-spooling mode with Client v3, the print jobs are not replicated to the cloud.



4.4.4 PRINT JOB SUBMISSION

Functionality	Client v3	IPP Gateway
Authenticated user (Externally managed user)	✓	✓
Authenticated user (Internally managed user)	✓	✓
Encrypted data transfer to the spooler	✓	✓
Windows	✓	✓
Mac OS	✓	✓

Functionality	Client v3	IPP Gateway
Linux	✗	✓
Print Roaming	✓	✓
Direct print queues – release without authentication (for reporting-only devices)	✓	✗
Emergency print	✓	✗
User Roaming - based on manual location change by end user	✓	✗
Deploy as MSI package (Windows)	✓	✗
Deploy as DMG package (Mac OS)	✓	✗
Billing codes selection at the workstation (before sending print job)	✗	✗
Client-based print roaming (CBPR)	✓	✗
Joblist view at the client	✓	✗
Automated direct print queue deployment	✓	✗

Client v3

Edge device spooling or client spooling.

CBPR mode is available only when you are not using global roaming, see the *Print Roaming* section of this document.

Deployment

Quick Print

IPP Gateway over secure IPPS

The main benefits of the IPP protocol are that it uses encryption and is supported natively on Windows, Mac, and Linux. Encryption is not only crucial when print jobs travel over the Internet, but oftentimes also in LAN environments. Or when adhering Zero Trust concepts so that attackers are unable to read the content of network communication or modify it. Furthermore, security certificates allow users to verify that the destination is the edge device and not an attacker.

To increase security, queue deployment is fully self-service and users may only register their print queues there once they have authenticated. The IPP gateway provides a web interface where users can register their own IPP queues once their identity has been confirmed. Each printer has a unique URL that allows the IPP Gateway to identify users and their domains.

LPR

While LPR is fully available and supported for edge devices, customers might see issues with username matching. In many cases, LPR transfers the print jobs under username which does not match the users' UPN (user principal name). An administrator must edit user details in the Dispatcher Paragon Cloud Management interface and add an alias to the user in order to pair the print job to the correct owner.

Security Remark for print job reception over LPR

The consideration that administrators should keep in mind when activating the LPR interface:

- There is no authentication available to a user, therefore everyone is effectively anonymous.
- An attacker might be able to:
  - make it look like a job is coming from a different user.
  - trick a user into printing a modified document instead of their own.
  - access the user's data by impersonating the server.

4.4.5 PRINT JOB SUBMISSION FOR TRAVELING USERS (USER ROAMING)

For scenarios when customers have multiple locations where each is managed by one edge device, traveling users need to be considered. User Roaming is a mechanism that ensures that the print queue is always connected and communicating with the same edge device as the MFD where

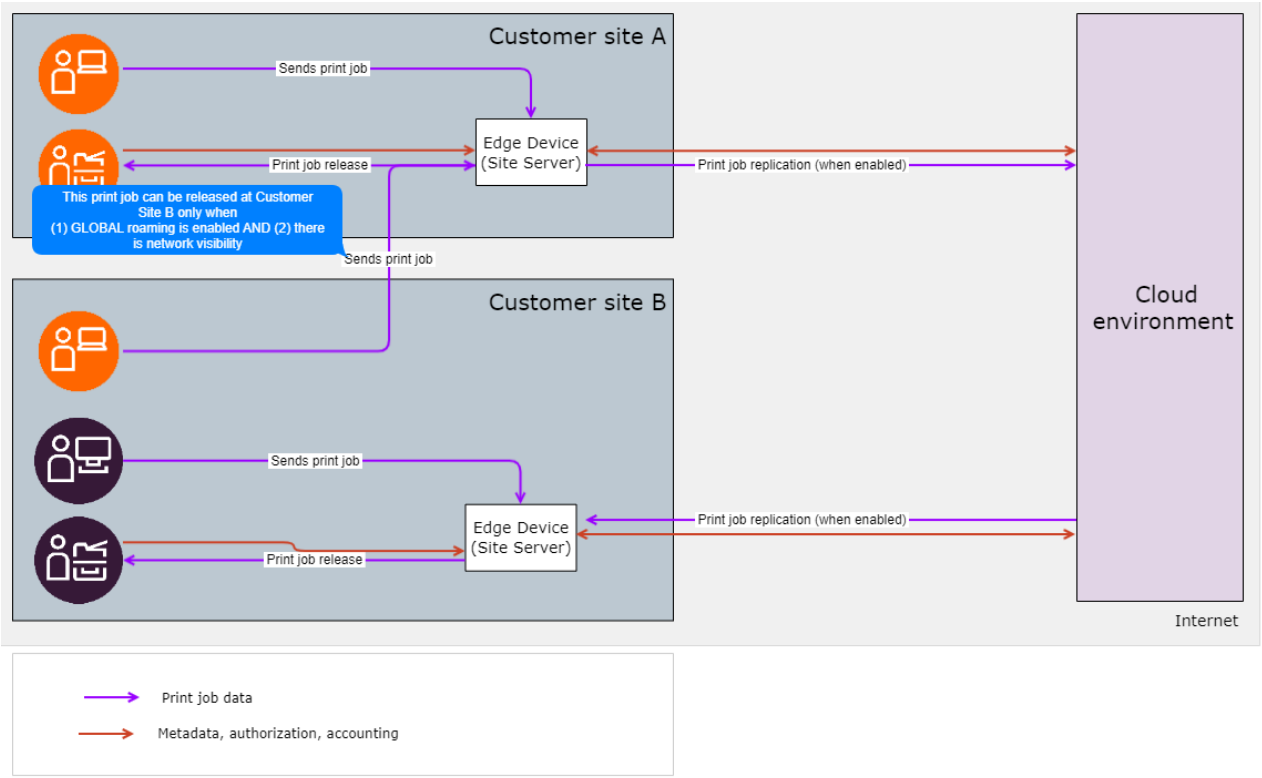
the print job will be released. That way users are able to release print jobs as expected and without delay.

All traveling users must have User Roaming enabled and configured.

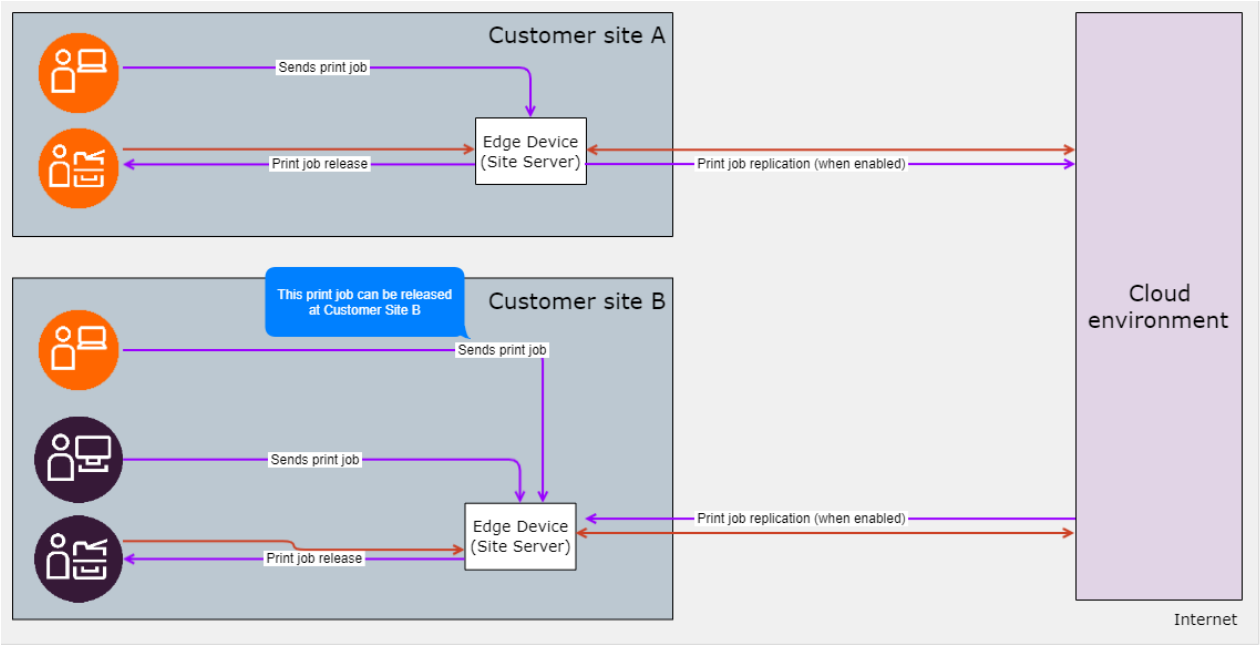
Consequences of incorrect/missing User Roaming:

- Users at home locations can print without issues.
- Users at any other than their home location can see their print jobs at the MFD but cannot release them.

The following diagram shows a case when users DO NOT use user roaming:



The following diagram displays a case when a traveling user sends the print job to the correct edge device because User Roaming is configured:



Client v3 with User roaming

Options to ensure users are connected to the correct spooler:

- DHCP 9 configuration to discover local edge device (or default to cloud service)
- Manual selection

IPP Gateway over secure IPPS

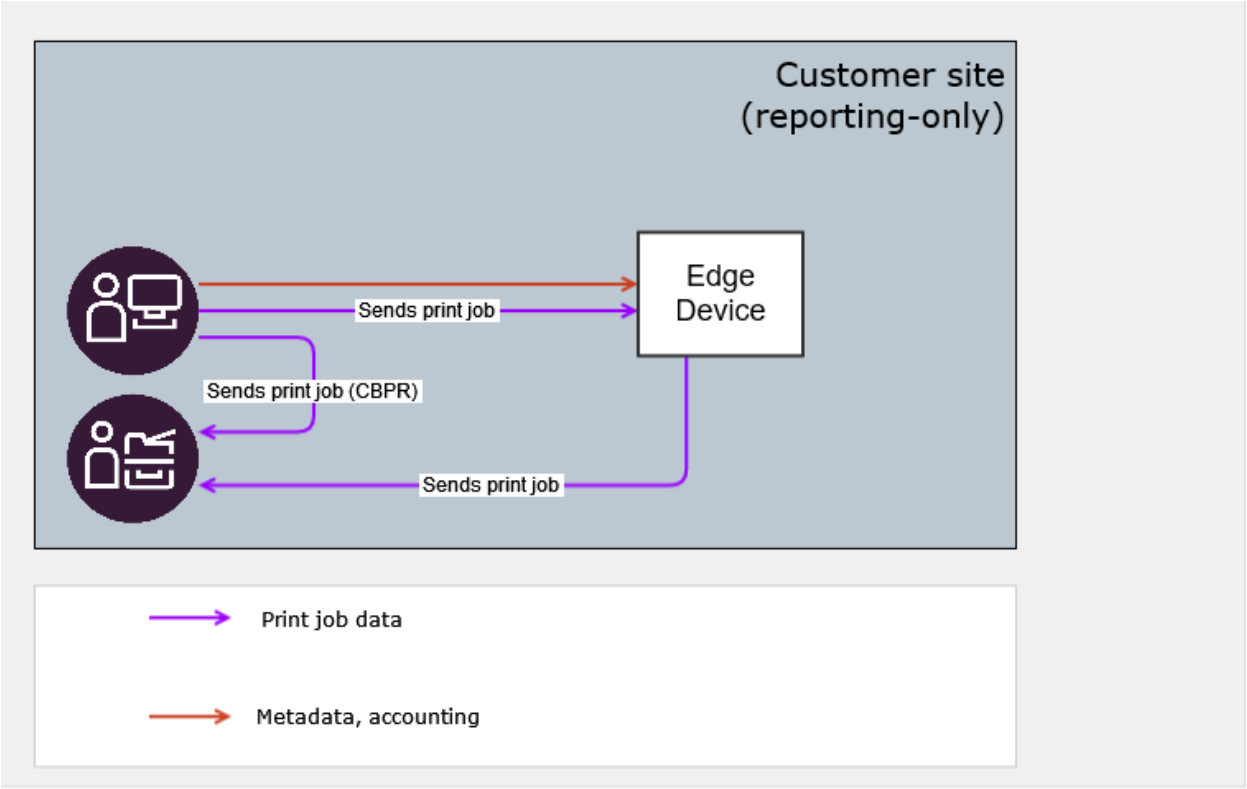
You can create more than one print queue to allow users to send the print job to the correct edge device.

Reporting-only devices

At devices with this license type, the print jobs are immediately released. There is no authentication required at the MFD/SFD. Offline accounting is used, see Architecture and solution design, section *Accounting methods*.

Client v3 is required at the workstation:

- Client spooling mode is supported (CBPR).
- Edge device spooling mode is supported



4.4.6 DEVICE MANAGEMENT

Edge devices support Konica Minolta Terminal Embedded (browser or native). For specific model compatibility, see the Hardware Compatibility List (HCL).

Authentication at the MFD

Supported authentication methods:

Method	Externally managed users	Internally managed users
Card	✅	✅
PIN	✅	✅
Card and PIN	✅	✅
Card or PIN	✅	✅

Method	Externally managed users	Internally managed users
Username and password	✗	✗

4.4.7 SIZING

- Number of edge devices per one customer is not limited.
- Number of MFDs per one edge device is limited to:
  - 15 with YSoft OMNI Bridge (expects peak performance of 15 print jobs/minute).
  - 15 with Virtual Appliance (expects peak performance of 15 print jobs/minute) with the following parameters:
    - AMD x64 architecture, Dual Core 2GHz (or faster) processor, 8GB of free RAM, 1Gbps network connection (LAN), 100GB of free disk space (after installation). Connection to storage with a throughput of at least 150MB/s and 300 IOPS.

      ⚠ Only AMD x64 architecture is supported.
  - Using CBPR increases the edge device capacity by 60%.
    - 25 with YSoft OMNI Bridge.
    - 25 with Virtual Appliance with the following parameters:
      - AMD x64 architecture, Dual Core 2GHz (or faster) processor, 8GB of free RAM, 1Gbps network connection (LAN), 100GB of free disk space (after installation). Connection to storage with a throughput of at least 150MB/s and 300 IOPS.

        ⚠ Only AMD x64 architecture is supported.

4.4.8 SECURITY

Security is not only about authentication/authorization but also encryption. Users can interact with Dispatcher Paragon Cloud in different ways, but all of them are protected using TLS v1.2 or TLS v1.3. See the communication paths in the following table:

Purpose	Protocol
Account creation via an external Identity Provider	HTTPS

Purpose	Protocol
Interaction with MFDs	HTTPS
Print job release	HTTPS
Print job submission using Client v3 in client spooling mode	LPR on localhost
Print job submission using Client v3	HTTPS
Print job submission using IPP Gateway	IPP over HTTPS
Scan job delivery to Dispatcher Paragon Cloud	WebDAV over HTTPS
Scan job delivery to email	SMTPS
System management	HTTPS

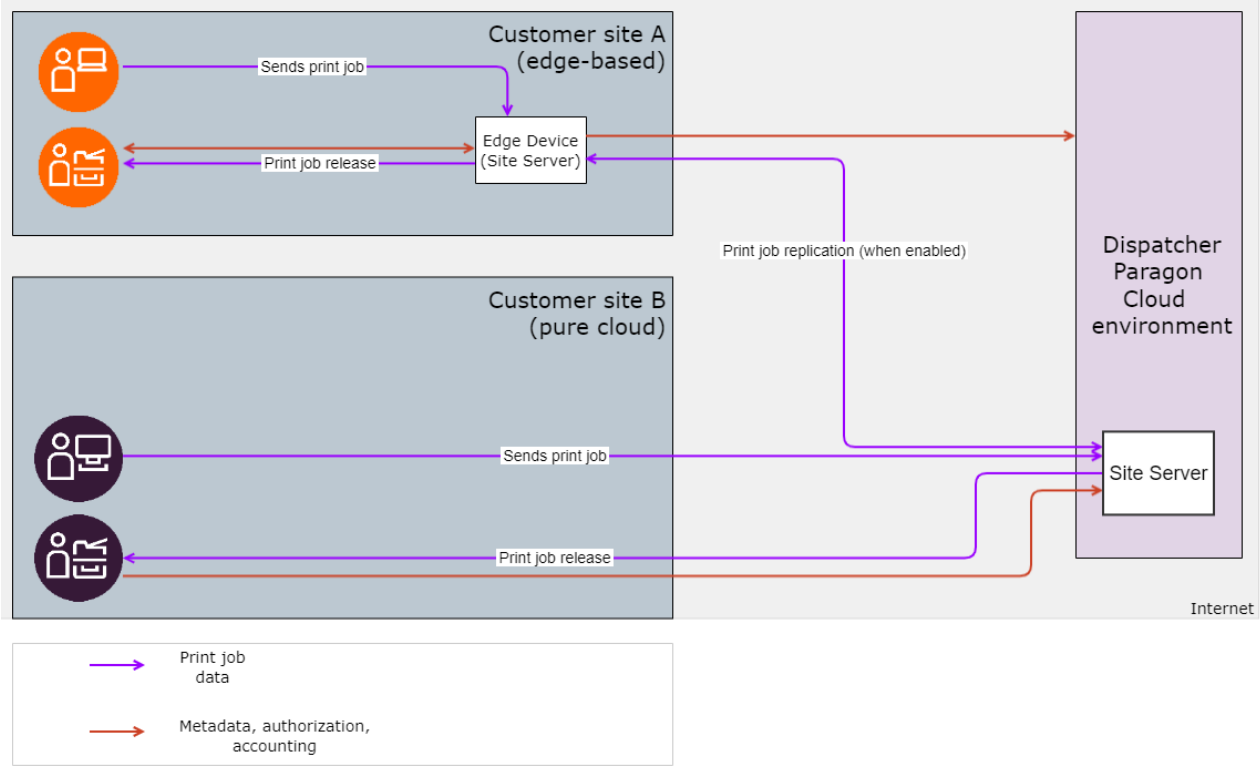
For more information, see Requirements.

YSoft OMNI Bridge security

See Security and privacy, section *Edge device security*.

4.5 HYBRID ARCHITECTURE

4.5.1 ARCHITECTURE



4.5.2 PRINT ROAMING

For more details, see Edge architecture.

We recommend you to use Global Print roaming.

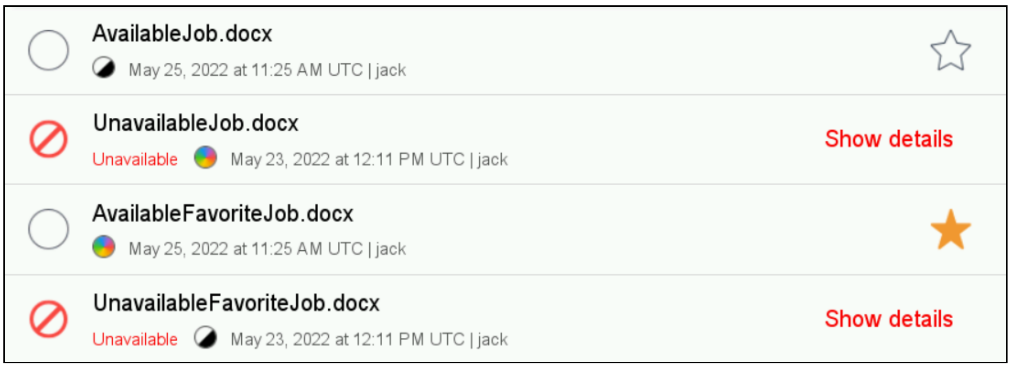
> ⚠ When using Global print roaming, be aware that print jobs spooled on user workstation (CBPR) cannot be printed at MFDs with the Cloud Terminal. The Cloud Terminal will display such print jobs as unavailable.

When using Local Print roaming, be aware that:

- Print jobs spooled on cloud site server are not visible and cannot be released at MFDs connected to any Edge device.
- Print jobs spooled on any Edge device are not visible and cannot be released at MFDs connected to the cloud site server (i.e MFDs with the Cloud Terminal).
- Print jobs spooled at user workstations (Client v3 in client spooling mode, connected to cloud site server) are visible at MFDs connected to the cloud site server, but their status is

"unavailable." Therefore, users cannot release them at such MFDs.

If a print job cannot be printed at an MFD with Cloud Terminal, it's marked as unavailable.



4.5.3 PRINT JOB SUBMISSION FOR TRAVELING USERS (USER ROAMING)

For more details, see Edge architecture.

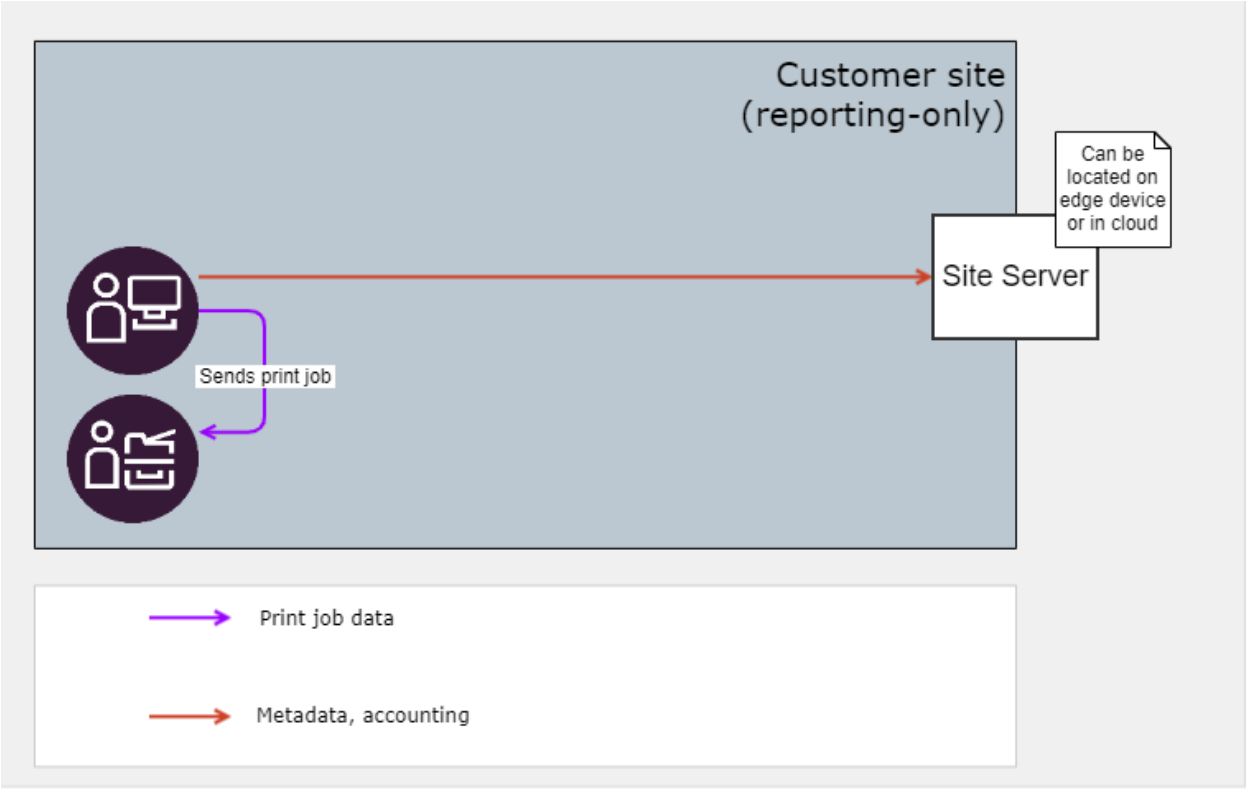
All traveling users must have User roaming enabled and configured. Client-spooled print jobs are not available at MFDs with Dispatcher Paragon Cloud Terminal.

4.5.4 REPORTING-ONLY DEVICES

You can set up a direct print queue to a reporting-only device, see the Configuration and administration guide, chapter Managing devices, section *Adding reporting-only devices*.

In that case, use Offline accounting, see Offline accounting.

Client v3 in client-spooling mode is required at the workstation in order to set up a direct queue to the reporting-only device.



4.6 SECURITY AND PRIVACY

4.6.1 ZERO TRUST

Zero trust is:

- a cybersecurity paradigm
- focused on resource protection
- a premise that trust is never granted implicitly but must be continually evaluated

Zero Trust has the following 5 pillars that MSP follows when implementing and maintaining the cloud service:

1. **Identity** – See the section *Identity providers* for users and *Edge device security* for devices.
2. **Device** – See the section *Edge device security.*
3. **Networks** – See the section *Data in transit*.
4. **Applications and Workflows** – See the section *Data in transit*, we do not really discuss internal cloud components.
5. **Data** – See the section *Data at rest* and *Operating the Cloud*.

4.6.2 IDENTITY PROVIDERS

On the Internet, user identity is one of the most valuable assets, and its security management is critical. Dispatcher Paragon Cloud allows customers to integrate their existing Identity Provider and allow their users to authenticate as they normally do – securely in their browser at their device, with their credentials (i.e. modern authentication).

Managed users

Dispatcher Paragon Cloud is built on modern authentication methods (OAuth 2.0) and utilizes Single sign-on (SSO) provided by Identity Providers. SSO is a session and user authentication service that permits a user to use one set of login credentials to access multiple applications.

There are two kinds of available Identity Providers:

- External – a provider already used by the customer, such as Microsoft Azure AD.
- Internal – a provider managed by the Dispatcher Paragon Cloud solution. From the customer's point of view, users self-register in Dispatcher Paragon Cloud.

For more details, see the *Configuration and administration guide*, chapter User management.

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

Externally managed users

Customers who want to use Dispatcher Paragon Cloud can use their existing 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). User credentials are safely confirmed by their external Identity Provider and never shared with the service provider (Dispatcher Paragon Cloud). The external Identity Provider provides Dispatcher Paragon Cloud only basic user details such as their first name, last name, and username.

Available external Identity Providers:

- Microsoft Azure AD
- others are planned to be added later

Security considerations:

- Dispatcher Paragon Cloud does not store passwords.
  - The exception is Internally managed users where user identity is maintained by Keycloak.
- Dispatcher Paragon Cloud only stores users' refresh tokens.

- When a user account is canceled/deleted/disabled on the Identity Provider side, Dispatcher Paragon Cloud does the same.

For more details, see the *Configuration and administration guide*, chapter Externally managed users.

Internally managed users

User accounts created and managed in the Dispatcher Paragon Cloud Portal. They use OpenID connect Integration with external Identity Providers via OpenID Connect, but these accounts are NOT from an external Identity Provider.

Internally managed user accounts are intended for customers who have not yet migrated their identity platform to the cloud or have concerns about granting Dispatcher Paragon Cloud permissions necessary for accessing their external Identity Provider platform.

These accounts can coexist with Externally managed users.

4.6.3 USER SECURITY

User Authentication and Identity

Users are required to authenticate themselves through an Identity Provider for the following services:

- The user self-service IPP Gateway allows users to create their print queue only after they have proved their identity (authenticated).
- Administrators may pre-deploy client packages (print queue, print driver, client SW). Users are asked to authenticate when printing for the first time.
- Dispatcher Paragon Cloud management interface.

All browser access to any portal is configured through HTTPS, using role-based access within the application, authenticated via OAUTH2 and OpenID Connect industry standards.

Azure AD-based two-factor authentication can be enabled when customers have this configured on their Azure AD. In Dispatcher Paragon Cloud it is then used every time that authentication is required:

- In all of the above cases above (IPP Gateway, client SW, Management interface).
- When accepting the invitation to the service and authorizing access to the service for the users.
- When registering a card at the MFD.

Authentication at the MFD

Access to print devices is secured in the following way:

- Externally managed users can only register their cards after they have authenticated through Azure AD SSO. Internally managed users must first register in Dispatcher Paragon Cloud and then authenticate to generate their card activation codes.
- Both Externally and Internally managed users can generate a PIN code after logging into the Management interface. PIN authentication can only be set up for MFDs that are authorized via a device code flow. See the Configuration and administration guide, chapter Configuring Konica Minolta MFDs for Dispatcher Paragon Cloud Terminal, section *Device authorization grant*.
- Two-factor authentication (card and PIN) managed by Dispatcher Paragon Cloud is available for MFDs with Terminal Embedded. Azure AD-based two-factor authentication is unavailable for authentication at the MFD.

Authorization

Once a user is correctly authenticated at the device, they may have access to print, copy, and scan features. Alternatively, a user's authentication credentials may authorize them to use only some functions (or even only some Automated Scan Workflows) and block others. In the printing context, securing sensitive or confidential documents is still a concern. Print Roaming, also known as pull printing or "follow me", solves this by holding a print job in a secure print queue until the user authenticates at their chosen print device (see options for Print Roaming in Edge architecture).

Users can also be assigned various permission levels, system access, or rules, based on roles replicated from Azure AD.

4.6.4 EDGE DEVICE SECURITY

YSoft OMNI Bridge security

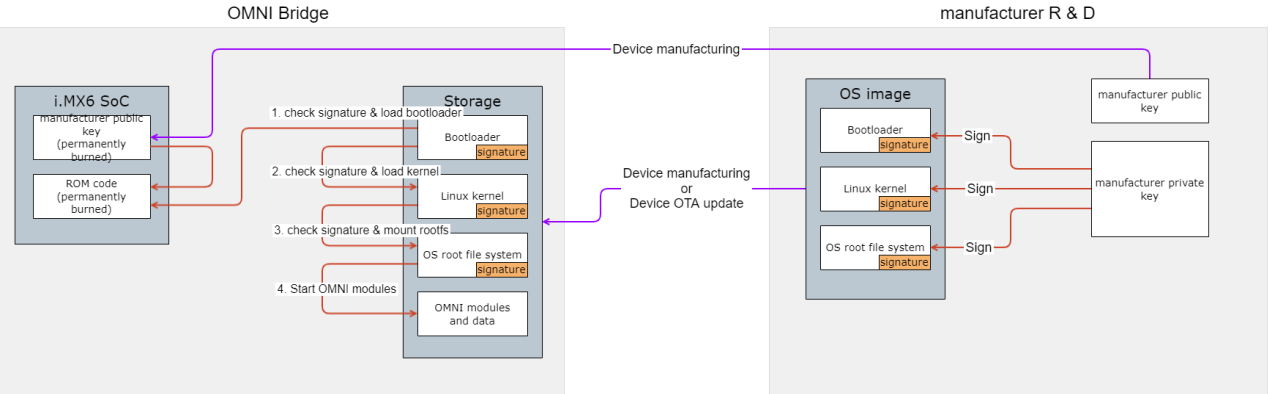
Operating system security

- 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 the 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, and the public key is permanently and immutably burned to the i.MX6 processor in the device.

When connecting to your OMNI Bridge via SSH, make sure that the security of your workstation is not compromised by any malware.

OMNI Bridge device boot process

- i.MX6 boot ROM loads and authenticates a bootloader image.
- Bootloader loads and authenticates the 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 finishes.
- OMNI modules (applications) start.



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 separated environments.

OMNI Bridge application storage

- Customer data: only print jobs and their metadata are stored in the OMNI Bridge. See the *Data locality* and the d *Data at rest* sections of this document.

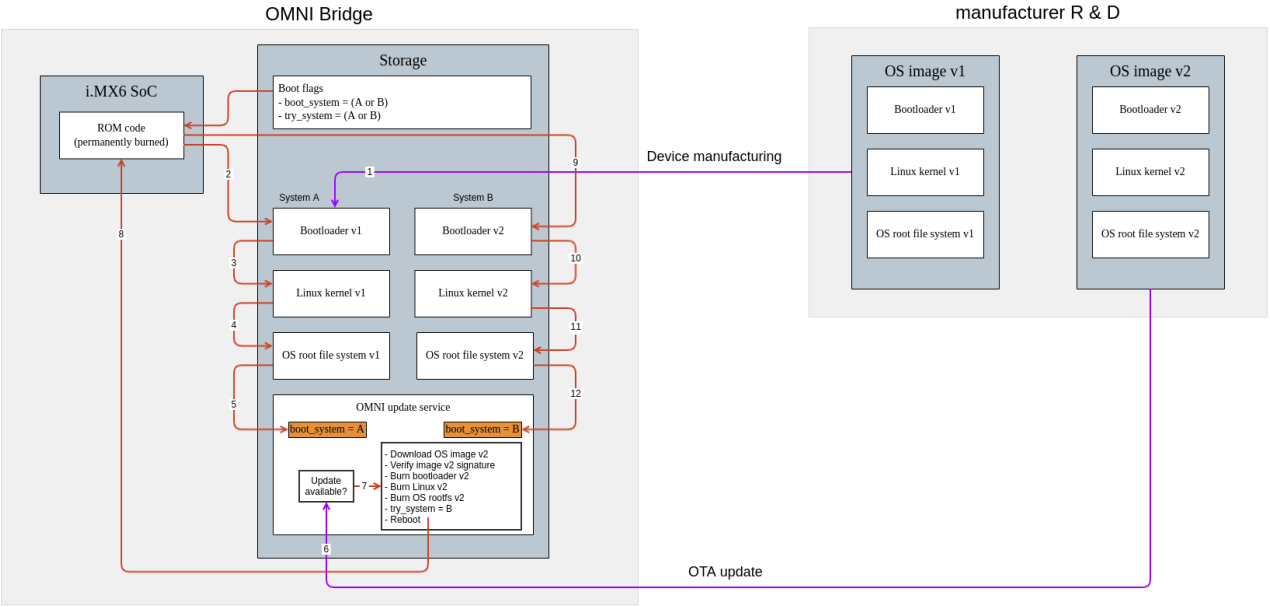
  > Both released and unreleased print jobs are automatically deleted from the OMNI Bridge after 24 hours. Favorite print jobs are never deleted.

- Only authorized modules may access the application (customer) data. There is no kind of admin account with rights to access the application data. However, the storage itself is not encrypted on HW level for performance reasons. The OMNI Bridge uses the i.MX6 integrated CAAM to ensure the chain of trust from the boot level and as secure storage of

Azure enrolment certificates, but it's not used for application data encryption. Accessing the stored data would require disassembling the device and unsoldering the storage chip. Such operation cannot be done without specialized equipment and expert HW skills, and would likely result in destruction of the OMNI Bridge. To increase security even further, we recommend that the customers keep their OMNI Bridges in a physically secure area.

OS update process

- The operating system on the device can be safely and securely updated.
- The update mechanism uses the 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 can only be decrypted 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 the necessary API.
  - The main use case is the signing of intermediate certificates for the Azure world.

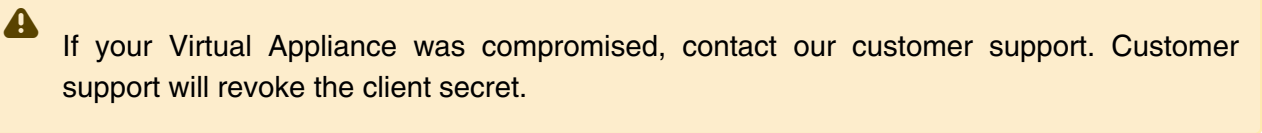
OMNI Bridge Factory reset process

- The factory reset process wipes all customer data present on the device and all applications (modules).

Virtual Appliance security

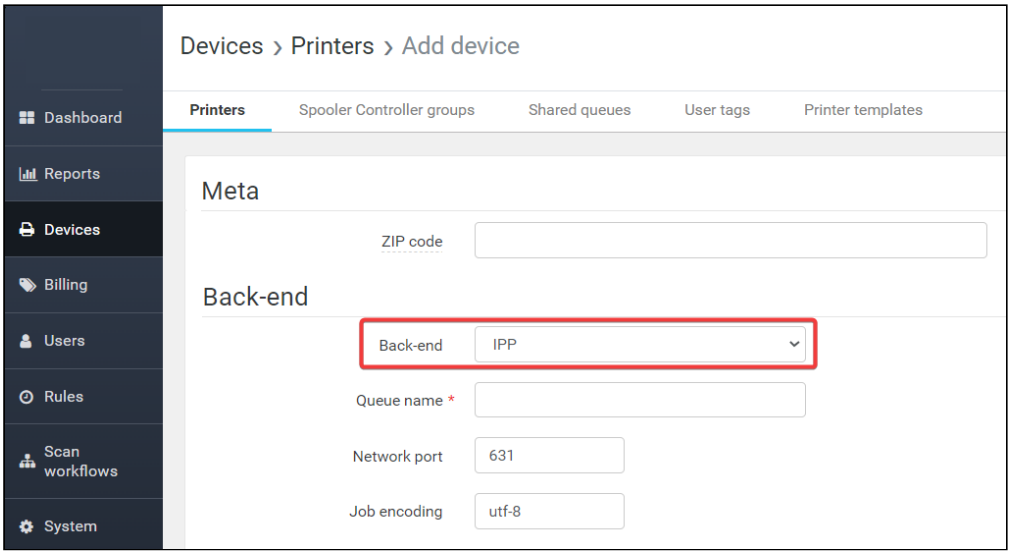
The customer must ensure that:

- The virtual machine in Hyper-V Manager is secured (no unauthorized access to the Virtual Appliance drive).
- The admin password for the virtual appliance is strong and prevent the password from leaking.



If your Virtual Appliance was compromised, contact our customer support. Customer support will revoke the client secret.

If your MFD supports IPP/IPPS, use this option when installing an Embedded terminal from the Management interface. If not, you can use **TCP/IP Raw**.



4.6.5 MFD AND SFD SECURITY

Dispatcher Paragon Cloud software embedded in the MFD is rigorously secured, using the same protocols and processes employed by customers who use it today as an on-premise or private cloud solution.

4.6.6 ENFORCING SECURE PRINT POLICIES

The Management interface provides administrators with access to an online dashboard protected by Azure AD single sign-on (or credentials for Internally managed users). The dashboard enables the administrator to set up user controls that meet the organization's print governance policies. Many of the user/workflow/document security features mentioned above are set by the administrator. Some of those controls can be implemented through the **Rule-based Engine**:

- Watermarks can include a unique job ID as a digital signature.
- Time restrictions to limit device access.
- Tags for flagging restricted jobs/devices.
- User role-based access: permitting or restricting features.

Another administrator tool for monitoring security is **Reporting**. All activity is tracked by recording the metadata associated with the activity. Reporting provides an audit trail for security purposes. Usernames and job titles can be hidden from administrators in reports. In that case, the metadata remain in the database, but cannot be displayed by administrators.

4.6.7 INFRASTRUCTURE SECURITY

The service uses software-defined infrastructures in Cloud and Edge to provide auto-scaling and advanced networking and security.

Cloud service provider

Now and in the future, Dispatcher Paragon Cloud services will only be hosted by world-class cloud service providers equipped to ensure both data security and business continuity. The first cloud service provider is Microsoft with their Microsoft Azure Cloud Platform. To learn more about Microsoft's Azure security features, visit https://azure.microsoft.com/en-us/overview/trusted-cloud/

Operated by a limited centralized group of MSP's specialists (based in the European Union).

Shared infrastructure

Dispatcher Paragon 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:

- Each tenant owns a unique security certificate associated with its metadata.
- Based on that unique certificate, the metadata is identified and directed to a unique area of the application database assigned to the respective tenant.
- Each tenant has a unique schema for its assigned area of the application's database.
- Processing of the tenant's data (print & scan job spooling / processing and storage and MFD/workstation endpoints are separated containers/workers assigned to the individual tenant only).

Sharing the underlying infrastructure brings one significant benefit – cost-sharing. Some components can be used by multiple customers while maintaining data separation/isolation and protection. As a result, the shared expense among multiple customers allows for a more cost-effective offering on the market.

4.6.8 DATA SECURITY AND PRIVACY

Data locality/regionality

Customers can decide on a region based on the available Azure data centers.

Customers can choose between Pure cloud printing architecture and Edge printing architecture, or they can combine them, resulting in a Hybrid architecture. See Pure Cloud architecture, Edge architecture, and Hybrid architecture.

Data	Pure Cloud locations	Edge-based locations with Local print roaming	Edge-based locations with Global print roaming
Print jobs	Cloud	Customer LAN (Edge device)	Customer LAN (Edge device) Cloud
Scan jobs (not stored, only processed)	Cloud	Cloud	Cloud

Data	Pure Cloud locations	Edge-based locations with Local print roaming	Edge-based locations with Global print roaming
Metadata Metadata includes print, copy, and scan activity on printers or groups of printers: • Job title • Origin • Timestamp • Number and type of pages • Thumbnail (first-page preview) • Print summary statistics • Cost centers • Billing codes • User identities (username, name, email, assigned roles) • Device and device metadata (names, locations - if provided, serial numbers, MFD types)	Cloud	Customer LAN (Edge device) Cloud	Cloud

Data in transit

Refer to the *Deployment guide*, chapter Requirements.

What	Transfer	Involves transfer over the Internet?	Description
Print job	Workstation to Cloud	Yes	The data is transferred over the Internet • When using IPP Gateway: IPPS (secured by HTTPS) • When using Client v3: HTTPS
Print job	Cloud to MFD	Yes	The data is transferred over the Internet via secured IPPS (secured by HTTPS), OAUTH2 authenticated, protocol to cloud, and downloaded by an authenticatedMFD.
Print job	Workstation to Edge Device	No	The data is transferred inside the customer's LAN • When using IPP Gateway: IPPS (secured by HTTPS) • When using Client v3: HTTPS • Support for legacy unsecured protocol LPR is also available
Print job	Edge Device to MFD	No	The data is transferred inside the customer's LAN using IPPS (secured by HTTPS). Support for legacy, unsecured protocols, such as LPR or TCP/IP RAW is also available.
Print job	Workstation to MFD (when using CBPR)	No	The data is transferred inside the customer's LAN using IPPS (secured by HTTPS). Support for legacy, unsecured protocols, such as LPR or TCP/IP RAW is also available.

What	Transfer	Involves transfer over the Internet?	Description
Print job	Edge Device to Cloud	Yes	Customer administrators can enable Global print roaming in the Management interface, which provides a better user experience when traveling to a different location. In this scenario, print jobs are synchronized over the Internet using HTTPS.
Print job	Cloud to Edge Device	Yes	With Global print roaming enabled in the Management interface, print jobs are synchronized to the Cloud using HTTPS. The data is transferred over the Internet.
Scan job	MFD to Edge device	No	The scan job data is transferred inside the customer's LAN via WebDAV over HTTP protocol (unencrypted).
Scan job	MFD to cloud	Yes	The scan job data is transferred over the Internet to the cloud services using device-authenticated (with the context of a specific user) WebDAV/S protocol.
Scan job	Scan data to users' mailbox	Yes	The scan job data is transferred over the Internet: emails with the scanned documents are delivered via 3rd party service Sendgrid. Reference: • https://sendgrid.com/ • https://sendgrid.com/wp-content/uploads/pdf/SendGrid-FAQ-8-18.pdf

What	Transfer	Involves transfer over the Internet?	Description
Metadata	Edge device to Cloud	Yes	The print job metadata is transferred over the Internet and used for reporting purposes. Metadata includes print, copy, and scan activity on printers or groups of printers, users or groups of users, cost centers, or billing codes. It does not include the content of a document. Two-way communication (metadata transfer) between the Edge device and the cloud application uses a mutually authenticated secured messaging protocol.
Metadata	MFD to Cloud (Pure Cloud terminal authentication)	Yes	Using HTTPS with mutual authentication (mTLS).
Metadata	MFD to Edge device (Terminal Embedded authentication)	No	Using HTTPS.

Data at rest

Topic	Description	Data concerned	Access restriction
Data at rest at the Edge Device - YSoft OMNI Bridge	The YSoft OMNI Bridge is a true Edge device appliance designed to reside safely at your business premises. It provides storage, authentication, and backup in case of Internet disruption. Data is stored on an mSATA (mini-SATA) solid-state drive and conforms to the interface specification developed by the Serial ATA (SATA) International Organization. Its size is ideal for the Edge device's small form factor and typical devices such as kiosks, digital signs, and even MFDs.	Print jobs	Due to the Edge device being located in the customer network (LAN), all print jobs remain safely within company network boundaries.
At at rest at the Edge Device - Virtual Appliance	Data is stored in virtual/ logical disk storage space in the virtual machine.	Print jobs	Due to Edge Device being located in the customer network (LAN), all print jobs remain safely within company network boundaries.

Topic	Description	Data concerned	Access restriction
Data at rest in the cloud	Data in the cloud are securely stored in separate storage repositories provided by means of the cloud provider’s platform. Storage repositories are defined with separate access credentials, accessible only by 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 into the cloud provider’s audit logs. For (alternative) shared infrastructure deployments, data are stored in separated “folders” under application shared credentials.	(region decided by the customer - based on the available Azure data centers) Print jobs Scan jobs User identification, email, card ID, device identities, print and scan job identities, names, and page number/type reports Printed and scanned document data in the process.	Technically audited access via the MS Azure web console by a highly limited centralized group of MSP's specialists (Europe-based), accessible in emergencies only.
User Identities & Tokens (OIDC Provider)	The user database is based on the industry-standard state-of-the-art OpenID connect provider platforms.	(region decided by the customer - based on the available Azure data centers) User identities and access tokens	A very limited number of highly trained MSP's (Europe-based) specialists responsible for application maintenance and management on an as-needed basis via secured web console in emergencies have administrator access to the databases. Access to the data is logged into the cloud provider’s audit logs. User tokens and credentials are not accessible.

Topic	Description	Data concerned	Access restriction
Cloud SQL Database (metadata)	Application metadata, configuration, job metadata, reporting, and generic user information are stored in the cloud provider's managed SQL database. The Database is separated per customer with customer-specific access credentials (Separated database schemas are used for shared infrastructure customers).	(region decided by the customer - based on the available Azure data centers) System configuration, User identification, email, card ID, device identities, print and scan job identities, titles, and page number/type reports.	A very limited number of highly trained MSP's (Europe-based) specialists responsible for application maintenance and management on an as-needed basis in emergencies via the MS Azure web console have administrator access to the databases. Access to the data is logged into the cloud provider's audit logs.
SQL Database and infrastructure backups	Data (SQL/IDM/ Infrastructure setup) backups and snapshots using standard MS Azure tools. Don't contain actual document content.	(region decided by the customer - based on the available Azure data centers) All processed metadata.	Inaccessible, can be restored into a functional infrastructure by the centralized infrastructure management team (see 1st point) via the MS Azure web console.

Topic	Description	Data concerned	Access restriction
Customer (tenant) specific metadata (users, devices, reporting, print job information, endpoint addresses …)	Role-based administrator access allows portal management of devices and system reports. This access can be assigned to the business administrator and/or maintained by a certified MSP partner reseller. Access to the customer application management web interface is limited to support personnel on an as-needed basis upon authorization by the customer during incident management sessions. For (alternative) shared infrastructure deployments, there is also a set of support accounts 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 into the cloud provider's audit logs.	(region decided by the customer - based on the available Azure data centers) System configuration, User identification, email, card ID, device identities, print and scan job identities, names, and page number/type reports	**End-user**: own print/scan job metadata (title, origin/IP/hostname, timestamp, number and type of pages, thumbnail first-page preview) **Customer (tenant) administrator**: all users print/scan list: metadata (title, origin, timestamp, number, and type of pages, thumbnail first-page preview). Print summary statistics. User identities (username, name, email, assigned roles). Device list and device metadata (names, locations - if provided, serial numbers, printer types). Rules and workflow definitions. **Partner specialist and/or MSP specialist**: tenant region, customer name, contact details, and edge device identities. **MSP Support**: see the *Cloud SQL Database* (meta-data) section of this table.

Topic	Description	Data concerned	Access restriction
Application / Edge device updates	Edge device application is managed by industry-standard tools and 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 transferred via encrypted and device authenticated HTTP/S communication.	(Europe-based Azure IoT hub with regional Azure container registries) Application binaries/ containers	Application components are stored in the cloud provider's secured artifact repository and deployed to cloud instances and edge devices using automated and secured state-of-the-art 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. Partner specialist and MSP regional specialist may push approved available updates to the respective cloud zone or edge device.

Topic	Description	Data concerned	Access restriction
Credentials, tokens, and cryptographic keys	Credentials, encryption, and digital signature keys, as well as other secrets, are stored in a secure enclave on Edge devices and use Microsoft recommended/ required techniques and tools in Microsoft Azure.	System, device, and application secrets (not user-specific)	Edge: no access Cloud infrastructure: Very limited number of highly trained MSP's (Europe-based) specialists responsible for application maintenance and management on an as-needed basis in emergencies have administrator access to the databases and vaults. Access to the data is logged into the cloud provider's audit logs.

Data separation

Dispatcher Paragon Cloud provides services to multiple businesses, each one considered a separate *tenant* in a multi-tenant scenario. Each tenant has its own resources, data separation, and protection:

- separate namespace
- separate database scheme
- JWT-based data access protection

4.6.9 FIREWALL RULES

The following external domains and their communication ports must be allowed in the customer's network firewall for edge devices to function correctly.

FQDN (* = wildcard)	Outbound TCP Ports	Used for
mcr.microsoft.com	443	Microsoft Container Registry
*.data.mcr.microsoft.com	443	Data endpoint providing content delivery

FQDN (* = wildcard)	Outbound TCP Ports	Used for
*.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, 443	IoT Hub access
*.docker.io	443	Docker Hub access (optional)
*.dipa.cloud	443	Dispatcher Paragon Cloud Services
*.ysoft.cloud	443	Dispatcher Paragon CodeFlow
*.google.com	UDP 123	NTP server (time{1-12}.google.com) or any chosen NTP server

4.6.10 OPERATING THE CLOUD

Access to customer data is limited to authorized MSP or MSP partner reseller employees who require it for their job, and only in specific cases. These employees' data access is logged. Secure portal communication between an administrator and the Management interface uses TLS/HTTPS, compatible with the version supported by the client. MSP access is necessary for system maintenance since we provide and are responsible for the cloud-hosted application. Only a subset of highly trained employees has administrative access to the entire system.

Logs

Application logs for troubleshooting are collected in the cloud provider's central log repository and are made available to support personnel on an as-needed basis. Logs do not expose any access/credentials related to document content information. Personally identifiable information (user names and emails, or endpoint IP addresses) may be included in the log files.