Rollout Guide

Contents

Rollout Guide

Rollout Guide

Overview

> **Note:** The screenshots may vary depending on the latest release.

Make sure that you have read through the "Getting Started" section before proceeding. This section describes the recommended process of rolling out Lexmark Cloud Fleet Management and Cloud Print Management. This knowledge helps you to start managing your fleet and printing with the full capabilities of Lexmark Cloud Services.

- "Manage your organization" group

  - Set how users authenticate with Lexmark Cloud Services and default user roles.
  - For channel partners, create customer (child) organizations.
- "Add and edit your users" group

  - Create user accounts and set system permissions.
- "Enroll your printers" group

  - Register printers with Lexmark Cloud Services and enable remote management.
  - Select the agents to use.
- "Deploy applications and configure your printers" group

  - Remotely configure printers with eSF applications and device settings using Cloud Fleet Management tools.
- "Customize your print environment" group

  > **Note:** Applicable only if Cloud Print Management is enabled for the organization.

  - Set up organizational policies, including print quotas and print delegates.
  - Select the print release clients to use.
- "Using notification policies" group

  - Send email alerts on supplies levels, such as when the toner level is at or below a certain value.
  - Send email alerts on printer communications, such as when a data refresh has not occurred, or a printer has not communicated for a certain interval.

Manage your organization

Why I need to manage an organization?

There are many ways to set up an organization. The setup depends on how your company operates and in the case of channel partners, how their customers operate their business. Consider these factors when managing an organization:

- What printer models will be used?

  ◦ Are they all Lexmark models?
  ◦ Will third-party printers be used?
- Will a firewall or proxy server be used?
- What enrollment agents do you plan to use?
- What functions will each user perform as an administrator and as a user?
- Will identity federation be used?
- What embedded applications will be used on the printers?
- Will users need to authenticate at the printer? If yes, how do they plan to authenticate?
- Will Cloud Print Management be used?

  ◦ What print management policies will need to be configured?
  ◦ How will the user submit print jobs?
  ◦ What submission clients will be used?

For channel partners, there are more factors to consider. If you plan to use child organizations, then the answer to each of these questions will help determine the user accounts required in the child organization, if any.

- Will users in the channel partner organization need access to child organizations?
- Who will perform the ongoing management of users in the child organization?
- Will Cloud Print Management be used in the child organization?

  ◦ Will the channel partner or someone from the end customer manage Cloud Print Management for the child organization?

Understanding the Account Management dashboard

The Account Management dashboard is the landing page of the Account Management portal. The Account Management portal lets you manage organizational settings, create and manage users, assign user roles, and create child organizations under channel partner organizations. What can be seen depends upon the roles of the user.

> **Note:** A user must have either the Organization Administrator or User Administrator role to access the Account Management portal.

The following is a sample Account Management dashboard for a user with the Organization Administrator or User Administrator role.
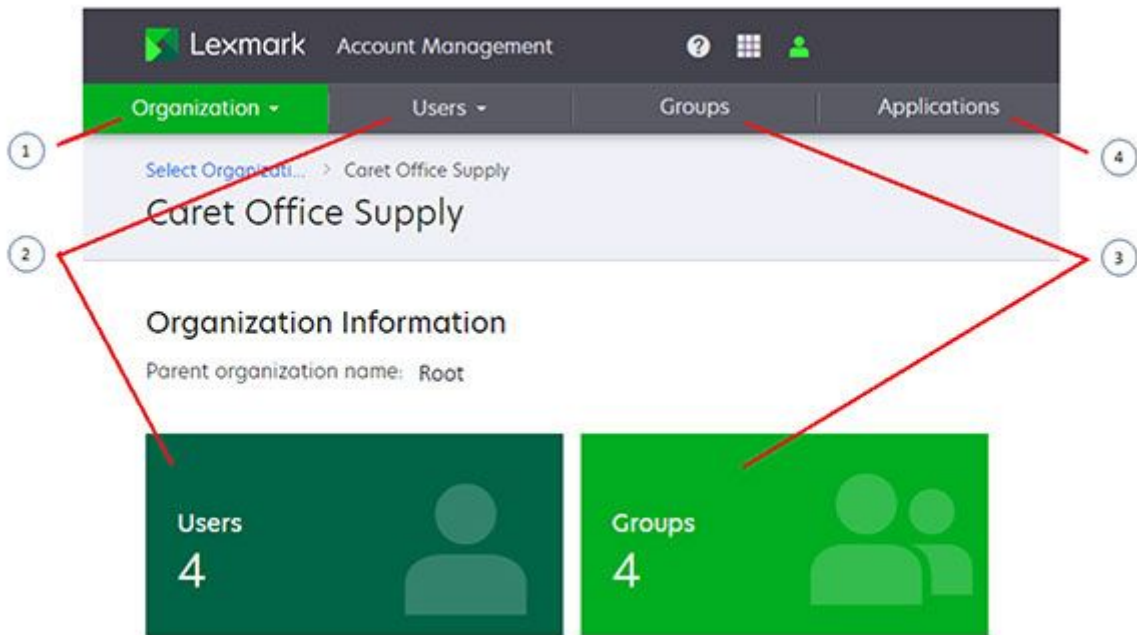
1. **Organization**
2. **Users**
3. **Groups**
4. **Applications**

The following is a sample Account Management dashboard for a user with the Organization Administrator or User Administrator role, and the Partner Administrator role.
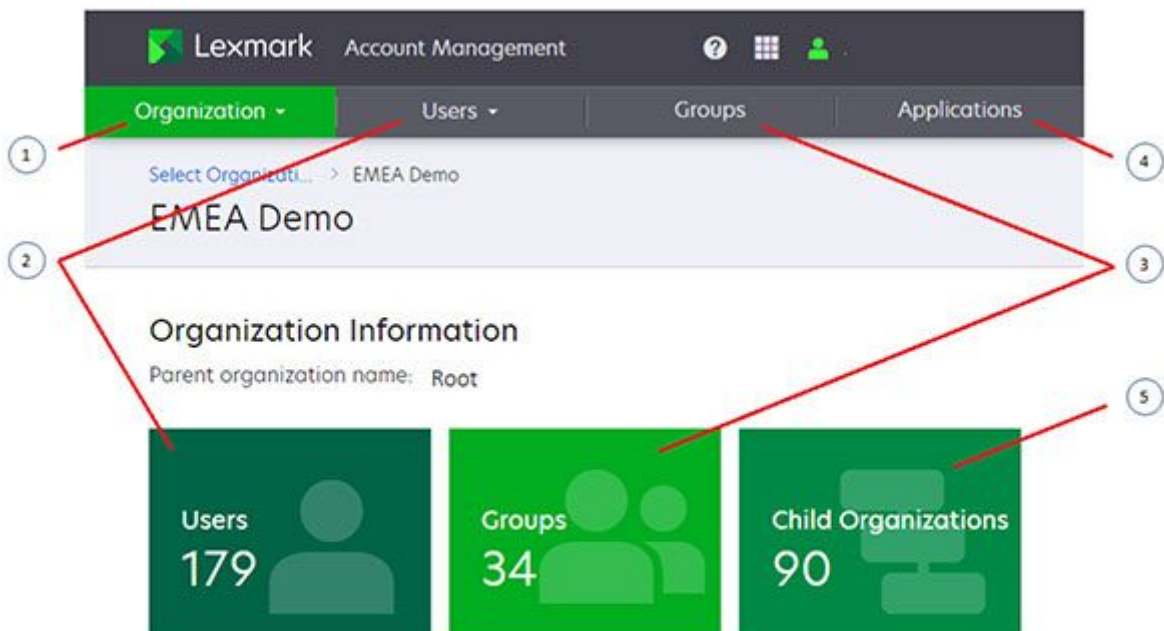
1. **Organization**
2. **Users**
3. **Groups**
4. **Applications**
5. **Child Organizations**

The Account Management dashboard provides access to the following:

1. The **Organization** menu, which provides links to the following:

   ∘ The Account Management dashboard
   ∘ The Organization Roles page—Lets you select a set of roles that are automatically assigned to all users in the organization
   ∘ The Authentication Provider page—The setup for federated identity management
   ∘ Child organizations—Lets you view child organizations defined under the partner organization.

   > **Note:** These organizations appear only to users who have the Partner Administrator role.

   ∘ Printer Login Configuration
2. The **Users** card and menu:

   ∘ Shows the list of user accounts in the organization
   ∘ Lets you create new user roles and modify existing ones
3. The **Groups** card and tab:

   ∘ Shows the list of user groups in the organization

   > **Note:** Groups provide a quick way to assign the same set of roles to several users.

4. The **Applications** tab:

   ∘ Shows the list of installed applications that provide authentication credentials for devices without user credentials, such as Fleet Management Printer Agent and Cloud Print Management
5. The **Child organizations** card:

   ∘ Shows the list of child organizations under an organization.

   > **Note:** This card appears only to users who have the Partner Administrator role.

Organization settings

Organization settings

The Organization menu provides quick access to various organizational settings and information.
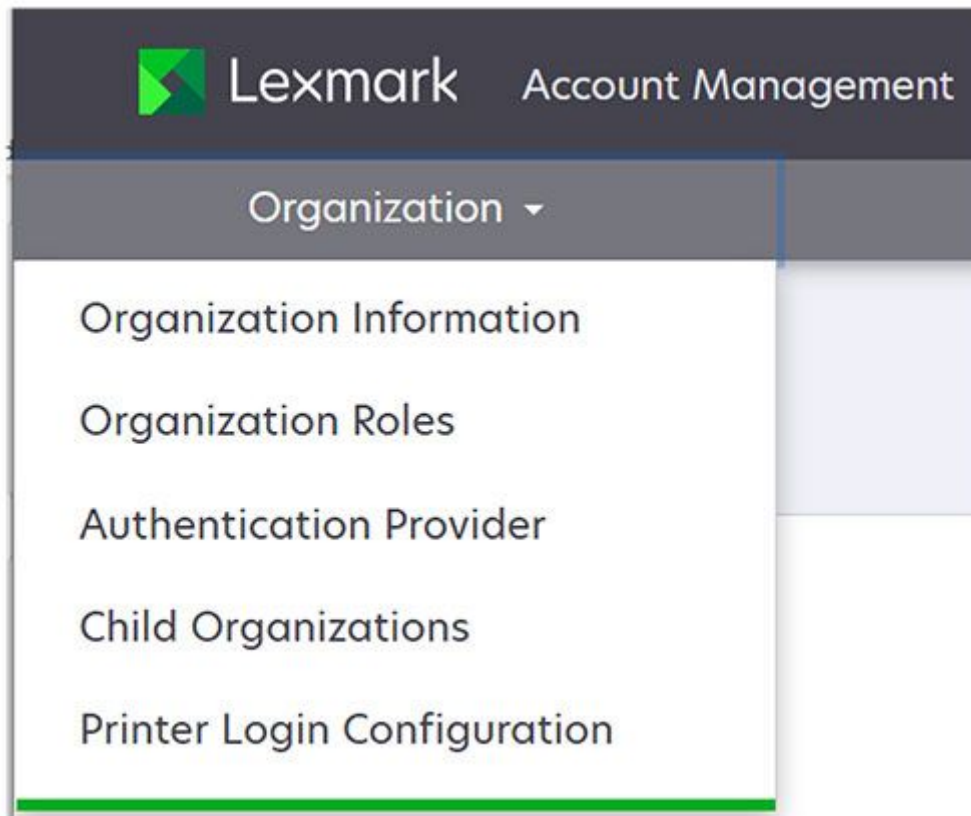
The Organization menu contains the following:

- Organization Information—A link to the Account Management dashboard, which provides links to the user and group management pages

    Note: For channel partners, there is also a link to the child organizations management page.

- Organization Roles—Lets you select a set of roles that are automatically assigned to all users in the organization
- Authentication Provider—The setup for federated identity management
- Child Organizations—Lets you view child organizations defined under the partner organization

    Note: This menu item appears only to channel partners.

- Printer Login Configuration—Defines the user authentication modes allowed at printers

    For more information, see "Managing printer logins" group in *Lexmark Cloud Services Administrator's Guide*.

Configuring user login at the printer

You must configure the authentication process for users who log in at the printer. If the user is accessing Lexmark's cloud-based functionality, such as Cloud Fleet Management or Cloud Print Management, then logging in to the printer is required.

1. From the Account Management web portal, click **Organization > Printer Login Configuration**.

The Organization Printer Login Configuration page allows you to select Single (Standard) and two-factor (Badge + PIN) authentication methods for user authentication.

2. You can either use Single (Standard) or two-factor (Badge + PIN) authentication methods for user authentication. Do either of the following:
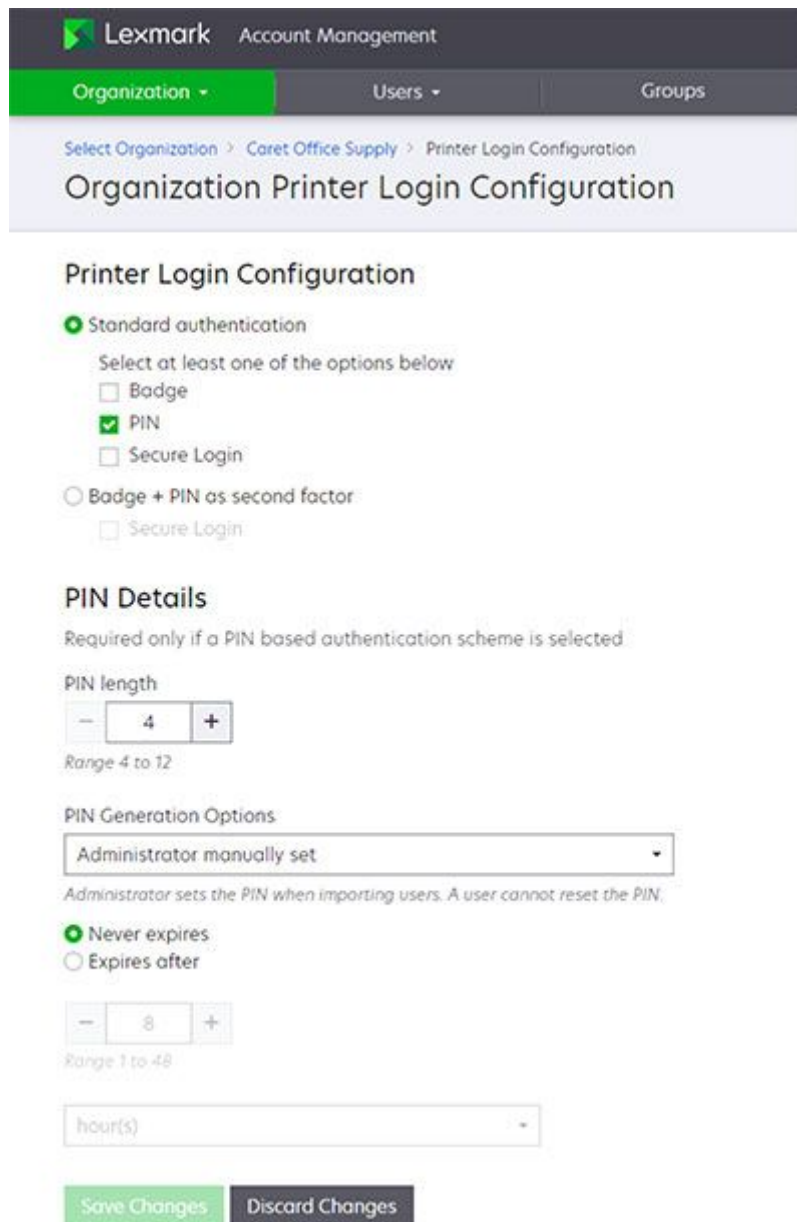
Standard authentication

One or more of the standard authentication methods can be enabled at the same time.

- ◦ **Badge**—Uses contactless card reader and user ID badges. Badges must be registered before they can be used. For more information, see "Managing badges" topic in *Lexmark Cloud Services Administrator's Guide*.
- ◦ **PIN**—Uses a 4-digit to 12-digit PIN. PINs can be set by the user, the administrator, or Lexmark Cloud Services. PINs can be set to never expire or to expire after 1 hour up to 180 days. For more information, see "Managing PINs" topic in *Lexmark Cloud Services Administrator's Guide*.
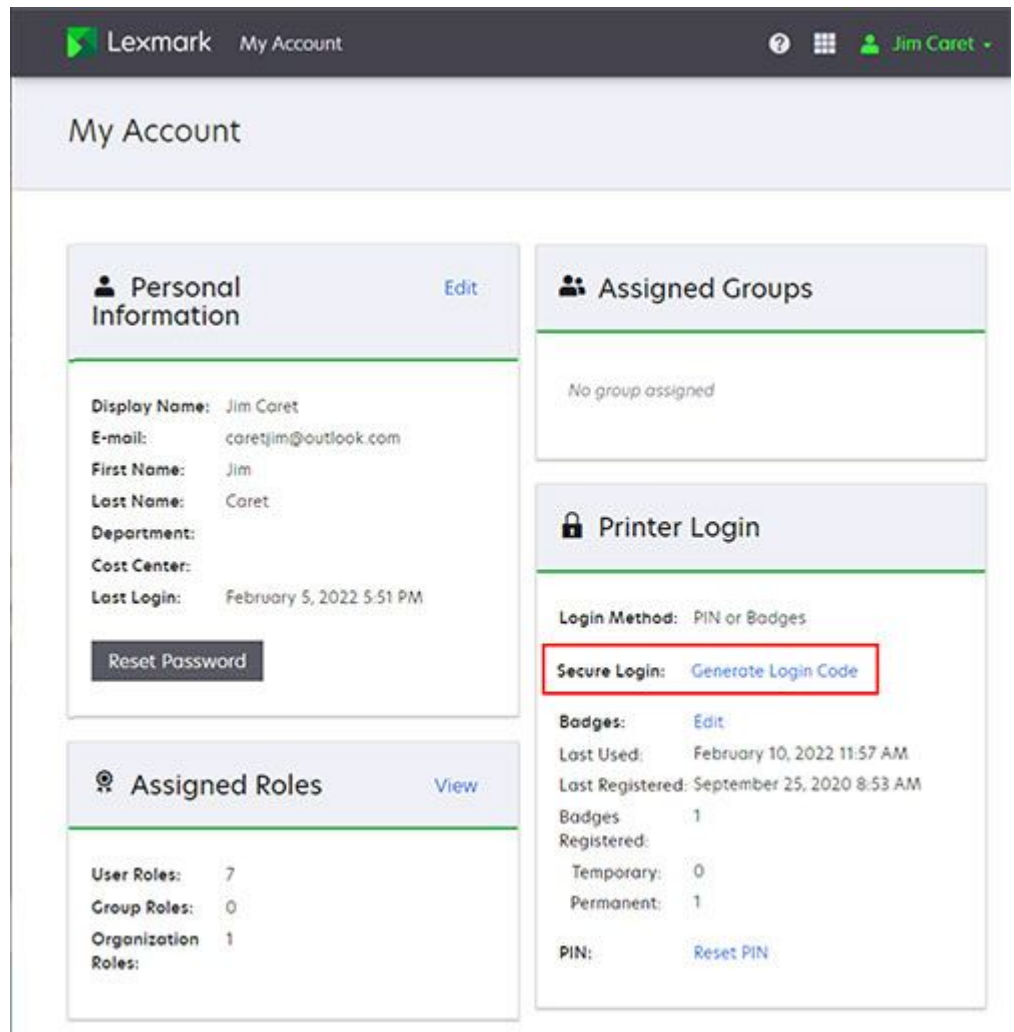
> **Note:** If an authentication provider has been configured, the PIN Generation option must be set to Administrator manually set and to Never expire.

- ◦ **Secure login**—Users must obtain a one-time PIN each time they authenticate at the printer. For more information, see "Configuring printer login" topic in *Lexmark Cloud Services Administrator's Guide*.

- The one-time PIN can be obtained from either of the following:

    - The My Account page, in the Printer Login section
    - The Lexmark Print application, by clicking the cloud icon.

> **Note:** If secure login is enabled for an organization, then the Secure
>
>
>
> Login icon appears on the printer control panel.

Badge + PIN as second factor

In this method users must use their badge and enter their PIN to authenticate. The badge and PIN stipulations as stated in the Standard Authentication section also apply.

- The Cloud Authentication eSF application polls the cloud for changes to the Printer Login Configuration settings every 15 minutes.
- The settings on the Printer Login Configuration page overwrite settings that are configured with the Cloud Authentication application installed in the printer.
- These settings are applied to all printers in the organization.

Understanding identity federation

Federation is the process of creating a trust relationship between a customer's identity provider (IDP) and an external service, such as Lexmark Cloud Services. The identity provider can be Microsoft Azure Active Directory (Azure AD), Google Identity, or any other Security Assertion Markup Language (SAML) 2.0-compliant identity management system. After this trust relationship is built, users can access Lexmark Cloud Services using the same credentials that they use for their other internal sites and services. The customer's identity provider manages all aspects of credential management, including password validation, complexity of requirements, expiration, and potential use of multifactor authentication. Additionally, the identity provider can support Single Sign-On (SSO), which reduces the number of times users are required to authenticate as they switch between services.

Notes

- Federation is supported by identity management services that use the SAML 2.0 standard.
- An organization can only be configured to federate with a single identity management provider.

To enable federation or to change the current federation configuration, do the following:

1. From the Account Management web portal, click **Organization > Authentication Provider**.
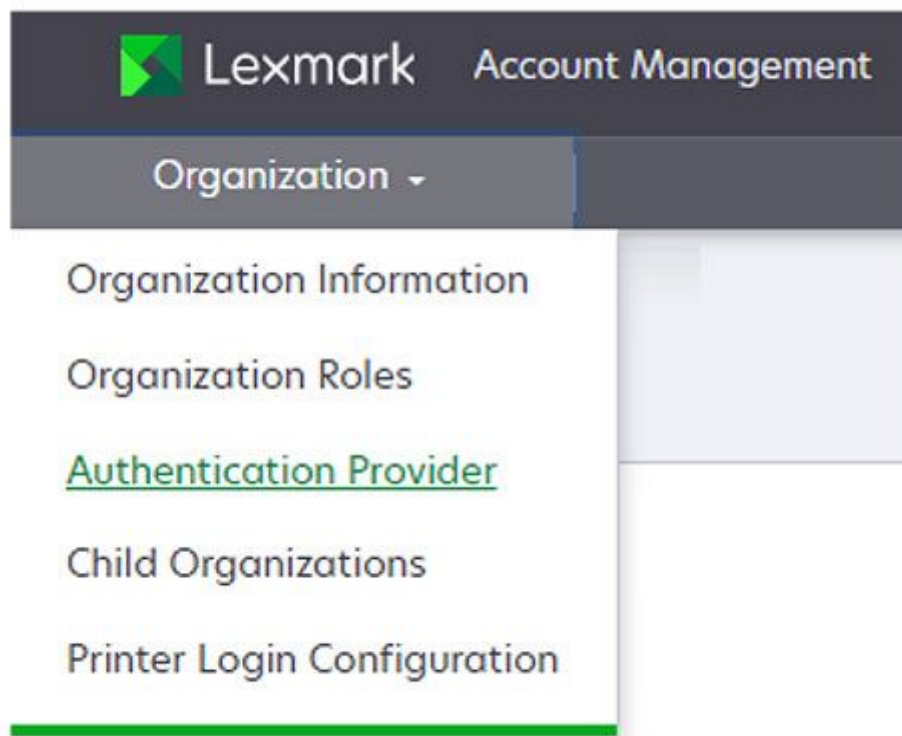
2. If federation is not enabled, then click **Configure an Authentication Provider**.

3. Enter the details in the Authentication Provider form.

Creating a child organization

Child organizations provide a means of grouping printers based on business needs. This grouping could be for customers of a channel partner or business units of an enterprise.

> **Note:** You must have the Partner Administrator role to create and manage child organizations. For more information, see "Partner administrator" group *Lexmark Cloud Services Administrator's Guide*.

Do I need to create a child organization?

There are two ways of organizing your customers' printers: a hierarchical structure or a flat structure. The structure you choose determines whether child organizations are needed.

> **Note:** We recommend using the hierarchical structure for organizing your customers' printers.

- **Hierarchical structure**—Uses a child organization for each of your customers. The printers of each customer are grouped in that customer's organization, separating printer information between customers. Also, a hierarchical structure lets you grant access to future Lexmark Cloud Services capabilities on a customer-by-customer basis.
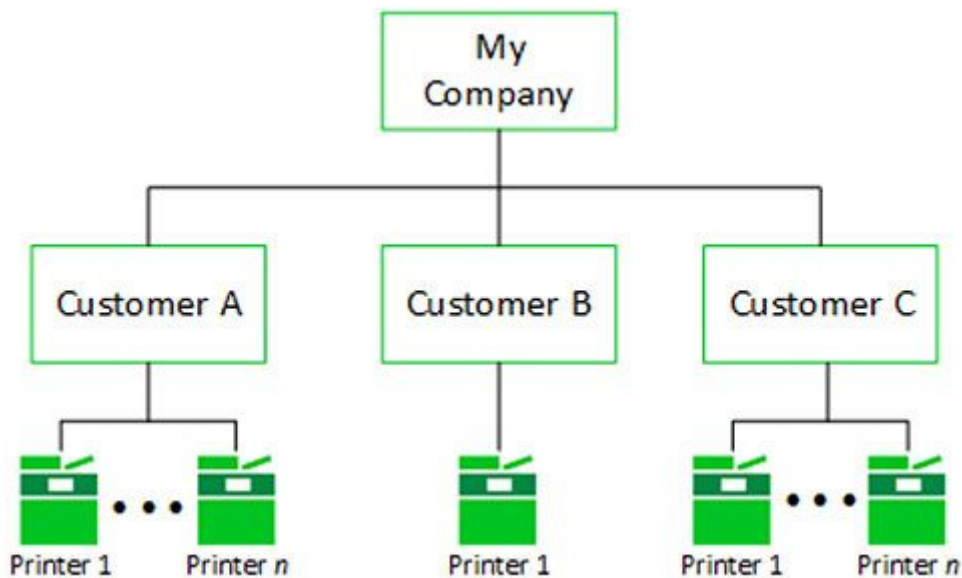
Flat structure—A flat structure places all printers from all customers in a single structure. Any future Lexmark Cloud Services capabilities added to one customer are available to all.
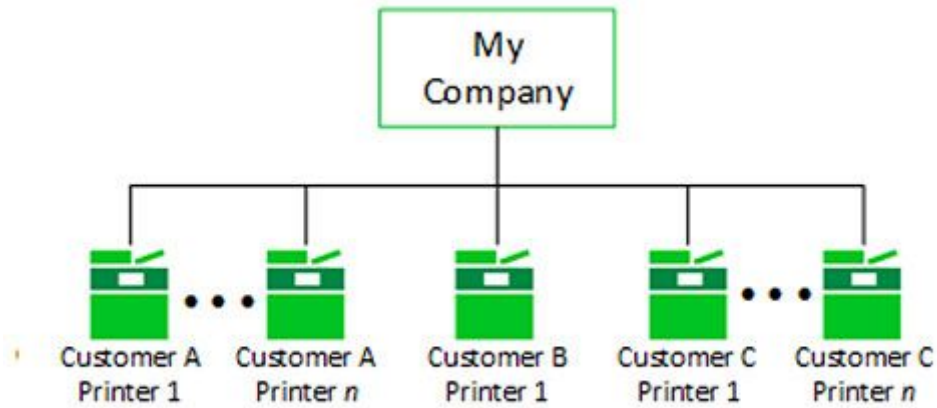
| Purpose	Hierarchical	Flat
Identifying a customer's printers	Printers for each customer are separated into different child organizations.	Printers must be tagged with an identifier to determine which customer is using it.
Finding a specific printer	The customer must be known, or each child organization must be individually searched for the specific printer.	All printers are in one list.
Print activity reporting	A customer's printer activity can be easily determined by reporting on the print activity of the entire child organization.	A customer's printer activity must be determined by filtering printers by customer-identifiable means. For example, you can filter printers by tags.
Future Lexmark Cloud Services functionality	Future Lexmark Cloud Services functionality can be selectively granted to individual customers.	Future Lexmark Cloud Services functionality made available to one customer is available to all. Some enhanced functionality may not be supported in a flat structure.
Account management by customers	A customer administrator can be added where needed in individual customer organizations without sharing access to information of other customers.	A customer administrator who is added can see all printer information for all customers.

Creating a child organization

1. In the Account Management web portal, click **Organization > Child Organizations**.
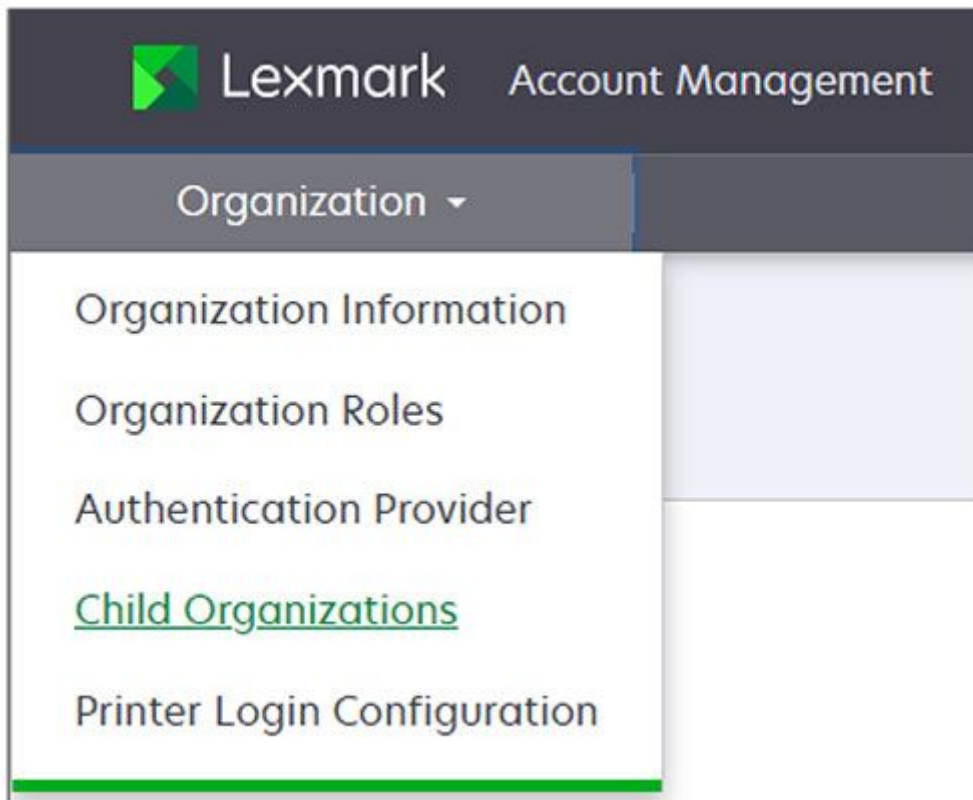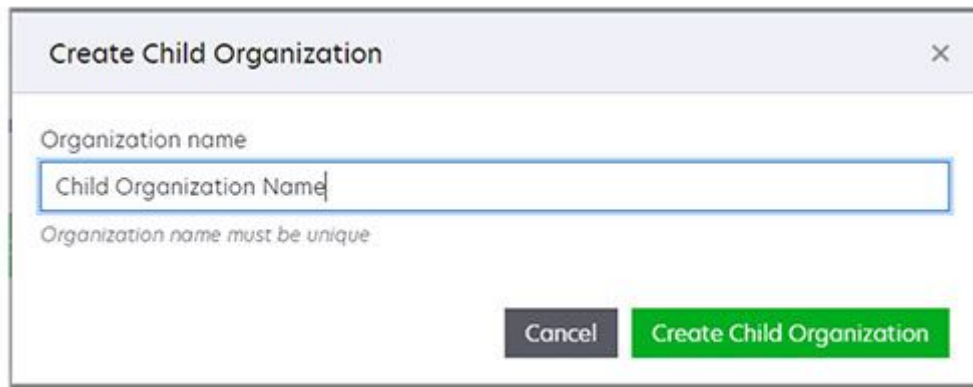
2. Click **Create**.

> **Note:** If there are no existing child organization, then click **Create Child Organization**.
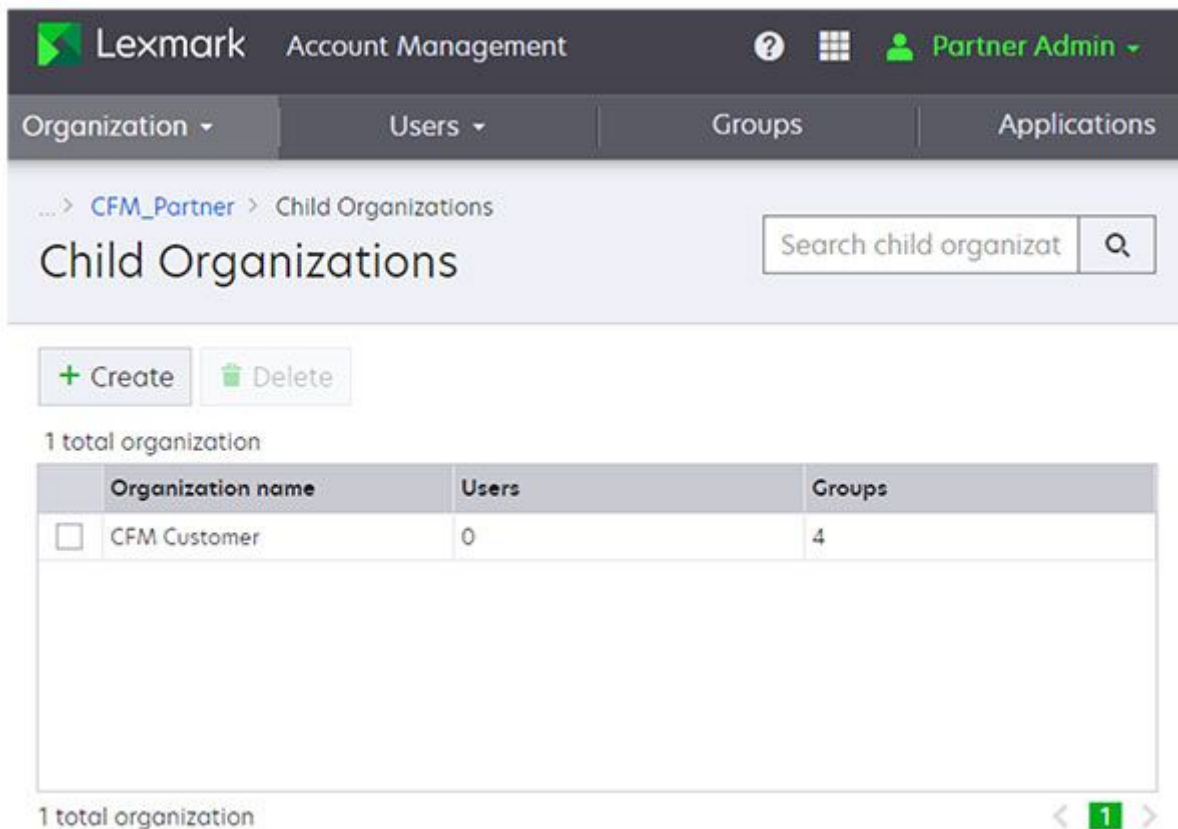
3. In the Organization name field, type a unique name and then click **Create Child Organization**.

Add and edit your users

Why do I need to manage users?

For users to use Lexmark Cloud Services, administrators must first create accounts for them based on their roles and responsibilities. It is common for a user's roles to change over time. You can easily make changes to those roles after the initial setup is complete. When creating Lexmark Cloud Services accounts for users, consider the following:

- What do users need to have access to the cloud?
- What functions will each user need to perform?

For channel partners, also consider the following if child organizations are created:

- Will users in your organization need access to child organizations?
- What users do you need to create in the child organization, and what functions will they need to perform?

Adding users

To give a user access to Lexmark Cloud Services, administrators must first create accounts for them in an organization in Lexmark Cloud Services. You can create user accounts in one of the following ways.

- Using the Add User form in the Account Management portal
- Importing users using a file in the Account Management portal
- Using federated identity management

Creating users manually by using the Add User form

You can create an account for a user manually in Lexmark Cloud Services by typing the user's information in the Add User form. Only one account can be created at a time. Use this method if you are adding only a few users.

1. From the Account Management web portal, click **Users**.
2. Click **Create User** or **Create**.
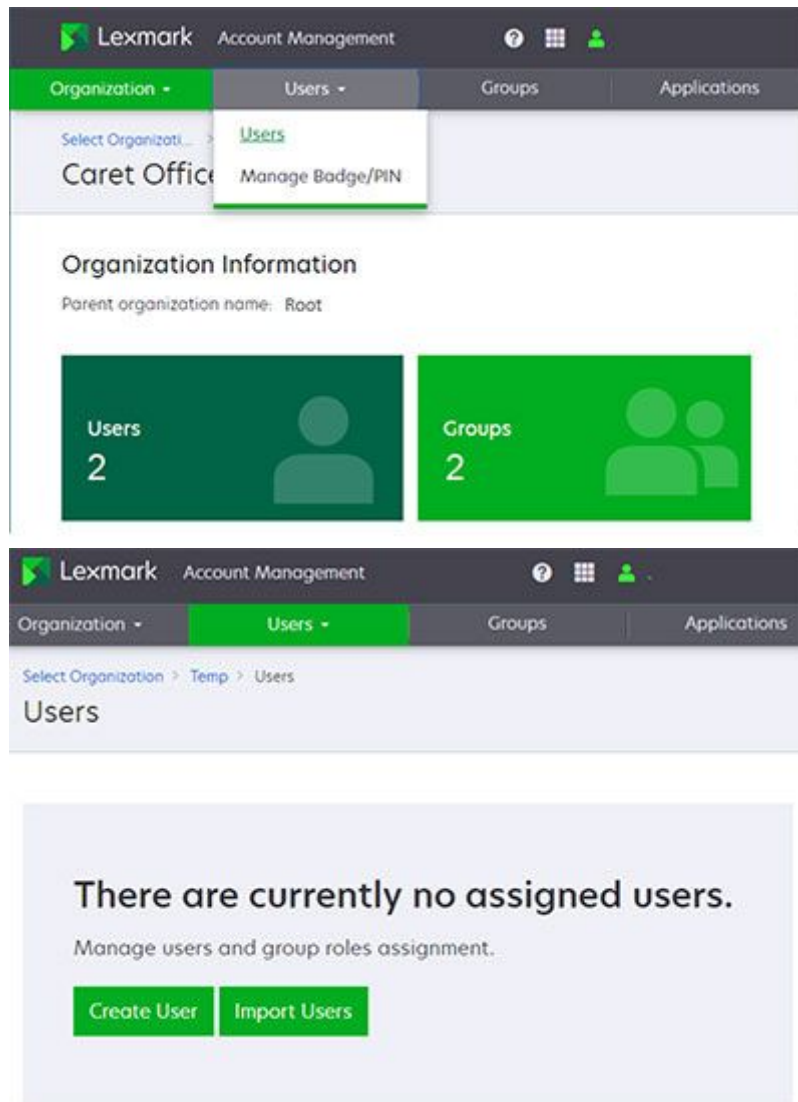
3. Type the following details:

    ◦ **E-mail**—Must be your Lexmark Cloud Services account name.
    ◦ **First Name**
    ◦ **Last Name**
    ◦ **Display Name**—The name that you want to appear in the Lexmark Cloud Services portal when you log in.
    ◦ **Department**
    ◦ **Cost Center**
    ◦ **Set Password**—This is required only when for Lexmark Customer Identity Management Services are used. The administrator can either manually set the user's password or email a link to the user. Users can use that link to create their own password.

4. Click **Create User**.

Importing users from a CSV file

You can create multiple user accounts simultaneously by importing them from a file. The Import feature lets you create, update, and delete multiple users in an organization using a CSV or TXT file. You can also create user groups, assign a user to those user groups, and set user PINs. For more information, see "Managing users" topic in *Lexmark Cloud Services Administrator's Guide*. Use this method if you are adding a large number of users.

Notes

- The CREATE command is used to create a new user account.
- The headers of the import file are case-sensitive.
- Count the commas. All columns must be accounted for on each line of the CSV file.
- The size of the CSV file must not exceed 1MB.

Creating users when using federated identity management

When federated identity management is used, you do not need to create or import users manually to create their accounts. A user account in a federated organization is automatically created when the user logs in to the following for the first time:

- Lexmark Cloud Services portal
- A Lexmark Cloud submission client
- The Lexmark Print application

Creating a user account in a federated organization is useful in the following ways:

- If your organization already uses an identity management system, then federating allows Lexmark Cloud Services to authenticate users with your identity management system. User accounts do not have to be manually created or imported into the Account Management portal. User credentials are not stored in Lexmark Cloud Services.
- If user badges are not maintained in your authentication provider, then they can be manually added for each user. Or a list can be imported using the CSV file import function. This action pre-registers user badges.

    Note: If your authentication provider maintains the users' badges, then they can be obtained directly through a claim from your authentication provider. This also allows badges to be used without having to register them.

- If the department or cost center definitions used in Lexmark Cloud Services do not correspond to definitions in your authentication provider, then you can resolve the mismatch. You can manually add missing definitions for each user, or you can import a list using the CSV file import function.

Note: If configured in the authentication provider setup, then user badges and department or cost center definitions can be obtained directly through claims from your authentication provider.

Assigning roles

User roles

Roles are used to manage access to specific features within Lexmark Cloud Services. A user can be assigned roles using any of the following methods:

- **Assigning roles individually**—Requires assigning roles manually to each user.
- **Assigning roles through groups**—Allows a set of roles to be given to users by making them a member of a group. Users can be members of more than one group.
- **Inheritance through organization roles**—Automatically assigns the organization roles to all users in the organization.

> **Note:** For more information on user roles, see "Understanding roles" topic in *Lexmark Cloud Services Administrator's Guide*.

Determining what roles are needed

Before assigning roles, you must determine the features of Lexmark Cloud Services that your organization plans to use, and which individual users plan to use them.

Administrative roles for account management

There are two administrative roles for account management: the **Organization Administrator** and the **User Administrator**.

Organization Administrator

- Role with the most privileges
- Can manage organizational settings for your organization
- Can manage user accounts for your organization

  - Can add and delete user accounts
  - Can add and remove roles assigned to user accounts
  - Can add and remove user accounts from groups

User Administrator

- Can manage user accounts for your organization

  - Can add and delete user accounts
  - Can add and remove roles assigned to user accounts
  - Can add and remove user accounts from groups

For channel partners, users who manage the configuration, user accounts, or printers in a customer organization must be added to a **Child Organization Access Group**. For more

information, see "Managing the Child Organization Access Group" topic in *Lexmark Cloud Services Administrator's Guide*.

The following table lists the roles required for actions to be performed in a customer (child) organization:

Action	Roles to assign to a child organization access group
Managing organizational settings	Organization Administrator
Managing user accounts	Organization Administrator or User Administrator
Managing printers	Fleet Management Administrator
Managing Cloud Print Management	Print Release Management Administrator

Roles for Cloud Fleet Management

- Users enrolling printers in Cloud Fleet Management must have the **Fleet Management Administrator** and the **File Service Administrator** roles.
- Users accessing Fleet Management reports but not enrolling printers in their organization must have the **Fleet Management Reporting Analyst** role.
- Users enrolling a customer's printers in Cloud Fleet Management must be added as members of a **Child Organization Access Group**. They must also be assigned the **Partner Administrator**, **Fleet Management Administrator**, and **File Service Administrator** roles.
- Users accessing Fleet Management reports for printers in customer organizations but not enrolling printers must be added as members of a **Child Organization Access Group**. They must also be assigned the **Partner Administrator**, **Fleet Management Reporting Analyst** roles.

Roles for Cloud Print Management

The roles support two methods of print job submission and release: **Cloud Print Management** and **Hybrid Print Management**.

Submitted print jobs are stored in the Lexmark Cloud Service until the user releases it at a Cloud Print Management–enabled printer.

- Users submitting and releasing print jobs using Cloud Print Management must have the **Print Release Management User** role.
- Users managing Print Management for their organization must have the **Print Release Management Administrator** role.
- Users generating organizational Cloud Print Management reports but not submitting and releasing jobs must have the **Print Release Management Reporting Analyst** role.

Roles for Hybrid Print Management

Submitted print jobs are held on the user's workstation until the user releases it at a Cloud Print Management–enabled printer that uses Hybrid Print Management.

- Users using Hybrid Print Management must have the **Hybrid Print Management User** role.
- Users managing Print Management for their organization must have the **Hybrid Print Management Administrator** role.
- Users generating organizational Print Management reports but not using Hybrid Print Management must have the **Print Release Management Reporting Analyst** role.

Assigning roles to an individual

1. From the Account Management web portal, click **Users > Users**.
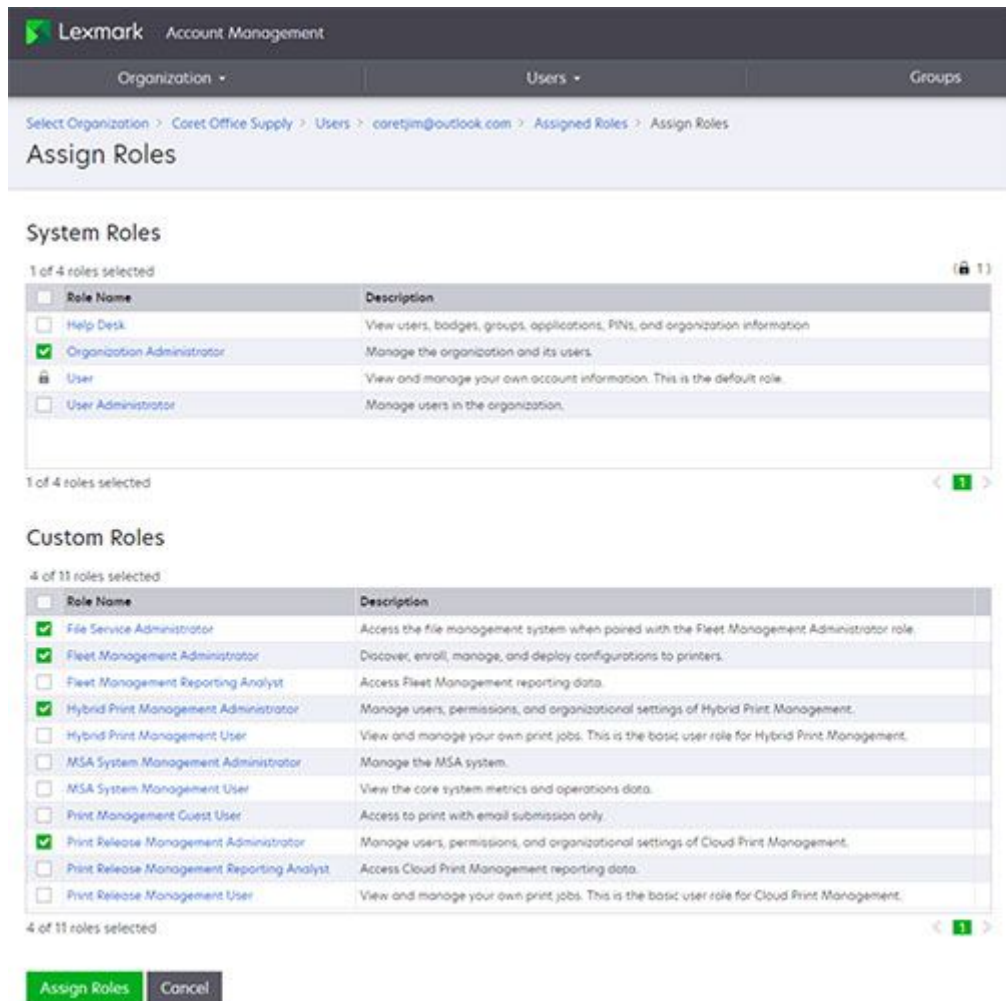2. On the Users page, click the E-mail of the user.
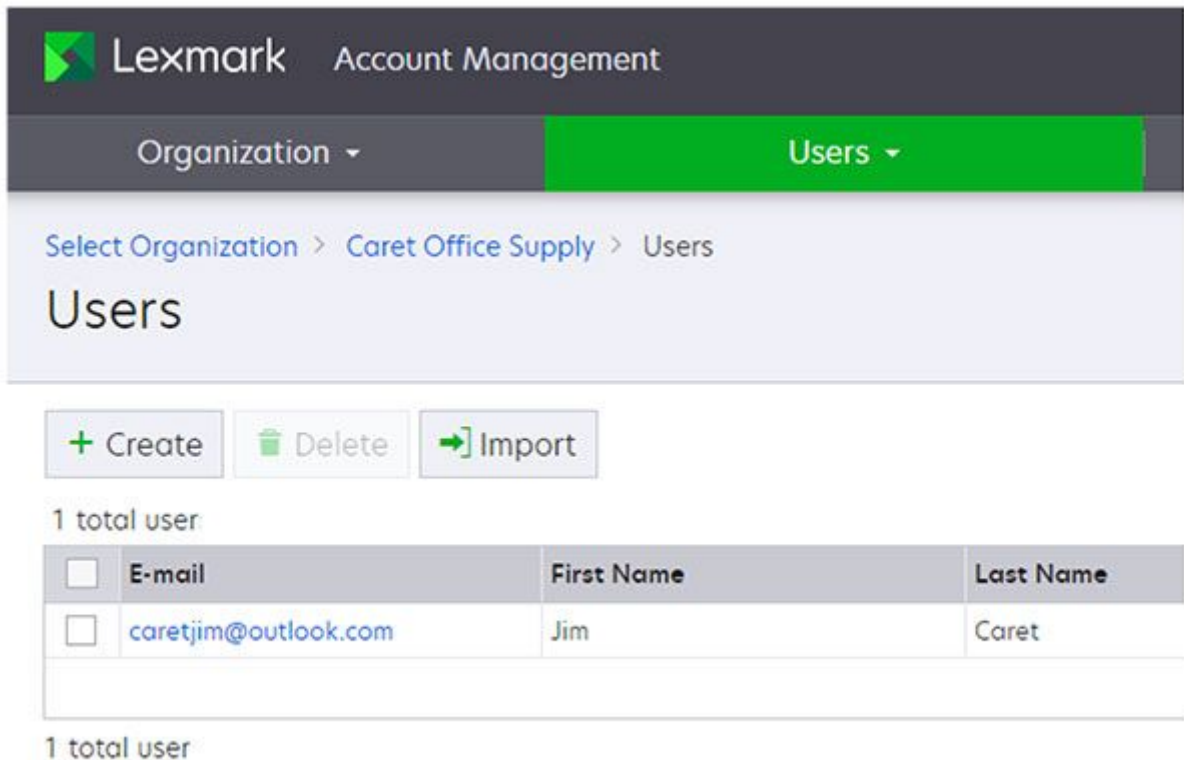
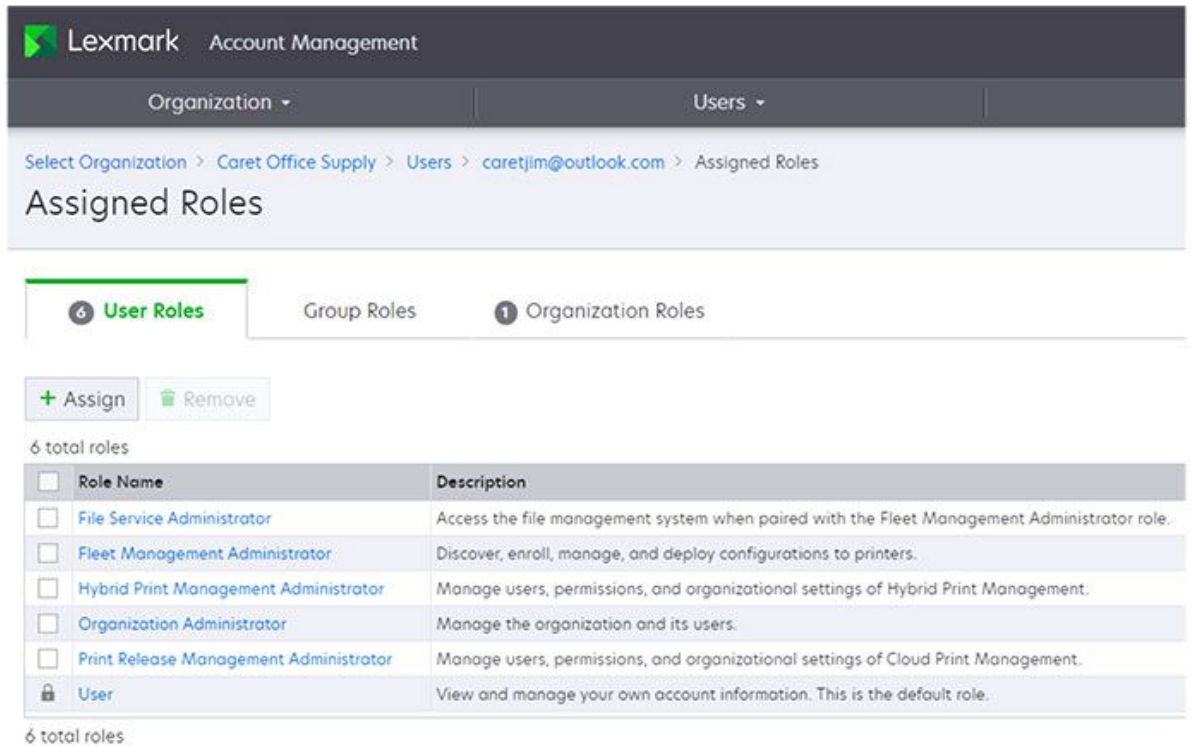3. In the Assigned Roles section, click **Edit**.
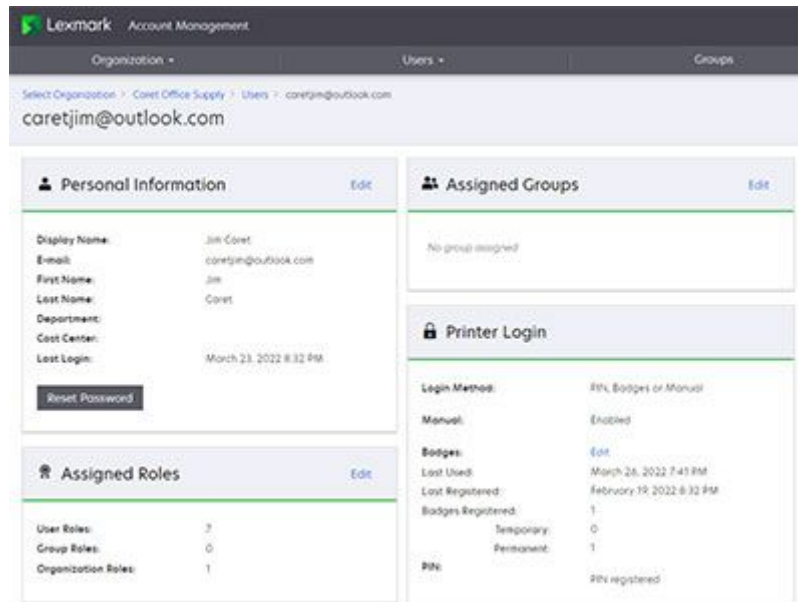
4. Do the following:

   ◦ To assign a role, click **Assign**.

      1. On the Assign Roles page, select or remove the roles.
      2. Click **Assign Roles**.

   ◦ To remove a role, select the role, and then click **Remove > Remove Role**.
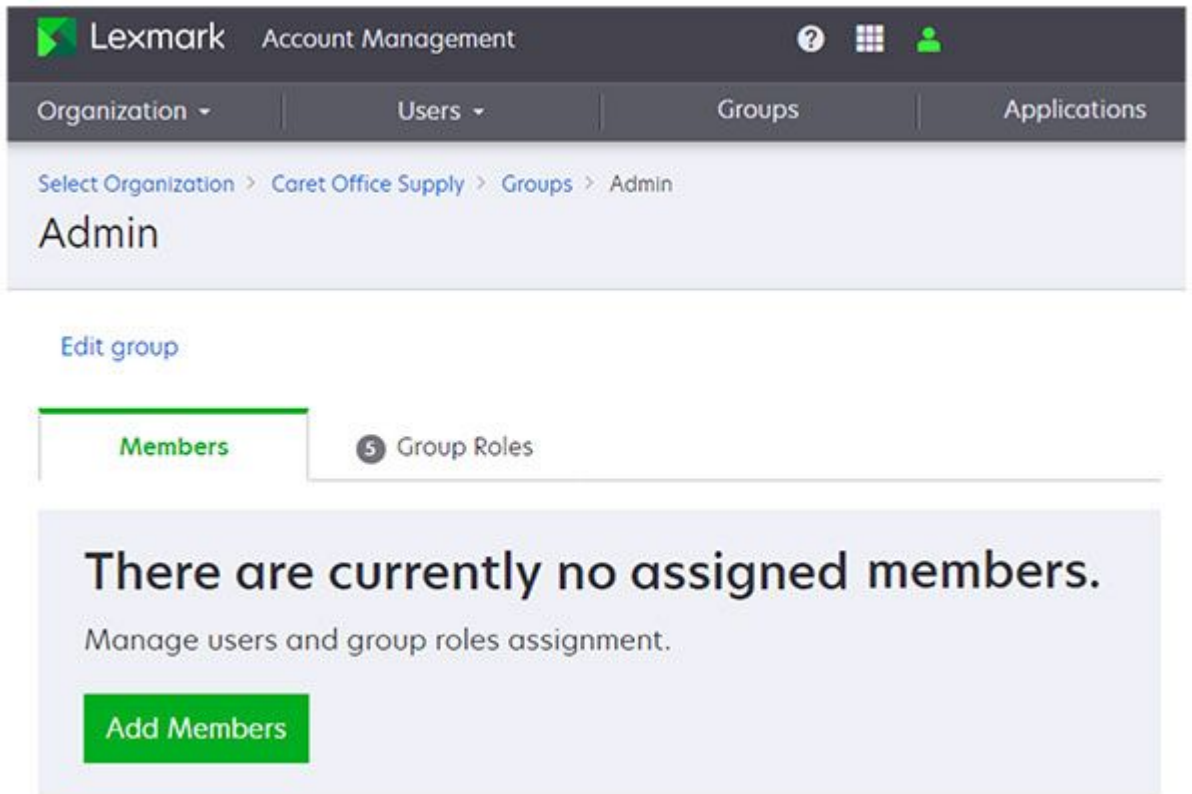
Assigning roles through groups

Assigning roles through groups allows a set of roles to be given to users by making them a member of a group. This method makes it easy to assign the same roles to multiple users.

**Note:** Users can be members of more than one group.

1. From the Account Management web portal, click **Groups** tab.
2. Do any of the following:

   ◦ To create a new group, click **Create**.
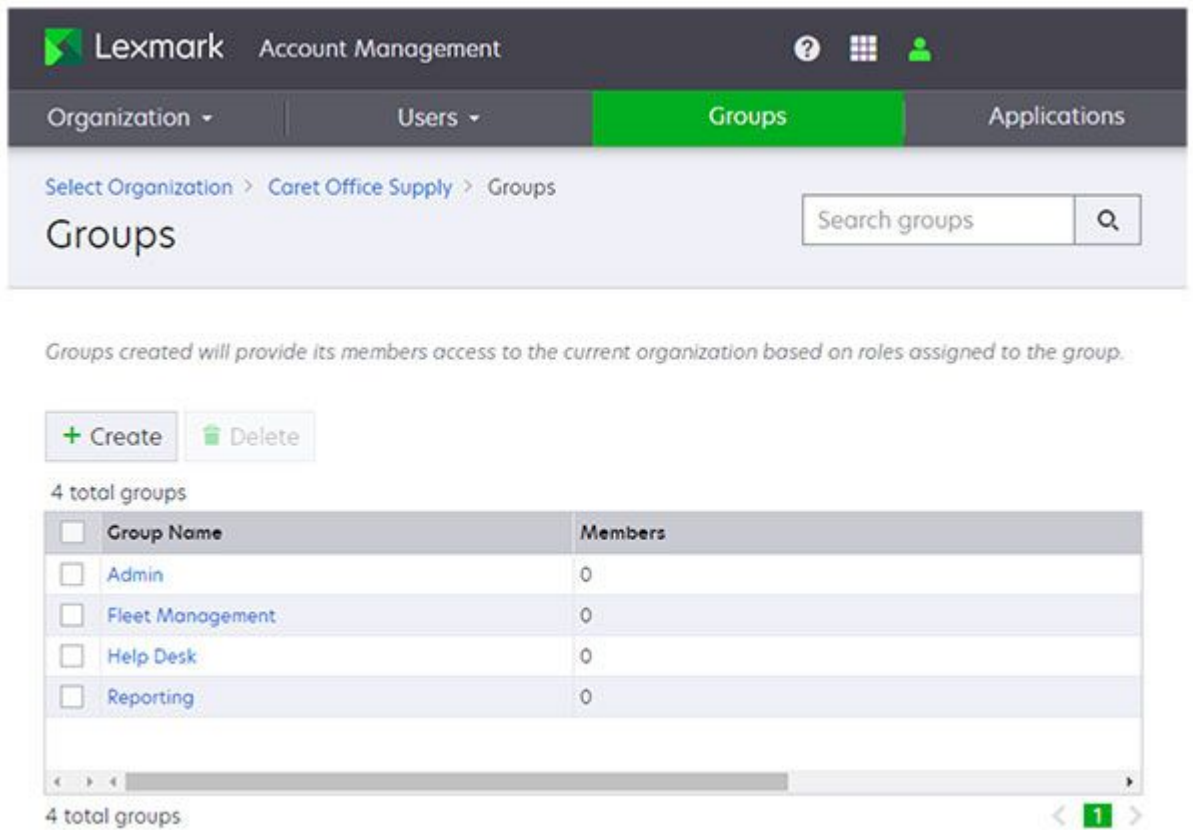
1. In the Group name field, type the name of the group.
2. Click **Create Group**.
   ◦ To edit an existing group, click the group under the Group Name column.
3. On the Edit group page, do the following:

   ◦ From the Members tab, add or remove members.

◦ From the Group Roles tab, you can either assign or remove roles.
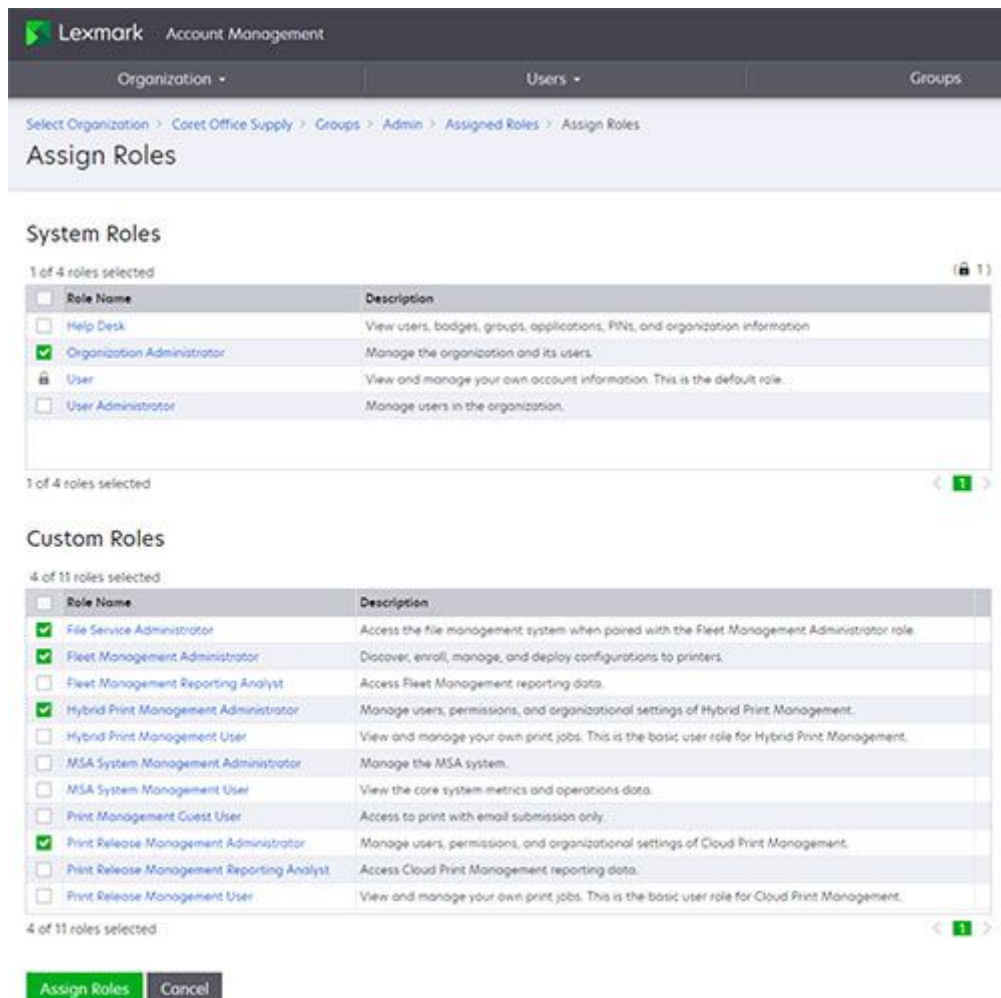
Assigning roles by membership in a child organization access group

Notes

- Child organization access groups are available only to channel partners.
- Roles assigned through membership in a child organization access group apply across all customer organizations.

For channel partners, the **Groups** tab shows two tabs: **Organization Access** and **Child Organization Access**. Organization access groups apply only to the channel partner's organization. Child organization access groups apply to the customer organization. The process for managing membership and roles for organization access and child organization access groups is the same.


The difference between organization access groups and child organization access groups is that child organization access groups are created with a default role, **Partner Administrator**. You cannot delete the Partner Administrator role from a child organization access group. You can add or remove additional roles as needed.

The Partner Administrator role is required for users to have access to customer (child) organizations. For example, a user who will be managing printers in a child organization using Fleet Management must be a member of a child organization access group. Moreover, that child organization access group has the Fleet Management Administrator role added along with the default Partner Administrator role.
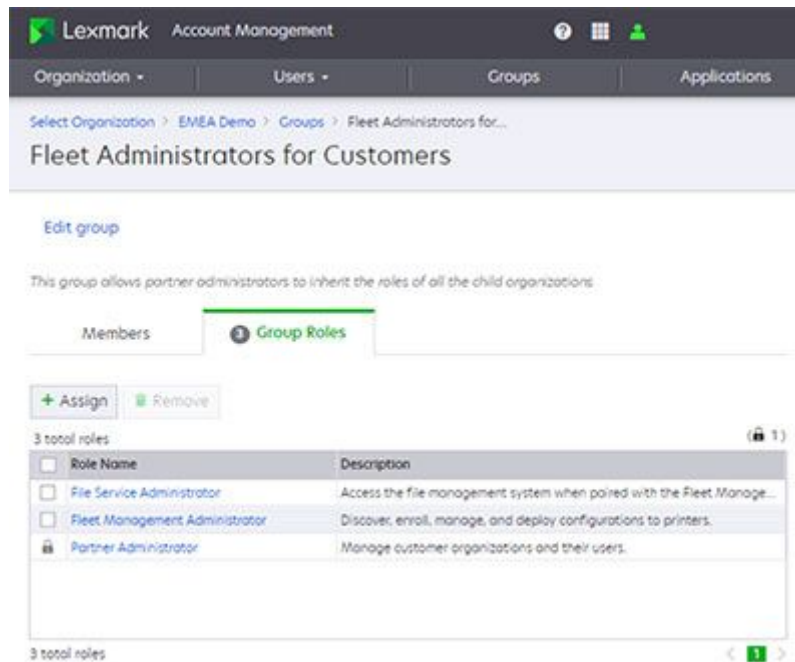
Assigning organization roles

Roles can be assigned at the organization level. Organization roles are automatically inherited by all users in the organization. For example, if all users can access Cloud Print Management, then they are all assigned the Print Release Management User or Hybrid Print Management User role. The roles can be automatically assigned to all users via the organization roles.

1. From the Account Management web portal, click **Organization > Organization Roles**.
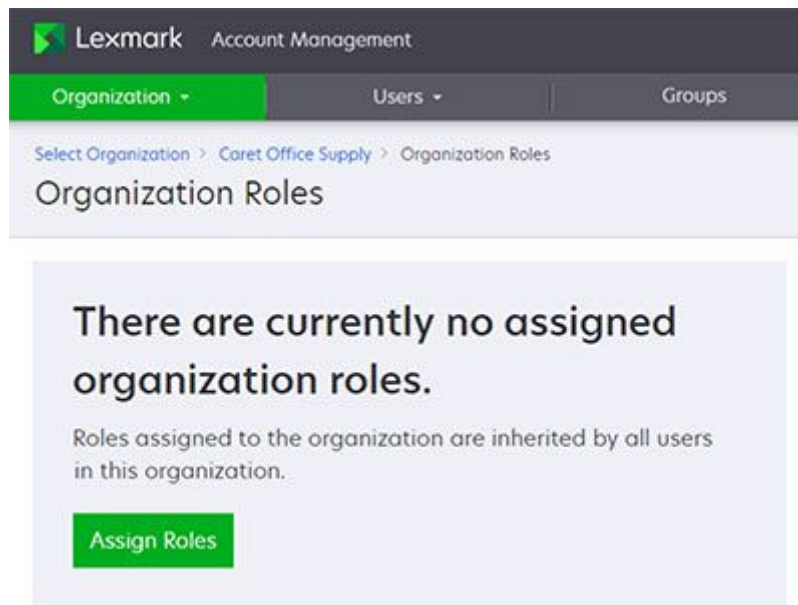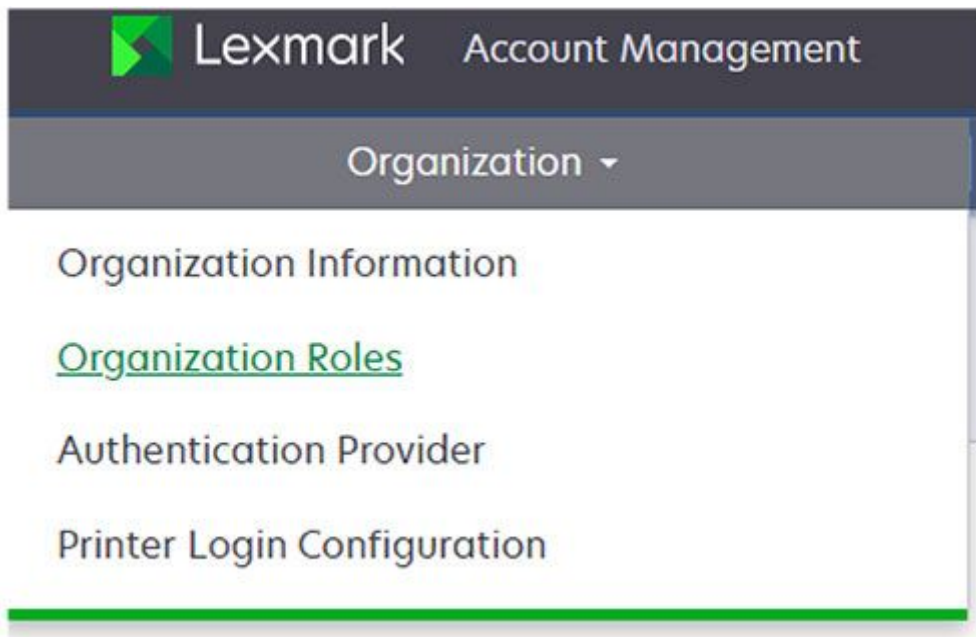
2. Click **Assign** or **Assign Roles**.
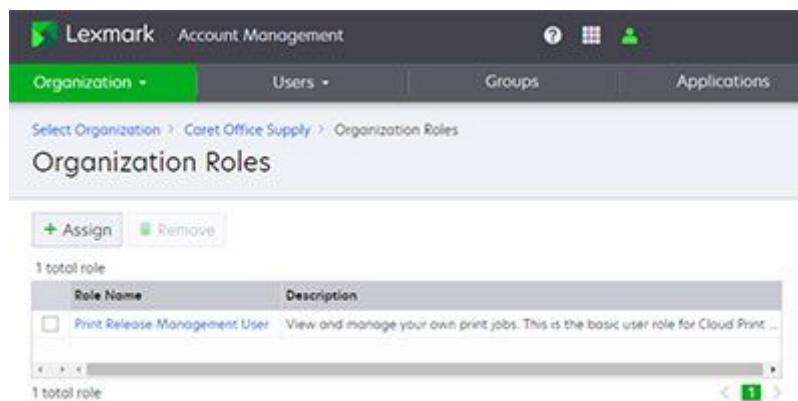
3. From the Assign Roles page, add or remove roles.

4. Click **Assign Roles**.

Managing user badges

If users are authenticating at the printer, then set up a badge or PIN for each user. For more information on badge configuration, see "Managing printer logins" group.
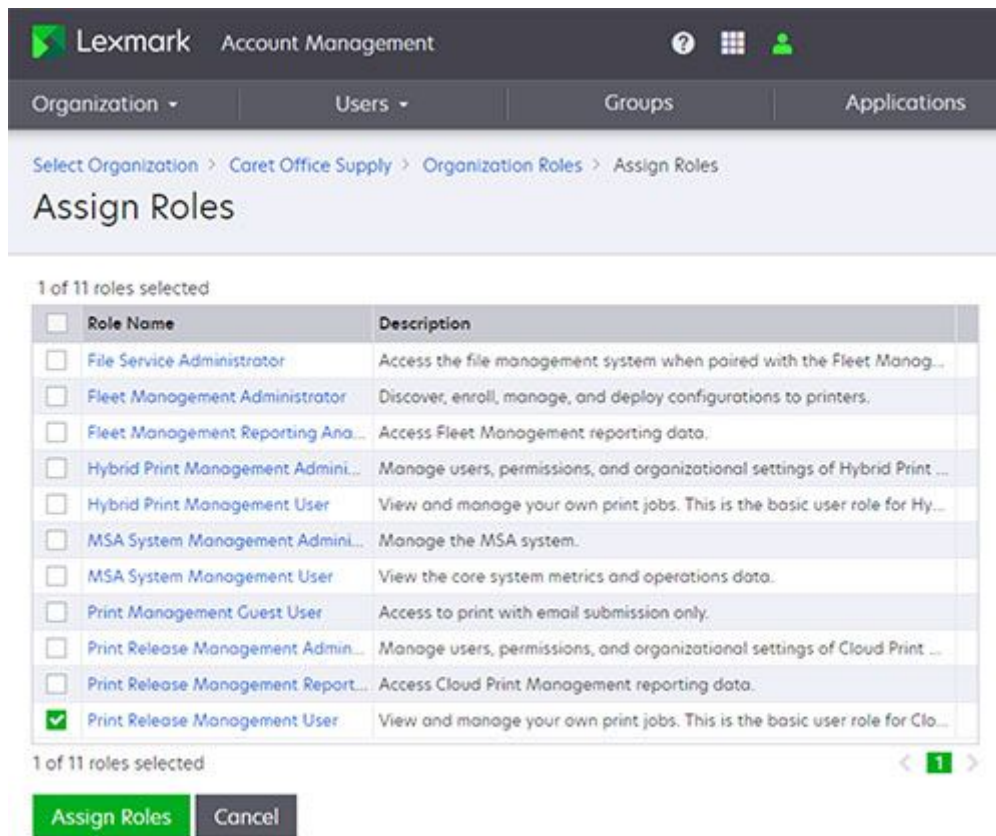**Assigning badges**

If identity federation is used and badge IDs can be retrieved using claims from your identity management service, you can automatically populate badge IDs from the service.

> **Note:** A user must log in to the Lexmark Cloud Services portal once before their badge ID is retrieved so that it can be used to authenticate at a printer.

If identity federation is not used or badge IDs are not available from your identity management service, then you can assign badge IDs in two ways. The method to use depends on how much of the process you want your users to participate in.

- **Assigned by an Organization Administrator or User Administrator in the Account Management portal**—Can be done manually, one user badge at a time, or by importing from a CSV file, for multiple user badges
- **Assigned by the user**—Can be done manually from the user's My Accounts page, which requires users to provide their badge ID, or manually at the printer

Badges registered manually by an Organization Administrator or a User Administrator in the Account Management portal

1. From the Account Management portal, use any one of the following methods to access the Registered Badges page:

   Note: If you are a channel partner with child organizations, then you must select the organization.

   Using the Users card in the Account Management portal

   a. Click the **Users** card.
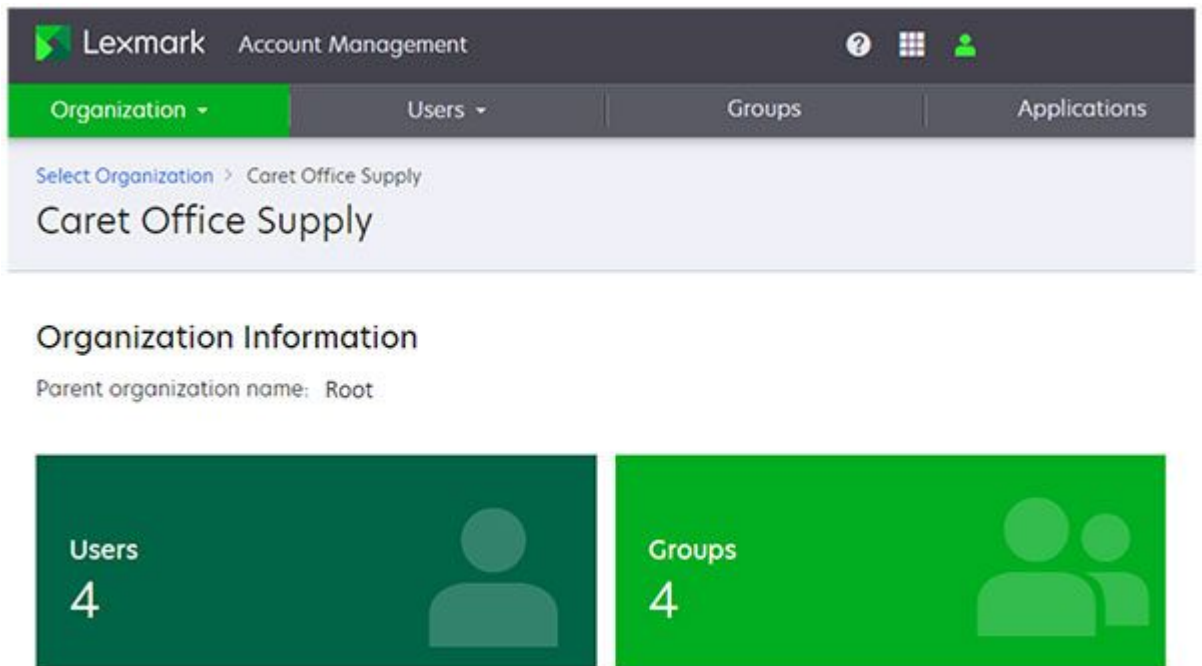
   b. Click the email address of the user.
   c. In the Printer Login section, for the Badges login, click **Edit**.

caretsally@outlook.com

Personal Information   Edit

Display Name: Sally Caret
E-mail: caretsally@outlook.com
First Name:
Last Name:
Department:
Cost Center:
Last Login: March 3, 2022 12:04 PM

Reset Password

Assigned Roles   Edit

User Roles: 1
Group Roles: 0
Organization Roles: 1

Assigned Groups   Edit

No group assigned

Printer Login

Login Method: PIN, Badges or Manual

Manual: Enabled

Badges: Edit
No badge registered

PIN: Set PIN

d. Click **Register** or **Register Badge**.

Select Organization > Caret Office Supply > Users > caretsally@outlook.com > Registered Badges

Registered Badges

+ Register   🗑 Delete

1 total badge
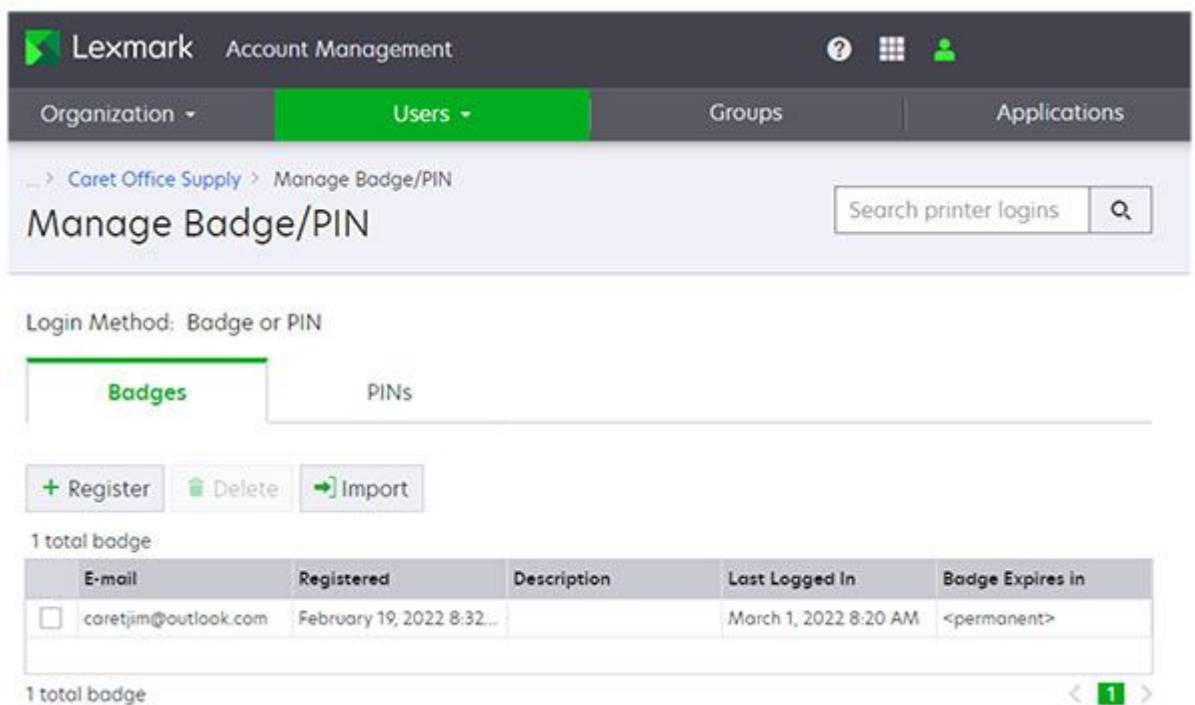
	Registered	Description	Last Logged In	Badge Expires in
☐	March 7, 2022 8:24 AM		<waiting for log in>	<permanent>

1 total badge   < **1** >
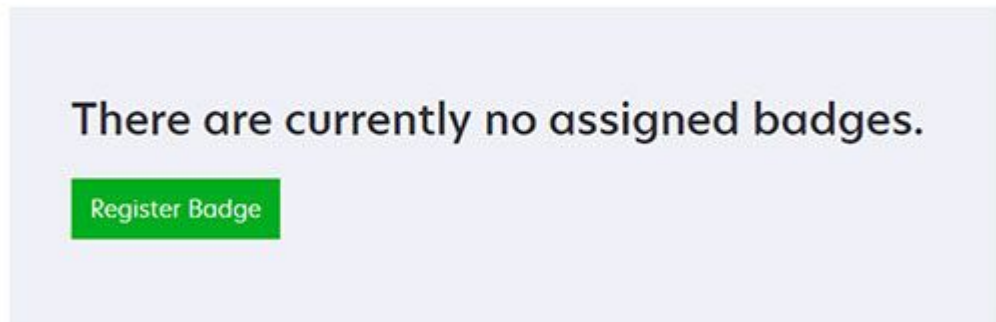
e. In the Register Badge window, enter the badge information.

Using the Users menu

a. From the Users menu, click **Manage Badge/PIN**.
b. Click **Register** or **Register Badge**.

c. In the Register Badge window, enter the user's email address and the badge information.

> **Note:** The user's email address must already exist in the organization.

2. Click **Register Badge**.

Badges imported by an Organization Administrator or a User Administrator in the Account Management portal

1. From the Account Management portal, use one of the following methods to access the Registered Badges page:
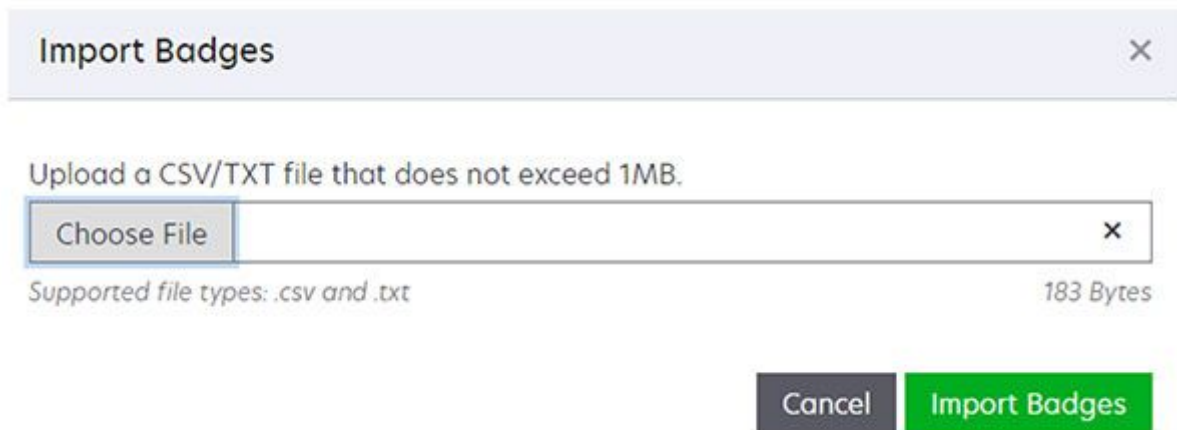
> **Note:** If you are a channel partner with child organizations, then you must select the organization.

2. From the Users menu, click **Manage Badge/PIN**.
3. Click **Import Badges**.

Manage Badge/PIN

Login Method: Badge

There are currently no assigned badges.

Register Badge   Import Badges
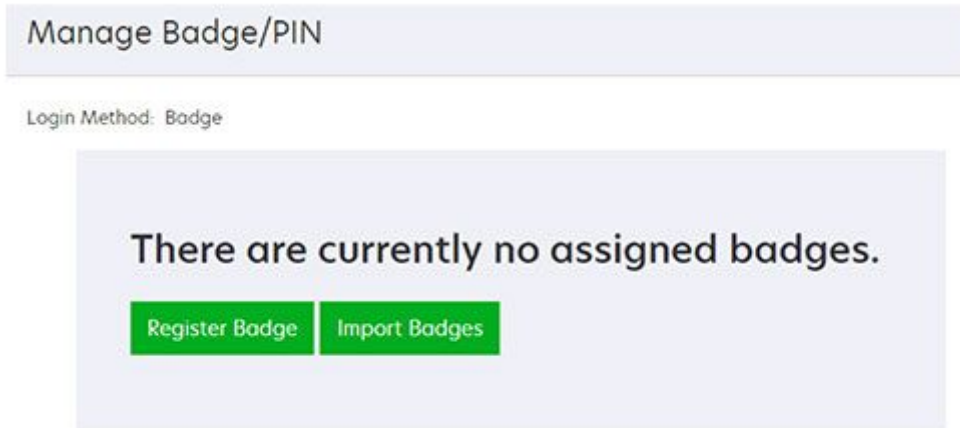
4. In the Import Badges window, browse to the CSV or TXT file that contains the list of badges.

> **Note:** For more information, see "Managing users" topic in *Lexmark Cloud Services Administrator's Guide*.

Import Badges   ✕

Upload a CSV/TXT file that does not exceed 1MB.

Choose File   ✕

Supported file types: .csv and .txt   183 Bytes

Cancel   Import Badges

5. Click **Import Badges**.

Badge registered by users through their My Account page

This action can only be performed by users for their own badge.

1. From the Lexmark Cloud Services portal, in the username menu, click **My Account**.
2. On the My Account page, in the Printer Login section, for the Badges login, click **Edit**.

3. Click **Register** or **Register Badge**.

4. In the Register Badge window, enter the badge information.
5. Click **Register Badge**.

Badge registered by a user at the printer control panel

This action can only be performed by users for their own badge. Badges can be registered by users at the printer control panel using one of the following methods:

- Manual badge registration using your email address and password

    1. Tap your badge on a card reader that is attached to a printer.
    2. From the control panel, touch **Manual Registration**.
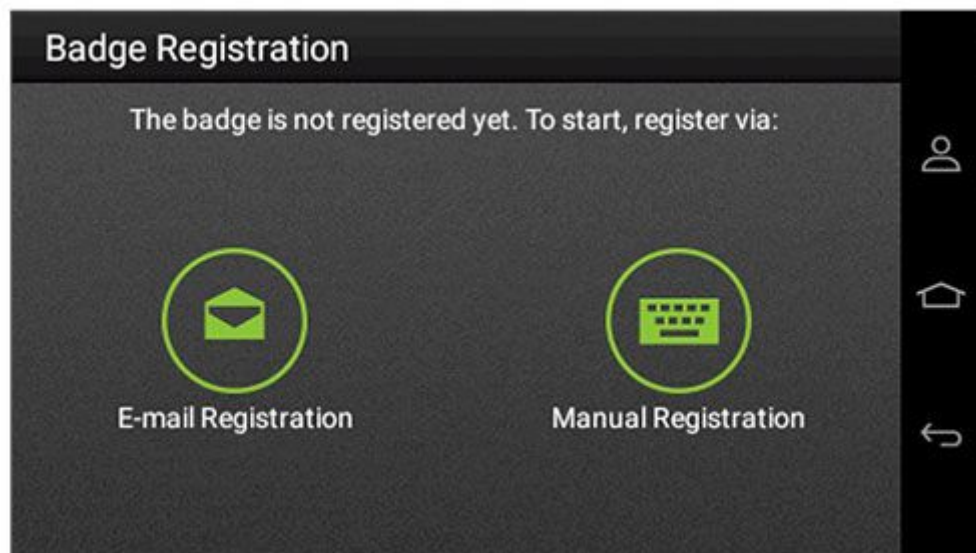
    3. In the Enter your existing account credentials field, type your email address and password.
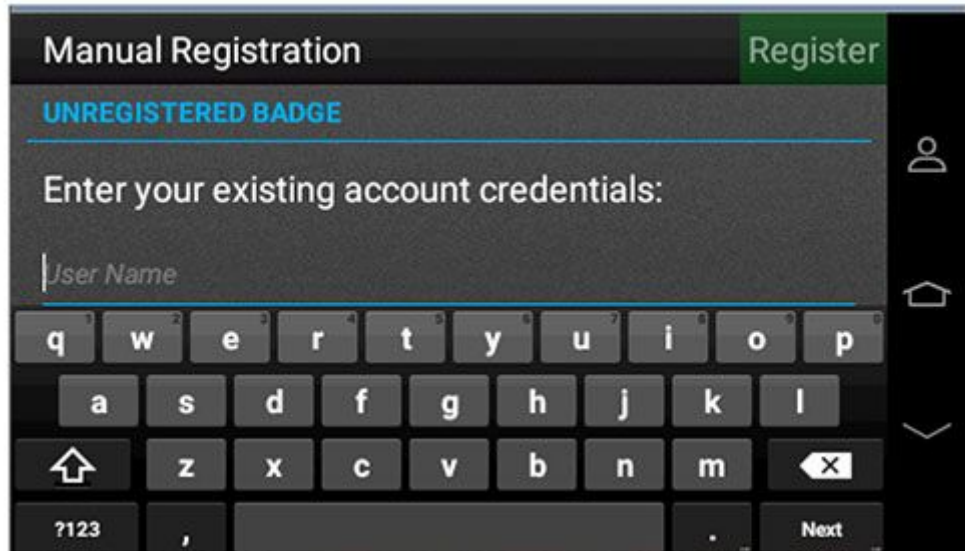
4. Touch **Register**.
- Email badge registration request sent from the printer

    1. Tap your badge on a card reader that is attached to a printer.
    2. On the control panel, touch **E-mail Registration**.
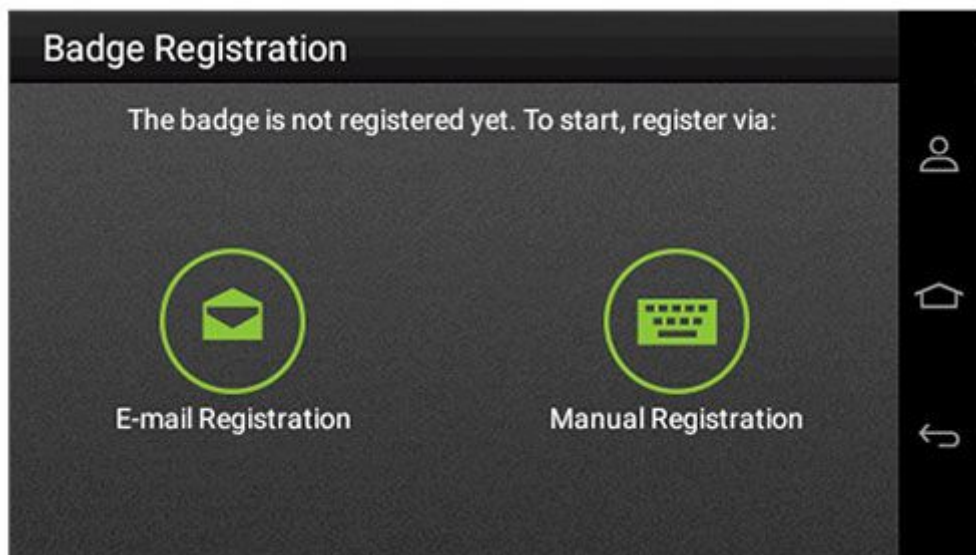
3. In the Send the registration link to field, type your email address.

4. Touch **Send > OK**.

5. Open your email account, and then click the badge registration link.

> **Note:** The following screen appears for 5 seconds before logging you into the My Account page of Lexmark Cloud Services portal .

Managing user PINs

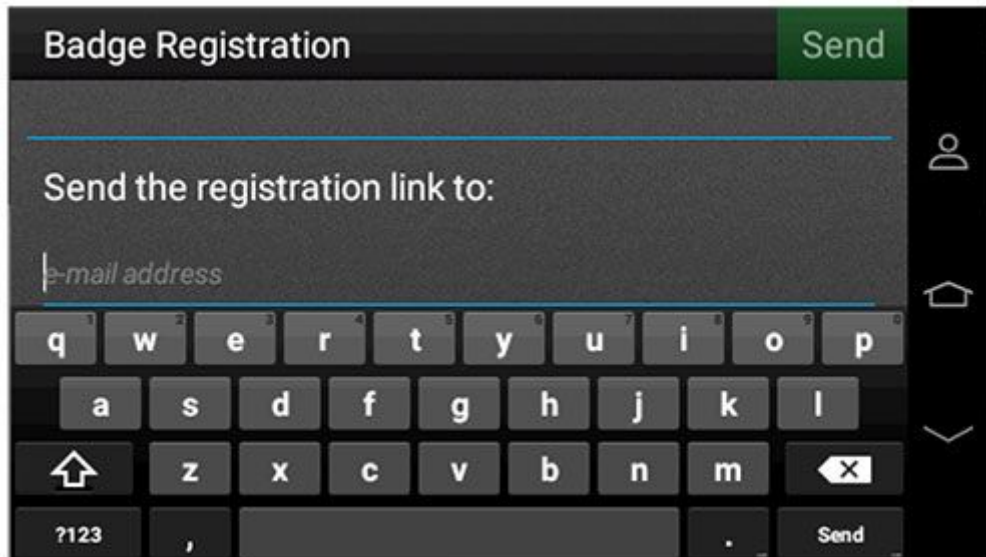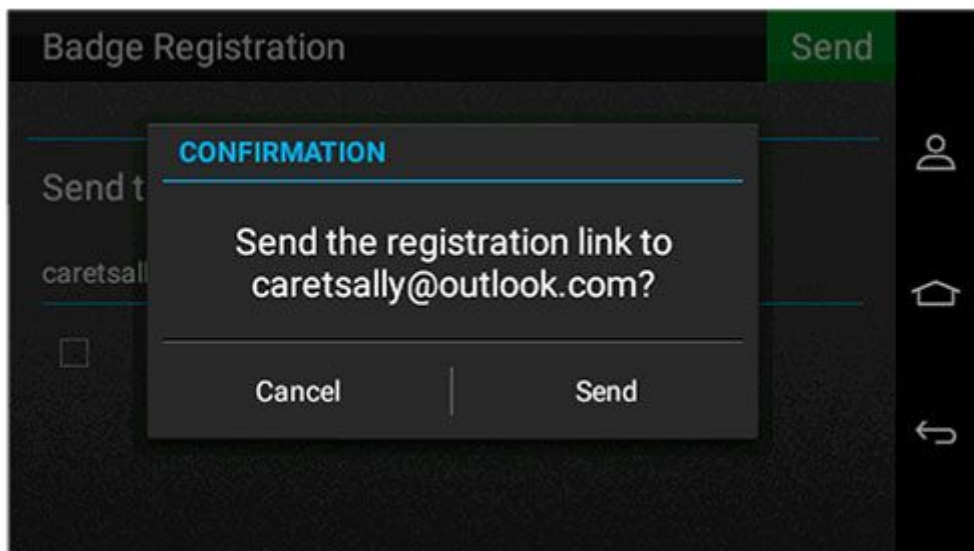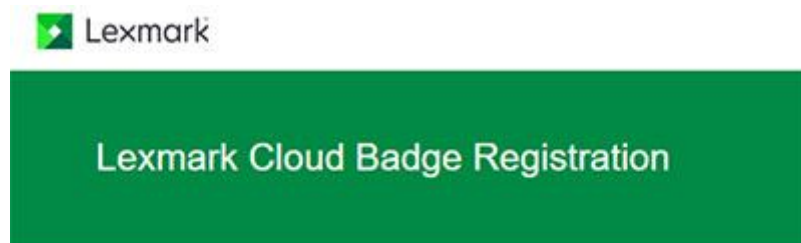If users are authenticating at the printer, then set up a badge or PIN for each user. For more information on PIN configuration, see "Managing printer logins" group in *Lexmark Cloud Services Administrator's Guide*.
Assigning PINs

If identity federation is used and PINs can be retrieved using claims from your identity management service, you can automatically populate PINs from the service.

Notes

- A user must log in to the Lexmark Cloud Services portal once before their PIN is retrieved, and it can be used to authenticate at a printer.
- If PINs are retrieved from your identity management system, then you must set the PIN Generation menu to **Administrator manually set** and to **Never expire**.
- Any PIN changes made in Lexmark Cloud Services is temporary. These temporary PINs are overwritten from your identity management system when the user logs in the next time.

If identity federation is not used or PINs are not available from your identity management service, then you can assign user PINs in two ways. The method to use depends on how much of the process you want your users to participate in.

- **Assigned by an Organization Administrator or User Administrator in the Account Management portal**—Can be done manually, one user badge at a time, or by importing from a CSV file, for multiple user badges

- **Assigned by the user**—Can be done manually from the user's My Accounts page, which requires users to provide their PIN

PIN generation options	Administrator	User
Automatically generate and email	Can request Lexmark Cloud Services to generate a new PIN for users[2]	Can request Lexmark Cloud Services to generate a new PIN for themselves[2]
Administrator manually sets	Can set or reset user PINs	Must request a new PIN from an administrator[1]
User sets	Cannot set or reset user PINs	Can set or reset their own PIN

[1] Administrator applies to Organization Administrators and User Administrators.

[2] PINs are sent to the user through email from Lexmark Cloud Services.

PINs assigned by an Organization Administrator or a User Administrator

An Organization Administrator or a User Administrator can set PINs for users one at a time or for multiple users at once by importing a file. New or reset pins are emailed to the user.

> **Note:** Make sure that PIN Generating Options is set to either **Automatically generate and email** or **Administrator manually sets**.

Setting the PIN for a single user

The Organization Administrator or User Administrator can use one of the following methods to set or reset a PIN for a user:

- **Using the users list**

    1. From the Account Management portal, select the **Users** card, or click **Users > Users**.

2. In the E-mail column, click the user email.
3. In the Printer Login section, for the PIN login, click either **Set PIN** or **Reset PIN**.

4. Based on the option chosen in the PIN Generation Option for the Organization Printer Login Configuration, do any of the following:

> **Note:** The result of clicking **Set PIN** or **Reset PIN** depends upon the PIN Generation Option chosen for the Organization Printer Login Configuration page.

- If **Automatically generate and email** is selected in the PIN Generation menu, then an email with the new PIN is sent as soon as you click **Set PIN** or **Reset PIN**.
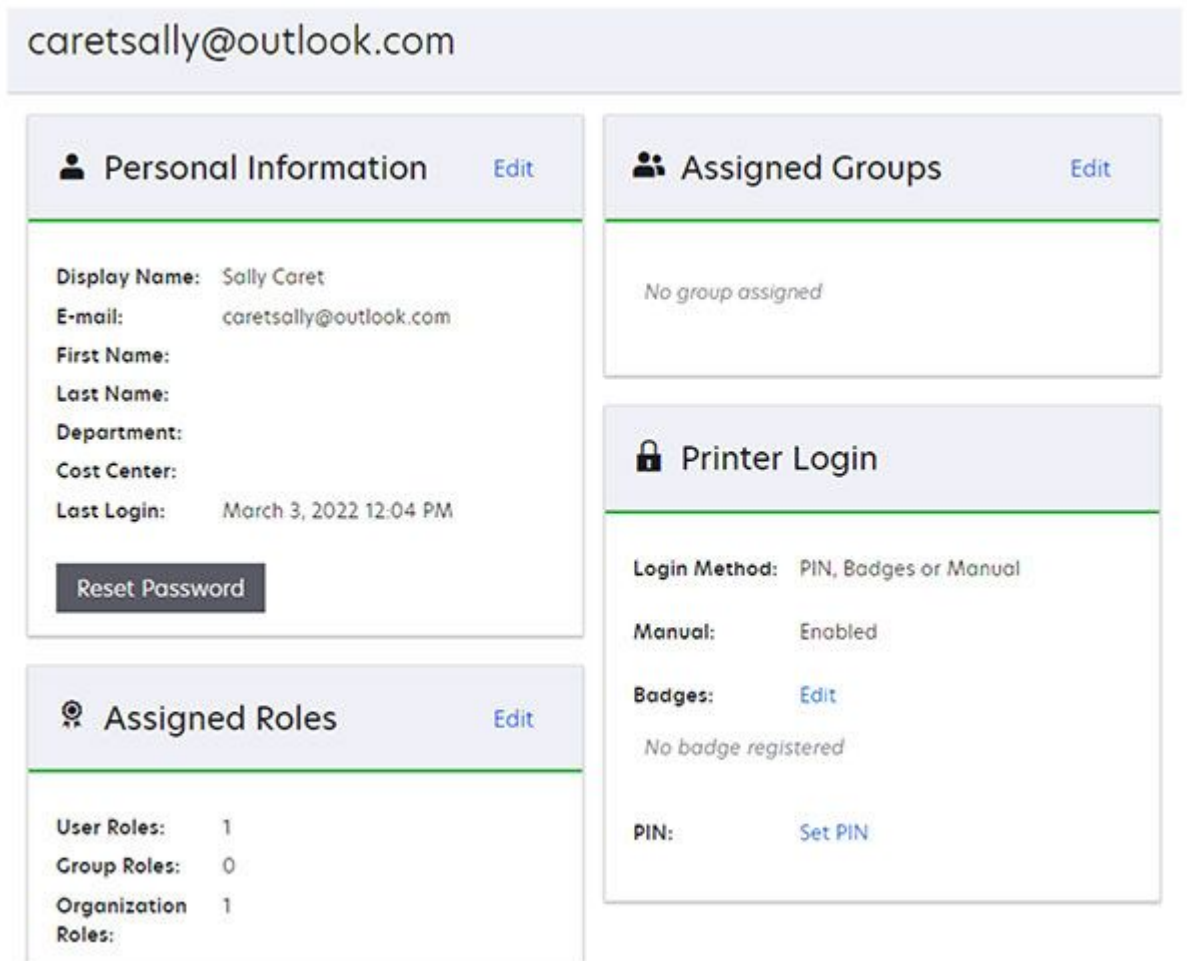- If **Administrator manually set** is selected in the PIN Generation menu, then a user must submit a request outside of Lexmark Cloud Services to an Organization Administrator or a User Administrator to set or reset their PIN.
- If **User set** is selected in the PIN Generation menu, then you can click **Set PIN** or **Reset PIN**, and then enter the new PIN, and then click **Generate PIN**.

An example of PIN received by the user.
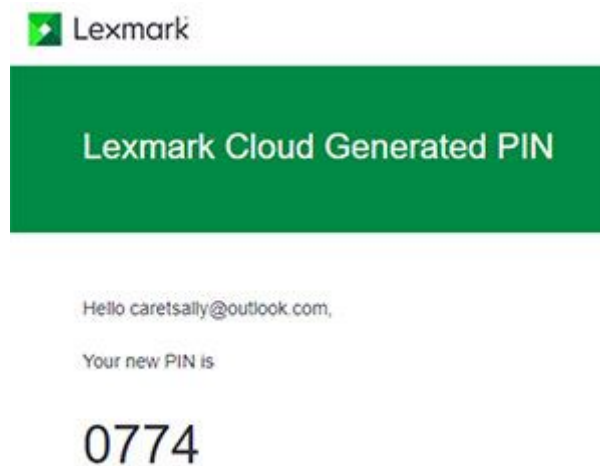
- **Using Manage Badge/PIN**

    1. From the Account Management portal, click **Users > Manage Badge/PIN**.
    2. Click the **PINs** tab.
    3. Click **Generate**.
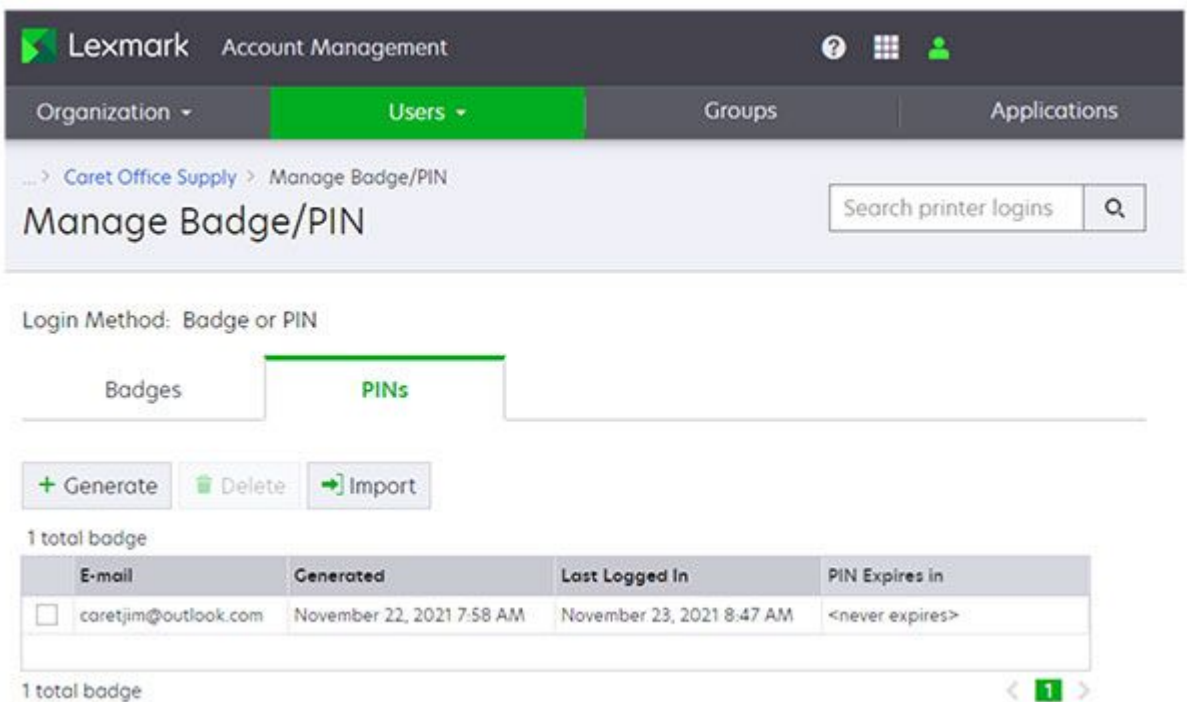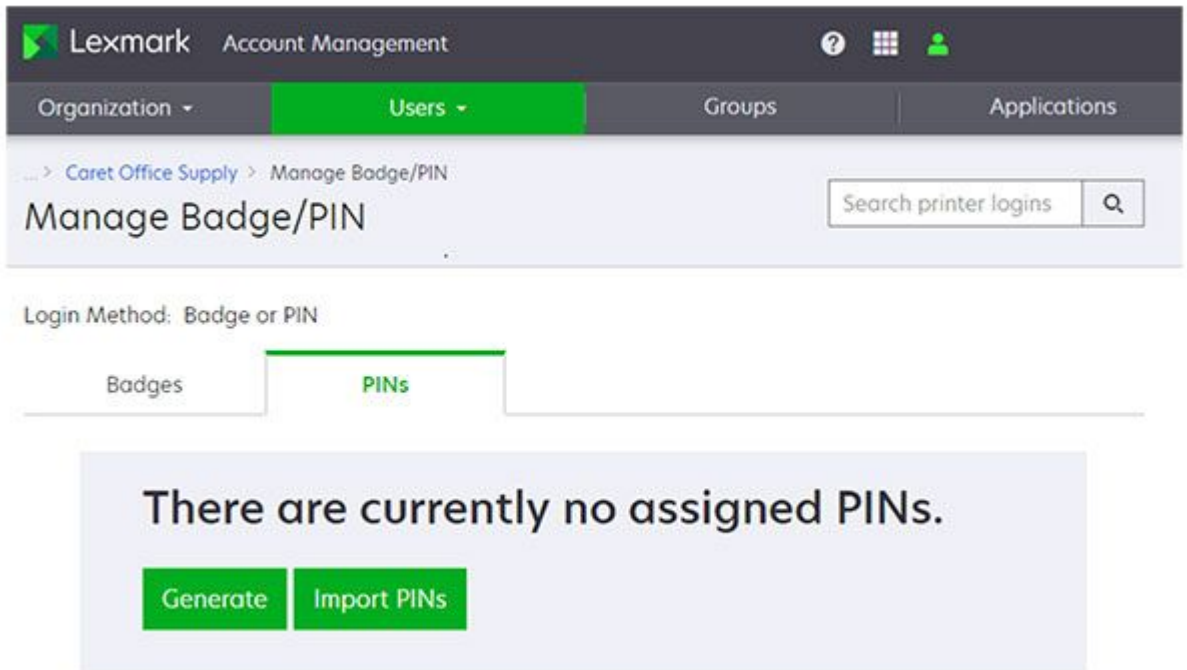
4. In the E-mail field, type the email address of the user, and then click **Generate PIN**.

> **Note:** The user receives an email with the PIN.
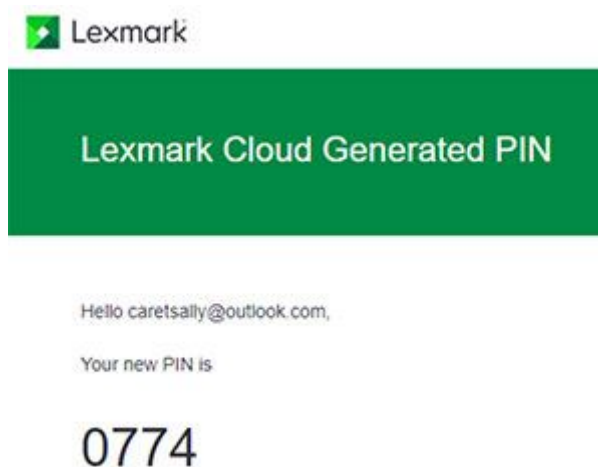
Importing user PINs

The Organization Administrator or User Administrator can set the PIN for one or more users by importing the PINs using a CSV or TXT file.

Notes

- PINs can be imported when user accounts are created using the file import method.
- If PIN Generation Options is set to **Automatically generate and email**, then any PINs set in the imported file are ignored. The PIN field should be left empty.
- For more information on the CSV and the TXT file, see *Lexmark Cloud Services Administrator's Guide*.
- The headers of the import file are case-sensitive.
- Count the commas. All columns must be accounted for on each line of the import file.

The Organization Administrator or User Administrator can use one of the following file import methods to set or reset a PIN.

- **Using the users list**

  1. From the Account Management portal, select the **Users** card, or click **Users > Users**.
  2. Click **Import**.
  3. In the Import Users window, browse to the CSV or the TXT file that contains the users list.
  4. Click **Import Users**.

  Note: The user receives an email with the PIN.

- **Using Manage Badge/PIN**

  1. From the Account Management portal, click **Users > Manage Badge/PIN**.
  2. Click the **PINs** tab.
  3. Click **Import** or **Import PINs**.
  4. In the Import PINs window, browse to the CSV or the TXT file that contains the PINs.
  5. Click **Import PINs**.

  Note: The user receives an email with the PIN.

- How PIN data in the imported file is used depends on the PIN generation options selected on the Printer Login Configuration page.
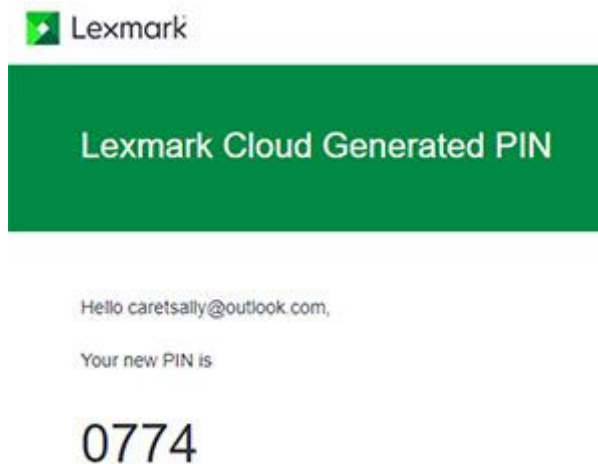
  - If the Automatically generate and email option is selected , then PIN values in the imported file are ignored. Lexmark Cloud Services automatically creates a PIN for each user in the file.
  - In the Administrator manually set option is selected , then users are assigned the PIN value associated with their entry in the imported file.

Setting PIN expiration

Administrators can select whether PINs will expire and how long before they expire by clicking **Organization > Printer Login Configuration**. If a PIN expires, then you must use one of the methods to reset the PIN. The PIN expiration and reset options depend on the selected PIN generation options.

- **Automatically generate and email**—You cannot set an expiration for the PINs.

PIN Generation Options

Automatically generate and email ▾

An auto generated PIN will be sent to users via e-mail. A user may request a new PIN.

- **Administrator manually set or User set**—You can set the PIN to never expire or to expire after 1 to 48 hours or 1 to 180 days.

PIN Generation Options

Administrator manually set ▾

Administrator sets the PIN when importing users. A user cannot reset the PIN.

◯ Never expires
◉ Expires after
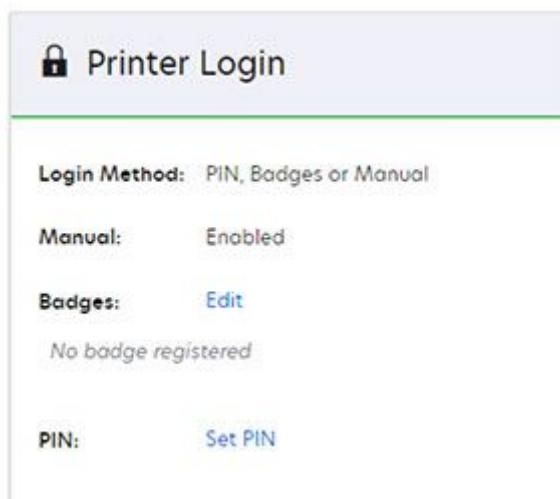
| — | 5 | + |

Range 1 to 180

day(s) ▾
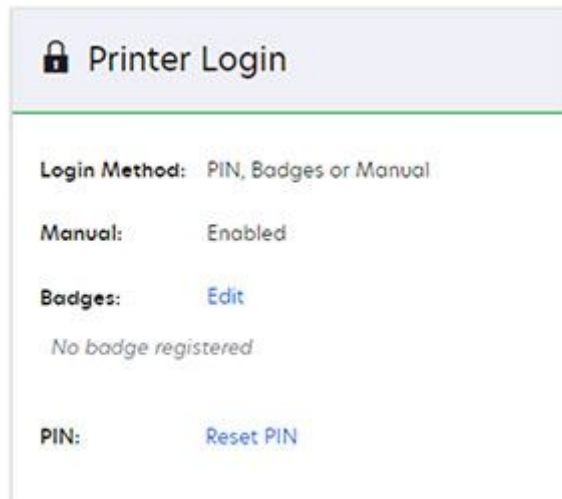
PINs assigned by the user

Users can set or reset their PINs from their My Account page.

- From the username menu, select **My Account**. In the Printer Login section, you can view following:

  ◦ Set PIN
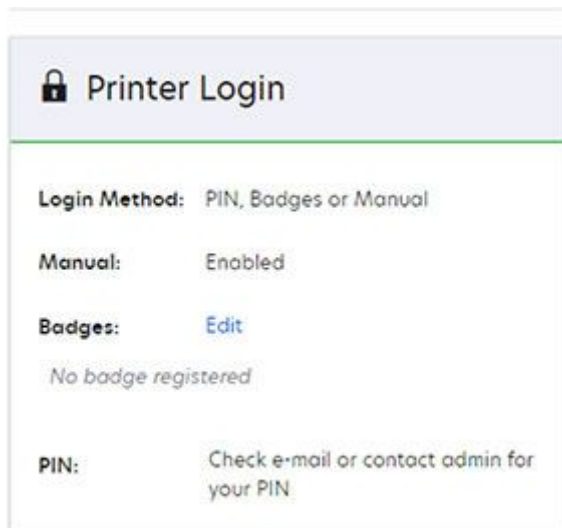
🔒 **Printer Login**

Login Method: PIN, Badges or Manual

Manual: Enabled

Badges: Edit
No badge registered

PIN: Set PIN

◦ Reset PIN

◦ Check e-mail or contact administrator for your PIN

Note: If you do not currently have a PIN, then in the Printer Login section, click **Set PIN**. If you currently have a PIN, then click **Reset PIN**.

Setting and resetting the PIN

Depending on the selected PIN generation option, clicking **Set PIN** or **Reset PIN** results in either of the following

- If PIN Generation Options is set to **Automatically generate and e-mail**, then Lexmark Cloud Services generates and emails a new PIN to the user.
- If PIN Generation Options is set to **User set**, then users are allowed to manually set or reset their PINs. They can do this task by entering a PIN with the required number of digits, and then clicking **Generate PIN**.

Note: If "Check e-mail or contact admin for your PIN" appears, then it means that PIN generation is manually set by the administrator. To set or reset their PIN, users must submit a request outside of Lexmark Cloud Services to an Organization Administrator or a User Administrator.

Modifying user information

If Identity Federation is used, then user information is retrieved from your authentication provider through claims. Any changes made to this data in Lexmark Cloud Services are overwritten when the user logs in for the next time.
If Identity Federation is not used, or if claims from your authentication provider do not work, then modify user information by doing one of the following:
Manually modify user information in the Account Management portal
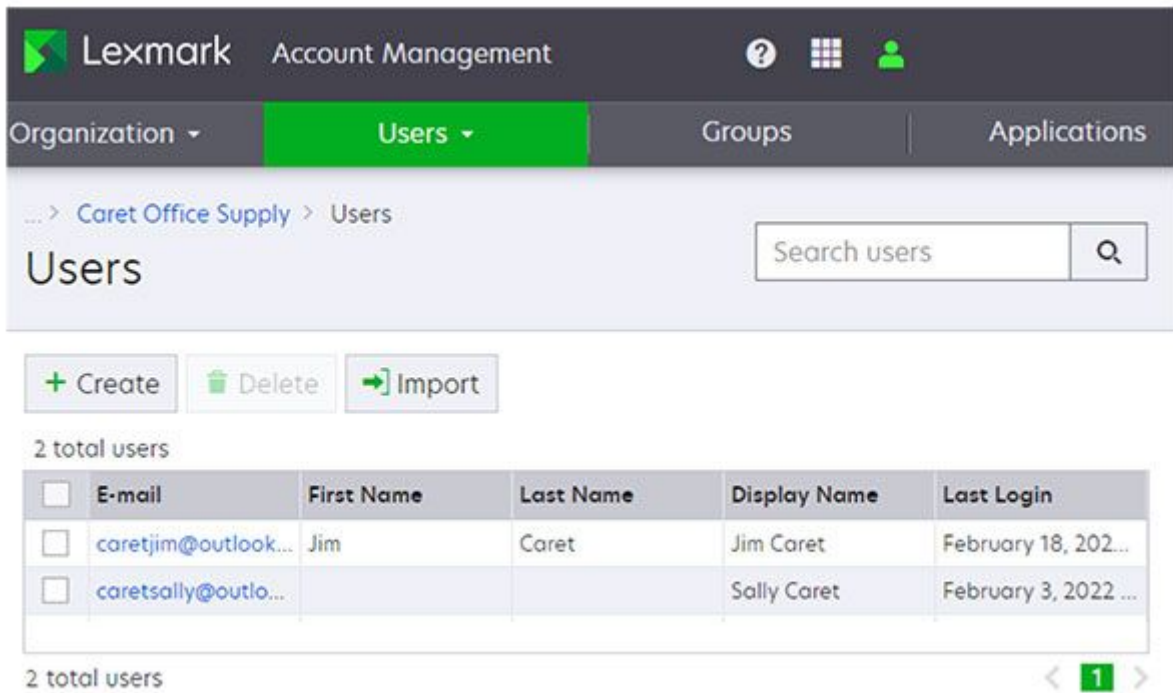
1. From the Account Management portal, select the **Users** card or click **Users > Users**.

2. In the E-mail column, click the user email.

3. In the Personal Information section, click **Edit**.

4. In the Personal Information page, enter the information, and then click **Update Profile**.

Import changes to user information using a CSV file

Use this method if you want to modify multiple user accounts simultaneously. The Import feature lets you create, update, and delete multiple users in an organization using a CSV or TXT file. You can also create user groups, and then assign a user to those groups. For more information, see "Managing users" topic in *Lexmark Cloud Services Administrator's Guide*.

When importing, note the following:

- Use the UPDATE command to modify the information of an existing user account.
- The headers of the import file are case-sensitive.
- Count the commas. All columns must be accounted for each line of the CSV file.
- The size of the CSV file must not exceed 1MB.

Deleting user accounts

If Identity Federation is used, then a user's account can only be permanently deleted from your authentication provider. A user account that is deleted only from Lexmark Cloud Services is restored when the user logs in the next time.
If Identity Federation is not used, then you can delete user accounts by doing one of the following:
Manually delete the user account in the Account Management portal

1. From the Account Management portal, select the **Users** card or click **Users > Users**.

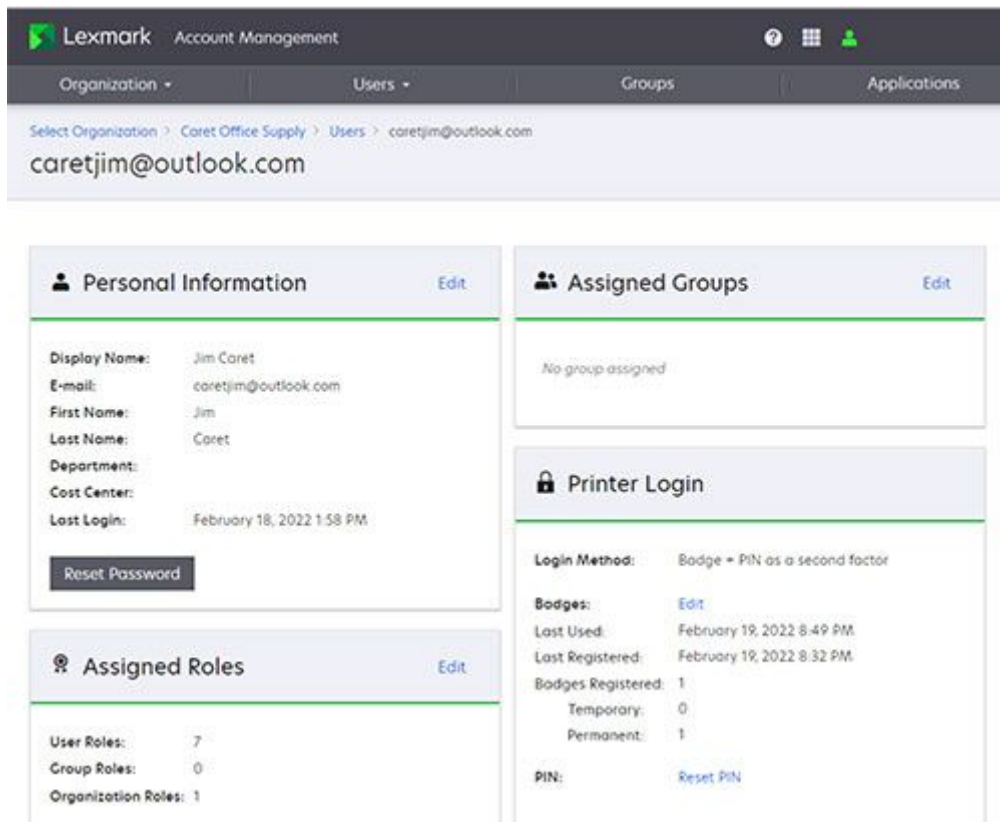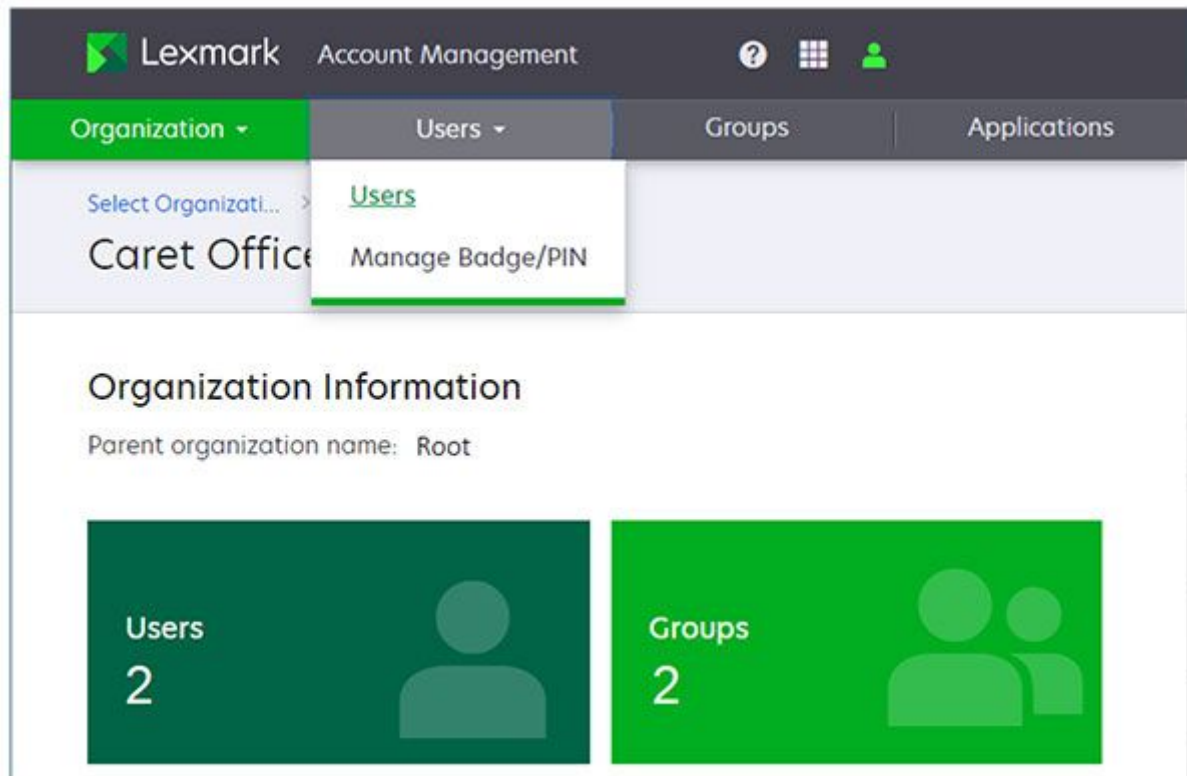2. Select the user, and then click **Delete**.
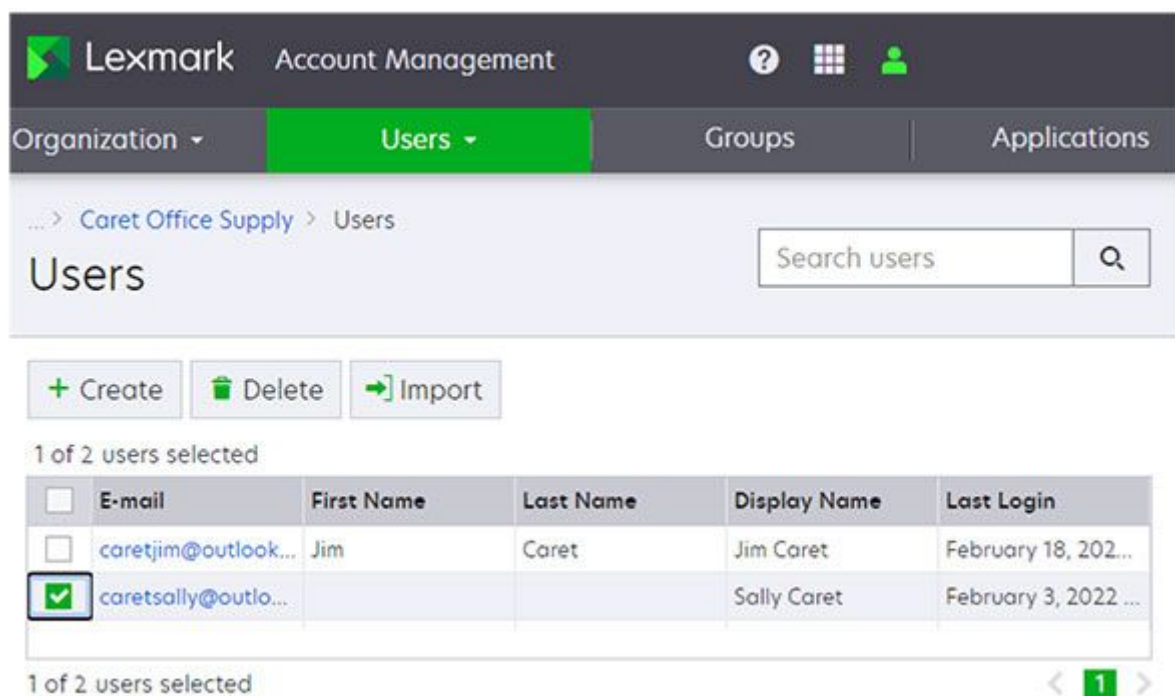
3. Click **Delete User**.

Delete user information by importing a file in the Account Management portal

For more information, see "Managing users" in *Lexmark Cloud Services Administrator's Guide*.

Enroll your printers

Fleet Management roles

The Fleet Management Administrator and File Service Administrator roles must be assigned to users who access the Fleet Management portal and enroll and manage printers

> **Note:** You must have the User Administrator or Organization Administrator role to assign these roles to users.

Fleet Management roles for channel partners

Channel partners who manage printers in their customers' organizations must be members of a Child Organization Access Group. The group must have the Fleet Management Administrator and File Service Administrator roles assigned to it.

> **Notes**
>
> - You must have the User Administrator or Organization Administrator role to create and manage Child Organization Access Groups.
> - Roles assigned through membership in a Child Organization Access Group apply across all customer organizations.

Creating Child Organization Access Groups

1. From the Account Management portal, click **Groups** tab.
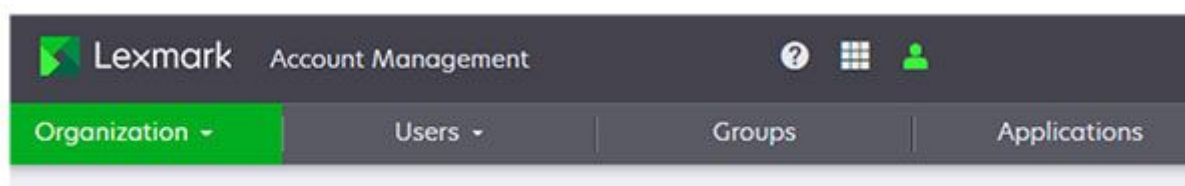
2. Click the **Child Organization Access** tab.

3. Click **Create**.
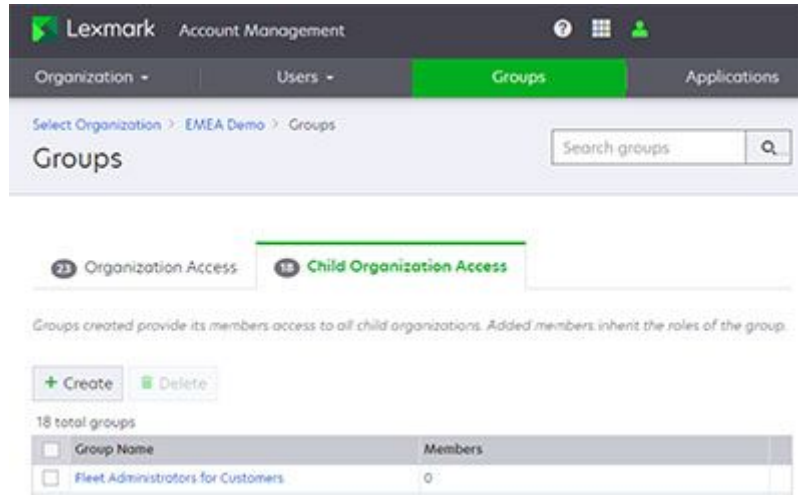
4. In the Group name field, type the name of the group, and then click **Create Group**.
5. Click the name of the group.
6. Click **Add** or **Add Members**.
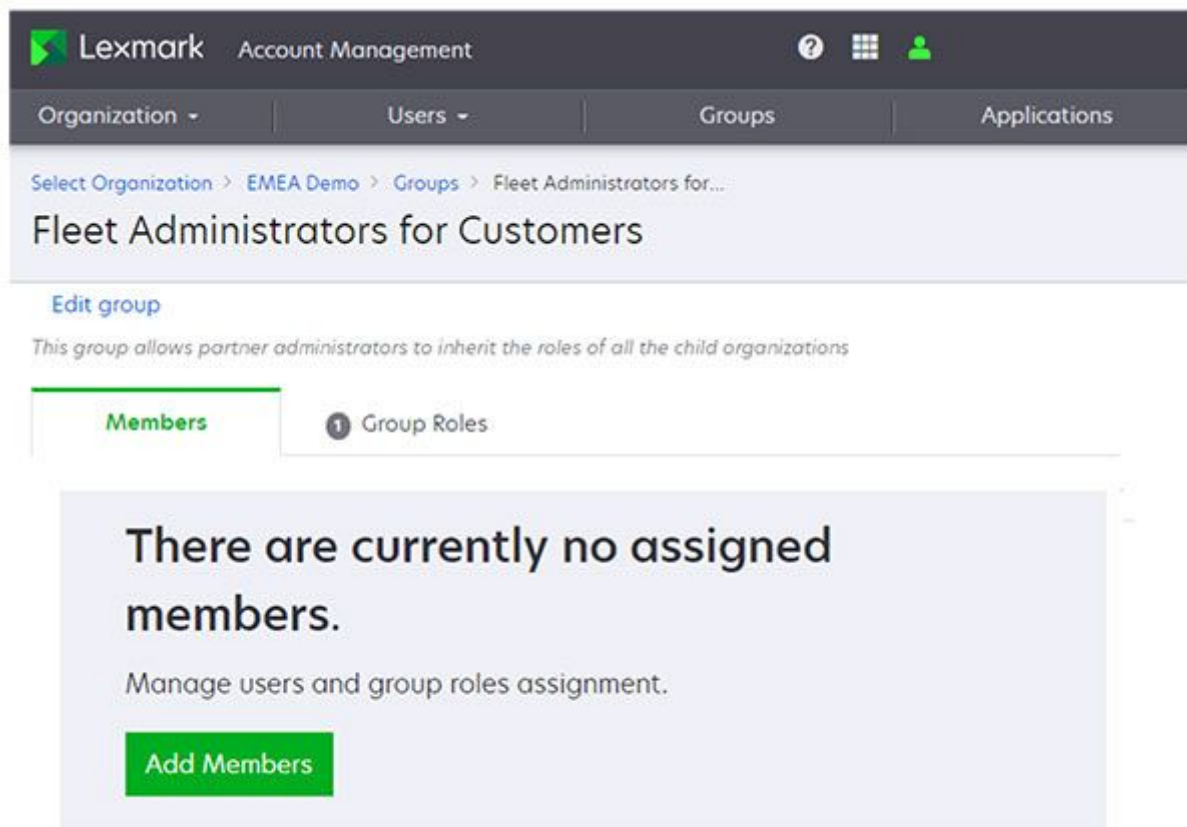
7. Select one or more members, and then click **Add Members**.
8. Click the **Group Roles** tab.
9. Click **Assign**.

> **Note:** By default, the Partner Administrator role is assigned to all Child Organization Access Groups.
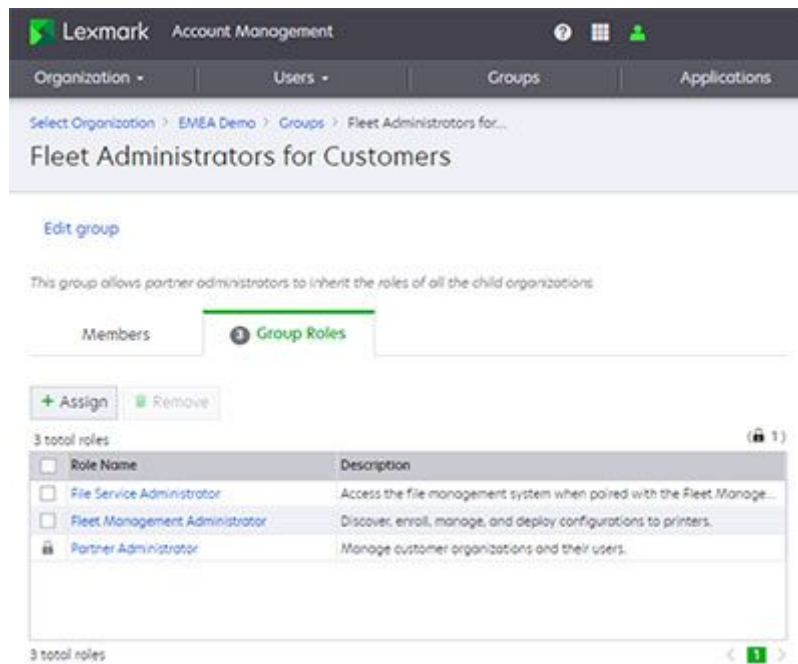
10. From the Custom Roles list, select **Fleet Management Administrator** and **File Service Administrator** roles, and then click **Assign Roles**.

Selecting an agent

The first step in enrolling printers is to decide which agent or agents to use. You may choose from the Native Agent, Fleet Agent, Printer Agent, or Local Agent.

Note: Collectively, the agents are referred to as Cloud Bridge.

Native Agent

The Native Agent is built into the printer firmware. It is available on all current-generation Lexmark printers. The control panel on current-generation Lexmark printers has a dark background.

Sample of the control panel from a current-generation printer that supports the Native Agent.
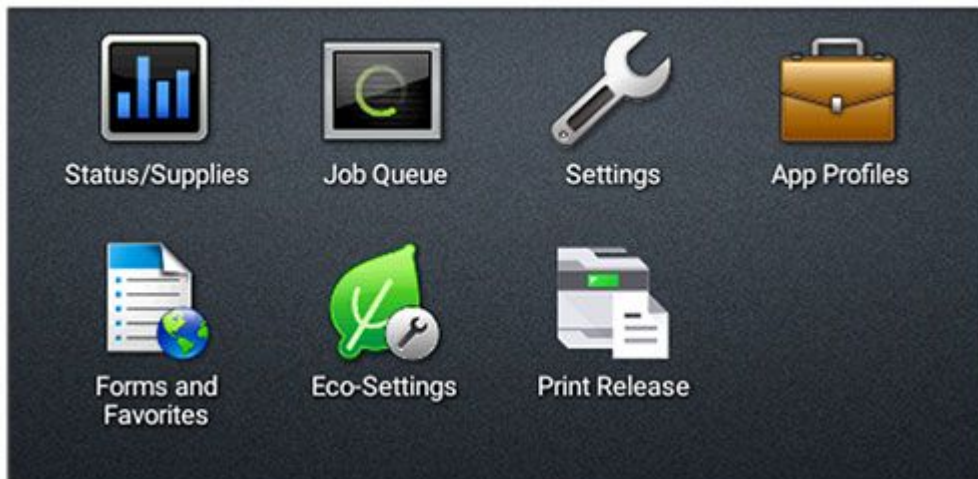
- Requires firmware 081.215 or later is required. For more information, see "Viewing the printer firmware version" topic in *Lexmark Cloud Services Administrator's Guide*.
- Supports data collection and configuration on all current generation printers.
- Supports the deployment of eSF applications on current generation, touch-screen printers. For more information, see "Supported printer models" topic in *Lexmark Cloud Services Administrator's Guide*.
- Native Agent–capable printers can be enrolled using the following methods:

    ◦ Cloud-based pre-enrollment
    ◦ Printer-based enrollment
    ◦ Printer Enrollment Tool (PET)
- Requires the printers to have a constant Internet connection.
- Uses Internet of Things (IoT) technology to reports printer data to the cloud.

Fleet Agent

The Fleet Agent is an application that is configured and installed on an on-site server or host computer. It enrolls Lexmark and third-party printers to the Lexmark Cloud Services.

- Uses Internet of Things (IoT) technology to report printer data to the cloud.
- Requires a stable, high-availability server or host computer with a constant Internet connection and with the following minimum specifications:

Operating system	x86, x64-bit or Linux 64-bit
Processor	1Ghz dual-core
RAM	2GB

Storage	32GB (Fleet Agent requires 12GB of storage)

- Supports printer configuration and data collection with Lexmark printers. For more information, see "Supported printer models" topic in *Lexmark Cloud Services Administrator's Guide*. Data collected and printer configuration capabilities may vary by model.
- Data is collected over Simple Network Management Protocol (SNMP) from the public and private printer MIBs available on the enrolled printers.
- Supports data collection for some third-party printers. Data collected varies by manufacturer and model.

Printer Agent

Printer Agent

The Printer Agent, also referred to as embedded agent, uses an embedded application, the Printer Configuration Agent (PCA), installed on each Lexmark printer. The Printer Configuration Agent collects and sends the printer information to Lexmark Cloud Services.

- Requires running the Printer Enrollment Tool on a network connected computer to discover and enroll printers.
- Supports data collection and configuration on Lexmark touch-screen printers with eSF version 3.0 or later. For more information, see "Supported printer models" topic in *Lexmark Cloud Services Administrator's Guide*.
- Requires the printers to have a constant Internet connection.
- Uses Internet of Things (IoT) technology to report asset inventory (meters, counters, and supplies) data. If the IoT hosts are blocked during enrollment, then this agent reverts to the https path.

Local Agent

Local Agent

The Local Agent is an application configured and installed on a Windows computer system that has USB-attached printers. It enrolls locally attached Lexmark printers into Lexmark Cloud Services. It uses an Internet of Things (IoT) connection to communicate with Lexmark Cloud Services.

- Automatically discovers and enrolls USB-connected, Lexmark printers.
- Uses Internet of Things (IoT) technology to report asset inventory (meters, counters, and supplies) data.
- Supports Windows 64-bit and 32-bit operating systems.

Comparing agents

To make sure that you have an optimal experience in enrolling and managing your print fleet, select the correct agent for your specific needs.

- If managing a current-generation Lexmark touch-screen printer with eSF version 5.0 or later, then use the Native Agent, Fleet Agent, or Printer Agent.

- If managing Lexmark touch-screen printers with eSF version 3.0 or later, then use either the Printer Agent or the Fleet Agent.
- If managing a group of touch-screen and non-touch-screen Lexmark printers, then use the Fleet Agent.
- If managing a group of Lexmark and third-party printers, then use the Fleet Agent.
- If managing USB-connected Lexmark printers, then use the Local Agent.
- If eSF applications cannot be installed on the printers to be managed, then use the Fleet Agent.
- If an on-site server or host computer cannot be used, then use either the Printer Agent or the Native Agent.
- All agents may be used in the same organization at the same time.
- A printer can only be managed by one agent.

Scenario	Native Agent	Fleet Agent	Printer Agent	Local Agent
Uses an agent native to printer firmware	✓	X	X	X
Uses an application running on an Internet-connected, on-site server or host computer	X	✓	x	X
Uses an embedded application running on enrolled printers	X	X	✓	X
Supports USB-connected printers	X	X	X	✓
Internet connection required for printers	✓	✓	✓	X
Uses Internet of Things (IoT) technology	✓[1]	✓[3]	✓[2]	✓[2]
Supports data collection and configuration in Lexmark printers with eSF version 5.0 or later (touch-screen models)	✓[4]	✓[4]	✓[4]	X

Scenario	Native Agent	Fleet Agent	Printer Agent	Local Agent
Supports data collection and configuration in Lexmark printers with eSF version 3.0 (touch-screen models)	**X**	✓ [4]	✓ [4]	**X**
Supports data collection and configuration for Lexmark printers with eSF version 2.0	**X**	✓ [4]	**X**	**X**
Supports data collection for non-eSF Lexmark printers	✓ [4]	✓ [4]	**X**	✓ [5]
Supports data collection from third-party printers	**X**	✓	**X**	**X**
Requires a user account on the printer with administrative access	**X**	**X**	✓	**X**
Performs data collection over SNMP	**X**	✓	**X**	**X**

[1] All printer-cloud communications use IoT. IoT support is resident in the printer firmware.

[2] IoT default communications path for asset inventory (meters and counters) data. If IoT connection cannot be established, then an https path is supported.

[3] All cloud communications use IoT.

[4] For more information, see "Supported printer models" topic in *Lexmark Cloud Services Administrator's Guide*.

[5] When the printer is connected to a workstation through USB.

Before enrolling

To make sure that the enrollment of printers is successful, do the following::

- Make sure that the printer to be enrolled supports the agent to be used. For more information, see "Supported printer models" topic in *Lexmark Cloud Services Administrator's Guide*.
- If a firewall or proxy is used, then add the proper host names to the Allow List.
- If the printer was previously used at another customer site, then unenroll the printer from its current organization in the Cloud Fleet Management portal. If necessary, also erase the printer memory.

   When erasing printer memory, note the following:

   ○ Unenrolling must be performed the first time a printer is enrolled with a customer.
   ○ Any configuration settings or customer data related to a prior installation is deleted. For more information, see Erasing printer memory.
- Make sure that all printers are online and in the Ready state with no unresolved errors, such as paper jams or incorrect email configurations.
- The printer firmware is updated to the latest recommended version.
- Printer permissions are set correctly.
- Printer login credentials for secure printers are available.
- Printer SNMP configurations are available.

   ○ When using the Fleet Agent, SNMP v3 must be enabled on eTask version 5.0 and higher printers.
   ○ By default, SNMP v3 must be enabled on these models.
   ○ SNMP v3 does not have to be configured. It must be enabled.
- Make sure that Firewall, DHCP, and DNS settings are correct.
- The date and time are configured correctly, preferably using a network time protocol server.
- If possible, enroll printers during off hours when the printers are not being used.

   ○ Firmware and configuration deployments from Cloud Fleet Management following enrollment may briefly take the printer offline.

Using the Native Agent

Enrolling printers with Native Agent

The Native Agent is available on all current-generation Lexmark printers that are Internet of Things (IoT)–capable. It is built into the firmware for any printer running firmware version 075.272 or later. The Native Agent can be used to enroll Lexmark printers in Lexmark Cloud Services. No applications are required to be installed on the printer or to run on an on-premises server or hosted computer. The printer must have a constant Internet connection. For more information on supported models, see "Supported printer models" topic in *Lexmark Cloud Services Administrator's Guide*.

You can enroll printers with the Native Agent using the Printer Enrollment Tool (PET), cloud-based pre-enrollment, or printer-based enrollment.

- **Printer Enrollment Tool**—Can be used to enroll any current-generation IoT-capable Lexmark printers. If you are unable to enroll the printer using the Cloud-based pre-enrollment or printer-based enrollment methods, then PET must be used.
- **Cloud-based pre-enrollment**—Lets you specify Lexmark printers that you want to enroll. In this process, you enter an enrollment code at the printer. The enrollment code is obtained from the Fleet Management portal for an organization and can be used to enroll all pre-enrolled printers for that organization. The list of pre-enrolled printers can be entered one at a time or imported from a CSV or TXT file before going on-site. This method is useful for large printer deployments because you can perform much of the needed work in advance.

- **Printer-based pre-enrollment**—Lets you initiate the enrollment at the printer. You obtain an enrollment code from the printer and enter it in the Fleet Management portal. This method is useful if you are deploying only a few printers or do not know in advance the serial numbers of the printers to be deployed.

Enrolling printers using the Printer Enrollment Tool

The Printer Enrollment Tool (PET) can be used to enroll any current-generation IoT-capable Lexmark printers with the Native Agent. Use this method when enrolling older models of the current-generation printers or if you cannot enroll printers using the cloud-based pre-enrollment or printer-based enrollment methods.

Downloading the Printer Enrollment Tool

If you do not have a copy of the PET, download it from the Cloud Fleet Management portal.

1. From the Fleet Management web portal, do one of the following:

   ○ If some printers are already enrolled, then click **Printers > Enroll Printer using > Printer Agent > Download PET**.
   ○ If enrolling printers for the first time, then click **Use Printer Agent > Download PET**.

2. Accept and download the End User License Agreement (EULA).
3. Extract the compressed folder.

Using the Printer Enrollment Tool

1. Run the Printer Enrollment Tool launcher.
2. Log in using the same email address and password used to connect to the Cloud Fleet Management portal.

   > **Note:** If a newer version of the PET is available, then you will be prompted to download it.

   Update Available

   A new version of this tool has been released.

   Download New Version

3. If you manage multiple organizations, then select the organization, and then click **Next**.

4. Click ⚙ on the upper-right corner of the page, and then configure the following:

   ○ **Discover and enroll native agent-capable printers using**—Determines whether Native Agent-capable printers are enrolled using the Native Agent or Printer Agent.

◦ **Time out for Printer Discovery**—Determines how long the PET waits for a response to each network broadcast. The value can be increased to improve printer discovery in slow networks.

◦ **Time out for Printer Enrollment**—Determines how long the PET waits for the Printer Agent to enroll the printer. The value can be increased to improve the printer enrollment process of older printers.

◦ **Logging detail levels**—Set the logging level to **Detailed**.

◦ **SNMP settings**—The SNMP settings in the PET must match those of the printers to be discovered.

> **Note:** Printer discovery first occurs using mDNS, and then by Simple Network Management Protocol (SNMP). If SNMP discovery is desired, then mDNS must be disabled on the printers.

5. From the Discovery Type menu, select any of the following:

- ◦ **Search local network**—Finds all printers on your local subnet. Use this method if you have several printers on the subnet but you do not know their network parameters. This method may take several minutes to complete.
- ◦ **Advanced search**—Lets you refine the search by specifying network parameters to find printers. Use this method if you have a small number of printers or if the network parameters of the printers are known. This method is usually faster than the Search local network method.

  The following are the network parameters:

  - ▪ Specific IP address
  - ▪ Subnet
  - ▪ Range
  - ▪ Fully qualified domain name (FQDN)

Notes
- ◦ To discover printers successfully, make sure that mDNS is enabled on the printer or that the SNMP configurations of the PET and the printers match.
- ◦ Printers in the Eligible to Enroll tab can be enrolled with the Native Agent if their agent type is set to Native.

	Address	▲	Model	Serial Number	Agent Type	Info
☐	192.168.86.22		Lexmark CS725	5028551010011	Native	❶
☐	192.168.86.29		Lexmark MX410de	7015207200004	Printer	❶

6. Select one or more printers to enroll, and then click **Enroll Printers**.

   Note: The selected printers do not have to be of the same agent type. Each selected printer is enrolled using the indicated agent type.

7. If necessary, log in to access the printer Embedded Web Server, and then click **Apply Credentials**. Otherwise, click **Skip This Step**.

   Note: Login credentials can be applied to limit access to printer settings to authorized individuals only.

Cloud-based pre-enrollment

Cloud-based Native Agent pre-enrollment lets you specify in advance the Lexmark printers that you want to enroll. You only need to enter an enrollment code at the printer. The enrollment code is obtained from the Fleet Management portal for an organization and can be used to enroll all pre-enrolled printers for that organization. The list of pre-enrolled printers can be entered one at a time or imported from a CSV or TXT file. This method is useful for large printer deployments.
Pre-enroll printers by doing the following:

- Entering their serial number in the Cloud Fleet Management portal
- Obtaining the organization's enrollment code
- Applying the organization's enrollment code to the printer, using the control panel or the Embedded Web Server (EWS)
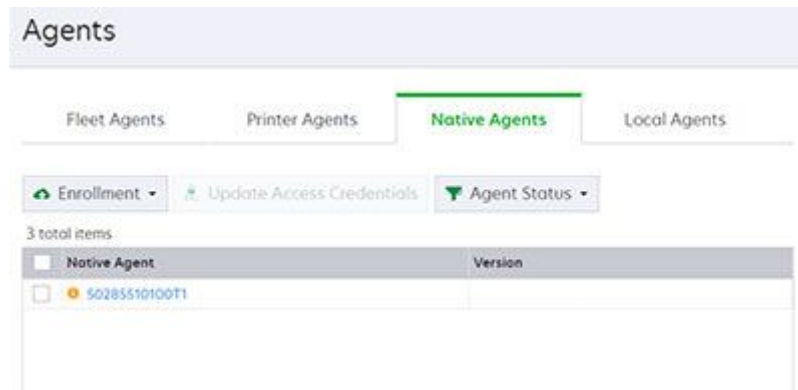
   Note: Cloud-based pre-enrollment is supported only in current-generation IoT-capable Lexmark printers. If enrollment using this method is unsuccessful, then enroll using the Printer Enrollment Tool.

Entering printer serial numbers in the Cloud Fleet Management portal

printer-serial-number2

1. From the Fleet Management web portal, do one of the following:

◦ If some printers are already enrolled, then click **Agents > Native Agents > Enrollment > Pre-enroll > Pre-enroll printers**.

Agents

Fleet Agents	Printer Agents	Native Agents	Local Agents

☁ Enrollment ▾   ⚡ Update Access Credentials   ▼ Agent Status ▾

3 total items

☐	Native Agent	Version
☐	⚠ 50285510100T1	

◦ If enrolling printers for the first time, then click **Agents > Native Agents > Pre-enroll Printers**.

Agents

Fleet Agents	Printer Agents	Native Agents	Local Agents

There are no native agents.

A native agent is included as part of the firmware for Lexmark printers that are Internet of Things (IoT) capable. When enabled, it can enroll the Lexmark printer to LCS. It also acts as the communication channel between the printer and the cloud.

[Pre-enroll Printers]   [Enroll Printer]
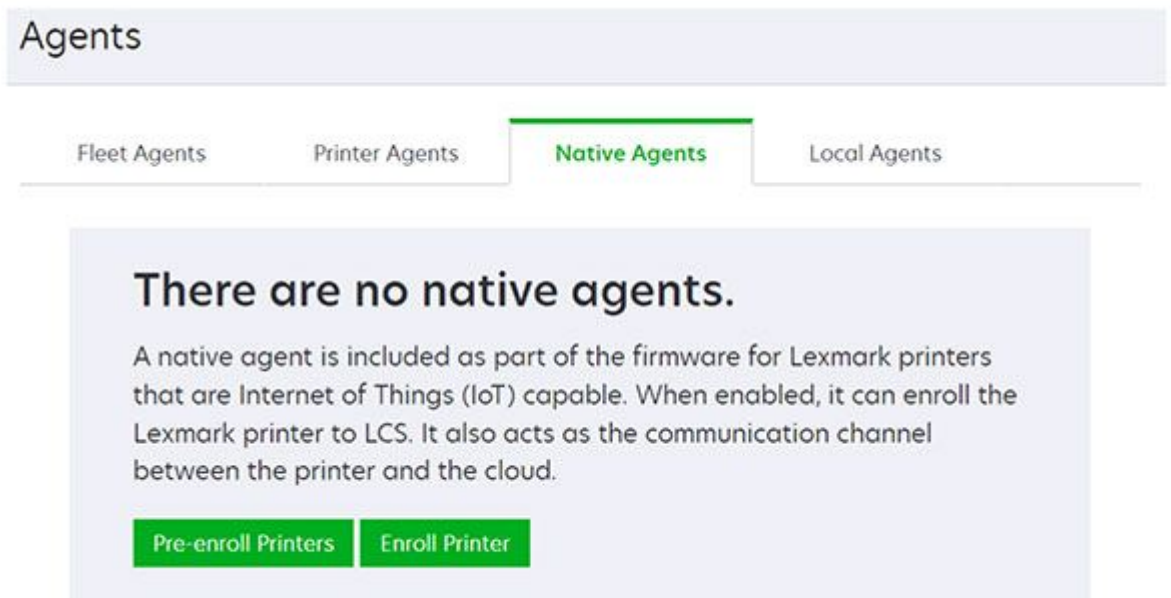
2. From the Pre-enroll Printers dialog, do one of the following:

◦ Select **Manually input serial number**, type the printer serial number, and then press **Enter**.
◦ Select **Import printer serial number from file**, and then browse to the CSV or TXT file.
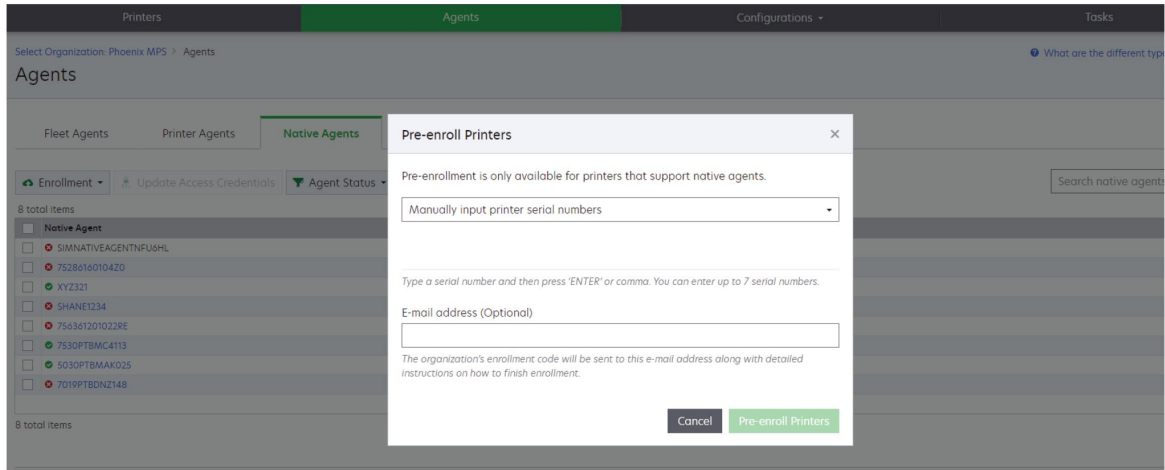
> **Note:** To receive the enrollment code and the complete enrollment instructions using email, type your email address.

Once pre-enrolled, the printer serial number is listed on the Native Agent page with a Printer pre-enrolled icon.
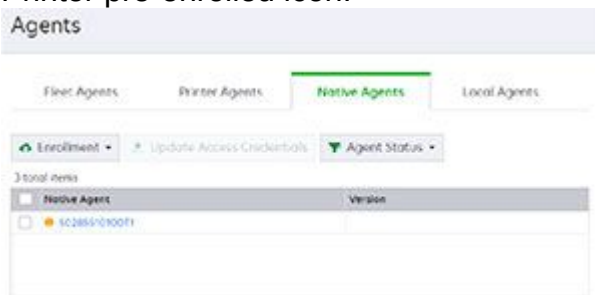
Obtaining the enrollment code

1. Click **Agents > Native Agents > Enrollment > Pre-enroll**.

2. Copy the organization's enrollment code.

Note: You can also obtain the enrollment code by clicking the pre-enrolled serial number. The code can be found in the Printer Information section.

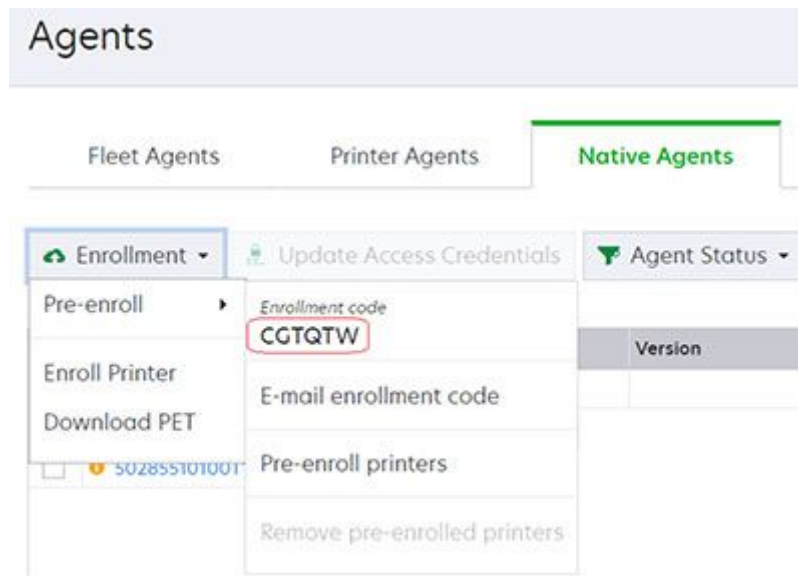**Note:** If the Enrollment menu is not visible, or there are no printer serial numbers listed, then no printers have been pre-enrolled. For more information, see .

Applying the enrollment code to the printer

- **Using the control panel**

    1. From the printer home screen, touch **Settings > Cloud Services > Cloud Services Enrollment**
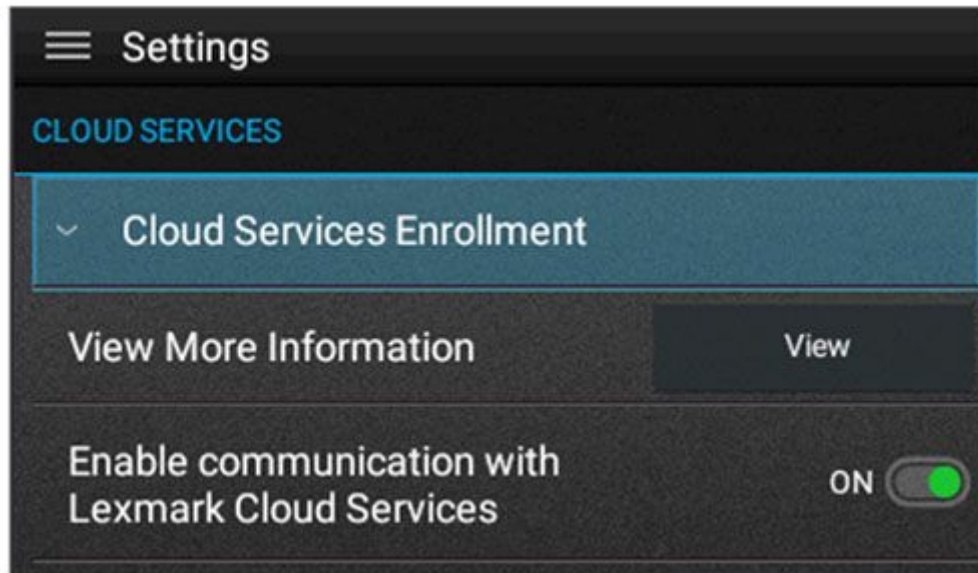
2. From the Enable communication with Lexmark Cloud Services menu, touch **On**.
3. Touch **Enroll Printer**, and then enter the enrollment code.
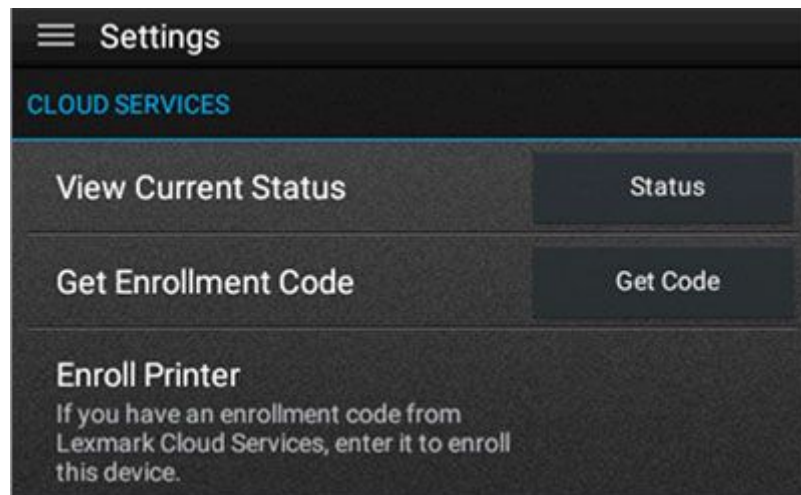
4. Touch **OK**

- **Using the Embedded Web Server**

   1. From the Embedded Web Server, click **Settings > Cloud Services > Cloud Services Enrollment**
   2. Select **Enable communication with Lexmark Cloud Services**, and then click **Save**.
   3. Click **Refresh** until the Enrollment Code field is visible. This may take a few minutes.
   4. In the Enrollment Code field, enter the enrollment code, and then click **Enroll Printer**.

   Notes
   - The enrollment code is case-sensitive.
   - The enrollment can be verified from the Cloud Fleet Management portal.
   - It may take a few minutes for the printer enroll.

Printer-based enrollment

Printer-based enrollment begins at the printer. You obtained an enrollment code from the printer, and enter it in the Fleet Management portal. This method is useful if you plan to only deploy a few printers or if you are unaware of the printer's serial number. Printer-based enrollment involves:

1. Obtaining the printer's enrollment code.

> **Note:** This is done from the printer control panel or using its Embedded Web Server (EWS).

2. Entering the printer's enrollment code in the Cloud Fleet Management portal.

> **Note:** The printer-based enrollment method is only supported for current generation Lexmark IoT-capable printers. If enrollment using this method is unsuccessful, then enroll using the Printer Enrollment Tool.

Obtaining the enrollment code

There are two methods for obtaining the printer enrollment code.

- Using the control panel of the printer
- Using the Embedded Web Server

### Obtaining enrollment code by using the control panel

1. From the printer home screen, touch **Settings > Cloud Services > Cloud Services Enrollment**
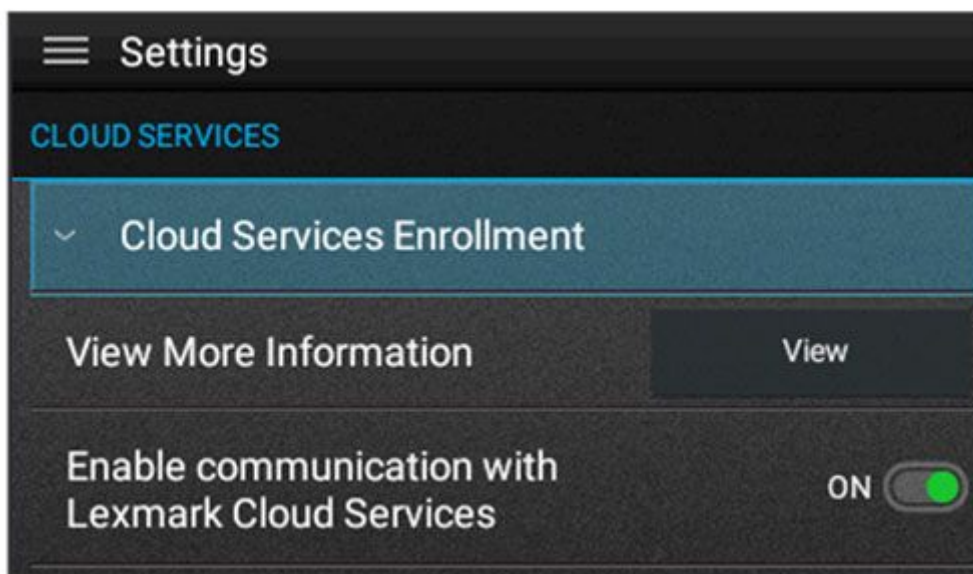
2. From the Enable communication with Lexmark Cloud Services menu, touch **On**.
3. From the Get Enrollment Code menu, touch **Get Code**, copy the enrollment code, and then touch **OK**.
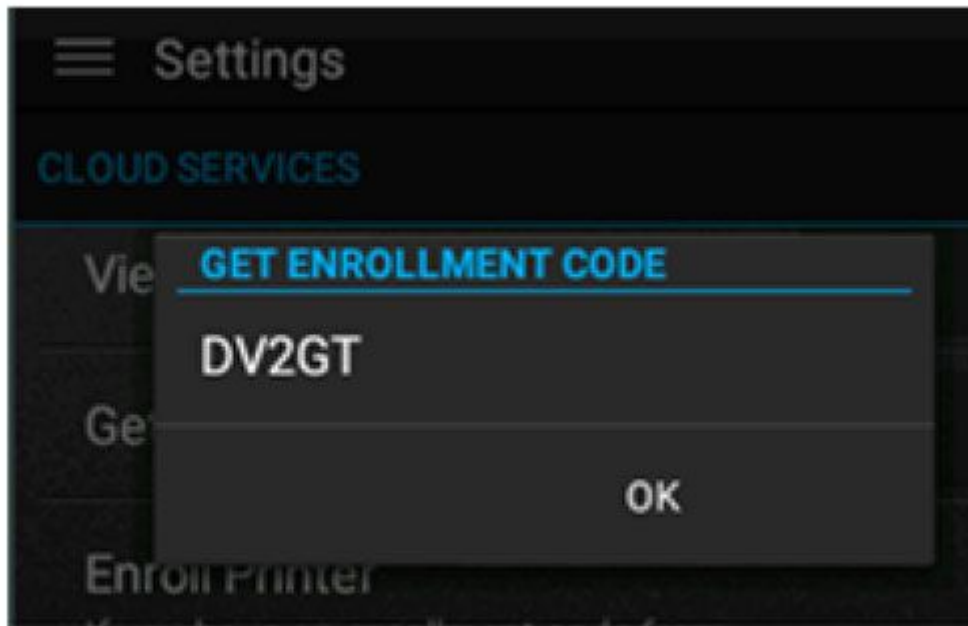
Obtaining the enrollment code by using the Embedded Web Server

1. From the Embedded Web Server, click **Settings > Cloud Services > Cloud Services Enrollment**.
2. Select **Enable communication with Lexmark Cloud Services**, and then click **Save**.
3. Click **Refresh** until the Get Enrollment Code is enabled. This may take a few minutes.
4. Click **Get Enrollment Code**, and then take note of the code.

Entering printer serial numbers in the Cloud Fleet Management portal

printer-serial-number

1. From the Fleet Management web portal, do one of the following:

   If no devices are enrolled:

   ◦ Click **Agents > Native Agents > Enroll Printer**.

If devices are already enrolled:

- ○ Click **Agents > Native Agents > Enrollment > Enroll Printer**.

2. Enter the enrollment code, and click **Enroll Printer**.

> **Note:** The enrollment code is case-sensitive.

> **Note:** In case of invalid code, you will get an error message.

Using the Fleet Agent

Creating a Fleet Agent

Before using Fleet Agent, you must create an agent and establish settings that work best for your environment.

1. From the Fleet Management portal, click **Agents > Fleet Agents > Create Fleet Agent**.
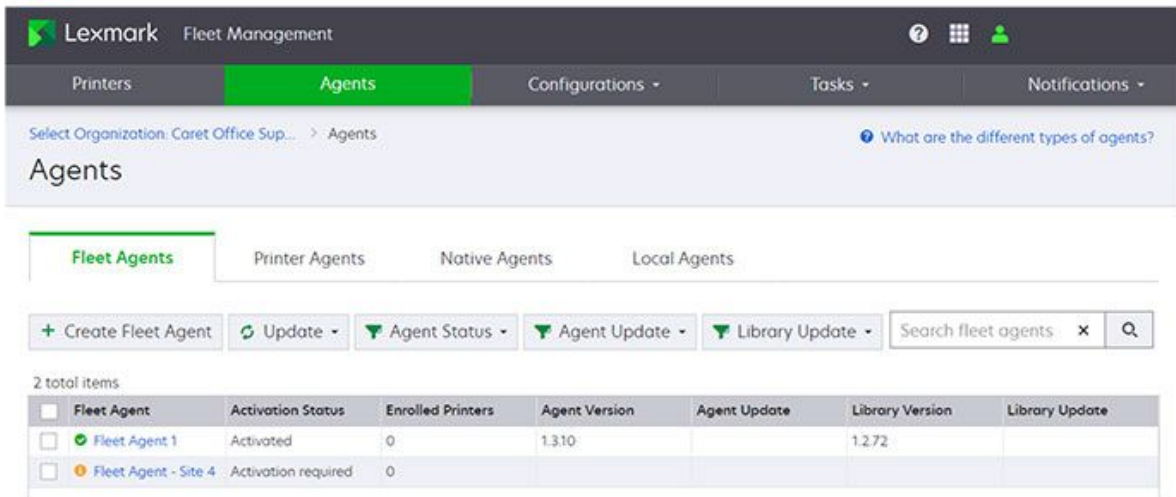
2. In the Create Fleet Agent form, configure the following:
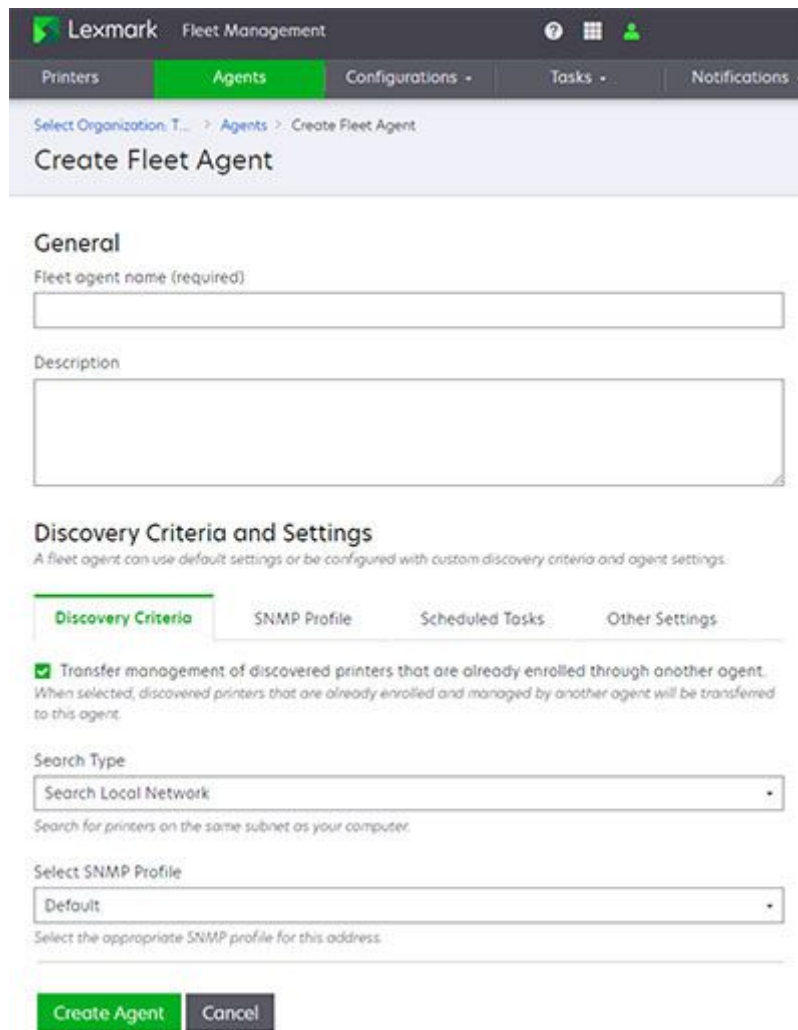
- ◦ **General**—Type a name and description for the Fleet Agent.
- ◦ **Discovery Criteria and Settings**:

  - ▪ **Discovery criteria**:

    - ▪ **Transfer management of discovered printers that are already through another agent**—Transfer all discovered printers that are already enrolled under another agent to this Fleet Agent. If not selected, then discovered

printers that are already enrolled under another agent will remain enrolled under their current agent.

> **Note:** Prevent overlapping Discovery Criteria between Fleet Agents. Overlapping criteria cause printers to switch between Fleet Agents.

▪ **Search Type**—Select the type of discovery to be done.

Discovery Criteria and Settings
A fleet agent can use default settings or be configured with custom discovery criteria and agent settings.

| Discovery Criteria | SNMP Profile | Scheduled Tasks | Other Settings |

☑ Transfer management of discovered printers that are already enrolled through another ag
When selected, discovered printers that are already enrolled and managed by another agent will be trans to this agent.

Search Type

Search Local Network

Search Local Network

Advanced Search

▪ **Search Local Network**—Search the local network subnet for printers. If the printers to be discovered have SNMP configured, then a matching SNMP profile must be added to the Fleet Agent configuration.

> **Note:** The Fleet Agent discovers only printers that match its SNMP profile.

▪ **Advanced Search**—Search or exclude printers by specific IP address, subnet, range, and fully qualified domain name (FQDN). If the printers to be discovered have SNMP configured, then a matching SNMP profile must be added to the Fleet Agent configuration.

   ▪ You can click **Add Discovery Criteria to Include** to enter the search criteria and select an SNMP profile. Repeat the process for each search criteria. After adding the search criteria, click **Add Discovery Criteria.**

> **Notes**
> - The Fleet Agent discovers only printers that match its SNMP profile.
> - If printers in the search criteria have different SNMP configurations, then the search criteria can be entered multiple times, each with a different SNMP profile.
> - A printer can be managed by only one agent. Care must taken when defining the Printer Discovery settings when using Native Agent, a Printer Agent, and a Fleet Agent, or multiple Fleet Agents within the same organization. If overlapping Printer Discovery criteria exist, then printers may not be managed by the intended agent. The printer data may roll up under the wrong agent and may appear to unenroll and re-enroll continually.

- You can click **Import** or **Export** to import or export functions to use predefined search criteria or saved search criteria for later use.
- **SNMP Profile**—Can be created to match the SNMP configuration of printers discoverable by the Fleet Agent. You can click **Create** to create profiles. Profiles can be created based on SNMP v1, v2c, or v3. The SNMP profile created and used by a Fleet Agent must match the SNMP configuration of the printers that the Fleet Agent manages.

Discovery Criteria and Settings

A fleet agent can use default settings or be configured with custom discovery criteria and agent settings.

| Discovery Criteria | **SNMP Profile** | Scheduled Tasks | Other Settings |

+ Create

NOTE: The default profile can be edited but not deleted.

Profile Name	Version	Discovery Timeout (secon...	Retries (number)
Default	V1	15	1
Site 1	V3	15	3

Create SNMP Profile   ✕

Profile name

SNMP Profile 1

SNMP version

Version 1   ▾

Community name

Discovery timeout (seconds)

[−] 15 [+]

Amount of time to wait for a device to respond. Range: 1 - 60 seconds.

Number of retries

[−] 1 [+]

The number of attempts to communicate with a device. Range: 0 - 20 retries.

Cancel   Create SNMP Profile

Notes
- The Fleet Agent discovers printers that match its SNMP profile.
- An SNMP profile using SNMP v3 is not required by the Fleet Agent. However, SNMP v3 must be enabled on eSF version 5 or later printers released since 2016. An SNMP v3 profile does not need to be configured on these printers, but SNMP v3 must be enabled. If you do not enable SNMP v3, then the Fleet Agent cannot update firmware, applications, and configurations.

- **Scheduled Tasks**—Set up the Fleet Agent to periodically rediscover printers and to refresh printer information. Setting a discovery interval lets you automatically add or remove printers as they are added, exchanged, or removed.

Discovery Criteria and Settings

A fleet agent can use default settings or be configured with custom discovery criteria and agent settings.

| Discovery Criteria | SNMP Profile | **Scheduled Tasks** | Other Settings |

Tasks will be automatically performed on the displayed schedule. Schedules can be edited.

Printer Discovery Task

Set the interval to run a discovery task and enroll newly found printers.

Task interval

> Once a week ▾

Day of the week

> Sunday ▾

Time of day

> 1:17 PM   🕐

Task will be run as close to the selected time as system allows.

Refresh Printer Information Task

Set the interval to refresh printer information, including statuses, alerts and meters. For printers managed by a fleet agent, the Last Data Refresh column on the Printers page updates only if printer information has changed.

Task interval

> Every hour ▾

- **Printer Discovery Task**—Set the Fleet Agent to rediscover and enroll printers on a regular basis or only when manually directed from the Cloud Fleet Management portal.

  - **None (Run tasks manually only)**—Run manually.
  - **Once a day**—Set a specific time.
  - **Once a week**—Set a specific time on a selected day of the week.
  - **Once a month**—Set a specific time on the last day of the month or on a selected day of the month.
- **Refresh Printer Information Task**—Set the Fleet Agent to refresh printer information at certain intervals.

  - **Every 15 minutes**
  - **Every 30 minutes**
  - **Every hour**
  - **Every 2 hours**
  - **Every 6 hours**
  - **Every 12 hours**

> **Notes**
> - The default setting is 1 hour. A shorter interval provides a more current printer status but puts more traffic on the local network. A longer interval reduces the local network traffic, but provides a slower printer status update.
> - The Fleet Agent reports printer information to the Fleet Management services if a page count change occurs. It also reports or when a printer or supplies alert has been detected.

- **Other Settings**

  - **Log level**—Set the level of detail provided when a log is run for the Fleet Agent. Always set the log level to **Detailed**.

 | Message Type | Summary | Detailed |
    |---|---|---|
    | Error | ✓ | ✓ |
    | Warn | ✓ | ✓ |
    | Informational | ✓ | ✓ |
    | Debug | **X** | ✓ |

  - **Network utilization delay (milliseconds)**—Limit the network traffic caused by the Fleet Agent printer discovery process. A higher number reduces the impact on network performance but makes the discovery process longer. The default delay setting is 250 milliseconds. The delay must not be set to zero.
3. Click **Create Agent**.

Installing a Fleet Agent

Fleet Agent installation package

After creating a Fleet Agent, install it on a server or host computer within the customer's network. The Fleet Agent installation package can be downloaded or provided through a link emailed from the Cloud Fleet Management portal.
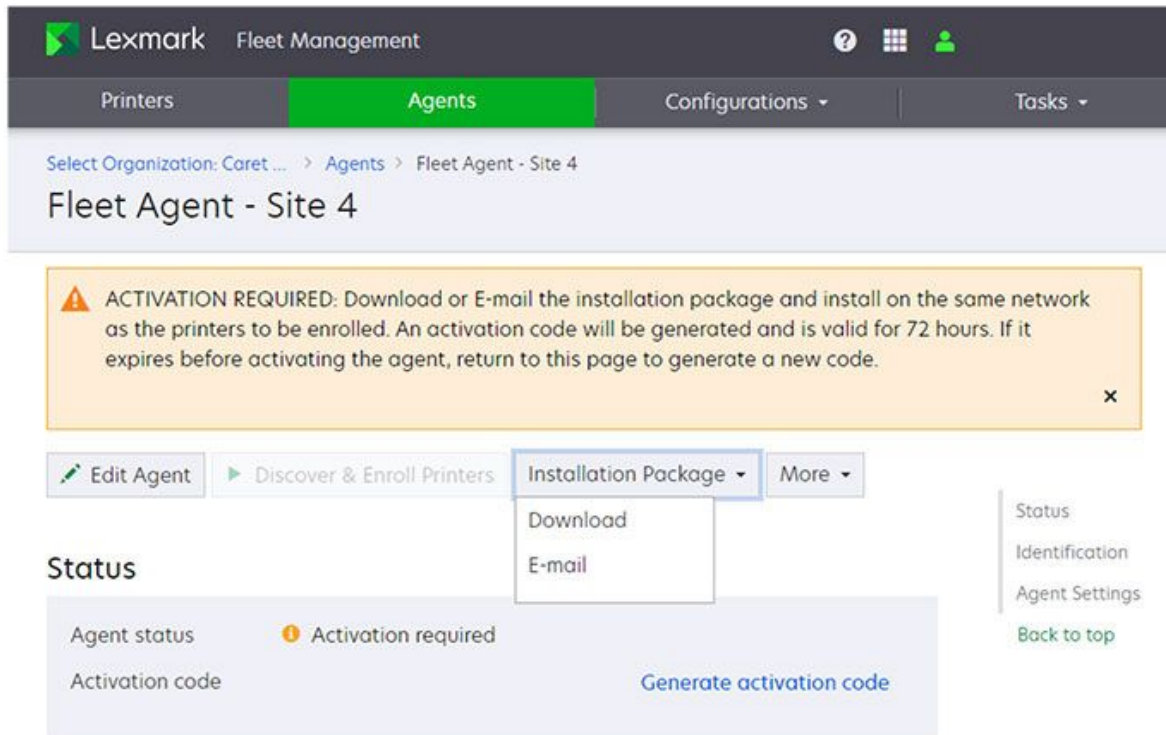
> **Note:** The size of the installation package is about 140MB.
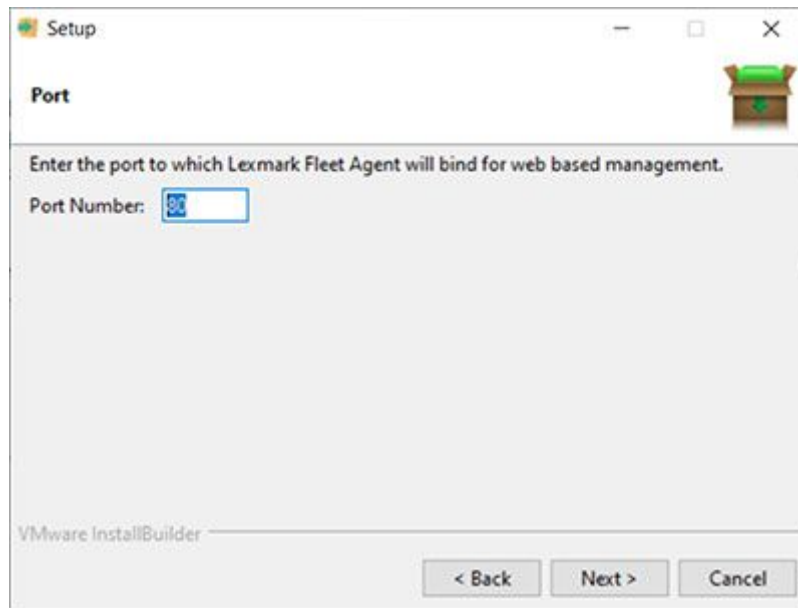
Fleet Agent activation code

You need an activation code during setup of the Fleet Agent. You can obtain the code by clicking the **Generate activation code** link. The code registers the installed Fleet Agent with a Fleet Agent definition. You can associate a Fleet Agent definition with only a single Fleet Agent installation. If the code is not used within 72 hours, then you must generate a new code.

Installing and activating a Fleet Agent

1. From a server or host computer, run the Fleet Agent installation package.
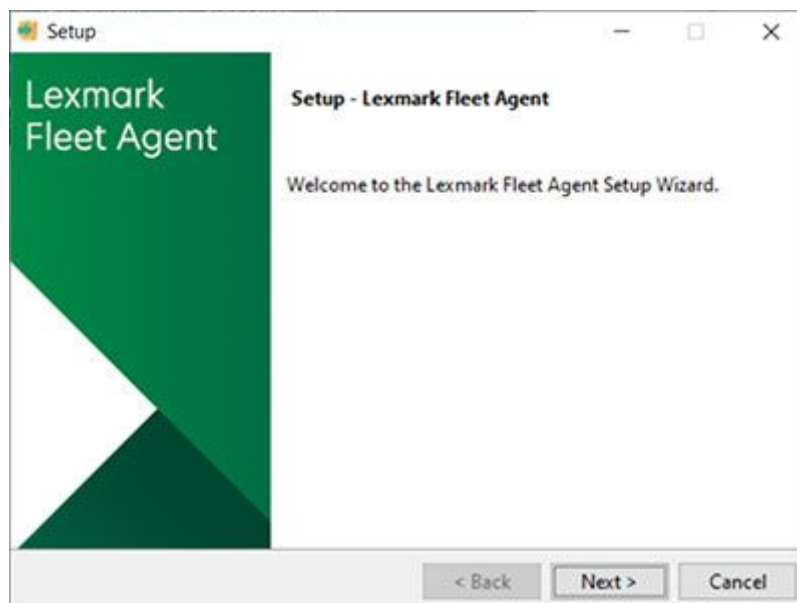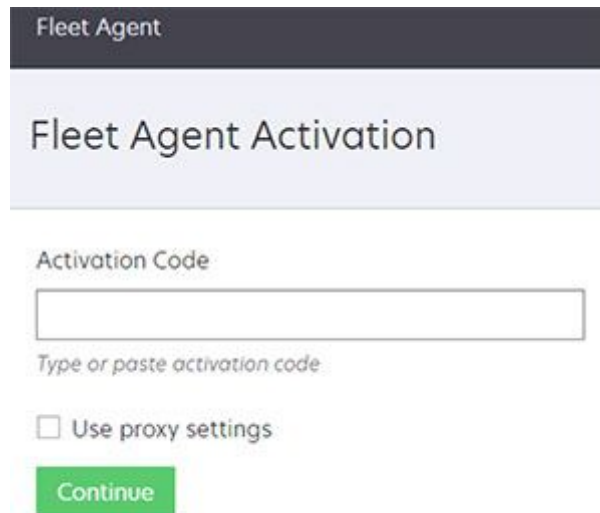
2. Accept the End-User License Agreement (EULA).
3. Enter the port number.

> **Notes**
> ◦ The default port number is 80.
> ◦ If port 80 is not available, then enter any available port, such as 8080 or 8088.

4. Click **Finish** to close the installation window, and launch the Fleet Agent on a web browser.
5. Enter the Fleet Agent's Activation Code, and then click **Continue**.

Notes

- A proxy can be set.
- You can apply a password to restrict access to the Fleet Agent.
- You can also set the initial printer discovery and enrollment to be performed automatically after the Fleet Agent is activated.

- After activation, the Fleet Agent details page shows its status as Communicating.
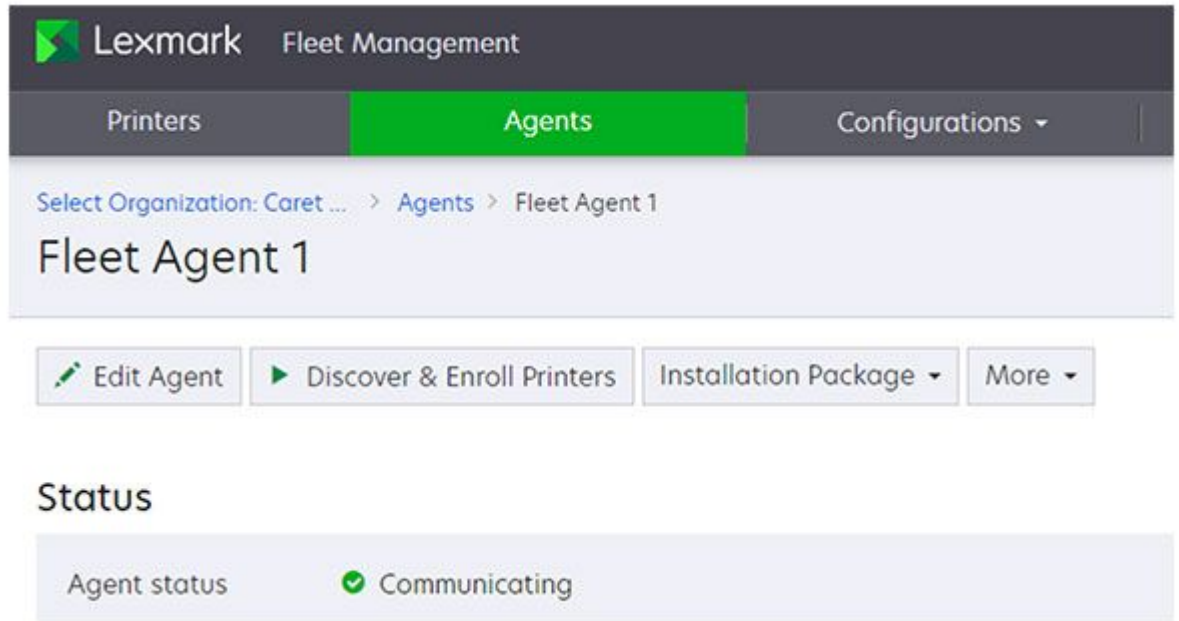
Using a proxy with the Fleet Agent

Sometimes you must change the proxy configuration after the Fleet Agent is installed. To change the proxy configuration, do the following:

1. Open a web browser, and then type https://localhost:*<portnumber>* .

   Note: *<portnumber>* is the port used when the Fleet Agent was installed. The default port number is 80.

2. Click ⚙ on the upper-right corner of the Fleet Agent home screen to access the Proxy Configuration settings.

Proxy Configuration   ✕

☑ Use proxy settings

Enter proxy settings as required by your network.

Proxy Host

[   ]

Proxy Port

[   ]

☑ Proxy requires username and password

Username

[   ]

Password

[   ]

[Cancel] [Verify Proxy Settings]

3. Click **Verify Proxy Settings**.

Discovering and enrolling printers

- To manually initiate the printer discovery and enrollment process, click **Discover & Enroll Printers** on the Fleet Agent details page in the Fleet Management portal.
- A Discover printers task is created on the Fleet Agent task queue. Discovered and enrolled printers appear on the Printers page in the Fleet Management portal.
- The initial discovery and enrollment task can be done manually or as part of the Fleet Agent activation process. Afterward, the task is automatically repeated on the schedule that you set when creating the Fleet Agent. For more information on installing and activating a Fleet Agent, see .
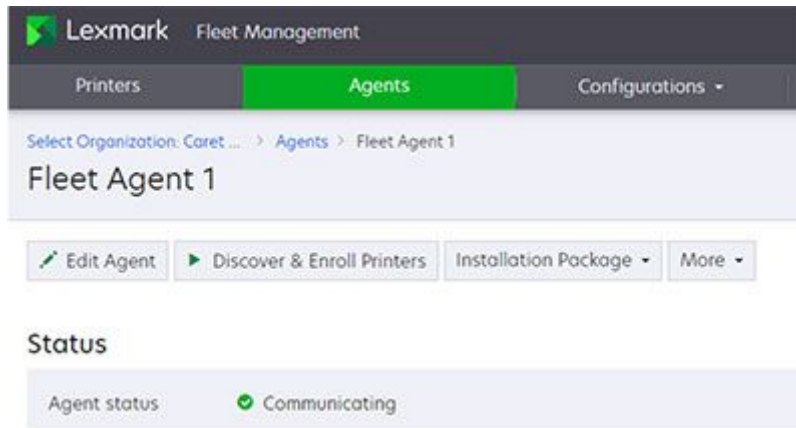
Printers not being discovered

You can use a MIB walk to determine why a printer is not being discovered. You can obtain a MIB walk log from the Cloud Fleet Management portal, and then contact Customer Support Center to review the log. To initiate a MIB walk, do the following:

1. From the Fleet Management web portal, click **Agents > Fleet Agents**.
2. Click the Fleet Agent name.
3. In the Log section, type the IP address of the printer, and then click **Request**.

4. Click **Download**.
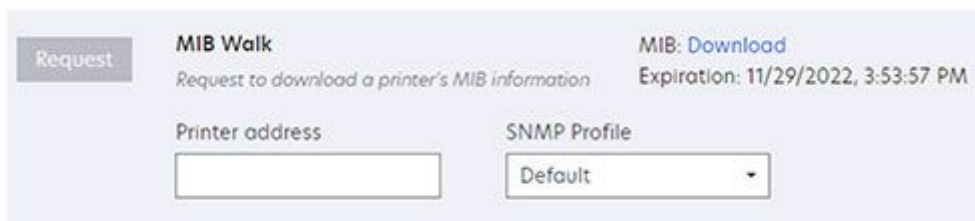
Managing an installed Fleet Agent

After a Fleet Agent is installed, you may need to change it for the following reasons:

- Printer discovery parameters
- Task scheduling
- Version update for the Fleet Agent or the Printer Support Library
- Deactivated or deleted Fleet Agent

Editing a Fleet Agent

1. From the Fleet Management web portal, click **Agents > Fleet Agents**.
2. Click the Fleet Agent name.
3. Click **Edit Agent**.
4. Click **Save Changes**.

Notes

- Changes made to the definition of an existing Fleet Agent take effect immediately.
- If the SNMP profile of a Fleet Agent definition is changed or deleted, then all printers associated with that profile are unenrolled and no longer discoverable by this Fleet Agent.
- After a Fleet Agent is updated, you can initiate a Discover printer task in the Fleet Agent details page by clicking **Discover & Enroll Printers**. This task discovers and enrolls printers based on the updated Fleet Agent definition.

Updating a Fleet Agent

Available updates to the Fleet Agent executable file or for Printer Support Library used by the Fleet Agent appear on the Fleet Agents page.

1. From the Fleet Management web portal, click **Agents > Fleet Agents**.
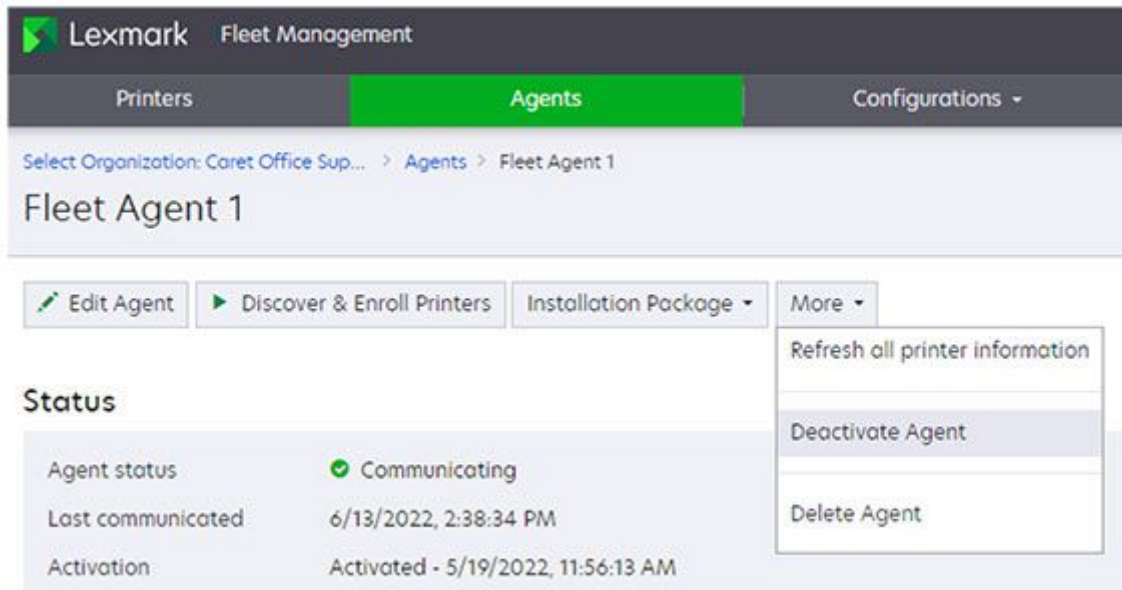2. Select one or more Fleet Agents, and then click **Update > Fleet Agent**.
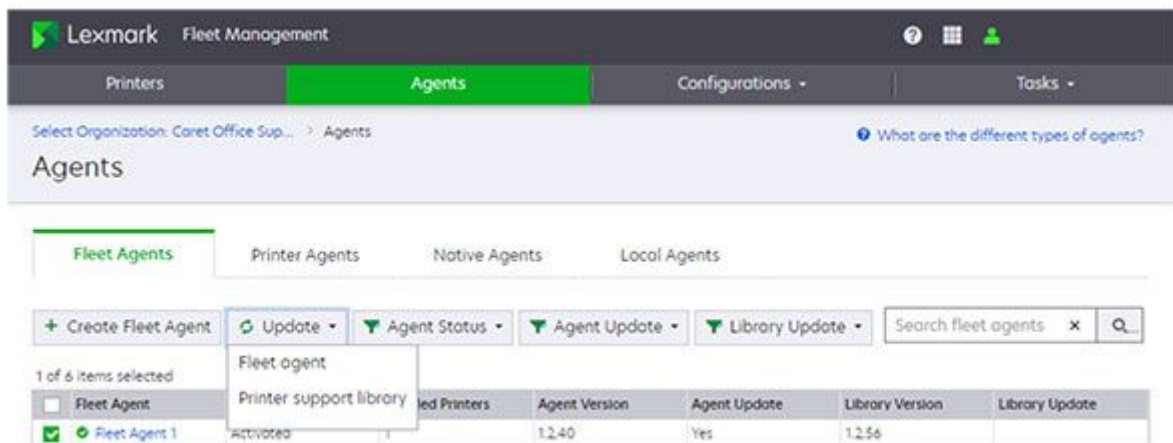
3. Click **Continue**.

Deactivating a Fleet Agent

Deactivating a Fleet Agent stops it from collecting printer data. After it is deactivated, you can no longer manage printers associated with that Fleet Agent. Printers associated with the deactivated Fleet Agent are unenrolled and no longer appear on the Printers page. The Fleet Agent definition is not deleted. Device data associated with the deactivated Fleet Agent is also retained.
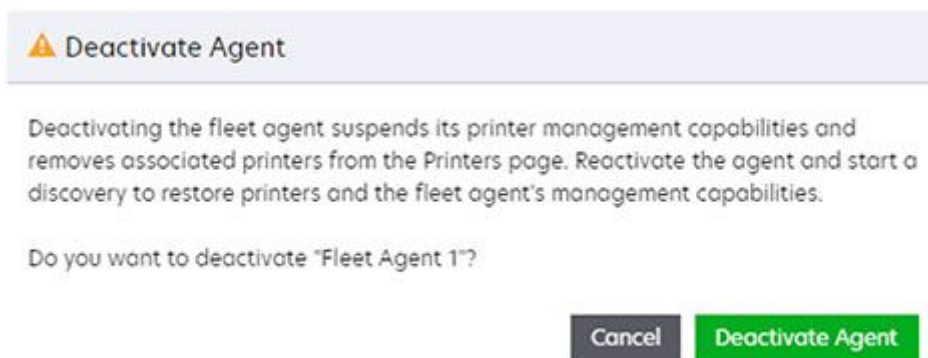
1. From the Fleet Management web portal, click **Agents > Fleet Agents**.
2. Click the Fleet Agent name.
3. Click **More > Deactivate Agent**.

4. Click **Deactivate Agent**.

Restoring a deactivated Fleet Agent

1. From the Fleet Management web portal, click **Agents > Fleet Agents**.
2. Click the Fleet Agent name.
3. In the Status section, click **Generate activate code**.
4. Copy the activation code.
5. Launch the Fleet Agent on a web browser, and then enter the activation code.
6. Click **Continue > Activate Agent**.

Fleet Agent

Fleet Agent Activation

Activation Code

Type or paste activation code

☐ Use proxy settings

Continue

Note: Once the Fleet Agent has been reactivated, you must initiate the Discover & Enroll Printers task from the Cloud Fleet Management portal. This restores the data collection and printer management functions of the Fleet Agent.

Deleting a Fleet Agent

If a Fleet Agent installation is no longer required at a customer location, it must be deleted. Deleting a Fleet Agent removes the Fleet Agent definition from the Cloud Fleet Management portal. It also unenrolls any printers associated with the deleted Fleet Agent, and deletes any data associated with those printers. The Fleet Agent executable running in the customer's environment will not be uninstalled. You must uninstall the Fleet Agent executable manually.

1. From the Fleet Management web portal, click **Agents > Fleet Agents**.
2. Click the Fleet Agent name.
3. Click **More > Delete Agent**.

Lexmark Fleet Management

Printers	Agents	Configurations ▾

Select Organization: Caret Office Sup... > Agents > Fleet Agent 1

Fleet Agent 1

✏ Edit Agent   ▶ Discover & Enroll Printers   Installation Package ▾   More ▾

Refresh all printer information

Deactivate Agent

Status

Delete Agent

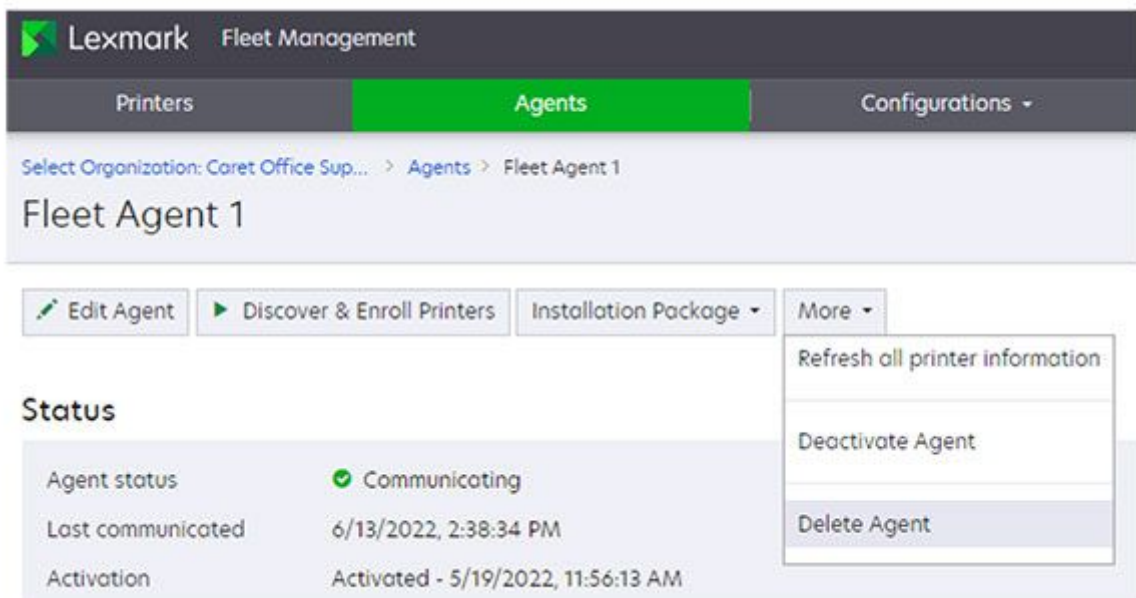| Agent status	✔ Communicating
Last communicated	6/13/2022, 2:38:34 PM
Activation	Activated - 5/19/2022, 11:56:13 AM

4. Click **Continue**.
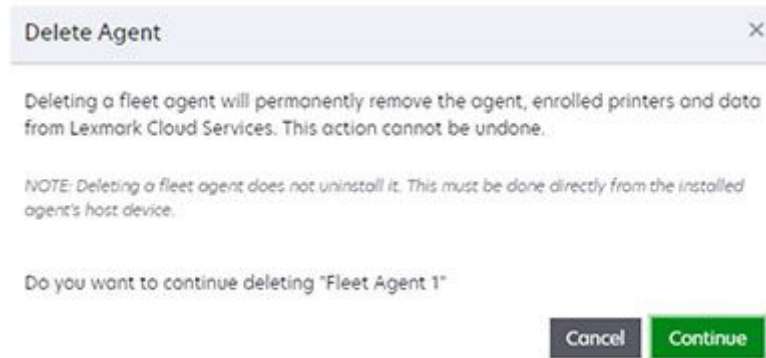
Notes

- A deleted Fleet Agent cannot be restored.
- A new Fleet Agent definition must be created. Once created, a new activation code for the definition can be applied to the Fleet Agent executable, if it was not manually uninstalled.
- For more information, see .

Using the Printer Agent

Using a Printer Agent

Downloading the Printer Enrollment Tool

If you do not have a copy of the Printer Enrollment Tool (PET), download it from the Cloud Fleet Management portal.

1. From the Fleet Management web portal, do one of the following:

   ◦ If some printers are already enrolled, then click **Printers > Enroll Printer using > Printer Agent > Download PET**.
   ◦ If enrolling printers for the first time, then click **Use Printer Agent > Download PET**.
2. To accept the End User License Agreement (EULA) and download, click **Accept and Download**.
3. Extract the compressed folder.

Using the Printer Enrollment Tool

1. Run the Printer Enrollment Tool launcher.
2. Log in using the same email address and password used to connect to the Cloud Fleet Management portal.

   Note: If a newer version of the PET is available, then you will be prompted to download it.

3. If you manage multiple organizations, then select an organization, and then click **Next**.

4. Click ⚙ on the upper-right corner of the page, and then configure the following:

    ◦ **Discover and enroll native agent-capable printers using**—Determines whether Native Agent-capable printers are enrolled using the Native Agent or Printer Agent.
    ◦ **Time out for Printer Discovery**—Determines how long the PET waits for a response to each network broadcast. The value can be increased to improve printer discovery in slow networks.
    ◦ **Time out for Printer Enrollment**—Determines how long the PET waits for the Printer Agent to enroll the printer. The value can be increased to improve the printer enrollment process of older printers.
    ◦ **Logging detail levels**—Set the logging level to **Detailed**.
    ◦ **SNMP settings**—The SNMP settings in the PET must match those of the printers to be discovered.

    > **Note:** Printer discovery first occurs using mDNS, and then by Simple Network Management Protocol (SNMP). If SNMP discovery is preferred, then mDNS must be disabled on the printers.

5. From the Discovery Type menu, select any of the following:

- ◦ **Search local network**—Finds all printers on your local subnet. Use this method if you have several printers on the subnet but you do not know their network parameters. This method may take several minutes to locate complete.
- ◦ **Advanced search**—Lets you refine the search by specifying network parameters to find printers. Use this method if you have a small number of printers or if the network parameters of the printers are known. This method is usually faster than the Search local network method.

  The following are the network parameters:

  - ▪ Specific IP address
  - ▪ Subnet
  - ▪ Range
  - ▪ Fully qualified domain name (FQDN)

  Notes
  - ◦ To discover printers successfully, make sure that mDNS is enabled on the printer or that the SNMP configurations of the PET and the printers match.
  - ◦ Printers in the Eligible to Enroll tab can be enrolled with the Native Agent if their agent type is set to Native.

6. Select one or more printers to enroll, and then click **Enroll Printers**.

> **Note:** The selected printers do not have to be of the same agent type. Each selected printer is enrolled using the indicated agent type.

7. If necessary, log in to access the printer Embedded Web Server, and then click **Apply Credentials**. Otherwise, click **Skip This Step**.

> **Notes**
> - When using a Native Agent or Printer Agent and a Fleet Agent, or multiple Fleet Agents within the same organization, care must taken while defining the Printer Discovery settings. Only one agent can manage a printer. If overlapping Printer Discovery criteria exist, then printers may not be managed by the intended agent.
> - The enrollment process may take several minutes to complete.
> - After successful enrollment, wait several minutes for the printers to appear in the Cloud Fleet Management printers list.
> - When a printer is enrolled using the Printer Agent, the PET installs an embedded (eSF) application, called the Printer Configuration Agent (PCA), on the printer. The PCA is the communications path between the printer and the cloud.

Verifying the printer enrollment status

After running the PET to enroll printers, do the following to verify that an enrolled printer can communicate with Cloud Fleet Management. For more information on troubleshooting, see "Fleet Management troubleshooting" group in *Lexmark Cloud Services Administrator's Guide*.

- Check for printer enrollment failures in the PET.

  - For security-related failures, re-enroll printers using the correct security credentials.

Address	Model	Serial Number	Agent Version
☒	The Printer Configuration Agent failed to enroll		
	• The printer's security settings may be preventing the Printer Configuration Agent from installing.		

  - If the printer date and time are not correct, then an error message appears.

Address	Model	Serial Number
☒	The Printer Configuration Agent failed to enroll	
	• The Printer Configuration Agent failed to enroll due to incorrect time on the printer.	

  - Make sure that the printer firmware is at least at the minimum recommended level.
- Verify that embedded applications appear on the printer Embedded Web Server (EWS) application page.

  - If no applications appear, then power cycle the printer.
  - If the issue persists, then re-enroll the printer.
- Verify that the PCA embedded application is enabled or running on the printer. If the PCA is disabled or stopped, then enable or start it.

- Verify that the PCA application status is enrolled.

    ◦ Open the Printer Configuration Agent application from the printer EWS. If the PCA status is unenrolled, then re-enroll the printer.

    ◦ Click **Test Agent Connection** to verify that the network and credential settings are correct.

Verifying the connection status after placing the printer in service

Do the following to verify the Cloud Fleet Management connection status of a printer after it is placed in service or its network environment is changed. For more troubleshooting information, see "Fleet Management troubleshooting" group in *Lexmark Cloud Services Administrator's Guide*.

- Click **Test Agent Connection** to verify that the network and credential settings are correct.
- On e-Task v5 or later printers, do the following:

    ◦ When editing contacts in the printer address book, do not modify or delete the Lexmark_PCA_User entry.
    ◦ When importing or applying the contactmanager.xml file, edit the contactmanager.xml file to set <addressbook clear="false">.
- On the Cloud Fleet Management portal Printers page, do the following:

    ◦ Verify that the printer is listed. If it is not, then re-enroll the printer.
    ◦ Check the communication status of the printer.

        ▪ If it is Communicating, then verify communications by going to the Printer Details page clicking **Refresh Printer Information**, and then checking the status in Task History.

        ▪ If it is Not communicating, then do the following:

            ▪ Verify that the printer is in service and has network connectivity. Open the Printer Configuration Agent application from the EWS, and then click **Test Agent Connection** to verify that the network and credential settings are correct.

- Verify that the printer is in service in this organization. If the printer that you are enrolling was previously enrolled in another organization, then its Communication status will be Not communicating in the previous organization. To prevent this scenario, unenroll printers that are being moved to a new organization.
- Re-enroll the printer, in any of the following cases:

  - The application status of the PCA is unenrolled.
  - The printer security login has changed since the printer was enrolled.
  - The Lexmark_PCA_User account has been modified in any e-Task v5 or later printers.
  - The printer DHCP/DNS configuration has changed or does not match the customer's environment.
 - The printer date and time settings are not correct.
- If a firewall is being used, then verify that the appropriate Lexmark Cloud Services URLs have been added to the Allow List. For more information, see "Deployment readiness checklist" in *Lexmark Cloud Services Administrator's Guide*.

- If "Agent needs credentials" appears, then the agent is communicating with Cloud Fleet Management, but administrator credentials have been applied to the printers after enrollment. A lock symbol appears in front of the IP addresses of these printers.

  You can apply credentials from the Cloud Fleet Management portal. For more information, see "Managing enrolled printers" group in *Lexmark Cloud Services Administrator's Guide*. You can also apply credentials by opening the Printer Configuration Agent eSF application and then clicking **Update Credentials**.
- If "gent not communicating" appears, then the Fleet Agent associated with the printer is no longer communicating with Cloud Fleet Management. Verify that the Fleet Agent is still running and that it has a constant Internet connection.

  If a firewall is being used, then verify that the appropriate Lexmark Cloud Services URLs have been added to the Allow List. For more information, see "Deployment readiness checklist" in *Lexmark Cloud Services Administrator's Guide*.

Setting the correct date and time

The printer date and time must be set correctly to avoid failures in printer enrollment or in the processing of Cloud Fleet Management tasks. If it is not set correctly, then printer enrollment or the processing of Cloud Fleet Management tasks may fail. It is best to configure the printer's date and time by enabling the use of a Network Time Protocol (NTP) server. NTP servers are usually available from domain servers. Publicly available NTP servers can be found through an internet search.

If the printer's date and time are not correct when it is enrolled, then the printer's date and time will be set to the date and time of the Printer Enrollment Tool (PET) workstation if:

- The Enable NTP is not selected
- The Enable NTP is selected and the NTP Server address is blank
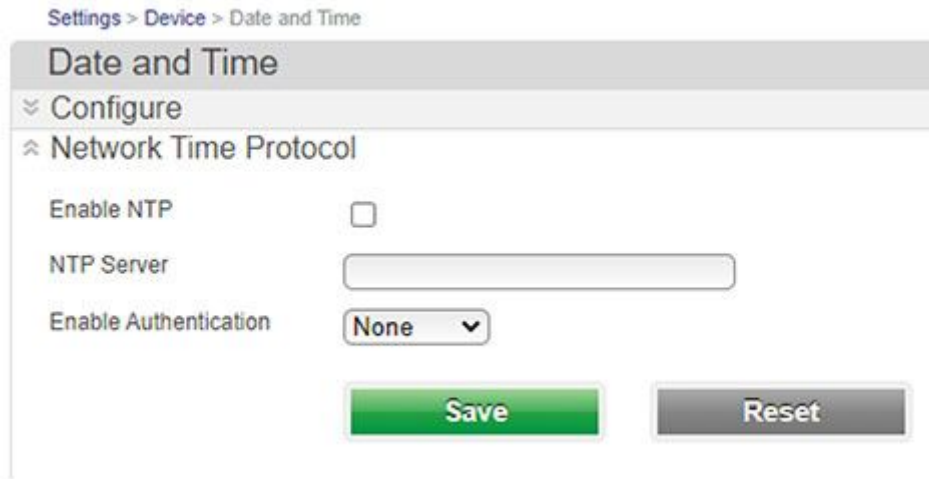
Managing user accounts and printer permissions

To use and manage the Printer Agent, you must set the function access controls (FACs) and maintain an administrator account on the current-generation Lexmark printers. When referring to the Printer Agent on printers, the printers can be Secured or Open.

e-Task version 5 or later printers

Printers with e-Task version 5 or later have a dark control panel background.
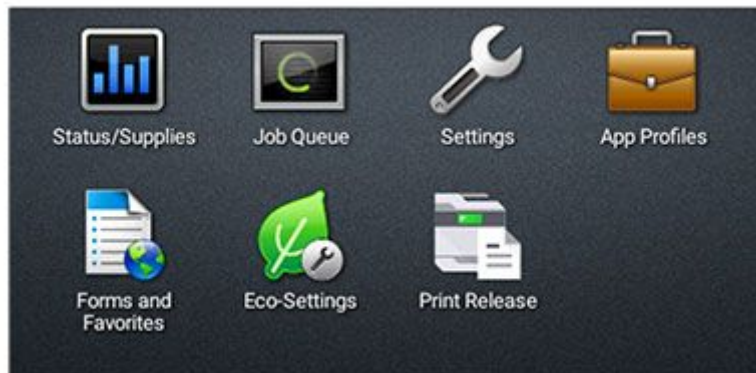
Secured Printers

If access to the Embedded Web Server (EWS) is protected, then provide the credentials in the Printer Enrollment Tool during enrollment.

The following permissions must be enabled in either the Public or All Users permissions groups to avoid a failed enrollment.

Access Control menu section	Access control to enable
Administration Menus	Security Menu

Access Control menu section	Access control to enable
Device Management	Remote Management

Open Printers

If access to the Embedded Web Server is not protected, then the following permissions must be enabled in the Public permissions group to avoid a failed enrollment.

Access Control menu section	Access control to enable
Administration Menus	Security Menu
Device Management	Remote Management
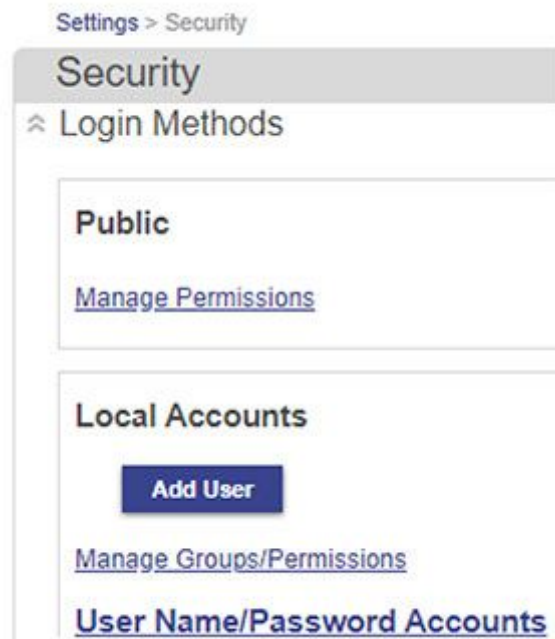
Lexmark_PCA_User account

When the Printer Configuration Agent (PCA) eSF application is installed on an e-Task version 5 or later printer, a Lexmark_PCA_User account and an administrator group are created. This account is used to process requests from Cloud Fleet Management.

> **Note:** The Lexmark_PCA_User account and the administrator group must not be changed or modified. Changing them after enrollment prevents the printer from processing Cloud Fleet Management requests.

If any of the following actions occur after the printer is enrolled, then Cloud Fleet Management functionality may be lost. To restore Cloud Fleet Management functionality without reenrolling the printer, do the following resolution actions:

Action	Resolution
Lexmark_PCA_User account has been deleted.	1. Recreate the Lexmark_PCA_User account. 2. Open the Printer Configuration Agent application. 3. Click **Update Credentials**, and then enter the credentials of an existing administrator account on the printer.
Lexmark_PCA_User account name has been changed.	Click **Update Credentials**, and then enter the credentials of an existing administrator account on the printer.
Lexmark_PCA_User account password has been changed.	1. Open the Printer Configuration Agent application. 2. Click **Test Agent Connection**. 3. Click **Update Credentials**, and then enter the credentials of an existing administrator account on the printer.
Administrator group has been deleted.	1. Recreate the administrator group with all permissions enabled. 2. Assign the recreated administrator group with the Lexmark_PCA_User account.
Administrator group permissions have been changed.	Re-enable all permissions under the administrator group.
Lexmark_PCA_User account removed from the administrator group.	Reassign the Lexmark_PCA_User to the administrator group.

e-Task version 4 or earlier printers

Printers with e-Task version or earlier have a light gray control panel background.

Secured Printers

If a Basic Security Setup template has been applied, then provide the credentials in the Printer Enrollment Tool during the device enrollment process. If this protection was applied or modified after the printer was initially enrolled, then the printer will not process requests from Cloud Fleet Management. For more information, see "Managing enrolled printers" group in *Lexmark Cloud Services Administrator's Guide*.
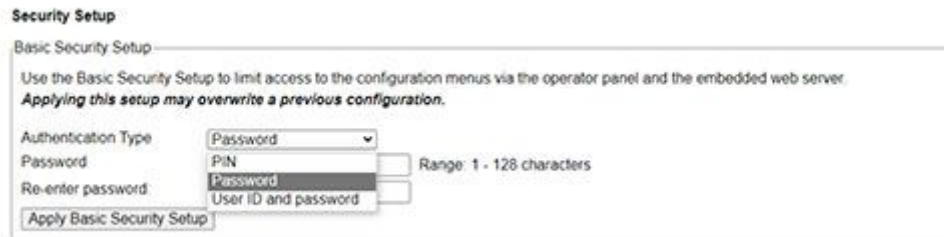
The following access controls must be set to either the **Basic Security Setup** template or **No Security**.

e-Task version	Access Controls menu	Access control
e3 and e4	Administration menus	Service Engineer Menus Remotely
e3 and e4	Management	Remote Management
e3 and e4	Management	Firmware Updates
e4	Management	Configuration File Import / Export

Open Printers

If access to the Embedded Web Server is not protected, then the following access controls must be set to **No Security** to avoid a failed enrollment.

e-Task version	Access Controls menu	Access control
e3 and e4	Administration menus	Service Engineer Menus Remotely
e3 and e4	Management	Remote Management
e3 and e4	Management	Firmware Updates
e4	Management	Configuration File Import / Export

Using the Local Agent

Using a Local Agent

The Local Agent is a Fleet Management agent for managing USB-connected printers that otherwise do not have a means of communicating directly with Cloud Fleet Management. For more information on the Fleet Management Agents, see .

> **Note:** The Local Agent supports Windows 64-bit and Windows 32-bit operating systems only

To use a Local Agent, do the following:

- Download the Local Agent
- Obtain an activation code
- Install the Local Agent
- Activate the Local Agent

Downloading the Local Agent

1. From the Fleet Management web portal, click **Agents > Local Agents > Download Local Agent** or **Download Agent**.
2. In the Download Local Agent window, select the installer package type.

> **Note:** You can select the Windows x64 or x86 installer package.

3. Select **Generate activation code**.

> **Notes**
>   ◦ The activation code is valid for 72 hours. If you are going to install the Local
>   Agent before the activation code expires, then generate the code now.
>   ◦ You can set the number of agents to be activated by the code.
>   ◦ If the code expires before activating the agent, then generate a new activation
>   code. From the Fleet Management portal, click **Agents > Local Agents >
>   Activation Code > Generate activation code**.

4. Click **Download Agent**.
5. Accept and download the End-User License Agreement (EULA).

> **Note:** The Local Agent installation files and activation code can be reused up to the
> number of activations specified when the activation code was generated. After the
> specified number of activations, the code is no longer valid, to prevent using it on
> more workstations than intended.

Downloading the Local Agent again
If the Local Agent is downloaded while a valid activation code exists, then the activation
code appears when the Local Agent installation package is downloaded. The time

remaining until the activation code expires and the number of activations remaining are shown. Click **Download Agent** to download the installation package.
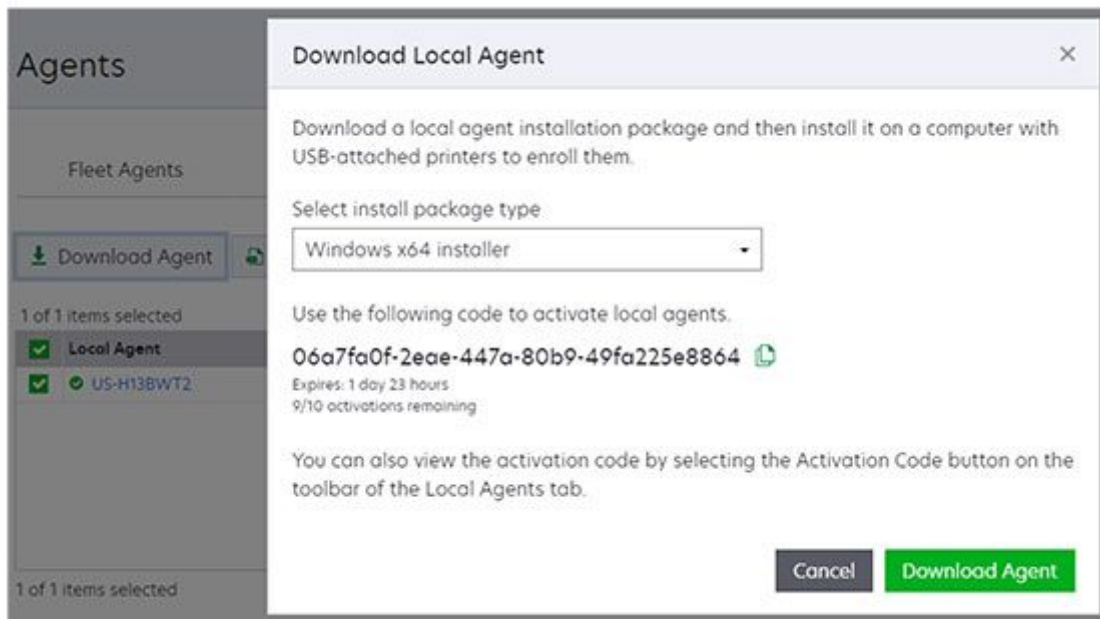
Obtaining the activation code

To use the Local Agent, you need an activation code. An activation code can be generated when the Local Agent installer is downloaded. For more information, see Downloading the Local Agent on page 102. You can also obtain the activation code by doing the following:

1. From the Fleet Management web portal, click **Agents > Local Agents > Activation Code > Generate activation code**.
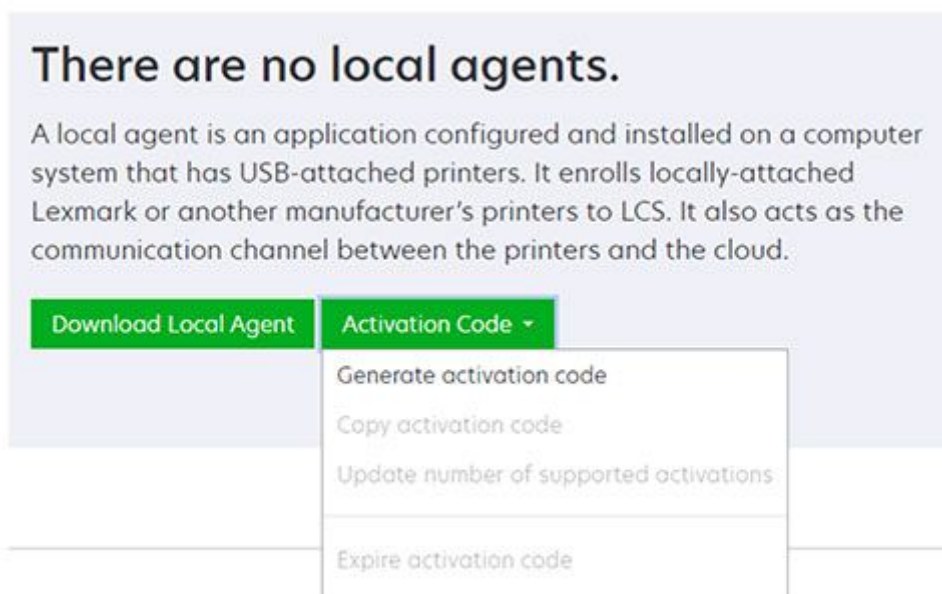
2. In the Generate activation code window, set the number of agents to be activated by the code.

3. Click **Generate Code**.

   If a valid activation code already exists, then you can view it by clicking the **Activation Code** menu.

4. Click **Copy activation code**

   Note: The time and the number of remaining activations for which the code is valid are shown.

Managing the activation code

If a valid activation code already exists, then you can view it by expanding the Activation Code menu.

Updating the number of activations allowed

The Local Agent installation files and activation code can be reused up to the number of activations specified when the code was generated. After the specified number of activations, the code is no longer valid. To increase the number of allowed activations for a valid activation code, do the following:

1. From the Fleet Management web portal, click **Agents > Local Agents > Activation Code > Update the number of supported activations**.
2. In the Update the number of supported activations window, set the number.
3. Click **Update Activations**.

> **Note:** If an activation code has expired, then you must generate a new one. You cannot increase the activations allowed for an expired activation code. Activation codes are valid for up to 72 hours.

Invalidating an activation code

If you no longer need a valid activation code, then you can force its expiration.

1. From the Fleet Management web portal, click **Agents > Local Agents > Activation Code > Expire activation code**.
2. In the Expire activation code window, click **Expire Code**.

Installing and activating a Local Agent

The Local Agent is designed to be installed on a Windows 64-bit or Windows 32-bit operating system. The downloaded Local Agent package must be extracted before it can be installed and then activated.
Installing the agent manually

To manually install the Local Agent, execute the Local Agent msi file. Follow the on-screen prompts. After the installation has completed, the Local Agent must be activated.

> **Note:** The Local Agent msi file must be executed from the same folder as the configuration .ini files.

1. Run the Local Agent MSI file.
2. Follow the instructions on the computer screen.

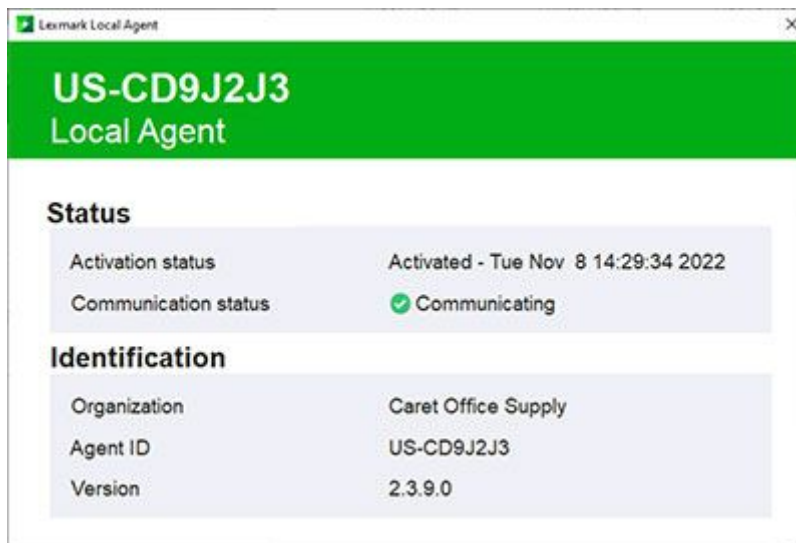### Activating the agent manually

1. To manually activate the Local Agent, find and open the Lexmark Local Agent entry in the Windows menu.
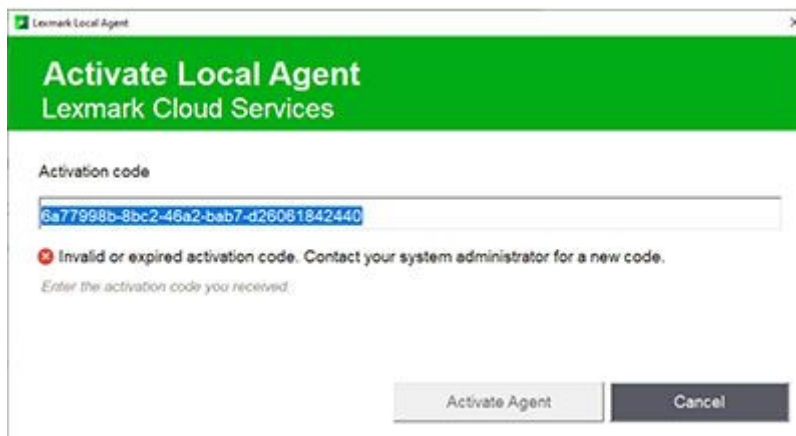

2. Enter the activation code, and then click **Activate Agent**.
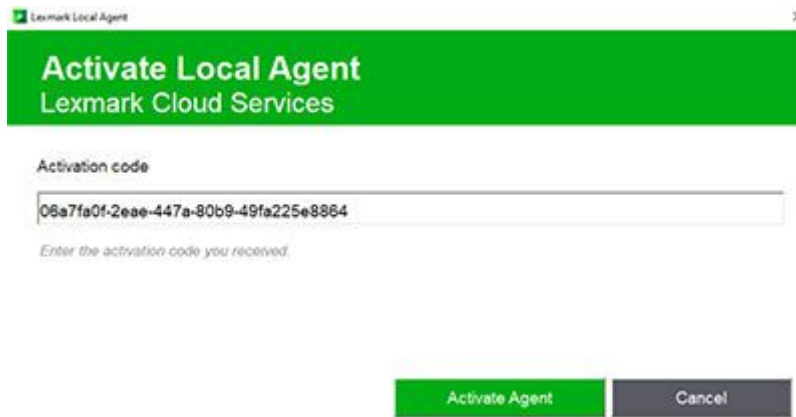
The following message appears

If the activation of the Local Agent fails, then the following message appears:

Make sure that the activation code is correct, or generate a new activation code.

Activating the agent during installation

You can configure the Local Agent to automatically activate during installation by adding the activation code to the LocalAgentConfig.ini file.

1. Unzip the installation package.
2. Open the LocalAgentConfig.ini file in a text editor.
3. Under the [IOT_HUB] block, add the CS_ACTIVATION_CODE parameter.

4. Enter the activation code generated from Lexmark Cloud Services as the value of the parameter.

   Sample code:

   ```
   [IOT_HUB]
       CS_ACTIVATION_CODE=ab23ftcd-12dt-edte-123hdtdk-ttrbd
   ```

5. Save the LocalAgentConfig.ini file.
6. Run the Local Agent MSI file.

Notes

- The Local Agent msi file must be executed from the same folder as the configuration ini files.
- If the activation code has expired, or was incorrectly copied into the LocalAgentConfig.ini file, then the Local Agent is installed, but is not activated. To verify the activation status of the Local Agent, click **Agents > Local Agents**.

Managing an installed Local Agent

Managing Local Agents includes the following:

- Updating the Local Agent version. For more information, see "Updating the Local Agent" topic in *Lexmark Cloud Services Administrator's Guide*.
- Editing the configuration of Local Agents or deactivating or deleting a Local Agent. For more information, see "Editing the Local Agent" topic in *Lexmark Cloud Services Administrator's Guide*.

Editing the configurations of a Local Agent

Local Agents have two configurable parameters:

- **Log level**—Must be set to **Detailed**. Detailed logs provide information on errors, warnings, and debugging.
- **Polling Interval**—How often the Local Agent reports printer data back to the Fleet Management services. The default value is 180 minutes.

Editing the Local Agents

1. From the Fleet Management web portal, click **Agents > Local Agents**.

2. Do either of the following:

    ◦   To edit a single Local Agent, click the name of the Local Agent, and then click **Edit Agent**.
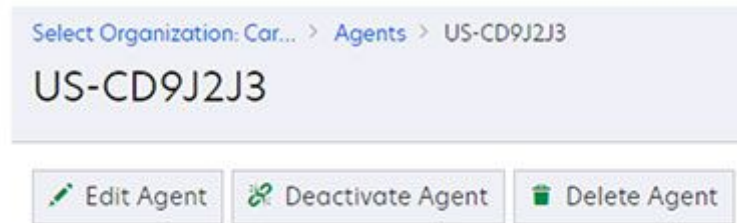
    ◦   To edit multiple Local Agents at the same time, select multiple Local Agents, and then click **Edit Settings**.

> **Note:** The Edit Local Agent window shows that Log level is set to **Detailed** and Polling Interval is set to **300**. These changes are automatically applied regardless of the current settings of the selected Local Agents.

Deactivating a Local Agent

To stop the Local Agent from collecting and reporting printer information to the Fleet Management services, you can deactivate it. After reactivating a Local Agent, you can reactivate it only by applying a valid activation code.

1. From the Fleet Management web portal, click **Agents > Local Agents**.
2. Click the name of the Local Agent.
3. Click **Deactivate Agent**.

4. Click **Deactivate Agent**.

Deleting a Local Agent

If a Local Agent is no longer needed, then it can be deleted from the Fleet Management portal. All information related to the agent is deleted.

1. From the Fleet Management web portal, click **Agents > Local Agents**.
2. Click the name of the Local Agent.
3. To delete a Local Agent, click **Delete Agent**.

4. Click **Delete Agent**.

Note: Deleting a Local Agent in the Fleet Management portal does not uninstall the Local Agent application installed on the workstation.

Deploy applications and configure your printers

Deploying file using configurations

Using configurations

You can deploy configurations to update managed printers from within the Fleet Management portal. A configuration can contain one or more of the following categories:
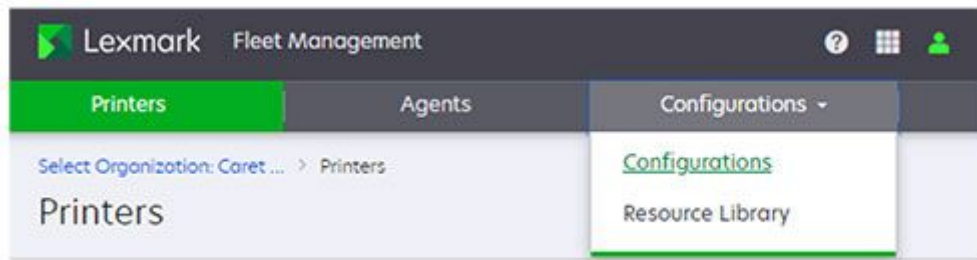
- Printer firmware
- eSF applications
- Printer settings files

You can deploy configurations to one or more printers in a single action. Fleet Management services determine the correct version of firmware or eSF applications to deploy to each printer.
Deploy configuration in the following order:

- Firmware
- Applications, in the same order that they appear in the configuration.
- Settings files, in the same order that they appear in the configuration.

Creating a configuration

1. From the Fleet Management portal, do either of the following:

   ◦ Click **Printers > Configure > Create Configuration**.
   ◦ Click **Configurations > Configurations > Create**.

2. In the Create Configuration page, type a unique name and description.

3. Select one or more of the following:

   ◦ Firmware

      ▪ The latest recommended Firmware versions
      ▪ Special version previously uploaded as a resource in Cloud Fleet Management
   ◦ Apps

      ▪ The latest version of the selected eSF applications
      ▪ Special version previously uploaded as a resource in Cloud Fleet Management
   ◦ Printer Setting Files

- UCF or setting bundle files previously uploaded as a resource in Cloud Fleet Management
4. Click **Create Configuration**.

Firmware

A configuration can be set up to deploy printer firmware. The firmware can be the latest recommended versions or the selected versions, previously uploaded as a resource in Cloud Fleet Management.

Notes

- If the Recommended Firmware option is selected, the latest recommended version available whenever the configuration is deployed, will be used.
- Firmware is deployed first, followed by apps and printer settings.

Recommended firmware

Select **Update all models to the recommended firmware version** to deploy the latest recommended version of firmware version. This deploys the latest recommended version whenever the configuration is deployed.

Other firmware

You can click **Select Firmware** to select a specific version from the Resource Library. Once you select a specific firmware, it overrides Update all models to the recommended

firmware version setting for models that use the specific firmware version. Multiple firmware versions can be selected, but only one version per printer model is allowed.

Specific firmware can also be uploaded to the Resource Library and automatically selected by clicking **Upload Firmware**, and then completing the form. For more information, see Using Cloud Print Management clients on page 142.

Apps

A configuration can deploy eSF applications to printers. The applications deployed can be standard eSF applications or the ones uploaded to the Resource Library.
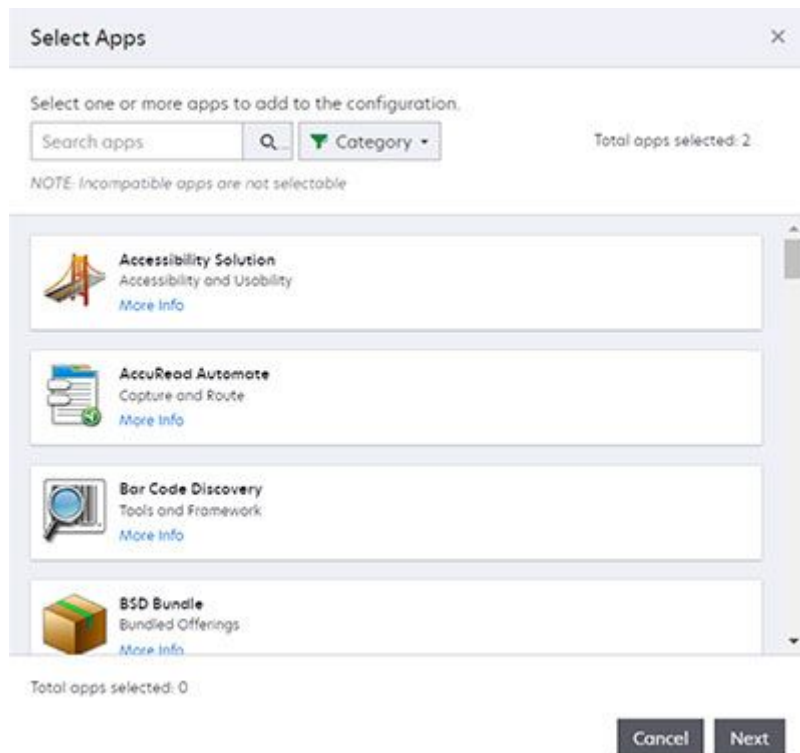
Note: Apps are deployed after firmware and in the order that they appear in the Apps list.

Select Apps
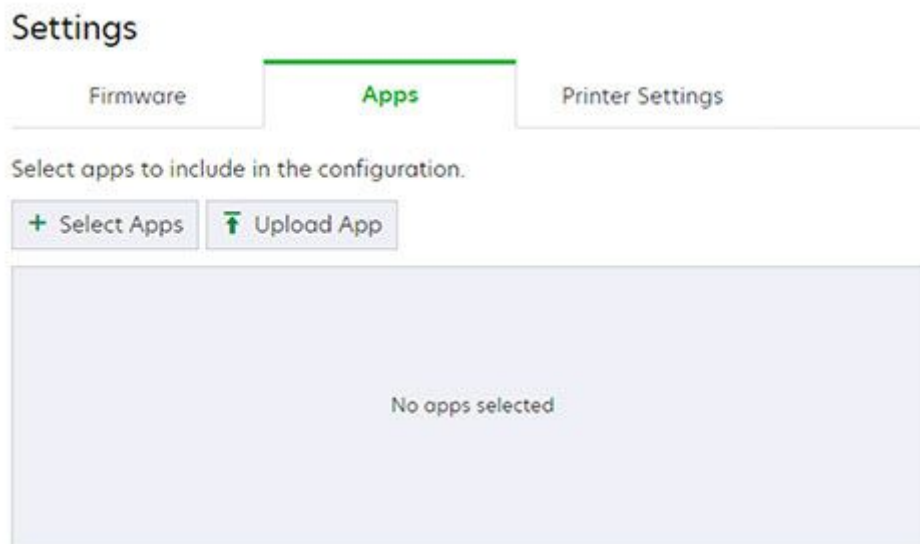
Click **Select Apps** to see eSF applications available for deployment

This list contains both the standard eSF applications, and those previously uploaded to the Resource Library. You can select one or more applications from the list, and then click **Next** to review your selection.
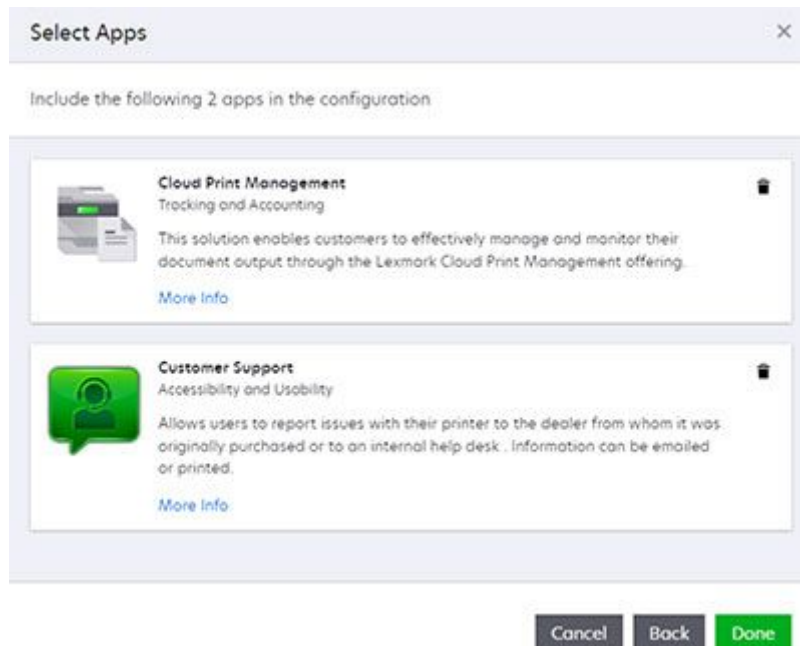
After reviewing the form, click **Done**.

Upload Apps

An eSF application can be uploaded to the Resource Library and automatically selected by clicking **Upload Apps**, and then completing the form. The application file selected must be an .fls file. The uploaded application will be automatically added to the list of applications included in the configuration. For more information, see Using Cloud Print Management clients on page 142.

Applications that have been uploaded to the Resource Library can be selected from the Apps catalog. Apps from the Resource Library are shown with the category type of Imported app.
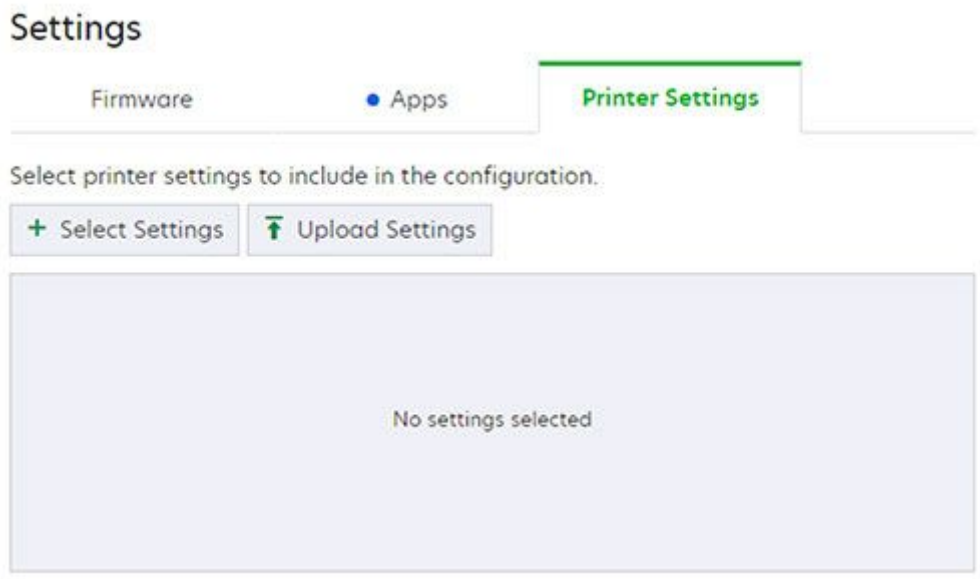
App settings

eSF applications may have configurable settings that can be deployed with the application. The settings available for each application can be viewed by clicking the arrow next to the name of the eSF application. Edit the settings to fit your specific needs. Repeat this process for each application in the configuration.
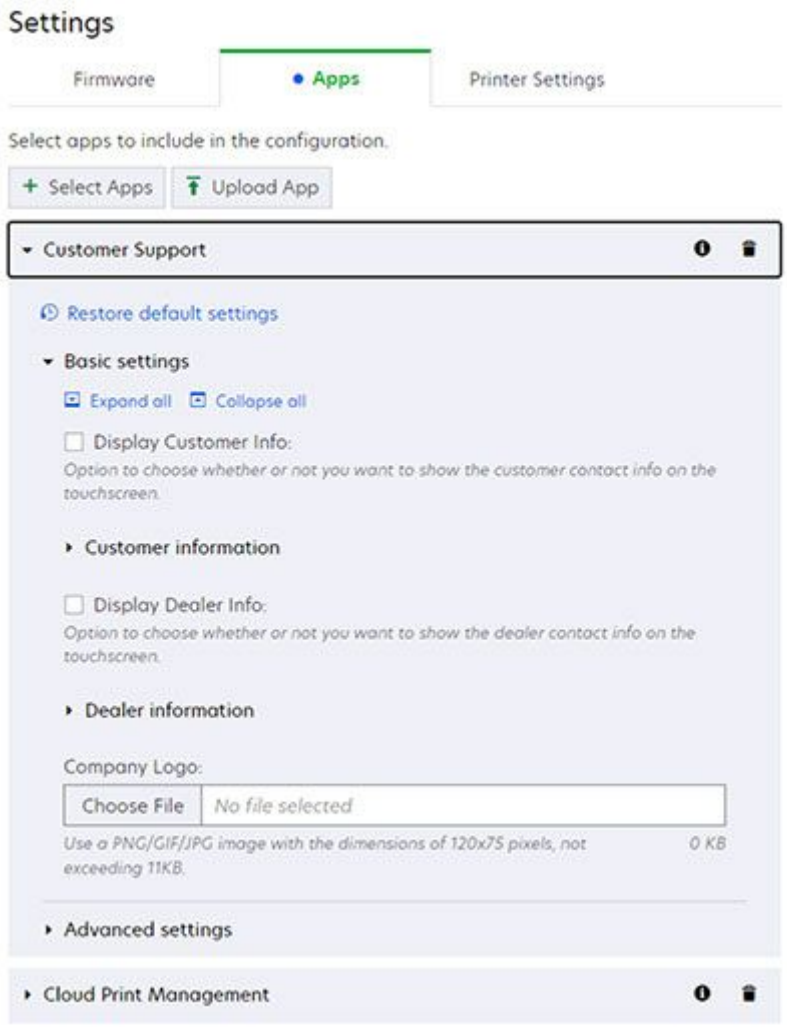
Printer Settings

A configuration can be used to deploy printer settings files. The settings file must be uploaded to the Resource Library before they can be deployed.

> **Note:** Settings will be deployed after firmware and apps, and in the order that they appear in the list.

Select Settings

Settings files that have been previously uploaded to the Resource Library can be selected by clicking **Select Settings**. To establish the proper settings for your needs, select one or more setting files, and then click **Select Settings**.

Upload Settings

A printer settings file can be uploaded to the Resource Library and automatically selected by clicking **Upload Settings** and completing the form. The settings file must be a UCF or a Setting Bundle file. The uploaded settings file is automatically added to the list of settings files included in the configuration. For more information, see Using Cloud Print Management clients on page 142.

Using a Resource Library

The Resource Library is a repository for your custom files that can be deployed to printers as part of a configuration. Resource files consist of the following types:

- Firmware
- eSF applications
- Printer setting files

  - Universal Configuration Files (UCF)
  - Bundles

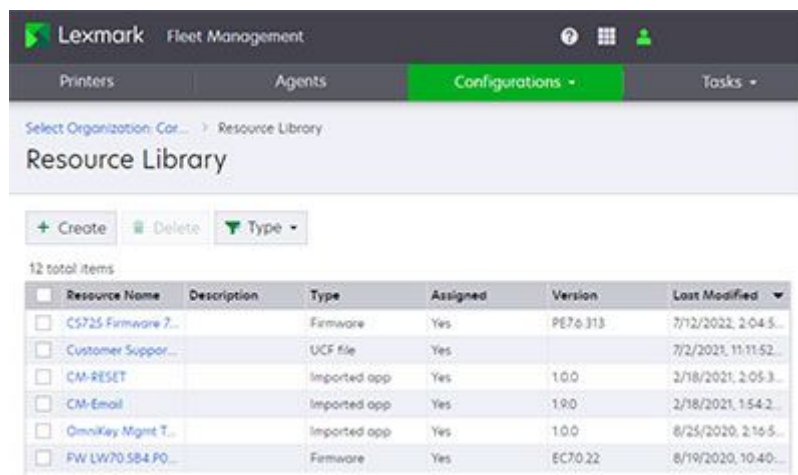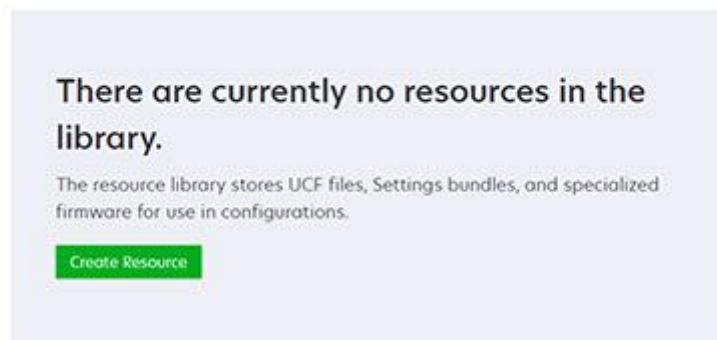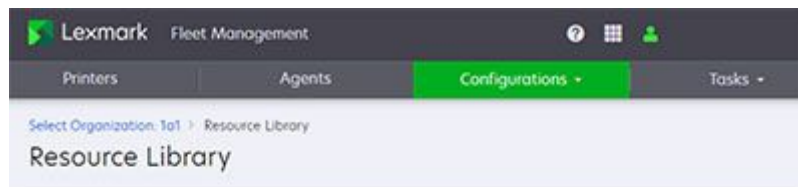There are two ways to add items to the Resource Library:

- Add files to the Resource Library for later use
- Add files to the Resource Library while creating a configuration

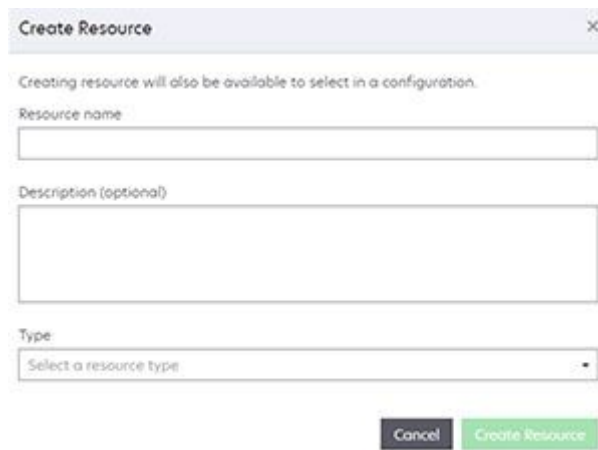**Adding files to the Resource Library**

1. From the Fleet Management portal, click **Configurations > Resource Library**.
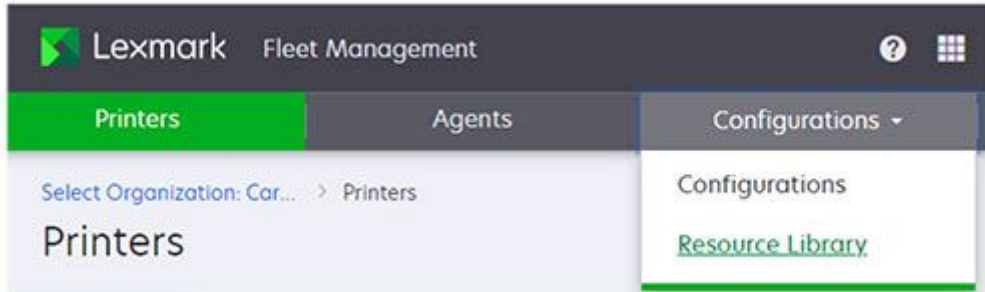
2. Click **Create Resource** or **Create**.

3. In the Create Resource window, do the following:

- ◦ Type a unique name and description.
- ◦ From the Type menu, select any of the following:

- ▪ **UCF file**—Files with a .ucf or .txt extension that contain printer or eSF application settings. Click **Choose File** to browse to the UCF file.

  Notes
  - ▪ You can use UCF files to clone settings from one printer to another or to define a standard configuration for printers.
  - ▪ UCF files are the preferred method of deploying settings to older-generation printers, with firmware versions beginning with LW and LHS.

- ▪ **Settings bundle**—Settings bundle are files with a .zip extension that contains printer or eSF application settings. You can click **Choose File** to browse for the settings bundle.

  Notes
  - ▪ You can use Settings bundle files to clone settings from one printer to another or to define a standard configuration for printers.
  - ▪ Settings bundles are the preferred method of deploying settings to the current-generation printers, with firmware versions beginning with CS, CX, MS, and MX.

- ▪ **Firmware**—Special versions of printer firmware that you can be add as a resource. Enter a specific firmware version, such as CSTAT.076.303, or a link provided by the Lexmark Customer Support Center for a specific version, and then click **Verify**. If the version or link is valid, then information about the firmware version is shown. An error is shown if the requested firmware cannot be found.

Type

Firmware   ▾

URL link or build name

CSTAT.076.308   Verify

Enter and verify either the firmware URL link (from the Lexmark Technical Support Center) or build name. Examples are 'https://ccs.lexmark.com/firmware/materials/123456/file' or 'ABCDE.123.456'.

Build name	CSTAT.076.308
Build type	IEC
Build version	7.6.308
Models supported	Lexmark C4150, Lexmark CS720, Lexmark CS725, Lexmark CS727, Lexmark CS728

Cancel   Create Resource

Note: If an error appears, then verify that the firmware version number, or the link provided by Lexmark. If the error persists, then contact the Lexmark Customer Support Center.

URL link or build name

CSTAT.077.303   Verify

⊗ No firmware found.
Enter and verify either the firmware URL link (from the Lexmark Technical Support Center) or build name. Examples are 'https://ccs.lexmark.com/firmware/materials/123456/file' or 'ABCDE.123.456'.

Cancel   Create Resource

- **Imported app**—eSF applications that are not available in the standard Cloud Fleet Management application catalog. These files have an .fls extension. Click **Choose File** to browse for the esf application file. When a valid file has been selected, information about the eSF application is shown. An error is shown if the requested eSF application file is not valid.

Type

Imported app ▾

Choose an app file to upload into this resource. An app file typically has a .fls extension

| Choose File | cloudAuth_e6-5.6.31.fls | ✕ |

11.85 MB

Application Name	Cloud Authentication
Application Version	5.6.31
Minimum Ram Required	3,000.00 MB
Models Supported	Lexmark (105):

C2240, C4150, C4342, C4352, C6160, C9235,
CS622, CS720, CS725, CS727, CS728, CS730,
CS735, CS820, CS827, CS920, CS921, CS923,
CS927, CS943, CX522, CX622, CX625, CX725,
CX727, CX730, CX735, CX820, CX825, CX827,
CX860, CX920, CX921, CX922, CX923, CX924,
CX927, CX928, CX930, CX931, CX942, CX943,
CX944, M3250, M5255, M5265, M5270,
MB2442, MB2546, MB2650, MB2770, MC2535,
MC2640, MS622, MS822, MS824, MS826,
MX421, MX521, MX521ade, MX521de, MX522,
MX622, MX622ade, MX622adhe, MX721,
MX722, MX725, MX822, MX824, MX826,
MX931, XC2235, XC2240, XC4140, XC4143,
XC4150, XC4153, XC4240, XC4342, XC4352,
XC6152, XC6153, XC8155, XC8160, XC8163,
XC9225, XC9235, XC9245, XC9255, XC9265,
XC9325, XC9335, XC9445, XC9455, XC9465,
XM1242, XM1246, XM3250, XM5365, XM5370,
XM7355, XM7365, XM7370, XM9335

Cancel   Create Resource

Note: If an error appears, then verify that the name is correct and that the file is an eSF application file. If the error persists, then contact the Lexmark Customer Support Center.

Type

Imported app ▾

Choose an app file to upload into this resource. An app file typically has a .fls extension

| Choose File | cloudAuth_e2-4_1.fls | ✕ |

❌ Invalid App File

1008.32 KB

Cancel   Create Resource

4. Click **Create Resource**.

Adding files to the Resource Library while creating a configuration

You can add files to the Resource Library while creating a configuration. For more information on creating a configuration, see "Creating a configuration" topic in *Lexmark Cloud Services Administrator's Guide*.

Adding firmware to a configuration and the Resource Library

1. From the Firmware tab on the Create Configuration page, click **Settings > Upload Firmware**.
2. Type a unique name and description.

3. Enter a specific firmware version, such as CSTAT.076.303, or a link provided by the Customer Support Center for a specific firmware version, and then click **Verify**.

> **Notes**
> - If the version or link is valid, information about the firmware version is shown. An error is shown if the requested firmware cannot be found.
> - If an error appears, then verify that the firmware version number, or the link provided by Lexmark, is entered correctly. If the error persists, then contact the Lexmark Customer Support Center.
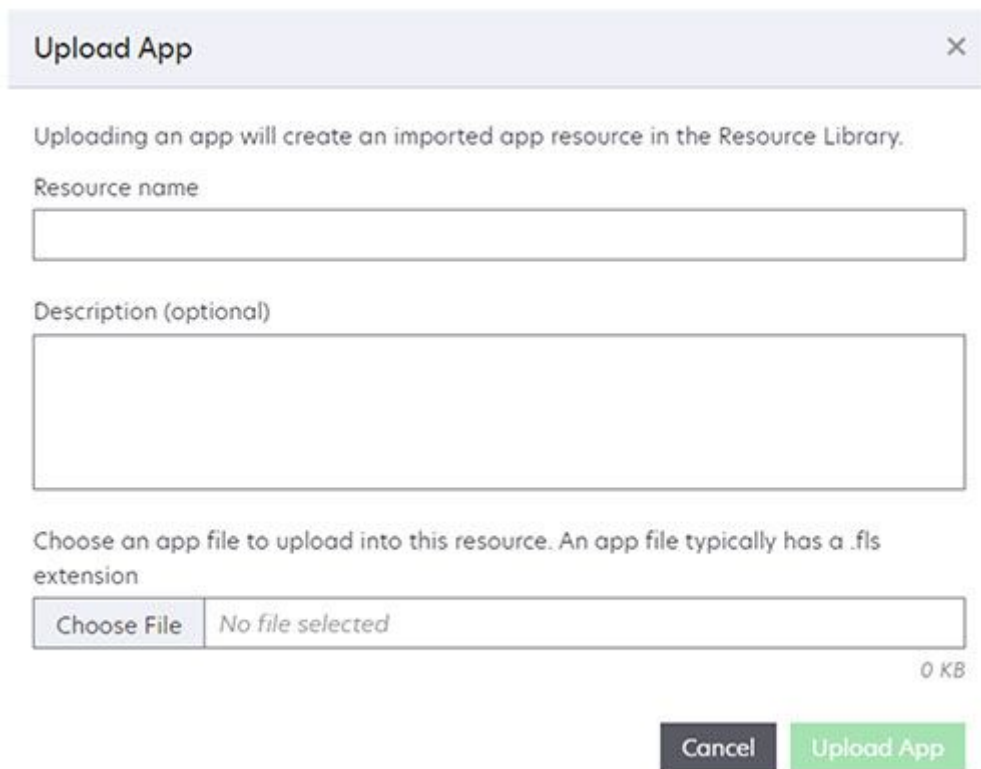
4. Click **Upload Firmware**.

Adding apps to a configuration and the Resource Library

1. From the Apps tab on the Create Configuration page, click **Apps > Upload App**.
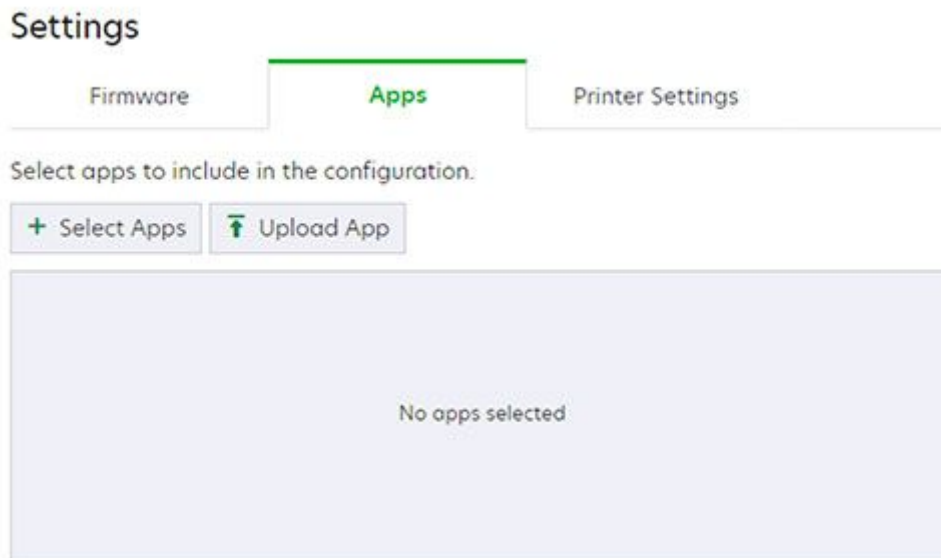
2. Type a unique name and description.

3. Click **Choose File** to browse to the esf application file.

Notes
- The file name must be an FLS file. The uploaded application is automatically added to the list of applications included in the configuration.
- When a valid file has been selected, information about the eSF application is shown. An error is shown if the requested eSF application file is not valid.
- If an error appears, then verify that the name is correct and that the file is an eSF application file. If the error persists, then contact the Lexmark Customer Support Center.

4. Click **Upload App**.

> **Note:** The eSF application is added to the current configuration and added to the Resource Library. Applications that have been uploaded to the Resource Library can be selected from the Apps catalog.
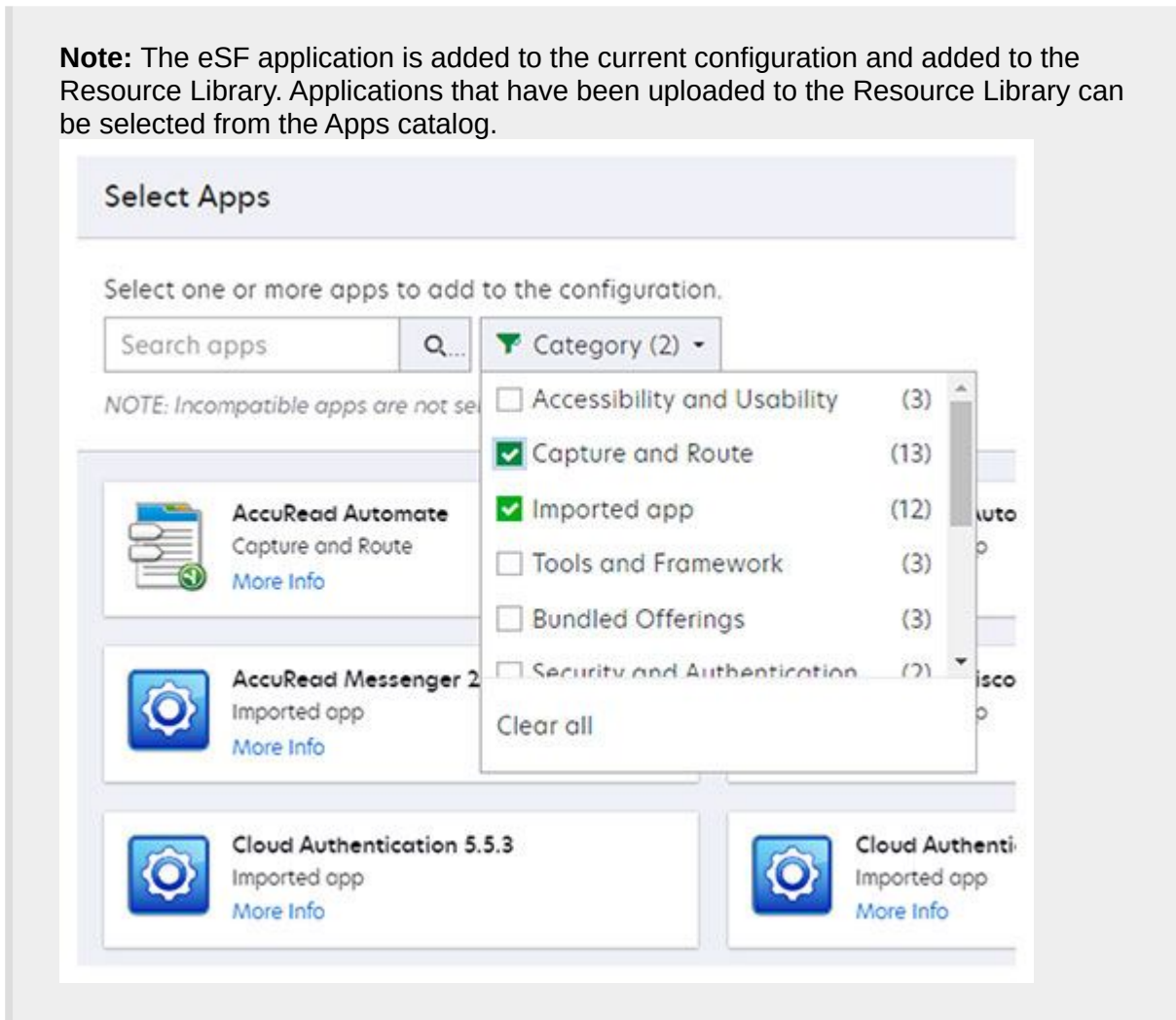
Adding a settings file to a configuration and the Resource Library

1. From the Printer Settings tab on the Create Configuration page, click **Printer Settings > Upload Settings**.
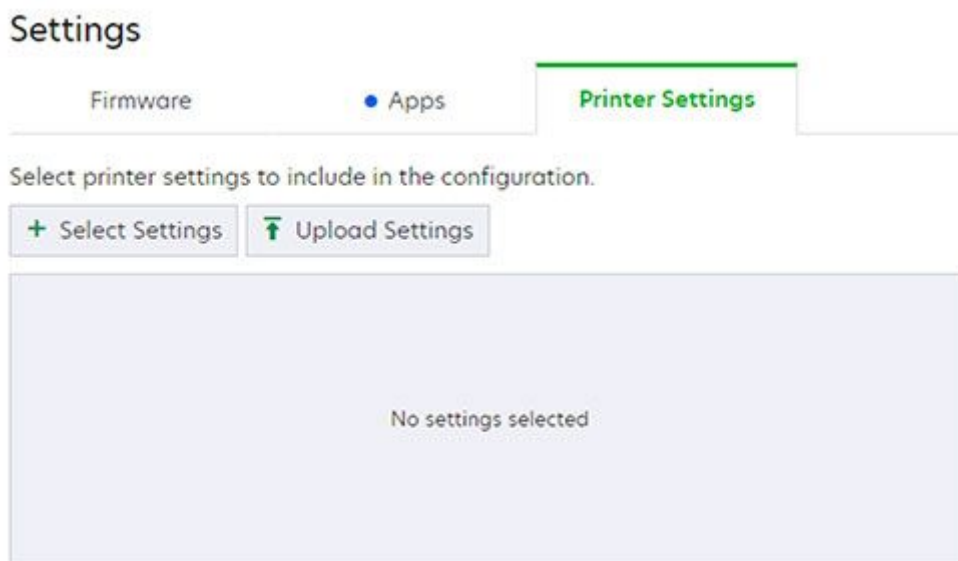
2. From the Type menu, select **UCF** or **Settings bundle**.

3. Click **Upload Settings**.

> **Note:** You can use UCF files and Settings bundle files to clone settings from one printer to another or to define a standard configuration for printers.

Deploying a configuration

You can apply a configuration to multiple printers simultaneously and then reuse it anytime.

- After a configuration is deployed, it cannot be edited.
- When a configuration is deployed, it deploys the latest recommended versions of the standard firmware and eSF applications that it contains.
- When a configuration is deployed, there is an implicit order of deployment to the printer.

  ◦ Firmware
  ◦ Applications, in the same order that they appear in the configuration
  ◦ Settings files, in the same order that they appear in the configuration

1. From the Fleet Management portal, click **Printers > Configure > Deploy configuration**.
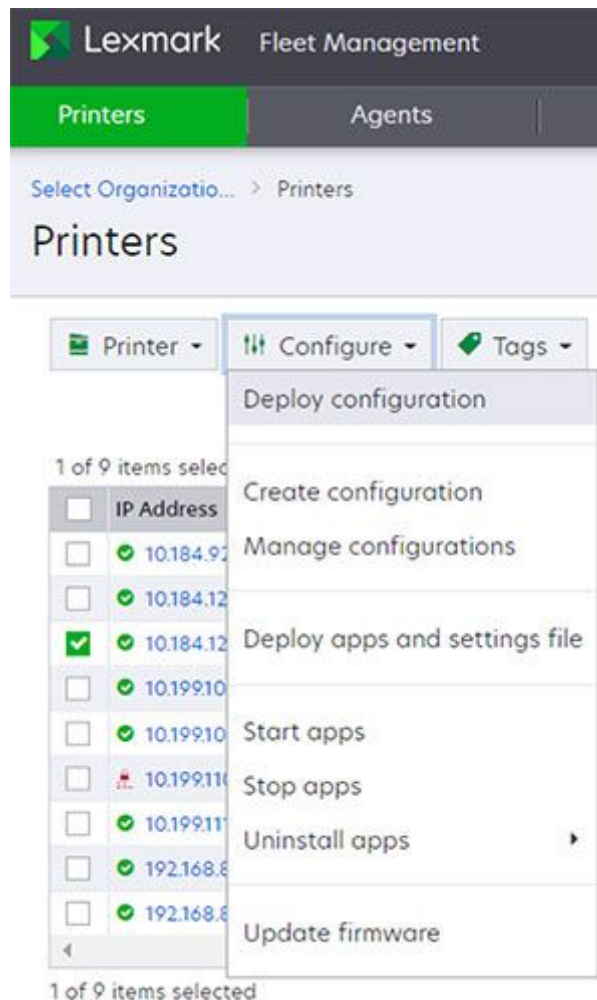
2. Choose the configuration to deploy, and then click **Deploy configuration**.
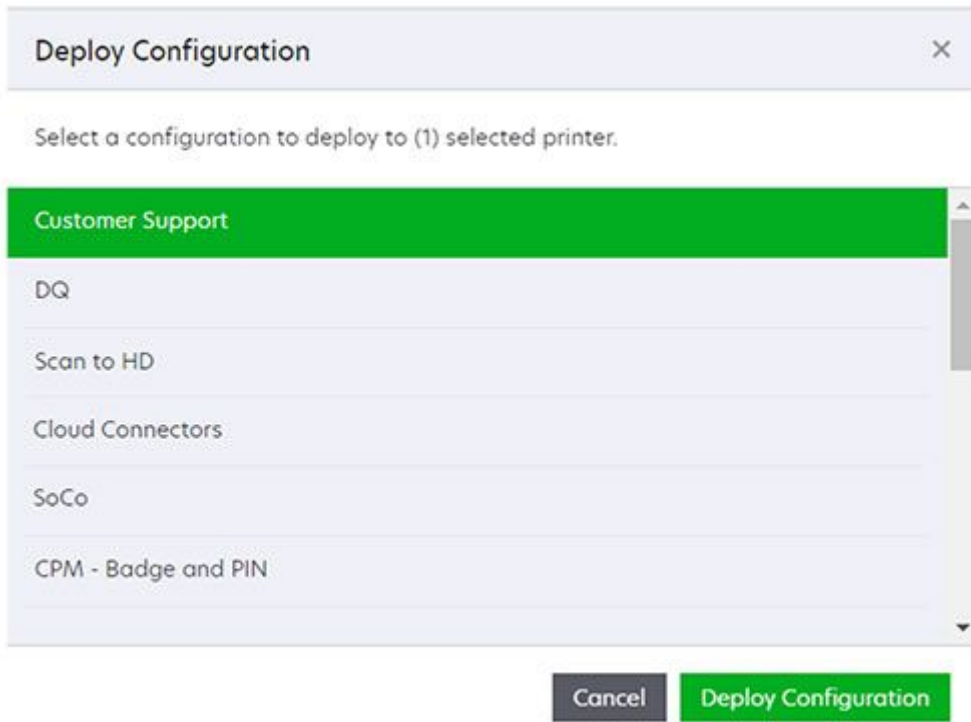
**Note:** You can view the status of the deployment in the Tasks tab.
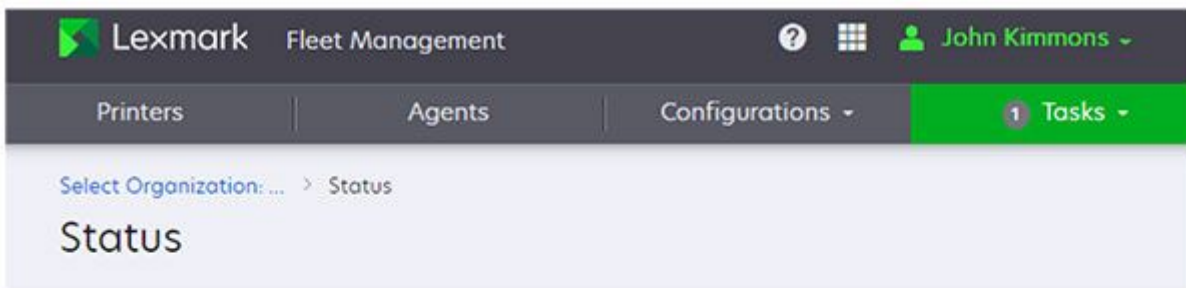
Redeploying a configuration

Configurations can be redeployed as many times as needed. Each time it deploys the latest recommended versions of the standard firmware and eSF applications that it contains. Items added from the Resource Library retain their original version.

Managing a configuration
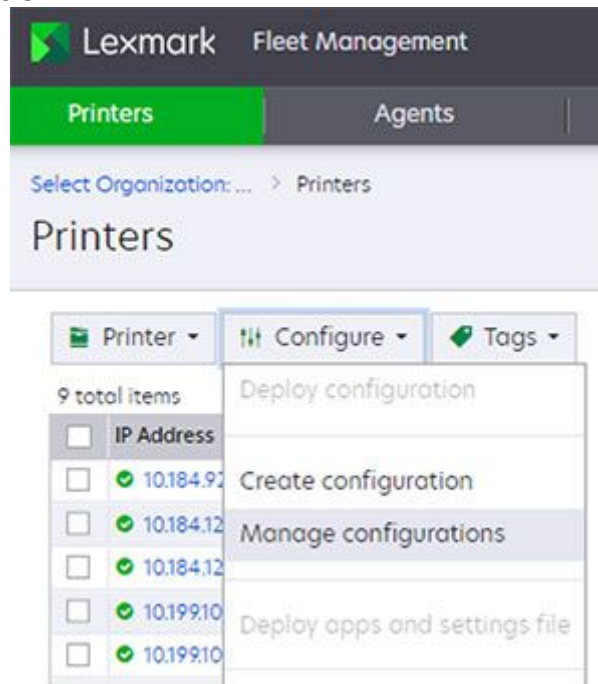
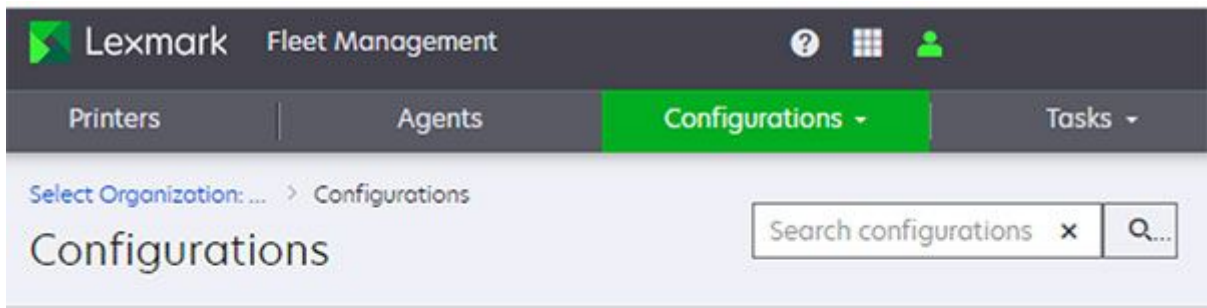After creating configurations, you can edit, copy, or delete them, or set them as default configurations.

Note: After deploying a configuration, it cannot be edited.

You can access the list of configurations by clicking **Configurations > Configurations**. You can also access the list of configurations by clicking **Printers > Configure > Manage configurations**.

Editing a configuration

Only configurations that have not been deployed can be edited. These configurations are indicated by a **No** in the Deployed column.

1. From the Configurations page, click the name of the configuration.

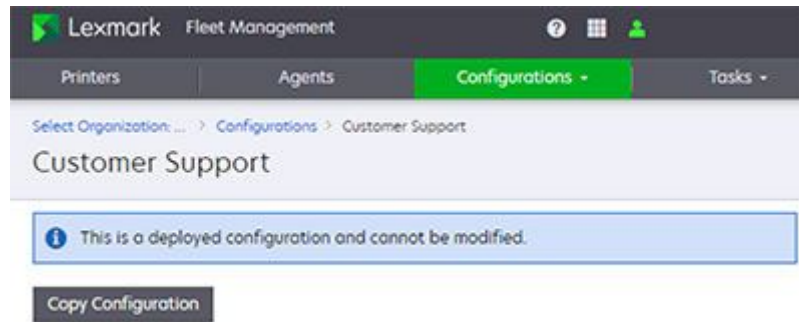**Note:** If the name of a deployed configuration is clicked, an error message is shown.

2. Edit the configuration, and then click **Save Changes**.

Copying a configuration

1. To copy a configuration do one of the following.

   ◦ From the Configurations page, select a configuration, and then click **Copy**.
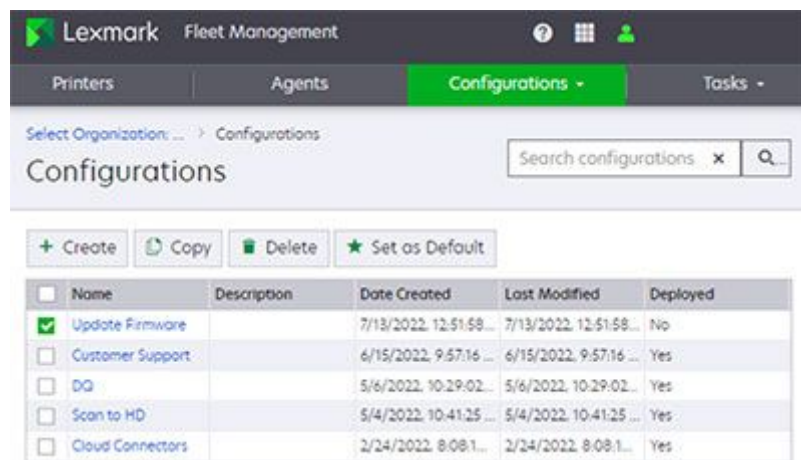
   ◦ Click the name of a deployed configuration, and then click **Copy Configuration**.

2. Type the name of the new configuration, and then click **Copy Configuration**.

> **Note:** Selecting Edit configuration after copy opens the newly created configuration in edit mode.

> **Note:** Users with the Partner Administrator role can copy a configuration to any organization under the channel partner's parent organization by entering the name of the destination organization.

Deleting a configuration

1. From the Configurations page, select one or more configurations.
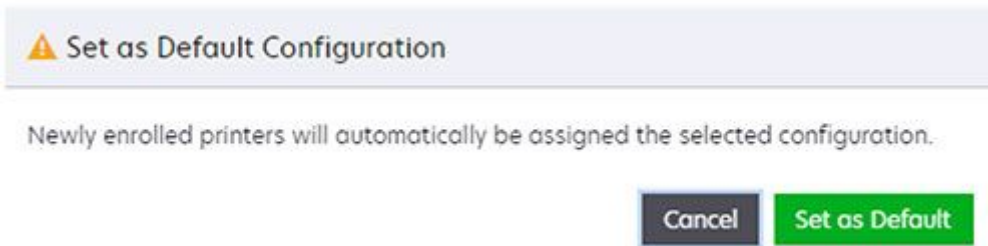2. Click **Delete > Delete configuration**.

Setting or removing a default configuration

A configuration can be designated as a default configuration. A default configuration is automatically deployed to newly enrolled printers.

Setting a default configuration

1. From the Configurations page, select a configuration, and then click **Set as Default**.
2. Click **Set as Default**.

⚠ Set as Default Configuration

Newly enrolled printers will automatically be assigned the selected configuration.

Cancel   Set as Default

Removing a default configuration

1. From the Configurations page, select a configuration, and then click **Remove Default**.
2. Click **Remove Default**.

⚠ Remove Default Configuration

This configuration will no longer be automatically deployed to printers newly enrolled to this organization.

Cancel   Remove Default

Deploying files without using a configuration

Deploying a firmware

You can update firmware without including it in a configuration. Firmware can either be updated now or you can schedule the update at a later time.
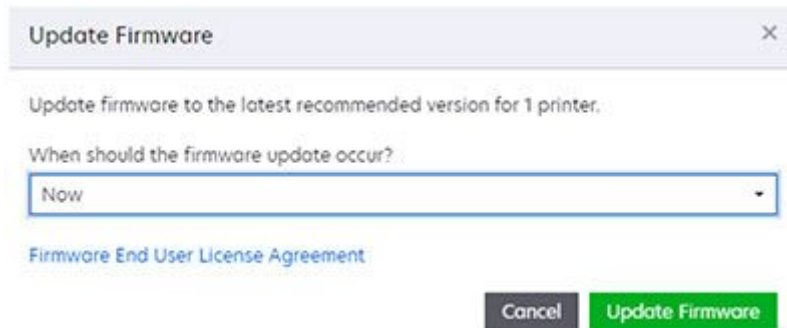
1. From the Fleet Management portal, in the Printers page, select one or more printers.
2. Click **Configure > Update Firmware**.
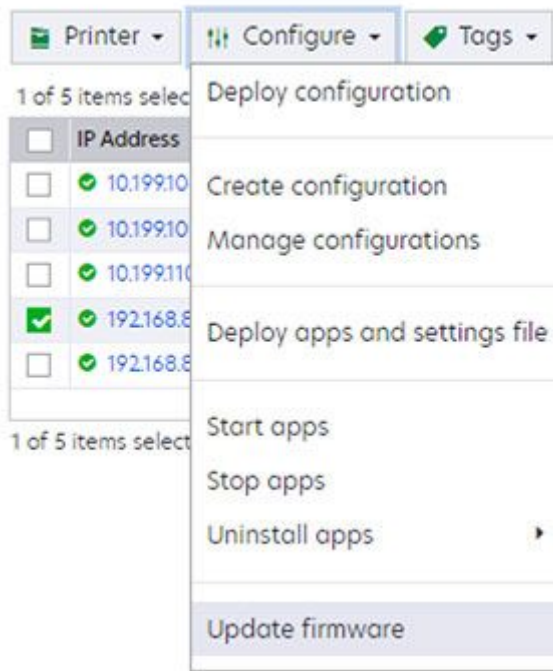
3. In the Update Firmware window, select any of the following:
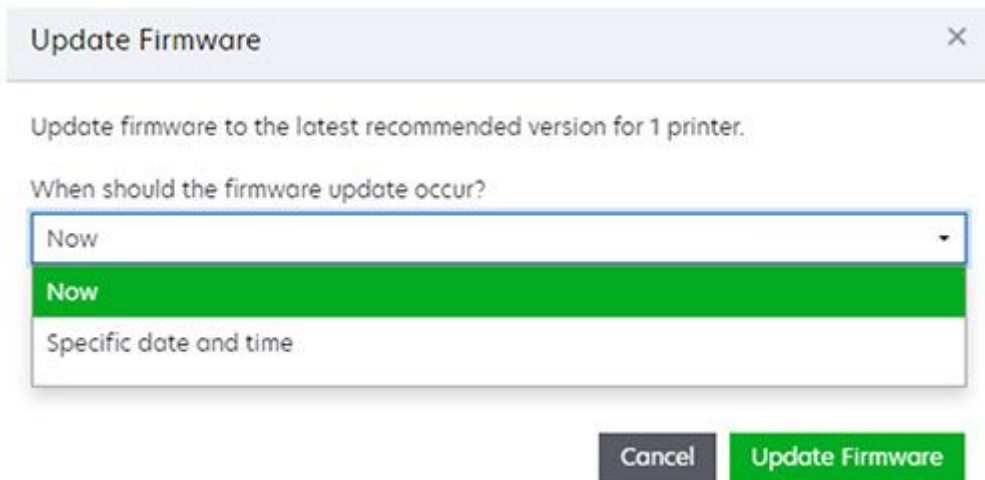
- ◦ **Now**—Sends an Update firmware task to the agent associated with each selected printer. The latest recommended version of firmware is sent to each selected printer.

> **Note:** This may adversely affect latency on your network.

- ◦ **Specific date and time**—Schedule the firmware updates in order to minimize network latency and impact on your business operations.

The Update Firmware window shows date and time selection options. Firmware on the selected printers are updated at the date and time specified. An Update firmware task is sent to the agent associated with each selected printer at the date and time specified. The latest recommended version of firmware is sent to each selected printer.

When should the firmware update occur?

This menu toggles the Update Firmware window between the Now and Specific date and time options.

Scheduled task name

This field allows you to name the firmware update operation. This name is used to identify the update task on the Schedule page.
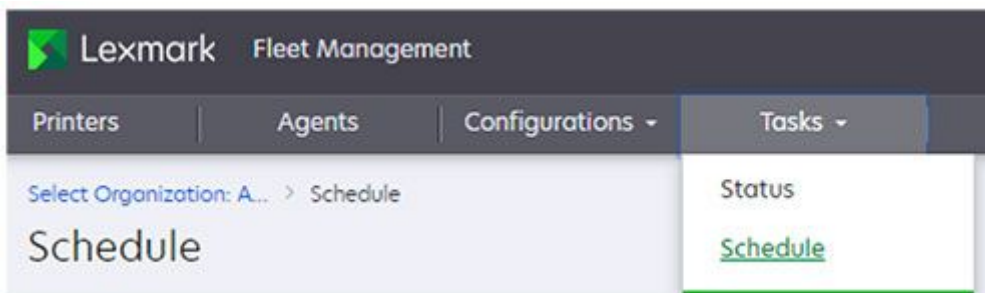
You can make changes to a scheduled task before it starts by clicking on the name of the task. You can also delete tasks that have not yet started by selecting them, and then clicking **Delete**.
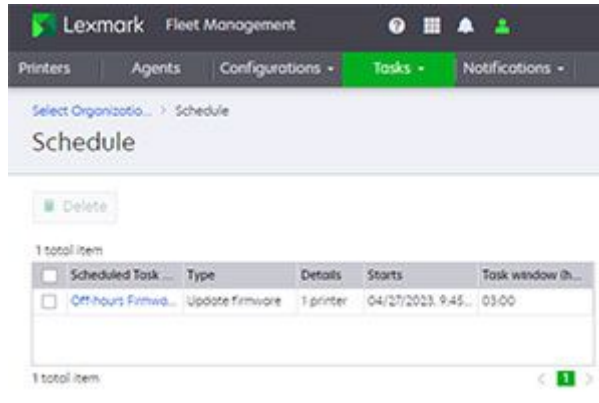
> **Note:** Once a scheduled task has started, it cannot be modified nor deleted.

Start date, Start time, and Time zone

These fields determine when the Firmware update task will start. The time zone field allows you to regionalize the start time. This is helpful if the locations of your printers span multiple time zones.

Task window

The task window parameters determine how much time will be allowed to update the firmware on all the selected printers. They are used to set a time limit on the duration of the updates to minimize the impact on your network. No firmware updates will be initiated after the task window expires.

> **Notes**
> - Any firmware update job that is not launched in the specified task window will expire.
> - If you are updating firmware for multiple printers, then make sure that the task window is large enough.
> - For a large number of printers, divide them into batches to further minimize the network impact.

4. Click **Update Firmware**.

Deploying applications and settings

You can deploy printer applications and settings files to printers without having to create a configuration.

> **Note:** This deployment is for one time only and is not saved for reuse.

1. From the Fleet Management portal, in the Printers page, select one or more printers.
2. Click **Configure > Deploy apps and settings file**.
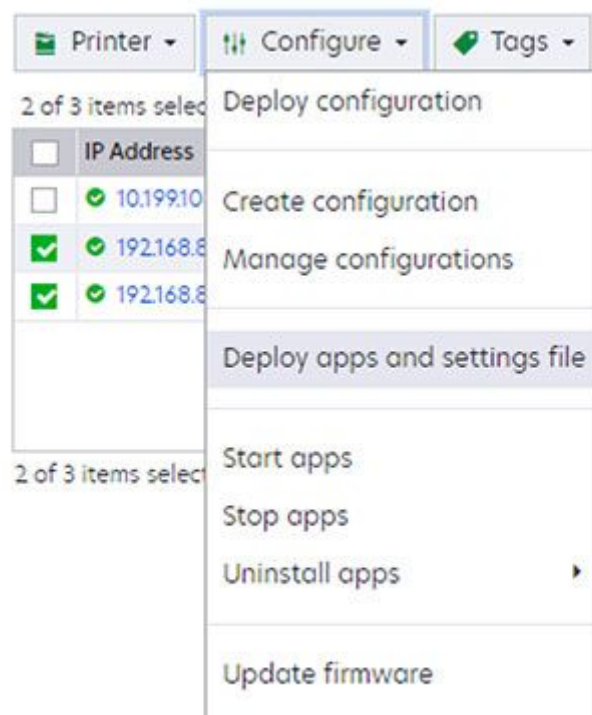
3. In the Upload Files window, click **Choose Files** to browse for the application and settings file or drag and drop the files onto the Upload Files window, and then click **Done**.
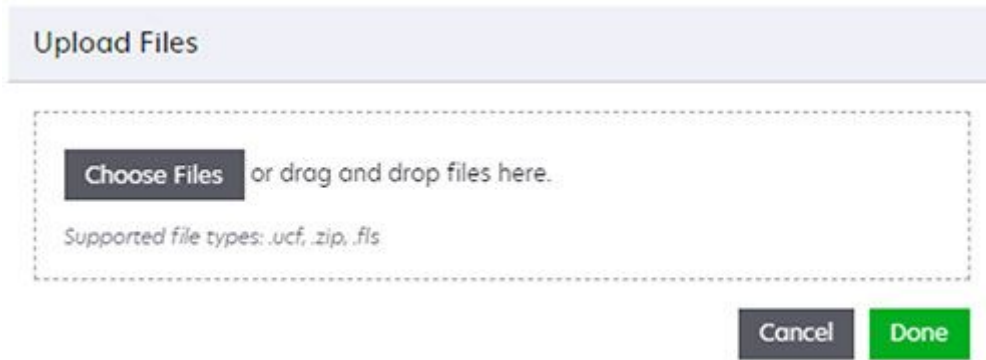
Customize your print environment

Cloud Print Management overview

Cloud Print Management lets you securely submit and release print jobs at an enabled printer and then capture that activity in Analytics. There are several ways you can choose to submit and release print jobs and any or all may be used in your organization. The various ways of submitting and release print jobs are as follows:

- Print Release
- Hybrid Print Release
- Direct Print

Notes

- All methods require connectivity with Lexmark Cloud Services.
- All printers used with Cloud Print Management must be enrolled in Cloud Fleet Management.

Print Release

Print Release lets you submit print jobs to Lexmark Cloud Services, where they are securely stored while waiting to be printed. To print submitted jobs, log in at a printer configured for Print Release and then select the jobs that you want to print. The printer reports the job metrics to the Analytics services for your review and analysis.

Print jobs may be submitted using any of the following methods:

- A client application on the workstation
- Dragging-and-dropping in the Cloud Print Management portal
- A print extension added to the Google Chrome browser
- The Lexmark Print application for the iOS operating system software or the Android platform
- An e-mail sent to an address configured for your organization

Hybrid Print Release

When you print using Hybrid Print Release, a client application on their workstation securely stores the print job on your workstation and then informs Lexmark Cloud Services that a user has a hybrid print job ready to be released. When the user authenticates, and selects their print job for release, the printer communicates directly with your workstation to release the print job. The print job never leaves your organization's network.

> **Note:** Make sure that your workstation is online when retrieving the hybrid print job, and that a client application is installed on each of your workstations.

Direct Print

Direct Print lets you submit print jobs directly to an administrator-designated, network-connected printer using port 9100 through a client application on your workstations. The print job never leaves your organization's network. The print job never leaves your organization's network.

Using Cloud Print Management

Cloud Print Management roles

Roles must be based upon the users' needs and job activities. Users who receive access to a print release method must have at least one of the following roles:

- Users who will be submitting and releasing print jobs:

    ◦ For Print Release—Print Release Management User
    ◦ For Hybrid Print Release—Hybrid Print Management User
    ◦ For Direct Print—Direct Print Management User
- Users who will be administering the print environment for their organization:

    ◦ For Print Release—Print Release Management Administrator
    ◦ For Hybrid Print Release—Hybrid Print Management Administrator
    ◦ For Direct Print—Direct Print Management Administrator
- Users who need to review the print activity of their organization, but will not be administering the print environment:

    ◦ For all print release methods—Print Release Management Reporting Analyst
- Channel Partners who can administer any of the print release methods in their customer's organization must be a member of a Child Organization Access Group that includes the appropriate administrator role for the print release method:

    ◦ Before you can administer a print release method in one of your customer organizations, it must be enabled in your organization.

For more information on user roles definition, see "Understanding roles" topic in *Lexmark Cloud Services Administrator's Guide*.

Assigning roles

User roles are managed from the Account Management portal. You can assign roles to users in three ways:

- **Assigned to an individual user**—Requires assigning roles manually to each user.
- **Assigned through group membership**—Allows a set of roles to be given to users by making them a member of a group. Users can be members of more than one group.
- **Assigned as an organization role**—Automatically assigns the organization roles to all users in the organization.

Note: The assignment method depends on the needs of the organization. For more information, see "Overview" topic in *Lexmark Cloud Services Administrator's Guide*.

Understanding Cloud Print Management administrative options

Various Cloud Print Management features and functions can be tailored through the Organizational Settings menu. From the Print Management portal, click **Administration > Organizational Settings**.
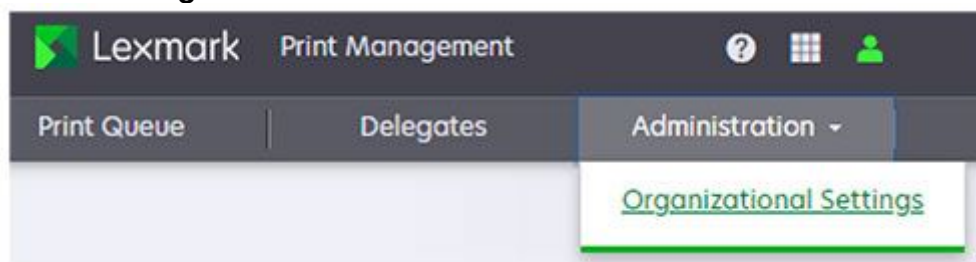
Note: The user must have the **Print Release Management Administrator** role to see and access the Administration menu. For more information, see "Configuring organizational settings" topic in *Lexmark Cloud Services Administrator's Guide*.

Deploying the Cloud Print Management bundle

Before you can use Cloud Print Management to release print jobs, you must deploy the Cloud Print Management eSF application bundle.

Creating a configuration for Cloud Print Management

The eSF applications that make up the Cloud Print Management bundle are deployed from the Fleet Management portal by creating a configuration. For more information on creating a configuration, see "Creating a configuration" topic in *Lexmark Cloud Services Administrator's Guide*.
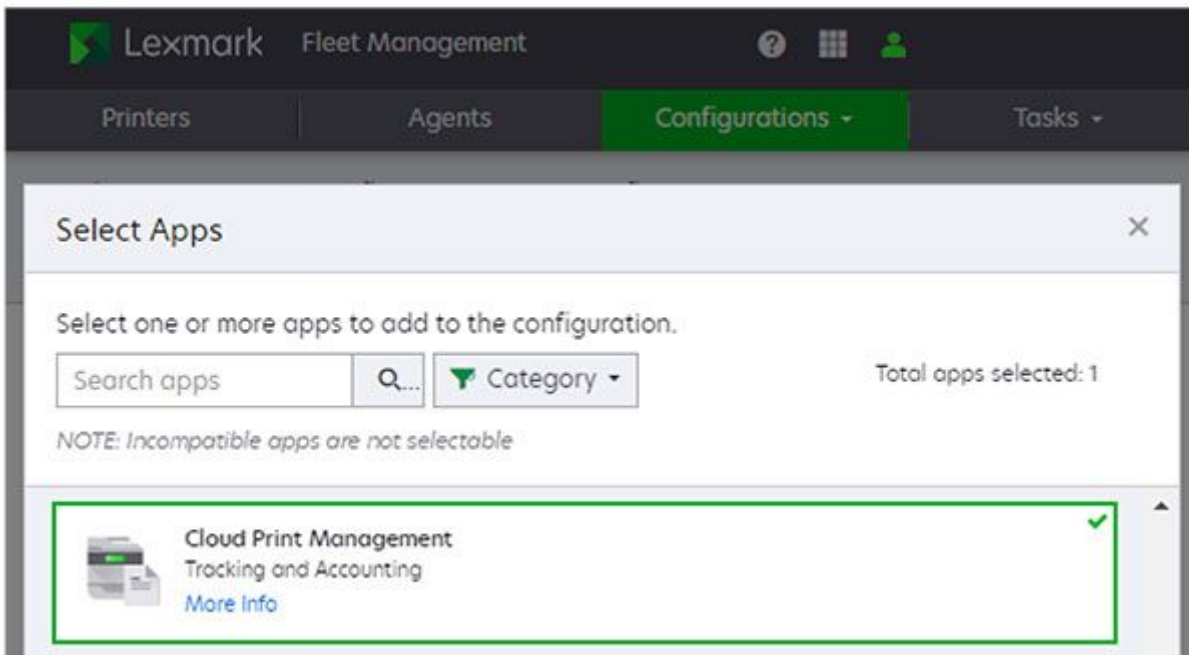
Note: Only printers managed by Cloud Fleet Management can have the Cloud Print Management bundle deployed from the Fleet Management portal.

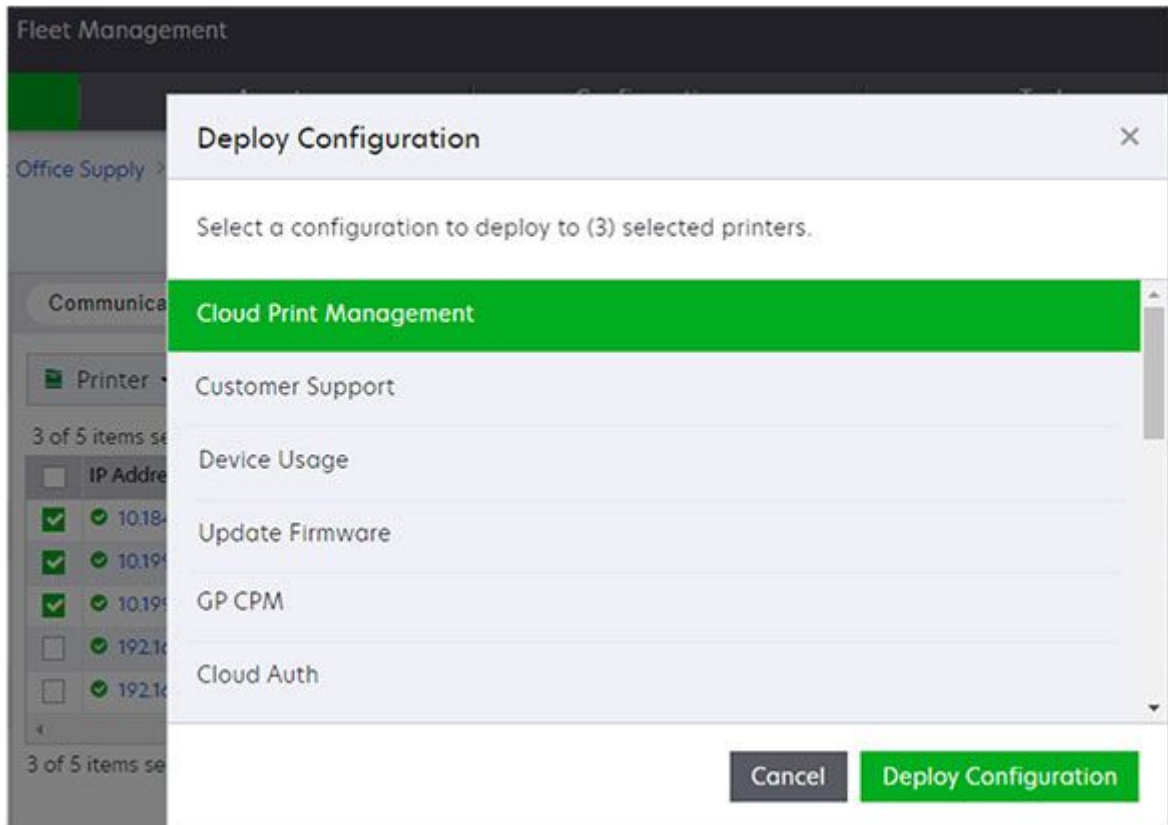**Deploying a Cloud Print Management configuration**

You can apply a configuration to multiple printers simultaneously and then reuse it anytime.

1. From the Fleet Management portal, click the **Printers** tab.
2. Select one or more printers, and then click **Configure > Deploy configuration**.
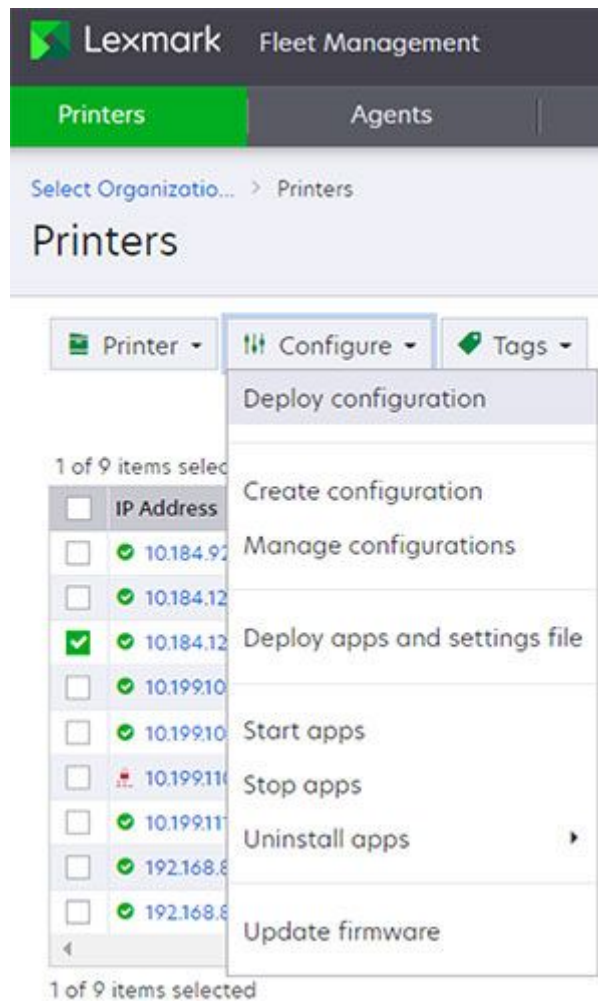
3. In the Deploy Configuration window, select the configuration, and then click **Deploy configuration**.

Note: For more information on deploying a configuration, see "Deploying a configuration" topic in *Lexmark Cloud Services Administrator's Guide*.
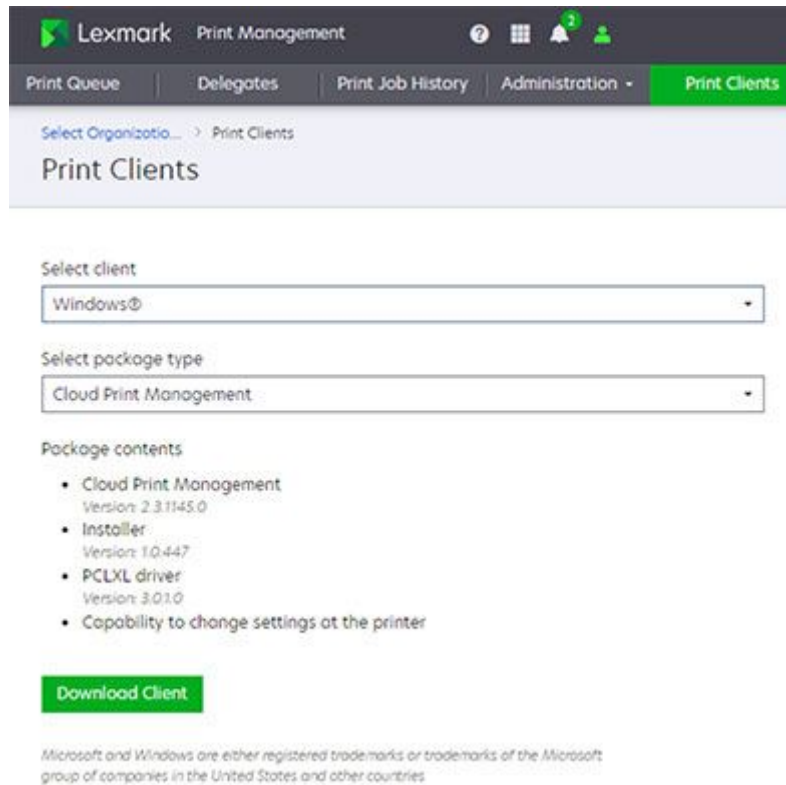
Using Cloud Print Management clients

To use Cloud Print Management, Hybrid Print Release, or Direct Print, you must install the Lexmark Print Management Client (LPMC) client application on the users' workstations.
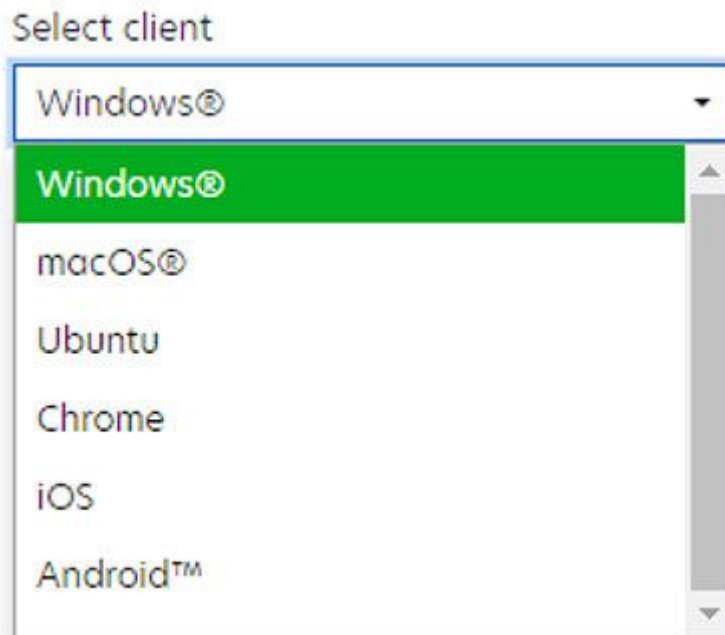
Downloading a client package

You can download the LPMC from the Print Clients tab in the Print Management portal.

1. From the Print Management portal, click **Print Clients**.
2. In the Print Clients page, do the following:

○ From the Select client menu, select any of the following:

- **Windows®**
- **macOS®**
- **Ubuntu**
- **Chrome**—The Cloud Print Management for Google Chrome™ extension on the Chrome Web Store for use with the Google Chrome operating system and Chrome browser
- **iOS**—The Lexmark Print application for iOS on the Apple App Store online store
- **Android™** —Lexmark Print application for Android on Google Play™ store

> **Note:** If you select Chrome, iOS, or Android, then you are provided a link to the external site for the Lexmark Cloud Services print client application.

◦ From the Select Package Type menu, select any of the following:

> **Note:** You can download an LPMC package with default settings for Cloud Print Management, Hybrid Print Release, or Direct Print. You can also create a customized LPMC package by selecting the Custom Package option.

Select package type

Cloud Print Management ▾
Cloud Print Management
Hybrid Print Management
Direct Print
Custom Package
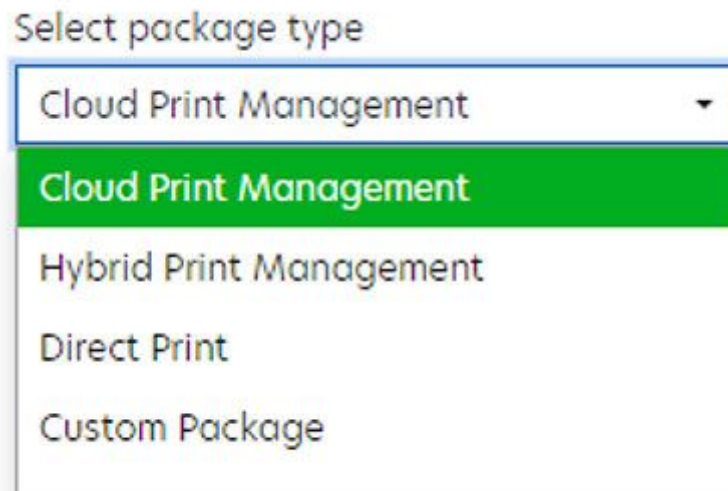
- Cloud Print Management
- Hybrid Print Management
- Direct Print
- Custom Package

3. If you selected Cloud Print Management or Hybrid Print Management, then click **Download Client** to download the package.

   If you selected Custom Package, then you have to create a custom package.

> **Note:** If you selected Direct Print, then see "Using Direct Print" topic in *Lexmark Cloud Services Administrator's Guide*.

Creating a custom LPMC package

The Custom Package option lets you create an LPMC installation package that is suited to your needs. To customize, you can do any of the following:

- Combine one or more submission types in a single package. A single package can include Cloud Print Management, Hybrid Print Management, and Direct Print.
- Change global client settings.
- Select the print driver to install.
- Set an LPMC print queue as the default print queue on the workstation.

Once the custom package is ready, click **Create > Download**.

Note: The package is a compressed file that must be extracted before installation.

Installing Lexmark Print Management clients on workstations

After downloading default LPMC client applications, from the Client Download page, you can install them on workstations. For custom packages, you must extract the downloaded file before installing them. For more information on installing LPMC, see "Installing the Lexmark Print Management Client" topic in *Lexmark Cloud Services Administrator's Guide*.

Printing with Cloud Print Management

You can submit print jobs using the following ways:

- From your workstation
- From your print queue in the Print Management portal
- From your mobile device

Printing from your workstation

From your workstation, you can submit print jobs by doing one of the following:

- From a desktop application, select **File > Print**, and then select a Print Management queue.
- From the Google Chrome operating system or browser, select **File > Print**, and then select a Print Management queue.

> **Note:** To print from the Chrome operating system or browser, you must install the Lexmark Cloud Print Management for Chrome extension. For more information, see "Sending print jobs from the Chrome OS operating system" in *Lexmark Cloud Services Administrator's Guide*.

- Using email

> **Note:** Your organization must be configured to accept print jobs using email. For more information, see "Sending print jobs using e-mail" topic in *Lexmark Cloud Services Administrator's Guide*.

Submitting a print job in the Print Management portal

1. From the Print Management portal, click **Print Queue > Upload File**.
2. Drag and drop files in the Upload File window or click **Choose Files** to browse to the file you want to print.

3. Click **Done**.

Submitting a print job from your mobile device

- Print jobs can be submitted from devices running the iOS operating system software or the Android platform. For more information, see "Mobile printing" group in *Lexmark Cloud Services Administrator's Guide*.

Using Cloud Print Management with third-party printers

You can use Cloud Print Management with printers that do not support eSF applications, including Lexmark printers that are not solutions-enabled and printers from third-party manufacturers.
Cloud Print Management is enabled on these printers by using the ELATEC TCP3 adapter, a device that connects between the customer's network and the printer. It also provides a USB connection for badge or card readers. The TCP3 adapter handles all user badge or card authentication and passes the user's print jobs from Lexmark's Cloud Print Management service to the printer. For more information, including limitations on using the ELATEC TCP3 adapter, see "Printing jobs from third-party printers using Cloud Print Management" topic in *Lexmark Cloud Services Administrator's Guide*.

Note: The Elatec TCP3 Adapter receives power either from an external 5Volt power source or from an Ethernet connection that supports power over ethernet. See the Technical Manual provided with the Elatec TCP3 for more details.

Using Direct Print

Direct Print overview

Direct Print lets you submit print jobs directly to an administrator-designated, network-connected printer using port 9100 through a client application on your workstations. The print job never leaves your organization's network.
Print jobs are sent using port 9100 by the Lexmark Print Management Client (LPMC) directly to an administrator-designated, network-attached printer. When using the Direct Print feature, print jobs never leave your organization's local network. The LPMC reports job metrics to Lexmark Cloud Services.

Enabling Direct Print

1. Enroll printers for Direct Print in Cloud Fleet Management and assign a tag to them. For more information, see .
2. Enable Direct Print for the organization. For more information, see .
3. Create Direct Print assignments. For more information, see .
4. Download and install the Lexmark Print Management Client configured for Direct Print. For more information, see .

Notes

- You must have the Direct Print Release Administrator role.
- Connectivity with Lexmark Cloud Services is required.
- A Direct Print configuration file must be applied when the LPMC is installed to enable Direct Print functionality.
- Printers used by Direct Print must be enrolled in Cloud Fleet Management.

Printing with Direct Print
You can submit print jobs by clicking **File > Print** from desktop applications, and then selecting a Direct Print queue.

Note: Using Direct Print to submit jobs is supported in desktops only, not in mobile devices.

Direct Print roles

Users given access to the Direct Print feature of Cloud Print Management must have at least one of the following roles based on tasks that they plan to perform:

- Users submitting and releasing print jobs using Direct Print must have the **Direct Print Management User** role.
- Users managing Print Management for their organization must have the **Direct Print Management Administrator** role.

- Users generating organizational Cloud Print Management reports but do not have the **Direct Print Management Administrator** role must have the **Print Release Management Reporting Analyst** role.
- Channel partners who manage printers in their customers' organizations must be members of a Child Organization Access Group. The group must have the **Direct Print Management Administrator** role assigned to it.

> **Notes**
> ○ Before a channel partner can administer Cloud Print Management in a customer organization, you must enable Cloud Print Management in the channel partner's organization. For more information, see "Assigning roles" group in *Lexmark Cloud Services Administrator's Guide*.
> ○ For more information on roles, see "Understanding roles" topic in *Lexmark Cloud Services Administrator's Guide*.

Assigning roles

User roles are managed from the Account Management portal. You can assign roles to the users in the following ways:

- **Assigned roles individually**—Requires that assigning roles manually to each user.
- **Assigned roles through groups**—Allows a set of roles to be given to users by making them a member of a group. Users can be members of more than one group.
- **Inheritance through organization roles**—Automatically assigns the organization roles to all users in the organization.

The assignment method depends upon the needs of the organization. For more information, see "Assigning roles" group in *Lexmark Cloud Services Administrator's Guide*.

Assigning printers to Direct Print

Printers used with Direct Print must be enrolled in Fleet Management. Each printer must also have at least one Fleet Management tag applied to it.
For more information on enrolling printers in Fleet Management, see "Enroll your printers" chapter in *Lexmark Cloud Services Administrator's Guide*.
For more information on applying tags to printers, see the following:

- "Creating tags" topic in *Lexmark Cloud Services Administrator's Guide*
- "Assigning tags to printer" topic in *Lexmark Cloud Services Administrator's Guide*
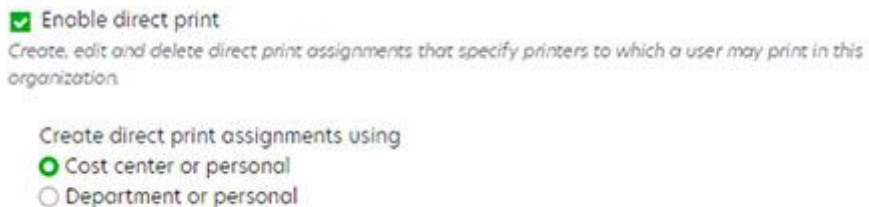
Enabling Direct Print

Direct Print is enabled on the Print Management Organizational Settings page.

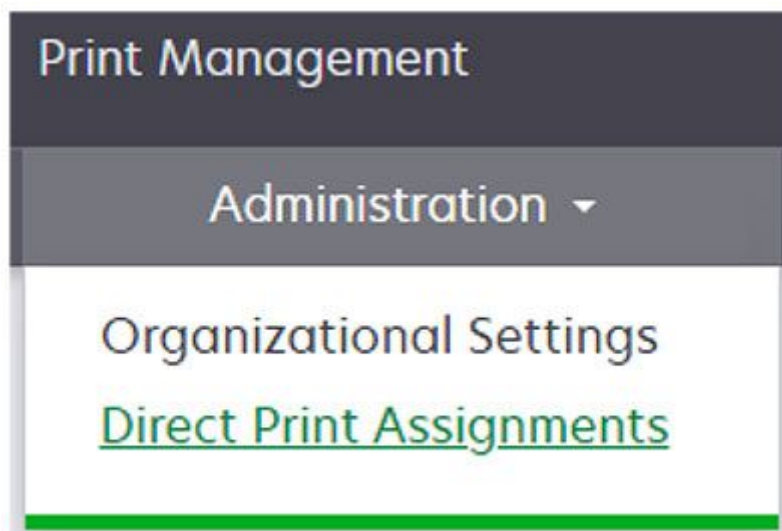1. From the Print Management web portal, click **Administration > Organizational Settings**.
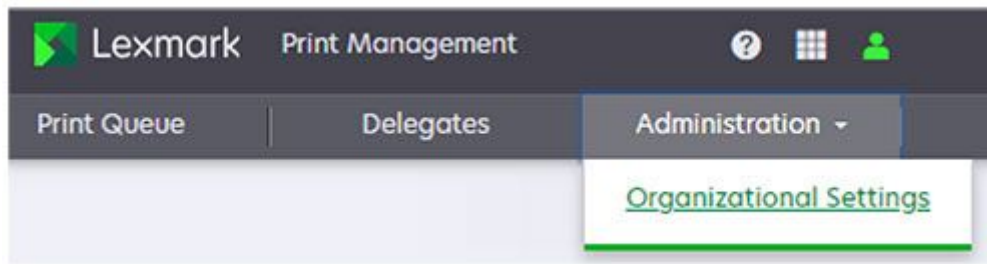
2. Select **Enable direct print**.
3. Select whether to use a cost center or a department.

Notes

- The Direct Print assignment applies to all members of the designated cost center or department. In either case, Direct Print assignments can also be applied to individual users.
- You must have the Direct Print Release Administrator role to enable Direct Print.
- Users must have the Direct Print Release User role to use Direct Print.
- Cost centers and departments are defined and assigned to users in the Account Management portal.

If Direct Print is enabled, then an additional menu item is available in the Administration menu.

Creating Direct Print assignments

1. From the Print Management web portal, click **Administration > Direct Print Assignments**.

2. Depending on your requirement, select the **Cost Center** or **Department** or **Personal** tab, and then click **Create Assignment**.

> **Note:** If there are existing Direct Print assignments, then the Direct Print Assignments page shows them.

Direct Print Assignments

ⓘ You can download a print client package for a direct print assignment from the Print Clients page.

Cost Centers   Personal

✚ Create Assignment   🗑 Delete Assignment   ▼ Printer Tags ▾

1 total item

	Assignment Name	Cost Centers	Printer Tags
☐	Direct Print by Cost Center	CC549	Direct Print

1 total item   View 25 ▾   ‹ **1** ›

3. In the Create Direct Print Assignment window, do the following:

> **Note:** The Direct Print assignment applies to all members of the designated cost center or department. In either case, Direct Print assignments can also be applied to individual users.

   ◦ **Cost Center or Department assignments**—Cost center and department assignments are applied to all members of that cost center or department.

Note: The Create Assignments forms are the same for cost centers and departments.

- **Assignment name**—Type a unique assignment name.
- **Cost center name** or **Department name**—Type the name of the cost center or department that will be associated with this assignment. A list of possible matches is shown as characters are entered.

Notes
- The cost center or department chosen must match one in the Account Management portal. If the name entered does not match, the caution symbol is shown before the name.
- You can apply only one cost center or department to a Direct Print assignment.
- A cost center or department can only be associated with one Direct Print Assignment.

- **Tags identifying printers this cost center may use for direct printing**—
  Printer tags are used to create the connection between a Direct Print
  Assignment and one or more printers. Type the tag name to be associated with
  this assignment. Multiple tags can be associated with a Direct Print
  assignment. Select a tag name from the list, and then click **Add**.

Tags identifying printers this cost center may use for direct printing

| Start typing... | + Add |

Find and select a tag from Fleet Management. The number of printers identified by
a specific tag can change.

Printers : 5

Mono ✕

Notes
- You can use only tags that were previously defined in the Fleet
  Management portal.
- When a tag is added, tag names and the total number of printers
  with the added tag names appear.
- You can associate an assignment to up to ten printers only. While
  you can save an assignment with more than ten printers, you
  cannot download a Print Client package associated with that
  assignment.

- **Personal**—Apply assignments only to specific individuals.

Create Direct Print Assignment ✕

Assignment name

Enter a unique name for this direct print assignment

E-mail addresses of registered users to be included in this assignment

| Start typing... | + Add |

Find and select an e-mail address.

Tags identifying printers these users may use for direct printing

| Start typing... | + Add |

Find and select a tag from Fleet Management. The number of printers identified by
a specific tag can change.

Printers : 0

⚠ To download a client for this assignment from the Print Clients page, it must contain 1 to 10
printers.

Cancel   Create Assignment

- **Assignment name**—Type a unique assignment name.
- **E-mail addresses of registered users to be included in this assignment**—
  Type the email address of an individual associated with this assignment. Multiple
  individuals can be associated with the same Direct Print assignment.

E-mail addresses of registered users to be included in this assignment

Start typing...   + Add

Find and select an e-mail address.

caretjim@outlook.com ✕

> **Note:** Only users with the Direct Print Release User or Direct Print Release Administrator User role are shown.

- **Tags identifying printers these users may use for direct printing**—Printer tags are used to create the connection between a Direct Print Assignment and one or more printers. Type the tag name to be associated with this assignment. Multiple tags can be associated with a Direct Print assignment. Select a tag name from the list, and then click **Add**.

> **Notes**
> - You can use only tags that were previously defined in the Fleet Management portal.
> - When a tag is added, tag names and the total number of printers with the added tag names appear.
> - You can associate an assignment to up to ten printers only. While you can save an assignment with more than ten printers, you cannot download a Print Client package associated with that assignment.

4. Click **Create Assignment**.

Download Direct Print Client Package Error

If you include an assignment containing more than ten printers when creating a direct print client package, then client package download fails. The Direct Print assignment that contains more than ten printers must be modified to reduce the number of printers to ten or less. The following error message is displayed when a download fails.

❌ Unable to Download Direct Print Client Package

None of the selected assignments contain 1 to 10 printers so they are not eligible for downloading in a client package.

Verify the Direct Print assignments specify the correct printer tags. If the tags are correct, then contact the Fleet Management administrator to verify the tags are assigned to the correct printers.

OK

Using Direct Print clients

To use Direct Print, you must install a Direct Print–capable version of the Lexmark Print Management Client (LPMC) on a user's workstation.

Downloading a Direct Print client package

You can download the LPMC configured for Direct Print from the Print Clients tab in the Print Management portal. You can create either a default Direct Print package or a Custom Package.
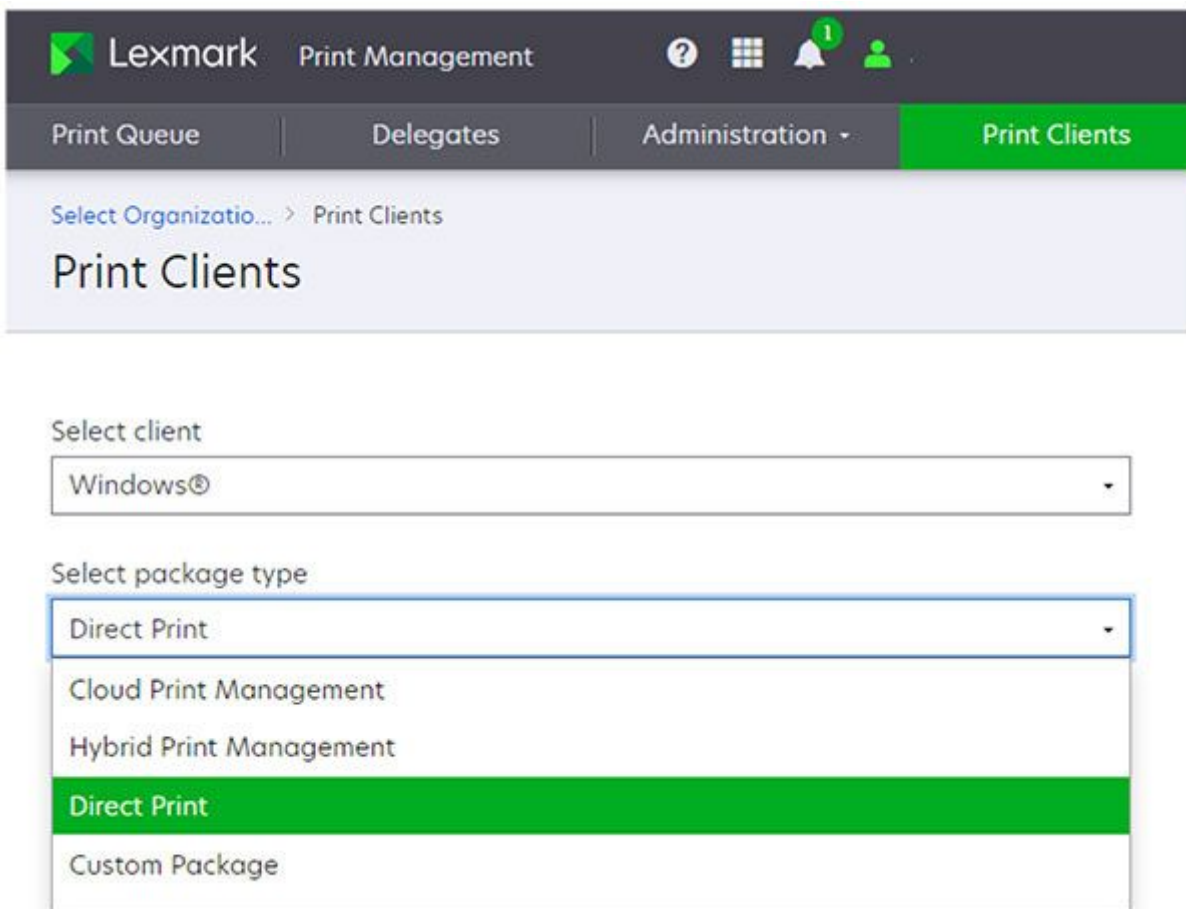
- **Direct Print**—Creates an LPMC package that only supports Direct Print.
- **Custom Package**—Allows you to create an LMC package that supports Direct Print along with Cloud Print Management, Hybrid Print Management, or both. For more information on creating a customer client package, see Using Cloud Print Management clients on page 142.

Notes

- Direct print is only available for the Windows operating system.
- The minimum LPMC version is 2.3.1145.0.
- The LPMC must be installed with a Direct Print configuration file for Direct Print to be available to the user

Selecting a default Direct Print package

1. From the Print management portal, click **Print Clients**.
2. In the Print Clients page, do the following:

   - From the Select client menu, select **Windows®**.
   - From the Select Package Type menu, select **Direct Print**.

Select package type

Direct Print

Package contents

- Direct Print
  Version: 2.3.1145.0
- Installer
  Version: 1.0.447
- PCLXL driver
  Version: 3.0.1.0
- Capability to change settings at the printer

Select one or more direct print assignments to include in the package.

Selected assignments: 0 cost centers, 1 personals

| | Cost Centers | Personal | |

1 of 1 items selected

	Assignment Name	E-mail	Printer Tags
☑	Jim's	caretjim@outlook.com	Local Printer

1 of 1 items selected   View   25 ▾   ‹ **1** ›

Download Client

3. Select one or more Direct Print assignments, and then click **Download Client**.

> **Note:** The package is a compressed file that must be extracted before installation.

Creating a custom Direct Print package

You can create a Direct Print package that can include either Cloud Print Management or Hybrid Print Management or both.

1. From the Print management portal, click **Print Clients**.
2. In the Print Clients page, do the following:

   ◦ From the Select client menu, select **Windows®**.
   ◦ From the Select Package Type menu, select **Custom Package**.

Select package type

Custom Package

Create and then download a custom package that includes:

- Global client settings
- Cloud Print Management and/or Hybrid Print Management and/or Direct Print
- Print driver selection
- Default printer selection

Create Package

3. Click **Create Package**.

Select Organization: Caret O... > Print Clients > Create Custom Windows Pa...

Create Custom Windows Package

4. Select any of the following:

   ◦ **Enable Cloud Print Management**
   ◦ **Enable Hybrid Print Management**
   ◦ **Enable Direct Print**
5. Select one or more Direct Print assignments, and then click **Download Client**.

Direct Print

☑ Enable Direct Print

Select one or more direct print assignments to include in the package.

Selected assignments: 0 cost centers, 1 personals

Cost Centers	**Personal**

1 of 1 items selected

☑	Assignment Name	E-mail	Printer Tags
☑	Jim's	coretjim@outlook.com	Local Printer

1 of 1 items selected   View   25 ▾   < **1** >

> **Note:** The package is a compressed file that must be extracted before installation.

Installing Direct Print clients on workstations

After downloading default LPMC client applications, from the Client Download page, you can install them on workstations. For custom packages, you must extract the downloaded file before installing them.

For more information on the LPMC, see "Installing the Lexmark Print Management Client" topic in *Lexmark Cloud Services Administrator's Guide*.

Printing with Direct Print

You can submit print jobs by clicking **File > Print** from desktop applications, and then selecting a Direct Print queue. Using Direct Print to submit jobs is supported in desktops only, not in mobile devices.

Using a secure login code

Using a secure login

User logins can be handled in various ways with Cloud Print Management. One method is the use of a secure login code, a one-time authentication code that lets users log in to a cloud-enabled printer. Secure login can be used when the badge or PIN login method is not configured, or the user does not have a badge or PIN available. A new secure login code must be obtained from Lexmark Cloud Services each time a user logs into a cloud-enabled printer.

Notes

- The secure is valid for 15 minutes.
- Secure login code is available when identity federation is used.
- A secure login code can be obtained from the Lexmark Cloud Services Print Management web portal and from the Lexmark Print application on iOS or the Android devices.

Setting up secure login

1. From the Account Management portal, click **Organization > Printer Login Configuration**.
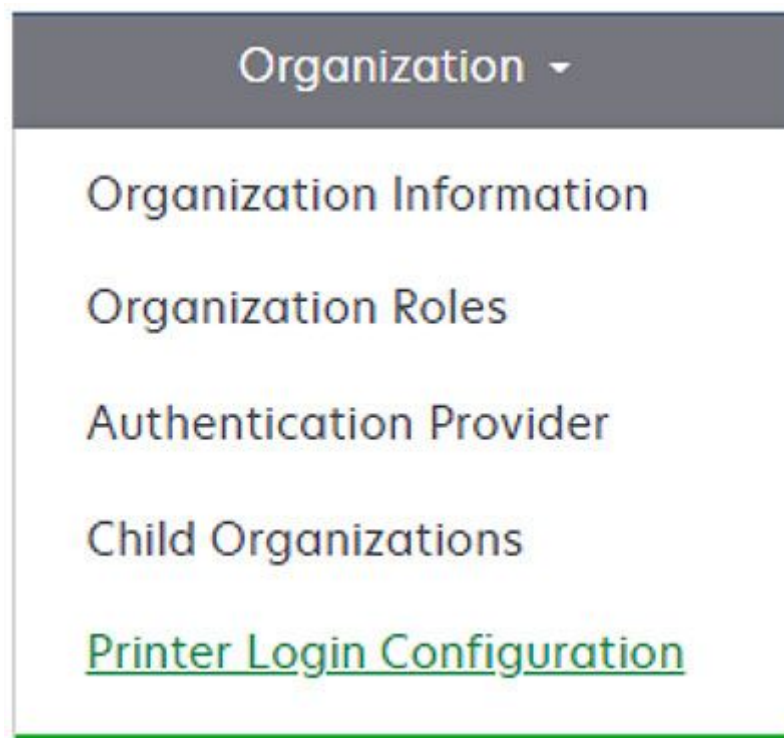
2. In the Printer Login Configuration page, select **Standard authentication > Manual/secure login**. For more information, see "Configuring printer login" topic in *Lexmark Cloud Services Administrator's Guide*.
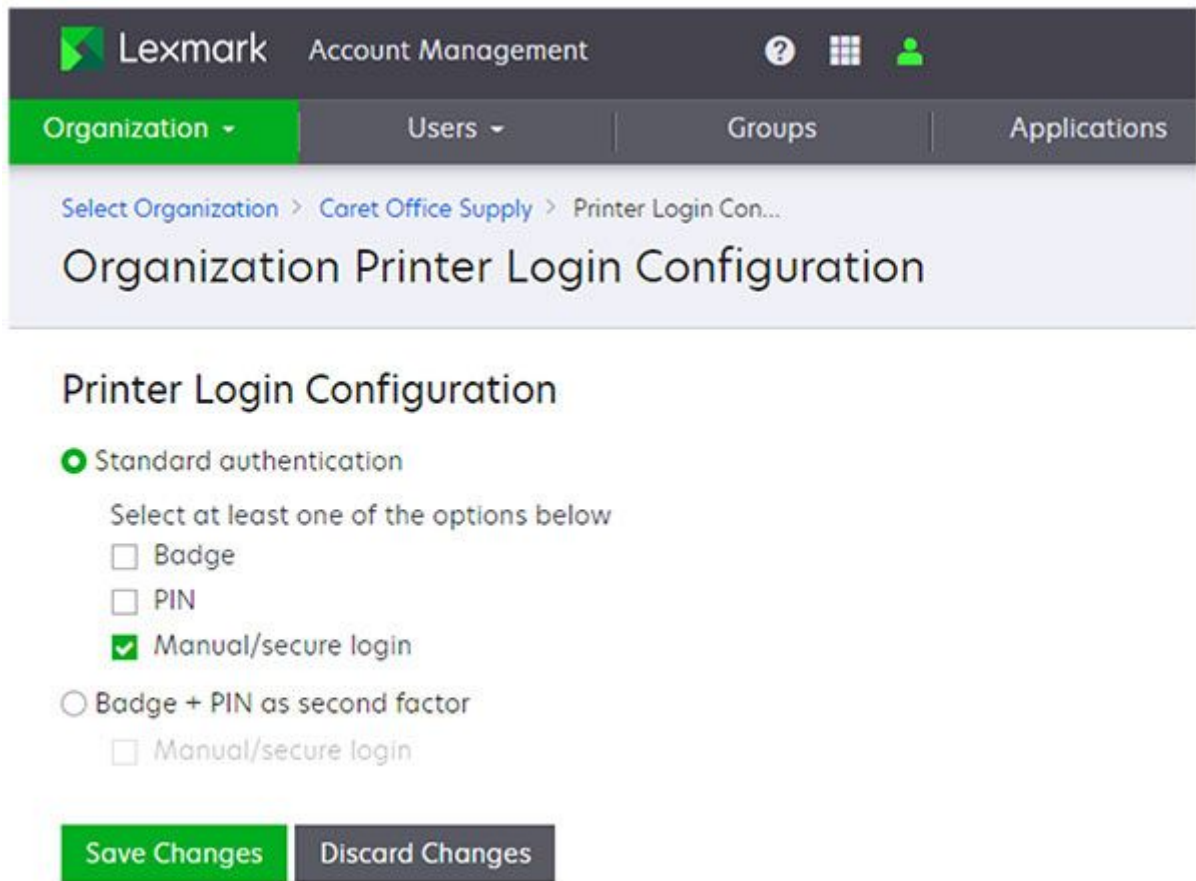
3. Click **Save Changes**.

Obtaining a secure login code

You can obtain a secure login code in the following ways:

- From the My Account page in the Lexmark Cloud Services portal
- From the Lexmark Print application on a mobile device.
- From the web address: https://us.iss.lexmark.com/device for North America, and https://eu.iss.lexmark.com/device for Europe.

User's Data Center	Value for *<env>*
European	eu
North American	us

From the My Account page

1. From the Lexmark Cloud Services portal, click your account name, and then click **My Account**.
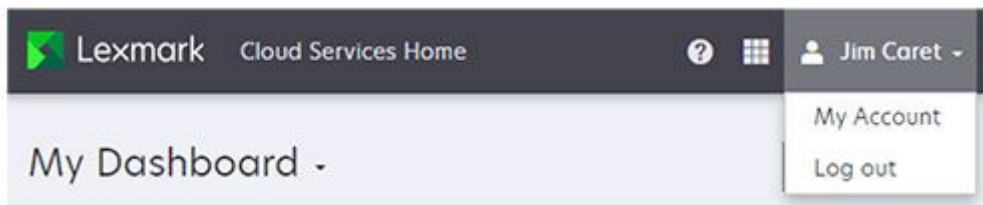
2. In the Printer Login section, click **Generate Login Code**.
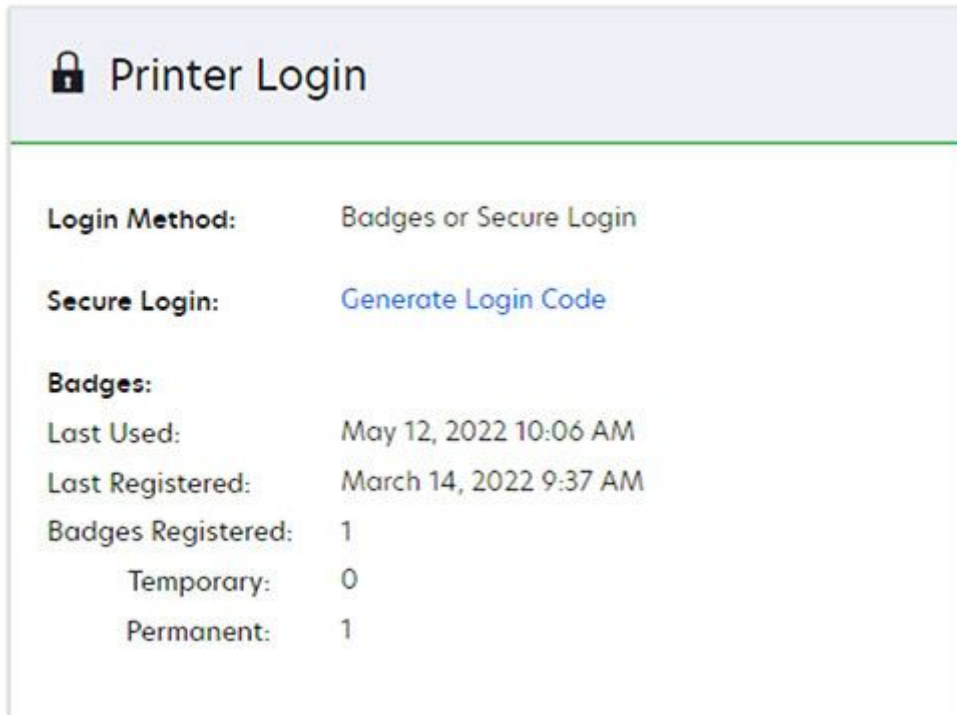
3. Use the secure login code shown to login to a cloud-enabled printer.
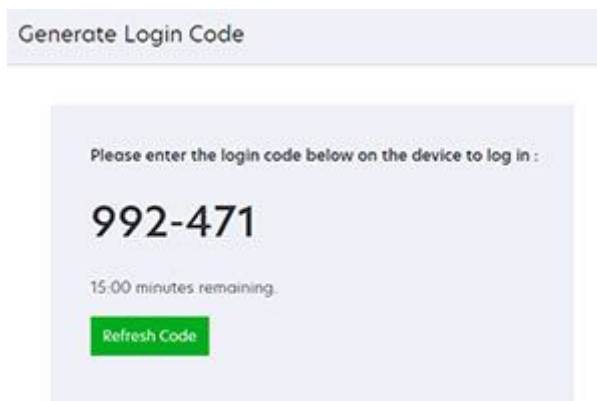
Note: A secure login code is only valid for 15 minutes. After 15 minutes, you can obtain a new code by clicking **Refresh Code**.

From the Lexmark Print application

1. Open the Lexmark Print application on a mobile device.
2. Log in to the Lexmark Cloud Services portal.
3. Touch the **Cloud** icon at the bottom of the screen.
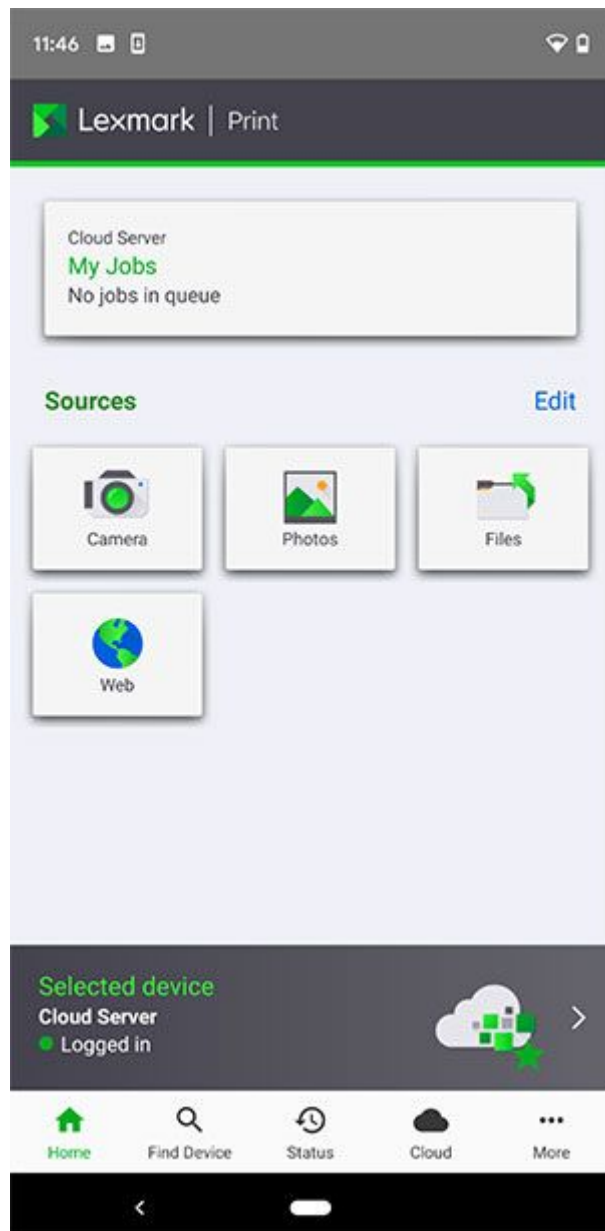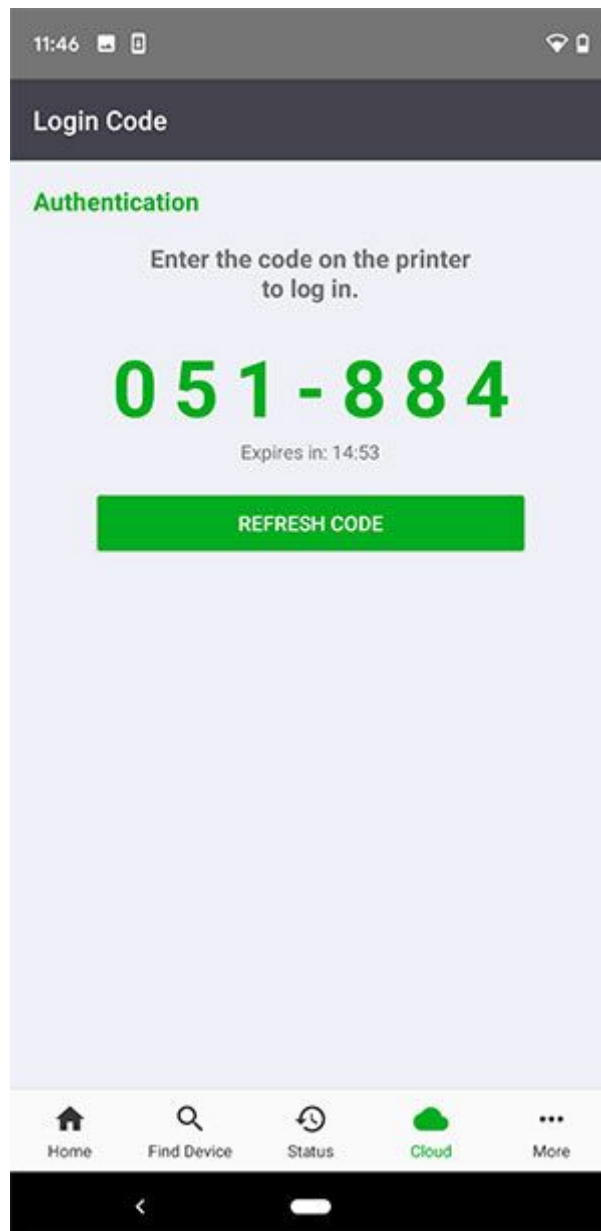
Notes

- A secure login code will be shown.
- A secure login code is only valid for 15 minutes. After 15 minutes, you can obtain a new code by clicking **Refresh Code**.

From the web address

1. Open a web browser.
2. Go to: https://*<env>*.iss.lexmark.com/device.

User's Data Center	Value for *<env>*
European	eu
North American	us

> **Note:** To determine the value of *<env>* , see the address on the browser address field when you log in to your Lexmark Cloud Services portal.

3. Use the secure login code shown to login to a cloud-enabled printer.

> **Note:** A secure login code is only valid for 15 minutes. After 15 minutes, you can obtain a new code by clicking **Refresh Code**.

Generate Login Code

Please enter the login code below on the device to log in :

992-471

15:00 minutes remaining.

Refresh Code

Using a secure login code

When secure login is enabled for an organization, the Secure Login icon will appear on the control panel.

1. From the printer home screen, touch **Secure Login**.

2. Touch the **Login Code** prompt.
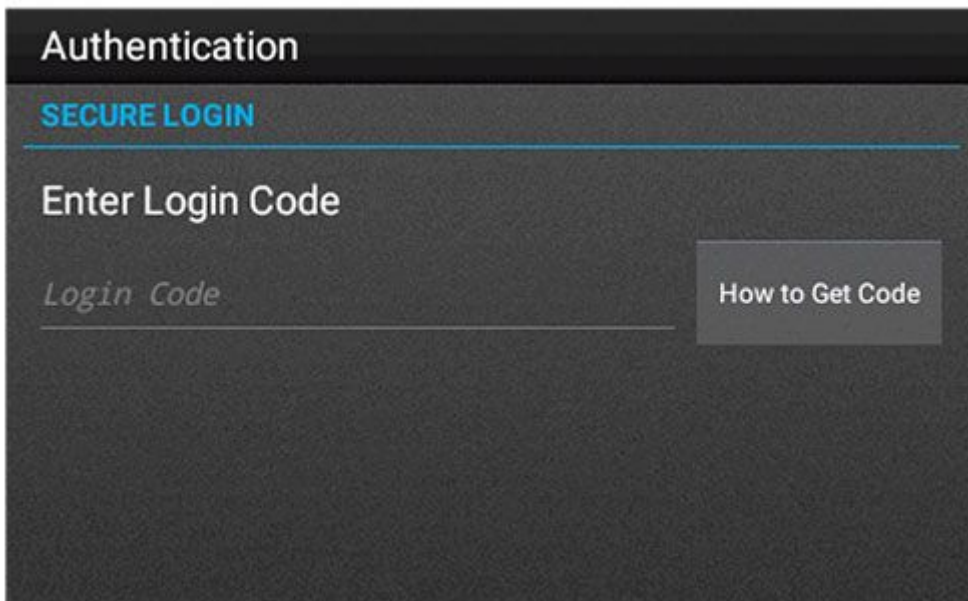
3. Enter the secure login code, and then touch **Log In**.
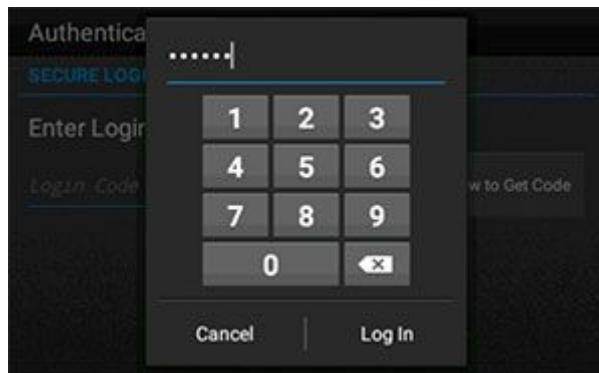
Note: For more information on obtaining secure login code, either touch **How to Get Code** on the control panel or see Obtaining a secure login code on page 161.
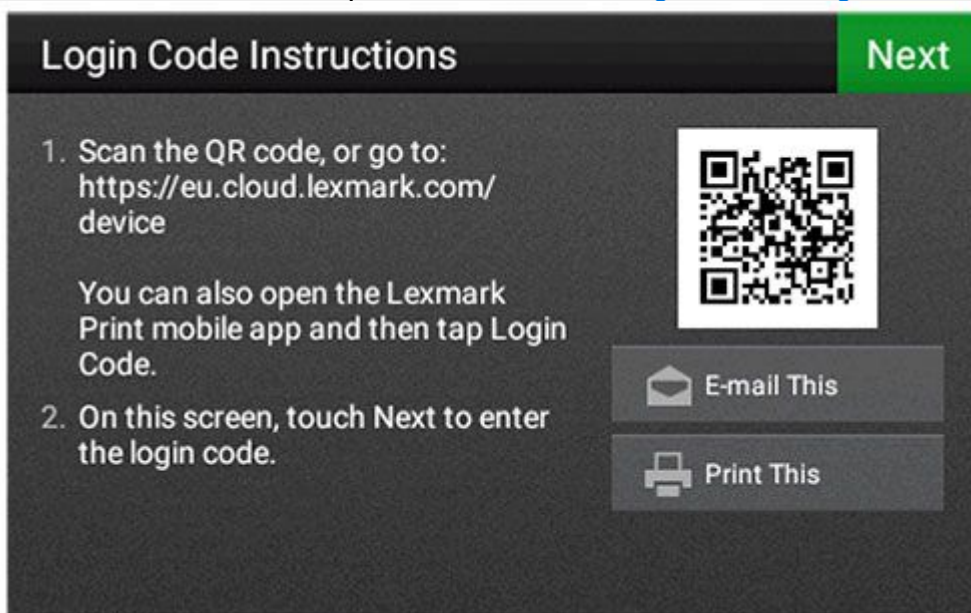
Using notification policies

Notification policies overview

Notification policies are a Fleet Management feature that lets the Fleet Management Administrator send email notifications when certain conditions occur. You can set the policies to send emails when toner is low or when a printer fails to communicate with Lexmark Cloud Services. Notification policies are available for:

- Supplies
- Printer Information

Supplies policies

Generates an email when the toner level threshold has been met or exceeded. Multiple supplies policies can be created with different threshold settings to provide notifications as supplies are depleted.

Supplies policies are available for:

- Toner
- Maintenance Kit
- Fuser
- Photoconductors
- Waste Toner Bottle
- Transfer Module

Printer Information policies

Generates an email when a printer fails to communicate or report its data to Lexmark Cloud Services after the interval threshold has been met or exceeded.

Printer Information policies are available for:

- Last data refreshed
- Last communicated

The following is an example of an email generated by a Notification Policy.

Creating a Notification Policy

Creating a supplies policy

Supplies policies notify users by email when the toner level of their printers reaches a specified percentage.

> **Note:** You can create up to 50 supplies policies for an organization.

1. From the Fleet Management web portal, click **Notifications > Notification Policies**.

2. Click the **Supplies** tab.

> **Note:** If there are existing supplies policies, then the Notification Policies page shows them.

3. On the Notification Policies page, click **Create**.
4. Configure the following:

- In the Policy name field, type the name of the policy.

  The following characters are not allowed in a Policy Name:

  - < >
  - &
  - #
  - ?
  - `
  - ~
  - !
  - %
  - ^

- *
- |
- +
- =
- ;
- ;
- "
- { }
- [ ]
- \ /

○ In the Policy type menu, select a supplies option.
○ In the "Notify when toner remaining is at" section, set the percentage at which the notification is sent.
○ In the Applies To section, select either of the following:

  ▪ **All printers in this organization**—Apply the policy to all printers in the organization.
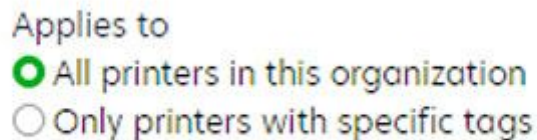
  ▪ **Only printers with specific tags**—Apply the policy to specific printers based on the tags entered. For more information on tags, see "Creating tags" topic and "Assigning tags to printers" topic in *Lexmark Cloud Services Administrator's Guide*.

    ▪ In the "Apply the policy to printers with the following tags" field, type the tags, and then click **Add**.

    Note: You can apply up to 10 tags to a policy.

○ In the "Notify the following e-mail addresses when the conditions of this policy are met" field, type the recipient email addresses, and then click **Add**.
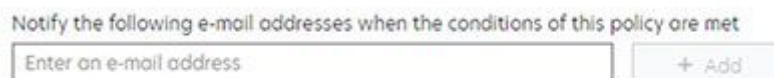
    Notes
      ▪ You can type up to 10 email addresses.
      ▪ Make sure that the email address is valid.
      ▪ You can type an email address from outside your organization.

◦ In the "Additional information to include in the e-mail notification (Optional)" field, type any information that you want to appear in the email body. For example, printer location or special access instructions.

Additional information to include in the e-mail notification (Optional)

◦ Select **Include notification data in a .json file as an attachment** to attach a JSON file of the data associated with the notification.

☑ Include notification data in a .json file as an attachment

The following is an example of an email notification.

7559040000075 [Caret Office Supply] : Toner Level Notification - Cyan
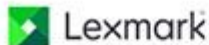
Lexmark

Toner Level Notification - Cyan

Lexmark Cloud Services

Notification details:
=======================

Asset tag:	
Location:	
Contact name:	
Additional information:	
Organization:	Caret Office Supply
Problem:	Toner Level
Notify at:	Toner below or equal to 55 %
Status description:	
Printer S/N:	7559040000075
Printer model:	CX922de
IP address:	10.184.81.250
Supply S/N:	LEX0001700303001300704900225
Supply type:	Cyan
Supply level:	44 %

The following is an example of notification data in JSON format.

```
{
    "assetTag": "",
    "location": "",
    "contactName": "",
    "additionalInfo": "",
    "policyType": "Toner Level",
    "notificationThreshold": 55,
    "statusDescription": "",
    "assetSerialNumber": "7559040000075",
    "assetModel": "CX922de",
    "assetIpAddress": "10.184.81.250",
    "supplySerialNumber": "LEX000170030300013007049002255",
    "color": "Cyan",
    "supplyLevel": 44,
    "supplyName": "Cyan Cartridge",
    "organization": "Caret Office Supply"
}
```

Creating a printer information policy

Printer information policies notify users by email when a printer fails to communicate with or report its data to Lexmark Cloud Services. Emails are sent after a specified time has elapsed.

> **Note:** You can create up to 50 policies.

1. From the Fleet Management web portal, click **Notifications > Notification Policies**.
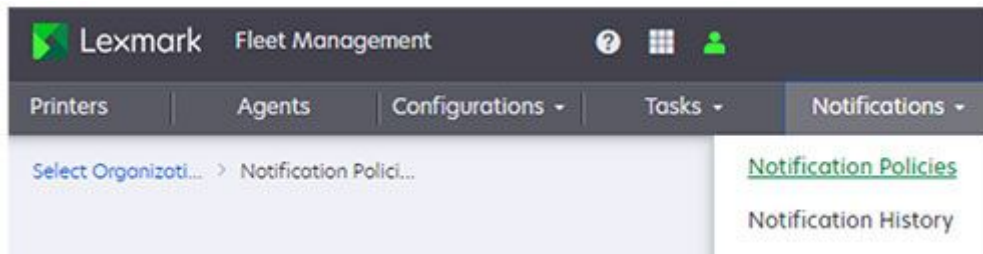
2. Click **Printer Information** tab.
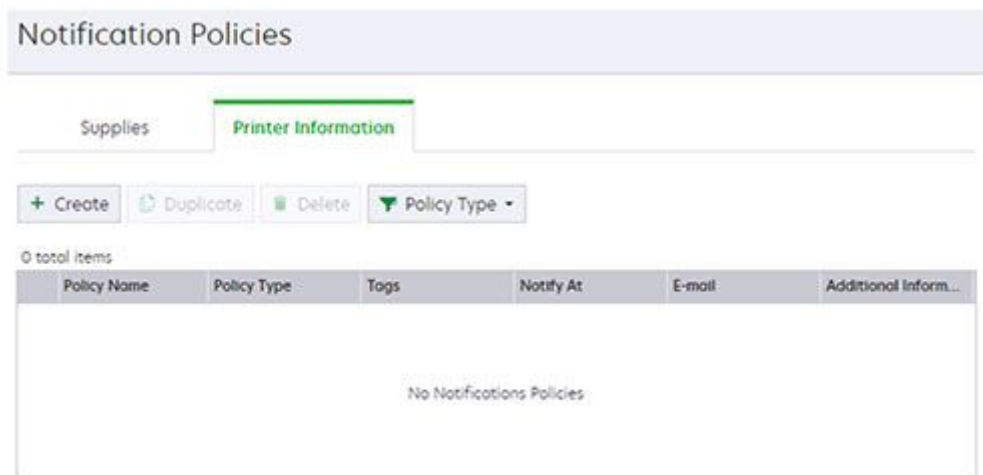
> **Note:** If there are existing printer information policies, then the Notification Policies
> page shows them.

3. On the Notification Policies page, click **Create**.
4. Configure the following:

Create Notification Policy

Policy name

Policy type

Applies to
- All printers in this organization
- Only printers with specific tags

Notify the following e-mail addresses when the conditions of this policy are met

Enter an e-mail address   + Add

Additional information to include in the e-mail notification (Optional)

☐ Include notification data in a .csv file as an attachment

Create Policy   Cancel

   ◦ In the Policy name field, type the name of the policy.

      The following characters are not allowed in a Policy Name:

      - < >
      - &
      - #
      - ?
      - `
      - ~
      - !
      - %
      - ^
      - *
      - |
      - +
      - =
      - ;
      - ;
      - "
      - { }
      - [ ]
      - \ /

- ◦ In the Policy type menu, select either of the following:

    - ▪ **Last data refresh**—Send an email notification based on the number of days since the last update of printer information or counters.

        - ▪ Set the "Notify when data has not been refreshed after" value to the number of days that must elapse before an email notification is sent.

            Notify when data has not been refreshed after

            | − | 3 | + | days

            1 - 7 days

    - ▪ **Last communicated**—Send an email notification based on the number of days since the printer last communicated with Lexmark Cloud Services.

        - ▪ Set the "Notify when a printer has not communicated for" value to the number of days that must elapse before an email notification is sent.

            Notify when a printer has not communicated for

            | − | 3 | + | days

            1 - 7 days

    e-mail
- ◦ In the Applies To section, select either of the following:

    - ▪ **All printers in this organization**—Apply the policy to all printers in the organization.

        Applies to
        ● All printers in this organization
        ○ Only printers with specific tags

    - ▪ **Only printers with specific tags**—Apply the policy to specific printers based upon the tags entered. For more information on tags, see "Creating tags" topic and "Assigning tags to printers" topic in *Lexmark Cloud Services Administrator's Guide*.

        Applies to
        ○ All printers in this organization
        ● Only printers with specific tags

        Apply the policy to printers with the following tags

        | Enter a tag | + Add |

        - ▪ In the "Apply the policy to printers with the following tags" field, type the tags, and then click **Add**.

> **Note:** You can apply up to 10 tags to a policy.

◦ In the "Notify the following e-mail addresses when the conditions of this policy are met" field, type the recipient email addresses, and then click **Add**.

Notify the following e-mail addresses when the conditions of this policy are met

Enter an e-mail address   + Add

Notes
- You can type a maximum of 10 email addresses.
- Make sure that the email address is valid.
- You can type an email address from outside your organization.

◦ In the "Additional information to include in the e-mail notification (Optional)" field, type any information that you want to appear in the email body. For example, printer location or special access instructions.

Additional information to include in the e-mail notification (Optional)

◦ Select **Include notification data in a .csv file as an attachment** to attach a CSV file of the data associated with the notification.

☑ Include notification data in a .csv file as an attachment

The following is an example of a notification email for last data refresh:

[Caret Office Supply] : Data Not Refreshed

The following is an example of a notification email for last communicated:

The following is an example of the notification data in CSV format:

Managing notification policies

Modifying a notification policy

You can modify notification policies at any time.

1. From the Fleet Management web portal, click **Notifications > Notification Policies**.
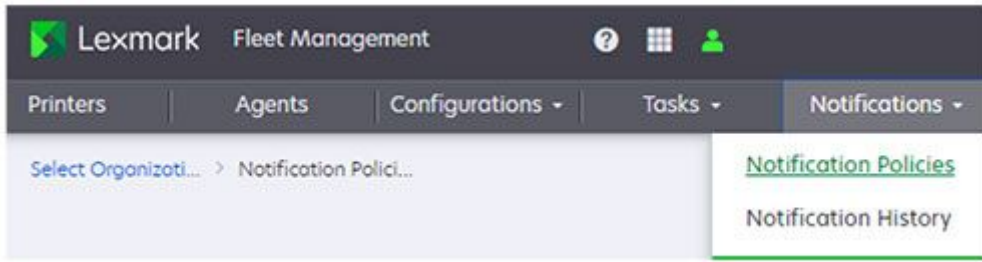
2. Select the **Supplies** or **Printer Information** tab.
3. Click the name of the policy that you want to modify.
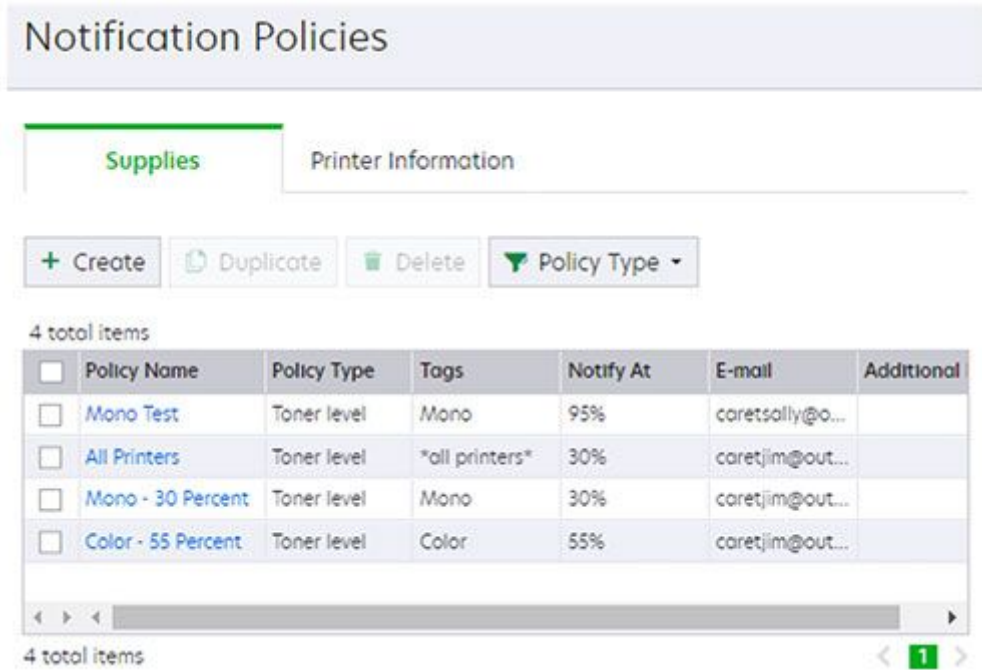
4. Modify the policy, and then click **Save Changes**.

Duplicating a notification policy

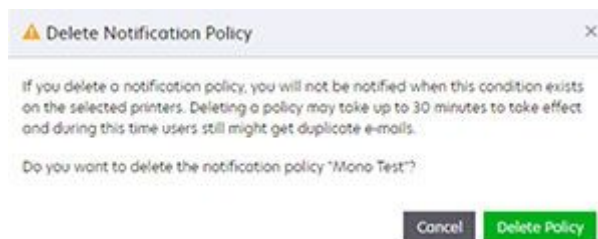You can duplicate notification policies to create additional policies.

1. From the Fleet Management web portal, click **Notifications > Notification Policies**.
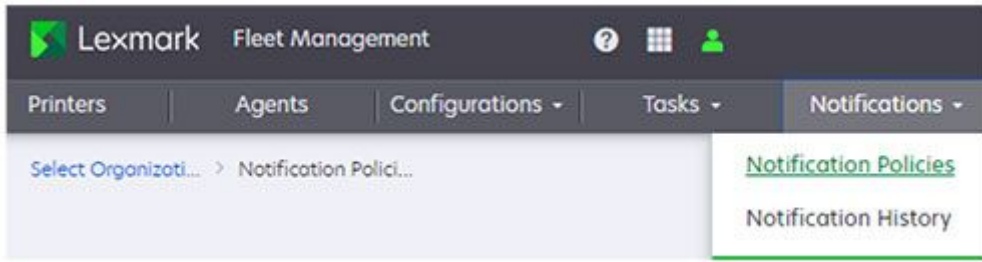
2. Select the **Supplies** or **Printer Information** tab.
3. Select an existing policy, and then click **Duplicate**.
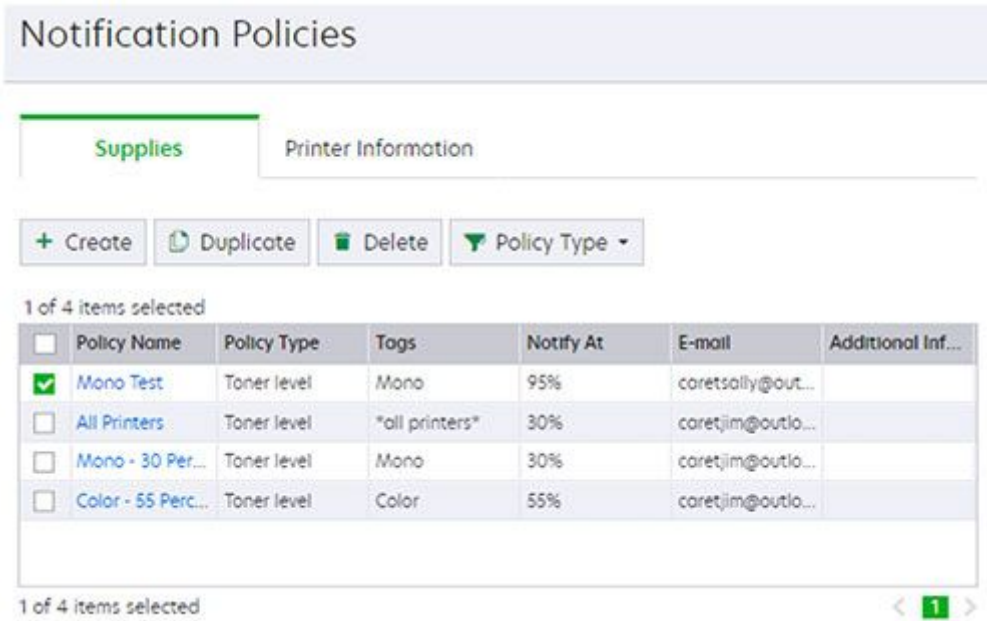
4. Type a new policy name, and then modify the details as required.

Select Organization:... > Notification Policies > Create Notification ...

Create Notification Policy

Policy name

Policy type

Toner level ▾

Notify when toner remaining is at

− 95 + %

Range: 0 to 100

Applies to
○ All printers in this organization
● Only printers with specific tags

Apply the policy to printers with the following tags

Mono ✕

Enter a tag | + Add

Notify the following e-mail addresses when the conditions of this policy are met

caretsally@outlook.com ✕

Enter an e-mail address | + Add

Additional information to include in the e-mail notification (Optional)

☐ Include notification data in a .json file as an attachment

NOTE: There can be up to a 30 minutes delay before the policy takes effect.

[Create Policy] [Cancel]

Notes
◦ When duplicating a policy, the Create Notification Policy page is prefilled with information from the policy that you are duplicating.
◦ Make sure that the new policy has a unique name.

5. Click **Create Policy**.

Deleting a notification policy

You can delete notification policies that are no longer needed.

1. From the Fleet Management web portal, click **Notifications > Notification Policies**.
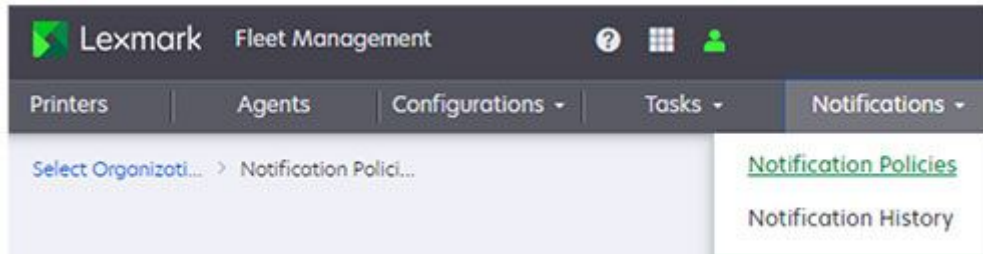
2. Select the **Supplies** or **Printer Information** tab.
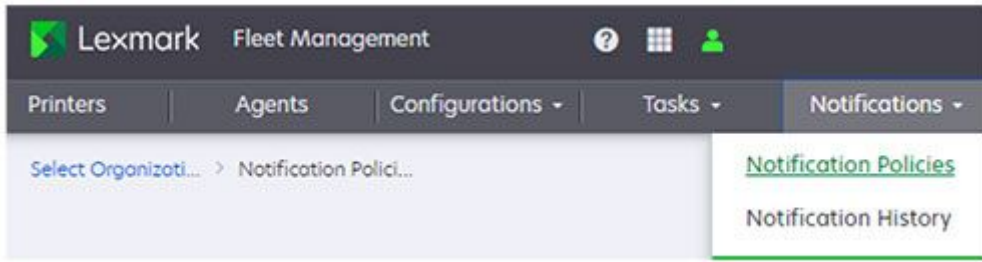3. Select one or more policies, and then click **Delete**.
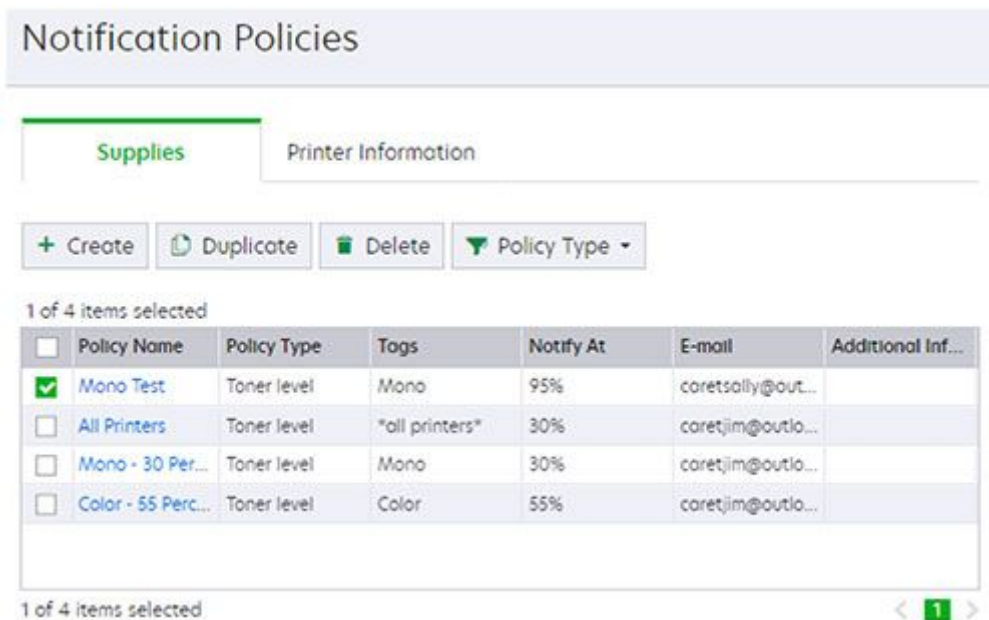
4. Click **Delete Policy**.

Viewing notification history

The Notification History menu option shows the notifications that were generated in the last 30 days.

1. From the Fleet Management web portal, click **Notifications > Notification History**.

2. Select the **Supplies** or **Printer Information** tab.

   You can view the following notifications generated in the last 30 days:

   ◦ Supplies notification

   ◦ Printer Information notification

Select Organization: Caret Office Supply > Notification History

Notification History (Last 30 Days)

Supplies	Printer Information

▼ Policy Type ▾   ▼ Model ▾   Search serial numbe... ✕   🔍

24 total items

Date	Policy Type	Printer Serial N...	Model	Asset Tag	E-mail	Notify At	Last Communic...	Last Data Refr...
2/19/2023, 8:00:12 PM	Last data refresh	74658250201HB	Lexmark MX822...		caretjim@outloo...	3 days	11/21/2022, 3:4...	11/21/2022, 3:4...
2/19/2023, 8:00:12 PM	Last data refresh	74634799062M1	Lexmark MX710		caretjim@outloo...	3 days	9/23/2022, 4:51...	9/23/2022, 4:51...
2/19/2023, 8:00:12 PM	Last data refresh	7464811020036	Lexmark MX722...		caretjim@outloo...	3 days	1/4/2022, 9:06:...	1/13/2022, 8:04:...
2/19/2023, 8:00:12 PM	Last data refresh	7529827140CDN	Lexmark CX625...		caretjim@outloo...	3 days	6/27/2022, 6:05...	6/27/2022, 6:05...
2/19/2023, 8:00:12 PM	Last communica...	7529827140CDN	Lexmark CX625...		caretjim@outloo...	3 days	6/27/2022, 6:05...	6/27/2022, 6:05...
2/19/2023, 8:00:12 PM	Last communica...	74658250201HB	Lexmark MX822...		caretjim@outloo...	3 days	11/21/2022, 3:4...	11/21/2022, 3:4...
2/19/2023, 8:00:12 PM	Last communica...	74634799062M1	Lexmark MX710		caretjim@outloo...	3 days	9/23/2022, 4:51...	9/23/2022, 4:51...
2/19/2023, 8:00:12 PM	Last communica...	7464811020036	Lexmark MX722...		caretjim@outloo...	3 days	1/4/2022, 9:06:...	1/13/2022, 8:04:...
2/18/2023, 8:00:07 PM	Last data refresh	74658250201HB	Lexmark MX822...		caretjim@outloo...	3 days	11/21/2022, 3:4...	11/21/2022, 3:4...
2/18/2023, 8:00:07 PM	Last data refresh	74634799062M1	Lexmark MX710		caretjim@outloo...	3 days	9/23/2022, 4:51...	9/23/2022, 4:51...
2/18/2023, 8:00:07 PM	Last communica...	7529827140CDN	Lexmark CX625...		caretjim@outloo...	3 days	6/27/2022, 6:05...	6/27/2022, 6:05...
2/18/2023, 8:00:07 PM	Last data refresh	7464811020036	Lexmark MX722...		caretjim@outloo...	3 days	1/4/2022, 9:06:...	1/13/2022, 8:04:...
2/18/2023, 8:00:07 PM	Last data refresh	7529827140CDN	Lexmark CX625...		caretjim@outloo...	3 days	6/27/2022, 6:05...	6/27/2022, 6:05...
2/18/2023, 8:00:07 PM	Last communica...	74658250201HB	Lexmark MX822...		caretjim@outloo...	3 days	11/21/2022, 3:4...	11/21/2022, 3:4...
2/18/2023, 8:00:07 PM	Last communica...	74634799062M1	Lexmark MX710		caretjim@outloo...	3 days	9/23/2022, 4:51...	9/23/2022, 4:51...
2/18/2023, 8:00:07 PM	Last communica...	7464811020036	Lexmark MX722...		caretjim@outloo...	3 days	1/4/2022, 9:06:...	1/13/2022, 8:04:...
2/17/2023, 8:00:07 PM	Last communica...	7529827140CDN	Lexmark CX625...		caretjim@outloo...	3 days	6/27/2022, 6:05...	6/27/2022, 6:05...
2/17/2023, 8:00:07 PM	Last data refresh	74658250201HB	Lexmark MX822...		caretjim@outloo...	3 days	11/21/2022, 3:4...	11/21/2022, 3:4...
2/17/2023, 8:00:07 PM	Last data refresh	74634799062M1	Lexmark MX710		caretjim@outloo...	3 days	9/23/2022, 4:51...	9/23/2022, 4:51...
2/17/2023, 8:00:07 PM	Last data refresh	7464811020036	Lexmark MX722...		caretjim@outloo...	3 days	1/4/2022, 9:06:...	1/13/2022, 8:04:...
2/17/2023, 8:00:07 PM	Last data refresh	7529827140CDN	Lexmark CX625...		caretjim@outloo...	3 days	6/27/2022, 6:05...	6/27/2022, 6:05...
2/17/2023, 8:00:07 PM	Last communica...	74658250201HB	Lexmark MX822...		caretjim@outloo...	3 days	11/21/2022, 3:4...	11/21/2022, 3:4...
2/17/2023, 8:00:07 PM	Last communica...	74634799062M1	Lexmark MX710		caretjim@outloo...	3 days	9/23/2022, 4:51...	9/23/2022, 4:51...
2/17/2023, 8:00:07 PM	Last communica...	7464811020036	Lexmark MX722...		caretjim@outloo...	3 days	1/4/2022, 9:06:...	1/13/2022, 8:04:...

24 total items   < **1** >

Index

Rollout Guide