

Version 1.0
November 2021
702P08730

Xerox® AltaLink® Series Identity Provider Configuration Guide

© 2021 Xerox Corporation. All rights reserved. Unpublished rights reserved under the copyright laws of the United States. Contents of this publication may not be reproduced in any form without permission of Xerox Corporation.

Copyright protection claimed includes all forms of matters of copyrightable materials and information now allowed by statutory or judicial law or hereinafter granted, including without limitation, material generated from the software programs which are displayed on the screen such as styles, templates, icons, screen displays, looks, and so on.

Xerox®, Xerox and Design®, AltaLink®, CentreWare®, Xerox Secure Access Unified ID System®, Xerox Extensible Interface Platform®, and ConnectKey® are trademarks of Xerox Corporation in the United States and/or other countries.

Adobe®, Adobe® PDF and Adobe PDF logo, Acrobat Reader®, Flash®, Macromedia®, Photoshop®, and PostScript® are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

Gmail™ email service, Google Chrome™ browser, Google Cloud Print™ Web printing service, Google Docs™ Web-based word-processing program, Google Drive™ online storage service, and Android™ mobile technology platform are trademarks of Google, Inc.

Microsoft®, Azure®, Office 365®, OneDrive®, Windows®, Windows Server®, and Windows Vista® are trademarks of Microsoft Corporation in the United States and other countries.

Okta is a trademark of Okta, Inc. in the United States.

Ping Identity, PingAccess, PingFederate, PingID, and PingOne are registered trademarks of Ping Identity Corporation ("Ping Identity").

All other trademarks or registered trademarks are the property of their respective owners.

Table of Contents

1 Okta	5
Overview of Configuration Procedure	6
Gather Prerequisite Information.....	7
Enable IdP Authentication and Download the Device Metadata File	8
Configure the Okta App and Download the IdP SAML Metadata File.....	9
Upload the SAML Metadata File and Connect to the IdP	11
2 Ping Identity	13
Overview of Configuration Procedure	14
Gather Prerequisite Information.....	15
Enable IdP Authentication and Download the Device Metadata File	16
Configure Ping Identity and Download the IdP SAML Metadata File.....	17
Upload the SAML Metadata File and Connect to the IdP	19
3 Microsoft Azure	21
Overview of Configuration Procedure	22
Gather Prerequisite Information.....	23
Enable IdP Authentication and Download the Device Metadata File	24
Configure Microsoft Azure and Download the IdP SAML Metadata File.....	25
Upload the SAML Metadata File and Connect to the IdP	27
4 Cloning Options	29
Overview of the Cloning Options	30
Clone Files	31
Fleet Orchestrator	32
Xerox® CentreWare Web	33
Xerox® Device Manager	34

Table of Contents

4	Xerox® AltaLink® Series Identity Provider Configuration Guide
---	--

Okta

This chapter contains:

- Overview of Configuration Procedure 6
- Gather Prerequisite Information..... 7
- Enable IdP Authentication and Download the Device Metadata File 8
- Configure the Okta App and Download the IdP SAML Metadata File..... 9
- Upload the SAML Metadata File and Connect to the IdP..... 11

Overview of Configuration Procedure

When cloud-based authentication through an identity provider (IdP) is configured, the device establishes a secure connection with the IdP, then passes the user credentials to the IdP for authentication. This method of authentication does not require any local server-based components or extra applications on the local network.

To configure cloud-based authentication through a third-party IdP, the administrator establishes a trust relationship between the Xerox® device and an IdP endpoint. When the trust relationship is established, the device passes user credentials to the IdP for authentication.

For an authenticated user, the IdP manages access to authorized applications and workflows on the Xerox® device.



Note: If your organization uses a proxy server, communications between the Xerox® device and the IdP endpoint include proxy server authentication.

To configure your Xerox® device to use an IdP authentication method, the following steps are required:

1. Gather the information required for the configuration process, for example, the device administrator credentials and the IdP developer administrator credentials.
2. On the Xerox® device, enable the authentication method for **Identity Provider (IdP) - Validate on Cloud**, then download the device metadata file.
3. Using the IdP, configure the IdP settings, then download the IdP SAML metadata file.
4. On the Xerox® device, upload the SAML metadata file, then connect to the IdP.

To configure more than one Xerox® device for IdP authentication, use the cloning options. For information, refer to [Cloning Options](#).

Gather Prerequisite Information

Before you begin, ensure that you have the following information or items available:

- Xerox multifunction printer:
 - The IP address of the printer: The Embedded Web Server is the administration and configuration software installed on the printer. This software allows you to configure and administer the printer from a Web browser. The IP address of the printer is needed to access the Embedded Web Server for the multifunction printer.
 - Administrator login credentials for the printer: These credentials are needed to access the **Properties** settings in the Embedded Web Server.
- Identity provider (IdP):
 - To ensure that you are able to complete the IdP configuration steps, familiarize yourself with the SAML configuration method.
 - To configure the SAML request, you require administrator credentials for the IdP portal.
 - For the new SAML app that you create, create or choose a .png image that is less than 1 MB.

Enable IdP Authentication and Download the Device Metadata File

To configure IdP as the authentication method on the printer, the administrator uses the Embedded Web Server and downloads a device metadata file from the Xerox® device. The file contains the device settings required to set up the trust relationship between the Xerox® device and an IdP endpoint. The file includes the Xerox root certificate.

To enable IdP authentication and download the Xerox® device metadata file, do the following:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.
4. For Control Panel Login, select **Identity Provider (IdP) - Validate on Cloud**.
5. Click **Save**.
6. From the Login Methods window, for Identity Provider (IdP) Connection, click **Edit**.
7. In the Configuration area, for Device Metadata File, click **Download**. A file named `Xerox_mfp_saml_metadata.xml` downloads.



Note: The Xerox® device metadata file is not specific to an individual device. This file is valid for other Xerox® devices.

For the next stage in the configuration procedure, you will use the downloaded metadata file to configure the SAML app settings.

Configure the Okta App and Download the IdP SAML Metadata File

To configure the identity provider, the administrator creates a SAML app and defines the SAML app settings. After defining the SAML settings, the administrator creates a metadata XML file from the IdP. The IdP metadata file is used to configure the authentication settings on the Xerox® device.

To create and configure the SAML app, then create the IdP metadata file, do the following:

1. Log in to Okta with your developer administrator credentials, then navigate to `okta.com/dev/console`.
2. Click **Dashboard**.
3. Click **Applications**, then click **Create App Integration**.
A selection for Integrate for Single Sign-on appears.
4. For Sign on method, click **SAML 2.0**, then click **Create**.
5. In the General Settings section, configure the settings as follows:
 - a. For App Name type an app name. For example `Xerox MFP Authentication`.
 - b. If required, add a logo to represent the new app. To upload an image file, for App Logo, click **Browse**, then browse to and select the image file required. Click **Upload Logo**. The new logo is shown.
 - c. If required, configure the app Visibility settings.
6. Click **Next**.
7. In the Configure SAML section, configure the settings as follows:
 - a. **Single Sign on URL**: This field identifies the location that the IdP provider uses to log in to the Xerox printer. The pathway is shown in the Xerox MFP metadata XML file named `Xerox_mfp_saml_metadata.xml`. In the field, type `http://localhost/DeviceSingleSignOnSP/service/index.php?acs`, then select the **Use this for Recipient URL and Destination URL** check box.
 - b. **Audience URI (SP Entry ID)**: This pathway is shown in the Xerox MFP metadata XML file named `Xerox_mfp_saml_metadata.xml`. In the field, type `urn:xerox:sp`.
 - c. **Application username**: This field defines the user name to use. To use your email address as the user name, from the menu, select **Email**.
8. To edit Advanced Settings, click **Show Advanced Settings**, then configure the settings as follows:
 - a. Response Signature: **Signed**.
 - b. Assertion Signature: **Signed**.
 - c. Signature Algorithm: **RSA-SHA256**.
 - d. Digest Algorithm: **SHA256**.
 - e. Assertion Encryption: **Encrypted**.
 - f. Enable Single Logout: **Enabled**.

- g. **Single Logout URL:** Type `http://localhost/DeviceSingleSignOnSP/service/index.php?sls`.
- h. **SP Issuer:** Type `urn:xerox:sp`.
- i. **Signature Certificate:** In the `Xerox_mfp_saml_metadata.xml` file, from the **KeyDescriptor use=signing** section, extract the value from the X509 certificate field, then save the value in a file named `signed_sp.crt`. Browse to the Xerox® device metadata file named `Xerox_mfp_saml_metadata.xml`, find your **Service Provider** certificate file named `sp.crt`, then click **Upload Certificate**. The message `upload is done` appears.
- j. **Authentication context class:** **PasswordProtectedTransport**.
- k. **Honor Force Authentication:** **Yes**.
- l. **SAML Issuer ID:** Type `http://www.okta.com/(org.externalKey)`.
- m. **Attribute Statements:** Create two attribute statements. For the first attribute statement, for **Attribute**, type `email`, then for **Value**, type `user.email`. For the second attribute statement, for **Attribute**, type `displayname`, then for **Value**, type `user.firstname`.



Note: For each attribute statement, you do not need to add a value in the **Name Format** field.

9. Click **Next**.
The SAML app is configured.
10. If required, assign people and groups to the SAML app. To add people and groups, select **Applications**, then select the new SAML app. Click **Assignments**, then assign people and groups as required. If the existing people and groups are sufficient, continue to the next step.
11. To create and download the IdP SAML metadata XML file:
 - a. In the SAML app, click the **Sign On** tab.
 - b. For Identity Provider metadata, select the metadata link.
 - c. Highlight the entire body of text in the file, then browse to the save location. Type the file name `IDP_metadata_forXerox.xml`, then save the file.
12. Log out, then exit Okta.

Upload the SAML Metadata File and Connect to the IdP


To create a connection between the Xerox® device and a new IdP endpoint, establish a trust relationship between the two endpoints.

To create a first-time connection, do the following:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. From the Login Methods window, for Identity Provider (IdP) Connection, click **Edit**.
3. In the Configuration area, for Validate IdP Server File, click **Browse**. Browse to the IdP metadata file downloaded from the IdP endpoint. For example, `IDP_metadata_forXerox.xml`.
4. Select the file, click **Open**, then click **Validate**. A message shows `Connecting to Identity Provider`.
5. If validation is successful, the message `Successfully validated Identity Provider file` appears. Click **Close**.

The Identity Provider (IdP) Connection area shows the status `Identity Provider (IdP) Configured`.

6. If validation fails, an error message appears. The error message indicates that the problem is either a connection issue, or that the IdP metadata file is not valid. Correct the issue, then repeat the procedure.
7. To test the connection between the Xerox® device and the IdP endpoint, click **Test Connection**. A message shows `Connecting to Identity Provider`. Do one of the following:
 - To abandon the test, click **Cancel**.
 - If the connection is successful, the message `Successfully connected to Identity Provider` appears. Click **Close**.
 - If the connection fails, the message `Could not connect to Identity Provider` appears. Click **Close**.

 **Note:** The connection test obtains the IdP endpoint URL from the IdP metadata file. Run this test only when the IdP metadata file is downloaded.

After you verify the connection, you can clone the IdP settings for use on other Xerox® devices. The clone file includes the device metadata file, the IdP metadata file, and the IdP configuration settings. When a device is configured from cloned IdP settings, a secure connection to the IdP endpoint is established.

For information, refer to [Cloning Options](#).

Okta

Ping Identity

This chapter contains:

- Overview of Configuration Procedure 14
- Gather Prerequisite Information..... 15
- Enable IdP Authentication and Download the Device Metadata File 16
- Configure Ping Identity and Download the IdP SAML Metadata File 17
- Upload the SAML Metadata File and Connect to the IdP..... 19

Overview of Configuration Procedure

When cloud-based authentication through an identity provider (IdP) is configured, the device establishes a secure connection with the IdP, then passes the user credentials to the IdP for authentication. This method of authentication does not require any local server-based components or extra applications on the local network.

To configure cloud-based authentication through a third-party IdP, the administrator establishes a trust relationship between the Xerox® device and an IdP endpoint. When the trust relationship is established, the device passes user credentials to the IdP for authentication.

For an authenticated user, the IdP manages access to authorized applications and workflows on the Xerox® device.



Note: If your organization uses a proxy server, communications between the Xerox® device and the IdP endpoint include proxy server authentication.

To configure your Xerox® device to use an IdP authentication method, the following steps are required:

1. Gather the information required for the configuration process, for example, the device administrator credentials and the IdP developer administrator credentials.
2. On the Xerox® device, enable the authentication method for **Identity Provider (IdP) - Validate on Cloud**, then download the device metadata file.
3. Using the IdP, configure the IdP settings, then download the IdP SAML metadata file.
4. On the Xerox® device, upload the SAML metadata file, then connect to the IdP.

To configure more than one Xerox® device for IdP authentication, use the cloning options. For information, refer to [Cloning Options](#).

Gather Prerequisite Information

Before you begin, ensure that you have the following information or items available:


- Xerox multifunction printer:
 - The IP address of the printer: The Embedded Web Server is the administration and configuration software installed on the printer. This software allows you to configure and administer the printer from a Web browser. The IP address of the printer is needed to access the Embedded Web Server for the multifunction printer.
 - Administrator login credentials for the printer: These credentials are needed to access the **Properties** settings in the Embedded Web Server.
- Identity provider (IdP):
 - To ensure that you are able to complete the IdP configuration steps, familiarize yourself with the SAML configuration method.
 - To configure the SAML request, you require administrator credentials for the IdP portal.
 - For the new SAML app that you create, create or choose a .png image that is less than 1 MB.

Enable IdP Authentication and Download the Device Metadata File

To configure IdP as the authentication method on the printer, the administrator uses the Embedded Web Server and downloads a device metadata file from the Xerox® device. The file contains the device settings required to set up the trust relationship between the Xerox® device and an IdP endpoint. The file includes the Xerox root certificate.

To enable IdP authentication and download the Xerox® device metadata file, do the following:


1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.
4. For Control Panel Login, select **Identity Provider (IdP) - Validate on Cloud**.
5. Click **Save**.
6. From the Login Methods window, for Identity Provider (IdP) Connection, click **Edit**.
7. In the Configuration area, for Device Metadata File, click **Download**. A file named `Xerox_mfp_saml_metadata.xml` downloads.

 **Note:** The Xerox® device metadata file is not specific to an individual device. This file is valid for other Xerox® devices.

For the next stage in the configuration procedure, you will use the downloaded metadata file to configure the SAML app settings.

Configure Ping Identity and Download the IdP SAML Metadata File

To configure the identity provider, the administrator creates a SAML app and defines the SAML app settings. After defining the SAML settings, the administrator creates a metadata XML file from the IdP. The IdP metadata file is used to configure the authentication settings on the Xerox® device.

 **Note:** This procedure applies to PingOne for Enterprise only. PingFederate is an on-premises solution and not a cloud-based solution.

To create and configure the SAML app, then create the IdP metadata file, do the following:

1. Log in to Ping Identity with your developer administrator credentials, then navigate to `admin.pingone.com/web-portal/dashboard`.
2. Click the **Applications** tab.
The My Applications screen appears.
3. Click **Add Application**, then click **New SAML Application**.
The options for setting up the new SAML application appear.
4. For Application Name, type an app name, for example `Xerox MFP Authentication`.
5. For Application Description, type a description of the app, for example `Xerox MFP SAML Application`.
6. For Category, from the list, choose an appropriate option.
7. For Graphics, if required, add an application icon to represent the new app. To upload an image file, click **Change**, then browse to and select the .png image file required.
8. Click **Continue to Next Step**.
The Application Configuration screen appears.
9. For Protocol Version, click **SAML v 2.0**.
10. To configure the SAML settings with the metadata downloaded from your Xerox® device, for Upload Metadata, click **Select File**. Browse to and select the metadata file named `Xerox_mfp_saml_metadata.xml` that you downloaded previously.
After the file uploads, the fields are populated with data from the Xerox® device metadata file.
11. For Encrypt Assertion, click the check box.
12. For Encryption Algorithm, from the menu, select **AES_256**.
13. For Signing, click **Sign Assertion**.
14. Click **Continue to Next Step**.
The SSO Attribute Mapping screen appears.

15. For SSO Attribute Mapping, create displayname and email attributes.
 - To create a displayname attribute, do the following:
 1. Click **Add new attribute**.
 2. In the Application Attribute column, type `displayname`.
 3. In the Identity Bridge Attribute or Literal Value column, select the attribute that you want to map to, for example **First Name**.
 4. Click the check box for **required**.
 - To create an email attribute, do the following:
 1. Click **Add new attribute**.
 2. In the Application Attribute column field, type `email`.
 3. In the Identity Bridge Attribute or Literal Value column field, select the attribute that you want to map to, for example **Email (Work)**.
 4. Click the check box for **required**.
16. Click **Continue to Next Step**.

The Group Access screen appears.
17. If required, configure additional users and groups for the SAML app. If the existing users and groups are sufficient, continue to the next step.
18. Click **Continue to Next Step**. Review the settings, then click **Finish**.

The SAML app is configured.
19. To create and download the IdP SAML metadata XML file:
 - a. Click the **Applications** tab, then from the My Applications screen, click **SAML**.
 - b. From the applications list, select the newly created SAML app.
 - c. For SAML Metadata, click **Download**.
 - d. Navigate to an appropriate save location, type the file name `IDP_metadata_forXerox.xml`, then save the file.
20. Log out, then exit Ping Identity.

Upload the SAML Metadata File and Connect to the IdP


To create a connection between the Xerox® device and a new IdP endpoint, establish a trust relationship between the two endpoints.

To create a first-time connection, do the following:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. From the Login Methods window, for Identity Provider (IdP) Connection, click **Edit**.
3. In the Configuration area, for Validate IdP Server File, click **Browse**. Browse to the IdP metadata file downloaded from the IdP endpoint. For example, `IDP_metadata_forXerox.xml`.
4. Select the file, click **Open**, then click **Validate**. A message shows `Connecting to Identity Provider`.
5. If validation is successful, the message `Successfully validated Identity Provider file` appears. Click **Close**.

The Identity Provider (IdP) Connection area shows the status `Identity Provider (IdP) Configured`.

6. If validation fails, an error message appears. The error message indicates that the problem is either a connection issue, or that the IdP metadata file is not valid. Correct the issue, then repeat the procedure.
7. To test the connection between the Xerox® device and the IdP endpoint, click **Test Connection**. A message shows `Connecting to Identity Provider`. Do one of the following:
 - To abandon the test, click **Cancel**.
 - If the connection is successful, the message `Successfully connected to Identity Provider` appears. Click **Close**.
 - If the connection fails, the message `Could not connect to Identity Provider` appears. Click **Close**.

 **Note:** The connection test obtains the IdP endpoint URL from the IdP metadata file. Run this test only when the IdP metadata file is downloaded.

After you verify the connection, you can clone the IdP settings for use on other Xerox® devices. The clone file includes the device metadata file, the IdP metadata file, and the IdP configuration settings. When a device is configured from cloned IdP settings, a secure connection to the IdP endpoint is established.

For information, refer to [Cloning Options](#).

Ping Identity

Microsoft Azure

This chapter contains:

- Overview of Configuration Procedure 22
- Gather Prerequisite Information..... 23
- Enable IdP Authentication and Download the Device Metadata File 24
- Configure Microsoft Azure and Download the IdP SAML Metadata File..... 25
- Upload the SAML Metadata File and Connect to the IdP..... 27

Overview of Configuration Procedure

When cloud-based authentication through an identity provider (IdP) is configured, the device establishes a secure connection with the IdP, then passes the user credentials to the IdP for authentication. This method of authentication does not require any local server-based components or extra applications on the local network.

To configure cloud-based authentication through a third-party IdP, the administrator establishes a trust relationship between the Xerox® device and an IdP endpoint. When the trust relationship is established, the device passes user credentials to the IdP for authentication.

For an authenticated user, the IdP manages access to authorized applications and workflows on the Xerox® device.



Note: If your organization uses a proxy server, communications between the Xerox® device and the IdP endpoint include proxy server authentication.

To configure your Xerox® device to use an IdP authentication method, the following steps are required:

1. Gather the information required for the configuration process, for example, the device administrator credentials and the IdP developer administrator credentials.
2. On the Xerox® device, enable the authentication method for **Identity Provider (IdP) - Validate on Cloud**, then download the device metadata file.
3. Using the IdP, configure the IdP settings, then download the IdP SAML metadata file.
4. On the Xerox® device, upload the SAML metadata file, then connect to the IdP.

To configure more than one Xerox® device for IdP authentication, use the cloning options. For information, refer to [Cloning Options](#).

Gather Prerequisite Information

Before you begin, ensure that you have the following information or items available:


- Xerox multifunction printer:
 - The IP address of the printer: The Embedded Web Server is the administration and configuration software installed on the printer. This software allows you to configure and administer the printer from a Web browser. The IP address of the printer is needed to access the Embedded Web Server for the multifunction printer.
 - Administrator login credentials for the printer: These credentials are needed to access the **Properties** settings in the Embedded Web Server.
- Identity provider (IdP):
 - To ensure that you are able to complete the IdP configuration steps, familiarize yourself with the SAML configuration method.
 - To configure the SAML request, you require administrator credentials for the IdP portal.
 - For the new SAML app that you create, create or choose a .png image that is less than 1 MB.

Enable IdP Authentication and Download the Device Metadata File

To configure IdP as the authentication method on the printer, the administrator uses the Embedded Web Server and downloads a device metadata file from the Xerox® device. The file contains the device settings required to set up the trust relationship between the Xerox® device and an IdP endpoint. The file includes the Xerox root certificate.

To enable IdP authentication and download the Xerox® device metadata file, do the following:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. Click **Login Methods**.
3. For Control Panel & Website Login Methods, click **Edit**.
4. For Control Panel Login, select **Identity Provider (IdP) - Validate on Cloud**.
5. Click **Save**.
6. From the Login Methods window, for Identity Provider (IdP) Connection, click **Edit**.
7. In the Configuration area, for Device Metadata File, click **Download**. A file named `Xerox_mfp_saml_metadata.xml` downloads.

 **Note:** The Xerox® device metadata file is not specific to an individual device. This file is valid for other Xerox® devices.

For the next stage in the configuration procedure, you will use the downloaded metadata file to configure the SAML app settings.

Configure Microsoft Azure and Download the IdP SAML Metadata File

To configure the identity provider, the administrator creates a SAML app and defines the SAML app settings. After defining the SAML settings, the administrator creates a metadata XML file from the IdP. The IdP metadata file is used to configure the authentication settings on the Xerox® device.

To create and configure the SAML app, then create the IdP metadata file, do the following:

1. Log in to Microsoft Azure with your developer administrator credentials, then navigate to `Enterprise applications`.

2. Click **New application**, then click **Create your own application**.

The Create your own application window appears.

3. To create the SAML app, do the following:

- a. For `What's the name of your app?`, type an app name, for example `Xerox MFP Authentication`.
- b. For `What are you looking to do with your application?`, click **Integrate any other application you don't find in the gallery (Non-gallery)**.
- c. Click **Create**.

The new app appears in the list.

4. To configure the SAML app settings, in the left pane, under **Manage**, click **Single-sign on**. Configure the settings as follows:

- To configure the Basic SAML Configuration settings with the metadata downloaded from your Xerox® device, do the following:
 1. Click **Upload Metadata file**.
 2. Browse to and select the metadata file named `xerox_mfp_saml_metadata.xml` that you downloaded previously.
 3. Click **Add**.

The Basic SAML settings are populated with data from the Xerox® metadata file.

- To create an email attribute and a displayname attribute, do the following:
 1. For `User Attributes & Claims`, click **Edit**.
 2. To create an email attribute, click **Add New Claim**. For `Name`, type `email`, then for `Source attribute`, select **user.email**.
 3. To create a displayname attribute, click **Add New Claim**. For `Name`, type `displayname`, then for `Source attribute`, select **user.displayname**.
 4. Click **Save**.

5. If additional users and groups are required, in the left pane, under **Manage**, click **Users and groups**, then configure the users and groups required. If the existing users and groups are sufficient, continue to the next step.

6. To configure user settings, in the left pane, click **Properties**, then do the following:

Microsoft Azure

- a. For Enabled for users to sign-in?, click **Yes**.
- b. For User assignment required?, click **Yes**.
- c. For Visible to users?, click **Yes**.

The SAML app is configured.

7. To create and download the IdP SAML metadata XML file:
 - a. In the left pane, under **Manage**, click **Single-sign on**.
 - b. In the SAML Signing Certificate section, for Federation Metadata XML, click **Download**.
 - c. Navigate to an appropriate save location, type the file name `IDP_metadata_forXerox.xml`, then save the file.
8. Log out, then exit Microsoft Azure.

Upload the SAML Metadata File and Connect to the IdP


To create a connection between the Xerox® device and a new IdP endpoint, establish a trust relationship between the two endpoints.

To create a first-time connection, do the following:

1. In the Embedded Web Server, click **Properties > Login/ Permissions/ Accounting**.
2. From the Login Methods window, for Identity Provider (IdP) Connection, click **Edit**.
3. In the Configuration area, for Validate IdP Server File, click **Browse**. Browse to the IdP metadata file downloaded from the IdP endpoint. For example, `IDP_metadata_forXerox.xml`.
4. Select the file, click **Open**, then click **Validate**. A message shows `Connecting to Identity Provider`.
5. If validation is successful, the message `Successfully validated Identity Provider file` appears. Click **Close**.

The Identity Provider (IdP) Connection area shows the status `Identity Provider (IdP) Configured`.

6. If validation fails, an error message appears. The error message indicates that the problem is either a connection issue, or that the IdP metadata file is not valid. Correct the issue, then repeat the procedure.
7. To test the connection between the Xerox® device and the IdP endpoint, click **Test Connection**. A message shows `Connecting to Identity Provider`. Do one of the following:
 - To abandon the test, click **Cancel**.
 - If the connection is successful, the message `Successfully connected to Identity Provider` appears. Click **Close**.
 - If the connection fails, the message `Could not connect to Identity Provider` appears. Click **Close**.

 **Note:** The connection test obtains the IdP endpoint URL from the IdP metadata file. Run this test only when the IdP metadata file is downloaded.

After you verify the connection, you can clone the IdP settings for use on other Xerox® devices. The clone file includes the device metadata file, the IdP metadata file, and the IdP configuration settings. When a device is configured from cloned IdP settings, a secure connection to the IdP endpoint is established.

For information, refer to [Cloning Options](#).

Cloning Options

This chapter contains:

- [Overview of the Cloning Options](#) 30
- [Clone Files](#) 31
- [Fleet Orchestrator](#) 32
- [Xerox® CentreWare Web](#) 33
- [Xerox® Device Manager](#) 34

Overview of the Cloning Options

Your Xerox® device provides cloning options that allow you to configure many devices in similar ways, automatically. After you configure one device, you can distribute any of the configuration settings to other devices, as needed.

The following options are available for cloning IdP settings:

- **Clone files:** A clone file contains configuration settings from a device. When you install a clone file on another device, the clone file changes the configuration settings to match the settings on the cloned device.
- **Fleet Orchestrator:** The Fleet Orchestrator feature allows you to configure many devices in similar ways automatically. After you configure one device, you can distribute any of the configuration settings to other devices, as needed.
- **Xerox® CentreWare Web:** This program enables you to manage print devices from a single interface. You can manage installations, configuration settings, run reporting, and perform periodic maintenance tasks.
- **Xerox® Device Manager:** This is another program that enables you to manage print devices from a single interface. You can manage installations, configuration settings, run reporting, and perform periodic maintenance tasks.

Clone Files

Clone files contain configuration settings from a device. You can use the clone file to overwrite the configuration settings on another device with the configuration settings from the original device. Clone files can contain general device settings, or a few settings like security policies, that you want to standardize across a fleet of devices.

Unique items, such as an IP address, are not cloned. You can save the current device settings to use later, as a backup.

You can create clone files to suit your cloning strategy. For example:

- To standardize general device settings across a group of devices, create a clone file that contains configuration settings from one device.
- To standardize security settings on all your devices, create a clone file with a set of specific settings, such as security policies.
- To clone the IdP settings only, you can choose to clone the Authentication & Authorization Configuration category only.

The Fleet Orchestrator feature allows you to create, install, and share clone files.

For information about using clone files to configure settings, refer to the *Xerox® AltaLink® Series Multifunction Printer System Administrator Guide* at www.xerox.com/office/support.

Fleet Orchestrator

The Fleet Orchestrator feature allows you to configure many devices in similar ways, automatically. After you configure one device, you can distribute any of the configuration settings to other devices, as needed. You can set up schedules to share configuration settings regularly and automatically.

For devices that have the Xerox Fleet Orchestrator feature installed:

- You can share clone files across different models of Xerox® AltaLink® multifunction printers. Devices can be on the same or different versions of system software.
- You can share software upgrade files across devices that use the same upgrade file only.
- You can share 1-Touch Add-On files to devices on the same or a higher version of system software.

If you are sharing all types of files, the software upgrade file installs first, followed by the clone files, then the 1-Touch Add-On files.

For information about using Fleet Orchestrator to configure multiple devices, refer to the *Xerox® AltaLink® Series Multifunction Printer System Administrator Guide* at www.xerox.com/office/support.

Xerox® CentreWare Web

Xerox® CentreWare Web allows you to manage print devices from a single interface. Xerox® CentreWare Web provides a browser window on most of your networked printers and multifunction devices. You can use Xerox® CentreWare Web to manage installations, configuration settings, run reporting and diagnostics, and perform maintenance tasks.

Xerox® CentreWare Web gives you the ability to find and manage printers and multifunction printers across your organization, whether they are networked or connected locally.

You can use Xerox® CentreWare® Web to transform a subset of your multifunction devices into firmware distribution hubs for the remaining devices in the fleet. Xerox® CentreWare® Web works with Fleet Orchestrator, which enables you to schedule configuration updates throughout the fleet.

For information about downloading and using Xerox® CentreWare® Web, go to www.xerox.com/CentreWareWeb.

Xerox® Device Manager

Xerox® Device Manager allows you to manage print devices from a single interface. Xerox® Device Manager provides a browser window on most of your networked printers and multifunction devices. You can use Xerox® Device Manager to manage installations, configuration settings, run reporting and diagnostics and, perform maintenance tasks. Xerox® Device Manager gives you the ability to find and manage printers and multifunction printers across your organization, whether they are networked or connected locally. You can use Xerox® Device Manager to transform a subset of your multifunction devices into firmware distribution hubs for the remaining devices in the fleet. Xerox® Device Manager works with Fleet Orchestrator, which enables you to schedule configuration updates throughout the fleet.

For more information about using Xerox® Device Manager, contact your local Xerox representative.

