VERSION 2.0
JULY 2025
702P09425

Xerox® AltaLink® and VersaLink® Series Printers

Identity Provider Configuration Guide

xerox™

BR41567

Contents

Introduction

This chapter contains:

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.

Supported Printers

The following devices support the IdP feature and can be enabled to send audit log events directly to compatible IdP systems using the syslog protocol.

- Xerox® AltaLink® C8130/8135/8145/8155/8170 Series Color Multifunction Printers
- Xerox® AltaLink® B8145/8155/8170 Series Multifunction Printers
- Xerox® AltaLink® C8230/C8235/C8245/C8255/C8270 Series Color Multifunction Printers
- Xerox® AltaLink® B8245/B8255/B8270 Series Multifunction Printers
- Xerox® VersaLink® C625 Color Multifunction Printer
- Xerox® VersaLink® B625 Multifunction Printer
- Xerox® VersaLink® C620 Color Printer
- Xerox® VersaLink® B620 Printer
- Xerox® VersaLink® C415 Color Multifunction Printer
- Xerox® VersaLink® B415 Multifunction Printer

Gathering 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.

Enabling IdP Authentication and Downloading 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_idplogin_setup.zip` downloads.
   This Zip file, `Xerox_mfp_idplogin_setup.zip`, contains the device metadata file (`Xerox_mfp_saml_metadata.xml`) and the device certificate file (`Xerox_mfp_saml_certificate.crt`).

   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.

Uploading the SAML Metadata File and Connecting 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

This chapter contains:

For more information on Overview, Prerequisites, Enabling IdP Authentication and Downloading the Device Metadata File, refer to Introduction.

Configuring the Okta App and Downloading 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: Browse to the Xerox® device certificate file named `Xerox_mfp_saml_certificate.crt` and 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, forAttribute, 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.

Uploading the SAML Metadata File and Connecting to the IdP

For more information about Upload the SAML Metadata File and Connect to the IdP, refer to Uploading the SAML Metadata File and Connecting to the IdP.

Ping Identity

This chapter contains:

For more information on Overview, Prerequisites, Enabling IdP Authentication and Downloading the Device Metadata File, refer to Introduction.

Configuring Ping Identity and Downloading 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.

Uploading the SAML Metadata File and Connecting to the IdP

For more information about Upload the SAML Metadata File and Connect to the IdP, refer to Uploading the SAML Metadata File and Connecting to the IdP.

Microsoft Entra ID (Formerly Known As Azure)

This chapter contains:

For more information on Overview, Prerequisites, Enabling IdP Authentication and Downloading the Device Metadata File, refer to Introduction.

Configuring Microsoft Entra ID and Downloading 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 Entra ID 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. To configure the SAML App Token encryption setting, click **Security > Token encryption** in the left side of the SAML application window. To import the device certificate file that you have downloaded from your Xerox device, follow these steps:
   a. Click **Import Certificate**.
   b. Browse and select the device certificate file named `Xerox_mfp_saml_certificate.crt` from the previous download.

c. Click **Add**.

6. 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.
7. To configure user settings, in the left pane, click **Properties**, then do the following:
   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.
8. 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.
9. Log out, then exit Microsoft Entra ID.

Missing the Device Certificate File

If the Device Metadata File downloaded from the printer does not have a ZIP file that contains the device certificate file, proceed with the following steps to create the certificate file manually:

1. Open the `Xerox_mfp_saml_metadata.xml` file.
2. Find the Signing section.
3. Copy the X509Certificate element value to a text editor.
4. Save the file as `Xerox_mfp_saml_certificate.crt`.

Example of Xerox_mfp_saml_metadata.xml:

- `<md:KeyDescriptor use="signing">`
- `<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">`
- `<ds:X509Data>`
- `<ds:X509Certificate>[COPY THIS VALUE]>/ds:X509Certificate>`
- `</ds:X509Data>`
- `</ds:KeyInfo>`
- `</md:KeyDescriptor>`

Overview of the IdP Sign-in Options

CONFIGURING MICROSOFT ENTRA ID TO ALLOW CERTIFICATE-BASED AUTHENTICATION

When Certificate-based Authentication (CBA) is enabled, the IdP login page will have the use certificate or smart card option for a sign-in. To login to the printer with the CBA sign-in option, use a USB card reader and smart card (PIV), or a USB security key with a smart card (PIV) interface.

To configure the Microsoft Entra ID certificate based authentication, do the following:

1. Sign in to the Microsoft Entra admin center as an administrator.
2. Browse to **Entra ID > Authentication methods > Policies**.
3. Under Manage, select **Authentication methods > Certificate-based Authentication**.
4. Ensure that the certificate-based authentication is enabled.

CONFIGURING MICROSOFT ENTRA ID TO ALLOW PASSKEY (FIDO2)

The IdP Sign-in options are Passkey (FIDO2) and Discoverable Passkey. Passkey uses the Sign in with a security key option, while Discoverable Passkey uses options such as face, fingerprint, PIN, or security key. Use your device to sign in with a passkey that appears on the IdP login page when FIDO2 is enabled. Both sign-in options are used to log-in with a USB security key using the FIDO2 interface.

To configure Microsoft Entra ID for Passkey (FIDO2), follow these steps:

1. Sign in to the Microsoft Entra admin center as an administrator.
2. Browse to **Protection > Authentication methods > Policies > Enable and Target**.
3. Under the method Passkey (FIDO2), set the toggle to Enable. Select **All users** or **Add groups** to select specific groups.
4. On the **Configure tab**, Set **Allow self-service set up** to Yes, to register a passkey by using Security information.
5. Set **Enforce Attestation** to Yes to ensure that the FIDO2 security key model or passkey provider is genuine.
6. **Enforce key restrictions** is set to Yes only if you want to allow or disallow certain security key models or passkey providers.
7. After you finish the configuration, select **Save**.

Note: For the Discoverable Passkey IdP sign-in option, you need to select a sign-in option before entering a username.

LOGIN USING FIDO2 DISCOVERABLE PASSKEY AND MICROSOFT ENTRA ID

A passkey is a discoverable FIDO2 credential. FIDO2 is a set of open standards for passwordless authentication. To avoid typing your User ID, you can use the discoverable credential sign-in option. To login using FIDO2 Discoverable Passkey and Microsoft Entra ID, follow these steps:

1. Insert your FIDO2 passkey into the USB port on the Xerox printer control panel.
2. The printer connects to the IdP and displays the login web page. Click **Sign-in** Options.

3. Click **Use your device to sign in with a passkey** option. The printer requests a security key PIN.
4. Enter the FIDO2 passkey PIN. The printer requests you to touch the **security key**.
5. Touch **FIDO2 passkey**. The printer enables you to access the control panel.

Uploading the SAML Metadata File and Connecting to the IdP

For more information about Upload the SAML Metadata File and Connect to the IdP, refer to Uploading the SAML Metadata File and Connecting to the IdP.

Cloning Options

This chapter contains:

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® and VersaLink® 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® and VersaLink® 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® and VersaLink® 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.