



Azure Setup for Single Sign-on with Onsight Admin Guide

Copyright

Onsight Platform Manager Guide

Doc #: 400391-00 Rev: A

March 2023 (v11.4.16)

Information in this document is subject to change without notice. Reproduction in any manner whatsoever without the written permission of Librestream is strictly forbidden.

Copyright Notice:

Copyright 2004-2022 Librestream Technologies Incorporated. All Rights Reserved.

Patents Notice:

United States Patent # 7,221,386, together with additional patents pending in Canada, the United States, and other countries, all of which are in the name of Librestream Technologies Inc.

Trademark Notice

Librestream, the Librestream logo, Onsight, the Onsight logo, Onsight Connect, Onsight Flow, Onsight Workspace, Onsight Cube, Onsight Collaboration Hub, Onsight Smartcam, Onsight Platform Manager, and Onsight Teamlink are either registered trademarks or trademarks of Librestream Technologies Incorporated in Canada, the United States, European Union and/or other countries. All other trademarks are the property of their respective owners.

Contents

- Copyright..... ii
- 1. Introduction..... 5
- 2. Azure AD Application Setup..... 7
 - 2.1. Prerequisites.....7
 - 2.2. Creating an Azure Application..... 7
- 3. Configure-Azure Application for SSO..... 9
 - 3.1. Configuring Azure for SSO using SAML..... 9
 - 3.1.1. Automatic Configuration using SAML Metadata..... 9
 - 3.1.2. Manual Configuration with SAML Metadata..... 12
 - 3.2. Configure Claims & Federation..... 14
 - 3.2.1. Configuring Claims & Federation.....14
 - 3.3. Assign Users and Groups..... 15
 - 3.3.1. Assign Users & Groups to Azure AD Application..... 15
 - 3.4. Validate Configuration..... 15
 - 3.4.1. Verifying the Configuration..... 15
 - 3.5. Alternate User Federation Options.....17
 - 3.5.1. Federating a User by Email Address..... 17
 - 3.6. SSO Auto-provisioning..... 18
- Index..... a

1. Introduction

Onsight enables users to authenticate using their Enterprise credentials using the Security Assertion Markup Language (SAML) 2.0 standard. SAML is widely adopted and a well-established standard for cross-domain enterprise authentication. It's supported by a variety of Identity Providers (IdP) including Azure Active Directory (Azure AD, AAD).

This guide describes the setup and configuration required to enable users to authenticate to **Onsight** using their Azure AD accounts. A typical SAML Single Sign-On (SSO) setup involves configuration of both the Identity Provider (Azure AD) and the Service Provider (Onsight) to ensure the two systems can communicate with each other and provide the expected claims lists. The focus for this document is on the **Azure AD** part of this setup using **Azure Portal**. Please refer to the [Onsight Platform Manager Administrator Guide](#) for a more detailed setup of Onsight SSO.

2. Azure AD Application Setup

You must create and configure an **Azure AD Enterprise Application** to manage SSO with **Onsight**. Please refer to Microsoft's documentation <https://learn.microsoft.com/en-us/azure/developer/> for more details about Azure application management.

2.1. Prerequisites

Prerequisites for Azure AD include:

- An active **Microsoft Azure** tenant license to create [Enterprise Applications](#)
- A **Microsoft Azure** user account with sufficient permissions to create and manage custom Azure applications
- An active Librestream tenant license for SSO
- **Onsight Platform Manager** account with Administrator permissions

2.2. Creating an Azure Application

1. Login to your **Microsoft Tenant** using the [Azure Portal](#).
2. From the **Search** bar or **Azure Services** list, select **Azure Active Directory**.

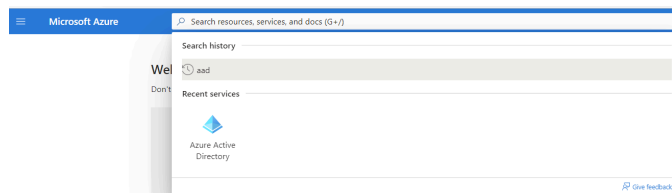


Figure 2-1 Search and Locate Azure Active Directory

3. Locate and select **Enterprise Applications** within the left-side pane.
4. From the top menu bar, select **New application**.
5. Select **Create your own application**.

Browse Azure AD Gallery ...

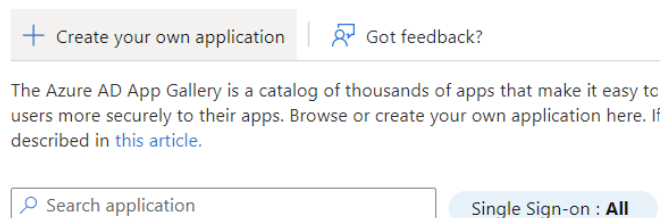
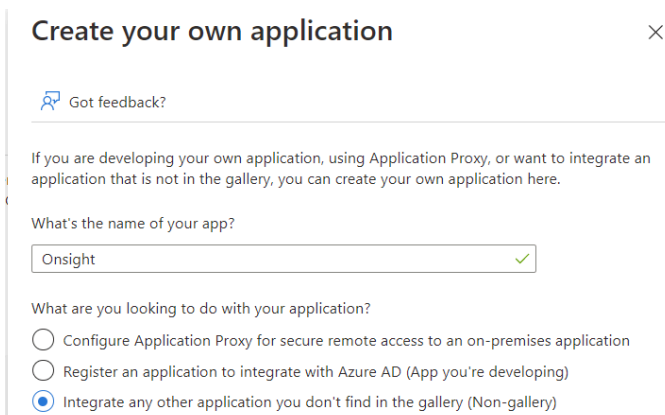


Figure 2-2 Browse Azure AD Gallery

6. In the **Create your own application** tab:
 - a. Enter an app name of your choice, such as *"Onsight"*.
 - b. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.

c. Click **Create**.



The screenshot shows a modal dialog titled "Create your own application" with a close button (X) in the top right corner. Below the title is a link "Got feedback?". The main text reads: "If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here." Below this is a question "What's the name of your app?" followed by a text input field containing "Onsight" and a green checkmark icon. Another question "What are you looking to do with your application?" is followed by three radio button options: "Configure Application Proxy for secure remote access to an on-premises application", "Register an application to integrate with Azure AD (App you're developing)", and "Integrate any other application you don't find in the gallery (Non-gallery)". The third option is selected.

Figure 2-3 Create Your Own Application

7. If successful, the new application **Overview** will display.
This completes the procedure.

3. Configure-Azure Application for SSO

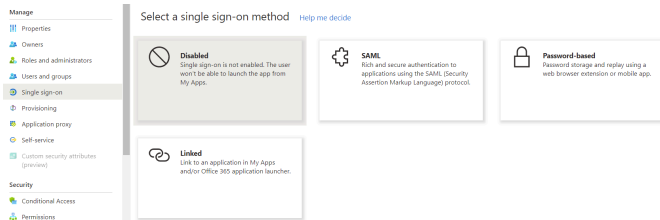
Overview

The process for configuring Azure for SSO, includes the following high-level steps:

1. Configure the Azure application for SSO using SAML.
2. Define your configuration method. Choose from:
 - Automatic configuration
 - Manual configuration
3. Configure Claims & Federation.
4. Assign users and groups.
5. Validate the configuration.
6. Explore alternate user federation options

3.1. Configuring Azure for SSO using SAML

1. Select an existing **Azure Enterprise Application** or follow [Creating an Azure Application \(on page 7\)](#) to create a new one.
2. Choose from one of the following options:
 - From application **Overview** > **Getting Started**, select **Set up single sign on**; or
 - From the left-side menu, select **Manage** > **Single sign-on**.
3. Select **SAML** as the single sign-on method.



This completes the procedure.

Next, you will need to define your configuration method as Automatic or Manual.

3.1.1. Automatic Configuration using SAML Metadata

Azure AD and Onsignt support the automatic configuration by exchange of SAML Extensible Markup Language (XML) metadata files. This configures fundamental SAML application parameters such as application Uniform Resource Locators (URLs), Entity Identifiers (IDs), and exchanging certificates.

3.1.1.1. Obtaining Onsignt SP Metadata

1. Open a new browser tab and login to [Onsignt Platform Manager](#) as an Administrator.
2. Browse to **Settings** > **SSO**. The **SSO** page contains information and configuration settings required to enable SSO for your Onsignt Domain. Please refer to the [Onsignt Platform Manager Administration Guide](#) for more details regarding SSO setup.
3. Set SSO to **Optional** for **Administrators** and **Standard Users** until the setup is complete and SSO login has been tested.

4. Locate the **LOCAL SERVICE PROVIDER SETTINGS** section and click **Export SP Metadata**. This downloads the Onsight SAML XML metadata file, named `SPMetadata.xml` by default.

SAML CONFIGURATION

LOCAL SERVICE PROVIDER SETTINGS

SSO Domain: azuresso

Entity ID: https://oam.vld.libreeng.com/OamAdministrator/azuresso/

ACS URL: https://oam.vld.libreeng.com/OamAdministrator/SSO/SAML/ACS/azuresso/

Local SAML Certificate SHA1 Hash: E20ABBB67C7C46E7BB5408A46AE69381EAE2328B

Export SP Metadata Download SP Certificate

Figure 3-2 SAML Configuration

3.1.1.2. Configuring an Azure Application with Onsight Metadata

1. Return to the **Azure AD Onsight** application **Single sign-on** settings within the **Azure Portal**.
2. Click **Upload metadata file**.
3. Select the `SPMetadata.xml` file downloaded in [Obtaining Onsight SP Metadata \(on page 9\)](#) and click **Add**.

Upload metadata file Change single sign-on mode

Upload metadata file.

Values for the fields below are provided by Onsight. You m

"SPMetadata.xml"

Add Cancel

Figure 3-3 Uploading Metadata

4. Locate the **Basic SAML Configuration** tab and verify that the **Entity ID** and **Assertion Consumer Service URL** match those shown on the **OPM > SETTINGS > SSO** page. These fields will have the following format:
 - a. Entity ID: `https://onsight.librestream.com/OamAdministrator/{Your Onsight domain suffix}`
 - b. ACS URL: `https://onsight.librestream.com/OamAdministrator/SSO/SAML/ACS/{Your Onsight domain suffix}`

Basic SAML Configuration

Save Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://oam.vld.libreeng.com/OamAdministrator/azuresso/

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

https://oam.vld.libreeng.com/OamAdministrator/SSO/SAML/ACS/azuresso/ 1

Add reply URL

Figure 3-4 Basic SAML Configuration

SAML CONFIGURATION

LOCAL SERVICE PROVIDER SETTINGS

SSO Domain: azuresso
 Entity ID: https://oam.vld.libreeng.com/OamAdministrator/azuresso/
 ACS URL: https://oam.vld.libreeng.com/OamAdministrator/SSO/SAML/ACS/azuresso/

Figure 3-5 SAML Configuration

- If the information is correct, click **Save** for the **Basic SAML Configuration**. Leave the following fields blank: **Sign On URL**, **Relay State**, and **Logout URL**. This completes the procedure.

3.1.1.3. Configuring Onsign with Azure Application Metadata

- Navigate to the **Azure Application > Single sign-on** page.
- Locate the **SAML Certificates** card and click **Download** next to **Federation Metadata XML**. This will download the Azure IdP SAML metadata XML file, titled {App Name}.xml.

SAML Certificates

Token signing certificate

Status	Active	Edit
Thumbprint	880B92B399FF4A8665BD33AA4C7517B8C00E5CF6	
Expiration	1/12/2026, 11:33:49 AM	
Notification Email	jon.hiley@librestream.com	
App Federation Metadata Url	https://login.microsoftonline.com/fab7ae4f-6e5a-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional) (Preview)

Required	No	Edit
Active	0	
Expired	0	

Figure 3-6 SAML Certificates

- Return to **OPM > SETTINGS > SSO**.
- Locate the **PARTNER IDENTITY PROVIDER SETTINGS** section and click **Import IdP Metadata**.
- Select **Upload from File** and the {App Name}.xml file downloaded in step 2.

PARTNER IDENTITY PROVIDER SETTINGS

Entity ID:
 Single Sign-on URL:

Import IdP Metadata

☒ Upload from File ☐ Paste Metadata Text ☐ Upload from URL

Choose Metadata File: [Browse...](#)

[Upload](#) [Cancel](#)

Assertion Encryption: ☐ Require Encrypted Assertions
 IdP Signing Certificate: None specified

[Import IdP Metadata](#) [Upload IdP Certificate](#)

Figure 3-7 Import IdP Metadata

- Verify that the **Partner IdP**, **Entity ID**, and **Single Sign-on URL** fields are updated. These will match those shown in the Azure AD Application **Setup {App Name}** card. Also verify the **IdP Signing Certificate** information updates. Onsign doesn't support **Single Logout** and that URL is not used.

PARTNER IDENTITY PROVIDER SETTINGS

Entity ID:

Single Sign-on URL :

Single Sign-on Binding:

Request Signature: ☐ Sign Authentication Requests

Signature Algorithm:

Digest Algorithm:

Response Signature: ☐ Require Signed Responses

Assertion Signature: ☐ Require Signed Assertions

Assertion Encryption: ☐ Require Encrypted Assertions

IdP Signing Certificate: CN=Microsoft Azure Federated SSO Certificate

Figure 3-8 Partner Identity Provider Settings

4 Set up Onsign

You'll need to configure the application to link with Azure AD.

Login URL:

Azure AD Identifier:

Logout URL:

Figure 3-9 Set Up Onsign

This completes the procedure.

3.1.1.4. Using Federation XML Metadata URL

As an alternative to first downloading the Azure XML metadata and uploading to OPM, you can provide the **Azure Federation XML Metadata URL** so that OPM can retrieve and configure SSO settings automatically.

1. Navigate to the **Azure Application Single** sign-on page.
2. Locate the **SAML Certificates** card and copy the **App Federation Metadata URL** value.
3. From **OPM > SETTINGS > SSO**, select **Import IdP Metadata**. Click to enable the **Upload From URL** option.
4. Paste the copied URL and click **Upload**. Verify that the **Entity ID**, **Single Sign-on URL**, and other **Partner IdP** configuration items update. These will match the values listed in the **Azure AD** application Setup {App Name} card.

Import IdP Metadata

☐ Upload from File ☐ Paste Metadata Text ☒ Upload from URL

Figure 3-10 Import IdP Metadata

This completes the procedure.

3.1.2. Manual Configuration with SAML Metadata

Azure AD and Onsign support the manual configuration by copying and pasting the information and setting specific fields that will retrieve their values from the XML metadata files. Use the manual configuration if the XML files can't be downloaded due to security policy or if the download/upload fails.

3.1.2.1. Manually Configuring Metadata using Copy/Paste

1. Login to **Azure Portal** and browse to the **Single Sign-on** settings of your Azure AD Onsign application.
2. Click **Edit** in the **Basic SAML Configuration** card.

3. Click **Add Identifier**.
4. Open a new browser tab and login to [Onsight Platform Manager](#) as an Administrator.
5. Browse to **OPM > Settings > SSO**. This page contains configuration and information settings required to enable SSO for you Onsight Domain.
6. Within **LOCAL SERVICE PROVIDER SETTINGS**, copy the **Entity ID**.

LOCAL SERVICE PROVIDER SETTINGS

SSO Domain: azuresso

Entity ID: <https://oam.vld.libreeng.com/OamAdministrator/azuresso/>

ACS URL: <https://oam.vld.libreeng.com/OamAdministrator/SSO/SAML/ACS/azuresso/>

Local SAML Certificate SHA1 Hash: E20ABBB67C7C46E7BB5408A46AE69381EAE2328B

Export SP Metadata Download SP Certificate

7. Within the **Azure Basic SAML Configuration**, click **Add Identifier**. Paste the copied **Entity ID**. Verify that the values match exactly, they include the https scheme, and aren't missing any trailing slashes, etc.

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

<https://oam.vld.libreeng.com/OamAdministrator/azuresso/> ✓ ⓘ

Add identifier

Figure 3-12 Identifier (Entity ID)

8. From **OPM > SETTINGS > SSO**, locate **LOCAL SERVICE PROVIDER SETTINGS** and copy the **ACS URL**.
9. In **Azure Basic SAML Configuration**, click the **Add reply URL** and **Paste** the copied ACS URL.

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

<https://oam.vld.libreeng.com/OamAdministrator/SSO/SAML/ACS/azuresso/> ✓ ⓘ

Add reply URL

Figure 3-13 Add Reply URL

10. Leave the fields blank: **Sign on URL**, **Relay State** and **Logout URL** and click **Save**.
11. From the **Azure AD Setup {App Name}** card, copy the **Azure AD Identifier** value.

4 Set up Onsight

You'll need to configure the application to link with Azure AD.

Login URL <https://login.microsoftonline.com/fab7aef4-6e5a-41ec-8023-239837f10285/>

Azure AD Identifier <https://sts.windows.net/fab7aef4-6e5a-41ec-8023-239837f10285/>

Logout URL <https://login.microsoftonline.com/fab7aef4-6e5a-41ec-8023-239837f10285/>

Figure 3-14 Set Up Onsight

12. Within **OPM > Settings > SSO**, locate **PARTNER IDENTITY PROVIDER SETTINGS** and paste this value within the **Entity ID** field.
13. From the **Azure AD Setup {App Name}** card, copy the **Login URL** value.
14. Navigate to **OPM > Settings > SSO** and locate **PARTNER IDENTITY PROVIDER SETTINGS** and paste this value in the **Single Sign-on Binding** field.

PARTNER IDENTITY PROVIDER SETTINGS

Entity ID: <https://sts.windows.net/fab7aef4-6e5a-41ec-8023-239837f10285/>

Single Sign-on URL : <https://login.microsoftonline.com/fab7aef4-6e5a-41ec-8023-239837f10285/s>

Figure 3-15 Partner Identity Provider Settings

15. From the **Azure AD SAML Certificates** panel, download **Certificate (Raw)**.
16. From the **OPM > Settings > SSO**, locate **PARTNER IDENTITY PROVIDER SETTINGS** and select **Upload IdP Certificate**.
 - a. Select the downloaded file and click **Upload**.
 - b. Verify that the upload succeeds and the **IdP Signing Certificate** details update.
 - c. Alternatively, you can download the **Base64** version of the certificate. In OPM select **Paste Certificate Text (PEM)** and paste the certificate contents.

This completes the procedure.


3.2. Configure Claims & Federation

Onsight maintains an account for users who authenticate using SSO. This account is federated to the enterprise account upon authentication. Onsight User Federation governs how the claims included in a SAML assertion map an enterprise (IdP) user to an Onsight (SP) user. This is done by matching a user property from the SAML assertion (source) to an Onsight user account attribute (target). Onsight allows you to specify which source and target attributes are used to federate identities.

Onsight doesn't require a specific set of user claims to be provided by the IdP. Depending on your desired Onsight federation and self-provisioning settings, you can include additional claims. Refer to the [Onsight Platform Manager Administrator Guide](#) for more information. Consider including:

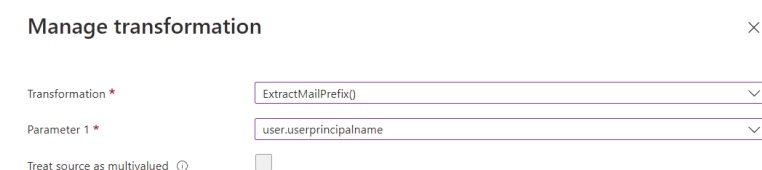
- `givenname: user.givenname`
- `surname: user.surname`
- `emailaddress: user.mail`
- `Subject Name ID (Unique User Identifier): user.userprincipalname`

The default and easiest federation setup is to match enterprise users by their SAML **Subject Name ID** from the IdP assertion to an Onsight account username. When a user authenticates to your IdP and Onsight receives the SAML assertion, the federated Onsight account is determined by matching the SAML **Subject Name ID** directly to the username.

 **Note:** When federating an assertion attribute to an Onsight username, that attribute value must not include an "@" suffix. For example, if the **Azure AD User Principal Name** (UPN) is used as the Subject Name ID, this will typically be of the form `{user}@{tenant}`. Transformation of the UPN must be performed to strip the `@{tenant}` suffix from the SAML assertion.

3.2.1. Configuring Claims & Federation

1. From the **Attributes and Claims Azure AD** application **Single sign-on** settings, click **Edit**.
2. Click the **Unique User Identifier (Name ID)** row.
3. From the **Manage Claim** screen, select **Source Transformation**.
4. From the **Manage Transformation** tab, select **ExtractMailPrefix()** as the **Transformation** type, enter `"user.userprincipalname"` as **Parameter 1** and click **Add**. As an example, suppose the **Azure AD UPN** for a user is `john.doe@acme.com`. The **ExtractMailPrefix** transformation will cause the SAML assertion **Name ID** to be `john.doe`. When receiving an assertion, OPM will federate this to the Onsight account `john.doe@{your Onsight domain}`.



Manage transformation ×

Transformation * ExtractMailPrefix()

Parameter 1 * user.userprincipalname

Treat source as multivalued ☐

Figure 3-16 Manage Transformation

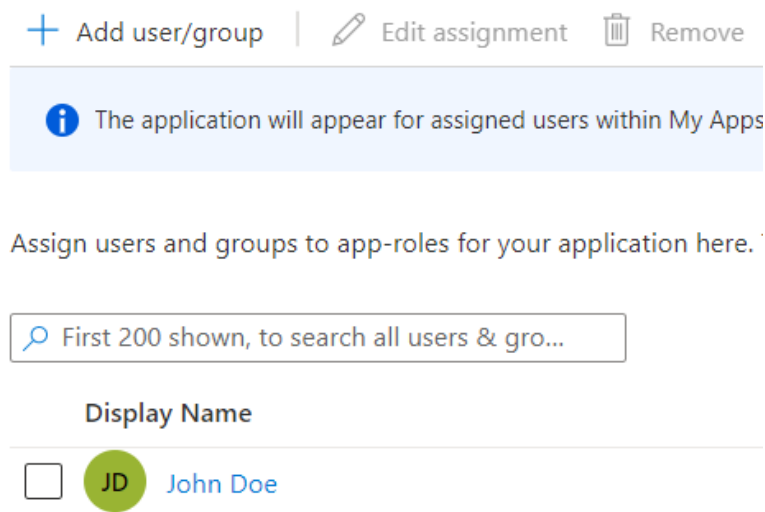
5. Leave **Claim Conditions** and **Advanced SAML Claims Options** as default and click **Save**.

3.3. Assign Users and Groups

The Onsight Azure AD application must be assigned to users who will be signing into Onsight using SSO. You can manage your organization's resources by providing access rights to a single user or to a group. If you assign access permissions to a group, then all members of the group inherit these permissions.

3.3.1. Assign Users & Groups to Azure AD Application

1. Within the **Azure Portal**, navigate to the **Onsight Azure AD** application.
2. Select **Users and groups**.
3. Click **Add user/group**.
4. Within **Users or Groups** click **None Selected**.
5. In the **Users/Groups** tab search for the user/group you would like to add to the application.
6. Select one or more entities and click **Select**.
7. Click **Assign** to complete the application assignment



This completes the procedure.

3.4. Validate Configuration

Validate the configuration of your AAD application and OPM by enabling SSO in your Onsight domain and testing login within a web browser. This validation must be done to ensure SSO can be completed successfully before enabling on your Onsight domain and notifying users.

3.4.1. Verifying the Configuration

1. Login to [Onsight Platform Manager](#) as an **Administrator**.
2. Navigate to **Settings > SSO**.
3. Verify that **Enable Single Sign-on** check box is enabled.
4. Verify that **Single Sign-On** is set to **Optional** for **Administrators** and **Standard Users**.

SINGLE SIGN-ON

☒ Enable Single Sign-On

Single Sign-On State: **ENABLED**

Standard Users: ☐ Required ☒ Optional (allow Onsign credential login)

Administrators: ☐ Required ☒ Optional (allow Onsign credential login)

Offline Login: ☐ Allow clients to operate offline

5. Locate **USER IDENTITY MAPPING** section and select:

- Onsign Account Field: User Name
- Mapped IdP Attribute: Subject Name ID

6. Locate **SELF REGISTRATION** and deselect the **Automatically create account for new users on login** check box.



Note: This can be used to provision a new Onsign account upon first authentication from your enterprise IdP. Refer to later sections and the [Onsign Platform Manager Administrator Guide](#) for more information on SSO auto-provisioning.

7. Click **Save**.

8. Launch a web-browser and navigate to **OPM > Settings > USERS (USERS)**, as needed and select  **New User**.

9. Configure the new user with a **Username** matching your Azure AD UPN prefix.

CREATE NEW USER

PROFILE

User Name:

First Name:

Last Name:

Email:

Language:

Country:

Figure 3-19 Create New User

10. Locate the **Azure AD** application Single Sign-on page and select **Test**.

11. Choose **Sign in as current user** and click **Test sign in**.

[Got feedback?](#)

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up. [Click here to get the extension](#) →

Testing sign in

Test the single sign-on configuration for Onsight by signing in here. Ensure that you have configured both the Azure Active Directory configuration and Onsight itself.

Select a way to test sign in

☒ Sign in as current user

☐ Sign in as someone else (requires browser extension)

[Test sign in](#)

Figure 3-20 Test Single Sign-on with Onsight

12. You are redirected to **Onsight Platform Manager** and signed in as the user created in Step 9 (on page 16).
13. Logout from OPM and return to the **Login** screen.
14. Enable the **Login with Single Sign On** check box.
15. Enter you Onsight domain in the **Domain** field and click **Sign in**.



Tip: If you have signed out from your Microsoft accounts, you will need to re-enter your credentials.

16. You are redirected to **Onsight Platform Manager** and signed in as the user created in Step 9 (on page 16).
17. Please refer to the [Onsight Platform Manager Administrator Guide](#) for configuring and testing **Onsight Connect** client login. This completes the procedure.

3.5. Alternate User Federation Options

The section [Configure Claims & Federation \(on page 14\)](#) describes the scenario where the Azure UPN is expected to match the Onsight username to perform account federation. Depending on your Azure/Onsight setup, this may not be applicable. For example:

- The Azure user has UPN john.doe@acme.com
- Onsight has previously been configured with usernames like jdoe@onsightacme

In this case, federation would fail to match to an existing account since jdoe doesn't match john.doe. If new user provisioning is disabled, you will see an Onsight sign-in error like:

Figure 3-21 Login Error

Instead, you can federate the user by their email address. You may configure Onsight to match the user by finding a claim in the SAML assertion named **emailaddress** and matching to the Onsight user account Email Address property.

3.5.1. Federating a User by Email Address

To federate a user by email address, you will need to:

1. Navigate to the **Azure AD** application **Single Sign-on** settings and **Edit** the **Attributes & Claims**.
2. Verify that there is an **emailaddress** claim listed within the **Additional claims** section.

Additional claims				
Claim name	Condi...	Type	Value	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	0	SAML	user.mail	***

Figure 3-22 Additional Claims

3. **Copy** the entire claim name, including the http namespace.
4. Navigate to the **OPM > SETTINGS > SSO** page.
5. Locate **USER IDENTITY MAPPING** and select:
 - **Onsight Account Field: Email Address**
 - **Mapped IdP Attribute: Attribute**
6. Paste the **Claim name** from Azure AD into the OPM **Attribute Name** field.

USER IDENTITY FEDERATION

USER IDENTITY MAPPING

Onsight Account Field:

Mapped IdP Attribute:

Attribute Name:

Figure 3-23 User Identify Federation

7. Navigate to the **OPM Users** list. Verify that your user account has the correct email which matches the address configured in Azure.



Note: For this configuration, you must verify that email addresses are unique among users in your Onsight domain. Verify that there aren't multiple Onsight accounts sharing the same email address.

8. Repeat the steps within Step 9 (on page 16) to verify login.
This completes the procedure.

Other combinations of enterprise and Onsight properties can be used to accomplish account federation. Options for this configuration depend on what attributes you expect from your **IdP** and how you want your Onsight accounts to be setup. Refer to the [Onsight Platform Manager Administrator Guide](#) for more details or contact a Librestream Support representative to explore more options.

3.6. SSO Auto-provisioning

In the previous examples, sign-on will only succeed if the authenticated Azure account was federated to an existing Onsight user account. Alternatively, you can enable SSO Self-Registration to automatically create an Onsight account upon first authentication.

A variety of options exist for self-Registration which are documented in more detail in the [Onsight Platform Manager Administrator Guide](#). As a summary, you may select:

1. Which Onsight license types are assigned to self-provisioned users?
2. Whether Administrators are notified when a new account is self-provisioned.
3. How properties are set for the new user account, including **email address**, **name**, etc. This includes options to:
 - **Prompt at login:** If any of the fields are set to prompt the user, they will need to complete a registration form at first login.
 - **Attribute:** You can specify a **SAML** attribute name. That attribute value used is the corresponding Onsight account property.

This configuration will retrieve the account email address from the given SAML attribute. The users **Name** and **Password** are prompted at login when the new account is created.

The screenshot shows the 'SELF REGISTRATION' configuration page. It includes several sections: 'Licenses' with checkboxes for 'Connect Enterprise', 'Workspace Enterprise', and 'Workspace Contributor'; 'Notification' with checkboxes for 'Notify Administrators by email when an account is registered' and 'Require Email Address for Self Registered Accounts'; 'Email' with a dropdown for 'Attribute' and a text field for 'Attribute Name' containing 'http://schemas.xmlsoap.org'; 'Allowed Email Domains' with a text field and a note to restrict user-created accounts to specified email domains; 'Name' with a dropdown for 'Prompt on First Login'; and 'Password' with a dropdown for 'Prompt on First Login'.

Figure 3-24 Self-Registration

The registration form in this case looks like:

The screenshot shows the 'COMPLETE YOUR ACCOUNT SETUP' registration form. It includes a header for 'ON SIGHT PLATFORM MANAGER' and a sub-header 'COMPLETE YOUR ACCOUNT SETUP'. Below this is a message: 'We just need a few more details before we can finish setting up your OnSight account.' The form is divided into two sections: 'PROFILE' and 'PASSWORD'. The 'PROFILE' section has fields for 'User Name' (with a dropdown showing 'jon.hiley' and '@azure'), 'First Name', 'Last Name' (with a dropdown showing 'Optional'), and 'Email' (with a dropdown showing 'jon.hiley@librestream.com'). The 'PASSWORD' section has a message: 'Choose an OnSight Account password. This will allow you to log in directly to OnSight in cases where your single-sign on provider is not available.' and fields for 'Password' and 'Confirm Password'. A 'Complete Registration' button is at the bottom.

Figure 3-25 Complete Your Account Setup

Index

- A**
 - Access 15
 - Access rights 15
 - Account Federation 17, 17
 - ACS URL 10, 12
 - Add Identifier 12
 - Add User/Group 15
 - Administrator 9, 15
 - Administrator permissions 7
 - Administrators 9, 18
 - Advanced SAML Claims Options 14
 - Alternate User Federation Options 9, 17
 - App Federation Metadata URL 12
 - App Name 7
 - Application 7
 - Application Assignment 15
 - Application Parameters 9
 - Assertion Consumer Service URL 10
 - Assign Users and Groups 15
 - Attribute Name 17
 - Attributes 14, 17
 - Authenticate 5
 - Automatic Configuration 9, 9, 9
 - Azure 17
 - Azure Active Directory 7
 - Azure Active Directory (Azure AD, AAD) 5
 - Azure AD 7, 9, 10, 12, 14, 17
 - Azure AD accounts 5
 - Azure AD application 15, 15
 - Azure AD application Setup 12
 - Azure AD Application Setup 11
 - Azure AD Gallery 7
 - Azure AD User Principal Name 14
 - Azure Application 7, 9, 10, 11, 12
 - Azure Enterprise Application 9
 - Azure IdP SAML Metadata XML File 11
 - Azure Portal 5, 7, 10, 12, 15
 - Azure User Account 7
- B**
 - Base64 12
 - Basic SAML Configuration 10, 12
- C**
 - Claim Conditions 14
 - Claims 14, 17
 - claims lists 5
 - Communicate 5
 - Configuration 5, 15
 - Configuration Items 12
 - Configuration Method 9
 - Configure Claims 9
 - Copying 12
 - Create your own application 7
 - Cross-domain Enterprise Authentication 5
 - Custom Azure Applications 7
- D**
 - Download 11, 12
- E**
 - Email Address 14, 17, 17, 18
 - Email Description 7
 - enterprise account 14
 - Enterprise Applications 7, 7
 - Enterprise credentials 5
 - Entity ID 10, 12, 12
 - Entity Identifiers 9
 - Exchange 9
 - Exchanging Certificates 9
 - Export SP Metadata 9
 - ExtractMailPrefix 14
- F**
 - Fails 12
 - Federate Identities 14
 - Federating 17
 - Federation 9
 - Federation Metadata XML 11
 - Federation XML Metadata URL 12
 - Format 10
- G**
 - Givenname 14
 - Graphical user interface 7
 - Groups 9, 15
 - Guide 5
- H**
 - High-level Steps 9
 - http Namespace 17
 - https Scheme 12
- I**
 - Identity Provider (Azure AD) 5
 - Identity Providers (IdP) 5
 - IdP 14, 17
 - IdP Certificate 12
 - IdP Signing Certificate 11, 12
 - IDs 9
 - Implementation 15
 - Import IdP Metadata 11, 12
 - Information 12
 - Integrate 7
- L**
 - Librestream Support 17
 - Librestream Tenant License 7
 - License Types 18
 - Local Service Provider Settings 9, 12
 - Login 15, 15
 - Login URL 12
 - Login Verification 17
 - Logout URL 10
- M**
 - Manage 15
 - Manual Configuration 9, 9, 12
 - Mapped IdP Attribute 15, 17
 - Metadata 11
 - metadata file 10
 - Microsoft Azure tenant license 7
 - Microsoft Tenant 7
- N**
 - Name 18
 - New application 7
 - New Application Overview 7
 - New User 15
 - New User Provisioning 17
 - Non-gallery 7
- O**
 - Onsight 5, 7, 9, 11, 12, 14, 15, 17

- Onsight account 14
- Onsight Account Field 15, 17
- Onsight Account Username 14
- Onsight Azure AD application 15
- Onsight Connect 15
- Onsight doesn't support Single Logout 11
- Onsight Domain 17
- Onsight Metadata 10
- Onsight Platform Manager 9, 12, 15
- Onsight Platform Manager account 7
- Onsight Platform Manager Administrator 18
- Onsight Platform Manager Administrator Guide 5
- Onsight Sign-in Error 17
- Onsight SP Metadata 9
- Onsight user account attribute 14
- Onsight User Federation 14
- OPM 10, 11, 11, 12, 14, 15, 17
- OPM Users 15
- OPM Users List 17

P

- Partner Identify Provider Settings 11
- Partner Identity Provider Settings 12
- PARTNER IDENTITY PROVIDER SETTINGS 11
- Partner IdP 12
- Partner IdP Entity ID 11
- Paste Certificate Text 12
- Pasting 12
- PEM 12
- Permissions 7, 15

R

- Registration Form 18
- Relay State 10
- Reply URL 12
- Retrieve Values 12

S

- SAML 9, 9
- SAML assertion 14, 14
- SAML Assertion 17
- SAML Certificates 11, 12, 12
- SAML Configuration 9, 10
- SAML Extensible Markup Language 9
- SAML Metadata 9
- SAML Single Sign-On (SSO) 5
- SAML XML metadata file 9
- Save 10
- Security Assertion Markup Language (SAML) 2.0 5
- Security Policy 12
- Self Registration 15
- Self-provisioning 14
- Self-Registration 18
- Service Provider (Onsight) 5
- Set Up Onsight 11
- Settings 10, 11, 11, 12, 12, 15, 17
- SettingsSSO 9
- Setup 5, 15
- Setup of Onsight SSO 5
- Sign in 15
- Sign On URL 10
- Single sign-on 10, 11, 14
- Single Sign-on 12, 15, 17
- Single Sign-on Method 9
- Single Sign-on settings 12
- Single Sign-on URL 11, 12
- Source Transformation 14
- SP 14

- Specific Fields 12
- SPMetadata.xml 10
- SSO 7, 9, 9, 10, 11, 11, 12, 12, 14, 15, 15, 15, 17, 18
- SSO login 9
- SSO page 9
- SSO setup 9
- Standard Users 9
- Subject Name ID 14
- Surname 14

T

- Test 15
- Testing 15
- Text 7

U

- Uniform Resource Locators 9
- Unique User Identifier 14
- Upload 12
- Upload From URL 12
- Uploading Metadata 10
- UPN 17
- URLs 9
- User Claims 14
- User Identity Mapping 15, 17
- user property 14
- user.userprincipalname 14
- Users 9, 15, 15
- Users and Groups 15
- Users or Groups 15

V

- Validate 15
- Verify 9, 15

W

- Web Browser 15

X

- XML 9
- XML Metadata 12