Configure Microsoft Entra ID SSO External Authentication for DMP

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Cisco Domain Protection (Part 1)
- Microsoft Entra ID
- Cisco Domain Protection (Part 2)

Verify

Troubleshoot

Introduction

This document describes how to configure Microsoft Entra ID single sign-on to authenticate to Cisco Domain Protection portal.

Prerequisites

Requirements

Cisco recommends that you have knowledge on these topics:

- Cisco Domain Protection
- Microsoft Entra ID
- Self-Signed or CA Signed (optional) X.509 SSL certificates in PEM format

Components Used

- Cisco Domain Protection administrator access
- Microsoft Entra ID admin center administrator access

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

- Cisco Domain Protection enables SSO log in for end-users via SAML 2.0 protocol.

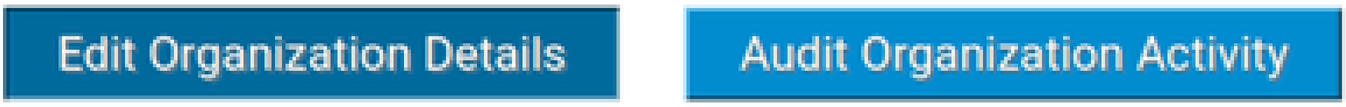
- Microsoft Entra SSO allows and controls access to your software as a service (SaaS) apps, cloud apps, or on-premises apps from anywhere with single sign-on.

- Cisco Domain Protection can be set as a managed identity application connected to Microsoft Entra with authentication methods that include multi-factor authentication as password-only authentication is not safe nor recommended.
- SAML is an XML-based open standard data format that enables administrators to access a defined set of applications seamlessly after the sign into one of those applications.
- To learn more about SAML, refer to: What is SAML?

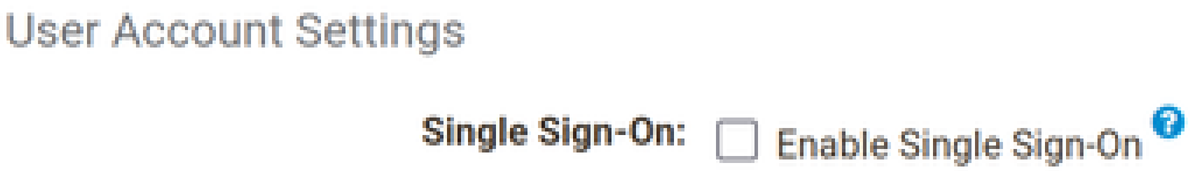
Configure

Cisco Domain Protection (Part 1)

1. Log into **Cisco Domain Protection admin portal** and navigate to **Admin** > **Organization.** Click **Edit Organization Details** button, as shown in the image:

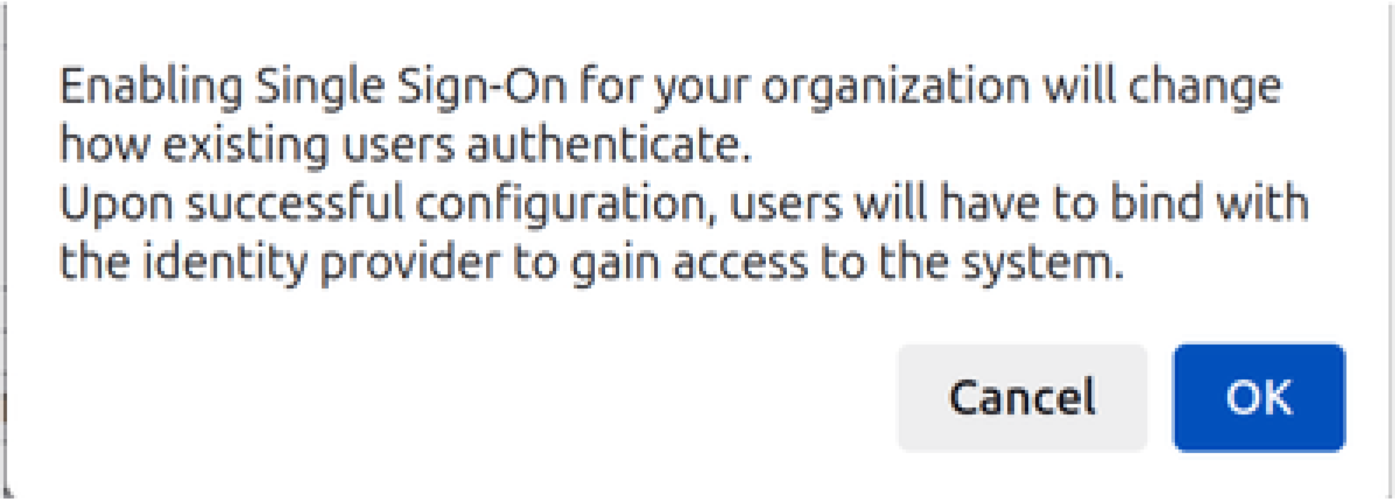


2. Navigate to the **User Account Settings** section and click **EnableSingle Sign-On** check box. A message appears as shown in the image:



User Account Settings

Single Sign-On: □ Enable Single Sign-On



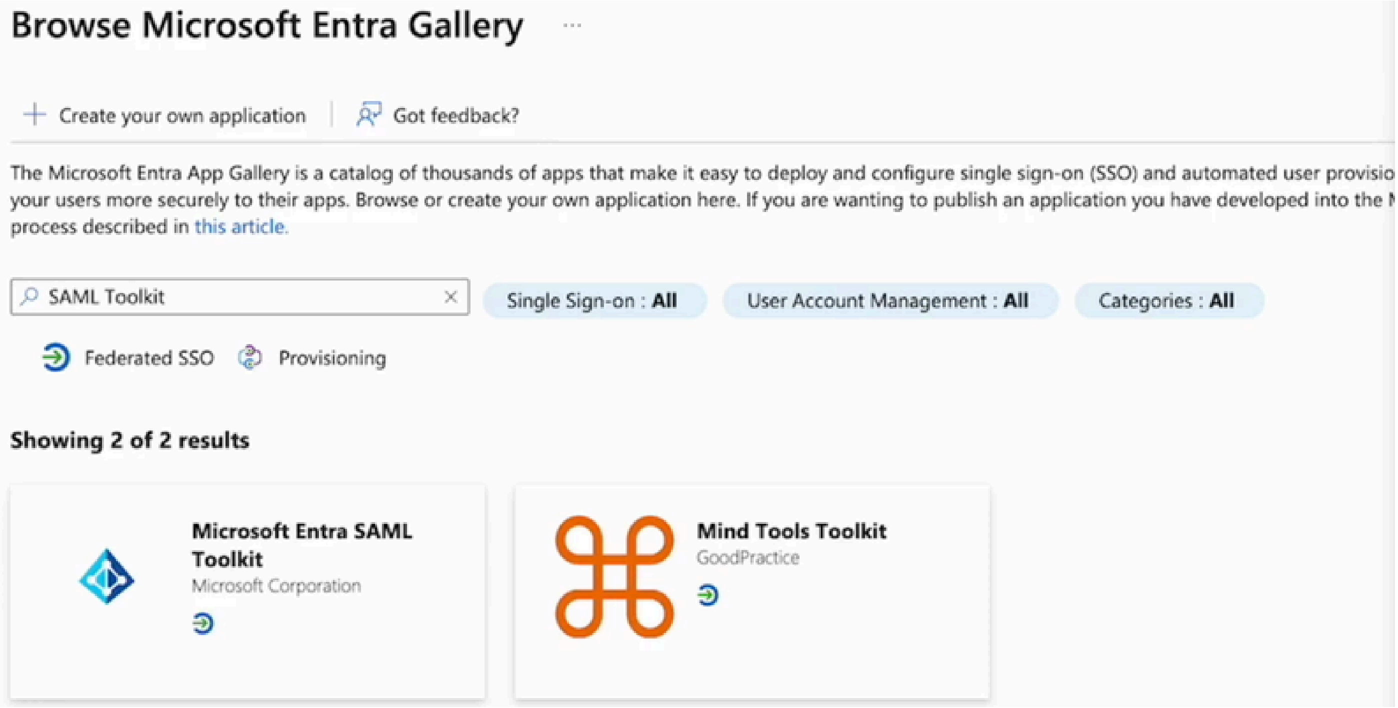
Enabling Single Sign-On for your organization will change how existing users authenticate.
Upon successful configuration, users will have to bind with the identity provider to gain access to the system.

3. Click the **OK** button and copy the **Entity ID and Assertion Consumer Service (ACS) URL parameters**. These parameters must be used in Microsoft Entra ID Basic SAML authentication. Return later for setting up the Name Identifier Format, SAML 2.0 Endpoint and Public Certificate parameters.

- **Entity ID:** dmp.cisco.com
- **Assertion Consumer Service URL:**https://<dmp_id>.dmp.cisco.com/auth/saml/callback

Microsoft Entra ID

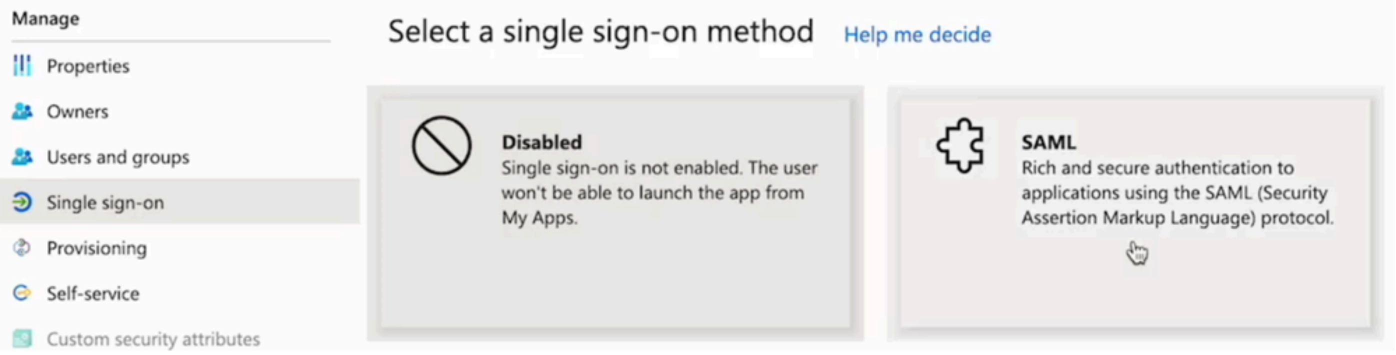
1. Navigate to **Microsoft Entra ID admin center** and click the **Add Button.** Select **Enterprise Application**, and search for **Microsoft Entra SAML Toolkit**, as shown in the image:



The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisio your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the M process described in this article.

2. Name it with a meaningful value and click **Create**. For example, **Domain Protection Sign On**.

3. Navigate to the left side panel, under the **Manage** section. Click **Single sign-on**, and select **SAML**.



Disabled: Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML: Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

4. In the **Basic SAML Configuration** panel, click **Edit**, and fill in the parameters:

- **Identifier (Entity ID):** dmp.cisco.com
- **Reply URL (Assertion Consumer Service URL):** https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- **Sign on URL:** https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Click **Save.**

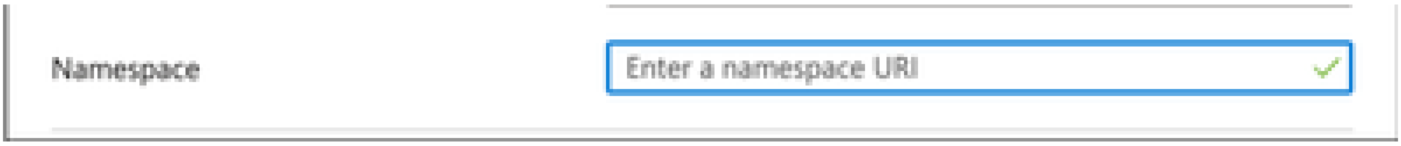
5. In the **Attributes & Claims** panel, click **Edit**.

Under **Required claim**, click the **Unique User Identifier (Name ID)** claim to edit it.

- Set the **Source attribute** field to **user.userprincipalname**. This assumes that the value of user.userprincipalname represents a valid email address. If not, set **Source** to **user.primaryauthoritativeemail**.
- Under **Additional Claims** panel, click **Edit** and create the **mappings** between Microsoft Entra ID user properties and SAML attributes.

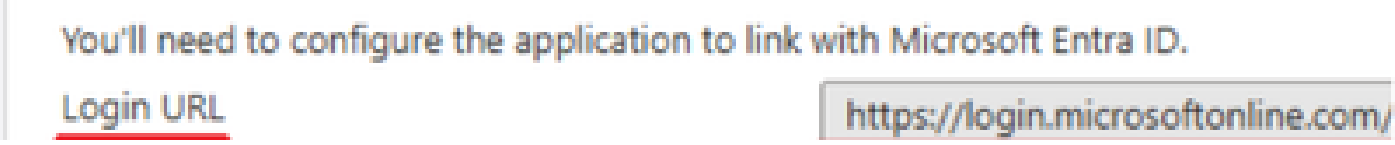
Name	**Namespace**	**Source Attribute**
emailaddress	No value	user.userprincipalname
firstName	No value	user.givenname
lastName	No value	user.surname

Be sure to clear the **Namespace** field for each claim, as shown below:



6. Once the Attributes & Claims sections are filled, the last section SAML Signing Certificate is populated.

- Save the **Login URL.**



You'll need to configure the application to link with Microsoft Entra ID.

Login URL https://login.microsoftonline.com/

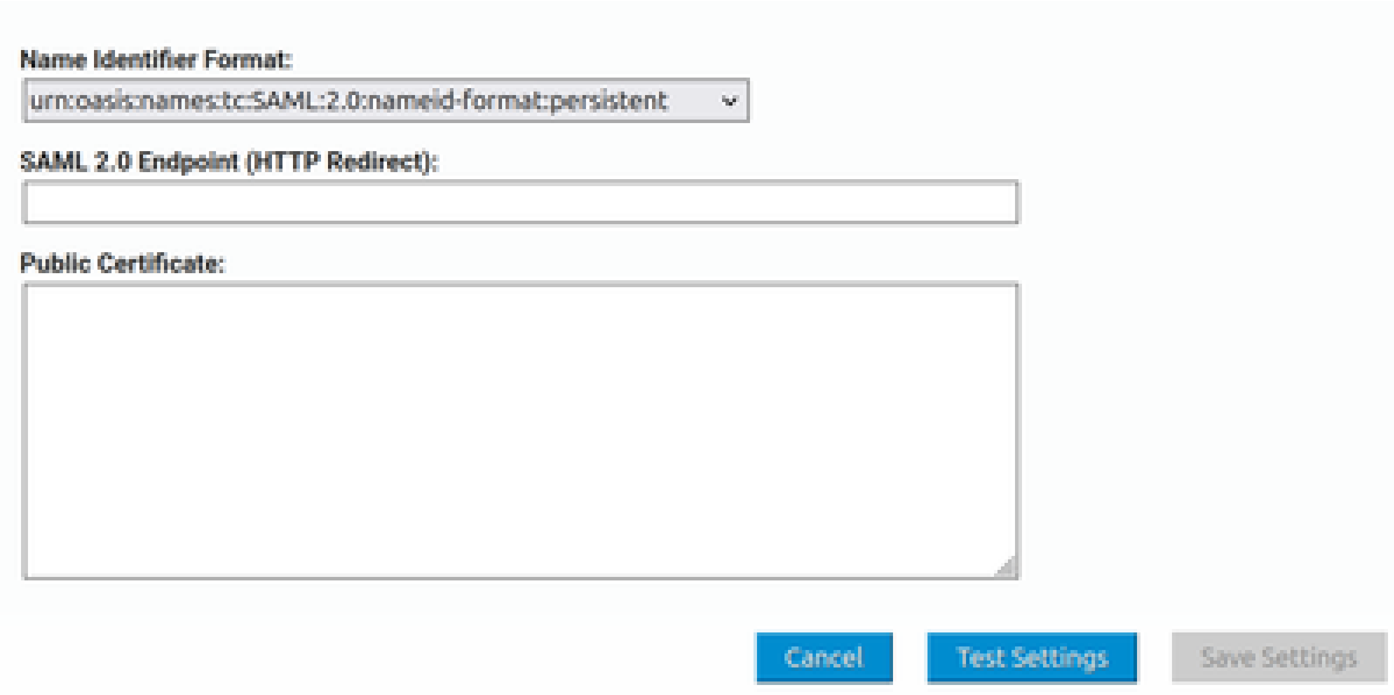
- Save the **Certificate (Base64).**

Certificate (Base64)
Download

Cisco Domain Protection (Part 2)

Return to **Cisco Domain Protection > Enable Single Sign-On** section.

- **Name Identifier Format:** urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- **SAML 2.0 Endpoint (HTTP Redirect):** Login URL provided by Microsoft Entra ID
- **Public Certificate**: Certificate (Base64) provided by Microsoft Entra ID



Name Identifier Format:

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

SAML 2.0 Endpoint (HTTP Redirect):

Public Certificate:

Verify

Click **Test Settings.** It redirects you to the login page of your Identity Provider. Log in using your SSO credentials.

After a successful log in, you can close the **window**. Click **Save Settings**.

Troubleshoot

```
Error - Error parsing X509 certificate
```

- Ensure the certificate is in Base64.

```
Error - Please enter a valid URL
```

- Ensure the Login URL provided by Microsoft Entra ID is correct.