Configure UCCE Single Sign-on with Azure Cloud Integration SAML 2.0

Contents

Introduction

This document describes the configuration of Microsoft Azure as the Identity Provider (IdP) for Single Sign-On (SSO) in Unified Contact Center Enterprise (UCCE) with Security Assertion Markup Language (SAML) and Cisco Identity Service (IDS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SAML 2.0
- Cisco UCCE and Packaged Contact Center Enterprise (PCCE)
- SSO
- IDS
- IdP

Components Used

The information in this document is based on these software and hardware versions:

- Azure IdP
- UCCE 12.0.1, 12.5.1, 12.5.2, ,12.6.1 and 12.6.2
- Cisco IdS 12.0.1, 12.5.1,12.52, ,12.6.1 and 12.6.2

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.

Configure

1. Export UCCE Metadata Files

The Cisco IDS provides authorization between the IdP and applications.

When Cisco IDS is configured, a metadata exchange is set up between the Cisco IDS and the IdP. This exchange establishes a trust relationship that allows applications to use the Cisco IDS for SSO. The trust relationship is established when a metadata file is downloaded from the Cisco IDS and uploaded to the IdP.

1.1. Procedure

- In Unified CCE Administration, navigate to Features > Single Sign-On .
- Click Identity Service Management and the Cisco Identity Service Management window opens
- Enter the User Name , and then click Next.
- Enter the password , and then click Sign In.
  - The Cisco Identity Service Management page opens, and it shows the Nodes, Settings, and Clients icons in the left pane.
- Click Nodes.
  - The Nodes page opens to the overall Node level view and identifies which nodes are in service. The page also provides the SAML Certificate Expiry details for each node, that indicate when the certificate is due to expire. The node Status options are Not Configured, In Service, Partial Service, and Out of Service. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.
- Click Settings.
- Click IdS Trust.
- To begin the Cisco IdS trust relationship, set up between the Cisco IdS and the IdP, click Download Metadata File to download the file from the Cisco IdS Server.

2. Generate Certificate Signing for Azure Responses

If you have OpenSSL installed, generate a certificate for Azure and provision it on the Azure application. Azure includes this certificate in its IdP metadata export and uses it to sign the SAML assertions that it sends to UCCE.

If you do not have OpenSSL, use your enterprise CA to generate a certificate.

2.1 Procedure (OpenSSL)

Here is the procedure to create a certificate via OpenSSL

- Create a certificate and a private key:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 1095 -out certificate.pem
```

- Combine the certificate and the key into a password-protected PFX file, which is required by Azure.

Ensure to take note of the password.

```
openssl pkcs12 -export -out certificate.pfx -inkey key.pem -in certificate.pem
```

- Generate a single certificate for UCCE.
- Upload the certificate to the Azure IdP.

3. Configure Azure Custom Application

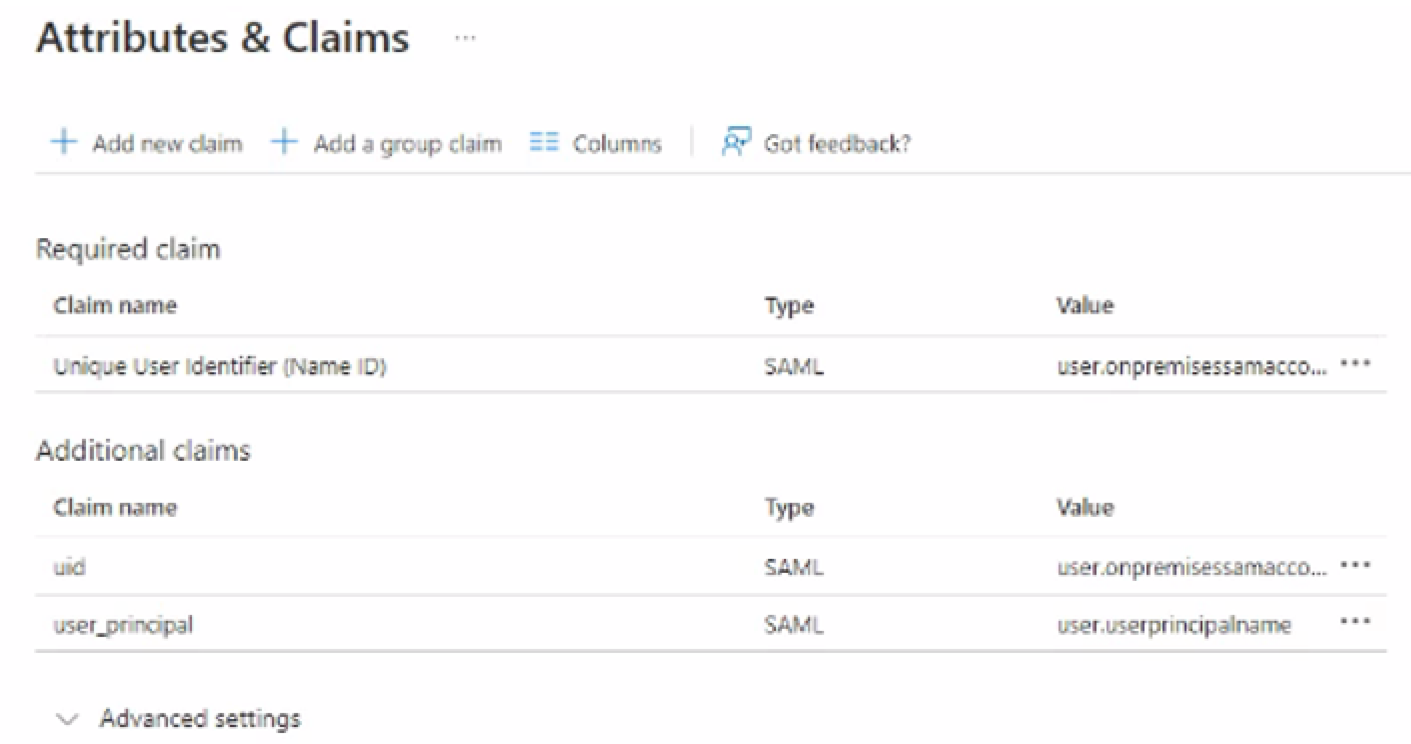
Before you configure Azure, you must export UCCE metadata from UCCE IDS Publisher. You can have both the UCCE metadata XML file and a certificate for the IdP connection before you start these steps on Azure.

3.1. Procedure

- In Microsoft Azure, navigate to Enterprise Applications and then select All Applications.
- To add a new application, select New application .
- In the Add an Application window, proceed with these steps:

  1. Click Create your own application (Non-gallery).
  2. Enter the Name of your new application (for example, UCCE) and click Create.
  3. In the left navigation bar for the new application, click Single sign-on .
  4. Click SAML .
  5. The Set up Single Sign-On with SAML window appears.
- Click Upload metadata file and then browse to the UCCE metadata XML file.
- After you select and open the file, click Add .
  - The Basic SAML Configuration populates with Identifier (EntityID) and Reply URL (Assertion consumer service URL) for the UCCE server.
  - Click Save .
- In the User Attributes & Claims section, click Edit :
  - Under Required Claim, click on Unique User Identifier (Name ID).
  - For the name identifier format, select Default.
  - For the Source attribute, select user.onpremisessamaccountname .
  - Click Save.
  - Under Additional claims, delete all the claims that exist. For each claim, click (â€¦) and select Delete. Click OK to confirm.
  - Click Add new claim to add the uid claim
  - For Name, enter uid.
  - Leave the Namespace field blank.
  - For Source, check the Attribute radio button.
  - From the Source attribute drop-down, select user.givenname (or user.onpremisessamaccountname).
  - Click Save.
  - Add a new claim to add the user_principal claim.
  - For Name, enter user_principal.
  - Leave the Namespace field blank.
  - For Source, check the Attribute radio button.
  - From the Source attribute drop-down, select user.userprincipalname.
  - Click Save.

Snapshot for reference to be configured:



Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.onpremisessamacco...

Additional claims

Claim name	Type	Value
uid	SAML	user.onpremisessamacco...
user_principal	SAML	user.userprincipalname

-
- Click SAML-based Sign-on to return to the SAML summary.
- In the SAML Signing Certificate section, click Edit:
  - Set the Signing Option to **Sign SAML Response and Assertion.**
  - Set the Signing Algorithm to the appropriate SHA algorithm. For example, SHA-256.
- Click Import Certificate.
- In the Certificate field, browse to and open the certificate.pfx file that was created earlier.
- Enter the password for the certificate and click Add .

This must be the only certificate in the list and must be active.

- If this certificate is not active, click the adjacent dots (â€¦), select Make certificate active and then click Yes.
- If there are other certificates in the list, click the adjacent dots (â€¦) for those certificates, select Delete Certificate and click Yes to delete those certificates.

- Click Save.
- Download the Federation Metadata XML file.
- Enable the Application in Azure and Assign Users:

Azure provides you with the ability to assign individual users for SSO with Azure, or all users. Assume that SSO is enabled for all users by DU.

- In the left navigation bar, navigate to Enterprise Applications > UCCE (or the application name as given by you).
- Select Manage > Properties .
- Set Enabled for users to sign in? to Yes.
- Set Visible to users? to No.
- Click Save.

As a final check, check the IdP metadata file and ensure that the certificate that you created previously is present in the <X509Certificate> field as the signing certificate in the IdP metadata file. The format is as follows:

```
<KeyDescriptor use="signing">
<KeyInfo>
<X509Data>
<X509Certificate>
--actual X.509 certificate--
</X509Certificate>
</X509Data>
</KeyInfo>
</KeyDescriptor>
```

4. Upload Azure Metadata File in UCCE

Before you go to UCCE IDS again, you must have the Federation Metadata XML file downloaded from Azure.

4.1 Procedure

- In Unified CCE Administration, navigate to Features > Single Sign-On.
- Click Identity Service Management and the Cisco Identity Service Management window opens
- Enter the user name, and then click Next .
- Enter the password , and then click Sign In .
    - The Cisco Identity Service Management page opens and shows the Nodes, Settings, and Clients icons in the left pane.
- Click Nodes .
    - The Nodes page opens to the overall Node level view and identifies which nodes are in service. The page also provides the SAML Certificate Expiry details for each node, that indicate when the certificate is due to expire. The node Status options are Not Configured, In Service, Partial Service, and Out of Service. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.
- To upload the Federation Metadata XML from Azure, browse to locate the file.
- Browse to the Upload IdP Metadata page and upload the Federation Metadata XML file.
    - When the file upload finishes, a notification message is received. The metadata exchange is now complete, and the trust relationship is in place.
- Clear browser cache.
- Enter valid credentials when the page is redirected to IdP.
- Click Next.
    - The Test SSO Setup page opens.
- Click Test SSO Setup .
    - A message appears that tells you that the Cisco IdS configuration has succeeded.
- Click Settings .
- Click Security.
- Click Tokens.
- Enter the duration for these settings:
    - **Refresh Token Expiry** - The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
    - **Authorization Code Expiry** - The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
    - **Access Token Expiry** - The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.
- Set the Encrypt Token (optional); the default setting is On.

- Click Save .
- Click Keys and Certificates .
- The Generate Keys and SAML Certificate page opens. It allows to:
    - Click Regenerate and regenerate the Encryption/Signature key. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration.
    - Click Regenerate and regenerate the SAML Certificate. A message appears to say that the SAML certificate regeneration is successful.
- Click Save .
- Click Clients.
    - This page identifies the Cisco IdS clients that already exist, and provide the client name, the client ID, and a redirect URL. In order to search for a particular client, click the Search icon at the top of the list of names and type the name of the client.
- To add a client:
    - Click New .
    - Enter the name of the client.
    - Enter the Redirect URL. In order to add more than one URL, click the plus icon.
    - Click Add (or click Clear and then click X to close the page and not add the client).
    - To edit or delete a client, highlight the client row and click the ellipses under Actions.
    - Then:
        - Click Edit to edit the name of the client, ID, or redirect URL. On the Edit Client page, make changes and click Save (or click Clear and then click the X to close the page and do not save edits).
        - Click Delete to delete the client.

Note: The certificate must be with SHA-256 Secure Hash Algorithm.