Enabling Single Sign-On for Common Identity using Active Directory Federation Services
Table of Contents

Introduction .................................................................................................................... 1

Enabling SSO for WebEx Messenger ............................................................................... 3

Configure Federated Web SSO ..................................................................................... 3

Create a Relying Party Trust ....................................................................................... 3

Add Claim Rules for Messenger ................................................................................ 4

Download the ADFS Metadata ................................................................................... 7

Import SAML Metadata in WebEx Messenger ............................................................. 7

Add the Rules for JIT (Just in Time Provision) ............................................................. 8

Enable Auto Account Creation and Auto Account Update in WebEx Messenger ...... 8

Migration from WebEx Messenger to Common Identity SSO Authentication ............ 11

Request to Add Domain to Common Identity .............................................................. 11

Create a Password in CI ............................................................................................. 11

Configure SSO in Cloud Collaboration Management ................................................ 11

Create a Relying Party Trust for CI ........................................................................... 12

Add Claim Rules for CI .............................................................................................. 12

Export and Edit the Metadata ................................................................................... 14

Complete SSO Configuration in Cloud Collaboration Management ....................... 15
Troubleshooting ........................................................................................................ 16
Redirect Authentication ...................................................................................................... 17

Verification of Cisco Jabber Authentication in CI ....................................................... 18
Introduction

This document covers the configuration of the required software components essential for achieving a Single Sign-on (SSO) solution with WebEx Messenger using Active Directory Federation Services (ADFS).
Enabling SSO for WebEx Messenger

Configure Federated Web SSO

1. Log into http://www.webex.com/go/connectadmin with your administration credentials.
2. Select the Configuration tab > System Settings > Security Settings.
3. Select Federated Web SSO Configuration.
4. In the WebEx SAML Issuer (SP ID) field, enter the name for the SAML agreement.
   
   **Note:** You can use the fully qualified domain name (FQDN) of your organization.

5. Complete all the required fields.
6. Select Export to export the metadata to a location on your computer. You will import this file later.

Create a Relying Party Trust

1. Go to your Active Directory Federation Services (ADFS) server.
2. In the Actions dialog box, select Add Relying Party Trust.
3. Select **Import data about the relying party from a file**.
4. Select **Browse** to navigate to and select the metadata file.
5. Select **Next**.
6. Enter the display name for the SAML agreement.
7. Select **Next**.
8. Select the **I do not want to configure multi-factor authentication settings for the relying party trust at this time** radio button.
9. Select **Next**.
10. Select the **Open the Edit Claim Rules dialog for the relying party trust when the wizard closes** check box.
11. Select **Close**.

**Add Claim Rules for Messenger**

1. In the **Edit Claim Rules for Messenger** dialog box, select **Add Rule**.
2. In the **Add Transform Claim Rule Wizard** from the **Claim rule template** drop-down, select the **Send LDAP Attributes as Claims** template.
3. Select Next.

4. Enter the claim name and select the **E-Mail-Addresses** and **IncomingClaim** attributes as shown below.

5. Select OK.

6. Create another new rule as before using the Claim rule template **Transform an Incoming Claim**.

7. Enter the claim name.

8. From the **Incoming claim type** drop-down, select **IncomingClaim**.

9. From the **Outgoing claim type** drop-down, select **Name ID**.

10. From the **Outgoingname ID format** drop-down, select **Unspecified**.
11. Select **OK**.
Download the ADFS Metadata

1. Download the ADFS metadata from https://<FQDN of your ADFS server>/FederationMetadata/2007-06/FederationMetadata.xml.

2. Select OK.

Import SAML Metadata in WebEx Messenger

1. Log into http://www.webex.com/go/connectadmin with your administration credentials.

2. Select the Configuration tab > System Settings > Security Settings.

3. Select Federated Web SSO Configuration.

4. Select Import SAML Metadata to import the metadata file you downloaded.


This string ensures that ADFS can deliver Kerberos and Form based authentication.
Chapter 2: Enabling SSO for WebEx Messenger

Add the Rules for JIT (Just in Time Provision)

1. In the **Edit Claim Rules for Messenger** dialog box, select **Add Rule**.
2. In the **Add Transform Claim Rule Wizard** from the **Claim rule template** drop-down, select the **Send LDAP Attributes as Claims** template.
3. Select **Next**.
4. Enter the claim name (JIT) and select the attributes as shown below.

![Edit Rule - JIT](image)

5. Select **OK**.

Enable Auto Account Creation and Auto Account Update in WebEx Messenger

2. Select the **Configuration tab > System Settings > Security Settings**.
3. Select **Federated Web SSO Configuration**.
4. Select the **Auto Account Creation** and **Auto Account Update** check boxes.

5. Select **Save**.

**Important:** For Cisco Jabber to work with Cisco WebEx Messenger Instant Messenger and Presence and deliver on-premise Cisco Unified Call Manager (CUCM) and Unity connection, you must provide the UC details for CUCM and connections in the WebEx Messenger administrator portal.

To use SSO in Cisco WebEx Messenger and Cisco WebEx Meeting Center, ensure loose integration is enabled for both.

See *Cisco Unified Communications Integration with Cisco WebEx* and *Provision Loosely Coupled Integration* in the *Cisco WebEx Messenger Administration Guide*. 
Migration from WebEx Messenger to Common Identity SSO Authentication

Request to Add Domain to Common Identity

Contact your Customer Success Manager (CSM) or Universal Agent (UA) to submit an ops request to add the domain to CI or email: ci-messenger-sync@cisco.com.

Create a Password in CI

As none of the users migrated from Cisco WebEx Messenger have a password, you must create a password for an existing administrator now.

1. Connect to https://web.ciscospark.com and enter the email address of the administrator.
2. Select Next.
3. Select Can't access your account?.

An email is automatically sent to that user asking them to reset their password.

Note: Any administrators in Cisco WebEx Messenger that are migrated to CI will remain administrators in CI.

Configure SSO in Cloud Collaboration Management

1. Connect to https://admin.ciscospark.com using the email address and password that you previously reset.
2. Select Users in the left navigation bar to display all the users from the Cisco WebEx Messenger organization.
3. From the top navigation bar, select Service Setup > Enterprise Settings to download the CI metadata to configure ADFS.

4. In the Enterprise Settings window, select Integrate a 3rd-party identity provider (Advanced).

5. Select Next.


**Create a Relying Party Trust for CI**

1. Go to your Active Directory Federation Services (ADFS) server.

2. In the Actions dialog box, select Add Relying Party Trust Select Import data about the relying party from a file.

3. Select Browse to navigate to and select the metadata file downloaded from CI previously.

4. Select Next.

5. Enter the display name for the SAML agreement.

6. Select Next.

7. Select the I do not want to configure multi-factor authentication settings for the relying party trust at this time radio button.

8. Select Next.

9. Select the Open the Edit Claim Rules dialog for the relying party trust when the wizard closes check box.

10. Select Close.

**Add Claim Rules for CI**

1. In the Edit Claim Rules for Messenger dialog box, select Add Rule.

2. In the Add Transform Claim Rule Wizard from the Claim rule template drop-down, select the Send LDAP Attributes as Claims template.

3. Select Next.

4. Enter the claim name and select two attributes, mail and uid, to be passed to CI and mapped to the user’s email address.
5. Add a second claim rule using the **Send Claim Using a Custom Rule** template.

6. Add the following test to the custom rule. The yellow highlighted text is the FQDN or your ADFS 3.0 server and the green highlighted text is the CI entityID from the metadata file downloaded from Cloud Collaboration Management.


7. The claim should now look like this:
1. Go to https://<FQDN> in your Active Directory Federation Services (ADFS) server.

2. Download the file /FederationMetadata/2007-06/FederationMetadata.xml.

3. Use an XML editor to remove the elements not required in CI.

   **Note:** There are several XML editors available online but we recommend Code Beautify http://codebeautify.org/xmlviewer.

4. In the XML editor, browse to the metadata file in ADFS.

5. Select **Beautify** to delete the elements 3,4,5, and 6. Make sure the idpssodescriptor and the contact person tags remain in the file.
15

6. Select **Download** to download the edited file.

7. The metadata file should look like this:

![XML Viewer](image)

```
<?xml version="1.0"?>
<ds:KeyInfo>
  <ds:KeyDescriptor>
  </ds:KeyDescriptor>
</ds:KeyInfo>
```

**Complete SSO Configuration in Cloud Collaboration Management**

1. Connect to [https://admin.ciscospark.com](https://admin.ciscospark.com) using the email address and password that you previously reset.

2. From the top navigation bar, select **Service Setup > Enterprise Settings** to download the CI metadata to configure ADFS.
3. In the **Enterprise Settings** window, select **Integrate a 3rd-party identity provider (Advanced)**.

4. Select **Next**.

5. Select **Import** to browse to and import the edited metatadata file. A success message is displayed when the import of the metadata file is complete.

6. Select **Next**.

7. Select **Test SSO Configuration**.

8. Sign in with the administrator details.

**Troubleshooting**

If you try to use SSO to login now, it will fail and you will see an error message. Using Firefox SAML tracer, you can see that AuthInstant is defined before NotBefore timer for that assertion. This makes it invalid.

To fix this issue you need to configure the ADFS Identity Provider (IdP) engine to define the AuthInstant assertion later.
To solve this problem, do the following:

1. In the ADFS server, execute the power shell command Set-ADFSRelyingPartyTrust -TargetIdentifier "https://idbroker.webex.com/8538f9ff-4f12-440a-9880-3488bc3eb146" -NotBeforeSkew 5.

2. The TargetIdentifier must be the EntityID from metadata file downloaded from CI.

3. Perform the configuration test in Cloud Collaboration Management again and it should be successful.

**Redirect Authentication**

- Before you can verify the Jabber authentication in CI, authentication must be redirected from the WebEx Messenger platform to the CI platform. To do this contact the CSM to update the existing ops request or submit a new ops request or email: ci-messenger-sync@cisco.com.
Verification of Cisco Jabber Authentication in CI

1. Start Cisco Jabber.
2. Verify that all the on-premise are still using SSO.
3. Verify that WebEx Meeting Center is enabled for loose Integration.
4. Finally, verify that Cisco Jabber logs contain the string `idbroker.webex.com`, indicating that it is connecting to CI.

```
2015-06-05 09:34:31.893 DEBUG [0x000016e4] [services\impl\TransportHttpClient.cpp(87)]
[csfunified.telemetry.TransportHttpClient]
2015-06-05 09:34:31.893 DEBUG [0x000016e4] [sf-netutils\src\common\PolicySet.cpp(84)]
[csf.common.PolicySet] [csf::common::PolicySet::getPolicy] - Successfully found Policy with nature EDGE_USAGE [NEVER_USE]
2015-06-05 09:34:31.893 DEBUG [0x000016e4] [ls\src\http\BasicHttpClientImpl.cpp(253)]
[csf.httpclient] [csf::http::BasicHttpClientImpl::execute] - Edge policy enforced successfully with transformed Url: https://idbroker.webex.com/idb/oauth2/v1/access_token for request #1
2015-06-05 09:34:31.893 DEBUG [0x000016e4] [etutils\src\http\HttpRequestData.cpp(71)]
[csf.httpclient] [csf::http::HttpRequestData::consumeEasyCURLConnection] - Acquired lock (_easyCurlConnectionMutex)
2015-06-05 09:34:31.893 DEBUG [0x000016e4] [etutils\src\http\HttpRequestData.cpp(80)]
[csf.httpclient] [csf::http::HttpRequestData::consumeEasyCURLConnection] - Releasing lock (_easyCurlConnectionMutex)
```
2015-06-05 09:34:31,894 INFO [0x000016e4] [etutils\src\http\CurlHttpUtils.cpp(1015)]
[csf.httpclient] [csf::http::CurlHttpUtils::configureEasyRequest] - "-----" Configuring request
#1 POST https://idbroker.webex.com/idb/oauth2/v1/access_token