QUICK START GUIDE FOR CISCO UNITY CONNECTION

SAML SSO Access- Release 10.0 (1) and Later

Revised December, 2018

1 Introduction

Cisco Unity Connection supports the single sign-on feature that allows users to log in once and gain access to Unity Connection web applications, such as Cisco Unity Connection Administration and Cisco Personal Communications Assistant. With Unity Connection 10.0(1), an enhancement to the sign-on feature, SAML SSO, is introduced that allows a user to gain single sign-on access with Unity Connection subscriber web interfaces and across the administrative web applications on the following Unified Communication products:

- Unity Connection
- Cisco Unified Communications Manager
- Cisco Unified IM/Presence

The SAML SSO feature is based on open industry standard protocol SAML (Security Assertion Markup Language). For more information on SAML protocol, see the **Understanding SAML Protocol, page 3** section.

Note Single Sign-On (both OpenAM and SAML) can now be enabled using only graphical user interface (GUI) as enabling the features through command line interface (CLI) is no longer supported.

SAML SSO supports both LDAP and non-LDAP users to gain single sign-on access. LDAP users are the users integrated to Active Directory. Non-LDAP users are the users that reside locally on Unity Connection server.

- The **LDAP** user are allowed to login with a username and password that authenticates on Identity Provider. For more information on Identity Provider, see the **Understanding Service Provider and Identity Provider, page 2** section.
- The **non-LDAP** users with administrator rights login to Cisco Unity Connection Administration using Recovery URL. Recovery URL provides alternate access to the administrative and serviceability web applications via username and password. A non-LDAP user can access the following web applications on Unity Connection using Recovery URL:
  - Unity Connection Administration
  - Cisco Unity Connection Serviceability
  - Cisco Unified Serviceability

Note The LDAP or non-LDAP users of Unity Connection do not gain single sign-on access to Disaster Recovery System or Cisco Unified Operating System Administration using SAML SSO.

2 Understanding Service Provider and Identity Provider

Updated December, 2018

Service Provider (**SP**) is a protected entity on Unity Connection that provides the web applications. A Service Provider relies on a trusted Identity Provider (IdP) or Security Token Service (STS) for authentication and authorization.

Identity Provider is an online service or website that authenticates users by means of security tokens. It authenticates the end user and returns a SAML Assertion. SAML Assertion shows either a **Yes** (authenticated) or **No** (authentication failed) response.

A user must authenticate his or her user credentials on Identity Provider to gain access to the requested web application. If the authentication gets rejected at any point, the user will not gain access to any of the requested web applications. If the authentication is accepted, then the user is allowed to gain single sign-on access to the requested web application.

For information on the currently supported Identity Providers, see SAML-Based SSO Solution chapter of *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

The definitions of Service Provider and Identity Provider further help to understand the SAML protocol mechanism.

3 Understanding SAML Protocol

Security Assertion Markup Language (SAML) is an XML based open standard data format for exchanging data. It is an authentication protocol used by Service Providers to authenticate a user. The security authentication information is passed between an Identity Provider and Service Provider.

SAML is an open standard that enables clients to authenticate against any SAML enabled Collaboration (or Unified Communication) service regardless of the client platform.

All Cisco Unified Communication web interfaces (e.g. CUCM or Unity Connection) use SAML 2.0 protocol in SAML SSO feature. To authenticate the LDAP user, Unity Connection delegates an authentication request to the Identity Provider. This authentication request generated by the Unity Connection is SAML Request.

The Identity Provider authenticates and returns a SAML Assertion. SAML Assertion shows either **Yes** (authenticated) or **No** (authentication failed).

Single SAML SSO mechanism:

SAML 2.0 protocol is a building block that helps to enable single sign-on access across collaboration services and also helps to enable federation between collaboration services and customer's Identity Provider.

Once SSO has been enabled on Unity Connection server, a .xml file named, **SPMetadata<hostname of Unity Connection>.xml** is generated by Unity Connection that acts as a Service Provider metadata. The SAML SP metadata must be exported from SAML Service Provider (on Unity Connection) and then import it to Identity Provider (ADFS).

The administrator must export SAML metadata from Cisco Unity Connection Administration and import that metadata on Identity Provider. The administrator must also export SAML metadata from Identity Provider and import that metadata on Cisco Unity Connection Administration. This is a two way handshake process between the Service Provider (that resides on Unity Connection) and Identity Provider that is essential for SAML Authentication.

The SAML metadata contains the following information:

- URL information for Identity Provider and Service Provider.
- Service Provider Assertion Consumer Service (ACS) URLs that instructs Identity Provider where to POST assertions.
- Certificate information for Identity Provider and Service Provider.

The exchange of SAML metadata builds a trust relationship between Identity Provider and Service Provider. Identity Provider issues SAML assertion and Identity Provider digitally signs it. On receiving the SAML assertion, Service Provider validates the assertion, using Identity Provider certificate information that guarantees that assertion was issued by Identity Provider.

When single sign-on login fails (e.g. If Identity Provider or Active Directory is inactive), Recovery URL provides alternate access to administrative and serviceability web applications via username and password.

4 Prerequisites for Enabling SAML SSO

To configure the SAML SSO feature, you must ensure the following requirements to be in place:

- Unity Connection 10.0(1) and later release on both the servers in the cluster.
- Install Identity Provider on Microsoft Windows 2008 with SP2 platform. You must configure Identity Provider on the same domain as Unity Connection server.
- Make sure that the clocks on Unity Connection and Identity Provider (chosen for SAML SSO) synchronize with each other.
- When enabling SSO mode from Cisco Unity Connection Administration, make sure you have at least one LDAP user with administrator rights in Unity Connection to **Run SSO Test** for SAML SSO.
- Assign the system administrator role to the user accounts to allow them to access Unity Connection administrative and serviceability web applications.

Once the above requirements are met, the Unity Connection server is ready to be configured for SAML SSO feature.

5 Configuring SAML SSO in Unity Connection

This section outlines the key steps and/or instructions that must be followed for Unity Connection specific configuration. However, if you are configuring SAML SSO feature for the first time, it is strongly recommended to follow the detailed instructions given below:

Configuring Identity Provider

You must configure one of the following Identity Providers before configuring SAML SSO in Unity Connection:

Configuring ADFS Server

If you select ADFS as the Identity Provider for SAML SSO:

Step 1 Download the ADFS 2.0 and install it after accepting the license. Select **FINISH** when the installation is complete.

Step 2 From **Administrative Tools**, select the **ADFS 2.0 Management** menu to launch the ADFS configuration wizard. Select the **ADFS 2.0 Federation Server Configuration Wizard Link** from the **ADFS Management** console.

Step 3 Run the **ADFS 2.0 Federation Server Configuration Wizard** and select **Next**. This creates a new Federation Service.

Step 4 Select **Standalone Federation Server** and select **Next**. Select your SSL certificate and the default **Federation Service Name**. Select **Next** and select **Close**.

Note Make sure that the SSL certificate is signed by a provider, such as Thawte or Verisign.

Step 5 Select **Required: Add a trusted relying party** and select **Start**. If you have a URL or file containing the configuration use this option otherwise select **Enter data about the relying party manually** and then select **Next**.

Step 6 Enter a **Display Name** and then select **Next**. Select **ADFS 2.0** profile and then select **Next**. Select **Browse** and select the same certificate you used earlier and then select **Next**.

Step 7 Select **Enable support for SAML 2.0 WebSSO protocol** and then enter the URL to the service providing the integration. Select **Next** and enter the Relying party trust identifier. Select **Add** and then select **Next**.

Step 8 Select **Next**. This permits all users to access this relying party. You may change this settings later after the testing is completed. Select **Next** and select **Close.**

Step 9 This opens the **Edit Claim Rules** dialog for the relying party trust. Select **Add Rule** and select **Next.** The **Send LDAP Attributes as Claims** dialog is automatically selected.

Step 10 Enter a claim rule name and then select **Active Directory** under Attribute store. Select an LDAP Attribute and a corresponding **Outgoing Claim Type**. Select **Finish** and select **OK**.

Step 11 In addition to the above configuration, ensure the following points:

- Launch **ADFS 2.0** from programs menu and select **Add Relying Party Trust**.
- Select **Start** button and select **Import data** option about the relying party from a file. Select **Fedlet metadata file** from a desktop which you downloaded either from Cisco Unified CM or using REST API. Select **Next**.
- Enter **Display Name** and select **Next**. Select **Permit all users to access this relying party** and select **Next**.
- Review the settings and select **Next**. Select **Close** and ensure that the **Add Claim Rules** check box is checked.
- Select **Add Rule**. Enter the claim rule name and select the **Attribute Store**.The syntax for the **Name ID** claim rule is:

"c:[Type=="http://schemas.microsoft.com/ws/2008/06/identity/claims/windows account name"]=> issue(Type= "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer= c.Issuer, Originallssuer= c.Originallssuer, Value= c.Value, ValueType=c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]="urn:oasis:names:tc:SAML:2.0:nameid-format: transient", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]="http:// <FQDN of ADFS server>/adfs/com/adfs/service/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]="<FQDN of Unity Connection server>");"

Note A default **Name ID** claim rule is necessary to configure ADFS to support SAML SSO. A default **Name ID** claim rule is necessary to configure ADFS to support SAML SSO.

- Select **Next** with default claim rule template. On **Send LDAP Attributes as Claims In Configure Rule**, enter the **Claim Rule** name and select **Attribute store** as Active Directory. Configure **LDAP Attribute** and **Outgoing Claim Types**. Select **Finish** and **Apply** followed by **OK**.

Configuring OpenAM

If you select OpenAM Server as the Identity Provider for SAML SSO:

Step 1 To configure policies on OpenAM server, you must log in to OpenAM and select the **Access Control** tab. Click the **Top Level Realm** option, select the Policies tab, and then create a new policy. Follow the steps as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462, for creating a new policy. While following the instructions given in the white paper, make sure to create policies with the below mentioned Unity Connection-specific information:

- Ensure the following points while adding rules to the policy:
  - Each rule should be of the URL Policy Agent service type.
  - Make sure to check the **GET** and **POST** check box for each rule.
  - Create a rule for each of the following resources, where 'fqdn' is the fully qualified domain name of your Unity Connection server:

  https://<fqdn>:8443/*

  https://<fqdn>:8443/*?*

  https://<fqdn>/*

  https://<fqdn>/*?*

  http://<fqdn>/*

  http://<fqdn>/*?*
- Ensure the following points while adding a subject to the policy:
  - Make sure that the **Subject Type** field is **Authenticated Users**.
  - Specify a subject name.

  Do not check the **Exclusive** check box.
- Ensure the following points while adding a condition to the policy:
  - Mention the **Condition** type as **Active Session Time** and specify a condition name.
  - Configure active session timeout as 120 minutes and select **No** for the **Terminate Session** option.

Step 2 Configure a Windows Desktop SSO login module instance. Follow the instructions for configuring Windows Desktop as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462.

Step 3 Configure a J2EE Agent Profile for Policy Agent 3.0. Follow the instructions to create a new J2EE agent as given in the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462 with the below mentioned Unity Connection-specific settings:

- The name mentioned as agent profile name is the name that you need to enter when enabling SSO on the Unity Connection server, when it prompts as: "**Enter the name of the profile configured for this policy agent**."
- The agent password entered here is the password that is entered on the Unity Connection server when it prompts as: "**Enter the password of the profile name**."
- Make sure to add the following URIs to the **Login Form URI** section on the Application tab:

  –/cuadmin/WEB-INF/pages/logon.jsp

  –/cuservice/WEB-INF/pages/logon.jsp

  –/ciscopca/WEB-INF/pages/logon.jsp

  –/inbox/WEB-INF/pages/logon.jsp

  –/ccmservice/WEB-INF/pages/logon.jsp

  –/vmrest/WEB-INF/pages/logon.jsp
- Under the Application tab, add the following URI in the **Not Enforced URI Processing** session:
  –/inbox/gadgets/msg/msg-gadget.xml

In addition to above Unity Connection-specific configuration, ensure the following points:

- Import users from LDAP to Unity Connection. Users must be configured with the appropriate roles to log in to Cisco Unity Connection Administration, or Cisco Unity Connection Serviceability.
- Upload the OpenAM certificate into Unity Connection as described in the *Configuring SSO on Cisco Unified Communications Manager 8.6* section of the Cisco white paper, https://supportforums.cisco.com/docs/DOC-14462.

Configuring Ping Federate Server

If you select Ping Federate Server as the Identity Provider for SAML SSO:

Step 1 Install JDK. Download JDK from the given location: www.oracle.com/technetwork/java/javase/downloads.

Step 2 Set the JAVA_HOME environment variable to the JDK installation directory path and add the /bin directory to the PATH variable for your platform.

MyComputer> Properties> Advanced> Environment variables> Path.

C:\WINDOWS\java;C:\Program Files\Java\jdk1.7.0_21\bin

Step 3 Download Ping federate.zip file and lic file.

Step 4 Unzip the Ping Federate file.

Step 5 Save the license key file in the directory:

<pf_install>/pingfederate/server/default/conf

Step 6 sRun the Ping Federate as service.

run install-service.bat from the directory:

<pf_install>\pingfederate\sbin\win-x86-32

Step 7 Access the PingFederate administrative console:

https://<IP >:9999/pingfederate/app

Step 8 Login to Ping Federate.

Username: Administrator

Password: 2Federate

Step 9 Change your password on the **Change Password** screen and select **Save**.

Step 10 Configure server. Browse to **Welcome** page and select **Next.**

Step 11 Accept the lic file and select **Next.**

Step 12 Select **Single-user Administration** and select **Next.**

Step 13 Add System Info details as below and select **Next.**

Step 14 Select **Next** on **Runtime Notifications.**

Step 15 Select **Next** on **Runtime Reporting.**

Step 16 Enable Account Management details as below:

- Select Roles and Protocols.
- Provide the **Base URL** and **Realm**. Base URL is the IP address of Ping Federate server.

Select **Next**. Select **Save** on Summary page.

Configuring SP Connection

Step 1 Select **Create New under SP Connections** and select **Next.** Select the **Browser SSO** option and select **Next.**

Step 2 Browse sp.xml file and select **Next.**

Note sp.xml file is downloaded from Cisco Unified CM

Step 3 After importing the sp.xml file successfully, select **Next.**

Step 4 Configure Base URL as **https://<server name>:8443**. Select **Next.**

Step 5 Select **Configure Browser SSO** and select **Next.**

Step 6 Select **SP-Initiated SSO**. Select **Next.** Specify the **Assertion Lifetime** and select **Next**.

Step 7 Select **Assertion Creation.** Select **Transient** and make sure Include attributes in addition to the transient identifier check box is checked.

Step 8 Select snap shot details under **Attribute Contract.**

Step 9 Select **Map New Adapter Instance.** Select **Next.**

Step 10 Select **LDAP** under **Adapter Instance.** Select **Next.**

Configuring Oracle Identity Provider Server

If you select Oracle Identity Provider Server as the Identity Provider for SAML SSO:

Step 1 Login to Oracle Enterprise Manager where Oracle Identity Federation has been installed as a component.

Step 2 Under **Identity and Access** in the drop down, select **Oracle Identity Federation.**

Step 3 Under **Oracle Identity Federation** drop down, select **Federations.**

Step 4 Select **Federations.** In the **Federations** window, select **Add New Federations.** In this case the Metadata file is imported from Cisco Unified CM. After the Metadata has been loaded, the Cisco Unified CM hostname is displayed under **Federations.**

Step 5 Select the Cisco Unified CM node and select **Edit.** From **Edit,** select **Attribute Mappings and Filters.** Check the **Enable Attributes in Single Sign-On (SSO)** check box.

Step 6 Check the following check boxes:

a. **Unspecified**

b. **Email Address**

c. **Persistent Identifier**

d. **Transient/One-Time Identifier**

Apply the above changes with the **Apply** button on the window and then select **Attribute Mappings and Filters** that opens up a new window.

Step 7 Under **Name Mappings**, select **Add** to add new attributes, **"User Attribute Name"** uid and **"Assertion Attribute Name"** uid. The **Send with SSO Assertion** check box should be checked.

Step 8 Another attribute to be added as email are **"User Attribute Name"** mail and **"Assertion Attribute Name"** email. The **"Send with SSO Assertion"** check box should be checked.

Step 9 Select **OK** and exit out after saving the configuration.

Generating and Importing Metadata into Cisco Unified CM

Navigate to Oracle Identity Federation drop down, select **Administration** and select **Security and Trust**.

1. From the Security and Trust Window, generate Metadata xml with the option Provider Type as Identity Provider and Protocol as SAML 2.0.
2. Import the Metadata into the CUCM.

Configuring SAML SSO in Unity Connection

To configure SAML SSO feature on Unity Connection server, you must perform the following steps:

Step 1 Sign in to Cisco Unity Connection Administration and select **System Settings**.

Note The cluster status is not affected while enabling or disabling the SAML SSO feature. SAML SSO cannot be enabled from publisher server if subscriber server is inactive or vice versa. SAML SSO cannot be enabled from publisher server if subscriber server is inactive or vice versa.

Step 2 Select **SAML Single Sign-On** and select the **Enable SAML SSO** option. When you select this option, a wizard opens as **Web server connections will be restarted**, select **Continue**.

Note When enabling SAML SSO from Unity Connection, make sure you have at least one Unity Connection LDAP user with administrator right.

Step 3 To initiate the IdP Metadata import, navigate to **Identity Provider (IdP) Metadata Trust File** and select the **Browse to upload the IdP metadata** option from your system. Then select the **Import IdP Metadata** option. Follow the link below to download IdP metadata trust file for ADFS:

https://localhost/FederationMetadata/2007-06/FederationMetadata.xml

Step 4 If the import of metadata is successful, a success message **Import succeeded for all servers** appears on the screen. Select **Next** to continue the wizard.

Step 5 For SAML metadata exchange, select the **Download Trust Metadata Fileset** option.

Caution If the Trust Metadata has not been imported then a warning message prompts on the screen as **The server metadata file must be installed on the IdP before this test is run.**

Select **Next** and a window appears for valid administrator IDs that automatically populates the LDAP user with administrator rights into that window. If you find the LDAP user with administrator rights automatically populated in the above window, then select **Run Test** to continue.

Step 6 The wizard continues and a window appears for user login to IdP. Enter the credentials for the LDAP user with administrator role that was automatically populated in the previous window.

This enables the SAML SSO feature completely. Select **Finish** to complete the configuration wizard.

Note After enabling/disabling SAML SSO on Unity Connection, a user must wait for approximately (2-3 minutes) to get the web applications initialized properly and then the Tomcat service needs to be restarted from Cisco Unity Connection Serviceability page or using the CLI command **utils service restart Cisco Tomcat.**

6 Access to Web Applications in Unity Connection Using SAML SSO

SAML SSO allows a LDAP user to login to client applications using username and password that authenticates on Identity Provider. A user sign-in to any of the supported web applications on Unified Communication products (after enabling the SAML SSO feature) also gains access to the following web applications on Unity Connection (apart from Cisco Unified Communications Manager and Cisco Unified CM IM/Presence):

Unity Connection users	Web applications
LDAP users with administrator rights	• Unity Unity Connection Administration • Cisco Unity Connection Serviceability • Cisco Unified Serviceability • Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox(desktop version)
LDAP users without administrator rights	• Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox(desktop version)

Note To access Web Inbox and Mini Web Inbox, you must have a user with mailbox. Also navigate to **Unity Connection Administration> Class of Service> Licensed features** and make sure that **Allow Users to Use the Web Inbox, Messaging Inbox and RSS Feeds** check box is checked.

The non-LDAP users with administrator role can login to Cisco Unity Connection Administration using Recovery URL. The **Recovery URL** option is present in Unity Connection product deployment selection window just below the **Cisco Unity Connection** option. When SSO login fails (if Identity Provider or Active Directory is inactive), Recovery URL provides alternate access to the administrative and serviceability web applications via username and password.

7 Running CLI Commands in Unity Connection

SAML SSO feature introduced the following commands in addition to the above three commands:

- utils sso enable
- utils sso disable
- utils sso status
- utils sso recovery-url enable
- utils sso recovery-url disable
- set samltrace level <trace level>
- show samltrace level

- **utils sso enable**

This command when executed returns an informational text message that prompts that the administrator can enable SSO feature only from graphical user interface (GUI). Both OpenAM SSO and SAML SSO cannot be enabled from CLI interface.

- **utils sso disable**

This command disables (both OpenAM based or SAML based) SSO mode. Within a cluster, the command needs to be executed on both the nodes. You may also disable the SSO from graphical user interface (GUI) by selecting the **Disable** option under the specific SSO mode.

Note When SSO is disabled from graphical user interface (GUI) of Unity Connection, it disables the SSO mode on both nodes in case of cluster.

- **utils sso status**

This command shows the SSO status, enabled or disabled, on each node. This command is executed on each node individually.

- **utils sso recovery-url enable**

This command enables the Recovery URL SSO mode. It also verifies that this URL is working successfully. Within a cluster, the command needs to be executed on both the nodes.

- **utils sso recovery-url disable**

This command disables the Recovery URL SSO mode on that Connection node.

- **set samltrace level <trace-level>**

This command enables the specified traces to locate the following information:

  - error
  - warning
  - debug
  - fatal
  - info

- **show samltrace level**

This command displays the logs selected for SAML SSO.

8 Troubleshooting SAML SSO in Unity Connection

SAML SSO allows a user to have single sign-on access to web applications until a web browser is active. Ensure that you have taken care of all the requirements and checklist while enabling the SAML SSO mode. However, for any SAML SSO related issues, see *Troubleshooting Guide for Cisco Unity Connection Release 10.x*, available at

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/10xcuctsg208.html.