Managing Security Assertion Markup Language Single Sign-On (SAML SSO) in Cisco Unity Connection 10.x

See the following sections:

- Overview of SAML SSO in Cisco Unity Connection
- System Requirements for SAML SSO
- Configuring SAML SSO

Overview of SAML SSO in Cisco Unity Connection

Cisco Unity Connection 10.0(1) and later release introduces an enhanced signed in feature using open industry standard protocol SAML (Security Assertion Markup Language) referred to as SAML SSO. SAML SSO 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:

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

SAML SSO uses Identity Provider (LDAP based) to provide single sign-on access to client applications.

For more information on access to web applications on Unity Connection using SAML SSO, see Access to Unity Connection web applications using SAML SSO

Note With Cisco Unity Connection10.0(1), PAWS APIs are supported with SAML single sign-on access. Cisco Unity Connection Rest APIs are not supported using SAML SSO.

Cisco Unity Connection supports SAML 2.0 protocol for the SAML SSO feature.

SAML SSO allows the LDAP user to login with a username and password that authenticates on Identity Provider. **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. Currently, the supported Identity Providers are:

- ADFS (Active Directory Federated Services) version 2.0
- Ping Federate version 6.10.0.4
- Oracle Identity Provider version 11.0
- OpenAM version 10.1

Note Only one Identity Provider is deployed at one time as Identity Provider cluster is not supported with SAML SSO.

The non-LDAP users with administrator rights login to Cisco Unity Connection Administration using Recovery URL. The Recovery URL option is present in Unity Connection product landing page just below the Cisco Unity Connection option. When SSO login fails(e.g. If Identity Provider or Active directory is inactive), 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:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability

Note LDAP users are the users that are integrated to Active Directory. Non-LDAP users are the users that reside locally on Unity Connection server.

Access to Unity Connection web applications using SAML SSO

A user signed into 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 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 the **Allow Users to Use the Web Inbox, Messaging Inbox and RSS Feeds** check box is checked.

The users (LDAP or non-LDAP) do not gain access to the following web applications using SAML SSO:

- Disaster Recovery System
- Cisco Unified Operating System Administration

System Requirements for SAML SSO

The following Security Assertion Markup Language single sign-on requirements exist for Cisco Unity Connection:

- Cisco Unity Connection release 10.0(1) or later release on both the servers in case of cluster.

The feature requires the following third-party applications for configuring the SAML SSO feature:

- Microsoft Windows Server 2008 R2 Server / Windows Server 2012 Installation Media.
- Microsoft Active Directory server.
- Any of the following supported Identity Provider servers:
  - Active Directory Federated Service (ADFS) 2.0 Federation Server
  - OpenAM 10.1
  - Ping Federate 6.10.0.4
  - Oracle Identity Manager Server 11.0
- Self Signed Certificate (SSL) for Internet Information Services (IIS) Manager 7.0 and later.

The SAML SSO feature on Cisco Unity Connection uses Identity Provider (LDAP based) simultaneously to provide single sign-on access to many web applications on the Unity Connection server.

The third party applications required for the SAML SSO feature must meet the following configuration requirements:

- In case of Active directory, it must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The Identity Provider must be accessible by hostname on the network to Connection server, all client systems and the Active directory server.
- The clocks of all the entities participating in SAML SSO must be synchronized.

Note SAML SSO or single sign-on feature cannot be enabled on tenant partitions.

See the third party documentation for more information about these products.

Configuring SAML SSO

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 SAML SSO in Cisco Unity Connection
- Running CLI commands for SAML SSO

Configuring SAML SSO in Cisco Unity Connection

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

Step 1 To enable SAML SSO on Unity Connection server, log on to the Unity Connection Administrationon publisher server (with primary role) in caseof cluster.

Note The cluster status should not be 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.

Navigate to System settings>SAML Single Sign-On> select the option Enable SAML SSO. When you select **SAML SSO** option, a wizard opens as **Web server connections will be restarted**, select **Continue**.

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

Step 2 To initiate the IdP Metadata import, navigate to Identity Provider (IdP) Metadata Trust File, select the option Browse to upload the IdP metadata from your system. Then select the option Import IdP Metadata. Follow the link below to download IdP metadata trust file for ADFS:

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

Step 3 If the import of metadata is successful, a success message appears Import succeeded for all servers. Then select Next to continue the wizard.

Step 4 For SAML metadata exchange, select the option **Download Trust Metadata Fileset**.

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.

Then select **Next**. 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 5 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**.

Running CLI commands for SAML SSO

The following section describes the CLI commands for SAML single sign-on. All the commands are valid for cluster and stand- alone nodes as well:

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

- **utils sso disable**

This command disables both (OpenAM SSO or SAML SSO) based authentication. This command lists the web applications for which SSO is enabled. Enter Yes when prompted to disable SSO for the specified application. You must run this command on both the nodes if in a cluster. SSO can also be disabled from graphical user interfce (GUI) by selecting Disable button, under specific SSO in Cisco Unity Connection Administration.

Command Syntax

utils sso disable

- **utils sso status**

This command displays the status and configuration parameters of SAML SSO. It helps to verify the SSO status, enabled or disabled, on each node individually.

Command Syntax

utils sso status

- **utils sso enable**

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

Command Syntax

utils sso enable

- **utils sso recovery-url enable**

This command enables the Recovery URL SSO mode. It also verifies that this URL is working successfully. You must run this command on both the nodes if in a cluster.

Command Syntax

utils sso recovery-url enable

- **utils sso recovery-url disable**

This command disables the Recovery URL SSO mode on that node. You must run this command on both the nodes if in a cluster.

Command syntax

utils sso recovery-url disable

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

This command enables the specfic traces and trace-levels that can locate any error, debug, information, warning or fatal. You must run this command on both the nodes if in a cluster.

Command syntax

set samltrace level <trace-level>

- **show samltrace level**

This command displays the log level set for SAML SSO. You must run this command on both the nodes if in a cluster.

Command syntax

show samltrace level