QUICK START GUIDE FOR CISCO UNITY CONNECTION

SAML SSO access- Release 10.0 (1) and Later

Published November, 2013

1 Introduction

In Cisco Unity Connection 10.0(1) and later release, an enhanced signed in feature has been introduced using open industry standard protocol SAML (Security Assertion Markup Language). (SAML supports multiple binding protocols that works for HTTP Redirect binding and HTTP POST binding). Cisco Unity Connection 10.0(1) and later release supports both SAML single sign-on and OpenAM single sign-on but only one SSO feature can be enabled at a time.

Note A SAML binding is a mapping of a SAML protocol message onto standard messaging formats and communication protocols. e.g. HTTP Redirect binding and HTTP POST binding.

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

SAML SSO allows the LDAP user to login with a username and password that authenticates on Identity Provider. For more information on Identity Provider, see:

Understanding Service Provider and Identity Provider *chapter in Quick start guide.*

For more information on SAML protocol, see:

Understanding SAML protocol *chapter in Quick start guide.*

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

The Unity Connection (LDAP or non-LDAP) users donot gain single sign-on access to the following Unity Connection web applications using SAML SSO:

- Disaster Recovery System
- Cisco Unified Operating System Administration

For more information on the single sign-on access to web applications, see the section:

Access to web application pages in Cisco Unity Connection10.x using SAML SSO

The Unity Connection users use SAML SSO to gain single sign-on access to web applications on Unified Communication. SAML SSO allows the users to login once and gain access to the web applications.

To enable SAML SSO feature in Cisco Unity Connection, we need to meet some prerequisites and follow the configuration steps.

For more information on prerequisites for configuring SAML SSO, see the section:

Prerequisites for enabling SAML SSO in Unity Connection 10.0(1) and later

For more information on configuring SAML SSO, see the section:

Configuring Cisco Unity Connection 10.x for SAML SSO feature

The SAML SSO feature is enabled only from Cisco Unity Connection Administration. However, we may check the SSO status or disable SSO from CLI interface with a set of commands.

For more information on CLI commands for SAML SSO, see the section:

SAML SSO commands in Cisco Unity Connection

For more information on troubleshooting SAML SSO, see the section:

Troubleshooting SAML SSO in Cisco Unity Connection

2 Understanding Service Provider and Identity Provider

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 more information on SAML SSO mechanism, see

Understanding SAML protocol section in Quick start guide.

Currently, the supported Identity Providers are:

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

The above 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 Cisco Unity Connection server, a .xml file named, **SPMetadata<hostname of Unity Connection>.xml** is generated by Cisco 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.

4 Need for single sign-on (SSO) access to Unity Connection web applications

Cisco Unity Connection 8.6(2) and later release provides single sign-on (SSO) access to web applications to users using OpenAM based single sign-on. Single Sign-On (SSO) access in Cisco Unity Connection allows end users to log in once to Cisco Unity Connection Administration and also gain access to following Cisco Unity Connection applications without signing in again:

- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability
- Cisco Personal Communications Assistant
- Web Inbox

In Unity connection 8.6(2) and earlier releases, single sign-on access (SSO) used OpenAM and Active directory simultaneously to provide single sign-on access to web applications.

For more information on SSO, see Single Sign-On in Cisco Unity Connection chapter in security guide:

http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsec061.html

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.

The main advantage of SAML SSO is that it allows a user to gain single sign-on access across the web applications on the following Unified Communication products:

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

For more information on web applications accessed by a user using SAML SSO, see:

Access to web application pages in Cisco Unity Connection10.x using SAML SSO *section in Quick start guide.*

SAML SSO allows a LDAP user to login with a username and password that authenticates on Identity Provider. The non-LDAP users with administrator rights can login to Cisco Unity Connection Administration using Recovery URL. When SSO 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.

5 Prerequisites for enabling SAML SSO in Unity Connection 10.0(1) and later

To configure Cisco Unity Connection 10.x for SAML SSO feature, you must ensure the following requirements to be in place

- Cisco Unity Connection 10.0(1) and later release on both the servers in the cluster.
- Install Identity Provider on Micorosoft 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 atleast 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 Cisco Unity Connection server is ready to be configured for SAML SSO feature, that is explained in the next sub section.

6 Configuring Cisco Unity Connection 10.x for SAML SSO feature

The Cisco Unity Connection and the Identity Provider must be configured properly to support SAML SSO feature. This section describes the configuration steps on Unity Connection server for SAML SSO:

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 Cisco Unity Connection interface.

Browser 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 the next step of the wizard by selecting **Identity Provider (IdP) Metadata Trust File.** Then select the option **Browse** to upload the IdP metadata from your system. Then select the option **Import IdP Metadata.**

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

Step 3: 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 4: 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.

There is one more method of SAML SSO access to web applications through **Recovery URL**. The Recovery URL points to /ssosp/login. When a non-LDAP user with administrator rights selects the Recovery URL option on product landing page, he actually selects the /ssosp/login URL that sends a request to SSO Service Provider (SSOSP). If Recovery URL option is disabled, the new filter introduced at ssosp for intercepting /ssosp/login URL, redirects the request to Identity provider but if Recovery URL option is enabled, the new filter created redirects the request to /cuadmin/recoveryurl.do.

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**.

7 Access to web application pages in Cisco Unity Connection10.x 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 Directoryis inactive), Recovery URL provides alternate access to the administrative and serviceability web applications via username and password.

8 SAML SSO commands in Cisco 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.

9 Troubleshooting SAML SSO in Cisco Unity Connection

SAML SSO allows a user to gain single sign-on access to the web applications on the following Unified Communication prodcuts:

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

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. For more information on the requirements and checklist for SAML SSO, see **Prerequisites for enabling SAML SSO in Unity Connection 10.0(1) and later** *section in Quick start guide.*

Note To enable SAML SSO, make sure you configure Domain Name Server (DNS) in Cisco Unity Connection. SAML SSO does not work without Fully Qualified Domain Name(FQDN).

Task List for Troubleshooting Problems with SAML SSO in Unity Connection

When the SAML SSO in Unity Connection fails to operate properly, use the following suggestions to resolve the problem:

- **Error 1) Redirection to IdP fails**
- **Error 2) IdP authentication fails**
- **Error 3) Redirection to Unity Connection fails**
- **Error 4) Mismatch in SAML Status on Publisher and Subscriber servers**

Error 1) Redirection to IdP fails

When the end users attempt to log into a SAML-enabled web application using a Unity Connection supported web browser, they are not redirected to their configured Identity Provider (IdP) to enter the authentication details.

Solution

Check if the following conditions are met:

- The Identity Provider (IdP) is up and running.
- The correct IdP metadata file (idp.xml) is uploaded to Cisco Unity Connection.
- Verify if the Unity Connection and the IdP are synchronized in the same cycle of time (and timezone).

Error 2) IdP authentication fails

The end user is not getting authenticated by the IdP.

Solution

Check if the following conditions are met:

- The LDAP directory is mapped to the IdP.
- The user is added to the LDAP directory.If the problem still exists, then check the NTP servers associated with Unity Connection and Identity Provider. Make sure that the time on NTP servers associated to both these servers are in synchronization.
- The LDAP account is active.
- The User Id and password are correct.

Error 3) Redirection to Unity Connection fails

Even after getting authenticated by the IdP, the user is not redirected to SAML SSO enabled web applications.

Solution

- The clocks of the Unity Connection and the IdP are synchronized. See the NTP Settings section in *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* for information on synchronizing clocks.
- The mandatory attribute uid is configured on the IdP.
- The correct Unity Connection server metadata file is uploaded to the IdP.
- The user has the required privileges.

Error 4) Mismatch in SAML Status on Publisher and Subscriber servers

When there is a mismatch of SAML status on publisher and subscriber servers in Unity Connection.

Solution

- Check if IdP metadata is correct on Subscriber server, if not then select the option **Re-import Meta Data** from **SAML Single Sign-On** web page.
- If problem still exists, then select the option **Fix All Disabled Servers**.

Note There is no option to re-import meta data for Publisher server in case of Unity Connection cluster.

Diagnostics Traces for Problems with SAML SSO Acess

Apart from this, for all SAML SSO related problems enable the SSO logs using the command:

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

The traces defined are: Debug, Info, Warning, Error and Fatal.

The traces are collected from the following location on Unity Connection :

/var/log/active/tomcat/logs/ssosp

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.