SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 12.0(1)

First Published: 2017-08-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Purpose

The *SAML SSO Deployment Guide for Cisco Unified Communications Applications* provides information on how to enable the Security Assertion Markup Language Single Sign-On (SAML SSO) solution, which allows administrators to access a defined set of Cisco collaboration applications seamlessly after signing into one of those applications. This document describes the various applications that can be used with the SAML-based SSO solution as well as the supported Identity Providers (IdPs) that provide the user authentication for the solution. This document provides links to product documentation for configuration of specific collaboration applications.

Audience

This document is intended for system administrators who are familiar with the SAML-based SSO solution for the various Cisco Unified Communications applications and supported IdPs. This guide also requires knowledge of Network Time Protocol (NTP) and Domain Name System (DNS) server settings.

Organization

The following table provides the organization of this guide.

Chapter	Description
Chapter 1	"SAML-based SSO solution" Provides an overview of how the SAML-based SSO solution works and contains information about general topics, and components that are related to the configuration and operation of SAML SSO feature. It also details the basic configuration flow and system requirements.
Chapter 2	"SAML-based SSO configuration" Contains information on the various features of SAML SSO and the reconfiguration process of OpenAM SSO to SAML-based SSO solution.

Related Documentation

See the following documents for further information about related SAML SSO solutions and configurations:

- *Cisco Unified Communications Manager Documentation Guide, Release 10.0(1)*
- *Release Notes for Cisco Unified Communications Manager, Release 10.0(1)*
- *Release Notes for Cisco Unified Communications Manager, Release 10.5(1)*
- *Release Notes for Cisco Unified Communications Manager, Release 12.5(1)*
- *Cisco Prime Collaboration 10.0 Assurance Guide - Advanced*
- *Cisco Unified Communications Manager System Guide, Release 10.0(1)*
- *Features and Services Guide for Cisco Unified Communications Manager , Release 10.0(1)*
- *System Administration Guide for Cisco Unity Connection, Release 10.0(1)*
- *Troubleshooting Guide for Cisco Unified Communications Manager, Release 10.0(1)*
- *Cisco Unified Communications Operating System Administration Guide, Release 10.0(1)*
- *Troubleshooting Guide for Cisco Unity Connection, Release 10.0(1)*
- *Quick Start Guide for the Cisco Unity Connection SAML SSO, Release 10.0(1)*

Note Obtain the latest documentation by accessing Cisco product documentation page at https://www.cisco.com/cisco/web/support/index.html

Conventions

This document uses the following conventions.

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen font`	Terminal sessions and information the system displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means the information contains useful tips.

Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

`http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html`

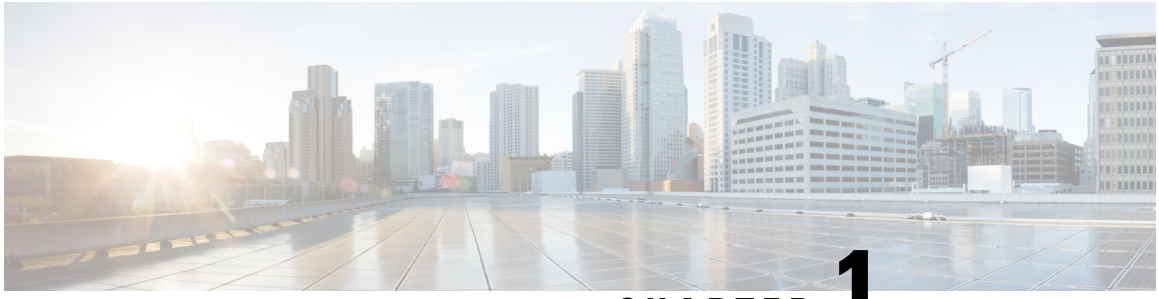
Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at
`http://www.access.gpo.gov/bis/ear/ear_data.html`



CHAPTER 1

SAML-Based SSO Solution

About SAML SSO Solution

Important When deploying Cisco Jabber with Cisco WebEx Meeting Server, Unified Communications Manager and the WebEx Meeting Server must be in the same domain.

SAML is an XML-based open standard data format that enables administrators to access a defined set of Cisco collaboration applications seamlessly after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. It is an authentication protocol used by service providers (for example, Unified Communications Manager) to authenticate a user. SAML enables exchange of security authentication information between an Identity Provider (IdP) and a service provider.

SAML SSO uses the SAML 2.0 protocol to offer cross-domain and cross-product single sign-on for Cisco collaboration solutions. SAML 2.0 enables SSO across Cisco applications and enables federation between Cisco applications and an IdP. SAML 2.0 allows Cisco administrative users to access secure web domains to exchange user authentication and authorization data, between an IdP and a Service Provider while maintaining high security levels. The feature provides secure mechanisms to use common credentials and relevant information across various applications.

The authorization for SAML SSO Admin access is based on Role-Based Access Control (RBAC) configured locally on Cisco collaboration applications.

SAML SSO establishes a Circle of Trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the Service Provider. The Service Provider trusts the IdP's user information to provide access to the various services or applications.

Important Service providers are no longer involved in authentication. SAML 2.0 delegates authentication away from the service providers and to the IdPs.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the Assertion to the Service Provider. Since there is a CoT established, the Service Provider trusts the Assertion and grants access to the client.

Single Sign on Single Service Provider Agreement

Single sign-on allows you to access multiple Cisco collaboration applications after logging on to one of them. In the releases earlier than Unified Communications Manager Release 11.5, when administrators enabled SSO, each cluster node generated its own service provider metadata (SP metadata) file with a URL and a certificate. Each generated file had to be uploaded separately on Identity Provider (IDP) server. As the IDP server considered each IDP and SAML exchange as a separate agreement, the number of agreements that were created was equivalent to the number of nodes in the cluster.

To improve the user experience and to reduce the total cost of the solution for large deployments, this release is enhanced. Now, it supports a single SAML agreement for a Unified Communications Manager cluster (Unified Communications Manager and Instant Messaging and Presence (IM and Presence)).

SAML-Based SSO Features

Enabling SAML SSO results in several advantages:

- It reduces password fatigue by removing the need for entering different user name and password combinations.
- It transfers the authentication from your system that hosts the applications to a third party system. Using SAML SSO, you can create a circle of trust between an IdP and a service provider. The service provider trusts and relies on the IdP to authenticate the users.
- It protects and secures authentication information. It provides encryption functions to protect authentication information passed between the IdP, service provider, and user. SAML SSO can also hide authentication messages passed between the IdP and the service provider from any external user.
- It improves productivity because you spend less time re-entering credentials for the same identity.
- It reduces costs as fewer help desk calls are made for password reset, thereby leading to more savings.

Basic Elements of a SAML SSO Solution

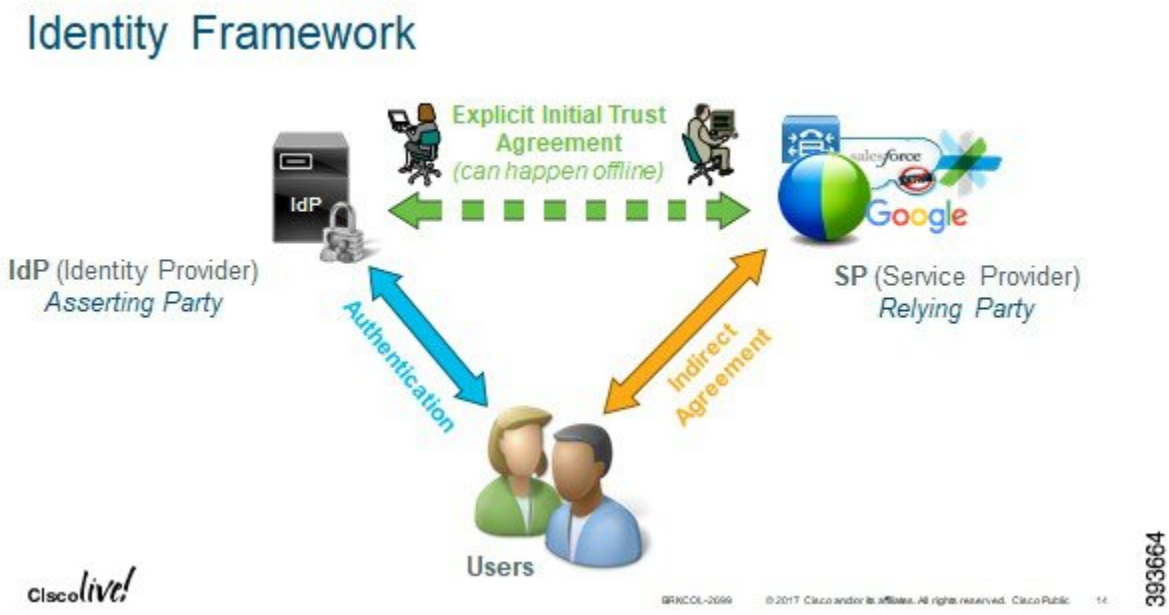
- Client (the user’s client): This is a browser-based client or a client that can leverage a browser instance for authentication. For example, a system administrator’s browser.
- Service provider: This is the application or service that the client is trying to access. For example, Unified Communications Manager.

- An Identity Provider (IdP) server: This is the entity that authenticates user credentials and issues SAML Assertions.
- Lightweight Directory Access Protocol (LDAP) users: These users are integrated with an LDAP directory, for example Microsoft Active Directory or OpenLDAP. Non-LDAP users reside locally on the Unified Communications server.
- SAML Assertion: It consists of pieces of security information that are transferred from IdPs to the service provider for user authentication. An assertion is an XML document that contains trusted statements about a subject including, for example, a username and privileges. SAML assertions are usually digitally signed to ensure their authenticity.
- SAML Request: This is an authentication request that is generated by a Unified Communications application. To authenticate the LDAP user, Unified Communications application delegates an authentication request to the IdP.
- Circle of Trust (CoT): It consists of the various service providers that share and authenticate against one IdP in common.
- Metadata: This is an XML file generated by an SSO-enabled Unified Communications application (for example, Unified Communications Manager, Cisco Unity Connection, and so on) as well as an IdP. The exchange of SAML metadata builds a trust relationship between the IdP and the service provider.
- Assertion Consumer Service (ACS) URL: This URL instructs the IdPs where to post assertions. The ACS URL tells the IdP to post the final SAML response to a particular URL.

Note All in-scope services requiring authentication use SAML 2.0 as the SSO mechanism.

See the following figure for the identity framework of a SAML SSO solution.

Figure 1: Identity Framework for the SAML SSO Solution



Cisco Unified Communications Applications that Support SAML SSO

- Unified Communications Manager
- Unified Communications Manager IM and Presence Service

Note See the "SAML Single Sign-On" chapter in the *Features and Services Guide for Cisco Unified Communications Manager, Release 10.0(1)* for detailed information on configuring SAML SSO.

- Cisco Unity Connection

Note See the "Managing SAML SSO in Cisco Unity Connection" chapter in the *System Administration Guide for Cisco Unity Connection Release 10.x* for additional information on configuring the SAML SSO feature on the Cisco Unity Connection server.

- Cisco Prime Collaboration

Note See the "Single Sign-On for Prime Collaboration" section under "Managing Users" chapter in the *Cisco Prime Collaboration 10.0 Assurance Guide - Advanced* guide to get detailed information on the SAML SSO configuration steps on the Cisco Prime Collaboration server.

- Windows version of Cisco Unified Real-Time Monitoring Tool (RTMT).

Note See the "Configure SSO for RTMT" procedure under "Configure Initial System and Enterprise Parameters" chapter in the *System Configuration Guide for Cisco Unified Communications Manager* guide to get detailed information on how to enable SAML SSOfor RTMT.

- Cisco Expressway

Note See the *Cisco Expressway Administrator Guide* to get SAML SSO setup information for Cisco Expressway.

SAML SSO Support for Cisco Unified Communications Manager Web Interfaces

With this release, the Cisco Unified OS Administration and Disaster Recovery System are now the Security Assertion Markup Language (SAML) SSO-supported applications. If SAML SSO is enabled, you can launch these applications or other supported applications, such as Unified Communications Manager, after a single sign-in with an Identity Provider (IdP). You no longer need to sign in to these applications separately.

To support SAML SSO for Cisco Unified OS Administration and Disaster Recovery System, the Level 4 administrator creates the Level 0 and Level 1 administrators in the active directory. The Level 4 administrator adds the platform administrators in all the nodes of a cluster. With this addition, the platform administrators are synchronized between the active directory and the platform database. While configuring users in platform database, the administrator must configure the **uid** value for the user. Cisco Unified OS Administration and Disaster Recovery System applications use the **uid** value to authorize a user. The IdP server authenticates their credentials against the active directory server and sends a SAML response. After authentication, Unified Communications Manager authorizes the users from the platform database using the **uid** value. For details on **uid** value, see Configure Unique Identification Value for Platform Users, on page 5 procedure.

If SAML SSO is enabled for the existing release and you upgrade from earlier release to the new release, the SAML SSO support is available for Unified OS Administration and Disaster Recovery System applications in the new release. The SAML SSO support for these applications is also enabled when you enable SAML SSO for any Unified Communications Manager web applications. To enable the SAML SSO support for the new release, see the SAML SSO Enablement topic from the *SAML SSO Deployment Guide for Cisco Unified Communications Applications* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note When SAML SSO support is enabled for a Unified Communications Manager administrator, it is applicable across the cluster. However, for the Cisco Unified OS Administration and Disaster Recovery System applications, each platform administrator is specific to a node and these user details are not replicated across the cluster. So, each platform user is created in each subscriber node of a cluster.

Configure Unique Identification Value for Platform Users

The unique identification (UID) value is used to authorize a platform user to do SSO login on platform pages. The Level 4 administrator can configure this value for platform administrators in one of the following ways:

- While creating the platform users by using the **set account name** command on the CLI.
- While updating the existing **uid** value.

Note For details, see the **set account name** and **set account ssouidvalue** commands in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Recovery URL Sign-in Option for Cisco Unified OS Administration

With this release, platform administrators can access Cisco Unified OS Administration either by signing in to one of the SAML SSO-enabled applications or by using the recovery URL option. This option is available as **Recovery URL to bypass Single Sign On** link on the main page of the SSO-enabled nodes. Platform users can sign in to Cisco Unified OS Administration if they have Recovery URL access.

The Level 4 administrator configures the recovery URL sign-in option for platform users. The administrator can enable this option while the platform administrators are being created through CLI or when their details are being updated using the CLI command. For details on the CLI commands for recovery URL login for new and existing platform administrators, see the **set account ssorecoveryurlaccess** command in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Note By default, the **Recovery URL to bypass Single Sign On** link is enabled for the Level 4 administrator. This link is enabled for the platform administrators Level 0 and Level 1 in case of upgrade from earlier release to the new release.

Software Requirements

The SAML SSO feature requires the following software components:

- Cisco Unified Communications applications, release 10.0(1) or later.
- An LDAP server that is trusted by the IdP server and supported by Cisco Unified Communications applications.
- An IdP server that complies with SAML 2.0 standard.
- Login flow supported by Unified Comunications Manager is SP-initiated.

Selecting an Identity Provider (IdP)

Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.

SAML-based SSO is an option for authenticating UC service requests originating from inside the enterprise network, and it is now extended to clients requesting UC services from outside via Mobile and Remote Access (MRA).

If you choose SAML-based SSO for your environment, note the following:

- SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard.
- SAML-based identity management is implemented in different ways by vendors in the computing and networking industry, and there are no widely accepted regulations for compliance to the SAML standards.
- The configuration of and policies governing your selected IdP are outside the scope of Cisco TAC (Technical Assistance Center) support. Please use your relationship and support contract with your IdP Vendor to assist in configuring the IDP properly. Cisco cannot accept responsibility for any errors, limitations, or specific configuration of the IdP.

Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following IdPs have been tested with Cisco Collaboration solutions:

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIG-IP 11.6.0
- Okta 2017.38

SAML Components

A SAML SSO solution is based on a particular combination of assertions, protocols, bindings, and profiles. The various assertions are exchanged among applications and sites using the protocols and bindings, and those assertions authenticate the users among sites. The SAML components are as follows:

- SAML Assertion: It defines the structure and content of the information that is transferred from IdPs to service providers. It consists of packets of security information and contains statements that service providers use for various levels of access-control decisions.

  SAML SSO provides the following types of statements:

  - Authentication statements- These statements assert to the service provider about the method of authentication that occurs between the IdP and the browser at a particular time.
  - Attribute statements- These statements assert about certain attributes (name-value pairs) that are associated with the user. The attribute assertions contain specific information about the user. The service providers use attributes to make access-control decisions.

- SAML protocol: A SAML protocol defines how the SAML requests for and gets assertions. This protocol is responsible for the SAML request and response elements that consist of certain SAML elements or assertions. The SAML 2.0 contains the following protocols:

  - Assertion Query and Request Protocol
  - Authentication Request Protocol

- SAML binding: A SAML binding specifies the mapping of SAML assertion and/or protocol message exchanges with standard messaging formats or communication protocols like SOAP exchanges. Unified Communications 10.0 supports the following SAML 2.0 bindings:

  - HTTP Redirect (GET) Binding
  - HTTP POST Binding

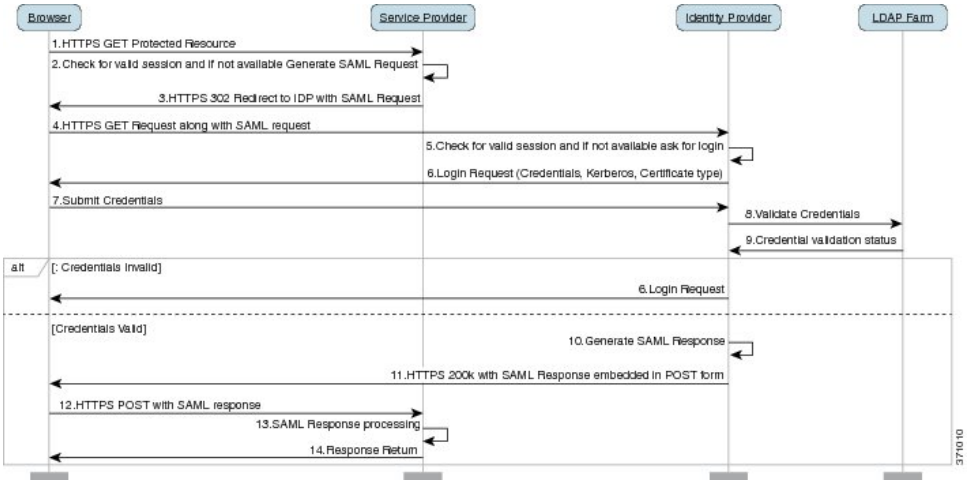
- SAML profile: A SAML profile provides a detailed description of the combination of SAML assertions, protocols, and bindings to support well-defined use cases. Unified Communications 10.0 supports the SAML 2.0 Web Browser SSO Profile.

SAML SSO Call Flow

This section describes how the SAML SSO feature enables single sign-on for Unified Communications applications. This section also explains the relationship between the IdP and the service provider and helps identify the importance of the various configuration settings to enable single sign-on.

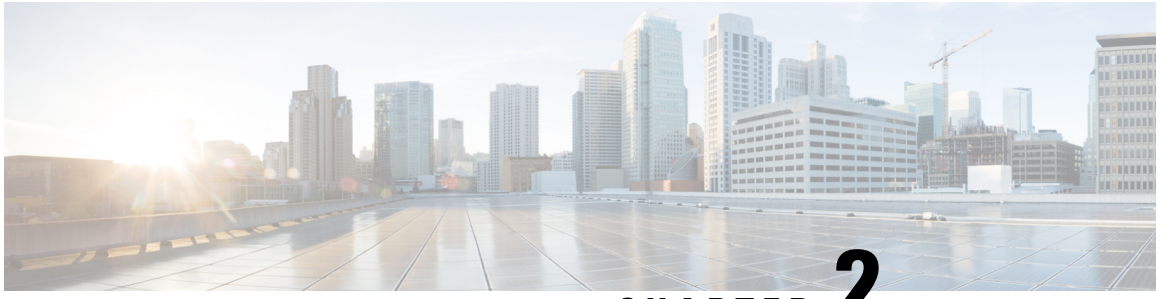
The following figure illustrates the SAML SSO call flow for cases where the IdP requests a username and password.

Figure 2: SAML SSO Call Flow for Credential Requests from IdP



1	A browser-based client attempts to access a protected resource on a service provider. **Note** The browser does not have an existing session with the service provider.
2	Upon receipt of the request from the browser, the service provider generates a SAML authentication request. **Note** The SAML request includes information indicating which service provider generated the request. Later, this allows the IdP to know which particular service provider initiated the request. The IdP must have the Assertion Consumer Service (ACS) URL to complete SAML authentication successfully. The ACS URL tells the IdP to post the final SAML response to a particular URL. **Note** Unified Communications Manager no longer uses the Assertion Consumer Service URL in SAML authentication requests, instead uses the Assertion Consumer Service Index URL. **Note** The authentication request can be sent to the IdP, and the Assertion sent to the service provider through either Redirect or POST binding. For example, Unified Communications Manager supports POST binding in either direction.
3	The service provider redirects the request to the browser. **Note** The IdP URL is preconfigured on the service provider as part of SAML metadata exchange.

4	The browser follows the redirect and issues an HTTPS GET request to the IdP. The SAML request is maintained as a query parameter in the GET request.
5	The IdP checks for a valid session with the browser.
6	In the absence of any existing cookie within the browser, the IdP generates a login request to the browser and authenticates the browser using whatever authentication mechanism is configured and enforced by the IdP. **Note** The authentication mechanism is determined by the security and authentication requirements of the customer. This could be form-based authentication using username and password, Kerberos, PKI, etc. This example assumes form-based authentication.
7	The user enters the required credentials in the login form and posts them back to the IdP. **Note** The authentication challenge for logging is between the browser and the IdP. The service provider is not involved in user authentication.
8	The IdP in turn submits the credentials to the LDAP server.
9	The LDAP server checks the directory for credentials and sends the validation status back to the IdP.
10	The IdP validates the credentials and generates a SAML response which includes a SAML Assertion. **Note** The Assertion is digitally signed by the IdP and the user is allowed access to the service provider protected resources. The IdP also sets its cookie here.
11	The IdP redirects the SAML response to the browser.
12	The browser follows the hidden form POST instruction and posts the Assertion to the ACS URL on the service provider.
13	The service provider extracts the Assertion and validates the digital signature. **Note** The service provider uses this digital signature to establish the circle of trust with the IdP.
14	The service provider then grants access to the protected resource and provides the resource content by replying 200 OK to the browser. **Note** The service provider sets its cookie here. If there is a subsequent request by the browser for an additional resource, the browser includes the service provider cookie in the request. The service provider checks whether a session already exists with the browser. If a session exists, the web browser returns with the resource content.



CHAPTER 2

SAML-Based SSO Configuration

Prerequisites

NTP Setup

In SAML SSO, Network Time Protocol (NTP) enables clock synchronization between the Unified Communications applications and IdP. SAML is a time sensitive protocol and the IdP determines the time-based validity of a SAML assertion. If the IdP and the Unified Communications applications clocks are not synchronized, the assertion becomes invalid and stops the SAML SSO feature. The maximum allowed time difference between the IdP and the Unified Communications applications is 3 seconds.

Note For SAML SSO to work, you must install the correct NTP setup and make sure that the time difference between the IdP and the Unified Communications applications does not exceed 3 seconds.

For information about synchronizing clocks, see the NTP Settings section in *Cisco Unified Communications Operating System Administration Guide*.

DNS Setup

Domain Name System (DNS) enables the mapping of host names and network services to IP addresses within a network or networks. DNS server(s) deployed within a network provide a database that maps network services to hostnames and, in turn, hostnames to IP addresses. Devices on the network can query the DNS server and receive IP addresses for other devices in the network, thereby facilitating communication between network devices.

Unified Communications applications can use DNS to resolve fully qualified domain names to IP addresses. The service providers and the IdP must be resolvable by the browser. For example, when the administrator enters the service provider hostname (`http://www.cucm.com/ccmadmin`) in the browser, the browser must resolve the hostname. When the service provider redirects the browser to IdP

(`http://www.idp.com/saml`) for SAML SSO, the browser must also resolve the IdP hostname. Moreover, when the IdP redirects back to the service provider ACS URL, the browser must resolve that as well.

Directory Setup

LDAP directory synchronization is a prerequisite and a mandatory step to enable SAML SSO across various Unified Communications applications. Synchronization of Unified Communications applications with an LDAP directory allows the administrator to provision users easily by mapping Unified Communications applications data fields to directory attributes.

Note To enable SAML SSO, the LDAP server must be trusted by the IdP server and supported by Unified Communications applications.

For more information, see the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab10/directry.html

Certificate Management and Validation

Important Cisco strongly recommends that server certificates are signed for SAML SSO and that multiserver certificates are used where product support is available.

Note

- Common Names (CN) and Subject Alternative Names (SAN) are references to the IP address or Fully Qualified Domain Name (FQDN) of the address that is requested. For instance, if you enter https://www.cisco.com, then the CN or SAN must have “www.cisco.com” in the header.
- If the Unified Communications Manager is already in Mixed/Secure Mode and there are changes made to the certificates, then the CTL certificate must be updated using the secure USB token. Otherwise the Cisco Jabber client will not be able to acquire telephony capability. The CTL token update requires a Unified Communications Manager restart.

In SAML SSO, each entity participating in the SAML message exchange, including the user's web browser, must establish a seamless secure HTTPS connections to the required entities. Cisco strongly recommends that signed certificates issued by a trusted Certificate Authority be configured on each UC product participating in the SAML SSO deployment.

Unified Communications applications use certificate validation to establish secure connections with servers. Certificates are used between end points to build a trust/authentication and encryption of data. This confirms that the endpoints communicate with the intended device and have the option to encrypt the data between the two endpoints.

When attempting to establish secure connections, servers present Unified Communications clients with certificates. If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

Certificates Signed by a Certificate Authority

Cisco recommends using server certificates that are signed by one of the following types of Certificate Authority (CA):

- **Public CA** - A third-party company verifies the server identity and issues a trusted certificate.
- **Private CA** - You create and manage a local CA and issue trusted certificates.

The signing process varies for each product and can vary between server versions. It is beyond the scope of this document to provide detailed steps for every version of each server. Refer the appropriate server documentation for detailed instructions on how to get certificates signed by a CA.

However, the following steps provide a high-level overview of the procedure:

Procedure

Step 1 Generate a Certificate Signing Request (CSR) on each product that can present a certificate to the client.

Step 2 Submit each CSR to the CA.

Step 3 Upload the certificates that the CA issues to each server.

Every server certificate should have an associated root certificate present in the trust store on client computers. Cisco UC applications validate the certificates that servers present against the root certificates in the trust store.

If you get server certificates signed by a public CA, the public CA should already have a root certificate present in the trust store on the client computer. In this case, you do not need to import root certificates on the client computers.

You should import root certificates if the certificates are signed by a CA that does not already exist in the trust store, such as a private CA.

In SAML SSO, the IdP and service providers must have CA signed certificates with the correct domains in the CN or SAN. If the correct CA certificates are not validated, the browser issues a pop up warning.

For example, when the administrator points the browser to `https://www.cucm.com/ccmadmin`; the Unified Communications Manager portal presents a CA certificate to the browser. When the browser is redirected to `https://www.idp.com/saml` , the IdP presents a CA certificate. The browser will check that the certificate presented by the servers contains CN or SAN fields for that domain, and that the certificate is signed by a trusted CA.

Alternatively, if the customer has their own private CA, then that CA must be installed as a root trust anchor on the computers that the administrator is launching their browser from.

Configure Multiserver SAN Certificates

Each Cisco product has its own process for generating multiserver SAN certificates. For information about the Cisco products that support multiserver SAN certificates see the relevant guide.

Related Topics

Release Notes for Cisco Unified Communications Manager, Release 10.5(1)

Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 10.x

Cisco Prime Collaboration

Deploy Certificate Issuer for Microsoft Edge Interoperability

An interoperability issue exists within SAML SSO deployments where the Microsoft Edge Browser is deployed. If the Edge Browser is deployed on an SSO-enabled machine, the Edge browser does not recognize the certificate issuer of the Unified Communications Manager certificate and does not provide access.

Use this procedure to fix this issue via the Group Policy Object (GPO) and Active Directory whereby you can push the certificate issuer of the Unified Communications Manager certificate to the Trusted Root Certification of local machines that use the Edge browser.

Note The "certificate issuer" depends on how your certificates are set up. For example, for third-party CA certificates, You may need to push the CA certificate only if the CA itself signs the Unified Communications Manager certificate. However, if an intermediate CA signs the Unified Communications Manager certificate, you may need to push the complete certificate chain, which will include the root certificate, intermediate certificate, and any leaf certificates.

Before you begin

Membership in the local **Administrators** group, or equivalent, of the local machine is the minimum required to complete this procedure

Procedure

Step 1 In Active Directory, Open Group Policy Management Console.

Step 2 Find an existing GPO or create a new GPO to contain the certificate settings. The GPO must be associated with the domain, site, or organizational unit whose users you want affected by the policy.

Step 3 Right-click the GPO, and select **Edit**.
The **Group Policy Management Editor** opens, and displays the current contents of the policy object.

Step 4 In the navigation pane, open **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Publishers**.

Step 5 Click the **Action** menu, and click **Import**.

Step 6 Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.

Step 7 If the certificate is self-signed, and cannot be traced back to a certificate that is in the **Trusted Root Certification Authorities** certificate store, then you must also copy the certificate to that store. In the navigation pane, click **Trusted Root Certification Authorities**, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

Note For additional information on Managing Trusted Root Certificates in Active Directory, see https://technet.microsoft.com/en-us/library/cc754841(v=ws.11).aspx.

SAML SSO Configuration Task Flow

Complete these tasks to configure Unified Communications Manager for SAML SSO.

Before you begin

SAML SSO configuration requires that you configure the Identity provider (IdP) at the same time that you configure Unified Communications Manager. For IdP-specific configuration examples, see:

- Active Directory Federation Services
- Okta
- Open Access Manager
- PingFederate

Note The above links are examples only. Refer to your IdP documentation for official documentation.

Procedure

	Command or Action	Purpose
Step 1	Export UC Metadata from Cisco Unified Communications Manager, on page 16	To create a trust relationship, you must exchange metadata files between Unified Communications Manager and the IdP.
Step 2	Configure SAML SSO on the Identity Provider (IdP)	Complete the following tasks: • Upload the UC metadata file that was exported from Unified Communications Manager in order to complete the Circle of Trust relationship. • Configure SAML SSO on the IdP • Export an IdP metadata file. This file will be imported into the Unified Communications Manager
Step 3	Enable SAML SSO in Cisco Unified Communications Manager	Import your IdP metadata and enable SAML SSO in Unified Communications Manager.
Step 4	Verify the SAML SSO Configuration, on page 18	Verify that SAML SSO has been configured successfully.

Export UC Metadata from Cisco Unified Communications Manager

Use this procedure to export a UC metadata file from the Service Provider (Unified Communications Manager). The metadata file will be imported into the Identity Provider (IdP) in order to build a Circle of Trust relationship.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**

Step 2 From the **SAML Single Sign-On** window, choose one of the options for the **SSO Mode** field:

- **Cluster wide**—A single SAML agreement for the cluster.

  Note If you choose this option, ensure that Tomcat servers for all the nodes in the cluster have the same certificate, which is the multi-server SAN certificate.

- **Per Node**—Each node has a separate SAML agreement.

Step 3 From the **SAML Single Sign-On** window, choose one of the options for the **Certificate** field.

- **Use system generated self-signed certificate**
- **Use Tomcat certificate**

Step 4 Click **Export All Metadata** to export the metadata file.

Note If you choose the **Cluster wide** option in Step 3, a single metadata XML file appears for a cluster for download. However, if you choose the **Per Node** option, one metadata XML file appears for each node of a cluster for download.

What to do next

Complete the following tasks on the IdP:

- Upload the UC metadata file that was exported from Unified Communications Manager
- Configure SAML SSO on the IdP
- Export an IdP metadata file. This file will be imported into the Unified Communications Manager in order to complete the Circle of Trust relationship.

Enable SAML SSO in Cisco Unified Communications Manager

Use this procedure to enable SAML SSO on the Service Provider (Unified Communications Manager). This process includes importing the IdP metadata onto the Unified Communications Manager server.

Important Cisco recommends that you restart Cisco Tomcat service after enabling or disabling SAML SSO.

Note The Cisco CallManager Admin, Unified CM IM and Presence Administration, Cisco CallManager Serviceability, and Unified IM and Presence Serviceability services are restarted after you enable or disable SAML SSO.

Before you begin

Prior to completing this procedure, make sure of the following:

- You require an exported metadata file from your IdP.
- Make sure that the end-user data is synchronized to the Unified Communications Manager database
- Verify that the Unified Communications Manager IM and Presence Cisco Sync Agent service has completed data synchronization successfully. Check the status of this test in **Cisco Unified CM IM and Presence Administration** by choosing **Diagnostics** > **System Troubleshooter** The “Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)” test indicates a "Test Passed" outcome if data synchronization has completed successfully
- At least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified Administration. For more information about synchronizing end-user data and adding LDAP-synchronized users to a group, see the “System setup” and “End user setup” sections in the Unified Communications Manager Administration Guide

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO** and then click **Continue**.

A warning message notifies you that all server connections will be restarted.

Step 3 If you have configured the **Cluster wide** SSO mode, click the **Test for Multi-server tomcat certificate** button. Otherwise, you can skip this step.

Step 4 Click **Next**.

A dialog box that allows you to import IdP metadata appears. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 5 Import the metadata file that you exported from your IdP:

a) **Browse** to locate and select your exported IdP metadata file.
b) Click **Import IdP Metadata**.
c) Click **Next**.
d) At the **Download Server Metadata and Install on IdP** screen, click **Next**.

Note The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

Step 6 Test the connection and complete the configuration:

a) In the **End User Configuration** window, choose a user that is LDAP-synchronized and has the permission as “Standard CCM Super User” from the **Permissions Information** list box

b) Click **Run Test**.

The IdP login window appears.

Note You cannot enable SAML SSO until the test succeeds.

c) Enter a valid username and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails, or takes more than 60 seconds to authenticate, a "Login Failed" message appears on the IdP login window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt logging in to the IdP again, select another user and run another test.

d) Click **Finish** to complete the SAML SSO setup.

SAML SSO is enabled and all the web applications participating in SAML SSO are restarted. It may take one to two minutes for the web applications to restart.

Verify the SAML SSO Configuration

After you configure SAML SSO on both the Service Provider (Unified Communications Manager) and on the IdP, use this procedure on Unified Communications Manager to confirm that the configuration works.

Before you begin

Confirm the following:

- The **SAML Single Sign-On Configuration** window in Unified CM Administration shows that you have successfully imported the **IdP Metadata Trust** file.
- The Service Provider metadata files are installed on the IdP.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On** and the **SAML Single Sign-On Configuration** window opens, click **Next**.

Step 2 Choose an administrative user form the **Valid Administrator Usernames** area and click the **Run SSO Test…** button.

Note The user for the test must have administrator rights and has been added as a user on the IdP server. The Valid Administrator Usernames area displays a list of users, which can be drawn on to run the test.

If the test succeeds, SAML SSO is successfully configured.

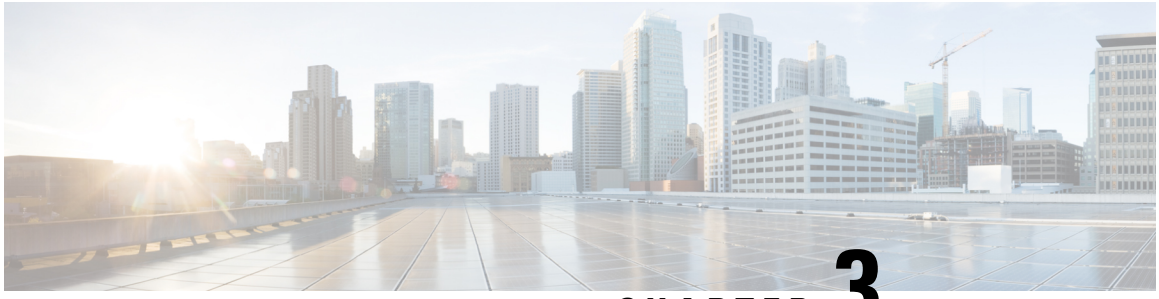
Reconfigure OpenAM SSO to SAML SSO Following an Upgrade

As of Release 11.0(1), Unified Communications Manager no longer offers the OpenAM SSO solution. If you have upgraded from an earlier release with the Open AM SSO solution configured, you must reconfigure your system to use the SAML SSO solution using one of the supported IdPs. Use the configurations that are documented in this guide to reconfigure your system to use SAML SSO.

Note Do not confuse the OpenAM SSO solution with a SAML SSO solution that uses OpenAM for the identity provider as they are different solutions. When you reconfigure your system to use SAML SSO, you can use any of the IdPs that are listed in this document.

SAML SSO Deployment Interactions and Restrictions

Feature	Feature Interaction
Tomcat Certificate Regeneration	If you regenerate the Tomcat Certificates, generate a new metadata file on the Service Provider and upload that metadata file to the IdP.
Metadata Regeneration	The metadata file regenerates if you perform one of the following: • Change Self-Signed Certificates to Tomcat Certificates and vice-versa. • Regenerate Tomcat Certificates to ITL Recovery Certificates. The CUCM downloads the regenerated metadata file and uploads to the IdP.



CHAPTER 3

End User SAML SSO

End User SAML SSO Configuration

End user or federated SSO is a standard that allows products to meet customer compliance requirements, reduce the total cost of ownership, and improve end user experience. The foundation for this support in the collaboration products has been introduced in the 10.0 and 10.5 releases. This allows administrators to configure the infrastructure in preparation for end user clients such as Cisco Unity Connection and Cisco Jabber, which is rolling out support for users with release 10.5 in the second half of 2014.

Once an Administrator enables this feature for users it will allow users in a Cisco collaboration application to log in to supported applications with their corporate username and password. If the Cisco application is accessed by way of a browser the user can use the same corporate username and password to log in. If the user has already logged in to another corporate application in that same browser they should be able to access the application without having to provide a username and password. All of these features are available within the customer network or accessible by way of a VPN.

The supported products are:

Product	Supports End User SAML SSO from Release...	More Information
Cisco Unified Communications Manager	10.5	Click here
IM and Presence Service	10.5	Click here
Cisco Unity Connection	10.5	Click here
WebEx Meeting Center	Cloud	Click here
WebEx Connect and Messenger	Cloud	Click here
Cisco WebEx Meetings Server	1.5 and 2.0	Click here

The supported end user clients are:

Product	Release	More Information
WebEx IOS	Available with all releases	Click here
WebEx Android	Available with all releases	Click here
WebEx Connect	Available with all releases	Click here
WebEx Messenger	Available with all releases	Click here
Jabber for Windows	10.5	Available in the second half of 2014
Jabber IOS	10.5	Available in the second half of 2014
Jabber for Android	10.5	Available in the second half of 2014
Jabber for Mac	10.5	Available in the second half of 2014

Note

- When deploying Cisco Jabber with Cisco WebEx Meeting Server, Unified Communications Manager and the WebEx Meeting Server must be in the same domain.
- When Cisco Jabber is running with SSO on a Mac, Jabber cannot automatically set a cookie once authorized for Jabber services. Mac behavior, by default, only allows cookies for sites the user navigates to. Each time Jabber needs to check for authentication it has to go to the IdP.
- The SAML Assertion must include the email address for WebEx; the SAML Schemas should be aligned to cover that.
- To trigger OAuth timer expiration correctly, ensure that the OAuthTokenExpiry value on Unified Communications Manager is greater than the WebsessionApp expiry value on Tomcat.

INDEX