SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.0(1)

First Published: December 06, 2013

Last Modified: May 08, 2014

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

Text Part Number: OL-31083-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface v

Purpose v

Audience v

Organization v

Related Documentation vi

Conventions vi

Additional Information vii

Cisco Product Security Overview viii

CHAPTER 1

SAML-Based SSO Solution 1

About SAML SSO Solution 1

SAML-Based SSO Features 2

Basic Elements of a SAML SSO Solution 2

SAML SSO Web Browsers 3

Cisco Unified Communications Applications that Support SAML SSO 4

Software Requirements 4

Supported IdPs 4

SAML Components 5

SAML SSO Call Flow 6

CHAPTER 2

SAML-Based SSO Configuration 9

Prerequisites 9

NTP Setup 9

DNS Setup 9

Directory Setup 10

Certificate Management and Validation 10

Certificates Signed by a Certificate Authority 10

High-Level Circle of Trust Setup 11
Create a Circle of Trust 12
Enable SAML SSO through the OpenAM IdP 13
SAML SSO Enablement 13
Configure Cisco Unified Communications Manager for SAML SSO Activation 13
Configure OpenAM and Cisco Unified Communications Manager for SAML SSO 14
Verify the SAML SSO Configuration 15
Reconfigure OpenAM SSO to SAML SSO 16

Preface

- Purpose, page v
- Audience, page v
- Organization, page v
- Related Documentation, page vi
- Conventions, page vi
- Additional Information, page vii
- Cisco Product Security Overview, page viii

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)*
- *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:

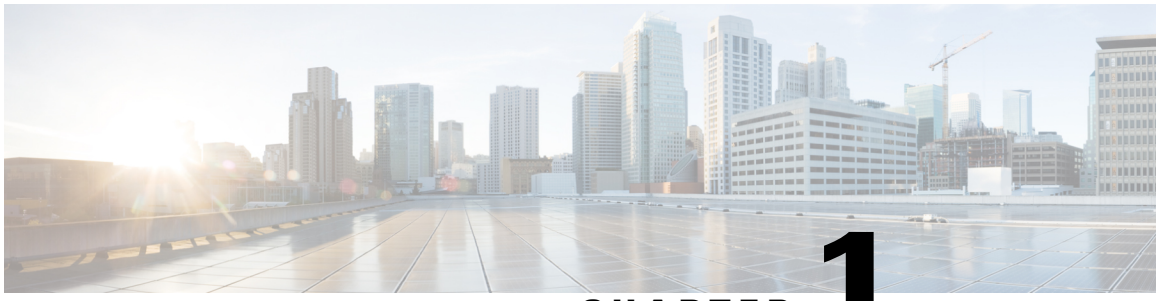
`http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html`

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, page 1
- SAML-Based SSO Features, page 2
- Basic Elements of a SAML SSO Solution, page 2
- SAML SSO Web Browsers, page 3
- Cisco Unified Communications Applications that Support SAML SSO, page 4
- Software Requirements, page 4
- Supported IdPs, page 4
- SAML Components, page 5
- SAML SSO Call Flow, page 6

About SAML SSO Solution

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, Cisco 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.

For information on how the administrative users access the various Cisco collaboration applications by enabling SAML SSO, see the SAML SSO Call Flow.

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

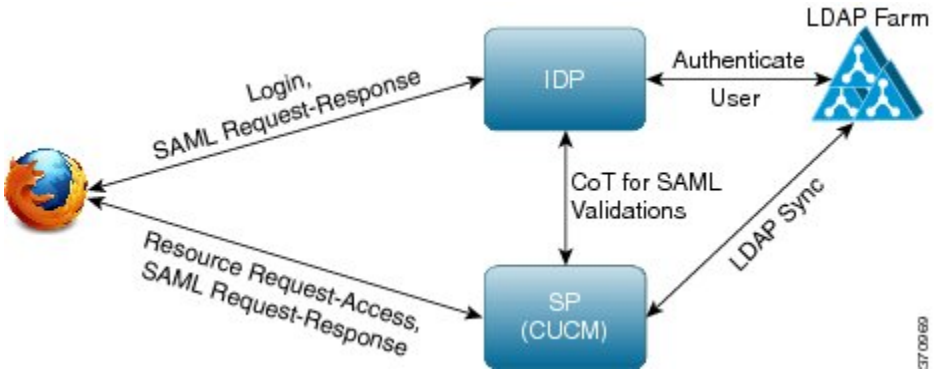
- Client (the user's client): This is a browser-based client or a client that can leverage a browser instance for authentication. For example, a system administrator's browser.
- Service provider: This is the application or service that the client is trying to access. For example, Cisco Unified Communications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

Figure 1: Basic Elements of SAML SSO



SAML SSO Web Browsers

The following operation system browsers support SAML SSO solution:

- On Microsoft Windows XP, Vista, and 7:
  - Microsoft Internet Explorer (IE) 8, IE 9
  - Mozilla Firefox 4.x, Firefox 10.x
  - Google Chrome 8.x
- On Apple OS X and later:
  - Apple Safari 5.x
  - Firefox 4.x, 10.x
  - Chrome 8.x

Cisco Unified Communications Applications that Support SAML SSO

- Cisco Unified Communications Manager
- Cisco 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.

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.
- A supported IdP server that complies with SAML 2.0 standard.

Supported IdPs

Identity Provider (IdP) is an authentication module that creates, maintains, and manages identity information for users, systems, or services and also provides authentication to other applications and service providers within a distributed network.

With SAML SSO, IdPs provide authentication options based on the user role or log in options for each of the Cisco collaboration applications. The IdPs store and validate the user credentials and generate a SAML response that allows the user to access the service provider protected resources.

Note You must be familiar with your IdP service, and ensure that it is currently installed and operational.

The Cisco Unified Communications SAML SSO feature has been tested with the following IdPs:

- Microsoft Active Directory Federation Services (ADFS) version 2.0
- Open Access Manager (OpenAM) version 10.0
- PingFederate version 6.10.0.4

Note For detailed information regarding the individual IdP setup and configuration settings, refer to the IdP documentation.

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

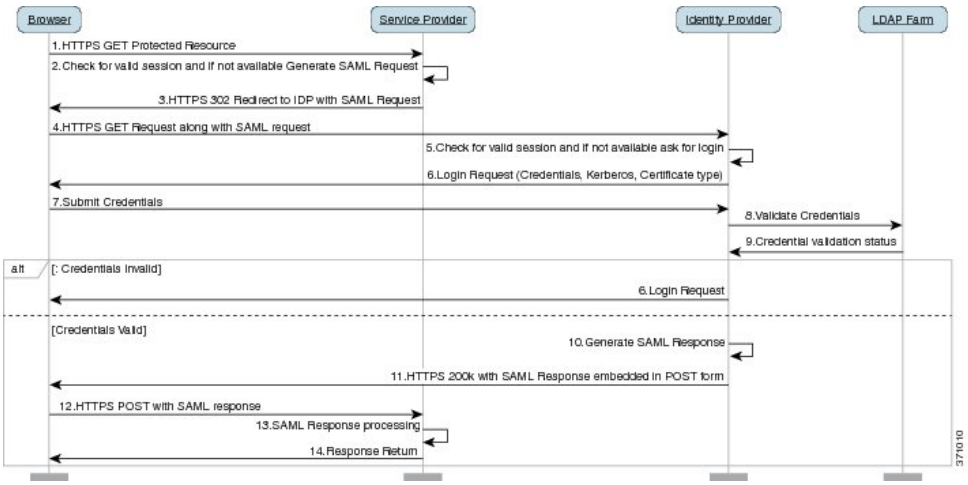
- SAML profile: A SAML profile provides a detailed description of the combination of SAML assertions, protocols, and bindings to support well-defined use cases. Unified Communications 10.0 supports the SAML 2.0 Web Browser SSO Profile.

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.

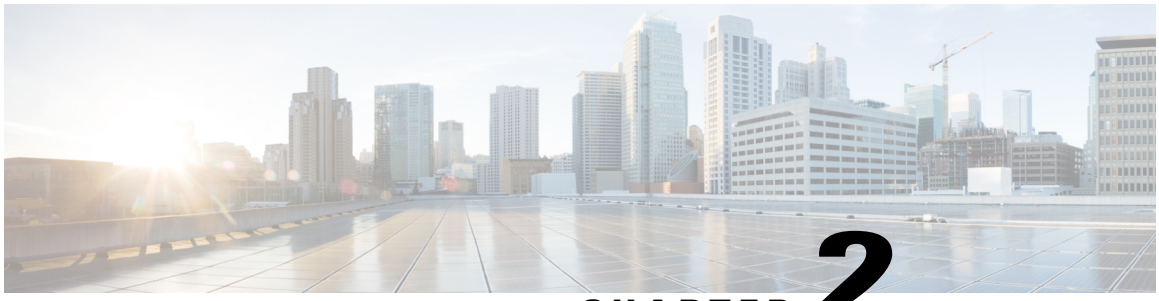
The following figure illustrates the SAML SSO call flow.

Figure 2: SAML SSO Call Flow



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** 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, Cisco 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 session with 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, page 9
- Enable SAML SSO through the OpenAM IdP, page 13
- Reconfigure OpenAM SSO to SAML SSO, page 16

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

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 Cisco 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 Cisco 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 CUCM 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.

High-Level Circle of Trust Setup

To enable SAML SSO across Unified Communications applications, the administrator must establish a Circle of Trust (CoT) between the Service Provider and the IdP. The following steps provide a high-level overview of the procedure.

Procedure

Step 1 Exchange of certificate between the IdP and the Service Provider:

a) Export a CA certificate from the Service Provider.

b) Go to the IdP server and import the CA certificate from the Service Provider.

c) Export a CA certificate from the IdP server.
d) Go to the Service Provider and import the CA certificate from the IdP server.

Note The administrator must ensure that the IdP trusts the certificate contained in the Service Providers metadata. In some instances importing the metadata to the IdP may be sufficient but in other cases the signing certs of the Service Provider certificate must be manually imported into the IdP's certificate trust store.

Step 2 Exchange of metadata between the IdP and the Service Provider:

a) Export the metadata from the IdP.
b) Import the metadata to the Service Provider.
c) Export the metadata from the Service Provider.
d) Go to the IdP server and provision the Service Provider by importing the metadata from the Service Provider.

Step 3 Configure the mandatory attribute uid on the IdP. This attribute must match the LDAP synchronized user id attribute that is used in Unified Communications applications.

Note uid is a mandatory attribute that IdP configures for a given Service Provider. Through this attribute, a Service Provider identifies the identity of an authenticated user. For information about configuring mandatory attribute mapping, refer the IdP product documentation.

Note For SAML SSO to work as expected, the Service Provider and the IdP must be in the same CoT.

Create a Circle of Trust

If there is no existing CoT to add Cisco Unified Communications Manager to, then a CoT must be created before SAML SSO becomes active.

This example uses OpenAM to create a CoT.

Procedure

Step 1 Log in to the OpenAM server user interface.

Step 2 Choose the **Federation** tab and in the Circle of Trust area, click the **New** button.

a) Create a circle of trust by giving a unique name for the IdP CoT. The Service Provider (in our case Cisco Unified Communications Manager) and the IdP should be in same CoT for SAML SSO to work.

Note You will assign the Service Provider and IdP to be in the same CoT in further steps.

Step 3 Create a SAMLv2 Identity Provider on the server.

a) Choose the **Common Tasks** tab and click the **Create Hosted Identity Provider** button to create a hosted IdP.
b) In the **Existing Circle of Trust** drop-down list, choose the CoT created in Step 2.
c) In the Attributes mapping area, set both **Name in Assertion** and **Local Attribute** values to be uid.
d) Click **Configure**.
e) Choose the **Federation** tab and click on the Hosted Entity Provider you created.
f) Browse to the Assertion Content section and in the Certificate Aliases area enter "test" as the **Signing** field value.

Note This is needed for signing SAML assertions with an alias.

Enable SAML SSO through the OpenAM IdP

SAML SSO Enablement

There are three required tasks and one optional task to enable SAML SSO regardless of the IdP used:

- Create a Circle of Trust
- Configure Cisco Unified Communications Manager for SAML SSO Activation
- Configure the IdP. In the following example we will configure OpenAM.
- [Optional] Verify the SAML SSO Configuration

Tip For SAML SSO to work, the Cisco Unified Communications Manager and the IdP (in this case OpenAM) clocks must be synchronized.

Configure Cisco Unified Communications Manager for SAML SSO Activation

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** user interface.

Step 2 Choose **System** > **SAML Single Sign-On** and the **SAML Single Sign-On Configuration** window opens.

Step 3 To enable SAML SSO on the cluster, click on the **Enable SAML SSO** link.

Step 4 In the **Reset Warning** window, click **Continue**.

Note For SAML SSO, Cisco supports these IdPs:

- Microsoft Active Directory Federation Services (AD FS)
- Open Access Manager (OpenAM)
- Ping Federate

Leave the **SAML Single Sign-On Configuration** window open as you will return to it to save the **IdP Metadata Trust** file and to verify a successful configuration.

Open AM is used in the following example.

What to Do Next

If you have not yet created a Circle of Trust, you can do it now or shift tasks while configuring OpenAM. We recommend that the Circle of Trust be created before you configure OpenAM for SAML SSO.

Related Topics

Supported IdPs, on page 4

Configure OpenAM and Cisco Unified Communications Manager for SAML SSO

This task involves switching actions between the OpenAM IdP server and Cisco Unified Communication Manager nodes.

Before You Begin

Create a Circle of Trust (CoT)

Configure Cisco Unified Communications Manager for SAML SSO

Procedure

Step 1 Log in to the **OpenAM IdP** server and download the metadata trust file.

a) To download the **IdP Metadata Trust** file for the OpenAM IdP server enter one of the following URLs in a browser where *server.example.com* is the FQDN of the OpenAM server and 8443 is the default port number:

- If a single realm is defined on the OpenAM server:

  https://*server.example.com*:8443/openam/saml2/jsp/exportmetadata.jsp.

- If multiple realms are defined on the OpenAM server:

  https://*server.example.com*:8443/openam/saml2/jsp/exportmetadata.jsp?entityid=

  https://*server.example.com*:8443/openam&realm=realm-name

  Note The two lines above (combined), are the complete URL for multiple realms.

Step 2 Access the **Cisco Unified CM Administration** user interface, and perform the following tasks:

a) Save the **IdP Metadata Trust** file and import it to the Cisco Unified Communications Manager node. If the import is successful, the **SAML Single Sign-On Configuration** window opens.

1. In the Import the IdP Metadata Trust File area, click **Browse** to locate the IdP Metadata Trust file.
2. Click the **Import IdP Metadata** button.
   Note If the import is successful, check marks appear announcing that the import is successful for all nodes.
3. Click **Next**.

b) Download the **Server Metadata** for the Cisco Unified Communications Manager nodes in the cluster to a convenient place in the local file system.

1. Click the **Download Trust Metadata File** link, and the **Opening SPMetadata** dialog box opens.
2. Save the compressed files locally.

3 Unzip the Metadata file folder. When the folder is unzipped, there will be one Metadata file for each node in the cluster.

Step 3 Access the OpenAM server user interface and upload the Metadata files for each node in the cluster.

Note If there is no existing CoT, to which the Cisco Unified Communications Manager is to be added, then a CoT must be created before you proceed to the next steps. See the **Create a Circle of Trust** task.

Step 4 Once the CoT has been created, the Cisco Unified Communications Manager node(s) need to be added as Entity providers. To do this:

a) In the OpenAM server user interface, choose the **Federation** tab and in the Entity Providers section click the **Import Entity..** button to import the Cisco Unified Communications Manager metadata file (*server*.xml), where *server* is the name of the Cisco Unified Communications Manager node.

b) Click **Save**.

c) Click on the entity imported in Step 3a, go to the Assertion Processing section, and add a mapping attribute for uid as per the Directory and OpenAM settings.

Note uid is a mandatory attribute that has to be configured on the IdP for a given Service Provider. This is how the Service Provider identifies an Authenticated user. While adding the uid attribute, you must map it to the correct attribute depending on the Directory/User store settings.

d) Repeat steps 3a-3c for any other nodes in the cluster, which need to be SAML SSO enabled.

e) Choose the **Federation** tab and click the **Circle of Trust** you added.

f) In the Entity Providers section, move the IdP(OpenAm server) and any Cisco Unified Communications Manager entities from the Available to the Selected sections.

This assigns the IdP server and Cisco Unified Communications Manager node(s), to the same CoT.

Step 5 In the OpenAM server you will also need to add a user whose credentials match the administrator level user, which were used to enable SSO on the Cisco Unified Communications Manager.

a) Choose **Access Control** > **(Top Level Realm)Subject** and add the administrator level user.

Once the OpenAM server and Cisco Unified Communications Manager node(s) have been configured, you can verify a successful enablement of SAML SSO on the **Cisco Unified CM Administration** user interface.

What to Do Next

Verify the SAML SSO Configuration.

Verify the SAML SSO Configuration

Before You Begin

- You have installed the required server metadata files on the IdP.
- The **SAML Single Sign-On Configuration** window under the **Cisco Unified CM Administration** user interface shows that you have successfully imported the **IdP Metadata Trust** file.

Procedure

Step 1 On the **Cisco Unified CM Administration** user interface, 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, then SAML SSO has been successfully configured.

Reconfigure OpenAM SSO to SAML SSO

Cisco currently offers the following types of Single Sign-On (SSO) solutions:

- OpenAM SSO (Release 8.6 and later)
- SAML SSO (Release 10.0(1) and later)

Cisco collaboration applications favor SAML SSO over the proprietary OpenAM SSO solution because OpenAM is complex in nature and the deployment does not scale as per the customers' requirements.

Note From release 10.0(1) and later, Agent Flow SSO is not compatible with FIPS mode.

To reconfigure OpenAM SSO to SAML SSO, the administrator must create a new federation service and service account. For SAML SSO to work as expected, the service provider and IdP must be in the same Circle of Trust (CoT). The administrator needs to configure a trust relationship between the service provider and IdP. The following steps describe the configuration of OpenAM SSO to SAML SSO on Cisco Unified Communications Manager.

In this case, you continue to use OpenAM as the IdP, however OpenAM must be reconfigured to SAML.

Before You Begin

- Make sure the OpenAM SSO that is deployed using Agent Flow is installed and operational.
- For SAML SSO to work, the Cisco Unified Communications Manager and OpenAM clocks must be synchronized with each other.

Procedure

Step 1 Disable OpenAM Agent Flow mode of operation on all servers where it is enabled by using CLI commands.

Note Refer to the respective Cisco Unified Communications product documents to get the list of the required CLI commands.
You must disable a previously configured OpenAM SSO solution as only one SSO deployment is allowed at a time.

Step 2 Enable SAML SSO on those servers.
Note Refer to the respective Cisco Unified Communications product documents on how to enable SAML SSO.

Step 3 Log in to the OpenAM server user interface.

Step 4 Choose the **Federation** tab and under Circle of Trust, click **New**.

Step 5 Create a CoT by entering a unique name for the IdP Circle of Trust.

Step 6 To create a hosted IdP, choose the **Common Tasks** tab and click **Create hosted Identity Provider**.

Step 7 Use the default values for other parameters and click **Save**.
Note You can view the circle of trust that you created in the Circle of Trust section.

Step 8 Choose the **Federation** tab and under the Entity Providers section, click the **Hosted Identity Provider** you created.

Step 9 Choose the **Assertion Content** tab and under the Certificate Aliases section, enter <test> as an alias for signing SAML assertions in the **Signing** field .

Step 10 Choose the **Federation** tab, and in the Entity Providers section, click **Import Entity**.

Step 11 Upload the Cisco Unified Communications Manager metadata file (sp.xml), and click **Save**.
Note The metadata file upload fails if the metadata is signed. In such cases, add the Cisco Unified Communications Manager tomcat certificate to openAMKeystore. Follow the procedure below.

1. Download the tomcat certificate (tomcat.pem) from the **Cisco Unified Communications Manager OS Administration** page and the upload the certificate to a location in OpenAM server. For example, `/temp/tomcat.pem`
2. Run the following command in OpenAM:
   keytool -import -v -alias *aliasname* **-keystore**
   /root/openam/openam/keystore.jks -trustcacerts -file
   location_of_cucm_tomcat_cert
3. Enter the password as <changeit>.
4. A dialog box appears asking whether you trust the certificate, click **Yes**.
   The following message is displayed:
   ```
   Certificate was added to keystore
   [Storing /root/openam/openam/keystore.jks]
   ```
5. Restart the tomcat in OpenAM and try to upload the sp.xml metadata file again.
6. Choose **File** during Entity provider upload.

Note Cisco Unified Communications Manager supports metadata upload only through the File option.

Step 12 Choose the entity imported in Step 10.

Step 13 Choose the **Assertion Processing** tab and add a mapping attribute for uid as per the Directory and OpenAM settings.
Note While adding the uid attribute, map it to the correct attribute depending on the Directory/User store settings. For example, you can enter uid=sAMAccountName or uid=mail or uid=uid.

Step 14 Choose the **Federation** tab, and click **Circle of Trust**.

Step 15 To assign the IdP and the Cisco Unified Communications Manager to be in the same CoT: in the Entity Providers area, move the IdP (OpenAM server) and the Cisco Unified Communications Manager entities from the **Available** section to the **Selected** section.
The OpenAM server is successfully configured as IdP.

INDEX

A

Assertion Consumer Service (ACS) 2

C

Certificate Authority (CA) 10
  Private CA 10
  Public CA 10
certificate management 10
Certificate Signing Request (CSR) 10
certificate validation 10
Circle of Trust 2
Cisco Prime Collaboration 4
Cisco Unified Communications Manager 4
Cisco Unity Connection 4
client 2
Common Names (CN) 10
CoT 1, 11
  certificate 11
  metadata 11
  setup 11
  steps 11
CUCM 10, 16

D

Domain Name System (DNS) 9

I

Identity Provider (IdP) 1
IdP 2, 4, 9, 16
  AD FS 4
  OpenAM 4
  Oracle Access Manager 4
  Ping Federate 4
IM and Presence 4

L

LDAP 2, 4

M

migration 16
  Circle of Trust (CoT) 16
  Fully Qualified Domain Name (FQDN) 16

N

Network Time Protocol (NTP) 9
NTP 9

S

SAML 1, 2, 5
  Assertion 2
  Assertion Attribute statements 5
    Authentication statements 5
  binding 5
  profile 5
  protocol 5
  Request 2
  SAML SSO 1
SAML 2.0 5
SAML SSO 2, 4, 5, 9
service provider 1, 2, 9
Service provider 2
SSO 16
  OpenAM 16
  SAML 16
Subject Alternative Names (SAN) 10

T

third-party 4

U

uid 11
Unified Communications 10
Unified Communications Manager 16

W

web browser 3