SAML-Based SSO Solution

- About SAML SSO Solution, on page 1
- Single Sign on Single Service Provider Agreement, on page 2
- SAML-Based SSO Features, on page 2
- Basic Elements of a SAML SSO Solution, on page 2
- Cisco Unified Communications Applications that Support SAML SSO, on page 3
- SAML SSO Support for Cisco Unified Communications Manager Web Interfaces, on page 4
- Software Requirements, on page 6
- Selecting an Identity Provider (IdP), on page 6
- SAML Components, on page 7
- SAML SSO Call Flow, on page 8
- Java Requirements for SAML SSO Login to RTMT via Okta, on page 10

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.

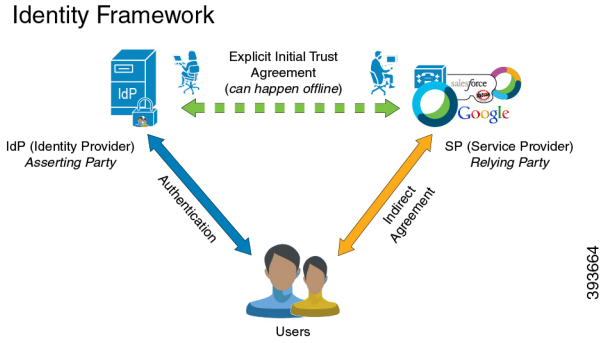
Basic Elements of a SAML SSO Solution

- 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.



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.

Note If you only enable SSO and not the Recovery URL, and an authenticating user has insufficient access privileges they will only receive a 403 Error (Access Denied Response). However, if you enable Recovery URL, the error occurrence will redirect an authenticating user to the Recovery URL page.

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, 3.0, 4.0, and 5.0
- Microsoft Azure
- 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:

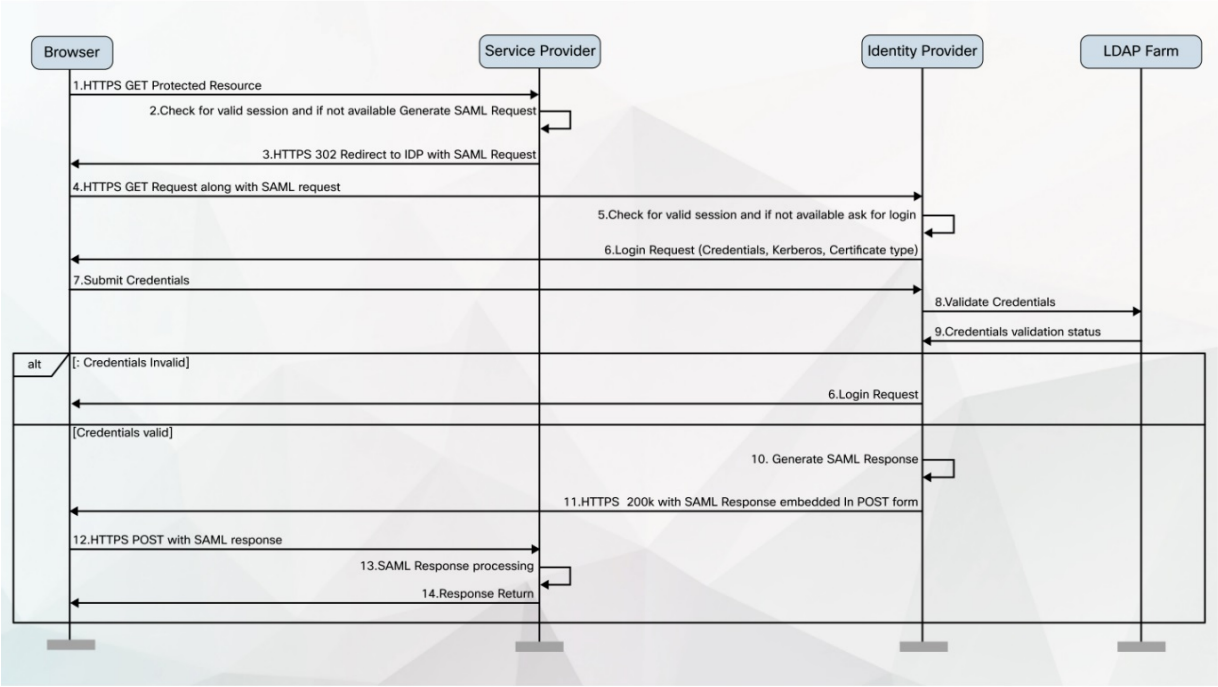
  - HTTP Redirect (GET) Binding
  - HTTP POST Binding

- 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.

Figure 1: 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 and VOS products use the Assertion Consumer Service Index URL, which is compliant with SAML 2.0 standards. **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 is responsible for resource authorization. For example, users may be authenticated successfully by the IdP, but still may not be able to login to the Cisco Unified CM Administration interface unless they have administrator role permissions, as configured on Cisco Unified Communications Manager. **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.

Java Requirements for SAML SSO Login to RTMT via Okta

If you have SAML SSO configured with Okta as the identity Provider, and you want to use SSO to log in to the Cisco Unified Real-Time Monitoring Tool, you must be running a minimum Java version of 8.221. This requirement applies to 12.5(x) releases of Cisco Unified Communications Manager and the IM and Presence Service.