SAML-Based SSO Solution

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

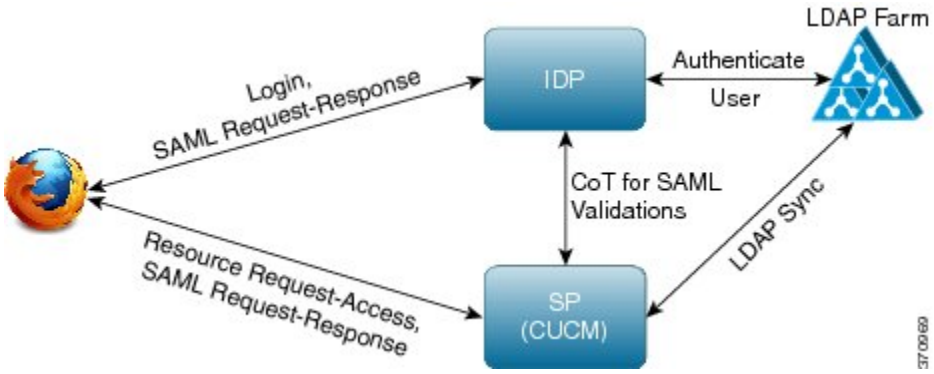
- Client (the user's client): This is a browser-based client or a client that can leverage a browser instance for authentication. For example, a system administrator's browser.
- Service provider: This is the application or service that the client is trying to access. For example, Cisco Unified Communications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

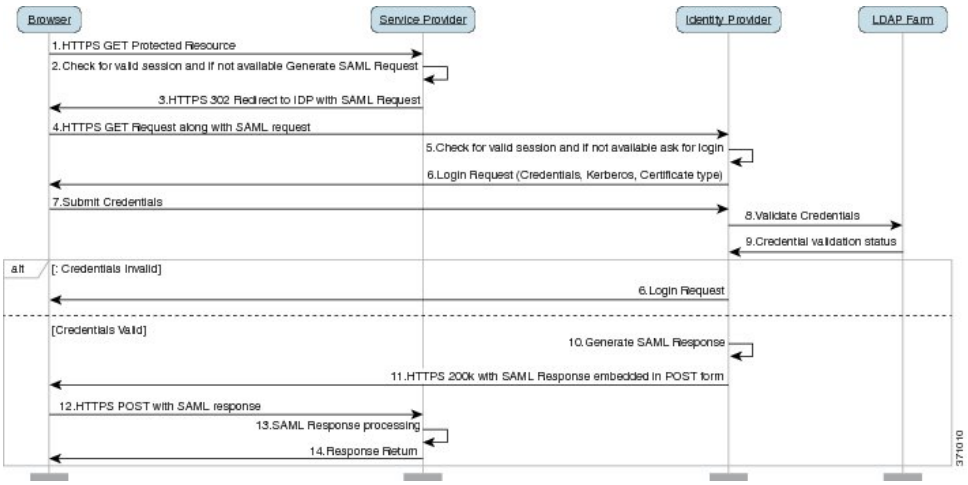
- SAML profile: A SAML profile provides a detailed description of the combination of SAML assertions, protocols, and bindings to support well-defined use cases. Unified Communications 10.0 supports the SAML 2.0 Web Browser SSO Profile.

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.