Single Sign-on

Overview

In a standard configuration, the sign in name and password of a user are independent from the authentication credentials used by their company or organization. This requires users to remember another set of sign in credentials. Additionally, Organization Administrators are required to manage a separate set of user accounts.

Single sign-on also permits companies to use their on-premise single sign-on system to simplify the management of Cisco WebEx Administration. With single sign-on, users securely sign in to the application using their corporate sign in credentials. The user's sign in credentials are not sent to Cisco WebEx, protecting the user's corporate sign in information.

As a single sign-on configuration option, user accounts can be automatically created the first time a user signs in. Single sign-on also prevents users from accessing Cisco WebEx application if their corporate sign in account has been deactivated.

The Cisco WebEx application supports single sign-on systems based on the industry standard Security Assertion Markup Language SAML2 and WS-Federation protocol.

Using SSO with the Cisco WebEx and Cisco WebEx Meeting Applications

One of the goals of the Cisco WebEx services is to provide comprehensive management of user identities for an organization. User identity management involves providing secure mechanisms for authentication and authorization. These mechanisms facilitate ease of use and policy controls based on the user’s role and group affiliations inside the organization.

Federated Single sign-on standards such as SAML2 (Security Assertion Markup Language) and WS-Federation provide such secure mechanisms for authentication. SAML-compliant identity management systems send

SAML assertion to Cisco WebEx services. A SAML assertion is an XML document containing trusted statements about a subject. Typically, these trusted statements include information such as user name, email and other profile information. SAML assertions are digitally signed to ensure their authenticity.

Normally, enterprises deploy a federated Identity and Access Management system (IAM) to manage user identities. These IAM systems use SAML, and WS-Federation standards for user identity management activities. Some of the more prominent enterprise-class IAM systems include CA SiteMinder, Ping Federate, and Windows Active Directory Federation Services (ADFS). These IAM systems form part of an organization's corporate intranet which handles the user authentication and single sign-on requirements for employees and partners. IAM systems use the SAML or WS-Federation protocols to interoperate with partner websites outside their firewalls. Customers, partners, and vendors can utilize their IAM systems to automatically authenticate their users to Cisco WebEx services. This will increase efficiency as users are not required to recall their username and password to use Cisco WebEx services.

Additionally, employees leaving an organization do not have to be explicitly disabled in external administration tools. As soon as they are removed from the customers IAM system, they are not able to authenticate against any of the Cisco WebEx services.

Note Contact your Customer Success Manager to enable Single sign-on for Cisco WebEx Messenger.

Single Sign-on Requirements

The following system requirements are required to implement federated single sign-on for your Cisco WebEx organization. These system requirements are the same for Cisco WebEx Messenger and the Cisco WebEx Meeting applications.

Item	Requirement	Notes
Identity and Access Management (IAM) system	Any IAM that conforms to SAML versions (for Cisco WebEx Meeting only) 2.0 or WS-Federation 1.0 standard.	Customers can develop their own SAML-compliant IAM system using programming libraries such as OpenSAML or purchase commercial third party IAM systems such as Ping Federate, CA SiteMinder, Microsoft Windows Server ADFS, Oracle Identity Federation/OpenSSO, Novell Identity Manager and IBM Tivoli Federated Identity Manager.
X509 Certificate has public key, digitally sign uses private key	From trusted organizations like VeriSign and Thawte in the PEM format.	Alternatively, customers can serve their own X.509 certificates developed in house using self-signed certificates.

Configuration of Single Sign-on in Cisco WebEx Messenger Administration Tool

The Cisco WebEx Administration Tool allows the Organization Administrator to configure Single sign-on settings and modify the security setting and certificates for your Cisco WebEx Organization. Options are displayed based on organization settings set by the Administrator. Not all options are displayed at all times.

- Select **Federated Web SSO Configuration** to display the dialog for an administrator whose organization has turned on single sign-on.
- Select **Organization Certificate Management** to display the dialog for an administrator whose organization has turned on single sign-on or is a "Delegated Authentication" administrator. Used to manually import, validate, or remove X.509 certificates, Organization Certification Management is a management tool for Organization Administrators.
- Select **WebEx Certificate Management** to display the dialog for an administrator whose organization has turned on single sign-on. Used as a management tool for Organization Administrators to create service provider certificates, this tool is used for SP-initiated situations. A self-signed certificate by Cisco WebEx is generated and requires upload to the IAM system. Certificates are generated:
  - for signing the AuthnRequest
  - for SAML assertion encryption
  - to enable Single Logout

  A self signed certificate or a certificate authority will have been previously generated and made available for import. Administrators can select which to apply to the organization.
- Select **Partner Web SSO Configuration** to display the dialog for an administrator whose organization is "Delegated Authentication. Partner delegation allows administrators to setup up a single user name and password authentication sign on page for partner applications. Administrators should use this functionality to increase security and reduce multiple sign on and password requirements, eliminating the need for users to track multiple sign on credentials.
- You can also set SAML 2.0 configurations. Attributes are displayed in the following table:

Attribute	Required (Yes/No)	Usage
uid	Yes	
firstname	Yes	
lastname	Yes	
email	Yes	
groupid	No	Supports only create, not update
updateTimeStamp	No, but recommended	Supports long value, UTC time format, & LDIF time format

Attribute	Required (Yes/No)	Usage
displayName	No	
companyName	No	
businessFax	No	
streetLine1	No	
streetLine2	No	
city	No	
state	No	
zipcode	No	
jobTitle	No	
mobilePhone	No	
businessPhone	No	
employeeid	No	
imloggingenabled	No	When an organization has IMLogging enabled, and if no such attribute exists, it would be set to false.
imloggingendpointname	No	When an organization has IMLogging enabled, and if no such attribute exists, it would be set to wbx_default_endpoint.
ISOCountry	No	2-letter ISO country code
upgrade site	No	If there is a not-null 'upgradesite' attribute, the action will correspond with the (enabled/disabled) auto account creation and auto account update features. If the 'upgradesite' attribute is not provided or the value is empty, no action is required.

Note The Allow Connect account username and password login via CAS API checkbox is selected in a transition phase when an organization is moving their authentication mechanism from "username/password store in the cloud" to SSO with an IdP. It allows the organization to move gradually over to SSO.

Configure Federated Web SSO

Procedure

Step 1 Select the **Configuration tab** > **System Settings > Security Settings**.

Step 2 Select **Federated Web SSO Configuration** .

Step 3 From the **Federation Protocol** drop down, select the federation protocol **SAML 2.0**.
The fields displayed in the window vary based on the selected federation protocol. By default, the configuration fields for SAML 2.0 is displayed each time the **Federated Web SSO Configuration** window opens.

Step 4 **Select Import SAML Metadata** to open the **Federated Web SSO Configuration - SAML Metadata** dialog box.

Step 5 Perform one of the following:

- Navigate to and import the SAML Metadata file to autofill the federated Web authentication fields.
- Select **Import**, **Back** to complete the import. Imported metadata fields include:
  - AuthnRequestSigned Destination
  - Issuer for SAML (Idp ID)
  - Customer SSO Service Login URL
- Enter the appropriate information for each field.
  See the Related Topics section.

Step 6 After the SAML Metadata file has been successfully imported, verify that the relevant fields in the **Federated Web SSO Configuration** window have been populated.

Related Topics

Federated Web SSO Settings, on page 6

Federated Web SSO Settings

Field	Description
SSO Profile	SP Initiated - When a user visits a service provider (SP) site and first accessing resources that do not require special authentication or authorization. In an SAML-enabled deployment, when they subsequently attempt to access a protected resource at the SP, the SP will send the user to the IdP with an authentication request in order to permit the user to sign in. AuthnRequest Signed Destination - When selected, a WebEx certificate and destination must be specified. This destination address must match the authnRequest signed configuration in the IAM.
	IdP Initiated Target page URL Parameter - If the user visits Cisco WebEx service (SP), SP sends the user to IDP without an authentication request.
WebEx SAML Issuer (SP ID)	The URI identifies the Cisco WebEx Messenger service as an SP. The configuration must match the settings in the customer Identity Access Management. The default value is http://www.webex.com.
Issuer For SAML (IdP ID)	A URI uniquely identifies the IdP.The configuration must match the settings in the customer IAM.
Customer SSO Service Login URL	URL for your enterprise's single sign-on service. Users in your enterprise will typically sign in via this URL.
You can export an SAML metadata WebEx SP configuration file: Exported metadata fields include: • AuthnRequestSigned Destination • Issuer for SAML (Idp ID) • Customer SSO Service Login URL	
NamedID Format	This field must match the IAM configuration. The following formats are supported: • Unspecified (default) • Email address • X509 Subject Name • Entity Identifier • Persistent Identifier
AuthnContextClassRef	The SAML statement that describes the act of authentication at the identity provider.This field must match the IAM configuration.

Field	Description
Default WebEx Target page URL	Optional. Upon authentication, displays a target page assigned for the web application only. The request does not contain a RelyState parameter.
Single Logout for Web Client	Check to require a sign out and set the log out URL. **Note:** This option is only applicable to the web IM application.
Auto Account Creation	Select to create a user account. UID, email, and first and last name fields must be present in the SAML assertion.
Auto Account Update	Specify the "updateTimeStamp" attribute in the SAML assertion and check this field to update an existing user account. The "updateTimeStamp" value is the last update time of a user's profile in the customer's Identity store. For example, in Active Directory, the "whenChanged" attribute has this value. If "updateTimeStamp" is not in the attribute, the user profile would not be updated since the last update. It updates the first time when the user profile is updated via Auto Account Update or Auto Account Creation. Unchecked indicates no updates will occur.
Remove uid Domain Suffix for Active Directory UPN	The Active Directory domain part will be removed from the UPN when selected. Cisco WebEx Messenger uid's require the email domain; therefore, when this field is checked, it will cause an error. In this case, use "ssoid" to identify the user. The default is unchecked for SAML 2.0 and WS-Federation 1.0.

Configure WS Federation

After the SAML Metadata file has been successfully imported, verify the relevant fields in the **Federated Web SSO Configuration** dialog box have been populated.

Procedure

Step 1 From the **Federation Protocol** drop down list, select the federation protocol **WS-Federation 1.0**. The fields displayed in the **Federated Web SSO Configuration** dialog box vary based on the selected federation protocol.

Step 2 Enter the following additional information:

- WebEx Service URI: The URI identifies the Cisco WebEx Service relying party.
- Federation Service URI: The URI identifies the enterprise's single sign-on service (IdP).

- Customer SSO Service Login URL: URL for your enterprise's single sign-on service. Users in your enterprise will typically sign in via this URL. Depending on the single sign-on Profile, the IdP-Initiated login URL and SP-Initiated sign in URL would be set accordingly to match IdP settings.

Step 3 Select **Save** to save the Federated Web single sign-on Configuration details and return to the **SSO Related Options** window.

Configure Organization Certificate Management

Procedure

Step 1 Select **Organization Certificate Management** to display the available certificates.
Certificates are limited to a maximum of three and only one can be active at any given time. Previously imported X.509 certificates are displayed.

Step 2 Select a certificate link in the **Certificate Alias** column to view certificate details and, optionally, select **Remove** to remove the certificate.

Step 3 Select **Import New Certificate**.
The **Organization Certificate Management** window appears.

Step 4 In the **Organization Certificate Management** window, enter your company's Cisco WebEx Organization name in the **Alias** field.

Step 5 Select **Browse** to navigate to the X.509 certificate.
The certificate should be in a cer or crt file format. Only certificates with 1024, 2048 or 4096 encryption bits and RC4-MD5 algorithms are supported.

Step 6 Select **Import** to import the certificate.
If the certificate is not according to the format specified for an X.509 certificate, an error is displayed.

Step 7 Select **Close**.

Step 8 Select **Save** to save your newly imported organization certificate and return to the **SSO Related Options** screen.

Configure WebEx Certificate Management

Procedure

Step 1 Select **WebEx Certificate Management** to display previously generated Cisco WebEx certificates.

Step 2 To generate a new certificate, select **Generate New Certificate**.
New certificates are typically generated when an existing certificate is about to expire.

Step 3 In the **WebEx Certificate Management** window, enter the following information:

- **Alias:** An alias that identifies the WebEx Certificate.
- **Val:** The number of days the WebEx Certificate is valid. A WebEx Certificate is valid for a minimum of 90 days and maximum of 3652 days.

Step 4 Select a Certificate Alias to view the complete details of the generated certificate.

Step 5 In the generated certificate screen, select:

- **Remove**: to delete the certificate. Active certificates cannot be removed.
- **Export**: to export and save the certificate as a .cer file to your computer.

Step 6 Select **Close** to return to the **WebEx Certificate Management** window.

Step 7 Select the **Active** option to apply this (newly-generated) WebEx Certificate as the active certificate for single sign-on related authentication purposes.

Step 8 Select **Save** to save your WebEx Certificate changes and return to the **SSO Related Options** window.

Step 9 Import the active Cisco WebEx certificate to the IdP.

Partner Delegated Authentication

Partner delegation allows administrators to setup up a single user name and password authentication sign on page for partner applications. Administrators should use this functionality to increase security and reduce multiple sign on and password requirements, eliminating the need for users to track multiple sign on credentials.

Requirements for partner delegated authentication

A trust must be established between a customer and a partner. The partner acts on behalf of its customer's user to log on to the Cisco WebEx service via the partner route. Partner Delegated Authentication consists of the following attributes used to build trusted and consented relationships:

- Customer and Cisco WebEx service (trust)
- Partner and Cisco WebEx service (trust)
- Customer and Partner (trust and consent)

Configure Partner Delegated Authentication

Procedure

Step 1 Use **WebEx Certificate Management** to upload the certificate.

Step 2 Use **Partner Web SSO Configuration** to configure SAML 2.0 settings.

Step 3 Select **Partner Delegated Authentication** to display the dialog for an administrator whose organization is not “Delegated Authentication”.

Step 4 Trust the partner to act as member or member plus an organization administrator

Step 5 Set the corresponding **NameID field**.

Configure Partner Web Single Sign-on

Procedure

Step 1 Select **Partner Web SSO Configuration**.

Step 2 If you have not imported SAML configurations, select **Import SAML Metadata** to open the Partner Web Single sign-on configuration - SAML metadata dialog box.
For more information, see Configure Federated Web SSO, on page 5