SAML SSO Configuration

Overview of Single Sign-On

Federated single sign-on (SSO) standards such as SAML 2.0 provide secure mechanisms for passing credentials and related information between different web sites that have their own authorization and authentication systems. SAML 2.0 is an open standard developed by the OASIS Security Services Technical Committee.

The SAML 2.0 protocol has seen significant success, gaining momentum in financial services, higher education, government, and other industry segments. SAML 2.0 support has been implemented by all major web-access management vendors. The U.S. Government General Services Administration (GSA) requires all vendors participating in the U.S. E-Authentication Identity Federation program to be SAML 2.0-compliant.

SAML 2.0-compliant web sites exchange user credential information using SAML assertions. A SAML 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.

Many large enterprises have deployed federated Identity and Access Management (IAM) and Identity Provider (IdP) systems, such as Ping Identity Ping Federate, CA SiteMinder, Open AM, and Windows ADFS 2.0 on their corporate intranets. These IAM and IdP systems handle the user authentication and SSO requirements for employees and partners. IAM and IdP systems use the SAML protocols to interoperate with partner websites outside their firewalls. Users can utilize their IAM and IdP systems to automatically authenticate their users to Cisco WebEx meeting services. This increases efficiency because users do not have to remember their usernames and passwords to start or join meetings on their Cisco WebEx sites.

Note WebEx Meetings Server supports SAML 2.0 IdPs only. It does not support IdPs based on the older SAML 1.1 and WS-Federate standards. This restriction stands in contrast to the cloud-based Cisco WebEx meeting services which continue to support SAML 1.1 and WS-Federate. The following is a list of SAML 2.0 IdPs that have been validated to work with Cisco WebEx Meetings Server:

- Microsoft ADFS 2.0 (a free add-on to Microsoft Active Directory 2010)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Because SAML 2.0 is an open standard, other SAML 2.0 IdPs might also operate with Cisco WebEx Meetings Server. However, other SAML 2.0 IdPs have not been tested by Cisco. It is therefore the user's responsibility to make any such integration operational.

Benefits of Single Sign-On

Single sign-on (SSO) can benefit you in the following ways:

- Simplified user authentication—Out of the box, Cisco WebEx Meetings Server requires users to sign in using email addresses and self-selected passwords specific to the Meetings Server system. Users select their passwords upon activating their Meetings Server accounts. While this approach works well for most small- and mid-sized organizations, larger organizations prefer user authentication using corporate credentials—that is, Active Directory—for enhanced security. You can accomplish this goal by using SAML 2.0 SSO.

  Note One added security benefit of SSO is that the corporate password is never actually sent to or stored in Cisco WebEx Meetings Server after the user authenticates successfully.

- Simplified user management—Large organizations with changing workforces due to normal attrition prefer to automate the process of user management when integrating with WebEx Meetings Server. This means automating the following:
  - User account creation when employees join the organization
  - User account updates when employees take on different roles within the organization
  - User account deactivation when employees leave the organization

  You can achieve automation for these events by configuring **Auto Account Creation** and **Auto Account Update** in the SSO section of the Cisco WebEx Meetings Server Administration site. We recommend that you turn on these features if they are also supported by your SAML IdPs. User accounts are automatically created and updated "on demand" when users authenticate successfully, thereby eliminating the need to create users manually using Cisco WebEx Administration. Similarly, users can no longer sign into their accounts after they leave the organization because the SAML 2.0 IdP blocks those users from signing in after they are removed from the SAML 2.0 IdP user database, which is usually a proxy for the underlying corporate directory.

Overview of Setting Up SAML 2.0 Single Sign-On

Important Unless you or someone in your organization has experience with SAML 2.0 single sign-on (SSO), we recommend that you engage the services of a qualified Cisco AUC partner or Cisco Advanced Services. We make this recommendation because SAML SSO configuration can be fairly complicated.

Review these general steps for setting up SAML 2.0 SSO:

1. Ensure that your SAML 2.0 SSO infrastructure is in place and is integrated with your corporate directory. This implies setting up SAML 2.0 IdP software and the SSO authentication website. The authentication website is a portal where users enter their corporate credentials.
2. Ensure that users can access the SSO authentication website. This step is important because, as part of the sign-in process, Cisco WebEx Meetings Server redirects users to this authentication website.

Note If your Cisco WebEx Meetings Server system is enabled for public access—allowing users to sign in and join meetings from the Internet—then it is critical to ensure that the SSO authentication website is also accessible from the Internet. This usually implies deploying the SAML 2.0 IdP in your DMZ. Without this extra step, users will see "404 site not found" errors when signing in to Cisco WebEx Meetings Server from the Internet.

3. Connect WebEx Meetings Server to the SAML 2.0 IdP using both of these methods:
    - Select **Settings** > **Security** > **Federated SSO** on your Cisco WebEx Meetings Server Administration site.
    - Follow the instructions in your SAML 2.0 IdP documentation. Note that these instructions vary from vendor to vendor and might even change from version to version of the SAML 2.0 IdP. This is another reason to ensure that you contact a qualified Cisco AUC partner or Cisco Advanced Services to help you implement the solution.

      Note Do not use the instructions found on the Cisco Developer Network to set up SAML 2.0 IdPs because those instructions are intended for cloud-based Cisco WebEx meeting services and therefore do not work optimally with Cisco WebEx Meetings Server.

SAML 2.0 Single Sign-On Differences Between Cloud-Based WebEx Meeting Services and WebEx Meetings Server

While the cloud-based Cisco WebEx meeting services employ unique user IDs when creating users accounts, Cisco WebEx Meetings Server uses email addresses as the basis for creating user accounts. This has the following important implications for SAML 2.0 single sign-on (SSO):

- It is mandatory for the SAML Assertion to carry the email address in the NameID field. Without this step, user authentication and account creation fail because Cisco WebEx Meetings Server does not permit the creation of user accounts without an associated email address.
- The cloud-based Cisco WebEx meeting services permit removal of the email domain, such as "@cisco.com," from the UPN (User Principal Name) when auto account creation is turned on. This results in the creation of a user account that resembles a user ID. Because WebEx Meetings Server uses a complete email address to create user accounts, you cannot remove the email domain from the UPN.

In practice, you can initially deploy Cisco WebEx Meetings Server without SAML 2.0 SSO and turn on SSO later. Doing so has the following important effects on the user authentication, auto account creation, and auto account update features:

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
You have not turned on SSO. User accounts were created in the system.	Users sign in using their email addresses and self-selected passwords.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
Next you turn on SSO. Users with existing accounts sign in to their WebEx site, WebEx Productivity Tools, or the Cisco WebEx Meetings app on their mobile devices.	Users are redirected to the SAML 2.0 IdP authentication website and asked to sign in using their corporate credentials, instead of email addresses and self-selected passwords. The users sign in successfully because they are recognized by the SAML 2.0 IdP as valid users. If they are not valid users, they will be informed by the SAML 2.0 IdP that they cannot use WebEx Meetings Server or that they are invalid users.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
SSO is turned on. Users do not have existing accounts in the system.	Same as the previous scenario.	User accounts in Cisco WebEx Meetings Server are created "on-demand" after users sign in. Prerequisite: The SAML Assertion contains a valid email address in the NameID field.	Users do not have existing accounts in the system. They can sign in but will not be able to use Cisco WebEx Meetings Server. The easiest way to remedy this situation is to do one of the following: • Leave AAC on. • Before users sign in, manually create user accounts using "CSV File Import" or "Create user" from the Cisco WebEx Administration site.	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
SSO is turned on. Users previously signed in using SSO and are now signing in again.	Same as the second scenario.	N/A	N/A	Existing user accounts are automatically updated with any changes to the user credentials (usually first name or last name) as long as the NameID remains unchanged.	N/A
Subsequently you turn off SSO. This is an uncommon scenario because customers tend to leave SSO on after turning it on. Users previously signed in using SSO and are now signing in again.	If users enter their corporate credentials, they cannot sign in because WebEx Meetings Server expects them to enter their email addresses and self-selected passwords. In this situation, educate the users about resetting the self-selected passwords in their WebEx accounts and allow them enough time to act before you turn off SSO. After resetting their passwords, users can sign in using their email addresses and self-selected passwords.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
Special case: A user is also a system administrator. Scenario A: The user signs in to the WebEx Site. Scenario B: The user signs in to the Cisco WebEx Administration site.		Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	Scenario A: Same results as the previous scenario Scenario B: In contrast to the behavior on a WebEx site, when the user signs in to the Cisco WebEx Administration site, he or she is always prompted to enter the email address and self-selected password. In other words, SSO has no effect when you sign in to the Cisco WebEx Administration site. This is a security measure built into the product because of the need to ensure that systems administrators can always sign in to the Cisco WebEx Administration site. If the Cisco WebEx Administration site also supports SSO, then malfunctions in				

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	the SAML 2.0 IdP or a loss of network connectivity between Cisco WebEx Meetings Server and the SAML 2.0 IdP might result in a situation in which systems administrators can no longer sign in and manage the product. This is the reason why SSO is not supported for the Cisco WebEx Administration site.				