End User SAML SSO

End User SAML SSO Configuration

End user or federated SSO is a standard that allows products to meet customer compliance requirements, reduce the total cost of ownership, and improve end user experience. The foundation for this support in the collaboration products has been introduced in the 10.0 and 10.5 releases. This allows administrators to configure the infrastructure in preparation for end user clients such as Cisco Unity Connection and Cisco Jabber, which is rolling out support for users with release 10.5 in the second half of 2014.

Once an Administrator enables this feature for users it will allow users in a Cisco collaboration application to log in to supported applications with their corporate username and password. If the Cisco application is accessed by way of a browser the user can use the same corporate username and password to log in. If the user has already logged in to another corporate application in that same browser they should be able to access the application without having to provide a username and password. All of these features are available within the customer network or accessible by way of a VPN.

The supported products are:

Product	Supports End User SAML SSO from Release...	More Information
Cisco Unified Communications Manager	10.5	Click here
IM and Presence Service	10.5	Click here
Cisco Unity Connection	10.5	Click here
WebEx Meeting Center	Cloud	Click here
WebEx Connect and Messenger	Cloud	Click here
Cisco WebEx Meetings Server	1.5 and 2.0	Click here

The supported end user clients are:

Product	Release	More Information
WebEx IOS	Available with all releases	Click here
WebEx Android	Available with all releases	Click here
WebEx Connect	Available with all releases	Click here
WebEx Messenger	Available with all releases	Click here
Jabber for Windows	10.5	Available in the second half of 2014
Jabber IOS	10.5	Available in the second half of 2014
Jabber for Android	10.5	Available in the second half of 2014
Jabber for Mac	10.5	Available in the second half of 2014

Note

- When deploying Cisco Jabber with Cisco WebEx Meeting Server, Unified Communications Manager and the WebEx Meeting Server must be in the same domain.
- When Cisco Jabber is running with SSO on a Mac, Jabber cannot automatically set a cookie once authorized for Jabber services. Mac behavior, by default, only allows cookies for sites the user navigates to. Each time Jabber needs to check for authentication it has to go to the IdP.
- The SAML Assertion must include the email address for WebEx; the SAML Schemas should be aligned to cover that.
- To trigger OAuth timer expiration correctly, ensure that the OAuthTokenExpiry value on Unified Communications Manager is greater than the WebsessionApp expiry value on Tomcat.