

Last Modified: November 21, 2014

WebEx is an easy to use cloud-based web conferencing combines file and presentation sharing with voice, HD video and Meeting Spaces.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Cisco WebEx.
- Obtain the ACS URL information from Cisco WebEx.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

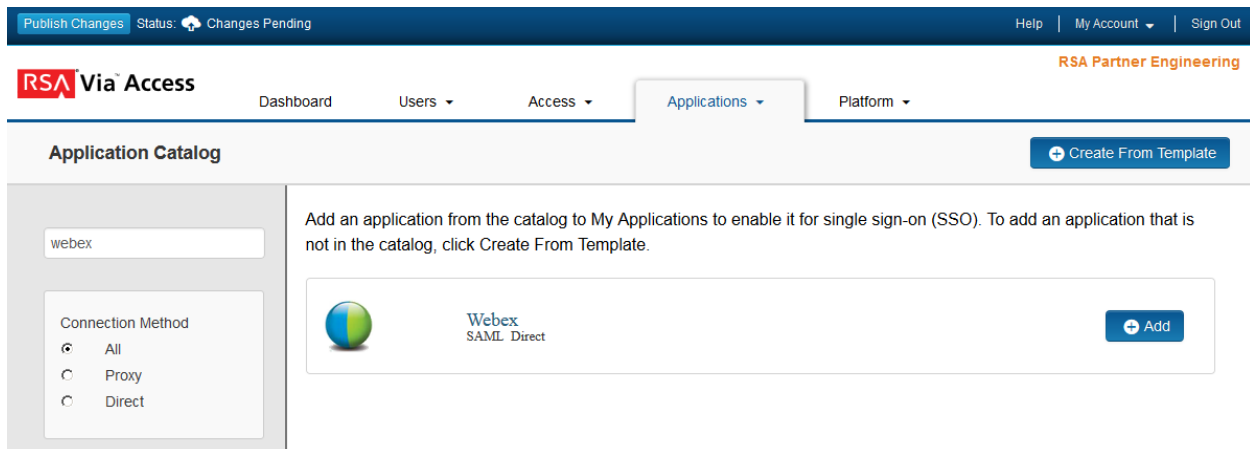
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure WebEx to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for **Webex** and click **+Add**.



The screenshot shows the RSA SecurID Access Administration Console interface. At the top, there is a navigation bar with 'Publish Changes', 'Status: Changes Pending', 'Help', 'My Account', and 'Sign Out'. Below this is the 'RSA Via Access' logo and a navigation menu with 'Dashboard', 'Users', 'Access', 'Applications', and 'Platform'. The 'Applications' tab is selected, leading to the 'Application Catalog' page. On the left, there is a search bar with 'webex' entered and a 'Connection Method' filter with options: 'All' (selected), 'Proxy', and 'Direct'. On the right, there is a message: 'Add an application from the catalog to My Applications to enable it for single sign-on (SSO). To add an application that is not in the catalog, click Create From Template.' Below this message, a card for 'Webex SAML Direct' is displayed with a globe icon and an '+ Add' button. A '+ Create From Template' button is also visible at the top right of the catalog area.

3. On the Basic Information page, specify the application name and click **Next Step**.



Note: The following IDP -initiated configuration works for both IDP -initiated and SP-initiated connections.

4. In the Connection URL replace <COMPANY_ACCOUNT> with your WebEx subdomain.
https://<COMPANY_ACCOUNT>.webex.com
5. Choose **IDP -initiated**.

Connection URL

https://<COMPANY_ACCOUNT>.webex.com

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

No certificate loaded

6. Scroll down to **SAML Identity Provider (Issuer)** section.

SAML Identity Provider (Issuer)

Identity Provider URL

https://pe110.pe-lab.com/IdPServlet?idp_id=webex

Issuer Entity ID

Default (idp_id): webex

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

private.key

Include Certificate in Outgoing Assertion

No certificate loaded

- a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
- b. Take note of the **Issuer Entity ID**.
- c. Select **Choose File** and upload the private key.

7. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL

`https://<COMPANY_ACCOUNT>.webex.com/dispatcher/SAML2AuthService.do?siteurl=<COMPANY_ACCOUNT>`

Audience (Service Provider Entity ID)

`http://www.webex.com`

- a. In the **Assertion Consumer Service (ACS) URL** field, replace <COMPANY_ACCOUNT> with your company's WebEx site subdomain.
 - b. In the **Audience (Service Provider Entity ID)** field, enter the Entity ID to match the configured value from the Service Provider.
8. Scroll down to **User Identity** section. Set the Identifier Type to **Email** and Property to **mail**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

9. Click **Next Step**.

10. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


11. Click **Next Step**.

12. On the **Portal Display** page, select **Display in Portal**.

13. Click **Save and Finish**.

14. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

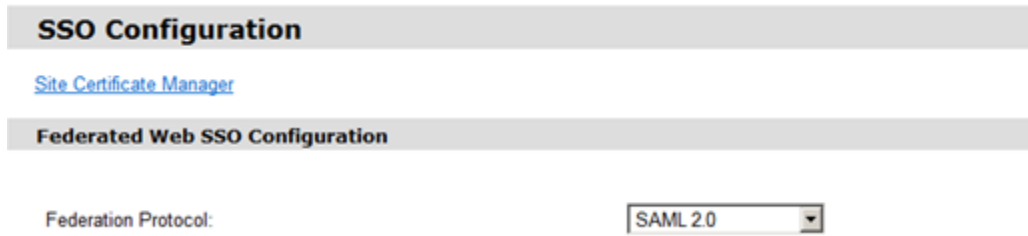
Next Steps

[Configure WebEx to Use RSA SecurID Access as an Identity Provider](#)

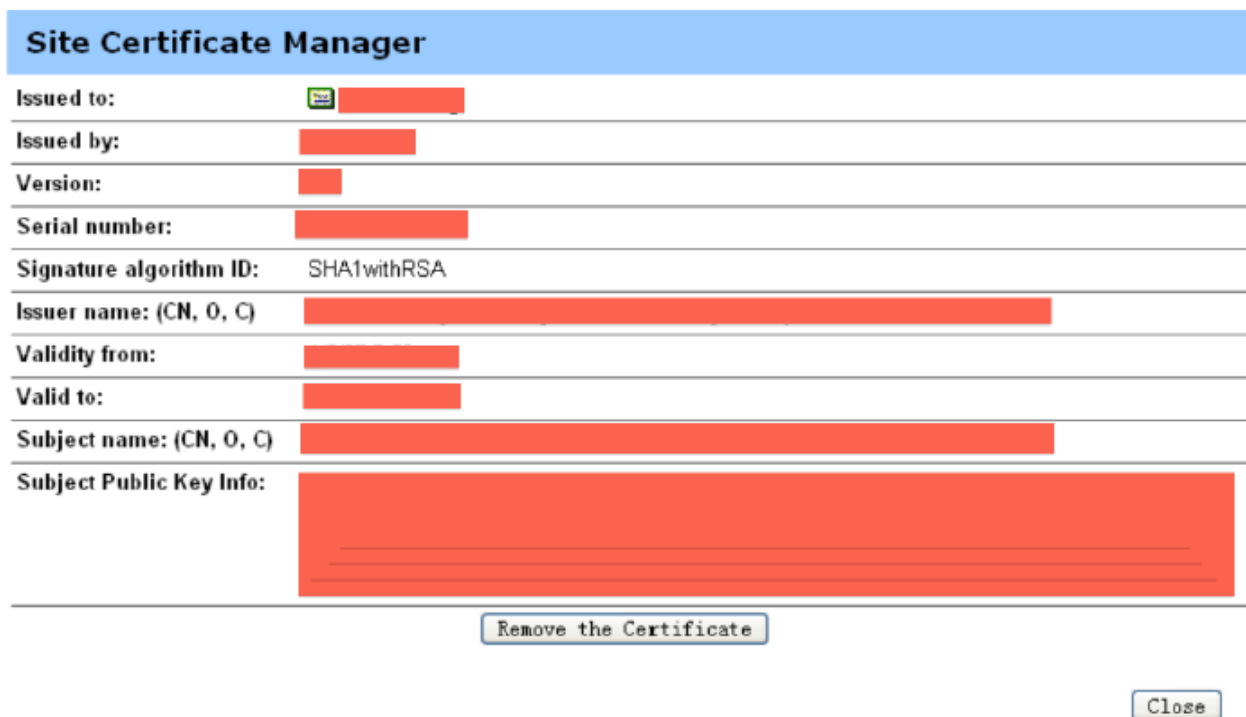
Configure WebEx to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login into the WebEx administration console <https://<Company Account>.webex.com/admin>.
2. Navigate to **Manage Site > SSO Configuration**.



3. Select **Site Certificate Manager** under the SSO Configuration section.
4. Select **Browse** and upload the public key you generated from the RSA SecurID Access.



5. Scroll down to the Federation Web SSO Configuration section and choose **SAML 2.0** from the **Federation Protocol** pull down menu.

SSO Configuration

[Site Certificate Manager](#)

Federated Web SSO Configuration

Federation Protocol:

SSO Profile: SP Initiated
 AuthnRequest Signed
 IdP Initiated

Target page URL Parameter:
[Import SAML Metadata](#)

WebEx SAML Issuer (SP ID): *

Issuer for SAML (IdP ID): *

Customer SSO Service Login URL: *

You can export a SAML metadata WebEx SP configuration file:

NameID Format:


AuthnContextClassRef: *

Default WebEx Target page URL:

Customer SSO Error URL:

Single Logout
 Auto Account Creation
 Auto Account Update
 Remove uid Domain Suffix for Active Directory UPN

- a. Under SSO Profile select SP Initiated or IdP Initiated.

 **Note:** To enable both, choose SP Initiated. Use IdP Initiated in cases where you only want pre-authenticated users to be able to access WebEx directly via the RSA SecurID Access portal. Use SP Initiated for cases in which you (also) want users to have the option of clicking a link from the WebEx site.

- b. Verify that the **WebEx SAML Issuer (SP ID)** matches the Audience (Service Provider Entity ID) field under the Service Provider section on the RSA SecurID Access Application page.
 - c. In the **Issuer for SAML (IdP ID)** field enter the Identity Provider Entity ID from the RSA SecurID Access Application page.
 - d. In the **Customer SSO Service Login URL** enter the Identity Provider URL you copied from the RSA SecurID Access Application page.
 - e. Change the **NameID Format** to Email address.
 - f. Modify the **AuthnContextClassRef** to urn:oasis:names:tc:SAML:2.0:ac:classes:Password.
6. Click **Update**.

7. Navigate to **Manage Users> Add User**.
8. Fill in all required fields. The User name field must match the Active Directory email credentials used to login to the RSA SecurID Access portal.

[Home](#)

Manage Site

- [Site Settings](#)
- [Tracking Codes](#)
- [Company Addresses](#)
- [Email Templates](#)
- [Meetings in Progress](#)
- [SSO Configuration](#)

Manage Users

- [Add User](#)
- [Edit User List](#)
- [Import/Export Users](#)
- [Edit Privileges](#)
- [Send Email to All](#)

Session Types

- [Add Custom Type](#)
- [Session Type List](#)

Assistance

Edit User

Account Type:
 Host Site administrator Site Admin - View only

** Denotes required fields*

Account Information:

First name:	Alicia	*
Last name:	Sal	*
User name:	alicia@pe-lab.com	*
Email:	alicia@pe-lab.com	*
Password:	●●●●●●●●●●●●●●●●	*
Confirm password:	●●●●●●●●●●●●●●●●	*
Language:	English ▾	
Time zone:	San Francisco (Pacific Standard Time, GMT-08:00) ▾	

Send "Welcome" email to this host when account is created

9. Click **Add**.