

RSA SECURID[®] ACCESS

Implementation Guide

Cisco Spark

Gina Salvazo, RSA Partner Engineering
Last Modified: March 13, 2018



Solution Summary

Cisco Spark is a collaboration suite that does it all; business messaging, screen sharing, video conferencing, and telephony. This integration supports single sign on via SAML SP initiated flows only. Cisco Spark does not support auto-provisioning.

RSA SecurID Access Features	
Cisco Spark	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-
Identity Assurance	
Collect Device Assurance and User Behavior	✓



Configuration Summary

All of the supported use cases of RSA SecurID Access with Cisco Spark require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Cisco Spark can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

[Cloud Authentication Service – Identity Router IdP Configuration](#)
[Cisco Spark SAML Configuration](#)



RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Cisco Spark in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Configure RSA Identity Router SAML IdP

Procedure

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for Cisco Spark and click **+Add** to add the connector.



Cisco Spark
SAML Direct

+ Add

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Select **Import Metadata** and choose the file you download from Cisco Spark from step 5 on page 11.
4. Click **Save** to import the settings from the metadata file.

All fields are required (except where noted)

Connection Profile

Configure the relationship between the identity router, acting as the SAML identity provider (IdP), and the application, acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP options. You can edit these values if necessary.

No metadata loaded

Import Metadata






5. Under the Initiate SAML Workflow section, paste the Identity Provider URL found below in the next section into the Connection URL field.

 **Note: Cisco Spark supports SP-initiated only.**

Initiate SAML Workflow

Connection URL 

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

Choose File

Generate Cert Bundle



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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 1ueu5kranxsow

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded

?

Certificate Loaded

CN=gslab.com, Valid Until: Aug
11, 2019 03:34 PM IST

Include Certificate in Outgoing Assertion

- a. Select **Choose File** and upload the private key.
- b. Select **Choose File** to import the public signing certificate.
- c. Select the checkbox for **Include Certificate in Outgoing Assertion**.



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

Service Provider

Assertion Consumer Service (ACS) URL ?

`https://idbroker.webex.com/idb/Consumer/metaAlias/34d534d5-93d8-42eb-9b0f-0ee0c3dd07f4/sp`

Audience (Service Provider Entity ID) ?

`https://idbroker.webex.com/34d534d5-93d8-42eb-9b0f-0ee0c3dd07f4`

8. In the **Assertion Consumer Service (ACS) URL** field, verify that the metadata import replaced `<OrgID>` with your Cisco Spark organization ID.
9. Verify the **Audience (Service Provider Issuer ID)** field imported correctly.
10. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

10. Click **Next Step**.



- 12. Click **Show Advanced**.
- 13. Verify that the Cisco Spark certificate imported correctly.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response
- Assertion within response

Signature Algorithm

Digest Algorithm

Encrypt Assertion

cert.pem

Certificate valid until: Jun 18,
2018 07:59 PM EDT

Encryption Algorithm

Encryption Key Transport

Relay State URL Encoding

Send encoded URL in outgoing assertion

Include Issuer NameID Format

NameID Format



- On the User Access page, select **Allow All Authenticated Users** user policy from the available options.

Access Policy

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

- Allow All Authenticated Users
- Select Custom Policy ?

No Access Allowed ▼

- Click **Next Step**.
- On the **Portal Display** page, select **Display in Portal**.
- Click **Save and Finish**.
- Click **Publish Changes**. Your application is now enabled for SSO.

[Publish Changes](#) Status: Changes Pending

- Navigate to **Applications > My Applications**.
- Locate Cisco Spark in the list and from the **Edit** option, select **Export Metadata**.



Cisco Spark
Created From: Cisco Spark
SAML Direct

Edit ▼

Edit

Export Metadata

Delete



Partner Product Configuration

Before You Begin

This section provides instructions for configuring Cisco Spark with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Cisco Spark components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Cisco Spark SAML Configuration

Procedure

1. Login to Cisco Spark. <https://admin.ciscospark.com>
2. Navigate to **Settings > Authentication**.
3. Select **Modify**.

The screenshot displays the Cisco Spark Control Hub interface. On the left is a dark sidebar with the Cisco Spark logo and navigation menu items: Overview, Users, Services, Reports, Support, and Settings (which is highlighted in blue). The main content area is divided into sections. The 'Authentication' section shows 'Single Sign-On' with a radio button selected for 'Disabled' and a blue 'Modify' button. The 'Email' section shows 'Suppress Admin Invite Emails' with a toggle switch that is currently turned off. Below this toggle, there is explanatory text: 'When enabled, users will not receive the automated Cisco invitation e licenses are assigned. Only use this feature if you wish to send your c campaign. This setting only works if you turn on Single-Sign-On (SSC



4. Select **Integrate a 3rd-party identity provider (Advanced)**.

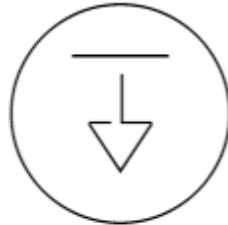
Enterprise Settings

Single Sign-On

- Use the built-in identity service for user authentication. (Simple)
- Integrate a 3rd-party identity provider. (Advanced)

● Single sign-on is not enabled

5. Select **Download Metadata File**.



Export Directory Metadata


Download the following trust metadata file from the Cisco Spark Control service, and upload it into your identity provider (IdP) management interface. When you have finished uploading the file into your IdP, return to this screen and press Next.

[Download Metadata File](#)



6. Select **file browser** and select the metadata file you download in step 20 on page 9.
7. Select if the certificate must be signed by a certificate authority or self-signed.
8. Click **Next**.

Enterprise Settings



Import IdP Metadata

Begin configuring the trust relationship between your identity provider (IdP) and the Cisco Collaboration Cloud by obtaining a trust metadata file from your IdP and uploading it here.

Drag and drop a file or use the [file browser](#)

Signing of Metadata (Advanced)

Require certificate signed by a certificate authority in Metadata (more secure)

Allow self-signed certificate in Metadata (less secure)

[Back](#) [Next](#)



9. Click **Test SSO Connection**.

Enterprise Settings

Test SSO Setup

Press the button below to test your SSO configuration. The test will open in a new browser window. Enter valid SSO credentials and verify the login was successful.

Test SSO Connection

If your test was successful, enable Single Sign On below. Otherwise, disable Single Sign On or return to the previous steps.

- The test was successful. Enable Single Sign On.
- The test was unsuccessful. Disable Single Sign On.

Save

10. If successful, click **"The test was successful. Enable Single Sign On."**
11. For SP initiated login, go to <https://web.ciscopark.com>.