RSA SECURID® ACCESS
Implementation Guide

Cisco Spark

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

RSA READY

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)

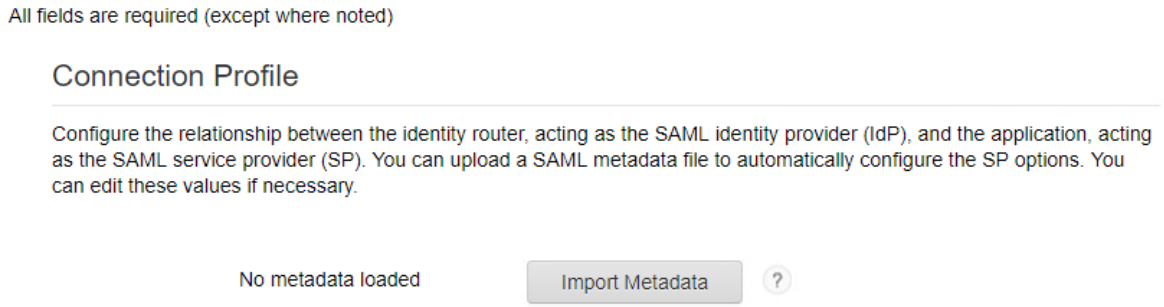
To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Cisco Spark in the RSA SecurID Access Console. During configuration of the IdP you will need some Information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and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

Configure RSA Identity Router SAML IdP

Procedure

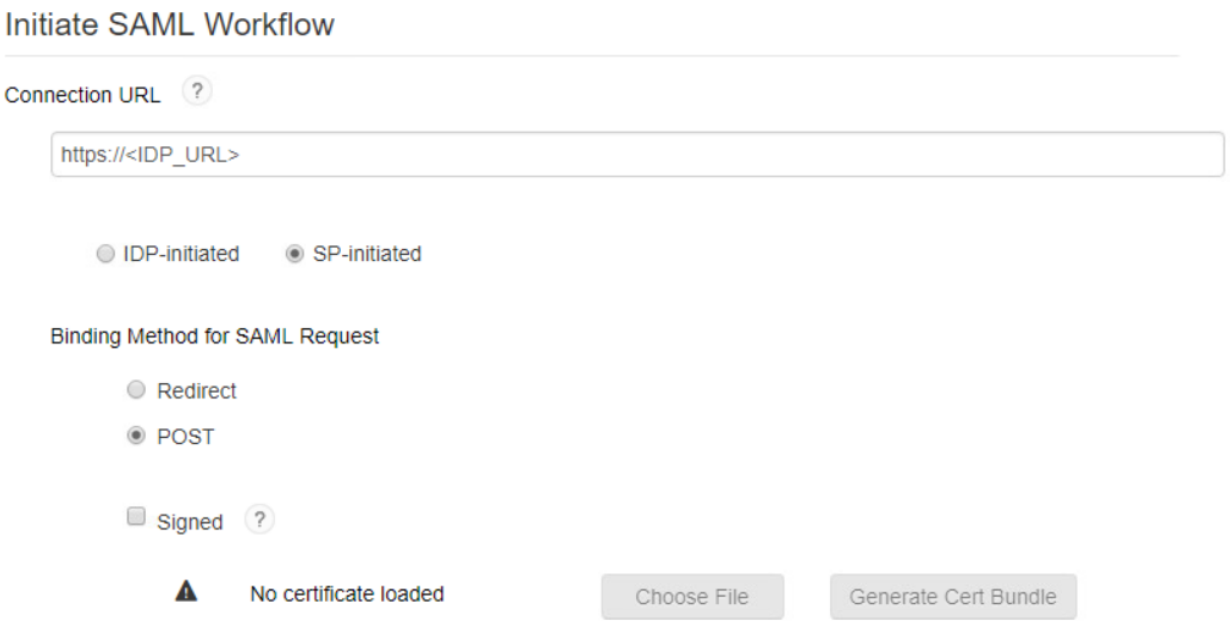
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Cisco Spark and click **+Add** to add the connector.

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.

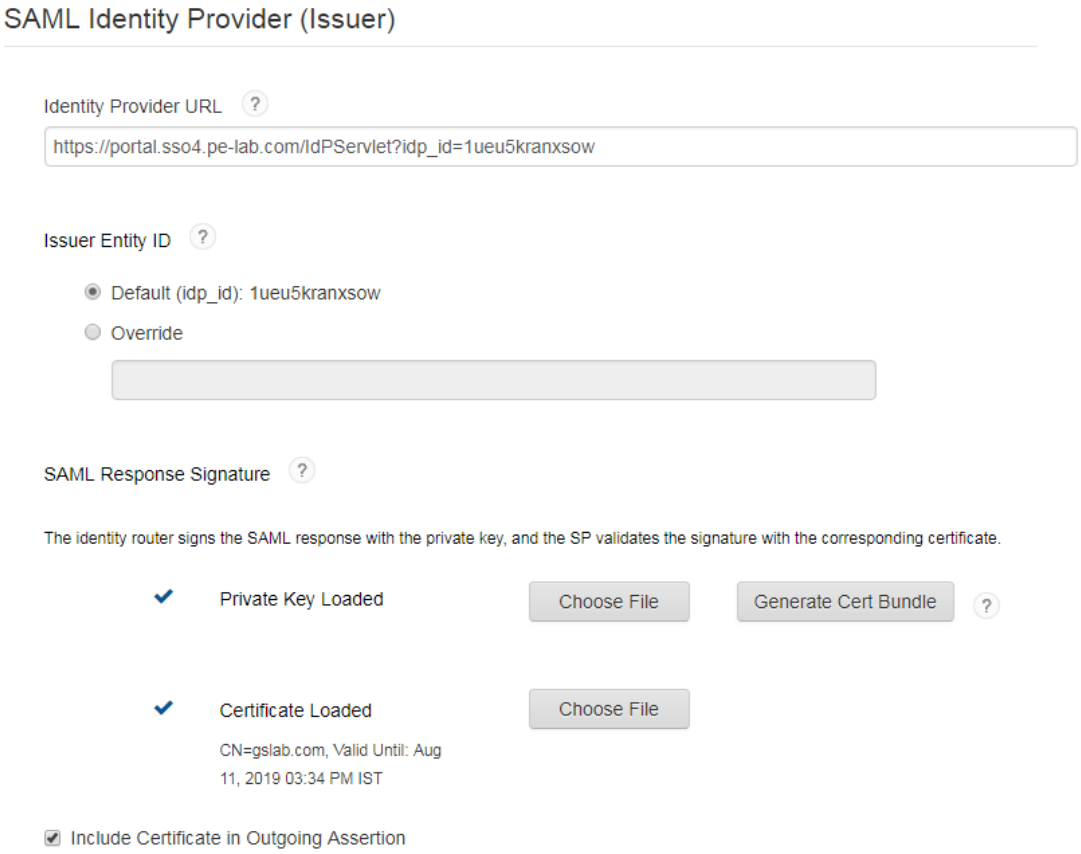


5. Under the Initiate SAML Workflow section, paste the Identity Provider URL found below in the next section into the Connection URL field.

Note: Cisco Spark supports SP-initiated only.

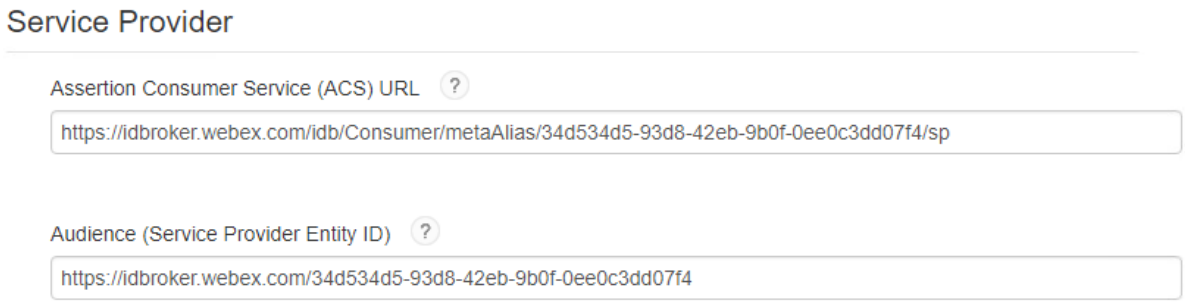


6. Scroll down to SAML Identity Provider (Issuer) section.

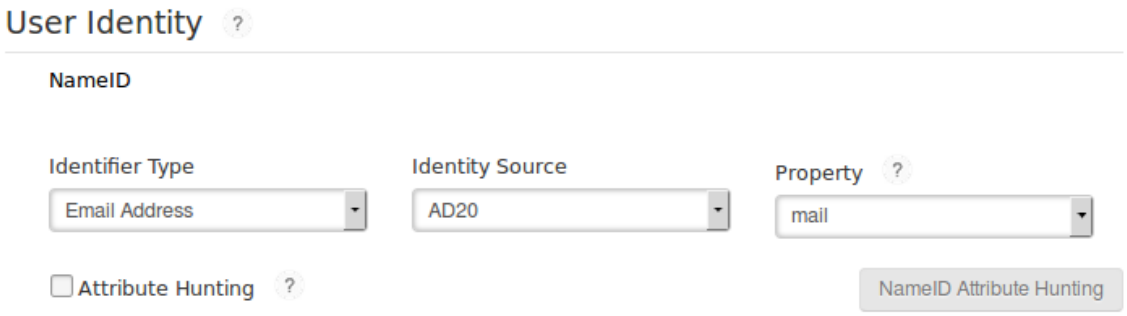


a. Select **Choose File** and upload the private key.
b. Select **Choose File** to import the public signing certificate.
c. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

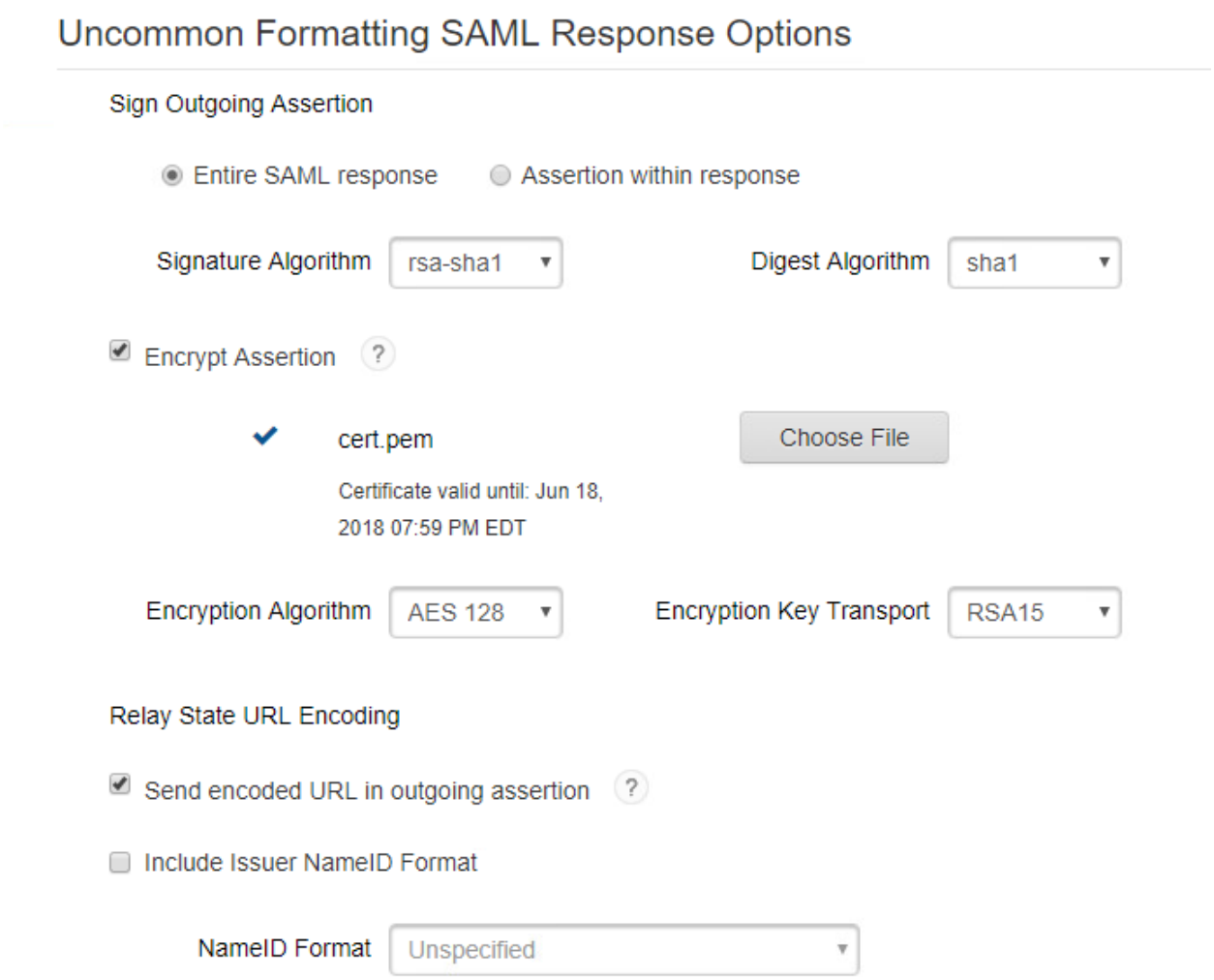


8. In the **Assertion Consumer Service (ACS) URL** field, verify that the metadata import replaced <OrgID> with your Cisco Spark organization ID.
9. Verify the **Audience (Service Provider Issuer ID)** field imported correctly.
10. Scroll down to the **User Identity** section. Verify the settings are 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.

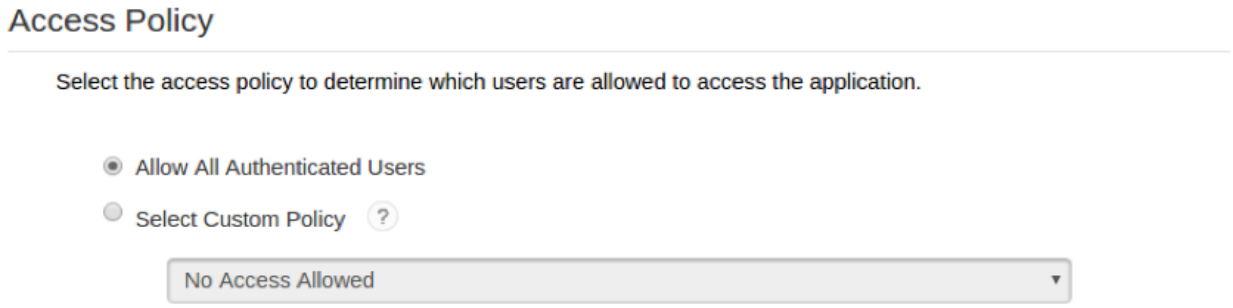


10. Click **Next Step**.

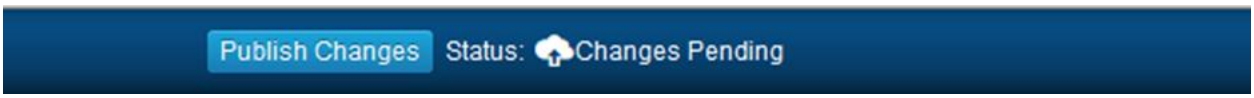
12. Click **Show Advanced**.
13. Verify that the Cisco Spark certificate imported correctly.



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



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



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

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.

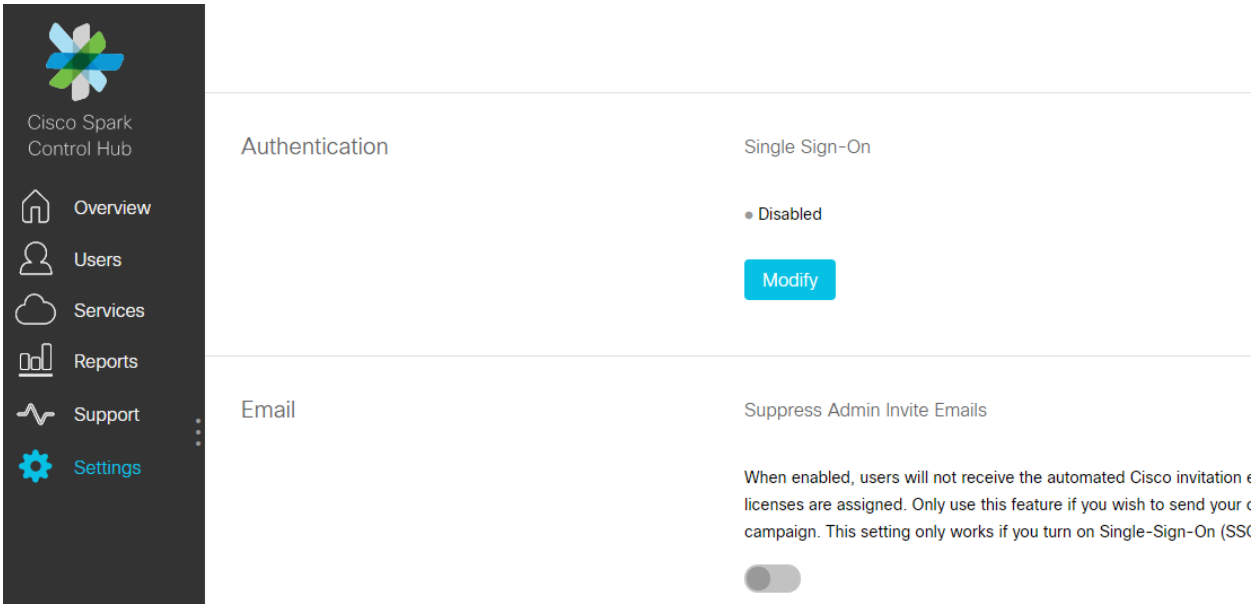
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

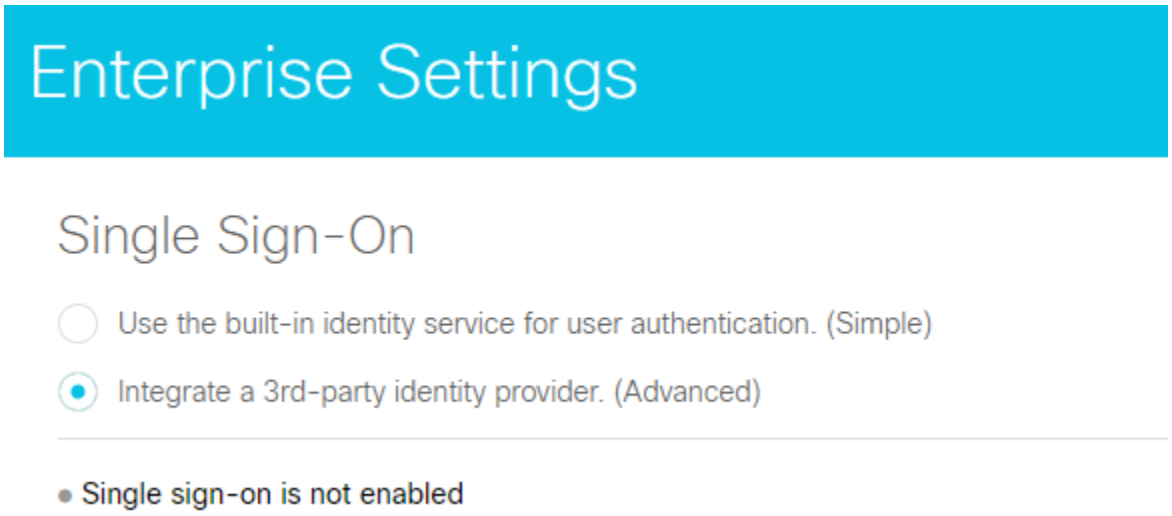
Cisco Spark SAML Configuration

Procedure

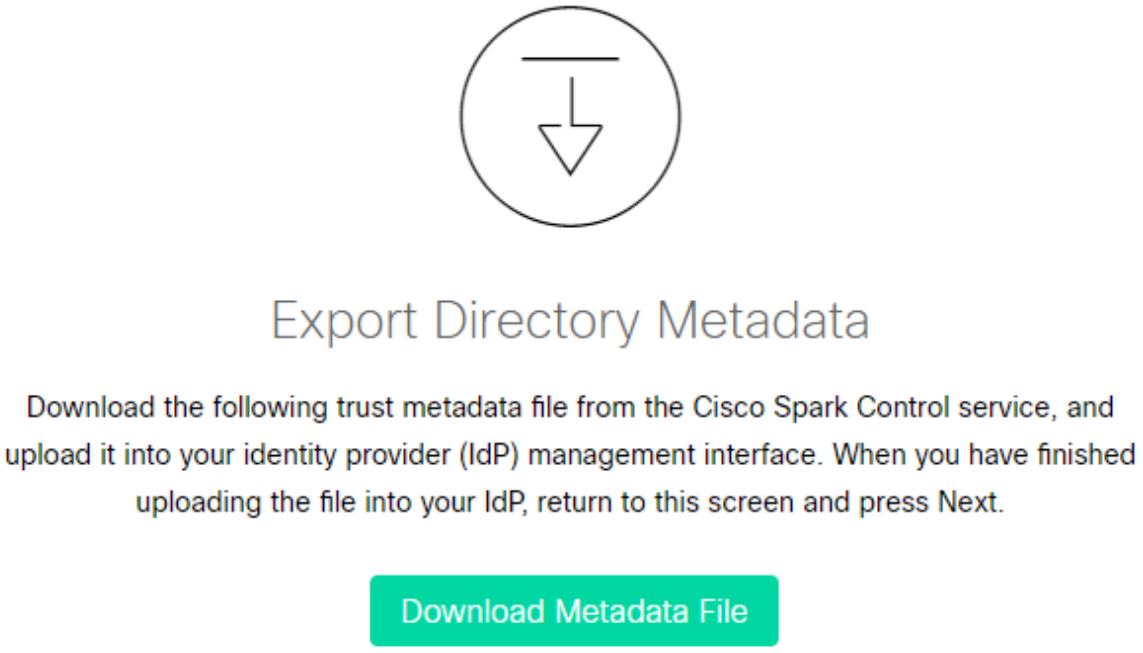
1. Login to Cisco Spark. **https://admin.ciscospark.com**
2. Navigate to **Settings > Authentication**.
3. Select **Modify**.



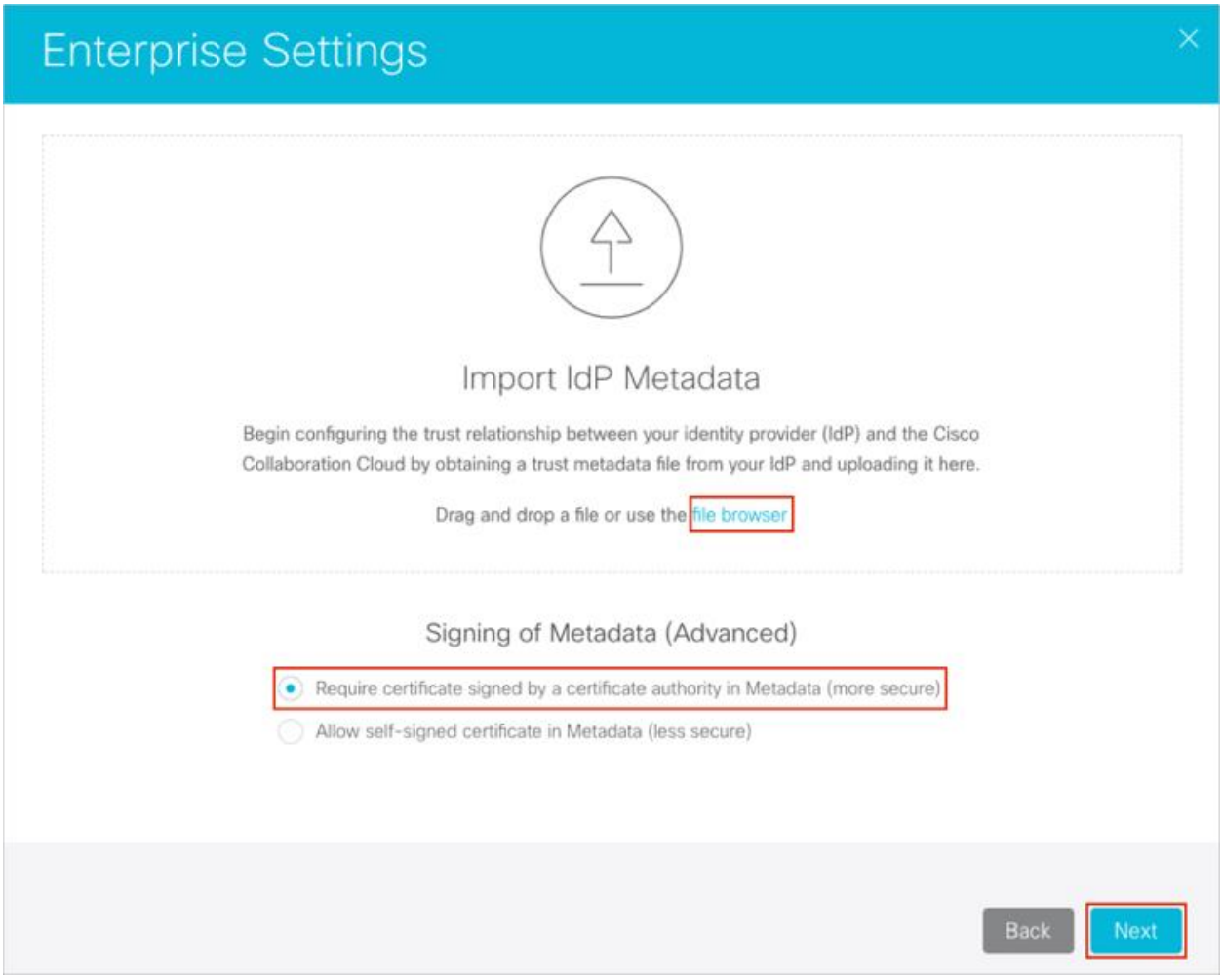
4. Select **Integrate a 3rd-party identity provider (Advanced).**



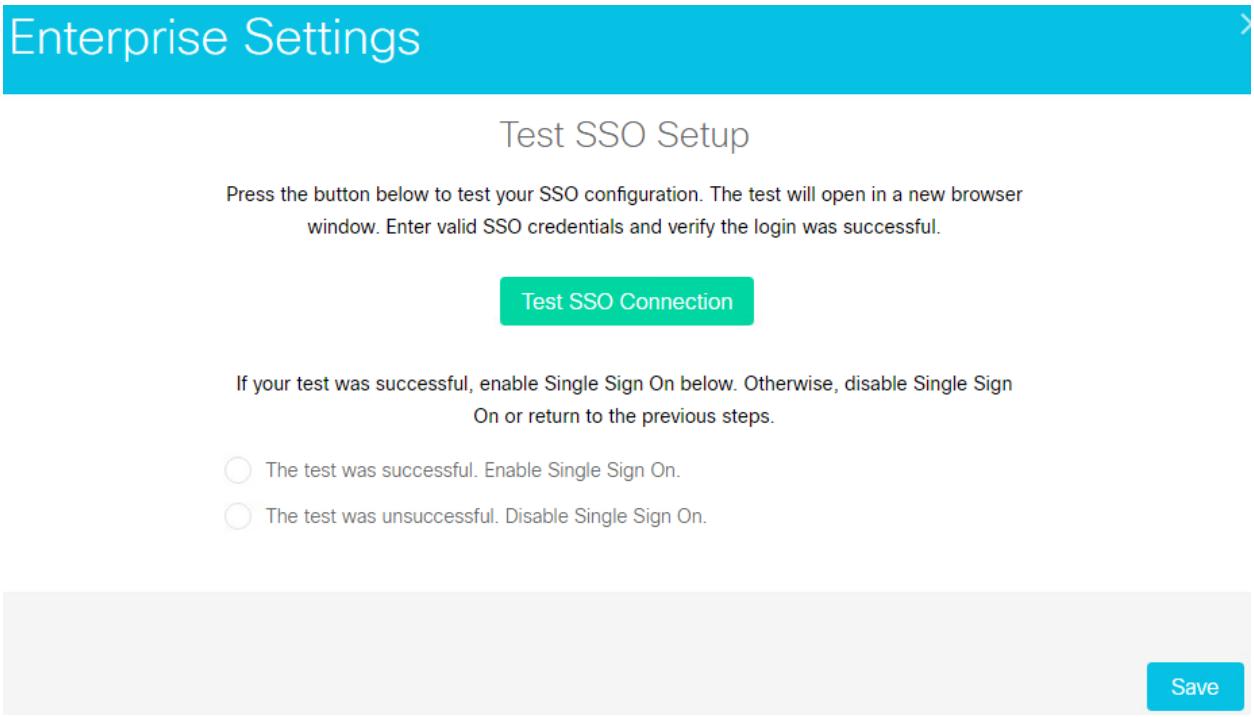
5. Select **Download Metadata File**.



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.**



9. Click **Test SSO Connection**.



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