Configure Cisco Umbrella for Single Sign-On

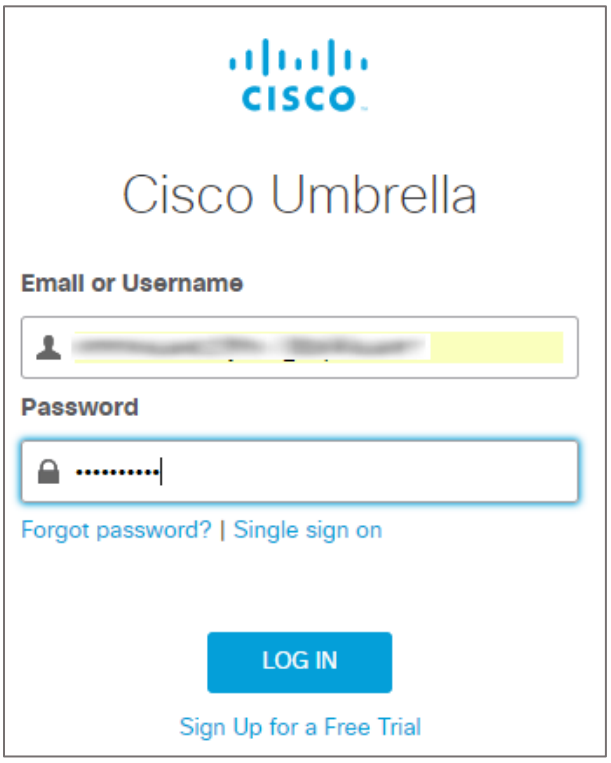
Configuring Cisco Umbrella for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Cisco Umbrella by using the enterprise credentials.

Prerequisite

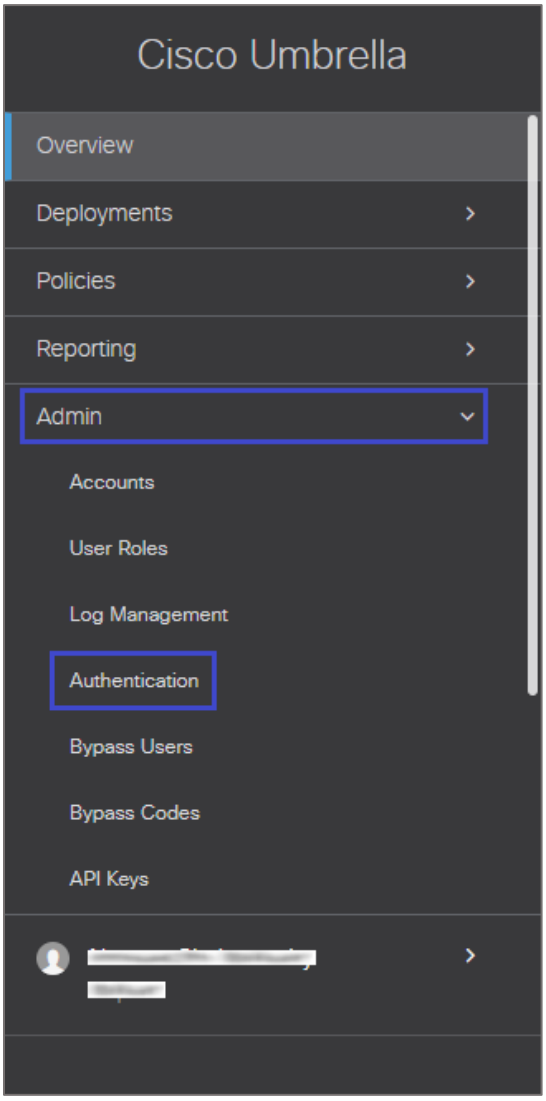
Browser Requirements: Internet Explorer 11 and above

To configure Cisco Umbrella for SSO by using SAML:

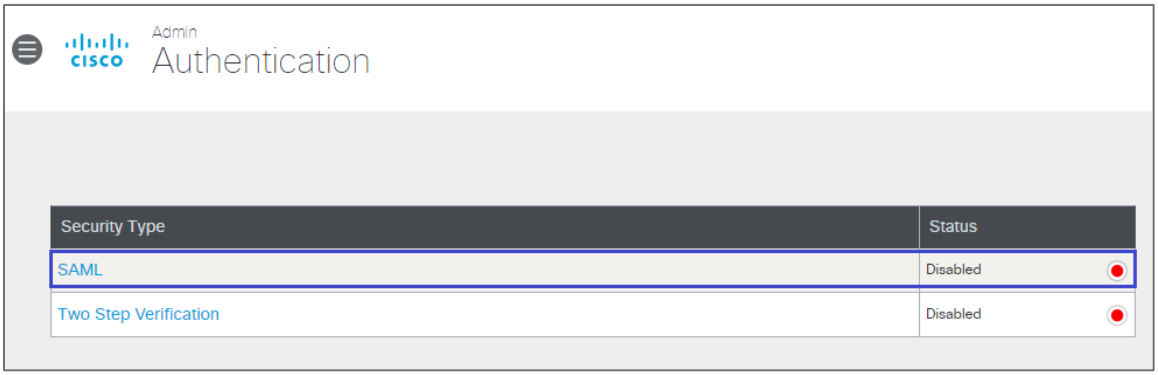
1. In a browser, type https://login.umbrella.com/ and press **Enter**.
2. Type your Cisco Umbrella admin account credentials (**Email or Username** and **Password**) and click **Login**.



3. In the dashboard page, click **Admin** and select **Authentication** from the left panel.

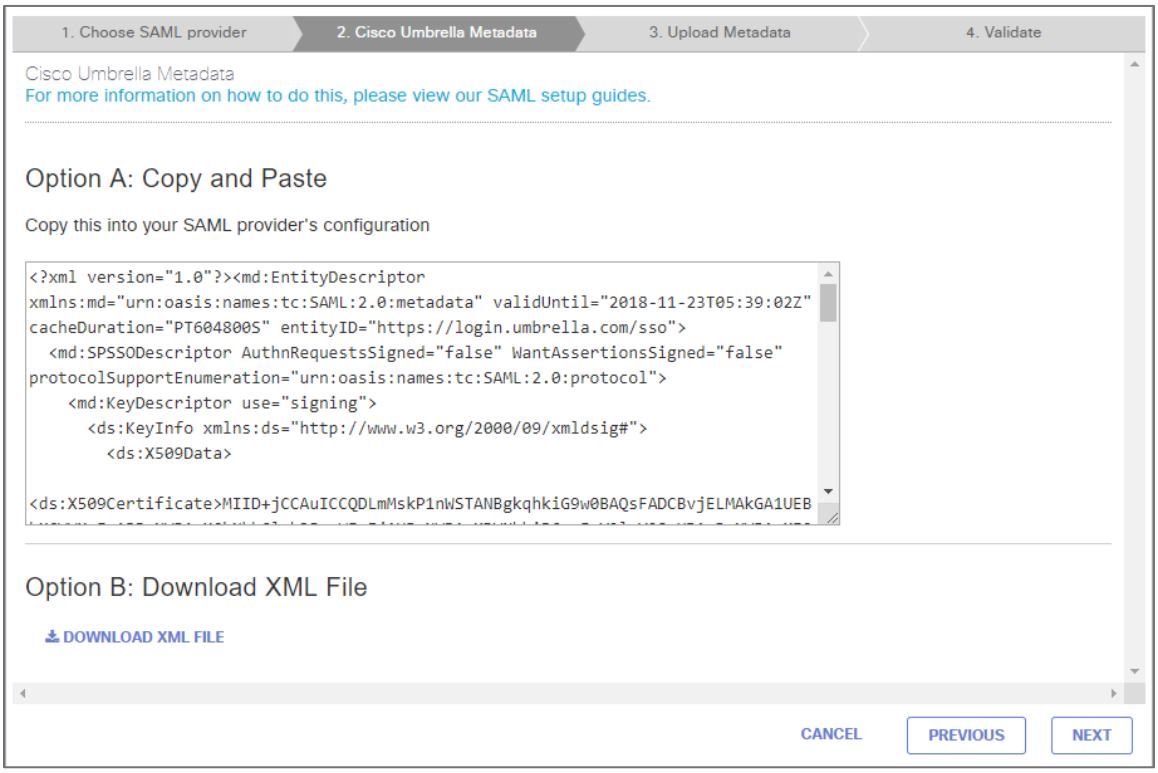


4. In the **Authentication** page, click **SAML**.



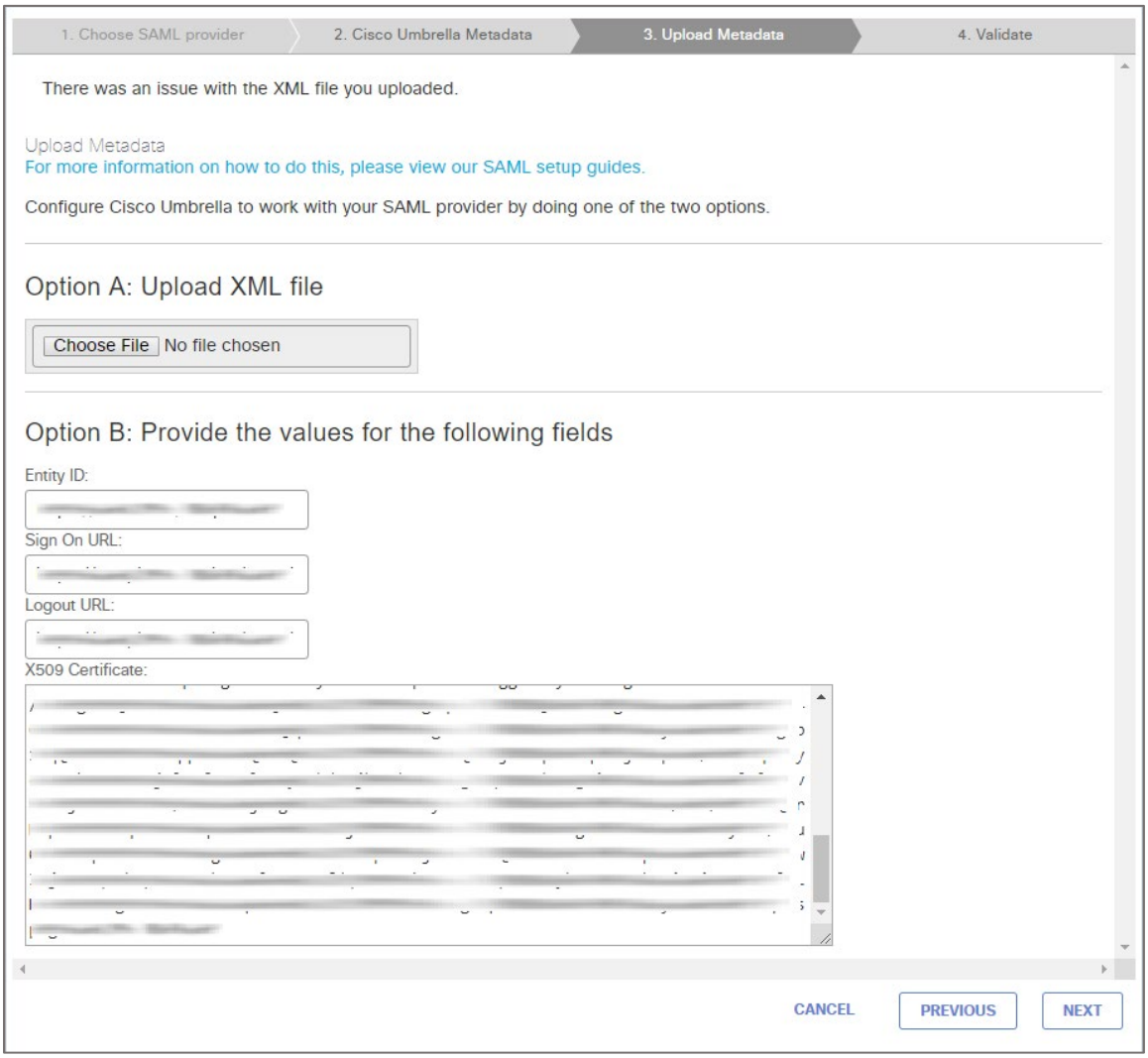
5. Click **Other** in **Choose SAML provider** and click **NEXT**.

6. Copy the metadata or download the XML file and click **NEXT**.

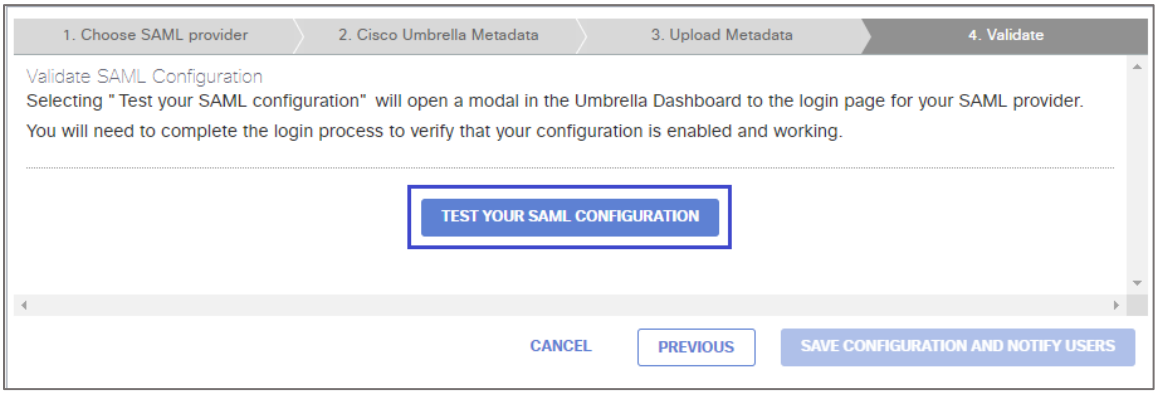


7. Browse and upload the metadata file or enter the values for the following fields:

Field Name	Description
Entity ID	Issuer ID
Sign On URL	IdP logon URL
Logout URL	IdP logout URL
X509 Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with - - - - -Begin Certificate- - - - - and - - - - -End Certificate- - - - - **Note:** The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml



8. Click **TEST YOUR SAML CONFIGURATION**.



9. Finally, click **SAVE CONFIGURATION AND NOTIFY USERS**.

   Note: The **SAVE CONFIGURATION AND NOTIFY USERS** button is activated after the SAML configuration is validated successfully.