

Configure Cisco Umbrella for Single Sign-On

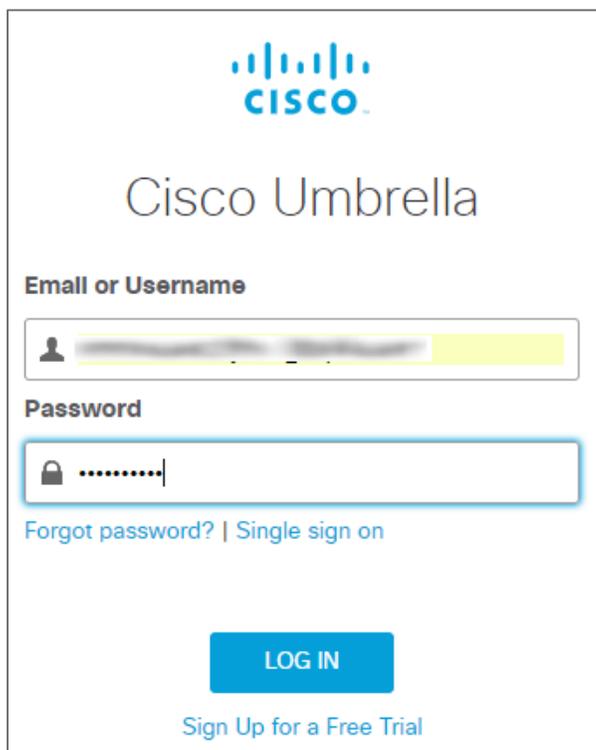
Configuring Cisco Umbrella for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Cisco Umbrella by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

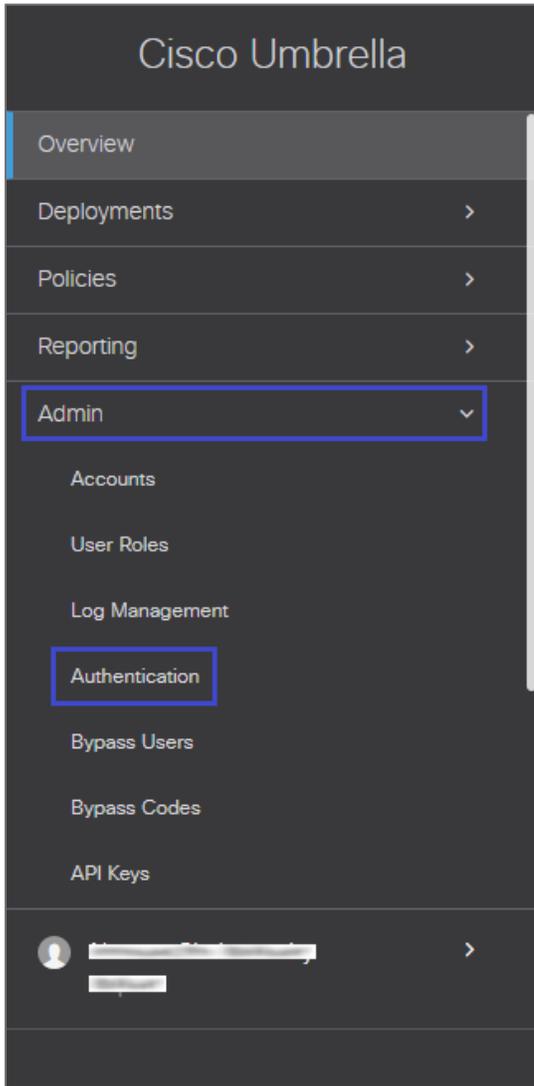
To configure Cisco Umbrella for SSO by using SAML:

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**.

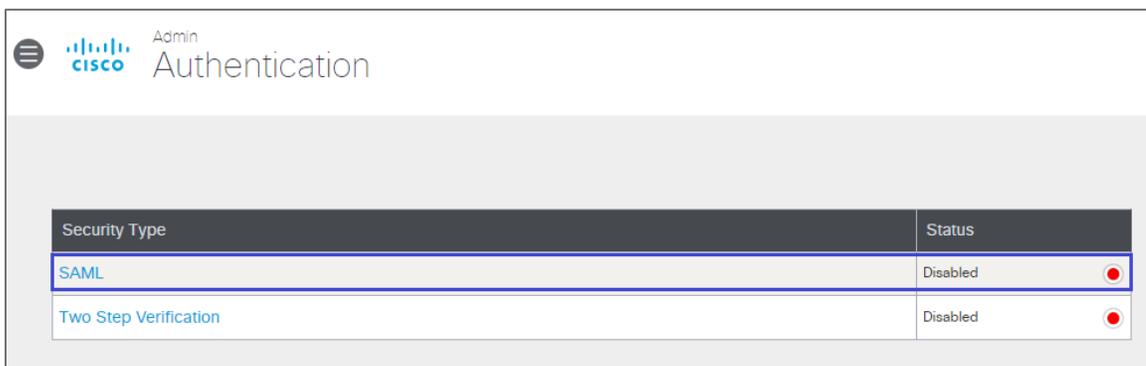


The screenshot shows the Cisco Umbrella login interface. At the top is the Cisco logo. Below it, the text "Cisco Umbrella" is displayed. There are two input fields: "Email or Username" and "Password". The "Email or Username" field has a blurred email address. The "Password" field has a blurred password. Below the password field, there are links for "Forgot password?" and "Single sign on". At the bottom, there is a blue "LOG IN" button and a link for "Sign Up for a Free Trial".

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**.

1. Choose SAML provider 2. Cisco Umbrella Metadata 3. Upload Metadata 4. Validate

Which SAML based SSO Service would you like to use?

Okta Ping Identity onelogin Other

CANCEL NEXT

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

1. Choose SAML provider 2. Cisco Umbrella Metadata 3. Upload Metadata 4. Validate

Cisco Umbrella Metadata
[For more information on how to do this, please view our SAML setup guides.](#)

Option A: Copy and Paste

Copy this into your SAML provider's configuration

```
<?xml version="1.0"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2018-11-23T05:39:02Z"
cacheDuration="PT604800S" entityID="https://login.umbrella.com/sso">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIID+jCCAuICCCQLmMskP1nWSTANBgkqhkiG9w0BAQsFADCBvjELMAkGA1UEB
```

Option B: Download XML File

[DOWNLOAD XML FILE](#)

CANCEL PREVIOUS 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. <a href="https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml

1. Choose SAML provider
2. Cisco Umbrella Metadata
3. Upload Metadata
4. Validate

There was an issue with the XML file you uploaded.

Upload Metadata
[For more information on how to do this, please view our SAML setup guides.](#)

Configure Cisco Umbrella to work with your SAML provider by doing one of the two options.

Option A: Upload XML file

No file chosen

Option B: Provide the values for the following fields

Entity ID:

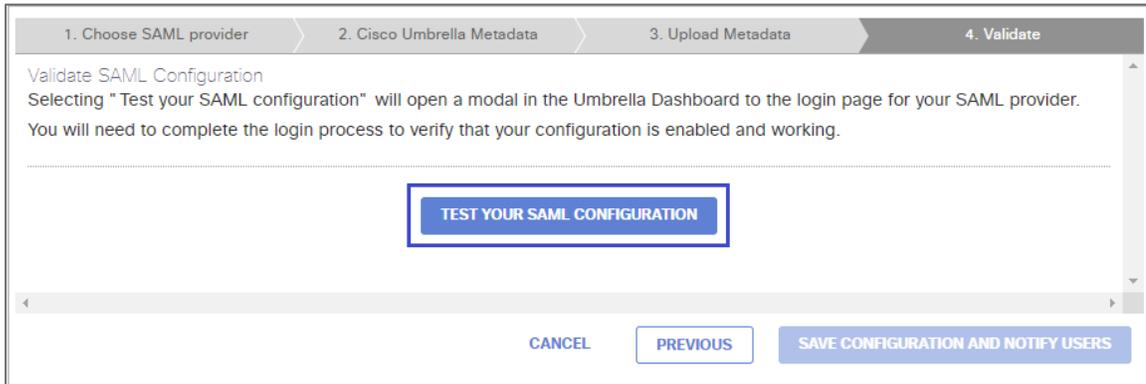
Sign On URL:

Logout URL:

X509 Certificate:

```
-----Begin Certificate-----
-----End Certificate-----
```

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.