

Last Modified: May 12th, 2017

Cisco Umbrella (OpenDNS earlier) is the enterprise network security product suite designed to enforce security policies for mobile employees who work beyond the corporate network using roaming devices like laptops, mobiles etc. and provides granular network security for all devices behind the network perimeter. IT administrators can define policies, provision devices, and view reports across users, sites, networks, groups, and devices. The company also launched the Security Graph which is a data-driven threat intelligence engine that automatically updates malware, botnet, phishing domain and IP blacklists enforced time to time. Cisco Umbrella does not provide feature of auto-provisioning the user.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Cisco Umbrella.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from IDR portal.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	https://dashboard.umbrella.com/
ACS URL	https://login.umbrella.com/sso
Service Provider Issuer ID	https://login.umbrella.com/sso

Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Cisco Umbrella 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, click **+Add** Cisco Umbrella.



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

The screenshot shows the 'Add Connection' page in Cisco Umbrella. The navigation bar includes 'Dashboard', 'Users', 'Access', 'Applications', 'Authentication Clients', and 'Platform'. The page title is 'Cisco Umbrella'. A sidebar on the left lists steps: '1. Basic Information', '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area is titled 'Basic Information' and contains the following fields: 'Name' (text input with 'Cisco Umbrella'), 'Description (optional)' (text area), and a 'Disabled' checkbox. At the top right and bottom right of the form are 'Cancel' and 'Next Step' buttons.

4. Navigate to **Connection Profile** section. Click on **Import Metadata** button to configure SAML settings by providing path to the metadata file of service provider you downloaded and go to *step – 9* directly.

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



Follow below instructions *step – 5* onwards only when you have not chosen to configure SAML settings by importing metadata file mentioned in *step – 4* and wish to configure SAML settings manually.

5. Navigate to **Initiate SAML Workflow** section.
 - a. In the **Connection URL** field, keep the field blank as the value is not required.
 - b. Choose **IDP-initiated**.

 **Note:** The following IdP-initiated configuration works for SP-initiated Cisco Umbrella connections as well.

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): 6imt198ktjjq

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:
08/09/2020

Include Certificate in Outgoing Assertion

- Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- Select **Choose File** and upload the private key.
- Select **Choose File** to import the public signing certificate.
- 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://login.umbrella.com/sso

Audience (Service Provider Entity ID) ?

https://login.umbrella.com/sso

- a. In the **Assertion Consumer Service (ACS) URL** field, provide value as per received from service provider.
 - b. In the **Audience (Service Provider Issuer ID)** field, provide value as per received from service provider.
8. 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

unspecified

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Next Step**.
10. 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

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.



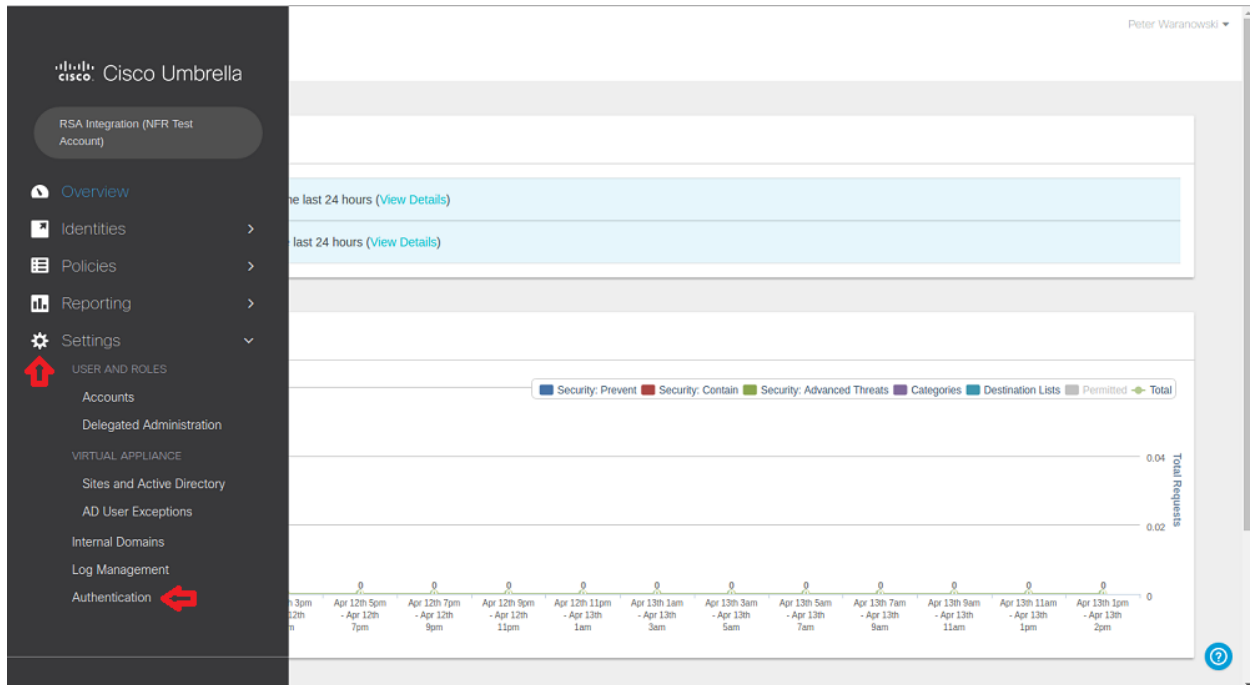
15. Navigate to **Applications > My Applications**.
16. Locate Cisco Umbrella in the list and from the **Edit** option, select **Export Metadata**.



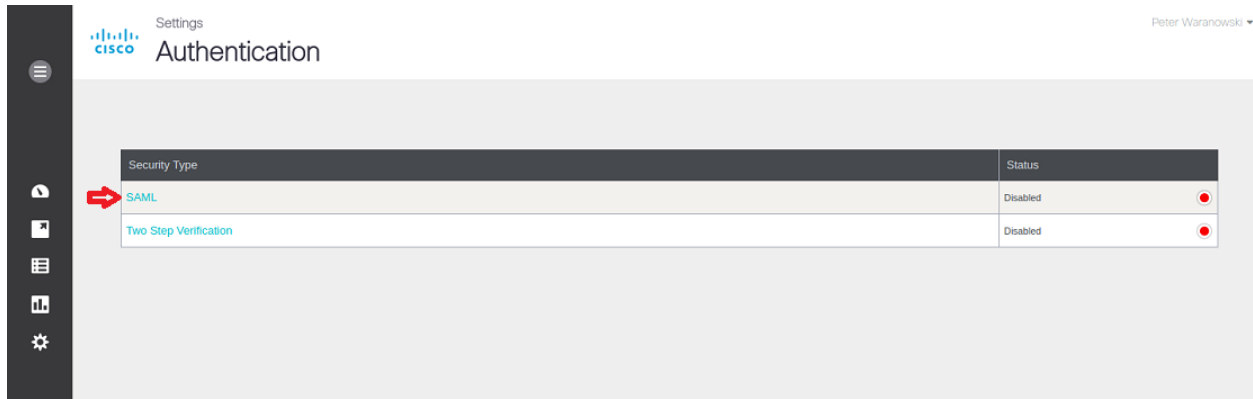
Configure Cisco Umbrella to Use RSA SecurID Access as an Identity Provider

Procedure

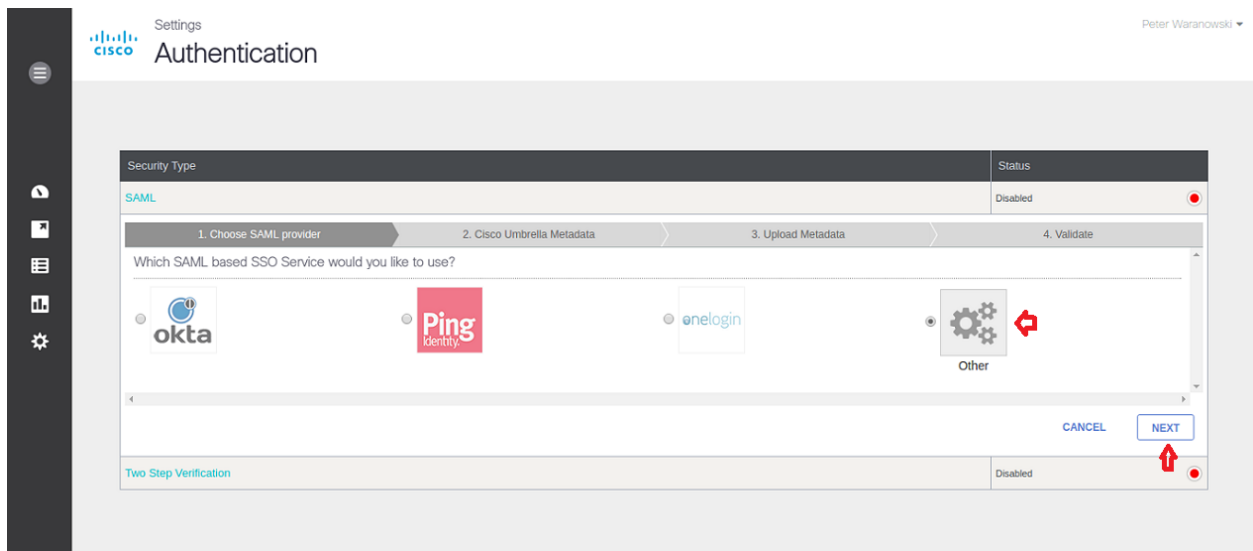
1. Login to your Cisco Umbrella application web account. (<https://dashboard.umbrella.com/>)
2. Following UI will be displayed. Go to **Settings** > **Authentication**.



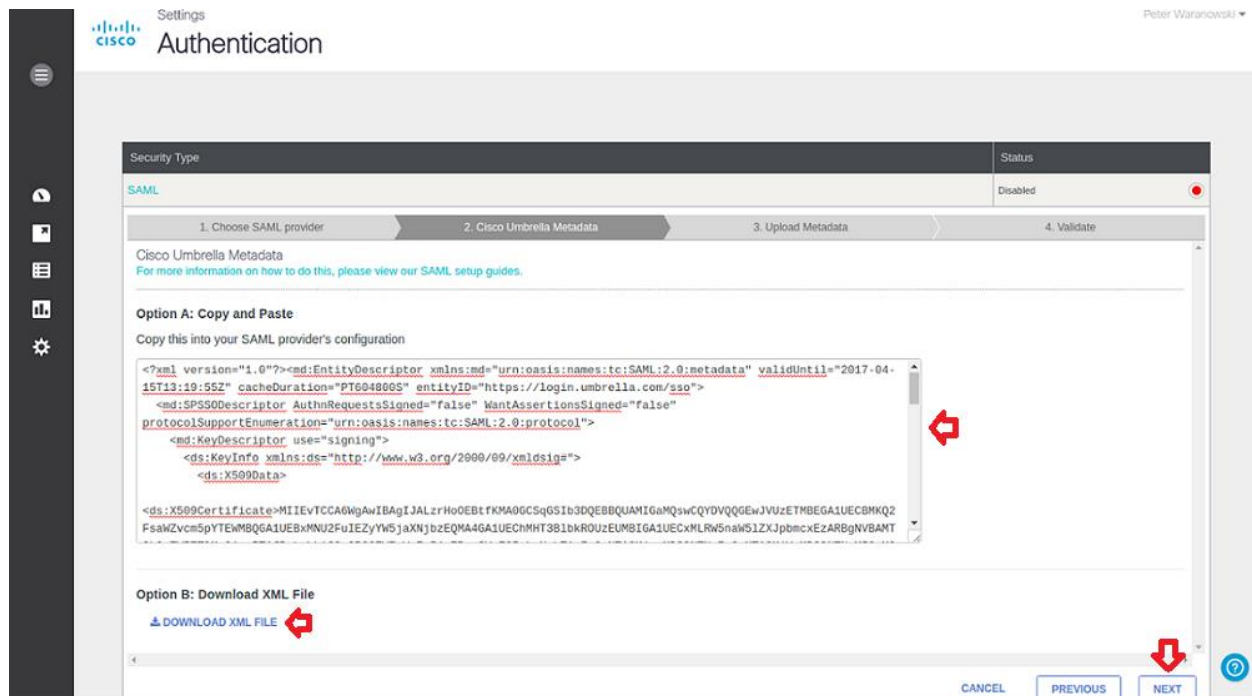
3. Click on **SAML**.



4. Following pop-up will be displayed. Click on **Other** checkbox to configure our own identity provider amongst available ones. Once selected, click on **NEXT** button.

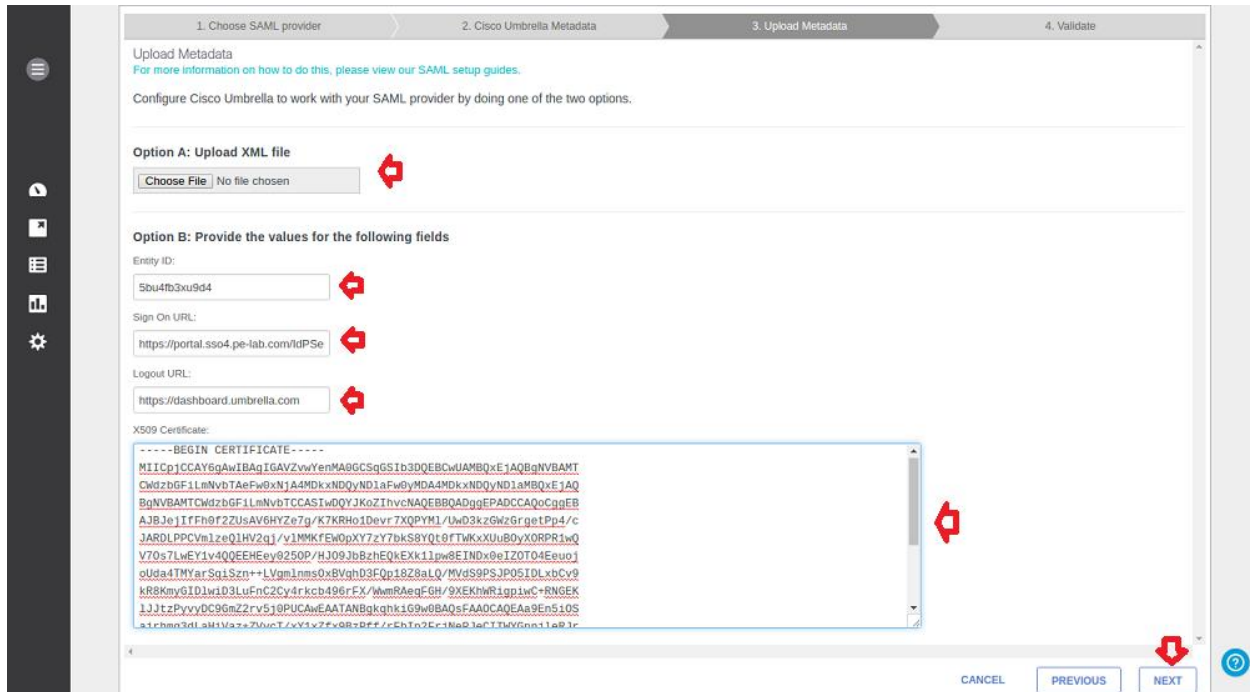


5. Following pop-up will be displayed which specifies service provider metadata details.



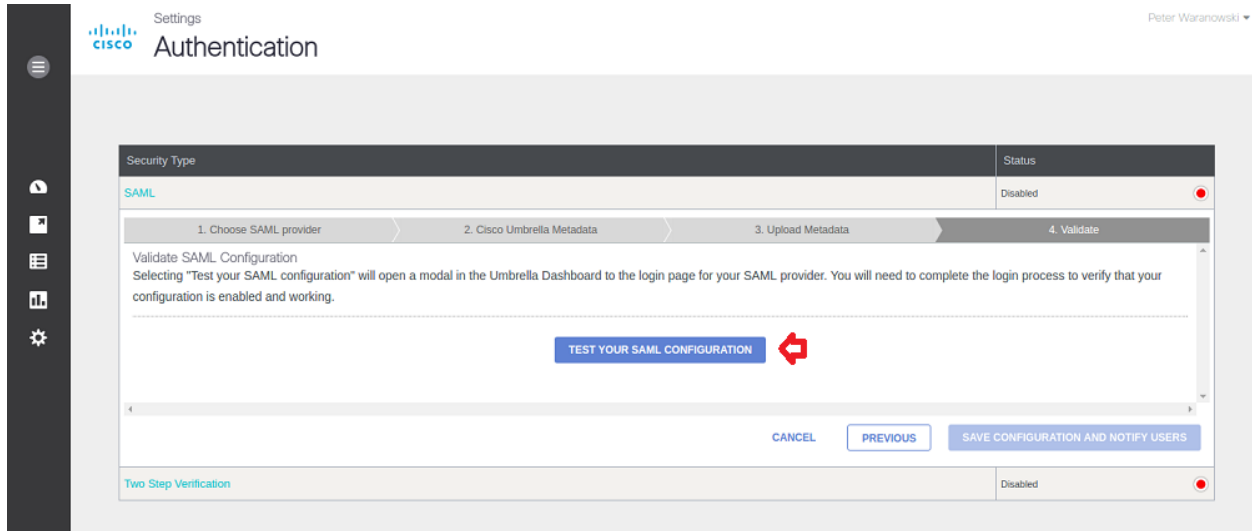
- Option A : Copy and Paste** – Copy metadata details about service provider to some xml file (For ex. - metadata.xml).
- Option B : Download XML File** – Download metadata file to the machine. This file can be directly imported to configure SAML settings at identity provider end in *step – 4 on page – 2* above.
- Click **NEXT** button.

6. Configure the SAML settings and click **Next**.

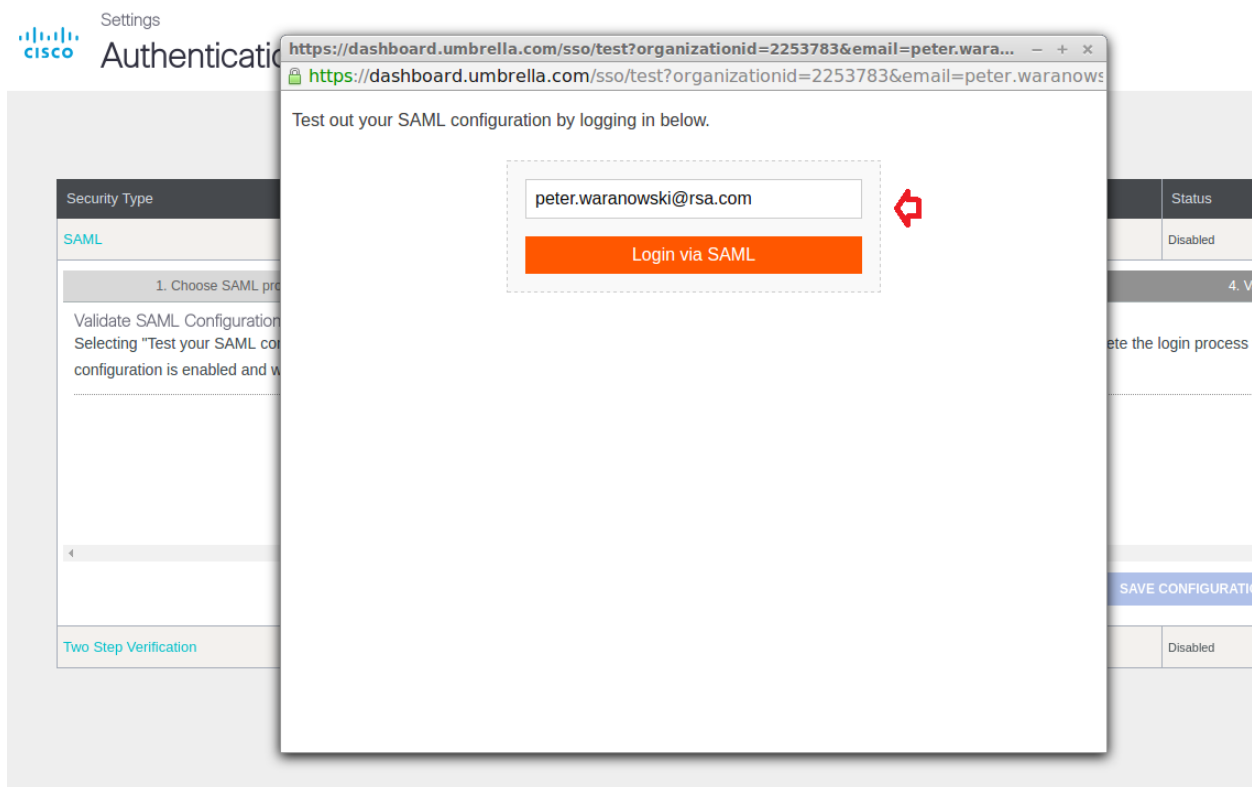


- a. **Option A : Upload XML file** – Here identity provider metadata file can be directly uploaded to configure SAML settings which is downloaded in *step – 16 on page – 6* above.
- b. **Option B : Provide the values for the following fields** – If chosen to configure settings manually, configure as below –
 1. **Entity ID** : Provide the value of IdP Issuer field here that is received from RSA Admin portal.
 2. **Sign On URL** : Enter the Identity Provider URL found in *step – 6* on page - 4. It is of following format : https://<Your Portal URL>?idp_id=<Unique IdP ID>
 3. **Logout URL** : Provide URL here where user will be redirected after logging out from the account.
 4. **X509 Certificate** : Provide the RSA SecurID Access IdP public certificate here.

7. Following pop-up will be displayed which will ask you to test the SAML settings done till now. Click on button **TEST YOUR SAML CONFIGURATION**.



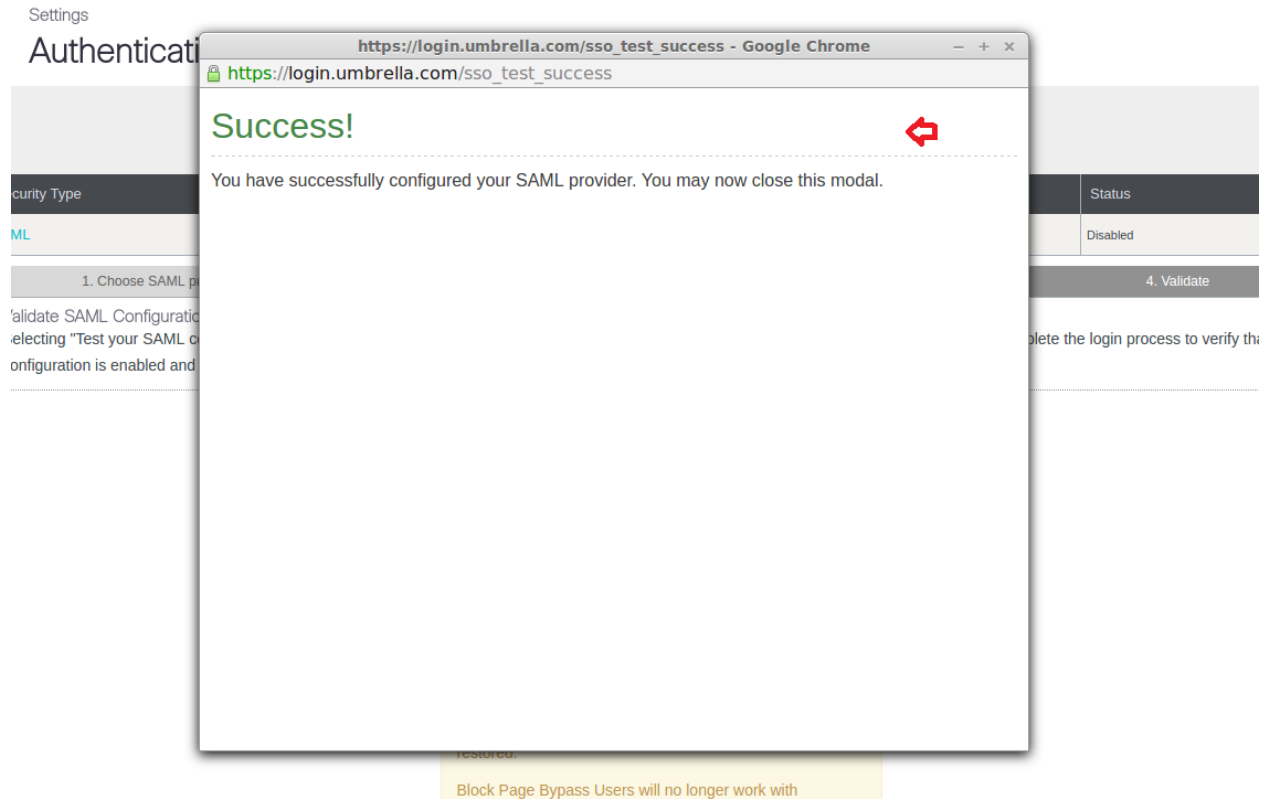
8. After clicking, will result into opening of new window on same page as below. Verify your account for which SSO needs to be tested and click on **Login via SAML** button.



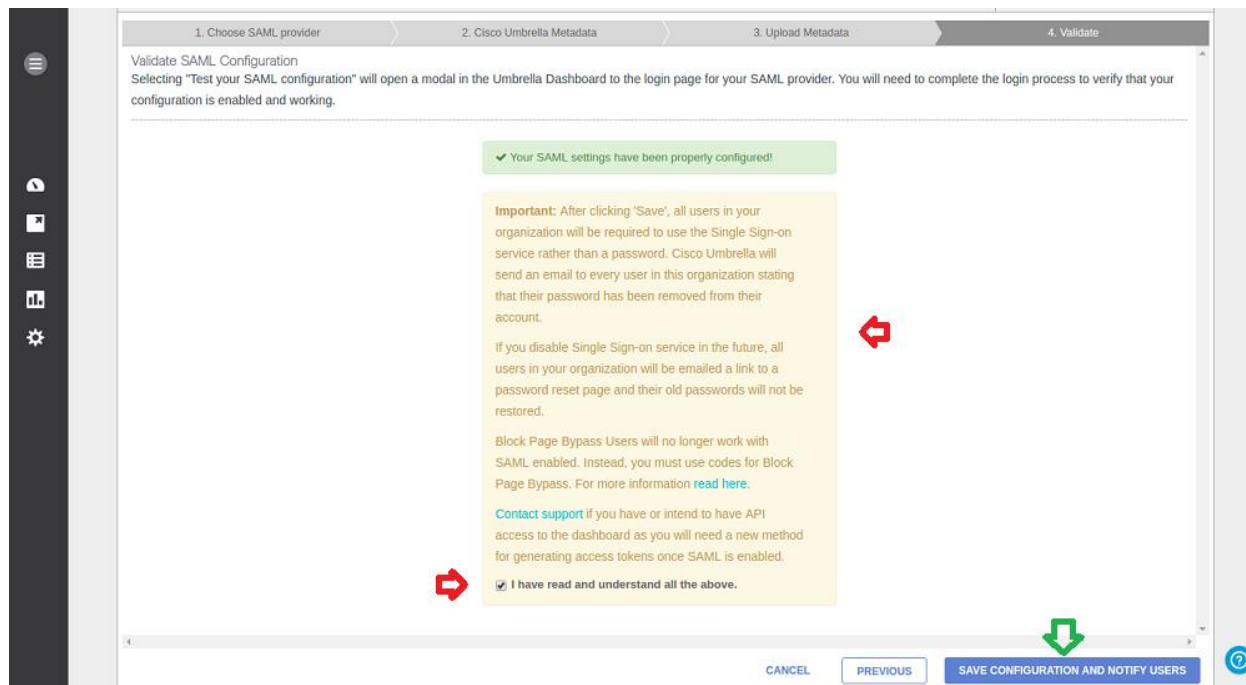
9. Following IDR portal appears as SAML Request will be initiated. Provide admin credentials here and click on **Sign In** button.

The image shows a browser window titled "RSA SecurID Access Application Portal - Google Chrome" with the URL <https://portal.sso4.pe-lab.com/WebPortal/?singlepoint-error-message=Not%20authenticated>. The main content area displays the "RSA SecurID Access Application Portal" login form. The form includes a "User ID" field with the placeholder text "User ID", a "Password" field with the placeholder text "Password", and a blue "Sign In" button. A red arrow points to the "Sign In" button. Below the form, the copyright notice "© 2015-2017 EMC Corporation. All rights Reserved" is visible. The background shows a blurred administrative interface with sections like "Settings", "Authenticati...", "Security Type", "Status", "Disabled", "1. Choose SAML p...", "Validate SAML Configuration", "Selecting 'Test your SAML co...", "Configuration is enabled and...", "Step Verification", "Disabled", and "SAVE CONFIGURA...".

10. Upon successful SAML Response reception, you will be greeted with **Success** message on the screen as following. Thus, Admin and Cisco Umbrella SAML integration is successfully performed. Close this window now to proceed with next steps.



11. Following page is displayed now informing about successful SAML SSO configurations. One checkbox will appear to accept all the terms and conditions to use Cisco Umbrella features. Click on checkbox **I have read and understand all the above**. Finally, click on **SAVE CONFIGURATION AND NOTIFY USERS** button to save all changes and enable SAML authentication for the account.



12. At the end, following pop-up is displayed with checkbox in front of **SAML** option marked with *green* color to notify SAML is now enabled for account.

