



ZSCALER AND CYBERARK DEPLOYMENT GUIDE

Contents

Terms and Acronyms	4
About This Document	5
Zscaler Overview	5
CyberArk Overview	5
Audience	5
Software Versions	5
Request for Comments	5
Zscaler and CyberArk Introduction	6
ZIA Overview	6
ZPA Overview	6
Zscaler Resources	6
CyberArk Access Management Overview	7
CyberArk Resources	7
Zscaler SAML Single Sign-On (SSO)	8
Zscaler Requirements for SSO	8
Zscaler SAML Properties	8
Configure Zscaler in the CyberArk Admin Portal (Part 1)	9
Configure Zscaler on the Zscaler Portal	11
Enable SAML Auto Provisioning	13
Enable SAML	14

Provision Accounts with SCIM	15
Enable SCIM Provisioning for Your App in the Admin Portal	15
Verify Users to Synchronize	18
Enable SCIM Synchronization	20
Provision Users with Custom Attributes with SCIM	21
Appendix A: Requesting Zscaler Support	23
Gather Support Information	23
Save Company ID	23
Enter Support Section	24

Terms and Acronyms

The following terms and acronyms are used in this document.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
IKE	Internet Key Exchange (RFC2409)
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SSL	Secure Socket Layer (RFC6101)
XFF	X-Forwarded-For (RFC7239)
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access

About This Document

This section describes the organizations and requirements for the integration covered in this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: [ZS](#)) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information, go to [Zscaler's website](#) or follow Zscaler on Twitter @zscaler.

CyberArk Overview

CyberArk (NASDAQ: [CYBR](#)) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides comprehensive security offerings for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more go to [CyberArk's website](#), read the CyberArk blogs, or follow on Twitter via @CyberArk, LinkedIn, or Facebook.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, refer to:

- [Zscaler Resources](#)
- [CyberArk Resources](#)
- [Appendix A: Requesting Zscaler Support](#)

Software Versions

This document was authored using the latest version of the Zscaler software.

Request for Comments

- **For prospects and customers:** we value reader opinions and experiences. Contact us at partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees:** contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and CyberArk Introduction

Below are overviews of the Zscaler and CyberArk applications described in this deployment guide.

ZIA Overview

ZIA is a secure Internet and web gateway delivered as a service from the cloud. Think of it as a secure Internet onramp—all you do is make Zscaler your next hop to the Internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the Internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and Internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, CASB, and Browser Isolation, allowing you start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on cloud or data center using a zero trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler support portal for submitting requests and issues.

CyberArk Access Management Overview

CyberArk provides full protection from advanced and insider threats to mitigate your risks and meet high stakes compliance requirements. CyberArk supports any device, any data center, for on-premises, hybrid, and cloud environments, as well as throughout the DevOps pipeline. CyberArk is with a native solution that provides full protection, monitoring, detection and reporting of all privileged access.

CyberArk Resources

The following table contains links to CyberArk support resources.

Name	Definition
CyberArk Online Help	Online help articles for CyberArk solutions.

Zscaler SAML Single Sign-On (SSO)

The following is an overview of the steps required to configure ZIA or ZPA for single sign-on (SSO) via SAML. Zscaler offers both IdP-initiated SAML SSO (for SSO access through the user portal or CyberArk mobile applications) and SP-initiated SAML SSO (for SSO access directly through ZIA). You can configure Zscaler for either or both types of SSO. Enabling both methods ensures that users can log in to Zscaler in different situations such as clicking through a notification email.

SP-initiated SSO for Zscaler is automatically enabled when the SAML feature is activated.

1. Prepare Zscaler for single sign-on (see Zscaler requirements for SSO).
2. Configure ZIA or ZPA for single sign-on.
3. In the Admin Portal, add the application and configure application settings.

After the application settings are configured, complete the user account mapping and assign the application to one or more roles.

After you have finished configuring the application settings in the ZIA or ZPA Admin Portal, users are ready to launch the application from the CyberArk Identity User Portal.

4. Configure the end-user web browser proxy.

Zscaler Requirements for SSO

Before you configure the ZIA or ZPA for SSO, you need the following:

- An active Zscaler account with administrator rights for your organization.
- A signed certificate. You can either download one from the Admin Portal or use your organization's trusted certificate.

Zscaler SAML Properties

Each SAML application is different. The following table lists features and functionality specific to Zscaler.

Capability	Supported?	Support Details
Web browser client	Yes	
SAML 2.0	Yes	
SP-initiated SSO	Yes	
Force user login via SSO only	Yes	
Separate administrator login after SSO is enabled	Yes	
Automatic user provisioning	Yes	
Multiple User Types	Yes	Only administrators can log in.
Access restriction using a corporate IP range	Yes	



The examples in this deployment guide use ZIA screens, but the steps apply to ZPA as well.

Configure Zscaler in the CyberArk Admin Portal (Part 1)

To add and configure ZIA or ZPA in the CyberArk Admin Portal:

1. In the CyberArk Admin Portal, click **Apps & Widgets > Web Apps > Add Web Apps**. The **Add Web Apps** screen appears.

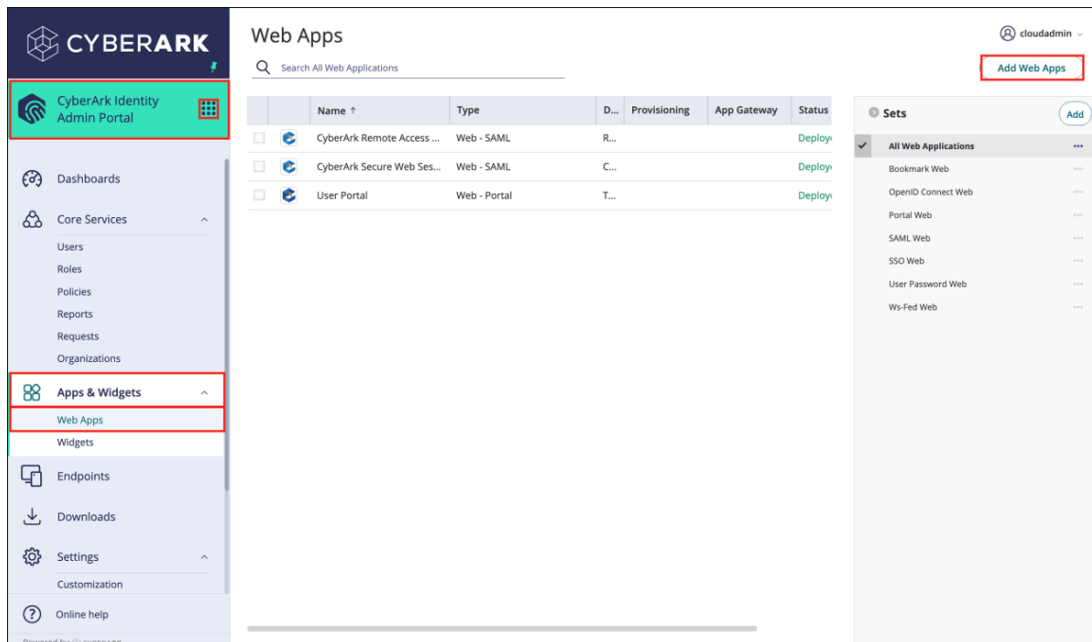


Figure 1. CyberArk Web Apps

2. On the **Search** tab, enter **zscaler** in the **Search** field and click **Search**.
3. Next to the application, click **Add**.
4. In the **Add Web App** screen, click **Yes** to confirm.
5. Admin Portal adds the application.

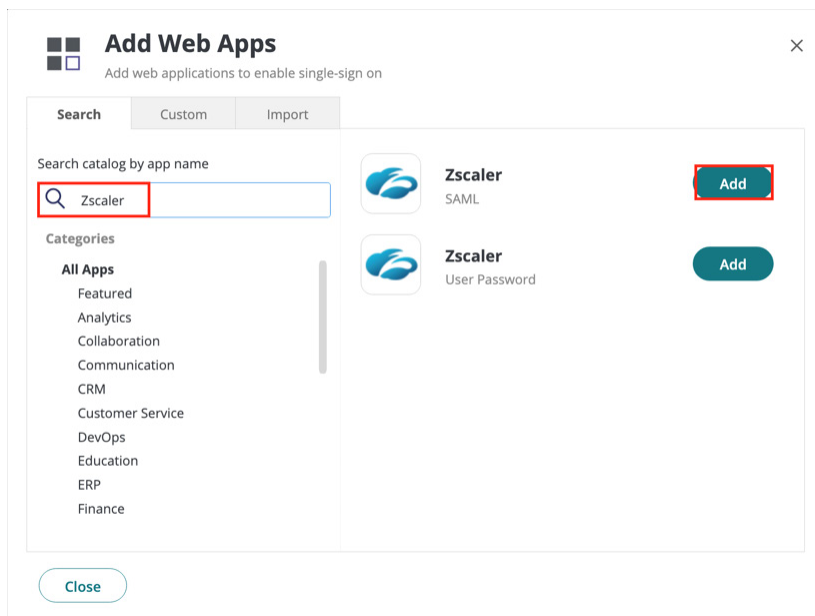


Figure 2. Add Web Apps

6. Click **Close**.

Selecting **Add Zscaler** opens the initial configuration screen and asks for your Zscaler cloud name. This is the Zscaler cloud your organization's tenant is associated with. The Zscaler Cloud domain is one of the following cloud domains (but continues to expand): zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, or zscloud.net. This information can be found in your Zscaler Admin Portal under **Administration > Company Profile > Company ID**.

In the following Company ID example, (**zscloud.net-3173833**) "**zscloud.net**" is the Zscaler cloud that is the **Zscaler Domain**.

1. Enter your Zscaler cloud name.
2. Enter your Company ID under **Org ID**.
3. Click **Save**.

The screenshot displays the CyberArk Identity Admin Portal interface for Zscaler settings. The top navigation bar includes the CyberArk logo and a user profile dropdown for 'cloudadmin'. The left sidebar contains a menu with categories like Dashboards, Core Services, Apps & Widgets, Endpoints, Downloads, and Settings. The 'Settings' category is expanded, showing a list of settings including Trust, SAML Response, Permissions, Policy, Account Mapping, Linked Applications, Provisioning, Workflow, Changelog, Secure Web Sessions, and Settings. The 'Settings' option is selected, leading to the 'Zscaler Settings' page. The page title is 'Zscaler' and the status is 'Not Configured'. The 'Settings' section has a 'Learn more' link. The 'Your Zscaler Cloud Name' field is set to 'zscloud.net' and the 'Your Zscaler Org ID' field is set to '3173833'. The 'Description' section has a checkbox for 'Customize Name and Description for each language' which is unchecked. The 'Name' field is set to 'Zscaler' and the 'Description' field contains the text: 'Zscaler securely enables mobility, cloud applications and social media, without having to deploy any hardware or software.' The 'Category' field is set to 'Security'. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 3. CyberArk Zscaler Settings

4. Select the **Trust** tab.
5. Select **Manual Configuration**.
6. Copy the **SAML Portal URL** and save it in a location that allows you to paste it into another browser tab when configuring Zscaler.
7. Click **Download Signing Certificate**.
8. Rename the certificate filename extension for the signing certificate to .pem.

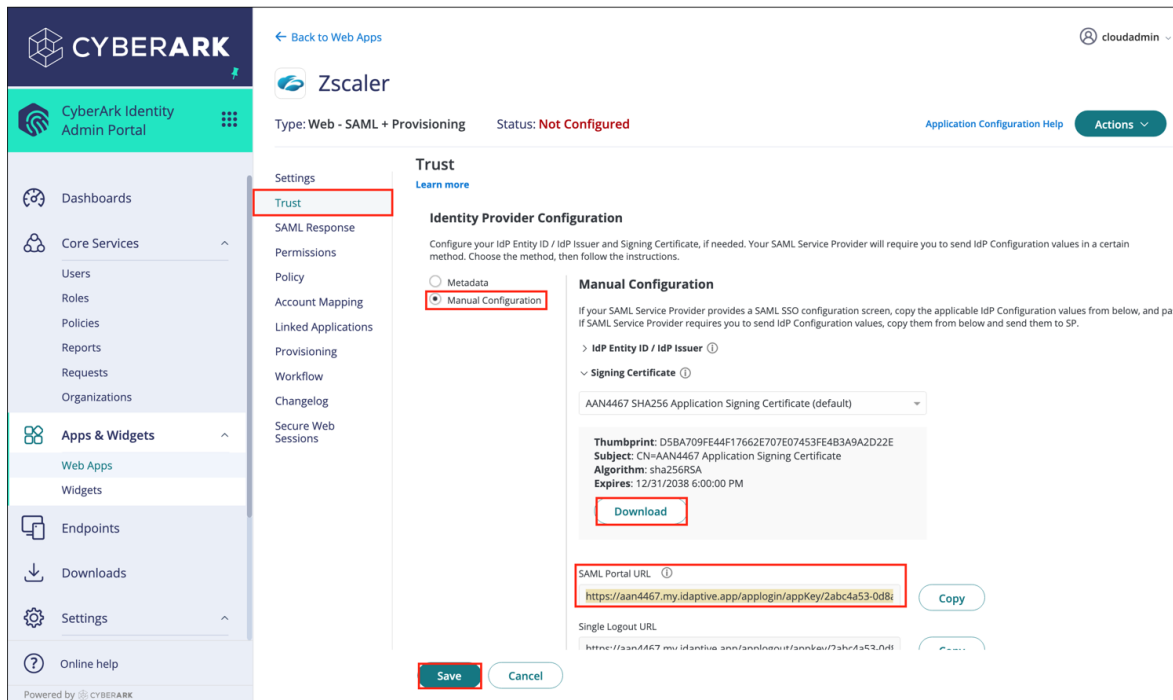


Figure 4. CyberArk Zscaler Trust

Configure Zscaler on the Zscaler Portal

To configure CyberArk as an IdP log into your ZIA or ZPA Admin Portal:

1. Go to **Administration > Authentication > Authentication Settings > Identity Providers > Add IdP**.

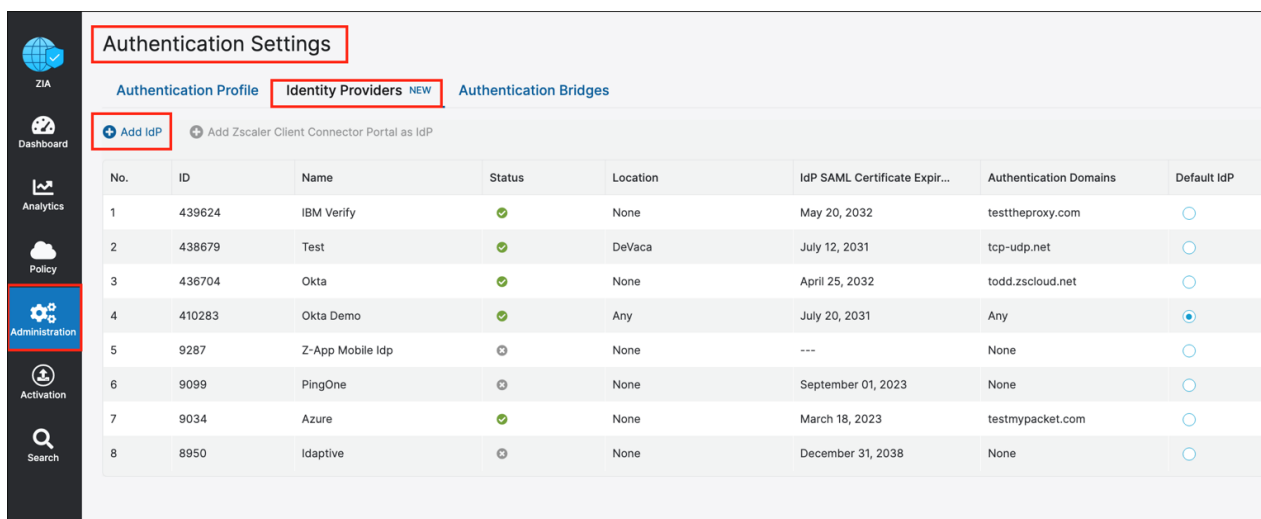


Figure 5. ZIA Add Idp

2. Give the IdP a **Name**.
3. Set the **Status** to **Enabled**.
4. Paste in the **SAML Portal URL** copied from CyberArk.
5. Enter NameID as case-sensitive name for the **Login Name Attribute**.
6. Upload the CyberArk Public Certificate.
7. Select **Others** as the **Vendor**.
8. Leave the **Locations** and **Authentication Domains** as **none** for **Default IdP**, or select the authentication domain for this specific IdP.
9. Enable the **Sign SAML Request** setting.
10. Select the latest **Signing SAML Certificate**.
11. Download the SP Metadata to be uploaded on the CyberArk configuration.
12. If enabling SCIM, **Save** the configuration. It must be saved before SCIM can be enabled, or proceed to the next section to enable SAML auto-provisioning.

Edit IdP

GENERAL INFO

Name
CyberArk

Status
☒ Enabled ☐ Disabled

SAML Portal URL
https://aan4174.my.idaptive.app/applogin/a...

Login Name Attribute
NameID

Entity ID
zscloud.net

Org-Specific Entity ID
☐ Enabled ☒ Disabled

IdP SAML Certificate
AAN4174 SHA256 Application Signing Certificate1.pem [Upload](#)

IdP SAML Certificate Expiration Date
December 31, 2038

Vendor
Others

Default IdP
☒ Disabled

CRITERIA

Locations
None

Authentication Domains
todd.zscloud.net

SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request
☒

Signature Algorithm
☒ SHA-1 (160-bit) ☐ SHA-2 (256-bit)

Request Signing SAML Certificate
saml_2022

SP SAML Certificate Expiration Date
November 16, 2022


SP Metadata
[Download Metadata](#)

SP SAML Certificate
[Download Certificate](#)

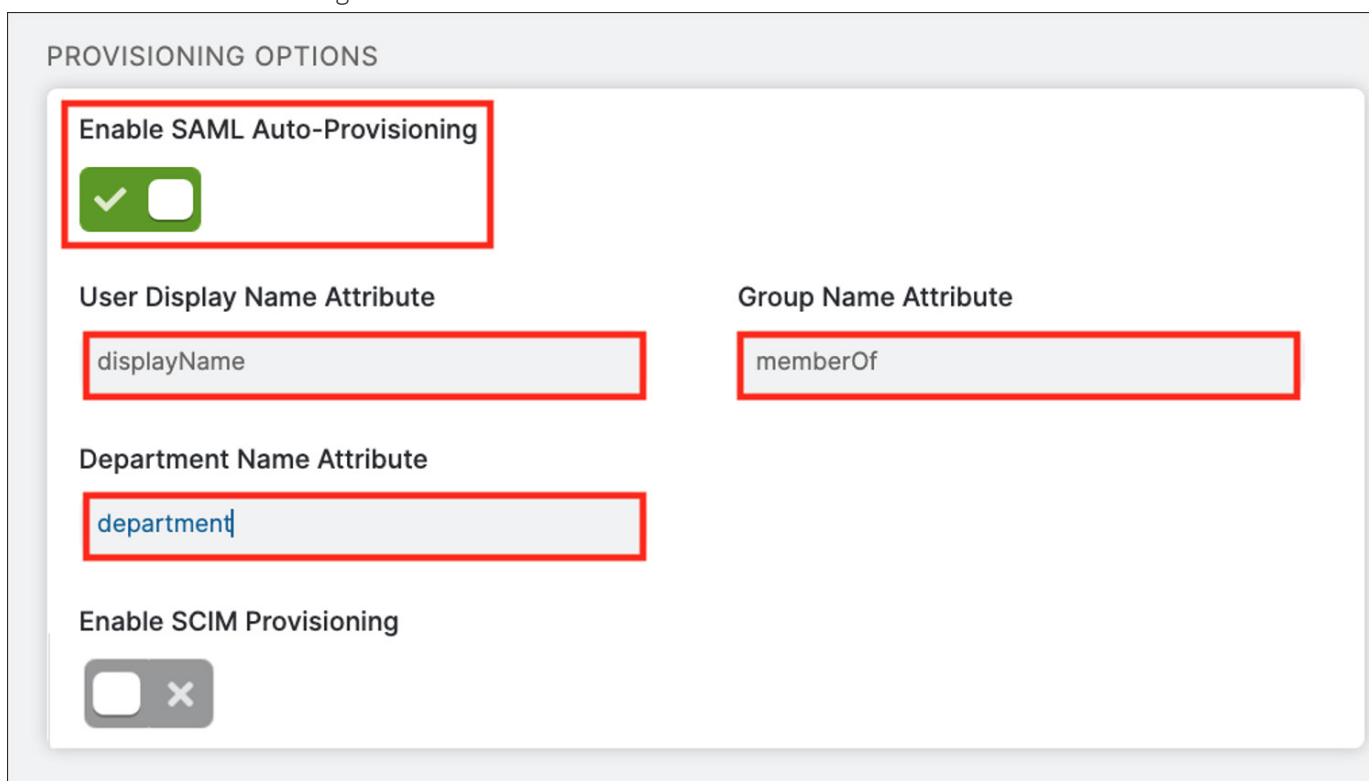
Figure 6. Edit IdP

Enable SAML Auto Provisioning

To enable SAML auto-provisioning:

 If enabling SCIM, save and activate the configuration and skip to the Enable SAML section.

1. Enable **SAML Auto-Provisioning**.
2. For the **User Display Name Attribute** enter `displayName` (case-sensitive).
3. For the **Group Name Attribute** enter `memberOf` (case-sensitive).
4. For the **Department Name Attribute** enter `department` (case-sensitive).
5. **Save** and **Activate** the configuration.



PROVISIONING OPTIONS

Enable SAML Auto-Provisioning

☒

User Display Name Attribute

displayName

Group Name Attribute

memberOf

Department Name Attribute

department

Enable SCIM Provisioning

☐

Figure 7. Provisioning Options

Enable SAML

Enable the SAML configuration once an IdP has been configured, It cannot be enabled until an IdP is configured.

To enable the SAML configuration on the **Authentication Settings** page:

1. Go to **Administration > Authentication > Authentication Profile**.
2. Select **SAML** as the authentication type.
3. **Save** and **Activate** the configuration.

Authentication Settings

Authentication Profile Identity Providers NEW Authentication Bridges

AUTHENTICATION PROFILE UPDATED

User Repository Type

☒ Hosted DB ☐ Active Directory ☐ OpenLDAP

Authentication Frequency

▼

Authentication Type

☐ Form-Based ☒ SAML ☒ Open Identity Providers

Temporary Authentication

☒ Disabled ☐ One-Time Link

KERBEROS AUTHENTICATION

Enable Kerberos

☒

Domain Trust Password

***** [Reveal Password](#) [Generate New Password](#)

Figure 8. Authentication Profile

Provision Accounts with SCIM

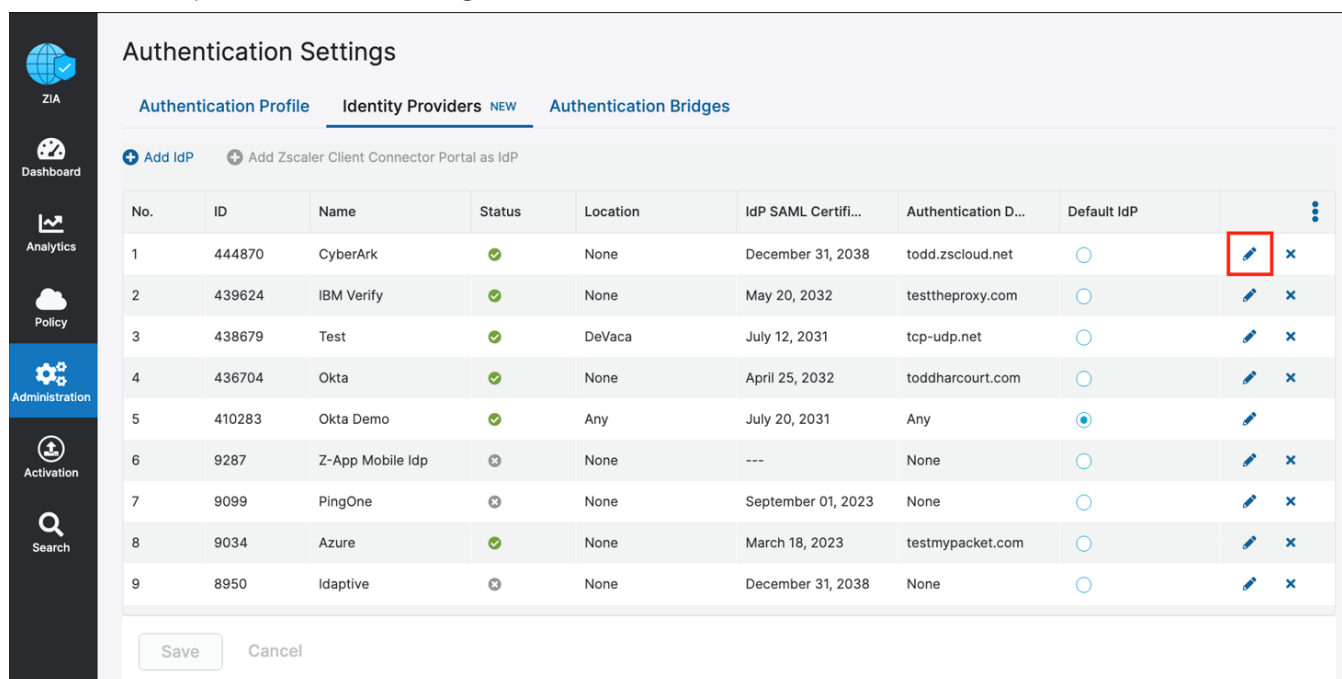
This topic describes how to provision users to SAML applications using SCIM (System for Cross-domain Identity Management). SCIM support varies by service provider. Always consult your service provider's documentation for details regarding their SCIM implementation.

SCIM is an open standard for automating the exchange of user identity information between identity domains, or IT systems. It can be used to automatically provision and deprovision accounts for users in external systems such as SAML apps. For more information about SCIM, see www.simplecloud.info.

Enable SCIM Provisioning for Your App in the Admin Portal

To enable SCIM, go back into the IdP configuration after it has been saved and activated. The feature is grayed out until saved.


















1. On the Identity Providers page go back into the configuration.
2. Select the blue pencil to edit the configuration.



Authentication Settings

Authentication Profile Identity Providers **NEW** Authentication Bridges

+ Add IdP + Add Zscaler Client Connector Portal as IdP

No.	ID	Name	Status	Location	IdP SAML Certifi...	Authentication D...	Default IdP	
1	444870	CyberArk	✓	None	December 31, 2038	todd.zsccloud.net	<input type="radio"/>	 
2	439624	IBM Verify	✓	None	May 20, 2032	testtheproxy.com	<input type="radio"/>	 
3	438679	Test	✓	DeVaca	July 12, 2031	tcp-udp.net	<input type="radio"/>	 
4	436704	Okta	✓	None	April 25, 2032	toddharcourt.com	<input type="radio"/>	 
5	410283	Okta Demo	✓	Any	July 20, 2031	Any	<input checked="" type="radio"/>	
6	9287	Z-App Mobile Idp	✗	None	---	None	<input type="radio"/>	 
7	9099	PingOne	✗	None	September 01, 2023	None	<input type="radio"/>	 
8	9034	Azure	✓	None	March 18, 2023	testmypacket.com	<input type="radio"/>	 
9	8950	Idaptive	✗	None	December 31, 2038	None	<input type="radio"/>	 

Save Cancel

Figure 9. Identity Providers

3. In the **Provisioning Options** section:
 - a. Select **Enable SCIM Provisioning**.
 - b. Copy and save the **Base URL** and the **Bearer Token** to finish the CyberArk Configuration.
 - c. Click **Save** and **Activate** the configuration.

PROVISIONING OPTIONS

Enable SAML Auto-Provisioning

✓

User Display Name Attribute

displayName

Group Name Attribute

memberOf

Department Name Attribute

department

Enable SCIM Provisioning

✕

Figure 10. Provisioning Options

4. To enable SCIM provisioning on CyberArk:
 - a. Select the **Provisioning** tab in ZIA or ZPA.
 - b. Enter the **SCIM Service URL** copied from the **Zscaler SCIM Identity Provider** field.
 - c. Enter the **Bearer Token** value into the **Bearer Token** field.
 - d. Select **Verify** to test the API credentials.



You must save the Zscaler configuration and enable SAML for Verify to pass.

- e. Select **Delete user** under **User Deprovisioning Options**.
- f. Select **Add** under **Role Mappings** and select the **Groups/Roles** to synchronize.
- g. Click **Save**.

PROVISIONING OPTIONS

Enable SAML Auto-Provisioning

☐

Enable SCIM Provisioning

☒

Base URL

https://scim.zscloud.net/3173833/444870/scim

Bearer Token

AQypxoiD2v5fuAxayPAAbopM5dldfxHDP42IoAl3wG3UvWTvKryBN9P6nae7McXgWw==

Generate Token

DEVICE TRUST

Device Trust Attribute

Enter Text

Device Trust Attribute Value

Enter Text

Save

Cancel

Figure 11. ZIA Provisioning

Verify Users to Synchronize

To verify which users get synchronized:

1. Select **Core Services** > **Roles**.
2. Select the **Role** selected in the SCIM configuration.

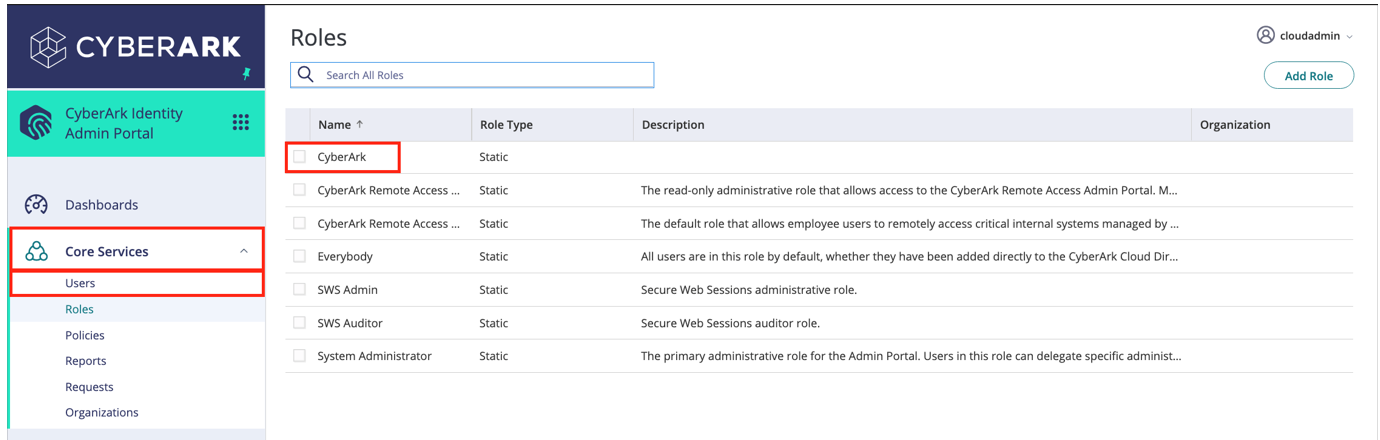


Figure 12. CyberArk User Roles

3. Select **Members** to verify the uses that get synchronized.

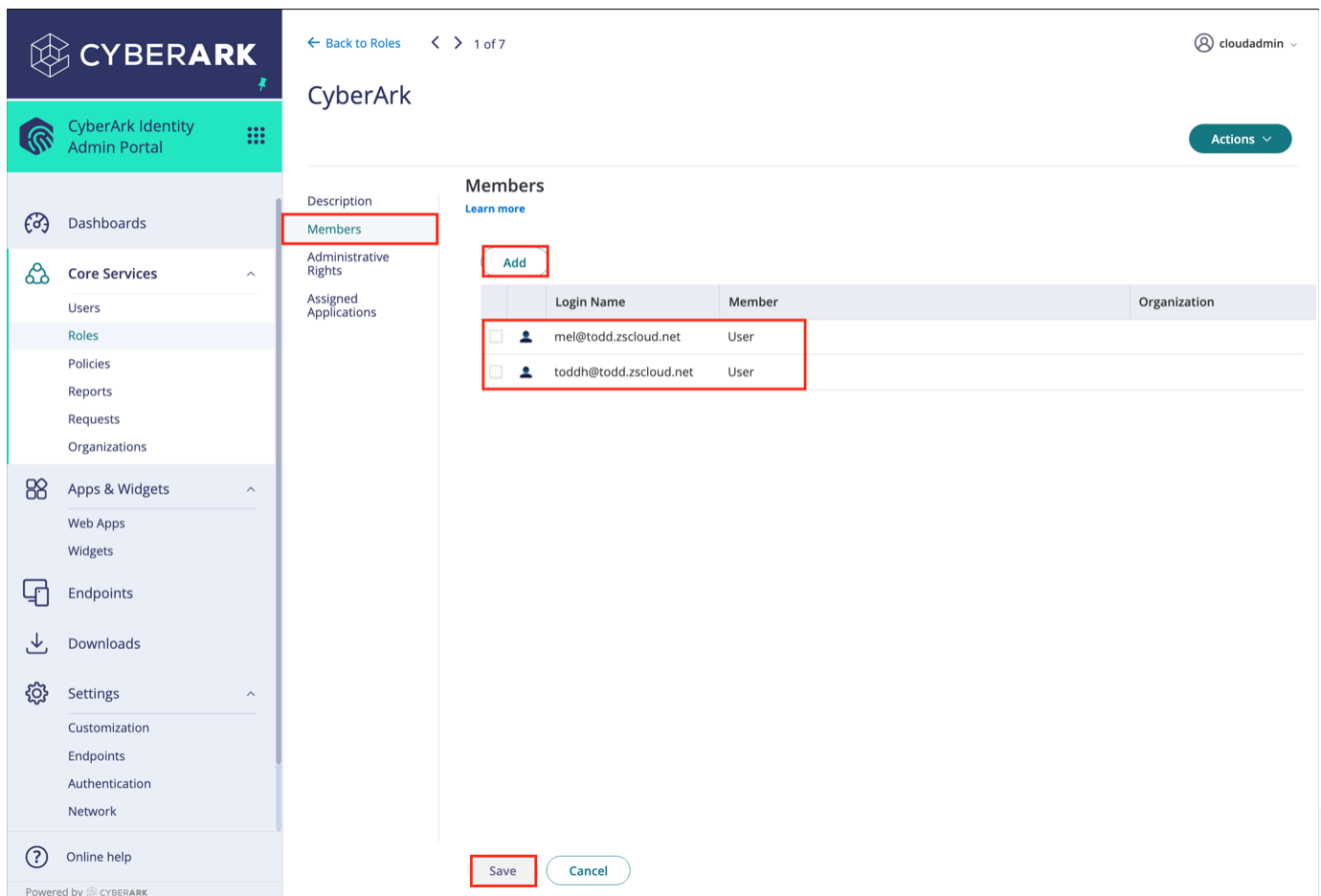


Figure 13. CyberArk Member Roles

4. Select **Assigned Applications** and add Zscaler Internet Access.
5. Click **Save**.

The screenshot displays the CyberArk Identity Admin Portal interface. On the left, a sidebar contains navigation links: Dashboards, Core Services (Users, Roles, Policies, Reports, Requests, Organizations), Apps & Widgets (Web Apps, Widgets), Endpoints, Downloads, Settings (Customization, Endpoints, Authentication, Network), and Online help. The 'Assigned Applications' link under 'Administrative Rights' is highlighted. The main content area is titled 'Assigned Applications' with the instruction 'Assign existing applications to this role.' An 'Add' button is highlighted in red. Below it is a table with the following data:

	Name	Type	Description
<input type="checkbox"/>	Zscaler Internet Access	Web - SAML	Zscaler securely enables mobility, cloud applications and social media, wit...

At the bottom of the main area, 'Save' and 'Cancel' buttons are visible, with 'Save' highlighted in red. The top right shows a user profile 'cloudadmin' and an 'Actions' dropdown. A URL bar at the bottom left shows 'https://aan4174.my.idaptive.app/admin#/RoleList'.

Figure 14. CyberArk Assigned Applications

Enable SCIM Synchronization

To enable SCIM synchronization:

1. Select **Settings > Users > Outbound Provisioning**.
2. Select **Zscaler Internet Access**.
3. Select **Start Sync** to start the initial SCIM sync.
4. Check the box for run synchronization for all enabled applications.
5. Select a time for the daily **SCIM Sync**.
6. Click **Save**.

The screenshot displays the CyberArk Identity Admin Portal interface. On the left, the navigation sidebar includes sections for Core Services, Apps & Widgets, Endpoints, Downloads, Settings, and Online help. The 'Settings' section is expanded, showing 'Customization', 'Endpoints', 'Authentication', 'Network', and 'Users'. The 'Users' section is further expanded, highlighting 'Outbound Provisioning'. The main content area is titled 'Outbound Provisioning' and contains the following settings:

- Email address for report delivery:** A text input field.
- Reporting options (note: a report is always sent if an error is encountered during sync):**
 - ☒ Send report on full sync
 - ☐ Send report on individual user sync
 - ☐ Include debug trace in the report
- Synchronization:**
 - Select the provisioned application and click the Start Sync button to begin synchronization. A summary report is mailed to the report delivery address on job completion. Note: no account changes are committed for applications in preview mode.
- Provisioning Enabled Applications:**
 - A dropdown menu showing 'Zscaler Internet Access'.
 - A 'Start Sync' button.
- View Synchronization Job Status and Reports:** A link.
- Run synchronization daily for all enabled applications:** A checkbox that is checked.
- Sync Start Time (UTC / local time):** A dropdown menu showing '06:00 - 07:00 (01:00 - 02:00 CDT)'.
- Save:** A button at the bottom of the page.

Figure 15. CyberArk Outbound Provisioning

Provision Users with Custom Attributes with SCIM

After your application is configured for SCIM provisioning, SCIM provisioning can discover the target application's schema and populate the provisioning script with the attributes that it discovers. This includes any custom attributes that you have added to the target application. Attributes discovered by SCIM are commented out; you only have to remove the comment syntax and enter a source attribute to map your source attribute to the custom attribute in your application.

1. Configure your app to use SCIM, as described in previous steps.
2. Expand the Provisioning Script section and find the commented attributes discovered using SCIM that you want to map to source directory attributes.

For example, the following image shows the custom attribute Last_4_Digits_of_SSN_c__c discovered using SCIM.

Provisioning

[Learn more](#)

```

72 // // region : ,
73 // // 'streetAddress': '',
74 // // 'value': ''
75 // };
76 // destination.externalId = '';
77 // destination.locale = '';
78 // destination.meta = {
79 // // 'created': '' /* xsd:dateTime, e.g. Date.toISOString() */,
80 // // 'lastModified': '' /* xsd:dateTime, e.g. Date.toISOString() */,
81 // // 'version': ''
82 // };
83 // destination.nickName = '';
84 // destination.photos = {
85 // // 'display': '',
86 // // 'primary': false,
87 // // 'value': ''
88 // };
89 // destination.preferredLanguage = '';
90 // destination.profileUrl = '';
91 // destination.timezone = '';
92 // destination.title = '';
93 // destination['urn:salesforce:schemas:extension:00DE0000000ddVjMAI'] = {
94 // // 'echosign_dev1__EchoSign_Allow_Delegated_Sending__c': false,
95 // // 'echosign_dev1__EchoSign_Email_Verified__c': false
96 // // // 'Last_4_Digits_of_SSN_c__c': 0.0
97 // };
98 // destination.userType = '';
99 }

```

Figure 16. Provisioning script

3. Remove the comment syntax and enter the source attribute as needed.

Provisioning is done with the [SCIM PUT operation](#). The payload includes only the attributes that are explicitly set.

For example, if you have a custom AD user attribute last4SSN, the provisioning script would look like the following:

```
91 // destination.timezone = '';
92 // destination.title = '';
93 destination['urn:salesforce:schemas:extension:00DE0000000ddVjMAI'] = {
94   'echosign_dev1__EchoSign_Allow_Delegated_Sending__c': false,
95   'echosign_dev1__EchoSign_Email_Verified__c': false,
96   'Last_4_Digits_of_SSN_c__c': 'source.last4SSN'
97 };
98 // destination.userType = '';
99 }
100
```

Figure 17. Provisioning script example

4. Save your changes, then start a provisioning job for your application.

The value for the specified AD attribute is synced to the custom attribute in your application.

Refer to [Synchronize user accounts with provisioned applications](#) for more information.

Appendix A: Requesting Zscaler Support

Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round. To contact Zscaler support, select **Administration** > **Settings** > **Company profile**.

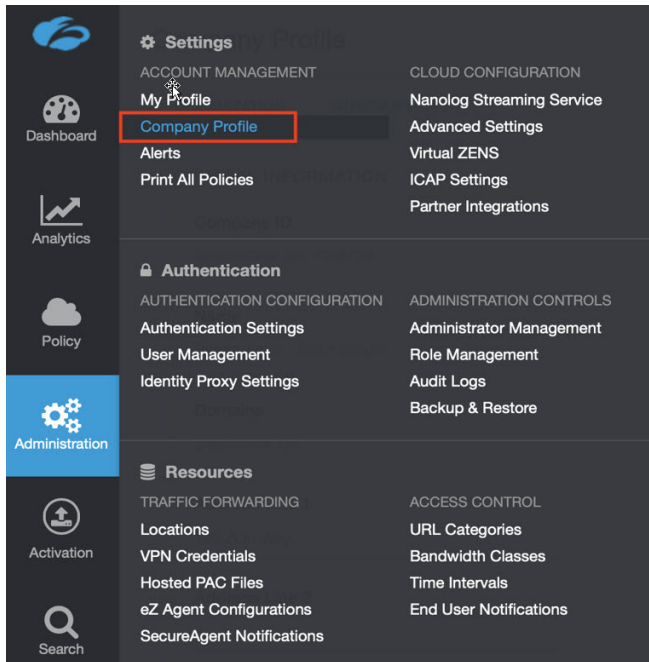


Figure 18. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.

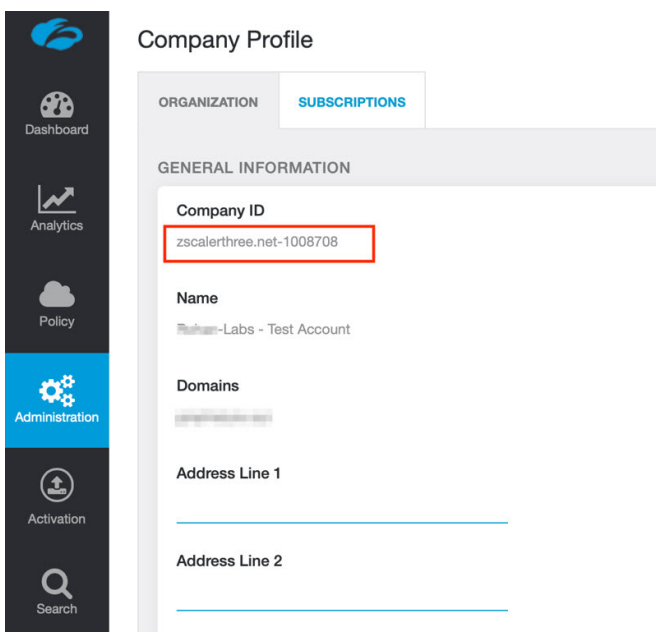


Figure 19. Company ID

Enter Support Section

With your company ID information, you can open a support ticket. Navigate to **Dashboard > Support > Submit a Ticket**.

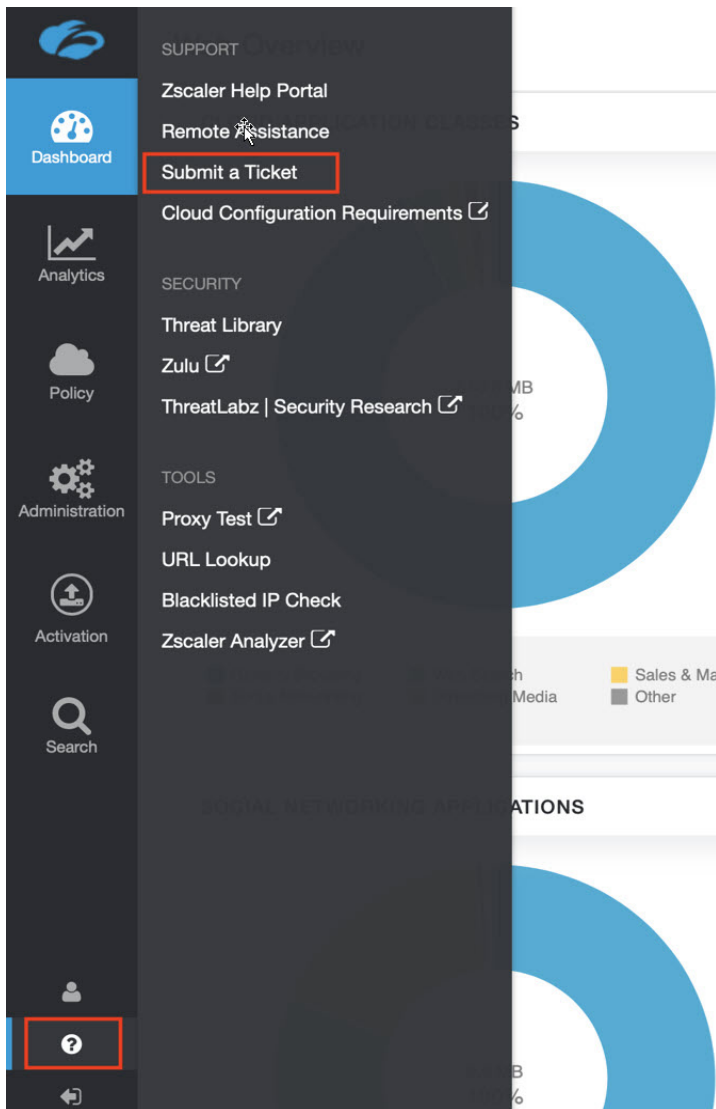


Figure 20. Submit a ticket

