# ZSCALER, OKTA, AND CROWDSTRIKE DEPLOYMENT GUIDE

FEBRUARY 2024, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

# Contents



 

 

# Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

| Acronym | Definition |
|---|---|
| CA | Central Authority (Zscaler) |
| CSV | Comma-Separated Values |
| CVE | Common Vulnerabilities and Exposures |
| DLP | Data Loss Prevention |
| DNS | Domain Name Service |
| DPD | Dead Peer Detection (RFC 3706) |
| EDR | Endpoint Detection and Response |
| GRE | Generic Routing Encapsulation (RFC2890) |
| ICMP | Internet Control Message Protocol |
| IdP | Identity Provider |
| IKE | Internet Key Exchange (RFC2409) |
| IOC | Indicators of Compromise |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol Security (RFC2411) |
| IWA | Integrated Windows Authentication |
| NGAV | Next-Generation Antivirus |
| PFS | Perfect Forward Secrecy |
| PSK | Pre-Shared Key |
| RFM | Risk Management Framework |
| SaaS | Software as a Service |
| SAML | Security Assertion Markup Language |
| SCIM | System for Cross-domain Identity Management |
| SSL | Secure Socket Layer (RFC6101) |
| TLS | Transport Layer Security |
| VDI | Virtual Desktop Infrastructure |
| WFA | Work From Anywhere |
| WS-Fed | Web Services Federation Protocol |
| XFF | X-Forwarded-For (RFC7239) |
| ZPC | Zscaler Posture Control (Zscaler) |
| ZDX | Zscaler Digital Experience (Zscaler) |
| ZIA | Zscaler Internet Access (Zscaler) |
| ZPA | Zscaler Private Access (Zscaler) |

 

# Trademark Notice

# About This Document

In WFA environments, users need access to apps outside the corporate network. This access must be based on Zero Trust to provide robust, secure access to all applications (SaaS and private apps). Zero Trust applies not only to identity, but also to device posture and access policy to provide application access.

Okta Identity Cloud centralizes identity management with a context-based policy engine. Okta and CrowdStrike establish a user and device trust chain, while Okta and Zscaler automate access restriction policies. CrowdStrike Falcon Zero Trust Assessment (ZTA) provides continuous, real-time security and compliance checks for endpoint posture, making sure that only authenticated users and compliant devices can access authorized applications at any given time. The Zero Trust Exchange service and Okta Workforce Cloud use data derived from the Falcon ZTA score to automatically update policies as needed to secure access to private apps and internet apps based on the device posture and health scores.

The following sections describe the organizations and requirements of 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. Its flagship 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. To learn more, see **Zscaler's website** or follow Zscaler on Twitter @zscaler.

## Okta Overview

Okta, Inc (Nasdaq: OKTA) is a publicly traded identity and access management company based in San Francisco. It provides cloud software that helps companies manage and secure user authentication into modern applications, and for developers to build identity controls into applications, website web services, and devices. To learn more, refer to **Okta's website**.

## CrowdStrike Overview

CrowdStrike (NASDAQ: CRWD), is a leading cybersecurity company protecting customers from all cyber threats by leveraging its Security Cloud to stop breaches. From its inception in 2011, driven by George Kurtz's vision, CrowdStrike was created as a different kind of cybersecurity company. Cloud-native, CrowdStrike immediately brought a threat perspective, effectiveness, scalability, and flexibility never seen before in the industry—seamlessly aligning People, Technology, and Processes. The CrowdStrike Falcon platform has revolutionized enterprise security for the cloud era. Its single lightweight-agent architecture leverages artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. To learn more, refer to **CrowdStrike's website**.

## 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, see:

- **Zscaler Resources**
- **Okta Resources**
- **CrowdStrike Resources**
- **Appendix A: Requesting Zscaler Support**

 

## Software Versions

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

## Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact 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, Okta, and CrowdStrike Introduction

Overviews of the Zscaler, Okta, and CrowdStrike applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

## ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just 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, and Browser Isolation, allowing you to 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 a 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, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel 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. |

 

The following table contains links to Zscaler resources for government agencies.

| 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. |

 

## Okta IWA Server Overview

The Okta IWA Web agent is a lightweight Internet Information Services (IIS) web agent that enables Desktop Single Sign-on (DSSO) on the Okta service. DSSO allows users to be automatically authenticated by Okta and any apps accessed through Okta, whenever they sign in to your Windows network.

The Okta IWA Web agent uses Microsoft's IWA and ASP.NET to authenticate users from specified gateway internet providers.

## Okta Device Trust Overview

Okta Device Trust for Windows allows you to prevent unmanaged Windows computers from accessing corporate SAML and WS-Fed cloud apps. It works with any browser or native app that can access the certificate store when performing the federated authentication flow to Okta. This includes Google Chrome, Microsoft Edge, Microsoft Internet Explorer, and Microsoft Office clients that support Modern Authentication.

## Okta Resources

The following table contains links to Okta support resources.

| Name | Definition |
|---|---|
| Okta Help Center | Okta online help for IT administrators and developers. |
| Okta How to Configure SAML 2.0 for Zscaler 2.0 | Online help for configuring SAML 2.0 for Zscaler 2.0. |
| Okta IWA Server | Online help for installing and configuring the Okta IWA Web agent for Desktop Single Sign-On. |
| Okta Device Trust | Online help for installing and configuring the Okta Device Trust for managed Windows computers. |

 

## CrowdStrike Falcon Endpoint Protection Enterprise Overview

CrowdStrike Falcon Endpoint Protection Enterprise is a cloud-native security platform that delivers an endpoint breach prevention solution. It unifies NGAV, EDR, managed threat hunting, and threat intelligence automation in a single cloud-delivered agent.

## CrowdStrike Zero Trust Assessment Overview

CrowdStrike Zero Trust Assessment (ZTA) delivers real-time security posture assessments across all endpoints regardless of location, network, and user. CrowdStrike ZTA enables enforcement of dynamic conditional access based on device health and compliance checks that mitigate the risk to users and the organization. Every endpoint is granted least-privileged access and is assessed before gaining access to sensitive data and corporate assets—ensuring Zero Trust enforcement across all endpoints. By expanding Zero Trust beyond authentication and including device security, CrowdStrike ZTA helps organizations maintain a holistic cybersecurity approach that protects their data and users from the sophisticated tactics of cyber adversaries.

## CrowdStrike Resources

The following table contains links to CrowdStrike support resources.

| Name | Definition |
|---|---|
| CrowdStrike Falcon Admin Portal | Link to CrowdStrike administration portal. |
| CrowdStrike Customer Center | CrowdStrike support portal for submitting requests and issues. |
| CrowdStrike Documentation | Link to all CrowdStrike online documentation. |
| CrowdStrike ZTA Documentation | Documentation for CrowdStrike ZTA. |
| CrowdStrike ZTA Demo | Link to a video demonstration of CrowdStrike ZTA. |
| CrowdStrike Falcon IOC Sharing integration with ZIA | GitHub repository of examples that show CrowdStrike and Zscaler integration. |

 

# Configure Okta and ZIA: SAML and SCIM

This section describes how to configure SAML and SCIM for Okta and ZIA.

This guide assumes you have a working Okta installation in your environment. If you need further information on configuring an Okta installation, see the Zscaler and Okta Deployment Guide.

## Overview

Authentication verifies a user's identity using credentials and (optionally) other additional identity factors. Security Assertion Markup Language (SAML) is the preferred method for authentication for both ZIA and ZPA. This document shows how you can configure Okta as the IdP.

SAML is an open protocol standard that allows Okta to authenticate a user and pass the authorization credentials to Zscaler services as a SAML service provider (SP). SAML also provides single sign-on (SSO) to any SAML SP (though this is beyond the scope of this document). An example is gaining access to both ZIA and ZPA by entering user credentials only once instead of having to enter it for both ZIA and ZPA. SSO enhances the user experience by providing a cohesive solution to a modern cloud and SaaS environment. SAML and SSO are the catalyst to make a unified solution possible.

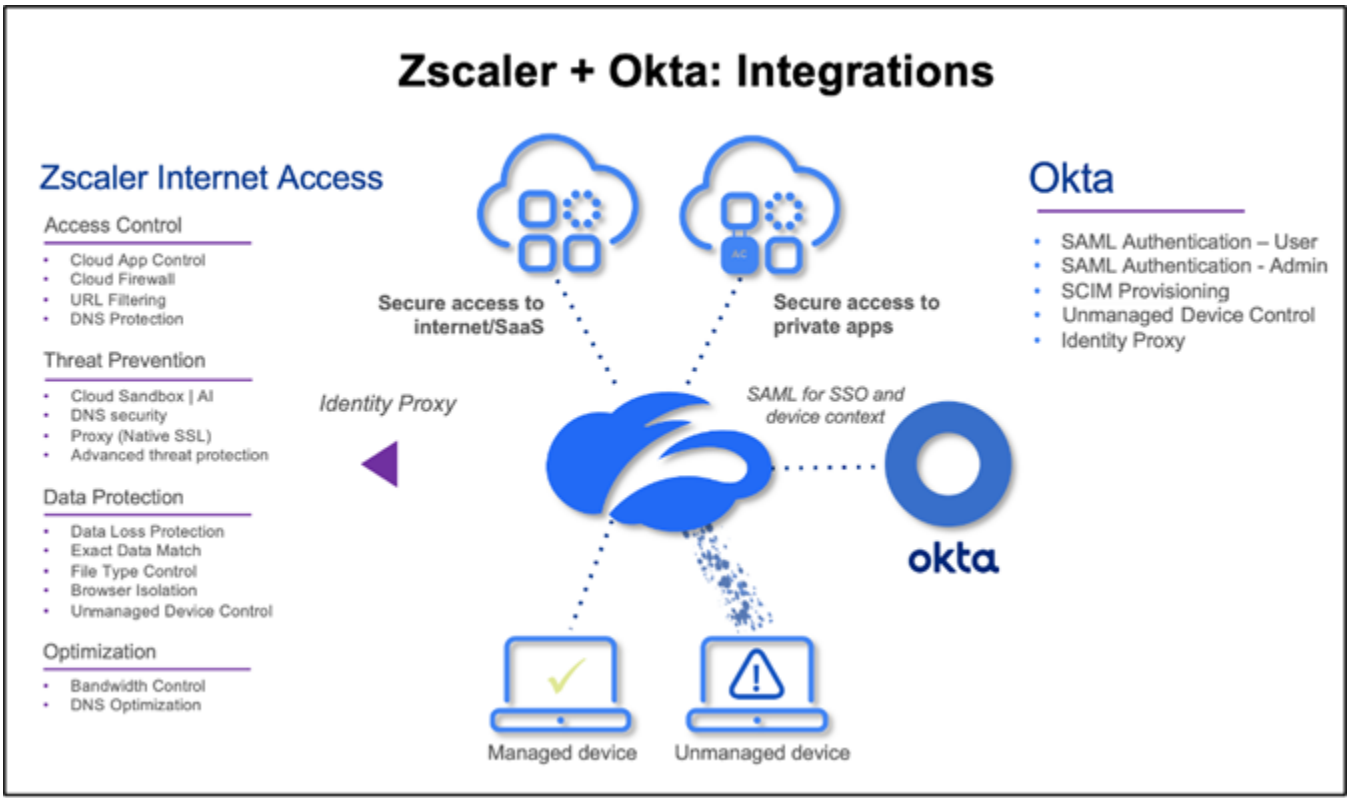


*Figure 1. ZIA and ZPA in an Okta authentication environment*

Provisioning with regards to authentication involves automating provisioning and deprovisioning users and security groups to Zscaler services. System for Cross-domain Identity Management (SCIM) is a standards-based protocol used for signaling and automating the changes in an environment. When a user is added to the user database, SCIM automatically provisions the user and the associated security groups in the Zscaler database. When deprovisioned, the user, associated groups, and credentials are removed (preventing access to resources). The primary use case is onboarding and offboarding users from an organization.

 

When a user leaves an organization, they are deprovisioned from the user directory. SCIM makes the associated changes in the Zscaler databases, eliminating all ZIA and ZPA access. SCIM then deprovisions the user from all associated databases, preventing further access to company resources.

For more information, see the resources in **Zscaler Resources**.

## Enable Okta

This document assumes that the user has a working Okta environment, and that only Zscaler applications need to be installed and configured to get the Zscaler and Okta solution up and running. This document uses a no-cost Okta developer instance created via https://developer.okta.com/. Each step was validated for functionality in a live environment.

The following steps are based on procedures documented on the Okta website using an Okta admin account.

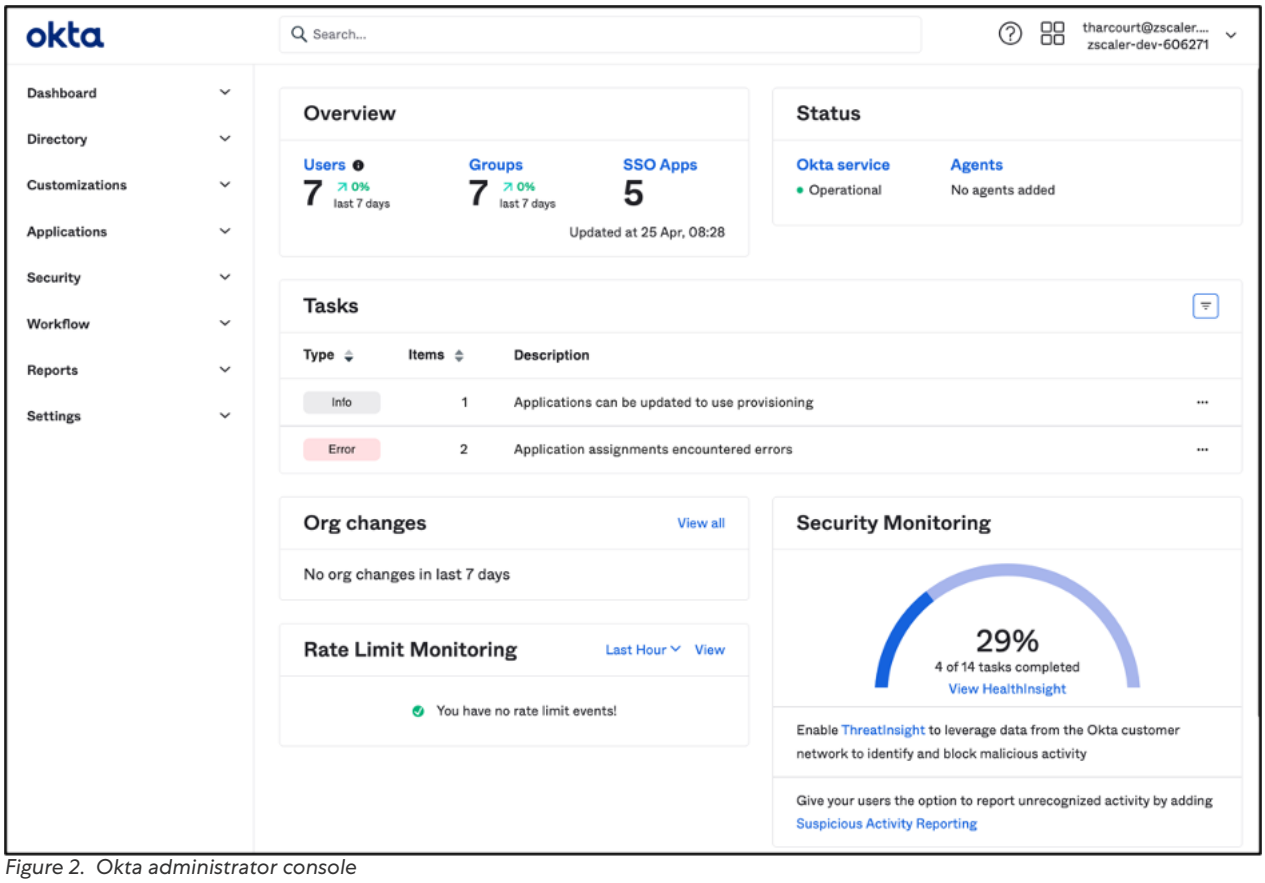


*Figure 2. Okta administrator console*

 

## Add the Zscaler ZIA Application

First, add the Zscaler applications that Okta uses for authentication and provisioning to the Zscaler service. From the Okta administrator console:

1. Open **Applications**.
2. Select **Applications**.
3. Select **Browse App Catalog**.

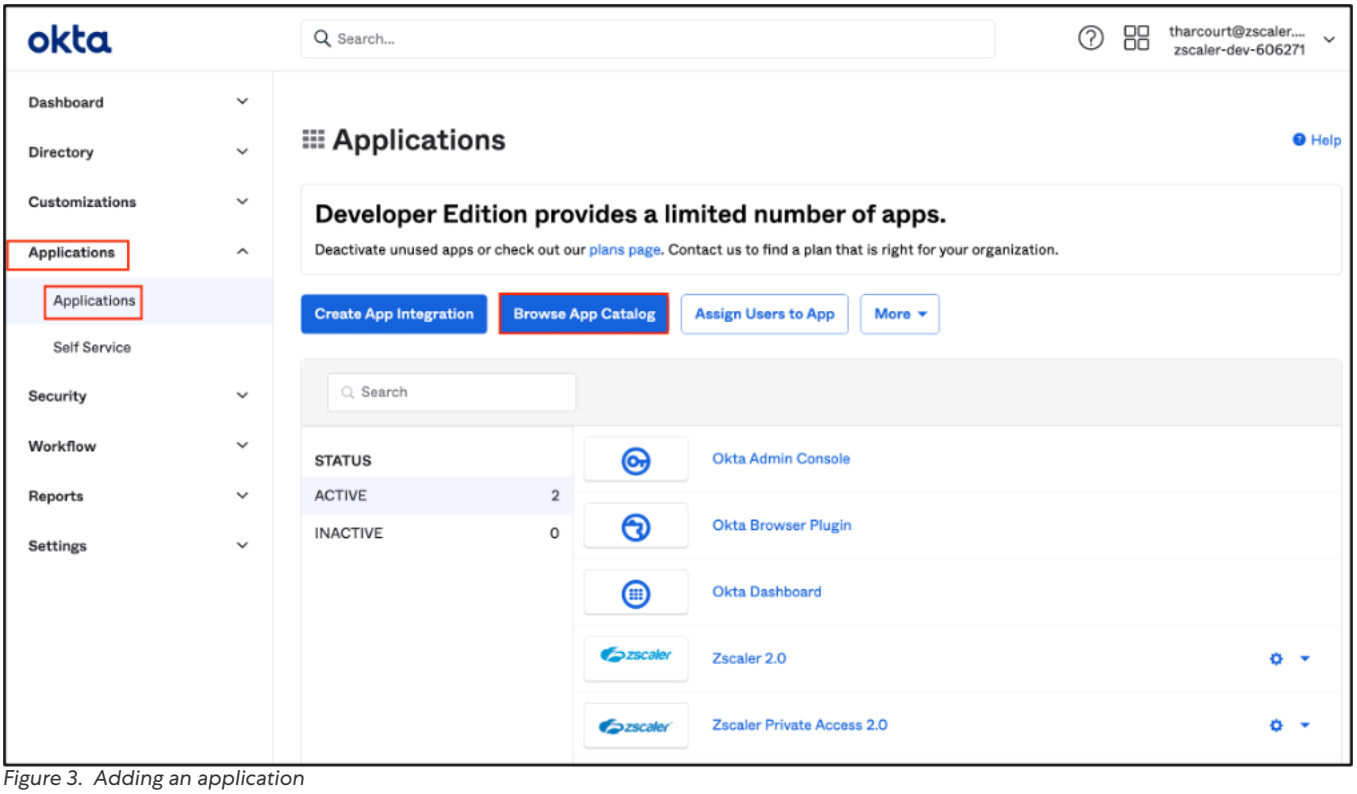


*Figure 3. Adding an application*

 

4. To add the appropriate Zscaler application, search for `zscaler`.
5. Select the **Zscaler 2.0** application.

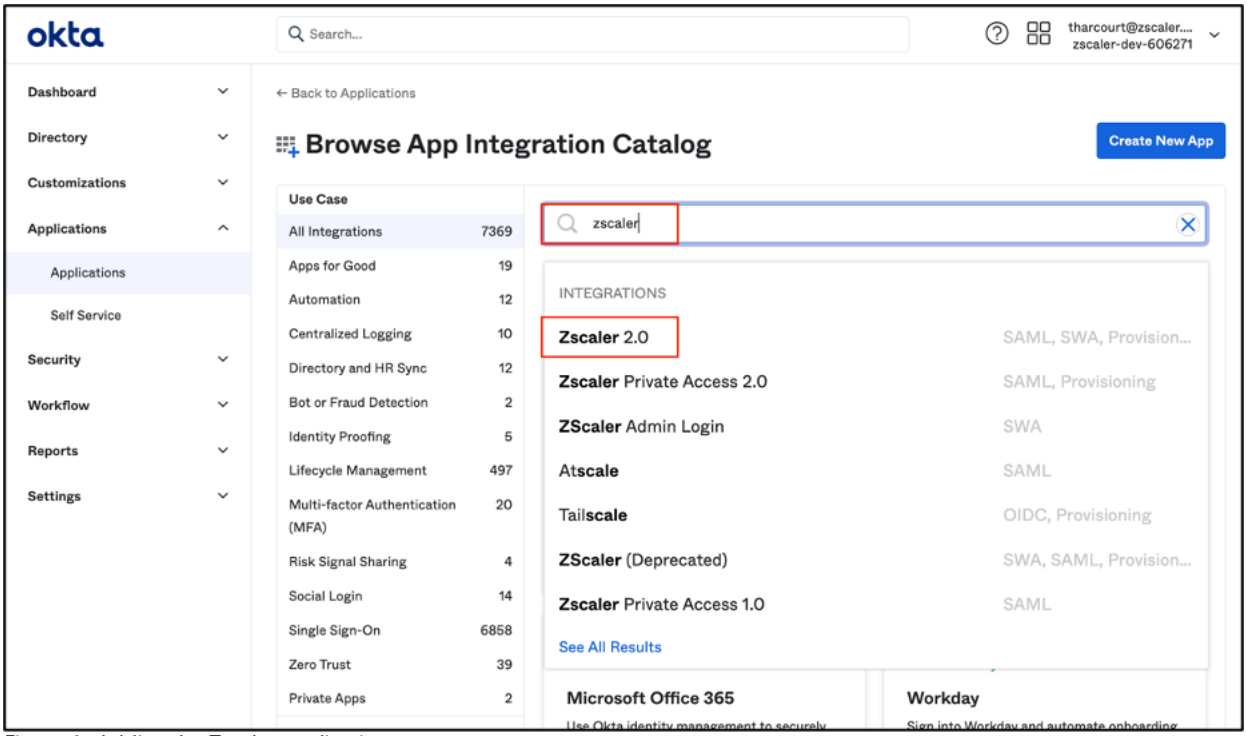


*Figure 4. Adding the Zscaler application*

6. Select **Add**.

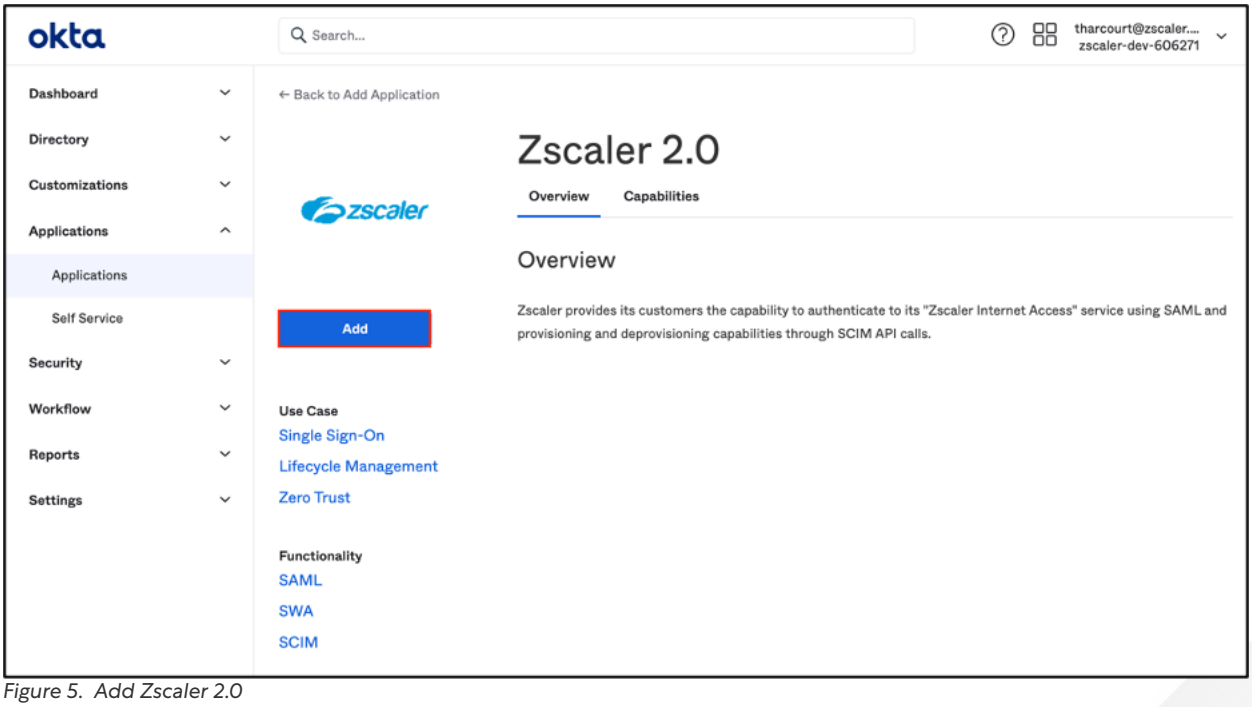


*Figure 5. Add Zscaler 2.0*

 

When you add Zscaler 2.0, the initial configuration screen is displayed and needs your Zscaler domain. This is the ZIA cloud with which your organization's tenant is associated. The current Zscaler cloud domains include zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscloud.net, and zscalerbeta.net.

You can find this information in your ZIA Admin Portal under **Administration** > **Company Profile** > **Company ID**.

In the following Company ID example, zscloud.net is the Zscaler cloud that is entered as the Zscaler domain for the Okta setup:

1. Enter **Your Zscaler Domain**.
2. Select both options for **Application Visibility**.
3. Select **Next**.

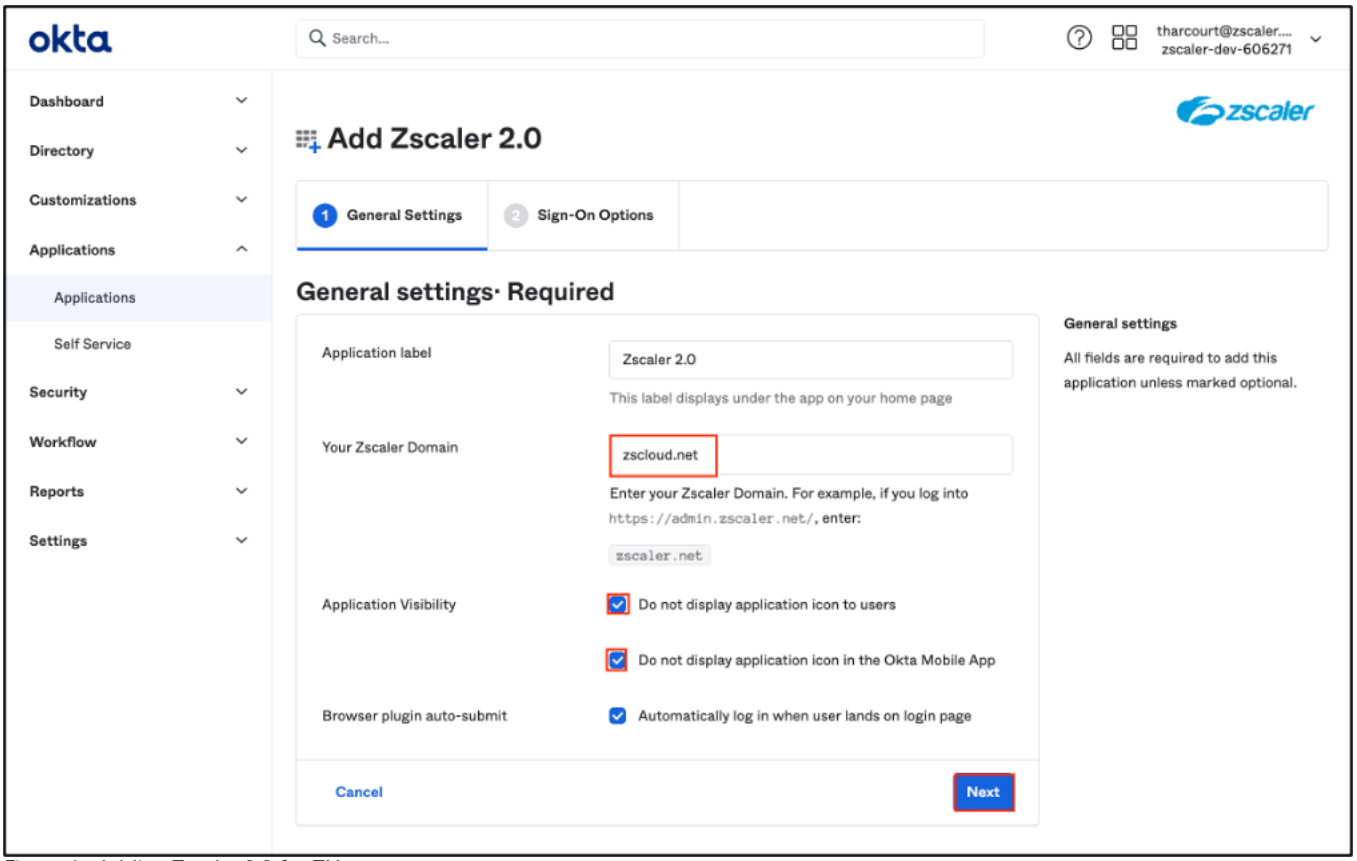


*Figure 6. Adding Zscaler 2.0 for ZIA*

 

## Configure Okta for ZIA

On the Sign-On Options window:

1. Select **SAML 2.0**.
2. Using the **memberOf** drop-down menu, select **Matches regex**.
3. In **memberOf Match**, enter `*.` (asterisk, period).
4. Select **View Setup Instructions**. Selecting **View Setup Instructions** launches a window where you find the **SAML Portal URL** and the download link to the Okta Public Certificate.

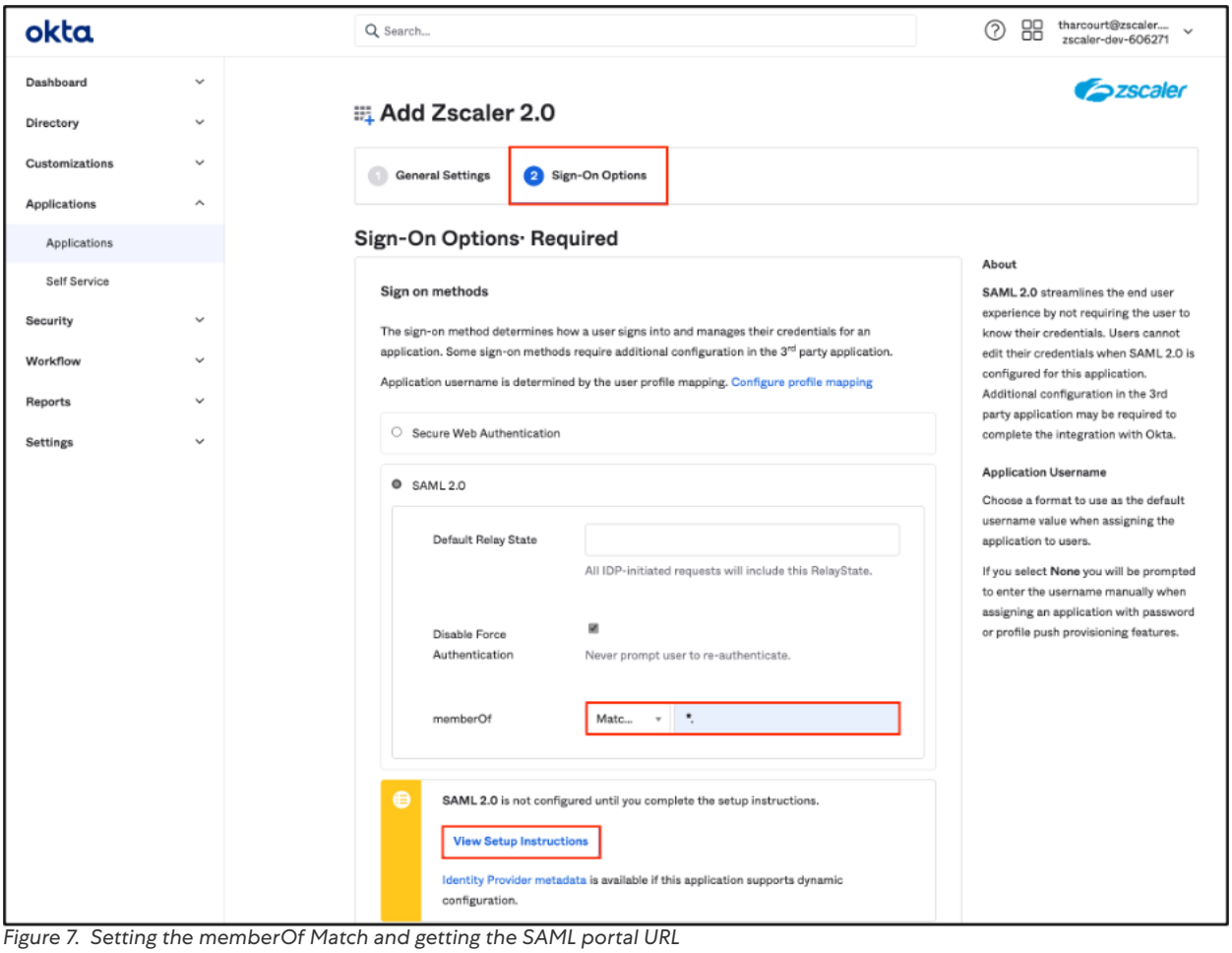


*Figure 7. Setting the memberOf Match and getting the SAML portal URL*

 

5. Copy the **SAML Portal URL**.
6. Download and save the **Public SSL Certificate** for the ZIA setup as a PEM file (i.e., cert.pem).
7. Select **Done**.

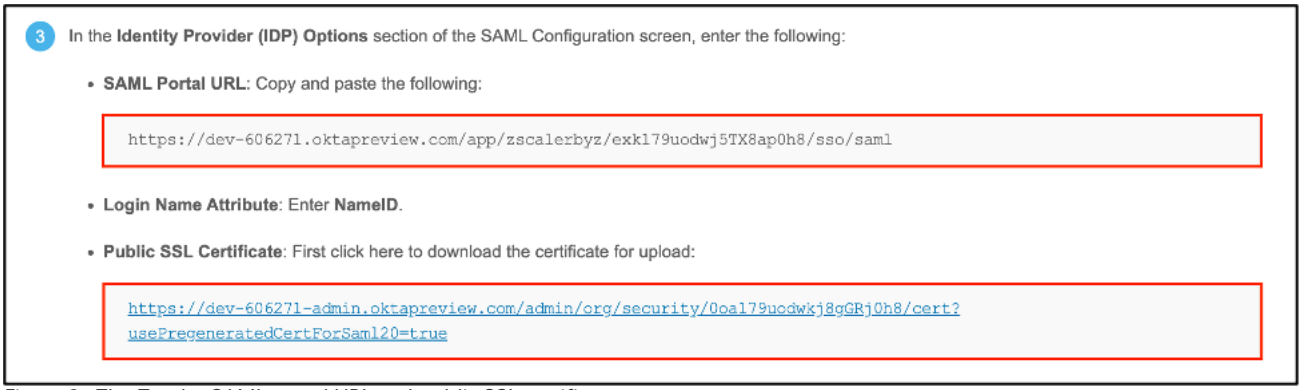


*Figure 8. The Zscaler SAML portal URL and public SSL certificate*

## Configure ZIA for an Okta IdP

To add Okta as an IdP, log in to your ZIA Admin Portal:

1. Go to **Administration > Authentication Settings**.

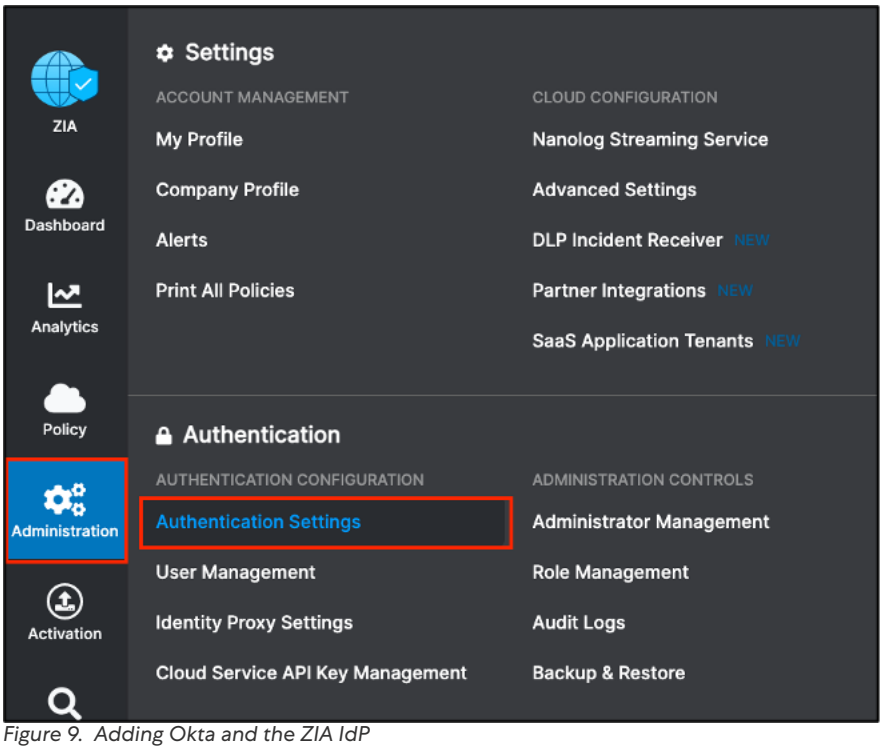


*Figure 9. Adding Okta and the ZIA IdP*

2. Select the **Identity Providers** tab.

 

3. Select **Add IdP**.

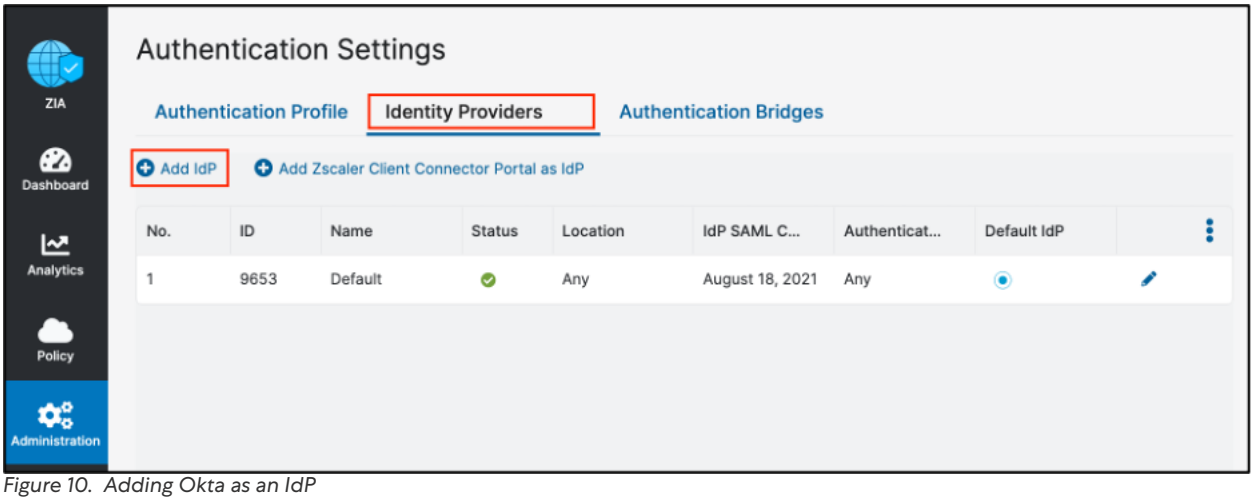


*Figure 10. Adding Okta as an IdP*

4. If this is the second IdP to assign to an additional authentication domain, select **Add another SAML IdP for a subnet of users or locations**. This opens the **Add IdP** screen.

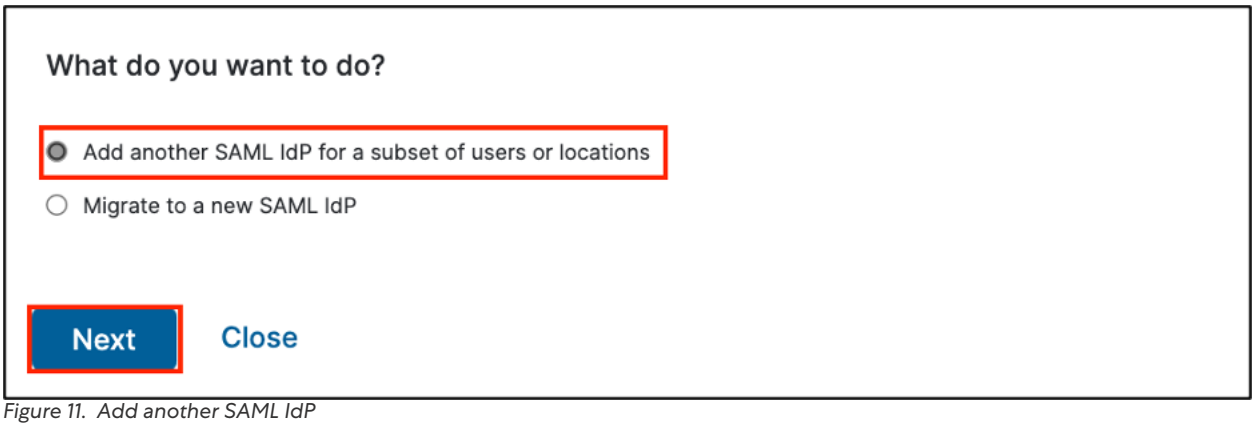


*Figure 11. Add another SAML IdP*

 

5. Give the IdP a **Name**.
6. Set the **Status** to **Enabled**.
7. Paste in the **SAML Portal URL**.
8. Enter **NameID** as case-sensitive name for the **Login Name Attribute**.
9. Upload the **Okta Public Certificate**.
10. Select **Okta** as the **Vendor**.
11. Leave the **Locations** and **Authentication Domains** as **None** for **Default IdP** (or select the authentication domain for this specific IdP).
12. Disable the **Sign SAML Request** setting.

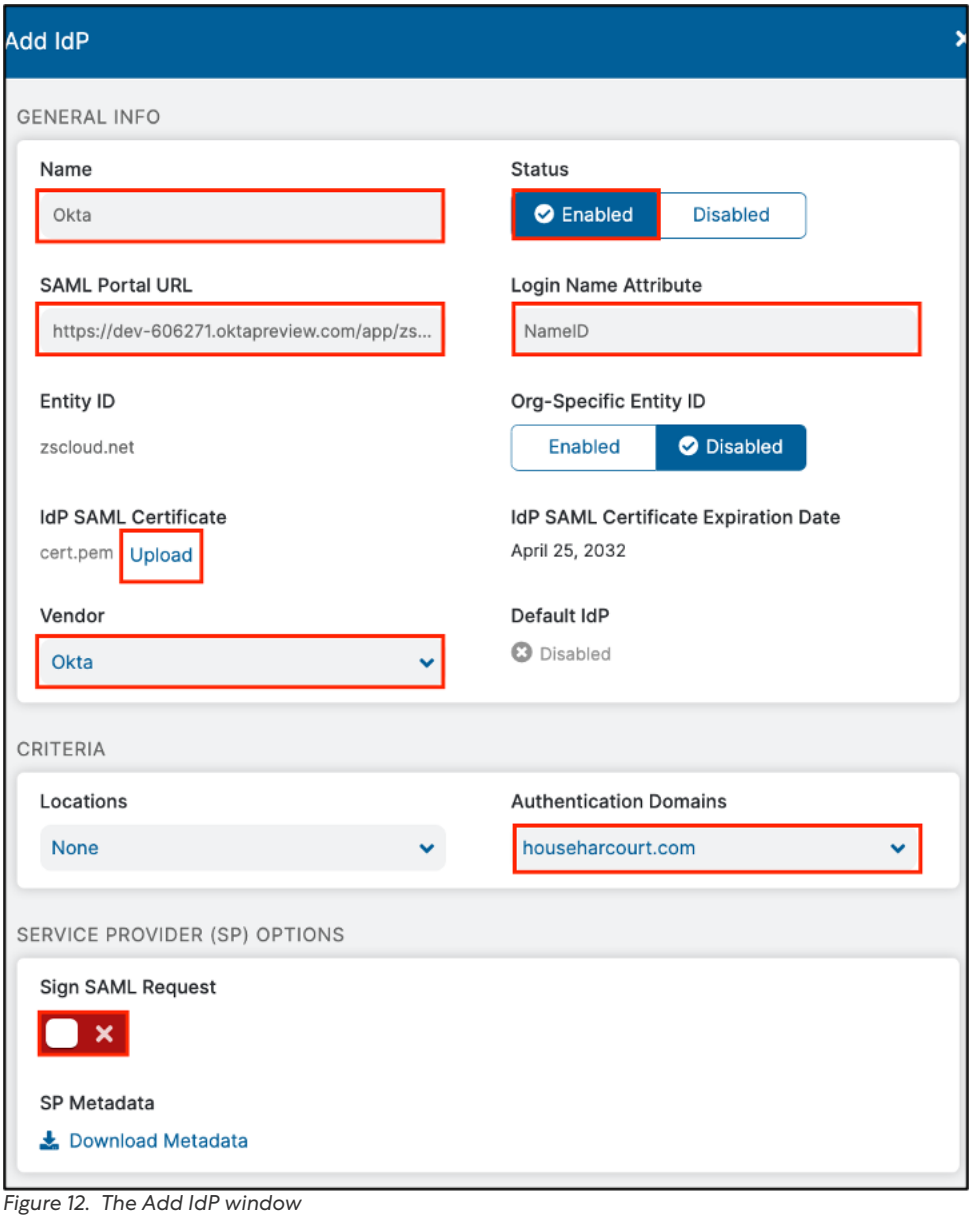


*Figure 12. The Add IdP window*

 

## Enable SAML Auto-Provisioning

To enable SAML auto-provisioning:

1. Select **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. Click **Save**, then **Activate** the configuration.

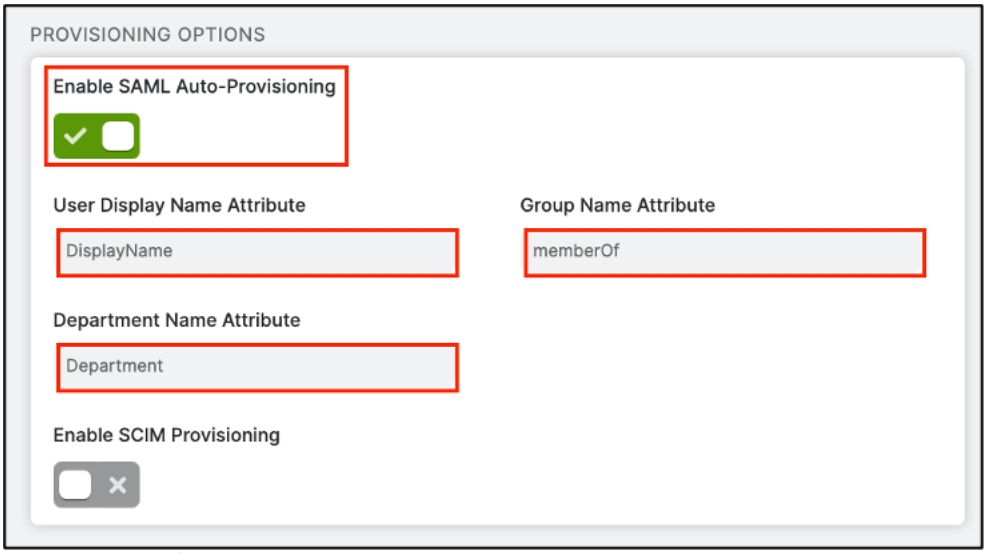


*Figure 13. Enable SAML Provisioning*

To enable SCIM, skip to Enable SCIM Provisioning.

 

To enable the SAML configuration on the Authentication Settings page:

1. Select the **Authentication Profile** tab.
2. Select **SAML** as the **Authentication Type**.
3. Click **Save**, then **Activate** the configuration.

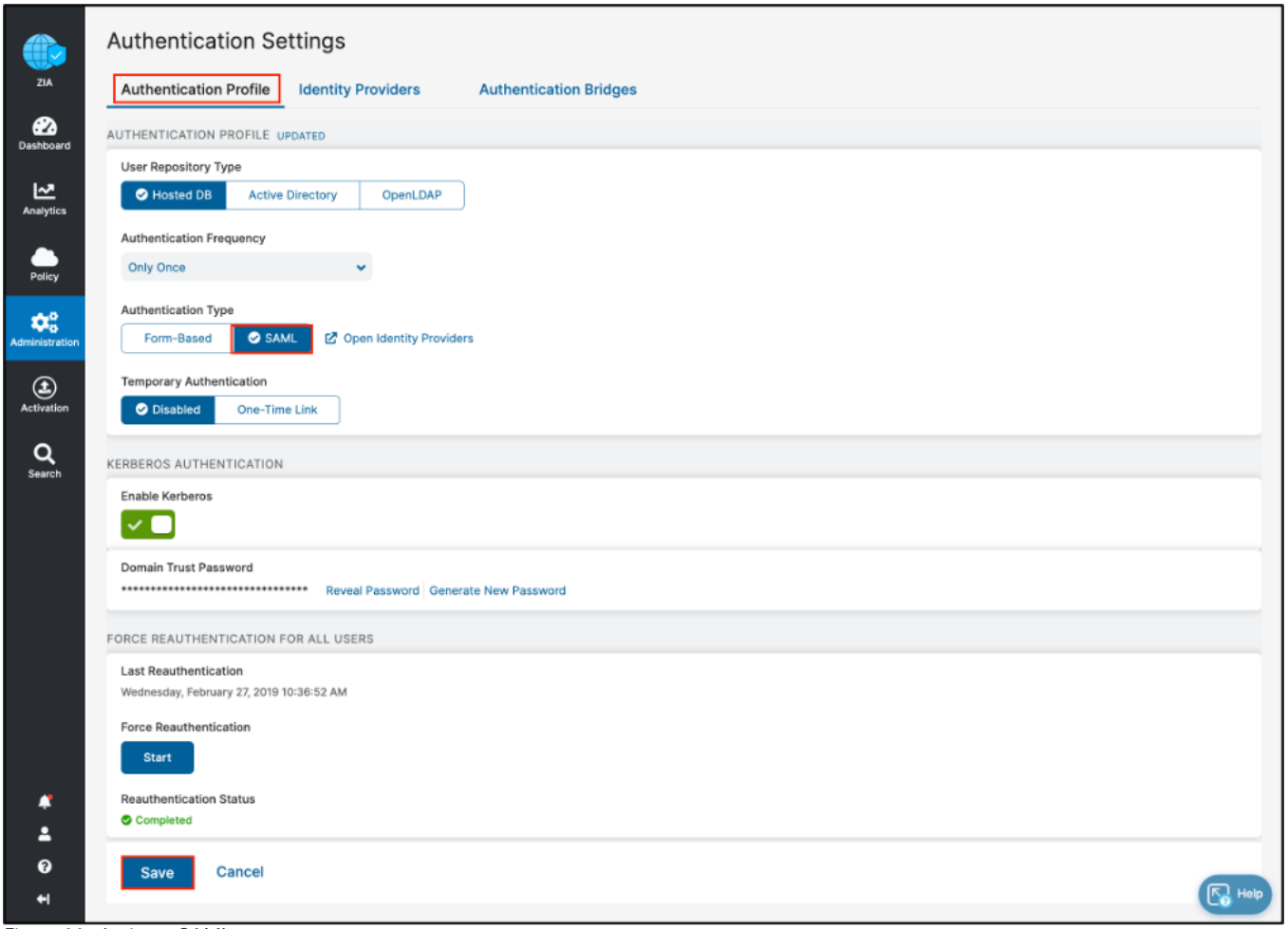


*Figure 14. Activate SAML*

 

## Enable SCIM Provisioning

To enable SCIM:

1. Return to the IdP configuration after it has been saved and activated.

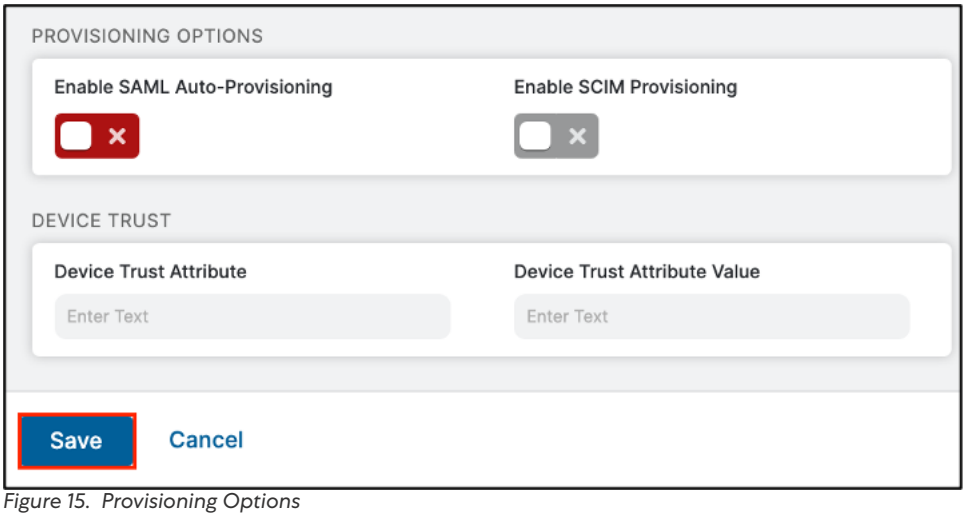


*Figure 15. Provisioning Options*

2. On the **Identity Providers** tab, return to the configuration and select the Edit icon to edit the configuration.

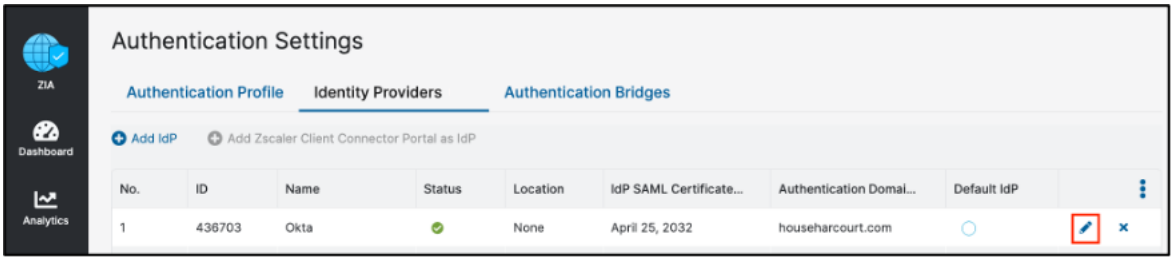


*Figure 16. Identity Providers*

 

3. In the **Provisioning Options** section, select **Enable SCIM Provisioning**.
4. Copy and save the **Base URL** and the **Bearer Token** to finish the Okta configuration.
5. Click **Save**, then **Activate** the configuration.

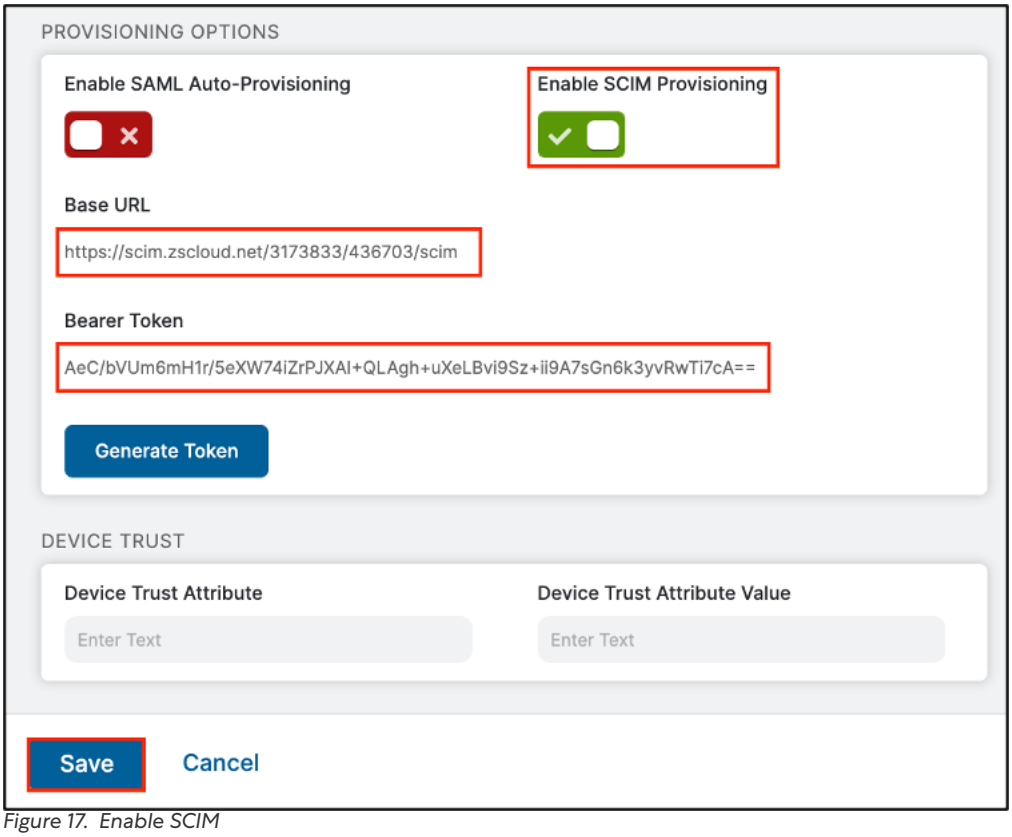


*Figure 17. Enable SCIM*

 

6. To enable the SAML and SCIM configuration on the **Authentication Settings** page, select the **Authentication Profile** tab.
7. Select **SAML** as the **Authentication Type**.
8. Click **Save**, then **Activate** the configuration.

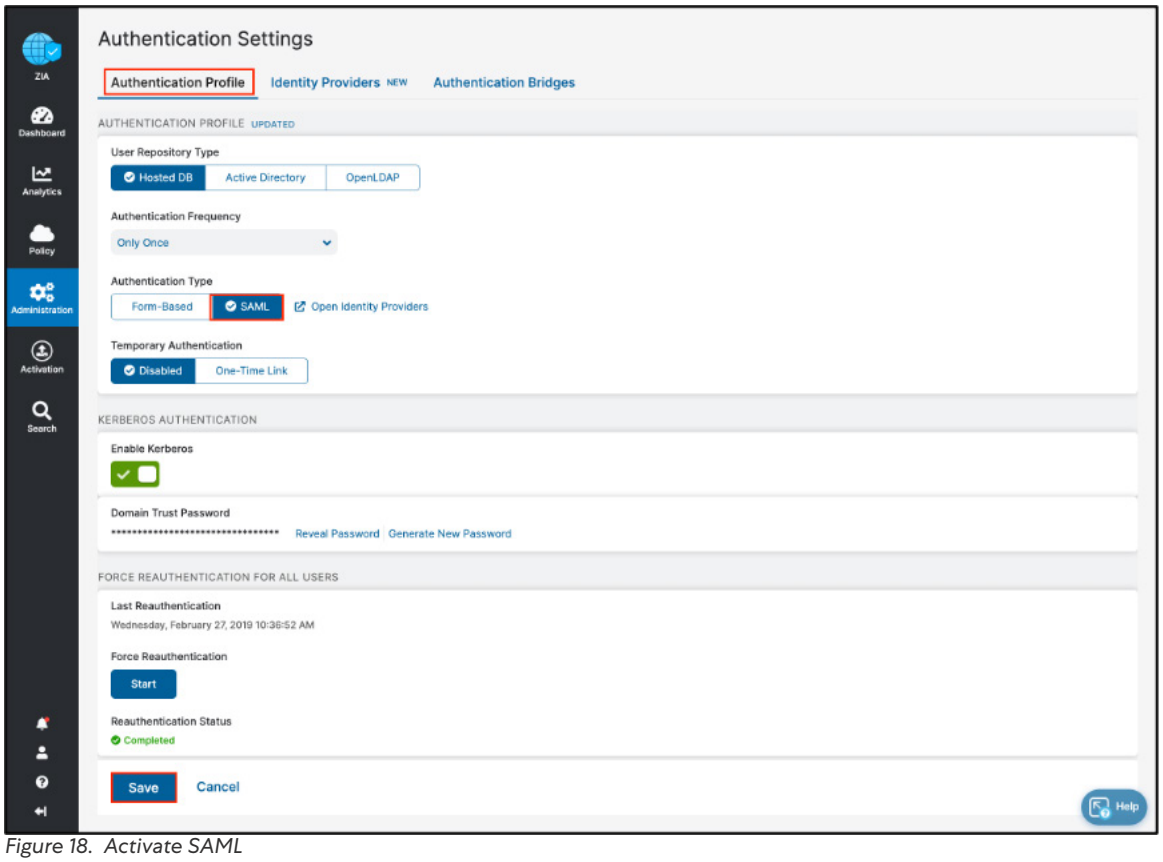


*Figure 18. Activate SAML*

 

9. To enable SCIM Provisioning on Okta, select the **Provisioning** tab.
10. Select **Configure API Integration**.

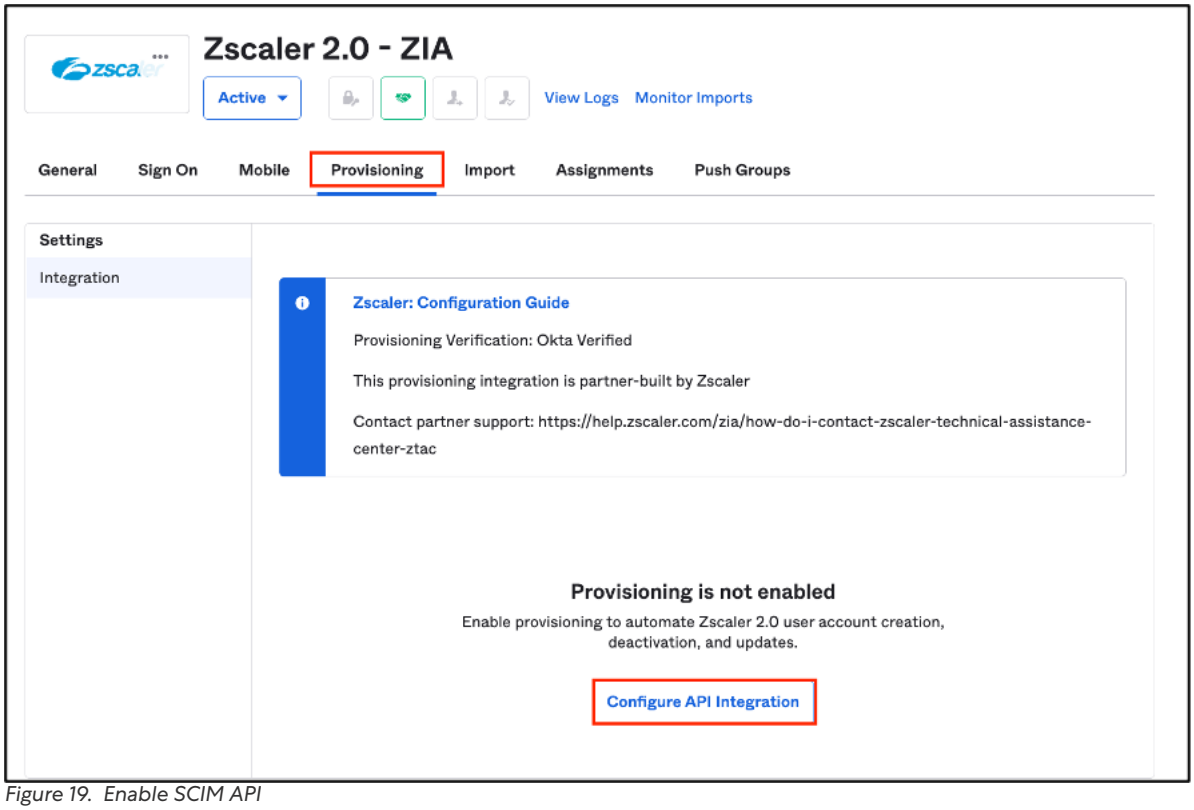


*Figure 19. Enable SCIM API*

 

11. Enter the **Base URL** copied from the **Zscaler SCIM Identity Provider** field into the **Zscaler ID** field.

    Although the Base URL looks like a traditional URL, enter only the numbers in the **Zscaler ID** field. For example, enter only `3173833/436704` if the Base URL is:

    ```
    https://scim.zscalerthree.net/3173833/436704/scim
    ```

12. Enter the **Bearer Token** value into the **API Token** field.
13. Select **Test API Credentials**. If the credentials are valid and Okta can communicate with the ZIA cloud, you see the response highlighted in red. If you receive an error, re-copy the URL and token, generate a new Bearer Token, or save the ZIA configuration.
14. After you have verified your credentials, click **Save**.

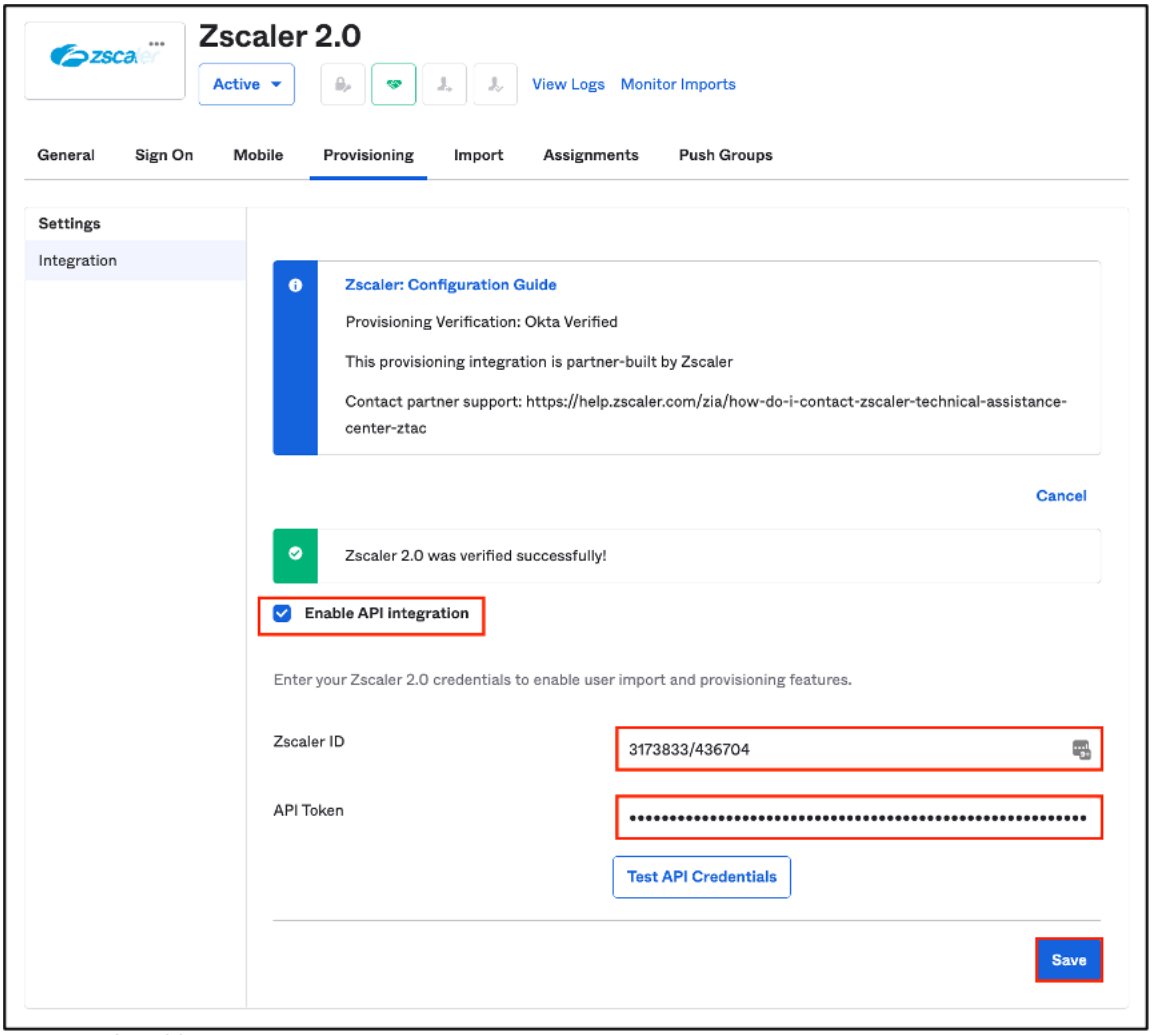


*Figure 20. Okta SCIM provisioning*

When **Enable API Integration** is activated, new settings that are visible to define the events are synchronized by SCIM from Okta to Zscaler (i.e., the provisioning or de-provisioning of a new user).

 

15. Select **To App** under **Settings** on the left-side pane.
16. Select **Edit**.

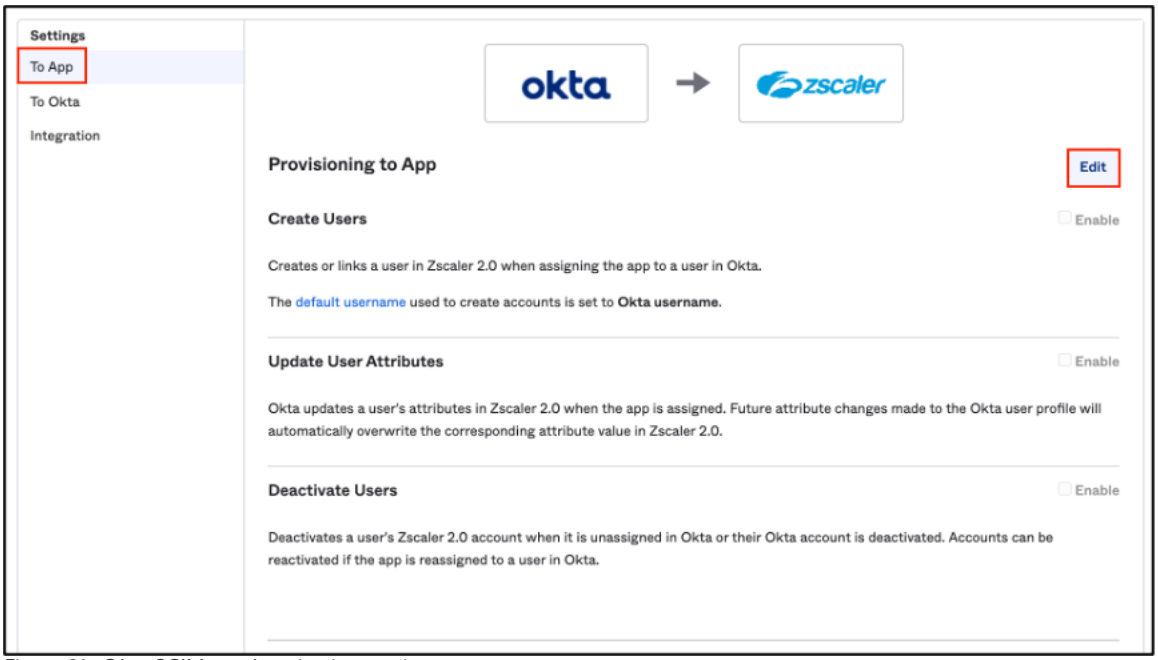


*Figure 21. Okta SCIM synchronization settings*

17. Set **Create Users**, **Update User Attributes**, and **Deactivate Users** to **Enable**.
18. Click **Save**.

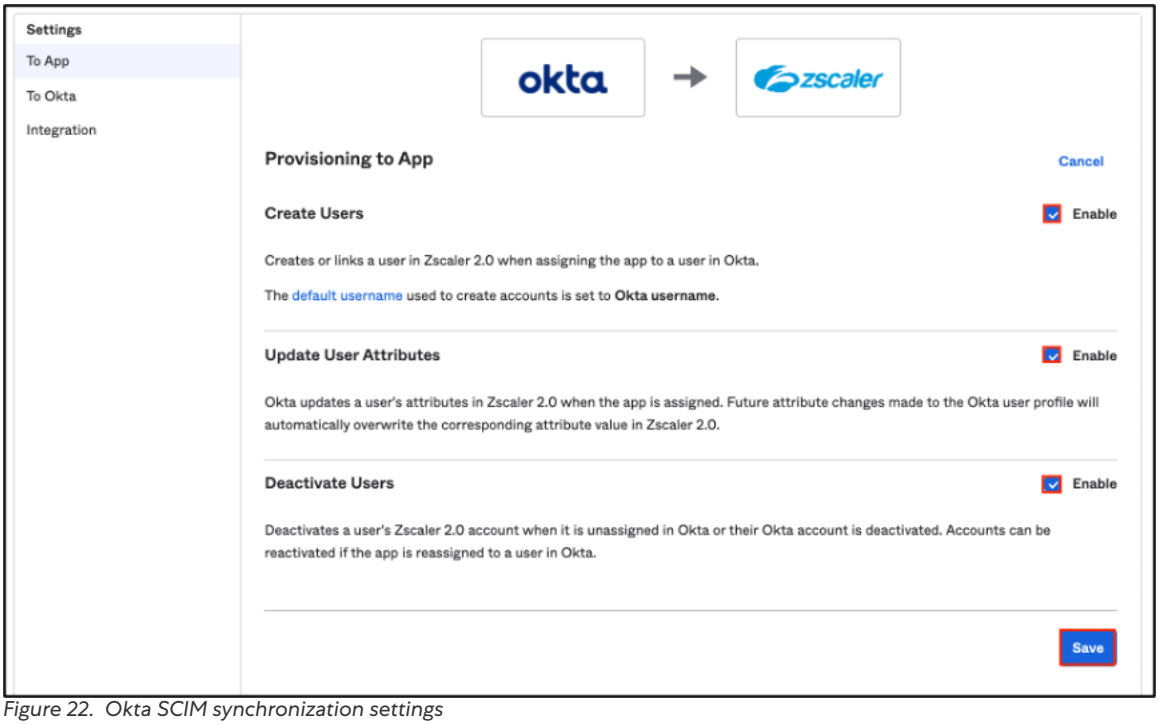


*Figure 22. Okta SCIM synchronization settings*

 

## Assign ZIA to Users or Groups

To assign the ZIA application to users authenticating into Okta from ZIA:

1. Select the **Assignments** tab.
2. Select **People** or **Groups**.
3. Select **Assign**.

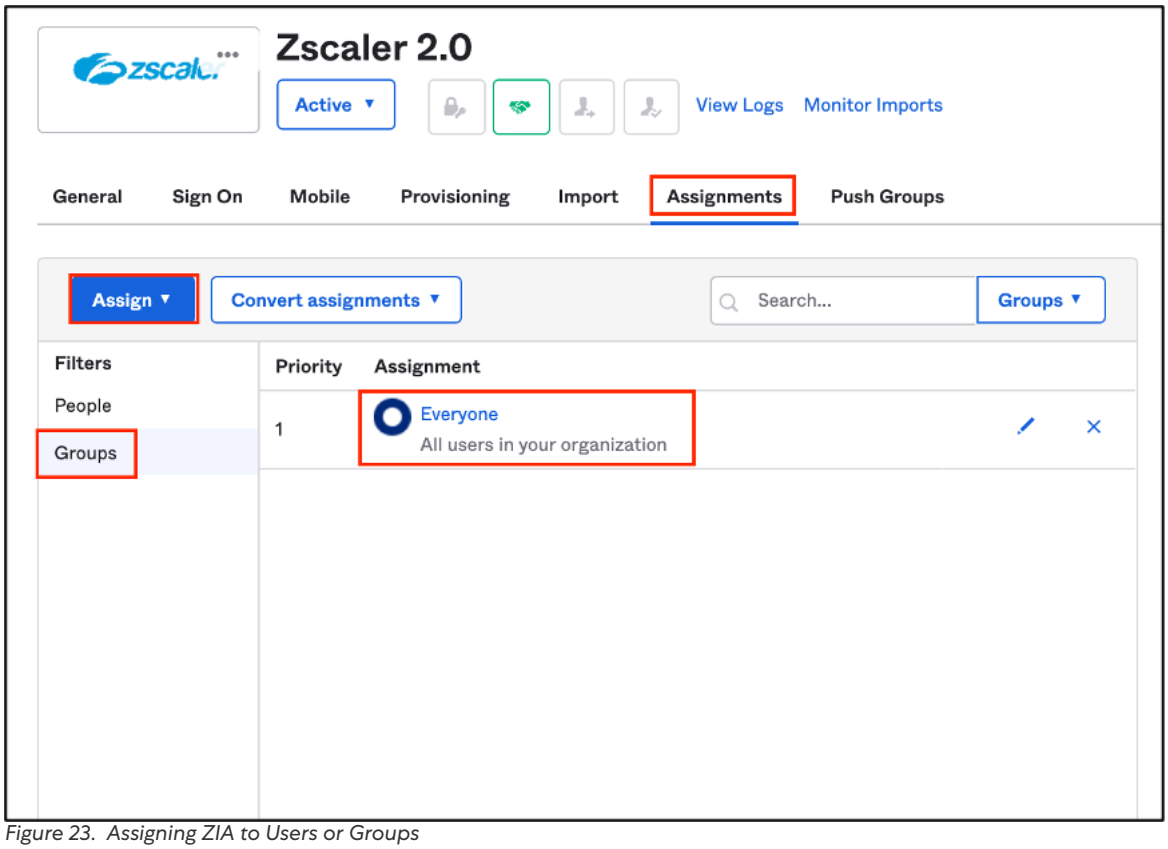


*Figure 23. Assigning ZIA to Users or Groups*

In the example, the **Everyone** group is selected (all users in the company can authenticate).

If interoperability issues arise, update your CrowdStrike policy's sensor visibility exclusions to account for Zscaler Client Connector-related details and re-test.

 

## Configure Groups to Push to ZIA

Select the security groups that are pushed to Zscaler. This enables and immediately pushes the groups to ZIA. Any adds, moves, or changes to the Okta database are immediately pushed to Zscaler.

To select which security groups are pushed to Zscaler:

1. Select the **Push Groups** tab.
2. Select **Push group memberships immediately**.
3. Search for the groups to add.
4. Click **Save & Add Another** or **Save** if completed. The groups are immediately pushed, and any new user changes to those groups are immediately synchronized to Zscaler.

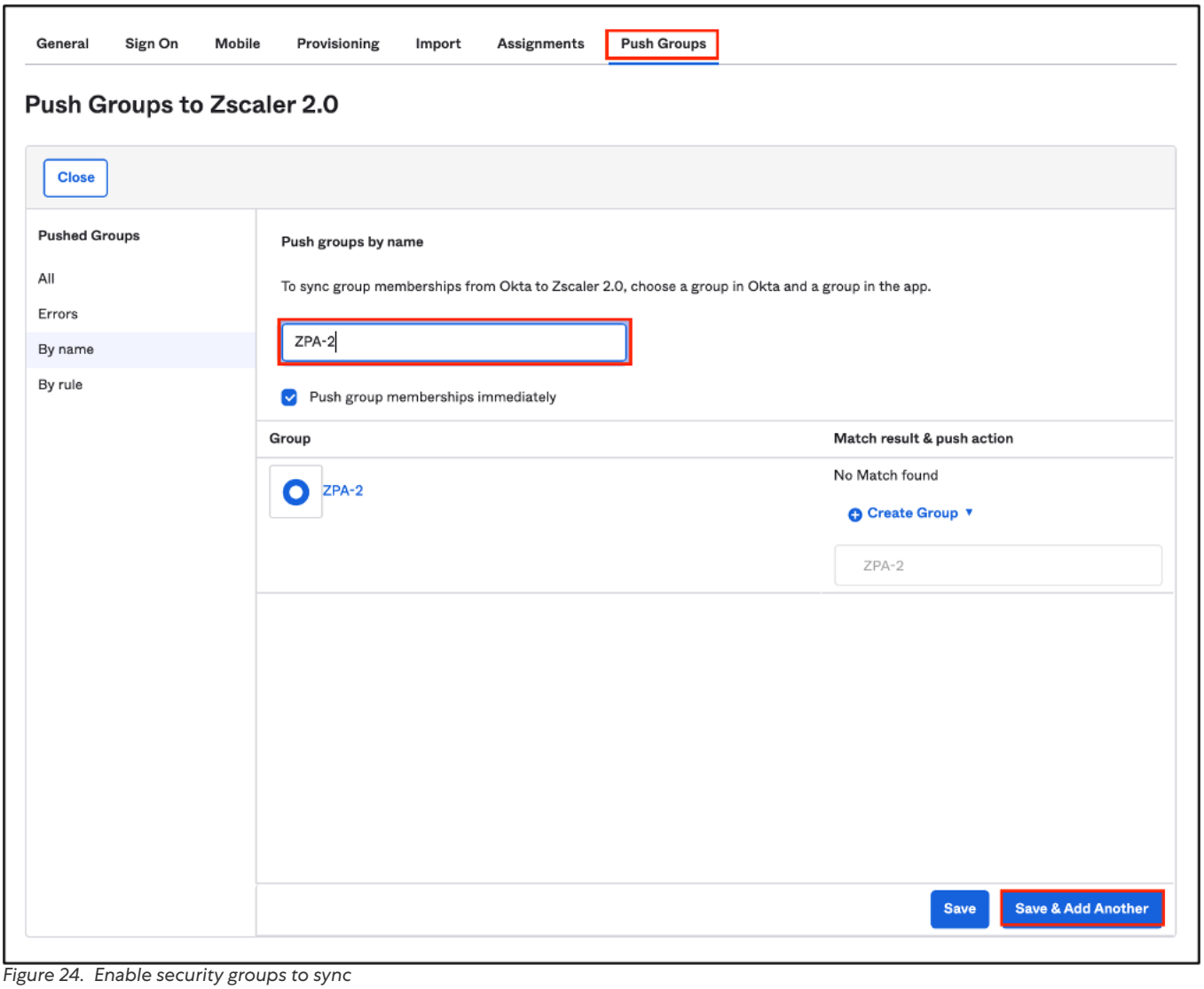


*Figure 24. Enable security groups to sync*

 

# ZIA Posture Check Integration with CrowdStrike ZTA

In this use case:

- CrowdStrike calculates a ZTA security score from 1 to 100 for each host. A higher score indicates a better security posture for the host.
- Security scores are derived from two distinct assessment sources:
  - OS settings: Settings that track native OS security options, firmware availability, and CVE mitigations.
  - CrowdStrike Falcon sensor settings (Windows and macOS): CrowdStrike Falcon sensor configurations that track RFM status as well as prevention and Real-Time Response policies.
- ZIA uses CrowdStrike's ZTA score (also known as a device posture score) and allows only compliant endpoints to access selected applications. ZIA checks for any changes to the CrowdStrike's device posture score because the score can change over time. ZTA check integration is supported currently for Windows and macOS endpoints.
- ZIA achieves conditional access based on Device Trust level. Device Trust levels are determined by ZIA posture profiles that, in turn, reference device level posture check profiles. ZIA administrators can simply specify that a minimum ZTA score is needed for the endpoint to grant access to resources that are referenced via various ZIA policies (such as URL filtering policy, Firewall policy, File Control policy, Cloud apps policy, or SSL inspection policy). You can combine the ZTA score threshold requirement with other device posture policies to allow only compliant devices to access resources through ZIA.

The following diagram shows a conceptualization of the integration.

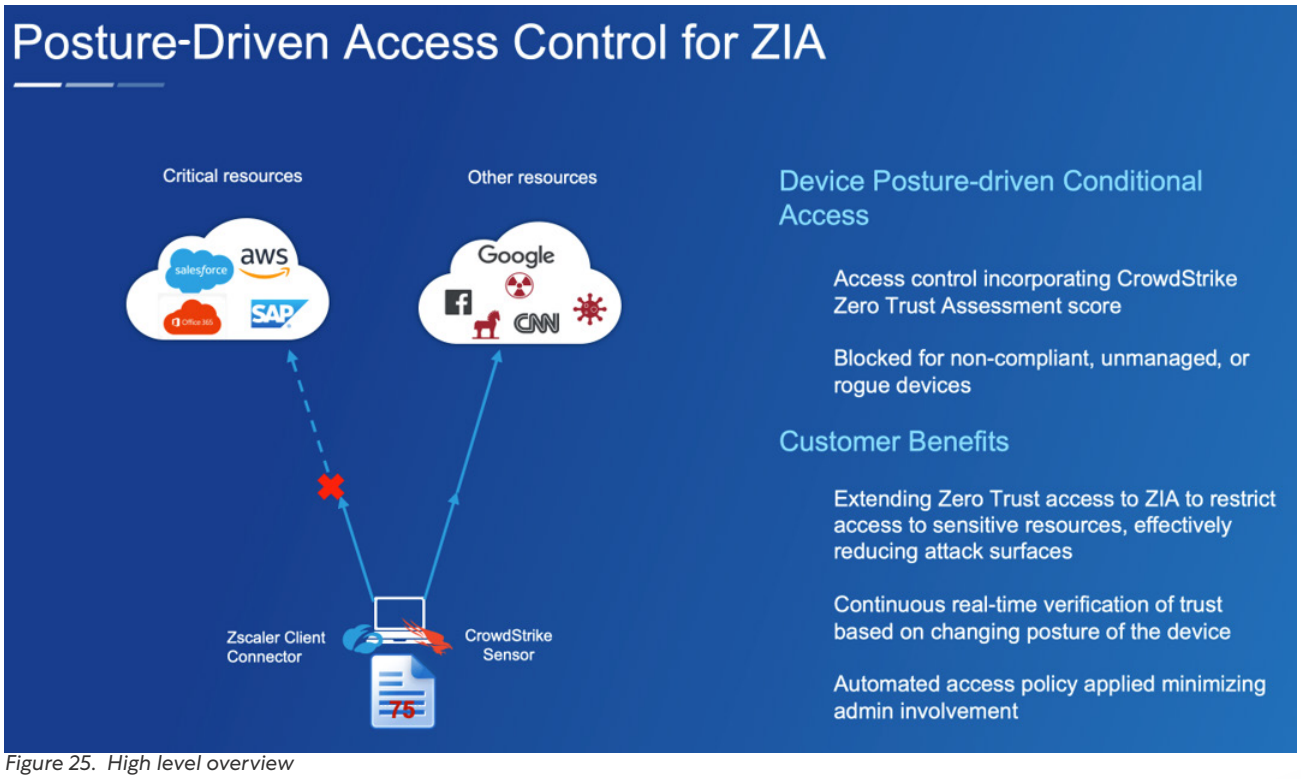


*Figure 25. High level overview*

This guide assumes you have a working CrowdStrike installation in your environment. If you need further information on configuring a CrowdStrike installation, see the [Zscaler and CrowdStrike Deployment Guide].

 

## Configuring CrowdStrike ZTA Integration in the CrowdStrike Tenant

Currently, to integrate with Zscaler, you must contact the CrowdStrike Support team to turn on a ZTA feature flag in their CrowdStrike tenant.

When enabled on the CrowdStrike back end, ZIA can access and use the per-device ZTA score.

Also, ensure that you use Zscaler Client Connector version 3.4 or later on the end host from which you are testing. CrowdStrike Falcon sensor version must be 6.20 or later.

## Configuring ZIA

This guide assumes that you have a working ZIA set up and provides instructions to integrate ZTA-based conditional access into your existing ZIA deployment.

### Log in to ZIA Admin Portal

Log in to the ZIA Admin Portal as an administrator.

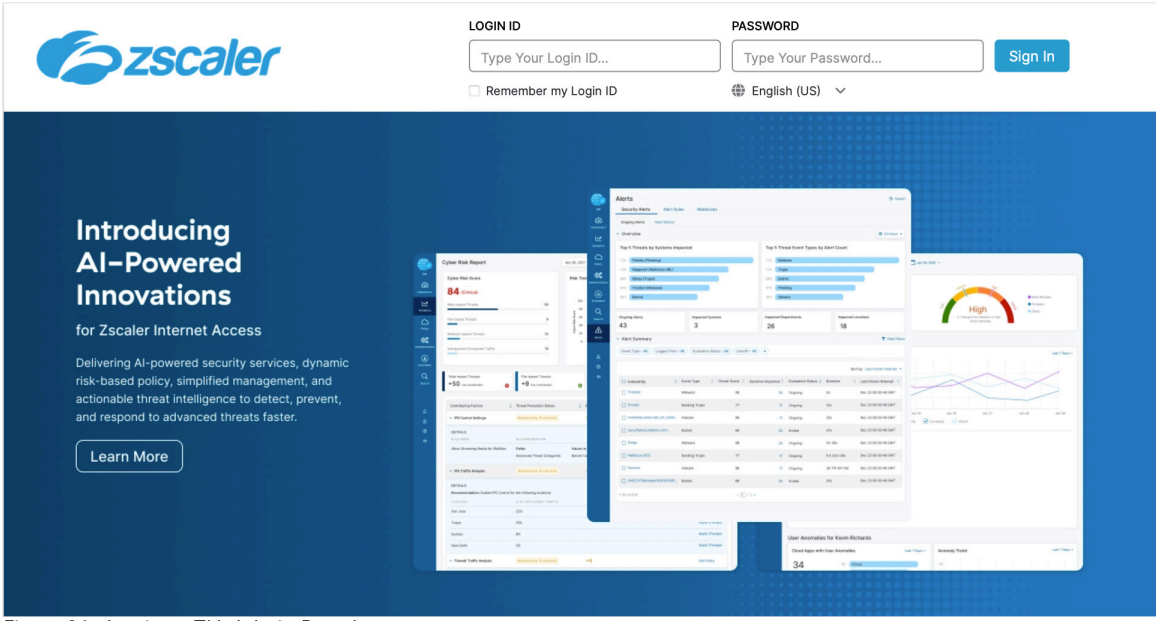


*Figure 26. Log in to ZIA Admin Portal*

 

## Go to Zscaler Client Connector

Click the **Zscaler Client Connector Portal** link under the **Policy** section to access the Zscaler Client Connector Portal.

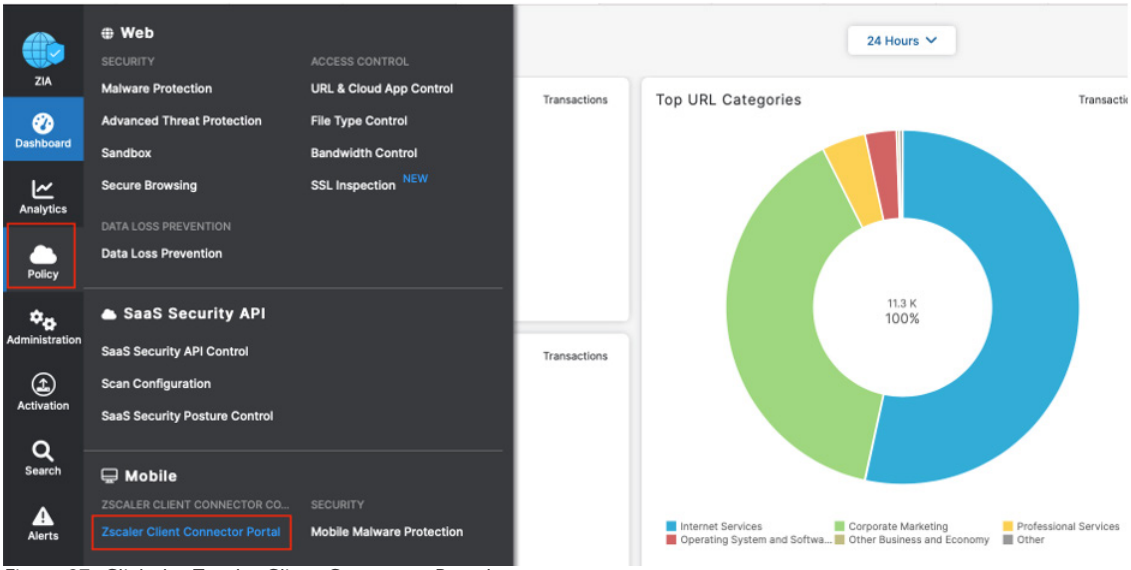


*Figure 27. Click the Zscaler Client Connector Portal*

## Create New Posture Profile

Log in to the Zscaler Client Connector Portal and go to **Administration** > **Device Posture** > **Add Device Posture Profile**.

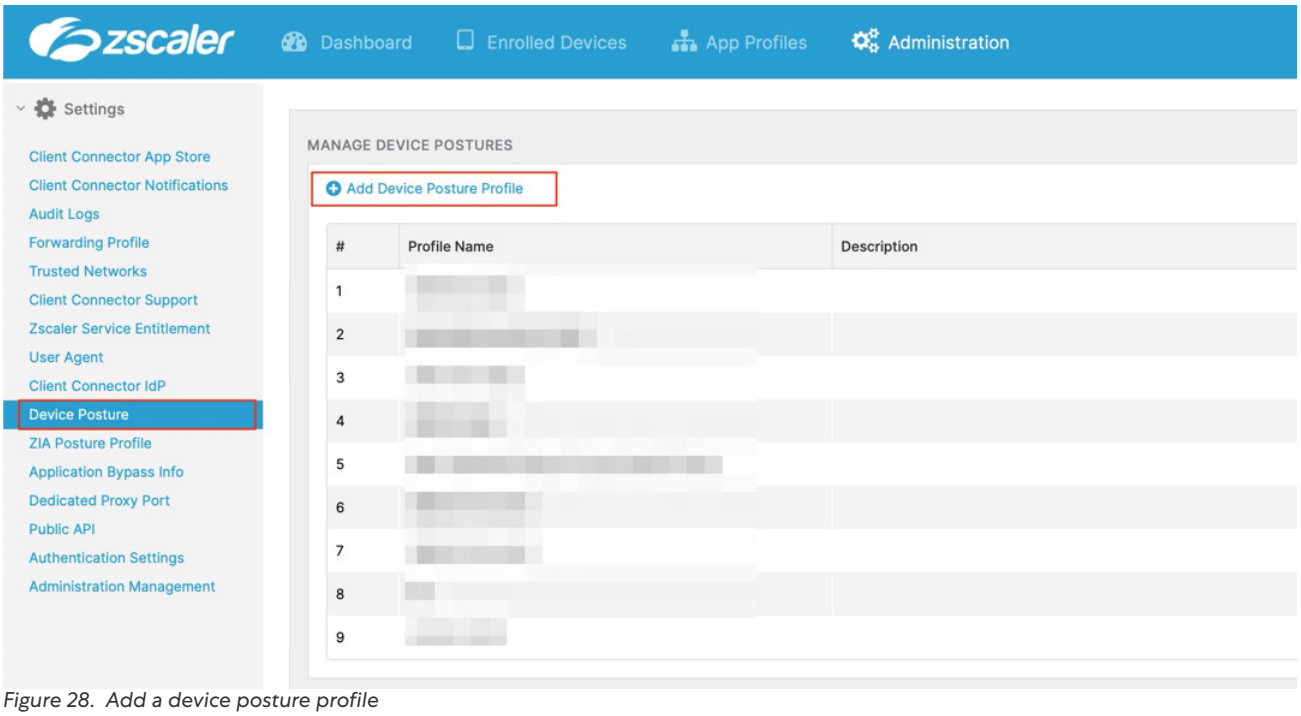


*Figure 28. Add a device posture profile*

 

## Add a New CrowdStrike ZTA Posture Profile

To add a new CrowdStrike ZTA posture profile:

1. Select only **Windows**, **macOS**, or both.
2. Select **CrowdStrike ZTA Score** from the **Posture Type** drop-down menu.
3. **Name** this policy.
4. Provide the minimum value for the **CrowdStrike ZTA Score**.
5. Click **Save**.

The device posture check passes if the end device's ZTA score (calculated by CrowdStrike) is greater than or equal to the value configured in this procedure. This device posture profile is, in turn, referenced in a ZIA posture profile to determine the trust bucket or level that a device falls in. You can set up conditional access policies to allow or deny access through ZIA based on device trust levels.

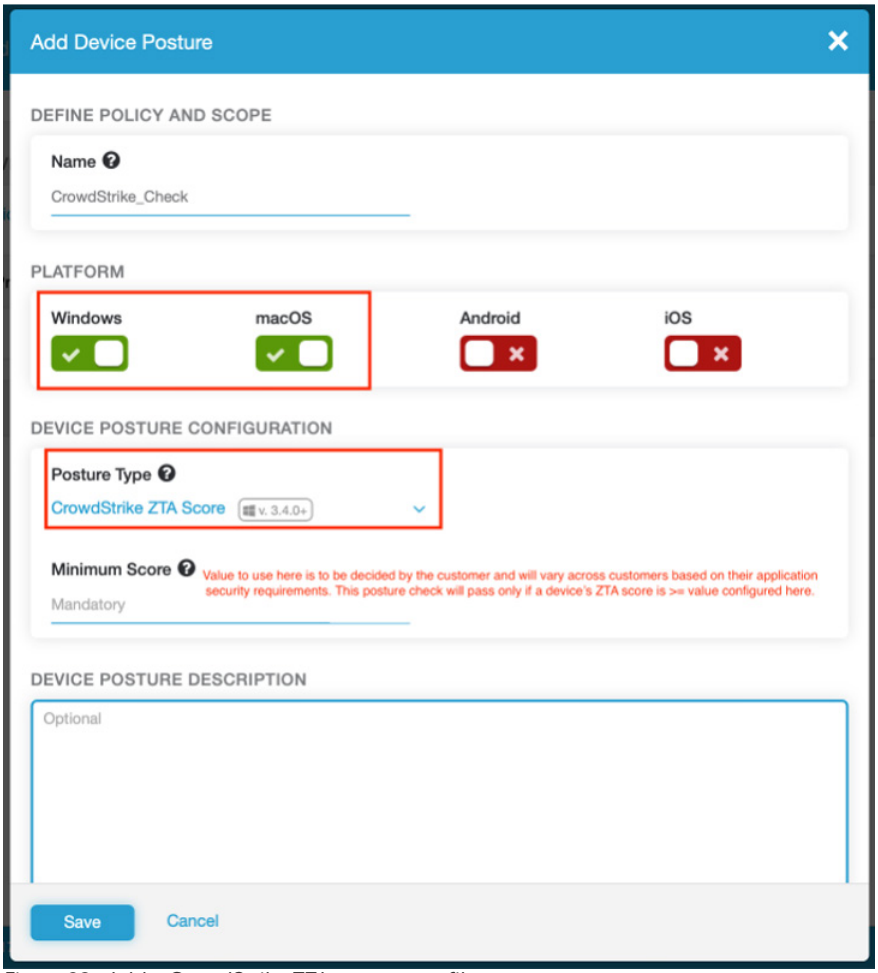


*Figure 29. Add a CrowdStrike ZTA posture profile*

 

## Multiple Device Posture Profiles Defined Referencing Different ZTA Scores

You can define multiple ZTA-based device posture templates to correspond to different Device Trust levels. As an example, you can set up multiple device posture profiles referencing different ZTA scores.

The following example defines three different device posture profiles, which set the minimum device ZTA threshold scores to be 75, 65, and 50 respectively. These are used for qualifying a device to fall in the High, Medium, Low trust level (respectively) via ZIA posture profile configuration.

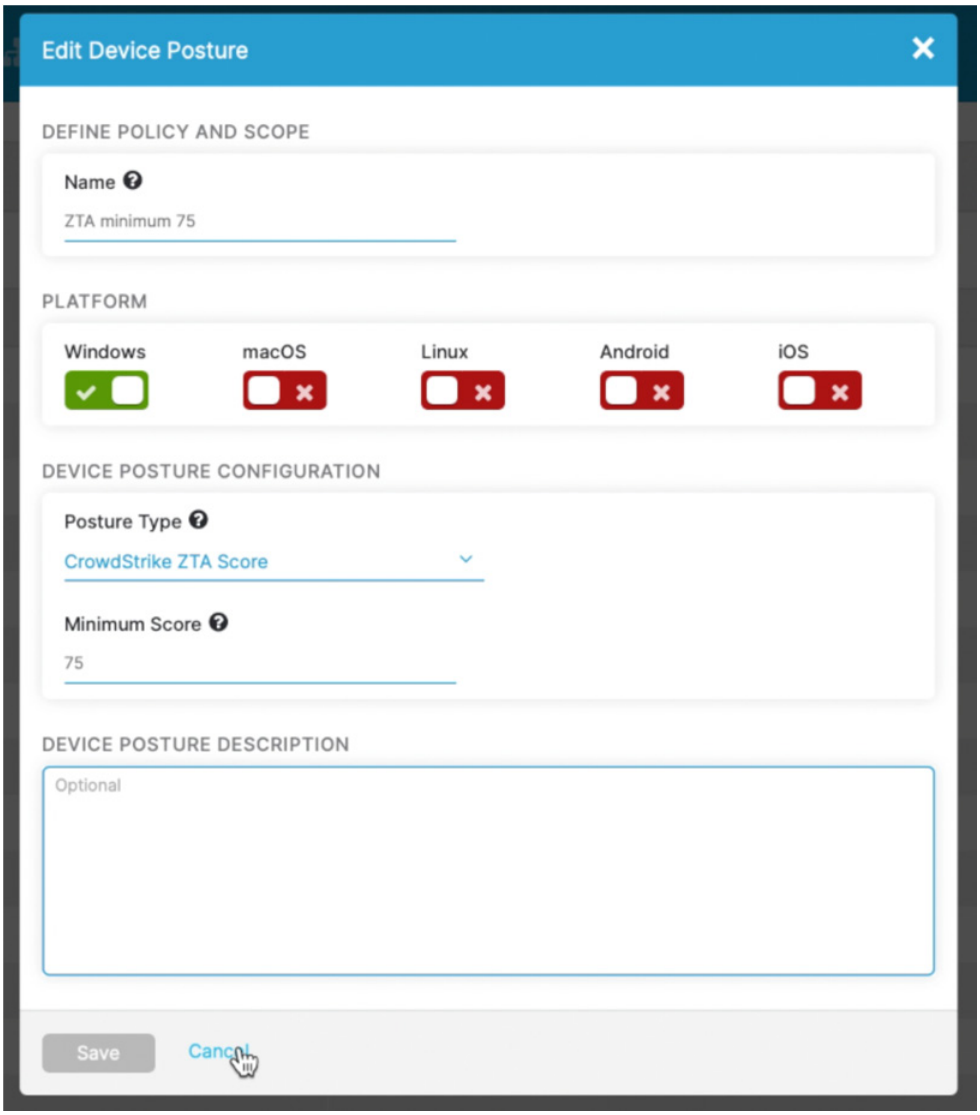


*Figure 30. Device posture policy based on 75 ZTA score*

 

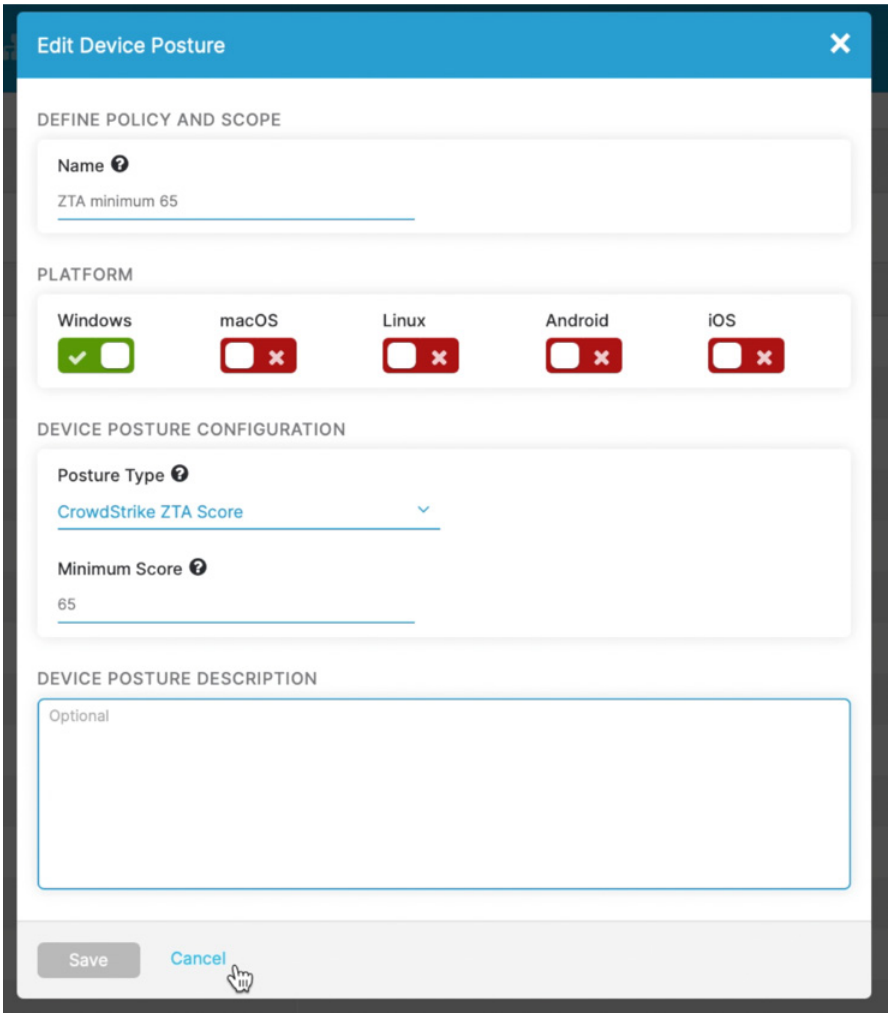


*Figure 31. Device posture policy based on 65 ZTA score*

 

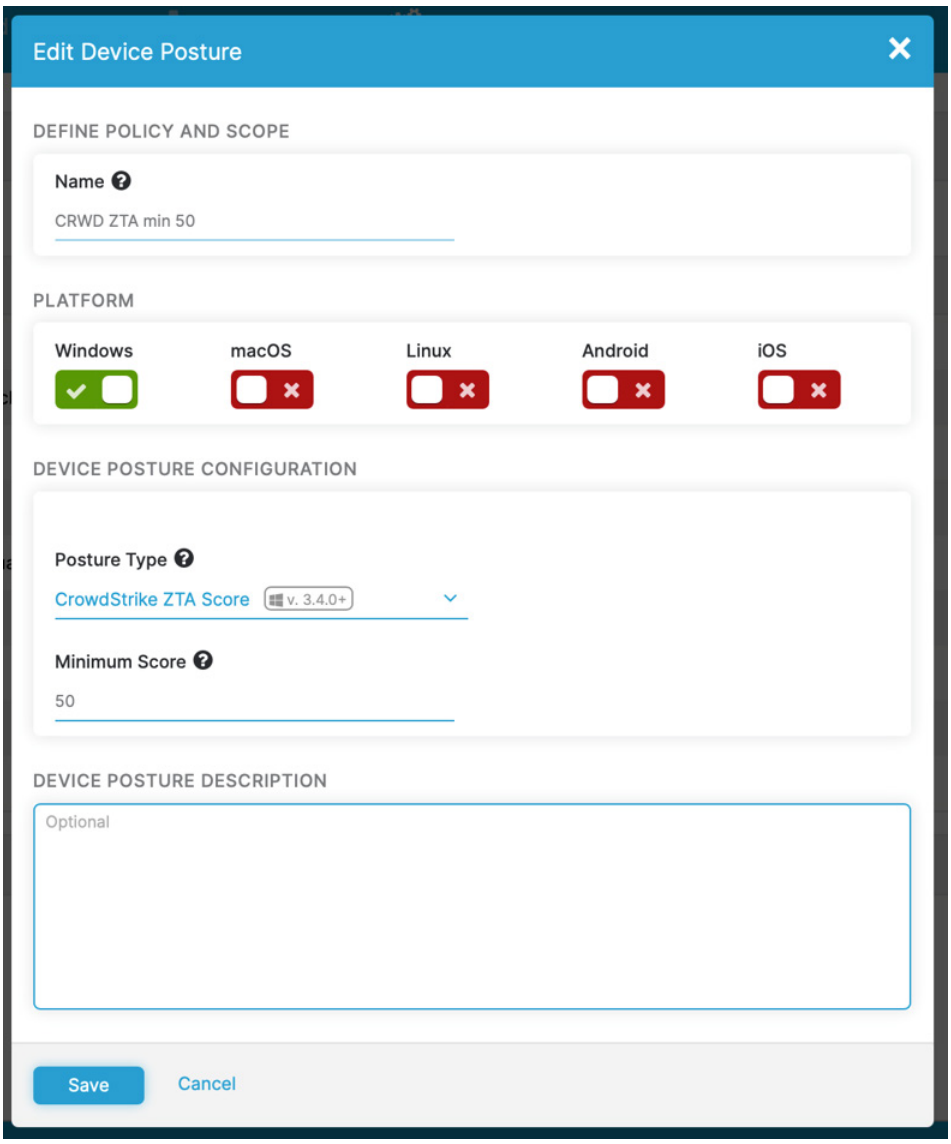


*Figure 32. Device posture policy based on 50 ZTA score*

 

## Reference the Device Posture Profile in ZIA Posture Profile

To add a ZIA posture profile for Zscaler Client Connector:

1. In the Zscaler Client Connector Portal, go to **Administration**.
2. From the left-side navigation, select **ZIA Posture Profile**.
3. Click **Add ZIA Posture Profile**.

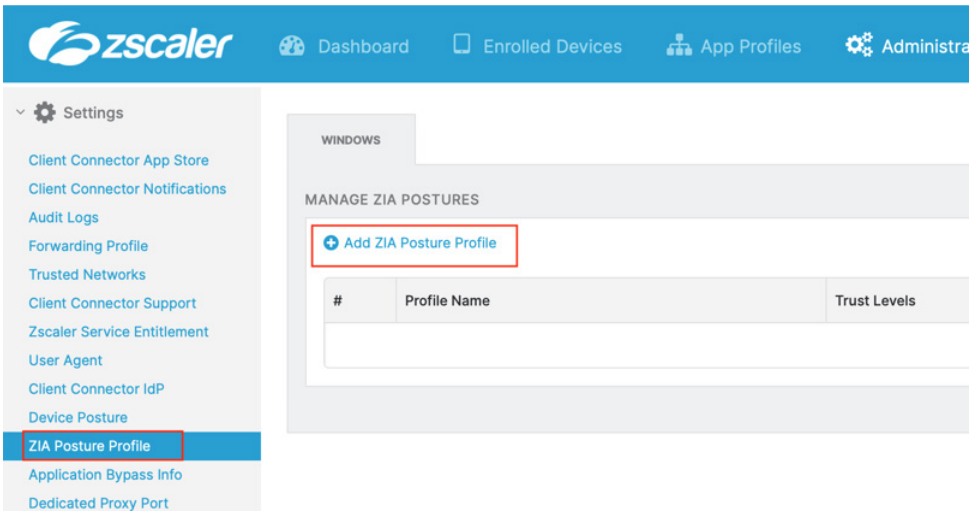


*Figure 33. Add a new ZIA Posture Profile*

In this new ZIA Posture Profile, reference the previously created device posture profiles to establish Device Trust criteria.

In the following example, as long as the device's ZTA score is greater than or equal to 75, it falls into the High trust level. A device with a ZTA score greater than or equal to 65 (but less than 75) falls into the Medium trust level. A device with a ZTA score greater than or equal to 50 (but less than 65) falls into the Low trust bucket.

Trust criteria are evaluated in the top-down order, and the evaluation stops at the first match.

 

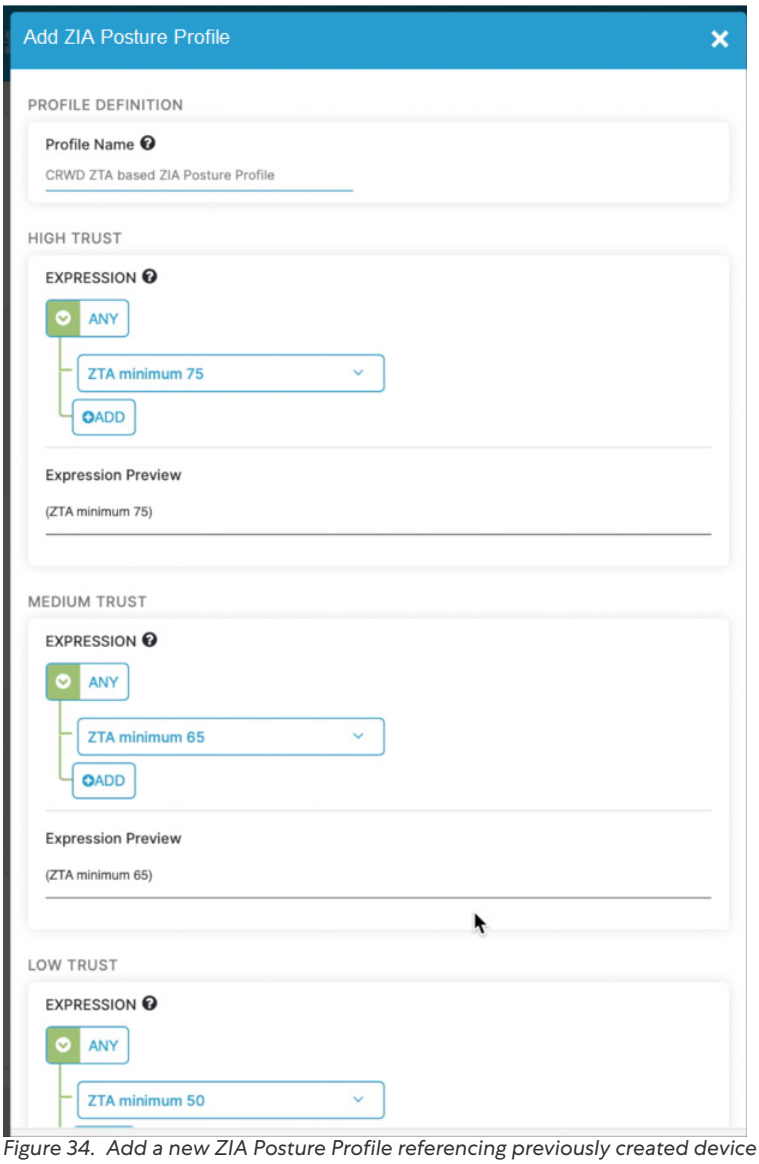


*Figure 34. Add a new ZIA Posture Profile referencing previously created device posture profiles*

 

## Create an App Profile to Reference the ZIA Posture Profile

The following example creates an App Profile for Windows machines. To add a posture profile to the new App Profile, follow these steps:

1. In the Zscaler Client Connector Portal, go to **App Profiles**.
2. Choose the OS platform you want to add the policy to, and click **Add Policy**.

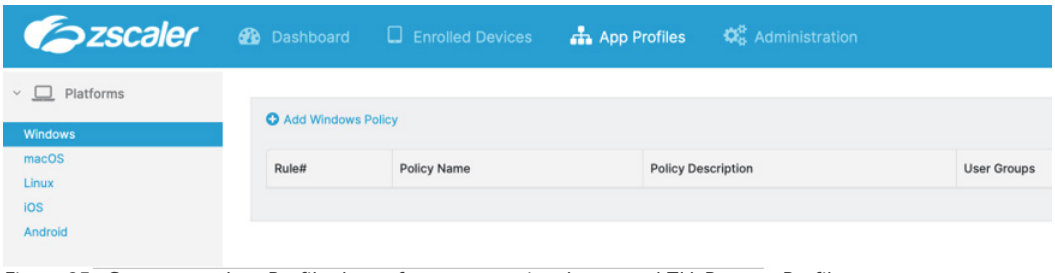


*Figure 35. Create new App Profile that references previously created ZIA Posture Profile*

3. In the **ZIA Posture Profile** field, click **Selected**.
4. Select the ZIA posture profile you created earlier.
5. Click **Save**.
6. Configure the App Profile.

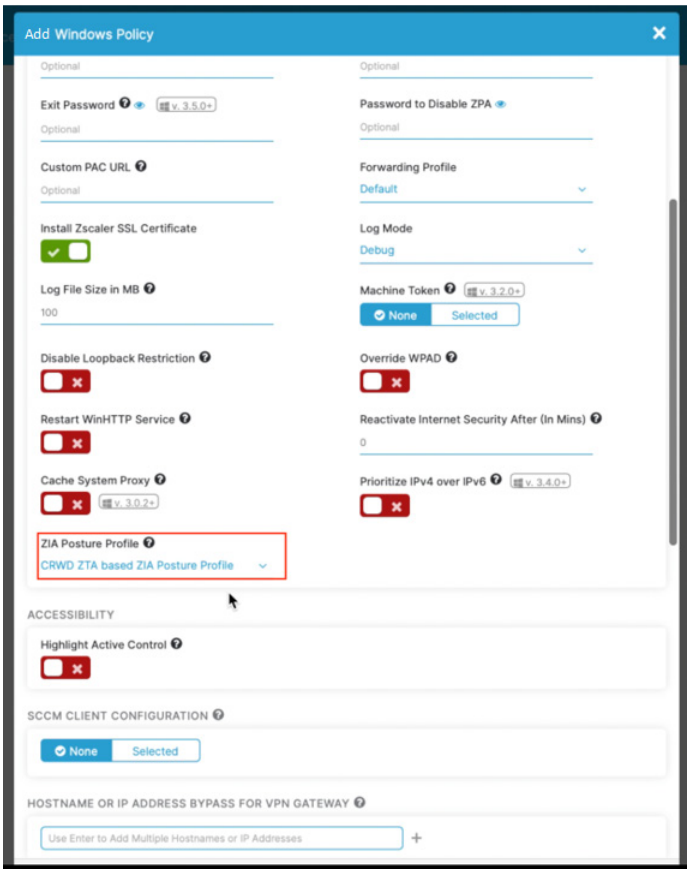


*Figure 36. Select previously created CrowdStrike ZTA-based posture profile*

 

## Create a Traffic Enforcement Policy Using Device Trust Level as Criteria

The following example creates a URL and App Control policy that uses the Device Trust level as a criterion for conditional access that allows access, shows a caution page, or blocks access through ZIA based on Device Trust level. You can set up such policies for File Type Control, SSL Inspection, Firewall Control, etc.

1. Go to **Policy** > **URL & Cloud App Control**.

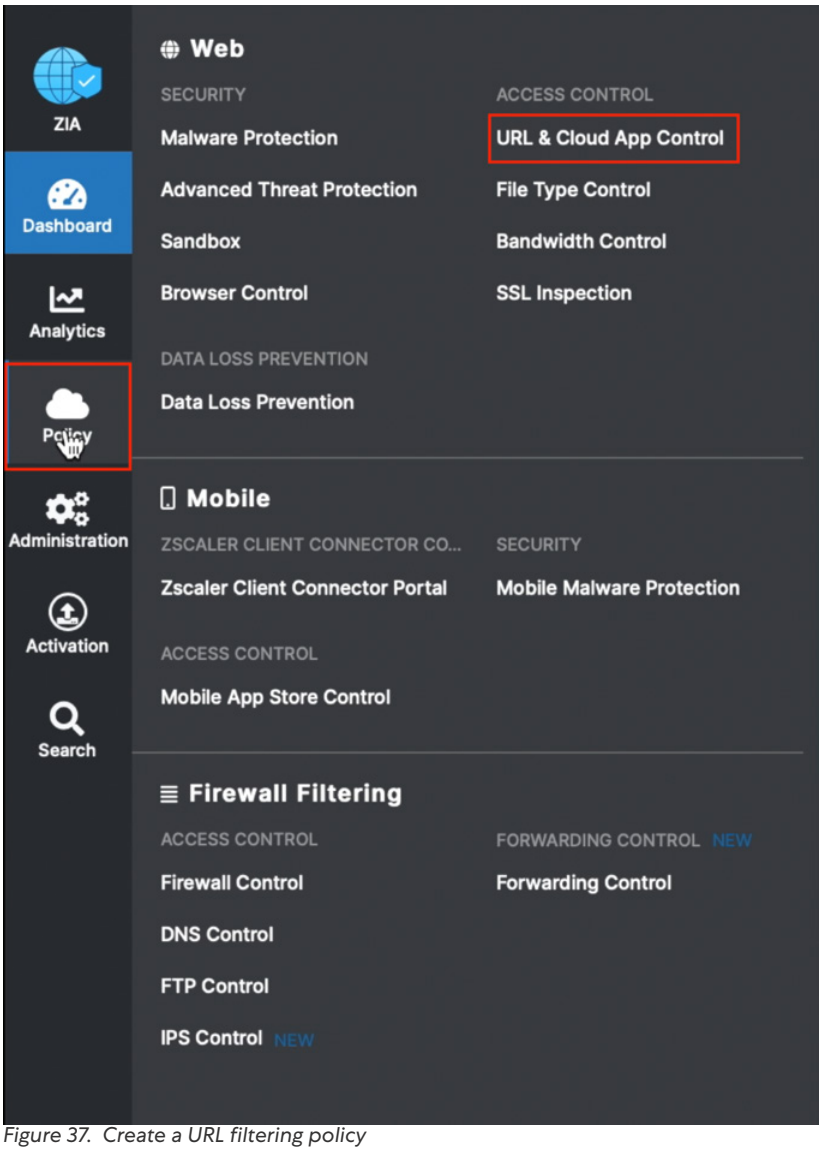


*Figure 37. Create a URL filtering policy*

 

2. Click **Add URL Filtering Rule**. You can also copy an existing rule by clicking the **Duplicate** icon. The **Add URL Filtering Rule** window appears.
3. Use the **Device Trust Level** as a criterion for policy enforcement. To learn more, see [Configuring the URL Filtering Policy](#).

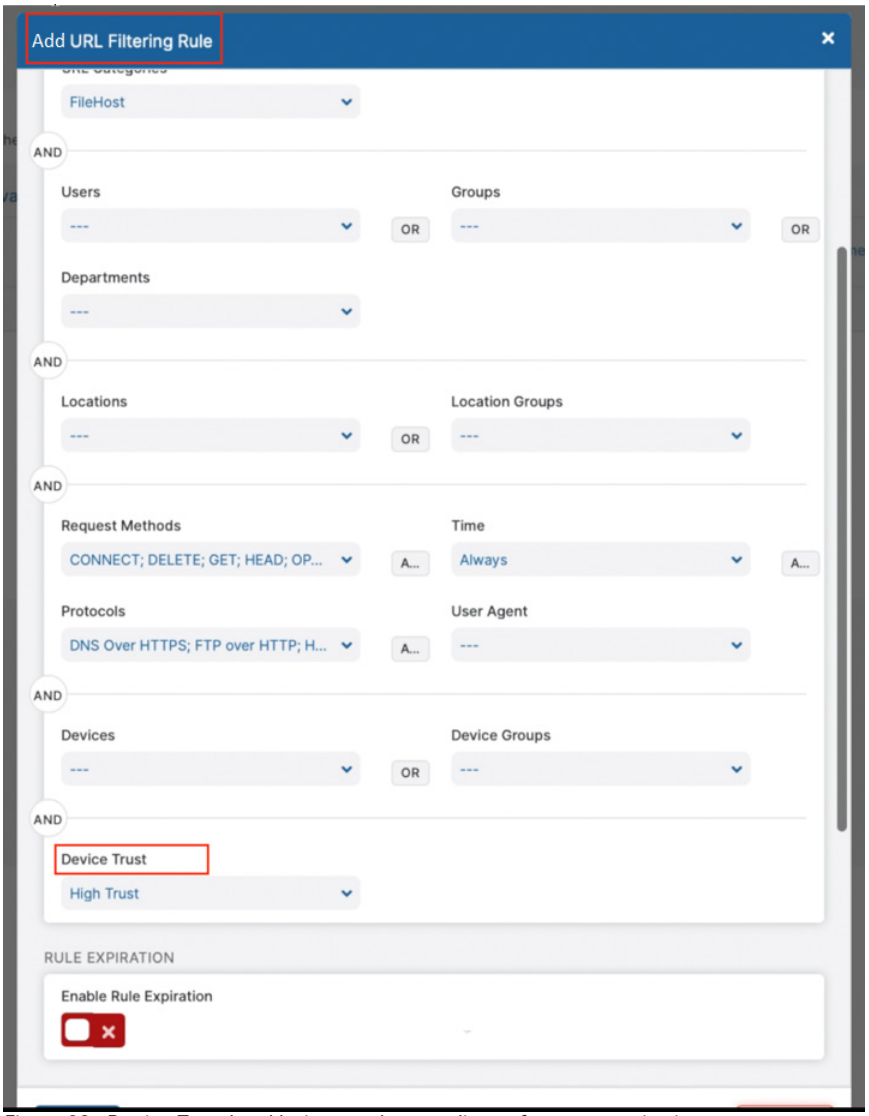


*Figure 38. Device Trust level being used as a policy enforcement criterion*

 

The following image shows different actions associated in the URL filtering policy based on the Device Trust level.

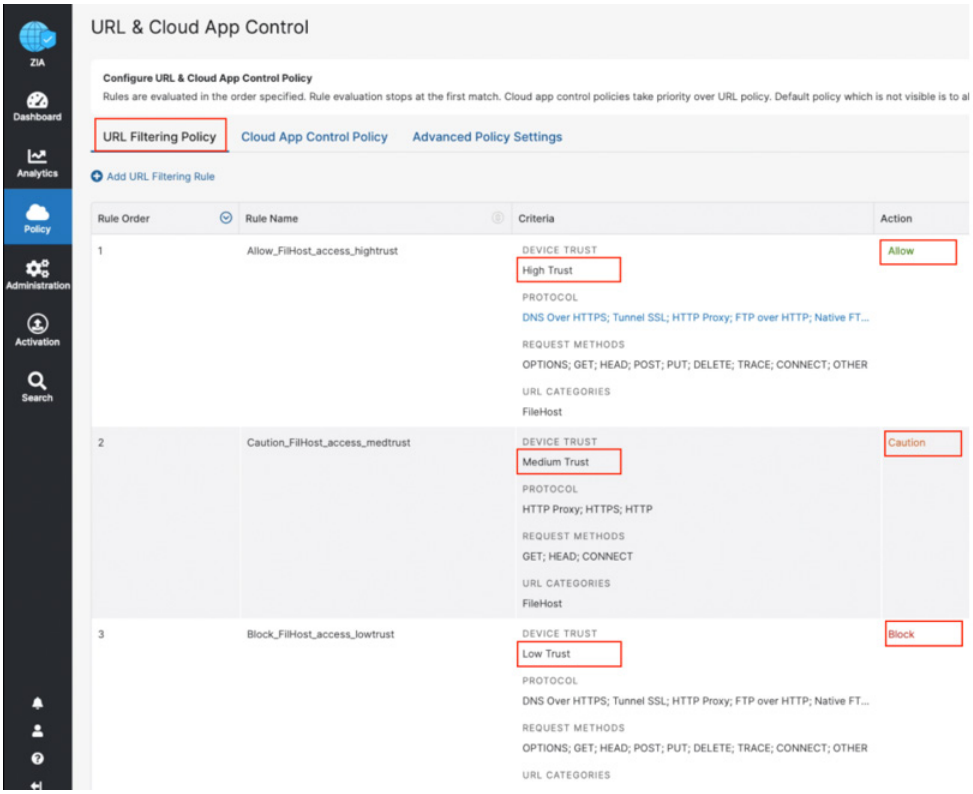


*Figure 39. URL filtering policy based on Device Trust criterion*

The same user who logged in to Zscaler Client Connector on three different machines sees pertinent URL filtering policies enforced based on Device Trust level.

In this case, you see the same user accessing a file-hosting website from three different machines that fall under High (in the following example, a ZTA greater than or equal to 75), Medium (a ZTA greater than or equal to 65, but less than 75), and Low (greater than or equal to 50, but less than 65) trust levels due to those machines' CrowdStrike ZTA scores.

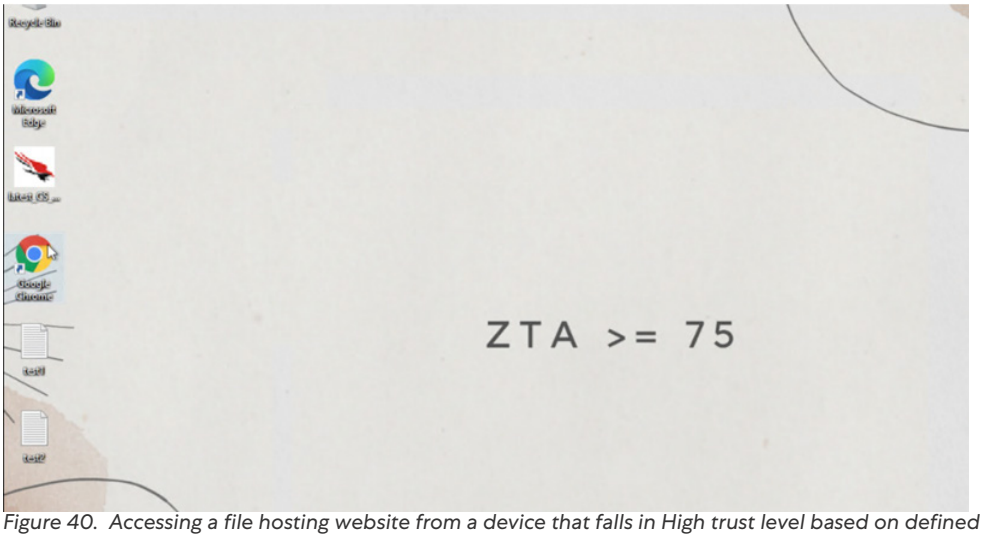


*Figure 40. Accessing a file hosting website from a device that falls in High trust level based on defined ZIA posture policies*

 

Access is allowed by ZIA per the URL filtering policy:

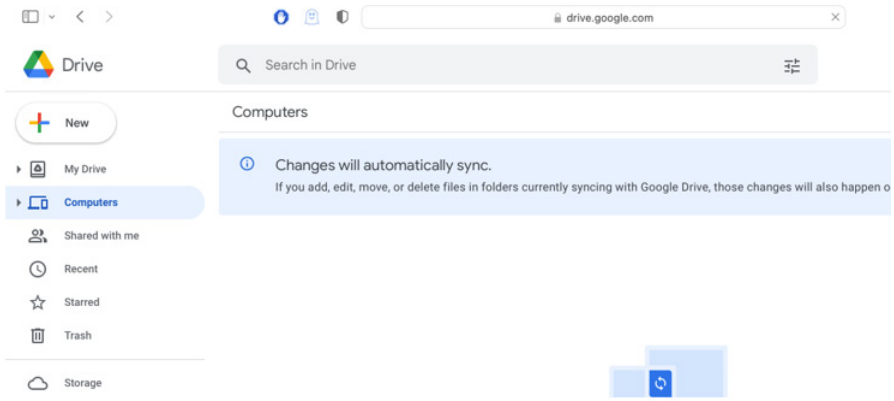


*Figure 41. Access allowed by ZIA per the URL filtering policy due to Device Trust level*

Devices that fall in the Medium trust level:

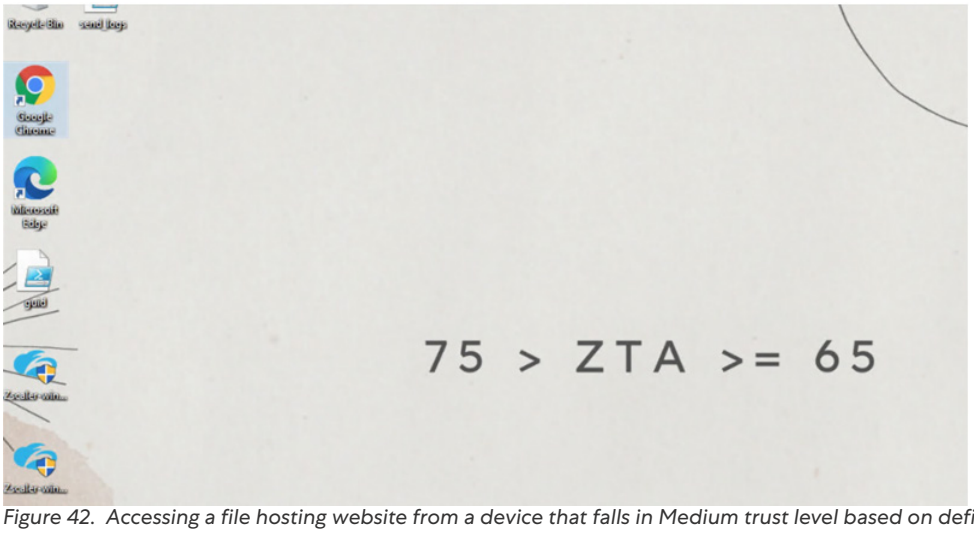


*Figure 42. Accessing a file hosting website from a device that falls in Medium trust level based on defined ZIA posture policies*

Caution warning from a URL filtering policy based on trust level:

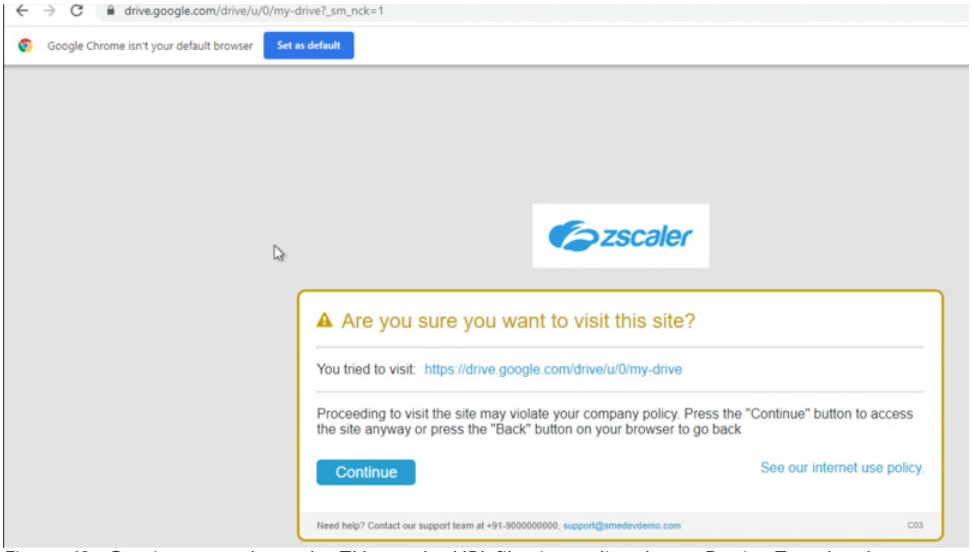


*Figure 43. Caution page shown by ZIA per the URL filtering policy due to Device Trust level*

 

Low Trust level based on posture policy:

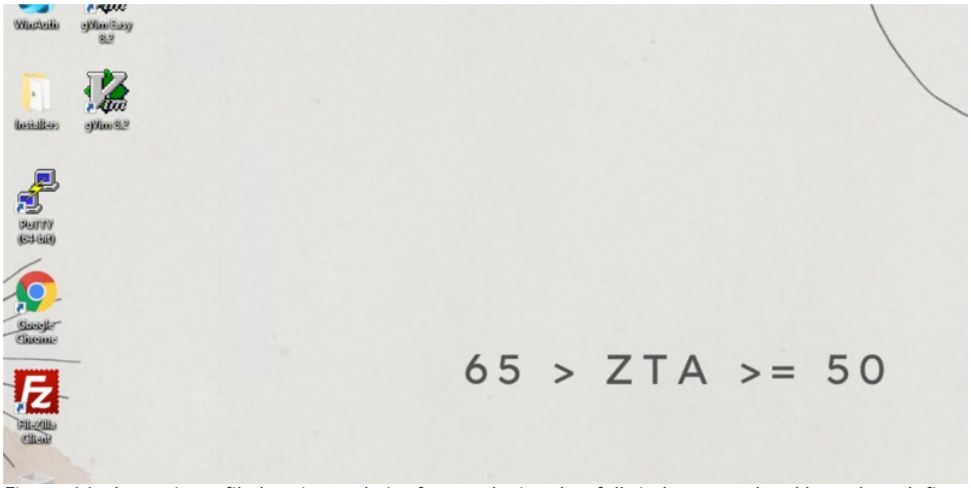


*Figure 44. Accessing a file hosting website from a device that falls in Low trust level based on defined ZIA posture policies*

Access blocked due to Device Trust level:

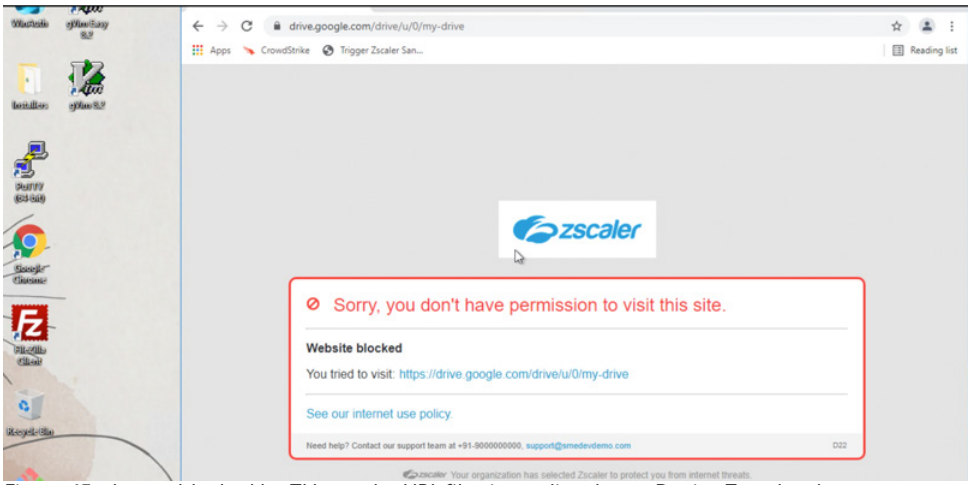


*Figure 45. Access blocked by ZIA per the URL filtering policy due to Device Trust level*

The same user logged into different machines under different trust levels gets pertinent enforcement policies applied by ZIA.

 

# Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

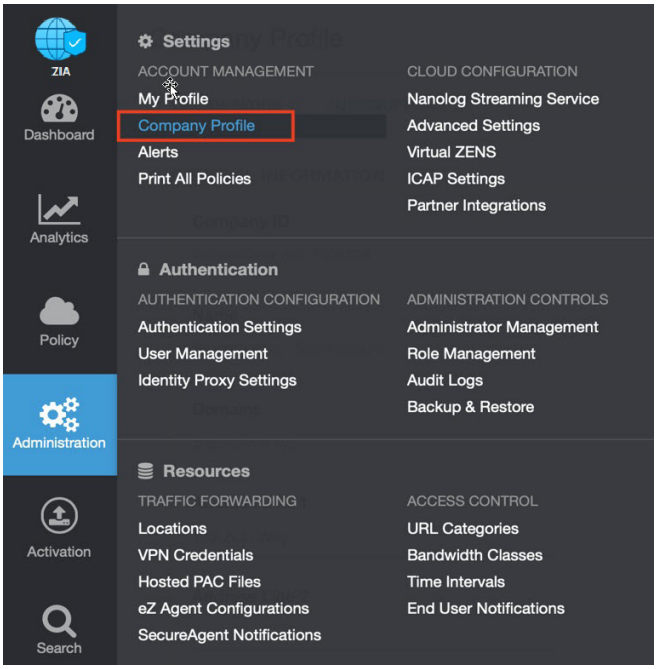


*Figure 46. Collecting details to open support case with Zscaler TAC*

2. Copy your **Company ID**.

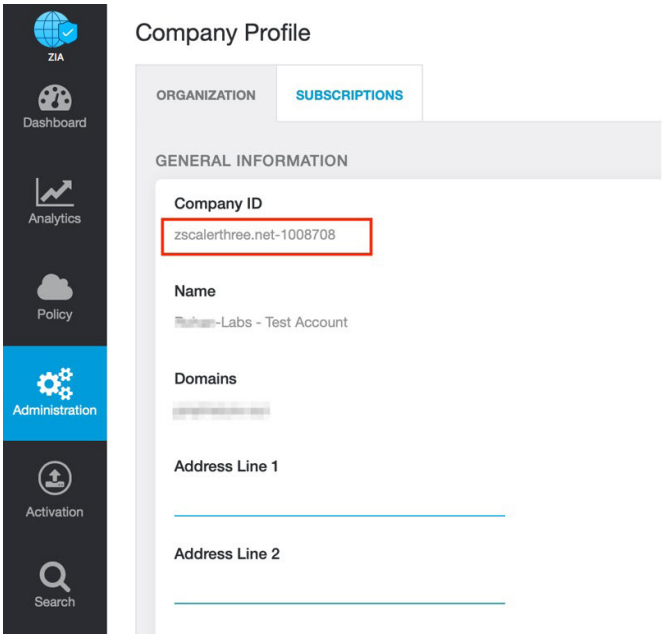


*Figure 47. Company ID*

 

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

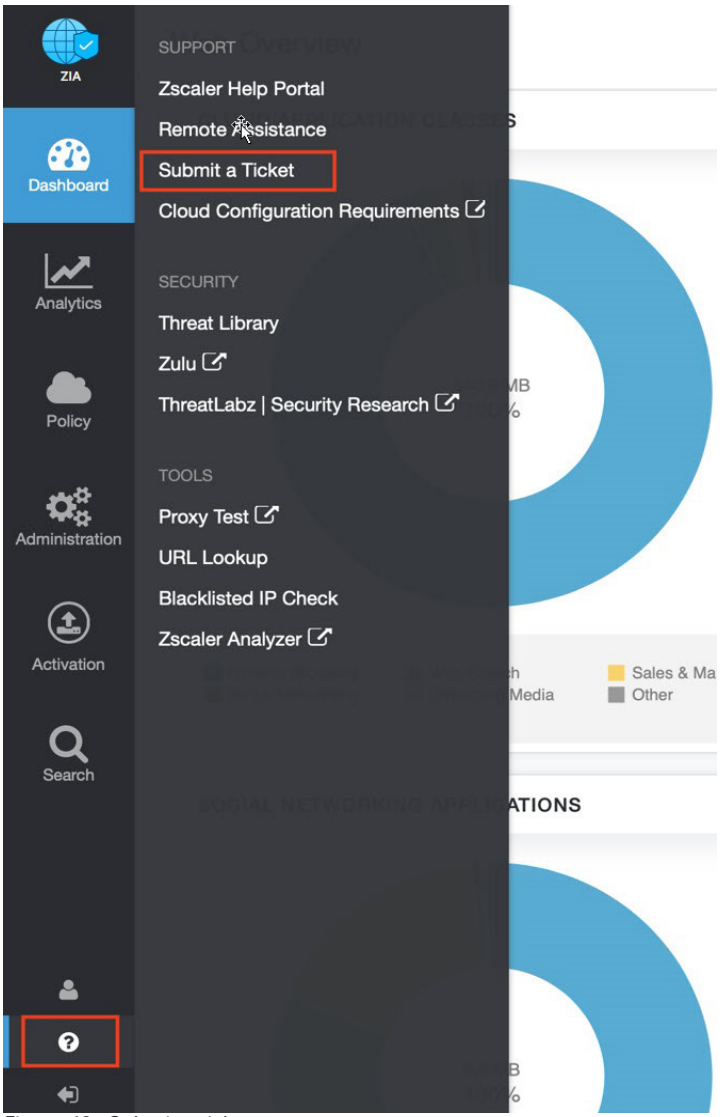


*Figure 48. Submit a ticket*

 