



# ZSCALER AND OKTA DEPLOYMENT GUIDE

# Contents

<b>Terms and Acronyms</b>	<b>6</b>
<b>About This Document</b>	<b>8</b>
Zscaler Overview	8
Okta Overview	8
Audience	8
Software Revisions	8
Prerequisites	9
Request for Comments	9
<b>Zscaler and Okta Introduction</b>	<b>10</b>
ZPA Overview	10
ZIdentity Overview	10
Deception Overview	11
Okta Authentication and Provisioning	12
Identity Threat Protection Overview	12
Okta Resources	12
<b>Okta Authentication and Provisioning in Use with Zscaler Services</b>	<b>13</b>
Overview for ZIdentity	13
Overview for ZIA and ZPA	14
<b>Okta OIDC App Configuration</b>	<b>15</b>
Configure Okta OIN App for Use as OP in ZIdentity	15
Configure ZIdentity Identity Provider with Okta as OP	18
Configure User Provisioning via SCIM to ZIdentity	20
Assigning ZIdentity Entitlements	34
<b>Configure Okta and ZIA: SAML and SCIM</b>	<b>38</b>
Enable Okta	38

Add the Zscaler ZIA Application	39
Configure Okta for ZIA	42
Configure Zscaler ZIA for an Okta IdP	43
Enable SAML Auto Provisioning	46
Enable SCIM Provisioning	48
Assign ZIA to Users or Groups	54
Configure Groups to Push to ZIA	55
<b>Configure Okta and ZPA: SAML and SCIM</b>	<b>56</b>
Add the Zscaler ZPA Application to Okta	56
Configure Okta for ZPA: SAML and SCIM	59
Configure ZPA for Okta: SAML and SCIM	60
Assign ZPA to Authenticating Users	66
Configure Okta SCIM for ZPA	67
Configure Which Groups to Push Using SCIM	71
Test the ZPA Authentication Configuration	72
SAML Assertion:	73
<b>Using Okta for ZIA Admin Access</b>	<b>74</b>
Add the Okta SAML Application	74
Okta SAML Service Provider Application	75
Configure the Application	76
Save the Certificate	78
Assign the App to the ZIA Administrators	80
Configure ZIA for Admin SSO	81
Enable SAML for ZIA Admins	82
Add ZIA Administrators	83
Test the Admin SSO Access	84

<b>Using Okta for ZPA Admin Access</b>	<b>85</b>
Add the Okta Application for ZPA SAML Administrator Access	85
Configure the Okta IdP: Save the Metadata	87
Add the ZPA IdP for Admin SSO on the ZPA Admin Portal	88
Configure the ZPA IdP Information on the ZPA Admin Portal	89
Copy the ZPA SP URLs	90
Configure the Okta IdP on the ZPA Admin Portal	91
Define the Administrators for SAML Access	92
Finish the Okta Configuration on the Okta Portal	94
Assign the Administrators or Groups to the Application	96
Test the ZPA Authentication Configuration	97
Administrator Sign In Using SAML from the ZPA Admin Portal	97
<b>Okta Device Trust for Managed Devices</b>	<b>98</b>
Installing Okta Device Trust	99
SAML Variable Returned in the User's SAML Assertion	99
Configure ZIA to Use Okta Device Trust	100
Configure ZIA Identity Proxy to Use Okta Device Trust	101
The User Experience	102
Configure ZPA to Use Okta Device Trust	103
<b>Deception and Identity Threat Protection Integration</b>	<b>106</b>
Overview	106
Finding Your Okta Domain	107
Create a Shared Signals Framework Receiver in Okta	107
Configure the Containment Integration Between Deception and Okta	108
Configure an Orchestration Rule	109
Configure an Entity Risk Policy Rule	112
Reviewing Events	114



<b>Avalor Unified Vulnerability Management and Okta Integration</b>	<b>118</b>
Overview	118
Finding Your Okta Domain	118
Create API Token	119
Configure the Avalor Data Connector	120
Review and Adjust Data Model Mapping	121
Review and Adjust Risk Scoring	123
<b>Transparent SSO Using IWA with Okta</b>	<b>130</b>
<b>PAC File and Zscaler Client Connector: Authentication Bypasses</b>	<b>131</b>
<b>Appendix A: Capture the SAML Request for Troubleshooting</b>	<b>132</b>
How to View a SAML Response in Your Browser for Troubleshooting	132
Google Chrome: To View a SAML Response in Chrome	132
Mozilla Firefox: To View a SAML Response in Firefox	132
Apple Safari: To View a SAML Response in Safari	133
Microsoft Windows: To View a SAML Response in Windows	133
Configure Your Browser to Capture the SAML Response	134
<b>Appendix B: Requesting Zscaler Support</b>	<b>140</b>

## 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)
CPU	Central Processing Unit
CSV	Comma-Separated Values
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
IIS	Internet Information Services
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
ITP	Identity Threat Protection
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSF	Shared Signals Framework
SSL	Secure Socket Layer (RFC6101)
SSO	Single Sign-On
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

## Trademark Notice

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at [zscaler.com/legal/trademarks](https://zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

## About This Document

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](#) or follow them on Twitter @okta.

### 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](#)
- [Okta Resources](#)
- [Appendix B: Requesting Zscaler Support](#)

### Software Revisions

This document was authored using ZIA v6.2 and Okta Production Release 2024.04.1 E.

## Prerequisites

Make sure the following prerequisites are met for ZIdentity:

- ZIdentity:
  - ZIdentity version 2.1.151-8d3b140-8808-UI-1694502295
  - Administrator login credentials to ZIdentity
- ZIA:
  - ZIA v6.2
  - Administrator login credentials to ZIA
- Okta:
  - Okta version 2024.04.1 E (Okta Identity Engine)
  - SCIM support, which requires Lifecycle Management (LCM) SKU
  - Administrator login credentials to Okta

Make sure the following prerequisites are met for Zscaler Deception:

- Deception:
  - Deception v4.2 or later
  - Essentials or Advanced license
  - Administrator privileges to Deception
- Zscaler Client Connector:
  - Endpoint deception capabilities require [supported versions](#).
- Okta:
  - Identity Threat Protection enabled
  - Administrator privileges to Okta

## Request for Comments

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

# Zscaler and Okta Introduction

Overviews of the Zscaler and Okta 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 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 a 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, 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.

## ZIdentity Overview

ZIdentity is a unified identity service for Zscaler that centralizes and simplifies identity management, user authentication, and entitlement assignment for users to Zscaler services, such as Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), Zscaler Digital Experience (ZDX), etc. The services are managed through individual Zscaler Admin Portals (e.g., ZIA Admin Portal). If you have subscribed to more than one Zscaler service or just one service for multiple organizations, you typically must access these portals using different login credentials. A single authentication into ZIdentity allows admins and users to seamlessly access Zscaler services in use by their organization, without worrying about remembering or managing multiple passwords.

Additionally, you can use the ZIdentity service to enroll users to your subscribed Zscaler services using the ZIdentity user database. This mitigates the effort of creating a separate user database in each service's portal for provisioning users.

## Deception Overview

Zscaler Deception is a simple, faster, and more effective targeted threat detection solution built on the Zscaler Zero Trust architecture. Deception uses advanced lures and decoys to detect and disrupt sophisticated threats that consistently bypass traditional defenses, such as advanced persistent threats (APTs), exploits, reconnaissance, lateral movement, active directory, supply chain, human-operated ransomware, supervisory control and data acquisition (SCADA), and industrial control system (ICS) attacks.

As an integral part of the Zscaler Zero Trust Exchange (ZTE), Deception integrates with Zero Trust, tracking the full attack sequence and initiating automated response actions across the Zscaler platform.

## Zscaler Resources

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

Name	Definition
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">ZPA Help Portal</a>	Help articles for ZPA.
<a href="#">ZIdentity Help Portal</a>	Help articles for ZIdentity.
<a href="#">Zscaler Deception Help Portal</a>	Help articles for Zscaler Deception.
<a href="#">ZPA Authentication Test URL</a>	Online authentication test for ZPA.
<a href="#">Zscaler Enforcement Node Ranges</a>	A list of IP ranges to add to your access lists, firewalls, and application allowlists.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

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

Name	Definition
<a href="#">ZIA Help Portal</a>	Help articles for ZIA.
<a href="#">ZPA Help Portal</a>	Help articles for ZPA.
<a href="#">ZIdentity Help Portal</a>	Help Articles for ZIdentity.
<a href="#">Zscaler Deception Help Portal</a>	Help Articles for Zscaler Deception.
<a href="#">ZPA Authentication Test URL</a>	Online authentication test for ZPA.
<a href="#">Zscaler Enforcement Node Ranges</a>	A list of IP ranges to add to your access lists, firewalls, and application allowlists.
<a href="#">Zscaler Tools</a>	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
<a href="#">Zscaler Training and Certification</a>	Training designed to help you maximize Zscaler products.
<a href="#">Submit a Zscaler Support Ticket</a>	Zscaler Support portal for submitting requests and issues.

## Okta Authentication and Provisioning

In the last decade, enterprises everywhere have embraced cloud apps like Salesforce.com and NetSuite; GoToMeeting and WebEx; and Workday and SuccessFactors. They've shrunk their IT infrastructure, lowered their total cost of ownership, and made it possible for employees to get work done anywhere, at any hour.

Controlling who has access to which applications becomes a real challenge when users can get access from any browser, from any place, at any time. This situation is exacerbated with the cloud as IT is often not involved in the purchasing process. Okta lets IT take back control, while simultaneously adding a critical layer of security and ease of use.

## Identity Threat Protection Overview

Identity Threat Protection (ITP) with Okta AI is a new Workforce Identity Cloud (WIC) product that provides continuous evaluation of user risk and authentication policies throughout active sessions to detect identity-based threats such as session hijacking attempts and compromised accounts. Powered by machine learning and broad signal ingestion from an organization's best-in-breed security stack, it extends observability beyond initial authentication to any time after a user is logged in. This enables real-time detection, and inline response to attacks at the identity layer.

## Okta Resources

The following table contains links to Okta support resources.

Name	Definition
<a href="#">Okta Help Center</a>	Okta online help for IT administrators and developers.
<a href="#">Okta IWA Server</a>	Online help for installing and configuring the Okta IWA Web agent for Desktop Single Sign-On.
<a href="#">Okta Device Trust</a>	Online help for installing and configuring the Okta Device Trust for managed Windows computers.
<a href="#">ITP Help Portal</a>	Documentation on Okta's Identity Threat Protection with Okta AI.



# Okta Authentication and Provisioning in Use with Zscaler Services

Identity, authentication, and provisioning are inherent parts of the Zscaler solution and provide granular user visibility, logging, and security down to the individual level.

## Overview for ZIdentity

Authentication verifies a user's identity using credentials and (optionally) other additional identity factors. OpenID Connect (OIDC) is the preferred method for authentication with ZIdentity. This document shows how you can configure an Identity Provider (IdP) as an OpenID Provider (OP).

OIDC is an authentication protocol based on the OAuth 2.0 framework that allows an IdP to authenticate a user and pass the authorization credentials to Zscaler services as a Relying Party (RP). 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.

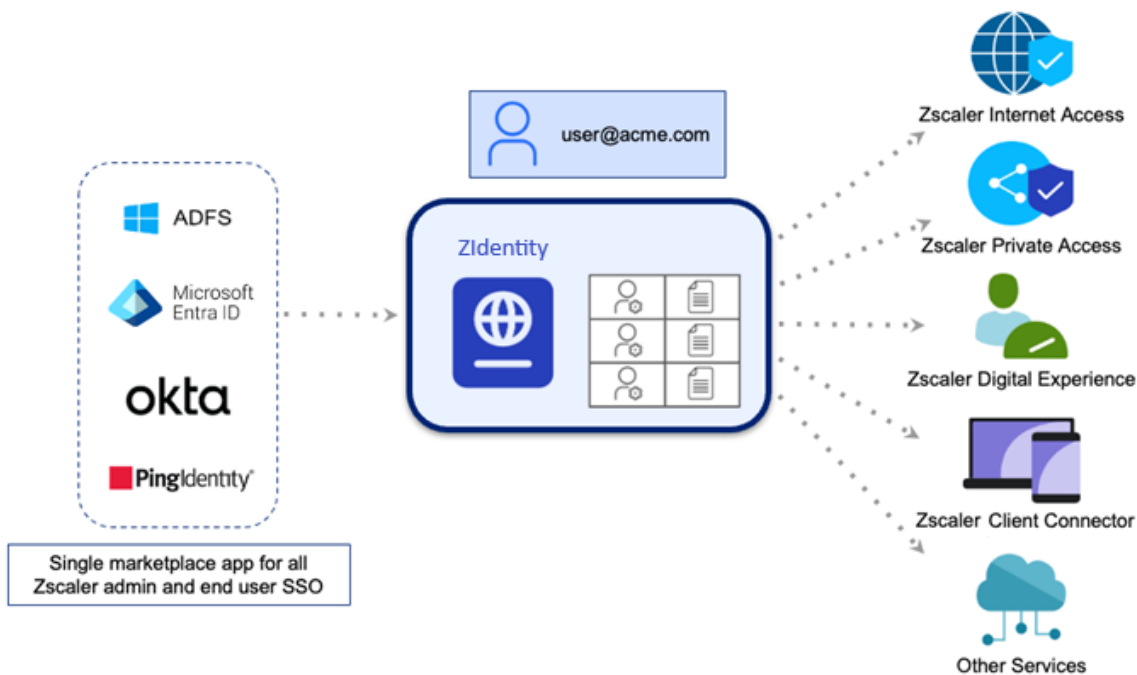


Figure 1. ZIdentity in an authentication environment

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 deactivated (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.

If you use ZIdentity, follow the steps in [Okta OIDC App Configuration](#).

## Overview for ZIA and ZPA

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 section shows how you can configure Okta as the SAML 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 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 catalysts to make a unified solution possible.

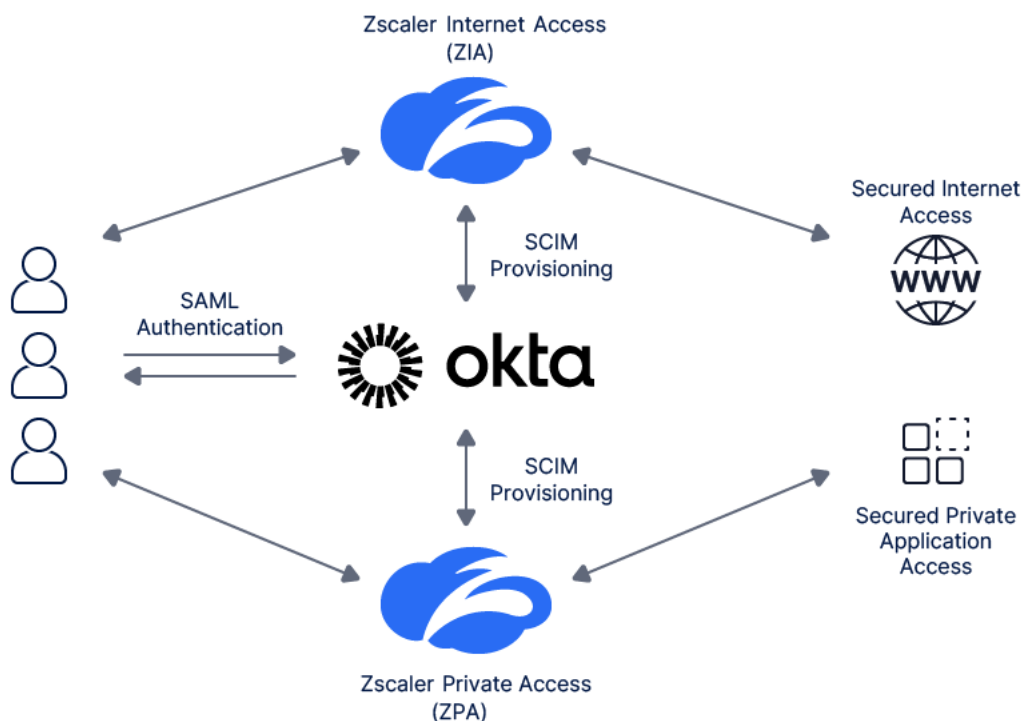


Figure 2. ZIA and ZPA in an Okta authentication environment

Provisioning with regards to authentication involves automating provisioning and deprovisioning users and security groups to Zscaler services. 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 [Zscaler Resources](#).

If you use ZIA or ZPA without Zidentity, follow the steps in [Configure Okta and ZIA: SAML and SCIM](#) and [Configure Okta and ZPA: SAML and SCIM](#).

# Okta OIDC App Configuration

This section provides information on how to use the Okta Integration Network (OIN) app to configure Okta as your OpenID Provider (OP) for Zidentity for facilitating SSO to various Zscaler services for admin access management and user authentication. The OIN-based integration uses SCIM-based provisioning. To learn more, see [OIDC-Based Authentication via OIN App Integration](#).

If your Okta subscription does not include SCIM provisioning, you can use a custom app integration for OIDC with Just-in-Time (JIT) provisioning. To learn more, see [OIDC-Based Authentication via Custom App Integration](#). To use SAML instead of OIDC, see [SAML-Based Authentication](#). The SAML-based integration supports either SCIM or JIT.

## Configure Okta OIN App for Use as OP in Zidentity

Log in to the Okta Admin Console.

1. Go to **Applications > Applications** and click **Browse App Catalog**.

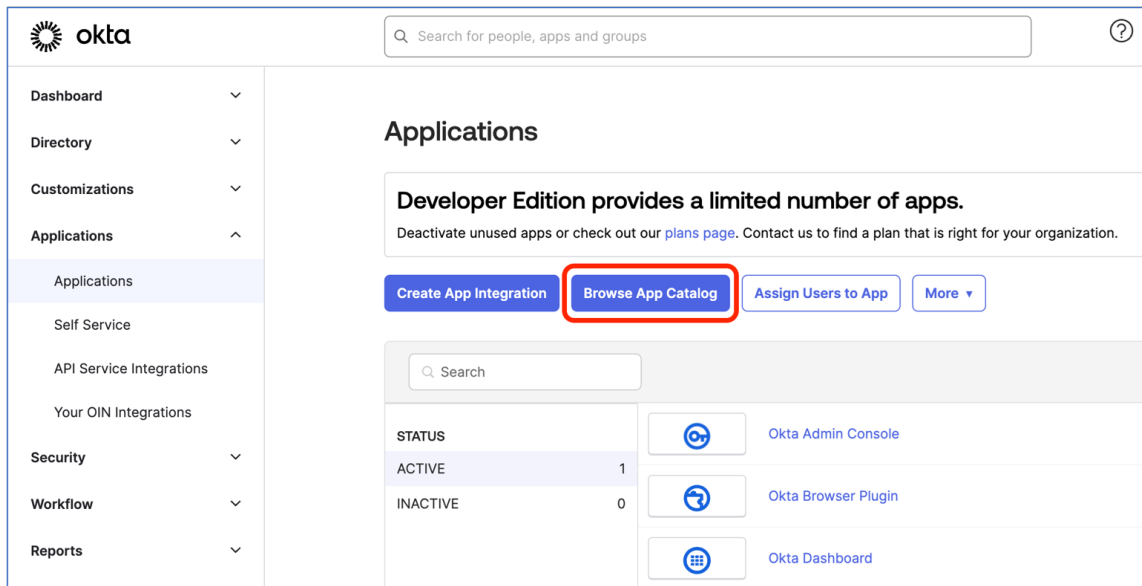


Figure 3. Browse App Catalog

2. Search for **Zscaler** in the search bar, and select the **Zscaler (SCIM, OIDC)** app.

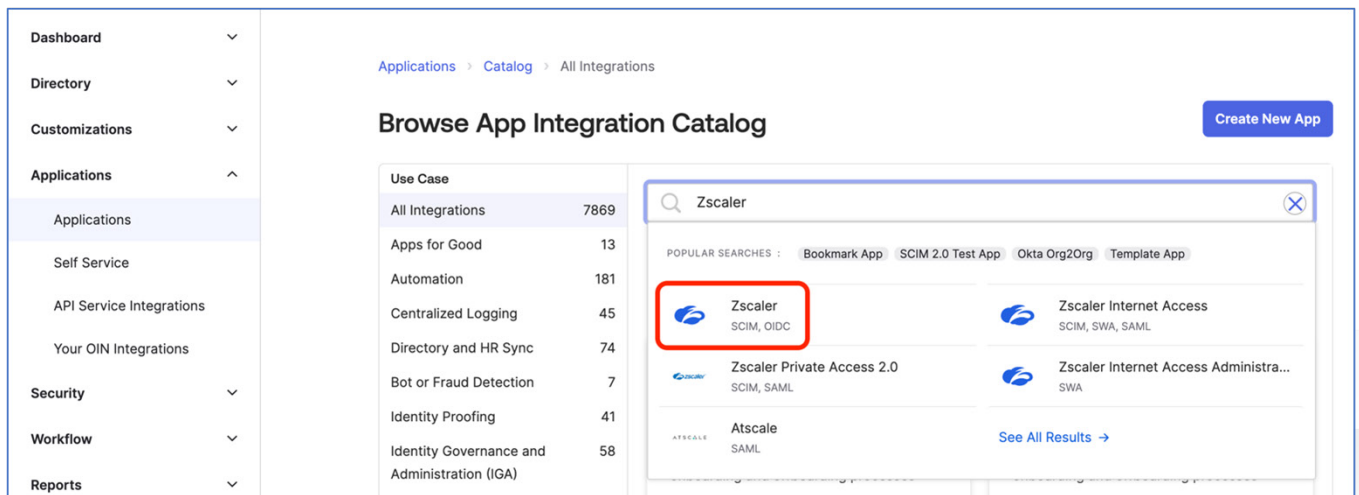


Figure 4. Search for Zscaler OIN App

3. In the app details page, click **Add Integration**.

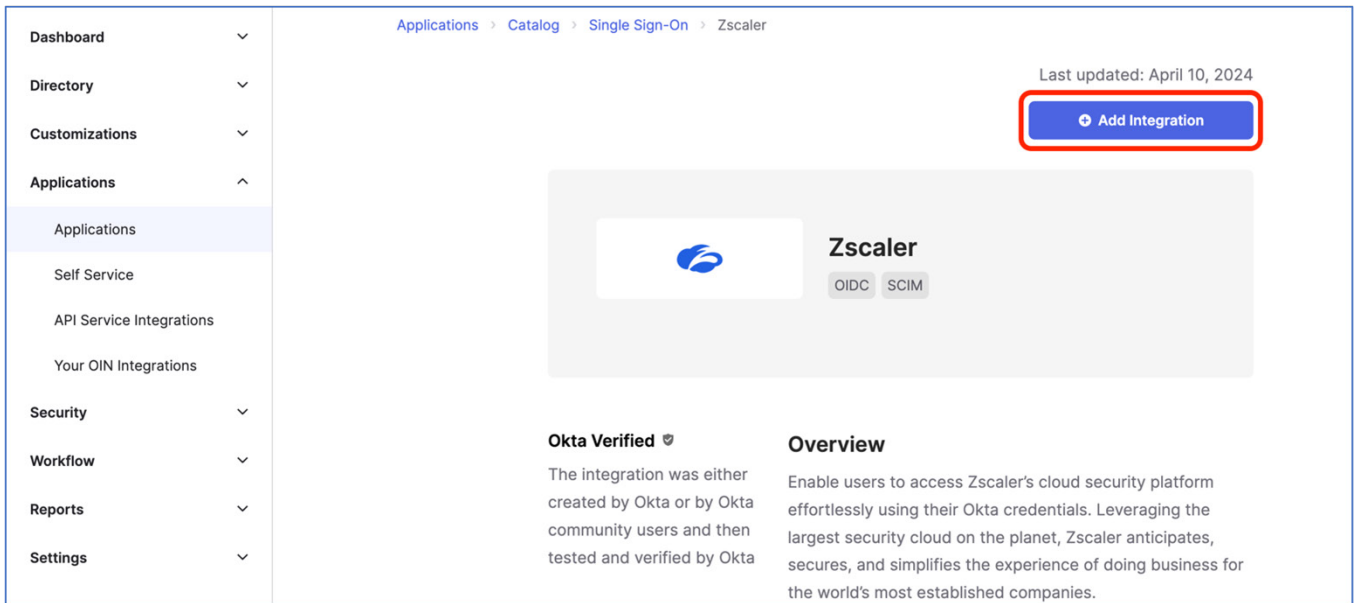


Figure 5. Add Integration

4. Enter a name in the **Application label** field.
5. Click **Done**.

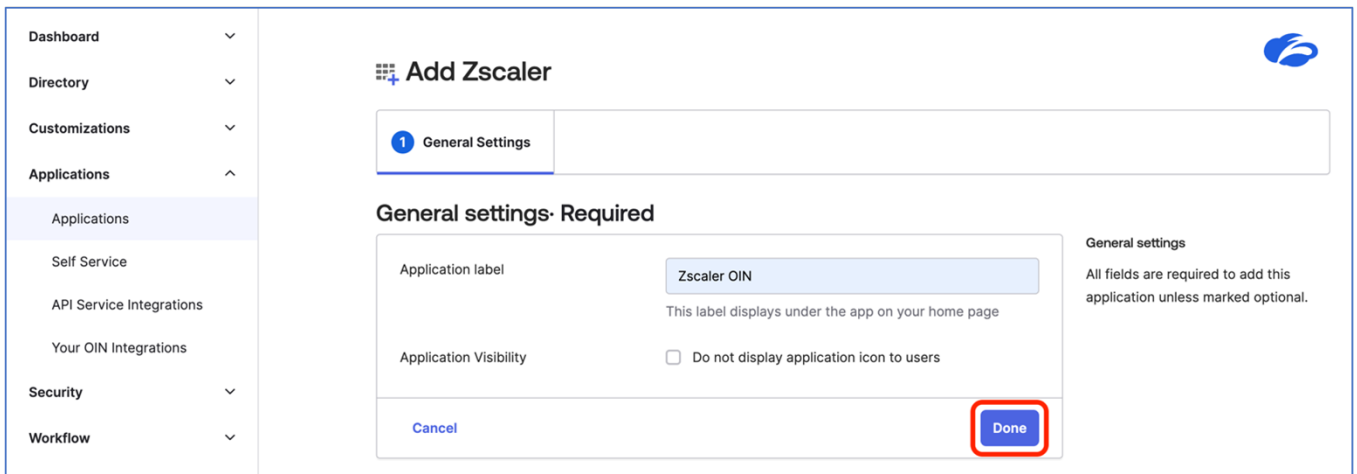


Figure 6. Application label

6. In the app configuration, go to the **Sign On** tab and copy the **Client ID** and **Client secret** values for use later.

← Back to Applications

**Zscaler OIN** Active View Logs Monitor Imports

General **Sign On** Provisioning Import Assignments Push Groups Okta API Scopes Application Rate Limits

**Settings** Edit

**Sign on methods**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ OpenID Connect

**Client ID** [Redacted] [Copy]

Public identifier for the client that is required for all OAuth flows.

**Client secret** [Redacted] [Copy]

Secret used by the client to exchange an authorization code for a token. This must be kept

**About**

**OpenID Connect** allows users to sign-on to applications using the OpenID Connect protocol.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Figure 7. Copy Sign-on method credentials

7. Scroll further down on the page and right-click the **OpenID Provider Metadata** link to copy the URL for use later.

☒ OpenID Connect

**Client ID** [Redacted] [Copy]

Public identifier for the client that is required for all OAuth flows.

**Client secret** [Redacted] [Copy]

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

**OpenID Connect** is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[OpenID Provider Metadata](#) is available if this application supports dynamic configuration.

**About**

**OpenID Connect** allows users to sign-on to applications using the OpenID Connect protocol.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Figure 8. Copy Metadata URL

The metadata URL has the following format:

`https://<your_subdomain>.okta.com/oauth2/default/.well-known/openid-configuration`

## Configure Zidentity Identity Provider with Okta as OP

Log in to the Zidentity Landing Page.

1. Go to **Integration > External Identities** and click **Add Primary IdP** (or **Add Secondary IdP**).

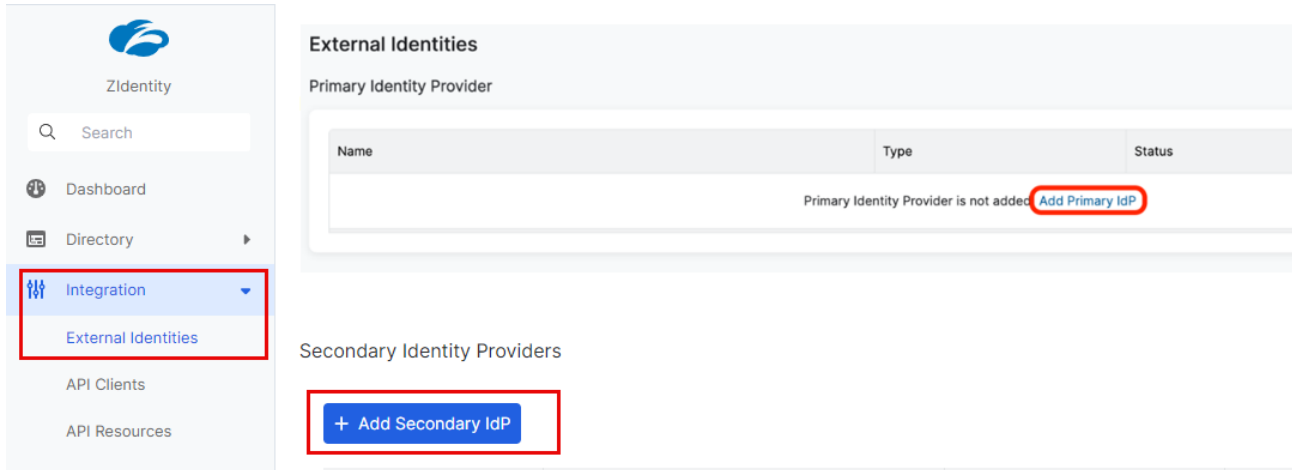


Figure 9. Add Identity Provider

2. On the **Basic** tab of the **Identity Provider** configuration page:
  - a. Enter a **Name**.
  - b. Select **Okta** for **Identity Vendor**.
  - c. For **Domain**, select the authentication domain that is used to authenticate the users.
  - d. For **Protocol**, select **OIDC**. Selecting OIDC as the protocol displays an **OIDC Configuration** section.
  - e. Enable **Status**.
  - f. Enter the OpenID Provider Metadata link recorded previously in the **Metadata URL** field and click **Fetch**.

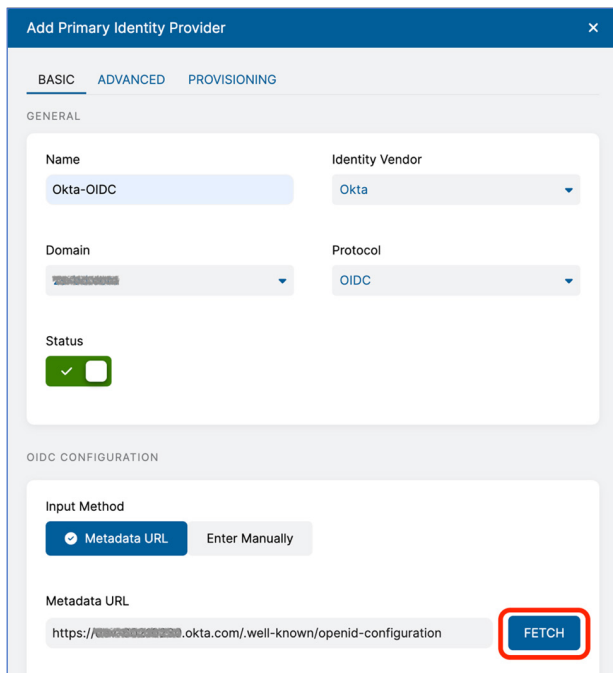


Figure 10. Configure Identity Provider

3. Scroll down and copy the **Redirect URI** for use later. Paste the **Client ID** and **Client Secret** saved previously from Okta in their respective areas and enter the items **email** and **profile** in the **Requested Scopes** section.
4. Click **Save**.

**Add Primary Identity Provider**

Redirect URI  
<https://zscaler.zsloginbeta.net/authn/login/oauth2/code/default>

Token Endpoint Authentication Method  
☒ Client Secret Basic ☐ Client Secret Post

Client ID

Client Secret

Requested Scopes

Search...

openid  
☒ email  
☒ profile

1-3 of 3 < 1 / 1 > Remove

Default Requested Authentication Context (Optional)

**Save** Cancel

Figure 11. Copy OIDC Info

5. Return to the Okta Admin Console.
6. On the OIN app's configuration page, go to the **Sign On** tab and click **Edit** to enter the **Advanced Sign-on Settings**.

**Dashboard** **Directory** **Customizations** **Applications**

**Applications**

Applications  
 Self Service  
 API Service Integrations

← Back to Applications

**Zscaler OIN** Active View Logs Monitor Imports

General **Sign On** Provisioning Import Assignments Push Groups Okta API Scopes Application Rate Limits

**Settings** **Edit**

About  
 OpenID Connect allows users to sign-on to applications using the OpenID Connect protocol.

Figure 12. Edit Settings on the Sign-On tab

- Paste the **Redirect URI** saved earlier into the corresponding field on the form. For the **Initiate Login URI** field, you must construct the URI to match the following example (substituting your ZIdentity tenant's FQDN and your authentication domain):

`https://<your_ZIdentity_tenant_FQDN>/?login_hint=xyz@<your_auth_domain>`

- Click **Save**.

**Dashboard** ▾

**Directory** ▾

**Customizations** ▾

**Applications** ▴

Applications

Self Service

API Service Integrations

Your OIN Integrations

**Security** ▾

**Workflow** ▾

**Reports** ▾

**Settings** ▾

[View Setup Instructions](#)

OpenID Provider Metadata is available if this application supports dynamic configuration.

**Advanced Sign-on Settings**

These fields may be required for a Zscaler proprietary sign-on option or general setting.

Redirect URI

Enter your Redirect URI. Refer to the Setup Instructions to obtain this value.

Initiate Login URI

Enter your Initiate Login URI. Refer to the Setup Instructions to obtain this value.

**Credentials Details**

Application username format

Update application username on

Password reveal ☐ Allow users to securely see their password (Recommended)

**Save**

Figure 13. Sign-On Settings

## Configure User Provisioning via SCIM to ZIdentity

Return to the ZIdentity Landing Page.

- Click **Edit** for your **Primary (or Secondary) Identity Provider**.

**External Identities**

Primary Identity Provider

Name	Type	Status	Actions
Okta-OIDC	SAML	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>

Secondary Identity Providers

Figure 14. OIDC Identity Provider



2. On the **Provisioning** tab, select **Enable Just-in-time (JIT) Provisioning**.
  - a. Enter your email in the **Just-in-time Attribute** field.
  - b. Select **Login Name** for the **User Attribute** from the drop-down menu.

The screenshot shows the 'Edit Primary Identity Provider' dialog with the 'PROVISIONING' tab selected. The 'STATUS' section shows 'SCIM Provisioning Status' as 'Disabled'. The 'JUST-IN-TIME (JIT) PROVISIONING' section has a toggle for 'Enable Just-in-time (JIT) Provisioning' which is turned on. The 'JUST-IN-TIME ATTRIBUTE MAPPING' section shows a 'Just-in-time User Group Attribute' field with a placeholder 'Enter Text...'. Below this, there are two fields: 'Just-in-time Attribute' with the value 'email' and 'User Attribute' with the value 'Login Name'. Both fields are circled in red. There is a '+ Add More' link at the bottom right of the mapping section.

Figure 15. Enable JIT

3. In the **SCIM Provisioning** section, select **Enable SCIM Provisioning**.
  - a. Copy the **SCIM Endpoint URL** for use later.
  - b. Click **Generate Token** and copy the **Bearer Token** for use later.
  - c. (Optional) Map additional SCIM attributes under **SCIM Attribute Mapping** (e.g., the **SCIM Attribute department** to the **User Attribute Department**).
  - d. Click **Update**.

**Edit Primary Identity Provider**

Just-in-time Attribute: email

User Attribute: Login Name

+ Add More

**SCIM PROVISIONING**

Enable SCIM Provisioning: ☒

SCIM Endpoint URL: https://zscalerbeta.net/scim/h1ho8mqgp

Authentication Method: Bearer Token

Bearer Token: ..... Generate Token

**SCIM ATTRIBUTE MAPPING**

SCIM Attribute: Enter Text... User Attribute: Select

+ Add More

Update Cancel

Figure 16. Edit Primary Identifier Provider

4. Return to the Okta Admin Console. On the **Zscaler OIN** page, go to the **Provisioning** tab and click **Configure API Integration**.

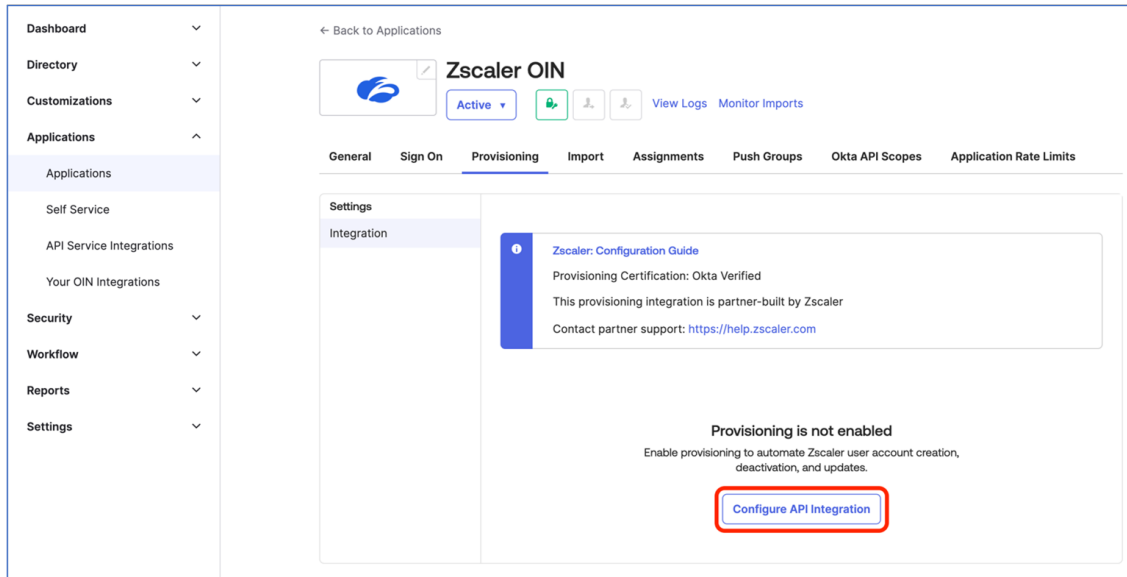


Figure 17. Provisioning tab

5. Select **Enable SCIM Integration**.
  - a. Paste the **SCIM Endpoint URL** previously copied into the **Base URL** field.
  - b. Paste the **Bearer Token** previously copied into the **API Token** field.
  - c. Click **Test API Credentials** to validate connectivity.

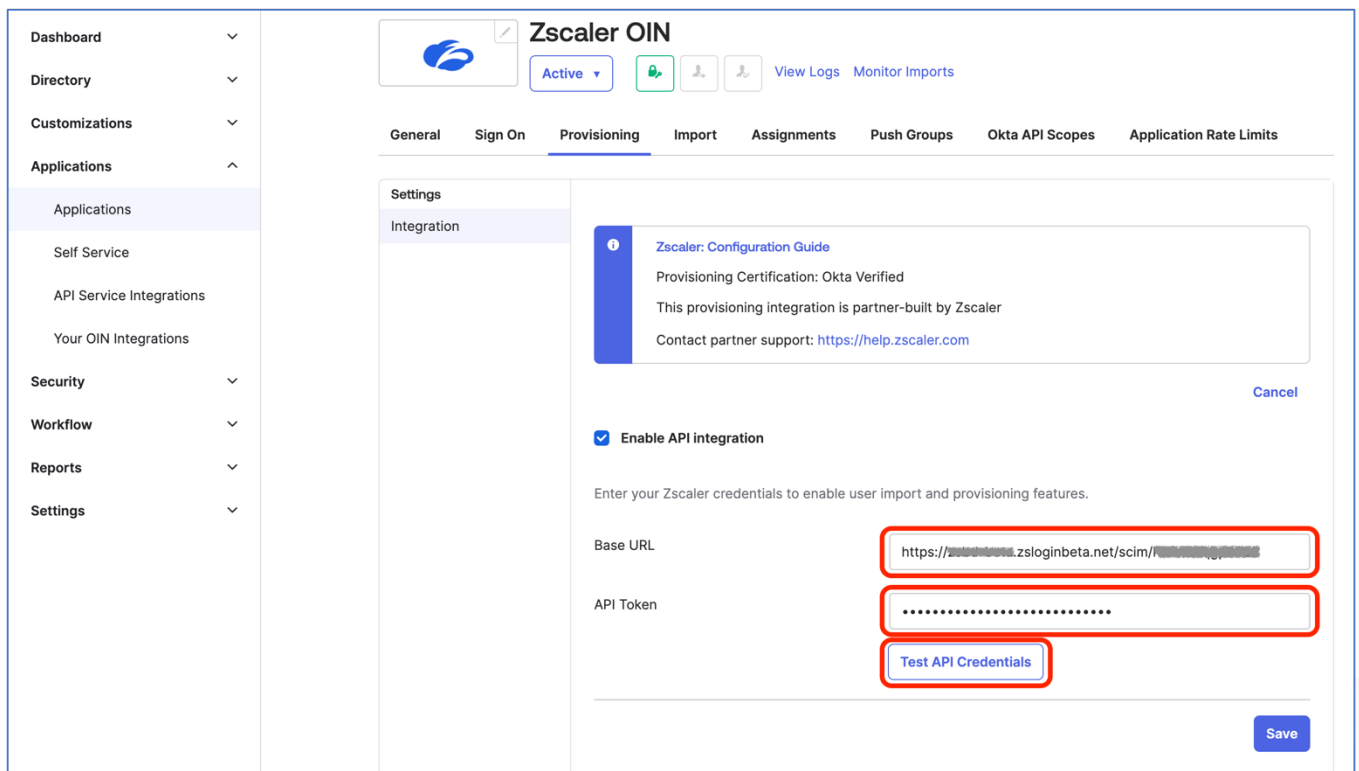


Figure 18. Configure SCIM integration

6. After you verify success, click **Save** to save the configuration.

Dashboard ▾  
Directory ▾  
Customizations ▾  
Applications ▴  
Applications  
Self Service  
API Service Integrations  
Your OIN Integrations  
Security ▾  
Workflow ▾  
Reports ▾  
Settings ▾

General Sign On **Provisioning** Import Assignments Push Groups Okta API Scopes Application Rate Limits

Settings  
Integration

**Zscaler: Configuration Guide**  
Provisioning Certification: Okta Verified  
This provisioning integration is partner-built by Zscaler  
Contact partner support: <https://help.zscaler.com>

Cancel

**Zscaler was verified successfully!**

☒ **Enable API integration**

Enter your Zscaler credentials to enable user import and provisioning features.

Base URL

API Token

Test API Credentials

Save

Figure 19. Verify SCIM integration

7. Click **Edit** to configure **Provisioning to App**.

Dashboard ▾  
Directory ▾  
Customizations ▾  
Applications ▴  
Applications  
Self Service  
API Service Integrations  
Your OIN Integrations  
Security ▾  
Workflow ▾  
Reports ▾  
Settings ▾

← Back to Applications

**Zscaler OIN**  
Active ▾ View Logs Monitor Imports

General Sign On **Provisioning** Import Assignments Push Groups Okta API Scopes Application Rate Limits

Settings  
To App  
To Okta  
Integration

**Provisioning to App**

**Create Users** ☐ Enable

Creates or links a user in Zscaler when assigning the app to a user in Okta.  
The **default username** used to create accounts is set to **Okta username**.

Edit

Figure 20. Edit Provisioning to App

8. Enable **Create Users**, **Update User Attributes**, and **Deactivate Users**.
9. Click **Save**.

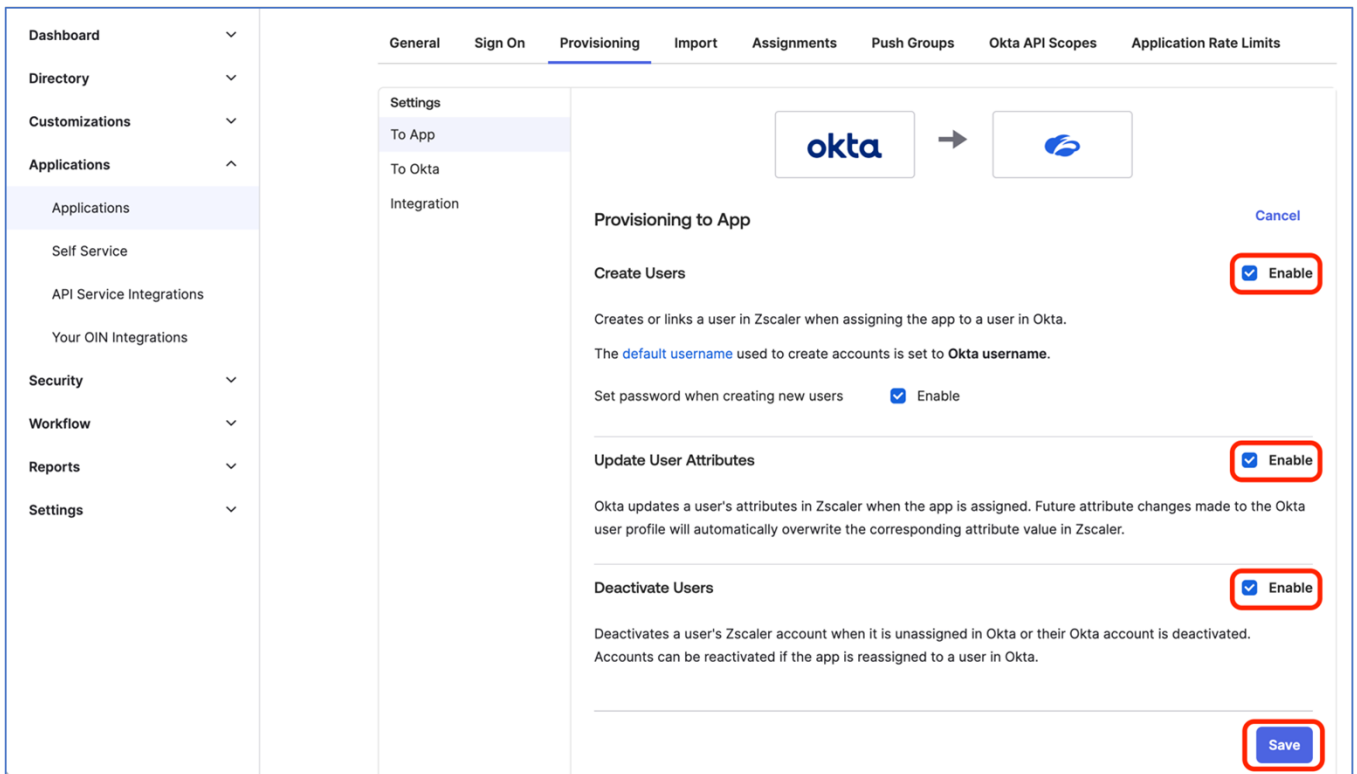


Figure 21. Select provisioning options

10. You must assign either individual users to this app or all users in a group. To assign a user:
  - a. Change to the **Assignments** tab, click **Assign**, and select **Assign to People** from the drop-down menu.

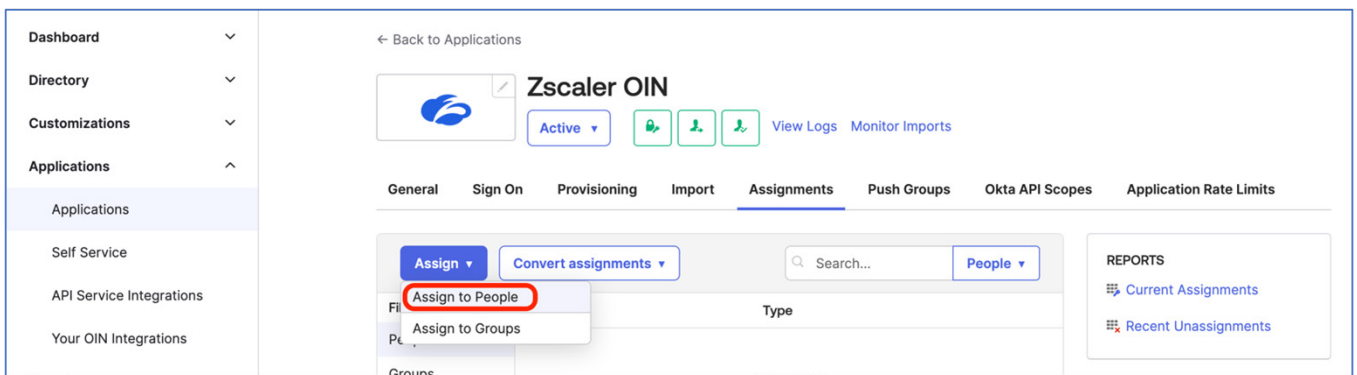
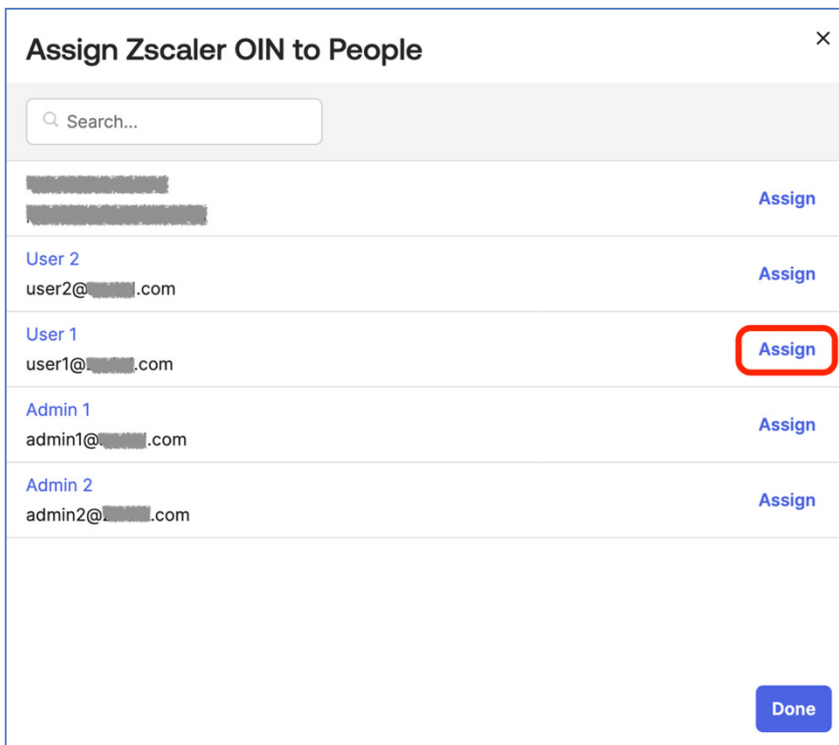


Figure 22. Assign users to OIN app

- b. To assign a specific user, click **Assign** to the right of their name.



**Assign Zscaler OIN to People** ×

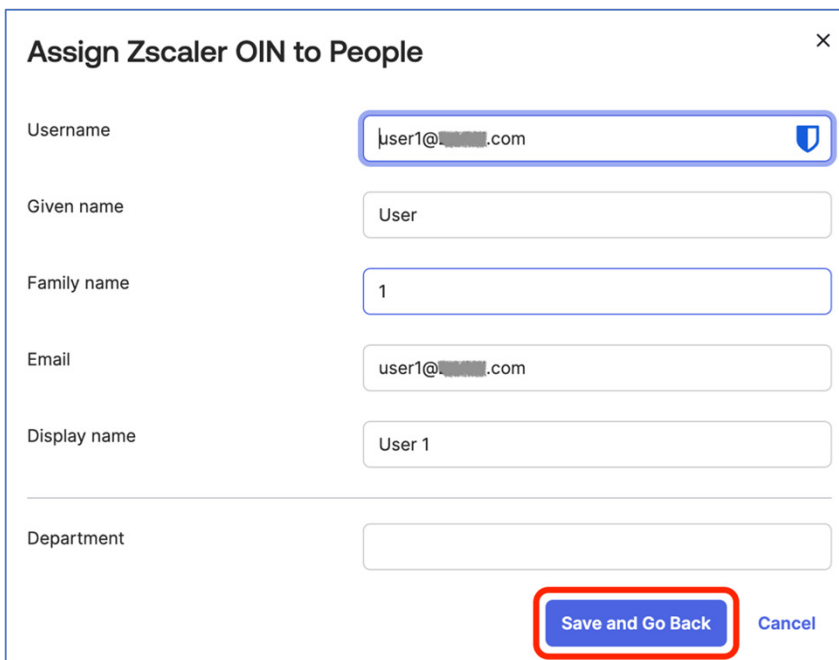
Search...

[Redacted]	Assign
User 2 user2@[Redacted].com	Assign
User 1 user1@[Redacted].com	Assign
Admin 1 admin1@[Redacted].com	Assign
Admin 2 admin2@[Redacted].com	Assign

Done

Figure 23. Select user to assign

- c. Verify the user's details and click **Save and Go Back**. Repeat for any additional users.



**Assign Zscaler OIN to People** ×

Username: user1@[Redacted].com

Given name: User

Family name: 1

Email: user1@[Redacted].com

Display name: User 1

Department:

Save and Go Back Cancel

Figure 24. Verify user to assign

- d. Click **Done**. The assigned users are automatically provisioned into Zidentity.

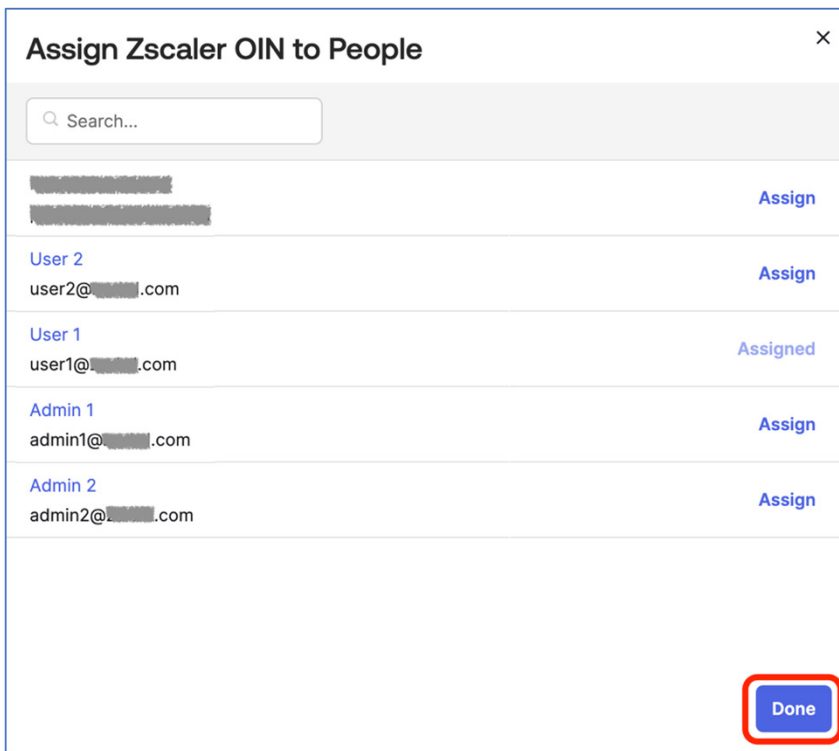


Figure 25. Finish assigning users

11. Alternatively, to assign a group of users:
- Click **Assign** and select **Assign to Groups** from the drop-down menu.

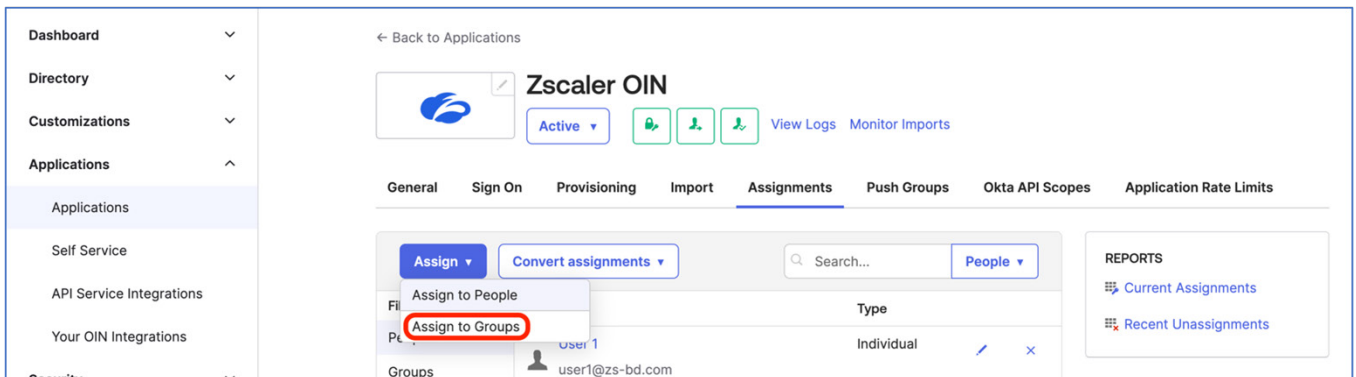
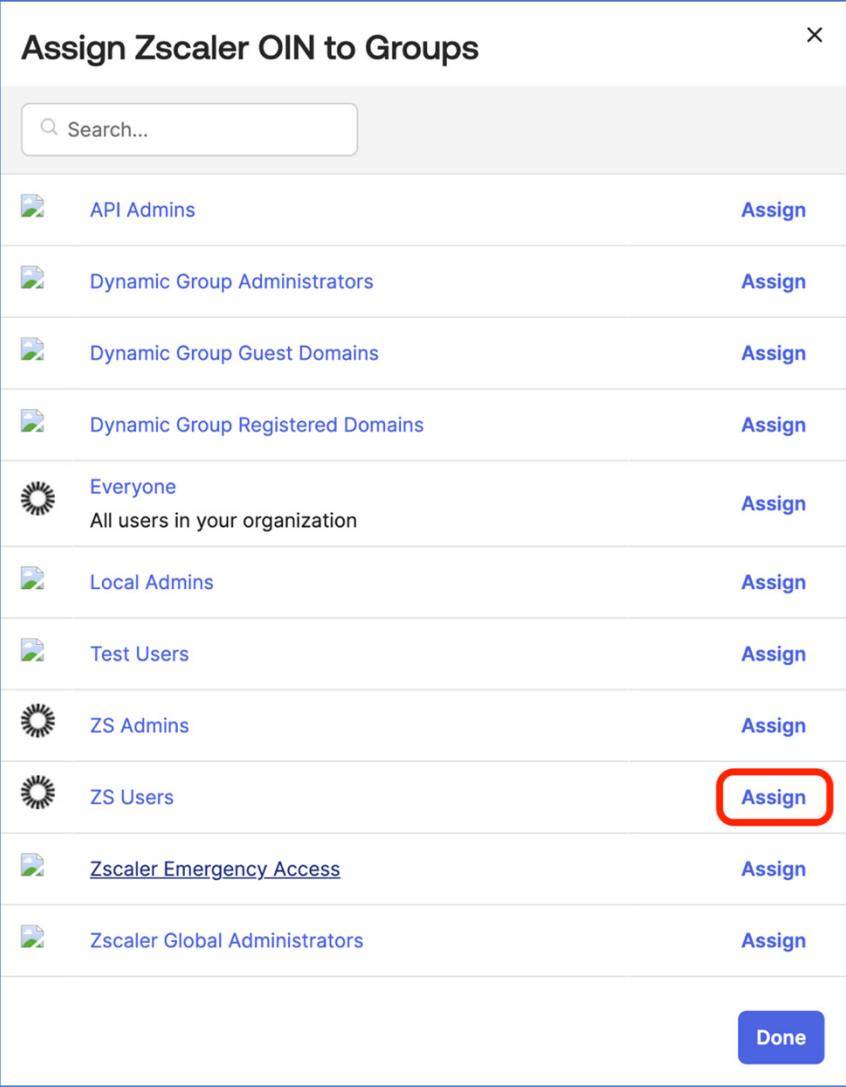













Figure 26. Assign groups to OIN app

- b. To assign a specific group, click **Assign** to the right of the group name.



**Assign Zscaler OIN to Groups** ✕

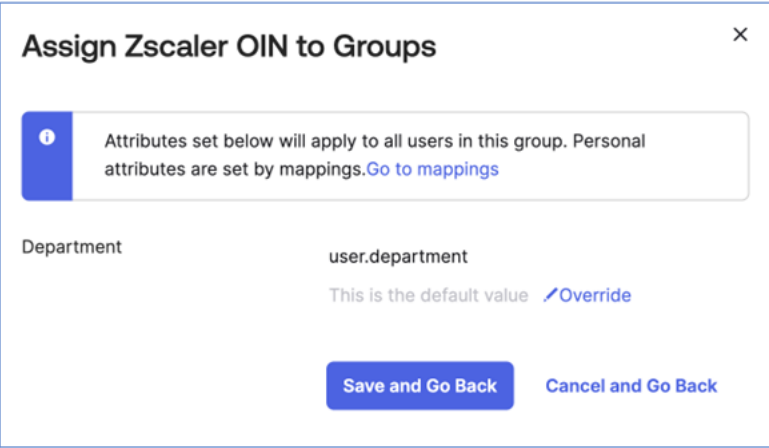
Search...

	API Admins	Assign
	Dynamic Group Administrators	Assign
	Dynamic Group Guest Domains	Assign
	Dynamic Group Registered Domains	Assign
	Everyone All users in your organization	Assign
	Local Admins	Assign
	Test Users	Assign
	ZS Admins	Assign
	ZS Users	<b>Assign</b>
	<a href="#">Zscaler Emergency Access</a>	Assign
	Zscaler Global Administrators	Assign

Done

Figure 27. Select Group to Assign

- c. Verify the group's attribute details and click **Save and Go Back**. Repeat for any additional groups.



**Assign Zscaler OIN to Groups** ✕

Attributes set below will apply to all users in this group. Personal attributes are set by mappings. [Go to mappings](#)

Department: user.department  
This is the default value [Override](#)

Save and Go Back Cancel and Go Back

Figure 28. Verify attributes in Group to Assign



- d. Click **Done** when finished. You must still push the assigned groups into ZIdentity, as it does not happen automatically.

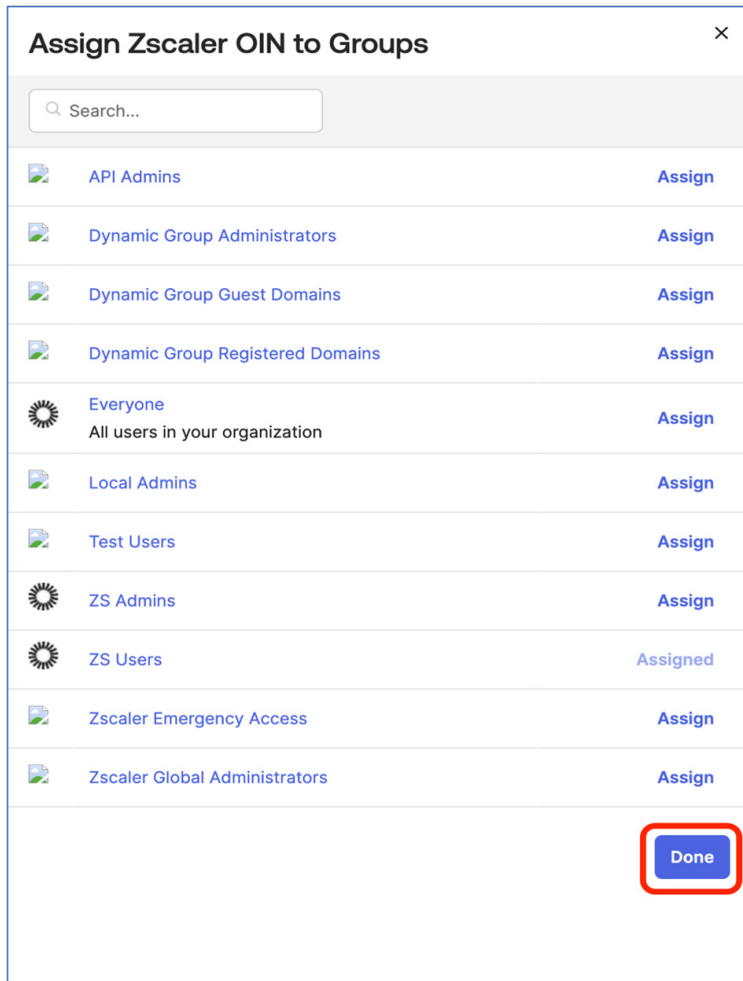


Figure 29. Finish assigning groups

12. Assign groups by either name or rule on the **Push Groups** tab. To assign a group by name:
- Click **Push Groups** and select **Find groups by name** from the drop-down menu.

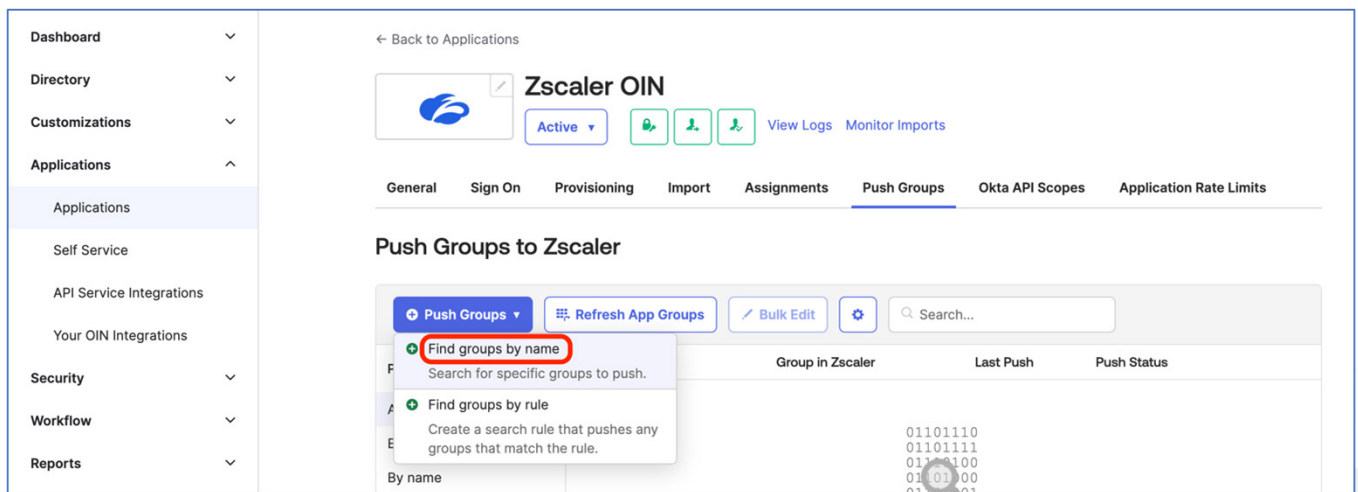


Figure 30. Push groups by name

- b. Search for the group by name in the **Enter a group to push** field. A list of options is displayed as you type. The **Push group memberships immediately** option is selected by default, but you can disable it if you prefer.

Figure 31. Choose group to push

- c. Validate the group selection and click **Save** (or **Save & Add Another**).

Figure 32. Validate group name

- d. Verify that the selected group is active.

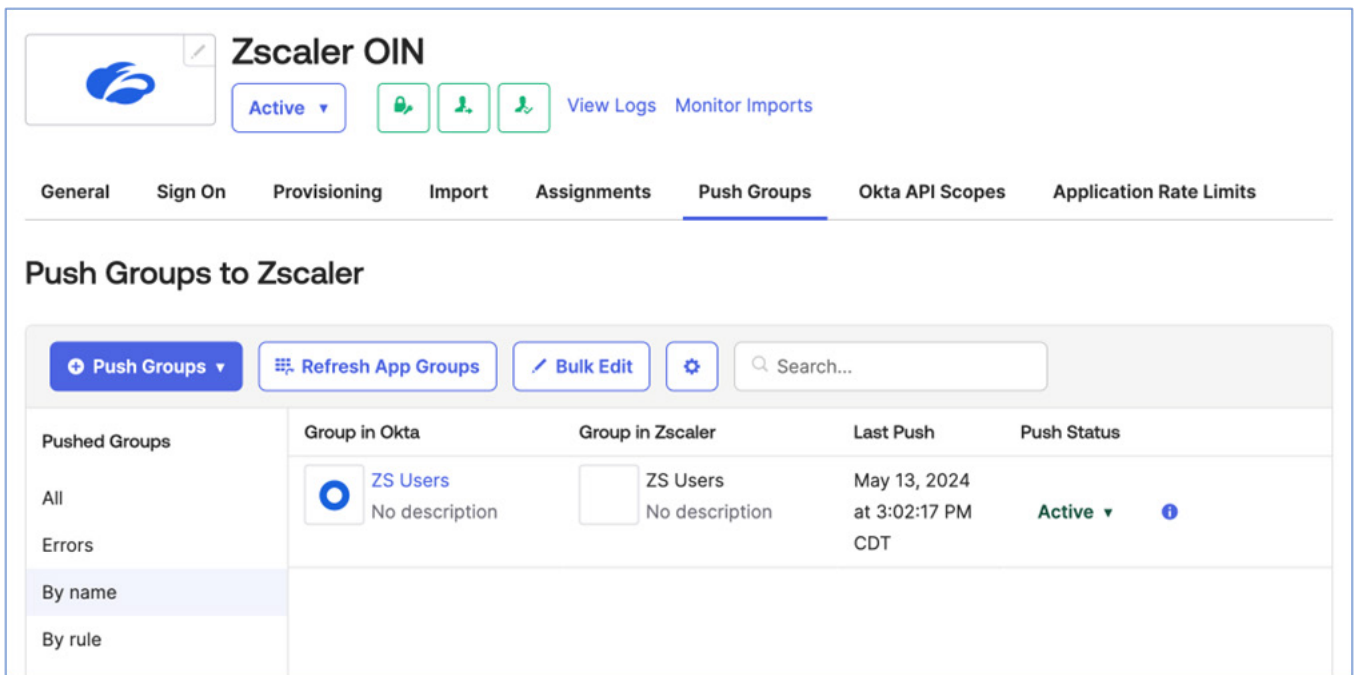


Figure 33. Verify named group is active

13. Alternatively, to assign a group by rule:
- Click **Push Groups** and select **Find groups by rule** from the drop-down menu.

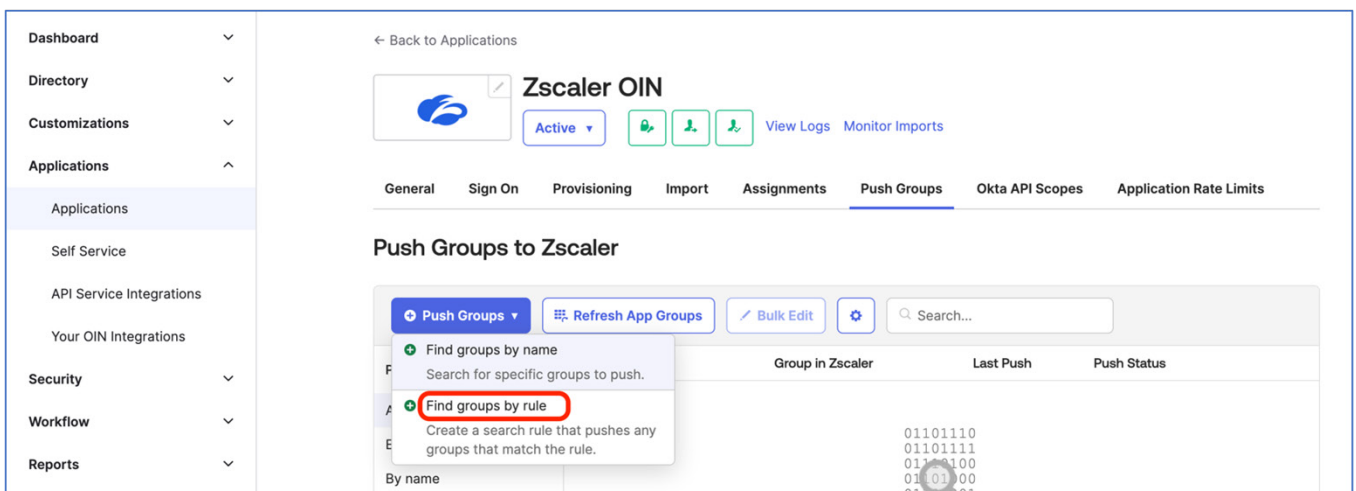


Figure 34. Push groups by rule

b. Enter a rule name. You must enter match criteria for either (or both):

- **Group name:** The name of the desired group starts with, ends with, or contains the string.
- **Group description:** The group description starts with, ends with, or contains the string.

The **Immediately push groups found by this rule** option is selected by default, but you can disable it if you prefer.

c. Click **Create Rule** when done.

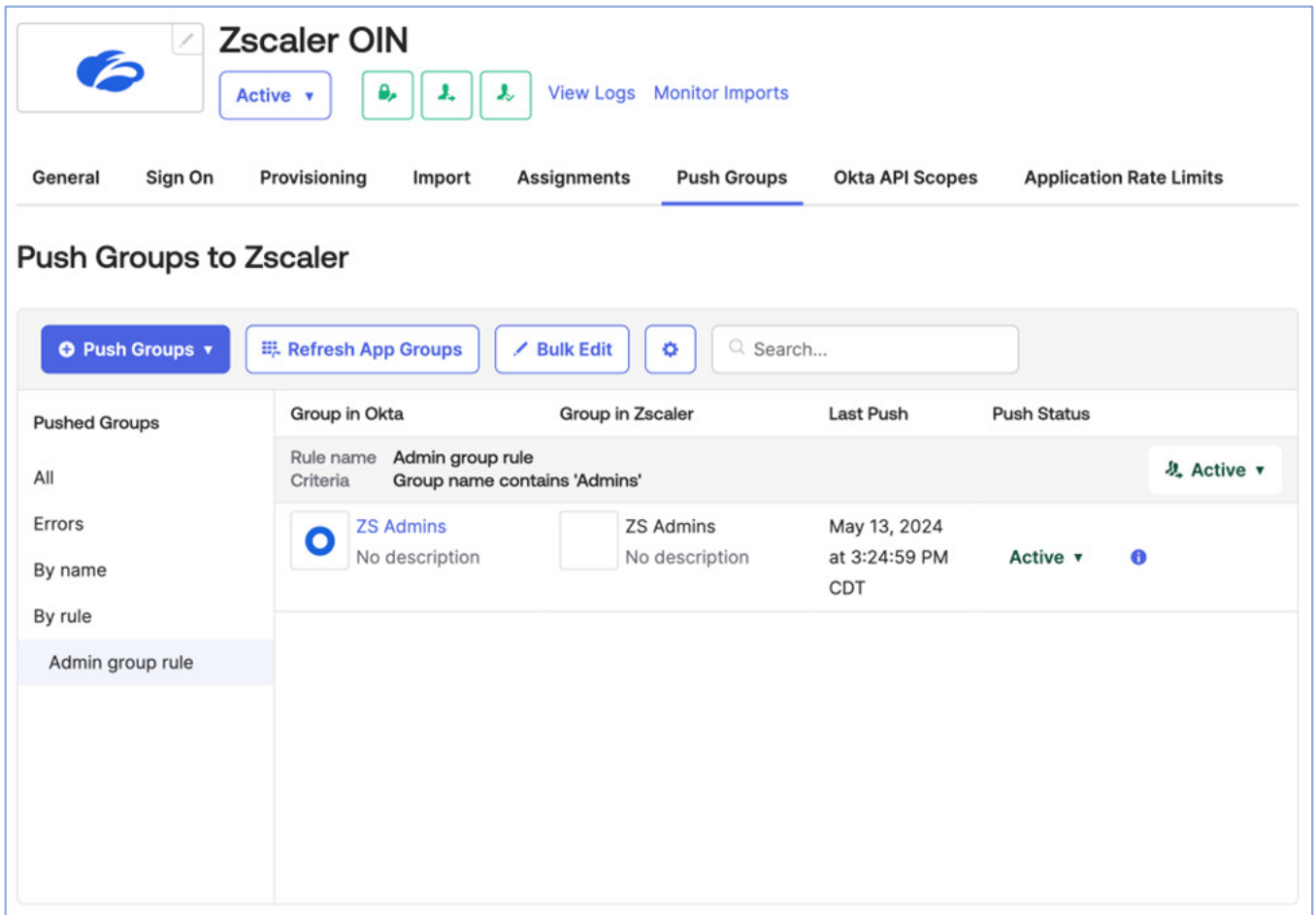
The screenshot shows the Zscaler OIN interface for configuring push groups. The top navigation bar includes 'General', 'Sign On', 'Provisioning', 'Import', 'Assignments', 'Push Groups' (selected), 'Okta API Scopes', and 'Application Rate Limits'. The 'Push Groups' section is titled 'Push Groups to Zscaler'. On the left, a sidebar shows 'Pushed Groups' with options: 'All', 'Errors', 'By name', 'By rule' (selected), and 'Admin group rule'. The main content area is titled 'Push groups by rule' and contains the following fields:

- Rule name:** Admin group rule
- Group name:** contains (dropdown) Admins (text input)
- Group description:** starts with (dropdown) Enter string to match... (text input)
- ☒ Immediately push groups found by this rule

A red box highlights the 'Create Rule' button at the bottom right, next to a 'Cancel' button.

Figure 35. Define rule to match groups to push

d. Validate that the rule is active.

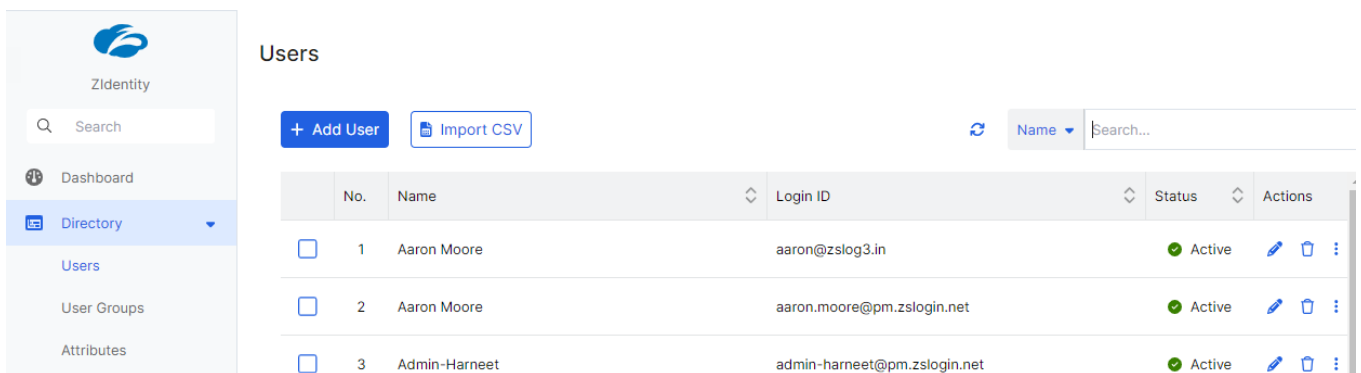


The screenshot shows the Zscaler OIN interface. At the top, there's a header with the Zscaler logo, a status bar (Active), and links for View Logs and Monitor Imports. Below this is a navigation menu with tabs: General, Sign On, Provisioning, Import, Assignments, **Push Groups**, Okta API Scopes, and Application Rate Limits. The main section is titled 'Push Groups to Zscaler'. It contains a sidebar with filters (Push Groups, Errors, By name, By rule) and a main table. The table has columns: Group in Okta, Group in Zscaler, Last Push, and Push Status. The 'Admin group rule' is listed with criteria 'Group name contains 'Admins'', and its status is 'Active'. The last push was on May 13, 2024 at 3:24:59 PM CDT.

Pushed Groups	Group in Okta	Group in Zscaler	Last Push	Push Status
All	Rule name: Admin group rule Criteria: Group name contains 'Admins'			Active
Errors				
By name				
By rule				
Admin group rule	<div> <b>ZS Admins</b>            No description         </div>	<div> <b>ZS Admins</b>            No description         </div>	May 13, 2024 at 3:24:59 PM CDT	Active

Figure 36. Verify rule is active

14. To verify that users and groups have been provisioned, in the Zidentity Landing Page, go to **Directory > Users** and review the users or search for them by name.



The screenshot shows the Zidentity 'Users' page. On the left is a sidebar with navigation links: Dashboard, **Directory**, Users, User Groups, and Attributes. The main area has a search bar and buttons for '+ Add User' and 'Import CSV'. Below is a table of users.

No.	Name	Login ID	Status	Actions
1	Aaron Moore	aaron@zslog3.in	Active	
2	Aaron Moore	aaron.moore@pm.zslogin.net	Active	
3	Admin-Harneet	admin-harneet@pm.zslogin.net	Active	

Figure 37. Verify users provisioned

- To verify that your groups are provisioned, go to **Directory > User Groups** and review or search for them by group name.

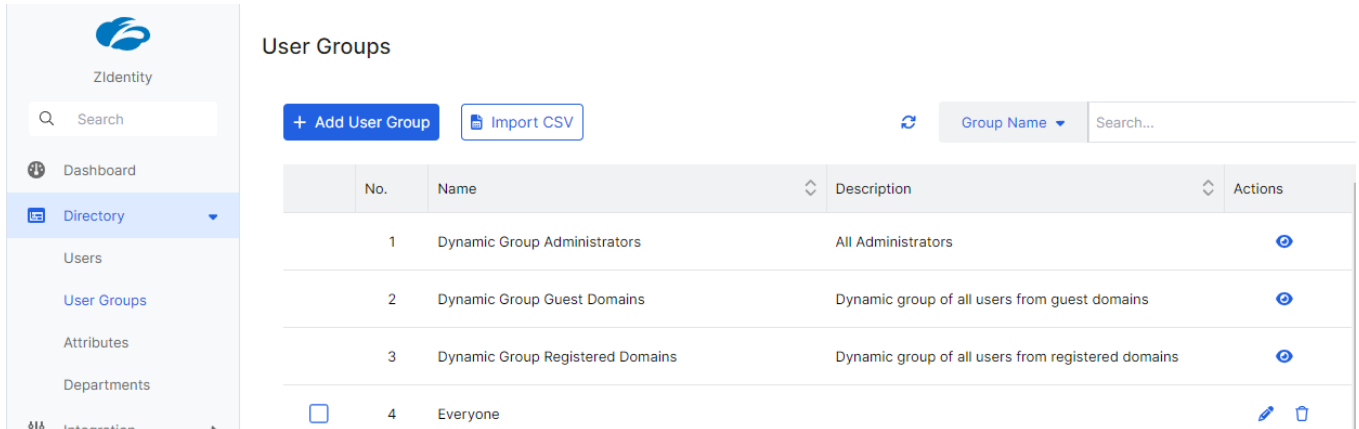


Figure 38. Verify groups provisioned

## Assigning Zidentity Entitlements

To use Okta for authentication to Zscaler tenants (like ZIA, ZPA, etc.), you must assign entitlements in Zidentity. To learn more about Administrative entitlement, see [About Administrative Entitlements](#). To learn more about service entitlements, see [About Service Entitlements](#).

- To entitle a user to log in as an admin to one of the Zscaler services, go to **Administration > Entitlements > Administrative** in the Zidentity Landing Page and select the service.

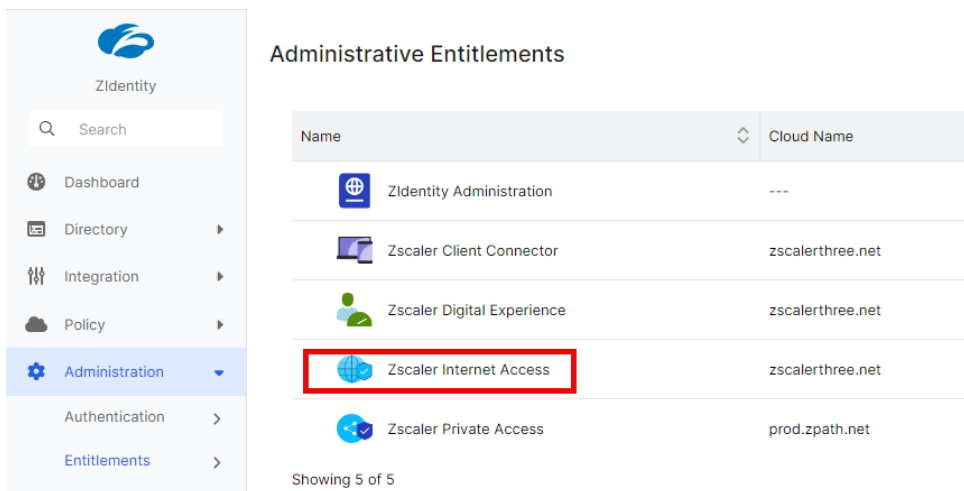


Figure 39. Select Service for Admin

- Select the **Users** tab, and click **Assign Users** (you can also assign based on user groups).

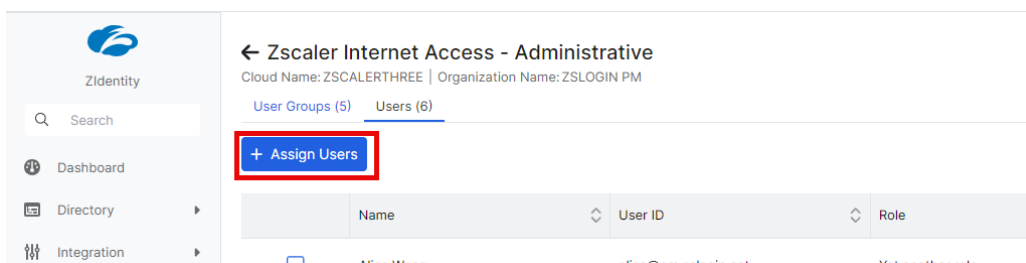


Figure 40. Assign Users for Admin

3. Select an admin user (or users) and then click **Next**.

**← Assign Users**

**Select Users & Roles**  
Zscaler Internet Access - Administrative | Cloud Name: ZSCALERTHREE | Organization Name: ZSLOGIN PM

☐ Set same role for all selected users

Search...

	Name	User ID	Role
<input checked="" type="checkbox"/>		aaron@...n	Super Admin
<input type="checkbox"/>		aaron.moore@...net	Select
<input type="checkbox"/>	Admin-Harneet	admin-harneet@...	Select
<input type="checkbox"/>		alice@pm...	Select

Showing 27 of 27

Cancel **Next**

Figure 41. Select Admin Users

4. Verify assignment and then click **Assign**.

**← Assign Users**

**Summary**  
Zscaler Internet Access - Administrative | Cloud Name: ZSCALERTHREE | Organization Name: ZSLOGIN PM

Name	User ID	Role
	aaron@...in	Super Admin

Showing 1 of 1

Cancel **Back** **Assign**

Figure 42. Verify Admin Assignment

5. To entitle a user to log in as a user to one of the Zscaler services, go to **Administration > Entitlements > Administrative** in the Zidentity Landing Page and select the service.

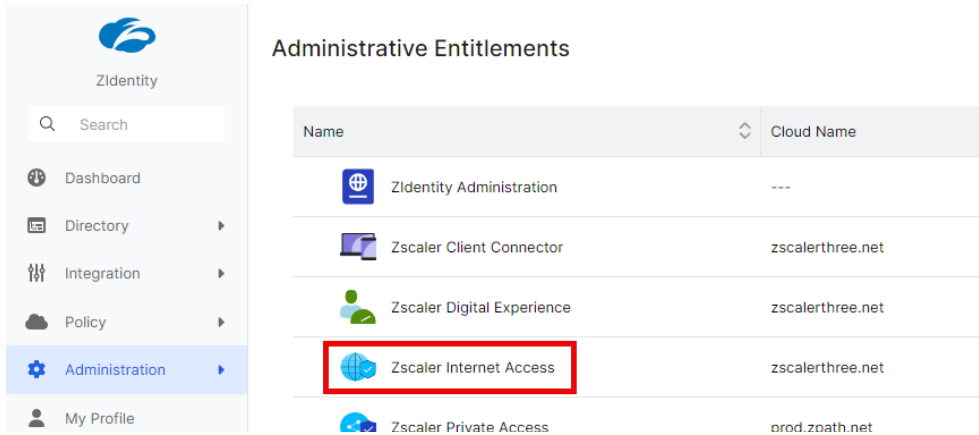


Figure 43. Select Service for Users

6. Select the **Users** tab and then click **Assign Users** (you can also assign based on user groups).

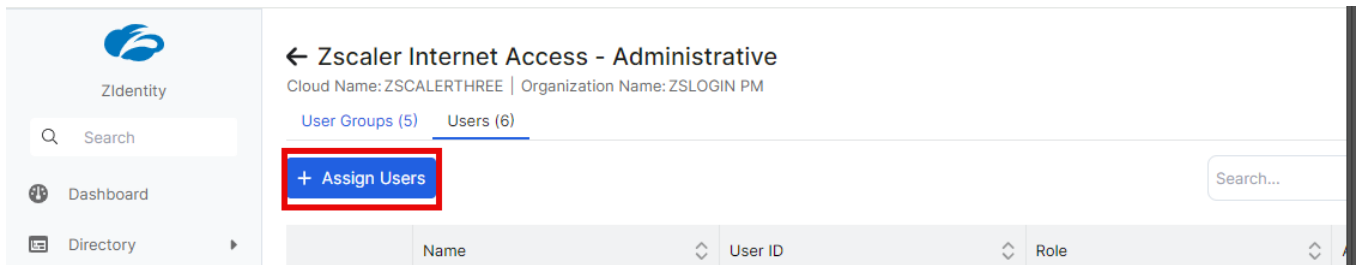


Figure 44. Assign Users for Service

7. Select a user (or users), the **Role**, and then click **Next**.

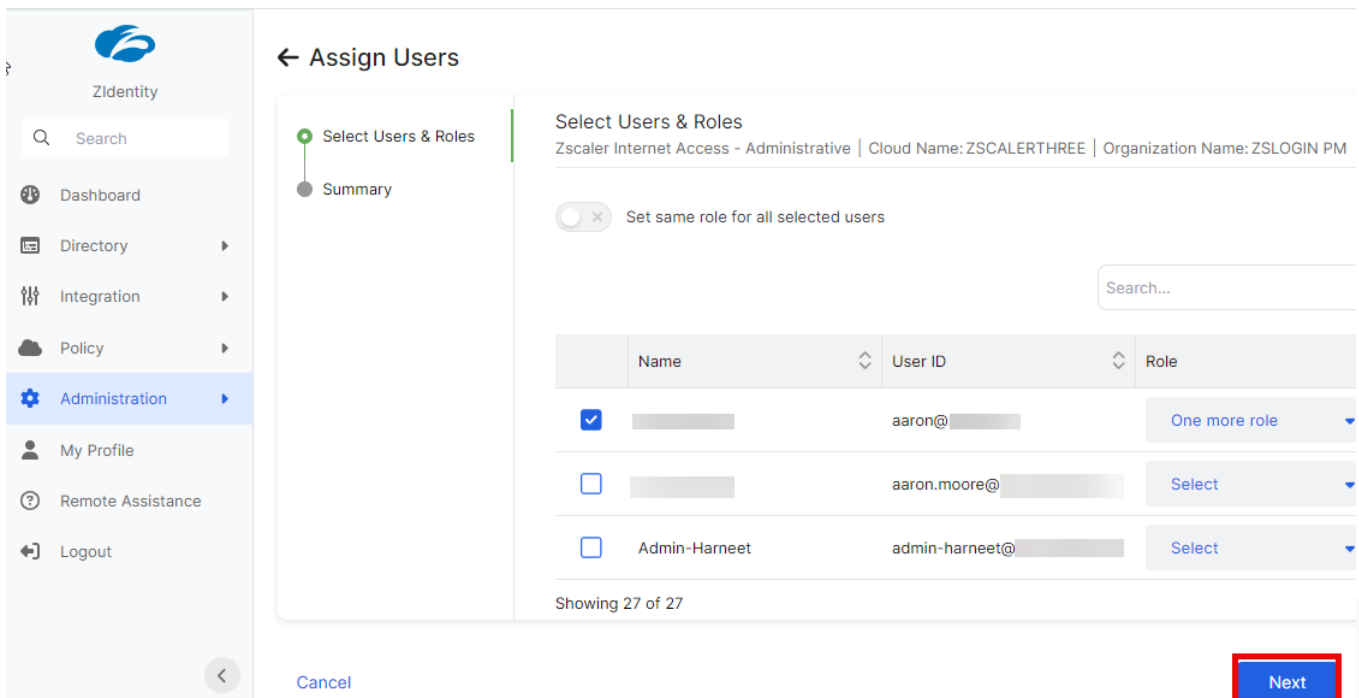


Figure 45. Select Users



8. Verify assignment and then click **Assign**.

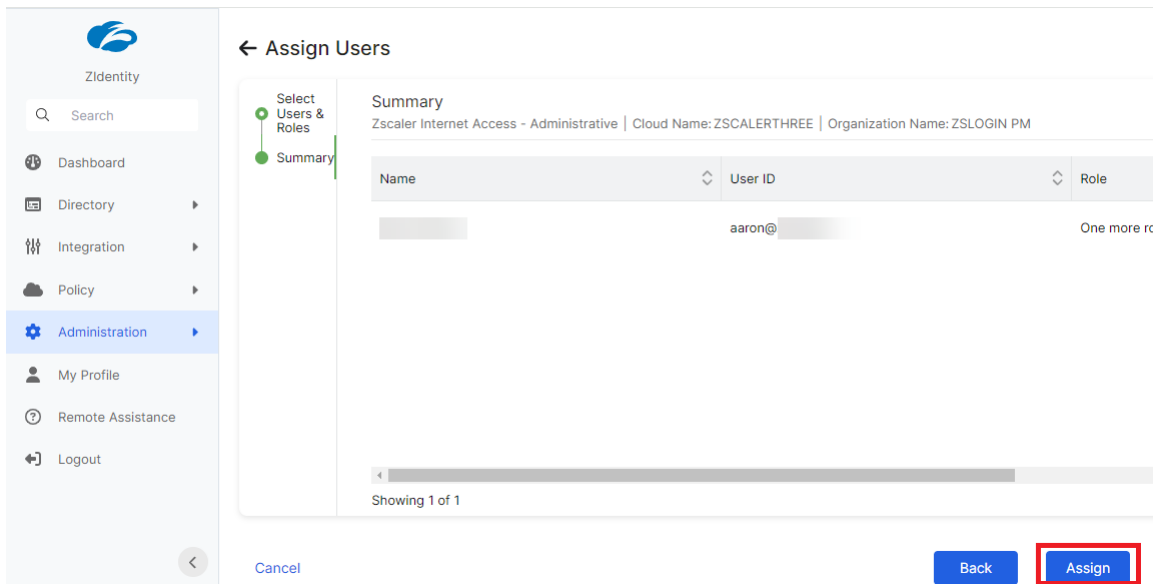


Figure 46. Verify user assignment

# Configure Okta and ZIA: SAML and SCIM

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

## Enable Okta

This document assumes that the user has a working Okta environment, and that only Zscaler applications must 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 Administrator account.

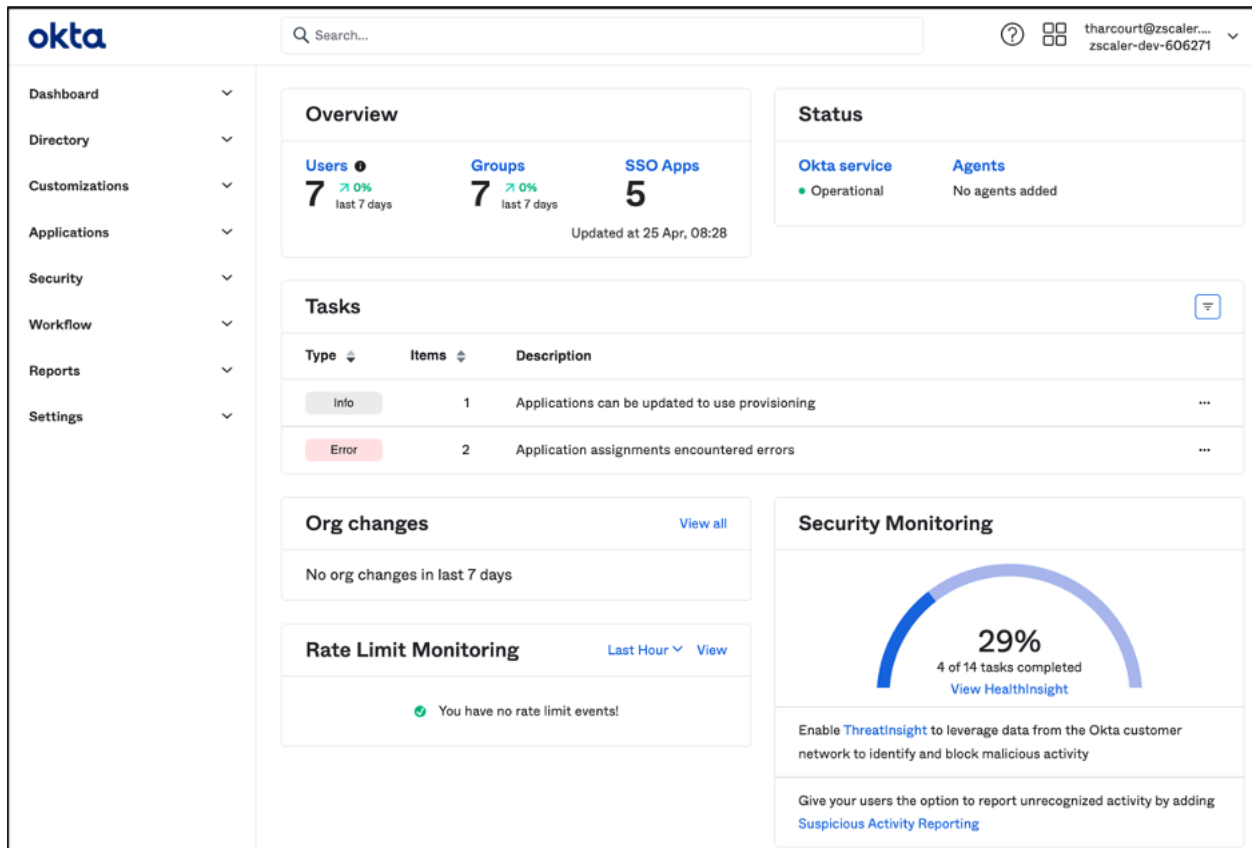


Figure 47. Okta administrator console

## 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**.

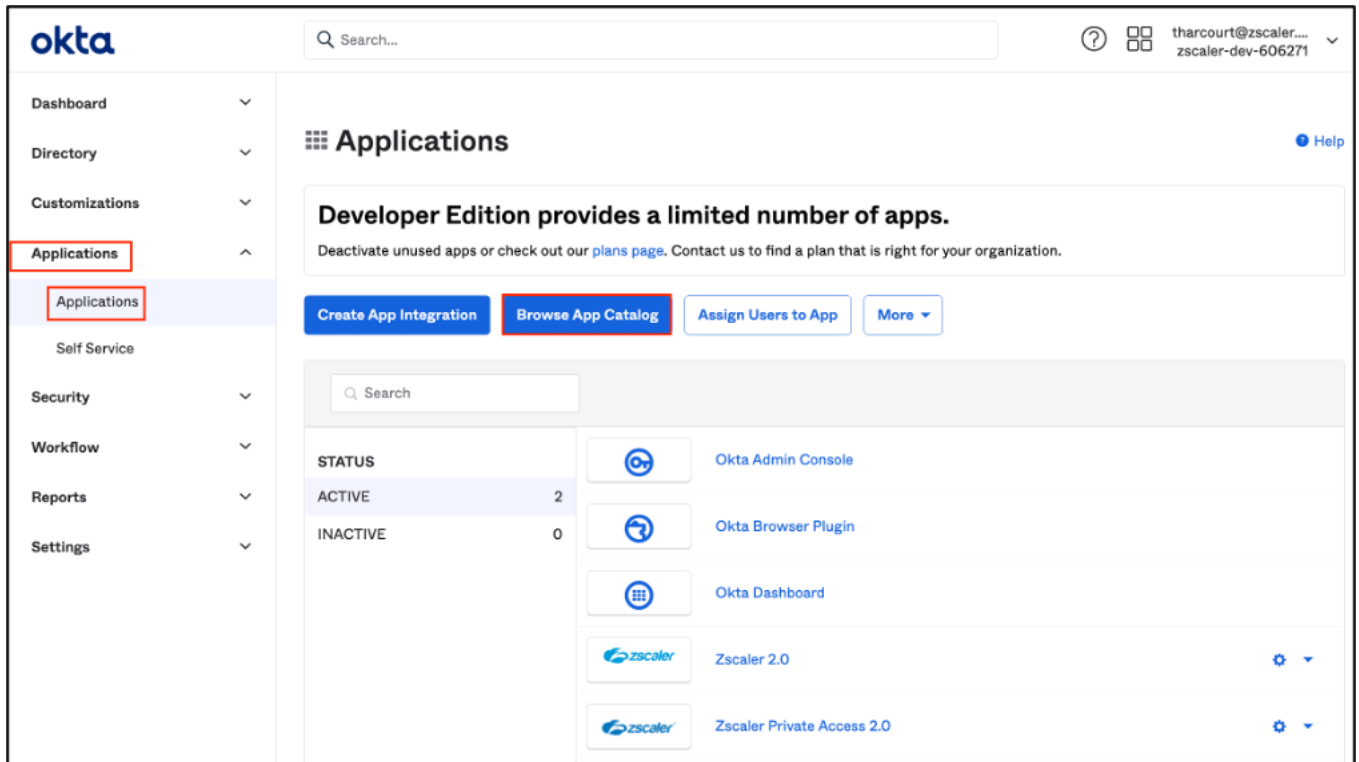


Figure 48. Adding an application

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

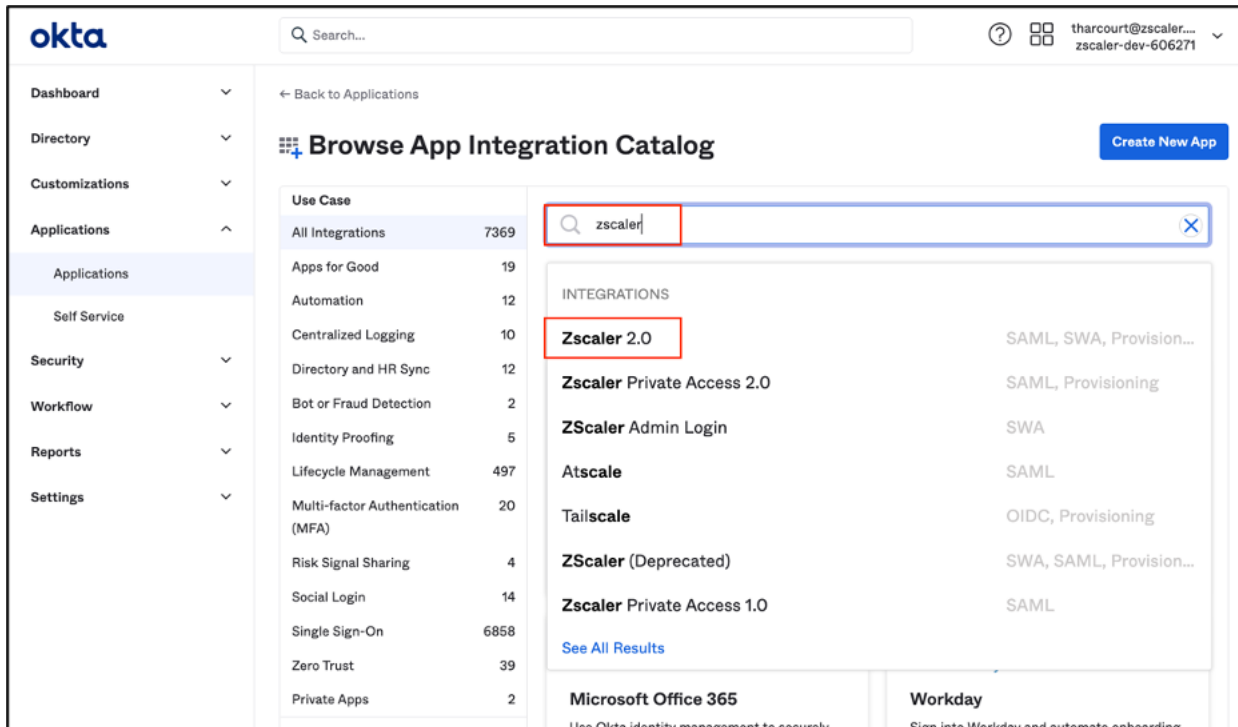


Figure 49. Adding the Zscaler applications

6. Select **Add**.

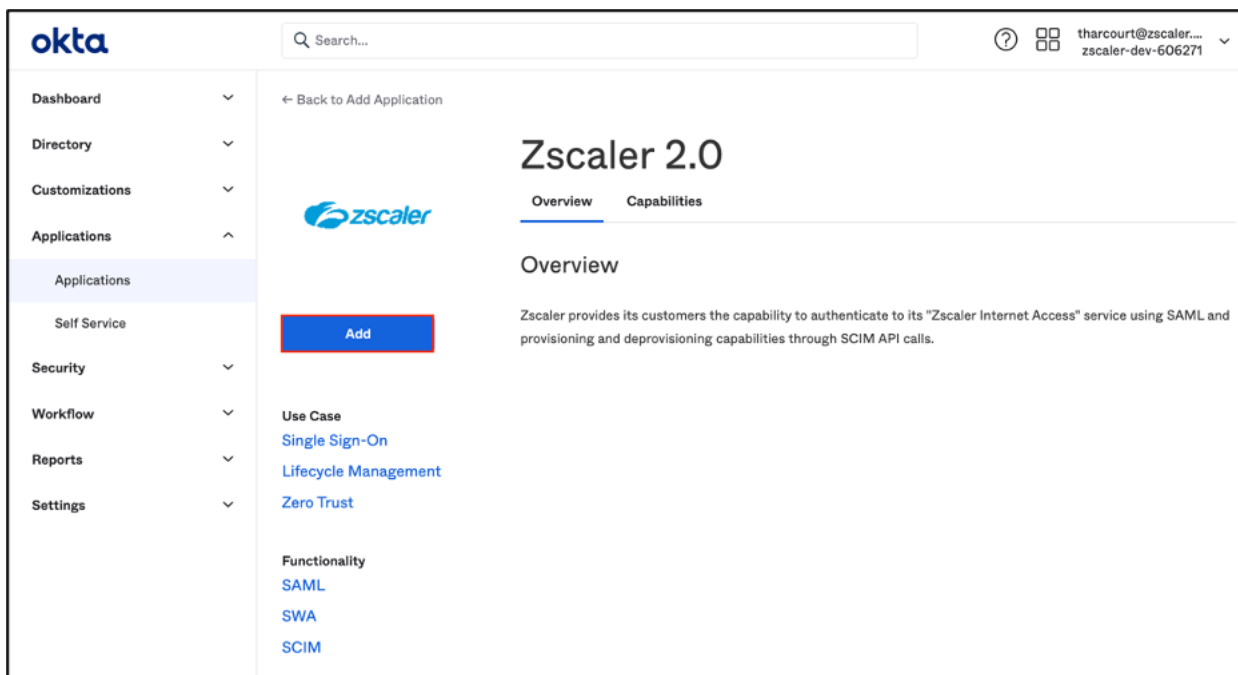


Figure 50. Zscaler app

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.

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

In the following Company ID example, zsccloud.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**.

The screenshot shows the Okta Admin Portal interface for adding a Zscaler 2.0 application. The left sidebar contains navigation links: Dashboard, Directory, Customizations, Applications (selected), Self Service, Security, Workflow, Reports, and Settings. The main content area is titled 'Add Zscaler 2.0' and has two tabs: 'General Settings' (active) and 'Sign-On Options'. Under 'General settings - Required', there are several fields and checkboxes:

- Application label:** Zscaler 2.0. A note below says: 'This label displays under the app on your home page'.
- Your Zscaler Domain:** zsccloud.net. A note below says: 'Enter your Zscaler Domain. For example, if you log into https://admin.zscaler.net/, enter: zscaler.net'.
- Application Visibility:** Three checkboxes are checked:
  - ☒ Do not display application icon to users
  - ☒ Do not display application icon in the Okta Mobile App
  - ☒ Automatically log in when user lands on login page
- Browser plugin auto-submit:** ☒ Automatically log in when user lands on login page

At the bottom, there are 'Cancel' and 'Next' buttons. The 'Next' button is highlighted with a red box. On the right side, a 'General settings' note states: 'All fields are required to add this application unless marked optional.'

Figure 51. Adding Zscaler 2.0 for ZIA

## Configure Okta for ZIA

On the Sign-On Options window:

1. Select **SAML 2.0**.
2. From the **memberOf** drop-down menu, select **Matches regex**.
3. Enter the match to **\*.** (asterisk, period).
4. Select **View Setup Instructions**.

The screenshot shows the Okta Admin Console interface for configuring a Zscaler 2.0 application. The 'Sign-On Options' tab is active, and the 'SAML 2.0' sign-on method is selected. The 'memberOf' attribute is configured with the value '\*'. The 'View Setup Instructions' button is highlighted. The left sidebar shows the navigation menu with 'Applications' selected. The right sidebar contains 'About' and 'Application Username' sections.

Figure 52. Setting the memberOf match and getting the SAML portal URL

5. Select **View Setup Instructions** to launch a window where you find the **SAML Portal URL** and the download link to the Okta Public Certificate.
6. Copy the **SAML Portal URL**.
7. Download and save the **Okta Public Certificate** for the Zscaler setup as a PEM file (e.g., cert.pem).
8. Select **Done**.

3 In the **Identity Provider (IDP) Options** section of the SAML Configuration screen, enter the following:

- **SAML Portal URL:** Copy and paste the following:
- **Login Name Attribute:** Enter `NameID`.
- **Public SSL Certificate:** First click here to download the certificate for upload:

Figure 53. The Zscaler SAML portal URL and public certificate

## Configure Zscaler ZIA for an Okta IdP

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

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

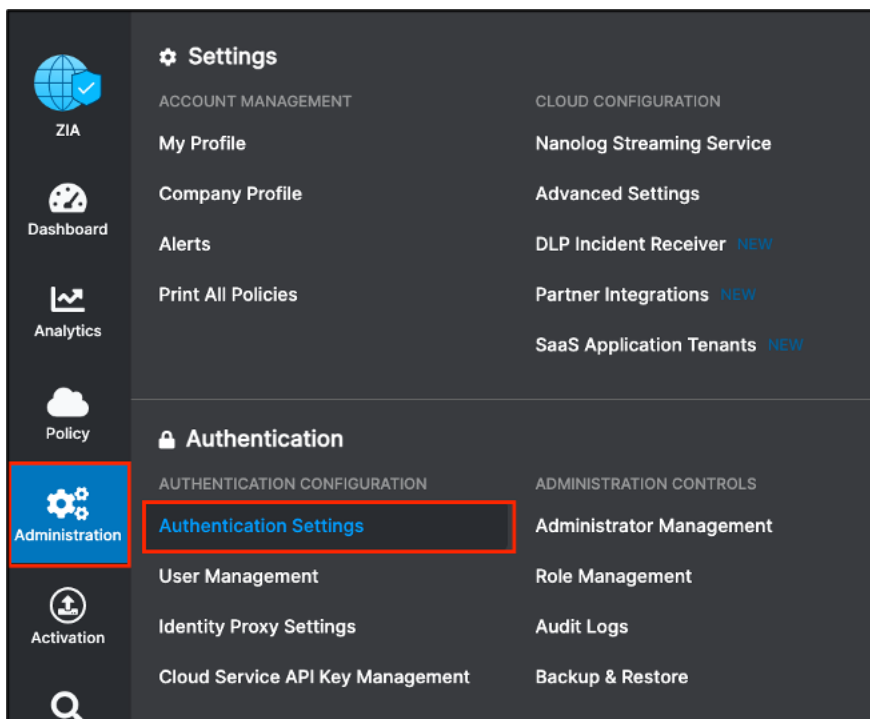


Figure 54. Adding Okta and the ZIA IdP

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

3. Select **Add IdP**.

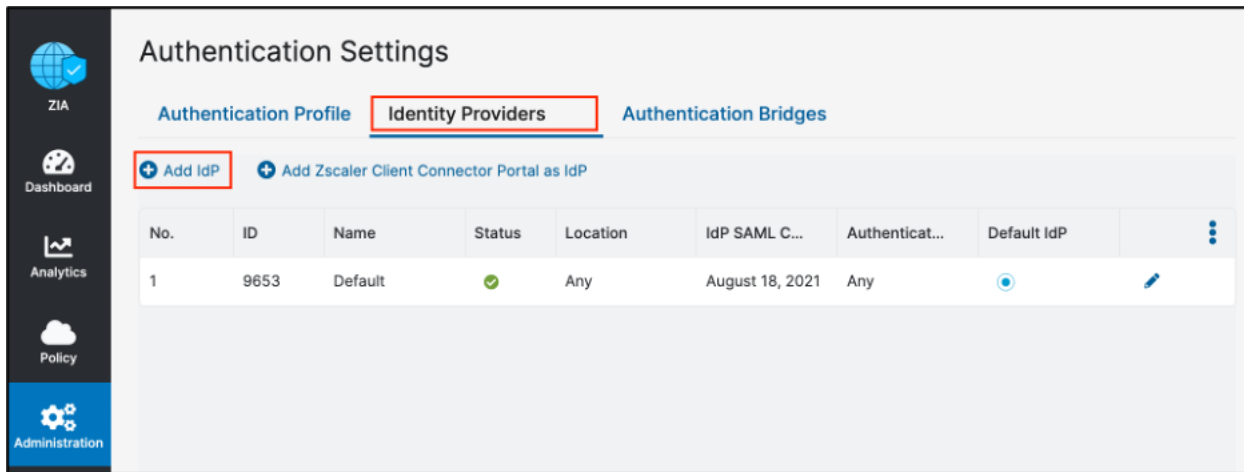


Figure 55. Adding Okta as an IdP

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

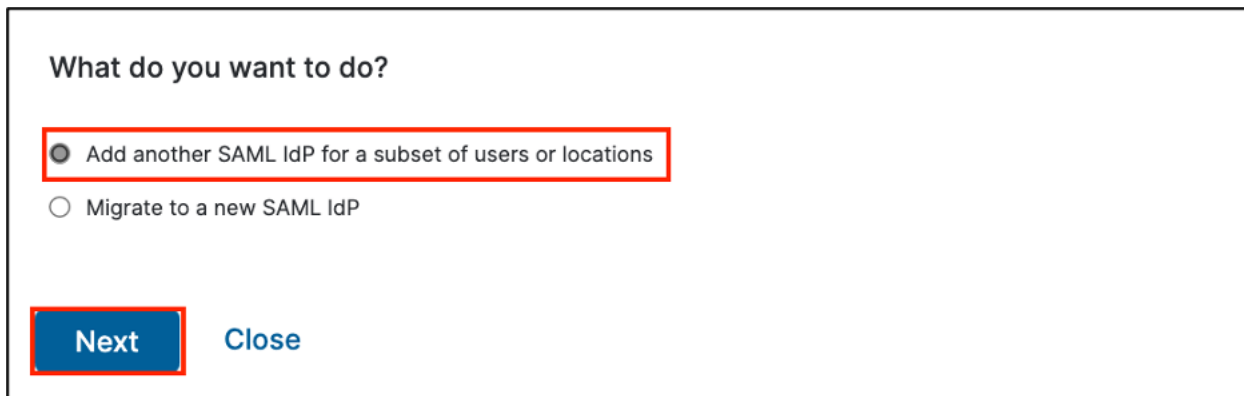


Figure 56. Add Another SAML IdP



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

**Add IdP**

**GENERAL INFO**

**Name**  
Okta

**Status**  
☒ Enabled ☐ Disabled

**SAML Portal URL**  
https://dev-606271.oktapreview.com/app/zs...

**Login Name Attribute**  
NameID

**Entity ID**  
zsccloud.net

**Org-Specific Entity ID**  
☐ Enabled ☒ Disabled

**IdP SAML Certificate**  
cert.pem [Upload](#)

**IdP SAML Certificate Expiration Date**  
April 25, 2032

**Vendor**  
Okta

**Default IdP**  
☒ Enabled

**CRITERIA**

**Locations**  
None

**Authentication Domains**  
None

**SERVICE PROVIDER (SP) OPTIONS**

**Sign SAML Request**  
☒ ☐

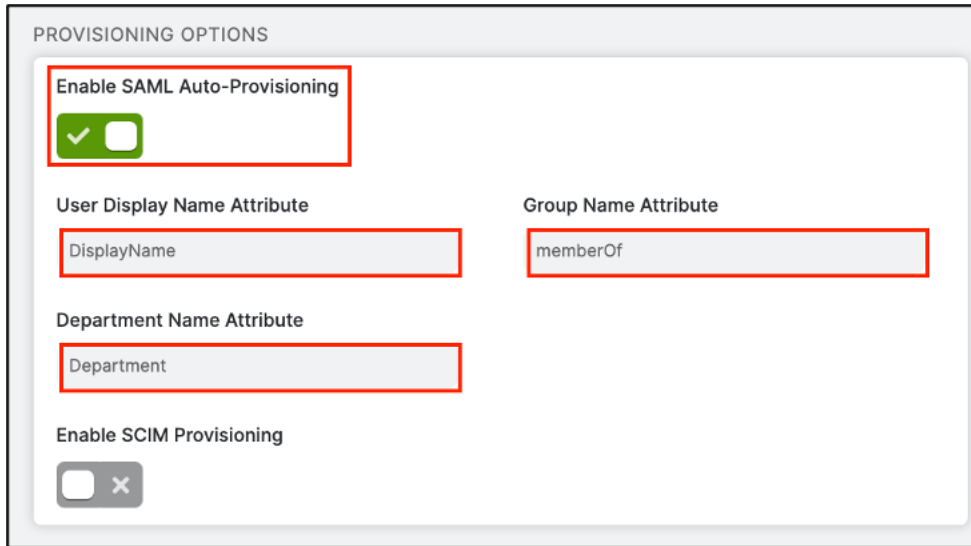
**SP Metadata**  
[Download Metadata](#)

Figure 57. The Add Identity Provider dialog

## Enable SAML Auto Provisioning

To enable SAML auto-provisioning:

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



The screenshot shows a configuration window titled "PROVISIONING OPTIONS". Inside, there is a section for "Enable SAML Auto-Provisioning" with a green checkmark icon and a toggle switch. Below this, there are three text input fields: "User Display Name Attribute" containing "DisplayName", "Group Name Attribute" containing "memberOf", and "Department Name Attribute" containing "Department". At the bottom, there is a section for "Enable SCIM Provisioning" with a grey 'x' icon and a toggle switch. Red rectangular boxes highlight the "Enable SAML Auto-Provisioning" section, the "User Display Name Attribute" field, the "Group Name Attribute" field, and the "Department Name Attribute" field.

Figure 58. Enable SAML Auto-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.

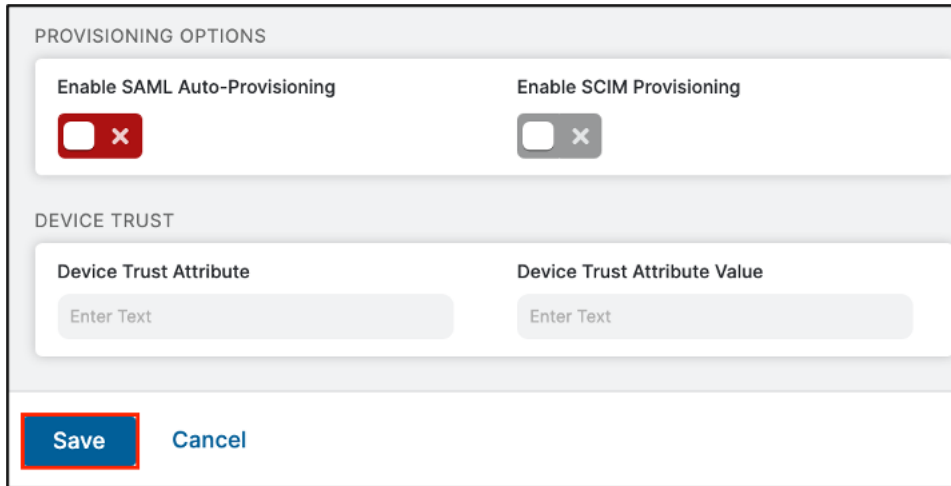
The screenshot displays the 'Authentication Settings' page in the Zscaler interface. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy, Administration (highlighted), Activation, and Search. The main content area is titled 'Authentication Settings' and features three tabs: 'Authentication Profile' (selected and highlighted with a red box), 'Identity Providers NEW', and 'Authentication Bridges'. Below the tabs, a status bar indicates 'AUTHENTICATION PROFILE UPDATED'. The configuration section includes: 'User Repository Type' with buttons for 'Hosted DB' (selected), 'Active Directory', and 'OpenLDAP'; 'Authentication Frequency' set to 'Only Once'; 'Authentication Type' with buttons for 'Form-Based', 'SAML' (selected and highlighted with a red box), and 'Open Identity Providers'; and 'Temporary Authentication' with buttons for 'Disabled' (selected) and 'One-Time Link'. A 'KERBEROS AUTHENTICATION' section shows 'Enable Kerberos' as a checked checkbox and a 'Domain Trust Password' field with 'Reveal Password' and 'Generate New Password' links. The 'FORCE REAUTHENTICATION FOR ALL USERS' section shows 'Last Reauthentication' on Wednesday, February 27, 2019, at 10:36:52 AM, a 'Force Reauthentication' 'Start' button, and a 'Reauthentication Status' of 'Completed'. At the bottom, there are 'Save' (highlighted with a red box) and 'Cancel' buttons, and a 'Help' icon in the bottom right corner.

Figure 59. Activate SAML

## Enable SCIM Provisioning

To enable SCIM:

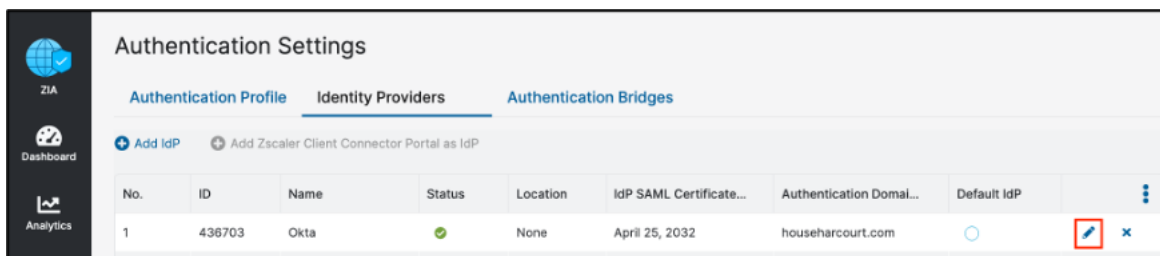
1. Return to the IdP configuration after it has been saved and activated.



The image shows a 'PROVISIONING OPTIONS' form. It contains two toggle switches: 'Enable SAML Auto-Provisioning' (disabled, red) and 'Enable SCIM Provisioning' (disabled, grey). Below these are two text input fields labeled 'Device Trust Attribute' and 'Device Trust Attribute Value', both with 'Enter Text' placeholders. At the bottom are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a red border.

Figure 60. Provisioning options

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



The image shows the 'Authentication Settings' page with the 'Identity Providers' tab selected. It features a table with one entry for 'Okta'. The 'Edit' icon (pencil) in the actions column is highlighted with a red box.



No.	ID	Name	Status	Location	IdP SAML Certificate...	Authentication Domal...	Default IdP	
1	436703	Okta	✓	None	April 25, 2032	househarcourt.com	○	 

Figure 61. 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.

The screenshot shows the 'PROVISIONING OPTIONS' dialog box. It has two main sections: 'PROVISIONING OPTIONS' and 'DEVICE TRUST'. In the 'PROVISIONING OPTIONS' section, there are two toggle switches: 'Enable SAML Auto-Provisioning' (disabled, red 'x' icon) and 'Enable SCIM Provisioning' (enabled, green checkmark icon). Below these are two text input fields: 'Base URL' containing 'https://scim.zsccloud.net/3173833/436703/scim' and 'Bearer Token' containing 'AeC/bVUm6mH1r/5eXW74iZrPJXAI+QLAgh+uXeLBvi9Sz+ii9A7sGn6k3yvRwTI7cA=='. A blue 'Generate Token' button is below the Bearer Token field. The 'DEVICE TRUST' section has two text input fields: 'Device Trust Attribute' and 'Device Trust Attribute Value', both with 'Enter Text' placeholder. At the bottom, there are two buttons: 'Save' (blue) and 'Cancel' (grey).

PROVISIONING OPTIONS

Enable SAML Auto-Provisioning ☐ x

Enable SCIM Provisioning ☒

Base URL

https://scim.zsccloud.net/3173833/436703/scim

Bearer Token

AeC/bVUm6mH1r/5eXW74iZrPJXAI+QLAgh+uXeLBvi9Sz+ii9A7sGn6k3yvRwTI7cA==

Generate Token

DEVICE TRUST

Device Trust Attribute

Enter Text

Device Trust Attribute Value

Enter Text

Save Cancel

Figure 62. Enable SCIM

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

The screenshot displays the 'Authentication Settings' page in the Zscaler interface. The left sidebar contains navigation icons for ZIA, Dashboard, Analytics, Policy, Administration (highlighted), Activation, and Search. The main content area is titled 'Authentication Settings' and has three tabs: 'Authentication Profile' (selected and highlighted with a red box), 'Identity Providers', and 'Authentication Bridges'. Below the tabs, a status bar indicates 'AUTHENTICATION PROFILE UPDATED'. The 'User Repository Type' section shows 'Hosted DB', 'Active Directory', and 'OpenLDAP' buttons. The 'Authentication Frequency' section has a dropdown menu set to 'Only Once'. The 'Authentication Type' section shows 'Form-Based', 'SAML' (selected and highlighted with a red box), and 'Open Identity Providers' buttons. The 'Temporary Authentication' section has 'Disabled' and 'One-Time Link' buttons. The 'KERBEROS AUTHENTICATION' section includes an 'Enable Kerberos' toggle (checked), a 'Domain Trust Password' field with 'Reveal Password' and 'Generate New Password' links, and a 'FORCE REAUTHENTICATION FOR ALL USERS' section with 'Last Reauthentication' details, a 'Force Reauthentication' 'Start' button, and a 'Reauthentication Status' showing 'Completed'. At the bottom, there are 'Save' (highlighted with a red box) and 'Cancel' buttons, and a 'Help' button in the bottom right corner.

Figure 63. Activate SAML

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

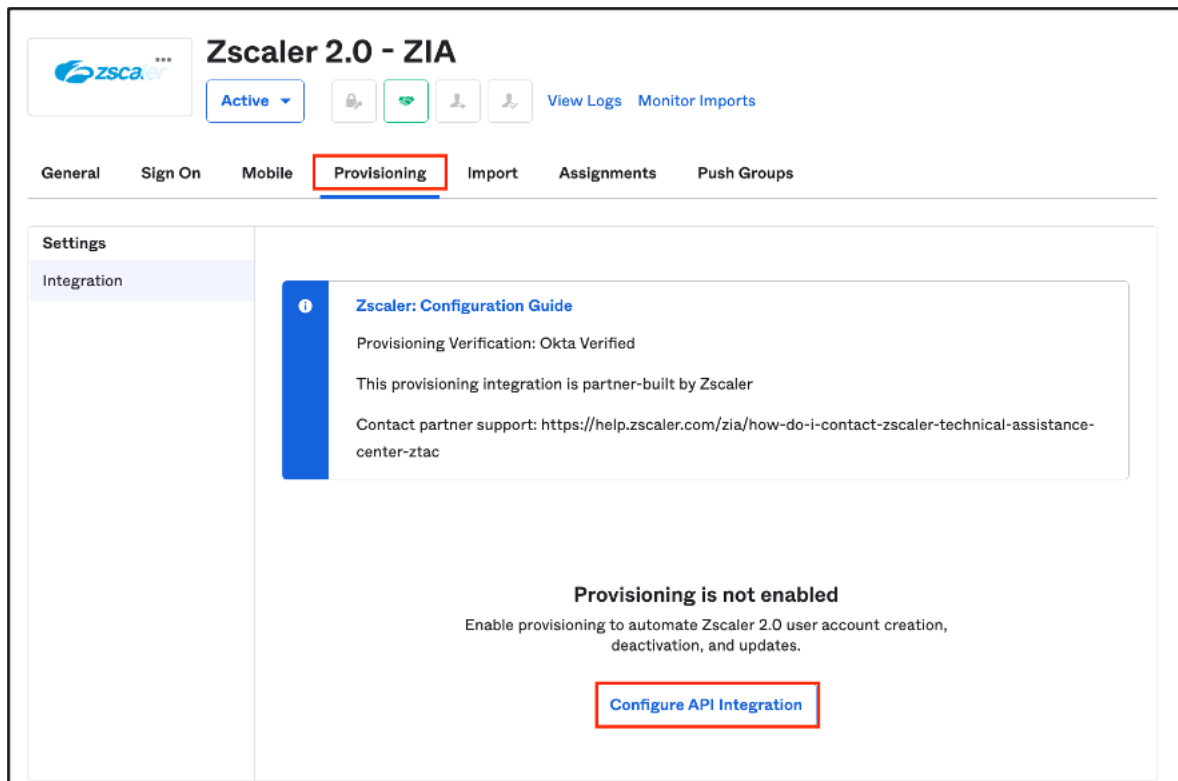


Figure 64. Enable SCIM API

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**.

**Zscaler 2.0**

Active [Status Icons] View Logs Monitor Imports

General Sign On Mobile **Provisioning** Import Assignments Push Groups

**Settings**  
Integration

**Zscaler: Configuration Guide**  
Provisioning Verification: Okta Verified  
This provisioning integration is partner-built by Zscaler  
Contact partner support: <https://help.zscaler.com/zia/how-do-i-contact-zscaler-technical-assistance-center-ztac>

Cancel

**Zscaler 2.0 was verified successfully!**

☒ **Enable API integration**

Enter your Zscaler 2.0 credentials to enable user import and provisioning features.

Zscaler ID: 3173833/436704

API Token: .....

Test API Credentials

Save

Figure 65. Okta SCIM provisioning

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



15. Select **To App** under **Settings** in the left-side navigation.
16. Select **Edit**.

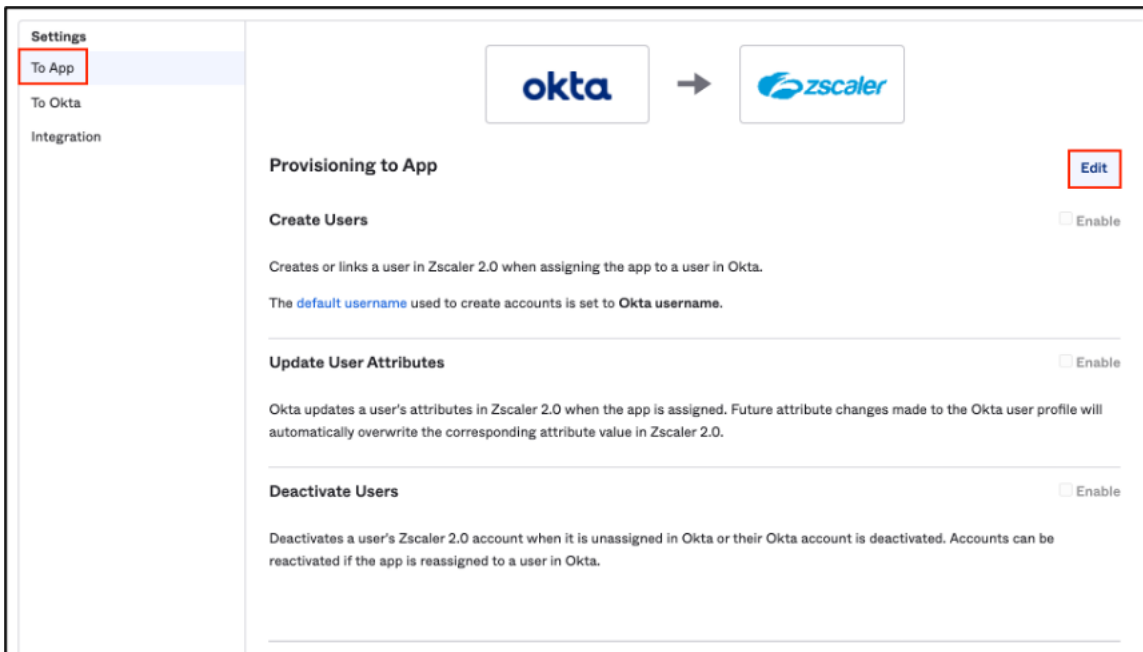


Figure 66. Okta SCIM synchronization settings

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

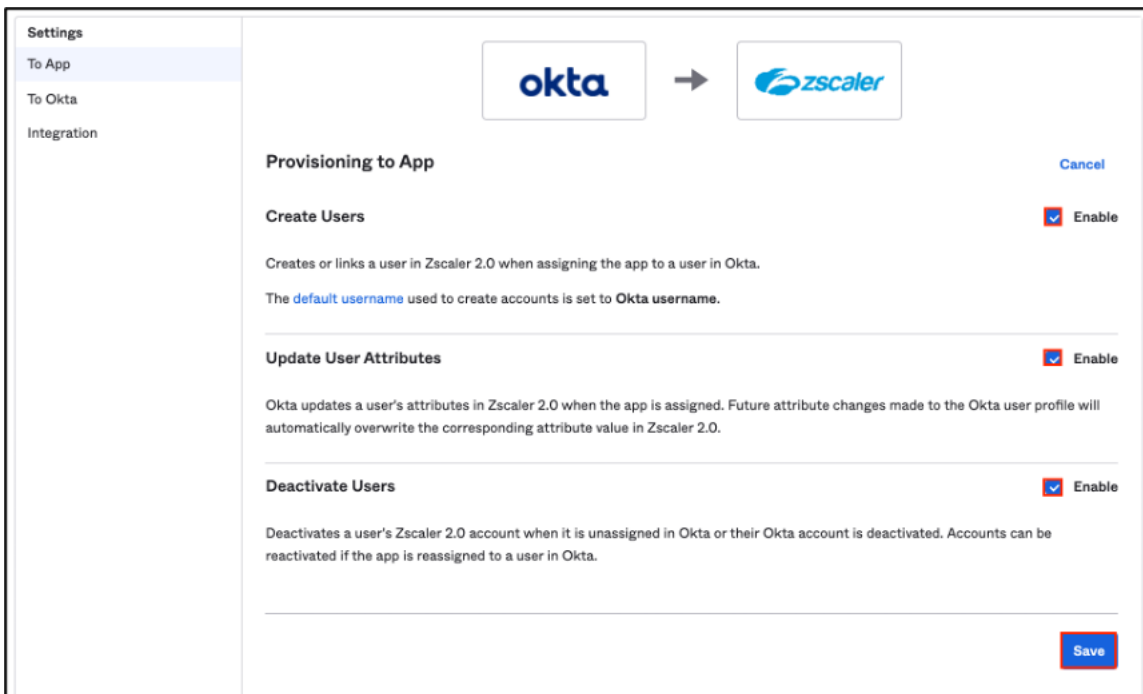


Figure 67. Okta SCIM synchronization settings

## Assign ZIA to Users or Groups

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

1. Select **Assignments**.
2. Select **People** or **Groups**.
3. Select **Assign**. In the example, the **Everyone** group is selected (all users in the company can authenticate).

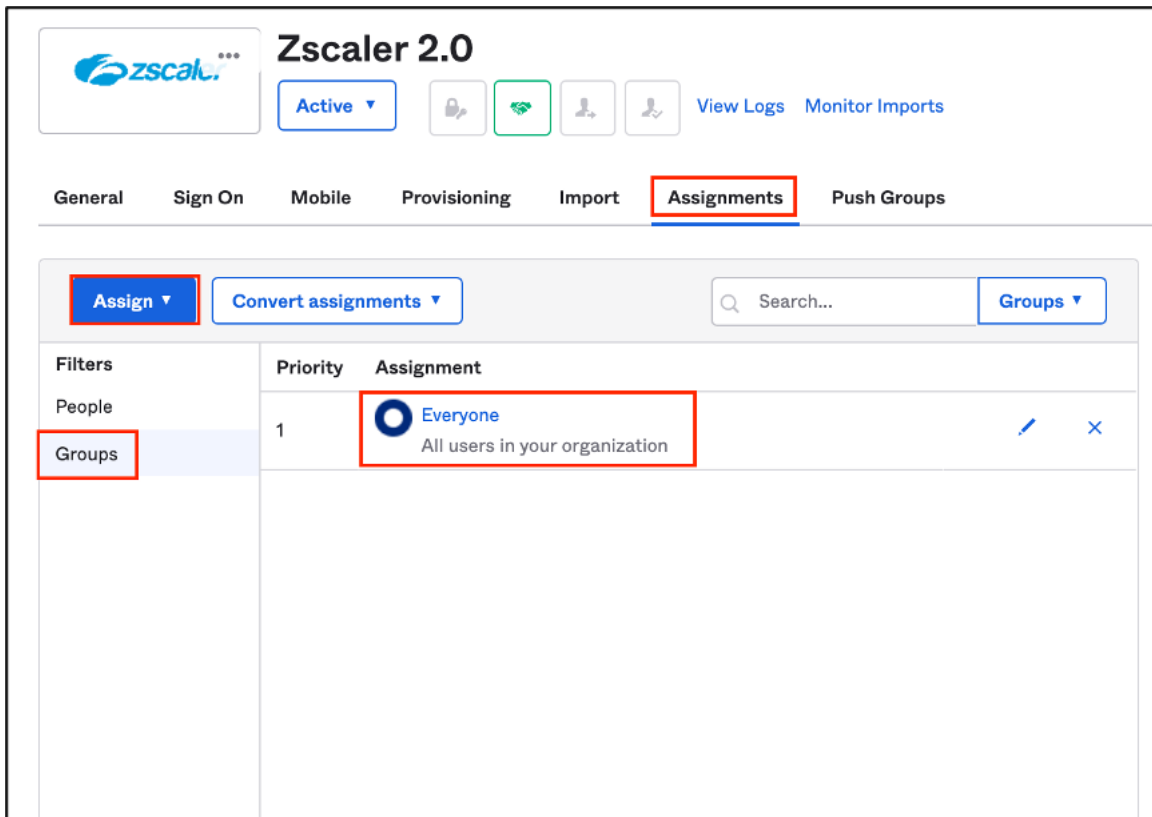


Figure 68. Assigning the ZIA application

## 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.

The screenshot shows the 'Push Groups to Zscaler 2.0' configuration page. The 'Push Groups' tab is active. On the left, the 'Pushed Groups' sidebar has 'By name' selected. The main area has a search box containing 'ZPA-2'. Below the search box, the 'Push group memberships immediately' checkbox is checked. The 'Match result & push action' section shows 'No Match found' with a '+ Create Group' button. At the bottom right, the 'Save & Add Another' button is highlighted.

Figure 69. Enable security groups to sync

# Configure Okta and ZPA: SAML and SCIM

Configure SAML and SCIM for Okta and ZPA integration.

## Add the Zscaler ZPA Application to Okta

Add the Zscaler applications by Okta used for authentication and provisioning to ZPA. From the Okta administrator console:

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

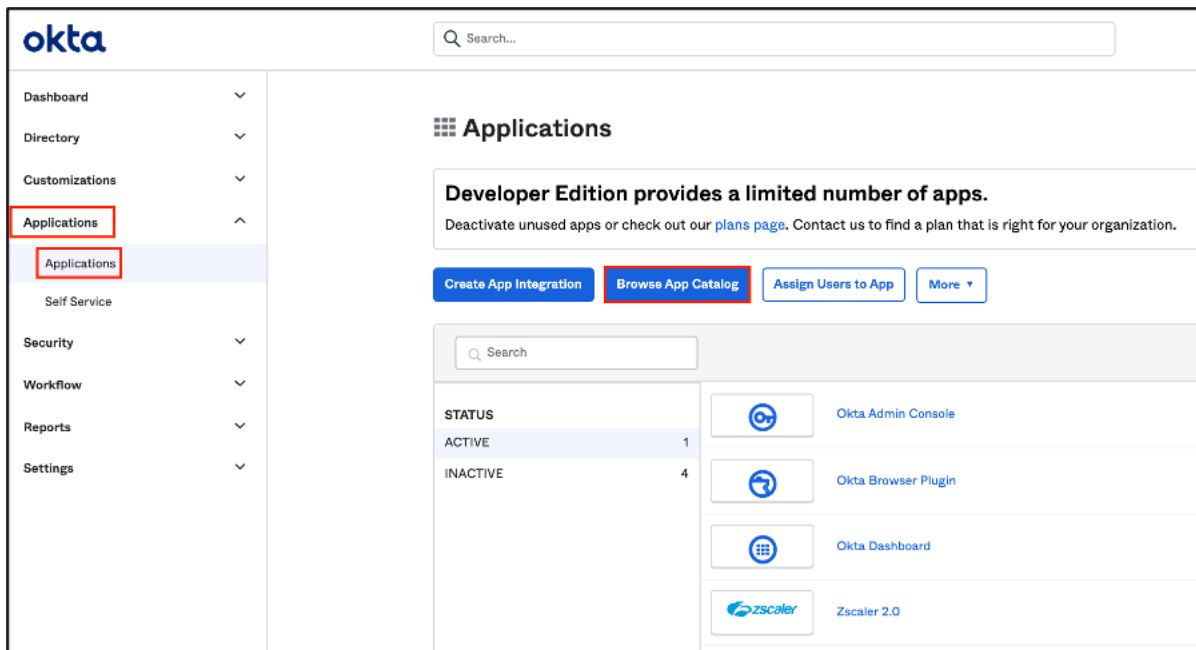


Figure 70. Adding an application

4. Search for `zscaler`.
5. Select **Zscaler Private Access 2.0**.

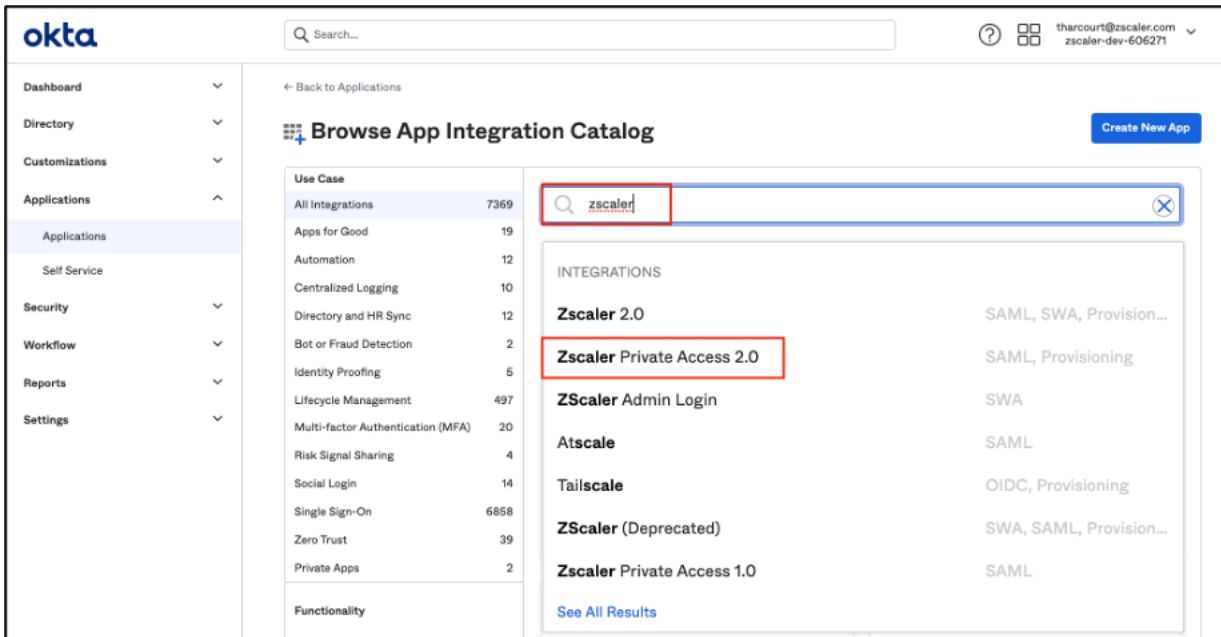


Figure 71. Adding the Zscaler ZPA application

6. On the **Overview** page, click **Add**.

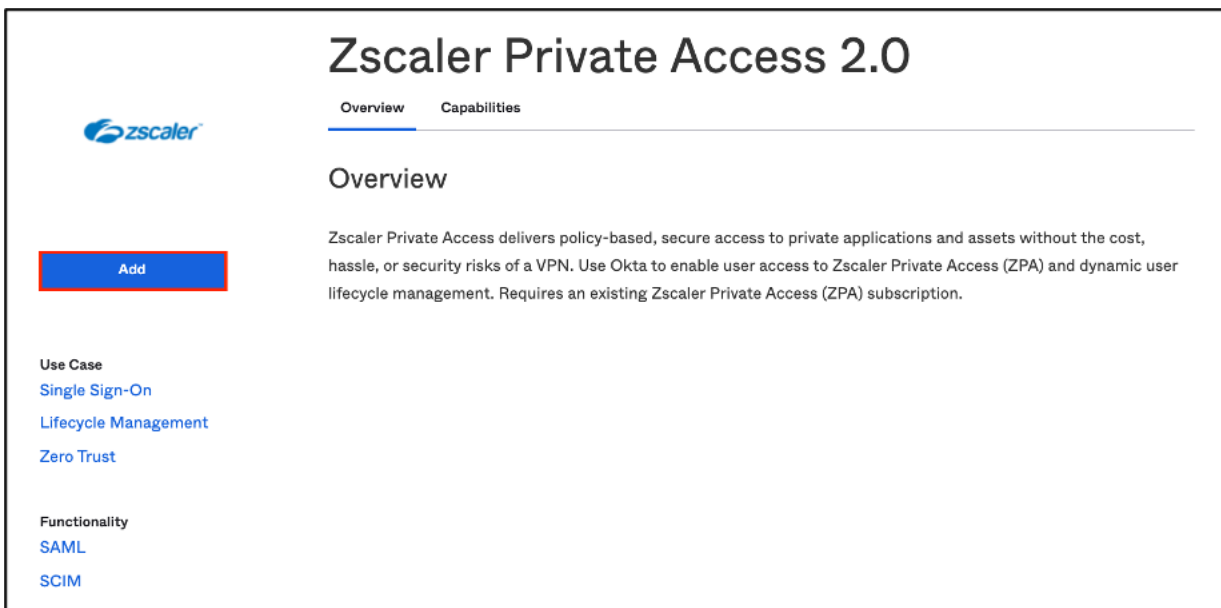


Figure 72. ZPA application display settings

7. Enter an application name (or keep the default).
8. Select **Do not display application icon to users**.
9. Select **Do not display application icon in the Okta Mobile App**.
10. Click **Done**.

**Add Zscaler Private Access 2.0**

1 General Settings

**General settings Required**

Application label: Zscaler Private Access 2.0  
This label displays under the app on your home page

Application Visibility:  
☒ Do not display application icon to users  
☒ Do not display application icon in the Okta Mobile App

Cancel Done

**General settings**  
All fields are required to add this application unless marked optional.

Figure 73. ZPA application display settings

## Configure Okta for ZPA: SAML and SCIM

1. Select the **Sign On** tab.
2. Select **View SAML setup instructions** on the bottom right.

**Zscaler Private Access 2.0**

Active View Logs Monitor Imports

General **Sign On** Mobile Provisioning Import Assignments Push Groups

### Settings

**Sign on methods**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ SAML 2.0

Default Relay State

Disable Force Authentication ☒

GroupName None

### Advanced Sign-on Settings

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL

Service Provider Entity ID

### Credentials Details

Application username format Okta username

Update application username on Create and update [Update Now](#)

Password reveal ☒ Allow users to securely see their password (Recommended)

### SAML Signing Certificates

[Generate new certificate](#)

Type	Created	Expires	Status	Actions
SHA-2	Today	Apr 2032	Active	<a href="#">Actions</a>

### About

**SAML 2.0** streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3<sup>rd</sup> party application may be required to complete the integration with Okta.

### Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

### SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

Figure 74. Okta SAML setup

- Copy the Identity Provider metadata to an XML file. This file is used when setting up ZPA.
- Close the window and open the ZPA Admin Portal.

## Before you Begin

The Zscaler Private Access OIN application supports two configuration types:

- For Administrators
- For Users

In order to add administrator/user configurations, you need to add a separate Zscaler Private Access application instance in Okta and create a separate IDP Configuration in Zscaler.

The Okta metadata file is different for each application instance in Okta, so it will be different for both configurations. Save the following metadata file and add a required prefix (admin or user), so the file name will be: `metadata_admin.xml` (for administrator configuration) or `metadata_user.xml` (for user configuration):

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://www.okta.com/exk17ax4kk1bAmloJ0h8"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="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>MIIDpDCCAoygAwIBAgIGAYBnLUWKMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
          A1UECAwKQ2FsaWZvcms5pyTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
```

Figure 75. Okta ZPA application metadata

## Configure ZPA for Okta: SAML and SCIM

Log in to the ZPA Admin Portal with administrator credentials.

- Go to **Authentication > User Authentication > IdP Configuration**.

The screenshot shows the Zscaler Private Access Admin Portal interface. On the left is a dark blue sidebar with the Zscaler logo and a search bar. Below the search bar are menu items: Dashboard, Analytics, Authentication, User Authentication, Device authentication, Resource Management, and Policy. The 'Authentication' menu is expanded, showing 'User Authentication' and 'Device authentication'. 'User Authentication' is further expanded, showing 'IdP Configuration', 'Settings', 'SAML MANAGEMENT', and 'SAML Attributes'. The 'IdP Configuration' option is highlighted with a red box. The main content area has tabs for Applications, Users, Health, App Connectors, Security, and Sources. Under the 'Applications' tab, there are two sections: 'Recent Applications Accessed' and 'Discovered Applications', both showing a count of 0. A red box highlights the 'IdP Configuration' option in the sidebar.

Figure 76. Creating the Okta IdP on ZPA



- On the **IdP Configuration** tab, select the **Add** icon to add the IdP configuration.

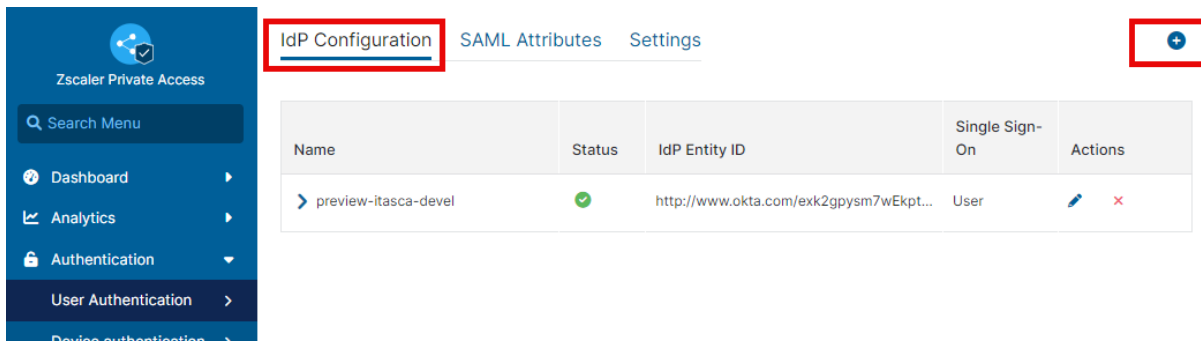


Figure 77. Add a new IdP

- In the **Add IdP Configuration** window, enter a **Name** for the IdP.
- Select the **Domains** for this IdP.
- Click **Next**.

**Add IdP Configuration** [X]

1 IdP Information   2 SP Metadata   3 Create IdP

Name  
Okta

Single Sign-On  
Admin ☒ User

User SP Certificate Rotation  
ZPA User SSO Service Provider Certificate - Jan 18 03:14:07 2038 GMT

Domains  
househarcourt.com

Next Cancel

Figure 78. IdP information

6. Copy and save the **Service Provider URL** and the **Service Provider Entity ID URL**.
7. Select **Next**.

**Add IdP Configuration** [X]

1 IdP Information 2 **SP Metadata** 3 Create IdP

Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

**Service Provider Metadata**  
Download Metadata

**Service Provider Certificate**  
Download Certificate

**Service Provider URL**  
https://samlsp.private.zscaler.com/auth/144121552143647691/sso

**Service Provider Entity ID**  
https://samlsp.private.zscaler.com/auth/metadata/144121552143647691

**Next** Pause

Figure 79. SP Metadata

8. In the **Add IdP Configuration** window, click **Select File** to upload the **IdP Metadata File**, and select the Okta metadata file. This loads the certificate and the Okta URL information.

**Add IdP Configuration** [X]

1 IdP Information 2 SP Metadata 3 **Create IdP**

Name  
Okta

Authentication Domains  
househarcourt.com

SAML CONFIGURATION

**IdP Metadata File**  
Upload Metadata File [Select File]

**IdP Certificate**  
Upload the Certificate File... [Select File]

Single Sign-On URL

IdP Entity ID

Figure 80. Add IdP configuration

9. Select **Signed** for the **ZPA (SP) SAML Request**.
10. Select **Enabled** for the **HTTP-Redirect**.
11. Leave the **Single Sign-On** setting at **User**.
12. Select **Enabled** for **SCIM Sync**.
13. Select **Enabled** for **SCIM Attributes for Policy**.
14. Click **Generate New Token**.
15. Save the URLs of the **SCIM Service Provider Endpoint** and the **Bearer Token** for the Okta configuration.
16. Click **Save**.

**Add IdP Configuration**

1 IdP Information 2 SP Metadata 3 Create IdP

Name  
Okta

Authentication Domains  
househarcourt.com

SAML CONFIGURATION

IdP Metadata File  
metadata\_a\_user.xml Change Remove

IdP Certificate  
Upload the Certificate File Select File  
-----BEGIN CERTIFICATE-----  
MIIDpQCCAoygAwIBAgIGAYBnLUWKMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQGEwJVUzETMBEGATUECAwKQ2FsaWZvcms5PjTEWMBQGA1UEBwwwNUZFuEZYyYW5jaXNjbzENMAsgATUECgwET210Y  
TEU

Single Sign-On URL  
https://dev-606271.oktapreview.com/app/zscaler\_private\_access/exk17ax4kk1bAmIoJ0h8/sso/saml

IdP Entity ID  
http://www.okta.com/exk17ax4kk1bAmIoJ0h8

Status Enabled Disabled ZPA (SP) SAML Request Signed Unsigned

HTTP-Redirect Enabled Disabled Single Sign-On Admin User Both

User SP Certificate Rotation  
ZPA User SSO Service Provider Certificate - Jan 18 03:14:07 2038 GMT

SAML Attributes for Policy Enabled Disabled

SCIM CONFIGURATION

SCIM Sync Enabled Disabled SCIM Attributes for Policy Enabled Disabled

SCIM Service Provider Endpoint  
https://scim1.private.zscaler.com/scim/1/144121552343847692/v2

Bearer Token  
This client secret will not display again. Copy it to your clipboard before exiting.  
DFngBttuOkkT0izVh4Nvz2QCFn9-HdxgFTMQ36k4547UseFDV7ZjxW50mmq-GsxxZ7rXyzsdGhGPQ0WWYQ

Generate New Token

Save Pause

Figure 81. IdP configuraiton options

17. Return to the Okta configuration, then select the **Sign On** tab.
18. Select **Edit**.

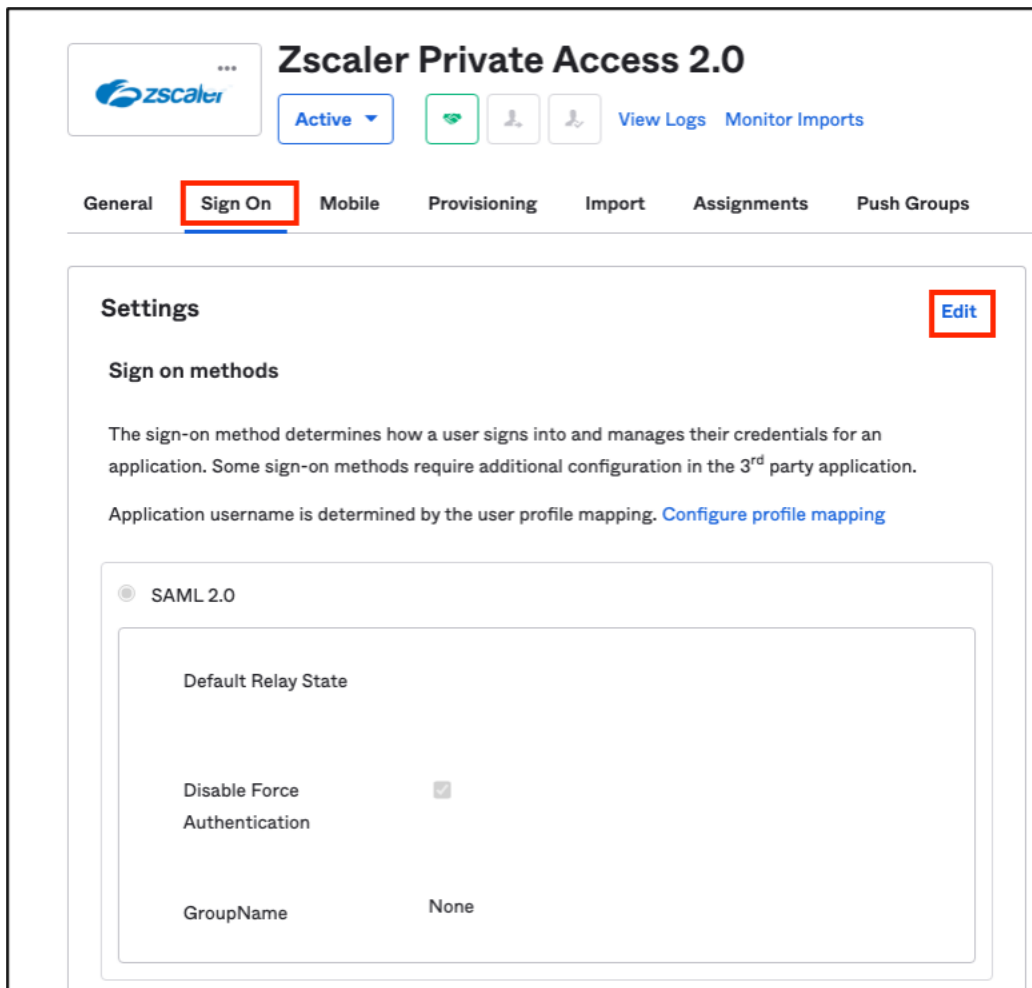


Figure 82. Editing the Okta sign-on configuration

19. In **GroupName**, select **Matches regex** and enter **. \*** (period, asterisk) for the GroupName.
20. Enter the **Service Provider URL** and the **Service Provider Entity ID** from the ZPA IdP setup.
21. Click **Save**.

**Zscaler Private Access 2.0**

Active View Logs Monitor Imports

General **Sign On** Mobile Provisioning Import Assignments Push Groups

### Settings

**Sign on methods**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0 is the only sign-on option currently supported for this application.

**SAML 2.0**

Default Relay State: All IDP-initiated requests will include this RelayState.

Disable Force Authentication: ☒ Never prompt user to re-authenticate.

GroupName: **Matches regex** **. \***

### Advanced Sign-on Settings

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL: **https://samlsp.private.zscaler.com/auth/1441215521436**  
Please enter your Service Provider URL. Refer to the Setup Instructions above to obtain this value.

Service Provider Entity ID: **https://samlsp.private.zscaler.com/auth/metadata/1441**  
Please enter your Service Provider Entity ID. Refer to the Setup Instructions above to obtain this value.

### Credentials Details

Application username format: **Okta username**

Update application username on: **Create and update**

Password reveal: ☐ Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

**Save**

**About**

**SAML 2.0** streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3<sup>rd</sup> party application may be required to complete the integration with Okta.

**Application Username**

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Figure 83. Okta sign-on configuration detail

## Assign ZPA to Authenticating Users

1. Select the **Assignments** tab.
2. Select **People** or **Groups** to assign ZPA as an application in the organization.
3. Click **Assign**. In the following example, the **Everyone** group is selected (all users in the company can authenticate).

The screenshot shows the Zscaler Private Access 2.0 interface. At the top, there's a header with the Zscaler logo, an 'Active' status button, and icons for monitoring. Below this is a navigation bar with tabs: General, Sign On, Mobile, Provisioning, Import, **Assignments** (highlighted with a red box), and Push Groups. The main content area has a sub-header with an 'Assign' button (highlighted with a red box), a 'Convert assignments' dropdown, a search bar, and a 'Groups' dropdown. On the left, there's a 'Filters' sidebar with 'People' and 'Groups' options. The main table has columns for 'Priority' and 'Assignment'. A single row is visible, with '1' in the Priority column and 'Everyone' in the Assignment column. The 'Everyone' group is highlighted with a red box, and its description 'All users in your organization' is visible below it. There are also edit and delete icons for this entry.

Priority	Assignment
1	<b>Everyone</b> All users in your organization

Figure 84. Assigning the ZPA application

## Configure Okta SCIM for ZPA

To configure SCIM provisioning:

1. Select the **Provisioning** tab.
2. Select **Configure API Integration**.

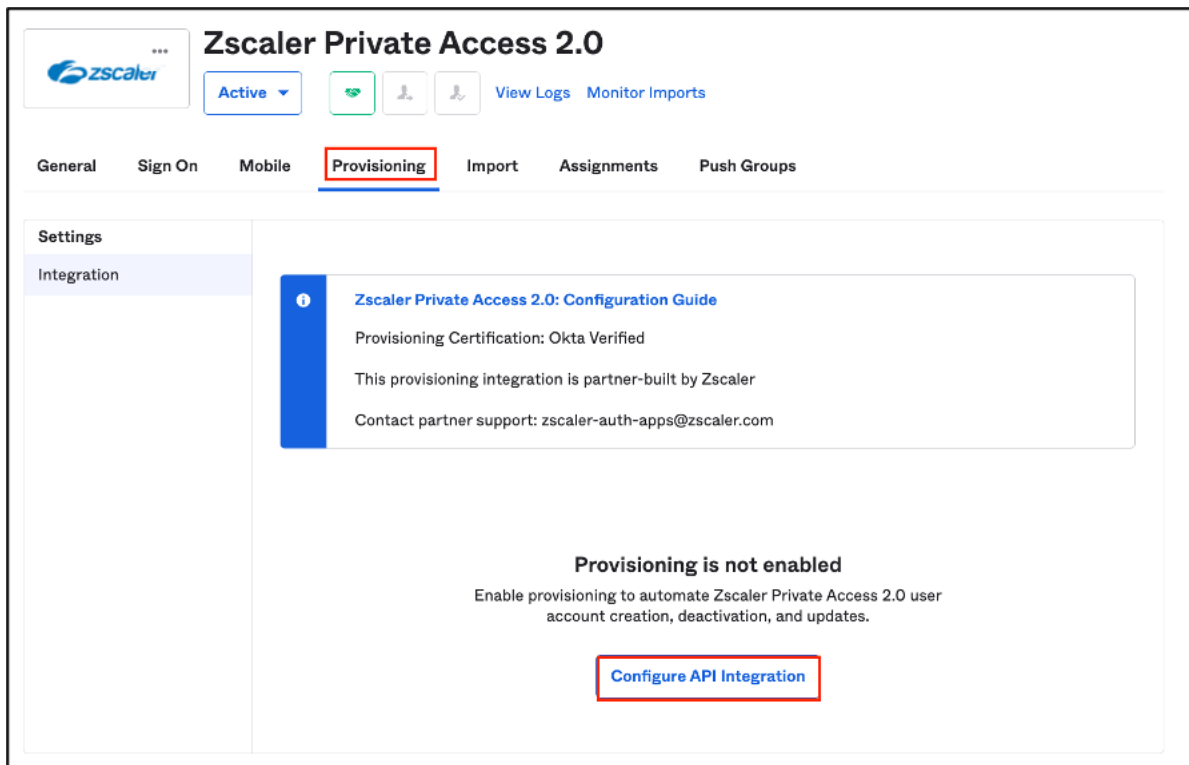


Figure 85. Okta provisioning

3. Select **Enable API Integration**.
4. Enter the **SCIM Service Provider Endpoint URL** and the **Bearer Token** saved from ZPA.
5. Select **Test API Credentials** to verify your credentials. If the credentials are valid and Okta can communicate with the ZPA cloud, you see the response highlighted in red. If you receive an error, re-copy the URL and token, possibly generate a new **Bearer Token**, or save the ZPA configuration.
6. After you have verified your credentials, click **Save**.

The screenshot shows the Zscaler Private Access 2.0 interface. At the top, there's a header with the Zscaler logo, a status 'Active' dropdown, and icons for provisioning. Below the header is a navigation bar with tabs: General, Sign On, Mobile, Provisioning (highlighted with a red box), Import, Assignments, and Push Groups. The main content area is titled 'Settings' and 'Integration'. It features an information box about the Zscaler Private Access 2.0 Configuration Guide, stating that provisioning certification is Okta Verified and providing contact information for partner support. Below this, the 'Enable API integration' checkbox is checked and highlighted with a red box. A text prompt asks the user to enter their Zscaler Private Access 2.0 credentials. The 'Base URL' field contains 'https://scim1.private.zscaler.com/scim/1/144121552143647692/v' and is highlighted with a red box. The 'API Token' field contains a masked token '.....' and is also highlighted with a red box. A 'Test API Credentials' button is highlighted with a red box. At the bottom right, there is a 'Save' button highlighted with a red box.

Figure 86. SCIM integration API setup



7. Select **To App**.
8. Select **Edit**.

The screenshot shows the Zscaler Private Access 2.0 interface. At the top, there's a header with the Zscaler logo, a menu icon, and the title "Zscaler Private Access 2.0". Below the title, there's a status bar with "Active", a green checkmark icon, a user icon, and a group icon, followed by links for "View Logs" and "Monitor Imports". A navigation bar contains tabs: "General", "Sign On", "Mobile", "Provisioning" (highlighted with a red box), "Import", "Assignments", and "Push Groups". On the left, a "Settings" sidebar has "To App" (highlighted with a red box), "To Okta", and "Integration". The main content area is titled "Provisioning to App" and features a diagram showing "Okta" pointing to "Zscaler". Below this, there are three sections: "Create Users" with an "Enable" checkbox, "Update User Attributes" with an "Enable" checkbox, and "Deactivate Users" with an "Enable" checkbox. Each section has a brief description of its function. An "Edit" button (highlighted with a red box) is located in the top right corner of the main content area.

**Zscaler Private Access 2.0**

Active View Logs Monitor Imports

General Sign On Mobile **Provisioning** Import Assignments Push Groups

**Settings**

**To App**

To Okta

Integration

**Provisioning to App** Edit

**Create Users** Enable

Creates or links a user in Zscaler Private Access 2.0 when assigning the app to a user in Okta.

The default username used to create accounts is set to Okta username.

**Update User Attributes** Enable

Okta updates a user's attributes in Zscaler Private Access 2.0 when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Zscaler Private Access 2.0.

**Deactivate Users** Enable

Deactivates a user's Zscaler Private Access 2.0 account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

Figure 87. Selecting provisioning events

9. Select **Enable** for **Create Users**, **Update User Attributes**, and **Deactivate Users**.
10. Click **Save**.

**Zscaler Private Access 2.0**

Active View Logs Monitor Imports

General Sign On Mobile **Provisioning** Import Assignments Push Groups

**Settings**

- To App
- To Okta
- Integration

**Provisioning to App** Cancel

**Create Users** ☒ Enable

Creates or links a user in Zscaler Private Access 2.0 when assigning the app to a user in Okta.

The [default username](#) used to create accounts is set to **Okta username**.

**Update User Attributes** ☒ Enable

Okta updates a user's attributes in Zscaler Private Access 2.0 when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Zscaler Private Access 2.0.

**Deactivate Users** ☒ Enable

Deactivates a user's Zscaler Private Access 2.0 account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

**Save**

Figure 88. Provisioning events enabled

## Configure Which Groups to Push Using SCIM

To select which groups SCIM pushes to ZPA automatically:

1. Select the **Push Groups** tab.
2. Search and add the desired groups.
3. Click **Save & Add Another** or **Save**.

**Zscaler Private Access 2.0**

Active View Logs Monitor Imports

General Sign On Mobile Provisioning Import Assignments **Push Groups**

### Push Groups to Zscaler Private Access 2.0

Close

**Pushed Groups**

All

Errors

**By name**

By rule

**Push groups by name**

To sync group memberships from Okta to Zscaler Private Access 2.0, choose a group in Okta and a group in the app.

ZPA-2

☐ Push group memberships immediately

Group	Match result & push action
ZPA-2	No Match found <a href="#">Create Group</a>
	ZPA-2

Save **Save & Add Another**

Figure 89. Push groups

## Test the ZPA Authentication Configuration

To import the SAML variables from Okta. In the ZPA Admin Portal:

1. Select **User Authentication**.
2. Select **IdP Configuration**.
3. Select the **Expand** icon to the left of your IdP name.
4. Select **Import** next to your domain under **Import SAML Attributes**. When selected, it authenticates to Okta using your existing user if you are authenticated. If you aren't authenticated, it opens the **Okta Login** window. The SAML variables and the SAML assertion are displayed. You might need to use an incognito window to complete this task.

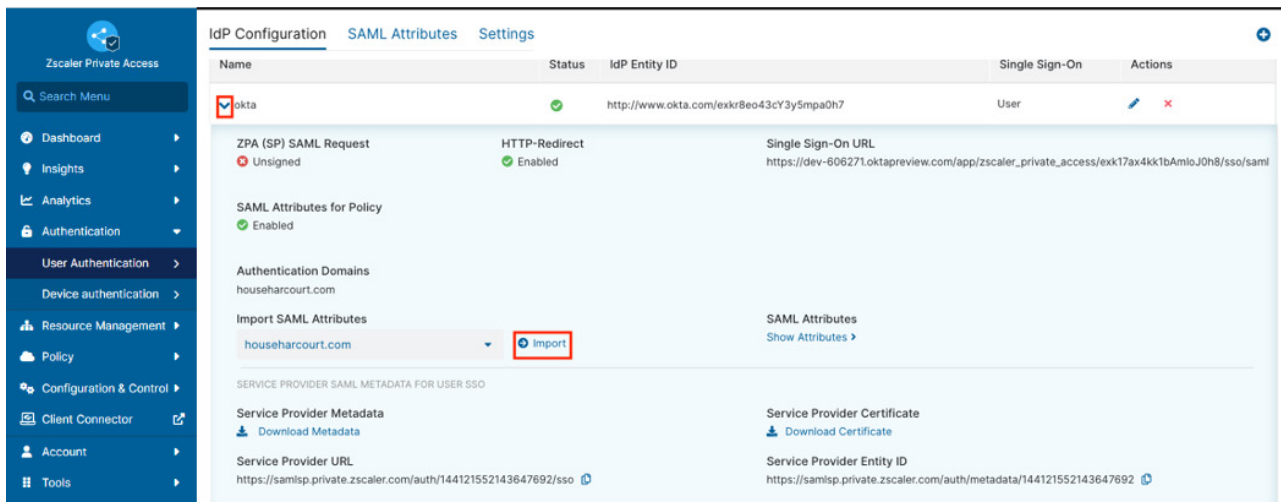


Figure 90. SAML variable import

5. Review your mappings.
6. Click **Save**.

**Import SAML Attributes**

Name	SAML Attribute Name
FirstName_Okta	FirstName
LastName_Okta	LastName
Email_Okta	Email
DepartmentName_Okta	DepartmentName
GroupName_Okta	GroupName

**Save** **Cancel**

**Import SAML JSON**

```
{
  "nameid": "tharcourt@zscaler.com",
  "orgId": "144121552143646720",
  "idpEntityID": "http://www.okta.com/exk17b2wjxvdy5kJ0n8",
  "idpid": "144121552143647707",
  "samlAttributes": {
    "FirstName": "Todd",
    "LastName": "Harcourt",
    "Email": "tharcourt@zscaler.com",
    "DepartmentName": ""
  }
}
```

Figure 91. SAML Assertion and SAML Attributes

You can also test by using the Test URL.

In the URL show, replace `testmypacket.com` with your domain. Your SAML Assertion is returned if you are already an authenticated user. Otherwise, you are prompted to authenticate. After you are authenticated, your SAML assertion is displayed.

### SAML Assertion:

```
{
  "nameid": "toddh@househarcourt.com",
  "orgId": null,
  "idpEntityID": null,
  "idpid": null,
  "saml_attributes": {
    "FirstName": "Todd",
    "LastName": "Harcourt",
    "Email": "toddh@househarcourt.com",
    "DepartmentName": null,
    "GroupName": ["Group1", "Every-one", "Group3"]
  },
  "samlassertion": null
}
```

## Using Okta for ZIA Admin Access

To use Okta SAML authentication for ZIA admin users, install the **SAML Service Provider** application.

### Add the Okta SAML Application

From the Okta administrator console:

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

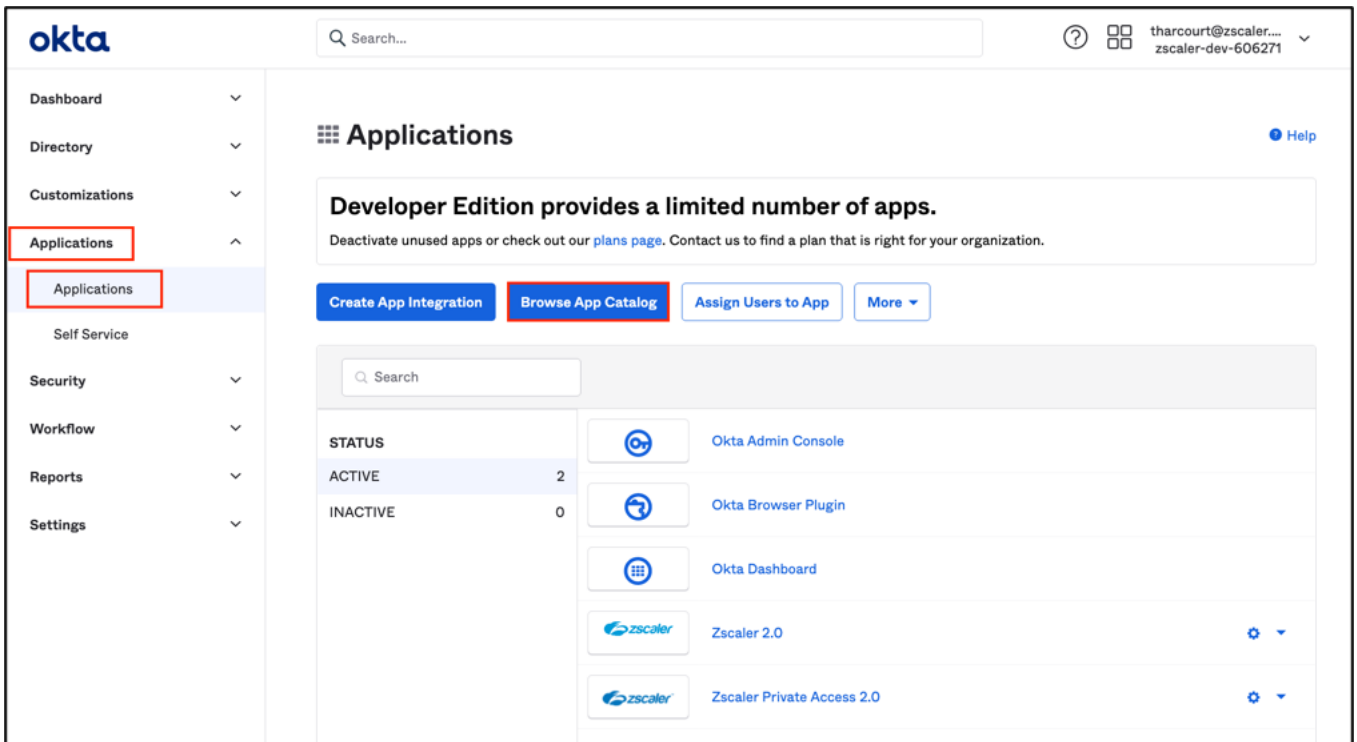


Figure 92. Adding the Okta SAML application for ZIA admin authentication

## Okta SAML Service Provider Application

1. Search for `saml`.
2. Add the **SAML Service Provider** application.

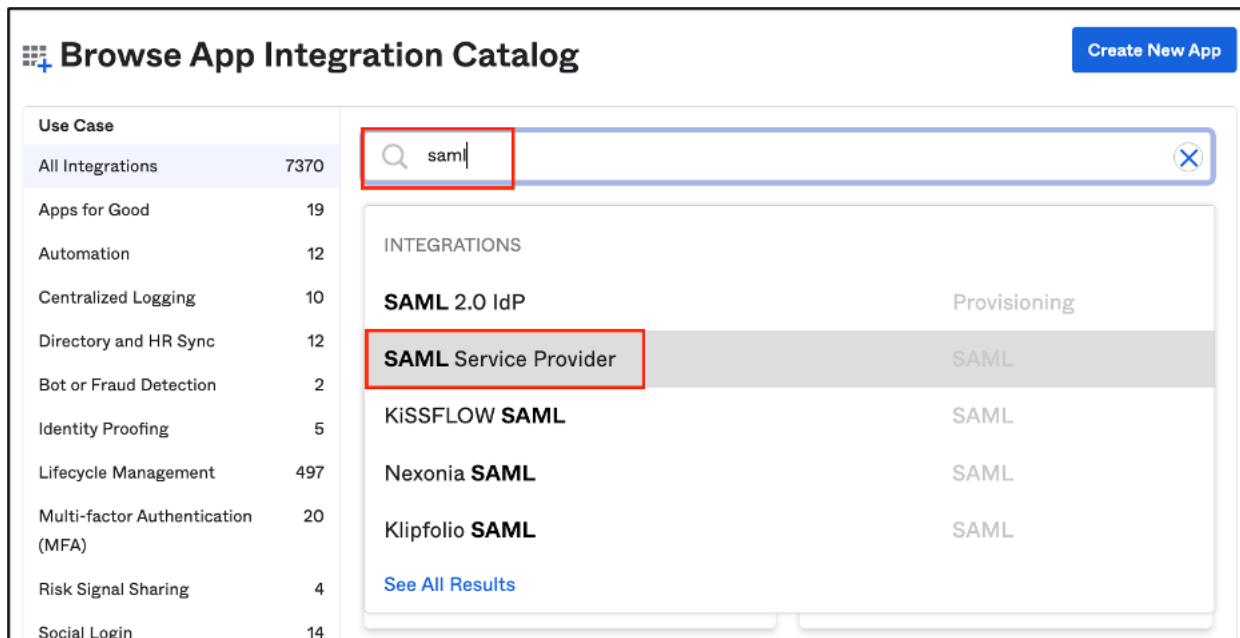
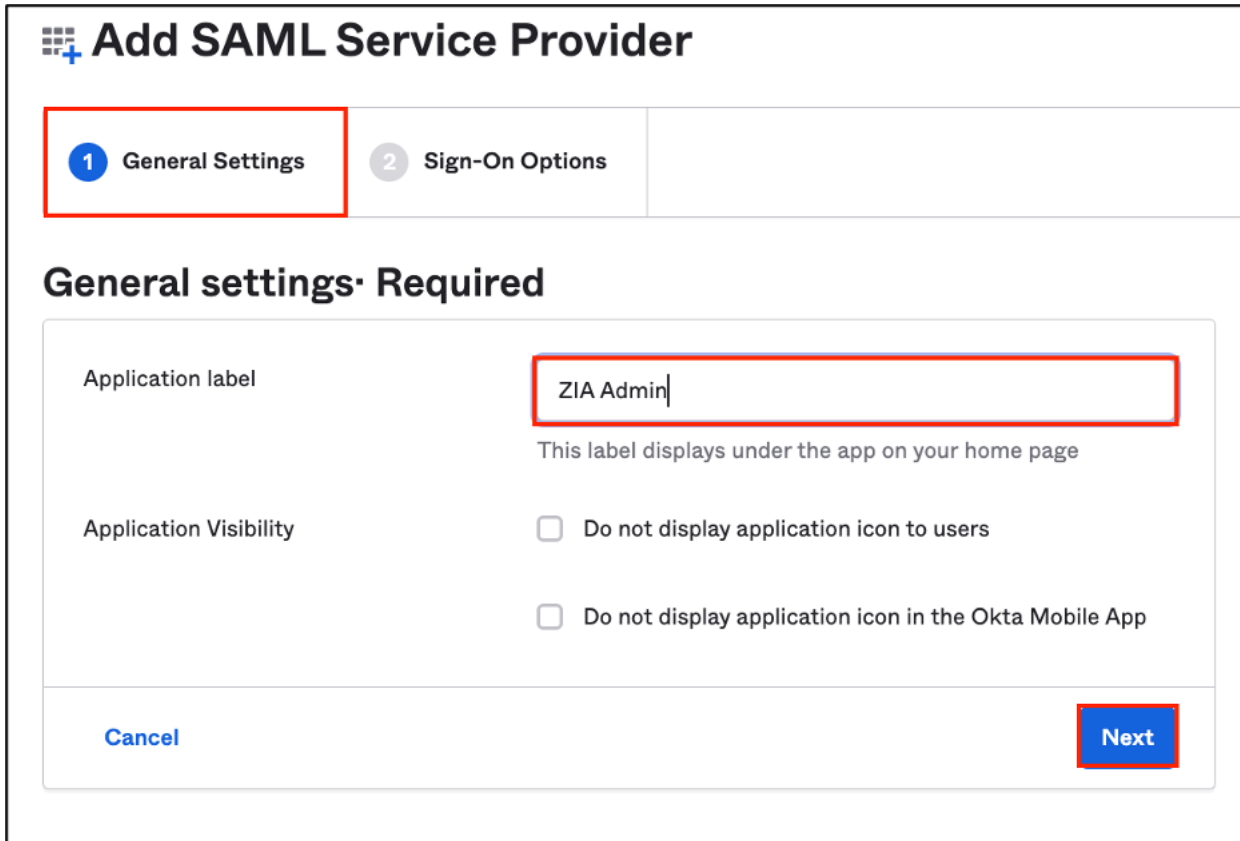


Figure 93. The Okta SAML Service Provider application

## Configure the Application

1. Enter a name as the **Application label**.
2. Click **Next**.



### Add SAML Service Provider

**1 General Settings** 2 Sign-On Options

#### General settings- Required

Application label

ZIA Admin

This label displays under the app on your home page

Application Visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile App

Cancel

Next

Figure 94. General settings



3. Select **View Setup Instructions**.

## Add SAML Service Provider

1 General Settings

2 Sign-On Options

### Sign-On Options Required

#### Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application.


Application username is determined by the user profile mapping. [Configure profile mapping](#)

☐ Bookmark-only

☒ SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState.



**SAML 2.0** is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Figure 95. Sign-on options

## Save the Certificate

This displays a window to download the **Identity Provider Certificate**:

1. Save the link to a file and rename the file to `okta.pem`. This file is imported into the Zscaler setup.
2. Close the window.

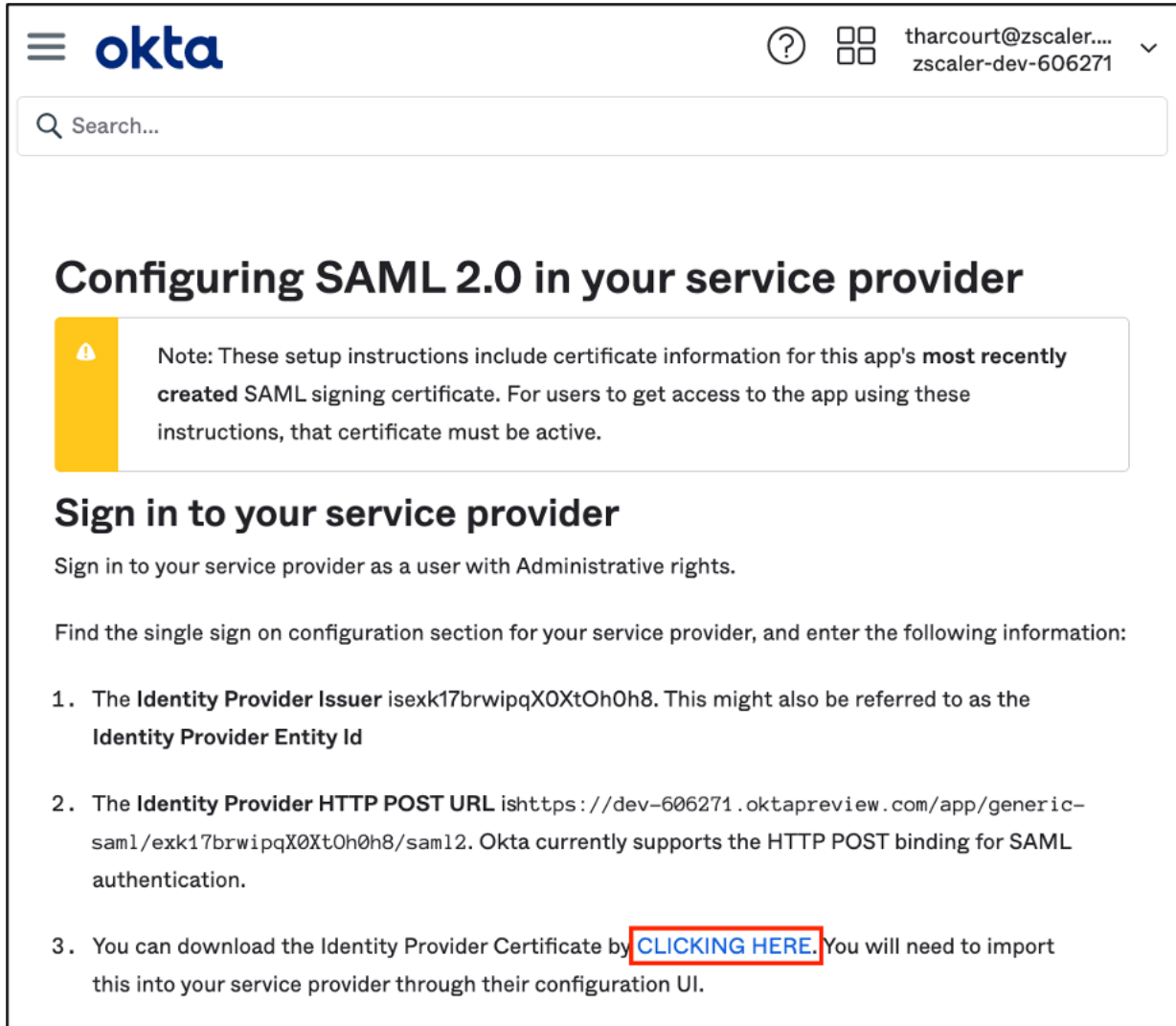


Figure 96. Save the Okta Cert

3. Enter the **Assertion Consumer Service URL** and the **Service Provider Entity Id**.

The current Zscaler clouds include: zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, zscaler.beta.net, or zsccloud.net. For example, if your cloud domain is zcloud.net:

- The Service URL is `https://admin.zsccloud.net/adminsso.do`.
- The Entity Id is `admin.zsccloud.net`.

4. Click **Done**.

The screenshot displays the 'SAML 2.0' configuration page. At the top, there is a 'Default Relay State' field with a note: 'All IDP-initiated requests will include this RelayState.' Below this is a yellow banner stating 'SAML 2.0 is not configured until you complete the setup instructions.' with a 'View Setup Instructions' button. The 'Advanced Sign-on Settings' section contains two fields: 'Assertion Consumer Service URL' with the value 'https://admin.zsccloud.net/adminsso.do' and 'Service Provider Entity Id' with the value 'admin.zsccloud.net'. Both fields are highlighted with red boxes. The 'Credentials Details' section includes 'Application username format' set to 'Okta username', 'Update application username on' set to 'Create and update', and 'Password reveal' checked with the option 'Allow users to securely see their password (Recommended)'. A message at the bottom states 'Password reveal is disabled, since this app is using SAML with no password.' At the bottom of the form are 'Previous', 'Cancel', and 'Done' buttons.

Figure 97. Sign-on configuration

## Assign the App to the ZIA Administrators

The final Okta step is to assign the application to the ZIA administrators.

1. Select the **Assignments** tab, and under **Filters**, select **People**.
2. Click **Assign**.
3. Select the administrators you want to assign to the application.

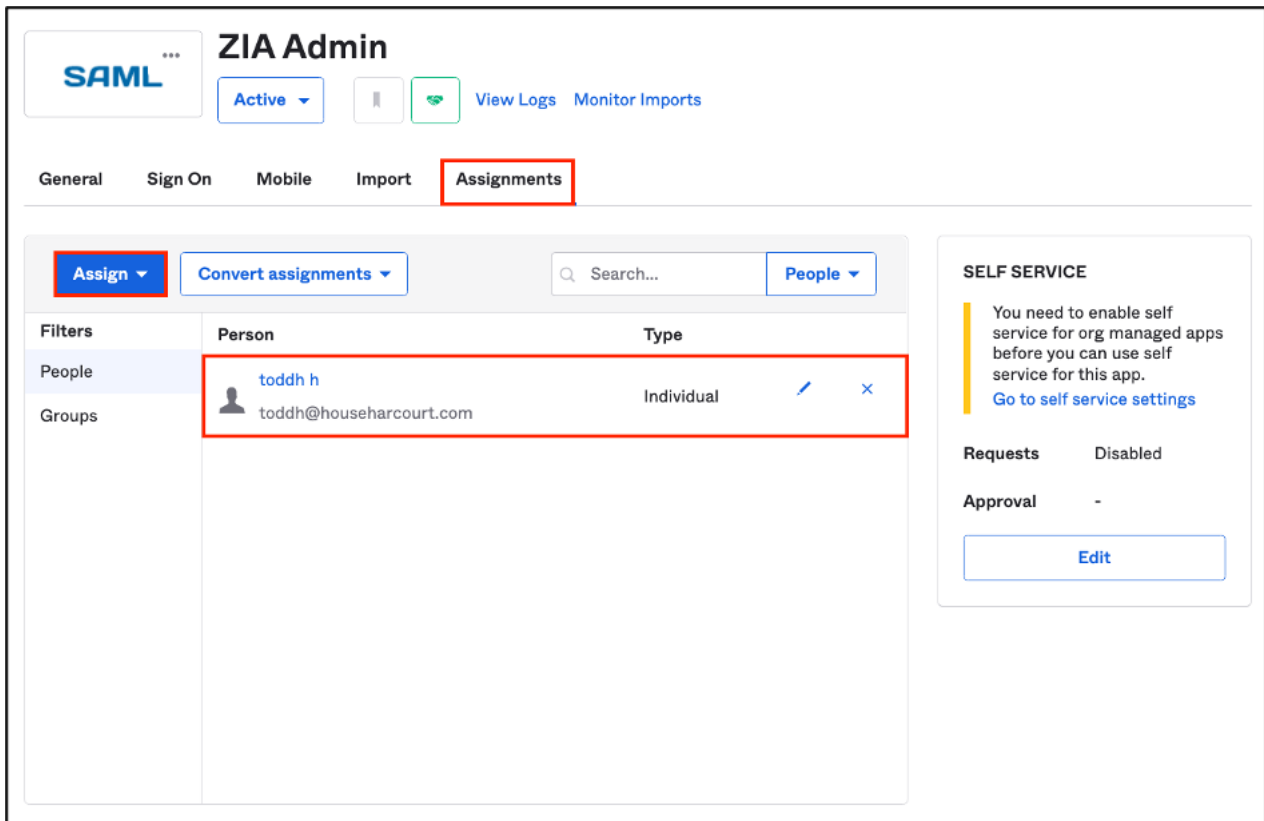


Figure 98. Assigning administrators

## Configure ZIA for Admin SSO

1. Log in to the ZIA Admin Portal.
2. Go to **Administration > Administrator Management**.

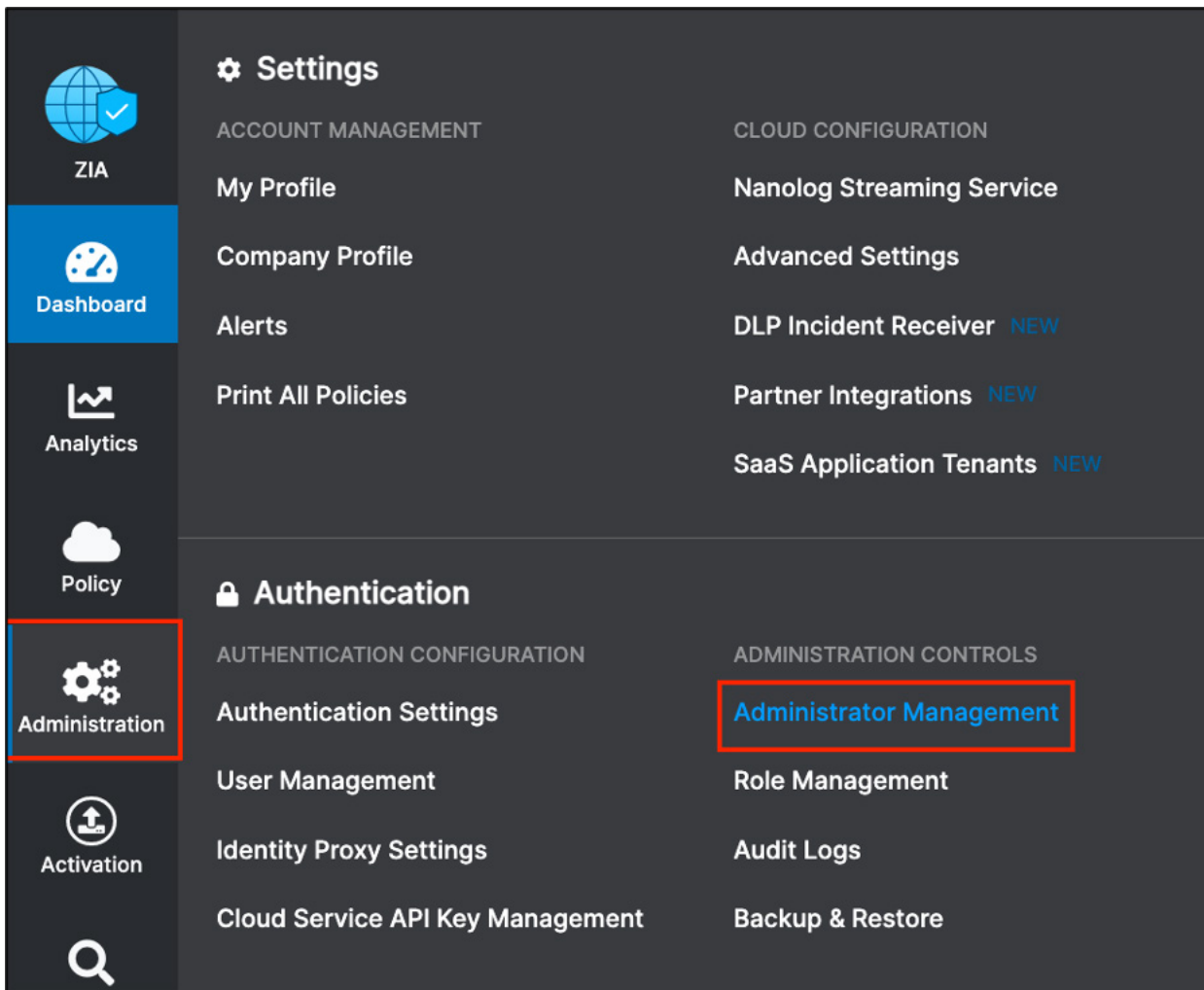


Figure 99. Create the ZIA administrator

## Enable SAML for ZIA Admins

1. Select the **Administrator Management** tab.
2. Select **Enable SAML Authentication**.
3. Under **IdP SAML Certificate**, select **Upload** to upload the okta.pem file.
4. **Save** the configuration.

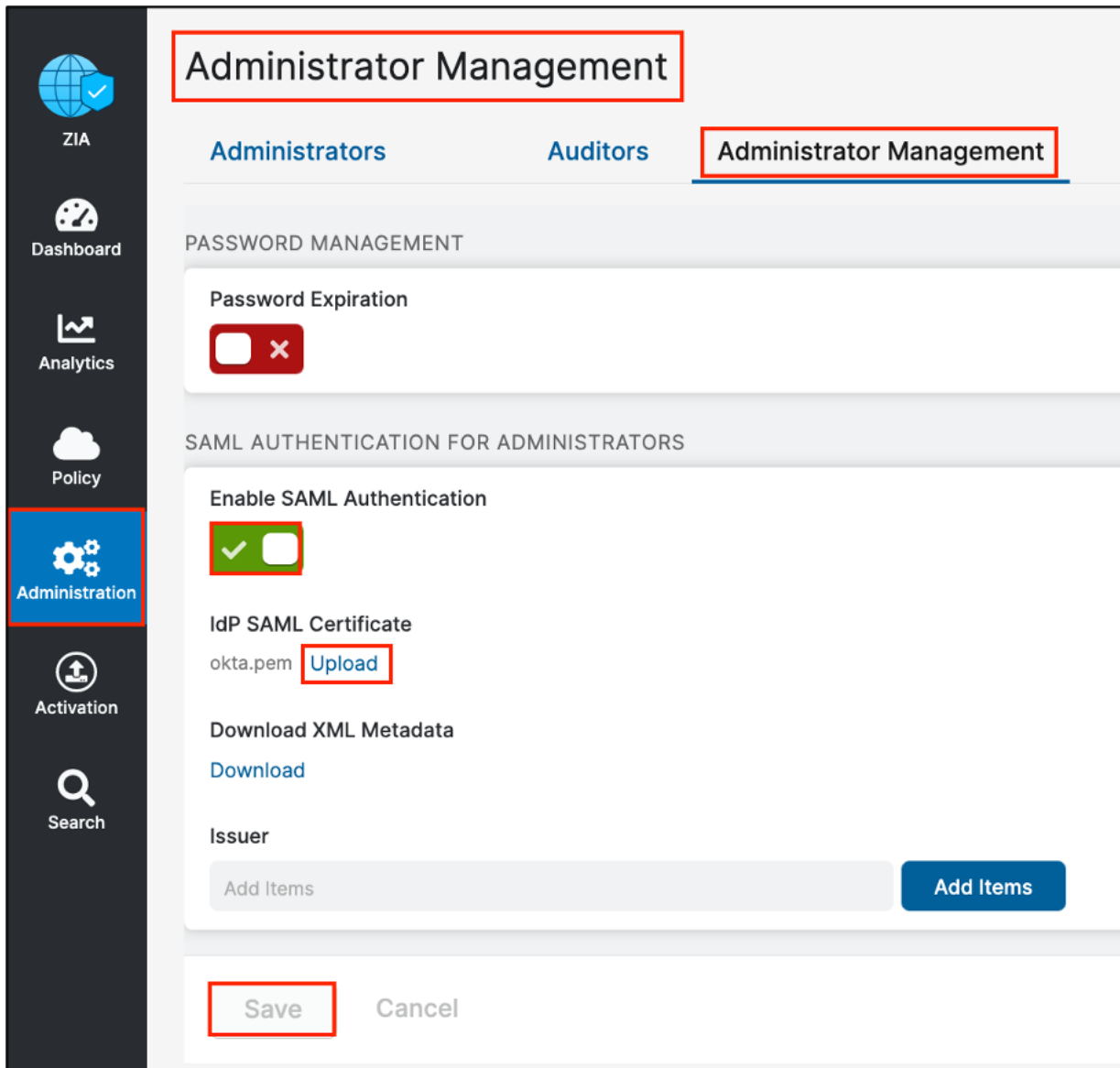


Figure 100. Enable SAML authentication

## Add ZIA Administrators

Add an administrator for every user who will use SAML and the Okta application:

1. Select the **Administrators** tab.
2. Select **Add Administrator**.
3. Enter each **Administrator**.

No.	Login ID	Name	Role	Scope	Login Type
1	admin@3173833.zscloud....	DEFAULT ADMIN	Super Admin	Organization	SAML, Password
2	admin@todd.zscloud.net	DEFAULT ADMIN (Deprec...	Super Admin	Organization	SAML, Password
3	api_tester@todd.zscloud....	api_tester	apitester	Organization	SAML, Password
4	toddh@househarcourt.com	toddh H	Super Admin	Organization	SAML, Password

Figure 101. Adding administrators

## Test the Admin SSO Access

1. Launch the ZIA Admin Portal from the Okta administrator console and the SAML application.
2. Select the **SAML ZIA Admin** tile to launch the ZIA Admin Portal with SSO.

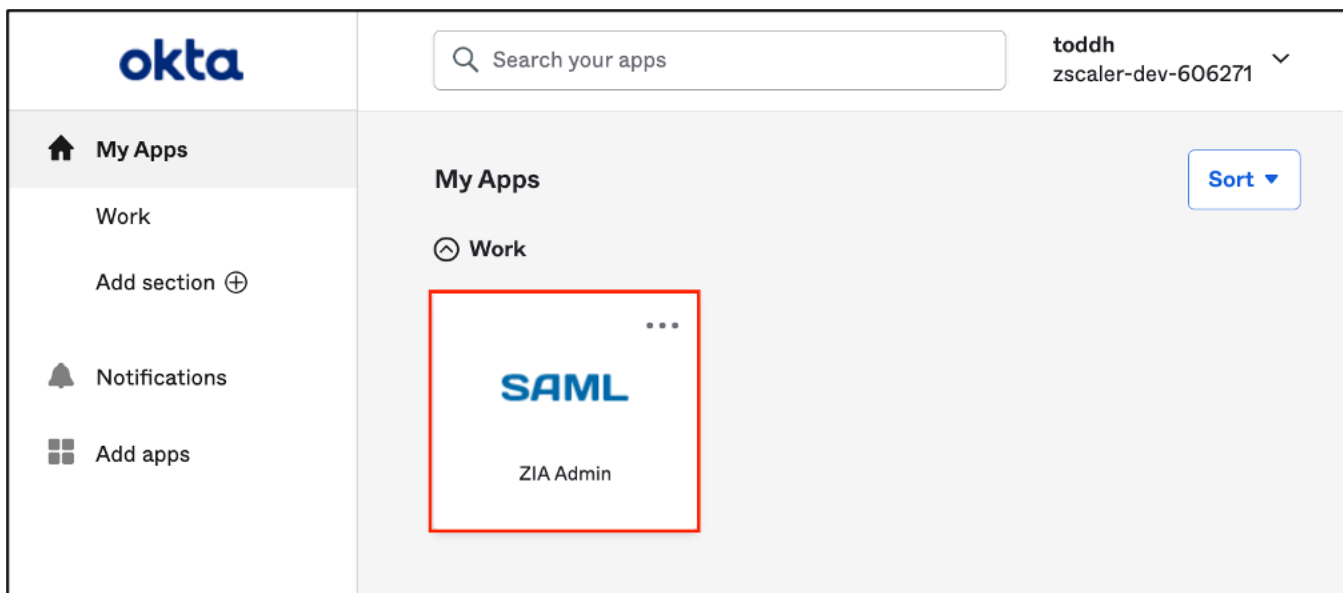


Figure 102. Launch SAML app from the Okta portal



## Using Okta for ZPA Admin Access

To configure admin access using SAML SSO, configure a second IdP specifically for ZPA admin SSO.

### Add the Okta Application for ZPA SAML Administrator Access

Install a second instance of the Zscaler Private Access 2.0 application used for admin access. From your Okta administrator console:

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

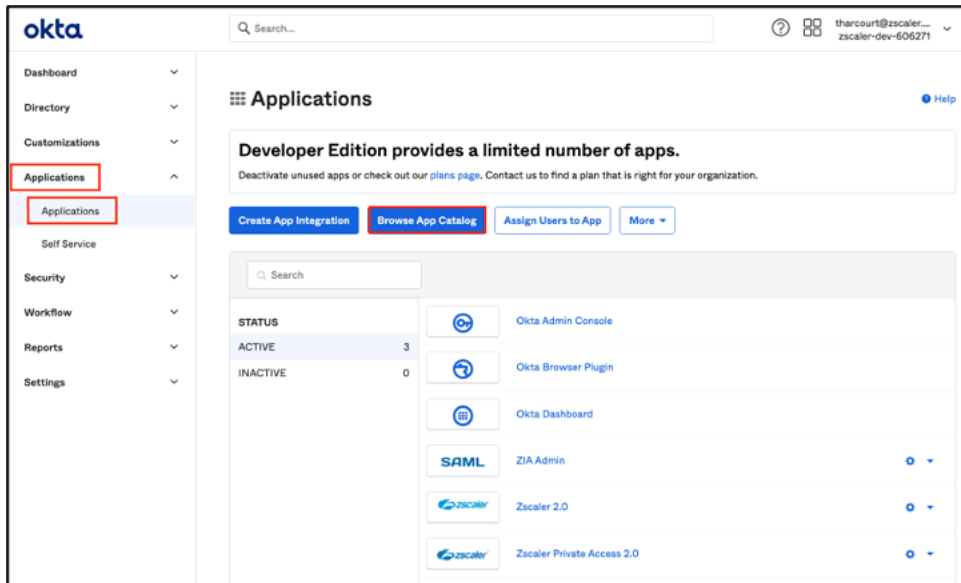


Figure 103. Add the ZPA Okta application

4. Search for **zscaler** in the search bar.
5. Select **Zscaler Private Access 2.0**.

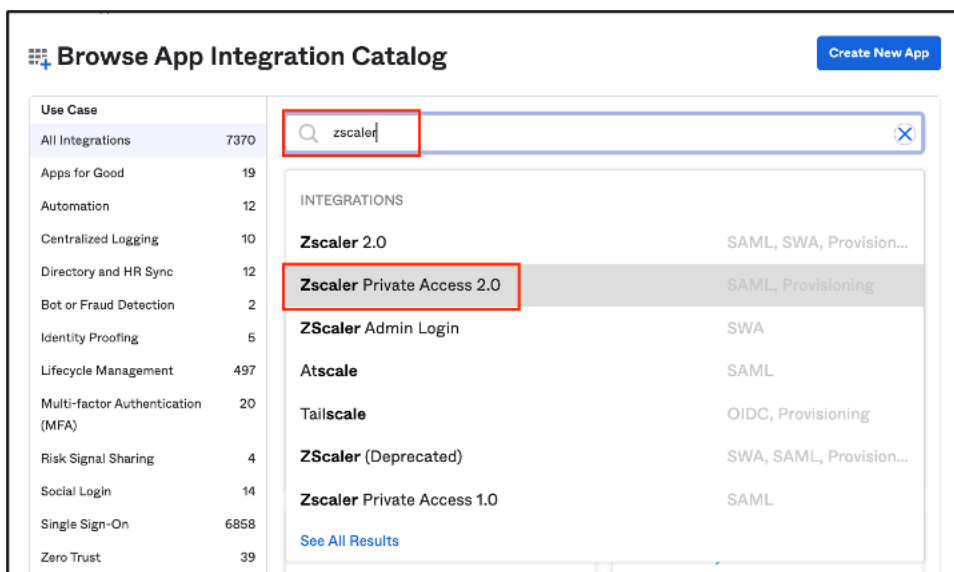


Figure 104. Select the ZPA application

6. Select **Add** on the **Overview** page.

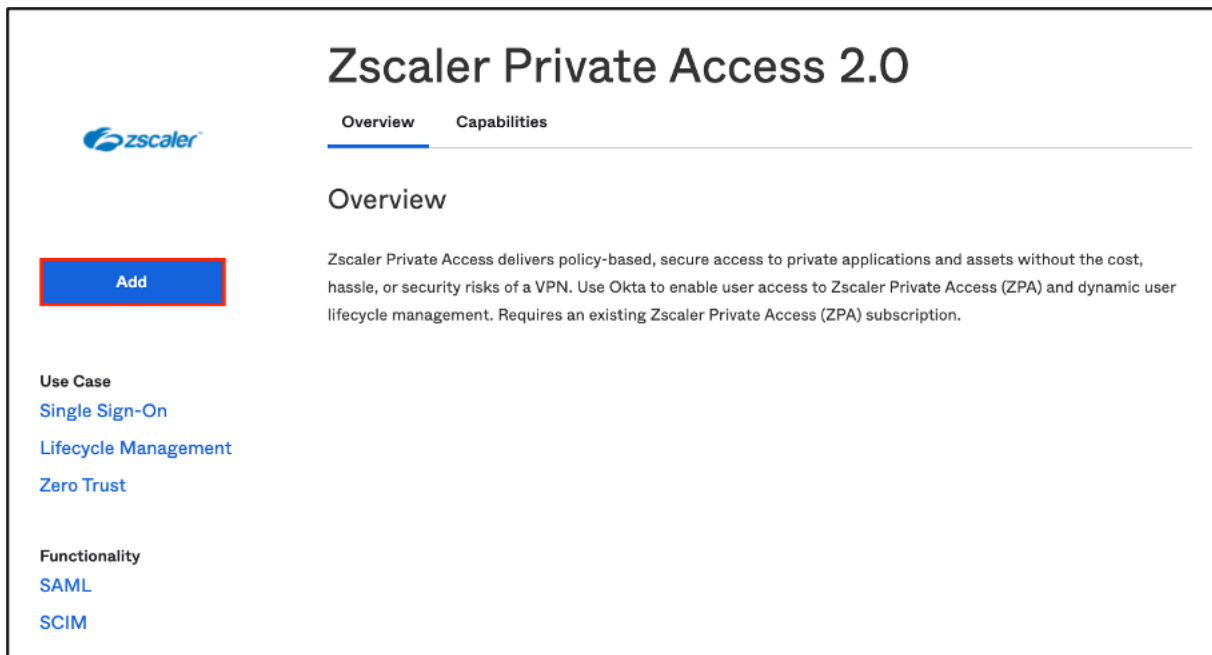


Figure 105. Select Add on the overview page

7. Enter a unique name for the **Application label**.
8. Click **Done**.

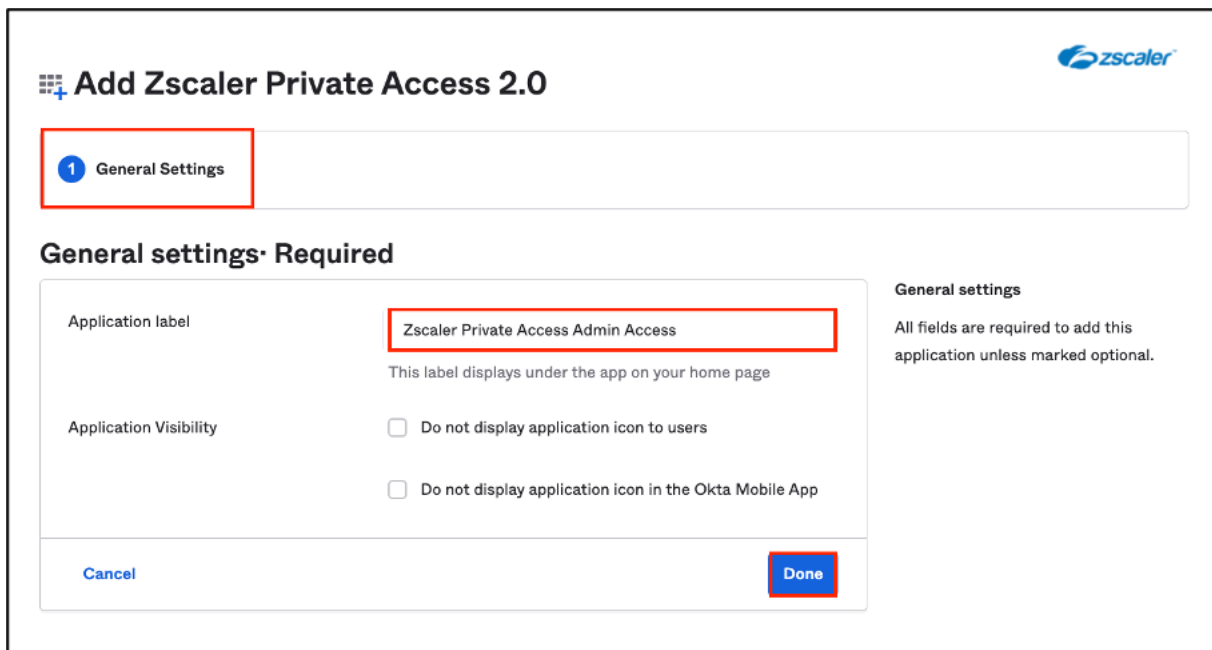


Figure 106. General settings

## Configure the Okta IdP: Save the Metadata

Download and save the Okta application metadata.

1. Select the **Sign On** tab.
2. Select **View SAML setup instructions**.

The screenshot displays the Okta Admin Console interface for the application 'Zscaler Private Access Admin Access'. The left sidebar shows the navigation menu with 'Applications' expanded. The main content area has tabs for 'General', 'Sign On' (highlighted with a red box), 'Mobile', 'Provisioning', 'Import', 'Assignments', and 'Push Groups'. Under the 'Sign On' tab, the 'Settings' section is active, showing 'SAML 2.0' configuration options. The 'Advanced Sign-on Settings' section includes fields for 'Service Provider URL', 'Service Provider Entity ID', and 'Credentials Details'. The 'SAML Signing Certificates' table lists a single certificate. The 'SAML Setup' section on the right contains a link to 'View SAML setup instructions', which is highlighted with a red box.

Figure 107. Application metadata location

- Copy the metadata and save to a file named `metadata_admin.xml`.
- Close the window.

### Before you Begin

The Zscaler Private Access OIN application supports two configuration types:

- For Administrators
- For Users

In order to add administrator/user configurations, you need to add a separate Zscaler Private Access application instance in Okta and create a separate IDP Configuration in Zscaler.

The Okta metadata file is different for each application instance in Okta, so it will be different for both configurations. Save the following metadata file and add a required prefix (admin or user), so the file name will be: `metadata_admin.xml` (for administrator configuration) or `metadata_user.xml` (for user configuration):

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="http://www.okta.com/exk17bu7yi75rzYdp0h8"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <xmldsig:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:X509Data>
            <ds:X509Certificate>MIIDpDCCAoygAwIBAgIGAYBrpKBKMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
            A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Figure 108. Okta metadata

## Add the ZPA IdP for Admin SSO on the ZPA Admin Portal

In the ZPA Admin Portal, add the Okta IdP:

- Go to **Administration > IdP Configuration**.
- Select the **Add** icon to add the IdP configuration.

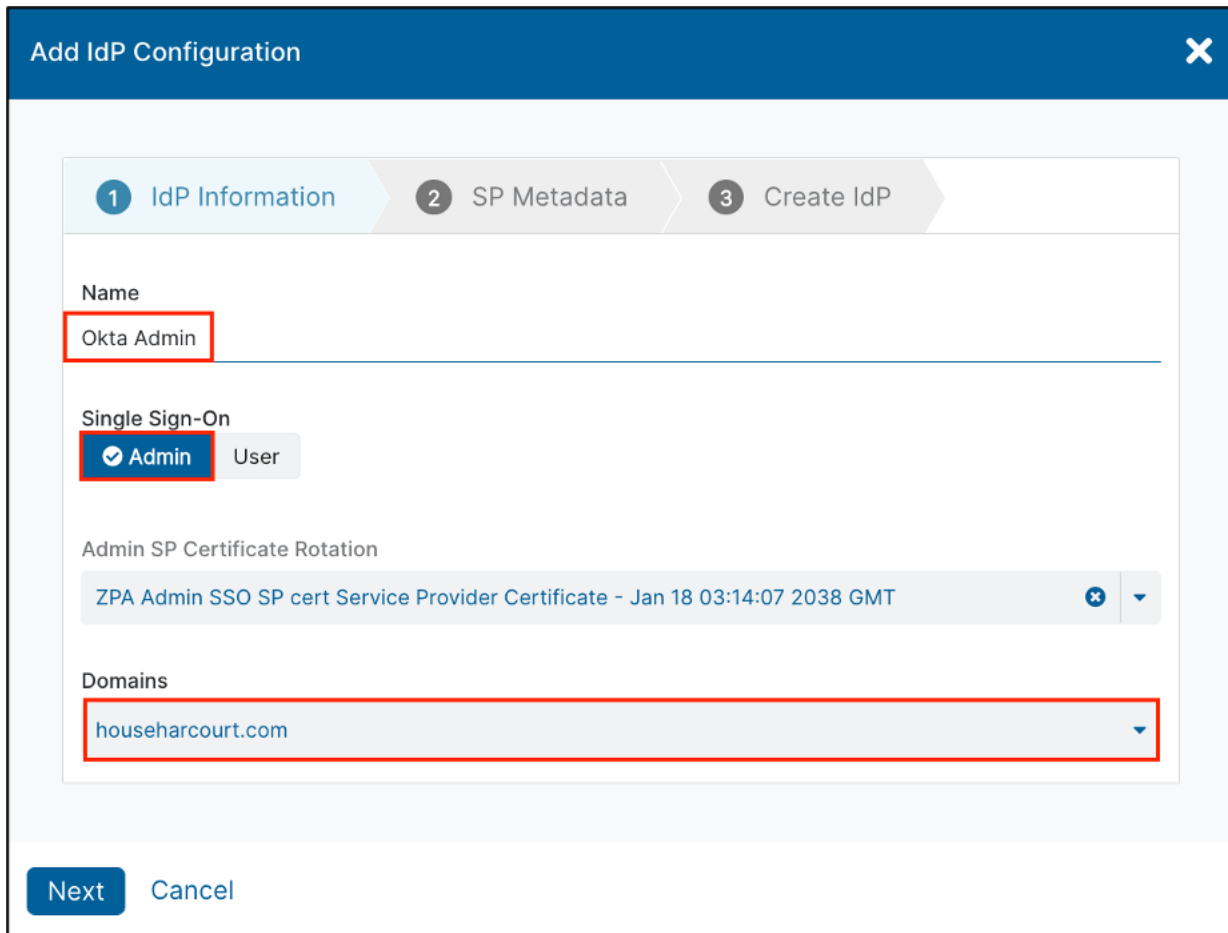
Name	Status	IdP Entity ID	Single Sign-On	Actions
Okta	✓	http://www.okta.com/exk15gsy15bP0Xrhn0h8	User	<a href="#">Edit</a> <a href="#">Delete</a>

Figure 109. Add the Okta IdP in the ZPA Admin Portal

## Configure the ZPA IdP Information on the ZPA Admin Portal

Selecting Add IdP Configuration launches the Add IdP Configuration wizard.

1. Enter a unique **Name** for the IdP.
2. Select **Admin** under **Single Sign-On**.
3. Select the organization's domain from which the administrators sign in.
4. Click **Next**.



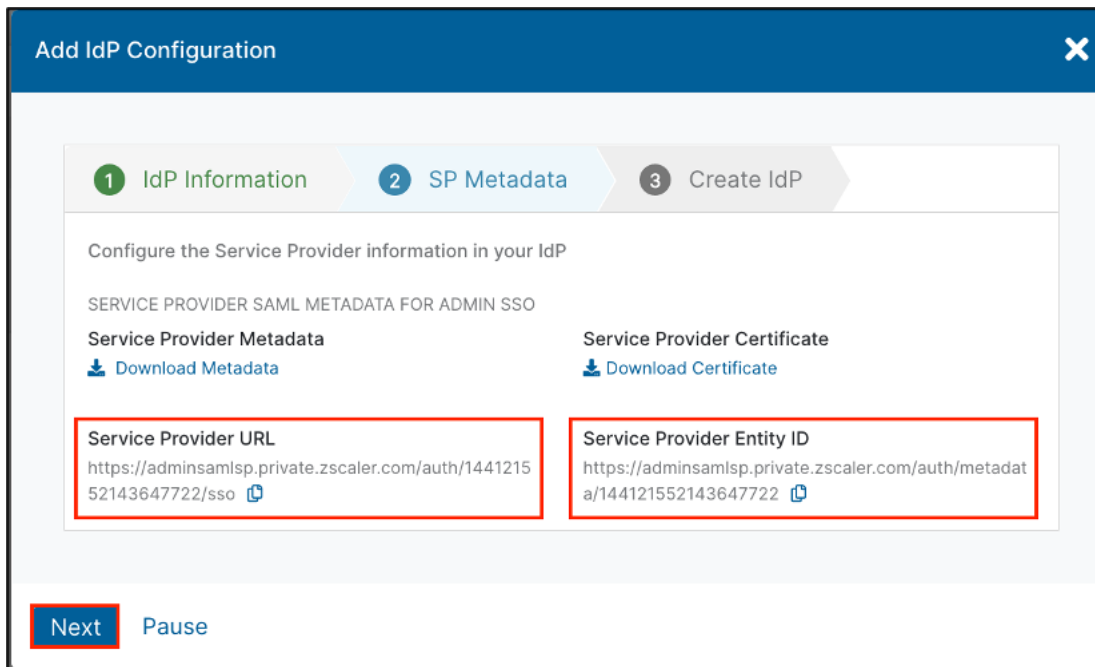
The screenshot displays the 'Add IdP Configuration' wizard with a blue header bar containing a close button (X). The wizard has three steps: 1. IdP Information (active), 2. SP Metadata, and 3. Create IdP. The 'Name' field is labeled 'Name' and contains the text 'Okta Admin'. The 'Single Sign-On' section has two radio buttons: 'Admin' (selected) and 'User'. The 'Admin SP Certificate Rotation' section shows a dropdown menu with the text 'ZPA Admin SSO SP cert Service Provider Certificate - Jan 18 03:14:07 2038 GMT'. The 'Domains' section has a dropdown menu with the text 'househarcourt.com'. At the bottom, there are 'Next' and 'Cancel' buttons.

Figure 110. Add IdP Configuration wizard

## Copy the ZPA SP URLs

The SP Metadata page is displayed:

1. Copy and save the **Service Provider URL** and the **Service Provider Entity ID URL**.
2. Click **Next**.



**Add IdP Configuration** [X]

1 IdP Information   2 **SP Metadata**   3 Create IdP

Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR ADMIN SSO

<b>Service Provider Metadata</b> <a href="#">Download Metadata</a>	<b>Service Provider Certificate</b> <a href="#">Download Certificate</a>
<b>Service Provider URL</b> <code>https://adminsamlsp.private.zscaler.com/auth/144121552143647722/sso</code> <a href="#">Copy</a>	<b>Service Provider Entity ID</b> <code>https://adminsamlsp.private.zscaler.com/auth/metadata/144121552143647722</code> <a href="#">Copy</a>

**Next**   Pause

Figure 111. SP URLs for the Okta configuration

## Configure the Okta IdP on the ZPA Admin Portal

To configure the Okta IdP:

1. Choose **Select File** for the **IdP Certificate**.
2. Click **Save**.

**Add IdP Configuration**

1 IdP Information   2 SP Metadata   3 Create IdP

Name  
Okta Admin

Authentication Domains  
househarcourt.com

**SAML CONFIGURATION**

IdP Metadata File  
metadata\_admin.xml   Change   Remove

IdP Certificate  
Upload the Certificate File...   Select File

-----BEGIN CERTIFICATE-----  
MIIDpDCCAoygAwIBAgIGAYBrpKBKMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG  
A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FueZyYW5jaXNjbzENMAAsGA1UECgwET2t0Y  
TEU

Single Sign-On URL  
https://dev-606271.oktapreview.com/app/zscaler\_private\_access/exk17bu7yi75rzYdp0h8/sso/saml

IdP Entity ID  
http://www.okta.com/exk17bu7yi75rzYdp0h8

Status  
☒ Enabled   Disabled

ZPA (SP) SAML Request  
☒ Signed   Unsigned

HTTP-Redirect  
Enabled   ☒ Disabled

Single Sign-On  
☒ Admin   User   Both

Admin SP Certificate Rotation  
ZPA Admin SSO SP cert Service Provider Certificate - Jan 18 03:14:07 2038 GMT

**Save**   Pause

Figure 112. Import the Okta metadata

## Define the Administrators for SAML Access

Administrators using the SAML IdP for authentication must be added as administrators. To configure the administrators:

1. Go to **Configuration & Control > Administration Control > Administrators**.

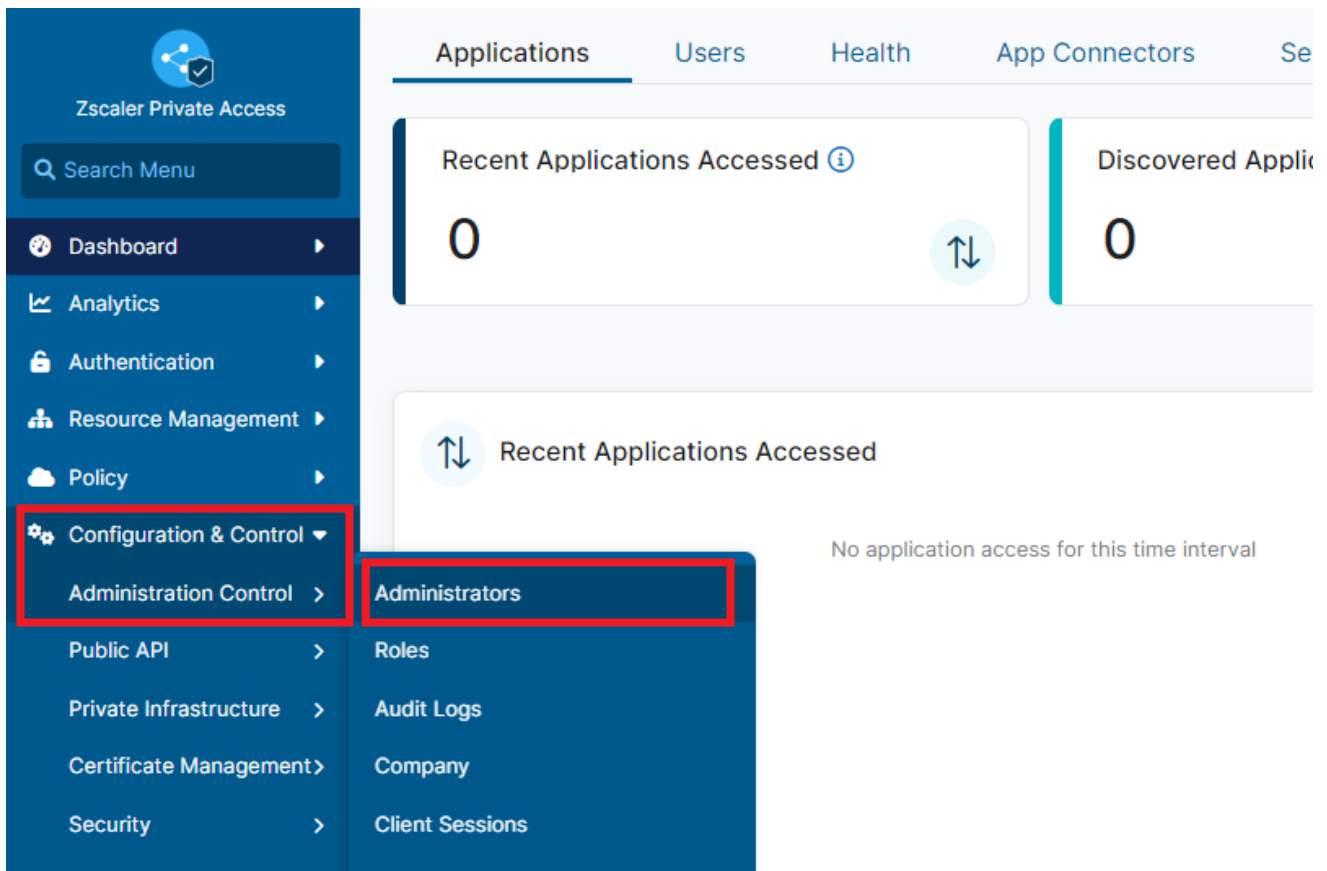


Figure 113. Creating an administrator



2. Select the **Add** icon to add an administrator.

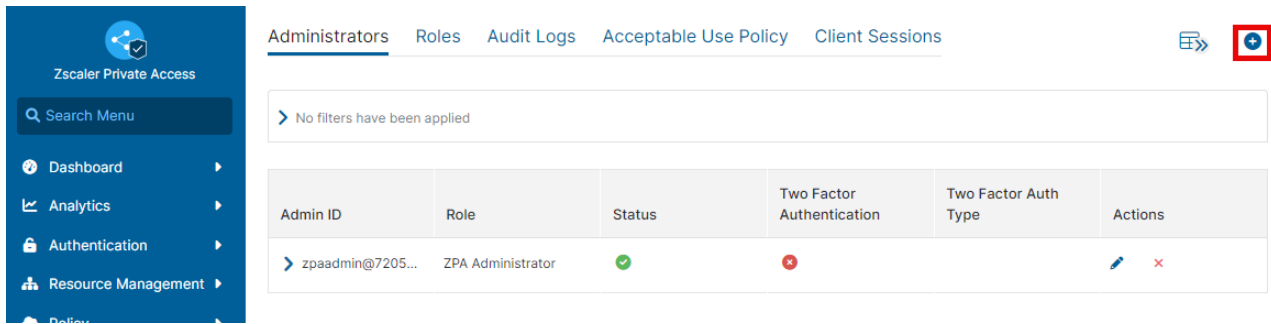


Figure 114. Add Administrator

3. In the **Add Administrator** window, enter an **Admin ID**.
4. Enter an **Email** address.
5. Enter a **Phone** number (without formatting).
6. Select **ZPA Administration** from the **Role** drop-down menu.
7. Click **Enabled** for **Status**.
8. Enter a **Password**.
9. Enter the password again to **Confirm Password**.
10. Click **Save** to complete the ZPA configuration.

The screenshot shows the 'Add Administrator' form. It has the following fields and values:
 

- Admin ID:** toddh@househarcourt.com
- Email:** toddh@househarcourt.com
- Phone:** 7132994968
- Role:** ZPA Administrator (selected from a dropdown)
- Status:** Enabled (selected from a radio button group)
- Two Factor Authentication:** Off (selected from a radio button group)
- Force Password Reset:** Yes (selected from a radio button group)
- Pin Session:** Yes (selected from a radio button group)
- Password:** \*\*\*\*\*
- Confirm Password:** \*\*\*\*\*

 At the bottom, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a red box.

Figure 115. Create an administrator

## Finish the Okta Configuration on the Okta Portal

1. Select **Sign On**.
2. Select **Edit**.

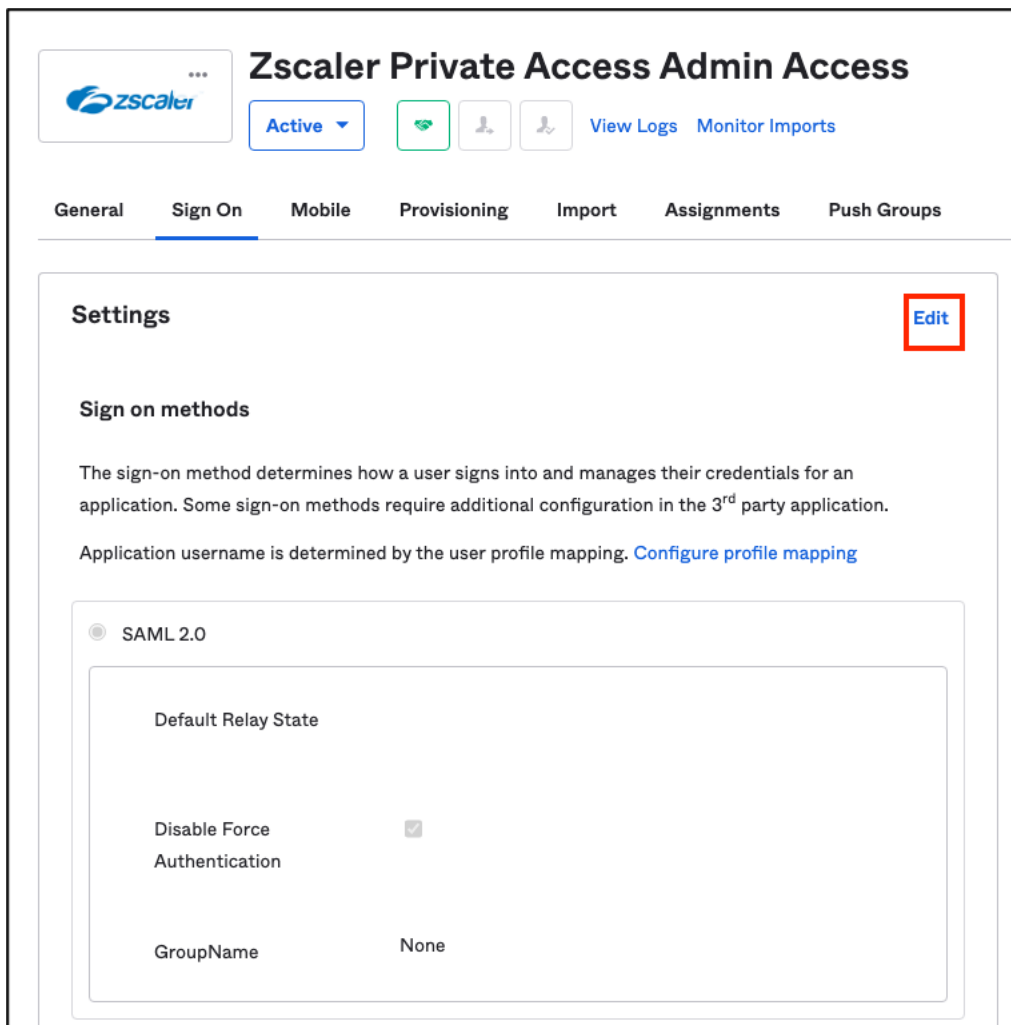


Figure 116. SAML sign-on methods

3. Enter the **Service Provider URL** and the **Service Provider Entity ID** copied from ZPA.
4. Click **Save**.

The screenshot shows the Okta Admin console interface. On the left is a navigation menu with options like Dashboard, Directory, Customizations, Applications, Self Service, Security, Workflow, Reports, and Settings. The main content area is titled 'Zscaler Private Access Admin Access' and has tabs for General, Sign On, Mobile, Provisioning, Import, Assignments, and Push Groups. The 'Sign On' tab is active. Below the tabs, there's a 'Settings' section with a 'Cancel' button. Under 'Sign on methods', it states that SAML 2.0 is the only supported option. The 'SAML 2.0' configuration section includes fields for 'Default Relay State', 'Disable Force Authentication' (checked), and 'GroupName' (set to None). Below this is the 'Advanced Sign-on Settings' section, which contains the 'Service Provider URL' and 'Service Provider Entity ID' fields, both of which are highlighted with red boxes. The 'Service Provider URL' is 'https://adminsamlsp.private.zscaler.com/auth/14412155' and the 'Service Provider Entity ID' is 'https://adminsamlsp.private.zscaler.com/auth/metadata'. Below these are 'Credentials Details' including 'Application username format' (Okta username), 'Update application username on' (Create and update), and 'Password reveal' (disabled). A 'Save' button is located at the bottom right of the configuration area.

Figure 117. Okta sign-on configuration

## Assign the Administrators or Groups to the Application

Assign the ZPA administrators to the application using individual users, a security group, or both.

1. Select the **Assignments** tab.
2. Select **People** or **Groups** to define the type of assignment variable.
3. From the **Assign** drop-down menu, select the **User** or **Group** for the **Administrators**. In the following example, user **toddh h** is selected.

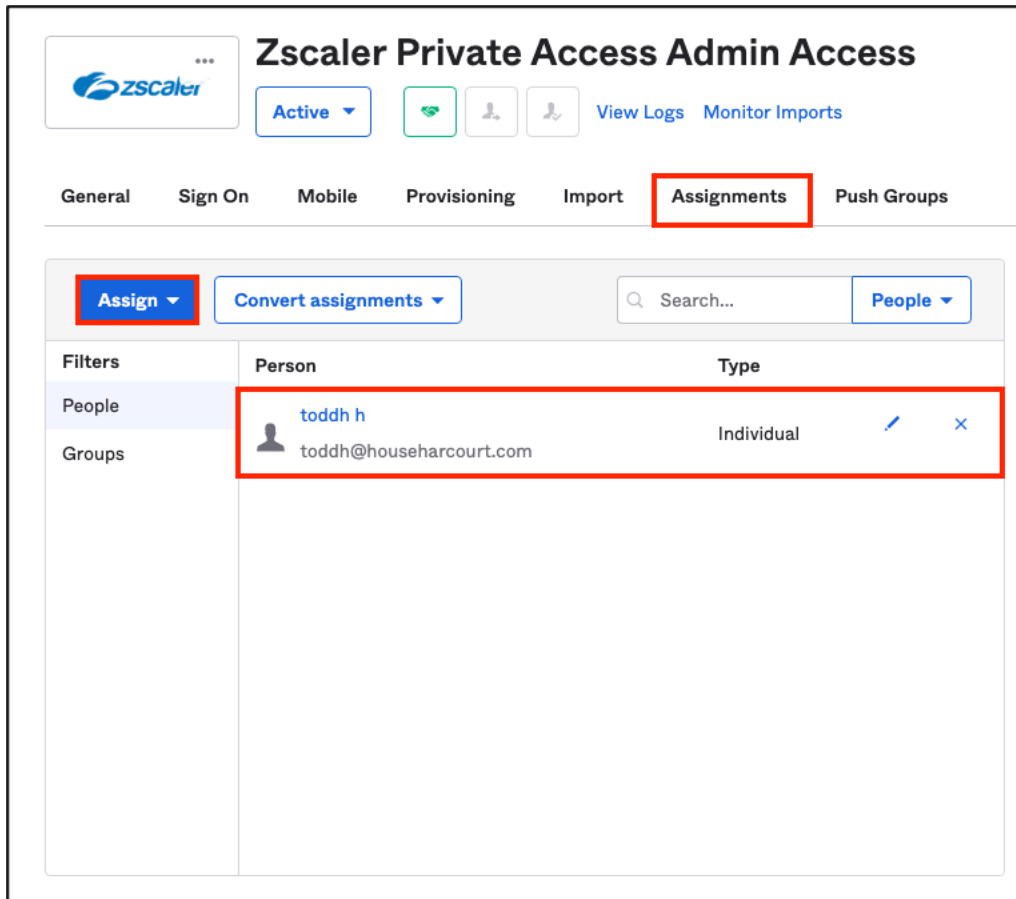


Figure 118. Assigning a user or group to the SAML app

## Test the ZPA Authentication Configuration

On the Okta administrator console, click the **Zscaler** tile. The app launches the ZPA Admin Portal and authenticates the user. You can also log in from the ZPA Admin Portal sign-on screen.

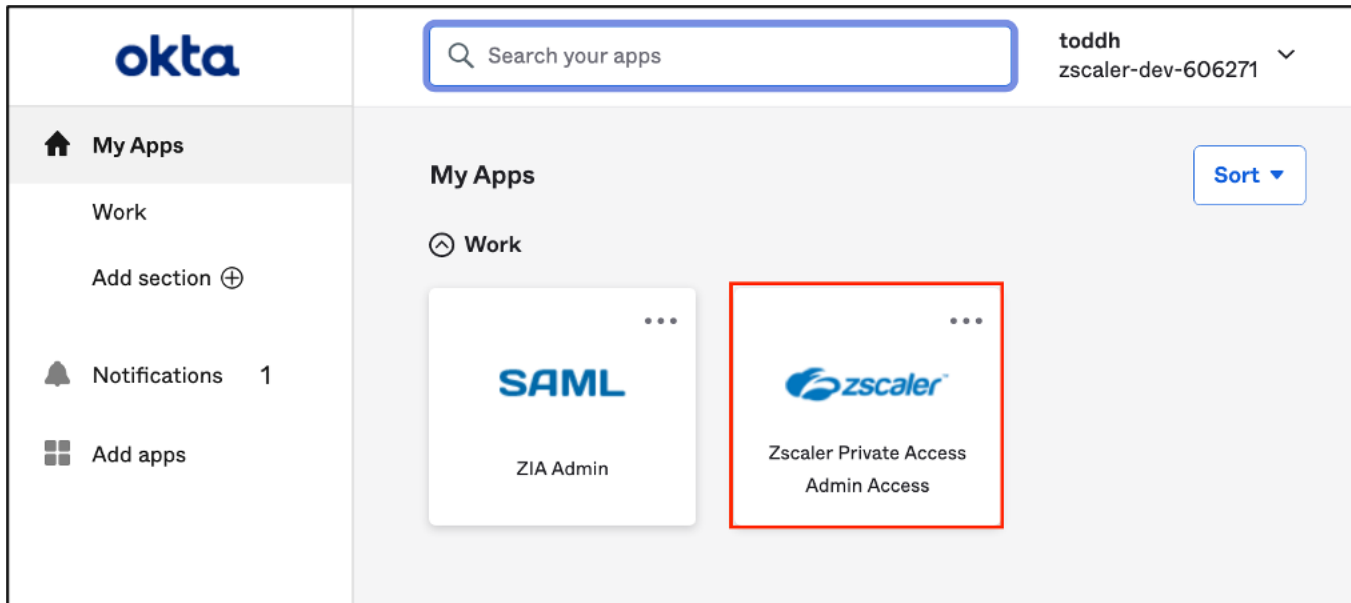


Figure 119. User Okta apps

## Administrator Sign In Using SAML from the ZPA Admin Portal

To sign in from the ZPA Admin Portal using the Okta SAML IdP:

1. Select **Single Sign-On Using IdP**.
2. Click **Sign In**.



Figure 120. Administrator sign-on using your SAML IdP

## Okta Device Trust for Managed Devices

Zscaler has device control integrations with Okta that use Okta Device Trust for Windows, macOS, and iOS. This allows you to identify managed, unmanaged, and unknown devices connected to ZIA and ZPA. ZIA and ZPA then create additional security controls based on the state of the device.

Okta's Device Trust works in conjunction with endpoint security and, when installed along with the Okta Integrated Windows Authentication (IWA) server, returns a SAML variable that is included in the user authentication process. IWA also provides a transparent authentication process to Zscaler users and authenticates into ZIA and ZPA using the credentials of the Windows user authenticated into the device.

Zscaler integrations utilizing Okta Device Trust include:

- ZIA Identity Proxy that blocks unmanaged and unknown devices from accessing SaaS applications front-ended by Identity Proxy.
- ZIA Identity Proxy that redirects unmanaged and unknown devices to Isolation when accessing SaaS applications front-ended by Identity Proxy.
- ZPA Access and Reauthentication policies that secure against unmanaged devices.

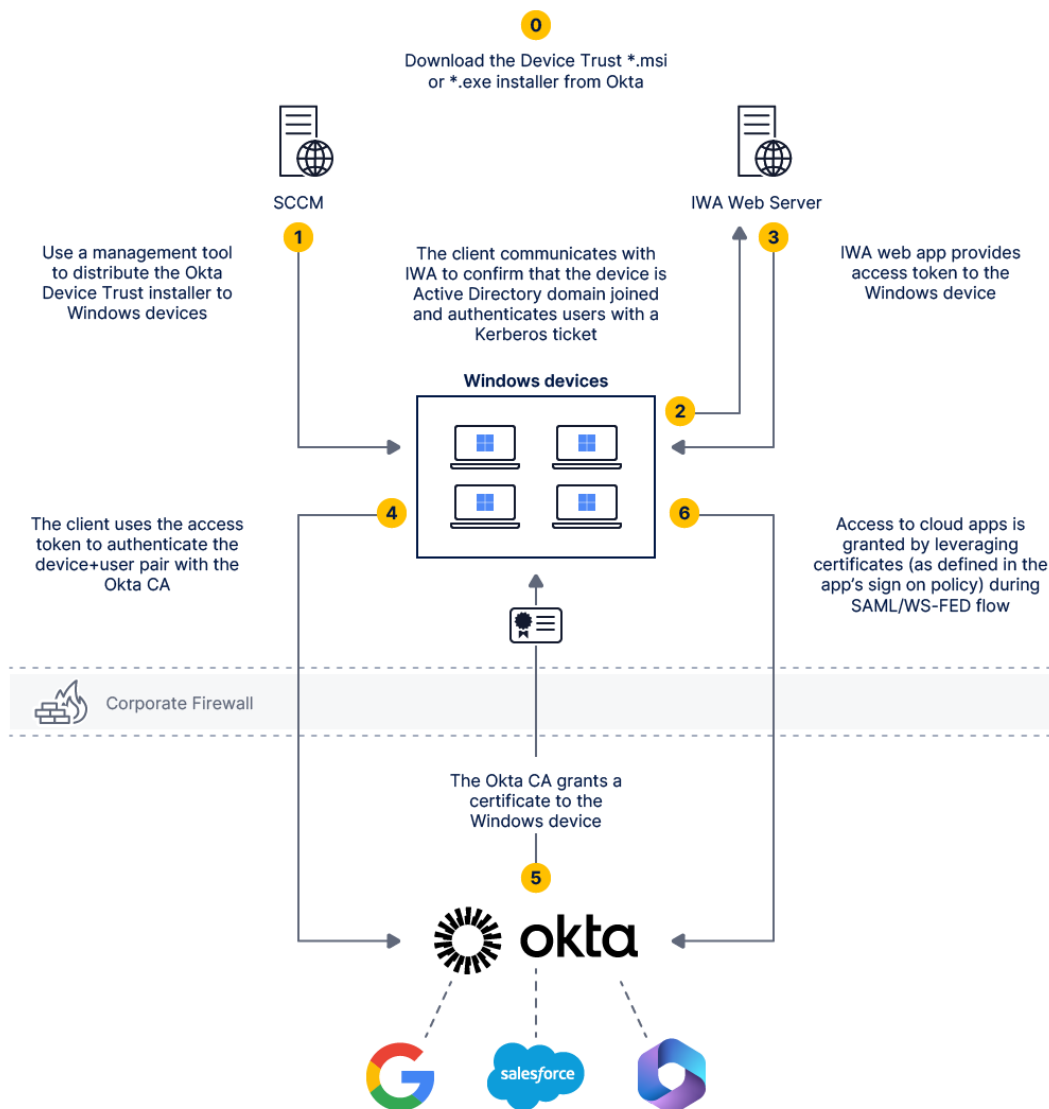


Figure 121. Okta Device Trust

## Installing Okta Device Trust

You must install the Okta IWA server and Okta Device Trust in the environment, and domain join the device, in order to use the Zscaler integration with Okta Device Trust.

Follow the steps at: [https://help.okta.com/en-us/Content/Topics/Mobile/Okta\\_Mobile\\_Device\\_Trust\\_Windows-desktop.htm](https://help.okta.com/en-us/Content/Topics/Mobile/Okta_Mobile_Device_Trust_Windows-desktop.htm) to install Okta Device Trust.

## SAML Variable Returned in the User's SAML Assertion

The following attributes and variables are included when you install Okta Device Trust. The SAML attribute *Trust* is defined as the data source and the variable used for the Zscaler integrations.

### SAML Trust Attribute and Variable for a Trusted Device:

```
<saml2:Attribute Name="Trust" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">TRUSTED</saml2:AttributeValue>
```

### SAML Trust Attribute and Variable for an Untrusted Device:

```
Name="Trust" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">NOT_TRUSTED</saml2:AttributeValue>
```

### SAML Trust Attribute and Variable for an Unknown Device:

```
Name="Trust" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">UNKNOWN</saml2:AttributeValue>
```

Figure 122. Okta Device Trust attributes

## Configure ZIA to Use Okta Device Trust

To use Okta Device Trust for the Zscaler Identity Proxy, define the attribute and variable in the SAML Identity Provider:

1. Go to **Administration > Authentication Settings > Identity Providers**.
2. Select the IdP that uses Okta Device Trust.
3. Enter `Trust` for the **Device Trust Attribute** (case sensitive).
4. Enter `TRUSTED` for the **Device Trust Attribute Value** (case sensitive).
5. Click **Save**.

The screenshot displays the Zscaler Identity Proxy Administration interface. On the left, the 'Administration' menu is highlighted. The main panel shows 'Authentication Settings' with the 'Identity Providers' tab selected. A table lists identity providers, with 'Okta Demo' selected. The 'Edit IdP' modal is open, showing the 'DEVICE TRUST' section where 'Device Trust Attribute' is set to 'Trust' and 'Device Trust Attribute Value' is set to 'TRUSTED'. The 'PROVISIONING OPTIONS' section shows 'Enable SAML Auto-Provisioning' as disabled and 'Enable SCIM Provisioning' as enabled. The 'Base URL' and 'Bearer Token' fields are also visible.

No.	ID	Name
1	410283	Okta Demo
2	9287	Z-App Mobile Idp
3	9099	PingOne
4	9034	Azure
5	8950	Idaptive
6	8780	okta-2

**DEVICE TRUST**

Device Trust Attribute	Device Trust Attribute Value
Trust	TRUSTED

**PROVISIONING OPTIONS**

Enable SAML Auto-Provisioning	Enable SCIM Provisioning
<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Base URL**

https://scim.zsccloud.net/3173833/scim (Deprecated)  
https://scim.zsccloud.net/3173833/410283/scim

**Bearer Token**

AT3Tr8QeEF0hbRjxv9riLPILB2GT218V19LJsNkqrRP1tRX3Pws7IG0JiQV2gO1UPA==

**Generate Token**

Figure 123. Okta Device Trust attributes



## Configure ZIA Identity Proxy to Use Okta Device Trust

To use Okta Device Trust for Zscaler Identity Proxy, first add the attribute to the Managed Device settings in each cloud application using Identity Proxy:

1. Go to **Administration > Identity Proxy Settings**.
2. Select or add the cloud application that uses Okta Device Trust.
3. Select **Proxied via Zscaler with IdP Attribute**.
4. Select **Browser Isolate** or **Block** for traffic from **Unmanaged Device Action**.
5. Select the **Isolation Profile** if **Browser Isolate** is selected.
6. Click **Save**.

The screenshot displays the 'Identity Proxy Settings' page in the Zscaler console. On the left sidebar, the 'Administration' menu is highlighted. The main content area shows a table of cloud applications with 'Okta' selected. The 'Edit Cloud Application' modal is open, showing the following configuration:

- CLOUD APPLICATION:**
  - Name: Okta
  - Status: ☒ Enable ☐ Disable
  - Cloud Application: ServiceNow
  - ACS URL: https://zscalerbdteam.service-now.com/nav...
  - Entity ID: https://zscalerbdteam.service-now.com
- IDENTITY PROXY SETTINGS:**
  - Response Signing SAML Certificate: saml\_2022
  - SAML Certificate Expiration Date: November 16, 2022
- IDENTITY TRANSFORMATION RULES:**
  - Identity Transformation: ☒ Pass-through Zscaler Identity ☐ Change Domain to ☐ Remove Domain Name
- GROUP:**
  - Pass-on Group Details: ☐ Enable ☒ Disable
  - Group Identifier Name: Enter Text
- MANAGE DEVICE SETTING:**
  - Managed Device: ☐ Proxied via Zscaler ☒ Proxied via Zscaler with IdP Attribute
  - Device Trust Attribute: Trust
  - Device Trust Attribute Value: TRUSTED
- UNMANAGED DEVICE ACTION:**
  - Action: ☒ Browser Isolate ☐ Block
  - Isolation Profile: Okta-Untrusted-Device

At the bottom of the modal, there are buttons for 'Save', 'Cancel', and 'Delete'.

Figure 124. Identity Proxy

## The User Experience

Users receive a warning if they try logging into a SaaS app using Isolation and are not logged into Zscaler.

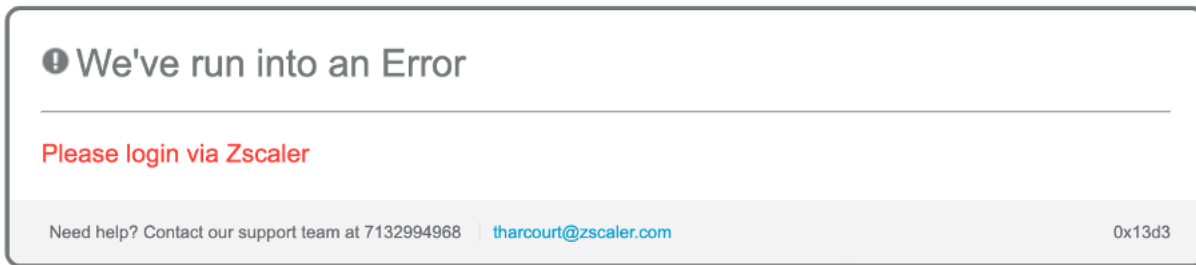


Figure 125. Identity Proxy warning

Users receive a warning if they try logging into a SaaS app that is using Identity Proxy and are logged into Zscaler with an unmanaged device (and there is a block action defined for an unmanaged device).

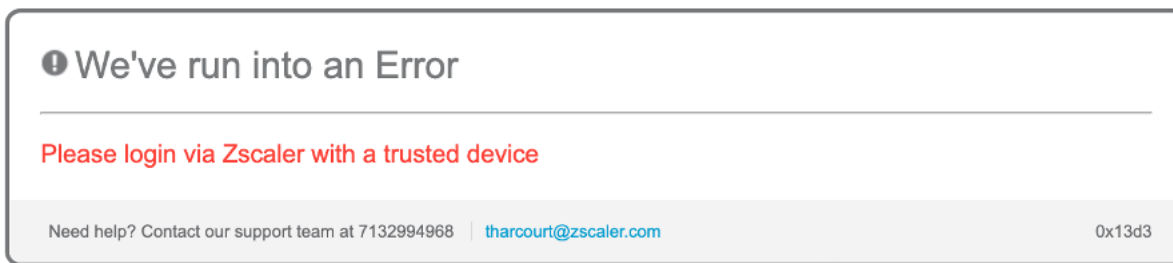


Figure 126. Unmanaged Block Action

Users receive a warning if they try logging into a SaaS app using Identity Proxy and are logged into Zscaler with an unmanaged device (and there is an Isolation action for an unmanaged device).

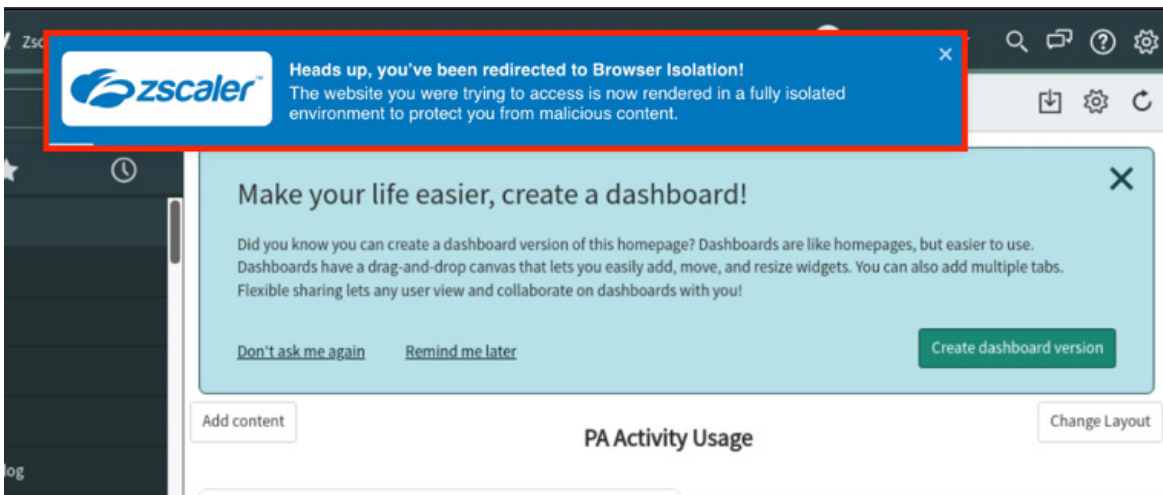


Figure 127. Unmanaged Browser Isolation Action

## Configure ZPA to Use Okta Device Trust

Using the Okta Device Trust variable in ZPA requires importing the variable, then defining access and reauthentication policies with the SAML variable. This variable is returned in the user's SAML assertion during the authentication process.

Import the trust attribute for policies from a device using Okta Device Trust. The device does not need to be trusted, but it must have the Okta Device Client installed with the IWA Server enabled and active.

In the ZPA Admin Portal:

1. Select **Authentication** > **User Authentication** > **IdP Configuration**.
2. Select the arrow next to the **Okta IdP**.
3. Click **Import**.
4. **Save** the new attributes.

The screenshot shows the ZPA Admin Portal interface. On the left is a navigation menu with options like Dashboard, Analytics, Authentication, User Authentication, Device authentication, Resource Management, Policy, Configuration & Control, Client Connector, Account, and Tools. The main content area is titled 'IdP Configuration' and has tabs for 'SAML Attributes' and 'Settings'. A table lists IdP configurations, with the first one 'preview-itasca-devel' selected. Below the table, the configuration details for 'Okta IdP' are shown, including 'ZPA (SP) SAML Request' (Signed), 'Login Hint' (Enabled), 'SAML Attributes for Policy' (Enabled), and 'Authentication Domains' (72057629471408128.zpa-customer.com). At the bottom, the 'Import SAML Attributes' section shows a dropdown menu with 'househarcourt.com' selected and an 'Import' button highlighted with a red box.

Figure 128. SAML variable import

- To confirm that the variable is available, select **Authentication > User Authentication > SAML Attributes**.

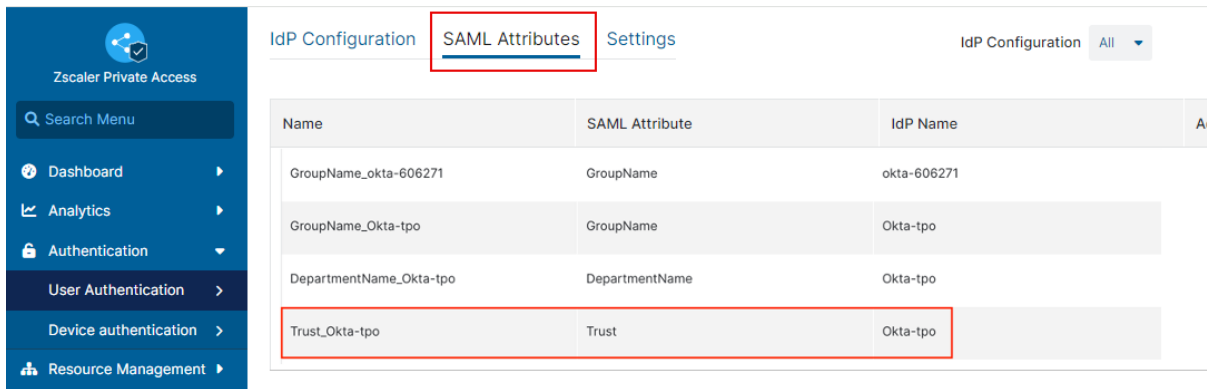


Figure 129. SAML Trust attribute

- To enable the **SAML Trust** variable for policies, select **Authentication > User Authentication > IdP Configuration**.
- Select the **Edit** icon next to the **Okta IdP**.
- Select **Enabled** for the **SAML Attributes for Policy**.
- Click **Save**.

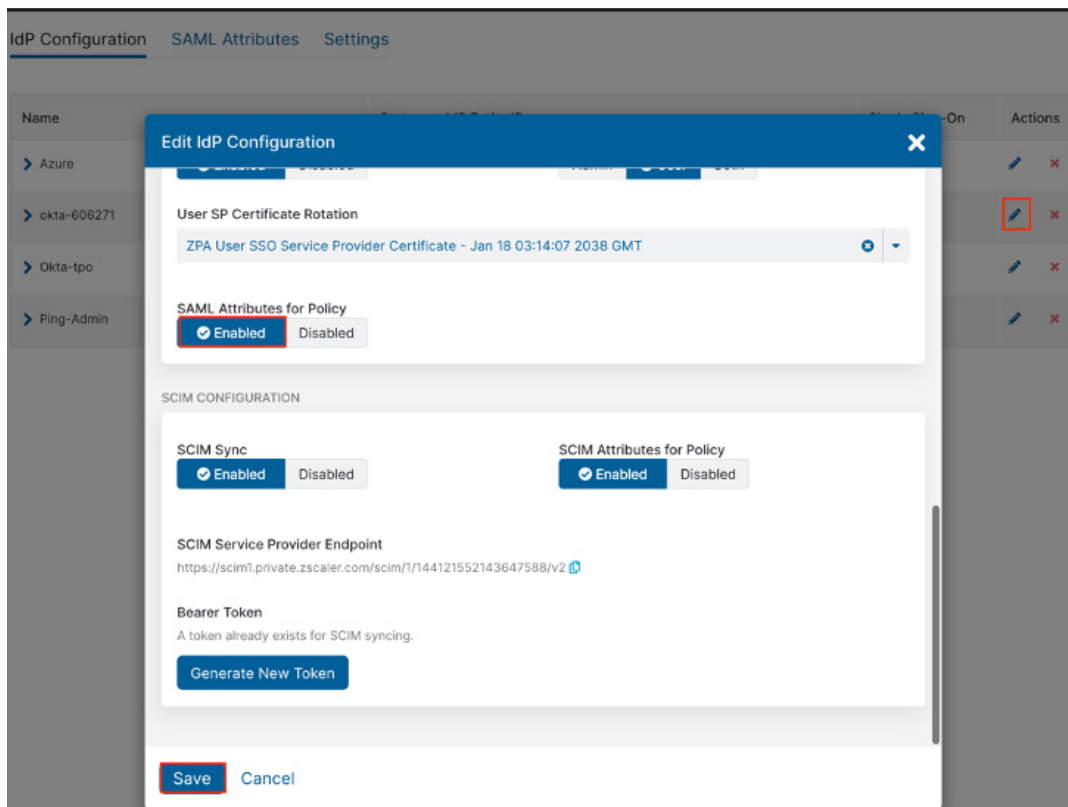


Figure 130. ZPA IdP configuration

In the ZPA Admin Portal:

1. Select **Policy > Access Policy**.
2. Edit the **Access Policy** to add **Device Trust**.
3. Select **Add Criteria** and select **SAML** and **SCIM Attributes** from the drop-down menu. The **SAML and SCIM Attributes** area is added in the **Criteria** section.
4. In the **Criteria** section, under **SAML and SCIM Attributes**, select the **Okta IdP** from the **Select IdP** drop-down menu.
5. Select **SAML Attributes**.
6. Select the **Trust\_IdP** attribute.
7. Enter a value of **TRUSTED** (case sensitive).
8. Click **Save**.

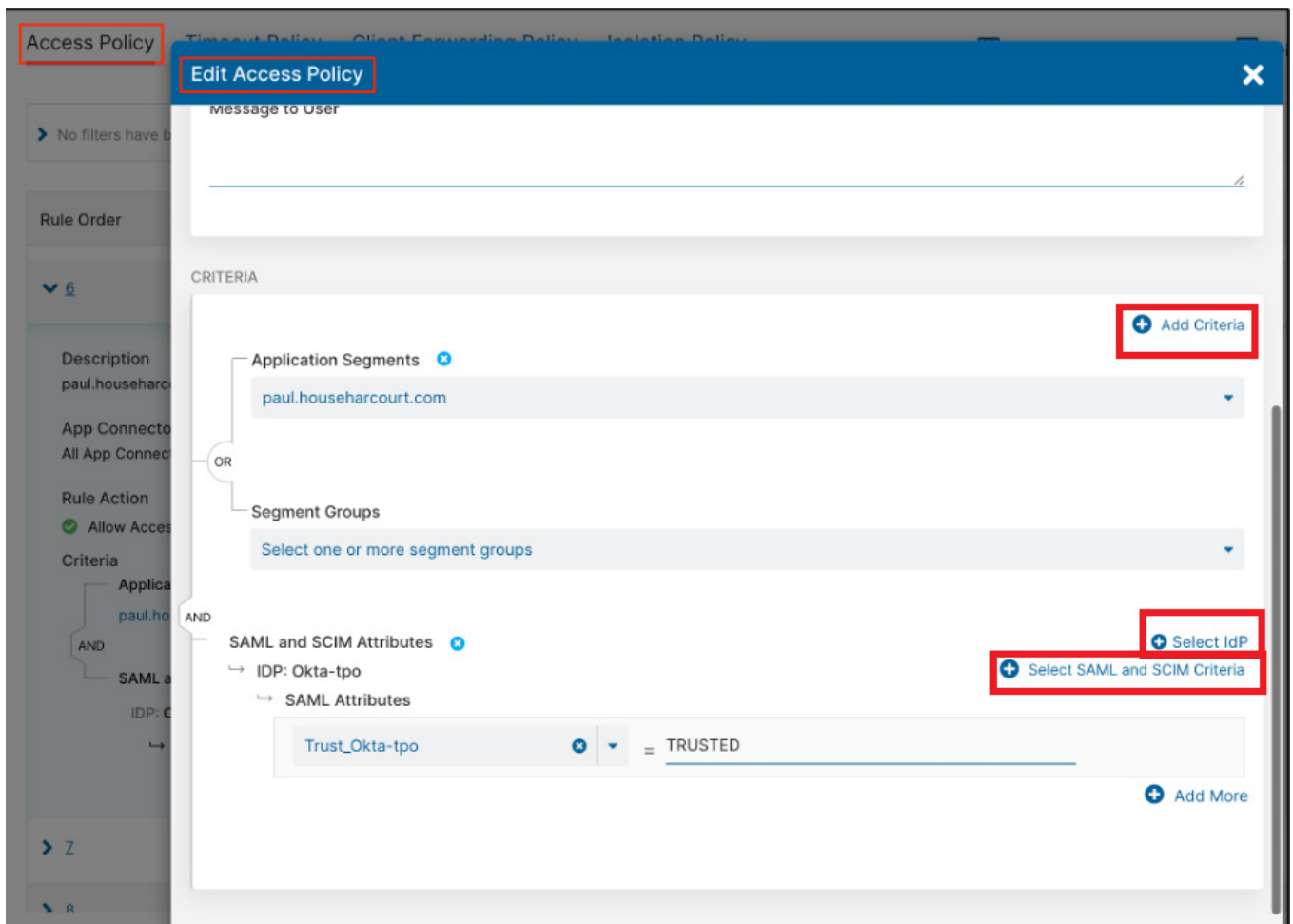


Figure 131. Using the Okta device trust attributes

## Deception and Identity Threat Protection Integration

This guide provides prerequisites and instructions on configuring a containment integration for Identity Threat Protection with Okta AI. Identity Threat Protection with Okta AI is a risk assessment and response solution from Okta that continuously analyzes the risk signals that are native to Okta, the risk signals from integrated security partner vendors, and your policy conditions to safeguard your organization against identity attacks.

With this integration, Deception pushes user risk scores to Okta for Zscaler Client Connector users based on the events generated when users interact with the decoys. Based on the risk score and Okta policies, Okta can end the user's sessions, prompt a Multi-Factor Authentication (MFA) challenge, or invoke a workflow to restore your organization's security posture. The risk score is pushed to Okta via SSF using the orchestration rules configured in the Zscaler Deception Admin Portal. For example, if a Zscaler Client Connector user interacts with a landmine decoy, an event is logged as an attack in the Deception dashboard. You can have orchestration rules configured for such events and transmit an updated risk score to Okta.

### Overview

Zscaler's Deception and Okta's Identity Threat Detection solutions can detect identity-based attacks with a high degree of certainty. Zscaler has partnered with Okta to stream high-fidelity risk signals into Identity Threat Protection with Okta AI. This enables policy-based actions and workflow-driven responses in Okta for identity-related risk events in real time, empowering organizations to configure countermeasures that can mitigate further risk.

The following shows the Zscaler Deception and Okta environment.

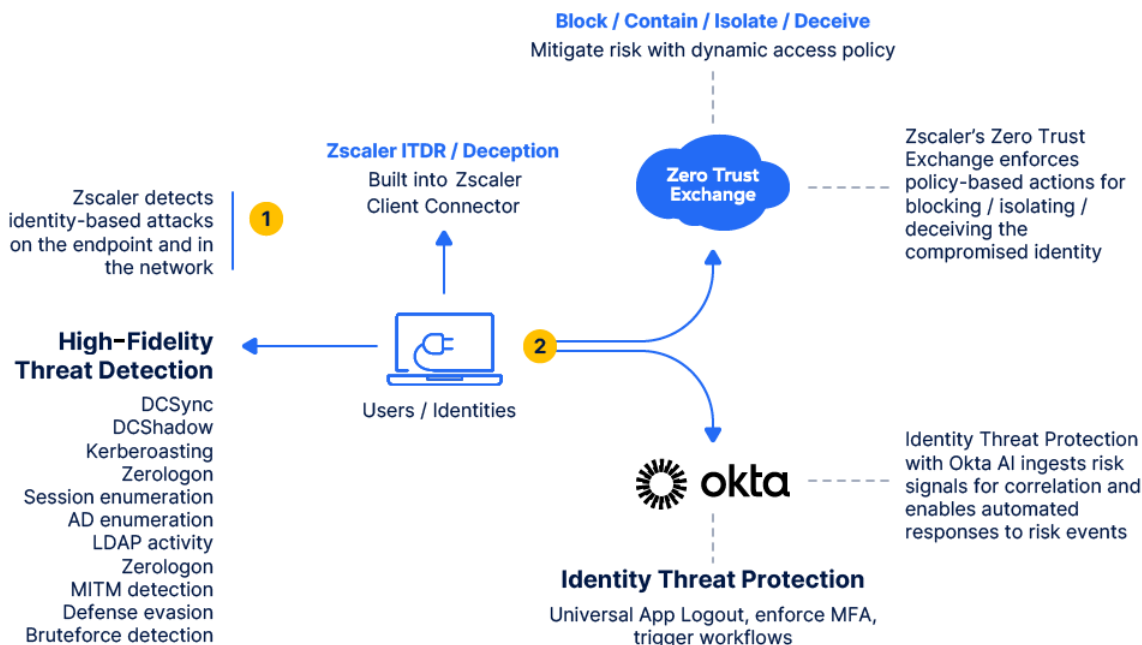


Figure 132. Deception environment

An attacker on a compromised endpoint attempts to kill the EDR process to evade detection. Zscaler Deception is running a decoy EDR process as a compensating control to detect such evasion techniques. When the Kernel driver stops the decoy EDR process along with the real one, the identity's risk level changes to *High* and the alert is pushed to Identity Threat Protection where an Entity Risk Policy for Universal Logout is enforced for supported applications with functionality enabled. This immediately revokes the user's Okta and application sessions, containing the threat from potentially stolen tokens invisible to network security tools.

## Finding Your Okta Domain

To find your Okta domain:

1. Log in to the Okta administrator console.
2. Click your username in the upper right-side corner of the Okta administrator console. The domain appears in the drop-down menu. For domain examples, refer to the [Okta documentation](#).

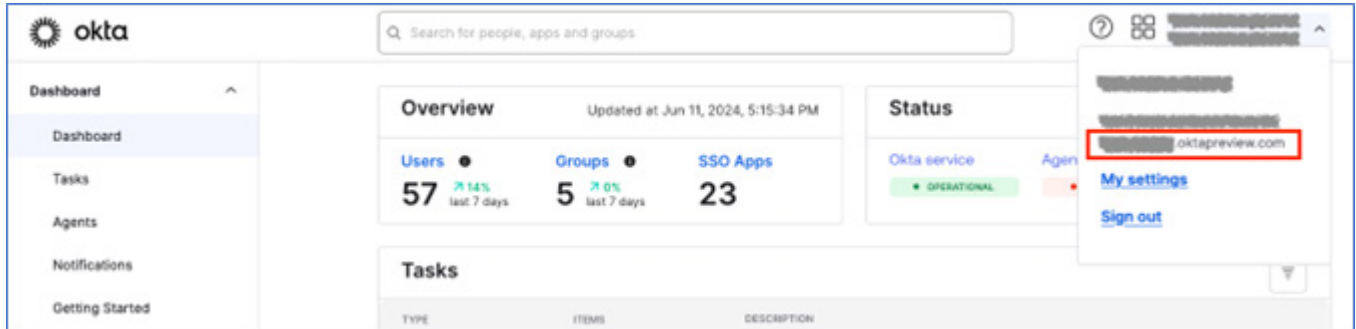


Figure 133. Find your Okta domain

## Create a Shared Signals Framework Receiver in Okta

To create an SSF receiver in Okta:

1. Log in to the Okta administrator console.
2. Go to **Security > Device Integrations > Receive shared signals** and click **Create stream**.

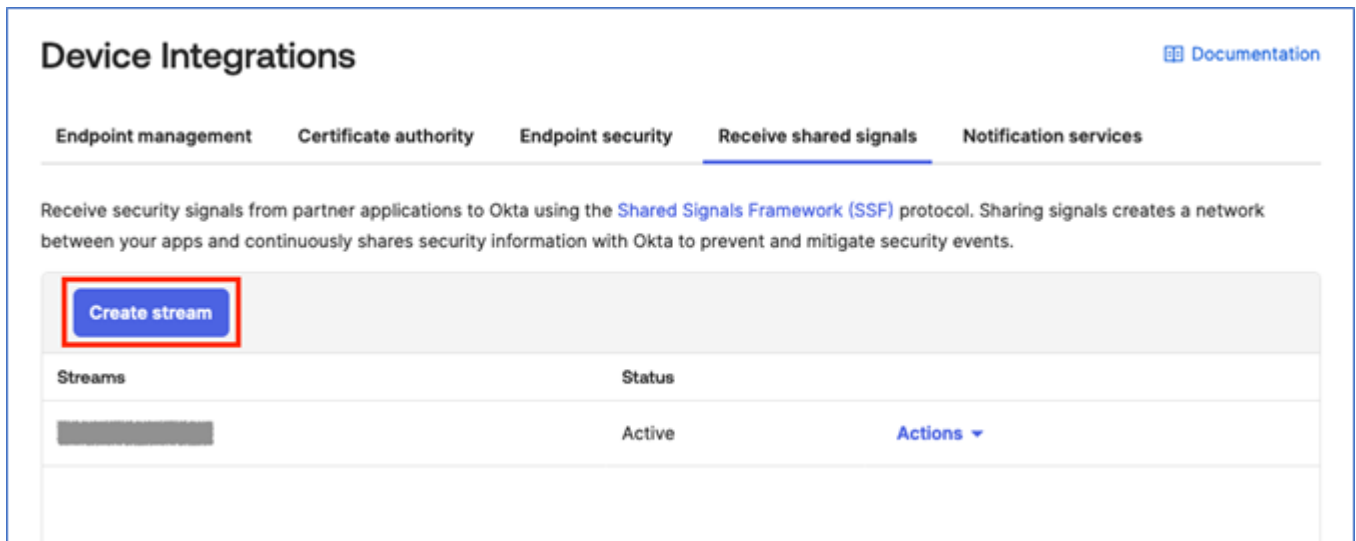


Figure 134. Create stream

3. Enter the following in the stream creation window:
  - a. A **Name** in the **Integration name** field.
  - b. For **Set up integration with**, select **Well-known URL**.
  - c. For **Well-known URL**, enter the following URL for Deception:

`https://zscaler.ssf.transmitter.smokescreen.io/.well-known/sse-configuration`

- Click **Create** to create the Security Events Provider.

**Create a stream to receive a signal**

Receive signals from a partner app to Okta. Your organization can use these signals in authentication policies or entity risk policies.

For instructions, see the [SSF documentation](#).

Integration name:

Set up integration with: ☒ Well-known URL ☐ Issuer URL & JWKS URL

Well-known URL:

**Create** Cancel

Figure 135. Define stream

## Configure the Containment Integration Between Deception and Okta

To configure the Containment Integration between Zscaler Deception and Okta:

- Log in to the Deception Admin Portal.
- Go to **Orchestrate** > **Containment** and click the **Edit** icon for the **Okta (SSF)** entry.

**Containment**  
Integrations with third party security tools for automated containment.

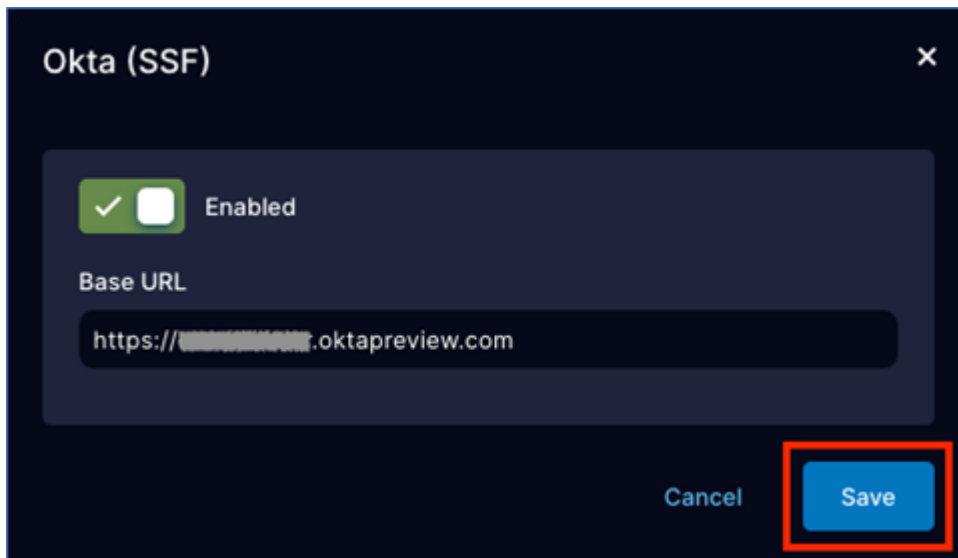
#	Enabled	Settings	Blocked Identities	Actions
1	<input checked="" type="checkbox"/>	Zscaler Internet Access	0	<a href="#">Edit</a>
2	<input checked="" type="checkbox"/>	Zscaler Private Access	0	<a href="#">Edit</a>
3	<input checked="" type="checkbox"/>	Okta (SSF)	0	<a href="#">Edit</a>
4	<input checked="" type="checkbox"/>	CrowdStrike	Contained IP IOC Hash IOC IP	<a href="#">Edit</a>

Figure 136. Edit Okta (SSF)

- Enter the following in the **Okta (SSF)** window:
  - Select **Enabled**.
  - Enter the **Okta tenant URL** with your Okta domain in the **Base URL** field.



- Click **Save** to save the containment configuration.



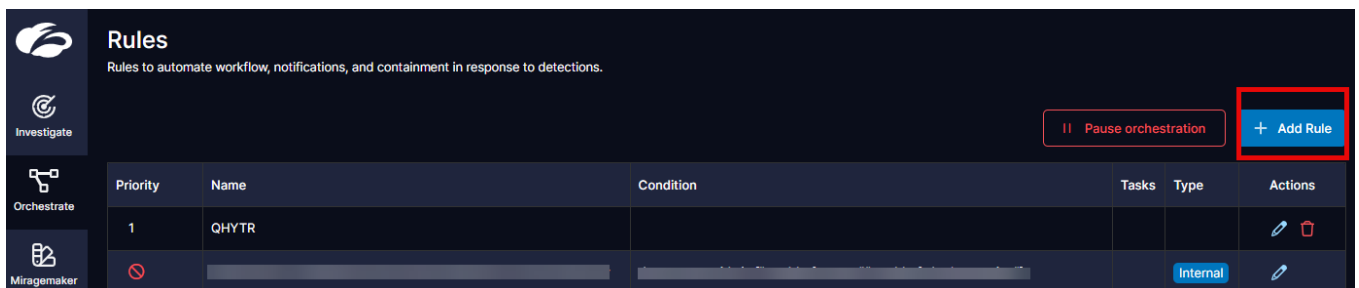
The image shows a dark-themed dialog box titled "Okta (SSF)". At the top right is a close button (X). Below the title, there is a green checkmark icon and a toggle switch labeled "Enabled". Underneath, the text "Base URL" is followed by a text input field containing "https://[redacted].oktapreview.com". At the bottom right, there are two buttons: "Cancel" and "Save". The "Save" button is highlighted with a red rectangular border.

Figure 137. Configure Okta (SSF)

## Configure an Orchestration Rule

To configure the orchestration rule:

- Go to **Orchestrate > Rules** and click **Add Rule**.



The image shows the "Rules" configuration page in a dark-themed interface. On the left is a sidebar with icons for "Investigate", "Orchestrate", and "Miragemaker". The main area has a header "Rules" with a subtitle "Rules to automate workflow, notifications, and containment in response to detections." Below the header, there are two buttons: "Pause orchestration" and "+ Add Rule". The "+ Add Rule" button is highlighted with a red rectangular border. Below the buttons is a table with columns: Priority, Name, Condition, Tasks, Type, and Actions.





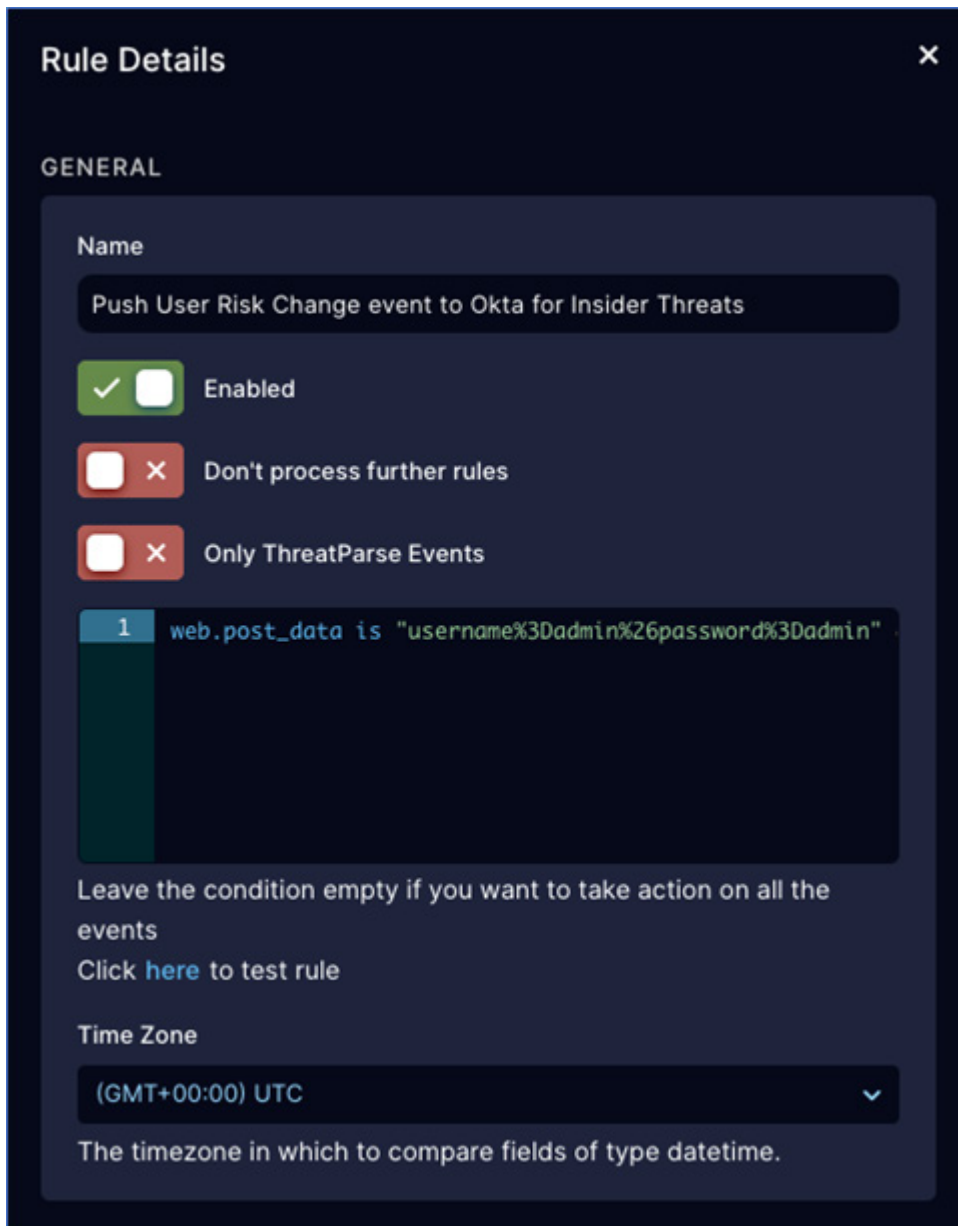
Priority	Name	Condition	Tasks	Type	Actions
1	QHYTR				 
				Internal	

Figure 138. Add Orchestration Rule

2. Enter the following in the **Rule Details** window:
  - a. A name in the **Name** field.
  - b. Select **Enabled**.
  - c. Create a rule to automate the containment of attackers. (See [Understanding and Building Queries](#) to learn more about writing queries.)



The screenshot shows the 'Rule Details' window with a dark theme. The 'GENERAL' tab is selected. The 'Name' field contains 'Push User Risk Change event to Okta for Insider Threats'. The 'Enabled' checkbox is checked. The 'Don't process further rules' and 'Only ThreatParse Events' checkboxes are unchecked. A single condition is listed: '1 web.post\_data is "username%3Dadmin%26password%3Dadmin"'. Below the conditions, there is a note: 'Leave the condition empty if you want to take action on all the events' and a link 'Click here to test rule'. The 'Time Zone' dropdown is set to '(GMT+00:00) UTC'.

**Rule Details** ✕

**GENERAL**

**Name**

Push User Risk Change event to Okta for Insider Threats

☒ Enabled

☐ ✕ Don't process further rules

☐ ✕ Only ThreatParse Events

1 web.post\_data is "username%3Dadmin%26password%3Dadmin"

Leave the condition empty if you want to take action on all the events

Click [here](#) to test rule

**Time Zone**

(GMT+00:00) UTC ▼

The timezone in which to compare fields of type datetime.

Figure 139. Rule Details

- d. Scroll to the **Okta (SSF)** section and select **Enabled**.
- e. Set **User Risk Level** to **High**.
- f. Enter a reason in the **Risk Change Reason** field to describe why the risk score changed. This reason is reflected in the Okta logs.
- g. Click **Save** to add the rule.

The screenshot shows a configuration window titled "OKTA (SSF)". At the top, there is a toggle switch labeled "Enabled" which is currently turned on, indicated by a green checkmark. Below this, the "User Risk Level" is set to "High" in a dropdown menu. The "Risk Change Reason" field contains the text "Zscaler detected a potential threat originating from this user." At the bottom right, there are two buttons: "Cancel" and "Save". The "Save" button is highlighted with a red rectangular box.

Figure 140. Enable Okta (SSF)

## Configure an Entity Risk Policy Rule

You can also define what Okta should do when it receives a risk signal about a user.

1. Return to the Okta administrator console.
2. Go to **Security > Entity Risk Policy** and click **Add rule**.

**Entity Risk Policy** [Documentation](#)

Configure automated responses to entity risk changes related to identity-based threats, like brute-force attacks, sign-in events from high-threat IP addresses, and residual session risk from session hijacking, etc.

**Add rule**

Priority	Rule	Status	Actions
1	<b>Catch-all Rule</b>  IF Group: Any Detection: Any Entity risk level: Any THEN No further action	ENABLED	Actions ▾

Figure 141. Entity Risk Policy rule

3. Enter the following in the **Add Rule** window:
  - a. A name in the **Rule name** field.
  - b. For **AND Detection**, select **Include at least one of the following detections**.
  - c. Select **Security Events Provider Reported Risk** from the **Detections** drop-down menu. This detection description is reflected in the Okta logs.
  - d. For **Then Take this action**, select **Logout and revoke tokens**.
4. Click **Save** to create the Risk Policy Rule.

### Add Rule

If all conditions are true, the entity risk settings will apply. Otherwise, Okta will evaluate the next rule. A maximum of 100 rules can be configured.

Rule name

Zscaler Reported User Risk Change

IF

IF User's group membership includes

Any group

AND Detection

Include at least one of the following detections:

Security Events Provider Reported Risk x

[Go to Detections](#)

AND Entity risk level

Any

THEN

THEN Take this action

☐ No further action

☒ Logout and revoke tokens

☐ Run a Workflow

Save

Cancel

Figure 142. Define rule

The status of your Risk Policy rule is **ENABLED**.

## Entity Risk Policy Documentation

Configure automated responses to entity risk changes related to identity-based threats, like brute-force attacks, sign-in events from high-threat IP addresses, and residual session risk from session hijacking, etc. Add rule

Priority	Rule	Status	Actions
1	<b>Zscaler Reported User Risk Change</b>  IF Group: Any THEN Logout and revoke tokens  Detection includes: Security Events Provider Reported Risk  Entity risk level: High	ENABLED	<span>Actions</span>
2	<b>Catch-all Rule</b>  IF Group: Any THEN No further action  Detection: Any  Entity risk level: Any	ENABLED	<span>Actions</span>

Figure 143. Risk Policy Enabled

## Reviewing Events

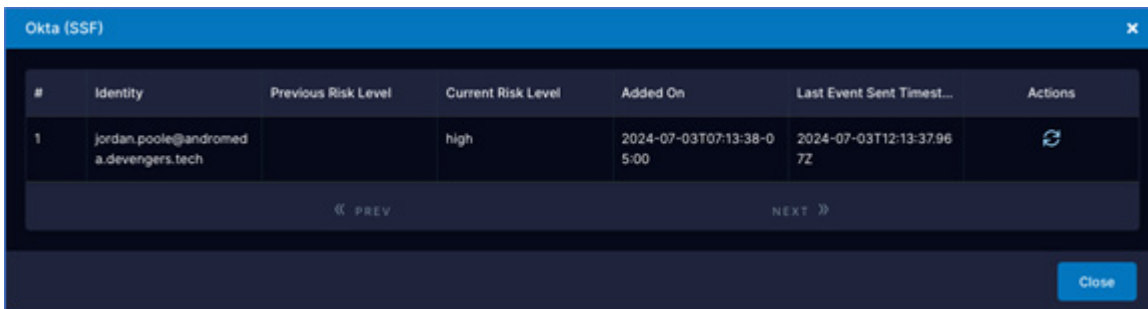
To review an event sent from Deception to Identity Threat Protection:

1. Return to the Deception Admin Portal.
2. Go to **Orchestrate** > **Containment** and click the number in the Okta (SSF) row under **Blocked Identities**.

#	Enabled	Settings	Blocked Identities	Actions
1	×	Zscaler Internet Access	0	<span></span>
2	×	Zscaler Private Access	0	<span></span>
3	×	Okta (SSF)	1	<span></span>

Figure 144. Select Containment Block

- Review details about the event such as the username and change in risk level.



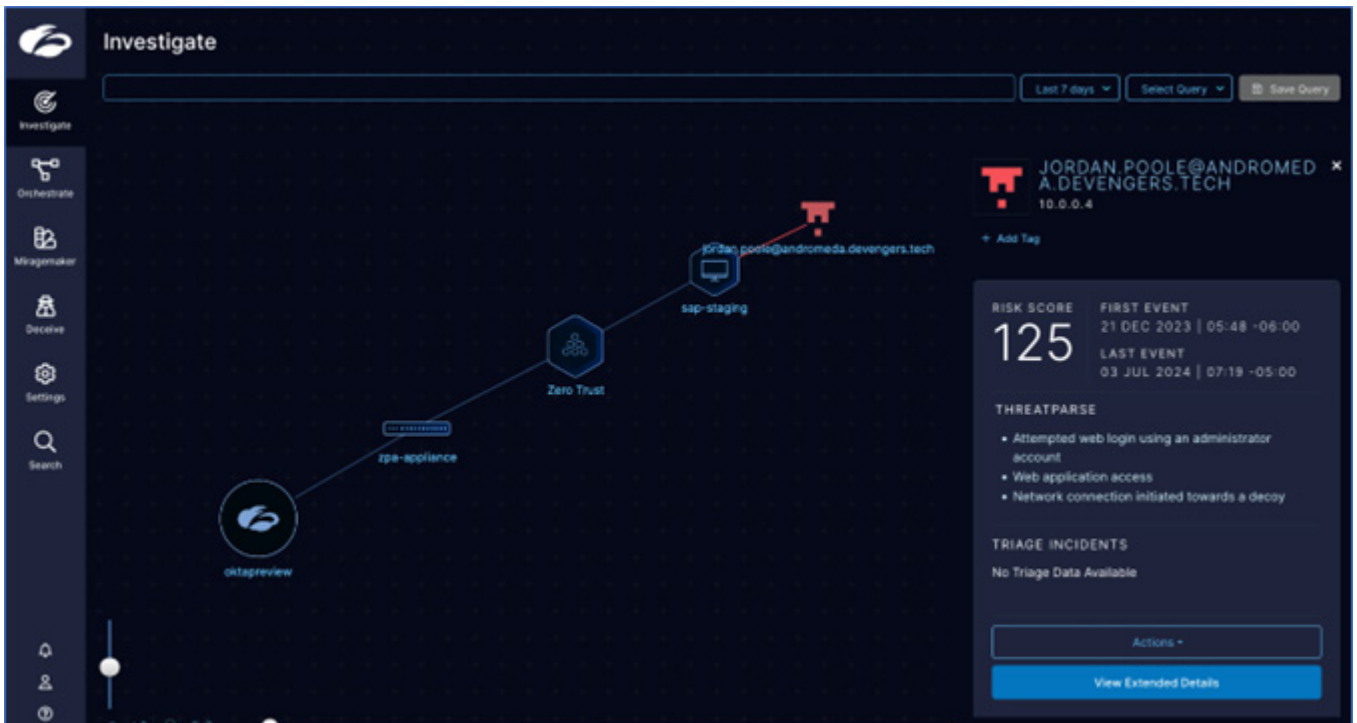
#	Identity	Previous Risk Level	Current Risk Level	Added On	Last Event Sent Timest...	Actions
1	jordan.poole@andromeda.developers.tech		high	2024-07-03T07:13:38-05:00	2024-07-03T12:13:37.967Z	

« PREV      NEXT »

Close

Figure 145. Review Containment Block

- Go to **Investigate** and click the user to review more details displayed on the right-side panel.



**Investigate**

Search:  Last 7 days Select Query Save Query

**JORDAN.POOLE@ANDROMEDA.DEVELOPERS.TECH**  
10.0.0.4

+ Add Tag

**RISK SCORE**  
**125**

**FIRST EVENT**  
21 DEC 2023 | 05:48 -06:00

**LAST EVENT**  
03 JUL 2024 | 07:19 -05:00

**THREATPARSE**

- Attempted web login using an administrator account
- Web application access
- Network connection initiated towards a decoy

**TRIAGE INCIDENTS**  
No Triage Data Available

Actions +

View Extended Details

Network Diagram: oktagreview → zpe-appliance → Zero Trust → sap-staging → jordan.poole@andromeda.developers.tech

Figure 146. Investigate incident

- (Optional) Review the Okta logs by returning to the Okta administrator console, and going to **Reports > System Log**.
- Enter the following in the **Search** field:  
`security.events.provider.receive_event`

7. Click the **Search** icon to search the logs.
8. Expand the log by clicking the arrow to the left of it.

### System Log

[← Back to Reports](#)

From

To

06/26/2024 00:00:00 07/03/2024 23:59:59 (GMT-5) Central Time - America/Chicago


Search

security.events.provider.receive\_event

Q Save

Advanced Filters / Reset Filters

#### Count of events over time



[Show event trends by category](#)

Events: 1

Download CSV

	Time	Actor	Event Info	Targets
🔍	Jul 03 07:13:38	https://zscaler.ssf.transmitter.smokescreen.io (Se...	Security events provider reported risk SUCCESS	Jordan Poole (User)

Figure 147. Search for event logs



The detection description **Security events provider reported risk** is displayed in the **Event > DisplayMessage** detail.

The screenshot shows the 'Events: 1' section with a 'Download CSV' link. The event table has columns: Time, Actor, Event Info, and Targets. The event details are expanded, showing a tree view on the left with 'Actor', 'Client', 'Event', 'AuthenticationContext', 'DisplayMessage', 'EventType', 'Outcome', 'Published', 'SecurityContext', 'Severity', 'System', 'Request', and 'Target'. The 'DisplayMessage' field is highlighted with a red box and contains the text 'Security events provider reported risk'. Other fields include 'Actor' (https://zscaler.ssf.transmitter.smokescreen.io), 'Client' (zscaler.ssf.transmitter.smokescreen.io), 'Event' (security.events.provider.receive\_event), 'Published' (2024-07-03T12:13:38.581Z), 'Severity' (INFO), 'System' (Transaction(id: faa177e09d097f3e18b853101e457420)), 'Request' (Jordan Poole (id: 00uabkkfdnK09DjkQ1d7)User), and 'Target' (Jordan Poole (User)).

Figure 148. Log detail

Your **Risk Change Reason** from the Deception Orchestration rule is displayed in the **System > DebugContext > DebugData > SecurityEventsProviderReportedRisk** detail.

The screenshot shows the 'System' section with a tree view on the left. The 'DebugContext' section is expanded, showing 'DebugData' with fields: 'DtHash' (45a903419f90f73a1e69dc3b7fd0dd3076d6c315bf7c6caa9404f0451bf3049), 'RequestId' (faa177e09d097f3e18b853101e457420), 'RequestUri' (/security/api/v1/security-events), 'SecurityEventsProviderReportedRisk' (highlighted with a red box), 'TraceId' (0cc4c115-7a7e-4614-a4f0-18c47c890d24), 'Url' (/security/api/v1/security-events?), 'LegacyEventType', 'Transaction', 'UUID' (adececb0-3935-11ef-9701-fd50fa4cc879), and 'Version' (0). The 'SecurityEventsProviderReportedRisk' field contains a JSON object: {"issuer": "https://zscaler.ssf.transmitter.smokescreen.io", "https://schemas.okta.com/secevent/okta/event-type/user-risk-change": {"subject": {"user": {"format": "email", "email": "jordan.poole@andromeda.devengers.tech"}}, "event\_timestamp": 1720008817, "reason\_admin": {"en": "Zscaler detected a potential threat originating from this user."}, "previous\_level": "none", "current\_level": "high"} } }.

Figure 149. Log System Debug detail

# Avalor Unified Vulnerability Management and Okta Integration

This guide provides prerequisites and instructions on configuring an integration between Okta and [Avalor Unified Vulnerability Management \(UVM\)](#). Avalor's Data Fabric and UVM solution ingests, normalizes, and unifies data across enterprise security and business systems to deliver actionable insights, analytics, and operational efficiencies. The following steps demonstrate how Avalor UVM can leverage Okta logs, combined with data from other sources, to contextualize and calculate personalized risk assessments for the organization.

## Overview

The Avalor UVM platform can ingest many Okta logs to aid in quantifying risk. For example, you can query the [Apps API](#) to retrieve which users are assigned specific applications. Should a vulnerability be identified within the organization, Avalor can adjust the associated potential risk based on which applications the user has access to. For instance, a Remote Code Exploit vulnerability might carry a lower risk if the affected asset is a test machine in an isolated network. However, the same vulnerability might have its risk rating dramatically increased if found on an asset that has a user logging into it with access to critical applications. By default, the solution pulls Okta [System Logs](#).

## Finding Your Okta Domain

To find your Okta domain:

1. Log in to the Okta administrator console.
2. Click your username in the upper right-side corner of the Okta administrator console. The domain appears in the drop-down menu. For domain examples, refer to the [Okta documentation](#).

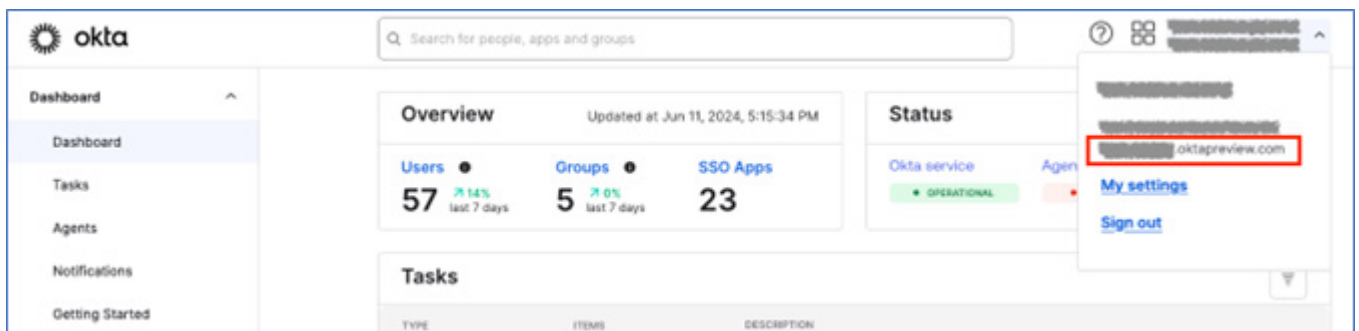


Figure 150. Find your Okta domain

## Create API Token

To configure the API Key for Avalor:

1. Go to the **Security** tab of the Okta administrator console.
2. Click **API**.
3. Click the **Tokens** tab in the **API** window.
4. Click **Create Token**.
5. Enter a name and select **Any IP** from the drop-down menu.
6. Click **Create token**.

✕

### Create token

What do you want your token to be named?

Avalor

The token name is used for tracking API calls.

API calls made with this token must originate from

Any IP

Create token
Cancel

Figure 151. Create token

7. Copy the **Token Value** that appears to a secure location, then click **OK, got it**.

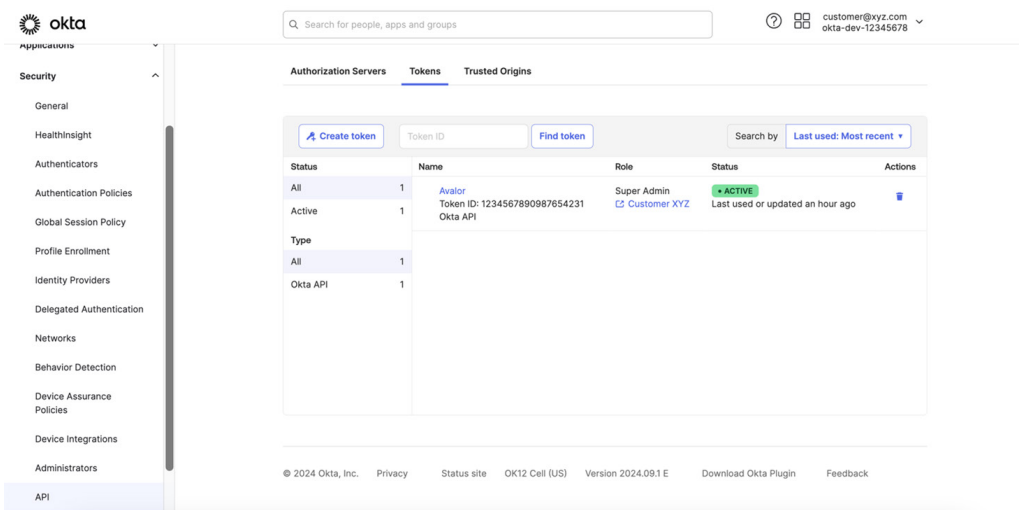


Figure 152. Token created

## Configure the Avalor Data Connector

To configure the integration between Avalor and Okta:

1. Log in to the Avalor UVM Dashboard.
2. Go to the **Configure Data Sources** window by clicking the **Options** icon (the gear) in the upper right.

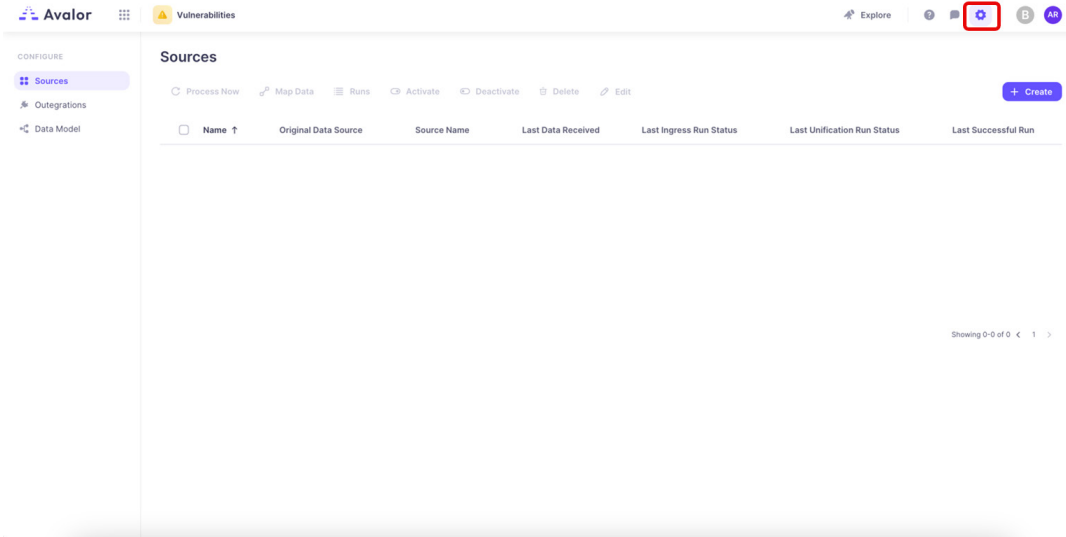


Figure 153. Configure Data Sources

3. Click **Create** and search for Okta in the search filter.

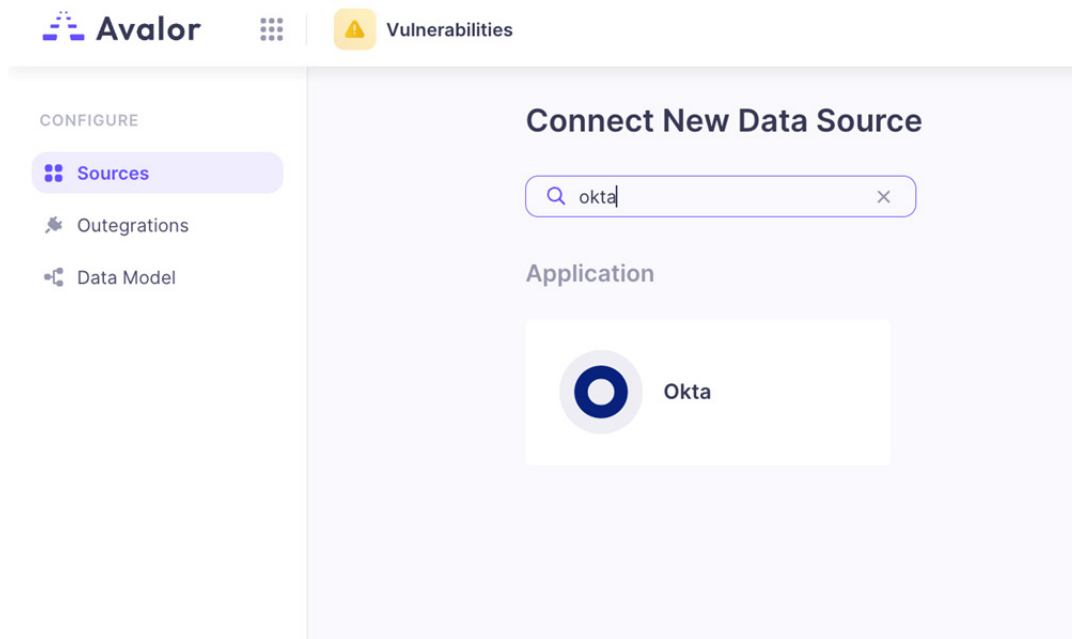


Figure 154. Connect New Data Source

4. Click the **Okta** tile.
  - a. Enter a **Name** for the connector and toggle the **Active** slider to enable the connector.
  - b. In the **Okta domain** field, enter your Okta domain.
  - c. In the **Okta url** field, enter your Okta URL.
  - d. In the **API token** field, enter your API token that you copied [previously](#).

Figure 155. Configure Data Connector

## Review and Adjust Data Model Mapping

Avalor UVM automatically maps ingested data to the default Data Model, so analysis can begin immediately. However, many data sources also provide additional data points that might provide additional context to risk prioritization.

The following example shows how to map additional Okta data into the data model so that you can use it to provide additional context when evaluating risk. From the Avalor UVM Sources page:

1. Select the Okta connector configured in the previous section.
2. Click **Map Data**.

Name	Original Data Source	Source Name	Last Data Received	Last Ingress Run Status	Last Unification Run Status	Last Successful Run
Okta connector	Okta	Okta	10/8/2024, 9:00:03 AM	Success	Success	10/8/2024, 9:31:20 AM

Figure 156. Map Data

3. In the **Map Okta connector** window:
  - a. Review the ingested data fields in the left-side column.
  - b. Review the **Entities** in the right-side column.
  - c. (Optional) Click **Add Entity** to create a custom entity within the **Data Model** to map to.
  - d. Review the default mappings in the center column.
  - e. In preparation for the following example, map the **actor.alternateId** field from the Okta data source to the **OrgEntity.Key** field.

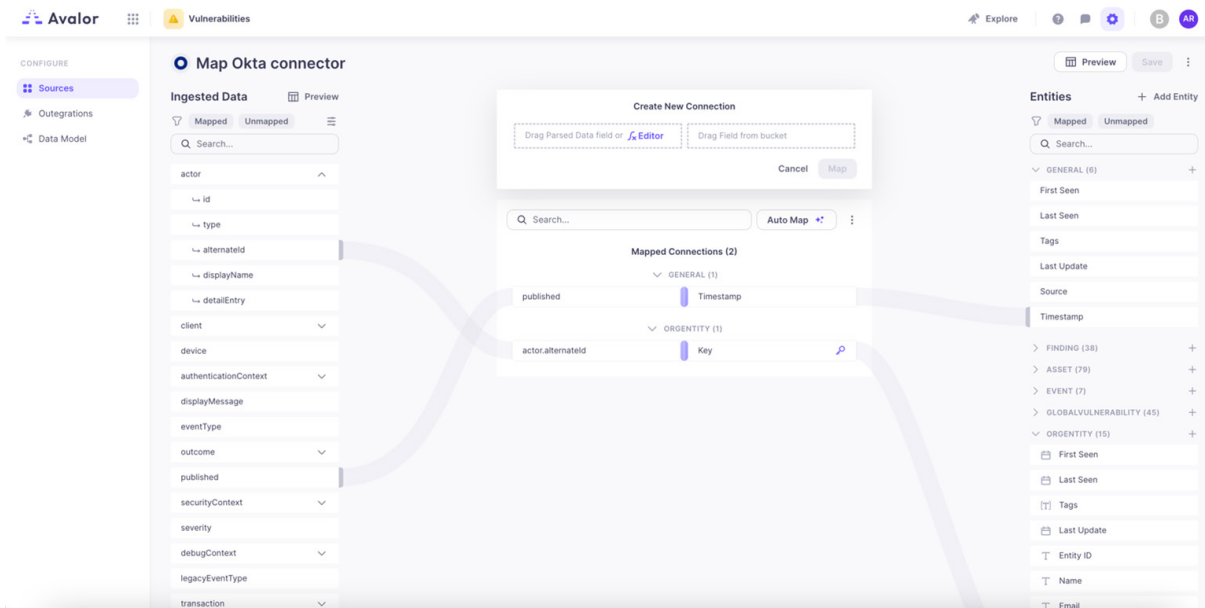


Figure 157. Map Okta Connector

- f. (Optional) Click **Auto Map** to allow the software to automatically map additional fields to the Data Model.
- g. (Optional) Click **Preview** to review the updated Data Model mappings.
- h. Click **Save**.

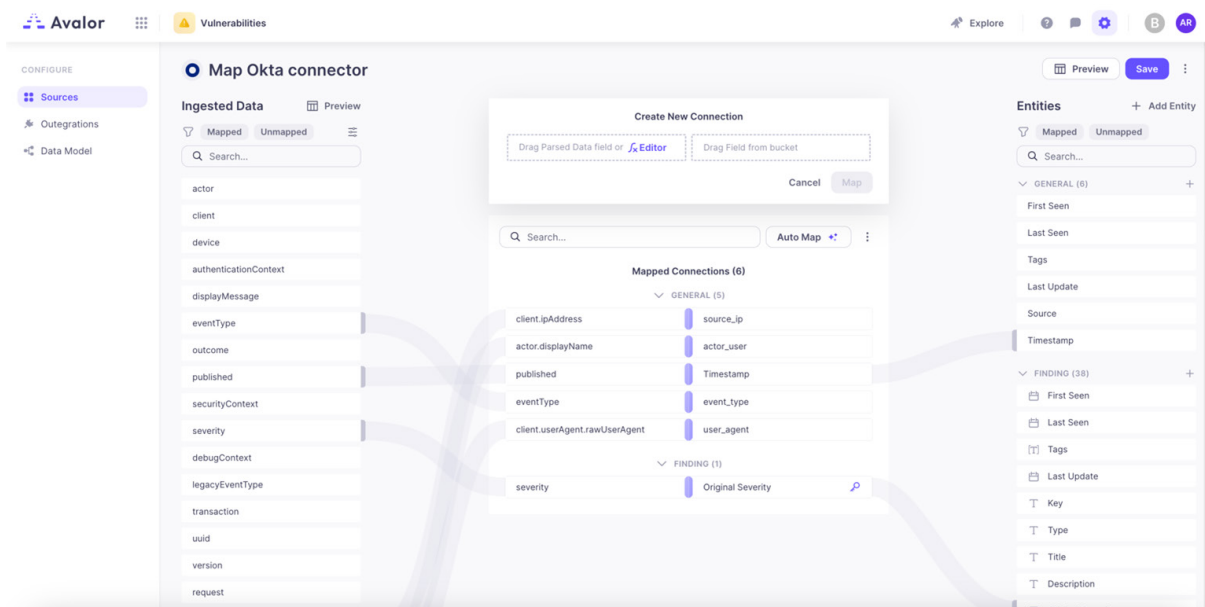


Figure 158. Data Mapping

- On the **Sources** page, select the Okta connector and click **Process Now**.

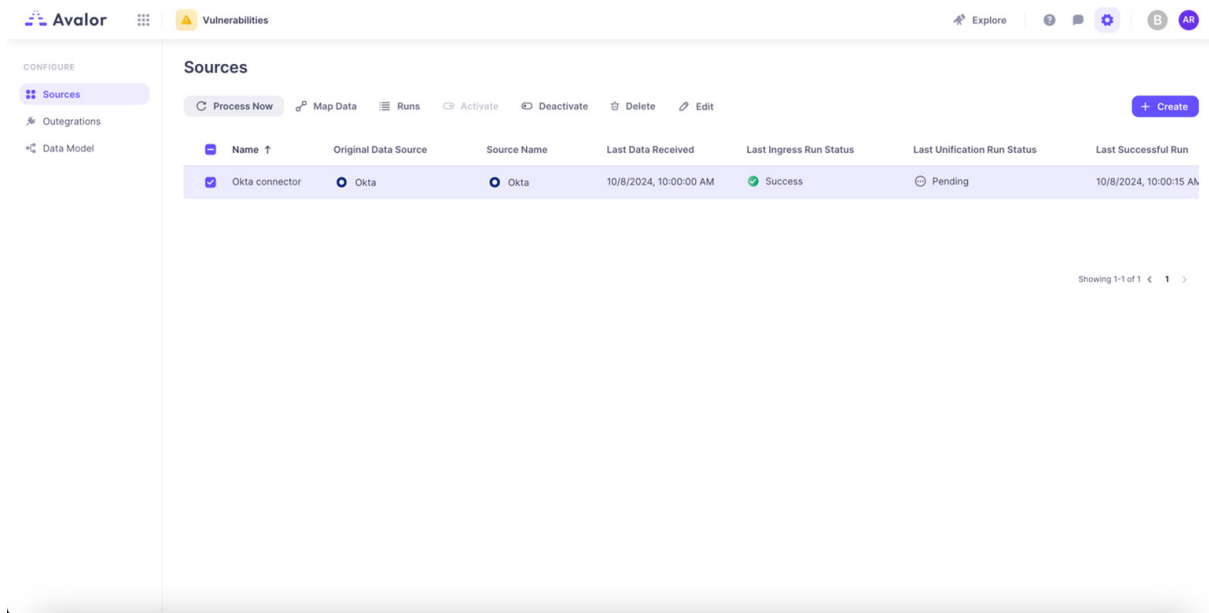


Figure 159. Process Now

## Review and Adjust Risk Scoring

After ingested data has been normalized and mapped to the Data Model, Avalor UVM evaluates the risk.

The following example shows how you can ingest a custom data source (AnySource) to identify which users have access to critical applications. Having this additional context allows the UVM application to apply user access context against vulnerability findings. You then create a Risk Factor that raises the assets vulnerability score if the owner of that asset has a value of True for access to critical applications. A value of False leaves the risk calculation unaffected.

From the **Data Sources** tab in the Avalor dashboard:

- Click **Create** and search for the **AnySource** connector.
- For this example, prepare a CSV file that identifies which users have access to critical applications (you can pull user application lists directly from the Okta API, should you want to automate this step). For example:

Email	CriticalAppAccess
User1@customer.com	True
User2@customer.com	True
User3@customer.com	True

- Enter a name for the connector and toggle the **Active** slider to enable the connector.
- For the **Retrieval**, select **Upload File**.
- Upload the CSV file created previously.

The screenshot displays the 'Create AnySource Source' configuration page in the Avalor application. The interface is divided into a left sidebar and a main content area. The sidebar, under the 'CONFIGURE' section, includes links for 'Sources', 'Outegrations', and 'Data Model'. The main content area is titled 'Create AnySource Source' and contains two sections: 'Details' and 'Retrieval'.

**Details Section:**

- Name:** A text input field containing 'Critical App Access'.
- Source Name:** A dropdown menu with 'AnySource' selected.
- Description:** An empty text input field.
- Active:** A toggle switch that is currently turned on.

**Retrieval Section:**

- Method:** A dropdown menu with 'Upload File' selected.
- Parser Type:** A dropdown menu with 'Auto' selected.
- File Upload:** A large dashed blue box containing a cloud icon with an upward arrow and the text 'DRAG & DROP files here, or Browse'. Above this box, a checkmark and the text 'Uploaded applist.csv' indicate a successful upload.
- Accepted File Types:** A small text label at the bottom of the upload area listing 'JSON, JSONL, CSV, ZIP, XML, ZST, ZSTD'.

**Navigation and Footer:**

- Back:** A button with a left arrow and the text 'Back'.
- Progress Indicators:** A series of four dots representing steps: 'Connect' (active), 'Preview', 'Mapping', and 'Mapping Preview'.
- Buttons:** 'Cancel' and 'Next' (with a right arrow) buttons.

Figure 160. Upload CSV file



6. Click **Next** and review the imported data for accuracy.
7. Click **Map**.
8. In the mapping screen, map the **Owner/E-mail** field to the **OrgEntity.Key** field.
9. In the **OrgEntity Entity**, click **Add (+)** to create a new field.
  - a. Enter **Access to Critical Apps** or similar as the **Field Name**.
  - b. Choose **Boolean** as the **Field Type**.
  - c. Click **Add**.

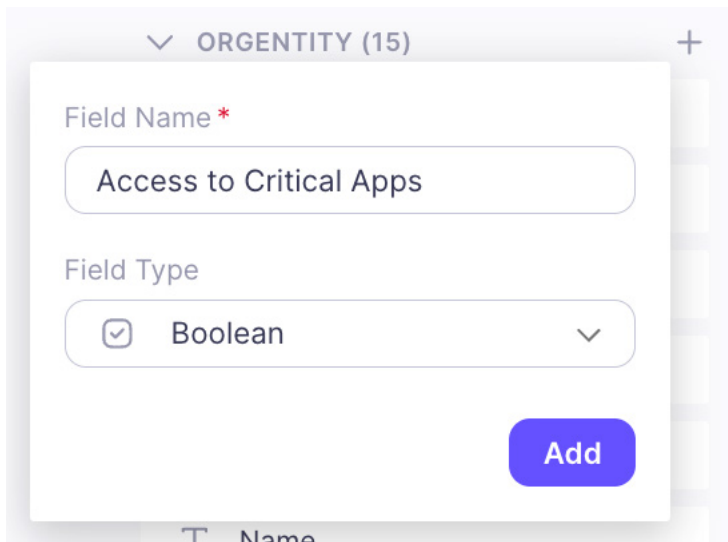


Figure 161. Add OrgEntity

10. Map the **CriticalAppAccess** field to the newly created **OrgEntity Access to Critical Apps** field.

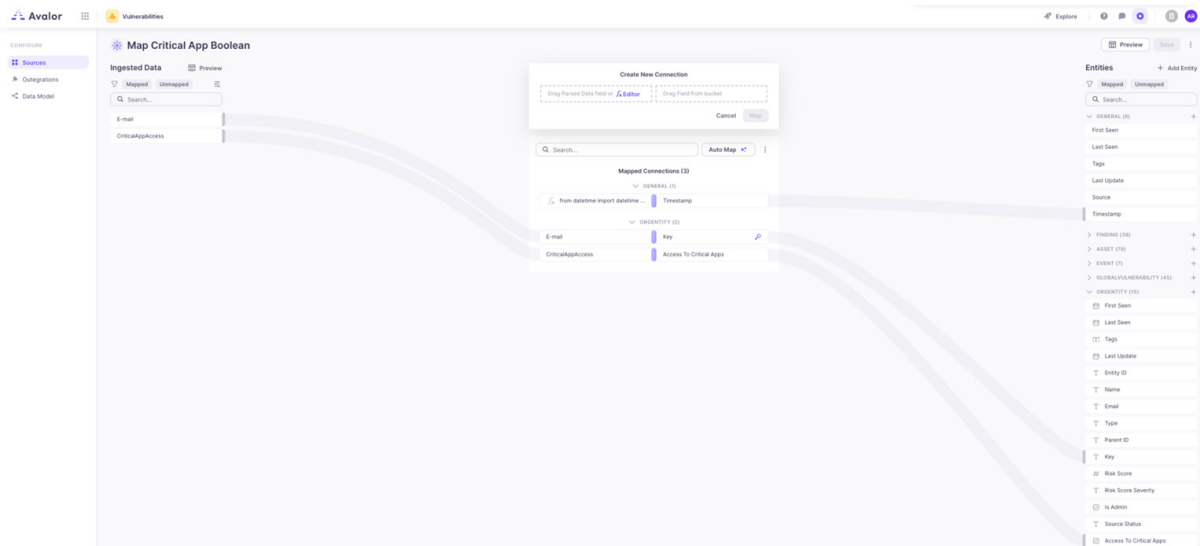


Figure 162. New mapping

11. Click **Save**.
12. Highlight the new **AnySource** connector and click **Process Now**.

Next, you must ensure that the Asset owner information is ingested correctly and mapped to the user information being pulled from Okta so that you can leverage this data in risk scoring.

From the **Data Sources** tab in the Avalor dashboard:

1. Locate the data source that provides asset Owner ID information such as ServiceNow, Microsoft Intune, etc.
2. Select the data source and click **Mapping**.
3. Ensure that the User ID field (for the user that owns the asset) from this data source is mapped to the Asset OwnerID field of the Data Model. In the following example, Microsoft Intune is shown with necessary mapping:

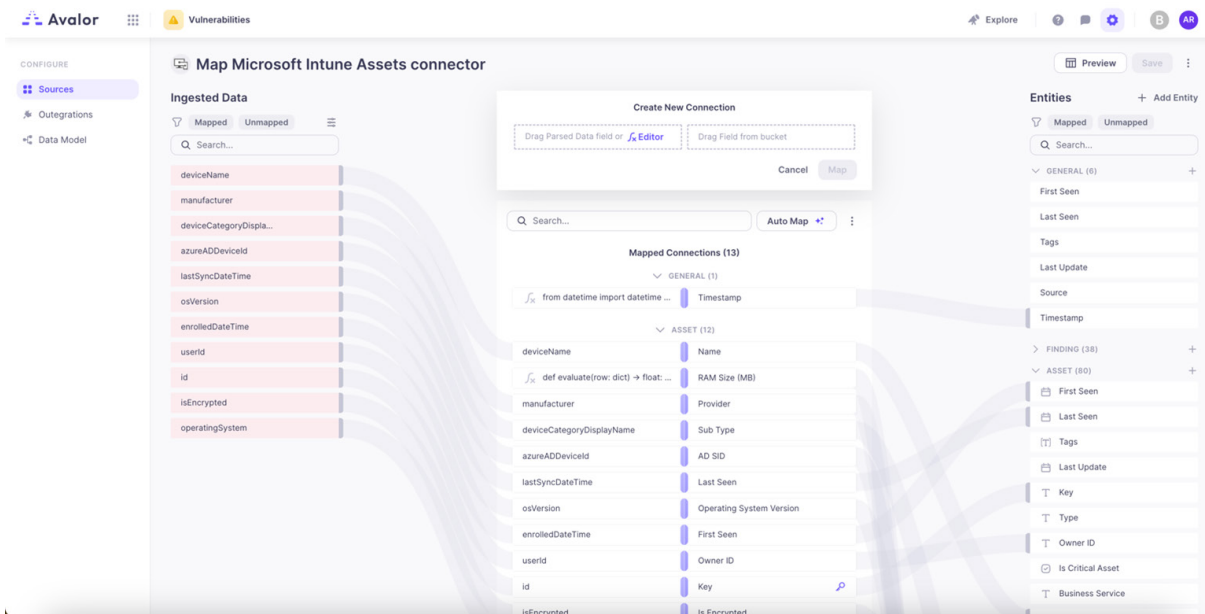


Figure 163. Map Microsoft Intune Assets connector

Next, create a custom field in the Asset entity to adjust risk scoring based on ingested data.

From the **Data Sources** page:

1. Click the **Data Model** tab in the left-side navigation.
2. Click **Add (+)** next to the **Asset Entity**.
  - a. For **Field Name**, enter a name such as `Owner Access to Critical Apps`.
  - b. For **Field Type**, choose **Boolean**.
  - c. Click **Add**.

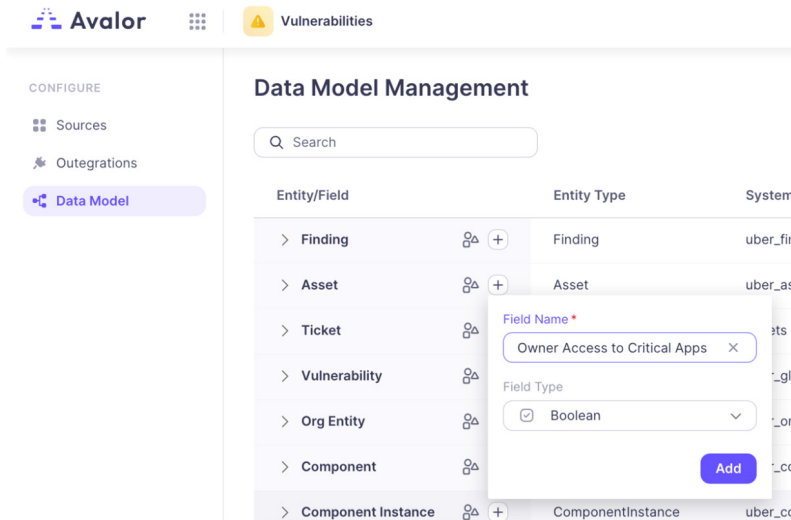


Figure 164. Data Model Management

Finally, set a Risk Factor to manipulate risk based on the data collected and analyzed. From the **Vulnerabilities** tab in the Avalor dashboard (Remediation Hub):

1. Click the **Settings** drop-down menu in the left-side navigation.
2. Click **Score**.
3. Click **Add Factor**.
  - a. Select **Risk Factors** as the **Factor Type**.
  - b. Enter a name, such as **Owner Access to Critical Apps**.
  - c. In the **Field** drop-down, select the **Owner Access to Critical Apps** field under the **Asset Entity**.
  - d. In the **True** field, enter the percentage to increase risk when the user evaluates to **True**.
  - e. Click **Apply**.

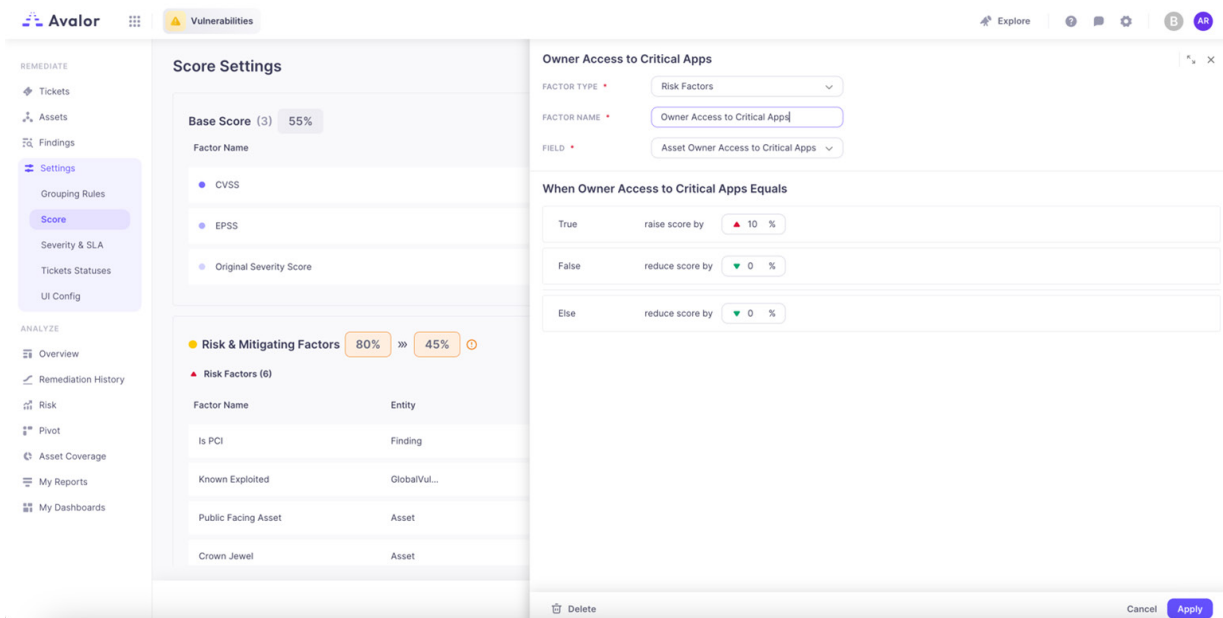


Figure 165. Vulnerabilities tab

- Go to the **Assets** tab in the left-side navigation.
- Click one of your assets (it might take some time for the UVM application to process findings and update scoring).
- Click the **Findings** tab to review the asset's score. (In the following example, note how the score was elevated by 10% due to the owner having access to critical apps.)

**Asset MacBook-Pro.local**ID / 1   

First Seen: Jun 23 2024, 7:00 PM (4 months ago)

 **10.0** CRITICAL


Details

Asset Merging




**Findings (591)**

Tickets (1)

### Findings


Severity score ▾ Original Severity Score ▾ State ▾ + More Clear Filters

591 found

<input type="checkbox"/>	SEVERITY ▾	ORIGINAL SEVERITY SCORE	STATUS ▴	SOURCE	FIRST SEEN	LAST SE
<input type="checkbox"/>	 <b>10.0</b> Critical	 <b>10.0</b> Critical	Active		5/16/2024, 6:12:36 PM	8/5/2024

**DESCRIPTION**

An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sonoma 14. A sandboxed process may be able to restrictions.


**FIX**

Update Apple Mac OS 12 to version 14.0 or newer

**AVALOR SCORE WAS DEFINED CONSIDERING:**

Base Score	Value	Score Share %	Score Change
Original Severity Score	10.0	+90%	+9.0
CVSS, EPSS		0%	0

Score Adjustments	Value	Score Share %	Score Change
Access to Critical Apps	True	+10%	+1.0
Is PCI, Known Exploited, Public...		0%	0

**Final Score**  **10.0** Critical

Showing 1-20 of 591 < 1 2 3 4 5 ... 30 >

Figure 166. Assets tab

## Transparent SSO Using IWA with Okta

Take advantage of IWA for transparent authentication when using Okta and Zscaler if it has been configured for the Okta environment. IWA works between Okta and the Windows Active Directory (AD) Server.

IWA is a Microsoft feature that allows a user to automatically authenticate using the users' Windows Active Directory authentication credentials. IWA works in an Okta environment by using either the Okta Desktop or the Okta IWA Web App that runs on an IIS server in your domain. For a demonstration of using IWA in an Okta environment, see [Mark Ryan's IWA and Okta Demonstration](#).

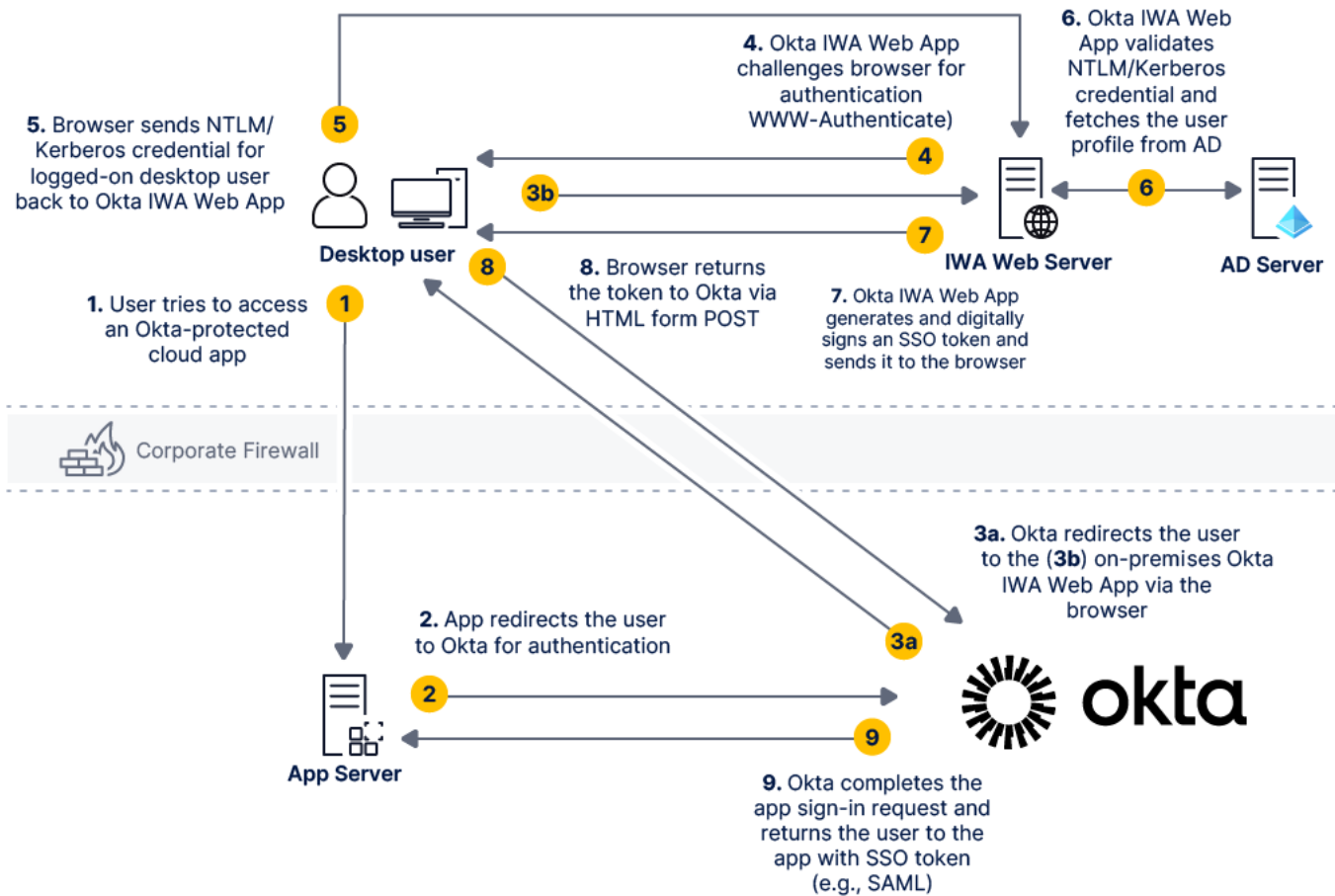


Figure 167. Okta IWA Web Server authentication flow

## PAC File and Zscaler Client Connector: Authentication Bypasses

When using ZIA, successful authentication requires you to bypass the IdP provider login URLs. It isn't required for ZPA. The destination URLs can flow through ZIA, but bypassing the URLs for ZIA is a requirement for both browser PAC files and for the Zscaler Client Connector.

You must bypass the IdP provider login URLs in your browser PAC and the Zscaler Client Connector custom PAC file for the application profile:

PAC File Bypasses:

```
// Okta Authentication Bypass

if (
  dnsDomainIs(host, ".okta.com") ||
  dnsDomainIs(host, ".oktacdn.com") ||
  dnsDomainIs(host, ".oktapreview.com"))
  return "DIRECT";
```

## Appendix A: Capture the SAML Request for Troubleshooting

Troubleshooting SAML can be challenging. The procedures find and decode the SAML assertion to look at the attributes returned by the IdP. These steps capture the assertion by using the Developer Tools for the browser, and then decoding it using a Base64 decoder on the desktop. This is the most secure method. You can use browser extensions, and/or cloud-based Base64 decoders. When clear text passwords are present in the data, it's always more secure to keep things in-house.

You can use any browser to capture the SAML assertion. The procedures for the most common browsers are in the next sections.

### How to View a SAML Response in Your Browser for Troubleshooting

Retrieving your service provider SAML response in your browser can help you troubleshoot SSO login issues.

#### Google Chrome: To View a SAML Response in Chrome

1. Press **F12** to start the developer console.
2. Select the **Network** tab, and then select **Preserve** log.
3. Reproduce the issue.
4. Look for a POST SAML in the developer console pane. Select that row, and then view the Headers tab at the bottom. Look for the SAML Response attribute that contains the encoded request.



The SAMLResponse attribute contains the encoded request. Use a Base64 decoder to investigate the decoded response.

#### Mozilla Firefox: To View a SAML Response in Firefox

1. Press **F12** to start the developer console.
2. In the upper-right of the developer tools window, click the **Options** icon (the gear).
3. Under **Common Preferences**, select **Enable persistent logs**.
4. Select the **Network** tab.
5. Reproduce the issue.
6. Look for a POST SAML in the table. Select that row. In the **Form Data** window on the right, select the **Params** tab and find the **SAMLResponse** element.



The SAMLResponse attribute contains the encoded request. Use a Base64 decoder to investigate the decoded response.



## Apple Safari: To View a SAML Response in Safari

1. Enable **Web Inspector** in Safari. Open the **Preferences** window, tap the **Advanced** tab, and then tap **Show Develop** in the menu bar.
2. Open **Web Inspector**. Click **Develop**, then tap **Show Web Inspector**.
3. Tap the **Resources** tab.
4. Reproduce the issue.
5. Look for a POST method with a **samlconsumer** file in the table.
6. Scroll down to find **Request Data** with the name SAMLResponse.



The SAMLResponse attribute contains the encoded request. Use a Base64 decoder to investigate the decoded response.

## Microsoft Windows: To View a SAML Response in Windows

The best way to analyze network traffic in Windows is through a third-party tool called Fiddler. To download and install Fiddler and capture the data, follow the steps at:

<https://www.telerik.com/download/fiddler>

### What to do with the Base64-Encoded SAML Response

After you find the Base64-encoded SAML response element in your browser, copy it, and use your favorite Base64 decoding tool to extract the XML tagged response.

### Security Tip

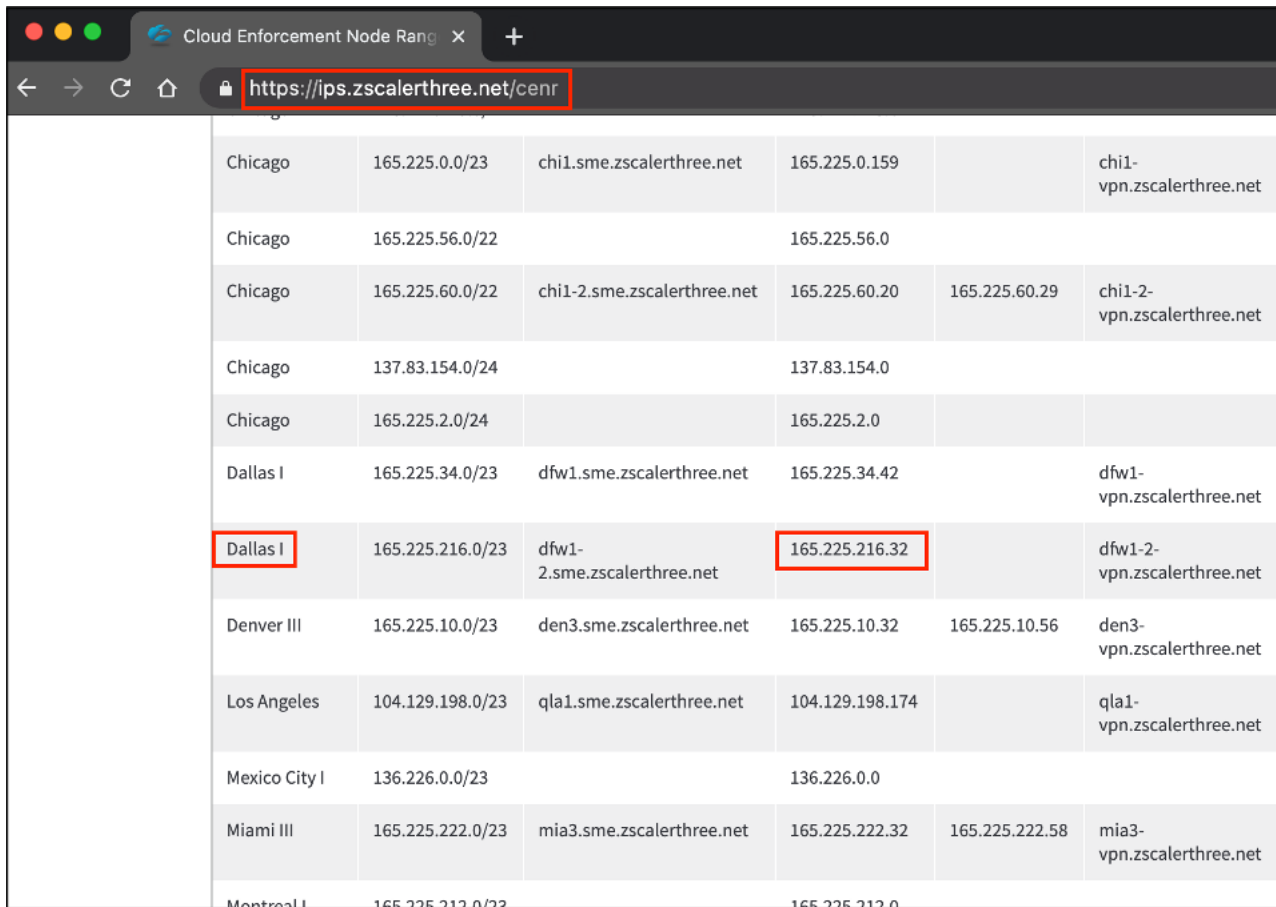
The SAML response data might contain sensitive security data. Zscaler recommends that you do not use an online Base64 decoder. Instead, use a tool installed on your local system.

## Configure Your Browser to Capture the SAML Response

Configure Zscaler as a proxy for your Google Chrome browser. You can configure the automatic FQDN to select the fastest gateway response as the proxy. The FQDN is `gateway.zscalerthree.net`, where `zscalerthree` is replaced by your cloud (e.g., `gateway.zscloud.net`, `gateway.zscalertwo.net`, etc.).

For this exercise, manually select the proxy from the list of Public Service Edges:

1. Enter your cloud's information center. The URL is `ips.zscalerthree.net/cenr`, for example. This lists the Public Service Edges for the Zscalerthree cloud. The Dallas IP is used as the proxy address defined in the browser.



Chicago	165.225.0.0/23	chi1.sme.zscalerthree.net	165.225.0.159		chi1-vpn.zscalerthree.net
Chicago	165.225.56.0/22		165.225.56.0		
Chicago	165.225.60.0/22	chi1-2.sme.zscalerthree.net	165.225.60.20	165.225.60.29	chi1-2-vpn.zscalerthree.net
Chicago	137.83.154.0/24		137.83.154.0		
Chicago	165.225.2.0/24		165.225.2.0		
Dallas I	165.225.34.0/23	dfw1.sme.zscalerthree.net	165.225.34.42		dfw1-vpn.zscalerthree.net
Dallas I	165.225.216.0/23	dfw1-2.sme.zscalerthree.net	165.225.216.32		dfw1-2-vpn.zscalerthree.net
Denver III	165.225.10.0/23	den3.sme.zscalerthree.net	165.225.10.32	165.225.10.56	den3-vpn.zscalerthree.net
Los Angeles	104.129.198.0/23	qla1.sme.zscalerthree.net	104.129.198.174		qla1-vpn.zscalerthree.net
Mexico City I	136.226.0.0/23		136.226.0.0		
Miami III	165.225.222.0/23	mia3.sme.zscalerthree.net	165.225.222.32	165.225.222.58	mia3-vpn.zscalerthree.net
Montreal I	165.225.212.0/23		165.225.212.0		

Figure 168. Select a test proxy

- Open the **Proxy Configuration** window for your test browser and enter the proxy IP address you just copied. You must also enter the Azure Active Directory domains as bypasses so the request makes it to Azure Active Directory and isn't blocked by ZIA. The three Azure Active Directory domains to bypass are `login.microsoftonline.com`, `config.microsoftonline-p.net`, and `*.autodiscover.testmypacket.com`. Save the changes. You are now ready to test.

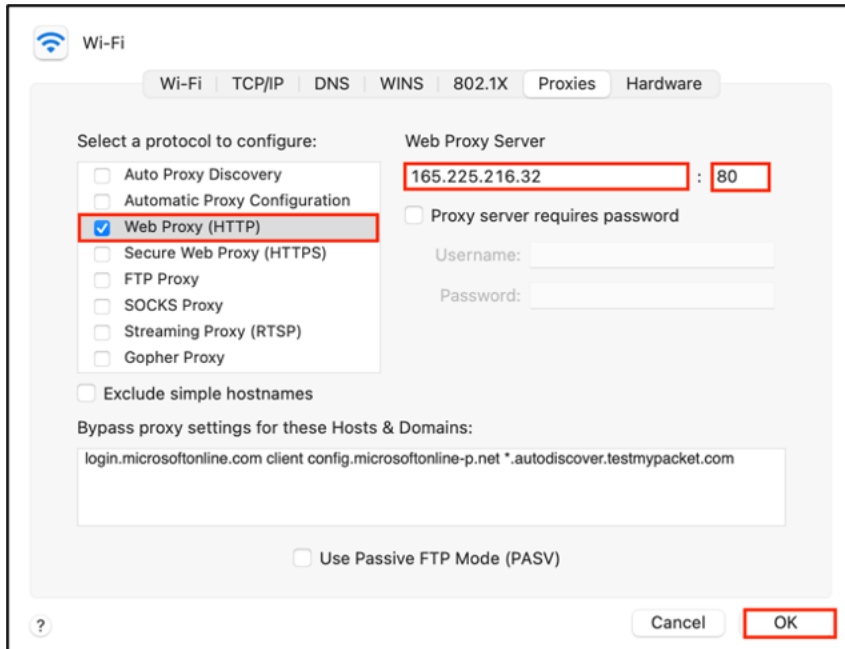


Figure 169. Setting your browser proxy settings

- Enter any URL in the browser, and ZIA prompts you for authentication credentials.
- Start your developer tools.
- Select the **Kebab** icon (vertical ellipsis) at the top-right of the browser to open the command menu.
- Select **More Tools**.
- Select **Developer Tools**.

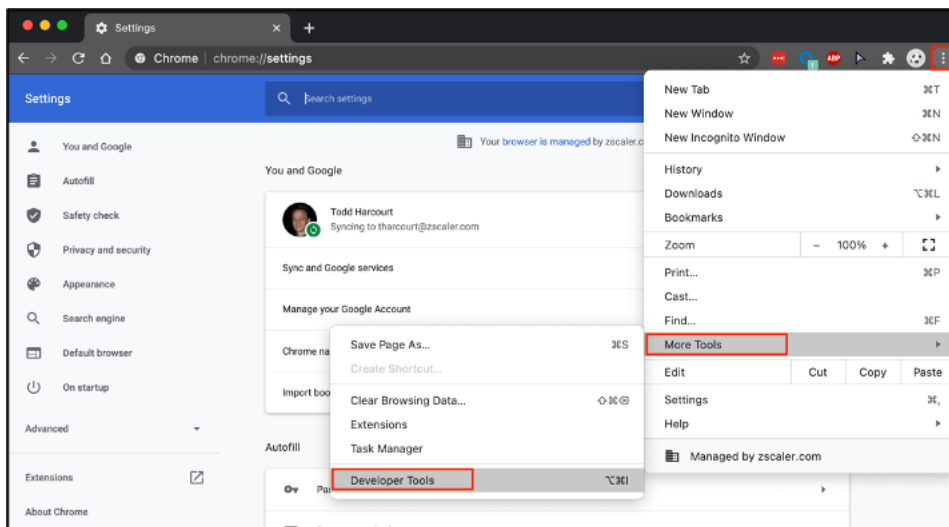


Figure 170. Selecting developer tools

The network trace shows you the connection and packet information as it authenticates into Zscaler and Azure Active Directory. The initial authentication window is only looking for the user domain appended to the User ID, so Zscaler knows which Zscaler instance to which to direct the request. In this case, it is `testmypacket.com`. Zscaler redirects the authentication request to Azure Active Directory.

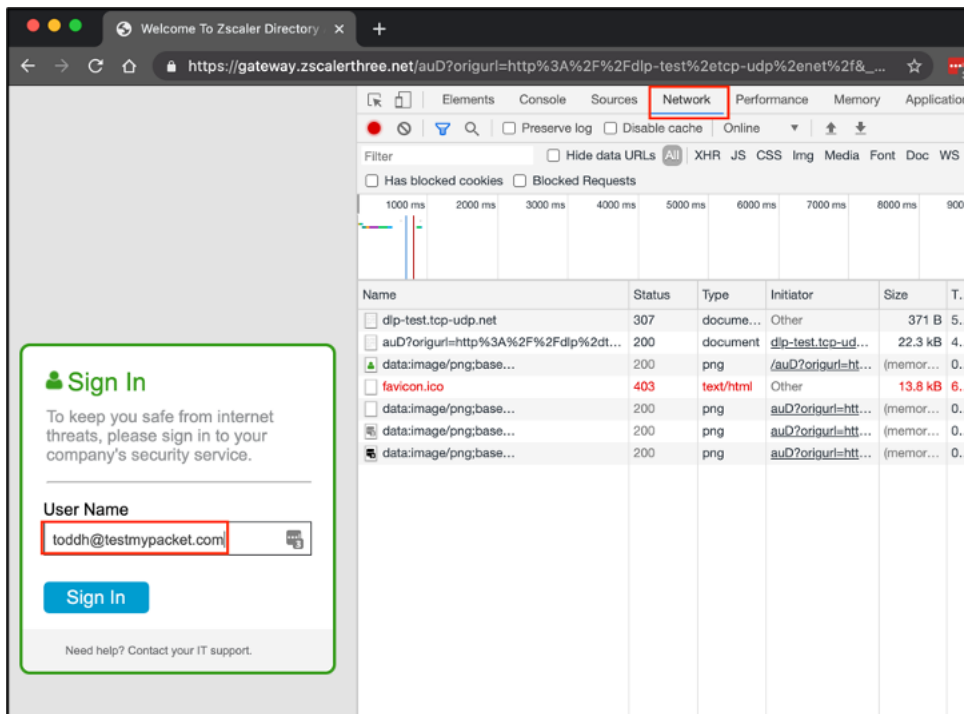


Figure 171. Capturing the SAML request

8. On the Azure Active Directory authentication window, log in with a valid user ID in the Azure Active Directory database associated with the Zscaler instance.

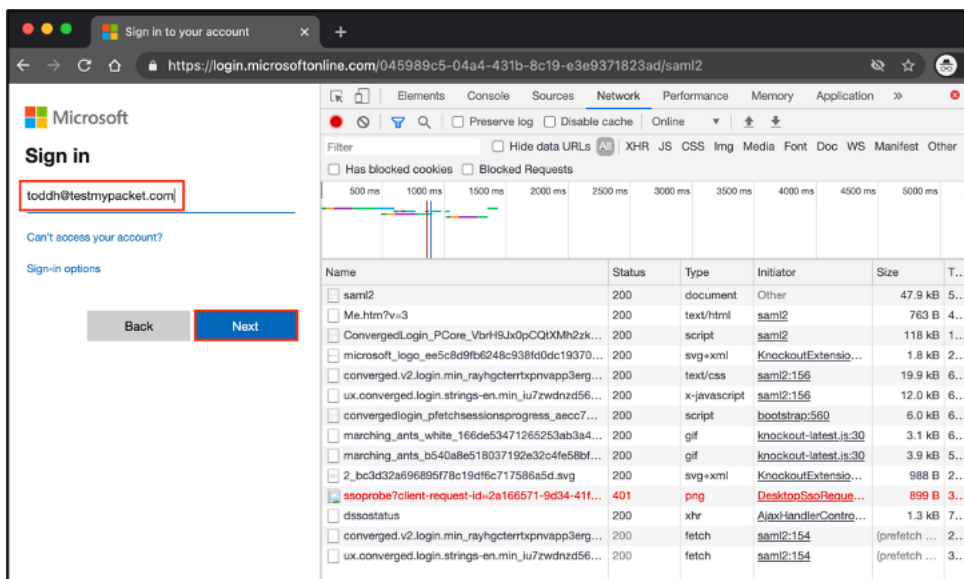


Figure 172. Authenticate to the Azure Active Directory IdP

- After authentication has completed, select the **sfc\_sso** packet destined to login.zscalerthree.net. This is the SAML response from Azure Active Directory and contains the SAML assertion. The assertion is Base64-encoded and you must use a decoder to get the clear text information. Select the SAML response data.

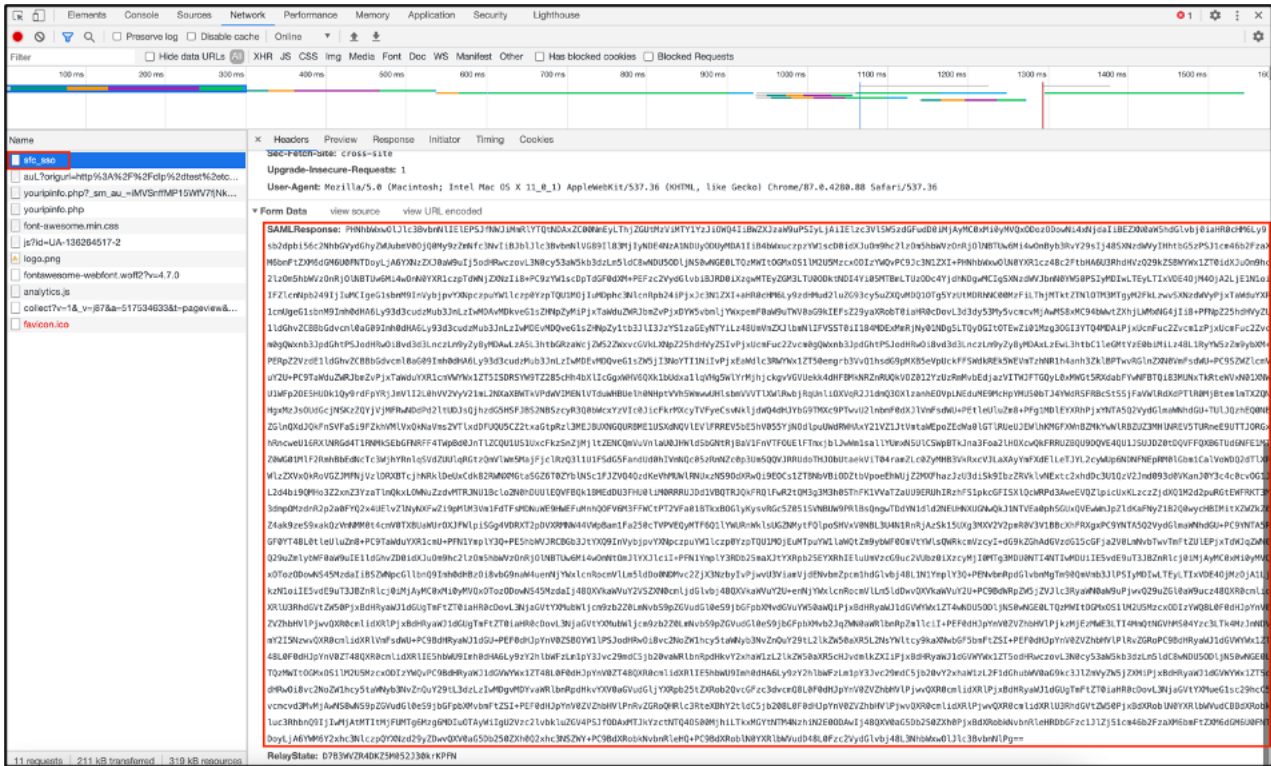


Figure 173. SAML response containing the assertion

10. Using a Base64 decoder, paste the encoded text into the application and then copy the decoded SAML assertion. For this demonstration, the Base64Anywhere app was downloaded free from the App Store for Mac. There are also free decoders in the Windows store if you are a Microsoft user, and command line options. For example, for macOS, you can use a CLI command `base64 -D data` to decode the assertion.

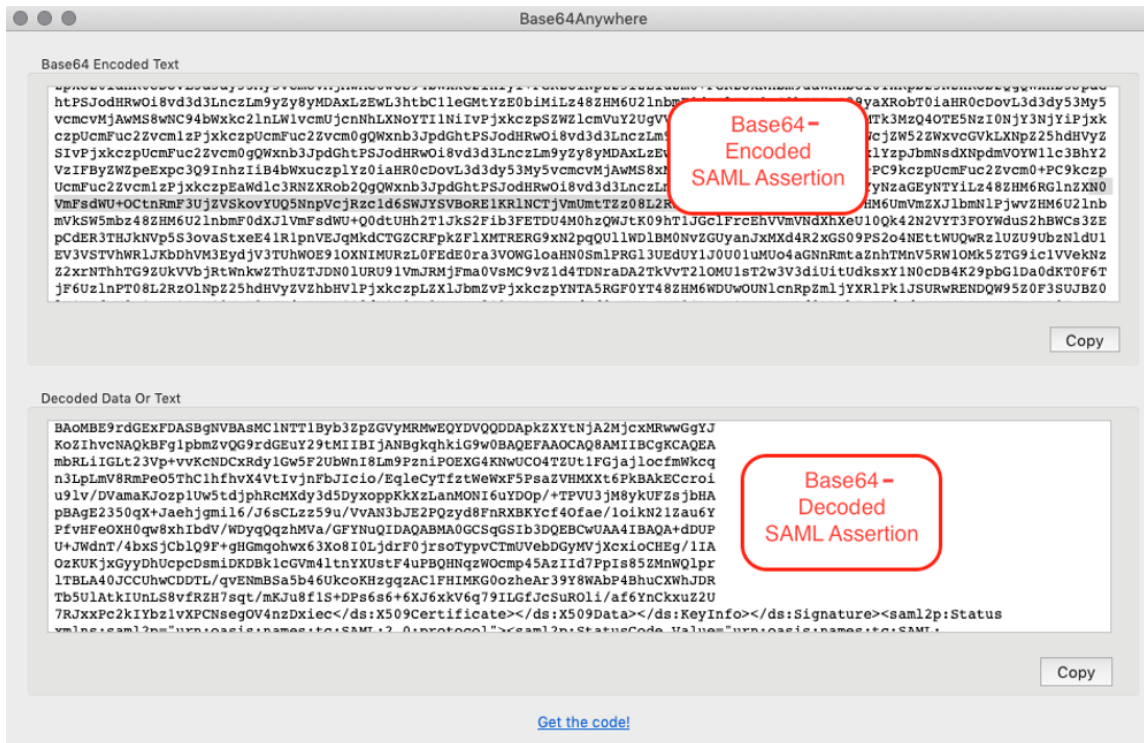


Figure 174. Decoding the Base64-encoded assertion



11. See the clear text assertion with the NameID of the user and other attributes. In this example, the user is part of a group called **Everyone**. All groups and attributes associated with the user are seen in this response.

```
<?xml version="1.0" encoding="UTF-8"?><saml2p:Response ID="id121708133819734891972466766"
InResponseTo="_6409506983574799128" IssueInstant="2020-08-13T19:27:17.996Z" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xs="http://www.w3.org/2001/
XMLSchema"><saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">exksledki8oMrgEVy0h7</saml2:Issuer><ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ds:SignatureMethod Algorithm="http://
www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:Reference
URI="#id121708133819734891972466766"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/
2000/09/xmldsig#enveloped-signature"/><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"><ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></
ds:Transform></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/
><ds:DigestValue>8-gFawR6UJJ/aD96zUr4ssWzIbXIPhDMJFSBN5fRkSg=</ds:DigestValue></ds:Reference></
ds:SignedInfo><ds:SignatureValue>CGmPxv0RdKaboqDL583HsAbm+0aORFrQkpHUVeMuxWymtBN67eX0qNagnKhAX+7dJBtD
wLrd5ZyKz/
i+qxN5GZgTbJ2GBLfBDZddYw14DDoq7jjAIE9A3Code2jrq1wxGLFK00Kj84KMYD0G9Te0To3euMDWuRMXVFRJl8U3q2v5wMHV80
u9sH1Ds/
ADtM+kuNXihstJi0DiwPGTcRtSMN1J8hcgFkZfxS2uyEmN2NYLobsUUzCsglk58aLoYREUn4mZy0e8Te2C7ITE0uVbQ21fkEl0/
ogWxL3kh06NEo0iN1M10L7WwBr+TvK1cStp0x+oilMckGJOAZN1zS9g==</
ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIIDpDCCAOygAwIBAgIGAVz1ojBcMA0GCSqGSI
b3QDEBQwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvc5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MB1GA1UECwwLUlNPUHJvdmlkZXIxEzARBgNVBAMTCmRldi02MDYyNzExHDAaBgkqhkiG9w0BCQEW
DWluZm9Ab2t0YSSjb2wHhcNMTcwNjI5MjA1MzI2WmcNMjcwNjI5MjA1NDI1WjCBkqELMAkGA1UE
BhMCMVVMxEzARBgNVBAGMCKNhbG1mb3JuaWExFjAUBGNVBAcMDVNBb1BGcmFuY2lzY28xDALBgNV
BAoMBE9rdGExFzA8BGNVBAcMCINTT1B3Z3ZGVyMRMwEQYDVQDDApkZXkYtNjA2MjcXMRwwGgYJ
KozIhvcNAQKBGFlpbmZvQ9rdG9uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
MbRLiIGL23Vp+vvKcNDCKRdy1Gw5F2UbwNl8Lm9PznpOEXG4KNwUC04TZut1FGjajlocfmWkcq
n3LpLmV8RmPe05ThChfhwX4VtIvJnFbJjIcio/EgleCyTfztWeWxFSaZVHMXXt6PkBAKEccroi
u9lv/DVamaKJozp1Uw5tdjphRcMXdy3d5DyxoppKkXzLanMONI6uYD0p/+TPVU3iM8vklUE7sjbHA
pBAgE2350qX+Jaehjgmil6/J6sCLzz59u/VvAN3bJE2PQzyd8FnRXP
PfvHFeOXH0qW8xhIbdV/WDyqQqzhMva/GFYNUQIDAQABMA0GCSqGSI
U+Jwdnt/74bxSjCblQ9F+gHGmqohwX63Xo8I0LjdrF0jrsoTypvCTM
OzKUKjxGyyDhUcpDsmiDKDbk1CGVm4ltnYXUstF4uPBQHNqzW0cm
lTBLA40JCCUhwCDDTL/qvENmBSa5b46UkcoKHgzqzAC1FHIMKG0oz
Tb5ULAtkIUUnLS8vfrZH7sq/mKJu8f1S+DPs6s6+6XJ6xkV6qJ79IL
7RJxxPc2kiYbZ1vXPCnsegOV4nzDxiec</ds:X509Certificate></
ds:Signature><saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status><saml2:Assertion
ID="id121708133820716391854568022" IssueInstant="2020-08-13T19:27:17.996Z" Version="2.0"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"><saml2:Issuer Format="urn:oasis:names:tc:SAML:
2.0:nameid-format:entity">exksledki8oMrgEVy0h7</saml2:Issuer><saml2:Subject><saml2:NameID
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">toddh@househarcourt.com</
saml2:NameID><saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:
2.0:cm:bearer"><saml2:SubjectConfirmation><saml2:ResponseTo="_6409506983574799128"
NotOnOrAfter="2020-08-13T19:32:00Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"><saml2:SubjectConfirmation></
saml2:SubjectConfirmation><saml2:Condition NotOnOrAfter="2020-08-13T19:32:00Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"><saml2:Condition></
saml2:Condition><saml2:Audience><saml2:Audience>zsccloud.net</
saml2:Audience></saml2:Audience><saml2:AuthnStatement
AuthnInstant="2020-08-13T19:27:17.996Z" SessionIndex="_6409506983574799128" Context="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"><saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef></saml2:AuthnContext></
saml2:AuthnStatement><saml2:AttributeStatement><saml2:Attribute Name="DisplayName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"><saml2:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">toddh</saml2:AttributeValue></saml2:Attribute><saml2:Attribute
Name="Department" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"></
saml2:Attribute><saml2:Attribute Name="memberOf" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified"><saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xs="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Everyone</
saml2:Attribute></saml2:Attribute></saml2:AttributeStatement></saml2:Assertion></
saml2p:Response>
```

Figure 175. SAML attributes in the decoded assertion

## Appendix B: Requesting Zscaler Support

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:

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

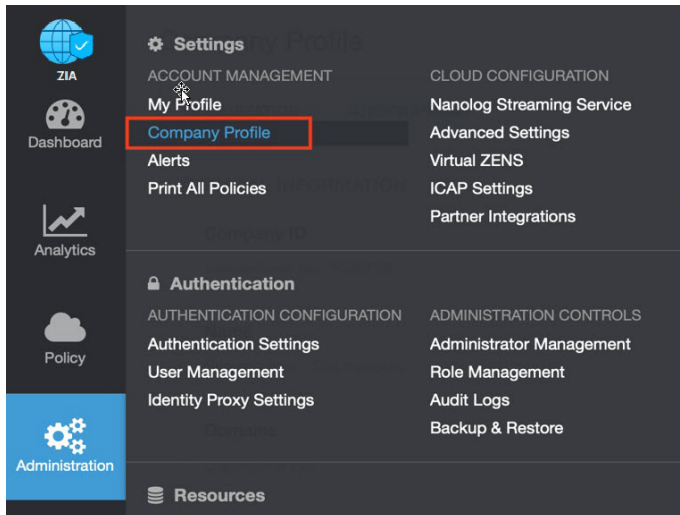


Figure 176. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

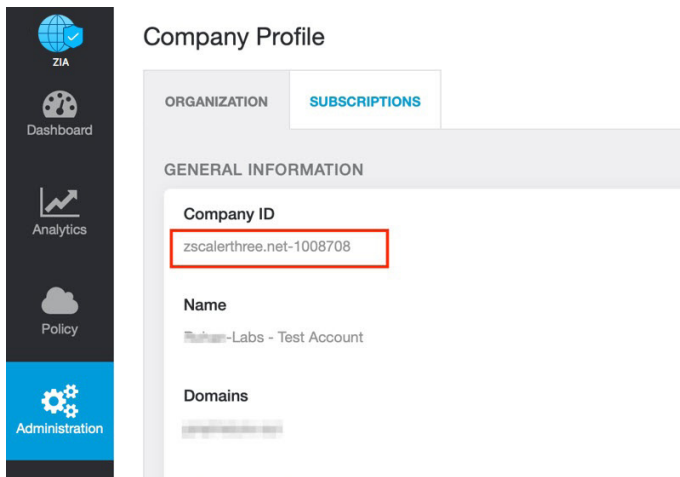


Figure 177. Company ID



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

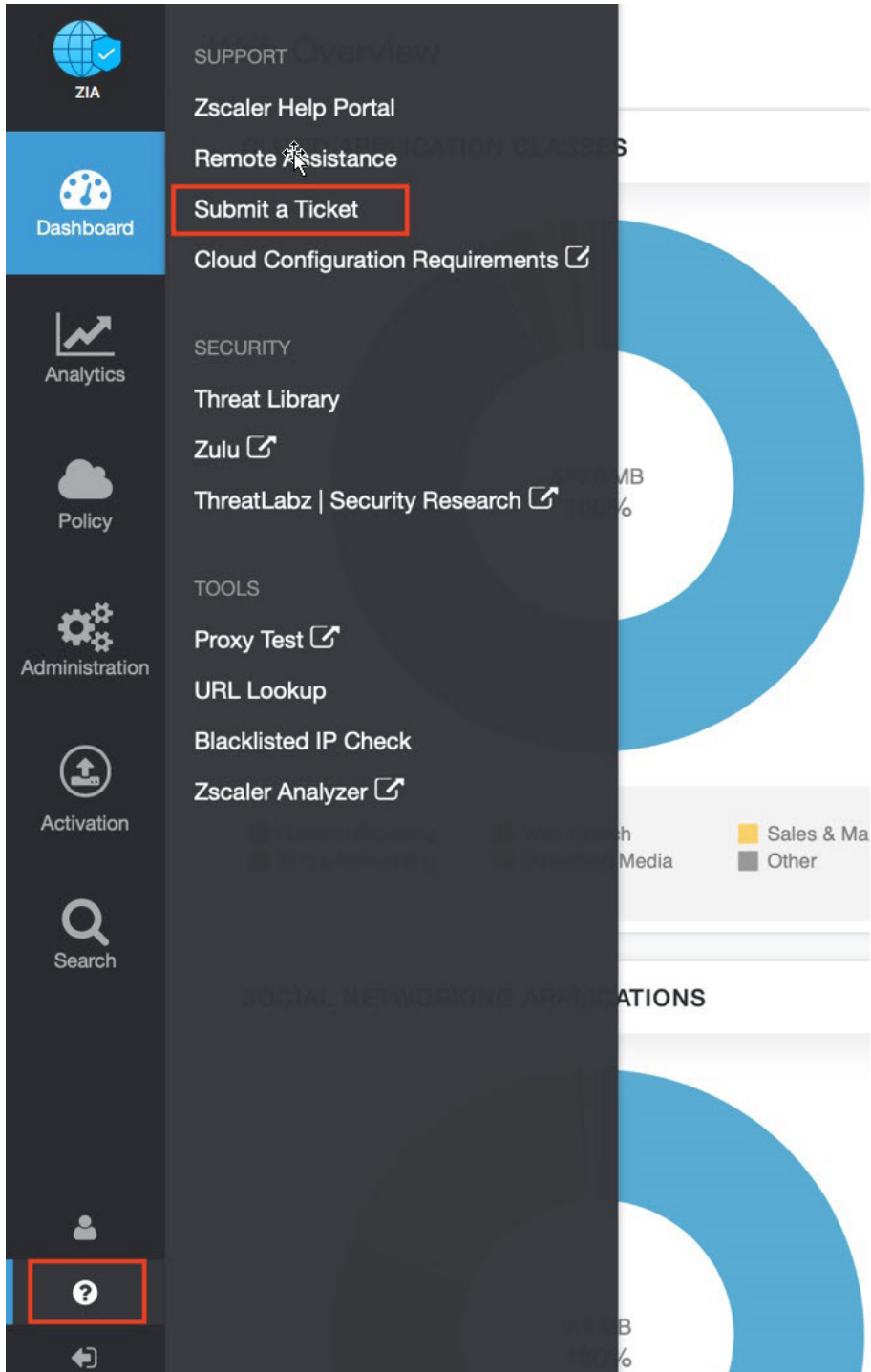


Figure 178. Submit a ticket