ZSCALER AND BEYOND IDENTITY DEPLOYMENT GUIDE

OCTOBER 2022, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

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

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
NFC	Near-Field Communication
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SCIM	System for Cross-domain Identity Management
SIM	Security Information Management
SSL	Secure Socket Layer (RFC6101)
SSO	Single Sign-On
TLS	Transport Layer Security
TPM	Trusted Platform Module
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZCP	Zscaler Cloud Protection
ZDX	Zscaler Digital Experience
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

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. For more information, see Zscaler's website or follow Zscaler on Twitter @zscaler.

Beyond Identity Overview

Beyond Identity is changing how the world logs in with an invisible, unphishable Multi-Factor Authentication MFA platform that provides the secure and frictionless authentication. They stop ransomware and account takeover attacks to improve the user experience. Beyond Identity's state-of-the-art platform eliminates passwords and other phishable factors, enabling organizations to confidently validate users' identities. The solution ensures users log in from authorized devices, and that every device meets the security policy requirements during login and continuously after that. Beyond Identity empowers zero trust by cryptographically binding the user's identity to their devices and analyzing hundreds of risk signals on an ongoing basis. The company's advanced risk policy engine enables organizations to implement foundationally secure authentication and use risk signals for protection, rather than just for detection and response. For more information, see Beyond Identity's website.

Audience

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

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- Beyond Identity Resources

Software Versions

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

Request for Comments

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

Zscaler and Beyond Identity Introduction

Overviews of the Zscaler and Beyond Identity applications are described in this section.

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 Virtual Desktop Infrastructure (VDI) instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

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

ZPA Overview

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

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

Zscaler Resources

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

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

Beyond Identity Overview

Beyond Identity Secure Workforce provides a passwordless authentication solution and leverages X.509 certificates without the need for a certificate authority or any certificate management. It extends the chain of trust established by Transport Layer Security (TLS) to users and their devices.

Using X.509 certificates and public-private key pairs is more secure than other authentication methods. A password, passphrase, and PIN use a shared secret—data that's stored in a database that might be vulnerable to compromise. Hardware keys have known security issues with Bluetooth and Near-Field Communication (NFC). They also lack a comprehensive, granular device security posture.

In addition to the vulnerabilities mentioned, Multi-Factor Authentication (MFA) increases exposure through Security Information Management (SIM) hacking, malware, and notification flooding. However, with X.509 and TLS technologies, the private key is securely stored in the Trusted Platform Management (TPM) of a personal device. The private key cannot be removed or viewed by anyone—not even the user.

Some organizations have legacy systems that still require users to have a password in the directory. You can use passwordless authentication for these systems, too. In the Beyond Identity console, you can set up an access policy so that no one can use a password to login. If an attacker attempts to access systems with a stolen password, an alarm is set off and the attacker is denied access.

Beyond Identity Resources

The following table contains links to Beyond Identity support resources.

Name	Definition
Beyond Identity Documentation	Help articles for Beyond Identity solutions.
Beyond Identity Support	Request Beyond Identity customer support.
Beyond Identity Slack Community	Beyond Identity Slack community.

Introduction

This guide provides information on how to:

- Set up Beyond Identity as a passwordless authentication solution for your ZIA and ZPA services.
- Set up Beyond Identity to enforce corporate Zero Trust policies by using Zscaler Client Connector API.

Notes

- For passwordless authentication, the customer might decide to integrate Zscaler with Beyond Identity, either directly or via their existing SSO. This document describes the direct integration between Zscaler and Beyond Identity. For integration via SSO, contact Beyond Identity.

  Zscaler's direct integration with Beyond Identity is applicable to Zscaler Client Connector for ZIA and ZPA, and ZPA Admin Portal. You do not integrate Beyond Identity with ZIA Admin Portal because ZIA Admin Portal does not support SP-initiated SAML flow, and Beyond Identity does not support IdP-initiated SAML flow.
- Both ZIA and ZPA provisioning is supported with SCIM supported directory or SSO while supporting Authentication directly with Beyond Identity as the IdP.

Prerequisites

Ensure that you have the following:

- A Zscaler account with "Super" admin privileges to configure SAML IdP.
- Zscaler Client Connector API enabled for your tenant (mobileadmin.<Zscaler cloud>.net). Look for Administration tab and "Public API" on the left-hand menu.

ZPA Admin Authentication Configuration

To configure Beyond Identity as the IdP for ZPA Admin Login, complete the following steps. Then, enable Beyond Identity for Admin Login to ZPA Admin Portal.

1. Sign into the ZPA Admin Portal as Administrator.
2. Select **Administration** > **IdP Configuration**.

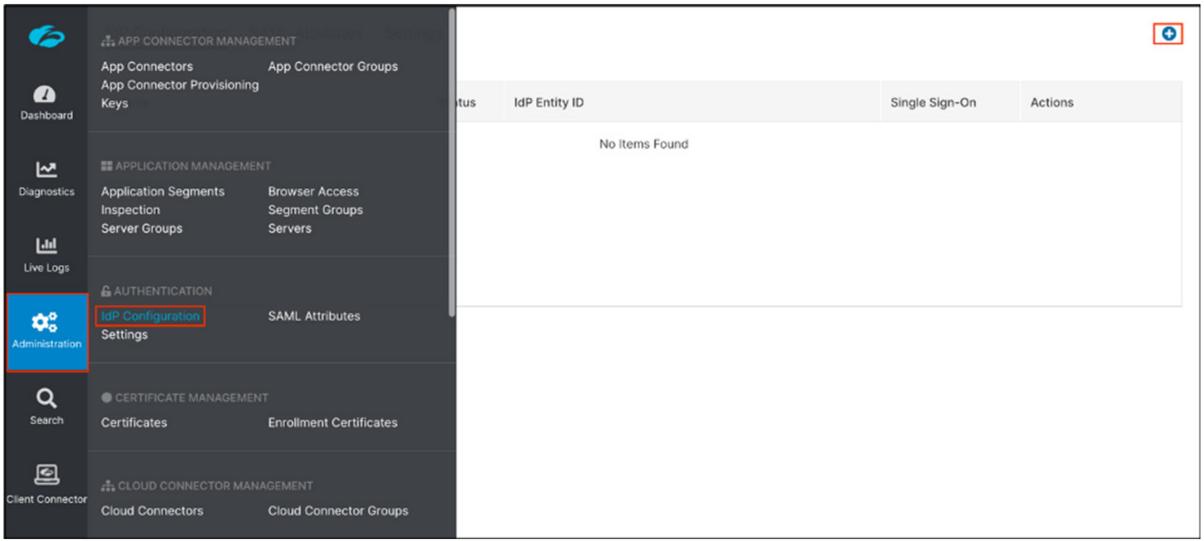
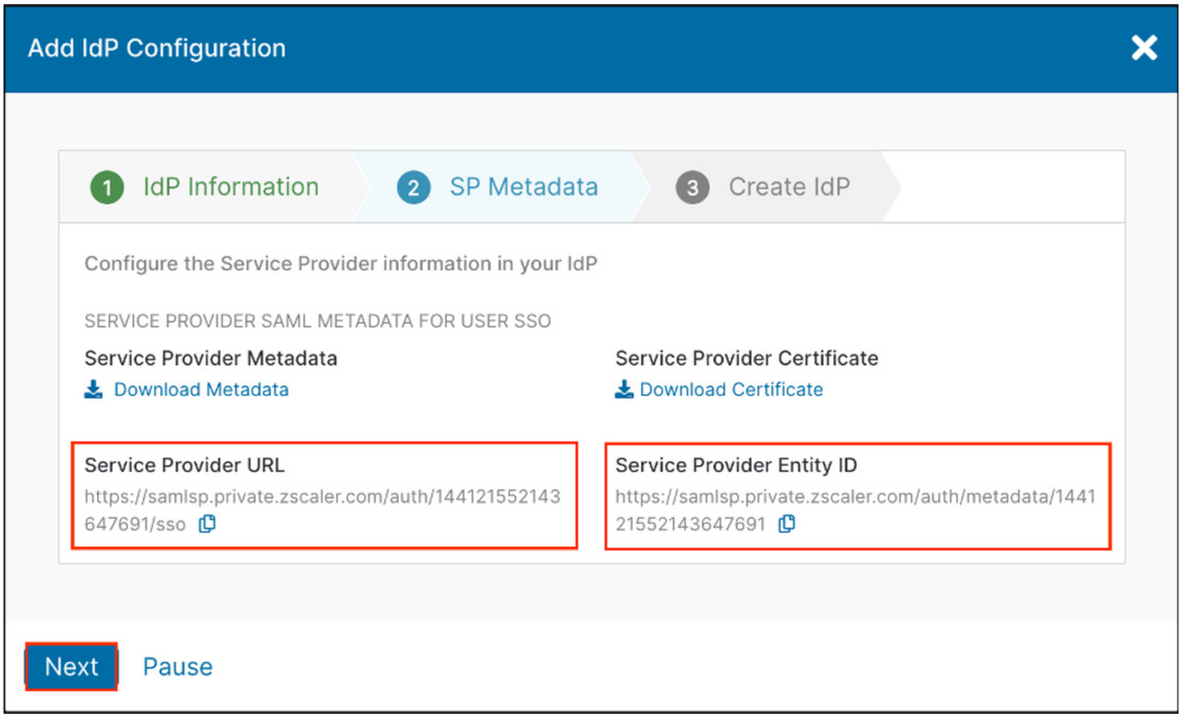


Figure 1. ZPA IdP Configuration

3. On the **IdP Configuration** tab, select the **Add** icon to add an IdP Configuration.
4. In the **IdP Information** tab, provide following Information.
   - **Name**: Type `Beyond Identity Admin SSO`.
   - **Single Sign-on**: Select **Admin**.
   - Select the correct certificate for the Admin SP Certificate Rotation.
   - **Domains**: Select the appropriate domain from the drop-down menu.
5. Click **Next**.

6. On the **SP Metadata** tab, download the **Service Provider Metadata**.
7. Click **Next**.



Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata

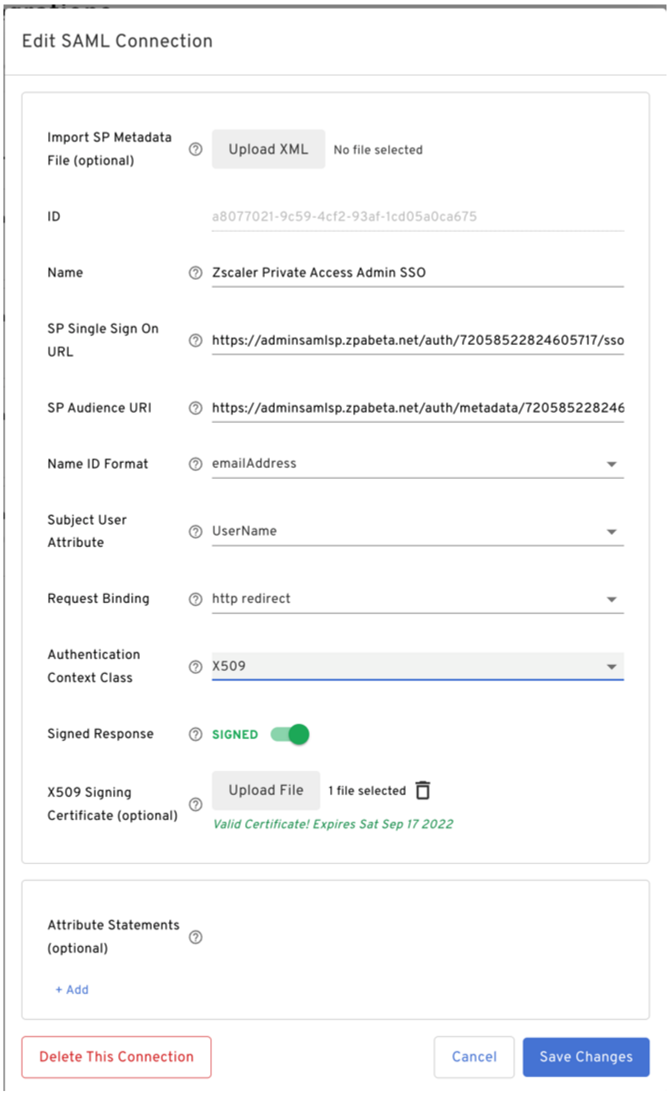
Service Provider Certificate

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

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

Figure 2. ZPA Add IdP Configuration

8. After logging into Beyond Identity Admin Console, select **Integrations** > **SAML** > **SAML Connections**.
9. Select **Add SAML Connection** and update the fields as follows:
   a. Upload the SP Metadata .xml file (downloaded in an earlier step).
   b. **Name**: Type `Zscaler Private Access Admin SSO`.
10. Click **Save Changes**.



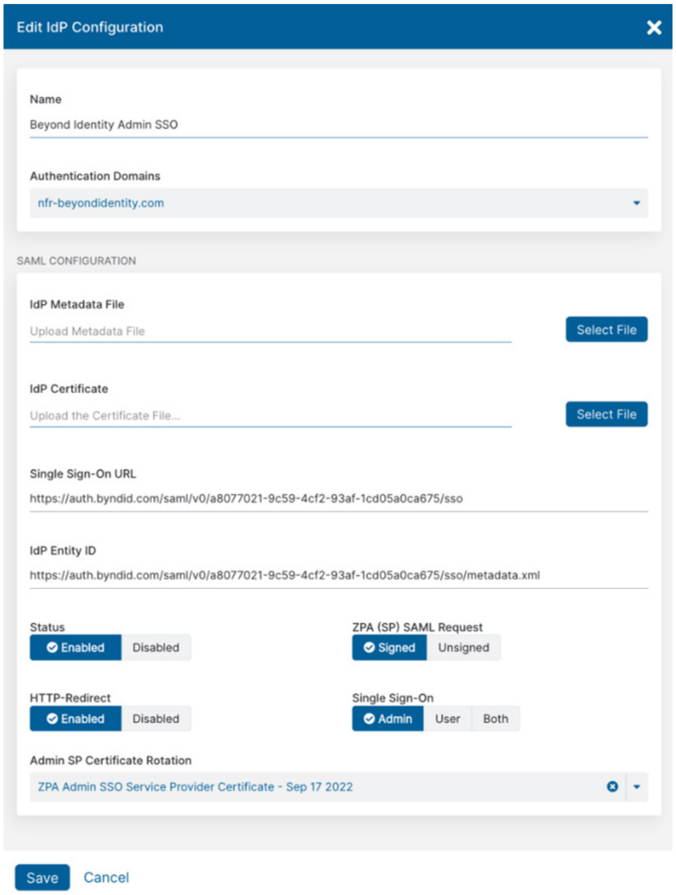
Edit SAML Connection

Import SP Metadata File (optional)	Upload XML No file selected
ID	a8077021-9c59-4cf2-93af-1cd05a0ca675
Name	Zscaler Private Access Admin SSO
SP Single Sign On URL	https://adminsamlsp.zpabeta.net/auth/72058522824605717/sso
SP Audience URI	https://adminsamlsp.zpabeta.net/auth/metadata/720585228246
Name ID Format	emailAddress
Subject User Attribute	UserName
Request Binding	http redirect
Authentication Context Class	X509
Signed Response	SIGNED
X509 Signing Certificate (optional)	Upload File 1 file selected *Valid Certificate! Expires Sat Sep 17 2022*

Attribute Statements (optional)

Figure 3. ZPA Edit SAML Connection

11. Note the following fields from the recently created SAML connection. They are required in the next step.
    - **IdP ID**: (Beyond Identity Connection ID).
    - **IdP Single Sign-On URL**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso
    - **IdP Issuer**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso/metadata.xml
12. Download the IdP Signature Certificate.
13. Switching back to ZPA Admin Portal, on the **IdP Configuration** tab, configure following fields:
    - **IdP Certificate**: (downloaded in an earlier step).
    - **Single Sign-On URL**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso (noted in an earlier step).
    - **IdP Entity ID**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso/metadata.xml (noted in an earlier step).
    - **Status**: Enabled.
    - **HTTP-Redirect**: Enabled.
    - **ZPA (SAML) Request**: Signed.
14. Click **Save**.


Edit IdP Configuration

Name
Beyond Identity Admin SSO

Authentication Domains
nfr-beyondidentity.com

SAML CONFIGURATION

IdP Metadata File
Upload Metadata File

IdP Certificate
Upload the Certificate File...

Single Sign-On URL
https://auth.byndid.com/saml/v0/a8077021-9c59-4cf2-93af-1cd05a0ca675/sso

IdP Entity ID
https://auth.byndid.com/saml/v0/a8077021-9c59-4cf2-93af-1cd05a0ca675/sso/metadata.xml

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 Service Provider Certificate - Sep 17 2022

Figure 4. ZPA Edit IdP Configuration

ZPA User Authentication Configuration

To configure Beyond Identity as the IdP for ZPA User Login, complete the following steps. Then enable Beyond Identity for User Login to the ZPA Client Connector.

1. Sign into the ZPA Admin Portal as Administrator.
2. Select **Administration** > **IdP Configuration**.

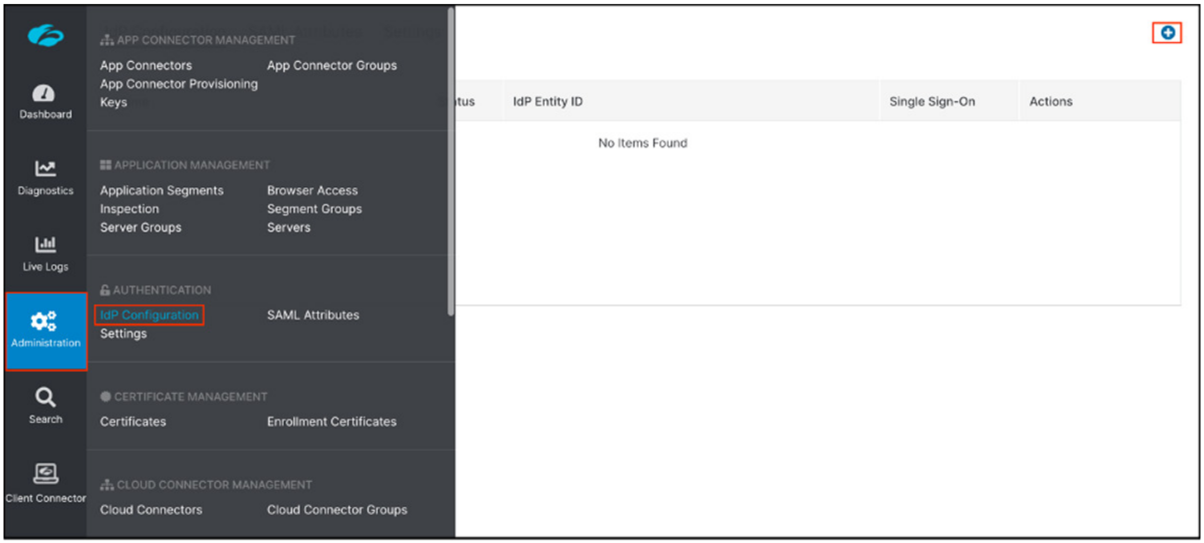
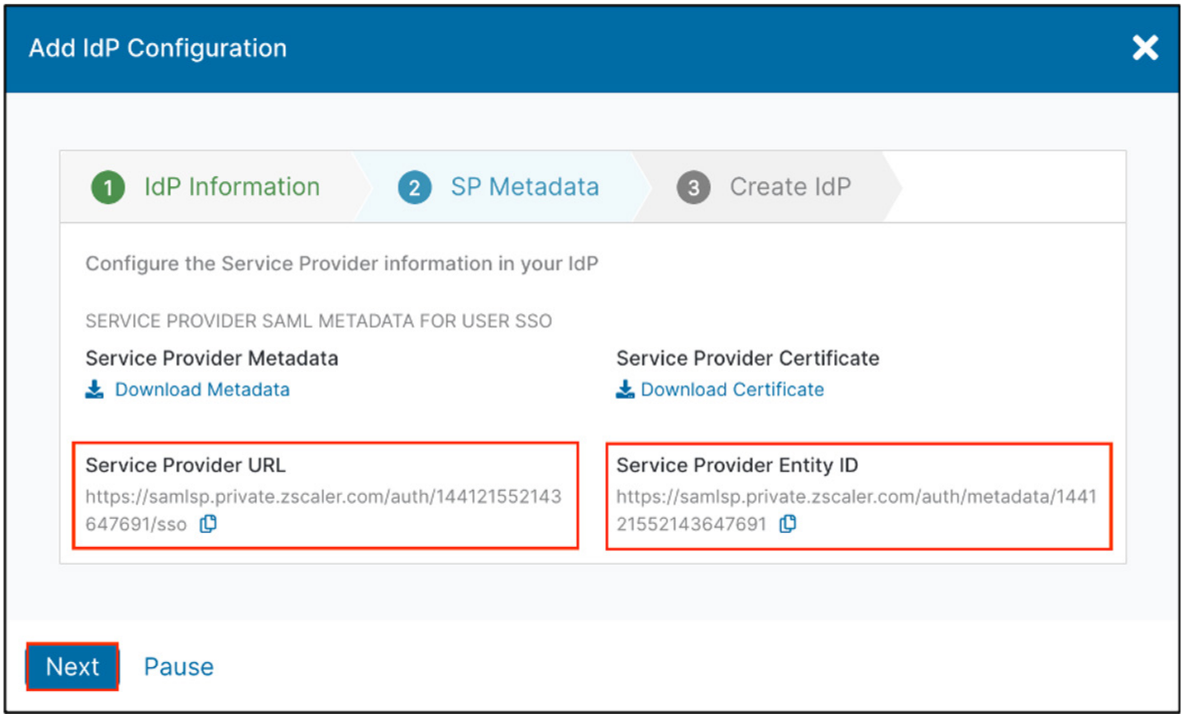


Figure 5. ZPA IdP Configuration

3. On the **IdP Configuration** tab, select the **Add** icon to add an IdP Configuration.

4. In the **IdP Information** tab, provide following Information.
   a. **Name**: Type `Beyond Identity User SSO`.
   b. **Single Sign-on**: Select **User**.
   c. Select the correct certificate for the User SP Certificate Rotation.
   d. **Domains**: Select the appropriate domain from the drop-down menu.
5. Click **Next**.
6. On the **SP Metadata** tab, download the **Service Provider Metadata**.
7. Click **Next**.



Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata

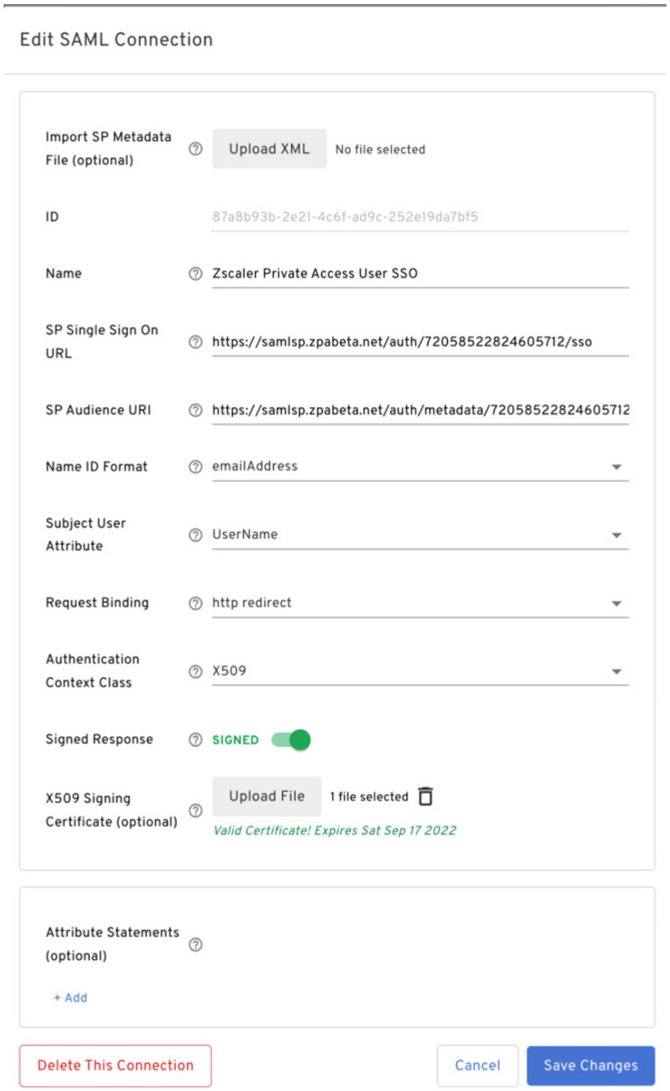
Service Provider Certificate

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

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

Figure 6. ZPA Add IdP Configuration

8. After logging into Beyond Identity Admin Console, navigate to **Integrations** > **SAML** > **SAML Connections**.
9. Click **Add SAML Connection** and update the following fields:
    - Upload the SP Metadata .xml file (downloaded in step 6).
    - **Name**: Enter `Zscaler Private Access User SSO`.
10. Click **Save Changes**.



Edit SAML Connection

Import SP Metadata File (optional): No file selected

ID: 87a8b93b-2e21-4c6f-ad9c-252e19da7bf5

Name: Zscaler Private Access User SSO

SP Single Sign On URL: https://samlsp.zpabeta.net/auth/72058522824605712/sso

SP Audience URI: https://samlsp.zpabeta.net/auth/metadata/72058522824605712

Name ID Format: emailAddress

Subject User Attribute: UserName

Request Binding: http redirect

Authentication Context Class: X509

Signed Response: SIGNED

X509 Signing Certificate (optional): 1 file selected

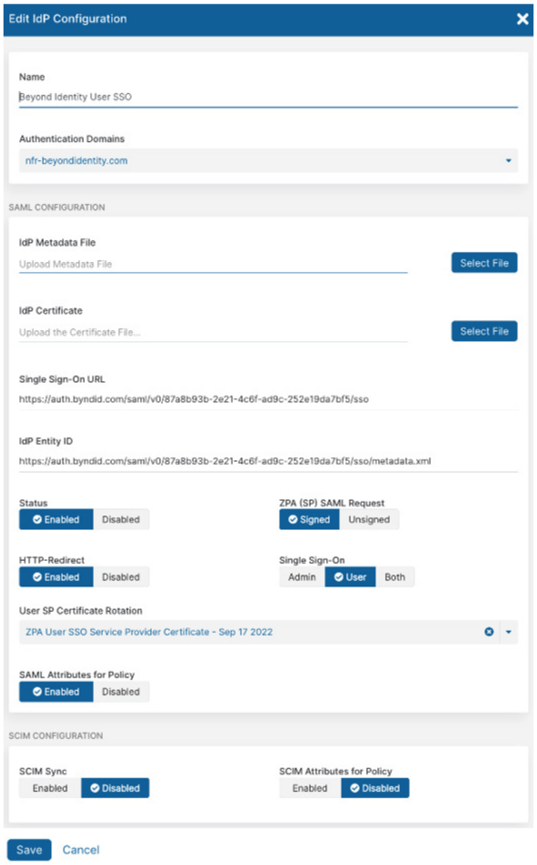
Valid Certificate! Expires Sat Sep 17 2022

Attribute Statements (optional)

Figure 7. ZPA Edit SAML Configuration

11. Note the following fields from the recently created SAML Connection. They are required in the next step.
    a. **IdP Id:** (Beyond Identity Connection ID).
    b. **IdP Single Sign-On URL**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso
    c. **IdP Issuer**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso/metadata.xml
    d. Download the **IdP Signature Certificate**.

12. Return to the ZPA Admin Portal, on the **IdP Configuration** tab, configure following fields.
    a. **IdP Certificate**: (Downloaded in the previous step).
    b. **Single Sign-On URL**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso (noted in the previous step).
    c. **IdP Entity ID**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso/metadata.xml (noted in the previous step).
    d. **Status**: Enabled.
    e. **HTTP-Redirect**: Enabled.
    f. **ZPA (SAML) Request**: Signed.
    g. **SCIM Sync**: Disabled.
    h. **SCIM Attributes for Policy**: Disabled.
13. Click **Save**.



Edit IdP Configuration

Name
Beyond Identity User SSO

Authentication Domains
nfr-beyondidentity.com

SAML CONFIGURATION

IdP Metadata File
Upload Metadata File

IdP Certificate
Upload the Certificate File...

Single Sign-On URL
https://auth.byndid.com/saml/v0/87a8b93b-2e21-4c6f-ad9c-252e19da7bf5/sso

IdP Entity ID
https://auth.byndid.com/saml/v0/87a8b93b-2e21-4c6f-ad9c-252e19da7bf5/sso/metadata.xml

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 - Sep 17 2022

SAML Attributes for Policy: [✓ Enabled] Disabled

SCIM CONFIGURATION

SCIM Sync: Enabled [✓ Disabled]

SCIM Attributes for Policy: Enabled [✓ Disabled]

Figure 8. ZPA Edit IdP Configuration

ZIA User Authentication Configuration

To configure Beyond Identity as the IdP for ZIA User Login, complete the following steps. Then enable Beyond Identity for User Login to ZIA Client Connector.

1. Sign into the ZIA Admin Portal as an Administrator.
2. Select **Administration** > **Authentication Settings**.

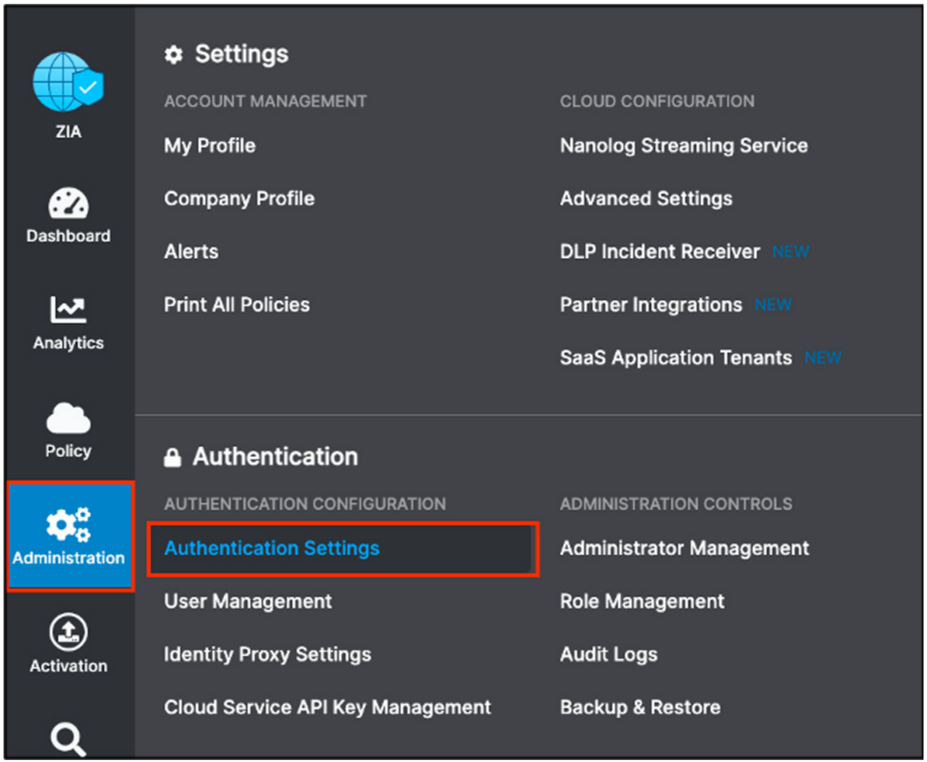
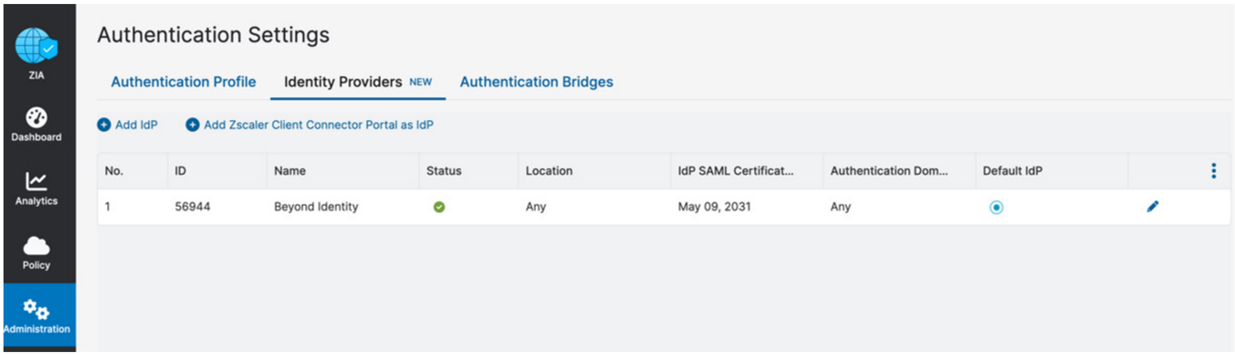


Figure 9. ZIA Authentication Settings

3. Select the **Identity Providers** tab.

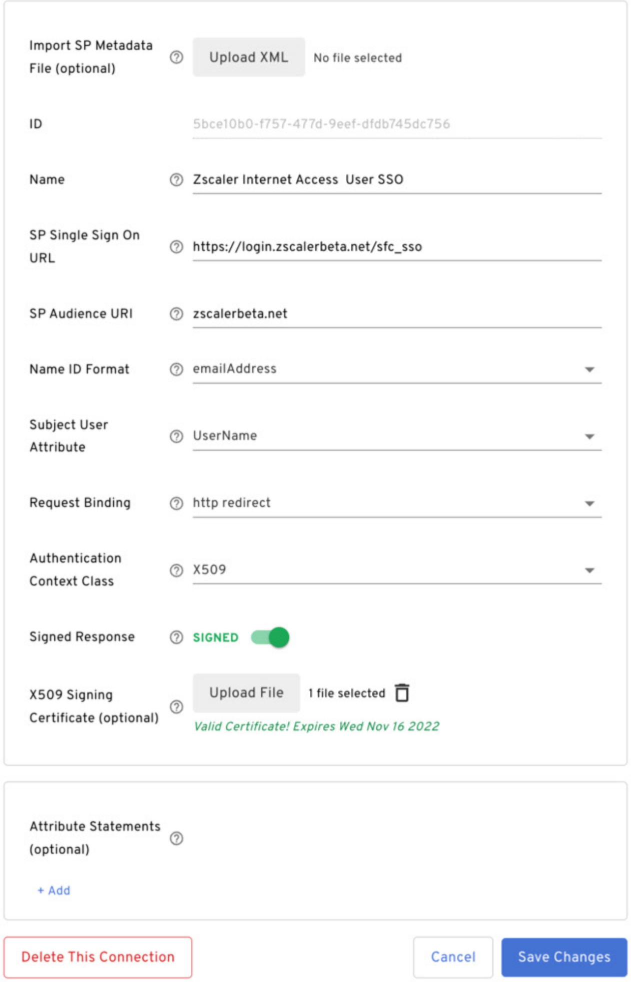


No.	ID	Name	Status	Location	IdP SAML Certificat...	Authentication Dom...	Default IdP
1	56944	Beyond Identity	●	Any	May 09, 2031	Any	◉

Figure 10. ZIA Providers tab

4. Click **Add IdP**.
5. Download the SP Metadata file and save it to use in the next step.
6. Log on to the Beyond Identity Admin Console, and navigate to **Integrations** > **SAML** > **SAML Connections**.

7. Click **Add SAML Connection** and update the following fields:
   a. Upload the SP Metadata .xml file downloaded in an earlier step.
   b. **Name**: Enter `Zscaler Internet Access User SSO`.
   c. Click **Save Changes**.



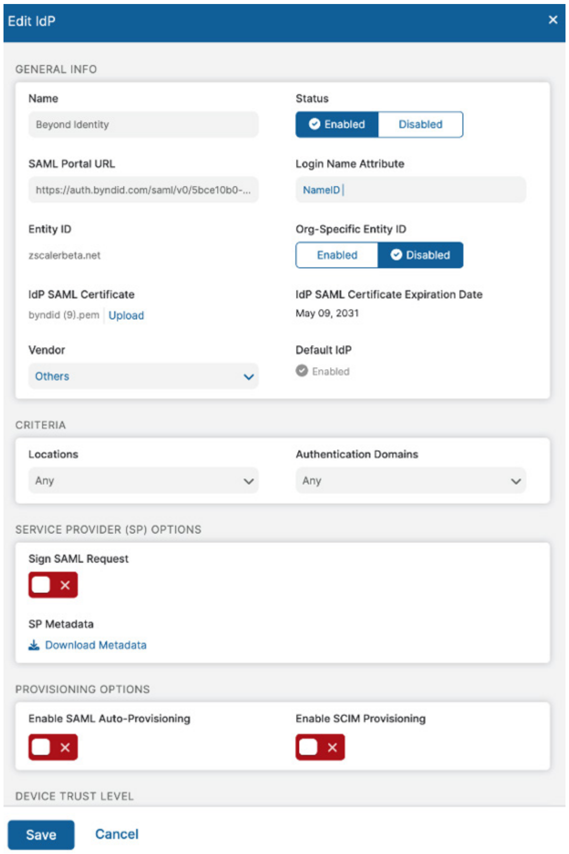
Import SP Metadata File (optional)	Upload XML No file selected
ID	5bce10b0-f757-477d-9eef-dfdb745dc756
Name	Zscaler Internet Access User SSO
SP Single Sign On URL	https://login.zscalerbeta.net/sfc_sso
SP Audience URI	zscalerbeta.net
Name ID Format	emailAddress
Subject User Attribute	UserName
Request Binding	http redirect
Authentication Context Class	X509
Signed Response	SIGNED
X509 Signing Certificate (optional)	Upload File 1 file selected *Valid Certificate! Expires Wed Nov 16 2022*
Attribute Statements (optional)	

Figure 11. Edit SAML Configuration for users

8. Note the following fields from the recently created SAML Connection. They are required in the next step.
   a. **IdP Id**: (Beyond Identity Connection ID).
   b. **IdP Single Sign-On URL**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso
   c. **IdP Issuer**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso/metadata.xml
   d. Download the **IdP Signature Certificate**.

9. Return to the ZIA Admin Portal, on the **IdP Configuration** tab, configure following fields:
    a. **IdP SAML Certificate**: Upload (downloaded in the previous step).
    b. **SAML Portal URL**: https://auth.byndid.com/saml/v0/<BI-Connection-ID>/sso (noted in the previous step).
    c. **Status**: Enabled.
    d. **Login Name Attribute**: NameID.
    e. **Vendor**: Others.
    f. **Sign SAML Request**: Disable.
    g. **HTTP-Redirect**: Enabled.
    h. **Enable SAML Auto Provisioning**: Disable.
    i. **Enable SCIM Provisioning**: Disable.

10. Click **Save**.


Edit IdP ×

GENERAL INFO

Name: Beyond Identity

Status: [✓ Enabled] Disabled

SAML Portal URL: https://auth.byndid.com/saml/v0/5bce10b0-...

Login Name Attribute: NameID

Entity ID: zscalerbeta.net

Org-Specific Entity ID: Enabled [✓ Disabled]

IdP SAML Certificate: byndid (9).pem | Upload

IdP SAML Certificate Expiration Date: May 09, 2031

Vendor: Others

Default IdP: Enabled

CRITERIA

Locations: Any

Authentication Domains: Any

SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request: ☒

SP Metadata: Download Metadata

PROVISIONING OPTIONS

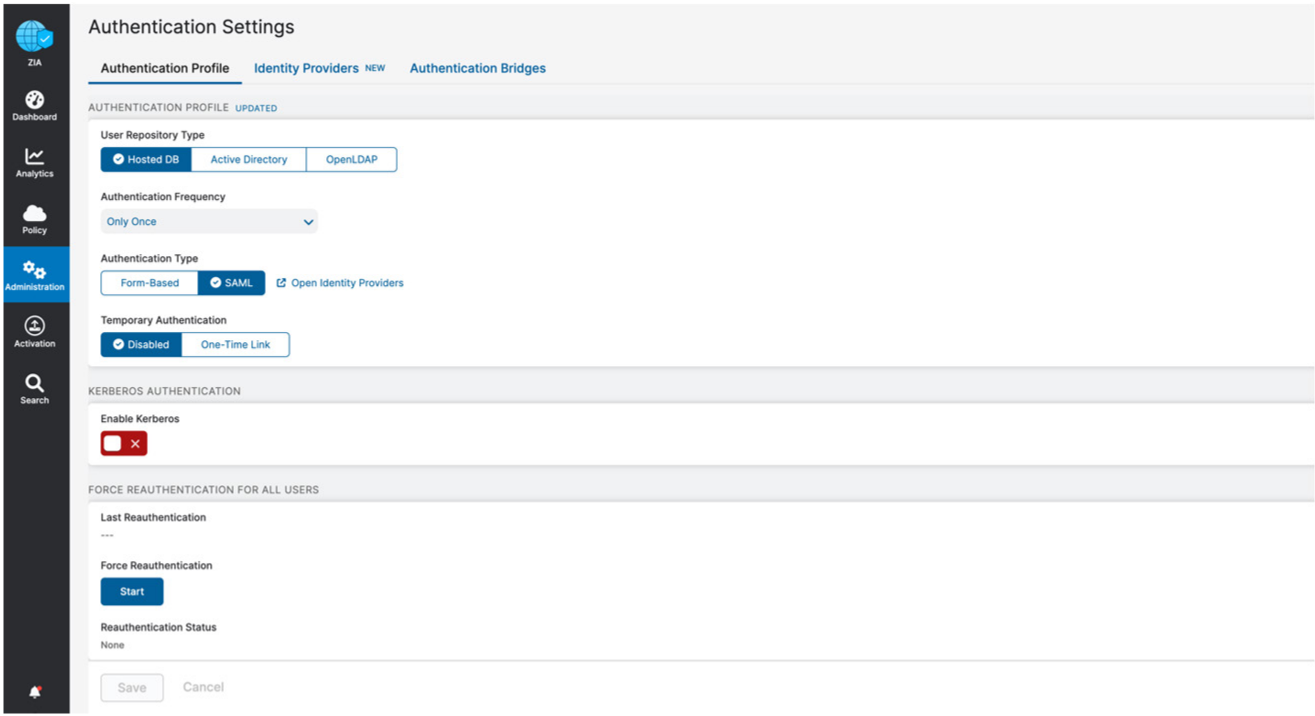
Enable SAML Auto-Provisioning: ☒

Enable SCIM Provisioning: ☒

DEVICE TRUST LEVEL

Figure 12. Edit IdP for users

11. To enable the SAML configuration on the **Authentication Settings** page, select the **Authentication Profile** tab.
12. Select **SAML** as the **Authentication type**.
13. Click **Save**, then **Activate** the configuration.



Authentication Settings

Authentication Profile | Identity Providers NEW | Authentication Bridges

AUTHENTICATION PROFILE UPDATED

User Repository Type: ● Hosted DB | Active Directory | OpenLDAP

Authentication Frequency: Only Once

Authentication Type: Form-Based | ● SAML | Open Identity Providers

Temporary Authentication: ● Disabled | One-Time Link

KERBEROS AUTHENTICATION

Enable Kerberos: ✕

FORCE REAUTHENTICATION FOR ALL USERS

Last Reauthentication

Force Reauthentication
Start

Reauthentication Status
None

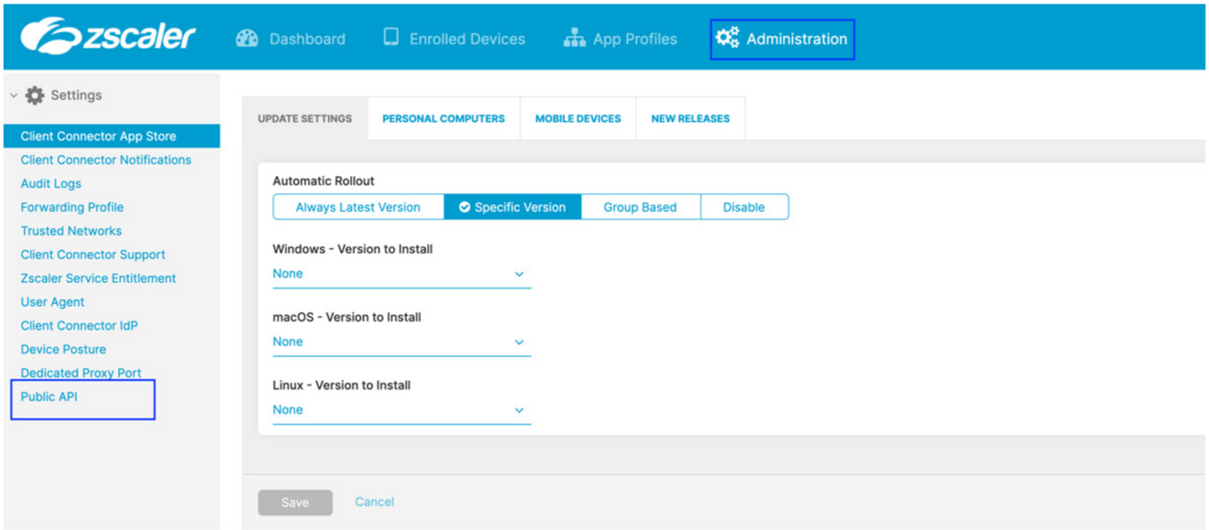
Save Cancel

Figure 13. ZIA Save the configuration

Zscaler Client Configuration to Enable API Access

This section describes changes required on Zscaler Client Connector I to enable API access.

1. In the ZIA or ZPA Admin Portal, sign into the Zscaler Client Connector in the left-hand navigation.
2. Click **Administration** and look for **Public API** in the left-hand navigation.



Automatic Rollout: Specific Version

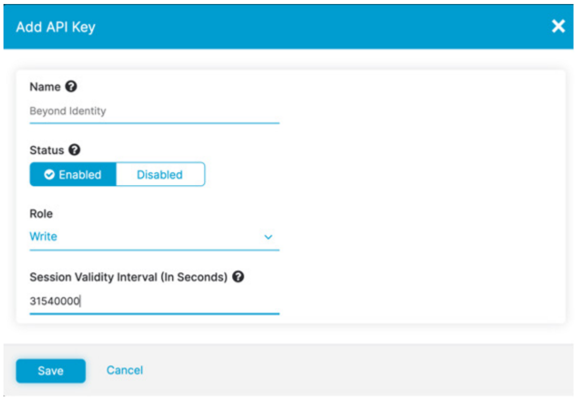
Windows - Version to Install: None

macOS - Version to Install: None

Linux - Version to Install: None

Figure 14. Public API in Client Connector

3. Select **Public API** and click **Add API Key**. Enter the following:
   - **Name**: Enter `Beyond Identity`.
   - **Status**: Enabled.
   - **Role**: Write.
   - **Session Validity Interval in seconds**: Enter `31540000` (Approx. 1 year).
4. Click **Save**.



Name: Beyond Identity

Status: Enabled

Role: Write

Session Validity Interval (In Seconds): 31540000

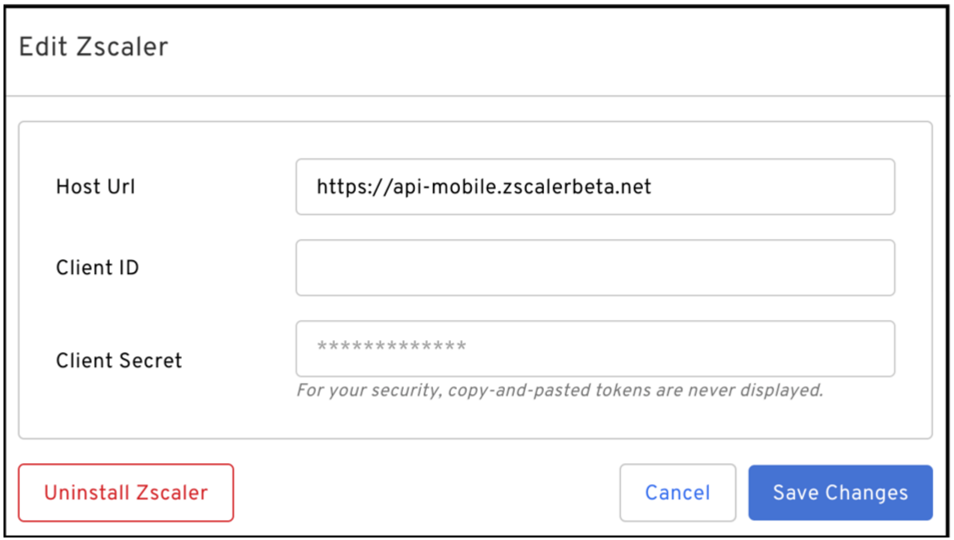
Figure 15. Add API Key in Client Connector

5. Note the following fields.
   - **Client Secret**.
   - **Client ID**.

Beyond Identity Console Configuration for Zscaler API Access

Beyond Identity supports continuous authentication and monitors device security posture even when the user is not actively trying to authenticate. Beyond Identity uses Zscaler Client Connector API to force reauthentication of the Zscaler Client Connector in case the device security posture does not meet enterprise policies.

1. Maker sure you have the **Client ID**, **Client Secret**, and **Zscaler Client Connector URL** before proceeding with the next steps of configuring Beyond Identity Integration with the Zscaler cloud.
2. Log in to the Beyond Identity Admin Console and navigate to **Integrations** > **End Point Management** > **Zscaler** > **Edit Zscaler**.



Edit Zscaler

Host Url: https://api-mobile.zscalerbeta.net

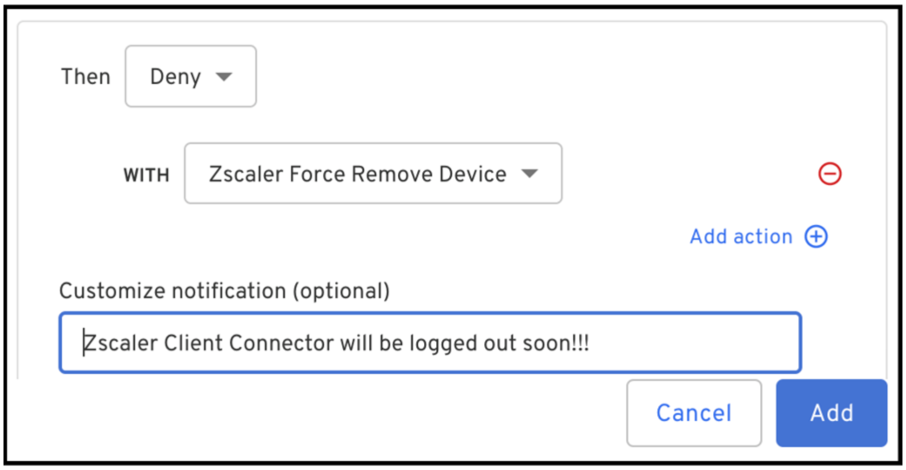
Client ID:

Client Secret: *************

For your security, copy-and-pasted tokens are never displayed.

Figure 16. Edit Zscaler in Beyond Identity

3. Add a new rule in the policy to force remove an authenticated device. During the test phase:
   - Create a test group.
   - Add a single user to the test group.
   - Create a **Deny Rule** to deny authentication and invoke Zscaler Force Remove Device API.
   - Add a custom notification: Enter `Zscaler Client Connector will be logged out soon!!!`.
4. Click **Add**.



Then: Deny

WITH: Zscaler Force Remove Device

Customize notification (optional): Zscaler Client Connector will be logged out soon!!!

Figure 17. Add new rule in Beyond Identity

5. Change the rule order as needed.
6. Log in to Zscaler Client Connector using the test user.
7. Publish the policy:
    - Authenticate to any application using Beyond Identity and verify that the authentication meets the criteria to trigger the Deny rule.
    - This displays the custom notification and the Zscaler Client Connector logs out in about three minutes.
8. Configure the policy to target all the users.

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support, select **Administration** > **Settings** > **Company Profile**.

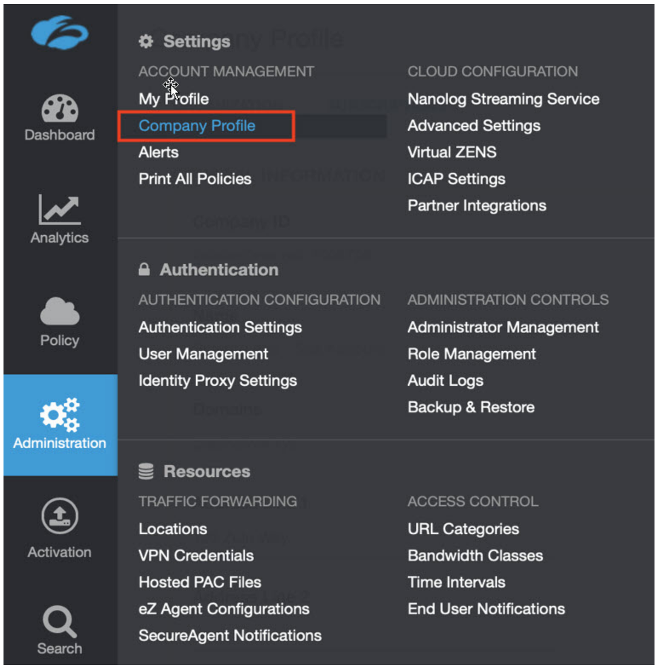
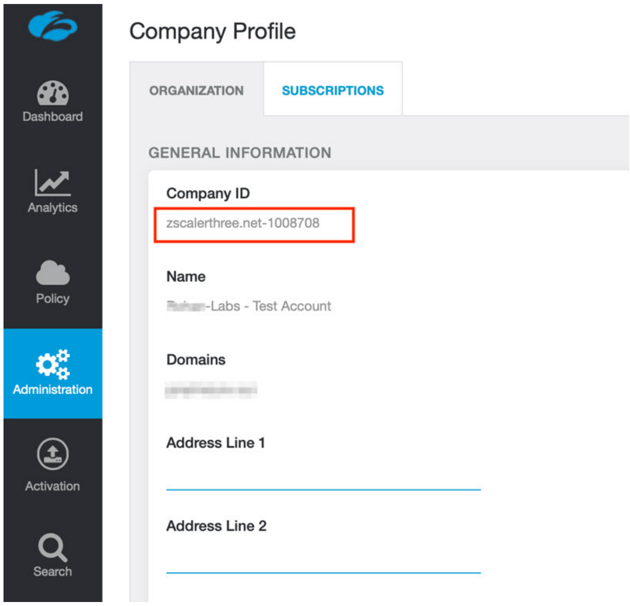


Figure 18. Collecting details to open support case with Zscaler TAC

Save Company ID

Copy your Company ID.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 19. Company ID

Enter Support Section

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

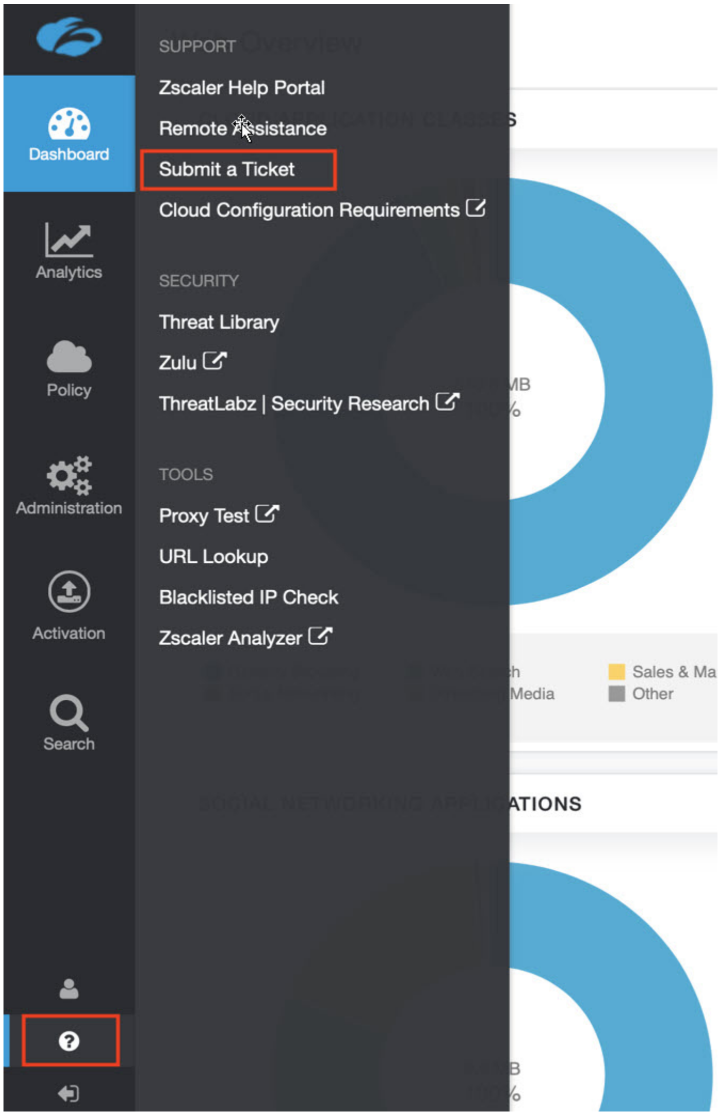


Figure 20. Submit a Ticket