ZSCALER AND FORGEROCK DEPLOYMENT GUIDE

OCTOBER 2022, VERSION 1.0

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms 4

About This Document 5

Zscaler Overview 5

ForgeRock Overview 5

Audience 5

Software Versions 5

Request for Comments 5

Zscaler and ForgeRock Introduction 6

ZIA Overview 6

ZPA Overview 6

Zscaler Resources 6

ForgeRock Access Management Overview 7

ForgeRock Resources 7

ForgeRock and Zscaler SAML SSO Overview 8

ZIA SSO 9

Create a Hosted IdP in the ForgeRock Environment 9

Add ForgeRock as the IdP in ZIA 12

Configure ZIA as the Remote SP 15

Configure the Circle of Trust 17

Testing 18

ZPA SSO 20

Create a Hosted IdP in the ForgeRock environment 20

Add IdP to ZPA 22

Configure ZPA as Remote SP 24

©2022 Zscaler, Inc. All rights reserved.

Configure Circle of Trust 25

Testing 26

Appendix A: Requesting Zscaler Support 27

©2022 Zscaler, Inc. All rights reserved.

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
ASIC	Application-Specific Integrated Circuit
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
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
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)

©2022 Zscaler, Inc. All rights reserved.

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.

ForgeRock Overview

ForgeRock (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. To learn more, refer to ForgeRock's website.

Audience

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

- Zscaler Resources
- ForgeRock Overview
- Appendix A: Requesting Zscaler Support

Software Versions

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

Request for Comments

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

Zscaler and ForgeRock Introduction

Overviews of the Zscaler and ForgeRock 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 Virtual Desktop Interface (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, Intrusion Prevention System (IPS), Sandboxing, Data Loss Prevention (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 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.
ZPA Posture Profiles	Help link for how to configure ZPA posture profiles.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

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

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
ZPA Posture Profiles	Help link for how to configure ZPA posture profiles.
ZPA Access Policies	Help link for how to configure ZPA access policies with a set of configuration examples.
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.

ForgeRock Access Management Overview

ForgeRock Access Management is a unified solution that addresses the complex access needs of today's modern organization. Access Management enables organizations to deliver great online experiences, migrate away from burdensome legacy platforms, and provide stronger security.

ForgeRock Access Management supports all user profiles from a single platform:

- Customers. Ensuring that your customers have frictionless access to online accounts and easy ways to manage their profiles means exceptional online experiences that lead to repeat business.
- Workforce. Employees, contractors, partners, and vendors typically have access to sensitive systems, applications, and networks and require instant, hassle-free access. Organizations need assurance of who these users are before granting access to valuable business assets.
- Things. Organizations need to know what IoT devices are on their networks and need to manage these devices just as they do their human identities.

ForgeRock Resources

The following table contains links to ForgeRock support resources.

Name	Definition
ForgeRock Documentation	Online help for ForgeRock applications.
ForgeRock Community	ForgeRock online community forum.
ForgeRock Support	ForgeRock support requests.

©2022 Zscaler, Inc. All rights reserved.

ForgeRock and Zscaler SAML SSO Overview

ForgeRock's Access Management uses the concept of a "Circle of Trust" to manage the relationship between identity providers (IdPs) and service providers (SPs). When configuring ForgeRock Access Management Single Sign-On using SAML v2.0, you can map accounts at the IdP to accounts at the SP, including mapping to an anonymous user. The IdP can then make assertions to the SP. The SP then consumes assertions from the IdP to make authorization decisions.

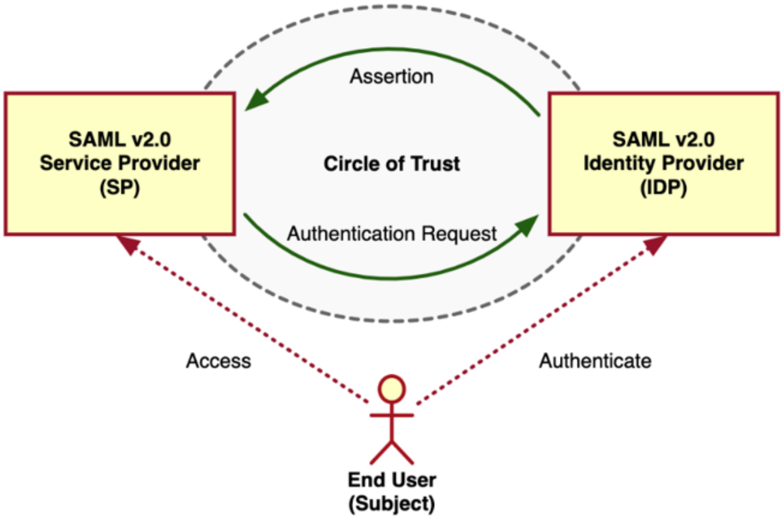


Figure 1. ForgeRock Access Management

In this SAML SSO integration, ForgeRock is the IdP and Zscaler is the SP. Zscaler has two services: ZIA and ZPA. This guide walks through configuring both services to work with ForgeRock.

ZIA SSO

The following sections describe configuring ZIA to work with ForgeRock as the SSO provider.

Create a Hosted IdP in the ForgeRock Environment

The following steps are based on procedures documented on the ForgeRock website. To create a hosted IdP:

1. Login to your ForgeRock tenant.
2. In the platform console, select **Native Consoles** > **Access Management**.

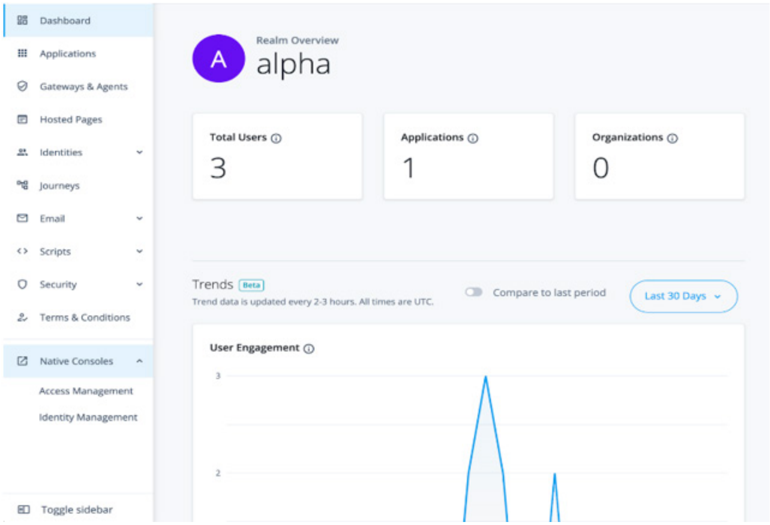


Figure 2. Access Management

3. Select **SAML Applications** from the **Quick Start** menu in the **Alpha Realm**. This displays the **Entity Providers** tab.
4. Select **Hosted** in the drop-down menu in **Add Entity Provider**.

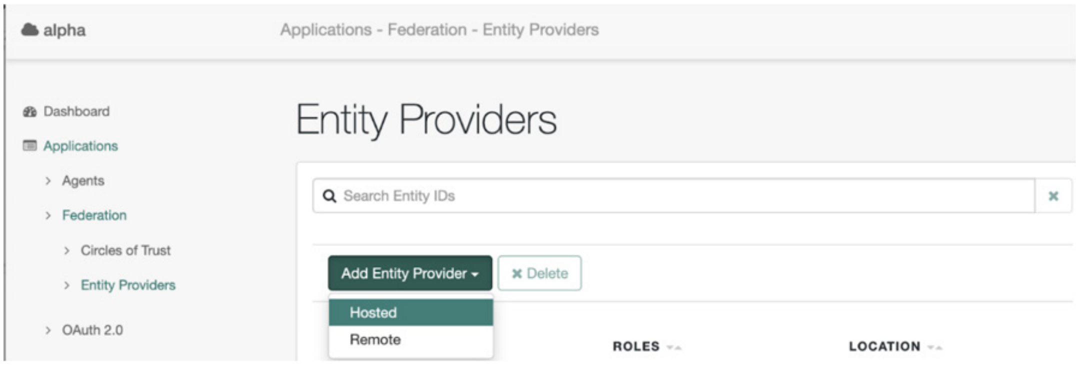
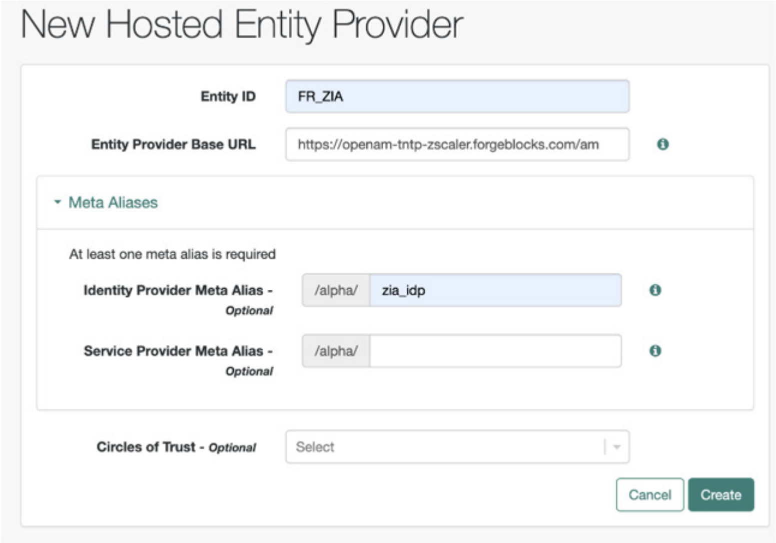


Figure 3. Entity Providers

©2022 Zscaler, Inc. All rights reserved.

5. In **New Hosted Entity Provider**, create an **Entity ID** name (i.e., `FR_ZIA`).
6. Create an **Identity Provider Meta Alias** name (i.e., `zia_idp`).
7. Click **Create**.



New Hosted Entity Provider

Entity ID: FR_ZIA

Entity Provider Base URL: https://openam-tntp-zscaler.forgeblocks.com/am

Meta Aliases

At least one meta alias is required

Identity Provider Meta Alias - *Optional*: /alpha/ zia_idp

Service Provider Meta Alias - *Optional*: /alpha/

Circles of Trust - *Optional*: Select

Figure 4. New Hosted Entity Provider

8. Create a URL for metadata in the following format:

```
[ServerURL]/saml2/jsp/exportmetadata.jsp?entityid=[entityID]&realm=/realmname
```

Where:

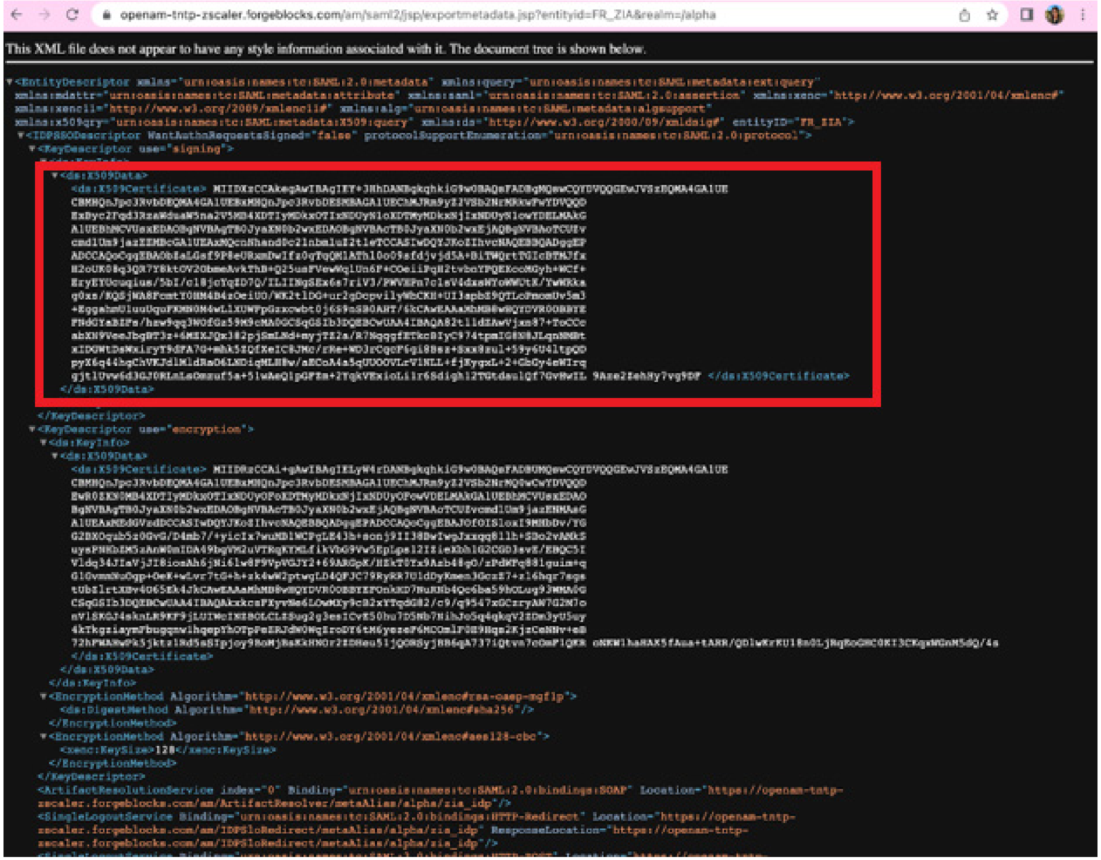
- `[ServerURL]` is the full AM server URL.
- `[entityID]` is the name of your entity provider.
- `realmname` is the name of the realm in which the entity provider is configured.

9. Ensure your URL looks like the following example:

```
https://openam-tntp-zscaler.forgeblocks.com/am/saml2/jsp/exportmetadata.jsp?entityid=FR_ZIA&realm=/alpha
```

To learn more, see How do I export and import SAML2 metadata in AM (All versions).

10. Copy the URL, open a new browser tab, and paste in the metadata URL into the tab URL field. The URL takes you to the output that contains the certificate information.
11. Save the certificate portion of the metadata as a .pem. The .pem is used later when you add the IdP configuration to the ZIA Admin Portal. You upload the .pem file as the IdP SAML Certificate.



openam-tntp-zscaler.forgeblocks.com/am/saml2/jsp/exportmetadata.jsp?entityid=FR_ZIA&realm=/alpha

This XML file does not appear to have any style information associated with it. The document tree is shown below.

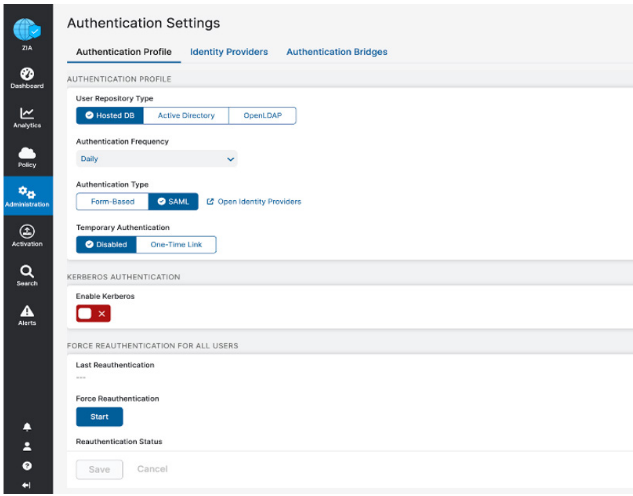
```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query"
  xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:xenc11="http://www.w3.org/2009/xmlenc11#" xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
  xmlns:x509qry="urn:oasis:names:tc:SAML:metadata:X509:query" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="FR_ZIA">
 ▼<IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   ▼<KeyDescriptor use="signing">
     ▼<ds:KeyInfo>
       ▼<ds:X509Data>
          <ds:X509Certificate> MIIDXzCCAkegAwIBAgIEY+JHhDANBgkqhkiG9w0BAQsFADBgMQswCQYDVQQGEwJVSzEQMA4GA1UE
          CBMHQnJpc3RvbDEQMA4GA1UEBxMHQnJpc3RvbDESMBAGA1UEChMJRm9yZ2VSb2NrMRkwFwYDVQQD
          ExByc2FqdJRzaWduaW5na2V5MB4XDTIyMDkxOTIxNDUyN1oXDTMyMDkxNjIxNDUyN1owYDELMAkG
          A1UEBhMCVUsxEDAOBgNVBAgTB0JyaXN0b2wxEDAOBgNVBAcTB0JyaXN0b2wxEjAQBgNVBAoTCUZv
          cmdlUm9jazEZMBcGA1UEAxMQcnNhandDc21nbmluZ2tleTCCASIwDQYJKoZIhvcNAQEBBQADggEP
          ADCCAQoCggEBAOb8aLGsf9P8eURxmDwIfz0qTqQMlATh10o09sfdjvjd5A+BiTWQrtTGIcBTMJfx
          H2oUK08q3QX7Y8ktOV2ObmeAvkThB+Q25usFVewWqlUn6P+COeiiPqH2tvbnYPQEKcoMGyh+WCf+
          EryEYUcuqius/5bI/cl8jcYqZD7Q/ILIINgSEx6s7riV3/PWVHPn7clsV4dzsWYoWWUtK/YwWKka
          q0xs/KQSjWASFcmtY0HM4B4zOeiU0/WK2tlDG+ur2gDcpvilyWbCKH+UIJapbZ9QTLcPmomUv5mJ
          +EggahmUluuUquFXMN0M4wLlXUWFpGzxcwbt0j6S9nSBOAHT/6kCAwEAAaMhMB8wHQYDVR0OBBYE
          FNdGYaBIFs/hzw9qq3N0fGz59M9cMA0GCSqGSIb3DQEBCwUAA4IBAQA82tlldZAwVjxn87+ToCCo
          abXN9VeeJbqBT3z+6MZXJQxl82pjSmLNd+myjTZ2a/R7NqqqfETkcBIyC974tpmIG8X8JLqnNMBt
          xIDOWtDsWxiryT9dFA7G+mhk5ZQfXe1C8JMo/rRe+WDJrCqcF6qi8Bsz+Sxx8zul+59y6U4ltpQD
          pyX6q44hgChVKJdlMldRaO6LNDiqMLH8w/aECoA4a5qUUOOVLrV1NLL+fjKyqxL+2+GbGy4eWIrq
          gjtlUvw6d3GJ0RLnLsGmzuf5a+5lwAeQlpGFZm+2YqkVExioLilr6Sdigh12TGtdaulQf7GvHwIL 9Azs2ZehHy7vg9DF </ds:X509Certificate>
        </ds:X509Data>
    </KeyDescriptor>
   ▼<KeyDescriptor use="encryption">
     ▼<ds:KeyInfo>
       ▼<ds:X509Data>
          <ds:X509Certificate> MIIDRzCCAi+gAwIBAgIELyW4rDANBgkqhkiG9w0BAQsFADBUMQswCQYDVQQGEwJVSzEQMA4GA1UE
          CBMHQnJpc3RvbDEQMA4GA1UEBxMHQnJpc3RvbDESMBAGA1UEChMJRm9yZ2VSb2NrMQ0wCwYDVQQD
          EwR0ZXN0MB4XDTIyMDkxOTIxNDUyOFoXDTMyMDkxNjIxNDUyOFowVDELMAkGA1UEBhMCVUsxEDAO
          BgNVBAgTB0JyaXN0b2wxEDAOBgNVBAcTB0JyaXN0b2wxEjAQBgNVBAoTCUZvcmdlUm9jazENMAsG
          A1UEAxMEdGVzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ0f0ISloxI9MHbDv/YG
          G2BXOqub5z0GvG/D4mb7/+yicIx7wuMBlWCPqLE4Jb+sonj9Il38BwIwgJxxqq8llh+SBo2vANkS
          uysPNHbZM5zAnW0mIDA49bgVM2uVTRqKYMLfikVbG9Vw5EpLps12IZieXbh1G2CGDlevE/EHQC5I
          Vldq34JIaVjJIBiosAh6jNi6lw8F9VpVGJY2+69ARGpK/HEkT0Tx9Azb48g0/zPdWFq88lquim+q
          G1GvmmNuOgp+OeK+wLvr7tG+h+zk4wW2ptwgLD4QFJC79RyRR7UldDyKmen3GczZ7+zl6hqr7sgs
          tUbZlrtXBv4O65Ek4JkCAwEAAaMhMB8wHQYDVR0OBBYEFOnkXD7NuRHb4Qc6ba59hOLuq93MMA0G
          CSqGSIb3DQEBCwUAA4IBAQAkxkcsFXyvNe6LOwMXy9cB2xYTqdG82/c9/q9547xGCzryAN7G2N7o
          nVlSKGJ4sknLR9KF9jLUIWcIXEBOLCLZSug2g3esICvE50hu7D5Nb7HihJo5q4qkqV2ZDm3yU5uy
          4kTkgziaymFbuggnw1hqepYhOTpPeZRJdW0WqIroDY6tM6yezeF6MCOmlF0S9Hqs2KjzCeNHv+eB
          72hFWAHwPk5jktzlNd5sBTpjoy9RoMjBsKkHNOr2ZDHeu51jQ0NSyjBB6qA737iQtvn7cOmFlQKR oNKWlhaHAX5fAua+tARR/QDlwKrKUl8nOLjRqKoGHC0KI3CKgxWGnM5dQ/4s
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
     ▼<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      </EncryptionMethod>
     ▼<EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc">
        <xenc:KeySize>128</xenc:KeySize>
      </EncryptionMethod>
    </KeyDescriptor>
    <ArtifactResolutionService index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://openam-tntp-
    zscaler.forgeblocks.com/am/ArtifactResolver/metaAlias/alpha/zia_idp"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://openam-tntp-
    zscaler.forgeblocks.com/am/IDPSloRedirect/metaAlias/alpha/zia_idp" ResponseLocation="https://openam-tntp-
    zscaler.forgeblocks.com/am/IDPSloRedirect/metaAlias/alpha/zia_idp"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://openam-tntp-
```

Figure 5. Metadata URL

Add ForgeRock as the IdP in ZIA

With ForgeRock configured as the hosted IdP in the ForgeRock admin console, add ForgeRock as an IdP in the ZIA Admin Portal:

1. In a browser, login to the ZIA Admin Portal.
2. Navigate to **Administration** > **Authentication**.
3. In the **Authentication Profile** tab:
   a. Select **Hosted DB** as **User Repository Type**.
   b. Set **Authentication Frequency** (Zscaler recommends **Daily**).
   c. Select **SAML** as **Authentication Type**.
   d. Check that the **Authentication Profile** looks like the following graphic:



Authentication Settings

Authentication Profile | Identity Providers | Authentication Bridges

AUTHENTICATION PROFILE

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

Authentication Frequency: Daily

Authentication Type: Form-Based | ● SAML

Temporary Authentication: ● Disabled | One-Time Link

KERBEROS AUTHENTICATION

Enable Kerberos: ✕

FORCE REAUTHENTICATION FOR ALL USERS

Last Reauthentication: ---

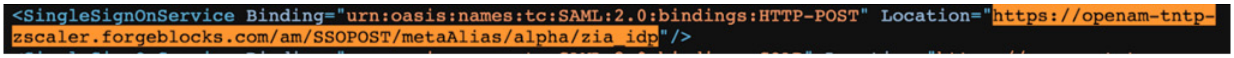
Force Reauthentication

Reauthentication Status

Figure 6. Checking the Authentication Settings in the ZIA Admin Portal

4. Under the **Identity Providers** tab, click **+ Add IdP** and fill out the following fields:

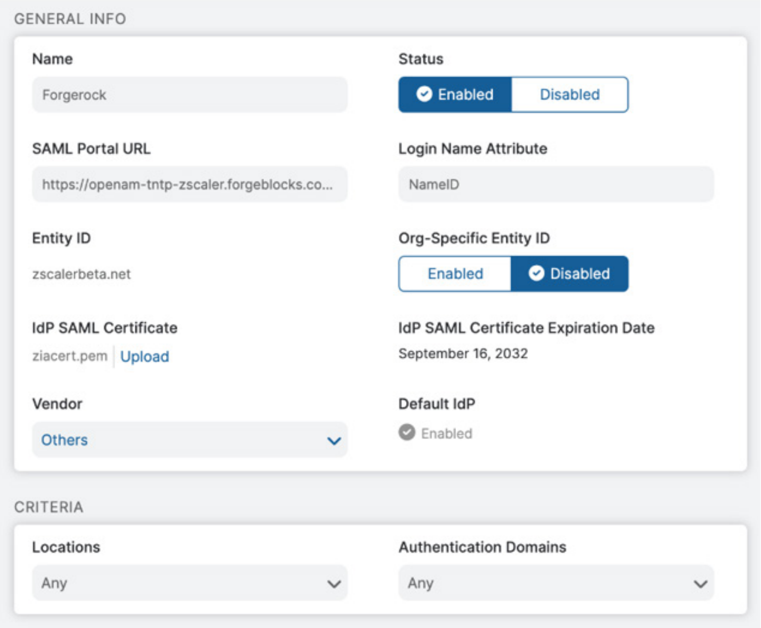
- **Name**: Enter a name for the IdP.
- **Status**: Enable the IdP.
- **SAML Portal URL**: Enter the SSO URL of the SAML portal to which users are sent for authentication. This information is in the XML metadata of the IdP that was previously exported. It is found in the following example, **SingleSignOnService SSO Post**.



```
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://openam-tntp-
zscaler.forgeblocks.com/am/SSOPOST/metaAlias/alpha/zia_idp"/>
```

- **Login Name Attribute**: Enter the SAML attribute that maps to the login name that users enter when they authenticate to the ZIA service. Typically, it's `NameID`, which is entered as one word, with no spaces. This field is case-sensitive.
- **Entity ID**: Enter the globally unique name for this SAML entity.
- **Org-Specific Entity ID**: Enable if you have more than one organization instance on the same Zscaler cloud. Otherwise, disable.
- **IdP SAML Certificate**: Upload the SAML certificate used to verify the digital signature of the IdP. This is the certificate you downloaded from your IdP. The certificate must be in Base64 encoded PEM format. The file extension must be .pem and have no other periods (.) in the file name.
- **Vendor**: Select **Others** from the drop-down menu.

- **Default IdP**: Enable as default.
- The **General Info** and **Criteria** looks similar to the following:



GENERAL INFO

Name: Forgerock

Status: ● Enabled | Disabled

SAML Portal URL: https://openam-tntp-zscaler.forgeblocks.co...

Login Name Attribute: NameID

Entity ID: zscalerbeta.net

Org-Specific Entity ID: Enabled | ● Disabled

IdP SAML Certificate: ziacert.pem | Upload

IdP SAML Certificate Expiration Date: September 16, 2032

Vendor: Others

Default IdP: ✓ Enabled

CRITERIA

Locations: Any

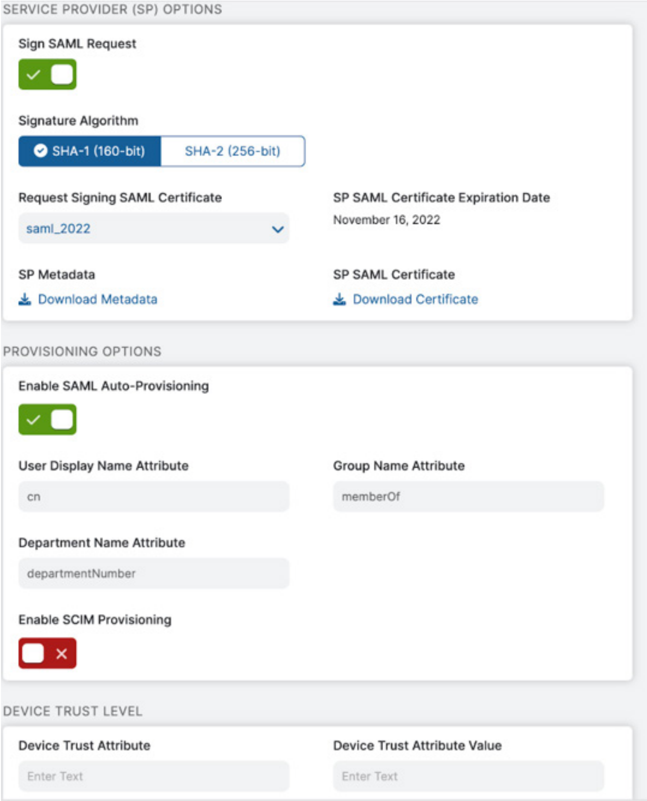
Authentication Domains: Any

Figure 7. Adding the Identity Providers General Info to the ZIA Admin Portal

- **SP Options**: Enable Sign SAML Request.
- **SP Metadata**: Download the metadata of the ZIA service. The metadata advertises the Zscaler SAML capabilities and is used for auto-configuration. ForgeRock requires importing the metadata to configure the ZIA service as a SP. You use this metadata when you configure ZIA as the remote SP in the ForgeRock console in later steps.

©2022 Zscaler, Inc. All rights reserved.

- **Enable SAML Auto-Provisioning**: Enable SAML for provisioning users on the Zscaler service. After enabling SAML auto-provisioning, enter the values shown in the following fields:
    - **User Display Name Attribute**: `cn`.
    - **Group Name Attribute**: `memberOf`.
    - **Department Name Attribute**: `departmentNumber`.



SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request: ✓

Signature Algorithm: ● SHA-1 (160-bit) | SHA-2 (256-bit)

Request Signing SAML Certificate: saml_2022

SP SAML Certificate Expiration Date: November 16, 2022

SP Metadata: Download Metadata

SP SAML Certificate: Download Certificate

PROVISIONING OPTIONS

Enable SAML Auto-Provisioning: ✓

User Display Name Attribute: cn

Group Name Attribute: memberOf

Department Name Attribute: departmentNumber

Enable SCIM Provisioning: ✕

DEVICE TRUST LEVEL

Device Trust Attribute: Enter Text

Device Trust Attribute Value: Enter Text

Figure 8. Setting the Identity Provider Options in the ZIA Admin Portal

5. Click **Save**.

Configure ZIA as the Remote SP

Return to the ForgeRock Access Management Console and configure ZIA as the remote SP:

1. In the platform console of ForgeRock Access Management, select **Applications** > **Federation** > **Entity Providers**.
2. Select **Remote** under **Add Entity Provider**.

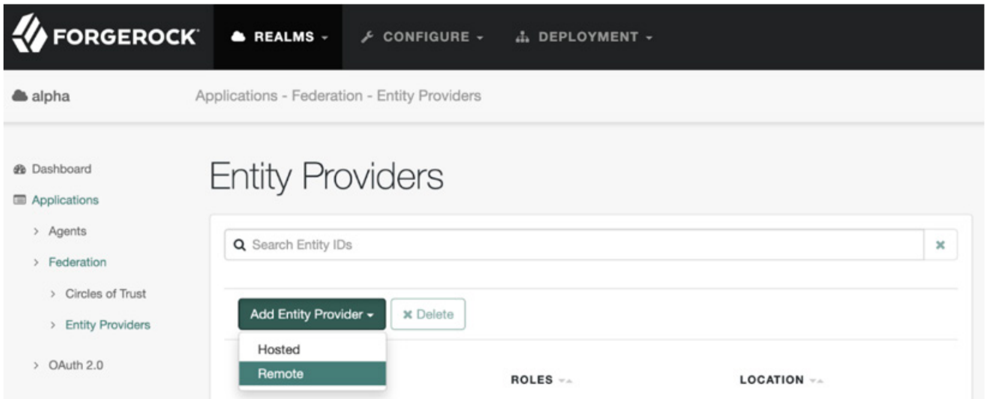


Figure 9. Entity Providers

3. In the **Import Files** section of **New Remote Entity Provider**, drag and drop the SP metadata downloaded from the ZIA Admin Portal.

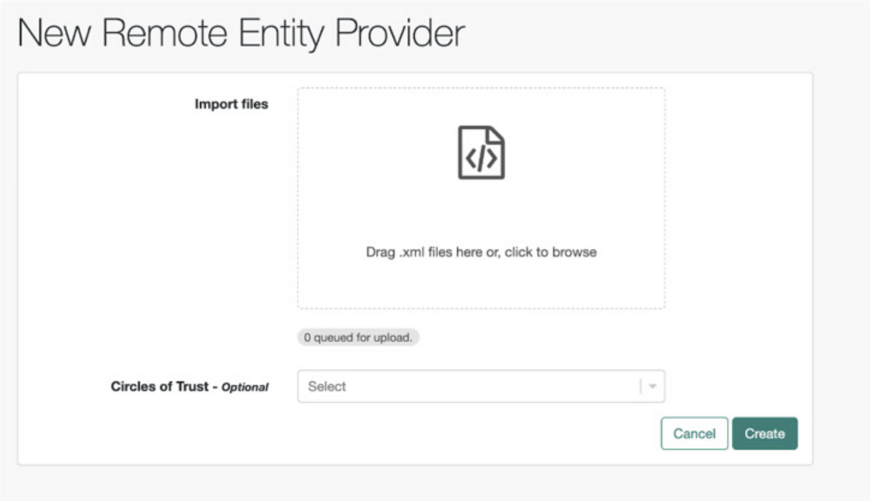
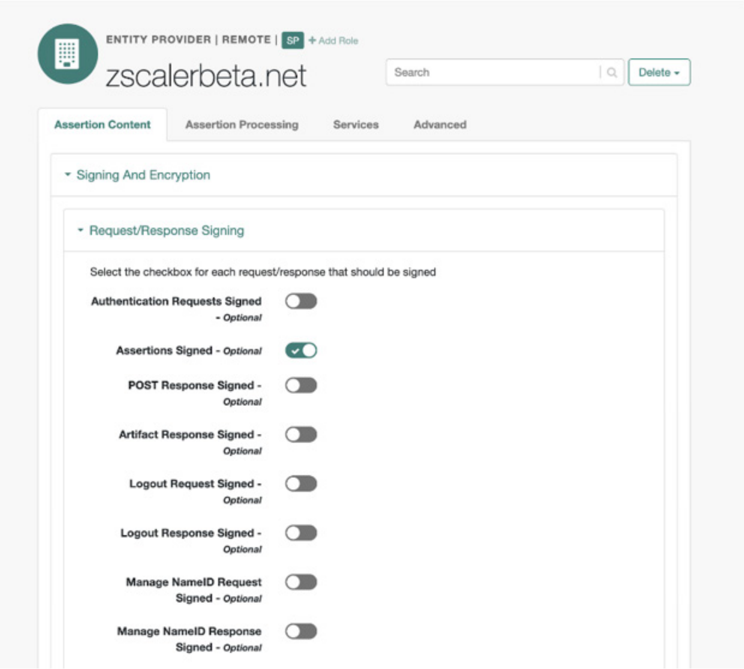

New Remote Entity Provider
Import files
Drag .xml files here or, click to browse
0 queued for upload.
Circles of Trust - Optional
Select
Cancel
Create

Figure 10. Upload metadata in ForgeRock Access Management

©2022 Zscaler, Inc. All rights reserved.

4. Click **Create** and the form is auto-filled.



ENTITY PROVIDER | REMOTE | SP + Add Role

zscalerbeta.net

Search

Delete

Assertion Content | Assertion Processing | Services | Advanced

Signing And Encryption

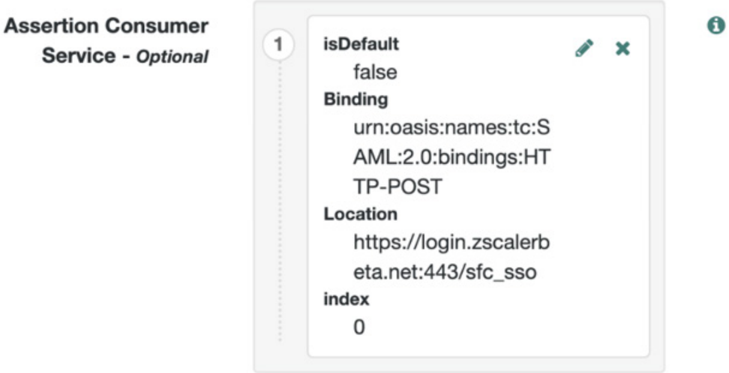
Request/Response Signing

Select the checkbox for each request/response that should be signed

- Authentication Requests Signed - *Optional* ☐
- Assertions Signed - *Optional* ☑
- POST Response Signed - *Optional* ☐
- Artifact Response Signed - *Optional* ☐
- Logout Request Signed - *Optional* ☐
- Logout Response Signed - *Optional* ☐
- Manage NameID Request Signed - *Optional* ☐
- Manage NameID Response Signed - *Optional* ☐

Figure 11. Assertion Content

5. Make one change to the auto-fill. In the **Services** tab, scroll down to **Assertions Consumer Service** and edit the **Location** section to include port 443.



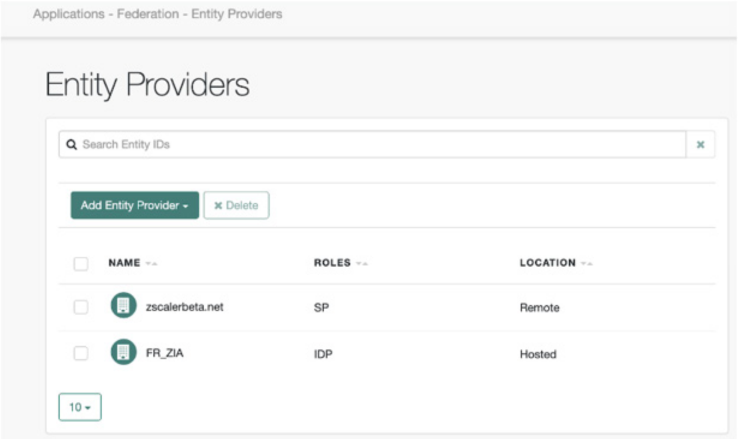
Assertion Consumer Service - *Optional*

1

isDefault
false
Binding
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
Location
https://login.zscalerbeta.net:443/sfc_sso
index
0

Figure 12. Port edit

6. In **Entity Providers**, and check that both your SP and IdP are created:



Applications - Federation - Entity Providers

Entity Providers

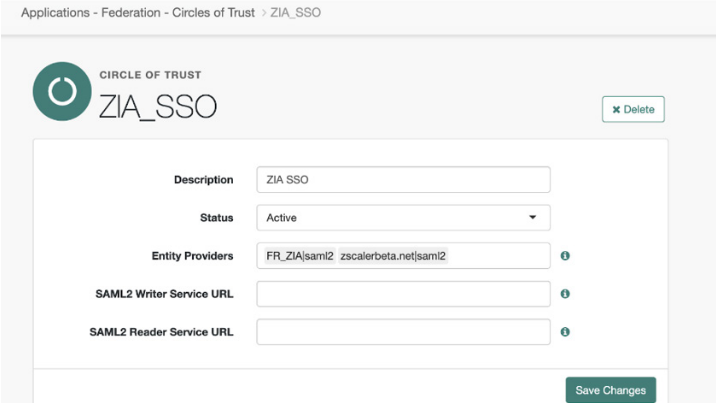
NAME	ROLES	LOCATION
zscalerbeta.net	SP	Remote
FR_ZIA	IDP	Hosted

Figure 13. Verify SP and IdP in Entity Providers

Configure the Circle of Trust

You must set up the Circle of Trust in ForgeRock:

1. In the platform console, select **Applications** > **Federation** > **Circle of Trust**.
2. Select **Add Circle of Trust**.
3. **Name** the Circle of Trust (i.e., `ZIA_SSO`).
4. Add a **Description** (i.e., `ZIA SSO`).
5. Select the IdP and SP under **Entity Providers**.



Applications - Federation - Circles of Trust > ZIA_SSO

CIRCLE OF TRUST

ZIA_SSO

Description: ZIA SSO

Status: Active

Entity Providers: FR_ZIA|saml2 zscalerbeta.net|saml2

SAML2 Writer Service URL:

SAML2 Reader Service URL:

Figure 14. Circle of Trust

6. Click **Save Changes**.

Testing

In order to test the IdP initiated SSO:

1. Go to the ForgeRock Admin Console.
2. In the platform console, select **Identities** > **Manage**.
3. Under **Manage Identities**, create and configure ForgeRock-hosted identity resources.
4. Click **+New Alpha Realm- User**.
5. In the **New Alpha realm - user** window, fill in the values.
6. Click **Save**.

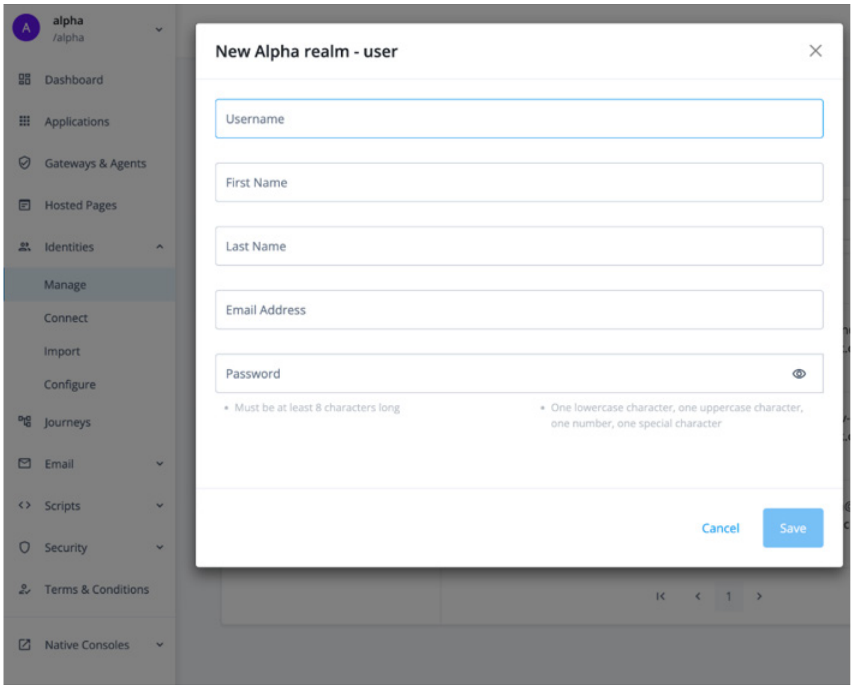
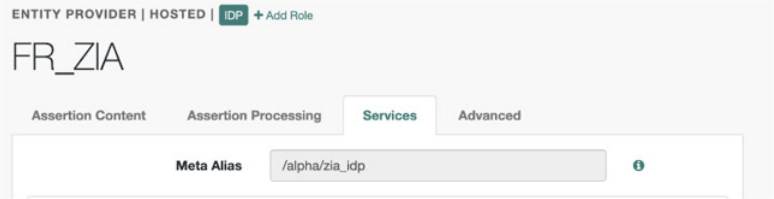


Figure 15. Test user

7. Generate a test URL. For instructions, see [How do I configure IdP or SP initiated Single Sign On in Identity Cloud or AM (All versions)?]()
8. Specify the following:
   - **Meta Alias**: Specify the local alias for the provider in the format `/realmname/providername`. For the top level realm, exclude the `realmname` element. You can find the Meta Alias under the **Entity Provider** section of **Access Management**:

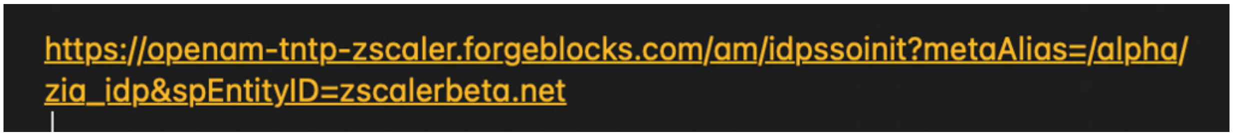


Meta Alias: /alpha/zia_idp

Figure 16. Services tab

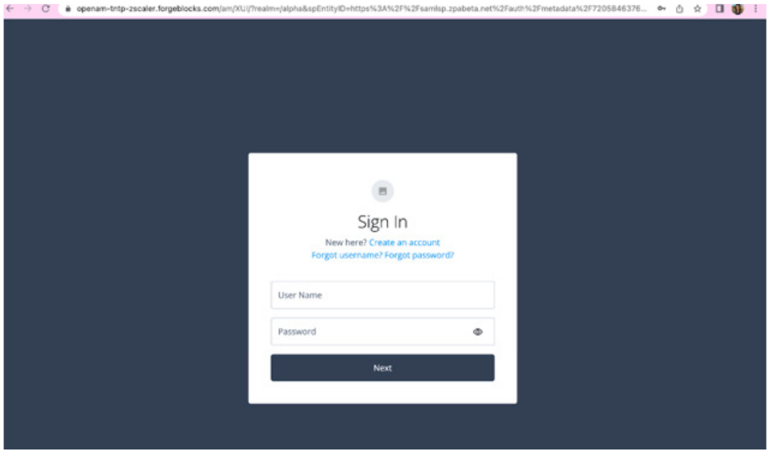
   - **spEntityID**: Specify the remote identity provider (for SP-initiated logins) and must be URL-encoded.

The generated URL appears:



https://openam-tntp-zscaler.forgeblocks.com/am/idpssoinit?metaAlias=/alpha/zia_idp&spEntityID=zscalerbeta.net

9. Paste the generated URL into an incognito window. You are prompted to a ForgeRock sign on screen.



openam-tntp-zscaler.forgeblocks.com/am/XUI/?realm=/alpha&spEntityID=https%3A%2F%2Fsamlsp.zpabeta.net%2Fauth%2Fmetadata%2F7205846376...

Sign In

New here? Create an account

Forgot username? Forgot password?

Figure 17. ForgeRock Sign In

10. Enter your login credentials for the ForgeRock test user.

This logs you into the ZIA Admin Portal.

ZPA SSO

The setup for the ZPA configuration is very similar to the setup for ZIA.

Create a Hosted IdP in the ForgeRock environment

1. Login to your ForgeRock tenant.
2. In the platform console, select **Native Consoles** > **Access Management**.

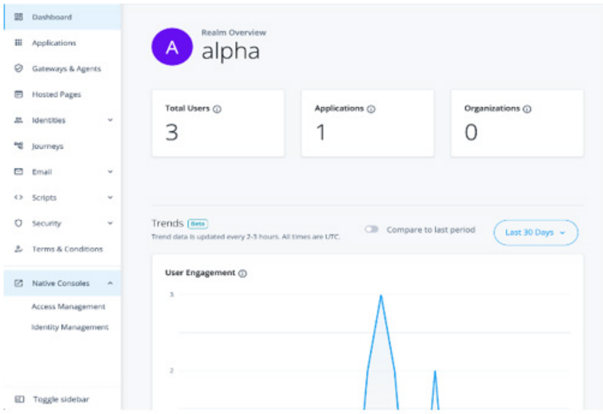


Figure 18. Access Management

3. Select **SAML Applications** from the **Quick Start** menu in the **Alpha Realm**.
4. In the **Entity Providers** tab, go to **Add Entity Provider** and select **Hosted** from the drop-down menu.

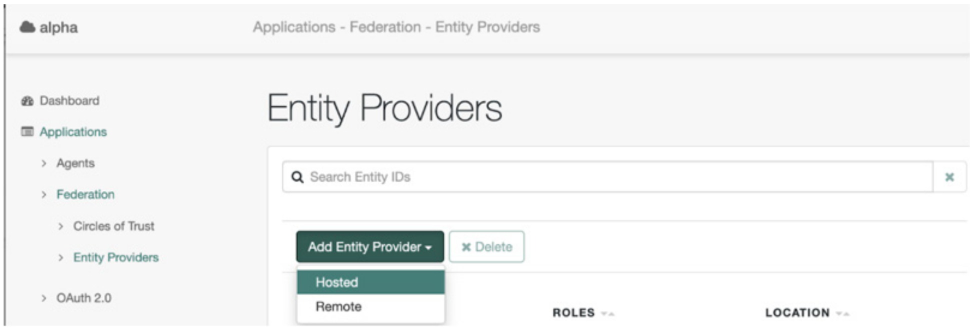
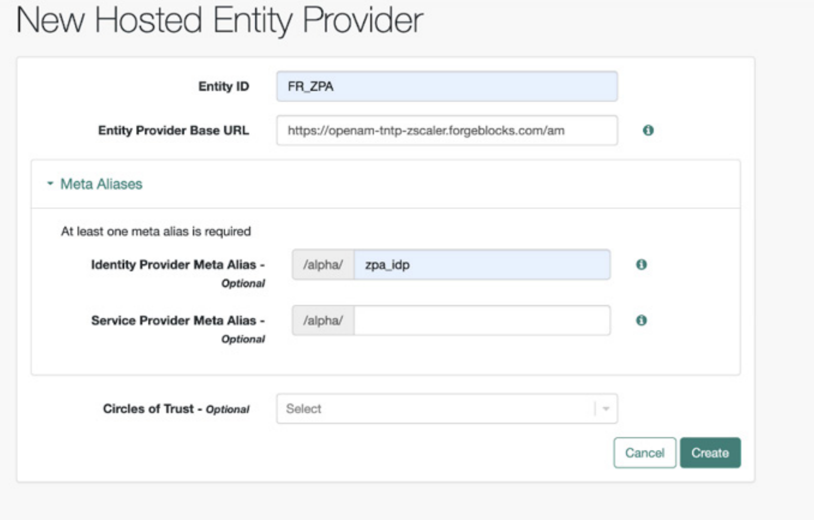


Figure 19. Entity Providers

5. In **New Hosted Entity Provider**, create an **Entity ID** name (i.e., `FR_ZPA`).
6. Create an **Identity Provider Meta Alias** name (i.e., `zpa_idp`).

©2022 Zscaler, Inc. All rights reserved.

7. Click **Create**.



New Hosted Entity Provider

Entity ID: FR_ZPA

Entity Provider Base URL: https://openam-tntp-zscaler.forgeblocks.com/am

Meta Aliases

At least one meta alias is required

Identity Provider Meta Alias - *Optional*: /alpha/ zpa_idp

Service Provider Meta Alias - *Optional*: /alpha/

Circles of Trust - *Optional*: Select

Figure 20. New Hosted Entity Provider

8. Create a URL for metadata in the following format:

```
[ServerURL]/saml2/jsp/exportmetadata.jsp?entityid=[entityID]&realm=/realmname
```

- `[ServerURL]` is the full AM server URL.
- `[entityID]` is the name of your entity provider.
- `realmname` is the name of the realm in which the entity provider is configured.

9. Using the details of the above configuration, ensure your URL looks like the following:

```
"https://openam-tntp-zscaler.forgeblocks.com/am/saml2/jsp/exportmetadata.jsp?entityid=FR_ZPA&realm=/alpha"
```

10. Export this URL to an .xml file and save it. It is needed when adding the IdP configuration to the ZPA Admin Portal.

Add IdP to ZPA

Next, add this IdP configuration to the ZPA Admin Portal:

1. Navigate to **Administration** > **Authentication** > **IdP Configuration**.

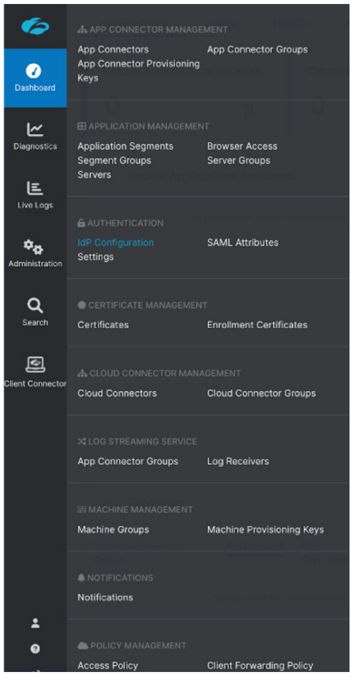
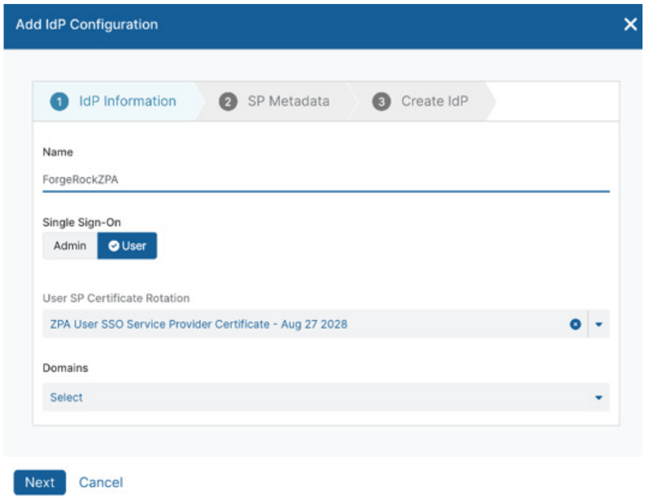


Figure 21. Authentication in the ZPA Admin Portal

2. Under **IdP Configuration**, click **+**.
3. In the **IdP Information** tab:
   - **Name** the IdP (i.e., `ForgeRockZPA`).
   - Select **User** for **Single Sign-On**.
   - Select **dev.forgerock** under **Domains**.
4. Click **Next**.


Add IdP Configuration

1 IdP Information | 2 SP Metadata | 3 Create IdP

Name: ForgeRockZPA

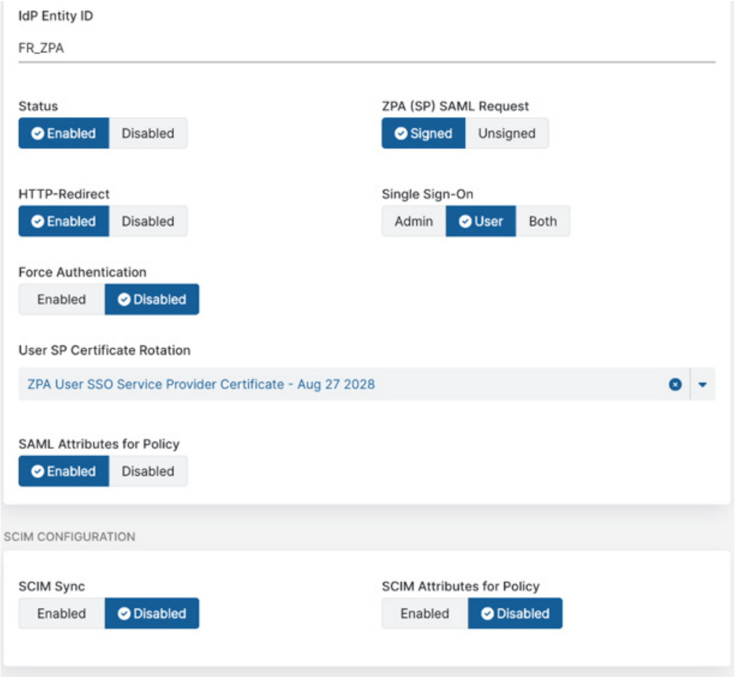
Single Sign-On: Admin [✓ User]

User SP Certificate Rotation: ZPA User SSO Service Provider Certificate - Aug 27 2028

Domains: Select

Figure 22. Adding IdP Information in the ZPA Admin Portal

5. In the **SP Metadata** tab, download the Service Provider Metadata.
6. In the **Create IdP** tab, select the Metadata file created in ForgeRock Access Management.
7. The **IdP certificate**, **Single Sign-On URL**, and **IdP entity ID** fields are auto-filled.
8. Make sure the fields correspond:



IdP Entity ID
FR_ZPA

Status: ● Enabled | Disabled

ZPA (SP) SAML Request: ● Signed | Unsigned

HTTP-Redirect: ● Enabled | Disabled

Single Sign-On: Admin | ● User | Both

Force Authentication: Enabled | ● Disabled

User SP Certificate Rotation
ZPA User SSO Service Provider Certificate - Aug 27 2028

SAML Attributes for Policy: ● Enabled | Disabled

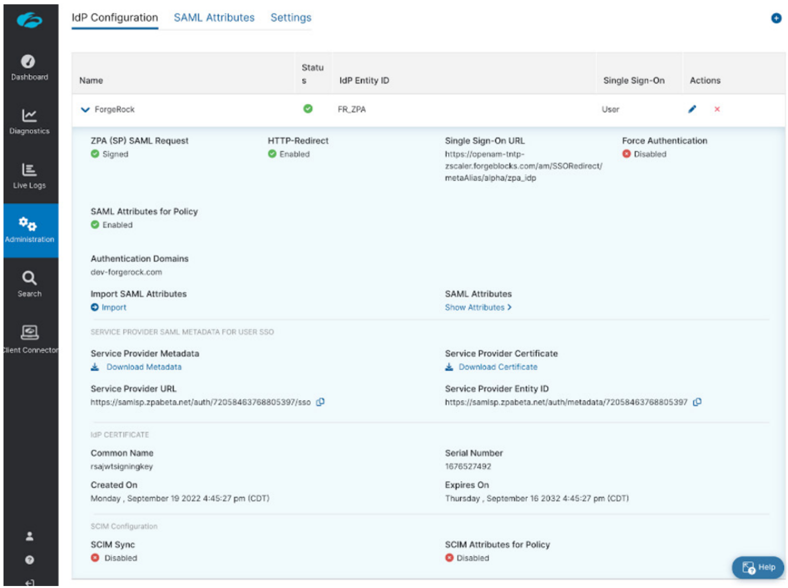
SCIM CONFIGURATION

SCIM Sync: Enabled | ● Disabled

SCIM Attributes for Policy: Enabled | ● Disabled

Figure 23. Checking the IdP Entity ID in the ZPA Admin Portal

9. Save the IdP configuration:



IdP Configuration | SAML Attributes | Settings

Name	Status	IdP Entity ID	Single Sign-On	Actions
ForgeRock	✓	FR_ZPA	User	

ZPA (SP) SAML Request
✓ Signed

HTTP-Redirect
✓ Enabled

Single Sign-On URL
https://openam-tntp-zscaler.forgeblocks.com/am/SSORedirect/metaAlias/alpha/zpa_idp

Force Authentication
✕ Disabled

SAML Attributes for Policy
✓ Enabled

Authentication Domains
dev-forgerock.com

Import SAML Attributes
Import

SAML Attributes
Show Attributes >

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata
Download Metadata

Service Provider Certificate
Download Certificate

Service Provider URL
https://samlsp.zpabeta.net/auth/72058463768805397/sso

Service Provider Entity ID
https://samlsp.zpabeta.net/auth/metadata/72058463768805397

IdP CERTIFICATE

Common Name
rsajwtsigningkey

Serial Number
1676527492

Created On
Monday , September 19 2022 4:45:27 pm (CDT)

Expires On
Thursday , September 16 2032 4:45:27 pm (CDT)

SCIM Configuration

SCIM Sync
✕ Disabled

SCIM Attributes for Policy
✕ Disabled

Figure 24. Saving the IdP Configuration details in the ZPA Admin Portal

Configure ZPA as Remote SP

Return to the ForgeRock Access Management Console and configure ZPA as the Remote SP:

1. In the platform console of ForgeRock Access Management, select **Applications** > **Federation** > **Entity Providers**.
2. Under **Add Entity Providers**, select **Remote**.

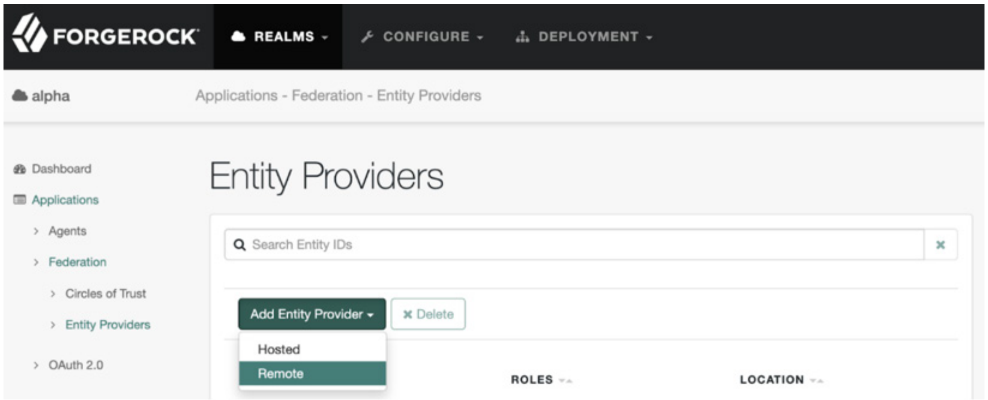


Figure 25. Entity Providers

3. In the import files section of **New Remote Entity Provider**, drag and drop the SP Metadata downloaded from the ZPA Admin Portal.

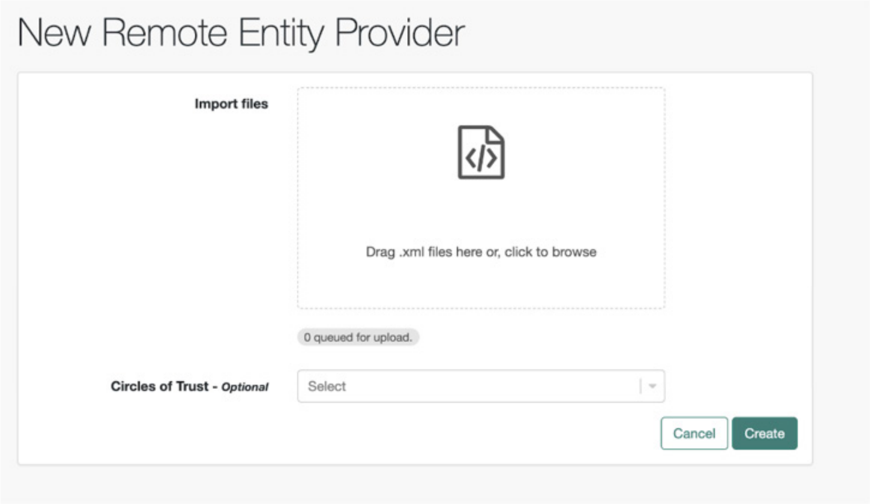
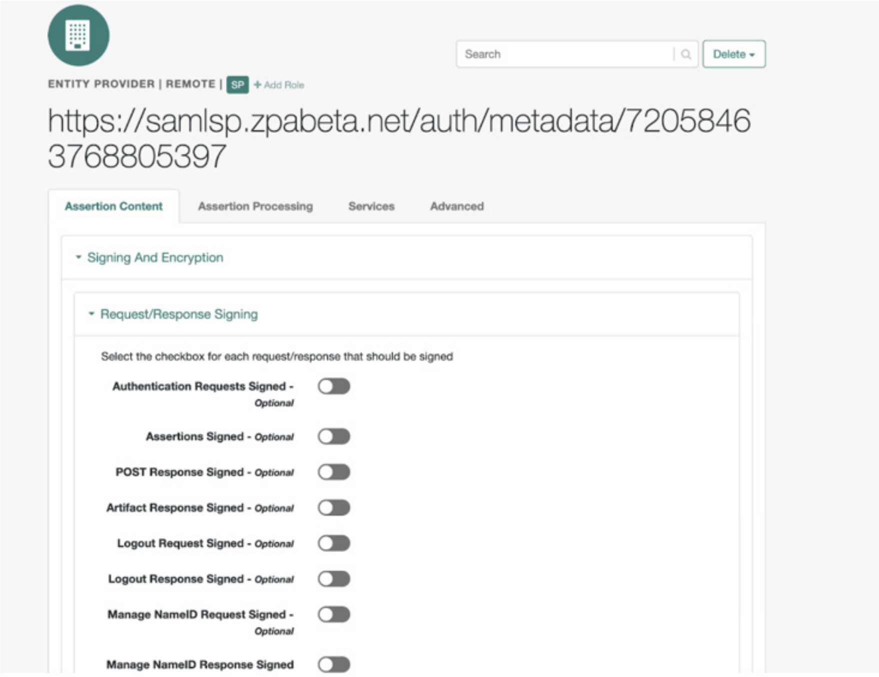

New Remote Entity Provider
Import files
Drag .xml files here or, click to browse
0 queued for upload.
Circles of Trust - Optional
Select
Cancel
Create

Figure 26. New Remote Entity Provider

4. Click **Create** and the form is auto-filled.



ENTITY PROVIDER | REMOTE | SP

https://samlsp.zpabeta.net/auth/metadata/7205846 3768805397

▾ Signing And Encryption

▾ Request/Response Signing

Select the checkbox for each request/response that should be signed

Authentication Requests Signed - *Optional*

Assertions Signed - *Optional*

POST Response Signed - *Optional*

Artifact Response Signed - *Optional*

Logout Request Signed - *Optional*

Logout Response Signed - *Optional*

Manage NameID Request Signed - *Optional*

Manage NameID Response Signed

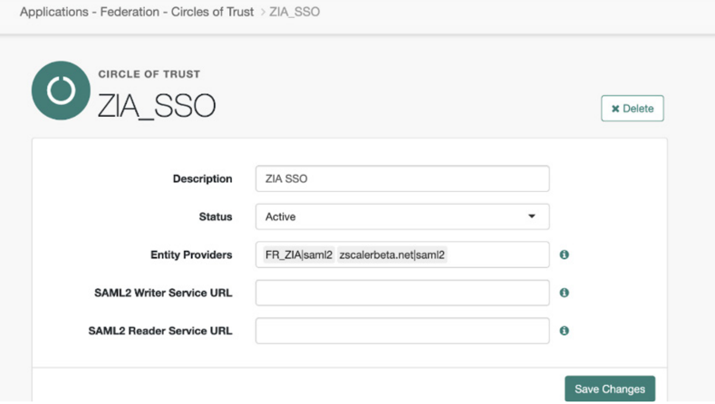
Figure 27. Add metadata

5. Navigate to **Entity Providers** and check that both your SP and IdP are created.

Configure Circle of Trust

To configure the Circle of Trust:

1. In the platform console, select **Applications** > **Federation** > **Circle of Trust**.
2. Select **Add Circle of Trust**.
3. **Name** the Circle of Trust (i.e., `ZPA_SSO`).
4. Add a **Description** (i.e., `ZPA SSO`).
5. Under **Entity Providers**, select the IdP and SP.
6. Click **Save Changes**.



Applications - Federation - Circles of Trust › ZIA_SSO

CIRCLE OF TRUST

ZIA_SSO

Description	ZIA SSO
Status	Active
Entity Providers	FR_ZIA|saml2 zscalerbeta.net|saml2
SAML2 Writer Service URL	
SAML2 Reader Service URL	

Figure 28. Circle of Trust

Testing

To test the IdP initiated SSO:

1. Go to the ForgeRock Admin Console.
2. In the platform console, select **Identities** > **Manage**.
3. Under **Manage Identities**, create and configure ForgeRock-hosted identity resources.
4. Click **+New Alpha Realm- User**.
5. In the **New Alpha realm - user** window, fill in the values.
6. Click **Save**.

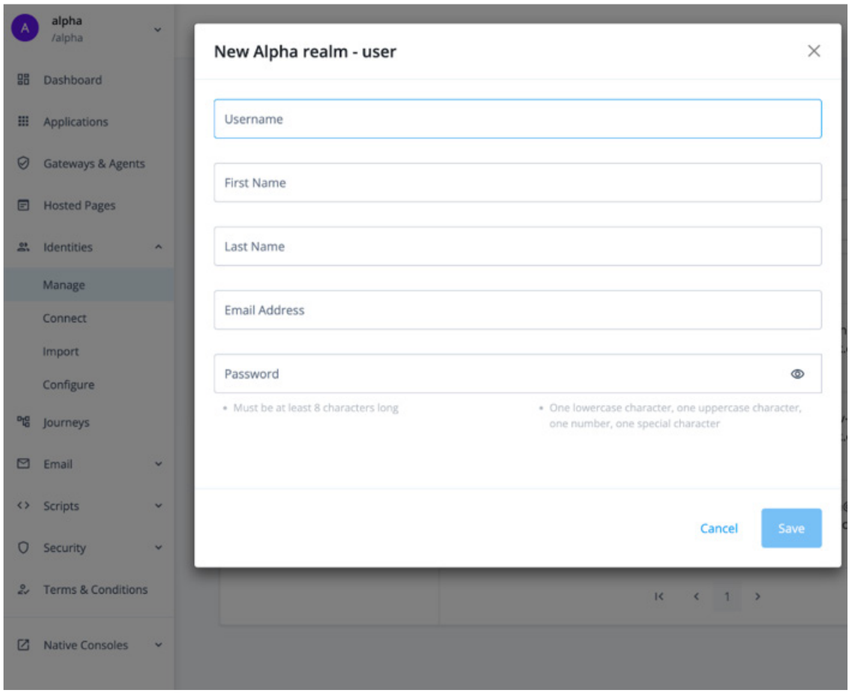


Figure 29. Test user

7. Use the beta cloud test URL in an incognito browser page. You are redirected to the **ForgeRock Sign In** page.

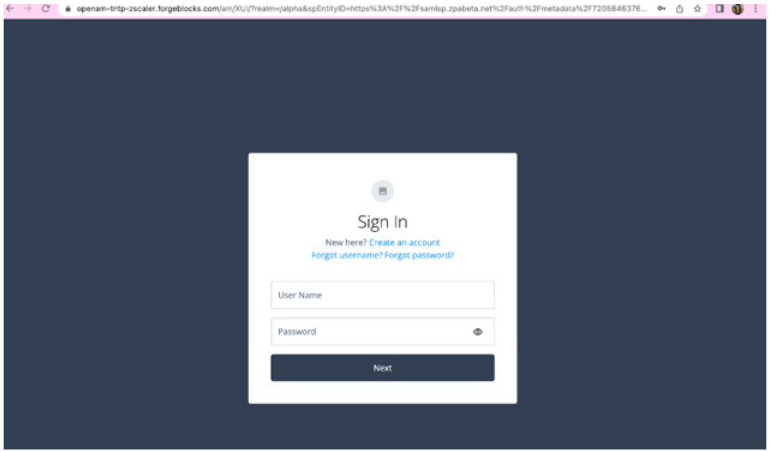

openam-tntp-zscaler.forgeblocks.com/am/XUI/?realm=/alpha&spEntityID=https%3A%2F%2Fsamlsp.zpabeta.net%2Fauth%2Fmetadata%2F7205846376...
Sign In
New here? Create an account
Forgot username? Forgot password?
User Name
Password
Next

Figure 30. ForgeRock Sign In

8. Enter the **User Name** and **Password**.

Appendix A: Requesting Zscaler Support

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

To contact Zscaler Support:

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

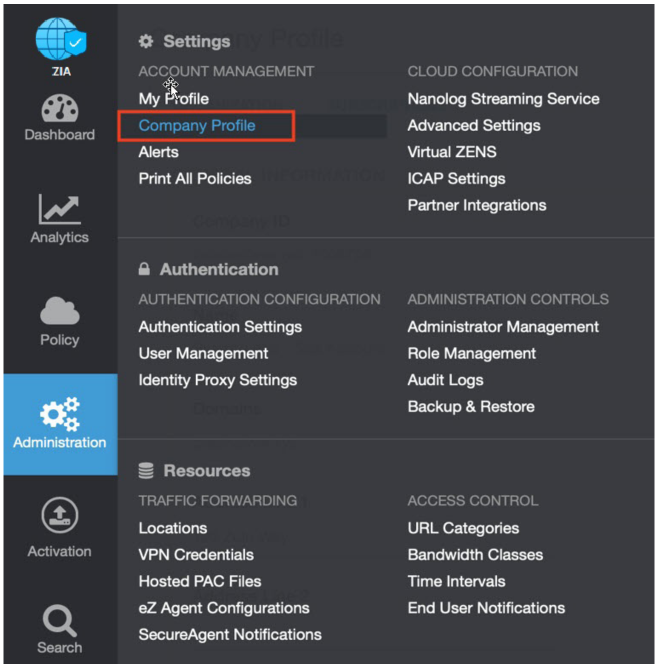
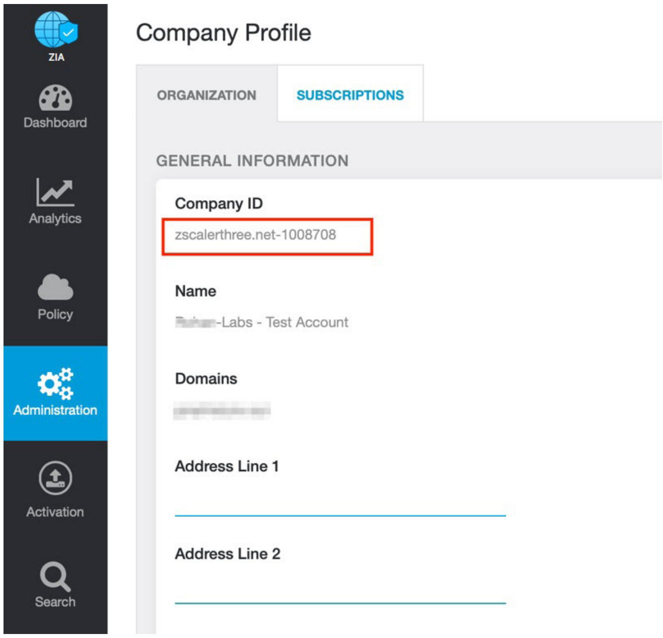


Figure 31. Collecting details to open support case with Zscaler TAC

2. Copy your Company ID.



Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 32. Company ID

©2022 Zscaler, Inc. All rights reserved.

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

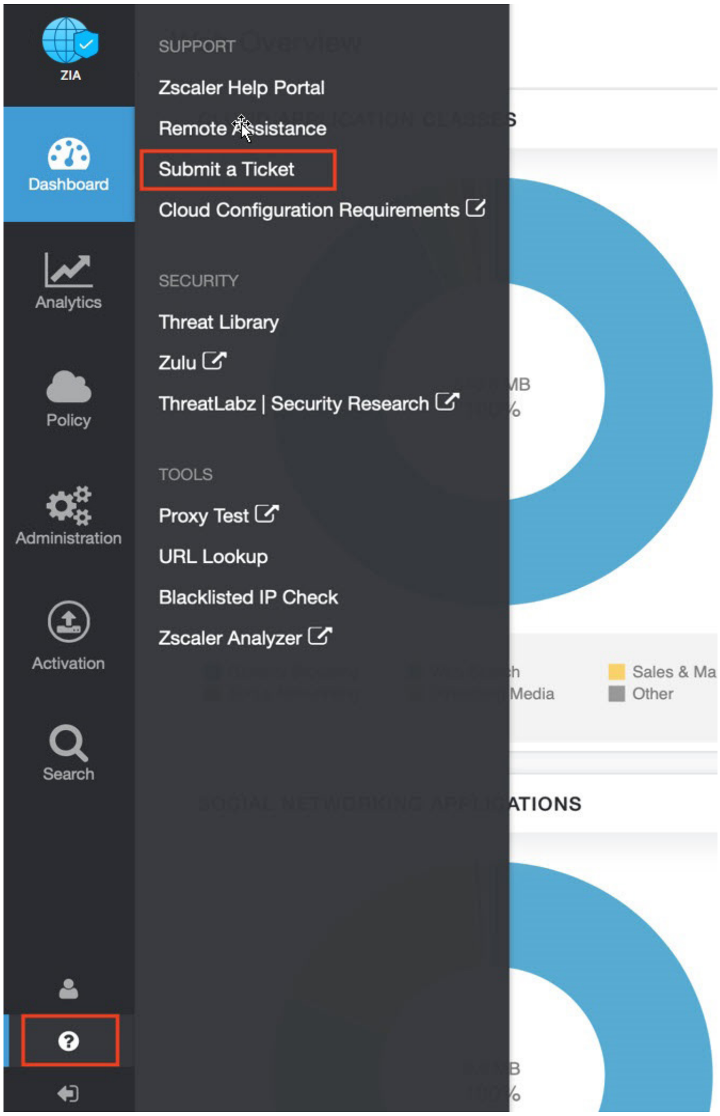


Figure 33. Submit a Ticket