# Table of Contents

1 Okta Authentication and Provisioning in use with Zscaler Services .......................... 7  
1.1 Overview .......................................................................................................................... 7  

2 Configure Okta and ZIA – SAML and SCIM ................................................................. 9  
2.1 Enable Okta ..................................................................................................................... 9  
2.2 Add the Zscaler ZIA Application ................................................................................... 10  
2.3 Configure Okta for ZIA ................................................................................................. 13  
2.4 Configure Zscaler ZIA for an Okta IdP ....................................................................... 16  
2.5 Assign ZIA to Users or Groups .................................................................................... 19  
2.6 Configure SCIM for ZIA ............................................................................................... 20  
2.7 Configure Groups to Push to ZIA ............................................................................... 22  

3 Configure Okta and ZPA – SAML and SCIM ............................................................... 23  
3.1 Add the Zscaler ZPA Application to Okta .................................................................... 23  
3.2 Configure Okta Initial Step for ZPA – SAML and SCIM ............................................. 26  
3.3 Configure ZPA for Okta – SAML and SCIM ................................................................. 27  
3.4 Configure Okta and ZPA Continued – SAML and SCIM ............................................ 32  
3.5 Assign ZPA to Authenticating Users .......................................................................... 34  
3.6 Configure Okta SCIM for ZPA ..................................................................................... 35  
3.7 Configure which Groups to Push using SCIM ............................................................. 39  
3.8 Test the ZPA Authentication Configuration .................................................................. 40  

4 Using Okta for ZIA Admin Access .................................................................................. 42  
4.1 Add the Okta SAML Application .................................................................................. 42  
4.2 Okta SAML Service Provider Application ................................................................. 43  
4.3 Configure the Application .......................................................................................... 44  
4.4 Save the Certificate ................................................................................................. 46  
4.5 Assign to App to the ZIA Administrators .................................................................. 48  
4.6 Configure ZIA for Admin SSO .................................................................................. 49  
4.7 Enable SAML for ZIA Admins ................................................................................... 50  
4.8 Add ZIA Administrators ......................................................................................... 51  
4.9 Test the Admin SSO Access ..................................................................................... 52  

5 Using Okta for ZPA Admin Access ................................................................................ 53  
5.1 Add the Okta Application for ZPA SAML Administrator Access ................................ 53  
5.2 Configuring the Okta IdP – Save the Metadata ......................................................... 56  
5.3 Add the ZPA IdP for Admin SSO on the ZPA UI ....................................................... 57  
5.4 Configuring the ZPA IdP Information on the ZPA UI ................................................. 58  
5.5 Copy the ZPA SP URLs .............................................................................................. 59  
5.6 Configure the Okta IdP on the ZPA UI ....................................................................... 60  
5.7 Define the Administrators for SAML Access .............................................................. 61
5.8 Finish the Okta Configuration on the Okta UI ................................................................. 64
5.9 Assign the Administrators or Groups to the Application .................................................. 66
5.10 Test the ZPA Authentication Configuration ...................................................................... 67
5.11 Administrator Sign In Using SAML from the ZPA Admin Portal ..................................... 68

6 Transparent SSO using IWA with Okta .............................................................................. 69

7 PAC File and Zscaler Client Connector – Authentication Bypasses .................................... 70

8 Appendix A: Capture the SAML Request for Troubleshooting ........................................ 71
8.1 How to View a SAML Response in Your Browser for Troubleshooting ............................. 71
  Google Chrome ...................................................................................................................... 71
  Mozilla Firefox ...................................................................................................................... 71
  Apple Safari ........................................................................................................................... 72
  Microsoft Internet Explorer ..................................................................................................... 72
8.2 Configuring your Browser to Capture the SAML Response .............................................. 73
8.3 Zscaler Resources ........................................................................................................... 81
8.4 Okta Resources ................................................................................................................ 82
# Terms and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SCIM</td>
<td>System for Cross-domain Identity Management</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>AD</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td>ADFS</td>
<td>Microsoft Active Directory Federation Services</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-factor Authentication</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
<tr>
<td>IWA</td>
<td>Integrated Windows Authentication</td>
</tr>
</tbody>
</table>
About This Document

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 services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to 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 on Zscaler, please visit www.zscaler.com or follow them 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. For more information on Okta, please visit www.okta.com or follow them on Twitter @okta.
Audience

This guide is written for Authentication Administrators, IT Administrators, and IT Analysts responsible for deploying, monitoring and managing authentication and provisioning services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Software Revisions

This document was authored using Zscaler Internet Access v6.0 and Okta Production Release 2020.08.0.

Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at partner-doc-support@zscaler.com.
1 Okta Authentication and Provisioning in use with Zscaler Services

1.1 Overview

Identity, Authentication, and Provisioning is an inherent part of the Zscaler solution and allows Zscaler to provide granular user visibility, logging, and security to an organization down to the individual user level.
Authentication is the process of verifying a user’s identity through the use of credentials and optionally other additional identity factors. SAML (Security Assertion Markup Language) is the preferred method for authentication for both Zscaler Internet Access and Zscaler Private Access and for this document Okta will be configured as the SAML identity provider (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). Although beyond the scope of this document, SAML also provides Single-Sign On to any SAML SP. An example of this would be gaining access to both Zscaler Internet Access (ZIA) and Zscaler Private Access by entering your credentials a single time instead of having to enter it for both ZIA and ZPA. SSO greatly enhances the user experience by providing a cohesive solution to a modern Cloud and SaaS environment. SAML and SSO are the catalyst to make a unified solution possible.

Provisioning as it relates to authentication is the automation of provisioning and deprovisioning of users and security groups to Zscaler services. SCIM (System for Cross-domain Identity Management) 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 will automatically provision the user and the associated security groups in the Zscaler database and likewise, when a user is deprovisioned, the user, associated groups, and credentials are also removed preventing access to resources. The primary use case would be for onboarding and offboarding users from an organization. When a user leaves an organization, the user is deprovisioned from the user directory and SCIM will make the associated changes in the Zscaler databases eliminating all ZIA and ZPA access. SCIM would then deprovision the user from all associated databases, preventing further access to company resources.

For more information, please see the resources in Appendix A: Zscaler Resources.
2 Configure Okta and ZIA – SAML and SCIM

2.1 Enable Okta

The scope of this document assumes that the user has a working Okta environment, and only the Zscaler applications need to be installed and configured to provide a working Zscaler / Okta solution. However, a new, no cost Okta developer instance was created from the Okta website at https://developer.okta.com/ and used to create this document. Each step was validated for functionality in a live environment. The above figure shows to select the Classic UI and the shortcuts at the right give us an indication of what needs to be configured for SAML authentication to work.
2.2 Add the Zscaler ZIA Application

The first step is to add the Zscaler Applications to Okta that will used to enable authentication and provisioning to the Zscaler service. From the Okta portal administrator account, select Application and then select Add Application.

Figure 3: Adding an Application
To add the appropriate Zcaler application, search for “zcaler” and then select the Zcaler 2.0 application for Zcaler Internet Access (ZIA).
When you select Add Zscaler 2.0 it will bring up the initial configuration screen and ask for your Zscaler Domain. This is the Zscaler Internet Access (ZIA) cloud your organization’s tenant is associated with. The Zscaler Cloud continues to expand but currently will be one of the following cloud domains (zscaler.net, zscalerone.net, zscalertwo.net, zscalerthree.net, or zscloud.net). This information can be found in your Zscaler UI under **Administration / Company Profile / Company ID**. In the following Company ID example (zscloud.net-3173833) “zscloud.net” would be the Zscaler Cloud that would be entered as the Zscaler Domain for the Okta setup. Select both options for Application Visibility as it does not apply to Zscaler Internet Access or Zscaler Private Access.
2.3 Configure Okta for ZIA

Select the Sign On tab and then select Edit under Settings.

Figure 6: Okta Sign On Configuration
Using the memberOf pulldown menu, select **Matches regex** and **set the match to “.*”** (period, asterisk). This will allow all memberOf groups to be included as SAML Assertion attributes. Likewise, the matching condition can be set to match only certain groups if needed.
for filtering. Select the **View Setup Instructions** button to gain access to the required SAML Portal URL and Public certificate. These will be used for the Zscaler side setup.

![SAML Portal URL and Public Certificate](image.png)

*Figure 8: The Zscaler SAML Portal URL and Public Certificate*

In step number 6 of the Okta setup instructions launched when selected View Setup Instructions, you will find the SAML Portal URL and the download link to the Okta Public Certificate. You will need to **copy the URL** and **download and save the Okta Public Certificate** for the Zscaler setup in the next step.
2.4 Configure Zscaler ZIA for an Okta IdP

To add Okta as an IdP log into your ZIA Portal and select **Administration / Authentication Settings**. This will bring up the Authentication settings screen.

![Figure 9: Adding Okta and the Zscaler Internet Access IdP](image-url)
Select **Add Identity Provider**. This will bring up the Edit Identity Provider screen.
This is the IdP configuration screen. **Give the IdP a Name**, make sure the Status is enabled, and then **paste in the SAML Portal URL** we saved from Page 14. **Enter in NameID** (Case Sensitive) for the Login Name Attribute, **Upload the Okta Public Certificate** from Figure 8, then **select Okta as the Vendor** profile. For the Default IdP leave the Locations and Authentication Domains as none. **Disable the Sign SAML Request** setting and **Enable SAML Auto Provisioning and SCIM-Based Provisioning**. Set the User Display Name Attribute to **DisplayName** (Case Sensitive), Set the Group Name Attribute to **memberOf** (Case Sensitive), and set the Department Name Attribute to **Department** (Case Sensitive). Lastly **copy the SCIM Base URL and Bearer Token** for the next step in the Okta Portal. **Save and Activate** the configuration. **Note**: Both Auto-Provisioning and SCIM-Provisioning will need to be enabled. SCIM will update any new additions, but existing users will initially use Auto-Provisioning.
2.5 Assign ZIA to Users or Groups

You must assign the ZIA Application to users who will be authenticating into Okta from ZIA. Select the Assignments tab at the top of the window, then select either People or Groups and then select Assign. In the above example the “Everyone” Group was selected so all users in the company will be able to authenticate.
## 2.6 Configure SCIM for ZIA

To enable SCIM Provisioning on the Okta portal select the **Provisioning Tab** and then select **Enable API Integration**. This will then bring up the Zscaler ID and API Token fields. **Enter the Base URL** copied from the Identity Provider config in the previous step into the **Zscaler ID** field. The Base URL will look like a traditional URL, but you will enter only the highlighted portion into the Zscaler ID field [https://scim.zscalernine.net/10656179/3585/scim](https://scim.zscalernine.net/10656179/3585/scim). Then **enter the Bearer Token** value into the **API Token** Field and save the configuration.
Once Enable API Integration has been enabled, new settings will appear for defining what events are synchronized by SCIM from Okta to Zscaler (i.e. the provisioning or de-provisioning of a new user). Select “To App” under SETTINGS in the side-bar on the left and then Select Create User, Update User Attributes, and Deactivate Users and then save the configuration.
2.7 Configure Groups to Push to ZIA

The final step is to select the Security Groups that will be pushed to Zcaler. This will enable and push the groups to Zcaler Internet Access immediately, and any new changes to the Okta data base will immediately be pushed to Zcaler. **Note:** However existing users will initially be provisioned by using Auto-Provisioning, not SCIM. This behavior is different from some of the other Identity Providers and is unique to Okta that both Auto-Provisioning and SCIM-Provisioning must be enabled simultaneously. To select the security groups to be pushed to Zcaler **select the Push Groups button** and then search and **add the appropriate group** or create a rule that matches multiple groups. The Groups will immediately be pushed, and any new user changes to those groups will be immediately synchronized to Zcaler.

Figure 15: Enable Security Groups to Sync
3 Configure Okta and ZPA – SAML and SCIM

3.1 Add the Zscaler ZPA Application to Okta

The first step is to add the Zscaler Applications to Okta that will used to enable authentication and provisioning to the Zscaler service. From the Okta portal administrator account, select Application and then select Add Application.

Figure 16: Adding an Application
To add the appropriate Zcaler application, **search for “zcaler”** and **select Zcaler Private Access 2.0** for Zcaler Private Access (ZPA).
Give the application a name or keep the default, **turn off application visibility** to the user by selecting the Do not display application icon to users or Okta Mobile, as it does not apply to Zscaler services and then **select Done**.
3.2 Configure Okta Initial Step for ZPA – SAML and SCIM

Now select the Sign On tab and save the Identity Provider metadata to a file. This file will be used on the ZPA side setup. The Next step in Okta will be to select Edit to edit the GroupName filter, and to enter the ZPA URLs. Let’s create the ZPA SP and configure Okta on the ZPA side. We will grab the URLs we need and then edit the above settings. Open a new browser window and Launch the ZPA UI.
3.3 Configure ZPA for Okta – SAML and SCIM

Figure 20: Creating the Okta IdP on ZPA

In the ZPA UI select Administration and then select IdP Configuration. This will bring up the IdP Configuration screen.
Figure 21: Add a new IdP

On the IdP configuration screen select Add IdP Configuration at the top right of the UI. This will bring up the IdP configuration wizard to walk you through the creation of the IdP.
Give the IdP an appropriate Name and leave the single Sign-on setting at User, **select the authentication domains** that will be services by this IdP, and then click **Next**.

**Note:** Multiple IdPs are supported in ZPA, and the IdP is bound to the domain in this step. ZPA only supports one domain for Client Connector deployments, additional IdPs are defined for Browser Access domains.
Figure 23: SP Metadata

For our next step in Okta we will need to copy the Service Provider URL and the Service Provider Entity ID. **Copy and Save both URL’s** and then **select Next**.
In our final ZPA IdP configuration screen, the first step is to upload the Okta Metadata file we saved on page 24. This will load the certificate and the Okta URL information. Then select Unsigned for the ZPA (SP) SAML Request, select Enable for the HTTP-Redirect. For SCIM select Enabled for SCIM Sync, then select Generate New Token. This will bring up our SCIM parameters we will need for the remaining Okta configuration. Save both the SCIM Service Provider Endpoint URL and the Bearer Token for the Okta configuration. Then select Save.
3.4 Configure Okta and ZPA Continued – SAML and SCIM

Back on the Okta config select the Sign On tab and then select Edit. This will open the SAML configuration screen.
Using the GroupName pulldown menu, select **Matches regex** and set the match to `.*` (period, asterisk). This will allow all groups to be included as SAML Assertion attributes. Likewise, the matching condition can be set to match only certain groups if needed for filtering. **Enter the Service Provider URL and the Service Provider Entity ID** copied from the ZPA IdP setup on page 29, then **select Save**. SAML is now configured for ZPA using Okta. The next step will assign ZPA 2.0 App to the users that will be authenticating from ZPA to Okta.
3.5 Assign ZPA to Authenticating Users

Figure 27: Assigning the ZPA Application

Select the Assignments tab at the top of the window and select Groups or Users to assign ZPA as an application in the organization. In this example it is all users in the company. To configure SCIM for auto provisioning and deprovisioning let move on to our next step.
3.6 Configure Okta SCIM for ZPA

To configure SCIM provisioning **select the Provisioning tab** under the Zcaler Private Access 2.0 Application. Then **select Configure API Integration**.

![Figure 28: Okta Provisioning](image)
Select Enable API Integration This will bring up the API parameters. Enter the SCIM Service Provider Endpoint URL and the Bearer Token that were save from the ZPA IdP screen on page 29 and then select the Test API Credentials. If the credentials are valid and Okta can communicate with the ZPA Cloud you should get the response highlighted in red above. If you receive an error, you will need to re-copy the URL and Token and possibly generate a new Bearer Token. Once you have verified your credentials select Save.
Select “To App” and then **select Edit**.
Select Enable for Create Users, Update User Attributes, and Deactivate Users then select Save.
3.7 Configure which Groups to Push using SCIM

The final step is to select which groups SCIM will push to ZPA automatically. **Select Push Groups** and search and add the desired groups.
3.8 Test the ZPA Authentication Configuration

We need to import the SAML variables in from Okta. To do this from the ZPA UI, select Administration / IdP Configuration, then select the little blue arrow next to your IdP. This will show the Okta configuration. Then select Import next to your domain under Import SAML Attributes. Once this is selected it will Authenticate to Okta using your existing User if you are authenticated or will bring up the Okta login screen. The SAML variables and the SAML assertion are then displayed in the screen on the next page.
Review your mappings and then save the variables by selecting Save.

You can also test by using the below URL. Replace testmypacket.com with your domain in the URL and your SAML Assertion will be returned if you are an already authenticated user or you will be prompted to authenticate. Once you are authenticated your SAML assertion will be displayed.

**Test URL:**

**SAML Assertion:**
{"nameid":"toddh@testmypacket.com","orgId":null,"idpEntityID":null,"idpId":null,"saml_attributes":{"FirstName":"Todd","LastName":null,"GroupName":[null,"Group1","Everyone","Group3"]},"samlassertion":null}
4 Using Okta for ZIA Admin Access

4.1 Add the Okta SAML Application

To use Okta SAML authentication for ZIA Admin users we must install the SAML Service Provider Application. From the Okta UI **select the Applications tab** at the top of the screen, and then **select Add Application**.
4.2 Okta SAML Service Provider Application

Figure 36: The Okta SAML Service Provider Application

Search for SAML and the **add the SAML Service Provider Application.**
4.3 Configure the Application

![General Settings](image)

**Figure 37: General Settings**

Give the application a name for the label and select Next.
Figure 38: Sign-On Options

This will bring up the Sign-On Options for the application. **Select View Setup Instructions.**
4.4 Save the Certificate

This will bring up a pop-up screen where we can download the Identity Provider Certificate. **Save the link to a file.** This will save the file as okta.cert, **rename the file to okta.cer.** This file will be imported into the Zscaler setup. Close the pop-up.
To finish the Okta sign-on configuration we need to **enter the Assertion Consumer Service URL and the Service Provider Entity Id.** The Service URL takes the form of https://admin.(zscalercloud).net/adminsso.do. The Zscaler Cloud continues to expand but currently will be one of the following cloud domains (zscaler.net, zscalerone.net, zscaltwo.net, zscalerthree.net, or zscloud.net). If your Cloud Domain is zscalerthree.net the Service URL would be [https://admin.zscalerthree.net/adminsso.do](https://admin.zscalerthree.net/adminsso.do) and the Entity Id would be admin.zscalerthree.net. Then **select Done** to finish the configuration.
4.5 Assign to App to the ZIA Administrators

The final Okta step is to assign the application to the ZIA Administrators. **Select the Assignments tab** at the top of the screen and then **select the Assign button**. Select the Administrators and save the configuration. We are now ready to configure Zscaler.
4.6 Configure ZIA for Admin SSO

Open the ZIA UI and select Administration / Administrator Management.
4.7 Enable SAML for ZIA Admins

Select Administrator Management at the top of the screen and then select Enable SAML Authentication. We now need to select and upload the okta.cer file we saved in the previous step on page 46 and then save the configuration.
4.8 Add ZIA Administrators

![Figure 44: Adding Administrators](image)

Select the Administrators tab at the top of the window and then select **Add Administrator**. You will need to add an administrator for every user that you will want to use SAML and the Okta application. You can select SAML only or SAML and Password as options for the user’s authentication methods.
4.9 Test the Admin SSO Access

Figure 45: SAML Variable Import

You are now ready to launch the ZIA UI from the Okta portal and the SAML application.
5 Using Okta for ZPA Admin Access

5.1 Add the Okta Application for ZPA SAML Administrator Access

To configure Admin Access using SAML SSO we need to configure a second IdP specifically for ZPA admin SSO. To do this we need to install a second instance of the Zscaler Private Access 2.0 Application. From your Okta UI select the Applications Tab at the top of the window and then select Add Application.
Search for Zscaler in the search bar and then select the Zscaler Private Access 2.0 Application.
Figure 48: General Settings

**Give the Application a unique name** and select **Done**.
5.2 Configuring the Okta IdP – Save the Metadata

The next step before we create the Zscaler ZPA IdP is to download and save the Okta Application Metadata. Select the Sign On Tab at the top of the Window and then download the Metadata information as a file. This can be accomplished by right clicking the hyperlink and saving the file with the Save Link As option.

Figure 49: Application Metadata Location
5.3 Add the ZPA IdP for Admin SSO on the ZPA UI

Now that we have the metadata for the configuration, the next step is to bring up the ZPA UI and add the Okta IdP. **Select Administration / IdP Configuration**, then **select Add IdP Configuration** at the top right of the ZPA UI. If the browser window is small the Add IdP Configuration may show up as only a blue circle with a white plus sign in it.
5.4 Configuring the ZPA IdP Information on the ZPA UI

When you click the Add IdP Configuration the IdP Configuration Wizard will be launch. **Give the IdP a unique name, select Admin under Single Sign-On, and select the organization’s domain/s that the Administrators will be signing in from. Then select Next.**
5.5 Copy the ZPA SP URLs

The SP Metadata page is now displayed. Copy and save the Service Provider URL and the Service Provider Entity ID URL. These will be used to finish the Okta side configuration. Once you have the URL saved select Next.
5.6 Configure the Okta IdP on the ZPA UI

To finish the configuration, **select and upload the Okta Metadata file** we saved on Page 56, **then select Save** to finish the IdP configuration.
5.7 Define the Administrators for SAML Access

Administrators that will be using the SAML IdP for authentication must be defined as Administrators. To configure the administrators that will be authenticating, select Administration / Administrators.

Figure 54: Creating an Administrator
This will bring up the Add Administrator Screen. **Select Add Administrator** in the upper right corner of the UI. If the browser window is small the Add Administrator Configuration may show up as only a blue circle with a white plus sign in it.
Figure 56: Create an Administrator

The Add Administrator window will now be displayed. Enter the Admin ID, the Password and Password Verification, Select ZPA Administration from the Role pulldown, and enter an Email Address and a Phone number (without formatting). Then select Save to complete the ZPA configuration. We are now ready to complete the Okta configuration.
5.8 Finish the Okta Configuration on the Okta UI

To finish the Okta configuration select the Sign On tab at the top of the configuration Window and then select Edit to edit the configuration.
Enter the Service Provider URL and the Service Provider Entity ID we saved from page 59. Then select Save.
5.9 Assign the Administrators or Groups to the Application

The final step is to assign the ZPA Administrators to the application. This can be defined by individual users and/or a security group. Select the Assignments tab at the top of the app configuration window, select People or Groups to define the type of assignment variable, and then select the User or Group. Our configuration is now complete.
5.10 Test the ZPA Authentication Configuration

We can now see our applications from the Okta portal for the Administrator. By clicking on the application, the app will launch the ZPA UI and Authenticate the user transparently. We can also login from the ZPA Admin sign-on screen.
5.11 Administrator Sign In Using SAML from the ZPA Admin Portal

To sign in from the ZPA Admin Screen using the Okta SAML IdP select the Single Sign-On Using IdP option and then select Sign In. This will launch the Okta Authentication Screen.

Figure 63: Administrator Sign-On using our SAML IdP
6  Transparent SSO using IWA with Okta

For transparent authentication when using Okta and Zscaler, Zscaler can take advantage of Integrated Windows Authentication (IWA) if it has been configured for the Okta environment. It is not a Zscaler feature or configuration and IWA works between Okta and the Windows Active Directory Server, however Zscaler is able to take advantage of a working IWA environment.

IWA is a Microsoft feature that will allow a user to automatically authenticate using the users Windows Active Directory authentication credentials. IWA will work in an Okta environment by using either the Okta Desktop or the Okta IWA Web App that runs on an IIS server in the customers domain. For more information and a demonstration of using IWA in an Okta environment, Please see Appendix A in the back of this guide.

Figure 64: Okta IWA Web Server Authentication Flow
7 PAC File and Zscaler Client Connector – Authentication Bypasses

When using Zscaler Internet Access you must bypass the IdP provider login URL’s for Authentication to succeed. For ZPA it is not a requirement and the destination URL’s can flow through ZIA, but bypassing the URLs for ZIA is a requirement for both Browser PAC files and for the Zscaler Client Connector.

The below entries need to be added to your Browser PAC and/or the Zscaler Client Connector Custom Pac File for the Application Profile. For more information see Appendix A in the back of this guide.

**PAC File Bypasses:**
```plaintext
// 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 and the below procedures can be used to find and decode the SAML Assertion to look at the attributes returned by the IdP. These steps were written to capture the Assertion by using the Chrome Browsers Developer Tools and then decoding it using a base 64 decoder on the desktop. This was selected as the most secure method. You can use browser extensions, and/or cloud based base64 decoders, but when clear text passwords are present in the data, keeping things in house are always more secure. Any browser can be used to capture the SAML Assertion and the procedures for the most common browsers are listed below.

8.1 How to View a SAML Response in Your Browser for Troubleshooting
To troubleshoot Single Sign On (SSO) login issues, it can be helpful to retrieve the SAML response from your service provider from in your browser.

Google Chrome - To view a SAML response in Chrome

- Press F12 to start the developer console.
- Select the Network tab, and then select Preserve log.
- Reproduce the issue.
- Look for a SAML Post in the developer console pane. Select that row, and then view the Headers tab at the bottom. Look for the SAMLResponse attribute that contains the encoded request. Note: 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

- Press F12 to start the developer console.
- In the upper right of the developer tools window, click options (the small gear icon). Under Common Preferences select Enable persistent logs.
- Select the Network tab.
- Reproduce the issue.
- 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. Note: 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

- Enable Web Inspector in Safari. Open the Preferences window, select
  the Advanced tab, and then select Show Develop menu in the menu bar.
- Now you can open Web Inspector. Click Develop, then select Show Web Inspector.
- Select the Resources tab.
- Reproduce the issue.
- Look for a POST method with a samlconsumer file in the table.
- Scroll down to find Request Data with the name SAMLResponse. Note:
  The SAMLResponse attribute contains the encoded request; use a Base64 decoder to
  investigate the decoded response.

Microsoft Internet Explorer
To view a SAML response in Internet Explorer
The best way analyze network traffic in Internet Explorer is through the use of a third-party

tool.

- Follow the steps at http://social.technet.microsoft.com/wiki/contents/articles/3286.ad-fs-
  2-0-how-to-use-fiddler-web-debugger-to-analyze-a-ws-federation-passive-sign-
  in.aspx to download and install Fiddler and capture the data.

What to do with the Base64-encoded SAML response
Once you find the Base64-encoded SAML response element in your browser, copy it and use
your favorite Base-64 decoding tool to extract the XML tagged response.

Security Tip
Because the SAML response data that you are viewing might contain sensitive security data,
we recommend that you do not use an online base64 decoder. Instead use a tool installed on
your local system.
8.2 Configuring your Browser to Capture the SAML Response

The first step is to configure Zscaler as a Proxy for your browser. You can configure the automatic FQDN that will select the fastest gateway response as the proxy. The FQDN is gateway.zscalerthree.net, where zscalerthree will be replaced by your cloud (i.e. gateway.zscloud.net, gateway.zscalertwo.net, etc...). However, for this exercise let’s manually select the proxy from our list of enforcement nodes. Enter your Clouds information center, in the above example the URL is ips.zscalerthree.net/cent this will list all of the enforcement nodes for the Zscalerthree Cloud. The Dallas IP will then be used as the Proxy address we will define in our Browser.
Open the proxy configuration screen for the browser you are going to test with and enter in the Proxy IP address we just copied. You will also need to enter in the Okta domains as bypasses so the request will make it to Okta and not be blocked by ZIA. The three okta domains to bypass are .okta.com, oktacdn.com, and .oktapreview.com. Save the changes and you are now ready to test.
Enter any URL in the browser and ZIA will now prompt you for authentication credentials. At this point we want to start our developer tools. Select the three dots at the top right of the browser. This will bring up a drop-down menu, then select More Tools, and then Developer Tools. This will start the developer screen.
We now have our network trace which will show us the connection and packet information as we authenticate into Zscaler and Okta. The initial authentication screen above is only looking for the user domain appended to the User ID so Zscaler knows which Zscaler instance to direct the request to. In this case testmypacket.com.
Zscaler has redirected the authentication request to Okta, and we now get the Okta authentication screen. Log in with a valid User ID in the Okta database associated with the Zscaler instance.

Figure 39: Authenticate to the Okta IdP
Once authentication has completed, select the packet called sfc_sso that is destined to login.zscalerthree.net. This is our SAML response from Okta and contains our SAML Assertion. The Assertion is base64 encoded and we will need to use a decoder to get the clear text information. Select the SAML Response data excluding “SAMLResponse:” we want only the data.
Using a base64 decoder, paste the encoded text into the application and then copy the decoded SAML Assertion and let’s take a look. The Base64Anywhere app was used for this demonstration and was downloaded free from the Mac App store. There are also free decoders on the Windows store if you are a Microsoft user.
Figure 42: SAML Attributes in the Decoded Assertion

We can now see our clear text Assertion with the NameID of the user and our other attributes. In this example you see that the user is part of a group called "Everyone". All groups and attributes associated with the user can be seen in this response.
8.3 Zscaler Resources

Zscaler Enforcement Node Ranges
https://ips.zscalerthree.net/cenr

Zscaler Internet Access (ZIA)
https://www.zscaler.com/products/zscaler-internet-access

ZIA Best Practices for Traffic Forwarding

ZIA – Configuring SAML and SCIM for Okta

ZPA – Configuring SAML and SCIM for Okta

IWA – Mark Ryan’s IWA / Okta Demonstration
https://www.youtube.com/watch?v=CtRljdMDchc&list=PLLCE8u9uBMMugp00PC91GOpmez5kD_V1hn&index=59&t=0s

Zscaler Client Connector – App Profile
https://help.zscaler.com/z-app/configuring-zscaler-app-profiles

Tunnel-2 Bypasses

Zscaler Hosted PAC files
8.4 Okta Resources

Okta Help Center
https://support.okta.com/help/s/?language=en_US

Okta How to Configure SAML for Zscaler

Okta IWA Server