

Slide 1 - ZCCP-IA



Authentication

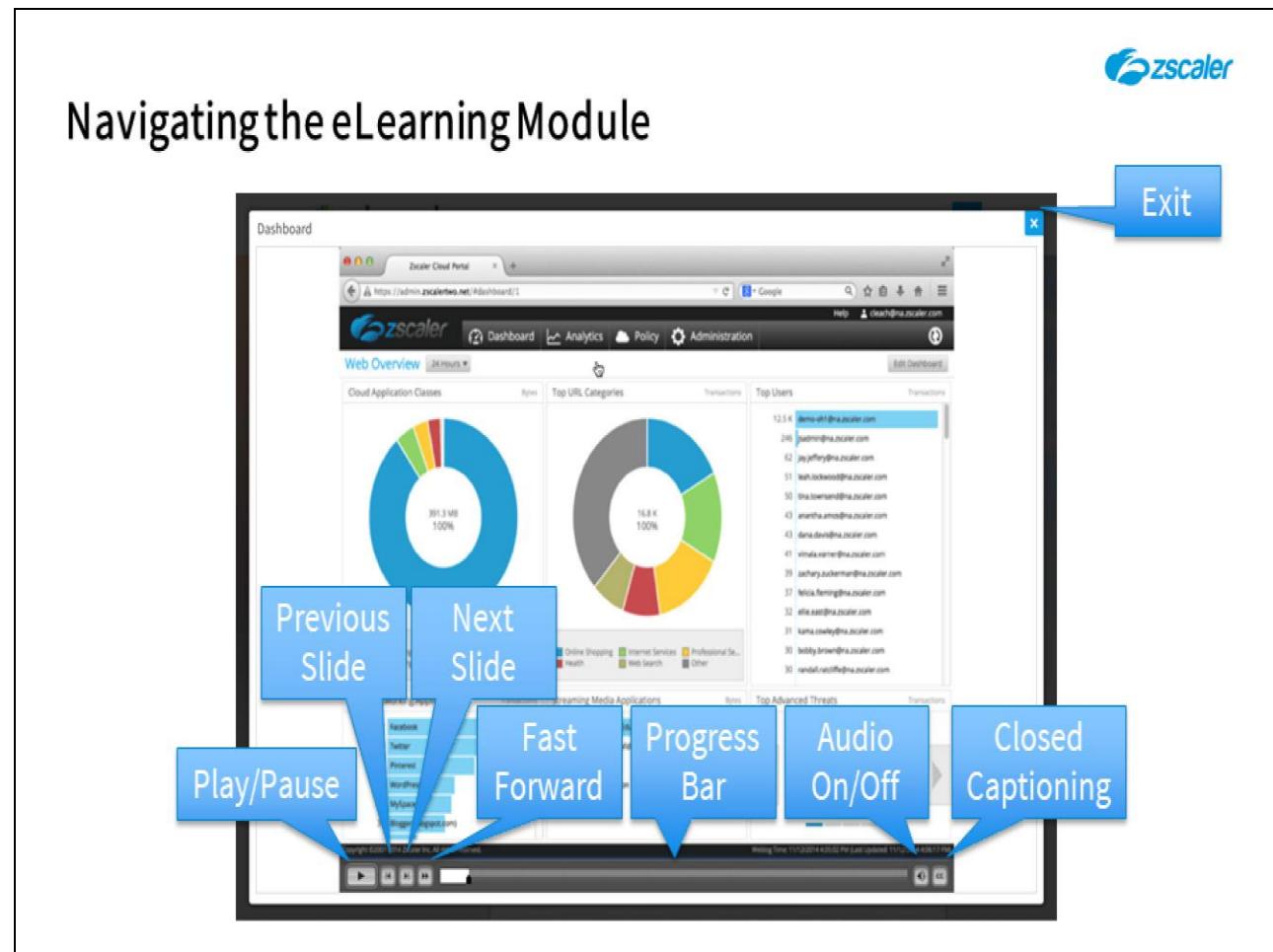
Security Assertion Markup Language (SAML)

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Hello and thank you for viewing this eLearning module on Zscaler user authentication with SAML.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and Next Slide, and Fast Forward. You can also mute the Audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the X button if you wish to exit.

**Slide 3 - Authentication with SAML
(Security Assertion Markup Language)**

Agenda



- SAML
 - User Provisioning
 - User Authentication
 - Transparent Desktop SSO
- Interactive Demo:
 - Configuring SAML
 - Enabling Authentication Exemption

Slide notes

In this module, we will look at SAML, user provisioning, user authentication, and Best Practices. An interactive demo showing the configuration process will follow the slides.

Slide 4 - Provisioning and Authentication Flow

Provisioning and Authentication Flow

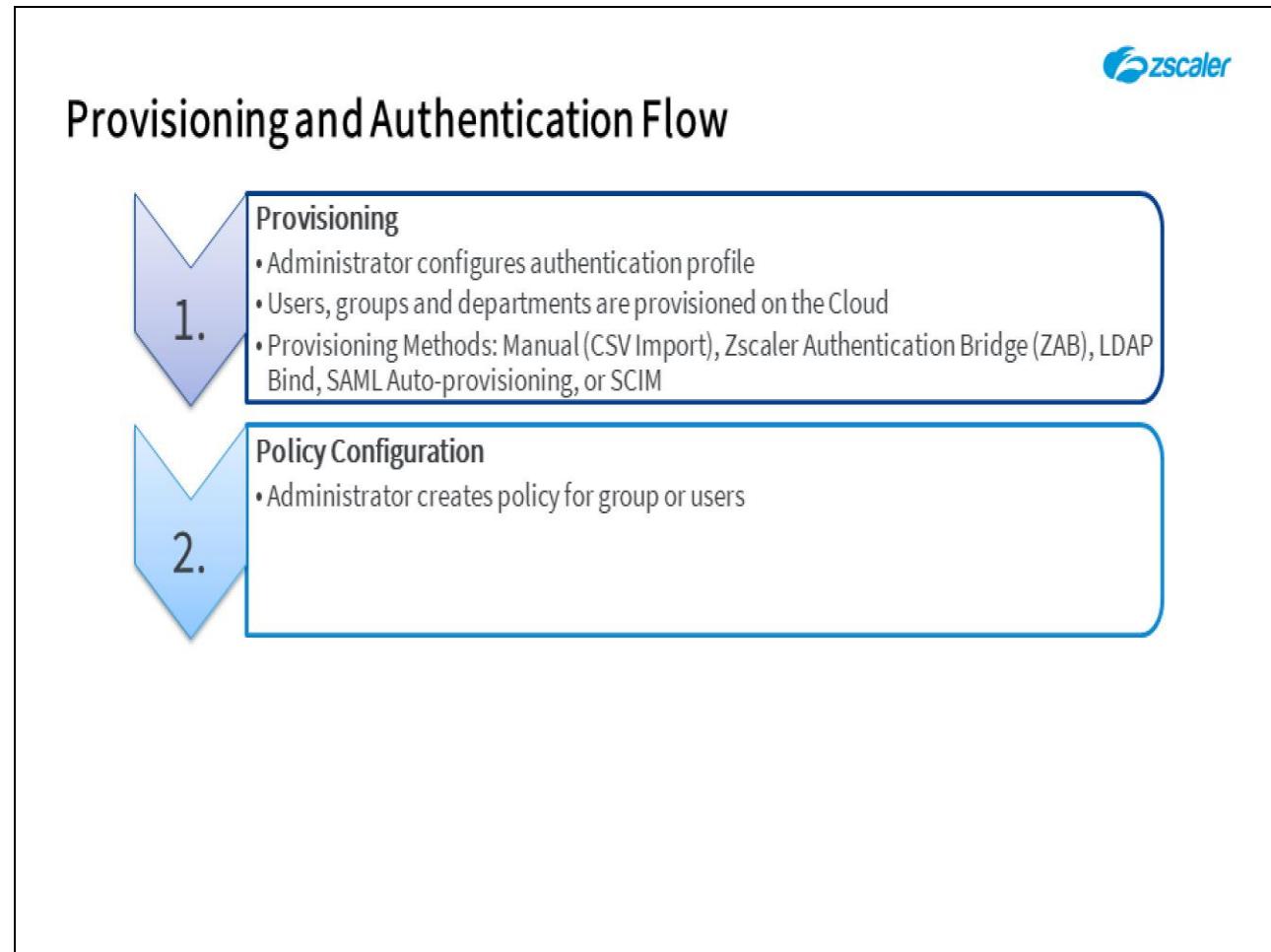
1.

Provisioning

- Administrator configures authentication profile
- Users, groups and departments are provisioned on the Cloud
- Provisioning Methods: Manual (CSV Import), Zscaler Authentication Bridge (ZAB), LDAP Bind, SAML Auto-provisioning, or SCIM

Slide notes

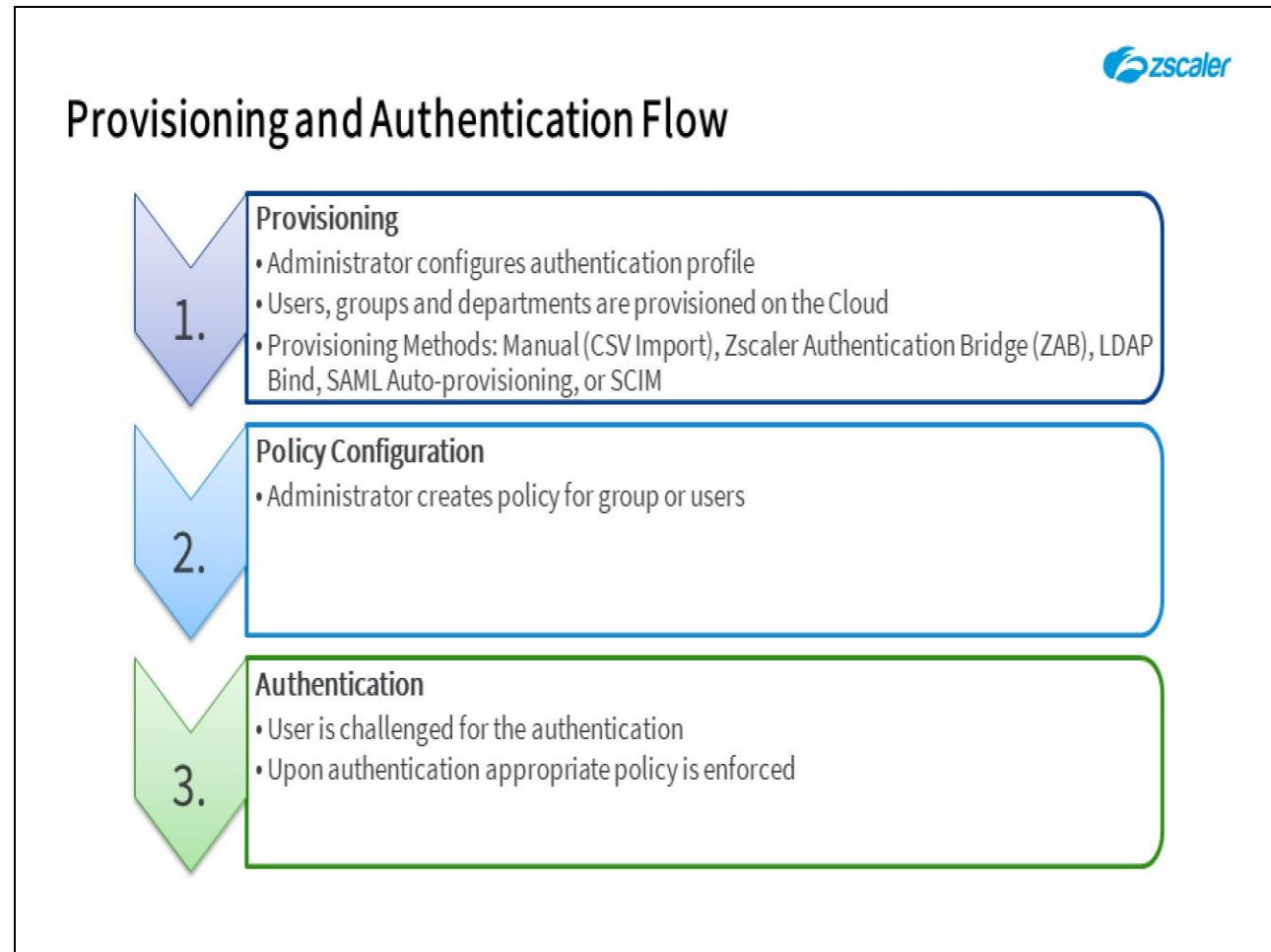
When using SAML for authentication it is important to understand that users must be provisioned in the Zscaler system and they are authenticated against the user database. How you populate the Zscaler database varies based on the authentication mechanism you employ for your organization. Provisioning methods include: Manual via the Admin Portal; CSV import; the Zscaler Authentication Bridge (ZAB), LDAP BIND; SAML auto-provisioning, or SCIM.

Slide 5 - Provisioning and Authentication Flow**Slide notes**

Once the user is created in the system the user should also be tied to a policy (covered in another module) or multiple policies, that determine levels of access. The user is also tied to a department for reporting.

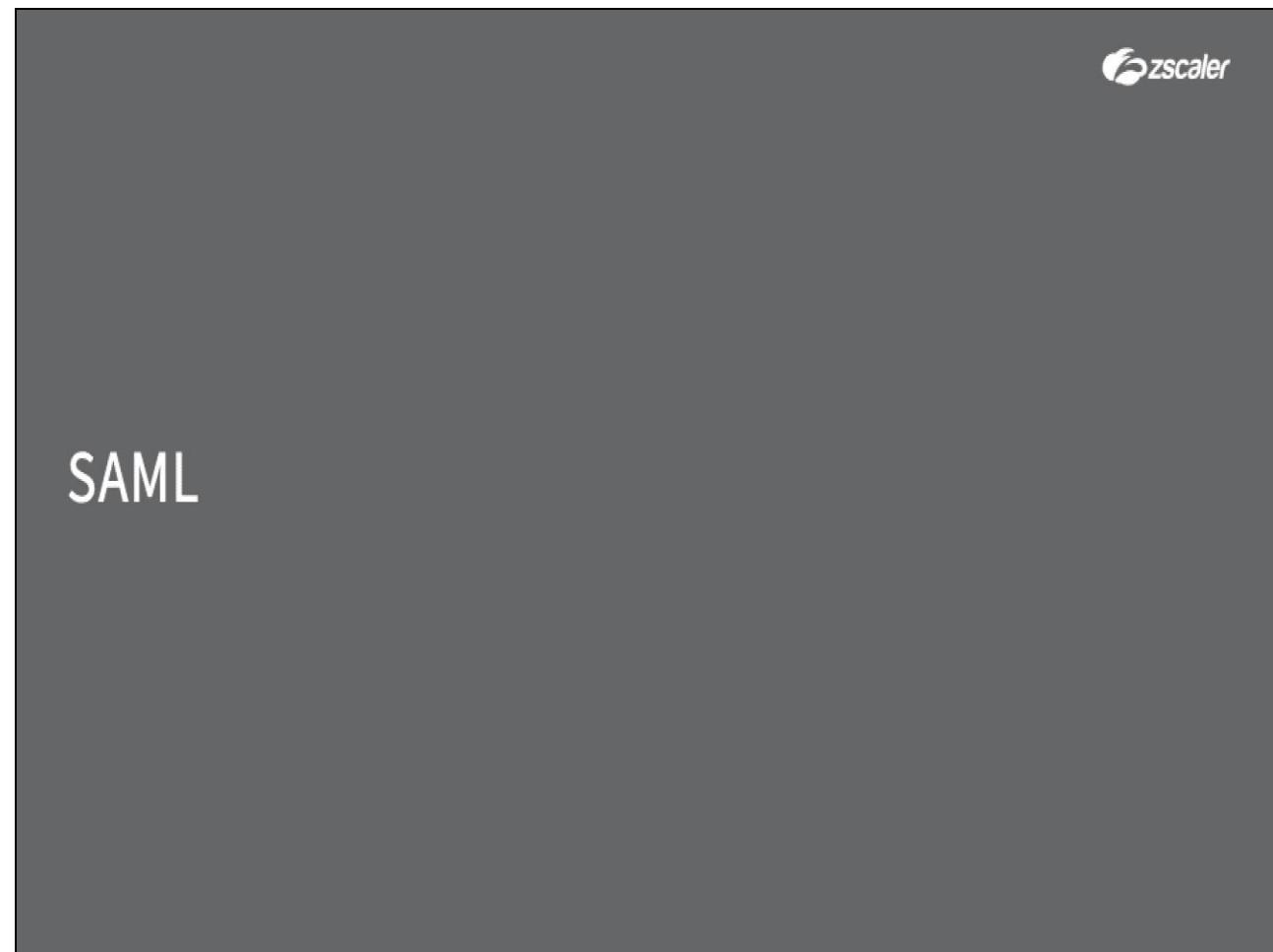
Once the user is created in the system the user should also be tied to a policy (covered in another module) or multiple policies, that determine levels of access. The user is also tied to a department for reporting.

Once the user is created in the system the user should also be tied to a policy (covered in another module) or multiple policies, that determine levels of access. The user is also tied to a department for reporting.

Slide 6 - Provisioning and Authentication Flow**Slide notes**

When the user is authenticated the system sees the policy that has been assigned to the user, either directly or via a group, which then determines access privileges.

Slide 7 - Provisioning Flow



Slide notes

Let's take a moment to discuss the components of SAML and supported providers.

Slide 8 - What is SAML

What is SAML



- Security Assertion Markup Language (SAML)
 - Federated Identification Standard for Web Authentication
 - Allows for ‘Single Sign-on’ (SSO) of users to services
- Components:

Identity Provider (IdP)	Service Provider (SP)	Security Assertions
<ul style="list-style-type: none">• Provides <i>Identifiers</i> and <i>Identity Assertions</i> for users that wish to access a service (IdP examples are: Okta, Ping, AD FS)	<ul style="list-style-type: none">• Also known as a <i>Relying party</i> (RP)• Employs the services of an IdP for the identification and authentication of users• Zscaler may act as an SP	<ul style="list-style-type: none">• Also known as Tokens• Issued to users by IdPs• Presented to SPs / RPs to confirm authentication• Trust based on PKI• Assertions may contain; Authentication, Attribute, or Authorization statements

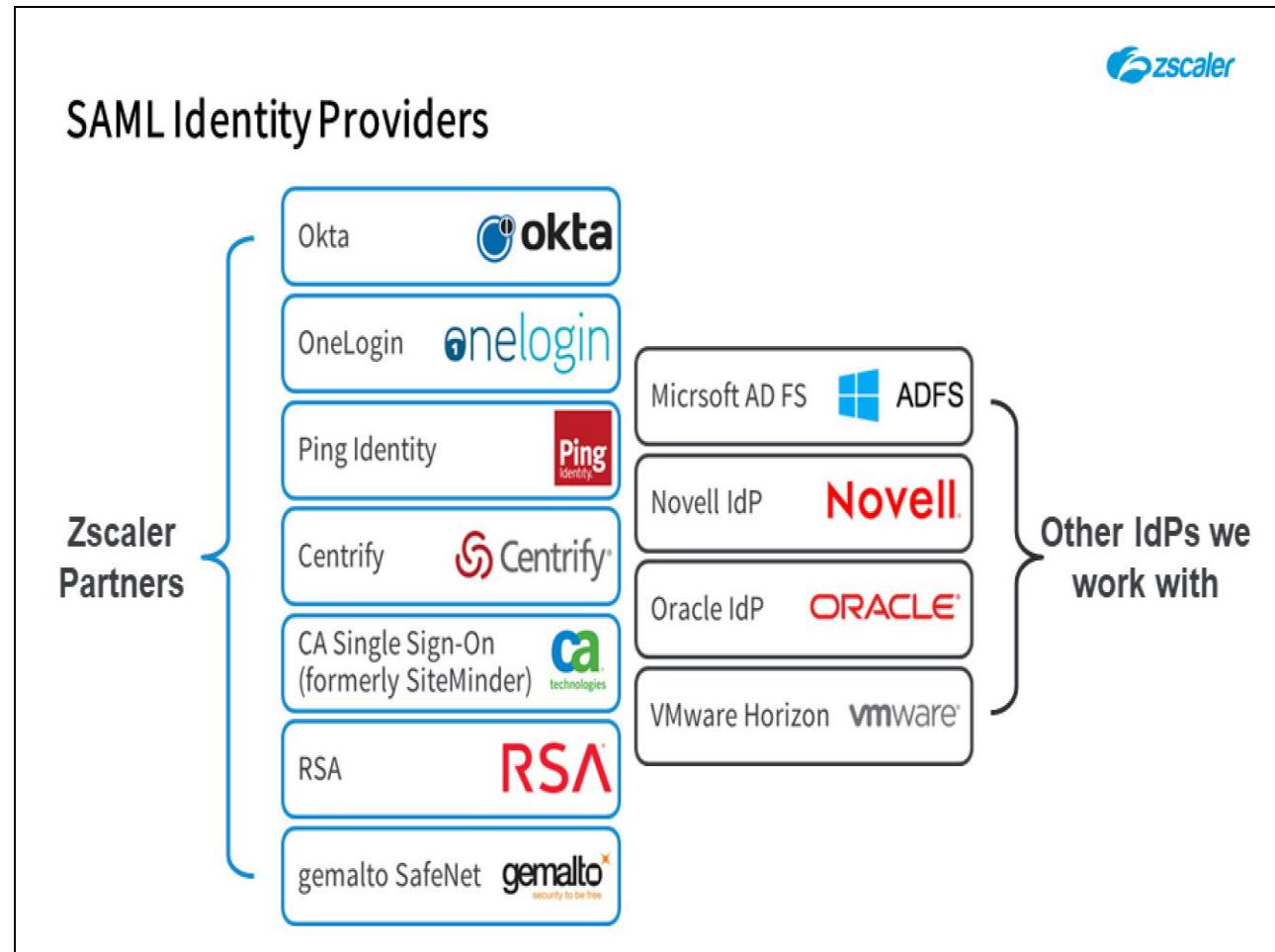
Slide notes

SAML, or Security Assertion Markup Language, is used to provide for single sign-on for users to multiple cloud applications. The user signs-in once and is then automatically signed in to other cloud applications the user subscribes to, such as Salesforce, or Box.

The basic components of a SAML installation are: The Identity Provider - this is the application that will handle the authentication requests and authenticate users into multiple applications. There are a number of SAML providers available such as Microsoft AD FS, Okta, etc.

...and the Service provider or application. These are your cloud applications. Zscaler counts as an application as well.

The Service provider or application - these are your cloud applications. Zscaler counts as an application as well.

Slide 9 - SAML Identity Providers**Slide notes**

SAML is a standards-based protocol, so Zscaler integrates with any compliant identity provider such as; Okta, OneLogin, PingOne, Microsoft AD FS, Novell IdP, Oracle IdP, VMware Horizon, and CA Single Sign-On (formerly known as SiteMinder).

Slide 10 - SAML IdP : In the Cloud or on premise?

SAML IdP : In the Cloud or on premise?

In The Cloud

- No servers to own or maintain
- Generally easier to implement
- Minimized downtime
- Generally, no inbound firewall rules required

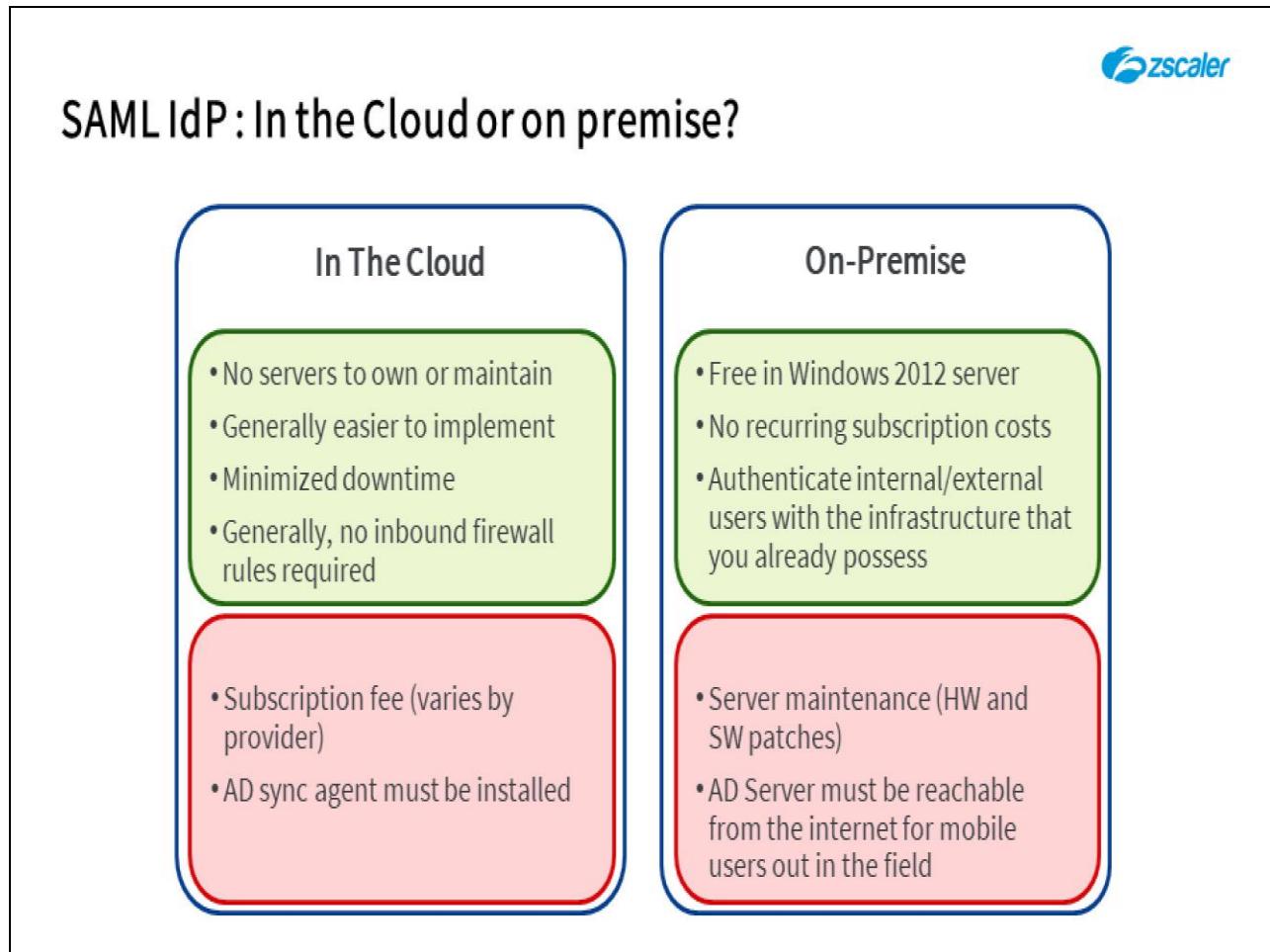
- Subscription fee (varies by provider)
- AD sync agent must be installed

Slide notes

As you have now seen you have multiple options when it comes to choosing your identity provider. One big choice you can make is whether to use a cloud-based identity provider or use an on-premise identity provider. Two popular options are Okta (in the cloud), or Microsoft AD FS. Let's first take a look at the Pros when it comes to using IdP in the cloud:

First, and most obvious, there are no servers to own or maintain; the cloud-based solution is generally easier to implement; there is minimized downtime as there is no hardware to be concerned with; and, generally, there are no inbound firewall rules to configure.

Some of the Cons for in the cloud IdP are: that there are subscription fees, and these vary by provider; and often times, an Active Directory sync agent must be installed on the Active Directory server.

Slide 11 - SAML IdP : In the Cloud or on premise?**Slide notes**

Next, let's take a look at on-premise solutions such as Microsoft AD FS. AD FS is free in Windows server and there are no recurring subscription costs. Some of the Cons of AD FS on-premise are: That there is server maintenance - both potential hardware and software patches; Active Directory must be reachable from the internet for mobile users out in the field which means that inbound firewall rules must be configured.

Slide 12 - Configuring SAML with Okta Summary

Configuring SAML with Okta Summary



1. Add the Zscaler service as an application and do the following.
 - o Adding the Zscaler service as an application includes defining its settings, choosing SAML 2.0 as the single sign-on option and assigning the service to users
2. Integrate Active Directory with Okta.
 - o Okta will verify the user credentials with your AD server
3. Import user information to Okta.
 - o Just as with Zscaler, user information must exist in the Okta user database
 - o The synchronization interval can be manual at any time or at specified intervals

**Slide notes**

Now that we have discussed the Pros and Cons of cloud based versus on-premise based solutions, let's take a quick look at the configuration steps for each solution. Let's begin with Okta. Okta can be configured with three simple steps: 1. First, add the Zscaler service as an application; 2. Next, integrate Active Directory with Okta; 3. And last, import user information into Okta's database.

Just as with Zscaler, user information must exist in the Okta user database. Note that user passwords are not imported. Also, the synchronization interval can be: Manual at any time; or at specified intervals.

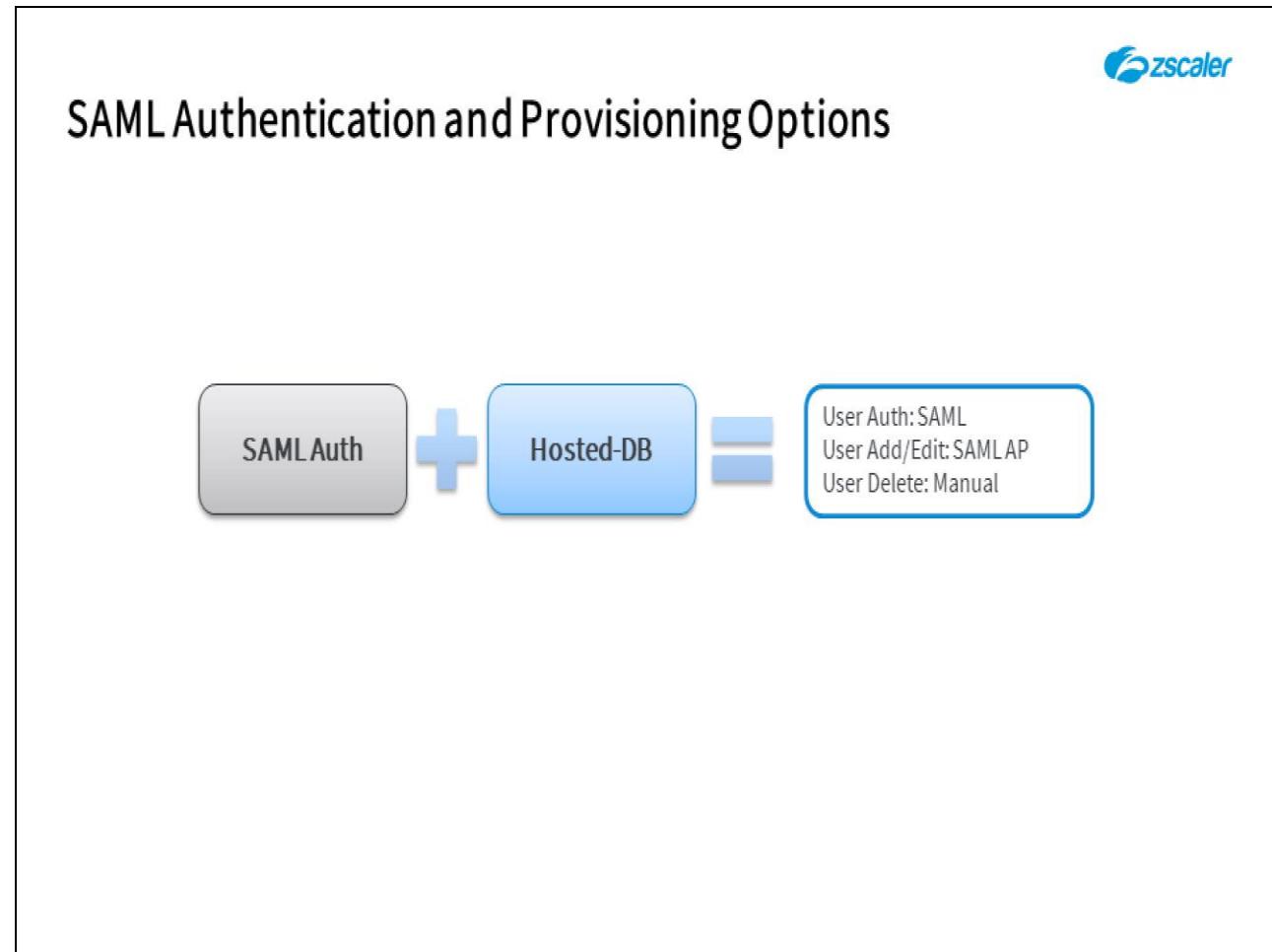
Slide 13 - Configuring SAML with AD FS Summary

Configuring SAML with AD FS Summary

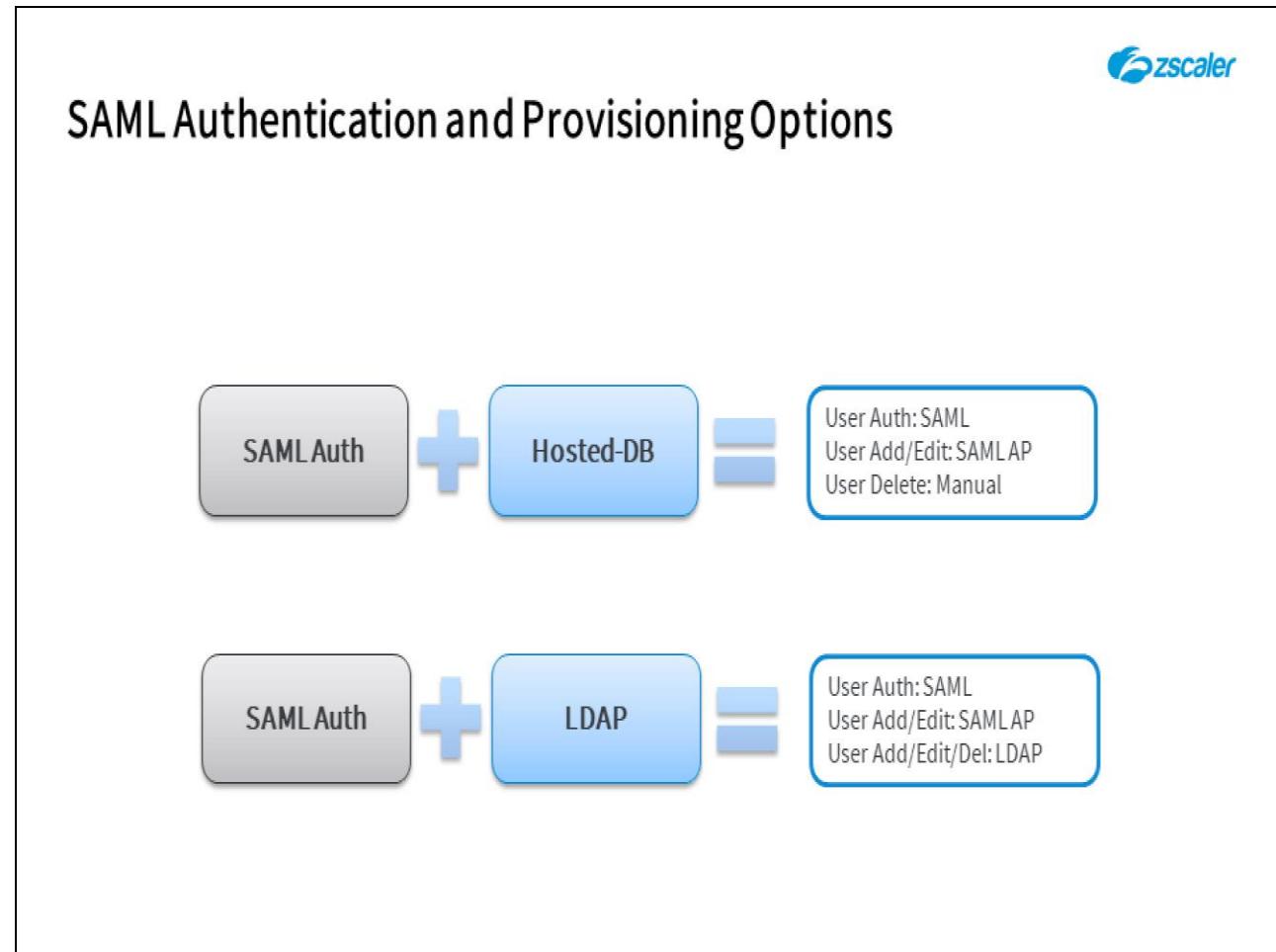
1. Add the Zscaler service as a relying party trust
 - o A 'Relying Party' is a Federation Service or application that requests and consumes claims
 - o Configure the Zscaler service as a Relying Party trust
2. Add the signature verification certificate from Zscaler
 - o In the SAML configuration on the ADFS server add the Zscaler signature verification certificate
3. Add a claims rule that provides information about a user.
 - o This is used by Zscaler to determine whether a user is allowed access
 - o Configure the SAML Assertions used (Group, Department, and full name parameters)
4. Export the certificate from ADFS and import to Zscaler
5. Optionally, restrict the groups that are federated
 - o AD FS 2.0 federates all the groups of a user, by default
 - o Restrict the groups to only those to which policies will be applied

Slide notes

Now let's take a look at configuring Microsoft AD FS from a high level: 1. First, add the Zscaler service as a relying party trust; 2. Next, add the signature verification certificate from Zscaler; 3. Next, add a claim rule, which is a statement that provides information about a user, it is used by the Zscaler service to determine whether a user is allowed access; 4. Export the certificate from AD FS into Zscaler; 5. And, optionally, restrict the groups that are federated.

Slide 14 - SAML Authentication and Provisioning Options**Slide notes**

There are two options for user provisioning and authentication. The first makes use of Zscaler's own internal User Database. This is typically NOT deployed in production unless the organization does not employ its own authentication scheme, such as Active Directory. The Internal, Hosted DB can also be useful in Proof of Concept testing.

Slide 15 - SAML Authentication and Provisioning Options**Slide notes**

The next, and most common method is the use of Active Directory or LDAP as the User database. The Identity provider will confirm the users Password in Active Directory and the password only exists in AD. This is the preferred method.

Slide 16 - Slide 16

SAML Advantages and Benefits

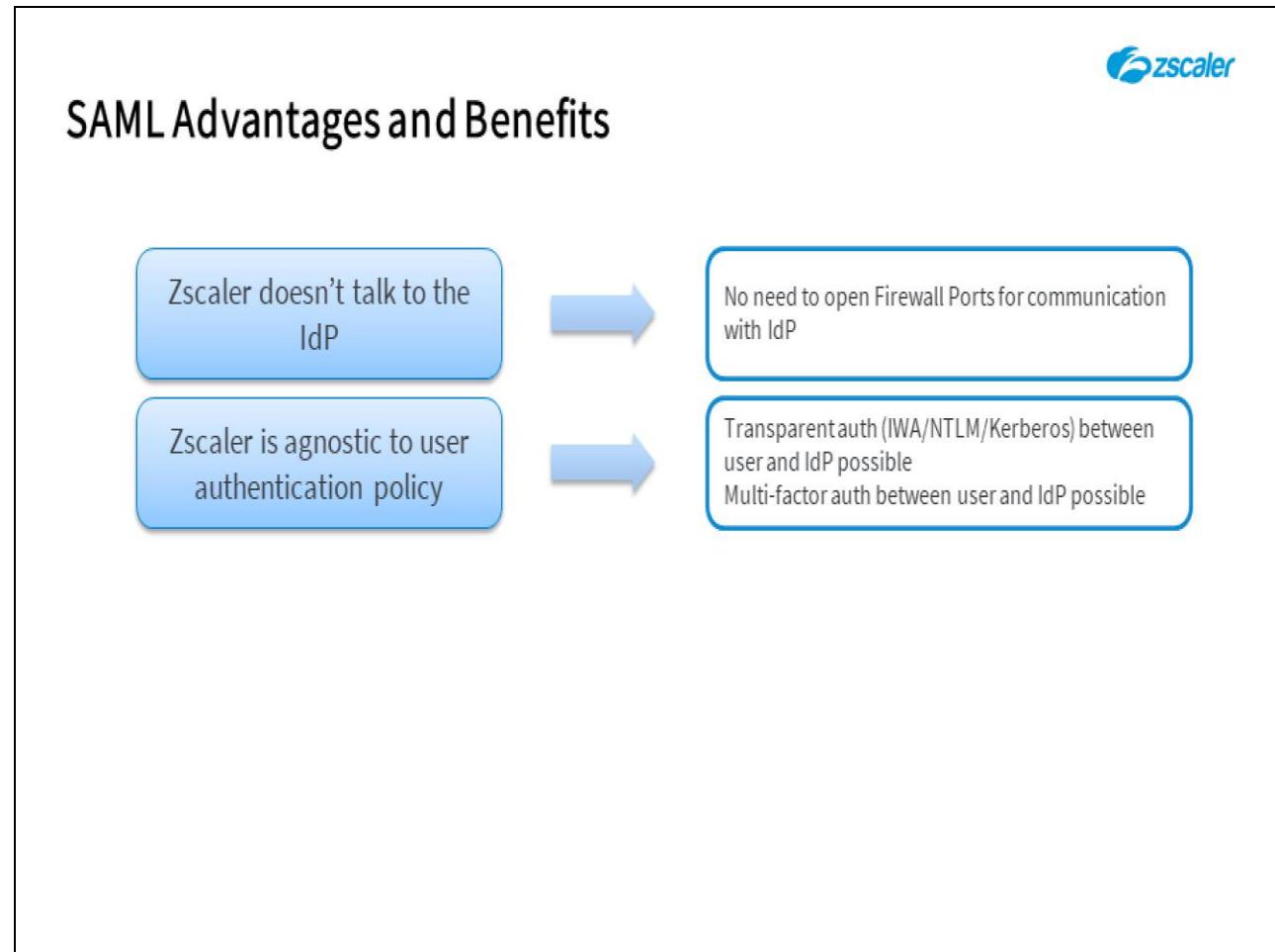
Zscaler doesn't talk to the IdP



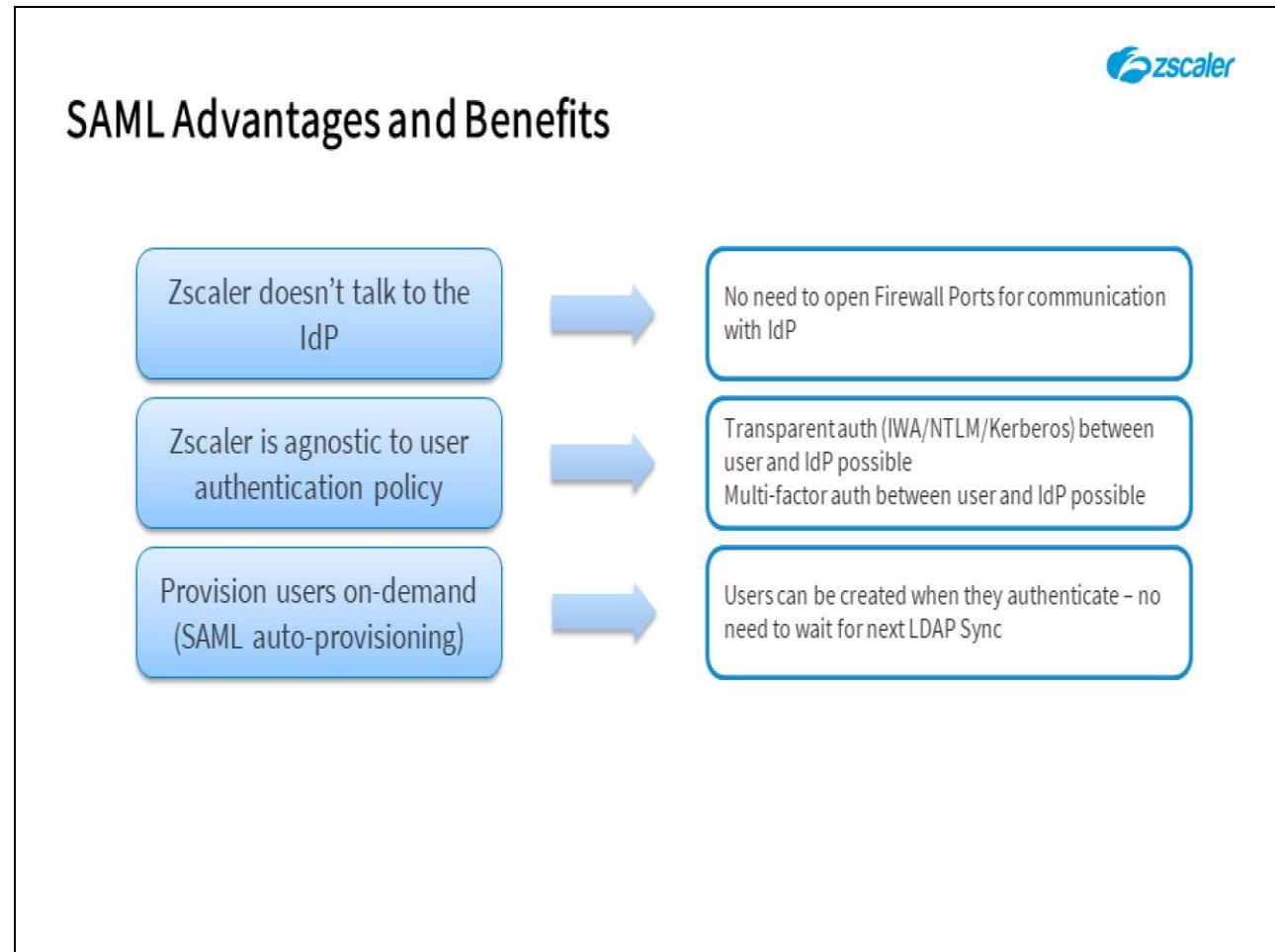
No need to open Firewall Ports for communication with IdP

Slide notes

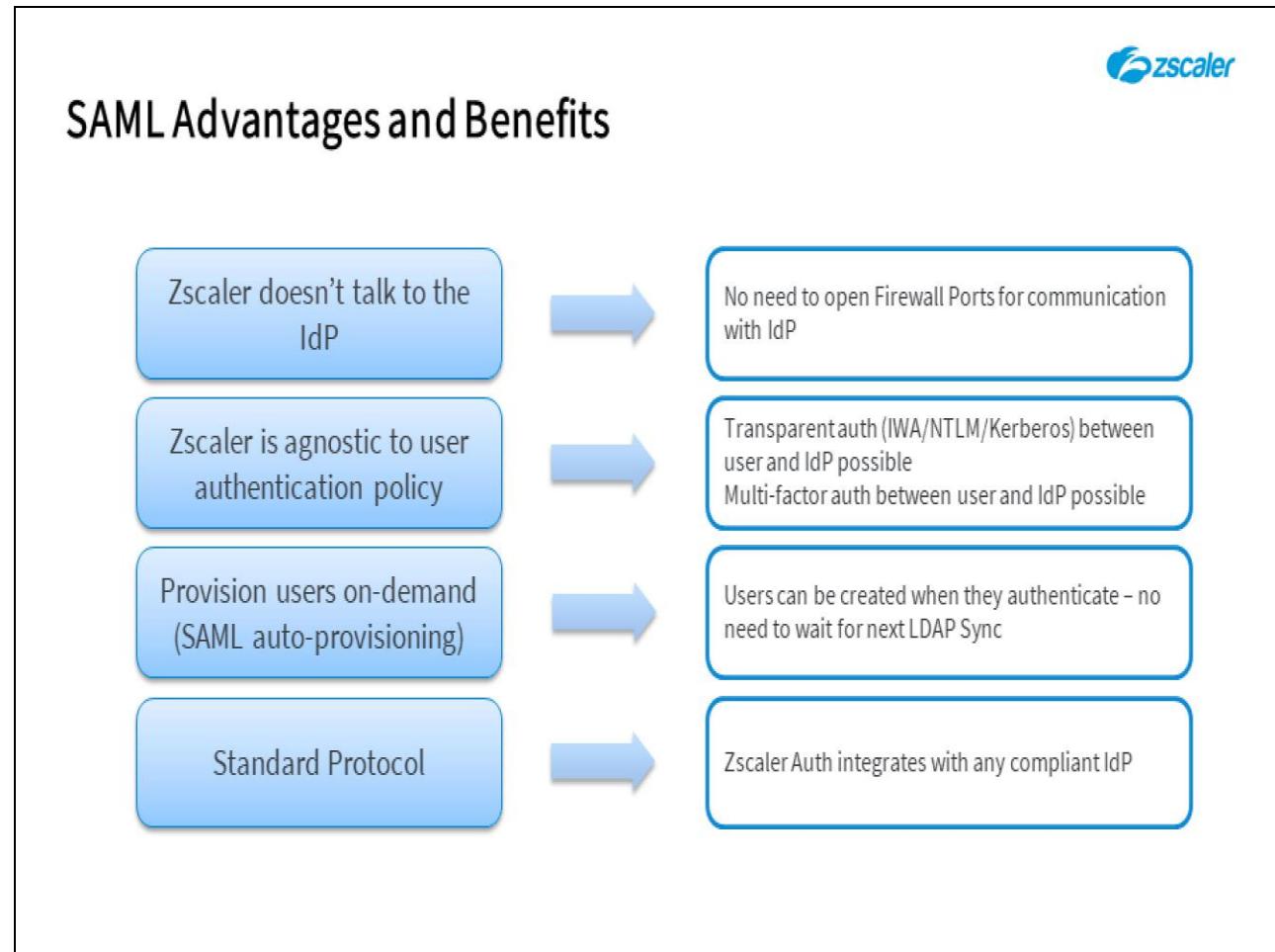
As you will see when we discuss the authentication flow, Zscaler does not communicate with either the IdP or Active Directory, so there is no need to open Firewall ports to Allow Zscaler to reach internal resources.

Slide 17 - SAML Advantages and Benefits**Slide notes**

SAML can provide for true Single-Sign On for end users in a Windows environment. Once the user authenticates to the PC desktop, he is automatically logged into the IdP in the background, which then authenticates him into his cloud applications.

Slide 18 - SAML Advantages and Benefits**Slide notes**

SAML Auto-provisioning is a feature that automatically adds new user's information (name, group membership, etc.) into Zscaler's database when the user is first seen making an authentication request, thus saving the administrator time.

Slide 19 - SAML Advantages and Benefits**Slide notes**

And SAML is a standards-based protocol, so Zscaler integrates with any compliant IdP.

Slide 20 - User Provisioning

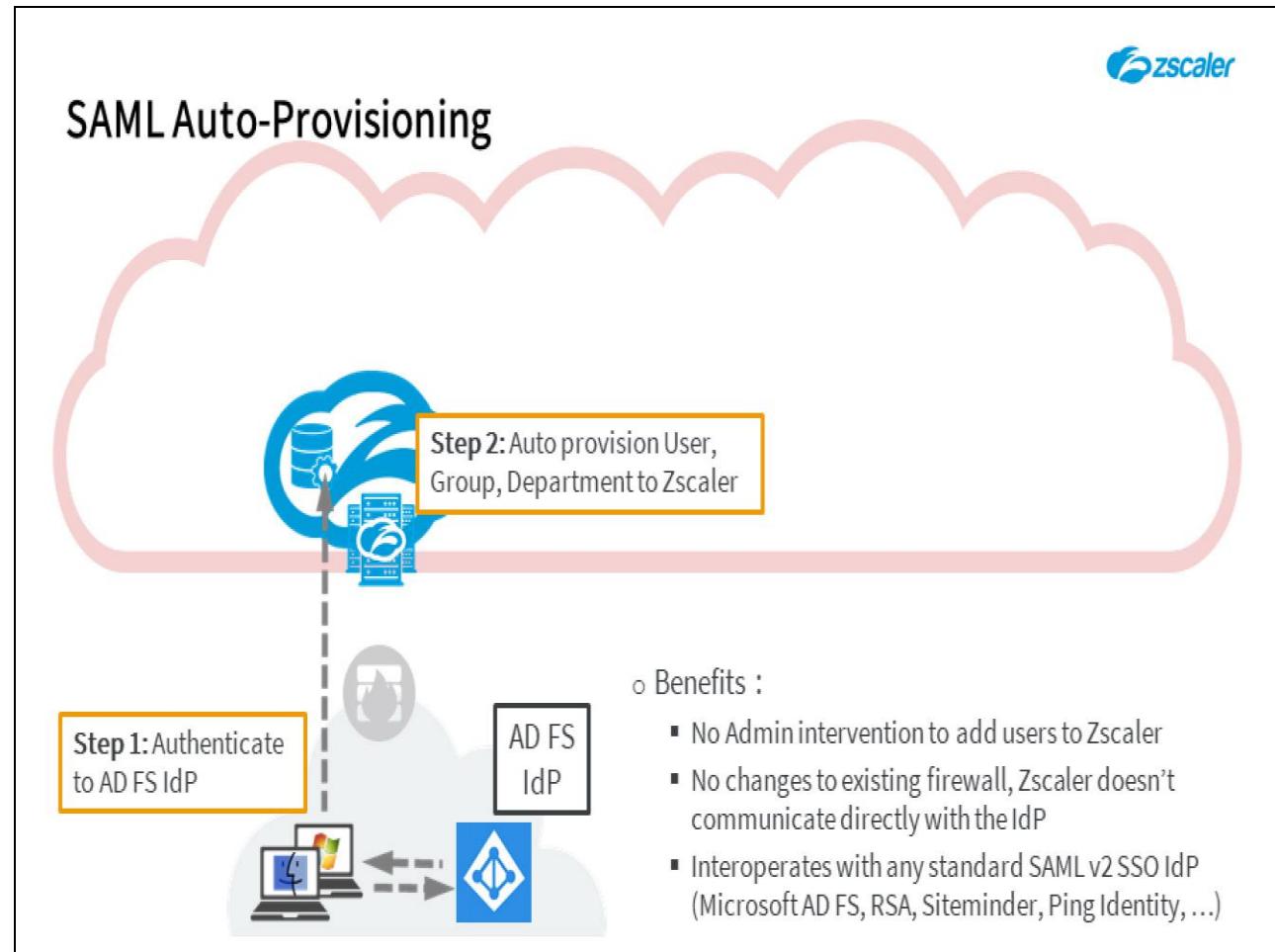
User Provisioning



Slide notes

Now let's take a look at the process of user provisioning into the Zscaler system.

Slide 21 - SAML Auto-Provisioning



Slide notes

Best practices when using SAML is to take advantage of SAML Auto-Provisioning. While not part of the standard most solutions provide for this function.

Slide 22 - SAML Auto-Provisioning

SAML with Auto-Provisioning

- Small evolution or extension from pure SAML authentication
 - Trust the Identity Provider not just for Authentication, but also for user provisioning

Creating Users on the Fly

- If user in the SAML response is unknown to Zscaler, create the user
- Authorization attributes: display name, group, department
- Configure the SAML attributes
 - If present, user will be associated with the attributes
 - Groups/departments will be created automatically if not already present

Slide notes

When a user tries to authenticate, Zscaler sees the username and group membership as part of the authentication request. If this user is not already in the Zscaler database, the information will automatically be imported. As mentioned previously, the password is never seen by Zscaler and is not imported - only the username and group membership.

The user information is checked each time the user logs in so any changes in group membership in Active Directory are reflected in the Zscaler database, such that the user receives the appropriate level of access as determined by the policy and group membership.

Slide 23 - SAML Auto-Provisioning

SAML with Auto-Provisioning



- Small evolution or extension from pure SAML authentication
 - Trust the Identity Provider not just for Authentication, but also for user provisioning

Creating Users on the Fly

- If user in the SAML response is unknown to Zscaler, create the user
- Authorization attributes: display name, group, department
- Configure the SAML attributes
 - If present, user will be associated with the attributes
 - Groups/departments will be created automatically if not already present

User Updates

- User information is checked at every login for modifications
- Modifications are immediately applied
- Force a user re-authentication to update authorization attributes

Slide notes

If the authentication interval in Zscaler, however, is long or is only required once, the change in group membership will not take place until the authentication interval expires and the user has to re-authenticate. In the case where the authentication interval is set to **Only Once**, then the administrator must manually log the user out of the system in the Zscaler Admin Portal, or the cookie must be deleted on the device, which will force the user to re-authenticate.

Slide 24 - What is SCIM?

What is SCIM?

SCIM

- System for Cross-domain Identity Management (SCIM)
 - Standard for automating the exchange of user identity information between identity domains
 - Automatic API driven updates to user attributes on a change in the home directory, e.g. automatic update to group memberships, or automatic user removal (to deny service)

SCIM Benefits	REST API - Operations
<ul style="list-style-type: none">• Same benefits as Auto-Provisioning plus....• SCIM communicates a users group / department membership change to Zscaler via the API. Zscaler automatically changes the membership information so the correct policies are applied in real time - no IT intervention.	<ul style="list-style-type: none">• Create: Add a resource (e.g. user, group)• Read: Get information about a resource• Replace: Change a resource• Delete: Remove a resource• Update: Update the attributes of a resource• Search: Find a resource• Bulk: Operations on multiple resources

Slide notes

Another, and newer method for user provisioning, is SCIM or System for Cross-Domain Identity Management. SCIM is a standard for automating the exchange of identity information between identity domains. Information is exchanged with Zscaler using Zscaler's API for the purpose of adding, updating, or deleting users from the Zscaler database. The main benefit of SCIM is that information is updated automatically via the API where Auto-Provisioning requires that the user first log out then log back in for changes to be detected by Zscaler. Additionally, where Auto Provisioning can add user information it cannot delete users from the database where SCIM can.

Slide 25 - How does it work?

How does it work?

- IdP (ex. Okta) makes REST API calls to Zscaler SCIM server (<https://scim.zscaler.net>)
- Simple configuration
 - Few clicks on Zscaler Admin UI
 - Updated, published apps on Azure AD and Okta
- Full CRUD operation (create user, update, delete) supported
 - Create Users or user attributes
 - Update user attributes (groups, departments etc.)
 - Delete and de-provision users

Slide notes

As mentioned on the previous slide, SCIM communicates directly between the IdP and Zscaler via the API. When the IdP receives an update about a user, whether this is a new user to be added to or deleted from the user database, or there is a change in group or department membership this information is automatically communicated to Zscaler without any user or IT intervention. Note that the time it takes for the IdP to communicate changes varies from IdP to IdP as they may batch updates and send them periodically or they may send them immediately as the IdP receives them. Be sure to check your IdP documentation.

As you will see during the interactive demo enabling SCIM on the Zscaler side is done with the click of one button then, depending on your IdP, you may only need to provide the IdP the "Bearer Token" which is, essentially, the password that allows the IdP to communicate with the Zscaler API. Some IdP's also need the "Base URL" as part of the configuration. Be sure to check your IdP documentation for their requirements. For example, Okta only needs the Bearer Token as it already knows the Base URL for your organization based on other parts of the configuration where Azure requires that you copy the Base URL from Zscaler and provide it during the Azure config.

Last, a big advantage that SCIM has over Auto-Provisioning is the ability to not only create a new user in the Zscaler database but also modify it without any intervention and delete it as well. Auto-Provisioning can only create a new user at initial login and can only detect modifications if the user logs out and logs back in.

Slide 26 - SCIM or Auto-Provisioning?

SCIM or Auto-Provisioning?

- In determining which provisioning method to use in your environment consider the following:

SCIM	Auto-Provisioning
<ul style="list-style-type: none">• Not supported by all IdP's with Zscaler	<ul style="list-style-type: none">• Supported by all IdP's

Slide notes

When determining whether to use SCIM or Auto-Provisioning consider the following: SCIM is not supported by all IdP's with Zscaler. Be sure to check your IdP documentation. SAML Auto-Provisioning is supported with all IdP's.

Slide 27 - SCIM or Auto-Provisioning?

SCIM or Auto-Provisioning?

- In determining which provisioning method to use in your environment consider the following:

SCIM	Auto-Provisioning
<ul style="list-style-type: none">• Not supported by all IdP's with Zscaler• Automatically adds user / group information to Zscaler DB via API	<ul style="list-style-type: none">• Supported by all IdP's• Automatically adds user / group information to Zscaler DB at initial user authentication

Slide notes

SCIM automatically adds a user and group information to the Zscaler database via the API where Auto-Provisioning adds the user and group information based on the user successfully authenticating.

Slide 28 - SCIM or Auto-Provisioning?

SCIM or Auto-Provisioning?



- In determining which provisioning method to use in your environment consider the following:

SCIM	Auto-Provisioning
<ul style="list-style-type: none">• Not supported by all IdP's with Zscaler• Automatically adds user / group information to Zscaler DB via API• Change in group membership is automatically announced to Zscaler via the API	<ul style="list-style-type: none">• Supported by all IdP's• Automatically adds user / group information to Zscaler DB at initial user authentication• Change in group membership is not automatically announced – the user must log out then log back in

Slide notes

With SCIM changes in group membership are automatically announced to Zscaler via the API where with Auto-Provisioning changes are not automatically propagated and the user must log out then log back in for the change to be detected then updated in the Zscaler database.

Slide 29 - SCIM or Auto-Provisioning?

SCIM or Auto-Provisioning?



- In determining which provisioning method to use in your environment consider the following:

SCIM	Auto-Provisioning
<ul style="list-style-type: none">• Not supported by all IdP's with Zscaler• Automatically adds user / group information to Zscaler DB via API• Change in group membership is automatically announced to Zscaler via the API• Can automatically delete users out of the Zscaler User DB if deleted out of AD / directory store	<ul style="list-style-type: none">• Supported by all IdP's• Automatically adds user / group information to Zscaler DB at initial user authentication• Change in group membership is not automatically announced – the user must log out then log back in• Cannot automatically delete users

Slide notes

And last, SCIM can automatically delete users out of the Zscaler database if the user is deleted out of your directory store where Auto-Provisioning cannot.

Slide 30 - User Authentication

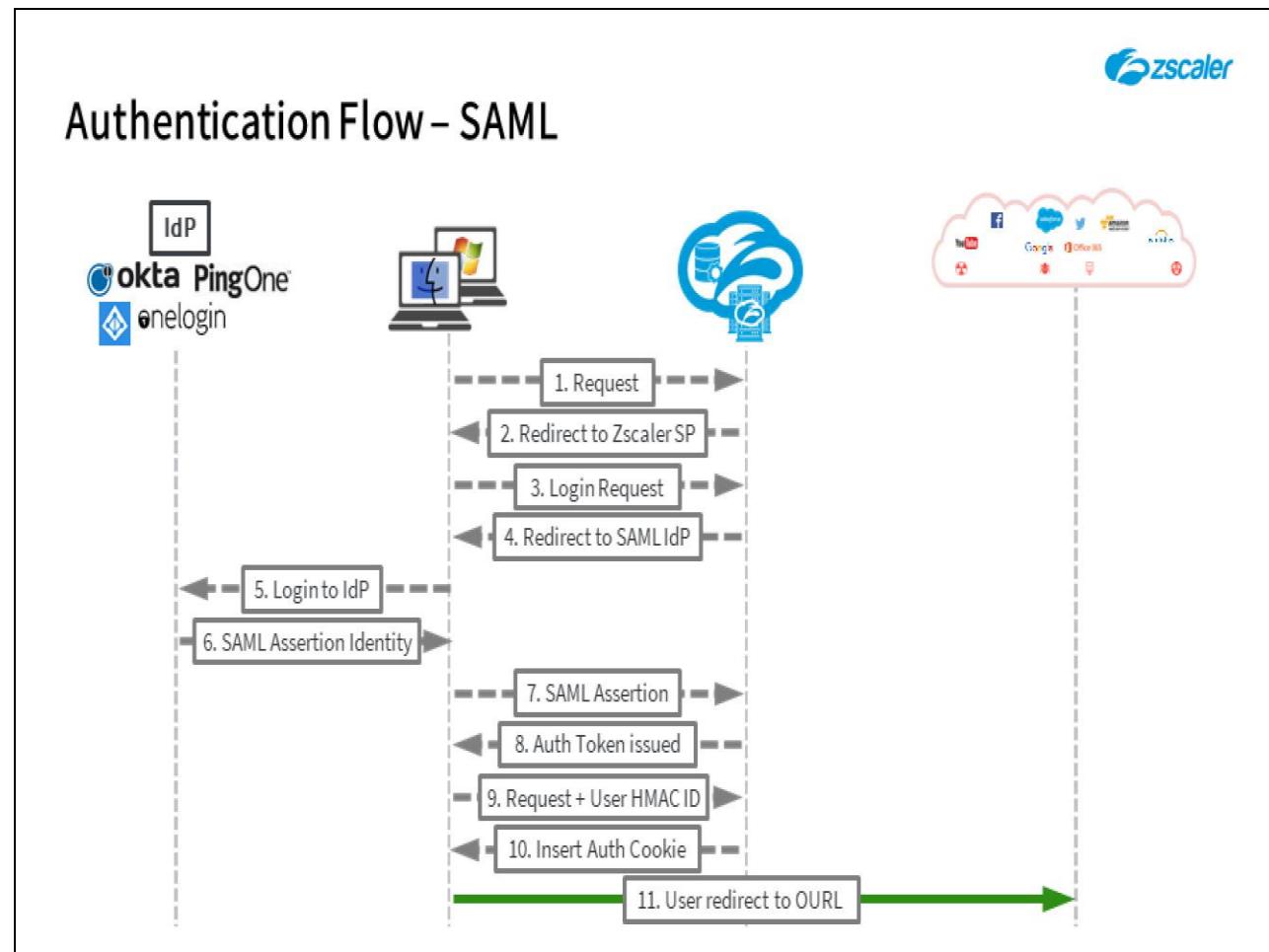
User Authentication



Slide notes

Now let's take a look at the authentication process when using SAML.

Slide 31 - Slide 31



Slide notes

Let's take a high-level look at the authentication process:

1. First, an unauthenticated user initiates a request for a web site to the Zscaler Enforcement Node (or ZEN);
2. Next, the unauthenticated user is redirected by the ZEN to the Zscaler Central Authority (or CA) to check the user name;
3. Next, the user sends the username to the CA;
3. Next, the user sends the username to the CA
4. And is redirected to the iDP
5. The user submits the username and password to the IDP and the IDP verifies the password with Active Directory.
7. The user device sends the SAML assertion to Zscaler;
8. Zscaler sends and authentication token to the user;
9. The user sends an authentication request with the HMAC ID;
10. The ZEN retrieves the user's policies which determine access privileges.
11. And last, the ZEN sends an authentication cookie to the user device, then the user is redirected back to its original destination request.

Slide 32 - Slide 32

Transparent Desktop SSO



Slide notes

Let's take a moment to discuss the components of SAML and supported providers.

Slide 33 - SAML Authentication Flow

Transparent/Desktop SSO

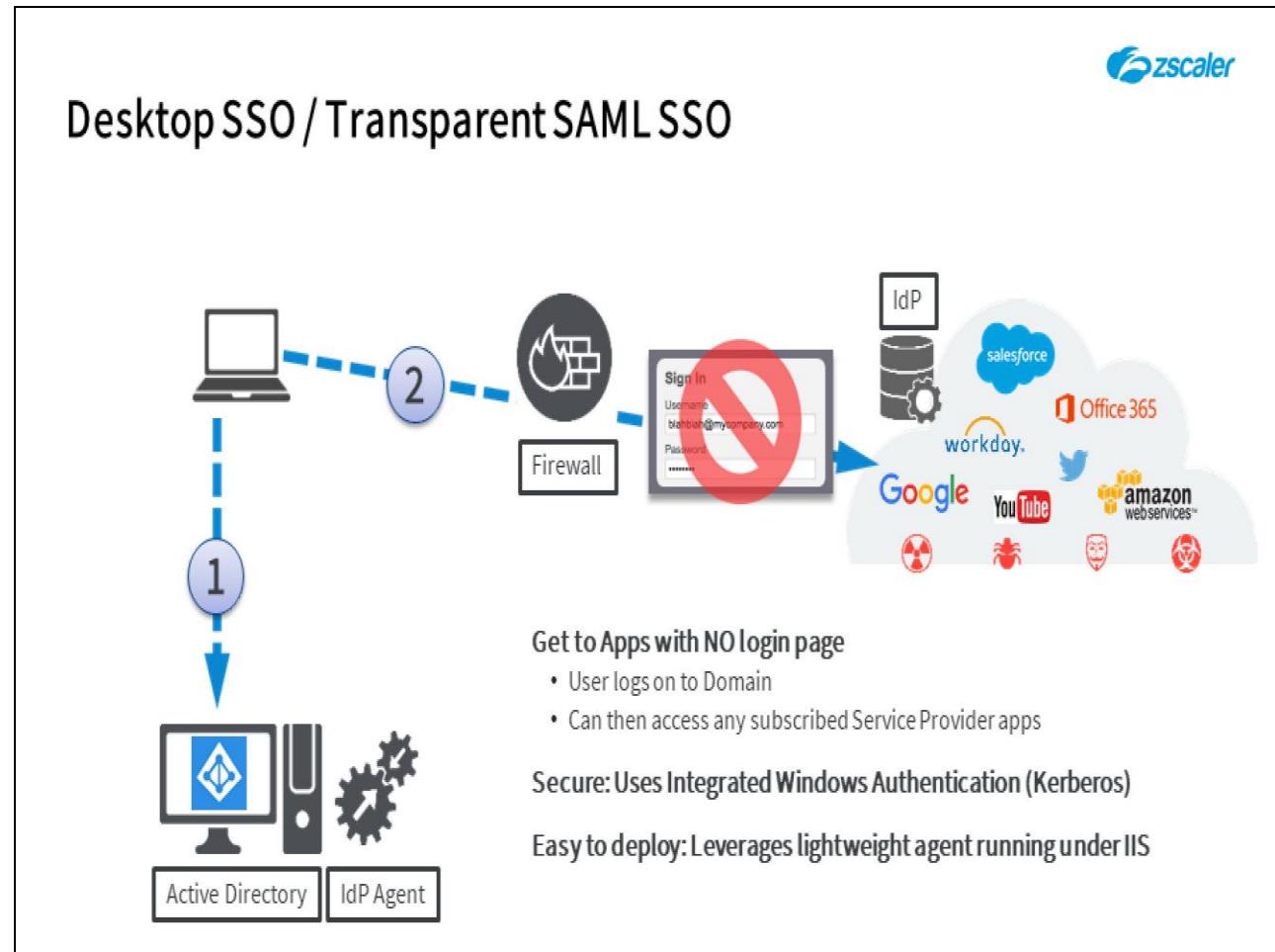


- Transparent / Desktop SSO provides authentication to all configured apps automatically once the user signs into their PC
- Configuring Transparent / Desktop SSO varies by IdP
 - Some may require an additional software agent to be installed on the AD Server along with additional browser configuration (Okta)
- In the eLearning demo and the ZCCP Hands-on Lab we deliberately do not configure or demonstrate Desktop SSO so you can see the redirection process occur

Slide notes

Transparent, or desktop single sign-on, provides authentication to all configured applications for a user automatically once the user signs into their PC. Configuring transparent, or desktop SSO, varies by identity provider, some may require an additional software agent be installed on the Active Directory server along with browser configurations, such as the case with Okta. In this eLearning demo and in the ZCCP-IA Hands-on Lab, we do not configure or demonstrate Desktop SSO so you can see the redirection process occur.

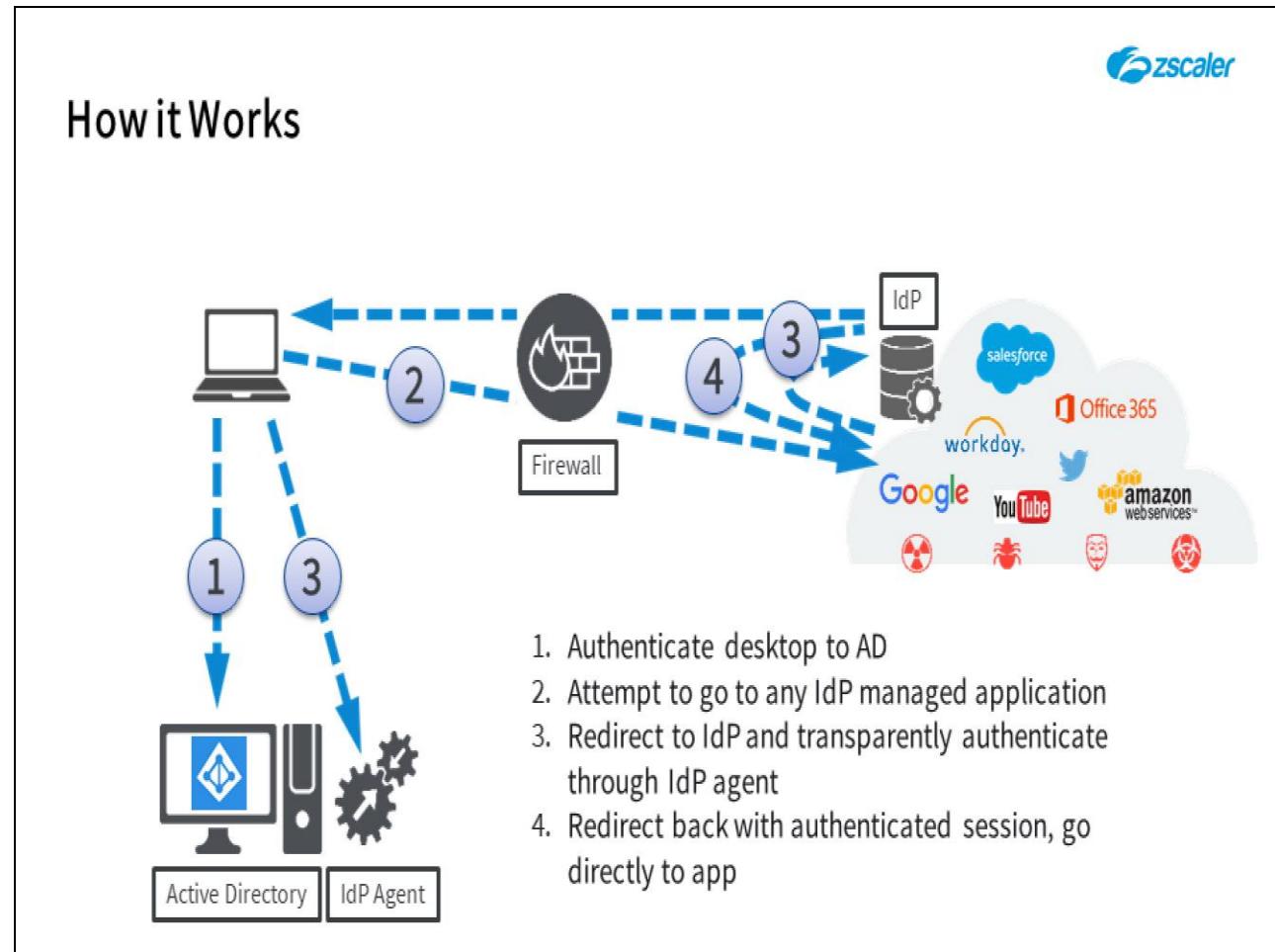
Slide 34 - Desktop SSO / Transparent SAML SSO



Slide notes

Desktop single sign-on is an option with Okta and other providers that streamlines the login process for users. With Desktop SSO, the user simply signs into their PC and they are then automatically logged into their applications. For information on the Desktop SSO option please see your Okta documentation.

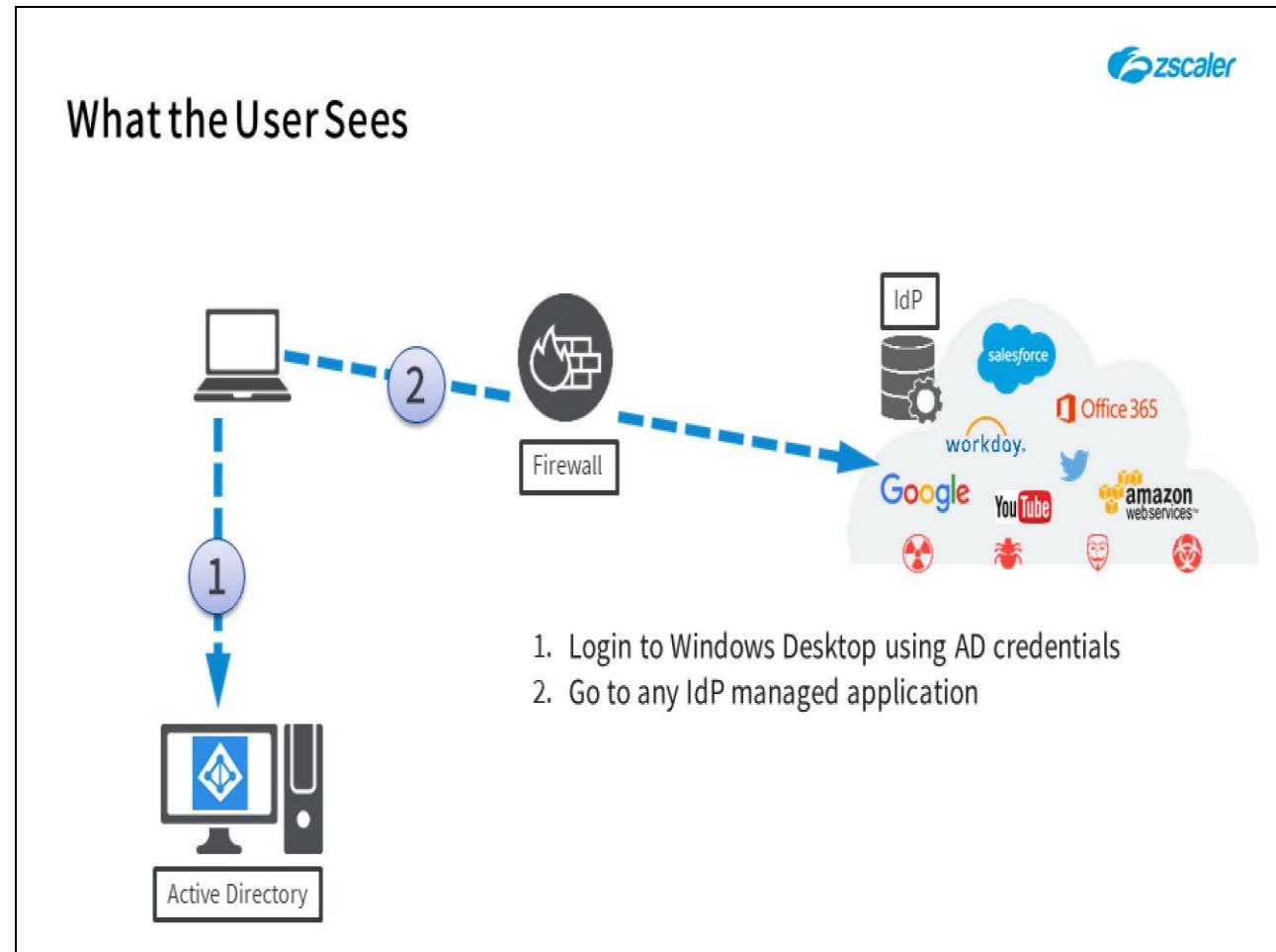
Slide 35 - How it Works



Slide notes

Let's take a quick look at how Desktop SSO works: 1. First, the user authenticates to the desktop and their Domain; 2. Next, they browse to any IdP managed application; 3. They are redirected to the IdP agent in the background and transparently authenticate; 4. Then they are redirected back with an authenticated session and go directly to their application without an additional login.

Slide 36 - What the User Sees



Slide notes

And this is what the end-user sees: 1. Again, first the user logs into their windows desktop using Active Directory credentials; 2. Then they continue on in their browser to any IdP managed application and no additional sign-in is required.

Slide 37 - SAML Authentication Options

Configuring SAML with Okta

**Slide notes**

Let's take a look at configuring a SAML solution. During this interactive demo you will participate in configuring a sample Okta account as well as enabling SAML in Zscaler.

Slide 38 - SAML Advantages and Benefits

Assumptions and tasks



- Assumptions

- This demo focuses on configuration of SAML in Zscaler only. Okta is used as the IdP; however, the Okta configuration is not shown.
- That you already have Active Directory installed and configured and users created
- You already have an Okta account (demo or paid) and have access to it from the web

- Tasks

1. Configure Zscaler for SAML
2. Show where to find your Zscaler Organization ID and Bearer Token
3. Configure Authentication Exemptions for IdP traffic
4. Enable authentication on a per-location basis.

Slide notes

For the purpose of this demonstration as well as your own production deployments the following assumptions are made: This demonstration shows how to enable SAML using Okta as the Identity Provider, should you choose to use one of the other IdPs their configuration steps will vary; you already have Active Directory installed and configured and your users already exist in AD; last, it is assumed that in your own production environment that you have obtained an Okta account, either the free demo account for testing or the full version, and have access to it from the web.

Tasks that will be demonstrated are: Configuring Zscaler to use SAML and show where to find your Zscaler Organization ID and Bearer Token for use in your IdP configuration, configuring Authentication Exemptions for IdP traffic, and enabling authentication on a per-location basis.

Slide 39 - Configuring SAML in Zscaler

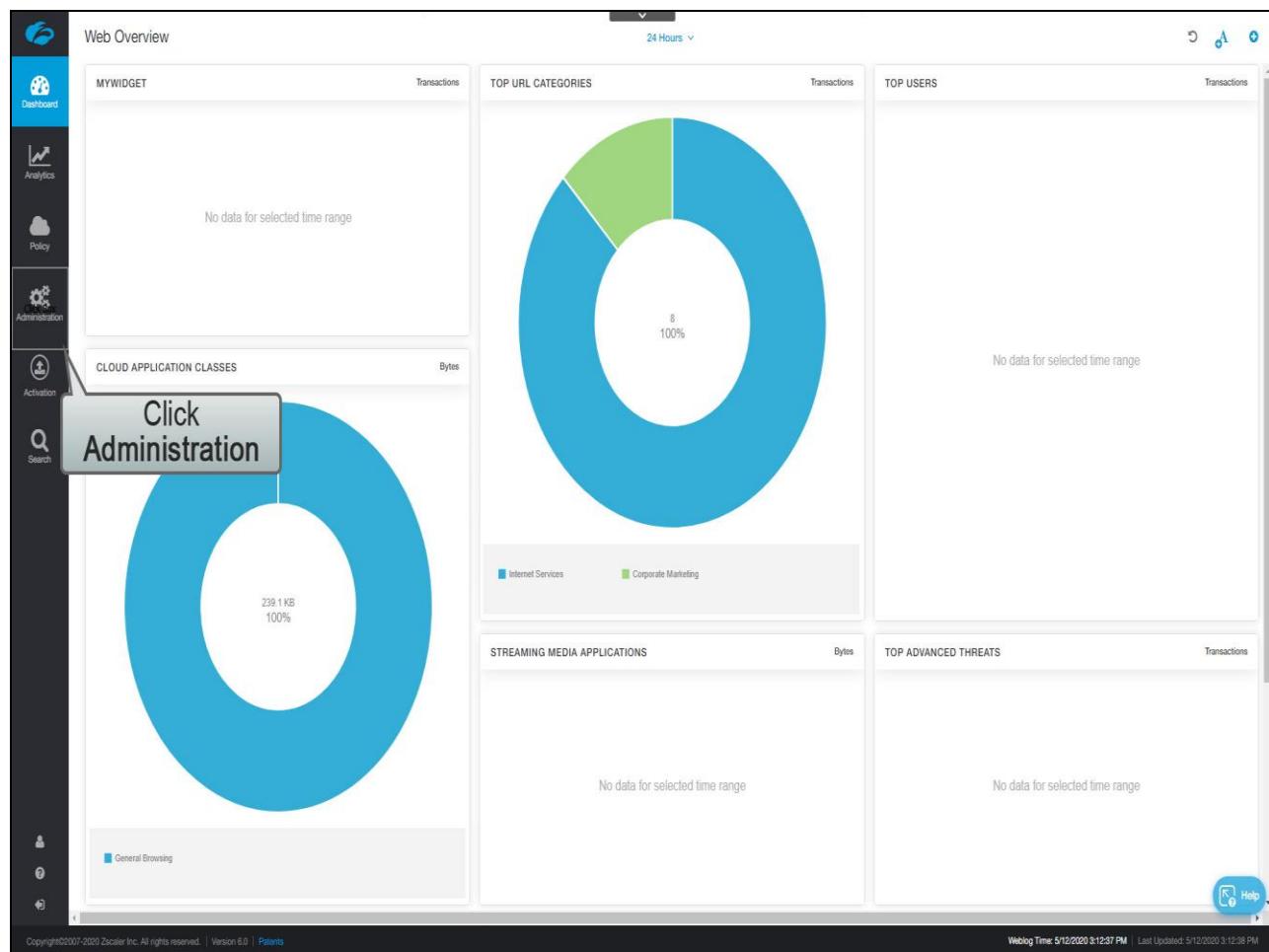


Demonstration: Configuring SAML in Zscaler

Slide notes

Now that we have configured Okta let's move into the Zscaler Admin Portal to finish the SAML configuration.

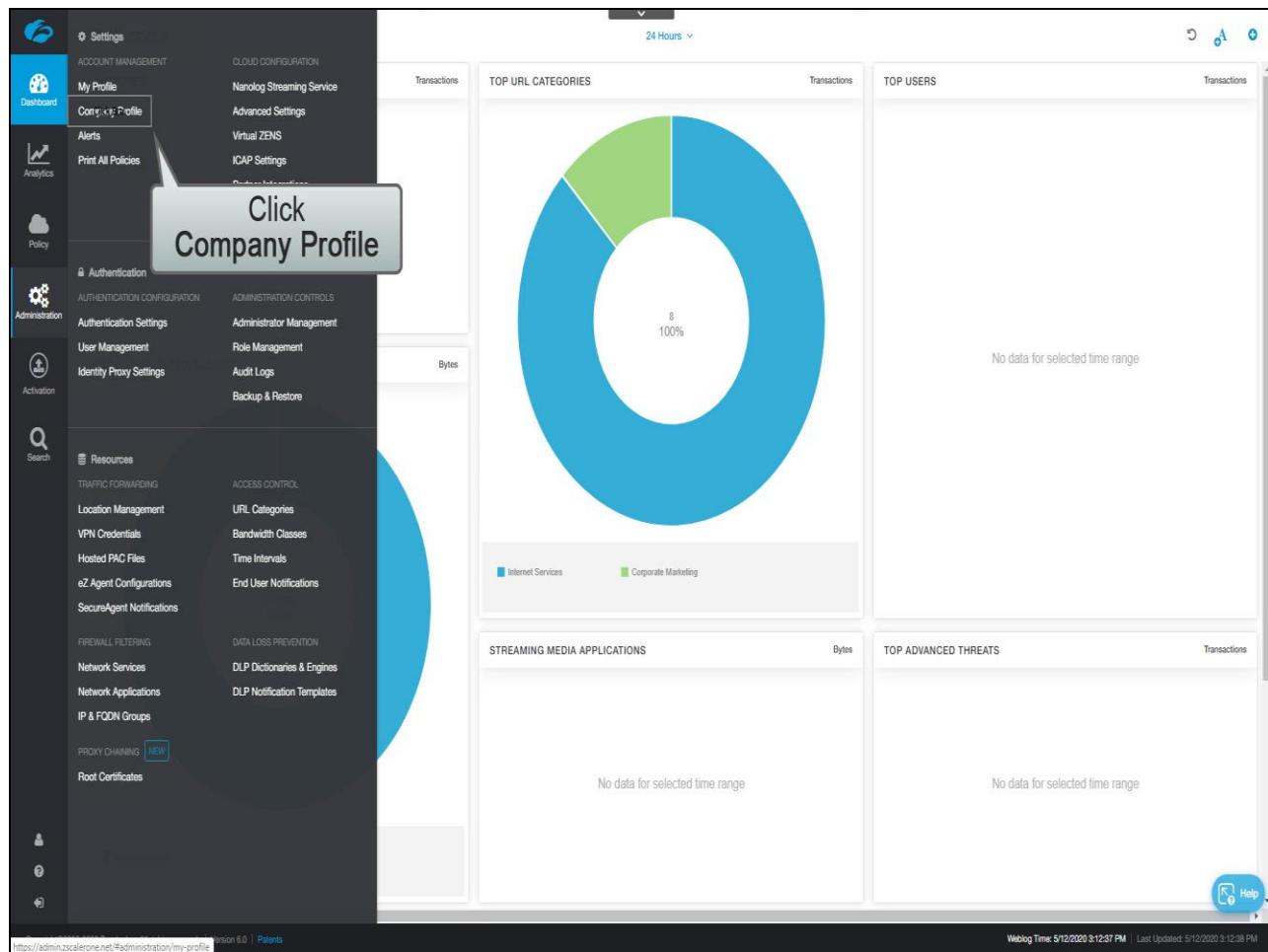
Slide 40 - Slide 40



Slide notes

Begin in the Zscaler Admin Portal by going to **Administration**, ...

Slide 41 - Slide 41



Slide notes

Then Company Profile.

Slide 42 - Slide 42

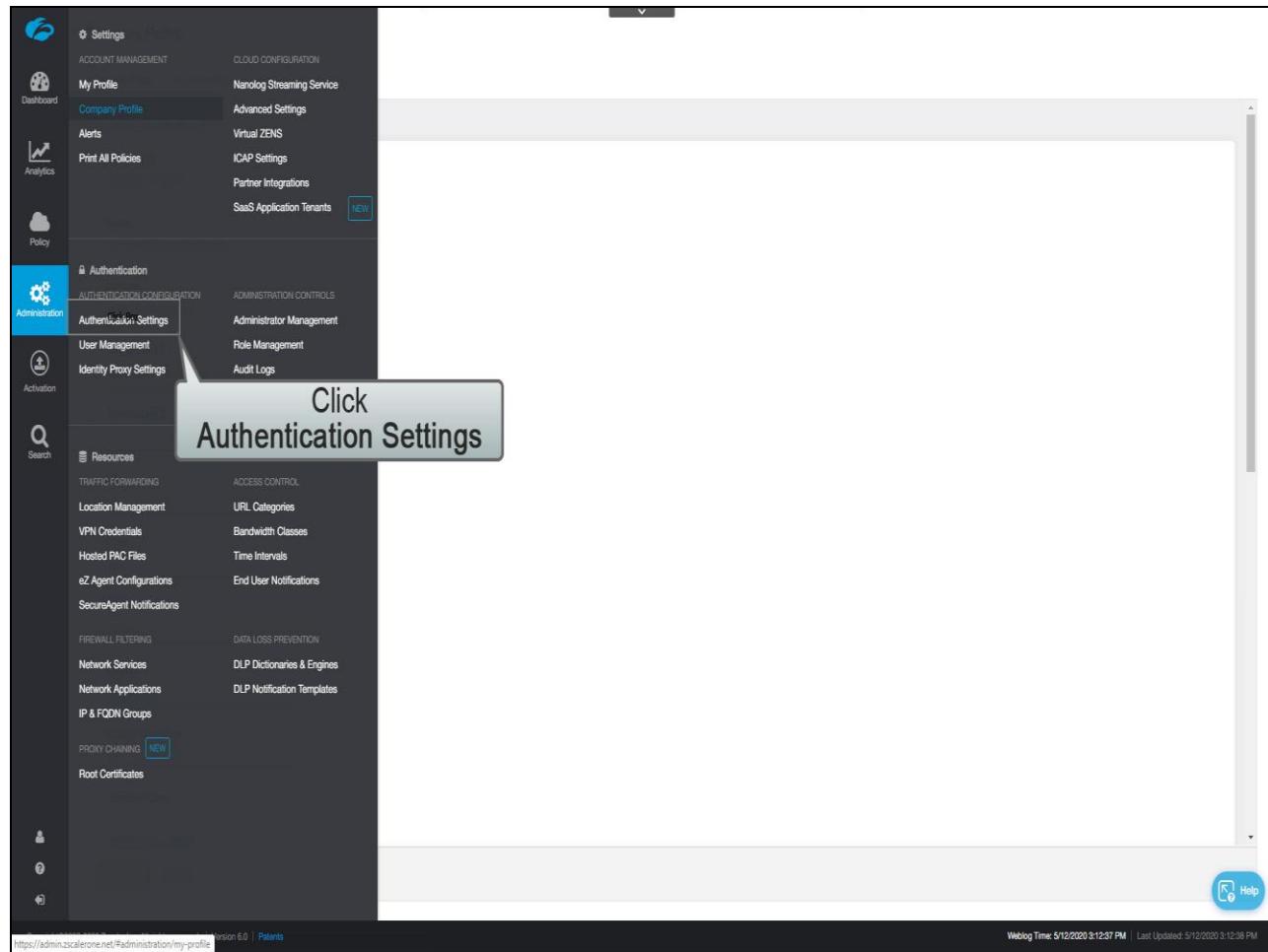
The screenshot shows the Zscaler Click Administration interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Click Administration (which is selected and highlighted in blue), Activation, Search, and Help. The main content area is titled "Company Profile". It has tabs for "ORGANIZATION" (selected) and "SUBSCRIPTIONS". Under "GENERAL INFORMATION", there is a "Company ID" field containing "zscalrone.net 8239192" with a yellow callout box highlighting the numerical part. Other fields include "Name" (Internal-training20.safemarch.com), "Domains" (training20.safemarch.com), and "Address Line 1" (Your company HQ location address). Below these are fields for "City", "State", "ZIP Code" (10110), "Country" (United States), "Primary Time Zone" (GMT), and "Company Logo" (Not Available, with a "Upload" link). At the bottom are "Save" and "Cancel" buttons, and a "Help" button on the right.

Slide notes

Under Company ID you will find part of the ID you will need later in the configuration process. For now, simply take note of the numerical portion of the Company ID.

We will now move on to configuring SAML. Click **Administration**.

Slide 43 - Slide 43



Slide notes

Then **Authentication Settings**.

Slide 44 - Slide 44

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a title 'Authentication Settings' and tabs for 'AUTHENTICATION PROFILE' (selected), 'IDENTITY PROVIDERS' (with a 'NEW' button), and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', there's a sub-section titled 'UPDATED' with 'Directory Type' set to 'Hosted DB'. 'Authentication Frequency' is set to 'Only Once'. 'Authentication Type' is currently set to 'Form-Based' (radio button selected). A callout box labeled 'Click SAML' points to the 'Click & Box' option in the dropdown menu for 'Authentication Type'. Other options shown are 'One-Time Token' and 'Two-Factor Authentication Email'. 'Password Strength' is set to 'Medium'. 'Password expiry' is set to 'Never'. Below this is a section for 'KERBEROS AUTHENTICATION' with an 'Enable Kerberos' checkbox. Under 'FORCE REAUTHENTICATION FOR ALL USERS', there's a 'Last Reauthentication' section and a 'Force Reauthentication' button labeled 'Start'. The status is 'None'. At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Slide notes

Under the **Authentication Type** select **SAML**, ...

Slide 45 - Slide 45

The screenshot shows the Zscaler Authentication Settings interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Authentication Settings' and has tabs for 'AUTHENTICATION PROFILE' (selected), 'IDENTITY PROVIDERS' (with a 'NEW' button), and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', there's a sub-section for 'Directory Type' with 'Hosted DB' selected. 'Authentication Frequency' is set to 'Only Once'. 'Authentication Type' includes 'Form-Based' and 'SAML' (selected). 'Temporary Authentication' is set to 'Disabled'. A 'Send Authentication Email' link is also present. Below this is a section for 'KERBEROS AUTHENTICATION' with an 'Enable Kerberos' toggle switch. A large modal window is open under 'FORCE REAUTHENTICATION FOR ALL USERS'. It contains fields for 'Last Reauthentication' (with a dropdown menu) and 'Force Reauthentication' (with a 'Start' button). Under 'Reauthentication', 'None' is selected. At the bottom of the modal are 'Save' and 'Cancel' buttons. A callout bubble points to the 'Save' button with the text 'Click Save'. The bottom right corner of the modal has a 'Help' icon. At the very bottom of the page, there's a copyright notice 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents' and a timestamp 'Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM'.

Slide notes

and click **Save**.

Slide 51 - Slide 51

The screenshot shows the Zscaler Authentication Settings interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, and Activation. The main content area has tabs for AUTHENTICATION PROFILE, IDENTITY PROVIDERS (highlighted in blue), and AUTHENTICATION BRIDGES. Under AUTHENTICATION PROFILE, settings include Directory Type (Hosted DB selected), Authentication Frequency (Only Once), Authentication Type (SAML selected), and Temporary Authentication (One-Time Link selected). A large, semi-transparent button labeled "Click Activation" is overlaid on the page. The bottom section shows FORCE REAUTHENTICATION FOR ALL USERS with a "Start" button and a status message indicating "None". At the bottom right is a "Help" icon.

Slide notes

Activate your changes.

Slide 52 - Slide 52

The screenshot shows the Zscaler Activation interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation (with a red notification dot), and Search. The main area has a light gray header with tabs: 'MY ACTIVATION STATUS' (highlighted in red), 'CURRENTLY EDITING (1)', 'IDENTITY PROVIDERS (NEW)', and 'AUTHENTICATION BRIDGES'. Below the header, it says 'admin@training02.welenu.com' and 'UPDATED'. Under 'QUEUED ACTIVATIONS (0)' it says 'None'. There is a checkbox labeled 'Force Activate' followed by a blue button labeled 'Click Box'. A large gray callout box with the text 'Click Activate' points to the 'Click Box' button. At the bottom right is a blue 'Help' icon.

Slide notes

Slide 55 - Slide 55

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left is a dark sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a light gray background. At the top, there are tabs for 'AUTHENTICATION PROFILE' (selected), 'IDENTITY PROVIDERS' (highlighted with a blue border and a callout box containing the text 'Click Identity Providers tab'), and 'AUTHENTICATION BRIDGES'. Below these tabs, there are sections for 'AUTHENTICATION PROFILE' (status: UPDATED), 'Directory Type' (Hosted DB selected), 'Authentication Frequency' (Only Once), 'Authentication Type' (SAML selected), and 'Temporary Authentication' (One-Time Link selected). A 'KERBEROS AUTHENTICATION' section is present with an 'Enable Kerberos' toggle switch. A 'FORCE REAUTHENTICATION FOR ALL USERS' section includes 'Last Reauthentication' (disabled), a 'Force Reauthentication' button, and 'Reauthentication Status' (None). At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Slide notes

You will now define the Identity Provider configuration. Click the **Identity Providers** tab.

Slide 57 - Slide 57

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a header 'Authentication Settings' with tabs for 'AUTHENTICATION PROFILE', 'IDENTITY PROVIDERS' (which is selected), and 'AUTHENTICATION BRIDGES'. Below the tabs is a button 'Add Identity Provider' and a link 'Add Zscaler App Portal as IdP'. A table lists identity providers:

No.	ID	Name	Status	Location	IdP SAML Certificate Expiratio...	Authentication Domains	Default IdP
1	760	Default	Green checkmark	Any	June 05, 2028	Any	

At the bottom of the table are 'Save' and 'Cancel' buttons. A callout box with the text 'Click Edit icon' points to the edit icon in the 'Default IdP' column for the first row. The footer contains copyright information, a help icon, and a timestamp.

Slide notes

At this point you have the option to use the Default IdP configuration, and edit it, or create a new IdP configuration by clicking the **Add Identity Provider** button. Creating a new IdP configuration is generally done, however, if you plan on using the Multiple IdP feature (or just MIdP for short). MIdP will be covered in a separate module.

For this example we will use the Default configuration. Click the **Edit icon** to the right of the default config.

Slide 58 - Slide 58

The screenshot shows the ZCCP interface with the 'Authentication Settings' menu selected. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays a table of identity providers, with one row selected for editing.

Edit Identity Provider Dialog:

- GENERAL INFO:**
 - Name: Default
 - Status: Enabled (radio button selected)
 - SAML Portal URL: https://xyz.zyx
 - Login Name Attribute: X
 - Entity ID: zscalerone.net
 - Org-Specific Entity ID: Enabled (radio button selected)
 - IdP SAML Certificate: okta.pem (Upload button)
 - IdP SAML Certificate Expiration Date: June 05, 2028
 - Vendor: Others
 - Default IdP: Enabled (radio button selected)
- CRITERIA:**
 - Locations: Any
 - Authentication Domains: Any
- SERVICE PROVIDER (SP) OPTIONS:**
 - Sign SAML Request: Off (checkbox unchecked)
 - Request Signing SSL Certificate: sami_1
 - SP SAML Certificate Expiration Date: October 11, 2020
 - SP Metadata: Download Metadata
 - SP SAML Certificate: Download Certificate
- AUTO-PROVISIONING OPTIONS:**
 - Enable SAML Auto-Provisioning: Off (checkbox unchecked)
 - Enable SCIM-Based Provisioning: Off (checkbox unchecked)

Buttons at the bottom: Save (grayed out), Cancel, Help (blue icon).

Copyright 2020 Zscaler Inc. All rights reserved. | Version 6.0 | Policies | Weblog Time: 5/12/2020 9:12:57 PM | Last Updated: 5/12/2020 9:12:58 PM

Slide notes

Provide a descriptive name if you wish. In our case, I will re-name Default to Okta.

Slide 60 - Slide 60

The screenshot shows the 'Edit Identity Provider' dialog box over a dark background of the Okta interface. The dialog is titled 'Edit Identity Provider' and contains several sections:

- GENERAL INFO**:
 - Name: Okta
 - Status: Enabled (radio button selected)
 - SAML Portal URL: https://xyz.zyx
 - Login Name Attribute: X
 - Entity ID: zscalerone.net
 - Org-Specific Entity ID: Enabled (radio button selected)
 - IdP SAML Certificate: okta.pem (Upload button)
 - IdP SAML Certificate Expiration Date: June 05, 2028
 - Vendor: Others
 - Default IdP: Enabled (radio button selected)
- CRITERIA**:
 - Locations: Any
 - Authentication Domains: Any
- SERVICE PROVIDER (SP) OPTIONS**:
 - Sign SAML Request: Off (checkbox unchecked)
 - Request Signing SSL Certificate: sami_1
 - SP SAML Certificate Expiration Date: October 11, 2020
 - SP Metadata: Download Metadata
 - SP SAML Certificate: Download Certificate
- AUTO-PROVISIONING OPTIONS**:
 - Enable SAML Auto-Provisioning: Off (checkbox unchecked)
 - Enable SCIM-Based Provisioning: Off (checkbox unchecked)

At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows a list of authentication providers and domains.

Slide notes

Next, you will need the SAML Portal URL and Login Name attribute from your IdP. Refer to your IdP documentation on where to obtain this information.

Slide 61 - Slide 61

The screenshot shows the Zscaler SAML Configuration interface. At the top, there's a navigation bar with links like 'Role Management', 'Audit Logs', 'Backup & Restore', and 'Temporary Authentication'. Below this is a 'Kerberos Authentication' section with a 'Enable Kerberos' button. A red arrow points to the 'Save' button at the bottom right of the main content area.

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

- SAML Portal URL: Copy and paste the following:
<https://trainingsafemarch20.okta.com/app/zscalerbyz/exk24yj9voene8lx1357/sso/saml>
- Login Name Attribute: Enter NameID.
- Public SSL Certificate: First click here to download the certificate for upload:
<https://trainingsafemarch20-admin.okta.com/admin/org/security/0oa24yj9rpRo2Qez2357/cert>

Then click Upload to upload it to Zscaler.

- Click Save.

A detailed view of the 'Edit SAML' dialog box is shown below, highlighting the fields entered in the previous steps:

- Identity Provider (IDP) Options:**
 - SAML Portal URL: <https://ohikadev.treecloud.com/app/zscalerkt1pdcmhNMlQGDQYKZ/sso/saml>
 - Login Name Attribute: NameID
 - Public SSL Certificate: [okta.pem](#) (with the 'Upload' button highlighted)
- Service Provider (SP) Options:**
 - Sign SAML Requests:
 - Signature Algorithm: [SHA-1 \(1024-bit\)](#) SHA-2 (256-bit)
 - SP's Public SSL Certificate: [Download](#)
 - SP's Metadata: [Download](#)
- Auto-Provisioning Options:**
 - Enable SAML Auto-Provisioning:
 - User Display Name Attribute: DisplayName
 - Group Name Attribute: memberOf
 - Department Name Attribute: Department

The 'Save' button at the bottom right of the dialog box is also highlighted with a red box.

Slide notes

In Okta, for example, they have a setup instructions page as part of their configuration wizard that provides this information. You can see the **SAML Portal URL for your specific Organization**, the **Login Name Attribute**, and the link to download the **Public SSL Certificate**.

Slide 62 - Slide 62

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

- SAML Portal URL: Copy and paste the following:
`https://trainingsafemarch20.okta.com/app/zscalerbyz/exk24yj9voene8lx1357/sso/saml`
- Login Name Attribute: Enter NameID.
- Public SSL Certificate: First click here to download the certificate for upload.
`https://trainingsafemarch20-admin.okta.com/admin/org/security/0ea24yj9rpAo2Qez2357/cert`

Then click Upload to upload it to Zscaler.

- Click Save.

Slide notes

Begin by copying and pasting the **SAML Portal URL** and the **Login Name Attribute**, which is **NameID**.

Slide 65 - Slide 65

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

- SAML Portal URL: Copy and paste the following:
https://trainingsafemarch20.okta.com/app/zscalerbyz/ext24y9noene8lx1357/sso/saml
- Login Name Attribute: Enter NameID.
- Public SSL Certificate: First click here to download the certificate for upload.
https://trainingsafemarch20-admin.okta.com/admin/org/security/0oa24y9npk

Then click Upload to upload it to Zscaler.

- Click Save.

The 'Edit SAML' dialog shows the configuration details:

- Identity Provider (IDP) Options:
 - SAML Portal URL: https://ohikadev.treecloud.com/app/zscalerkt1pcumhNMlQGDQYZ/sso/saml
 - Login Name Attribute: NameID
 - Public SSL Certificate: okta.pem (Upload button highlighted)
- Service Provider (SP) Options:
 - Sign SAML Requests: checked
 - Signature Algorithm: SHA-1 (1024-bit) SHA-2 (256-bit)
 - SP's Public SSL Certificate: Download
 - SP's Metadata: Download
- Auto-Provisioning Options:
 - Enable SAML Auto-Provisioning: checked
 - User Display Name Attribute: DisplayName
 - Group Name Attribute: memberOf
 - Department Name Attribute: Department

The 'Save' button is highlighted in red at the bottom right of the dialog.

Slide notes

Slide 66 - Slide 66

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

- SAML Portal URL: Copy and paste the following:
<https://trainingsafemarch20.okta.com/app/zscalerbyz/ext24yj9noene8lx1357/sso/saml>
- Login Name Attribute: Enter NameID.
- Public SSL Certificate: First click here to download the certificate for upload.
<https://trainingsafemarch20-admin.okta.com/admin/org/security/0ea24yj9rpAo2Qez2357/cert>

Then click Upload to upload it to Zscaler.

- Click Save.

Slide notes

Then click the link to download a copy of the SSL certificate.

Slide 70 - Slide 70

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

- SAML Portal URL: Copy and paste the following:
`https://trainingsafemarch20.okta.com/app/zscalerbyz/exk24yj9voene8lx1357/sso/saml`
- Login Name Attribute: Enter NameID.
- Public SSL Certificate: First click here to download the certificate for upload.
`https://trainingsafemarch20-admin.okta.com/admin/org/security/0ea24yj9rpAo2Qez2357/cert`

Then click Upload to upload it to Zscaler.

- Click Save.

Slide notes

Slide 71 - Slide 71

Click
SAML Portal URL
field

Slide notes

Paste in the SAML Portal URL you copied from the IdP.

Slide 72 - Slide 72

The screenshot shows the 'Edit Identity Provider' dialog for Okta in the Okta web interface. The 'GENERAL INFO' tab is selected. A context menu is open over the 'SAML Portal URL' input field, which contains the following options: Undo (Ctrl+Z), Redo (Ctrl+Shift+Z), Cut (Ctrl+X), Copy (Ctrl+C), Paste (Ctrl+V), Paste as plain text (Ctrl+Shift+V), Select all (Ctrl+A), Spell check, Writing Direction, and Inspect. A large callout box with the text 'Click Paste to paste the SAML URL copied from the IdP' points to the 'Paste' option in the menu. The 'Name' field is set to 'Okta'. The 'Status' is 'Enabled'. The 'Login Name Attribute' is empty. The 'Org-Specific Entity ID' is set to 'Enabled'. The 'IdP SAML Certificate Expiration Date' is listed as 'June 05, 2028'. The 'Default IdP' is 'Enabled'. The 'SERVICE PROVIDER' section includes fields for 'Request Signing SSL Certificate' (set to 'saml_1') and 'SP Metadata' (with download links). The 'AUTO-PROVISIONING OPTIONS' section includes checkboxes for 'Enable SAML Auto-Provisioning' and 'Enable SCIM-Based Provisioning', both of which are checked. At the bottom are 'Save' and 'Cancel' buttons.

Slide notes

Slide 73 - Slide 73

The screenshot shows the 'Edit Identity Provider' dialog box over a dark-themed Okta dashboard. The dialog is titled 'Edit Identity Provider' and contains several sections:

- GENERAL INFO**:
 - Name: Okta (Status: Enabled)
 - SAML Portal URL: https://trainingsafenet20.okta.com/app/zscal...
 - Login Name Attribute: X
 - Entity ID: zscalerone.net (Org-Specific Entity ID: Enabled)
 - IdP SAML Certificate: okta.pem (Upload button)
 - IdP SAML Certificate Expiration Date: June 05, 2028
 - Vendor: Others
- CRITERIA**:
 - Locations: Any
 - Authentication Domains: Any
- SERVICE PROVIDER (SP) OPTIONS**:
 - Sign SAML Request: Off
 - Request Signing SSL Certificate: sami_1 (SP SAML Certificate Expiration Date: October 11, 2020)
 - SP Metadata: Download Metadata (Download Certificate)
- AUTO-PROVISIONING OPTIONS**:
 - Enable SAML Auto-Provisioning: Off
 - Enable SCIM-Based Provisioning: Off

At the bottom of the dialog are 'Save' and 'Cancel' buttons. The main dashboard background shows a table with columns 'Authentication Domains' and 'Default IdP'.

Slide notes

Slide 74 - Slide 74

The screenshot shows the 'Edit Identity Provider' dialog box over a dark-themed Okta dashboard. The dialog is titled 'Edit Identity Provider' and contains several sections:

- GENERAL INFO**:
 - Name: Okta
 - Status: Enabled (radio button selected)
 - SAML Portal URL: https://trainingsafenet20.okta.com/app/zscal...
 - Login Name Attribute: Type "NameID" and hit enter
 - Entity ID: zscalerone.net
 - Org-Specific Entity ID: Enabled (radio button selected)
 - IdP SAML Certificate: okta.pem (Upload button)
 - IdP SAML Certificate Expiration Date: June 05, 2028
 - Vendor: Others
 - Default IdP: Enabled (radio button selected)
- CRITERIA**:
 - Locations: Any
 - Authentication Domains: Any
- SERVICE PROVIDER (SP) OPTIONS**:
 - Sign SAML Request: Off (checkbox unchecked)
 - Request Signing SSL Certificate: sami_1
 - SP SAML Certificate Expiration Date: October 11, 2020
 - SP Metadata: Download Metadata
 - SP SAML Certificate: Download Certificate
- AUTO-PROVISIONING OPTIONS**:
 - Enable SAML Auto-Provisioning: Off (checkbox unchecked)
 - Enable SCIM-Based Provisioning: Off (checkbox unchecked)

At the bottom of the dialog are 'Save' and 'Cancel' buttons. The main dashboard background shows a table with columns 'Location', 'Domain', and 'Default IdP'.

Slide notes

Enter the Login Name Attribute used in your IdP configuration. In this example, use **NameID**. Note: This is case sensitive.

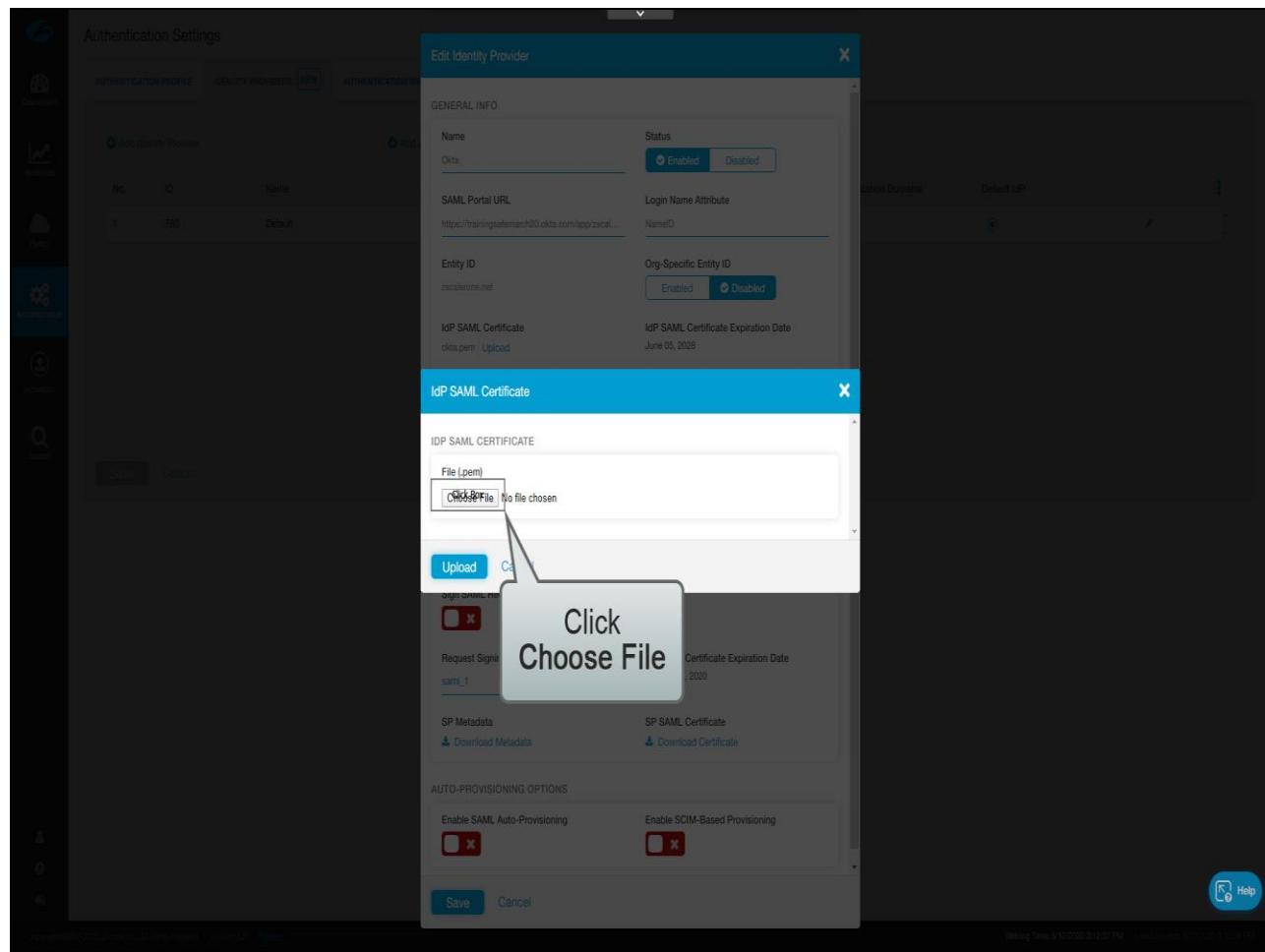
Slide 75 - Slide 75

The screenshot shows the Okta Authentication Settings interface. On the left, there's a sidebar with various icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area shows a table with one row: No. 1, ID 760, and Name Default. A modal window titled 'Edit Identity Provider' is open. Inside, under 'GENERAL INFO', there's a field for 'Name' (Okta) with two radio buttons for 'Status': 'Enabled' (selected) and 'Disabled'. Below it is 'SAML Portal URL' (https://trainingsafenet20.okta.com/app/zscal...), 'Entity ID' (zscalerone.net), and 'Vendor' (Others). There are also fields for 'Login Name Attribute' (NameID), 'Org-Specific Entity ID' (Enabled), 'IdP SAML Certificate' (okta.pem), and 'Default IdP' (Enabled). Under 'CRITERIA', there are dropdowns for 'Locations' (Any) and 'Authentication Domains' (Any). A large callout bubble with the text 'Click Box' points to the 'Click Box' button next to the 'IdP SAML Certificate' field. The 'SERVICE PROVIDER (SP) OPTIONS' section includes 'Sign SAML Request' (unchecked), 'Request Signing SSL Certificate' (saml_1), 'SP Metadata' (Download Metadata), and 'SP SAML Certificate' (Download Certificate). The 'AUTO-PROVISIONING OPTIONS' section includes 'Enable SAML Auto-Provisioning' (unchecked) and 'Enable SCIM-Based Provisioning' (unchecked). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

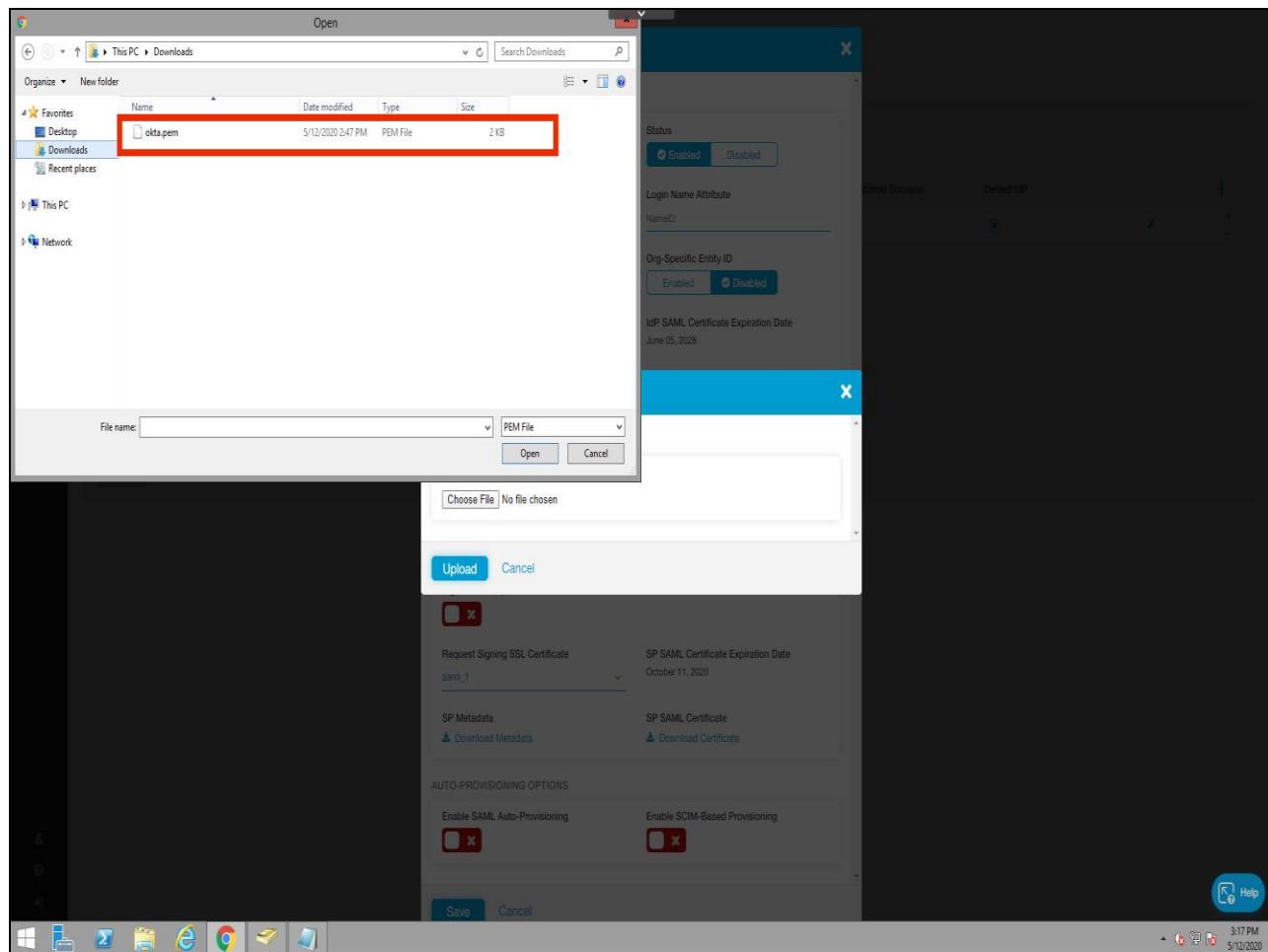
Now let's upload the Okta **Public SSL Certificate** we downloaded at the beginning of the configuration demonstration.

Slide 76 - Slide 76



Slide notes

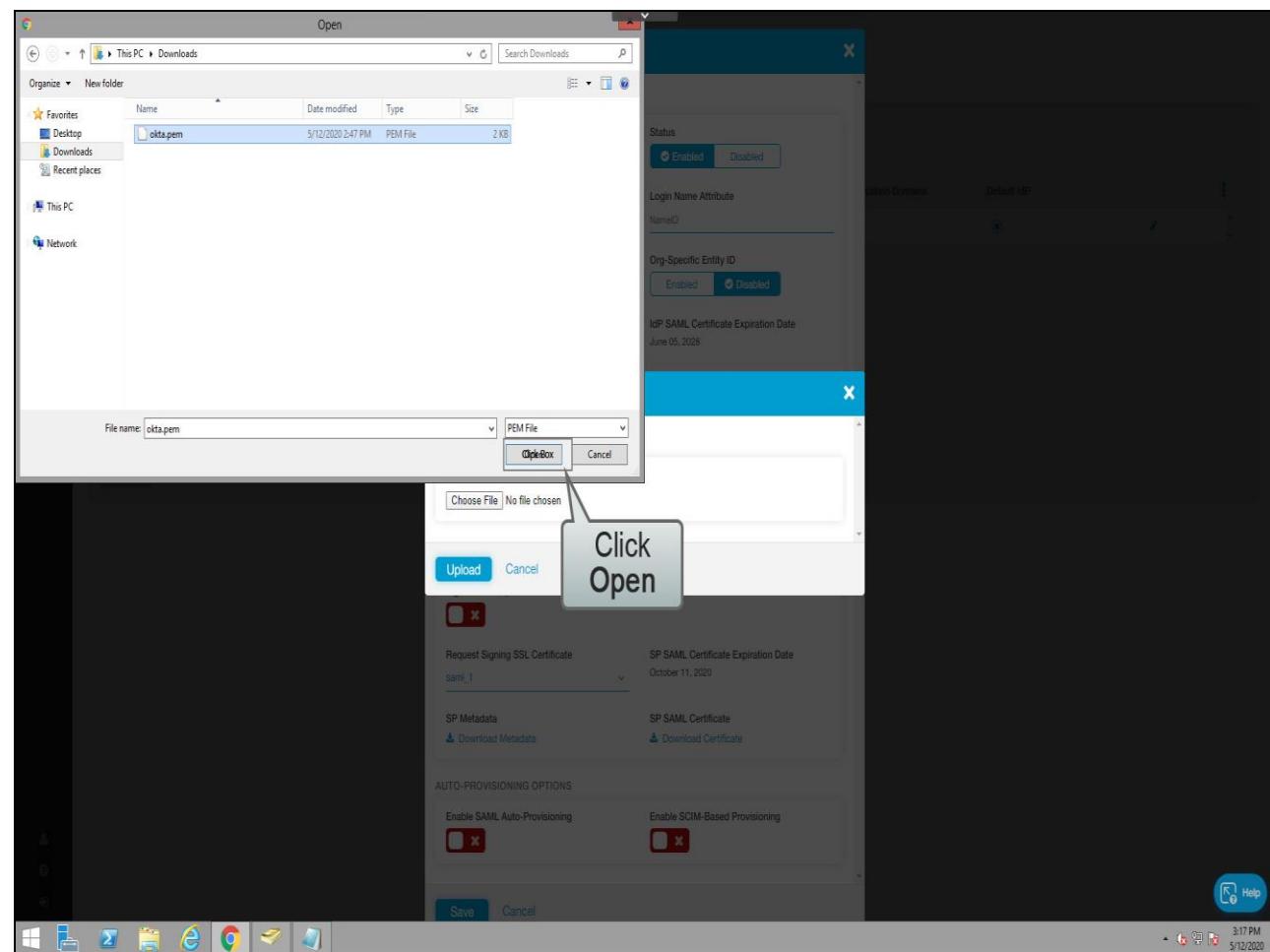
Slide 77 - Slide 77



Slide notes

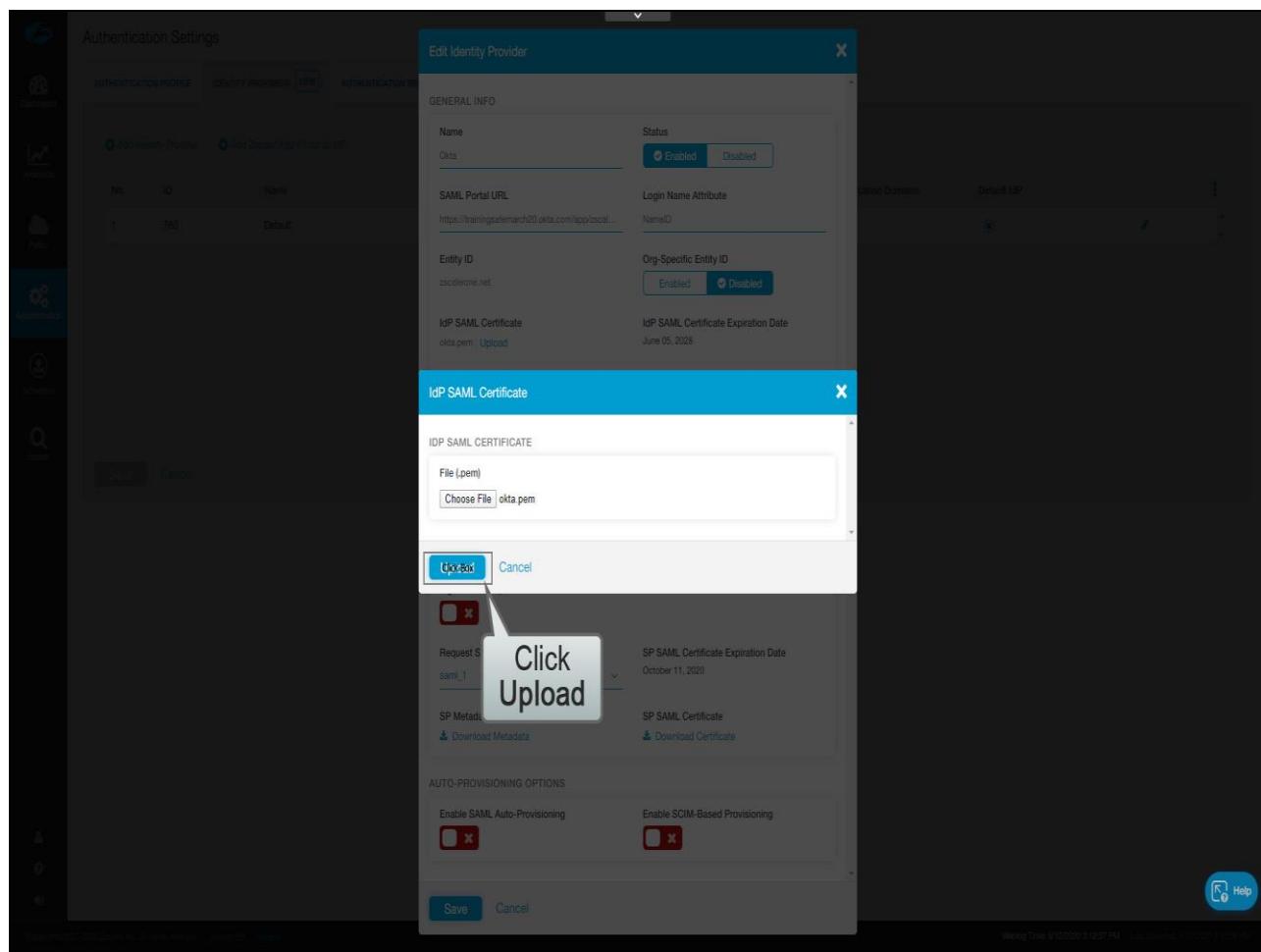
Highlight the file **okta.pem** then click **Open**.

Slide 78 - Slide 78



Slide notes

Slide 79 - Slide 79



Slide notes

Then **Upload**.

Slide 80 - Slide 80

The screenshot shows the Zscaler Authentication Settings interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has tabs for AUTHENTICATION PROFILE, IDENTITY PROVIDERS (highlighted), and AUTHENTICATION BRIDGE. A modal window titled 'Edit Identity Provider' is open, showing 'Uploaded Successfully' at the top. The 'GENERAL INFO' tab is selected. Inside, the 'Name' field contains 'Okta', 'Status' is set to 'Enabled', and 'SAML Portal URL' is 'https://trainingsafemarch20.okta.com/app/zscaler...'. The 'Entity ID' is 'zscalerone.net' and 'Org-Specific Entity ID' is also 'zscalerone.net'. The 'IdP SAML Certificate' is 'okta.pem' with an 'Upload' link, and its expiration date is 'June 05, 2028'. The 'Vendor' dropdown is set to 'Click Box'. A callout bubble points to this dropdown with the text 'Click Vendor drop-down'. Other sections include 'CRITERIA' (Locations set to 'Any'), 'SERVICE PROVIDER (SP) OPTIONS' (Sign SAML Request checked, Request Signing SSL Certificate set to 'saml_1'), 'AUTO-PROVISIONING OPTIONS' (Enable SAML Auto-Provisioning checked, Enable SCIM-Based Provisioning checked), and buttons for 'Save' and 'Cancel'. At the bottom right of the modal is a 'Help' icon.

Slide notes

Select the IdP from the **Vendors** drop-down.

Slide 84 - Slide 84

The screenshot shows the 'Edit Identity Provider' dialog box over a background of the 'Authentication Settings' page. The dialog is titled 'Edit Identity Provider' and has a tab bar with 'GENERAL INFO' selected.

GENERAL INFO

- Name:** Okta
- Status:** Enabled (radio button selected)
- SAML Portal URL:** https://trainingsafemarch20.okta.com/app/zscal...
- Login Name Attribute:** NameID
- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled (radio button selected)
- IdP SAML Certificate:** okta.pem (Upload button)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Others (dropdown menu)
 - Google Apps
 - Microsoft Azure Active Directory
 - Okta
 - OneLogin
 - Others
- Default IdP:** Enabled (radio button selected)
- Authentication Domains:** Any

SERVICE PROVIDER (SP) OPTIONS

- Sign SAML Request:** Enabled (checkbox checked)
- Request Signing SSL Certificate:** sami_1
- SP SAML Certificate Expiration Date:** October 11, 2020
- SP Metadata:** Download Metadata
- SP SAML Certificate:** Download Certificate

AUTO-PROVISIONING OPTIONS

- Enable SAML Auto-Provisioning:** Enabled (checkbox checked)
- Enable SCIM-Based Provisioning:** Enabled (checkbox checked)

Buttons: Save (blue button), Cancel (gray button), Help (blue icon).

Slide notes

Slide 85 - Slide 85

The screenshot shows the Zscaler Authentication Settings interface. On the left, there's a sidebar with various icons: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area shows 'Authentication Settings' with tabs for AUTHENTICATION PROFILE, IDENTITY PROVIDERS (highlighted), and AUTHENTICATION BRIDGE. Under IDENTITY PROVIDERS, there's a table with one row for 'Okta'. The 'Edit Identity Provider' dialog is open for the Okta entry. It has sections for GENERAL INFO (Name: Okta, Status: Enabled/Disabled, SAML Portal URL: https://trainingsafemarch20.okta.com/app/zscaler..., Entity ID: zscalerone.net, Org-Specific Entity ID: Enabled/Disabled, IdP SAML Certificate: okta.pem, IdP SAML Certificate Expiration Date: June 05, 2028, Vendor: Okta, Default IdP: Enabled), CRITERIA (Locations: Any, Authentication Domains: Any), and SERVICE PROVIDER (SP) OPTIONS (Sign SAML Request: checked). At the bottom of the dialog is a 'Save' button. A callout bubble with a red border and white background points to the 'Enable SCIM-Based Provisioning' checkbox in the AUTO-PROVISIONING OPTIONS section. This section also includes 'Enable SAML Auto-Provisioning' (unchecked) and a 'Download Certificate' link. The background shows a list of authentication domains and their default IdPs.

Slide notes

As discussed earlier in the slides, you have a choice when it comes to automatic user provisioning of user information into the Zscaler User Database. You can either use SAML Auto Provisioning or SCIM Based Provisioning.

For this example, however, we will leave Auto-Provisioning disabled and we will focus on the use and configuration of SCIM. Click **Enable SCIM-Based Provisioning**.

Slide 86 - Slide 86

The screenshot shows the 'Edit Identity Provider' dialog box over a dark background of the Okta dashboard. The dialog is titled 'Edit Identity Provider' and has tabs for 'GENERAL INFO', 'CRITERIA', 'SERVICE PROVIDER (SP) OPTIONS', and 'AUTO-PROVISIONING OPTIONS'. The 'GENERAL INFO' tab is active.

GENERAL INFO

Name	Status
Okta	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SAML Portal URL	Login Name Attribute
https://trainingsafemarch20.okta.com/app/zscal...	NameID
Entity ID	Org-Specific Entity ID
zscalerone.net	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IdP SAML Certificate	IdP SAML Certificate Expiration Date
okta.pem	June 05, 2028
Vendor	Default IdP
Okta	<input checked="" type="radio"/> Enabled

CRITERIA

Locations	Authentication Domains
Any	Any

SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request	<input type="checkbox"/>
Request Signing SSL Certificate	SP SAML Certificate Expiration Date
saml_1	October 11, 2020
SP Metadata	SP SAML Certificate
Download Metadata	Download Certificate

AUTO-PROVISIONING OPTIONS

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

Base URL: <https://trainingsafemarch20.okta.com/app/zscal...>

Save Cancel

Copyright © 2017-2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Help](#)

Weblog Time: 5/12/2020 9:12:57 PM | Last Updated: 5/12/2020 9:12:58 PM

Slide notes

Slide 87 - Slide 87

The screenshot shows the ZCCP interface with the 'Edit Identity Provider' dialog open over a background list of identity providers. The dialog is titled 'Edit Identity Provider' and contains the following sections:

- GENERAL INFO**:
 - Name: Okta
 - Status: Enabled (radio button selected)
 - SAML Portal URL: https://trainingsafemarch20.okta.com/app/zscal...
 - Login Name Attribute: NameID
 - Entity ID: zscalerone.net
 - Org-Specific Entity ID: Enabled (radio button selected)
 - IdP SAML Certificate: okta.pem (Upload button)
 - IdP SAML Certificate Expiration Date: June 05, 2028
 - Vendor: Okta
 - Default IdP: Enabled
- CRITERIA**:
 - Locations: Any
 - Authentication Domains: Any
- SERVICE PROVIDER (SP) OPTIONS**:
 - Sign SAML Request: Unchecked
 - Request Signing SSL Certificate: sami_1
 - SP SAML Certificate Expiration Date: October 11, 2020
 - SP Metadata: Download Metadata
 - SP SAML Certificate: Download Certificate
- AUTO-PROVISIONING OPTIONS**:
 - Enable SAML Auto-Provisioning: Unchecked
 - Enable SCIM-Based Provisioning: Checked

At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows a list of identity providers with columns for 'Name', 'Status', and 'Last Updated'. A copyright notice at the bottom left reads 'Copyright © 2017-2020 Zscaler Inc. All rights reserved.' and 'Version 6.0 | Policies'.

Slide notes

Slide 88 - Slide 88

The screenshot shows the Zscaler Authentication Settings interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has tabs for AUTHENTICATION PROFILE, IDENTITY PROVIDERS (which is selected), and AUTHENTICATION BR.

Edit Identity Provider Dialog:

- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled (button)
- IdP SAML Certificate:** okta.pem (Upload button)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Okta
- Default IdP:** Enabled
- Locations:** Any
- Authentication Domains:** Any
- SERVICE PROVIDER (SP) OPTIONS:**
 - Sign SAML Request:** Off (checkbox)
 - Request Signing SSL Certificate:** saml_1
 - SP SAML Certificate Expiration Date:** October 11, 2020
 - SP Metadata:** Download Metadata
 - SP SAML Certificate:** Download Certificate
- AUTO-PROVISIONING OPTIONS:**
 - Enable SAML Auto-Provisioning:** Off (checkbox)
 - Enable SCIM-Based Provisioning:** On (checkbox)
 - Base URL:** https://scim.zscalerone.net/8239192/scim (Deprecated)
https://scim.zscalerone.net/8239192/760/scim
 - Bearer Token:** AU/YyvBtNzyg5Q2iHYJCE3hSgSWdFrxxnfsgsUOF56+eYEnkBuwRKGGUOa7IA==
 - Generate Token:** Button

Buttons at the bottom: Save, Cancel, Help (with a question mark icon).

Slide notes

Depending on your IdP, you may or may not need to copy the Base URL. For example, Microsoft Azure requires the Base URL to be provided as part of its configuration where Okta knows the format based on information you provide in other parts of the configuration. As such, you do not need to copy it when using Okta. Be sure to check your IdP documentation.

For all IdPs, however, you do need to provide the Bearer Token which is issued to authenticate SCIM requests when the IdP to communicates with Zscaler's API.

Slide 89 - Slide 89

The screenshot shows the ZCCP interface with the 'Edit Identity Provider' dialog open. The dialog contains the following configuration details:

- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled
- IdP SAML Certificate:** okta.pem (Upload)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Okta
- Default IdP:** Enabled

CRITERIA:

- Locations: Any
- Authentication Domains: Any

SERVICE PROVIDER (SP) OPTIONS:

- Sign SAML Request:
- Request Signing SSL Certificate: sami_1
- SP SAML Certificate Expiration Date: October 11, 2020
- SP Metadata: [Download Metadata](#)
- SP SAML Certificate: [Download Certificate](#)

AUTO-PROVISIONING OPTIONS:

- Enable SAML Auto-Provisioning:
- Enable SCIM-Based Provisioning:

Base URL:

https://scim.zscalerone.net/8239192/scim (Deprecated)
https://scim.zscalerone.net/8239192/750/scim

Bearer Token:

AU/YyBtNzygLSQ2jHYJCE3hG-SWdFrxxnfsgsUOF56jeYEnkBuwRKGGUOoA7IA==

Buttons: Save, Cancel

Slide notes

Copy the **Bearer Token** for use in your IdP configuration.

Slide 91 - Slide 91

The screenshot shows the ZCCP interface with the 'Edit Identity Provider' dialog open. The dialog includes fields for Entity ID, Org-Specific Entity ID, IdP SAML Certificate, IdP SAML Certificate Expiration Date, Vendor, Default IdP, Criteria, Service Provider (SP) Options, Auto-Provisioning Options, and a Base URL field containing a Bearer Token.

Entity ID: zscalerone.net
Org-Specific Entity ID: Enabled
IdP SAML Certificate: okta.pem (Upload)
IdP SAML Certificate Expiration Date: June 05, 2028
Vendor: Okta
Default IdP: Enabled
Criteria: Locations: Any, Authentication Domains: Any
Service Provider (SP) Options: Sign SAML Request (checked)
Request Signing SSL Certificate: sami_1
SP SAML Certificate Expiration Date: October 11, 2020
SP Metadata: Download Metadata
SP SAML Certificate: Download Certificate
Auto-Provisioning Options: Enable SAML Auto-Provisioning (checked), Enable SCIM-Based Provisioning (checked)
Base URL: https://scim.zscalerone.net/8239192/scim (Deprecated)
https://scim.zscalerone.net/8239192/760/scim
Bearer Token: AU7yvB9NzygJ5Q2t+HYJCE3NsWdFrxtsgsUCF56+eYnBwRKGGU0gA7A=

Slide notes

Copy the **Bearer Token** for use in your IdP configuration.

Slide 92 - Slide 92

The screenshot shows the ZCCP interface with the 'Edit Identity Provider' dialog box open. The dialog box contains the following fields:

- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled (button)
- IdP SAML Certificate:** okta.pem (Upload button)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Okta
- Default IdP:** Enabled

Below the dialog box, the main interface shows a table of authentication providers:

No.	ID	Name
1	760	Okta

On the left side, there is a sidebar with various navigation icons: Dashboard, Analytics, Policy, Administration, Activation, and Search. At the bottom of the page, there is a footer with copyright information and a help link.

Slide notes

Slide 93 - Slide 93

Authentication Settings

Edit Identity Provider

Entity ID: zscalerone.net

Org-Specific Entity ID: Enabled

IdP SAML Certificate: okta.pem Upload

IdP SAML Certificate Expiration Date: June 05, 2028

Vendor: Okta

Default IdP: Enabled

CRITERIA

Locations: Any

Authentication Domains: Any

SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request:

Request Signing SSL Certificate: saml_1

SP SAML Certificate Expiration Date: October 11, 2020

SP Metadata: Download Metadata

AUTO-PROVISIONING OPTIONS

Enable SAML Auto-Provisioning:

Base URL: https://scim.zscalerone.net:8239192/scim
https://scim.zscalerone.net:8239192/760/scim

Bearer Token: AU/YyBtNzygLSQ2jHYJCE3iSvSWdFxxnsgsUOF56jeTEnkBuwRKGGUOa7A==

Generate Token:

Save: Cancel:

Copyright ©2017-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Policies

Help:

Weblog Time: 5/12/2020 9:12:57 PM | Last Updated: 5/13/2020 3:12:08 PM

Slide notes

At the beginning of this demo I showed you where to find the Company ID. The company ID is one of two ID's the IdP needs to properly identify your organization. With the addition of the MIdP functionality we have also added an IdP ID.

You can see in the Zoom field near the upper left corner the IdP ID for the Default configuration is 760.

The combination of these values equals the Zscaler ID. You can also see in the Zoom window that, nested within the Base URL is the complete Zscaler ID. So, in this example, you will copy that value and provide it to Okta.

Slide 94 - Slide 94

The screenshot shows the ZCCP interface with the 'Edit Identity Provider' dialog box open. The dialog box contains the following fields:

- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled (button)
- IdP SAML Certificate:** okta.pem (Upload button)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Okta
- Default IdP:** Enabled

CRITERIA:

- Locations:** Any
- Authentication Domains:** Any

SERVICE PROVIDER (SP) OPTIONS:

- Sign SAML Request:** Off (checkbox)
- Request Signing SSL Certificate:** saml_1
- SP SAML Certificate Expiration Date:** October 11, 2020
- SP Metadata:** Download Metadata
- SP SAML Certificate:** Download Certificate

AUTO-PROVISIONING OPTIONS:

- Enable SAML Auto-Provisioning:** Off (checkbox)
- Enable SCIM-Based Provisioning:** On (checkbox)

Base URL: https://scim.zscalerone.net/8239192/scim (Deprecated)
https://scim.zscalerone.net/8239192762/scim

Bearer Token: AU/YyBbNzygLSQ2jHYJCE3hG-SWdFxxnIsgsUOF56jeYEnkBuwRKGGUOoA7A==

Buttons: Save, Cancel, Help

Slide notes

Slide 95 - Slide 95

The screenshot shows the ZCCP interface with the 'Edit Identity Provider' dialog box open. The dialog box contains the following fields:

- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled (button)
- IdP SAML Certificate:** okta.pem (Upload button)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Okta
- Default IdP:** Enabled

Below these fields is a section titled 'CRITERIA' with dropdown menus for 'Locations' (Any) and 'Authentication Domains' (Any).

Under 'SERVICE PROVIDER (SP) OPTIONS':

- Sign SAML Request:** (checkbox)
- Request Signing SSL Certificate:** saml_1
- SP SAML Certificate Expiration Date:** October 11, 2020
- SP Metadata:** (Download Metadata button)
- SP SAML Certificate:** (Download Certificate button)

Under 'AUTO-PROVISIONING OPTIONS':

- Enable SAML Auto-Provisioning:** (checkbox)
- Enable SCIM-Based Provisioning:** (checkbox)

Below these options is a 'Base URL' field with a tooltip '(Deprecated)' and a context menu open over the URL 'https://scim.zscalerone.net/8239192/scim'. The context menu includes:

- Copy (Ctrl+C)
- Search Google for '8239192/760'
- Print... (Ctrl+P)
- Inspect (Ctrl+Shift+I)

At the bottom of the dialog box are 'Save' and 'Cancel' buttons.

Slide notes

Slide 96 - Slide 96

The screenshot shows the ZCCP interface with the 'Authentication Settings' page open. A modal window titled 'Edit Identity Provider' is displayed, specifically for the Okta identity provider. The modal contains the following fields:

- Entity ID:** zscalerone.net
- Org-Specific Entity ID:** Enabled (blue button)
- IdP SAML Certificate:** okta.pem (Upload button)
- IdP SAML Certificate Expiration Date:** June 05, 2028
- Vendor:** Okta
- Default IdP:** Enabled

Below these fields is a 'CRITERIA' section with dropdowns for 'Locations' (Any) and 'Authentication Domains' (Any).

The 'SERVICE PROVIDER (SP) OPTIONS' section includes:

- Sign SAML Request:** Unchecked (red X)
- Request Signing SSL Certificate:** sami_1
- SP SAML Certificate Expiration Date:** October 11, 2020
- SP Metadata:** Download Metadata
- SP SAML Certificate:** Download Certificate

The 'AUTO-PROVISIONING OPTIONS' section includes:

- Enable SAML Auto-Provisioning:** Unchecked (red X)
- Enable SCIM-Based Provisioning:** Checked (green checkmark)

Under 'Base URL', the URL https://scim.zscalerone.net/8239192/scim is shown, with a tooltip '(Deprecated)'. A context menu is open over this URL, displaying options: Copy (Ctrl+C), Search Google for '8239192/760', Print... (Ctrl+P), and Inspect (Ctrl+Shift+I). Below the URL is a 'Generate Token' button.

At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Slide 97 - Slide 97

Authentication Settings

Edit Identity Provider

Entity ID: zscalerone.net

Org-Specific Entity ID: Enabled

IdP SAML Certificate: okta.pem, Upload

IdP SAML Certificate Expiration Date: June 05, 2028

Vendor: Okta

Default IdP: Enabled

CRITERIA

Locations: Any

Authentication Domains: Any

SERVICE PROVIDER (SP) OPTIONS

Sign SAML Request:

Request Signing SSL Certificate: saml_1

SP SAML Certificate Expiration Date: October 11, 2020

SP Metadata: [Download Metadata](#)

SP SAML Certificate: [Download Certificate](#)

AUTO-PROVISIONING OPTIONS

Enable SAML Auto-Provisioning:

Enable SCIM-Based Provisioning:

Base URL: https://scim.zscalerone.net/8239192/scim (Deprecated)
https://scim.zscalerone.net/8239192760/scim

Bearer Token: AU/YyyBbNzygLS...
756jeYEnkBuwRKGGUOoA7IA==

Generate Token

Click Save

Cancel

Copyright © 2020 Zscaler Inc. All rights reserved. | Version 6.0 | [Products](#)

Help

Weblog Time: 5/12/2020 9:12:57 PM | Last Updated: 5/13/2020 3:12:08 PM

Slide notes

and click **Save**.

Slide 102 - Slide 102

The screenshot shows the Zscaler Authentication Settings interface. On the left is a dark sidebar with various icons: Dashboard, Analytics, Policy, Administration, Activation (which has a red notification badge), and Search. The main area is titled 'Authentication Settings' and has three tabs: 'AUTHENTICATION PROFILE' (selected), 'IDENTITY PROVIDERS' (with a 'NEW' button), and 'AUTHENTICATION BRIDGES'. Below these tabs is a table with one row. The columns are: No., ID, Name, Status, Location, IdP SAML Certificate Expiratio..., Authentication Domains, and Default IdP. The single row contains: No. 1, ID 760, Name Okta, Status Green (indicating active), Location Any, IdP SAML Certificate Expiration June 05, 2028, Authentication Domains Any, and Default IdP. A callout box with the text 'Click Activation' points to the 'Activation' link next to the Okta entry in the table.

No.	ID	Name	Status	Location	IdP SAML Certificate Expiratio...	Authentication Domains	Default IdP
1	760	Okta	Green	Any	June 05, 2028	Any	Okta

Slide notes

While you have saved the SAML configuration it is not yet live. Additionally, while the SCIM Bearer Token has been created it is not active until after you activate these changes. This is a critical step as the IdP will not be able to communicate with the Zscaler API until these changes have been activated.

Slide 103 - Slide 103

The screenshot shows the Zscaler Activation interface. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has tabs for 'CURRENTLY EDITING (1)' and 'AUTHENTICATION BRIDGES'. A table lists authentication providers. A tooltip 'Click Activation' points to the 'Force Activate' checkbox for the Okta row. The table columns are Name, Status, Location, IdP SAML Certificate Expiratio..., Authentication Domains, and Default IdP.

Name	Status	Location	IdP SAML Certificate Expiratio...	Authentication Domains	Default IdP
Okta	Green checkmark	Any	June 05, 2028	Any	Okta

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Help

Slide notes

Slide 107 - Slide 107

The screenshot shows the Okta interface for managing the Zscaler 2.0 application. At the top, there's a navigation bar with links for Dashboard, Directory, Applications, Security, Workflow, Reports, and Settings. The Applications section is active. Below the navigation is a search bar and a breadcrumb trail: Back to Applications > Zscaler 2.0. The main content area shows the Zscaler 2.0 application card with its logo, name, status (Active), and various management icons. Below the card, tabs for General, Sign On, Mobile, Provisioning, Import, Assignments, and Push Groups are visible, with 'Provisioning' being the selected tab. A large callout box highlights the 'Configure API Integration' button under the 'Integration' settings. The provisioning status is shown as 'Provisioning is not enabled' with a note about enabling it for account creation, deactivation, and updates. A 'Configure API Integration' button is located at the bottom of this section. At the very bottom of the page, there are links for 'Download Okta Plugin' and 'Feedback'.

Click Configure API Integration

Slide notes

Back in Okta you will need to enable their API Integration feature. Note that this will vary from vendor to vendor. Click **Configure API Integration**.

In your IdP you will now need to provide the Bearer Token and, in the case of Okta, the Zscaler Organization ID. Paste the Bearer Token you just copied into the API Token field.

Slide 108 - Slide 108

The screenshot shows the Okta Application Management interface for the Zscaler 2.0 application. The 'Provisioning' tab is selected. On the left, a sidebar shows 'SETTINGS' and 'Integration'. In the main area, there is a box titled 'Zscaler: Configuration Guide' with information about provisioning verification and partner-built integration. Below this is a section with a checkbox labeled 'Enable API integration' and a 'Save' button. A large callout box with the text 'Click Enable API Integration' points to the checkbox.

Slide notes

Then **Enable API Integration**.

Slide 109 - Slide 109

The screenshot shows the Okta application management interface. At the top, there's a search bar and navigation links for Dashboard, Directory, Applications, Security, Workflow, Reports, and Settings. The user is signed in as 'Admin_20'. Below the header, the 'Applications' section is visible, with 'Zscaler 2.0' selected. The main content area shows the 'Provisioning' tab selected. On the left, a sidebar titled 'SETTINGS' has 'Integration' selected. The main panel displays a configuration guide for Zscaler, stating 'Provisioning Verification: Okta Verified' and providing a link for partner support. A checkbox labeled 'Enable API integration' is checked. Below this, fields for 'Zscaler ID' and 'API Token' are present, along with a 'Test API Credentials' button and a 'Save' button. At the bottom of the page, there are footer links for © 2020 Okta, Inc., Privacy, Version 2020.04.2, OK7 Cell (US), Status site, Download Okta Plugin, and Feedback.

Slide notes

Then paste in the Organization ID / IdP ID combination you copied earlier and the Bearer Token. Note that Okta calls the Bearer Token the API Token.

Slide 110 - Slide 110

The screenshot shows the Okta application integration interface for the Zscaler 2.0 app. The top navigation bar includes links for Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, and Help and Support. The user is signed in as 'okta_Admin_20'. The main page displays the Zscaler 2.0 application card with options like Active, View Logs, and a 'View Details' button. Below the card, tabs for General, Sign On, Mobile, Provisioning, Import, Assignments, and Push Groups are visible, with 'Provisioning' selected. A 'SETTINGS' sidebar on the left has 'Integration' selected. The main content area shows a 'Zscaler: Configuration Guide' section with a note about provisioning verification and a link to contact support. A 'Cancel' button is present. Below this, there is a checkbox labeled 'Enable API integration' which is checked. A tooltip for the 'Test' button in the Zscaler ID field provides keyboard shortcuts for Undo (Ctrl+Z), Redo (Ctrl+Shift+Z), Cut (Ctrl+X), Copy (Ctrl+C), Paste (Ctrl+V), Paste as plain text (Ctrl+Shift+V), Select all (Ctrl+A), Spell check, Writing Direction, and Inspect. A 'Save' button is located at the bottom right of the input fields. At the bottom of the page, there are links for © 2020 Okta, Inc., Privacy, Version 2020.04.2, OK7 Cell (US), Status site, Download Okta Plugin, and Feedback.

Slide notes

Slide 111 - Slide 111

The screenshot shows the Okta application management interface. A modal window is open for the 'Zscaler 2.0' application, specifically for the 'Integration' settings. The modal title is 'Zscaler: Configuration Guide'. It contains a note about provisioning verification and a link to contact support. Below this, there is a checkbox labeled 'Enable API integration' which is checked. Underneath, fields for 'Zscaler ID' (containing '8239192/76') and 'API Token' are shown, along with a 'Test API Credentials' button and a 'Save' button. The background shows the main Okta dashboard with other application cards like 'Active', 'Logs', and 'View Logs'.

Slide notes

Slide 112 - Slide 112

The screenshot shows the Okta application management interface. A modal window is open for the 'Zscaler 2.0' application, specifically for the 'Integration' settings. The modal header says 'Zscaler: Configuration Guide'. It contains a note: 'Provisioning Verification: Okta Verified' and 'This provisioning integration is partner-built by Zscaler'. Below this, there's a link: 'Contact partner support: https://help.zscaler.com/zia/how-do-i-contact-zscaler-technical-assistance-center-ziac'. At the bottom right of the modal is a 'Cancel' button. Inside the main Okta page, there's a section for 'Enter your Zscaler 2.0 credentials to enable user import and provisioning features.' It includes fields for 'Zscaler ID' (containing '8239192/760') and 'API Token'. A context menu is open over the API Token field, showing options like 'Cut', 'Copy', 'Paste', 'Paste as plain text', 'Select all', 'Spell check', 'Writing Direction', and 'Inspect'. A 'Save' button is also visible in the menu. At the bottom of the page, there are links for '© 2020 Okta, Inc.', 'Privacy', 'Version 2020.04.2', 'OK7 Cell (US)', 'Status site', 'Upload Okta Plugin', and 'Feedback'.

Slide notes

Slide 113 - Slide 113

The screenshot shows the Okta application management interface. A modal window is open over the main content, specifically for the 'Zscaler 2.0' application. The modal title is 'Zscaler: Configuration Guide'. It contains a message stating 'Provisioning Verification: Okta Verified' and 'This provisioning integration is partner-built by Zscaler'. Below this, there is a link to 'Contact partner support: https://help.zscaler.com/zia/how-do-i-contact-zscaler-technical-assistance-center-ziac'. At the bottom right of the modal is a 'Cancel' button. Below the modal, in the main content area, there is a section titled 'SETTINGS' with a sub-section 'Integration'. Under 'Integration', there is a checkbox labeled 'Enable API integration' which is checked. Below this, there is a note: 'Enter your Zscaler 2.0 credentials to enable user import and provisioning features.' There are two input fields: 'Zscaler ID' containing '8239192/760' and 'API Token'. To the right of the 'API Token' field is a context menu with options: 'Cut' (Ctrl+X), 'Copy' (Ctrl+C), 'Paste' (Ctrl+V), 'Paste as plain text' (Ctrl+Shift+V), 'Select all' (Ctrl+A), 'Show all saved passwords', 'Spell check', 'Writing Direction', 'Inspect' (Ctrl+Shift+I), and a 'Save' button. At the bottom of the page, there is a footer with links: '© 2020 Okta, Inc.', 'Privacy', 'Version 2020.04.2', 'OK7 Cell (US)', 'Status site', 'Upload Okta Plugin', and 'Feedback'.

Slide notes

Slide 114 - Slide 114

The screenshot shows the Okta interface for managing the Zscaler 2.0 application. The top navigation bar includes 'Search people, apps', 'Dashboard', 'Directory', 'Applications', 'Security', 'Workflow', 'Reports', 'Settings', and 'My Apps'. The main content area displays the 'Zscaler 2.0' application card with options like 'Active', 'Edit', 'Logs', and 'View Logs'. Below the card, tabs for 'General', 'Sign On', 'Mobile', 'Provisioning', 'Import', 'Assignments', and 'Push Groups' are visible, with 'Provisioning' selected. A sidebar on the left shows 'SETTINGS' and 'Integration' is selected. The main panel contains a 'Zscaler: Configuration Guide' section with a note about provisioning verification and partner-built status. A 'Cancel' button is at the top right. Below this, there's a checkbox for 'Enable API integration' which is checked. A note says to enter Zscaler 2.0 credentials for user import and provisioning features. Fields for 'Zscaler ID' (containing '8239192/760') and 'API Token' (containing a redacted string) are shown. A 'Test API Credentials' button is highlighted with a callout bubble pointing to it. A 'Save' button is at the bottom right. The footer includes links for '© 2020 Okta, Inc.', 'Privacy', 'Version 2020.04.2', 'OK7 Cell (US)', 'Status site', 'Download Okta Plugin', and 'Feedback'.

Slide notes

Then click **Test API Credentials**. This will report back Success if Okta is able to communicate with Zscaler's API server for your Organization.

Slide 115 - Slide 115

The screenshot shows the Okta Integration Settings page for the Zscaler 2.0 application. The 'Integration' tab is selected under the SETTINGS section. A success message 'Zscaler 2.0 was verified successfully!' is displayed above the API token input fields. A callout bubble points to the green 'Click Box' button at the bottom right.

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

Zscaler 2.0 was verified successfully!

Enable API integration

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

Zscaler ID: 8239192760
API Token:

© 2020 Okta, Inc. Privacy Version 2020.04.2 OK7 Cell (US) Status site Download Okta Plugin Feedback

Slide notes

If the Success message is displayed, then click Save. If there is a failure go back to the Zscaler Admin Portal and be sure that the SAML configuration has been saved and Activated.

Slide 116 - Slide 116

The screenshot shows the Okta application management interface. A modal window is open over the main content, indicating a verification process. The main pane displays the 'Integration' settings for the 'Zscaler 2.0' application. It includes fields for 'Zscaler ID' (set to 8239192760) and 'API Token' (redacted). A 'Test API Credentials' button and a 'Save' button are at the bottom. The 'Import' tab is currently selected.

SETTINGS

Integration

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

Please wait while we verify your application setup...

Enable API integration

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

Zscaler ID: 8239192760

API Token:

Slide notes

Slide 117 - Slide 117

The screenshot shows the Zscaler Click Administration interface. On the left, there is a vertical sidebar with various icons and labels: Dashboard, Analytics, Policy, Click Administration (which is highlighted in blue), Activation, Search, and other smaller icons. The main content area is titled "Authentication Settings". At the top, there are three tabs: "AUTHENTICATION PROFILE" (selected), "IDENTITY PROVIDERS" (with a "NEW" button), and "AUTHENTICATION BRIDGES". Below the tabs, there is a table with one row. The columns are: No., ID, Name, Status, Location, IdP SAML Certificate Expiratio..., Authentication Domains, and Default IdP. The single row contains: No. 1, ID 760, Name Okta, Status Green (indicating OK), Location Any, IdP SAML Certificate Expiration June 05, 2028, Authentication Domains Any, and Default IdP. At the bottom of the main area, there are "Save" and "Cancel" buttons. A large callout box with a grey background and black text points to the "Click Administration" button on the sidebar. In the bottom right corner of the main area, there is a "Help" button.

Slide notes

Next, you will need to configure an Authentication Exemption to allow traffic destined to your IdP to pass even though the client has not yet been authenticated. This is required as, when authentication is enabled on a location, no user traffic is allowed to pass until the user has authenticated. Without the Authentication Exemption in place the authentication request itself would be unable to pass. Click **Administration**.

Slide 118 - Slide 118

The screenshot shows the Zscaler One Connect web interface. On the left, there is a navigation sidebar with various icons and sections: Dashboard, Analytics, Policy, Settings (selected), Account Management, My Profile, Company Profile, Alerts, Print All Policies, Cloud Configuration (selected), Nanolog Streaming Service, Advanced Settings (highlighted with a callout box containing the text 'Click Advanced Settings'), Virtual ZENS, ICAP Settings, Partner Integrations, SaaS Application Telemetry, Authentication (selected), Authentication Configuration, Authentication Settings (highlighted with a blue border), User Management, Identity Proxy Settings, Administration (selected), Activation, Search, Resources, Traffic Forwarding, Location Management, VPN Credentials, Hosted PAC Files, eZ Agent Configurations, SecureAgent Notifications, Firewall Filtering, Network Services, Network Applications, IP & FQDN Groups, PROXY CHAINING (NEW), Root Certificates, and Help.

On the right, there is a table titled 'APPLICATION BRIDGES' with columns: IdP SAML Certificate Expiration Date, Authentication Domains, Default IdP, and a header row. The table contains one row with the values: June 05, 2028, Any, and a blue circular icon.

At the bottom of the page, there is a footer bar with the URL <https://admin.zscaleone.net/#administration/my-profile>, the text 'Version 6.0 | Patents', and a timestamp 'Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM'.

Slide notes

Then Advanced Settings.

Slide 119 - Slide 119

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a title "Advanced Settings". It contains several sections: "ADMIN RANKING" (checkbox for "Enable Admin Ranking" is checked), "ADVANCED WEB APP CONTROL OPTIONS" (checkbox for "Allow Cascading to URL Filtering" is checked), "ADMIN UI SESSION TIMEOUT" (text input for "Session Timeout Duration (In Minutes)" is set to 600), "AUTHENTICATION EXEMPTIONS" (highlighted in blue), "SSL EXEMPTIONS", and "KERBEROS AUTHENTICATION EXEMPTION". Under "AUTHENTICATION EXEMPTIONS", there are dropdowns for "Exempted URL Categories" (set to "None") and "Exempted URLs" (input field with placeholder "Add Items" and a "Max: 25k Used: 0" note). There are also dropdowns for "Exempted Applications" (set to "None") and "Exempted URLs" (input field with placeholder "Add Items" and a "Max: 25k Used: 0" note). At the bottom are "Save" and "Cancel" buttons, and a "Help" link.

Slide notes

Under the Authentication Exemptions section, you can configure an exemption by URL Category, specific URL's, or by Application. You may configure specific URLs or by Application for a well known cloud hosted IdP such as Okta. Enter the Closed Caption Text

Slide 120 - Slide 120

The screenshot shows the 'Advanced Settings' page under the 'Administration' section of the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Activation, and Search.

ADMIN RANKING
Enable Admin Ranking:

ADVANCED WEB APP CONTROL OPTIONS
Allow Cascading to URL Filtering:

ADMIN UI SESSION TIMEOUT
Session Timeout Duration (In Minutes): 600

AUTHENTICATION EXEMPTIONS

- Exempted URL Categories: None
- Exempted URLs: Max: 25k Used: 0
Add Items
- Exempted Applications: None

SSL EXEMPTIONS
Override Zscaler Global SSL Exemptions List:

KERBEROS AUTHENTICATION EXEMPTION

- Exempted URL Categories: None
- Exempted URLs: Max: 25k Used: 0
Add Items

Buttons: Save, Cancel, Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

To manually exempt your IdP from authentication click in the Exempted URLs box, enter the required URL's, then click "Add Items". Be sure to check your IdP documentation for the required URL's.

Slide 121 - Slide 121

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Advanced Settings' and contains several sections:

- ADMIN RANKING**: A section with a toggle switch labeled 'Enable Admin Ranking'.
- ADVANCED WEB APP CONTROL OPTIONS**: A section with a toggle switch labeled 'Allow Cascading to URL Filtering'.
- ADMIN UI SESSION TIMEOUT**: A section where 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS**:
 - Exempted URL Categories**: A dropdown menu currently set to 'None'.
 - Exempted URLs**: A list containing '.okta.com'. An 'Add Items' button is available.
 - Exempted Applications**: A dropdown menu currently set to 'None'.
- SSL EXEMPTIONS**: A section with a toggle switch labeled 'Override Zscaler Global SSL Exemptions List'.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon. The footer includes copyright information and a timestamp: 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents' and 'Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM'.

Slide notes

In the case of Okta there are two URL's: .okta.com and .oktacdn.com.

Slide 122 - Slide 122

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration (selected), Activation, Search, and Help.

ADMIN RANKING
Enable Admin Ranking:

ADVANCED WEB APP CONTROL OPTIONS
Allow Cascading to URL Filtering:

ADMIN UI SESSION TIMEOUT
Session Timeout Duration (In Minutes): 600

AUTHENTICATION EXEMPTIONS

- Exempted URL Categories: None
- Exempted URLs: Max: 25k Used: 0
- Exempted Applications: None

SSL EXEMPTIONS
Override Zscaler Global SSL Exemptions List:

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

Slide 123 - Slide 123

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration (selected), Activation, Search, and Help.

ADMIN RANKING
Enable Admin Ranking:

ADVANCED WEB APP CONTROL OPTIONS
Allow Cascading to URL Filtering:

ADMIN UI SESSION TIMEOUT
Session Timeout Duration (In Minutes): 600

AUTHENTICATION EXEMPTIONS

- Exempted URL Categories: None
- Exempted URLs: Max: 25k Used: 0
Add Items
- Exempted Applications: None

SSL EXEMPTIONS
Override Zscaler Global SSL Exemptions List:

Save Cancel Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

Slide 124 - Slide 124

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Advanced Settings'.

- ADMIN RANKING:** 'Enable Admin Ranking' is turned off (unchecked).
- ADVANCED WEB APP CONTROL OPTIONS:** 'Allow Cascading to URL Filtering' is turned off (unchecked).
- ADMIN UI SESSION TIMEOUT:** 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS:**
 - 'Exempted URL Categories' dropdown is set to 'None'.
 - 'Exempted URLs' section shows a table with two entries: '.okta.com' and '.oktacdn.com'. A note says 'Max: 25k Used: 0'. Buttons for 'Add Items' and 'Remove' are present.
 - 'Exempted Applications' dropdown is set to 'None'.
- SSL EXEMPTIONS:** 'Override Zscaler Global SSL Exemptions List' is turned off (unchecked). Buttons for 'Save' and 'Cancel' are at the bottom.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Help

Slide notes

For this example, however, let's use the Exempted Applications list.

Slide 125 - Slide 125

The screenshot shows the 'Advanced Settings' page in the Zscaler interface. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area includes:

- ADMIN RANKING**: A section with a toggle switch labeled 'Enable Admin Ranking'.
- ADVANCED WEB APP CONTROL OPTIONS**: A section with a toggle switch labeled 'Allow Cascading to URL Filtering'.
- ADMIN UI SESSION TIMEOUT**: A section where 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS**:
 - Exempted URL Categories**: A dropdown menu showing 'None'.
 - Exempted URLs**: A table with a search bar and a 'Max: 25k Used: 0' note. It lists '.okta.com' and '.oktacdn.com' with remove buttons.
 - Exempted Applications**: A dropdown menu showing 'None'.
- SSL EXEMPTIONS**: A section with a toggle switch labeled 'Override Zscaler Global SSL Exemptions List'.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' link. Copyright and version information are at the very bottom.

Slide notes

Slide 126 - Slide 126

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search.

ADMIN RANKING
Enable Admin Ranking:

ADVANCED WEB APP CONTROL OPTIONS
Allow Cascading to URL Filtering:

ADMIN UI SESSION TIMEOUT
Session Timeout Duration (In Minutes): 600

AUTHENTICATION EXEMPTIONS
Exempted URL Categories: None
Exempted URLs: Max: 25k Used: 0
Add Items:
Search...
.okta.com
.oktacdn.com
1-2 of 2 / 1 > Remove ^
Remove 25K Items
Remove Page
Exempted Applications: None

SSL EXEMPTIONS
Override Zscaler Global SSL Exemptions List:
Save Cancel Help

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents
Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

Slide 127 - Slide 127

The screenshot shows the Zscaler Admin UI with the 'Advanced Settings' tab selected. On the left, there's a sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has several sections:

- ADMIN RANKING**: A toggle switch labeled "Enable Admin Ranking" is turned off.
- ADVANCED WEB APP CONTROL OPTIONS**: A toggle switch labeled "Allow Cascading to URL Filtering" is turned off.
- ADMIN UI SESSION TIMEOUT**: A field labeled "Session Timeout Duration (In Minutes)" is set to 600.
- AUTHENTICATION EXEMPTIONS**:
 - "Exempted URL Categories": A dropdown menu showing "None".
 - "Exempted URLs": A table with two entries: "okta.com" and "oktaadr.com". Each entry has a delete icon (X) next to it. Below the table are buttons for "Add items", "Search...", and "Remove".
- SSL EXEMPTIONS**: A section titled "Override Zscaler Global SSL Exemptions List" with a toggle switch turned off. It includes "Save" and "Cancel" buttons and a "Help" link.

A modal dialog box titled "Confirmation: Remove Page" is displayed in the center. It contains the message: "Please confirm that you want to remove all 2 items on page 1 of this list. This action cannot be undone." with "Confirm" and "Cancel" buttons.

At the bottom of the page, there are copyright notices: "Copyright 2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Policies" and "Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM".

Slide notes

Slide 128 - Slide 128

The screenshot shows the Zscaler Admin UI with the 'Advanced Settings' page open. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has several sections: 'ADMIN RANKING' (checkbox for 'Enable Admin Ranking'), 'ADVANCED WEB APP CONTROL OPTIONS' (checkbox for 'Allow Cascading to URL Filtering'), 'ADMIN UI SESSION TIMEOUT' (input field set to 600), 'AUTHENTICATION EXEMPTIONS' (dropdown set to 'None'), 'SSL EXEMPTIONS' (checkbox for 'Override Zscaler Global SSL Exemptions List'), 'KERBEROS AUTHENTICATION EXEMPTION' (dropdown set to 'None'), and 'Exempted URLs' (input field set to 'Max: 25k Used: 0'). At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon. A callout box with the text 'Click Exempted Applications drop-down' points to the 'Exempted Applications' dropdown in the SSL Exemptions section.

Slide notes

To add an exemption by application, click the **Exempted Applications** drop-down.

Slide 130 - Slide 130

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Advanced Settings". It contains several sections: "ADMIN RANKING" (Enable Admin Ranking is off), "ADVANCED WEB APP CONTROL OPTIONS" (Allow Cascading to URL Filtering is off), "ADMIN UI SESSION TIMEOUT" (Session Timeout Duration is set to 600 minutes), and "AUTHENTICATION EXEMPTIONS". Under "Exempted URL Categories", there is a dropdown set to "None". Under "Exempted URLs", there is a text input field containing "Add Items" and a button labeled "Add Items". Under "Exempted Applications", there is a dropdown set to "None". A search modal is open, showing a list of applications under the heading "Unselected Items". The list includes "okta" (which is selected), "Collaboration and Online Meetings" (which is expanded), and other items like "Acrobat Connect", "Active Collaboration", "Asana", "Google Calendar", and "Google Jamboard". At the bottom of the modal are "Done", "Cancel", and "Clear Selection" buttons. The status bar at the bottom of the screen shows "Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents" and "Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM".

Slide notes

Then search for and select Okta.

Slide 131 - Slide 131

The screenshot shows the Zscaler Admin UI with the 'Administration' tab selected. The main panel displays the 'Advanced Settings' configuration page. Key sections include:

- ADMIN RANKING:** A toggle switch labeled 'Enable Admin Ranking' is turned off.
- ADVANCED WEB APP CONTROL OPTIONS:** A toggle switch labeled 'Allow Cascading to URL Filtering' is turned off.
- ADMIN UI SESSION TIMEOUT:** A field labeled 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS:**
 - Exempted URL Categories:** A dropdown menu is set to 'None'.
 - Exempted URLs:** A list box shows 'Add Items' and 'Add Items' buttons. A tooltip indicates a max of 25k used items.
 - Exempted Applications:** A list box titled 'Unselected Items' shows entries like 'okta', 'IT Services', and 'ClickBox'. A callout box with the text 'Click Okta' points to the 'okta' entry. Other buttons include 'Selected Items (0)', 'Clear Selection', and a 'Help' button.

At the bottom of the page, copyright information reads 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents' and a timestamp says 'Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM'.

Slide notes

Slide 132 - Slide 132

The screenshot shows the Zscaler Admin UI with the 'Advanced Settings' page open. On the left, there is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has several sections: 'ADMIN RANKING' (Enable Admin Ranking is off), 'ADVANCED WEB APP CONTROL OPTIONS' (Allow Cascading to URL Filtering is off), 'ADMIN UI SESSION TIMEOUT' (Session Timeout Duration is set to 600 minutes), and 'AUTHENTICATION EXEMPTIONS'. Under 'Exempted URL Categories', it says 'None'. Under 'Exempted URLs', there is a text input field with 'Add Items' and a button 'Add Items'. Under 'Exempted Applications', it says 'None'. A modal dialog is open, showing a list of applications: 'okta' (selected) and 'IT Services'. A speech bubble points to the 'Click Done' button at the bottom of the modal. The footer of the page includes copyright information (Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents) and a timestamp (Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM).

Slide notes

Then click **Done**.

Slide 133 - Slide 133

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area contains several sections:

- ADMIN RANKING**: A toggle switch labeled 'Enable Admin Ranking' is turned off.
- ADVANCED WEB APP CONTROL OPTIONS**: A toggle switch labeled 'Allow Cascading to URL Filtering' is turned off.
- ADMIN UI SESSION TIMEOUT**: A text input field for 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS**:
 - Exempted URL Categories**: A dropdown menu showing 'None'.
 - Exempted URLs**: A list box with a placeholder 'Add Items' and a note 'Max: 25k Used: 0'. A blue 'Add Items' button is visible.
 - Exempted Applications**: A dropdown menu showing 'Okta'.
- SSL EXEMPTIONS**: A toggle switch labeled 'Override Zscaler Global SSL Exemptions List' is turned off.
- KERBEROS AUTHENTICATION EXEMPTION**:
 - Exempted URL Categories**: A dropdown menu showing 'None'.
 - Exempted URLs**: A list box with a placeholder 'Add Items' and a note 'Max: 25k Used: 0'. A blue 'Add Items' button is visible.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

Click Save.

Slide 139 - Slide 139

The screenshot shows the Zscaler Activation interface. The left sidebar contains navigation links: Dashboard, Analytics, Policy, Administration, Activation (which is selected and highlighted in blue), and Search. The main content area is titled "Activation" and shows the following sections:

- MY ACTIVATION STATUS:** Shows "Editing" status and a URL "http://training02.usenrich.com".
- CURRENTLY EDITING (1):** Shows "http://training02.usenrich.com".
- QUEUED ACTIVATIONS (0):** Shows "None".
- OPTIONS:** Includes a checkbox for "Force Activate" and a large blue "Activate" button.
- Activation Timeout (in minutes):** A dropdown menu currently set to "10".
- Activation Items:** A section with a progress bar at 0% completion, labeled "Max: 25k Used: 0", and a blue "Add Items" button.
- Activation Exemptions:** A section with a progress bar at 0% completion, labeled "Max: 25k Used: 0".

At the bottom of the screen, there is a footer with copyright information: "Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents" and a timestamp: "Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM". A "Help" button is located in the bottom right corner.

Slide notes

Slide 140 - Slide 140

The screenshot shows the 'Advanced Settings' configuration page. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration (selected), Activation, and Search. The main content area displays several sections:

- ADMIN RANKING**: A toggle switch labeled 'Enable Admin Ranking' is turned off.
- ADVANCED WEB APP CONTROL OPTIONS**: A toggle switch labeled 'Allow Cascading to URL Filtering' is turned off.
- ADMIN UI SESSION TIMEOUT**: A text input field for 'Session Timeout Duration (In Minutes)' contains the value '600'.
- AUTHENTICATION EXEMPTIONS**:
 - Exempted URL Categories**: A dropdown menu set to 'None'.
 - Exempted URLs**: A list box with a placeholder 'Add Items' and a note 'Max: 25k Used: 0'. It contains one item: 'Okta'.
- SSL EXEMPTIONS**: A toggle switch labeled 'Override Zscaler Global SSL Exemptions List' is turned off.
- KERBEROS AUTHENTICATION EXEMPTION**:
 - Exempted URL Categories**: A dropdown menu set to 'None'.
 - Exempted URLs**: A list box with a placeholder 'Add Items' and a note 'Max: 25k Used: 0'. It contains one item: 'Okta'.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

Slide 141 - Slide 141

The screenshot shows the 'Advanced Settings' configuration page. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a header 'Activation Completed!' with a close button. It contains several sections:

- ADMIN RANKING**: A toggle switch labeled 'Enable Admin Ranking' is turned off.
- ADVANCED WEB APP CONTROL OPTIONS**: A toggle switch labeled 'Allow Cascading to URL Filtering' is turned off.
- ADMIN UI SESSION TIMEOUT**: A text input field for 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS**:
 - Exempted URL Categories**: A dropdown menu is set to 'None'.
 - Exempted URLs**: A text input field shows 'Max: 25k Used: 0'. Below it are two buttons: 'Add Items' (highlighted in blue) and 'Add Items'.
 - Exempted Applications**: A dropdown menu is set to 'Okta'.
- SSL EXEMPTIONS**: A toggle switch labeled 'Override Zscaler Global SSL Exemptions List' is turned off.
- KERBEROS AUTHENTICATION EXEMPTION**:
 - Exempted URL Categories**: A dropdown menu is set to 'None'.
 - Exempted URLs**: A text input field shows 'Max: 25k Used: 0'.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon. The footer includes copyright information and a timestamp: 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents' and 'Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM'.

Slide notes

Slide 142 - Slide 142

The screenshot shows the 'Advanced Settings' page in the Zscaler Admin UI. The left sidebar has icons for Dashboard, Analytics, Policy, Administration (selected), Activation, and Search. The main content area contains several sections:

- ADMIN RANKING**: A toggle switch labeled 'Enable Admin Ranking' is turned off.
- ADVANCED WEB APP CONTROL OPTIONS**: A toggle switch labeled 'Allow Cascading to URL Filtering' is turned off.
- ADMIN UI SESSION TIMEOUT**: A text input field for 'Session Timeout Duration (In Minutes)' is set to 600.
- AUTHENTICATION EXEMPTIONS**:
 - Exempted URL Categories**: A dropdown menu is set to 'None'.
 - Exempted URLs**: A text input field shows 'Max: 25k Used: 0'. Below it are 'Add Items' and 'Add Items' buttons.
 - Exempted Applications**: A dropdown menu is set to 'Okta'.
- SSL EXEMPTIONS**: A toggle switch labeled 'Override Zscaler Global SSL Exemptions List' is turned off.
- KERBEROS AUTHENTICATION EXEMPTION**:
 - Exempted URL Categories**: A dropdown menu is set to 'None'.
 - Exempted URLs**: A text input field shows 'Max: 25k Used: 0'.

At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents

Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM

Slide notes

At this point you can now verify that SCIM is active and is importing users via the API by checking the User Database under Administration then **User Database**.

Slide 143 - Slide 143

The screenshot shows the Zscaler One Connect Administration interface. The left sidebar contains navigation links for Settings, Account Management, Cloud Configuration, Analytics, Policy, Administration, Activation, and Search. The main content area is titled "Nolog Streaming Service" and "Advanced Settings". It includes sections for URL Categories, Bandwidth Classes, Time Intervals, and End User Notifications. A note indicates "Max: 25k Used: 0" and a blue "Add Items" button. The bottom right corner features a "Help" icon.

Slide notes

Slide 144 - Slide 144

The screenshot shows the Zscaler User Management interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "User Management" and contains a table of users. The table has columns: No., User ID or Name, User Display Name, Groups, Department, and Comments. There are four rows of data:

No.	User ID or Name	User Display Name	Groups	Department	Comments
1	admin@8239192.zscalerone.net	DEFAULT ADMIN	Service Admin	Service Admin	---
2	admin@training20.safemarch.com	DEFAULT ADMIN (Deprecated)	Service Admin	Service Admin	---
3	marketinguser@training20.safemarch.com	marketinguser test	Marketing	---	---
4	student@training20.safemarch.com	student test	Marketing	---	---

At the bottom of the page, there is a copyright notice: "Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 6.0 | Patents". To the right of the notice is a timestamp: "Weblog Time: 5/12/2020 3:12:37 PM | Last Updated: 5/12/2020 3:12:38 PM". A "Help" button is located at the bottom right.

Slide notes

You can see that two accounts have been added by the IdP via SCIM and their Group membership has also been added. Note that the time it takes for the IdP to send the user information varies from IdP to IdP and ranges between 5 to 30 minutes. Be sure to check your IdP's documentation for their update intervals.

Slide 145 - Thank You and Quiz



Thank You and Quiz

Slide notes

Thank you for participating in this eLearning module on configuring SAML with Zscaler.

What will follow is a short quiz to test your knowledge. You can re-take the quiz as many times as necessary to pass.