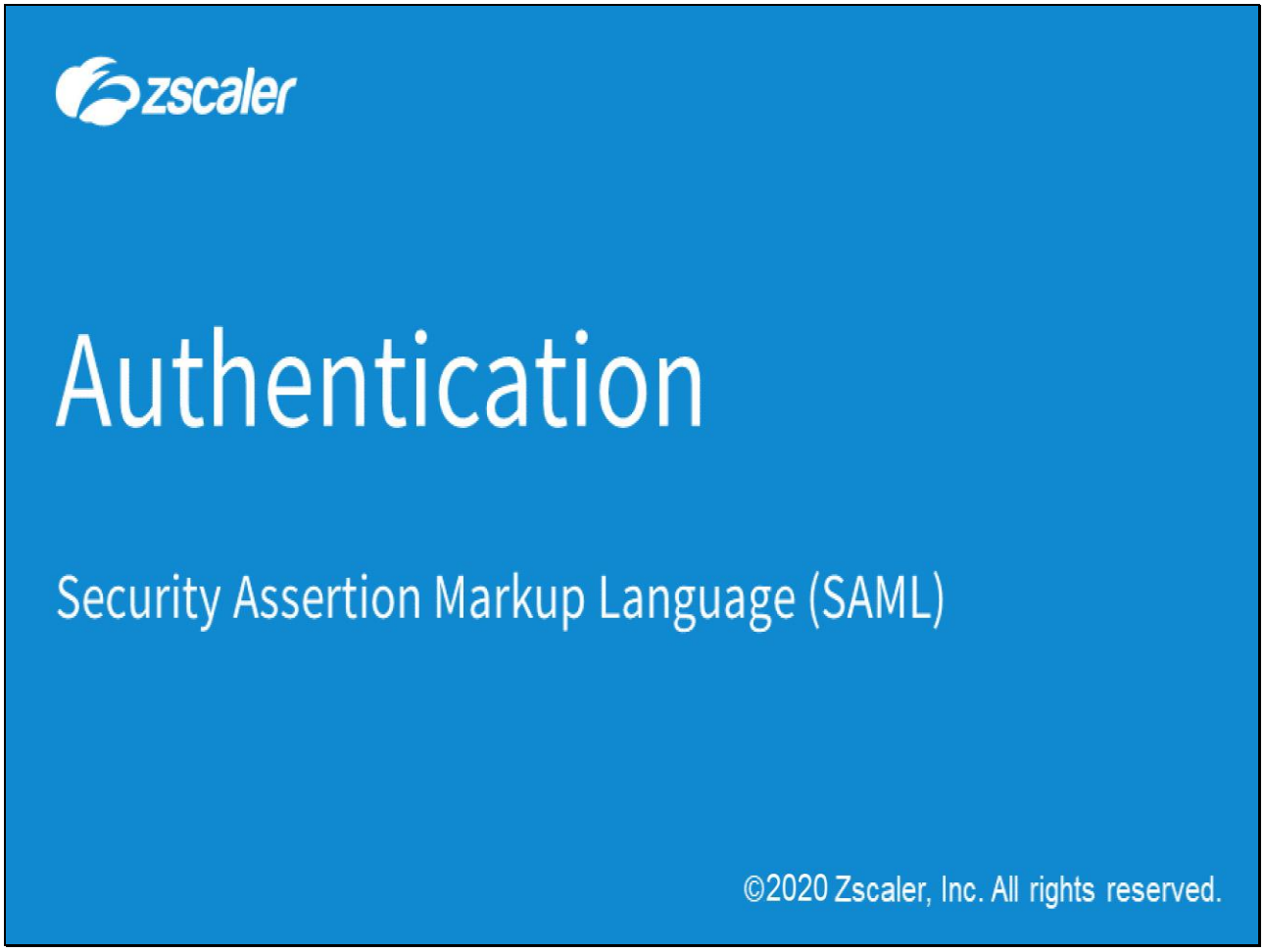
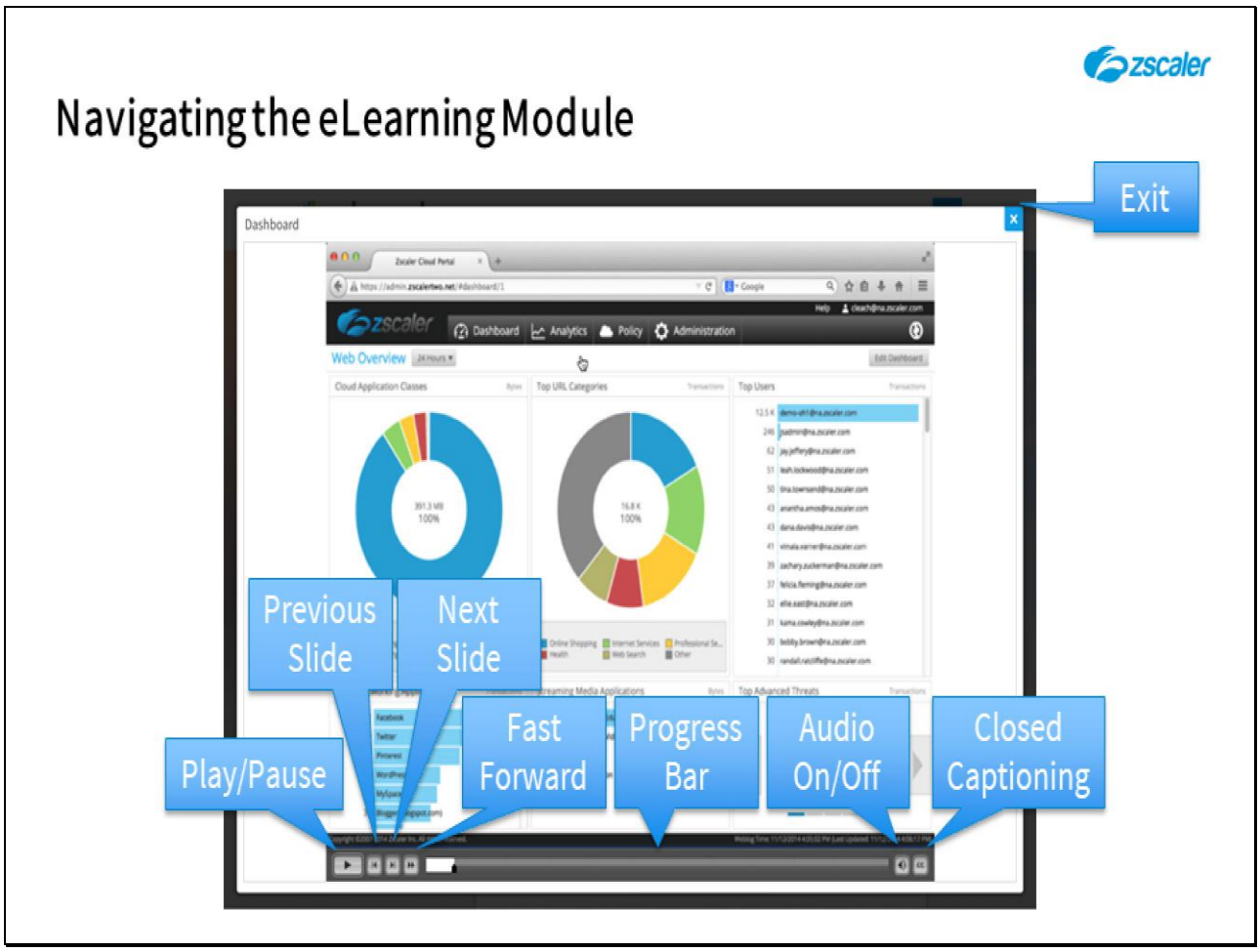
Slide 1 - ZCCP-IA



Slide notes

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

Slide 2 - Navigating the eLearning Module

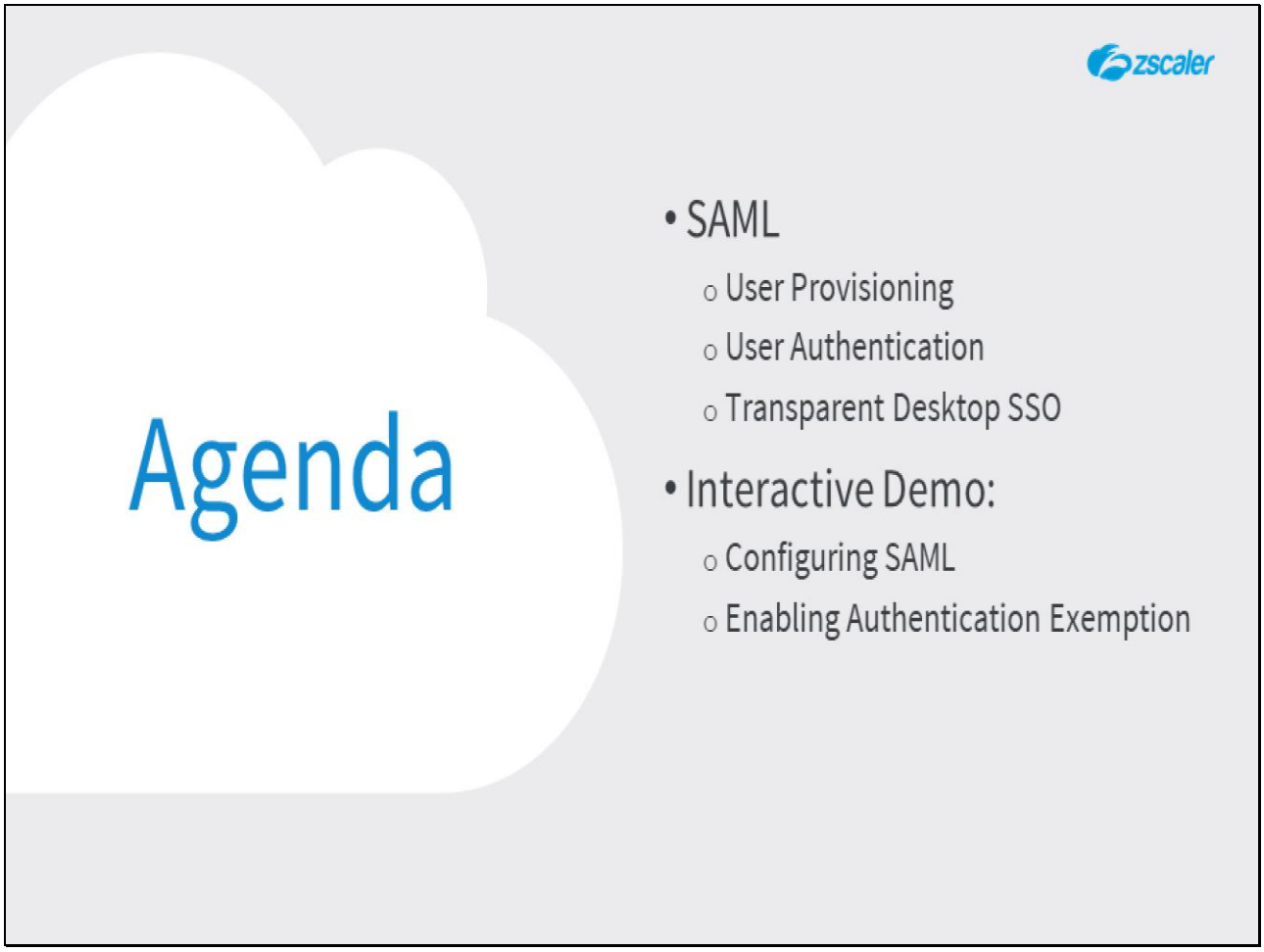


Slide notes

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

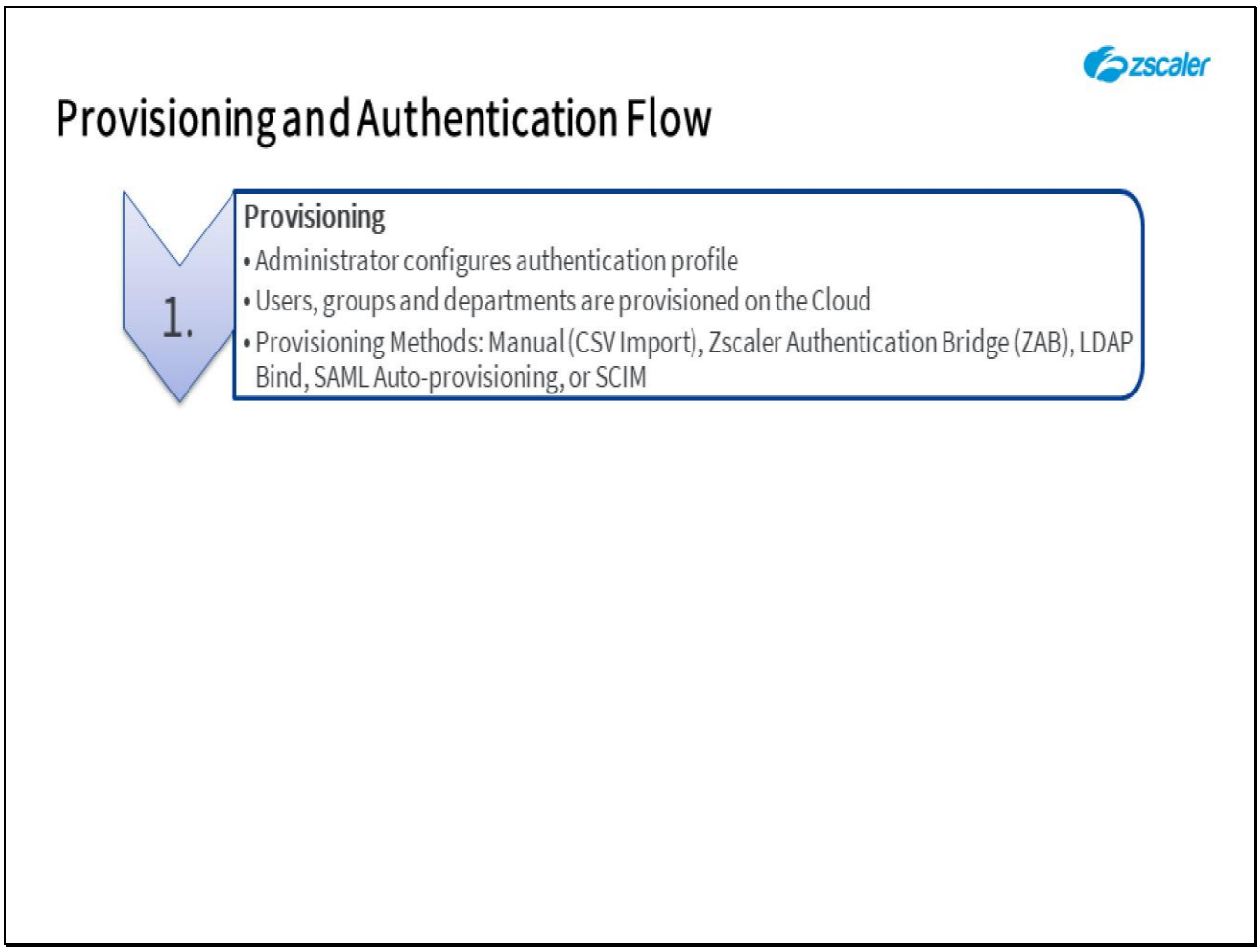
(Security Assertion Markup Language)



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.

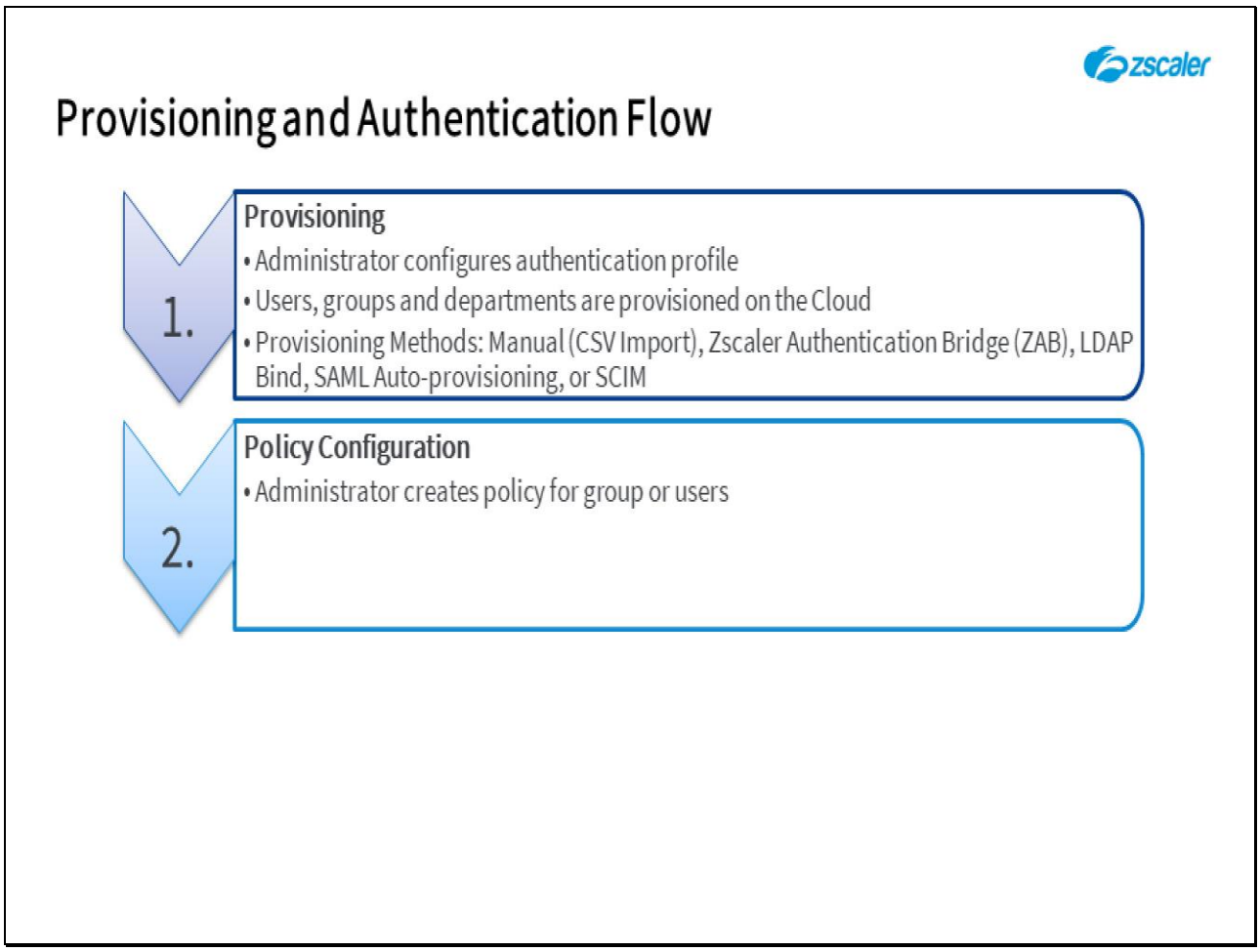
Slide 4 - Provisioning and Authentication Flow



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



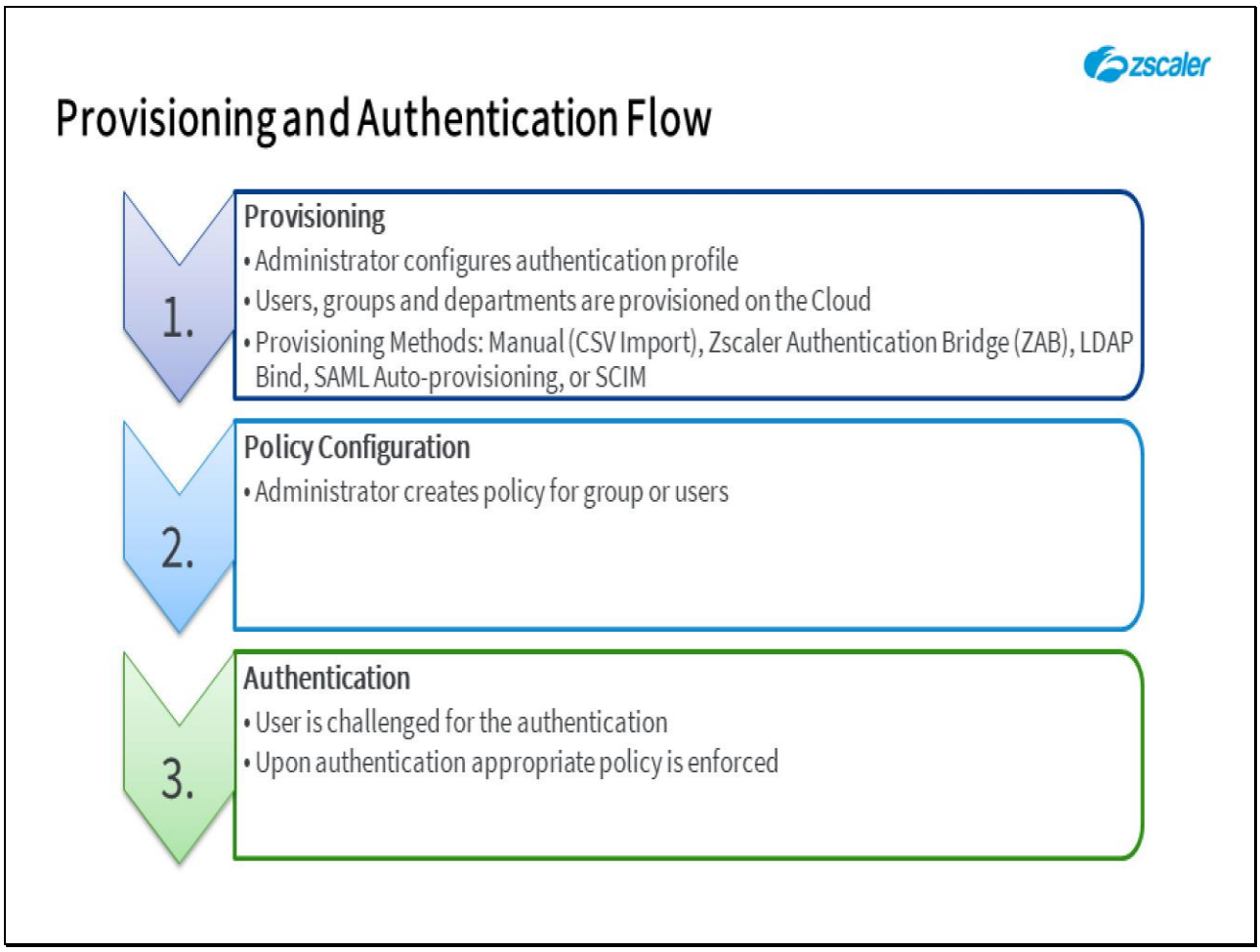
Slide notes

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

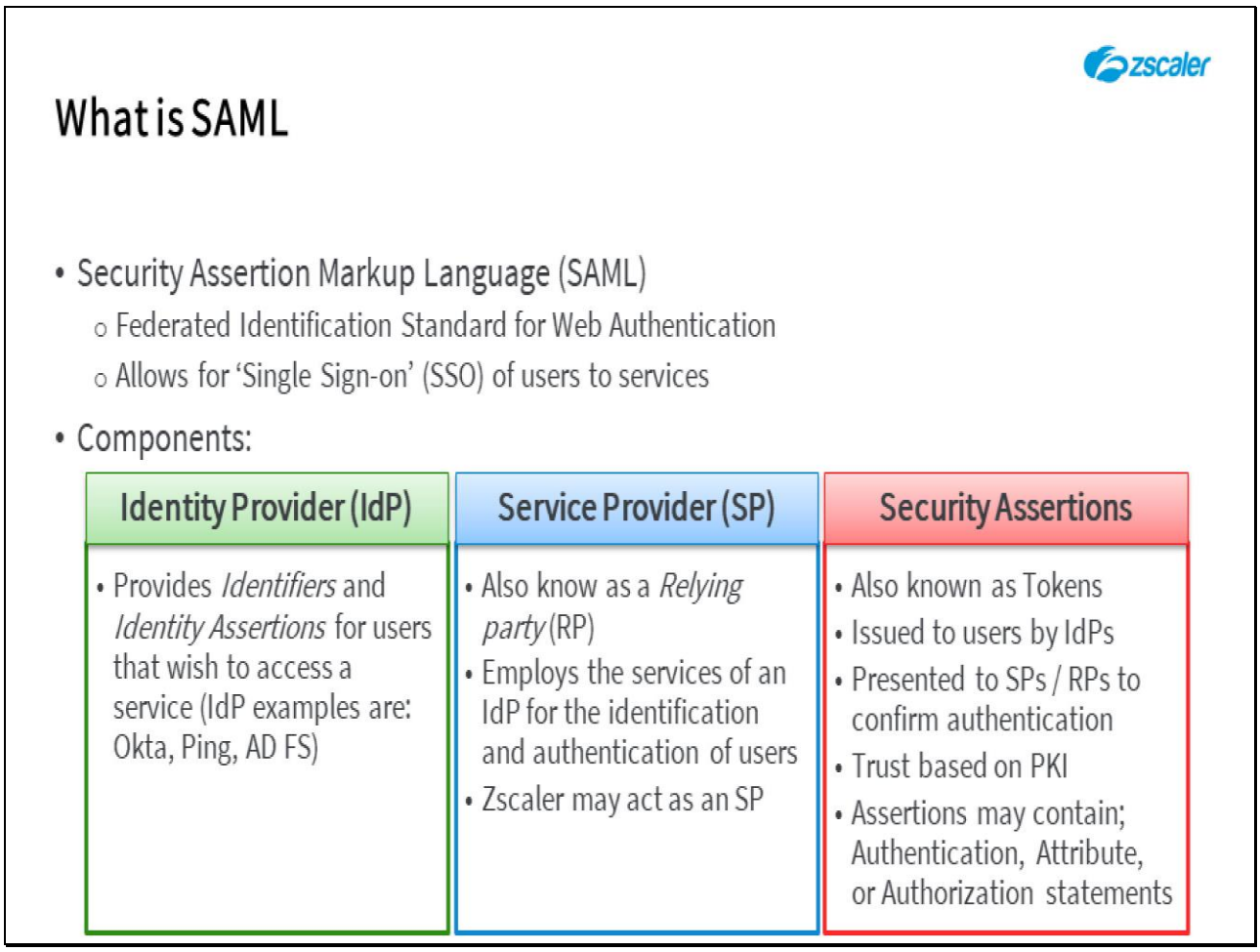
When the user is authenticated the system sees the policy that has been assigned to the user, either directly or via a group, which then determines access privileges.

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



Slide notes

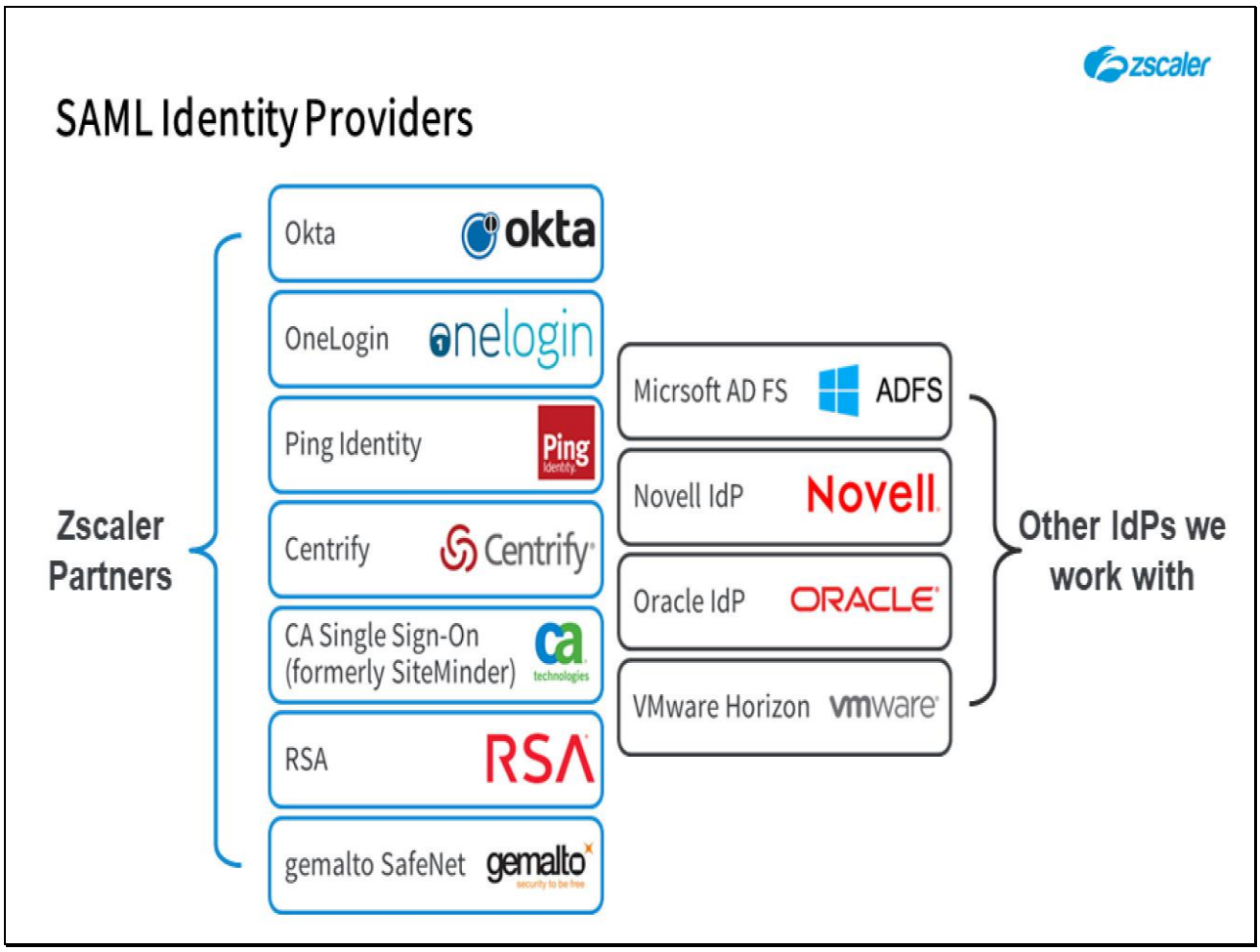
SAML, or Security Assertion Markup Language, is used to provide for single sign-on for users to multiple cloud applications. The user signs-in once and is then automatically signed in to other cloud applications the user subscribes to, such as Salesforce, or Box.

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.

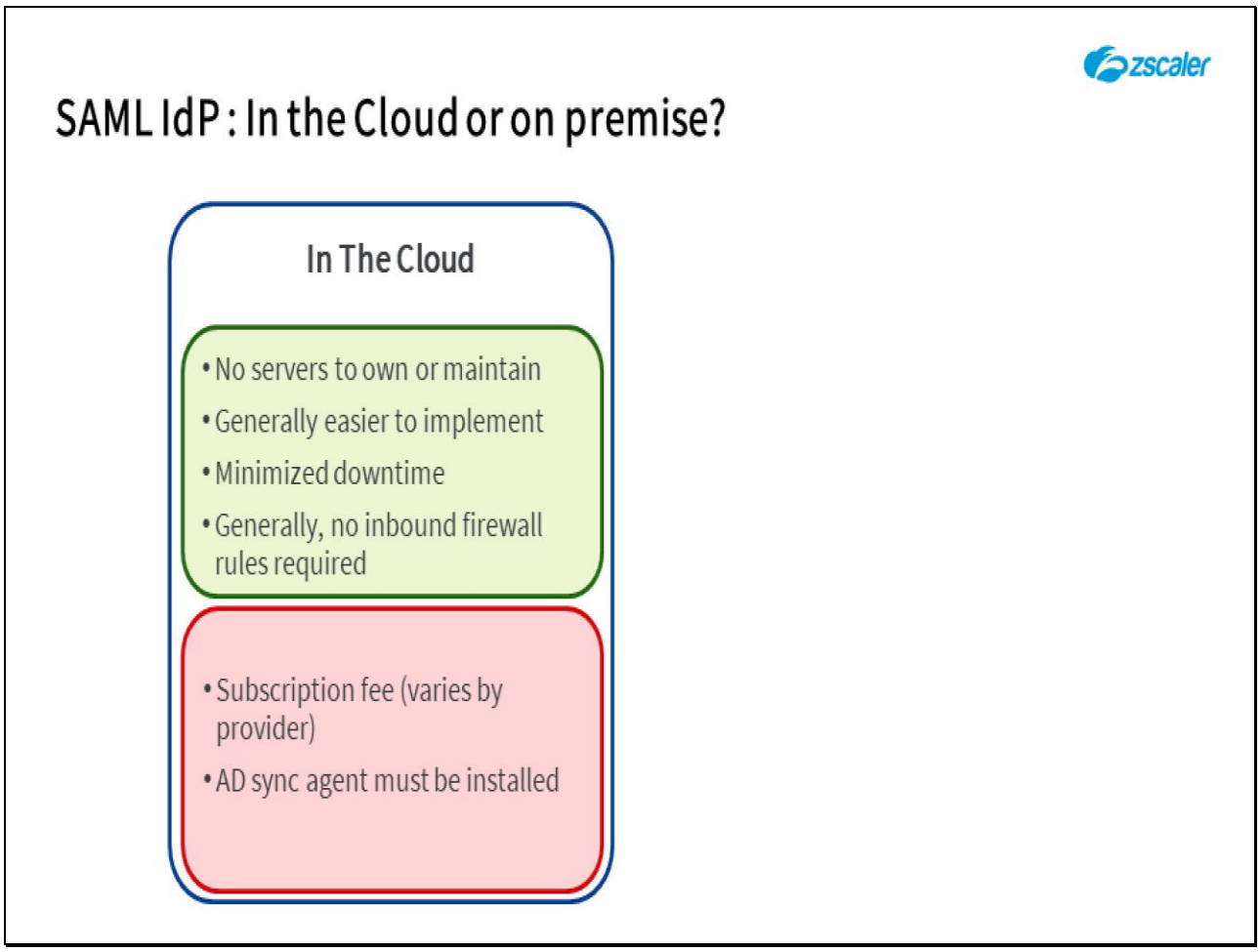
Slide 9 - SAML Identity Providers



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?



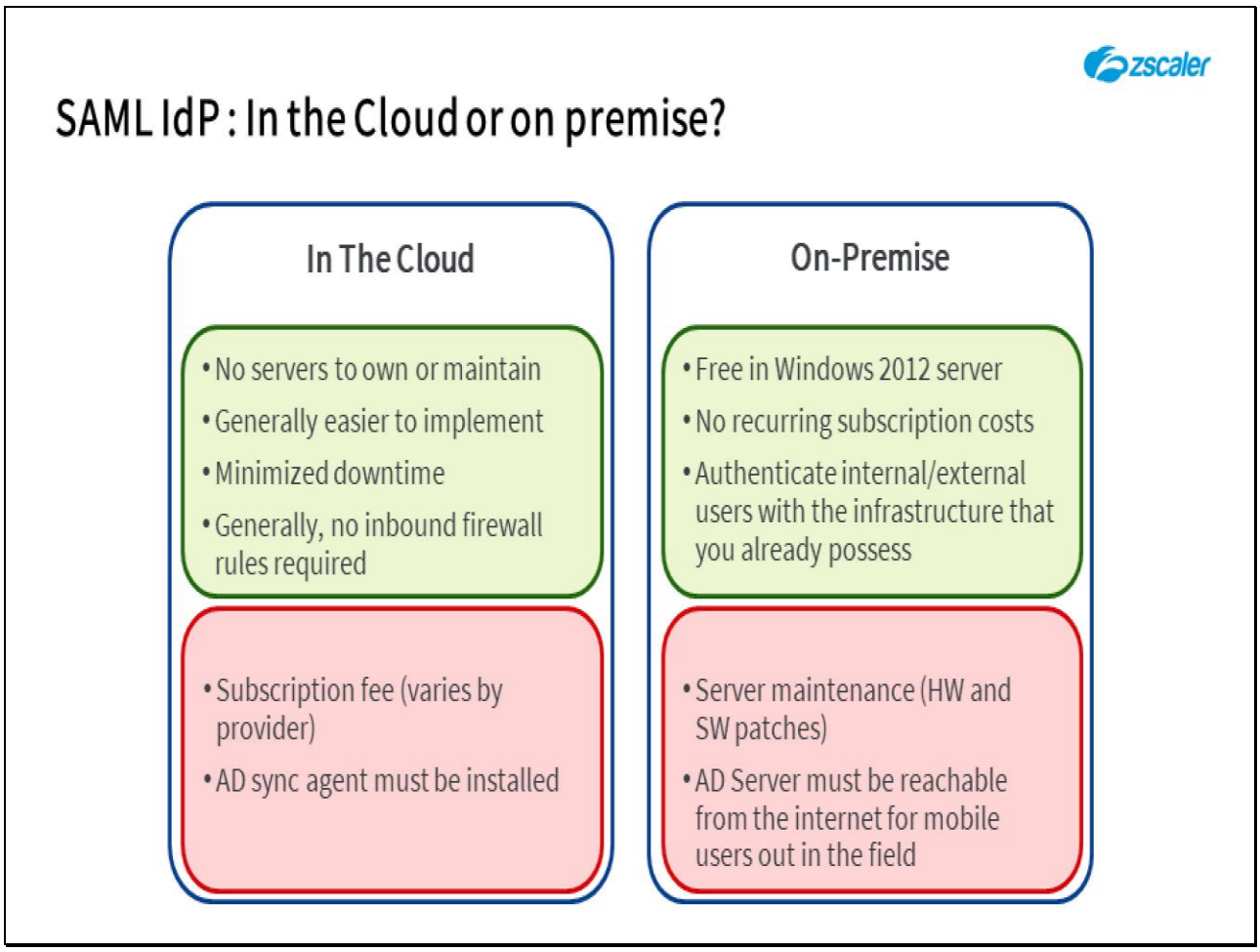
Slide notes

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.

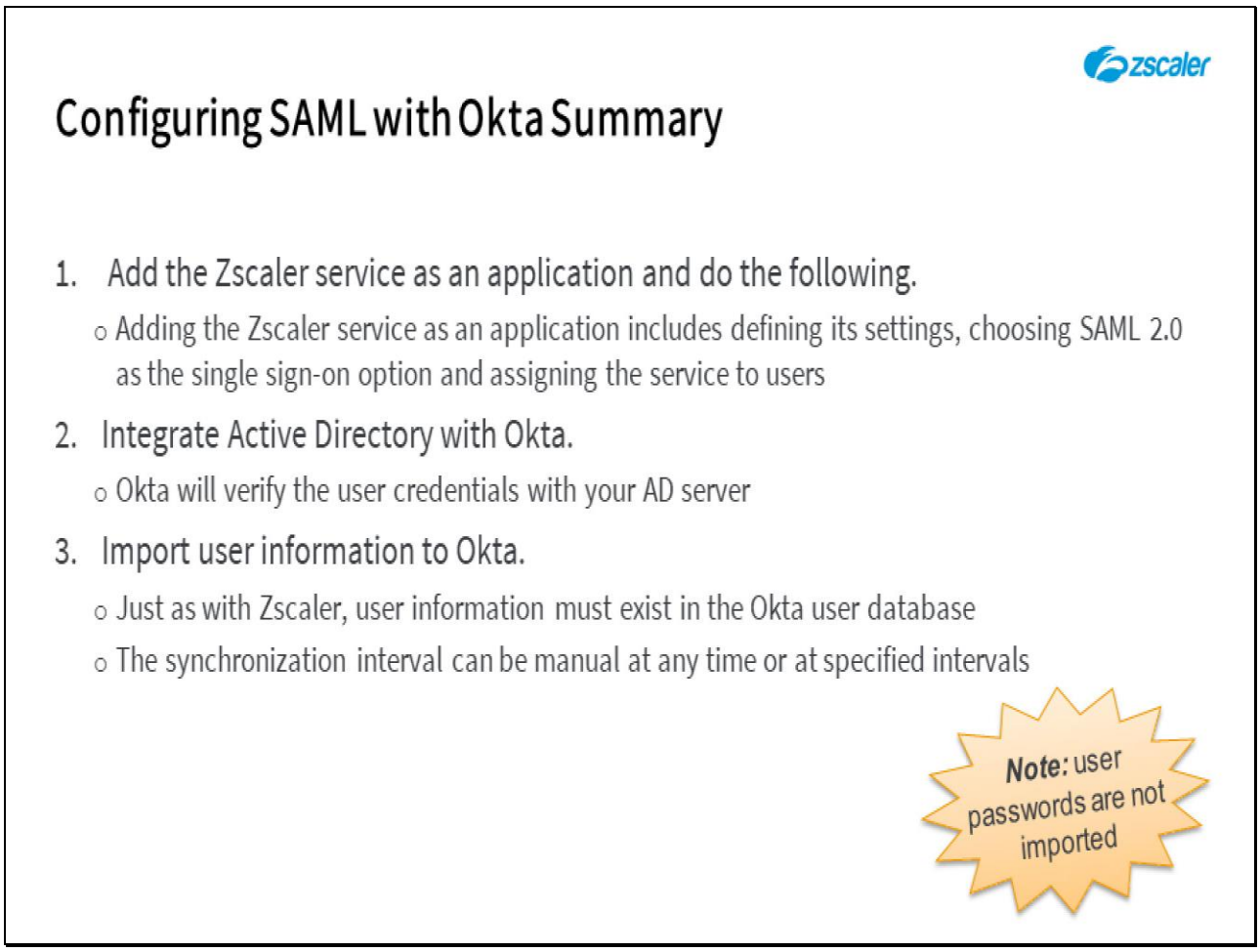
Slide 11 - SAML IdP : In the Cloud or on premise?



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

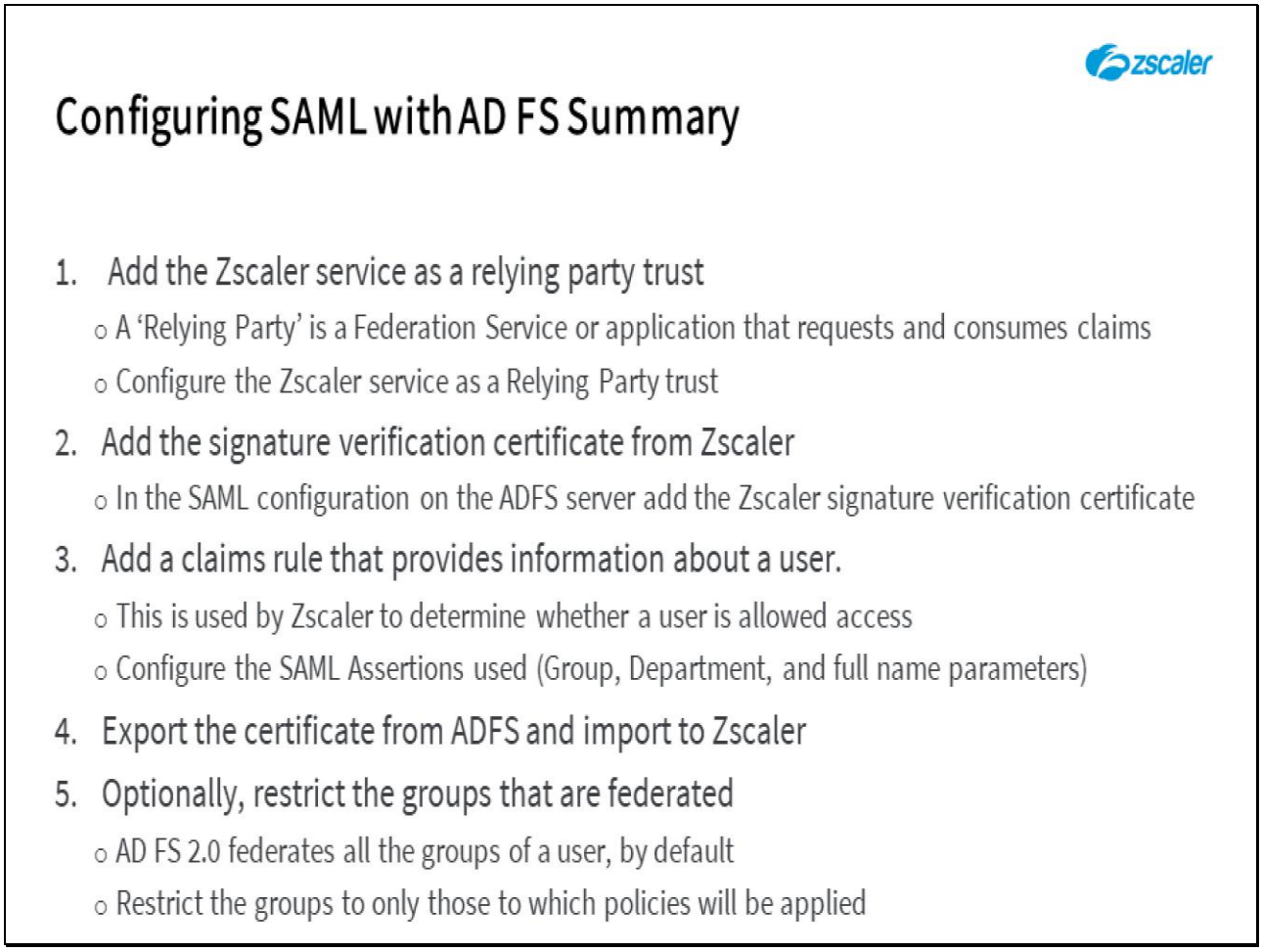


Slide notes

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.

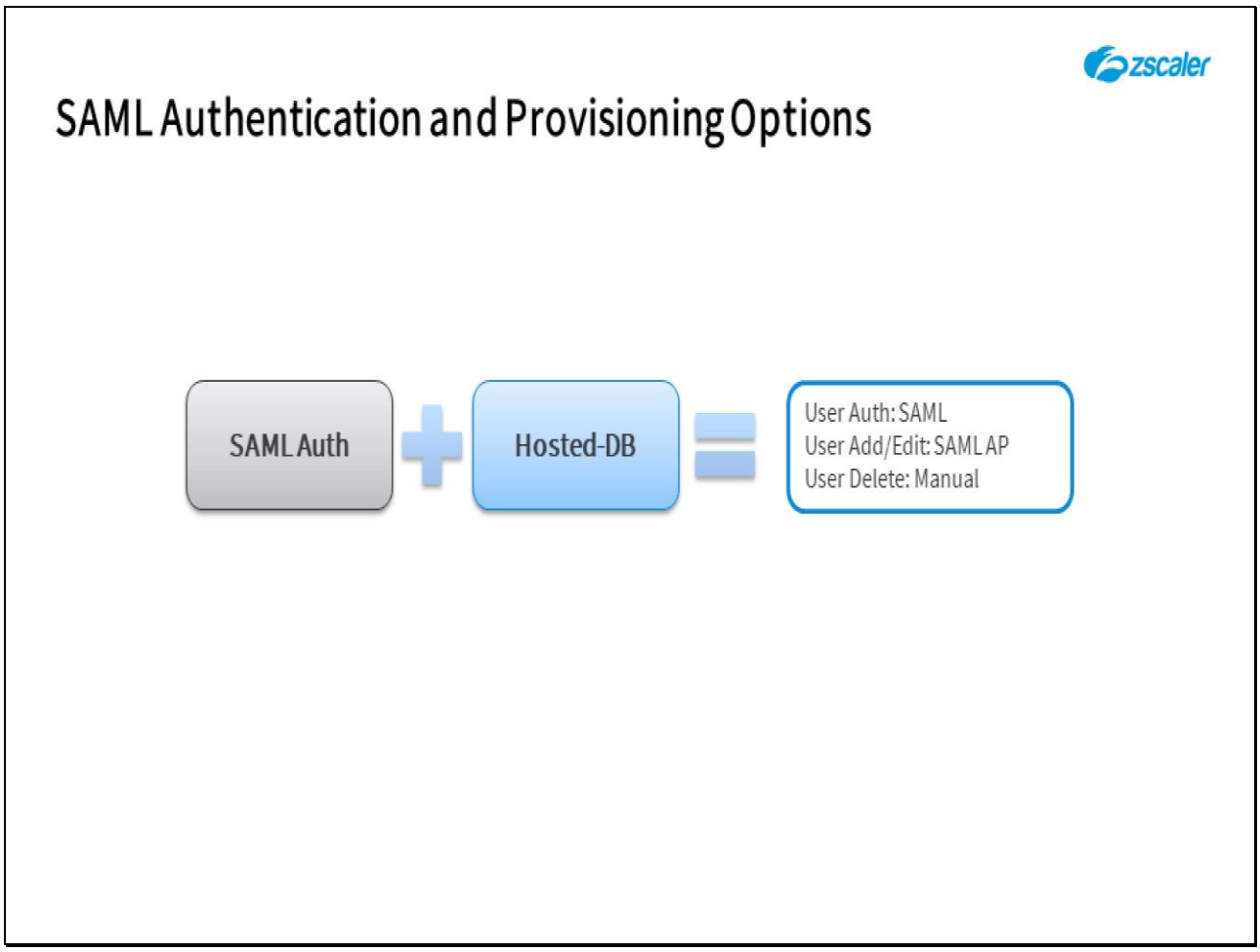
Slide 13 - Configuring SAML with AD FS Summary



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.

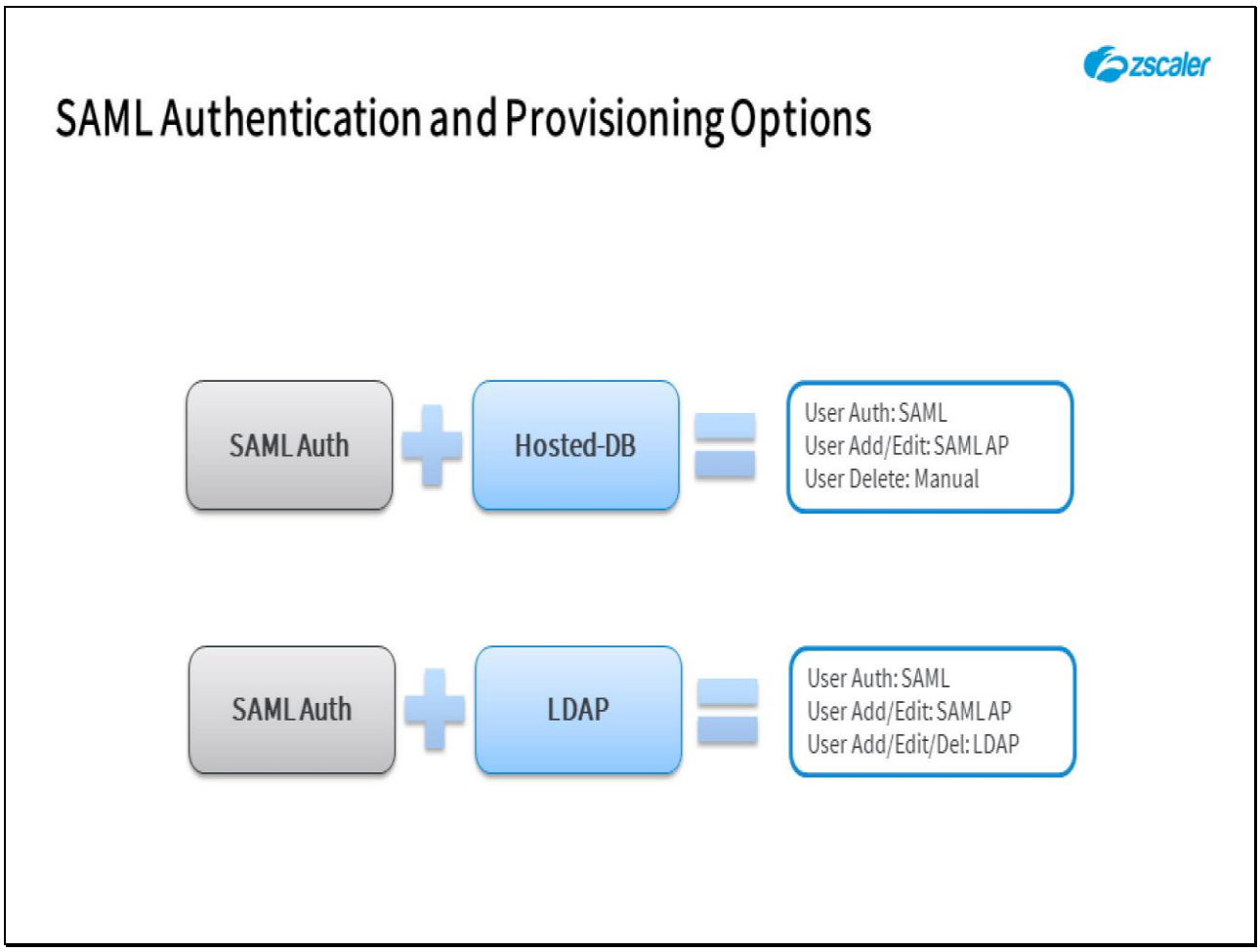
Slide 14 - SAML Authentication and Provisioning Options



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.

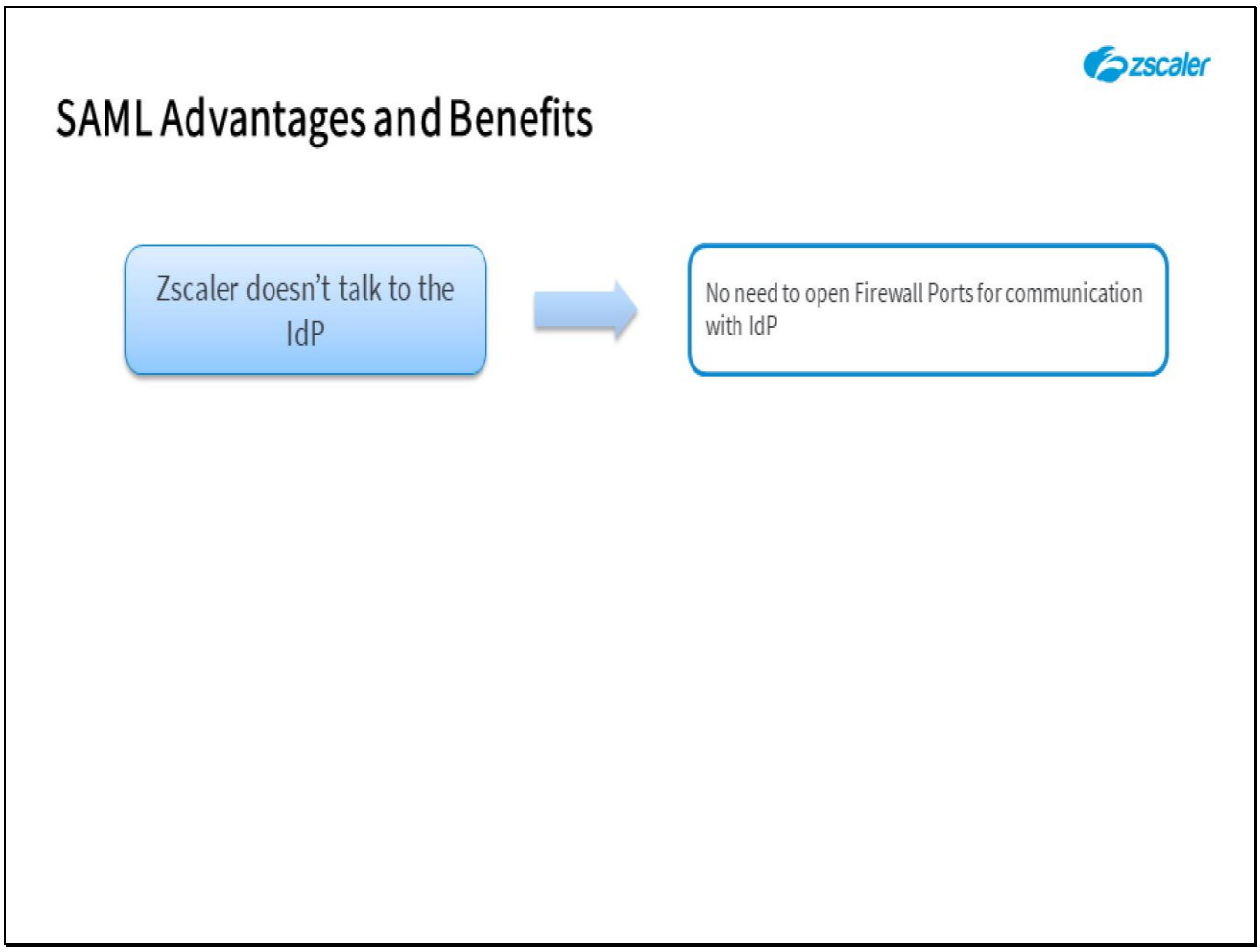
Slide 15 - SAML Authentication and Provisioning Options



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.

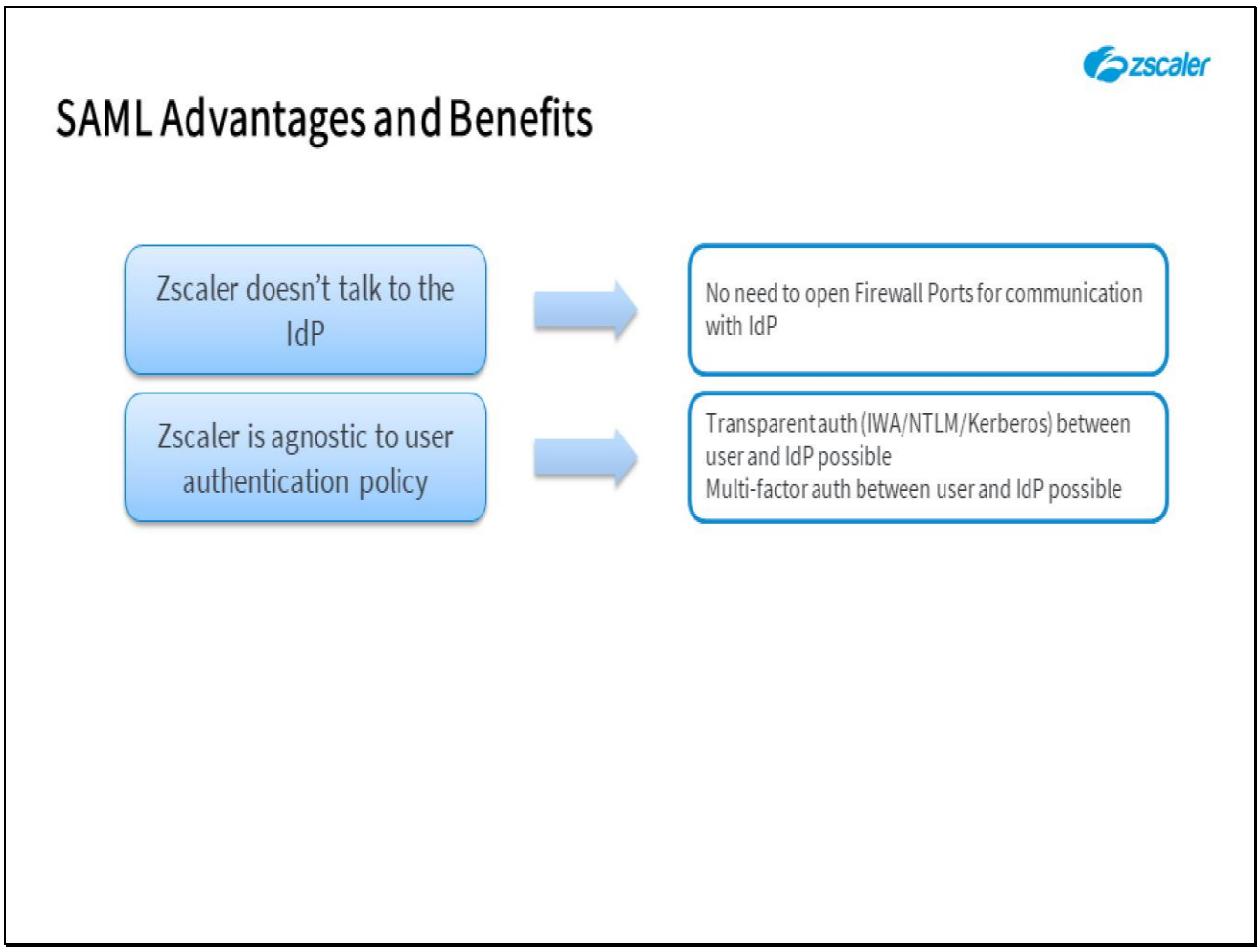
Slide 16 - Slide 16



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.

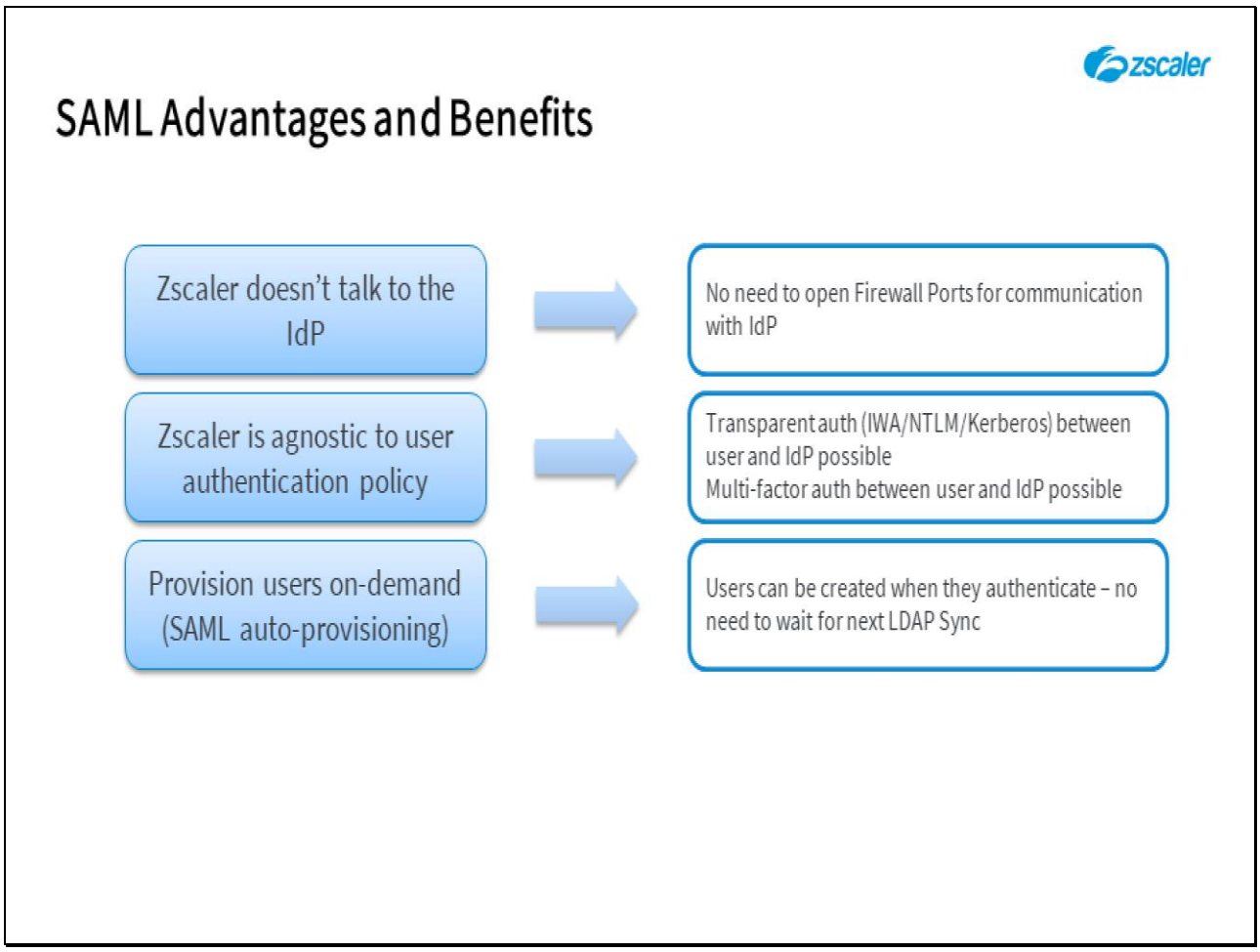
Slide 17 - SAML Advantages and Benefits



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.

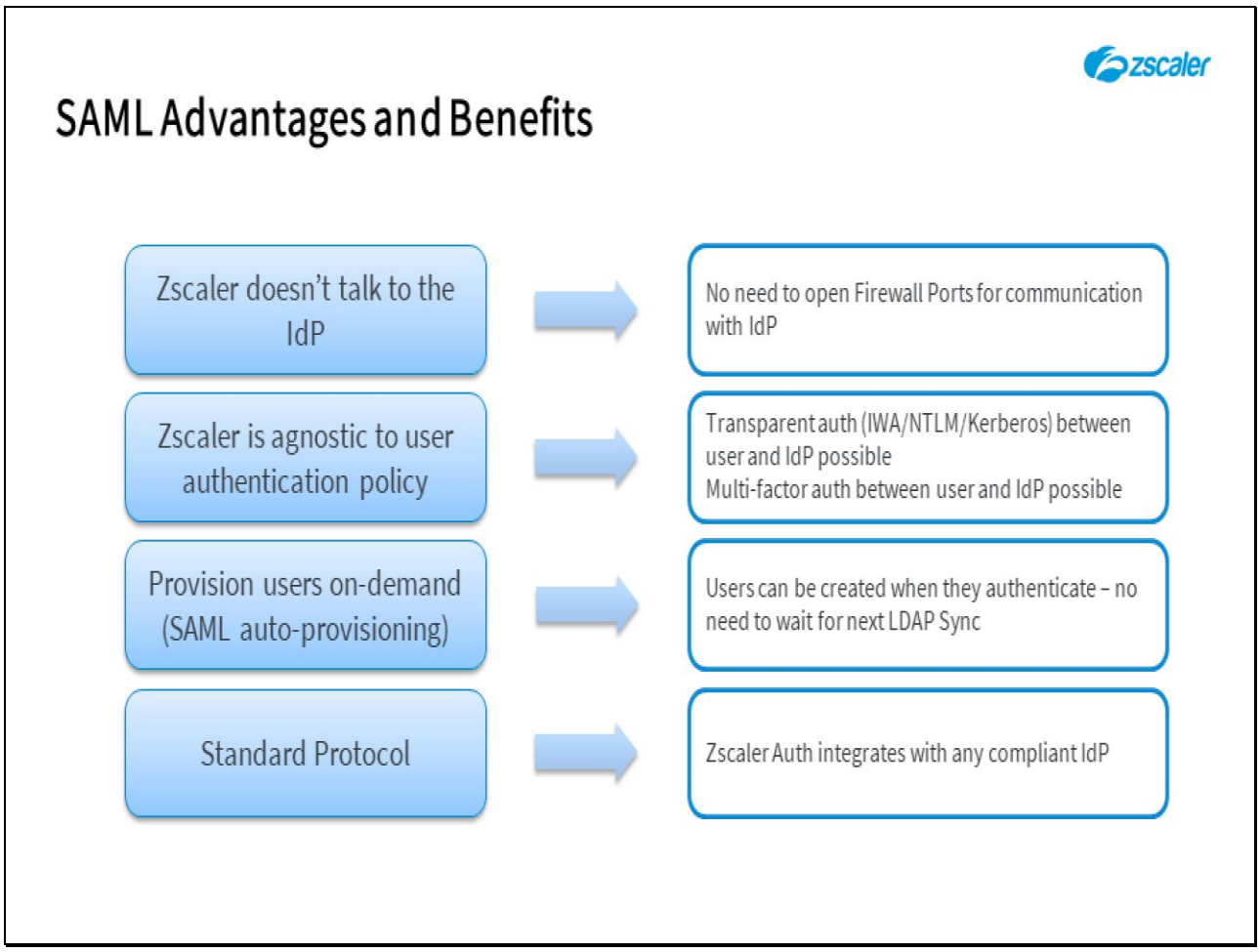
Slide 18 - SAML Advantages and Benefits



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.

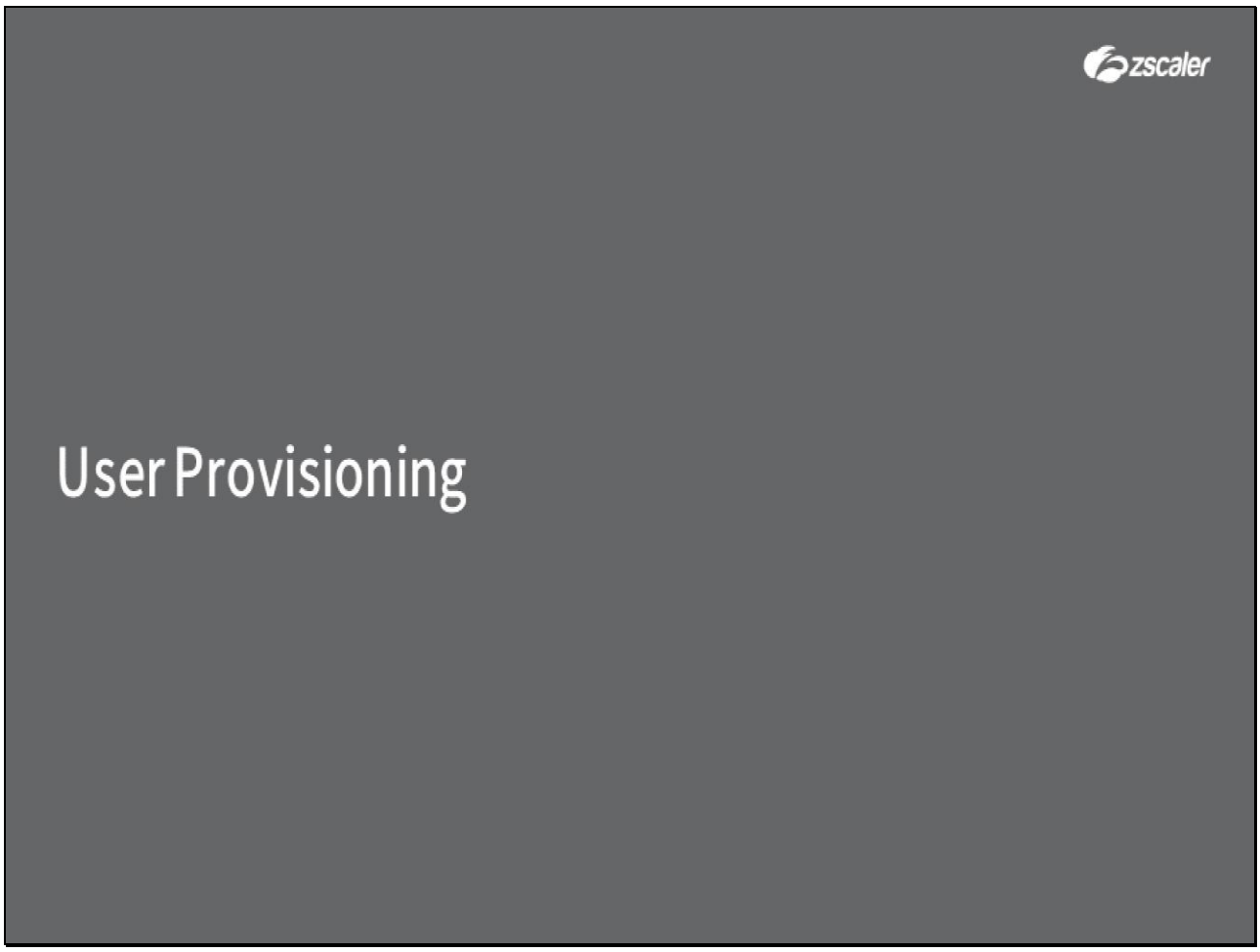
Slide 19 - SAML Advantages and Benefits



Slide notes

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

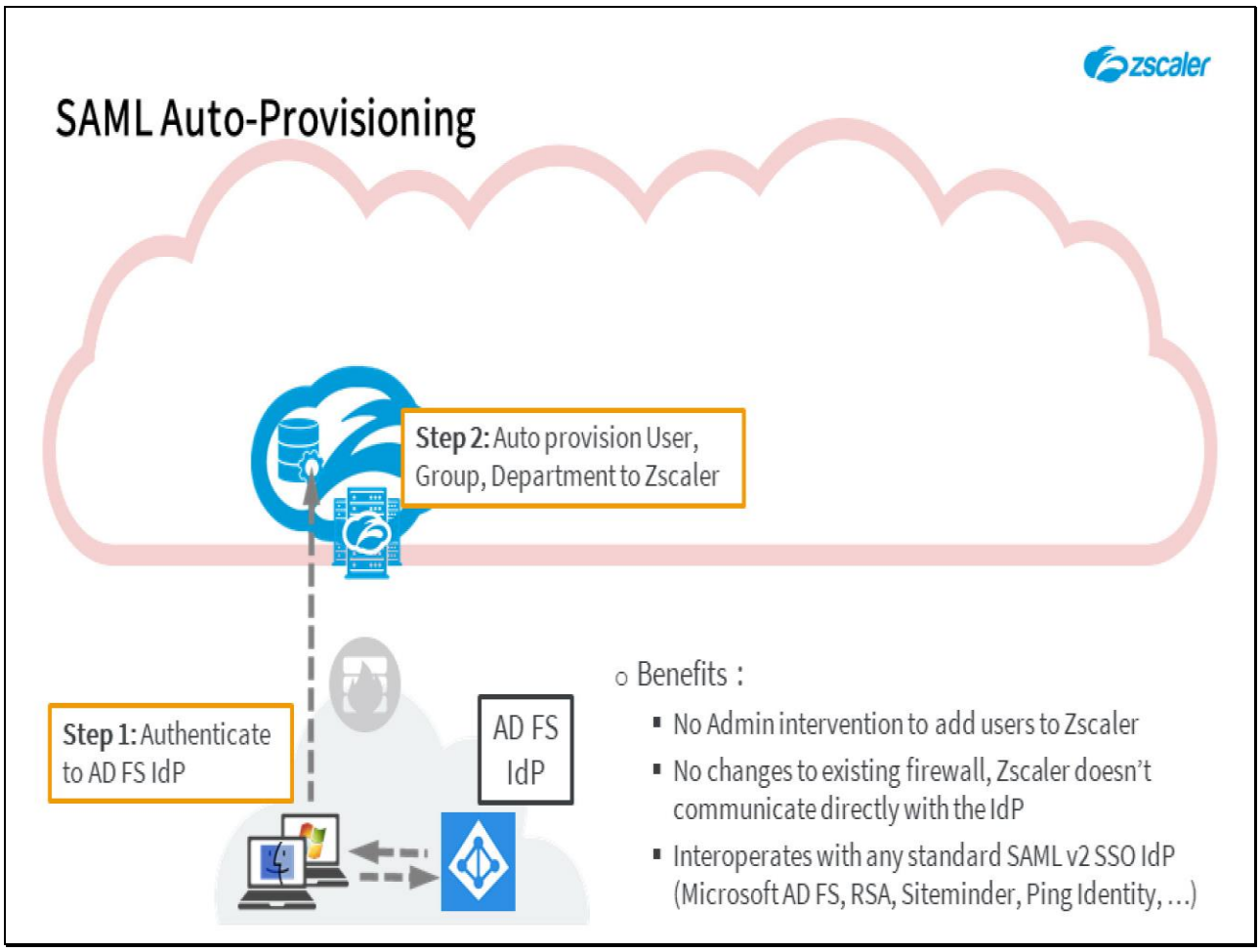
Slide 20 - User Provisioning



Slide notes

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

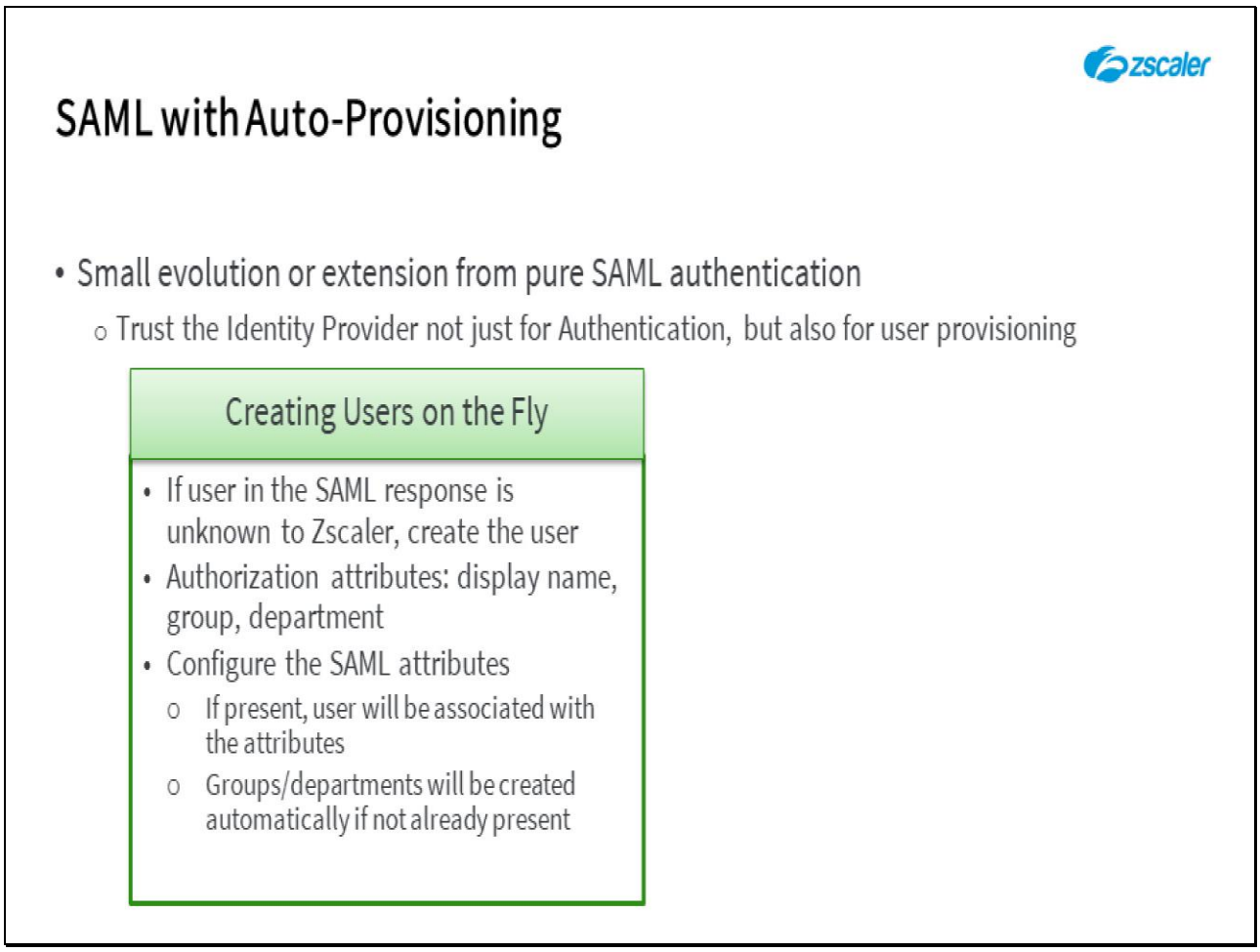
Slide 21 - SAML Auto-Provisioning



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

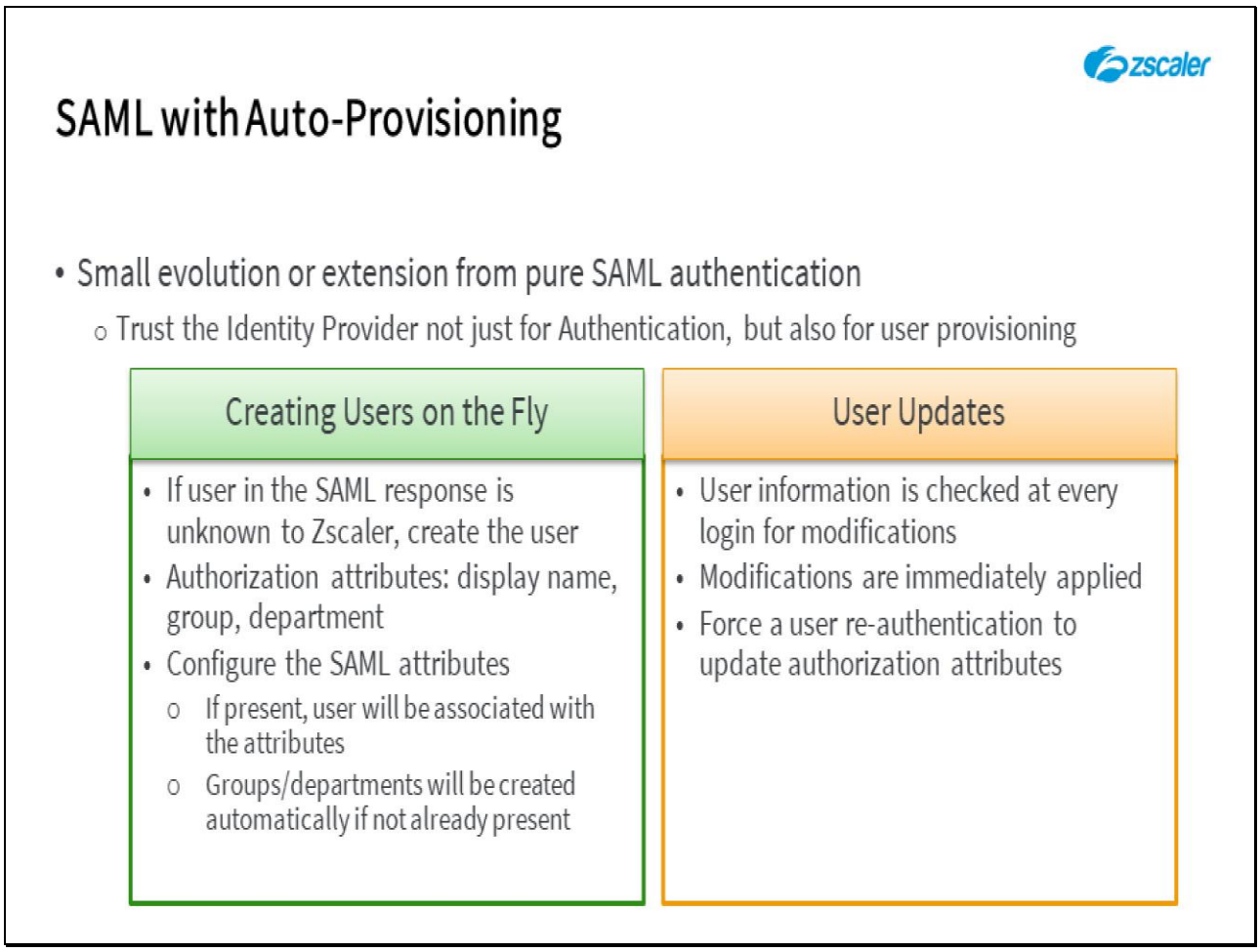


Slide notes

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.

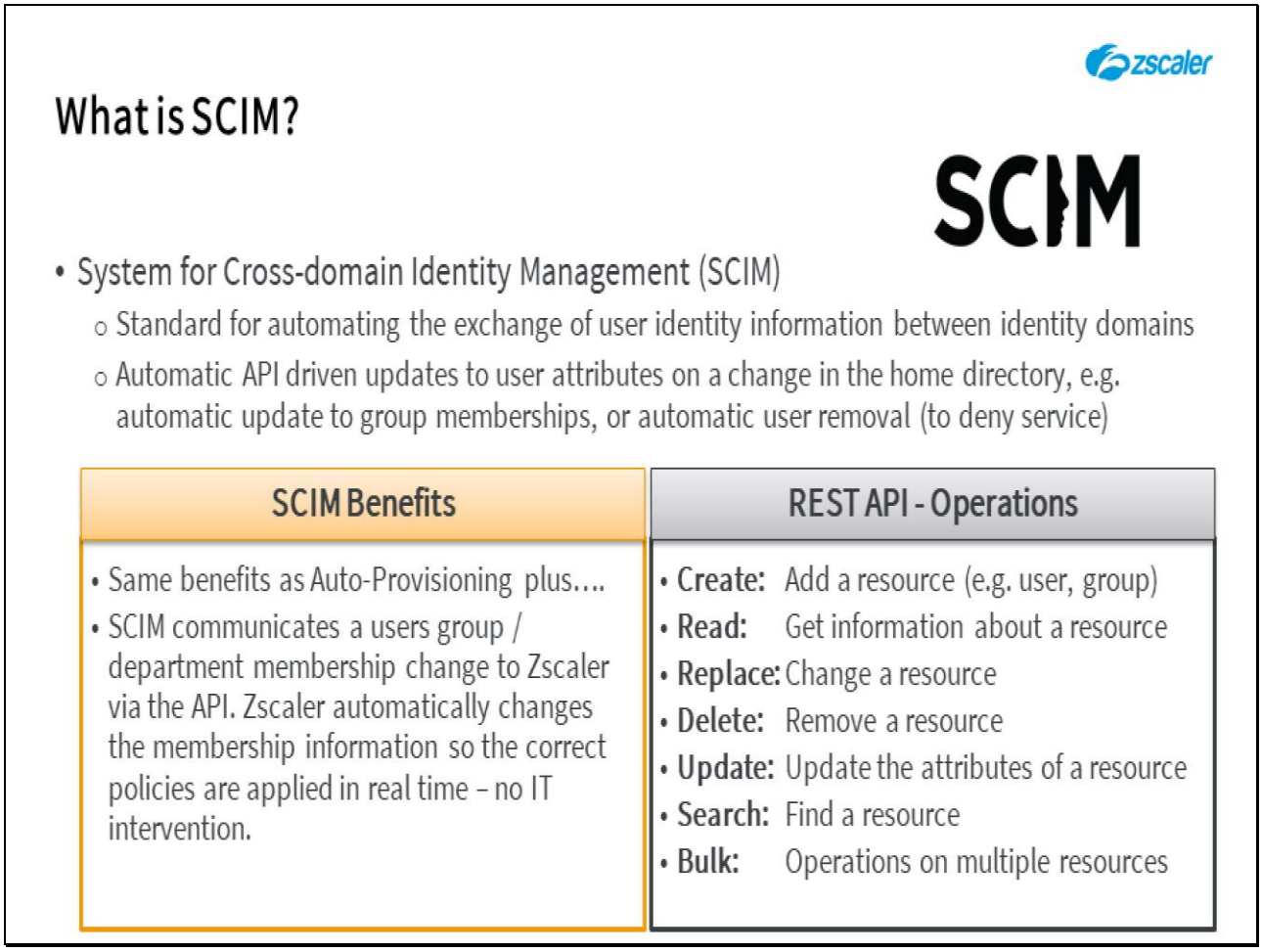
Slide 23 - SAML Auto-Provisioning



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.

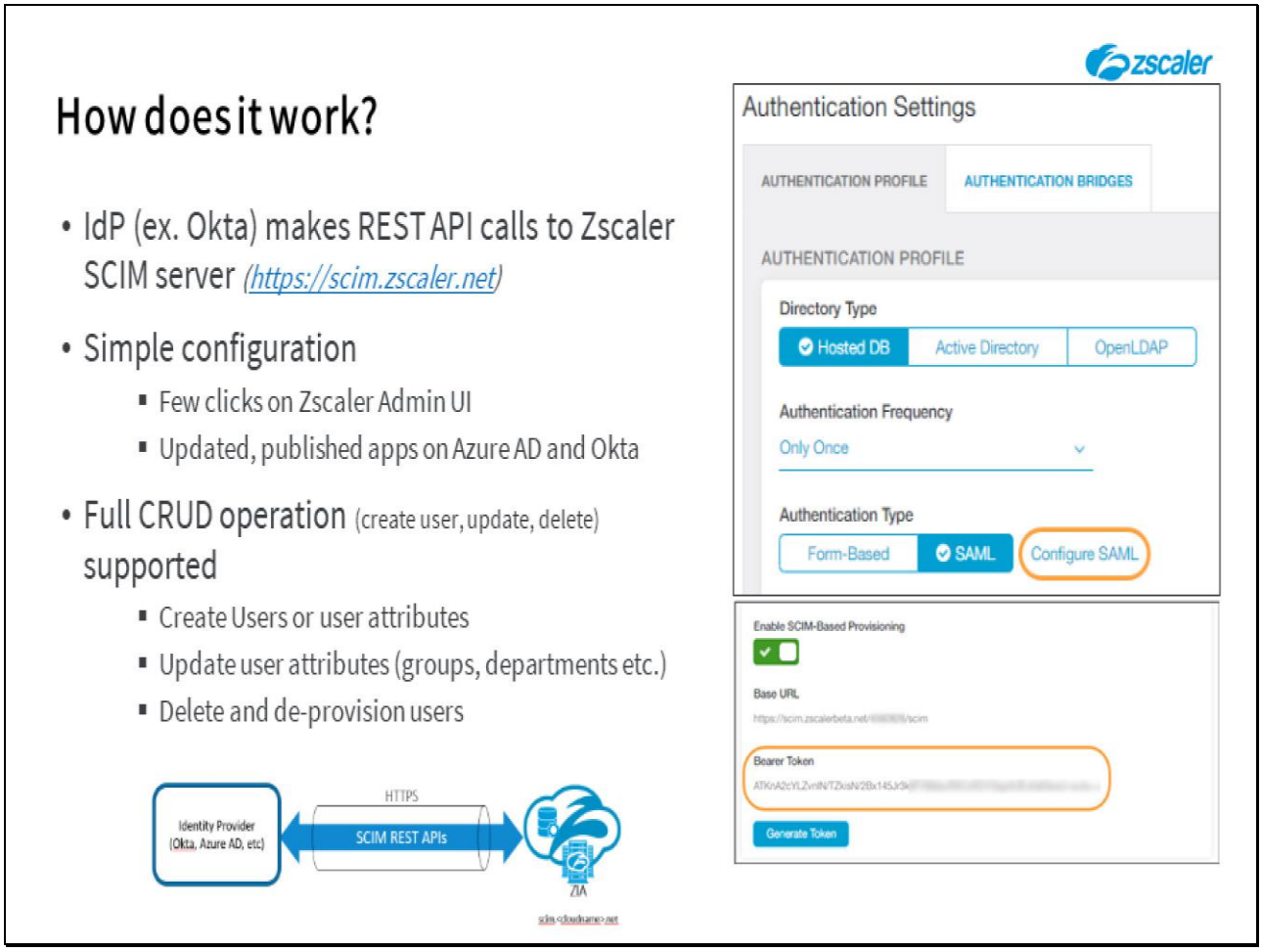
Slide 24 - What is SCIM?



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?



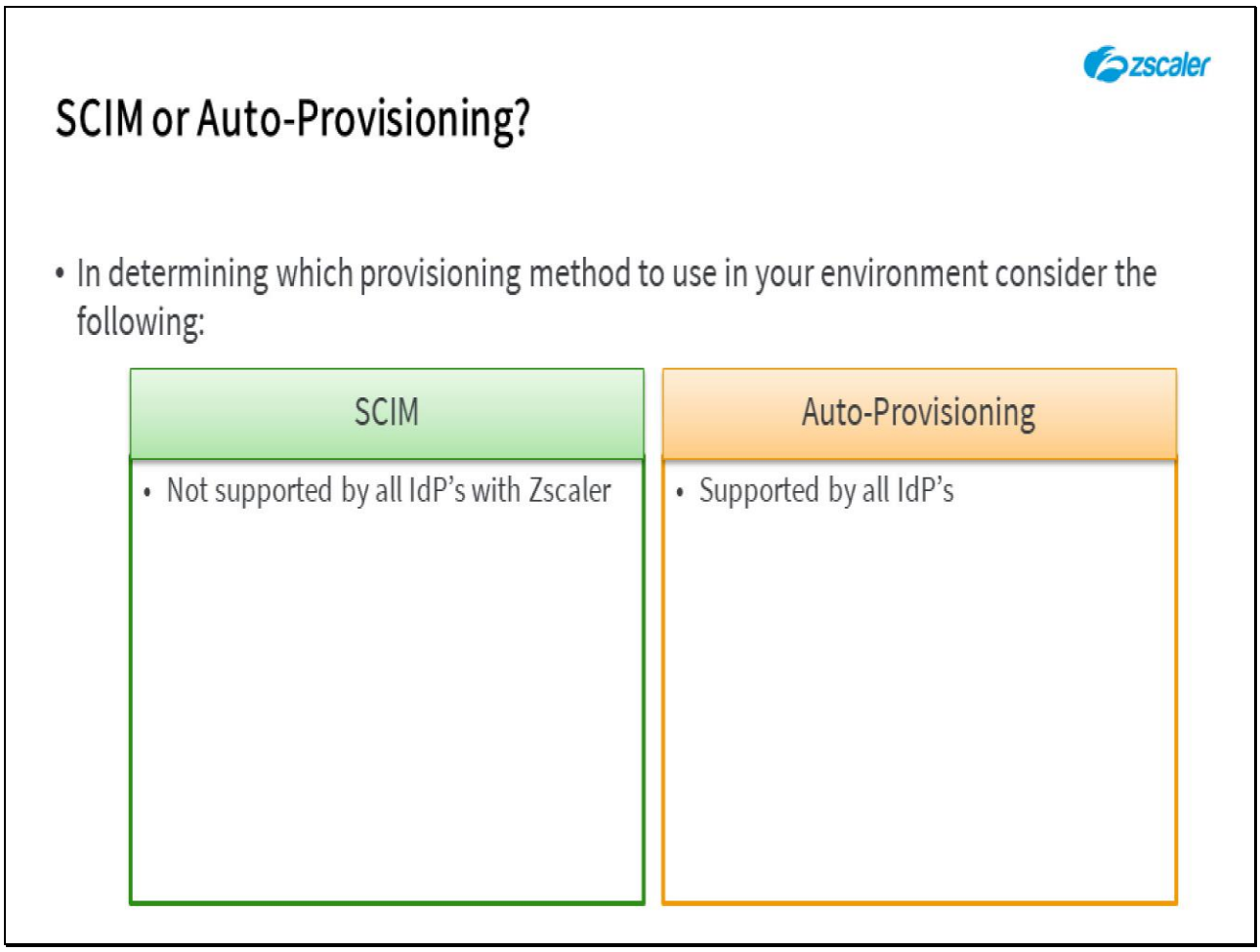
Slide notes

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 modfications if the user logs out and logs back in.

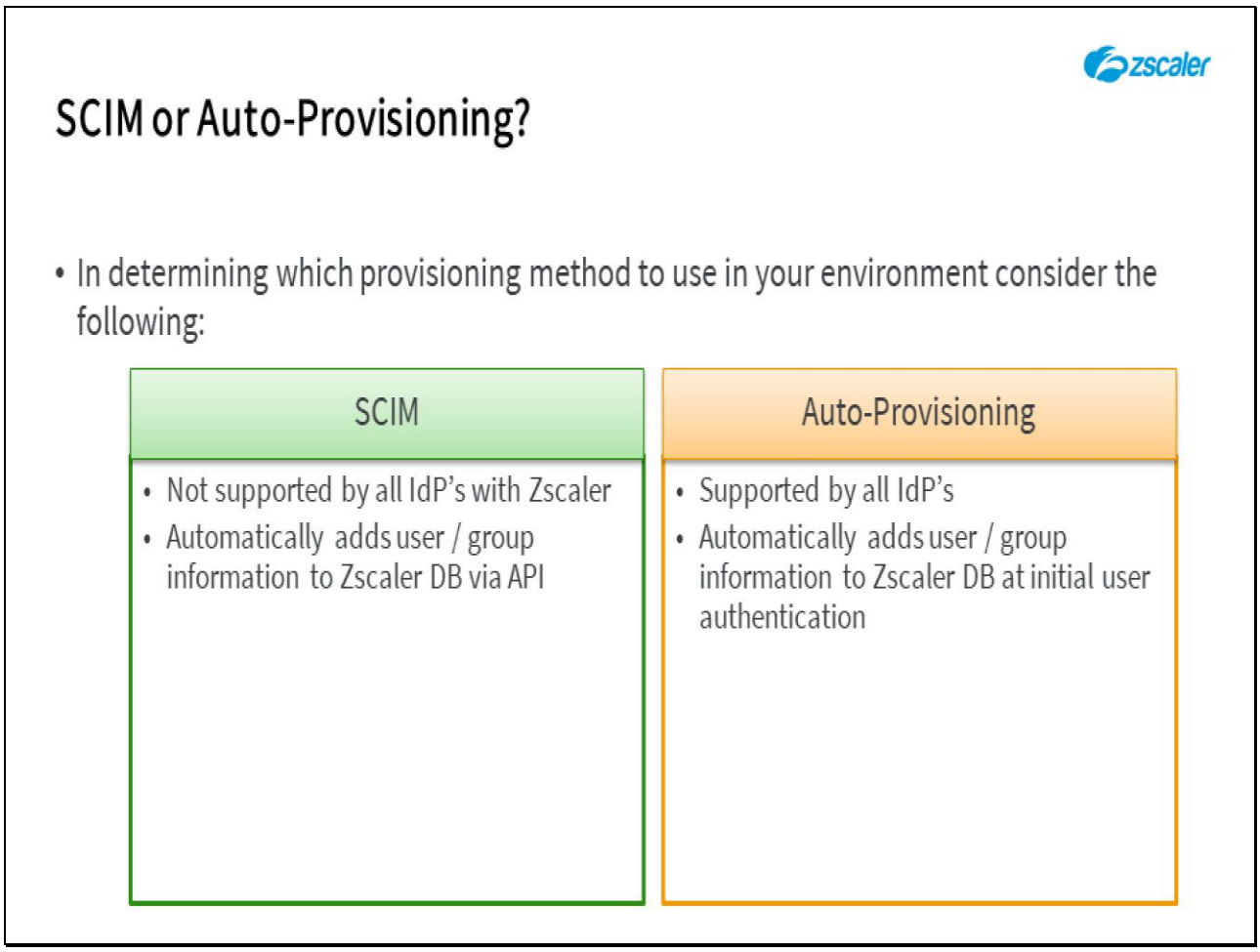
Slide 26 - SCIM or Auto-Provisioning?



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.

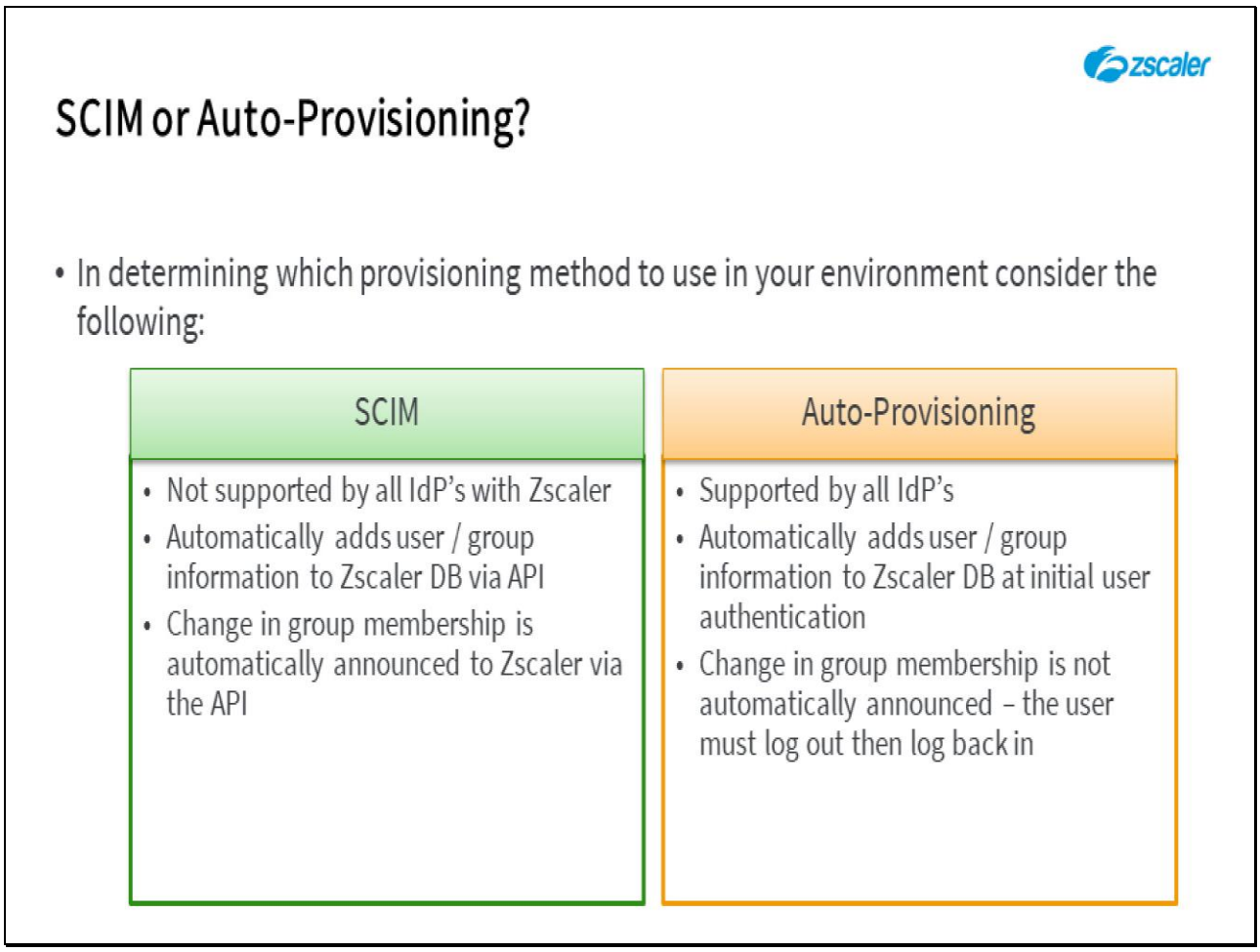
Slide 27 - SCIM or Auto-Provisioning?



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.

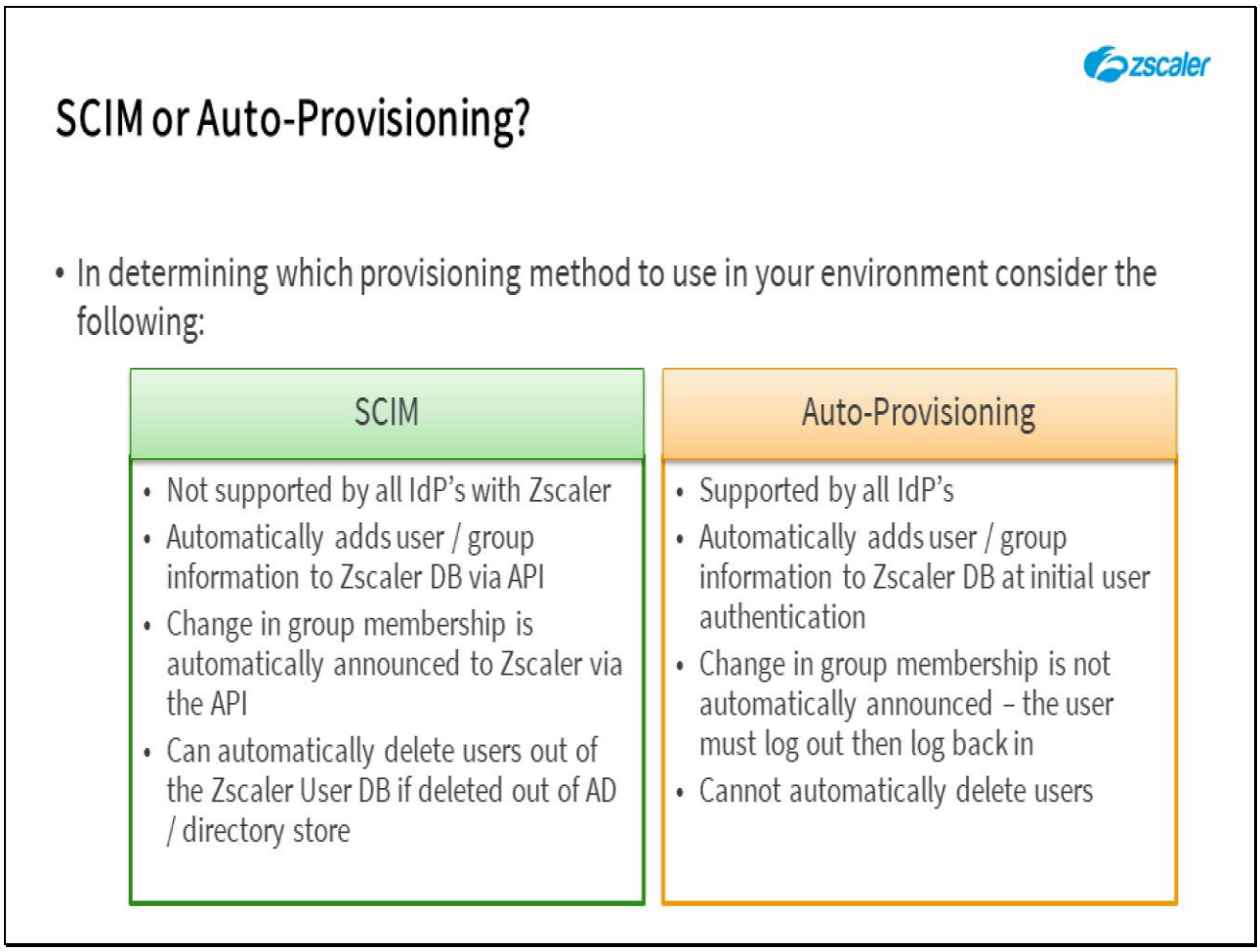
Slide 28 - SCIM or Auto-Provisioning?



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?



Slide notes

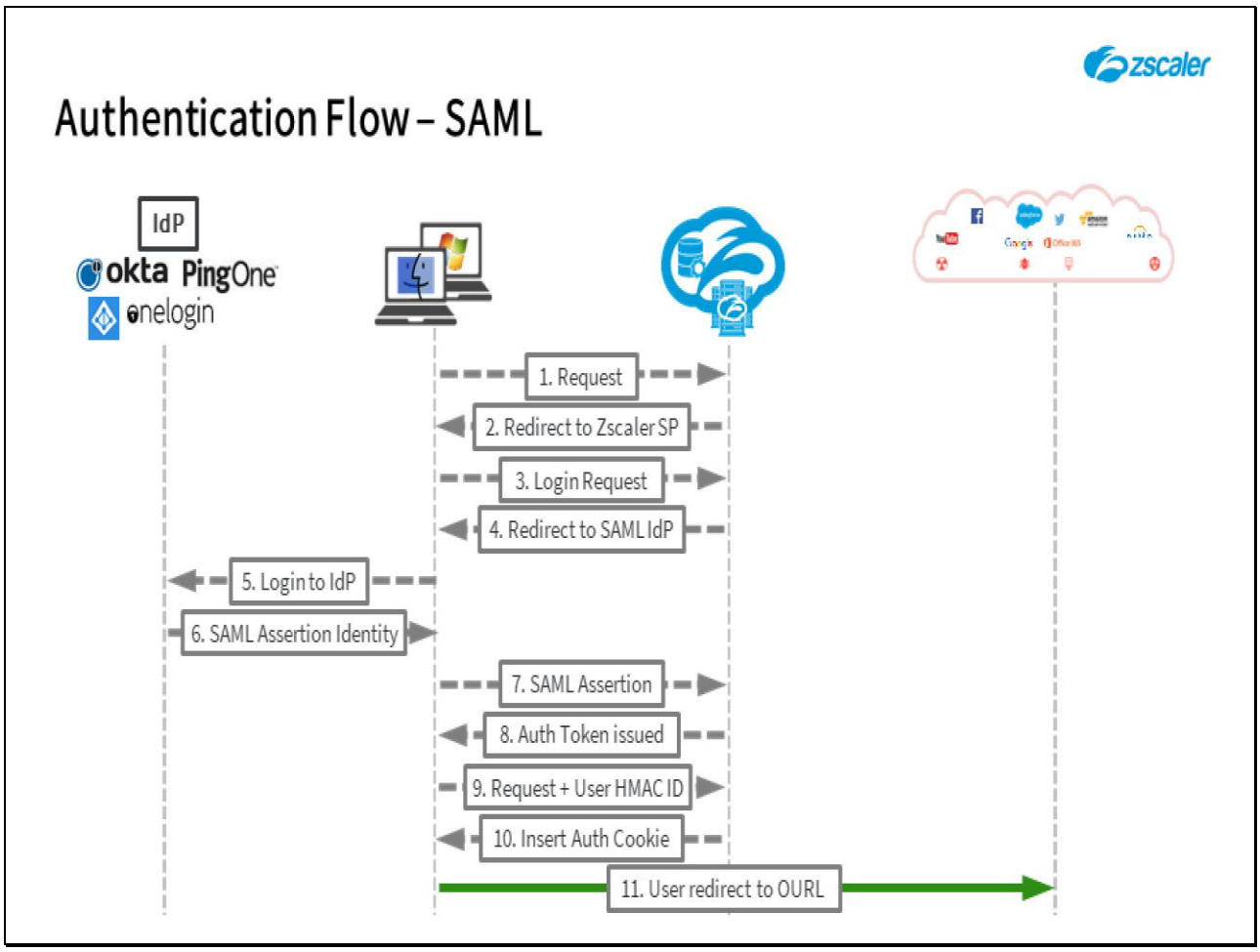
And last, SCIM can automatically delete users out of the Zscaler database if the user is deleted out of your directory store where Auto-Provisioning cannot.

Slide 30 - User Authentication

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.

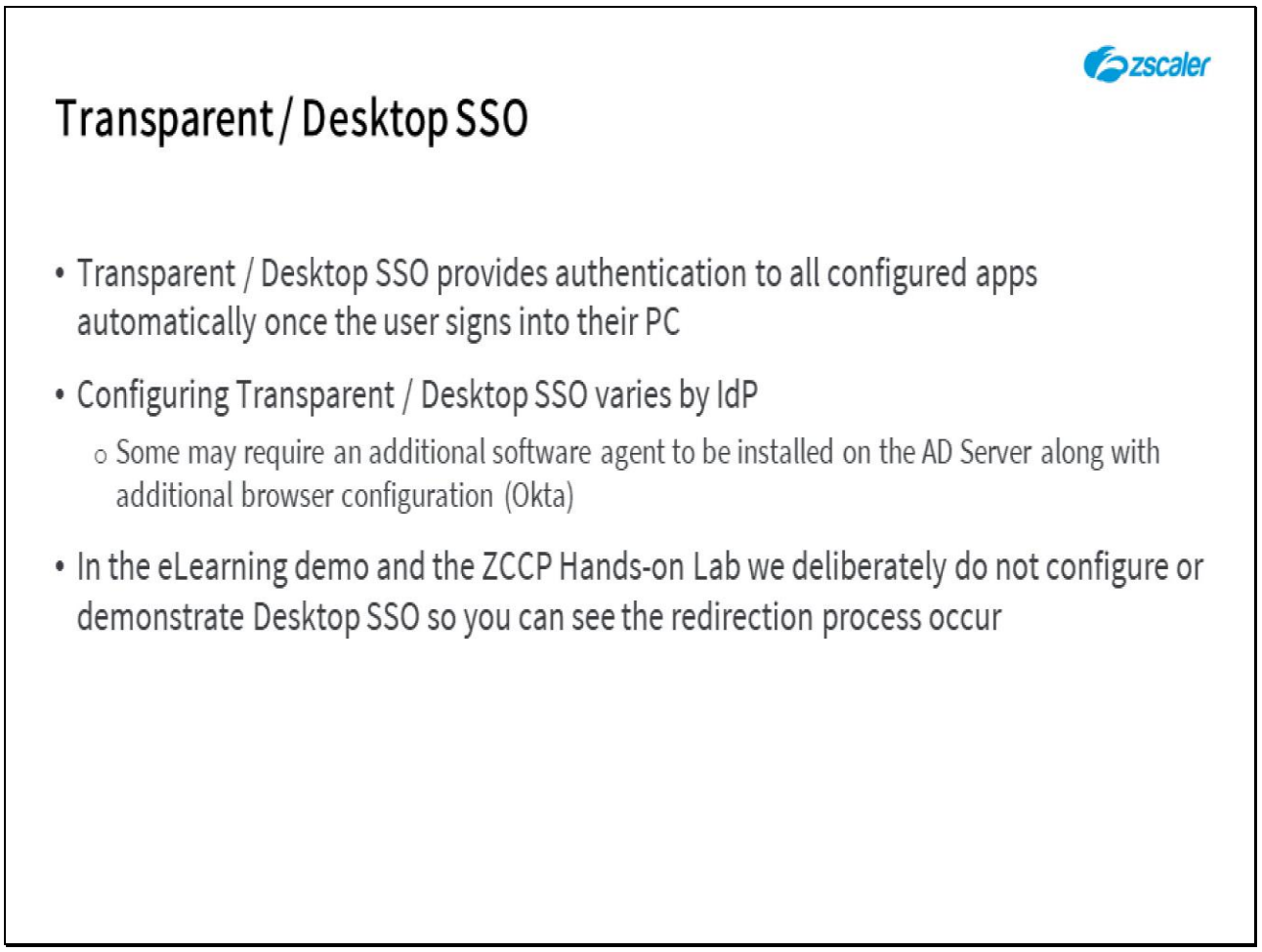
7. The user device sends the SAML assertion to Zscaler;
8. Zscaler sends and authentication token to the user;
9. The user sends an authentication request with the HMAC ID;
10. The ZEN retrieves the user's policies which determine access privileges.
11. And last, the ZEN sends an authentication cookie to the user device, then the user is redirected back to its original destination request.

Slide 32 - Slide 32

Slide notes

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

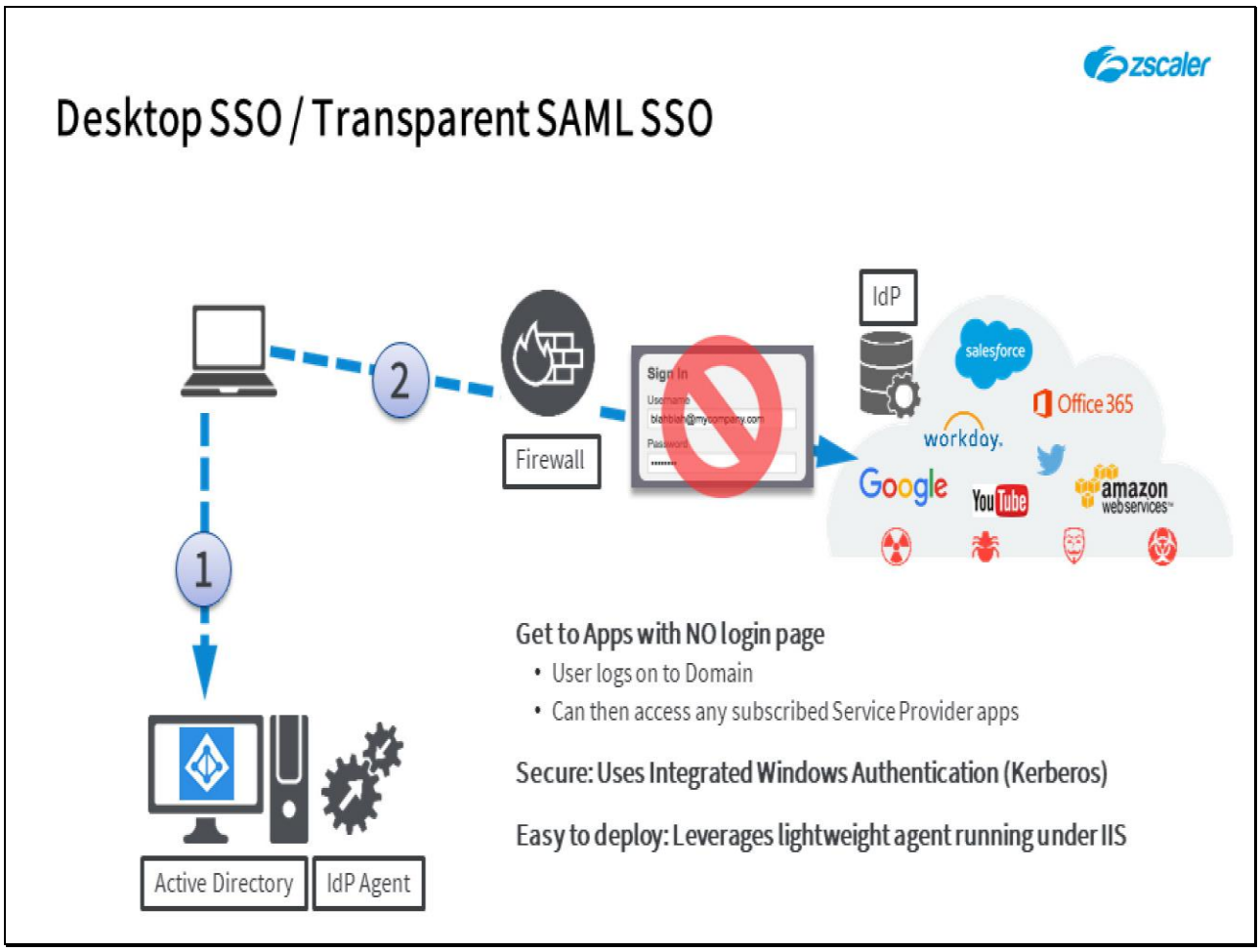
Slide 33 - SAML Authentication Flow



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.

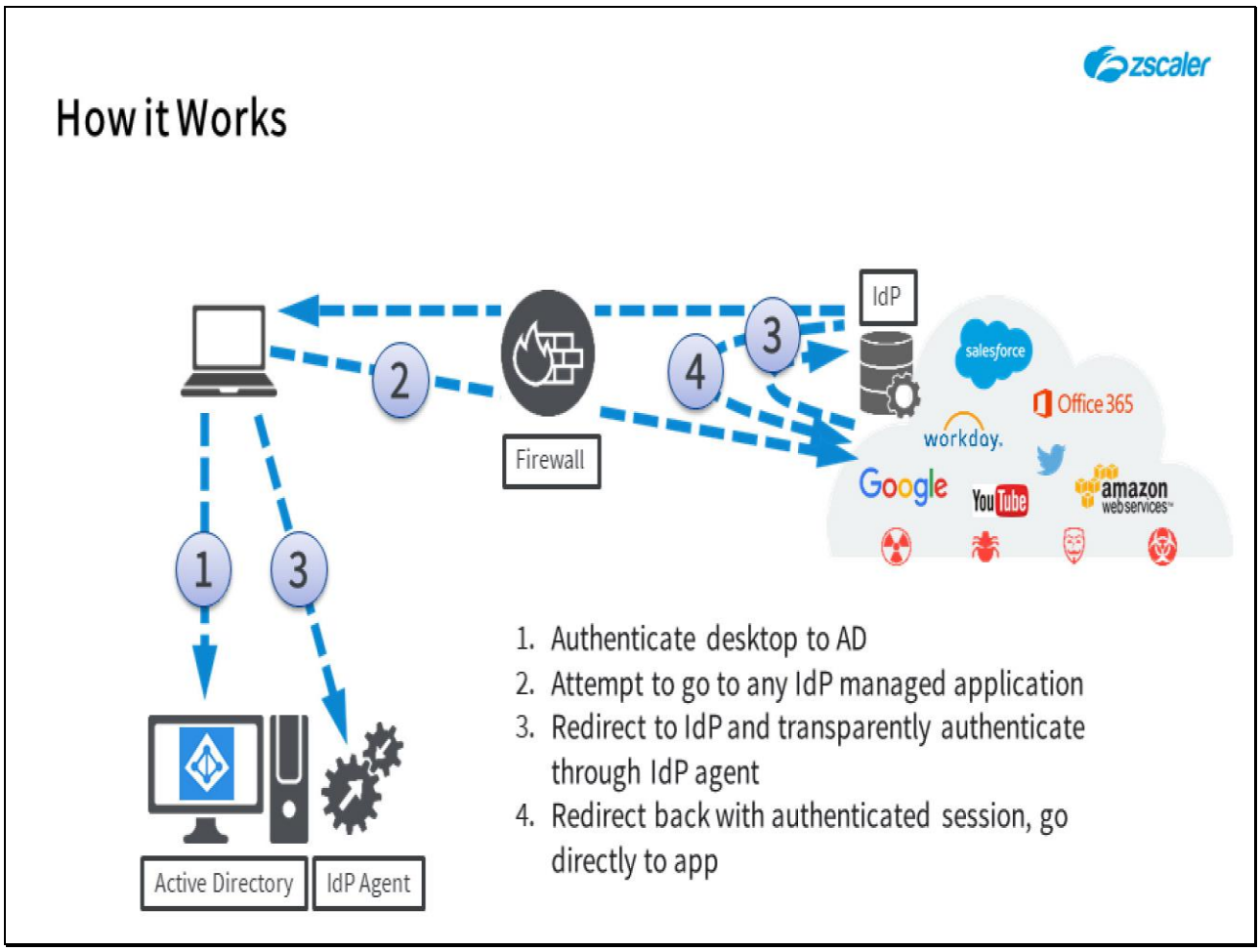
Slide 34 - Desktop SSO / Transparent SAML SSO



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.

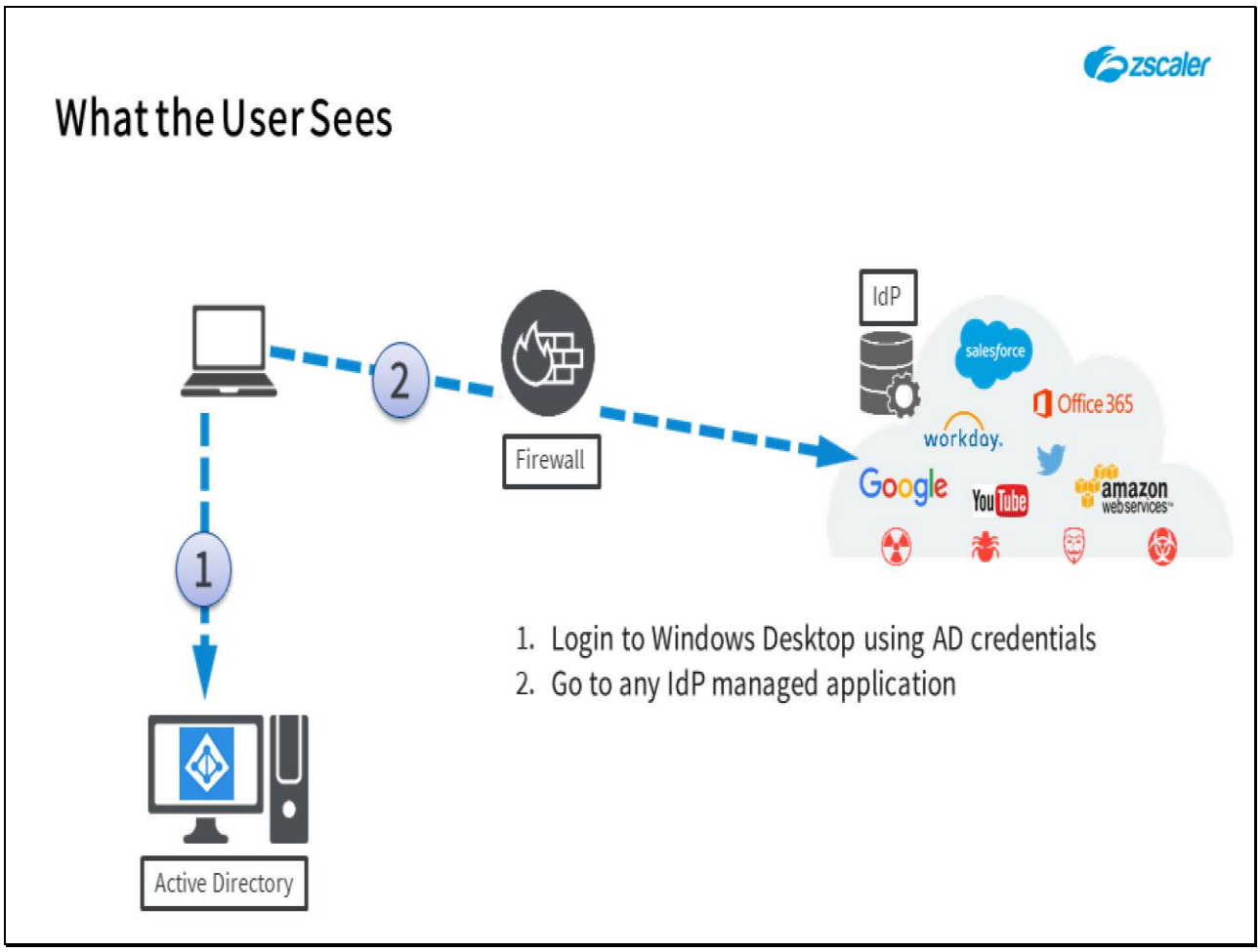
Slide 35 - How it Works



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

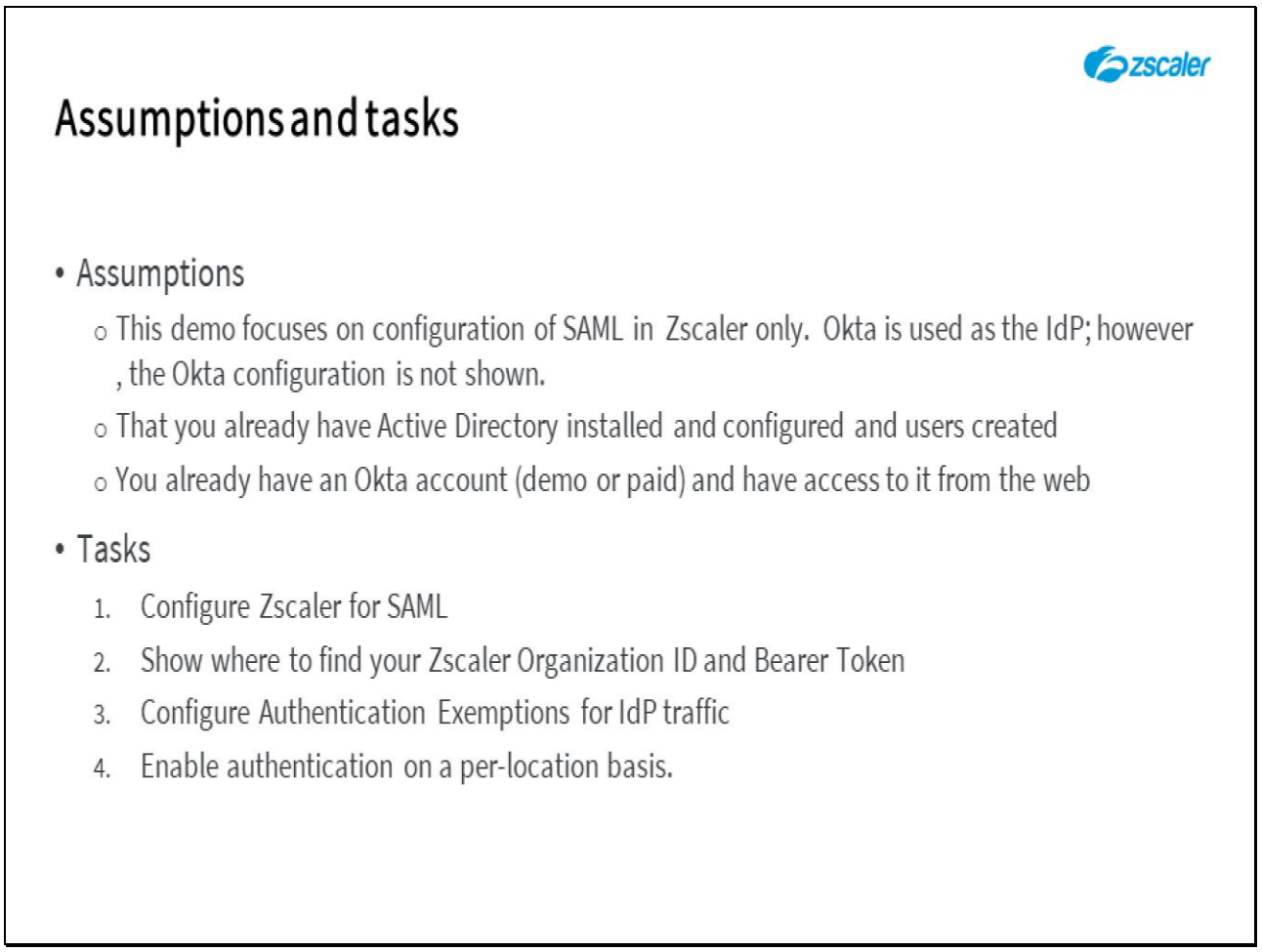
And this is what the end-user sees: 1. Again, first the user logs into their windows desktop using Active Directory credentials; 2. Then they continue on in their browser to any IdP managed application and no additional sign-in is required.

Slide 37 - SAML Authentication Options

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



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.

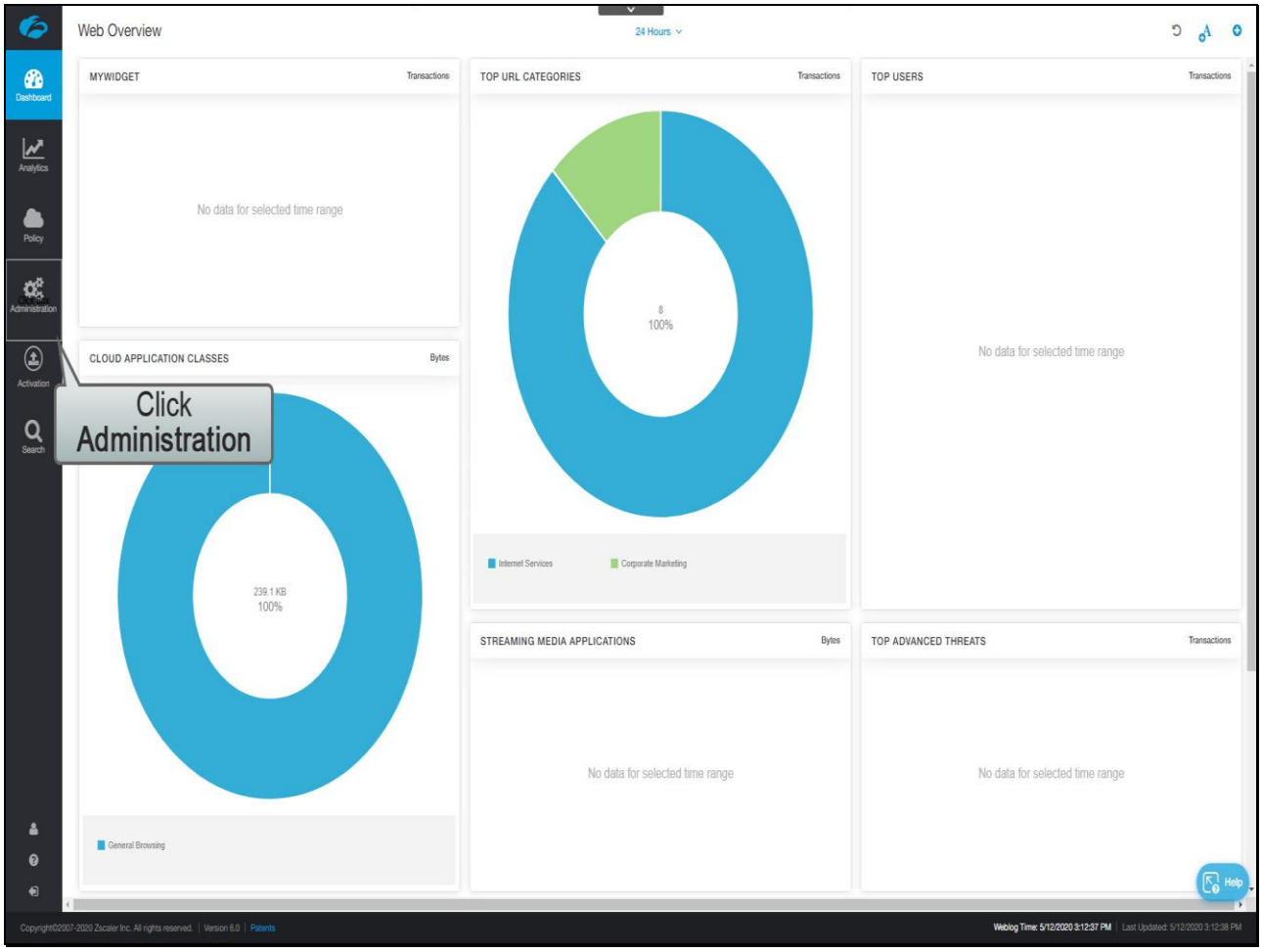
Tasks that will be demonstrated are: Configuring Zscaler to use SAML and show where to find your Zscaler Organization ID and Bearer Token for use in your IdP configuration, configuring Authentication Exemptions for IdP traffic, and enabling authentication on a per-location basis.

Slide 39 - Configuring SAML in Zscaler

Slide notes

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

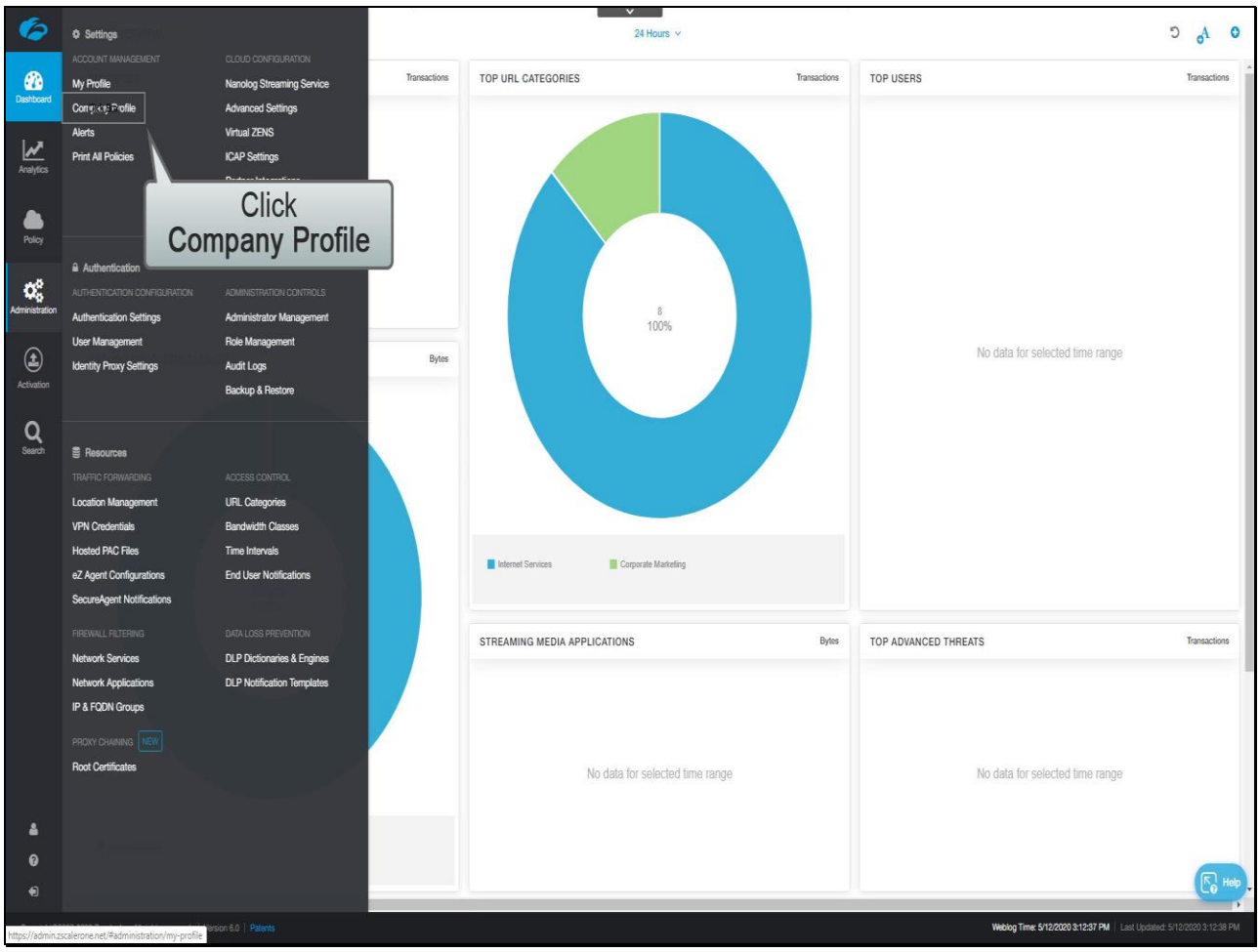
Slide 40 - Slide 40



Slide notes

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

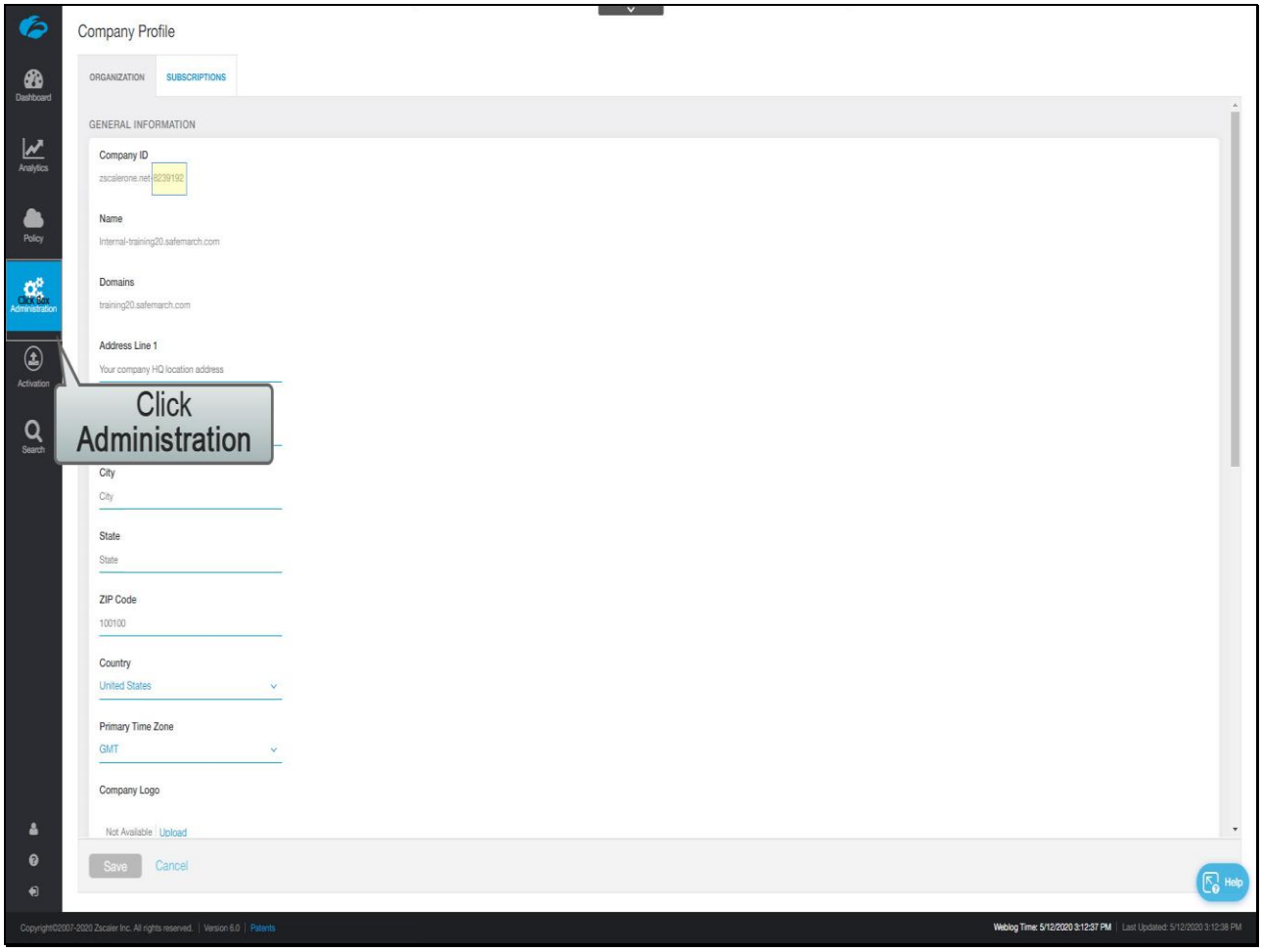
Slide 41 - Slide 41



Slide notes

Then **Company Profile**.

Slide 42 - Slide 42

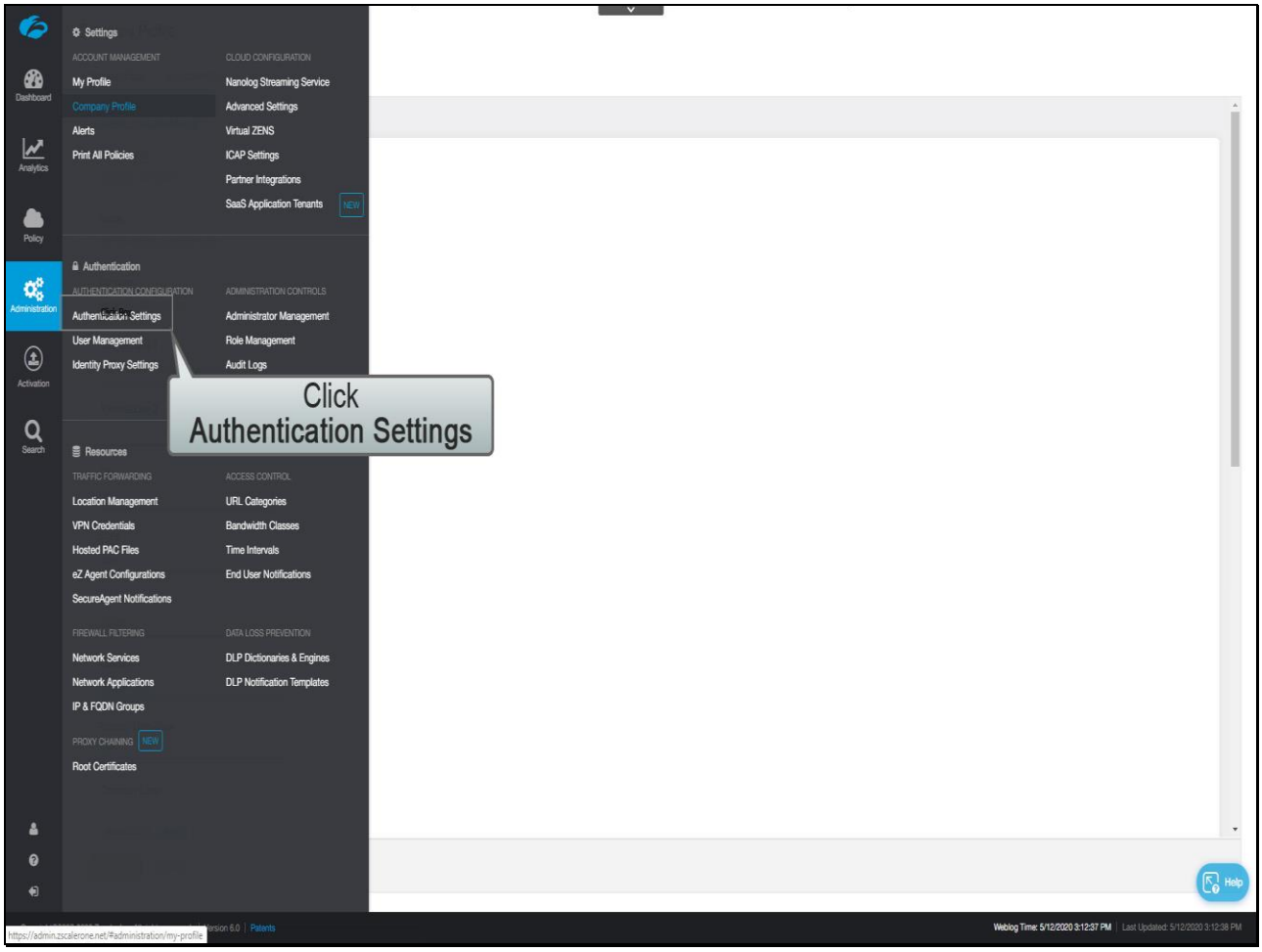


Slide notes

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**.

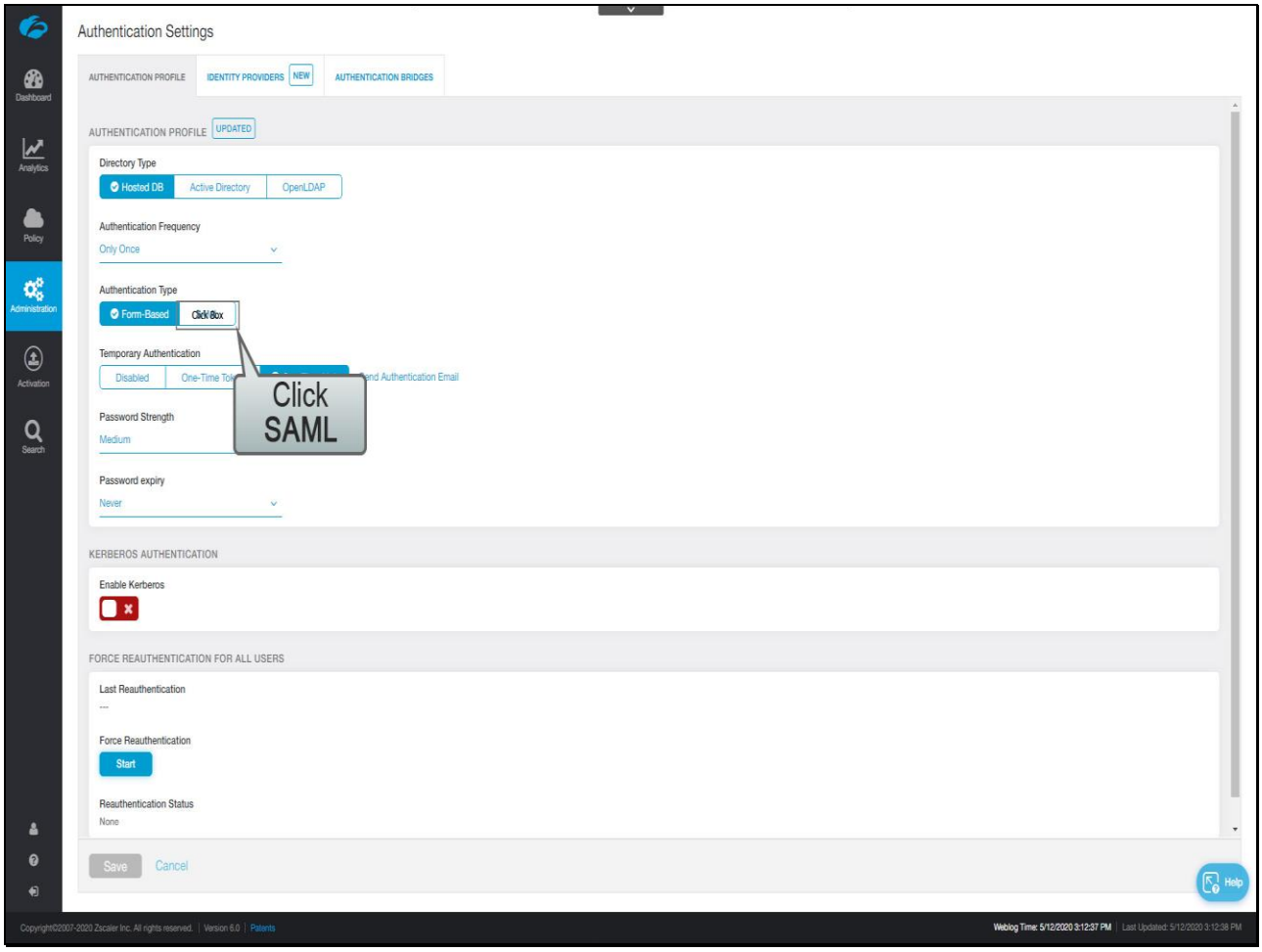
Slide 43 - Slide 43



Slide notes

Then **Authentication Settings.**

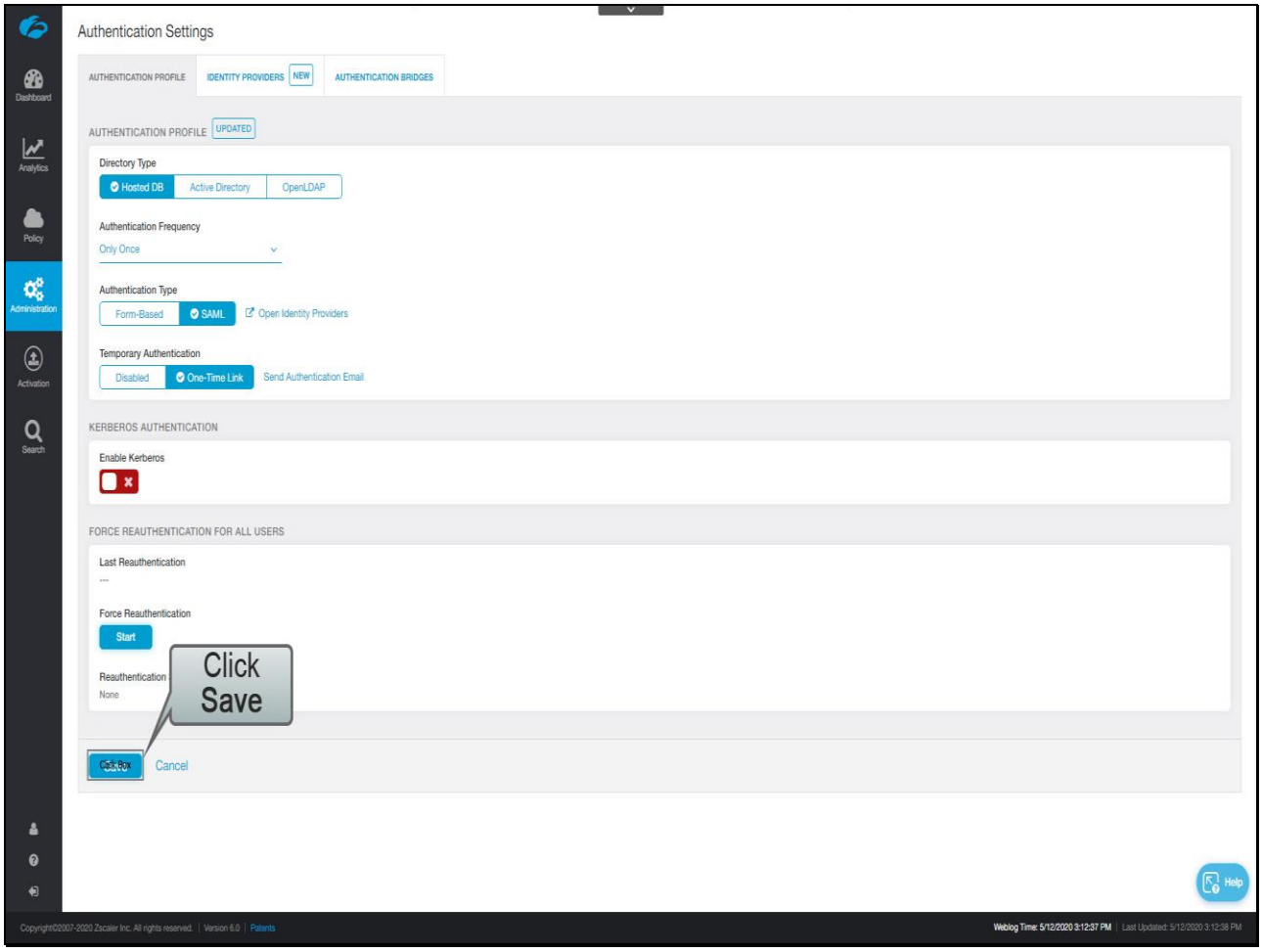
Slide 44 - Slide 44



Slide notes

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

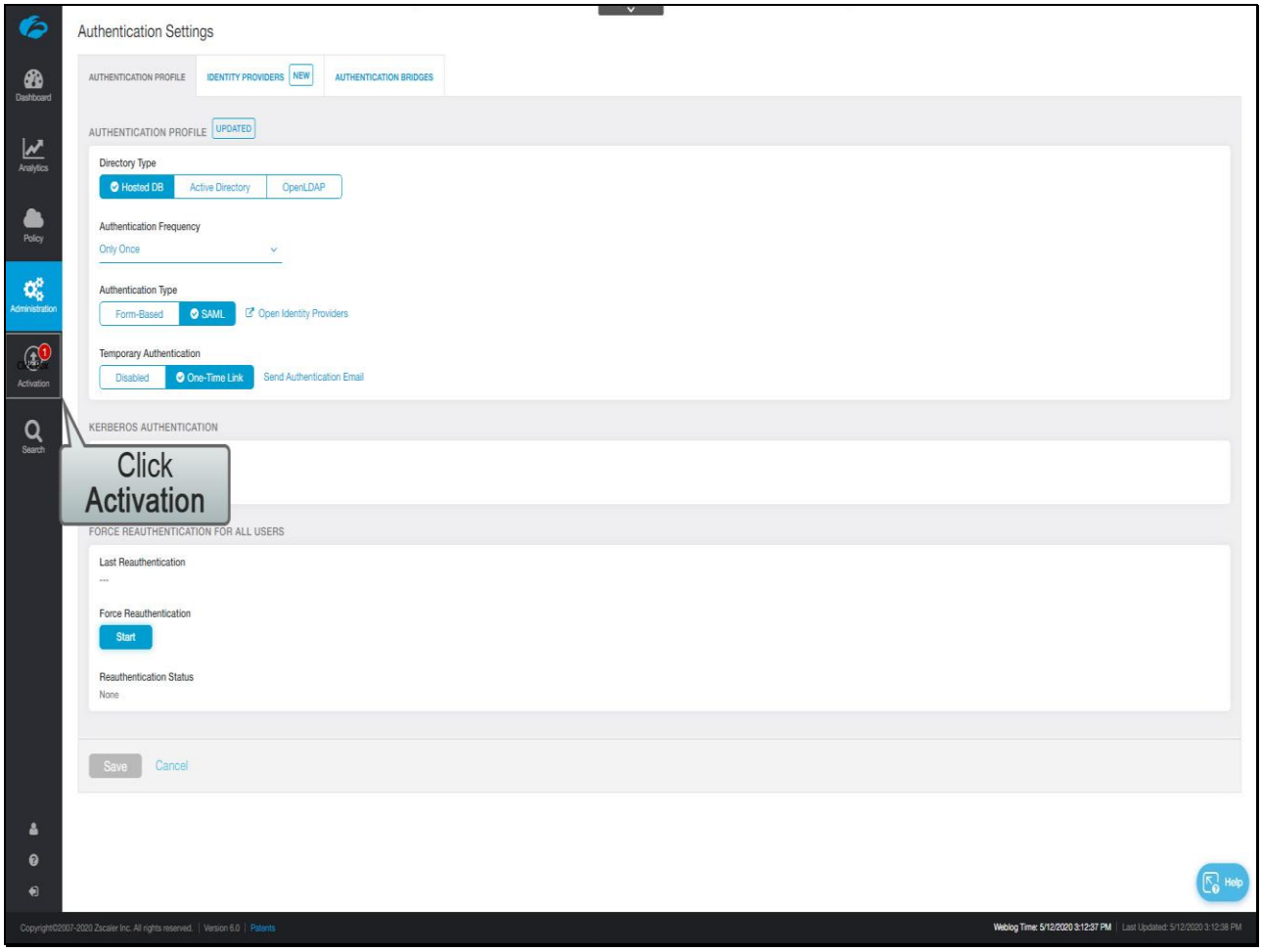
Slide 45 - Slide 45



Slide notes

and click **Save**.

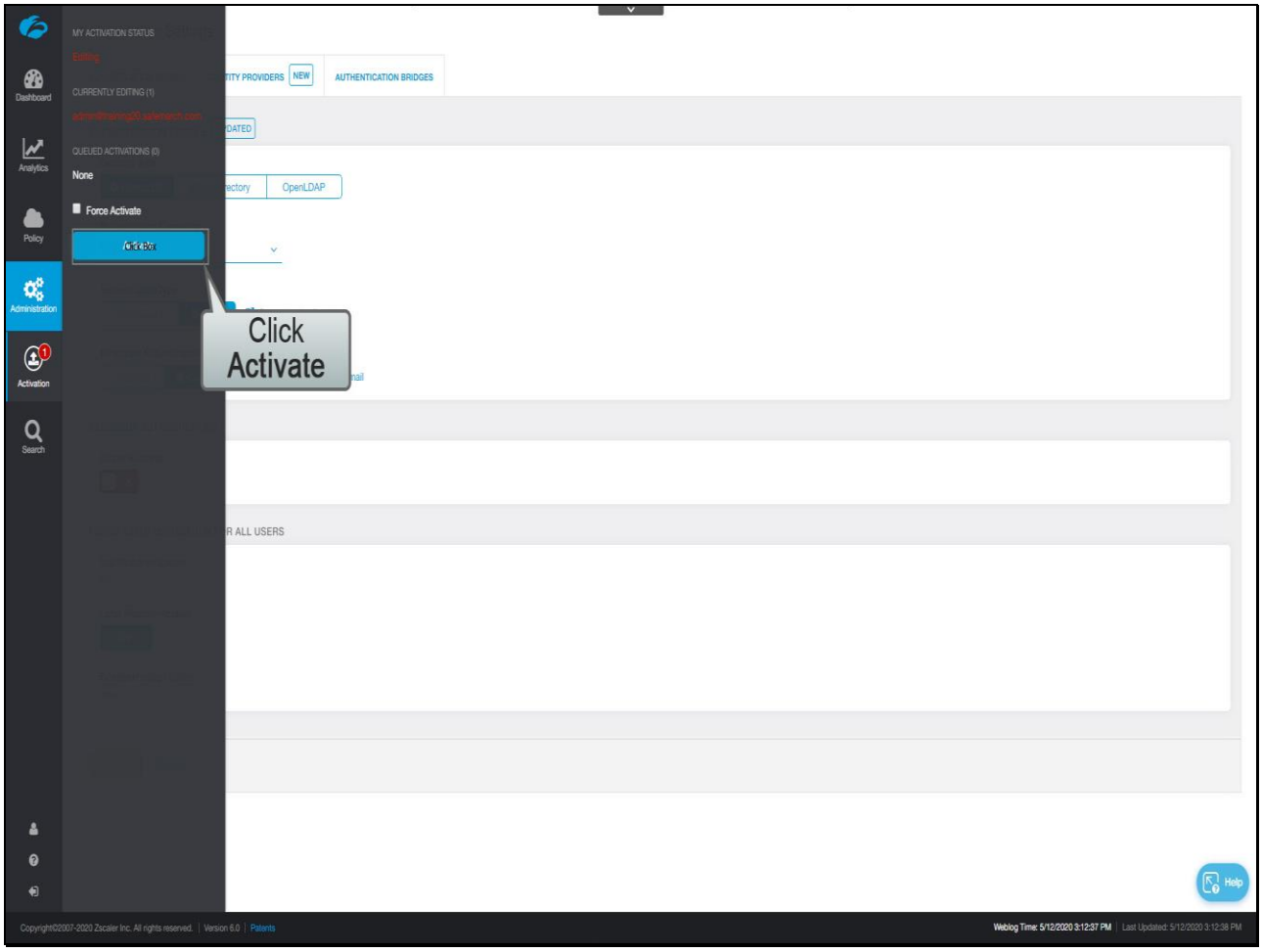
Slide 51 - Slide 51



Slide notes

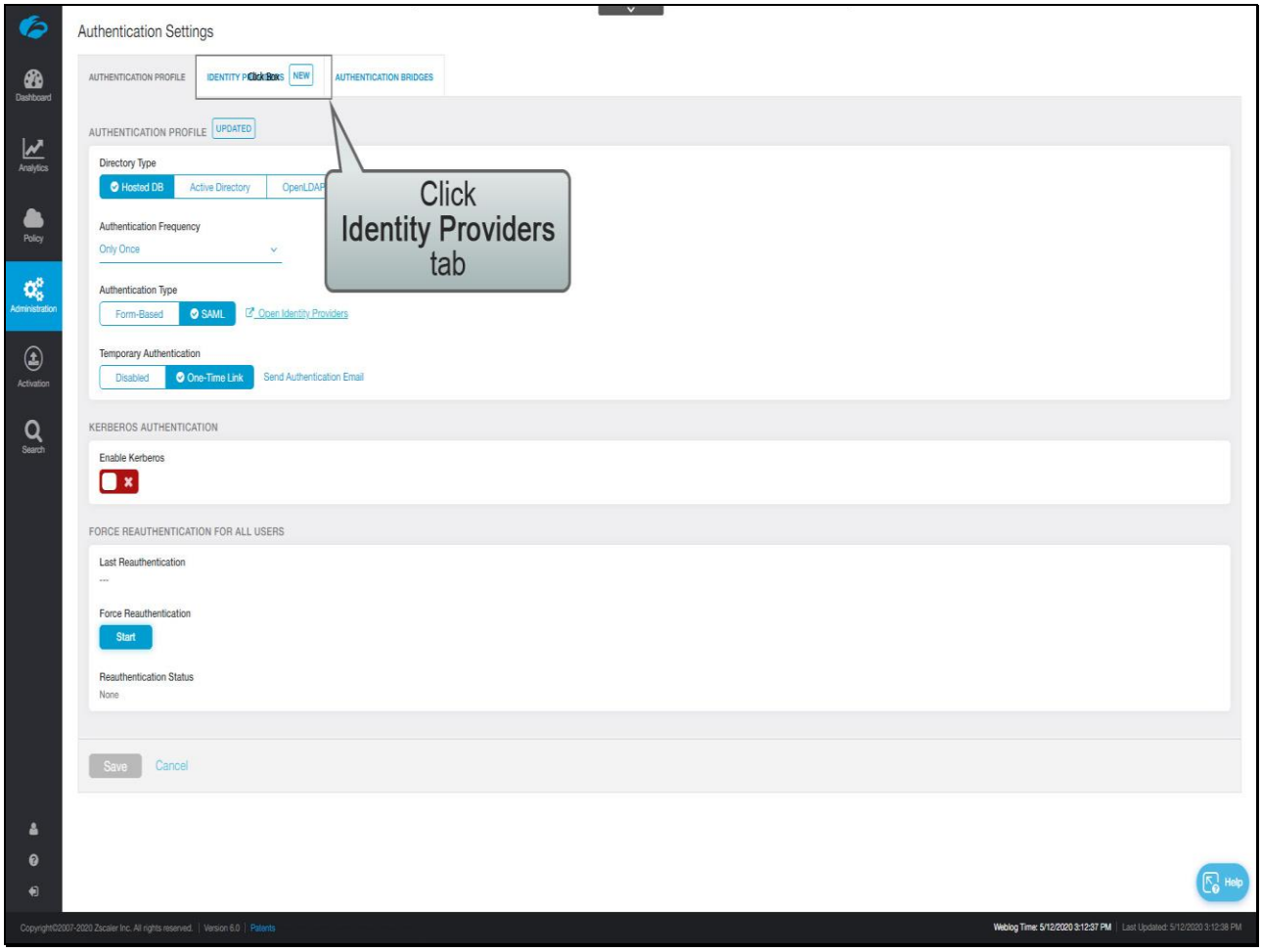
Activate your changes.

Slide 52 - Slide 52



Slide notes

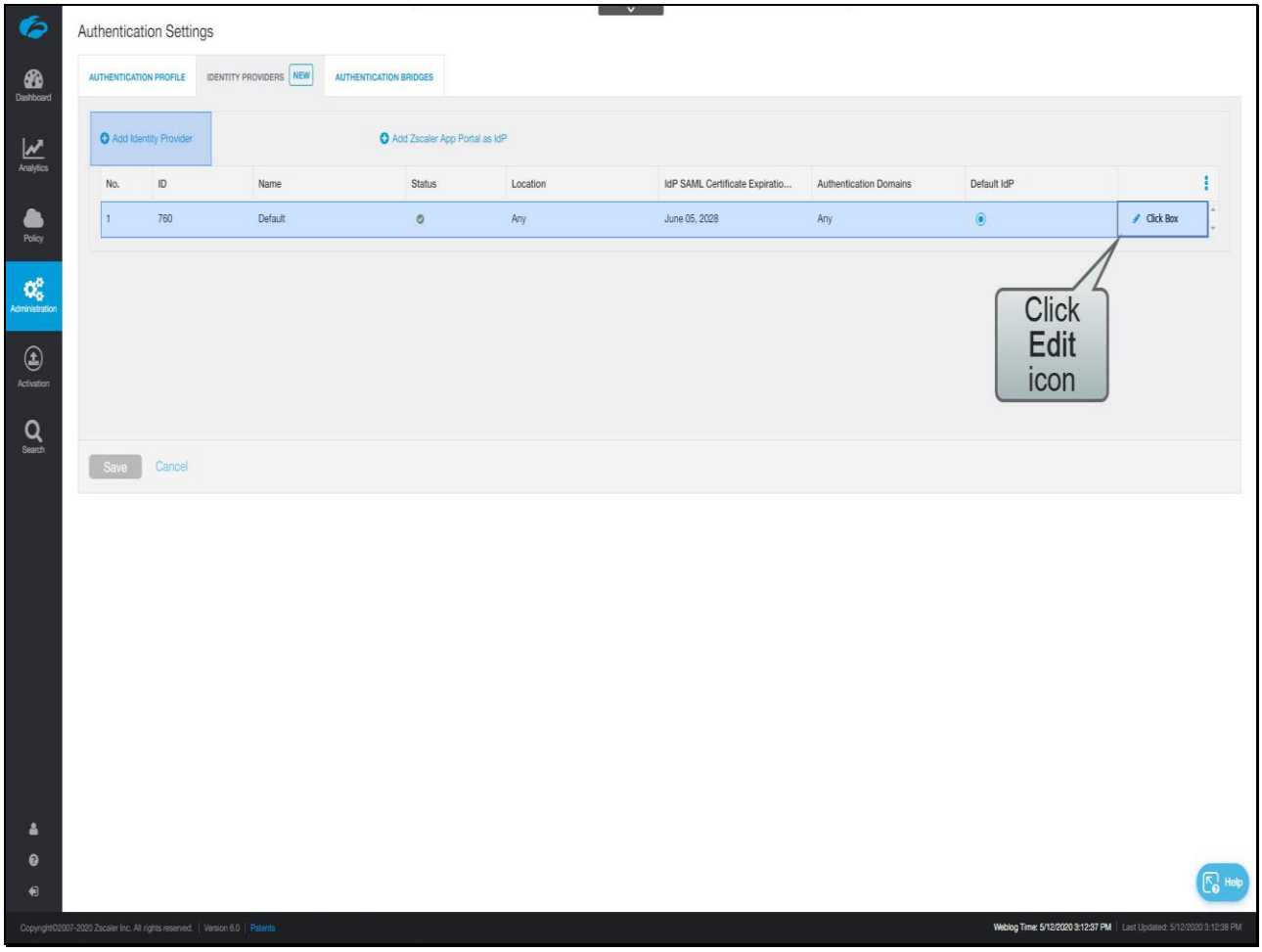
Slide 55 - Slide 55



Slide notes

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

Slide 57 - Slide 57

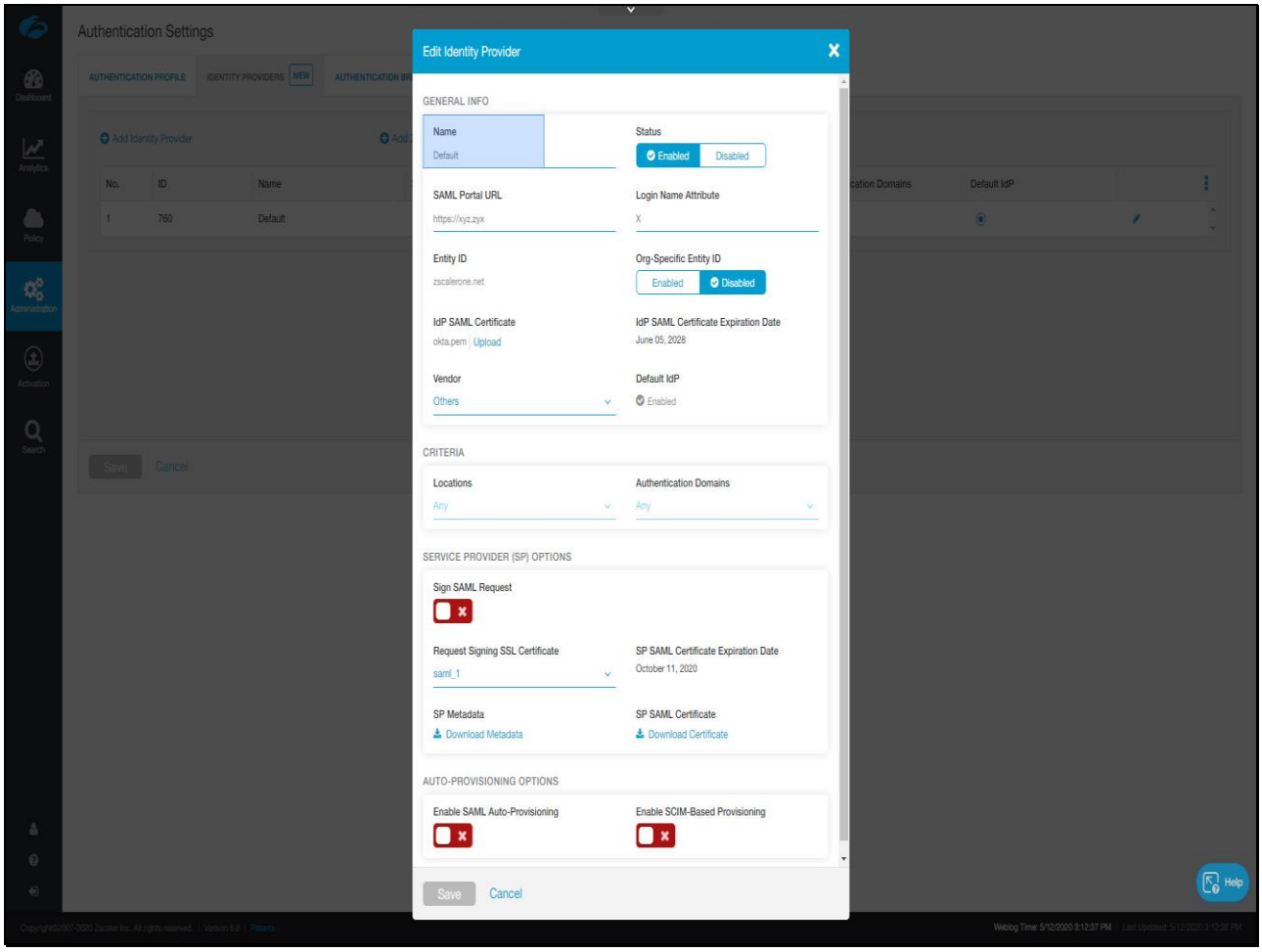


Slide notes

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.

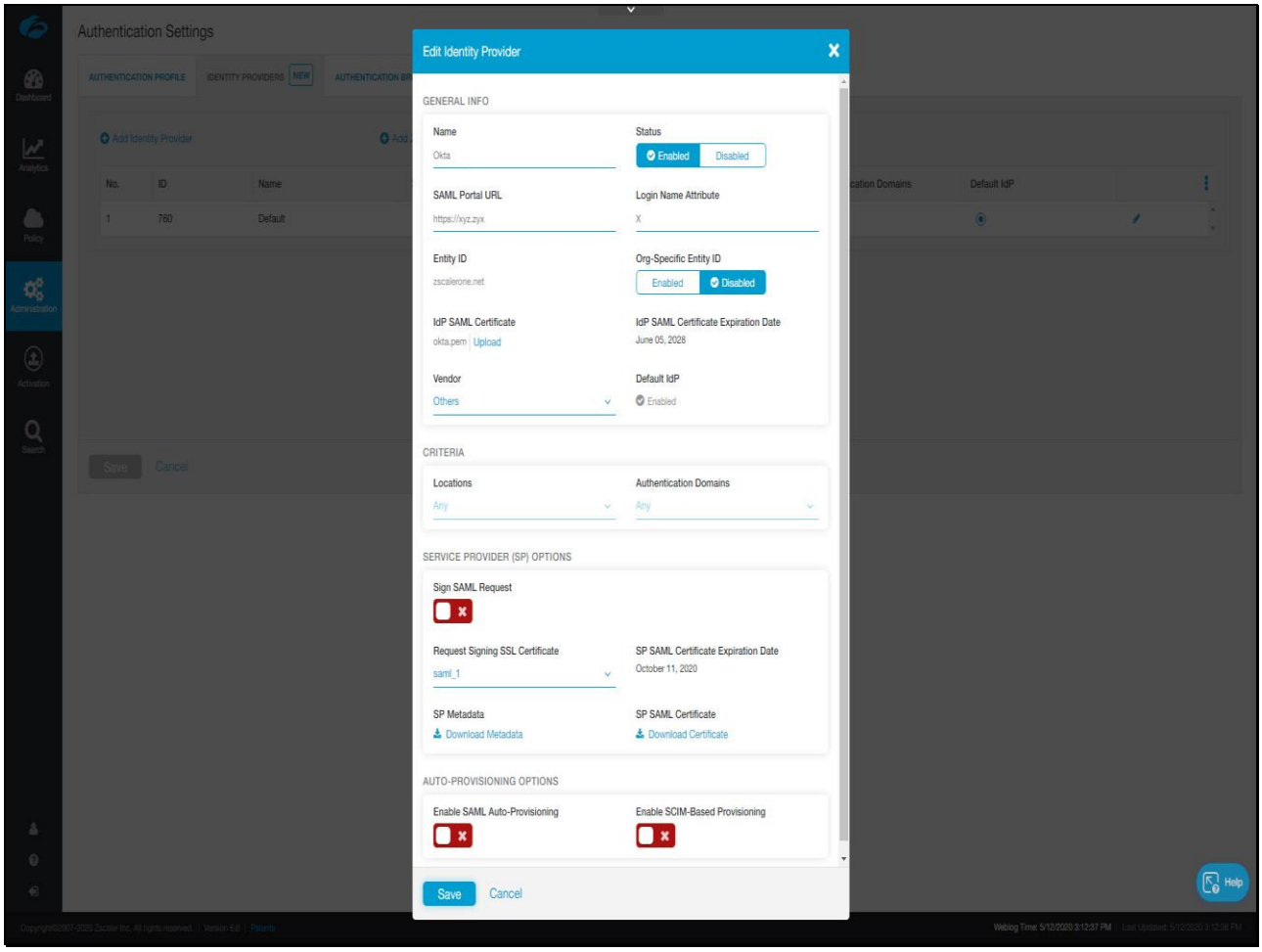
Slide 58 - Slide 58



Slide notes

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

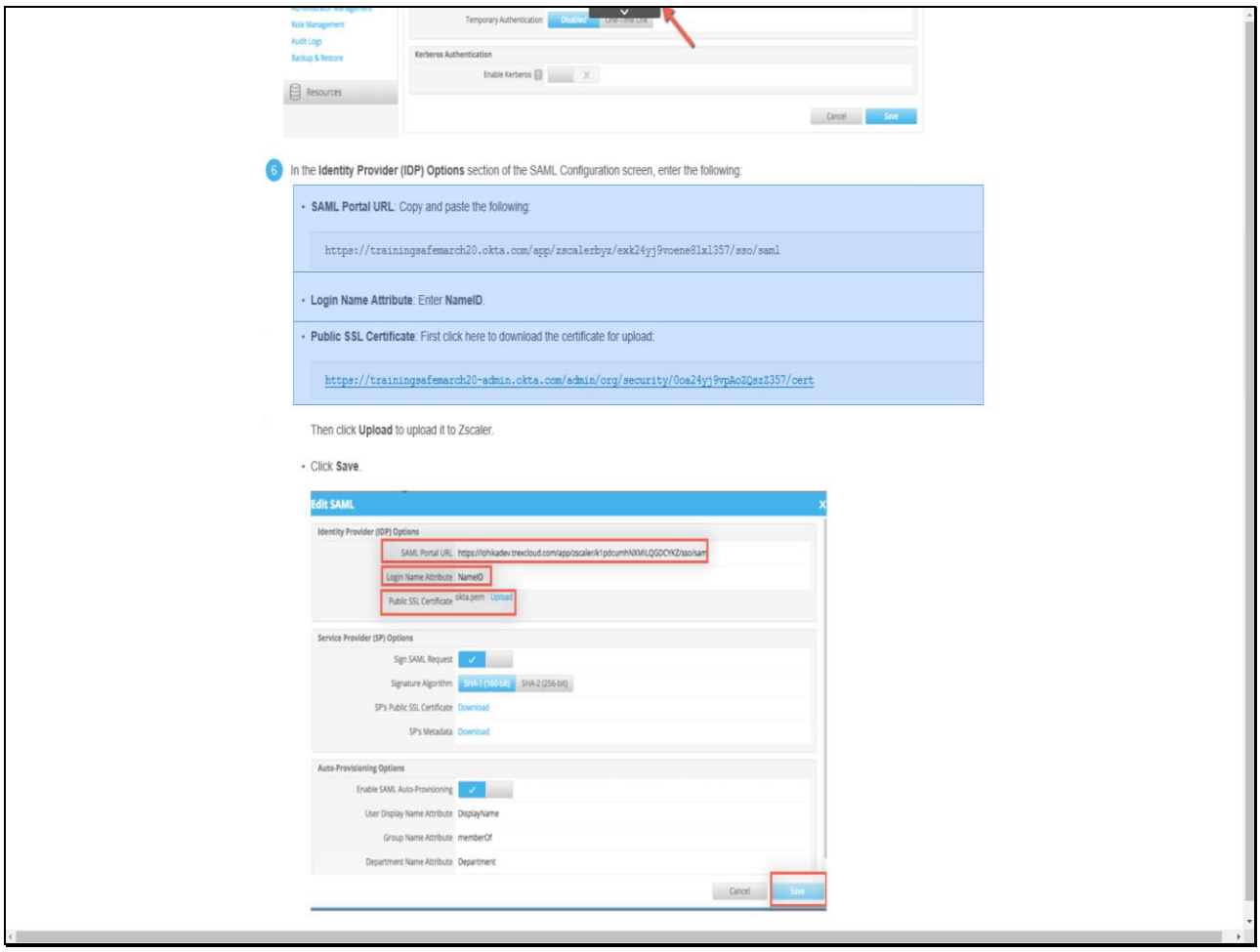
Slide 60 - Slide 60



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.

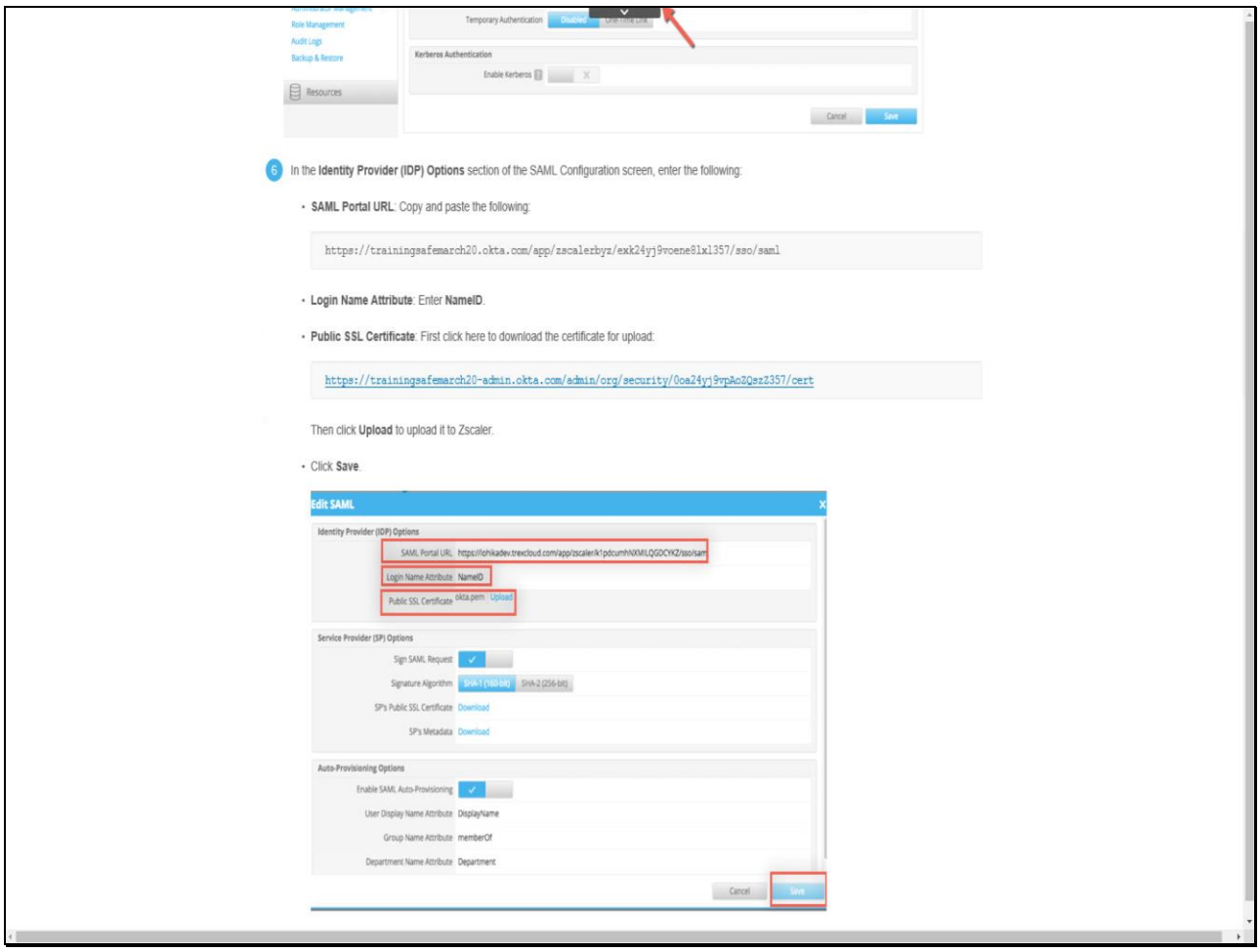
Slide 61 - Slide 61



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**.

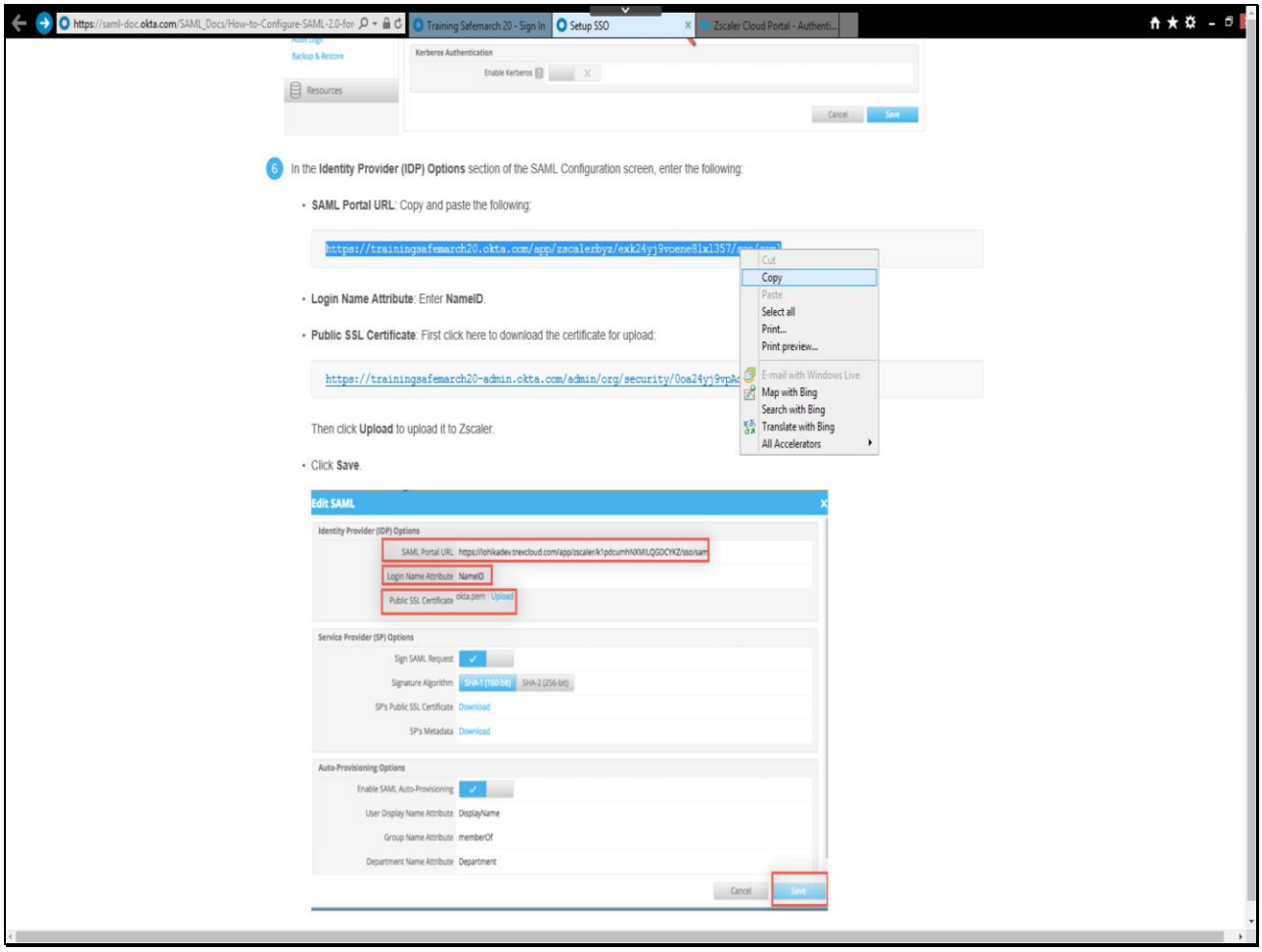
Slide 62 - Slide 62



Slide notes

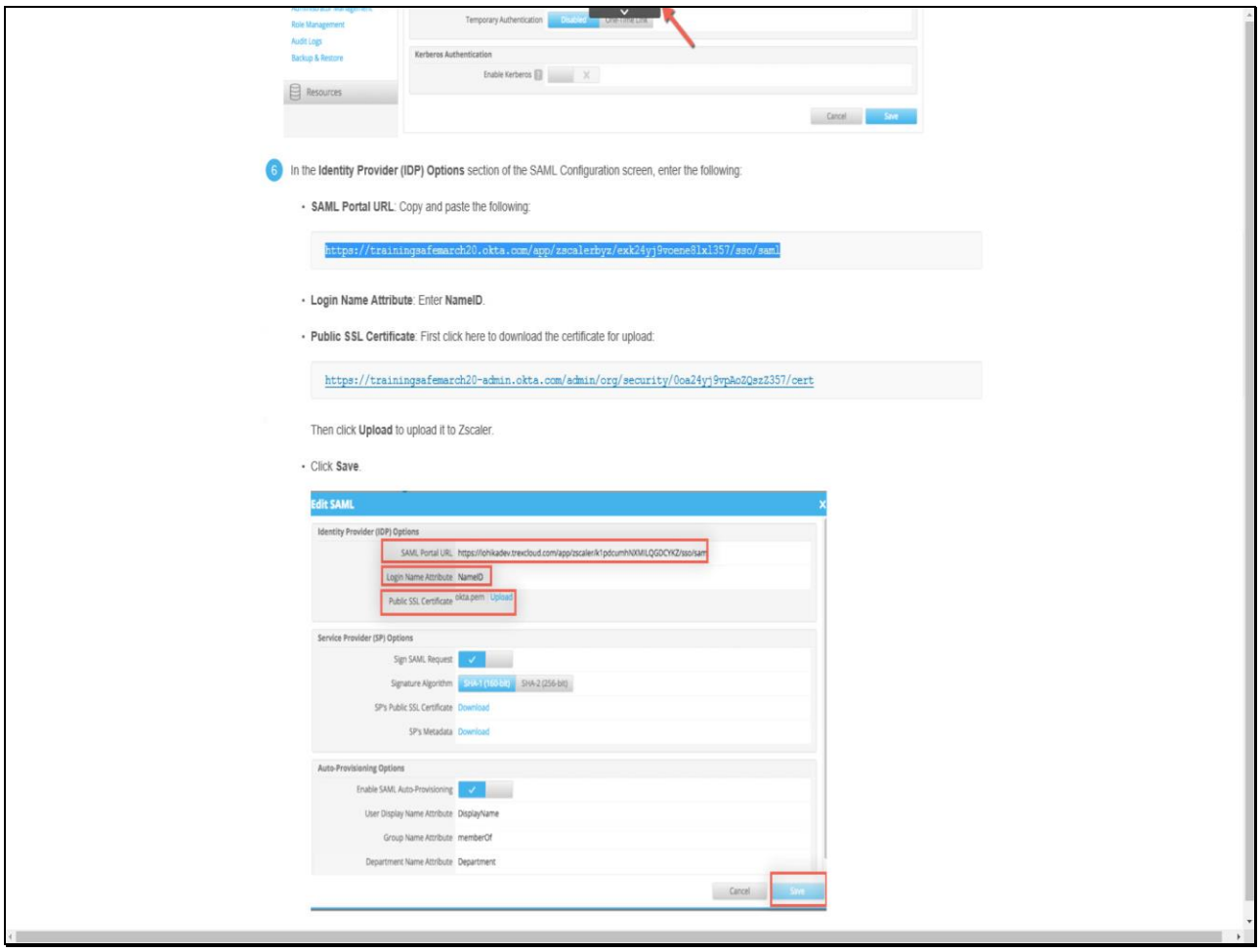
Begin by copying and pasting the **SAML Portal URL** and the **Login Name Attribute**, which is **NameID**.

Slide 65 - Slide 65



Slide notes

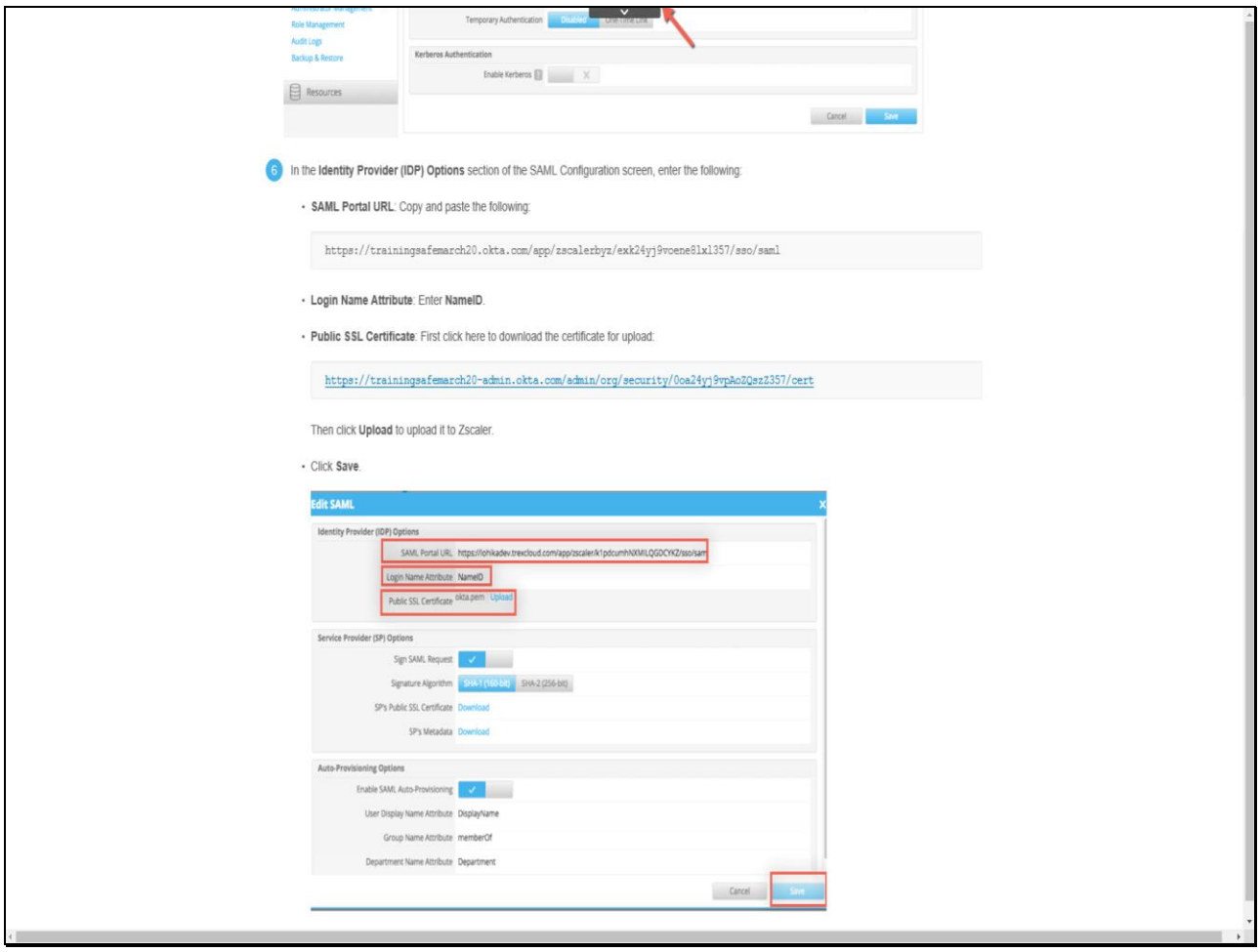
Slide 66 - Slide 66



Slide notes

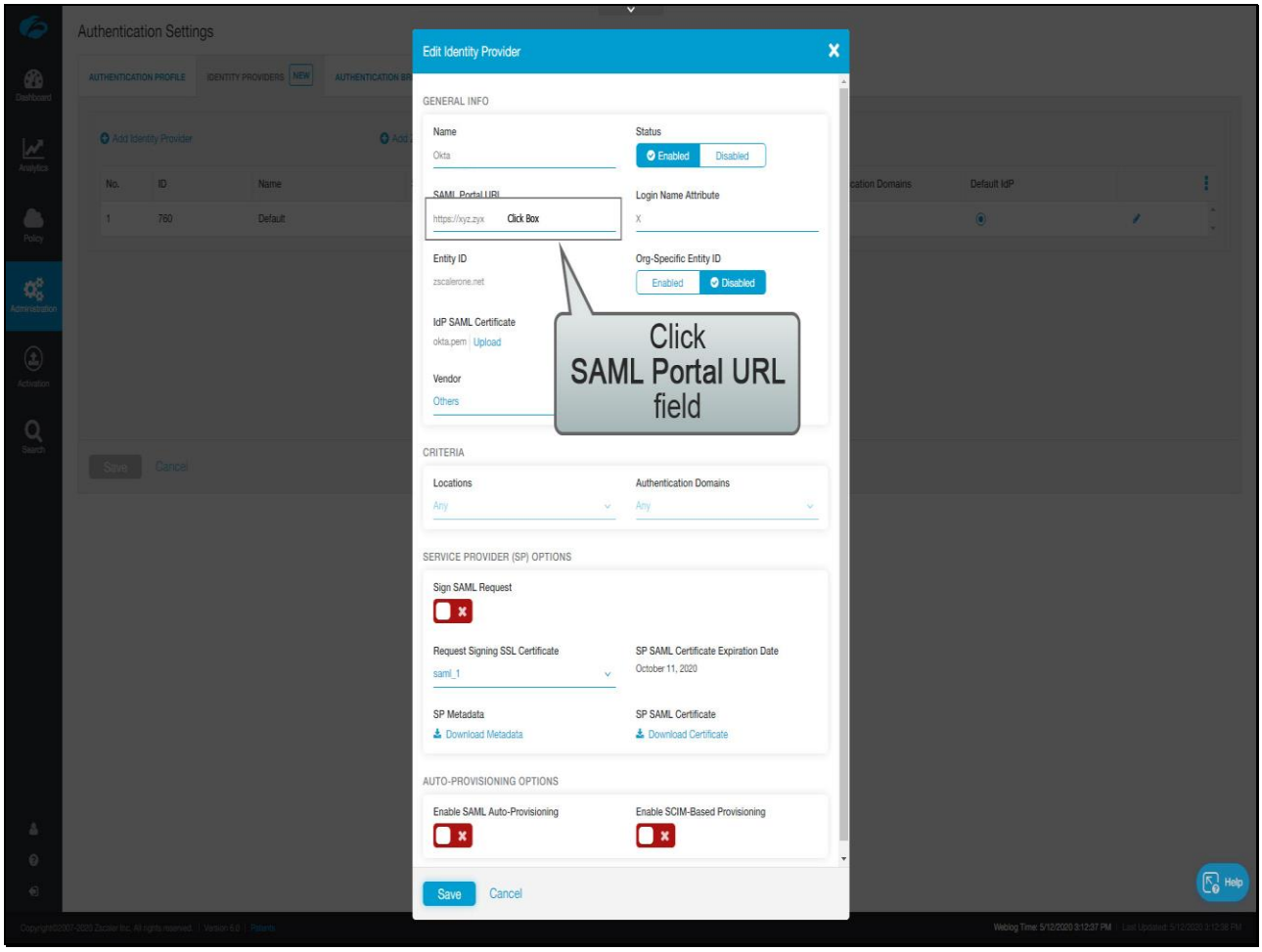
Then click the link to download a copy of the SSL certificate.

Slide 70 - Slide 70



Slide notes

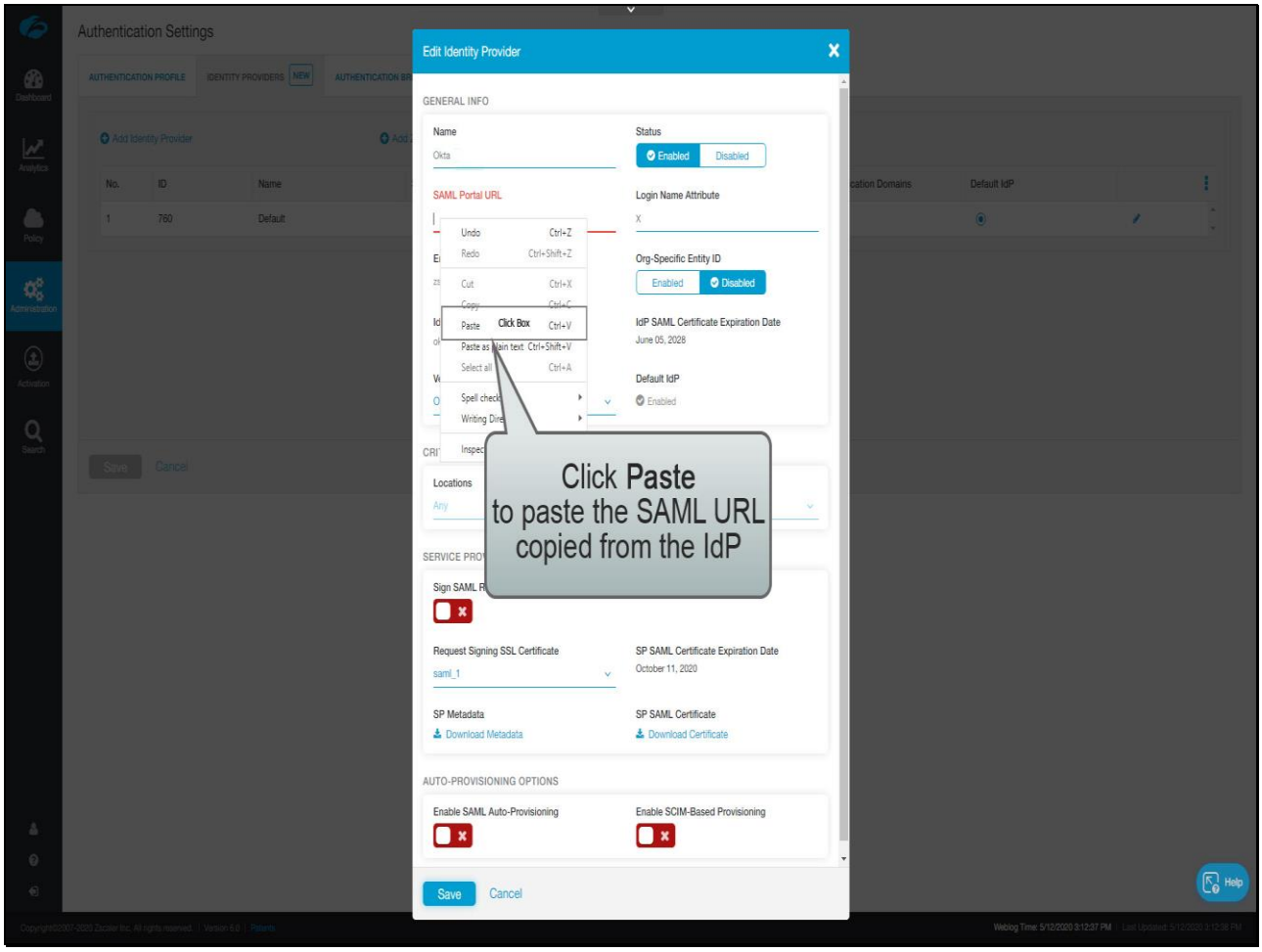
Slide 71 - Slide 71



Slide notes

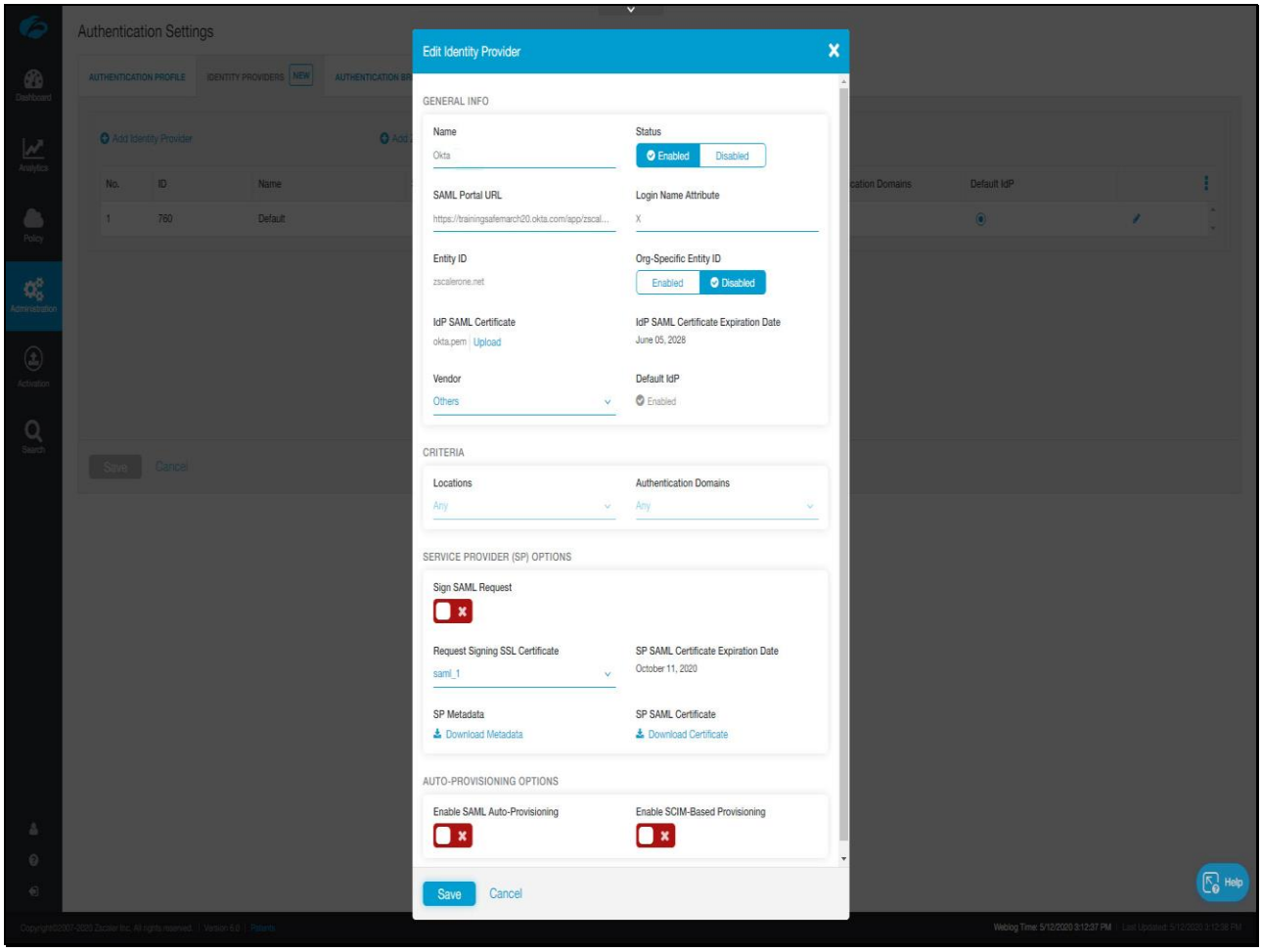
Paste in the SAML Portal URL you copied from the IdP.

Slide 72 - Slide 72



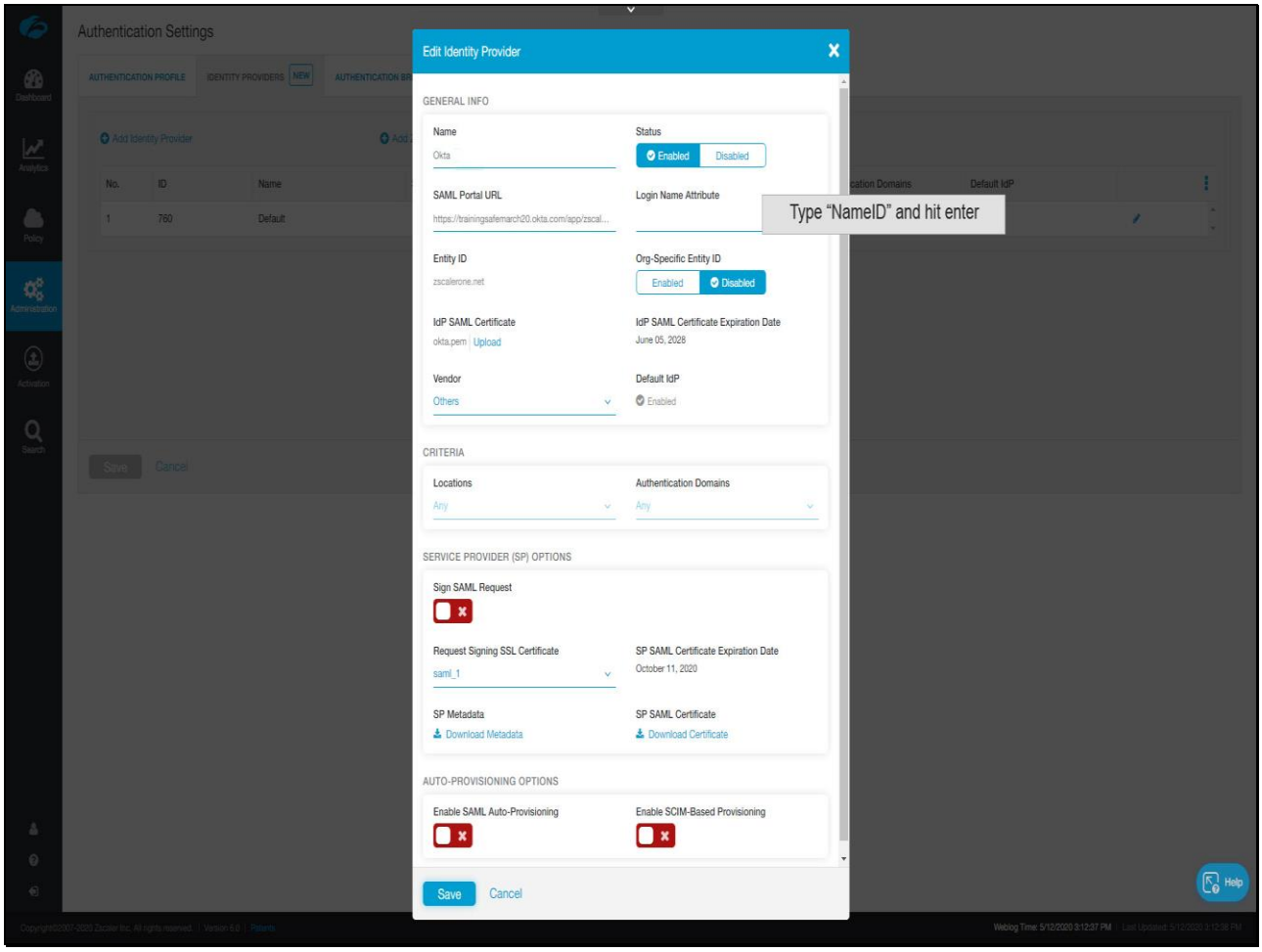
Slide notes

Slide 73 - Slide 73



Slide notes

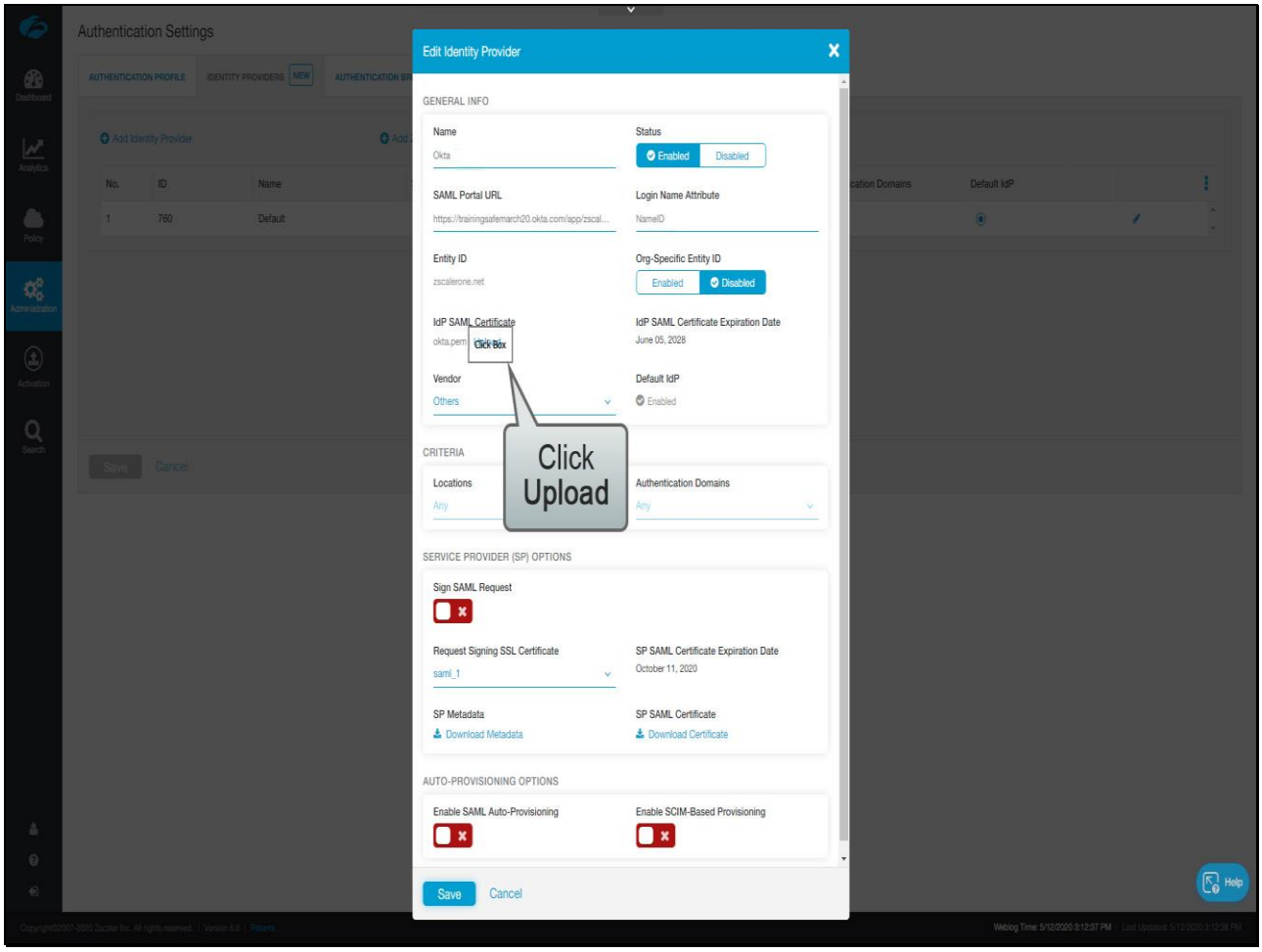
Slide 74 - Slide 74



Slide notes

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

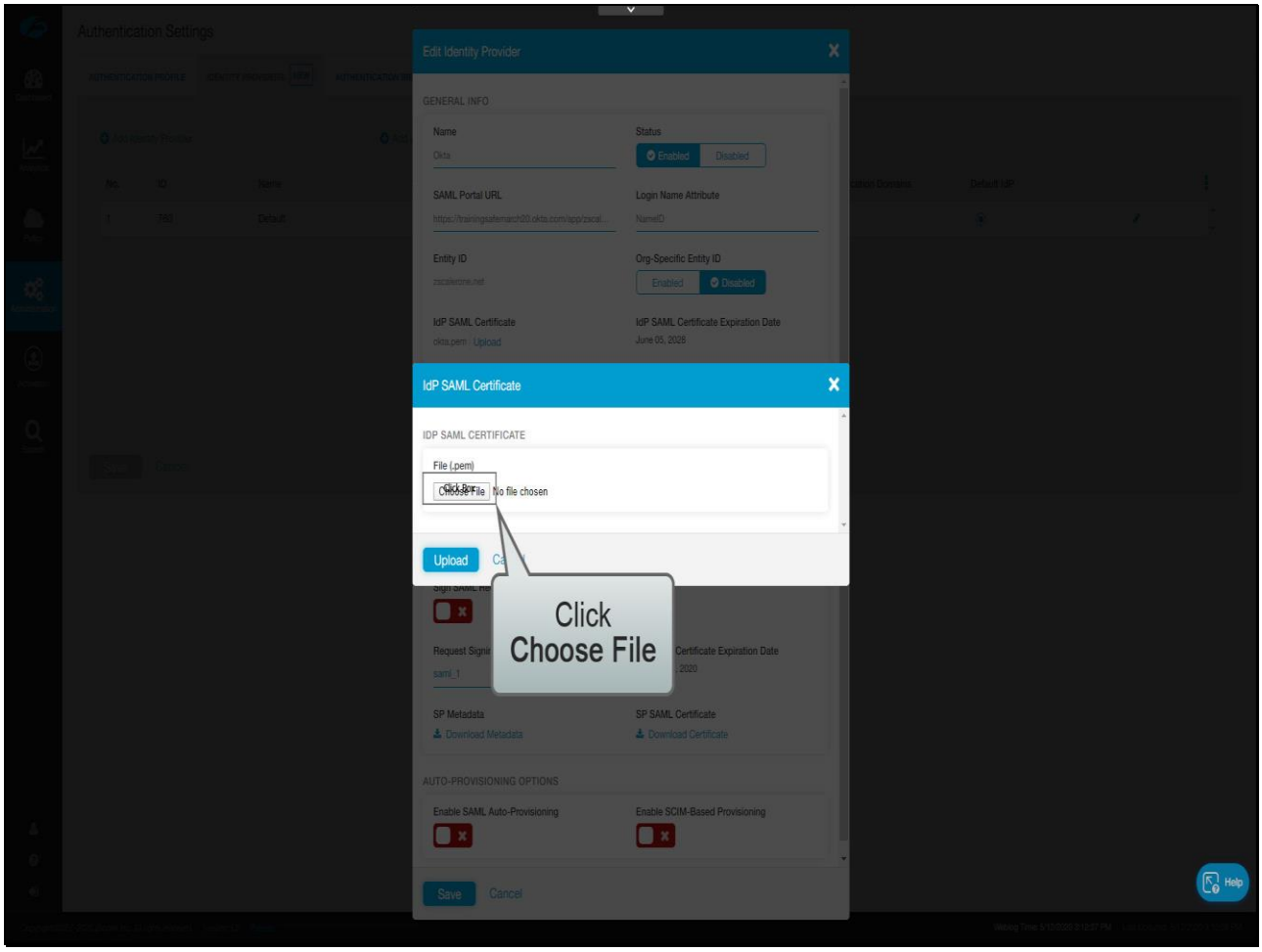
Slide 75 - Slide 75



Slide notes

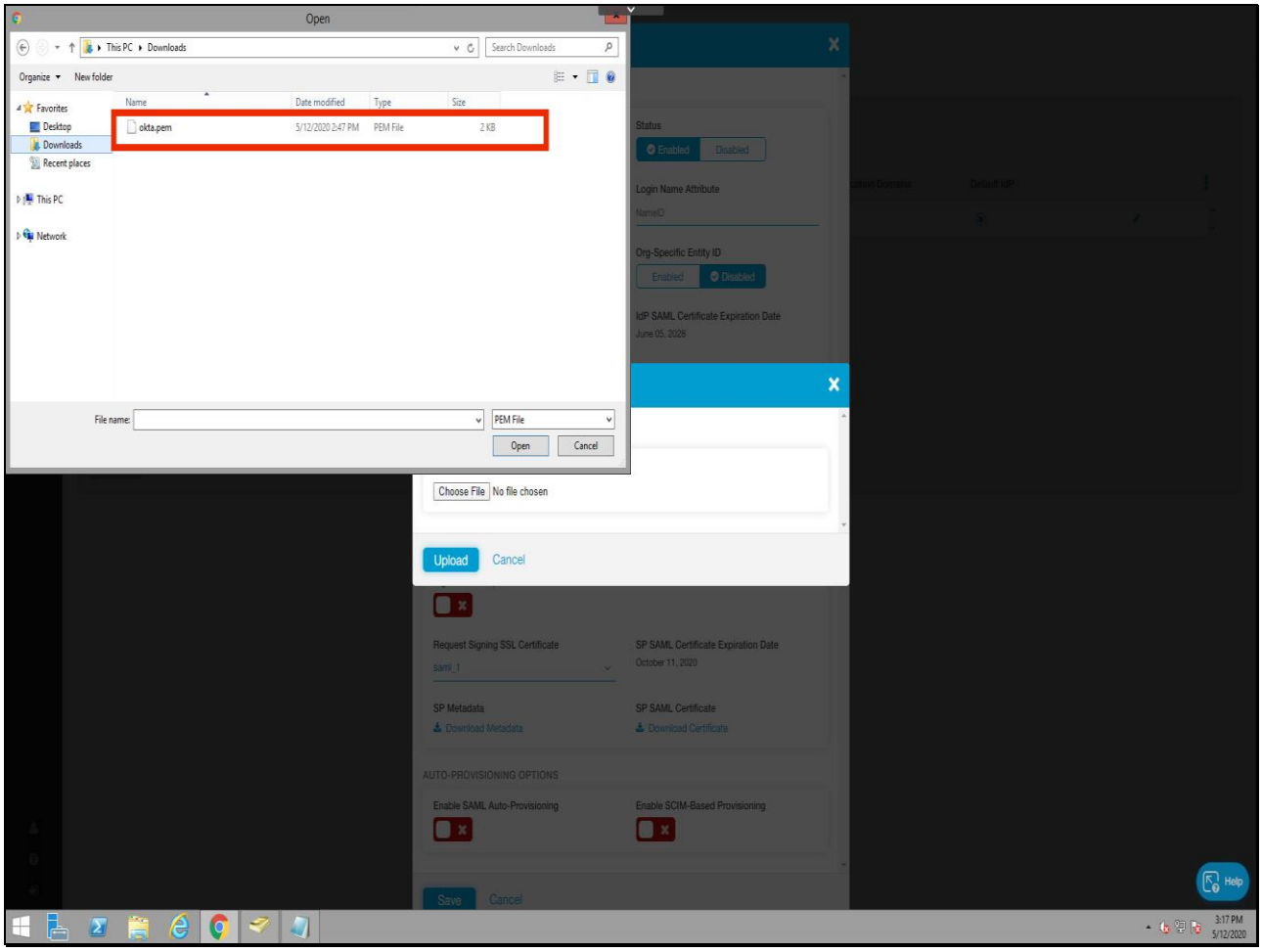
Now let's upload the Okta **Public SSL Certificate** we downloaded at the beginning of the configuration demonstration.

Slide 76 - Slide 76



Slide notes

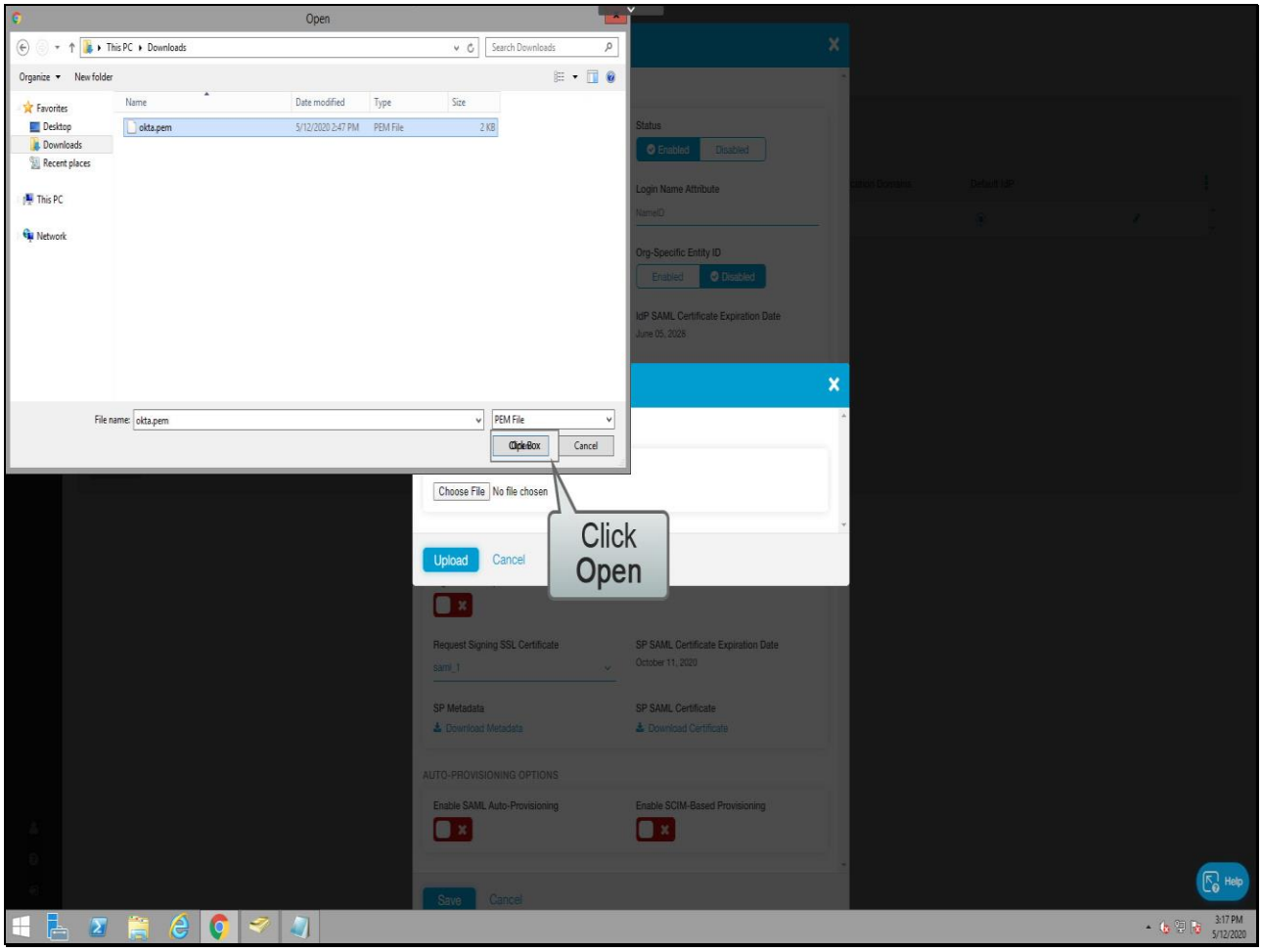
Slide 77 - Slide 77



Slide notes

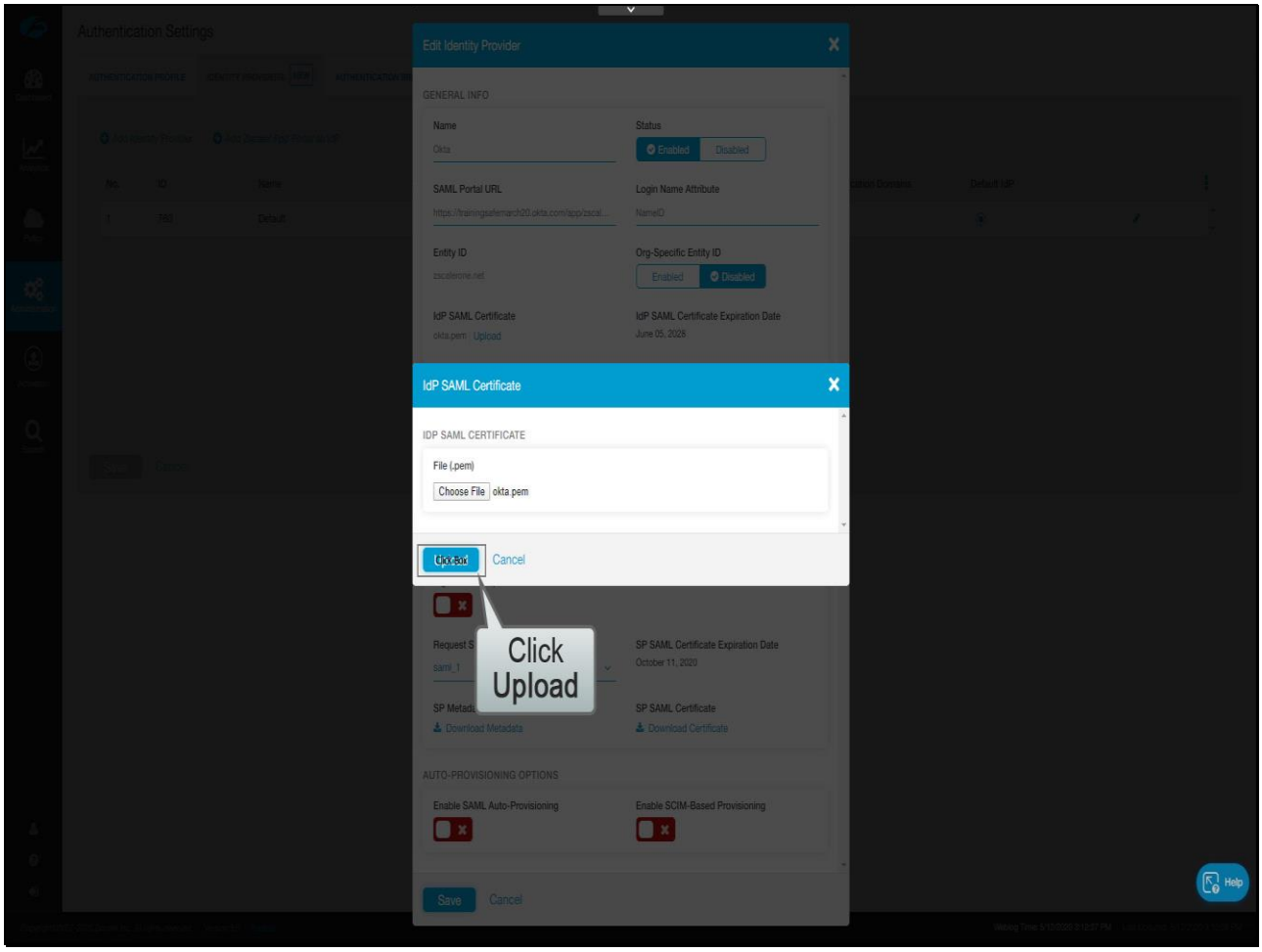
Highlight the file **okta.pem** then click **Open**.

Slide 78 - Slide 78



Slide notes

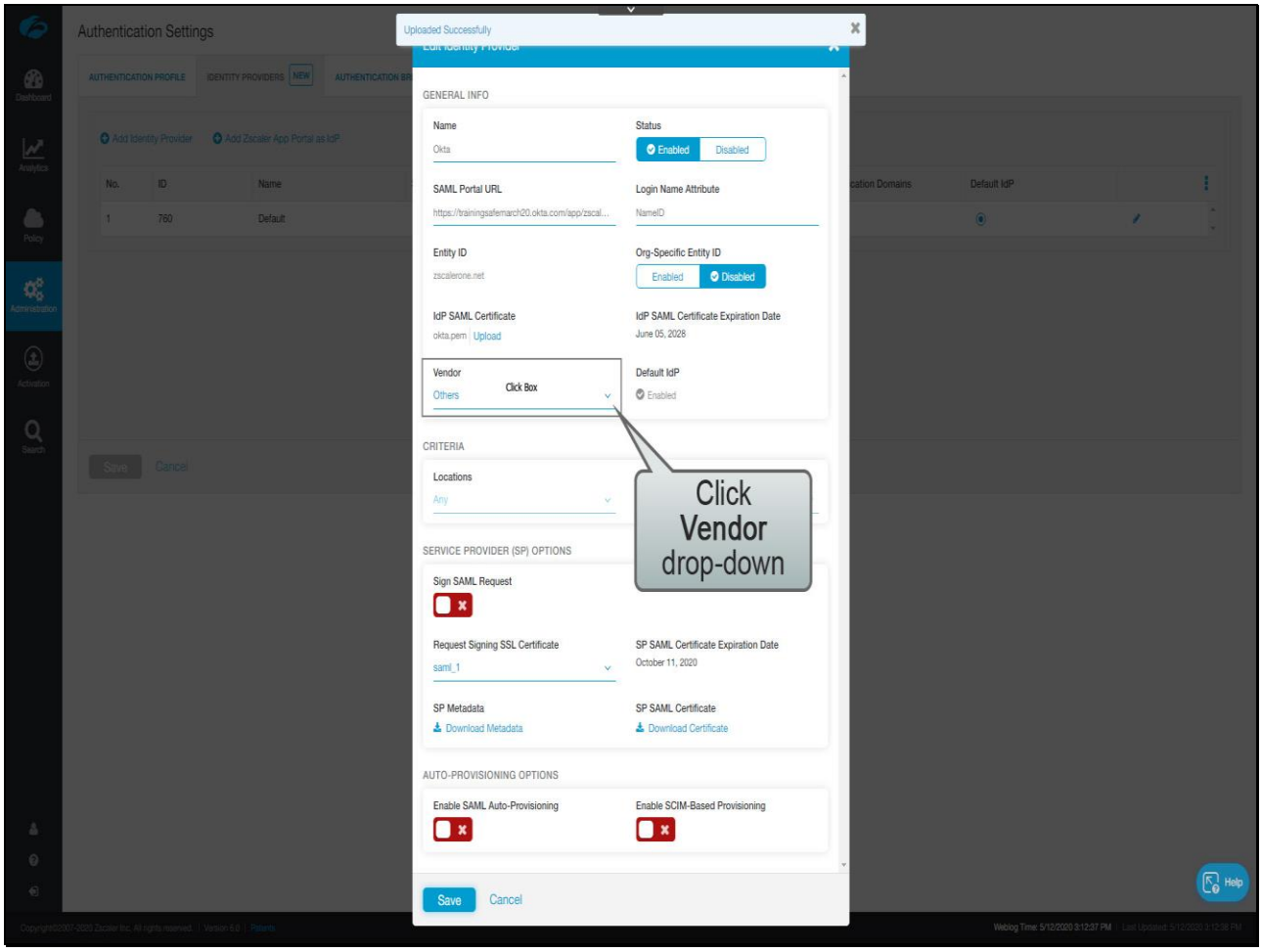
Slide 79 - Slide 79



Slide notes

Then **Upload**.

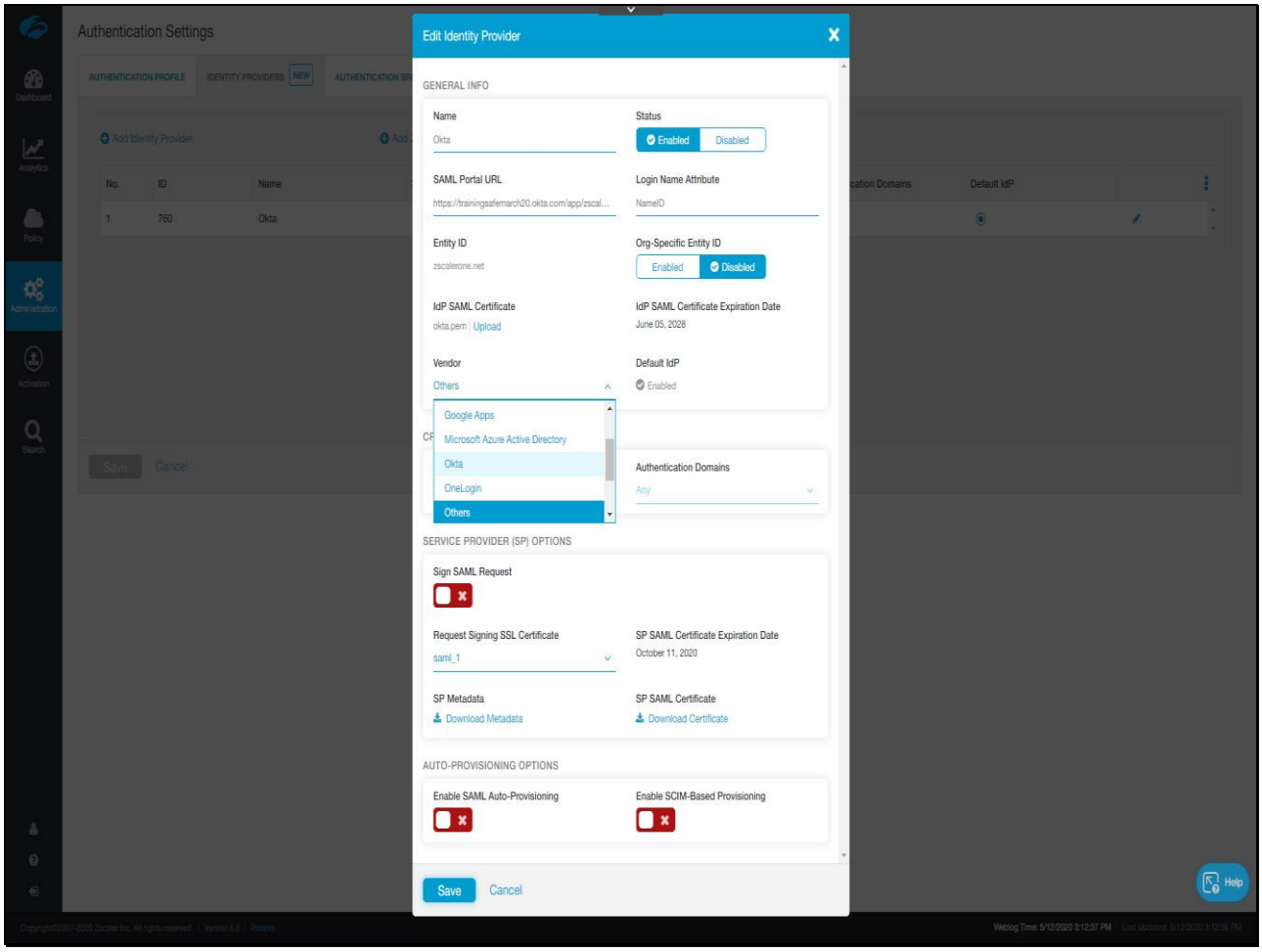
Slide 80 - Slide 80



Slide notes

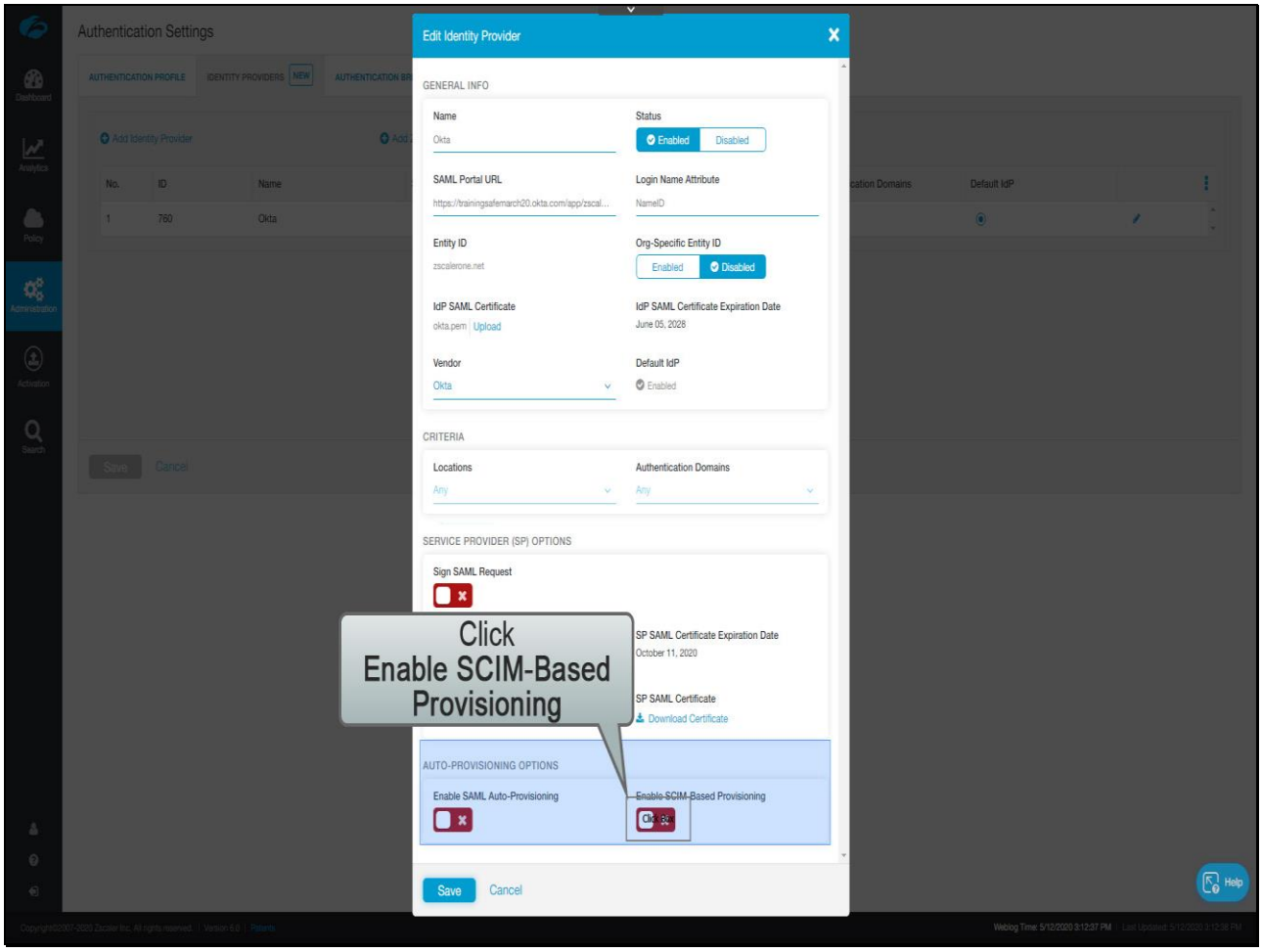
Select the IdP from the **Vendors** drop-down.

Slide 84 - Slide 84



Slide notes

Slide 85 - Slide 85

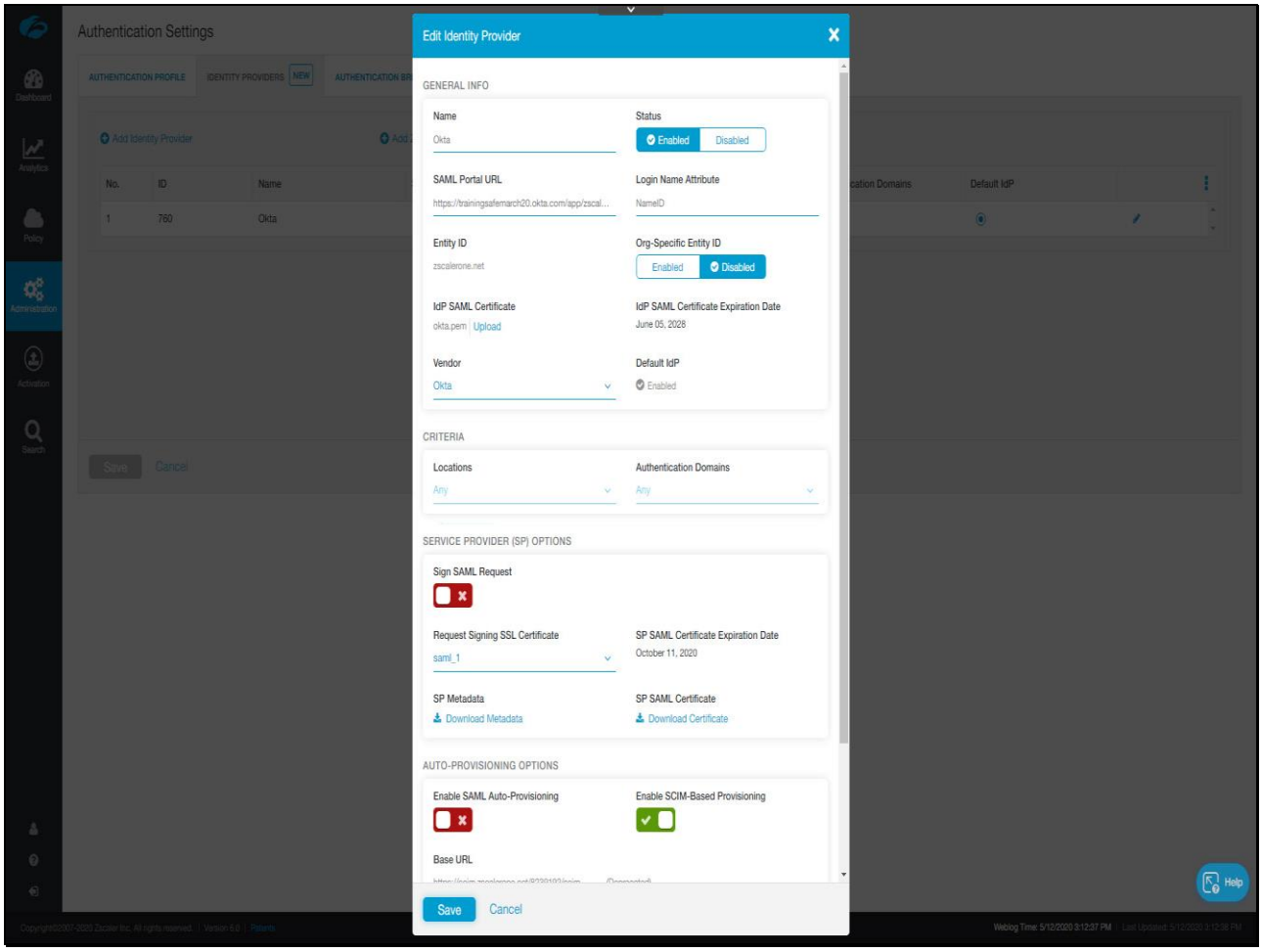


Slide notes

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.

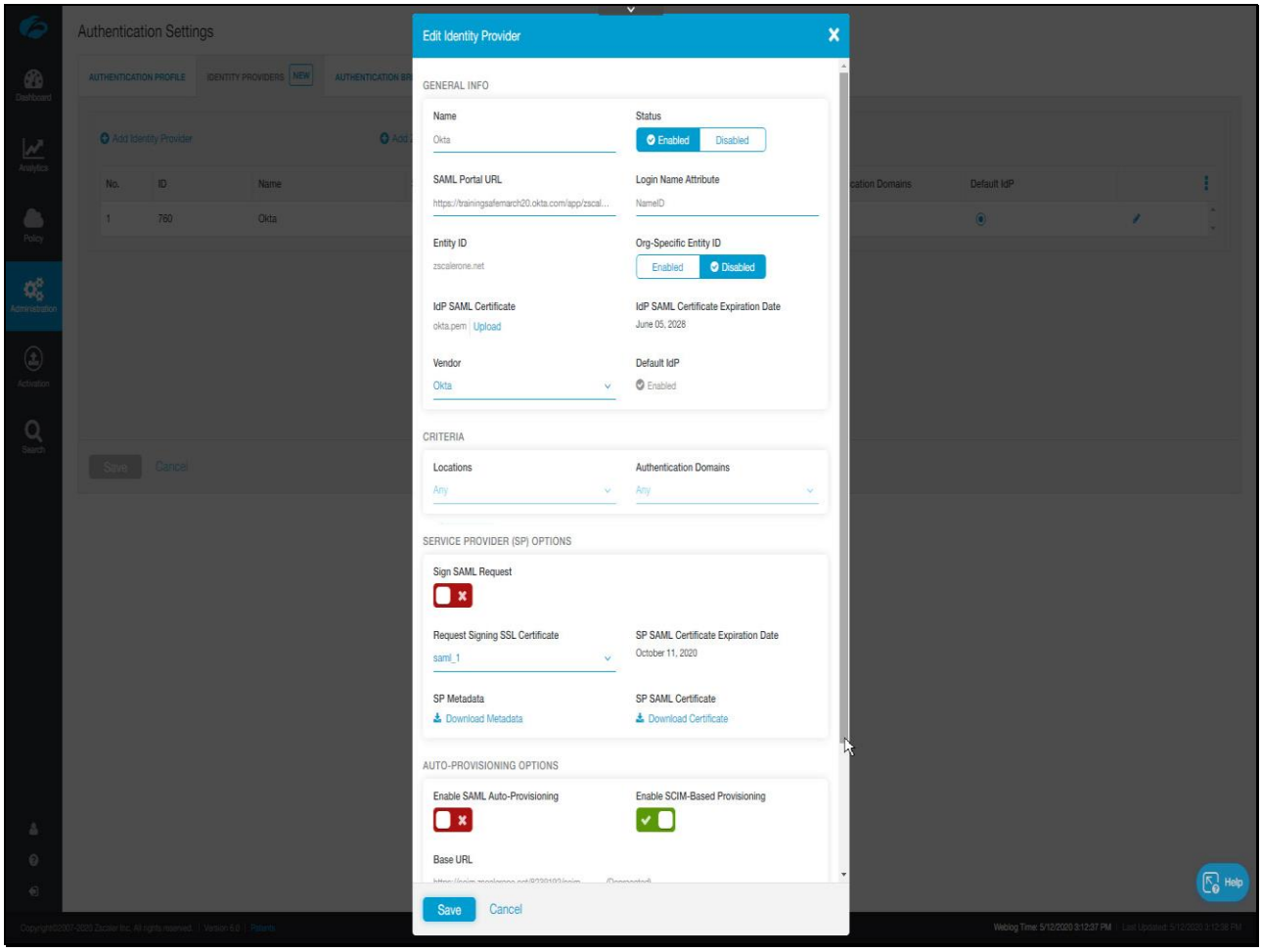
For this example, however, we will leave Auto-Provisioning disabled and we will focus on the use and configuration of SCIM. Click **Enable SCIM-Based Provisioning**.

Slide 86 - Slide 86



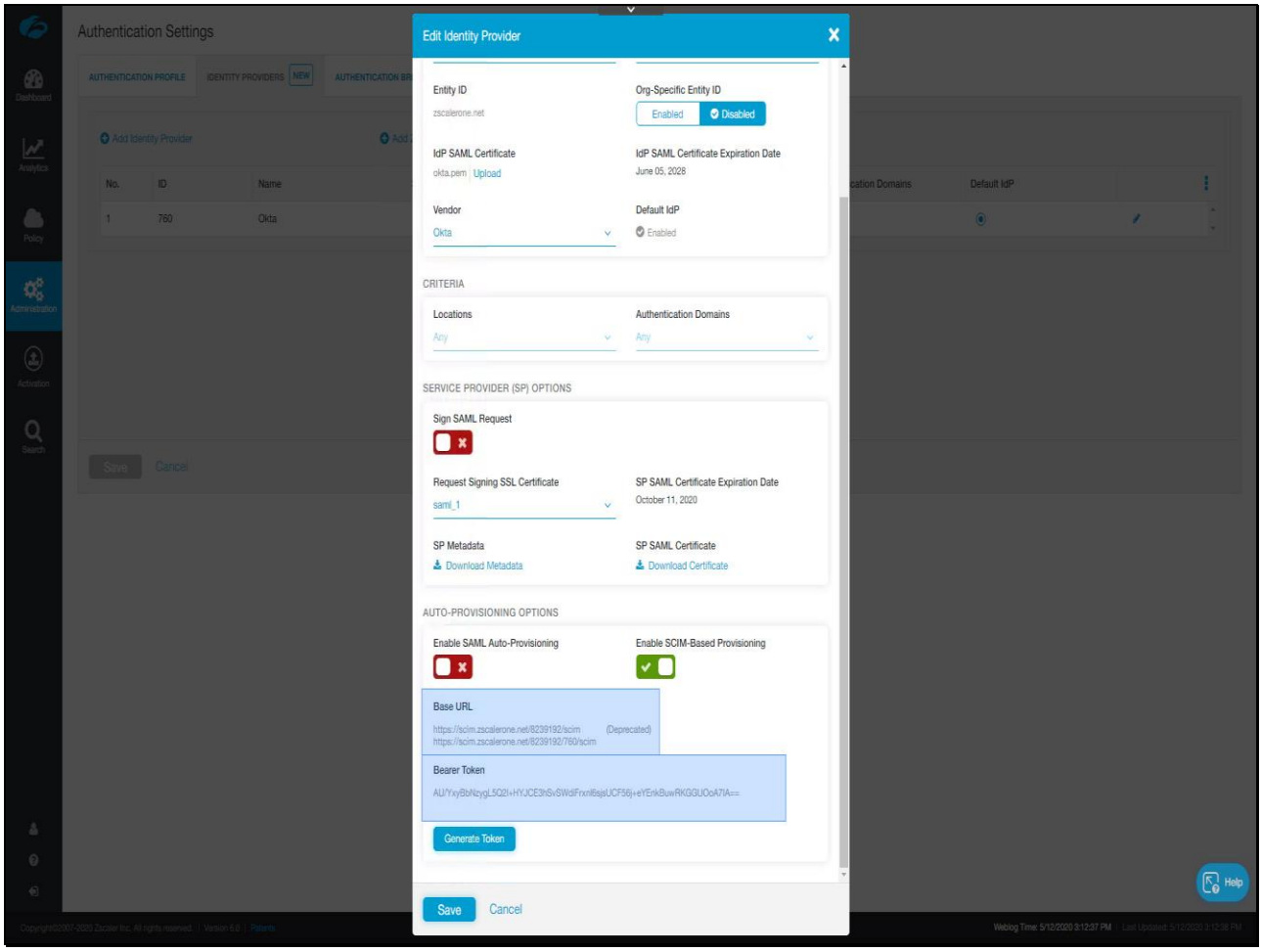
Slide notes

Slide 87 - Slide 87



Slide notes

Slide 88 - Slide 88

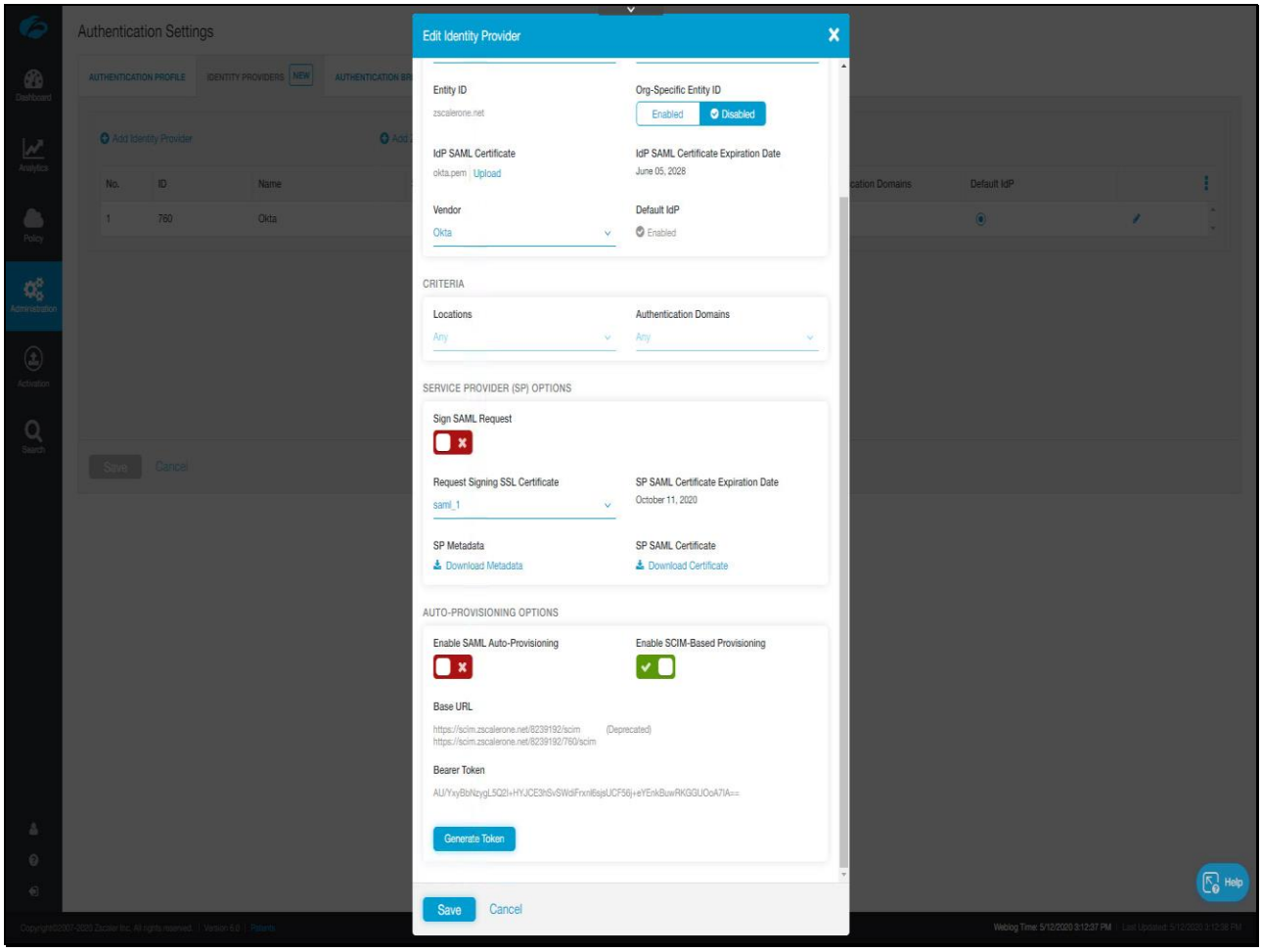


Slide notes

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.

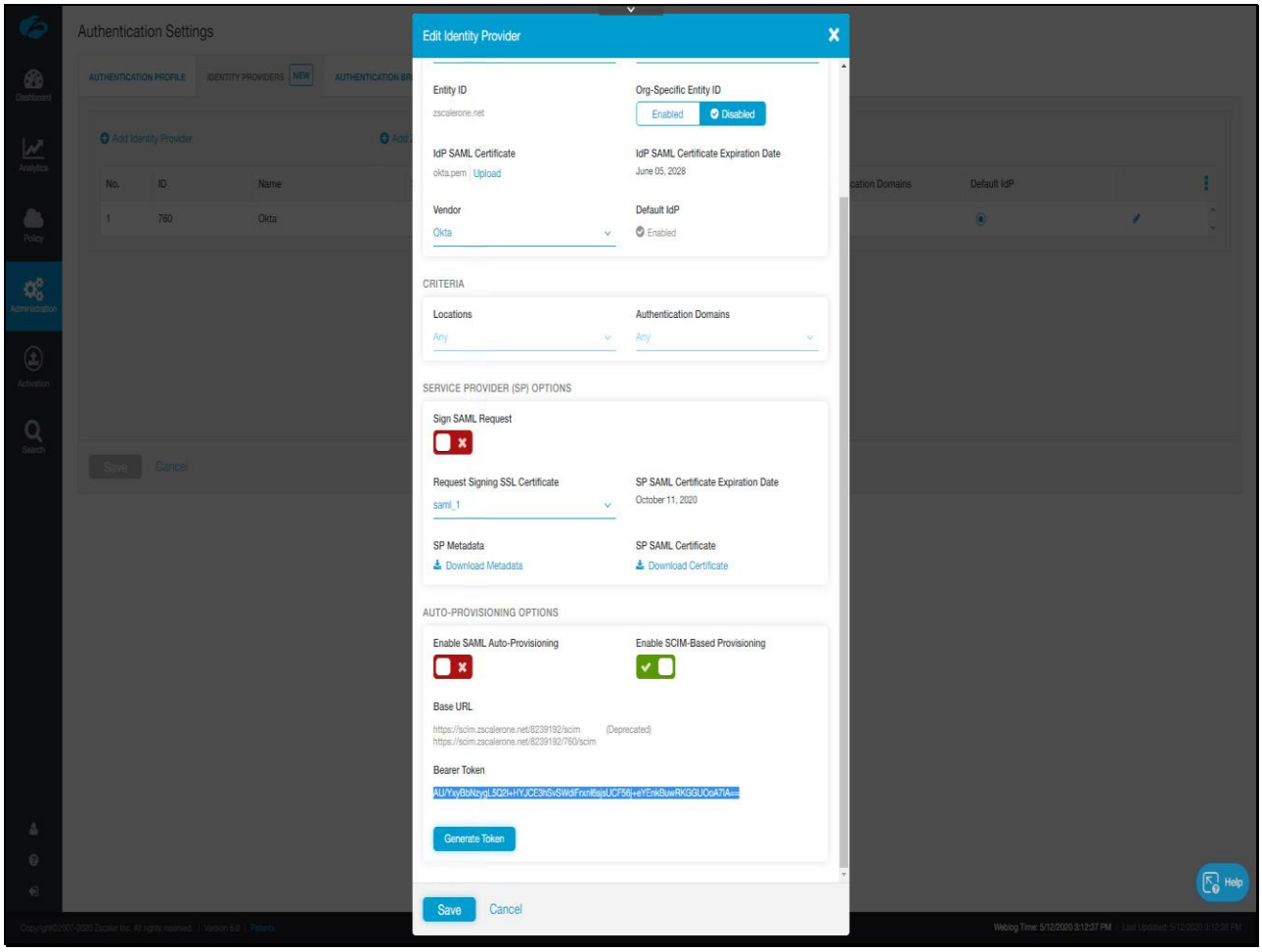
Slide 89 - Slide 89



Slide notes

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

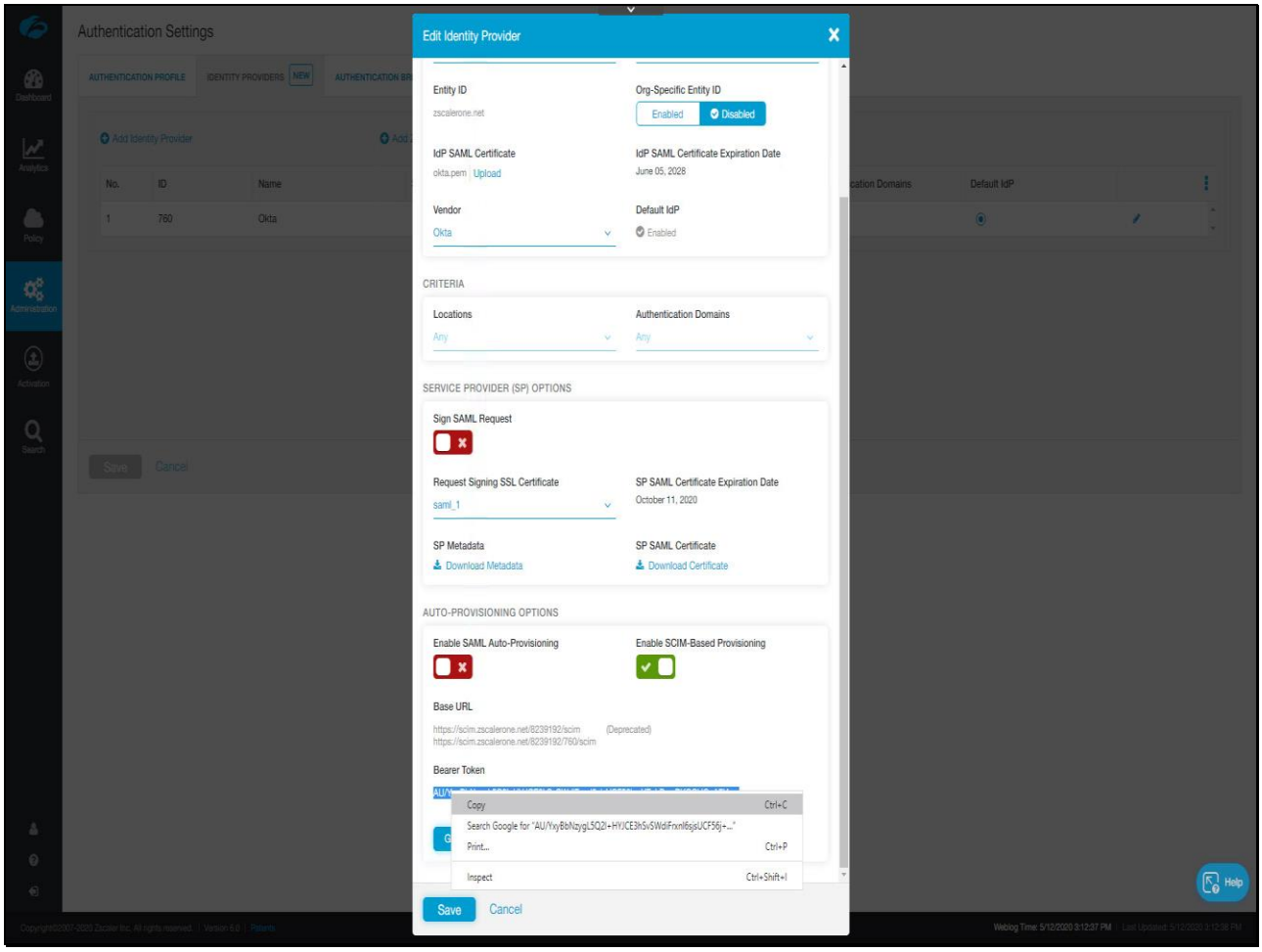
Slide 91 - Slide 91



Slide notes

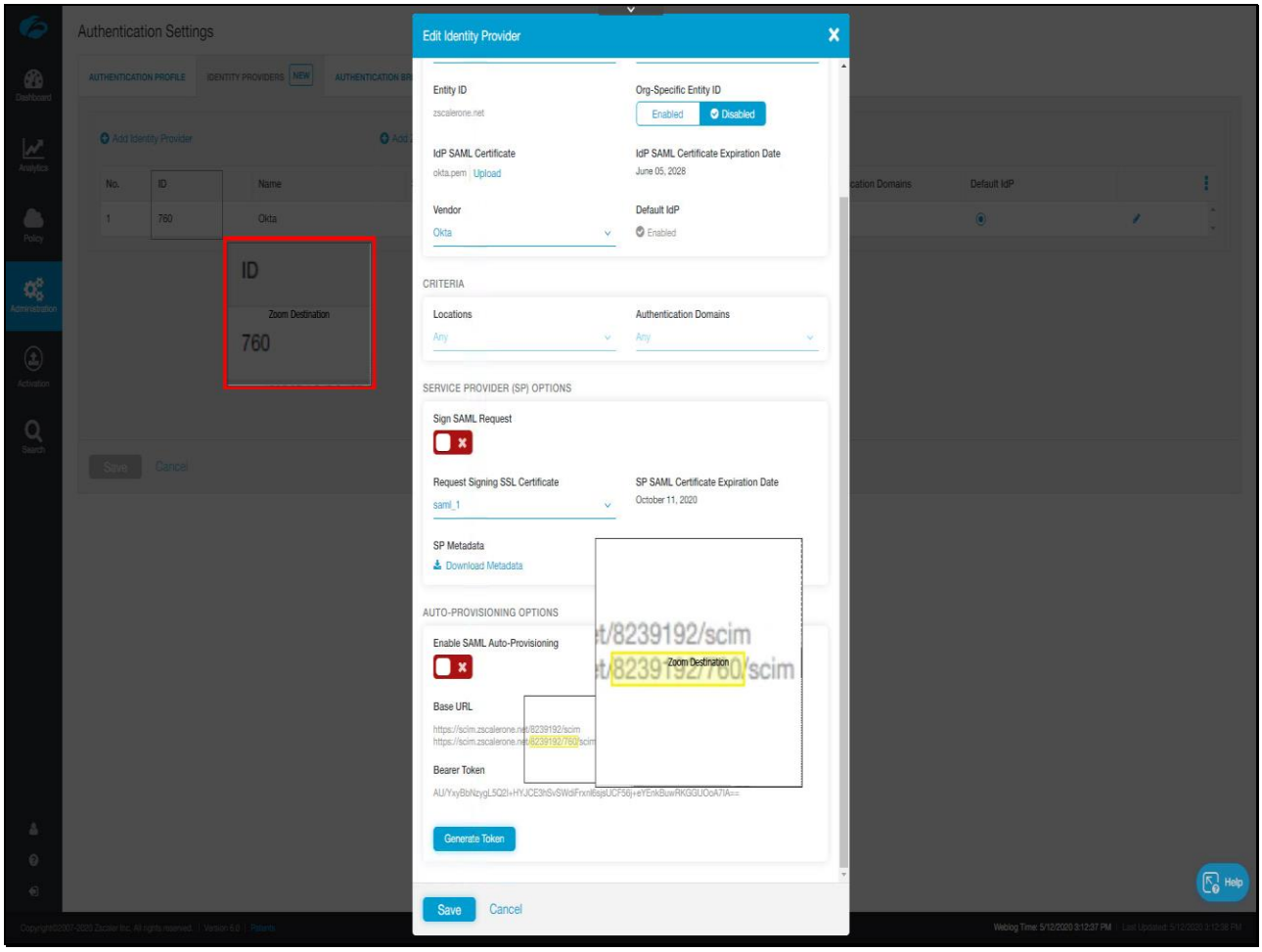
Copy the **Bearer Token** for use in your IdP configuration.

Slide 92 - Slide 92



Slide notes

Slide 93 - Slide 93



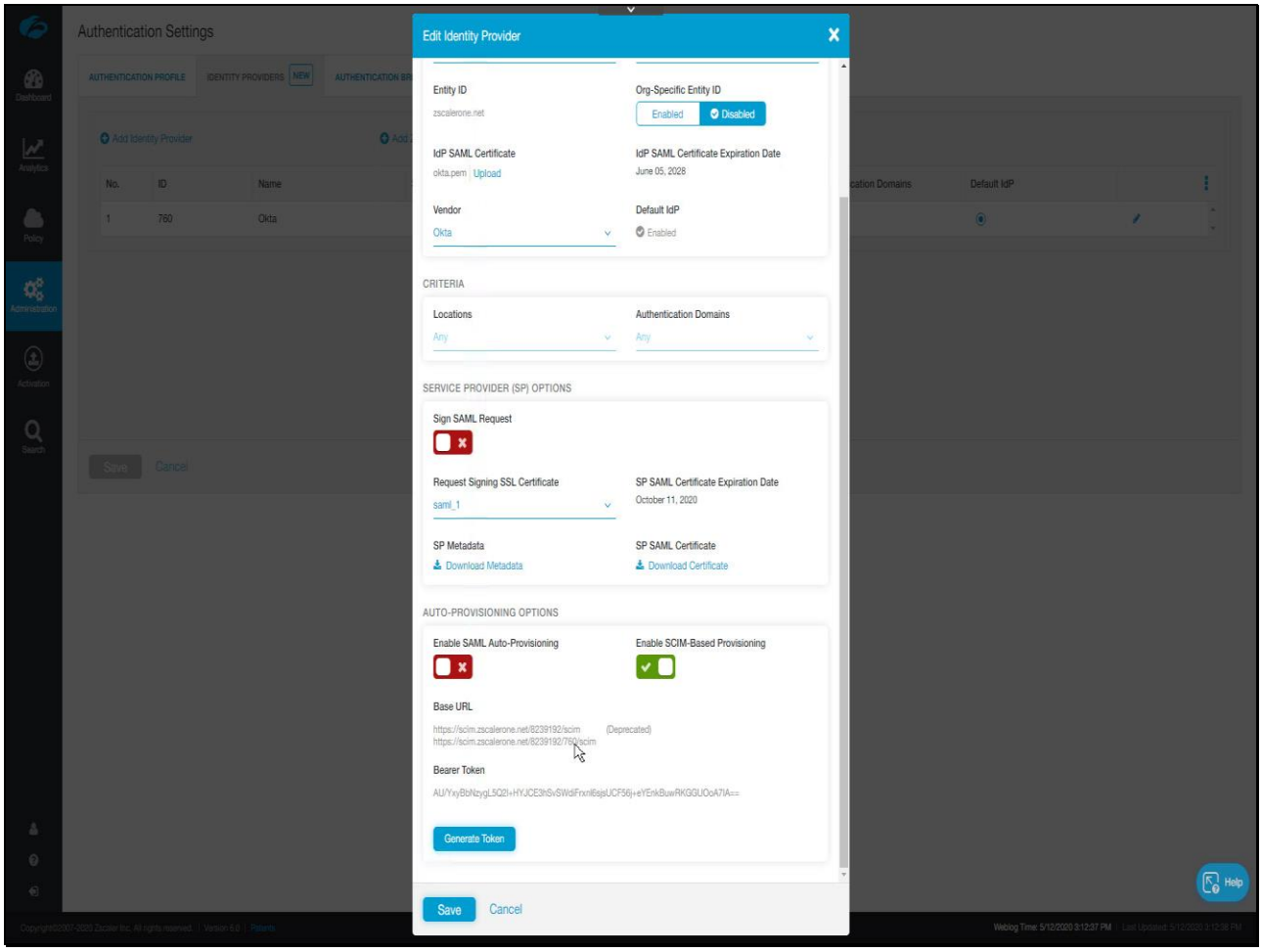
Slide notes

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.

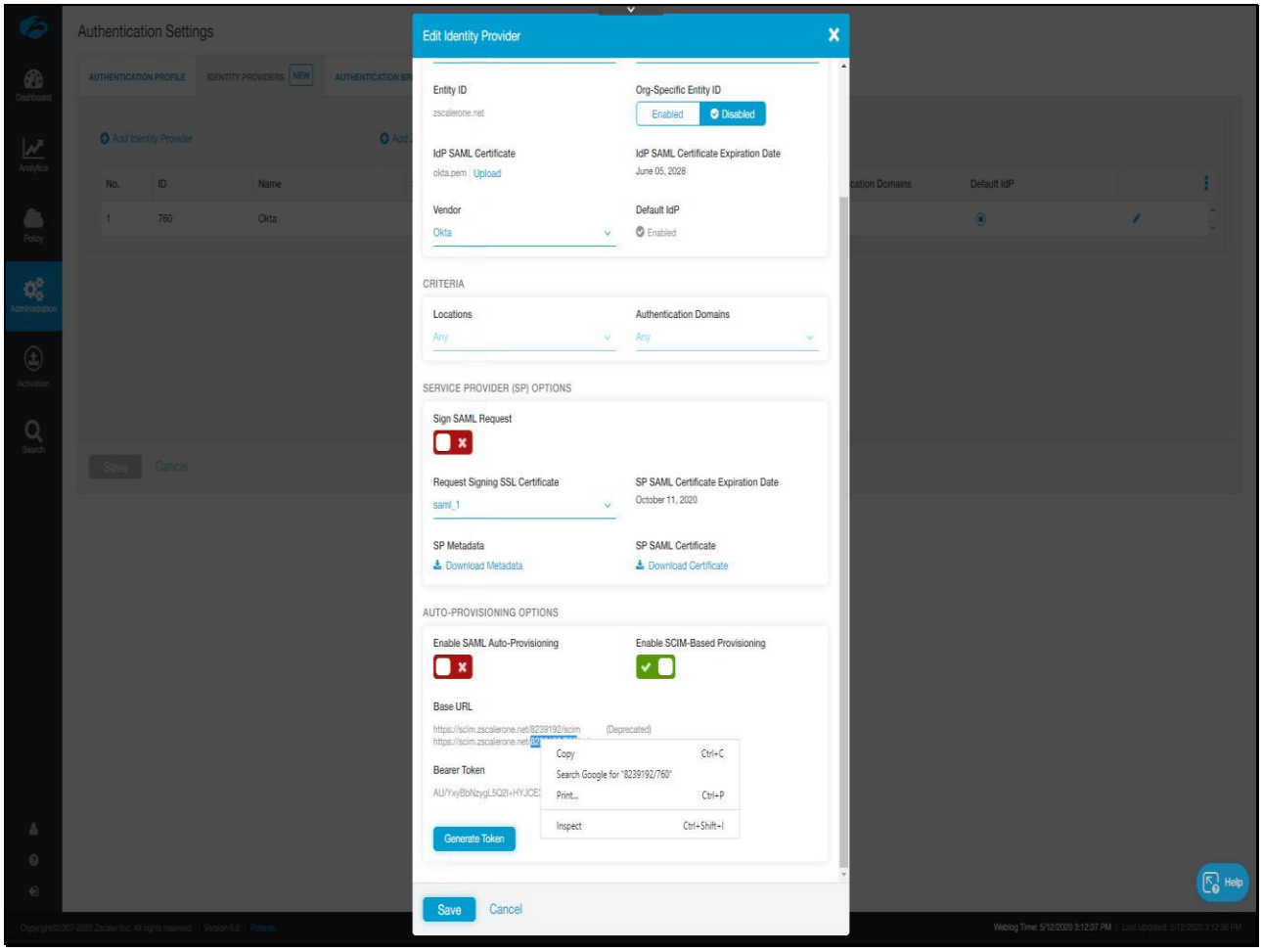
The combination of these values equals the Zscaler ID. You can also see in the Zoom window that, nested within the Base URL is the complete Zscaler ID. So, in this example, you will copy that value and provide it to Okta.

Slide 94 - Slide 94



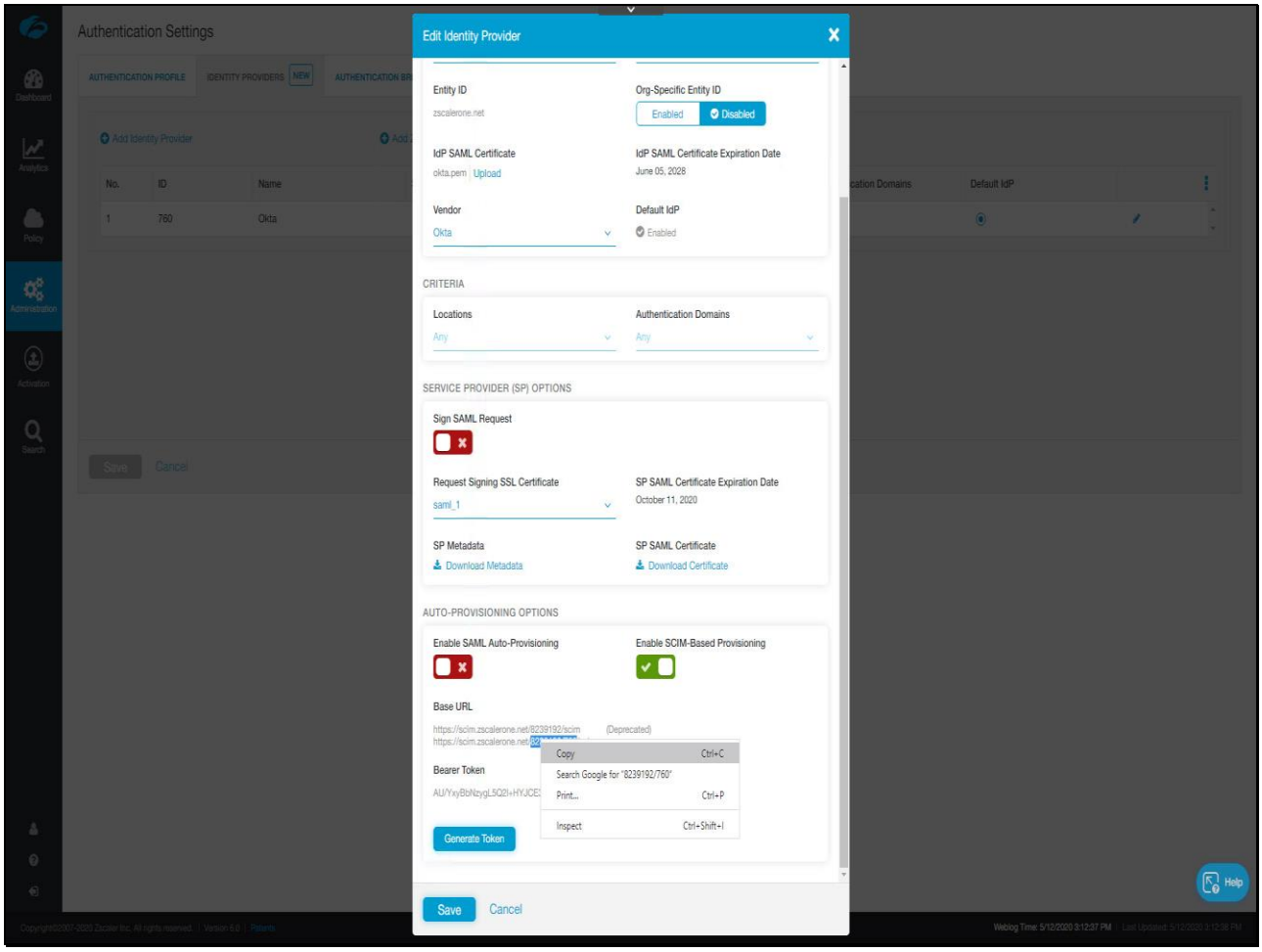
Slide notes

Slide 95 - Slide 95



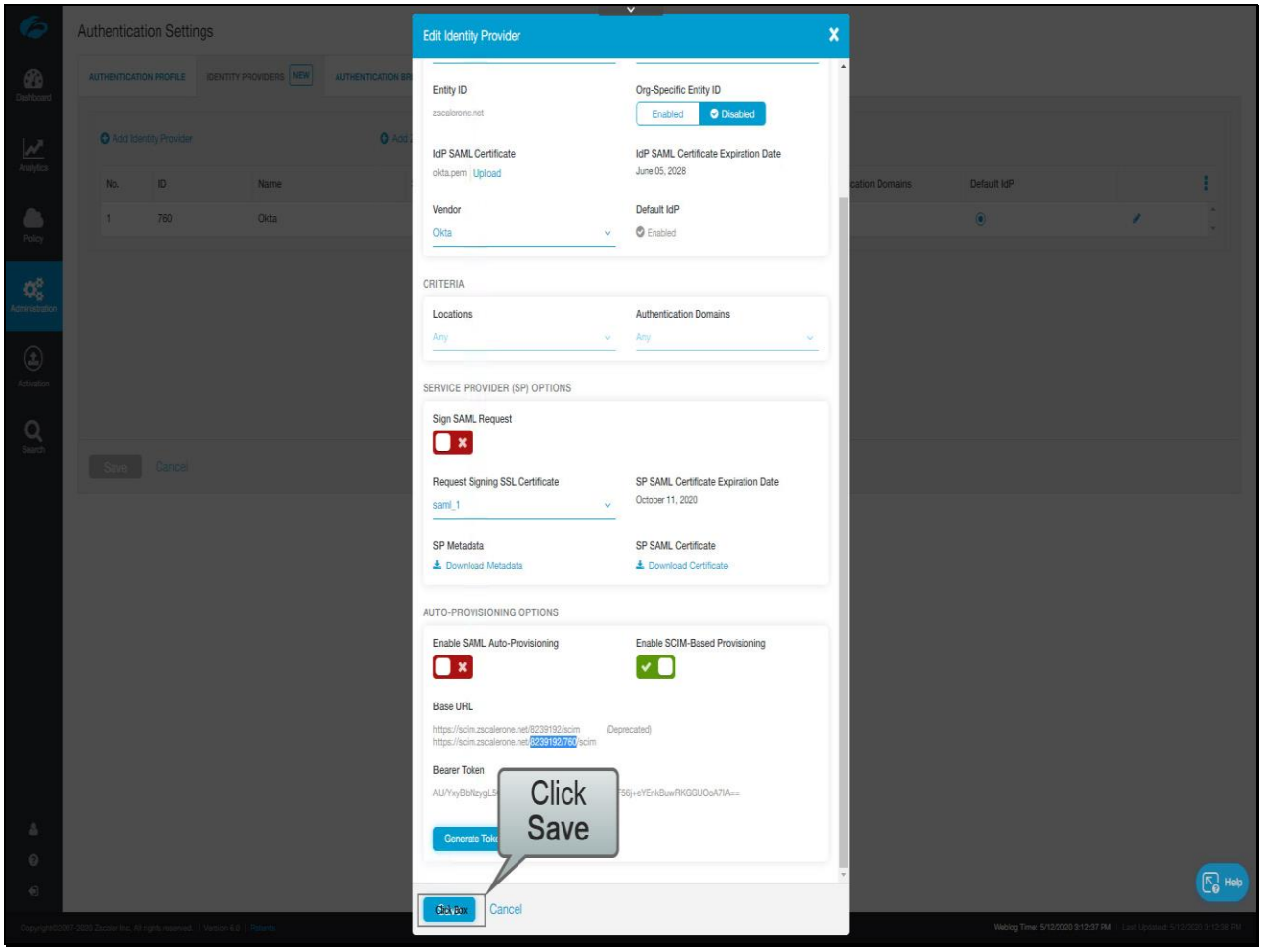
Slide notes

Slide 96 - Slide 96



Slide notes

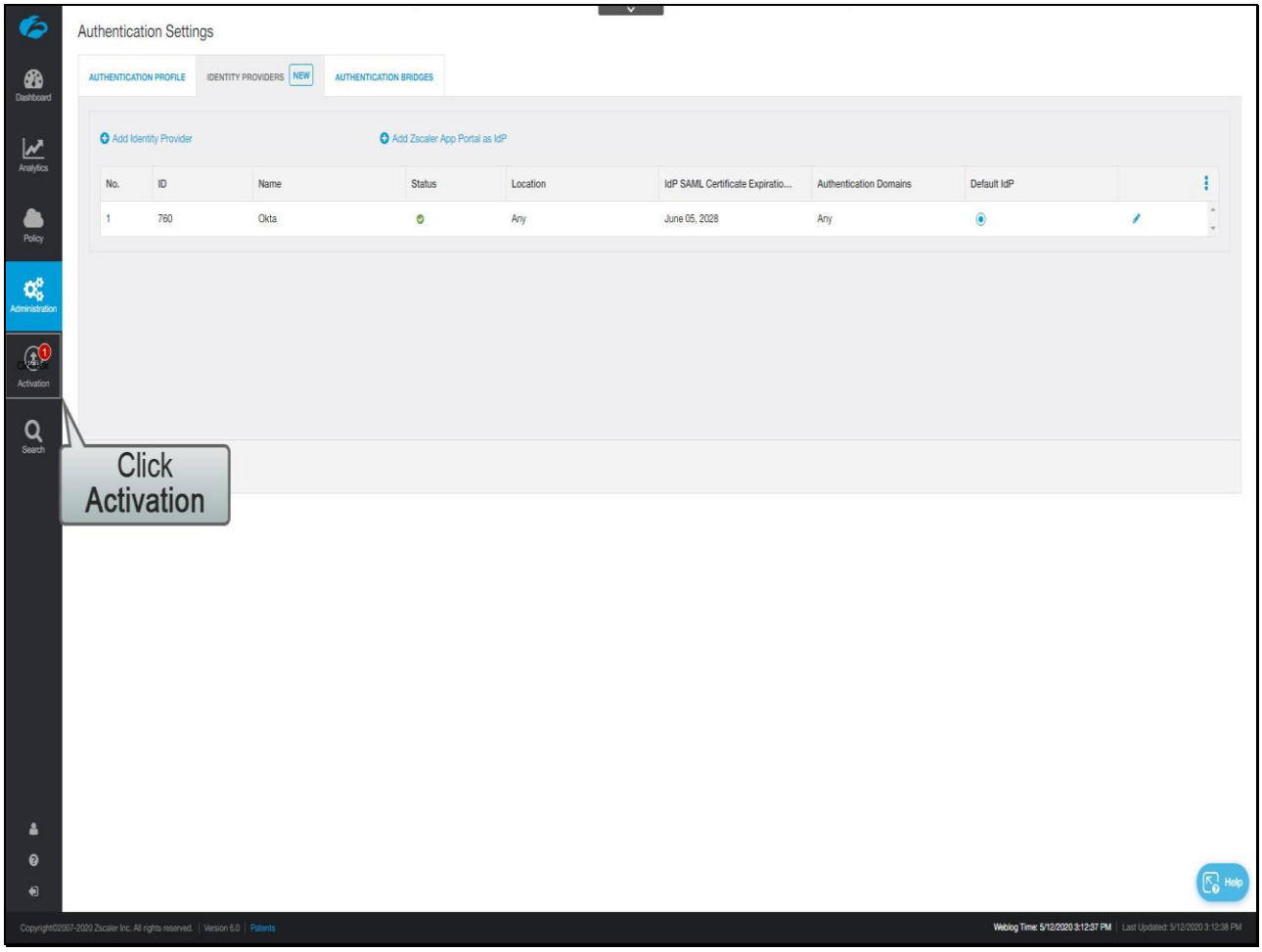
Slide 97 - Slide 97



Slide notes

and click **Save**.

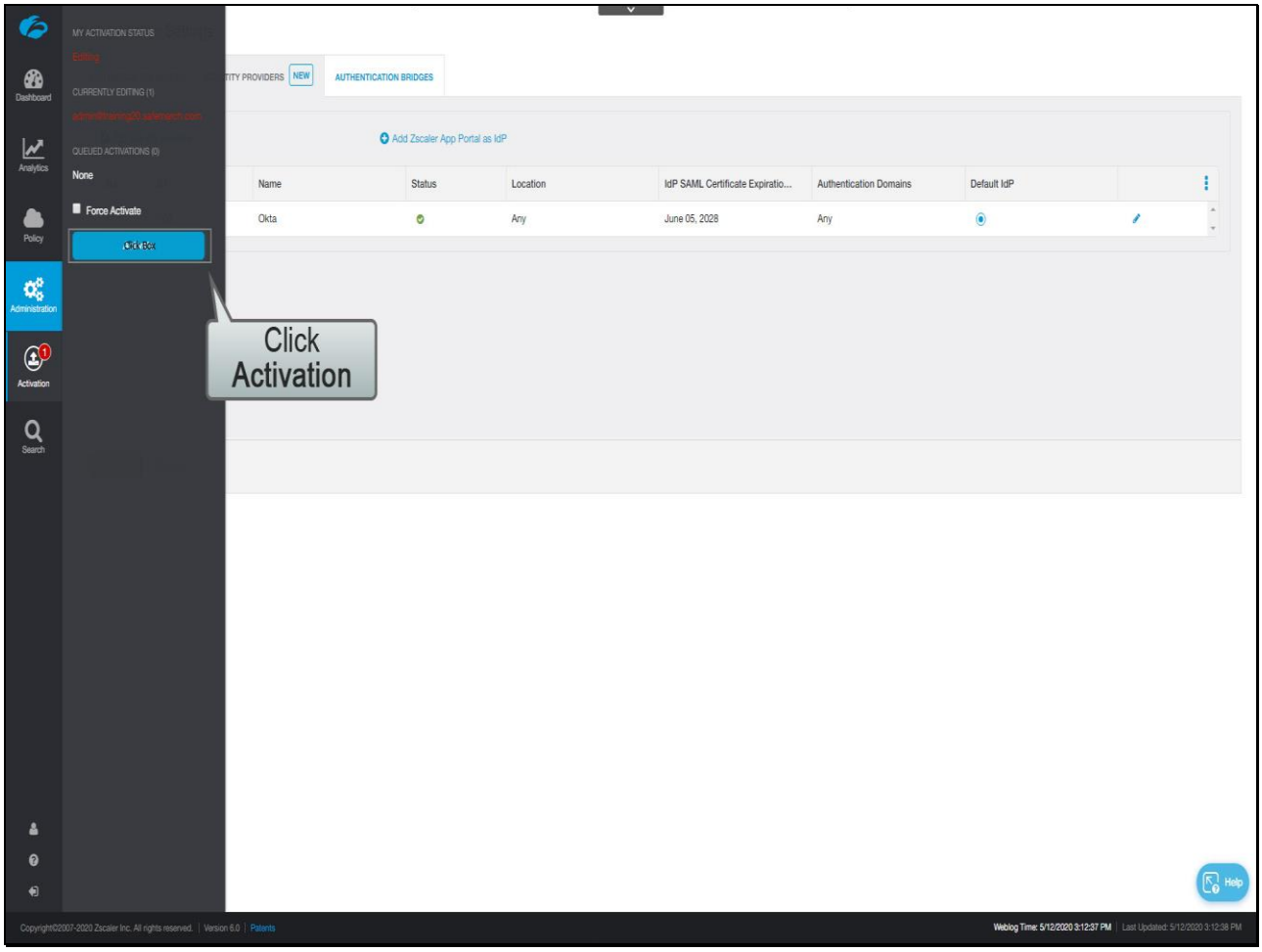
Slide 102 - Slide 102



Slide notes

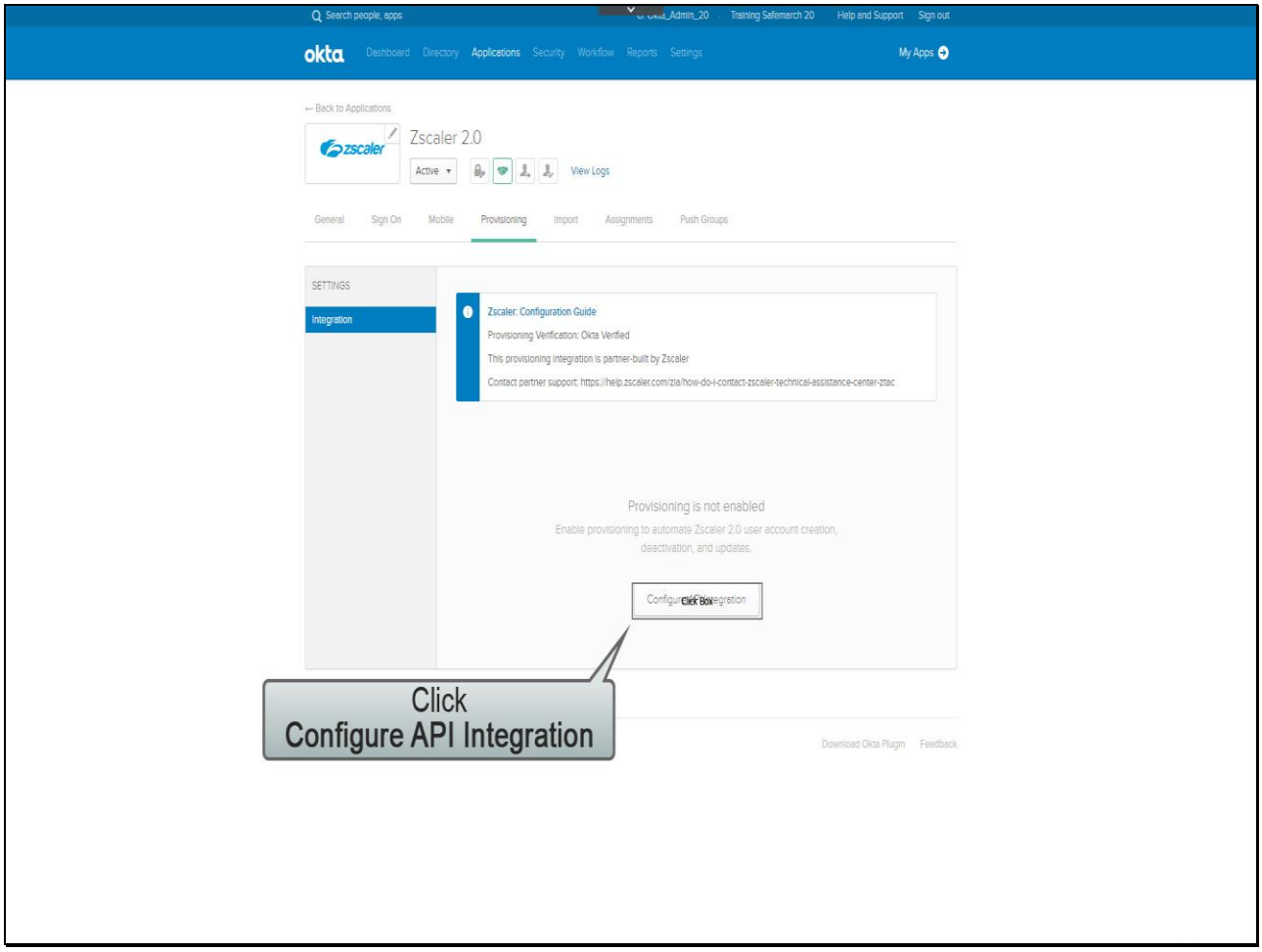
While you have saved the SAML configuration it is not yet live. Additionally, while the SCIM Bearer Token has been created it is not active until after you activate these changes. This is a critical step as the IdP will not be able to communicate with the Zscaler API until these changes have been activated.

Slide 103 - Slide 103



Slide notes

Slide 107 - Slide 107

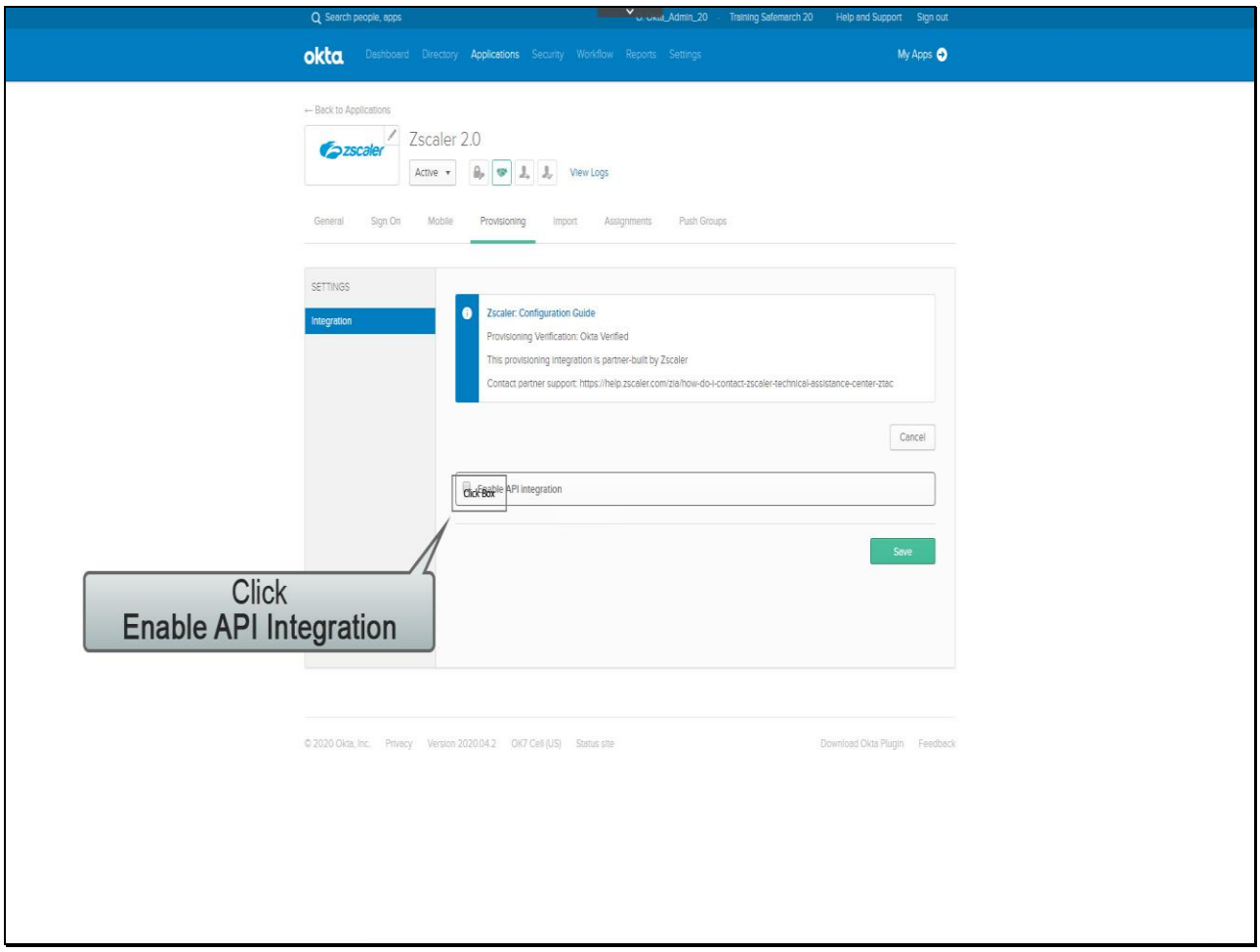


Slide notes

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.

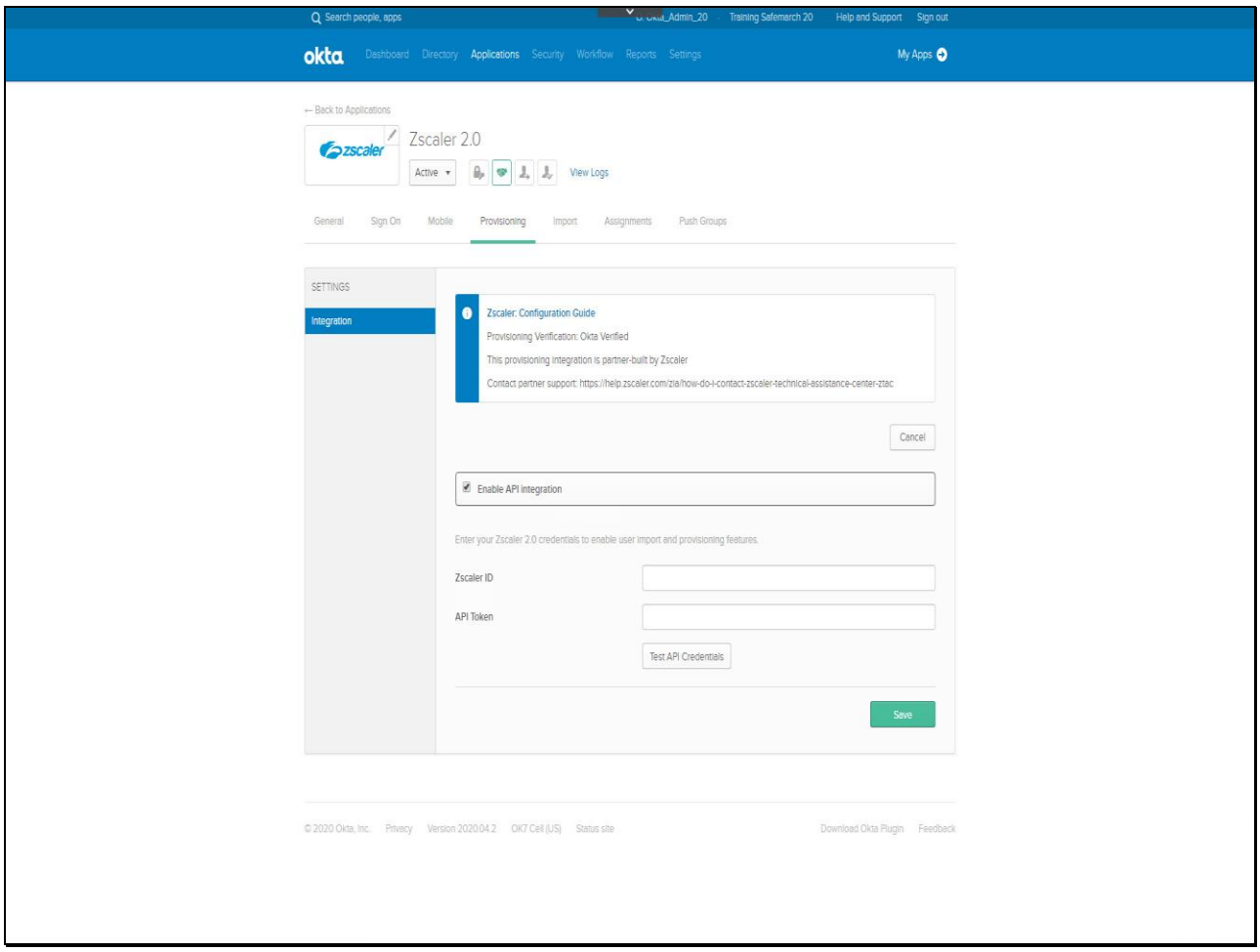
Slide 108 - Slide 108



Slide notes

Then **Enable API Integration**.

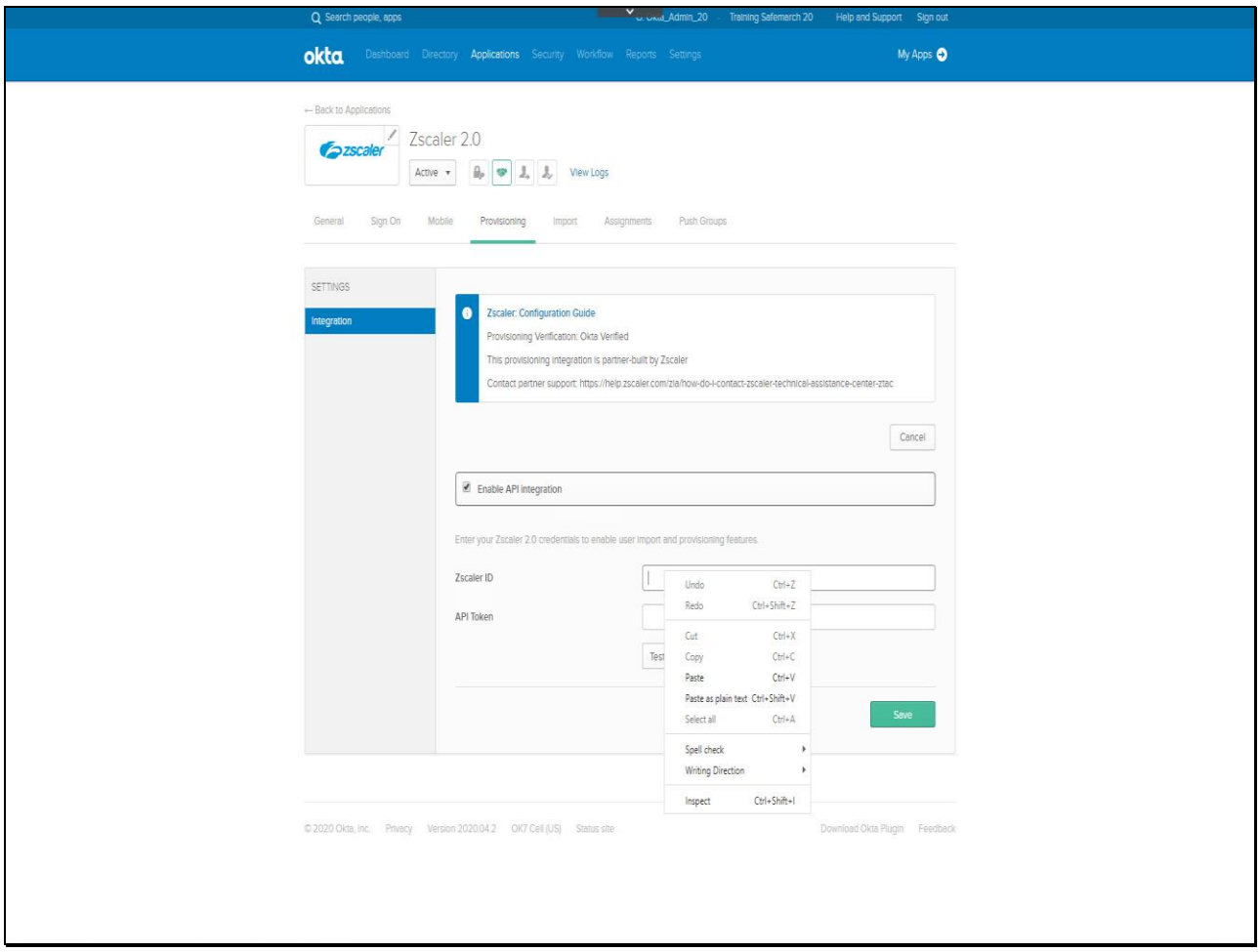
Slide 109 - Slide 109



Slide notes

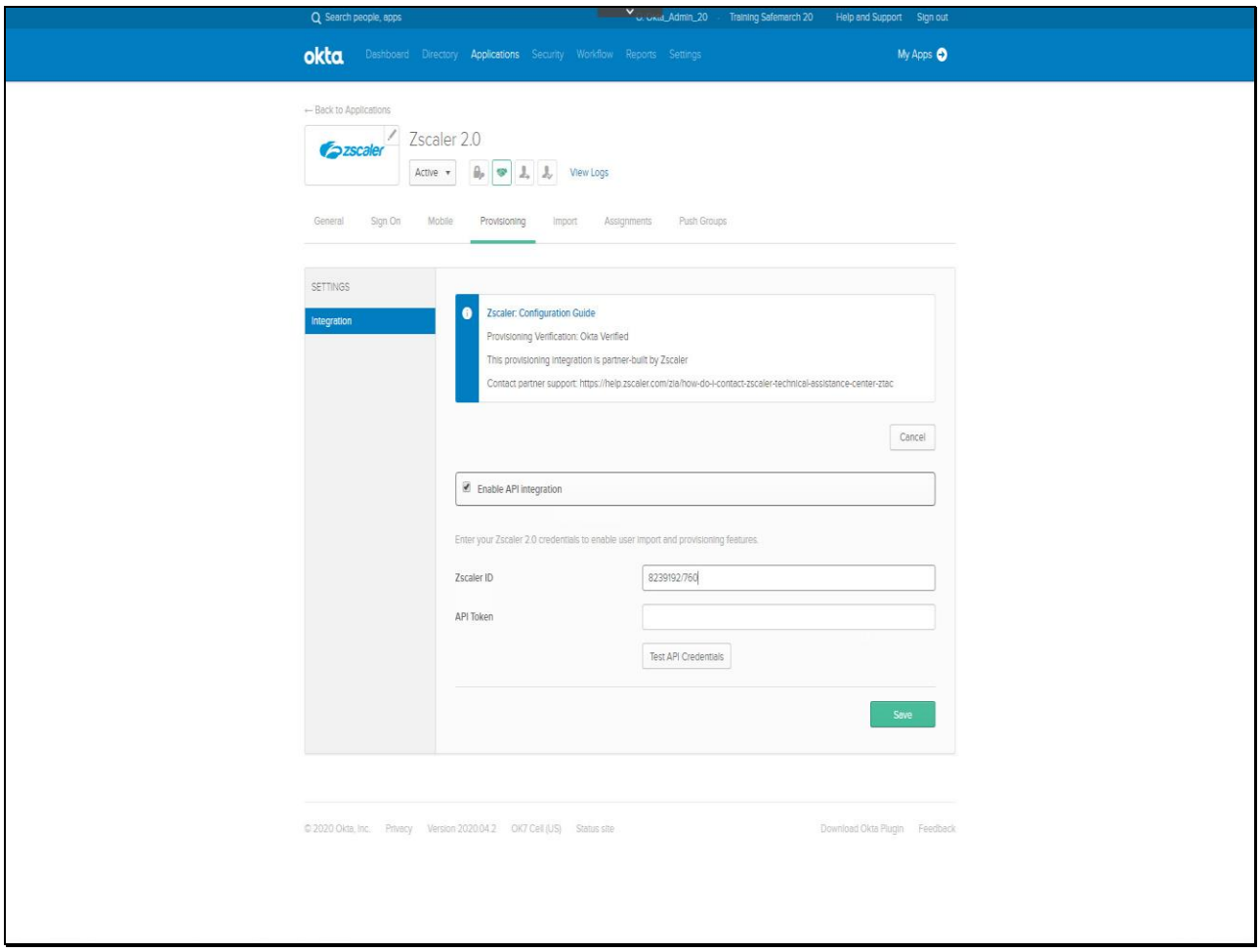
Then paste in the Organization ID / IdP ID combination you copied earlier and the Bearer Token. Note that Okta calls the Bearer Token the API Token.

Slide 110 - Slide 110



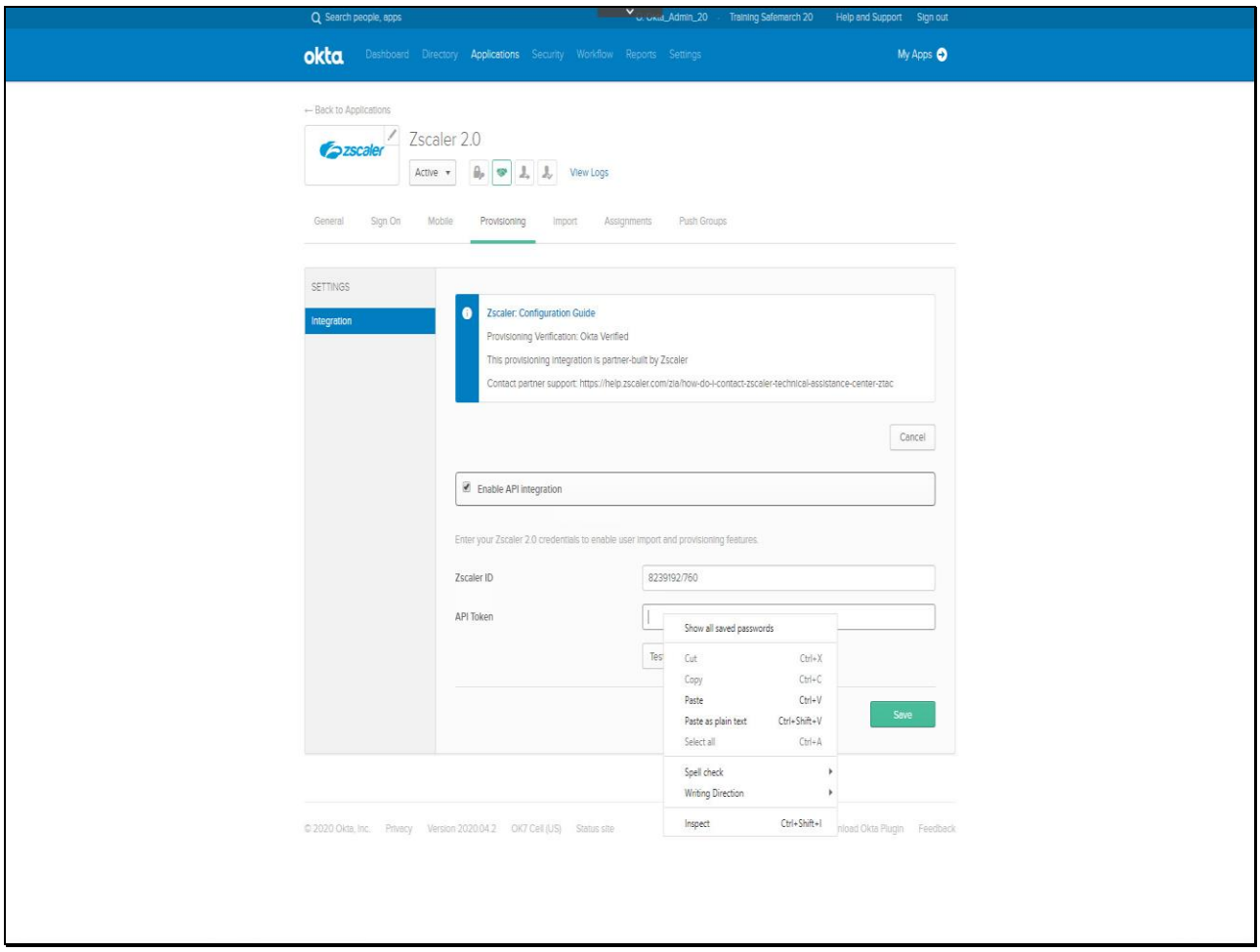
Slide notes

Slide 111 - Slide 111



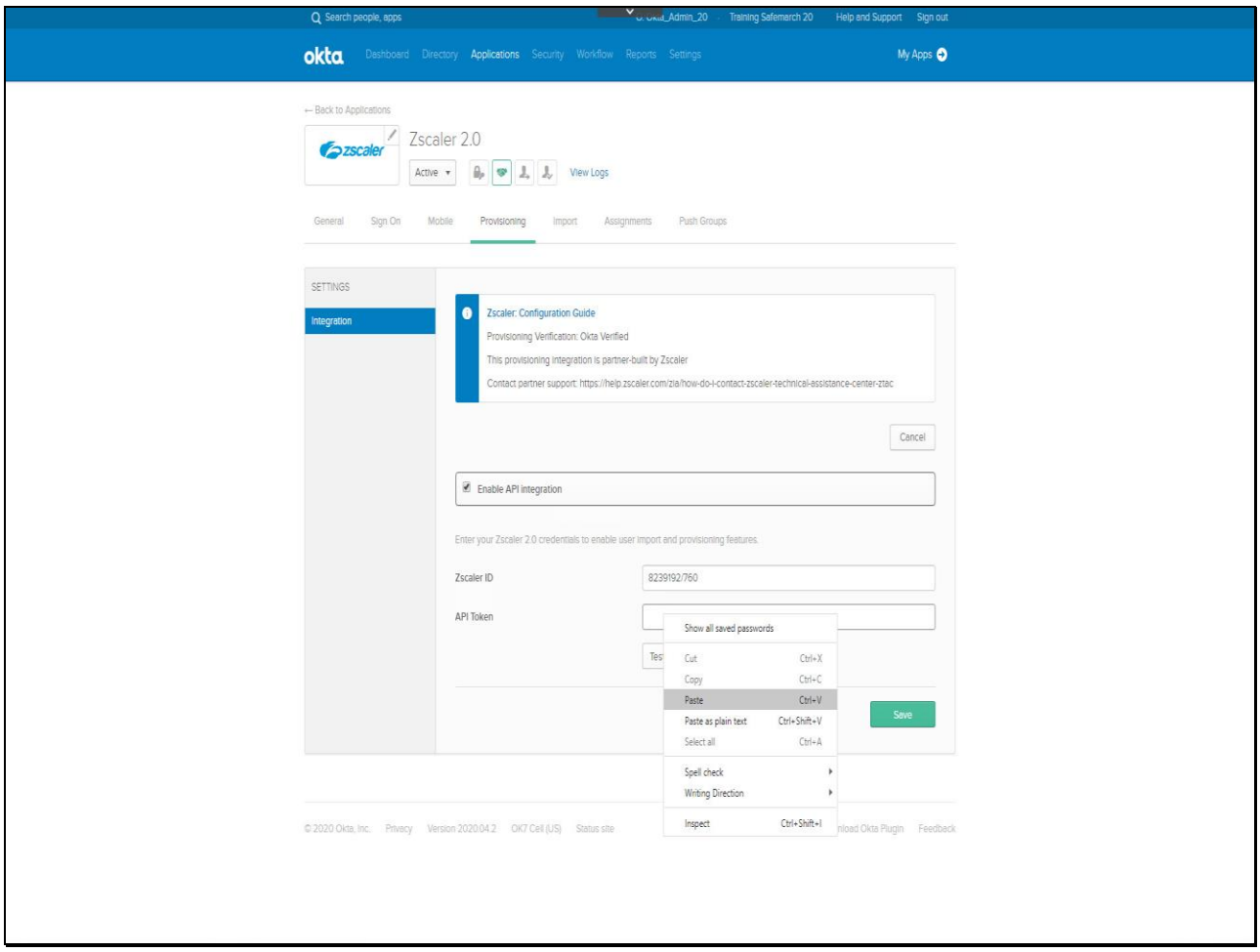
Slide notes

Slide 112 - Slide 112



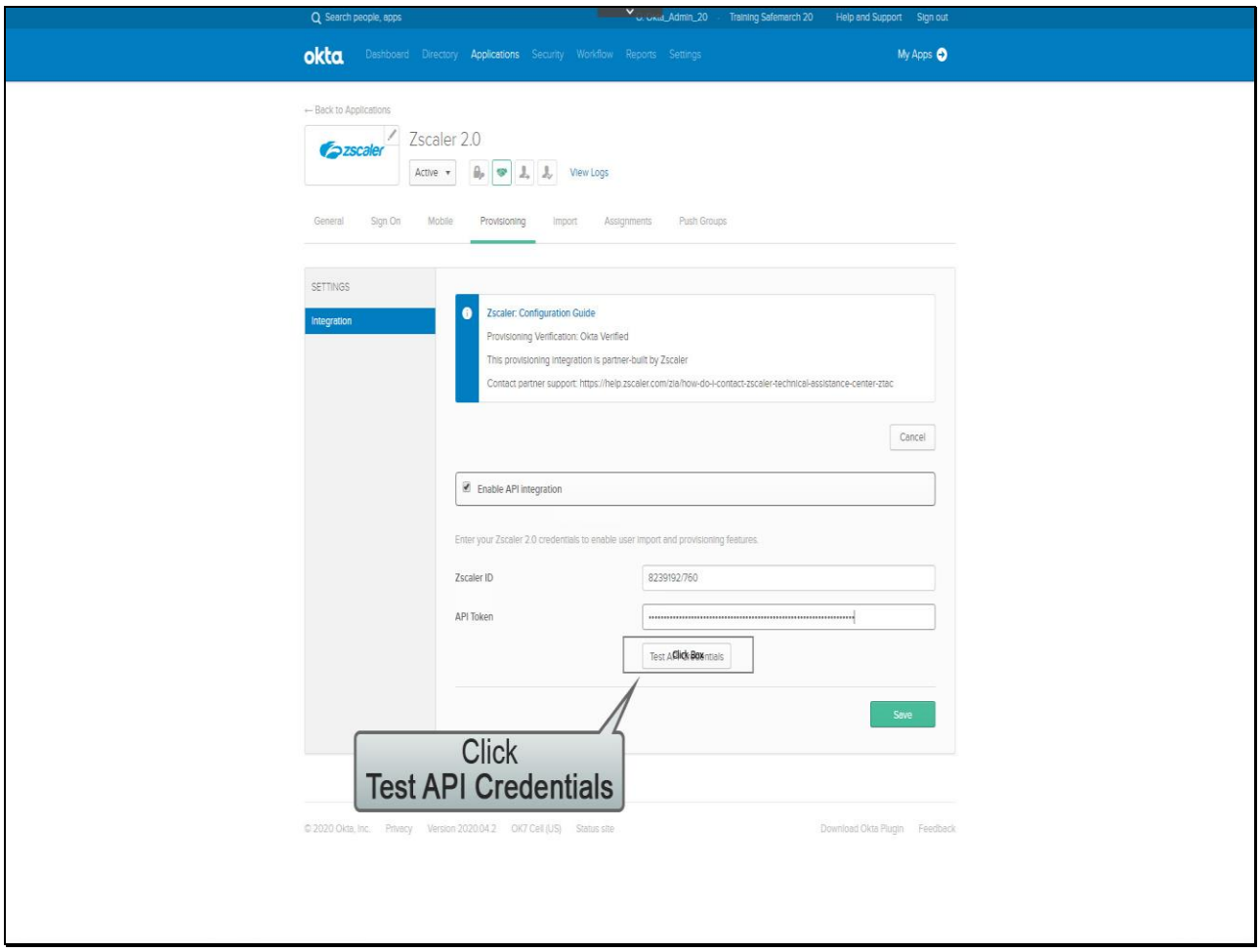
Slide notes

Slide 113 - Slide 113



Slide notes

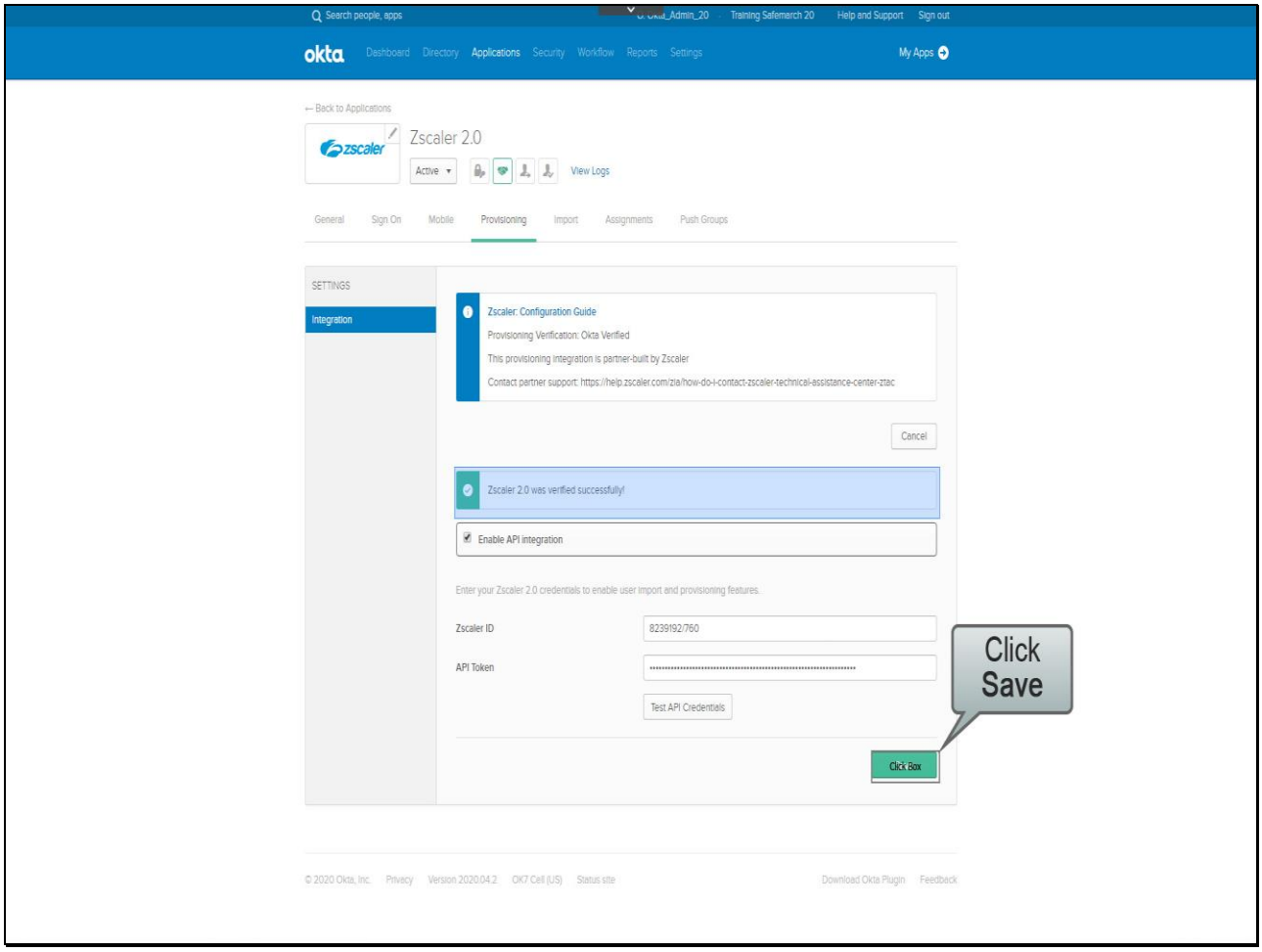
Slide 114 - Slide 114



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.

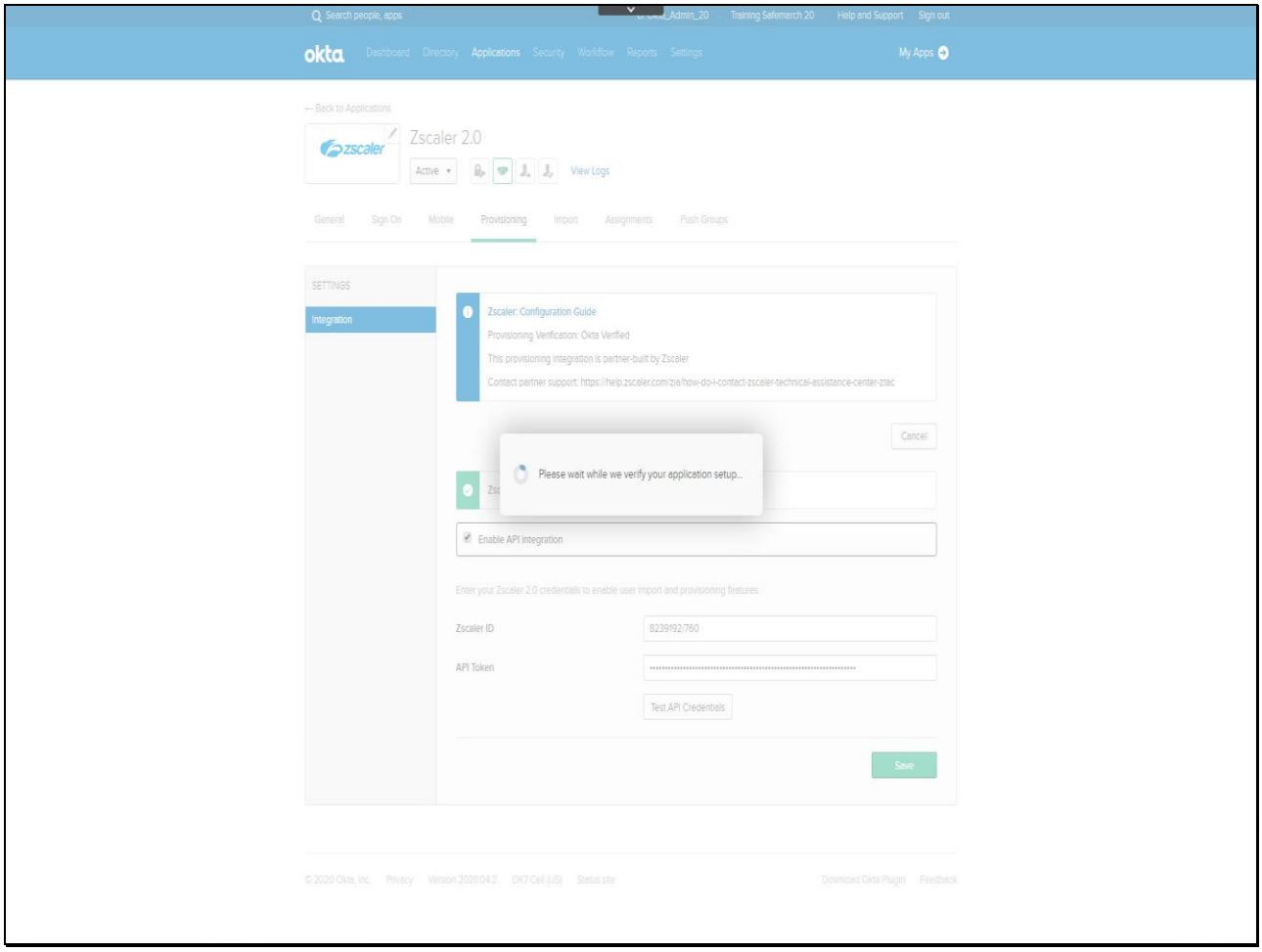
Slide 115 - Slide 115



Slide notes

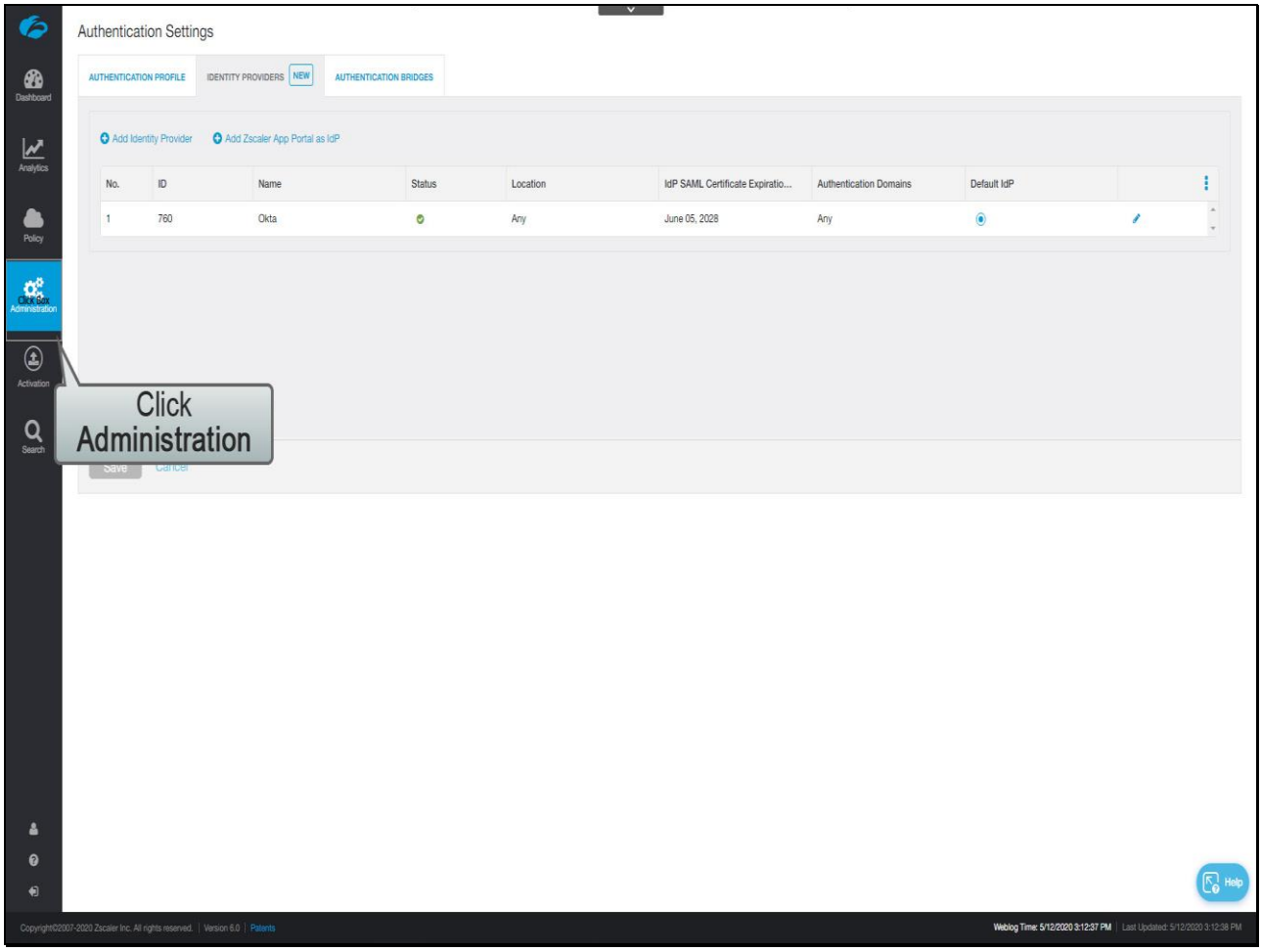
If the Success message is displayed, then click Save. If there is a failure go back to the Zscaler Admin Portal and be sure that the SAML configuration has been saved and Activated.

Slide 116 - Slide 116



Slide notes

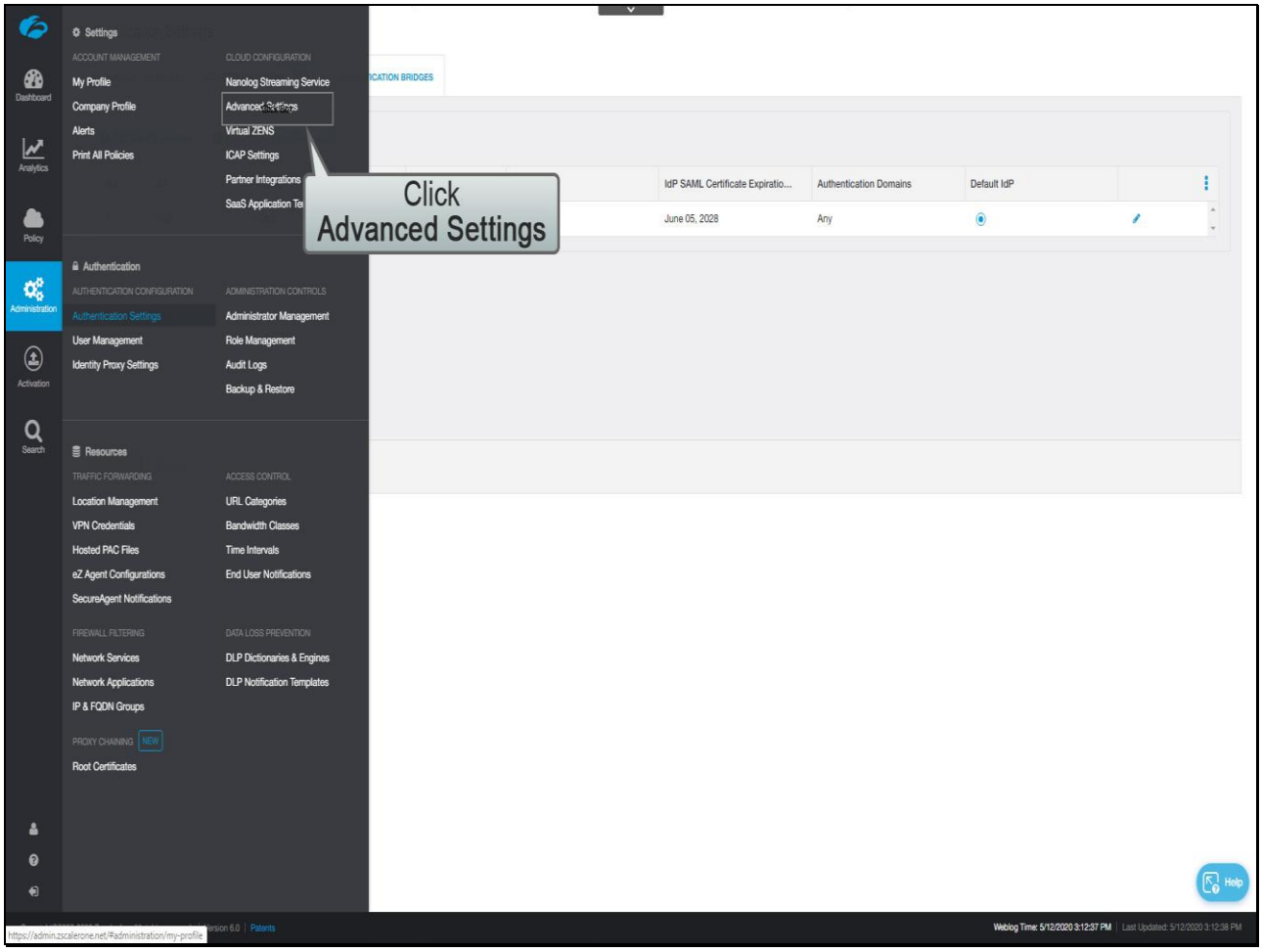
Slide 117 - Slide 117



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 I 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.**

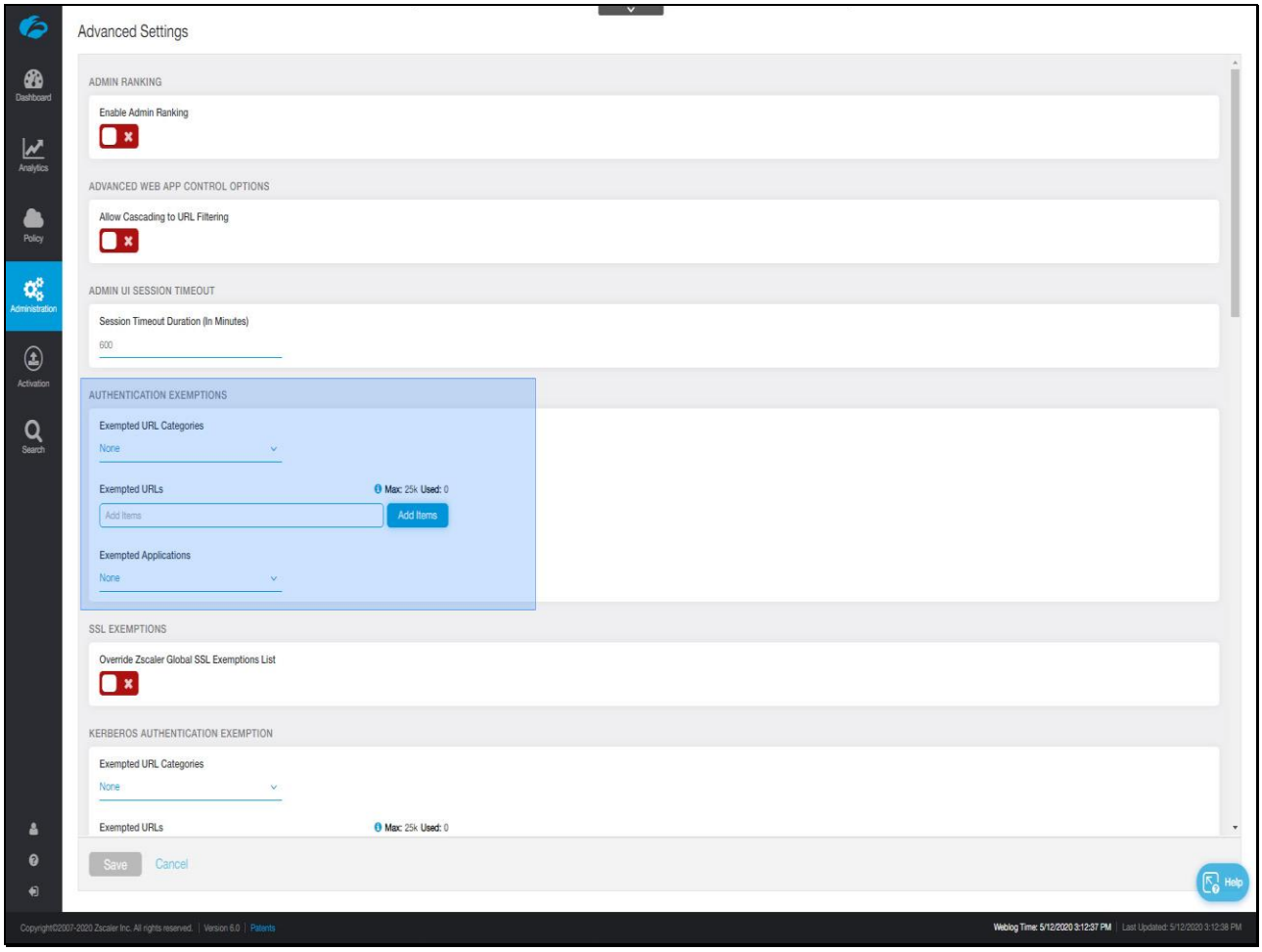
Slide 118 - Slide 118



Slide notes

Then **Advanced Settings**.

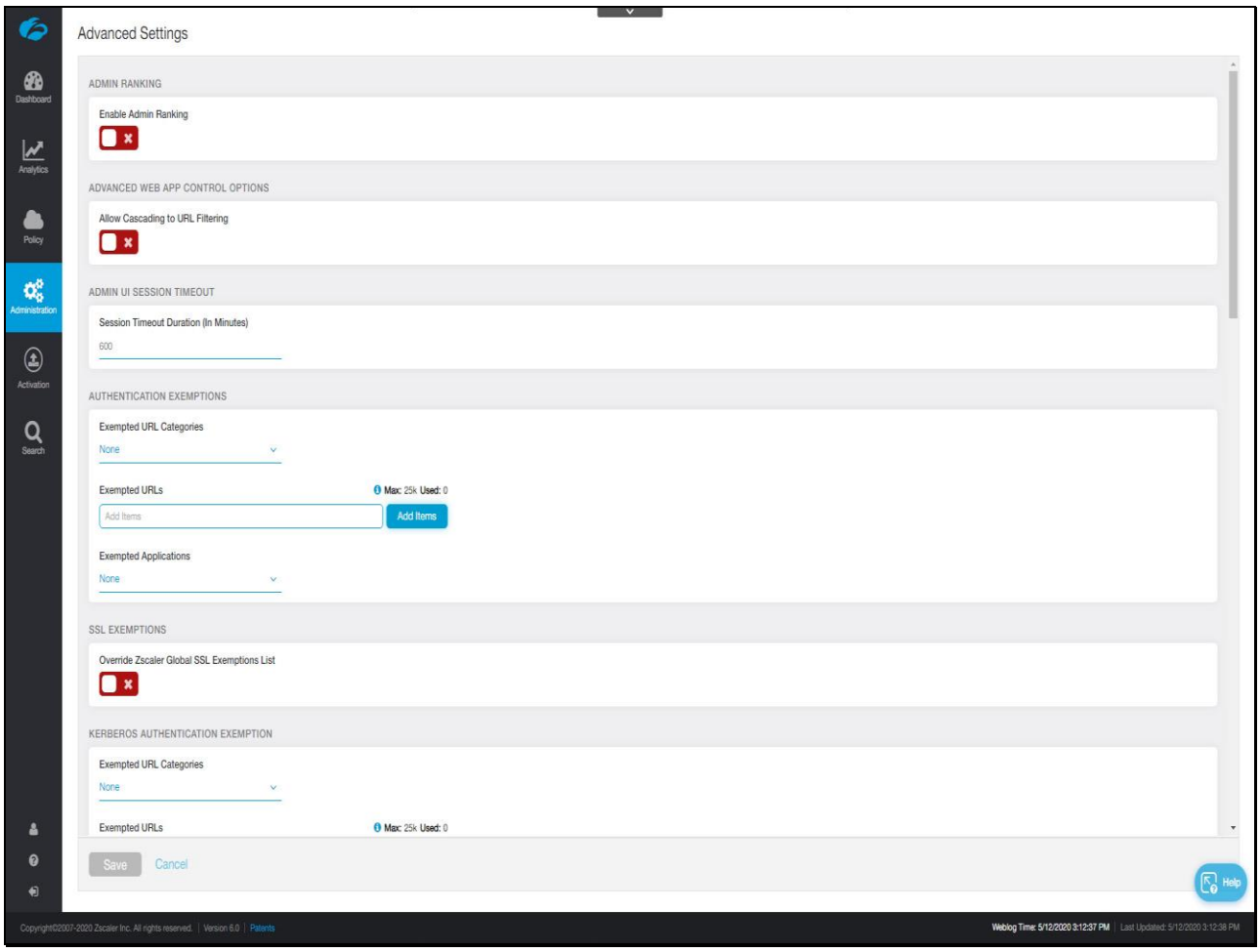
Slide 119 - Slide 119



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

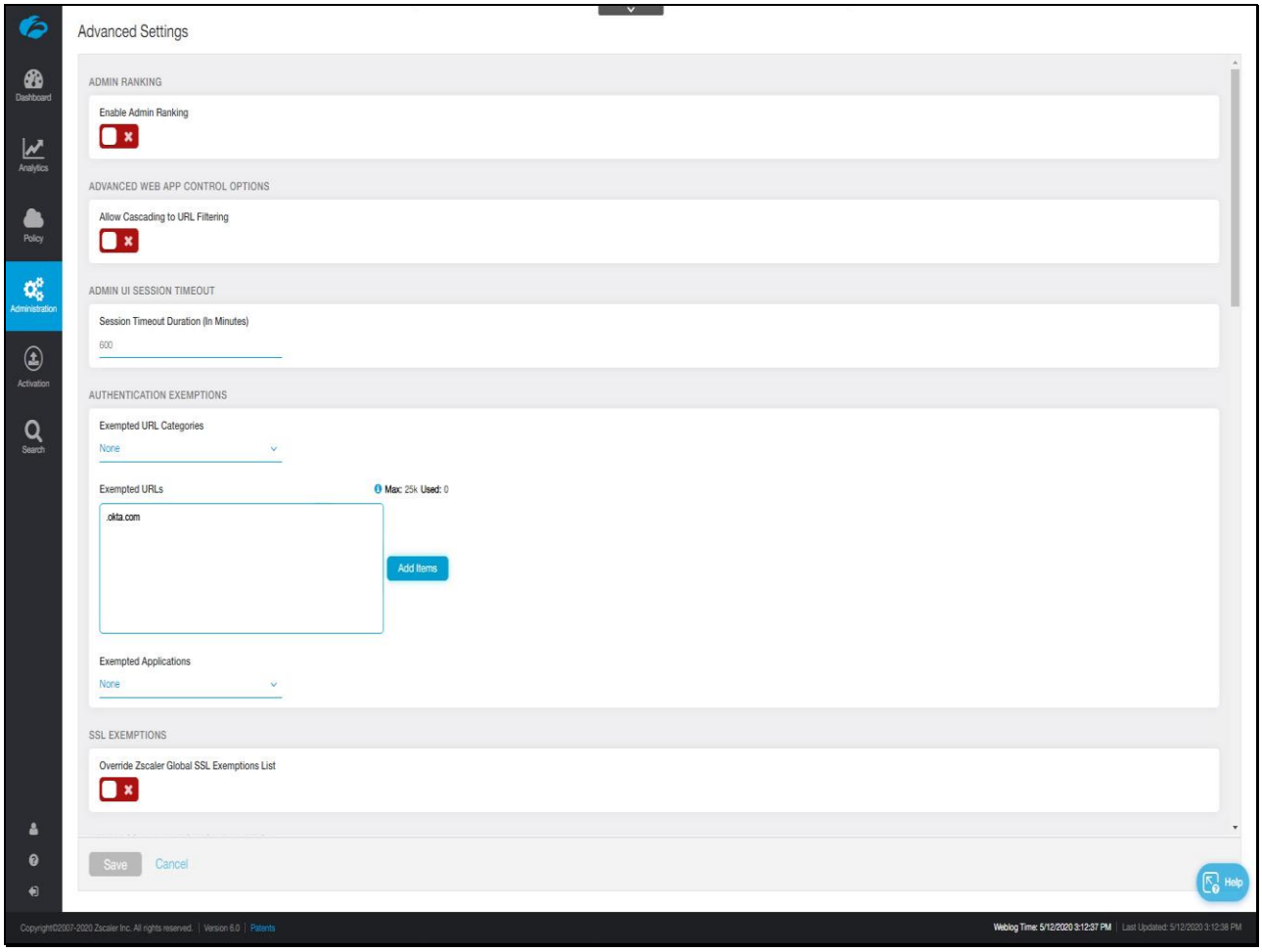
Slide 120 - Slide 120



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.

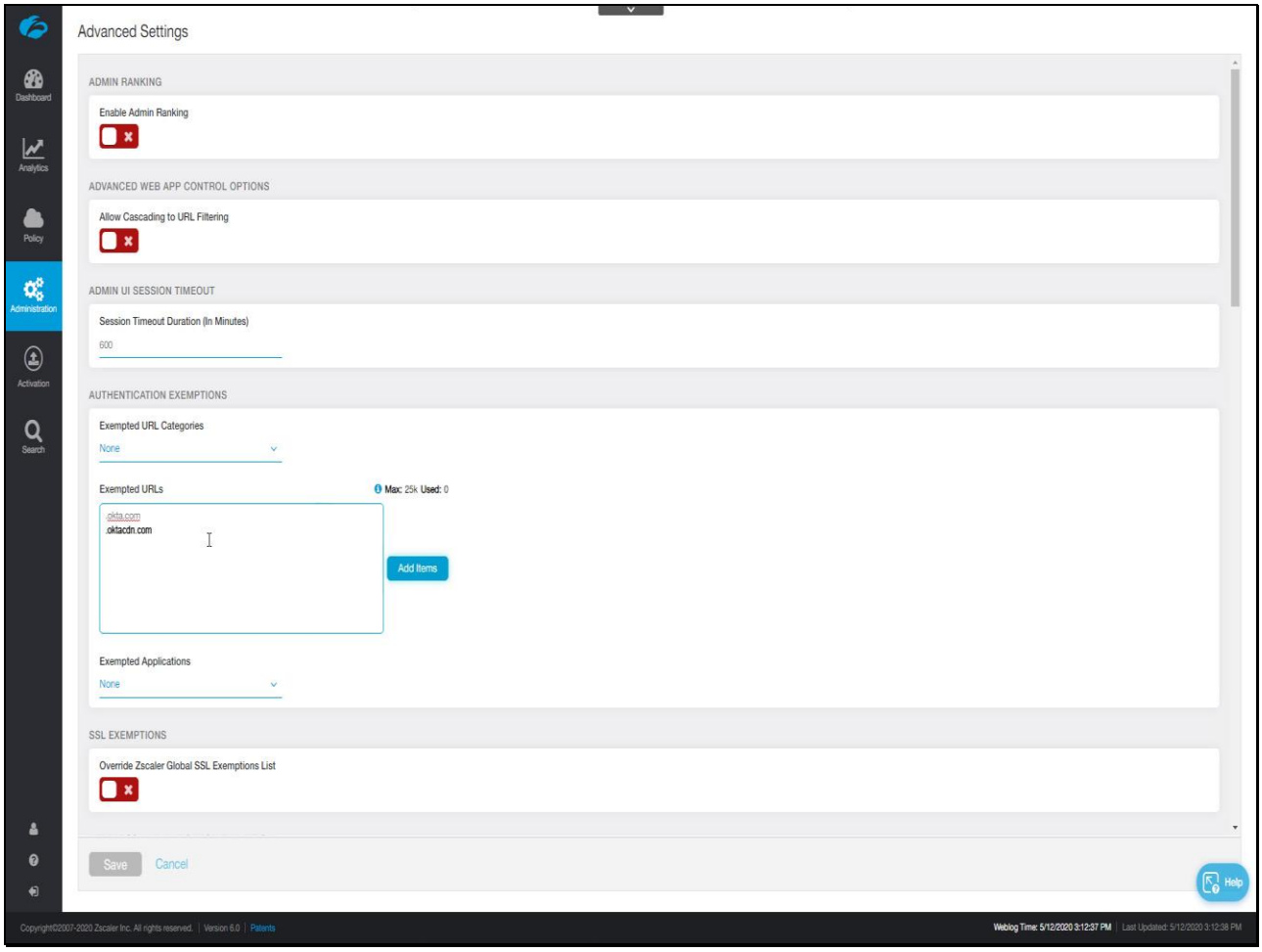
Slide 121 - Slide 121



Slide notes

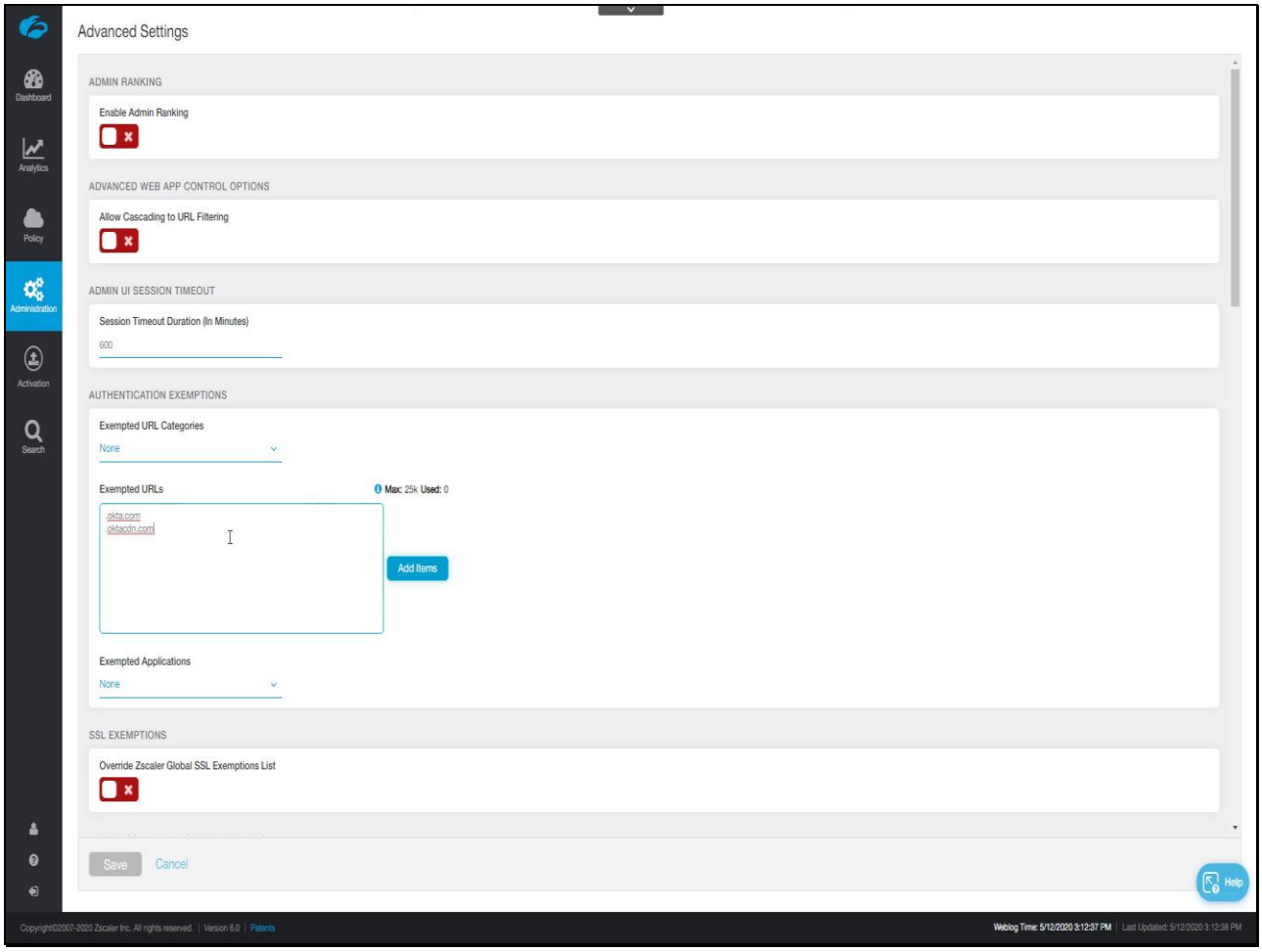
In the case of Okta there are two URL's: .okta.com and .oktacdn.com.

Slide 122 - Slide 122



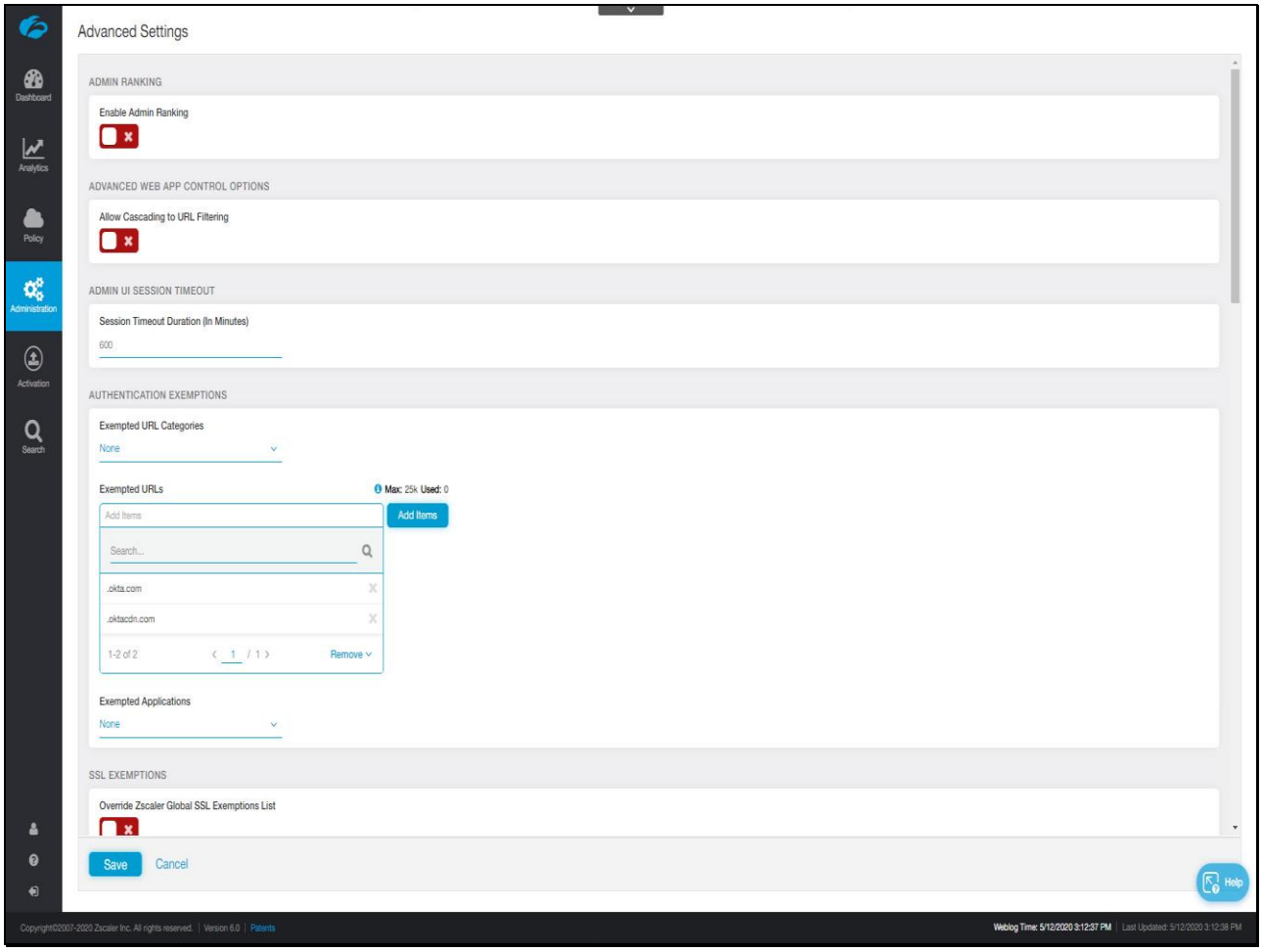
Slide notes

Slide 123 - Slide 123



Slide notes

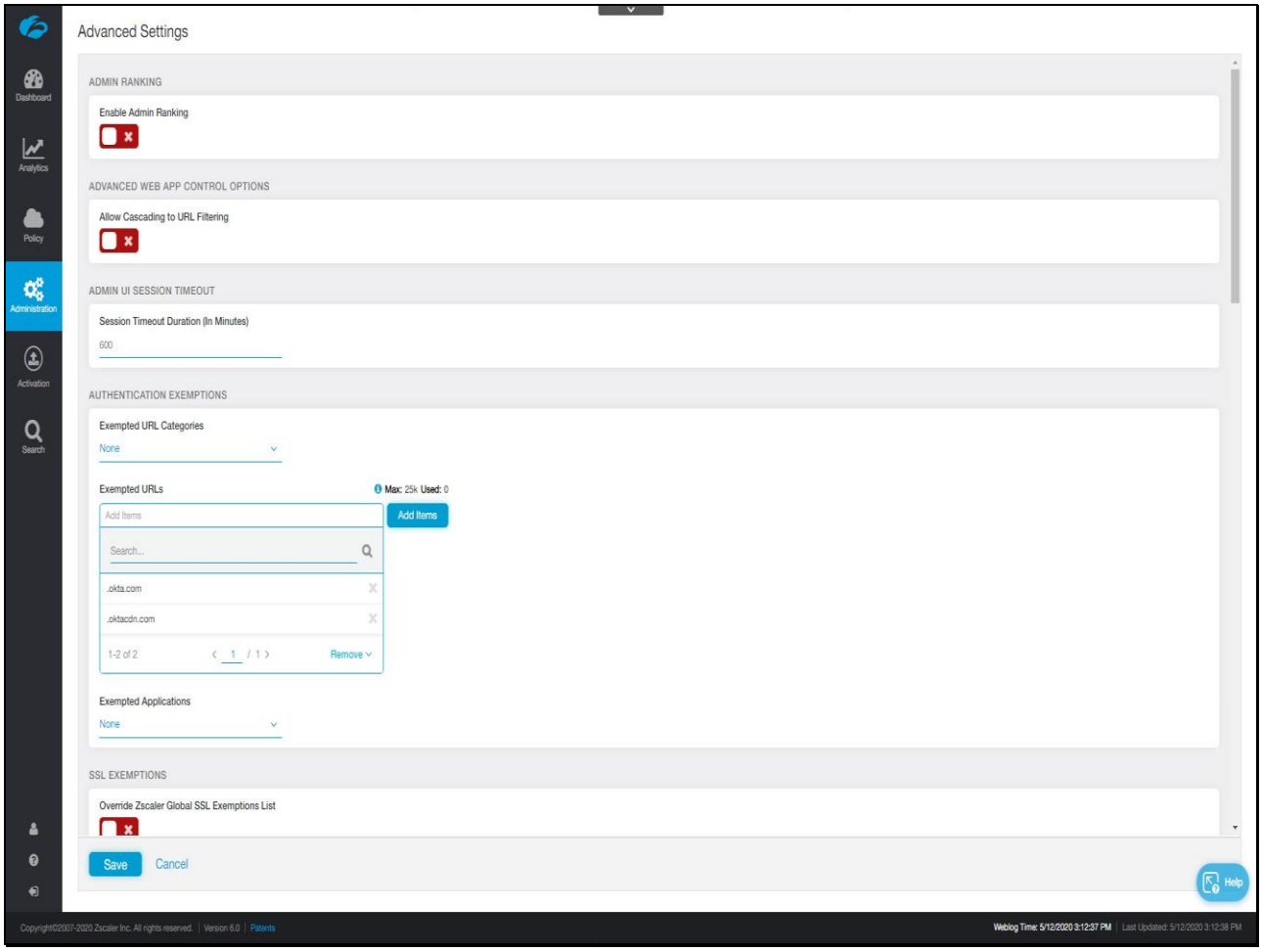
Slide 124 - Slide 124



Slide notes

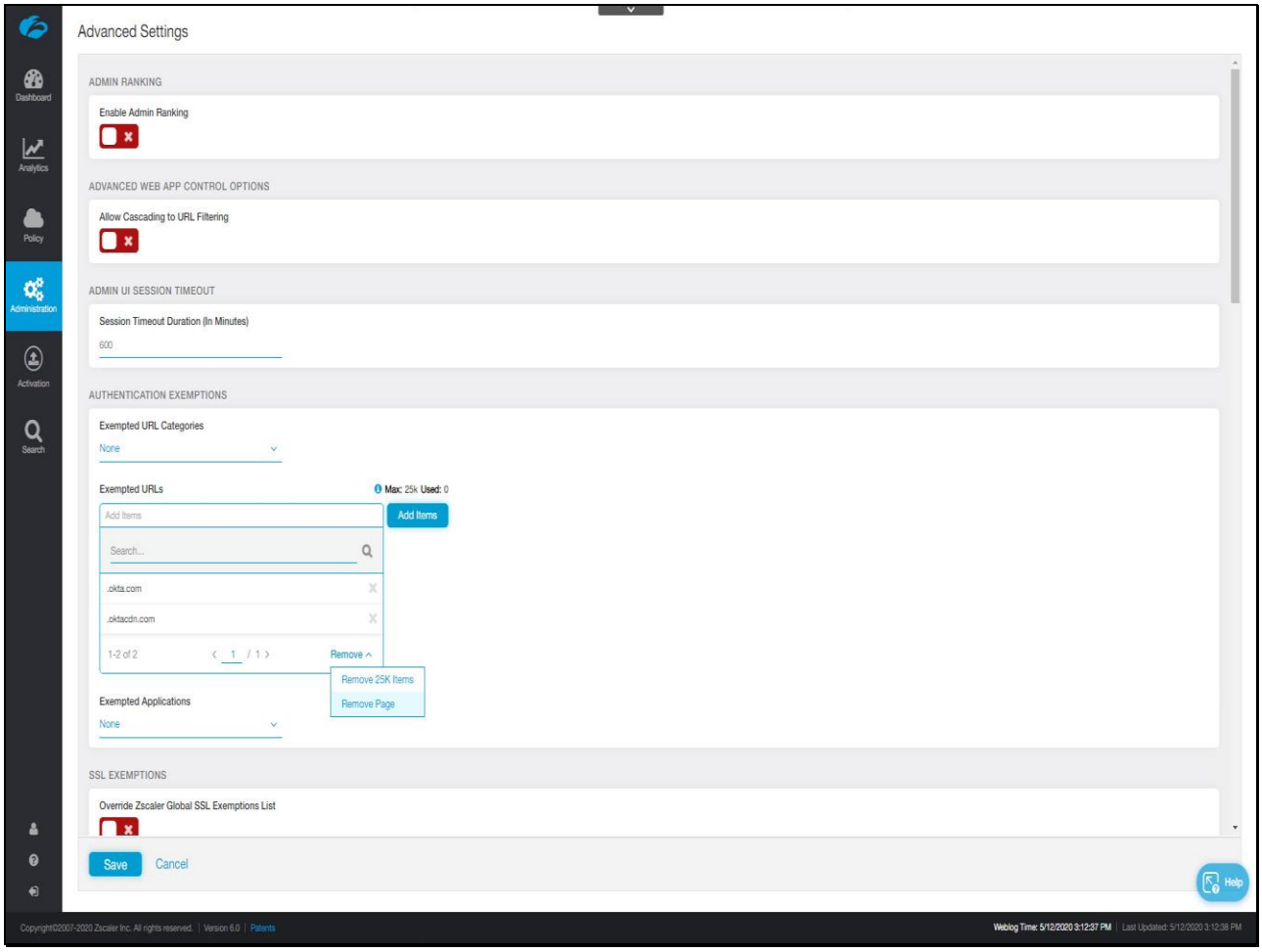
For this example, however, let's use the Exempted Applications list.

Slide 125 - Slide 125



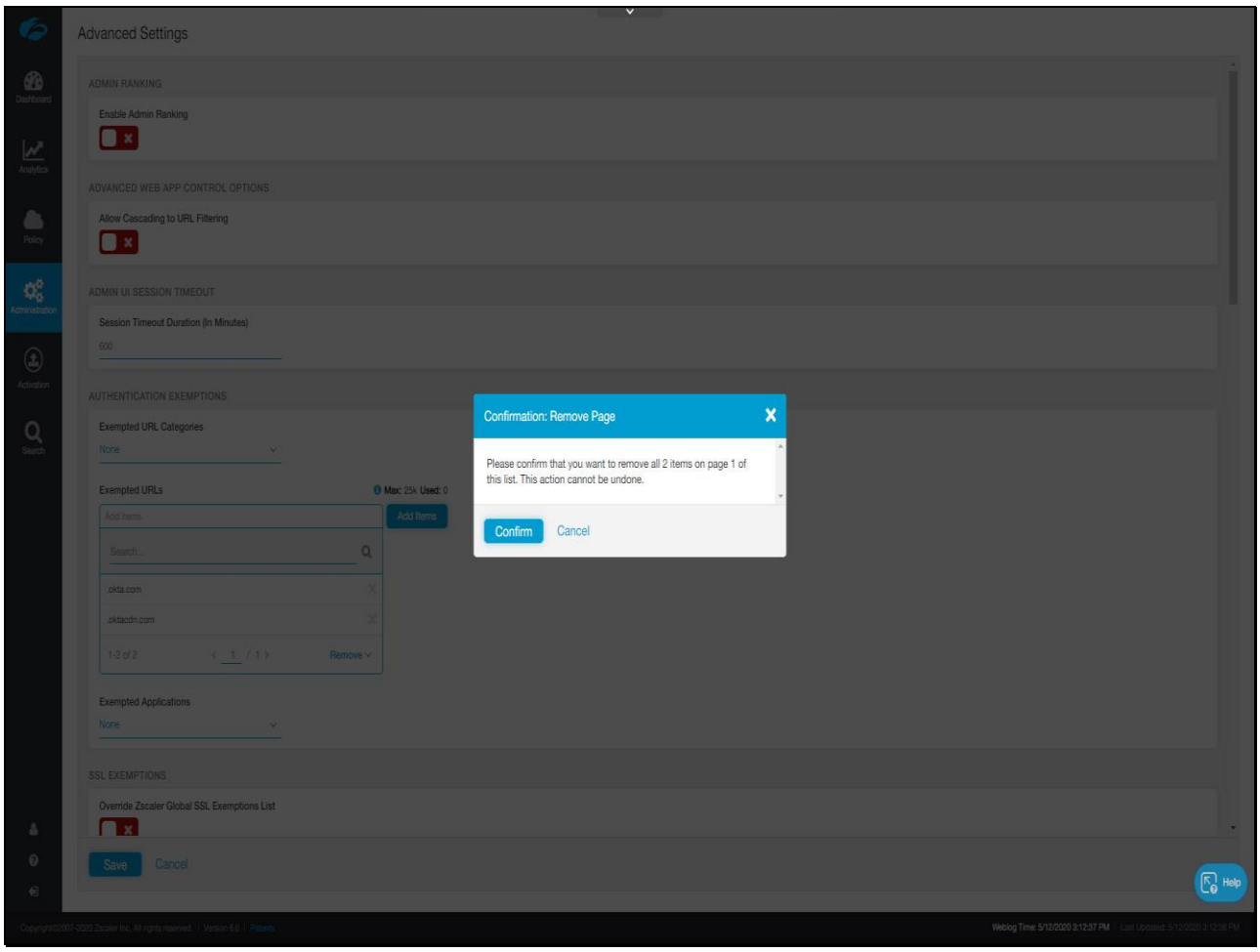
Slide notes

Slide 126 - Slide 126



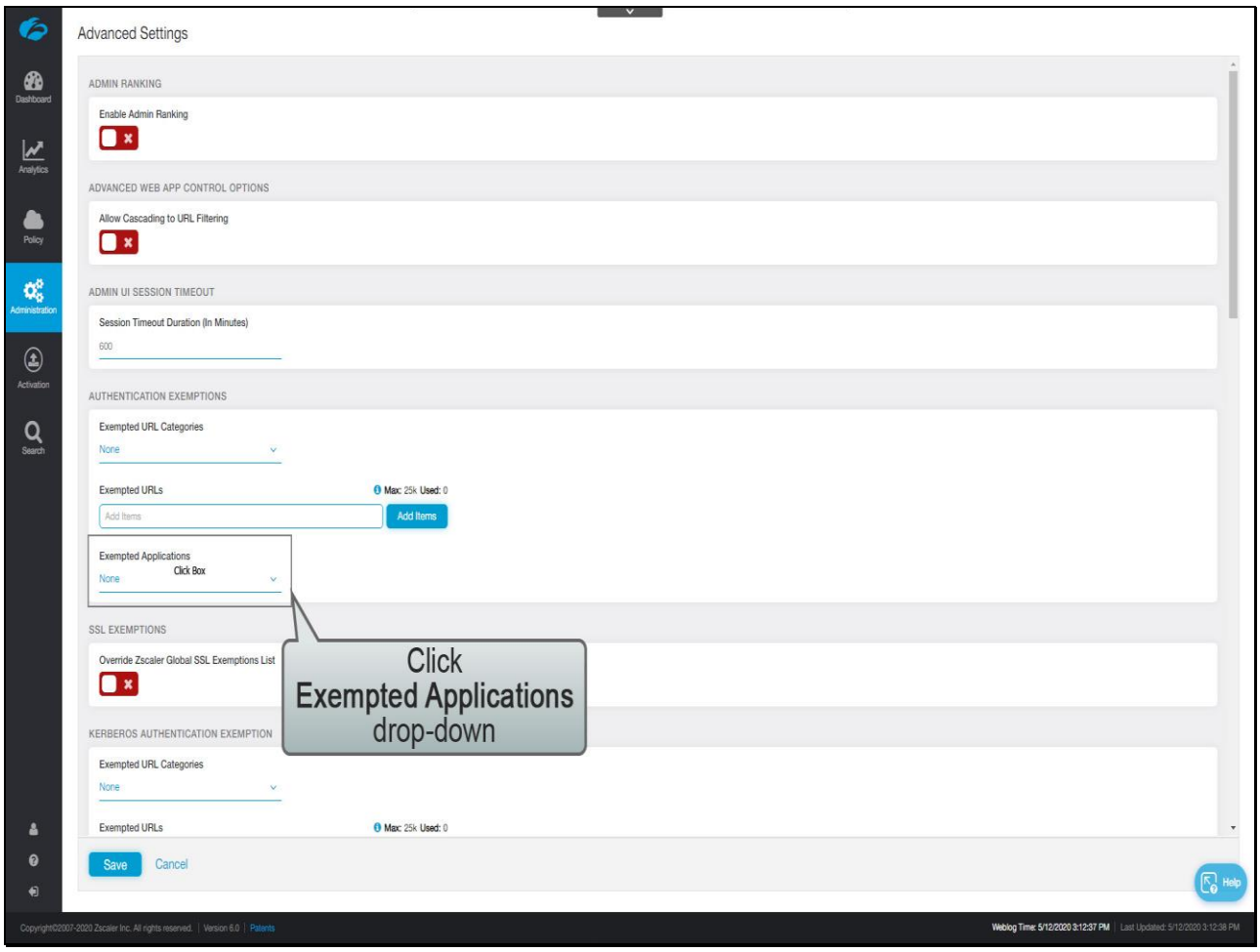
Slide notes

Slide 127 - Slide 127



Slide notes

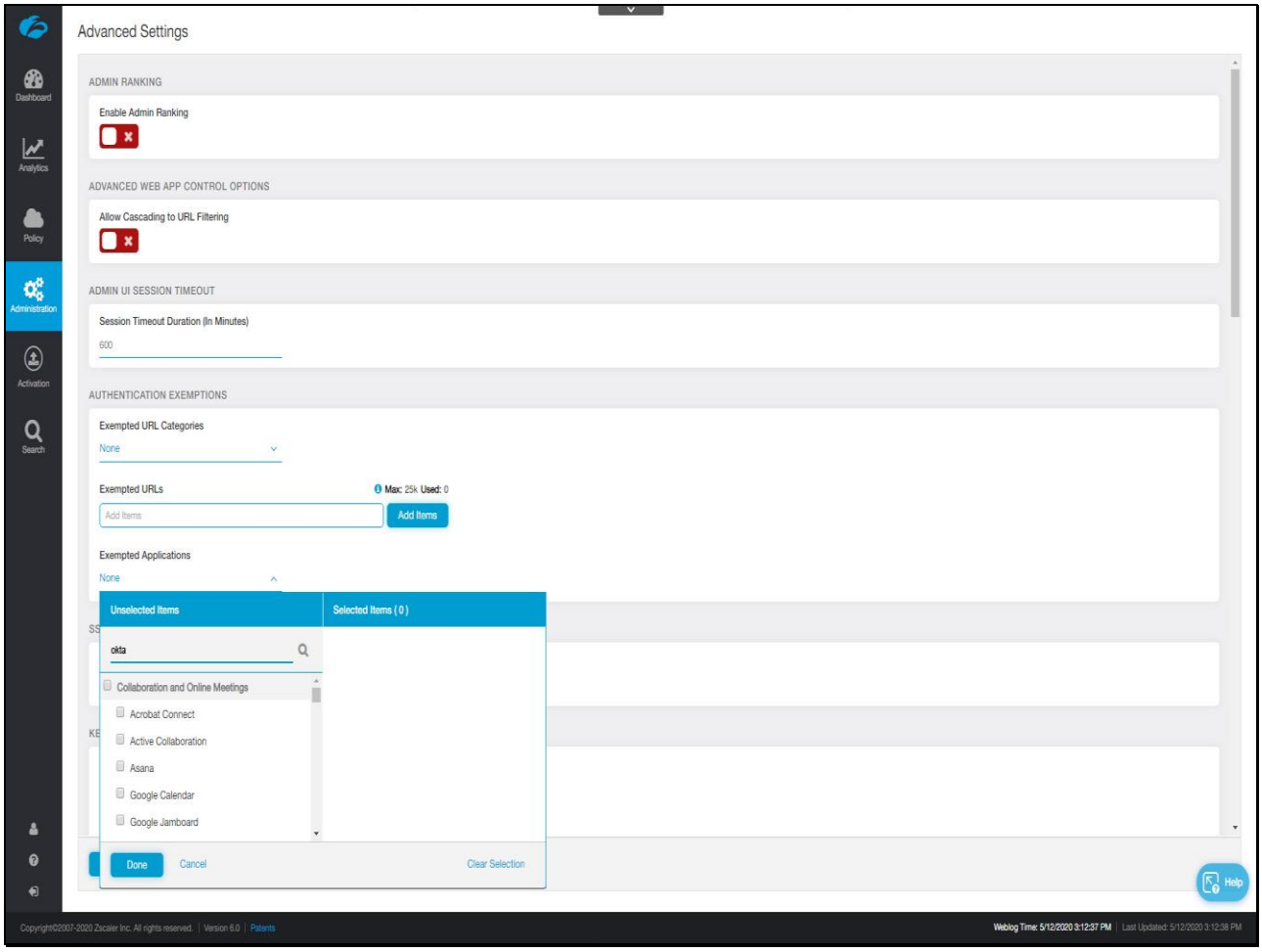
Slide 128 - Slide 128



Slide notes

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

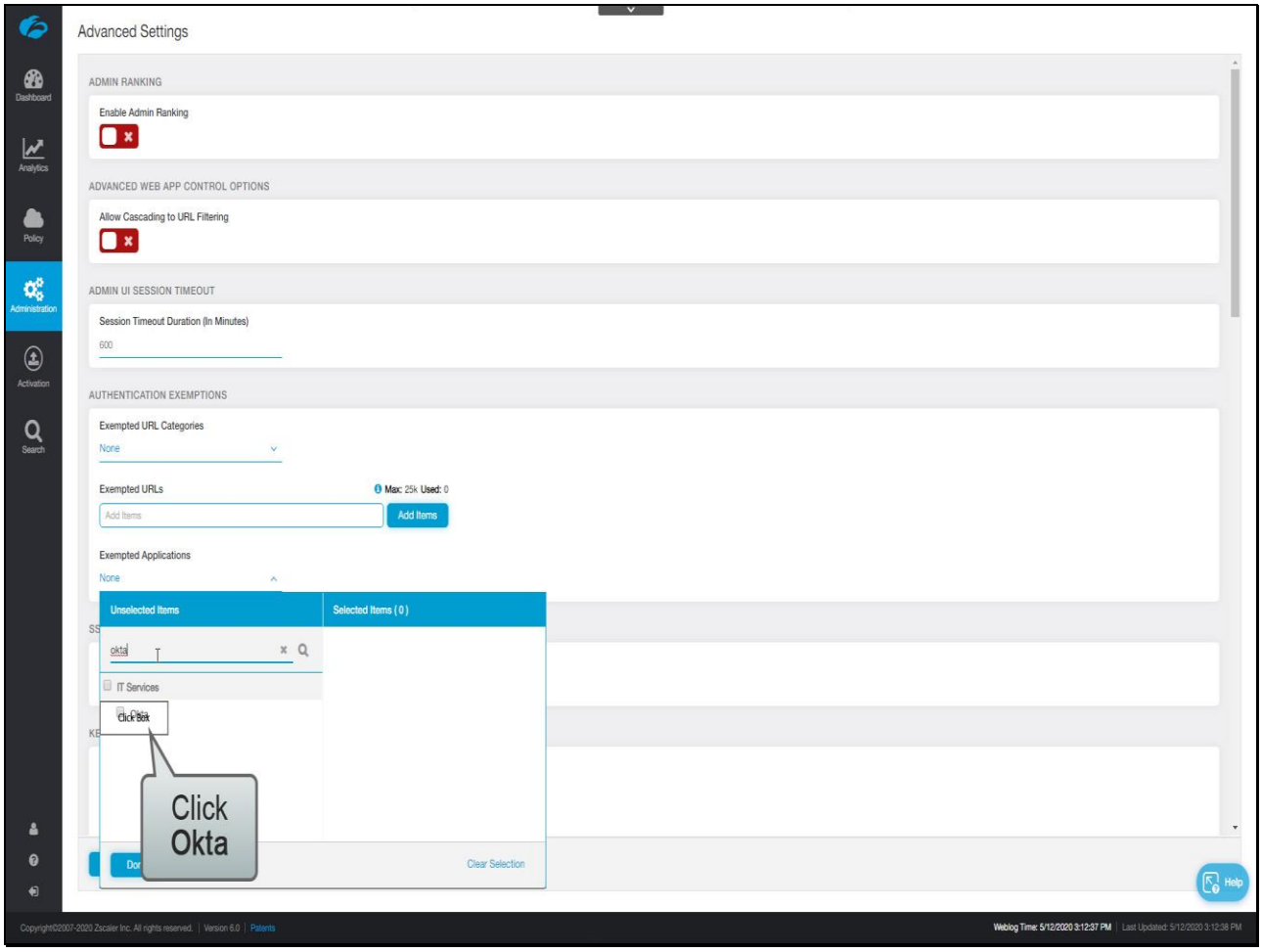
Slide 130 - Slide 130



Slide notes

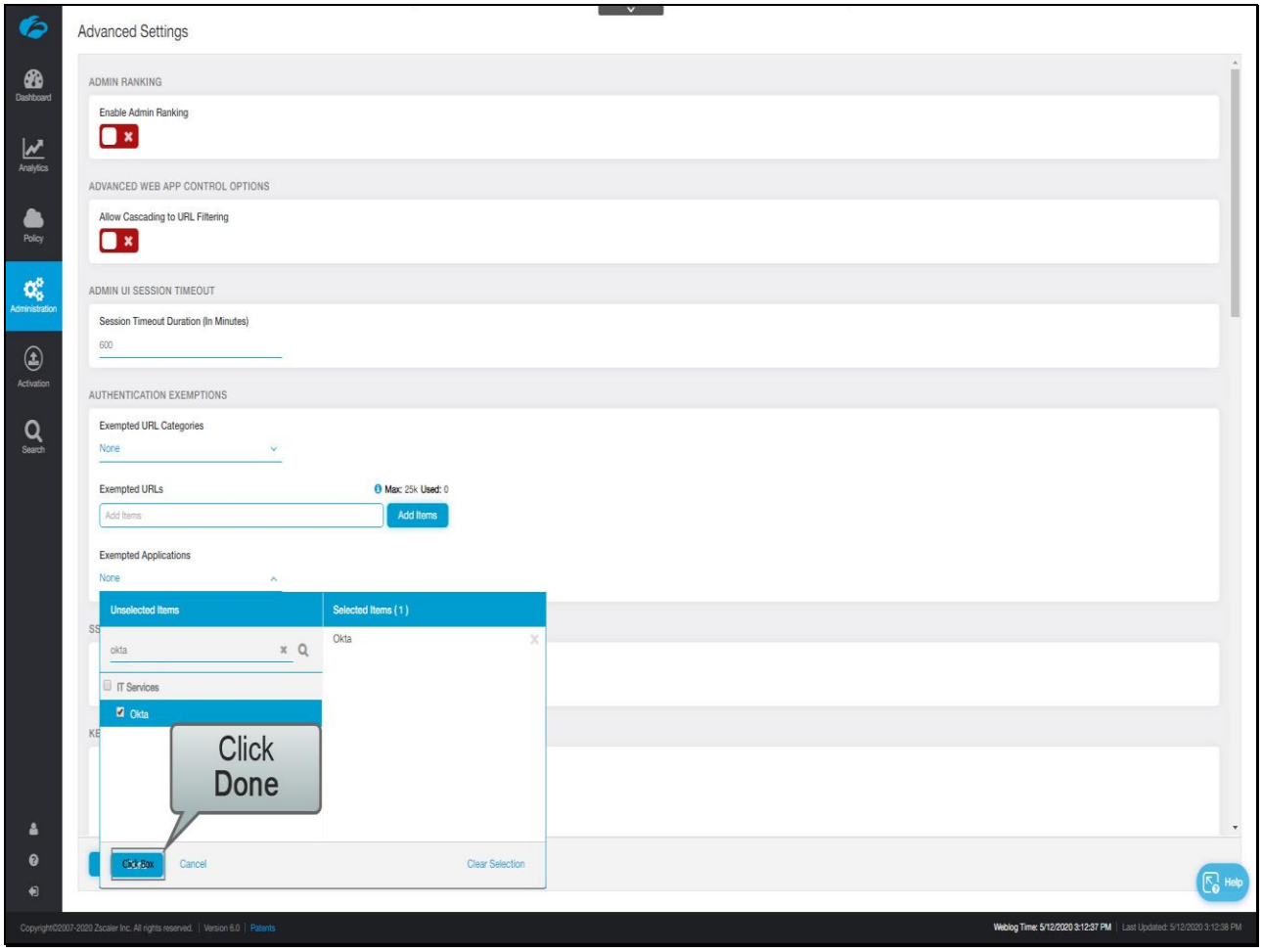
Then search for and select Okta.

Slide 131 - Slide 131



Slide notes

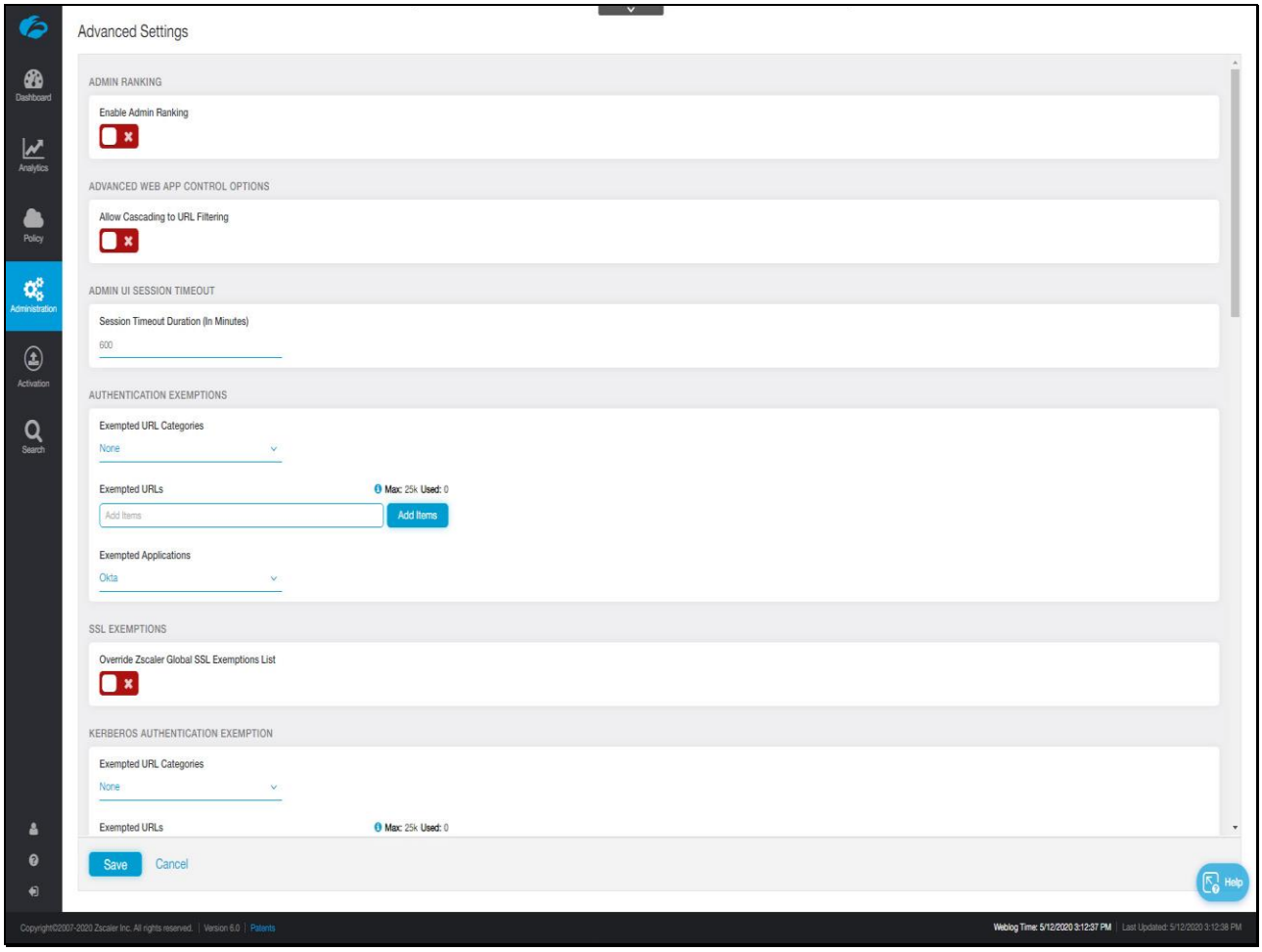
Slide 132 - Slide 132



Slide notes

Then click **Done**.

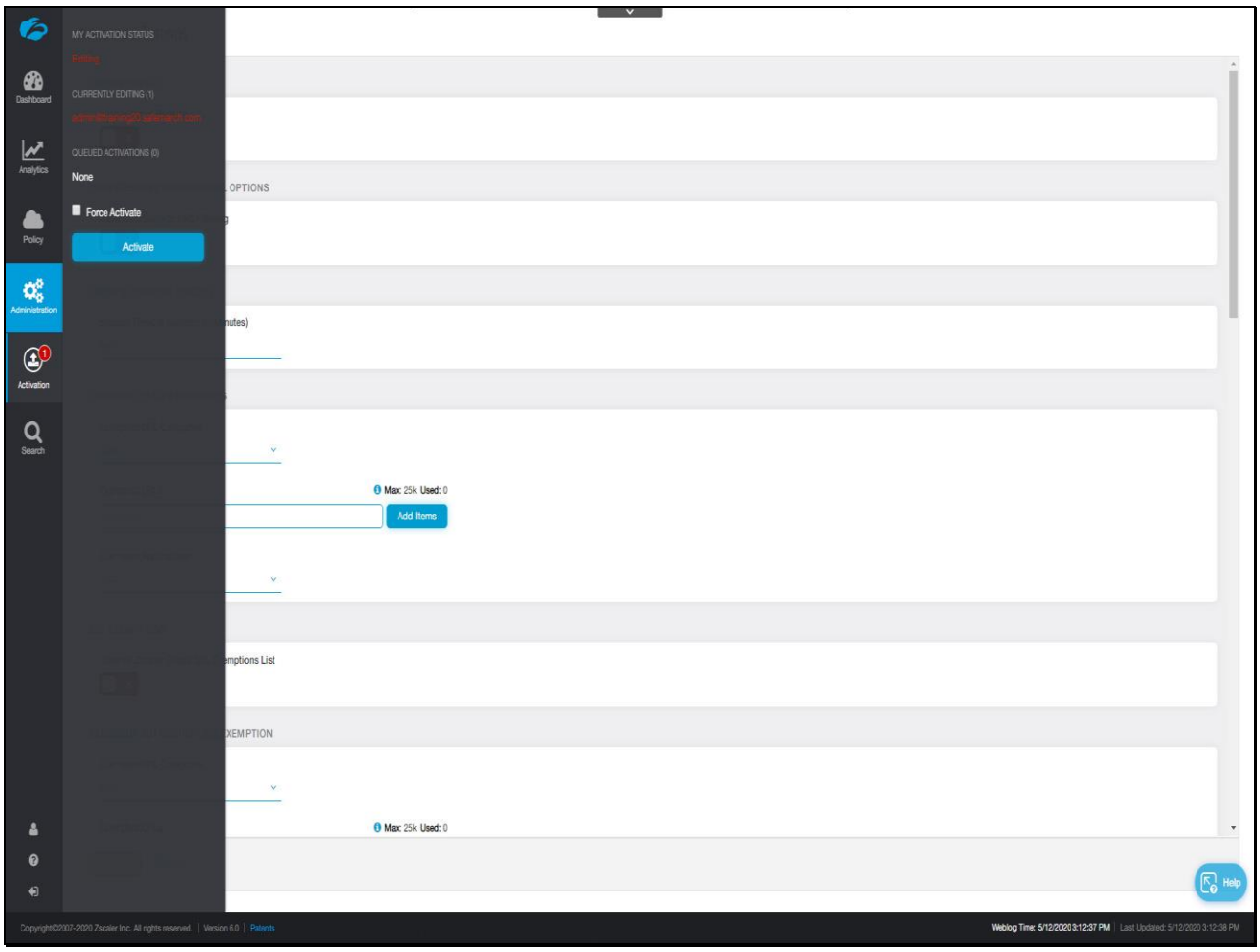
Slide 133 - Slide 133



Slide notes

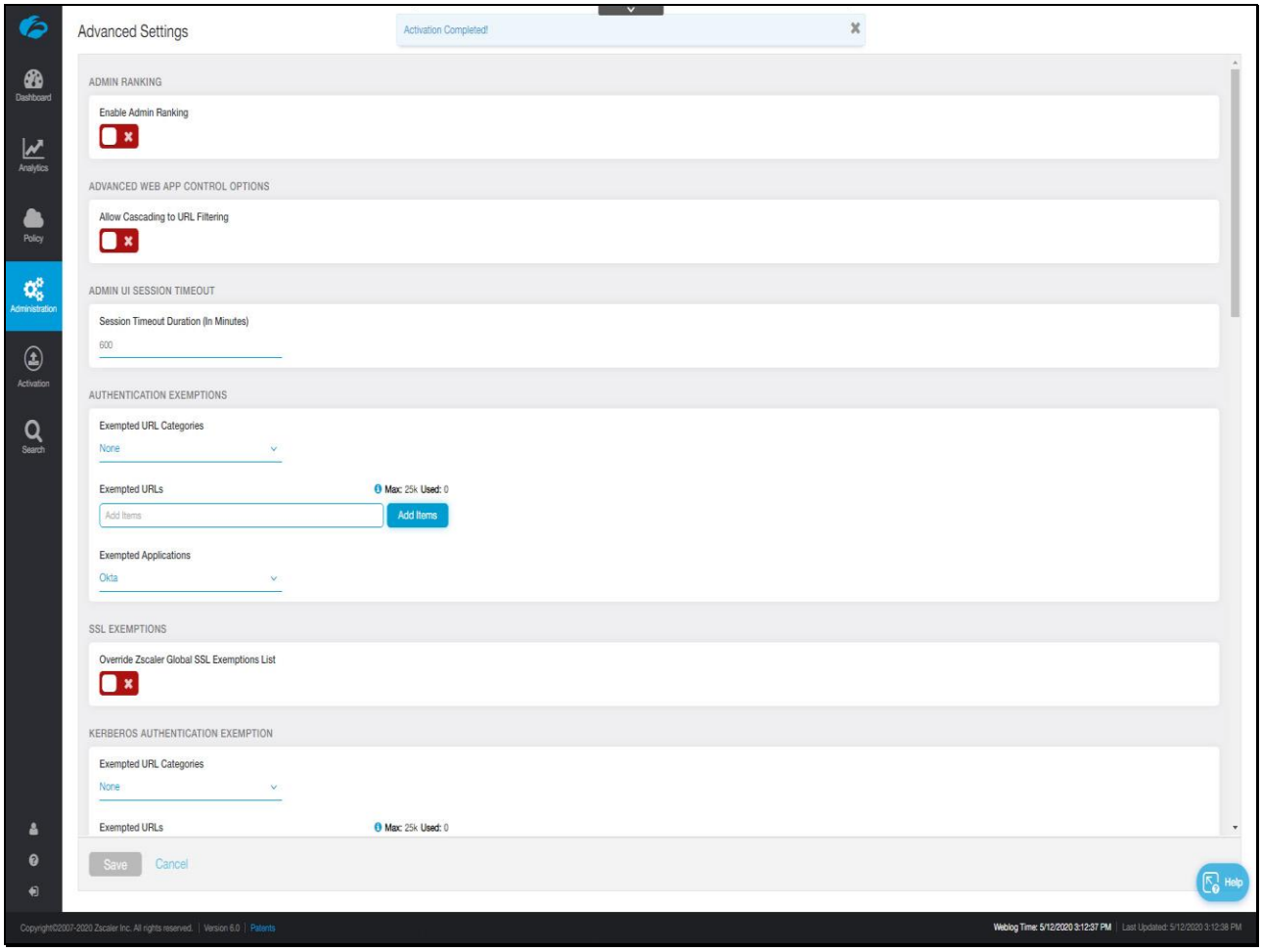
Click Save.

Slide 139 - Slide 139



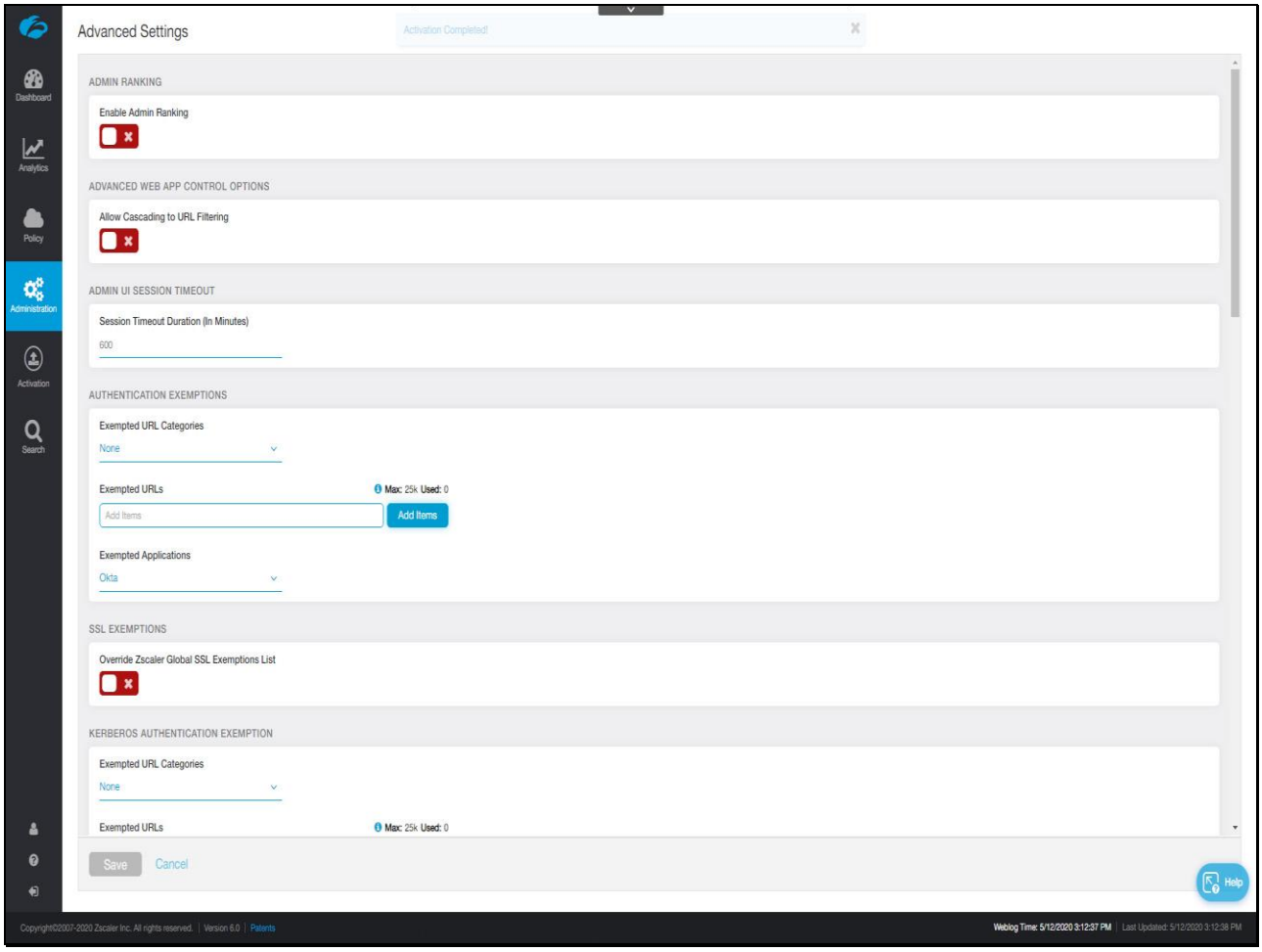
Slide notes

Slide 140 - Slide 140



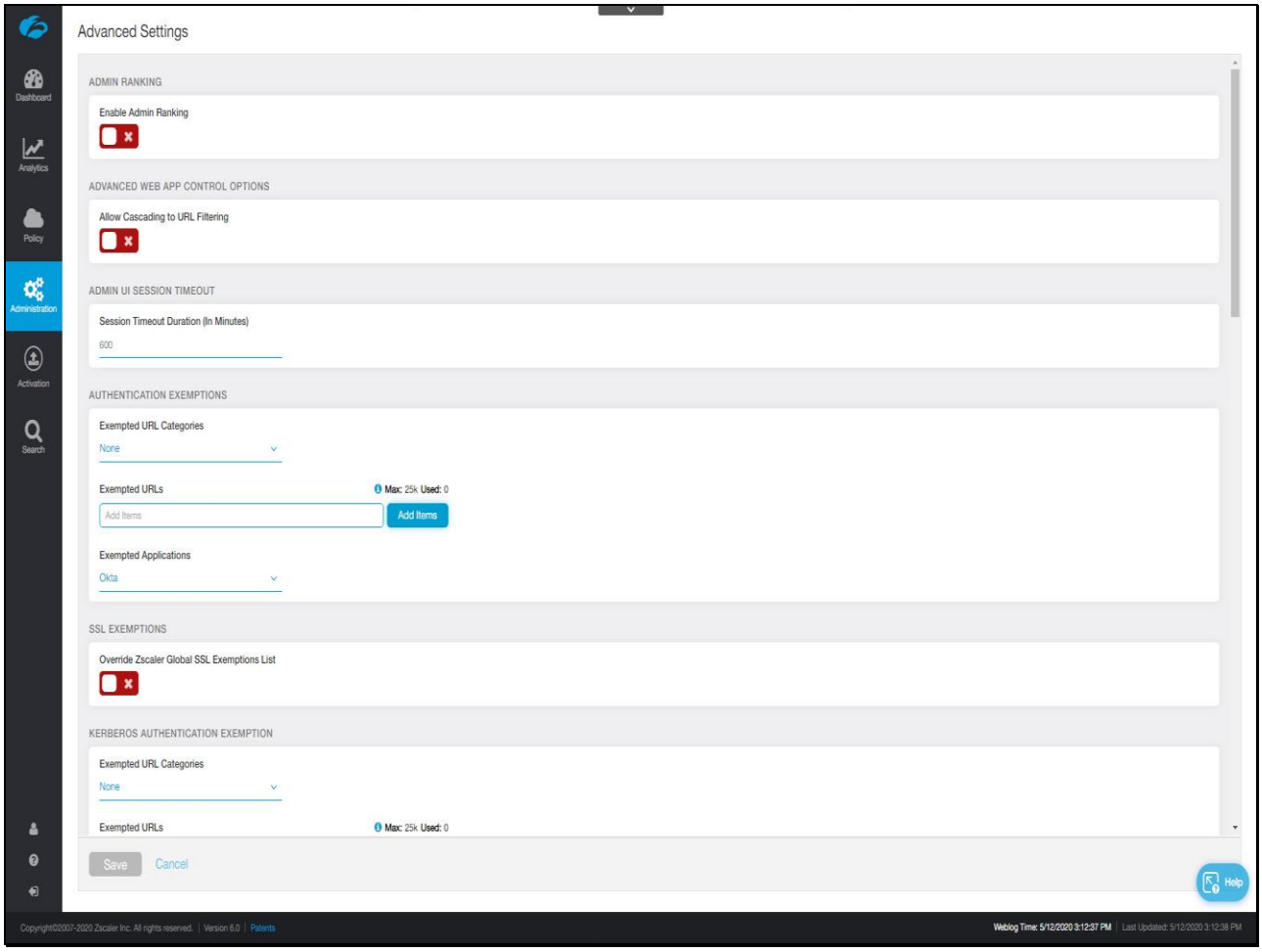
Slide notes

Slide 141 - Slide 141



Slide notes

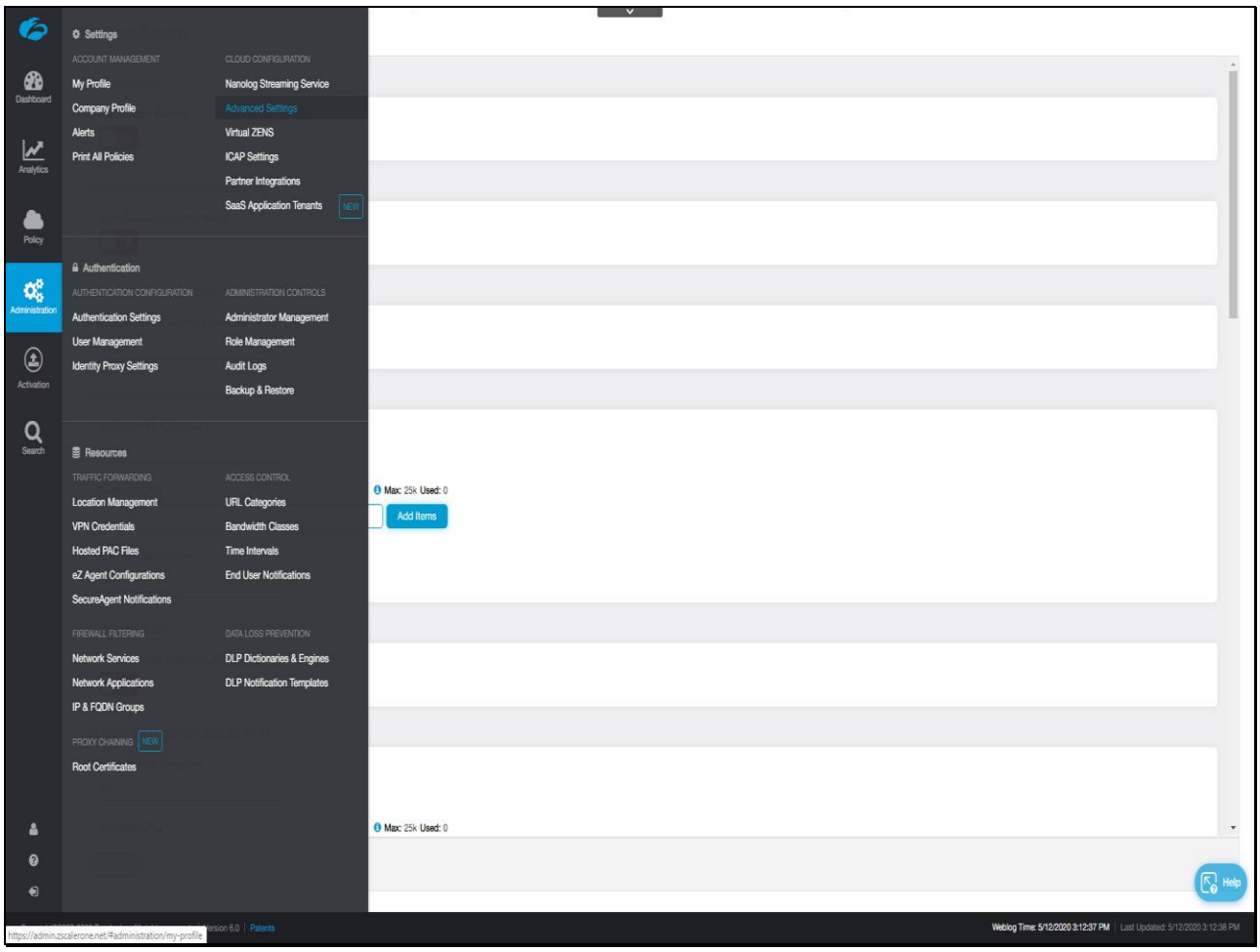
Slide 142 - Slide 142



Slide notes

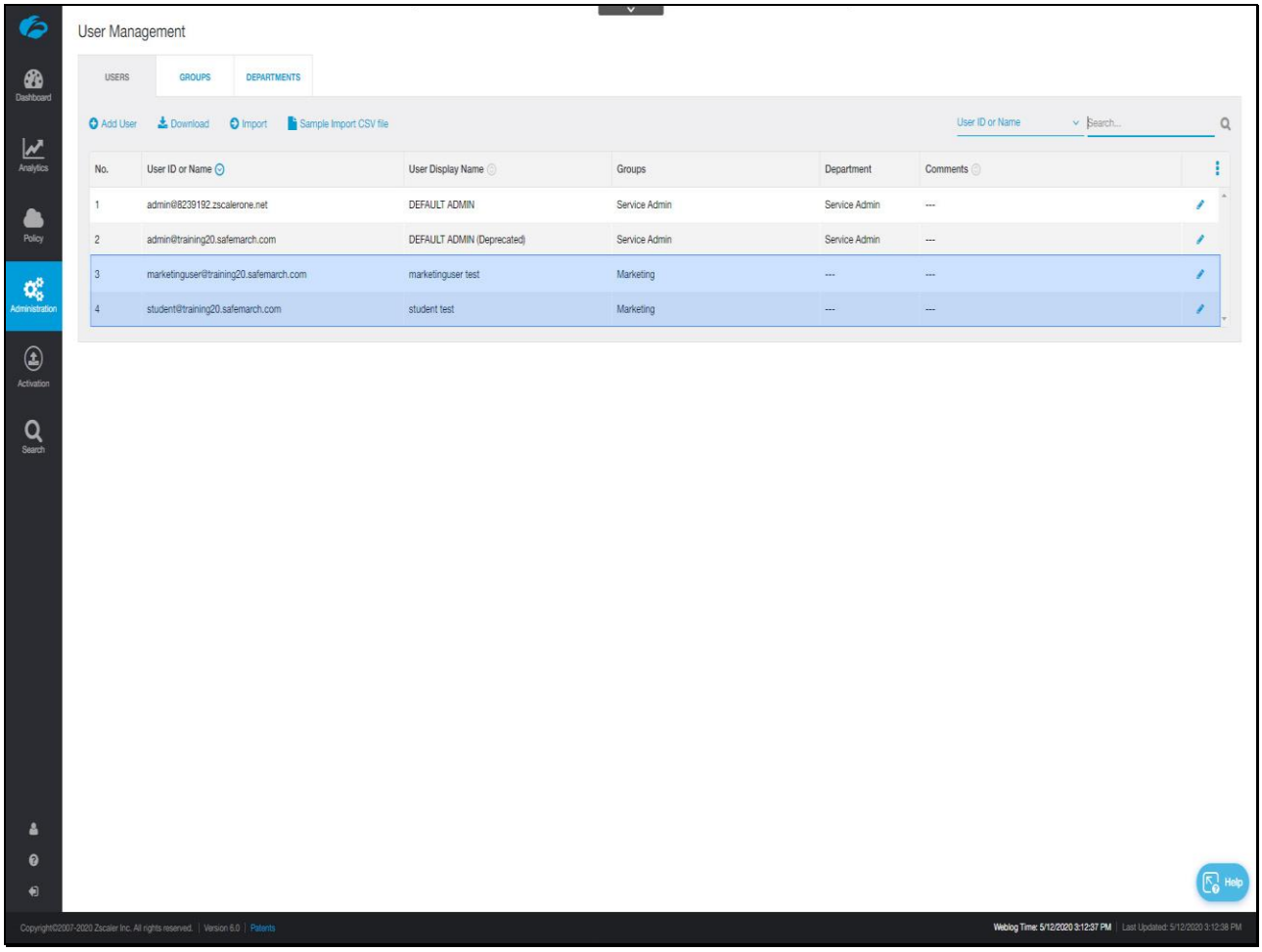
At this point you can now verify that SCIM is active and is importing users via the API by checking the User Database under Administration then **User Database**.

Slide 143 - Slide 143



Slide notes

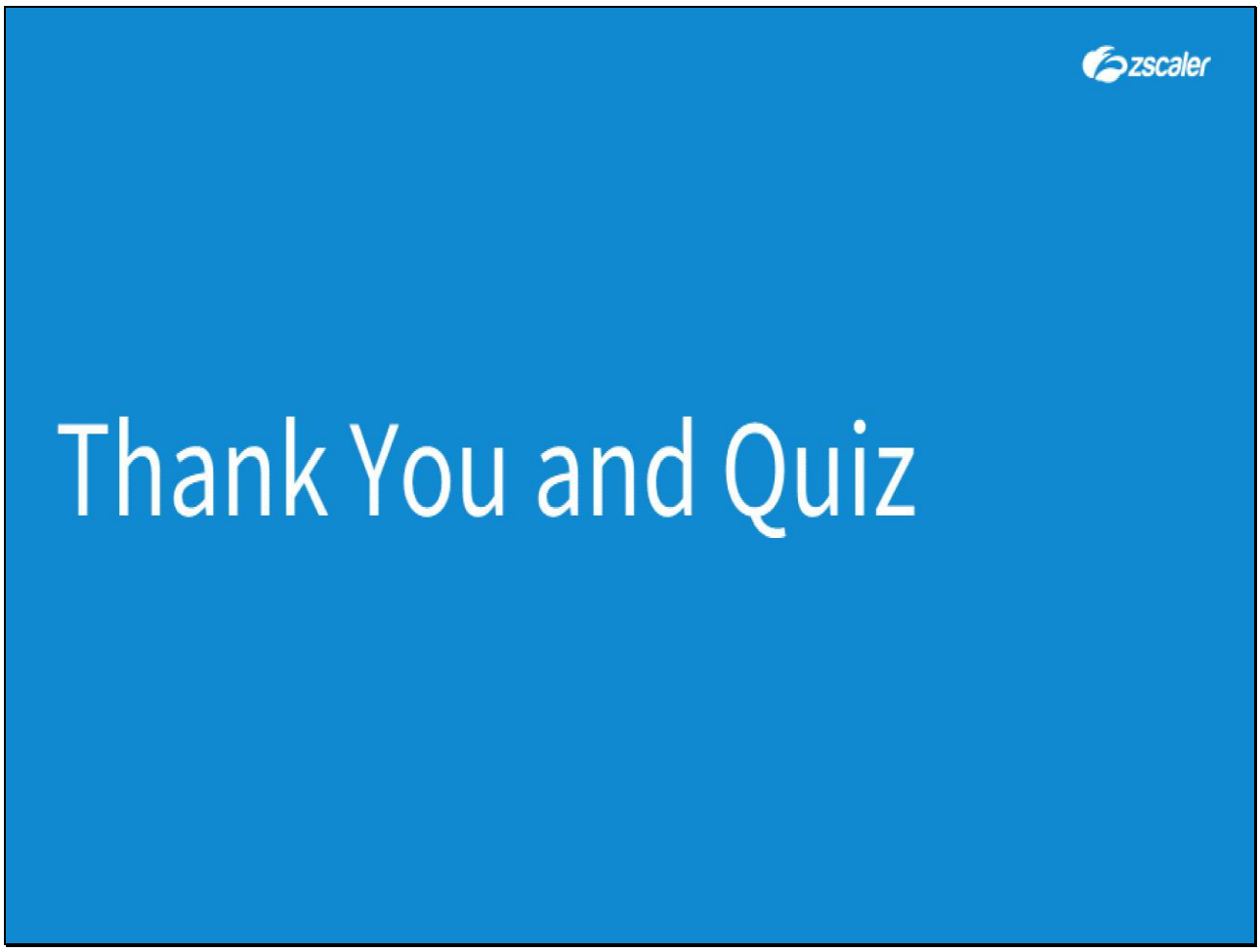
Slide 144 - Slide 144



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



Slide notes

Thank you for partipating 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.