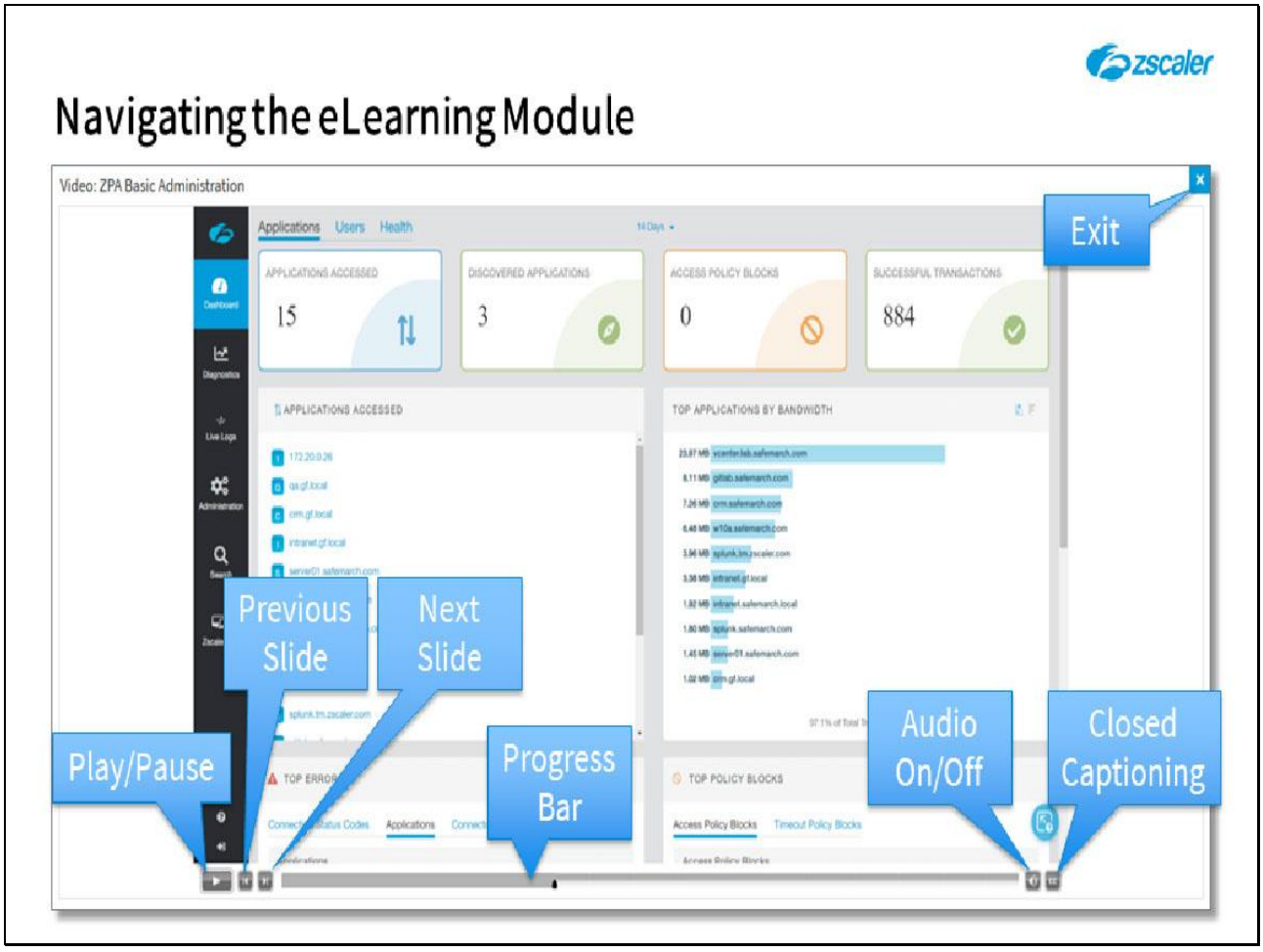
Slide 1 - Zscaler Private Access

Slide notes

Welcome to this training module on Zscaler Private Access basic administration.

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous**, **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 at the top to exit.

Slide 3 - Agenda

Slide notes

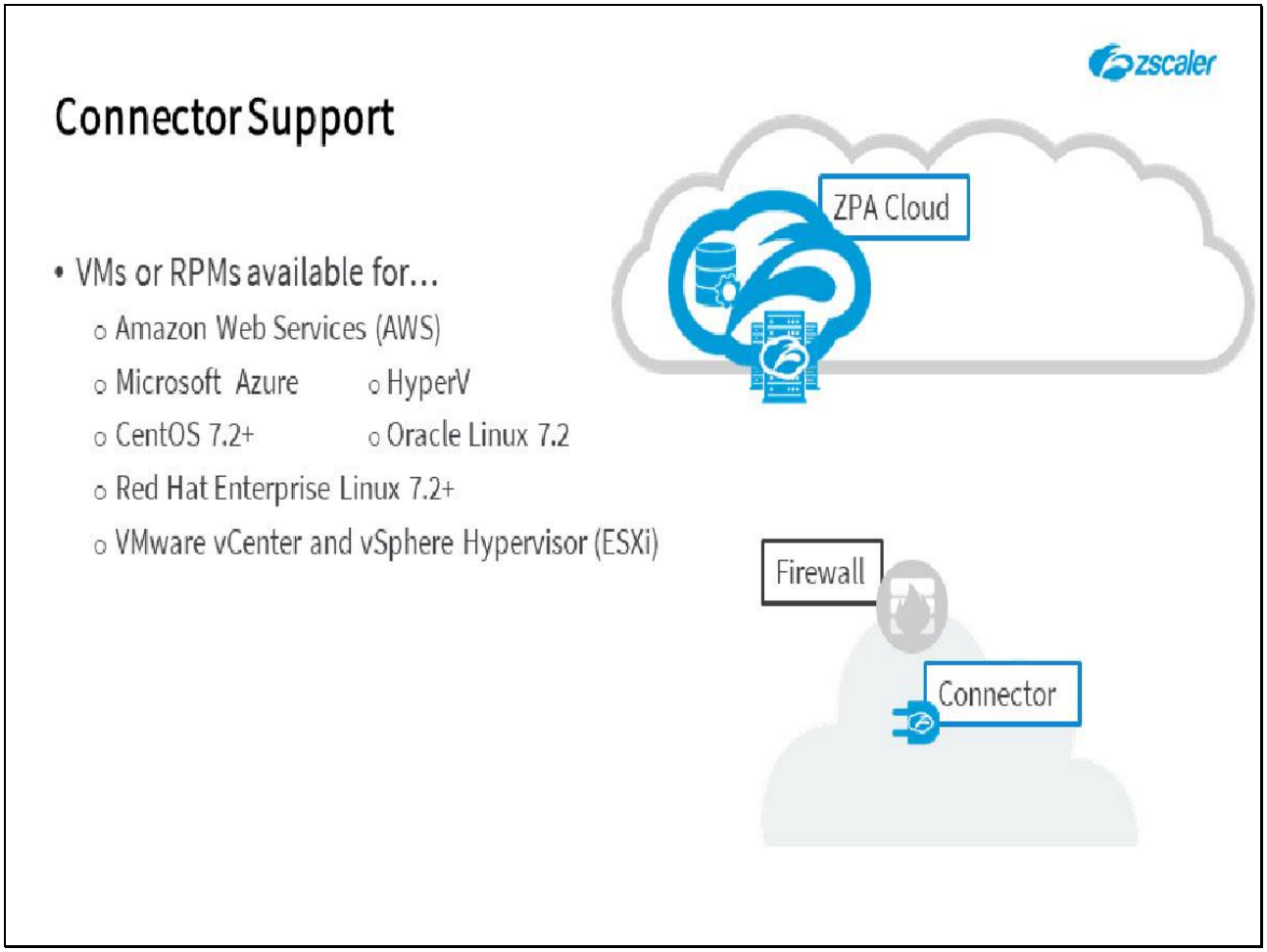
In this module, we will; look at some prerequisites for implementing ZPA, the steps for enabling and configuring ZPA, and at some of the preliminary configuration settings required.

Slide 4 - 1. Verify ZPA Requirements

Slide notes

The first topic that we will cover is a look at some prerequisites for implementing ZPA.

Slide 5 - Connector VMs

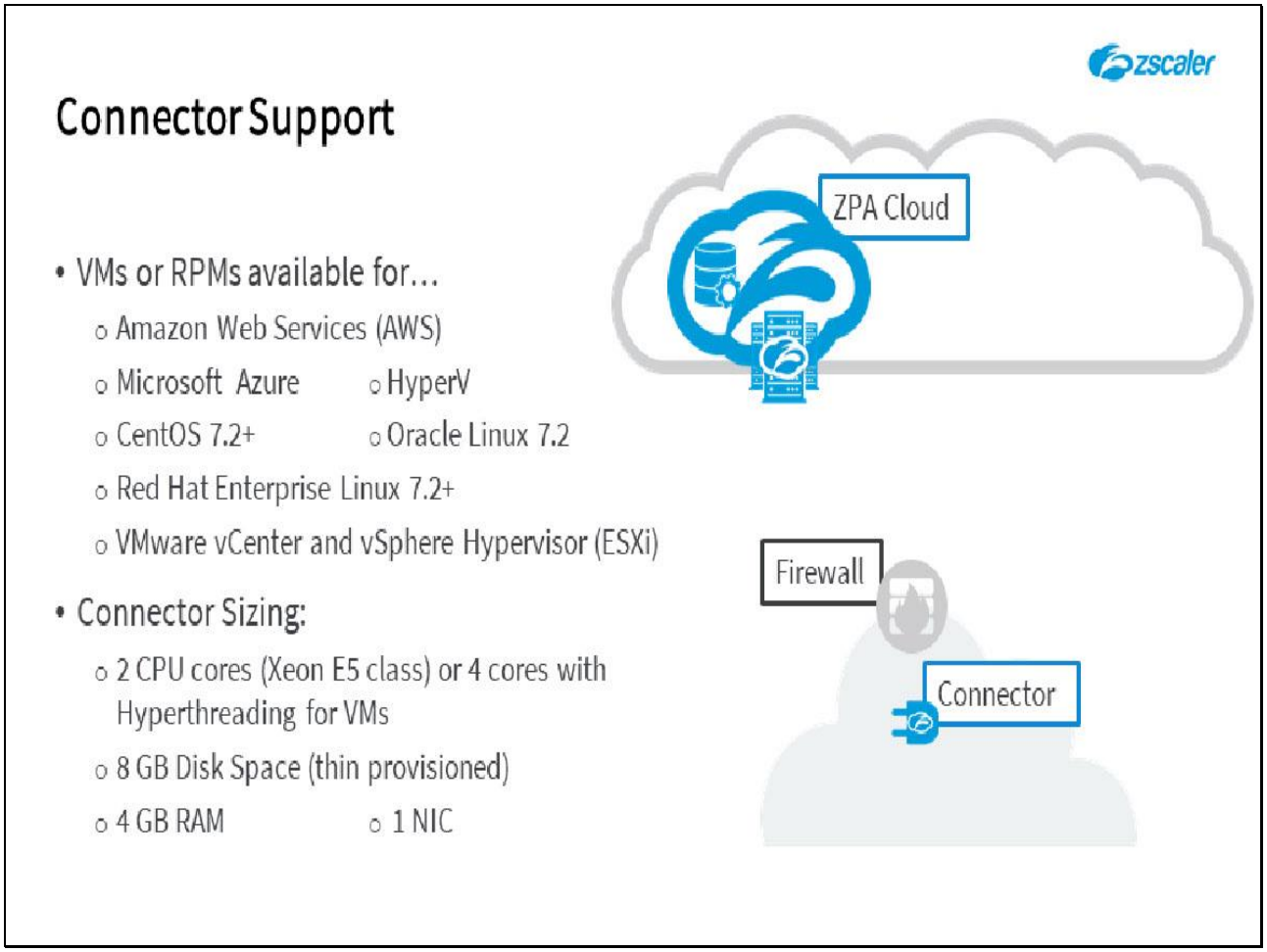


Slide notes

Connectors are lightweight software packages or virtual machines (VM) that are installed in the data centers, private or public cloud instances that host your servers and applications. They connect in the outbound direction to the ZPA Cloud infrastructure, to provide users access to the private applications in your data centers or clouds.

Connector install packages are available for: Amazon Web Services (available as an App in the AWS EC2 Dashboard); Microsoft Azure (available within the Azure App Store), also Microsoft HyperV; CentOS 7.2+; Oracle Linux 7.2; Red Hat Enterprise Linux 7.2+; and VMware, whether as an Appliance with VMware vCenter, or a VMware Appliance with the vSphere Hypervisor (ESXi).

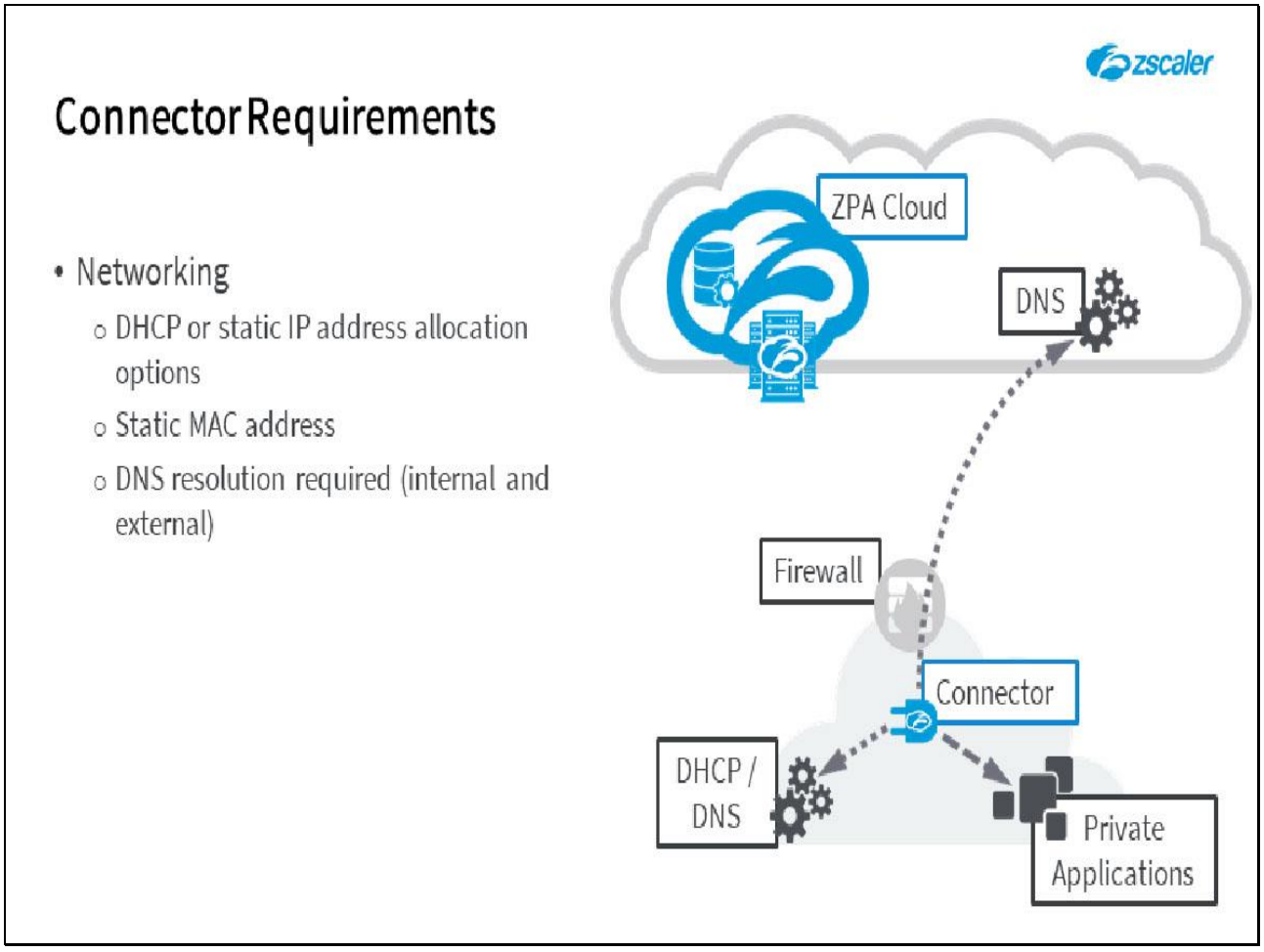
Slide 6 - Connector Support



Slide notes

The host environment must be sized appropriately for a Connector, they require: at least 4 GB RAM; at least 2 CPU cores for physical machines (Xeon E5 class), while VM Connectors need 4 cores with Hyperthreading; at least 8 GB Disk Space (thin provisioned); and of course, a NIC.

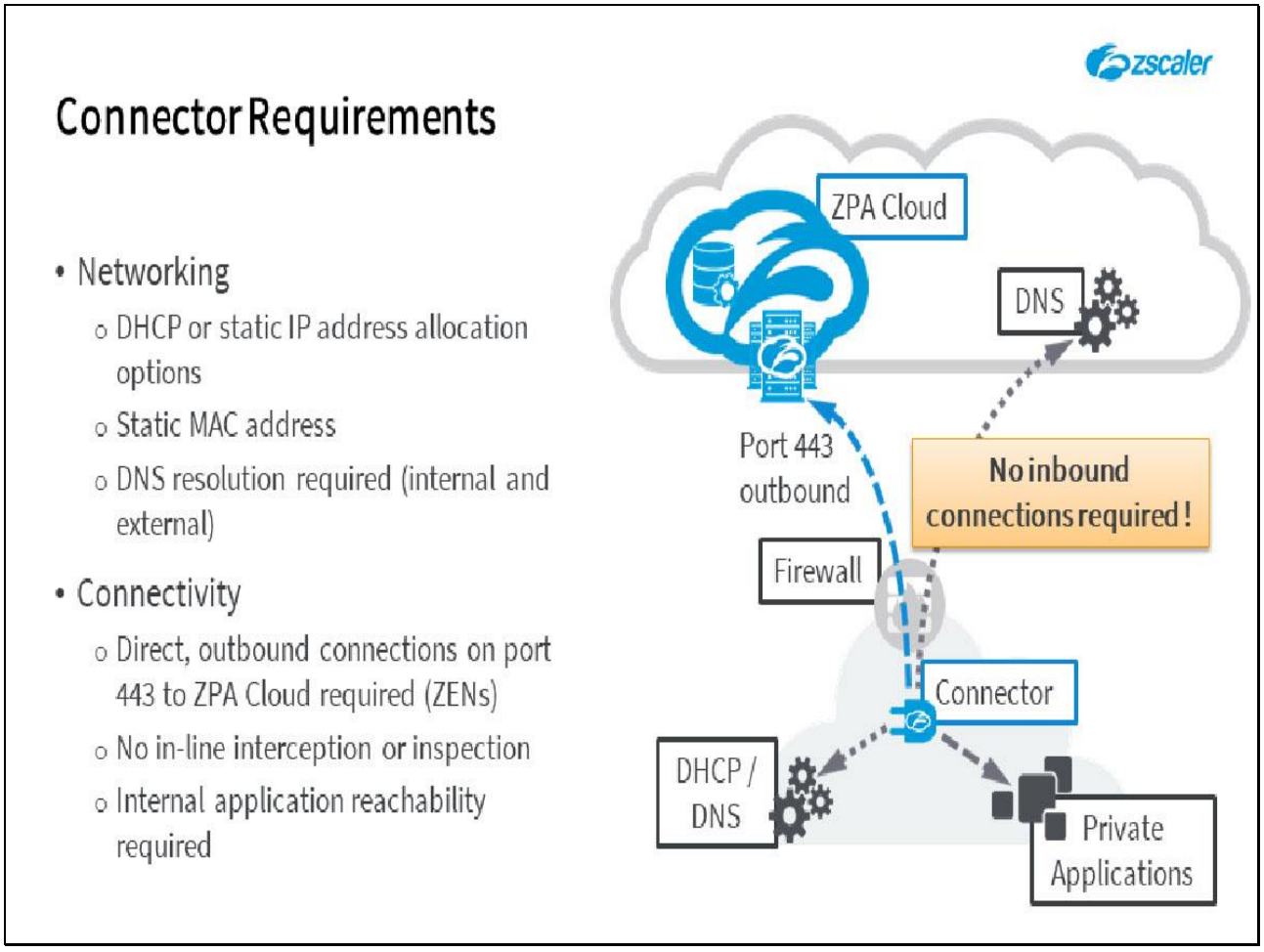
Slide 7 - Connector VMs



Slide notes

Connector VMs must of course have network connectivity, and may obtain their IP address, and DNS Server configurations dynamically by DHCP, or they may be configured with static IPs if required. They must use static MAC addresses. The Connectors must also be able to DNS resolve both internal and external hosts.

Slide 8 - Connector Requirements

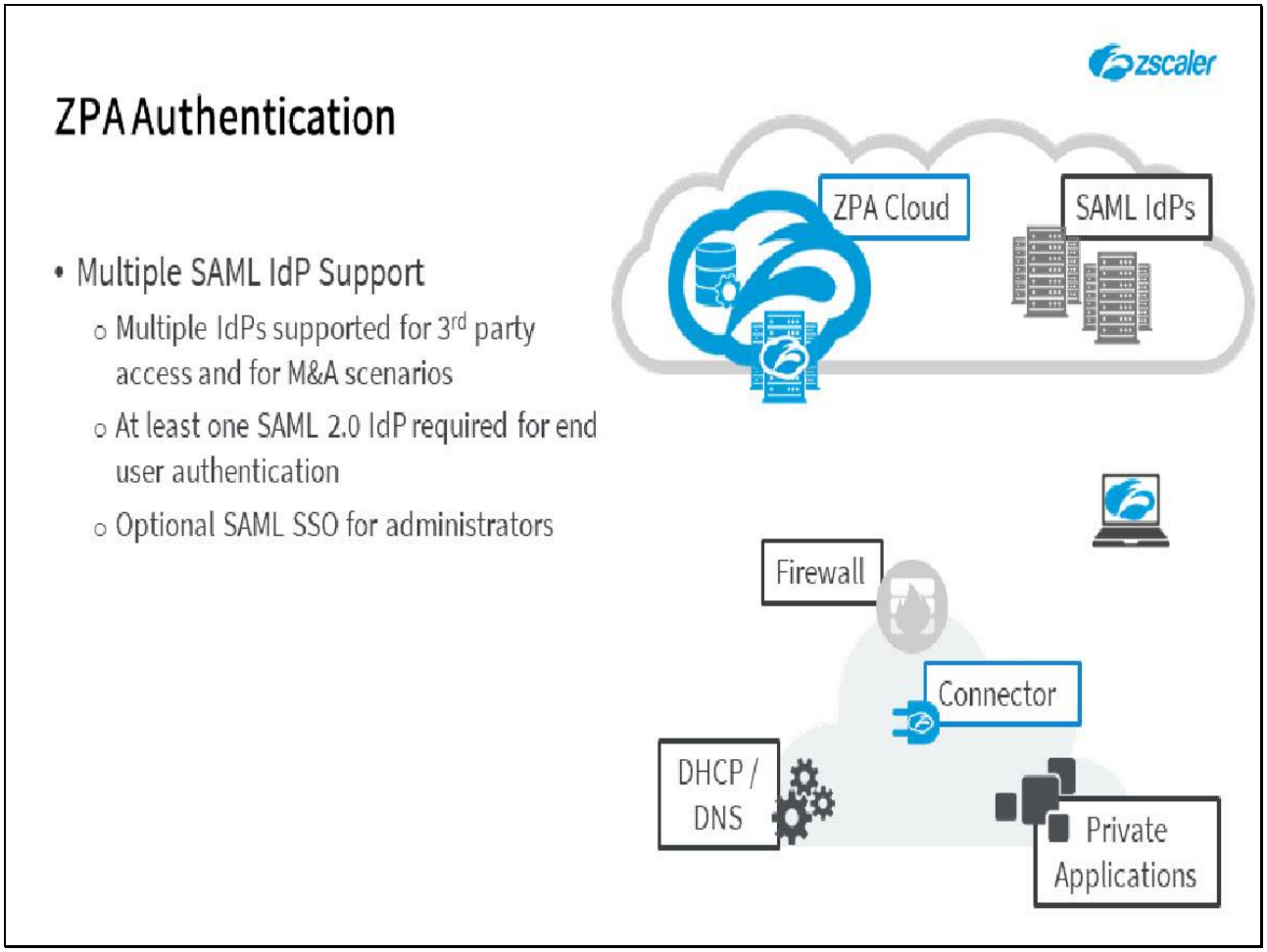


Slide notes

Connectors accept no inbound connections but must be able to connect to ZPA Cloud entities outbound on TCP port 443. Your firewall must be configured to allow outbound communications on port 443 and to perform NAT for the source IP addresses of the Connectors. Proxy implementations (including ZIA) are not recommended and in-line inspection, or man-in-the-middle attack interception by third parties is not supported at all (by design).

The Connectors must of course have connectivity across your internal network to the servers that host your private applications.

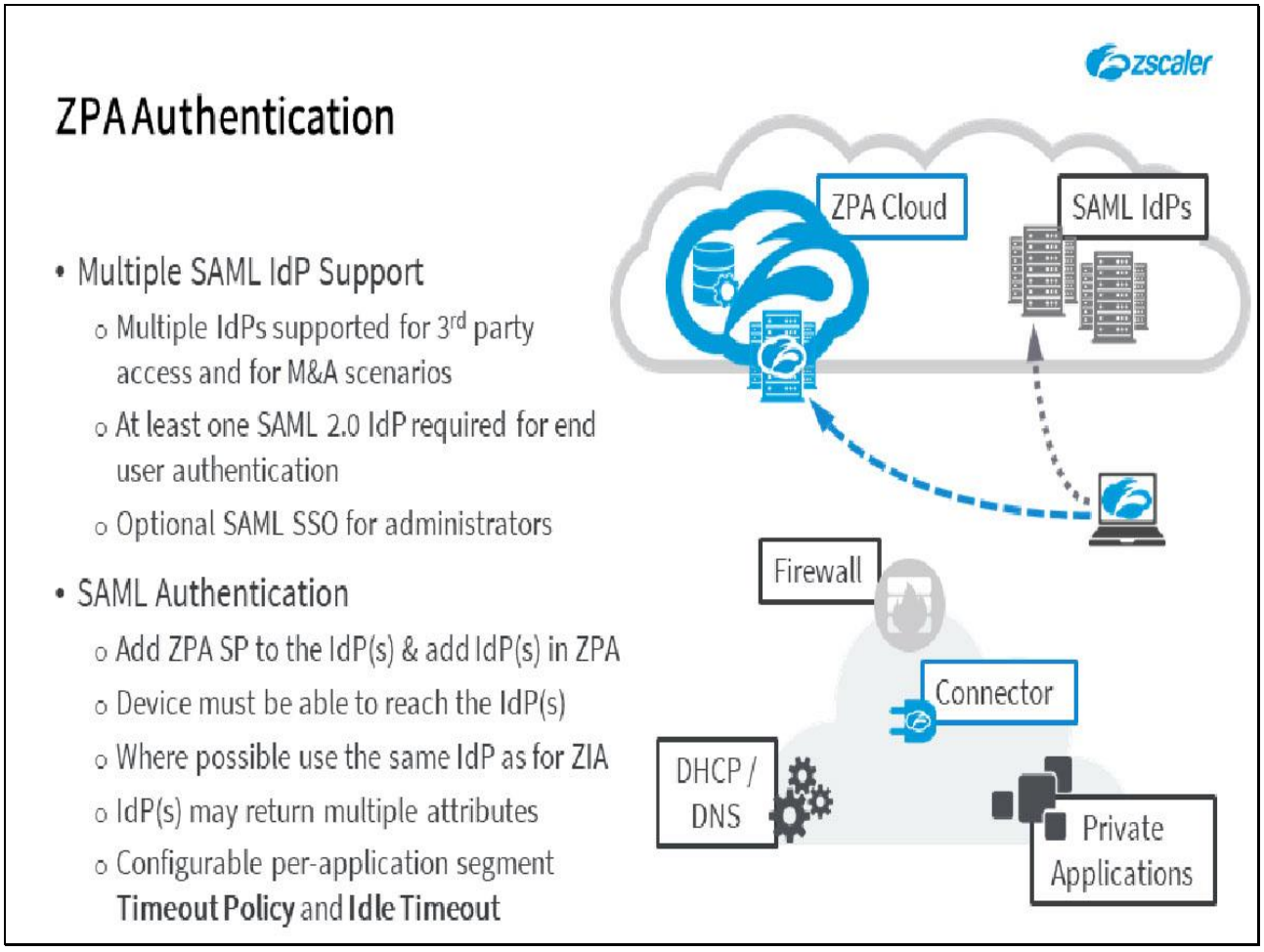
Slide 9 - ZPA Authentication



Slide notes

For users to connect to your ZPA applications, they must first authenticate either through the Zscaler App, or in a browser using any SAML 2.0 compliant Identity Provider (IdP). Multiple IdPs are supported to allow flexible end user authentication in Merger and Acquisition (M&A) and 3rd party access scenarios. Optionally, you may also use SAML single sign-on (SSO) authentication for your administrators.

Slide 10 - ZPA Authentication



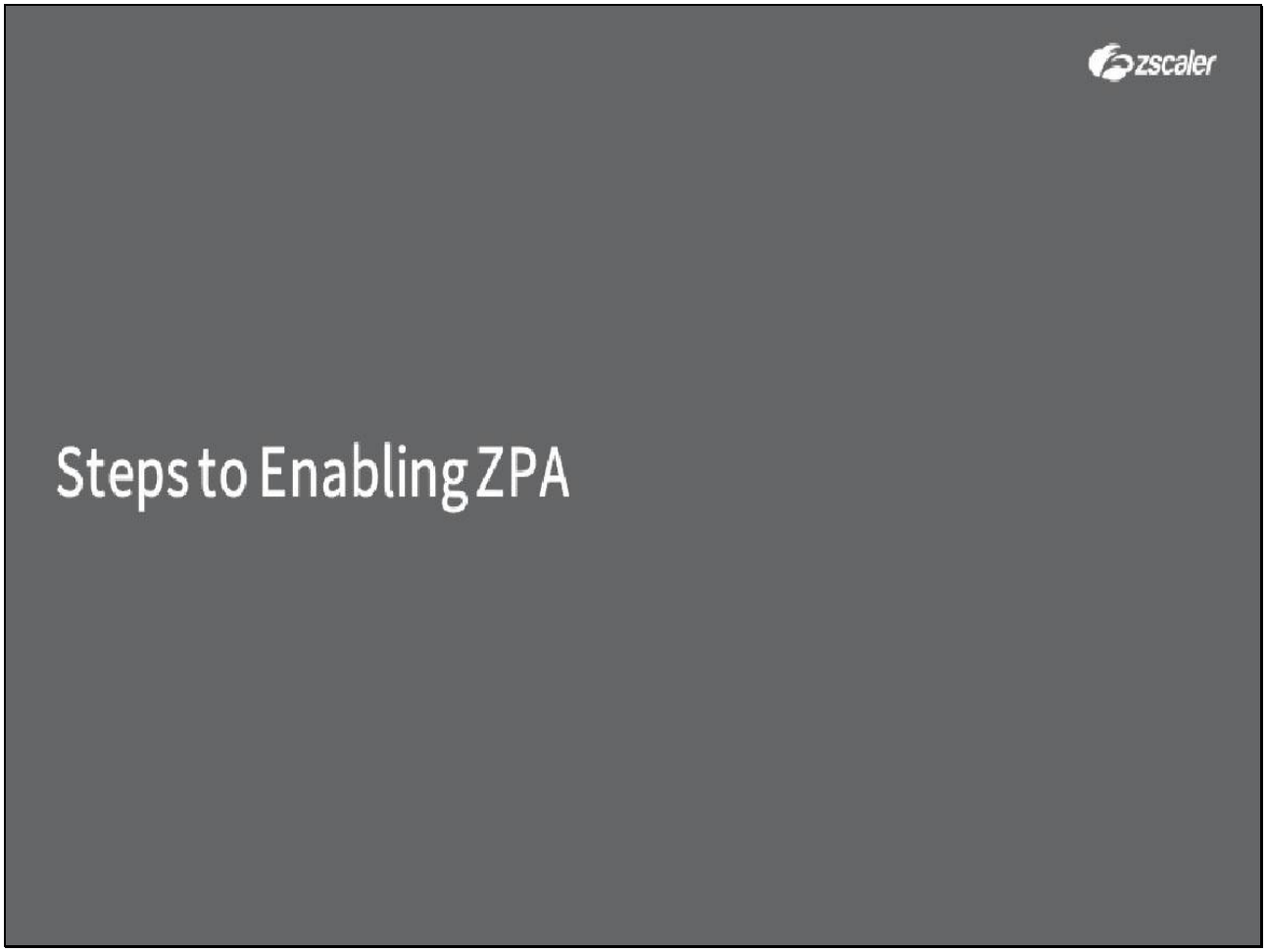
Slide notes

The IdP must be configured to recognize Zscaler as a valid Service Provider (aka Relying Party), and you must provide full details for the IdP in the ZPA Admin Portal. End user devices must of course be able to reach the IdP (also administrator devices if the administrator SSO option is enabled), which may require Firewall rules on the corporate network Firewalls, and an **Authentication Exemption** defined in the ZIA Admin Portal (if applicable).

If you also use the Zscaler App for Internet access, authentication into the App for the ZIA service should also use SAML, and ideally one of the same IdPs as for ZPA (to avoid the end user having to login twice). For the ZPA service, IdPs may provide multiple authorization attributes on a successful authentication, there are no limitations to the number or type of attributes supported. SAML attributes can later be used in your Access Policy rules to control access to your applications.

You have the option to create per-**Application Segment Timeout Policy** and **Idle Timeouts**, which can be set in days, hours or minutes. There is a default **Timeout Policy** rule with an interval of 7 days.

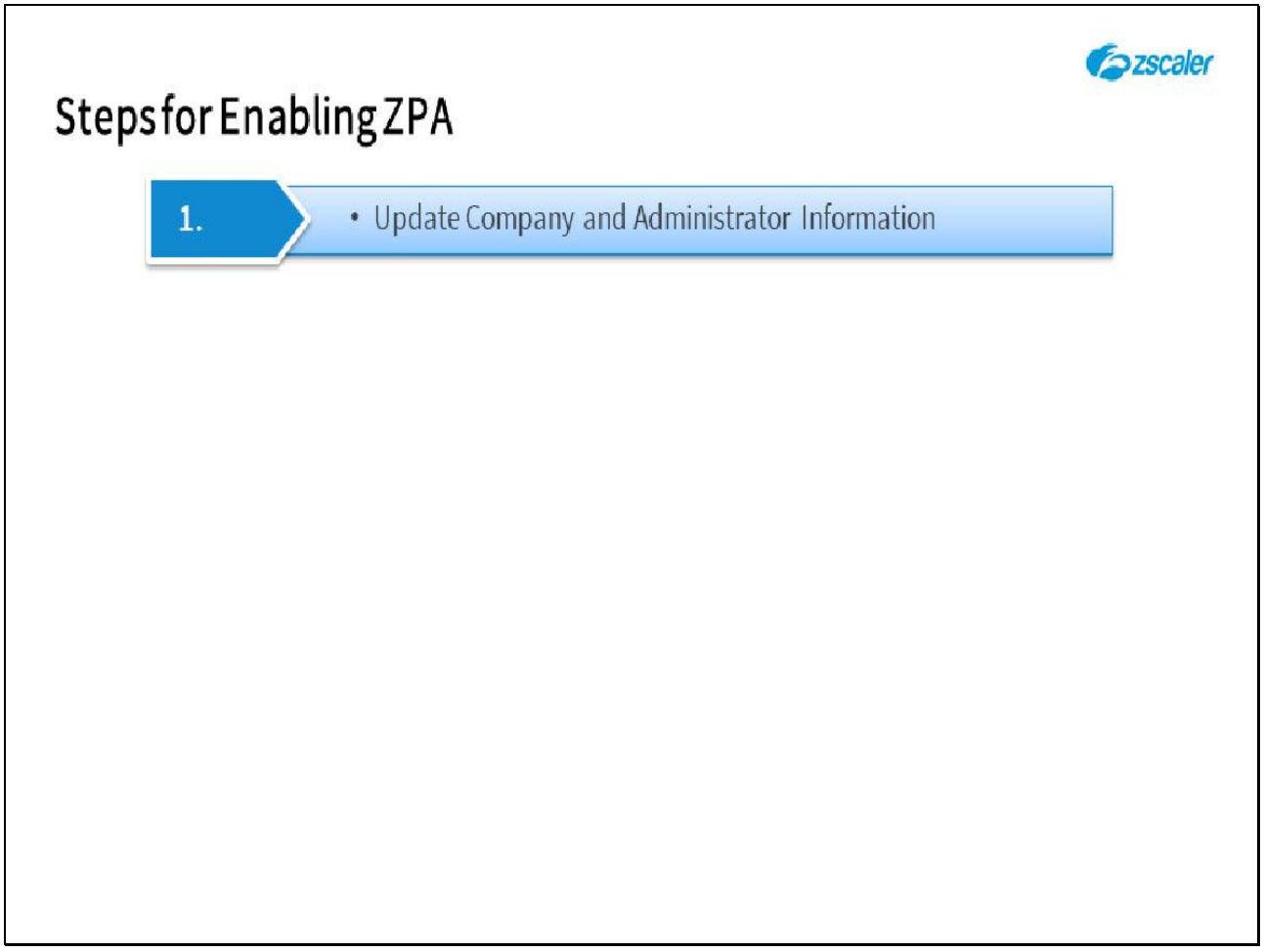
Slide 11 - Steps to Enabling ZPA



Slide notes

In the next section we will cover the steps required to enable and configure ZPA for first time use.

Slide 12 - Steps for Enabling ZPA

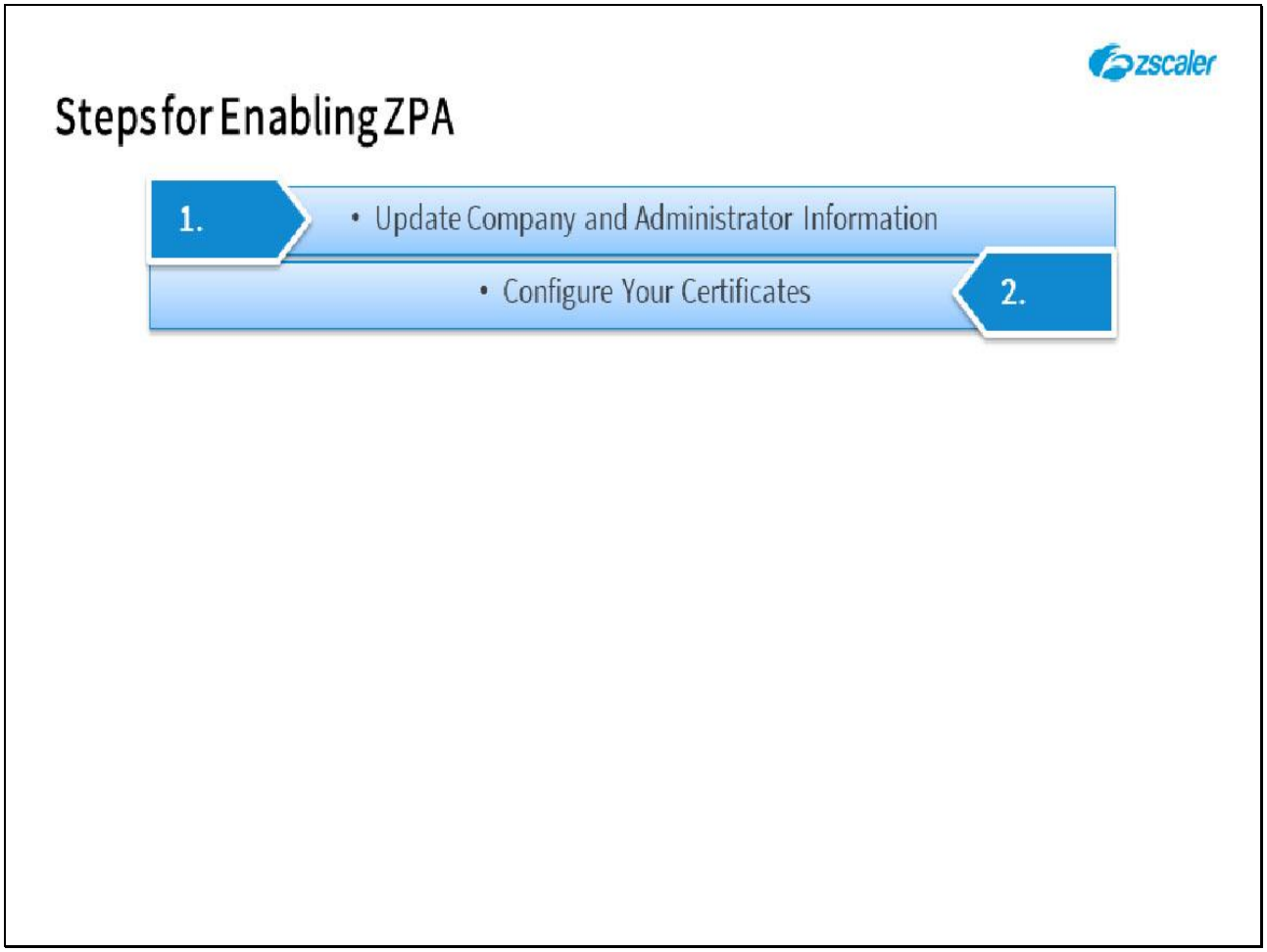


Slide notes

Refer to the ZPA Step-by-Step Configuration Guide on the Zscaler Help Portal for full details of the steps to enabling and configuring ZPA.

Step 1 of the process is to ensure that your Company data is correct in the ZPA Admin Portal and add and configure your admin users.

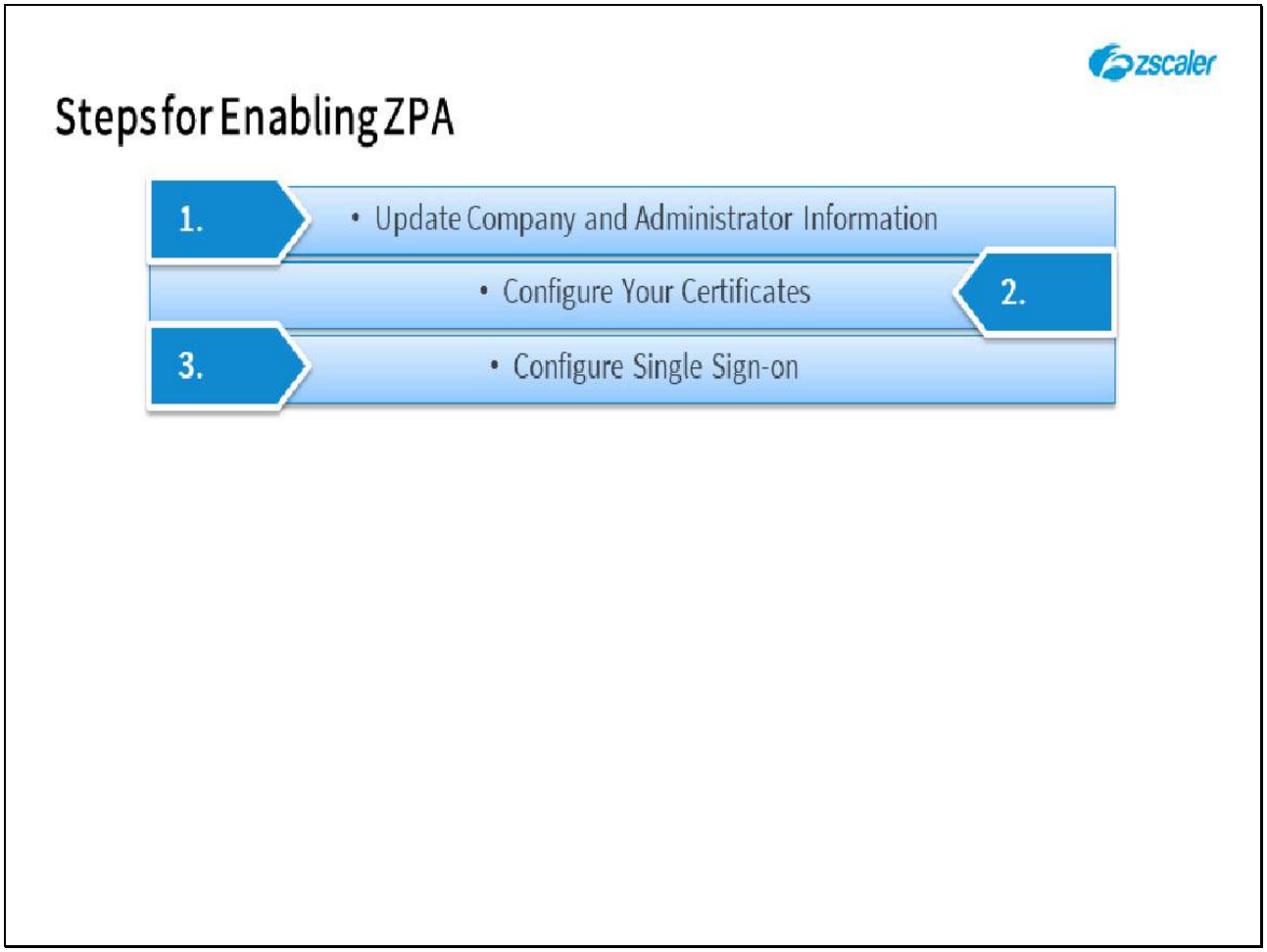
Slide 13 - Steps for Enabling ZPA



Slide notes

At **Step 2**, you must decide whether you want to use the default ZPA certificates, create your own set, or use custom certificates signed by the CA of your choice.

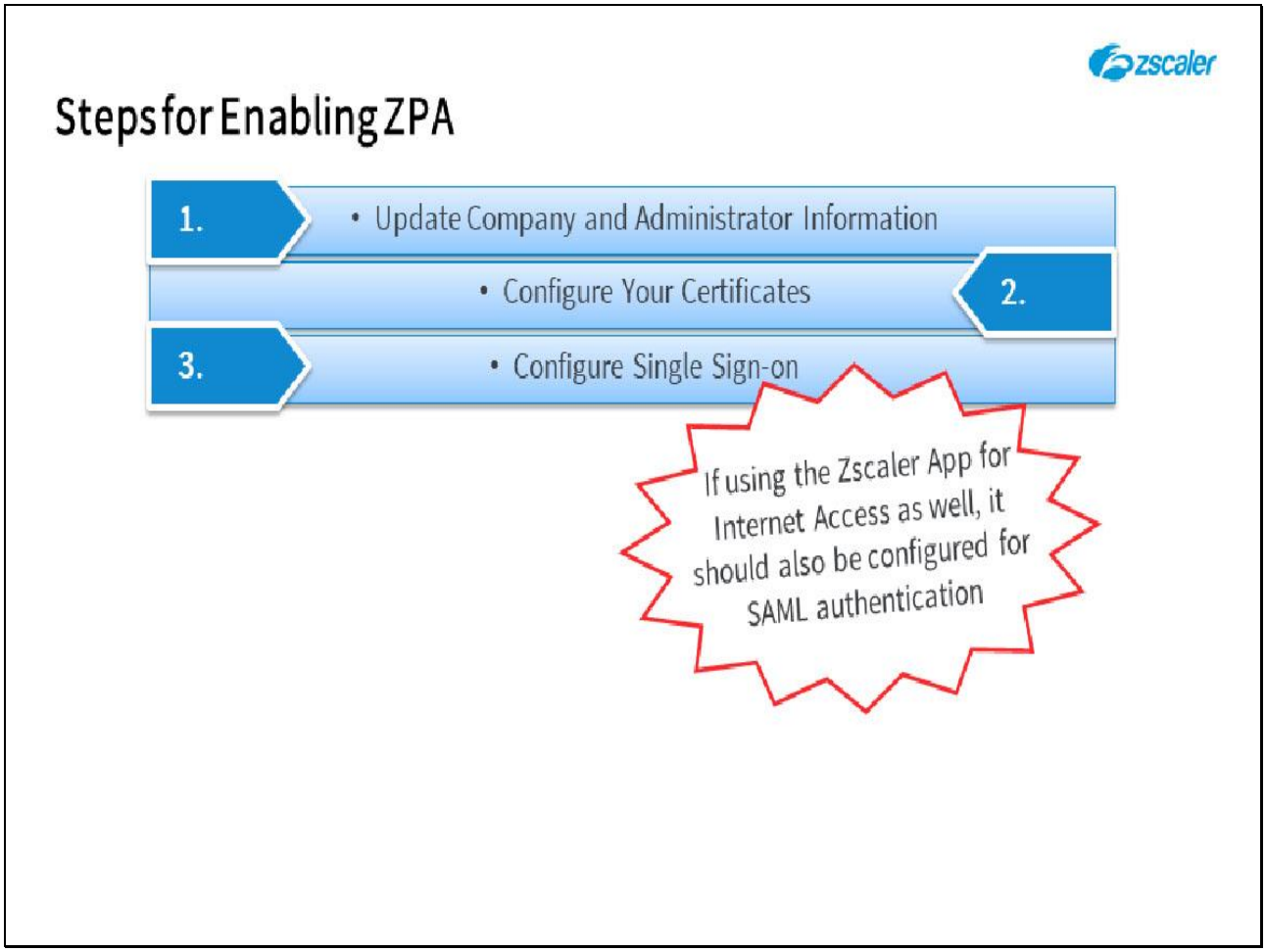
Slide 14 - Steps for Enabling ZPA



Slide notes

ZPA requires SAML authentication, so at **Step 3** you need to provide the details for your chosen Identity Provider (IdP).

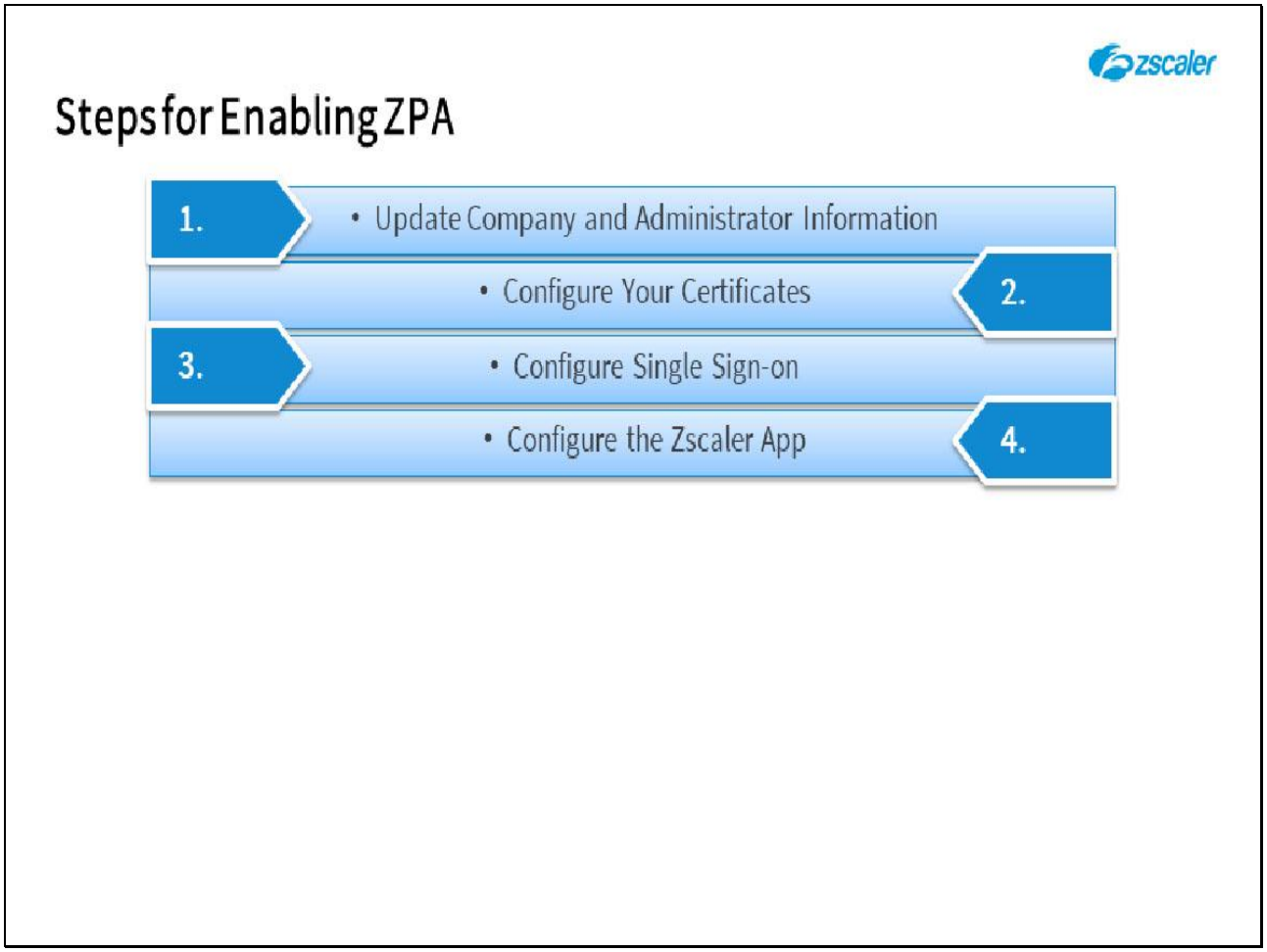
Slide 15 - Steps for Enabling ZPA



Slide notes

Note that if you also use the Zscaler App for Internet Access, it should also be configured for SAML authentication, ideally using the same IdP (otherwise the users will see 2 login screens).

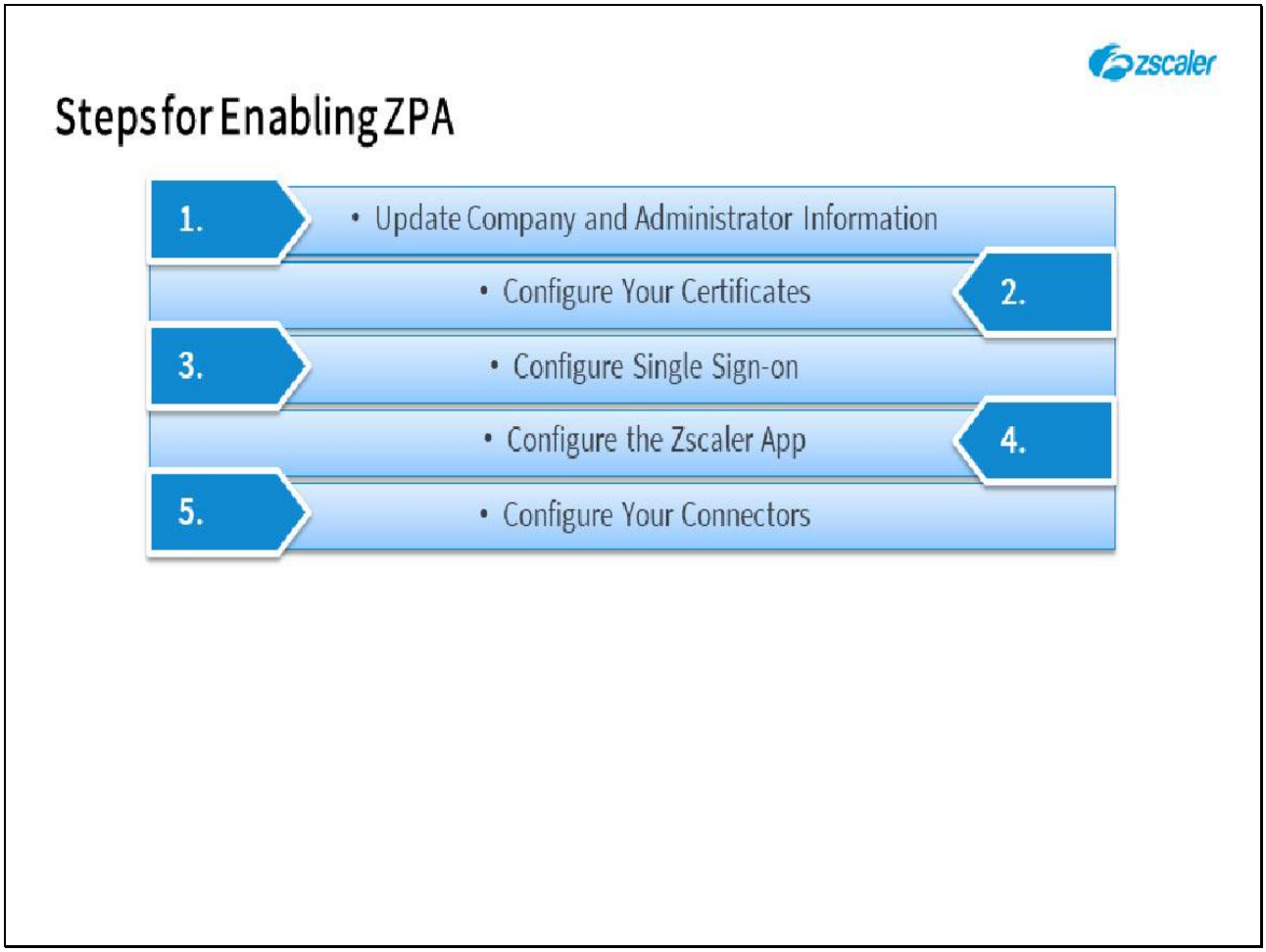
Slide 16 - Steps for Enabling ZPA



Slide notes

Normally, the Zscaler App is required for ZPA access to your private applications, so **Step 4** is to distribute it to those users who will need it and configure the App for your environment.

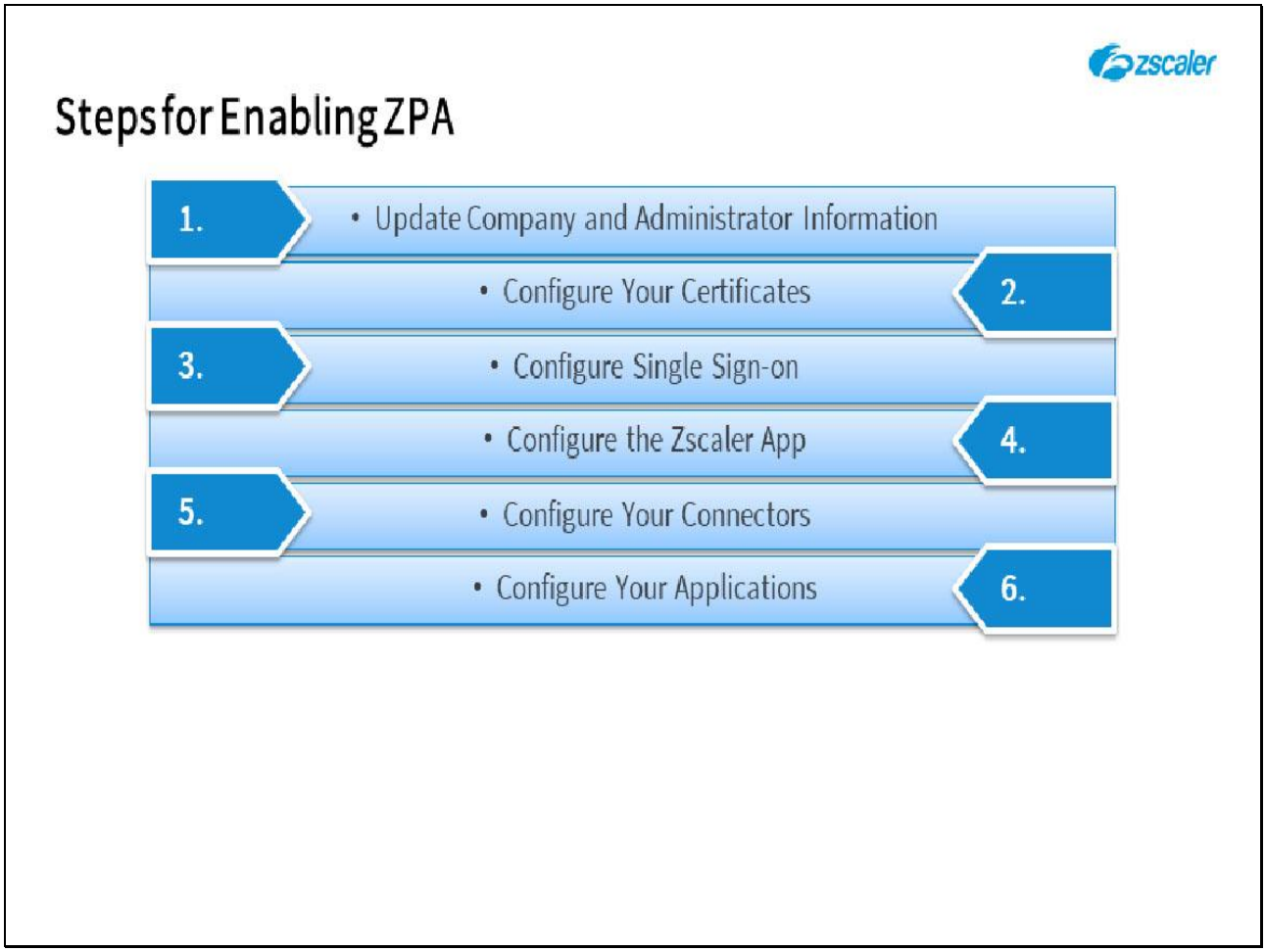
Slide 17 - Steps for Enabling ZPA



Slide notes

Step 5 is to add and provision the Connectors that you will need, adjacent to the applications that you want to allow ZPA access for. This step also includes downloading the Connector VM image, or Connector SW that you will require.

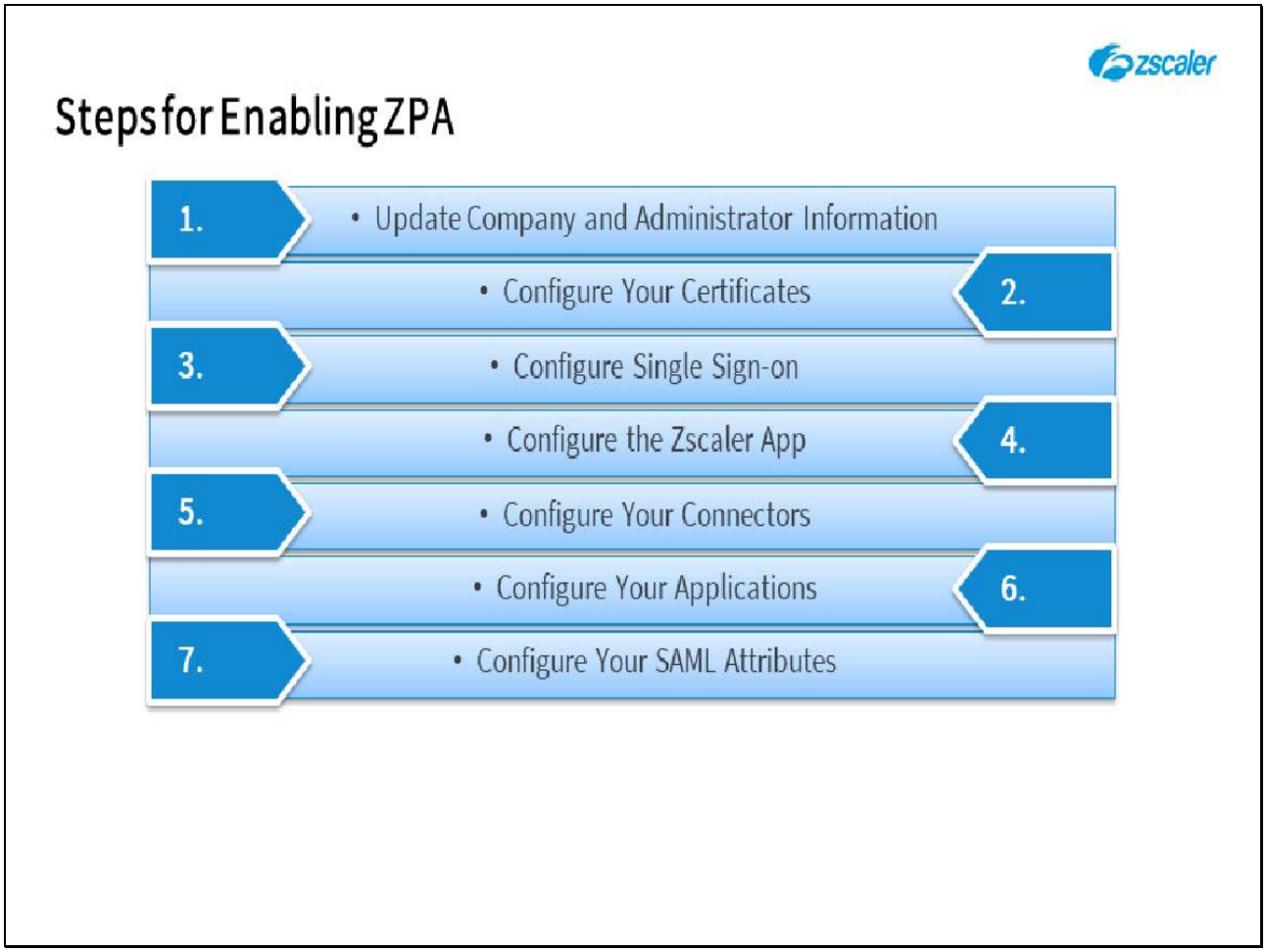
Slide 18 - Steps for Enabling ZPA



Slide notes

At **Step 6** you will configure the applications that you wish to enable ZPA access for, and optionally enable application discovery.

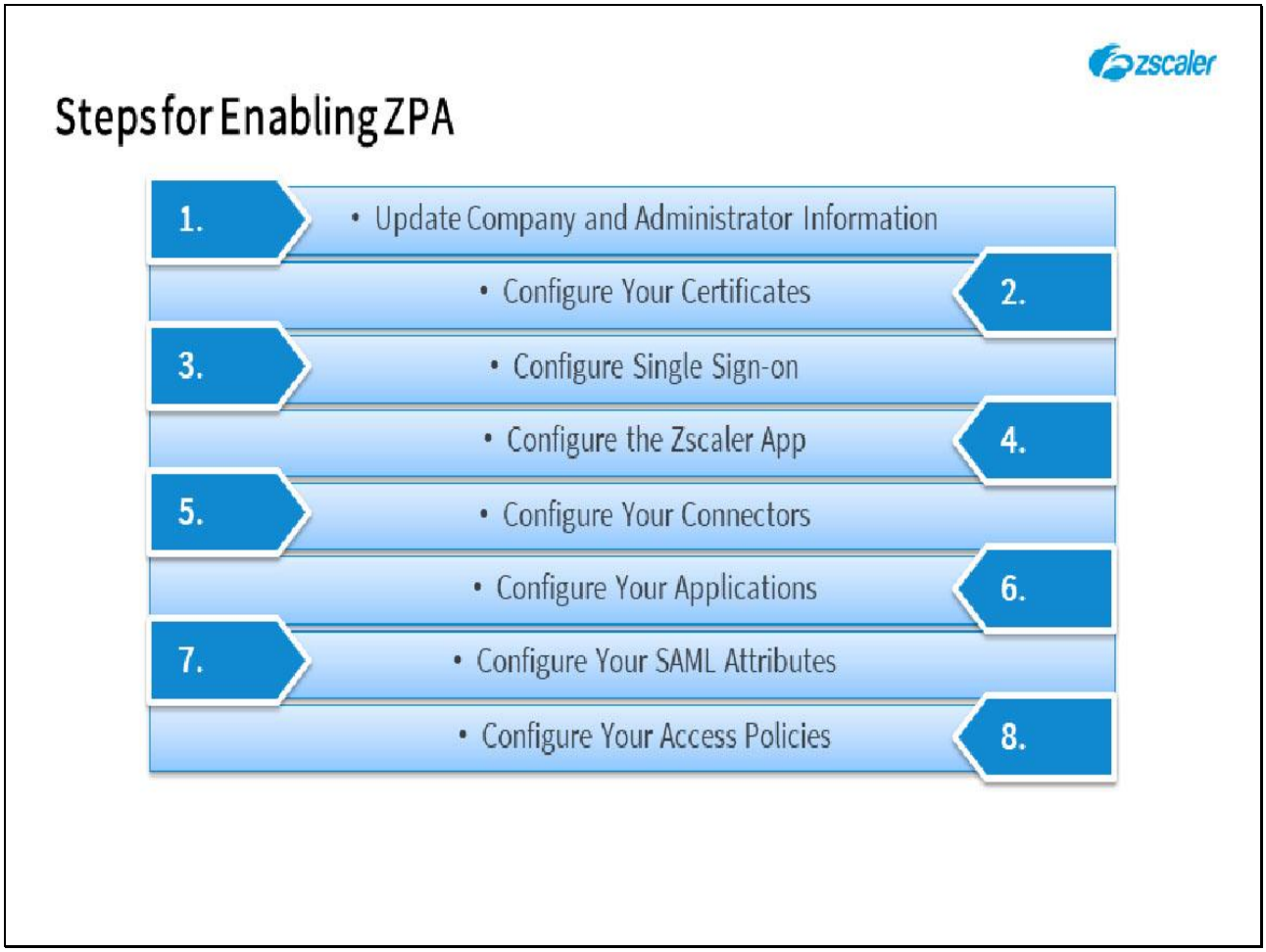
Slide 19 - Steps for Enabling ZPA



Slide notes

At **Step 7** you will add any SAML attributes that you need to refer to in your access policies…

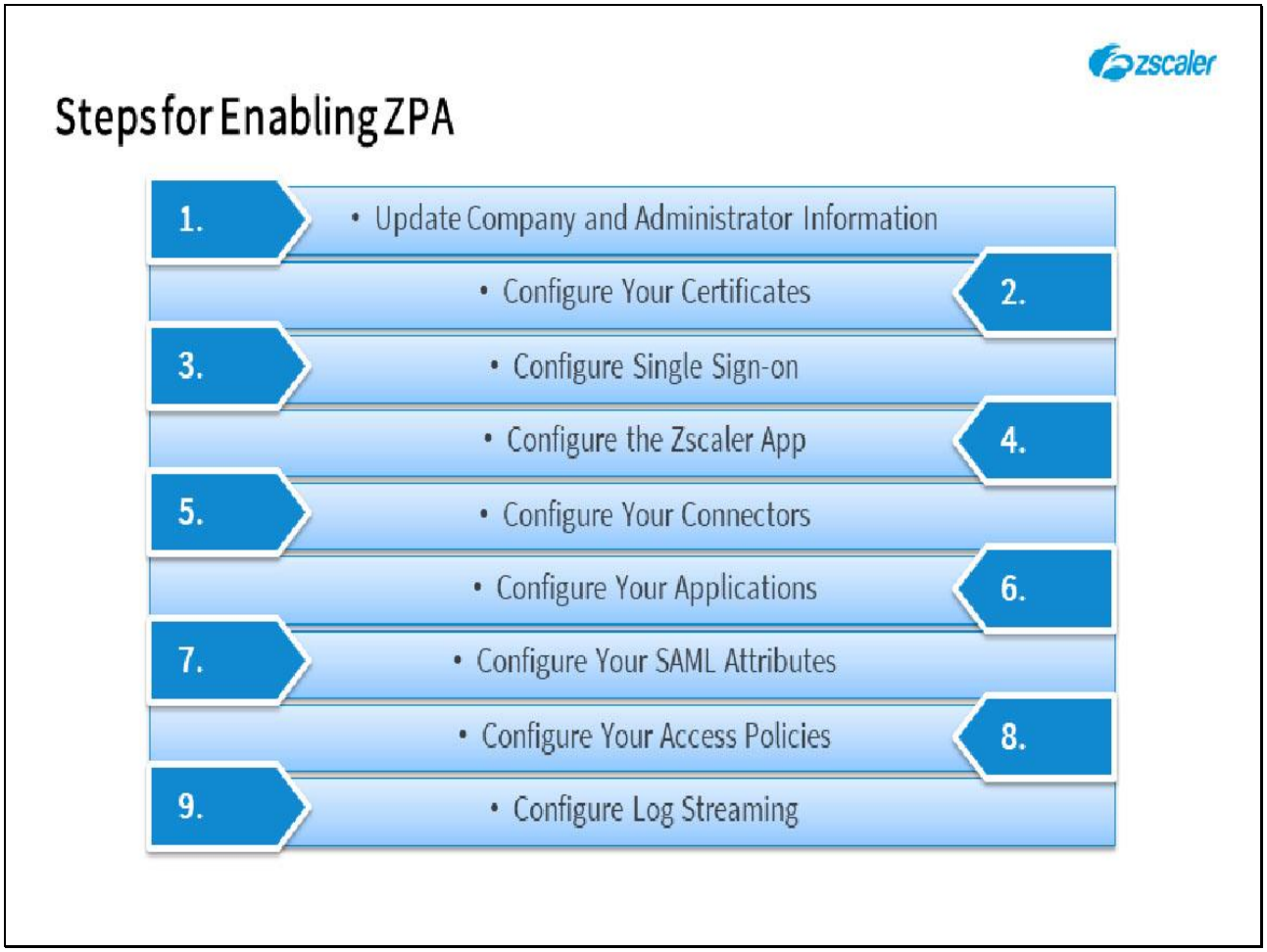
Slide 20 - Steps for Enabling ZPA



Slide notes

At **Step 8** you will create and configure your access policy rules, to control who is permitted to use the applications that you have enabled for ZPA access.

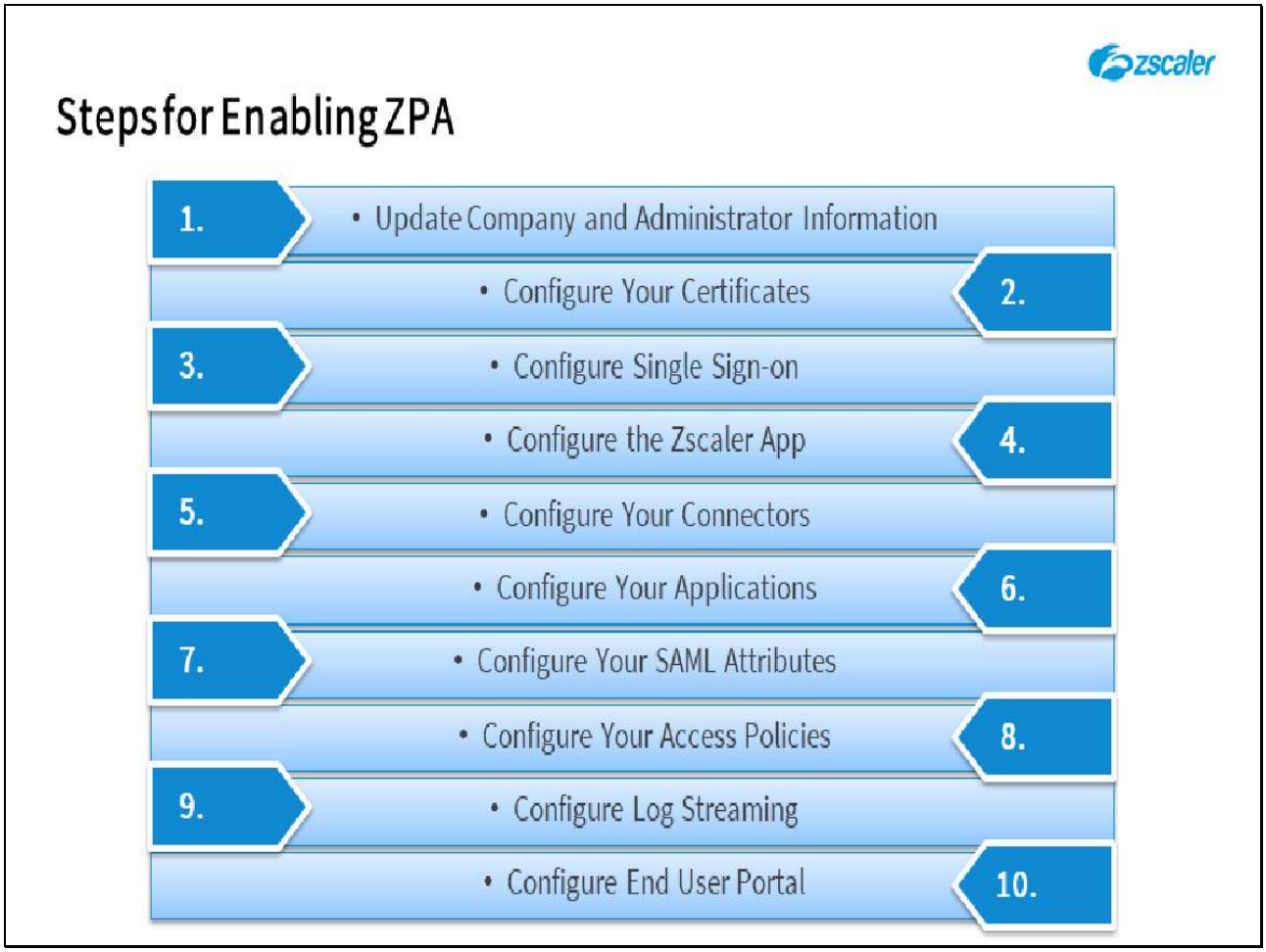
Slide 21 - Steps for Enabling ZPA



Slide notes

At **Step 9** you have the option to configure the **Log Streaming Service** (LSS) to send Connector status, user status, or user activity to your SIEM through a set of ZPA Connectors selected for this purpose.

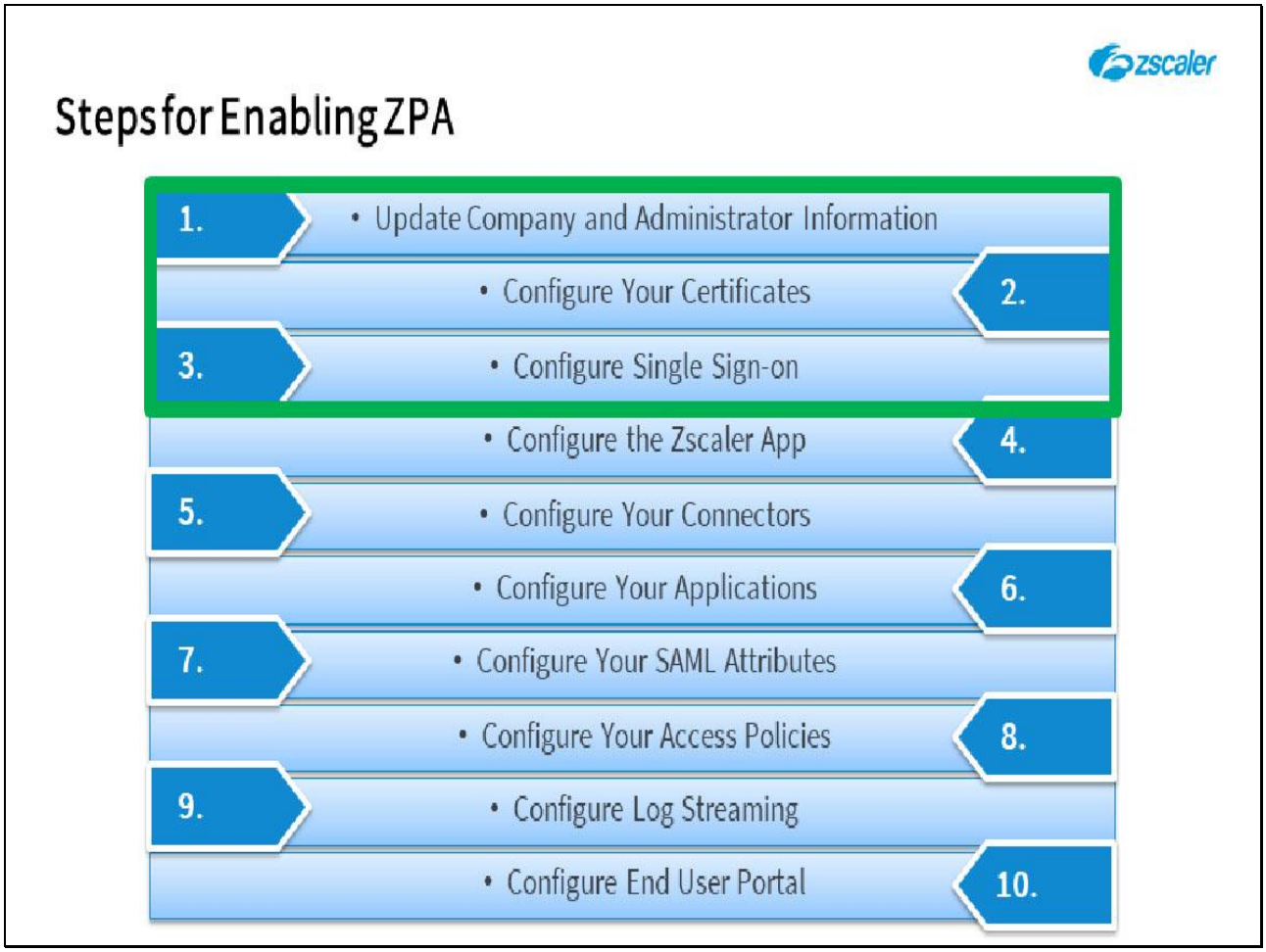
Slide 22 - Steps for Enabling ZPA



Slide notes

And finally, at **Step 10** you have the option to configure the **End User Portal**, which allows you to advertise the applications available from one or more customizable web portals.

Slide 23 - Steps for Enabling ZPA



Slide notes

In this module will focus on the preliminary steps of this process, specifically the first three steps indicated here.

Note, it would be a good idea to have access to the ZPA Admin Portal, prior to working through this training, so you can view the configuration options on a live system.

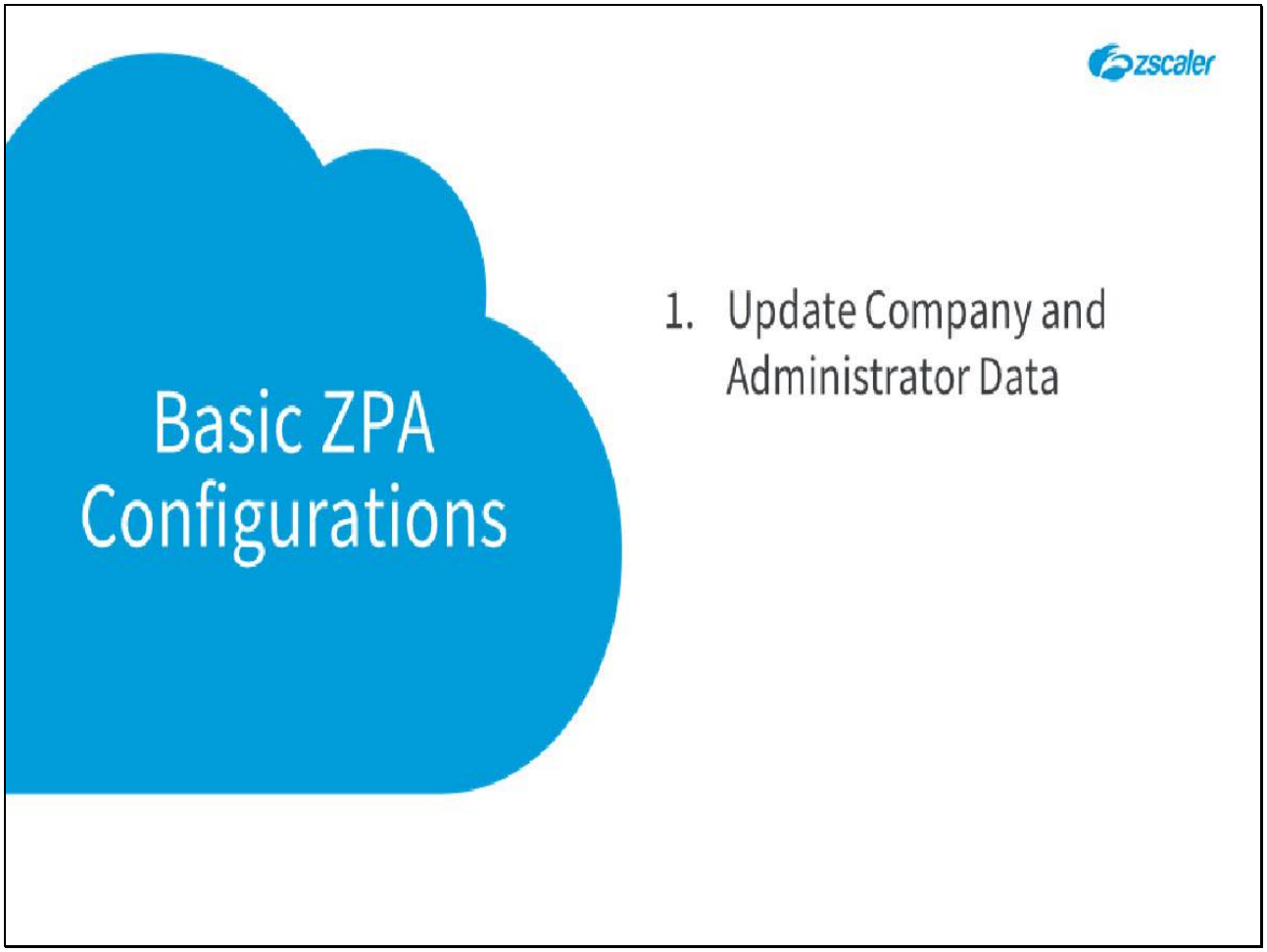
Slide 24 - 2. Update Company and Administrator Data

Slide notes

In the next section, we will look at some basic ZPA configurations.

This section has been created as an interactive demo to give you a feel for the navigation of the ZPA Admin Portal. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

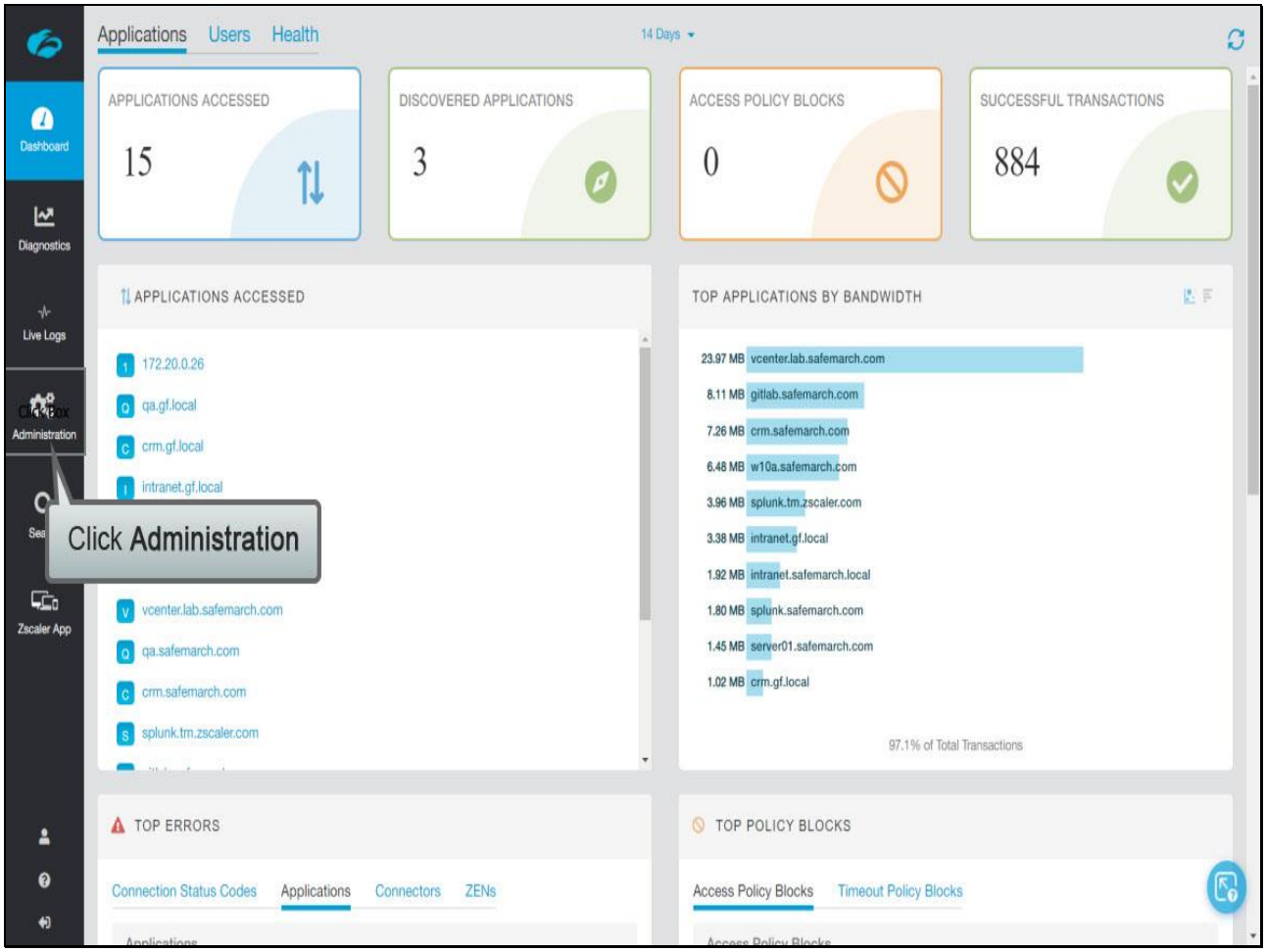
Slide 25 - Basic ZPA Configurations



Slide notes

In the first section we will look at updating **Company** and **Administrator** data in the ZPA Admin Portal.

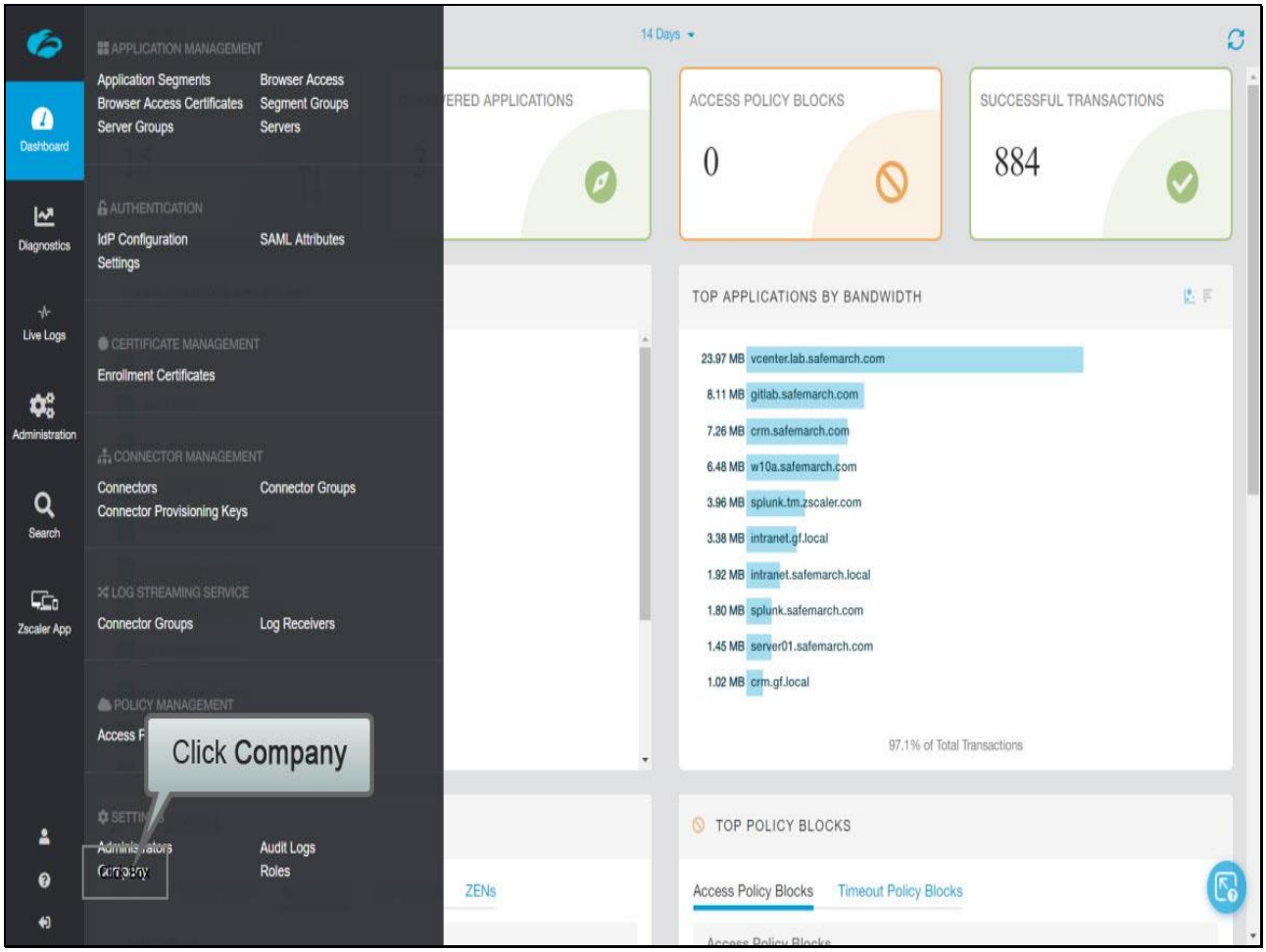
Slide 26 - Slide 26



Slide notes

To expand the configuration options, click **Administration**, ...

Slide 27 - Slide 27



Slide notes

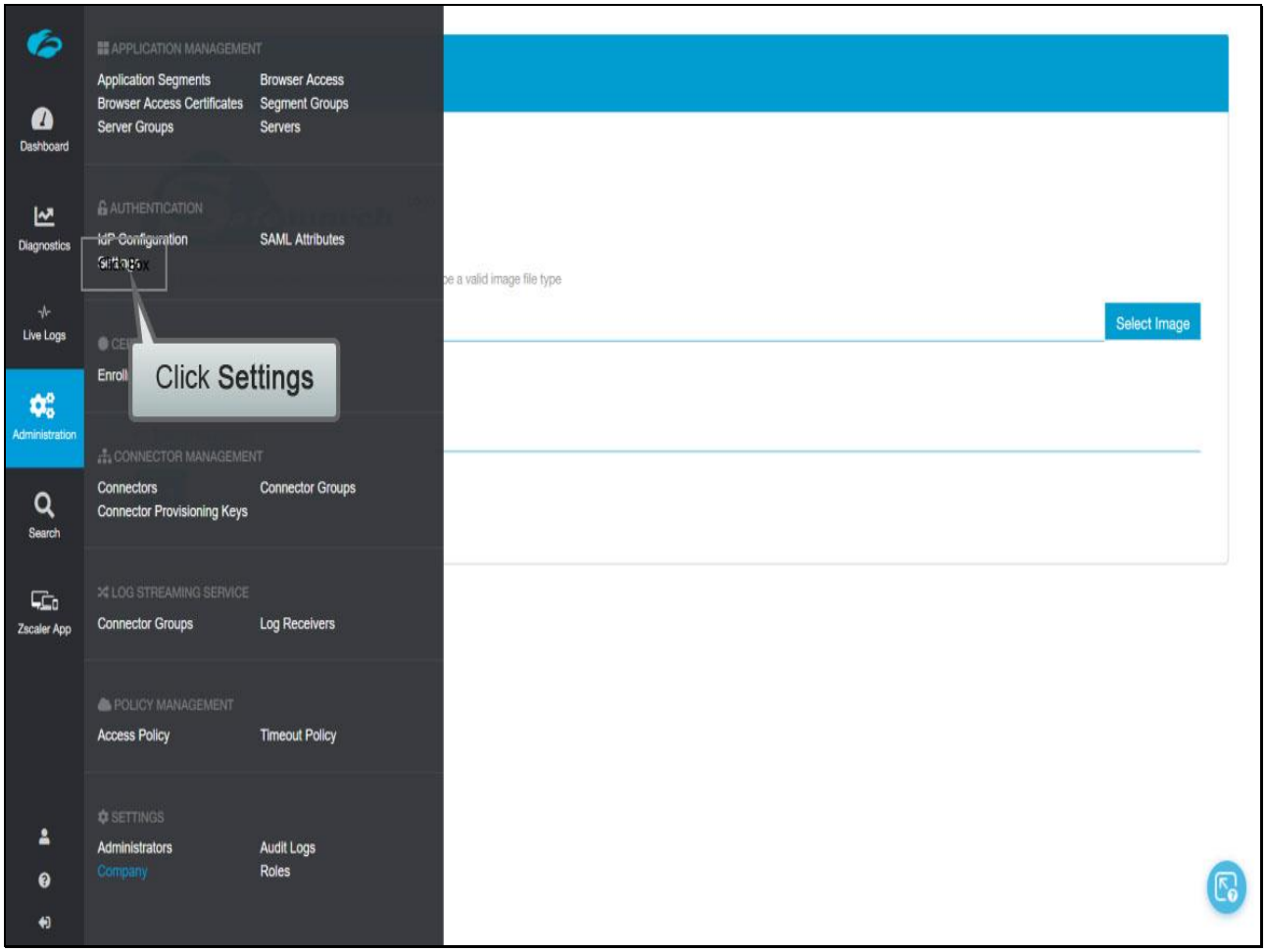
...then to review your company data, under the **SETTINGS** section, click **Company**.

Slide 28 - Slide 28

Slide notes

The **Company** data page allows you to provide the company **Name**, and optionally upload a **Logo**. To review other key settings, click **Administration**, ...

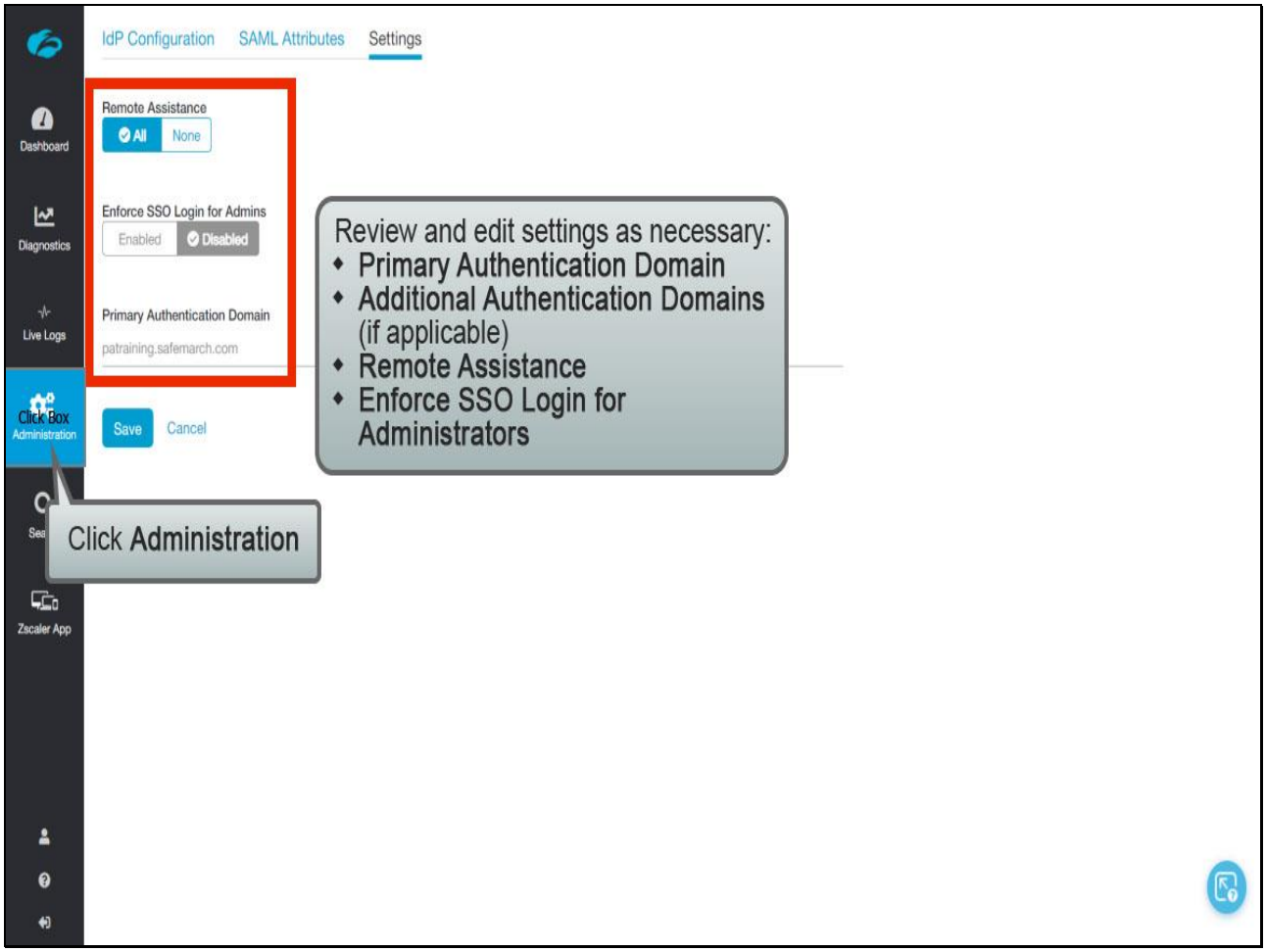
Slide 29 - Slide 29



Slide notes

...then under the **AUTHENTICATION** section, click **Settings**.

Slide 30 - Slide 30



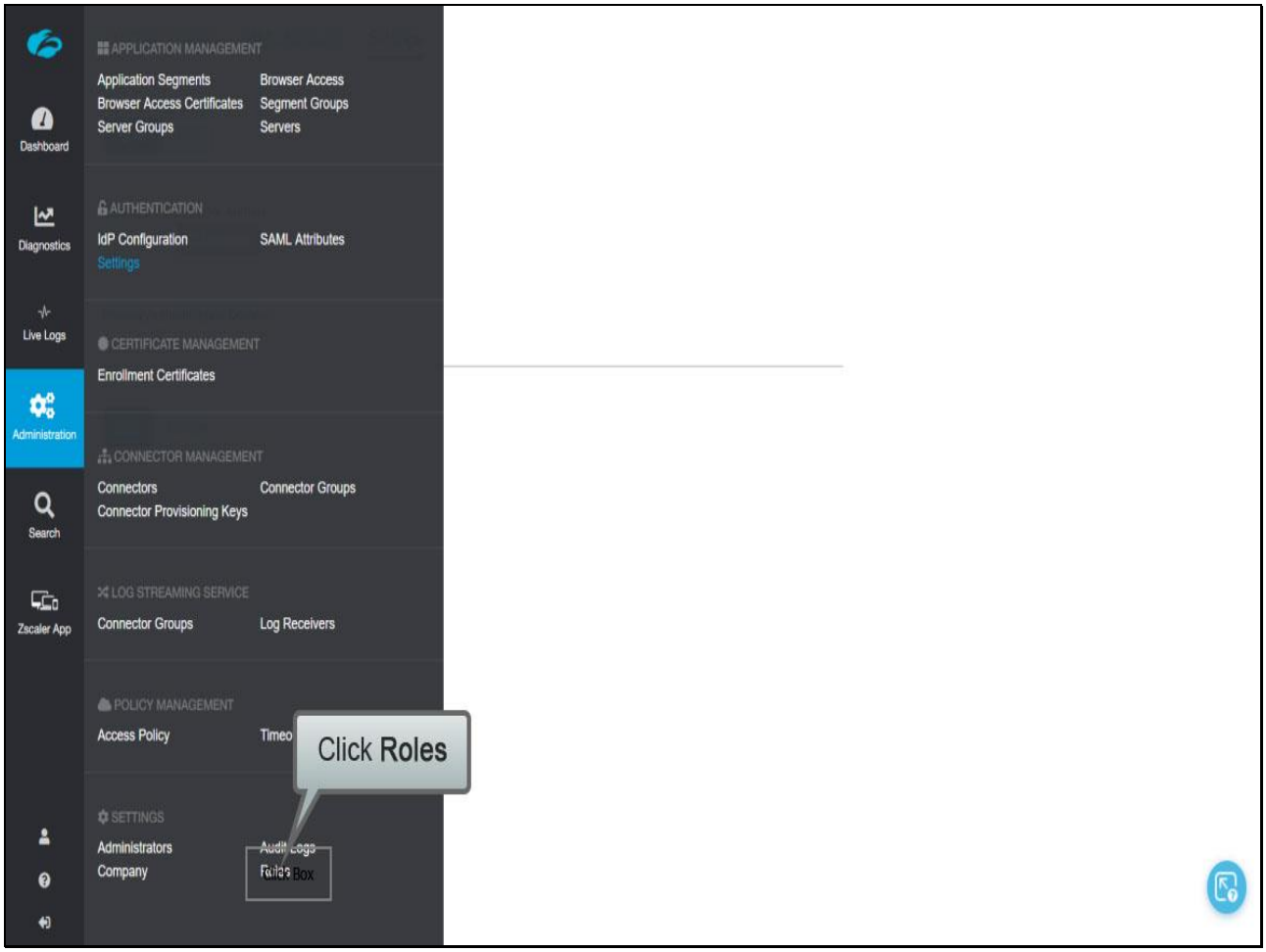
Slide notes

A key part of the company configuration are the authentication domains that can be reviewed here. The **Primary Authentication Domain** is the principal domain owned by your company; **Additional Authentication Domains** are domains owned by the company that are not configured as primary domains. Note that these domains can only be added by Zscaler support on request.

Other options that can be enabled here are: **Remote Assistance**, which allows Zscaler Support view-only access to your Admin Portal; and **Enforce SSO Login for Administrators**, which requires administrators to use SAML to authenticate into the Admin Portal. Note that for an administrator to authenticate using SAML, an IdP must be added at the **IdP Configuration** page for administrator SSO.

To manage administrator **Roles** defined on the service, click **Administration**, ...

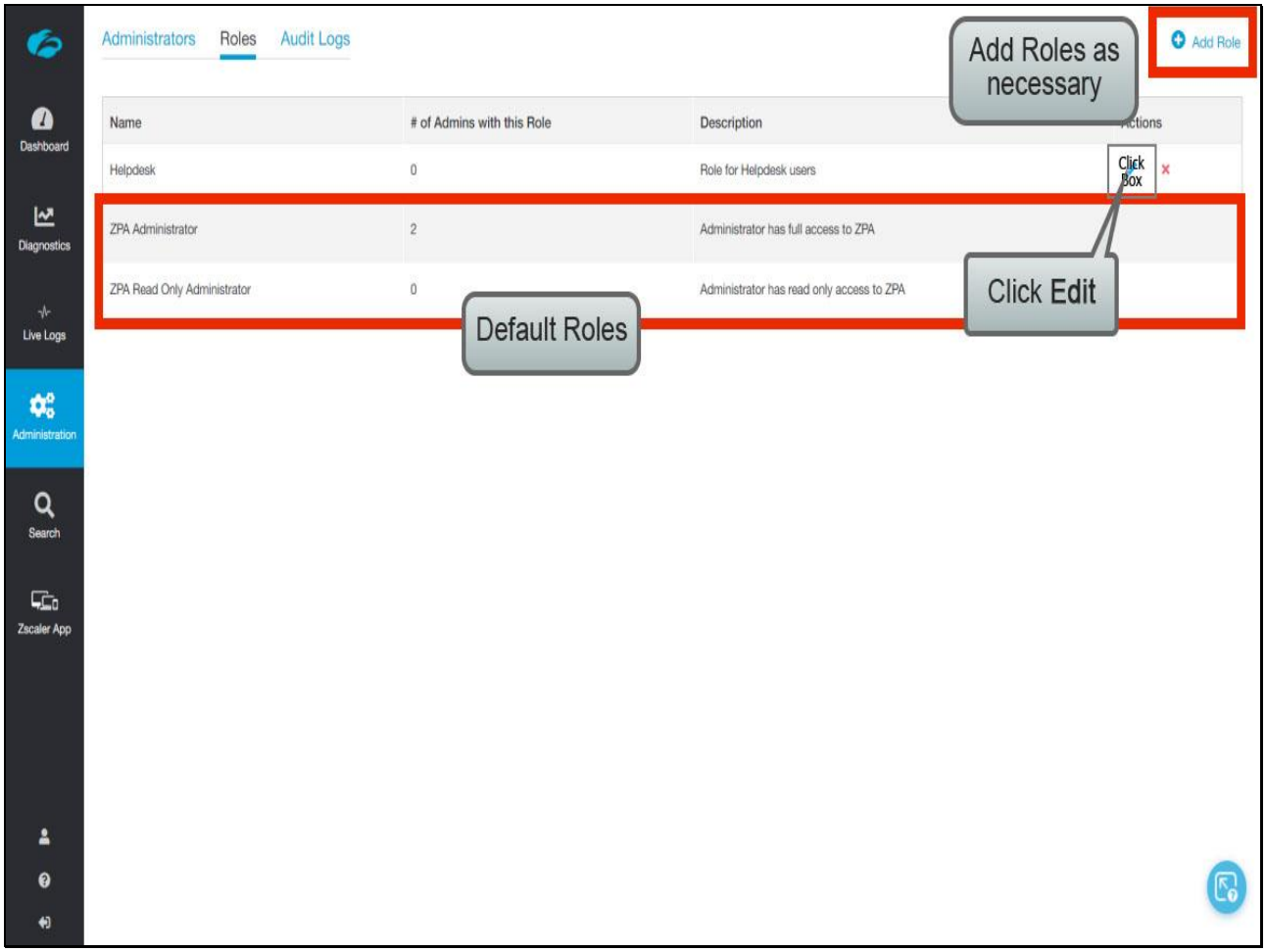
Slide 31 - Slide 31



Slide notes

...then under the **SETTINGS** section, click **Roles**.

Slide 32 - Slide 32

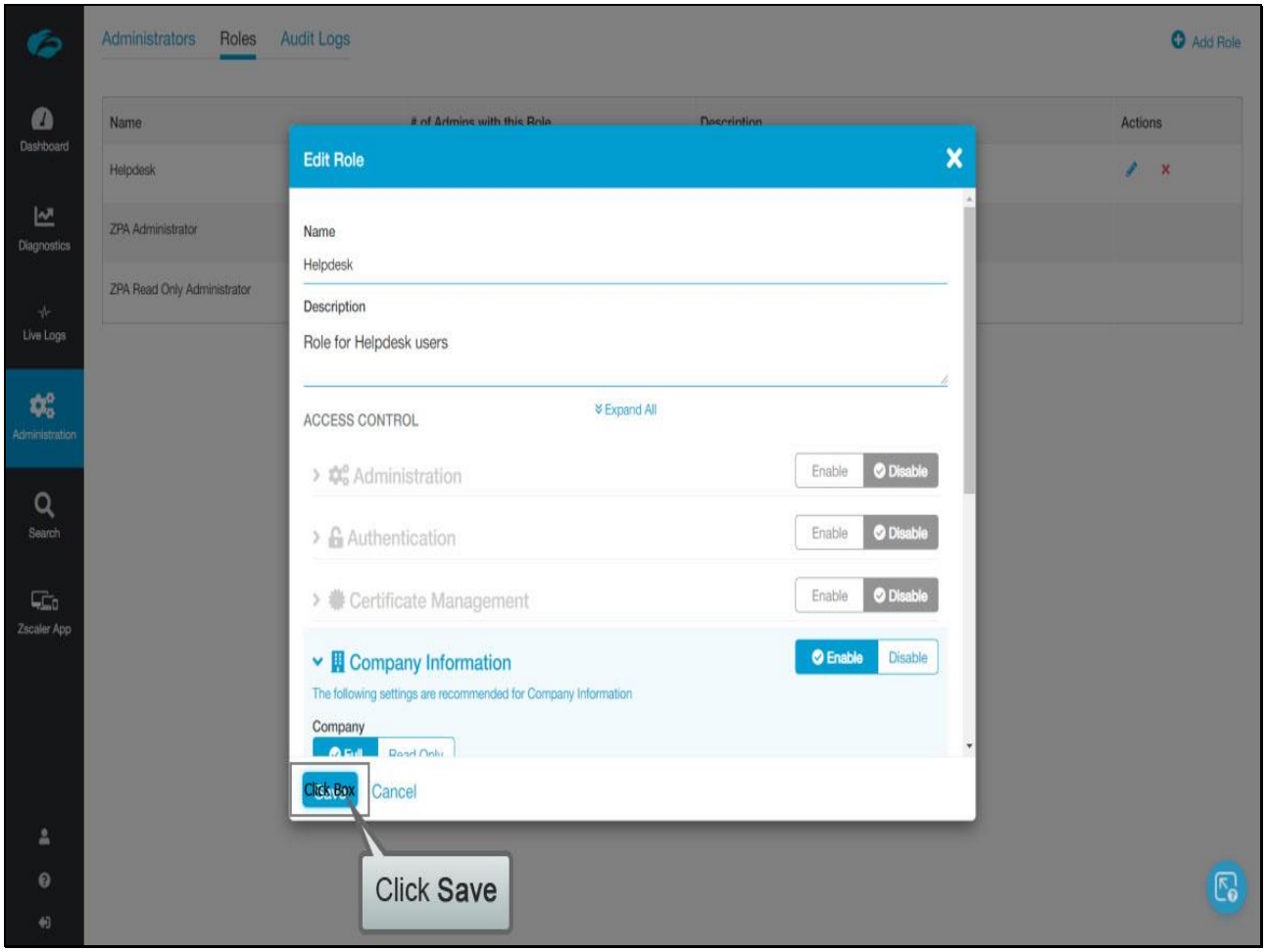


Slide notes

Here you can add and configure **Roles** for administrators as necessary. Two default **Roles** exist: **ZPA Administrator** with full control over the Admin Portal configurations; and **ZPA Read Only Administrator** with view-only access. Note that a **ZPA Read Only Administrator** admin can view the ZPA Admin Portal only, they have no access to the Zscaler App Portal.

The default roles cannot be deleted or edited, but any roles that you add can be changed or removed if necessary. To edit a **Role**, click the **Edit** icon, ...

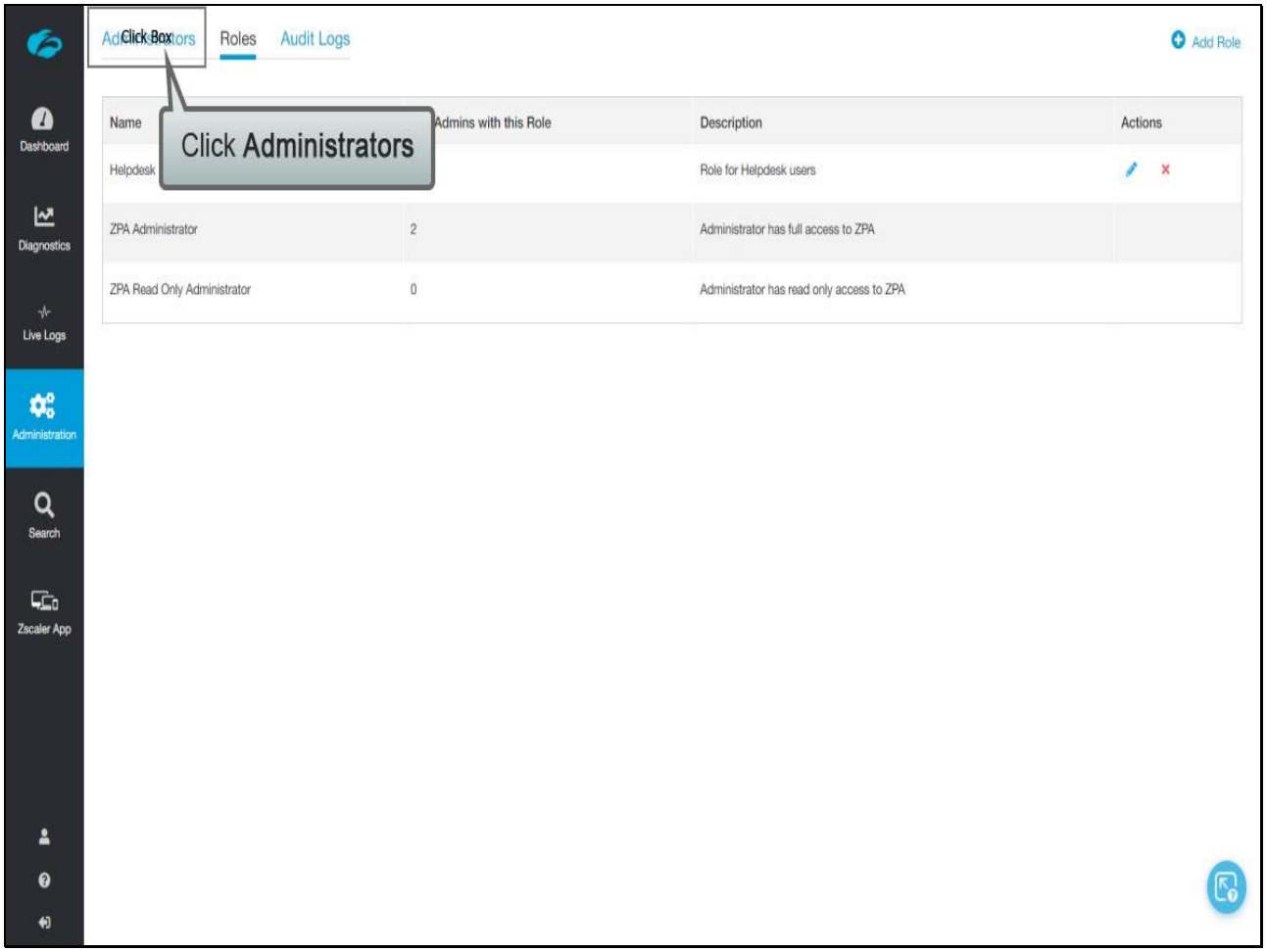
Slide 33 - Slide 33



Slide notes

...and adjust the configuration as necessary. Once you are done, click **Save**.

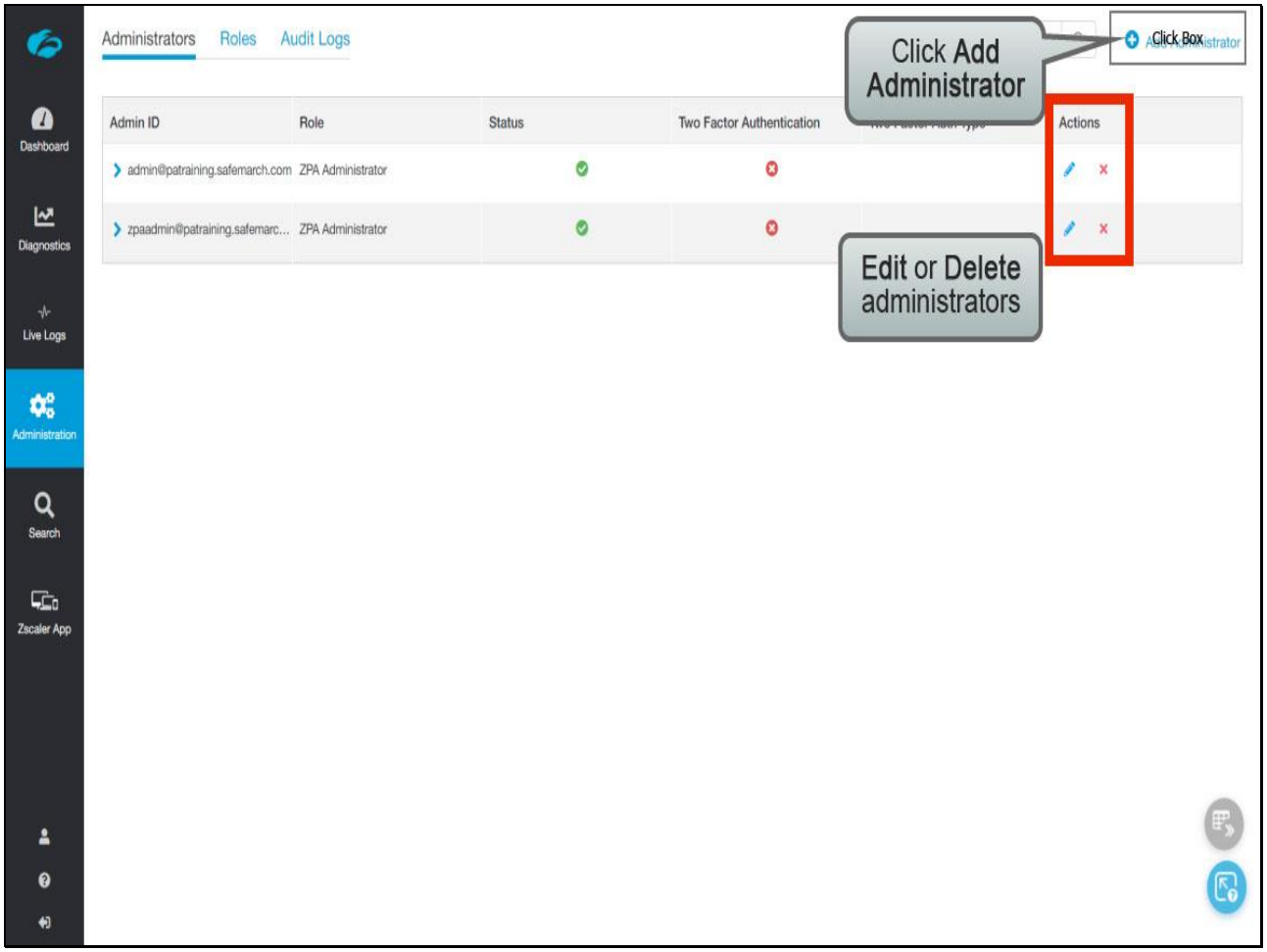
Slide 34 - Slide 34



Slide notes

To add, manage, and configure your admins, click **Administrators** in the ZPA **Administration** menu.

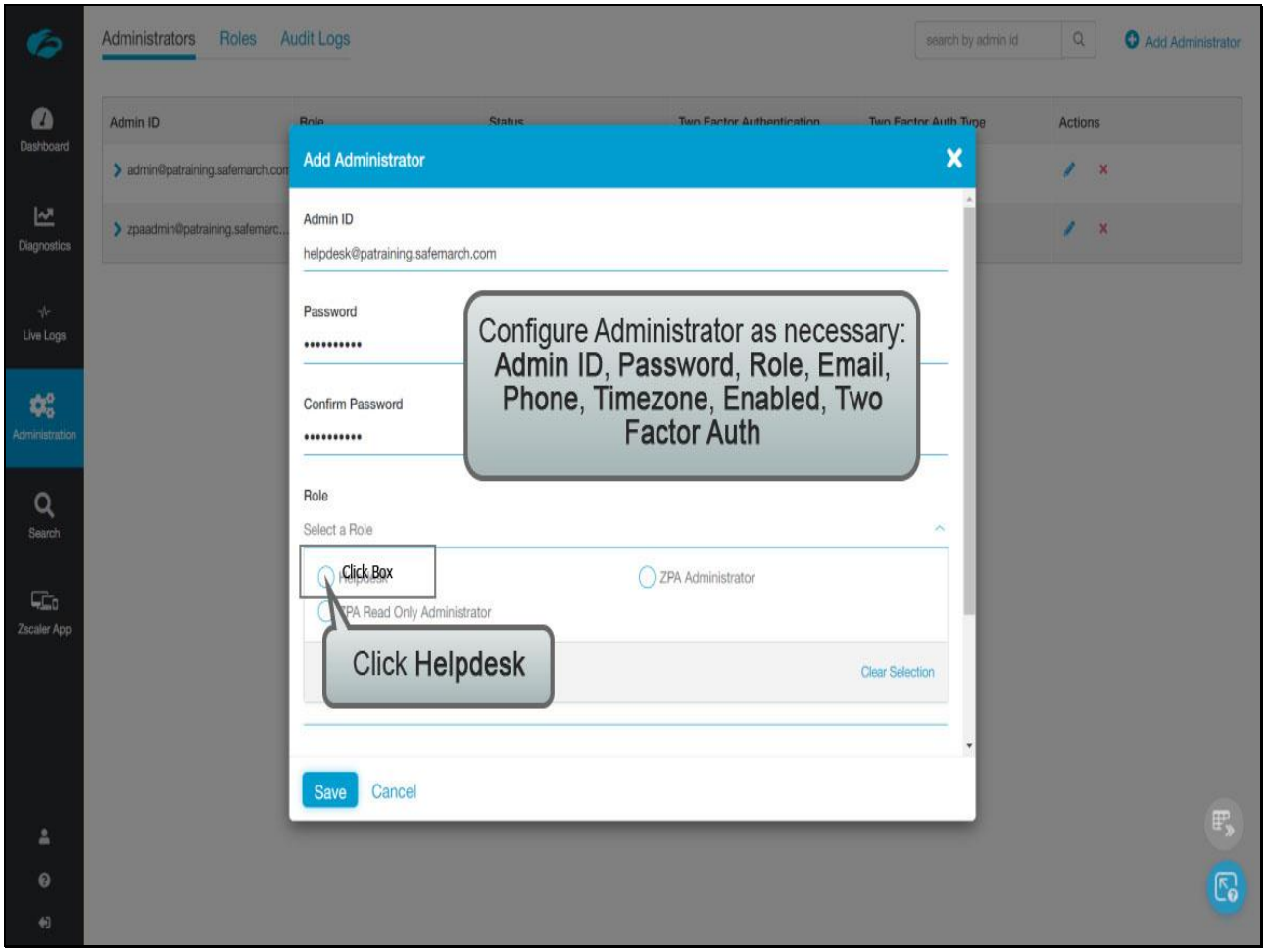
Slide 35 - Slide 35



Slide notes

You can edit, or delete existing administrators, or to add a new one, click the **Add Administrator** link, …

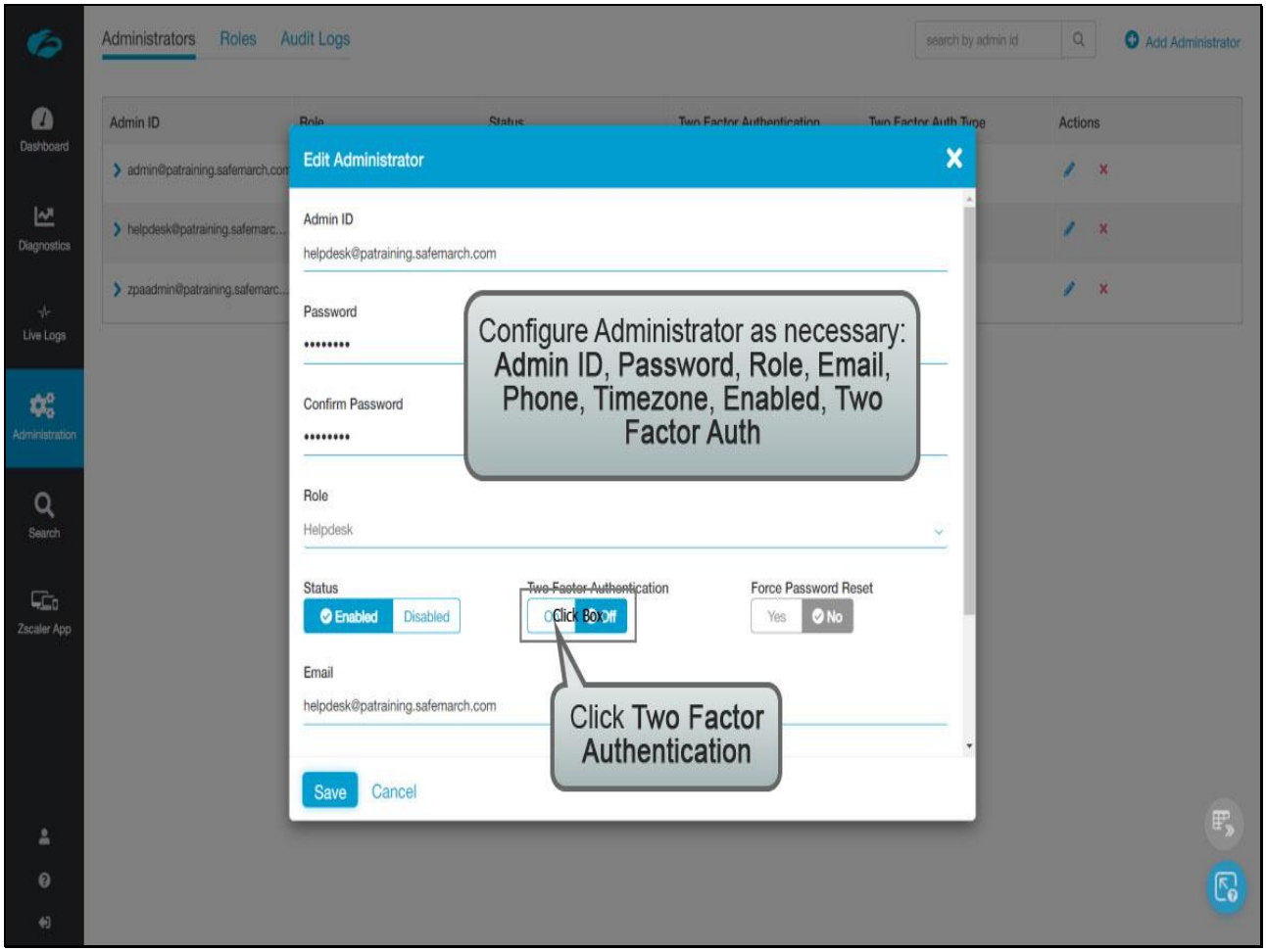
Slide 36 - Slide 36



Slide notes

…and configure the administrator as necessary. Administrators may have editing privileges in the Admin Portal, or monitor only privileges, depending on the **Role** that you assign to them. In this case we are creating a Helpdesk admin account, so click the **Helpdesk Role** that you just edited.

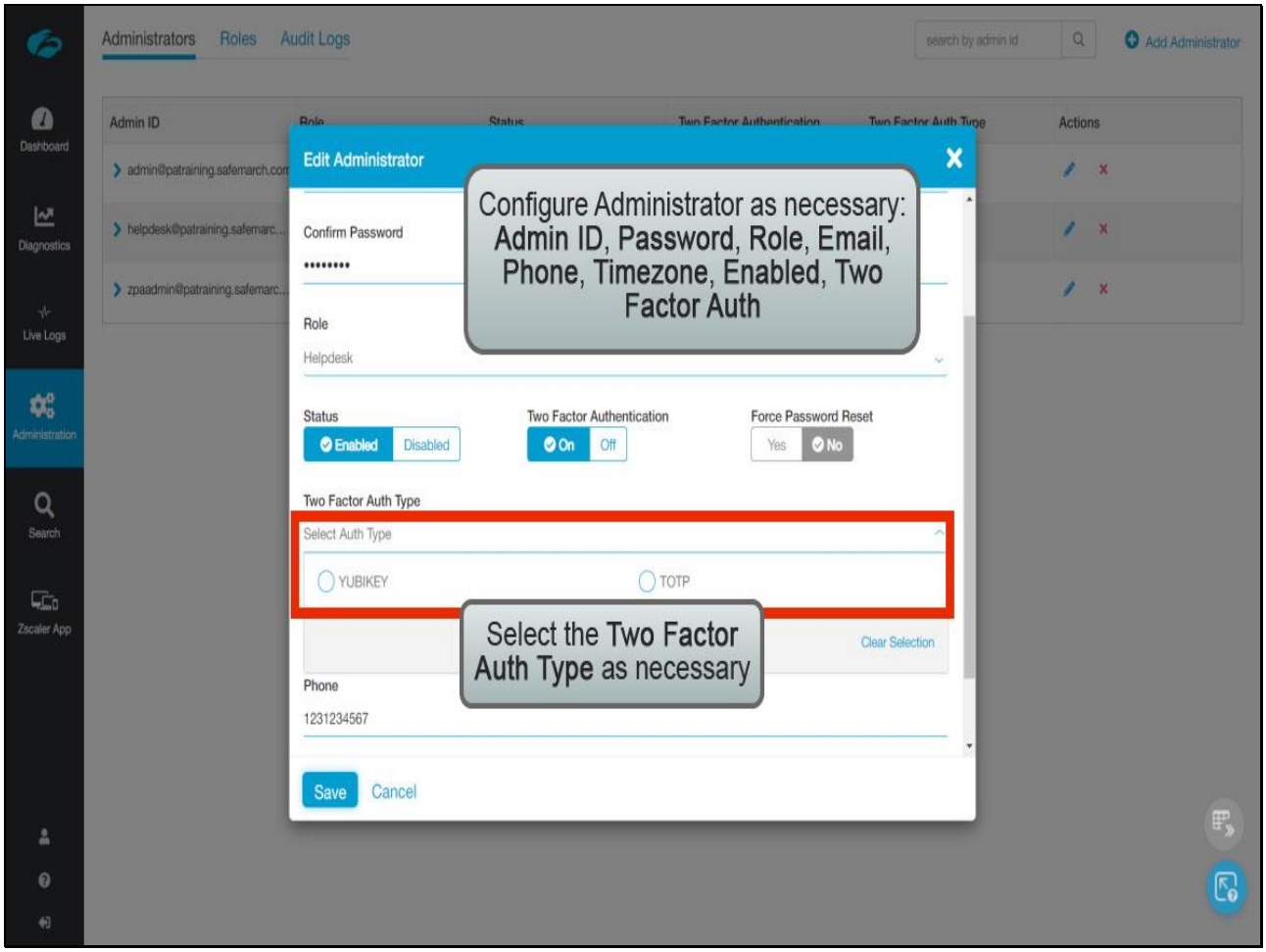
Slide 37 - Slide 37



Slide notes

You have the option to require two-factor authentication for your administrators, click to enable it here.

Slide 38 - Slide 38

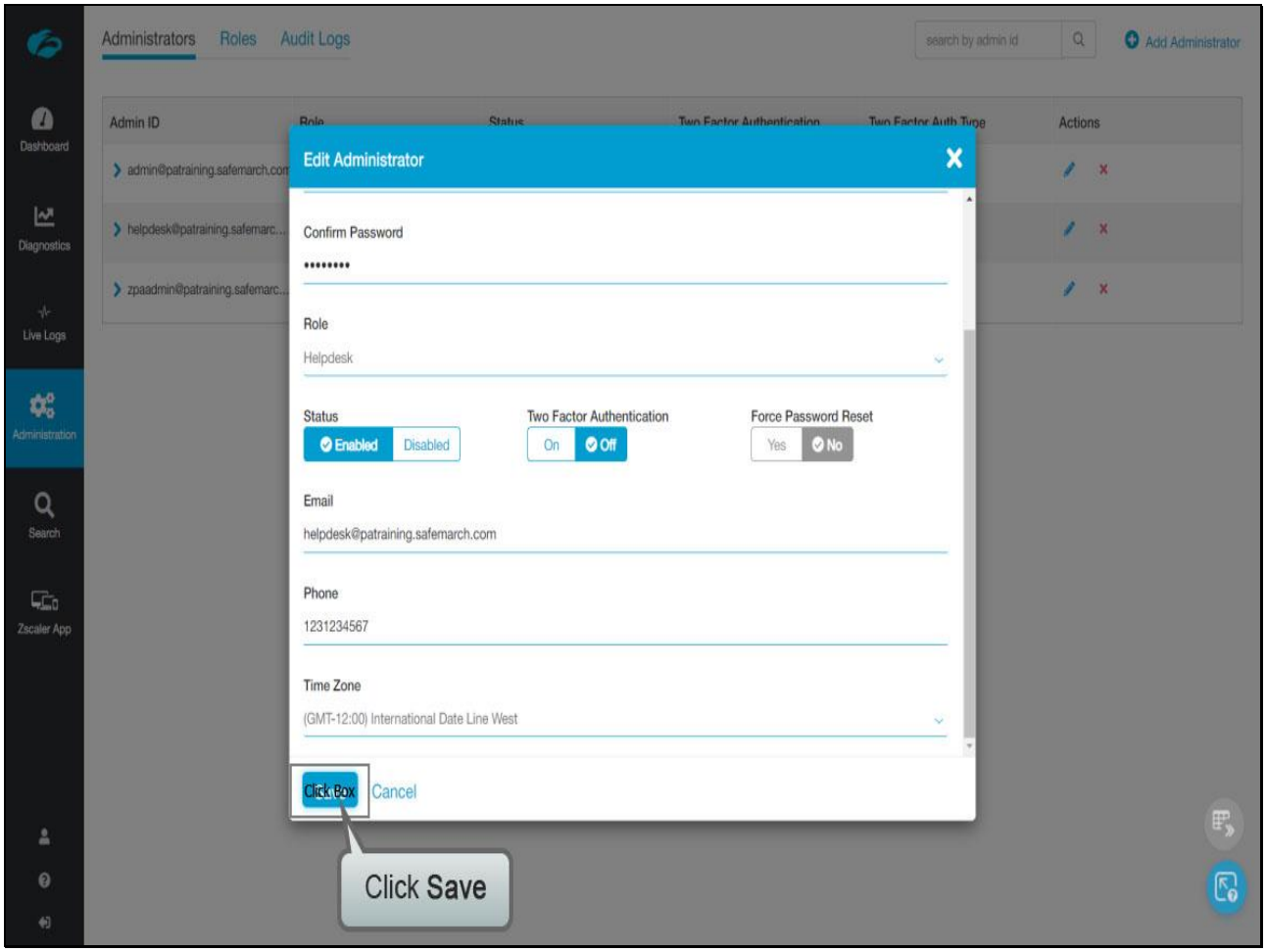


Slide notes

If you want to enable the **Two Factor Authentication** option for this administrator, you will need to select the appropriate provider, either **YUBIKEY**, or **TOTP**.

Note this option should not be enabled when first creating a new administrator. Create their account, ensure that they can login, then enable and configure this option.

Slide 39 - Slide 39

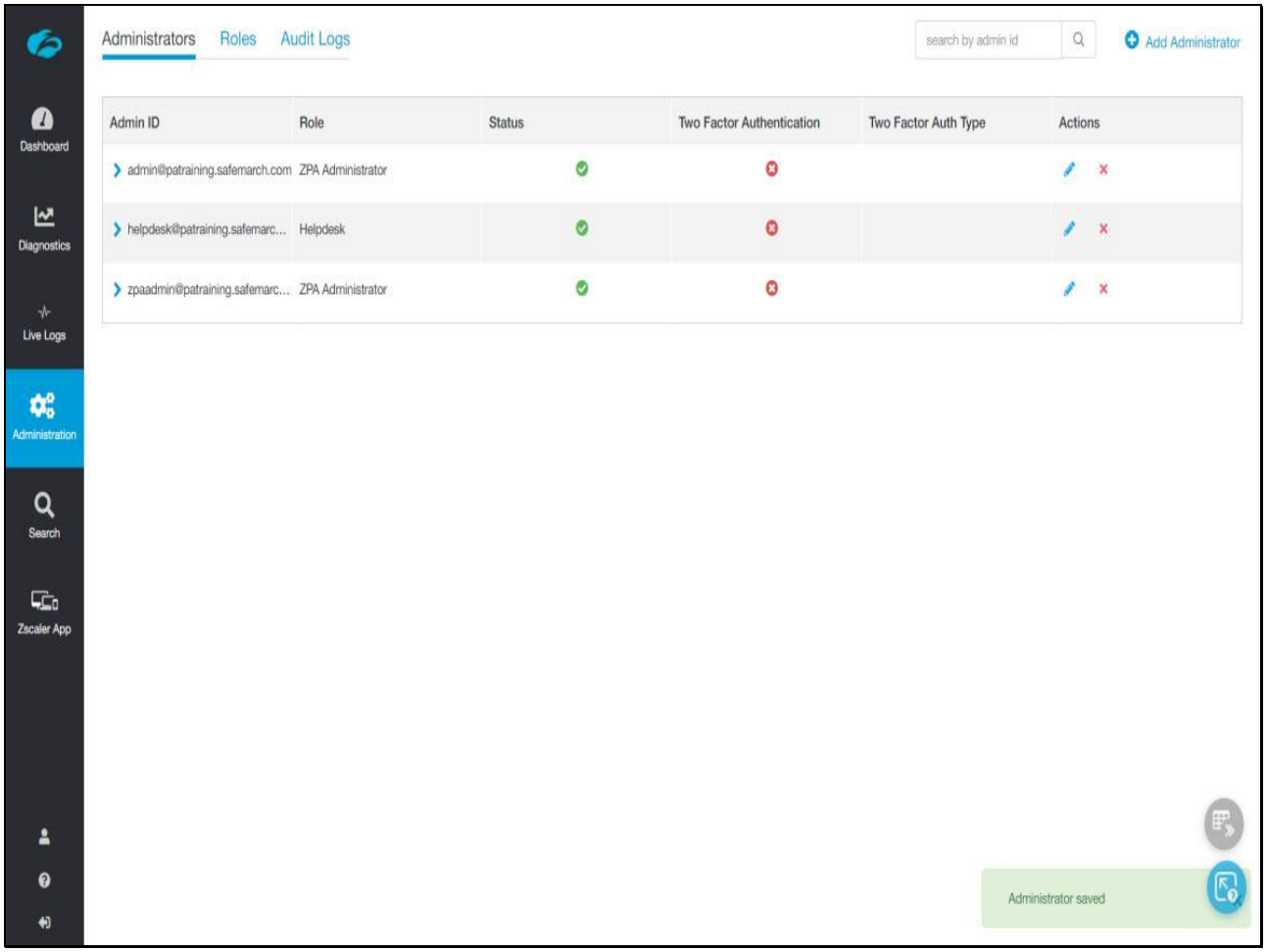


Slide notes

Complete the configuration and click **Save**.

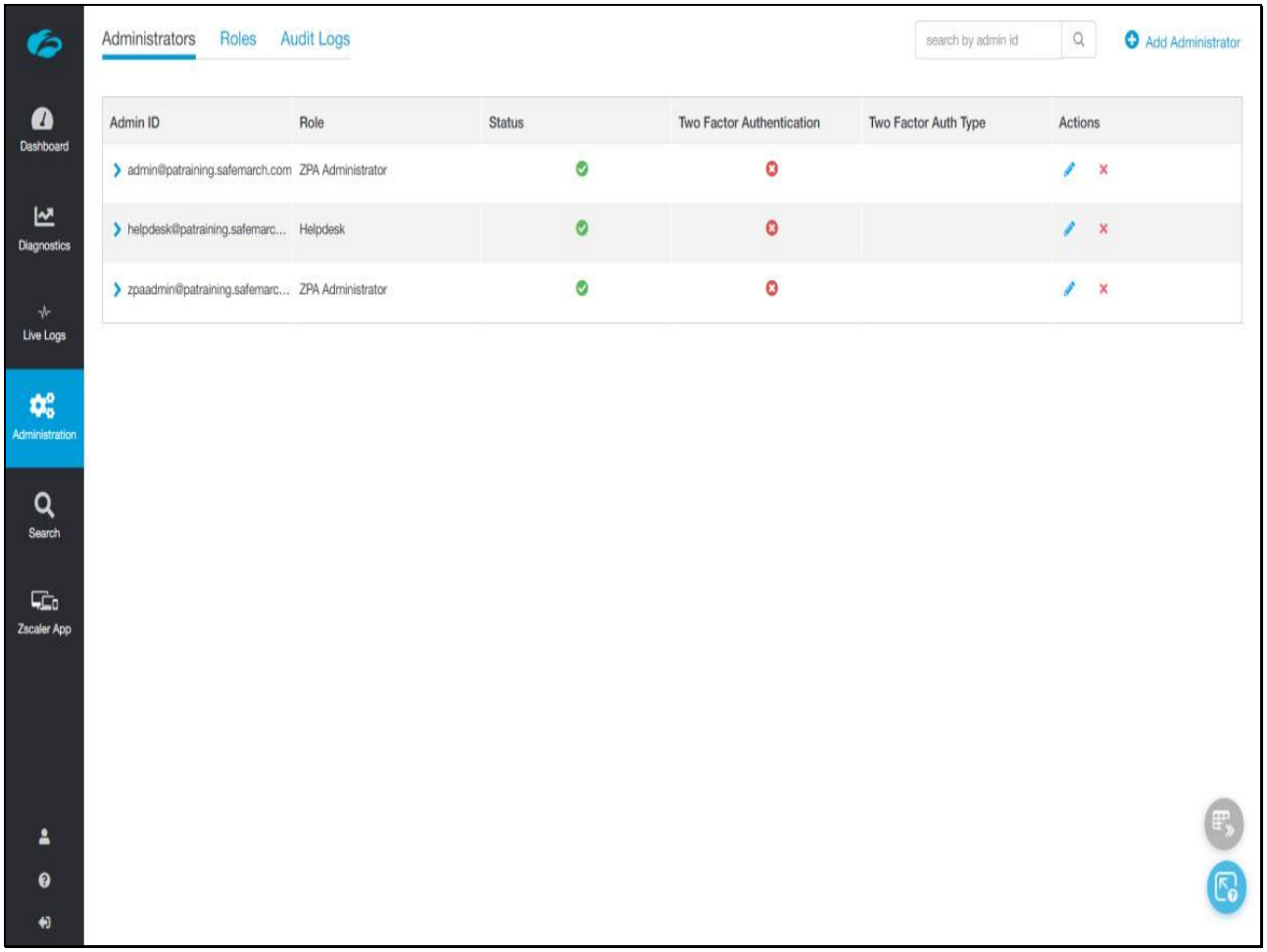
Note that when a new admin logs in for the first time, the ZPA Admin Portal displays an **End User License Agreement** (EULA). The admin must accept the EULA to proceed.

Slide 40 - Slide 40



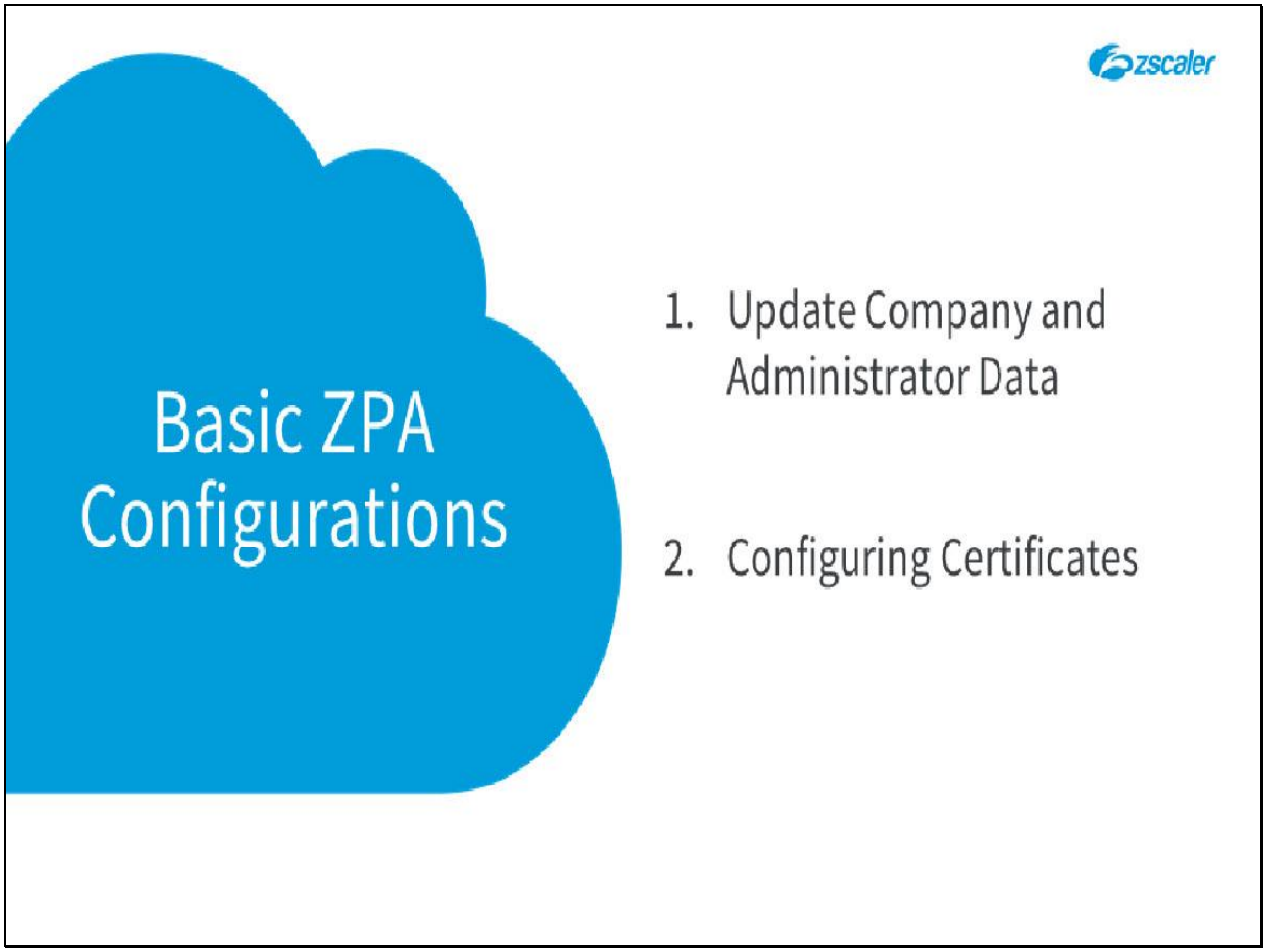
Slide notes

Slide 41 - Slide 41



Slide notes

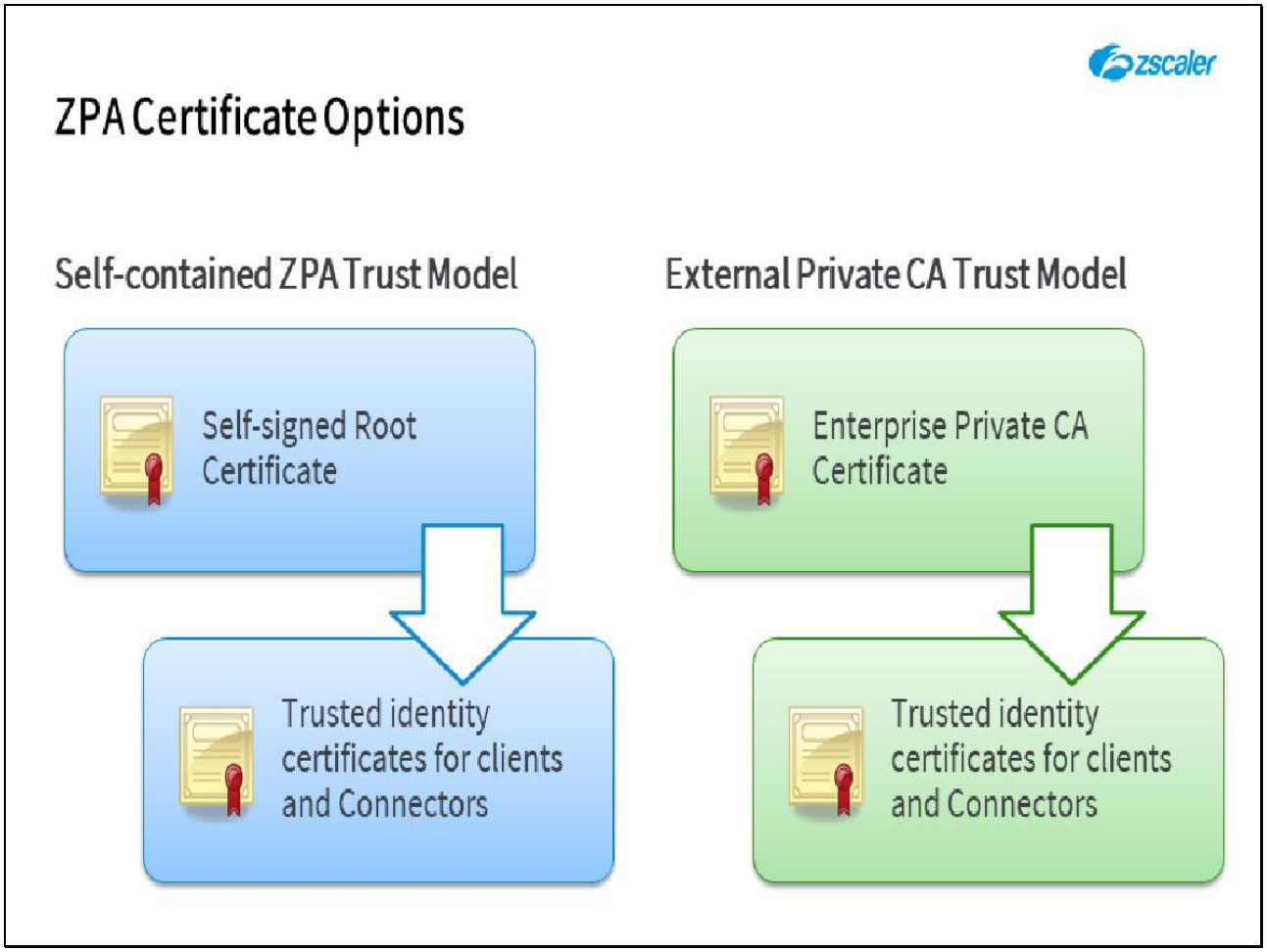
Slide 42 - Basic ZPA Configurations



Slide notes

In the next section, we will look at creating or uploading the required certificates for securing ZPA connections.

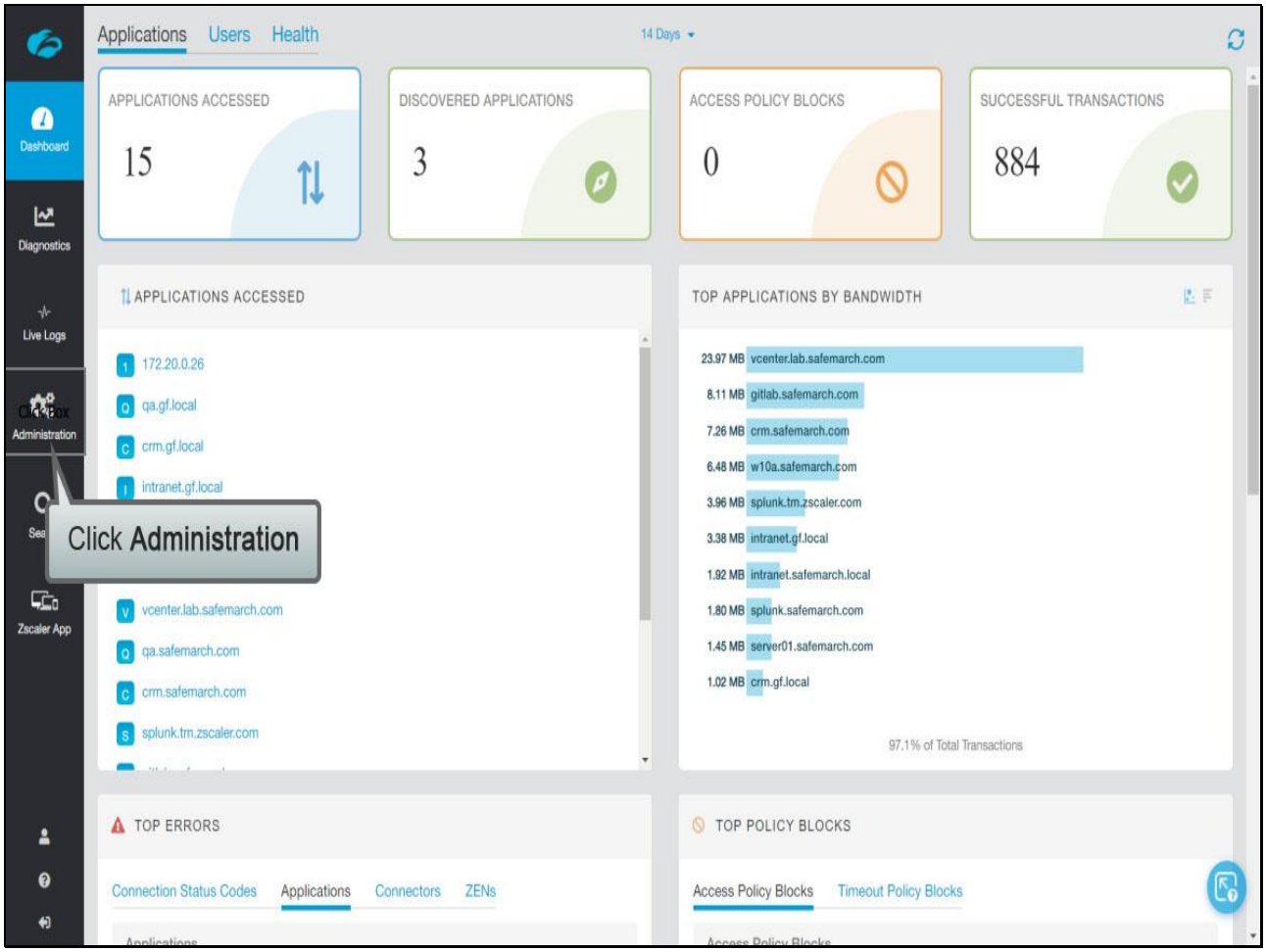
Slide 43 - ZPA Certificate Options



Slide notes

As a reminder, there are two options for provisioning certificates to the ZPA infrastructure; the self-contained trust model using self-signed certificates, or the fully trusted model using a subordinate certificate from a trusted external private CA. Note that public CAs are not suitable for this use case, as certificates purchased do not support the signing of subordinate certificates.

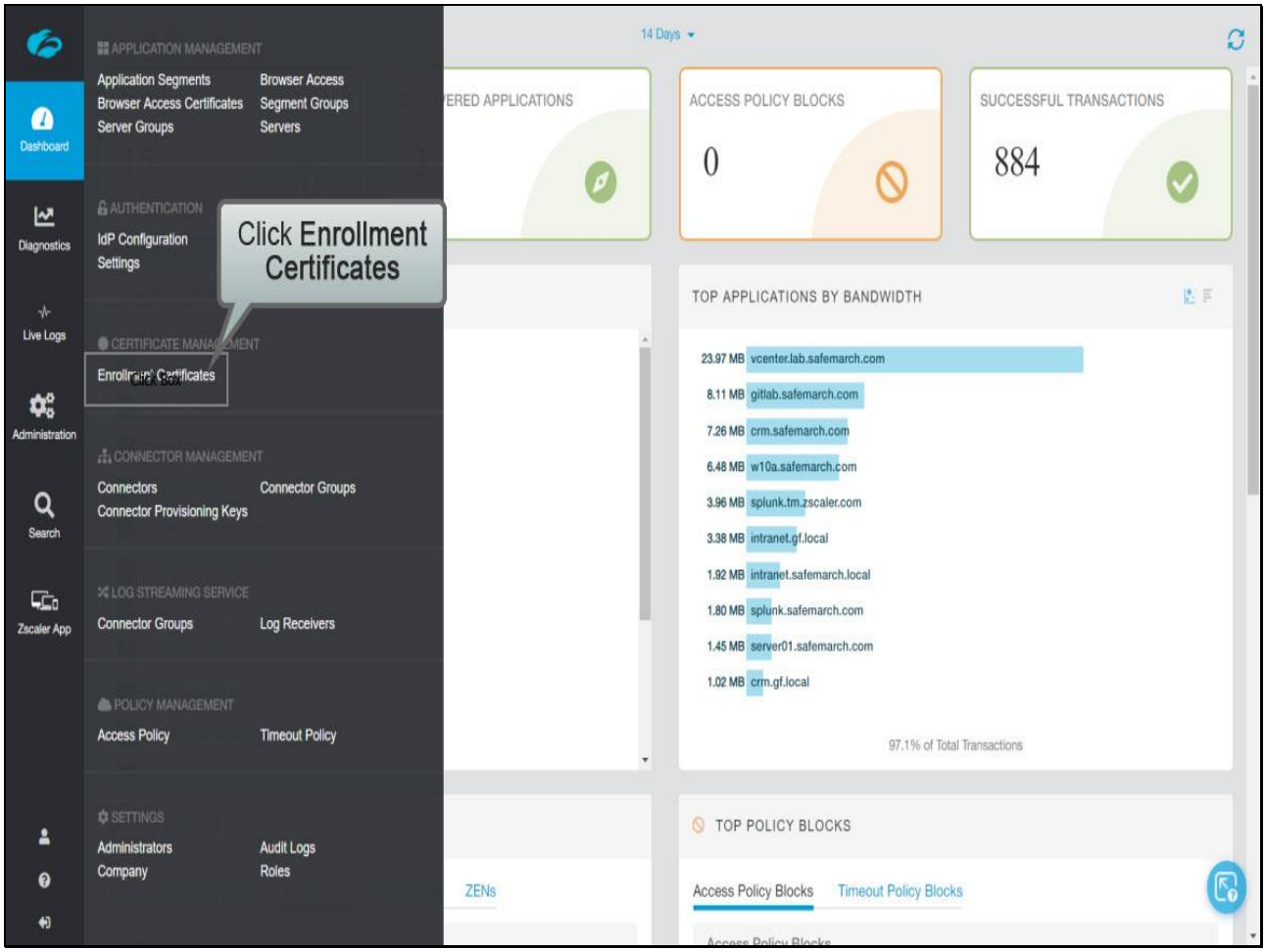
Slide 44 - Slide 44



Slide notes

To expand the configuration options, click **Administration**, ...

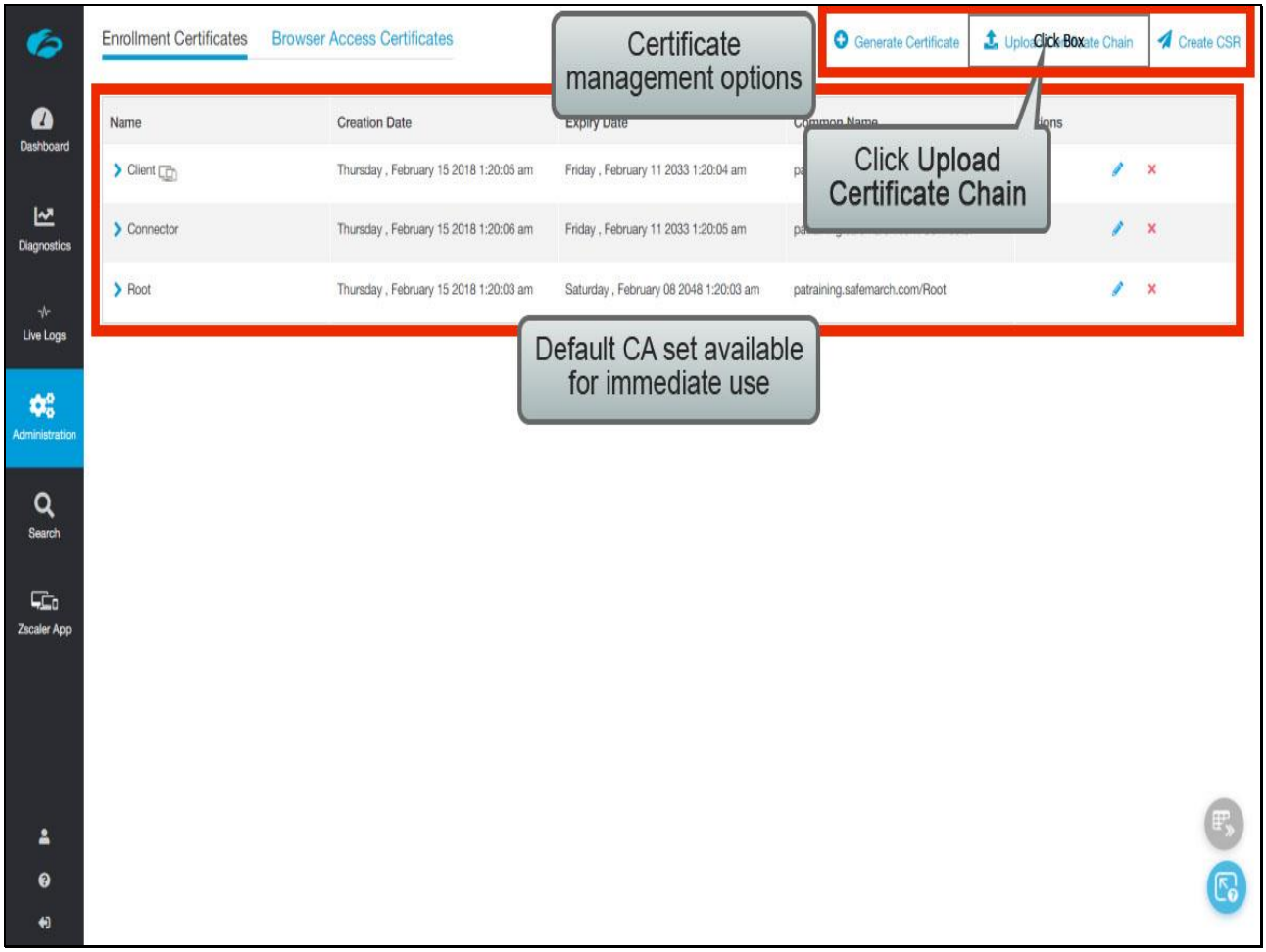
Slide 45 - Slide 45



Slide notes

...to manage the certificate environment for device enrollment, under the **CERTIFICATE MANAGEMENT** section, click **Enrollment Certificates**.

Slide 46 - Slide 46

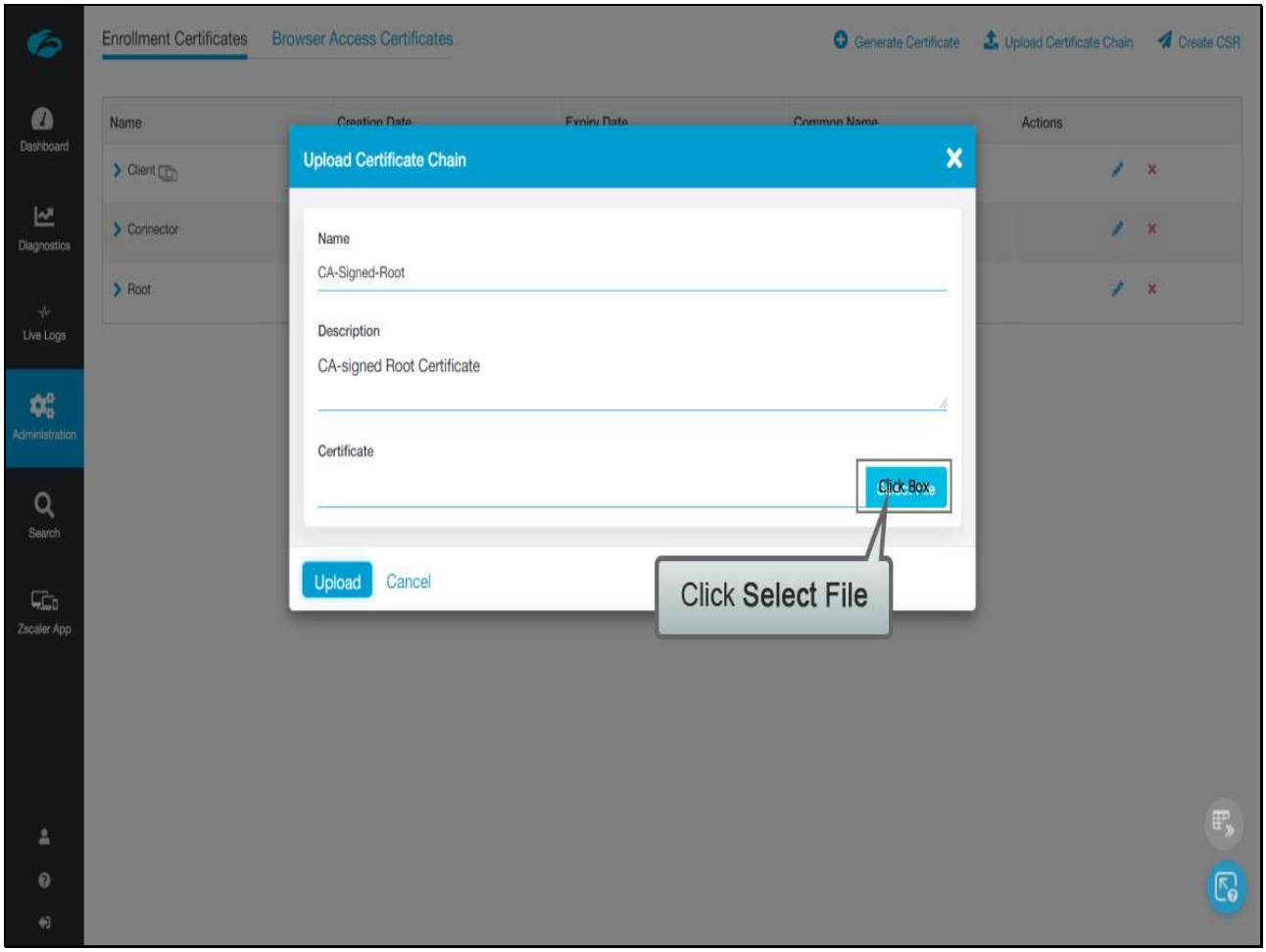


Slide notes

The ZPA service uses identity certificates to authenticate Connectors and the Zscaler App on the user's devices prior to establishing each connection. The identity certificates are generated on device enrollment by an intermediate CA created for that purpose. By default, we provide a set of CAs on your account that can be used immediately to enroll Connectors and Zscaler App devices. The set consists of a **Root** CA and two intermediate CAs generated from it, one for **Connectors** and one for **Client** devices.

You have the option to generate a complete new set of certificates, or to move to the Bring Your Own Encryption (BYOE) model by uploading certificates signed by your own internal PKI. For example, to upload a Root CA certificate or certificate chain, click **Upload Certificate Chain**, ...

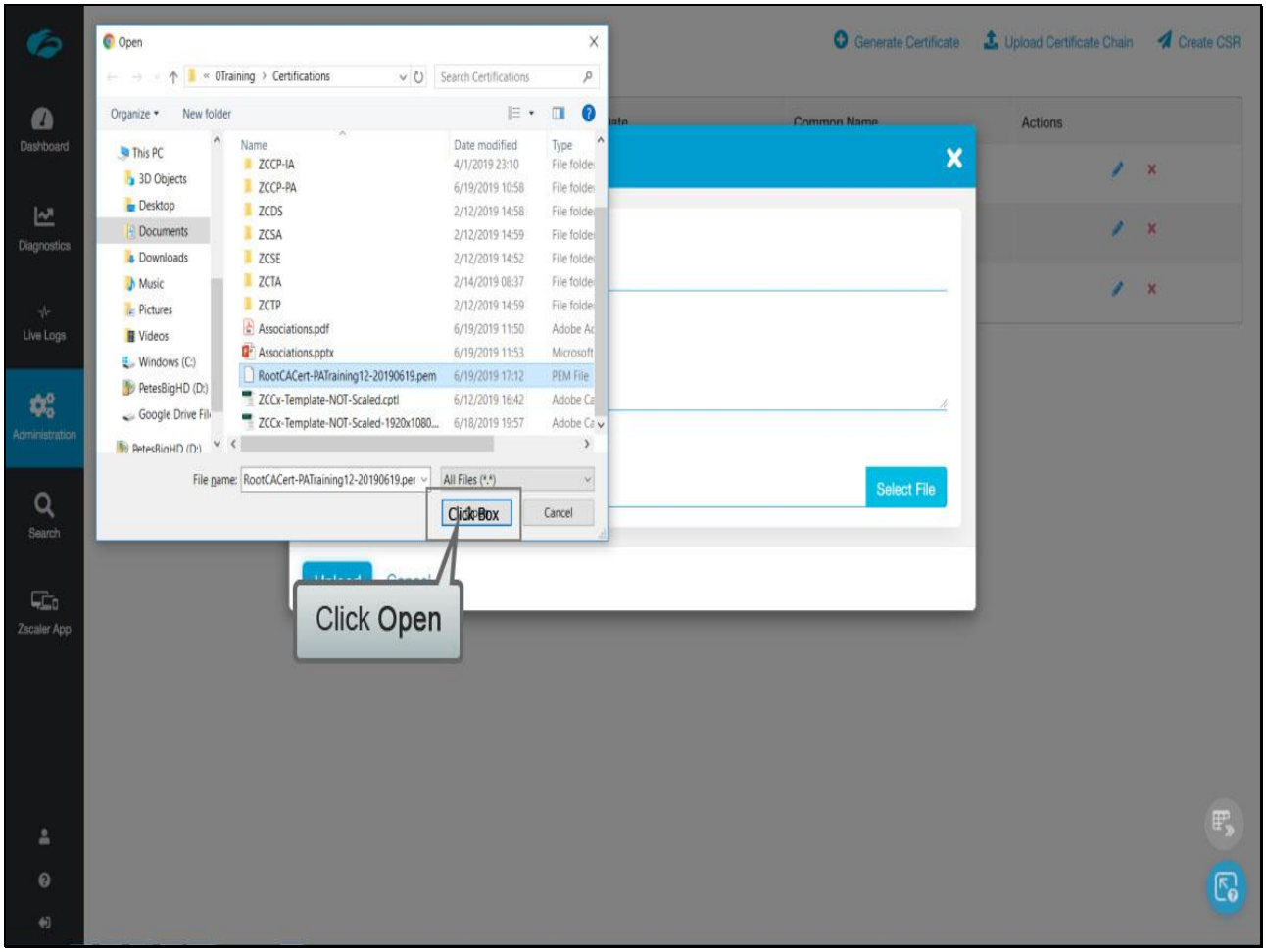
Slide 47 - Slide 47



Slide notes

...**Name** the certificate, add a **Description** if necessary and click **Select File**, ...

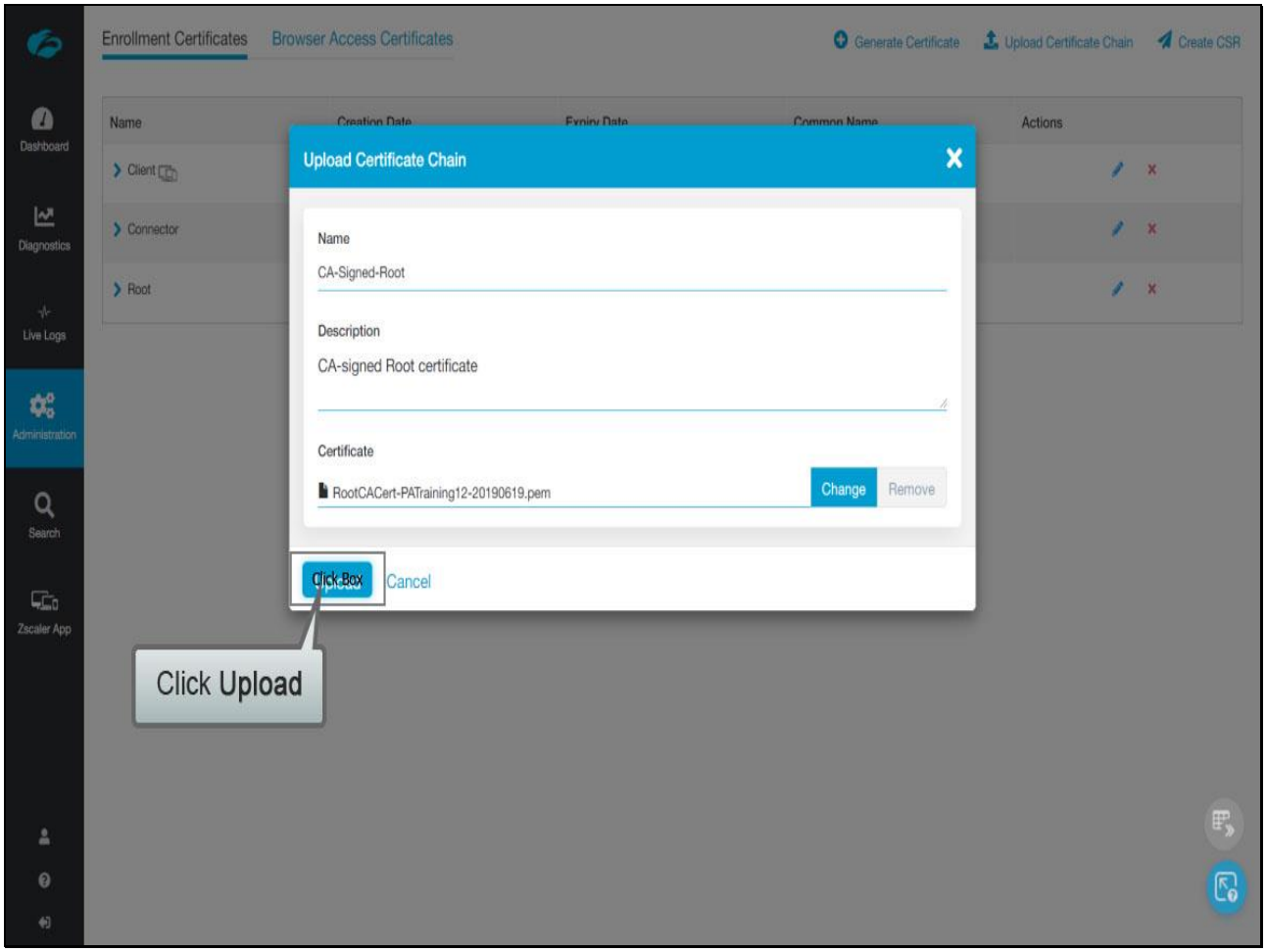
Slide 48 - Slide 48



Slide notes

...find the correct certificate file (.pem format) and click **Open**, ...

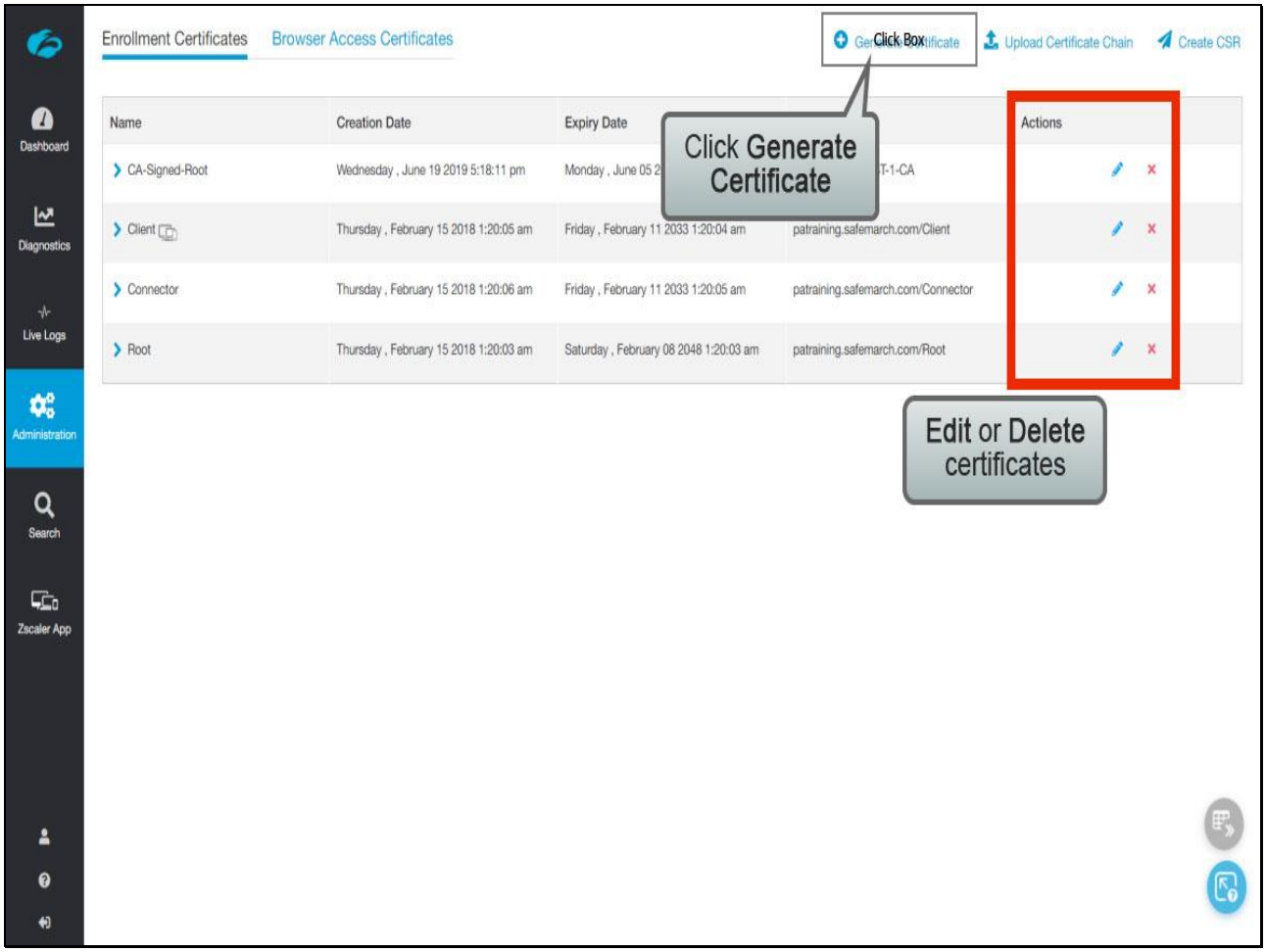
Slide 49 - Slide 49



Slide notes

...then click **Upload**.

Slide 50 - Slide 50

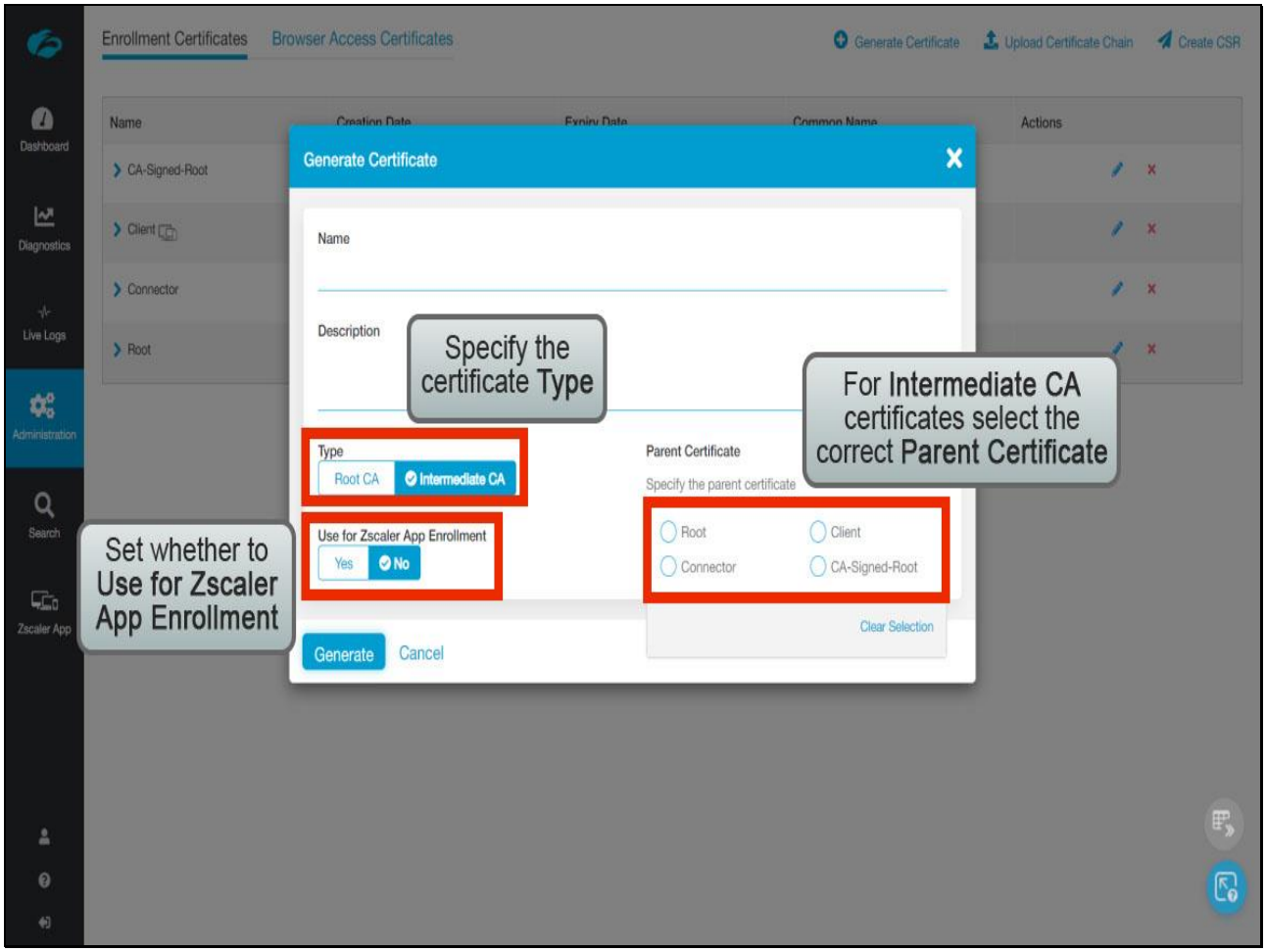


Slide notes

The new Root certificate will be added. You have the option to delete or edit both the default set of certificates and any that you upload or generate yourself. Deleting a Root CA will also delete the associated Intermediate CAs. If an Intermediate CA is deleted all identity certificates issued by it are immediately revoked, preventing any device with an identity certificate from that CA from connecting to the ZPA service.

To generate a certificate, click **Generate Certificate**, ...

Slide 51 - Slide 51

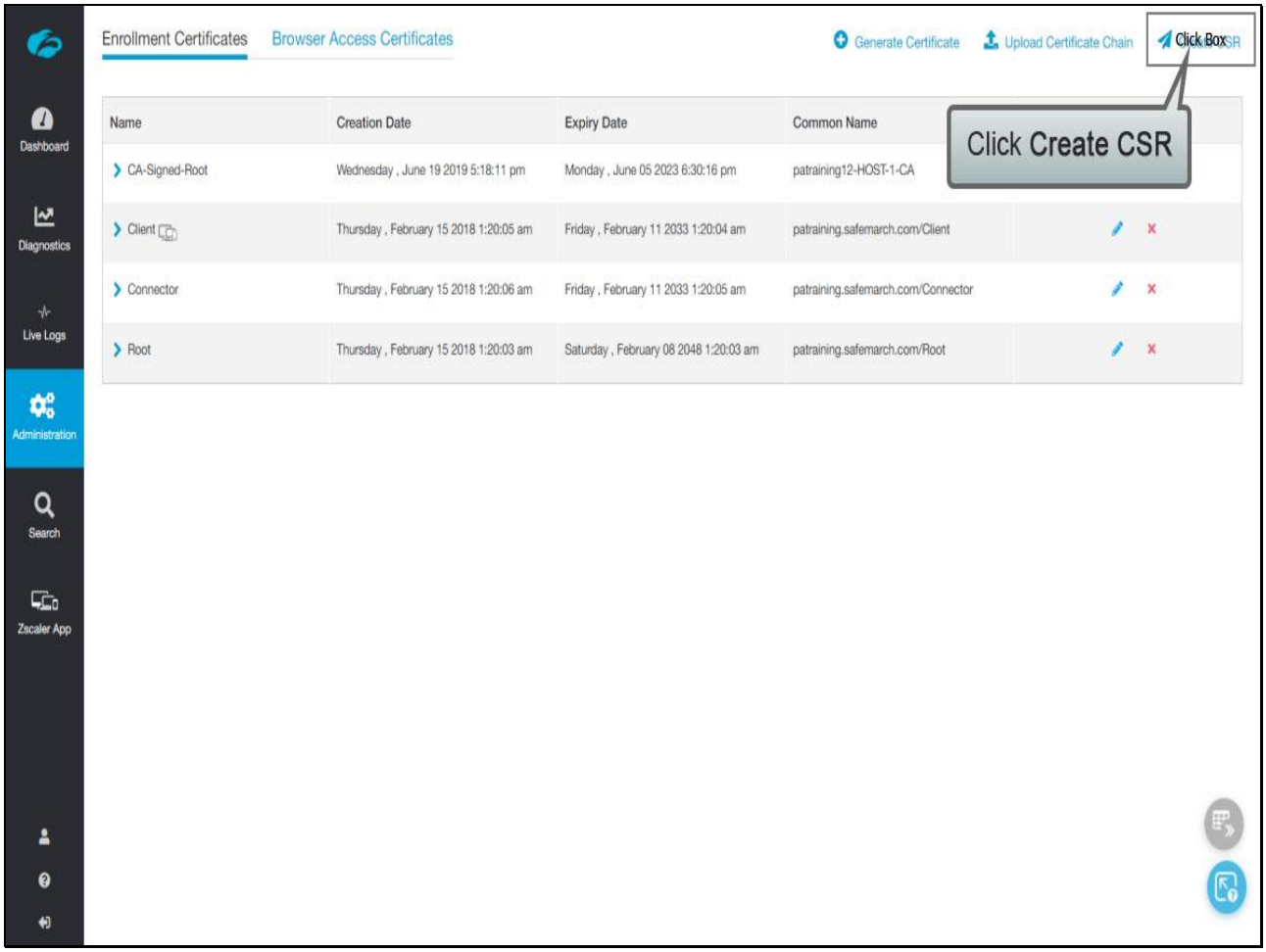


Slide notes

...you have the option to generate both a **Root CA** and one or more **Intermediate CAs**. When creating an **Intermediate CA**, you must select the **Root CA** to generate it from. We recommend that you generate at least two **Intermediate CAs**, one for enrolling Connectors and one for enrolling Zscaler App users. This then allows you to manage the certificate environments separately, for example to revoke only the Z App certificates after a compromise.

Also, when generating an **Intermediate CA**, you must specify whether it is to be the one to issue identity certificates when enrolling Zscaler App users. Only one Intermediate CA can be configured for this role at any time.

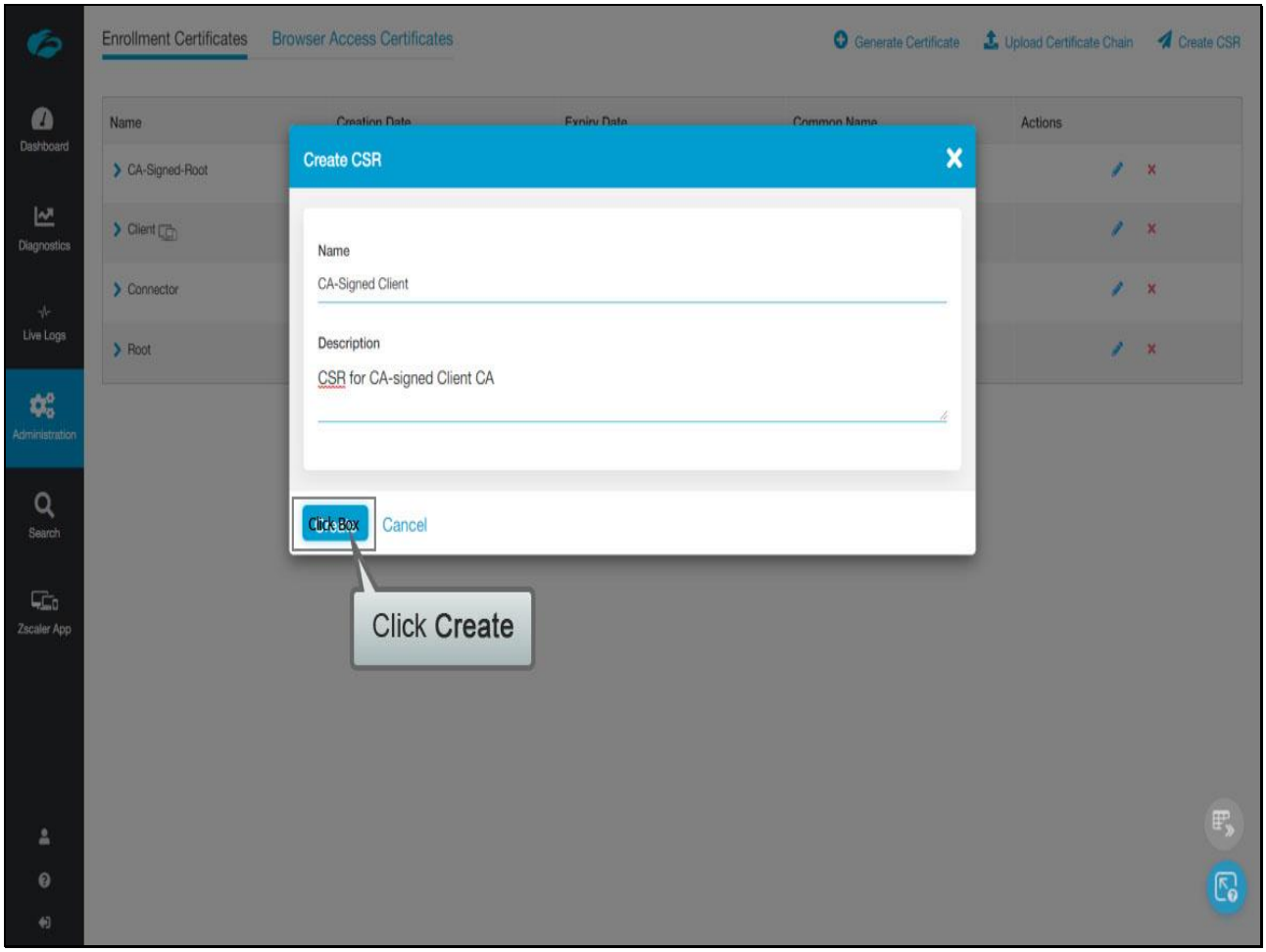
Slide 52 - Slide 52



Slide notes

To generate a Certificate Signing Request for an Intermediate CA that is to be signed by your own internal PKI, click **Create CSR**, ...

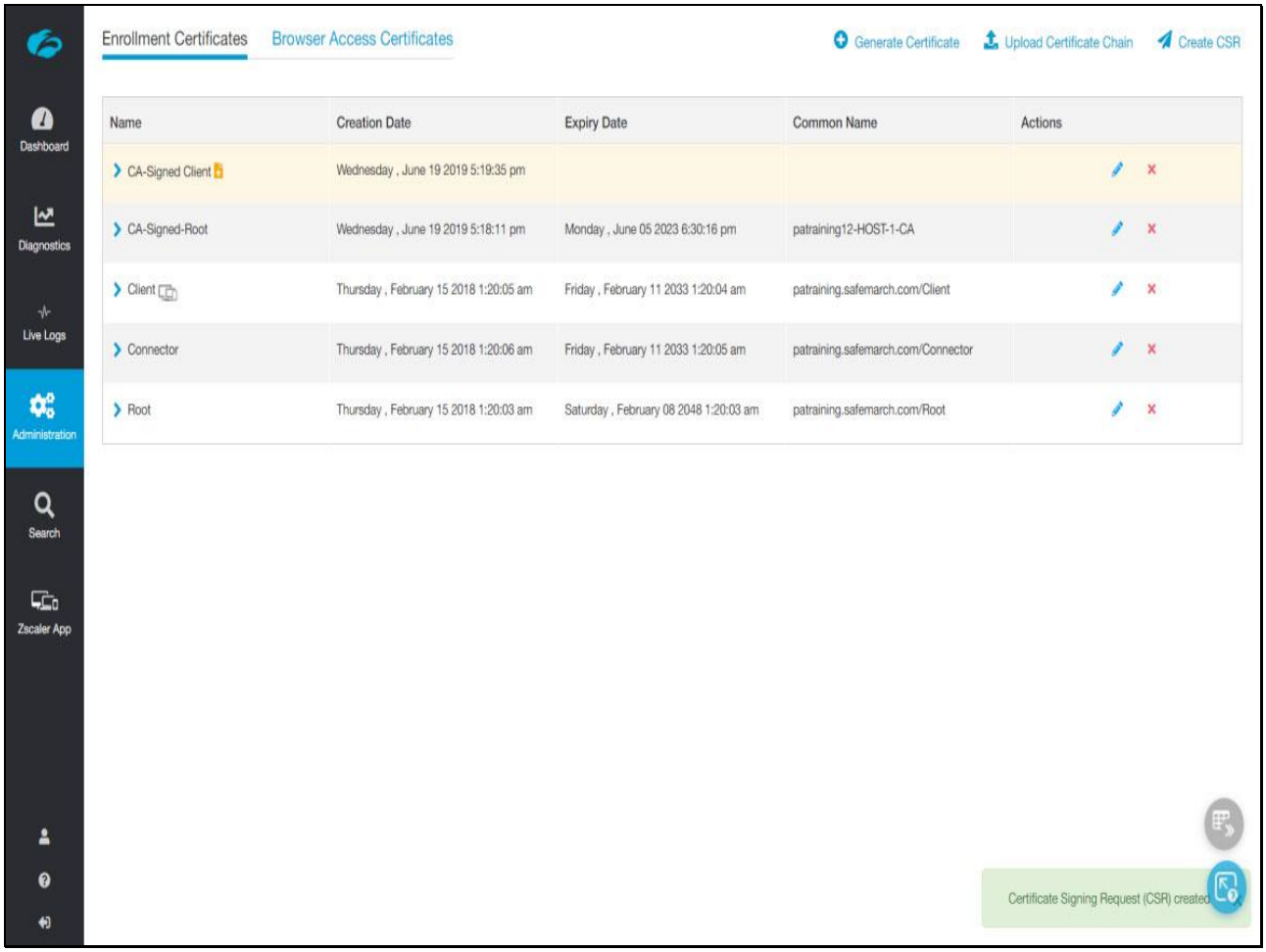
Slide 53 - Slide 53



Slide notes

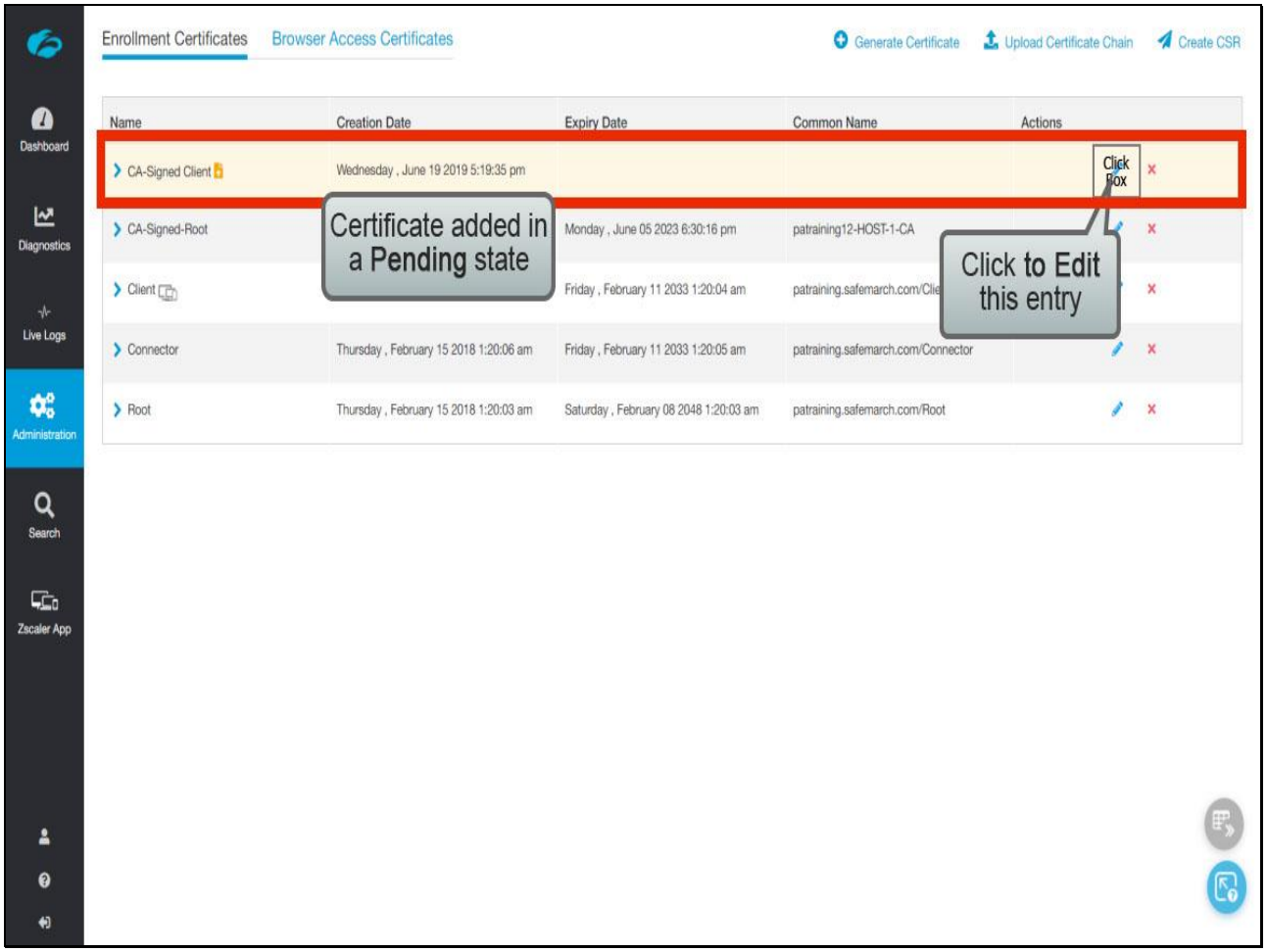
...configure the CSR as necessary and click **Generate**, ...

Slide 54 - Slide 54



Slide notes

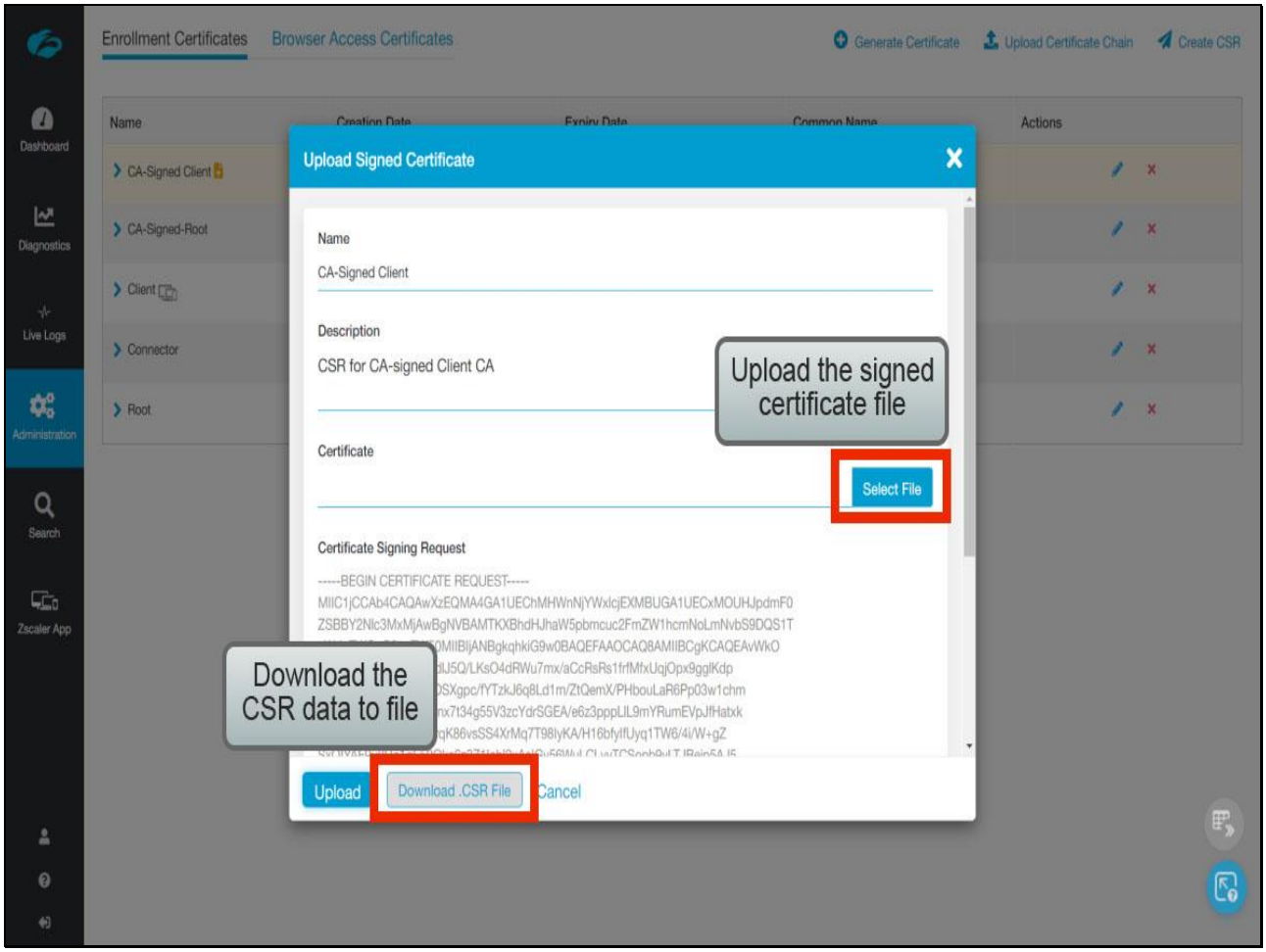
Slide 55 - Slide 55



Slide notes

...the **Intermediate CA** is added to the list in the pending state. To complete activation of this **Intermediate CA** you must have the CSR signed by the appropriate root CA (or a subordinate of it) and upload the resulting certificate. To manage this process, click to **Edit** this entry, ...

Slide 56 - Slide 56

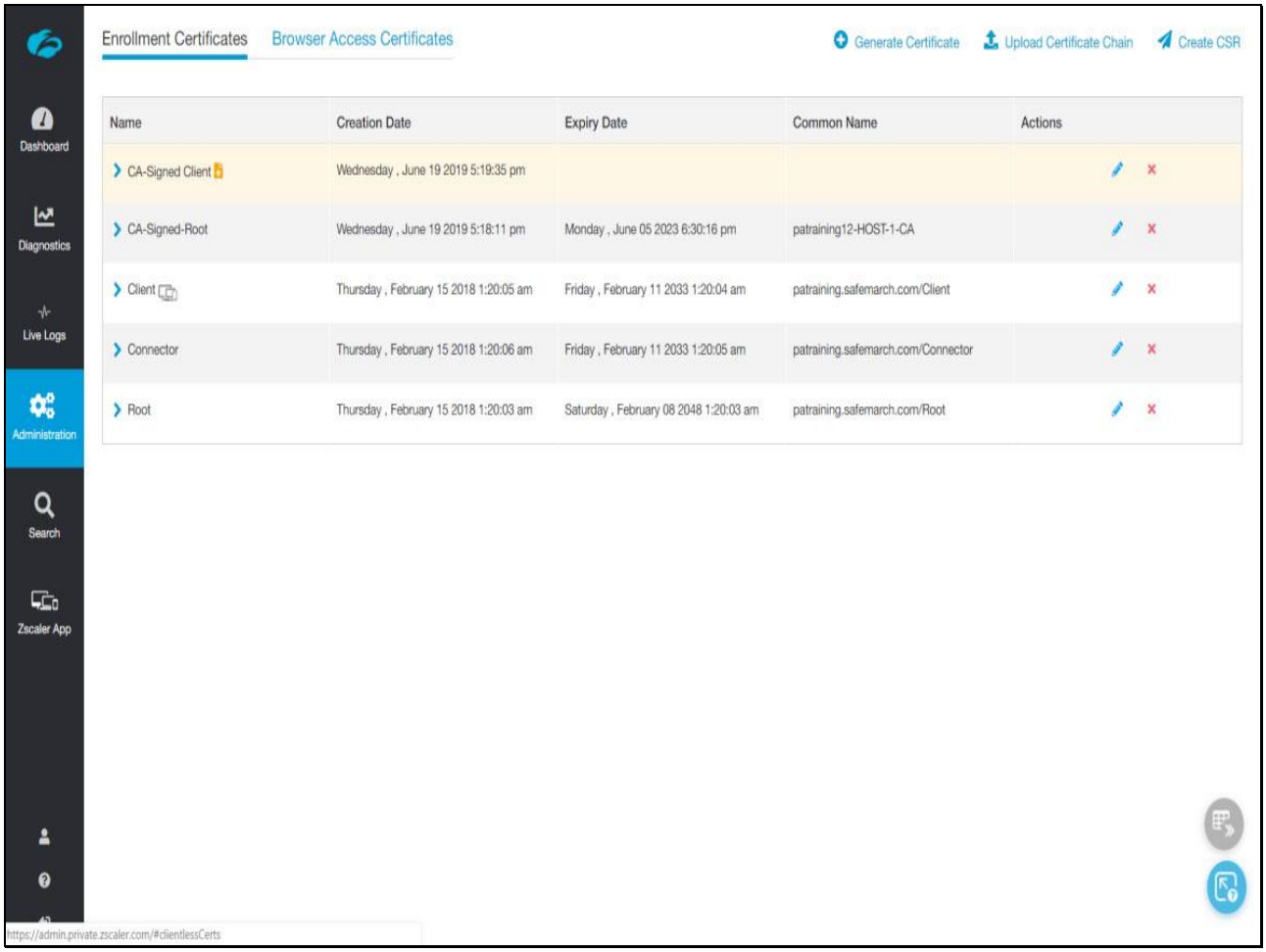


Slide notes

...you have the option here to **Download .CSR File**, to allow you to save the CSR data to file and take it to the appropriate CA to be signed. Once that is done the **Select File** option allows you to upload the signed certificate to activate this **Intermediate CA**.

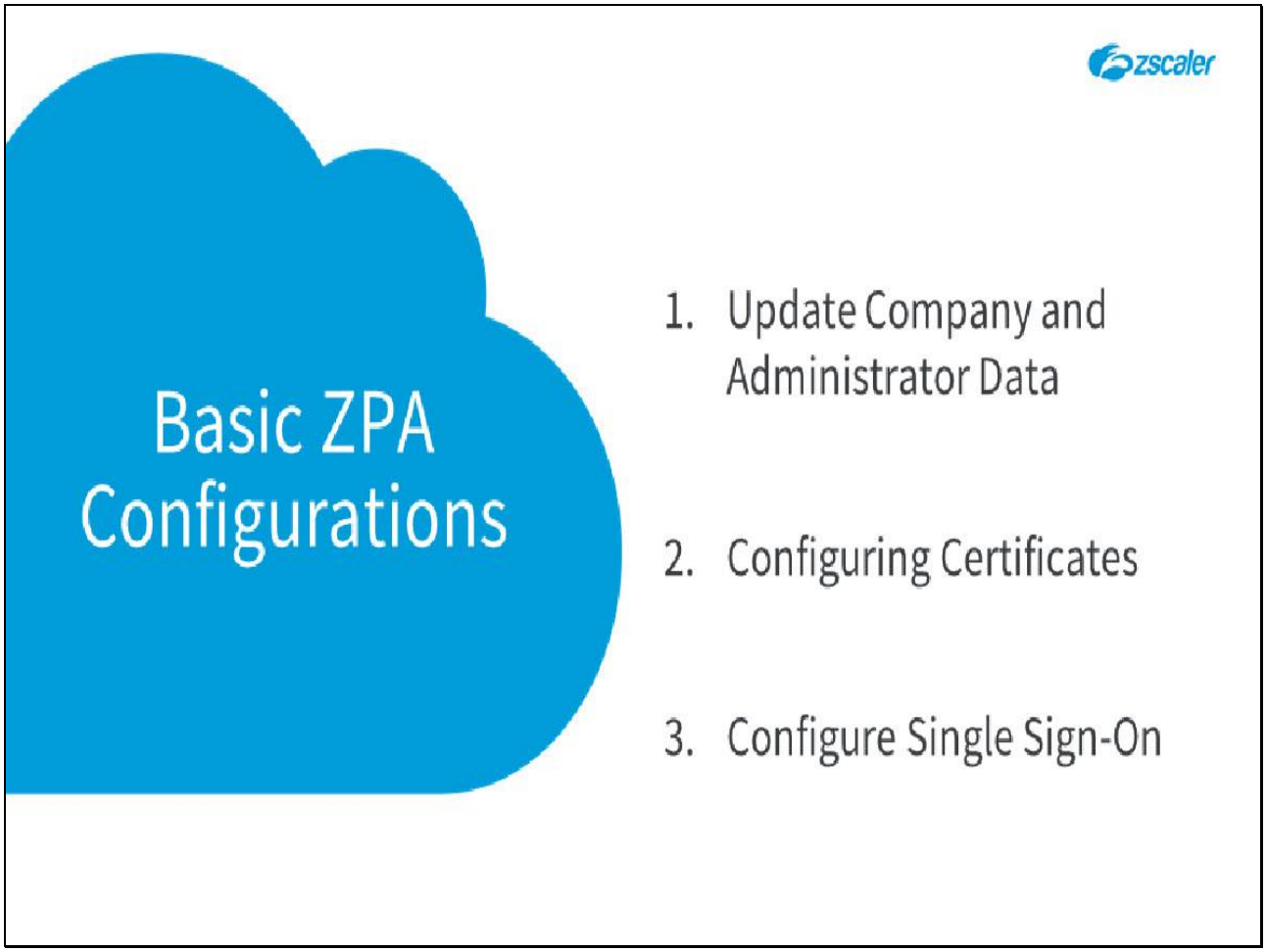
Note that for CA-signed **Intermediate CAs** of this nature, the signing CA's **Root** CA certificate must also be present in the certificate list.

Slide 57 - Slide 57



Slide notes

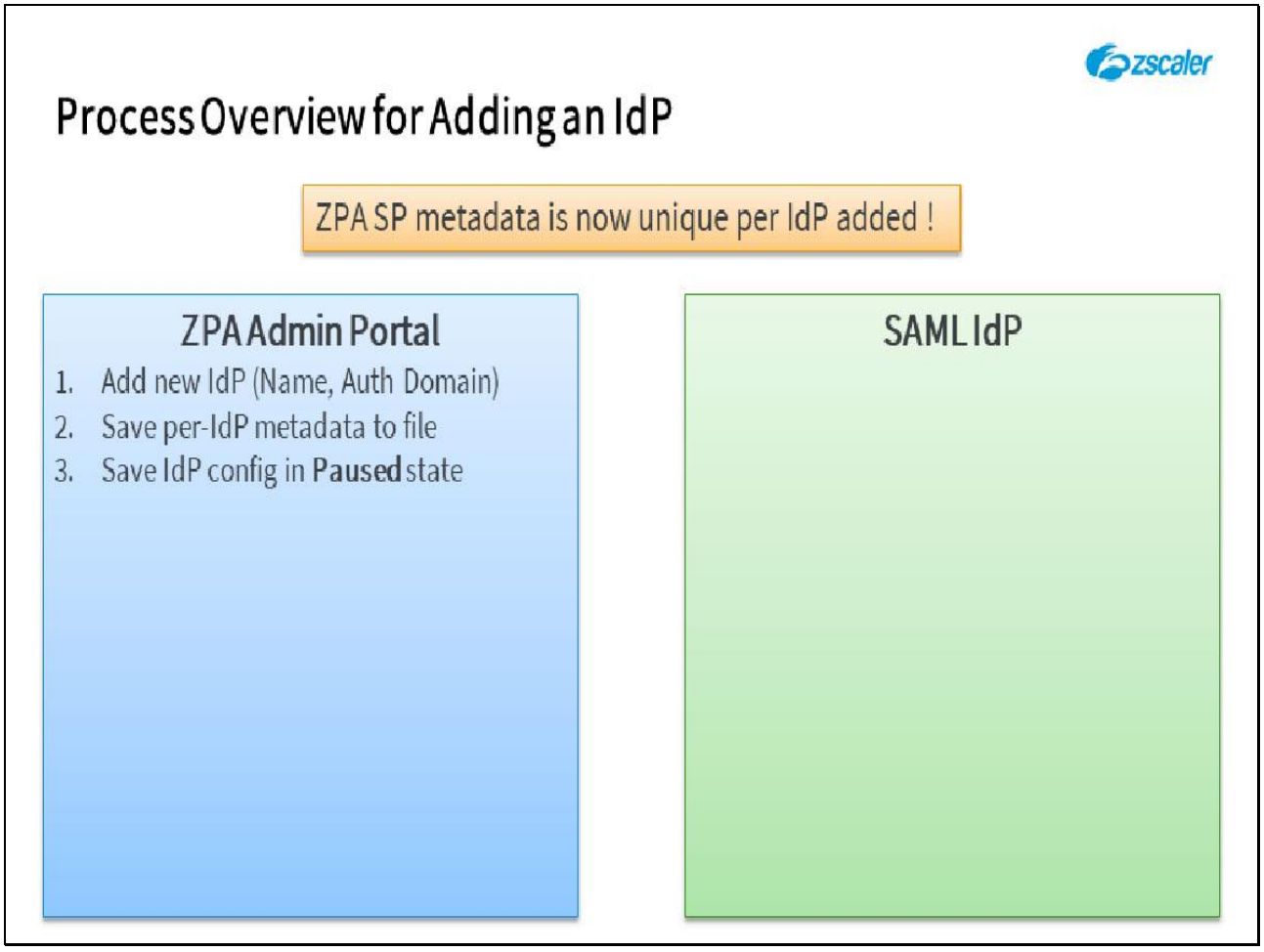
Slide 58 - Basic ZPA Configurations



Slide notes

In the final section we will look at configuring single sign-on for ZPA.

Slide 59 - Process Overview for Adding an IdP

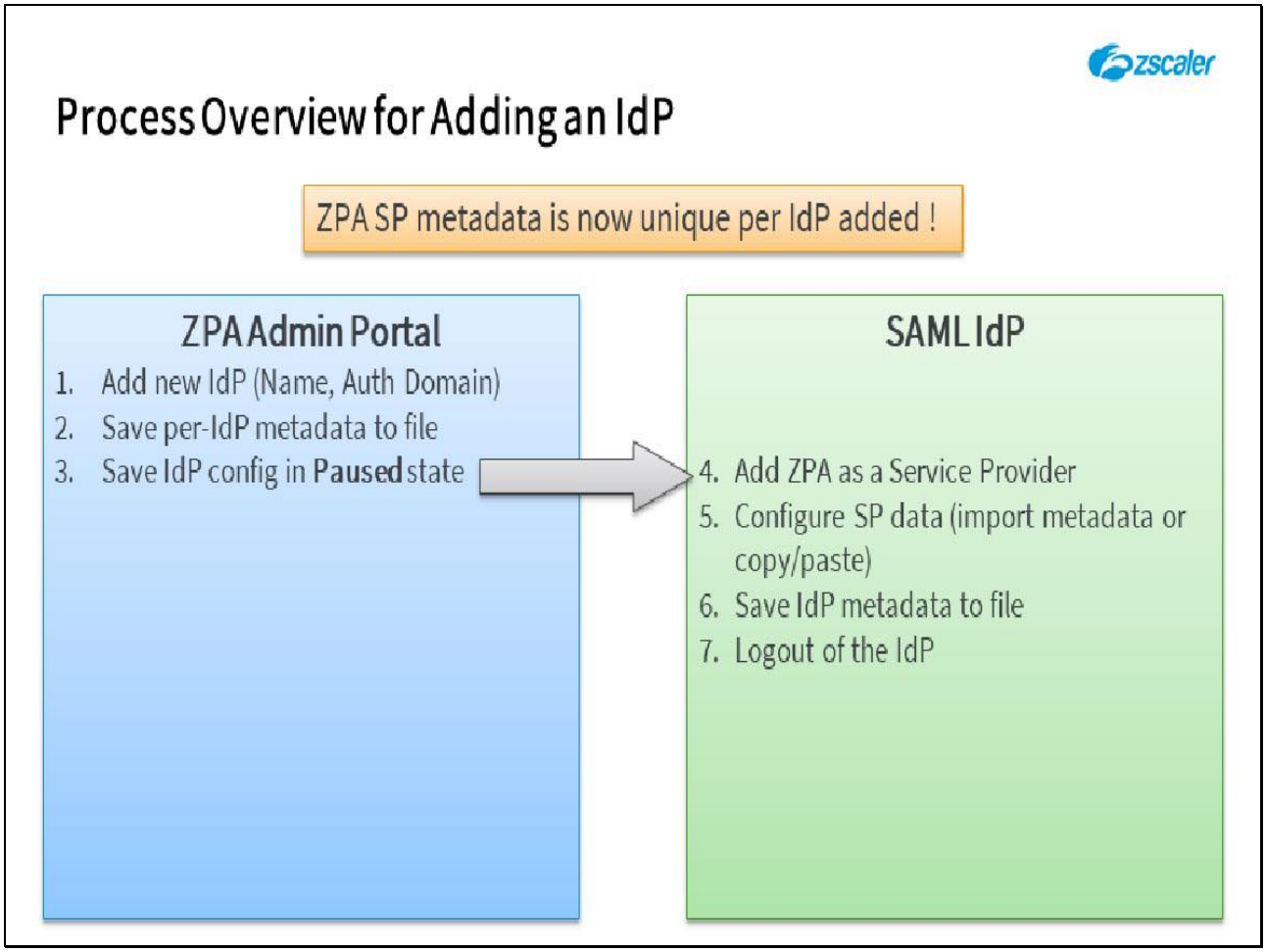


Slide notes

The ZPA service allows you to authenticate your user population against multiple IdPs if necessary, which requires that the ZPA Service Provider (SP) metadata be unique for each of the IdPs that you use. As a result, it is necessary for you to start the process of adding an IdP in the ZPA Admin Portal, even if you only plan to add the one.

The outline process for adding a new IdP is shown here: It starts in the ZPA Admin Portal with you adding a new IdP, giving it a name and selecting the **Authentication Domain** (or domains) to associate to it; the per-IdP SP metadata will be generated (including the **URL** and **Entity ID**) and can be saved to a metadata file if necessary; You can then **Pause** the addition of the IdP, which saves it to the Admin Portal in an incomplete state;

Slide 60 - Process Overview for Adding an IdP

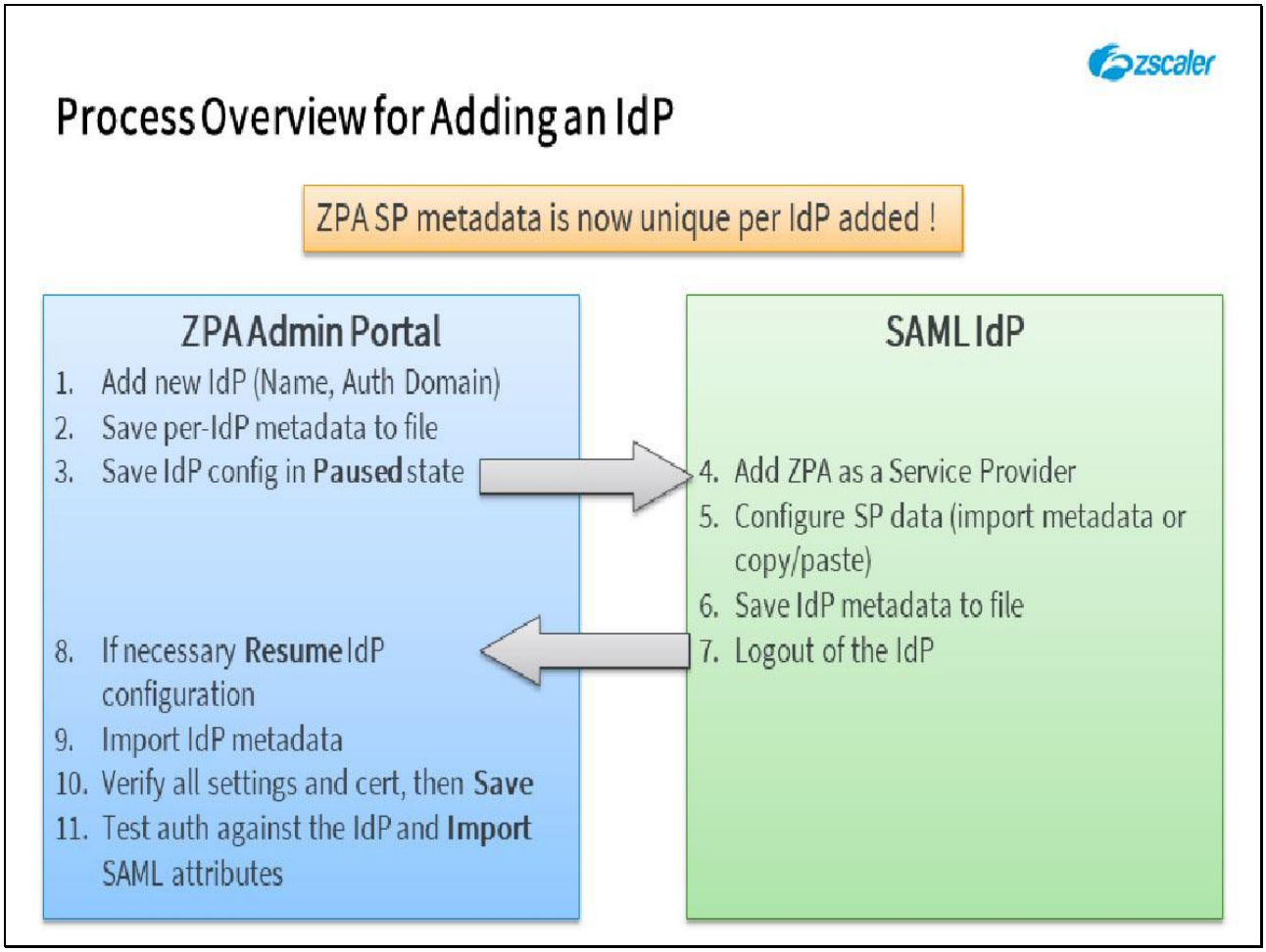


Slide notes

Next, you will need to step across to the Admin Portal of the IdP that you wish to add and find the latest version of the Zscaler **ZPA App** to add as a new SP, don't forget to assign it to the users who need to use it; You need to configure the SP using the data generated previously at the ZPA Admin Portal, with some IdPs you may be able to import the SP metadata file that you saved, others require you to manually configure the **URL** and **Entity ID**;

Having configured the App in the IdP, you can normally save the IdP metadata to file; you then need to logout of the IdP (so you can test the integration from ZPA).

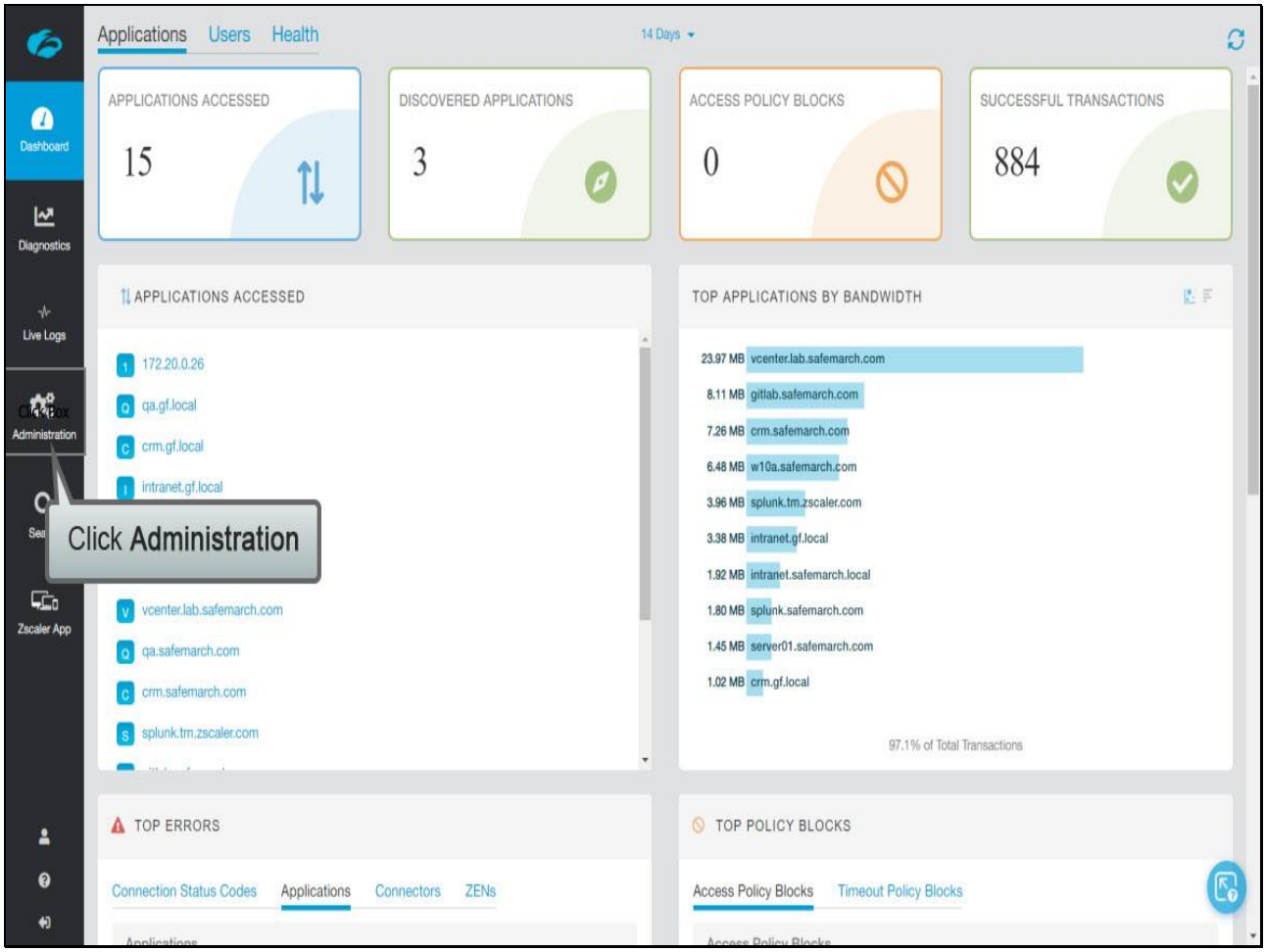
Slide 61 - Process Overview for Adding an IdP



Slide notes

Back in the ZPA Admin Portal, you can **Resume** the configuration of the IdP; import the IdP metadata file that you just saved to configure it in the ZPA Admin Portal and add the IdP certificate; verify or adjust configuration settings as required and save the IdP configuration; finally you can test that the integration works (by authenticating a regular user against the IdP) and import the **SAML Attributes** provided by the IdP.

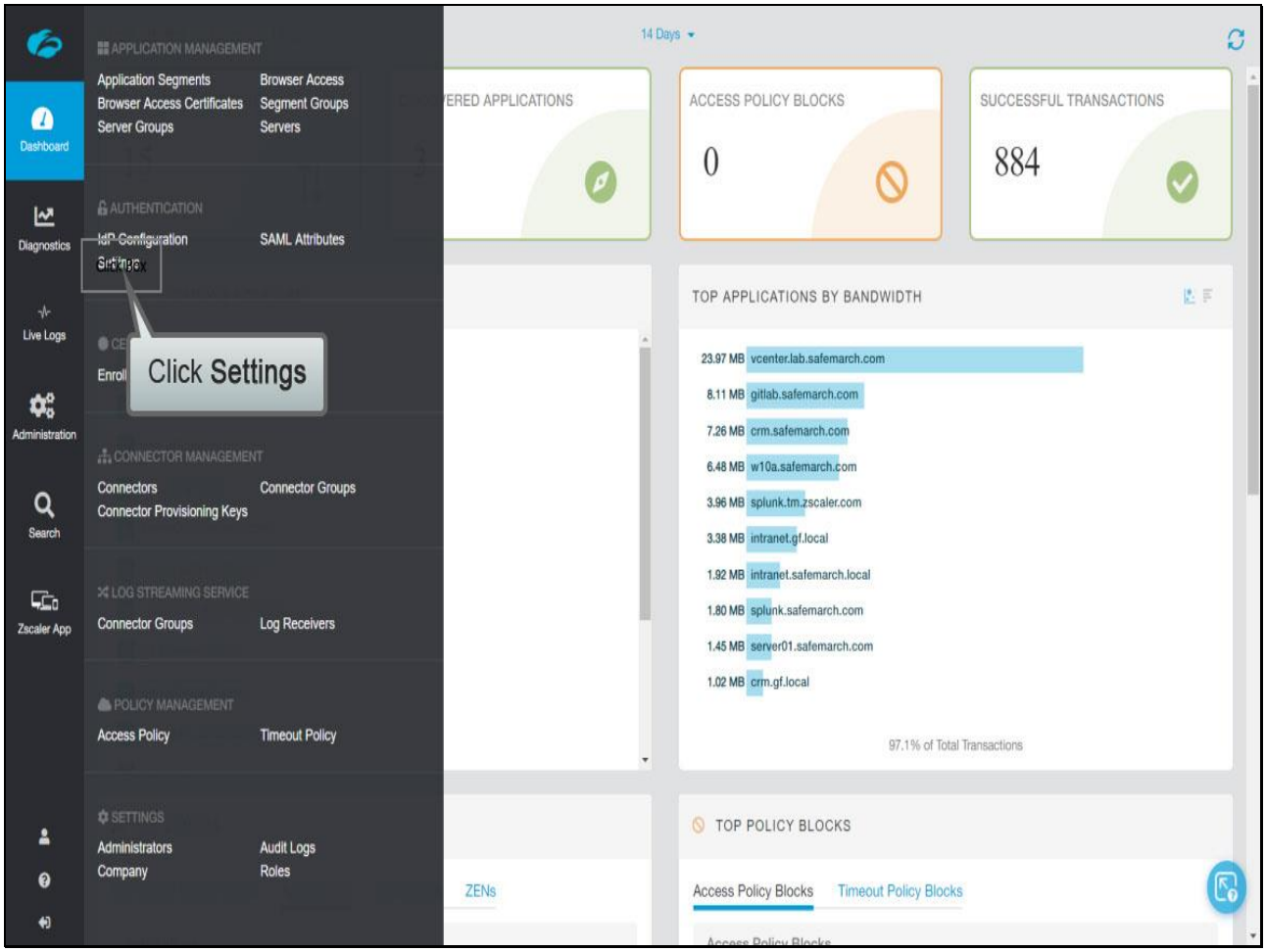
Slide 62 - Slide 62



Slide notes

To expand the configuration options, click **Administration**, ...

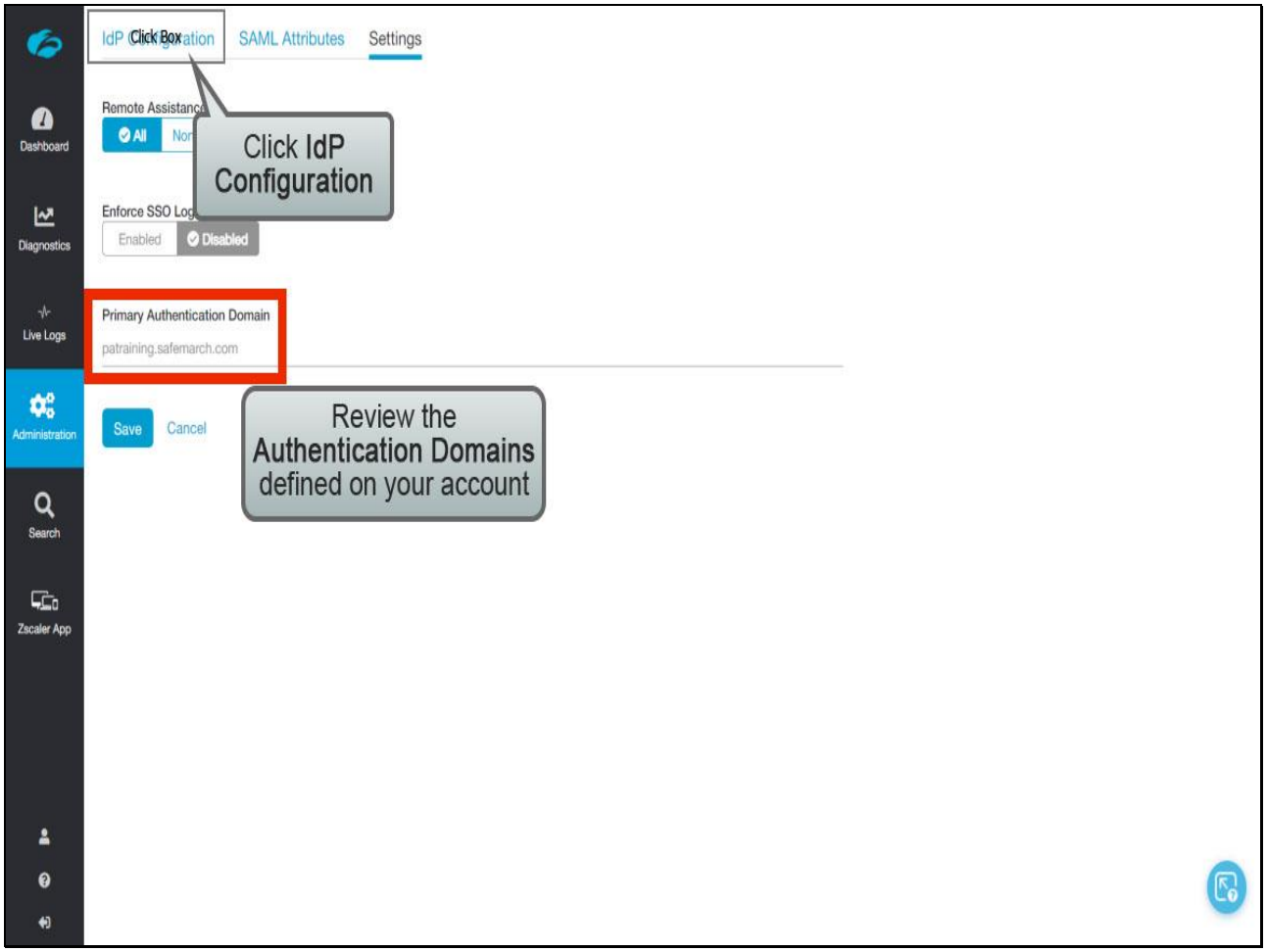
Slide 63 - Slide 63



Slide notes

...to review your primary and any additional authentication domains defined by Zscaler support on your account, under the **AUTHENTICATION** section, click **Settings**.

Slide 64 - Slide 64

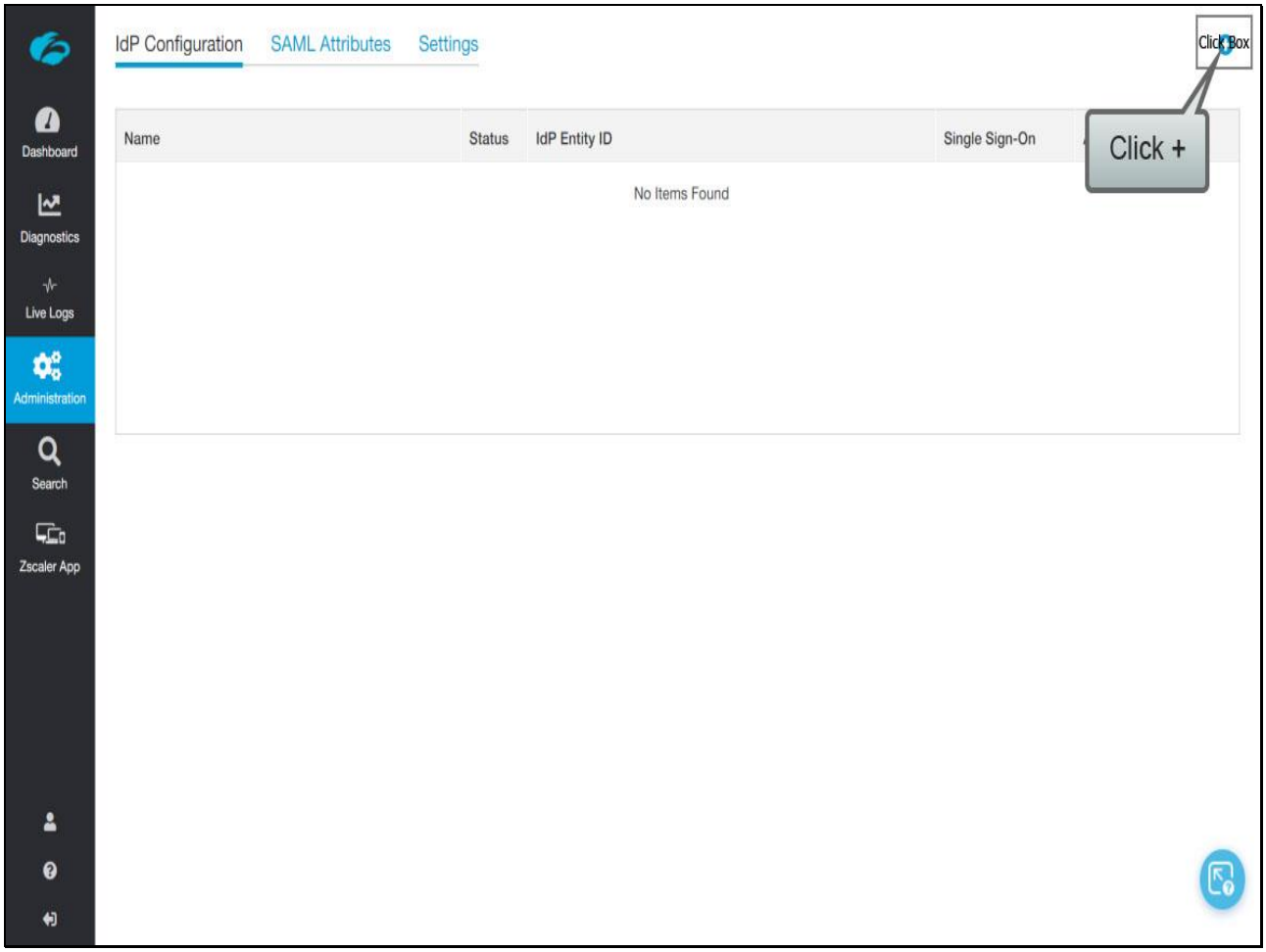


Slide notes

On this page you can review the **Authentication Domains** that are defined for the organization. If domains are missing or incorrect, you will need to contact Zscaler support. Note that if you need to add multiple IdPs to the ZPA Admin Portal then you must have at least one **Authentication Domain** per-IdP.

To access the ZPA Service Provider (SP) metadata and to add an IdP to the system, click **IdP Configuration**.

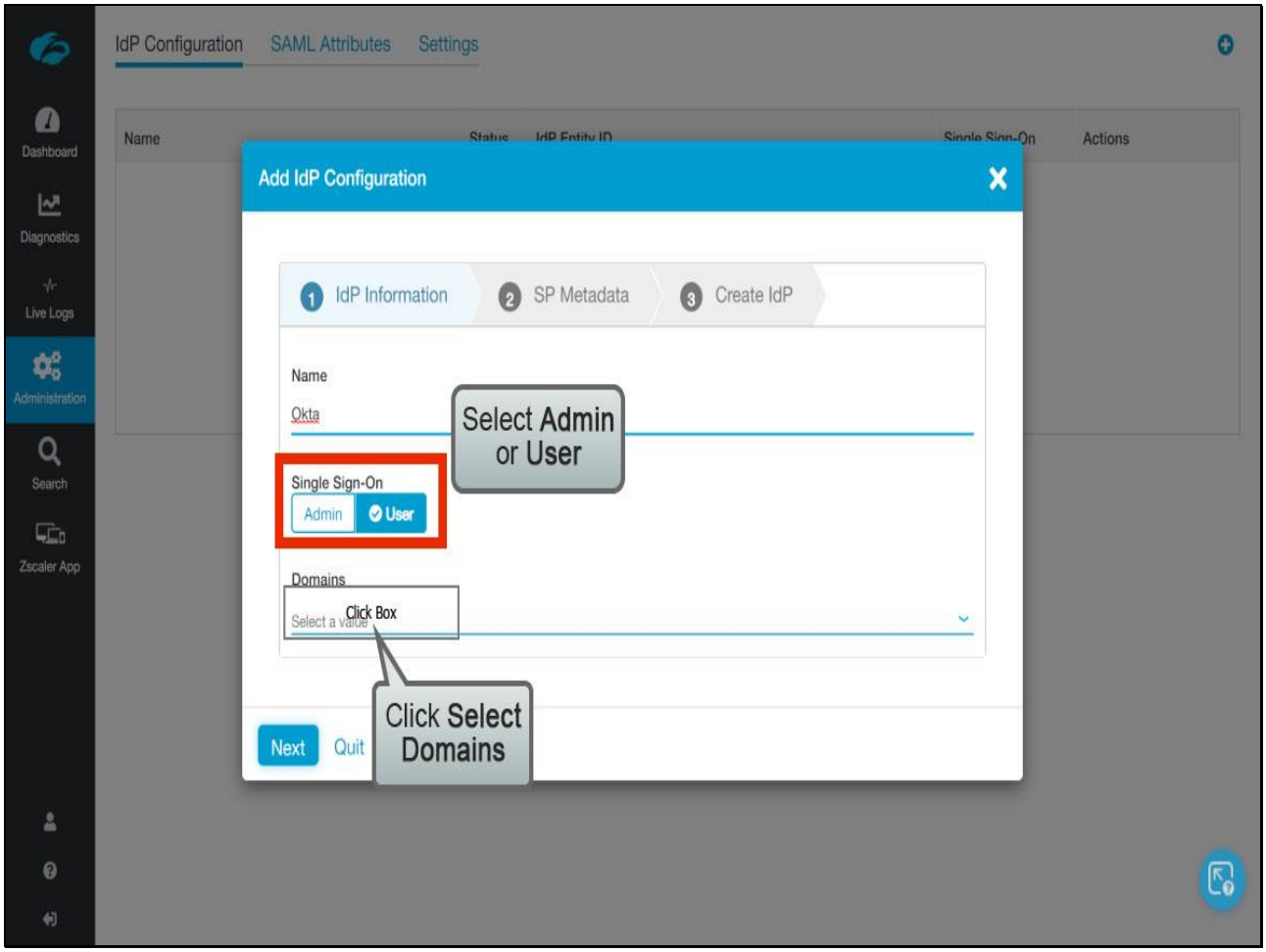
Slide 65 - Slide 65



Slide notes

To add an IdP, click the **+** icon, ...

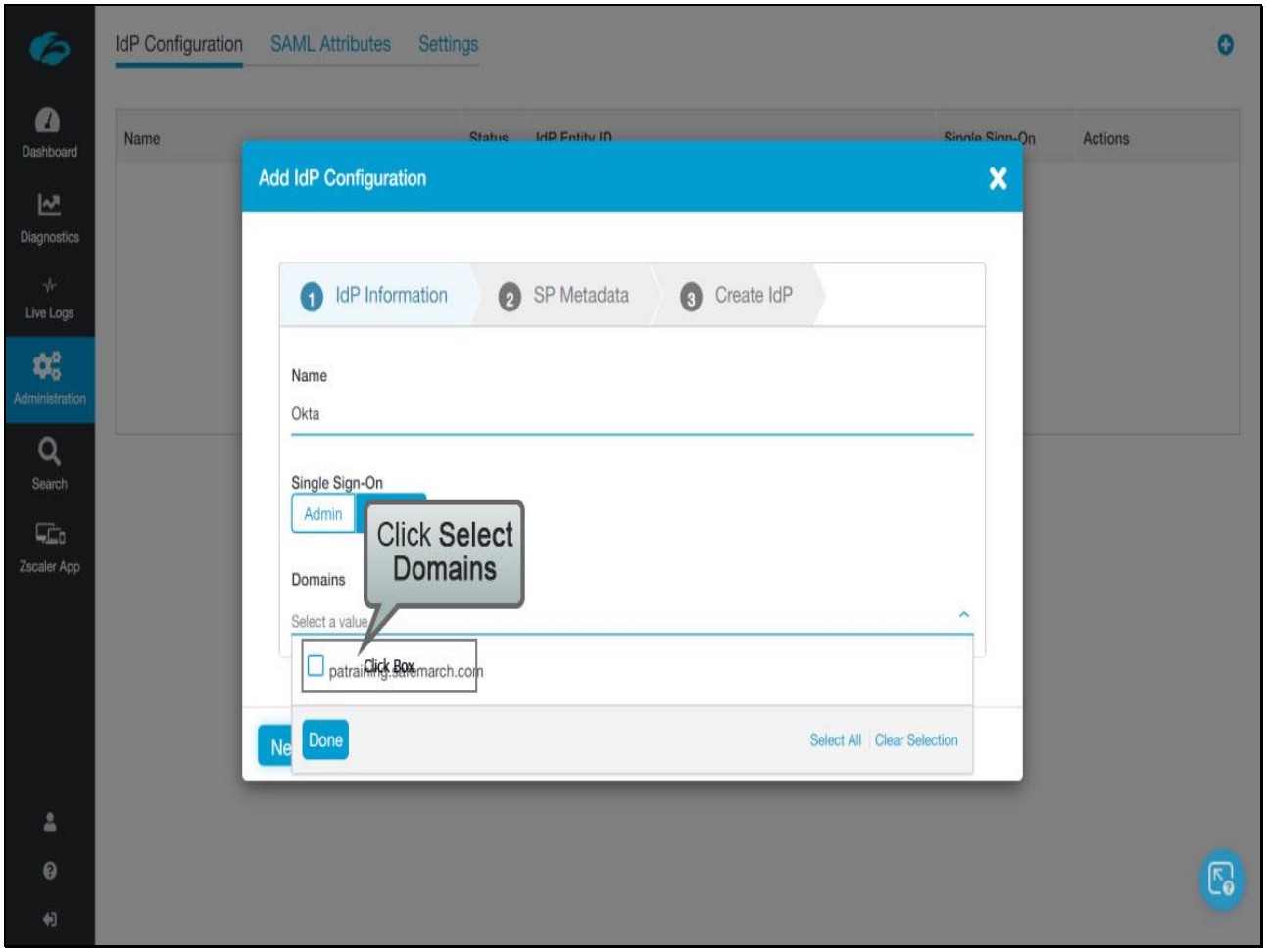
Slide 66 - Slide 66



Slide notes

...**Name** the IdP (in this example we are adding Okta), specify whether this IdP will be used for **Admin** or **User** SSO. Note that separate IdPs are required to authenticate your administrators. Click to select the **Authentication Domain**(s) to associate to it.

Slide 67 - Slide 67

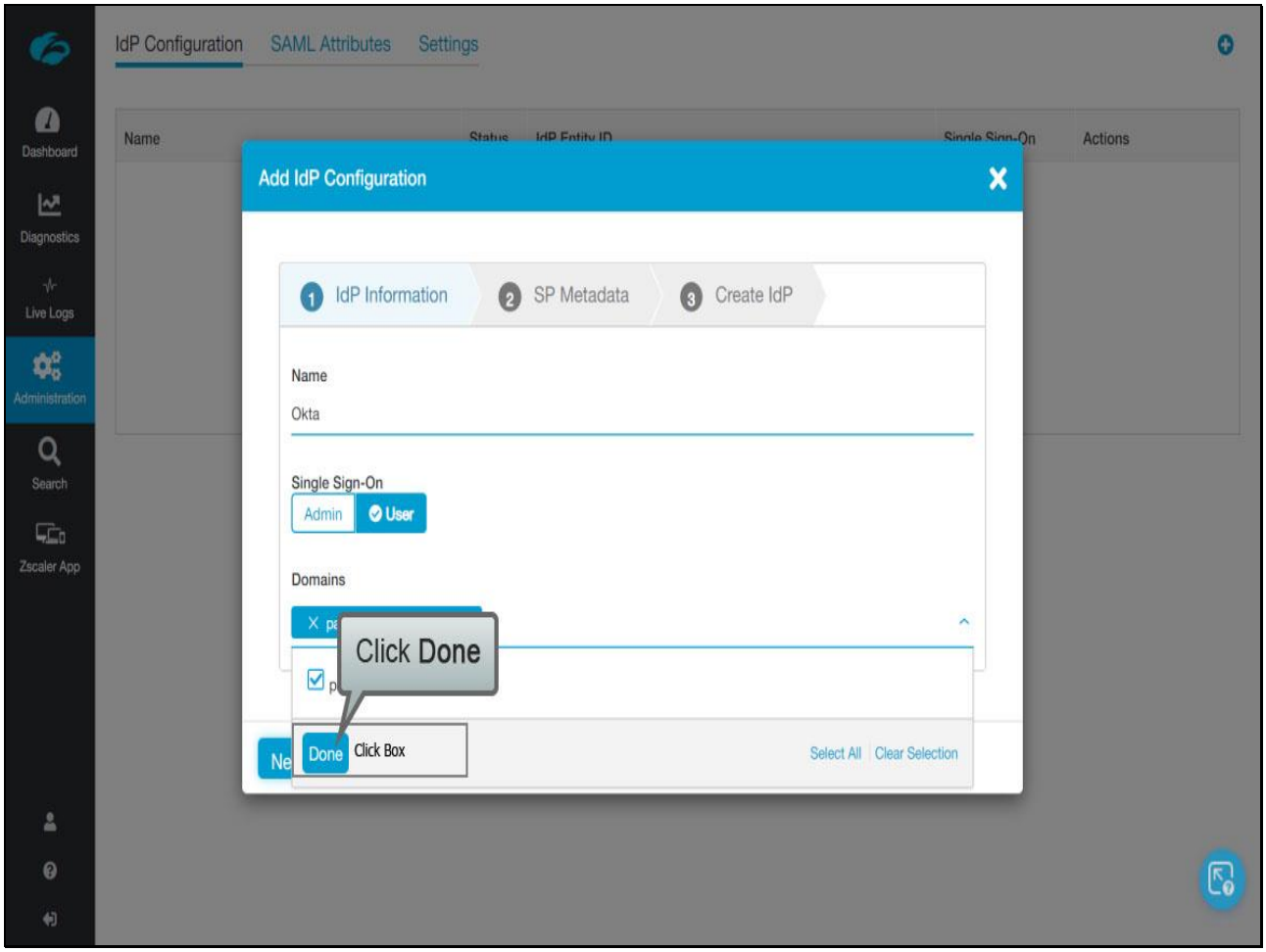


Slide notes

Select one or more of the listed domains to be matched for SSO with this IdP. Note that multiple Domains can be selected here, however a Domain can only be associated to one IdP, meaning that any Domains you select here cannot be used in another IdP configuration.

For administrator SSO you must select here the domain for your administrator users. This may be the same as one of the domains you use for user SSO, or it can be a completely different domain.

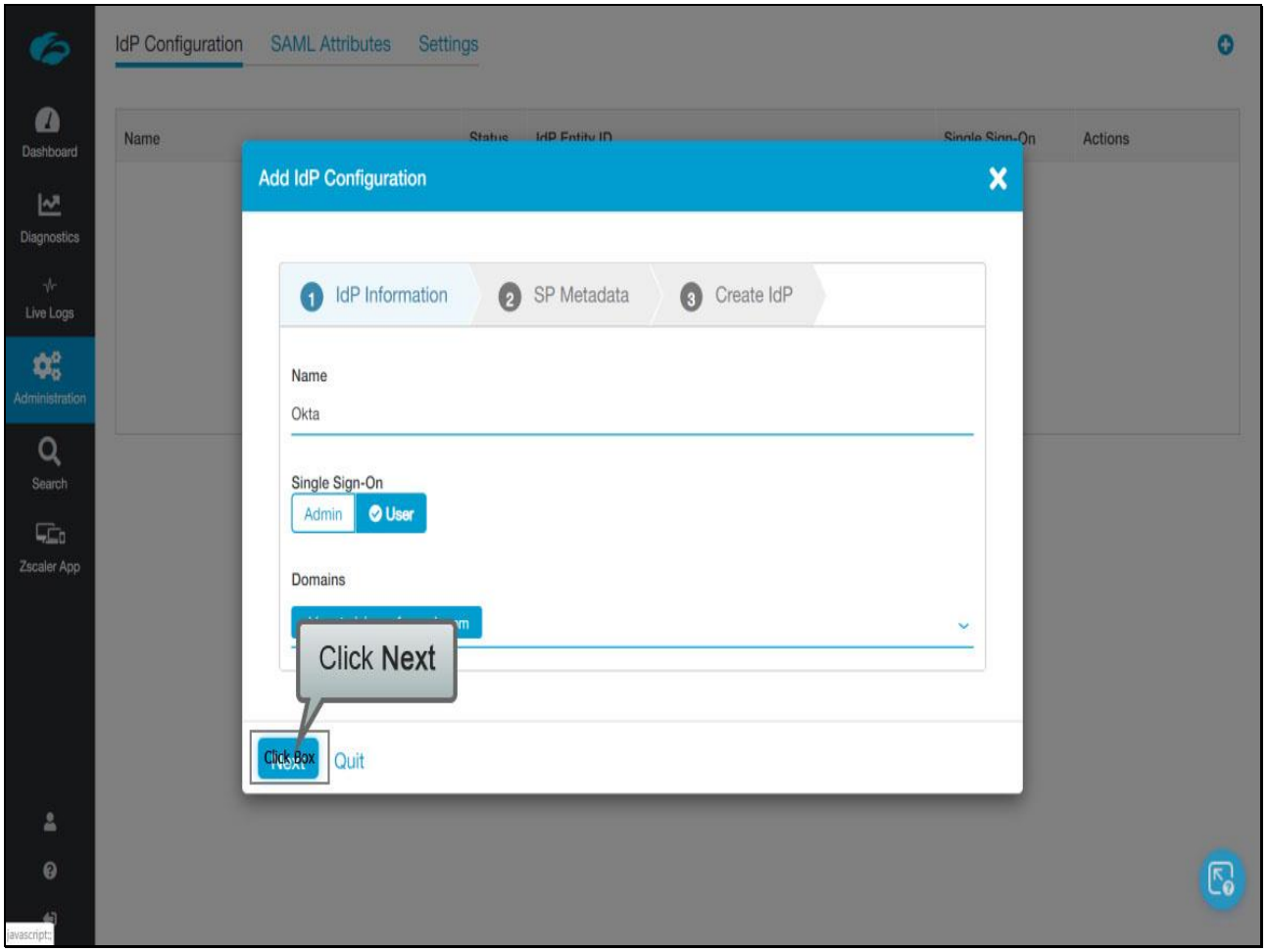
Slide 68 - Slide 68



Slide notes

Click **Done** to add the domains, ...

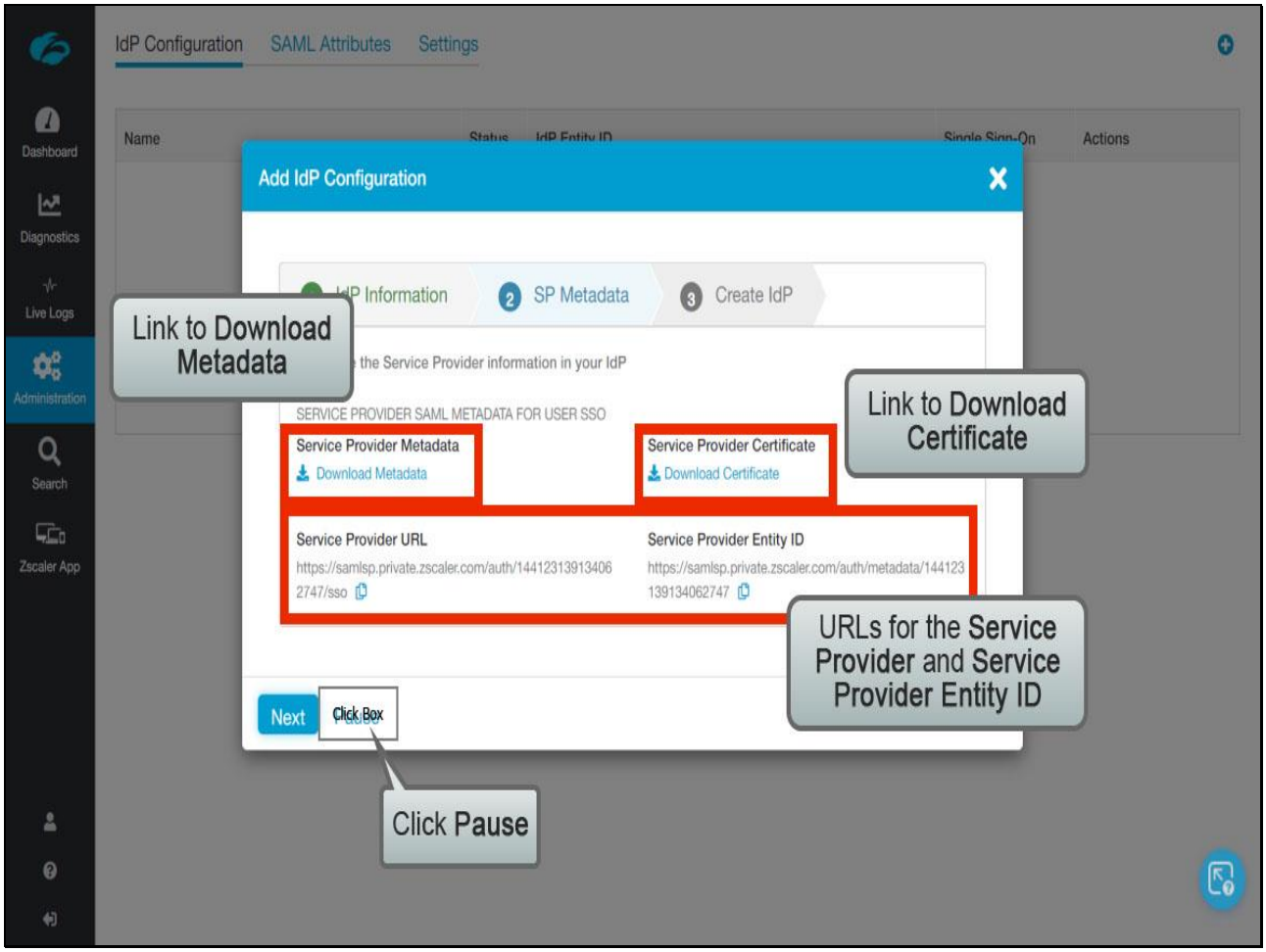
Slide 69 - Slide 69



Slide notes

...then click **Next**.

Slide 70 - Slide 70

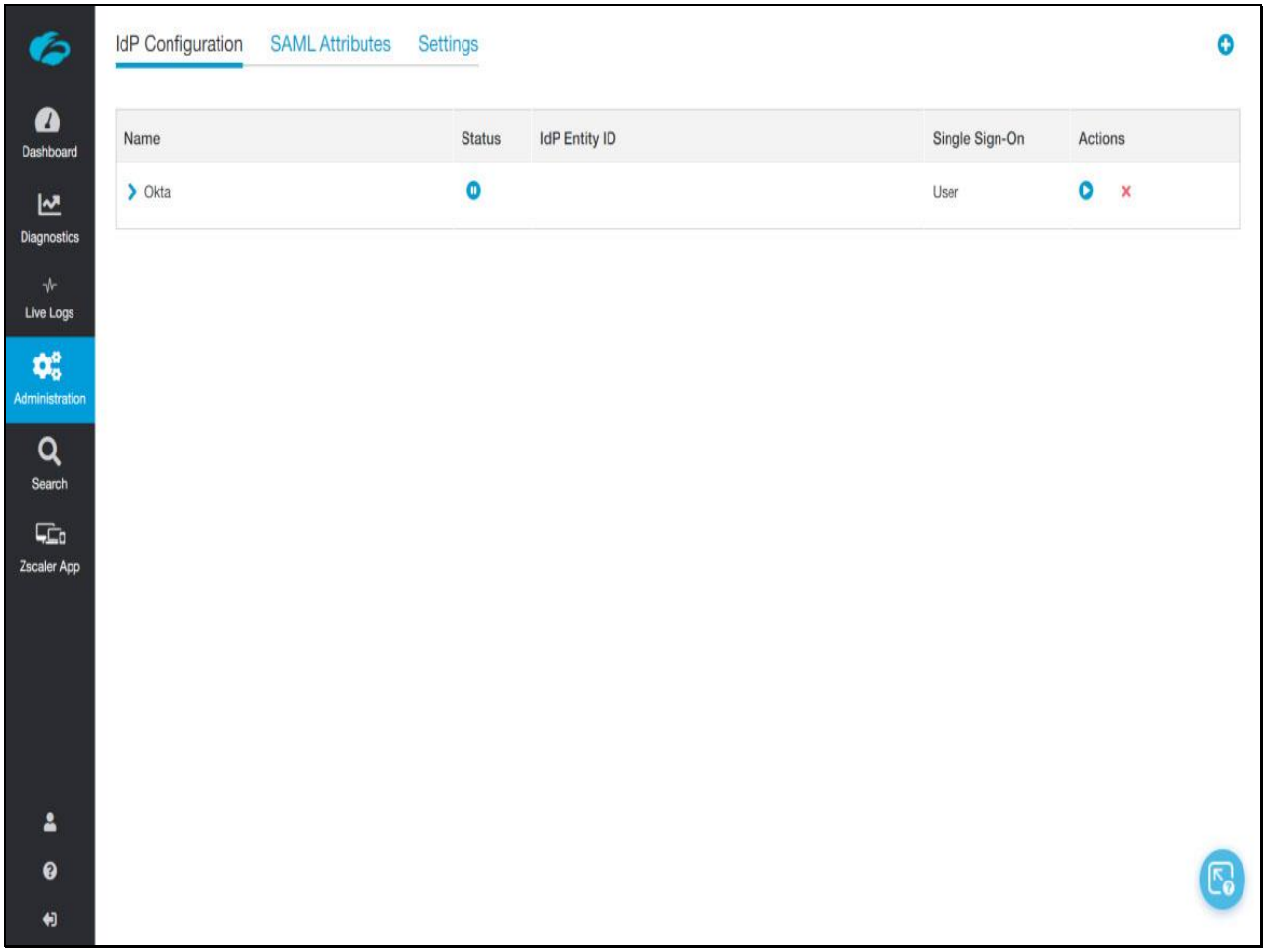


Slide notes

ZPA will generate the SP metadata for this new IdP and list it on this page. Links are provided to allow you to download the SP metadata and/or the certificate should your IdP require it. Plus, the **Service Provider URL** and **Service Provider Entity ID** are shown to allow you to copy/paste this data if required.

Either leave this page open while you configure the IdP or click the **Pause** button to save the IdP configuration in its current, incomplete state.

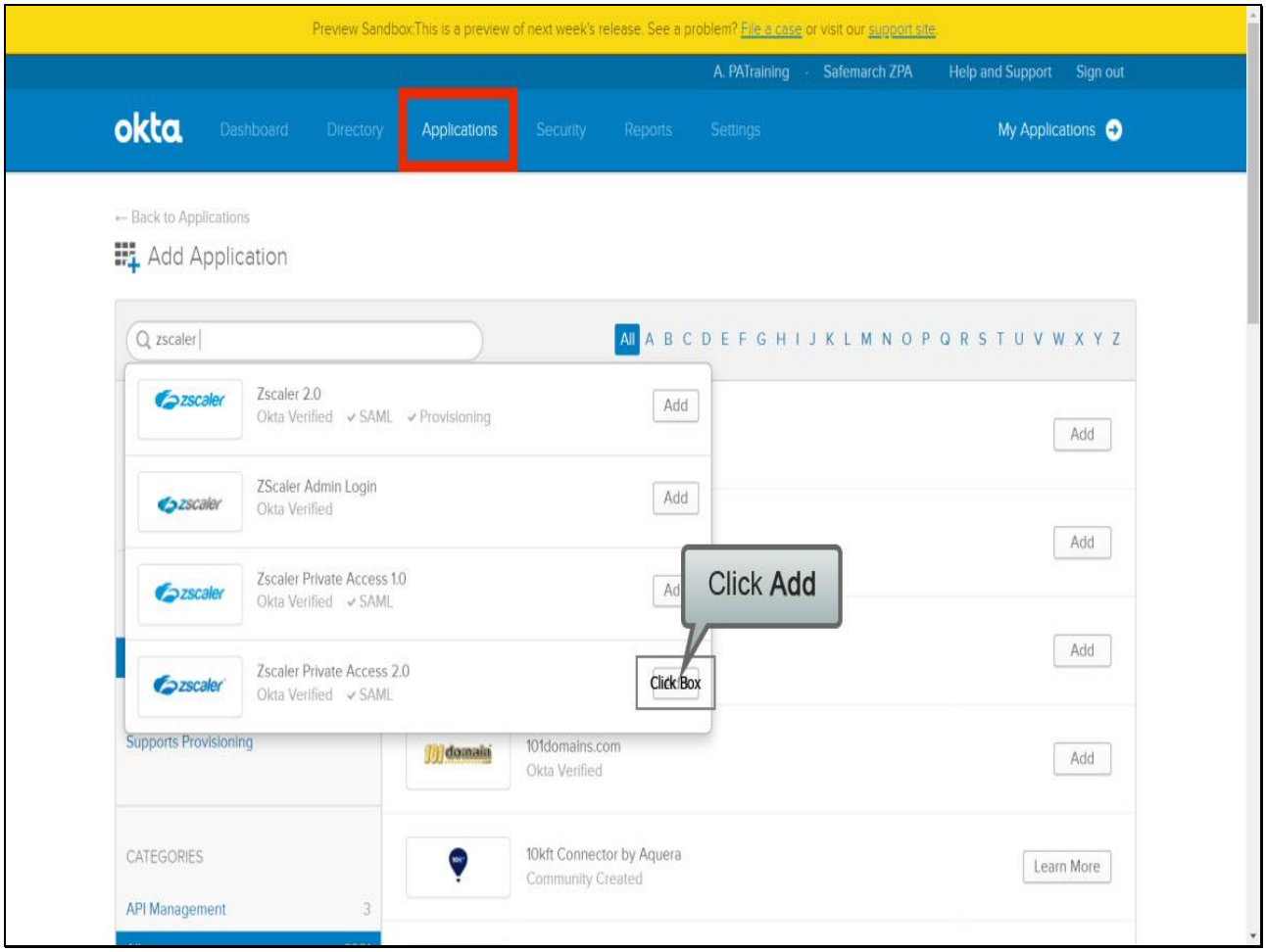
Slide 71 - Slide 71



Slide notes

You now need to step across to the Admin Portal for your IdP...

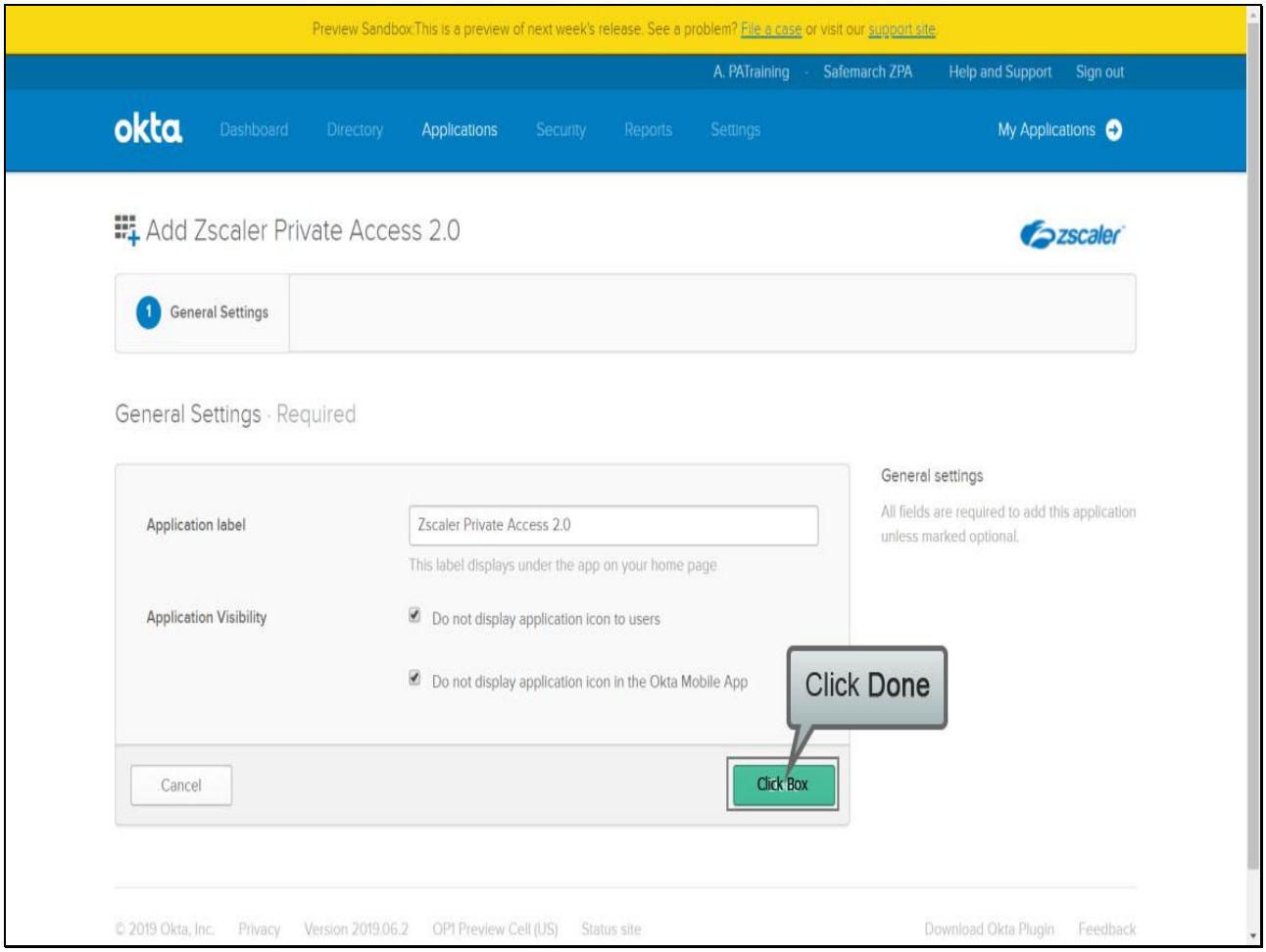
Slide 72 - Slide 72



Slide notes

...we are using Okta in this example. From the **Applications** page you will need to add the latest version of the Zscaler ZPA App (**Zscaler Private Access 2.0** currently).

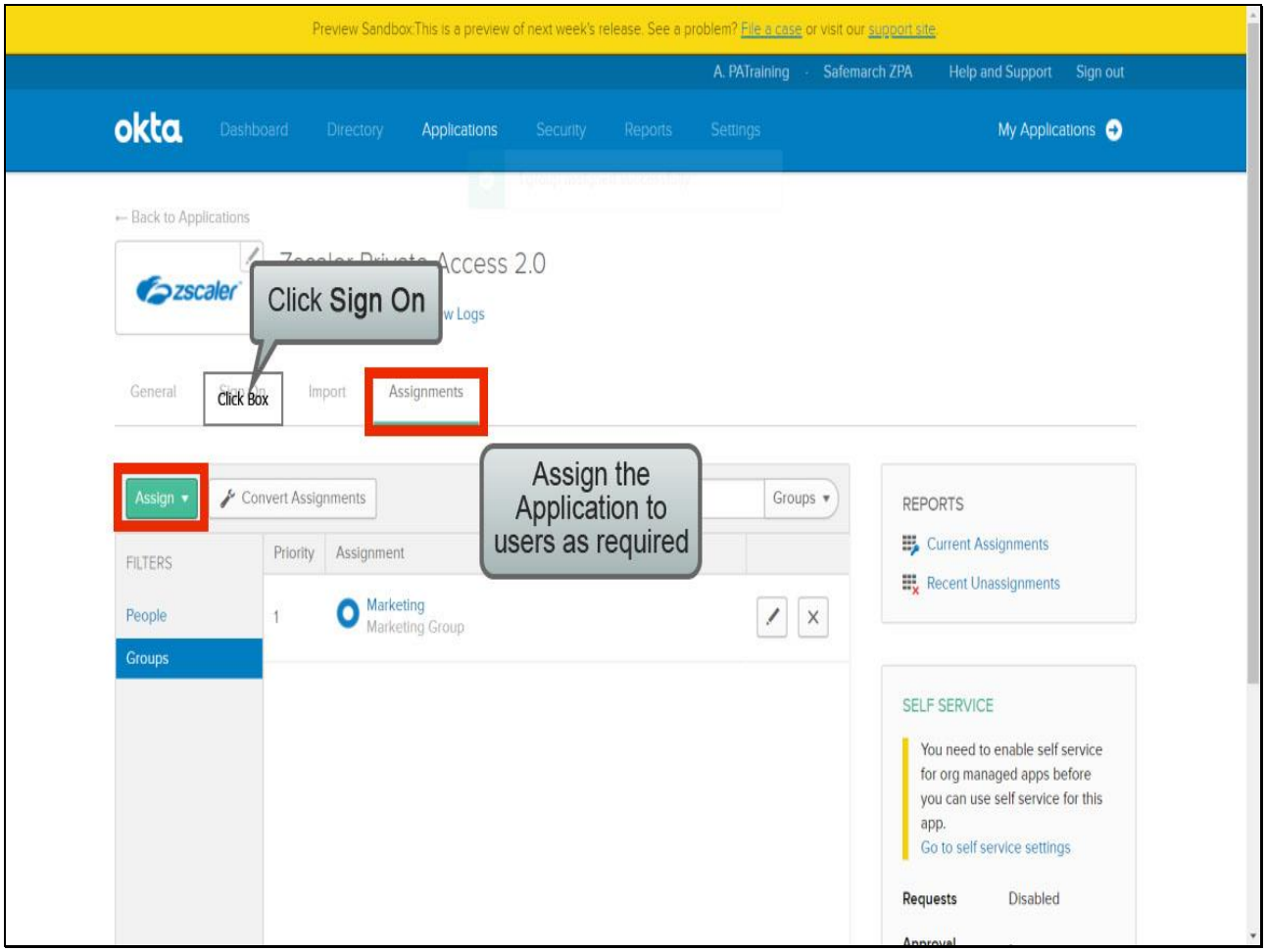
Slide 73 - Slide 73



Slide notes

Name it, configure it and click **Done**.

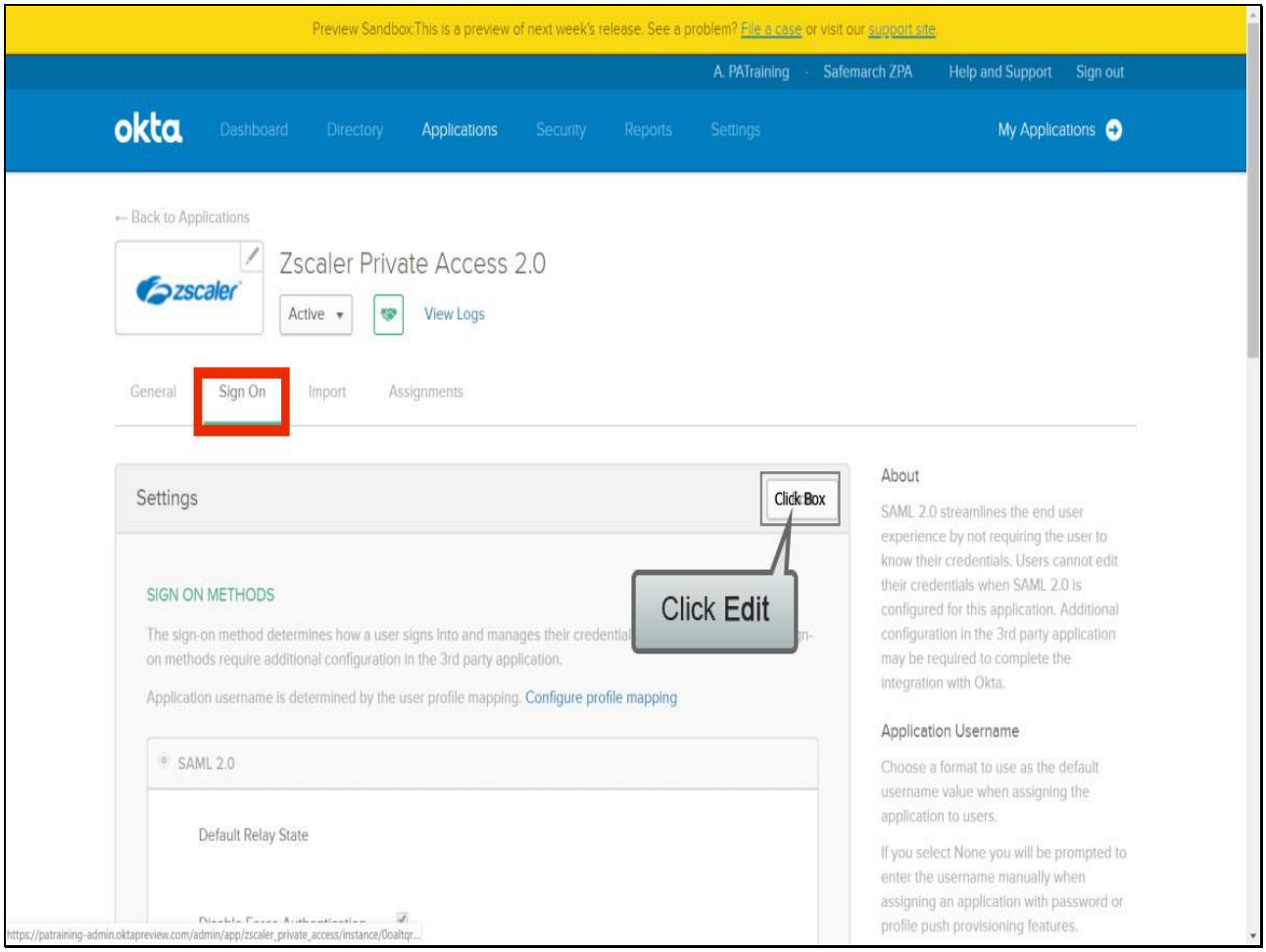
Slide 74 - Slide 74



Slide notes

On the **Assignments** page, assign the app to the users that require to authenticate to ZPA, either individually or by groups. Then go to the **Sign On** page, ...

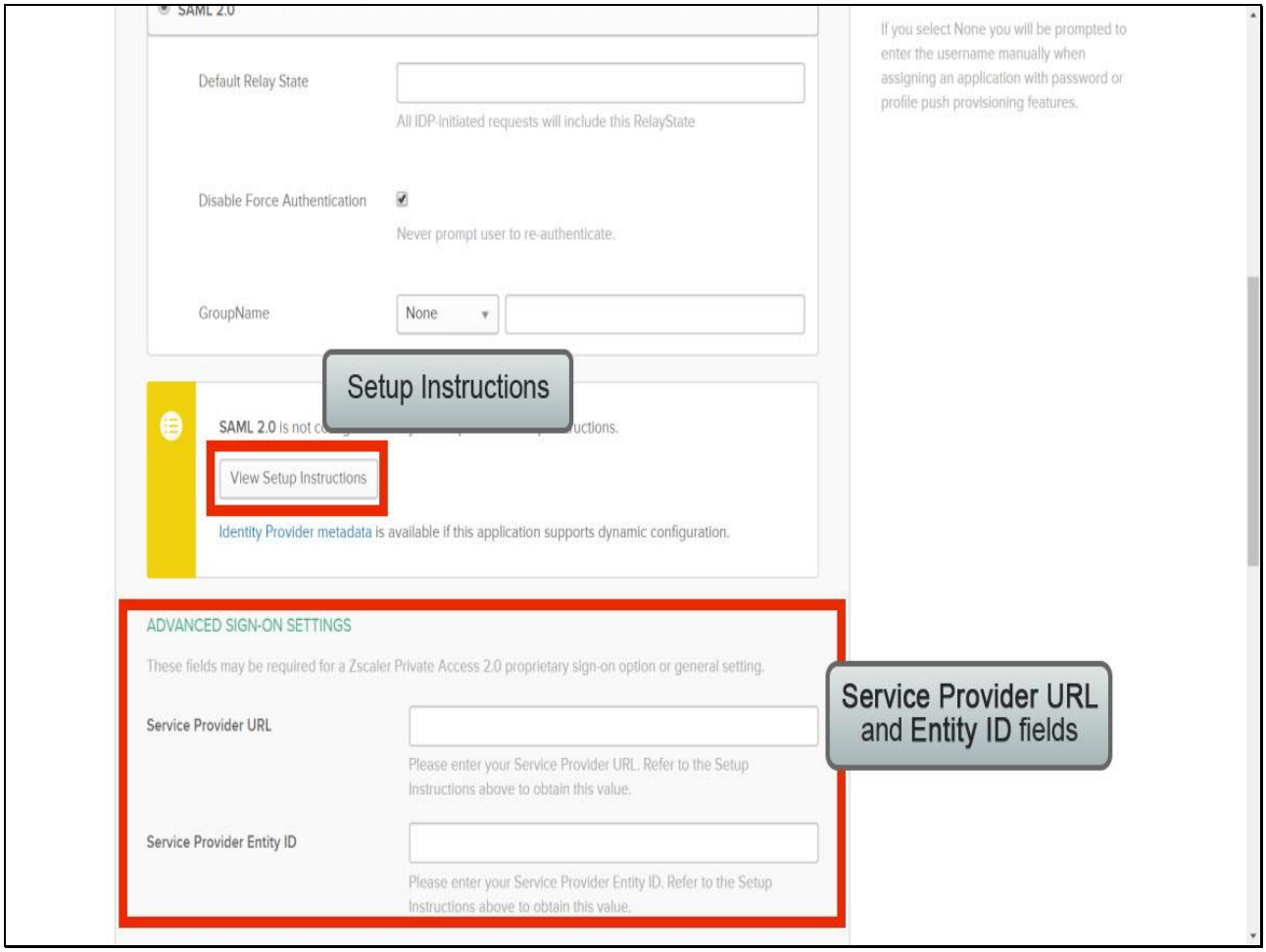
Slide 75 - Slide 75



Slide notes

...click to **Edit** the Settings and scroll down, ...

Slide 76 - Slide 76

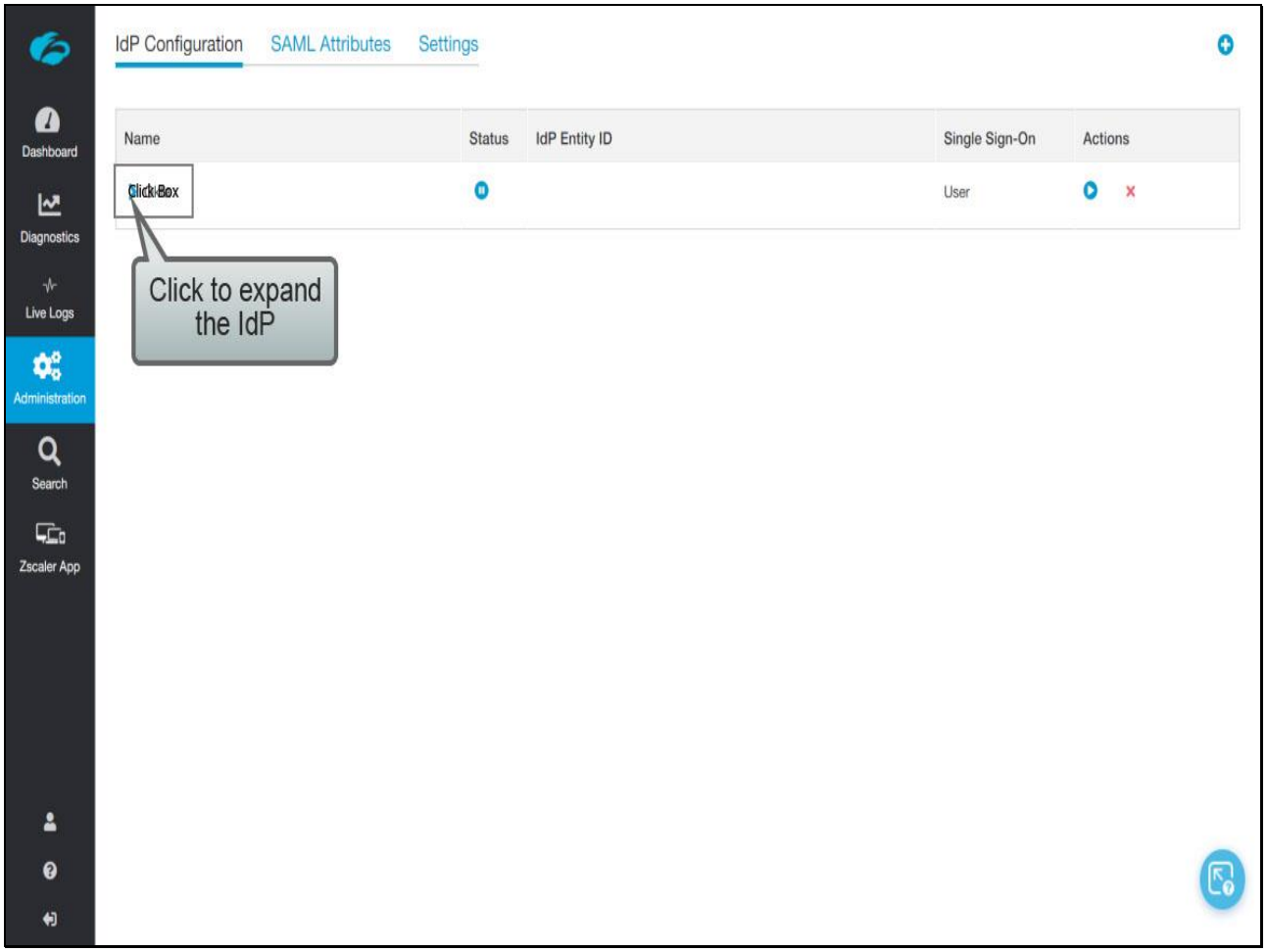


Slide notes

...to the **ADVANCED SIGN-ON SETTINGS** section. A link is provided to a **Setup Instructions** page (opens in a new Tab), with full instructions for the integration with Zscaler.

With Okta, there is no option to import the SP metadata, so you will need to copy/paste the required data from the ZPA Admin Portal.

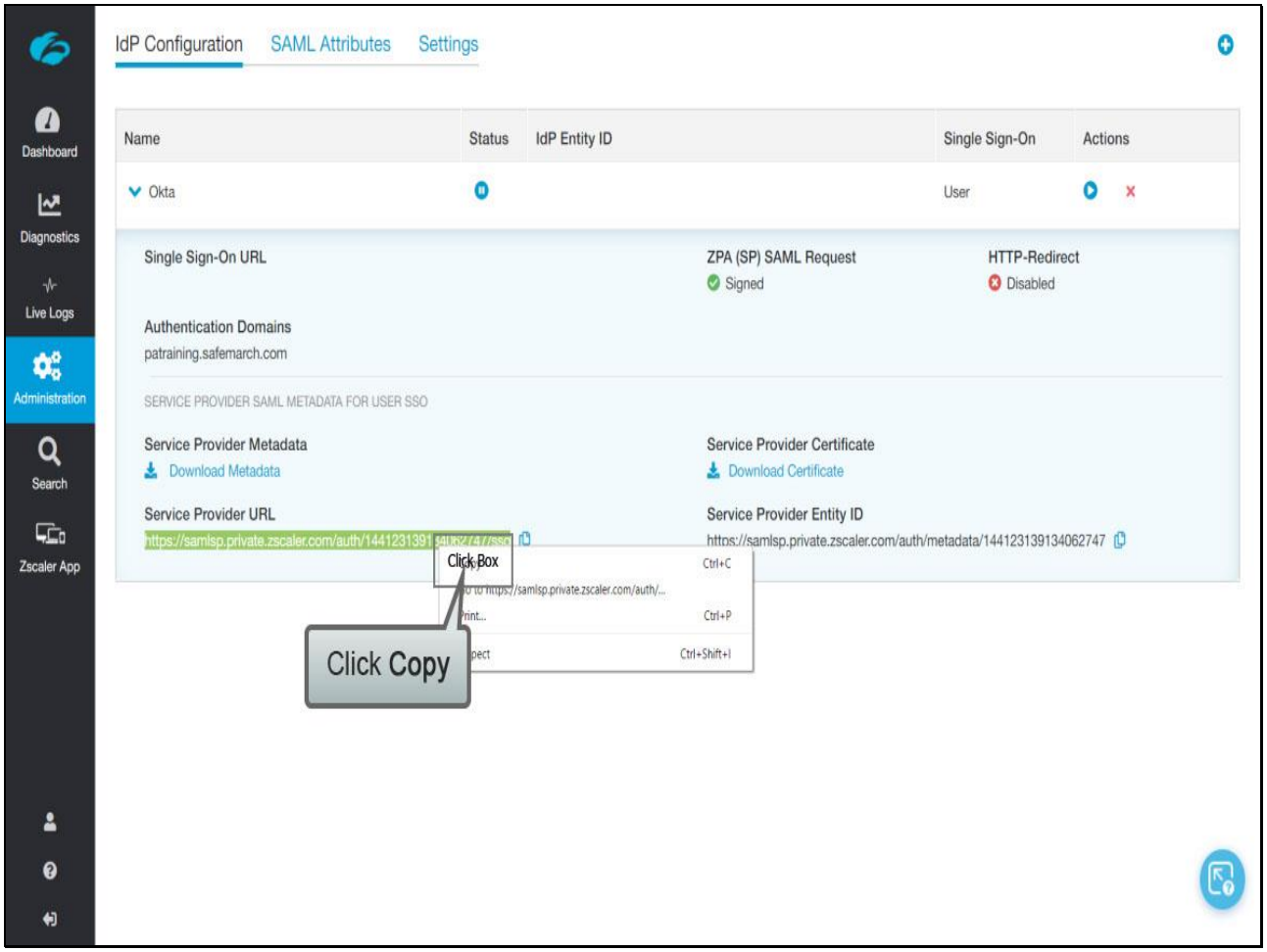
Slide 77 - Slide 77



Slide notes

Back on the ZPA Admin Portal, click to expand the paused IdP configuration that you saved previously, ...

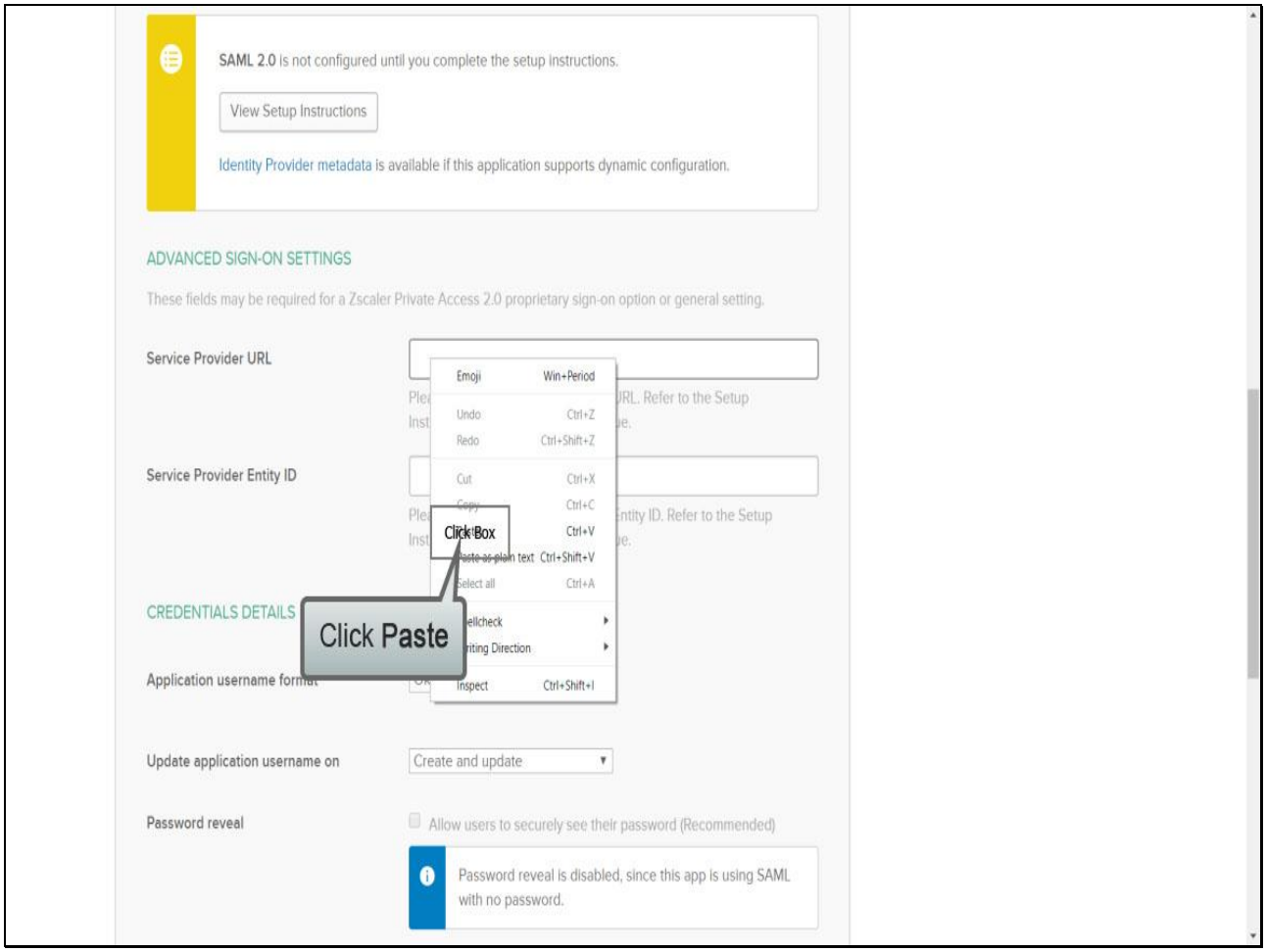
Slide 78 - Slide 78



Slide notes

...highlight the **Service Provider URL**, right-click and select **Copy**, ...

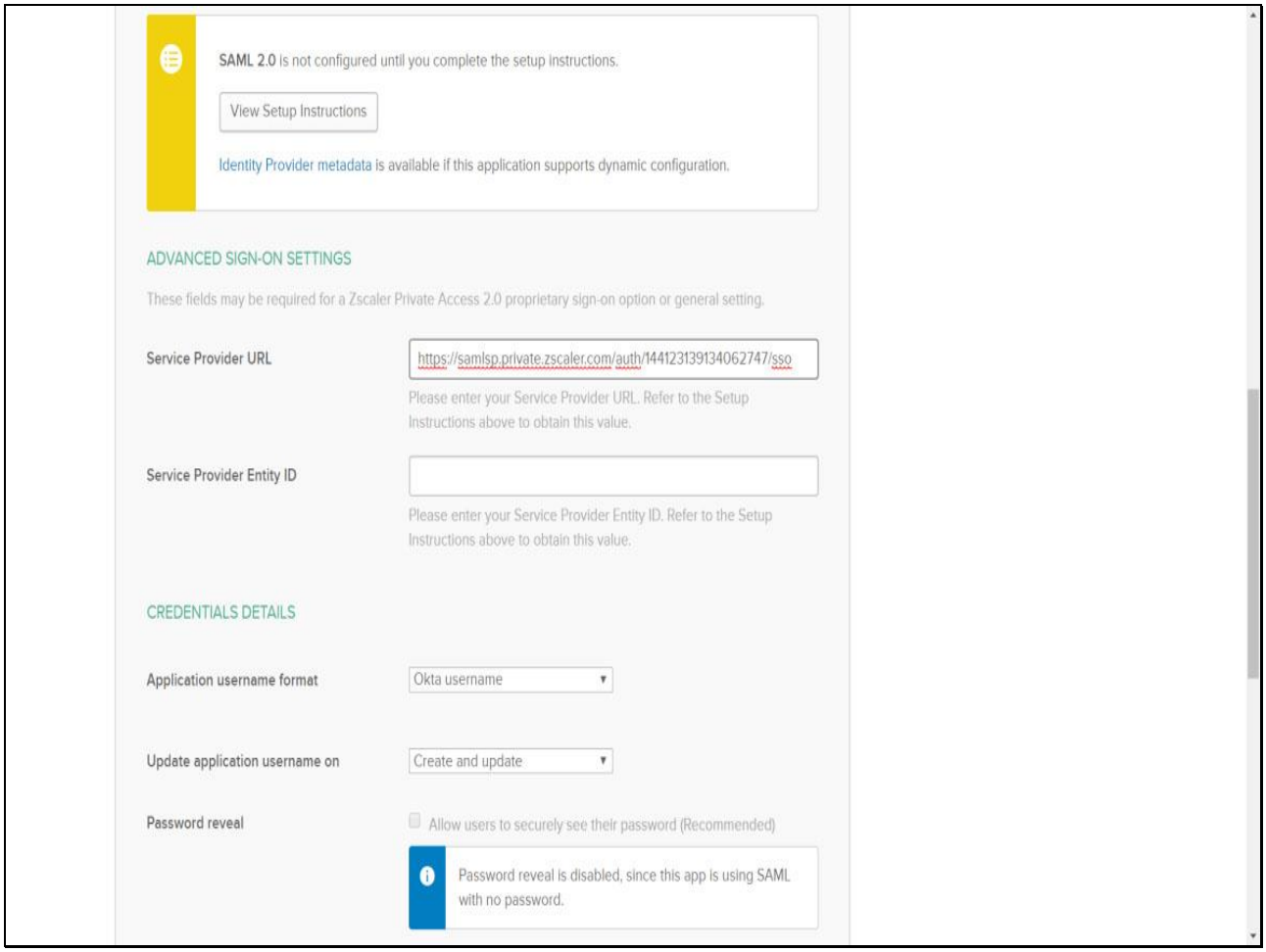
Slide 79 - Slide 79



Slide notes

...switch back to the Okta Admin Portal and **Paste** the value into the **Service Provider URL** field.

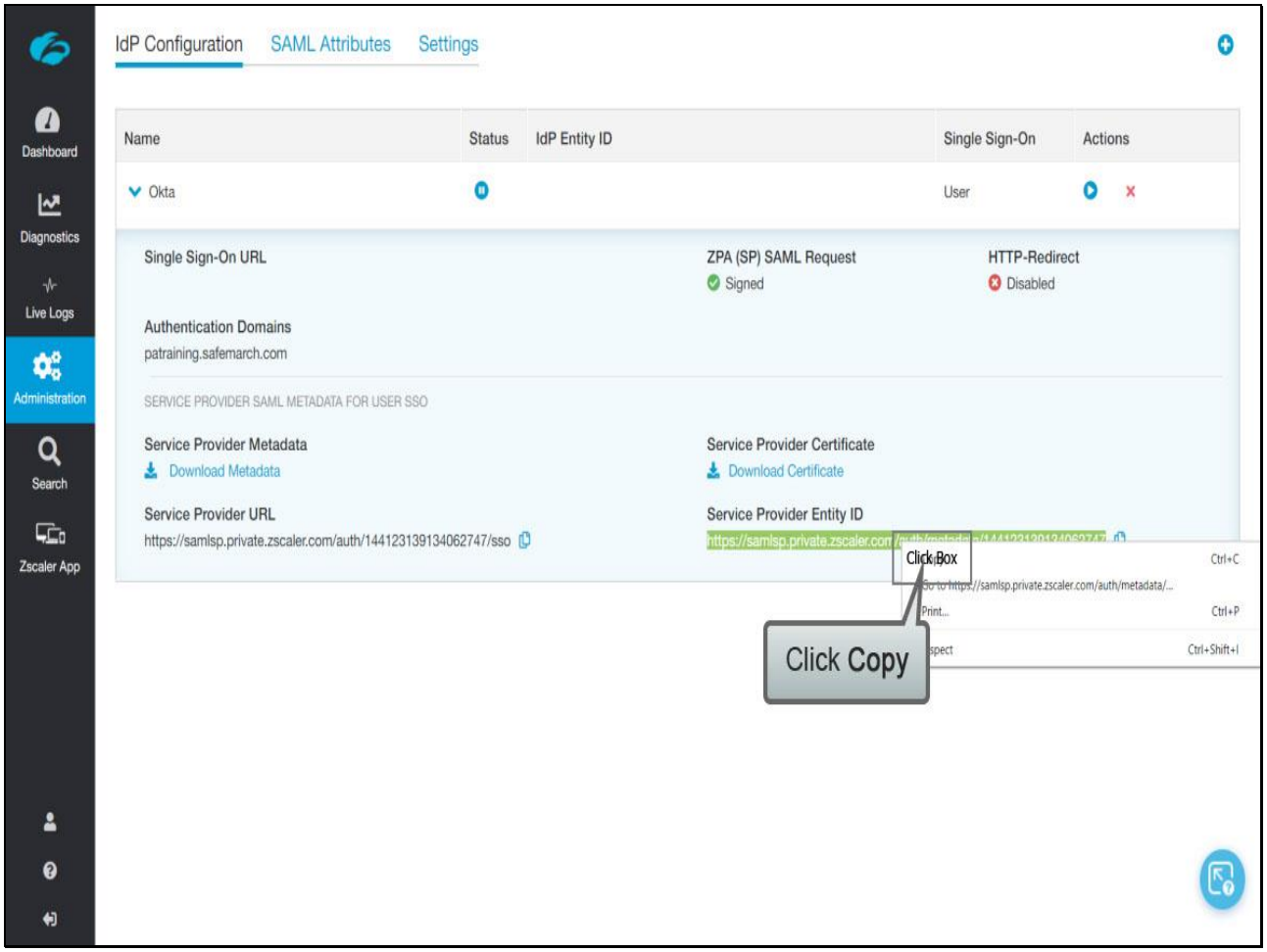
Slide 80 - Slide 80



Slide notes

Switch back to the ZPA Admin Portal, ...

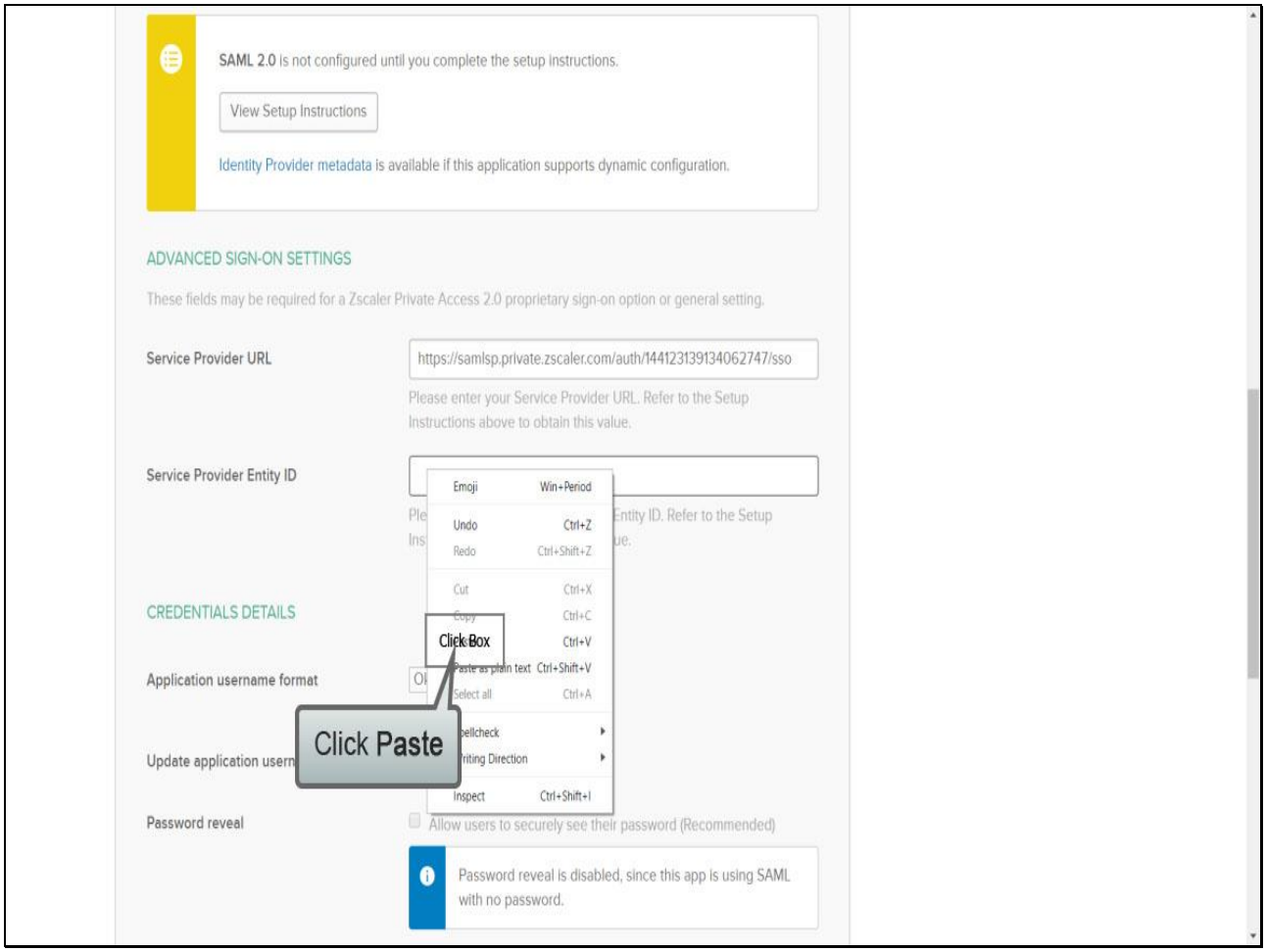
Slide 81 - Slide 81



Slide notes

...highlight and **Copy** the **Service Provider Entity ID** value, ...

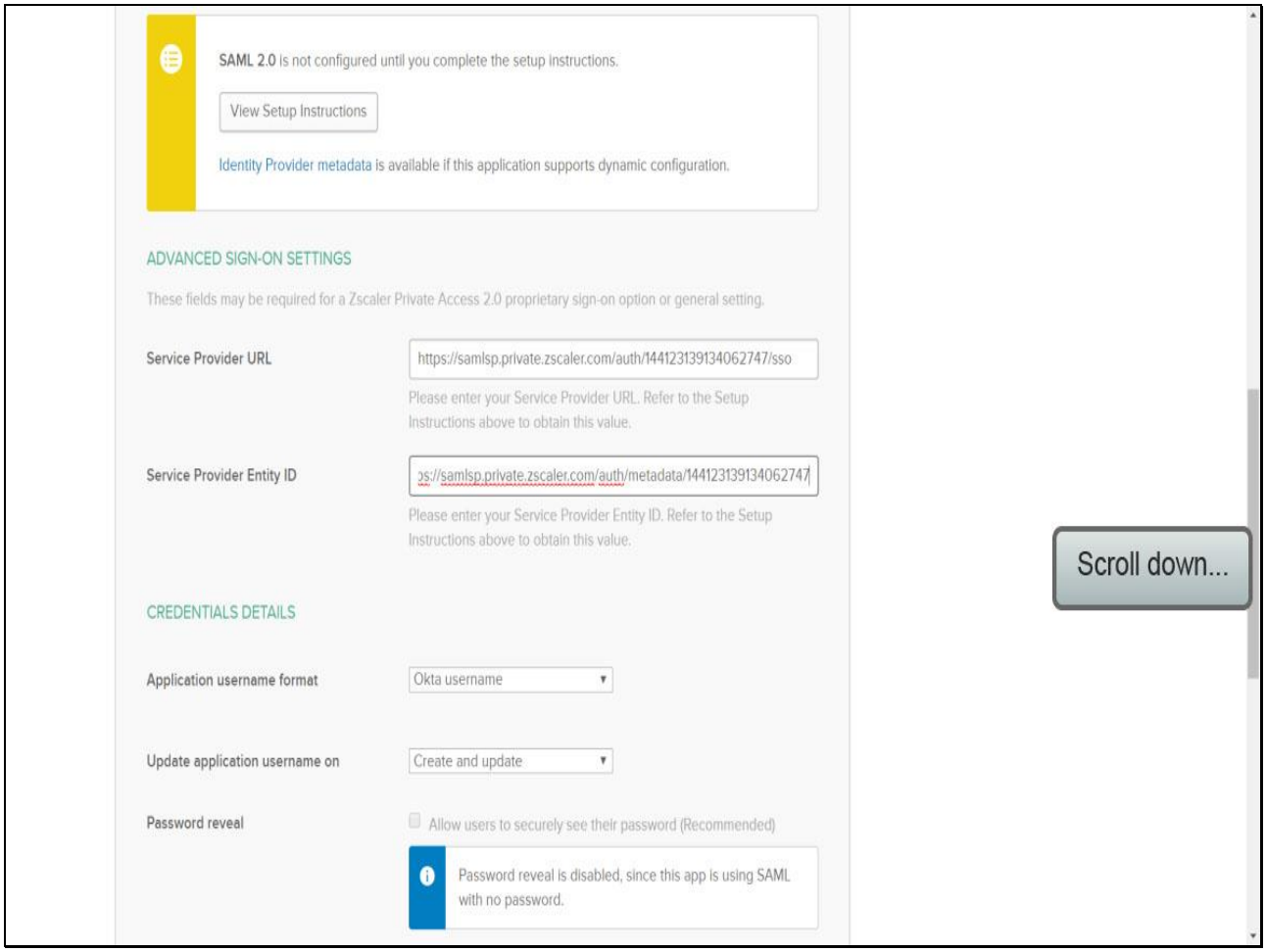
Slide 82 - Slide 82



Slide notes

...then back on the Okta Admin Portal, **Paste** that data into the **Service Provider Entity ID** field.

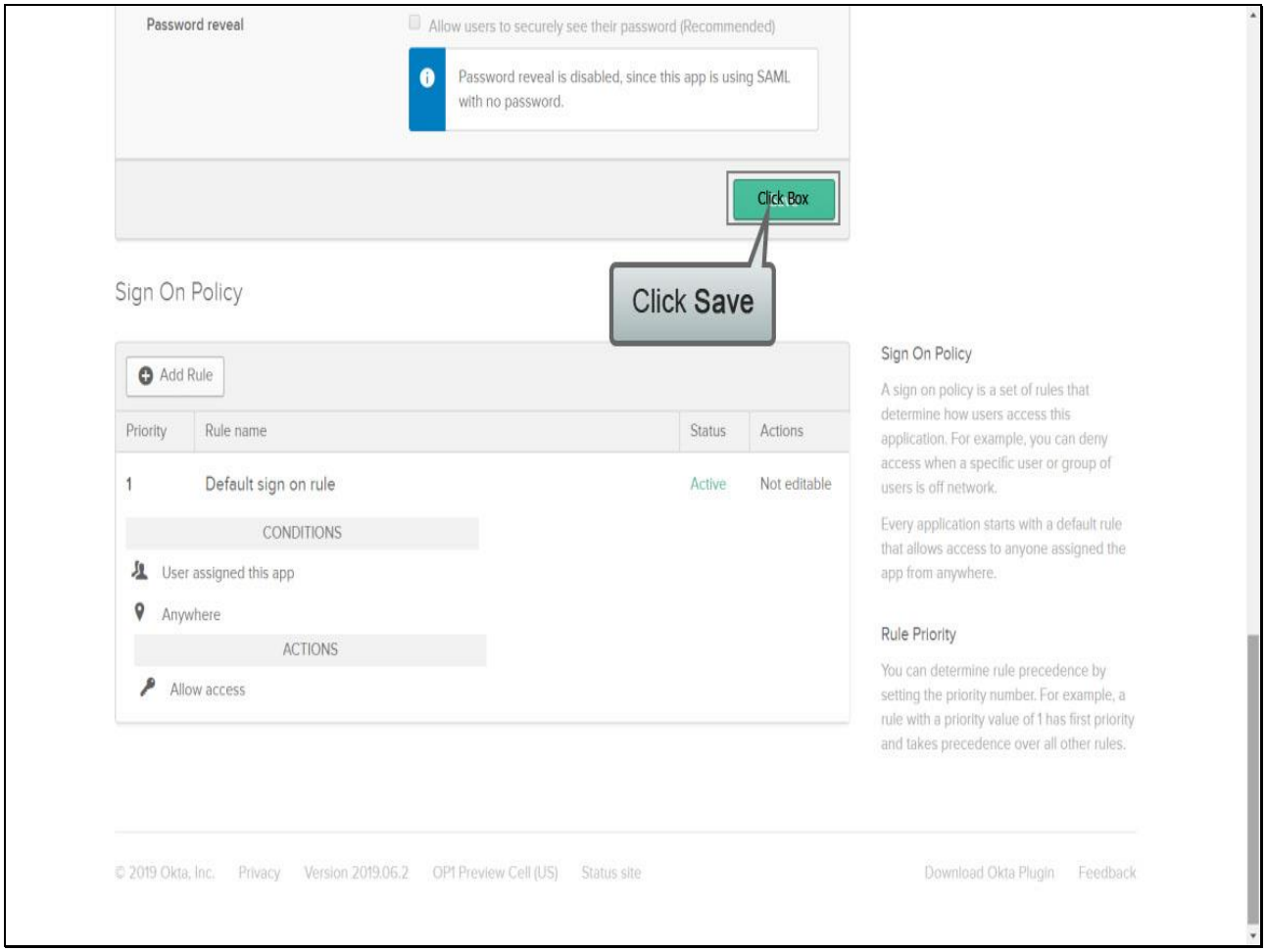
Slide 83 - Slide 83



Slide notes

Scroll down if necessary, ...

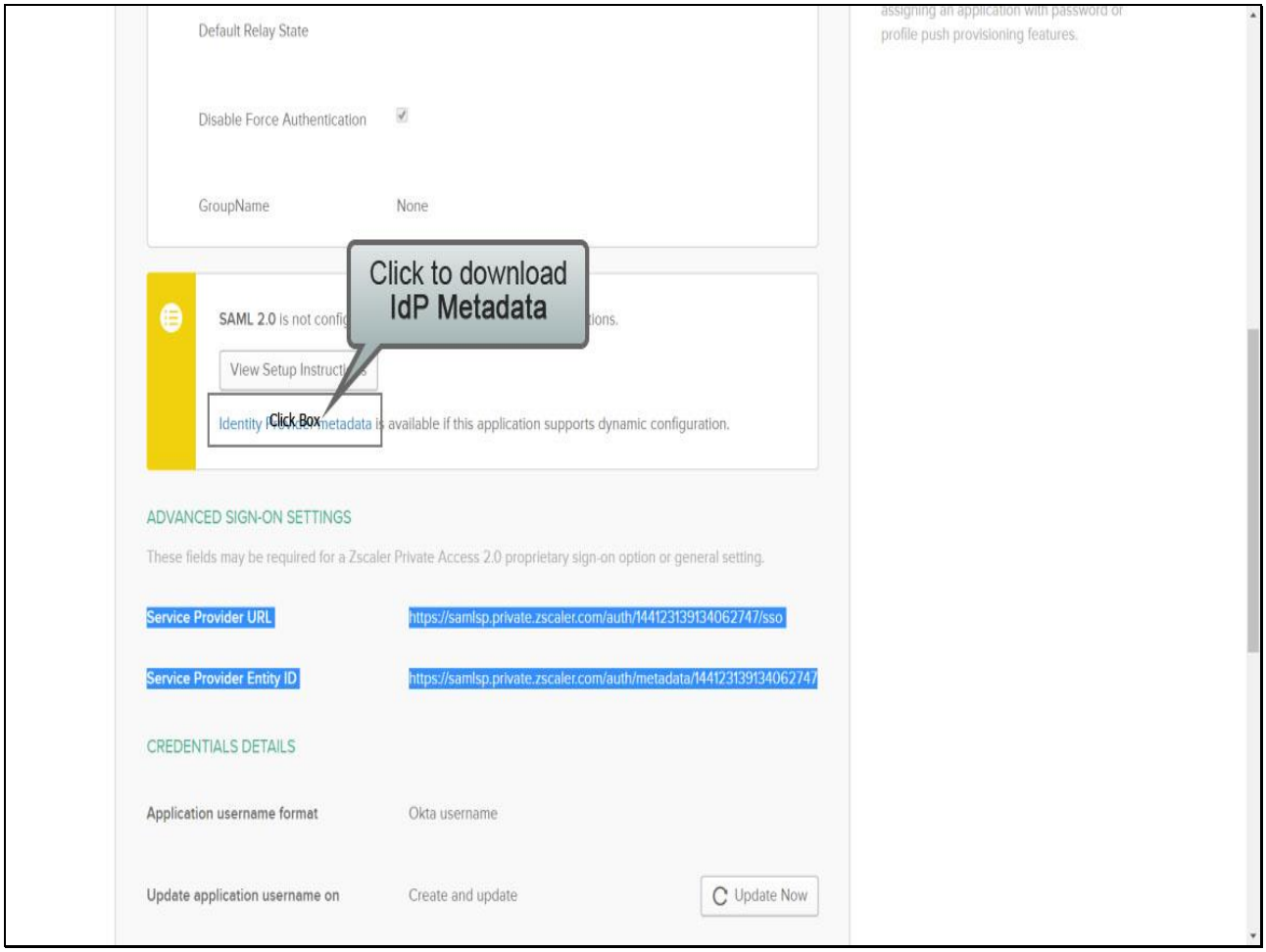
Slide 84 - Slide 84



Slide notes

...and click to **Save** the SP configuration.

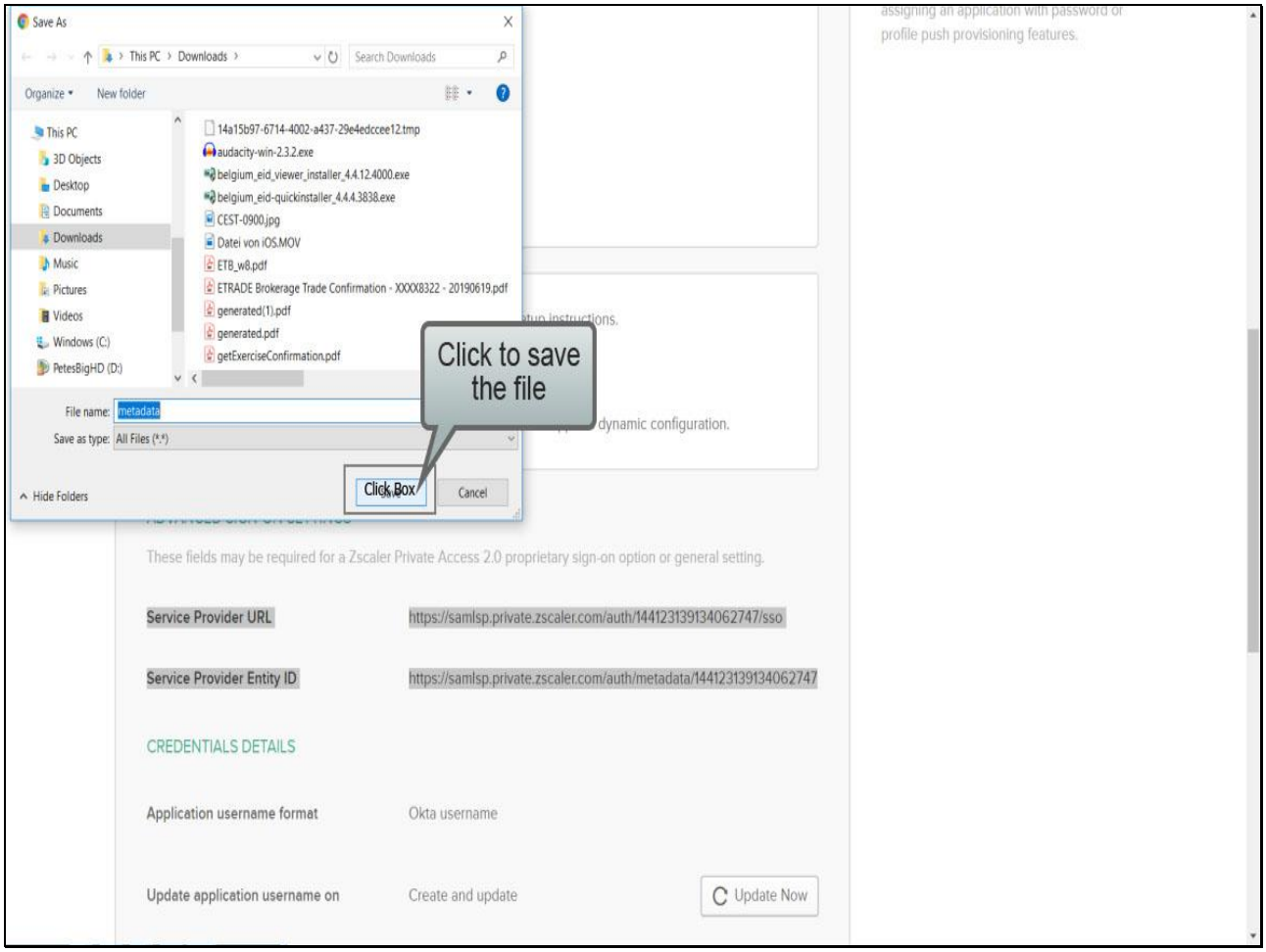
Slide 85 - Slide 85



Slide notes

Okta provide a link on this page to download the **Identity Provider metadata**, which you will need to finalize the configuration at the ZPA Admin Portal, so click the link, ...

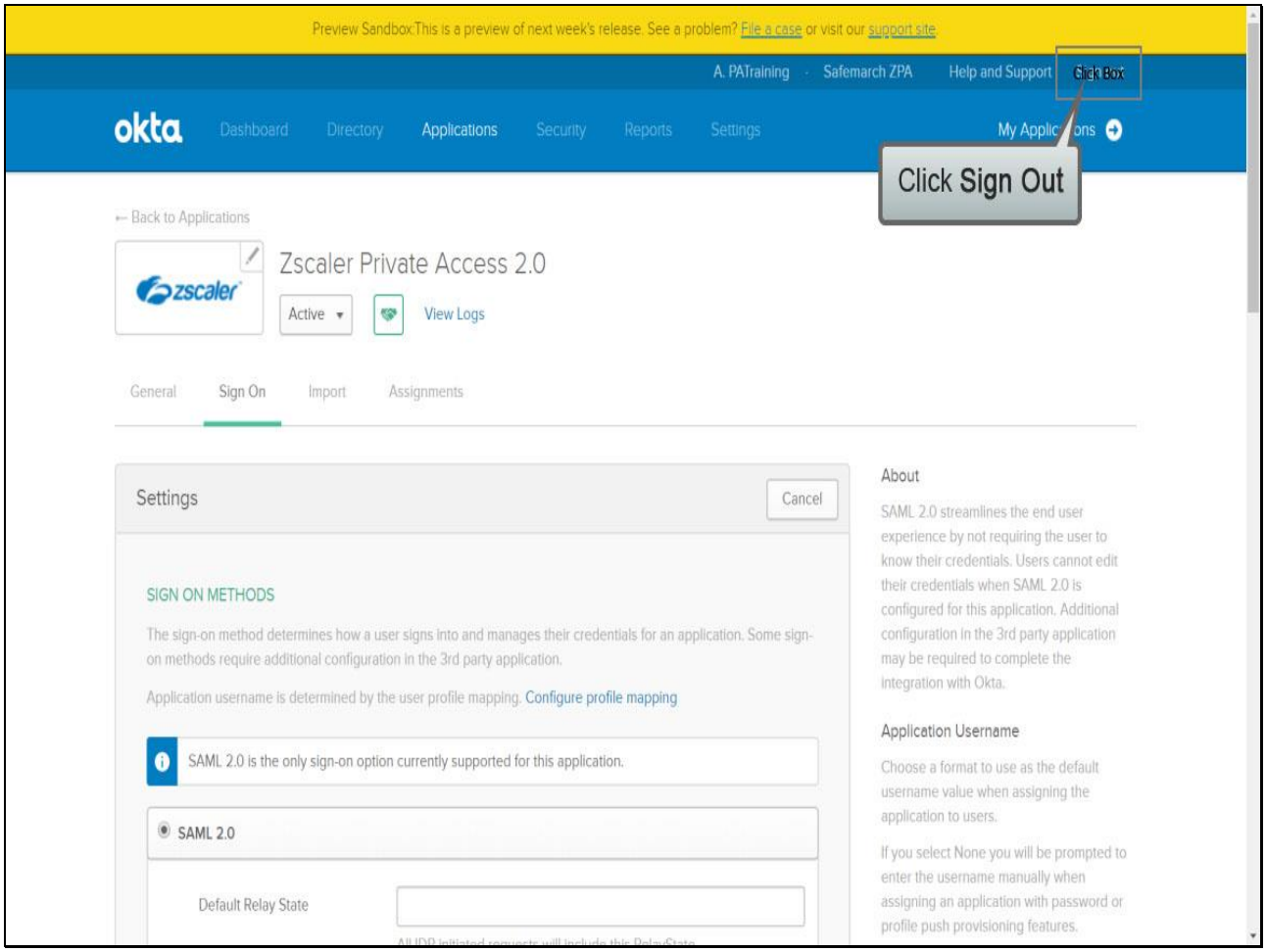
Slide 86 - Slide 86



Slide notes

...and **Save** the file to a suitable folder or share.

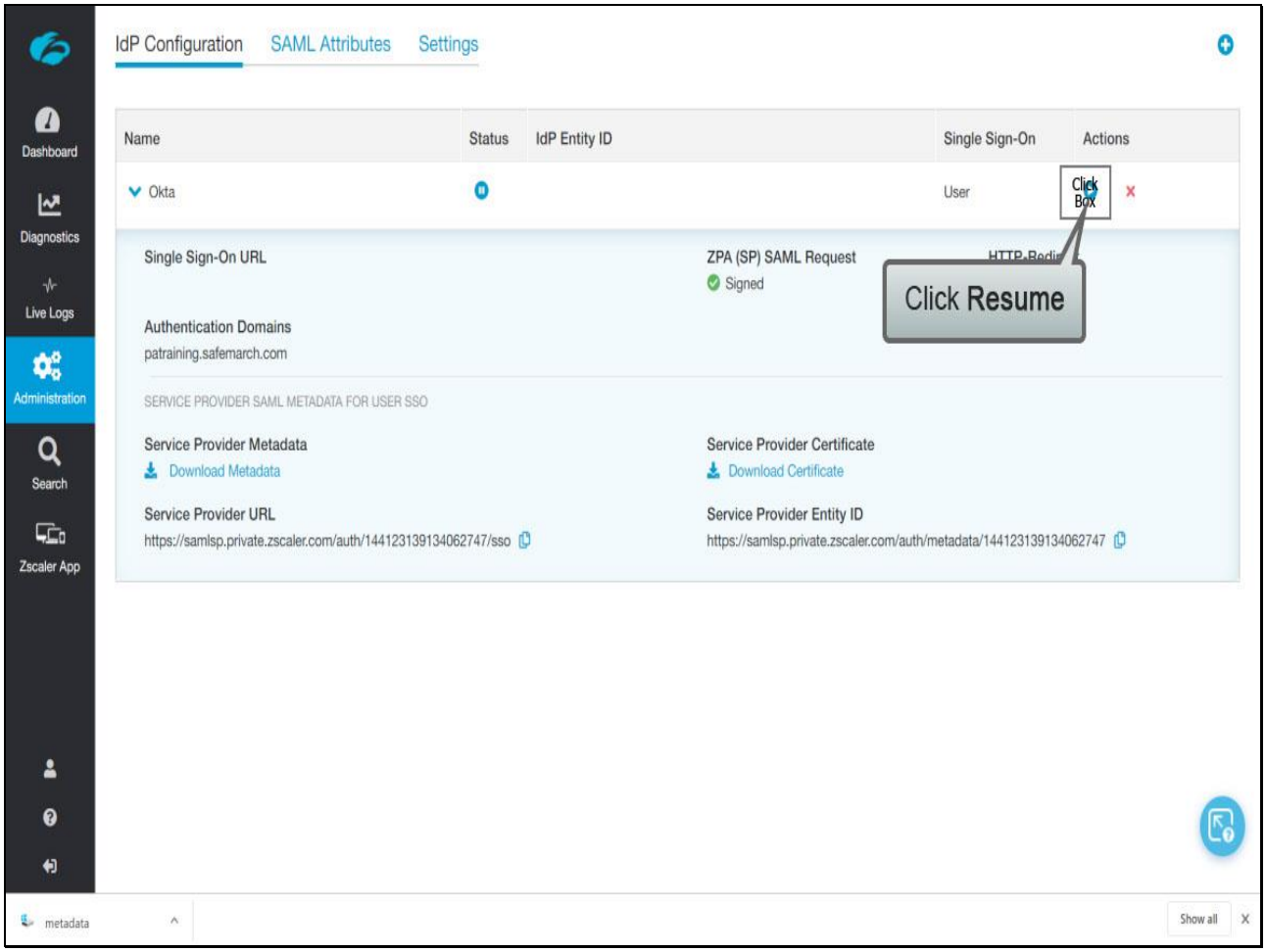
Slide 87 - Slide 87



Slide notes

Lastly, you need to sign out of the Okta Admin Portal, so you can test the integration from the Zscaler side. At top right, click **Sign Out**.

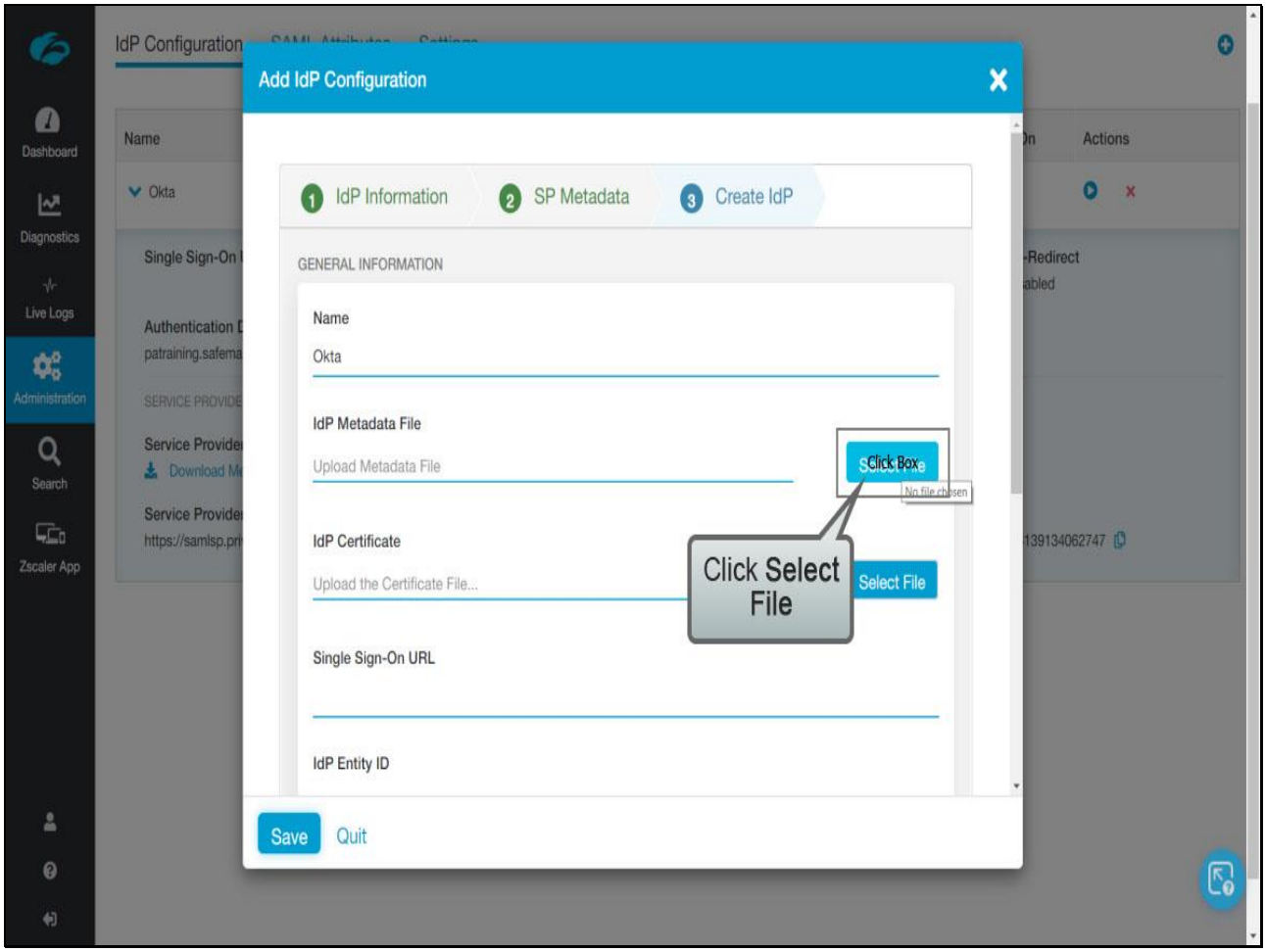
Slide 88 - Slide 88



Slide notes

Back in the ZPA Admin Portal, click to **Resume** configuration of the new IdP, ...

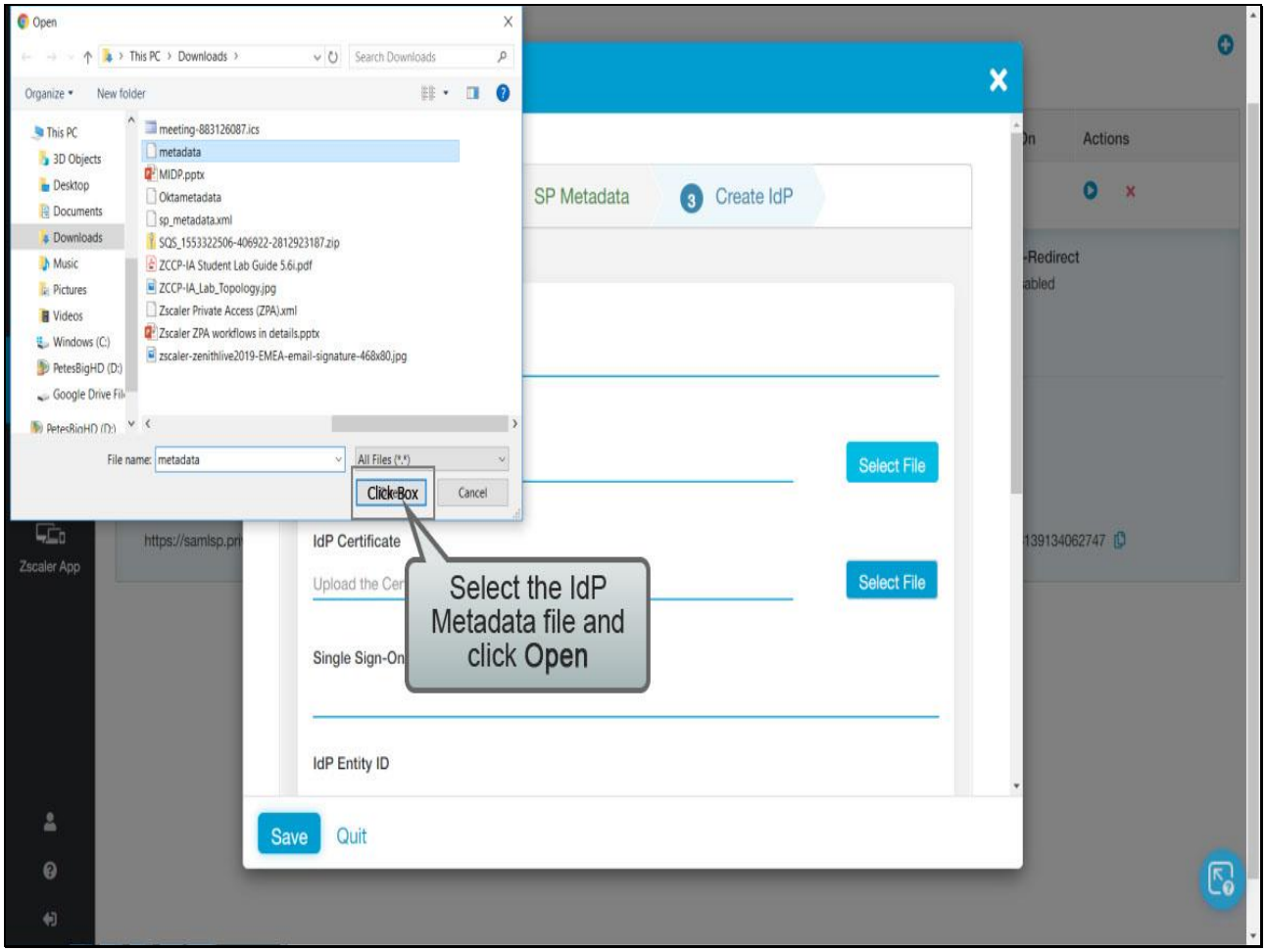
Slide 89 - Slide 89



Slide notes

...then click **Select File** to import the IdP metadata that you saved out of the Okta Admin Portal.

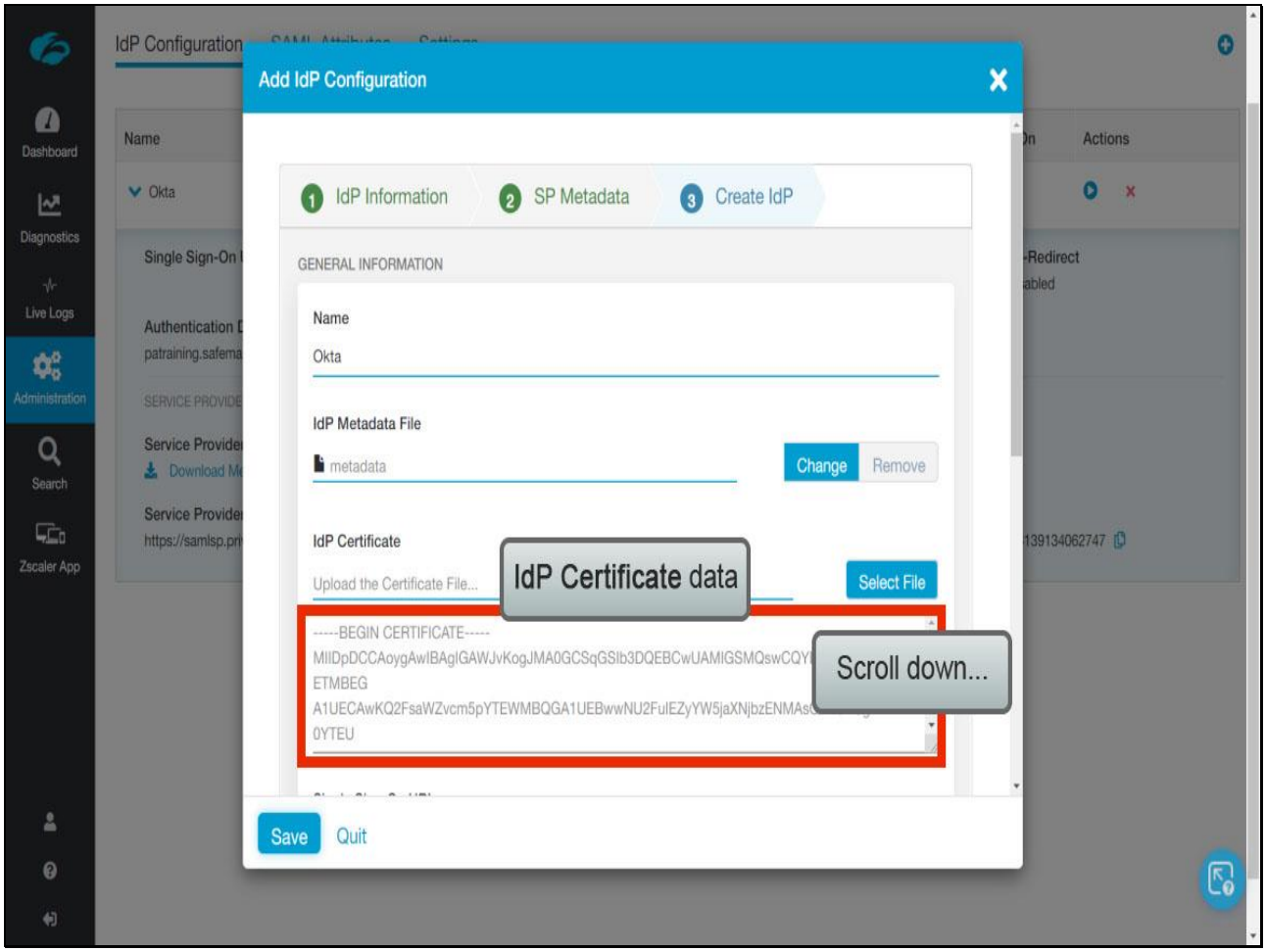
Slide 90 - Slide 90



Slide notes

Locate and select the file, then click **Open**.

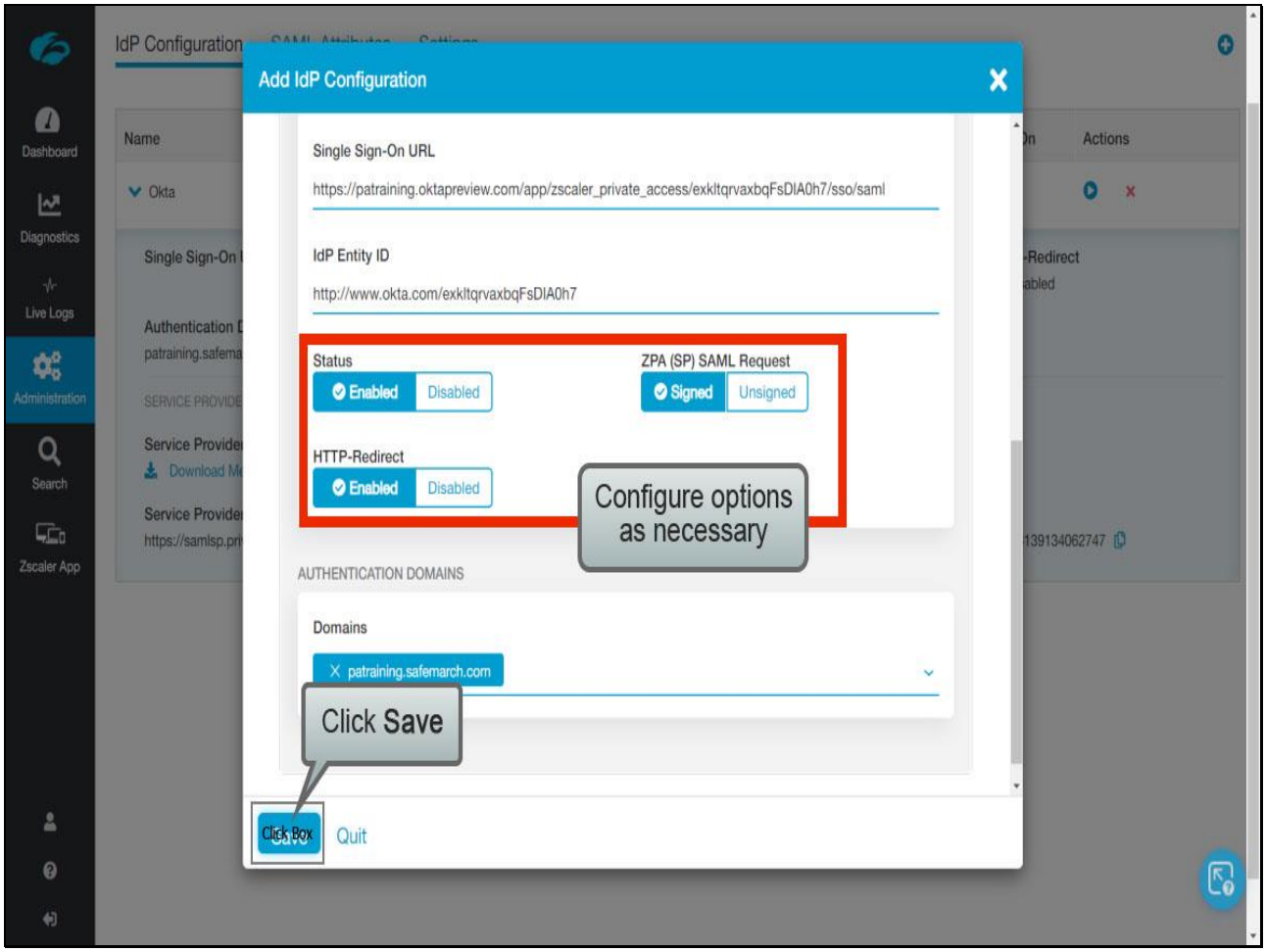
Slide 91 - Slide 91



Slide notes

Verify that the file was imported successfully and that the **IdP Certificate** has been added, then scroll down, ...

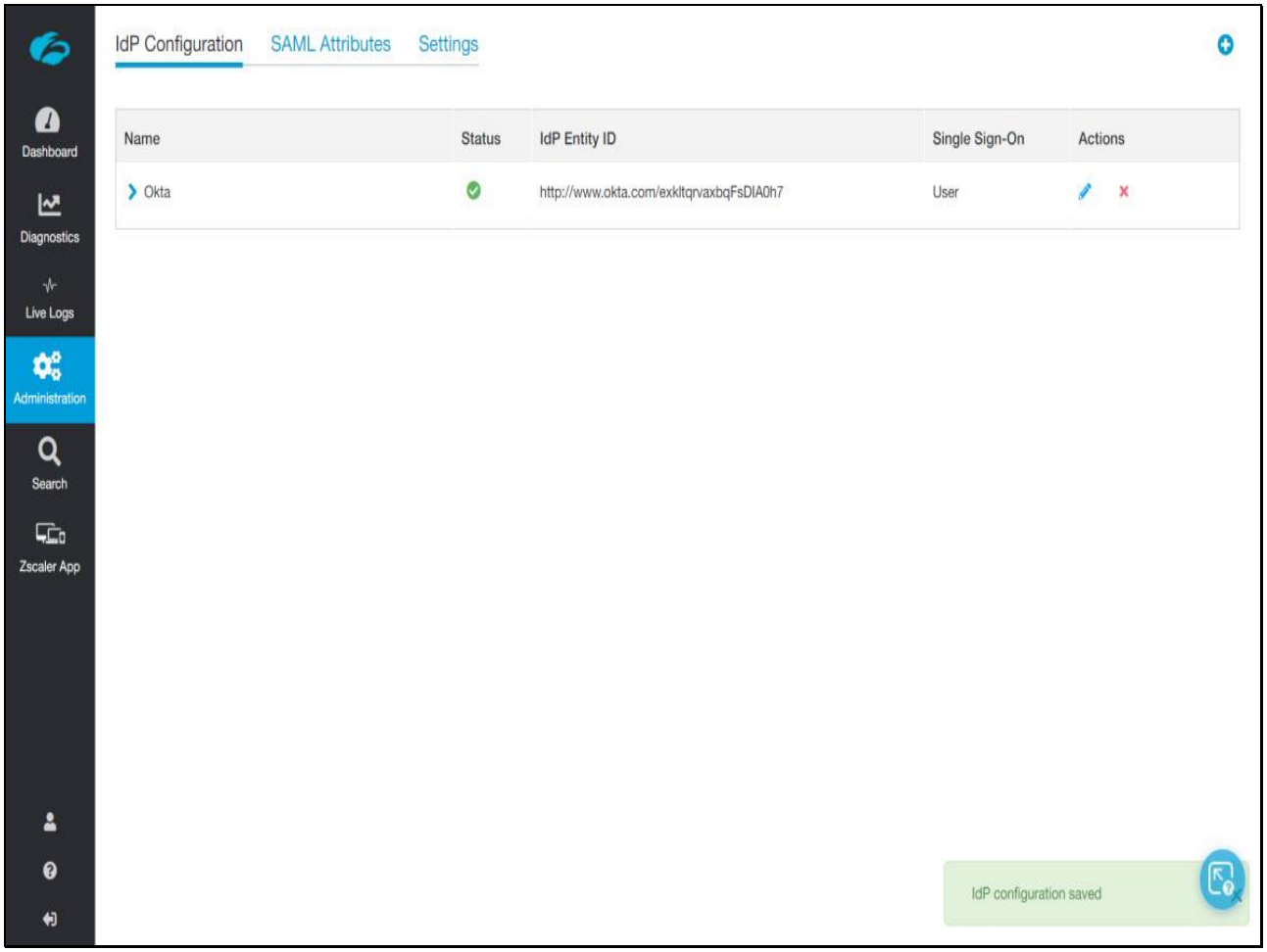
Slide 92 - Slide 92



Slide notes

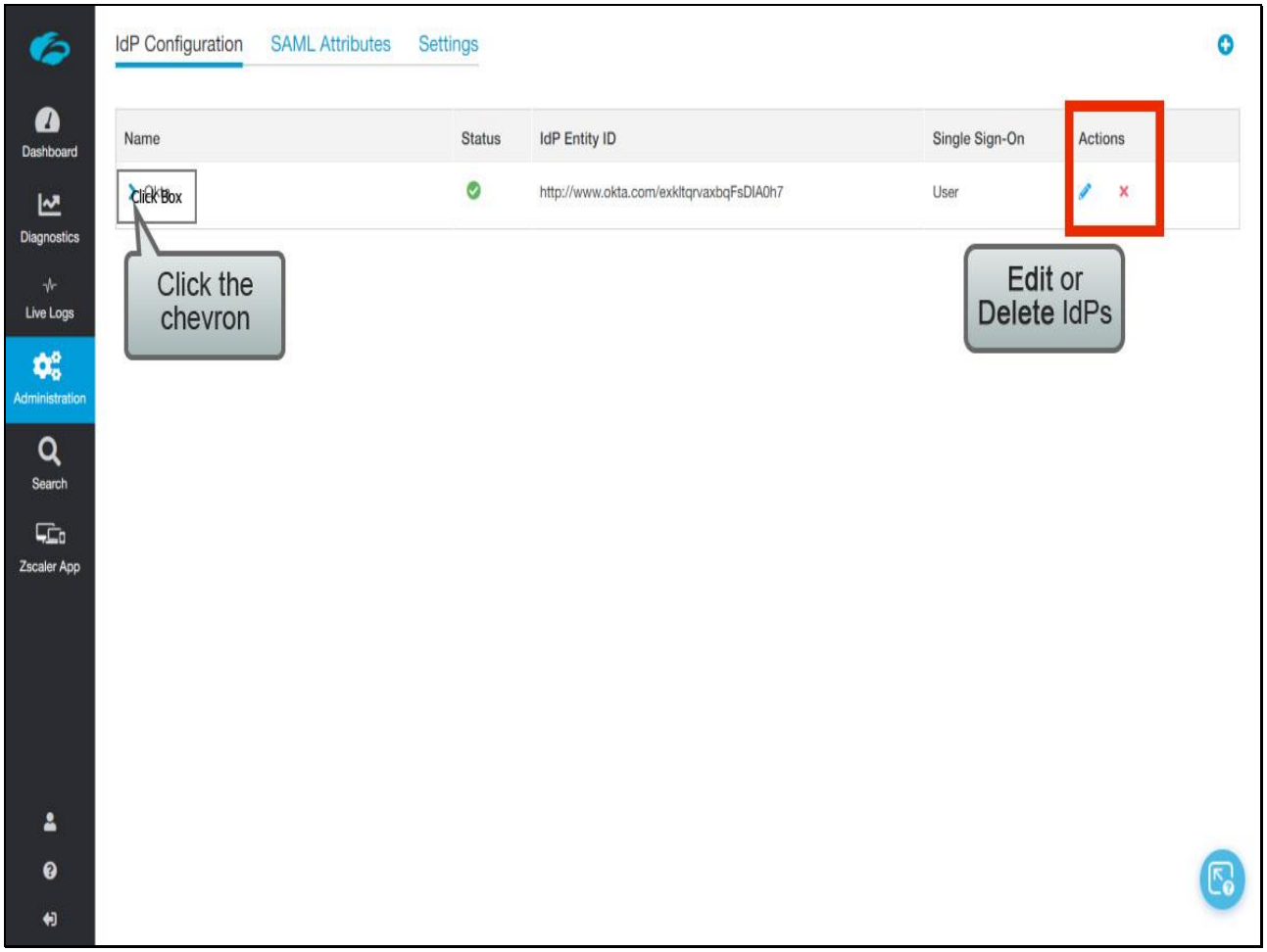
...and configure options as required. Enable the **Signed SAML Request** option if you want to sign the out-going requests to the IdP, the **HTTP-Redirect** option if the IdP requires a HTTP redirect rather than a POST and confirm that the IdP configuration is **Enabled**. Check that the associated Domains are correct and click **Save**.

Slide 93 - Slide 93



Slide notes

Slide 94 - Slide 94

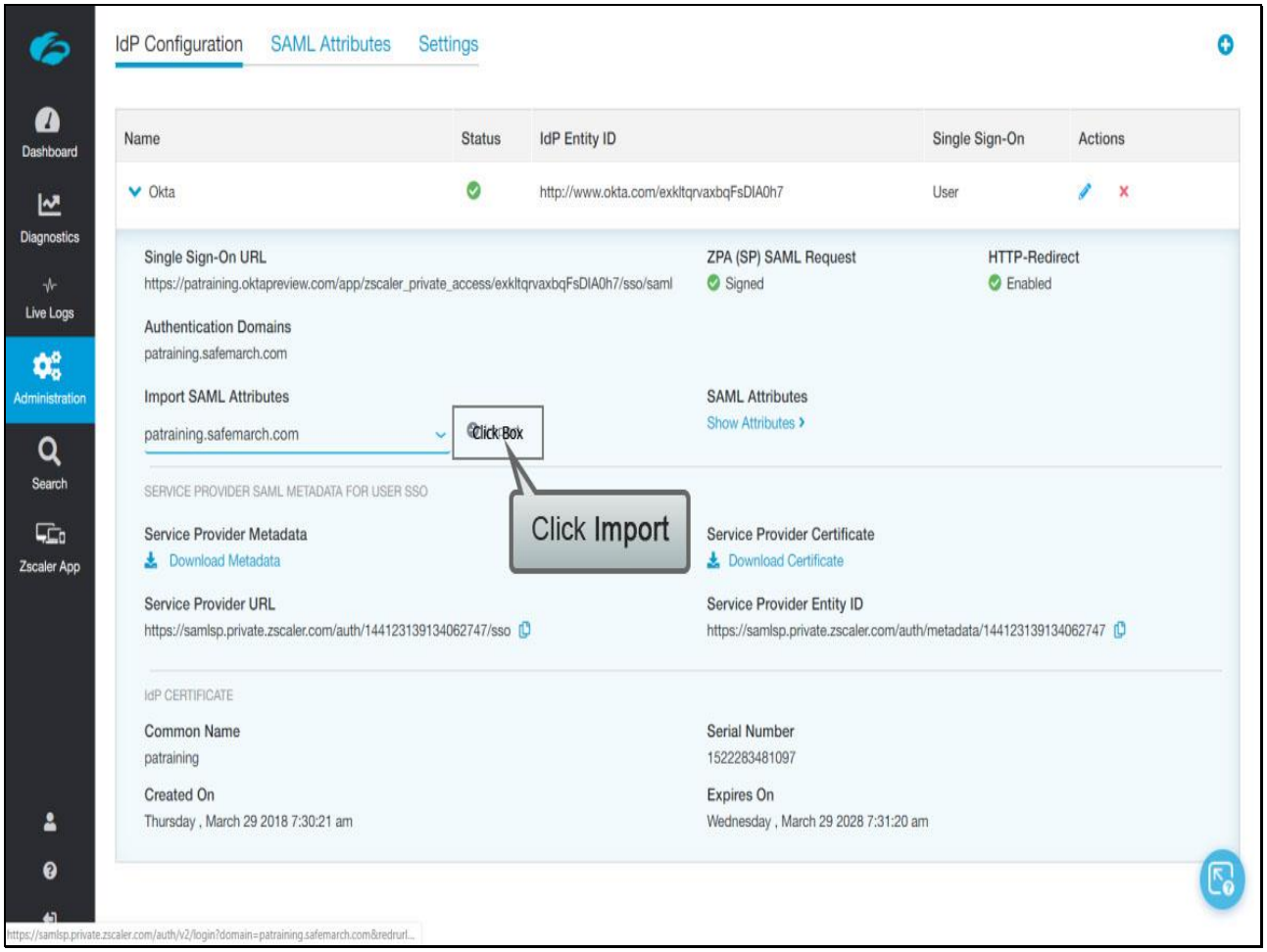


Slide notes

Multiple IdPs may be added for user authentication (as long as additional authentication domains have been defined), and for administrator SSO if it is to be used. On this page, you can of course edit, or delete the listed IdPs.

To view details for the IdP, click on the chevron next to the name.

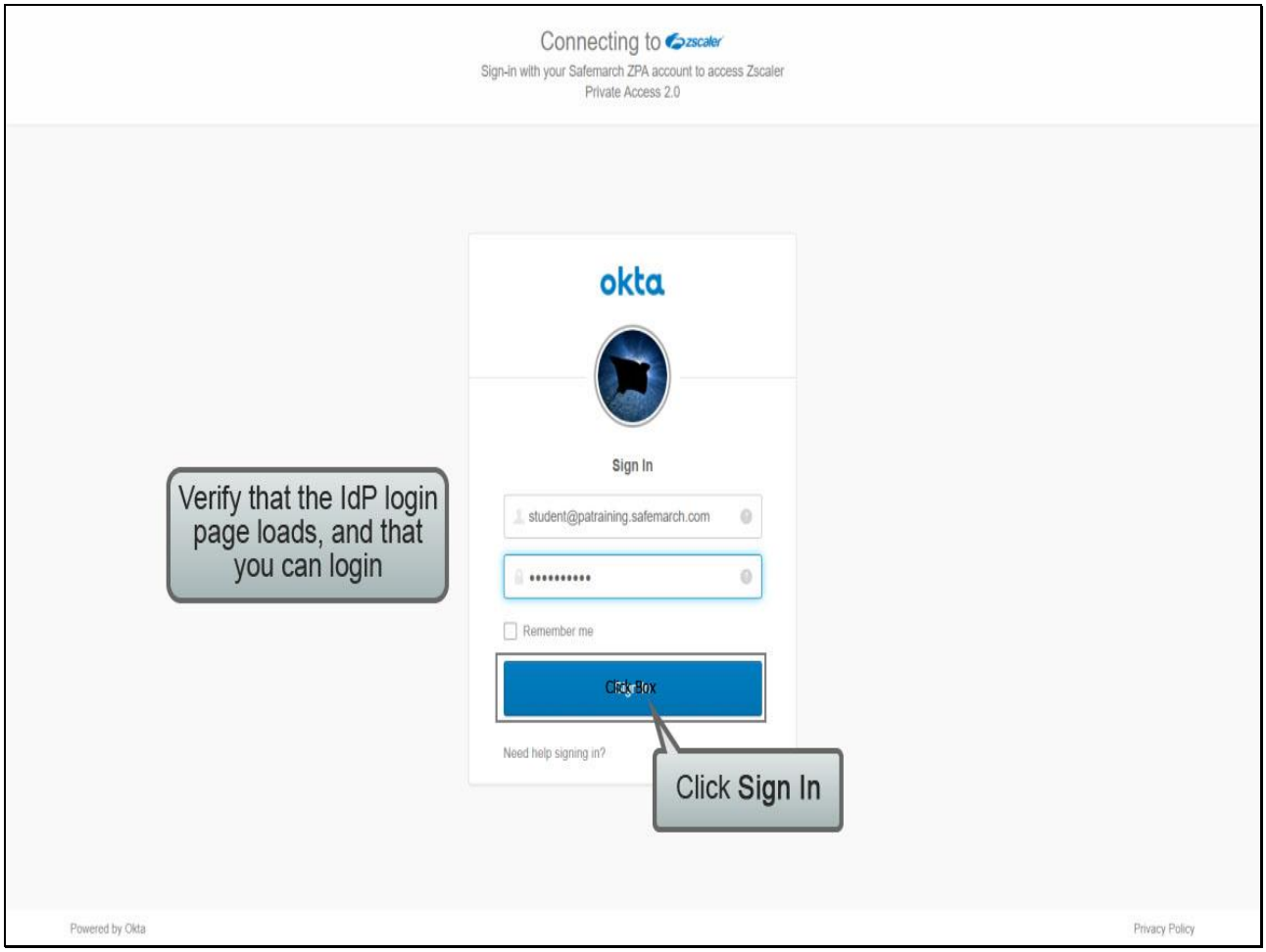
Slide 95 - Slide 95



Slide notes

To test the IdP configuration and import the SAML attributes supplied by it on a successful authentication, click **Import**, …

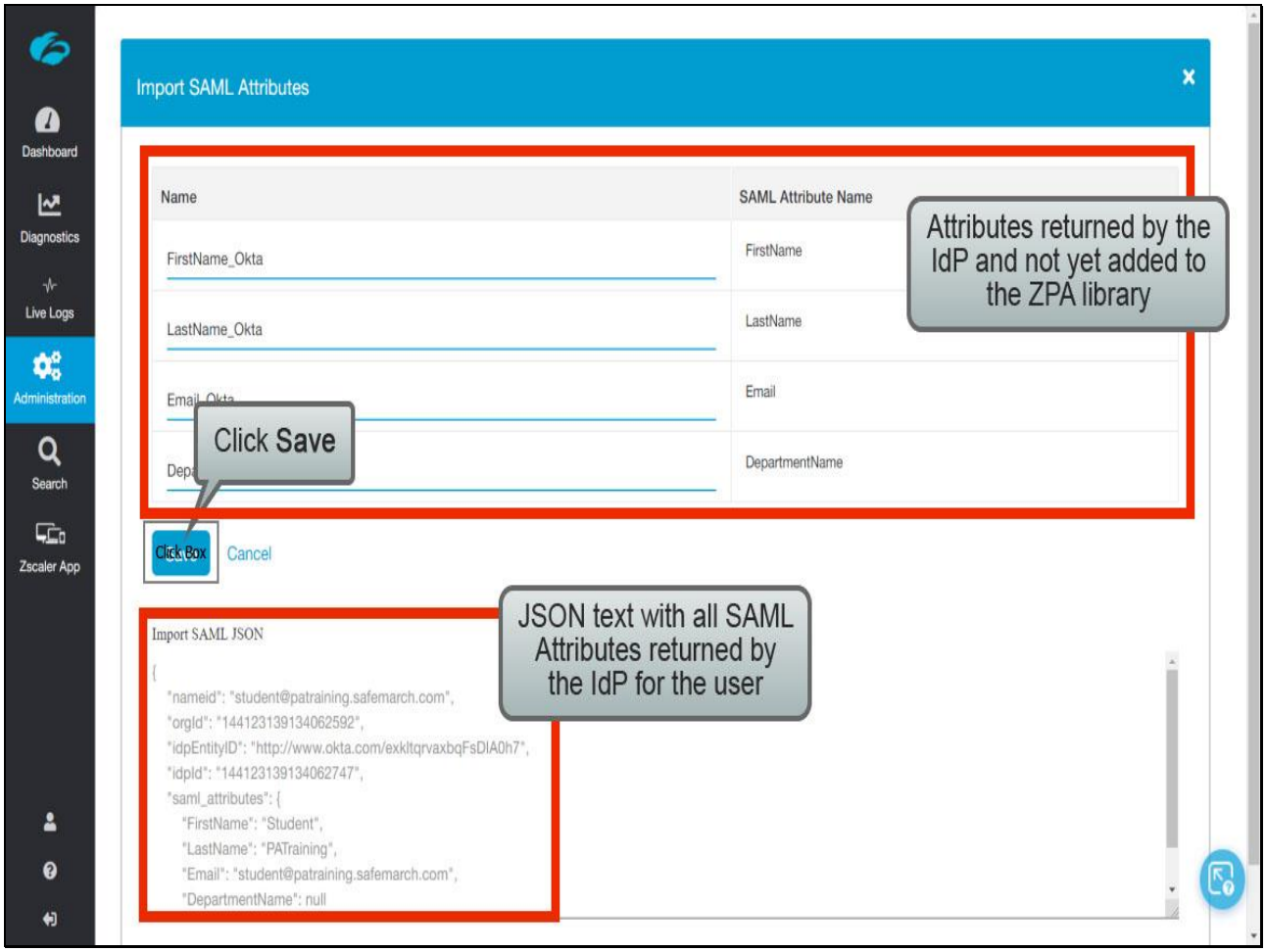
Slide 96 - Slide 96



Slide notes

…verify that the login page for the IdP Portal is loaded in a new Browser tab, and that you can login with a valid set of user credentials.

Slide 97 - Slide 97



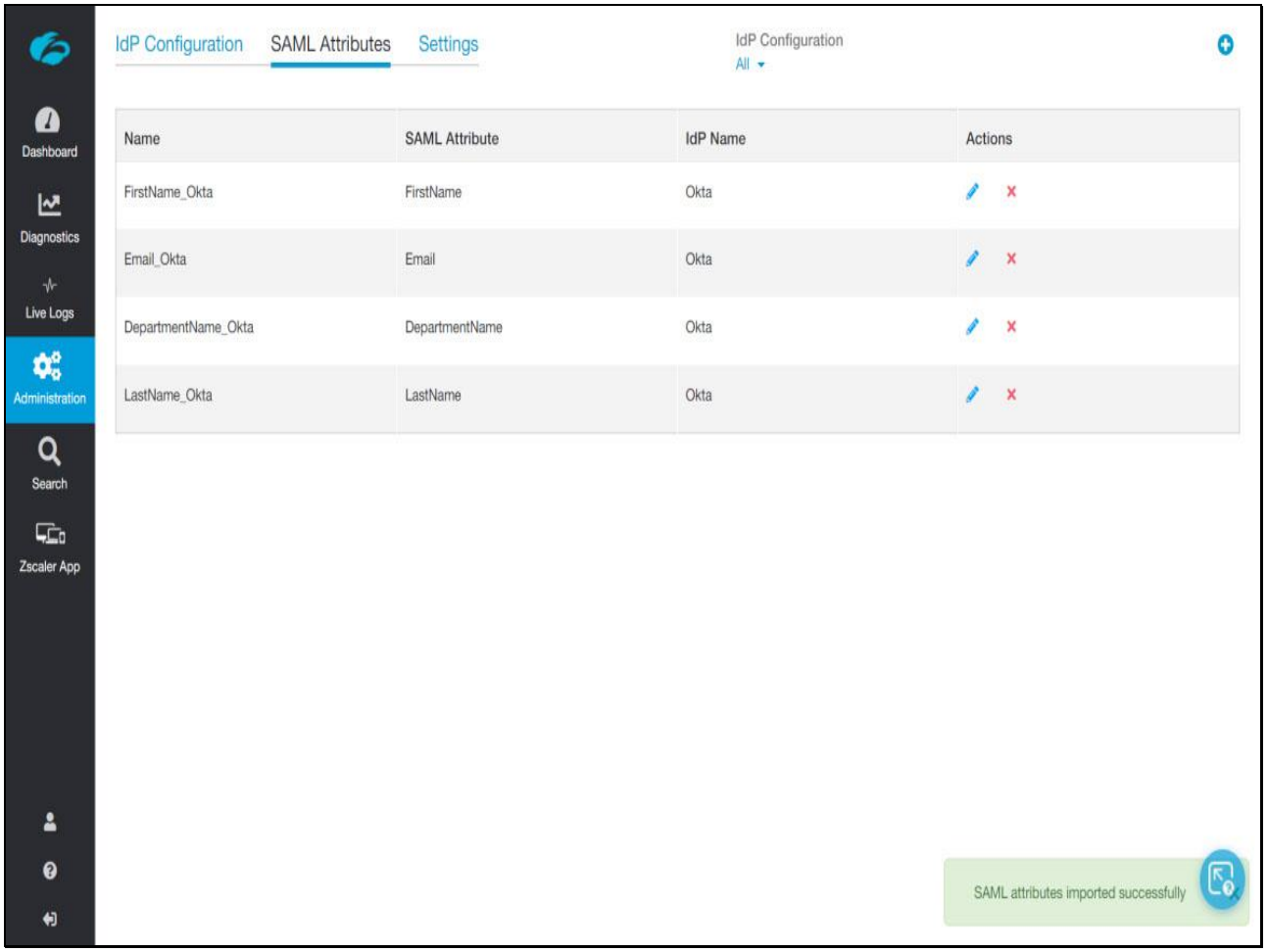
Slide notes

Once logged in, your screen displays a JSON text string similar to the example shown here. This text string includes all the SAML attributes returned for that user.

SAML attributes not already saved to the **SAML Attributes** library will be listed here. Note that if SAML attributes are present in the JSON text string but not listed above, that is because they are already defined in the configuration and no additional action is needed in order to use them for policy.

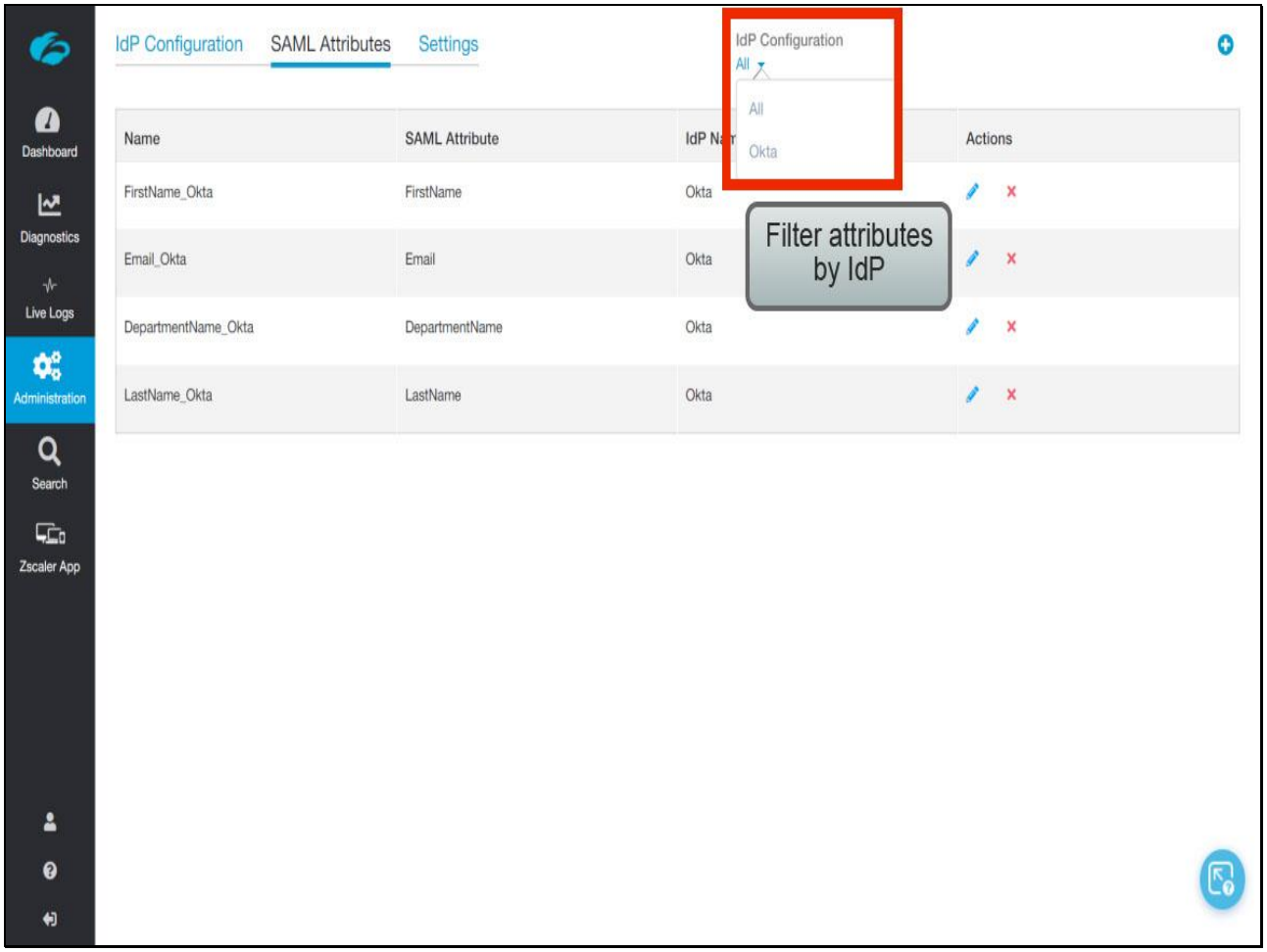
To import these attributes to the ZPA configuration, just click **Save**, …

Slide 98 - Slide 98



Slide notes

Slide 99 - Slide 99

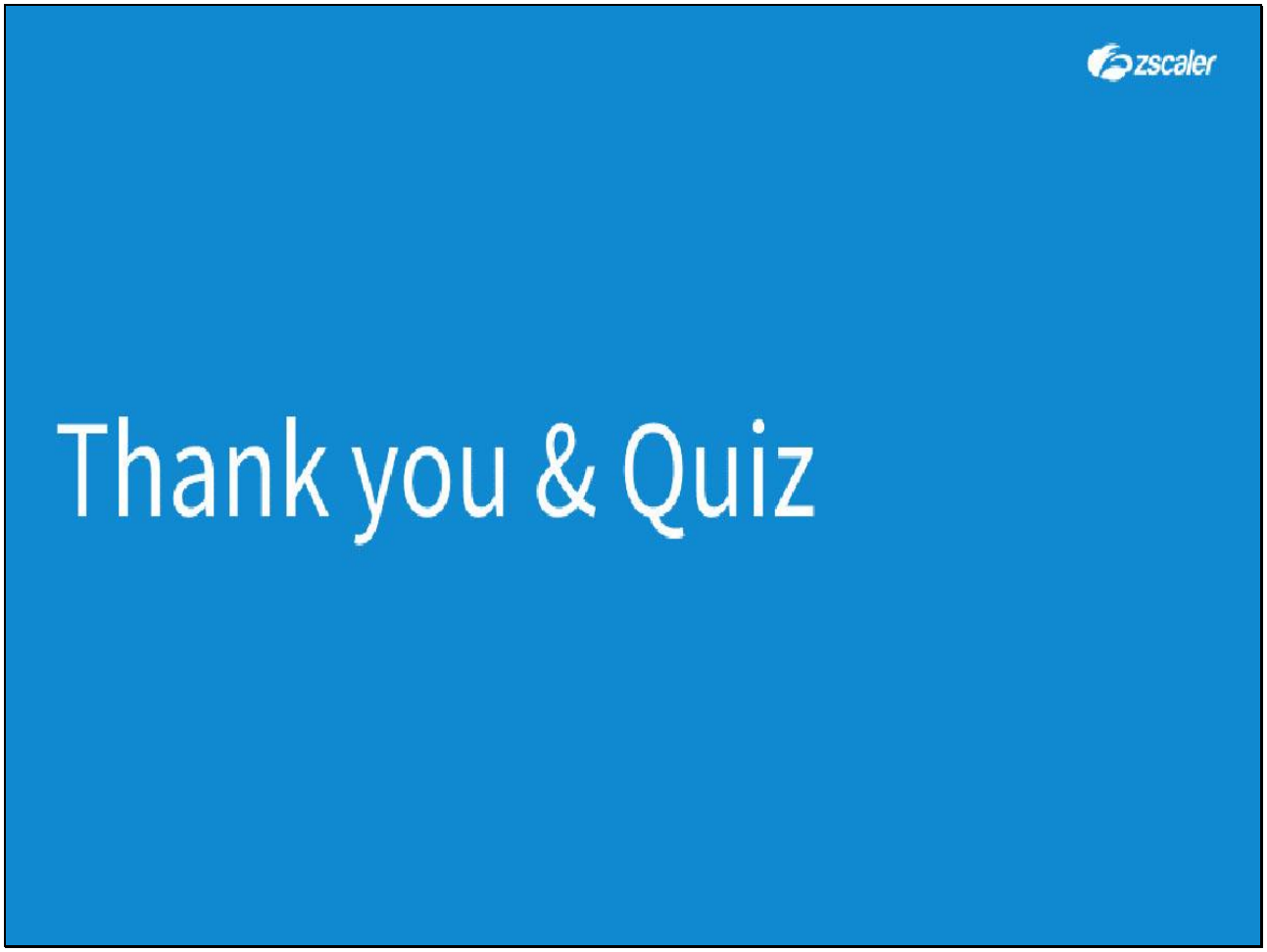


Slide notes

…the attributes will be imported to the **SAML Attributes** library and are immediately available for you to use to control access with your policy configurations.

Note that if attributes have been added from multiple IdPs, you have the option to filter the list by source IdP.

Slide 100 - Thank you & Quiz



Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

What follows is a short quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.