

Slide 1 - Zscaler Private Access



Zscaler Private Access

Basic Administration

©2020 Zscaler, Inc. All rights reserved.

Slide notes

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

Slide 2 - Navigating the eLearning Module

The screenshot shows a Zscaler eLearning module interface. At the top right is the Zscaler logo. The main title "Navigating the eLearning Module" is centered above a dashboard. The dashboard includes a video player for "ZPA Basic Administration", a navigation bar with tabs for Applications, Users, and Health, and a date range selector (14 Days). Key metrics are displayed in cards: "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). A large blue callout box highlights the "Exit" button in the top right corner of the dashboard area. On the left side, there's a sidebar with links for Dashboard, Diagnostics, Use Logs, Administration, and Search. Below the sidebar, a "Previous Slide" button is highlighted by a blue callout. In the center, a "Next Slide" button is highlighted by a blue callout. A "Play/Pause" button is shown at the bottom left, also with a blue callout. A "Progress Bar" is located at the bottom center. On the right side, a "TOP APPLICATIONS BY BANDWIDTH" chart is shown, listing applications and their bandwidth usage. A "Closed Captioning" button is highlighted by a blue callout at the bottom right. Another blue callout highlights the "Audio On/Off" button.

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

Agenda



- ZPA Prerequisites
- Steps to Enabling ZPA
- Basic ZPA Configurations
 1. Update Company and Administrator Data
 2. Configure Certificates
 3. Configure Single Sign-on

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

Connector Support

- VMs or RPMs available for...
 - Amazon Web Services (AWS)
 - Microsoft Azure ◦ HyperV
 - CentOS 7.2+ ◦ Oracle Linux 7.2
 - Red Hat Enterprise Linux 7.2+
 - VMware vCenter and vSphere Hypervisor (ESXi)

The diagram illustrates the ZPA Cloud architecture. At the top, a white cloud contains a blue icon of a hand holding a gear, labeled 'ZPA Cloud'. Below it, a larger grey cloud contains a blue icon of a connector port, labeled 'Connector'. Between the two clouds is a white rectangular box labeled 'Firewall' with a small fire icon.

Slide notes

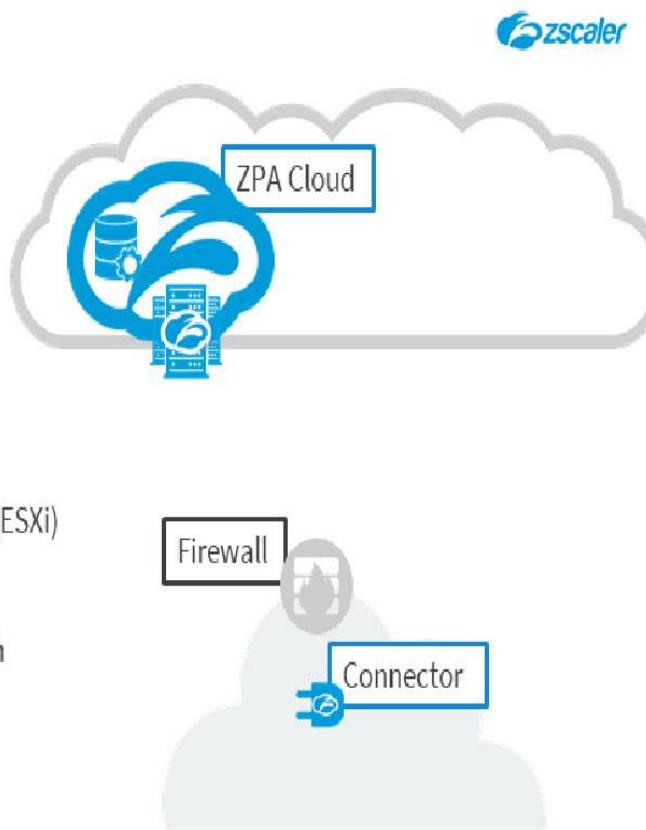
Connectors are lightweight software packages or virtual machines (VM) that are installed in the data centers, private or public cloud instances that host your servers and applications. They connect in the outbound direction to the ZPA Cloud infrastructure, to provide users access to the private applications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

Connector Support

- VMs or RPMs available for...
 - Amazon Web Services (AWS)
 - Microsoft Azure ◦ HyperV
 - CentOS 7.2+ ◦ Oracle Linux 7.2
 - Red Hat Enterprise Linux 7.2+
 - VMware vCenter and vSphere Hypervisor (ESXi)
- Connector Sizing:
 - 2 CPU cores (Xeon E5 class) or 4 cores with Hyperthreading for VMs
 - 8 GB Disk Space (thin provisioned)
 - 4 GB RAM ◦ 1 NIC



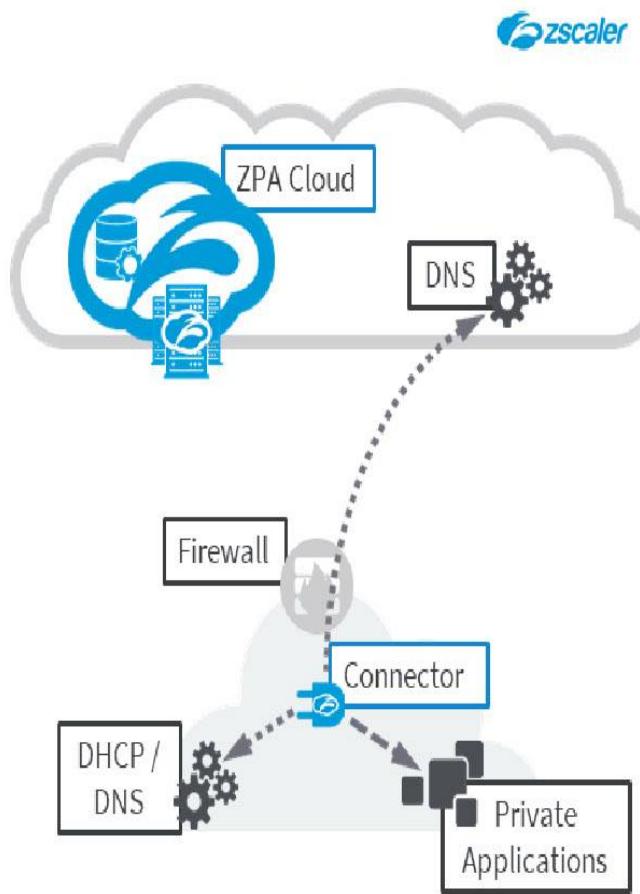
Slide notes

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

Connector Requirements

- Networking
 - DHCP or static IP address allocation options
 - Static MAC address
 - DNS resolution required (internal and external)



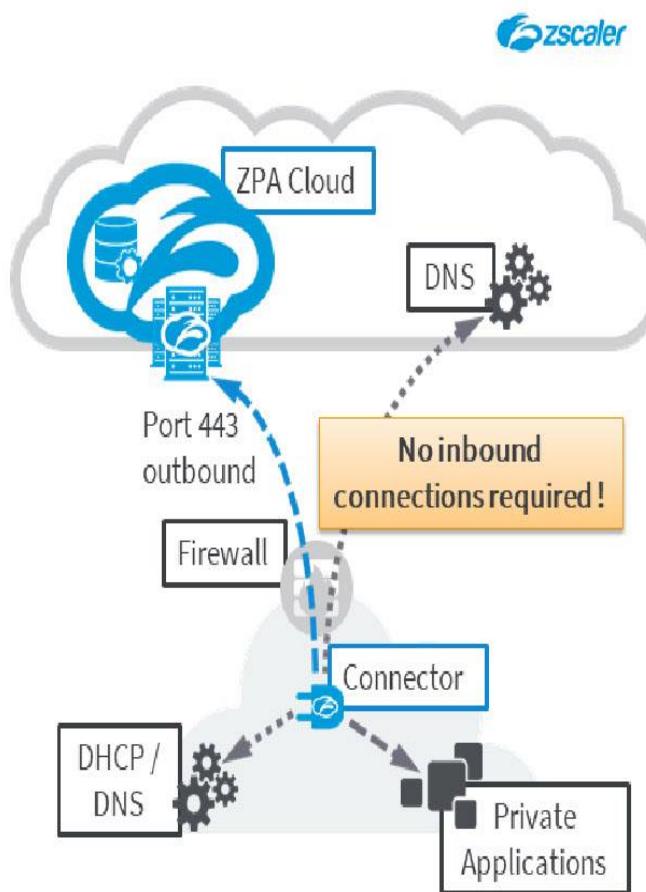
Slide notes

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

Connector Requirements

- Networking
 - DHCP or static IP address allocation options
 - Static MAC address
 - DNS resolution required (internal and external)
- Connectivity
 - Direct, outbound connections on port 443 to ZPA Cloud required (ZENs)
 - No in-line interception or inspection
 - Internal application reachability required

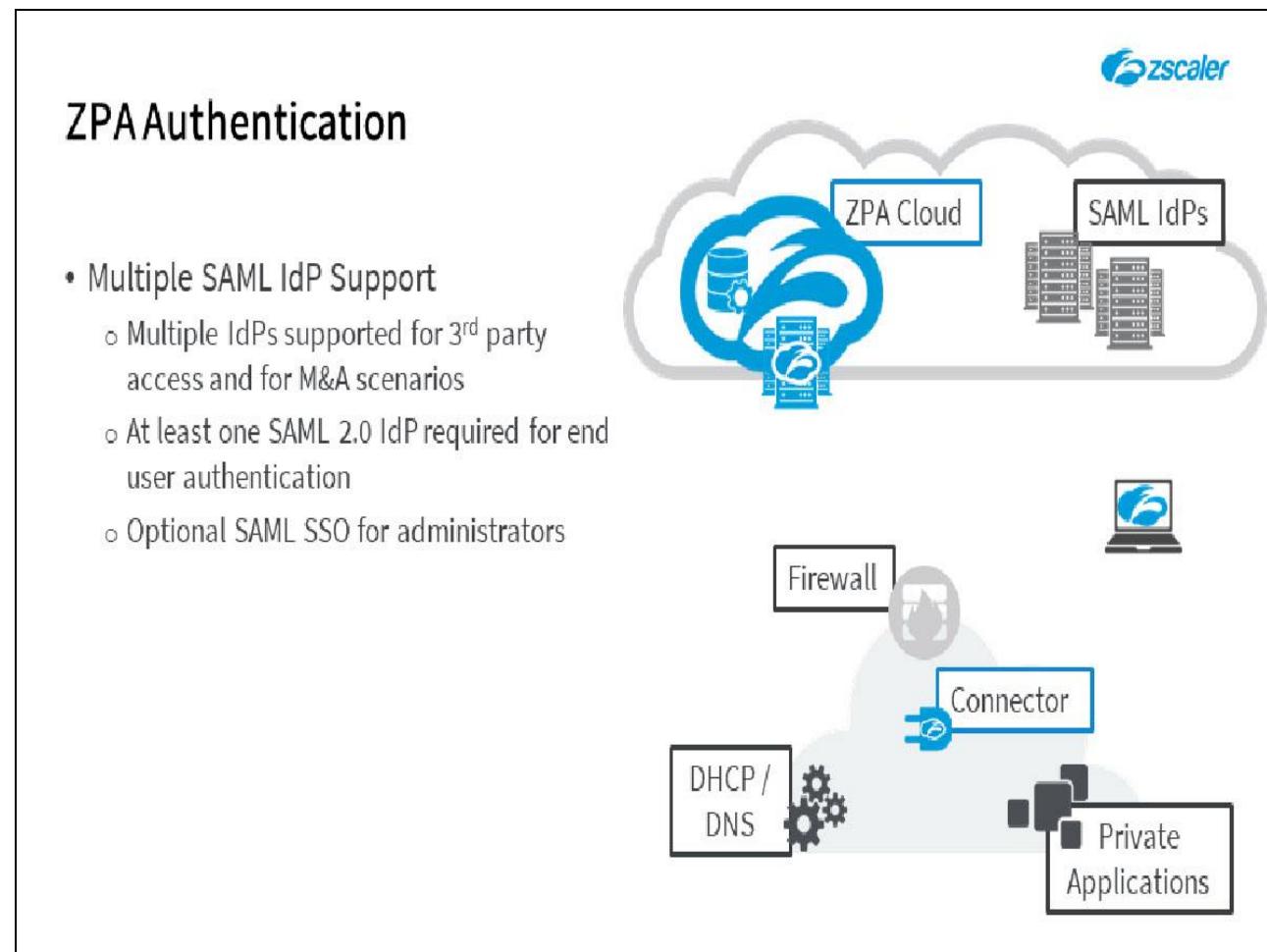


Slide notes

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



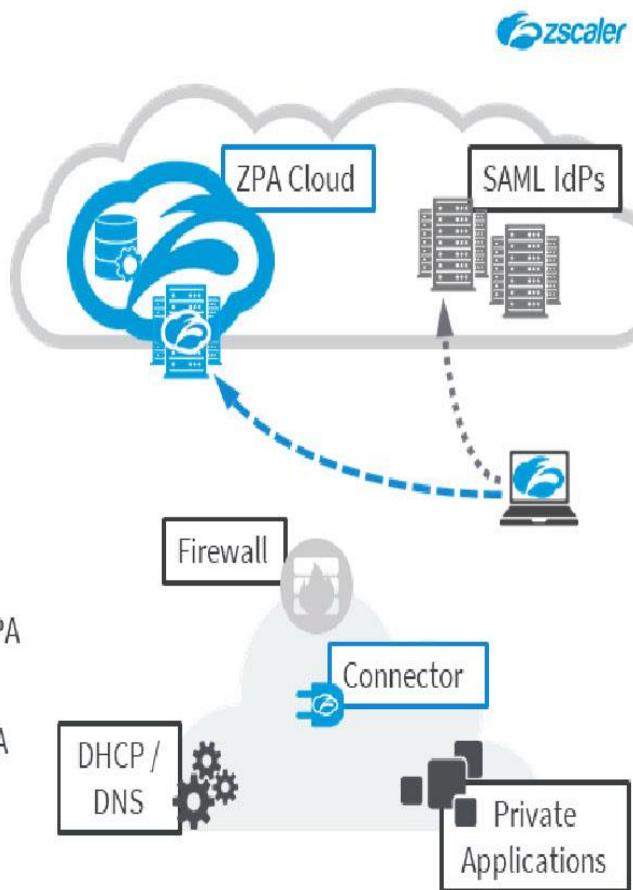
Slide notes

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

ZPA Authentication

- Multiple SAML IdP Support
 - Multiple IdPs supported for 3rd party access and for M&A scenarios
 - At least one SAML 2.0 IdP required for end user authentication
 - Optional SAML SSO for administrators
- SAML Authentication
 - Add ZPA SP to the IdP(s) & add IdP(s) in ZPA
 - Device must be able to reach the IdP(s)
 - Where possible use the same IdP as for ZIA
 - IdP(s) may return multiple attributes
 - Configurable per-application segment
Timeout Policy and Idle Timeout



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



Steps for Enabling ZPA

1. • Update Company and Administrator Information

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



Steps for Enabling ZPA

1. • Update Company and Administrator Information

• Configure Your Certificates 2.

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



Steps for Enabling ZPA

1.
 - Update Company and Administrator Information
 - Configure Your Certificates
- 2.
3.
 - Configure Single Sign-on

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



Steps for Enabling ZPA

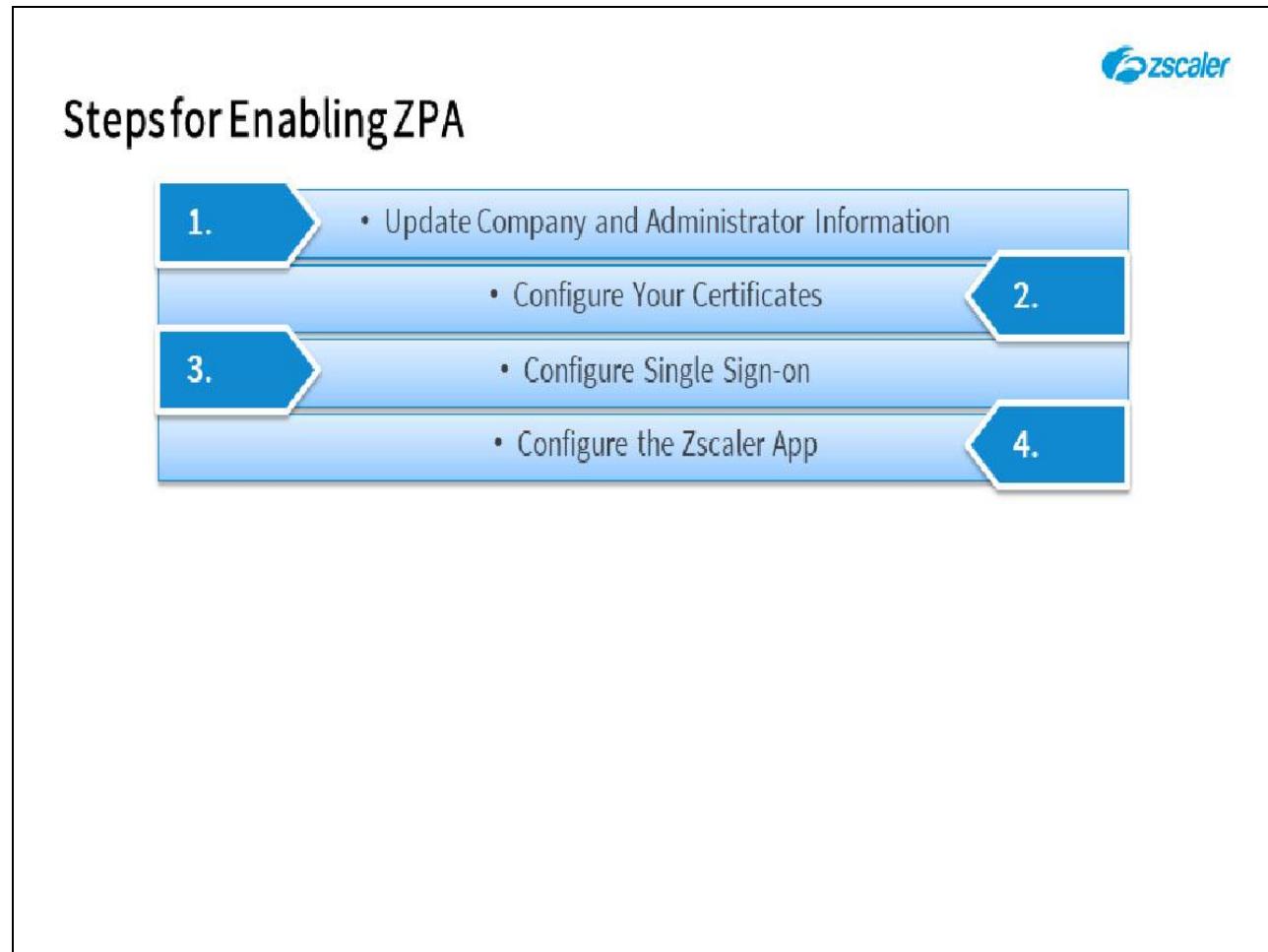
1.
 - Update Company and Administrator Information
 - Configure Your Certificates
- 2.
3.
 - Configure Single Sign-on

If using the Zscaler App for Internet Access as well, it should also be configured for SAML authentication

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



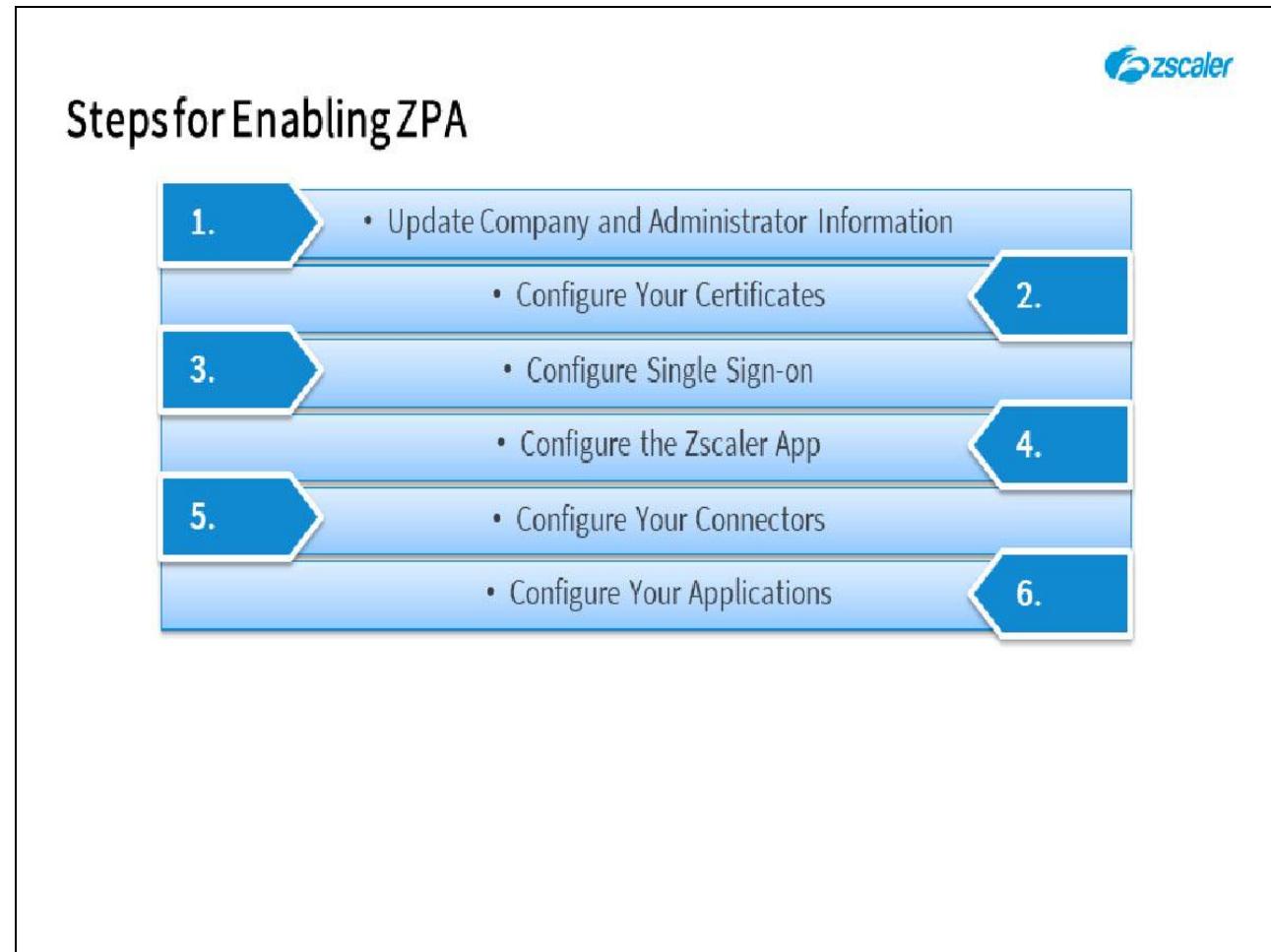
Steps for Enabling ZPA

1.
 - Update Company and Administrator Information
 - Configure Your Certificates
2.
 - Configure Single Sign-on
 - Configure the Zscaler App
3.
 - Configure Your Connectors
4.
 - Configure Your Connectors
5.
 - Configure Your Connectors

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.

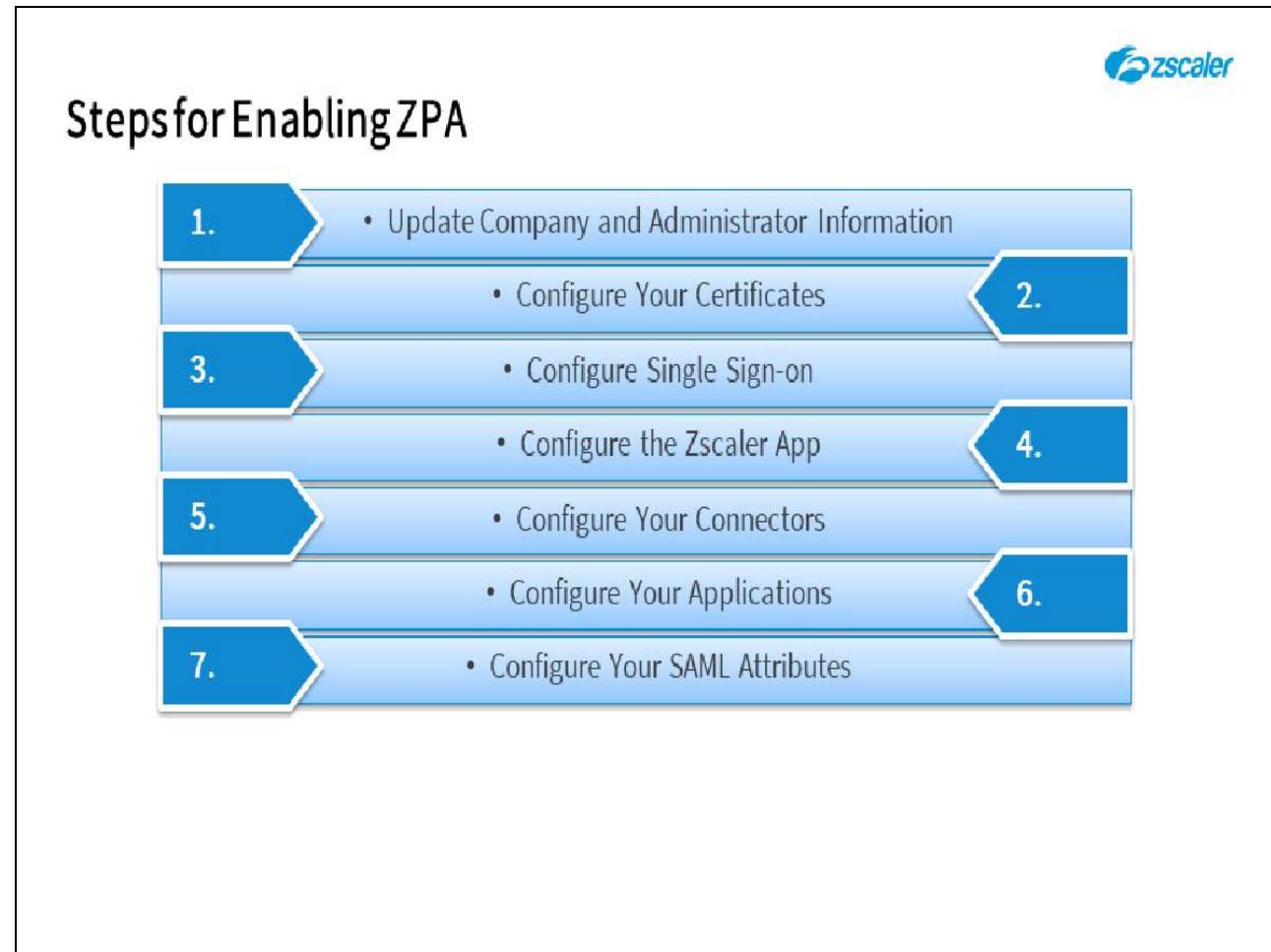
Slide 18 - Steps for Enabling ZPA



Slide notes

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

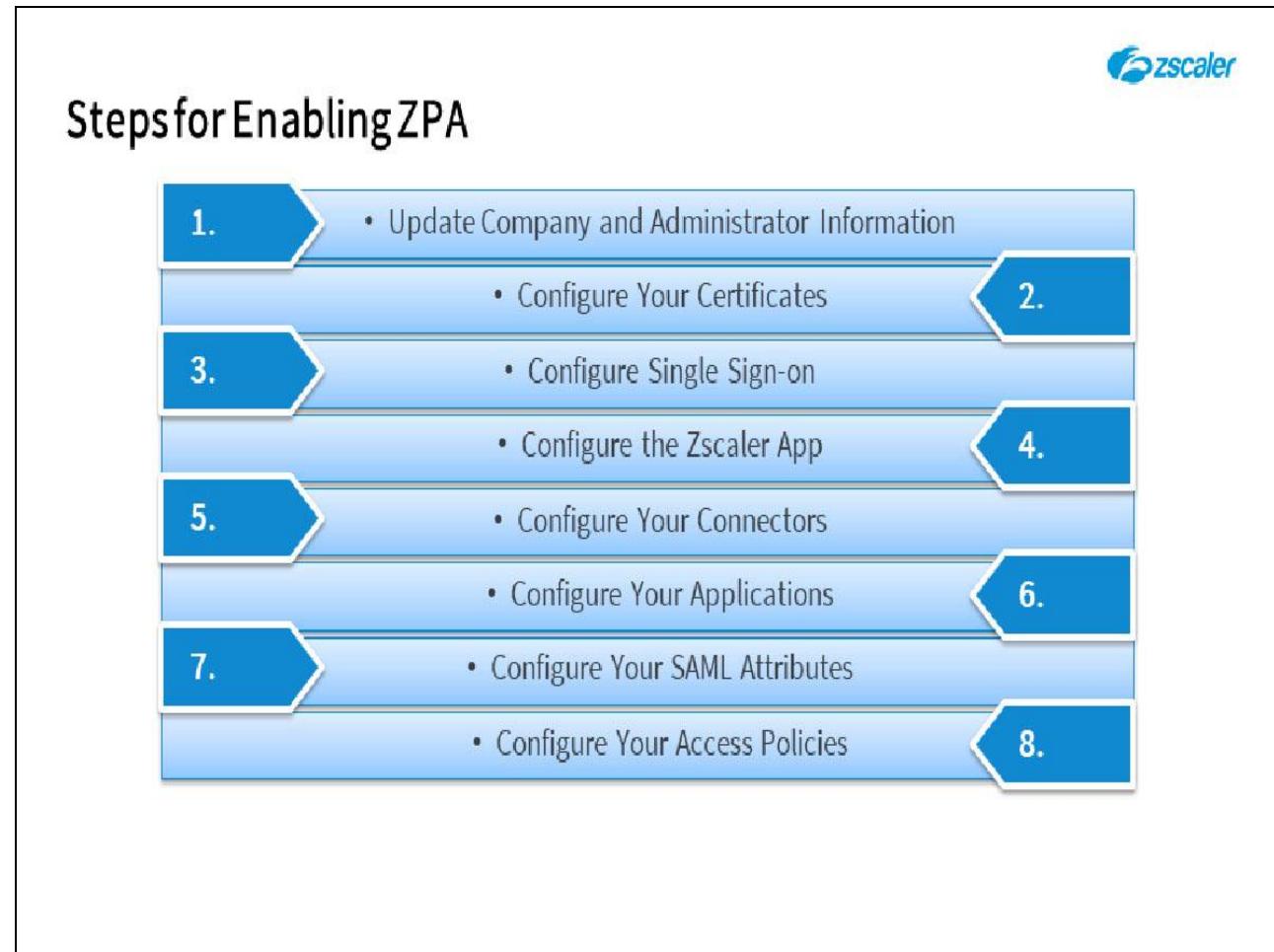
Slide 19 - Steps for Enabling ZPA



Slide notes

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

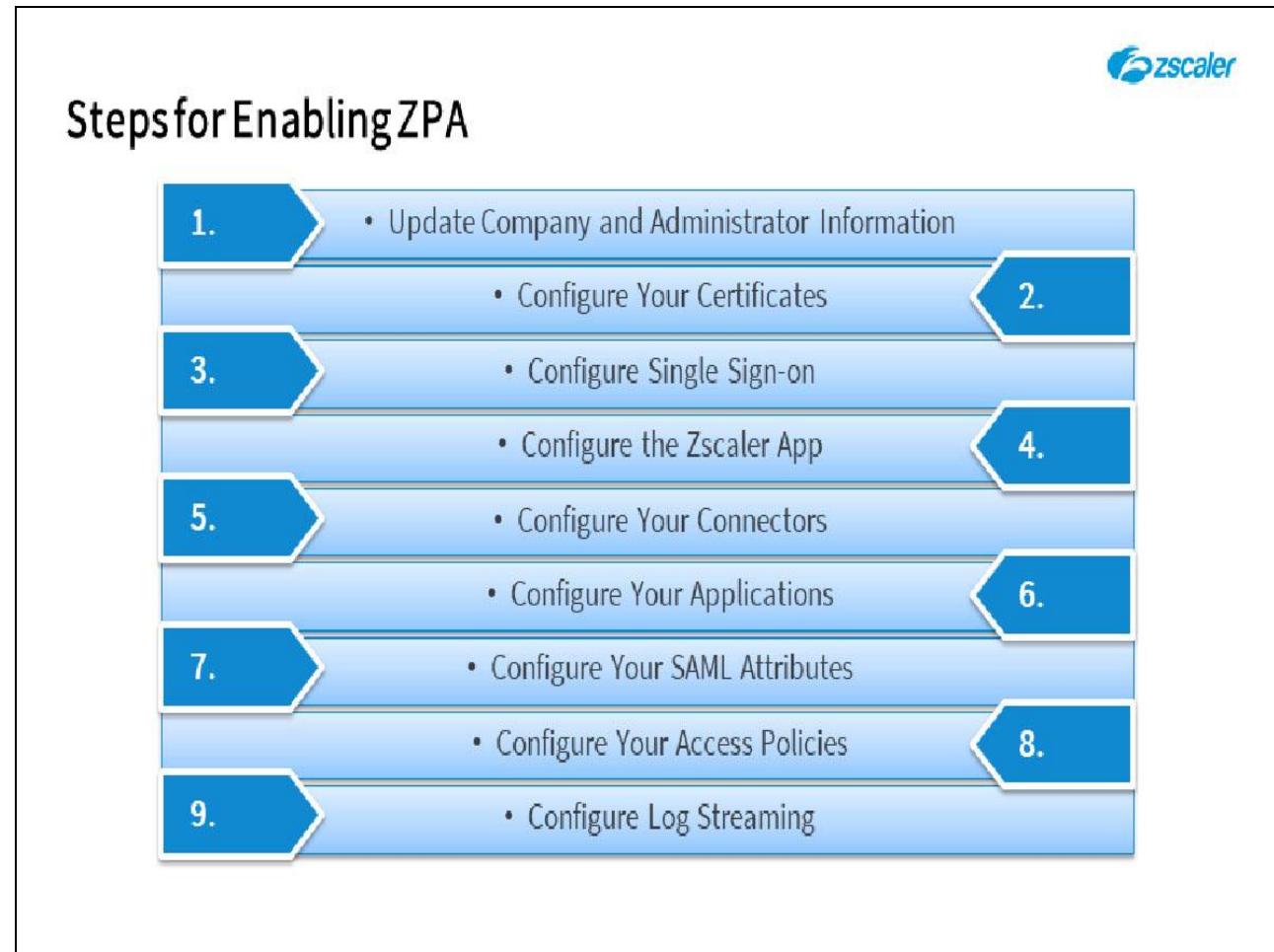
Slide 20 - Steps for Enabling ZPA



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.

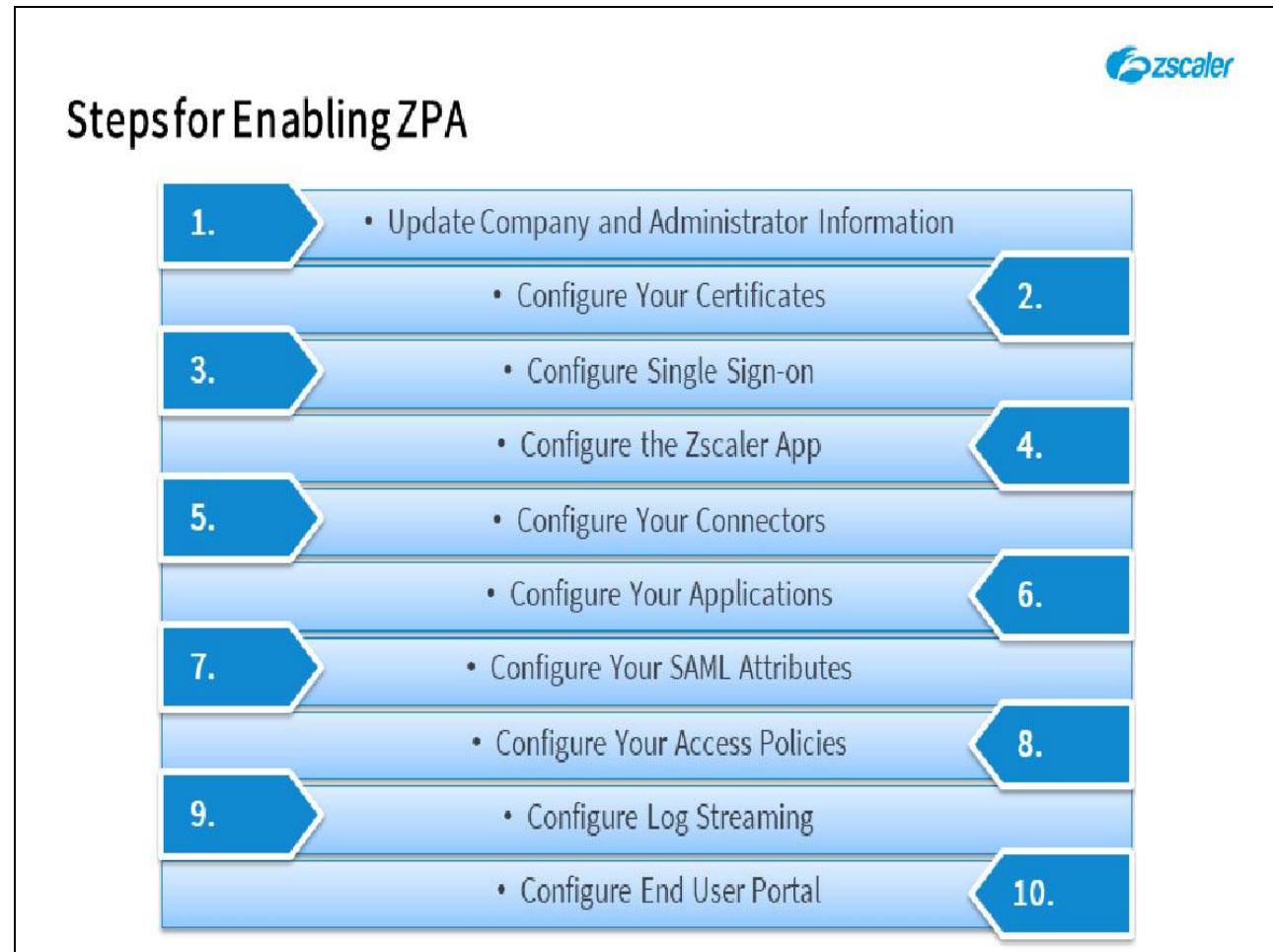
Slide 21 - Steps for Enabling ZPA



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.

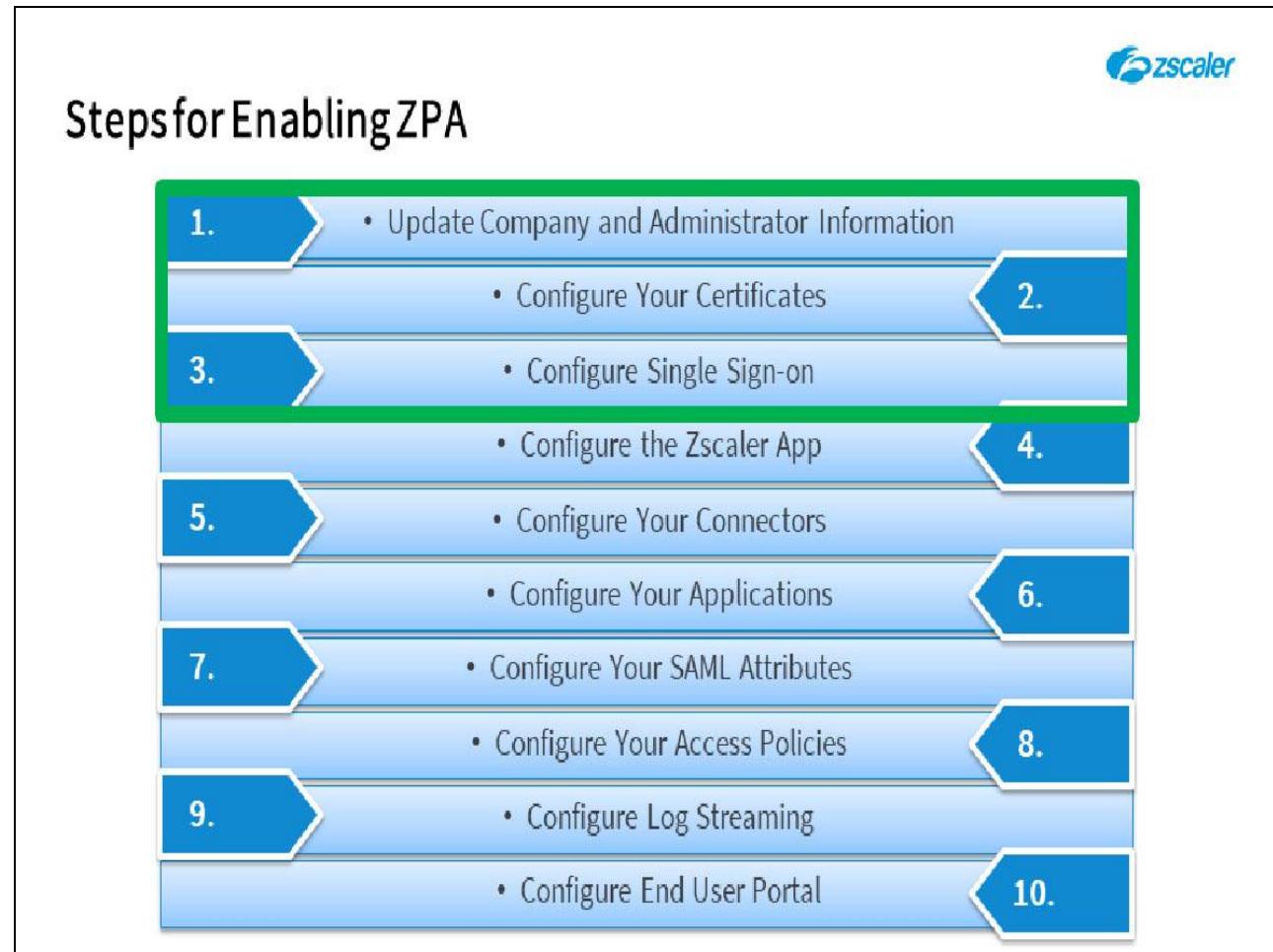
Slide 22 - Steps for Enabling ZPA



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

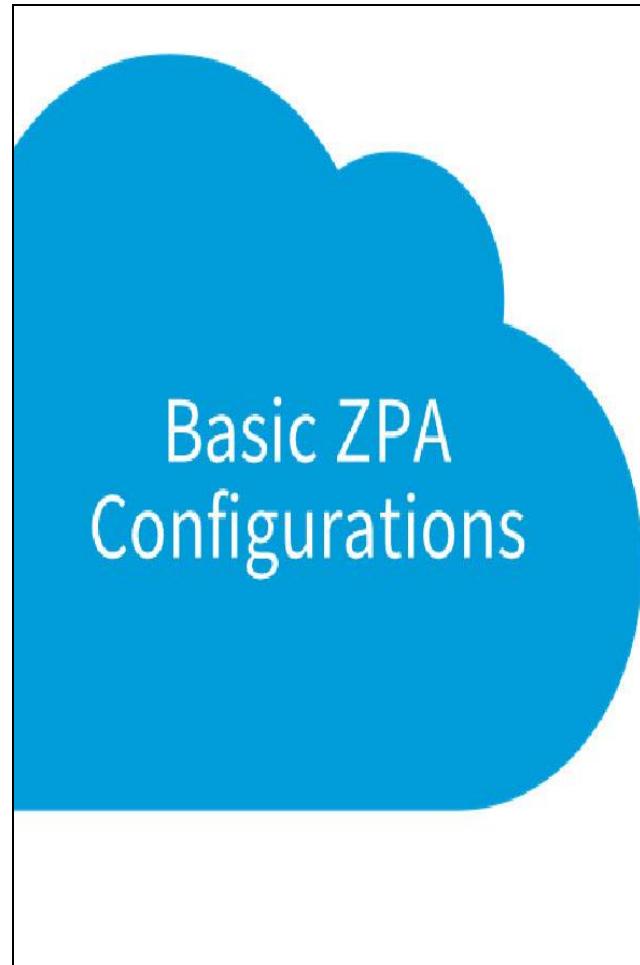
Basic ZPA Configurations

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



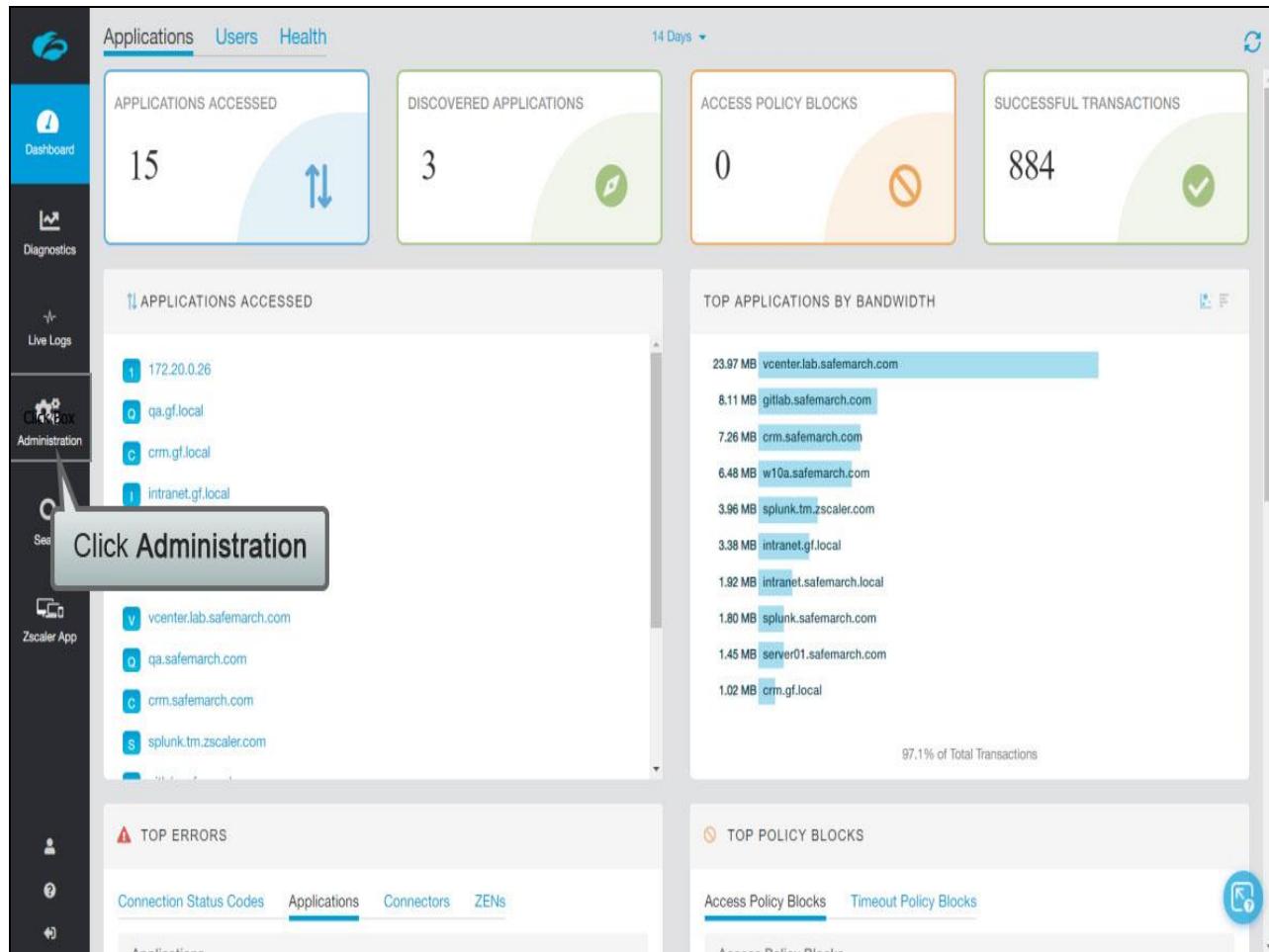
Basic ZPA Configurations

1. Update Company and Administrator Data

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**, ...

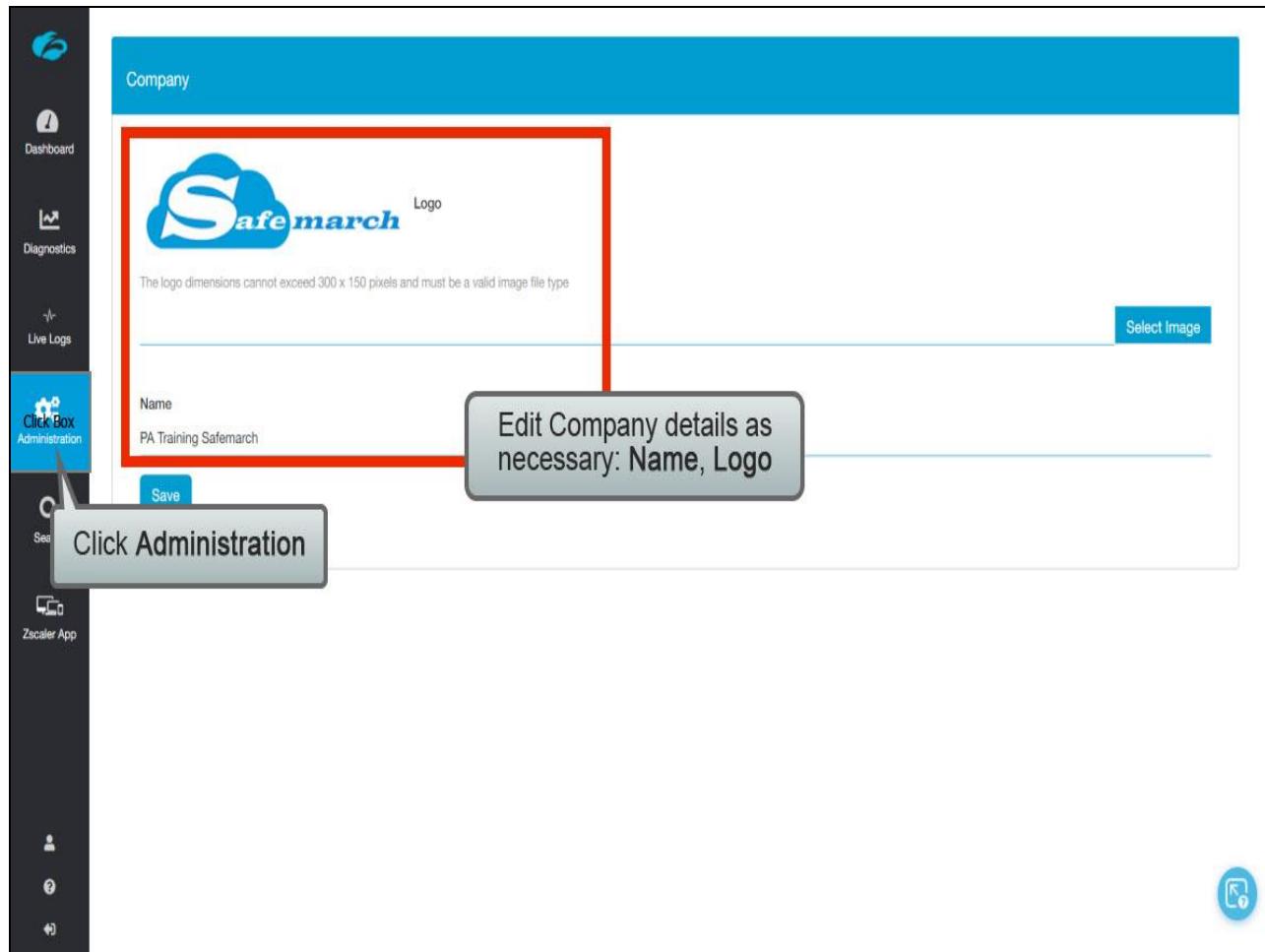
Slide 27 - Slide 27

The screenshot shows the Zscaler Cloud interface. On the left is a dark sidebar with various navigation links: Application Management, Authentication, Certificate Management, Connector Management, Log Streaming Service, Policy Management, and Settings. The Settings section is expanded, showing Administrators, Audit Logs, and Roles. A callout bubble points to the 'Company' link under Administrators with the text 'Click Company'. The main dashboard area has a '14 Days' time filter. It displays three summary cards: 'PUBLISHED APPLICATIONS' (0), 'ACCESS POLICY BLOCKS' (0), and 'SUCCESSFUL TRANSACTIONS' (884). Below these are two charts: 'TOP APPLICATIONS BY BANDWIDTH' (listing vccenter.lab.safemarch.com at 23.97 MB) and 'TOP POLICY BLOCKS' (listing Access Policy Blocks). The bottom of the dashboard shows a progress bar for 'Access Policy Blocks' at 97.1%.

Slide notes

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

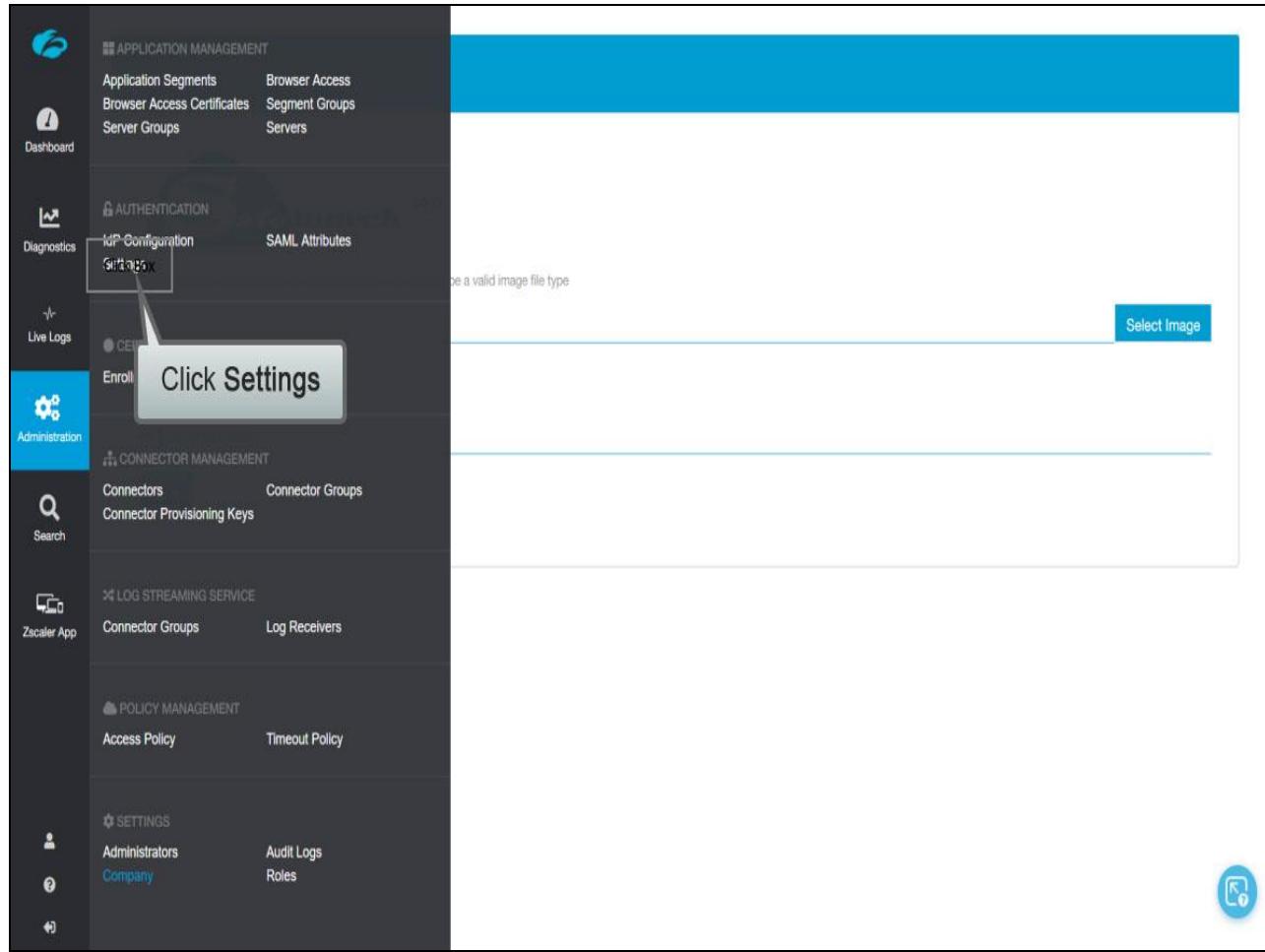
Slide 28 - Slide 28



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

Review and edit settings as necessary:

- ◆ Primary Authentication Domain
- ◆ Additional Authentication Domains (if applicable)
- ◆ Remote Assistance
- ◆ Enforce SSO Login for Administrators

Click Administration

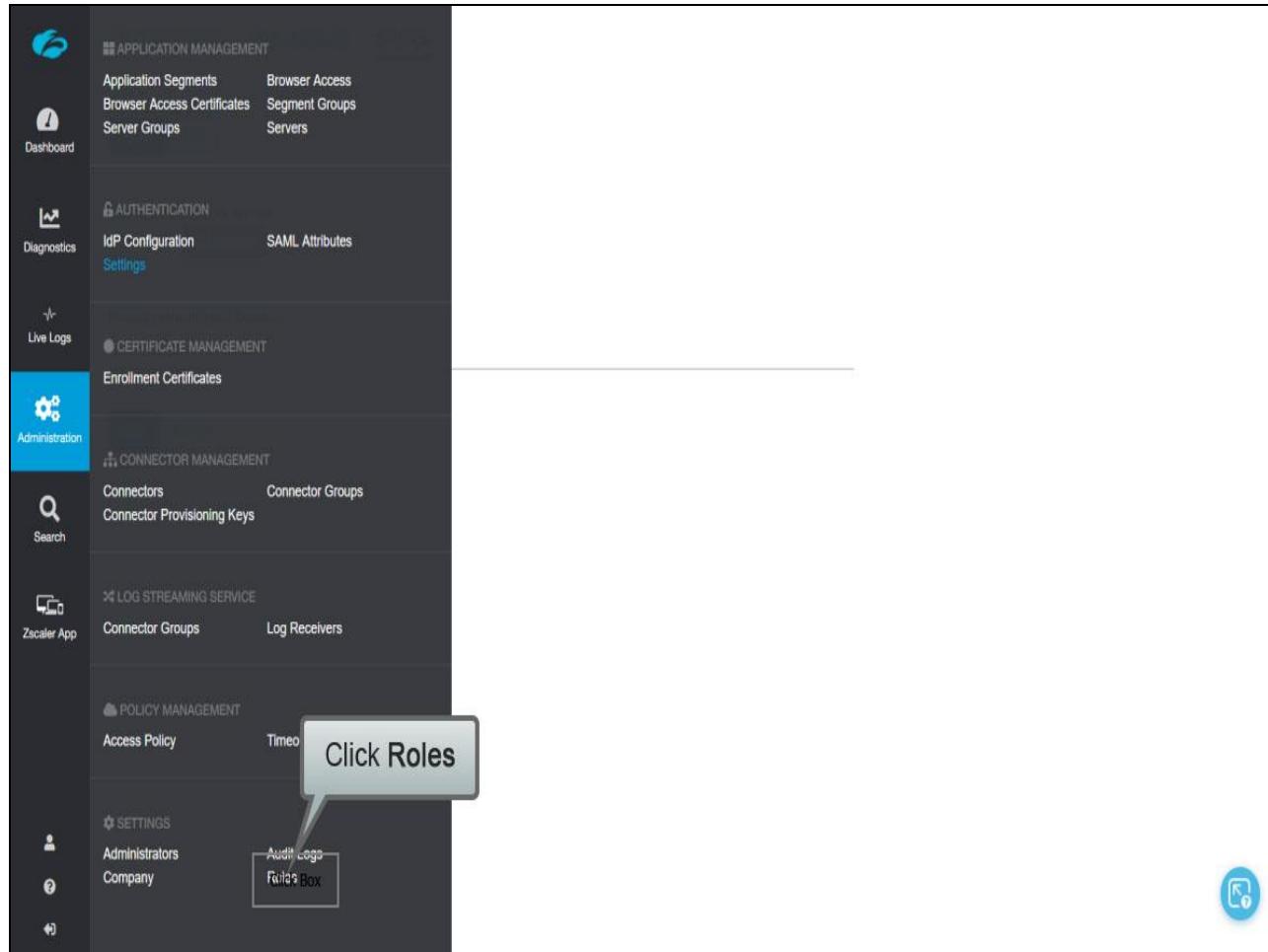
Slide notes

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

The screenshot shows the Zscaler Admin Portal interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help. The main area has a header with 'Administrators', 'Roles' (which is selected), and 'Audit Logs'. Below is a table with columns: Name, # of Admins with this Role, Description, and Actions. The table contains three rows: 'Helpdesk' (0 admins, role for Helpdesk users), 'ZPA Administrator' (2 admins, administrator has full access to ZPA), and 'ZPA Read Only Administrator' (0 admins, administrator has read only access to ZPA). A red box highlights the 'Default Roles' section. A callout box labeled 'Click Edit' points to the edit icon for 'ZPA Administrator'. Another callout box labeled 'Add Roles as necessary' points to the 'Add Role' button.

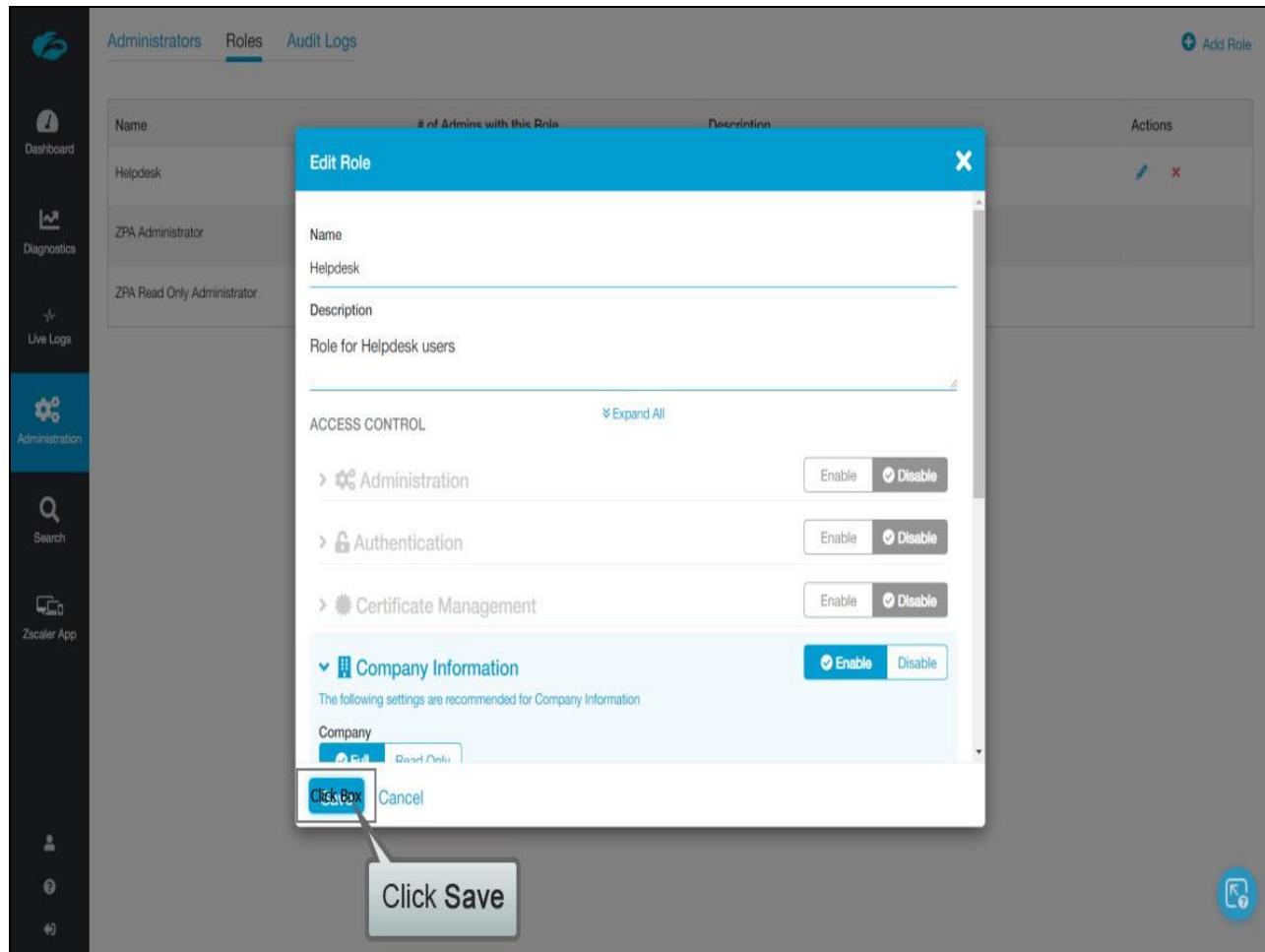
Name	# of Admins with this Role	Description	Actions
Helpdesk	0	Role for Helpdesk users	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
ZPA Administrator	2	Administrator has full access to ZPA	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
ZPA Read Only Administrator	0	Administrator has read only access to ZPA	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

The screenshot shows the ZPA Administration interface. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main content area has tabs for Click Boxes, Roles (selected), and Audit Logs. A callout box highlights the 'Click Administrators' link under the Roles tab. The Roles table lists three roles:

Name	Admins with this Role	Description	Actions
Helpdesk		Role for Helpdesk users	
ZPA Administrator	2	Administrator has full access to ZPA	
ZPA Read Only Administrator	0	Administrator has read only access to ZPA	

Slide notes

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

Slide 35 - Slide 35

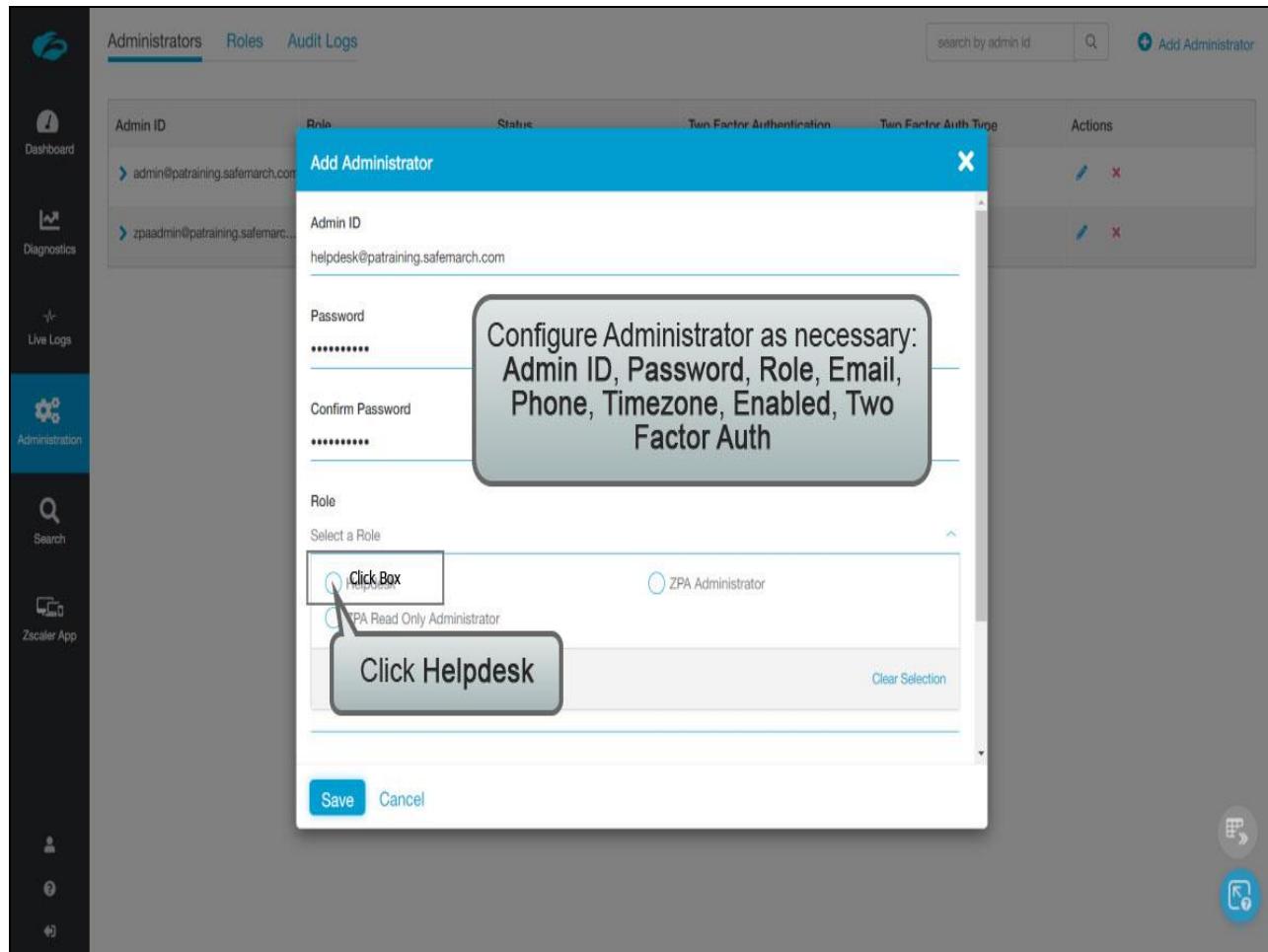
The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, Search, Zscaler App, and Help. The main area has tabs for Administrators, Roles, and Audit Logs, with 'Administrators' selected. A table lists two administrators: 'admin@patraining.safemarch.com' and 'zpaadmin@patraining.safemarc...'. The table columns are Admin ID, Role, Status, Two Factor Authentication, and Actions. The Actions column contains edit and delete icons. A red box highlights the Actions column. A tooltip 'Edit or Delete administrators' points to the Actions column. A second tooltip 'Click Add Administrator' points to the 'Add' button in the top right corner.

Admin ID	Role	Status	Two Factor Authentication	Actions
admin@patraining.safemarch.com	ZPA Administrator	✓	✗	
zpaadmin@patraining.safemarc...	ZPA Administrator	✓	✗	

Slide notes

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

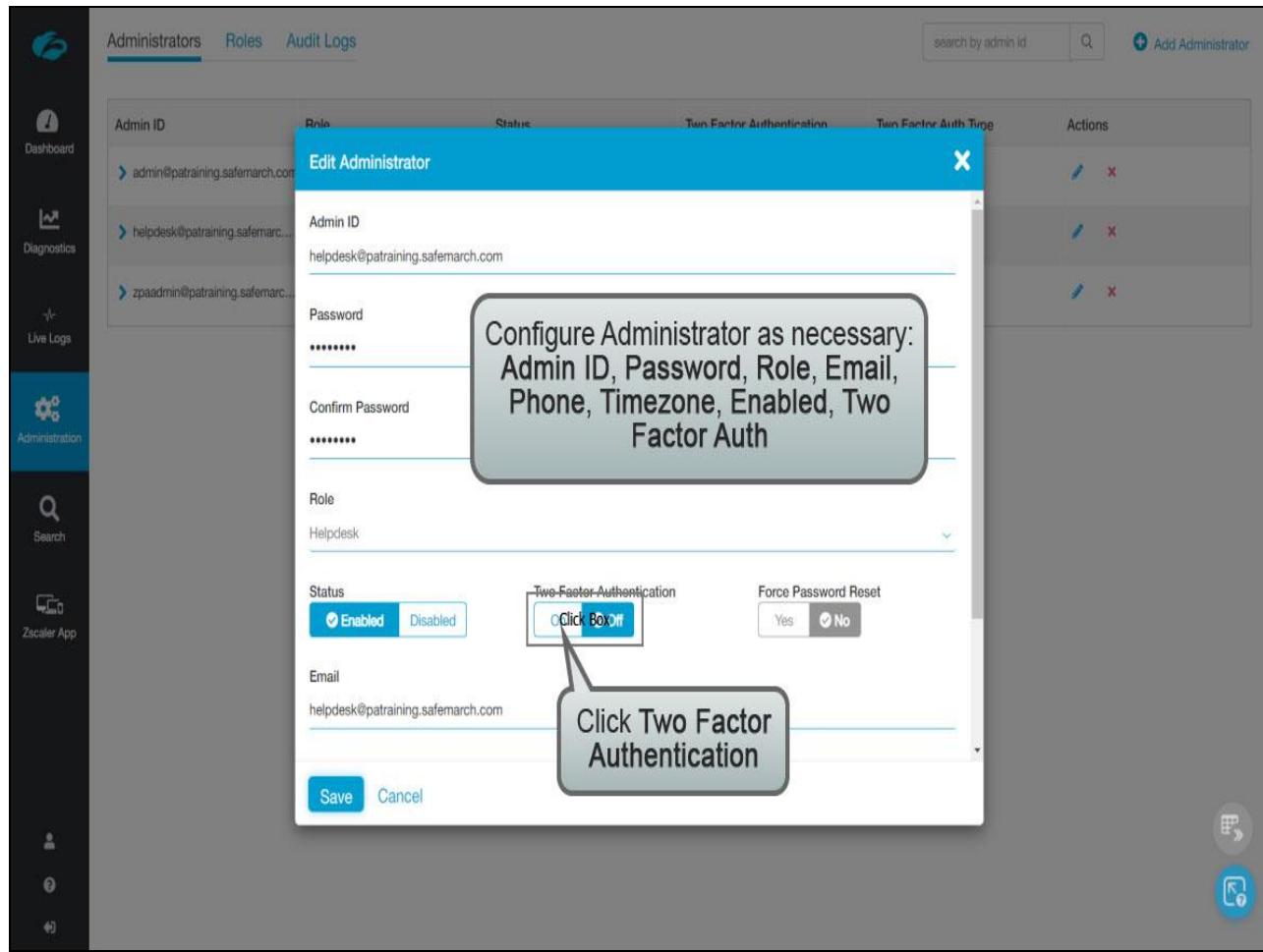
Slide 36 - Slide 36



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

Configure Administrator as necessary:
Admin ID, Password, Role, Email,
Phone, Timezone, Enabled, Two
Factor Auth

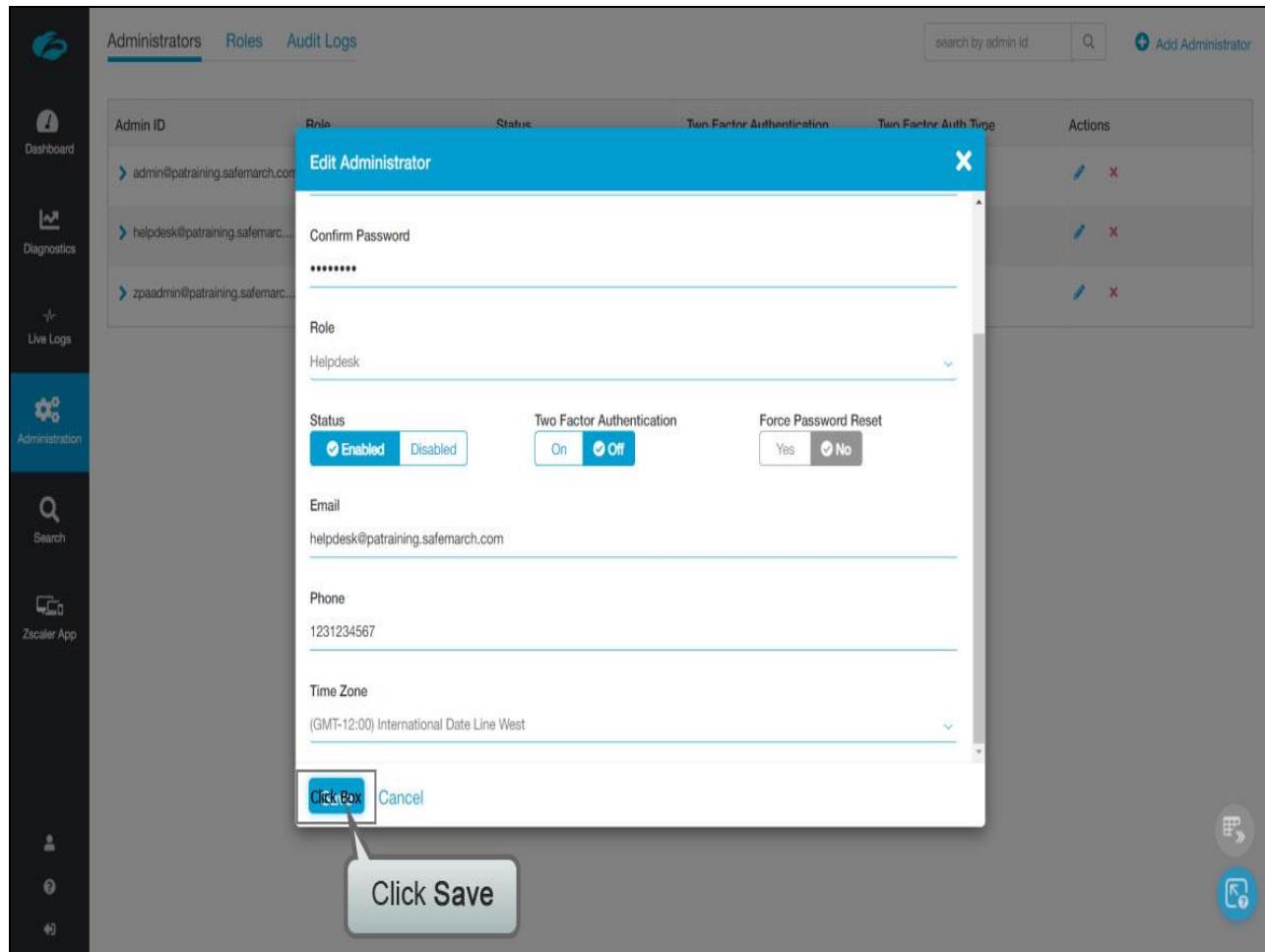
Select the Two Factor
Auth Type as necessary

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

The screenshot shows the Adobe Captivate Administration interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, Zscaler App, and Help. The main content area has tabs for Administrators, Roles (which is selected), and Audit Logs. At the top right are search and add administrator buttons. A table lists three administrators with columns for Admin ID, Role, Status, Two Factor Authentication, Two Factor Auth Type, and Actions. Each row has edit and delete icons in the Actions column. A green banner at the bottom right says "Administrator saved".

Admin ID	Role	Status	Two Factor Authentication	Two Factor Auth Type	Actions
admin@patraining.safemarch.com	ZPA Administrator	✓	✗		
helpdesk@patraining.safemarc...	Helpdesk	✓	✗		
zpaadmin@patraining.safemarc...	ZPA Administrator	✓	✗		

Slide notes

Slide 41 - Slide 41

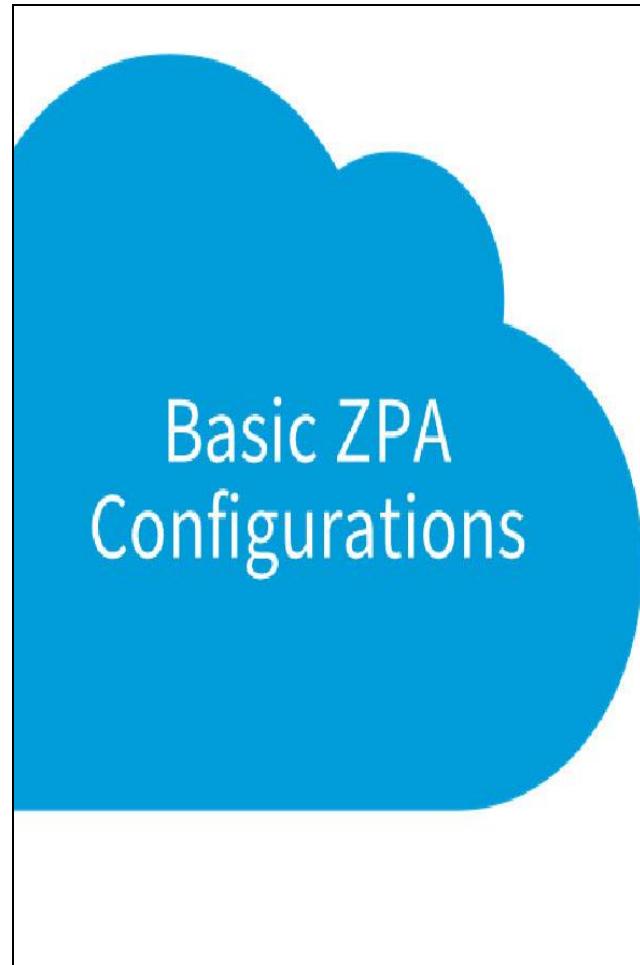
The screenshot shows the Zscaler Admin UI interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main content area has tabs for Administrators, Roles, and Audit Logs, with Administrators selected. It includes a search bar and an 'Add Administrator' button. A table lists three administrators:

Admin ID	Role	Status	Two Factor Authentication	Two Factor Auth Type	Actions
admin@patraining.safemarch.com	ZPA Administrator	✓	✗		
helpdesk@patraining.safemarc...	Helpdesk	✓	✗		
zpaadmin@patraining.safemarc...	ZPA Administrator	✓	✗		

On the right side of the main area, there are two circular buttons: one grey with a grid icon and one blue with a circular arrow icon.

Slide notes

Slide 42 - Basic ZPA Configurations



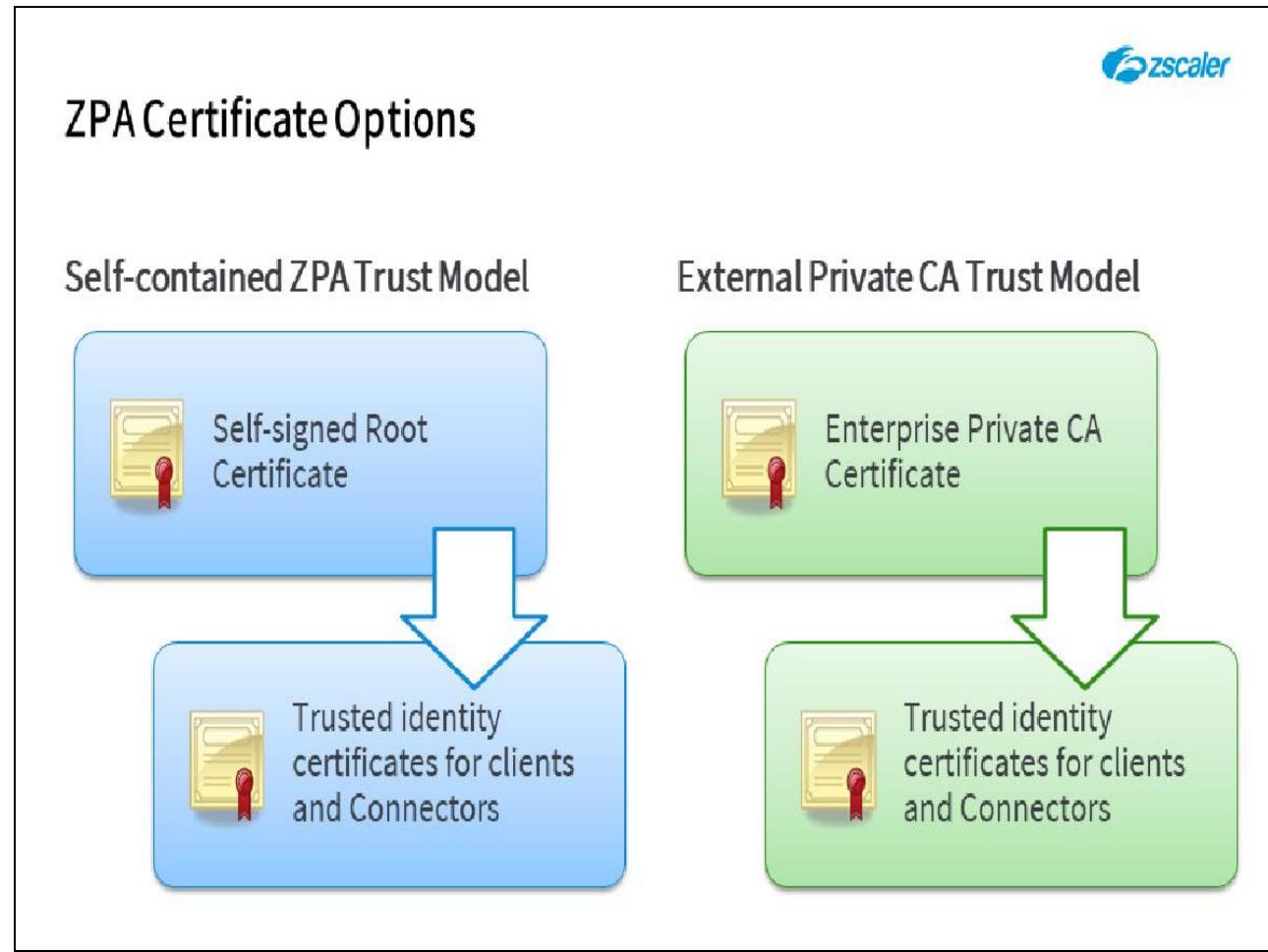
Basic ZPA Configurations

1. Update Company and Administrator Data
2. Configuring Certificates

Slide notes

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

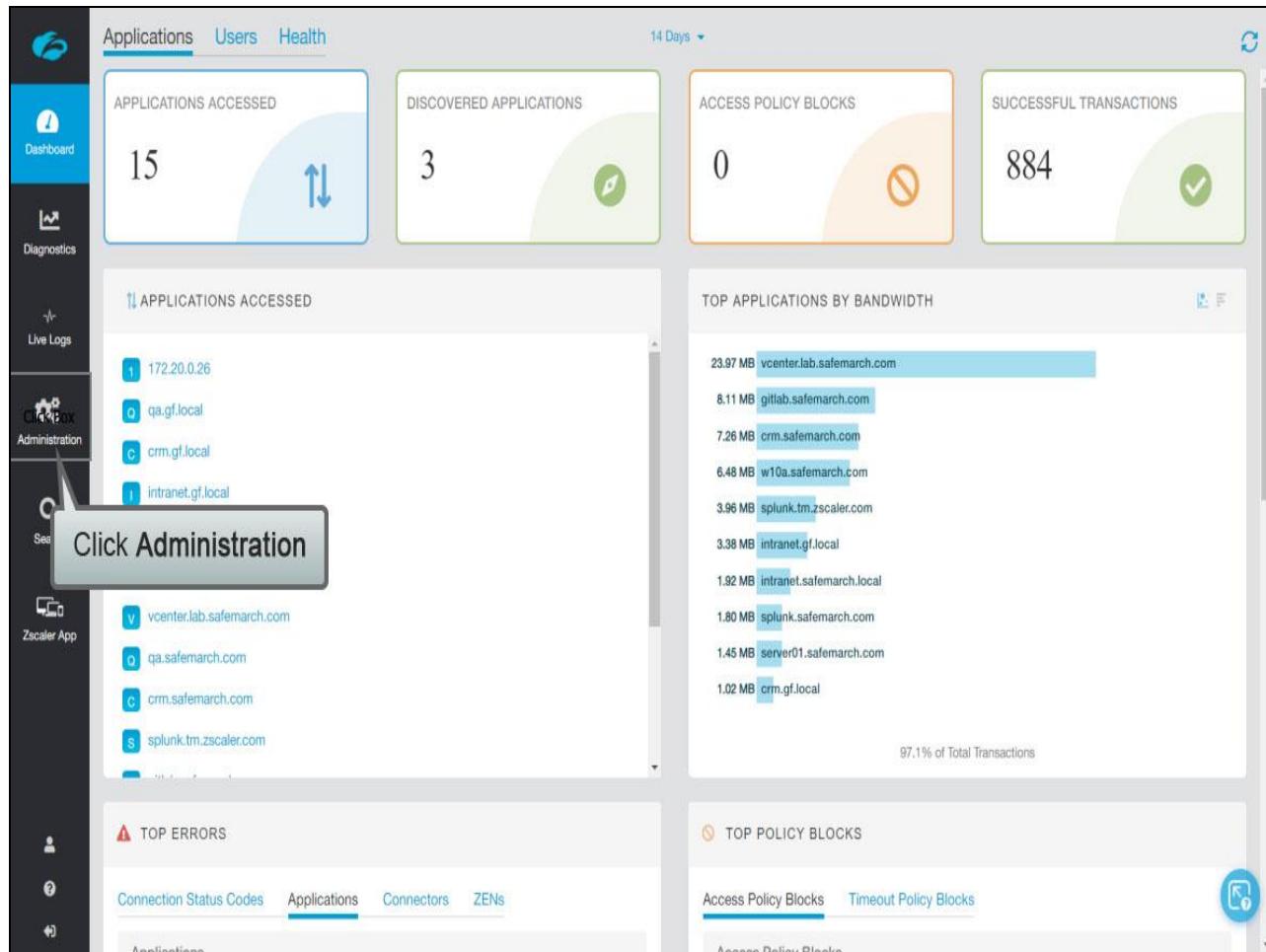
Slide 43 - ZPA Certificate Options



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

The screenshot shows the Zscaler Cloud interface. On the left, there's a navigation sidebar with various sections like Application Management, Authentication, Certificate Management (which is currently selected), Connector Management, Policy Management, and Settings. A callout bubble points to the 'Enrollment Certificates' link under Certificate Management. The main dashboard area displays several metrics: 'PENDING APPLICATIONS' (0), 'ACCESS POLICY BLOCKS' (0), and 'SUCCESSFUL TRANSACTIONS' (884). Below these are sections for 'TOP APPLICATIONS BY BANDWIDTH' and 'TOP POLICY BLOCKS'. The bandwidth chart shows the top 10 applications using the most bandwidth, with vcenter.lab.safemarch.com at the top. The policy blocks chart shows the top 10 policy blocks, with Access Policy Blocks being the active tab.

Rank	Application / Policy Block	Bandwidth / Transactions
1	vcenter.lab.safemarch.com	23.97 MB / 97.1% of Total Transactions
2	gitlab.safemarch.com	8.11 MB
3	crm.safemarch.com	7.26 MB
4	w10a.safemarch.com	6.48 MB
5	splunk.tm.zscaler.com	3.96 MB
6	intranet.gf.local	3.38 MB
7	intranet.safemarch.local	1.92 MB
8	splunk.safemarch.com	1.80 MB
9	server01.safemarch.com	1.45 MB
10	crm.gf.local	1.02 MB

Slide notes

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

Slide 46 - Slide 46

The screenshot shows the Zscaler Admin UI interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help. The main area has a header with tabs for Enrollment Certificates (selected) and Browser Access Certificates. A red box highlights the 'Upload Certificate Chain' button in the top right corner of the header. Below this is a table listing three certificates: Client, Connector, and Root. A callout box points to the 'Click Upload Certificate Chain' button in the table's header. Another callout box points to the table itself with the text 'Default CA set available for immediate use'. The table columns include Name, Creation Date, Expiry Date, Common Name, and Actions.

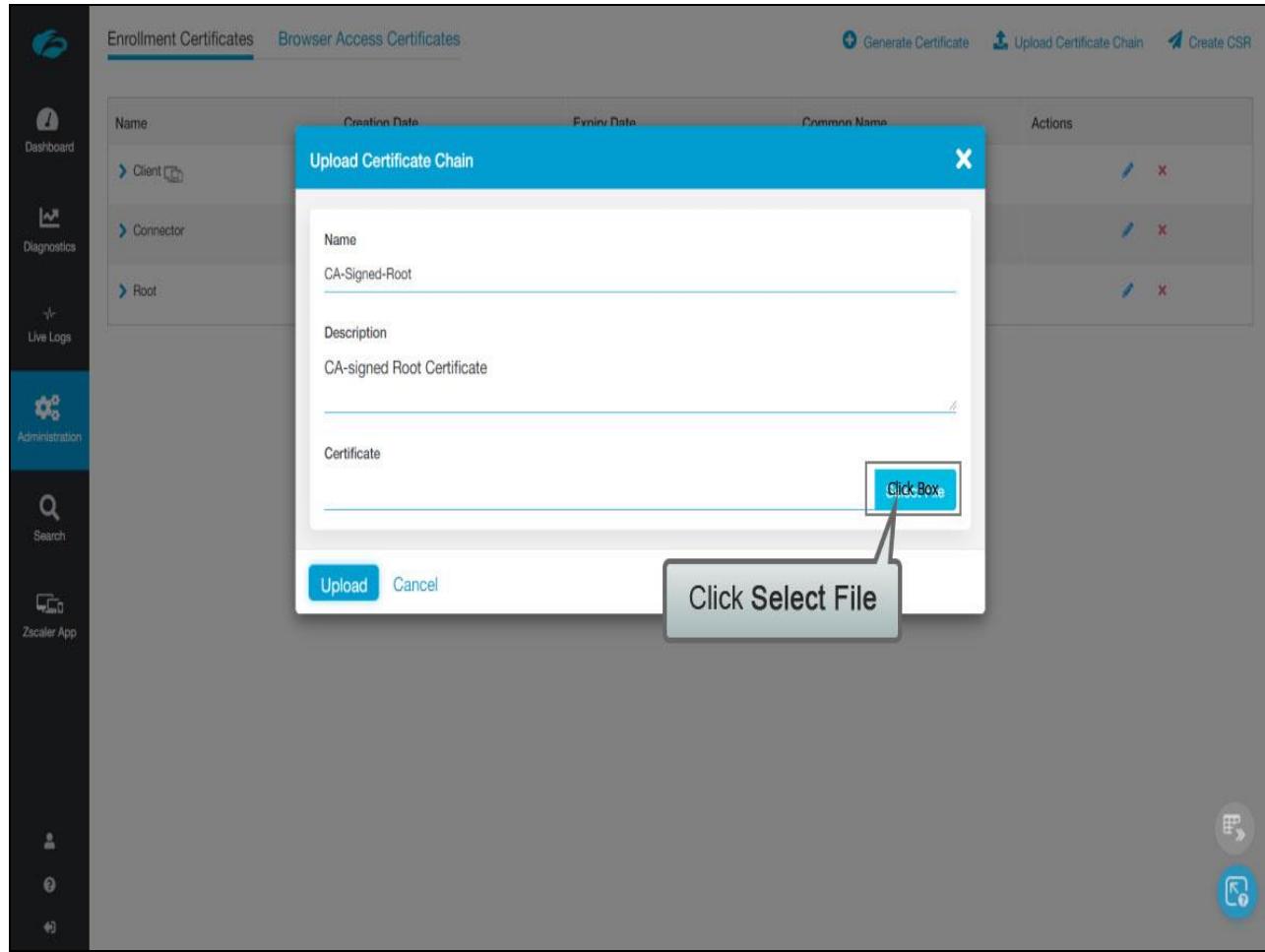
Name	Creation Date	Expiry Date	Common Name	Actions
Client	Thursday, February 15 2018 1:20:05 am	Friday, February 11 2033 1:20:04 am	patraining.safemarch.com/Client	
Connector	Thursday, February 15 2018 1:20:06 am	Friday, February 11 2033 1:20:05 am	patraining.safemarch.com/Connector	
Root	Thursday, February 15 2018 1:20:03 am	Saturday, February 08 2048 1:20:03 am	patraining.safemarch.com/Root	

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**, ...

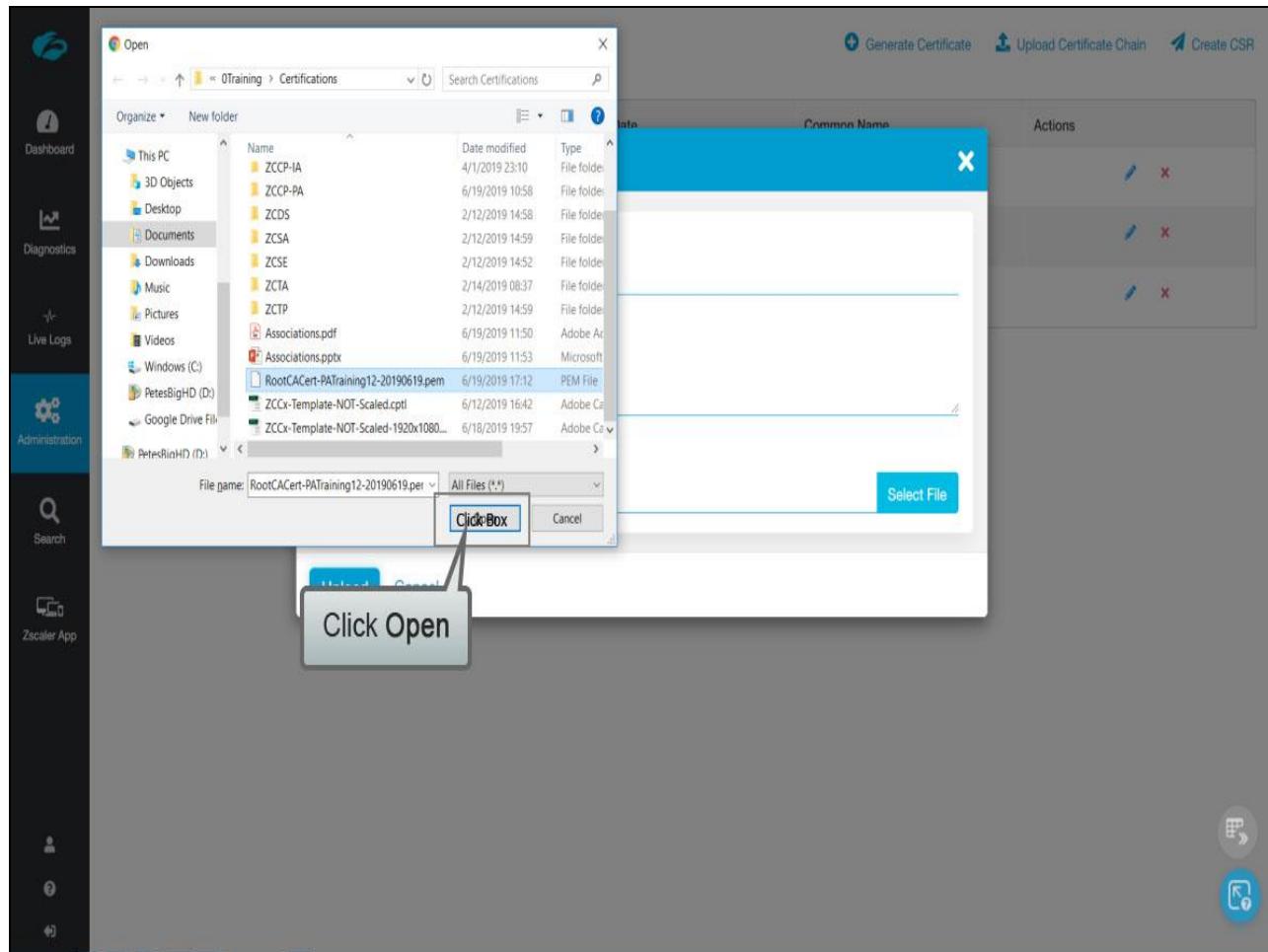
Slide 47 - Slide 47



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

The screenshot shows the Adobe Captivate interface with the 'Enrollment Certificates' tab selected. A modal dialog box titled 'Upload Certificate Chain' is open. Inside the dialog, there are fields for 'Name' (set to 'CA-Signed-Root'), 'Description' (set to 'CA-signed Root certificate'), and a 'Certificate' file input field containing 'RootCACert-PATraining12-20190619.pem'. Below the file input are 'Change' and 'Remove' buttons. At the bottom of the dialog are 'Click Box' and 'Cancel' buttons, with a callout pointing to the 'Click Box' button labeled 'Click Upload'.

Slide notes

...then click **Upload**.

Slide 50 - Slide 50

The screenshot shows the 'Enrollment Certificates' tab selected in the Adobe Captivate interface. At the top right, there are several buttons: 'Generate Certificate' (highlighted by a callout), 'Upload Certificate Chain', and 'Create CSR'. Below these are two rows of certificate details:

Name	Creation Date	Expiry Date	
CA-Signed-Root	Wednesday, June 19 2019 5:18:11 pm	Monday, June 05 2020	T-1-CA
Client	Thursday, February 15 2018 1:20:05 am	Friday, February 11 2033 1:20:04 am	patraining.safemarch.com/Client
Connector	Thursday, February 15 2018 1:20:06 am	Friday, February 11 2033 1:20:05 am	patraining.safemarch.com/Connector
Root	Thursday, February 15 2018 1:20:03 am	Saturday, February 08 2048 1:20:03 am	patraining.safemarch.com/Root

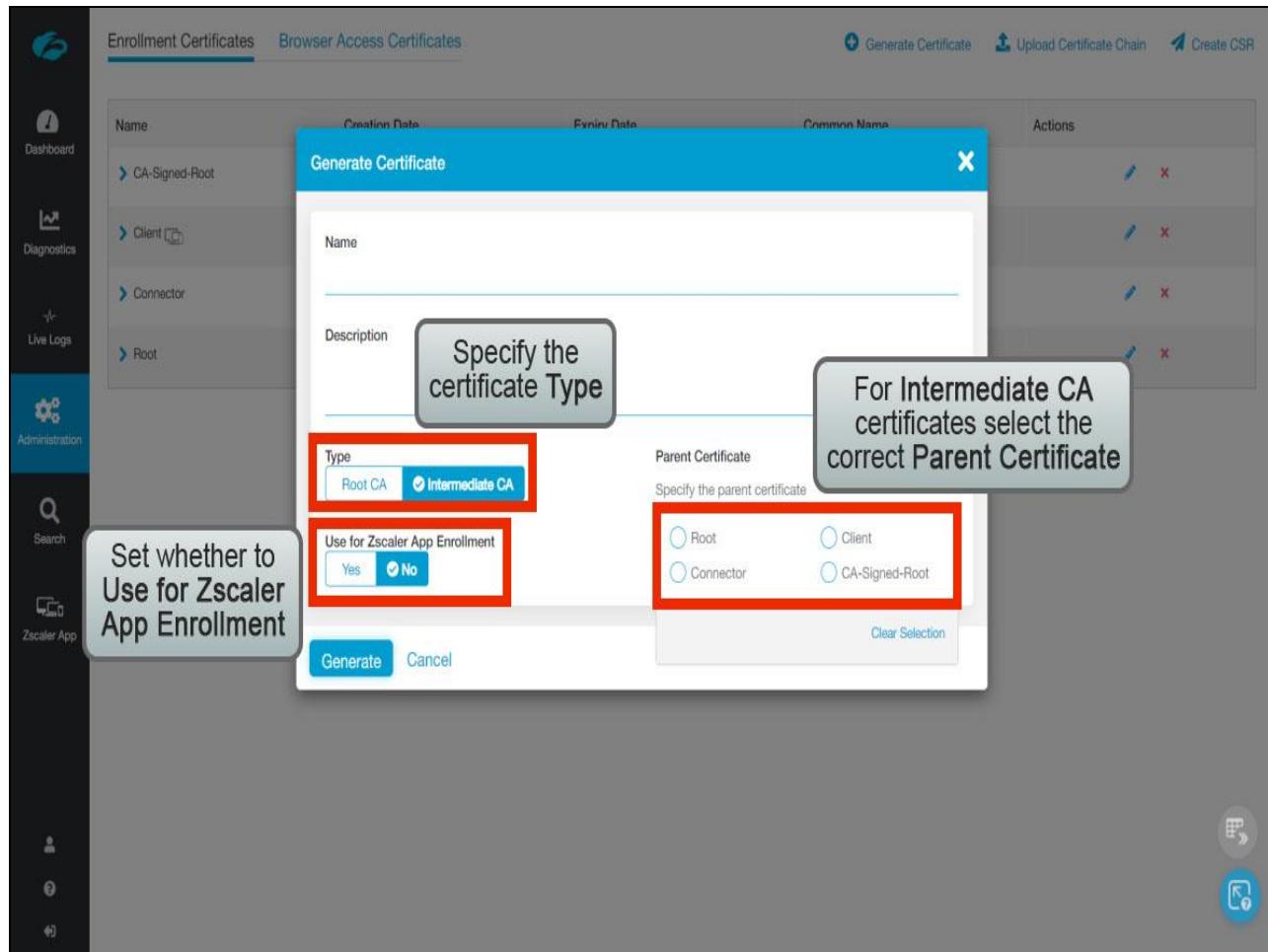
A large callout box labeled 'Click Generate Certificate' points to the 'Generate Certificate' button at the top right. Another callout box labeled 'Edit or Delete certificates' points to the 'Actions' column, which contains edit and delete icons for each certificate row. The 'Actions' column is highlighted with a red box.

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 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

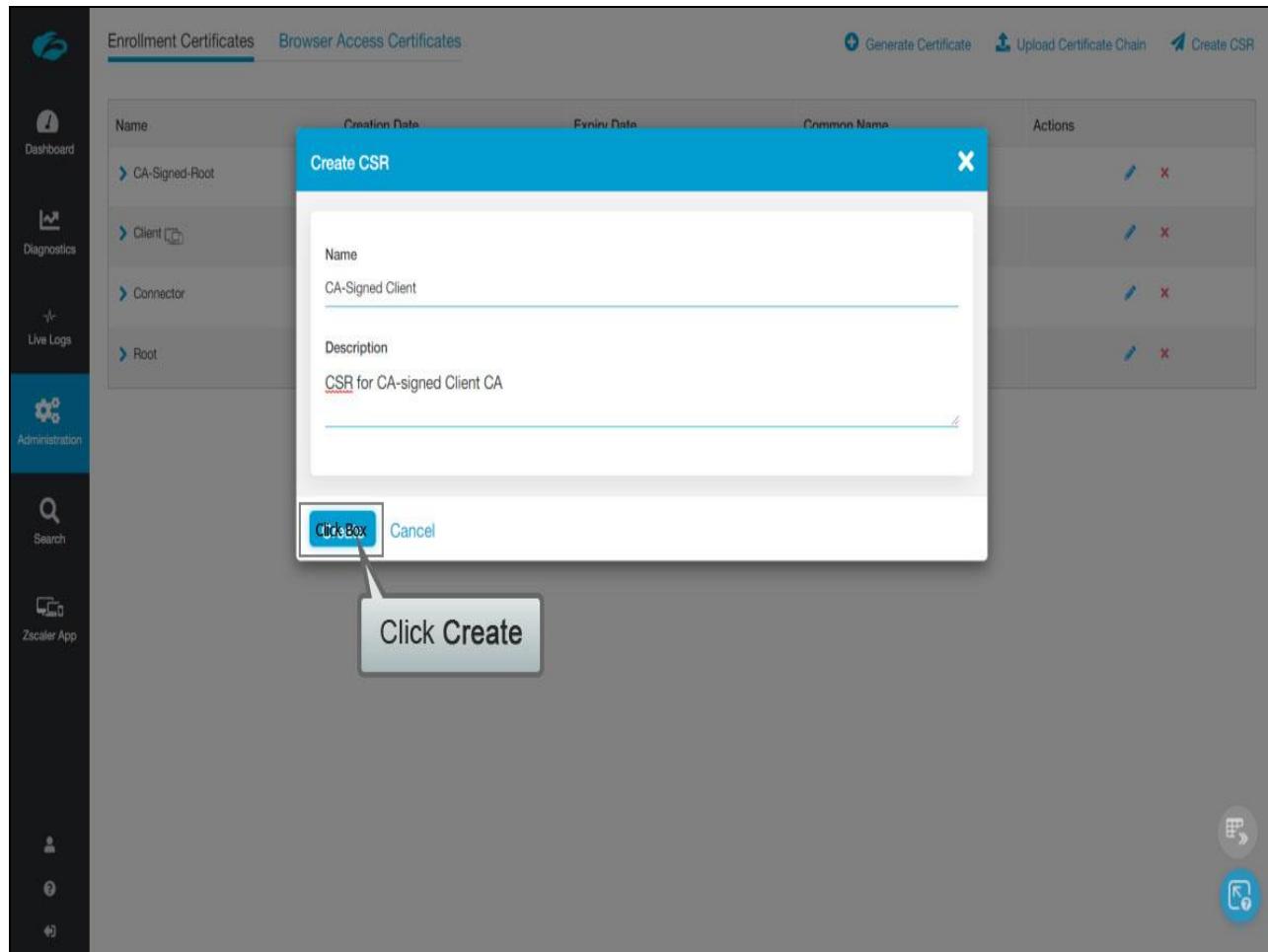
The screenshot shows the Adobe Captivate interface with the 'Enrollment Certificates' tab selected. The main area displays a table of certificates with columns for Name, Creation Date, Expiry Date, and Common Name. Four certificates are listed: CA-Signed-Root, Client, Connector, and Root. Each row has edit and delete icons. A callout box with the text 'Click Create CSR' points to the 'Generate Certificate' button at the top right of the table area.

Name	Creation Date	Expiry Date	Common Name
CA-Signed-Root	Wednesday, June 19 2019 5:18:11 pm	Monday, June 05 2023 6:30:16 pm	patraining12-HOST-1-CA
Client	Thursday, February 15 2018 1:20:05 am	Friday, February 11 2033 1:20:04 am	patraining.safemarch.com/Client
Connector	Thursday, February 15 2018 1:20:06 am	Friday, February 11 2033 1:20:05 am	patraining.safemarch.com/Connector
Root	Thursday, February 15 2018 1:20:03 am	Saturday, February 08 2048 1:20:03 am	patraining.safemarch.com/Root

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

The screenshot shows the Adobe Captivate interface with the 'Administration' sidebar open. The main content area displays a table of enrollment certificates. The table has columns for Name, Creation Date, Expiry Date, Common Name, and Actions. The 'Actions' column contains edit and delete icons. A green banner at the bottom right indicates a 'Certificate Signing Request (CSR) created'.

Name	Creation Date	Expiry Date	Common Name	Actions
CA-Signed Client	Wednesday, June 19 2019 5:19:35 pm			
CA-Signed-Root	Wednesday, June 19 2019 5:18:11 pm	Monday, June 05 2023 6:30:16 pm	patraining12-HOST-1-CA	
Client	Thursday, February 15 2018 1:20:05 am	Friday, February 11 2033 1:20:04 am	patraining.safemarch.com/Client	
Connector	Thursday, February 15 2018 1:20:06 am	Friday, February 11 2033 1:20:05 am	patraining.safemarch.com/Connector	
Root	Thursday, February 15 2018 1:20:03 am	Saturday, February 08 2048 1:20:03 am	patraining.safemarch.com/Root	

Slide notes

Slide 55 - Slide 55

The screenshot shows the 'Enrollment Certificates' tab selected in the Adobe Captivate interface. The main area displays a table of certificates with columns for Name, Creation Date, Expiry Date, Common Name, and Actions. A red box highlights the first row, 'CA-Signed Client', which has a yellow background. A callout bubble with the text 'Certificate added in a Pending state' points to this row. Another callout bubble with the text 'Click to Edit this entry' points to the edit icon in the Actions column of the same row. The left sidebar contains navigation links for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help.

Name	Creation Date	Expiry Date	Common Name	Actions
CA-Signed Client	Wednesday, June 19 2019 5:19:35 pm			Click Box X
CA-Signed-Root	Monday, June 05 2023 6:30:16 pm		patraining12-HOST-1-CA	X
Client	Friday, February 11 2033 1:20:04 am		patraining.safemarch.com/Clien	X
Connector	Thursday, February 15 2018 1:20:06 am	Friday, February 11 2033 1:20:05 am	patraining.safemarch.com/Connector	Click to Edit this entry X
Root	Thursday, February 15 2018 1:20:03 am	Saturday, February 08 2048 1:20:03 am	patraining.safemarch.com/Root	Click to Edit this entry X

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

The screenshot shows the Adobe Captivate interface with the 'Enrollment Certificates' tab selected. A modal dialog box titled 'Upload Signed Certificate' is open. Inside the dialog, there are fields for 'Name' (set to 'CA-Signed Client'), 'Description' (set to 'CSR for CA-signed Client CA'), and a 'Certificate' section. A large button labeled 'Select File' is highlighted with a red box. Below the certificate section, a 'Certificate Signing Request' is displayed as a long string of text. At the bottom of the dialog, there are three buttons: 'Upload' (highlighted with a red box), 'Download .CSR File' (highlighted with a red box), and 'Cancel'. The background shows a list of certificates in the 'Actions' column.

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

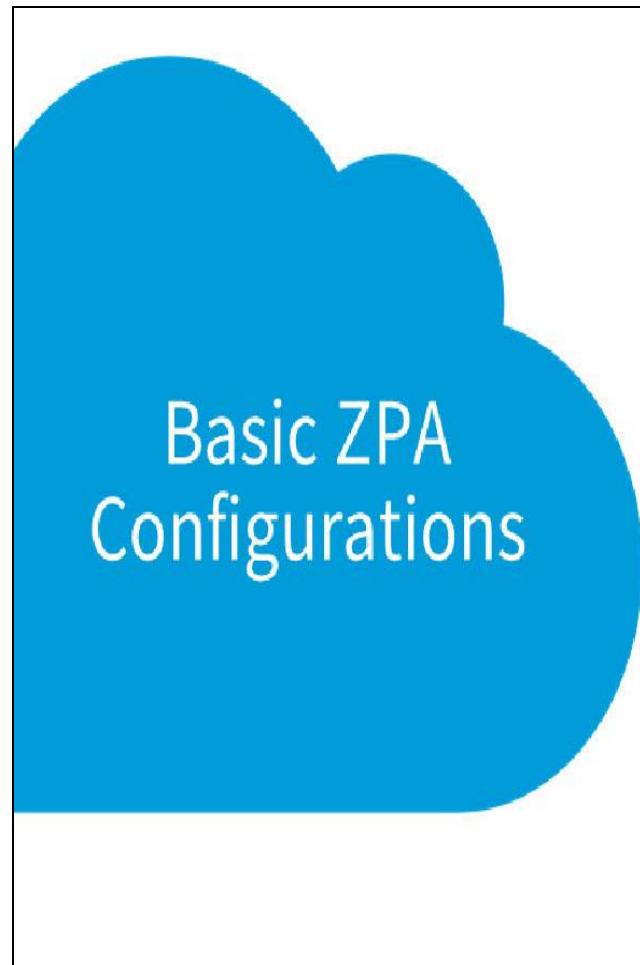
The screenshot shows the Zscaler Admin interface with the 'Enrollment Certificates' tab selected. The main area displays a table of certificates with columns: Name, Creation Date, Expiry Date, Common Name, and Actions. The table contains five rows of data:

Name	Creation Date	Expiry Date	Common Name	Actions
CA-Signed Client	Wednesday, June 19 2019 5:19:35 pm			Edit Delete
CA-Signed-Root	Wednesday, June 19 2019 5:18:11 pm	Monday, June 05 2023 6:30:16 pm	patraining12-HOST-1-CA	Edit Delete
Client	Thursday, February 15 2018 1:20:05 am	Friday, February 11 2033 1:20:04 am	patraining.safemarch.com/Client	Edit Delete
Connector	Thursday, February 15 2018 1:20:06 am	Friday, February 11 2033 1:20:05 am	patraining.safemarch.com/Connector	Edit Delete
Root	Thursday, February 15 2018 1:20:03 am	Saturday, February 08 2048 1:20:03 am	patraining.safemarch.com/Root	Edit Delete

The left sidebar includes links for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. A bottom navigation bar shows the URL <https://admin.private.zscaler.com/#clientlessCerts>.

Slide notes

Slide 58 - Basic ZPA Configurations

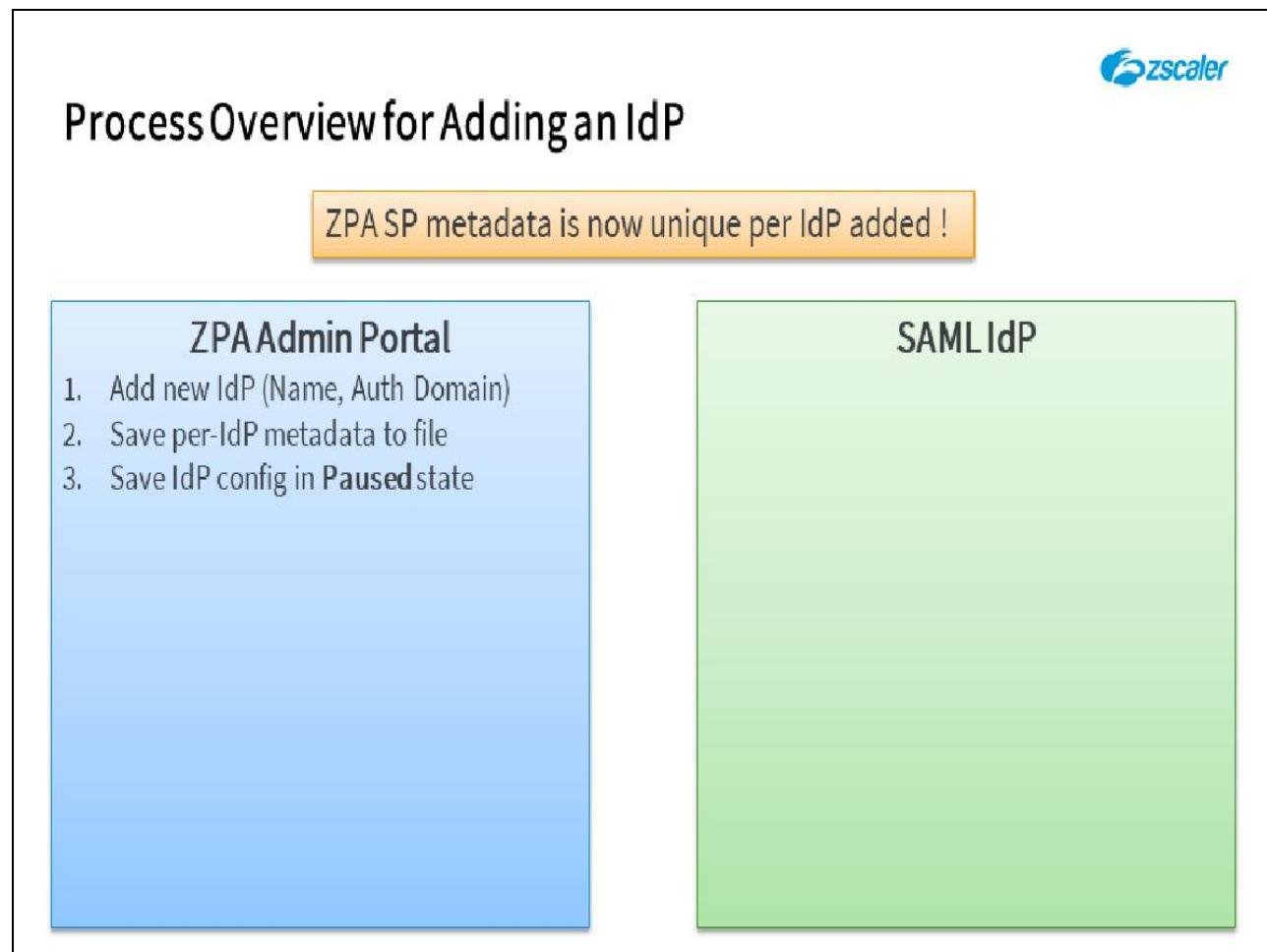


1. Update Company and Administrator Data
2. Configuring Certificates
3. Configure Single Sign-On

Slide notes

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

Slide 59 - Process Overview for Adding an IdP

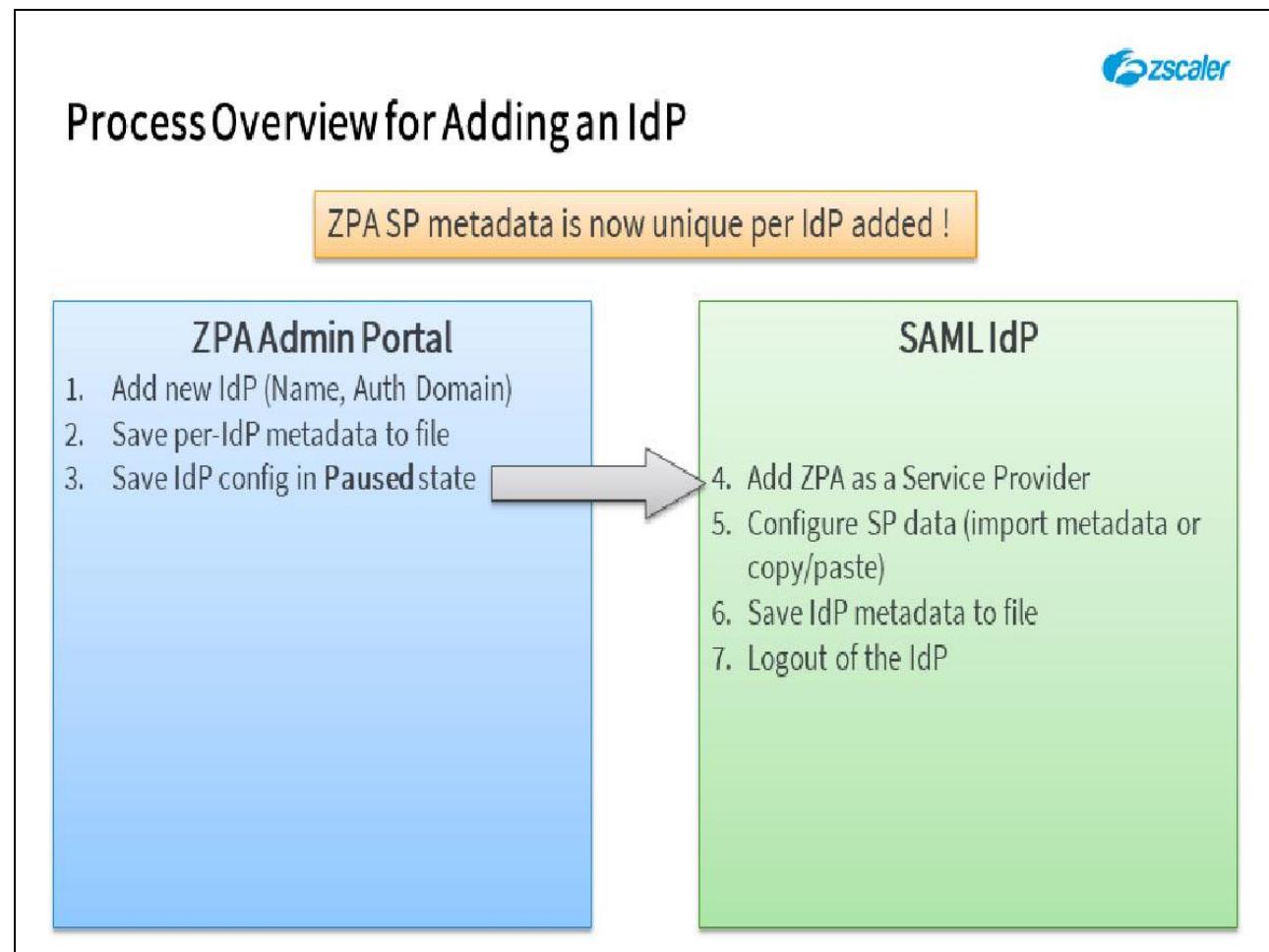


Slide notes

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

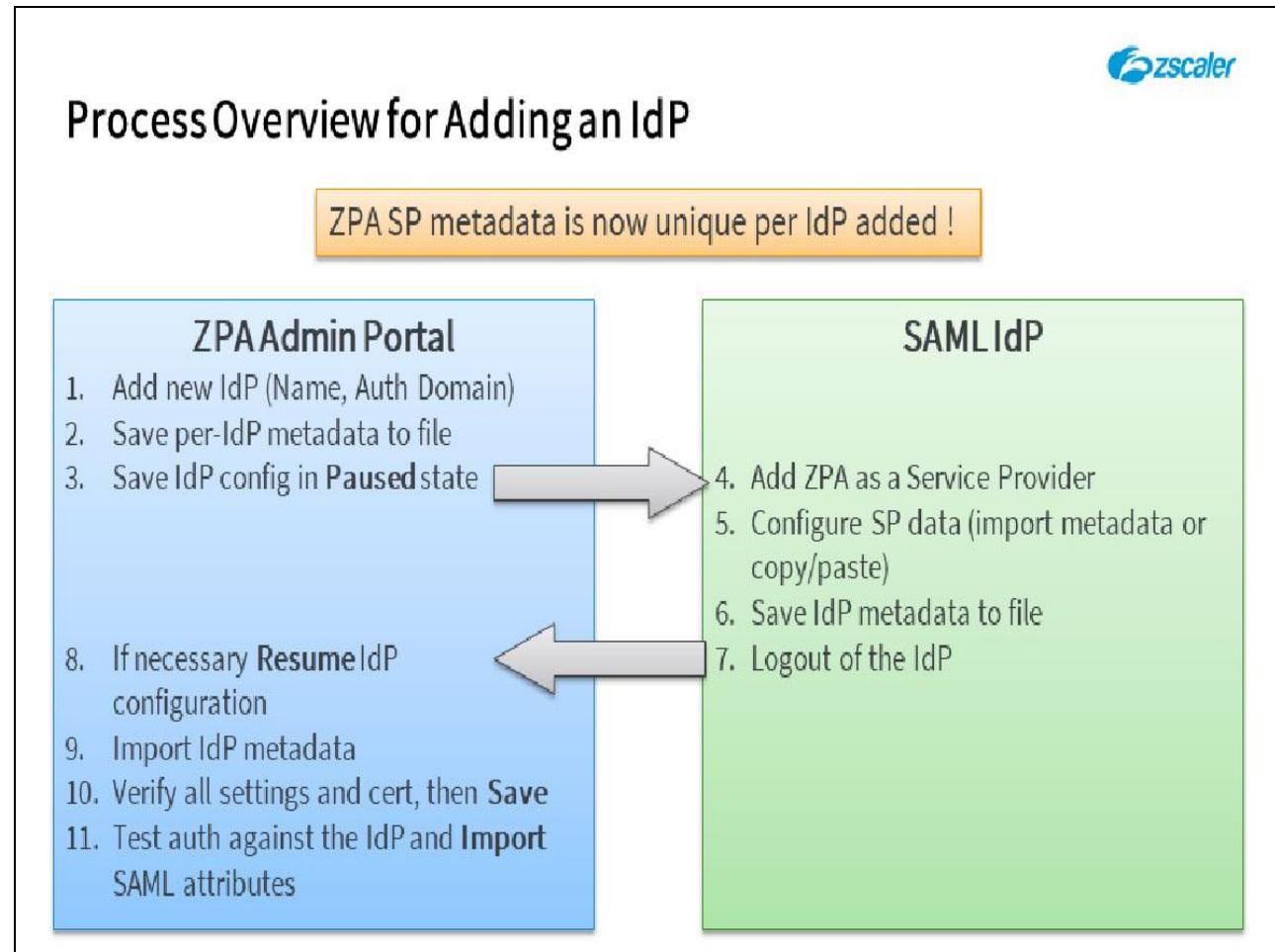


Slide notes

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).

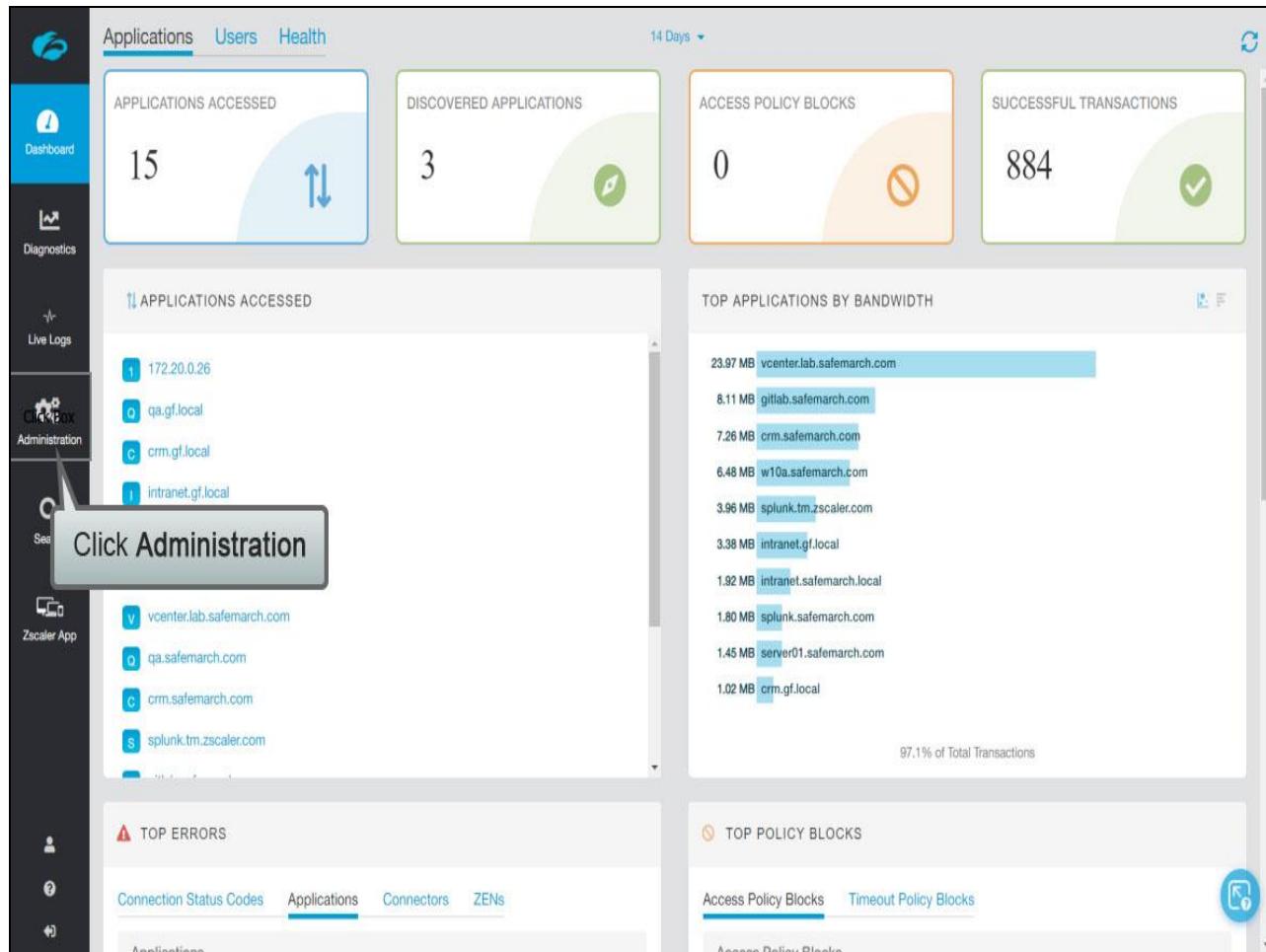
Slide 61 - Process Overview for Adding an IdP



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

The screenshot shows the Zscaler Cloud interface. On the left is a dark sidebar with various icons and links:

- APPLICATION MANAGEMENT**: Application Segments, Browser Access Certificates, Server Groups.
- AUTHENTICATION**: IdP Configuration, Settings (highlighted with a callout box labeled "Click Settings").
- Diagnostics**
- Live Logs**
- Administration**
- SEARCH**
- Zscaler App**
- POLICY MANAGEMENT**: Access Policy, Timeout Policy.
- SETTINGS**: Administrators, Company, Audit Logs, Roles.

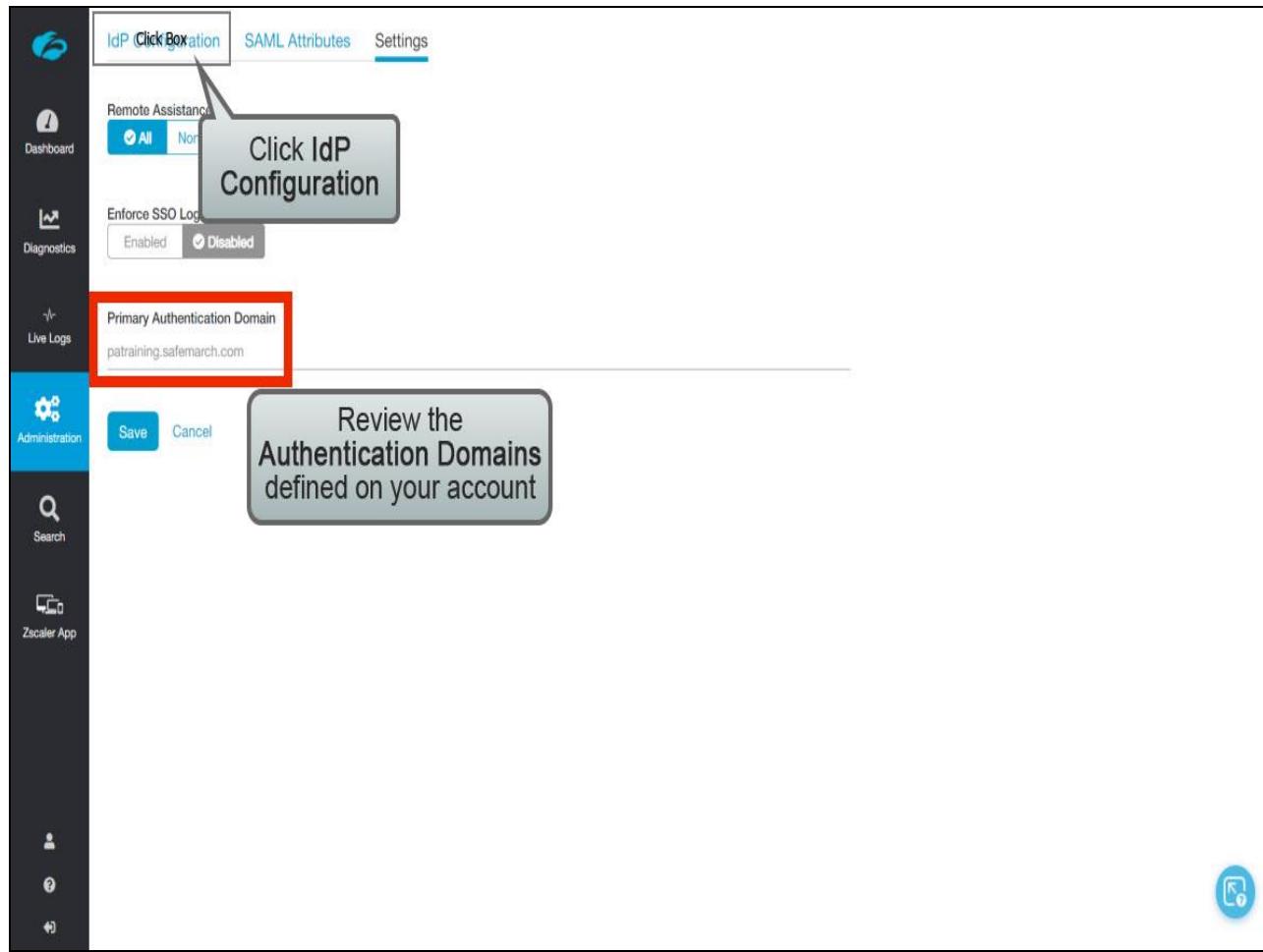
The main content area displays several cards:

- 14 Days** (dropdown).
- PERMISSIONED APPLICATIONS**: 0 (green icon).
- ACCESS POLICY BLOCKS**: 0 (orange icon).
- SUCCESSFUL TRANSACTIONS**: 884 (green icon).
- TOP APPLICATIONS BY BANDWIDTH**: A chart showing bandwidth usage for various domains. The top entry is vcenter.lab.safemarch.com at 23.97 MB.
- 97.1% of Total Transactions**.
- TOP POLICY BLOCKS**: A card showing policy blocks. The tab "Access Policy Blocks" is selected, showing 0 blocks.

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

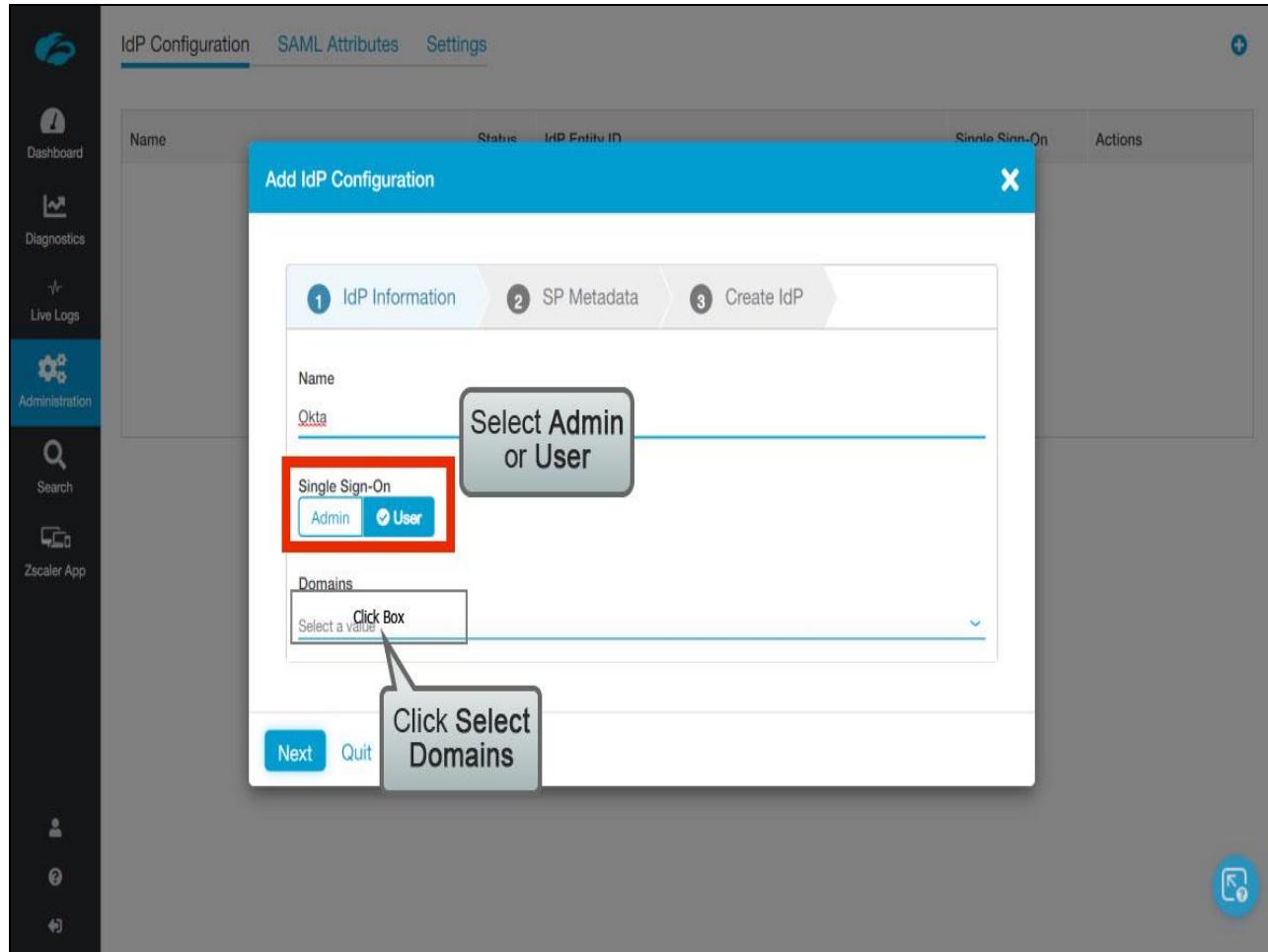
The screenshot shows the Adobe Captivate interface with the following details:

- Left Sidebar:** Contains icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help.
- Top Navigation:** Includes links for IdP Configuration (selected), SAML Attributes, and Settings.
- Main Content Area:** Titled "IdP Configuration". It features a table with columns: Name, Status, IdP Entity ID, and Single Sign-On. A message "No Items Found" is displayed below the table.
- Callout:** A blue-bordered box with a white background and a black arrow points to the "Click +" button located in the top right corner of the main content area.

Slide notes

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

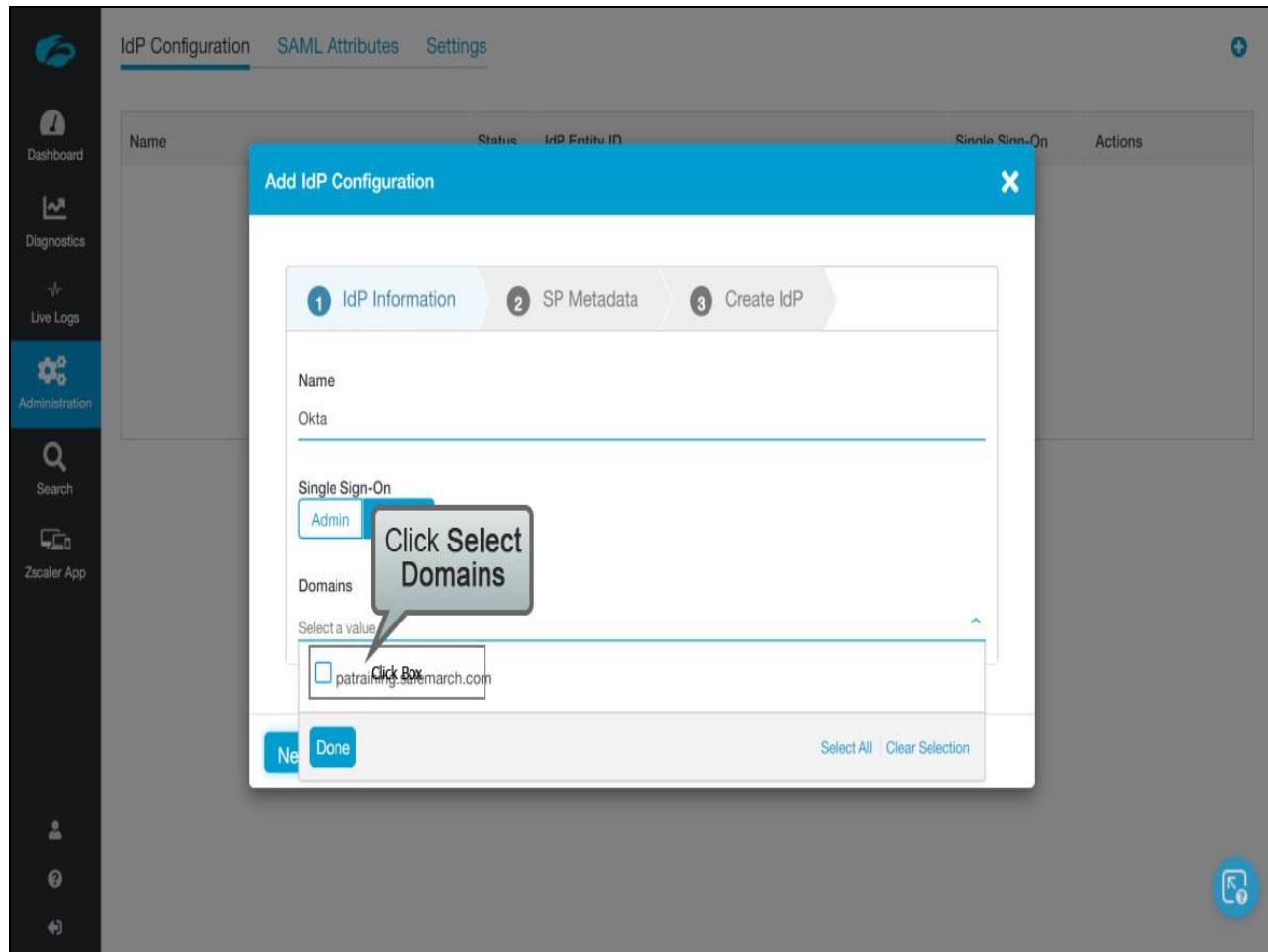
Slide 66 - Slide 66



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.

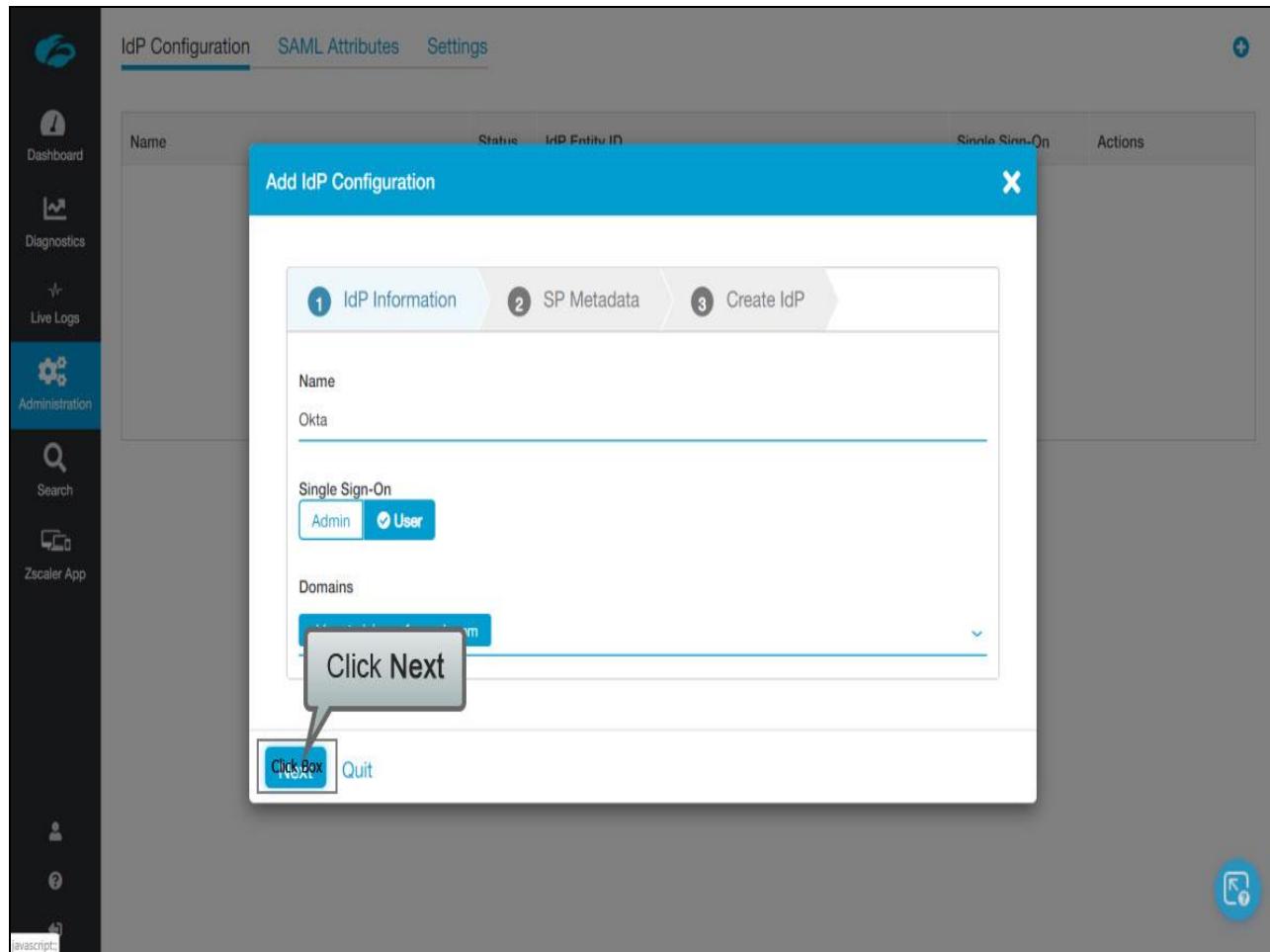
Slide 68 - Slide 68

The screenshot shows the Adobe Captivate interface with a dark theme. On the left, there is a vertical sidebar with various icons and sections: Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help. The main area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. A modal window titled "Add IdP Configuration" is open, divided into three steps: 1. IdP Information, 2. SP Metadata, and 3. Create IdP. Step 1 is active, showing a "Name" field with "Okta" typed in. Under "Single Sign-On", the "User" radio button is selected. In the "Domains" section, a list of domains is shown, with one domain highlighted. A callout bubble points to the "Done" button at the bottom of the list, with the text "Click Done". At the bottom right of the modal, there are "Select All" and "Clear Selection" buttons.

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

The screenshot shows the Zscaler Admin Portal interface. The left sidebar has a dark theme with blue highlights for the selected 'Administration' tab. The main content area has a light gray header with three tabs: 'IdP Configuration' (selected), 'SAML Attributes', and 'Settings'. Below the header is a table with columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. A single row is visible, showing 'Okta' in the Name column, a green 'OK' status icon in the Status column, and 'User' in the Single Sign-On column. The Actions column contains a blue circular icon with a white plus sign and a red circular icon with a white minus sign. The bottom right corner of the main area features a blue circular icon with a white square and a small '0'.

Name	Status	IdP Entity ID	Single Sign-On	Actions
Okta	OK		User	

Slide notes

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

Slide 72 - Slide 72

The screenshot shows the Okta Applications page. The top navigation bar includes links for Dashboard, Directory, Applications (which is highlighted with a red box), Security, Reports, Settings, and My Applications. A search bar at the top left contains the text 'zsclaler'. Below the search bar, there is a grid of application cards. One card for 'Zscaler 2.0' has a callout bubble pointing to its 'Add' button with the text 'Click Box' inside. Other visible cards include 'Zscaler Admin Login', 'Zscaler Private Access 1.0', 'Zscaler Private Access 2.0', '101domains.com', and '10kft Connector by Aquera'. The bottom of the screen shows categories like 'Supports Provisioning', 'CATEGORIES', and 'API Management'.

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

The screenshot shows the Okta application configuration interface. At the top, there's a yellow banner with the text "Preview Sandbox: This is a preview of next week's release. See a problem? File a case or visit our support site". Below the banner, the Okta navigation bar includes links for A. PATraining, Safemarch ZPA, Help and Support, and Sign out. The main header "okta" has sub-links for Dashboard, Directory, Applications, Security, Reports, and Settings. To the right of the header is a "My Applications" button with a plus sign.

The main content area shows a card for "Add Zscaler Private Access 2.0". Inside the card, a sub-card titled "General Settings · Required" is displayed. This sub-card contains fields for "Application label" (set to "Zscaler Private Access 2.0") and "Application Visibility" (with two checkboxes: "Do not display application icon to users" and "Do not display application icon in the Okta Mobile App").

To the right of the sub-card, there's a "General settings" section with the note: "All fields are required to add this application unless marked optional." Below this, a "Click Done" callout points to a green "Click Box" button at the bottom of the sub-card.

At the bottom of the page, there are footer links: © 2019 Okta, Inc., Privacy, Version 2019.06.2, OPI Preview Cell (US), Status site, Download Okta Plugin, and Feedback.

Slide notes

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

Slide 74 - Slide 74

Preview Sandbox: This is a preview of next week's release. See a problem? [File a case](#) or visit our [support site](#).

A. PATraining · Safemarch ZPA · Help and Support · Sign out

okta · Dashboard · Directory · Applications · Security · Reports · Settings · My Applications

← Back to Applications

Zscaler Drive Access 2.0 · Click Sign On · New Logs

General · Click Box · Import · **Assignments**

Assign · Convert Assignments · Groups

FILTERS · Priority · Assignment

People · 1 · Marketing · Marketing Group · **Groups**

Assign the Application to users as required

REPORTS · Current Assignments · Recent Unassignments

SELF SERVICE · You need to enable self service for org managed apps before you can use self service for this app. · Go to self service settings · Requests · Disabled · Approval

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

The screenshot shows the Okta application configuration interface for the Zscaler Private Access 2.0 application. At the top, there is a yellow banner with the text "Preview Sandbox: This is a preview of next week's release. See a problem? File a case or visit our support site". Below the banner, the Okta navigation bar includes links for Dashboard, Directory, Applications, Security, Reports, Settings, and My Applications.

The main content area displays the Zscaler Private Access 2.0 application details. It shows the application icon (Zscaler logo), the name "Zscaler Private Access 2.0", and status indicators for "Active" and "View Logs". Below this, there are tabs for General, Sign On (which is highlighted with a red box and a callout bubble labeled "Click Box"), Import, and Assignments.

In the "Sign On Methods" section, it is noted that the sign-on method determines how a user signs into and manages their credentials. A note states: "The sign-on method determines how a user signs into and manages their credentials. Some sign-on methods require additional configuration in the 3rd party application." A link "Configure profile mapping" is provided. A radio button is selected for "SAML 2.0".

The "Default Relay State" field contains the URL: https://patraining-admin.oktapreview.com/admin/app/zscaler_private_access/instance/001qr...

On the right side, there is an "About" section describing SAML 2.0 and its integration with Okta. It also includes fields for "Application Username" and "Application Password". A note states: "Choose a format to use as the default username value when assigning the application to users. If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features."

Slide notes

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

Slide 76 - Slide 76

The screenshot shows the 'SAML 2.0' configuration page. At the top, there's a section for 'Default Relay State' with a text input field and a note: 'All IDP-initiated requests will include this RelayState'. Below it is a checkbox for 'Disable Force Authentication' with the sub-note: 'Never prompt user to re-authenticate.' A dropdown for 'GroupName' is set to 'None'. A yellow sidebar on the left contains a 'View Setup Instructions' button, which is highlighted with a red rectangle and a callout bubble labeled 'Setup Instructions'. To the right of the sidebar, a note says: 'If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.' The main configuration area is outlined with a red border and contains two sections: 'ADVANCED SIGN-ON SETTINGS' and 'Service Provider URL and Entity ID fields'. The 'ADVANCED SIGN-ON SETTINGS' section has a note: 'These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.' It includes 'Service Provider URL' and 'Service Provider Entity ID' fields, each with a note: 'Please enter your Service Provider URL/Entity ID. Refer to the Setup Instructions above to obtain this value.' A callout bubble labeled 'Service Provider URL and Entity ID fields' points to these two fields.

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

The screenshot shows the Zscaler Admin Portal interface. On the left is a dark sidebar with various icons and labels: Dashboard, Diagnostics, Live Logs, Administration (which is selected and highlighted in blue), Search, Zscaler App, and three other icons with question marks. The main content area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. There is one row in the table with the name 'Click Box', status 'Up', IdP Entity ID 'User', and actions represented by a blue gear icon and a red X icon. A large gray callout box with a black border and rounded corners is positioned over the first column of the table. Inside the callout box, the text 'Click to expand the IdP' is displayed. An arrow points from the top-left corner of the callout box towards the 'Click Box' button in the table.

Slide notes

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

Slide 78 - Slide 78

The screenshot shows the Zscaler Admin UI interface. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main area has tabs for IdP Configuration, SAML Attributes, and Settings, with IdP Configuration selected. A table lists an entry for 'Okta'. Below the table, under 'SERVICE PROVIDER SAML METADATA FOR USER SSO', there are fields for Service Provider Metadata (with a 'Download Metadata' link), Service Provider URL (highlighted with a green background and a context menu), Service Provider Certificate (with a 'Download Certificate' link), and Service Provider Entity ID (with a link). A context menu is open over the Service Provider URL field, with a callout box containing the text 'Click Copy' pointing to the 'Copy' option. Other menu items include 'Ctrl+C', 'Ctrl+P', and 'Ctrl+Shift+I'. A blue circular icon with a copy symbol is in the bottom right corner.

Slide notes

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

Slide 79 - Slide 79

SAML 2.0 is not configured until you complete the setup instructions.
[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL
Please enter the URL. Refer to the Setup guide.

Service Provider Entity ID
Please enter the Entity ID. Refer to the Setup guide.

CREDENTIALS DETAILS

Application username format
Click Paste

Update application username on Create and update

Password reveal
 Allow users to securely see their password (Recommended)
i Password reveal is disabled, since this app is using SAML with no password.

A context menu is open over the "Click Paste" button, listing options: Emoji, Win+Period, Undo (Ctrl+Z), Redo (Ctrl+Shift+Z), Cut (Ctrl+X), Copy (Ctrl+C), Paste as plain text (Ctrl+Shift+V), Select all (Ctrl+A), Spellcheck, and Writing Direction.

Slide notes

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

Slide 80 - Slide 80

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL

Please enter your Service Provider URL. Refer to the Setup Instructions above to obtain this value.

Service Provider Entity ID

Please enter your Service Provider Entity ID. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

Application username format

Update application username on

Password reveal Allow users to securely see their password (Recommended)

i Password reveal is disabled, since this app is using SAML with no password.

Slide notes

Switch back to the ZPA Admin Portal, ...

Slide 81 - Slide 81

The screenshot shows the Adobe Captivate interface with the 'Administration' tab selected in the sidebar. The main area displays the 'IdP Configuration' screen for Okta SSO. Key details shown include:

- Name:** Okta
- Status:** Enabled (indicated by a green circle)
- IdP Entity ID:** https://samlsp.private.zscaler.com/auth/144123139134062747/sso
- Single Sign-On URL:** ZPA (SP) SAML Request
- HTTP-Redirect:** Disabled (indicated by a red circle)
- Signed:** Signed (indicated by a green circle)
- Authentication Domains:** patraining.safemarch.com

Below these settings, there are sections for 'SERVICE PROVIDER SAML METADATA FOR USER SSO' and 'ZSCALER APP'. The 'Service Provider Metadata' section includes a 'Download Metadata' button and a 'Service Provider Certificate' download link. The 'Service Provider URL' section shows the URL again. A context menu is open over the Service Provider Entity ID field, with a callout bubble containing the text 'Click Copy'. The menu options visible are:

- Copy (Ctrl+C)
- Print...
- Inspect (Ctrl+Shift+I)

Slide notes

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

Slide 82 - Slide 82

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL

Please enter your Service Provider URL. Refer to the Setup Instructions above to obtain this value.

Service Provider Entity ID

CREDENTIALS DETAILS

Application username format

Update application user

>Password reveal Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

Slide notes

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

Slide 83 - Slide 83

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Zscaler Private Access 2.0 proprietary sign-on option or general setting.

Service Provider URL

Please enter your Service Provider URL. Refer to the Setup Instructions above to obtain this value.

Service Provider Entity ID

Please enter your Service Provider Entity ID. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

Application username format

Update application username on

Password reveal Allow users to securely see their password (Recommended)

i Password reveal is disabled, since this app is using SAML with no password.

Scroll down...

Slide notes

Scroll down if necessary, ...

Slide 84 - Slide 84

The screenshot shows the Okta Sign On Policy configuration page. At the top, there is a note about Password reveal being disabled due to SAML usage. Below this, a 'Click Box' highlights the 'Click Save' button. The main section displays a table of rules:

Priority	Rule name	Status	Actions
1	Default sign on rule	Active	Not editable

Under the 'Default sign on rule' row, the 'CONDITIONS' and 'ACTIONS' sections are expanded. The 'CONDITIONS' section contains 'User assigned this app' and 'Anywhere'. The 'ACTIONS' section contains 'Allow access'.

Sign On Policy

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific user or group of users is off network.

Every application starts with a default rule that allows access to anyone assigned the app from anywhere.

Rule Priority

You can determine rule precedence by setting the priority number. For example, a rule with a priority value of 1 has first priority and takes precedence over all other rules.

At the bottom of the page, there are links for © 2019 Okta, Inc., Privacy, Version 2019.06.2, OPI Preview Cell (US), Status site, Download Okta Plugin, and Feedback.

Slide notes

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

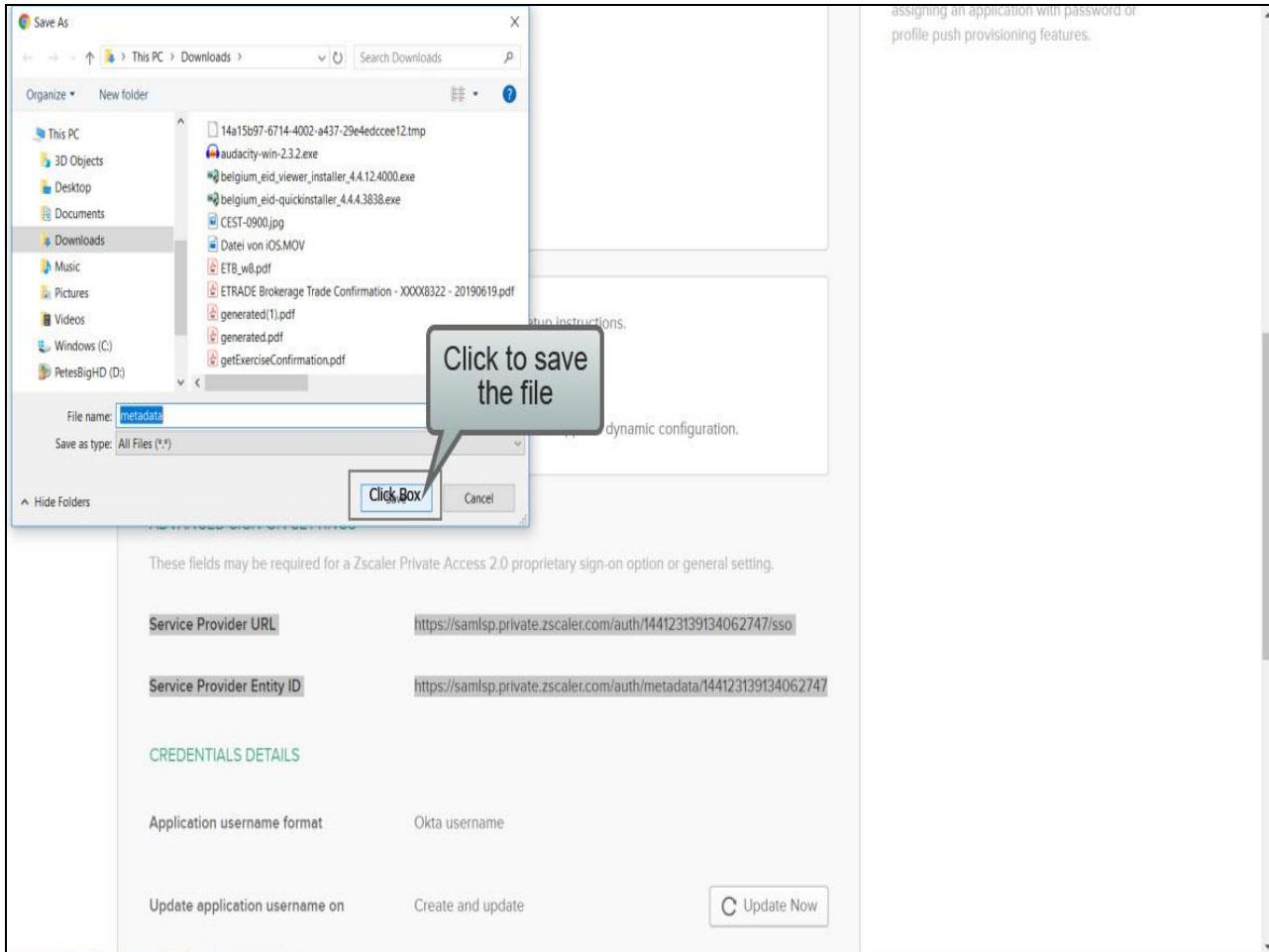
Slide 85 - Slide 85

The screenshot shows the configuration page for a Zscaler Private Access 2.0 application in Okta. The page includes sections for Default Relay State, Disable Force Authentication (checked), GroupName (None), and Advanced Sign-On Settings. A yellow callout box highlights the 'Click to download IdP Metadata' link, which is located under the SAML 2.0 configuration section. The link is preceded by an 'Identity Click Box' icon. Below this, there are Service Provider URL and Entity ID fields, both containing URLs starting with <https://samlsp.private.zscaler.com/auth/>. The CREDENTIALS DETAILS section shows the Application username format as 'Okta username'. At the bottom, there is a 'Create and update' button and a 'C Update Now' button.

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

The screenshot shows the Okta Admin Portal interface. At the top, there's a yellow banner with the text "Preview Sandbox: This is a preview of next week's release. See a problem? File a case or visit our support site". Below the banner is a blue header bar with navigation links: "A. PATraining", "Safemarch ZPA", "Help and Support", "My Applications" (with a dropdown arrow), and a "Click Box" highlighted by a red box. The main content area displays the "Zscaler Private Access 2.0" application card, which includes the Zscaler logo, status "Active", and a "View Logs" button. Below the card are tabs: "General" (selected), "Sign On", "Import", and "Assignments". The "Sign On" tab is expanded, showing the "Settings" section. In this section, there's a "SIGN ON METHODS" section with a note: "SAML 2.0 is the only sign-on option currently supported for this application." A radio button labeled "SAML 2.0" is selected. There's also a "Default Relay State" input field and a note: "All IDP initiated requests will include this RelayState". To the right of the "Settings" section is an "About" section with detailed information about SAML 2.0 integration. At the bottom right of the page, there's a "Click Sign Out" button highlighted by a large red box.

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**.

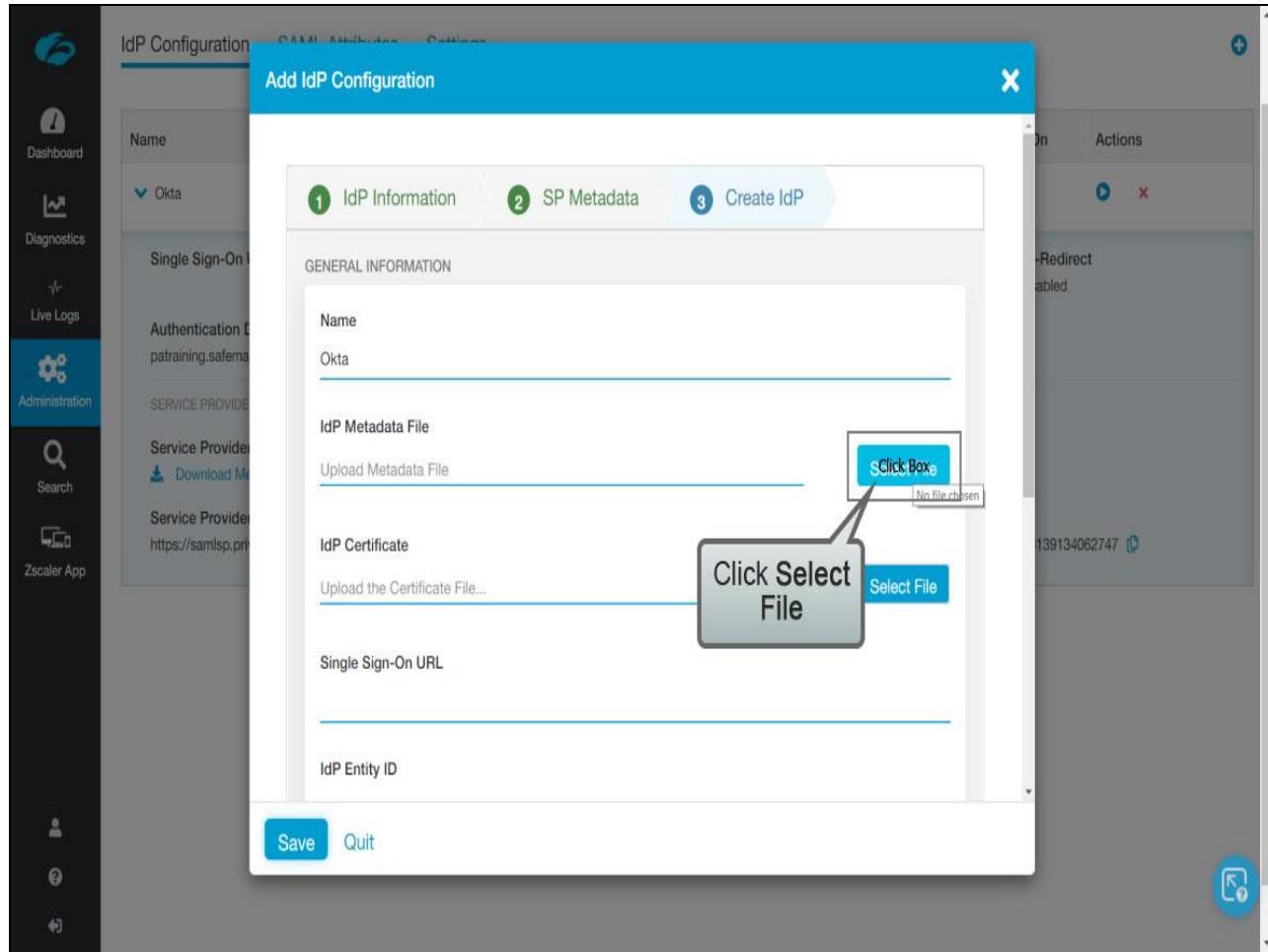
Slide 88 - Slide 88

The screenshot shows the ZPA Admin Portal's IdP Configuration screen. On the left is a navigation sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main content area has tabs for IdP Configuration, SAML Attributes, and Settings, with IdP Configuration selected. A table lists IdPs, with Okta currently selected. The table columns are Name, Status, IdP Entity ID, Single Sign-On, and Actions. The Actions column for Okta contains a 'User' link and a 'Click Box' button. A tooltip for the Click Box button says 'HTTP.Redirect'. Below the table, there are sections for Single Sign-On URL (ZPA (SP) SAML Request, Signed), Authentication Domains (patraining.safemarch.com), Service Provider Metadata (Download Metadata), Service Provider Certificate (Download Certificate), Service Provider URL (https://samlsp.private.zscaler.com/auth/144123139134062747/sso), and Service Provider Entity ID (https://samlsp.private.zscaler.com/auth/metadata/144123139134062747). At the bottom are links for metadata and a search bar.

Slide notes

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

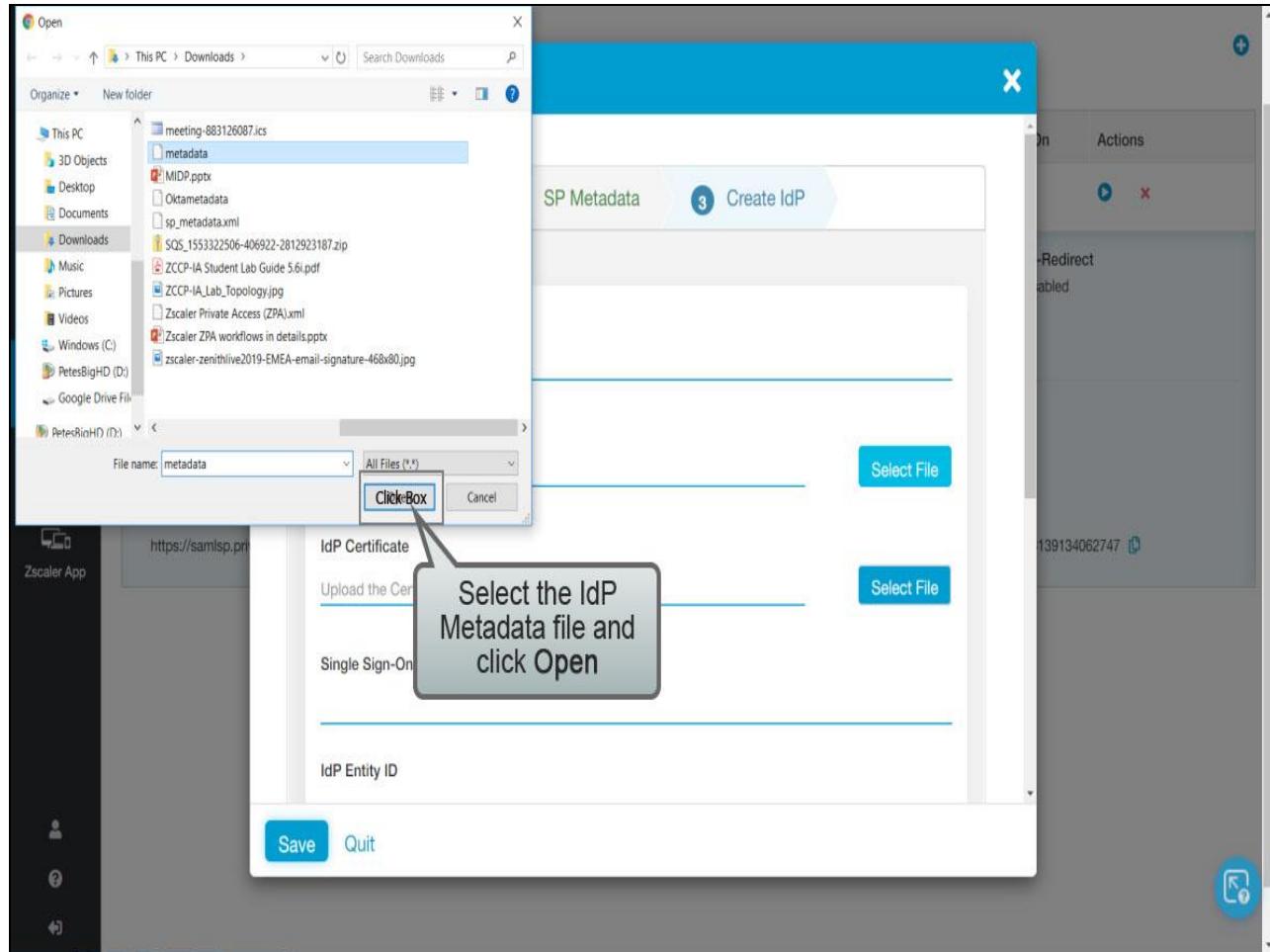
Slide 89 - Slide 89



Slide notes

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

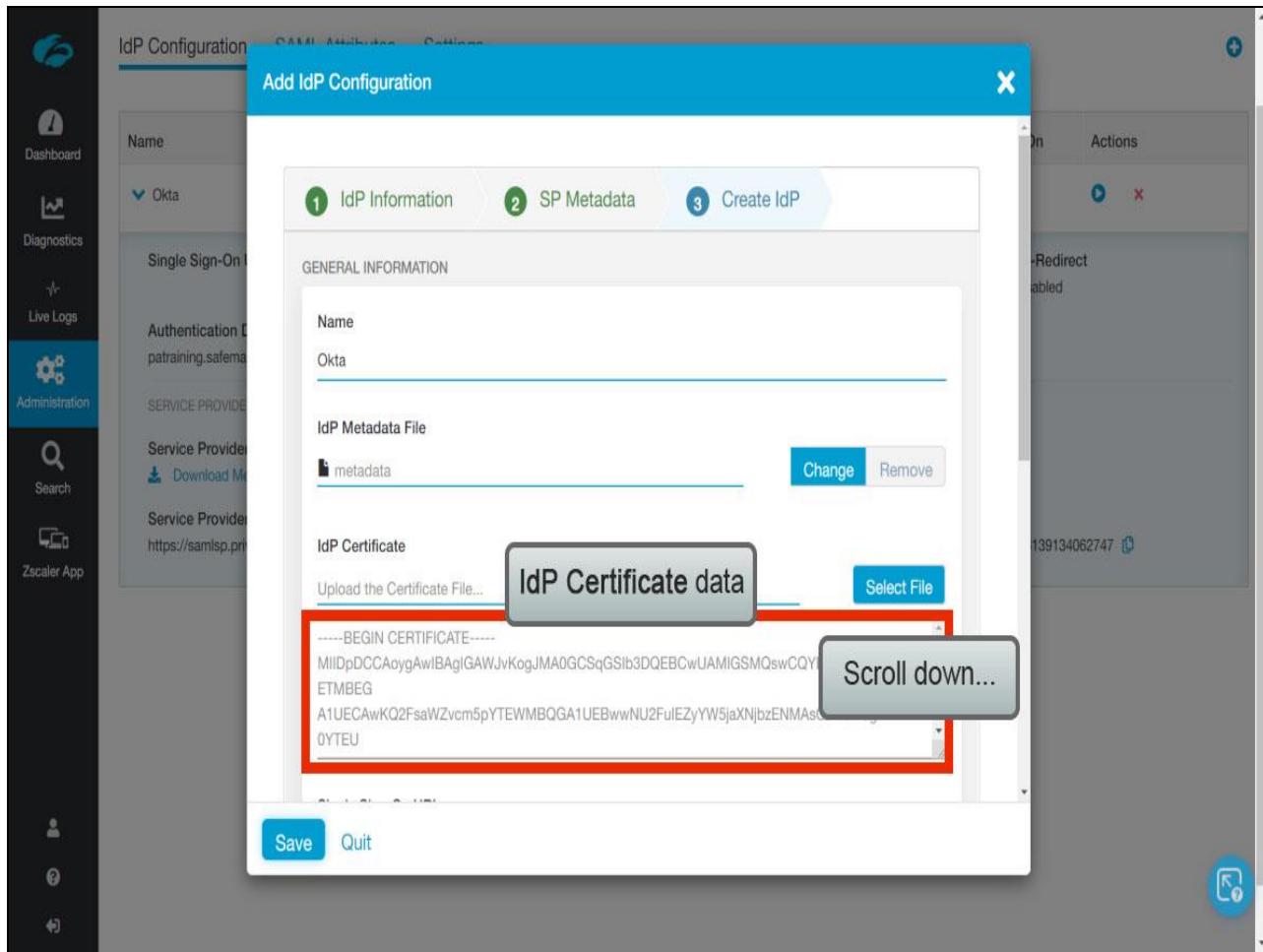
Slide 90 - Slide 90



Slide notes

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

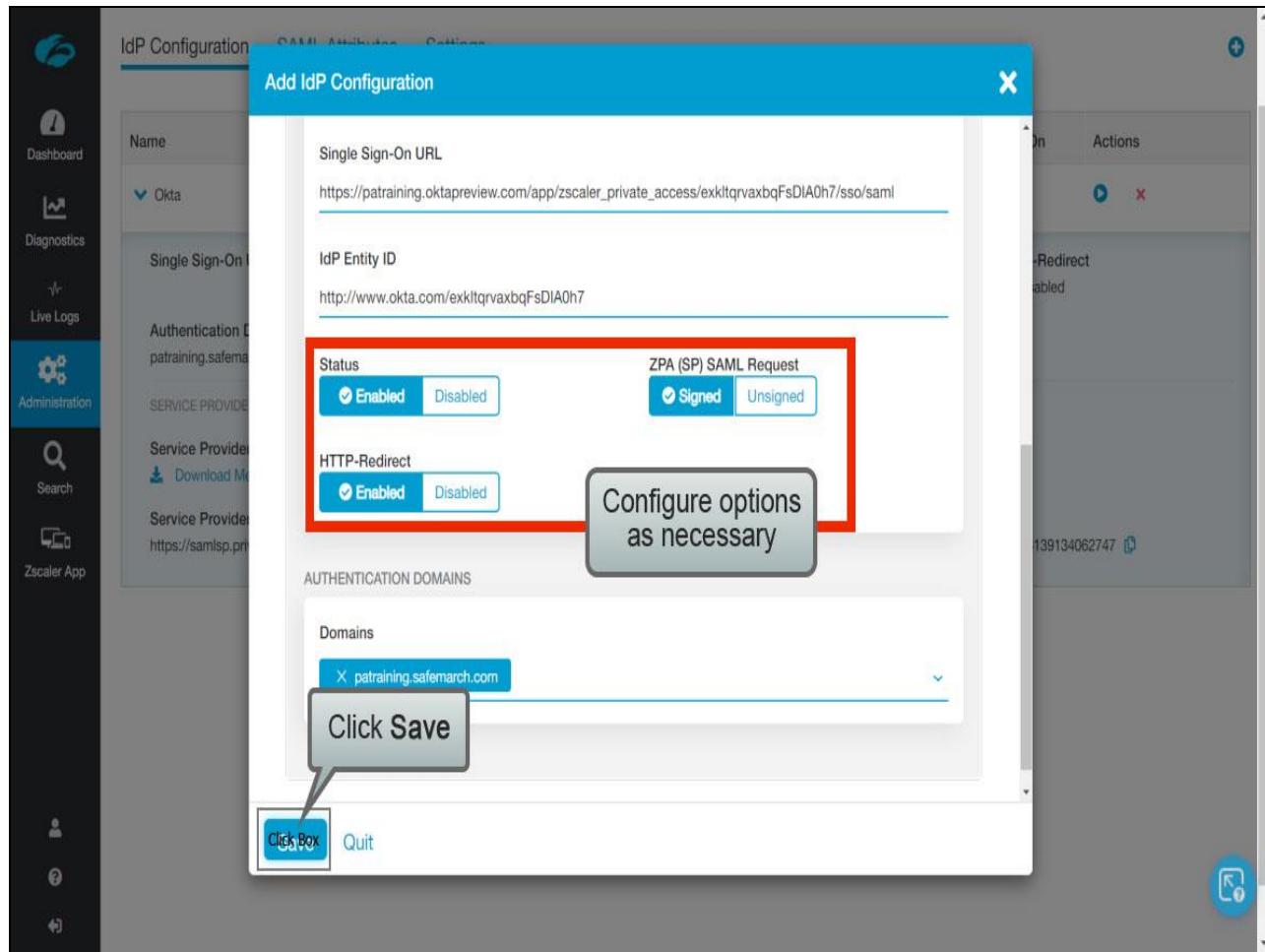
Slide 91 - Slide 91



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

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, Zscaler App, and other user-related options. The main content area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. A single row is present in the table, representing Okta, with a green checkmark icon next to its name. The IdP Entity ID is listed as <http://www.okta.com/exkltqraxbqFsDIAoh7>. The Actions column contains a blue edit icon and a red delete icon. In the bottom right corner of the main area, there is a green success message box with the text "IdP configuration saved" and a blue circular icon containing a white checkmark.

Name	Status	IdP Entity ID	Single Sign-On	Actions
Okta	✓	http://www.okta.com/exkltqraxbqFsDIAoh7	User	

Slide notes

Slide 94 - Slide 94

Name	Status	IdP Entity ID	Single Sign-On	Actions
Click Box	✓	http://www.okta.com/exkltqravxbqFsDIAoh7	User	

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

The screenshot shows the Adobe Captivate application's administration interface. On the left, there is a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, Zscaler App, and Help.

The main content area is titled "IdP Configuration". It displays a table of configurations:

Name	Status	IdP Entity ID	Single Sign-On	Actions
Okta	✓	http://www.okta.com/exkltqrvaxbqFsDIAoh7	User	Edit Delete

Below the table, there are sections for "Single Sign-On URL" (https://patraining.oktapreview.com/app/zscaler_private_access/exkltqrvaxbqFsDIAoh7/sso/saml), "ZPA (SP) SAML Request" (Signed), and "HTTP-Redirect" (Enabled).

The "Import SAML Attributes" section shows "patraining.safemarch.com" selected in a dropdown menu. A "Click Box" annotation is placed over this dropdown. A large callout box labeled "Click Import" points to this section.

Other sections include "SAML Attributes" (with a "Show Attributes" link), "Service Provider Metadata" (with a "Download Metadata" link), "Service Provider URL" (https://samlsp.private.zscaler.com/auth/144123139134062747/sso), "Service Provider Certificate" (with a "Download Certificate" link), "Service Provider Entity ID" (https://samlsp.private.zscaler.com/auth/metadata/144123139134062747), and "IdP CERTIFICATE" (with fields for Common Name (patraining), Serial Number (1522283481097), Created On (Thursday, March 29 2018 7:30:21 am), and Expires On (Wednesday, March 29 2028 7:31:20 am)).

A URL in the address bar at the bottom is https://samlsp.private.zscaler.com/auth/v2/login?domain=patraining.safemarch.com&redirect... .

Slide notes

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

...

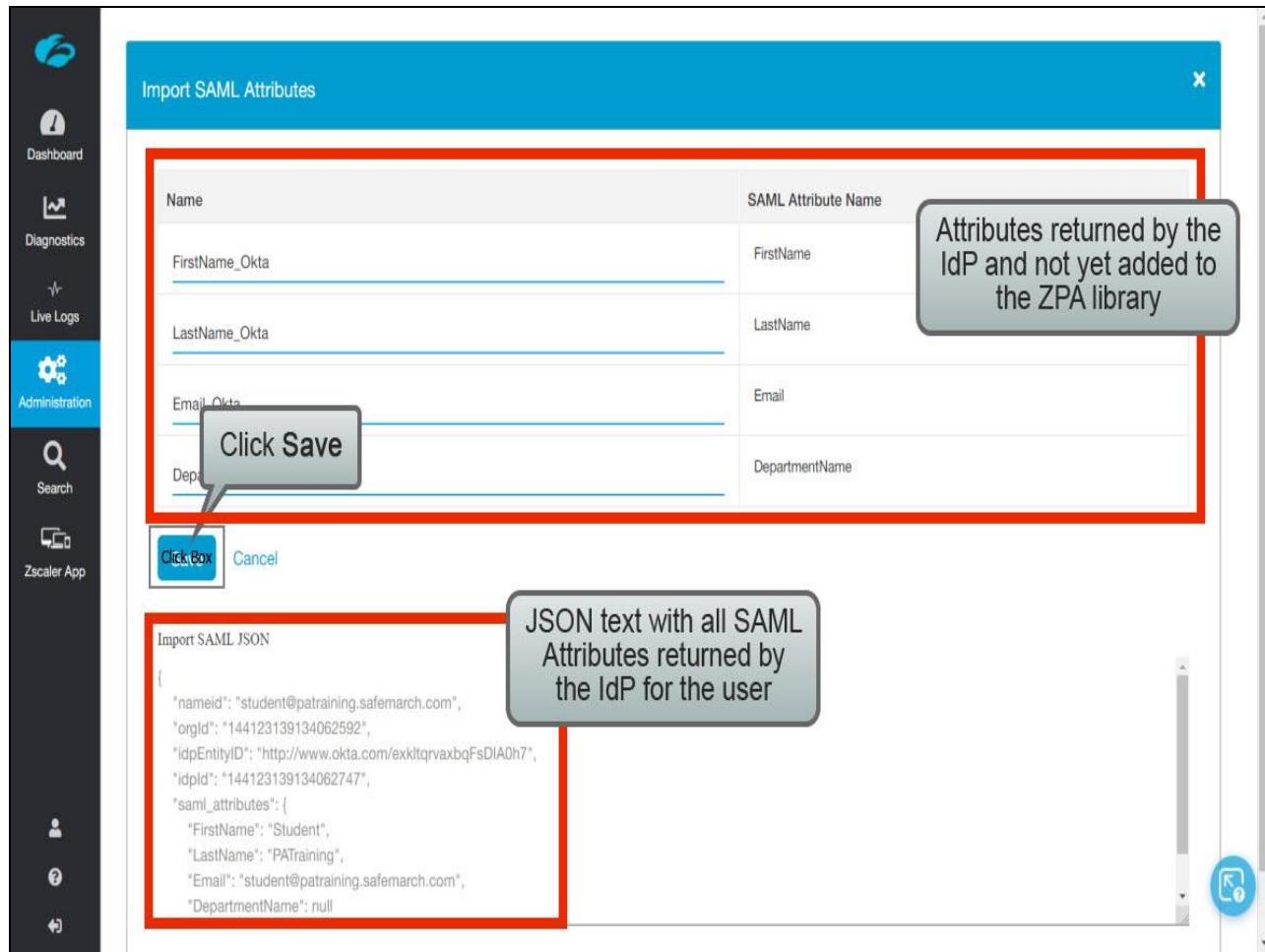
Slide 96 - Slide 96

The screenshot shows a web browser window with a login page for 'zscaler'. At the top, it says 'Connecting to zscaler' and 'Sign-in with your Safemarch ZPA account to access Zscaler Private Access 2.0'. Below this is the Okta sign-in page, which features the Okta logo and a placeholder user icon. The form includes fields for 'Email' (student@patraining.safemarch.com) and 'Password' (redacted), a 'Remember me' checkbox, and a large blue 'Sign In' button. A grey callout box on the left contains the text 'Verify that the IdP login page loads, and that you can login'. A grey callout box at the bottom right points to the 'Sign In' button with the text 'Click Sign In'.

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

The screenshot shows the Adobe Captivate interface with the 'Administration' sidebar open. The main area displays the 'SAML Attributes' tab of the 'IdP Configuration' screen. A table lists four attributes and their corresponding Okta names:

Name	SAML Attribute	IdP Name	Actions
FirstName_Okta	FirstName	Okta	
Email_Okta	Email	Okta	
DepartmentName_Okta	DepartmentName	Okta	
LastName_Okta	LastName	Okta	

A success message at the bottom right states 'SAML attributes imported successfully' with a checkmark icon.

Slide notes

Slide 99 - Slide 99

The screenshot shows the Adobe Captivate interface with the 'SAML Attributes' tab selected. On the left, there's a navigation sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area displays a table of SAML attributes. A red box highlights the 'IdP Configuration' dropdown in the top right corner of the table header. The dropdown is open, showing 'All' and 'Okta'. A callout bubble with the text 'Filter attributes by IdP' points to this dropdown. The table has columns for Name, SAML Attribute, and IdP Name. It contains four rows:

Name	SAML Attribute	IdP Name
FirstName_Okta	FirstName	Okta
Email_Okta	Email	Okta
DepartmentName_Okta	DepartmentName	Okta
LastName_Okta	LastName	Okta

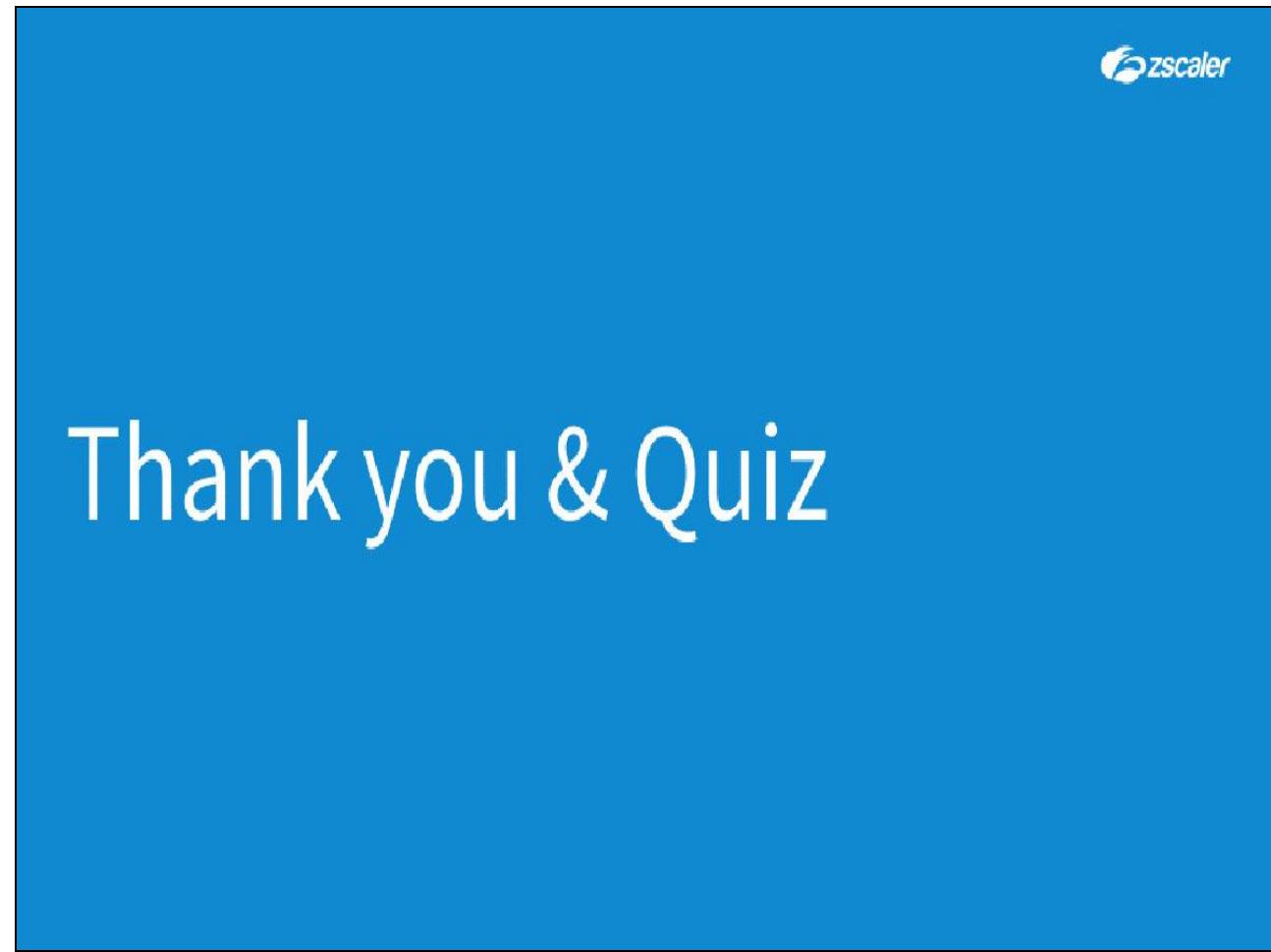
In the bottom right corner of the main area, there's a blue circular icon with a white square and a small circle inside.

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.