

Slide 1 – Authentication with SAML – Okta



Zscaler Private Access

Authentication with SAML – Okta

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on configuring ZPA to use Okta for authenticating users.

Slide 2 - Navigating the eLearning Module

The screenshot shows the Zscaler Application Performance Management (ZAPP) dashboard. At the top right is the Zscaler logo. Below it, the title "Navigating the eLearning Module" is displayed. On the left, there's a sidebar with "Dashboard", "Diagnostics", "Live Logs", "Administration", and a "Search" bar. The main area has tabs for "Applications", "Users", and "Health". A date range selector shows "14 Days". Key metrics include "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). Below these are sections for "TOP APPLICATIONS BY BANDWIDTH" and "TOP POLICY BLOCKS". A progress bar at the bottom indicates "97.11% of total traffic". Overlaid on the dashboard are several blue callout boxes with white text:

- Play/Pause (points to the play/pause button in the bottom left corner)
- Previous Slide (points to the previous slide button in the bottom left corner)
- Next Slide (points to the next slide button in the bottom left corner)
- Progress Bar (points to the progress bar at the bottom center)
- Exit (points to the exit button in the top right corner)
- Audio On/Off (points to the audio control icon in the bottom right corner)
- Closed Captioning (points to the closed captioning control icon in the bottom right corner)

Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play and Pause**, **Previous** and **Next** slide. 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



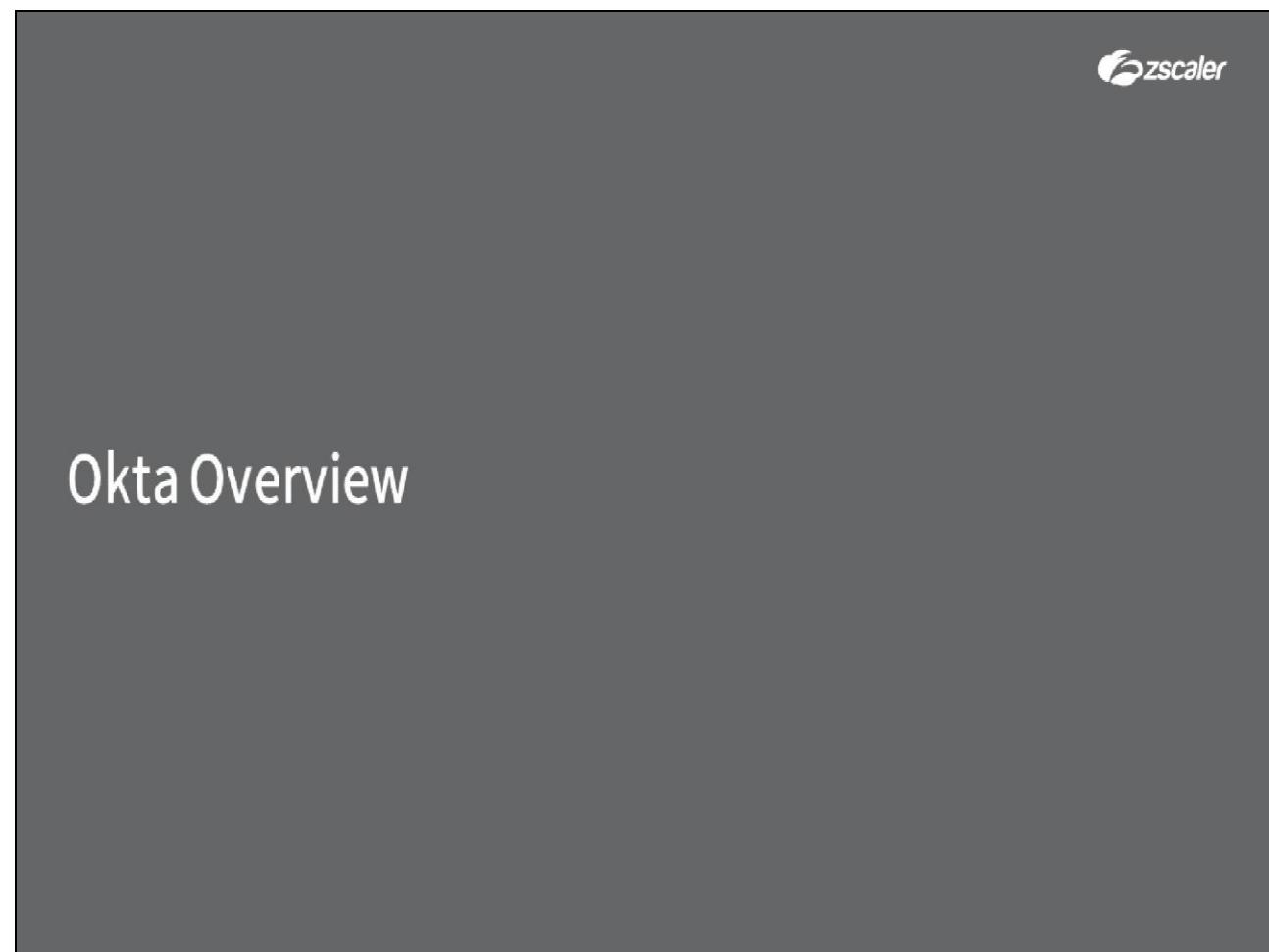
- Okta Overview
- Configuring Okta
 - A. Add a new IdP in ZPA for User Authentication
 - B. Add / Configure the ZPA Application in Okta
 - C. Complete the IdP Setup in ZPA
 - D. Test the configuration and Import Attributes
- The End User Experience

Slide notes

In this module we will:

- Provide an overview of the Okta solution;
- Look at the creation of a new SAML IdP in the ZPA Admin Portal for user SSO;
- Look at how to add ZPA to Okta as an **Application**;
- Look at the steps necessary to finalize the configuration of the IdP in the ZPA Admin Portal;
- Look at how to test that the integration is working and import the available **SAML Attributes**;
- And finally, look at the end user experience once it is configured.

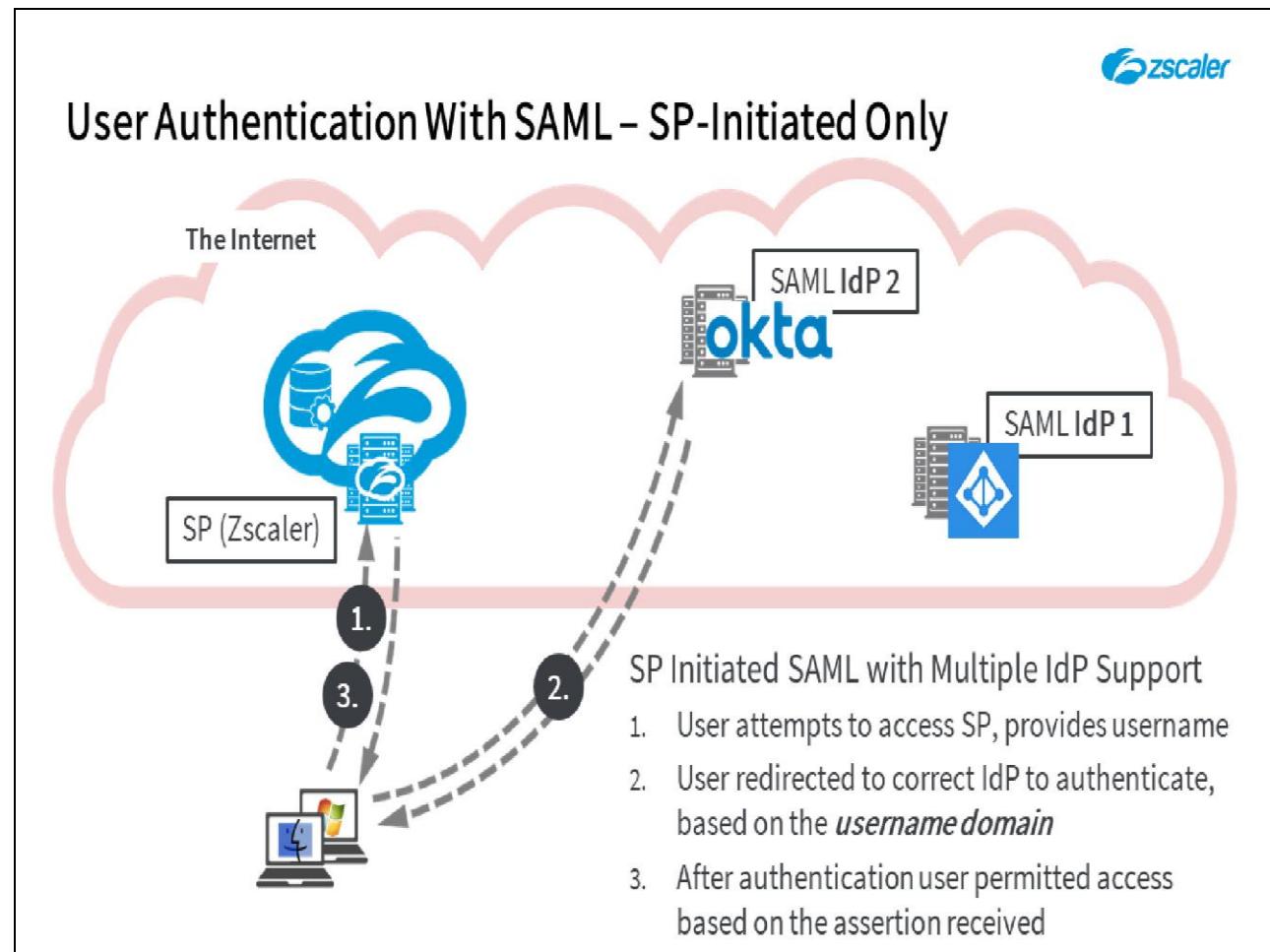
Slide 4 - Okta Overview



Slide notes

In the first section, we provide an overview of the Okta solution.

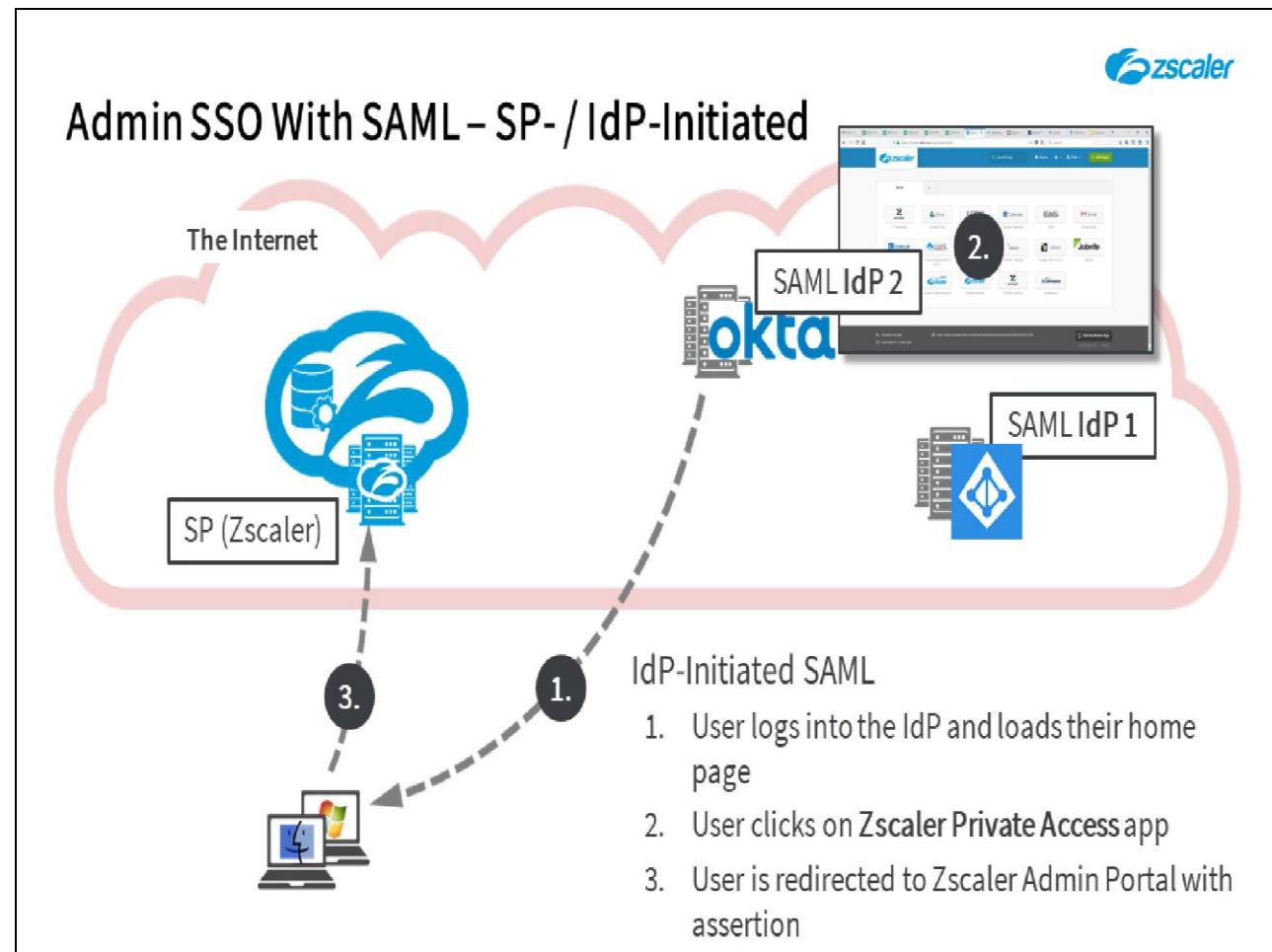
Slide 5 - User Authentication With SAML – SP-Initiated Only



Slide notes

As discussed elsewhere, SAML is required for end user authentication to the ZPA service through the Zscaler App or in a browser and the only SAML mode supported for end user authentication is SP-initiated SAML. Okta is a popular, cloud-based IdP that can be used for this purpose.

Slide 6 - Admin SSO With SAML – SP- / IdP-Initiated



Slide notes

For administrator SSO both SP-initiated and IdP-initiated SAML are supported. Okta is also a suitable platform to support admin SSO to the ZPA service.

Slide 7 - Useful Okta Features

Okta Directory Integration Options

- AD Integration Options
 - Sync Agent installed on one or more AD Domain Controller
 - Opens persistent TCP connection to Okta
 - Syncs user accounts to Okta
 - User passwords validated back to AD down the persistent connection
 - Desktop SSO agent for seamless SSO (IWA)
 - Okta AD Password Sync
- LDAP Integration
 - Integration with directories other than AD for delegated authentication

Slide notes

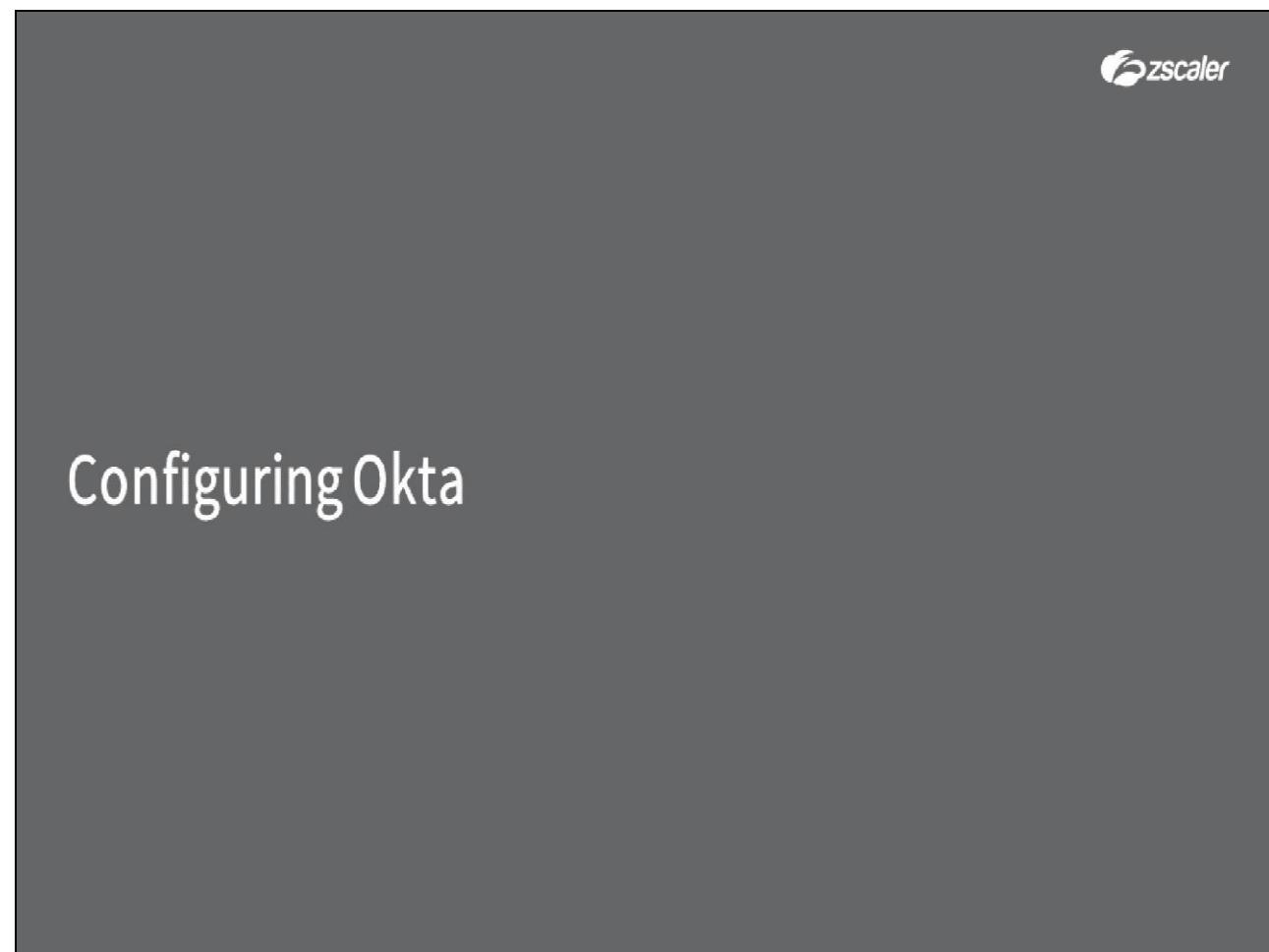
Okta can be used as a stand-alone directory for user authentication, or it can be integrated with an existing directory system, such as Microsoft Active Directory (AD). An AD Sync Agent is available that can be installed on one or more AD Domain Controllers (Okta recommend it is installed on at least two), which allows the synchronization of user accounts from AD to Okta. The Sync Agent establishes a persistent outbound TCP connection to Okta to allow the sync to happen, but also to allow the validation of user passwords back with the original directory server.

The Okta Desktop SSO agent allows users to be automatically authenticated by Okta, and apps accessed through Okta, when they log into the Windows network. Okta's IWA web app uses Microsoft's Integrated Windows Authentication and ASP.NET to authenticate users from specified gateway IPs.

The Okta AD Password Sync agent option automatically pushes users' AD passwords from your Domain Controllers to the Okta service. Passwords are synced from your Domain Controller to Okta whenever a user's password is changed. The agent must be installed on all Domain Controllers and Delegated Authentication must be enabled on your Okta organization.

For other LDAP-based directory services, delegated authentication can be enabled to allow your users to sign in to Okta using their LDAP credentials.

Slide 8 - Configuring Okta

**Slide notes**

In the next section, we will look at the configuration of Okta to act as an IdP for end user SSO to ZPA.

This section has been created as an interactive demo to give you a feel for the navigation of the Okta and ZPA Admin Portals. 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 9 - Configuring ZPA for Okta User SSO



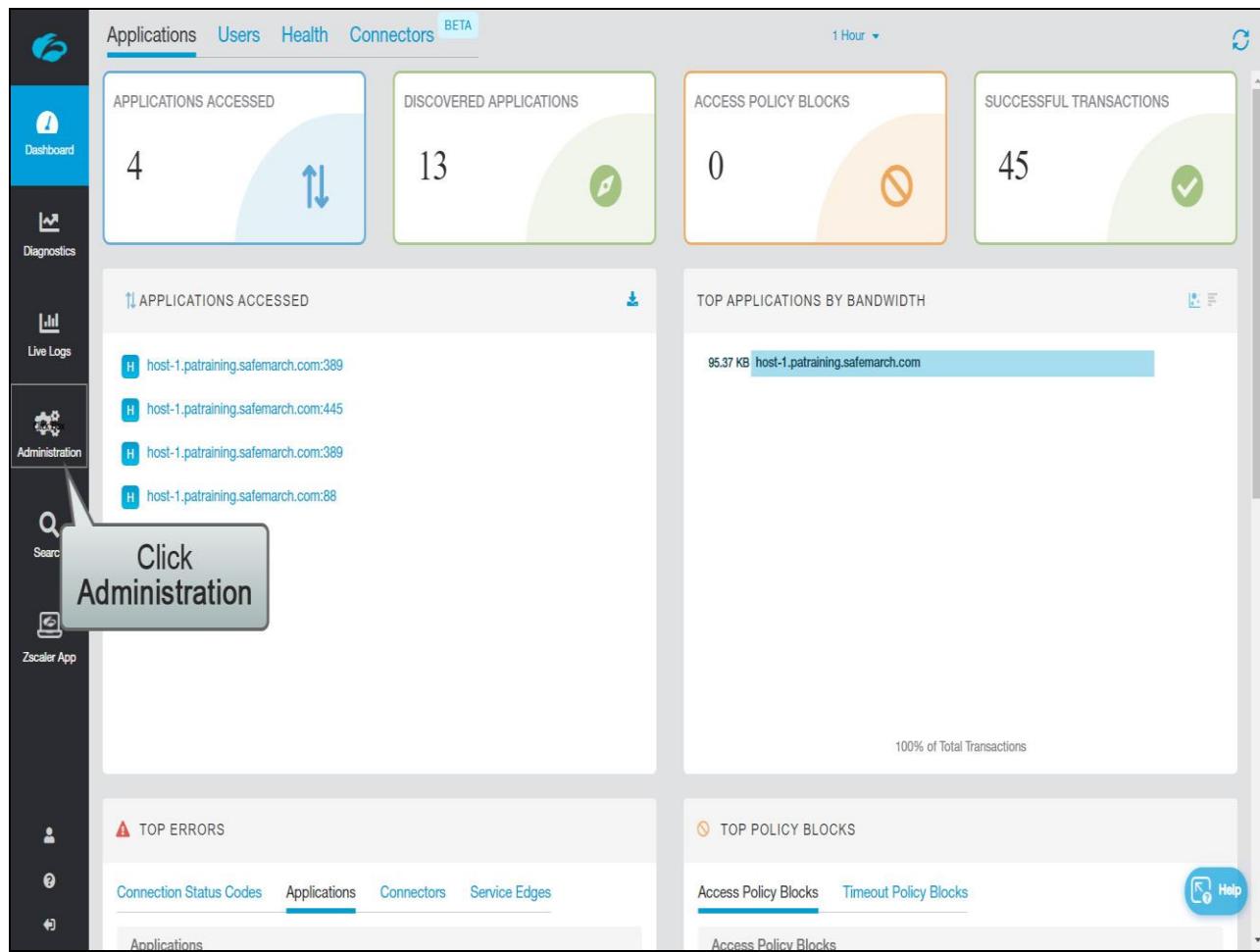
Configuring ZPA for Okta User SSO

A. Add a new IdP in ZPA for User Authentication

Slide notes

First, we will look at creating a new **IdP Configuration** in the ZPA Admin Portal. In this example the IdP added will be for authenticating a group of external consultants to give them secure access to select internal resources over ZPA.

Slide 10 - Slide 10



Slide notes

Login to the ZPA Admin Portal with suitable admin credentials and click **Administration**, ...

Slide 11 - Slide 11

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

- APPLICATION MANAGEMENT**: Application Segments, Segment Groups, Servers.
- AUTHENTICATION**: IdP Configuration (highlighted with a callout), Settings, SAML Attributes.
- Diagnostics**
- Live Logs**
- CERTIFICATES**: Browser Access, Client Certificates.
- Administration**: Connectors, Connector Groups, Connector Provisioning Keys.
- Zscaler App**: Connector Groups, Log Receivers.
- POLICY MANAGEMENT**: Access Policy, Client Forwarding Policy, Timeout Policy.
- REPORTING**: Executive Insights App, Access.

The main area is a light-colored dashboard with several cards:

- PERMISSIONED APPLICATIONS**: 0 (green icon).
- ACCESS POLICY BLOCKS**: 0 (orange icon).
- SUCCESSFUL TRANSACTIONS**: 45 (green icon).
- TOP APPLICATIONS BY BANDWIDTH**: A chart showing host-1.patraining.safemarch.com at 95.37 KB.
- TOP POLICY BLOCKS**: A chart showing 100% of Total Transactions.

A callout box points to the **IdP Configuration** link in the Authentication section of the sidebar.

Slide notes

...then under the **AUTHENTICATION** section click **IdP Configuration**.

Slide 12 - Slide 12

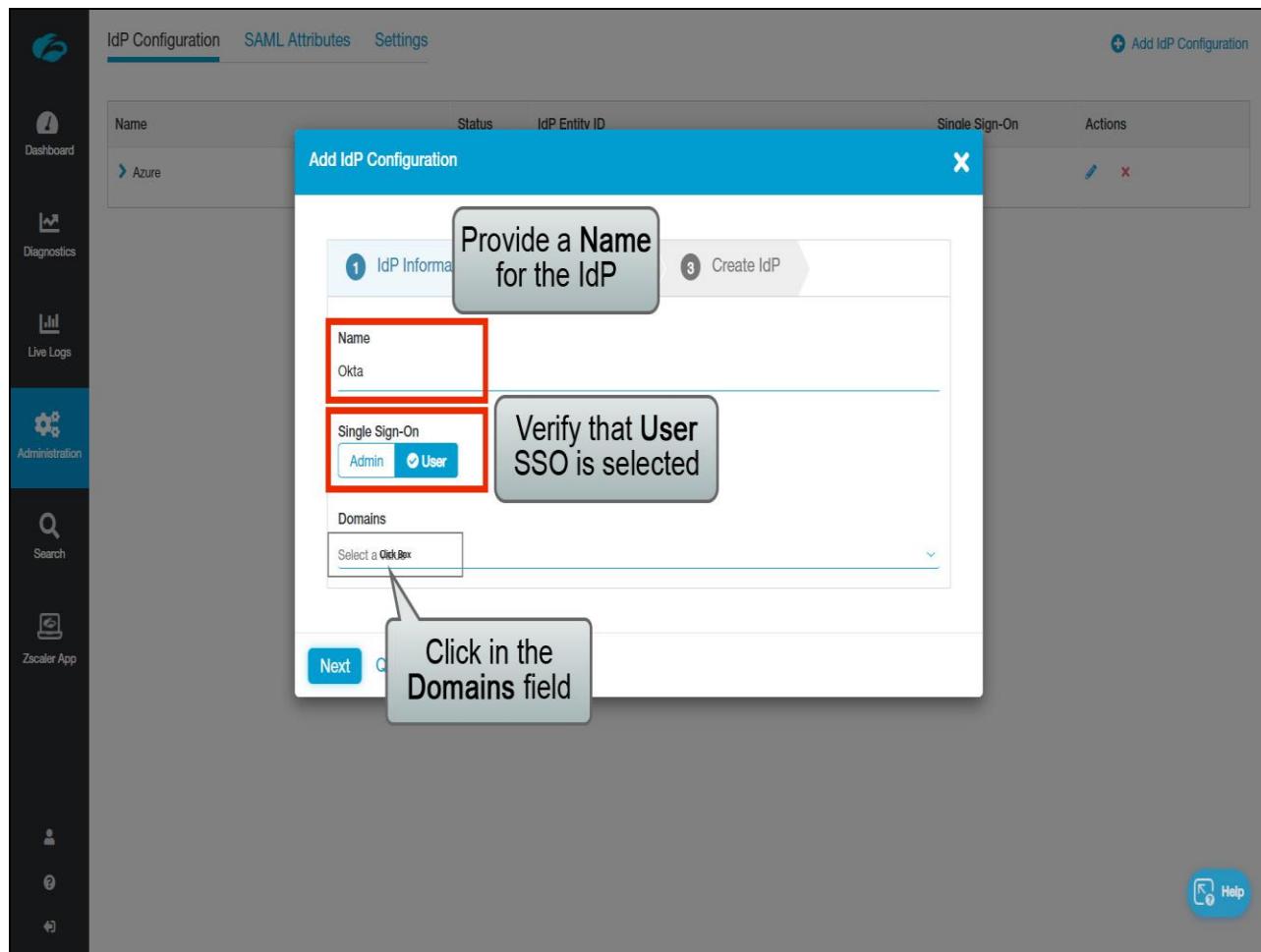
The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected. A callout box with the text 'Click Add IdP Configuration' points to the 'Add IdP Configuration' button in the top right corner of the main content area.

| Name | Status | IdP Entity ID |
|-------|--------|---|
| Azure | ✓ | https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/ |

Slide notes

An IdP already exists for authenticating internal users against Azure AD, so this will be the 2nd IdP that we add, click **Add IdP Configuration**.

Slide 13 - Slide 13



Slide notes

Give the new IdP a suitable **Name** and select the intended population for **Single Sign-On**; **Admin**, or **User** (the default setting). As with Azure AD it is necessary to map this IdP to one or more of the available authentication **Domains** defined on the tenant. To select the appropriate domains from those available on the tenant, click in the **Domains** field, ...

Slide 14 - Slide 14

The screenshot shows the Zscaler Admin interface with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, showing the 'IdP Information' step. The 'Name' field contains 'Okta'. Under 'Single Sign-On', the 'User' radio button is selected. In the 'Domains' section, a dropdown menu is open, showing 'Select a value' and one option: 'ClickBoxcon9.acmeconsult.net'. A callout box with the text 'Click to select the correct Domain' points to this dropdown. The background shows a table with other IdP configurations.

Slide notes

...then click to select one (or more) of the available Domains. Note that in this case, the **Primary Authentication Domain** has been consumed by assigning it to the Azure AD IdP Configuration. As a result, for this IdP, we only have the **Secondary Authentication Domain** available for us to select.

Slide 15 - Slide 15

The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, showing the first step: 'IdP Information'. The 'Name' field contains 'Okta'. Under 'Single Sign-On', the 'User' radio button is selected. In the 'Domains' section, 'con9.acmeconsult.net' is listed with a delete icon. A new domain, 'con9.acmeconsult.net', is being typed into the input field. A callout box with the text 'Click Done' points to the 'Next Step' button at the bottom of the dialog.

Slide notes

Click Done, ...

Slide 16 - Slide 16

The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected. A modal dialog box titled 'Add IdP Configuration' is open, showing the first step: 'IdP Information'. The form contains fields for 'Name' (set to 'Okta'), 'Single Sign-On' (with 'User' selected over 'Admin'), and 'Domains' (containing 'conf.acmeconsult.net'). At the bottom of the dialog, there are 'Next' and 'Quit' buttons, with 'Next' being highlighted by a callout box.

Slide notes

...then click **Next**, ...

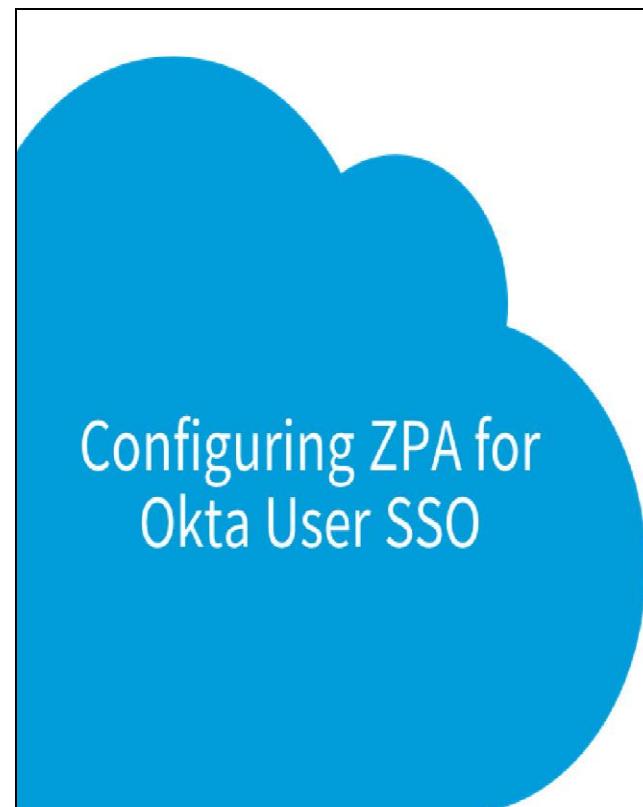
Slide 17 - Slide 17

The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, showing three steps: 1. IdP Information (selected), 2. SP Metadata, and 3. Create IdP. Step 1 displays the 'Service Provider URL' and 'Service Provider Entity ID' fields, which are highlighted with a red box. A callout bubble points to these fields with the text 'Unique Service Provider URL and Entity ID'. The background shows a table with columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. One row in the table is labeled 'Azure'.

Slide notes

...and the **SP Metadata** page will be shown. This page provides the unique **Service Provider URL** and **Entity ID** values that you will need to configure the IdP. You may copy the values to paste into the IdP configuration or, some IdPs support the import of the SP Metadata and certificate from file.

Slide 18 - Configuring ZPA for Okta User SSO



Configuring ZPA for Okta User SSO

B. Add / Configure the ZPA Application in Okta

Slide notes

Next, we will look at how to add the **ZPA Application** (Service Provider) to Okta.

Slide 19 - Slide 19

The screenshot shows the Okta Admin Portal dashboard. 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 top navigation bar includes a search bar, user information (A. PATraining9), and links for Dashboard, Directory, Applications (which is highlighted with a blue box and has a callout arrow pointing to it), Security, Workflow, Reports, Settings, and My Apps. The main content area features a "Dashboard" section with "Status" and "Usage - Last 30 Days" cards, and a "HealthInsight" card showing an audit status with a warning about incomplete security tasks. On the right side, there are sections for "Shortcuts" (Add Applications, Assign Applications, Add People, Activate People, Deactivate People, Reset Passwords, Unlock People, HealthInsight) and "Reports" (Okta Usage, Application Usage, Suspicious Activity, Current Assignments, App Password Health, Deprovisioning Details, SMS Usage, MFA Usage, System Log).

Slide notes

Login to the Okta Admin Portal with suitable admin credentials and click **Applications**, ...

Slide 20 - Slide 20

The screenshot shows the Okta Applications management 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 the Okta logo and navigation links: Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, My Apps, Help, and Sign out.

The main content area is titled "Applications". It features a search bar and two buttons: "Add Application" (highlighted with a green box and a callout bubble saying "Click Add Application") and "Assign Applications". A sidebar on the left shows a status filter with "ACTIVE" selected. The main table lists applications by status: ACTIVE (0) and INACTIVE (0). To the right of the table is a magnifying glass icon and the text "No active apps found". Below the table, there's a message: "Add application and assign access to have them appear on your users' Okta home Page". At the bottom of the page, there are copyright information, version details, and links for "Download Okta Plugin" and "Feedback".

Slide notes

...then click **Add Application**.

Slide 21 - Slide 21

The screenshot shows the Okta 'Add Application' search interface. A red box highlights the search bar containing the text 'zpa'. A callout bubble points to the 'Zscaler Private Access 2.0' result, which is listed under the 'INTEGRATIONS' section. The 'Zscaler Private Access 2.0' result includes a 'Click Box' button and 'SAML, Provisioning' options. Other visible results include Slack, Workday, Zoom, AWS Account, Atlassian Cloud, and Box.

Slide notes

Search for 'ZPA' and click to select the application named **Zscaler Private Access 2.0**, ...

Slide 22 - Slide 22

The screenshot shows the Okta application catalog interface. At the top, there's a yellow header bar 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 this is a blue navigation bar with the Okta logo and links for Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, and My Apps.

The main content area displays the "Zscaler Private Access 2.0" application. On the left, there's a sidebar with categories like Apps, Zero Trust Network, Single Sign-On (SSO), and others. Below this is a "POWERED BY G2" section with a "Zscaler Private Access 2.0 Details & Reviews" link. At the bottom of the sidebar, it says "LAST UPDATE 2020-03-24T11:09:15".

The main panel has a title "Zscaler Private Access 2.0" and a "Overview" section with a brief description of the product. Below this is a "Capabilities" section with a "Click Add" button highlighted by a green box and a callout bubble. To the right is a "Provisioning" section with several checked options: Create, Update, Deactivate, Group Push, Sync Password, Group Linking, Schema Discovery, Attribute Mastering, and Attribute Writeback.

Slide notes

...then click Add.

Slide 23 - Slide 23

The screenshot shows the Okta application configuration interface for "Zscaler Private Access 2.0". The top navigation bar includes links for "Search people, apps", "A. PATraining9", "PA Training 9", "Help and Support", and "Sign out". Below the navigation is a blue header bar with the "okta" logo and "My Apps". The main content area displays the "General Settings" tab for the application. A callout box labeled "Configure the application as necessary" points to the "General settings" section, which contains fields for "Application label" (set to "Zscaler Private Access 2.0") and "Application Visibility". Two checkboxes are present: "Do not display application icon to users" (checked) and "Do not display application icon in the Okta Mobile App" (checked). A green button labeled "Click Box" is highlighted with a callout box labeled "Click Done". The bottom of the screen shows copyright information: "© 2020 Okta, Inc. Privacy Version 2020.06.1 OPI Preview Cell (US) Status site Okta Plugin Feedback".

Slide notes

Configure **General Settings** as necessary and click **Done**.

Slide 24 - Slide 24

The screenshot shows the Okta interface for managing application assignments. 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 header includes a search bar, user information (A. PATraining9), and navigation links for Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, and My Apps.

The main content area displays the "Zscaler Private Access 2.0" application details. The "Assignments" tab is selected. On the left, there's a search bar with "Click Box" and "Convert Assignments" buttons, and a "FILTERS" section with dropdowns for "Person" and "Type". A large button labeled "Click Assign" is highlighted with a red box and an arrow pointing to it from the left.

The main pane shows a list of users assigned to the application, with entries like "01101110", "01101111", etc. Below the list, a message says "No users found". To the right, there are two boxes: "REPORTS" containing "Current Assignments" and "Recent Unassignments", and "SELF SERVICE" with a note about enabling self-service for org-managed apps and a "Go to self service settings" link.

Slide notes

You now need to assign the application to users or groups, so click **Assign**.

Slide 25 - Slide 25

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

Search people, apps

A. PATraining9 - PA Training 9 Help and Support Sign out

okta Dashboard Directory Applications Security Workflow Reports Settings My Apps +

← Back to Applications

Zscaler Private Access 2.0

Active View Logs

General Sign On Mobile Provisioning Import Assignments Push Groups

Assign Convert Assignments Search... People

Assign to People Type

Assign to Groups Click Box

Groups

Click Assign to Groups

No users found

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 -

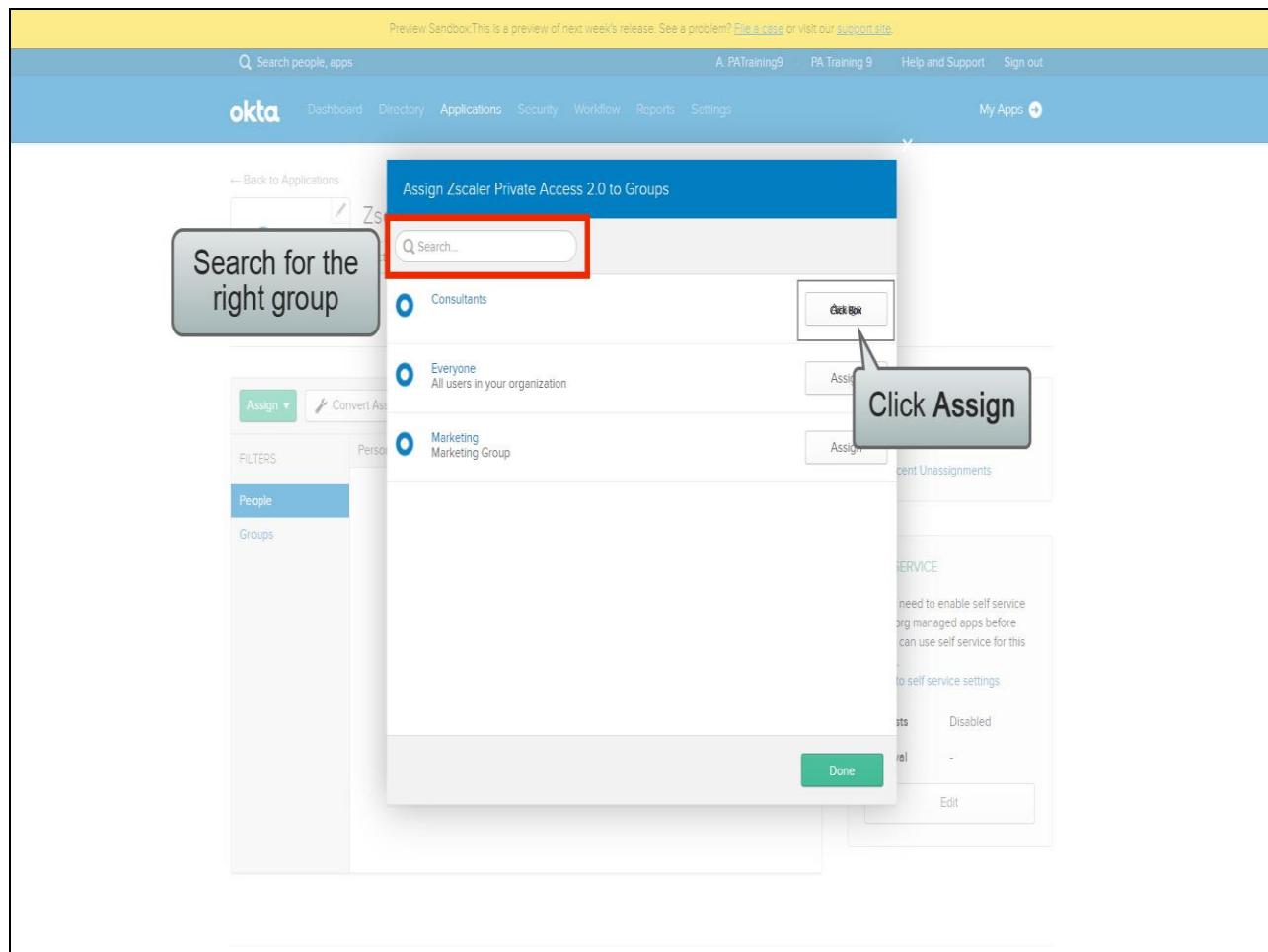
Edit

[https://patraining9-admin.oktapreview.com/admin/app/zscaler_private_access instance/0oas677el0rlzhuy0h#](https://patraining9-admin.oktapreview.com/admin/app/zscaler_private_access	instance/0oas677el0rlzhuy0h#)

Slide notes

Click Assign to Groups, ...

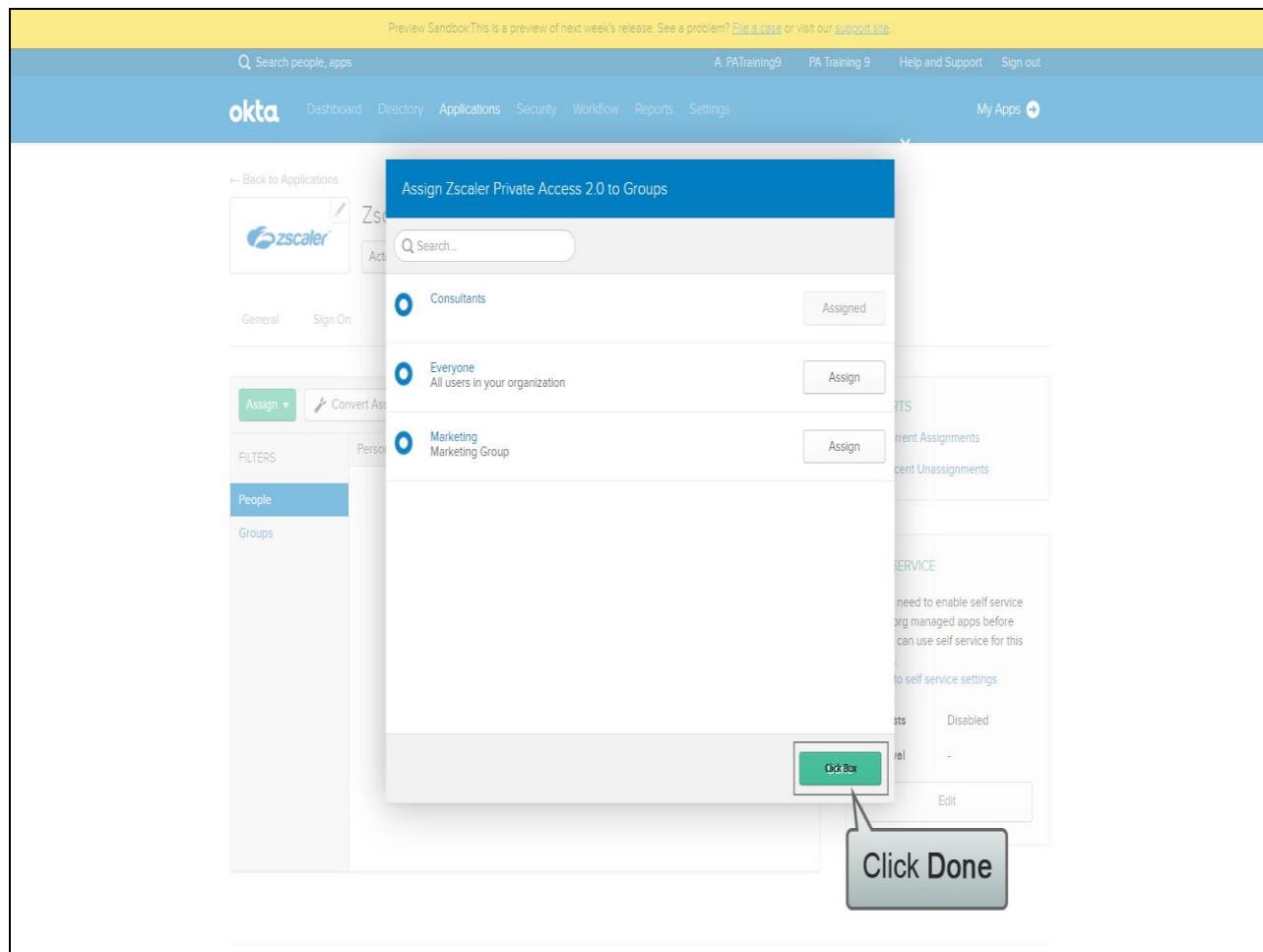
Slide 26 - Slide 26



Slide notes

...Search for the correct group to assign the **Application** to if necessary (we will use the group named **Consultants** for this example), then click **Assign**, ...

Slide 27 - Slide 27



Slide notes

...then click **Done**.

Slide 28 - Slide 28

The screenshot shows the Okta application management 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 header includes a search bar, user information (A. PATraining9), and navigation links for Dashboard, Directory, Applications, Security, Workflow, Reports, and Settings. On the right, there's a "My Apps" section with a plus sign icon.

The main area displays the "Zscaler Private Access 2.0" application card. The card has tabs for General, Sign On, Mobile, Provisioning, Import, Assignments (which is currently selected and highlighted in green), and Push Groups. Below the card, there are sections for "Assign" (with a dropdown menu), "Search..." (with a magnifying glass icon), and "Groups" (with a dropdown menu). There are also "FILTERS" sections for People and Groups.

A callout box with the text "Click Sign On" points to the "Sign On" tab in the navigation bar below the application card. To the right of the main content area, there are two boxes: "REPORTS" (listing "Current Assignments" and "Recent Unassignments") and "SELF SERVICE" (with a note about enabling self-service for org-managed apps, a "Requests" status of "Disabled", and an "Approval" status of "-").

Slide notes

To configure the IdP and download the **Okta IdP Metadata**, click the **Sign On** tab, ...

Slide 29 - Slide 29

The screenshot shows the Okta application management 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 header includes a search bar, user information (A. PATraining9), and navigation links for Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, and My Apps.

The main content area displays the "Zscaler Private Access 2.0" application details. It shows the Zscaler logo, status (Active), and options to View Logs. Below this, tabs for General, Sign On, Mobile, Provisioning, Import, Assignments, and Push Groups are present, with "Sign On" being the active tab.

In the "Sign On Methods" section, "SAML 2.0" is selected. Configuration options include "Default Relay State", "Disable Force Authentication" (unchecked), and "Configured SAML Attributes" (GroupName: None).

To the right, the "About" section provides a brief description of SAML 2.0 and its integration with Okta. A callout box with the text "Click Edit" points to the "Edit" button in the "About" section.

Slide notes

...and click **Edit**.

Slide 30 - Slide 30

The screenshot shows the Okta application configuration interface for the Zscaler Private Access 2.0 application. The top navigation bar includes a search bar, user information (A. PATraining9), and links for Help and Support, Sign out, and My Apps. Below the navigation is a breadcrumb trail: Back to Applications > Zscaler Private Access 2.0. The main content area displays the application's logo, status (Active), and log viewing options. A sub-menu bar below the logo includes General, Sign On (which is selected and highlighted in green), Mobile, Provisioning, Import, Assignments, and Push Groups. The 'Sign On' tab contains several configuration sections: 'SIGN ON METHODS' (with SAML 2.0 selected), 'Default Relay State' (disabled), 'Attributes (Optional)' (disabled), and 'Disable Force Authentication' (checked). To the right of the main content, there is an 'About' section describing SAML 2.0 integration, an 'Application Username' section, and a large callout box containing the text 'Scroll down...'. The entire interface has a light blue header and a white body.

Slide notes

Scroll down, ...

Slide 31 - Slide 31

The screenshot shows the ZPA Admin Portal configuration interface for SAML 2.0. At the top, there's a note about SAML 2.0 setup instructions and a preview button. Below that, a yellow sidebar provides setup instructions. The main area has sections for 'ADVANCED SIGN-ON SETTINGS' and 'CREDENTIALS DETAILS'. A red box highlights the 'Service Provider URL' and 'Service Provider Entity ID' fields. A callout bubble with the text 'Copy/Paste data from the ZPA Admin Portal' points to these fields. The 'CREDENTIALS DETAILS' section includes fields for application username format (set to 'Okta username') and password reveal options.

Group Name: None

Preview SAML

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: Okta username

Update application username on: Create and update

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

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

Save

Slide notes

...and copy/paste data from the ZPA Admin Portal into the **Service Provider URL** and **Service Provider Entity ID** fields.

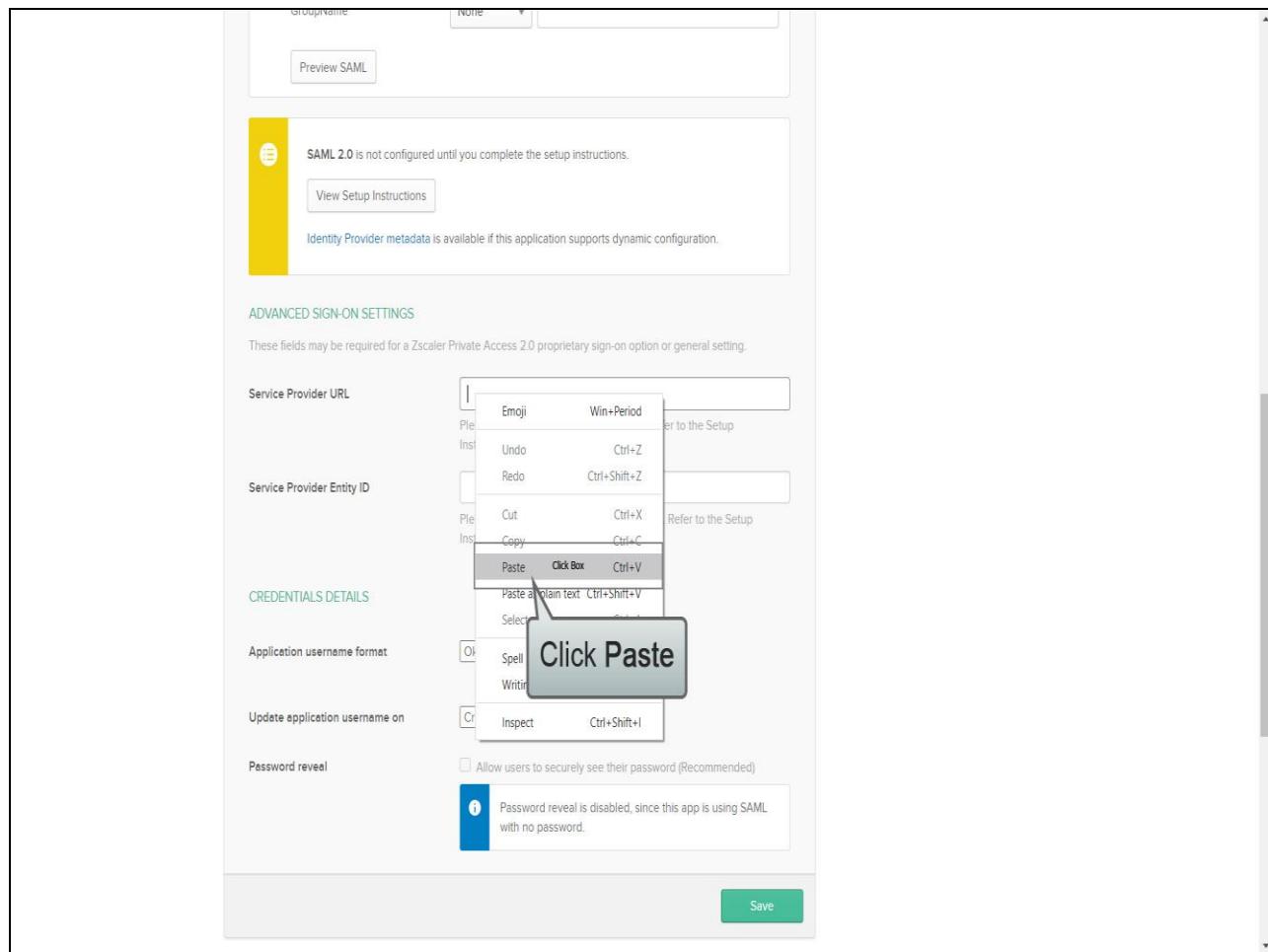
Slide 32 - Slide 32

The screenshot shows the Zscaler Admin Portal interface. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area is titled 'IdP Configuration' and shows a table with one row for 'Azure'. A modal window titled 'Add IdP Configuration' is open, showing three steps: 1. IdP Information (selected), 2. SP Metadata, and 3. Create IdP. Step 1 contains fields for Service Provider Metadata (with download links) and Service Provider URL (containing a placeholder URL). A context menu is open over the URL field, with 'Click Copy' highlighted. Other options in the menu include 'Ctrl+C', 'Ctrl+P', and 'Ctrl+Shift+I'.

Slide notes

In the ZPA Admin Portal, select the value for the **Service Provider URL** and click **Copy**, ...

Slide 33 - Slide 33



Slide notes

...then back in the Okta Portal, right click in the **Service Provider URL** field and click **Paste**.

Slide 34 - Slide 34

The screenshot shows the configuration interface for a Zscaler Private Access 2.0 application. At the top, there is a note indicating that SAML 2.0 is not configured until setup instructions are completed. A yellow sidebar on the left provides a link to 'View Setup Instructions'. Below this, under 'ADVANCED SIGN-ON SETTINGS', there are fields for 'Service Provider URL' (set to <https://samlsp.private.zscaler.com/auth/144123467699061842/sso>) and 'Service Provider Entity ID' (empty). Under 'CREDENTIALS DETAILS', there are dropdown menus for 'Application username format' (set to 'Okta username') and 'Update application username on' (set to 'Create and update'). A checkbox for 'Password reveal' is present, with a note stating it is disabled due to SAML configuration. A green 'Save' button is located at the bottom right.

Slide notes

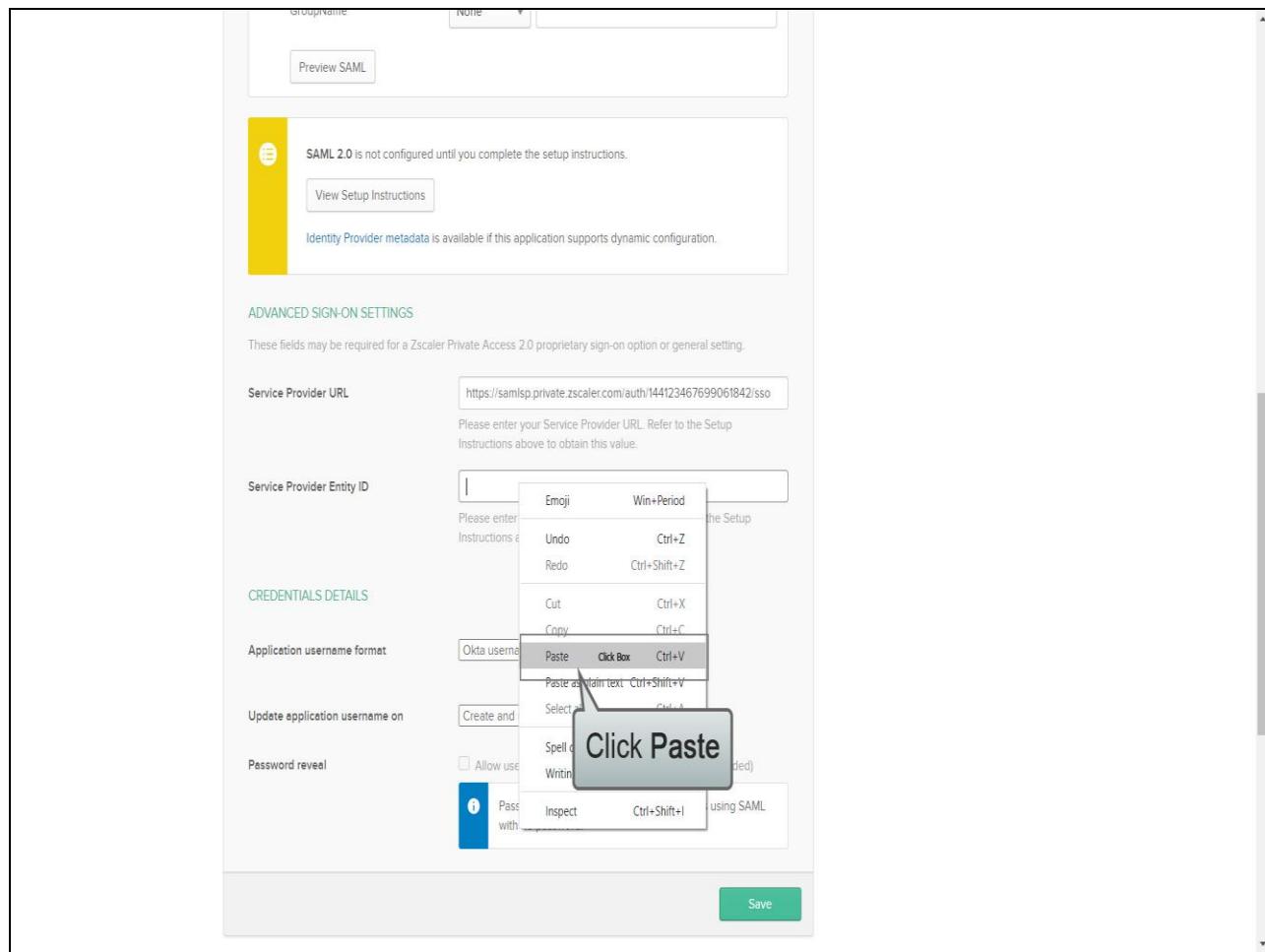
Slide 35 - Slide 35

The screenshot shows the Zscaler Admin Portal interface for managing SAML configurations. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for 'IdP Configuration' (which is selected), 'SAML Attributes', and 'Settings'. A modal window titled 'Add IdP Configuration' is open, showing three steps: 1. IdP Information (selected), 2. SP Metadata, and 3. Create IdP. The 'IdP Information' step is configured with a Service Provider URL (https://samlsp.private.zscaler.com/auth/144123467699061842/sso) and a Service Provider Entity ID (https://samlsp.private.zscaler.com/auth/metadata/144123467699061842). A context menu is open over the 'Service Provider Entity ID' field, with options including 'Ctrl+C' (Copy), 'Ctrl+P' (Print), and 'Ctrl+Shift+I' (Inspect). A callout box labeled 'Click Copy' points to the 'Ctrl+C' option.

Slide notes

Back in the ZPA Admin Portal, select the value for the **Service Provider Entity ID** and click **Copy**, ...

Slide 36 - Slide 36



Slide notes

...then back in the Okta Portal, right click in the **Service Provider Entity ID** field and click **Paste**.

Slide 37 - Slide 37

The screenshot shows a configuration dialog for a Zscaler Private Access 2.0 application. At the top, there is a note indicating that SAML 2.0 is not configured until setup instructions are completed. A yellow sidebar on the left provides a link to 'View Setup Instructions'. Below this, under 'ADVANCED SIGN-ON SETTINGS', there are two fields: 'Service Provider URL' set to <https://samisp.private.zscaler.com/auth/144123467699061842/sso>, and 'Service Provider Entity ID' set to <https://samisp.private.zscaler.com/auth/metadata/144123467699061>. Under 'CREDENTIALS DETAILS', there are three dropdown menus: 'Application username format' set to 'Okta username', 'Update application username on' set to 'Create and update', and 'Password reveal' which includes a checkbox for 'Allow users to securely see their password (Recommended)' and a note stating 'Password reveal is disabled, since this app is using SAML with no password.' A large green button at the bottom right is labeled 'Click Box'. A callout bubble points to this button with the text 'Click Save'.

Slide notes

Then click **Save**.

Slide 38 - Slide 38

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

Search people, apps

A. PATraining9 · PA Training 9 · Help and Support · Sign out

okta · Dashboard · Directory · Applications · Security · Workflow · Reports · Settings · My Apps +

← Back to Applications

Zscaler Private Access 2.0

Active · View Logs

General · Sign On · Mobile · Provisioning · Import · Assignments · Push Groups

Settings · Edit

Settings saved!

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Disable Force Authentication

Configured SAML Attributes

GroupName None

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

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.

Scroll down...

Slide notes

Scroll down again, ...

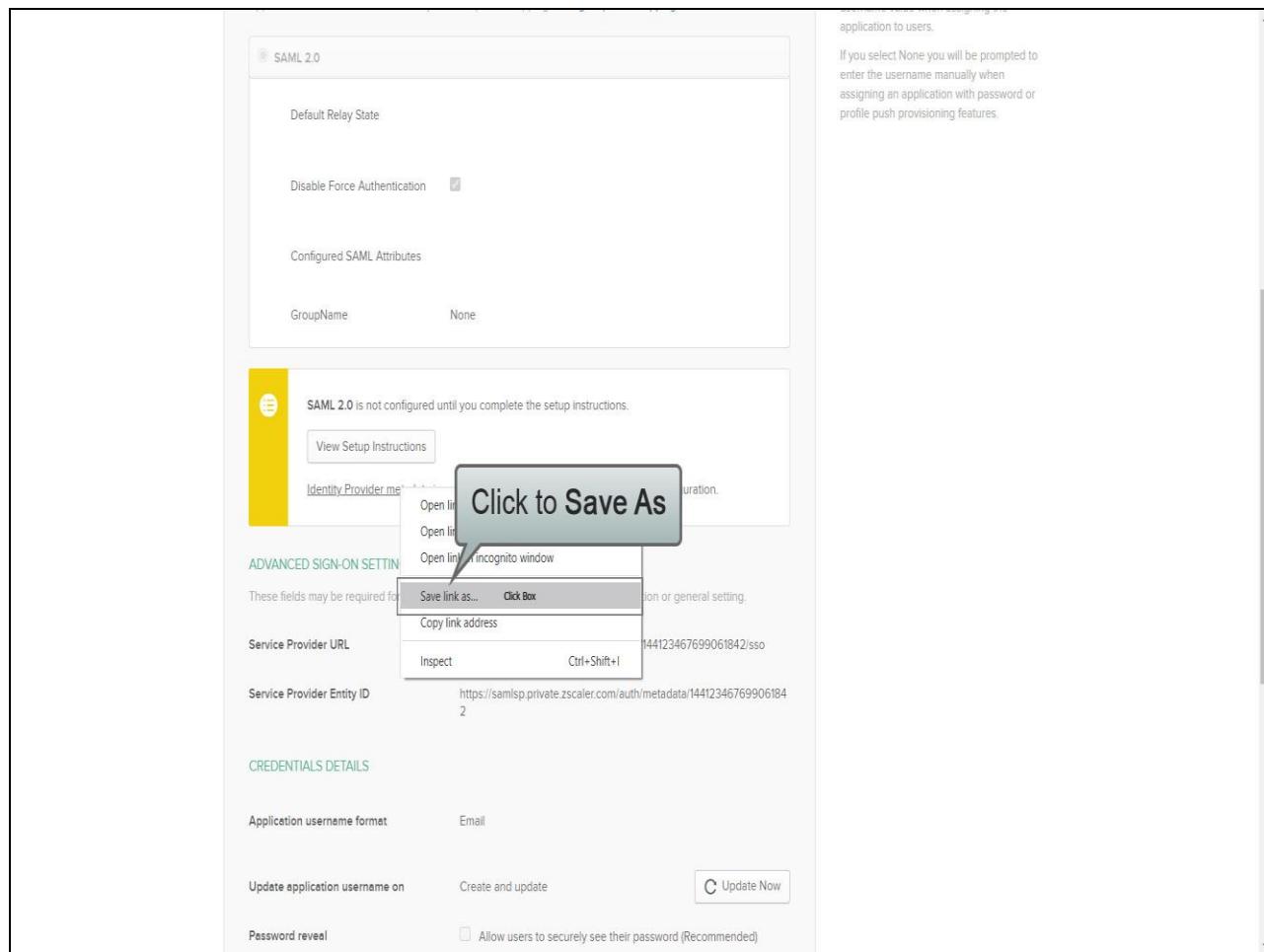
Slide 39 - Slide 39

The screenshot shows the configuration of a SAML 2.0 application. At the top, there is a section for 'Default Relay State' and a checkbox for 'Disable Force Authentication'. Below this, under 'Configured SAML Attributes', there is a 'GroupName' field set to 'None'. A note states: 'SAML 2.0 is not configured until you complete the setup instructions.' It includes a 'View Setup Instructions' button and a link to 'Identity Provider metadata'. A callout box points to this link with the text 'Click to download IdP Metadata'. In the 'ADVANCED SIGN-ON SETTINGS' section, there is a note about required fields and a 'Service Provider URL' field containing 'https://samlsp.private.zscaler.com/auth/metadata/144123467699061842/sso'. The 'CREDENTIALS DETAILS' section includes an 'Application username format' dropdown set to 'Email', an 'Update application username on' dropdown set to 'Create and update', and a 'C Update Now' button. There is also a 'Password reveal' checkbox and a note about secure password visibility.

Slide notes

...then click on the **Identity Provider metadata** link, ...

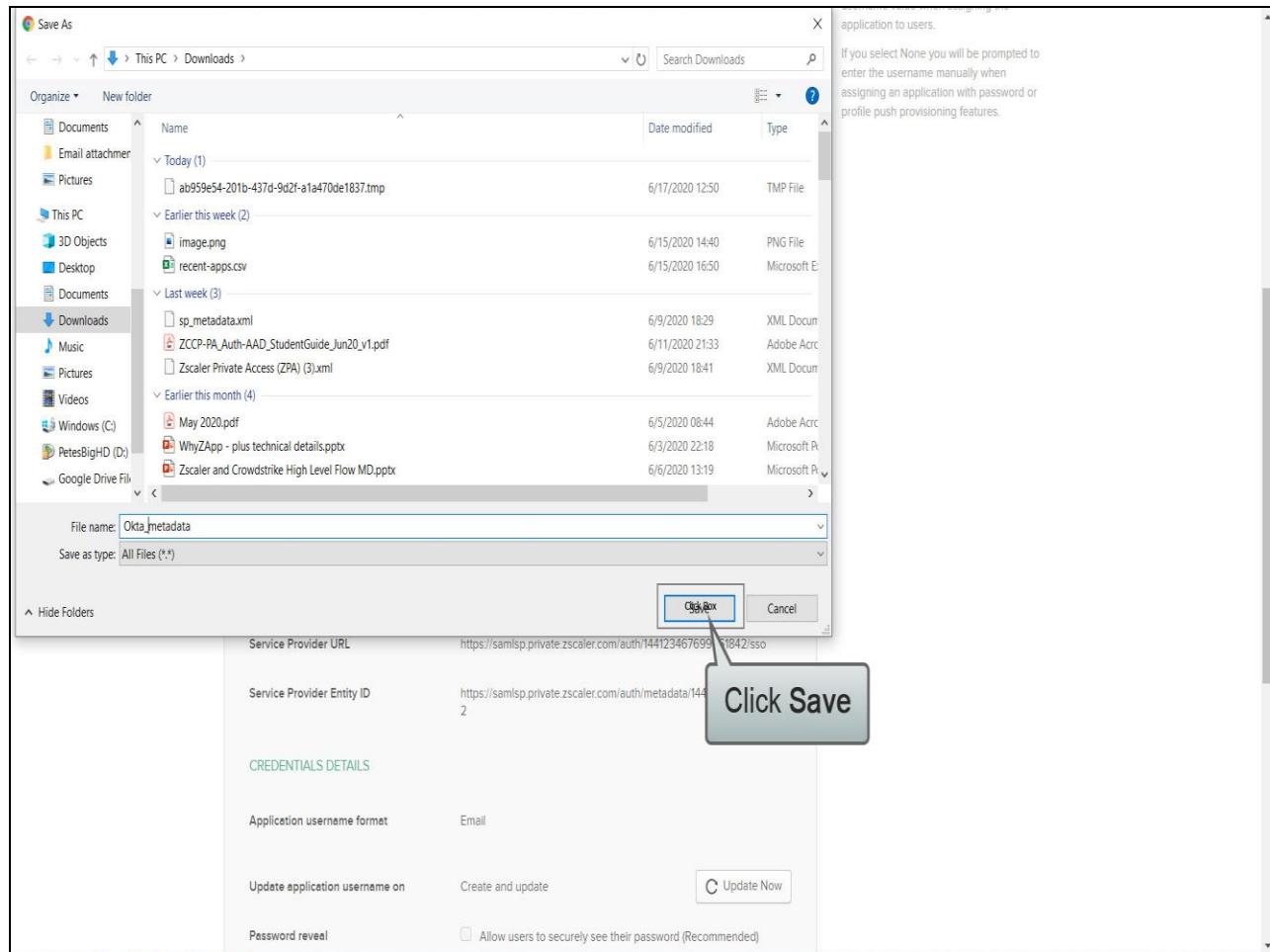
Slide 40 - Slide 40



Slide notes

...and click to save the file to a suitable folder.

Slide 41 - Slide 41



Slide notes

In this case we will rename the file **Okta_metadata**, click **Save** to save the file.

Slide 42 - Slide 42

The screenshot shows the configuration interface for a Zscaler Private Access 2.0 application. The main section is titled "SAML 2.0". It includes fields for "Default Relay State", "Disable Force Authentication" (with a checkbox), and "Configured SAML Attributes". A note states: "SAML 2.0 is not configured until you complete the setup instructions." Below this is a "View Setup Instructions" button and a note about "Identity Provider metadata". The interface also includes sections for "ADVANCED SIGN-ON SETTINGS" (with a note about proprietary sign-on) and "CREDENTIALS DETAILS" (with an "Application username format" set to "Email"). At the bottom, there are buttons for "Update application username on" (Create and update), "C Update Now", and navigation links like "Okta_metadata", "Show all", and "X".

Slide notes

Slide 43 - Slide 43

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, the Okta logo is on the left, followed by a search bar and navigation links: Dashboard, Directory, Applications, Security, Workflow, Reports, Settings, and Help and Support. On the right, there's a "My Apps" section with a plus sign and a "Sign Out" button highlighted with a red box and a callout bubble that says "Click Sign Out".

In the main content area, the user is viewing the "Zscaler Private Access 2.0" application. The application card shows the Zscaler logo, the name "Zscaler Private Access 2.0", and status indicators: Active, healthy, and View Logs. Below the card, tabs are available for General, Sign On, Mobile, Provisioning, Import, Assignments, and Push Groups. The "Sign On" tab is selected and highlighted with a green underline.

On the left side, under the "Settings" tab, there's a "SIGN ON METHODS" section. It includes a radio button for "SAML 2.0" (which is selected), a "Default Relay State" input field, a checkbox for "Disable Force Authentication" (unchecked), and a "Configured SAML Attributes" section. In this section, there's a "GroupName" input field containing "None".

On the right side, there's an "About" section with the following text:

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Below this, there's an "Application Username" section with the following text:

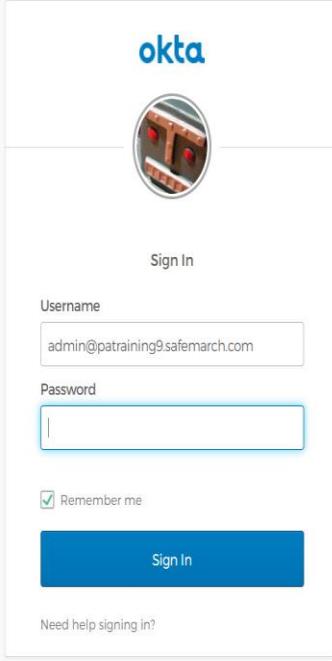
Choose a format to use as the default username value when assigning the application to users.

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 **Sign Out** to exit the Okta Admin Portal.

Slide 44 - Slide 44



A screenshot of the Okta sign-in page. The page features the Okta logo at the top left, followed by a circular profile picture placeholder. Below the logo is a "Sign In" button. The next section contains a "Username" label and an input field containing the text "admin@patraining9.safemarch.com". The subsequent section contains a "Password" label and an empty input field. A "Remember me" checkbox is checked and labeled "Remember me". At the bottom of the form is a large blue "Sign In" button. Below the form, there is a link "Need help signing in?".

Powered by Okta

Privacy Policy

Slide notes

Slide 45 - Configuring ZPA for Okta User SSO



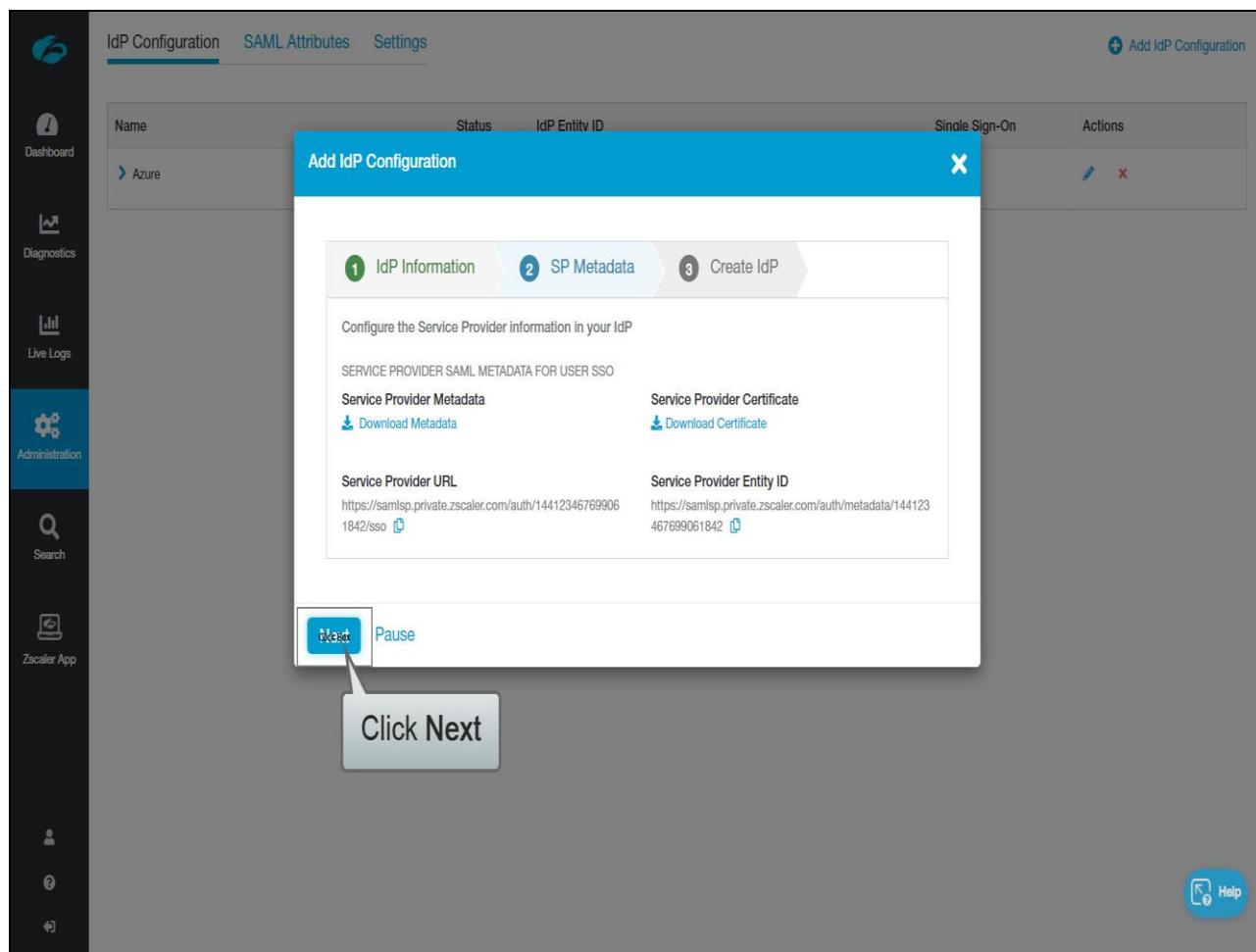
Configuring ZPA for Okta User SSO

C. Complete the IdP Setup in ZPA

Slide notes

Next, we will look at how to complete the Okta **IdP Configuration** in the ZPA Admin Portal.

Slide 46 - Slide 46



Slide notes

Back in the ZPA Admin Portal, in the **Add IdP Configuration** wizard, click **Next**, ...

Slide 47 - Slide 47

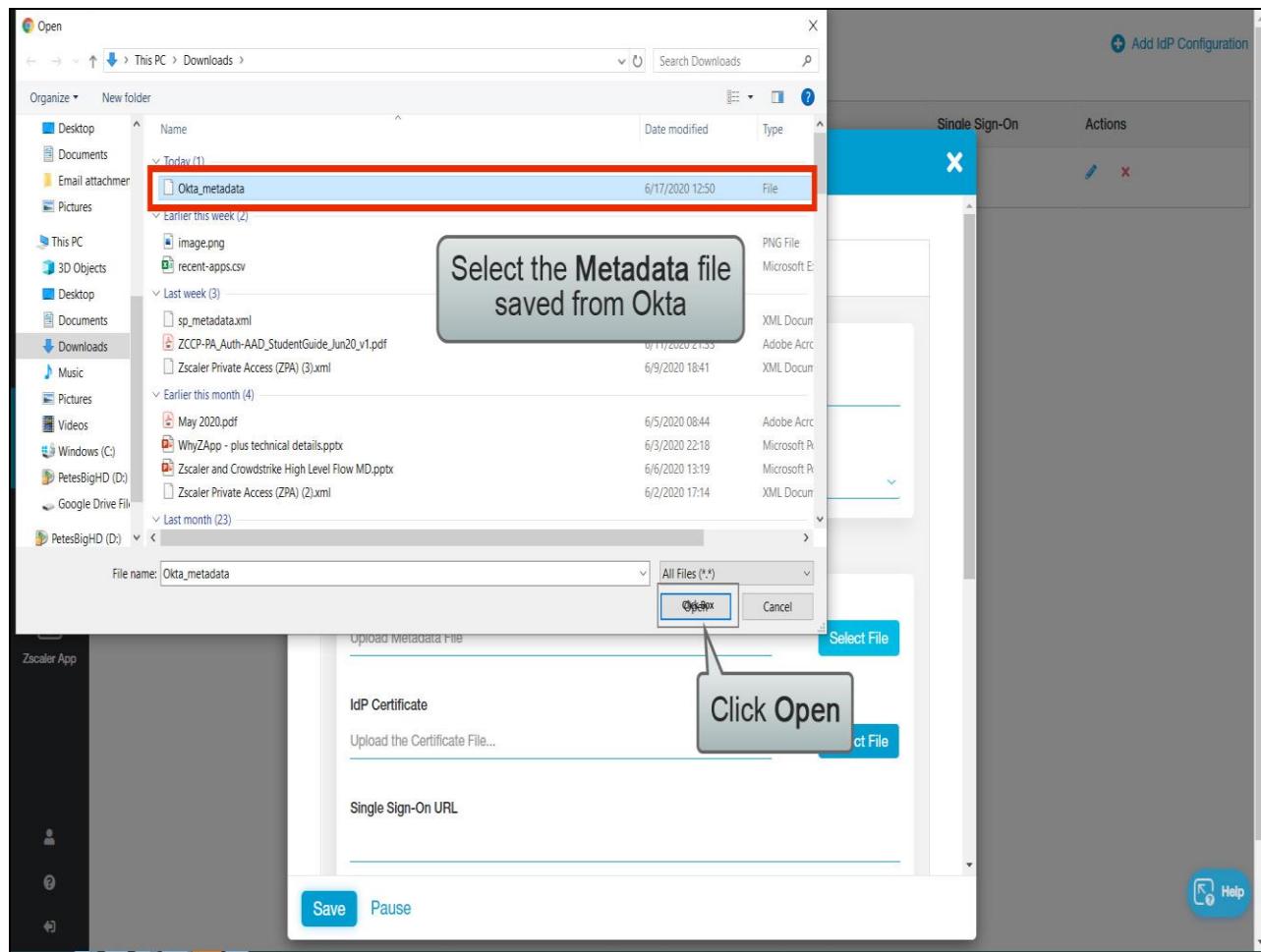
Verify the selected Authentication Domain

Click Select File

Slide notes

...verify that the selected **Authentication Domain** is correct, then next to the **IdP Metadata File** field, click **Select File**, ...

Slide 48 - Slide 48



Slide notes

...find the Okta metadata file you saved earlier, select it and click **Open**.

Slide 49 - Slide 49

The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected in the top navigation bar. A modal dialog box titled 'Add IdP Configuration' is open, showing the 'IdP Information' step. The 'Name' field contains 'Okta'. Under 'Authentication Domains', there is a dropdown menu with 'con9.acmeconsult.net' selected. In the 'SAML ATTRIBUTES' section, there is an 'IdP Metadata File' input field containing 'Okta_metadata'. Below it is an 'IdP Certificate' section with a 'Select File' button and a large text area containing a certificate's BEGIN and END sections. At the bottom of the dialog are 'Save' and 'Pause' buttons, and a 'Help' button on the right. A 'Scroll down...' callout points to the bottom of the dialog.

Slide notes

Scroll down...

Slide 50 - Slide 50

Click Save

Verify that the IdP Certificate has also been imported

Configure IdP settings as necessary

Slide notes

...verify that the **IdP Certificate** has also been imported, configure IdP settings as required, then click **Save**.

Slide 51 - Slide 51

The screenshot shows the Adobe Captivate interface with the 'Administration' tab selected in the sidebar. The main content area displays the 'IdP Configuration' page. At the top, there are three tabs: 'IdP Configuration' (selected), 'SAML Attributes', and 'Settings'. A blue button labeled 'Add IdP Configuration' is located in the top right corner. On the left side, there is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Search, Zscaler App, and other administration tools. The main content area contains a table with two rows of data:

| Name | Status | IdP Entity ID | Single Sign-On | Actions |
|-------|--------|---|----------------|---------|
| Azure | ✓ | https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/ | User | |
| Okta | ✓ | http://www.okta.com/exks677ekzbQQdCaz0h7 | User | |

In the bottom right corner of the main content area, there is a green notification box with the text 'IdP configuration saved' and a 'Help' button.

Slide notes

Slide 52 - Slide 52

The screenshot shows the Adobe Captivate interface with the 'Administration' sidebar open. The main content area displays the 'IdP Configuration' tab, which lists two entries: 'Azure' and 'Okta'. Each entry includes a status indicator (green checkmark), the 'IdP Entity ID', and the 'Single Sign-On' type ('User'). Action buttons for edit and delete are also present.

| Name | Status | IdP Entity ID | Single Sign-On | Actions |
|-------|--------|---|----------------|---------|
| Azure | ✓ | https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/ | User | |
| Okta | ✓ | http://www.okta.com/exks677ekzbQQdCaz0h7 | User | |

Slide notes

Slide 53 - Configuring ZPA for Okta User SSO



Configuring ZPA for Okta User SSO

D. Test the configuration and Import Attributes

Slide notes

Lastly, we'll look at how to test the Okta integration from the ZPA Admin Portal and import the available **SAML Attributes**.

Slide 54 - Slide 54

The screenshot shows the Adobe Captivate interface with the 'Administration' sidebar open. The main area displays the 'IdP Configuration' tab, which lists two entries: 'Azure' and 'Okta Box'. The 'Okta Box' entry is highlighted with a red border and a callout box containing the text 'Click to expand details for the IdP'. The 'Actions' column for each entry includes edit and delete icons.

| Name | Status | IdP Entity ID | Single Sign-On | Actions |
|----------|--------|---|----------------|---------|
| Azure | ✓ | https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/ | User | |
| Okta Box | ✓ | http://www.okta.com/exks677ekzbQQdCaz0h7 | User | |

Slide notes

Click on the name of the IdP that you just added, to expand details for it, ...

Slide 55 - Slide 55

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. The main table lists two Identity Provider (IdP) configurations: 'Azure' and 'Okta'. The 'Okta' row is expanded, showing its configuration details. A callout box with the text 'Click Import' points to the 'Import SAML Attributes' section, which contains a dropdown menu with the option 'click here'.

| Name | Status | IdP Entity ID | Single Sign-On | Actions |
|-------|--------|---|----------------|---------|
| Azure | ✓ | https://sts.windows.net/533d1d85-7ec5-41b4-96ff-f972486e0e2c/ | User | |
| Okta | ✓ | http://www.okta.com/exks677ekzbQQdCaz0h7 | User | |

Single Sign-On URL: https://patraining9.oktapreview.com/app/zscaler_private_access/exks677ekzbQQdCaz0h7/sso/saml

ZPA (SP) SAML Request: Signed

HTTP-Redirect: Disabled

Import SAML Attributes: con9.acmeconsult.net

SAML Attributes: Show Attributes >

SERVICE PROVIDER SAML METADATA FOR USER SSO:

Service Provider Metadata: Download Metadata

Service Provider URL: https://samlsp.private.zscaler.com/auth/144123467699061842/sso

Service Provider Certificate: Download Certificate

Service Provider Entity ID: https://samlsp.private.zscaler.com/auth/metadata/144123467699061842

IdP CERTIFICATE:

| | |
|--|---|
| Common Name: patraining9 | Serial Number: 1524683182930 |
| Created On: Thursday , April 26 2018 2:05:22 am | Expires On: Wednesday , April 26 2028 2:06:22 am |

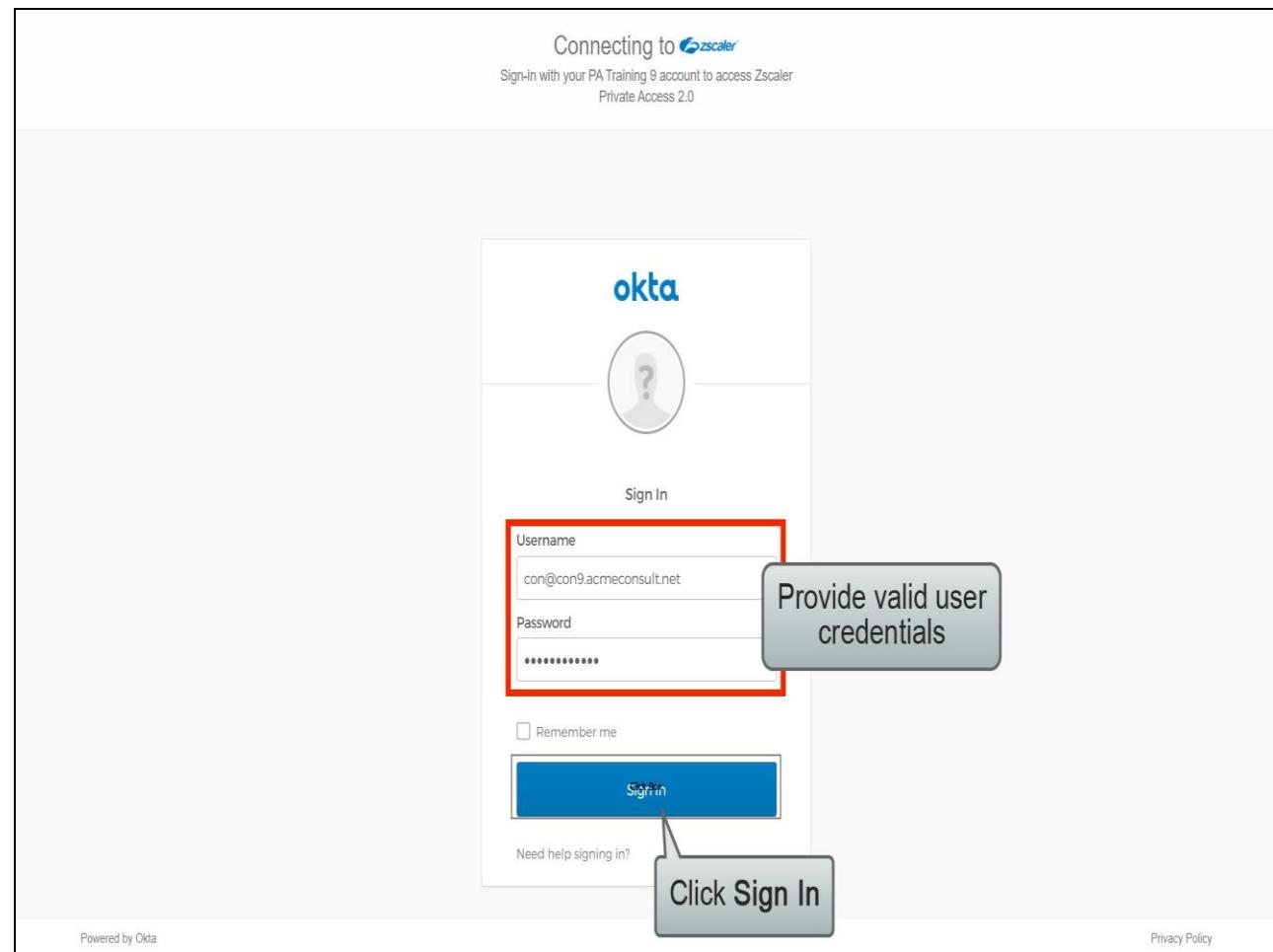
SCIM:

SCIM Sync: Disabled

Slide notes

...then click the **Import** link.

Slide 56 - Slide 56



Slide notes

At the Okta login page, provide valid credentials for a regular user (who has been assigned the ZPA Application) and click Sign In.

Slide 57 - Slide 57

Import SAML Attributes

| Name | SAML Attribute Name |
|---------------------|---------------------|
| FirstName_Okta | FirstName |
| LastName_Okta | LastName |
| Email_Okta | Email |
| DepartmentName_Okta | DepartmentName |

Import

```
{ "name": "Zscaler Consulting.net", "orgId": "14412040000000000000", "idpEntityID": "http://www.okta.com/exks677ekzbQQdCaz0h7", "idpId": "144123467699061842", "saml_attributes": { "FirstName": "Con", "LastName": "O", "Email": "training-team@zscaler.com", "DepartmentName": "Consultants" }}
```

Click Save

Review the list of SAML Attributes available for import

Help

Slide notes

If the sign in is successful, you will be shown the list of **SAML Attributes** that are available for import from this IdP. Note, we will only list attributes that do not yet exist on the **SAML Attributes** page. To import these attributes, click **Save**.

Slide 58 - Slide 58

The screenshot shows the Adobe Captivate interface with the 'Administration' tab selected. On the left, there is a sidebar with various icons: Dashboard, Diagnostics, Live Logs, Zscaler App, and Help.

The main content area displays a table titled 'SAML Attributes' under the 'IdP Configuration' section. The table has columns for 'Name', 'SAML Attribute', 'IdP Name', and 'Actions'. There are 12 rows in the table, each representing a different attribute mapping:

| Name | SAML Attribute | IdP Name | Actions |
|------------------------------|--|----------|---------|
| FirstName_Okta | FirstName | Okta | |
| LastName_Okta | LastName | Okta | |
| Email_Okta | Email | Okta | |
| DepartmentName_Okta | DepartmentName | Okta | |
| IdentityProvider_Azure | http://schemas.microsoft.com/identity/claims/identityprovider | Azure | |
| Surname_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#surname | Azure | |
| EmailAddress_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#emailaddress | Azure | |
| ObjectIdentifier_Azure | http://schemas.microsoft.com/identity/claims/objectidentifier | Azure | |
| Department_Azure | Department | Azure | |
| AuthnMethodsReferences_Azure | http://schemas.microsoft.com/claims/authnmethodsreferences | Azure | |
| Name_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#name | Azure | |
| DisplayName_Azure | http://schemas.microsoft.com/identity/claims/displayname | Azure | |
| TenantID_Azure | http://schemas.microsoft.com/identity/claims/tenantid | Azure | |

A green success message at the bottom right of the table says 'SAML attributes imported successfully' with a 'Help' link.

Slide notes

Slide 59 - Slide 59

The screenshot shows the 'SAML Attributes' page in Adobe Captivate. At the top, there are three tabs: 'IdP Configuration' (highlighted in blue), 'SAML Attributes' (selected), and 'Settings'. On the left, a vertical sidebar contains icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main area displays a table of SAML attributes:

| Name | SAML Attribute | IdP Name | Actions |
|------------------------------|--|----------|---------|
| FirstName_Okta | FirstName | Okta | |
| LastName_Okta | LastName | Okta | |
| Email_Okta | Email | Okta | |
| DepartmentName_Okta | DepartmentName | Okta | |
| IdentityProvider_Azure | http://schemas.microsoft.com/identity/claims/identityprovider | Azure | |
| Surname_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#surname | Azure | |
| EmailAddress_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#emailaddress | Azure | |
| ObjectIdentifier_Azure | http://schemas.microsoft.com/identity/claims/objectidentifier | Azure | |
| Department_Azure | Department | Azure | |
| AuthnMethodsReferences_Azure | http://schemas.microsoft.com/claims/authnmethodeferences | Azure | |
| Name_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#name | Azure | |
| DisplayName_Azure | http://schemas.microsoft.com/identity/claims/displayname | Azure | |
| TenantID_Azure | http://schemas.microsoft.com/identity/claims/tenantid | Azure | |

A callout box with the text 'Click the IdP Configuration list' points to the 'IdP Configuration Click Box' at the top right of the table header.

Slide notes

You will be taken to the **SAML Attributes** page to allow you to review all the attributes currently saved. To view a filtered list showing only the attributes for Okta, click on the **IdP Configuration** list, ...

Slide 60 - Slide 60

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Search, and Zscaler App. The main area has tabs for 'IdP Configuration', 'SAML Attributes' (which is selected), and 'Settings'. In the 'SAML Attributes' tab, there's a table with columns: Name, SAML Attribute, IdP Name, and Actions. The table lists various attributes mapped from Okta and Azure. A callout box with the text 'Click to select Okta' points to the 'Okta' button in the 'IdP Configuration' dropdown menu.

| Name | SAML Attribute | IdP Name | Actions |
|------------------------------|--|----------|---------|
| FirstName_Okta | FirstName | Okta | |
| LastName_Okta | LastName | Okta | |
| Email_Okta | Email | Okta | |
| DepartmentName_Okta | DepartmentName | Okta | |
| IdentityProvider_Azure | http://schemas.microsoft.com/identity/claims/identityprovider | Azure | |
| Surname_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#surname | Azure | |
| EmailAddress_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#emailaddress | Azure | |
| ObjectIdentifier_Azure | http://schemas.microsoft.com/identity/claims/objectidentifier | Azure | |
| Department_Azure | Department | Azure | |
| AuthnMethodsReferences_Azure | http://schemas.microsoft.com/claims/authnmethodsreferences | Azure | |
| Name_Azure | http://schemas.xmlsoap.org/ws/2005/05/identity/claimsschema#name | Azure | |
| DisplayName_Azure | http://schemas.microsoft.com/identity/claims/displayname | Azure | |
| TenantID_Azure | http://schemas.microsoft.com/identity/claims/tenantid | Azure | |

Slide notes

...and click to select Okta.

Slide 61 - Slide 61

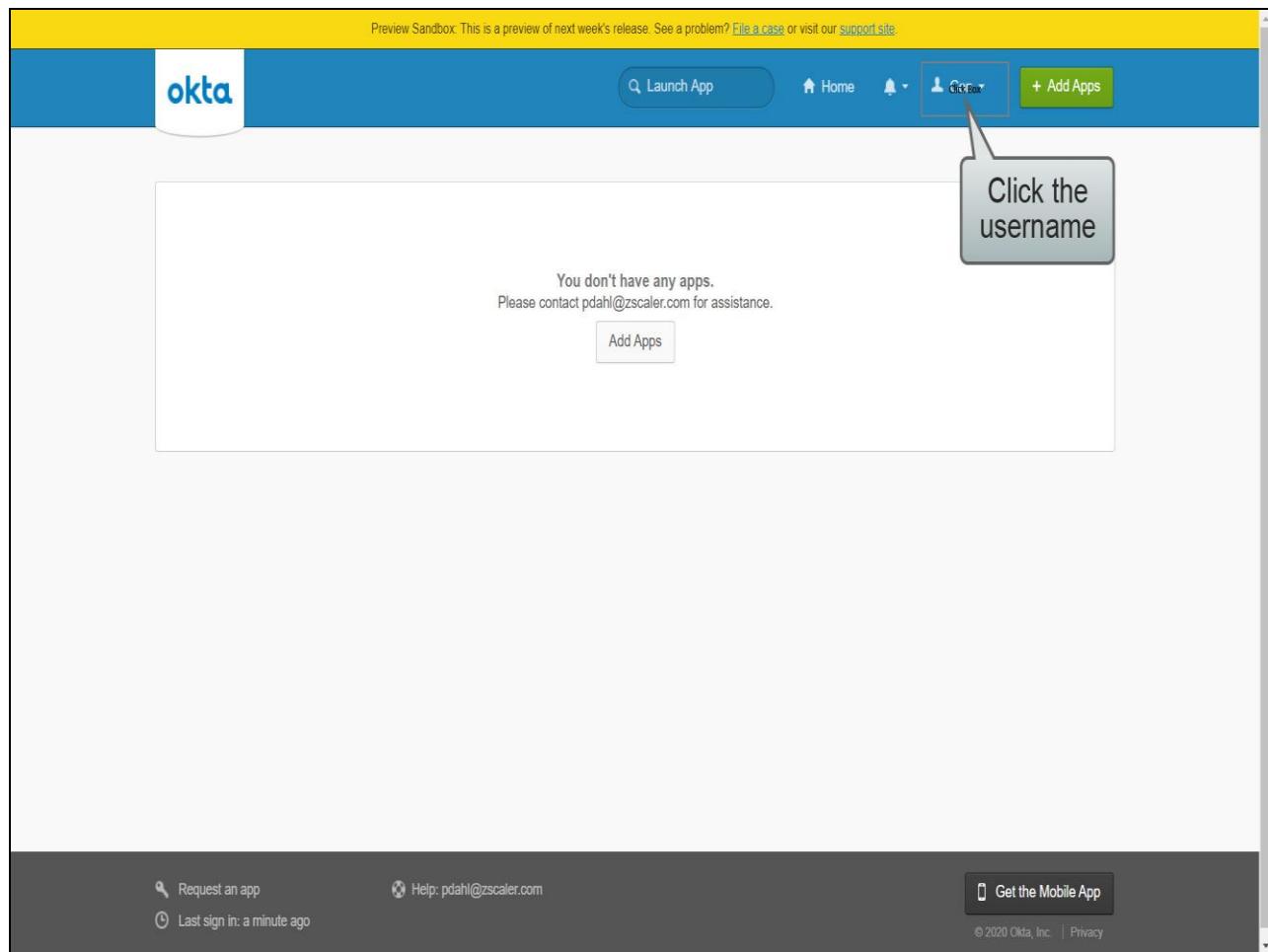
The screenshot shows the Okta SAML Attributes configuration interface. On the left is a navigation sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help. The main content area has tabs for IdP Configuration, SAML Attributes (which is selected), and Settings. It displays a table of attributes:

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

At the top right, there is a link to "Add SAML Attribute". The "IdP Configuration" dropdown is set to "Okta".

Slide notes

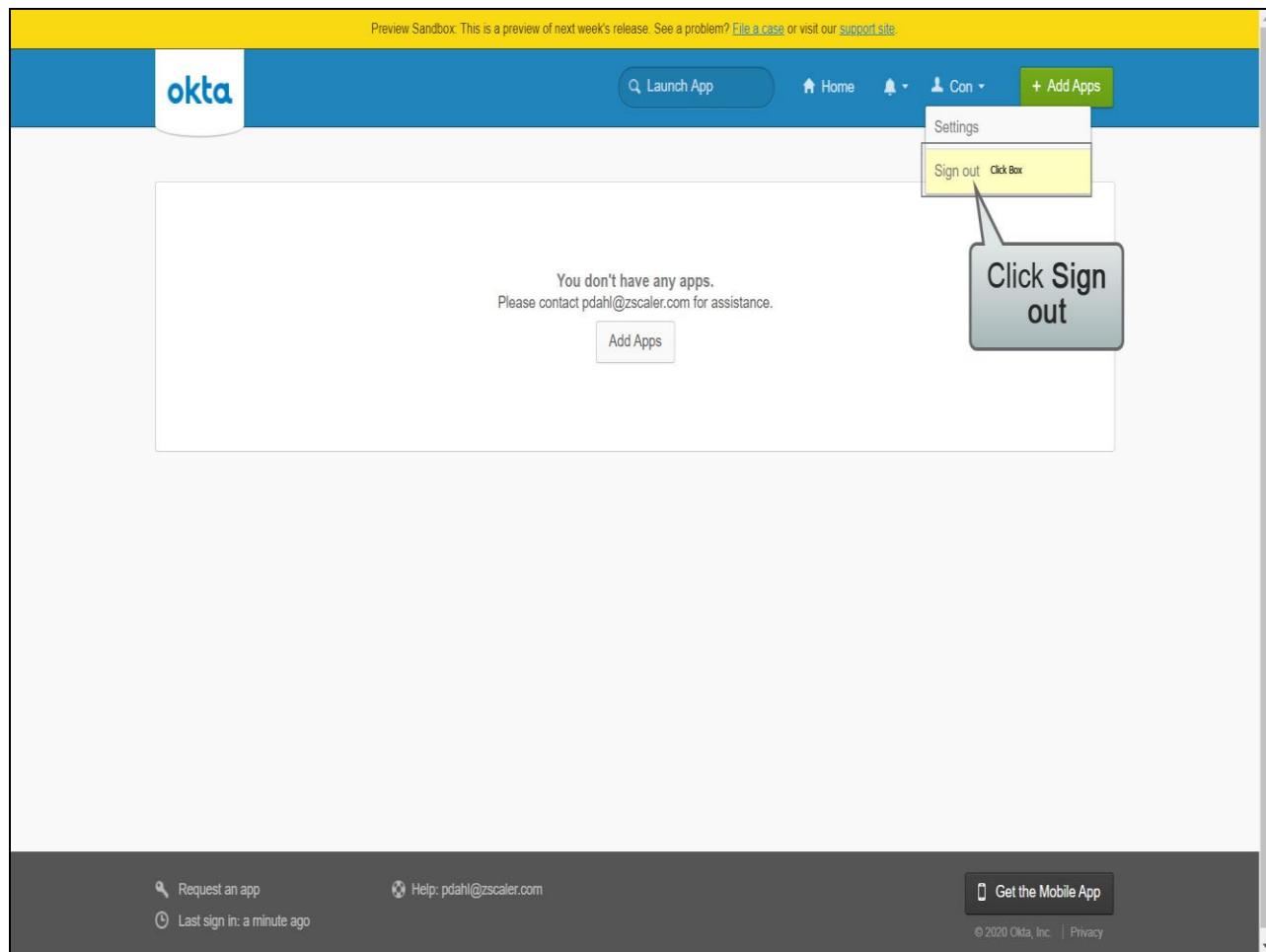
Slide 62 - Slide 62



Slide notes

Finally, don't forget to sign out of the Okta Portal! Reload the Okta page if necessary, then click the username, ...

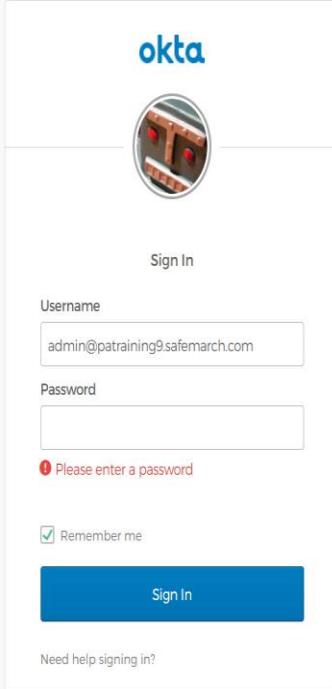
Slide 63 - Slide 63



Slide notes

...and click **Sign out**.

Slide 64 - Slide 64



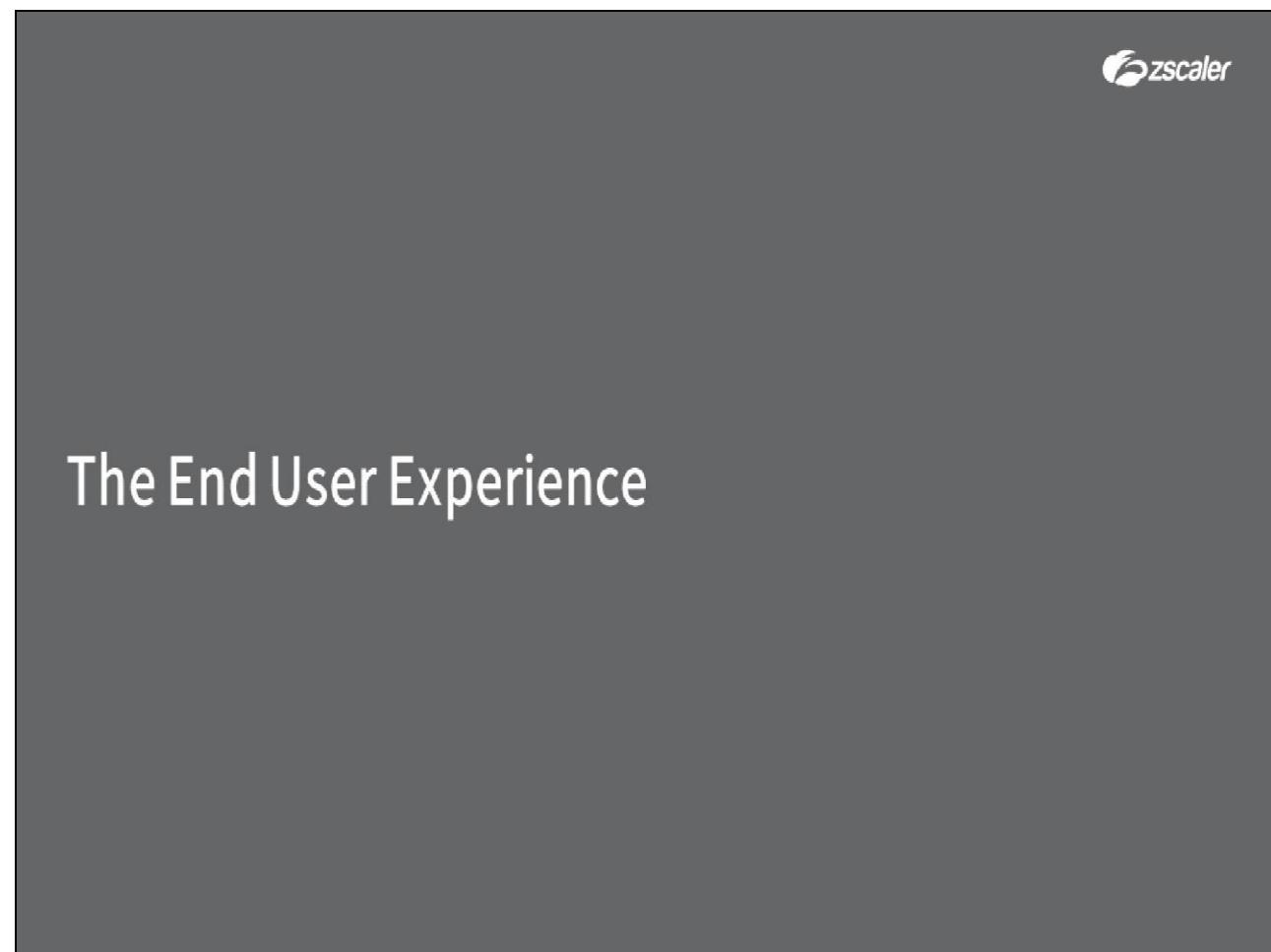
The image shows a screenshot of the Okta sign-in page. At the top center is the Okta logo. Below it is a circular profile picture placeholder. To the right of the logo is a "Sign In" button. The main area contains two input fields: "Username" with the value "admin@patraining9.safemarch.com" and "Password" which is currently empty. A red error message "Please enter a password" is displayed below the password field. There is a "Remember me" checkbox followed by a checked "Remember me" option. At the bottom is a large blue "Sign In" button. Below the button is a link "Need help signing in?".

Powered by Okta

Privacy Policy

Slide notes

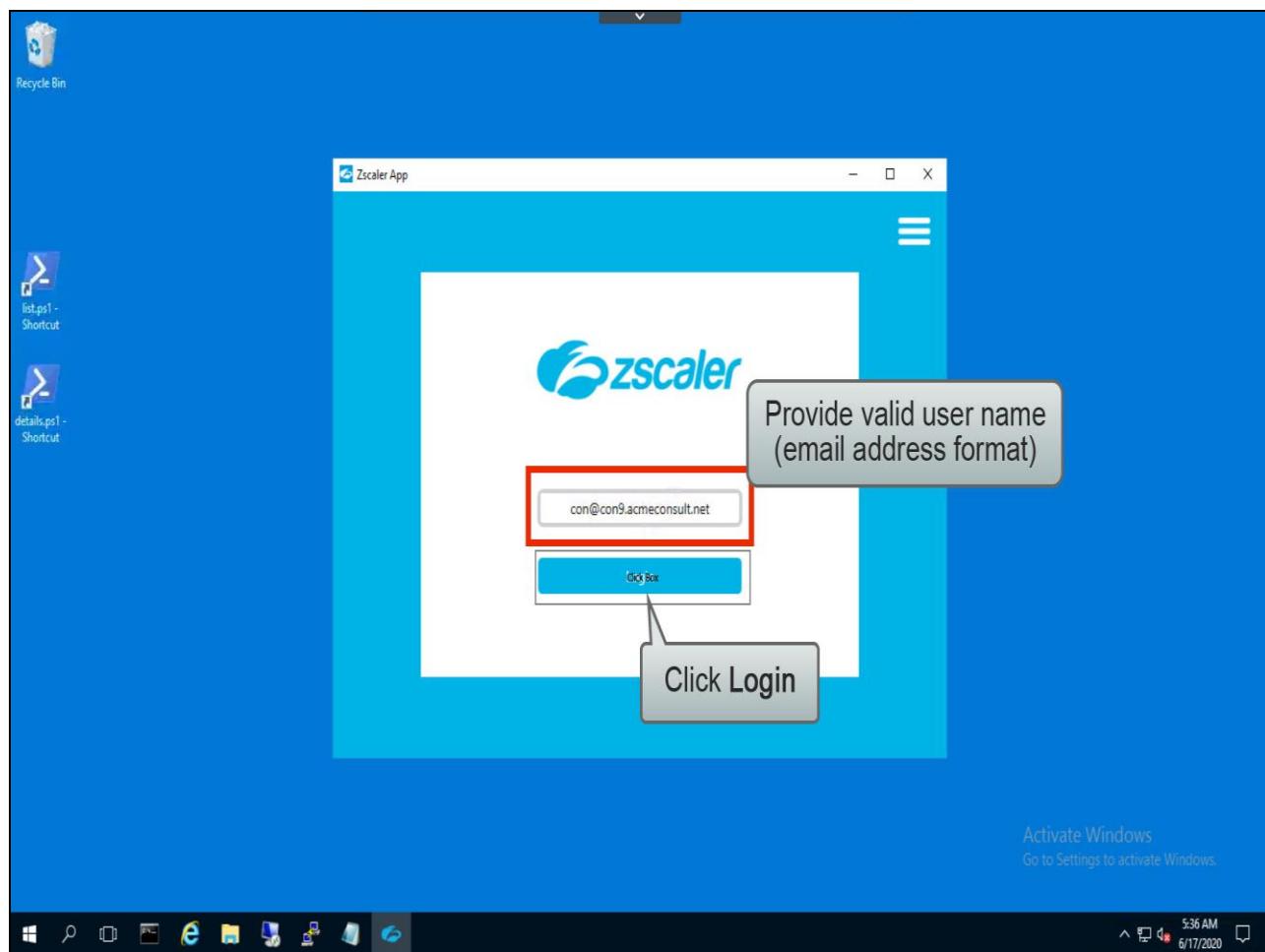
Slide 65 - The End User Experience

**Slide notes**

In the final section, we will have a look at the end user experience once authentication through Okta is configured.

This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler App UI. 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.

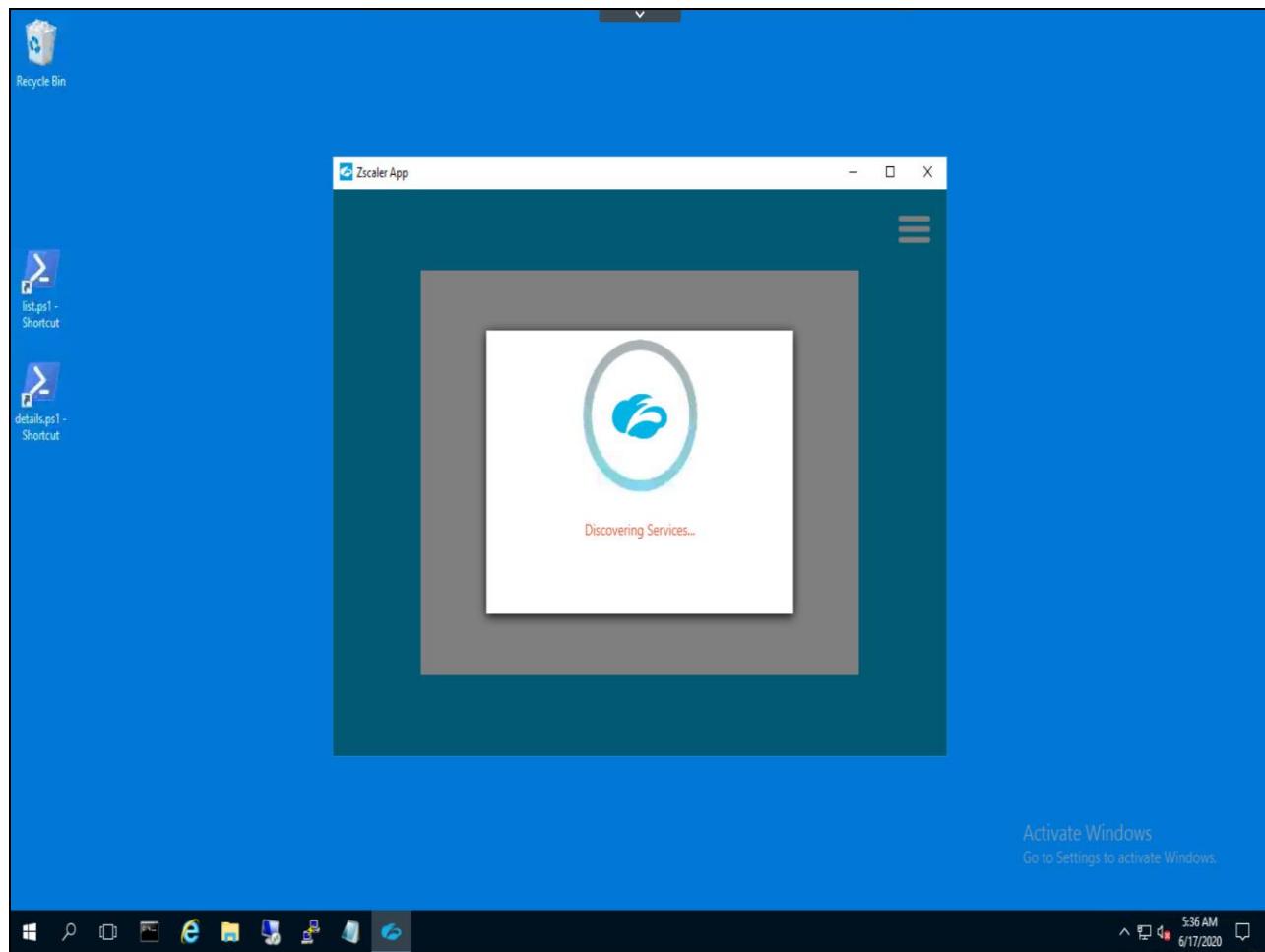
Slide 66 - Slide 66



Slide notes

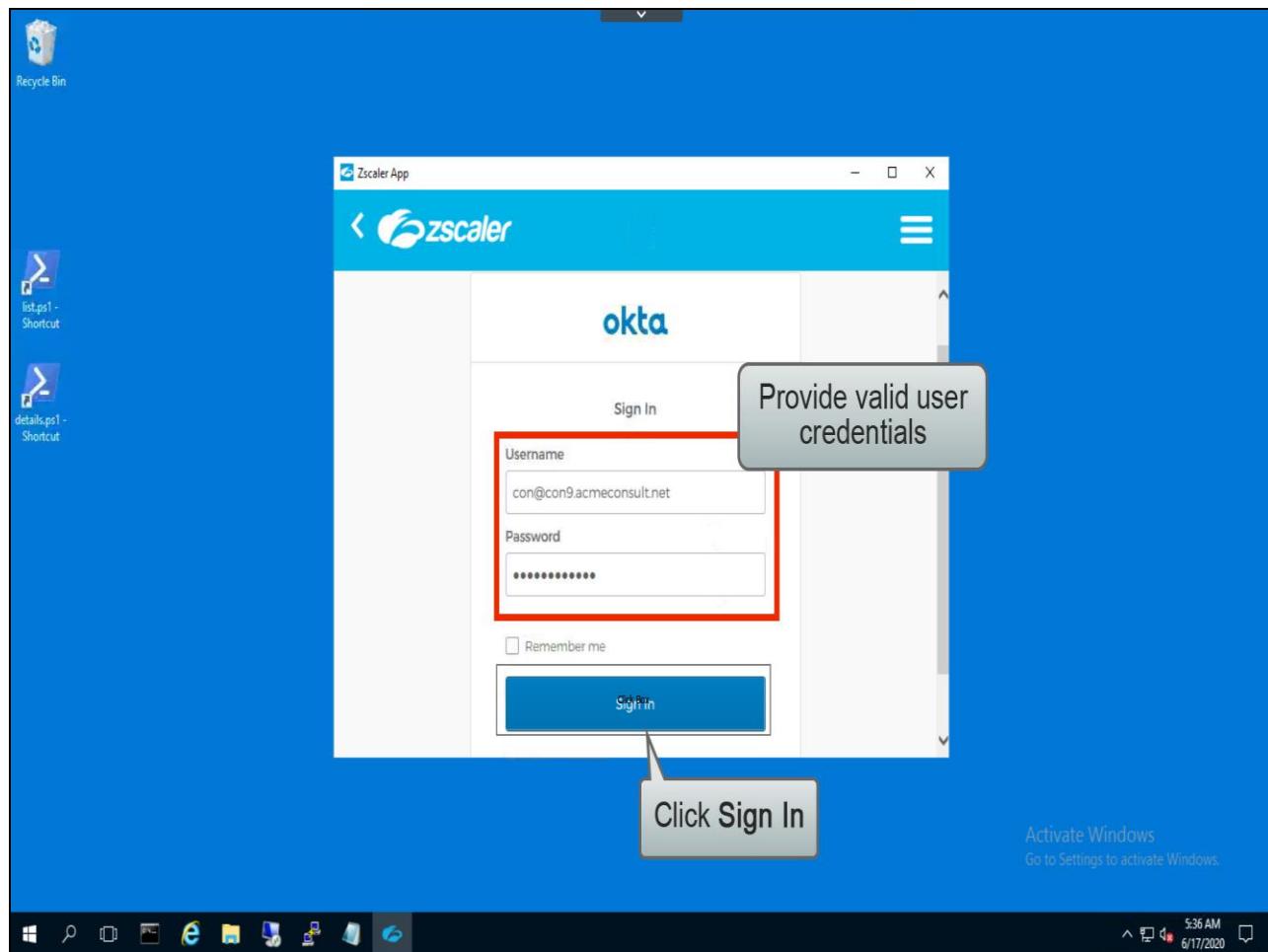
On a client machine that has the Zscaler App installed on it (PC or mobile, for this example we will use a Windows client), run the App, provide valid end user credentials (in the form of an email address) and click **Login**.

Slide 67 - Slide 67



Slide notes

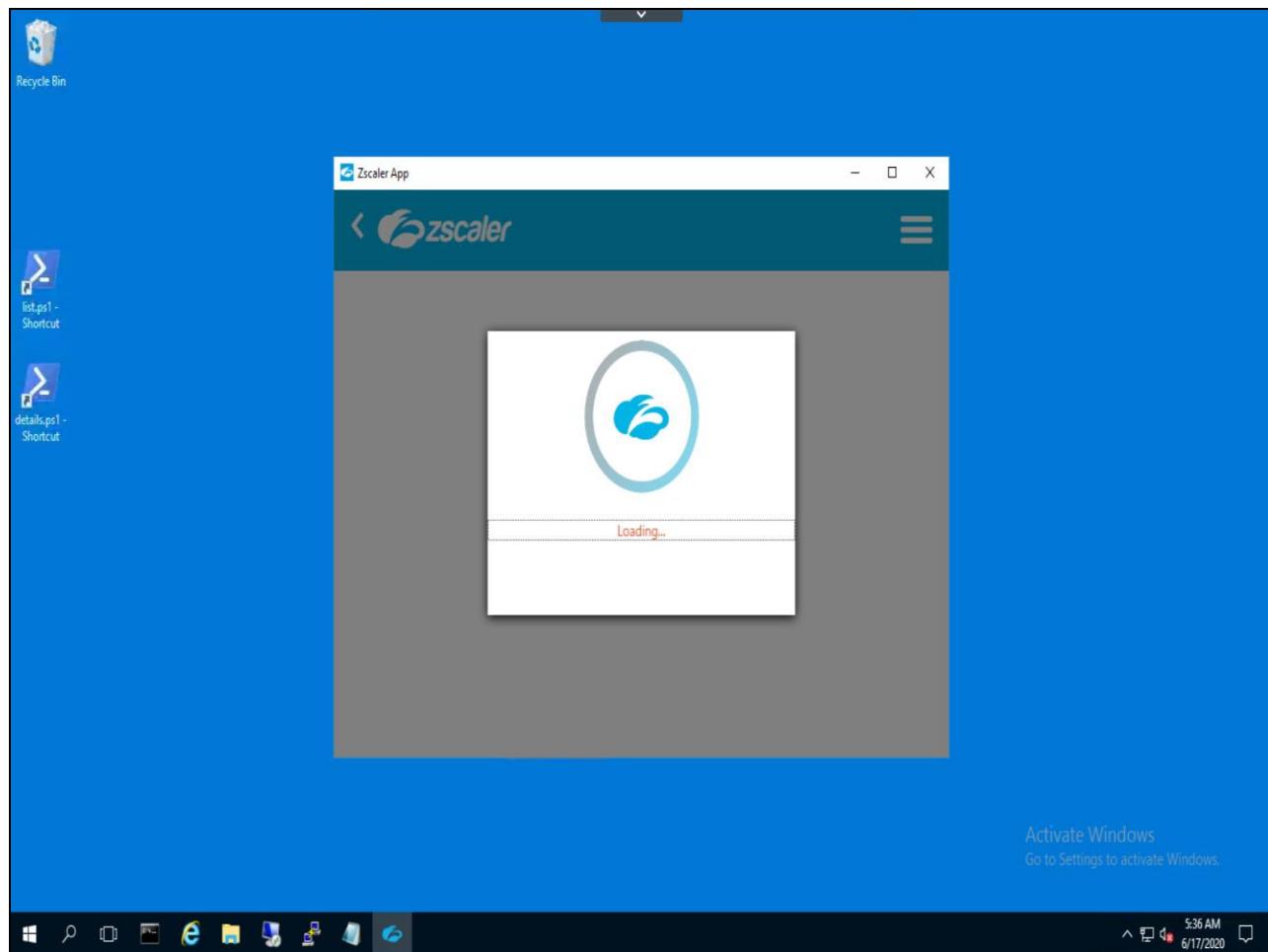
Slide 68 - Slide 68



Slide notes

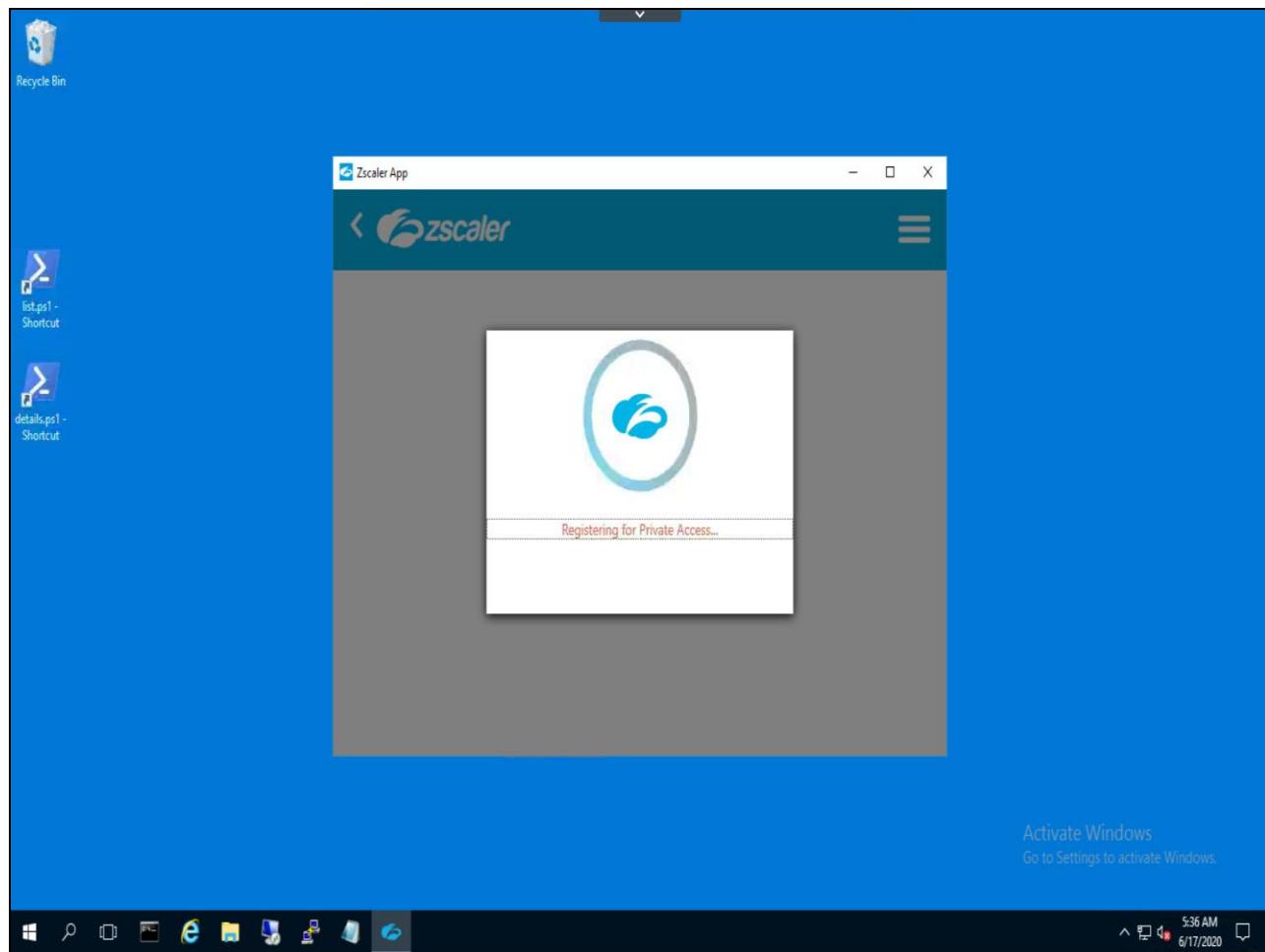
Once the Okta login page loads, provide the username and password and click **Sign In**.

Slide 69 - Slide 69



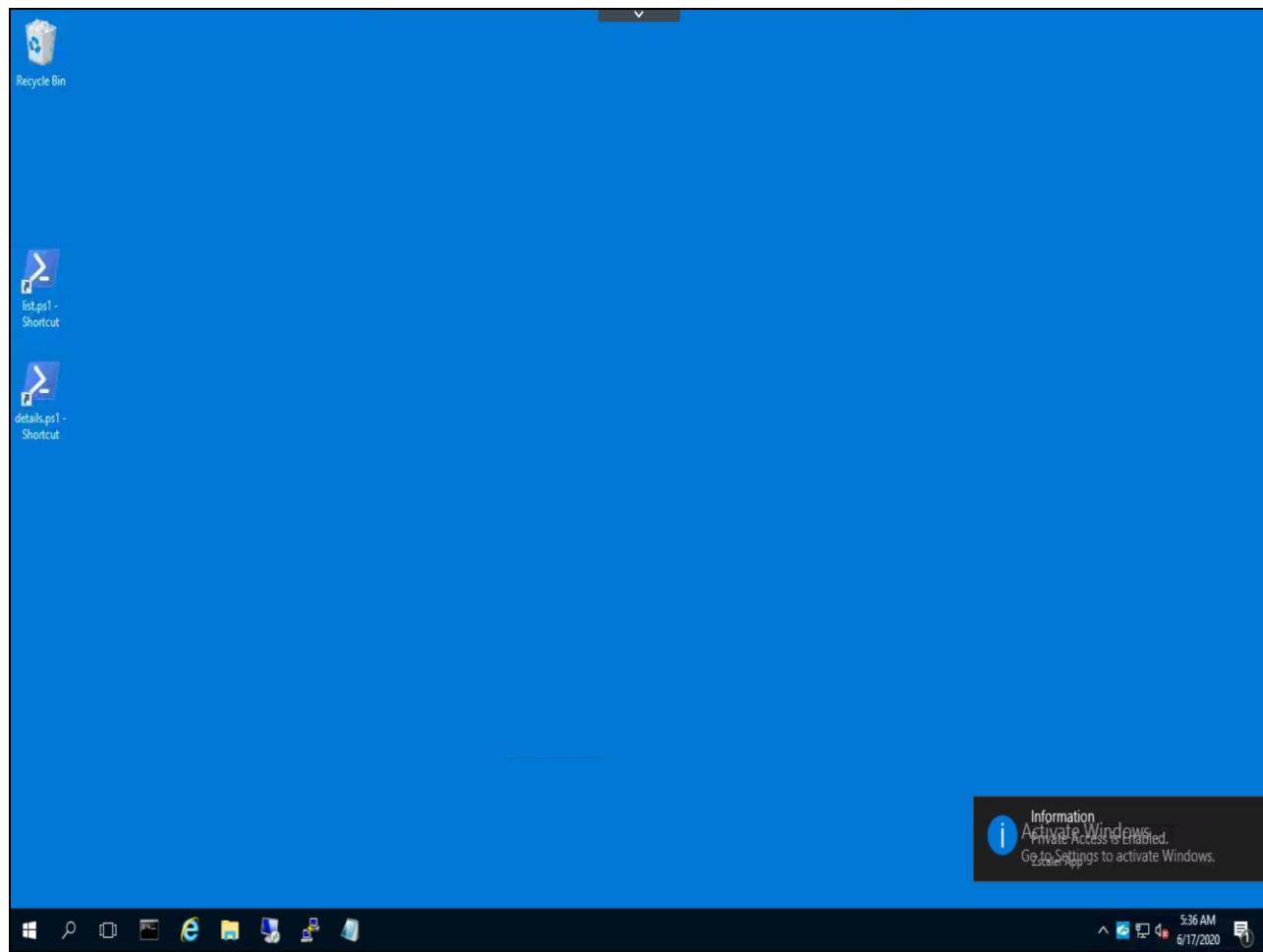
Slide notes

Slide 70 - Slide 70



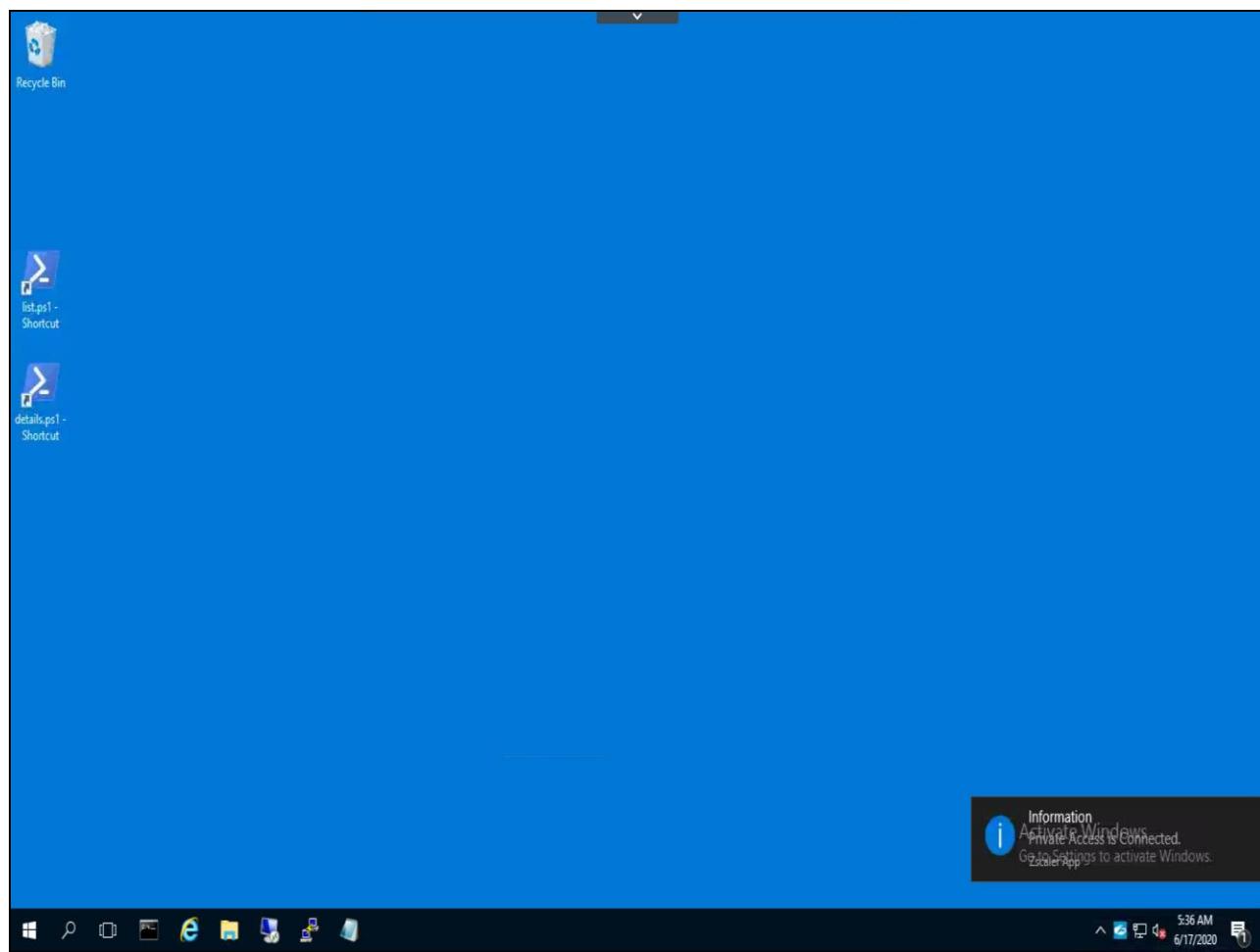
Slide notes

Slide 71 - Slide 71



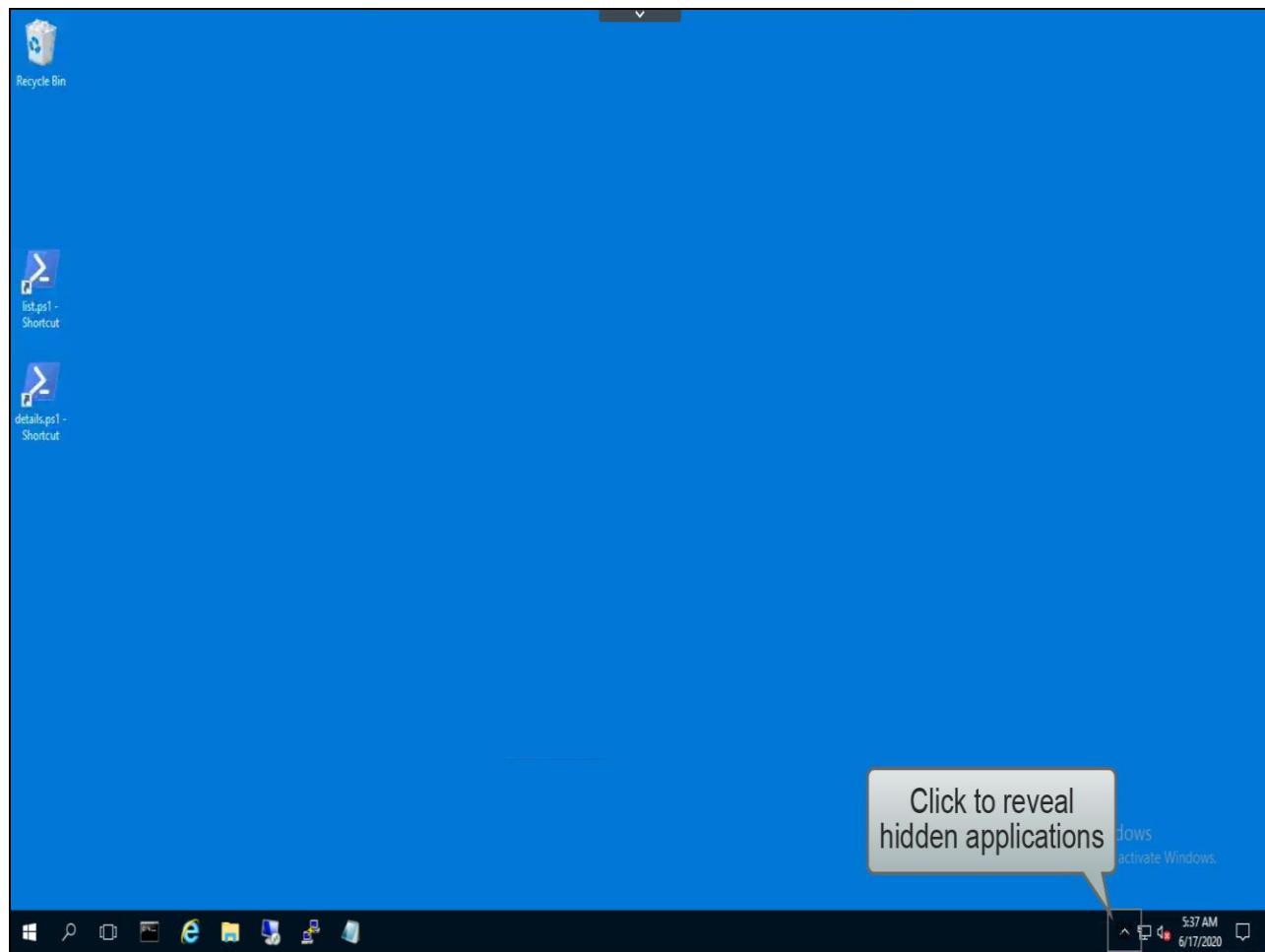
Slide notes

Slide 72 - Slide 72



Slide notes

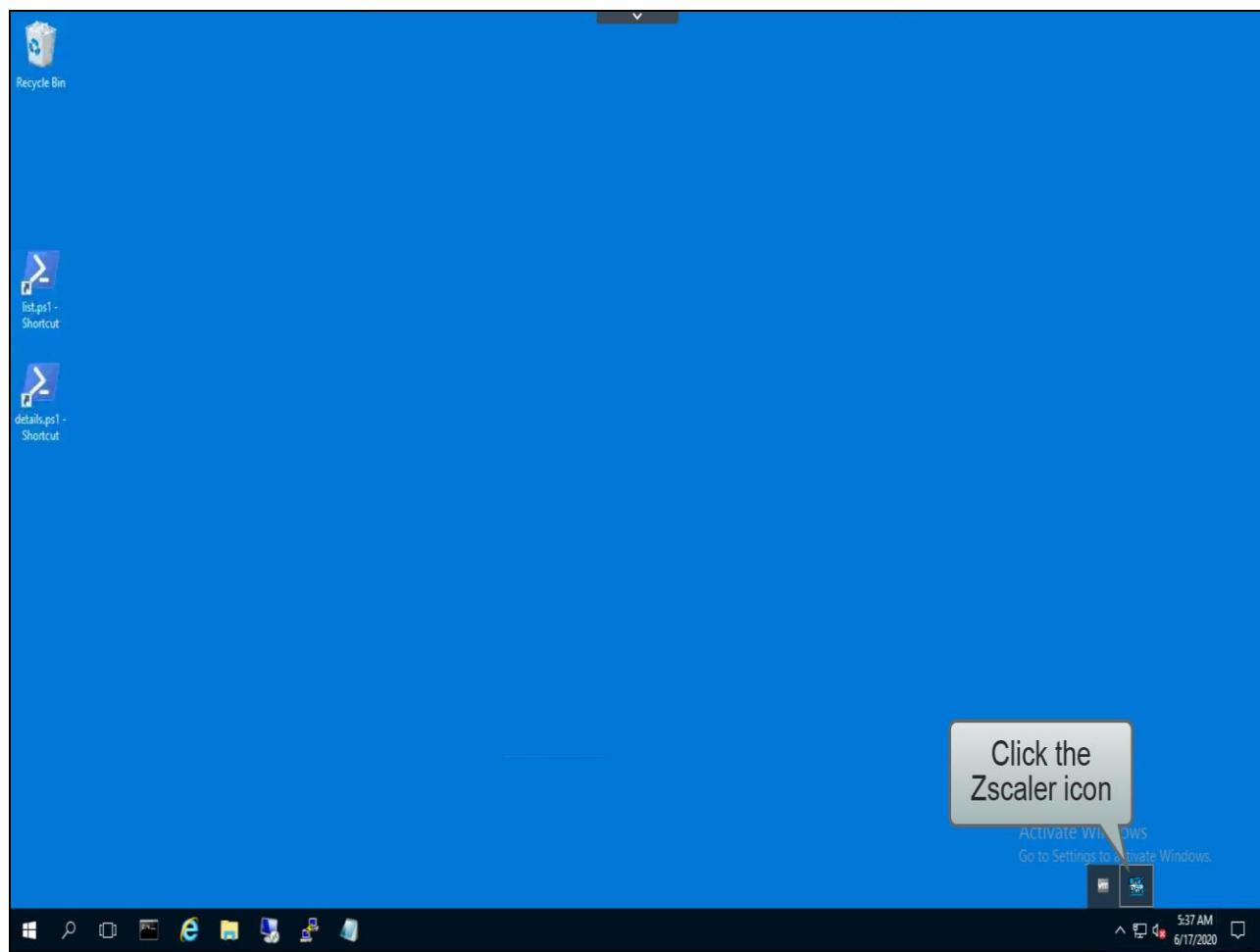
Slide 73 - Slide 73



Slide notes

On Windows, after a successful login, the Zscaler App will minimize itself to the Status Bar. To open it you will need to click to reveal hidden applications, ...

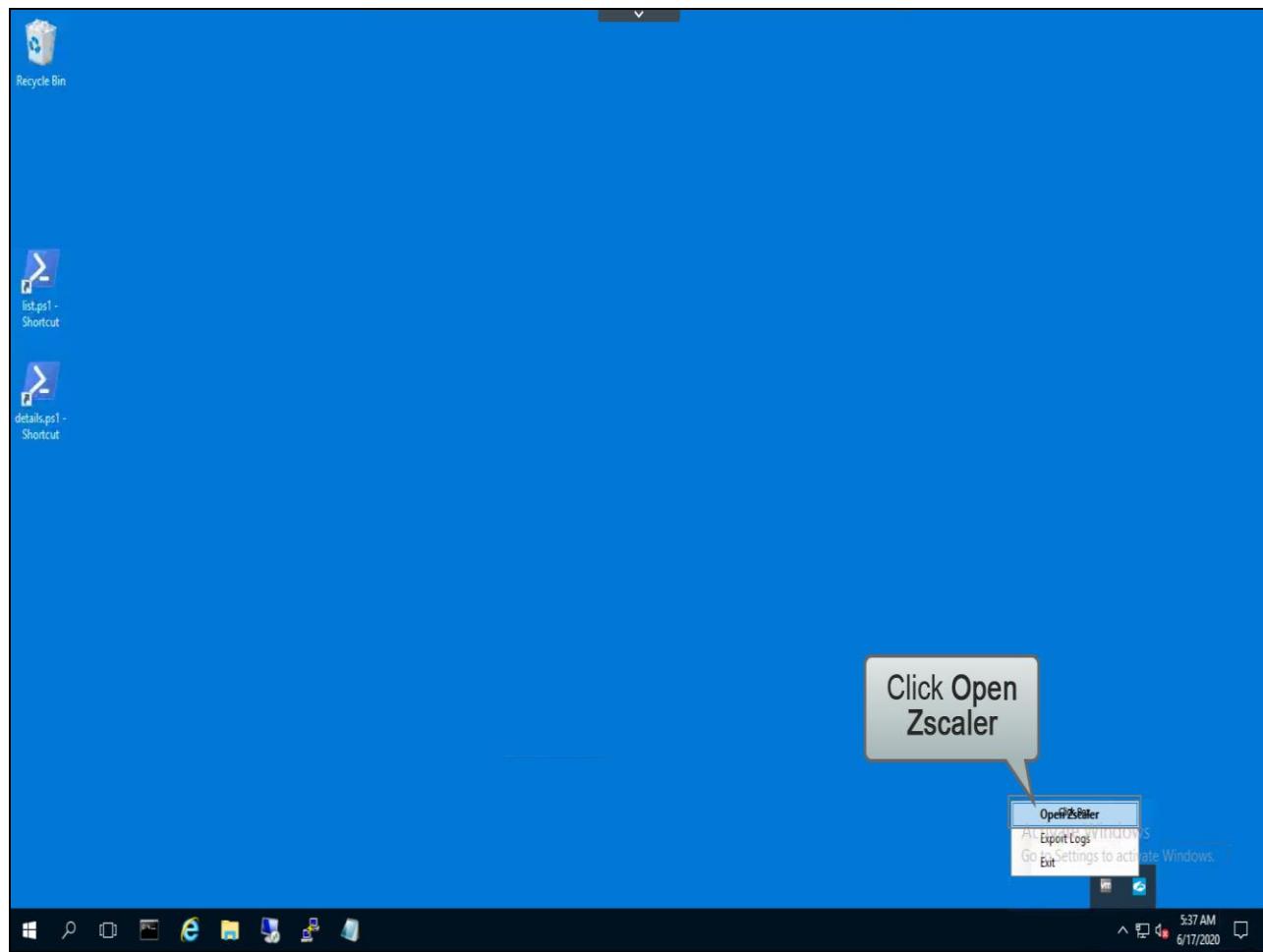
Slide 74 - Slide 74



Slide notes

...then click on the Zscaler App icon, ...

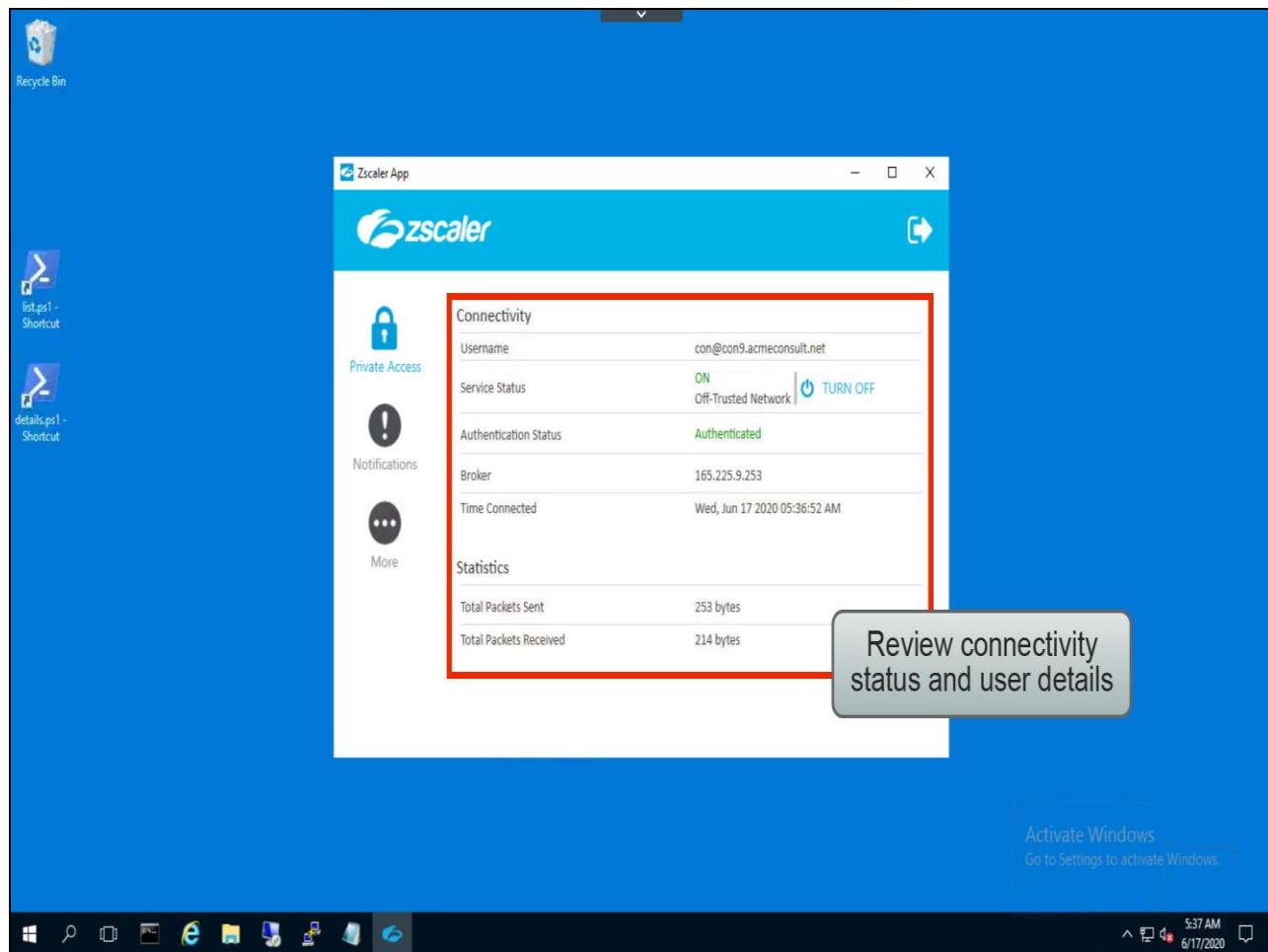
Slide 75 - Slide 75



Slide notes

...and click **Open Zscaler**.

Slide 76 - Slide 76



Slide notes

Review the user and connection status on the **Private Access** page, to:

- Verify that ZPA functionality is **On**;
- To see the **Username** that you are enrolled into the App with;
- To see your **Authentication Status** and **Time Connected**;
- And to see data volume statistics.

Slide 77 - Thank You and Quiz



Thank You and 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.