

Slide 1 – Authentication with SAML – Azure AD



Zscaler Private Access

Authentication with SAML – Azure AD

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on configuring ZPA to use Azure AD (AAD) for authenticating users.

Slide 2 - Navigating the eLearning Module

The screenshot shows the Zscaler ZPA Basic Administration 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 are displayed in cards: "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). To the right of these cards is a blue "Exit" button with a white "X". In the center, there are two main sections: "TOP APPLICATIONS BY BANDWIDTH" and "TOP POLICY BLOCKS". The bandwidth section lists applications with their data usage: 23.97 MB (safebarlab.safemarch.com), 8.11 MB (github.safemarch.com), 7.26 MB (crm.safemarch.com), 6.48 MB (w10.safemarch.com), 3.96 MB (splunk.myscaler.com), 3.38 MB (intranet.local), 1.92 MB (intranet.safemarch.local), 1.80 MB (splunk.safemarch.com), 1.45 MB (server01.safemarch.com), and 1.02 MB (crm.local). The policy blocks section shows "Access Policy Blocks" and "Timeout Policy Blocks". At the bottom left, there are playback controls: "Play/Pause", "Previous Slide", "Next Slide", and a "Progress Bar". At the bottom right, there are "Audio On/Off" and "Closed Captioning" controls.

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



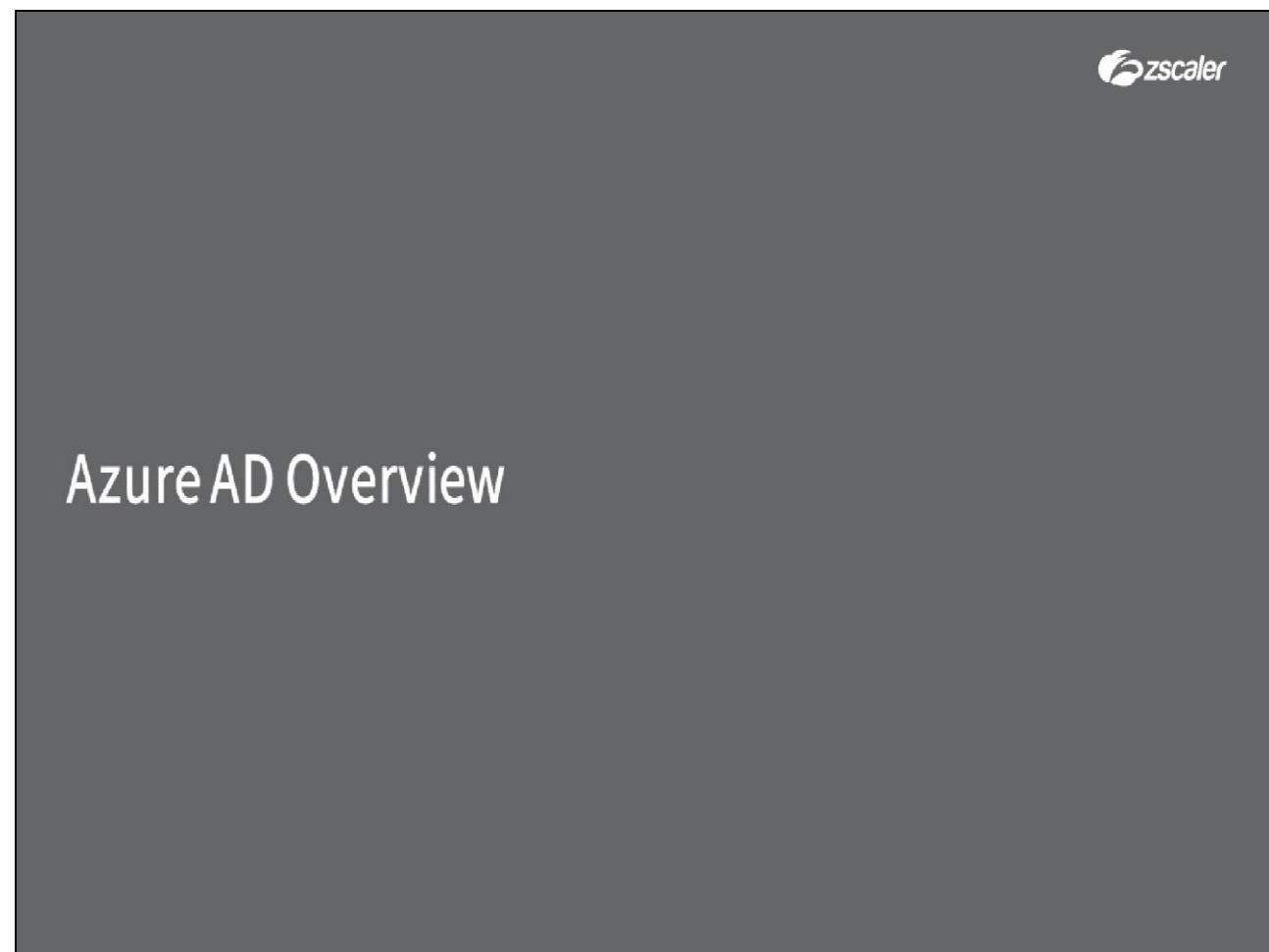
- Azure AD Overview
- Configuring Azure AD
 - A. Add a new IdP in ZPA for User Authentication
 - B. Add / Configure the ZPA Application in AAD
 - C. Complete the IdP Setup in ZPA
 - D. Test the Configuration and Import Attributes
- The End User Experience

Slide notes

In this module we will:

- Provide an overview of the Azure AD 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 AAD as an **Enterprise 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

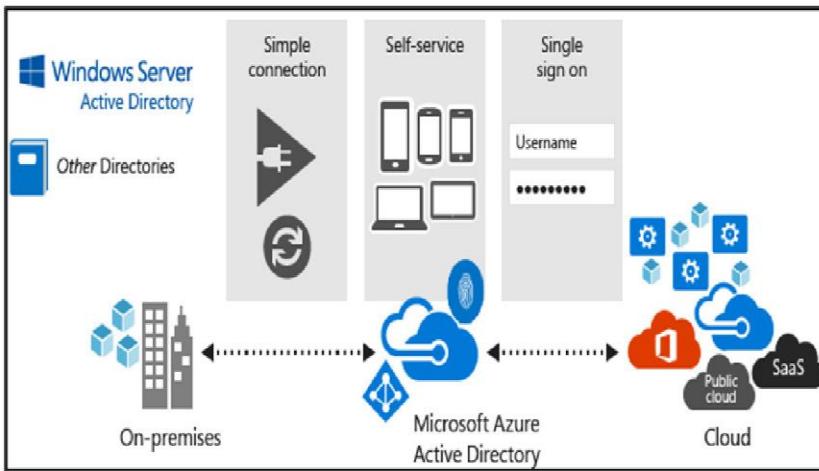
In the first section, we provide an overview of the Azure AD solution.

Slide 5 - Microsoft Azure Active Directory (AAD)



Microsoft Azure Active Directory (AAD)

- Microsoft Identity Management
 - AAD = Multi-tenant, cloud-based directory and identity management service
 - Compatible with and complements their on-premise Active Directory (AD) solution
 - Provides SAML 2.0 compatible authentication services

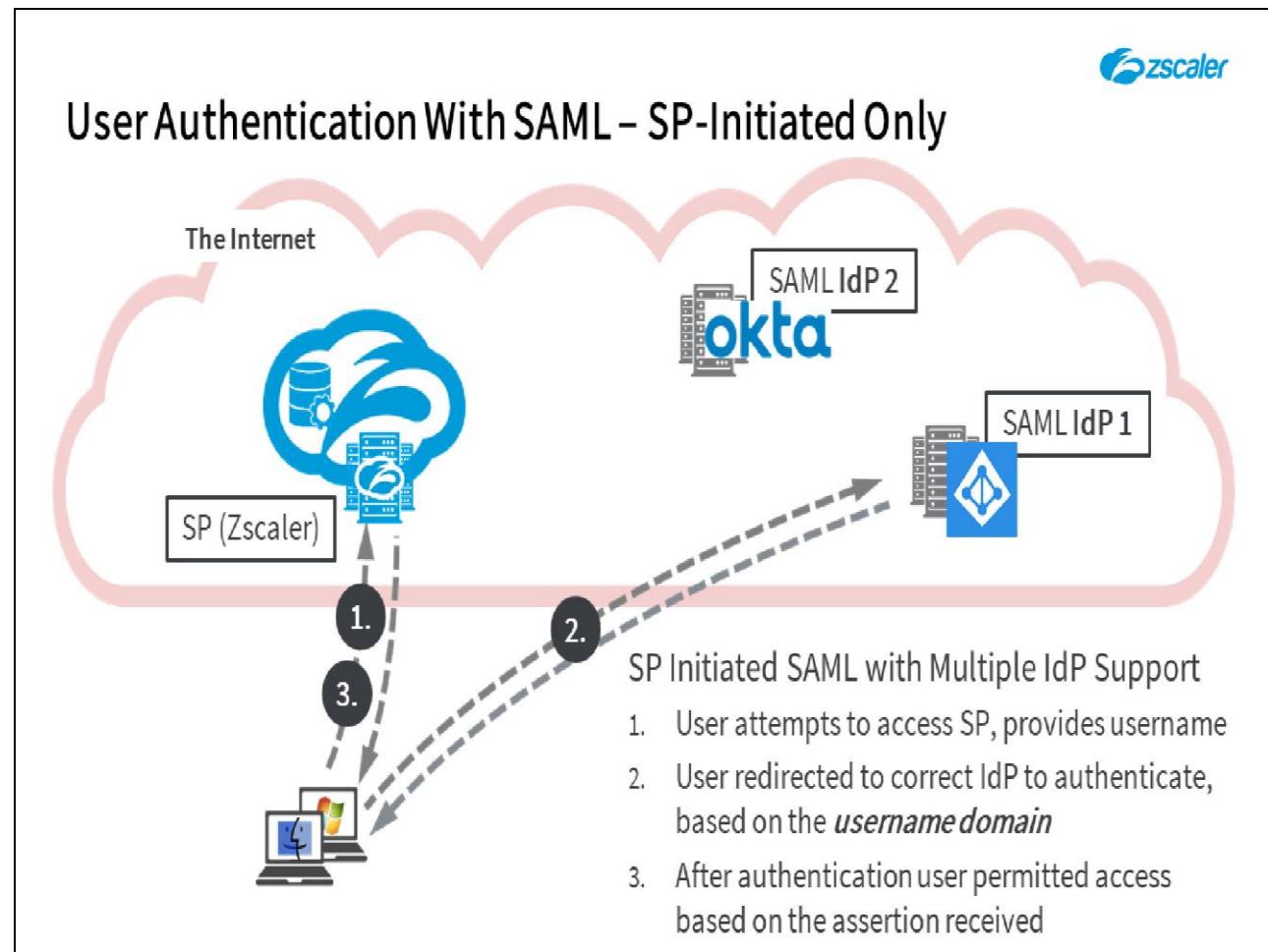


Slide notes

Azure Active Directory (AAD) is Microsoft's multi-tenant, cloud-based directory, and identity management service that combines core directory services, application access management, and identity protection into a single solution. AAD also offers a rich, standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules.

AAD is fully compatible with and complements the Microsoft on-premise Active Directory (AD) solution, and can be used to provide cloud-based, SAML 2.0 compliant authentication services, both SP-initiated and IdP-initiated.

Slide 6 - User Authentication With SAML – SP-Initiated Only

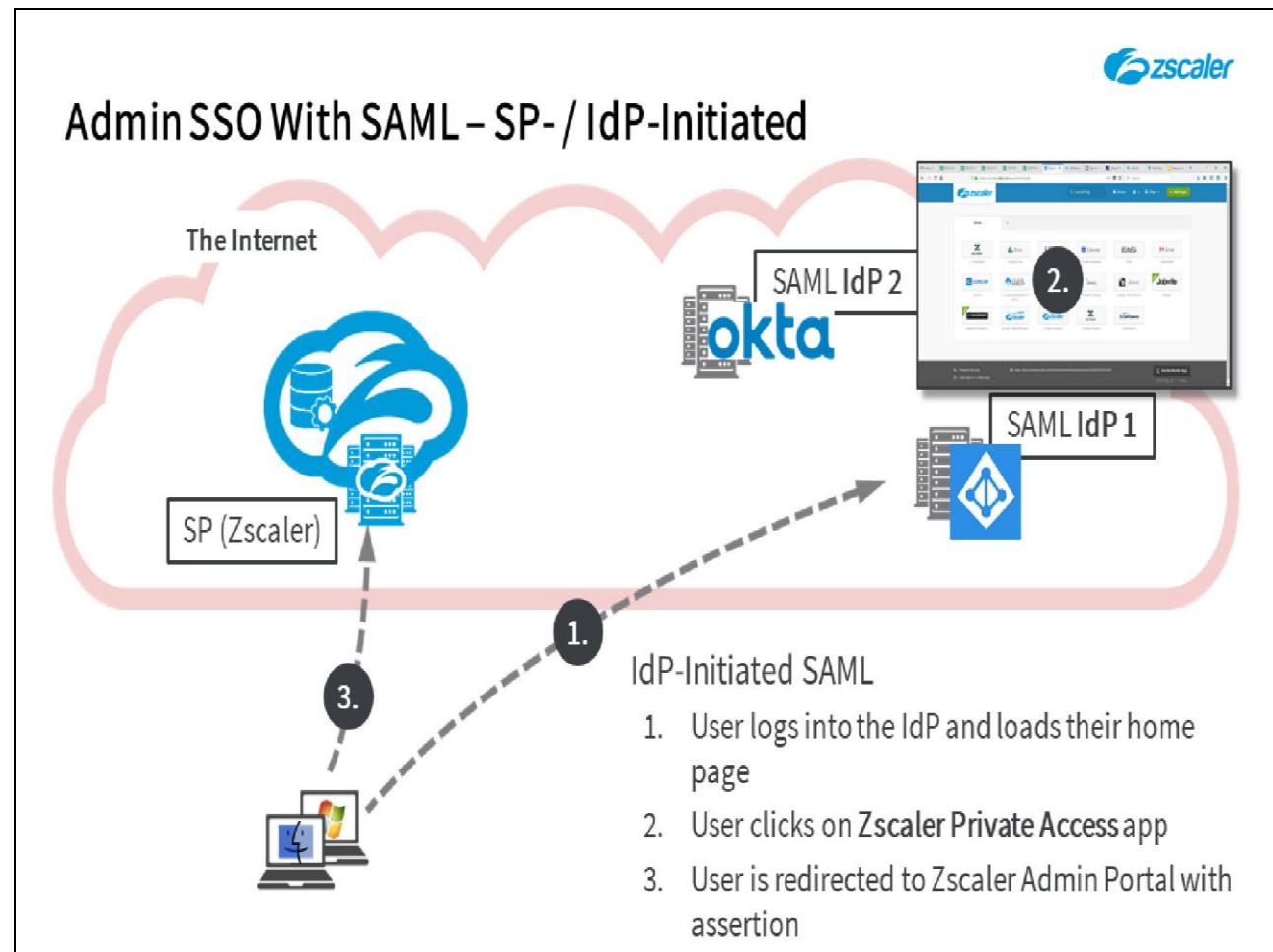


Slide notes

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

With the Multiple IdP capability, the user (or Z App Installer) must provide domain information at enrollment, to allow the ZPA service to identify the correct IdP to use to authenticate the user.

Slide 7 - Admin SSO With SAML – SP- / IdP-Initiated



Slide notes

For administrator SSO both SP-initiated and IdP-initiated SAML are supported. AAD is also a suitable platform to support admin SSO to the ZPA service, although note that an AAD Premium license is required for this.

Slide 8 - Useful Okta Features

AAD Directory Integration Options

The diagram illustrates the integration options between on-premises Active Directory (AD) and Azure AD. It features two clouds: a larger pink cloud at the top labeled "The Internet" containing a blue diamond icon representing Azure AD, and a smaller grey cloud at the bottom labeled "Azure AD Connect Agent" containing a blue diamond icon representing the Azure AD Connect Agent. A thick black arrow points from the Azure AD icon up towards the Azure AD Connect Agent icon, with the text "Account Sync" written vertically along the arrow. In the top right corner of the slide area, there is a small Zscaler logo.

- Azure AD Connect
 - Installed on one an AD Domain Controller per AD Forest
 - Syncs user accounts to AAD
 - Optional password write-back
 - AD FS for advanced authentication options such as 3rd party MFA
 - Health monitoring

Slide notes

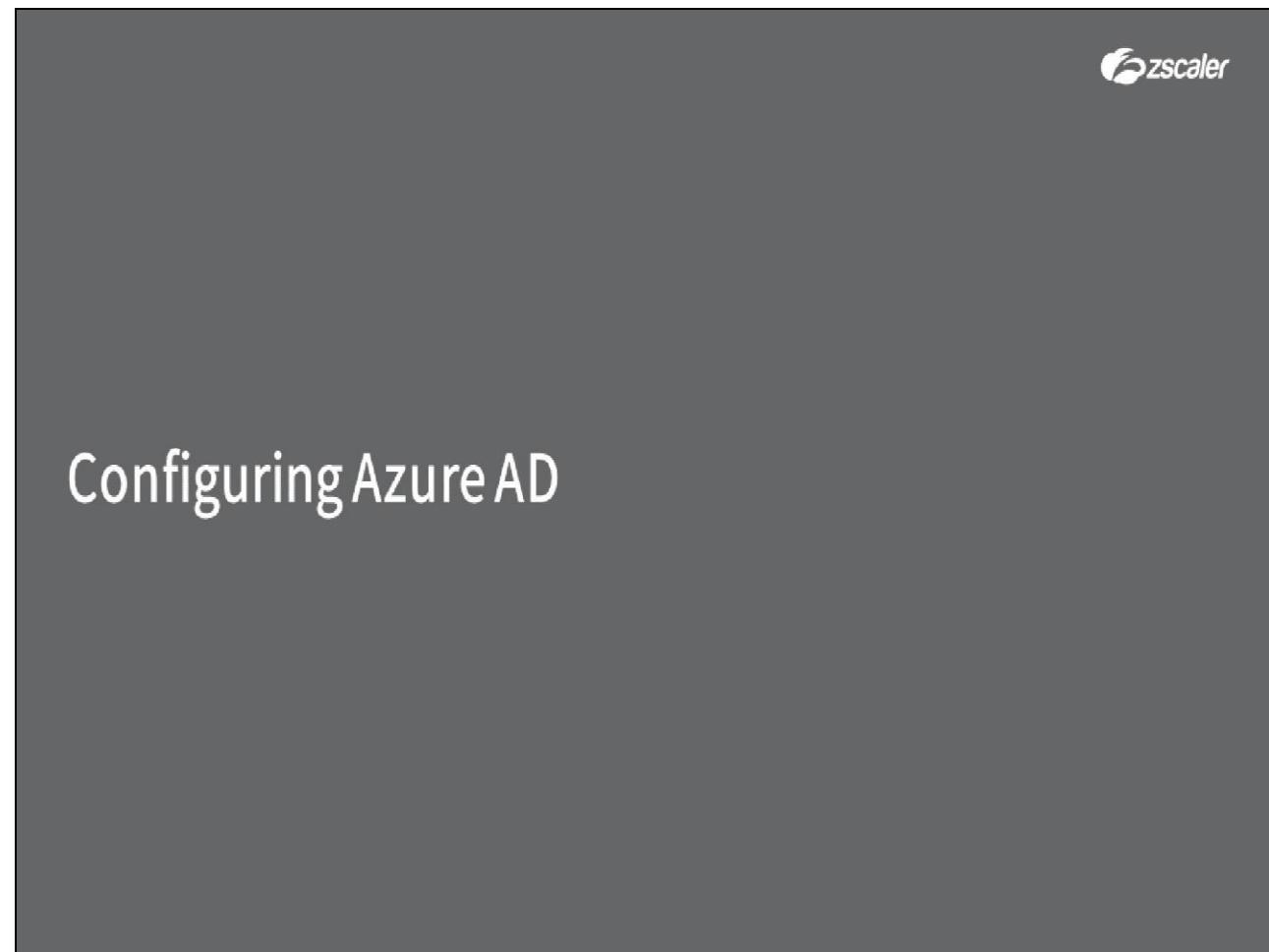
Azure AD can be used as a stand-alone directory for user authentication, or it can be integrated with an existing directory system, most commonly Microsoft AD. An **AAD Connect** agent is available that can be installed on one AD Domain Controller per Forest, which allows the synchronization of user accounts from AD to AAD.

AAD Connect is the only tool you need to get the integration done. **AAD Connect** provides capabilities to support your identity synchronization needs and replaces older versions of identity integration tools such as **DirSync** and **AAD Sync**. With **AAD Connect**, identity management and synchronization between on-premises and Azure AD is enabled through:

- **Synchronization** - This component is responsible for creating users, groups, and other objects. It is also responsible for making sure identity information for your on-premises users and groups is matching the cloud. Password write-back can also be enabled to keep on-premises directories in sync when a user updates their password in Azure AD.
- **AD FS** - Federation is an optional capability provided by **AAD Connect** that can be used to configure a hybrid environment using an on-premises AD FS infrastructure. Federation can be used by organizations to address complex deployments, such as smart card or third-party Multi-Factor Authentication (MFA).

- **Health Monitoring - AAD Connect Health** can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Slide 9 - Configuring Okta



Configuring Azure AD

Slide notes

In the next section, we will look at the configuration of Azure AD to act as a SAML IdP for ZPA.

This section has been created as an interactive demo to give you a feel for the navigation of the Azure AD 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 10 - Configuring ZPA for Okta User SSO



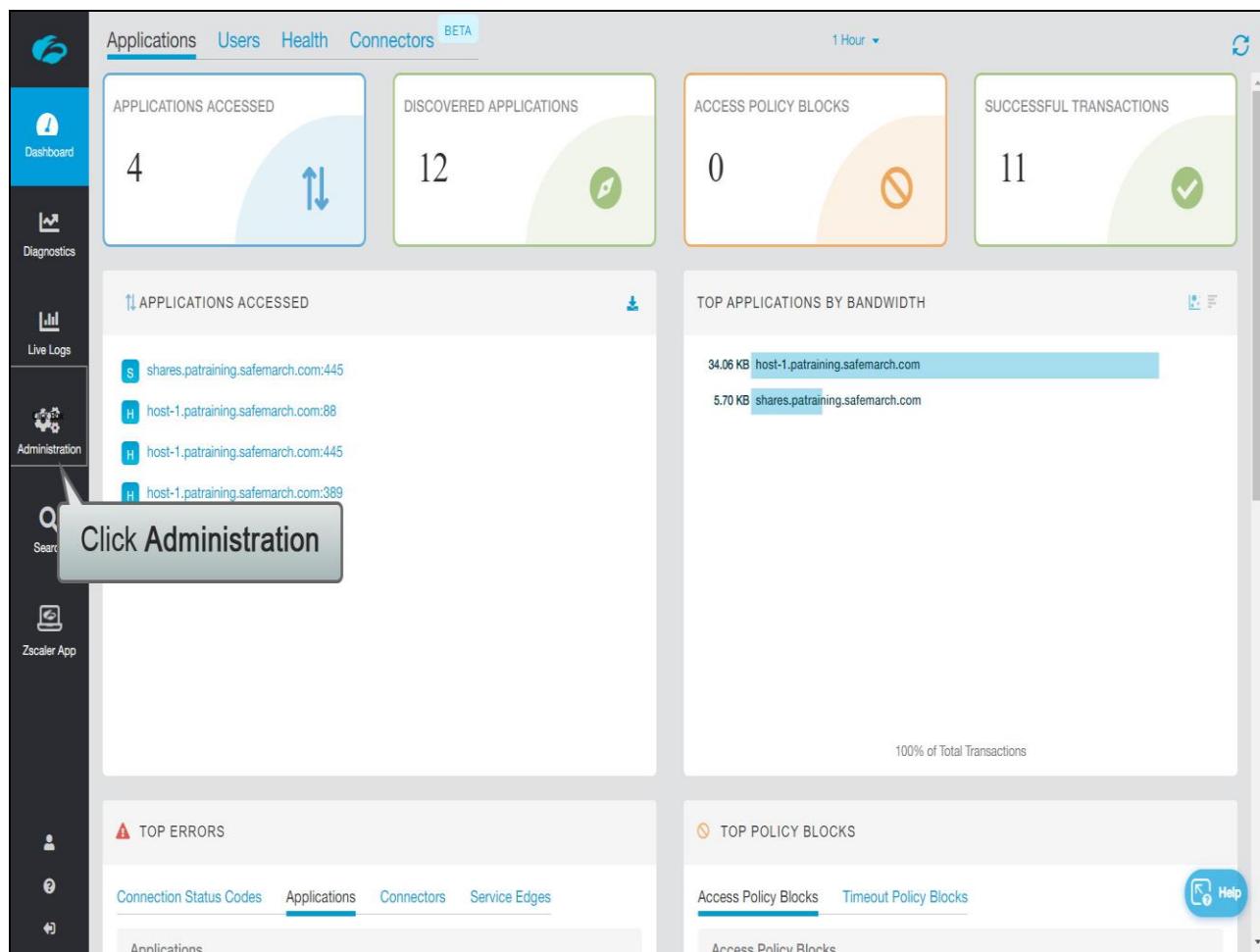
Configuring ZPA for AAD User SSO

A. Add a new IdP in ZPA for User Authentication

Slide notes

First, we will look at adding a new SAML IdP in the ZPA Admin Portal for end user SSO.

Slide 11 - Slide 11



Slide notes

Login to the ZPA Admin Portal with a suitable admin account, then to access the **IdP Configuration** page, click **Administration**, ...

Slide 12 - Slide 12

The screenshot shows the Zscaler Cloud interface. On the left, a dark sidebar contains various navigation links: Application Management (Application Segments, Segment Groups, Servers), Authentication (IdP Configuration, Settings, SAML Attributes), Diagnostics, Live Logs, Administration (Certificates, Browser Access), Search, Zscaler App, Connector Management (Connectors, Connector Groups, Connector Provisioning Keys), Log Streaming Service (Connector Groups, Log Receivers), Policy Management (Access Policy, Client Forwarding Policy, Timeout Policy), Reporting (Executive Insights App, Access), and Help.

A callout box with a grey border and black text points to the "IdP Configuration" link under the Authentication section, with the text "Click IdP Configuration".

The main dashboard area features several cards:

- BERED APPLICATIONS**: Shows 0 applications.
- ACCESS POLICY BLOCKS**: Shows 0 blocks.
- SUCCESSFUL TRANSACTIONS**: Shows 11 transactions.
- TOP APPLICATIONS BY BANDWIDTH**: A chart showing bandwidth usage. The top entry is "34.06 KB host-1.patraining.safemarch.com".
- TOP POLICY BLOCKS**: A chart showing policy blocks. The top entry is "Access Policy Blocks".

At the bottom right of the dashboard is a blue "Help" button with a gear icon.

Slide notes

...then IdP Configuration.

Slide 13 - Slide 13

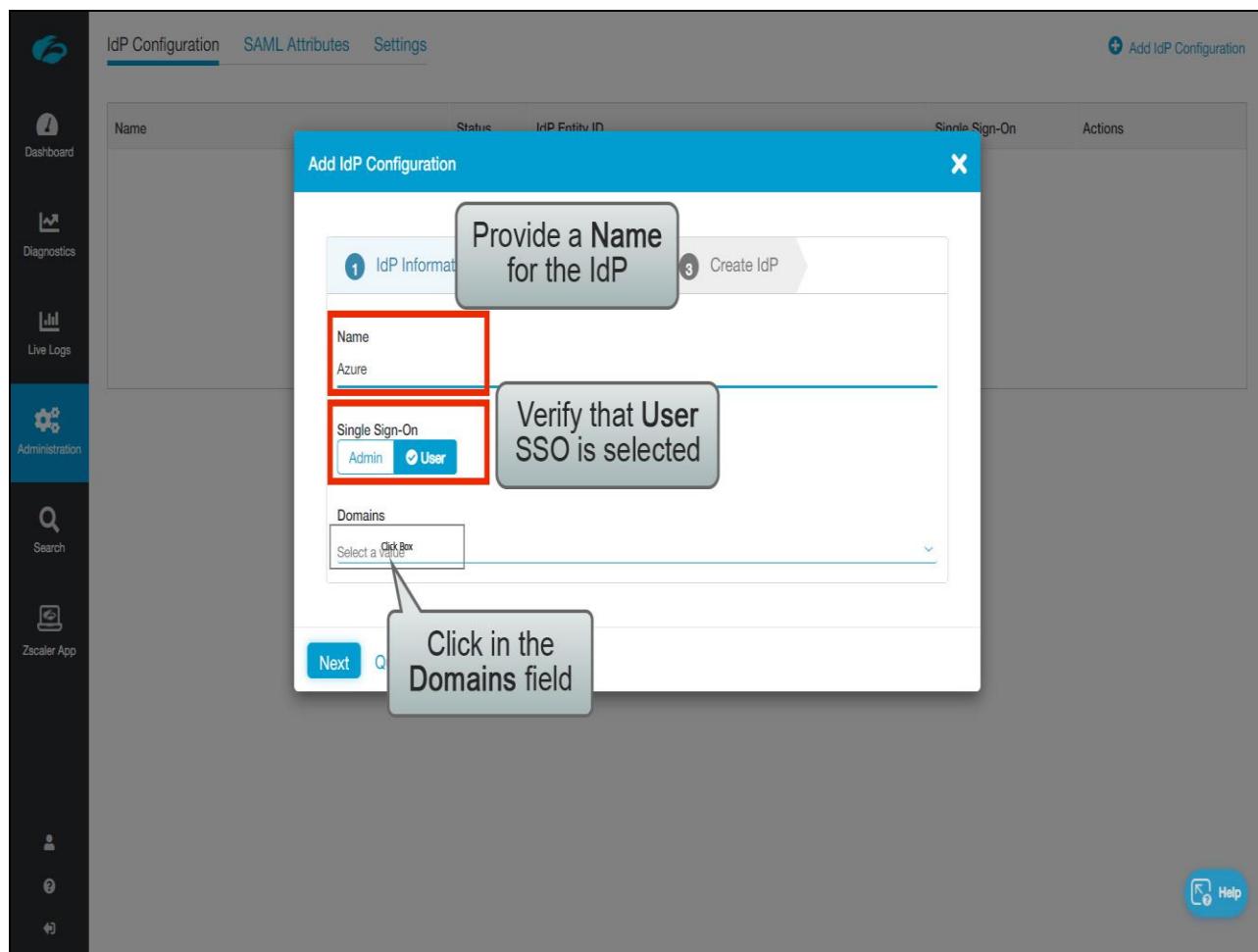
The screenshot shows the Zscaler Admin Portal interface. On the left is a vertical navigation bar with icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, Zscaler App, and other user-related options. The main content area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with columns: Name, Status, and IdP Entity ID. A message 'No Items Found' is displayed. In the top right corner of the main area, there is a blue button labeled 'Add IdP Configuration'. A large callout box with a blue border and white text points to this button, containing the instruction 'Click Add IdP Configuration'. In the bottom right corner of the main area, there is a 'Help' button.

Slide notes

You have the option to add up to 10 IdP configurations at the ZPA Admin Portal and each one that you add will be assigned a globally unique Service Provider **Entity ID** and **Login URL**. This is the reason that you must start the process to add an IdP in the ZPA Admin Portal.

To add a new IdP, click **Add IdP Configuration**.

Slide 14 - Slide 14



Slide notes

Give the new IdP a suitable **Name** and select the intended population for **Single Sign-On**; **Admin**, or **User** (the default setting). It is necessary to map this IdP to one or more of the available authentication Domains defined on the tenant. Every tenant will be configured with the requested **Primary Authentication Domain**, you may request that we add as many additional **Secondary Authentication Domains** as you need. Note that a domain can only be added to a single tenant.

To select the appropriate domains from those available on the tenant, click in the **Domains** field, ...

Slide 15 - Slide 15

The screenshot shows the Zscaler Admin interface with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, showing three steps: 1. IdP Information, 2. SP Metadata, and 3. Create IdP. The first step is active. The 'Name' field is populated with 'Azure'. Under 'Single Sign-On', the 'User' radio button is selected. In the 'Domains' section, a tooltip with the text 'Click to select the correct Domain (or Domains)' points to a dropdown menu containing 'clickboxtraining9.safemarch.com' and 'con9.acmeconsult.net'. The 'Help' button is visible in the bottom right corner of the modal.

Slide notes

...then click to select one or more of the available **Domains**, ...

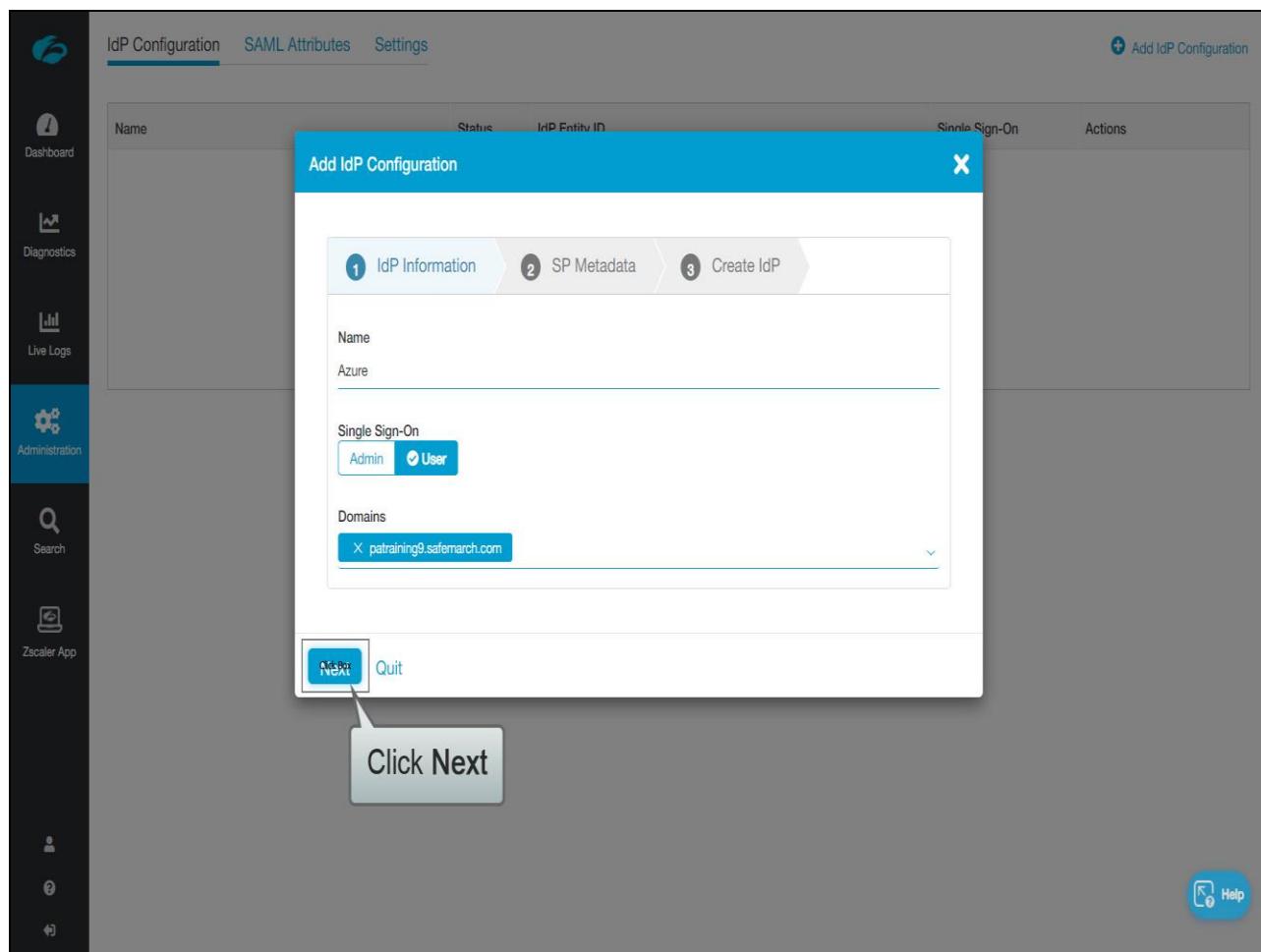
Slide 16 - Slide 16

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 'Azure'. Under 'Single Sign-On', the 'User' radio button is selected. In the 'Domains' section, 'patraining9.safemarch.com' is listed with a checked checkbox. Other options like 'con9.acmeconsult.net' are shown with unchecked checkboxes. A large callout box with the text 'Click Done' points to the 'Done' button at the bottom left of the modal.

Slide notes

...and click Done.

Slide 17 - Slide 17



Slide notes

To proceed with the wizard, click **Next**, ...

Slide 18 - Slide 18

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, showing three steps: 'IdP Information', 'SP Metadata' (which is highlighted), and 'Create IdP'. In the 'SP Metadata' step, there is a section for 'SERVICE PROVIDER SAML METADATA FOR USER SSO' containing 'Service Provider Metadata' and 'Service Provider Certificate' download links. Below this, the 'Service Provider URL' and 'Service Provider Entity ID' are displayed. A red box highlights the URL and Entity ID fields. A callout bubble points to the 'Download Metadata' link with the text 'Click Download Metadata'. Another callout bubble points to the highlighted URL and Entity ID fields with the text 'Unique Service Provider URL and Entity ID'.

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. To download the metadata, click the **Download Metadata** link.

Slide 19 - Slide 19

The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected in the top navigation bar. A modal window titled 'Add IdP Configuration' is open, showing a three-step process: 1. IdP Information, 2. SP Metadata (which is currently active), and 3. Create IdP. The 'SP Metadata' step contains fields for Service Provider Metadata (with download links) and Service Provider URL (with a value of <https://samlsp.private.zscaler.com/auth/14123467699061827/sso>). A large callout box with the text 'Click Pause' points to the 'Pause' button in the bottom left corner of the modal. The background shows a table with columns for Name, Status, IdP Entity ID, Single Sign-On, and Actions.

Slide notes

Save the file, then to suspend this configuration wizard while you setup the IdP, click the **Pause** option, ...

Slide 20 - Slide 20

The screenshot shows the Adobe Captivate Administration interface. The left sidebar has a dark blue header with the Adobe logo and several navigation items: Dashboard, Diagnostics, Live Logs, Administration (which is selected and highlighted in blue), Search, Zscaler App, and a user icon. The main content area has a light gray header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with the following columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. There is one row in the table with the following data: Name is 'Azure', Status is 'In Progress' (indicated by a blue progress bar icon), IdP Entity ID is 'urn:oid:...', Single Sign-On is 'User', and Actions include a blue circular icon with a play arrow and a red circular icon with a minus sign. At the bottom of the main content area, there is a file download button labeled 'sp_metadata.xml' and a 'Show all' link.

Slide notes

...and the **IdP Configuration** will be saved in an incomplete state. You may restart the configuration of this IdP at any time.

Slide 21 - Configuring ZPA for Okta User SSO



Configuring ZPA for AAD User SSO

B. Add / Configure the ZPA Application in AAD

Slide notes

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

Slide 22 - Slide 22

The screenshot shows the Microsoft Azure portal's Home page. On the left, a dark sidebar lists various services like Home, Dashboard, All services, App Services, and Azure Active Directory. The Azure Active Directory icon is highlighted with a blue arrow pointing to it from a callout bubble containing the text "Click Azure Active Directory". The main content area displays the "Azure services" section with icons for Create a resource, Virtual machines, Azure Active Directory, App Services, Storage accounts, Virtual networks, Connections, All resources, and Azure AD Connect Health. Below this is the "Recent resources" table:

Name	Type	Last Viewed
syslog	Virtual machine	4 days ago
host-1	Virtual machine	2 months ago
patraining9ResourceGroup-vnet	Virtual network	6 months ago
host-1-ip	Public IP address	2 years ago
host-1920	Network interface	2 years ago

At the bottom, there are navigation links for Subscriptions, Resource groups, and All resources, along with a link to the URL https://portal.azure.com/#blade/Microsoft_AAD_JAM/ActiveDirectoryMenuBlade.

Slide notes

Login to your Azure tenant with suitable admin credentials, then from the **Home** page, click to access **Azure Active Directory**.

Slide 23 - Slide 23

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes a search bar, account information for 'admin@patraining9.saf...', and various icons. The main content area is titled 'patraining9 | Overview' under 'Azure Active Directory'. It features a 'Getting started' section with a message about enabling remote work, followed by an 'Overview' section for 'patraining9'. This section displays the tenant ID (553d1d85-7ec5-41b4-96ff-f972486e0e2c), role (Global administrator), and license (Azure AD Free). Below this is a 'Find' section with a dropdown set to 'Users' and a search bar. A callout box with the text 'Click Enterprise applications' points to the 'Enterprise applications' link in the 'Administrative units (Preview)' section of the left sidebar.

Slide notes

To add ZPA to AAD as a Service Provider, from the AAD home page click **Enterprise applications**, ...

Slide 24 - Slide 24

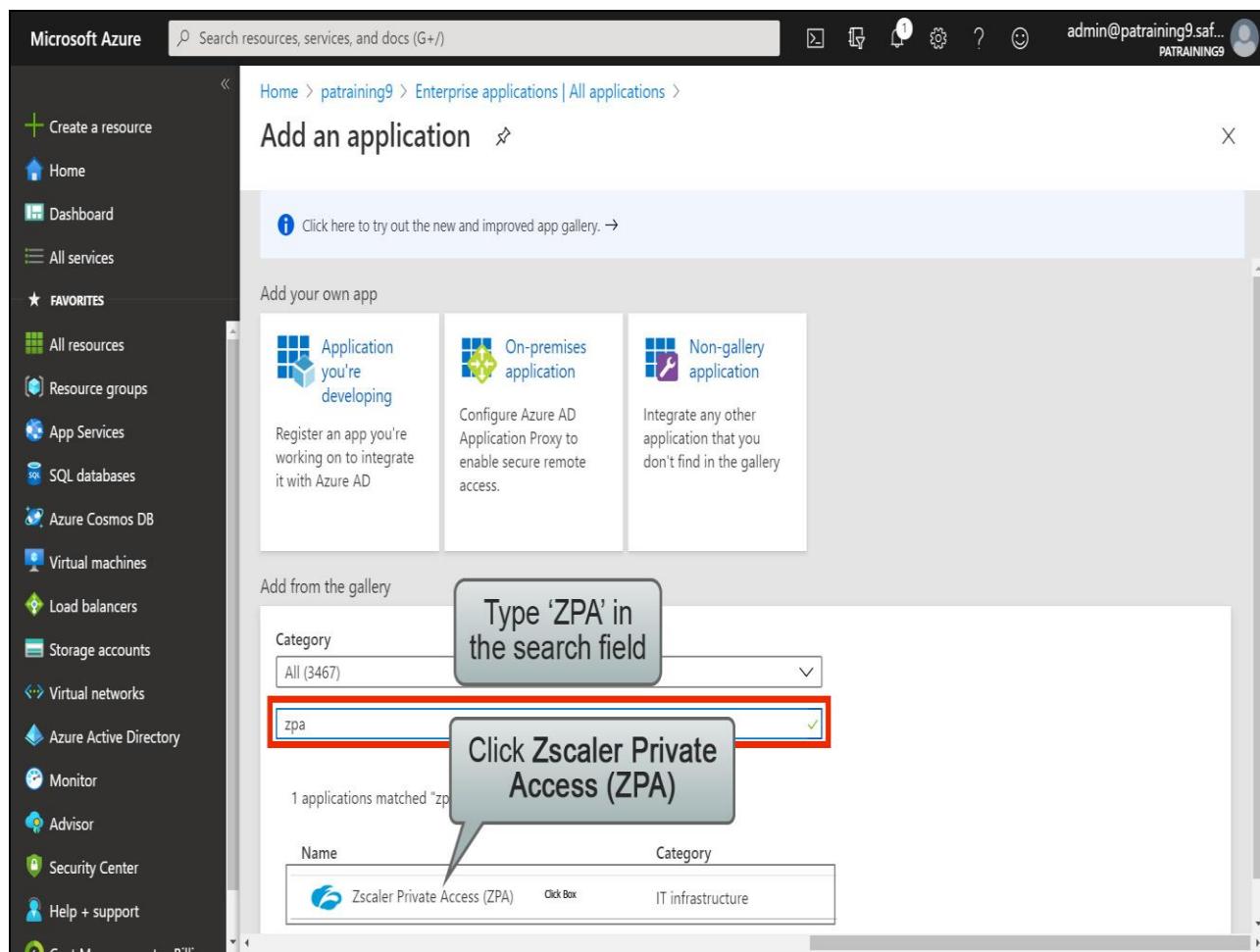
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', 'Security Center', and 'Help + support'. The main content area is titled 'Enterprise applications | All applications' under 'patraining9 - Azure Active Directory'. A callout bubble points to the '+ New application' button at the top left of the application list. The application list table has columns for Name, Homepage URL, Object ID, and Application ID. Several Microsoft services are listed, such as Azure DevOps, Office 365 Exchange Online, Office 365 Management, Office 365 SharePoint Online, Outlook Groups, and Skype for Business Online.

Name	Homepage URL	Object ID	Application ID
Azure DevOps	http://azure.com/devops	e815a67c-cf63-41b3-... 499b84ac-1321-427f...	
Office 365 Exchange Onlin...	http://office.microsoft.com/ou...	f08a4424-0605-416f-... 00000002-0000-0ff1...	
Office 365 Management		eaaf98eb-1d0f-46c9-... c5393580-f805-4401...	
Office 365 SharePoint Onlin...	http://office.microsoft.com/sh...	81dd92-770a-4db0-... 00000003-0000-0ff1...	
Outlook Groups		e4a486bb-685b-448c... 925eb0d0-da50-4604...	
Skype for Business Online		8f623252-efdf-43ac-8... 00000004-0000-0ff1...	

Slide notes

...and click New application.

Slide 25 - Slide 25



The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like App Services, SQL databases, and Storage accounts. The main area is titled 'Add an application'. It has two sections: 'Add your own app' and 'Add from the gallery'. In the 'Add from the gallery' section, a search bar contains the text 'zpa'. A callout bubble points to this search bar with the instruction 'Type 'ZPA' in the search field'. Another callout bubble points to the search result 'Zscaler Private Access (ZPA)' with the instruction 'Click Zscaler Private Access (ZPA)'. The result table shows one application entry:

Name	Category
Zscaler Private Access (ZPA)	Click Box IT infrastructure

Slide notes

Search for the ZPA application by typing 'ZPA' into the search field, then click on the **Zscaler Private Access (ZPA)** link, ...

Slide 26 - Slide 26

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Get started.

In the center, the 'Enterprise applications | All applications' section is displayed. A search bar at the top says 'Search resources, services, and docs (G+)'. Below it, a 'Home > patraining9 > Enterprise applications | All applications >' breadcrumb trail is shown. The main title is 'Add an application'.

The 'Add your own app' section contains three options:

- Application you're developing**: Register an app you're working on to integrate it with Azure AD.
- On-premises application**: Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**: Integrate any other application that you don't find in the gallery.

The 'Add from the gallery' section shows a search bar with 'Category' dropdown set to 'All (3467)' and a search term 'zpa'. The results table has columns 'Name' and 'Category'. One result is listed: **Zscaler Private Access (ZPA)** under the category **IT infrastructure**.

The right side of the screen displays detailed information about the 'Zscaler Private Access (ZPA)' application, including its publisher 'Zscaler Inc.' and a brief description: 'Zscaler Private Access delivers policy-based, secure access to private applications and assets without the cost, hassle, or security risks of a VPN.' A note states: 'Use Microsoft Azure AD to enable user access to Zscaler Private Access (ZPA).'. Another note says: 'Requires an existing Zscaler Private Access (ZPA) subscription.'

A callout bubble with the text 'Click Add' points to the blue 'Add' button at the bottom right of the application card.

Slide notes

...and click Add.

Slide 27 - Slide 27

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons such as Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cloud Shell. The main content area has a header 'Add an application' with a back arrow and a search bar containing 'Home > patraining9 > Enterprise applications | All applications >'. A tooltip says 'Click here to try out the new and improved app gallery. →'. Below this, there are three options: 'Application you're developing', 'On-premises application', and 'Non-gallery application'. Under 'Add from the gallery', the 'Category' dropdown is set to 'All (3467)'. A search input field contains 'zpa', which has a green checkmark next to it. Below the search results, a message says '1 applications matched "zpa".' A table lists the result: Name 'Zscaler Private Access (ZPA)' and Category 'IT infrastructure'. A status bar at the bottom right shows '6:33 PM'.

Slide notes

Slide 28 - Slide 28

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cloud Shell. The main content area shows a breadcrumb navigation path: Home > patraining9 > Enterprise applications | All applications > Add an application >. Below this, it says "Loading..." and "Enterprise Application". A success message box is displayed in the top right corner, stating "Adding application" with a checkmark icon, "Application Zscaler Private Access (ZPA) added successfully", and the time "6:33 PM".

Slide notes

Slide 29 - Slide 29

The screenshot shows the Microsoft Azure portal interface. On the left, there is a sidebar with various service icons: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cloud Shell.

The main content area displays the "Zscaler Private Access (ZPA) | Overview" page for an Enterprise Application. The navigation bar at the top shows the path: Home > patraining9 > Enterprise applications | All applications > Add an application >. A success message in the top right corner states: "Adding application" and "Application Zscaler Private Access (ZPA) added successfully" at 6:34 PM.

The "Properties" section contains the following details:

- Name: Zscaler Private Access (ZPA)
- Application ID: 572064ef-5768-40ed-8026...
- Object ID: e613c47e-2196-400a-baaf...

The "Getting Started" section provides two steps:

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials

Slide notes

Slide 30 - Slide 30

The screenshot shows the Microsoft Azure portal interface. On the left, there is a sidebar with various service icons: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support. The main content area has a header 'Home > patraining9 > Enterprise applications | All applications > Add an application > Zscaler Private Access (ZPA) | Overview'. The 'Properties' section displays the application's name (Zscaler Private Access (ZPA)), Application ID (572064ef-5768-40ed-8026...), and Object ID (e613c47e-2196-400a-baaf...). Below this, the 'Getting Started' section contains two numbered steps: 1. Assign users and groups (with a sub-note: Provide specific users and groups access to the application) and 2. Set up single sign on (with a sub-note: Enable users to sign into their application using their Azure AD credentials). A callout bubble points to the first step with the text 'Click Assign users and groups'.

Slide notes

Having added the application, the first thing you now need to do is assign it to users, so click the **Assign users and groups** box.

Slide 31 - Slide 31

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and Help + support. The main content area shows the 'Enterprise applications' section under 'patraining9'. A specific application, 'Zscaler Private Access (ZPA)', is selected. The 'Users and groups' tab is active. At the top of the main content, there's a toolbar with 'Add user', 'Edit', 'Remove', 'Update Credentials', 'Columns', and 'Got feedback?'. A callout box with the text 'Click Add user' points to the 'Add user' button. Below the toolbar, a note says 'The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent ...'. The main table displays columns for Display Name, Object Type, and Role assigned, with a message 'No application assignments found'.

Slide notes

Click Add user, ...

Slide 32 - Slide 32

Microsoft Azure Search resources, services, and docs (G+/-) ... > patraining9 > Enterprise applications | All applications > Add an application > Zscaler Private Access (ZPA) | Users and groups >

Add Assignment

patraining9

Groups are not available for assignment due to your Active Directory plan level.

Users

None Selected

Select Role

User

Click None Selected

Assign

Slide notes

...then click **Users None Selected**.

Slide 33 - Slide 33

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', 'Security Center', 'Help + support', and 'Cloud Shell'. The main area shows the path: 'patraining9 > Enterprise applications | All applications'. A modal window titled 'Add Assignment' is open, showing a message: 'Groups are not available for assignment due to your Active Directory settings.' Below this, a callout box contains the text: 'Click on the users who are to be assigned this application'. To the right, a list of users is displayed in a search-based interface:

User	Email
HT	hvac test hvac@patraining9.safemarch.com
PA	patraining9 admin@patraining9.safemarch.com
P6	pellis@zscaler.com 691ab608-615d-49ac-8f72-3a3f09a03a7d pellis@zscaler.com
ST	smadmin test smadmin@patraining9.safemarch.com

Below the list, there's a section for 'Selected items' which currently says 'No items selected'. At the bottom of the modal are two buttons: 'Assign' and 'Select'.

Slide notes

Click on the users who are to be allowed to use this application to select them, ...

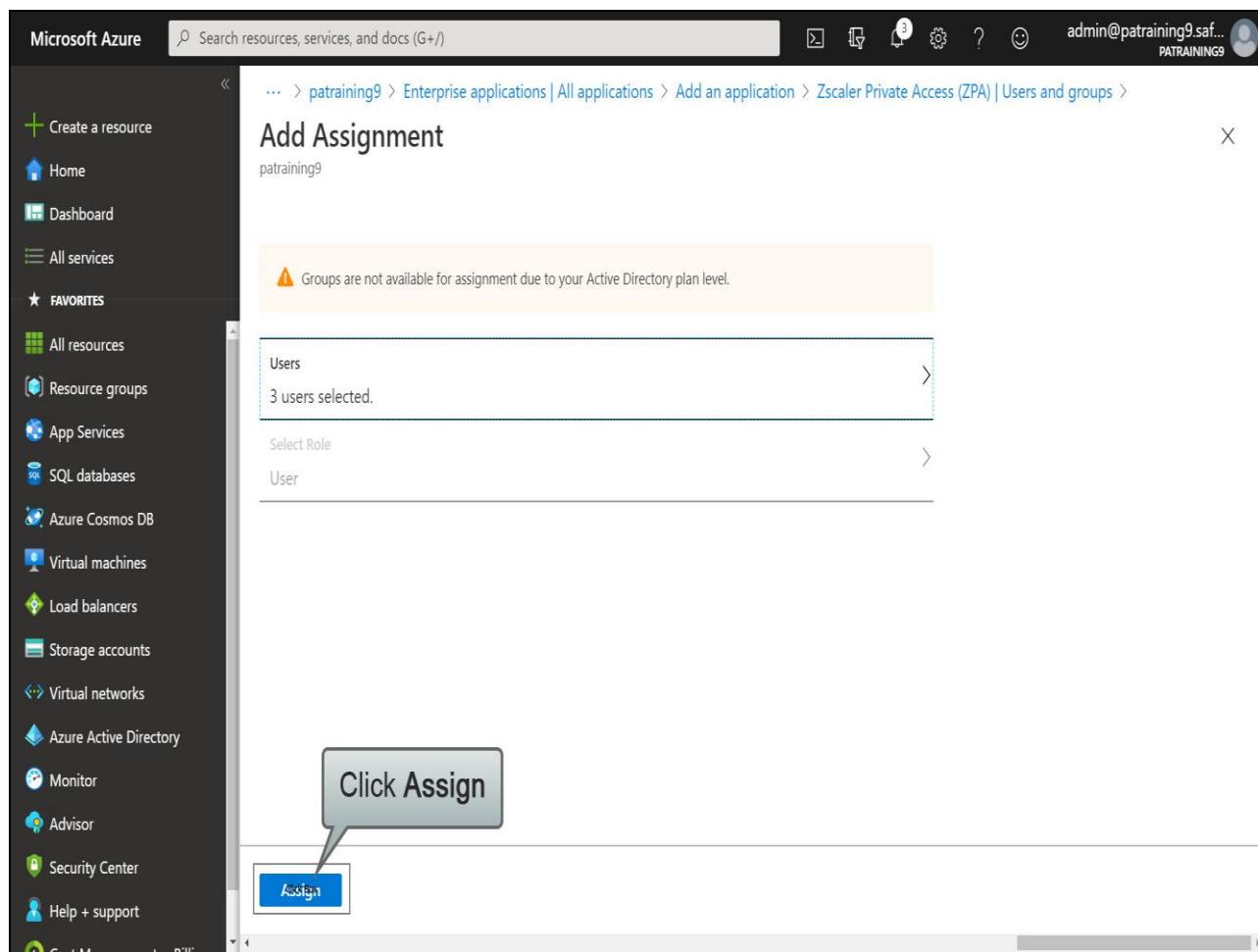
Slide 34 - Slide 34

The screenshot shows the Microsoft Azure portal interface. On the left is the navigation sidebar with various service icons. The main area displays the 'Enterprise applications | All applications' section under 'patraining9'. A sub-dialog titled 'Add Assignment' is open, showing a warning message: 'Groups are not available for assignment due to your Active Directory settings.' Below this, there are sections for 'Users' (listing 'None Selected') and 'Select Role' (set to 'User'). To the right, a larger 'Users' list is shown with three items: 'PA admin@patraining9.safemarch.com', 'P6 pellis@zscaler.com', and 'ST smadmin test'. The 'ST' entry is highlighted with a blue border and labeled 'Selected'. At the bottom of this list is 'student test student@patraining9.safemarch.com'. A callout bubble with the text 'Click Select' points to the 'Select' button at the bottom of the list. The 'Selected items' section on the right lists 'hvac test hvac@patraining9.safemarch.com', 'smadmin test smadmin@patraining9.safemarch.com', and 'student test student@patraining9.safemarch.com', each with a 'Remove' button.

Slide notes

...then click **Select**.

Slide 35 - Slide 35



Slide notes

To assign the selected user to the application, click **Assign**.

Slide 36 - Slide 36

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various service icons and links such as Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cloud Shell.

The main content area displays the 'Enterprise applications | All applications' section, specifically for the 'Zscaler Private Access (ZPA)' application. The title bar shows the path: Home > patraining9 > Enterprise applications | All applications > Add an application > Zscaler Private Access (ZPA) | Users and groups.

The 'Manage' section on the left includes options like Properties, Owners, Users and groups (which is selected), Single sign-on, Provisioning, Self-service, Security (Conditional Access, Permissions, Token encryption), and Activity.

The 'Users and groups' table lists three users:

Display Name	Object Type	Role assigned
HT hvac test	User	User
ST student test	User	User
ST smadmin test	User	User

A success message at the top right states: Application assignment succeeded 6:35 PM, 3 users & 0 groups have been assigned access.

Slide notes

Slide 37 - Slide 37

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation bar with various service icons like Create a resource, Home, Dashboard, etc. The main content area shows the 'Enterprise applications' blade for 'Zscaler Private Access (ZPA)'. In the center, there's a table listing users and their assigned roles. At the bottom of the left sidebar, there's a list of security-related links: Single sign-on, Provisioning, Self-service, Conditional Access, Permissions, and Token encryption. A callout box with the text 'Click Single sign-on' has an arrow pointing to the 'Single sign-on' link in the sidebar.

Display Name	Object Type	Role assigned
HT hvac test	User	User
ST student test	User	User
ST smadmin test	User	User

Slide notes

To configure SAML 2.0 functionality and to download the IdP metadata, click on the **Single sign-on** link, ...

Slide 38 - Slide 38

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and Help + support. The URL in the browser bar is <https://portal.azure.com/#>. The main content area shows the 'Zscaler Private Access (ZPA) | Single sign-on' configuration page under 'Enterprise Application'. The 'Single sign-on' option is highlighted in the left sidebar. In the center, there are three cards: 'Disabled' (disabled), 'SAML' (selected), and 'Linked'. A callout bubble with the text 'Click SAML' points to the 'SAML' card. The 'SAML' card includes a note: 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

Slide notes

...then click the SAML box.

Slide 39 - Slide 39

The screenshot shows the Microsoft Azure portal interface for managing enterprise applications. A specific application, "Zscaler Private Access (ZPA) | SAML-based Sign-on", is selected. The left sidebar lists various Azure services. The main pane shows the configuration steps for setting up Single Sign-On with SAML:

- 1 Basic SAML Configuration:** This section requires the following fields:
 - Identifier (Entity ID)
 - Reply URL (Assertion Consumer Service URL)
 - Sign on URL
 - Relay State
 - Logout Url
- 2 User Attributes & Claims:** This section maps user attributes to SAML claims:

User Attribute	SAML Claim
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups
- 3 Advanced Settings:** This section includes options for SSO mode, signing, and encryption.

A callout box highlights the "Upload metadata file" button with the text "Option to Upload (SP) metadata file". Another callout box points to the "Basic SAML Configuration" section with the text "Click to edit the Basic SAML Configuration".

Slide notes

Here you have the option to upload the SP metadata file that you saved from the ZPA Admin Portal. Or to configure the SAML settings manually, click to edit the **Basic SAML configuration**.

Slide 40 - Slide 40

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support. The 'Enterprise Application' section under 'All services' is selected. In the main content area, the title is 'Basic SAML Configuration' for the application 'Zscaler Private Access'. The 'Identifier (Entity ID)' field contains 'https://samlsp.private.zscaler.com/auth/metadata' and has a red border around it. A callout bubble labeled 'SP identifiers and URLs' points to this field. Below it, the 'Reply URL (Assertion Consumer Service URL)' field is empty. The 'Sign on URL' field contains 'Enter a sign on URL' and has a red border around it. A callout bubble labeled 'SP identifiers and URLs' also points to this field. The 'Patterns' for both fields are listed below them: 'Patterns: https://samlsp.private.zscaler.com/auth/metadata' for Identifier and 'Patterns: https://*.private.zscaler.com/auth/sso' for Reply URL.

Slide notes

This is where you need to paste those values from the ZPA Admin Portal, so...

Slide 41 - Slide 41

The screenshot shows the Zscaler Admin Portal's IdP Configuration page. On the left is a navigation 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 tabs for IdP Configuration, SAML Attributes, and Settings, with IdP Configuration selected. A table lists IdPs with columns for Name, Status, IdP Entity ID, Single Sign-On, and Actions. One row is highlighted with a blue border, showing 'Azure AD Box' in the Name column, 'Up' in Status, and 'User' in Single Sign-On. An 'Edit' icon (pencil) and a 'Delete' icon (trash can) are in the Actions column. A callout box with a grey background and a black border points to the 'Azure AD Box' name, containing the text 'Click the new IdP's Name'. In the bottom right corner of the main area, there is a 'Help' button with a question mark icon.

Slide notes

...go back to the ZPA Admin Portal and to expand details for it, click the name of the IdP you started to add.

Slide 42 - Slide 42

The screenshot shows the Adobe Captivate interface with the 'IdP Configuration' tab selected. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and other user-related options. The main content area displays an 'Azure' configuration entry. It includes fields for Name (Azure), Status (Up), IdP Entity ID (ZPA (SP) SAML Request), Single Sign-On (User), and Actions (Edit, Delete). Below this, there's a section for 'SERVICE PROVIDER SAML METADATA FOR USER SSO' with a 'Service Provider Metadata' link and a 'Download Metadata' button. To the right, there are fields for 'Service Provider Certificate' (with a 'Download Certificate' button) and 'Service Provider Entity ID' (which is highlighted with a green background and has a context menu open). The context menu for the Entity ID field includes options: Copy (Ctrl+C), Click Box, Go to https://samlsp.private.zscaler.com/auth/metadata/... (Ctrl+G), Print... (Ctrl+P), and Inspect (Ctrl+Shift+I). A callout bubble points to the 'Copy' option with the instruction: 'Select the value for the Service Provider Entity ID and click Copy.'

Slide notes

Select the value for the **Service Provider Entity ID** and click **Copy**.

Slide 43 - Slide 43

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services like Home, Dashboard, All services, and Resource groups. The main content area is titled "Basic SAML Configuration" for the "Zscaler Private" Enterprise Application. The "Identifier (Entity ID)" field is highlighted with a red box and contains the value "https://samlsp.private.zscaler.com/auth/metadata/144123467699061827". A callout bubble points to this field with the text "Paste in the value for the Identifier (Entity ID)". Other fields shown include "Reply URL (Assertion Consumer Service URL)", "Sign on URL", and "Patterns" for each.

Slide notes

In the Azure Admin Portal, paste that value into the field labelled **Identifier (Entity ID)**.

Slide 44 - Slide 44

The screenshot shows the Zscaler Admin Portal's IdP Configuration screen. On the left sidebar, there are various navigation options: Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help. The main content area is titled "IdP Configuration" and contains a table with one row for "Azure". The table columns are "Name", "Status", "IdP Entity ID", "Single Sign-On", and "Actions". Under "Actions", there are icons for "Edit" and "Delete". Below the table, there is a section titled "SERVICE PROVIDER SAML METADATA FOR USER SSO" which includes "Service Provider Metadata" (with a "Download Metadata" button) and "Service Provider Entity ID" (with a "Download Certificate" button). The "Service Provider URL" field contains the value "https://samlsp.private.zscaler.com/auth/144123467699061827". A context menu is open over this field, with the "Copy" option highlighted. A callout box with a thick border and a semi-transparent background points to the "Copy" option, containing the text: "Select the value for the Service Provider URL and click Copy".

Slide notes

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

Slide 45 - Slide 45

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and a link to the Microsoft Learn documentation.

The main content area is titled "Basic SAML Configuration" for the "Zscaler Private" Enterprise Application. It displays configuration settings:

- Identifier (Entity ID) ***: https://samlsp.private.zscaler.com/auth/metadata
- Reply URL (Assertion Consumer Service URL) ***: https://samlsp.private.zscaler.com/auth/144123467699061827/sso
- Sign on URL ***: (empty field)

A callout bubble with the text "Paste in the value for the Reply URL" points to the Reply URL field, which is highlighted with a red border.

Slide notes

Back in the Azure Admin Portal, paste that value into the field labelled **Reply URL (Assertion Consumer Service URL)**, and...

Slide 46 - Slide 46

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support. The main content area is titled "Basic SAML Configuration" for the "Zscaler Private" Enterprise Application. The "Single sign-on" section is highlighted with a red box. Inside this section, the "Sign on URL" field contains the value "https://samlsp.private.zscaler.com/auth/144123467699061827/sso". A callout bubble points to this field with the text "Paste in the value for the Sign on URL". Other fields in this section include "Patterns: https://*.private.zscaler.com/auth/sso" and "Relay State" (with an input field "Enter a relay state"). Below this, there are sections for "Logout Url" (with an input field "Enter a logout url") and "Default" (with a dropdown menu). At the top right, there are save and cancel buttons.

Slide notes

...into the field labelled **Sign on URL**.

Slide 47 - Slide 47

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support. The main content area is titled "Basic SAML Configuration" for the "Zscaler Private" Enterprise Application. It shows the "Reply URL" field set to "https://samlsp.private.zscaler.com/auth/144123467699061827/sso". A large callout box highlights the "Save" button. Other fields include "Sign on URL" (set to "https://samlsp.private.zscaler.com/auth/144123467699061827/sso"), "Relay State" (empty), and "Logout Url" (empty). The "Manage" sidebar on the left includes sections for Properties, Owners, Users and groups, Single sign-on, Provisioning, Self-service, Conditional Access, Permissions, Token encryption, and Activity.

Slide notes

Then click **Save**, ...

Slide 48 - Slide 48

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cloud Shell.

The main content area is titled "Basic SAML Configuration" for the "Zscaler Private" Enterprise Application. The "Single sign-on" section is currently active. It contains fields for "Reply URL (Assertion Consumer Service URL)" (https://samlsp.private.zscaler.com/auth/144123467699061827/sso), "Sign on URL" (https://samlsp.private.zscaler.com/auth/144123467699061827/sso), and "Logout Url". A tooltip indicates that the default reply URL will be the destination in the SAML response for IDP-initiated SSO. Below these fields are "Patterns" entries: https://*.private.zscaler.com/auth/sso for Reply URL and https://samlsp.private.zscaler.com/auth/login?domain=EXAMPLE for Sign on URL.

A modal window at the top right shows a progress bar with the message "Saving single sign-on configuration" and a timestamp of 6:39 PM.

Slide notes

Slide 49 - Slide 49

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support. The main content area is titled "Basic SAML Configuration" for the "Zscaler Private" Enterprise Application. It includes sections for Reply URL (Assertion Consumer Service URL), Sign on URL, Relay State, and Logout Url, each with input fields and validation messages. A success message at the top right indicates "Single sign-on configuration was saved successfully".

Slide notes

Slide 50 - Slide 50

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support. The main content area is titled "Basic SAML Configuration" for an "Enterprise Application" named "Zscaler Private". The configuration includes fields for Reply URL (Assertion Consumer Service URL), Sign on URL, Relay State, and Logout Url. A "Save" button is visible. A red "X" icon in the top right corner of the dialog has a gray callout box with the text "Click to Close".

Slide notes

...then click to close the **Basic SAML Configuration** dialog.

Slide 51 - Slide 51

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and Help + support. The main area is titled 'Zscaler Private Access (ZPA) | SAML-based Sign-on' under 'Enterprise Application'. It has tabs for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Users and groups, Single sign-on, Provisioning, Self-service), Security (Conditional Access, Permissions, Token encryption), and Activity. In the 'Manage' section, 'Single sign-on' is selected. A callout box with the text 'Click No, I'll test later' points to the 'No, I'll test later' button in a modal dialog. The dialog also contains fields for Identifier (Entity ID), Reply URL (Assertion URL), Sign on URL, Relay State, and Logout Url, each with their respective URLs listed. Below the 'Manage' section, there's a 'User Attributes & Claims' table with columns for Attribute and Claim. The table lists: givenname (user.givenname), surname (user.surname), emailaddress (user.mail), name (user.userprincipalname), Unique User Identifier (user.userprincipalname), and Group (user.groups). A blue number '2' is located near the bottom left of the 'User Attributes & Claims' section.

Slide notes

You will be prompted to **Test single sign-on with Zscaler Private Access (ZPA)**, however we will test this later from the ZPA Admin Portal, so click **No, I'll test later**.

Slide 52 - Slide 52

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and Help + support. The URL in the address bar is <https://portal.azure.com/#>.

The main content area displays the "Zscaler Private Access (ZPA) | SAML-based Sign-on" Enterprise Application page. The breadcrumb navigation shows: ... > Enterprise applications | All applications > Add an application > Zscaler Private Access (ZPA) | Single sign-on >. The top right corner shows the user's email (admin@patraining9.saf...) and a PATRINING9 profile icon.

The left sidebar under the "Manage" section lists: Properties, Owners, Users and groups (which is selected), Single sign-on, Provisioning, Self-service, Conditional Access, Permissions, Token encryption, and Activity.

The main content area has tabs at the top: Overview, Deployment Plan, Diagnose and solve problems, Upload metadata file, Change single sign-on mode, Test this application, and Got feedback?.

A callout box points to the "Single sign-on" tab in the sidebar with the text: "Click to edit the User Attributes & Claims".

The "Basic SAML Configuration" section contains the following details:

Identifier (Entity ID)	https://samlsp.private.zscaler.com/auth/metadata
Reply URL (Assertion Consumer Service URL)	https://samlsp.private.zscaler.com/auth/14412346 7699061827/sso
Sign on URL	https://samlsp.private.zscaler.com/auth/14412346 7699061827/sso
Relay State	Optional
Logout Url	Optional

The "User Attributes & Claims" section lists the following mappings:

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.usn
Unique User Identifier	user.usrid
Group	user.grp

Slide notes

To edit, add, or remove the attributes sent in the SAML Assertion on a successful user authentication, click to edit **User Attributes & Claims**.

Slide 53 - Slide 53

Microsoft Azure Search resources, services, and docs (G+) admin@patraining9.saf... PATRINING

User Attributes & Claims

Add new claim Add a group claim Columns

Required claim Claim name Value

Unique User Identifier (Name ID) user.userprincipalname [nameid-format:emailAddress]

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Slide notes

Review the value set for the **Unique User Identifier (Name ID)**, Zscaler recommends you use the `user.userprincipalname [nameid-format:emailAddress]` value for this.

Also, review the list of **Additional claims**, to be sure they meet your user identity needs; you can match against any of these attributes in a ZPA Access Policy. If you need to add a claim, click **Add new claim**.

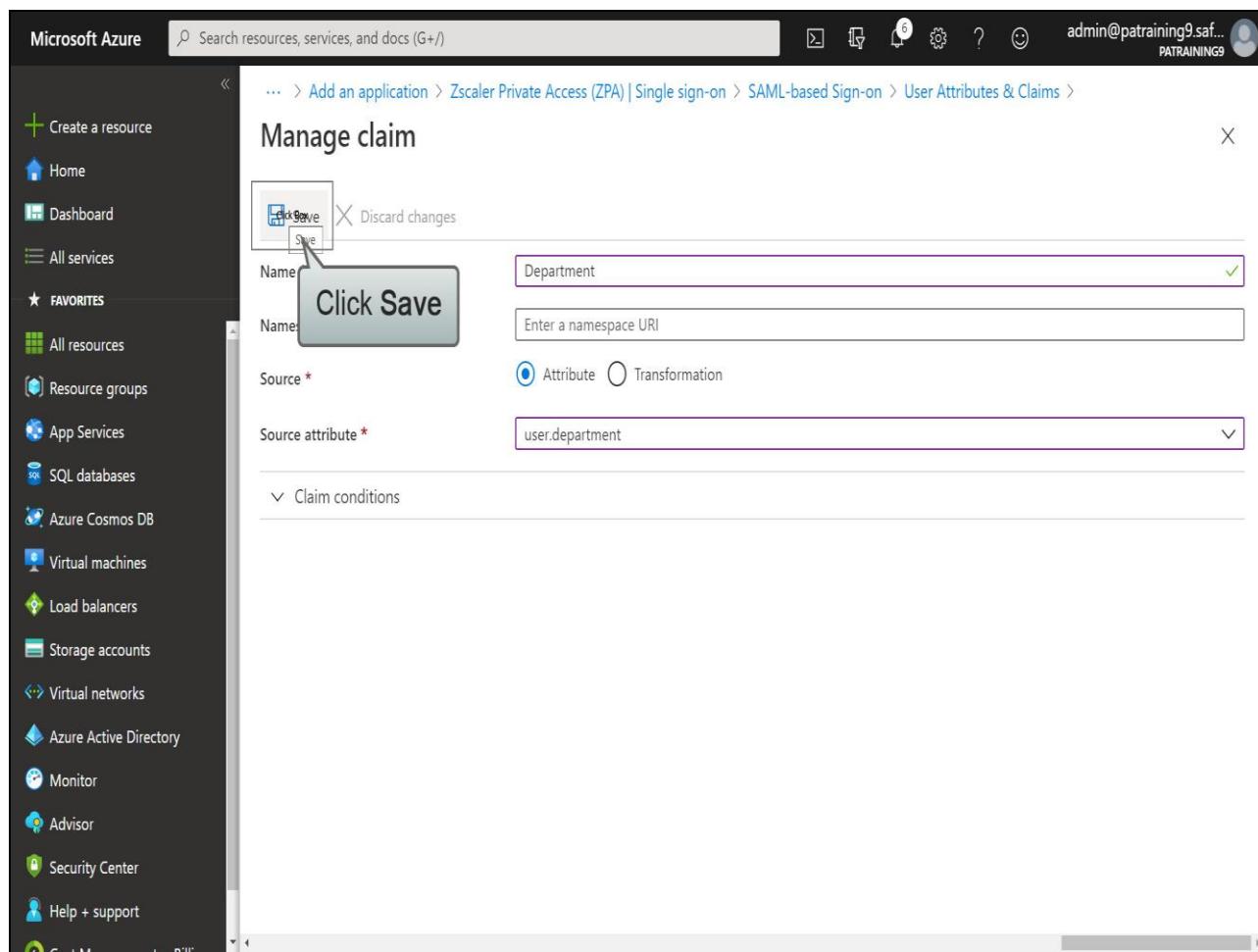
Slide 54 - Slide 54

The screenshot shows the 'Manage claim' dialog box in the Microsoft Azure portal. The 'Name' field is highlighted with a red border and contains the text 'Department'. A callout bubble with the text 'Give the new claim a Name' points to this field. The 'Source attribute' dropdown is open, showing various user attributes like 'user.department', 'user.displayname', etc. A callout bubble with the text 'Click user.department' points to the 'user.department' option in the list.

Slide notes

Give the new claim a **Name**, then from the **Source attribute** list click to select the applicable value, in this case **user.department**.

Slide 55 - Slide 55



Slide notes

Then click **Save**, ...

Slide 56 - Slide 56

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with various services like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and Cloud Shell.

The main content area is titled "User Attributes & Claims". It shows two sections: "Required claim" and "Additional claims".

Required claim:

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...]

Additional claims:

Claim name	Value
user.groups [SecurityGroup]	***
user.department	***
user.mail	***
user.givenname	***
user.userprincipalname	***
user.surname	***

A success message at the top right says "Successfully saved SSO SAML user claims" with a timestamp of "6:41 PM".

Slide notes

Slide 57 - Slide 57

The screenshot shows the Microsoft Azure portal interface. On the left is a dark sidebar with various service icons and links. The main area is titled "User Attributes & Claims". It has two sections: "Required claim" and "Additional claims", each with a table of claim names and their values. A large gray callout box with the text "Click to Close" and a red "X" button is overlaid on the top right of the dialog.

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...]

Claim name	Value
user.groups [SecurityGroup]	***
user.department	***
user.mail	***
user.givenname	***
user.userprincipalname	***
user.surname	***

Slide notes

...then click to close the **User Attributes & Claims** dialog.

Slide 58 - Slide 58

The screenshot shows the Microsoft Azure portal interface for managing enterprise applications. The left sidebar lists various services like App Services, SQL databases, and Azure Active Directory. The main content area is titled "Zscaler Private Access (ZPA) | SAML-based Sign-on" under "Enterprise Application". The "Single sign-on" section is selected in the navigation menu. The page displays two main sections: "User Attributes & Claims" and "SAML Signing Certificate".

User Attributes & Claims

Attribute	Claim
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Department	user.department
Unique User Identifier	user.userprincipalname
Group	user.groups

SAML Signing Certificate

Setting	Value
Status	Active
Thumbprint	2CD9461D0B479357EA2A77EA33C3E5A0
Expiration	6/9/2023, 6:35:27 PM
Notification Email	admin@patraining9.safemarch.com
App Federation Metadata Url	https://login.microsoftonline.com/553d1...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

A callout box with the text "Scroll down..." points to the bottom of the certificate table.

Slide notes

Scroll down, ...

Slide 59 - Slide 59

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Help + support, and a direct link to https://portal.azure.com/. The main content area displays the 'Zscaler Private Access (ZPA) | SAML-based Sign-on' configuration page for an Enterprise Application. The 'Manage' section is open, showing options like Properties, Owners, Users and groups, Single sign-on (which is selected), Provisioning, Self-service, Security, Conditional Access, Permissions, Token encryption, and Activity. Step 3 is highlighted over the 'Download' link for the Federation Metadata XML under the 'SAML Signing Certificate' section. Step 4 is highlighted over a callout box containing the text 'Click to Download the Federation Metadata XML'. The URL for the Federation Metadata XML is https://login.microsoftonline.com/553d1... .

Slide notes

To download the **Federation Metadata XML** for this IdP, click the **Download** link, ...

Slide 60 - Slide 60

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar includes options like Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | SAML-based Sign-on" under "Enterprise Application". The "Single sign-on" section is selected in the "Manage" sidebar. A callout box indicates step 3: "Download Federation Metadata Xml" has been completed successfully. Step 4: "Highly recommended: Install the Azure AD browser extension" is shown with a "Install the extension" button.

Slide notes

...save the file, ...

Slide 61 - Slide 61

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | SAML-based Sign-on" under "Enterprise Application". The navigation bar at the top includes "Search resources, services, and docs (G+)", a user profile for "admin@patraining9.saf...", and a "PATRINING" group icon. Below the title, there are tabs for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Users and groups, Single sign-on, Provisioning, Self-service), and Security (Conditional Access, Permissions, Token encryption). The "Single sign-on" tab is currently selected. The main content area has two sections: "Basic SAML Configuration" (Identifier, Reply URL, Sign on URL, Relay State, Logout Url) and "User Attributes & Claims" (givenname, surname, emailaddress, name, Department, Unique User Identifier). A callout bubble with the text "Click to Close" points to the "Close" button in the top right corner of the configuration pane.

Slide notes

...then click to close the **Zscaler Private Access (ZPA) | SAML-based Sign-on** dialog.

Slide 62 - Slide 62

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Enterprise applications | All applications" under "patraining9 - Azure Active Directory". It has sections for Overview, Manage, Security, and Activity. Under Manage, "All applications" is selected. The table lists several applications:

Name	Homepage URL	Object ID	Application ID
Azure DevOps	http://azure.com/devops	e815a67c-cf63-41b3-...	499b84ac-1321-427f...
Office 365 Exchange Or...	http://office.microsoft.com/ou...	f08a4424-0605-416f...	00000002-0000-0ff1...
Office 365 Managemen...		eaaf98eb-1d0f-46c9...	c5393580-f805-4401...
Office 365 SharePoint C...	http://office.microsoft.com/sh...	81ddd92-770a-4db0...	00000003-0000-0ff1...
Outlook Groups		e4a486bb-685b-448c...	925eb0d0-da50-4604...
Skype for Business Onli...		8f623252-efdf-43ac-8...	00000004-0000-0ff1...
Zscaler Private Access (https://www.zscaler.com/prod...	e613c47e-2196-400a...	572064ef-5768-40ed...

A callout box with the text "Click on the Admin Username" points to the user icon in the top right corner of the browser window.

Slide notes

If you plan to test the AAD configuration from this machine you need to log out of Azure, so click on your username at top right, ...

Slide 63 - Slide 63

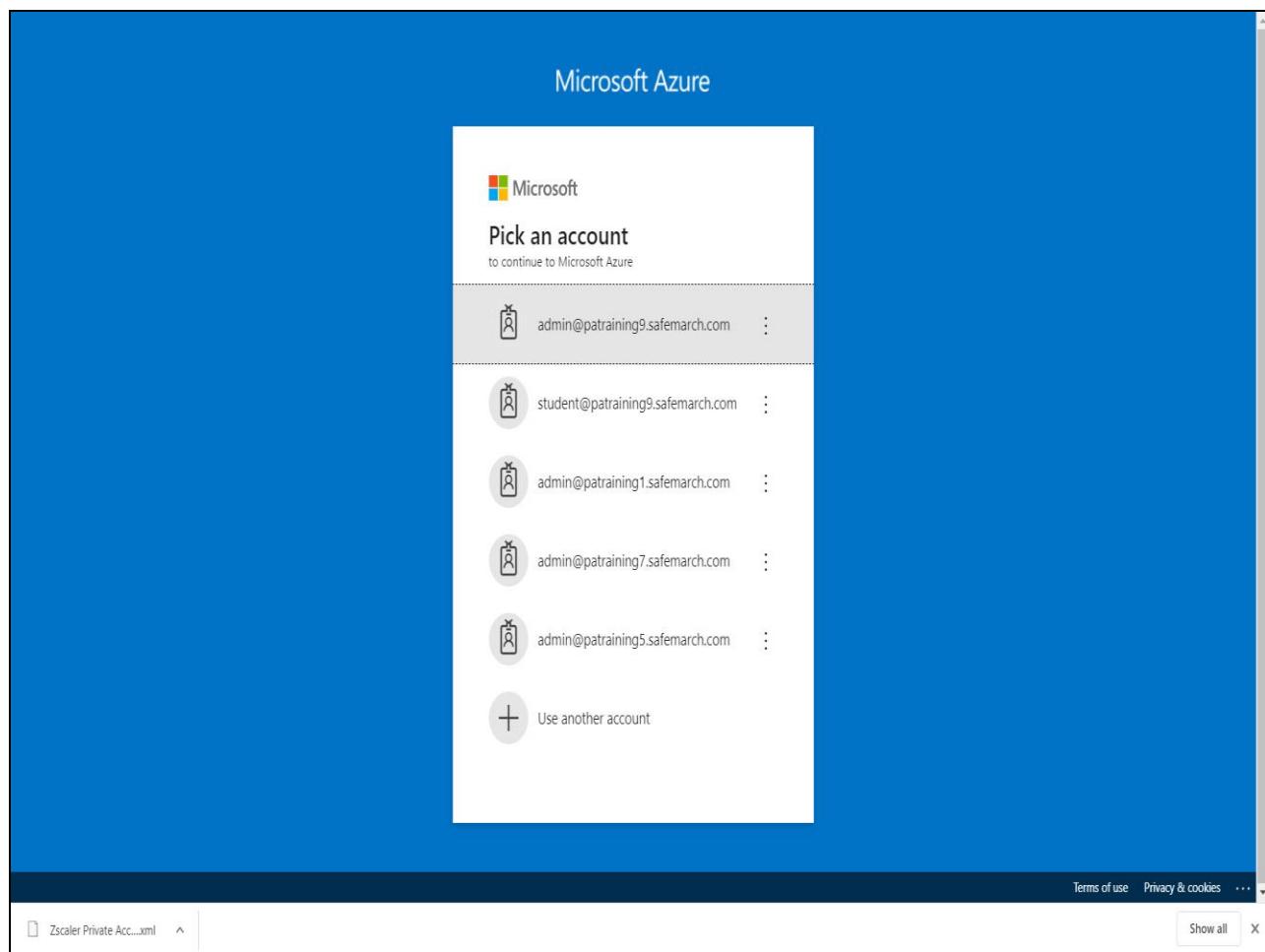
The screenshot shows the Microsoft Azure portal's Enterprise applications page. The left sidebar lists various services like Create a resource, Home, Dashboard, etc. The main area shows a list of applications under the 'All applications' tab. A large callout box highlights the 'Sign out' button in the top right corner of the page.

Name	Homepage URL
Azure DevOps	http://azure.com/devops
Office 365 Exchange Online	http://office.microsoft.com/ou...
Office 365 Management	
Office 365 SharePoint Online	http://office.microsoft.com/sh...
Outlook Groups	
Skype for Business Online	
Zscaler Private Access	https://www.zscaler.com/prod... e613c47e-2196-400a-8f00-0ff1...

Slide notes

...and click Sign out.

Slide 64 - Slide 64



Slide notes

Slide 65 - Configuring ZPA for Okta User SSO



Configuring ZPA for AAD User SSO

C. Complete the IdP Setup in ZPA

Slide notes

Next, we will look at how to complete the configuration of AAD as an IdP in the ZPA configuration.

Slide 66 - Slide 66

The screenshot shows the Zscaler Admin Portal's IdP Configuration screen. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main content area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with one row for 'Azure'. The table columns are: Name, Status, IdP Entity ID, Single Sign-On, and Actions. The 'Actions' column for Azure contains a 'Click Box' icon and a red 'X' icon. A large, semi-transparent gray button with the text 'Click Resume' is overlaid on the 'Actions' column. To the right of the table, there are sections for 'Single Sign-On URL' (ZPA (SP) SAML Request, Signed), 'Authentication Domains' (patraining9.safemarch.com), 'SERVICE PROVIDER SAML METADATA FOR USER SSO' (Service Provider Metadata, Download Metadata), 'Service Provider Entity ID' (https://samlsp.private.zscaler.com/auth/144123467699061827/sso), 'SCIM' (disabled), and 'SCIM Sync' (disabled). At the bottom of the main content area is a footer with a 'Help' button and links for 'Show all' and 'X'.

Slide notes

Back in the ZPA Admin Portal, click to **Resume** the configuration of the IdP that you paused earlier.

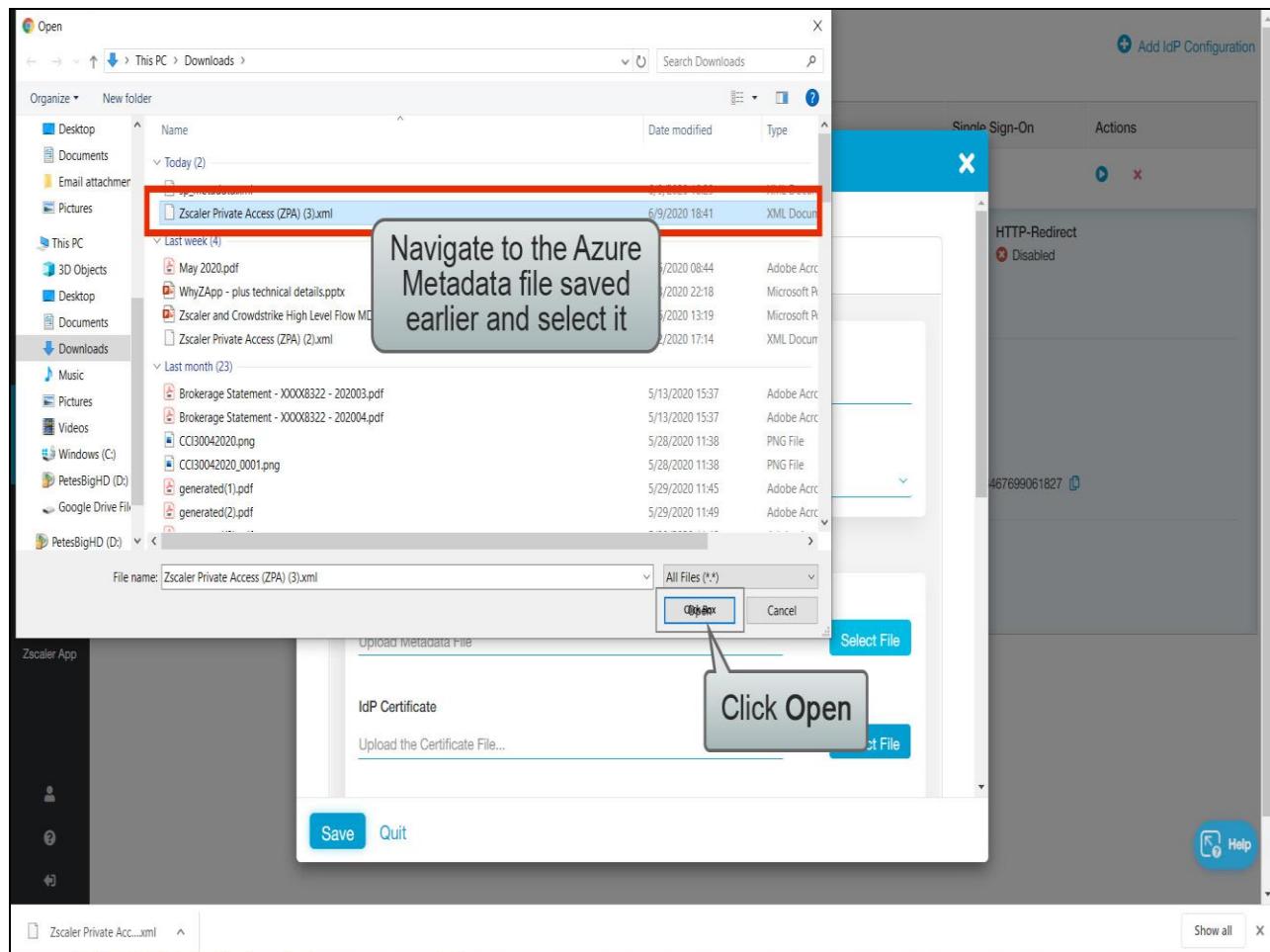
Slide 67 - Slide 67

The screenshot shows the Adobe Captivate interface for managing SAML configurations. A modal window titled "Add IdP Configuration" is open, specifically on the "IdP Information" tab. The "Name" field is set to "Azure". Under "Authentication Domains", the value "patraining9.safemarch.com" is listed. In the "SP Metadata" section, there is a "Select File" button next to the "IdP Metadata File" input field, which is highlighted with a callout bubble containing the text "Click Select File". The "Create IdP" tab is also visible. The background shows a list of existing IdP configurations, including "HTTP-Redirect" which is currently disabled. The left sidebar provides navigation links for various system components like Dashboard, Diagnostics, and Administration.

Slide notes

We are going to complete the configuration of this IdP by importing that metadata file, so by the **IdP Metadata File** field click **Select File**, ...

Slide 68 - Slide 68



Slide notes

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

Slide 69 - Slide 69

Verify the Authentication Domains

Scroll down...

Slide notes

Verify that the **Authentication Domains** configuration is correct, then scroll down.

Slide 70 - Slide 70

Verify that the IdP Certificate has been imported

Scroll down...

Slide notes

Verify that the **IdP Certificate** has also been imported. If not, it is available as a separate file from the Azure Admin Portal.
Scroll down, ...

Slide 71 - Slide 71

The screenshot shows the Zscaler Private Access (ZPA) interface for managing IdP configurations. On the left, there's a sidebar with various navigation options: Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area is titled 'IdP Configuration' and shows a list of existing configurations, with one entry for 'Azure' expanded. A modal window titled 'Add IdP Configuration' is open, prompting for 'Single Sign-On URL' (with a long URL pasted in) and 'IdP Entity ID' (with a URL pasted in). Below these fields are several configuration options:

- Status:** Buttons for 'Enabled' (checked) and 'Disabled'.
- ZPA (SP) SAML Request:** Buttons for 'Signed' (checked) and 'Unsigned'.
- HTTP-Redirect:** Buttons for 'Enabled' (checked) and 'Disabled'.
- SCIM:** Buttons for 'Enabled' and 'Disabled' (checked).

A large red box highlights the 'Status' and 'ZPA (SP) SAML Request' sections. A callout bubble with the text 'Configure other IdP settings as necessary' is positioned over the highlighted area. At the bottom of the modal are 'Save' and 'Quit' buttons, with 'Save' being highlighted by a callout labeled 'Click Save'. The background shows a list of other IdP configurations, including 'HTTP-Redirect' which is currently 'Disabled'.

Slide notes

...adjust other IdP configuration settings as required and click **Save**.

Slide 72 - Slide 72

The screenshot shows the Adobe Captivate interface with the 'Administration' menu selected. On the left, there's a sidebar with various icons: Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and other user-related icons. The main content area is titled 'IdP Configuration' and contains a table with one row. The table columns are 'Name', 'Status', 'IdP Entity ID', 'Single Sign-On', and 'Actions'. The single row shows 'Azure' as the name, a green checkmark status, the URL 'https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/' as the IdP Entity ID, 'User' as the Single Sign-On method, and edit and delete icons in the Actions column. A green notification bar at the bottom right says 'IdP configuration saved' with a 'Help' link. At the bottom left, there's a file tab for 'Zscaler Private Acc....xml'.

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

Slide notes

Slide 73 - Slide 73

The screenshot shows the Zscaler Admin UI interface. On the left is a vertical 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 'IdP Configuration' (which is selected, indicated by a blue underline), 'SAML Attributes', and 'Settings'. Below the header is a table with the following data:

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

At the bottom of the main content area, there is a file tab labeled 'Zscaler Private Acc....xml' with a dropdown arrow, and buttons for 'Show all' and 'X'. In the bottom right corner of the main content area, there is a 'Help' button with a question mark icon.

Slide notes

Slide 74 - Configuring ZPA for Okta User SSO



Configuring ZPA for AAD User SSO

D. Test the Configuration and Import Attributes

Slide notes

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

Slide 75 - Slide 75

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left sidebar, there are icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, Zscaler App, and User Management. The main content area is titled 'IdP Configuration' and contains a table with one row. The row has columns for Name (containing 'AzureBox'), Status (green checkmark), IdP Entity ID (https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/), Single Sign-On (User), and Actions (edit and delete icons). A callout box points to the 'AzureBox' name with the text 'Click to expand details for the IdP'.

Name	Status	IdP Entity ID	Single Sign-On	Actions
AzureBox	✓	https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/	User	

Slide notes

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

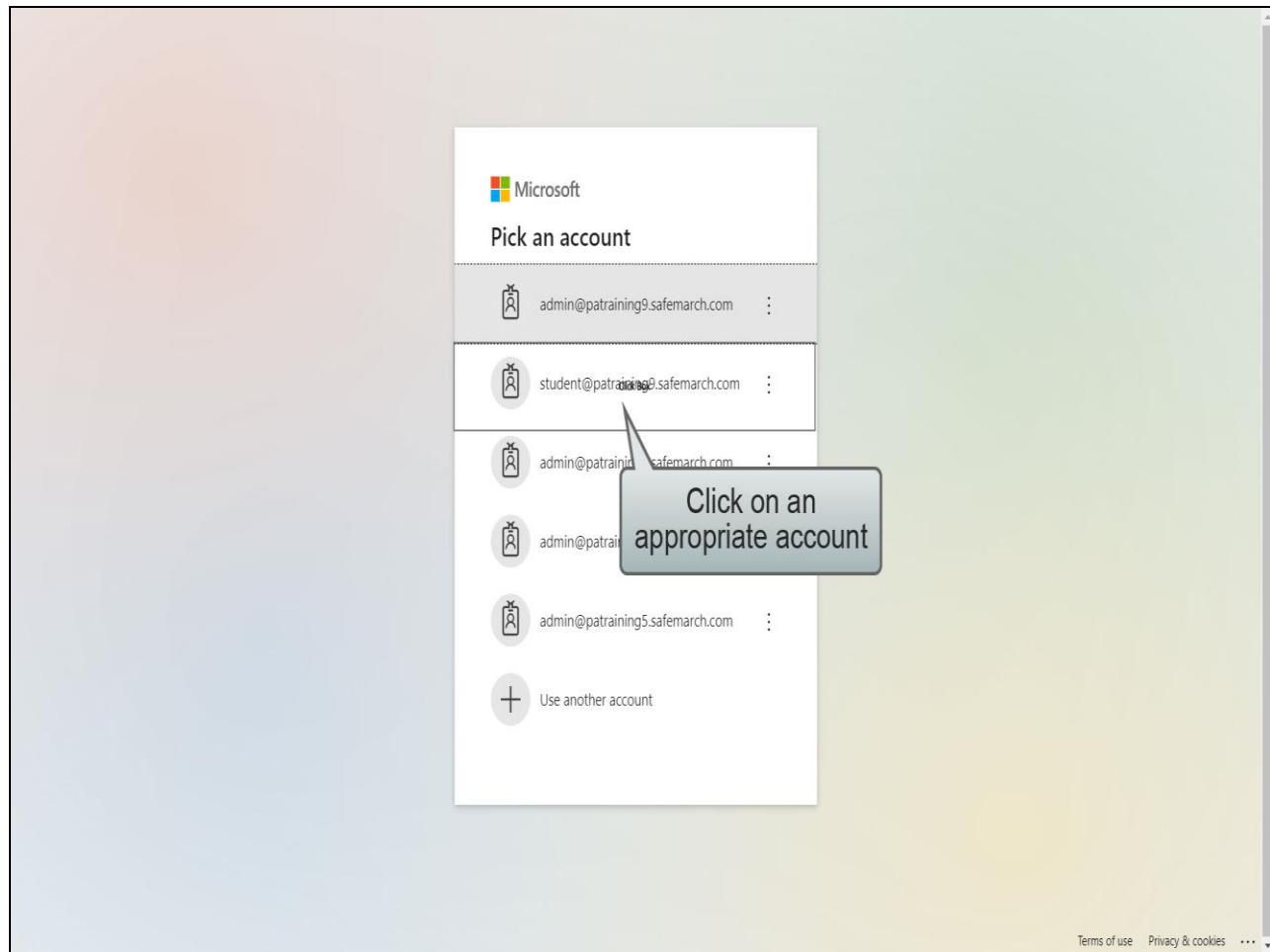
Slide 76 - Slide 76

The screenshot shows the Adobe Captivate interface for managing Identity Providers (IdPs). On the left, a vertical sidebar contains icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main content area is titled "IdP Configuration" and shows a table of configured IdPs. One row is selected for "Azure". The table columns include Name, Status, IdP Entity ID, Single Sign-On, and Actions. Below the table, there are sections for "Single Sign-On URL", "Authentication Domains", "Import SAML Attributes", and "SERVICE PROVIDER SAML METADATA FOR USER SSO". A callout box with the text "Click to Import SAML Attributes" points to the "Import SAML Attributes" section. At the bottom right of the main area is a "Help" button.

Slide notes

...then to import the **SAML Attributes** available from this IdP, click the **Import** link.

Slide 77 - Slide 77

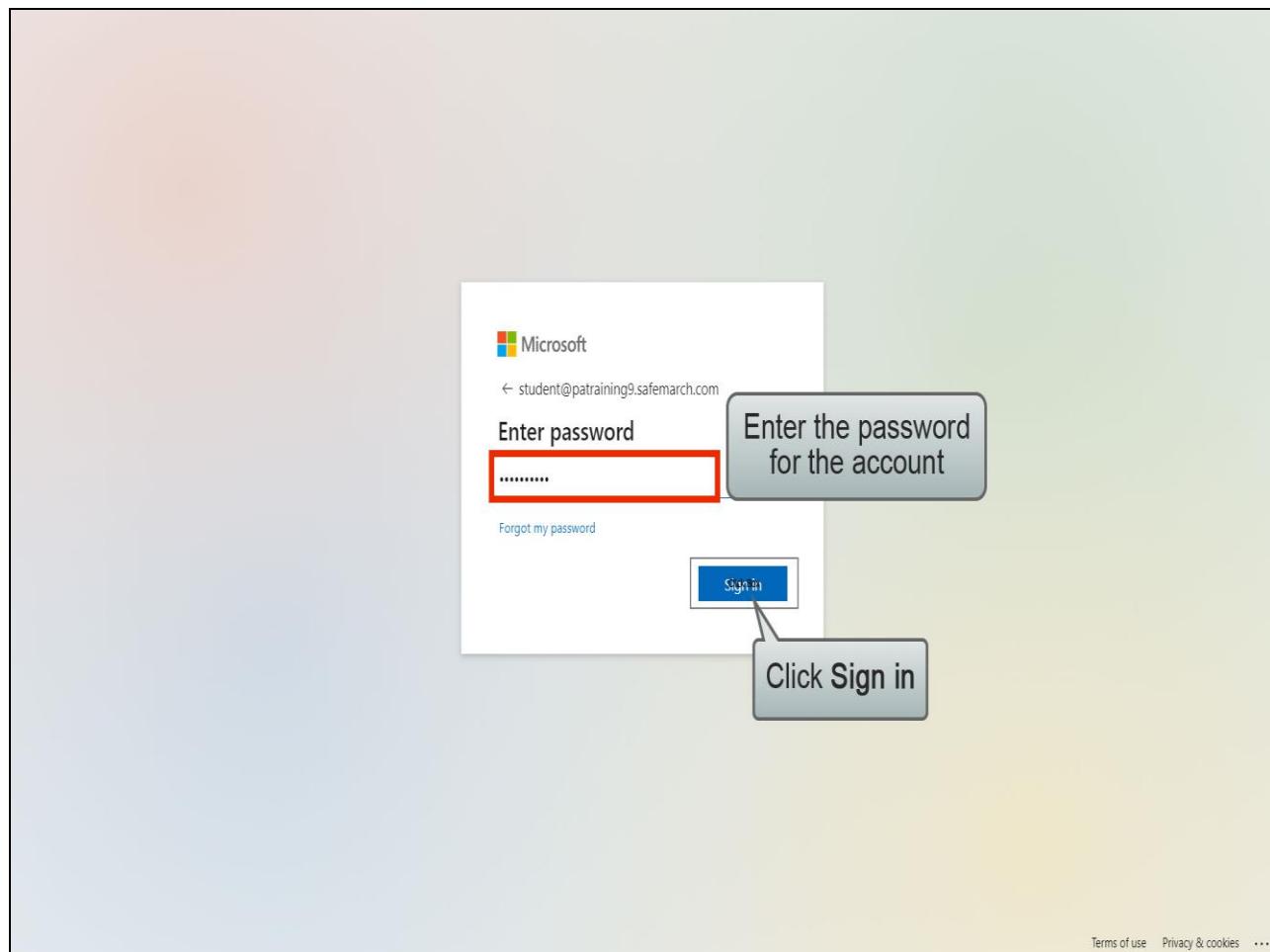


Slide notes

You need to login to Azure as a one of the end user's that were assigned the ZPA application in the **Enterprise Application** configuration. At the Azure login page, either use the **Use another account** option, or click on a user available in the list,

...

Slide 78 - Slide 78



Slide notes

...provide the user's password and click **Sign In**.

Slide 79 - Slide 79

The screenshot shows the 'Import SAML Attributes' dialog box. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and user profile. The main area has a blue header 'Import SAML Attributes' with a close button 'x'. It contains two columns: 'Name' and 'SAML Attribute Name'. The 'Name' column is highlighted with a red box and a callout bubble that says 'Edit the Attribute Names as necessary'. The 'SAML Attribute Name' column lists various URLs. At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' button with a question mark icon.

Name	SAML Attribute Name
TenantID_Azure	http://schemas.microsoft.com/identity/claims/tenantid
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier
http__schemas_microsoft_com_identity_claims_displayname_Azure	http://schemas.microsoft.com/identity/claims/displayname
http__schemas_microsoft_com_ws_2008_06_identity_claims_groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
http__schemas_microsoft_com_identity_claims_identityprovider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider
http__schemas_microsoft_com_claims_authnmethodsreferences_Azure	http://schemas.microsoft.com/claims/authnmethodsreferences
http__schemas_xmlsoap_org_ws_2005_05_identity_claims_surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
http__schemas_xmlsoap_org_ws_2005_05_identity_claims_emailaddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
http__schemas_xmlsoap_org_ws_2005_05_identity_claims_name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Department_Azure	Department

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 here that have not already been imported.

With the Attributes from AAD, the **Names** generally include protocol and schema prefixes that make them very hard to read, especially in the **Access Policy** configuration dialog. We recommend that you rename them to make the **Names** readable by humans. To do this simply click in the **Name** field for an Attribute and edit the text.

Slide 80 - Slide 80

Name	SAML Attribute Name
TenantID_Azure	http://schemas.microsoft.com/identity/claims/tenantid
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier
DisplayName_Azure	http://schemas.microsoft.com/identity/claims/displayname
Groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
IdentityProvider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider
AuthnMethodsReferences_Azure	http://schemas.microsoft.com/claims/authnmethodsreferences
Surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
EmailAddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Department_Azure	Department

Slide notes

Once you have renamed the attributes and verified that you have the complete list of attributes available, scroll down, ...

Slide 81 - Slide 81

The screenshot shows the Adobe Captivate interface with a sidebar on the left containing icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area displays a table of SAML attributes and a JSON import section.

AttributeName	AttributeValue
DisplayName_Azure	http://schemas.microsoft.com/identity/claims/displayname
Groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
IdentityProvider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider
AuthnMethodsReferences_Azure	http://schemas.microsoft.com/claims/authnmethodsreferences
Surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
EmailAddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Dep	Department

A callout box labeled "Click Save" points to the "Save" button in the bottom-left corner of the table's modal. Another callout box labeled "Verify the user's data in the Import SAML JSON" points to the JSON code in the "Import SAML JSON" text area. A red box highlights the JSON code.

```
[{"nameid": "student@patraining9.safemarch.com", "orgid": "144123467699060736", "idpEntityID": "https://sts.windows.net/553d1d85-7ec5-41b4-96ff-f972486e0e2c/", "idpId": "144123467699061827", "saml_attributes": [ {"http://schemas.microsoft.com/identity/claims/tenantid": "553d1d85-7ec5-41b4-96ff-f972486e0e2c", "http://schemas.microsoft.com/identity/claims/objectidentifier": "ac5d0d66-1fea-482f-ade8-2e06846e1132", "http://schemas.microsoft.com/identity/claims/displayname": "student test", "http://schemas.microsoft.com/ws/2008/06/identity/claims/groups": "b14d715a-644c-467a-809f-06b534fc2143", "http://schemas.microsoft.com/identity/claims/department": "IT", "http://schemas.microsoft.com/identity/claims/extension": "extension_value", "http://schemas.microsoft.com/identity/claims/extension2": "extension2_value"}]}
```

Slide notes

...and review the **Import SAML JSON** text, which are the values for the attributes returned by AAD for the user that you logged in with, verify that they are correct. Note, you can use this as a tool at any time to evaluate the attribute values for a user when troubleshooting authentication issues.

Once you are happy, click to **Save the SAML Attributes**.

Slide 82 - Slide 82

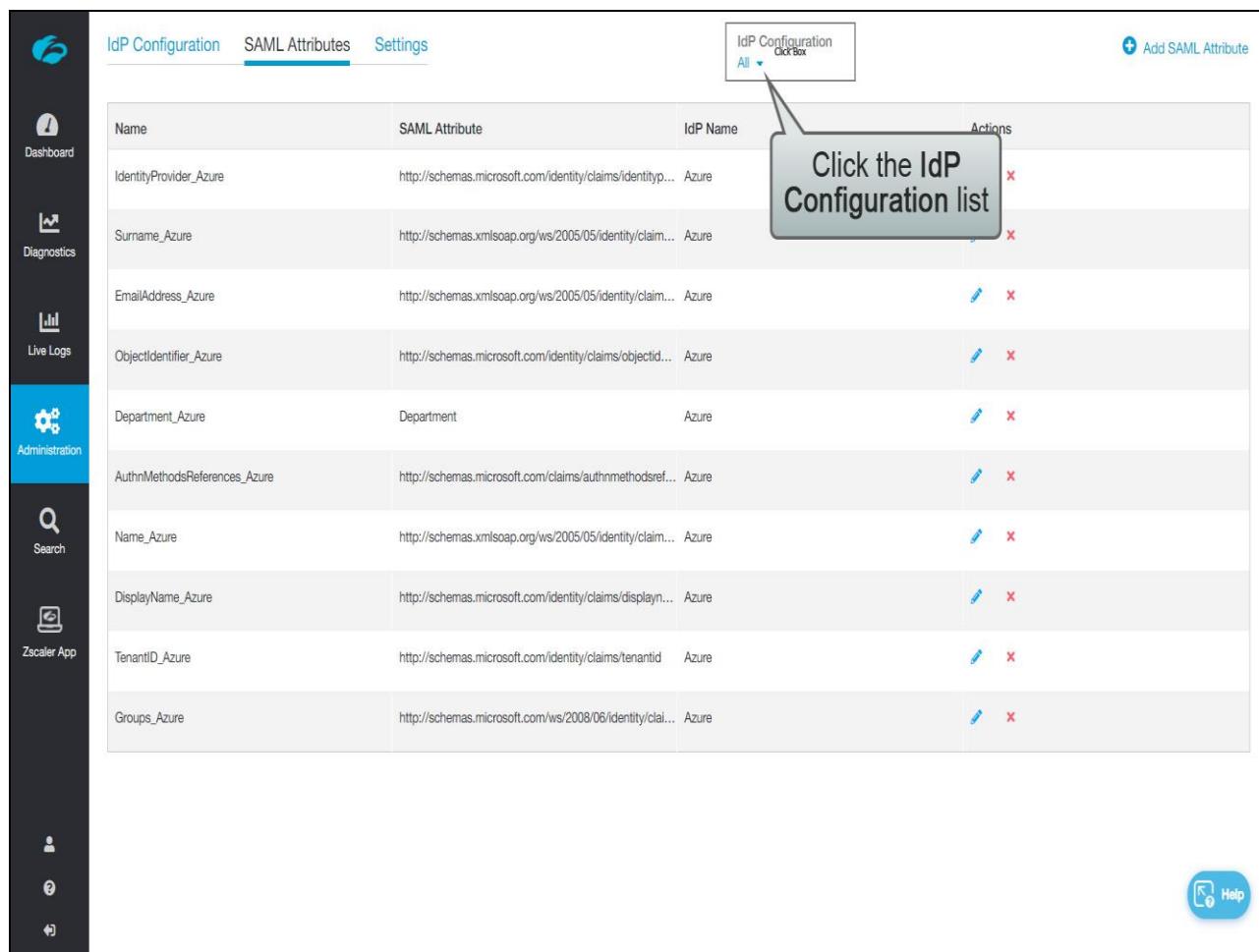
The screenshot shows the Adobe Captivate interface with the 'Administration' menu selected. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Zscaler App, and other system status indicators. The main content area is titled 'IdP Configuration' and has tabs for 'IdP Configuration', 'SAML Attributes', and 'Settings'. The 'SAML Attributes' tab is active. It displays a table of attributes with columns: Name, SAML Attribute, IdP Name, and Actions. The table lists ten attributes, all associated with 'Azure' as the IdP Name. Each row has edit and delete icons in the Actions column. A green notification bar at the bottom right says 'SAML attributes imported successfully'.

Name	SAML Attribute	IdP Name	Actions
IdentityProvider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider	Azure	
Surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Azure	
EmailAddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Azure	
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier	Azure	
Department_Azure	Department	Azure	
AuthnMethodsReferences_Azure	http://schemas.microsoft.com/claims/authnmethodsreference	Azure	
Name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Azure	
DisplayName_Azure	http://schemas.microsoft.com/identity/claims/displayname	Azure	
TenantID_Azure	http://schemas.microsoft.com/identity/claims/tenantid	Azure	
Groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/groups	Azure	

SAML attributes imported successfully

Slide notes

Slide 83 - Slide 83



The screenshot shows the Zscaler Admin UI with the 'SAML Attributes' tab selected. On the left, a vertical sidebar lists various navigation options: Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and three user-related icons. The main content area displays a table of SAML attributes. At the top of the table, there is a dropdown menu labeled 'IdP Configuration' with a sub-menu 'All'. A callout box with the text 'Click the IdP Configuration list' points to this dropdown. The table has columns for Name, SAML Attribute, IdP Name, and Actions (edit and delete icons). Below the table, there is a 'Help' button.

Name	SAML Attribute	IdP Name	Actions
IdentityProvider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider	Azure	
Surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Azure	
EmailAddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Azure	
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier	Azure	
Department_Azure	Department	Azure	
AuthnMethodsReferences_Azure	http://schemas.microsoft.com/claims/authnmethodsref	Azure	
Name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Azure	
DisplayName_Azure	http://schemas.microsoft.com/identity/claims/displayname	Azure	
TenantID_Azure	http://schemas.microsoft.com/identity/claims/tenantid	Azure	
Groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/groups	Azure	

Slide notes

You will be taken to the **SAML Attributes** page to allow you to review all the attributes currently saved. If you have added multiple IdPs, you have the option to filter this list by IdP, click the **IdP Configuration** list at the top, ...

Slide 84 - Slide 84

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, Administration (selected), Search, and Zscaler App. The main content area has tabs for 'IdP Configuration', 'SAML Attributes' (selected), and 'Settings'. A sub-header 'IdP Configuration' with dropdowns for 'All' and 'Azure' is visible. A button 'Add SAML Attribute' is at the top right. The main table lists various SAML attributes:

Name	SAML Attribute	IdP Name	Actions
IdentityProvider_Azure	http://schemas.microsoft.com/identity/claims/identityp...	Azure	
Surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claim...	Azure	
EmailAddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claim...	Azure	
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/objectid...	Azure	
Department_Azure	Department	Azure	
AuthnMethodsReferences_Azure	http://schemas.microsoft.com/claims/authnmethodsref...	Azure	
Name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claim...	Azure	
DisplayName_Azure	http://schemas.microsoft.com/identity/claims/display...	Azure	
TenantID_Azure	http://schemas.microsoft.com/identity/claims/tenantid	Azure	
Groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/clai...	Azure	

At the bottom left is the URL <https://admin.private.zscaler.com>. At the bottom right is a 'Help' button.

Slide notes

...and select the IdP of interest.

Slide 85 - The End User Experience

**Slide notes**

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

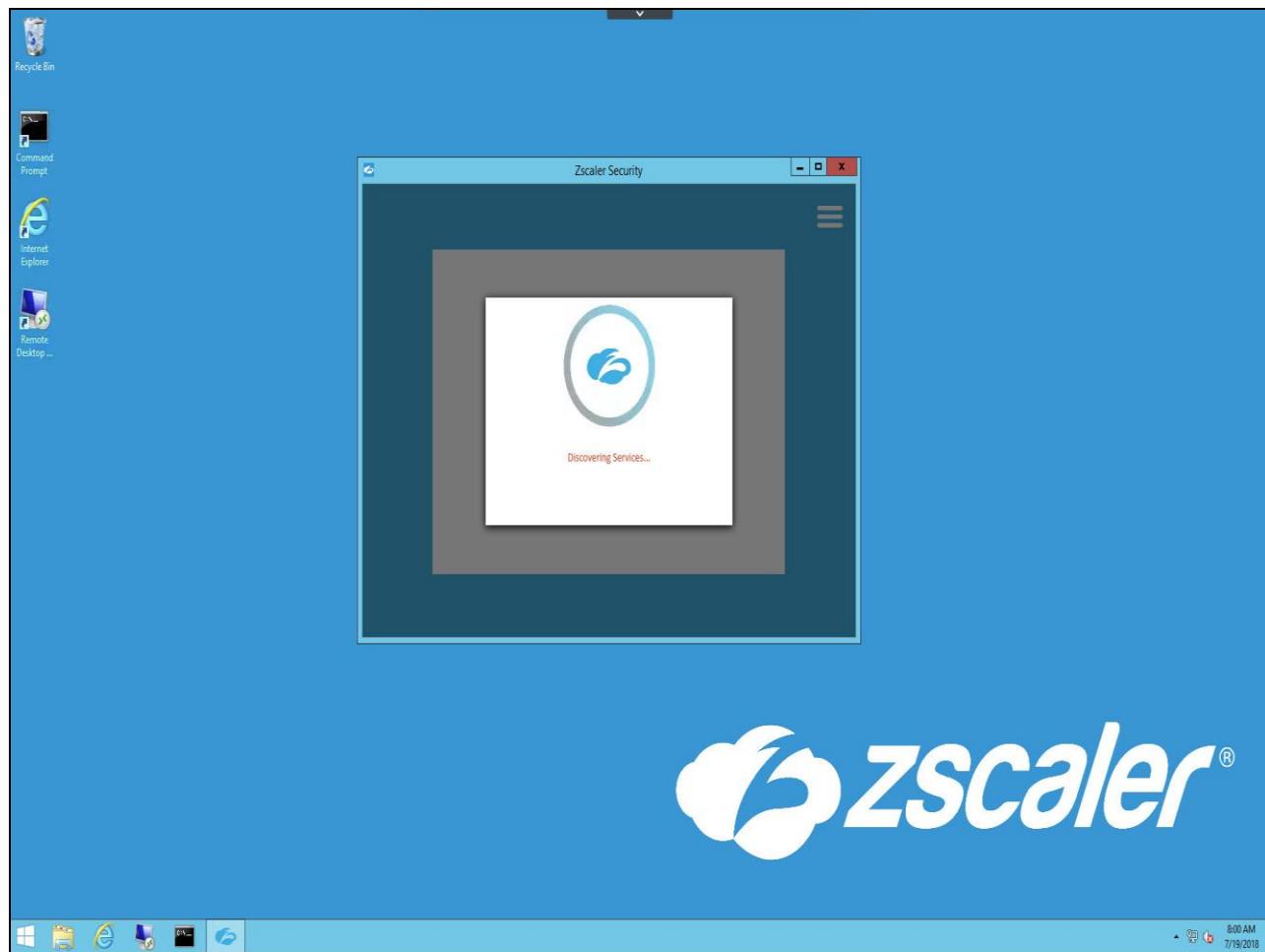
Slide 86 - Slide 86



Slide notes

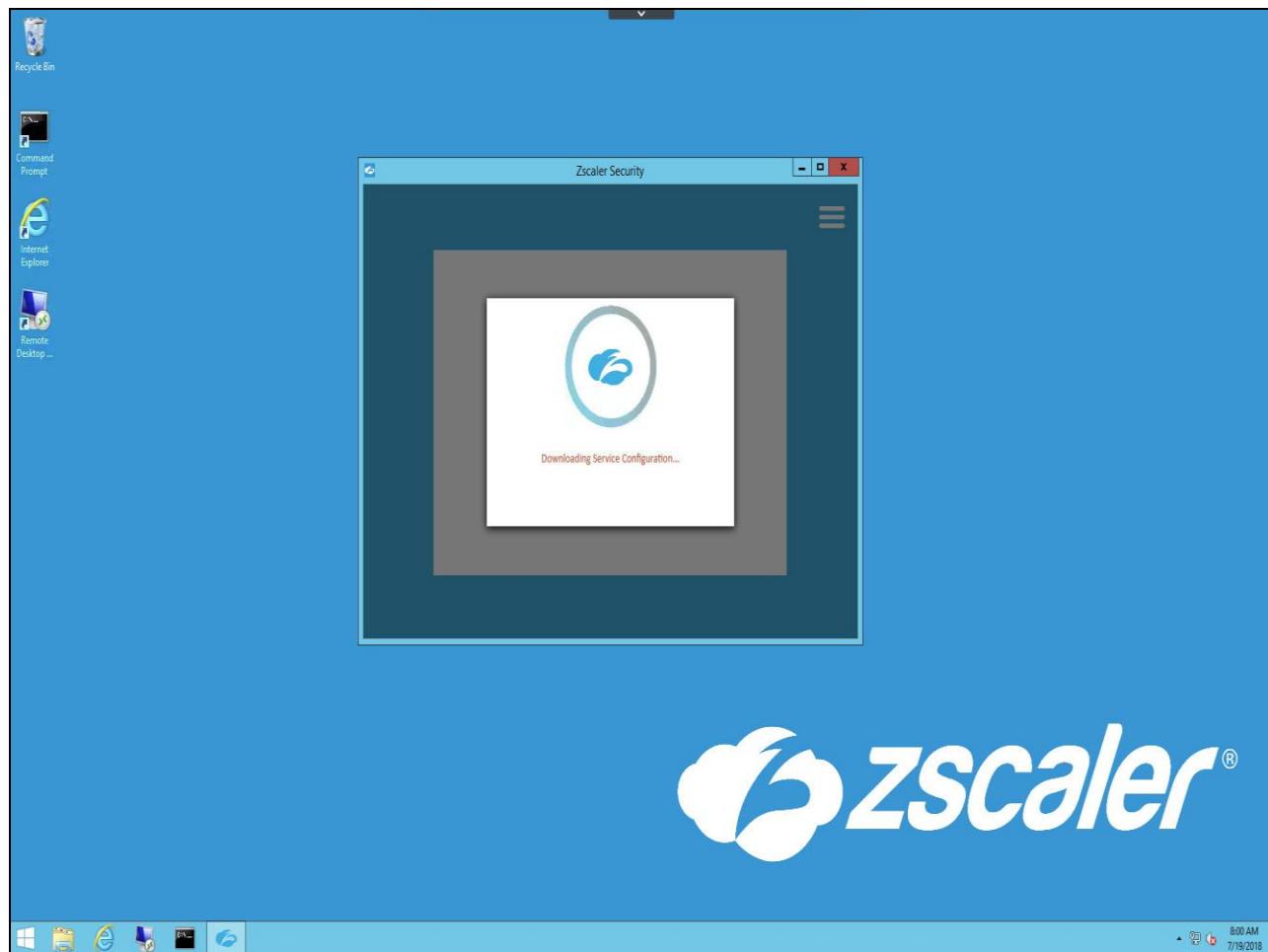
On a client machine that has the Zscaler App installed on it (PC or mobile, for this example we will use a Windows client), run the App, provide valid end user credentials (in the form of an email address) and click **Sign In**.

Slide 87 - Slide 87



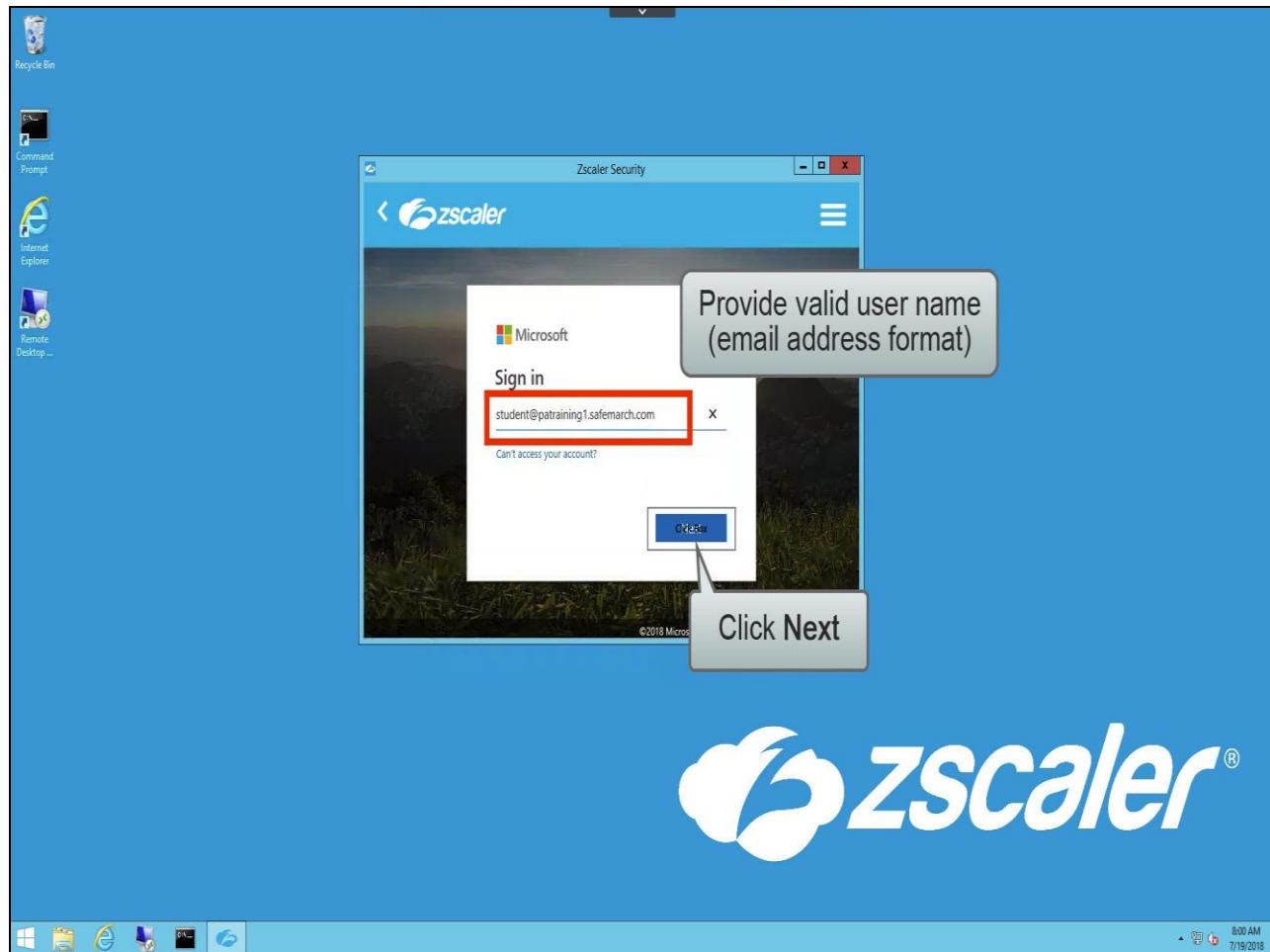
Slide notes

Slide 88 - Slide 88



Slide notes

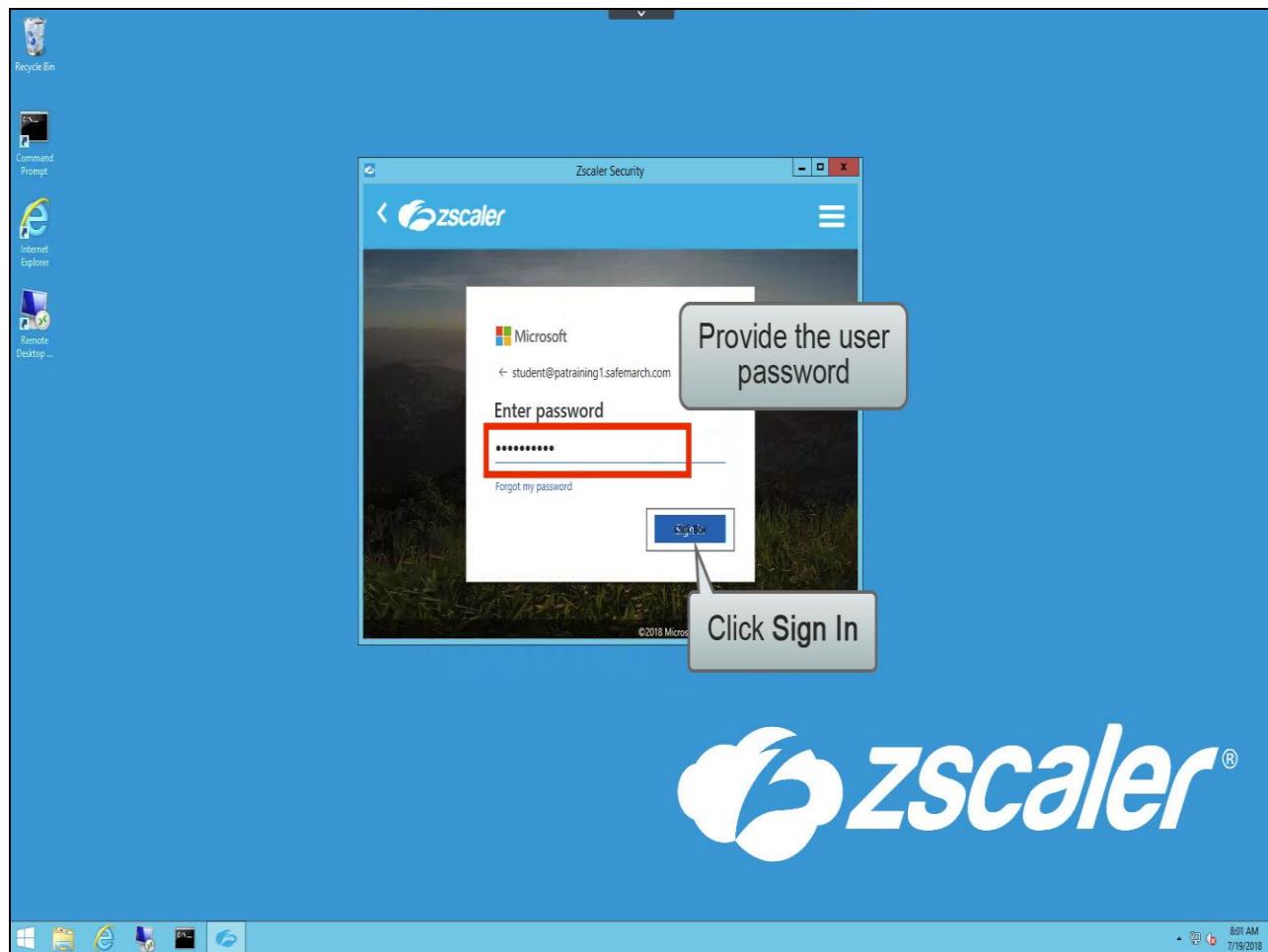
Slide 89 - Slide 89



Slide notes

Once the Azure login page loads, provide the username and click **Next**.

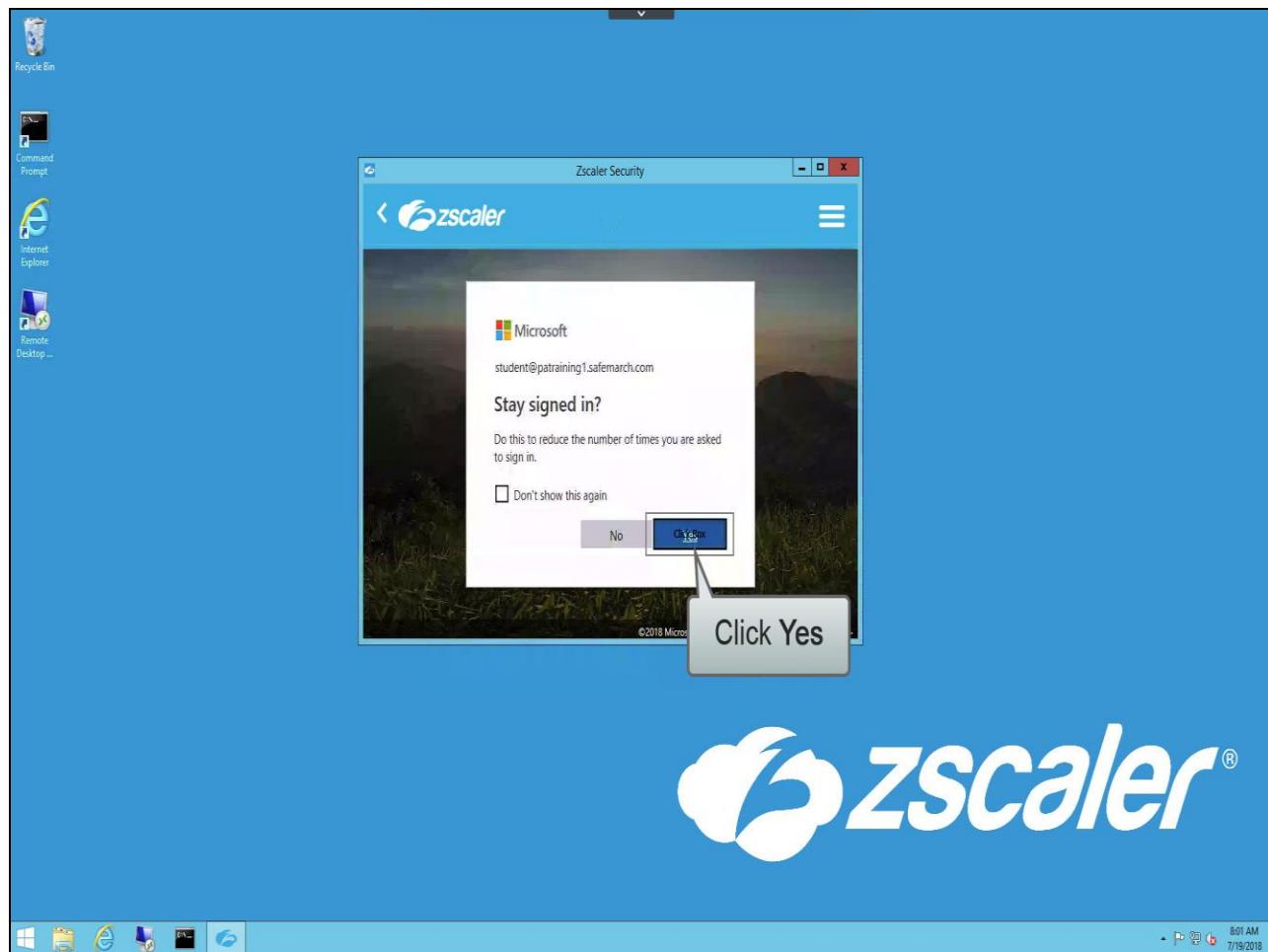
Slide 90 - Slide 90



Slide notes

Provide the user's password and click **Sign In**.

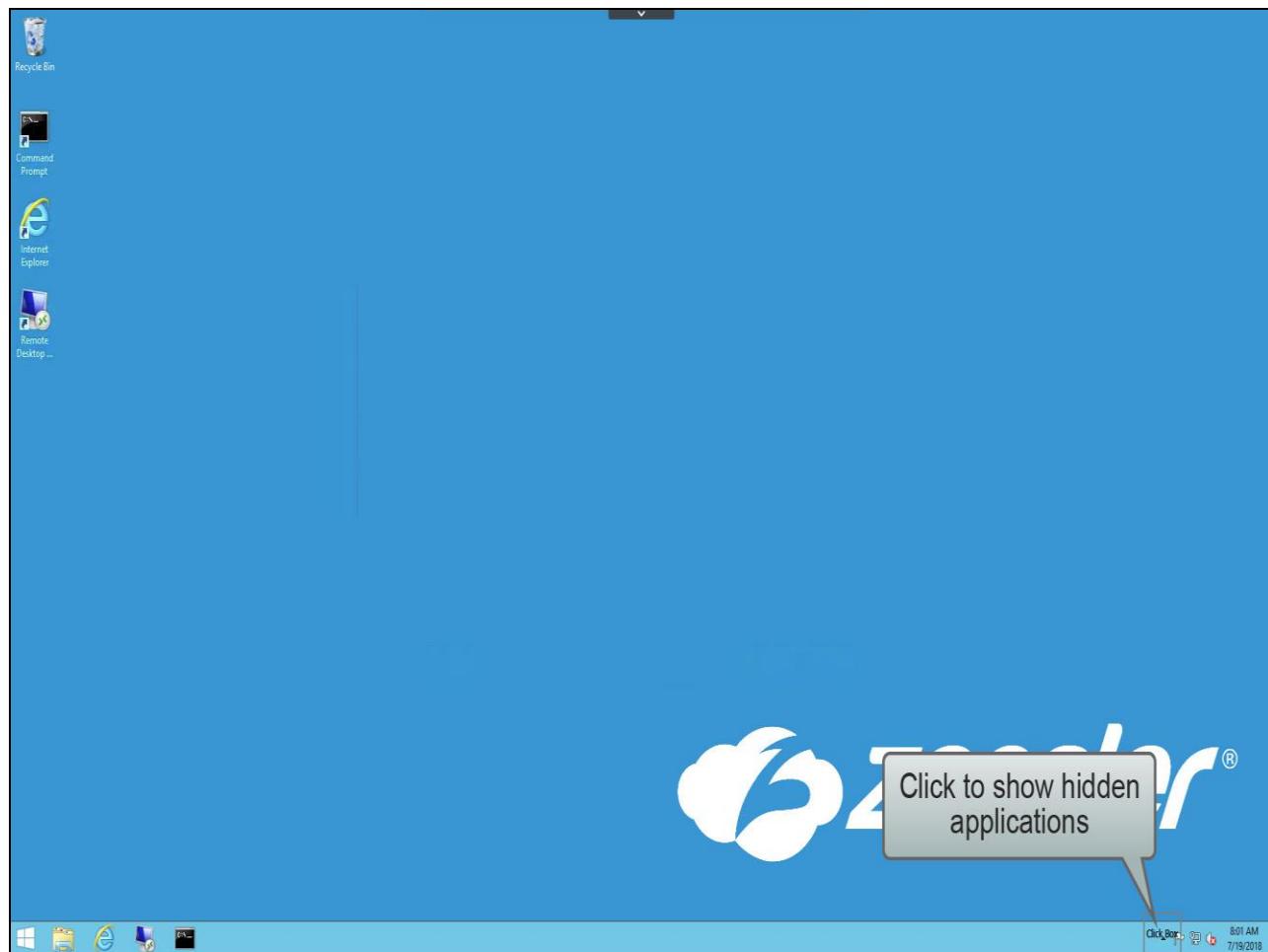
Slide 91 - Slide 91



Slide notes

Elect whether or not to stay signed in, in this instance click **Yes**.

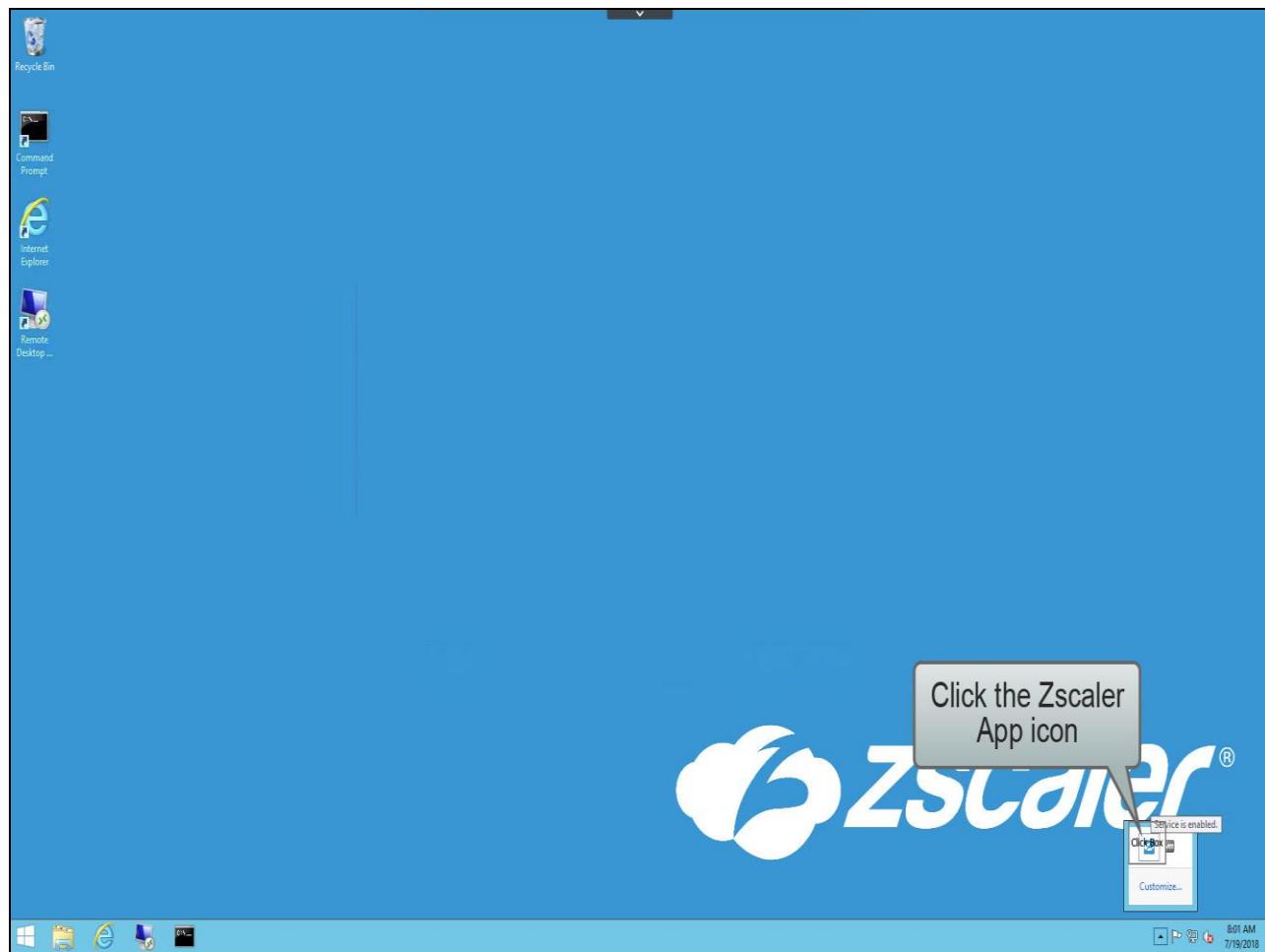
Slide 92 - Slide 92



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, ...

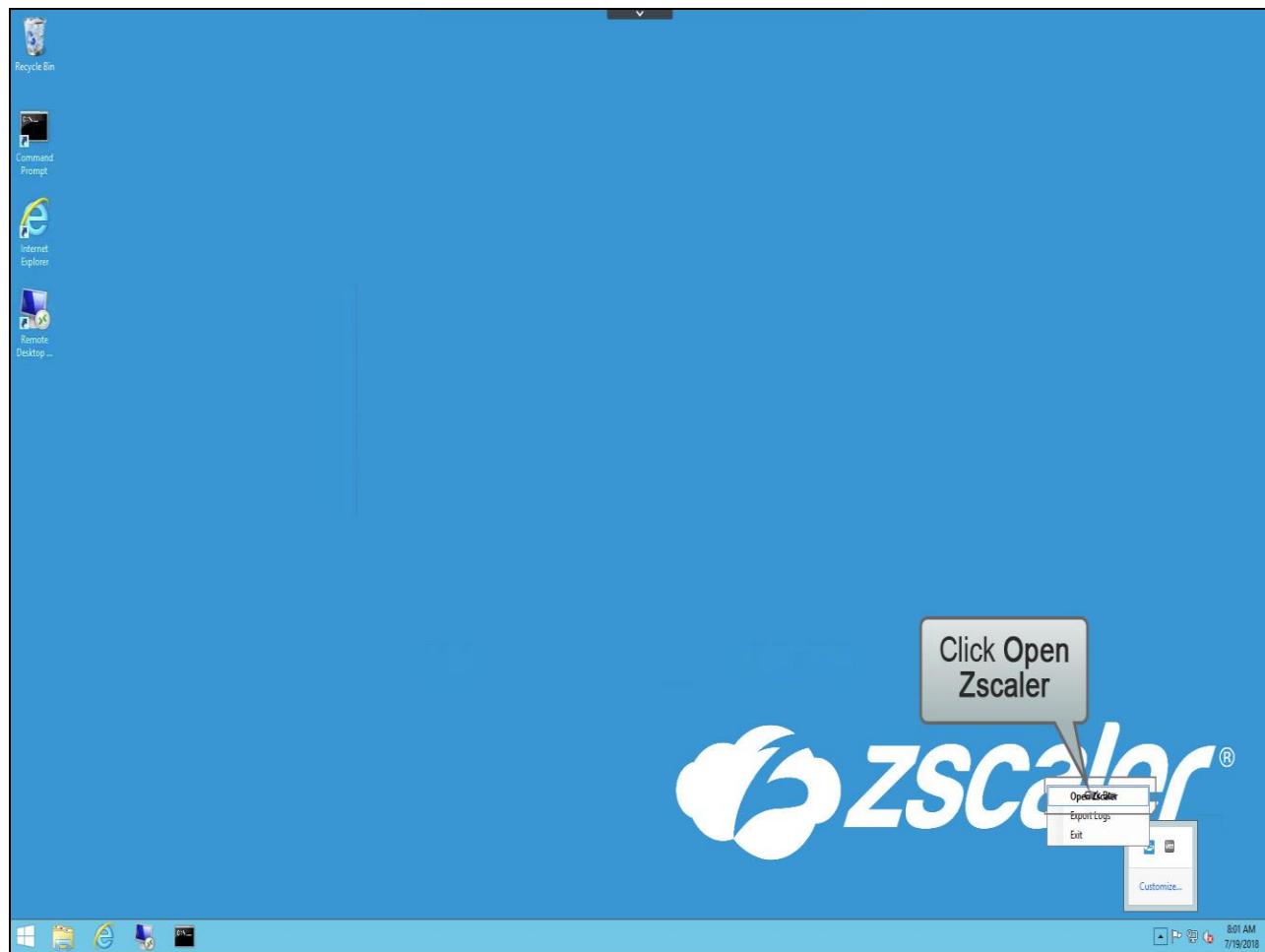
Slide 93 - Slide 93



Slide notes

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

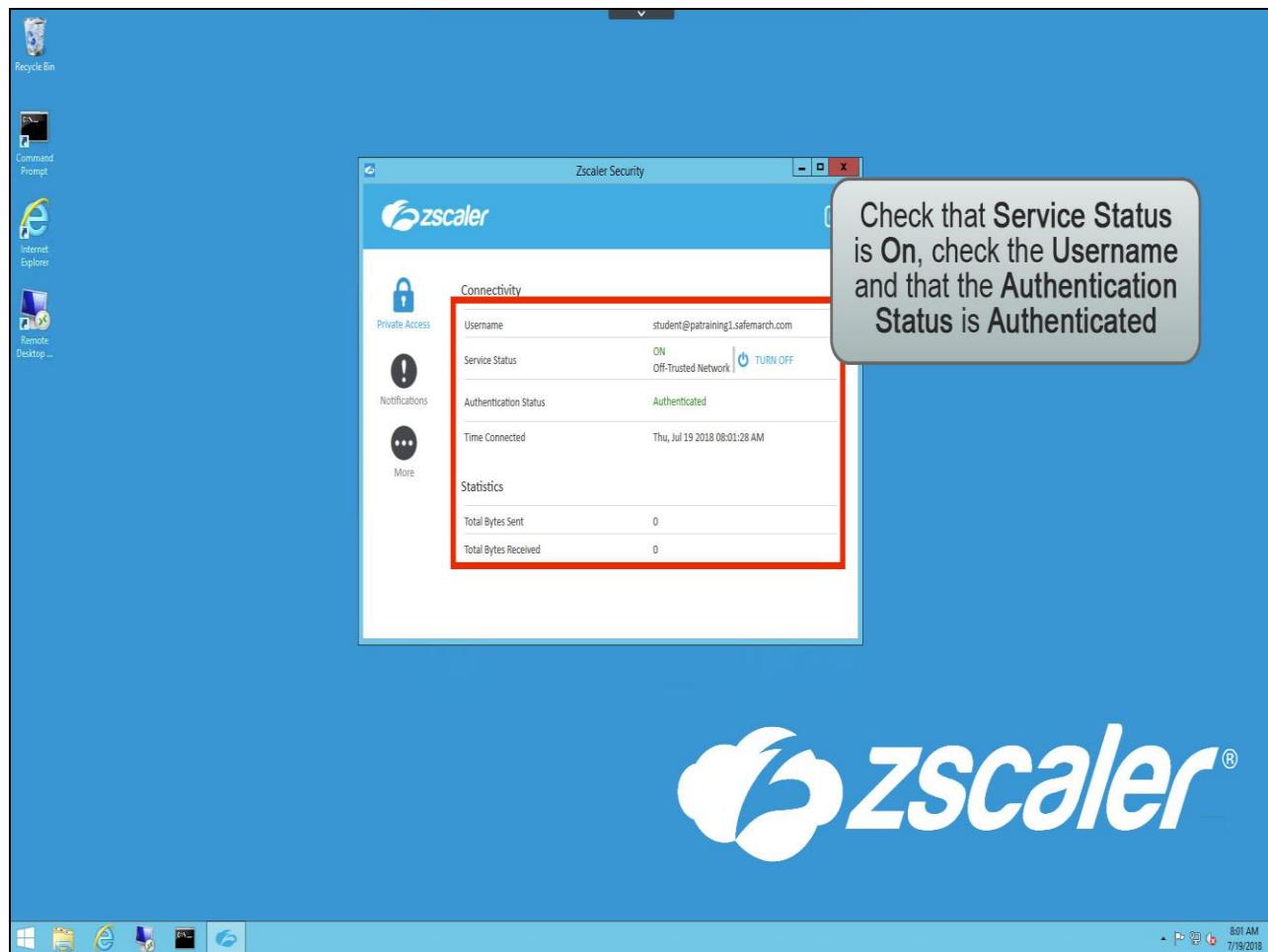
Slide 94 - Slide 94



Slide notes

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

Slide 95 - Slide 95

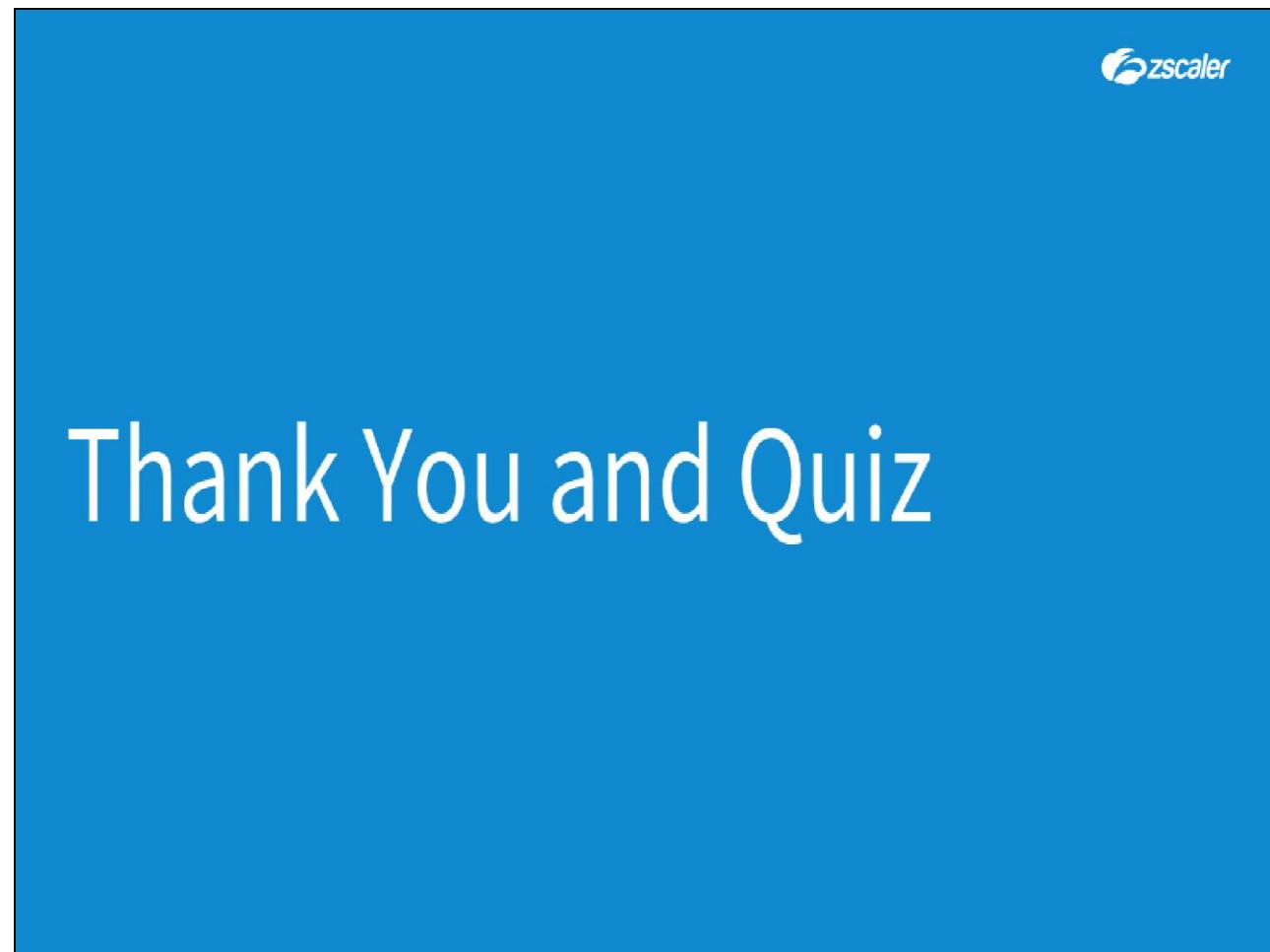


Slide notes

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 96 - 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.

Click the X at top right to close this interface, then launch the 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.