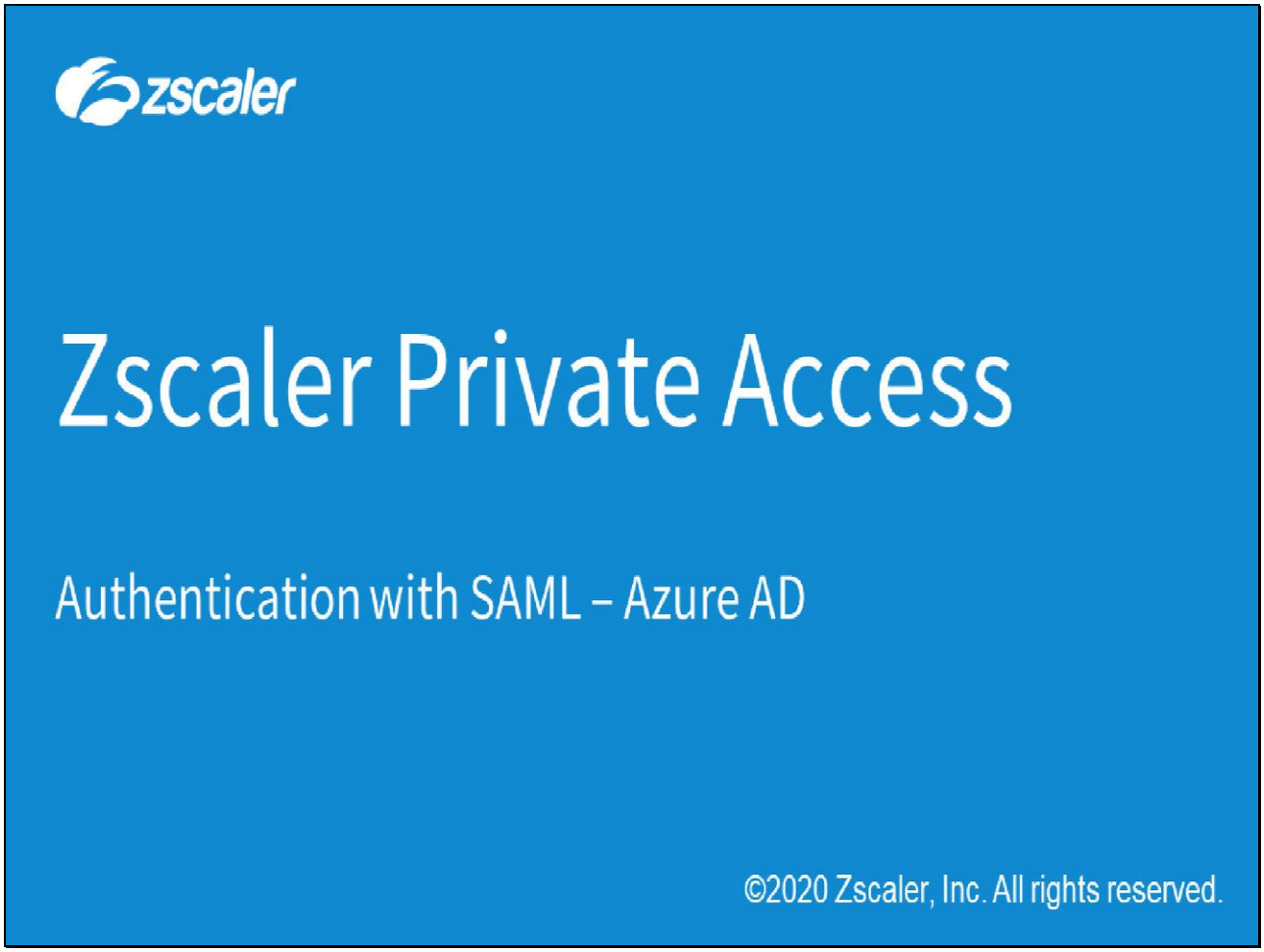
Slide 1 – Authentication with SAML – Azure AD



Slide notes

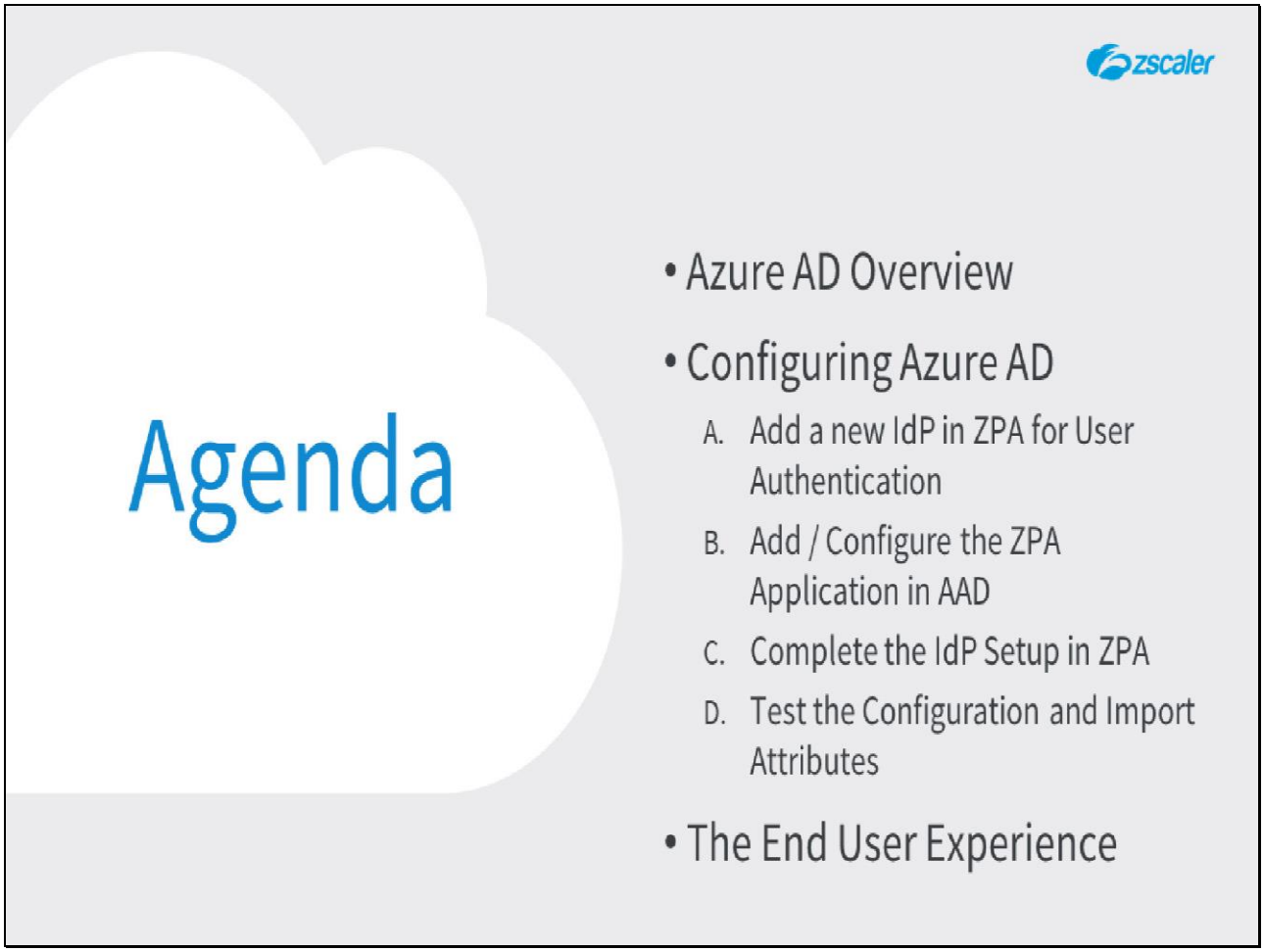
Welcome to this training module on configuring ZPA to use Azure AD (AAD) for authenticating users.

Slide 2 - Navigating the eLearning Module

Slide notes

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

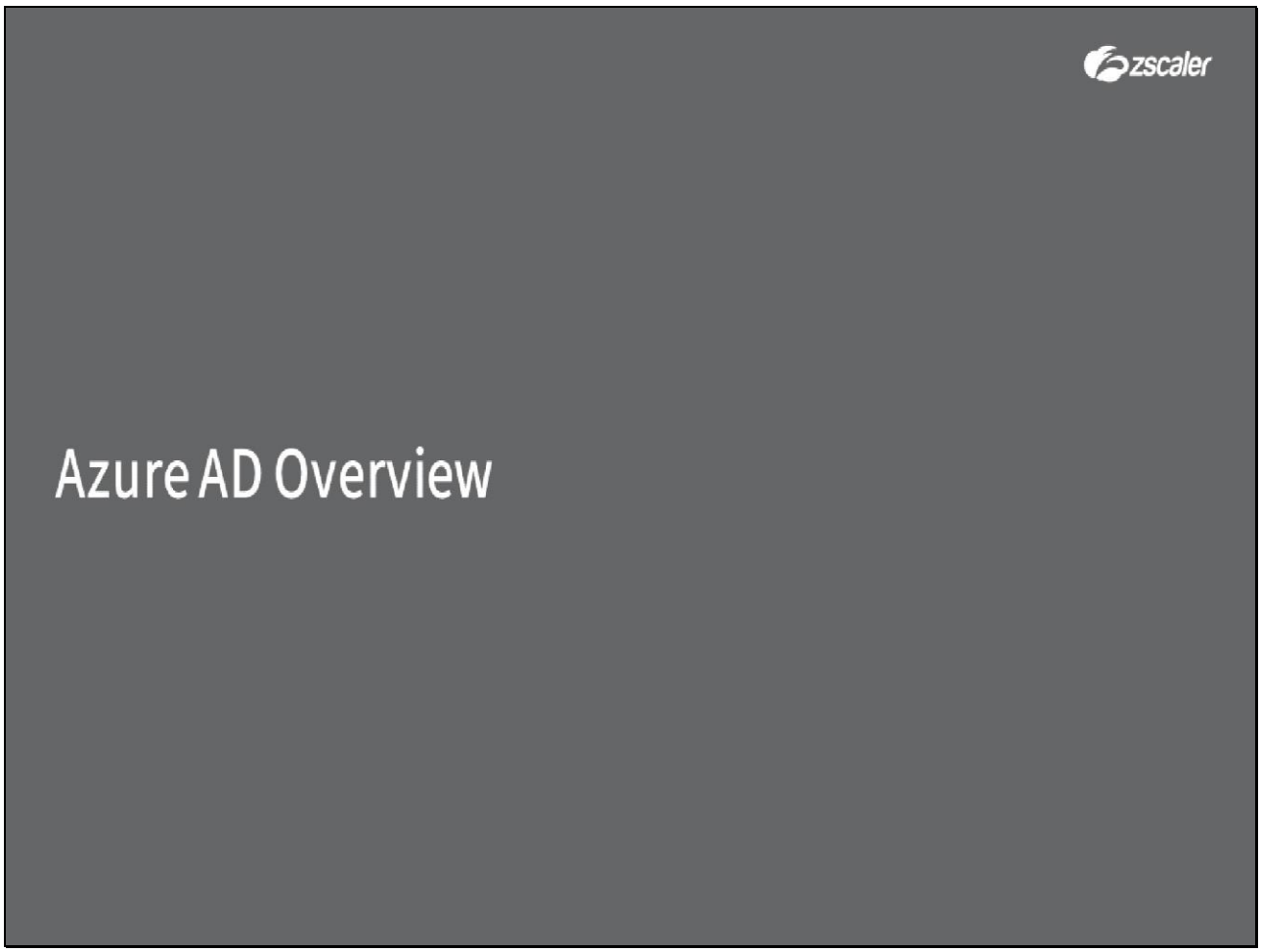


Slide notes

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.

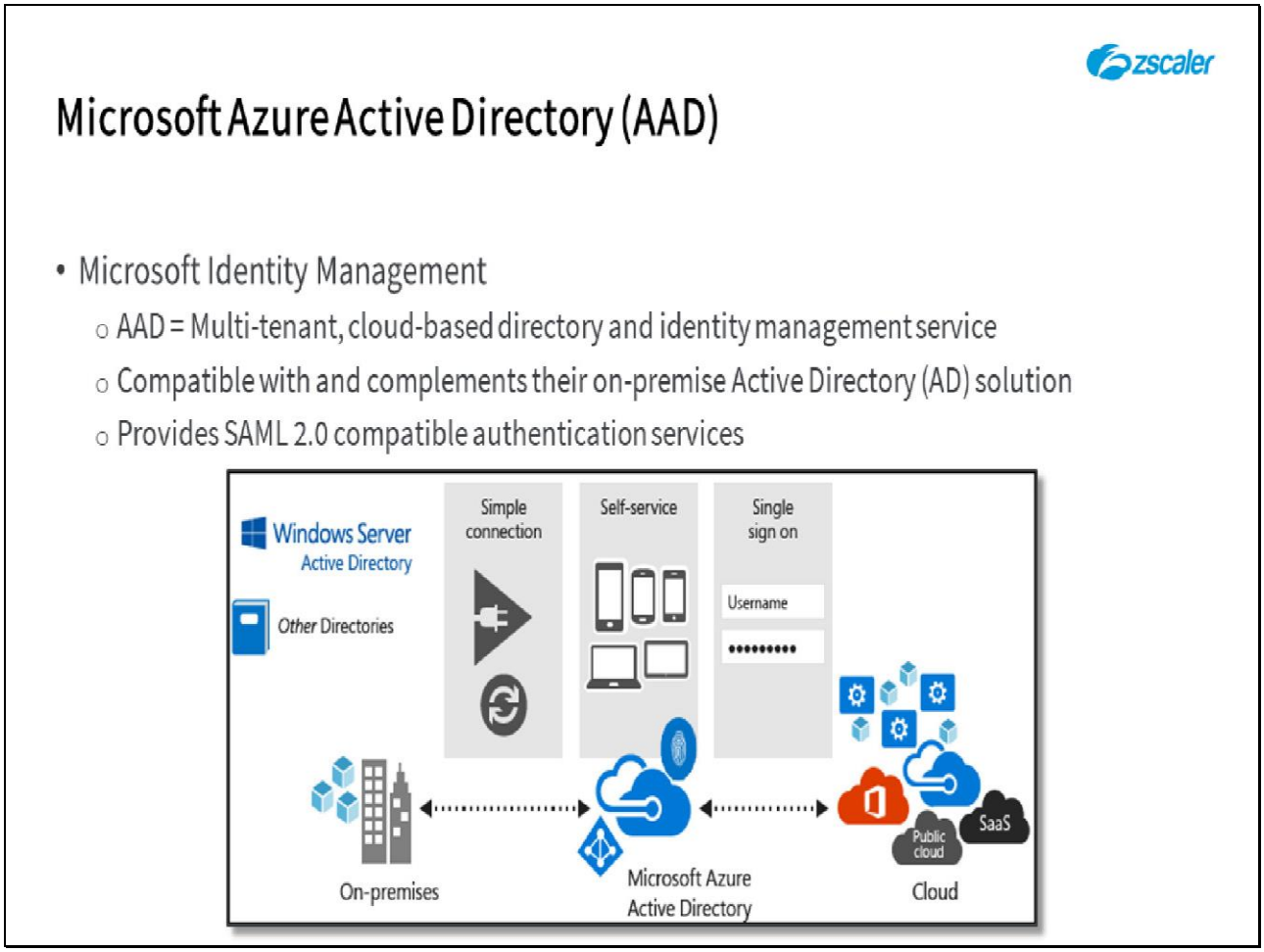
Slide 4 - Okta Overview



Slide notes

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

Slide 5 - Microsoft Azure Active Directory (AAD)

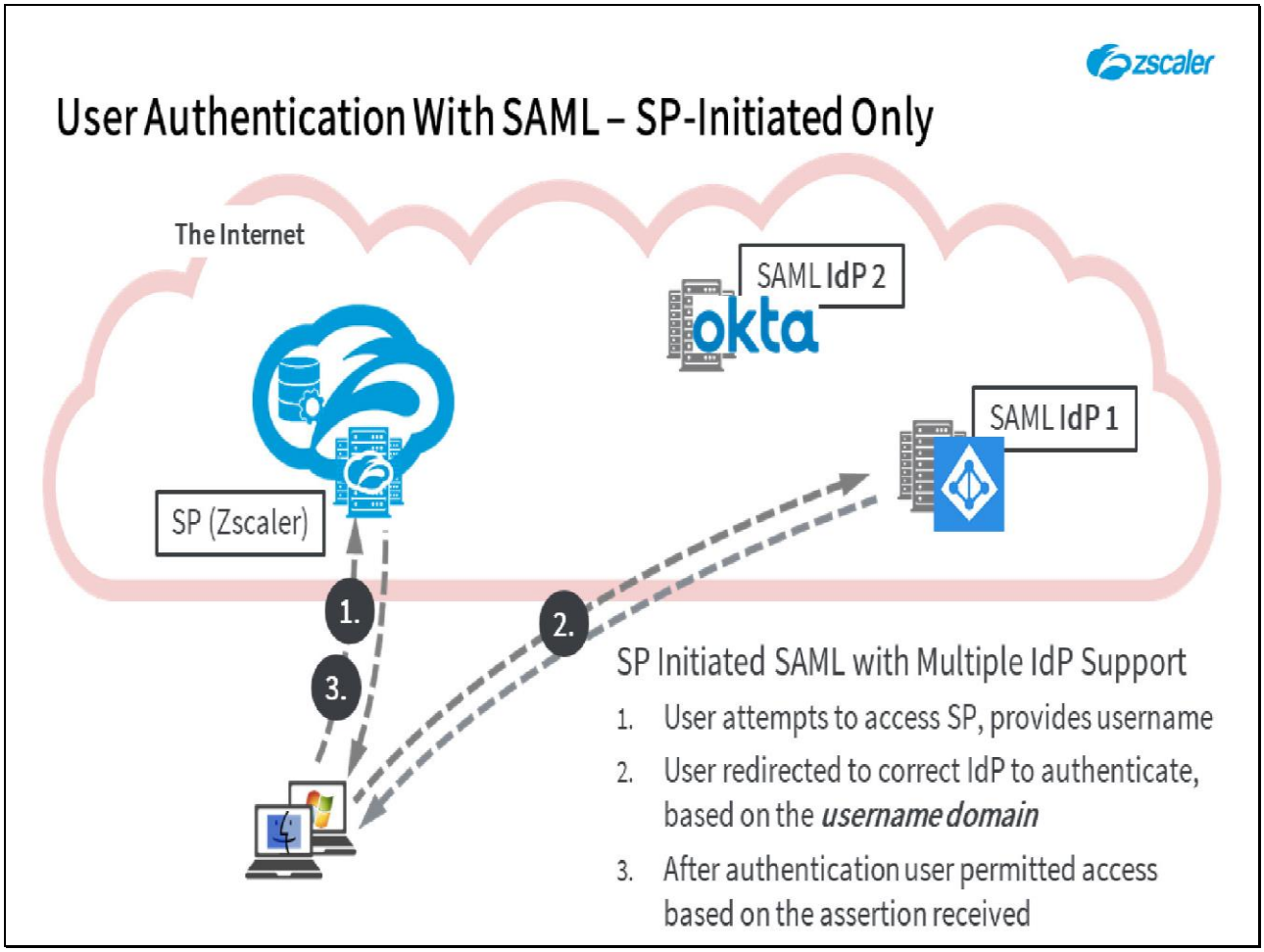


Slide notes

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 compliments 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

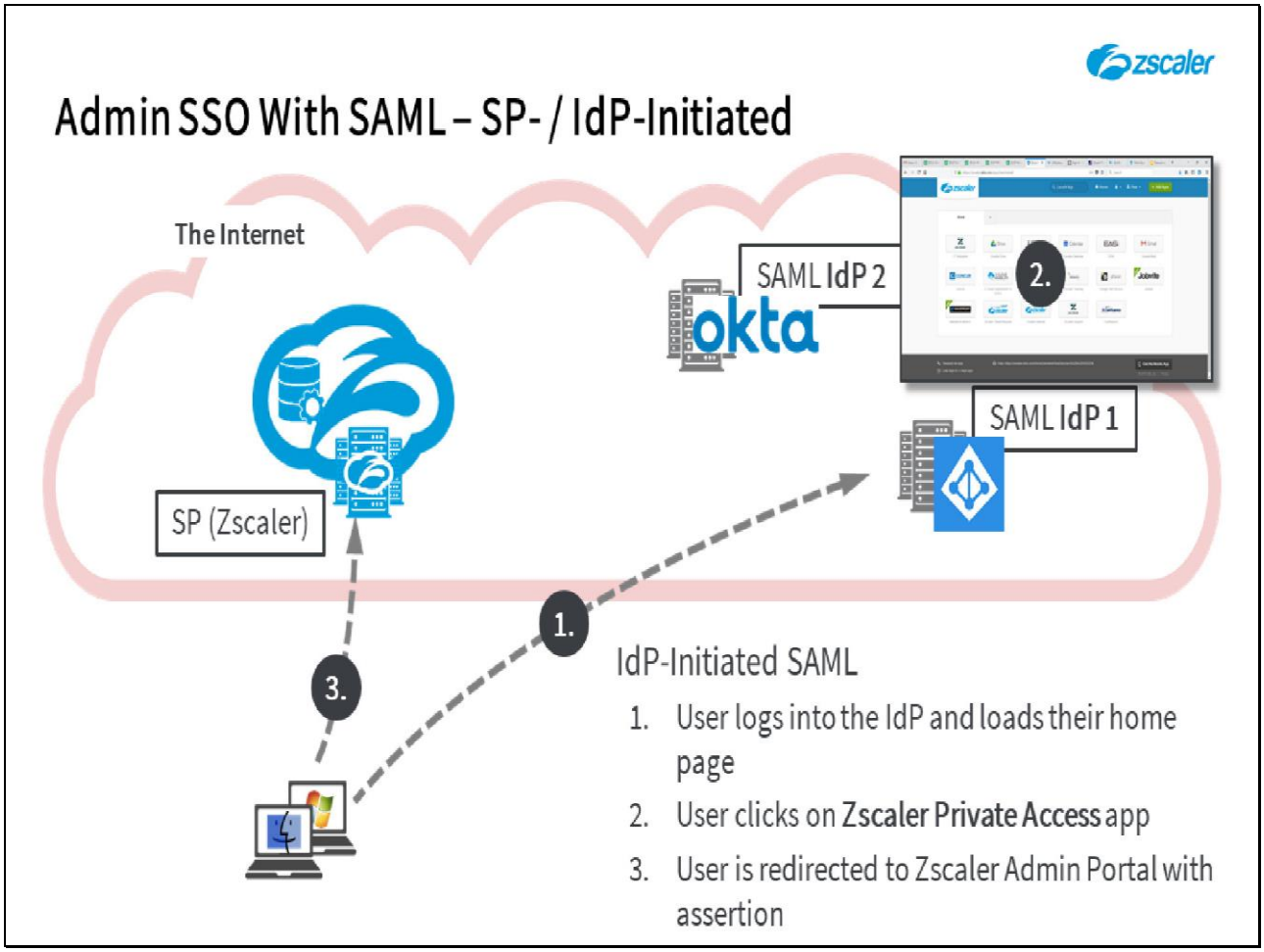


Slide notes

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.

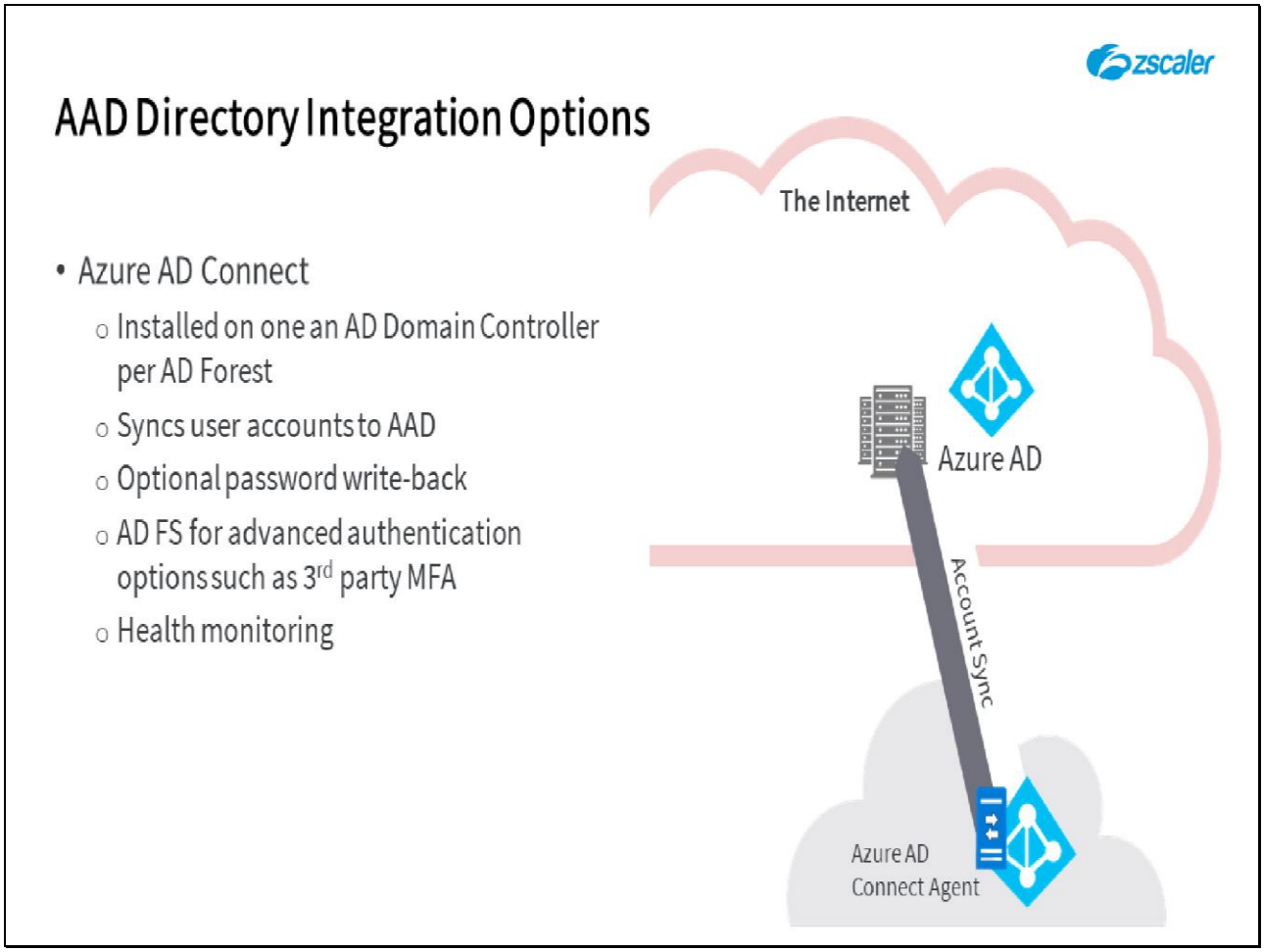
Slide 7 - Admin SSO With SAML – SP- / IdP-Initiated



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



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.

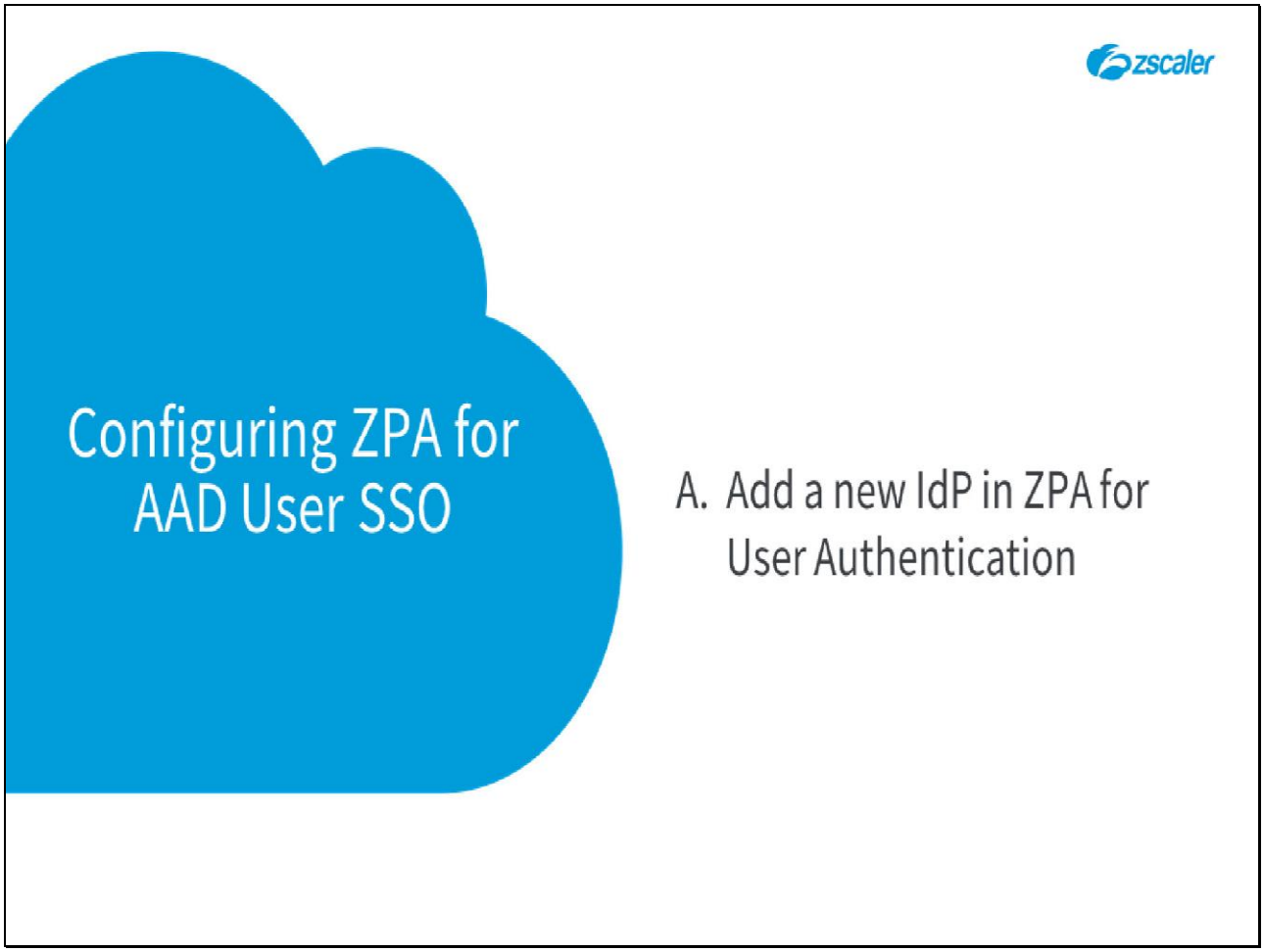
Slide 9 - Configuring Okta

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.

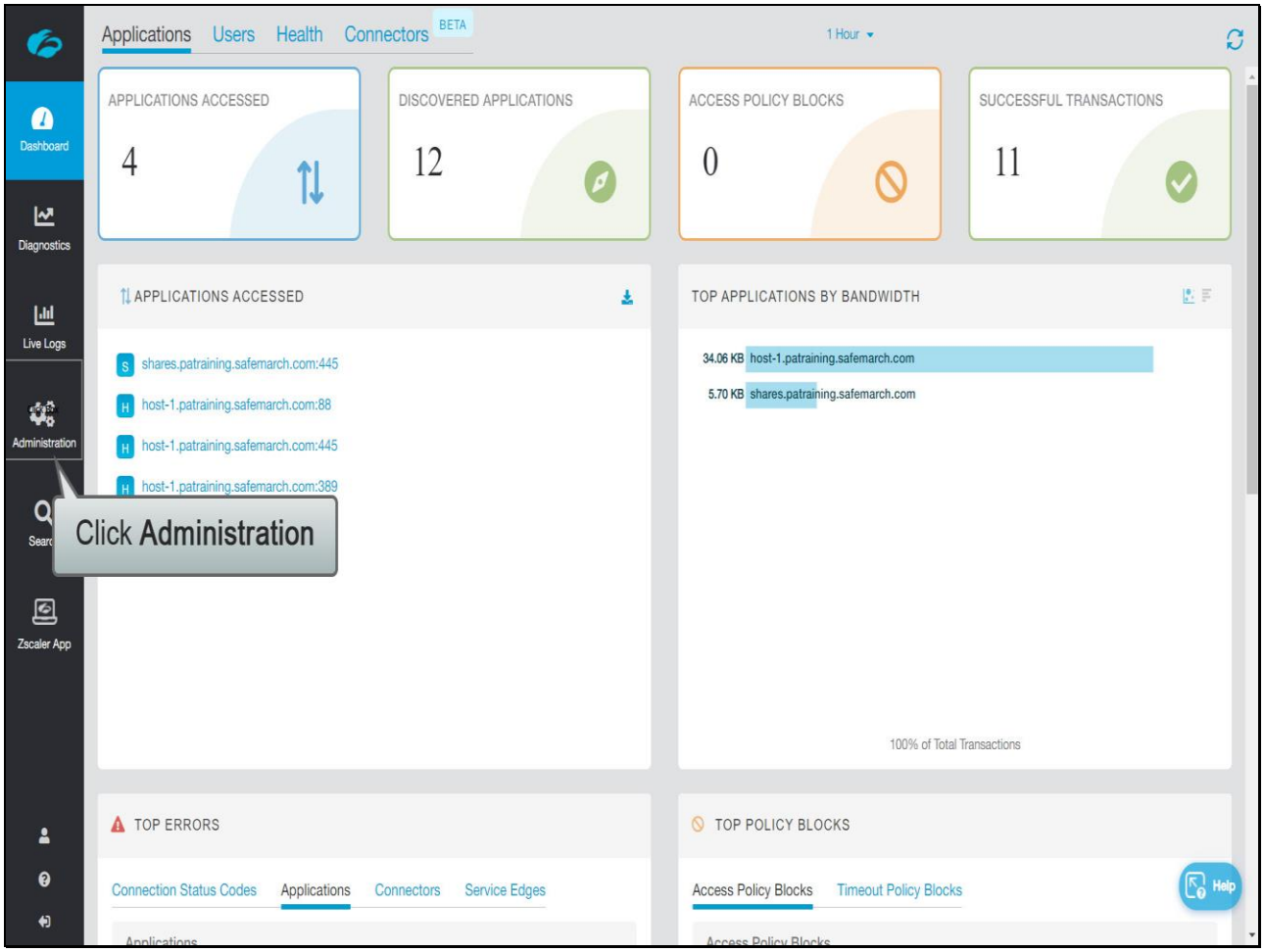
Slide 10 - Configuring ZPA for Okta User SSO



Slide notes

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

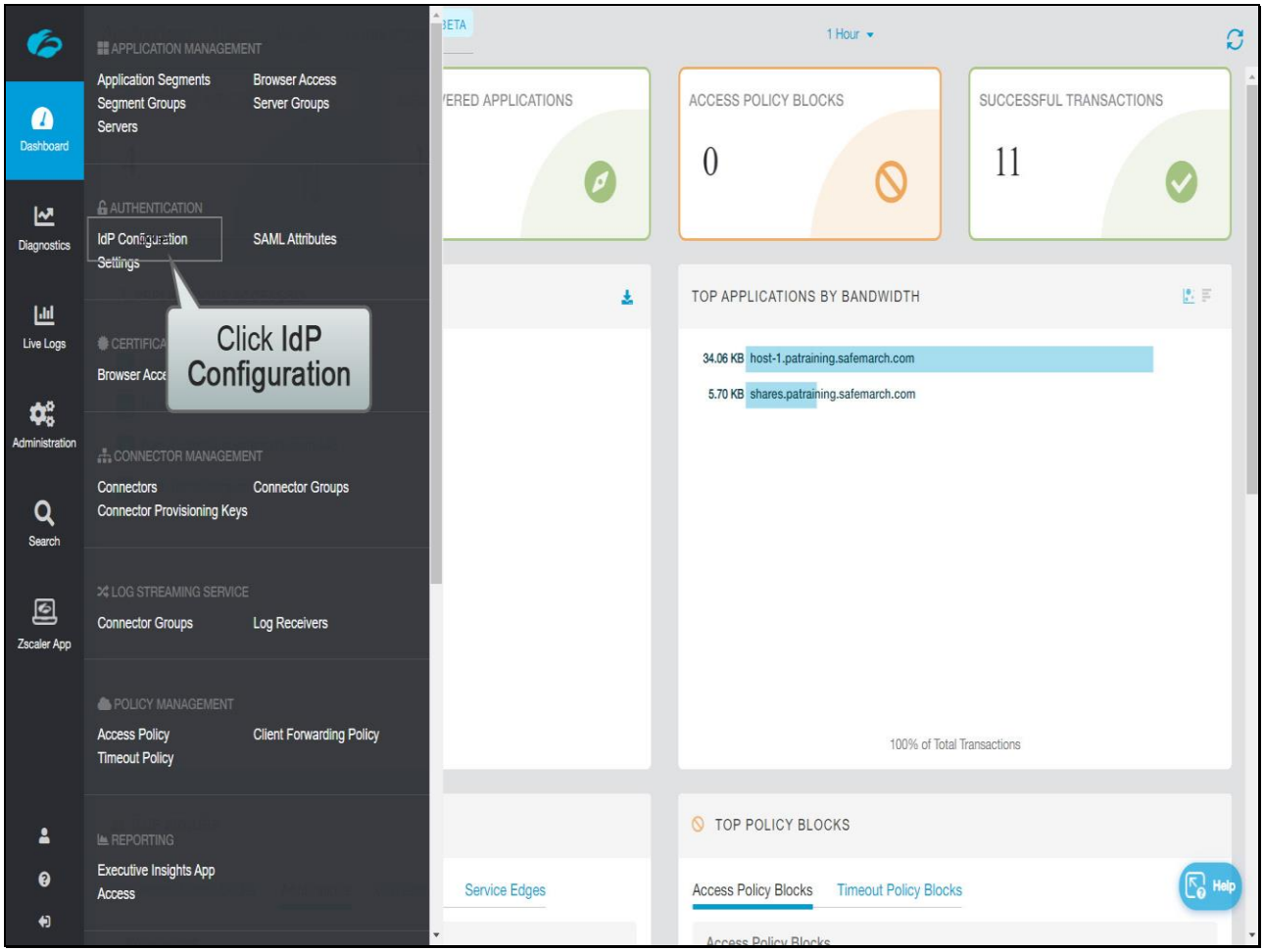
Slide 11 - Slide 11



Slide notes

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

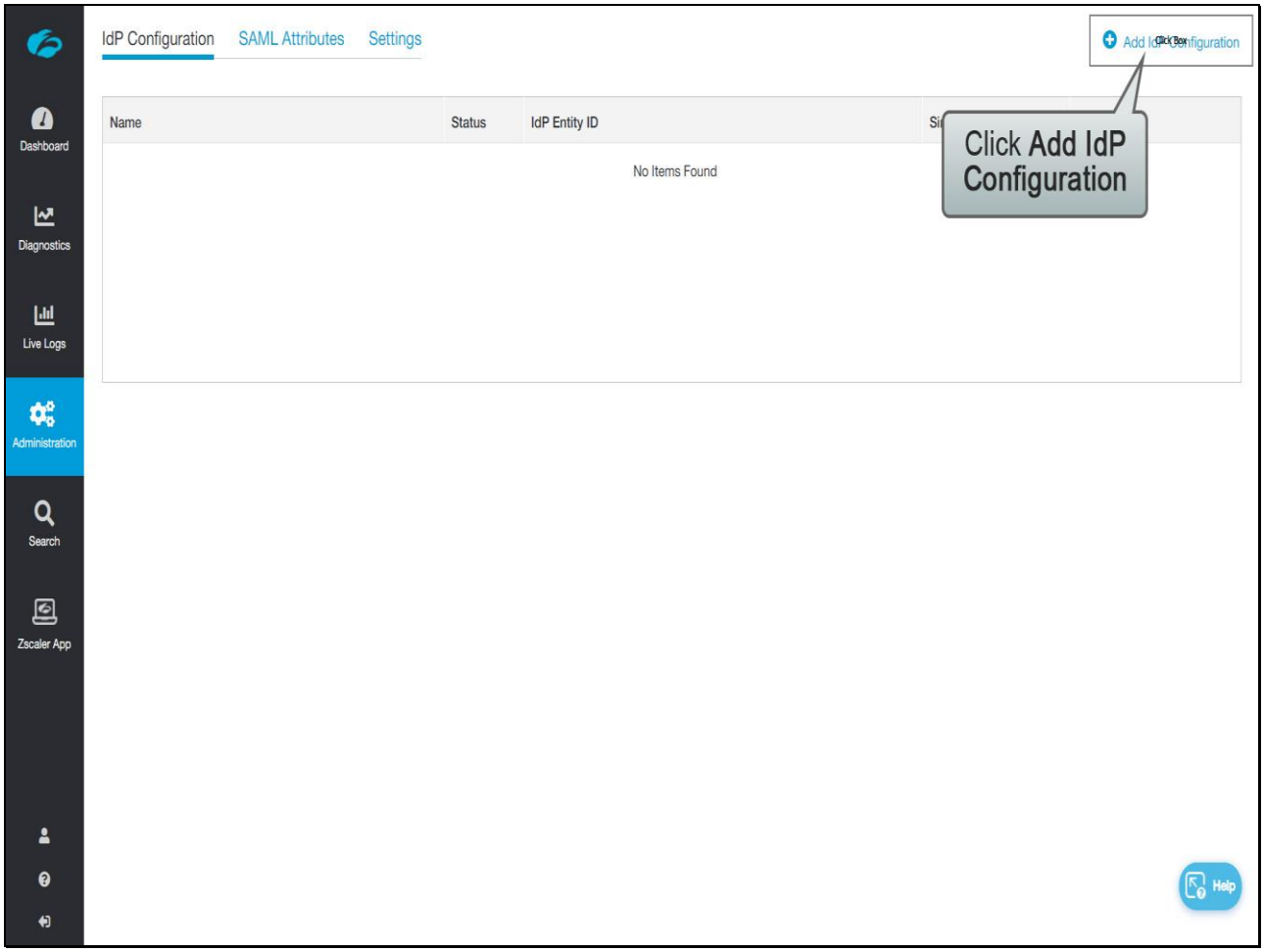
Slide 12 - Slide 12



Slide notes

...then **IdP Configuration**.

Slide 13 - Slide 13

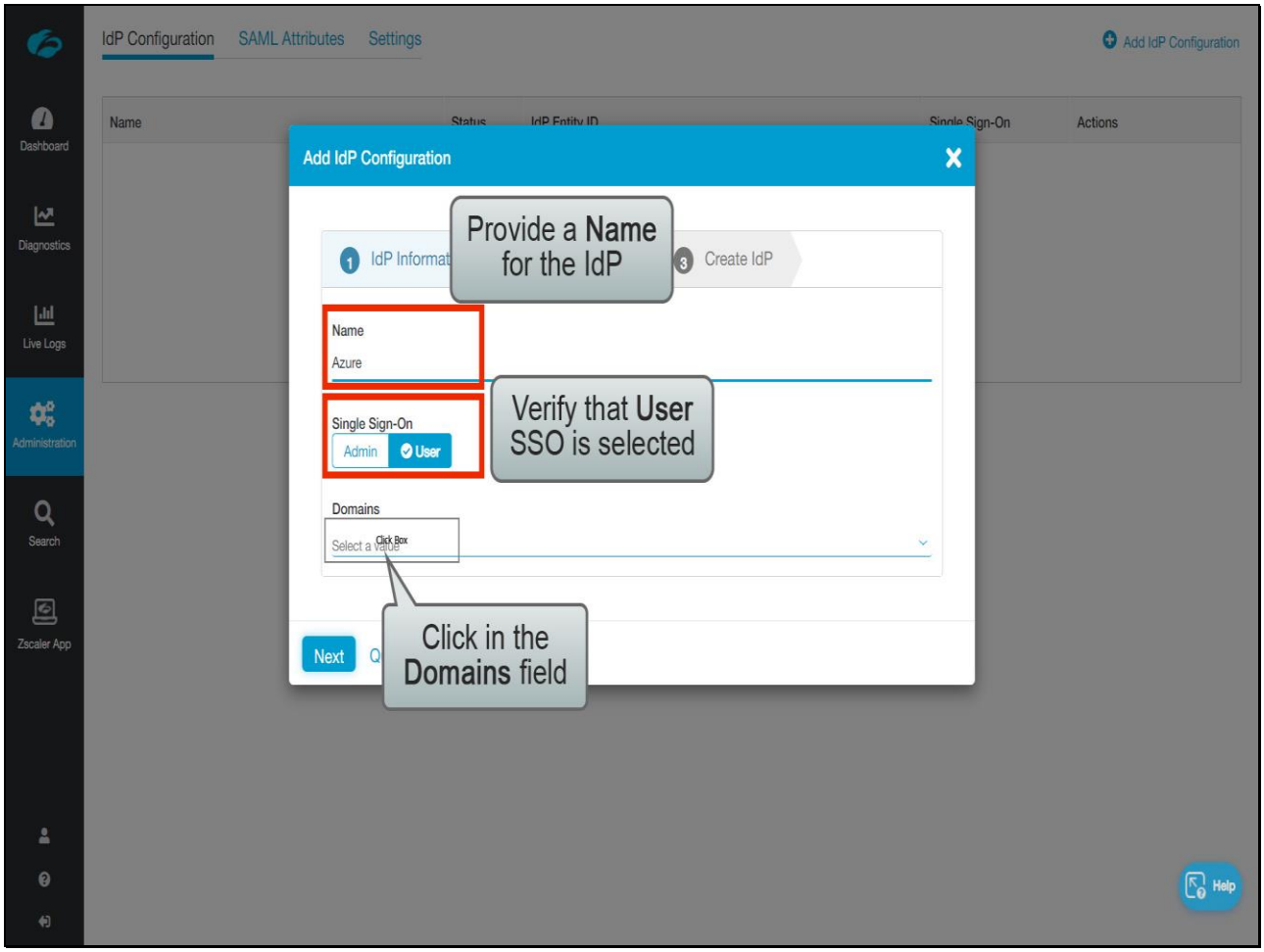


Slide notes

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

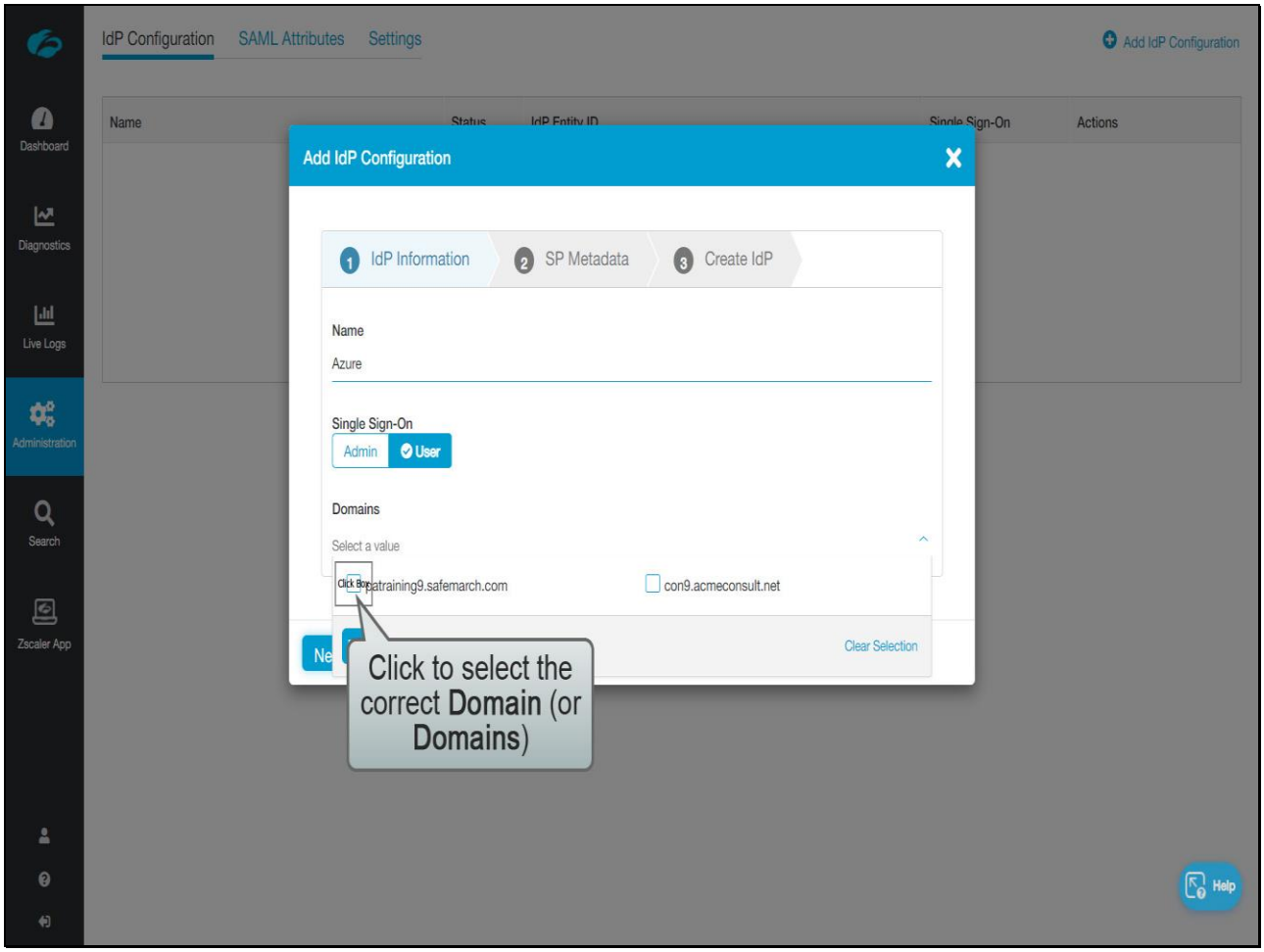


Slide notes

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, ...

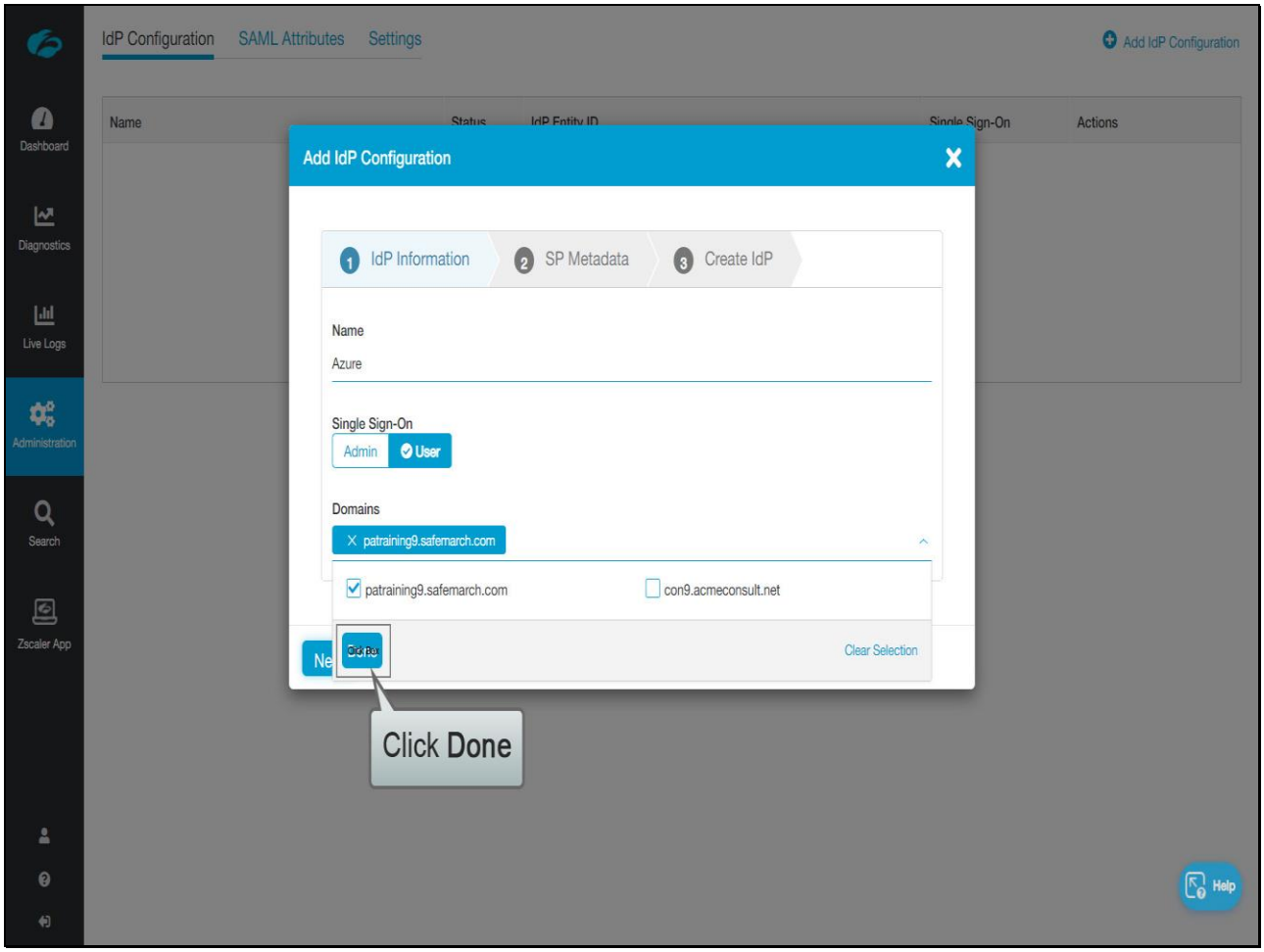
Slide 15 - Slide 15



Slide notes

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

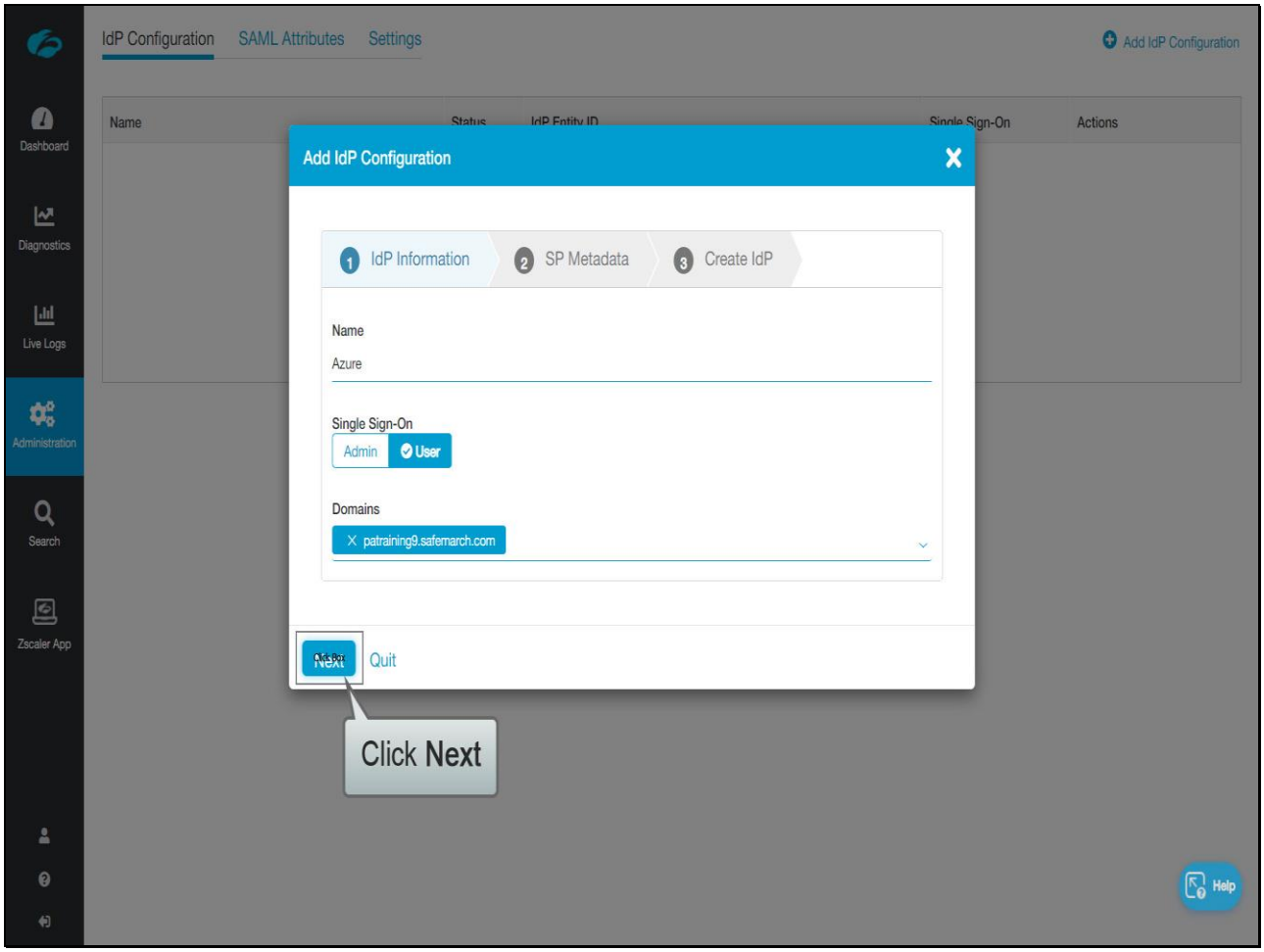
Slide 16 - Slide 16



Slide notes

...and click **Done**.

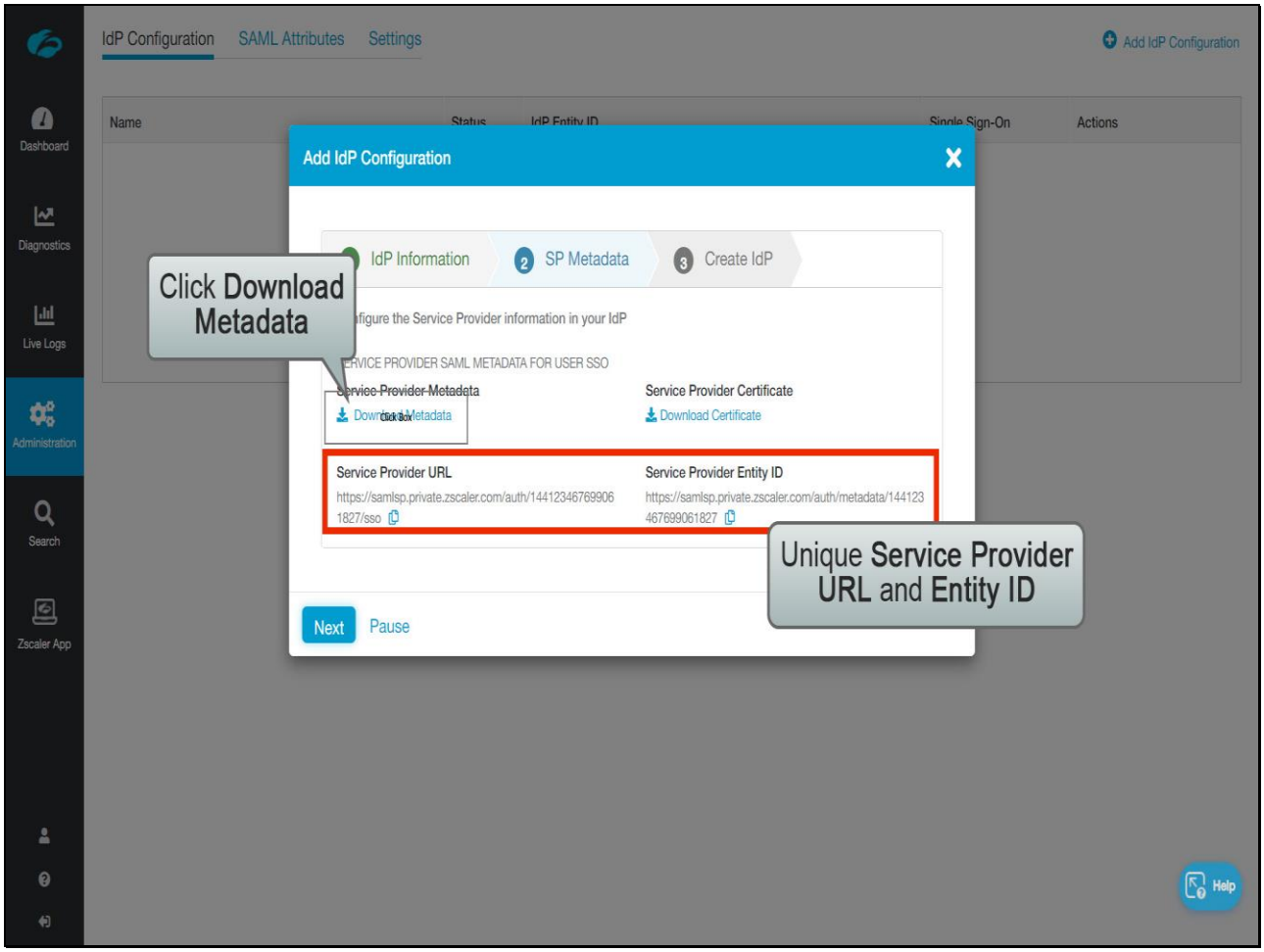
Slide 17 - Slide 17



Slide notes

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

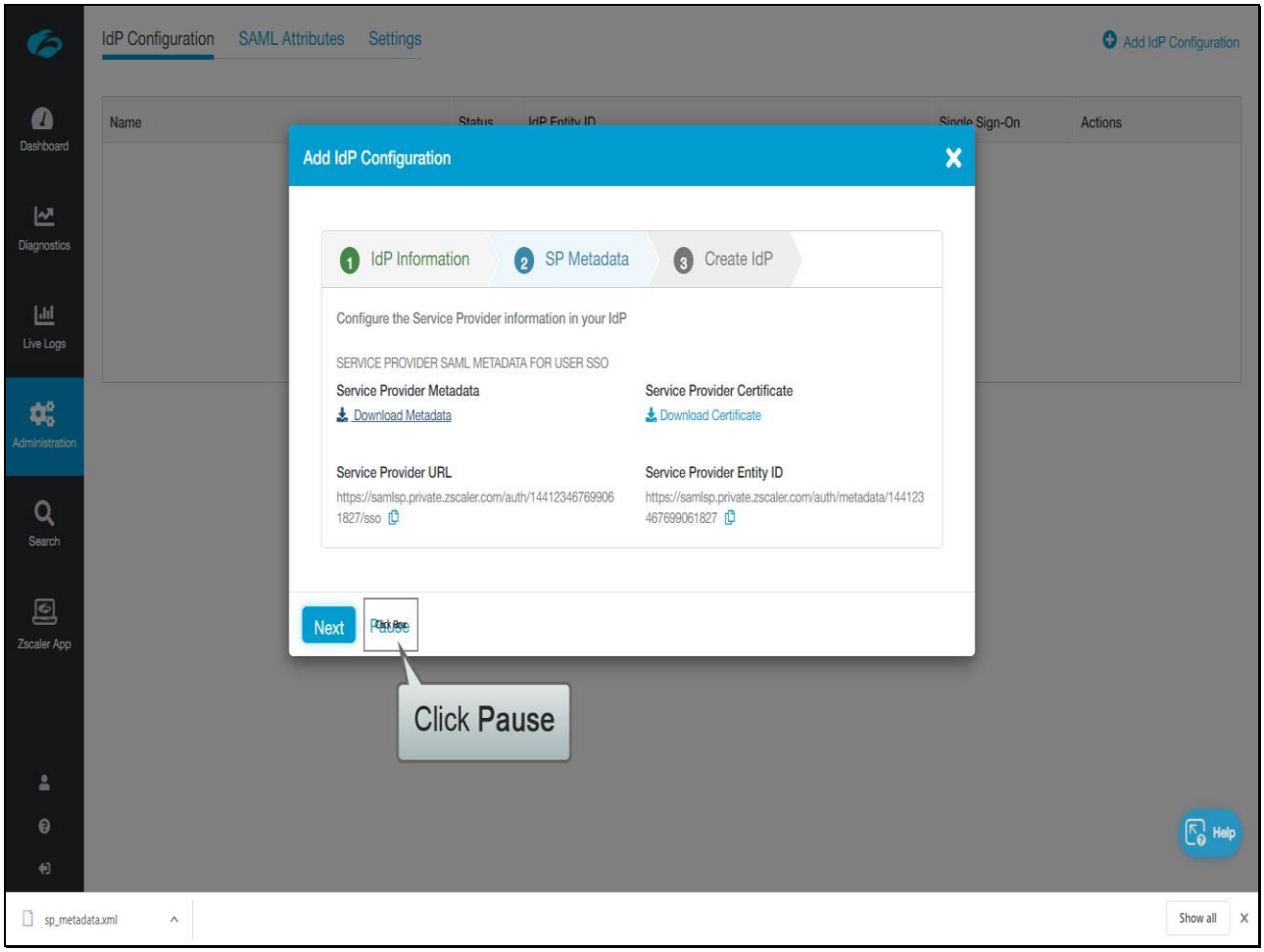
Slide 18 - Slide 18



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.

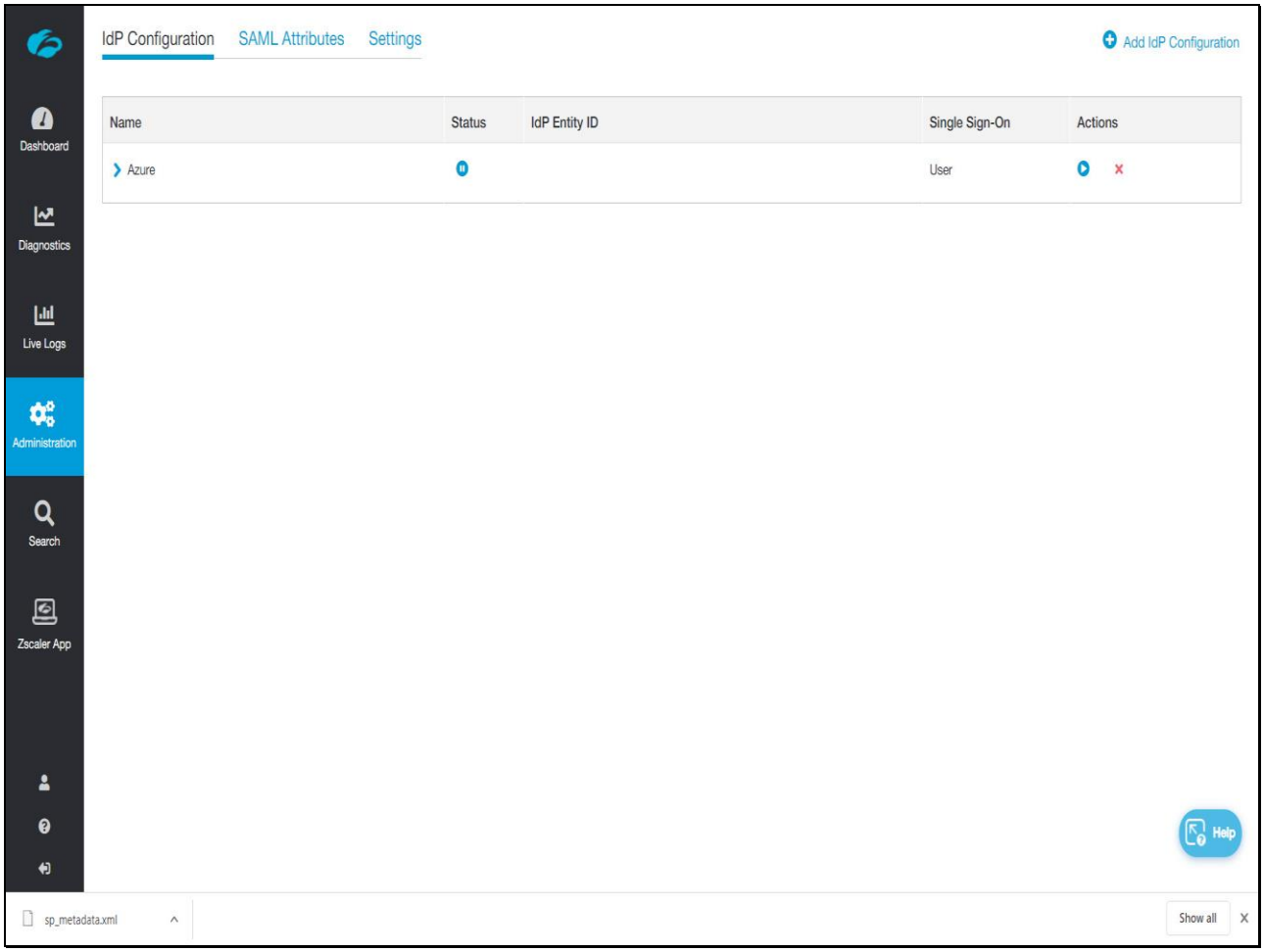
Slide 19 - Slide 19



Slide notes

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

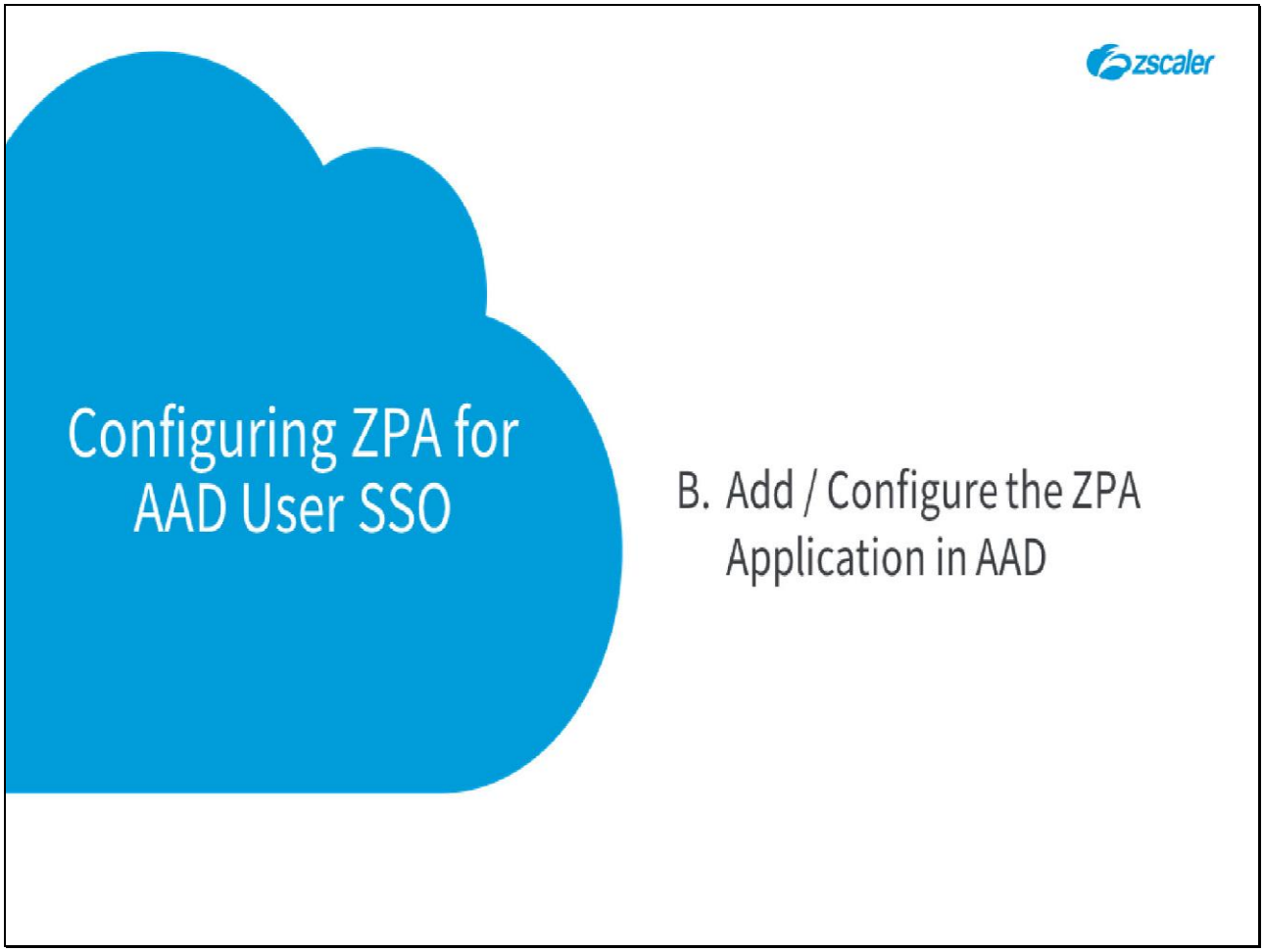
Slide 20 - Slide 20



Slide notes

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

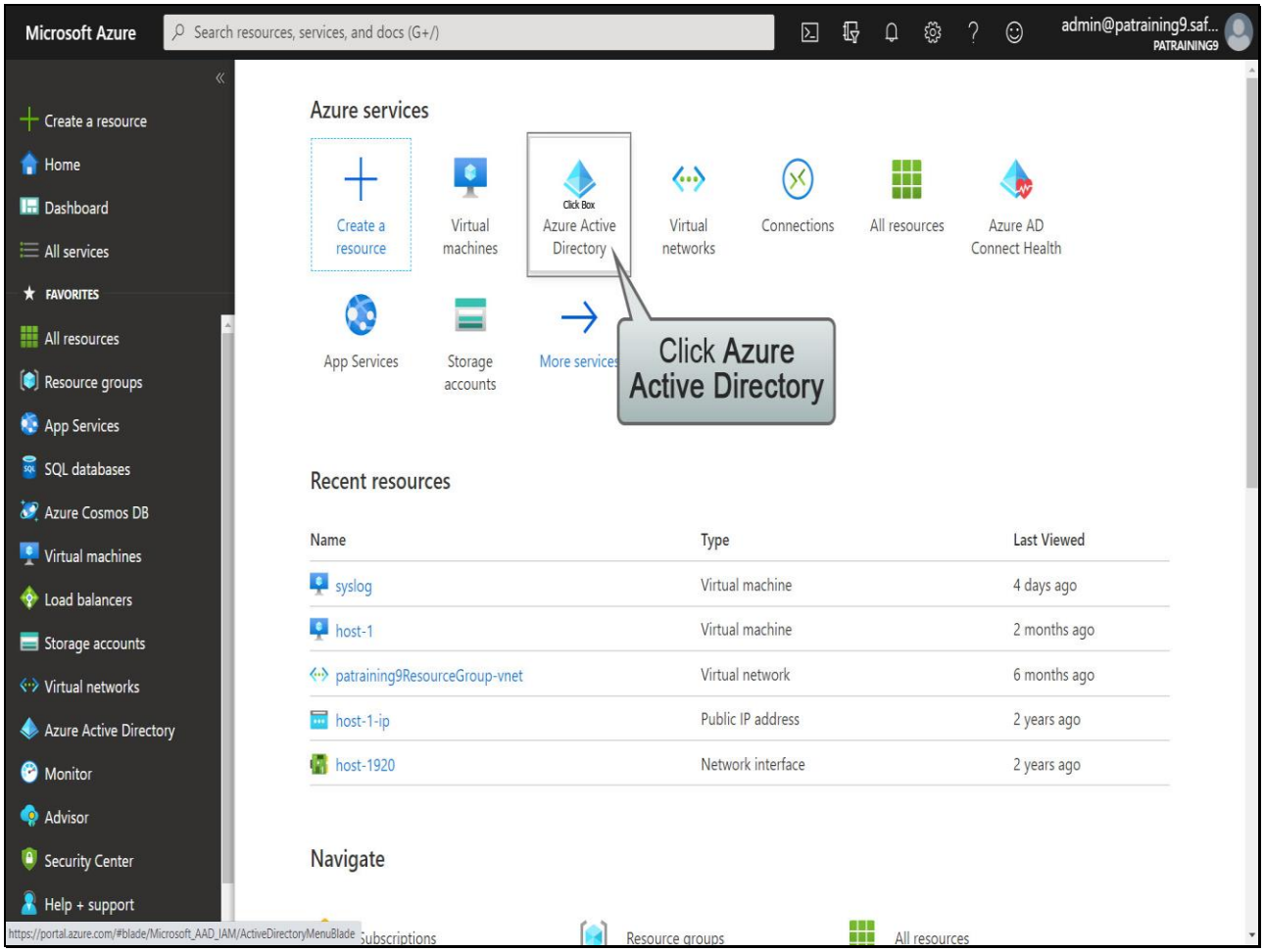
Slide 21 - Configuring ZPA for Okta User SSO



Slide notes

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

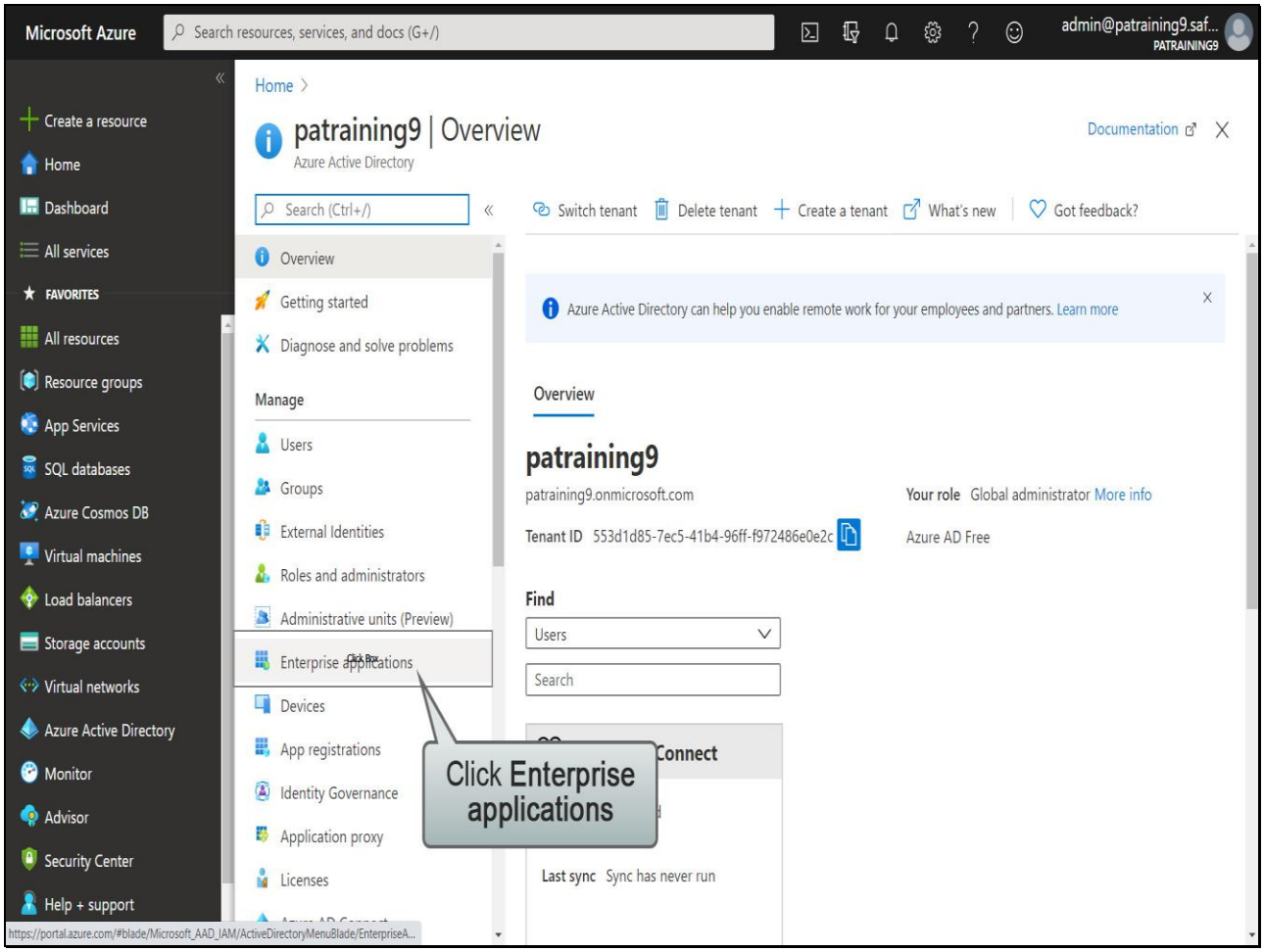
Slide 22 - Slide 22



Slide notes

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

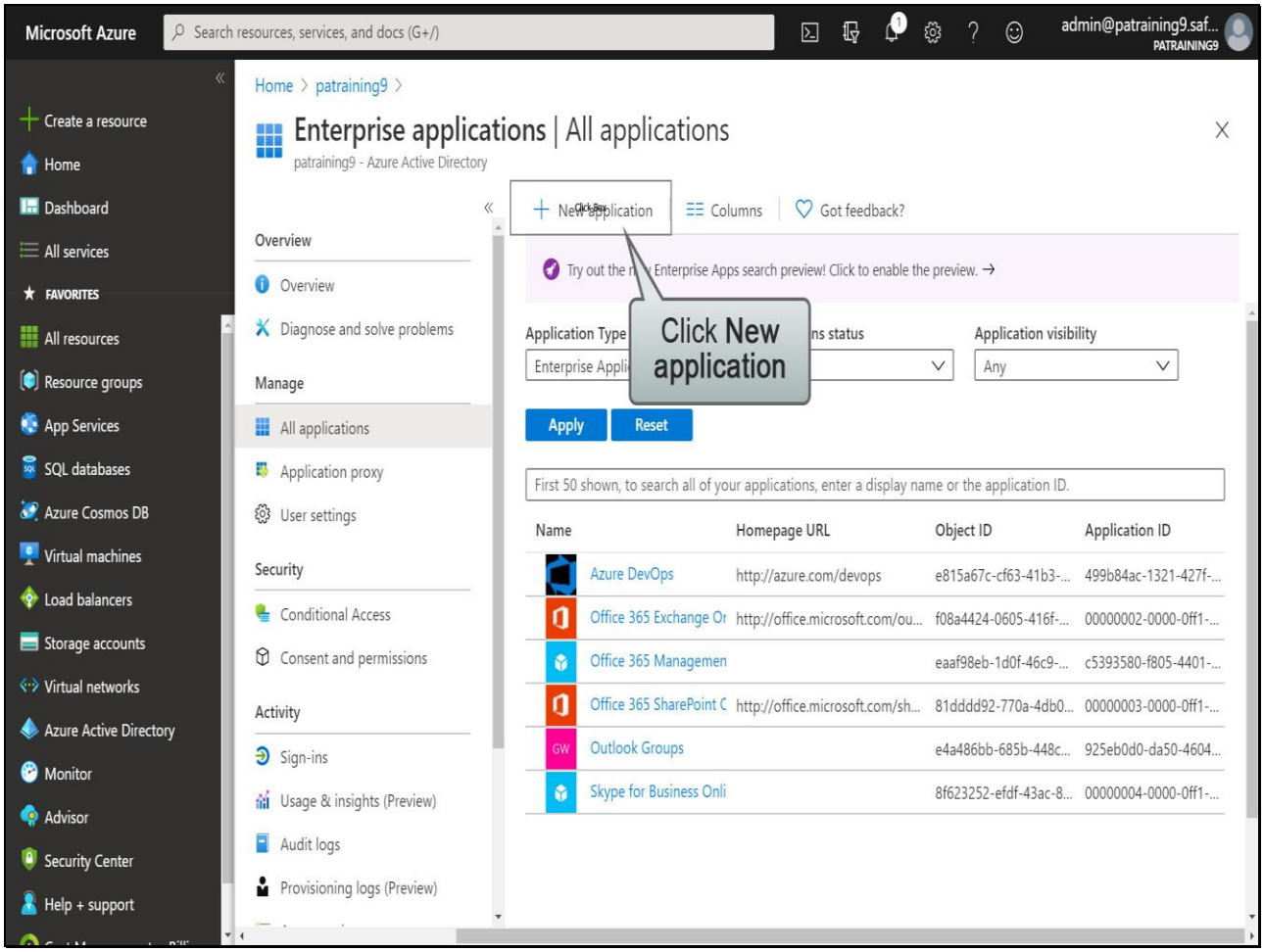
Slide 23 - Slide 23



Slide notes

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

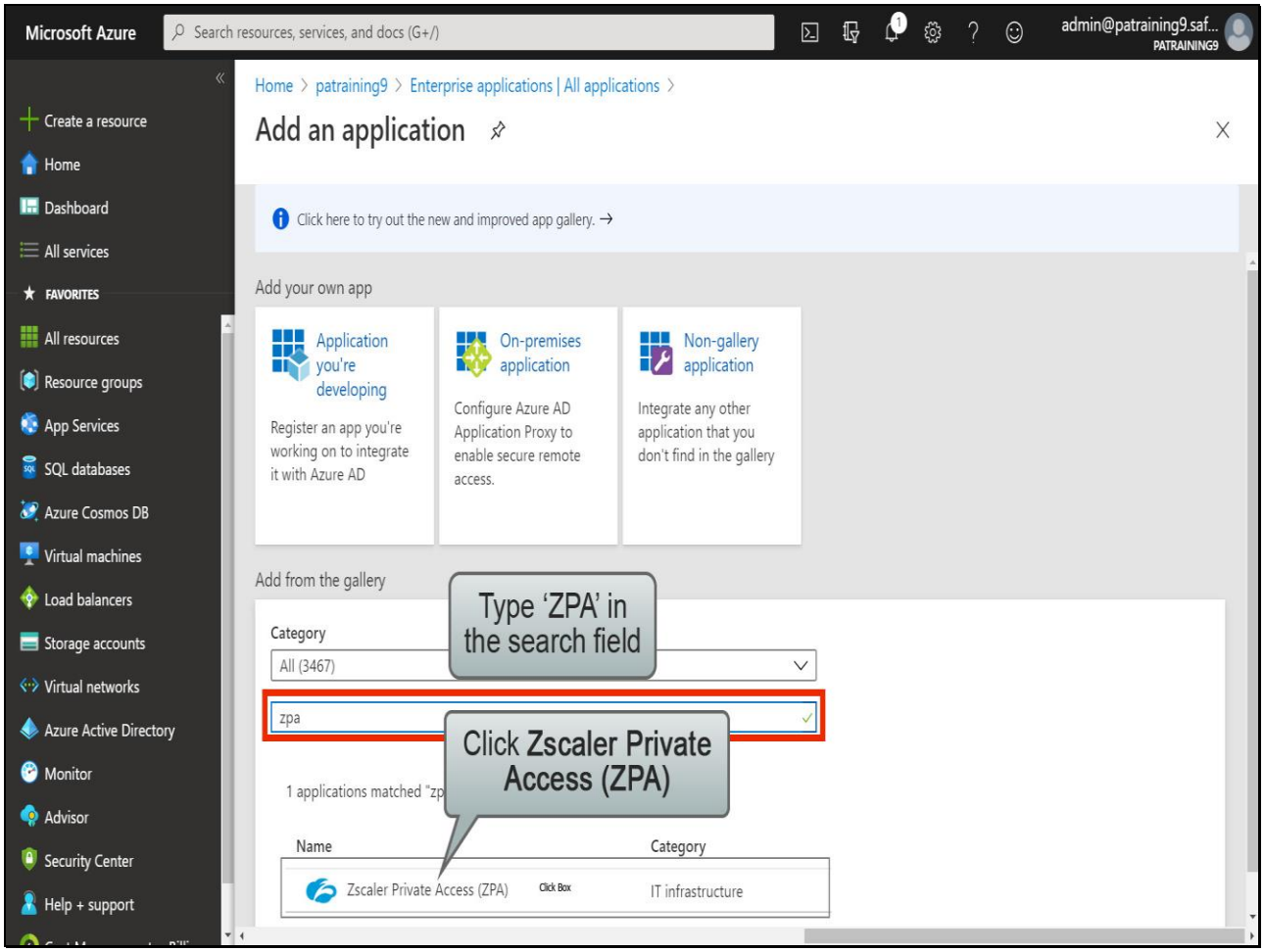
Slide 24 - Slide 24



Slide notes

...and click **New application**.

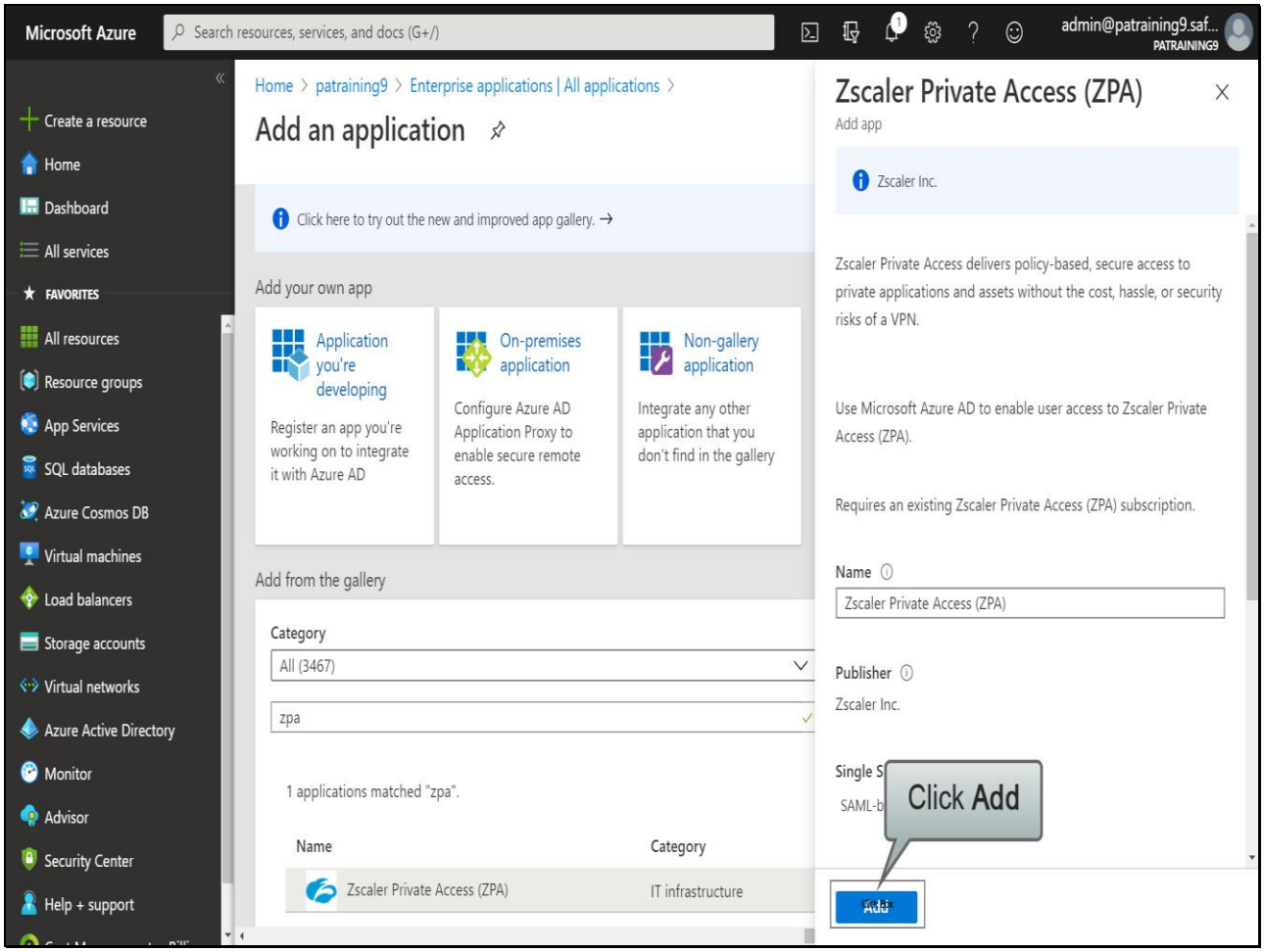
Slide 25 - Slide 25



Slide notes

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

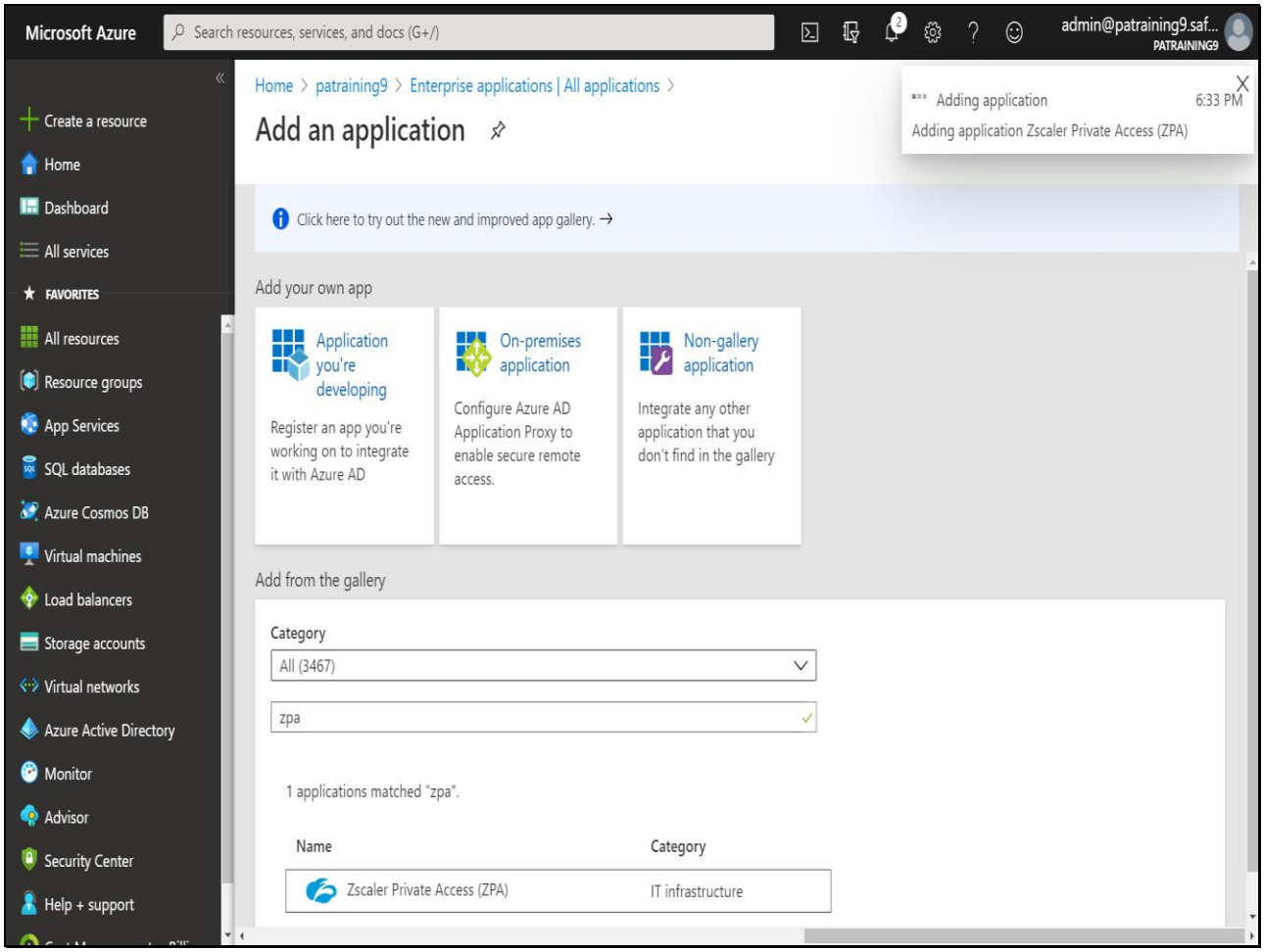
Slide 26 - Slide 26



Slide notes

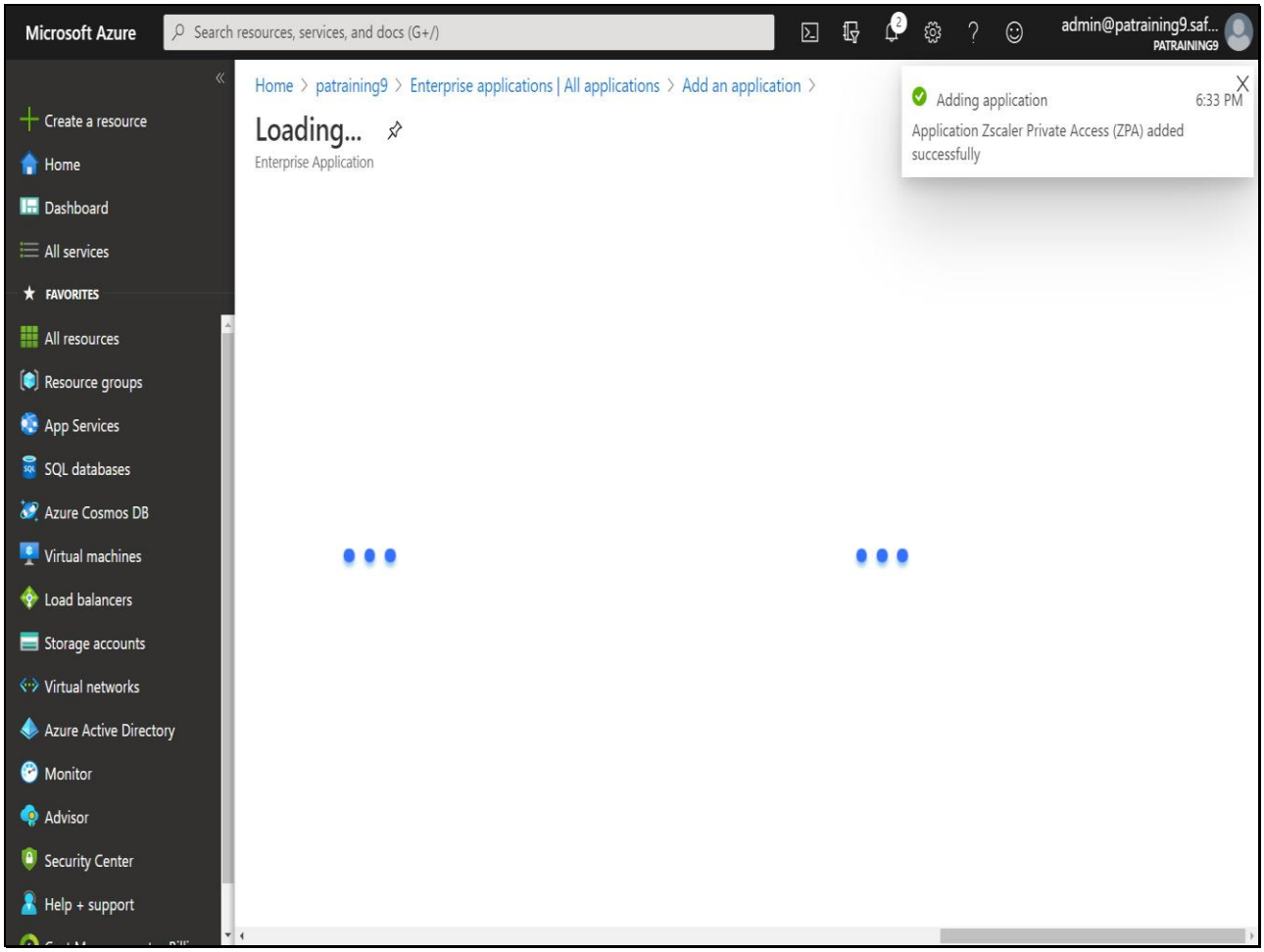
…and click **Add**.

Slide 27 - Slide 27



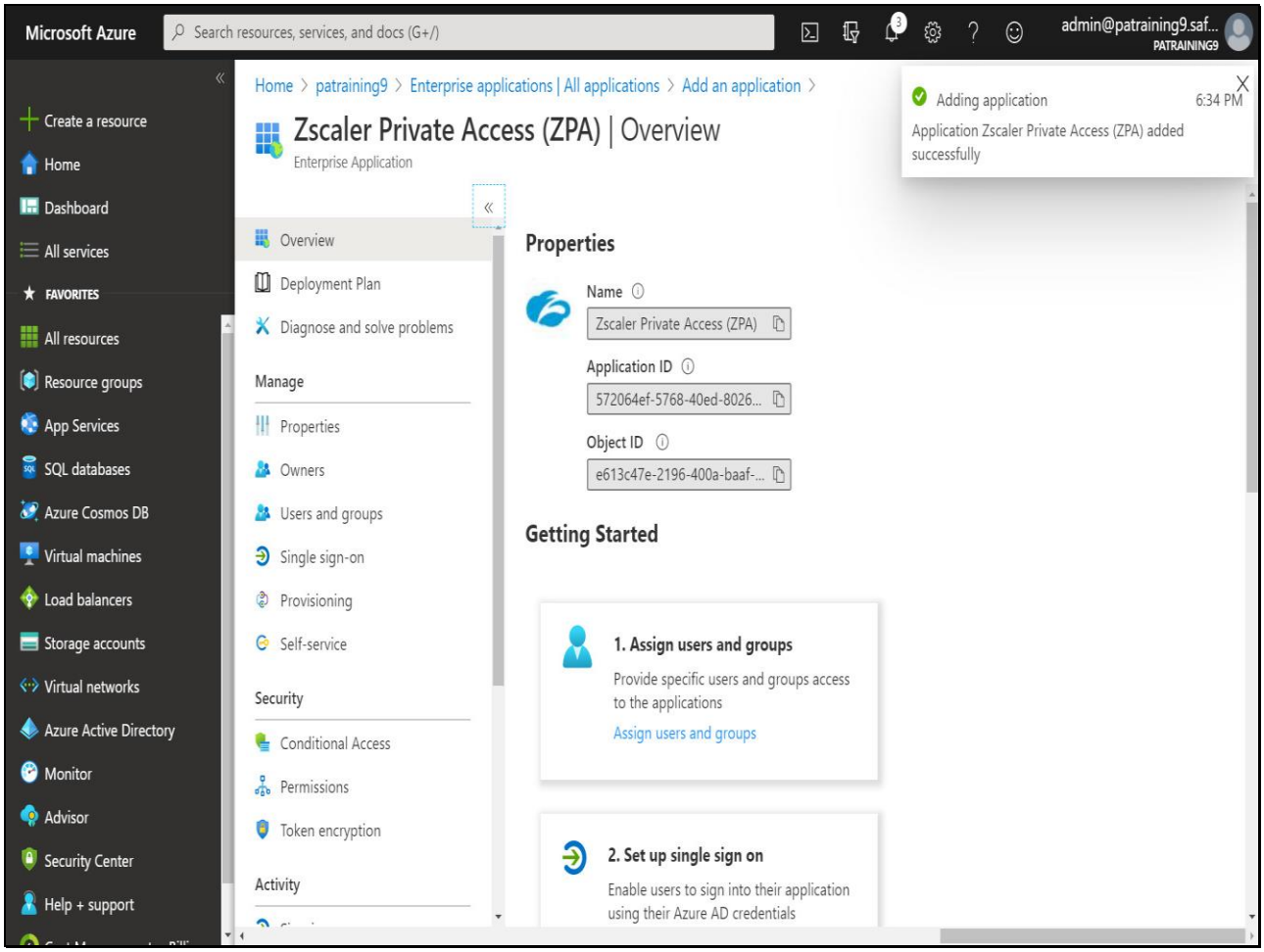
Slide notes

Slide 28 - Slide 28



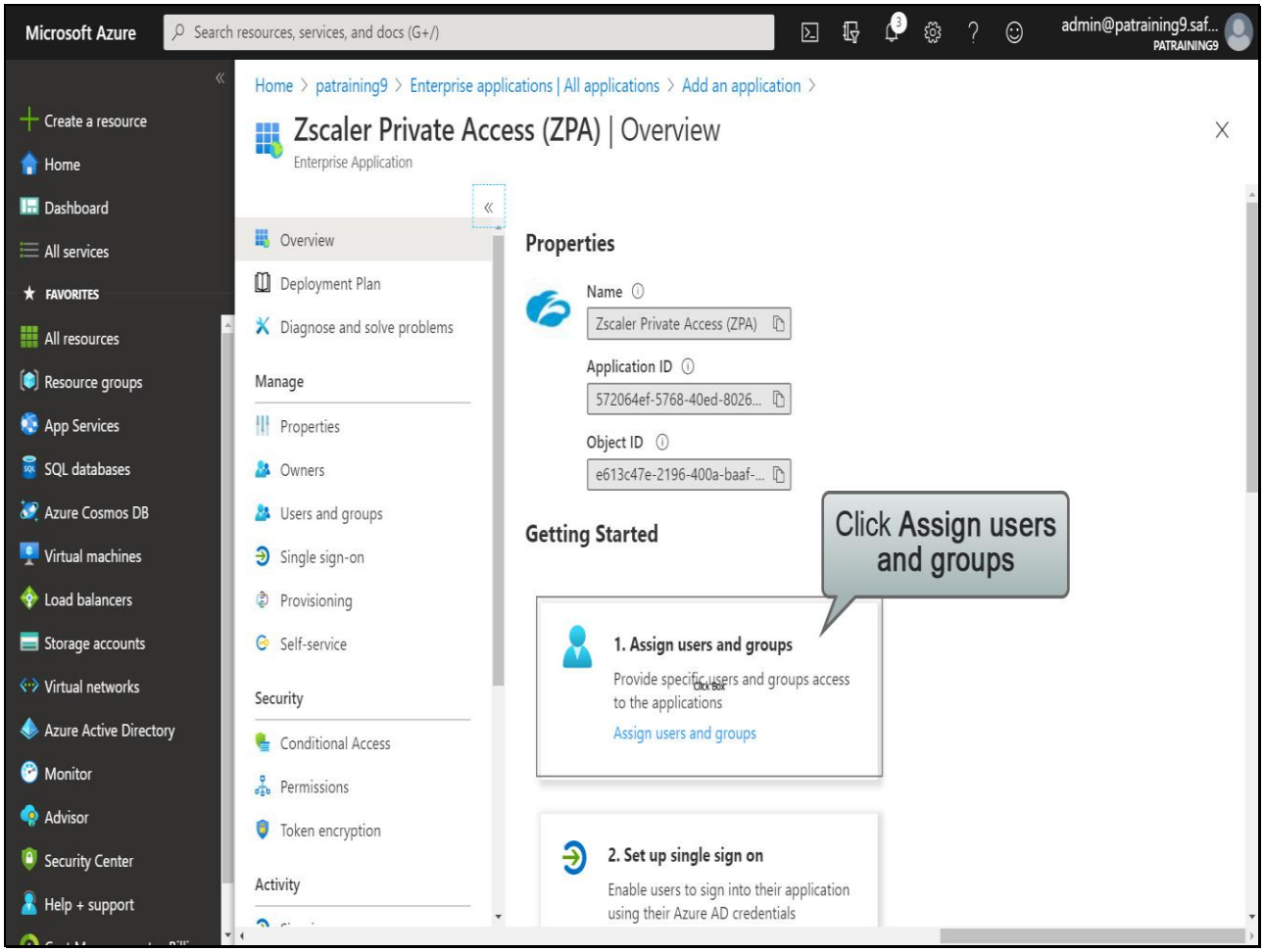
Slide notes

Slide 29 - Slide 29



Slide notes

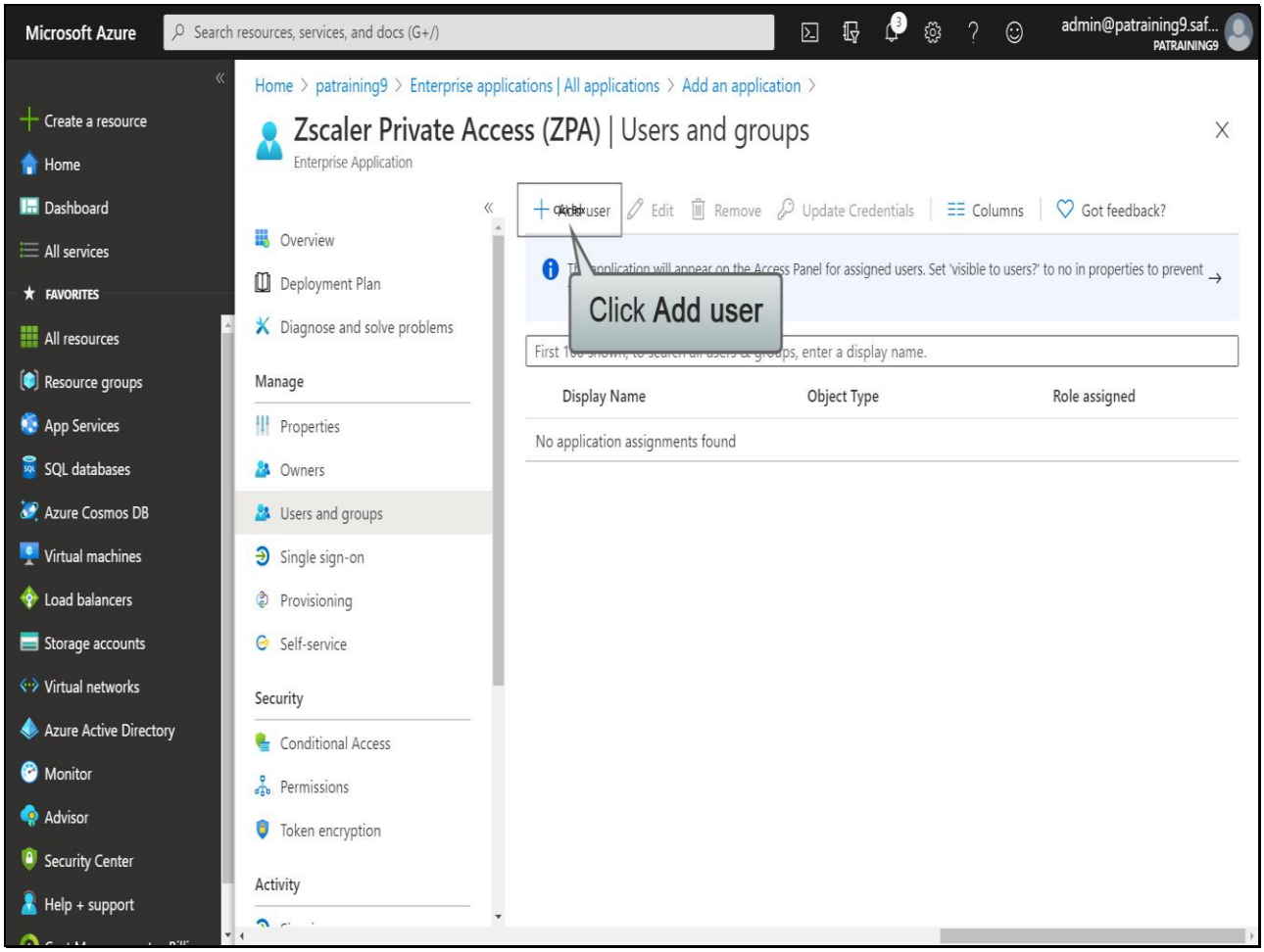
Slide 30 - Slide 30



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.

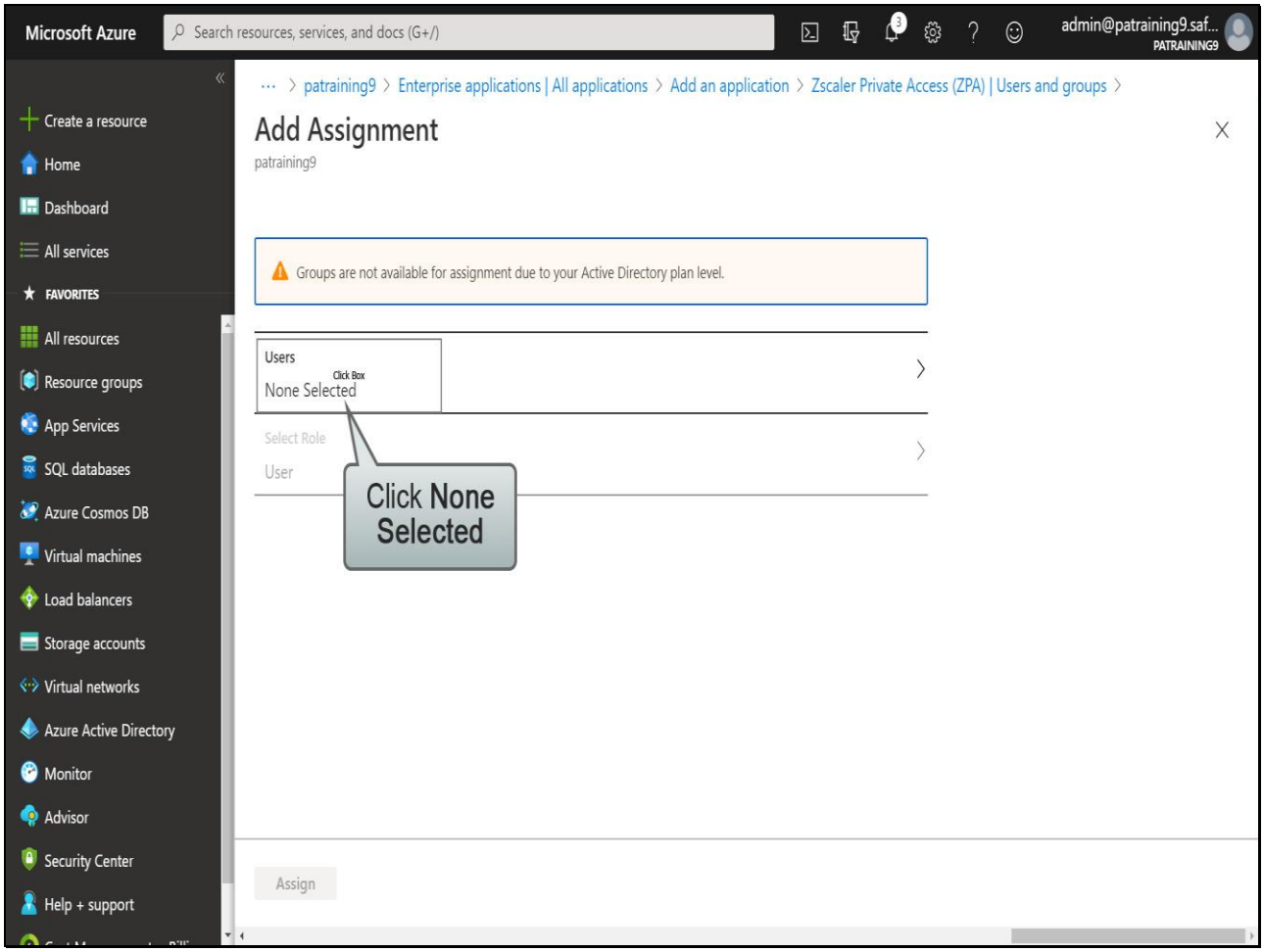
Slide 31 - Slide 31



Slide notes

Click **Add user**, ...

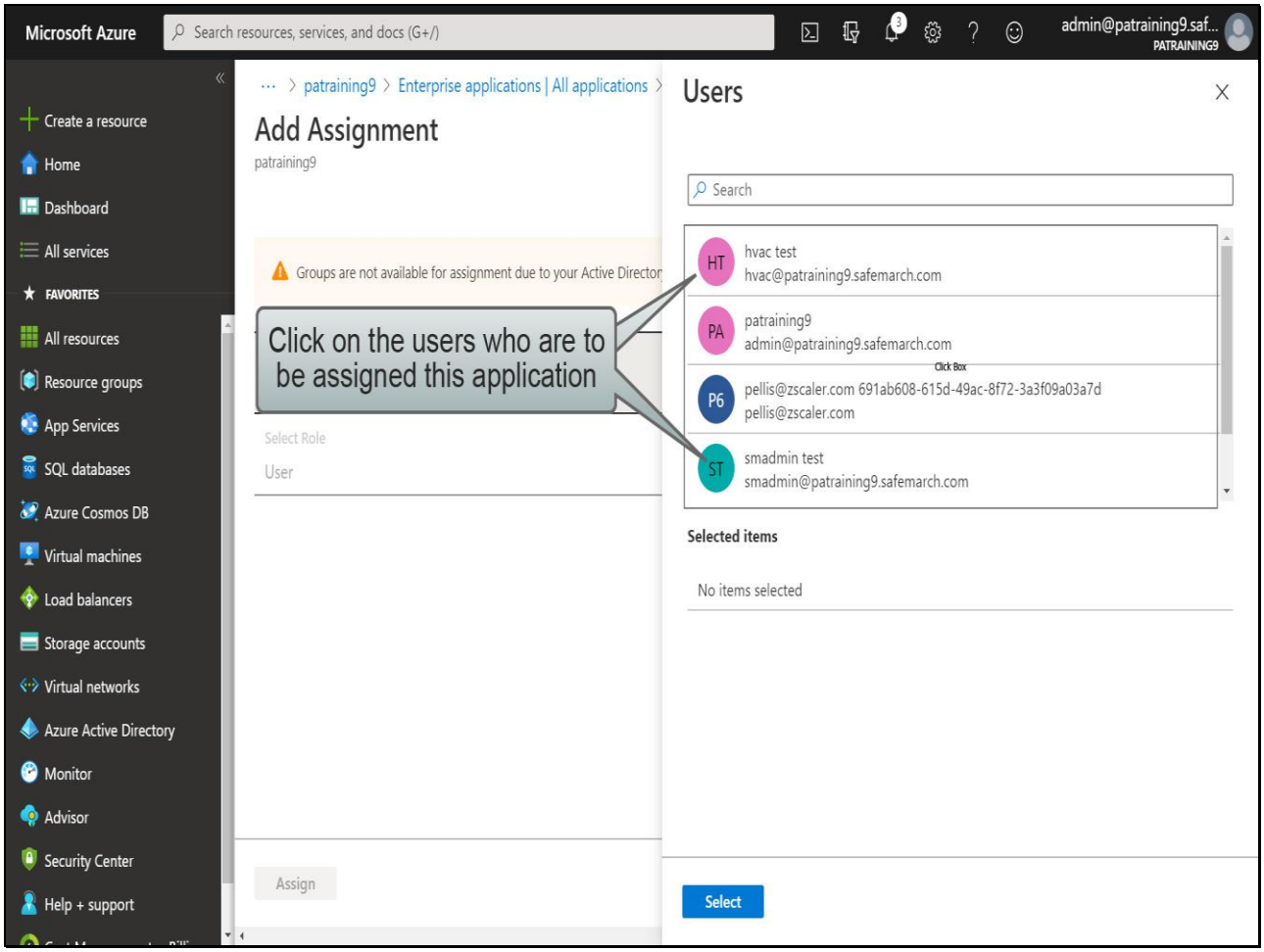
Slide 32 - Slide 32



Slide notes

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

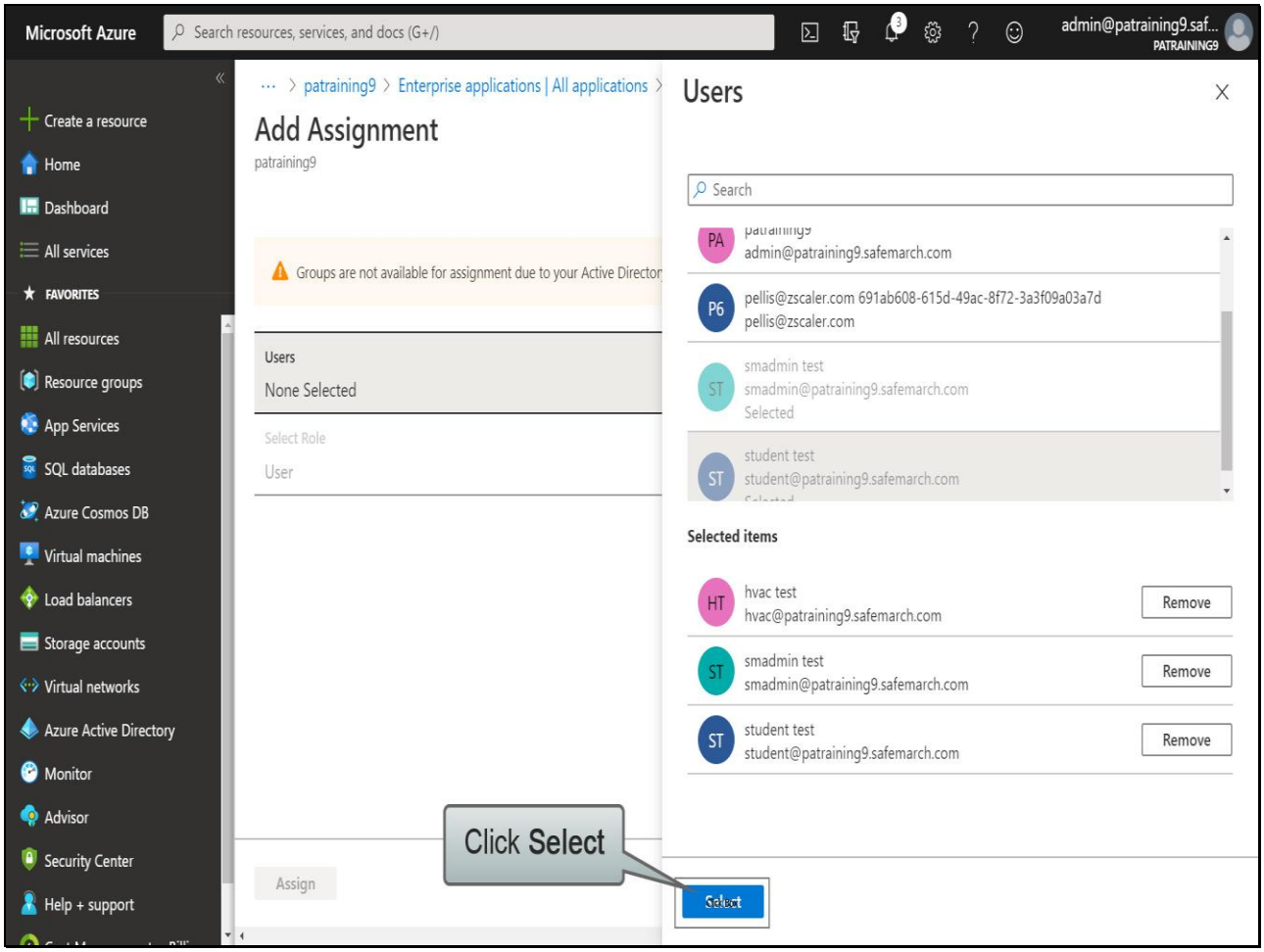
Slide 33 - Slide 33



Slide notes

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

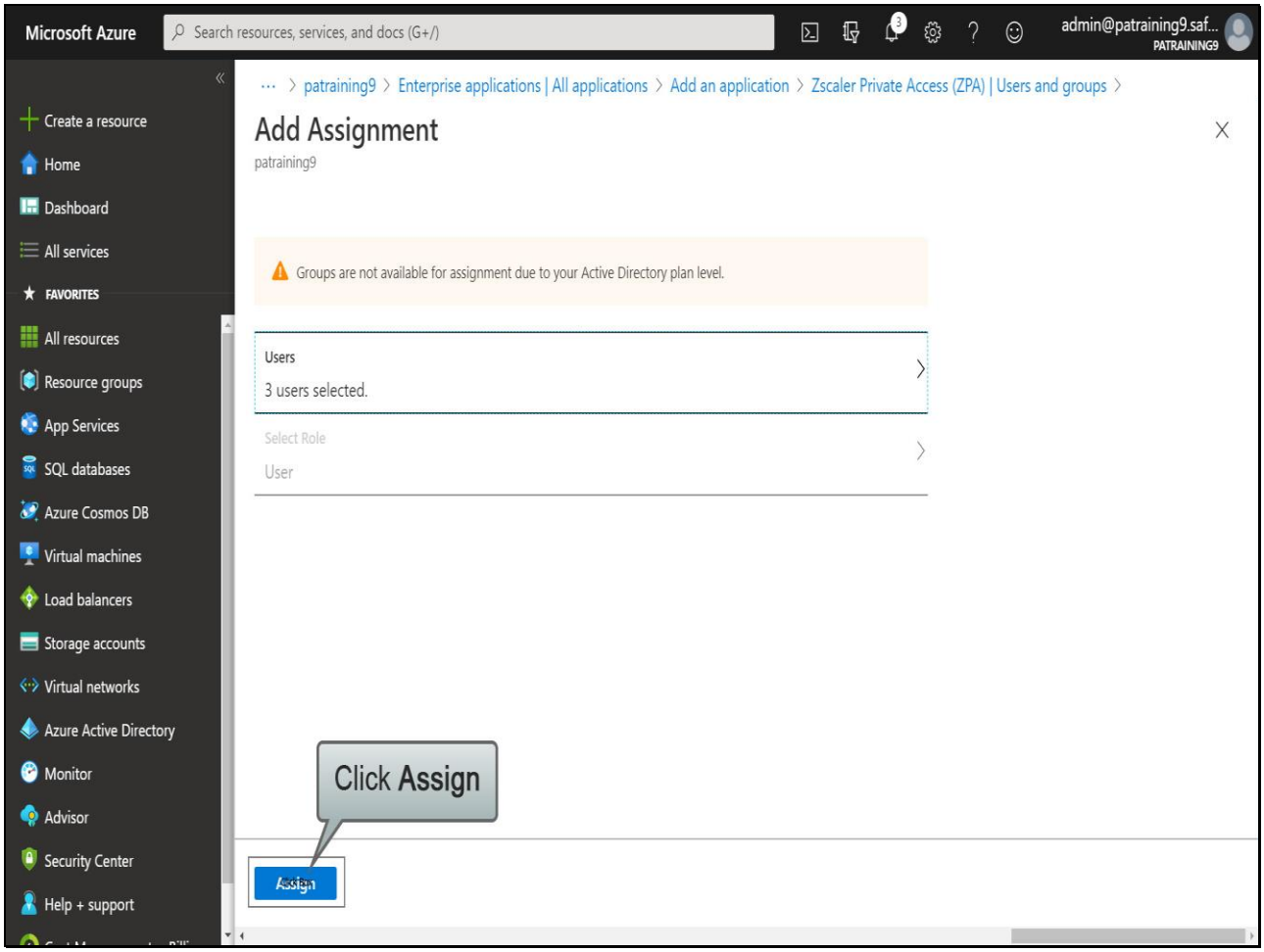
Slide 34 - Slide 34



Slide notes

...then click **Select**.

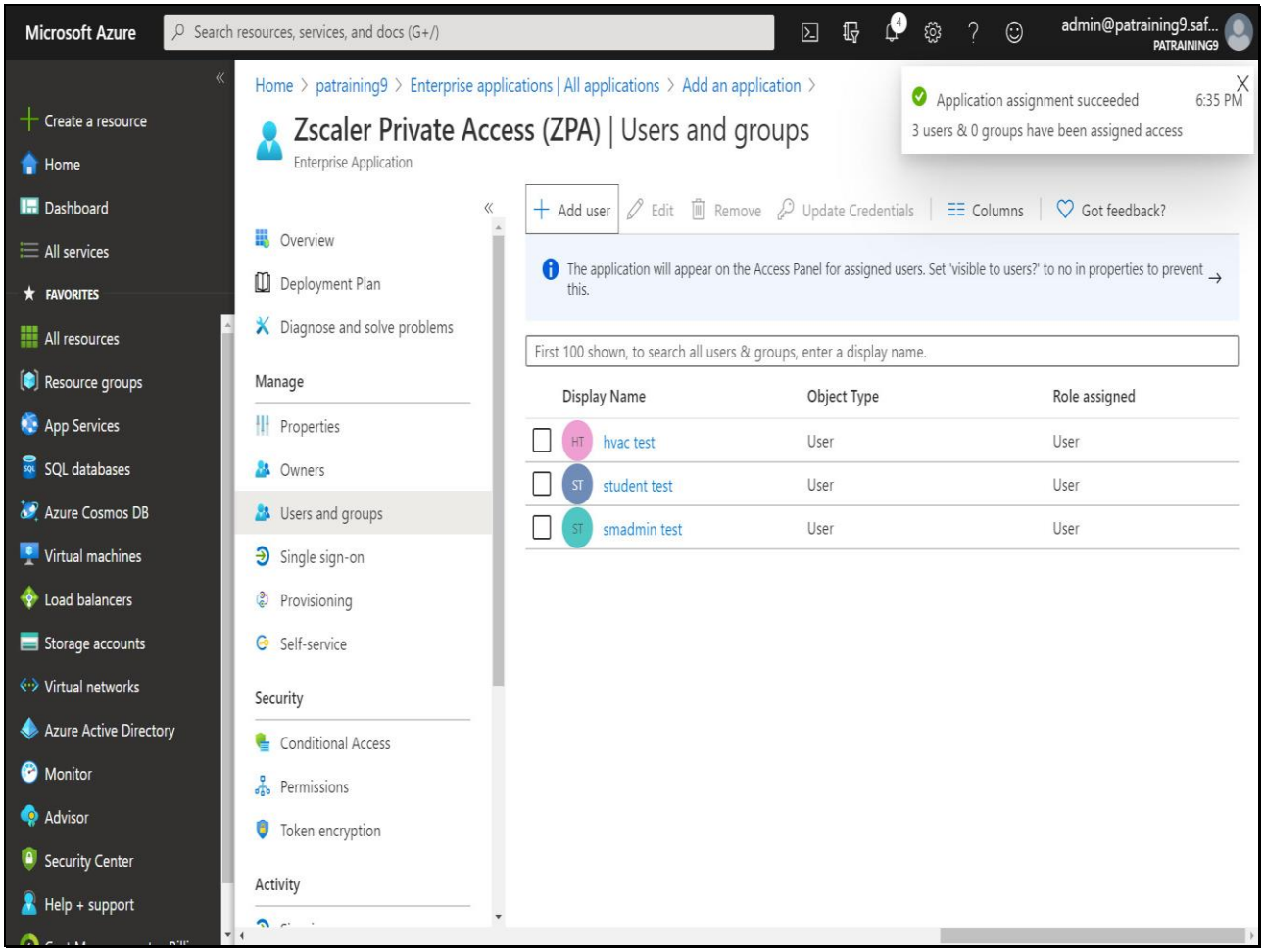
Slide 35 - Slide 35



Slide notes

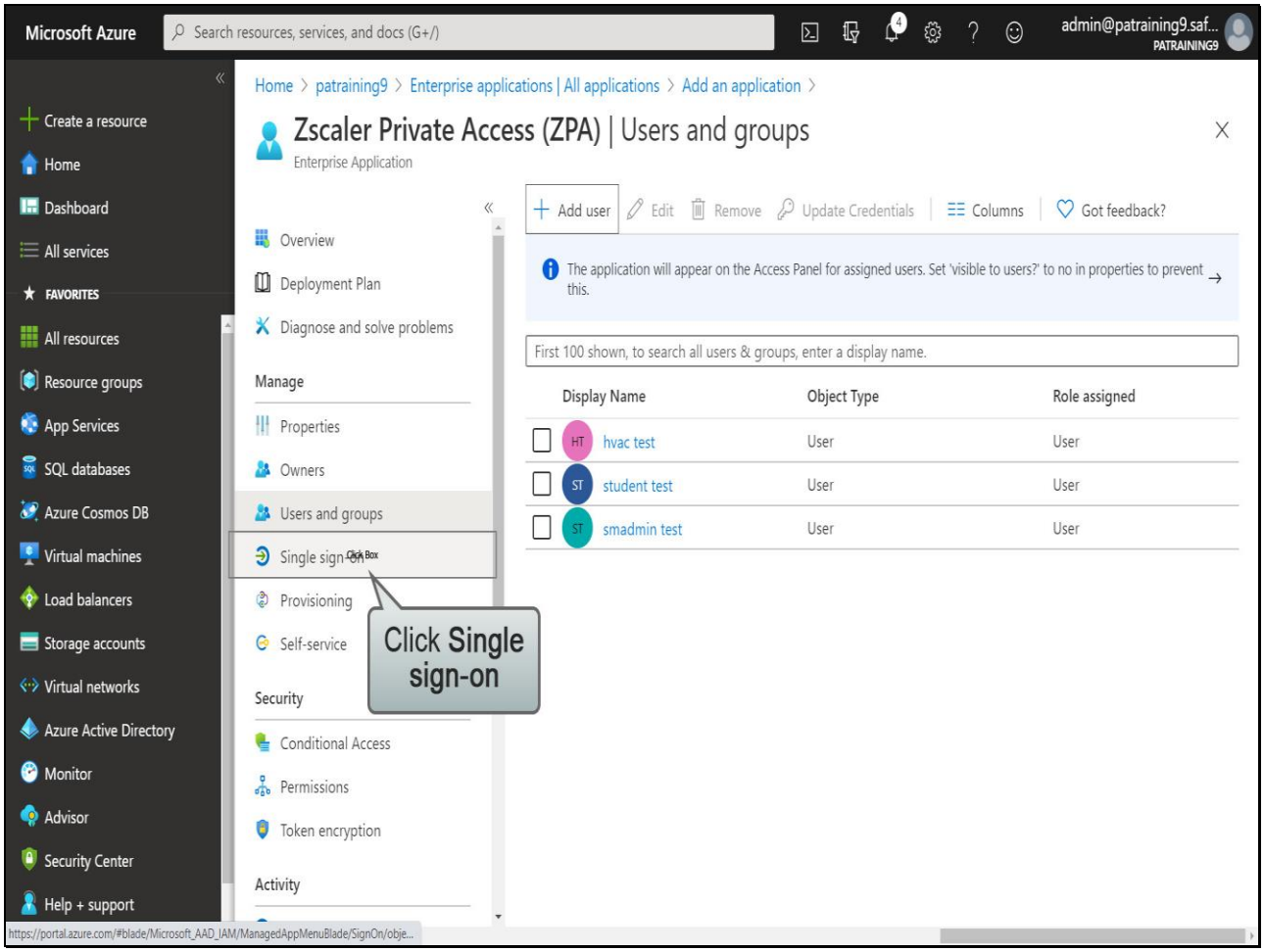
To assign the selected user to the application, click **Assign**.

Slide 36 - Slide 36



Slide notes

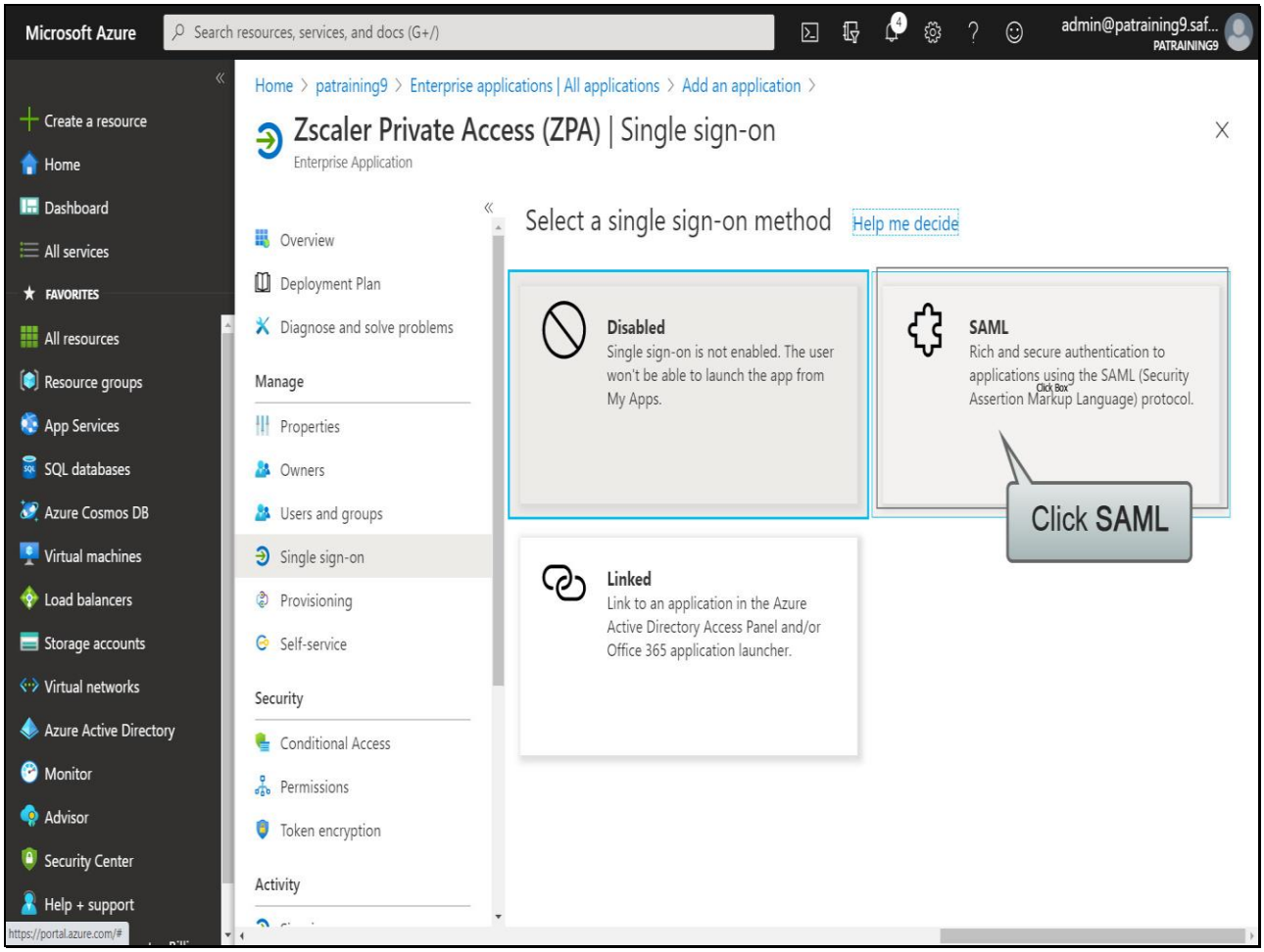
Slide 37 - Slide 37



Slide notes

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

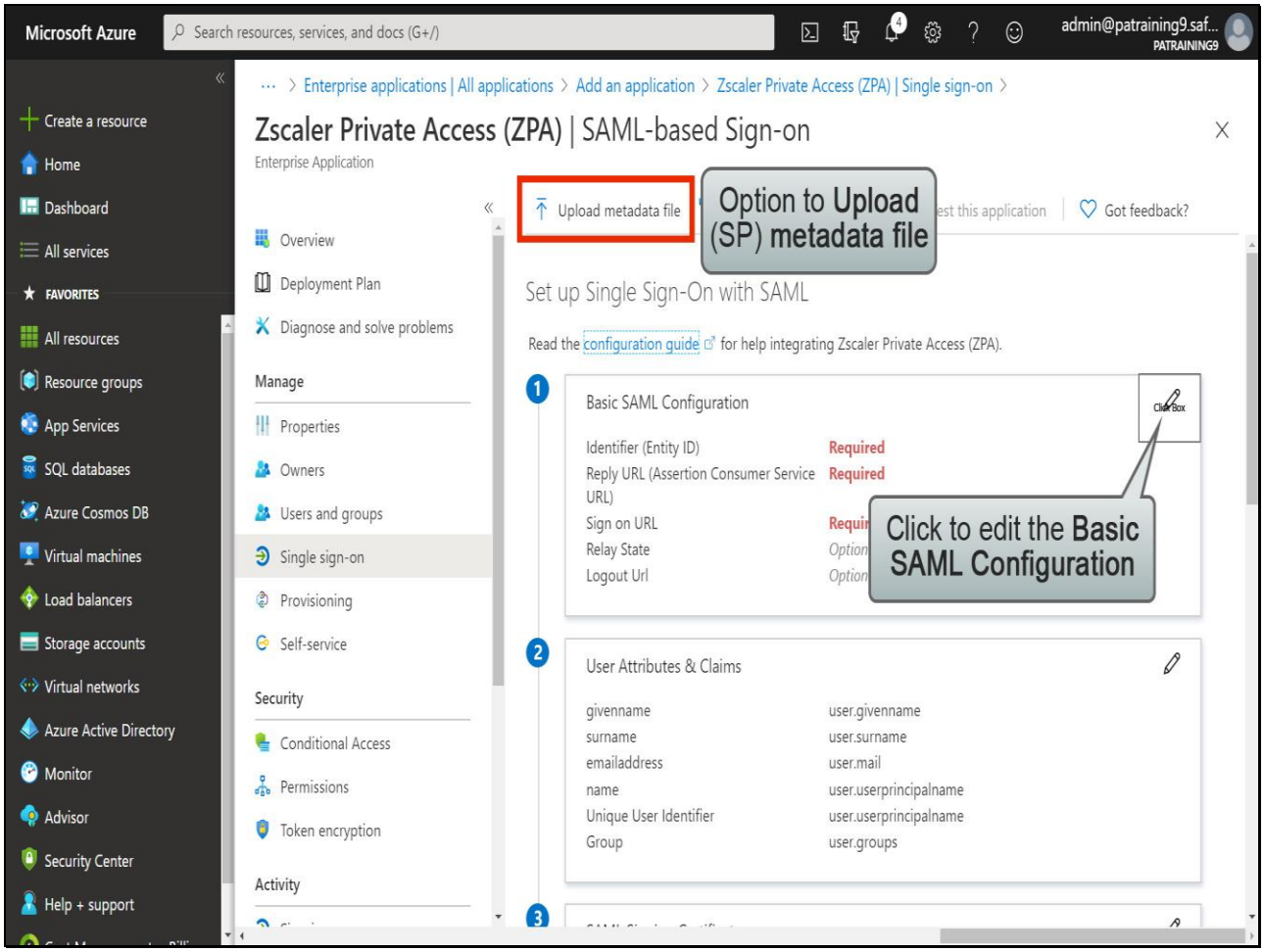
Slide 38 - Slide 38



Slide notes

...then click the **SAML** box.

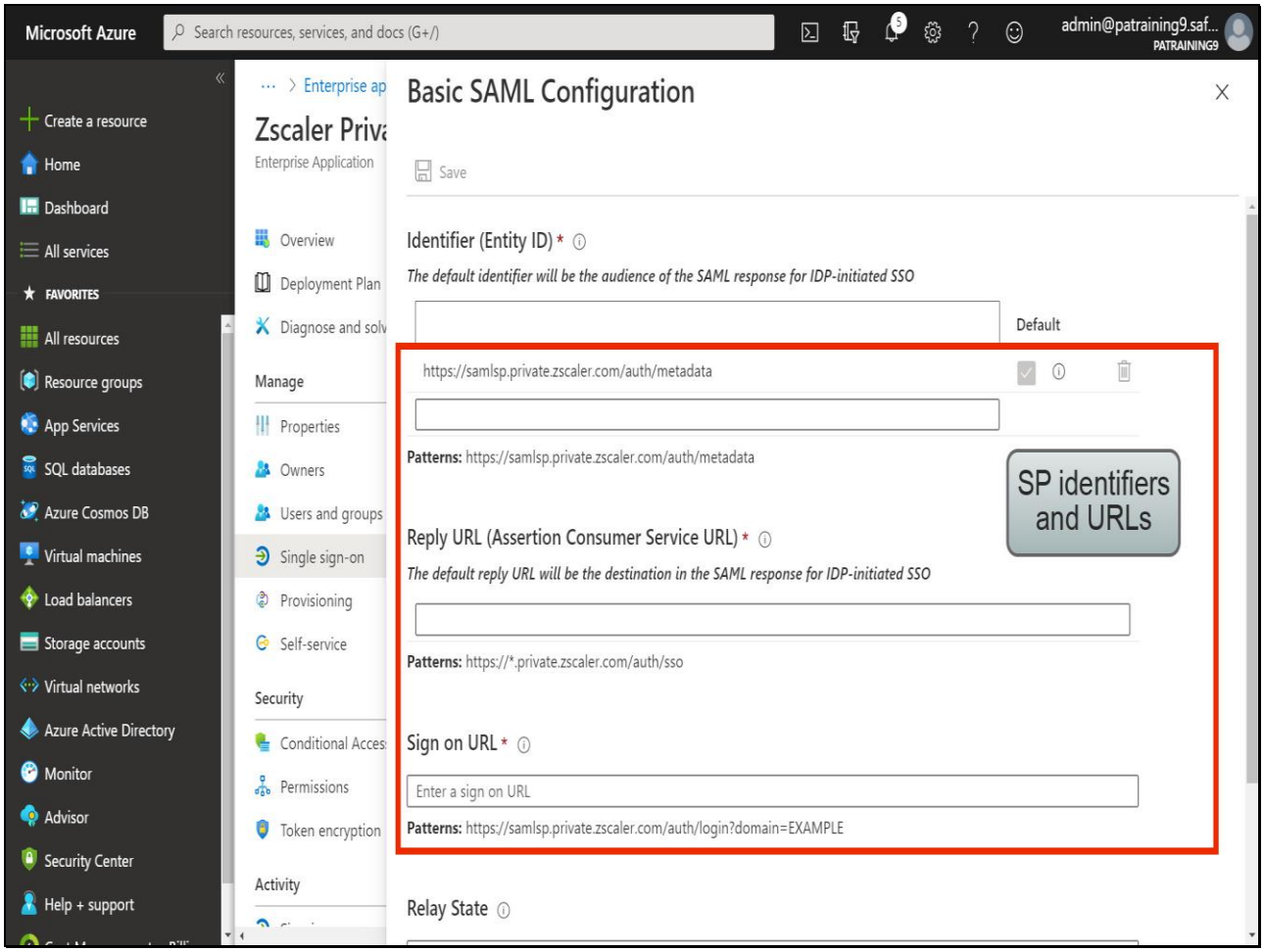
Slide 39 - Slide 39



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**.

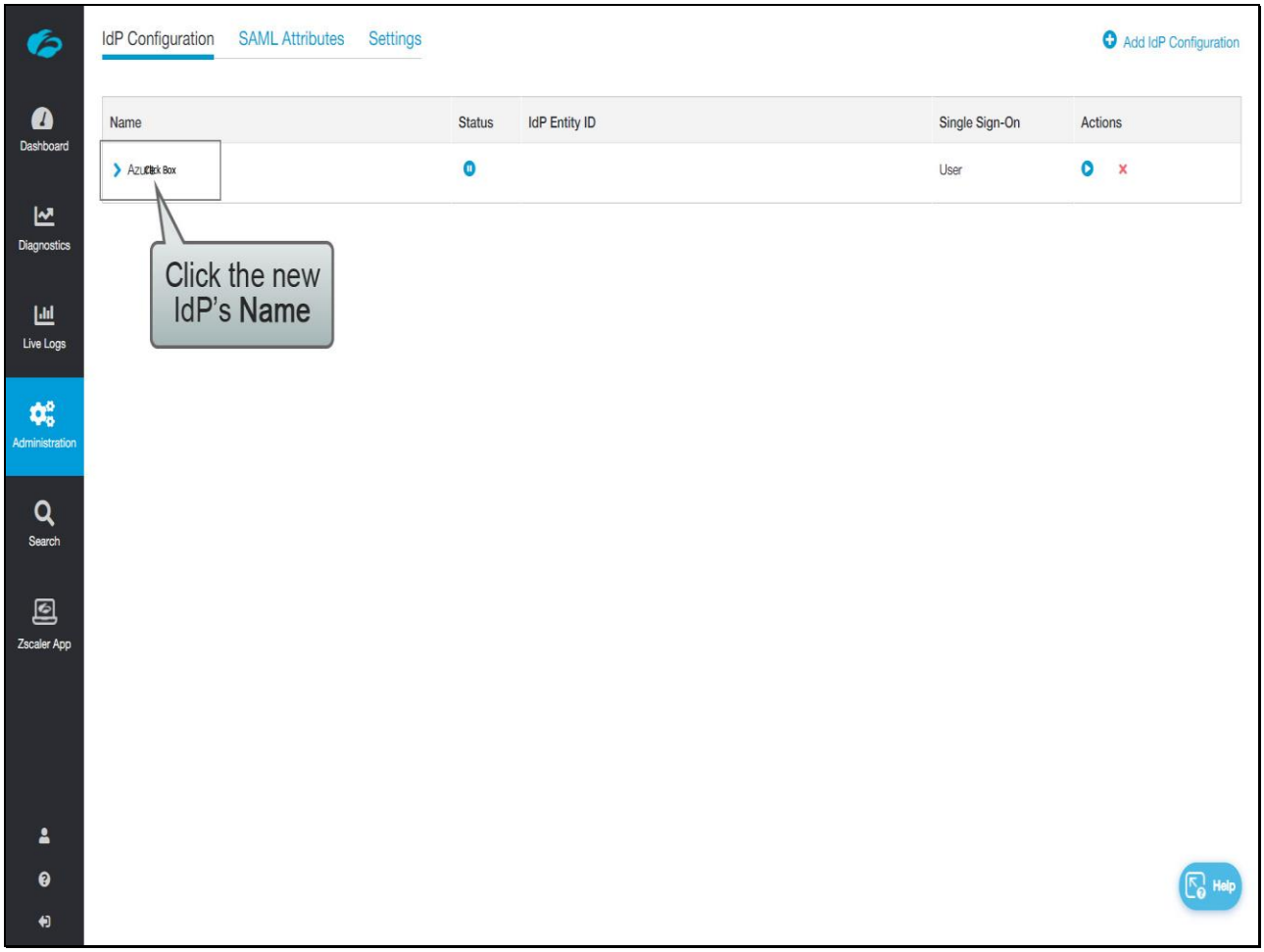
Slide 40 - Slide 40



Slide notes

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

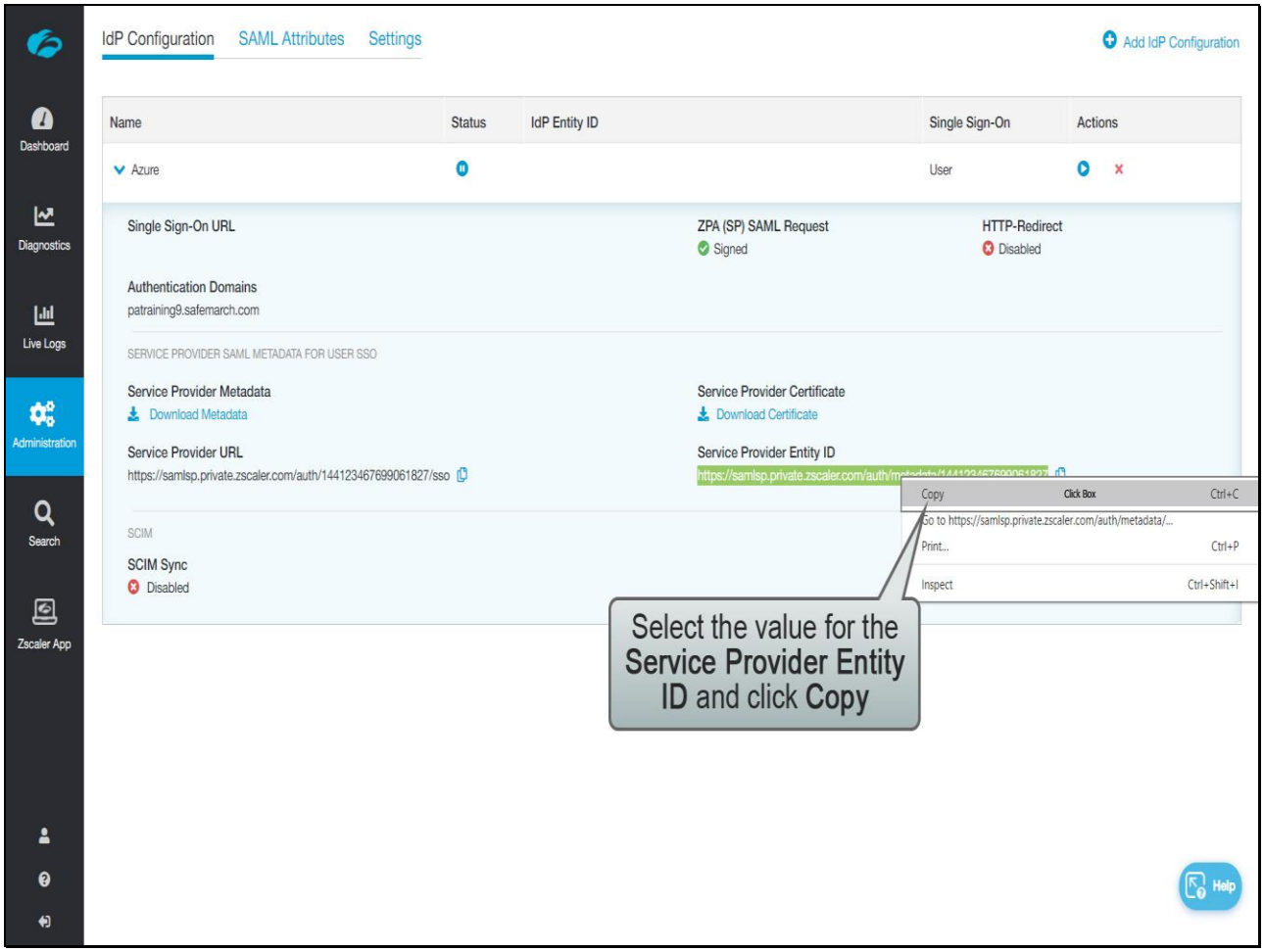
Slide 41 - Slide 41



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.

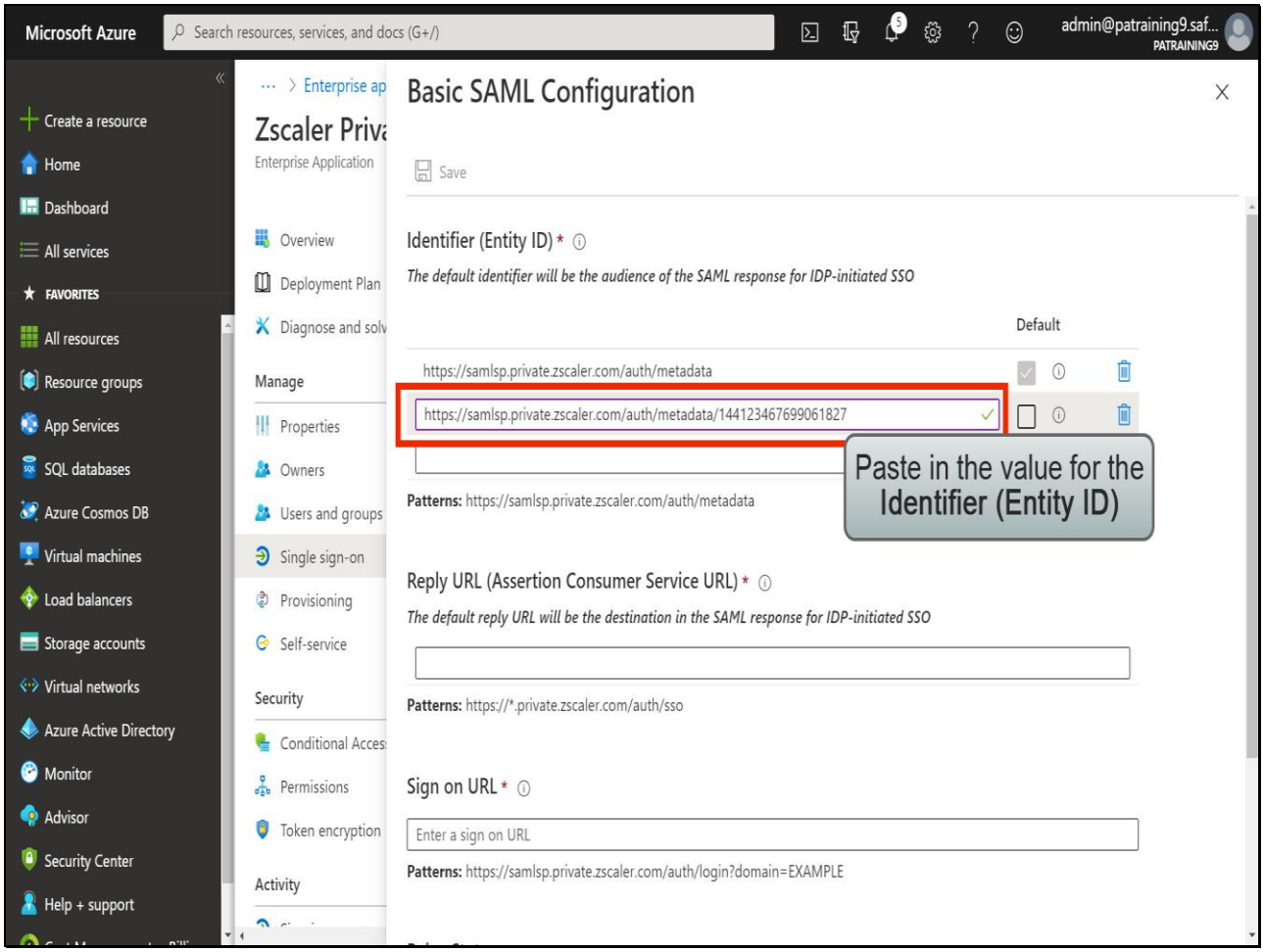
Slide 42 - Slide 42



Slide notes

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

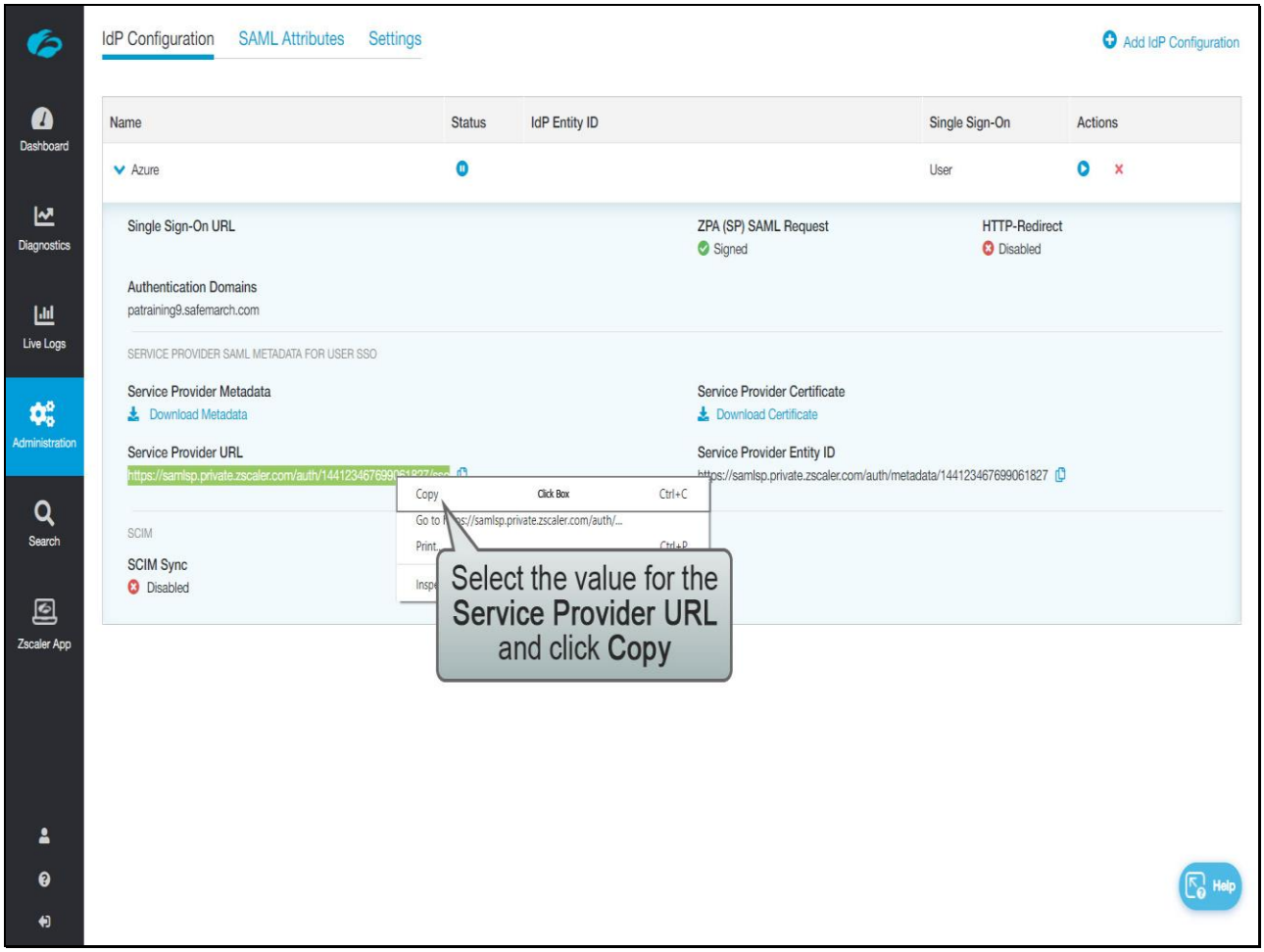
Slide 43 - Slide 43



Slide notes

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

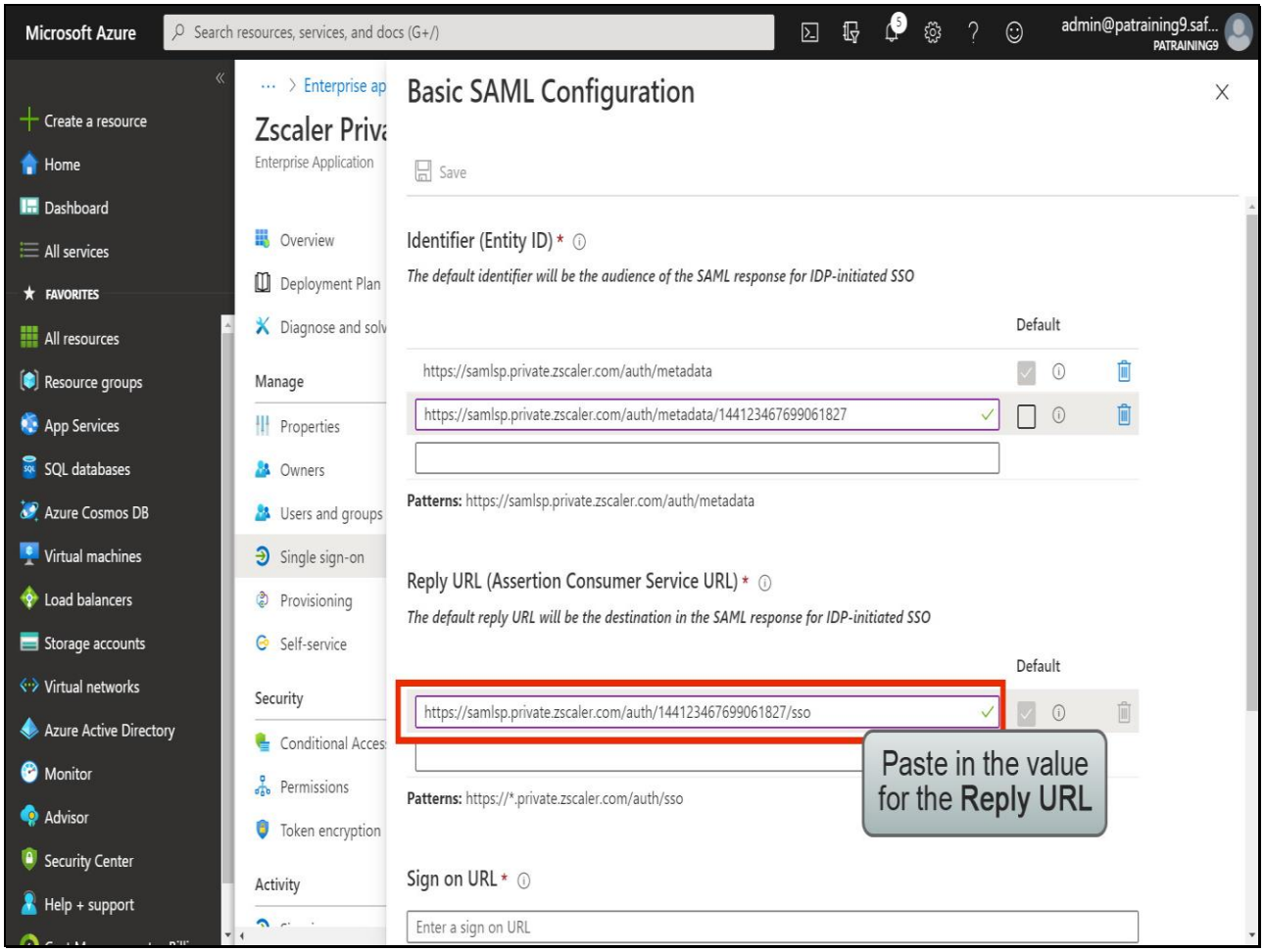
Slide 44 - Slide 44



Slide notes

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

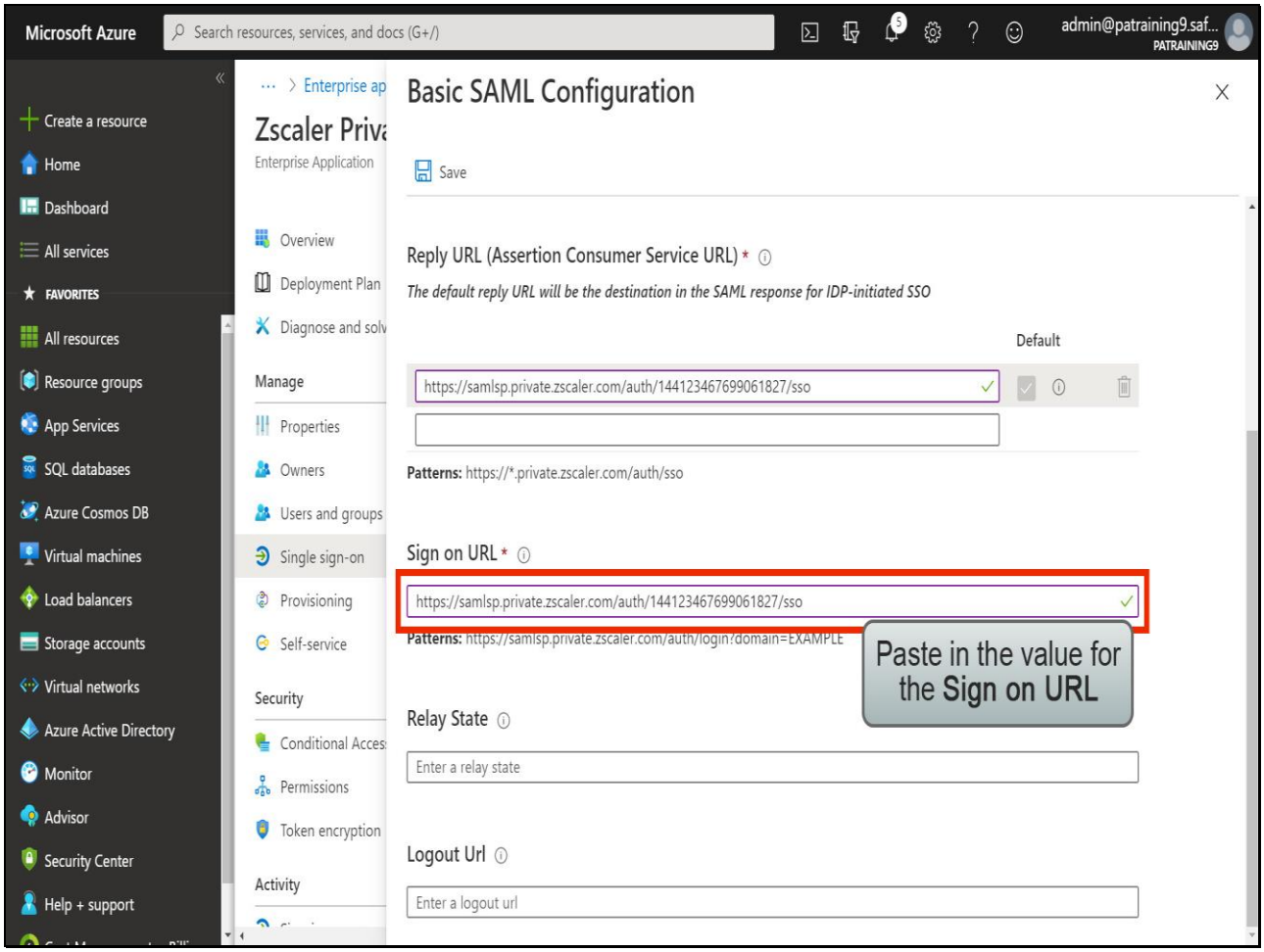
Slide 45 - Slide 45



Slide notes

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

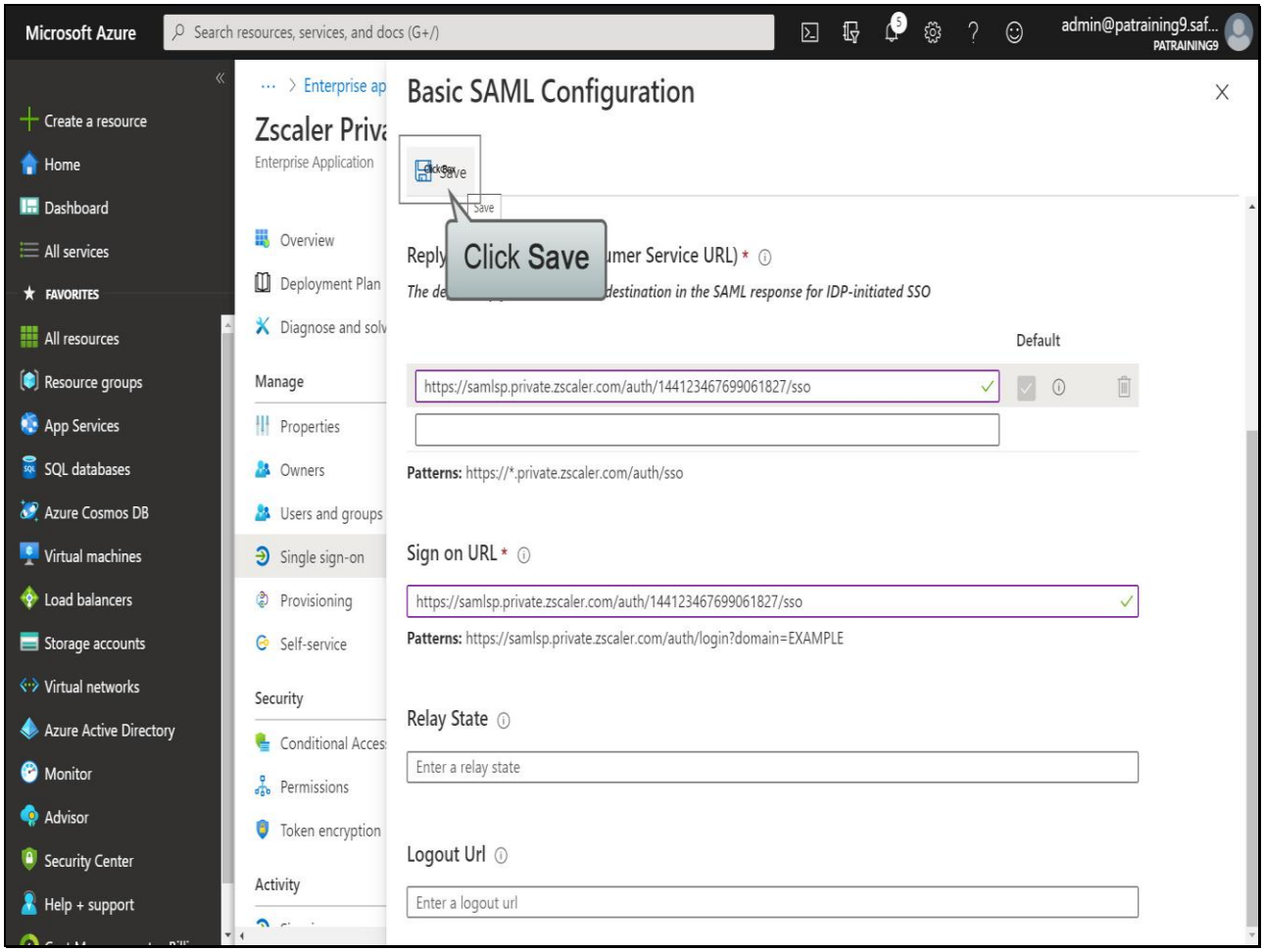
Slide 46 - Slide 46



Slide notes

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

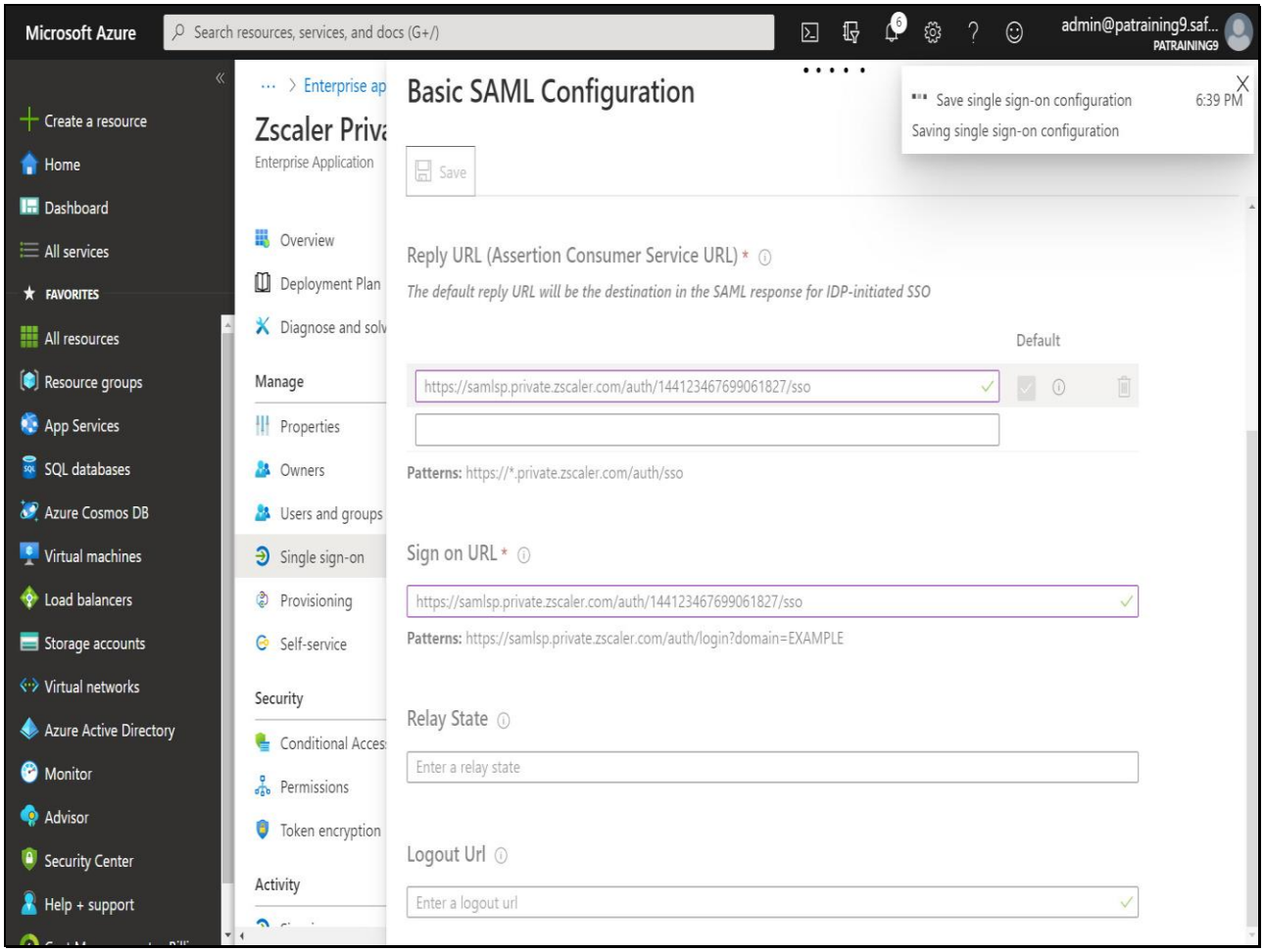
Slide 47 - Slide 47



Slide notes

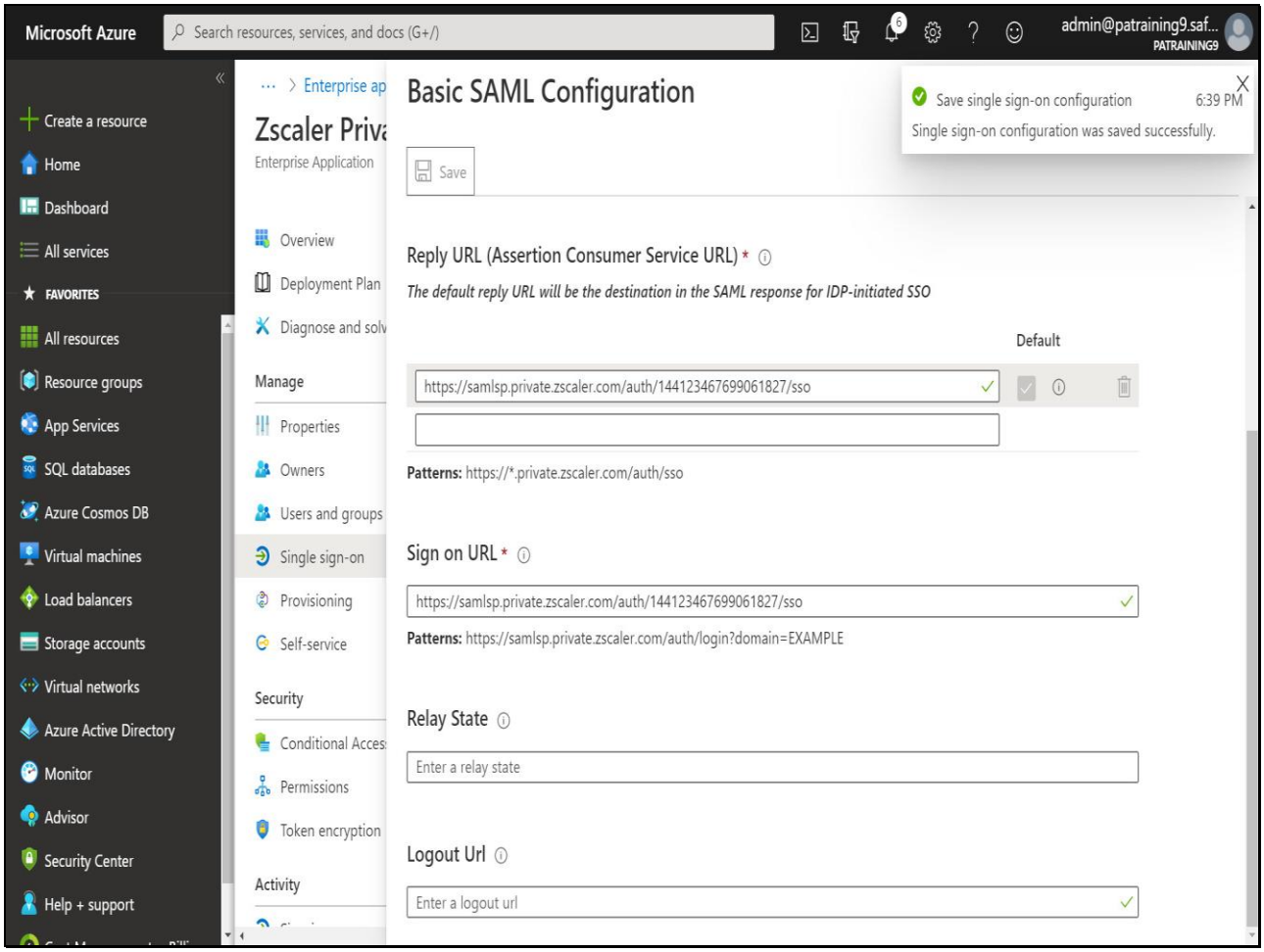
Then click **Save**, ...

Slide 48 - Slide 48



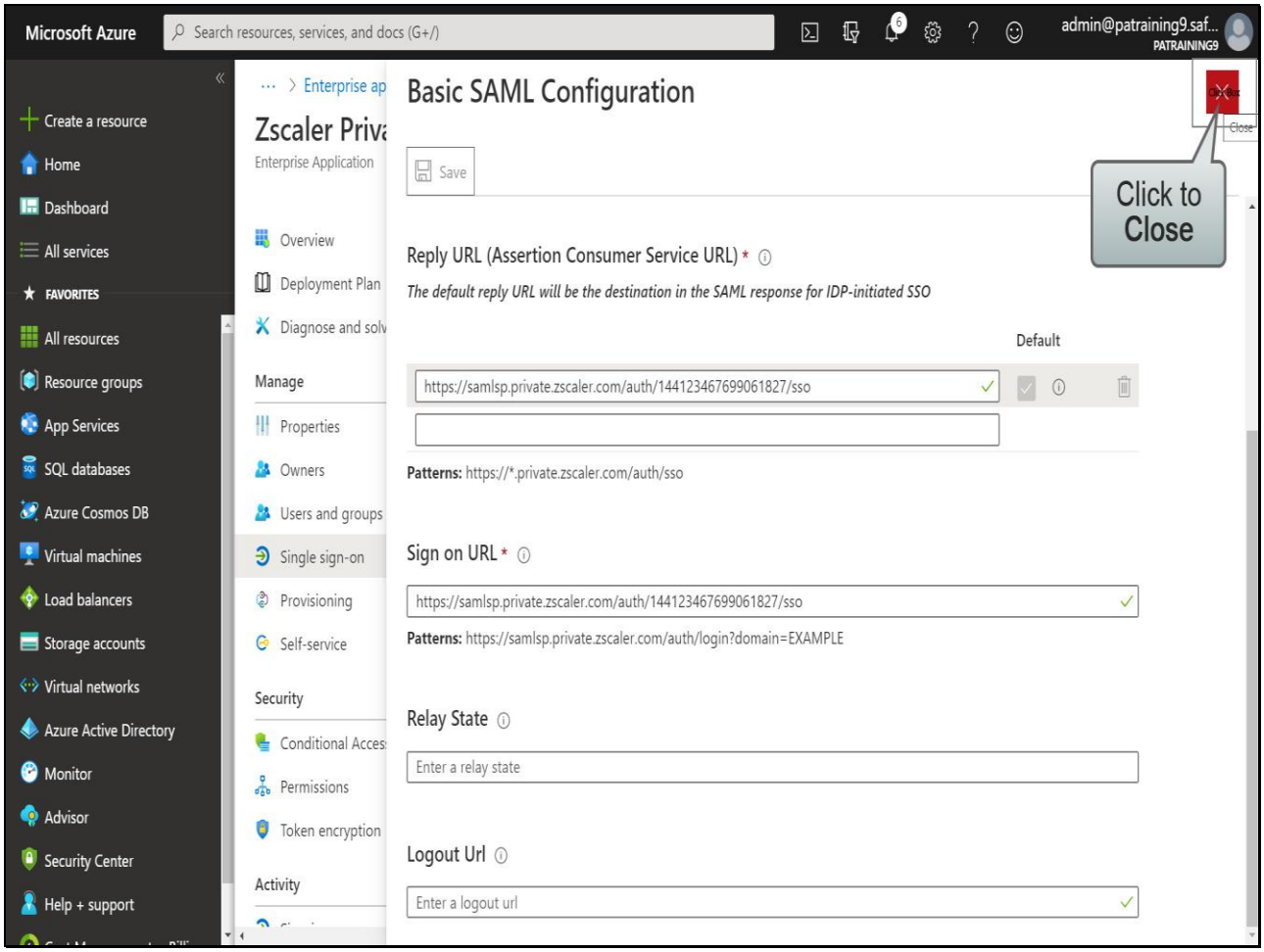
Slide notes

Slide 49 - Slide 49



Slide notes

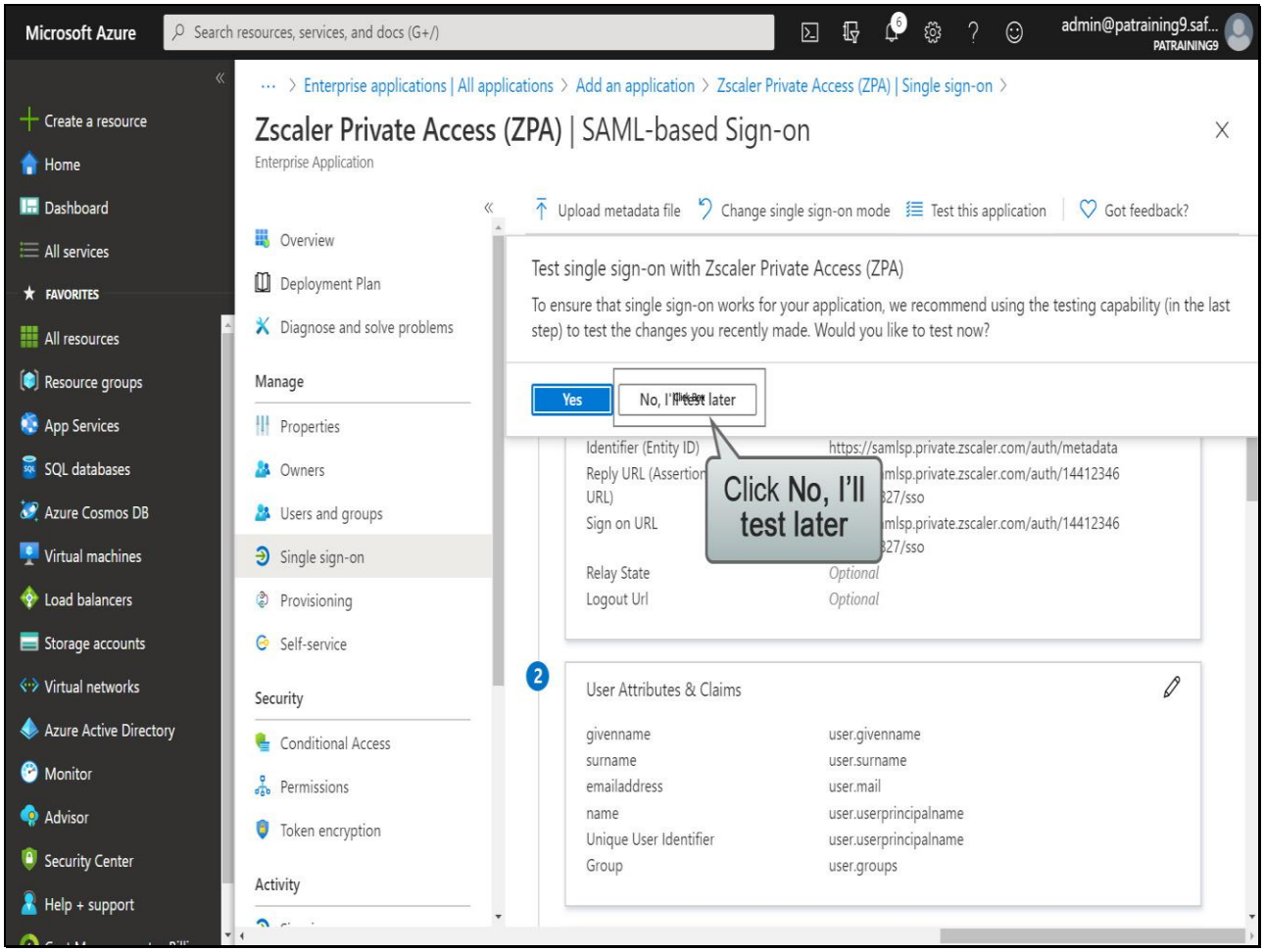
Slide 50 - Slide 50



Slide notes

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

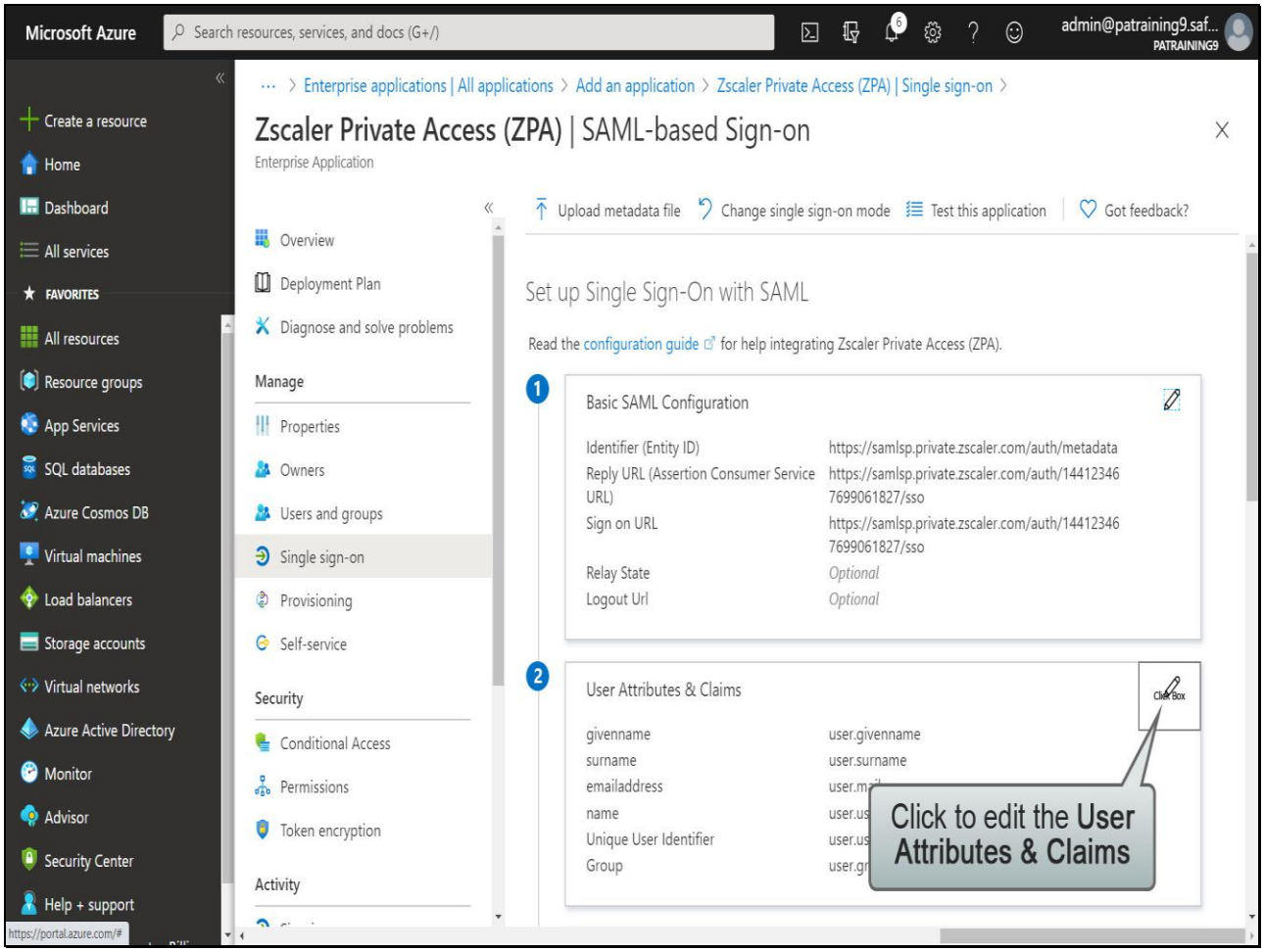
Slide 51 - Slide 51



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**.

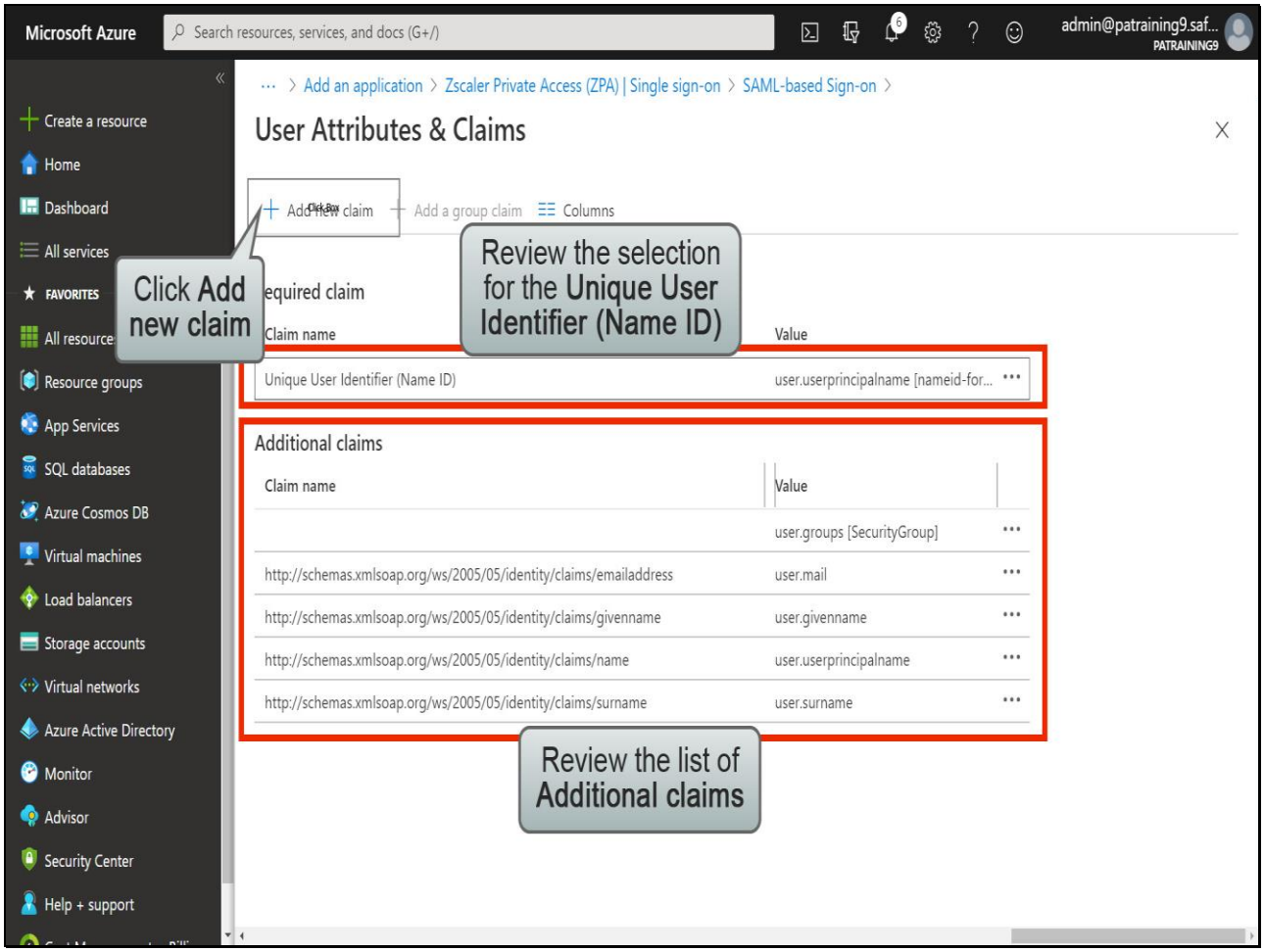
Slide 52 - Slide 52



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

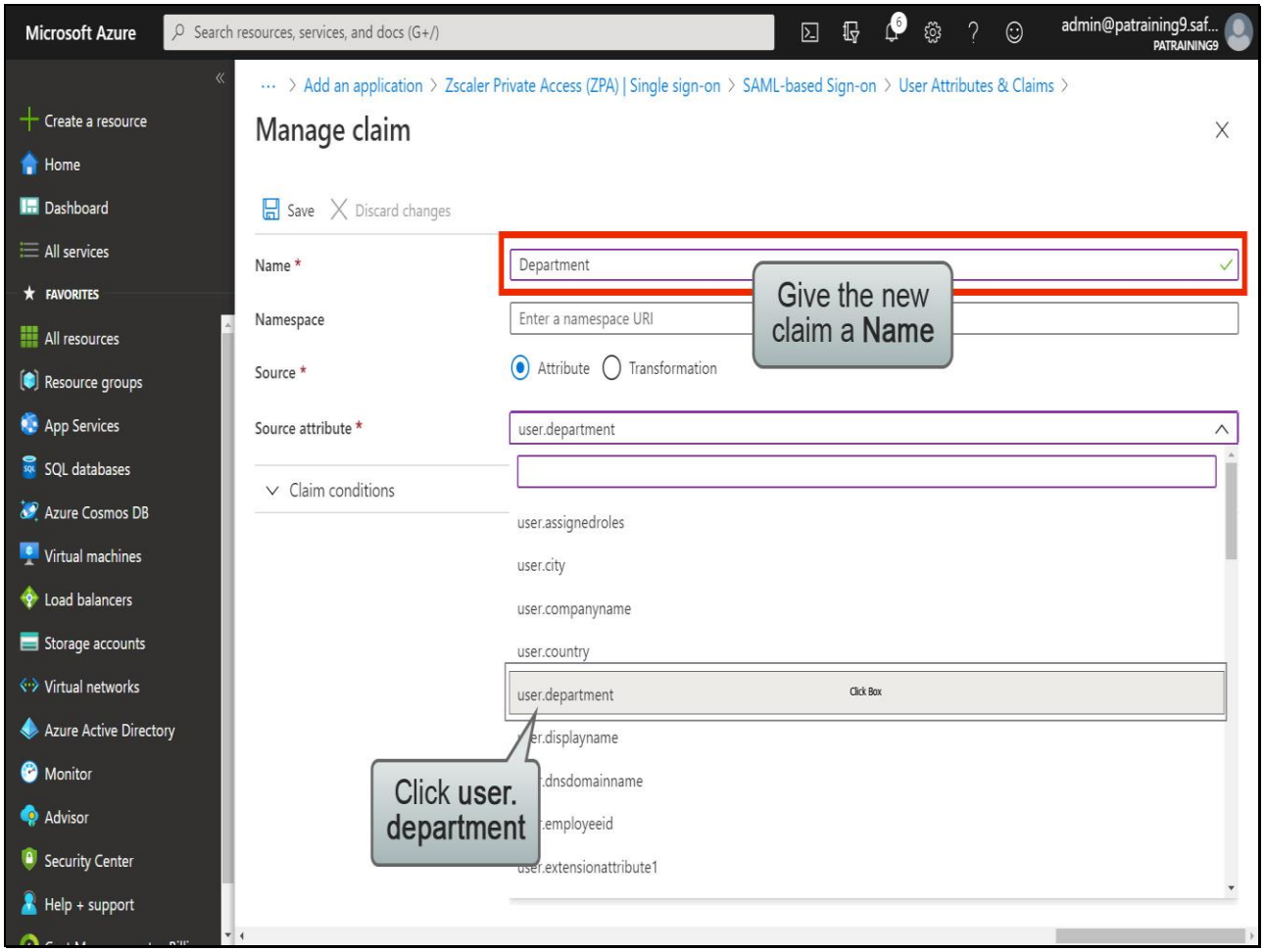


Slide notes

Review the value set for the **Unique User Identifier (Name ID)**, Zscaler recommends you use the **user.userprinciplename [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**.

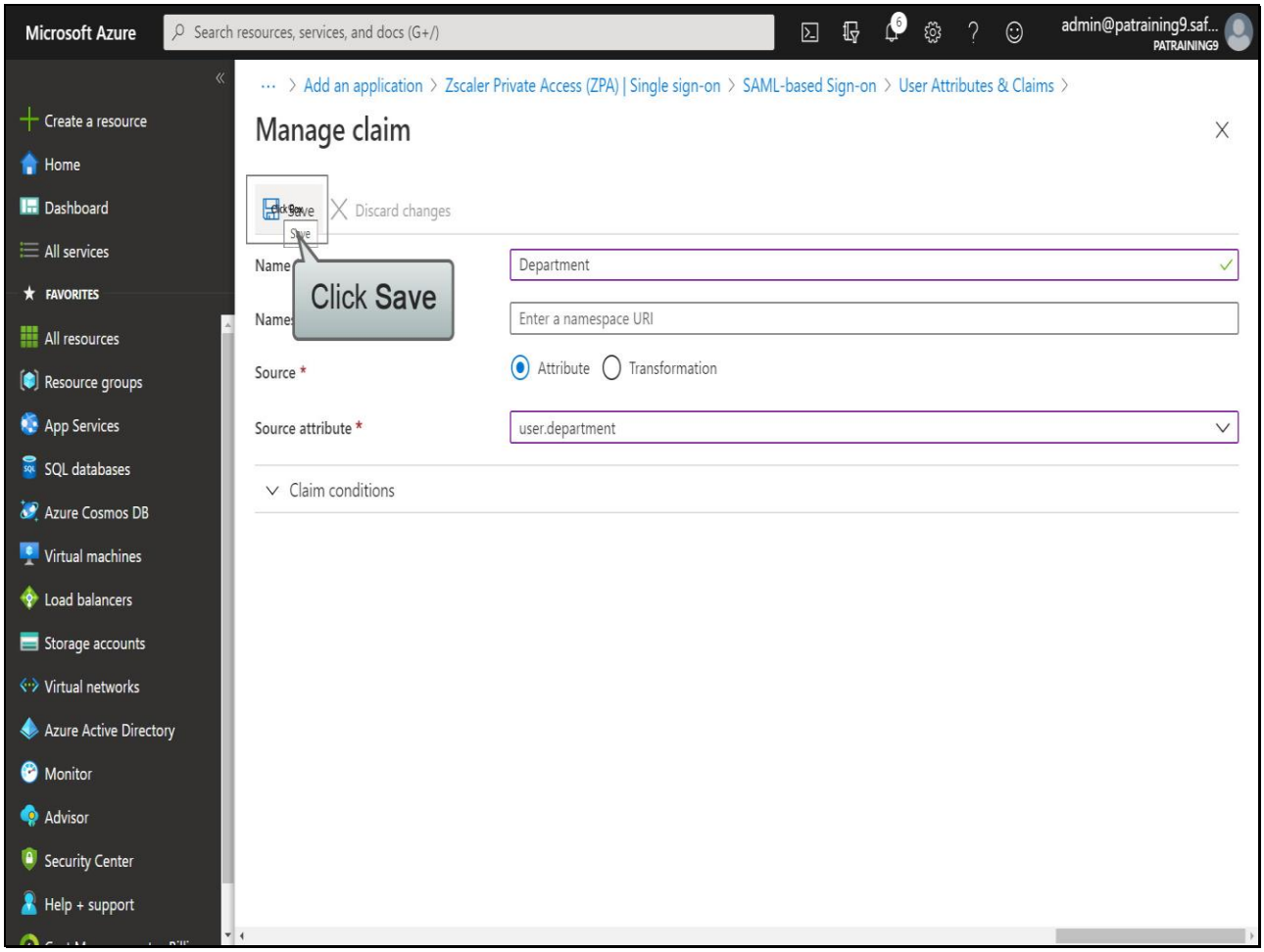
Slide 54 - Slide 54



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**.

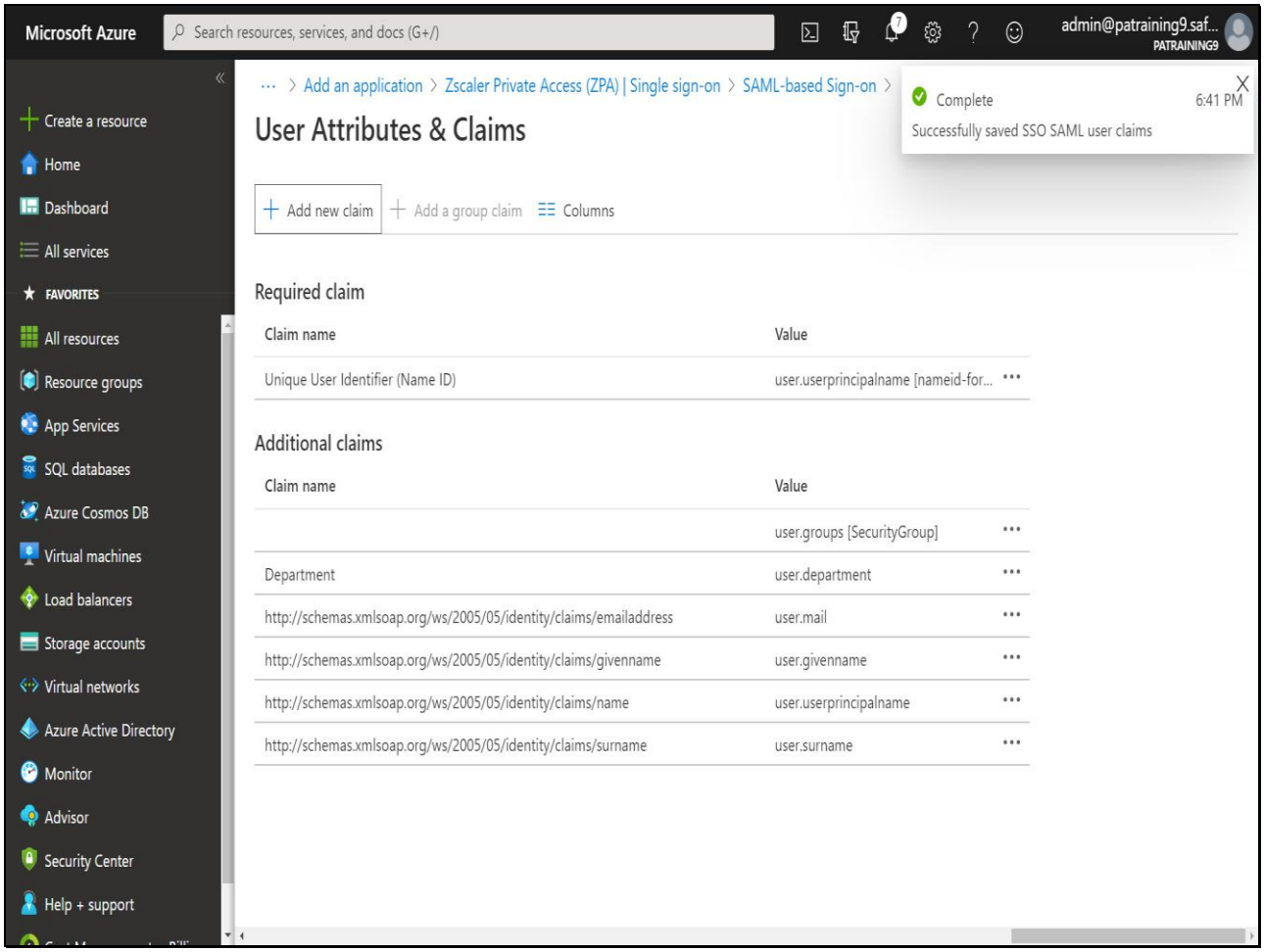
Slide 55 - Slide 55



Slide notes

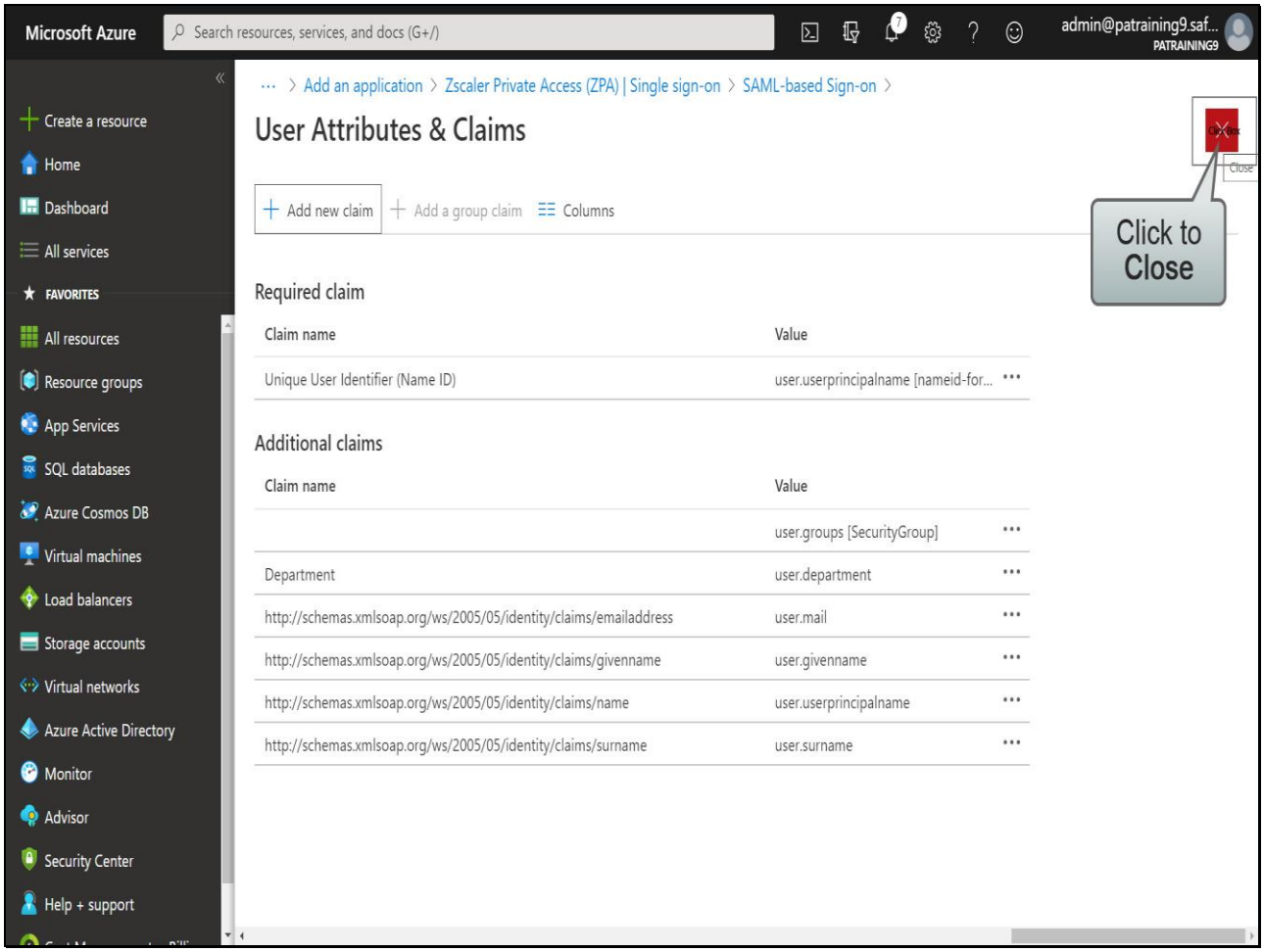
Then click **Save**, ...

Slide 56 - Slide 56



Slide notes

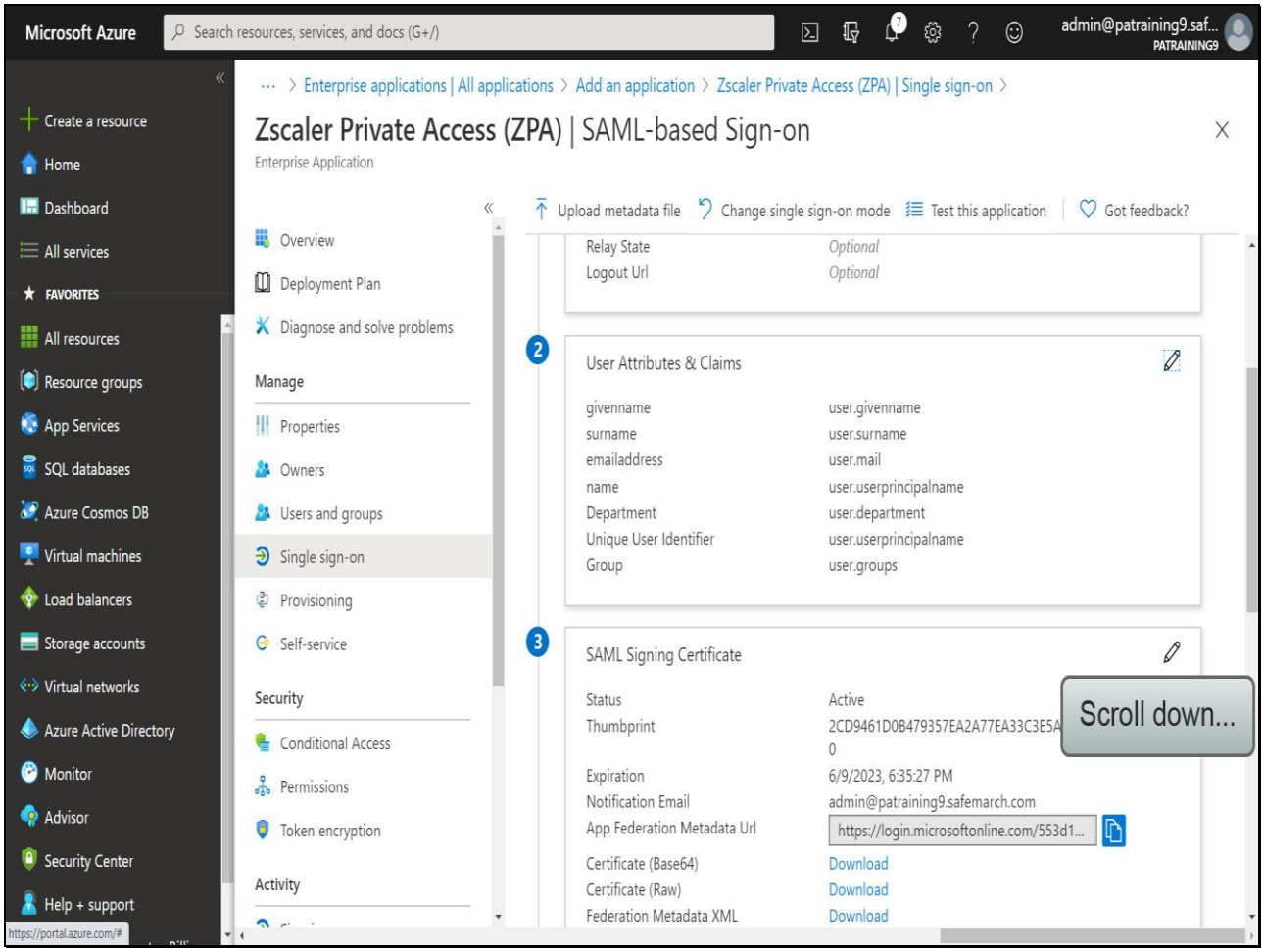
Slide 57 - Slide 57



Slide notes

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

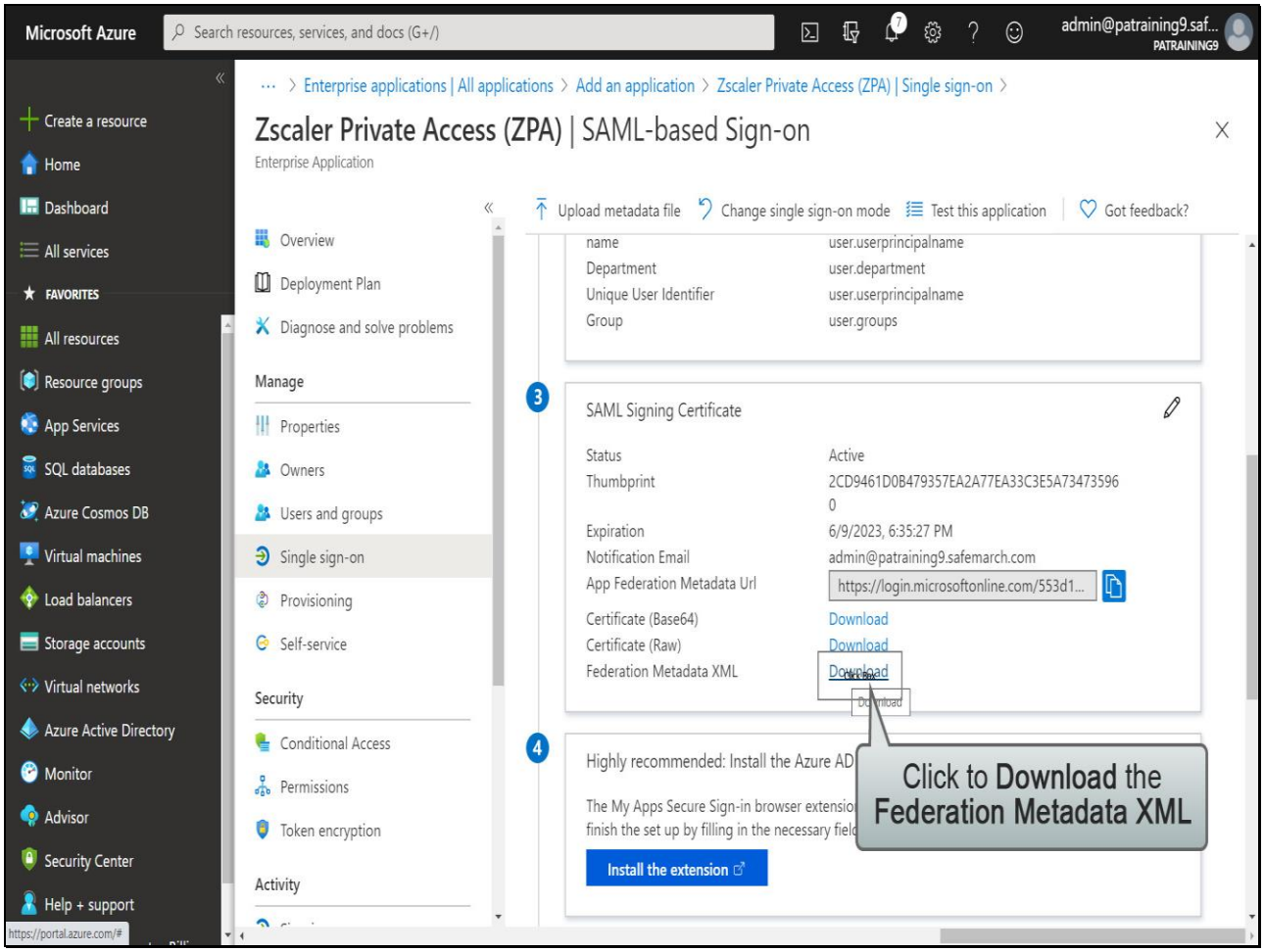
Slide 58 - Slide 58



Slide notes

Scroll down, ...

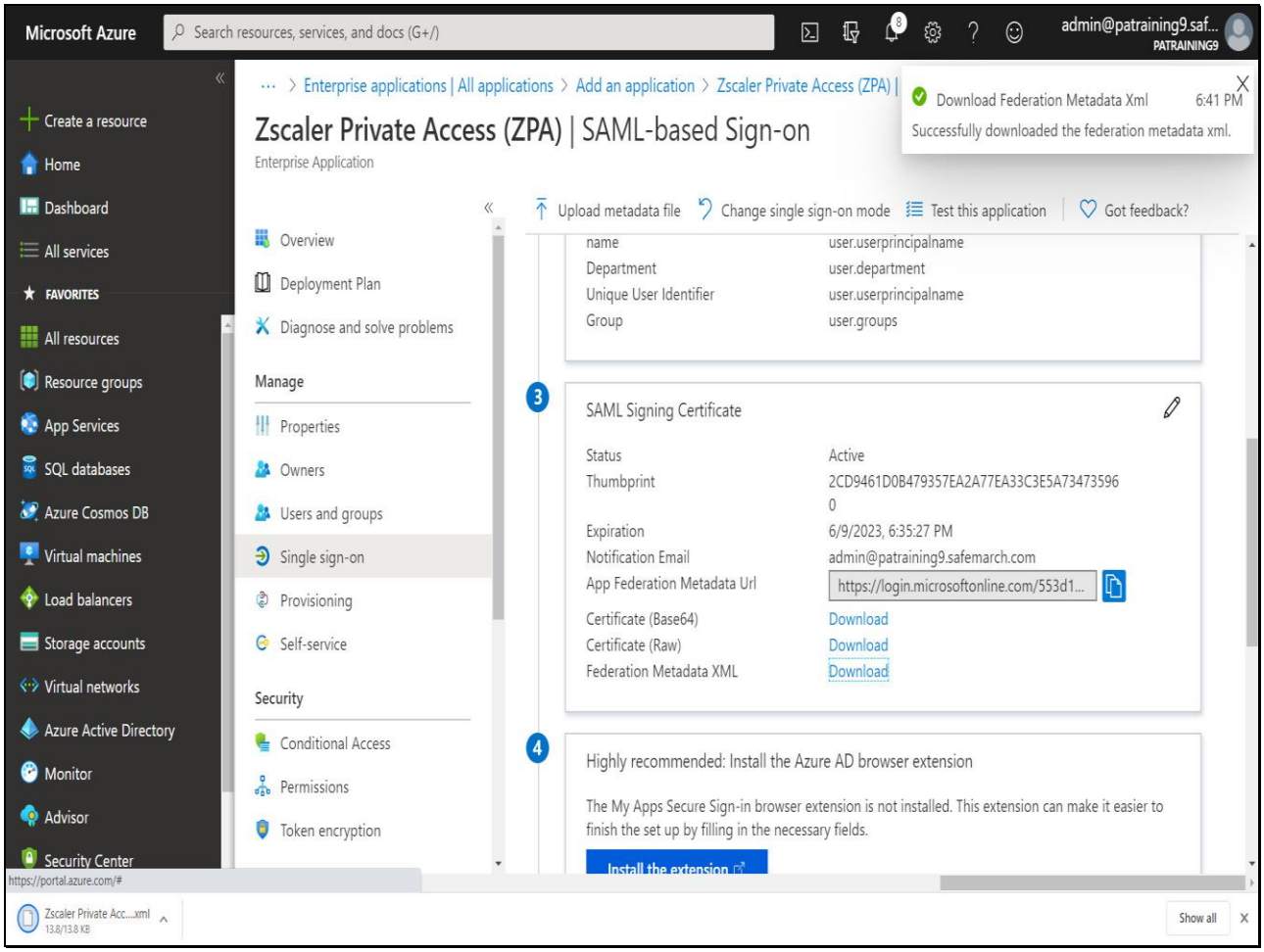
Slide 59 - Slide 59



Slide notes

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

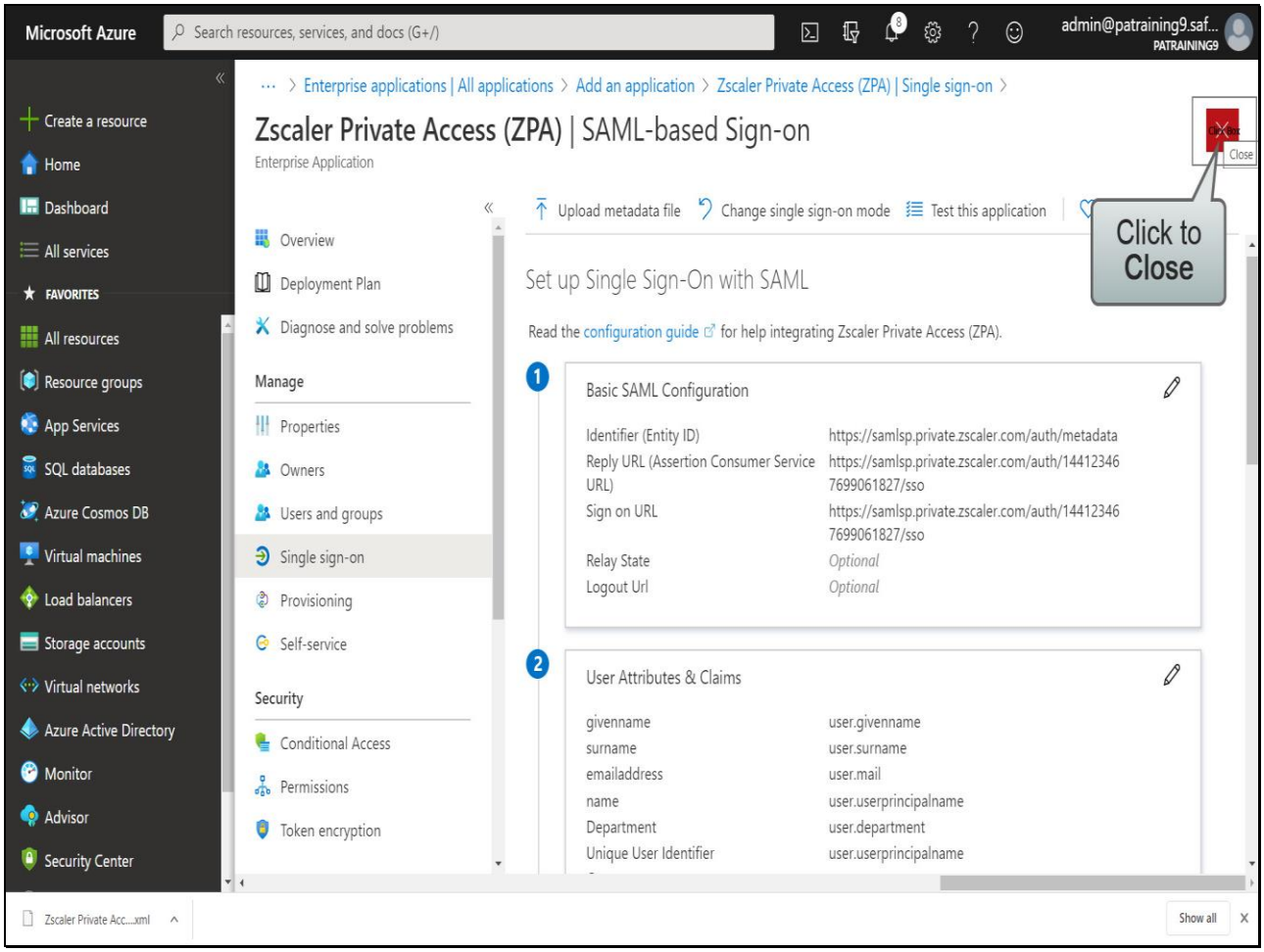
Slide 60 - Slide 60



Slide notes

...save the file, ...

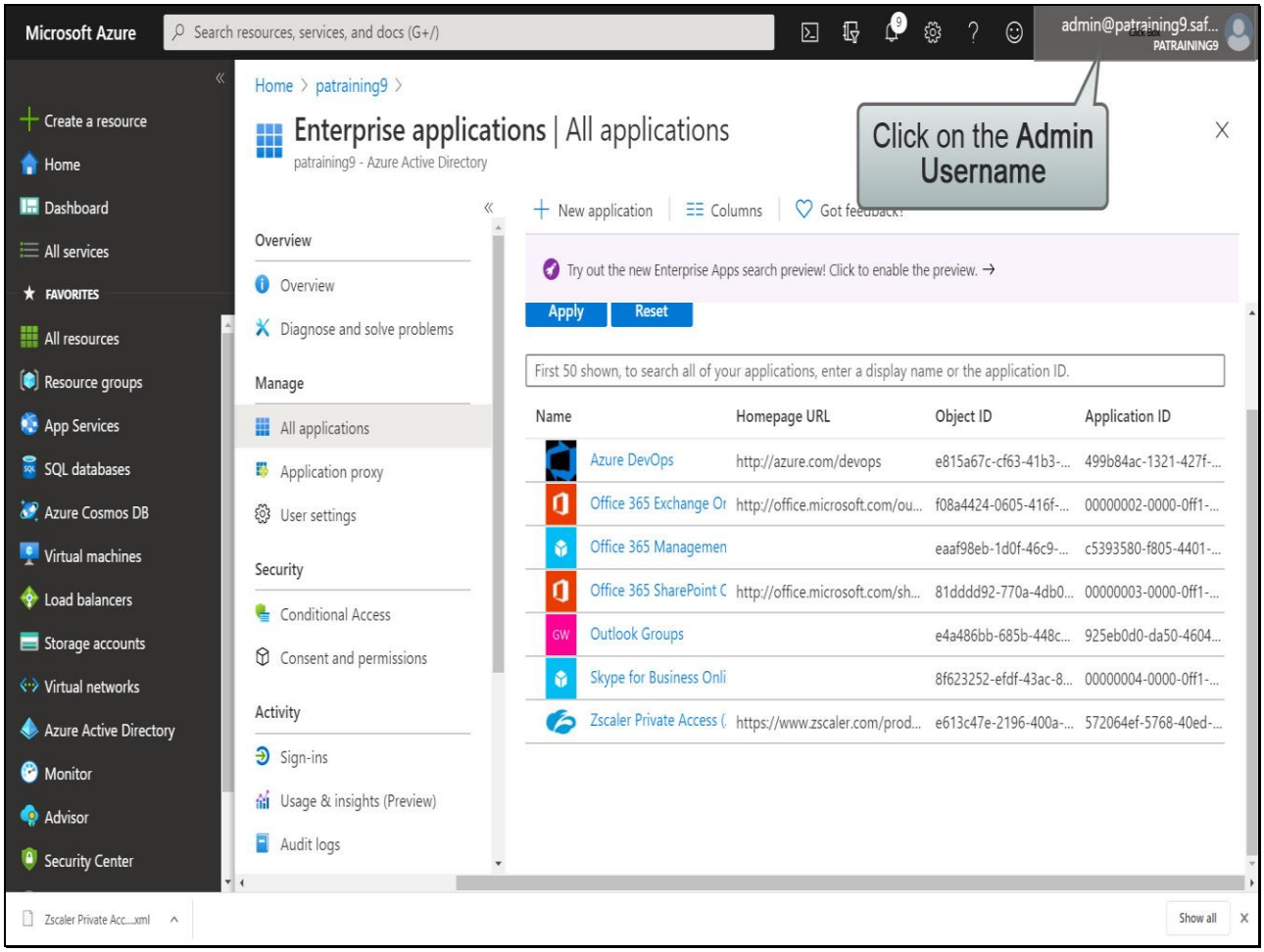
Slide 61 - Slide 61



Slide notes

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

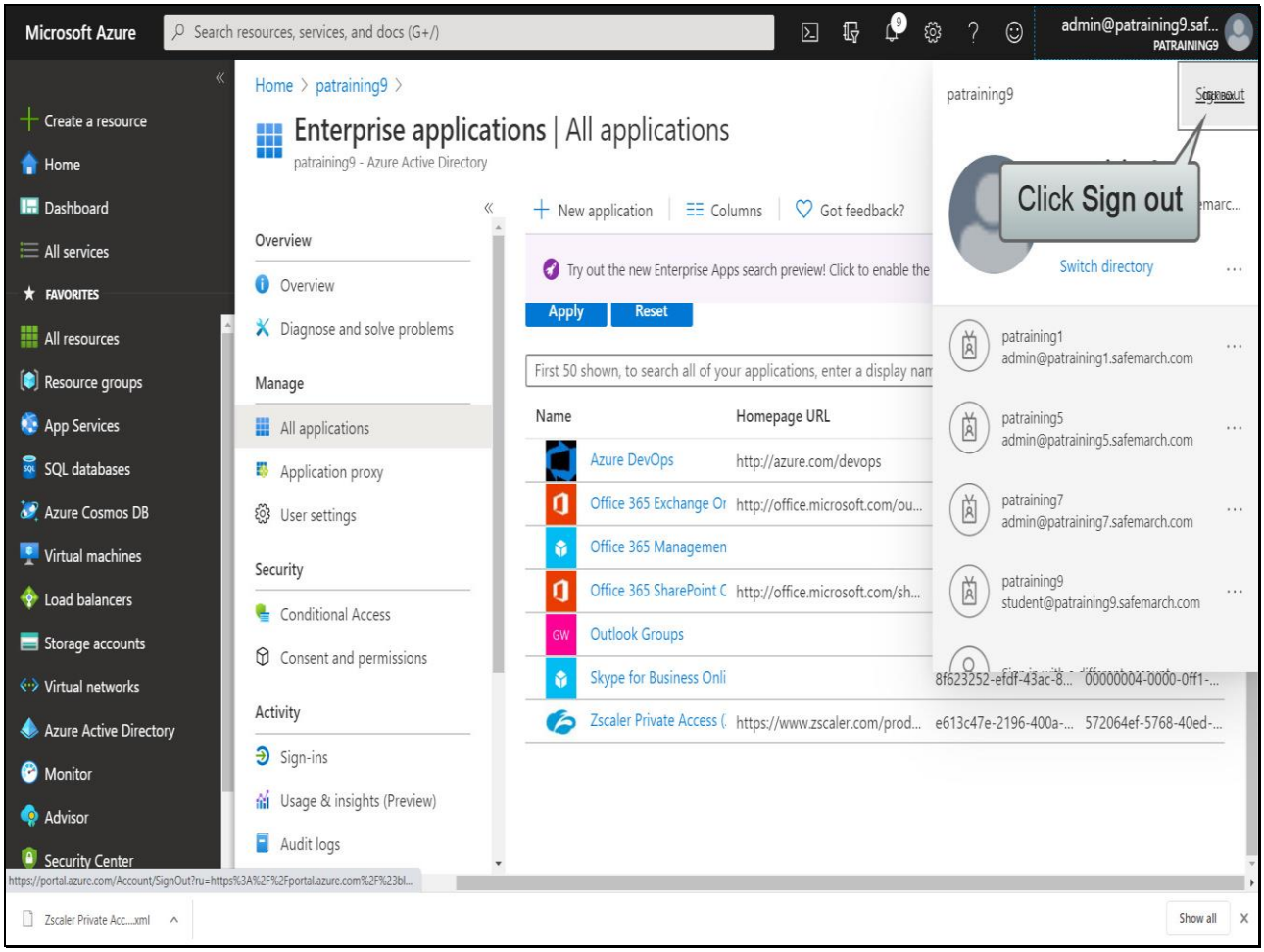
Slide 62 - Slide 62



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, ...

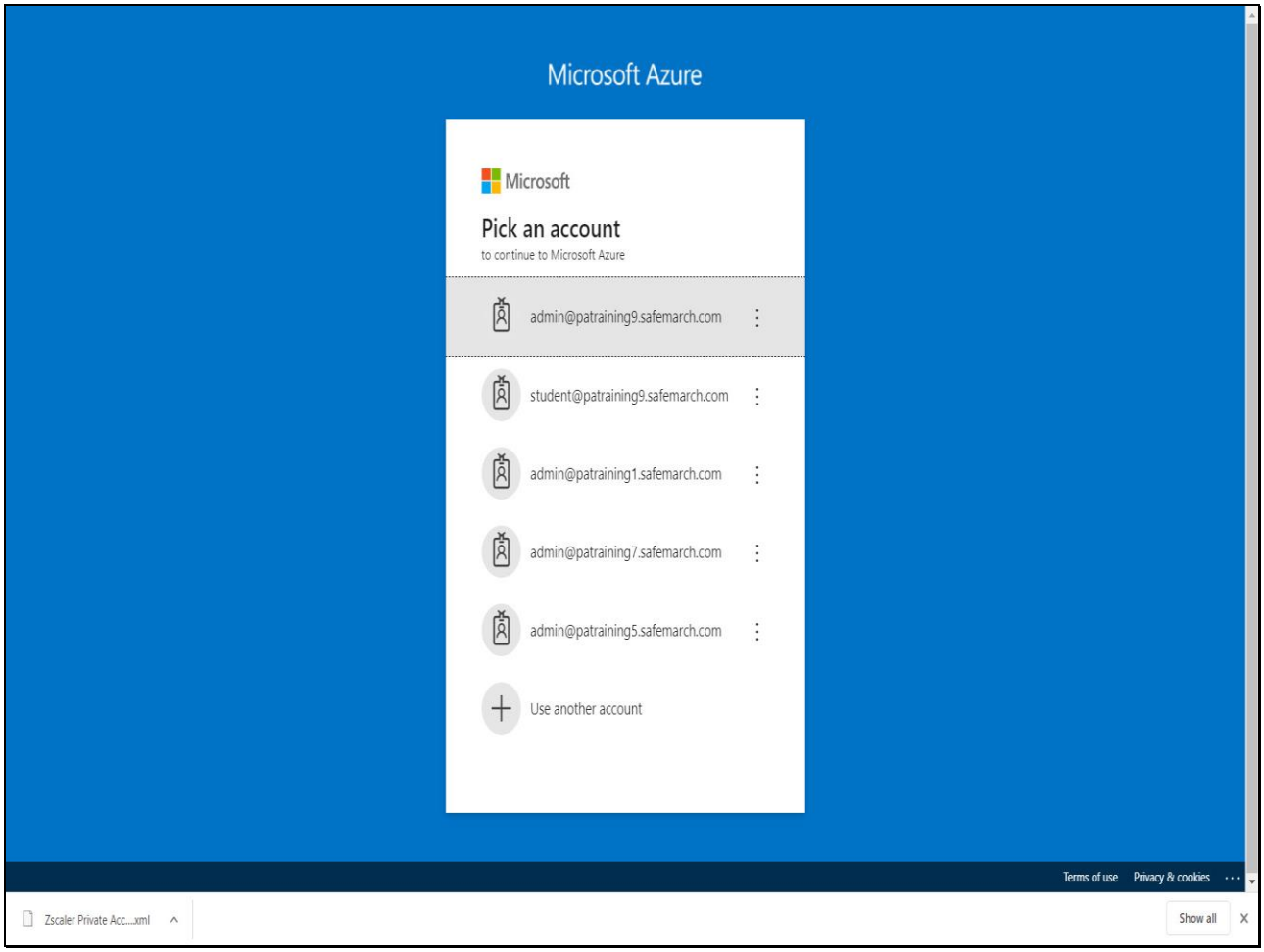
Slide 63 - Slide 63



Slide notes

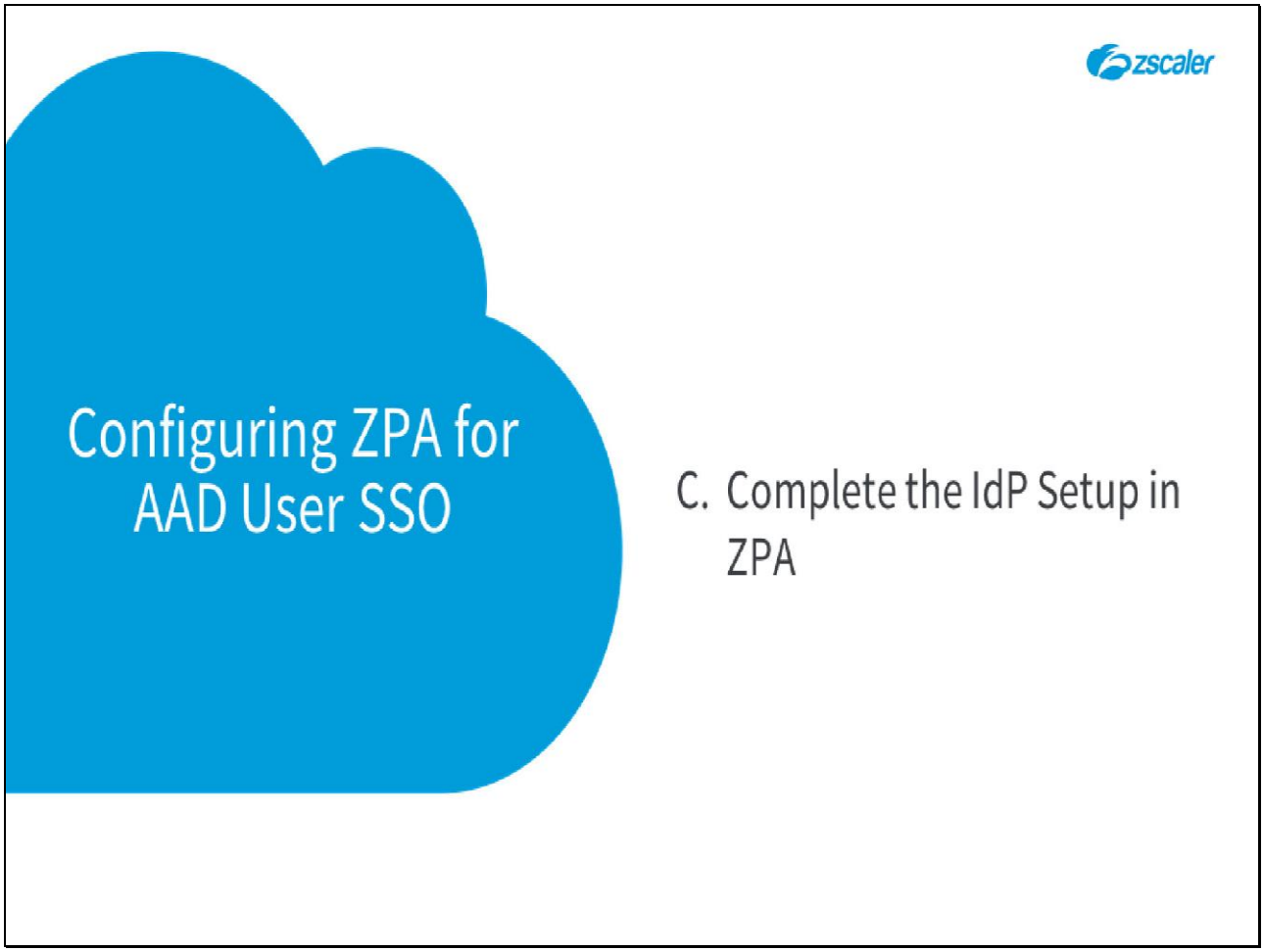
...and click **Sign out**.

Slide 64 - Slide 64



Slide notes

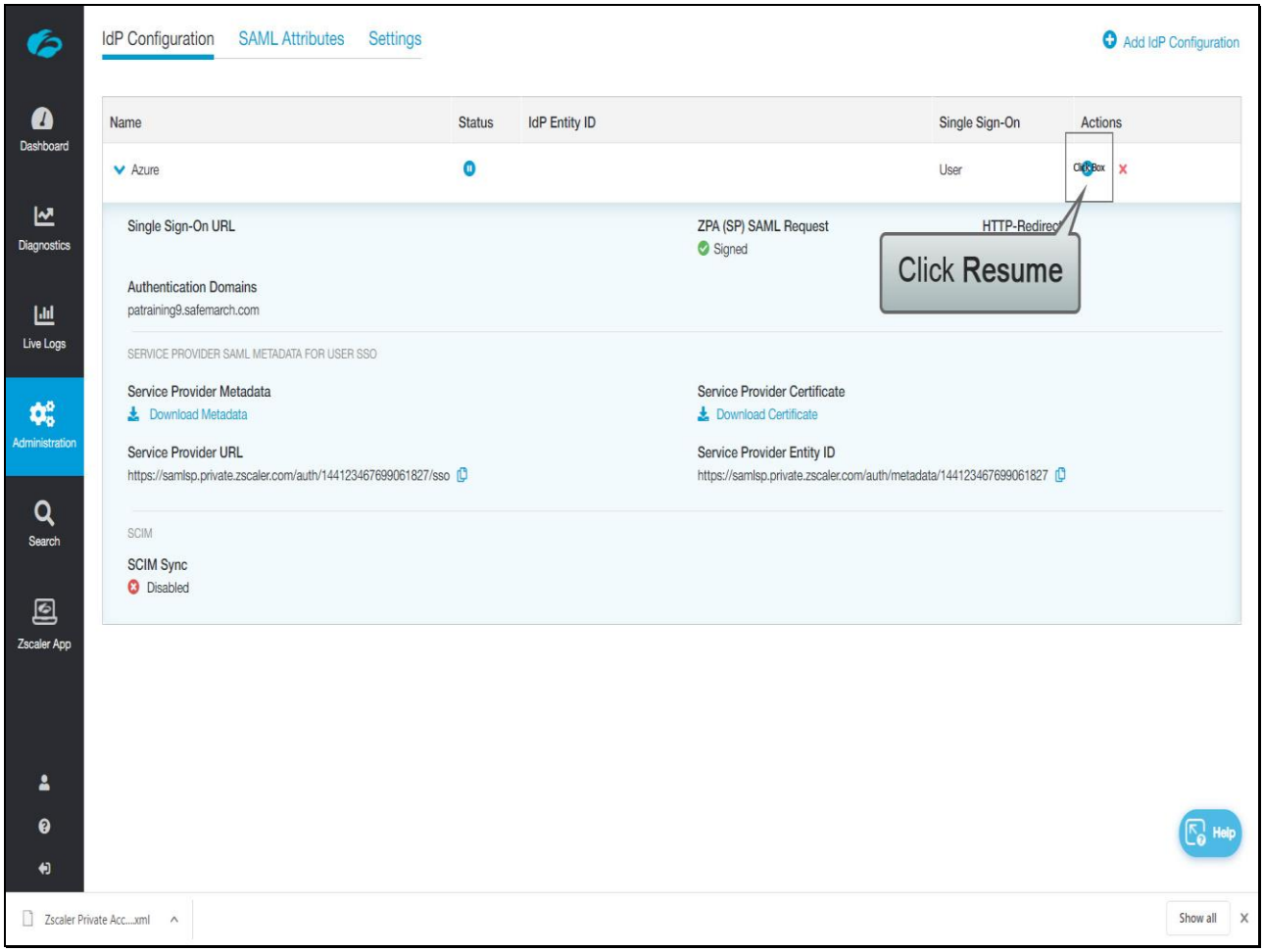
Slide 65 - Configuring ZPA for Okta User SSO



Slide notes

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

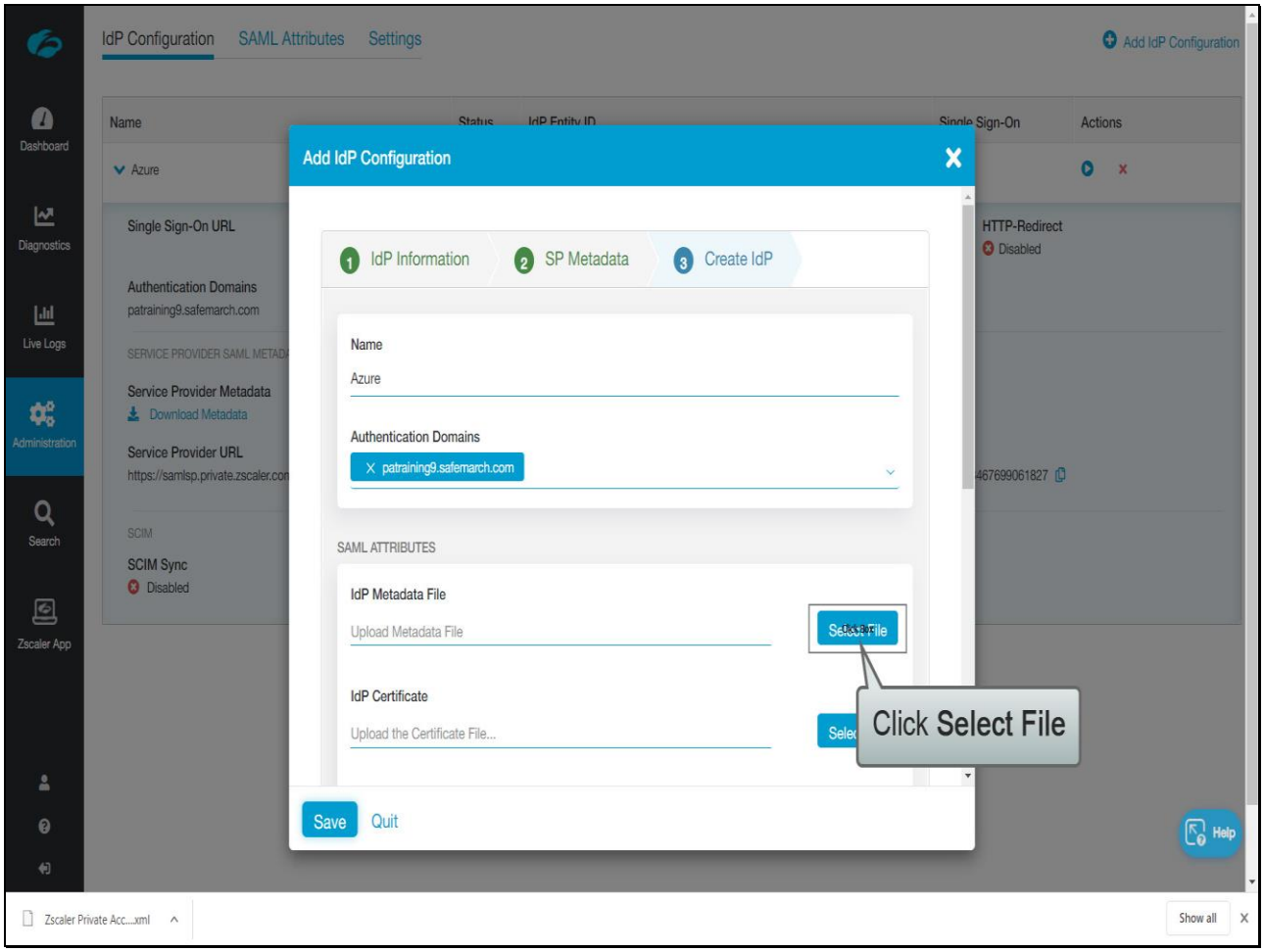
Slide 66 - Slide 66



Slide notes

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

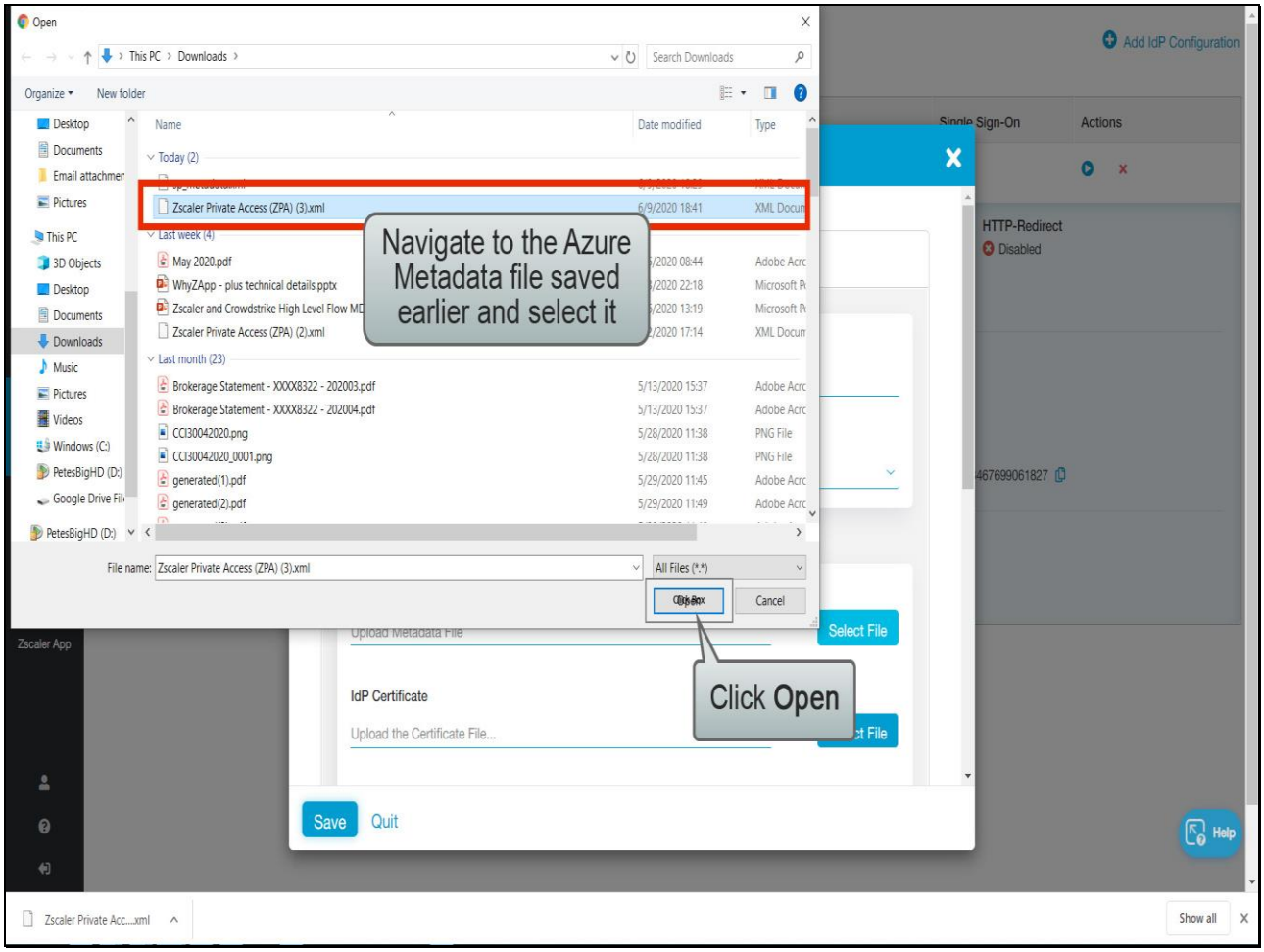
Slide 67 - Slide 67



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**, …

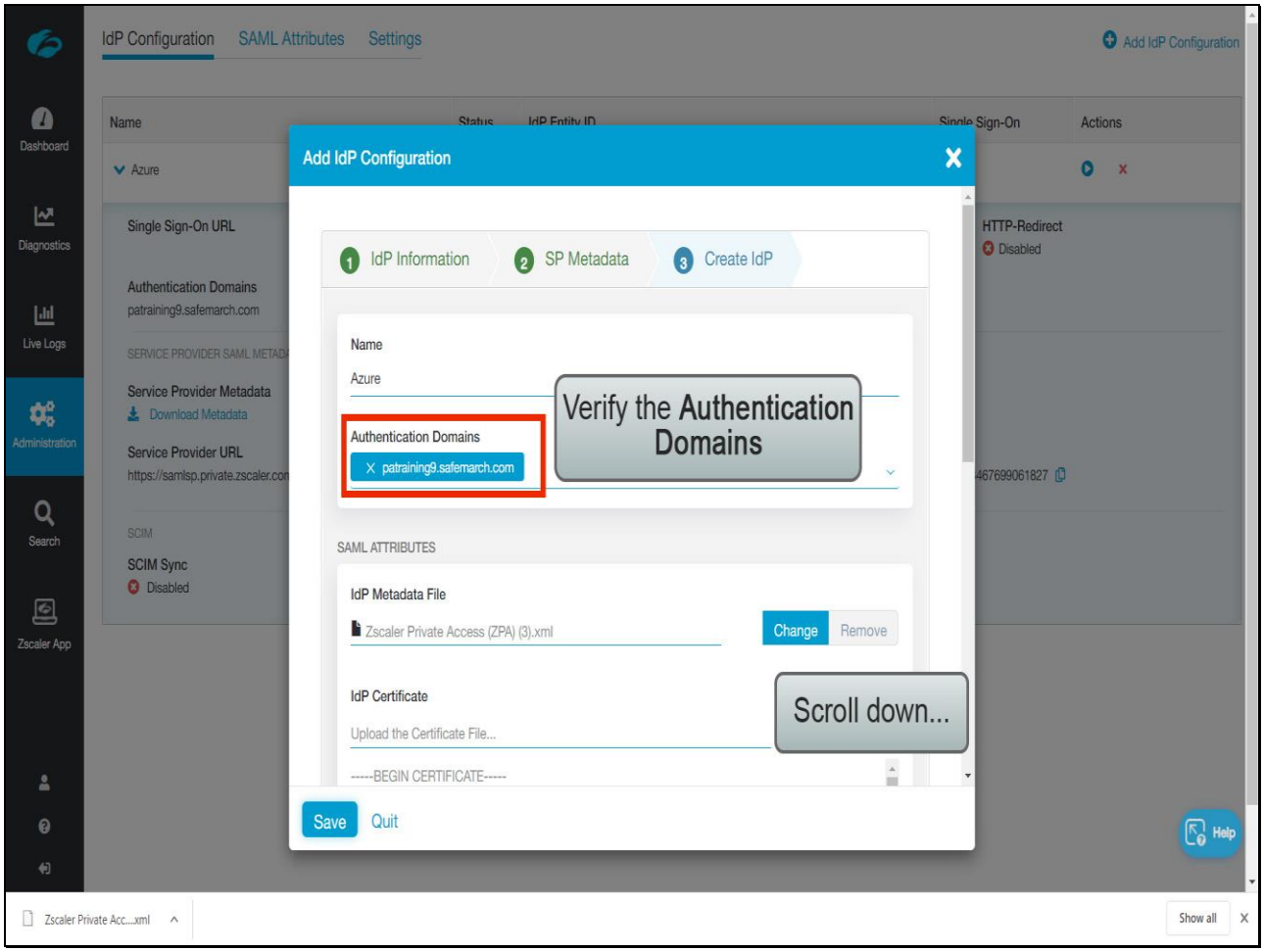
Slide 68 - Slide 68



Slide notes

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

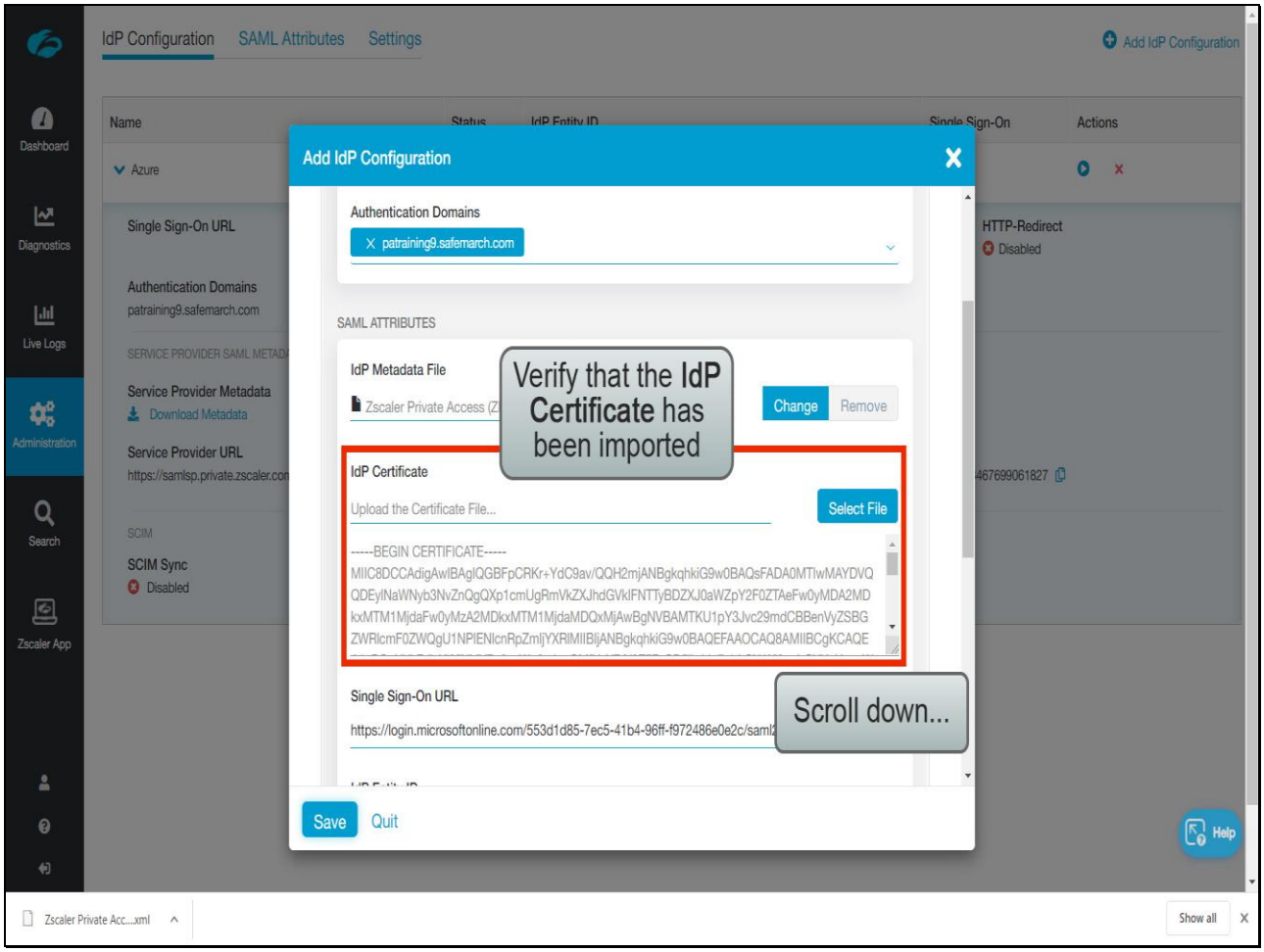
Slide 69 - Slide 69



Slide notes

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

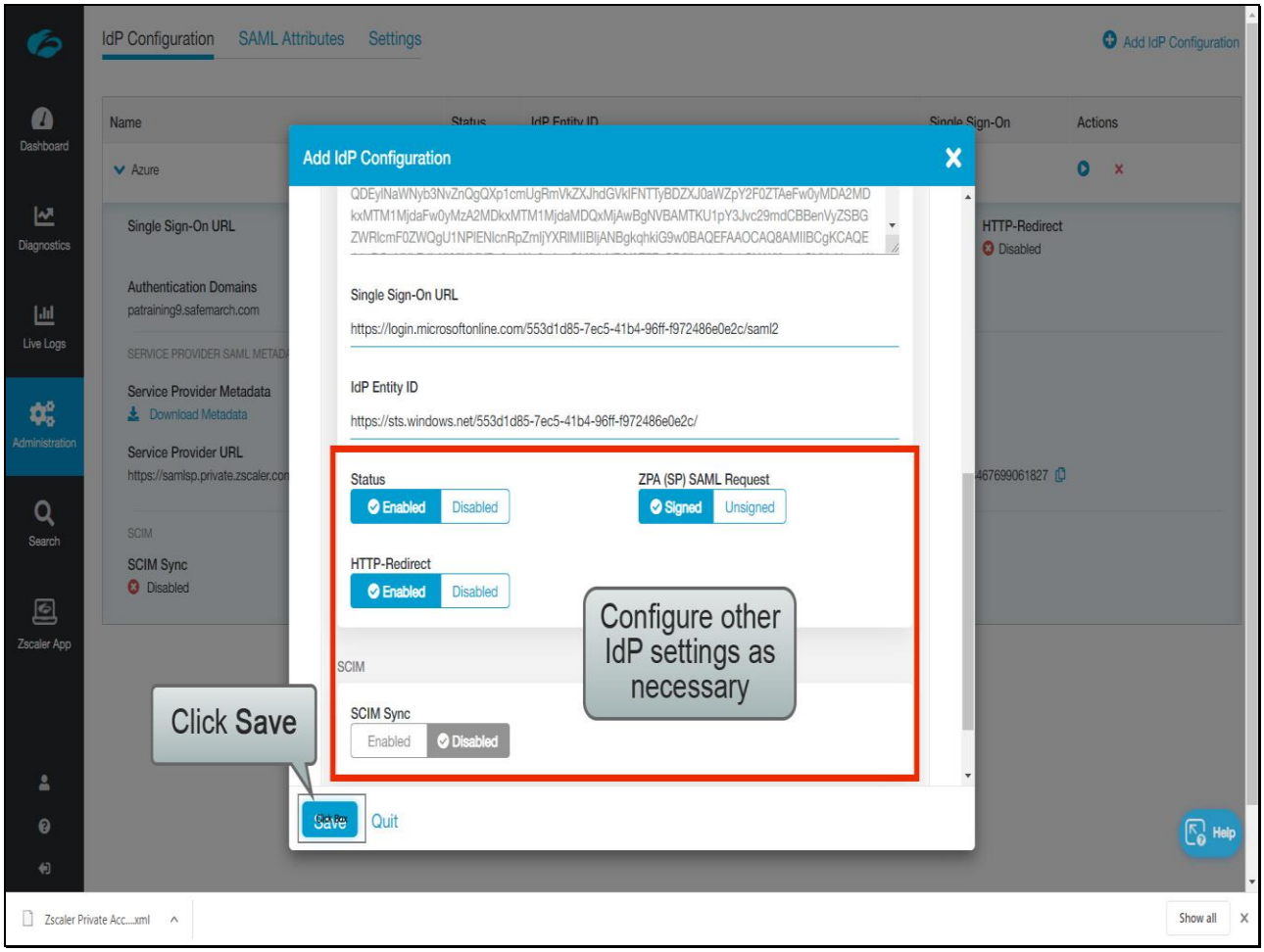
Slide 70 - Slide 70



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, ...

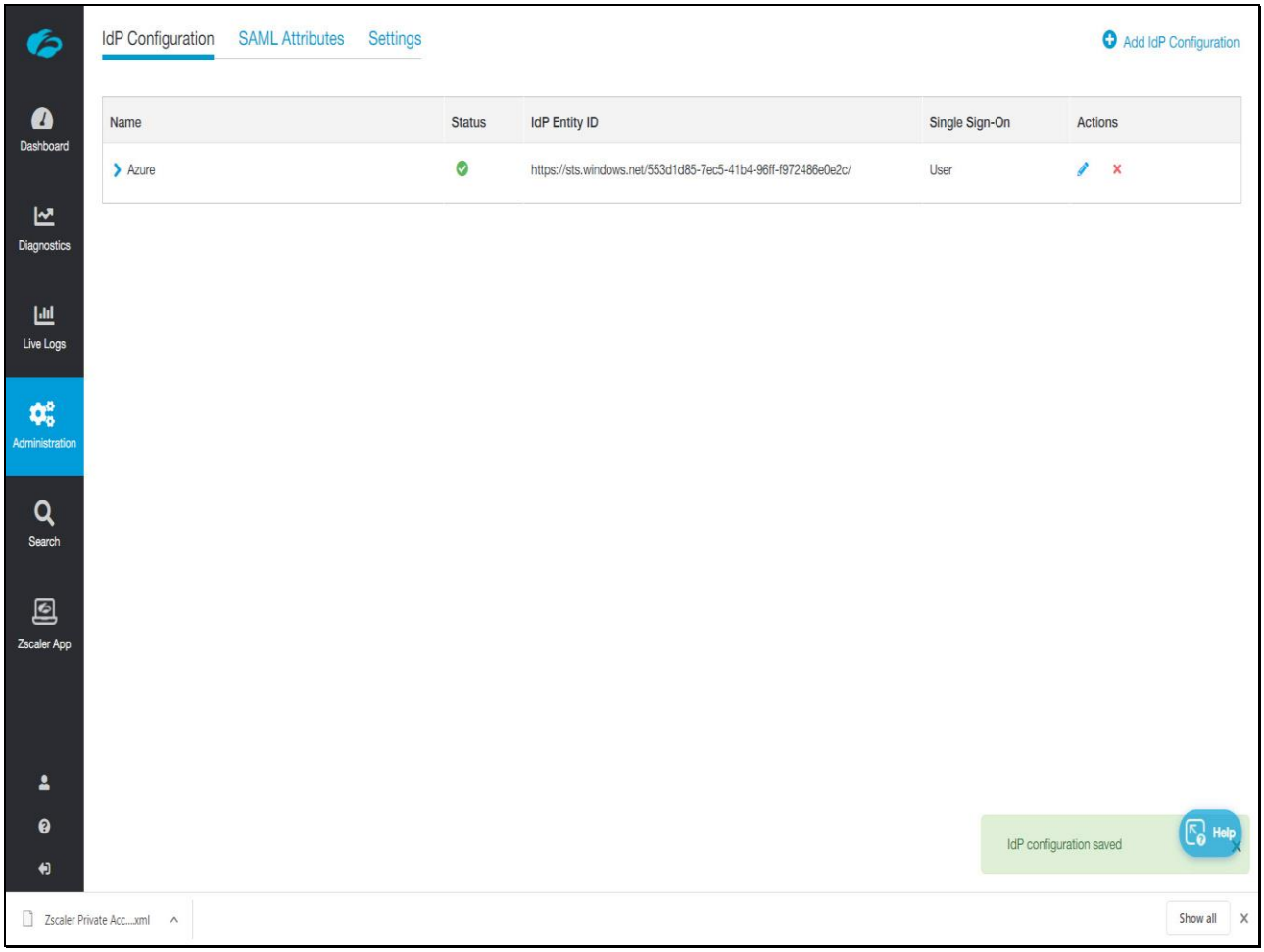
Slide 71 - Slide 71



Slide notes

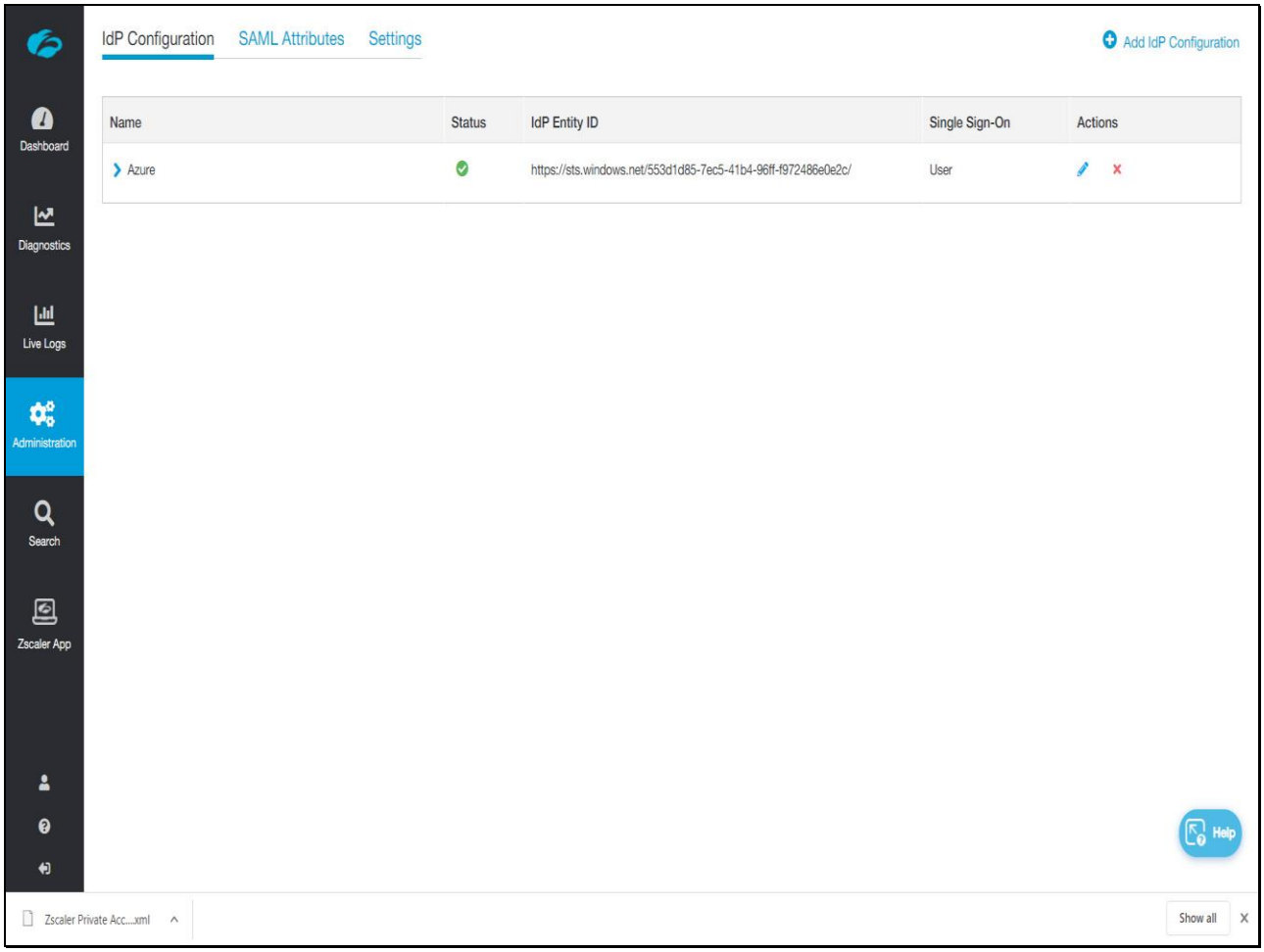
...adjust other IdP configuration settings as required and click **Save**.

Slide 72 - Slide 72



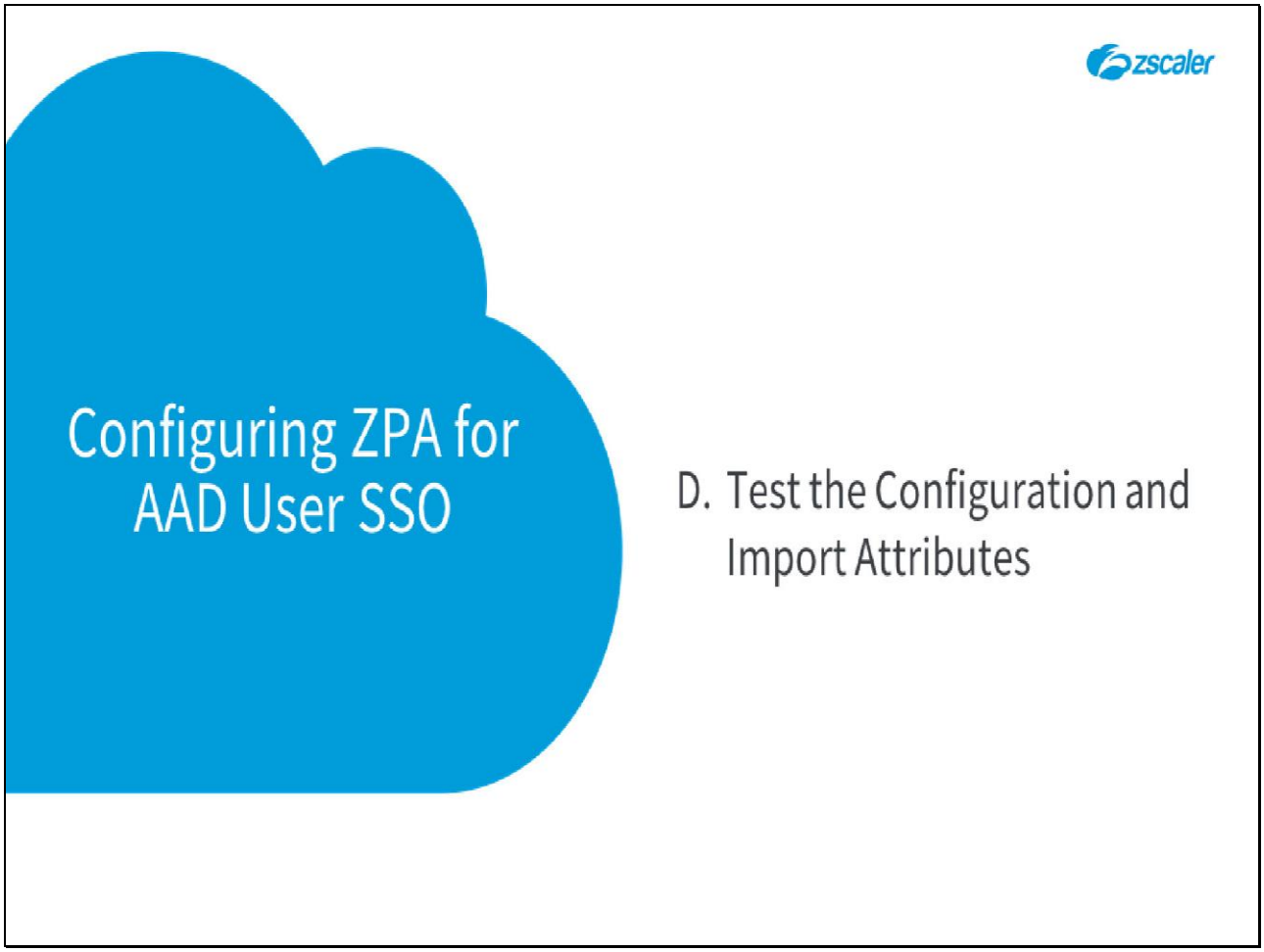
Slide notes

Slide 73 - Slide 73



Slide notes

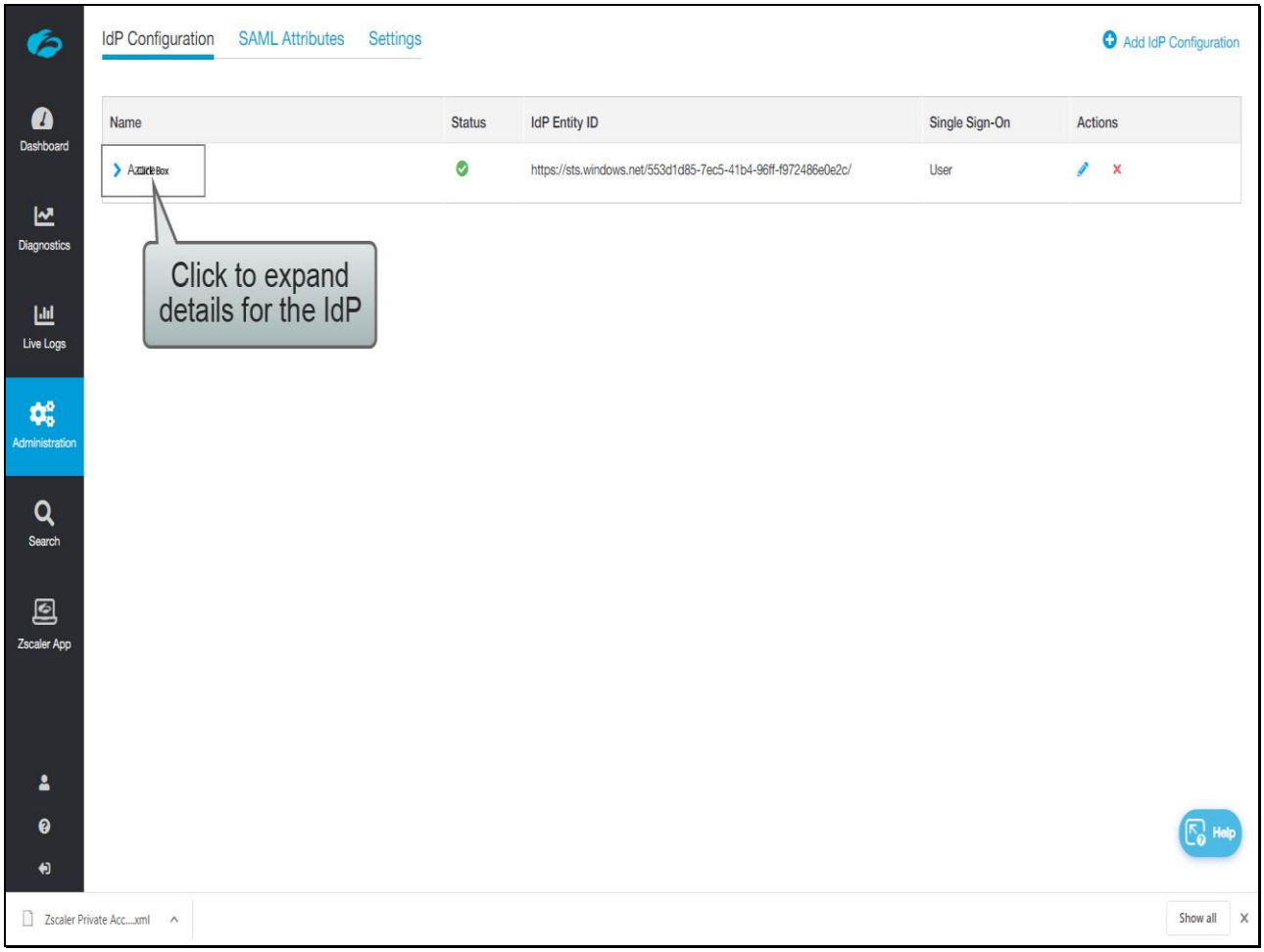
Slide 74 - Configuring ZPA for Okta User SSO



Slide notes

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

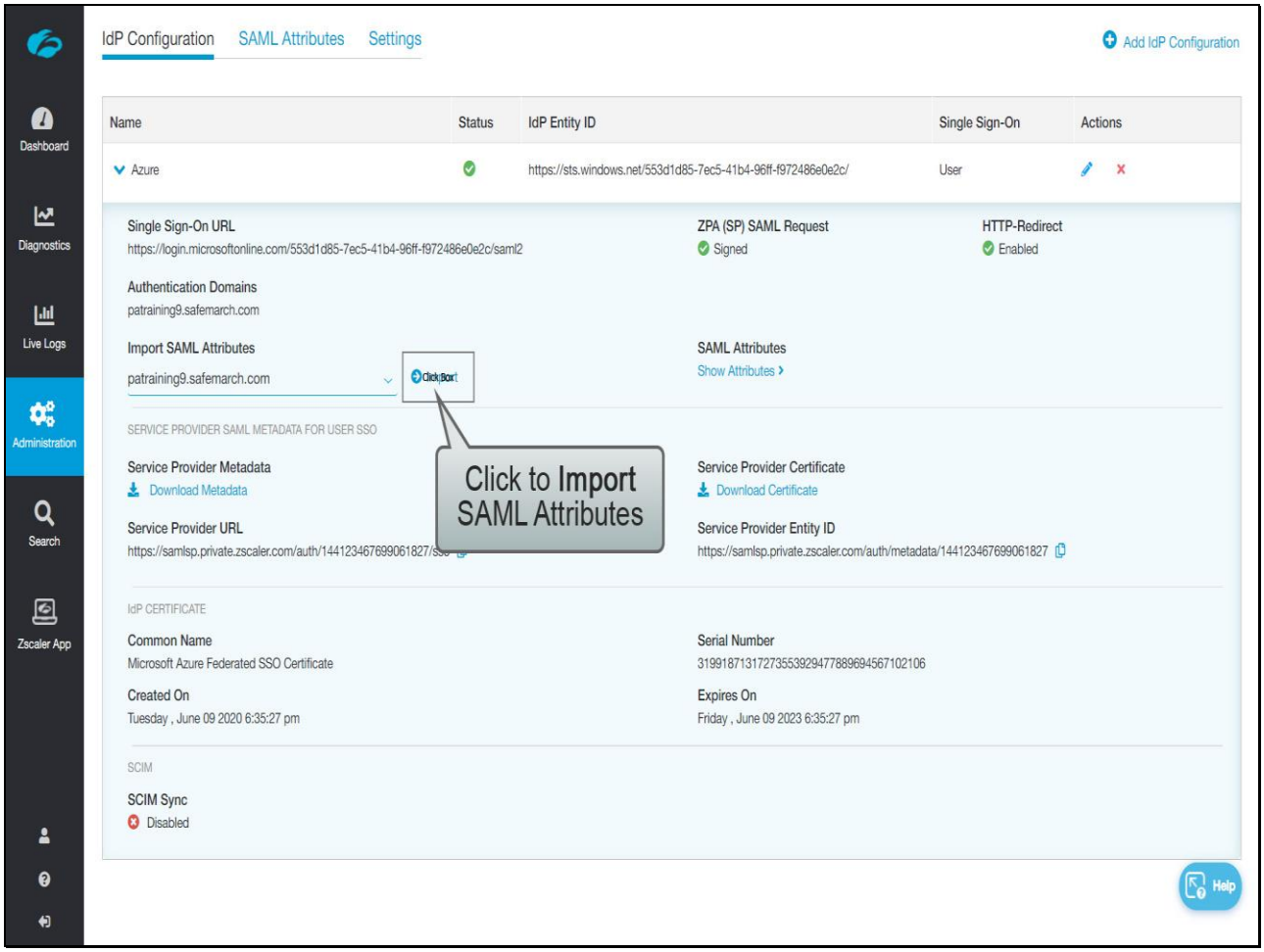
Slide 75 - Slide 75



Slide notes

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

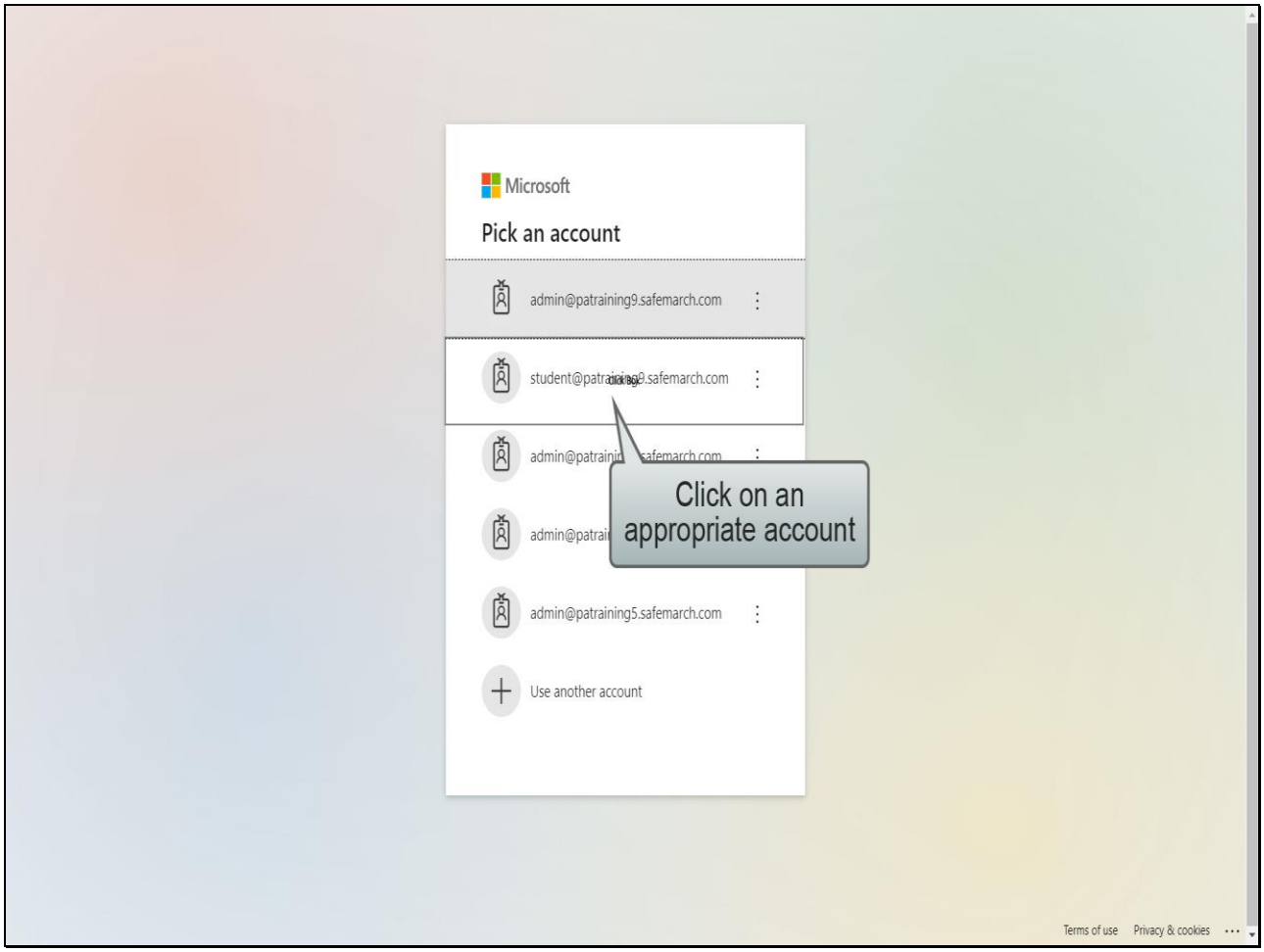
Slide 76 - Slide 76



Slide notes

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

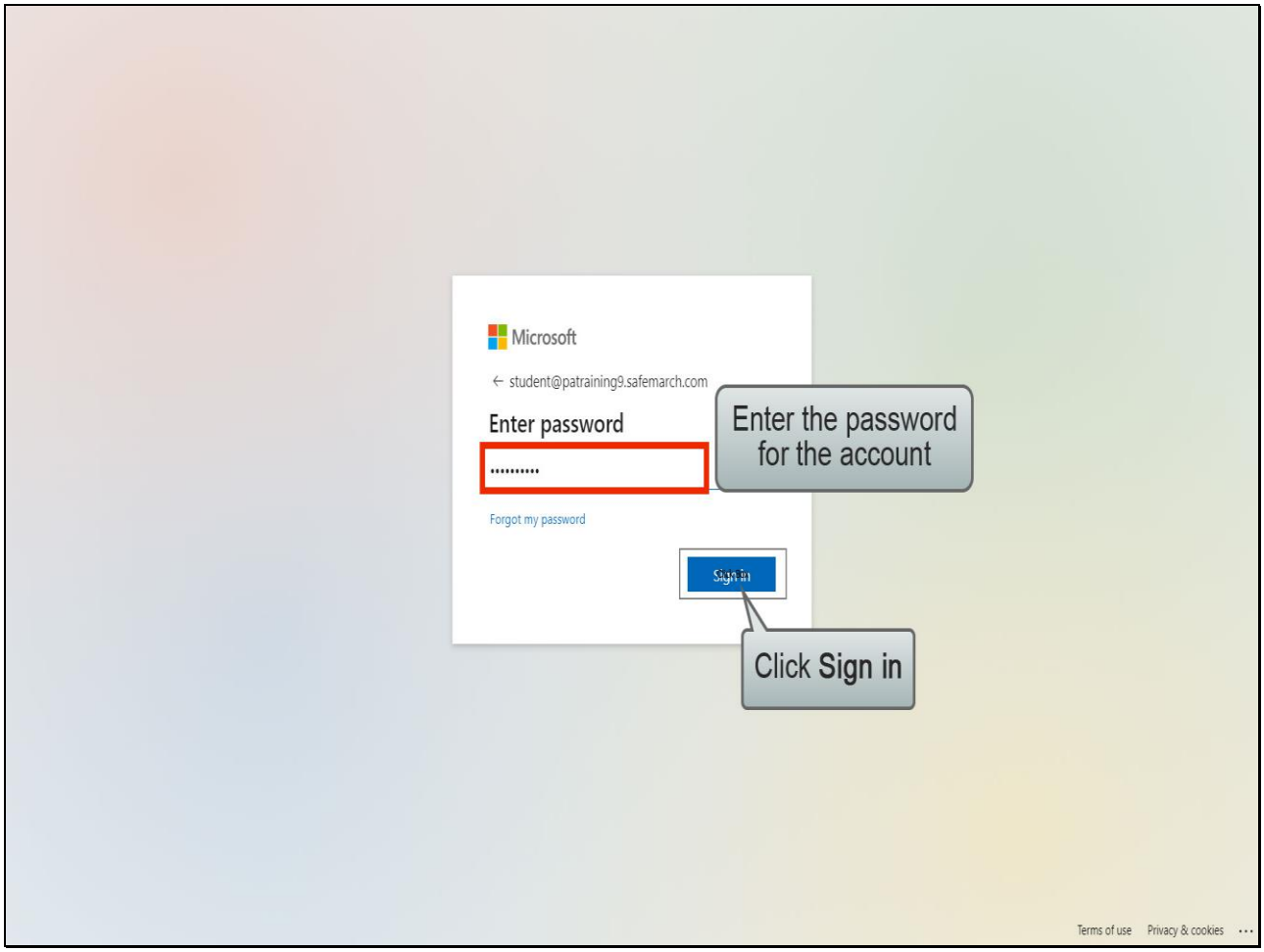
Slide 77 - Slide 77



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, ...

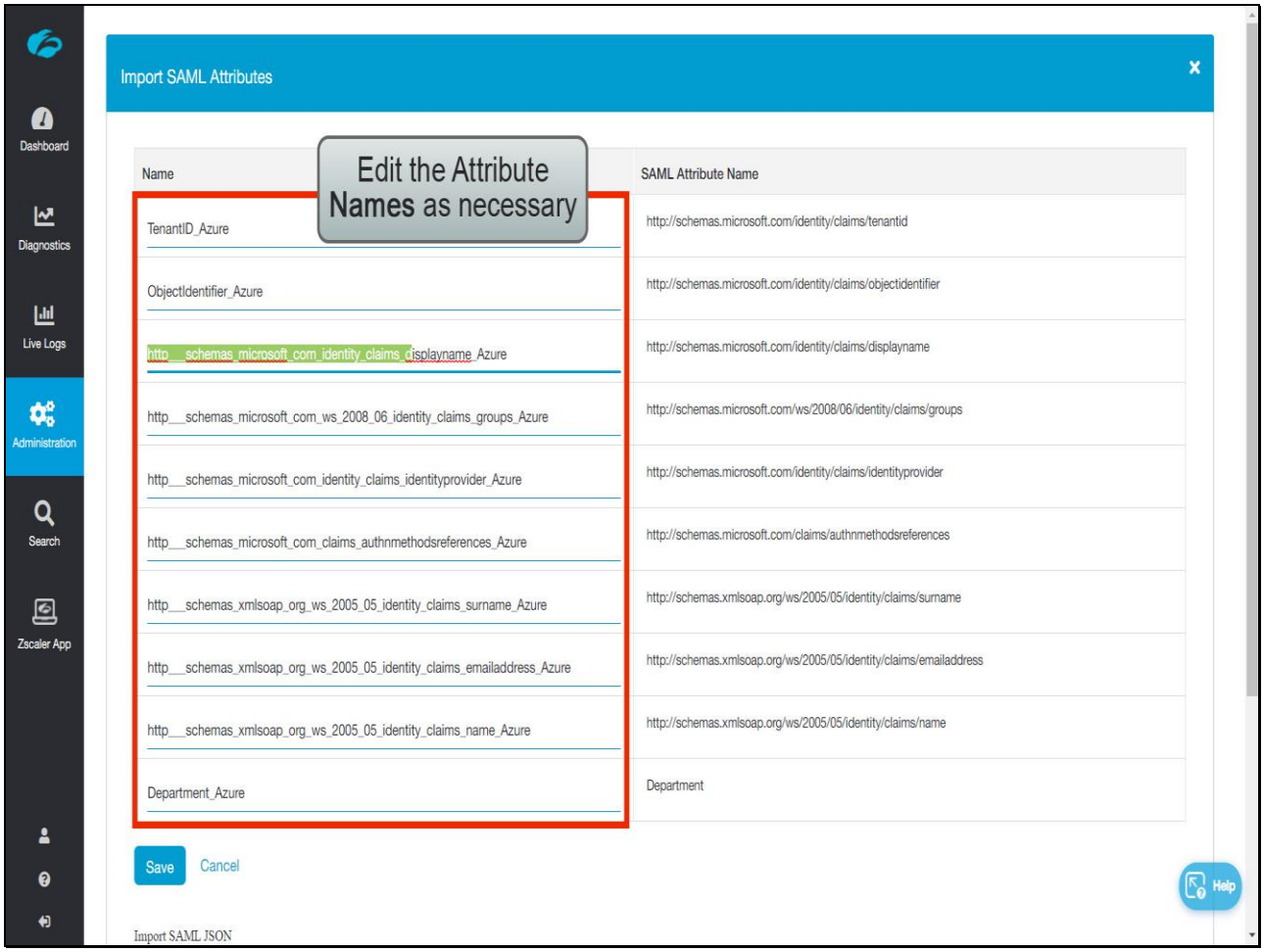
Slide 78 - Slide 78



Slide notes

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

Slide 79 - Slide 79

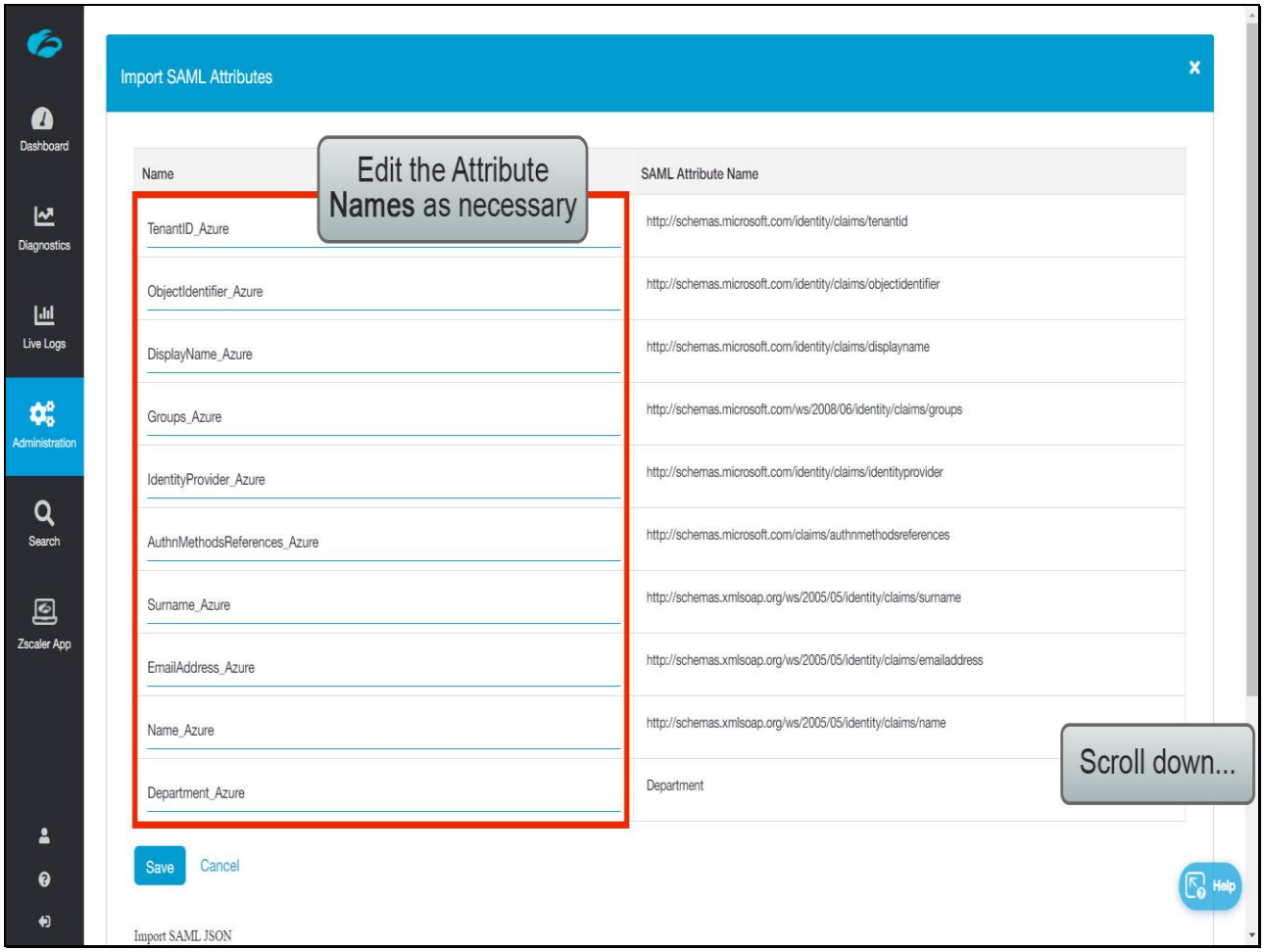


Slide notes

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.

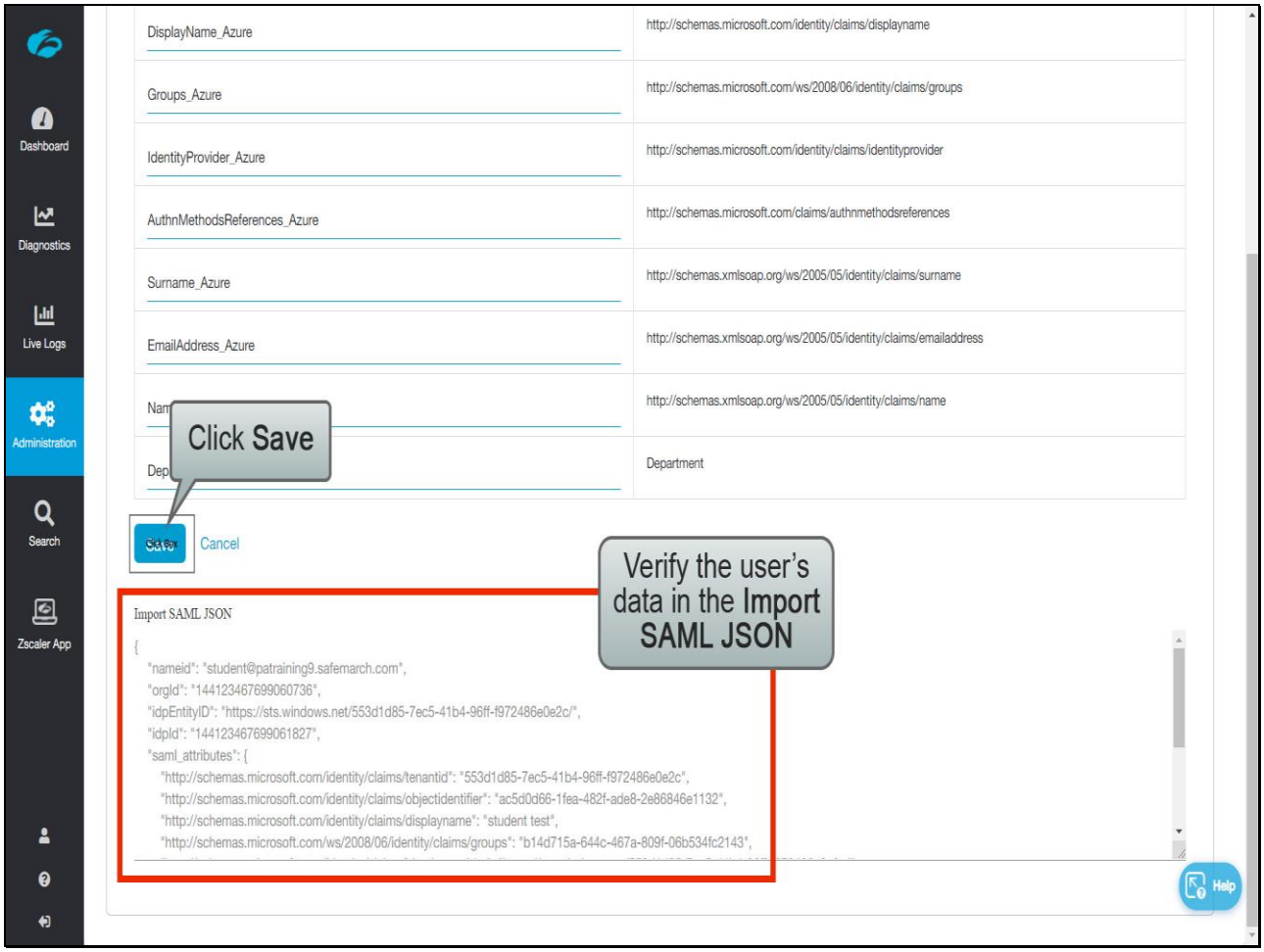
Slide 80 - Slide 80



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

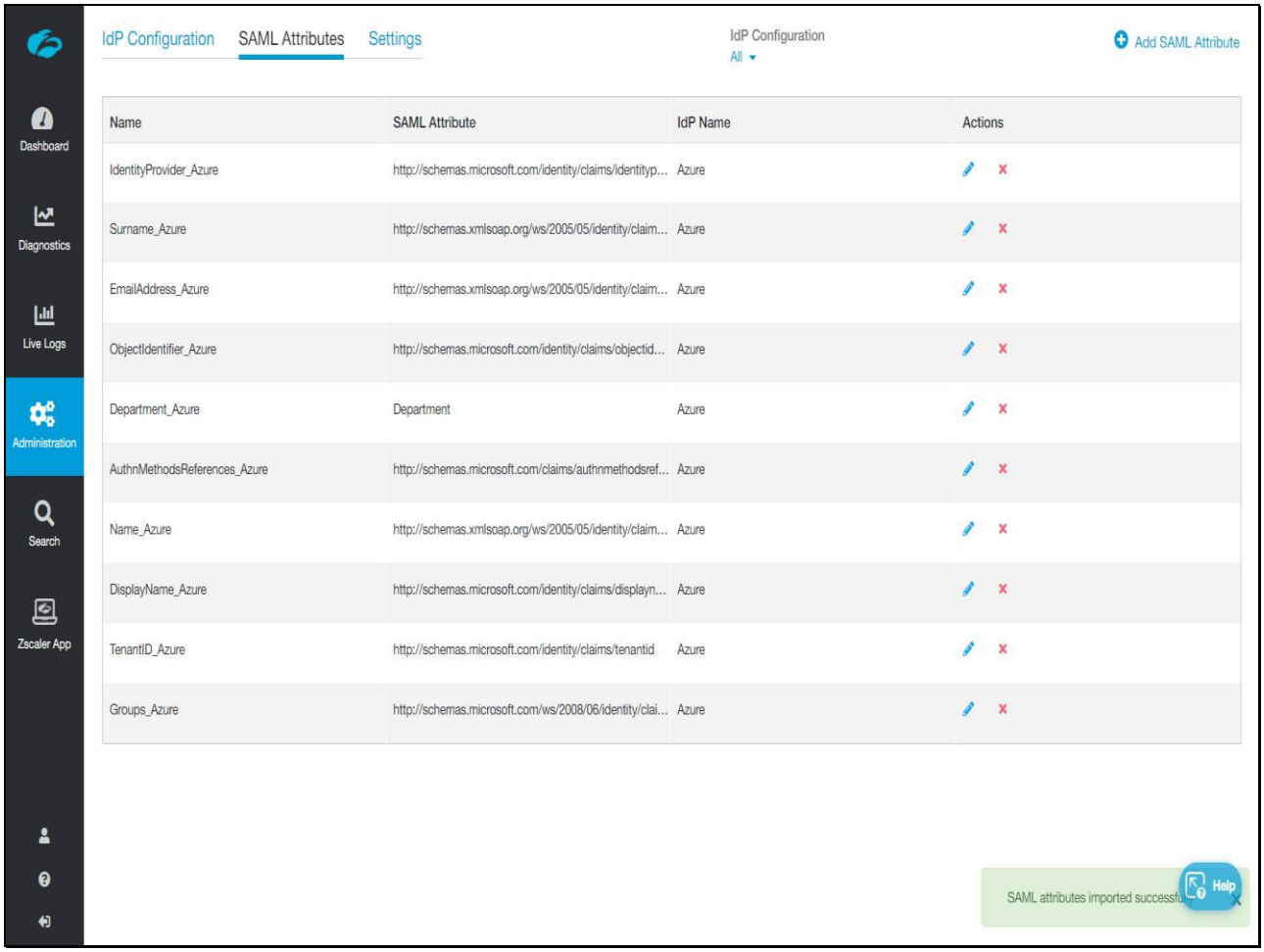


Slide notes

...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.

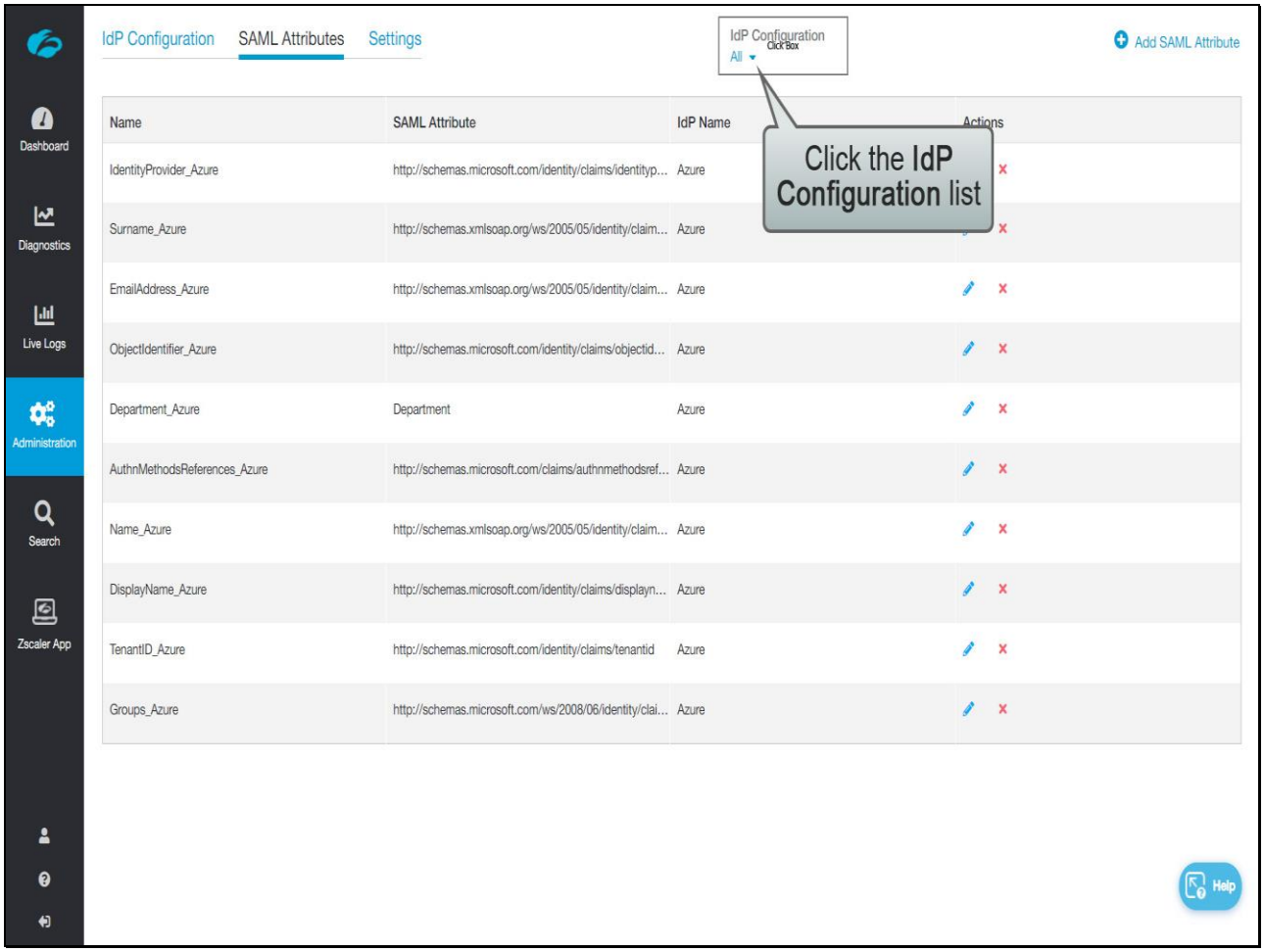
Once you are happy, click to **Save** the **SAML Attributes**.

Slide 82 - Slide 82



Slide notes

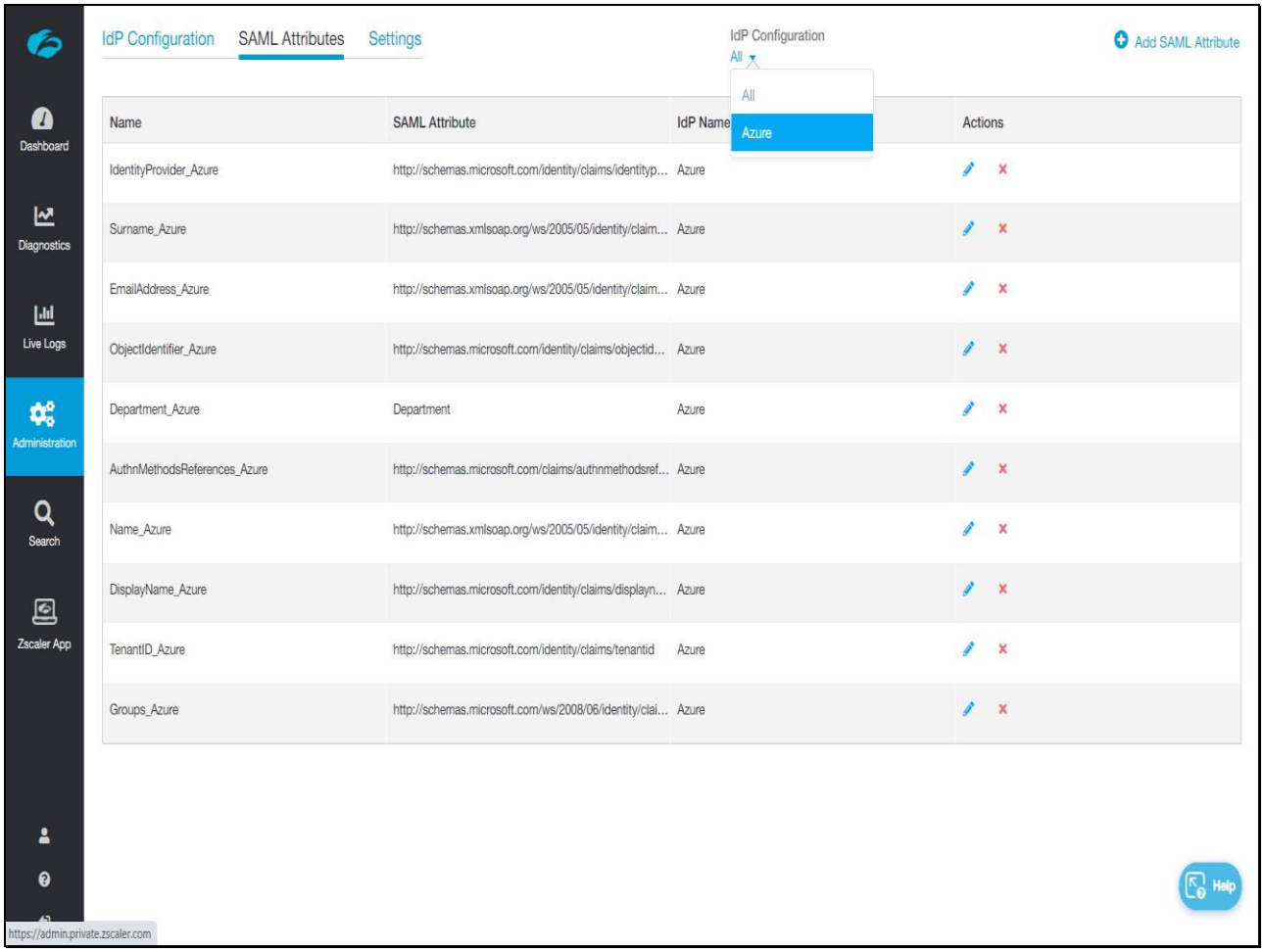
Slide 83 - Slide 83



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



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.

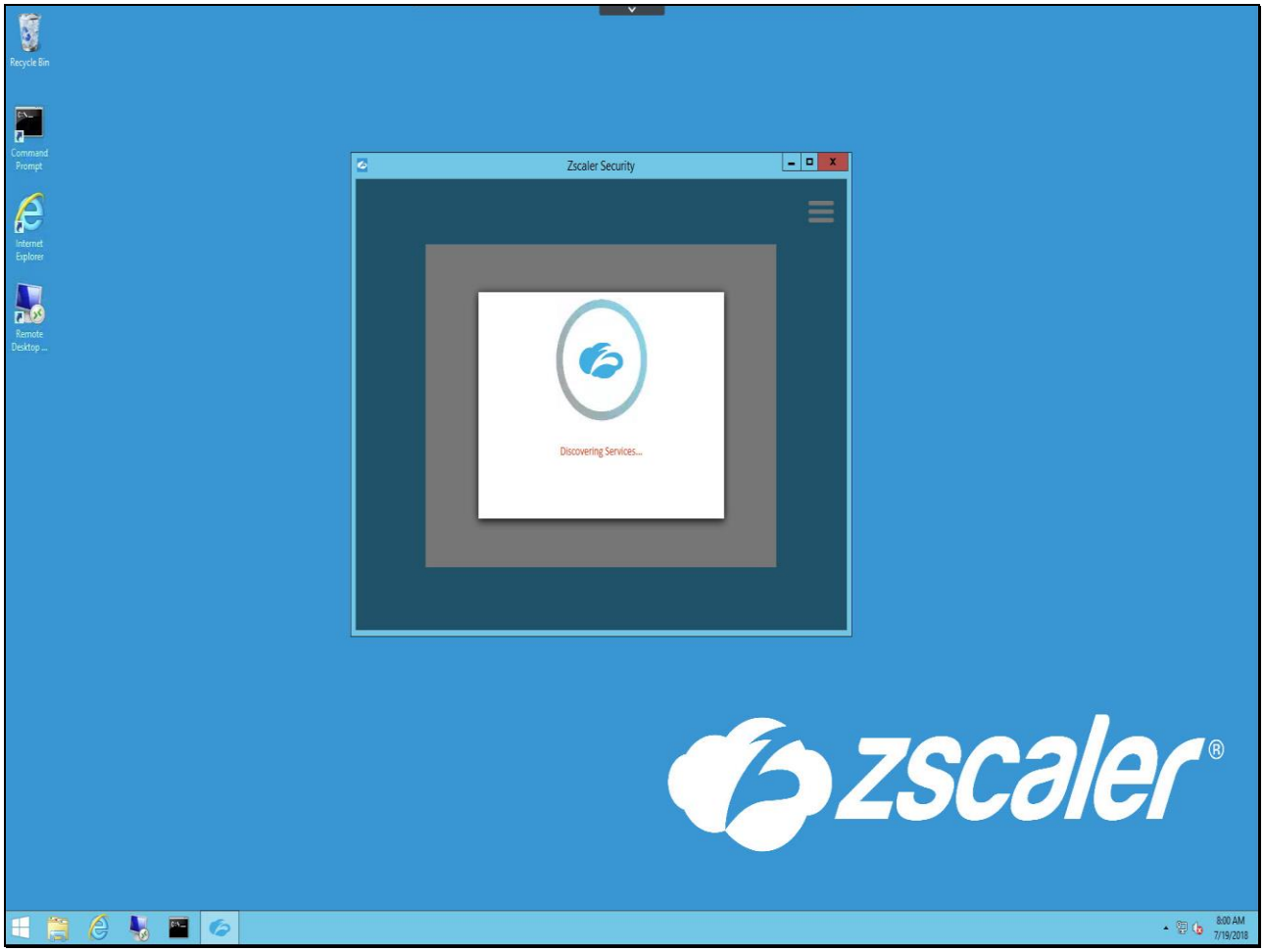
This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler App UI. You will be asked to select the appropriate menu options to navigate the UI. You may also use the Play control to proceed to the next step.

Slide 86 - Slide 86

Slide notes

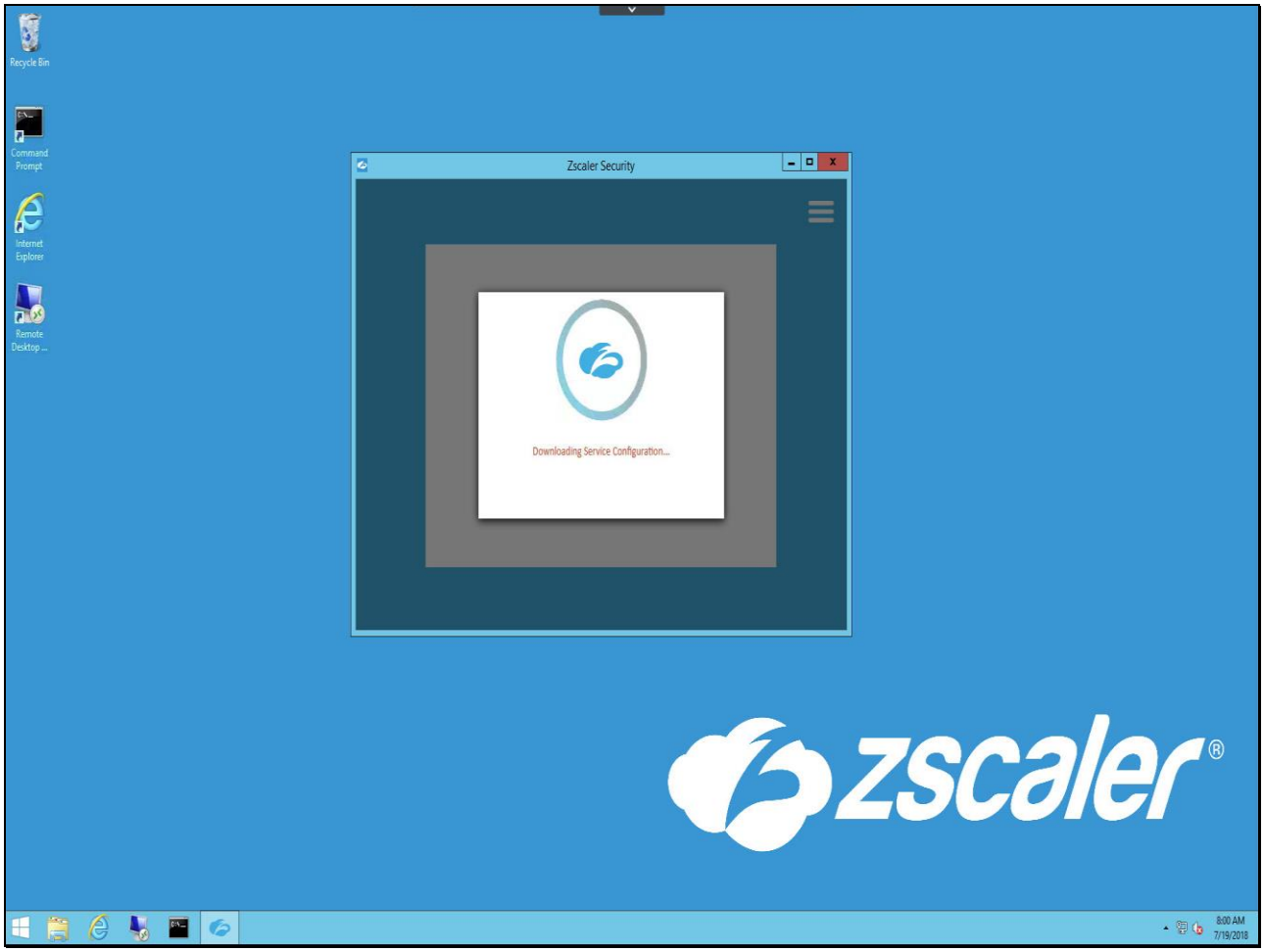
On a client machine that has the Zscaler App installed on it (PC or mobile, for this example we will use a Windows client), run the App, provide valid end user credentials (in the form of an email address) and click **Sign In**.

Slide 87 - Slide 87



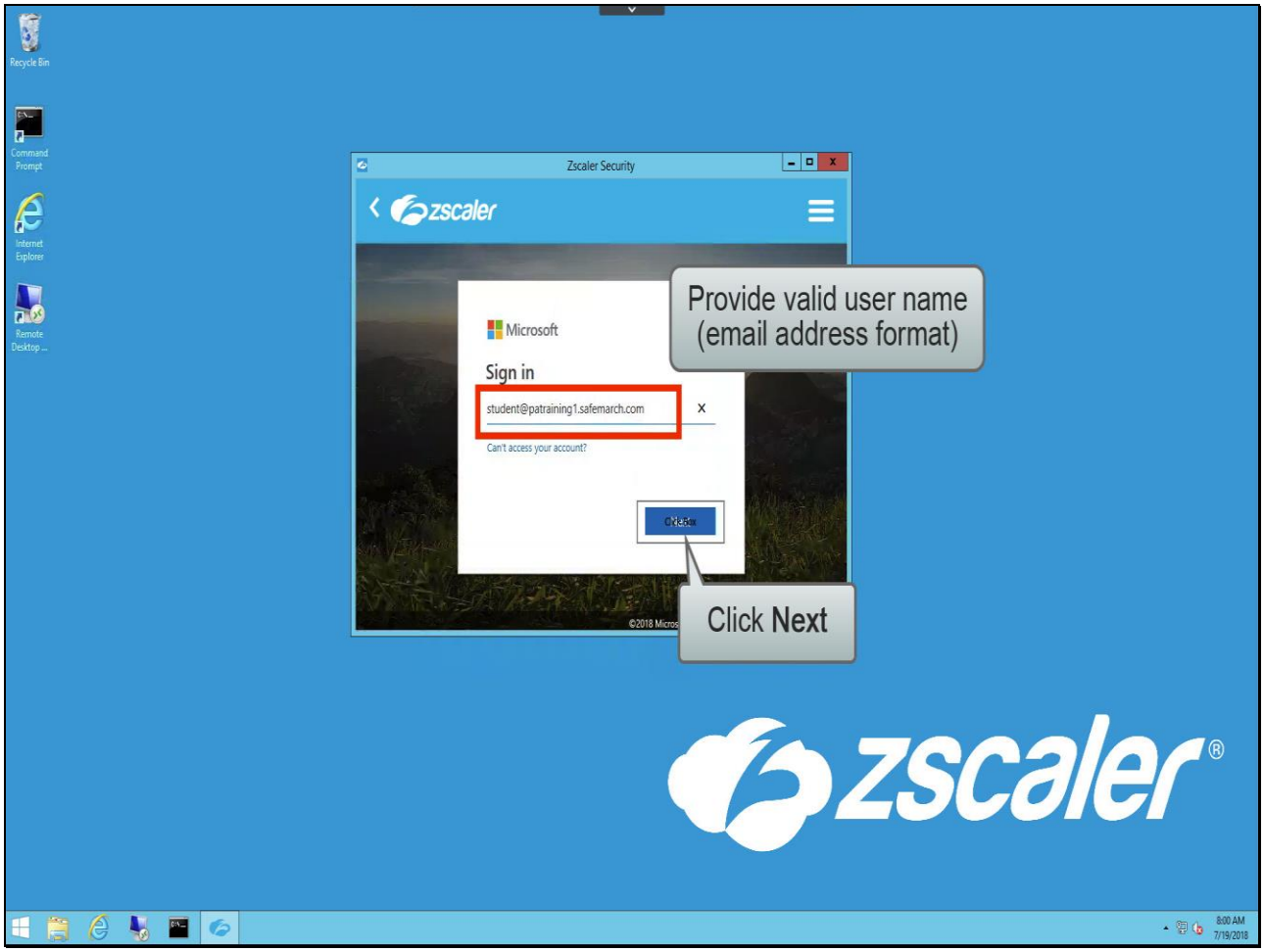
Slide notes

Slide 88 - Slide 88



Slide notes

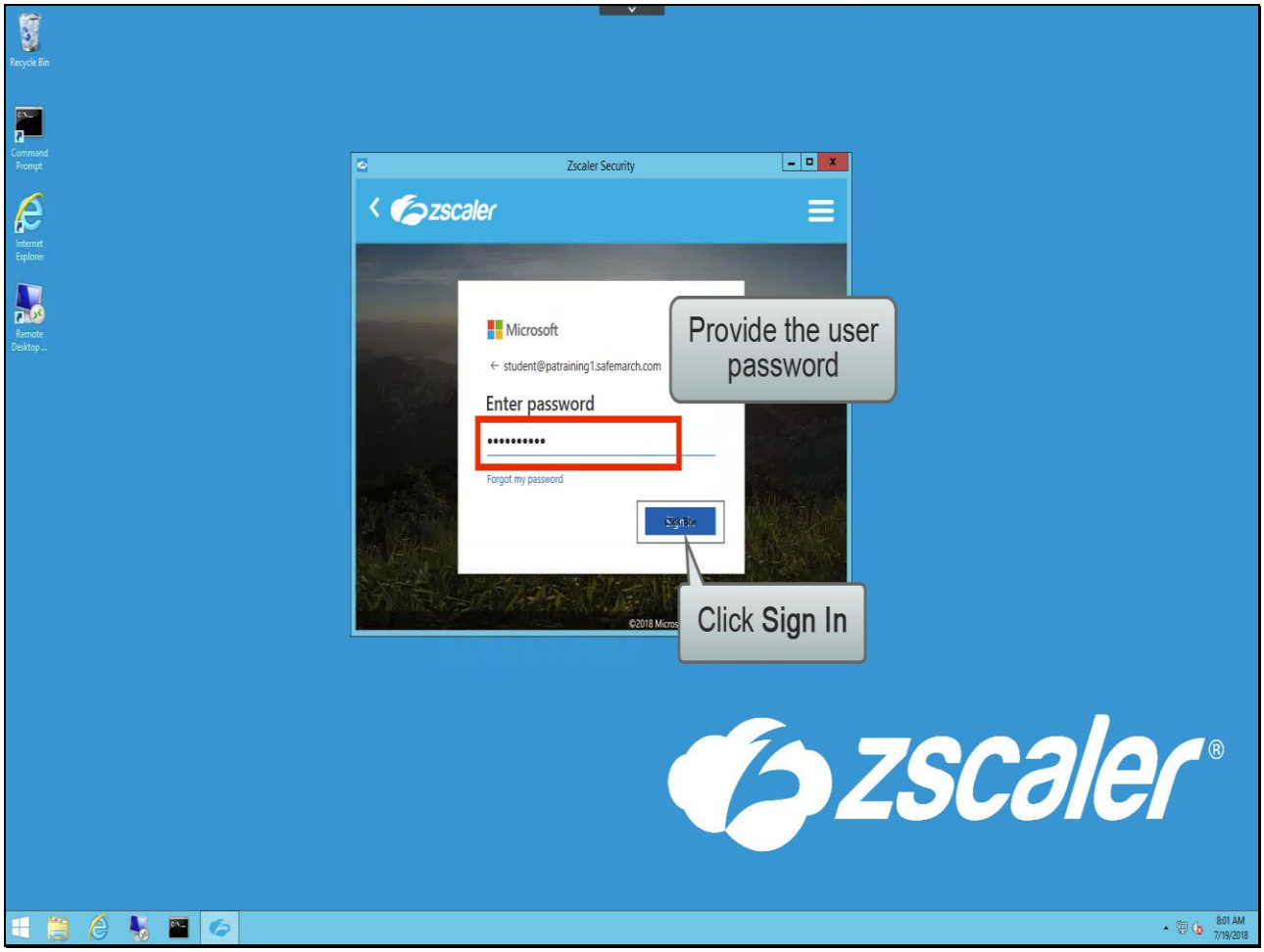
Slide 89 - Slide 89



Slide notes

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

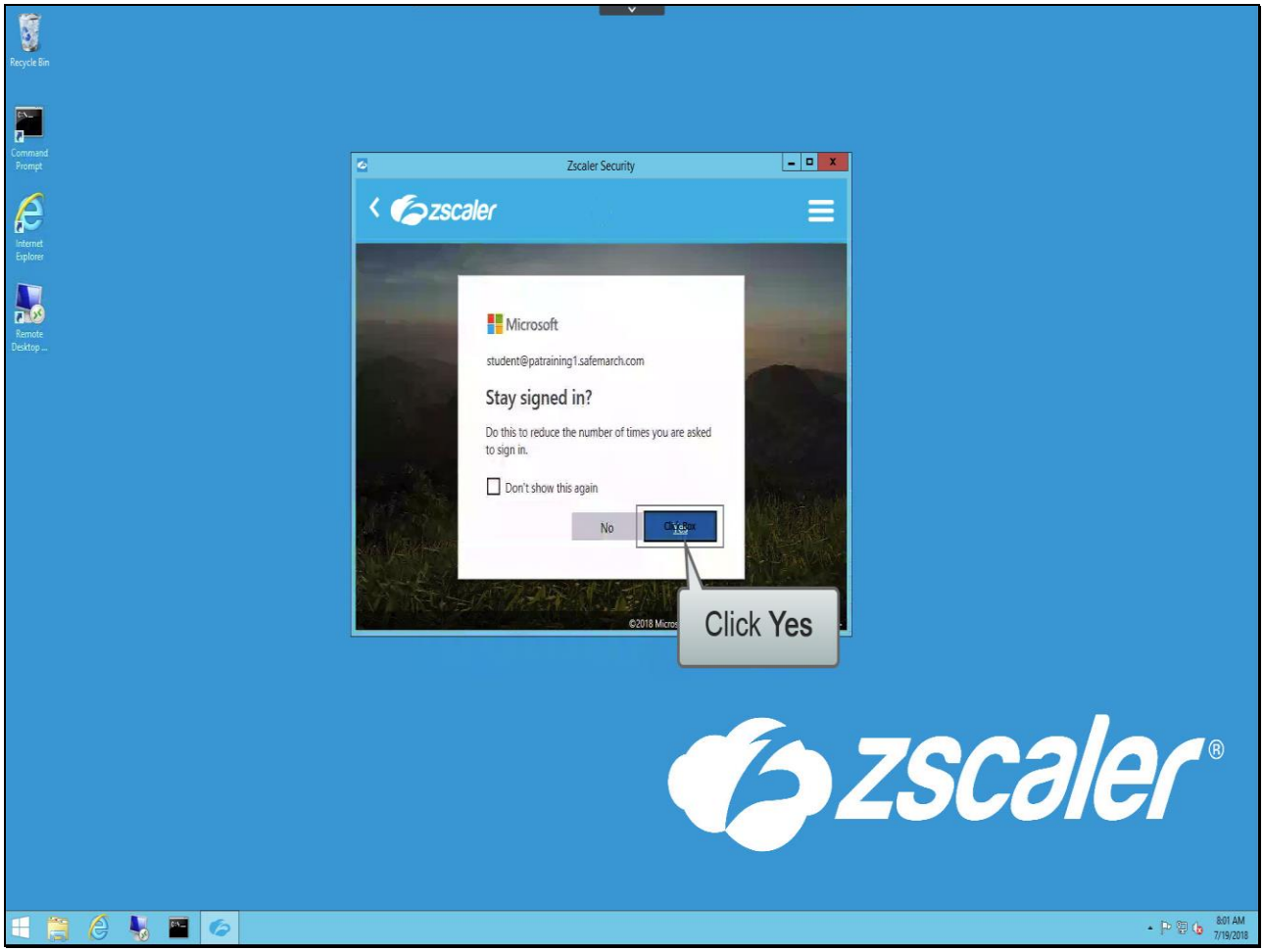
Slide 90 - Slide 90



Slide notes

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

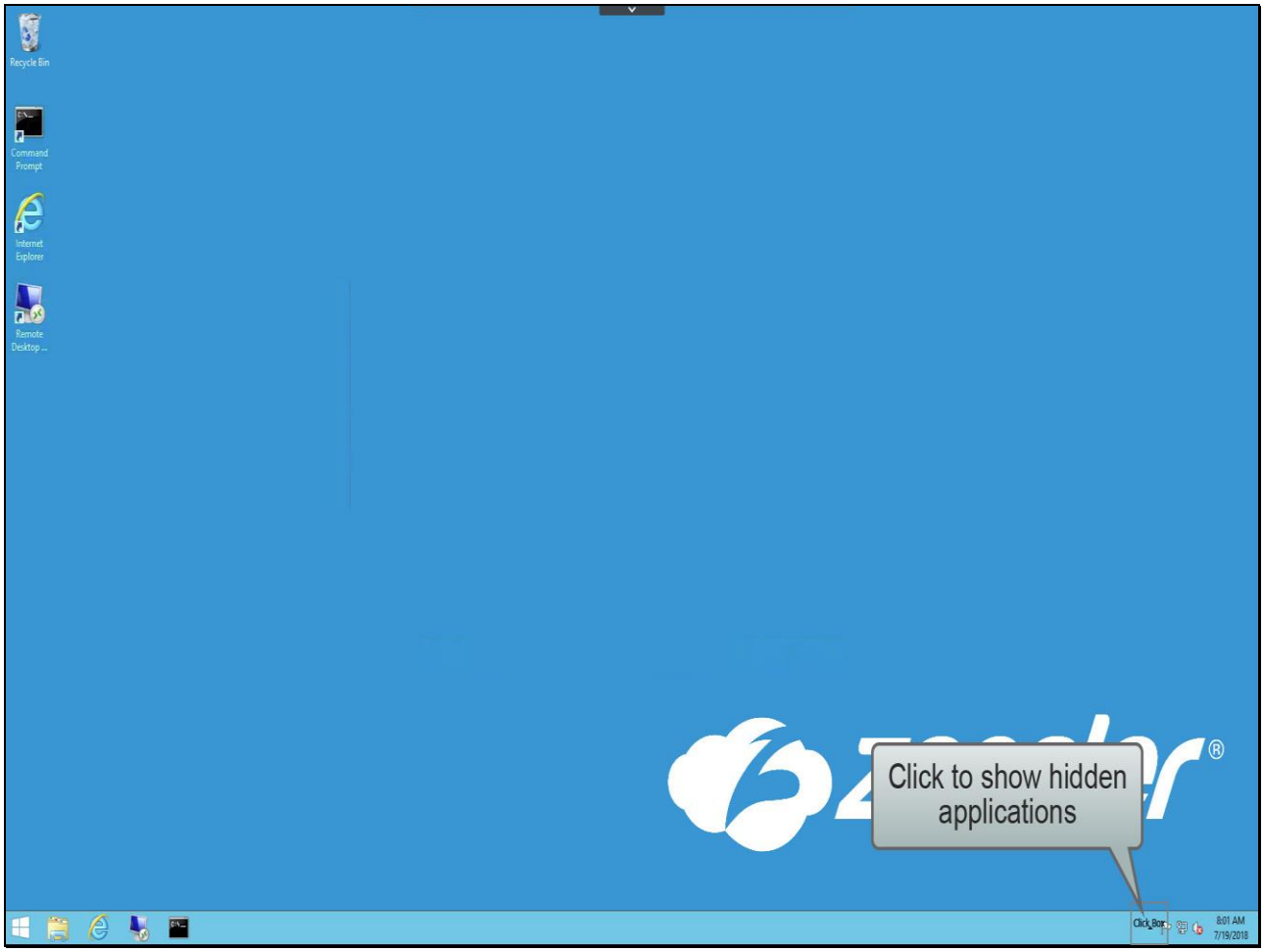
Slide 91 - Slide 91



Slide notes

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

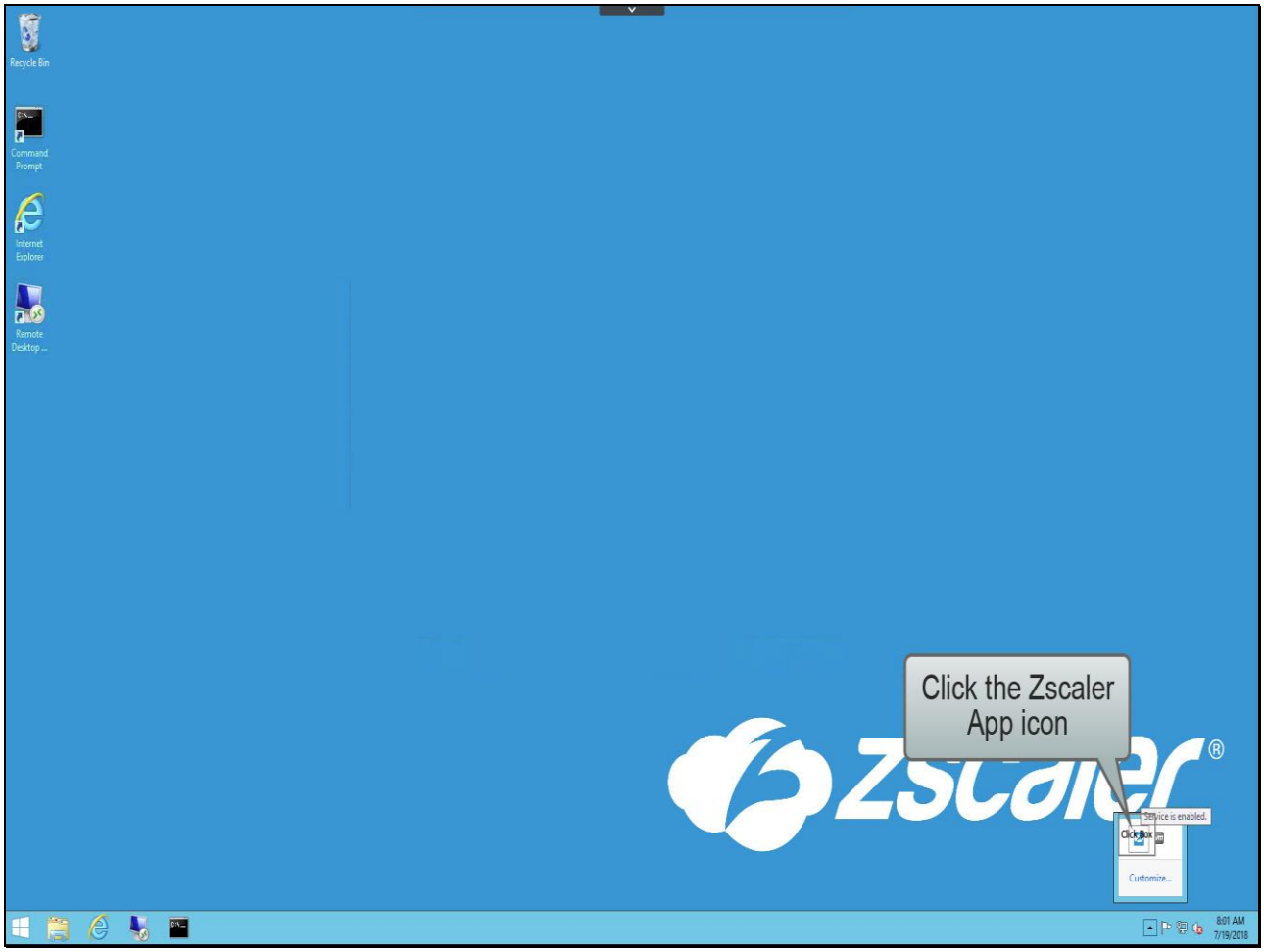
Slide 92 - Slide 92



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, …

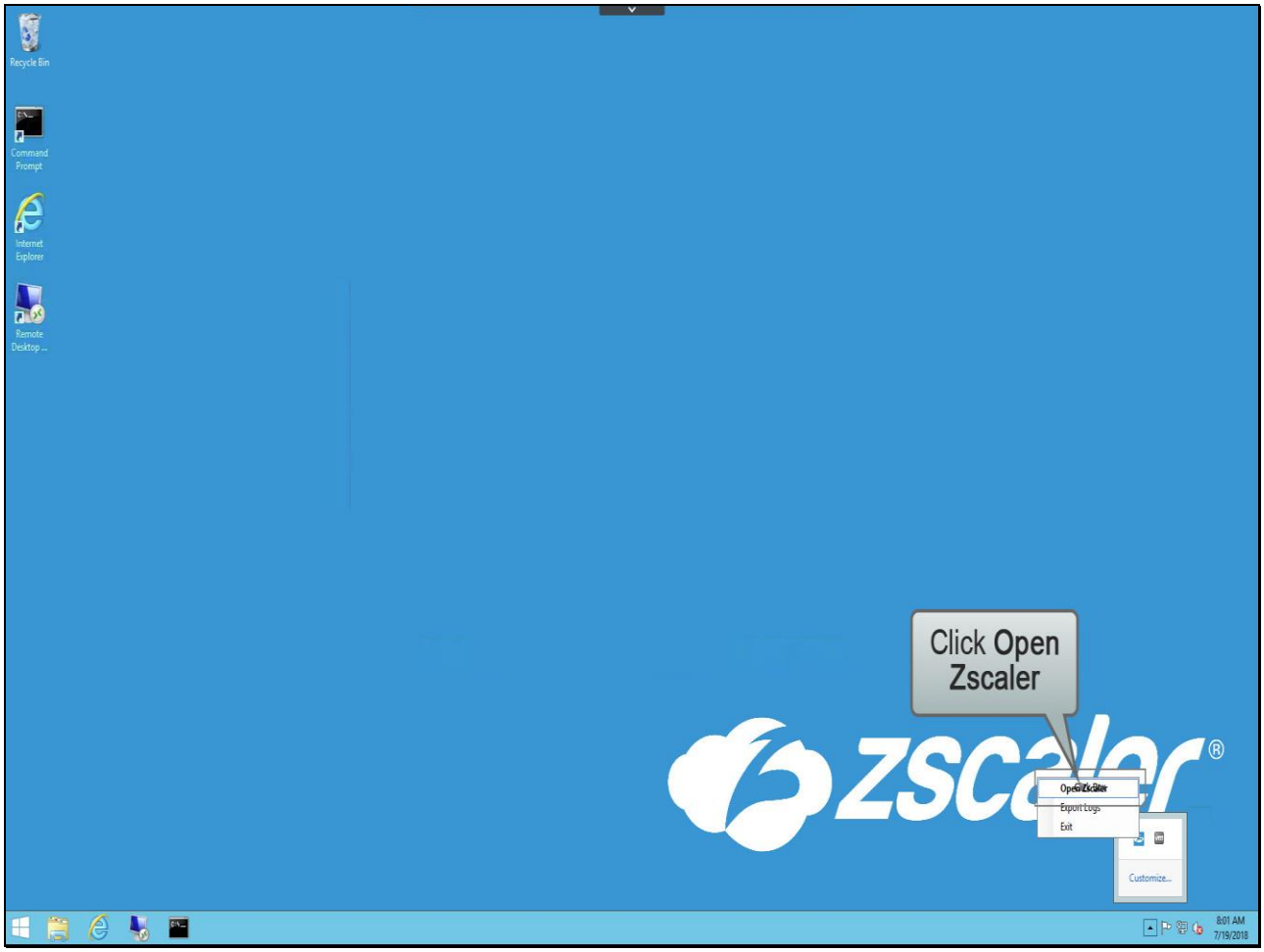
Slide 93 - Slide 93



Slide notes

…then click on the Zscaler App icon, …

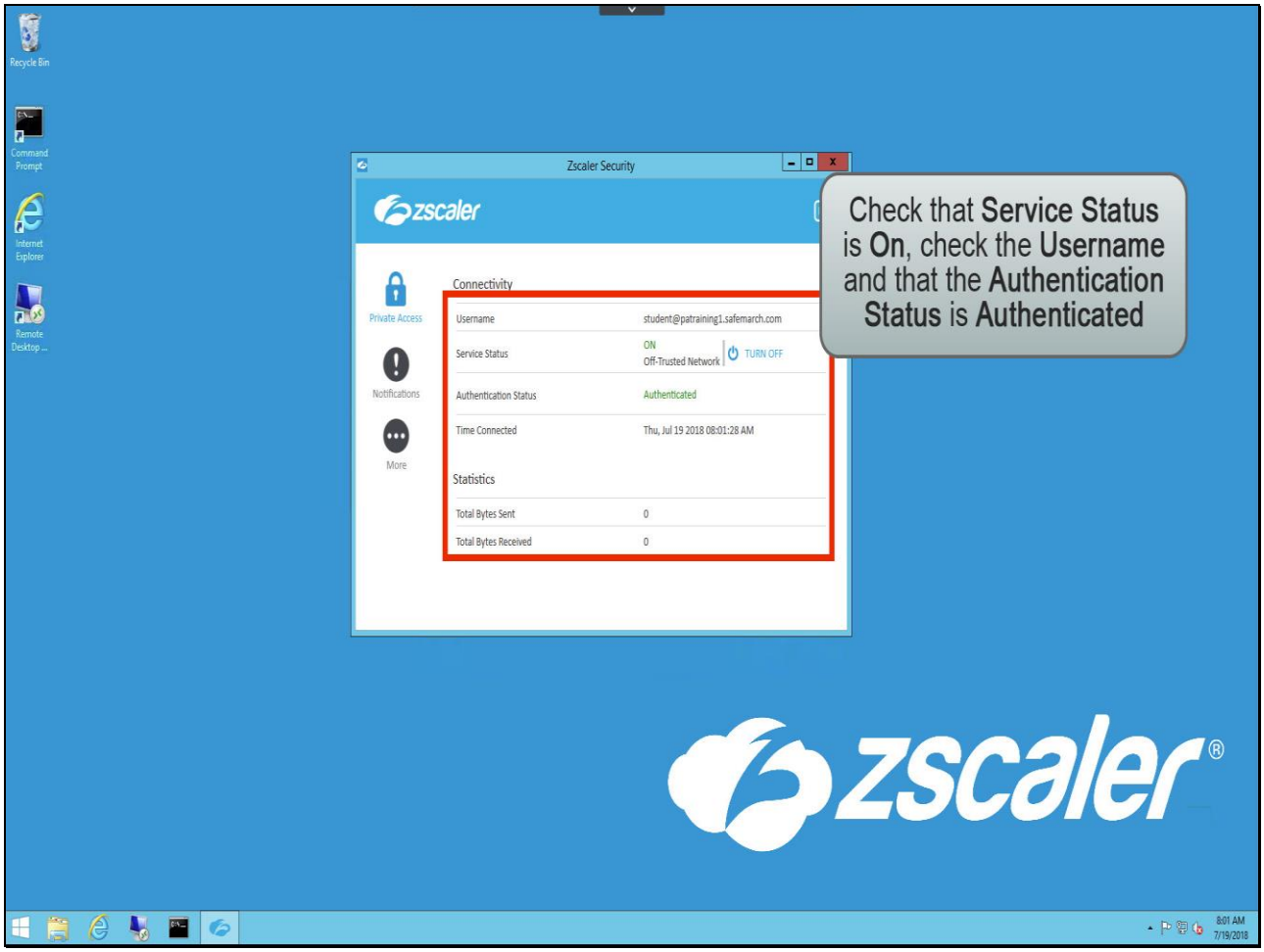
Slide 94 - Slide 94



Slide notes

…and click **Open Zscaler**.

Slide 95 - Slide 95

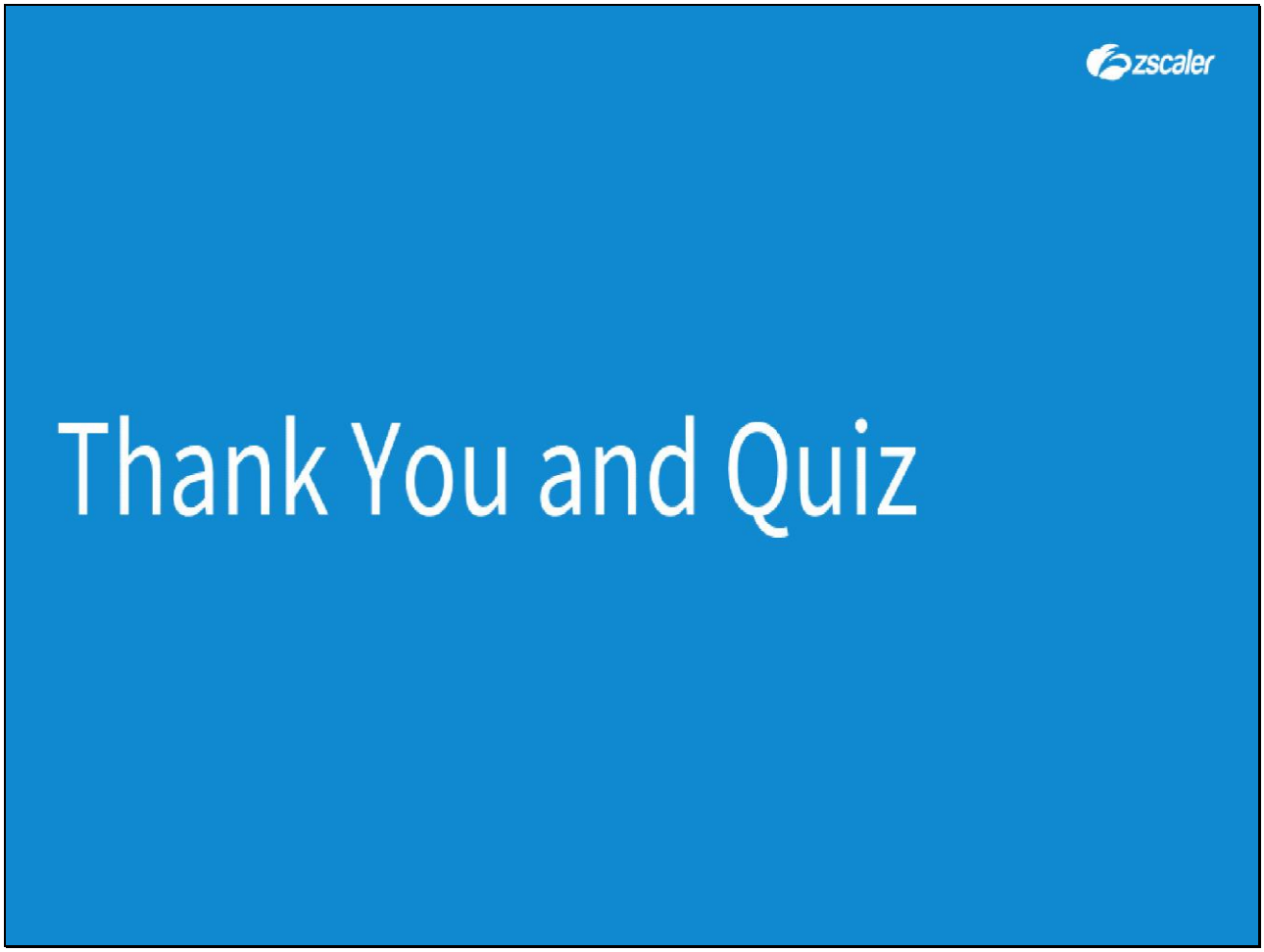


Slide notes

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.