

Slide 1 - Zscaler Private Access



# Zscaler Private Access

## Authentication with SAML – ADFS

©2019 Zscaler, Inc. All rights reserved.

### Slide notes

Welcome to this training module on configuring ZPA to use an ADFS server for authenticating users.

## Slide 2 - Navigating the eLearning Module

## Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal Dashboard. At the top right is the Zscaler logo. Below it, the title "Navigating the eLearning Module" is displayed. The dashboard features several data visualizations: a donut chart for "Cloud Application Classes" showing 391.3 MB (100%), another donut chart for "Top URL Categories" showing 16.8 K (100%), a list of "Top Users" with demo-vh1@zscaler.com at the top, and sections for "Streaming Media Applications" (Twitter, Pinterest, WordPress, MySpace, Blogger) and "Top Advanced Threats". A large video player control bar is overlaid on the bottom of the dashboard, containing the following controls: "Play/Pause", "Previous Slide", "Next Slide", "Fast Forward", "Progress Bar", "Audio On/Off", and "Closed Captioning". An "Exit" button is also highlighted in the top right corner of the video player area.

## Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play and Pause**, **Previous**, **Next slide** and **Fast Forward**. You can also **Mute** the audio or enable **Closed Captioning** which will cause a transcript of the module to be displayed on the screen. Finally, you can click the X button at the top to exit.

## Slide 3 - Agenda

# Agenda

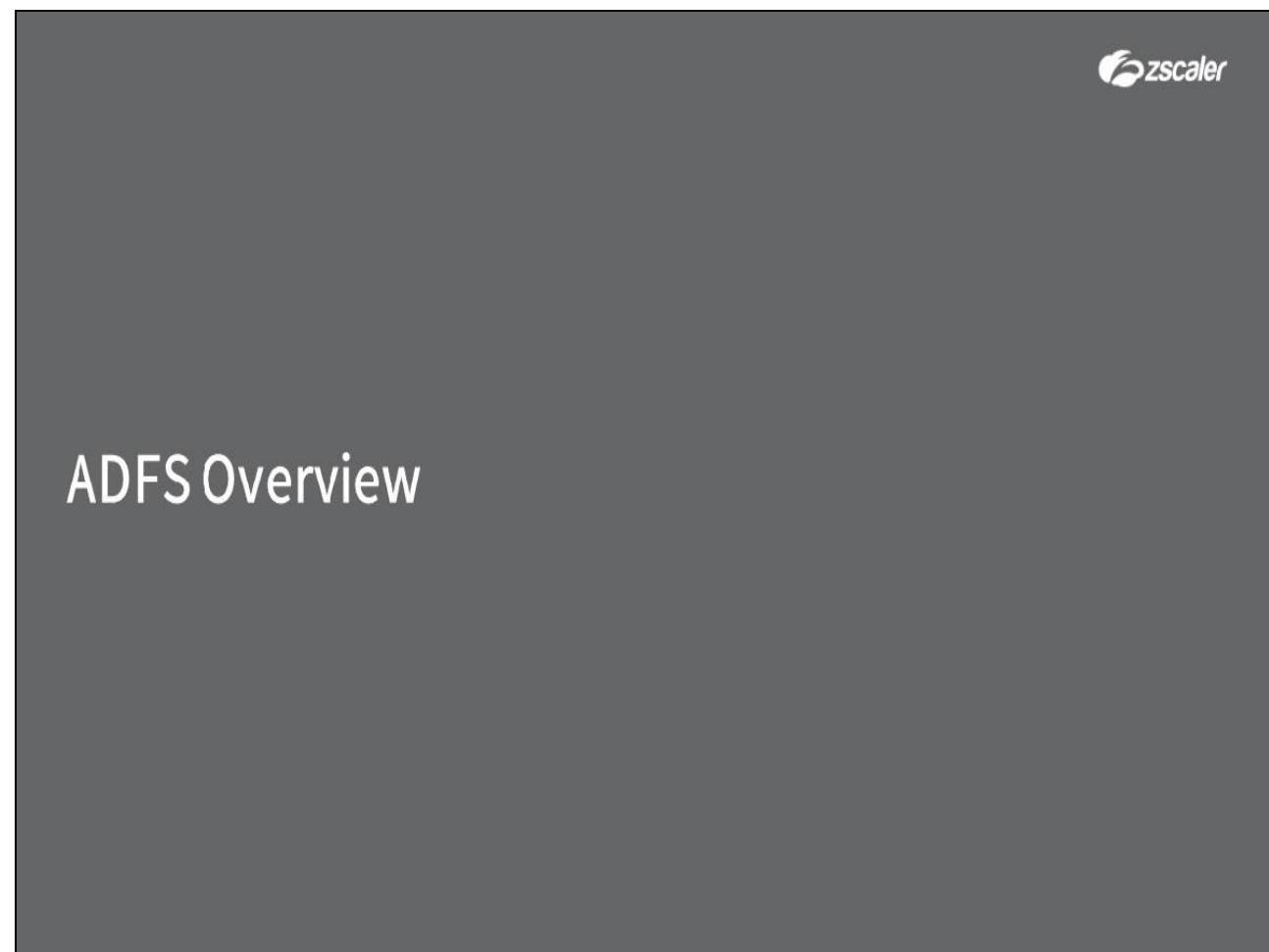


- ADFS Overview
- Configuring ADFS
  - A. Exporting the SP Metadata File
  - B. Adding a Relying Party Trust
  - C. Adding a Claim Rule
  - D. Exporting the IdP Metadata File
  - E. Configuring IdP information in ZPA
  - F. Testing the Configuration

## Slide notes

In this module we will: Provide an overview of the ADFS solution; look at the configuration of ADFS for ZPA; and look at the 6 steps to add ADFS to ZPA as an IdP.

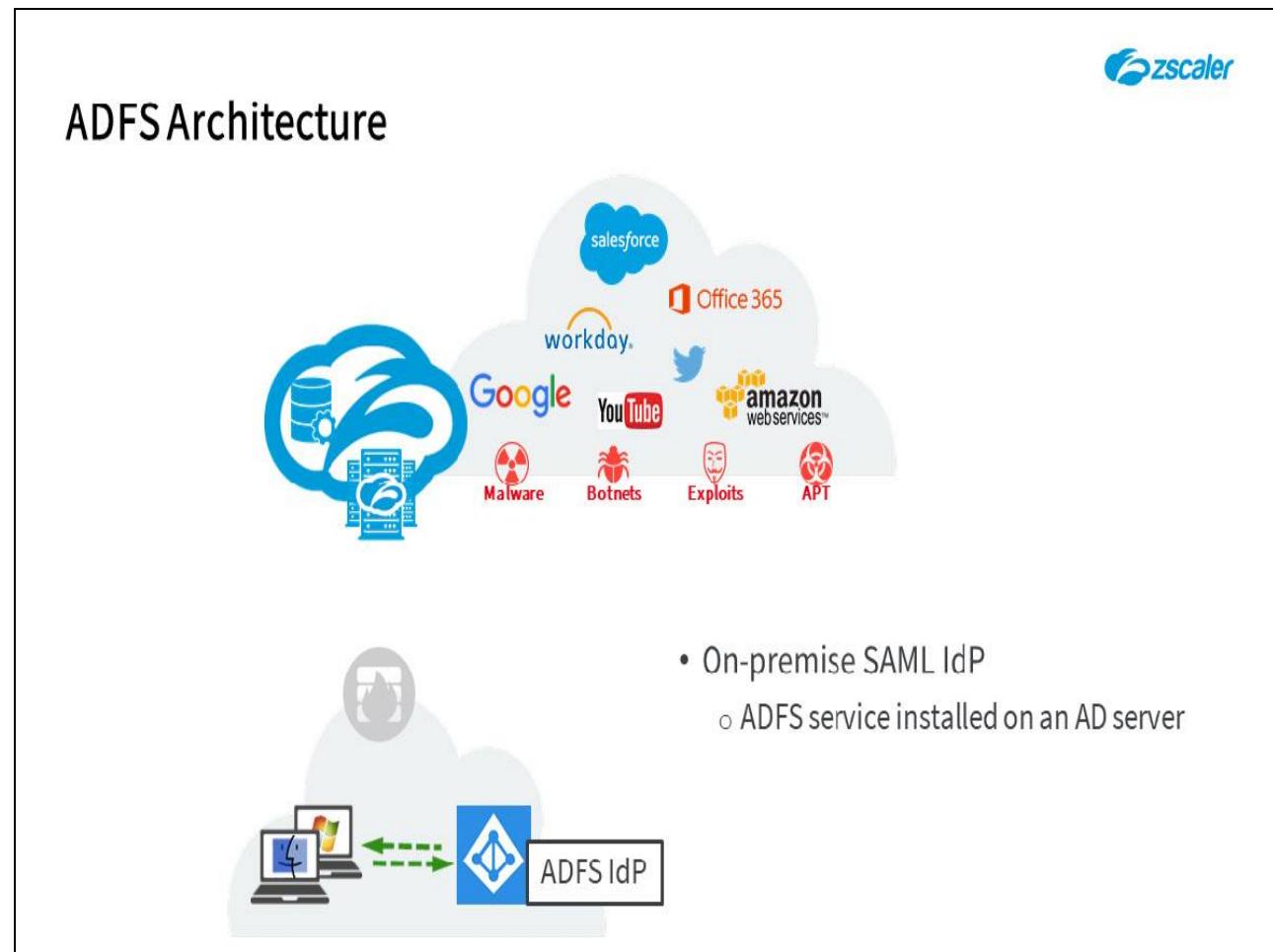
Slide 4 - ADFS Overview



**Slide notes**

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

## Slide 5 - ADFS Architecture

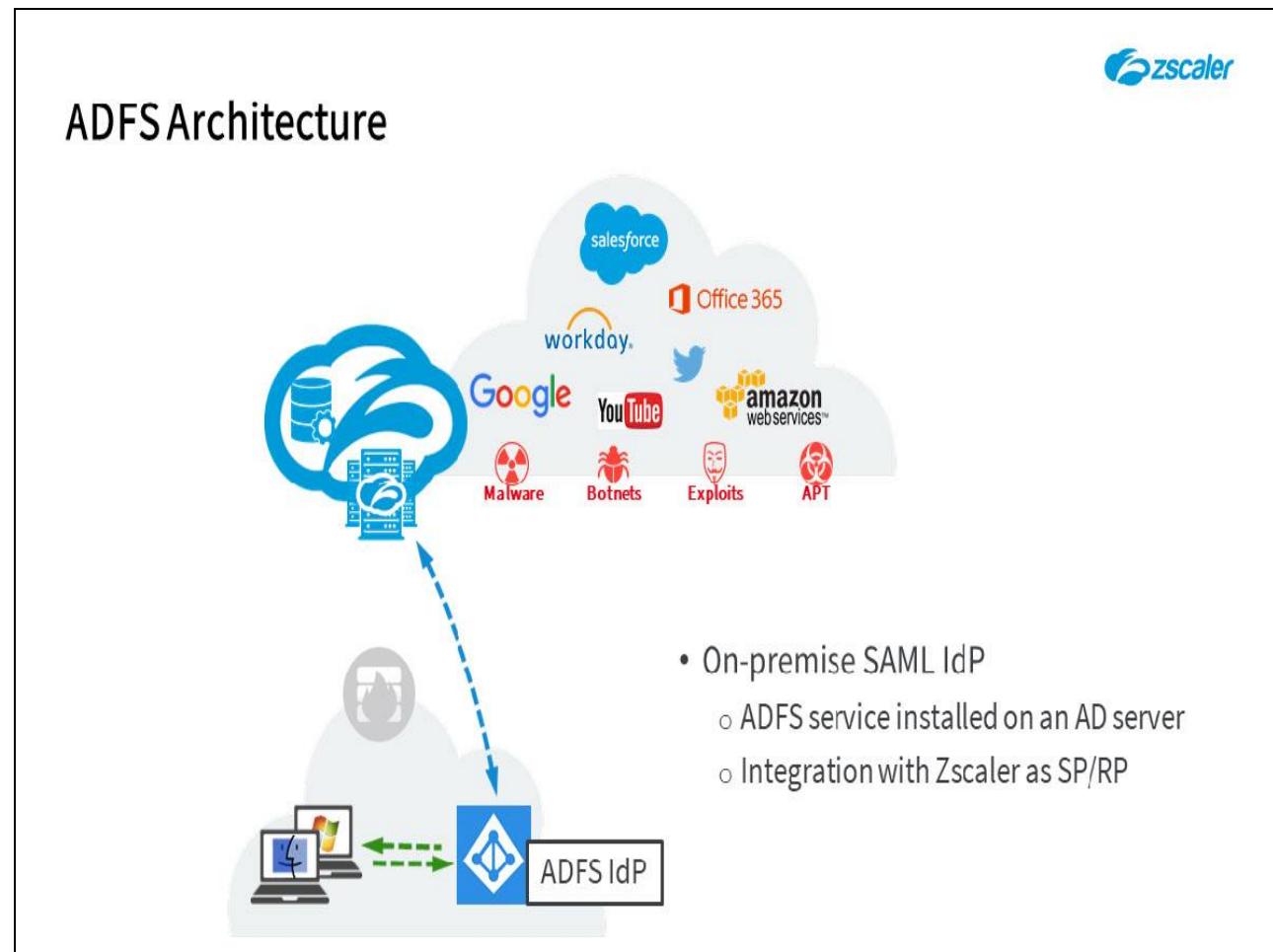


## Slide notes

The Microsoft Active Directory Federated Services solution (ADFS), is an implementation of a standards-based SAML 2.0 IdP for end user SSO and is the primary on-premise example of a SAML IdP. ADFS is a service that can be installed and configured on any AD server at no extra cost.

Once enabled and configured, it is available for use for internal users (i.e. those that can reach the server across the LAN) for authentication to any SAML compliant Service Provider (or “Relying Party” in Microsoft-speak). User authentication can be **forms-based**, or for domain-joined machines can use the Integrated Windows Authentication method (IWA), or even multi-factor authentication (MFA).

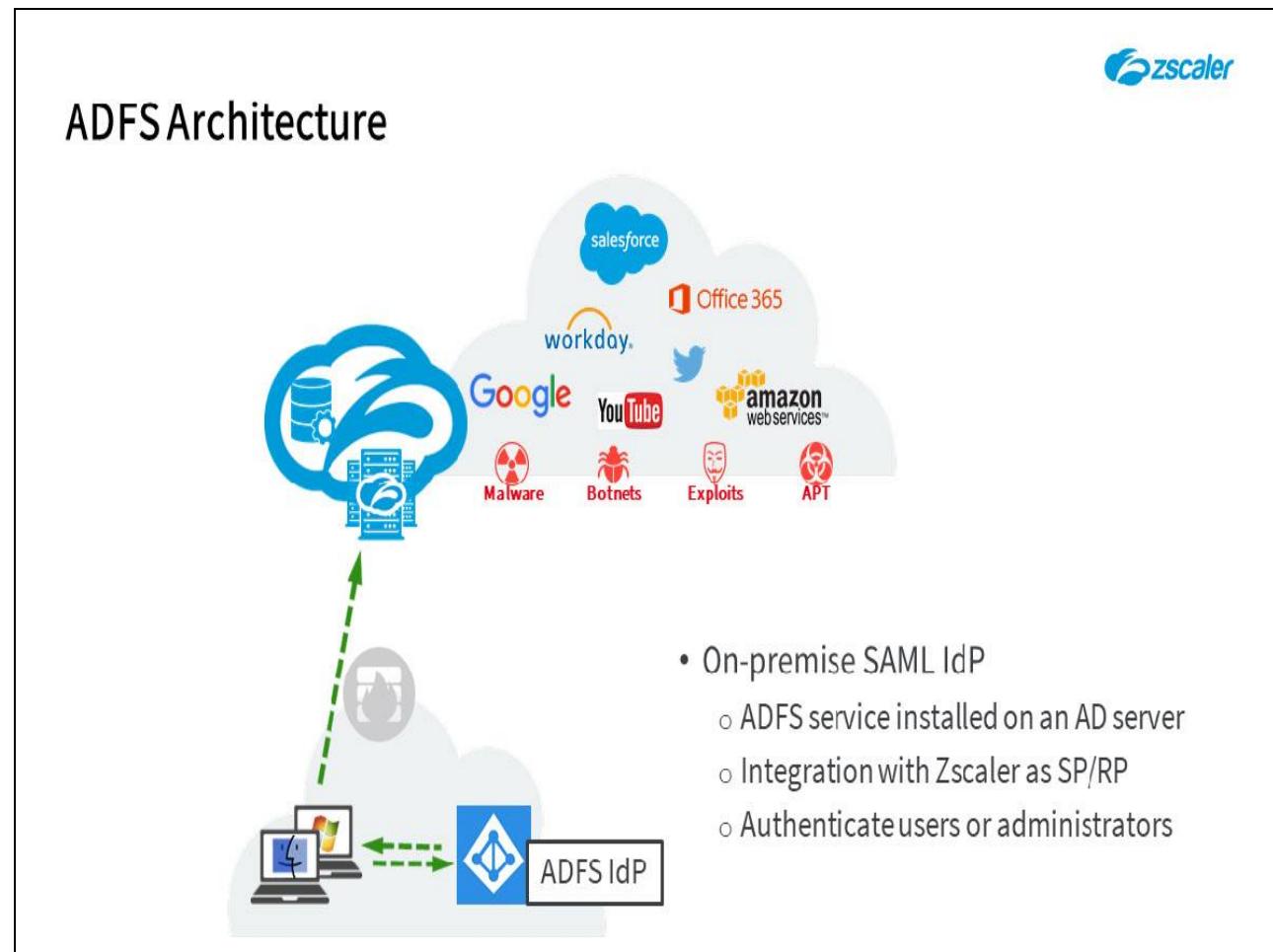
## Slide 6 - ADFS Architecture



## Slide notes

Authentication to Zscaler services (both ZIA and ZPA) can be done using a Microsoft ADFS solution, once Zscaler has been added to ADFS as a valid SP/RP, and the necessary trust relationship has been established.

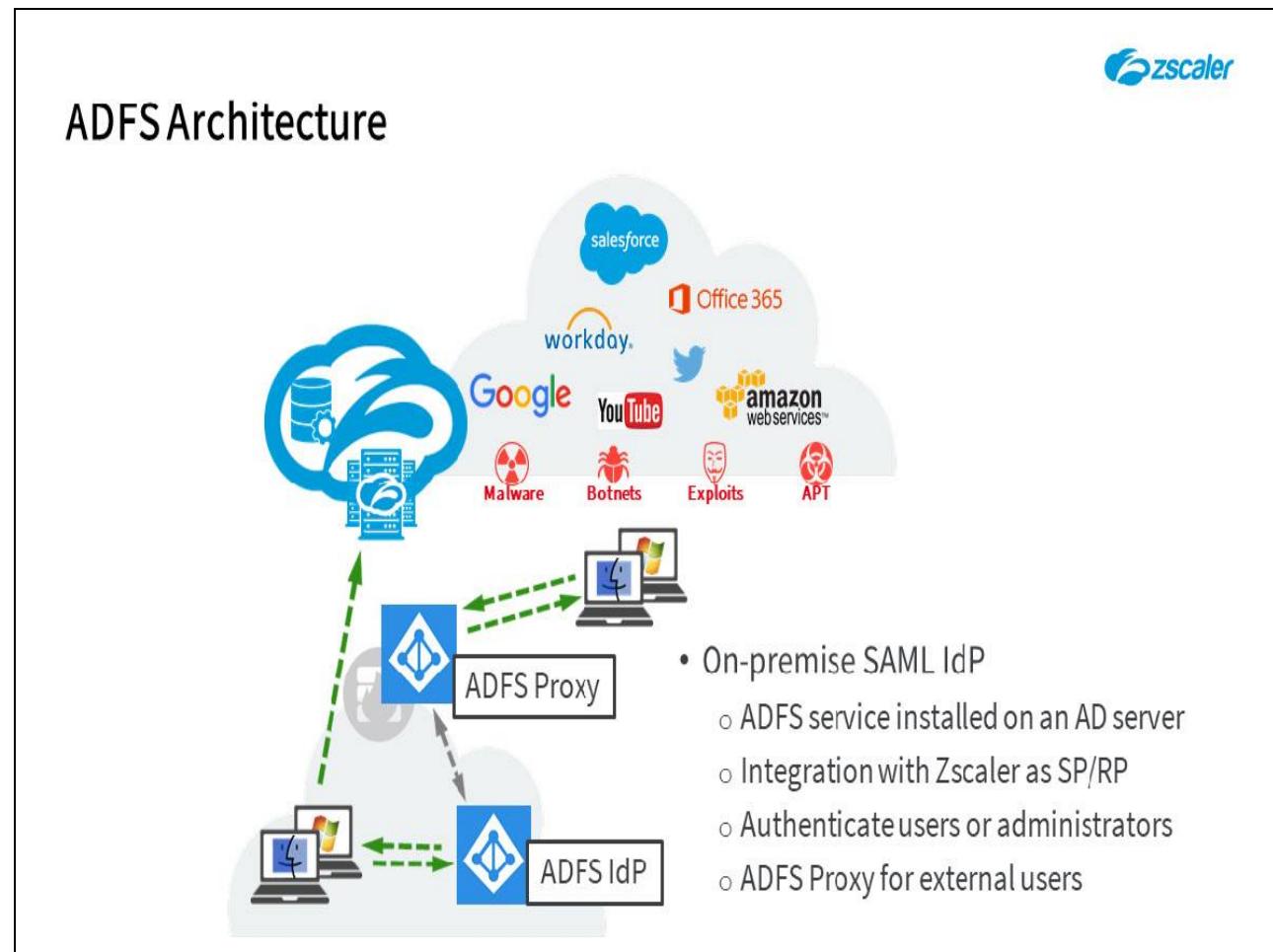
## Slide 7 - ADFS Architecture



## Slide notes

Both end user and administrator authentication into the ZPA service is supported using Microsoft ADFS as the IdP.

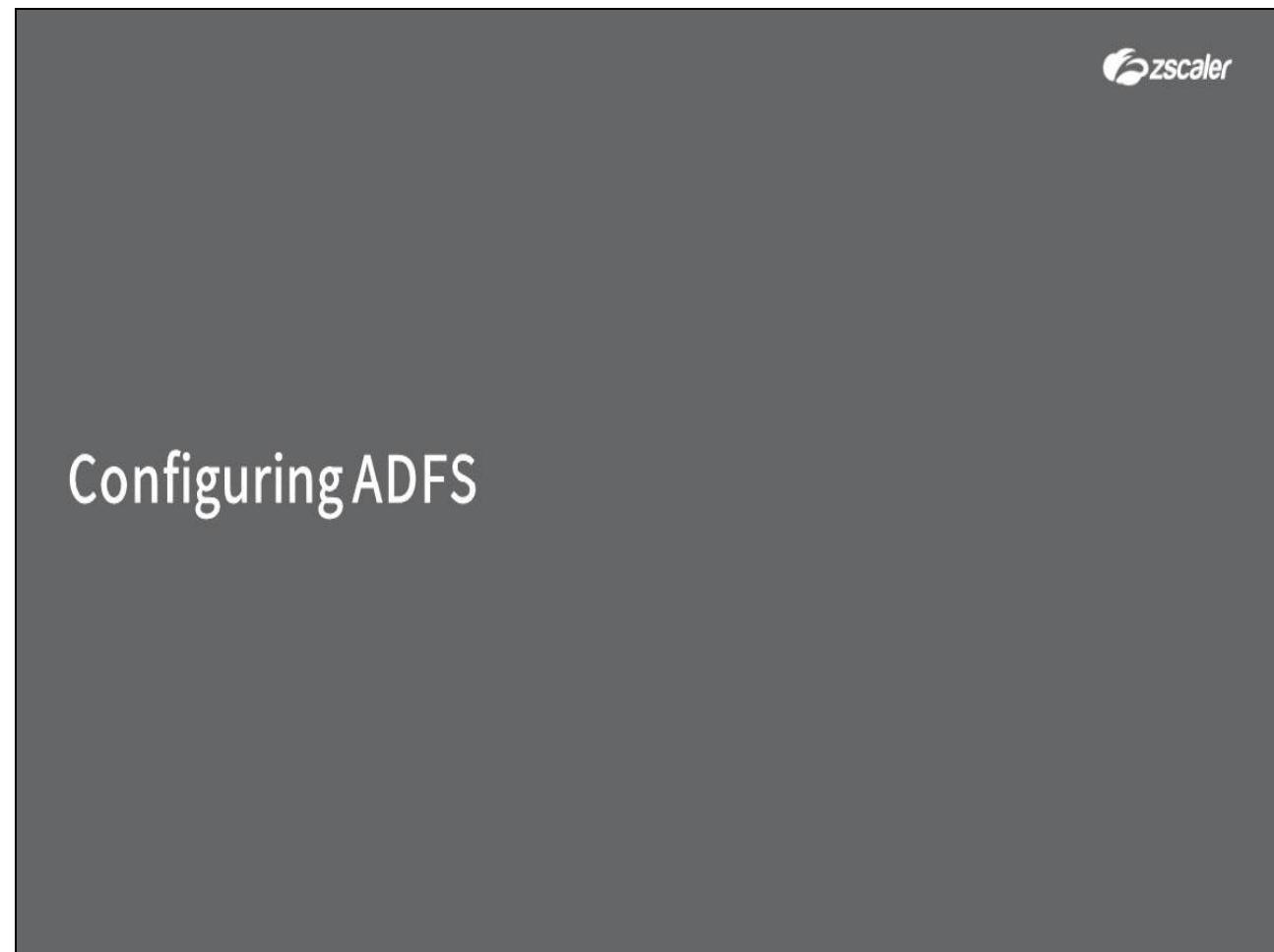
## Slide 8 - ADFS Architecture



## Slide notes

Note that for an ADFS server to support users on an external network (such as The Internet), then an additional component, and additional configuration is necessary. An ADFS Proxy is required on the DMZ network of your firewall, that has access to the internal ADFS server. In addition, a “split-horizon” DNS configuration is required, so that when users are local they resolve the local address of the ADFS server, but when they are remote, they resolve the public IP address of the ADFS Proxy.

## Slide 9 - SAML Overview



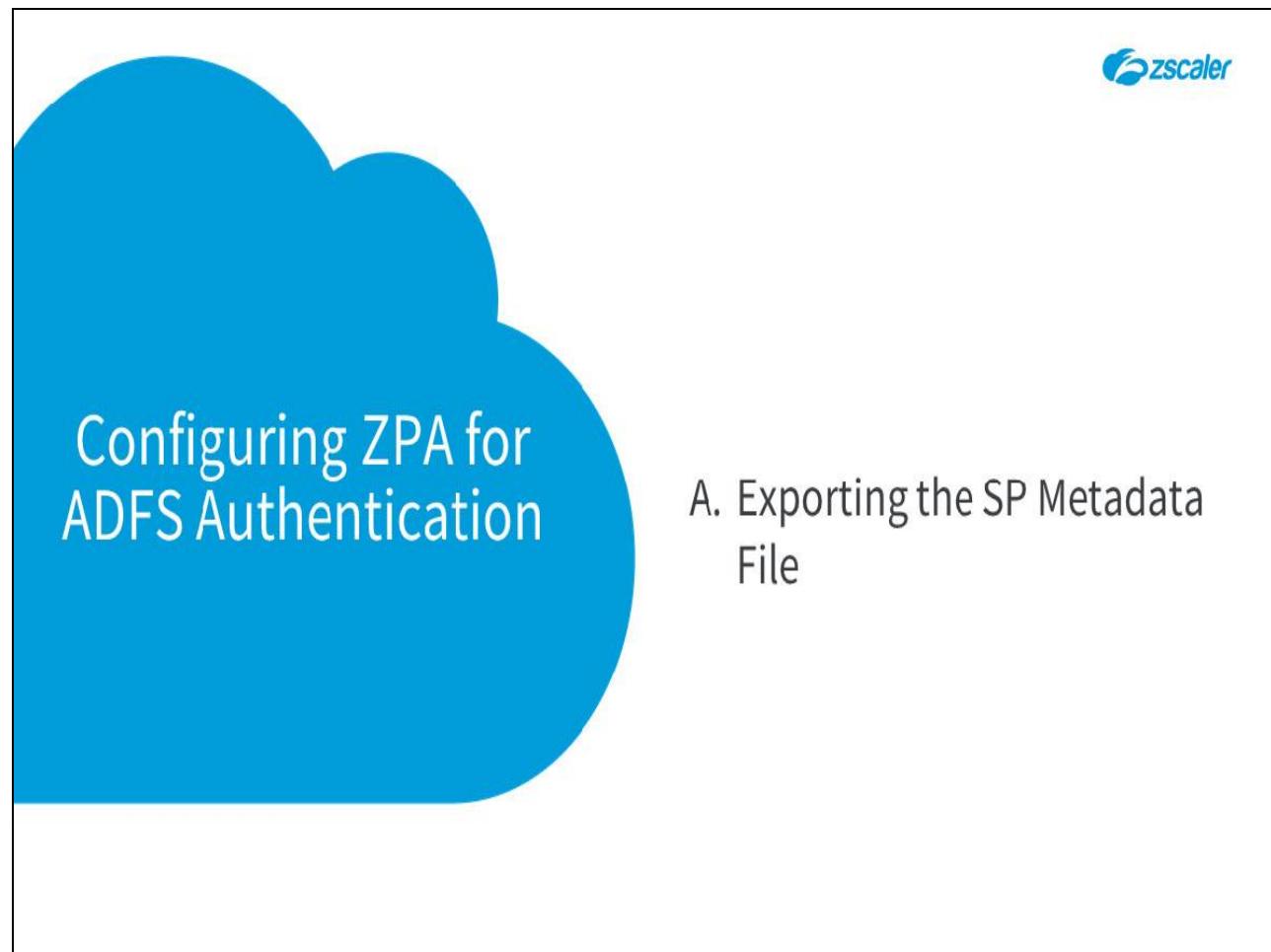
## Configuring ADFS

### Slide notes

In the next section, we will look at the configuration of the ADFS server.

This section has been created as an interactive demo to give you a feel for the navigation of the Windows 2012 Server Management Console. 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 ADFS Authentication



The slide features a large, semi-transparent blue cloud shape on the left side, containing the title text. In the top right corner of the slide area, there is a small Zscaler logo.

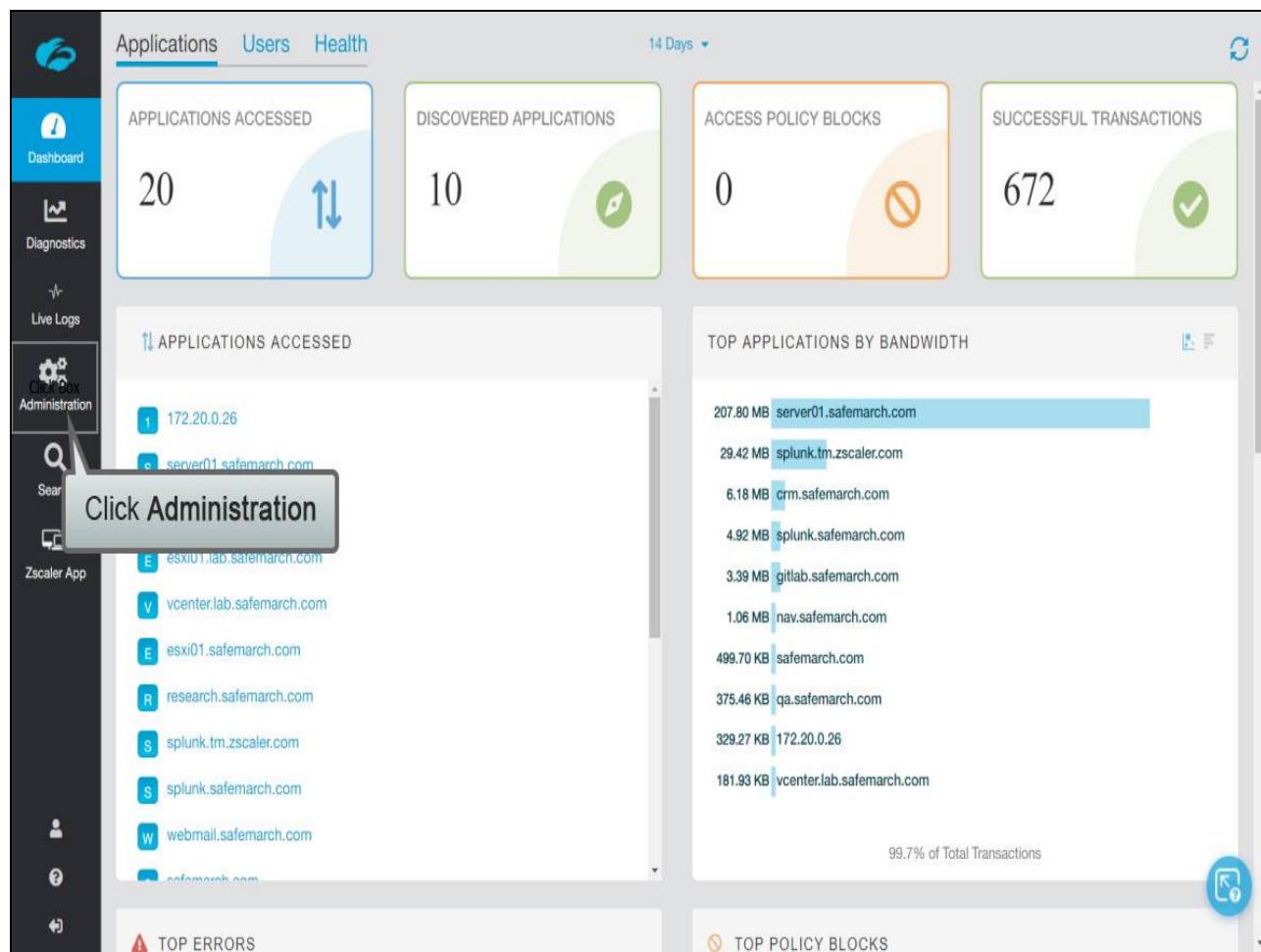
## Configuring ZPA for ADFS Authentication

A. Exporting the SP Metadata File

**Slide notes**

First, we will look at how to export the ZPA Service Provider metadata to file, for later import to ADFS. Note that a Service Provider is known as a “Relying Party” in the Microsoft world.

## Slide 11 - Slide 11



## Slide notes

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

## Slide 12 - Slide 12

The screenshot shows the Zscaler CASB dashboard. On the left sidebar, under the 'AUTHENTICATION' section, the 'IdP Configuration' option is highlighted with a blue box and the text 'Click IDP Configuration' overlaid. The main dashboard area displays various metrics: 'APPLICATION MANAGEMENT' (Application Segments, Segment Groups, Servers), 'APPLICATIONS' (0), 'ACCESS POLICY BLOCKS' (0), 'SUCCESSFUL TRANSACTIONS' (672), 'TOP APPLICATIONS BY BANDWIDTH' (server01.safemarch.com at 207.80 MB), and 'TOP POLICY BLOCKS' (99.7% of Total Transactions). The bottom right corner features a circular icon with a magnifying glass and a question mark.

## Slide notes

...then to add a SAML IdP, click **IdP Configuration**.

## Slide 13 - Slide 13

The screenshot shows the Zscaler Admin UI with the 'Administration' tab selected in the sidebar. The main page displays the 'IdP Configuration' section. A table lists existing IdP configurations, with one entry for 'Okta'. A callout box with the text 'Click the + icon' points to the plus sign icon located in the top right corner of the table's header area.

Name	Status	IdP Entity ID	Single Sign-On	Actions
Okta	✓	http://www.okta.com/exkltqh8up9sQl2z90h7	User	

## Slide notes

To add a new IdP configuration, click the + icon at top right, ...

## Slide 14 - Slide 14

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area is titled 'IdP Configuration' and shows a list of configurations with columns for Name, Status, IdP Entity ID, Single Sign-On, and Actions. A modal window titled 'Add IdP Configuration' is open, divided into three tabs: 1. IdP Information (selected), 2. SP Metadata, 3. Create IdP. The 'Name' field is populated with 'ADFS'. Under 'Single Sign-On', the 'User' radio button is selected. In the 'Domains' field, there is a placeholder text 'Select a Value' and a tooltip 'Click Box' with an arrow pointing to it. A callout bubble with the text 'Click in the Domains field' is overlaid on the 'Domains' field.

## Slide notes

...give the IdP a **Name**, select whether it is to be used for **Admin** or **User Single Sign-On** and click in the **Domains** field to select the authentication domains to match.

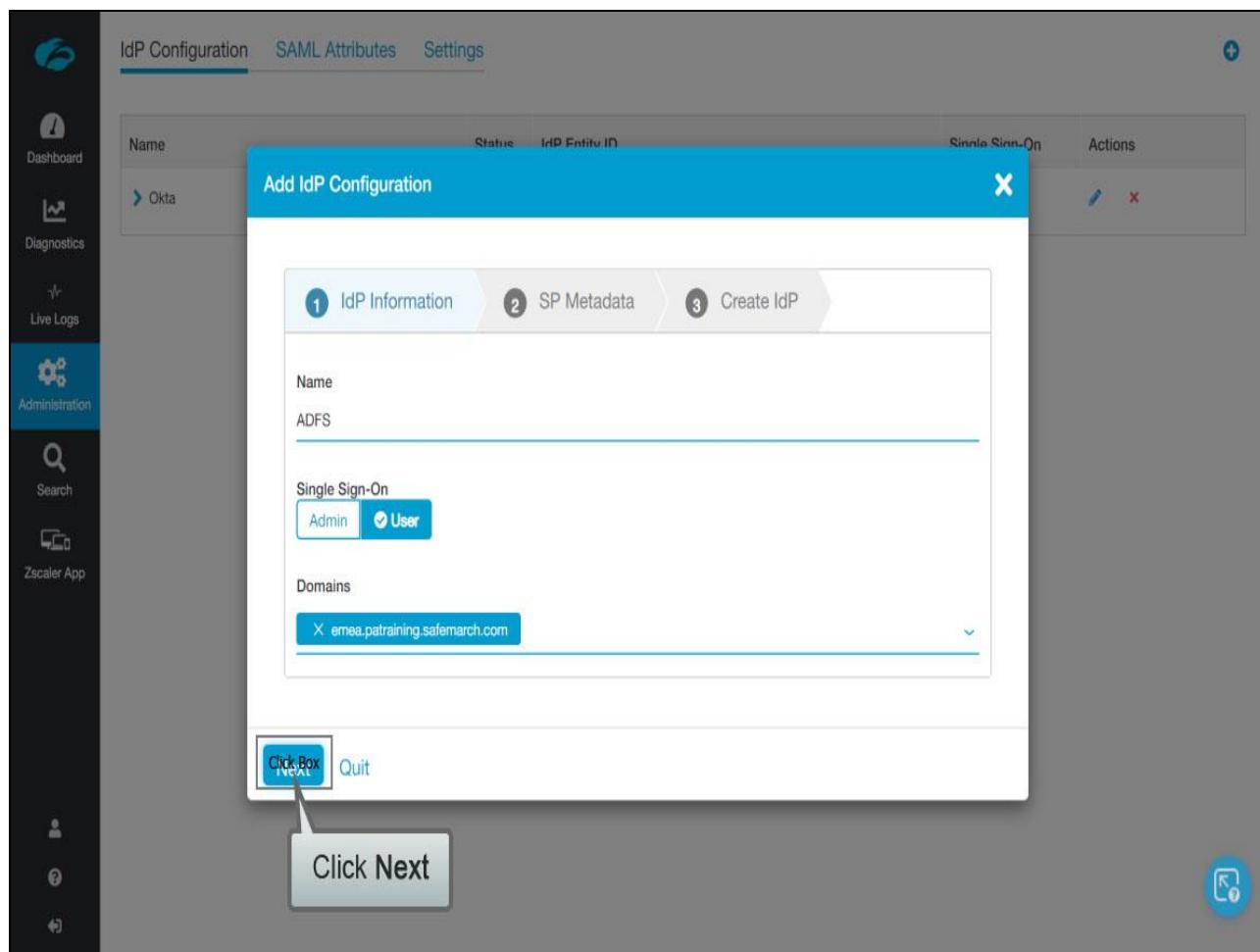
## Slide 15 - Slide 15

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for 'IdP Configuration', 'SAML Attributes', and 'Settings'. A modal window titled 'Add IdP Configuration' is open, showing three steps: 1. IdP Information, 2. SP Metadata, and 3. Create IdP. In the 'IdP Information' step, the 'Name' field is set to 'ADFS'. Under 'Single Sign-On', the 'User' radio button is selected. The 'Domains' section lists several domains: 'emea.patraining.safemarch.com' is checked and highlighted with a blue border; 'anz.patraining.safemarch.com', 'apac.patraining.safemarch.com', and 'us.patraining.safemarch.com' are unselected. At the bottom of the 'Domains' list, there are 'Select All' and 'Clear Selection' buttons. A callout box with the text 'Click Box' points to the 'Click Box' button at the bottom of the list. Another callout box with the text 'Click Done' points to the 'Click Done' button at the bottom of the modal.

## Slide notes

Select one or more of the available domains and click **Done**, ...

## Slide 16 - Slide 16



## Slide notes

...then click **Next**.

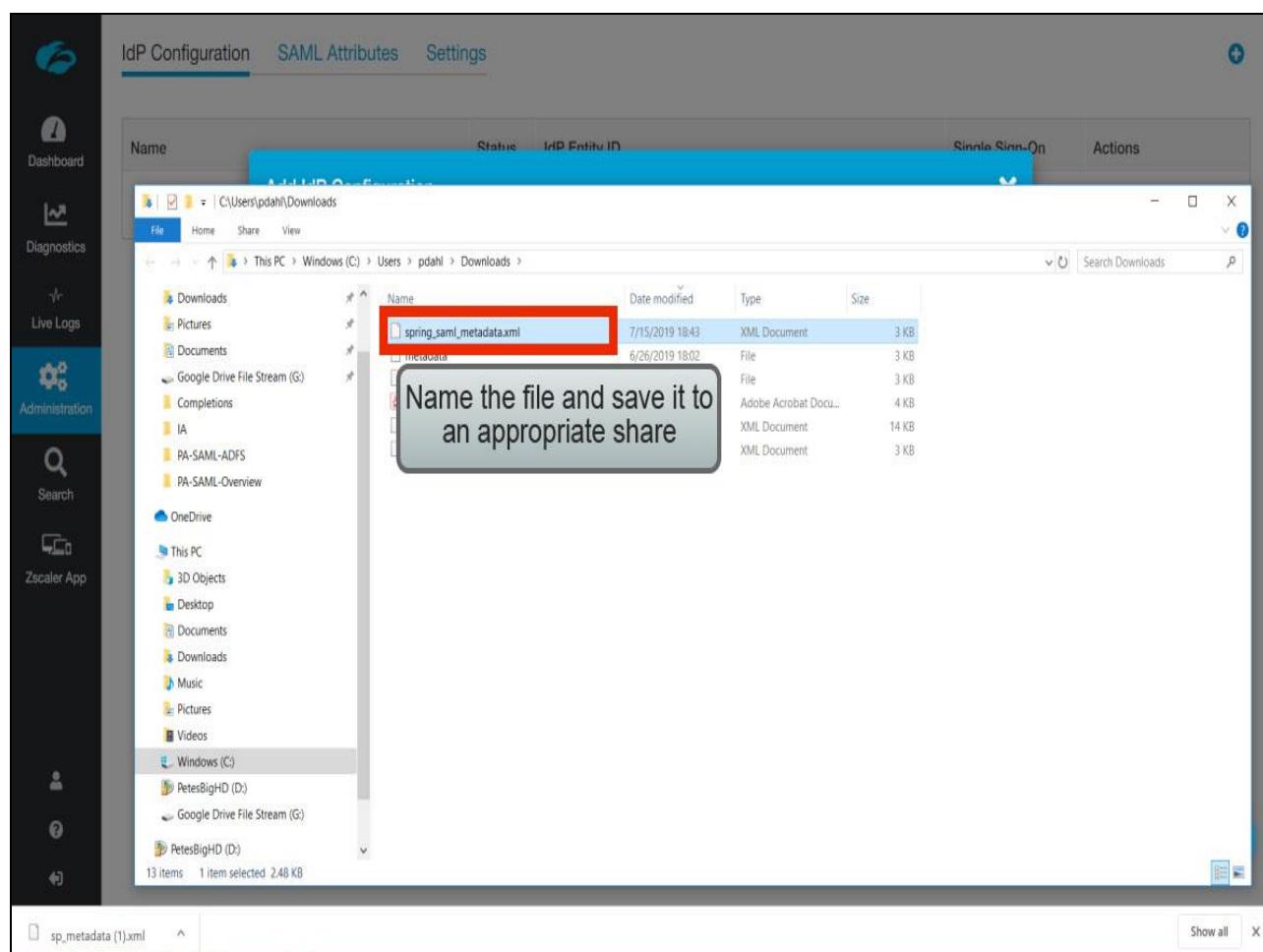
## Slide 17 - Slide 17

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, specifically for the 'Okta' provider. The modal has three tabs: '1 IdP Information', '2 SP Metadata', and '3 Create IdP'. The '2 SP Metadata' tab is active. Inside, there's a section for 'Service Provider Metadata' with a 'Download Certificate' link. A large gray callout bubble with the text 'Click Download Metadata' points to this link. The background shows a list of existing IdP configurations.

## Slide notes

Click Download Metadata, ...

## Slide 18 - Slide 18



## Slide notes

Make a note of where the file is located and move it to a share accessible to the AD server if necessary.

## Slide 19 - Slide 19

The screenshot shows the Okta Admin Console interface. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and User management. The main area has tabs for 'IdP Configuration', 'SAML Attributes', and 'Settings'. A modal window titled 'Add IdP Configuration' is open, divided into three steps: 1. IdP Information, 2. SP Metadata, and 3. Create IdP. Step 1 is active. It contains fields for Service Provider Metadata (with a 'Download Metadata' link), Service Provider URL (with a value and a 'Download' link), and Service Provider Entity ID (with a value and a 'Download' link). At the bottom of the modal, there are 'Next' and 'Pause' buttons. A large callout box with an arrow points from the text 'Click Pause' to the 'Pause' button. The background shows a list of IdPs with columns for Name, Status, IdP Entity ID, Single Sign-On, and Actions.

## Slide notes

Click **Pause** to save the configuration for the new IdP in its current incomplete state.

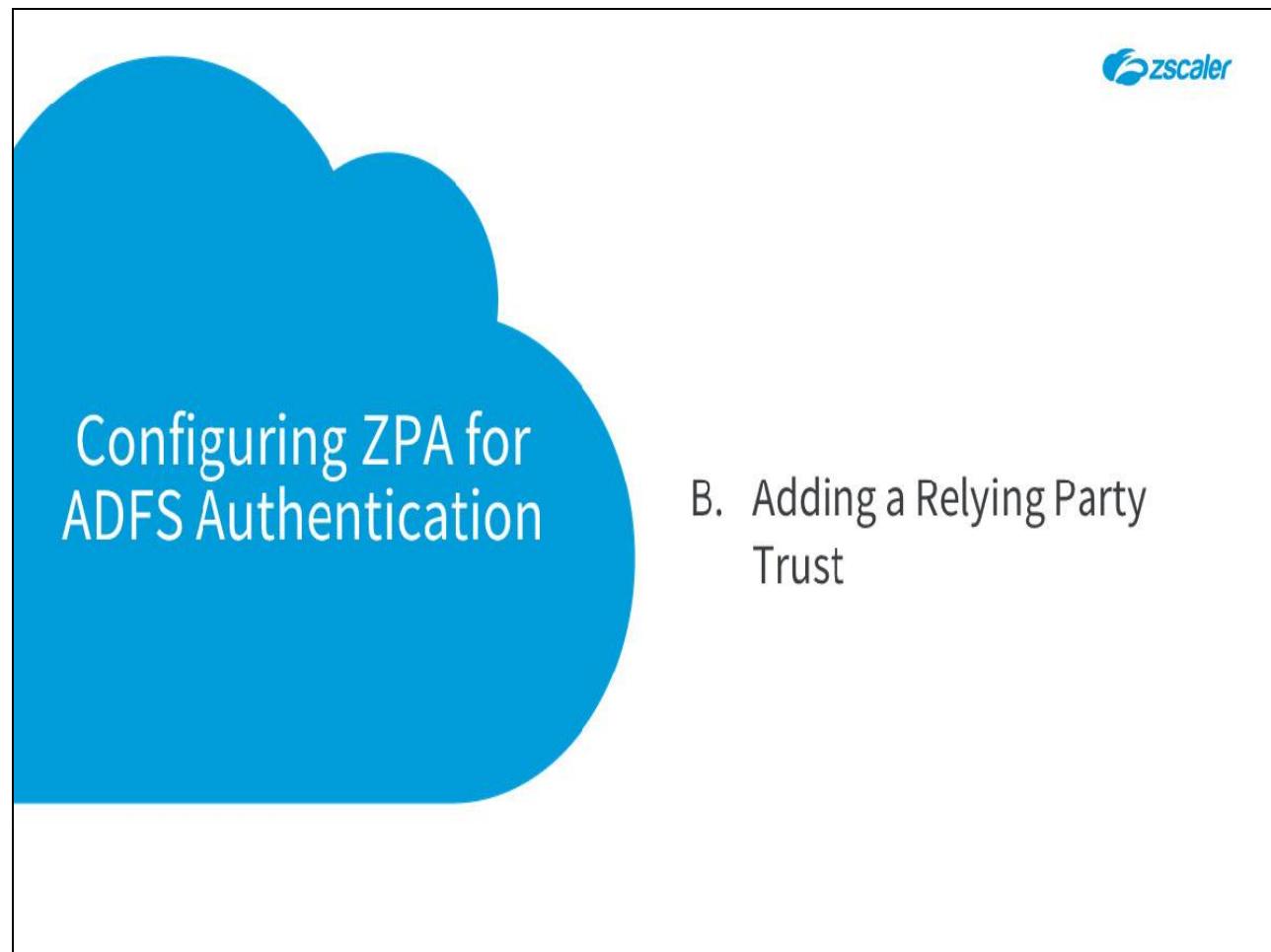
## Slide 20 - Slide 20

Name	Status	IdP Entity ID	Single Sign-On	Actions
ADFS	Paused		User	
Okta	Active	http://	User	

## Slide notes

The ADFS IdP is added to the list in the Paused state. As per the process discussed in the SAML Overview module, having generated the SP metadata that is unique for the ADFS IdP, you now need to step across to the IdP and configure it for ZPA.

## Slide 21 - Configuring ZPA for ADFS Authentication



The Zscaler logo is located in the top right corner of the slide area.

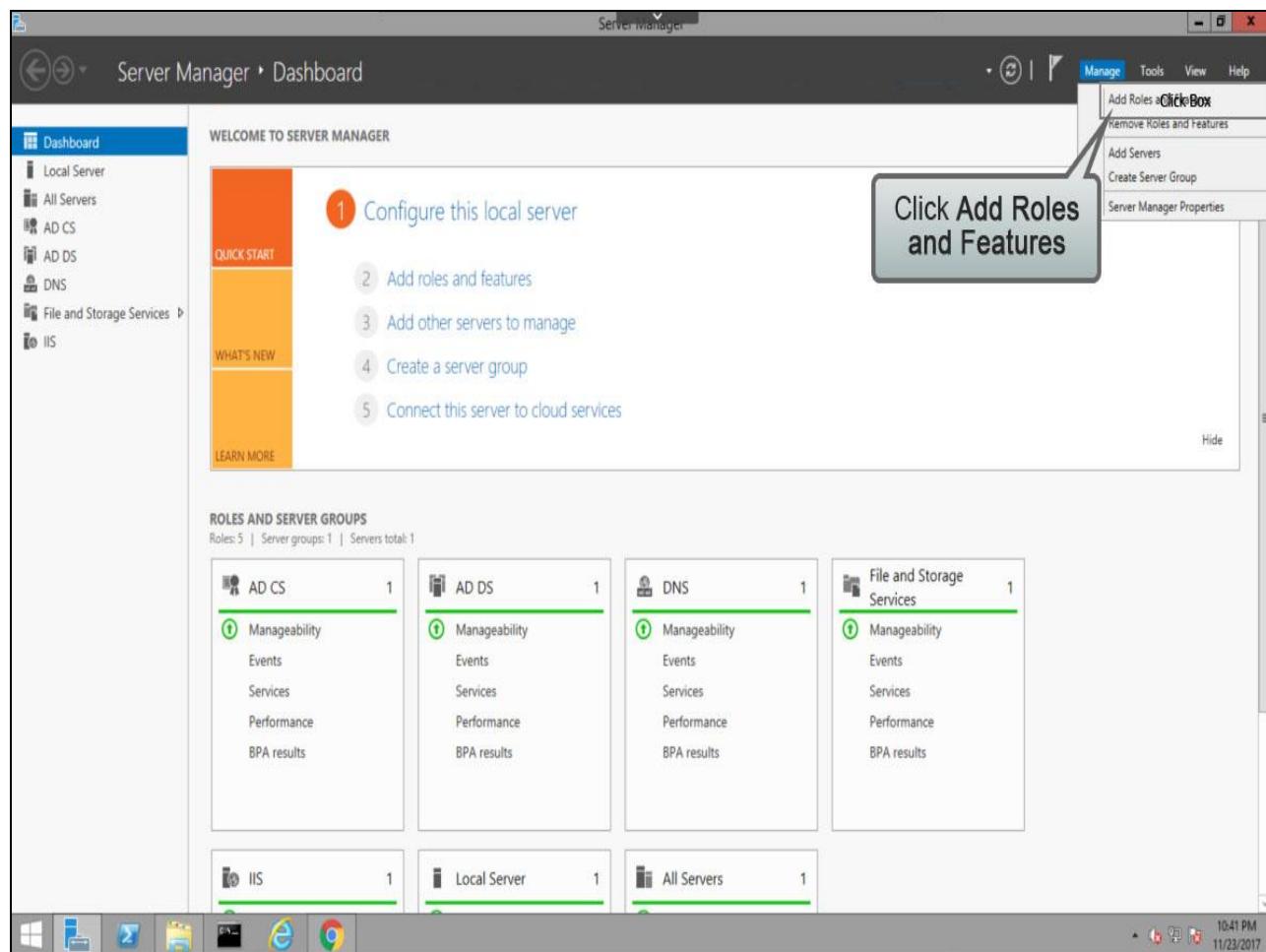
## Configuring ZPA for ADFS Authentication

B. Adding a Relying Party Trust

**Slide notes**

Next, we will look at installing Federation Services on the AD server and adding a **Relying Party Trust**.

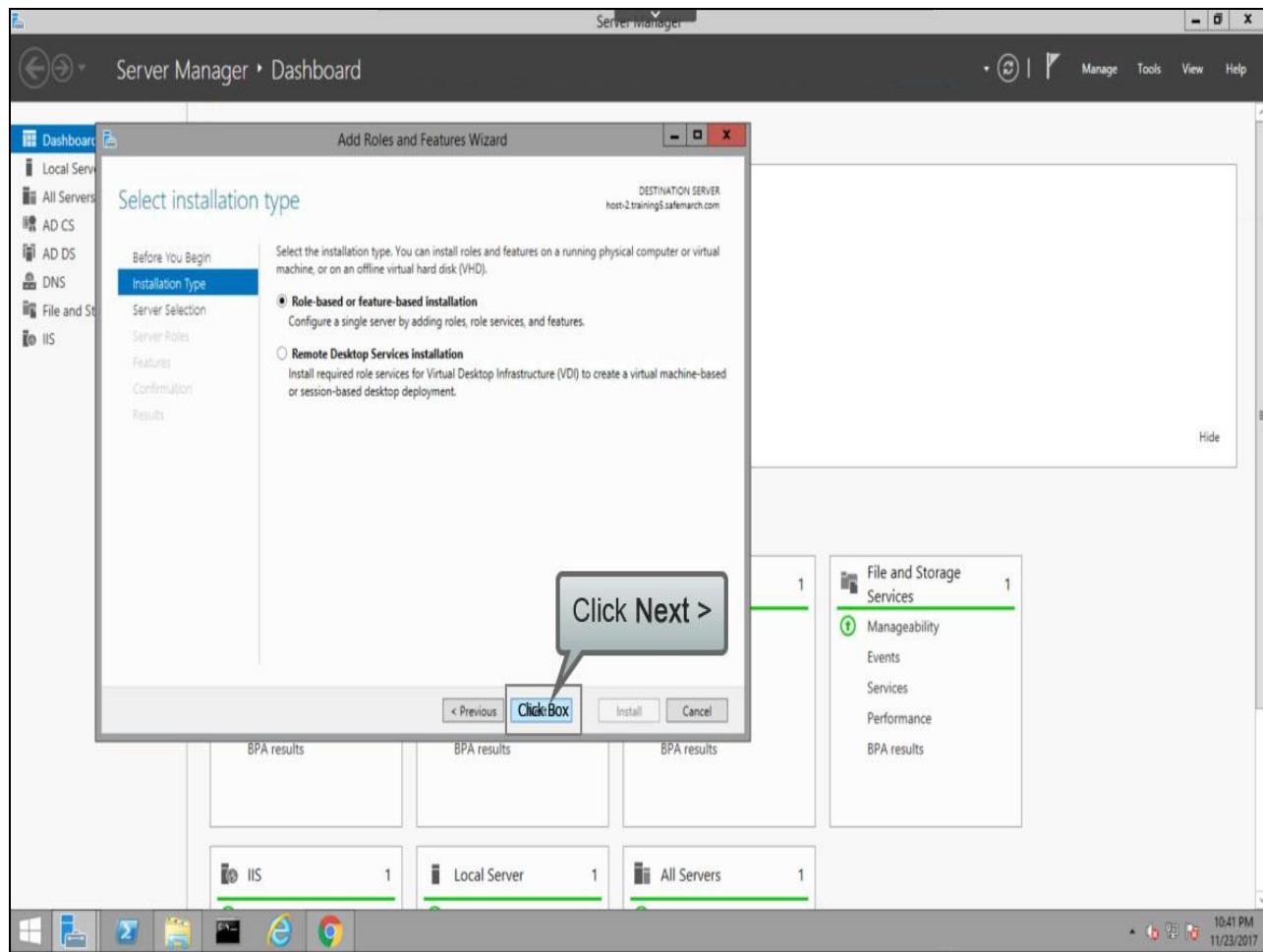
## Slide 22 - Slide 22



## Slide notes

On the AD server, in the **Server Manager** Dashboard, from the **Manage** menu, select **Add Roles and Features**.

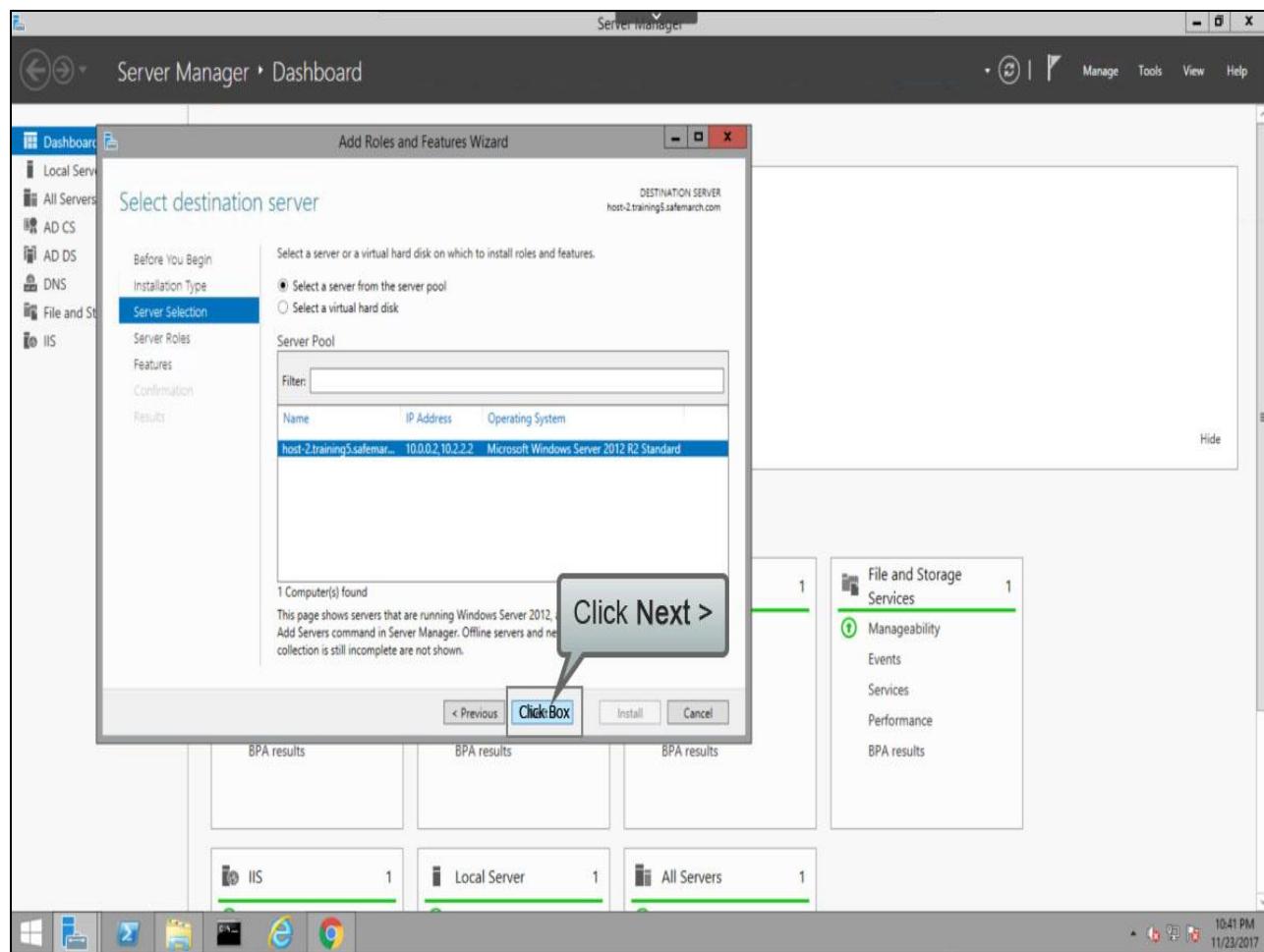
## Slide 23 - Slide 23



## Slide notes

Select the type of install and click **Next >**.

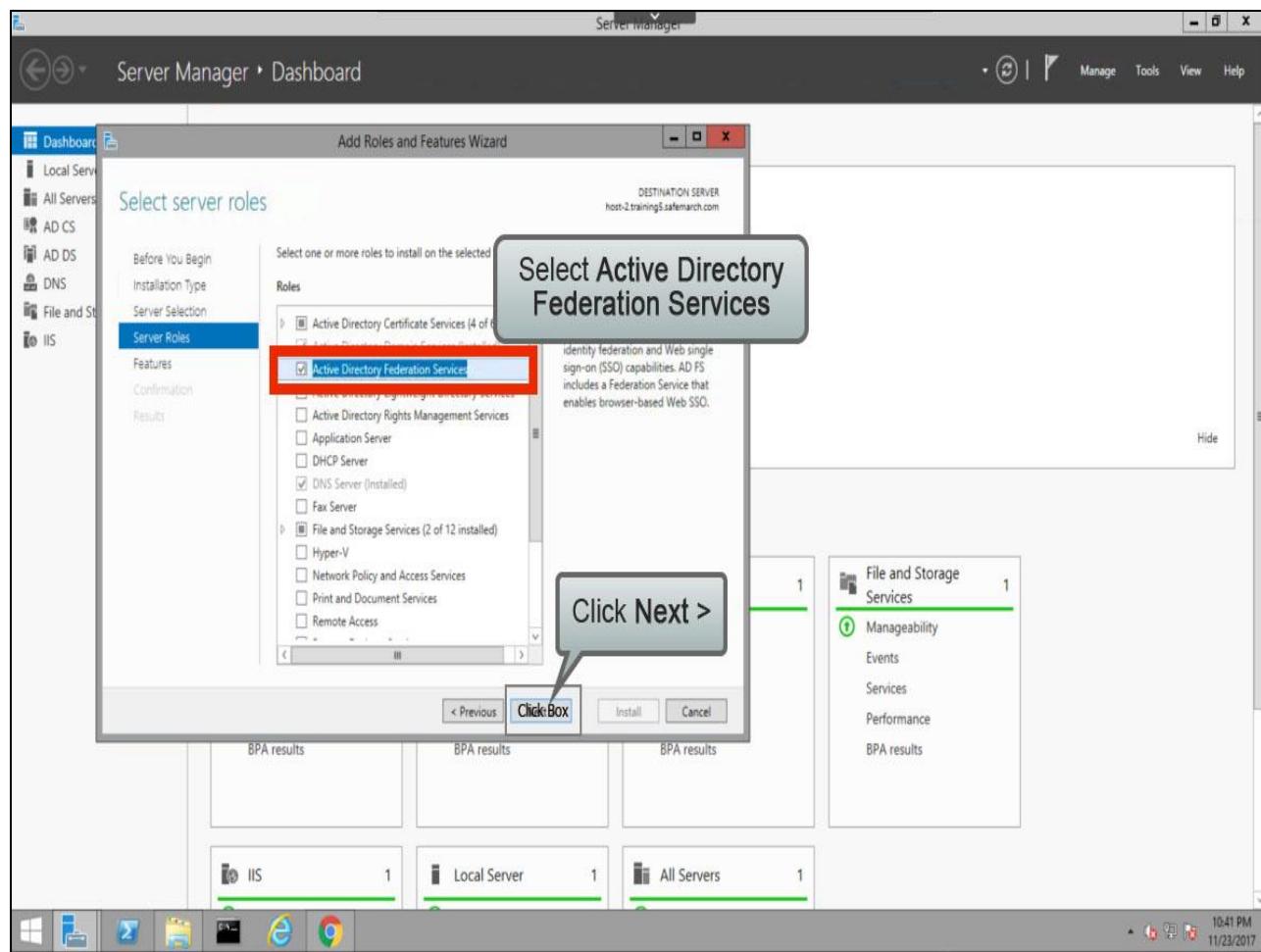
## Slide 24 - Slide 24



## Slide notes

Select the server to install this module on and click **Next >**.

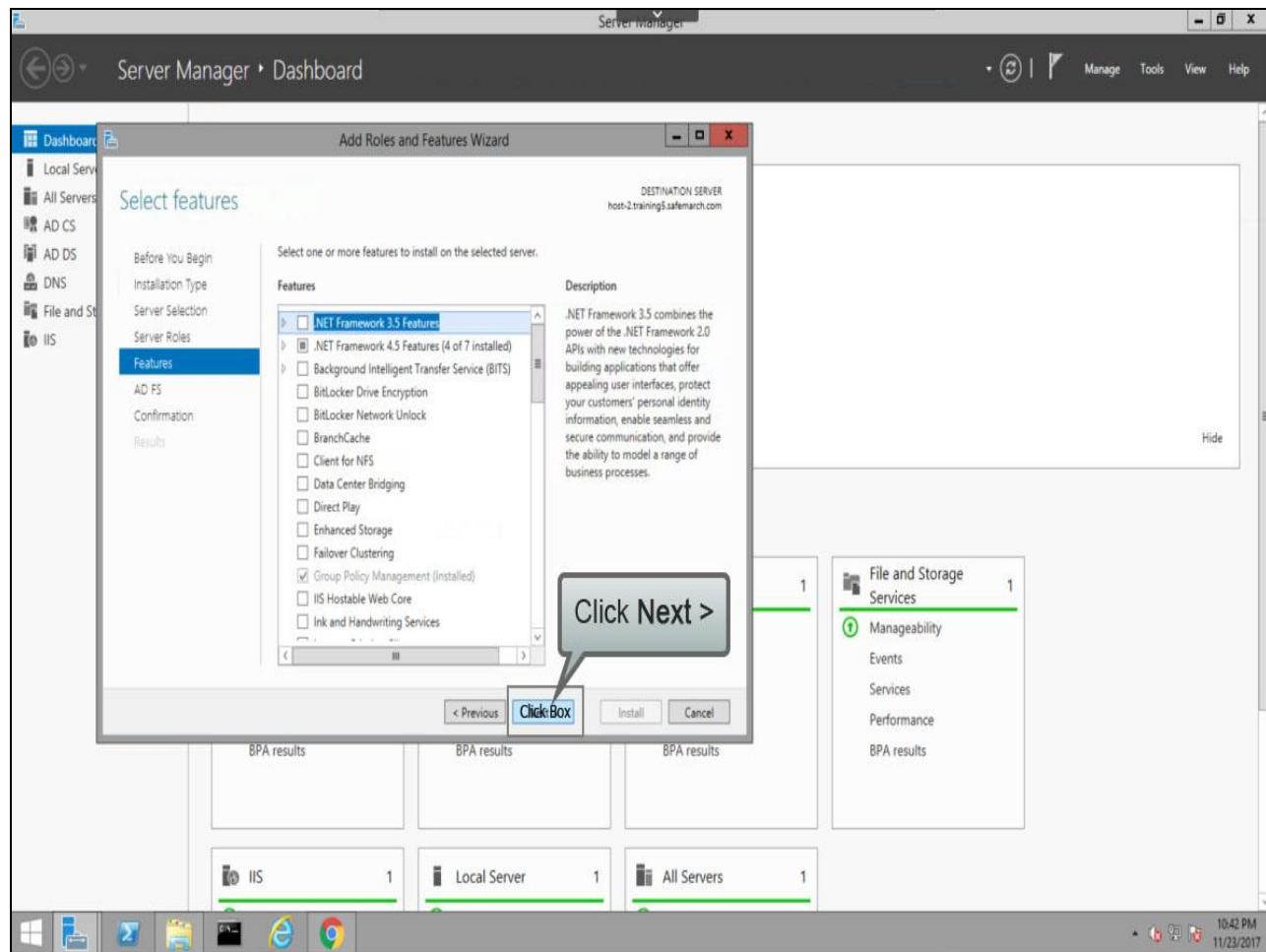
## Slide 25 - Slide 25



## Slide notes

Select Active Directory Federation Services and click Next >.

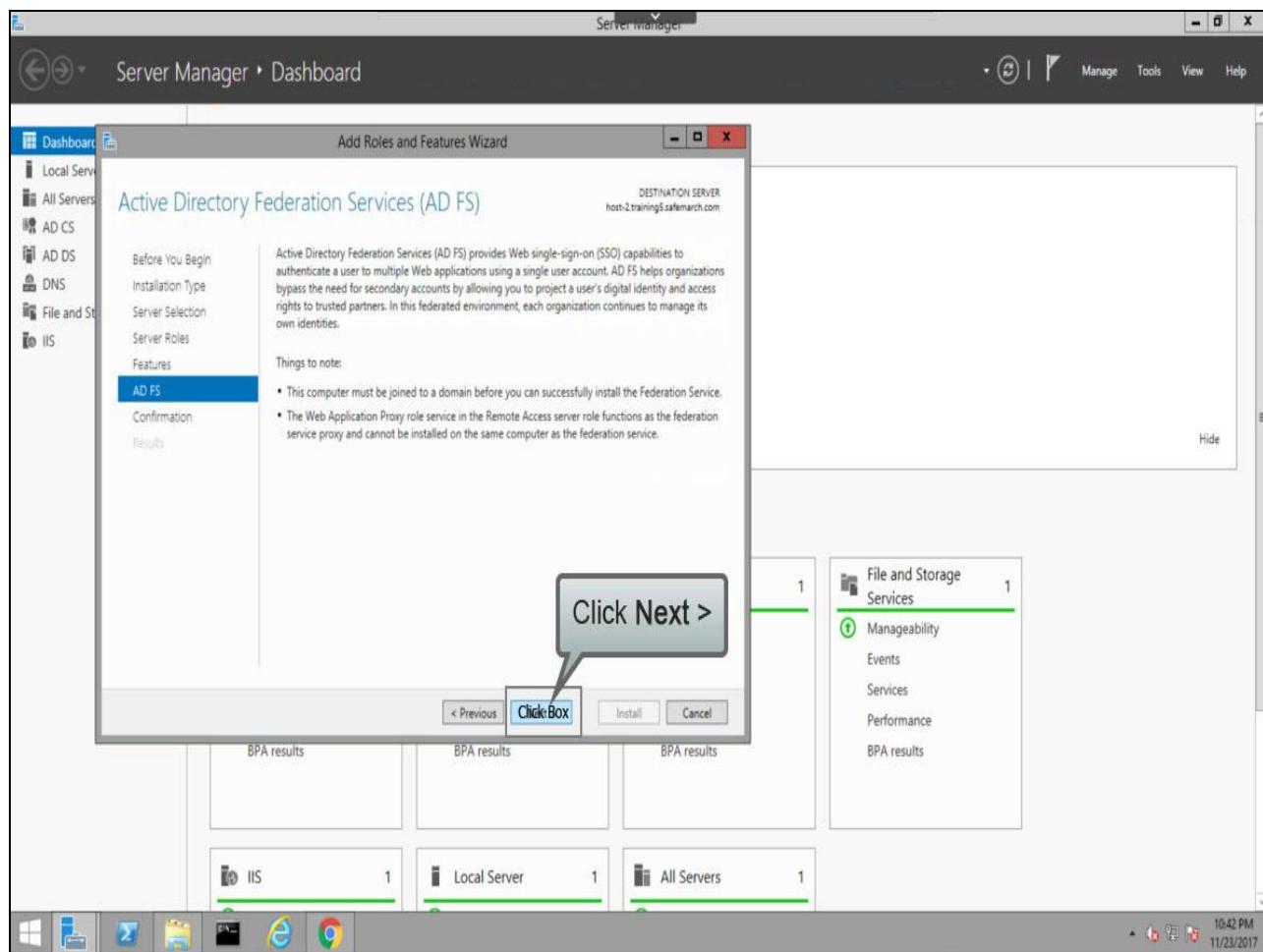
## Slide 26 - Slide 26



## Slide notes

We will accept the default set of features and just click **Next >**, ...

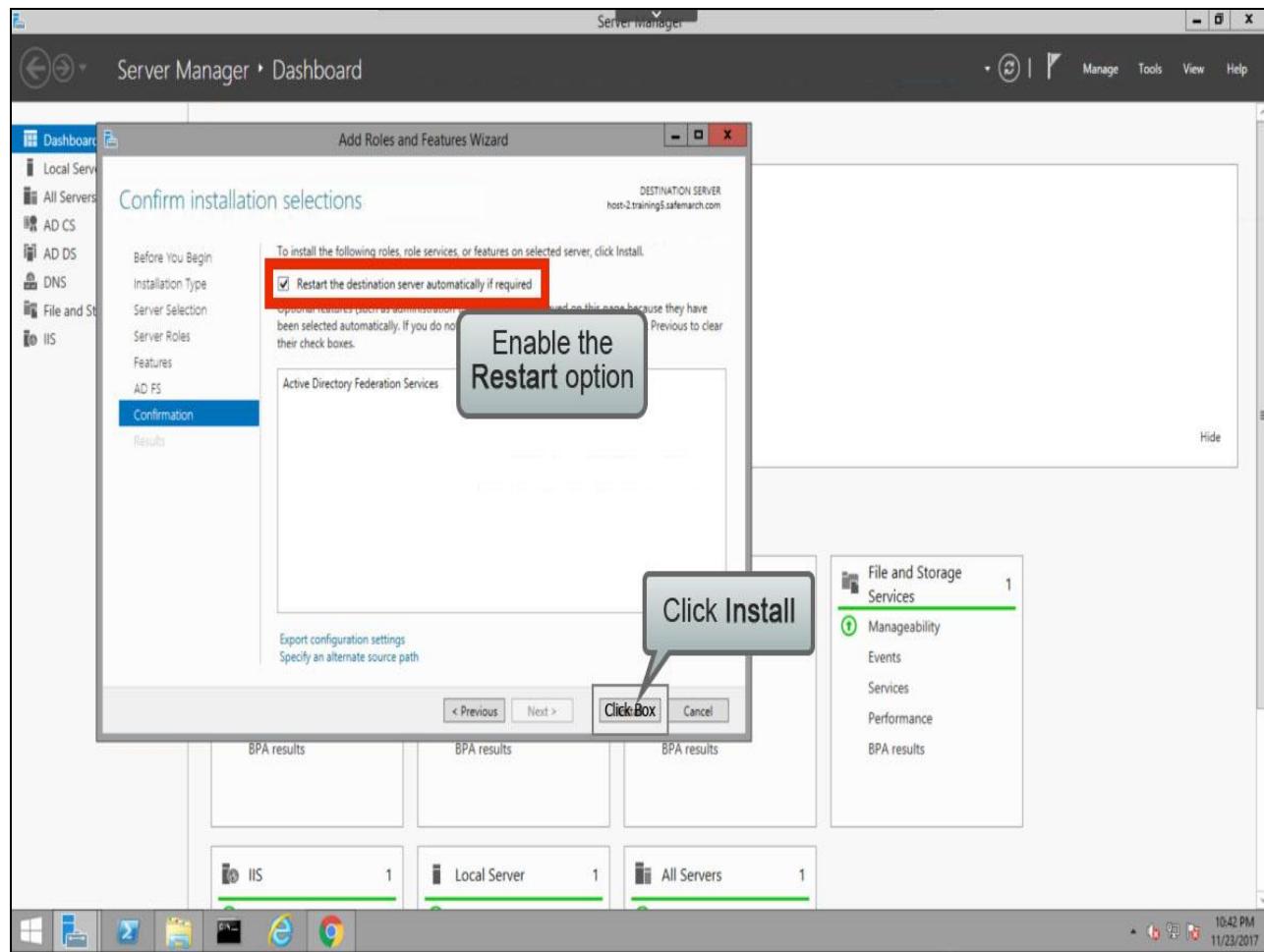
## Slide 27 - Slide 27



## Slide notes

...and click **Next >** again.

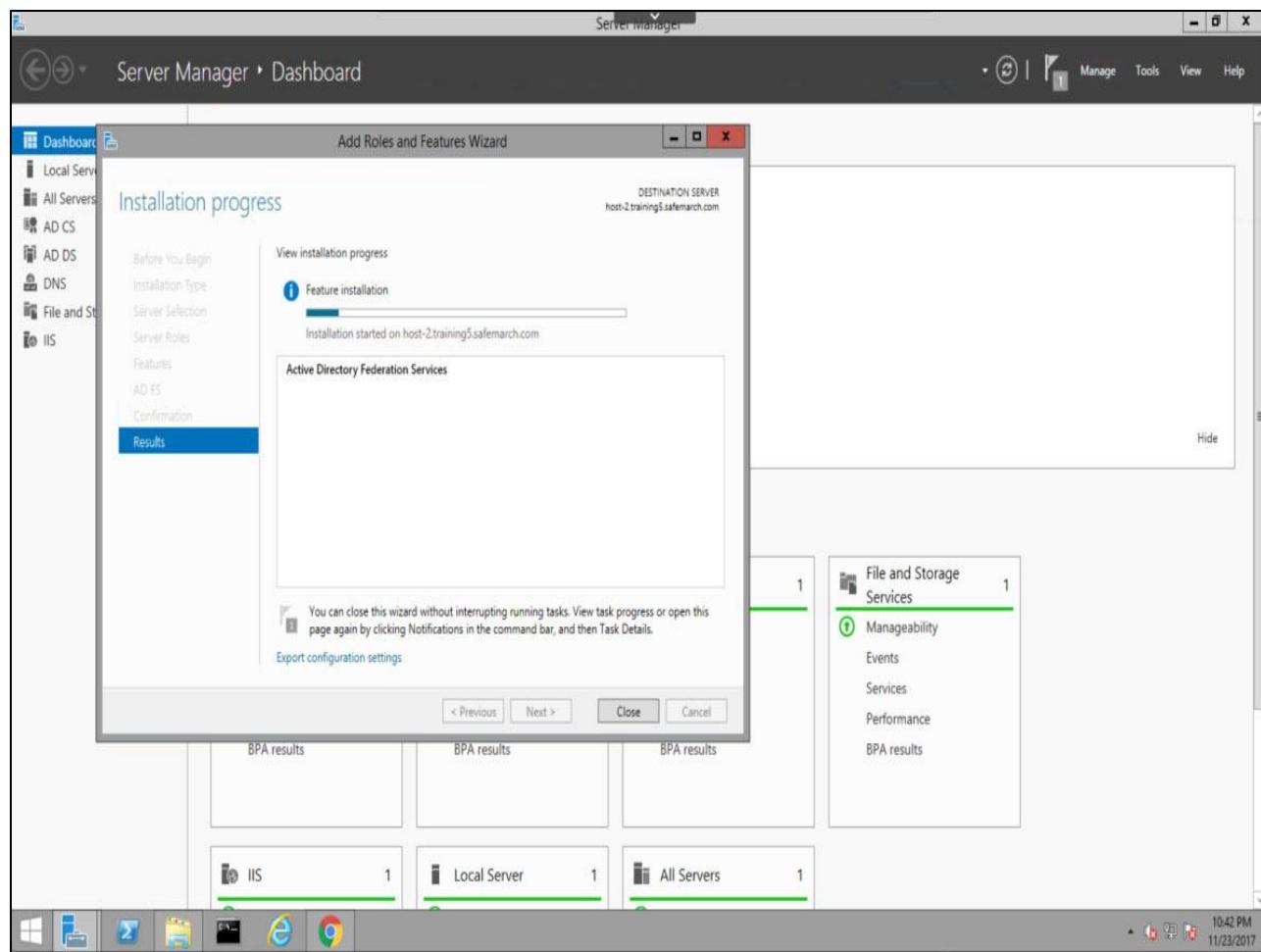
## Slide 28 - Slide 28



## Slide notes

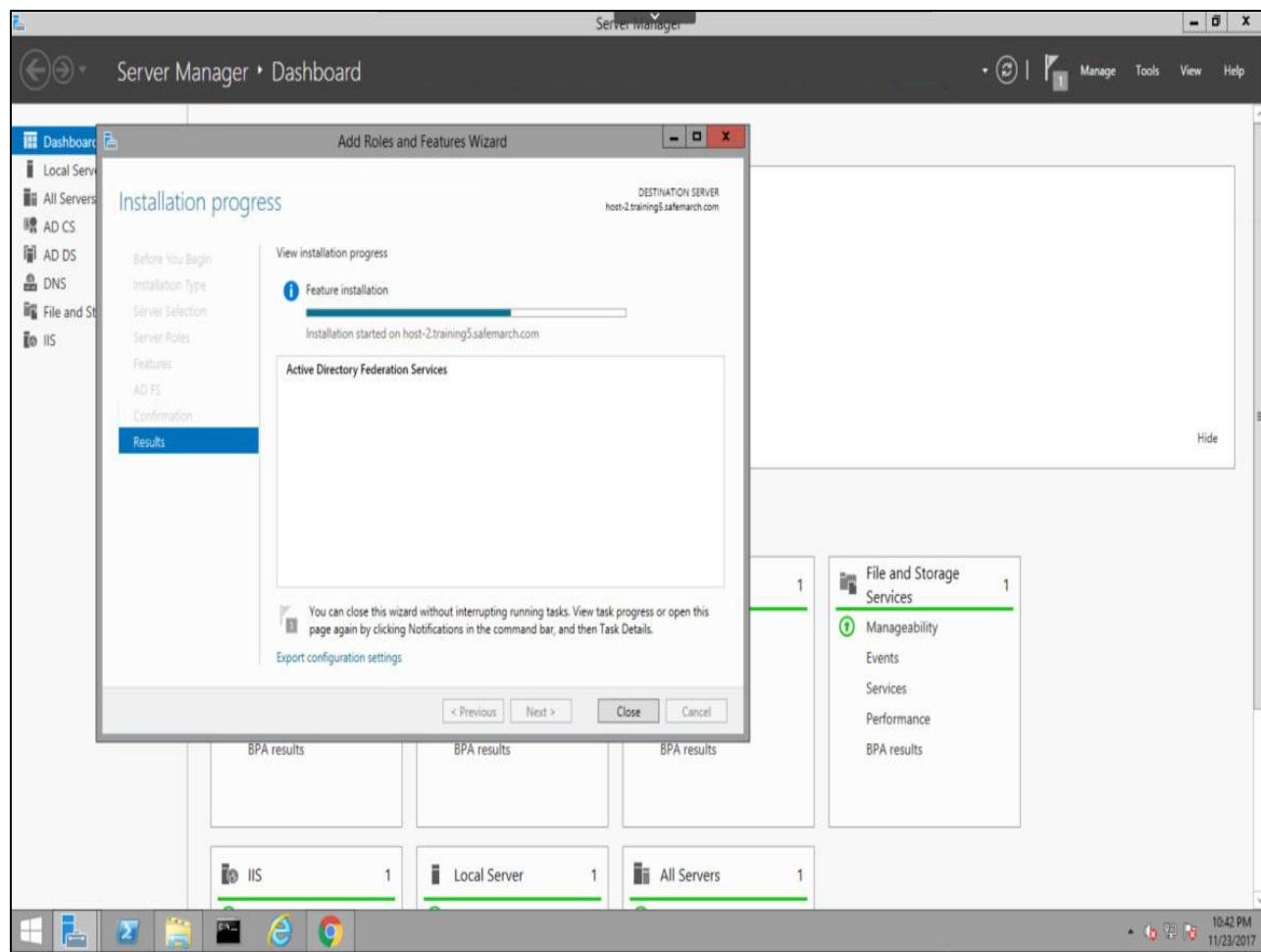
Enable the option to **Restart the destination server automatically if required**, then click **Install**.

## Slide 29 - Slide 29



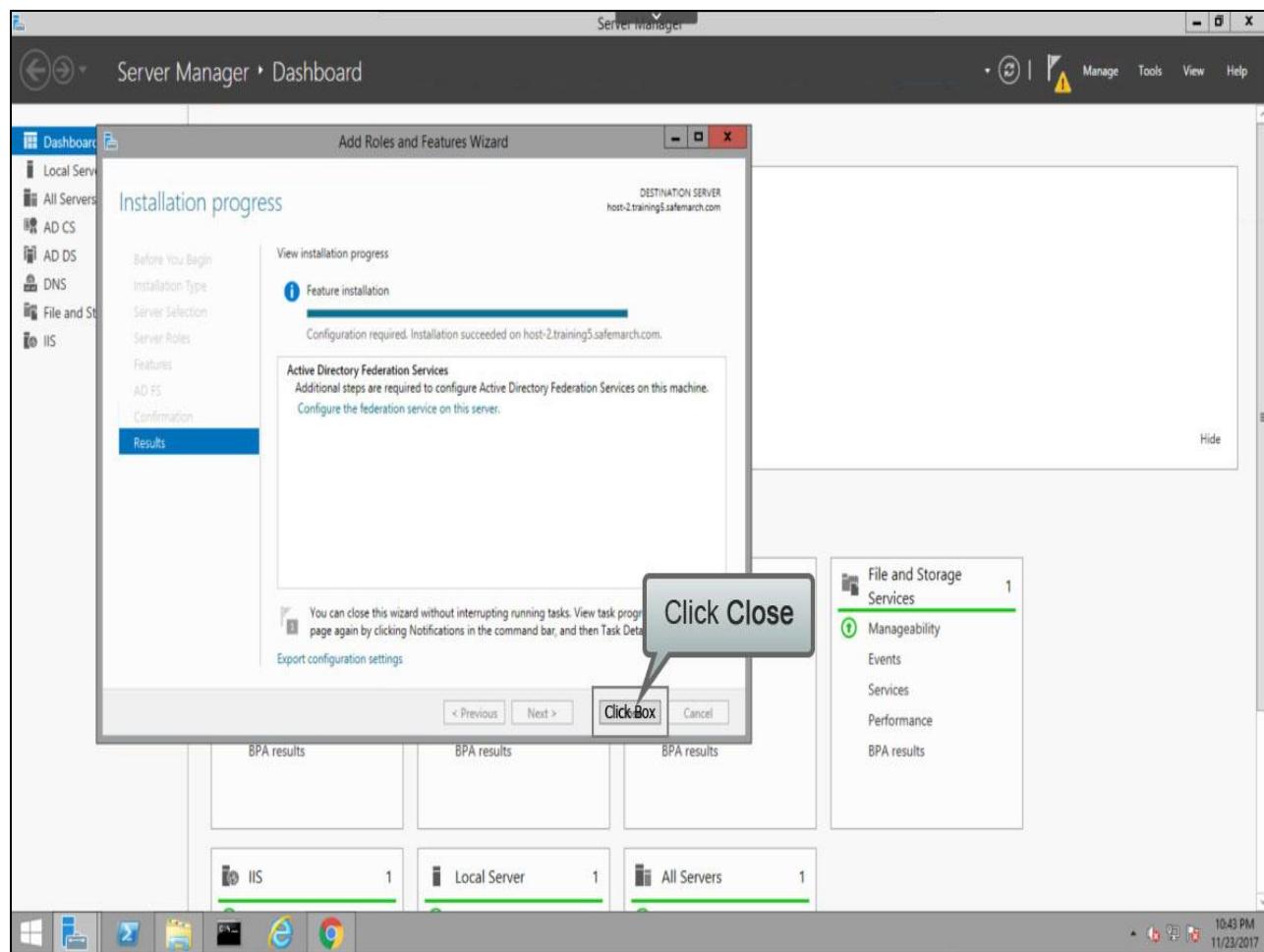
## Slide notes

## Slide 30 - Slide 30



## Slide notes

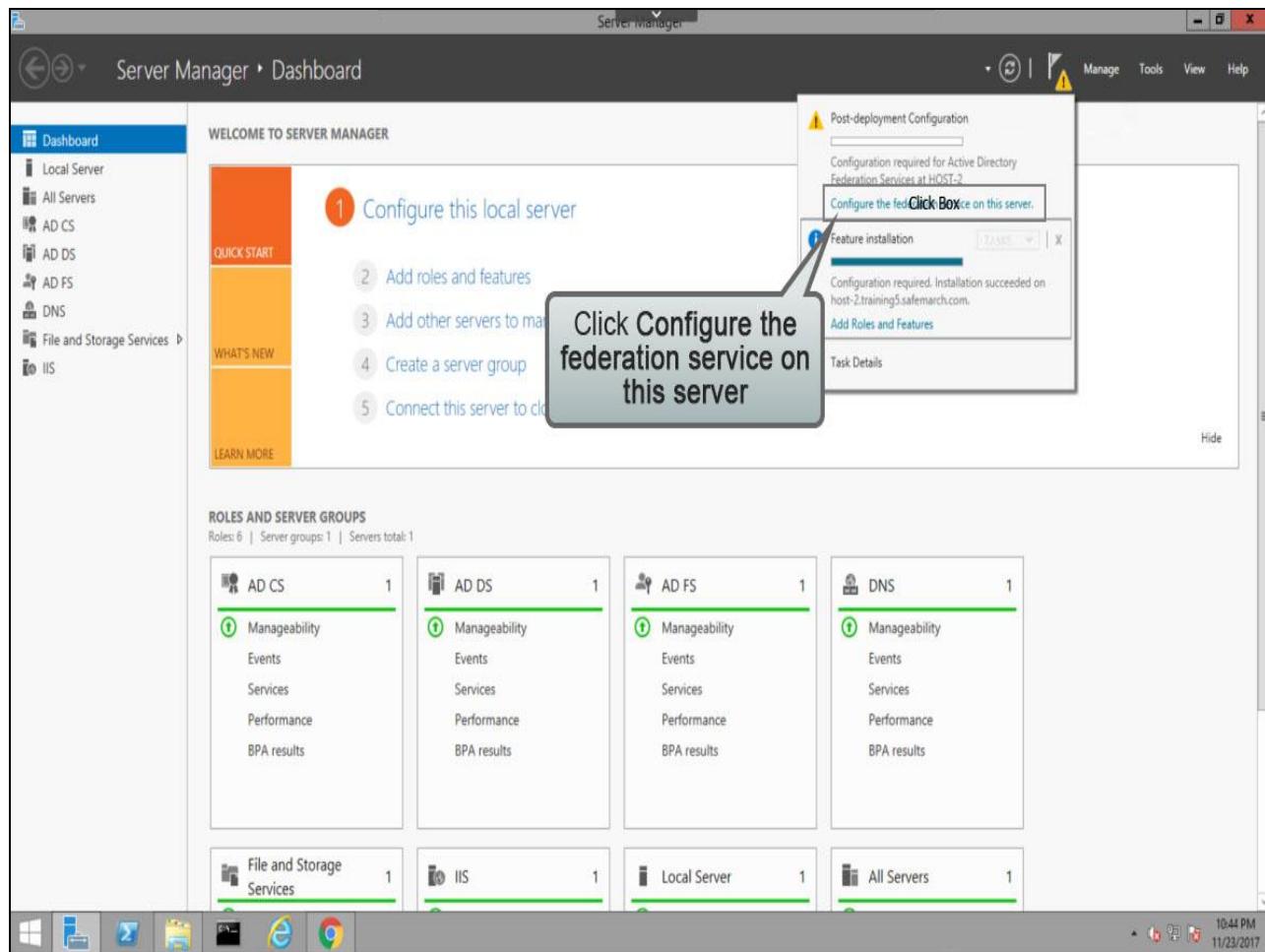
## Slide 31 - Slide 31



## Slide notes

Once the installation is complete, click **Close**.

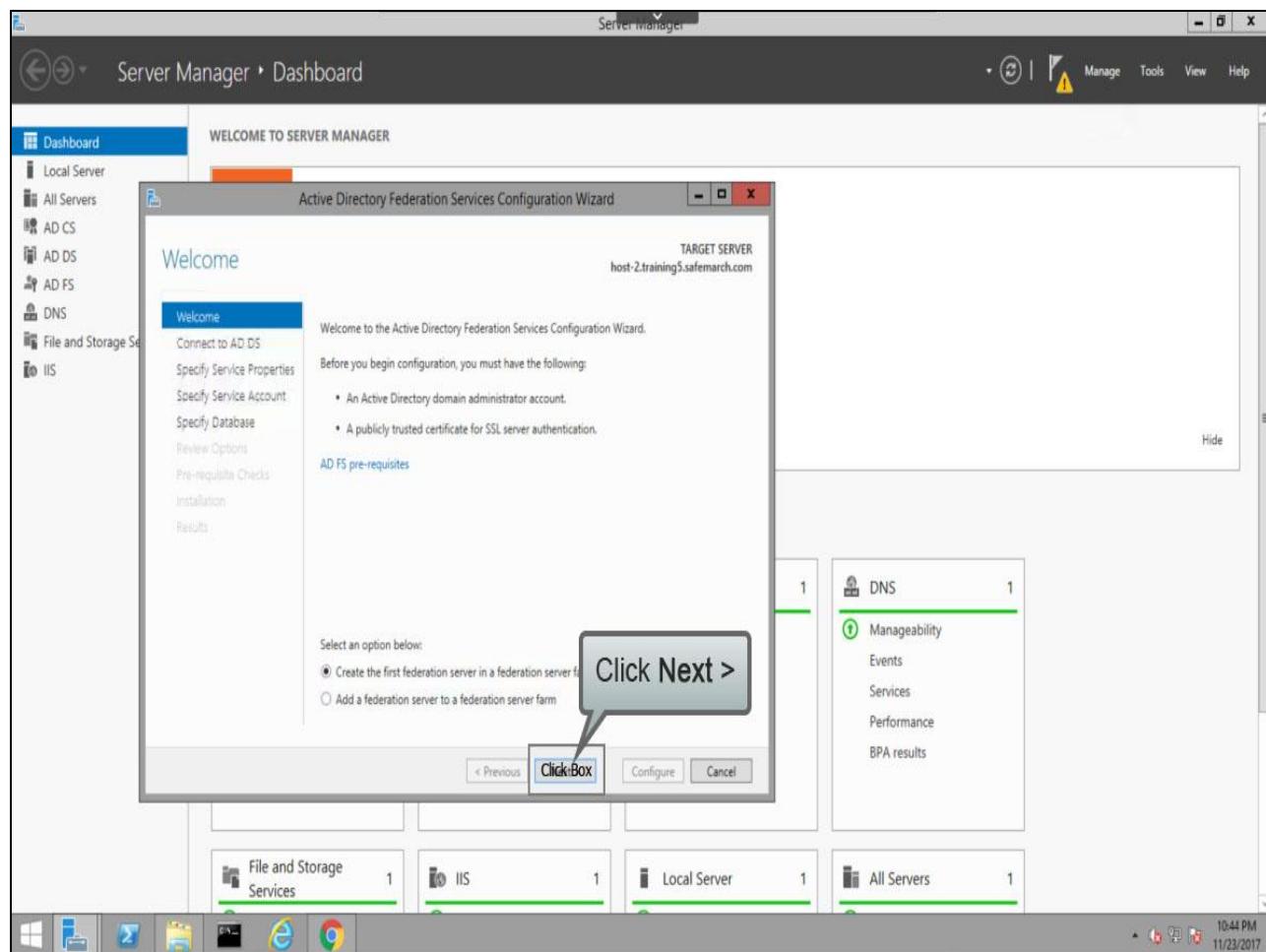
## Slide 32 - Slide 32



## Slide notes

Click the **warning triangle** in the Server Manager Dashboard and click **Configure the federation service on this server**.

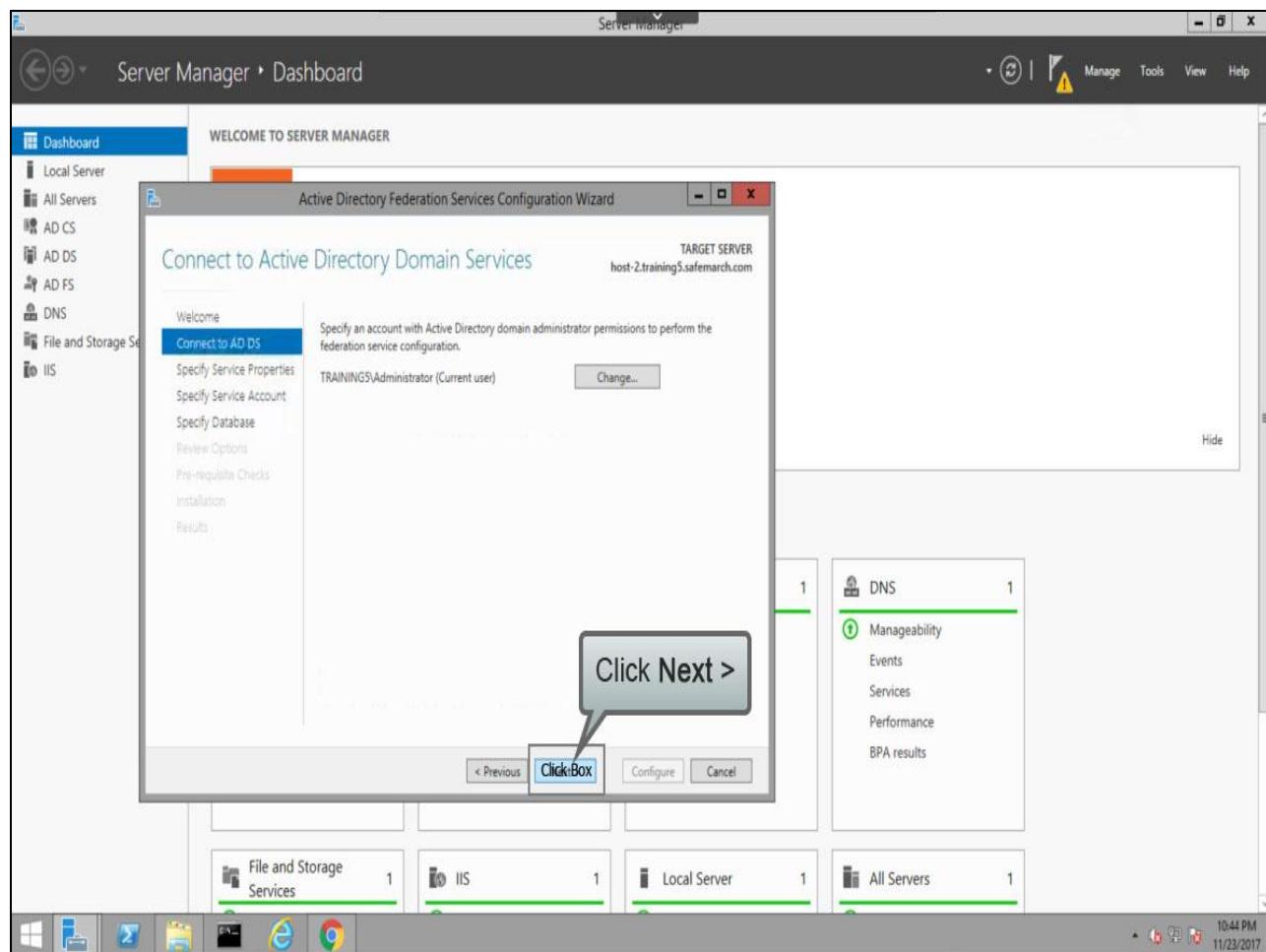
## Slide 33 - Slide 33



## Slide notes

In this case we are creating the first federation server in a server farm, so we just need to click **Next >**.

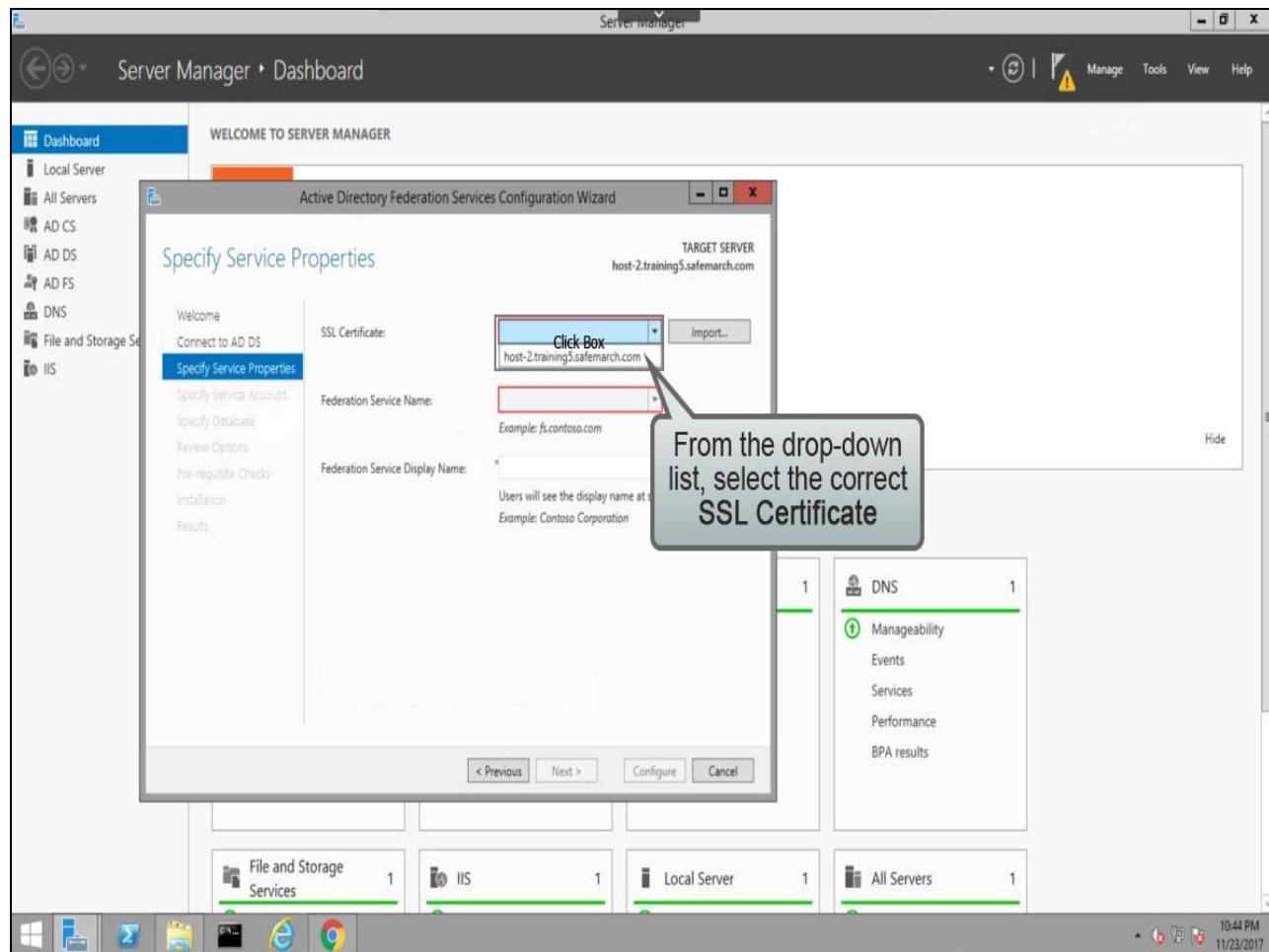
## Slide 34 - Slide 34



## Slide notes

To use the current admin user account for the configuration, click **Next >**.

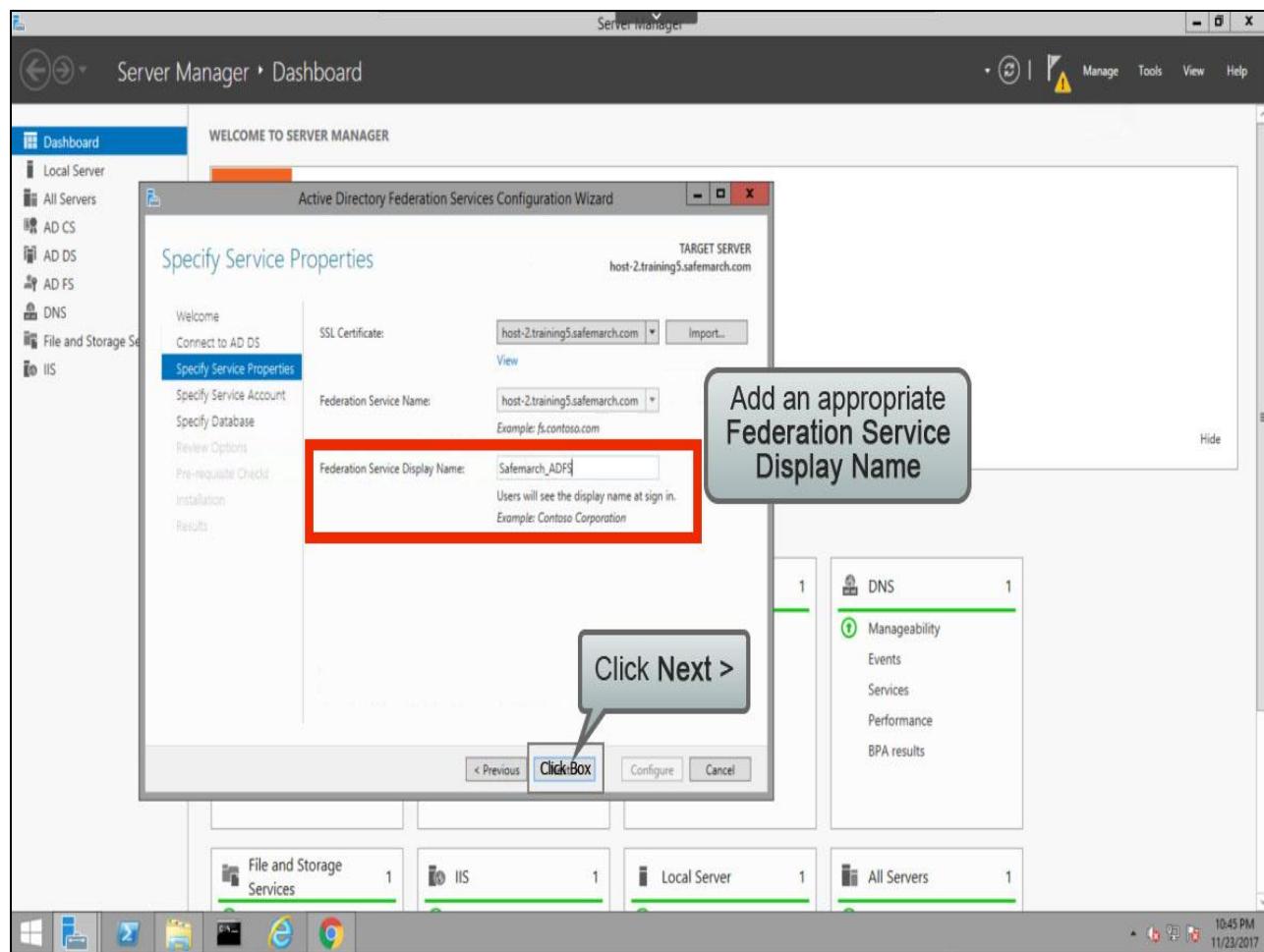
## Slide 35 - Slide 35



## Slide notes

From the drop-down list, select the correct **SSL Certificate** to use for signing the assertions.

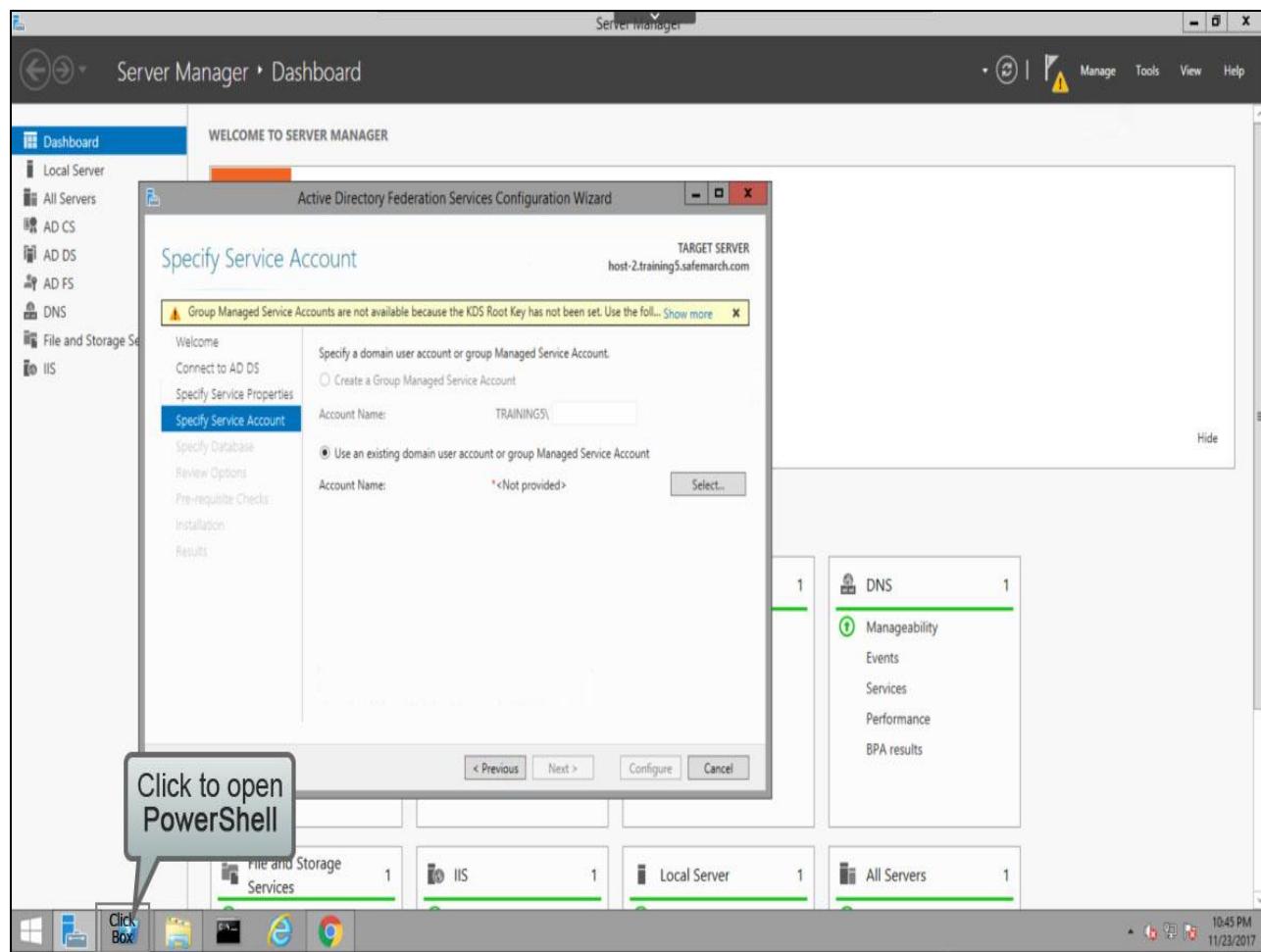
## Slide 36 - Slide 36



## Slide notes

Provide an appropriate **Federation Service Display Name** and click **Next >**.

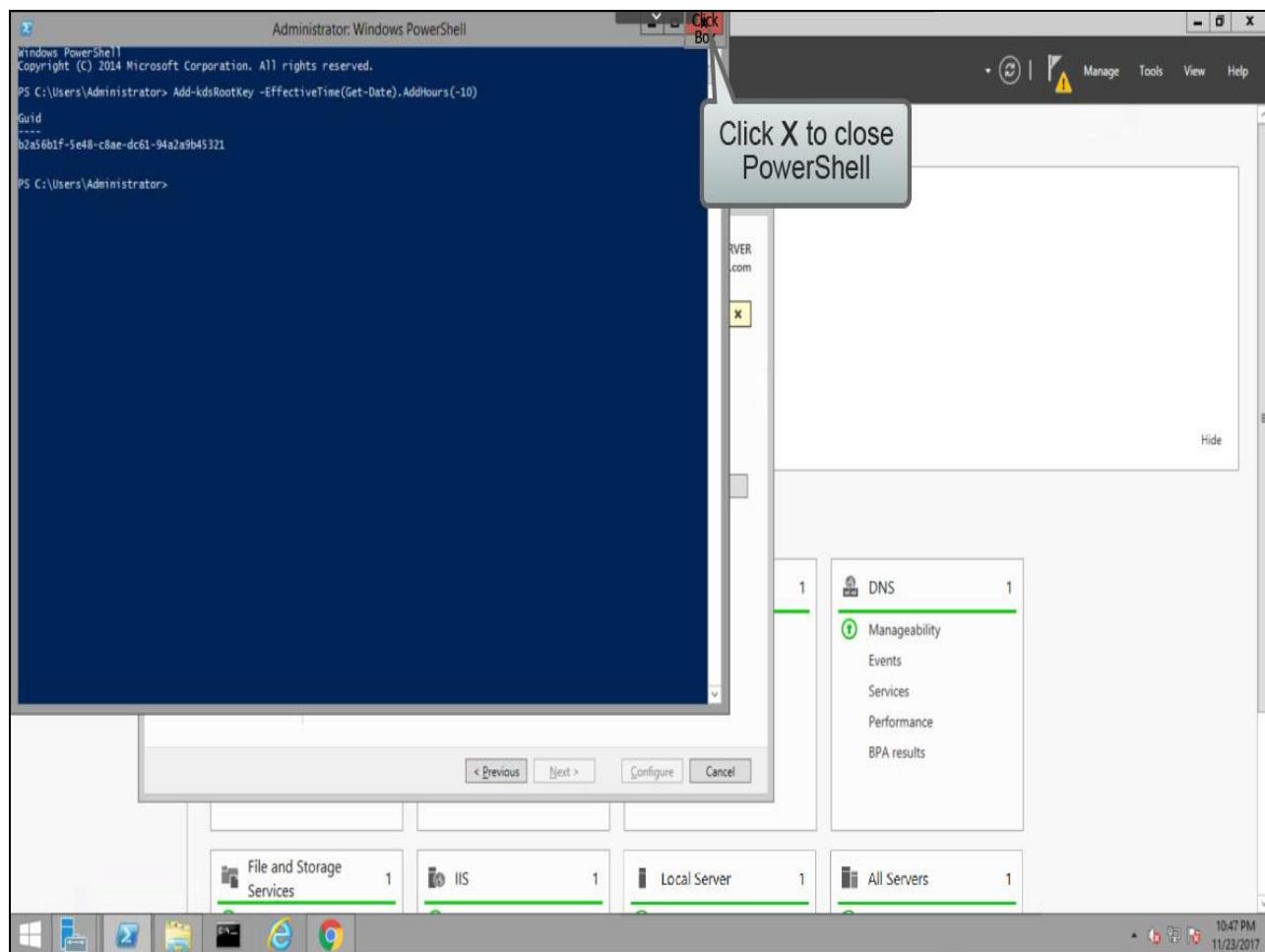
## Slide 37 - Slide 37



## Slide notes

At this point, we could use a regular domain user account for the service, however best practice is to create a **Group Managed Service Account**, however before we can do that there's a command we have to run in PowerShell, ...so click to open a **PowerShell** window, ...

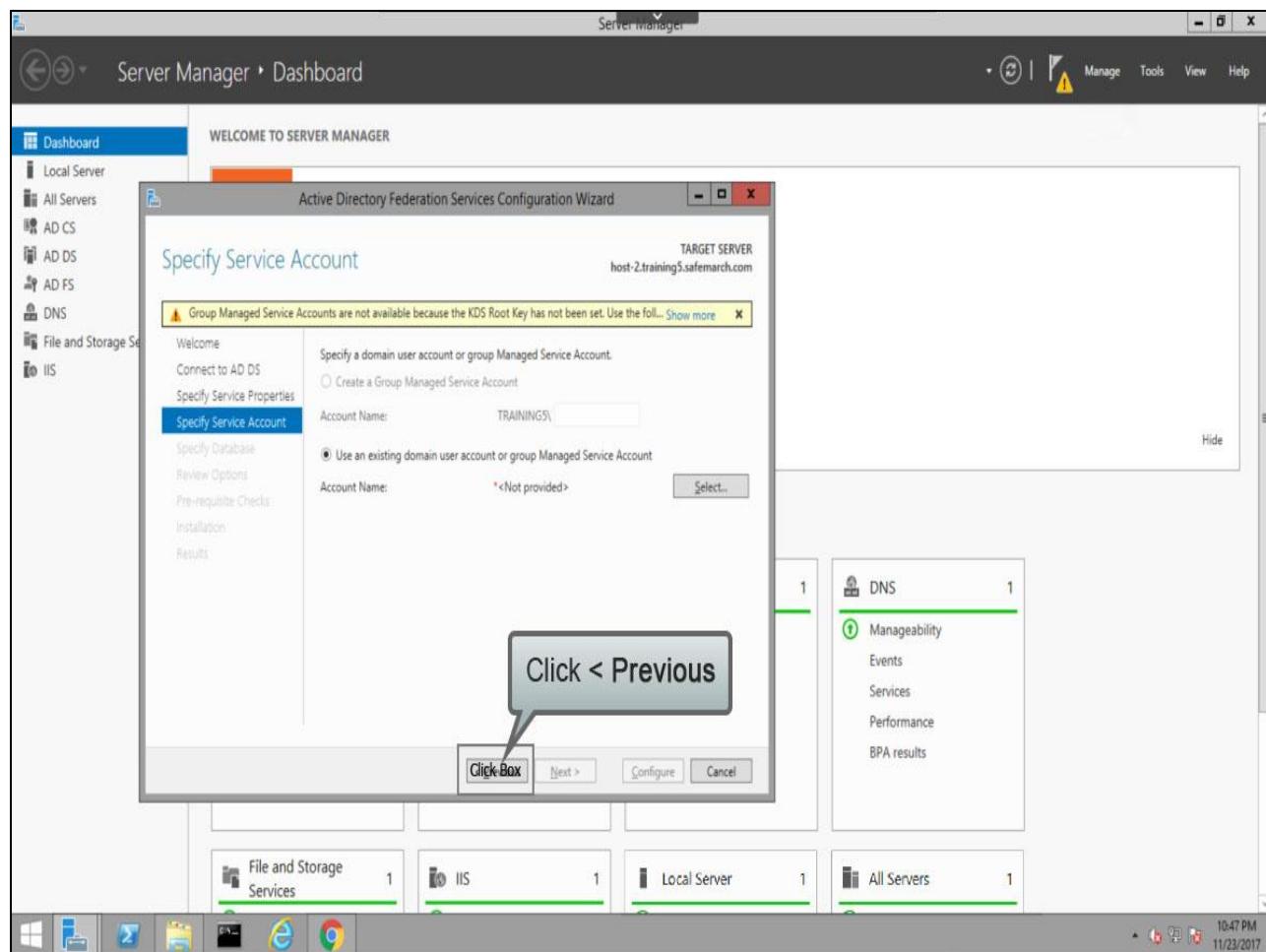
## Slide 38 - Slide 38



## Slide notes

...and enter the command shown here (`Add-kdsRootKey -EffectiveTime(Get-Date).AddHours(-10)`), then close the PowerShell window. Note that this command is case sensitive.

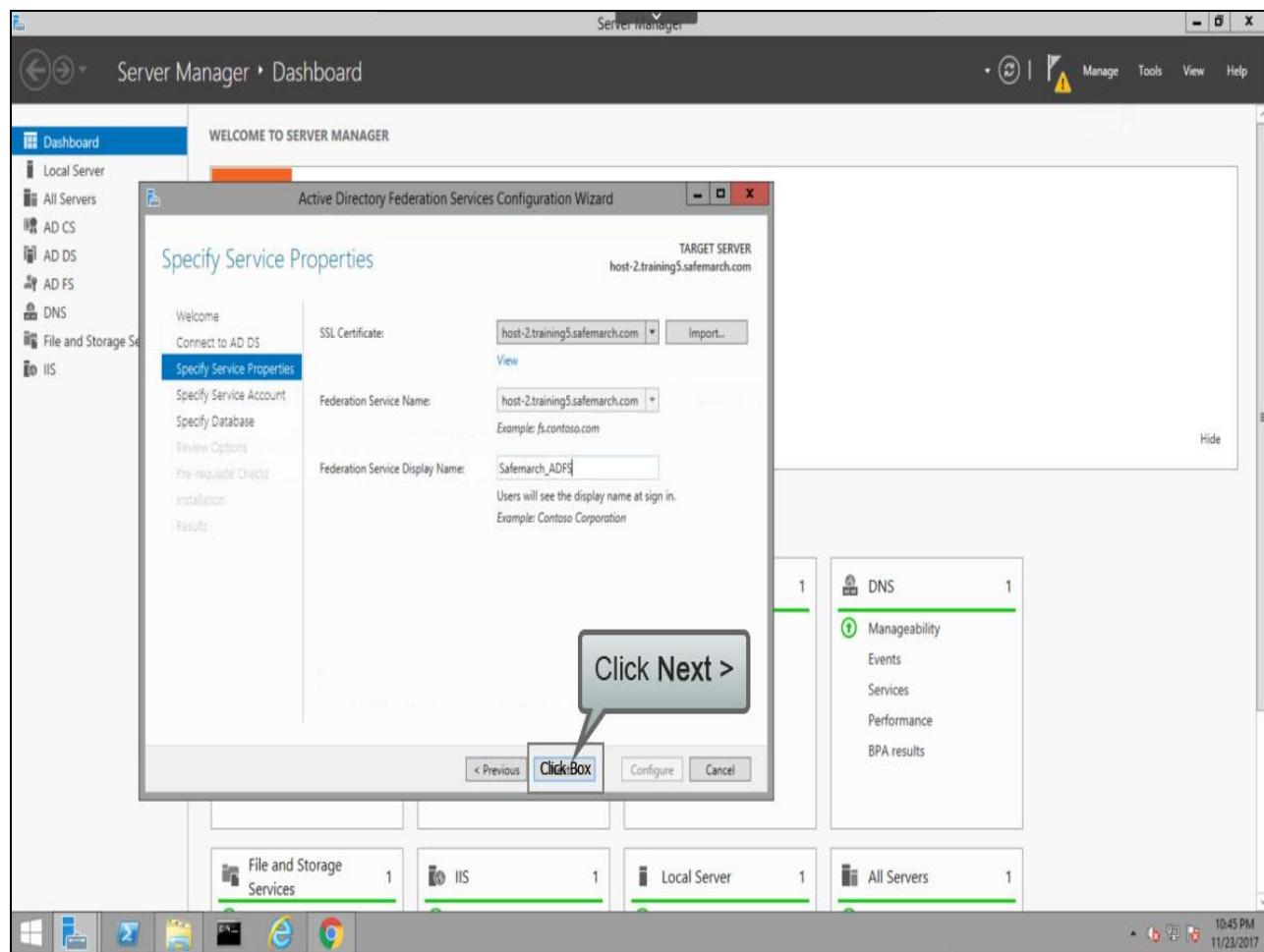
## Slide 39 - Slide 39



## Slide notes

Back in the ADFS configuration wizard, click < Previous, ...

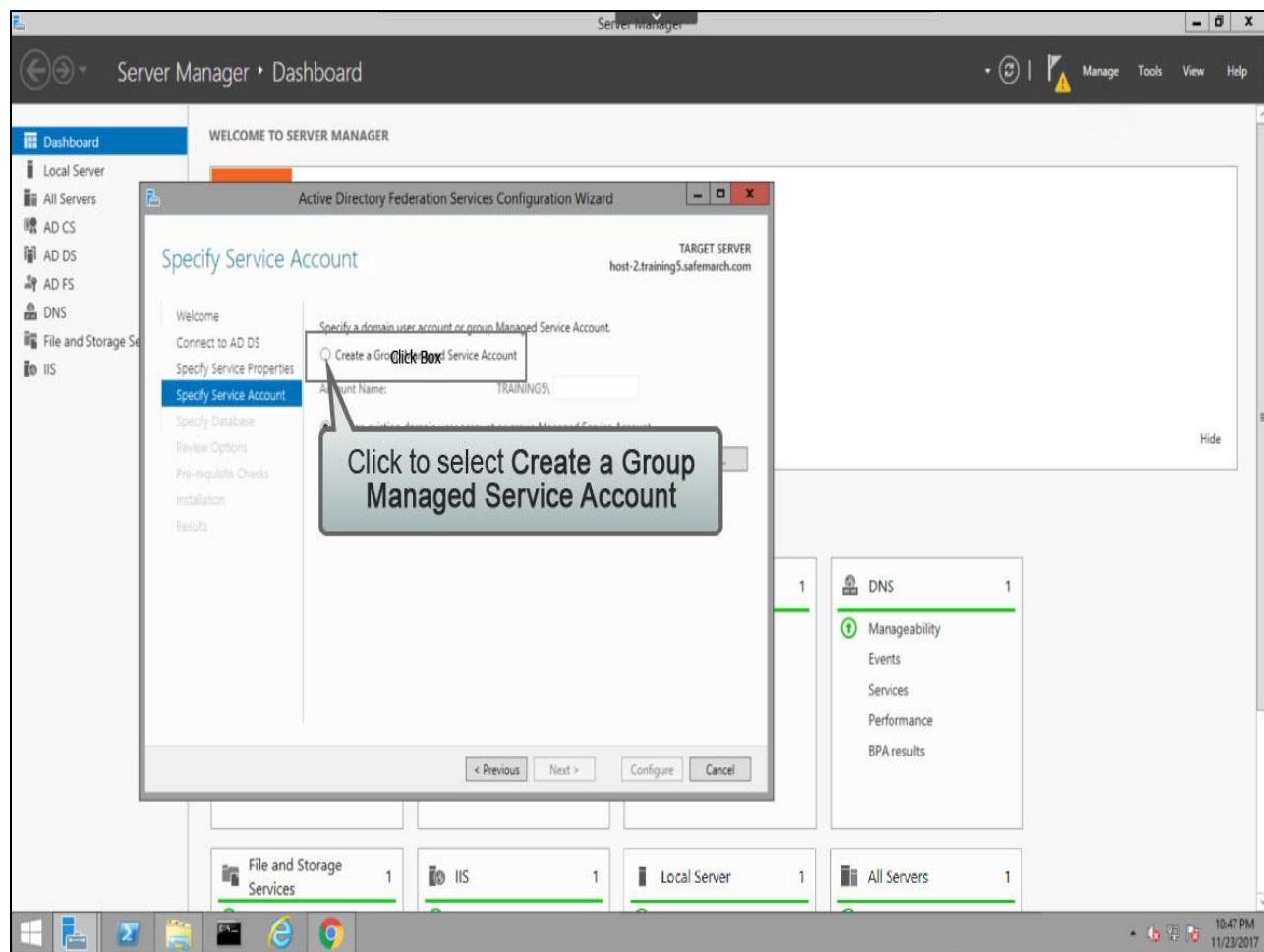
## Slide 40 - Slide 40



## Slide notes

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

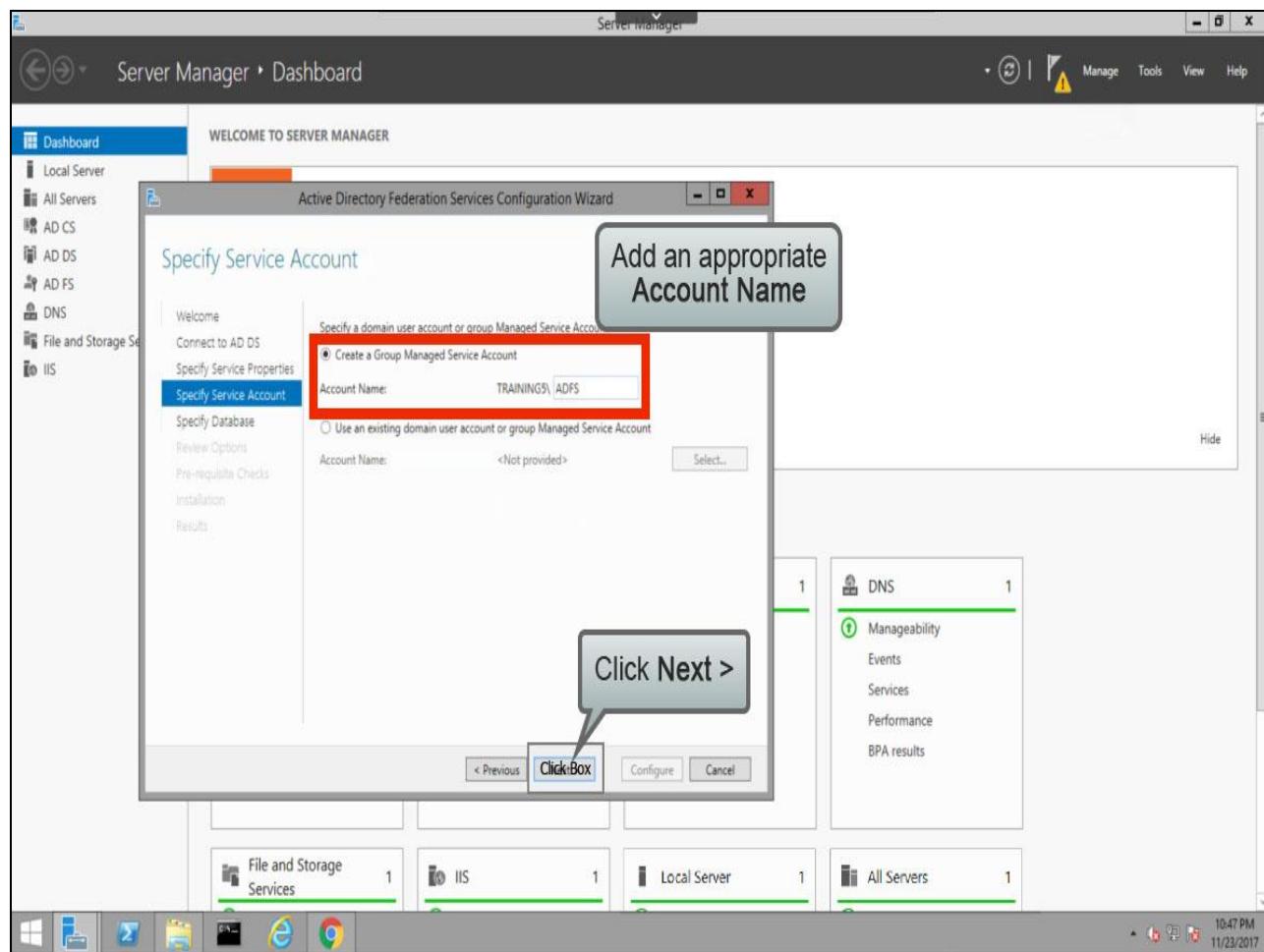
## Slide 41 - Slide 41



## Slide notes

...and now you have the possibility to select the **Create a Group Managed Service Account** option.

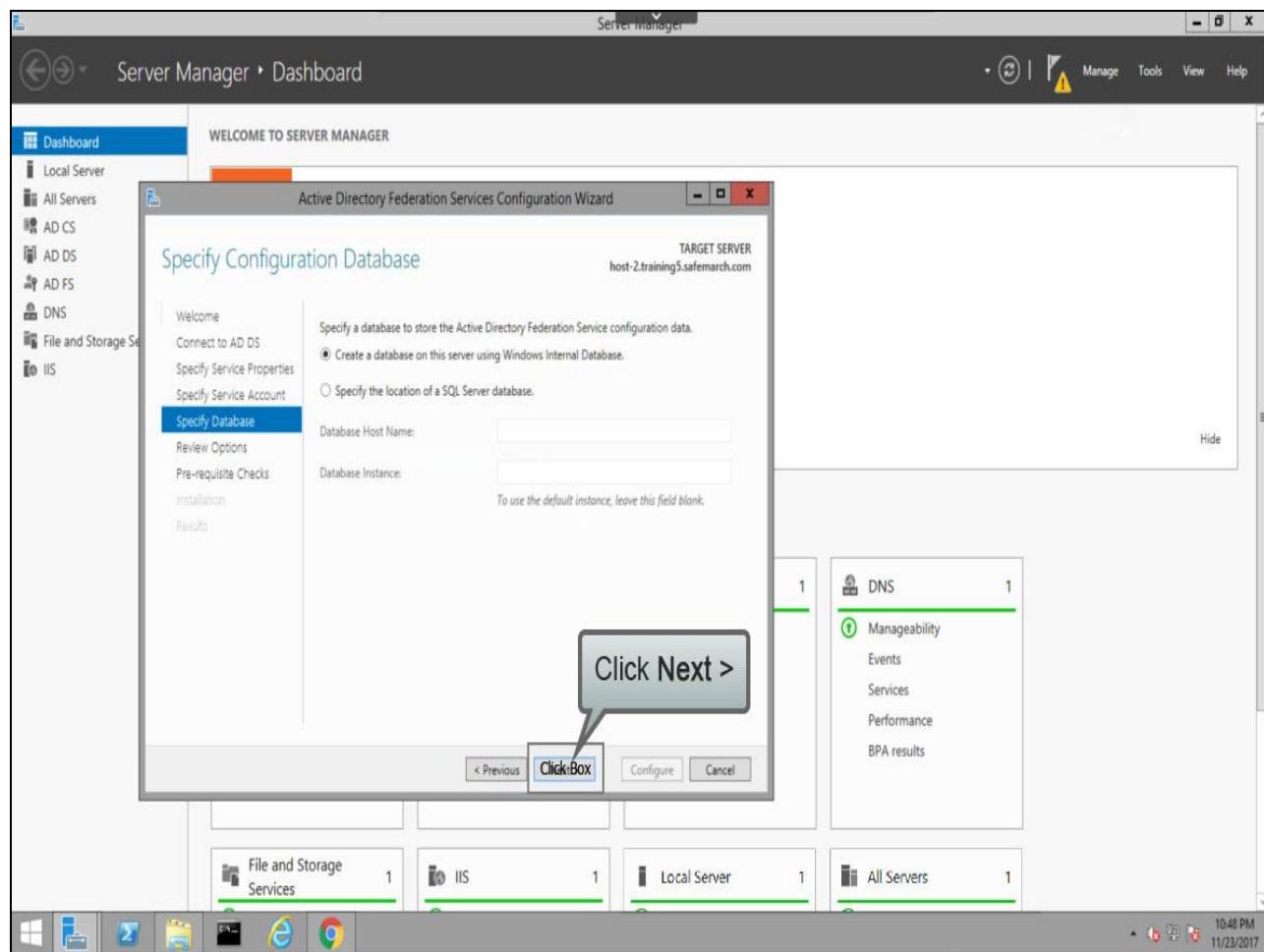
## Slide 42 - Slide 42



## Slide notes

Specify an appropriate **Account Name** and click **Next >**.

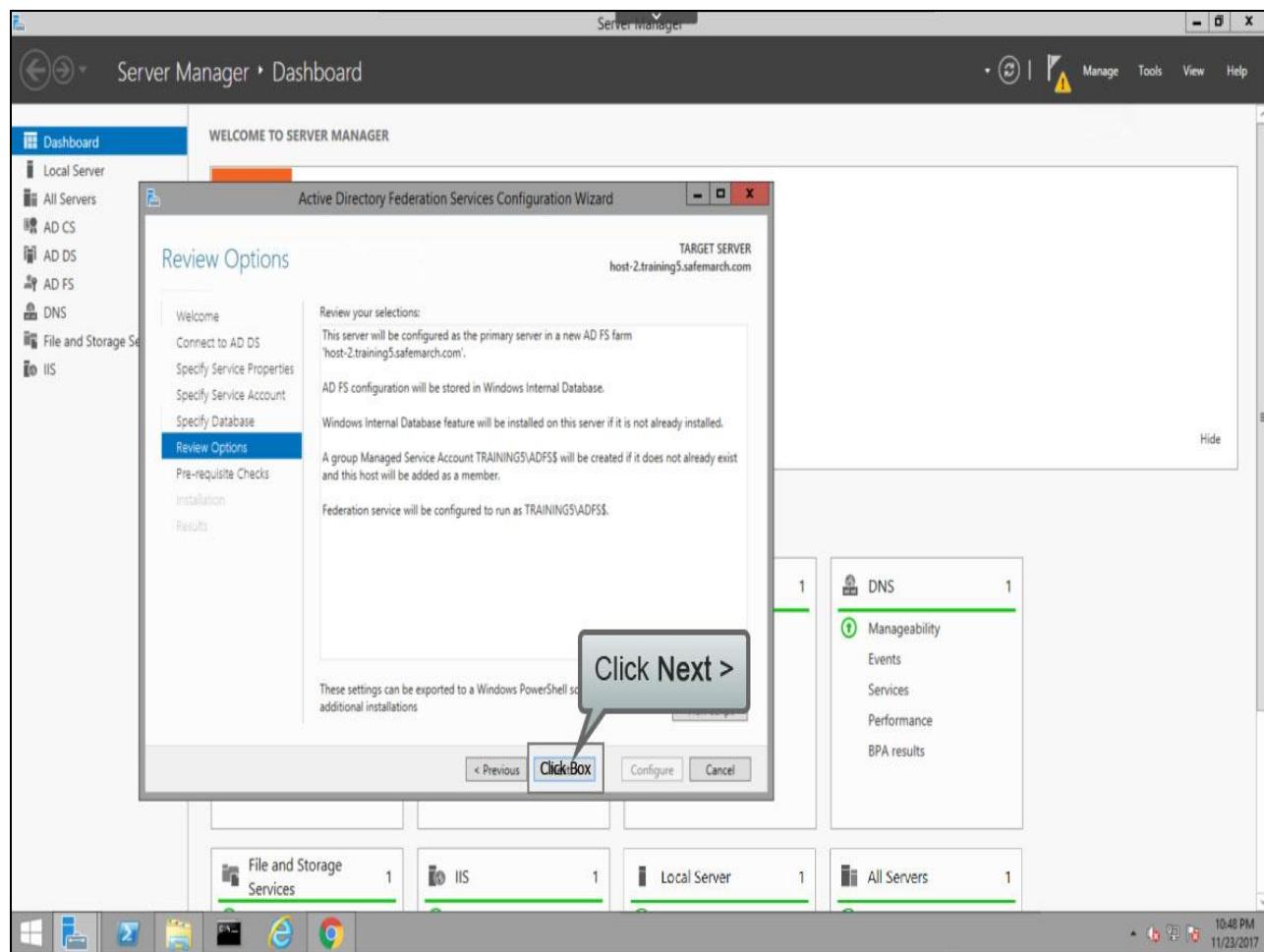
## Slide 43 - Slide 43



## Slide notes

Specify the location of the **Database** and click **Next >**.

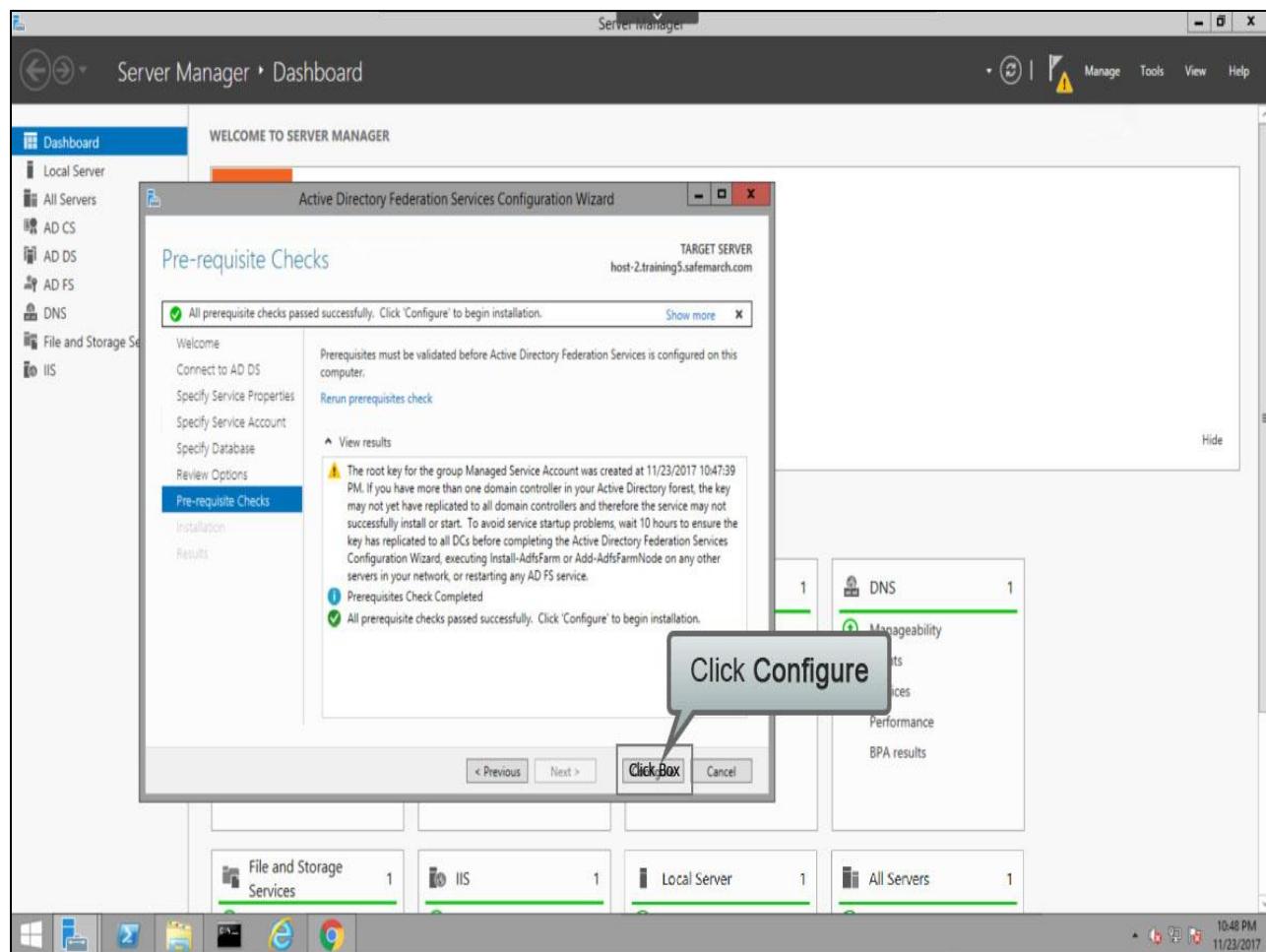
## Slide 44 - Slide 44



## Slide notes

Review the options selected and click **Next >**, ...

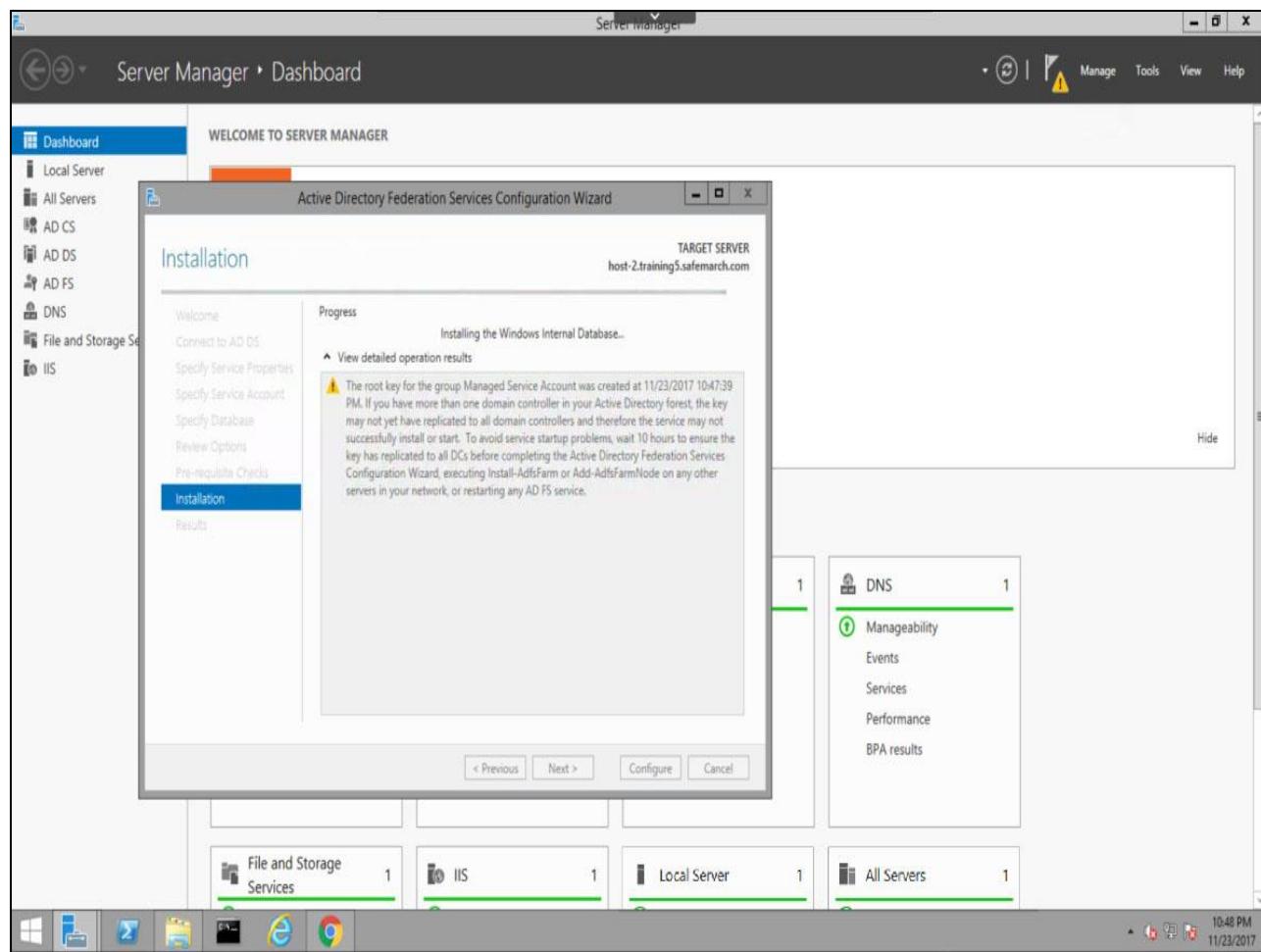
## Slide 45 - Slide 45



## Slide notes

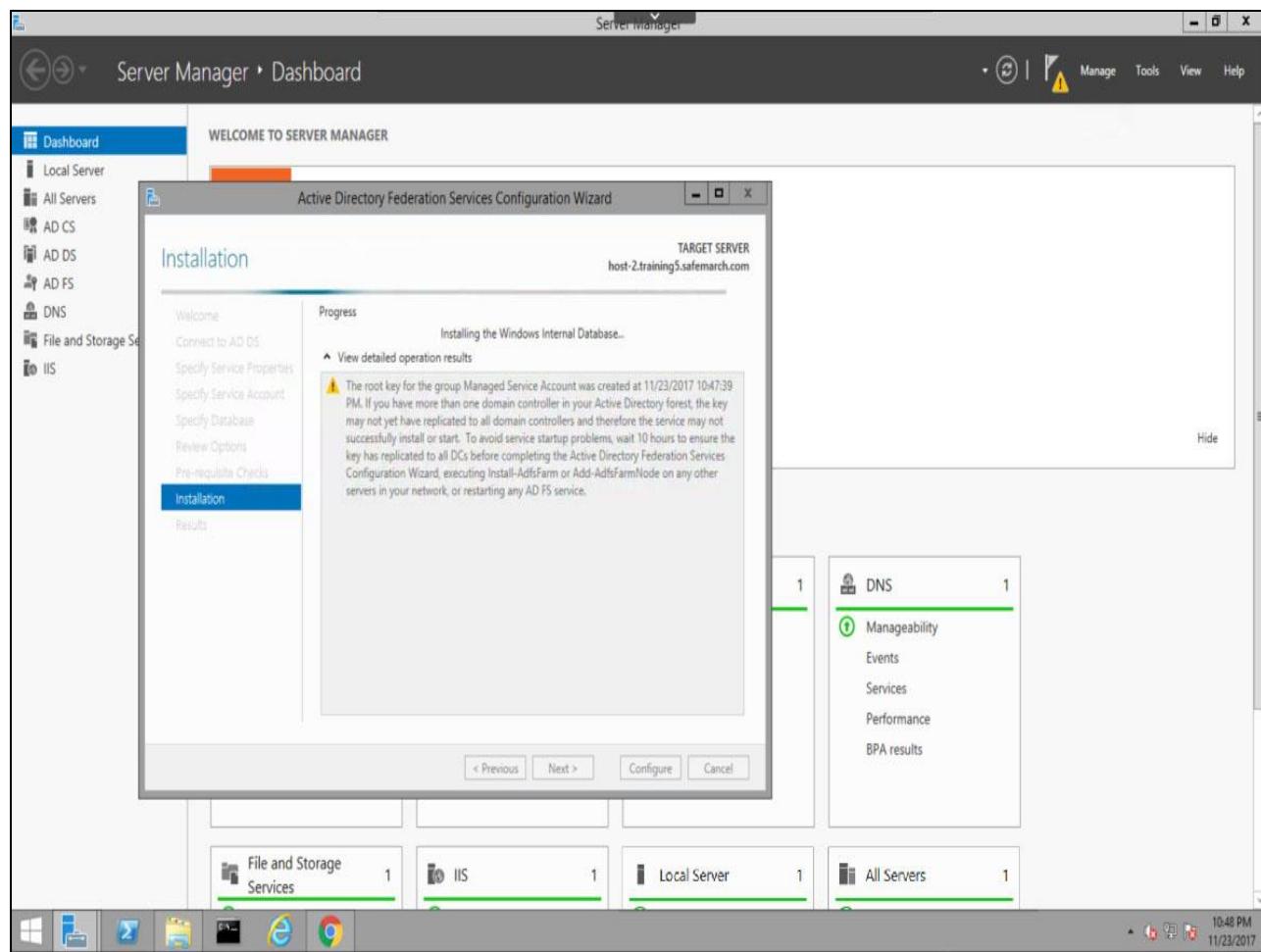
...then click **Configure**.

## Slide 46 - Slide 46



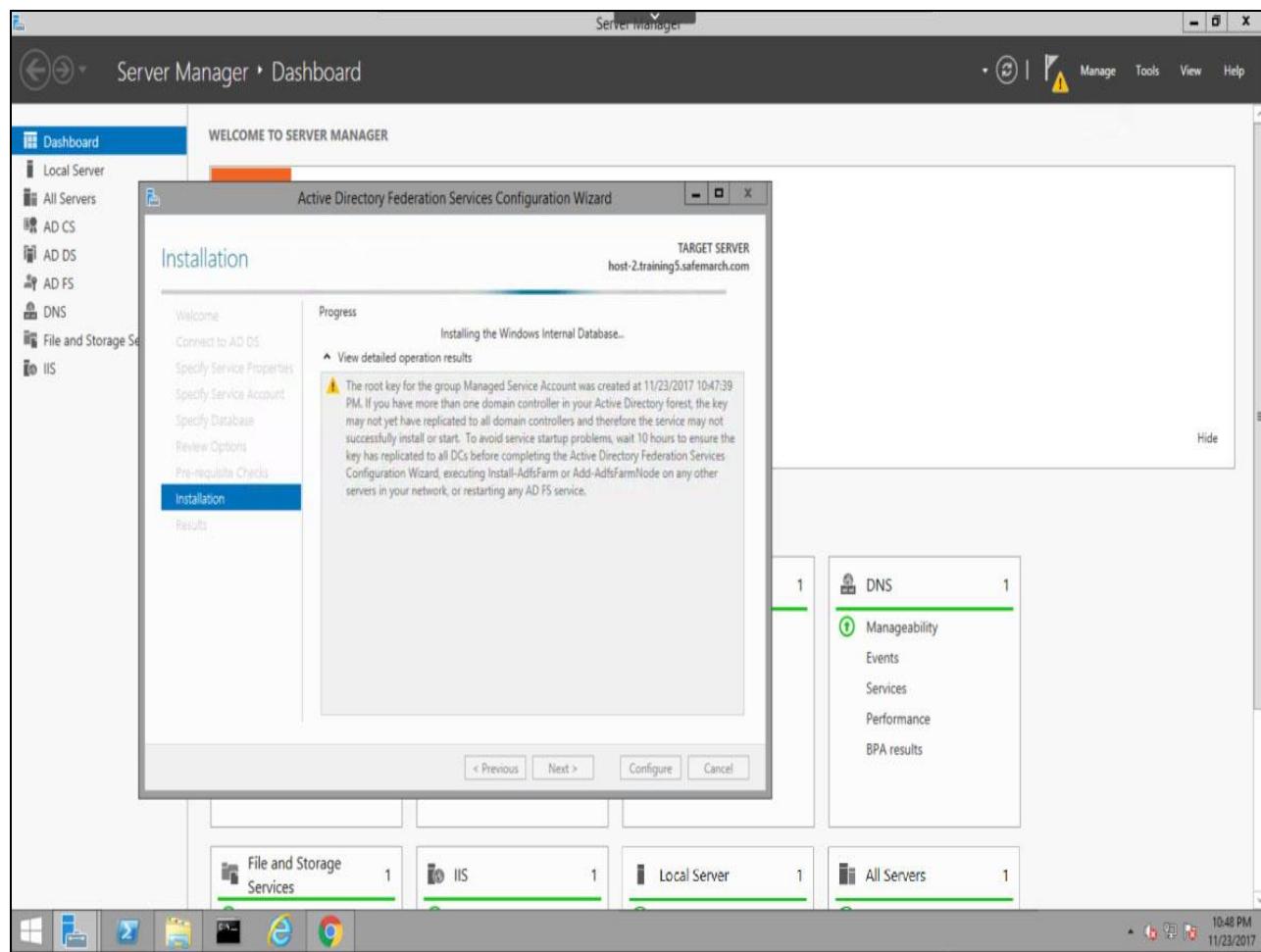
## Slide notes

## Slide 47 - Slide 47



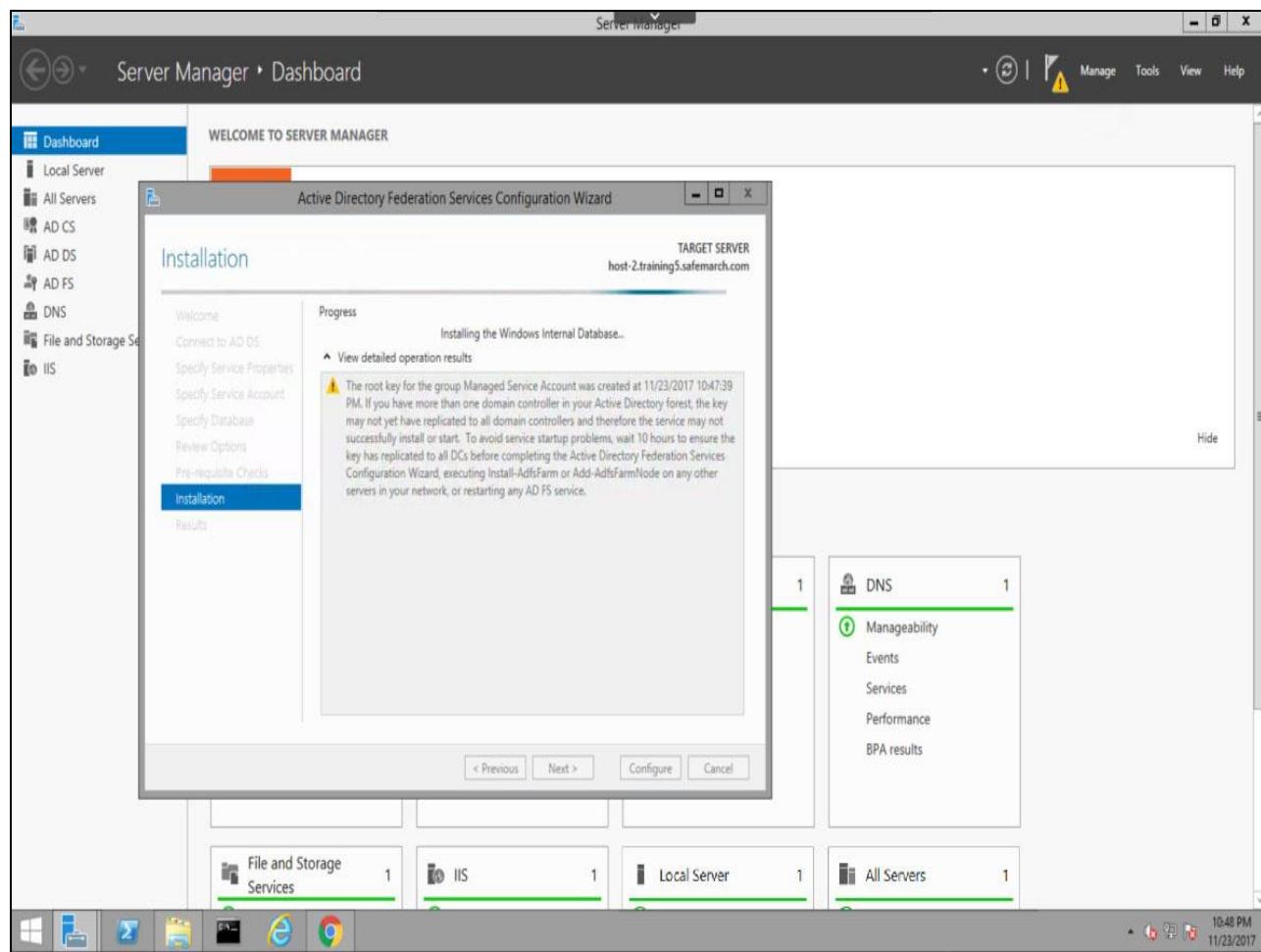
## Slide notes

## Slide 48 - Slide 48



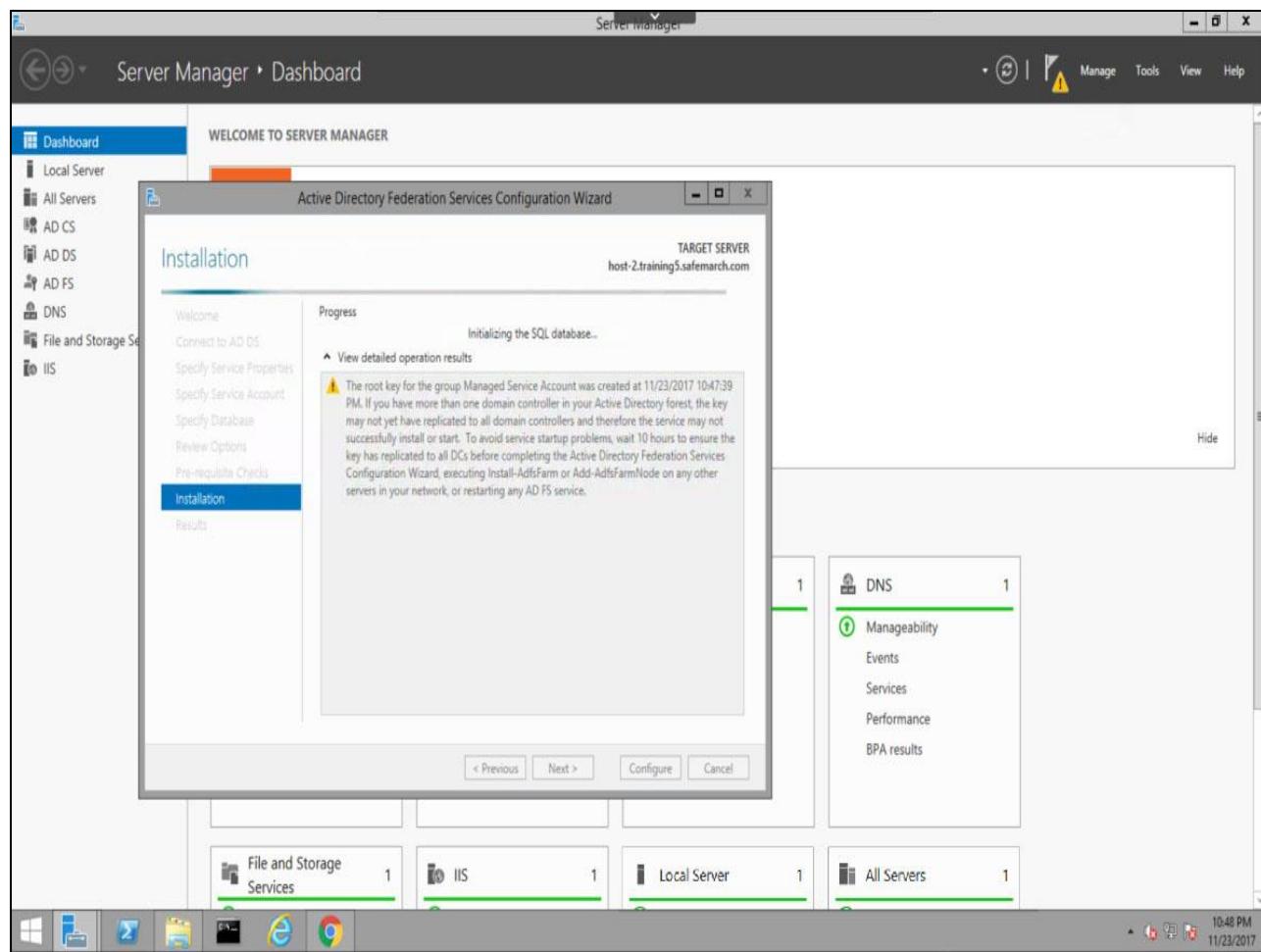
## Slide notes

## Slide 49 - Slide 49



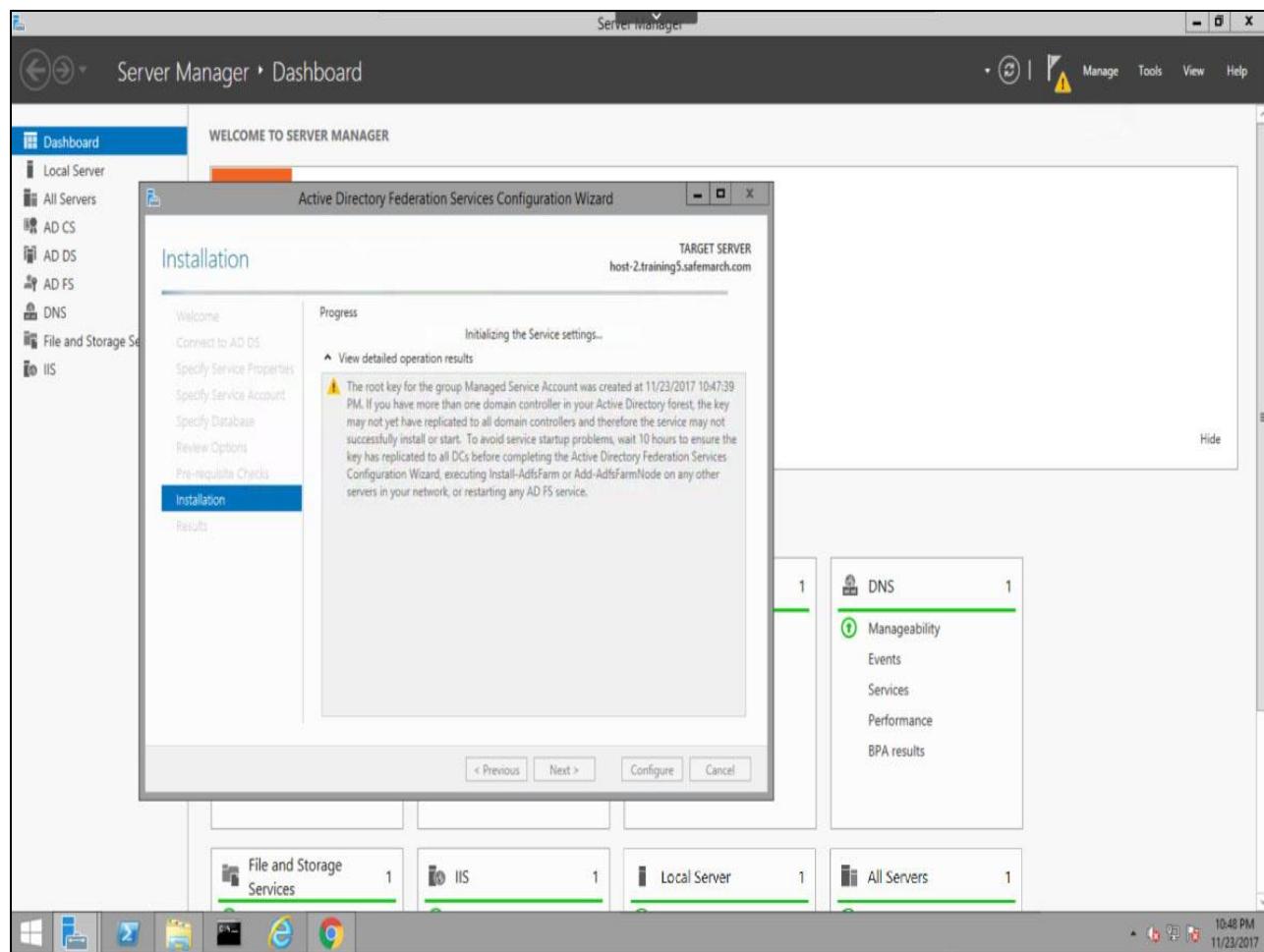
## Slide notes

## Slide 50 - Slide 50



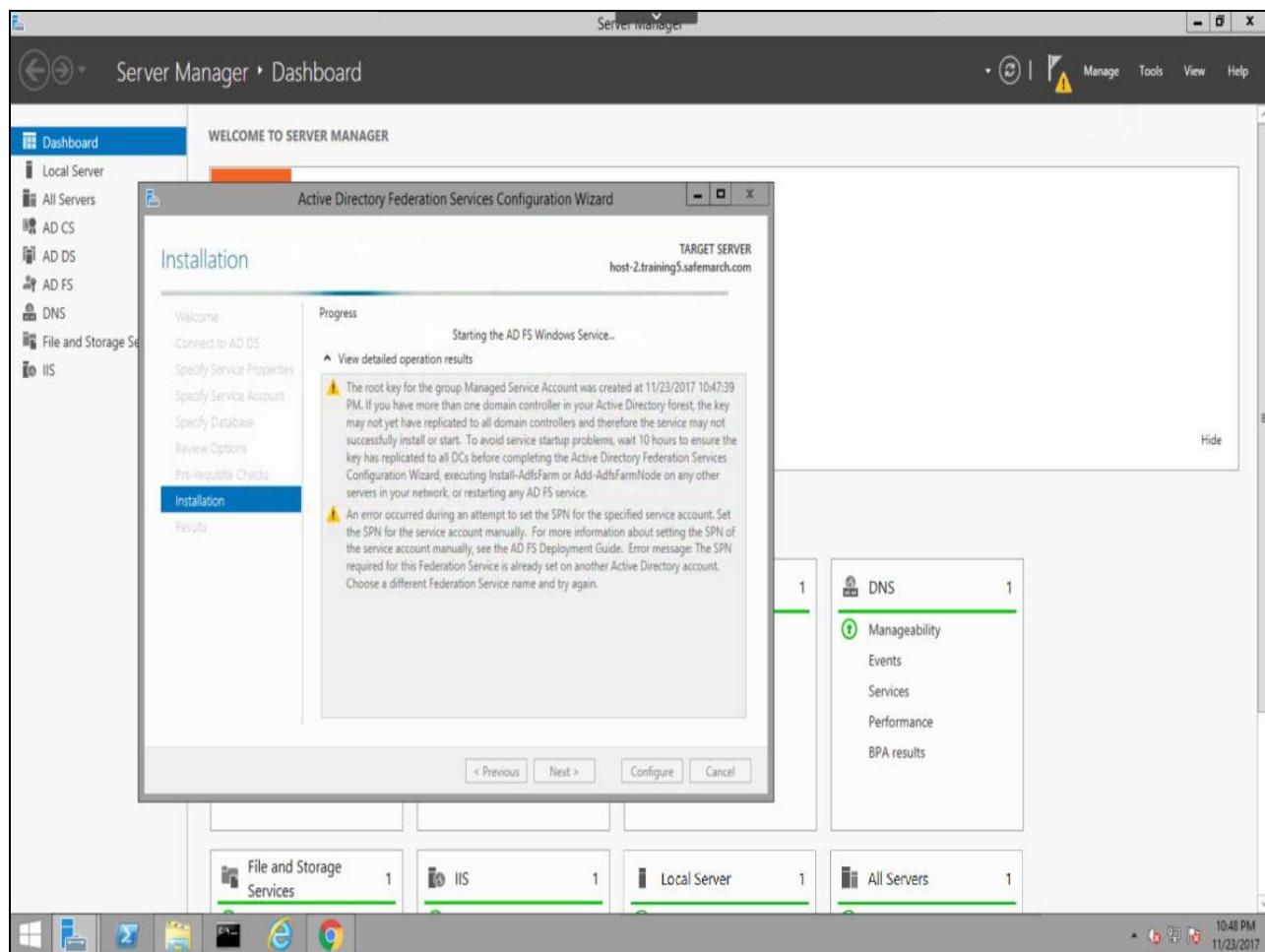
## Slide notes

## Slide 51 - Slide 51



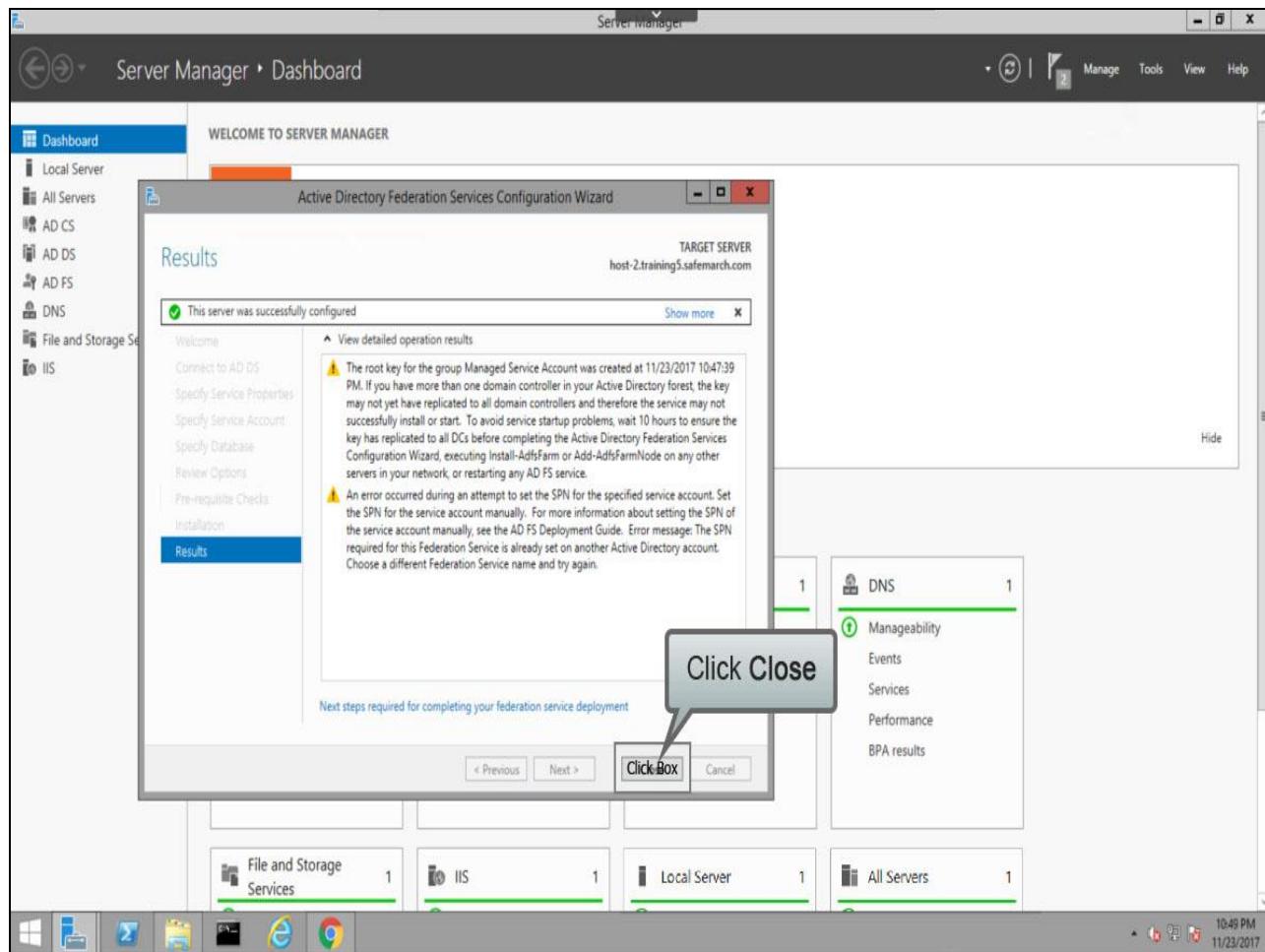
## Slide notes

## Slide 52 - Slide 52



## Slide notes

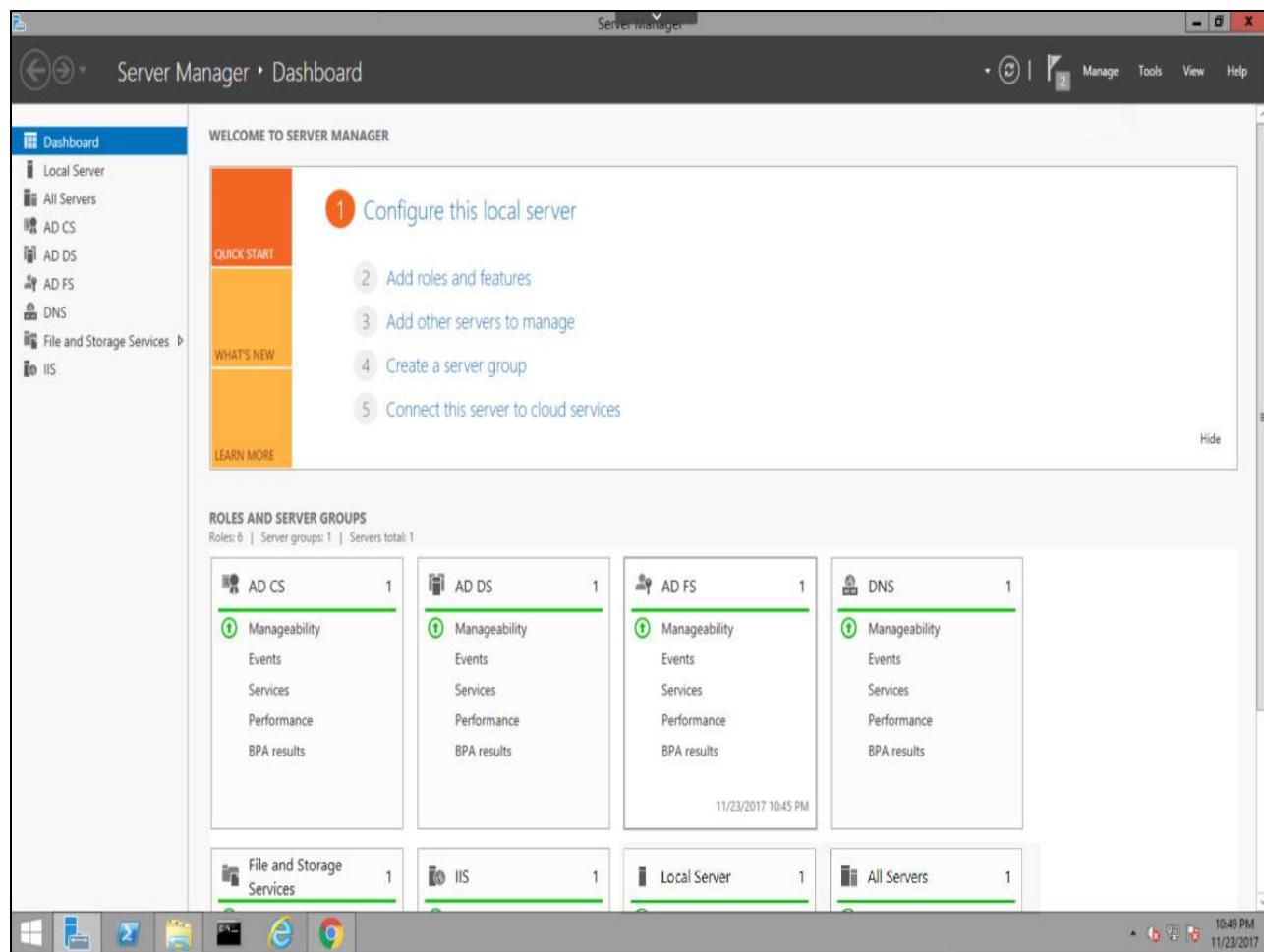
## Slide 53 - Slide 53



## Slide notes

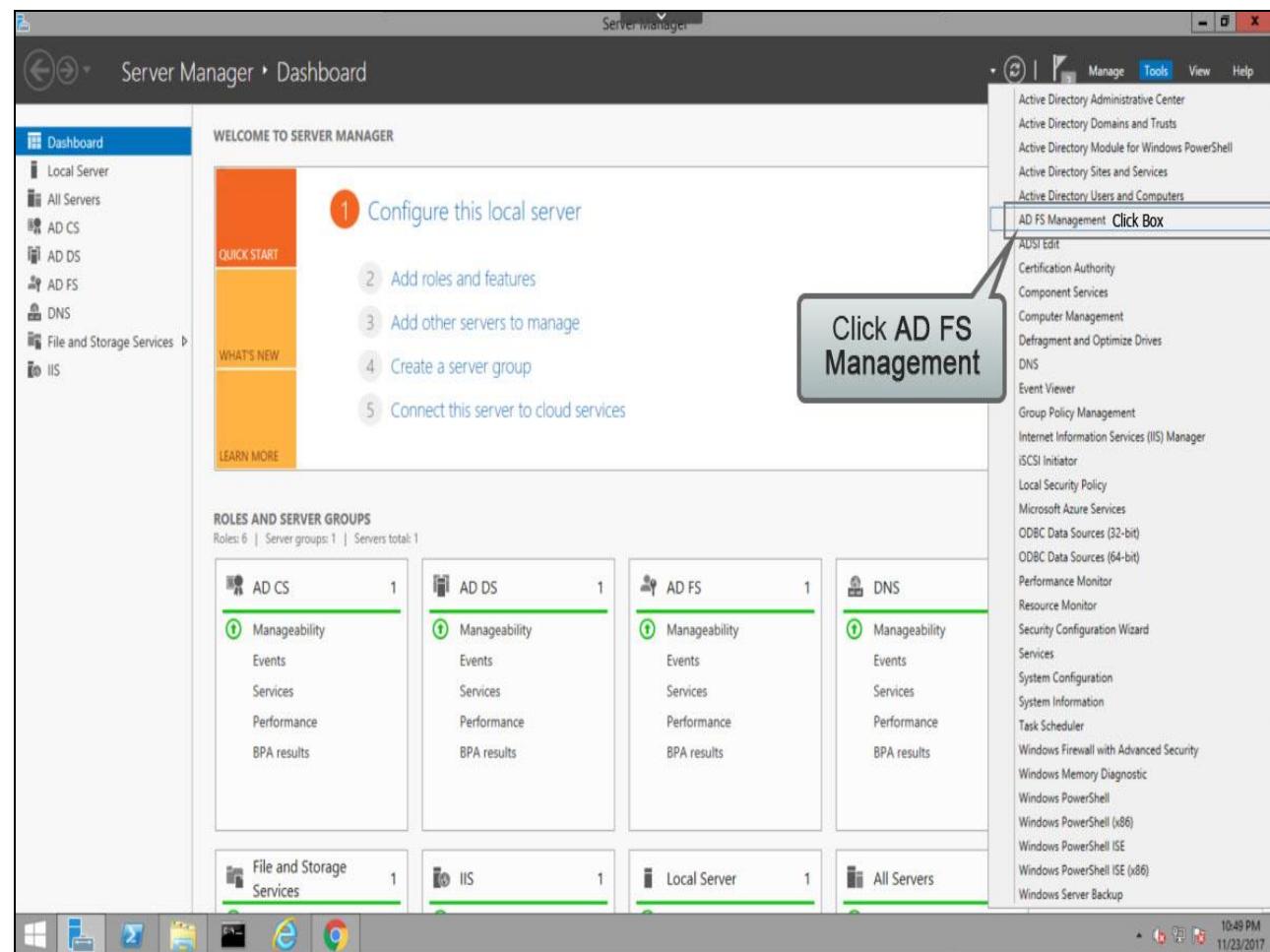
Once the configuration is complete, click **Close** to exit the wizard.

## Slide 54 - Slide 54



## Slide notes

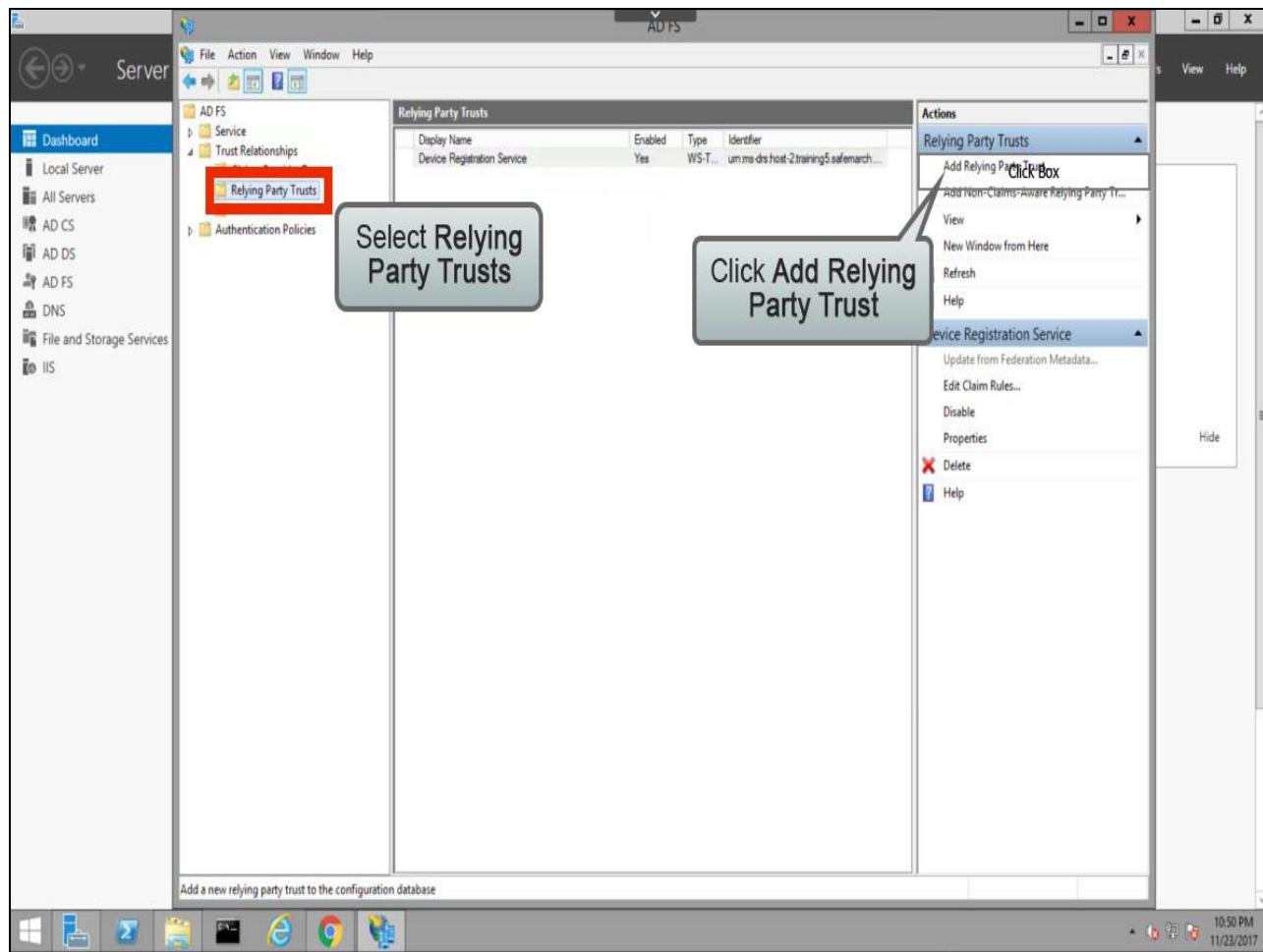
## Slide 55 - Slide 55



## Slide notes

At the Server Manager Dashboard, from the **Tools** menu, click **AD FS Management**.

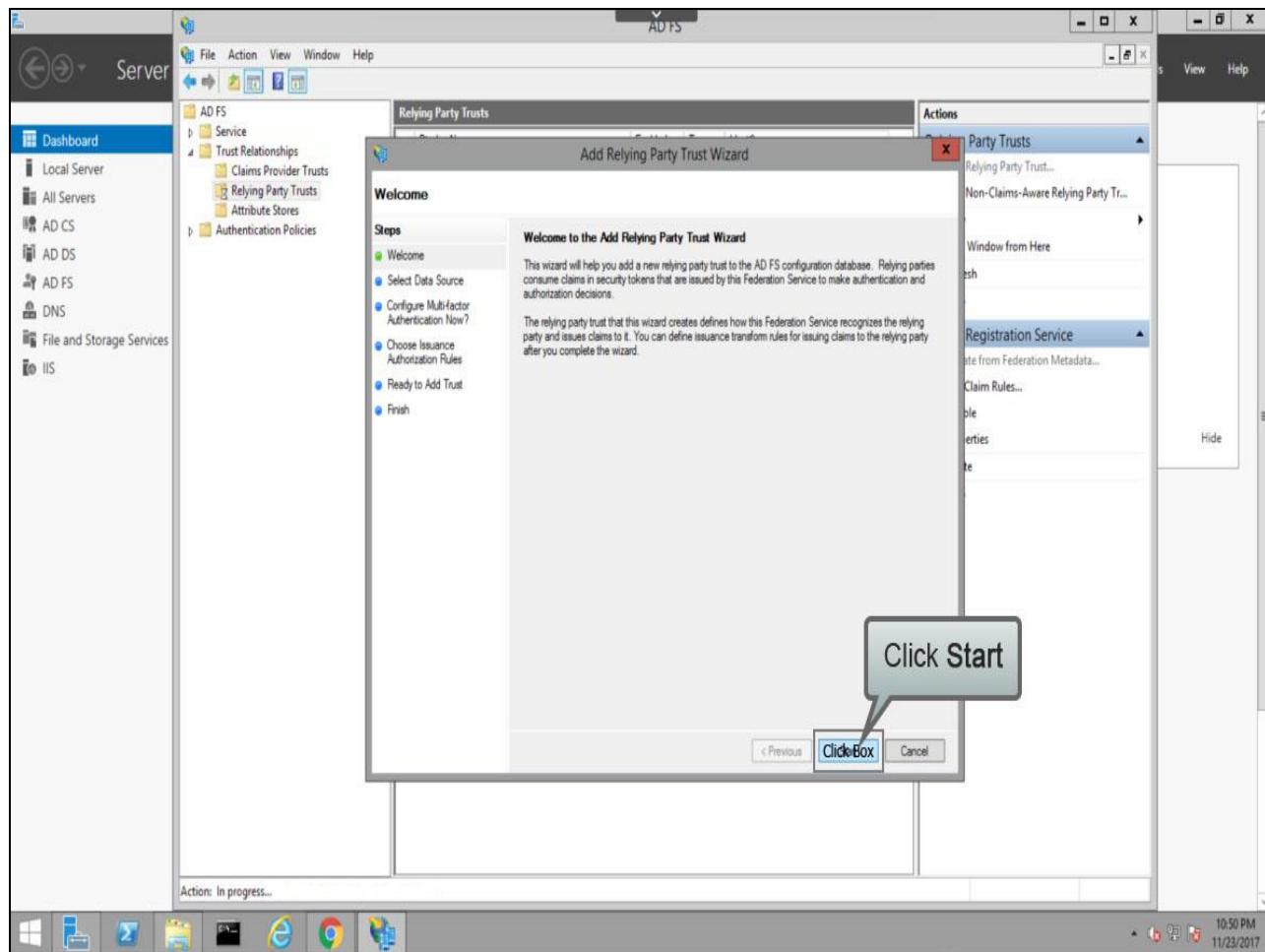
## Slide 56 - Slide 56



## Slide notes

In the left-hand navigation panel, expand the **Trust Relationships** folder, and select **Relying Party Trusts**. Then in the **Actions** panel, click **Add Relying Party Trust**.

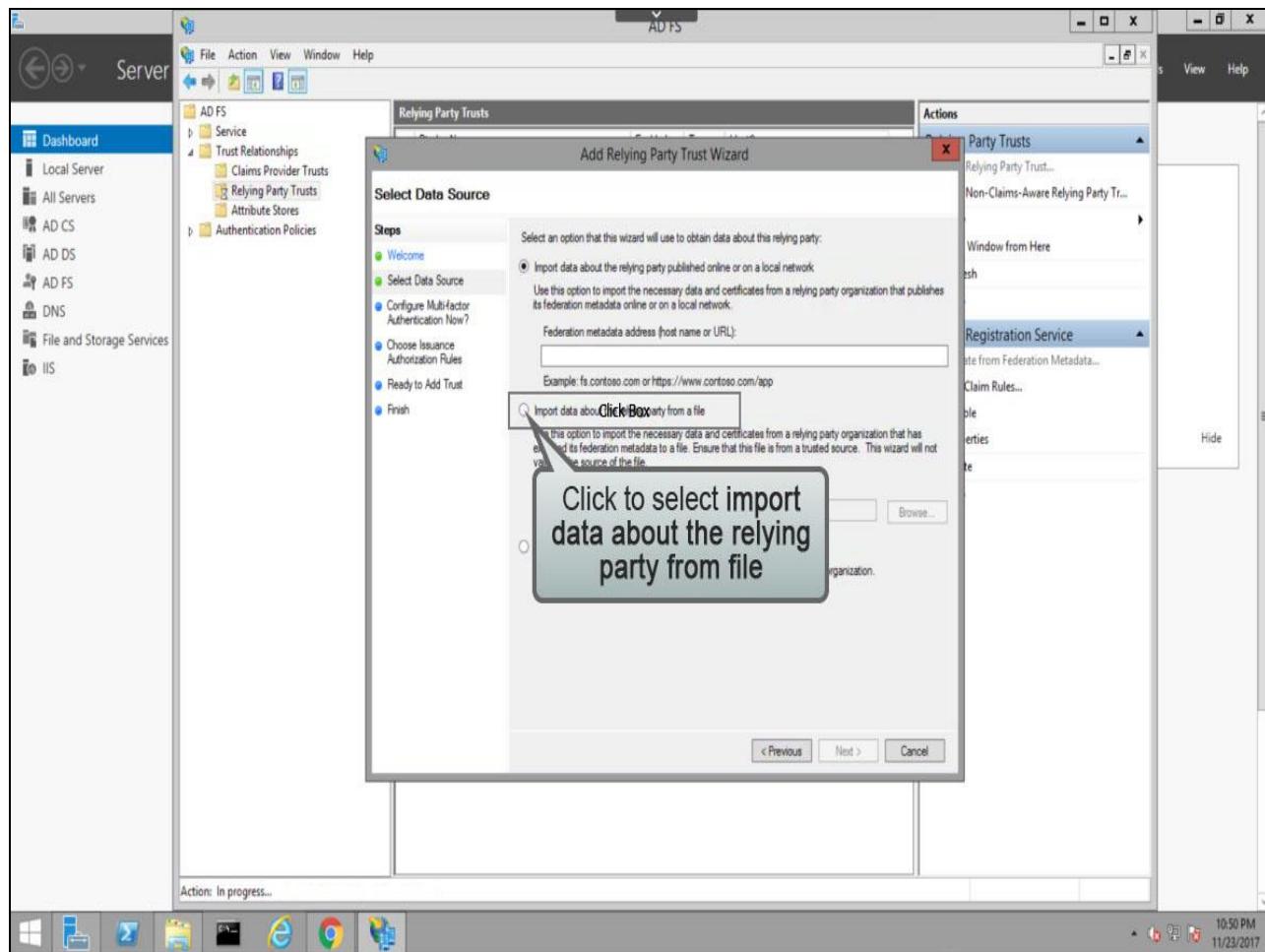
## Slide 57 - Slide 57



## Slide notes

To start the wizard, click **Start**, ...

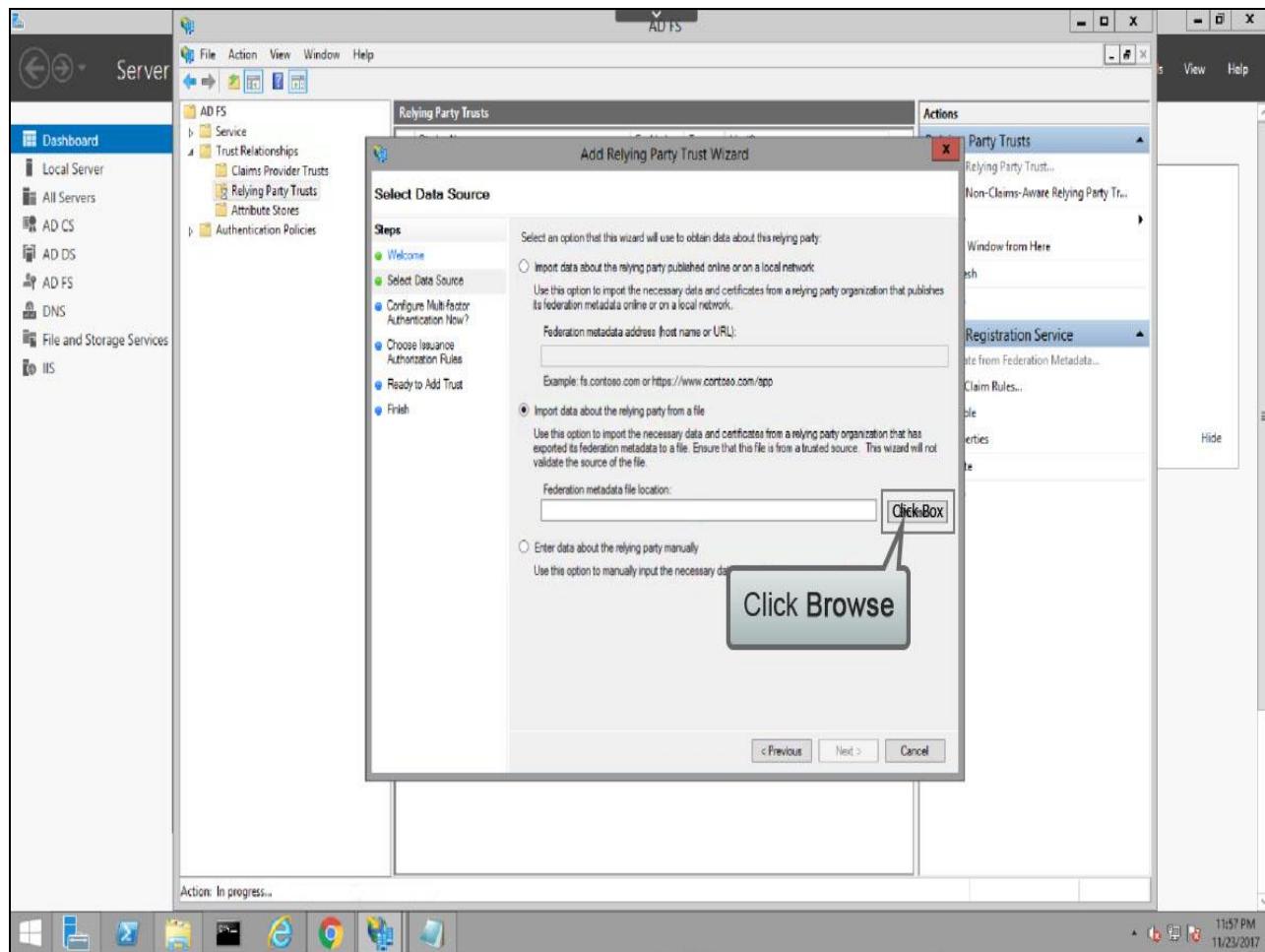
## Slide 58 - Slide 58



## Slide notes

You can add the details for a **Relying Party** manually, however we will do it using the Metadata file we saved earlier. Click to select **import data about the relying party from file**, ...

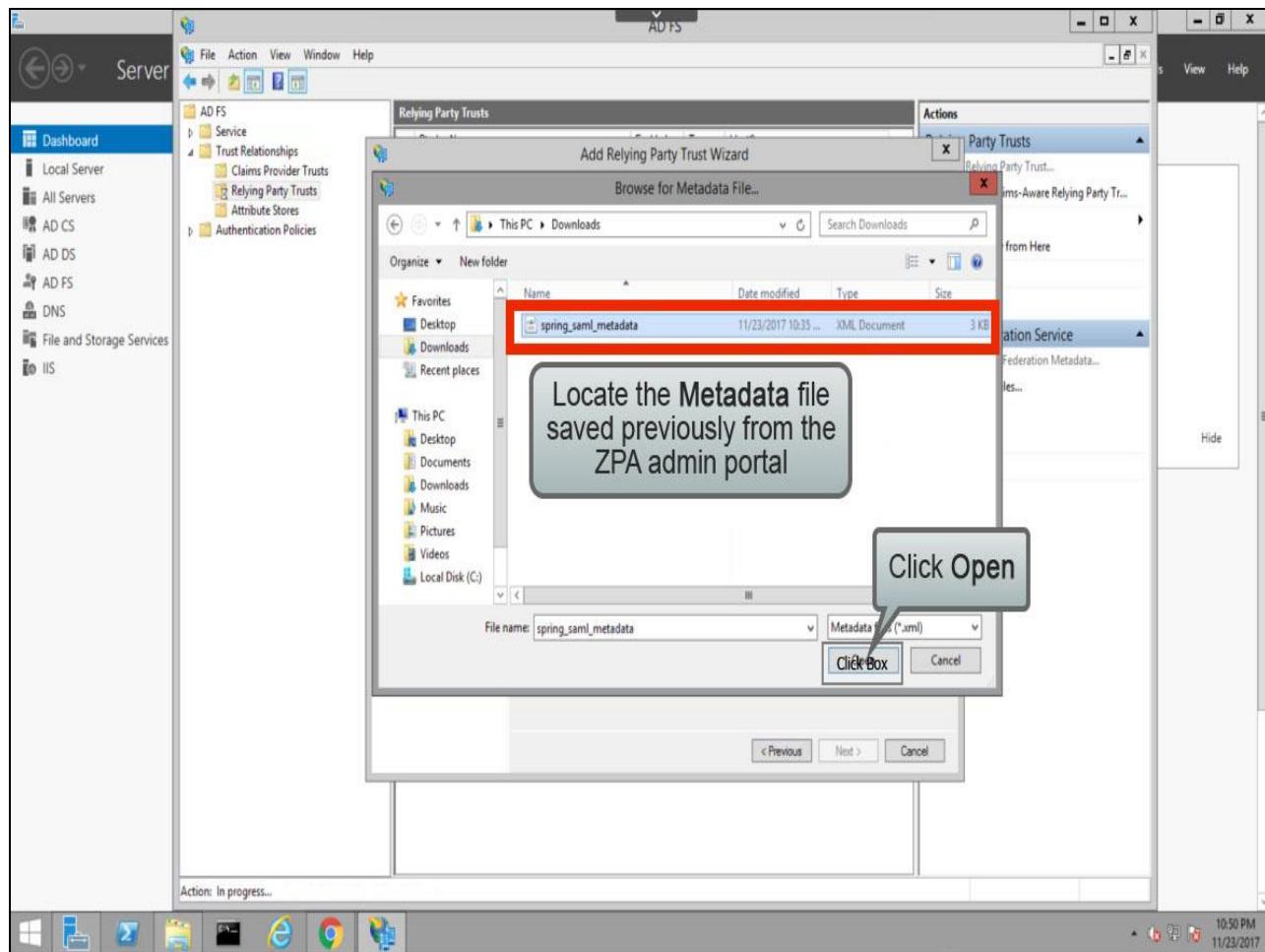
## Slide 59 - Slide 59



## Slide notes

...then click **Browse** to locate the file.

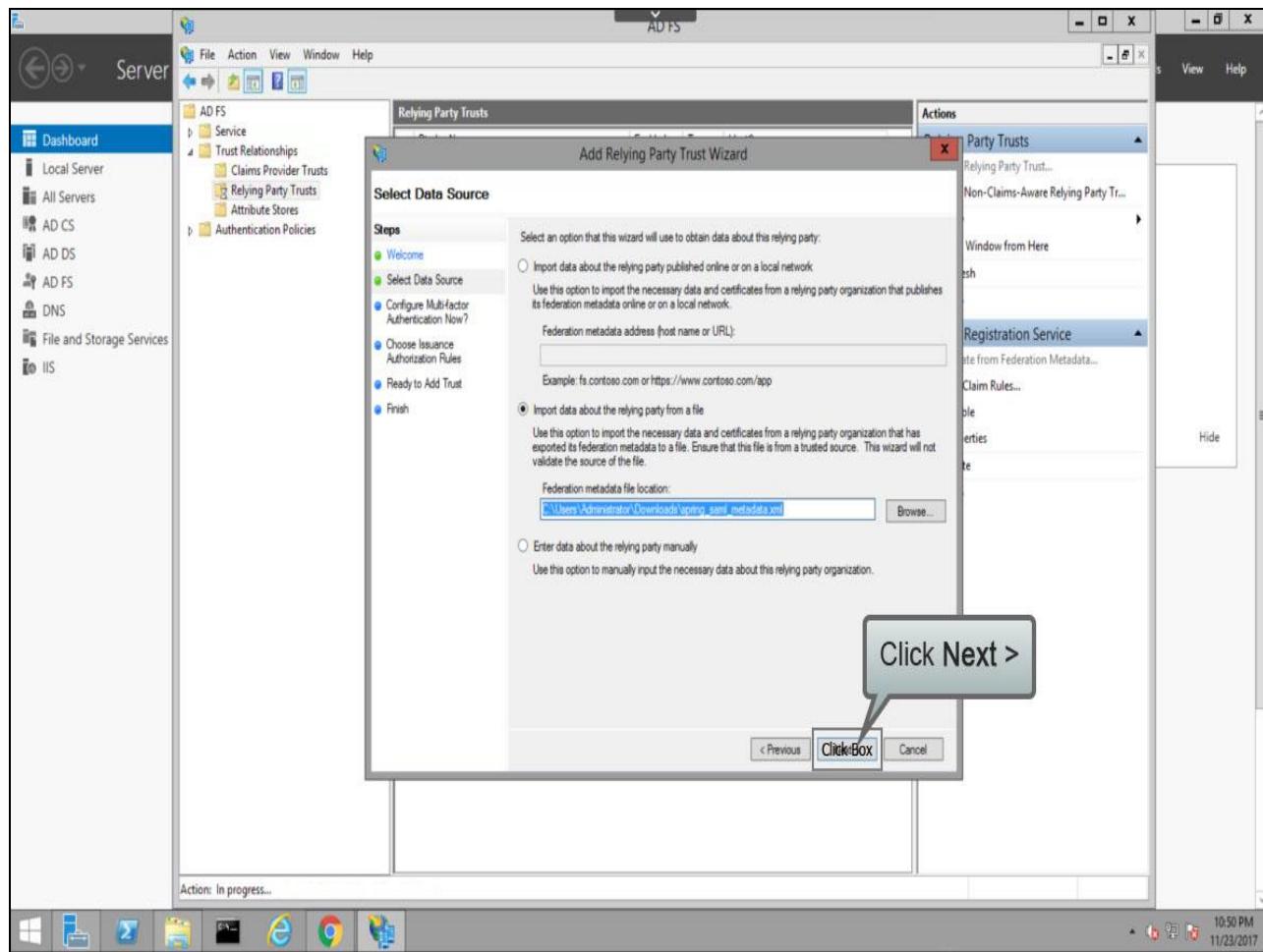
## Slide 60 - Slide 60



## Slide notes

Find the metadata file that you exported from the ZPA admin portal earlier, select it, click Open, ...

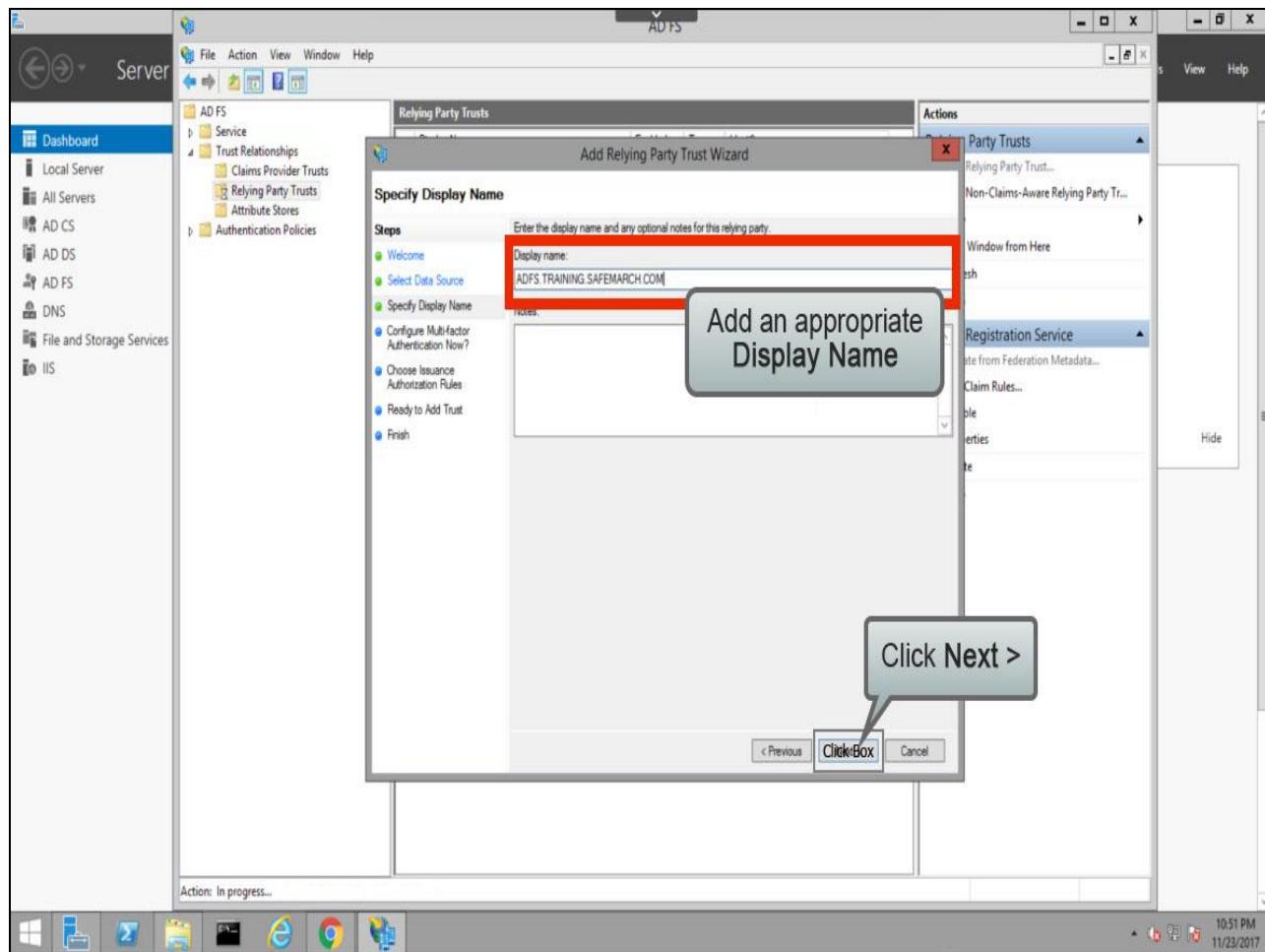
## Slide 61 - Slide 61



## Slide notes

...then click **Next >**.

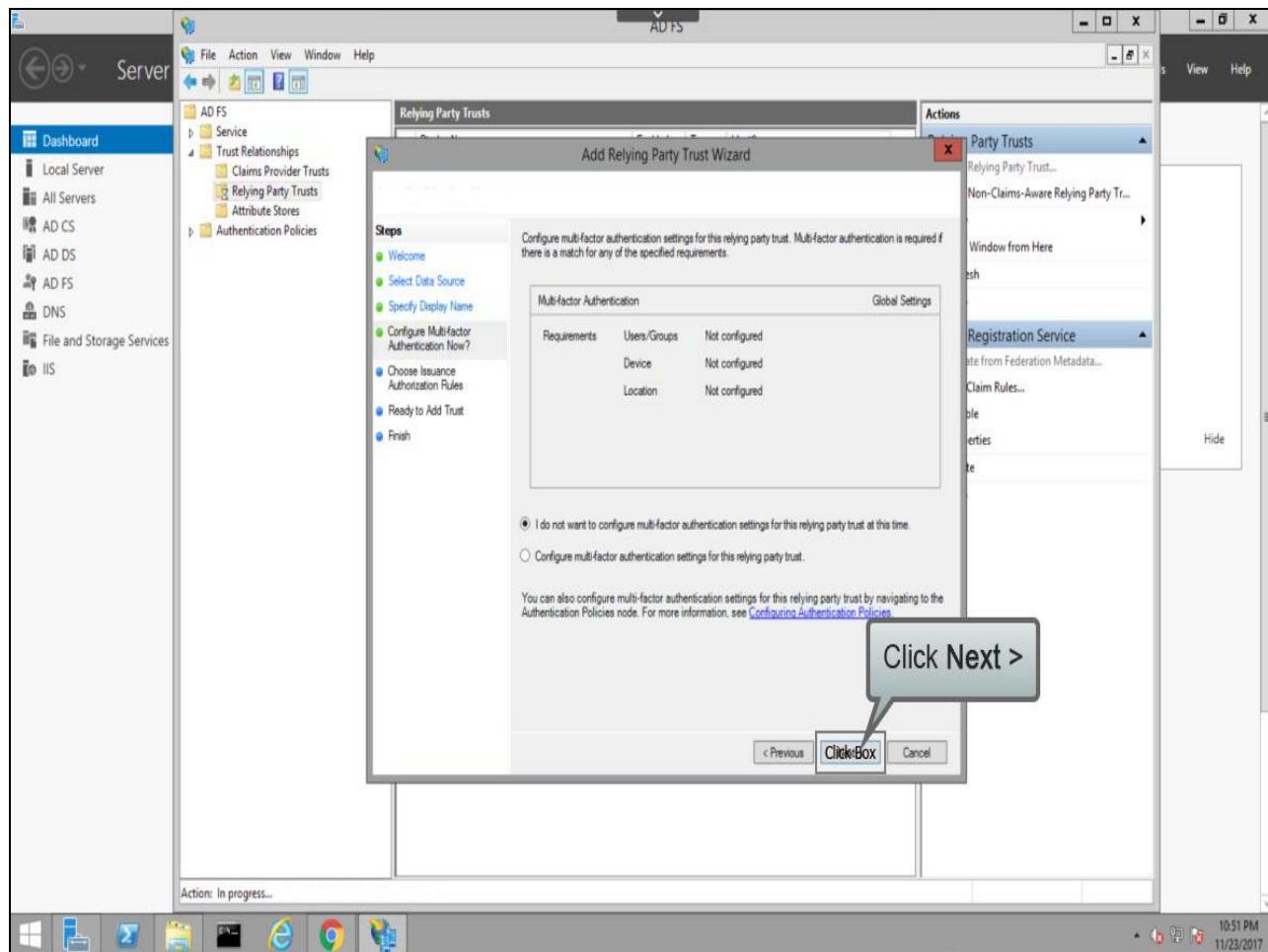
## Slide 62 - Slide 62



## Slide notes

Add an appropriate **Display Name** and click **Next >**.

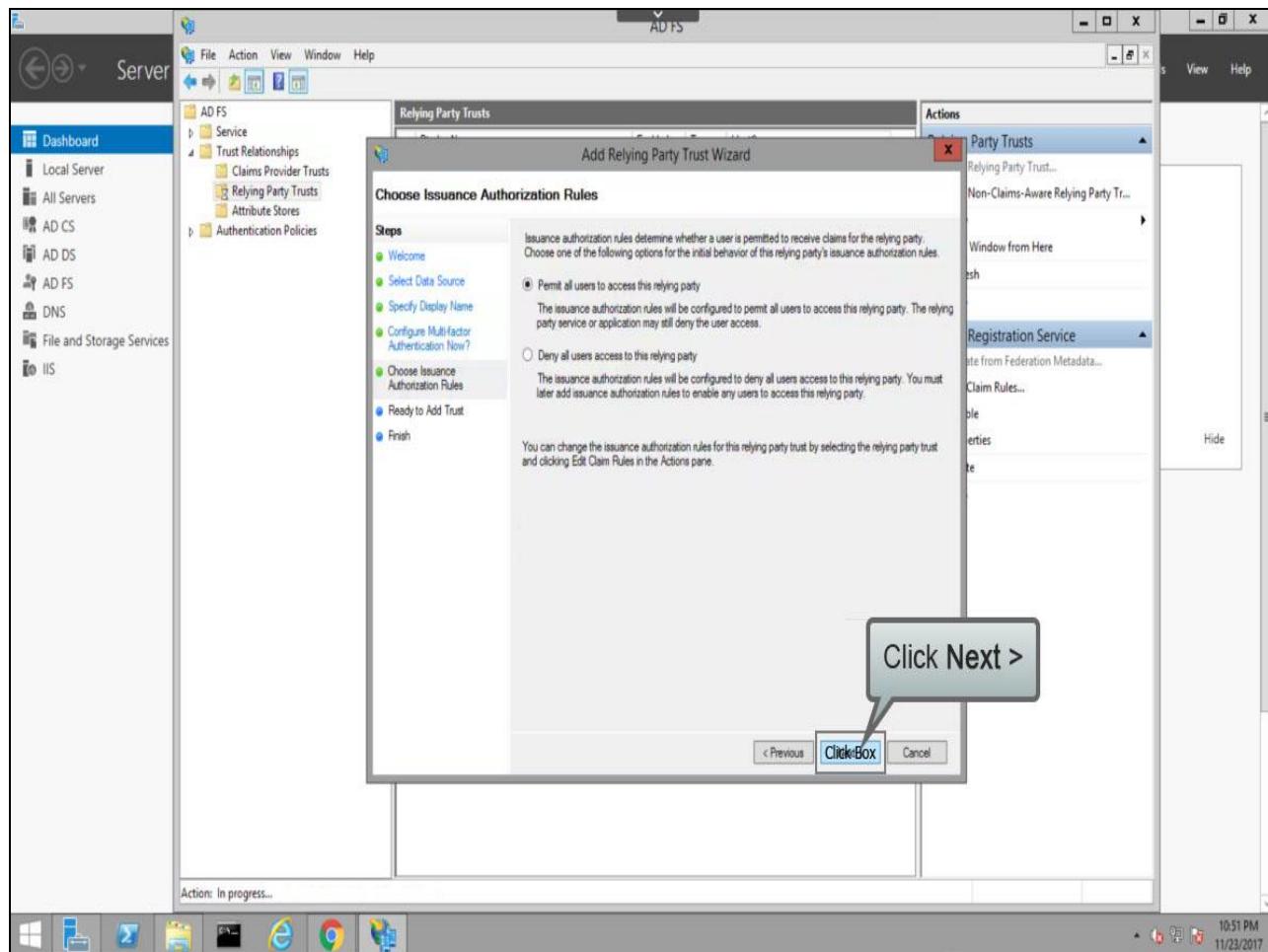
## Slide 63 - Slide 63



## Slide notes

It is possible to use multifactor authentication; however, we will skip this for now, and just click **Next >**.

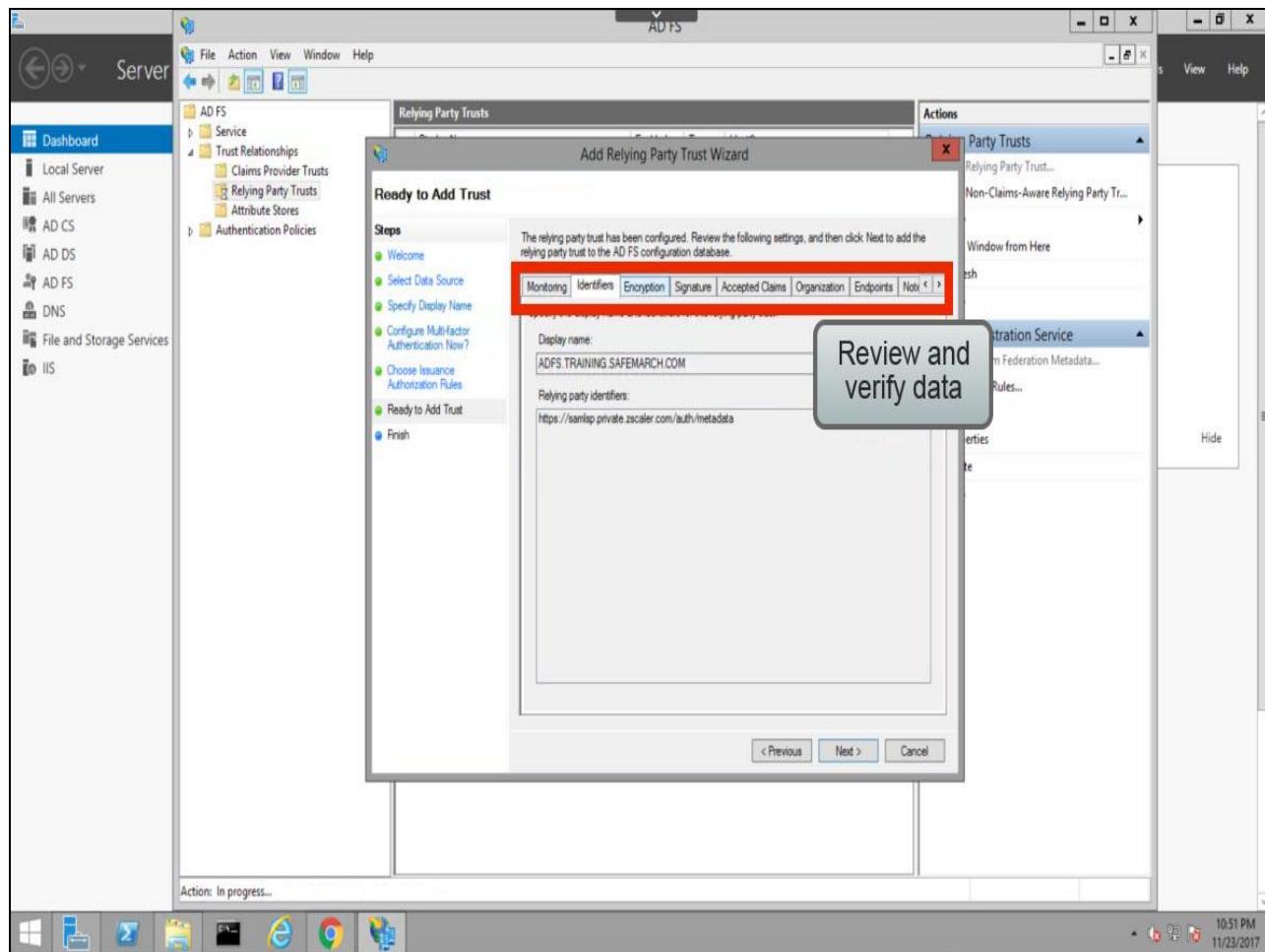
## Slide 64 - Slide 64



## Slide notes

We will allow all users to access this **Relying Party**, ...so click **Next >** again.

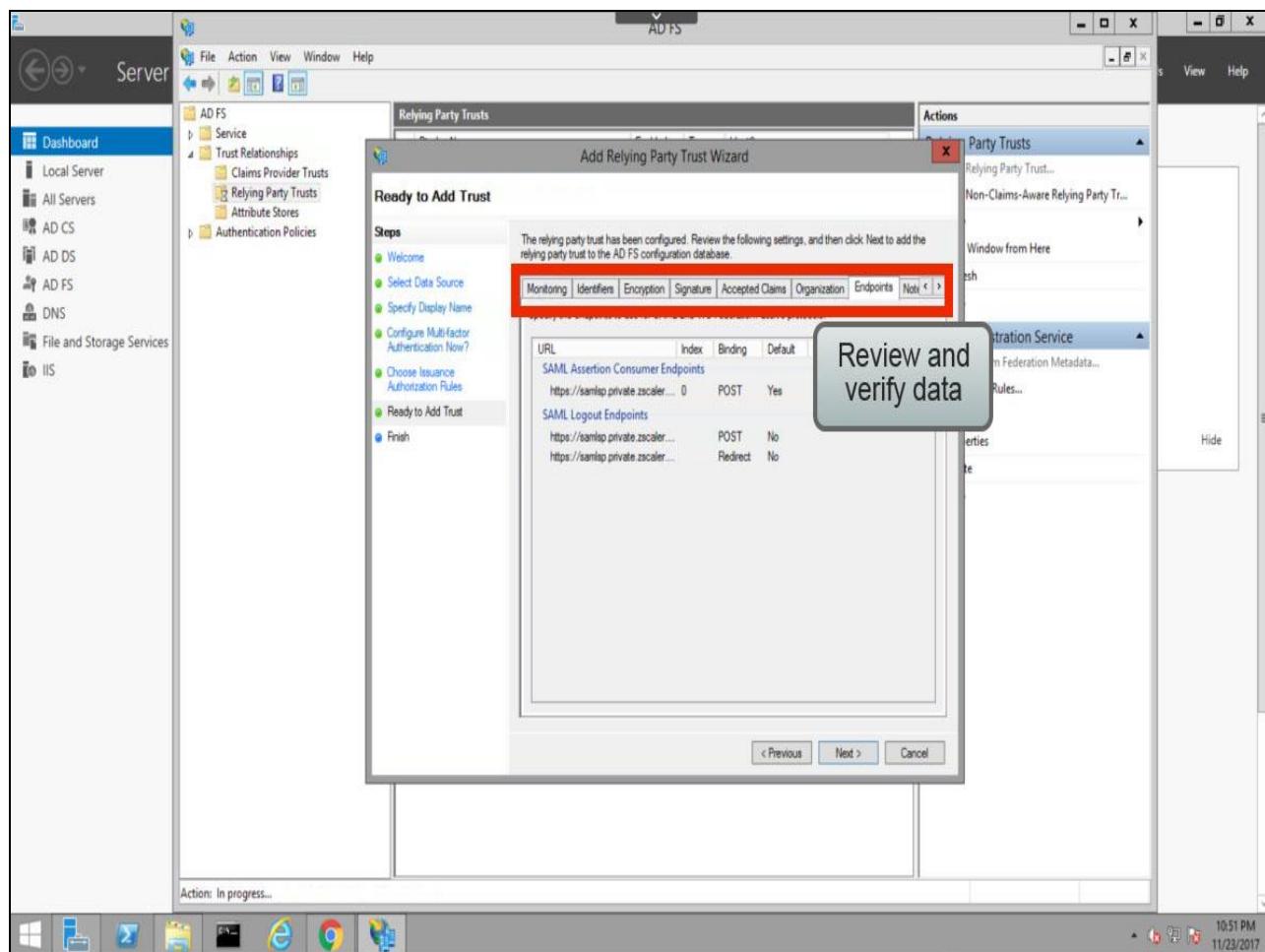
## Slide 65 - Slide 65



## Slide notes

Review the entered data carefully, in particular on the **Identifiers** tab, ...

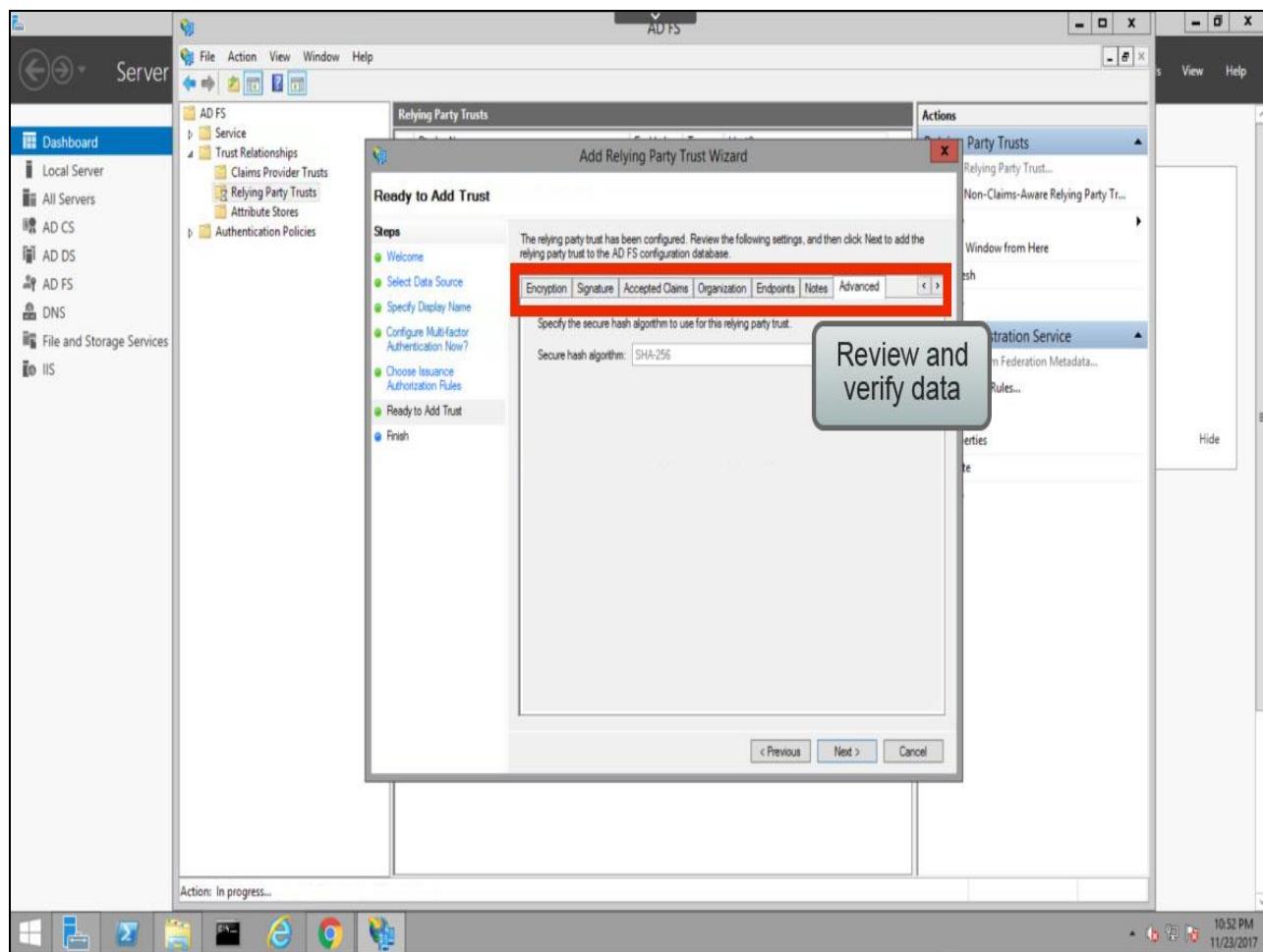
## Slide 66 - Slide 66



## Slide notes

...the Endpoints tab, ...

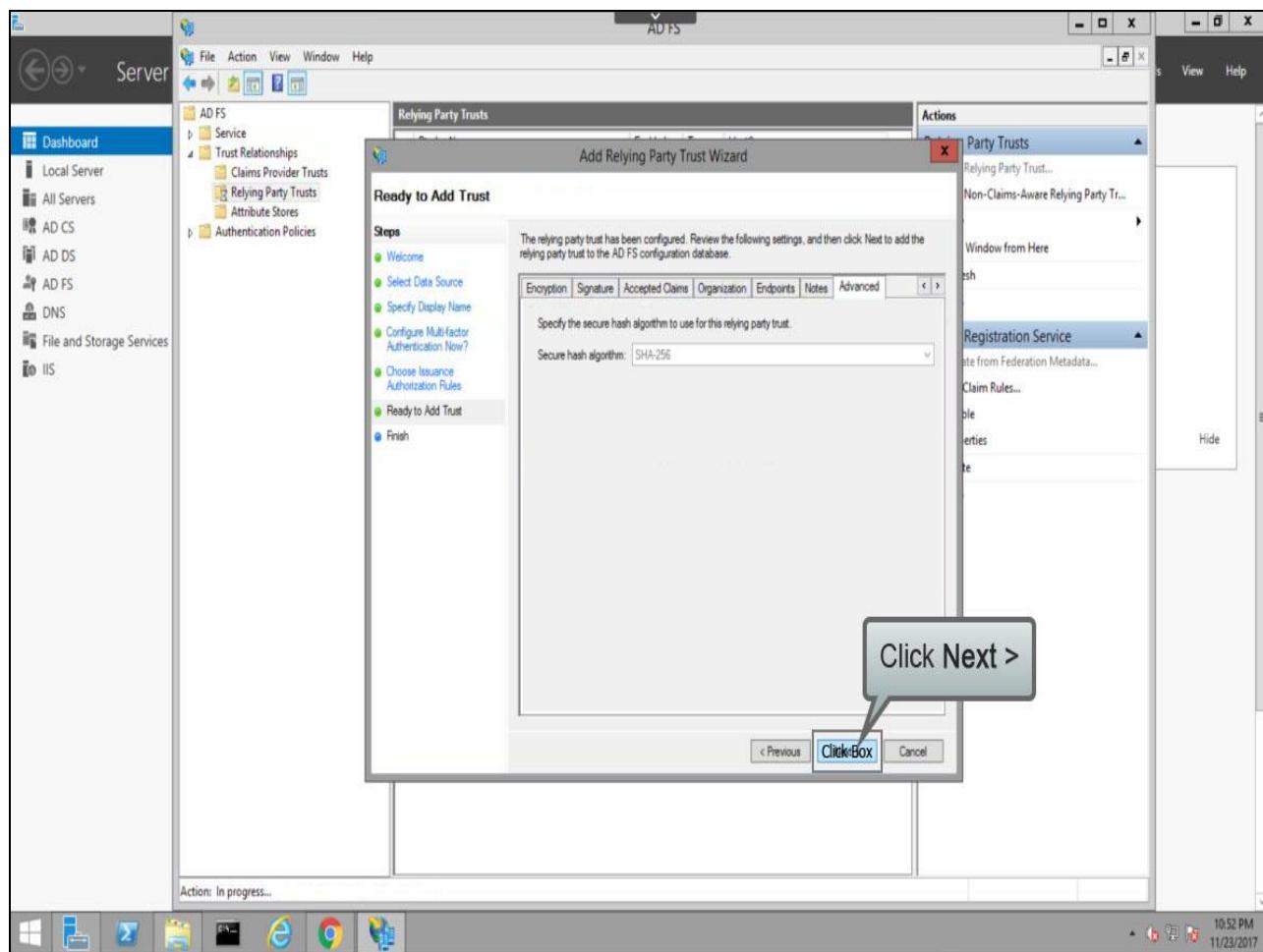
## Slide 67 - Slide 67



## Slide notes

...and the Advanced tab.

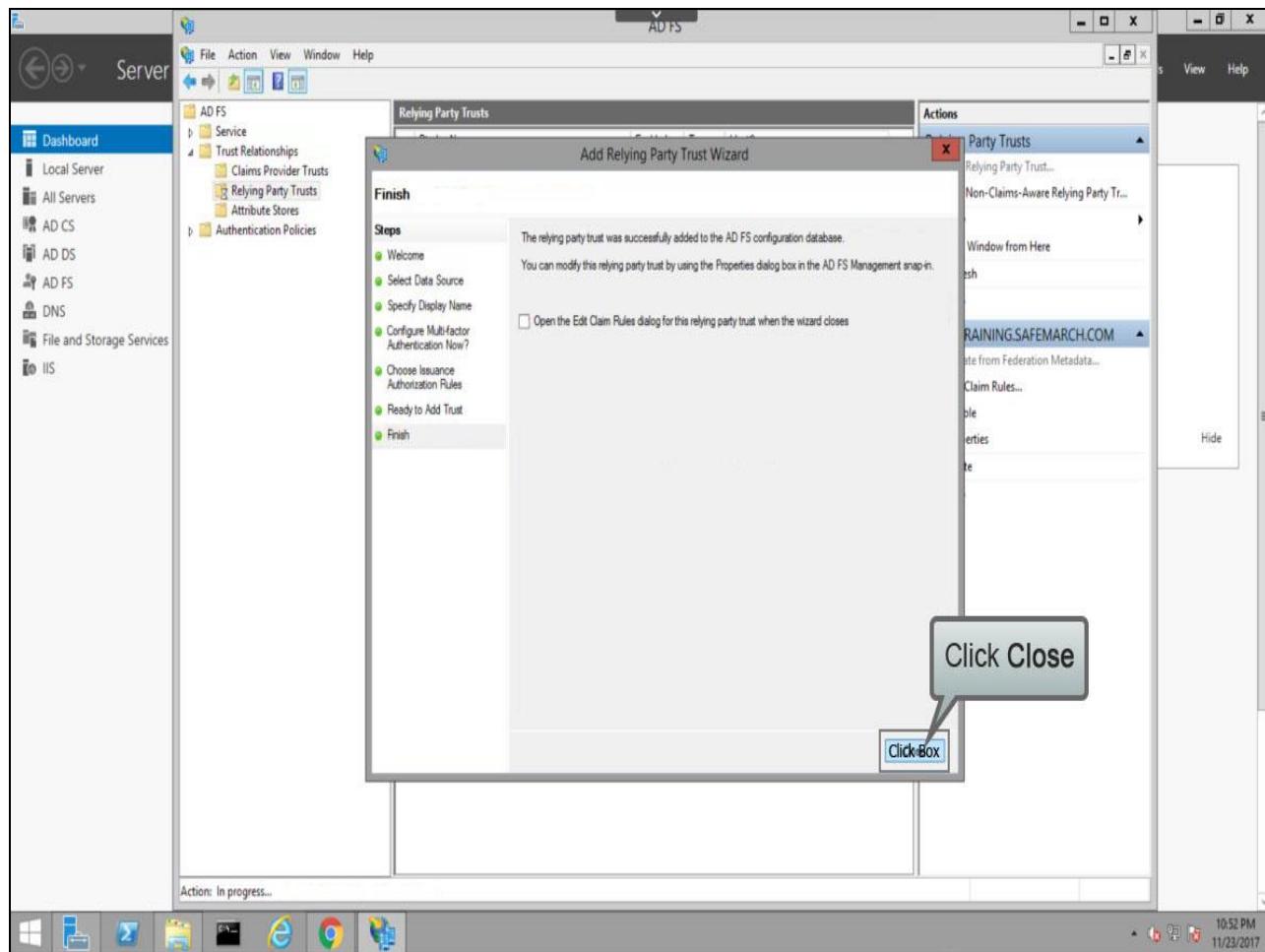
## Slide 68 - Slide 68



## Slide notes

Once you are happy, click **Next >** once more, ...

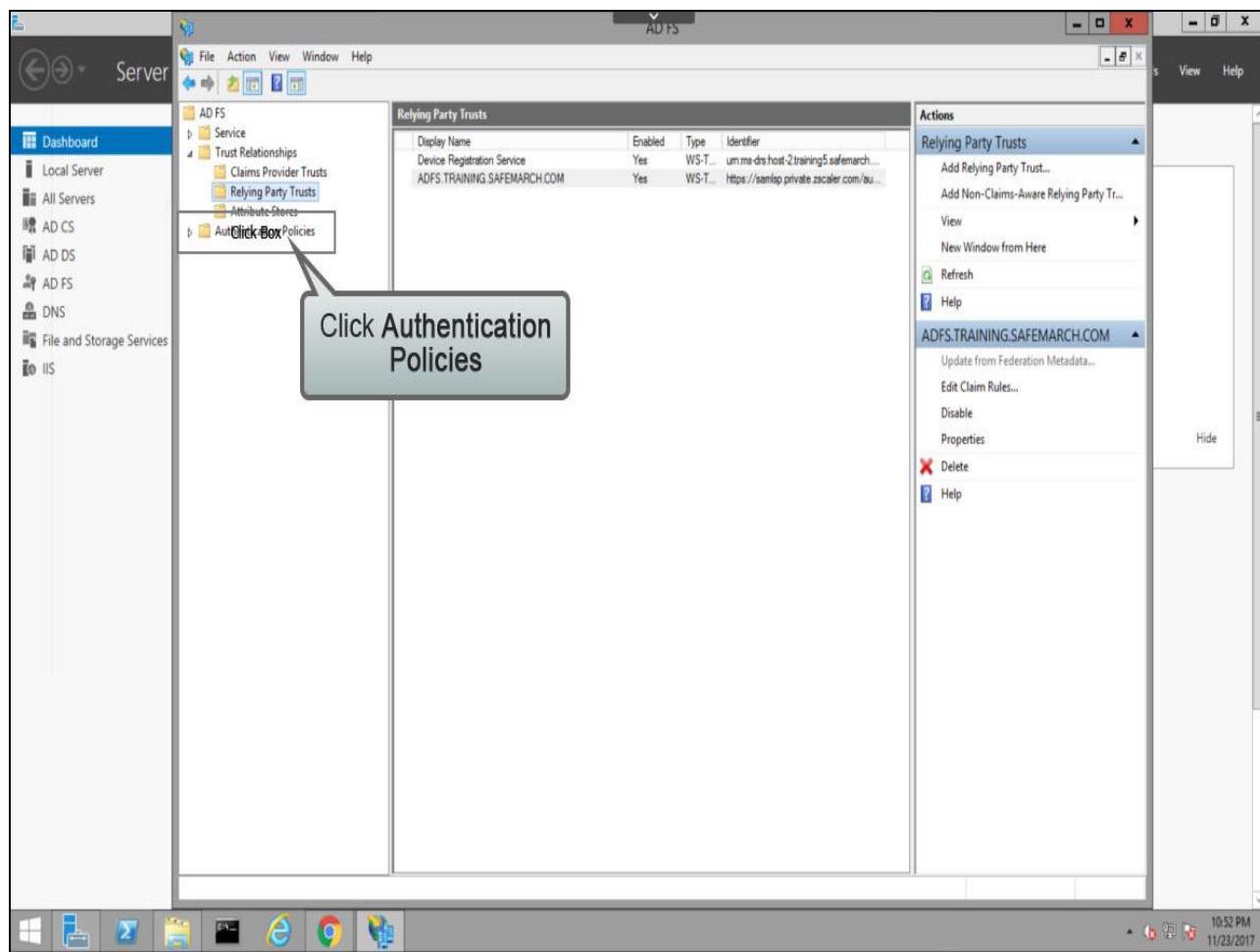
## Slide 69 - Slide 69



## Slide notes

...then select whether or not to open the **Edit Claims Rules** dialog immediately and click **Close**.

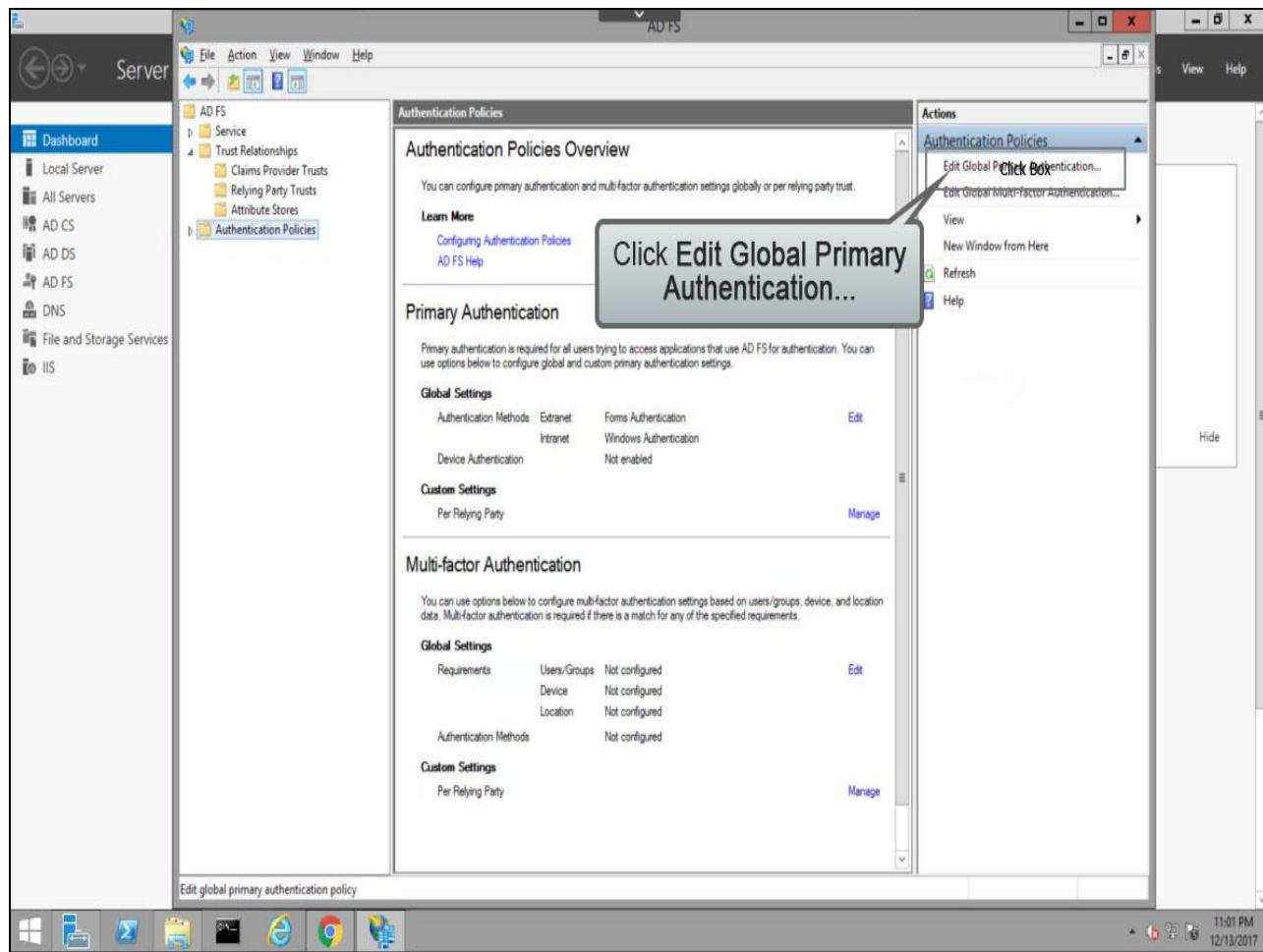
## Slide 70 - Slide 70



## Slide notes

To configure the authentication method to be used, click **Authentication Policies**, ...

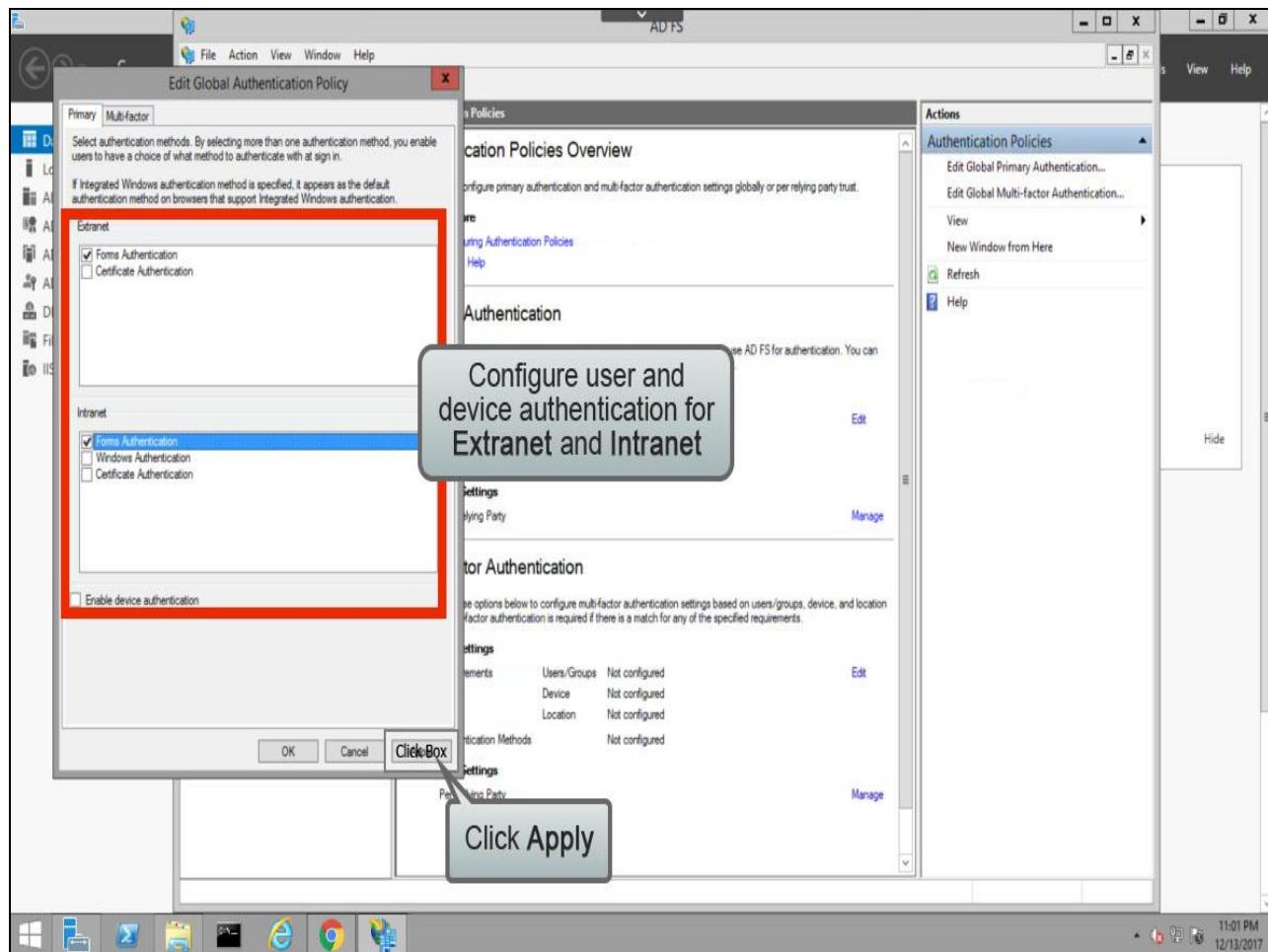
## Slide 71 - Slide 71



## Slide notes

...then in the Actions panel, click **Edit Global Primary Authentication....**

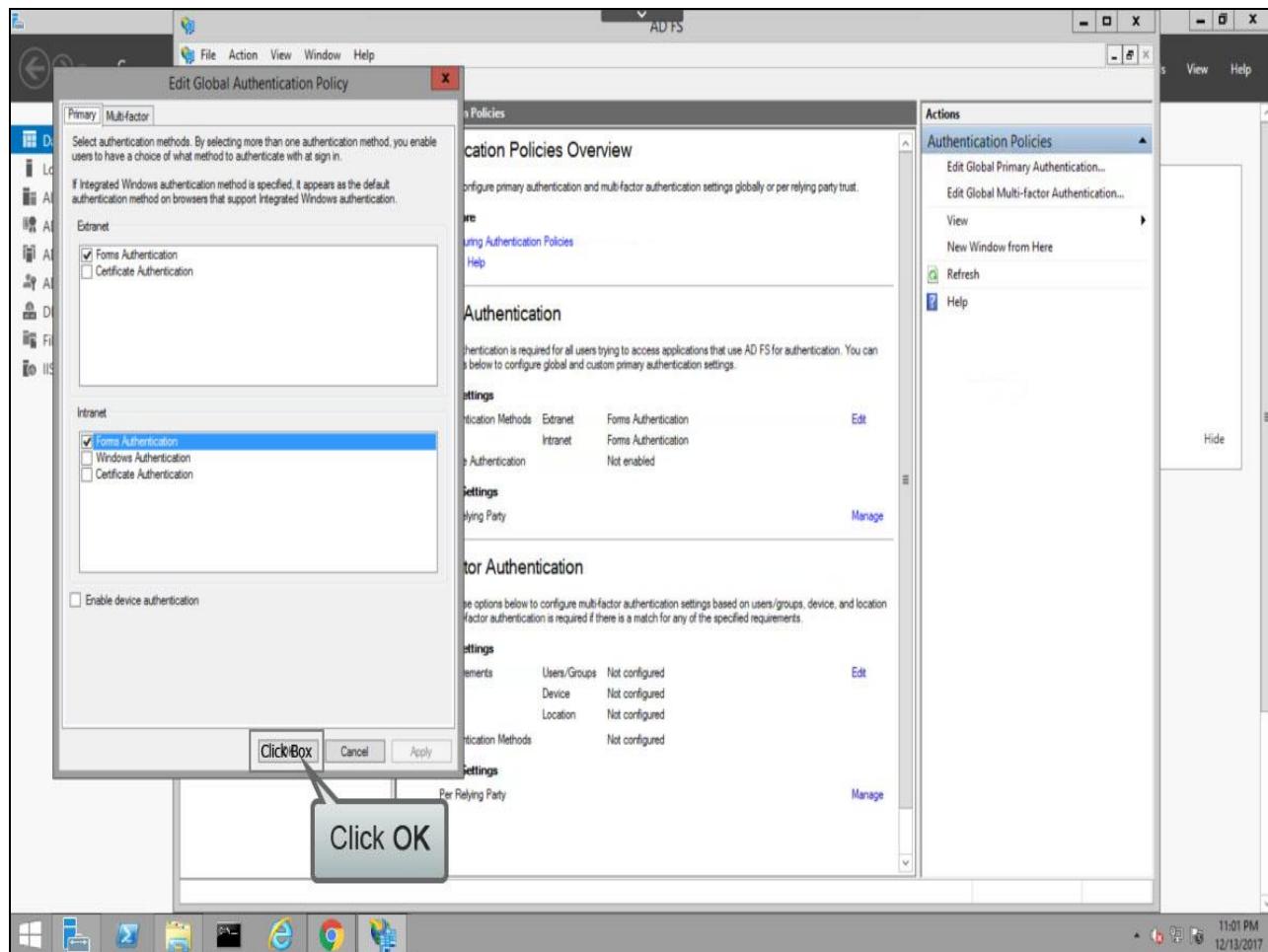
## Slide 72 - Slide 72



## Slide notes

Configure the authentication to be used by users on the **Extranet**, and **Intranet**, and select whether to enable **device authentication**. In this instance we will use **Forms Authentication** for both networks. Click **Apply**, ...

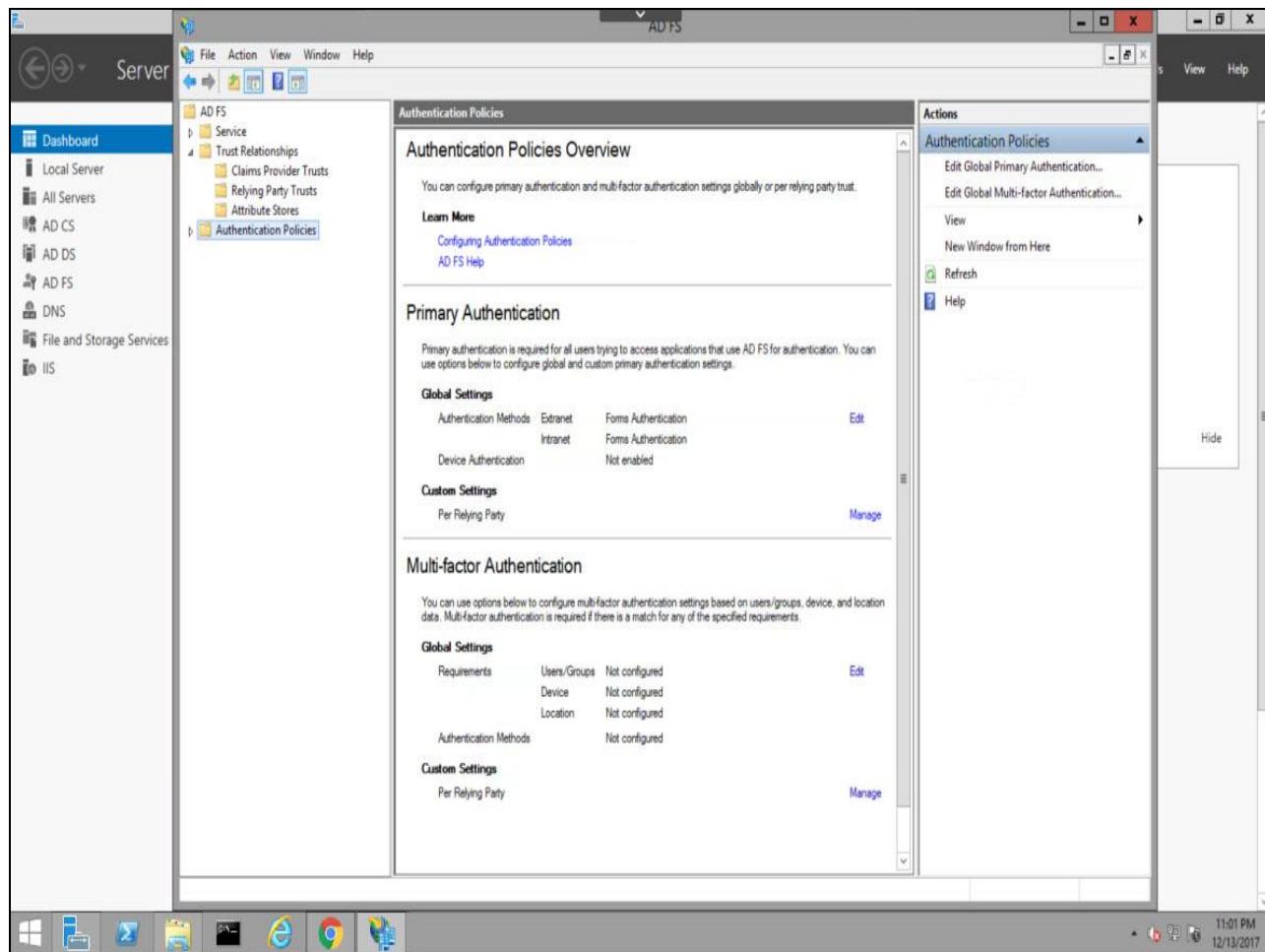
## Slide 73 - Slide 73



## Slide notes

...then OK.

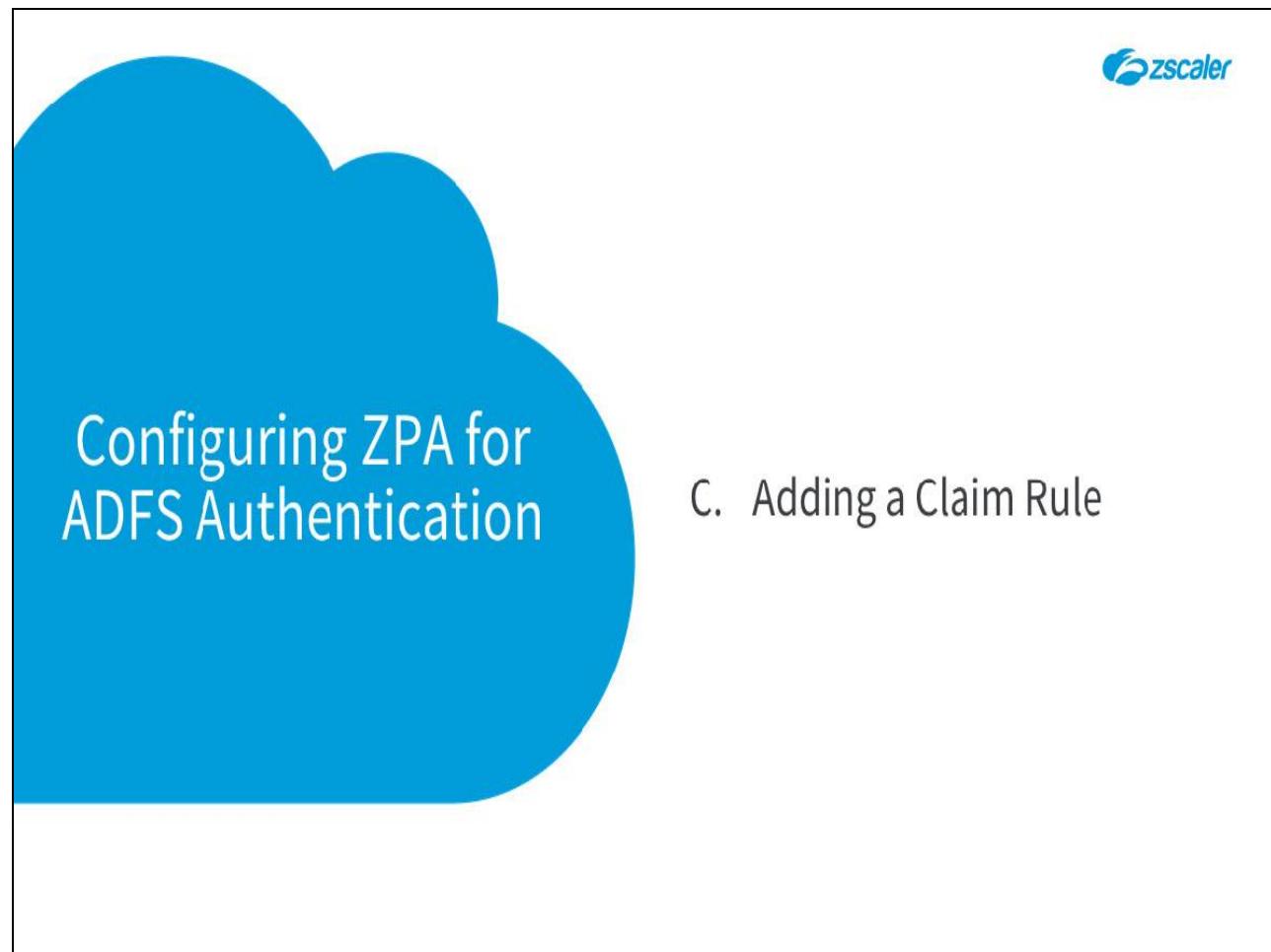
## Slide 74 - Slide 74



## Slide notes

Note, this is also where you would come to configure ADFS for multi-factor authentication.

## Slide 75 - Configuring ZPA for ADFS Authentication



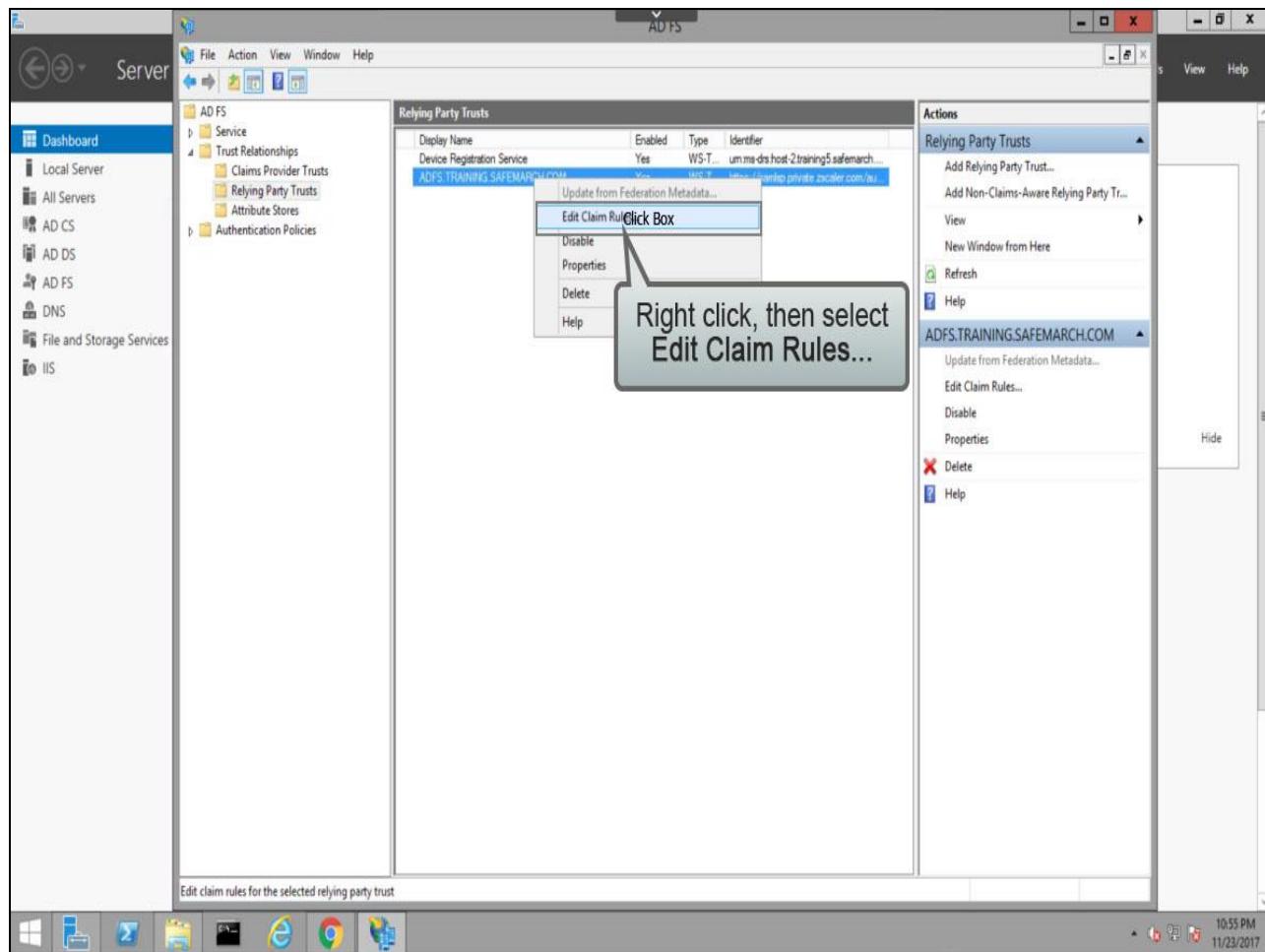
The slide features a large, semi-transparent blue cloud shape on the left side, containing the text "Configuring ZPA for ADFS Authentication". In the top right corner of the slide area, there is a small Zscaler logo.

C. Adding a Claim Rule

**Slide notes**

Having added ZPA as a **Relying Party**, we will next look at how to configure the **Claims** (authorization attributes) to be returned to ZPA on a successful authentication.

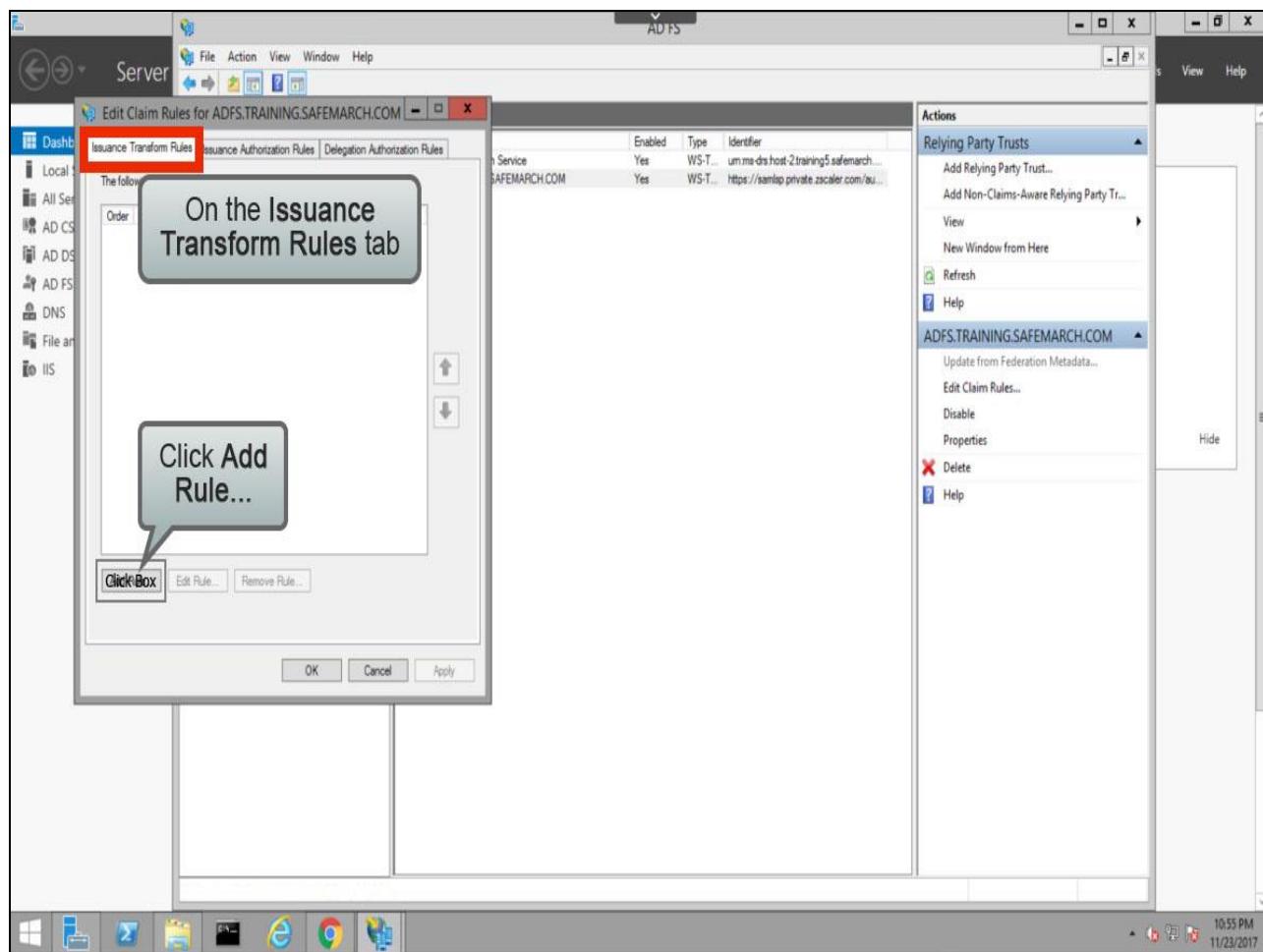
## Slide 76 - Slide 76



## Slide notes

To add claims rules for this **Relying Party**, right-click on the **Relying Party Trust** that you just added and select **Edit Claim Rules....**

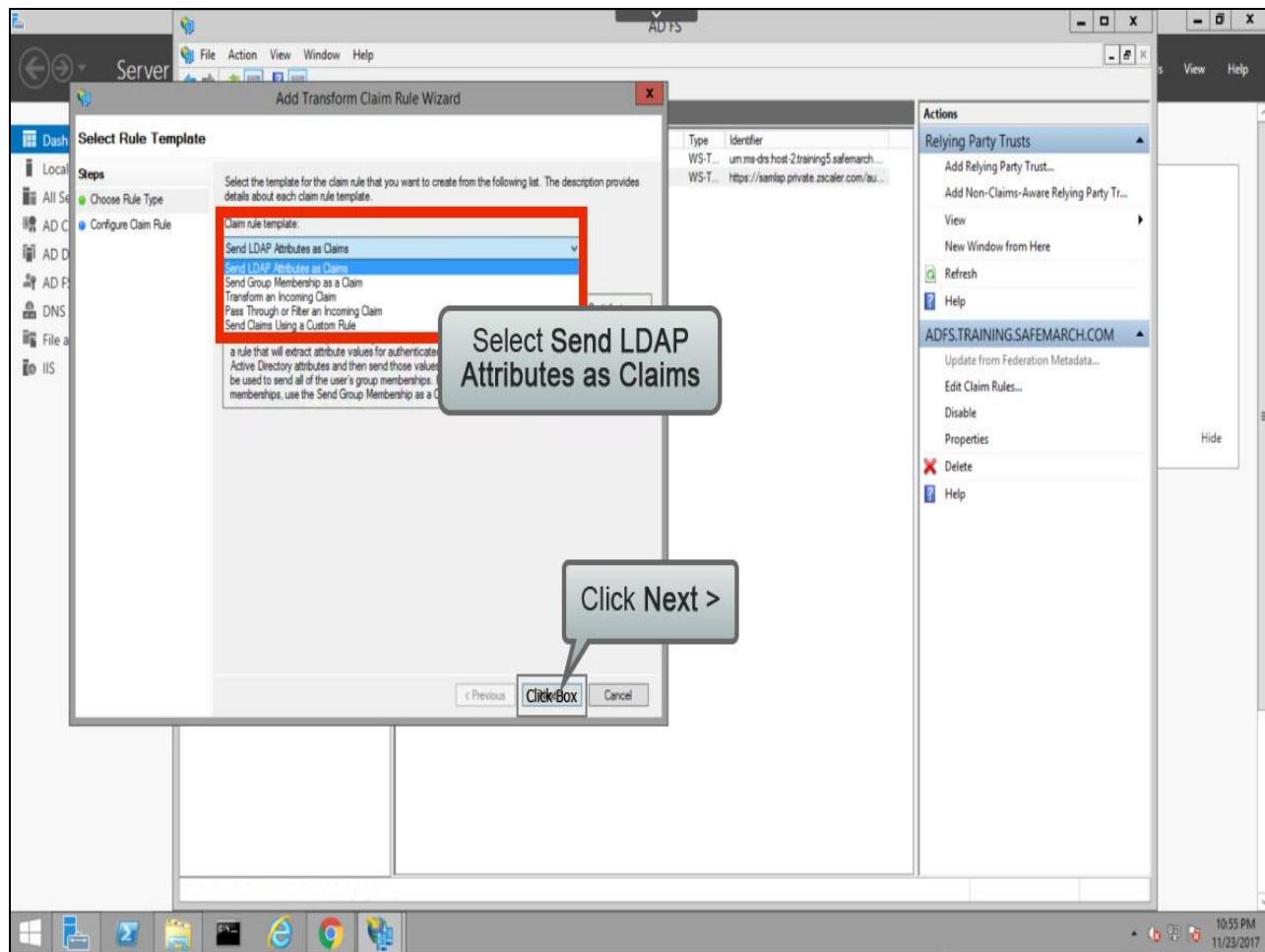
## Slide 77 - Slide 77



## Slide notes

On the Issuance Transform Rules tab, click Add Rule....

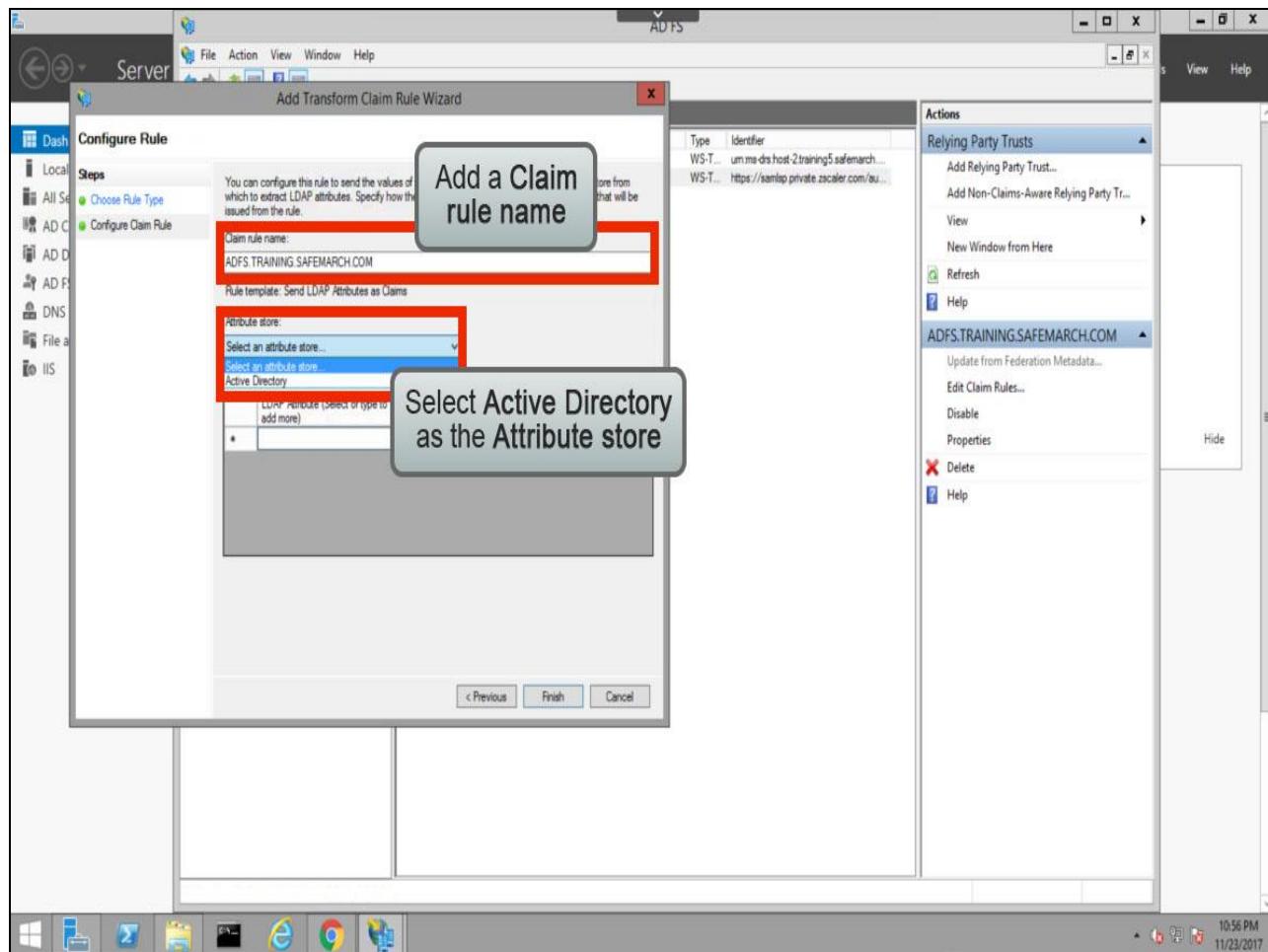
## Slide 78 - Slide 78



## Slide notes

In the **Claim rule template** field, select **Send LDAP Attributes as Claims**, and click **Next >**.

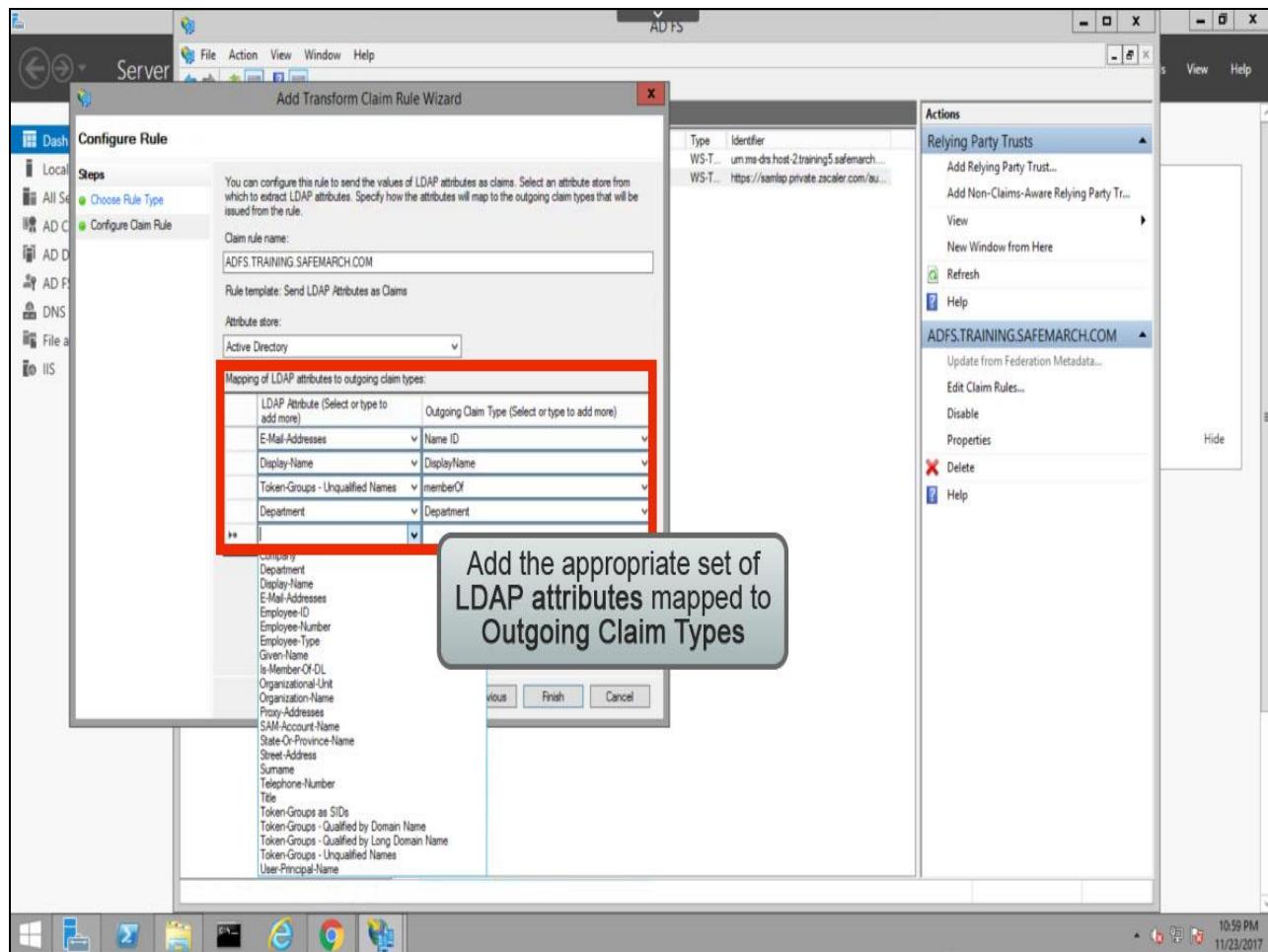
## Slide 79 - Slide 79



## Slide notes

Give the claim rule set an appropriate name and select **Active Directory** as the **Attribute store**.

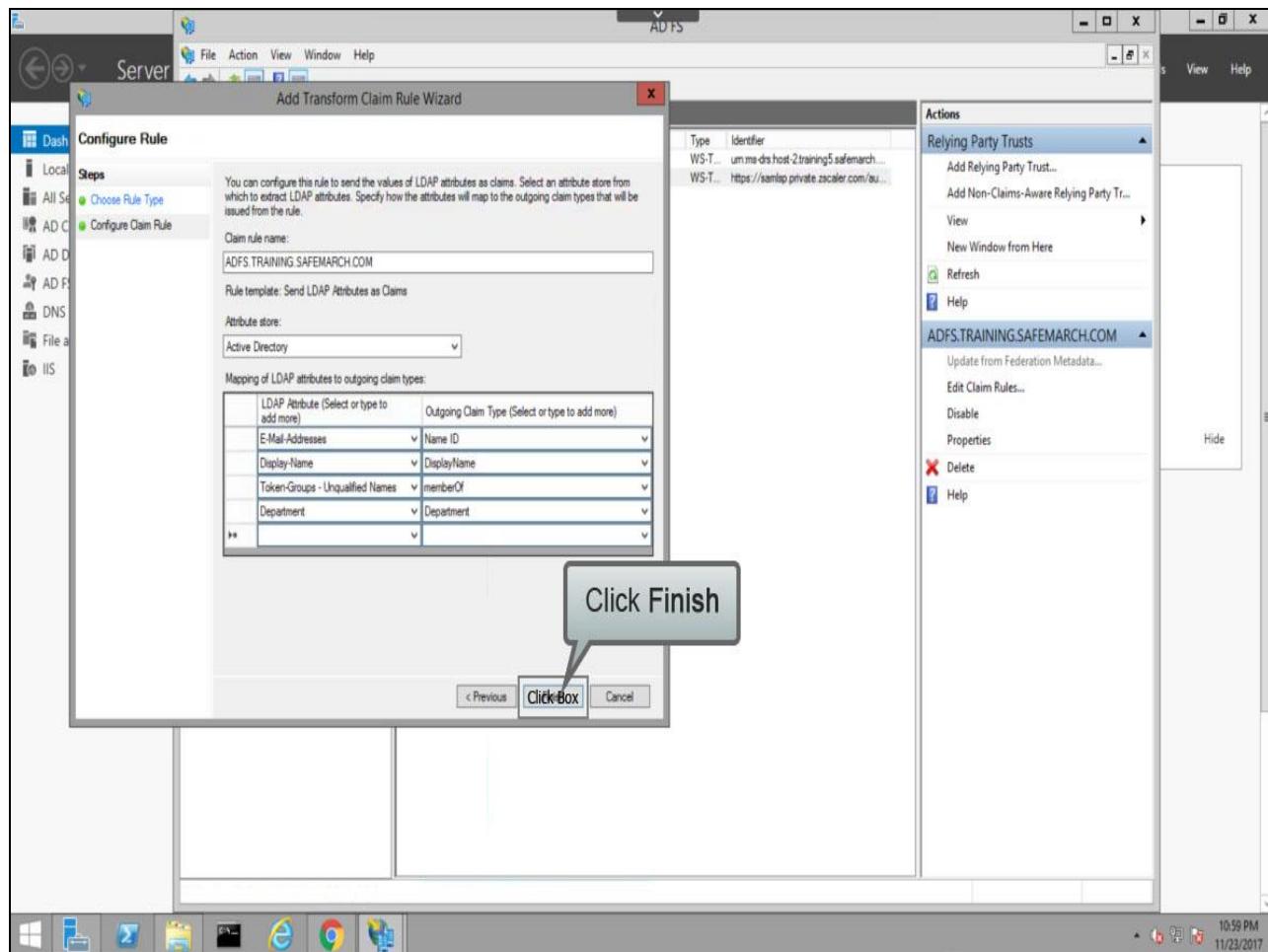
## Slide 80 - Slide 80



## Slide notes

Add attributes from the list of LDAP attributes available and specify what the **Outgoing Claim Type** should be for each.

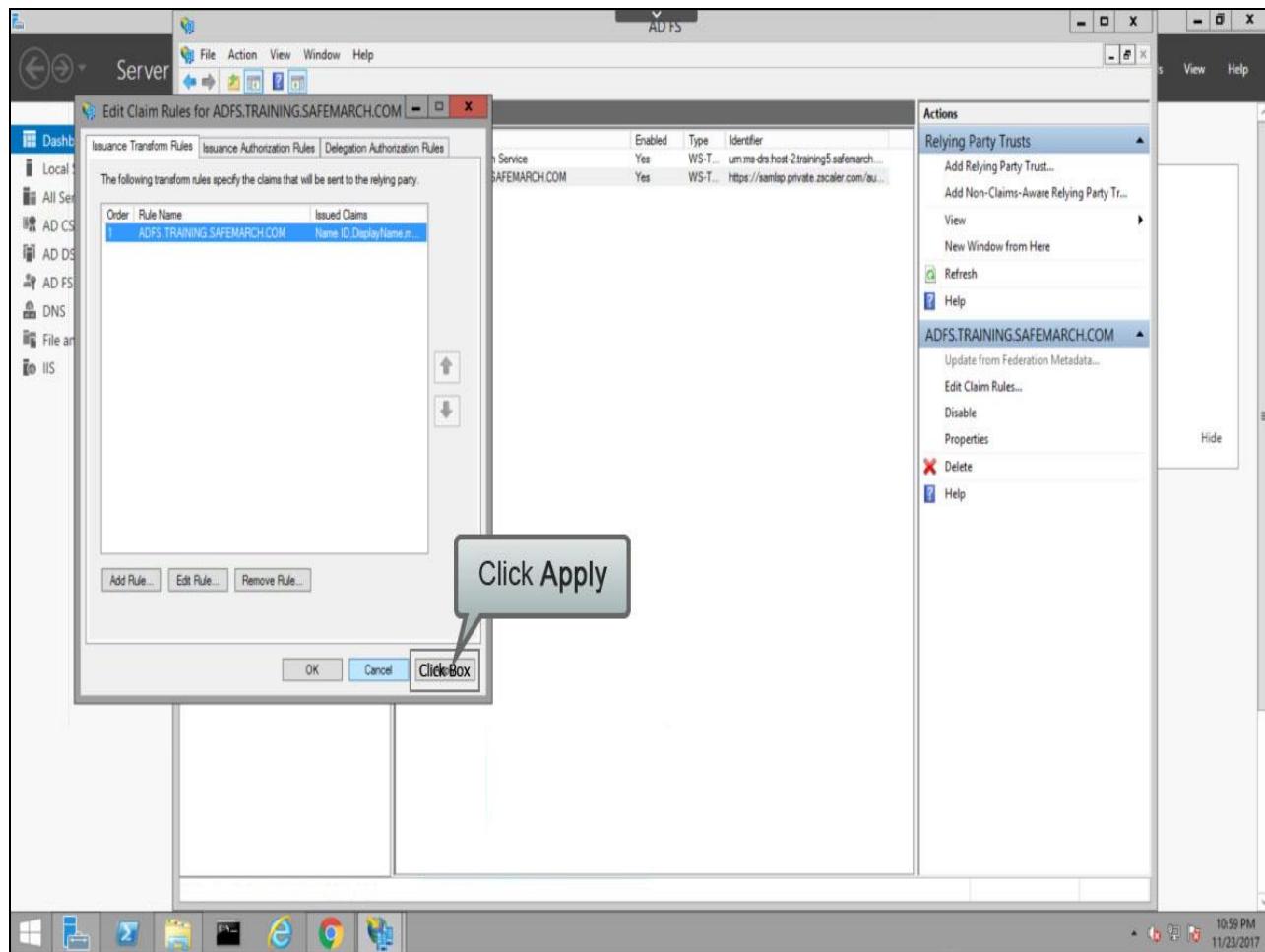
## Slide 81 - Slide 81



## Slide notes

Once the attribute to claims configuration is complete, click **Finish**.

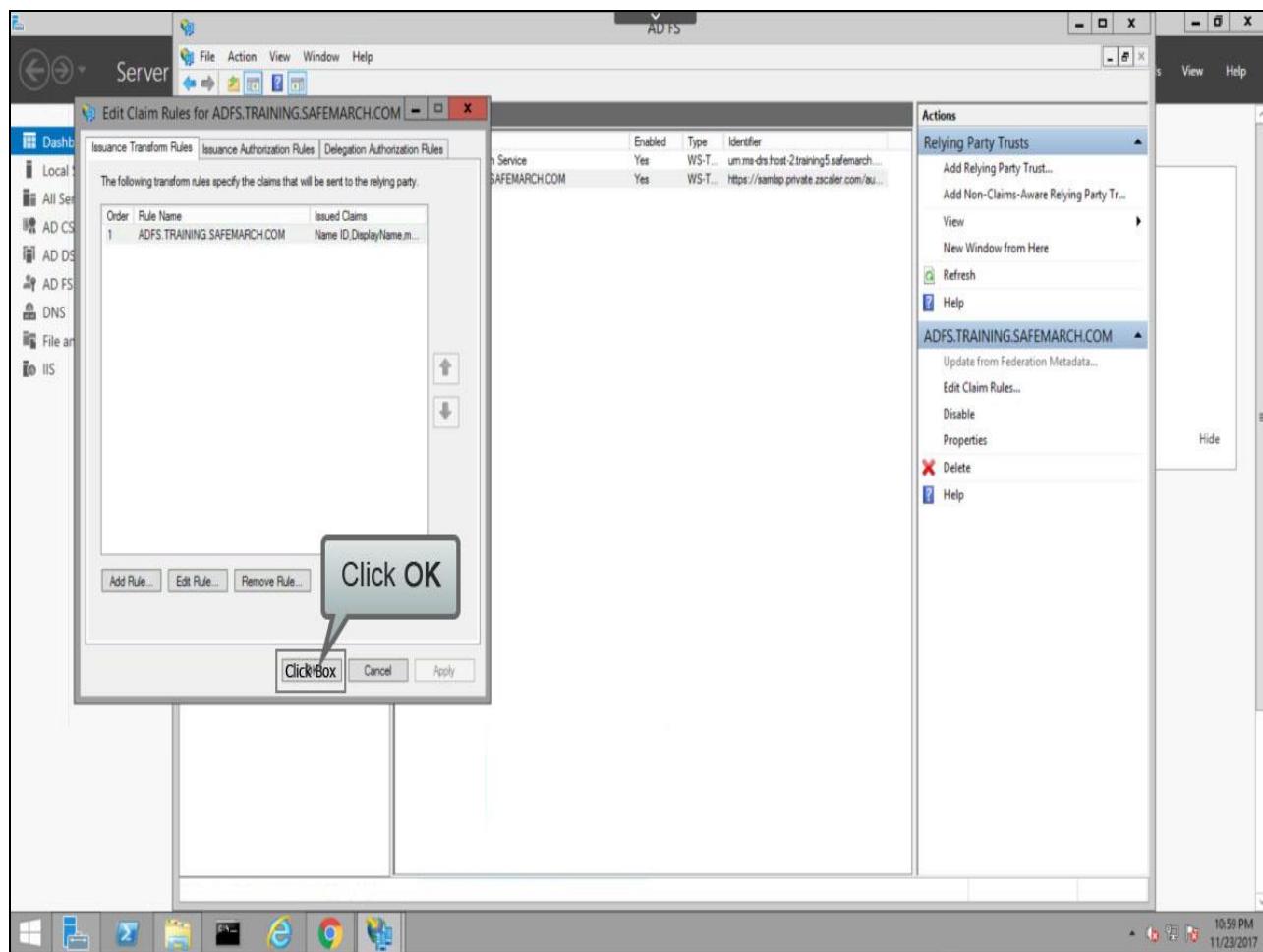
## Slide 82 - Slide 82



## Slide notes

Click Apply, ...

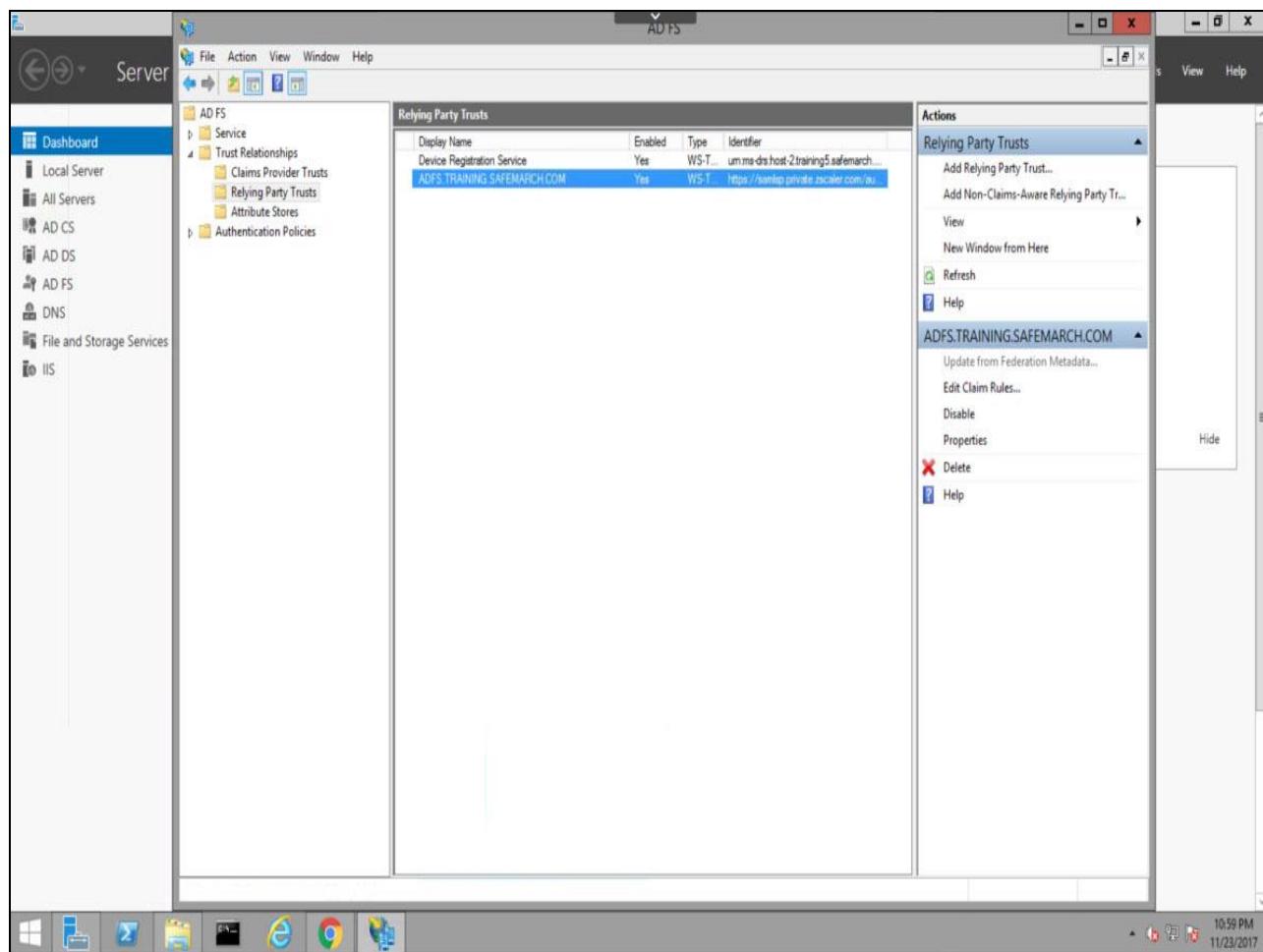
## Slide 83 - Slide 83



## Slide notes

...then OK.

## Slide 84 - Slide 84



## Slide notes

## Slide 85 - Configuring ZPA for ADFS Authentication



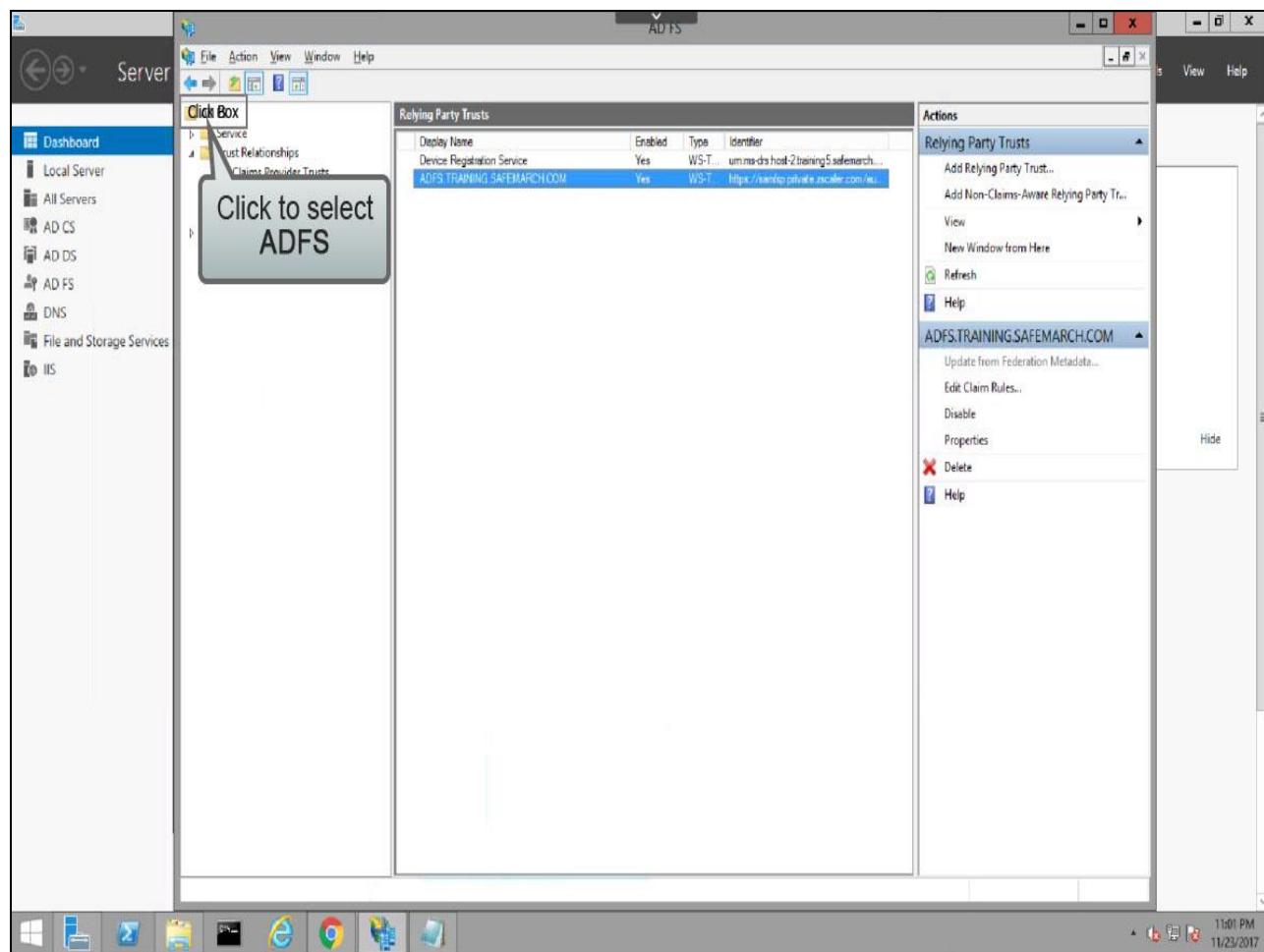
# Configuring ZPA for ADFS Authentication

D. Exporting the IdP Metadata File

**Slide notes**

Having fully configured the IdP, we'll next look at how to export the metadata for it to file, for import to the ZPA admin portal.

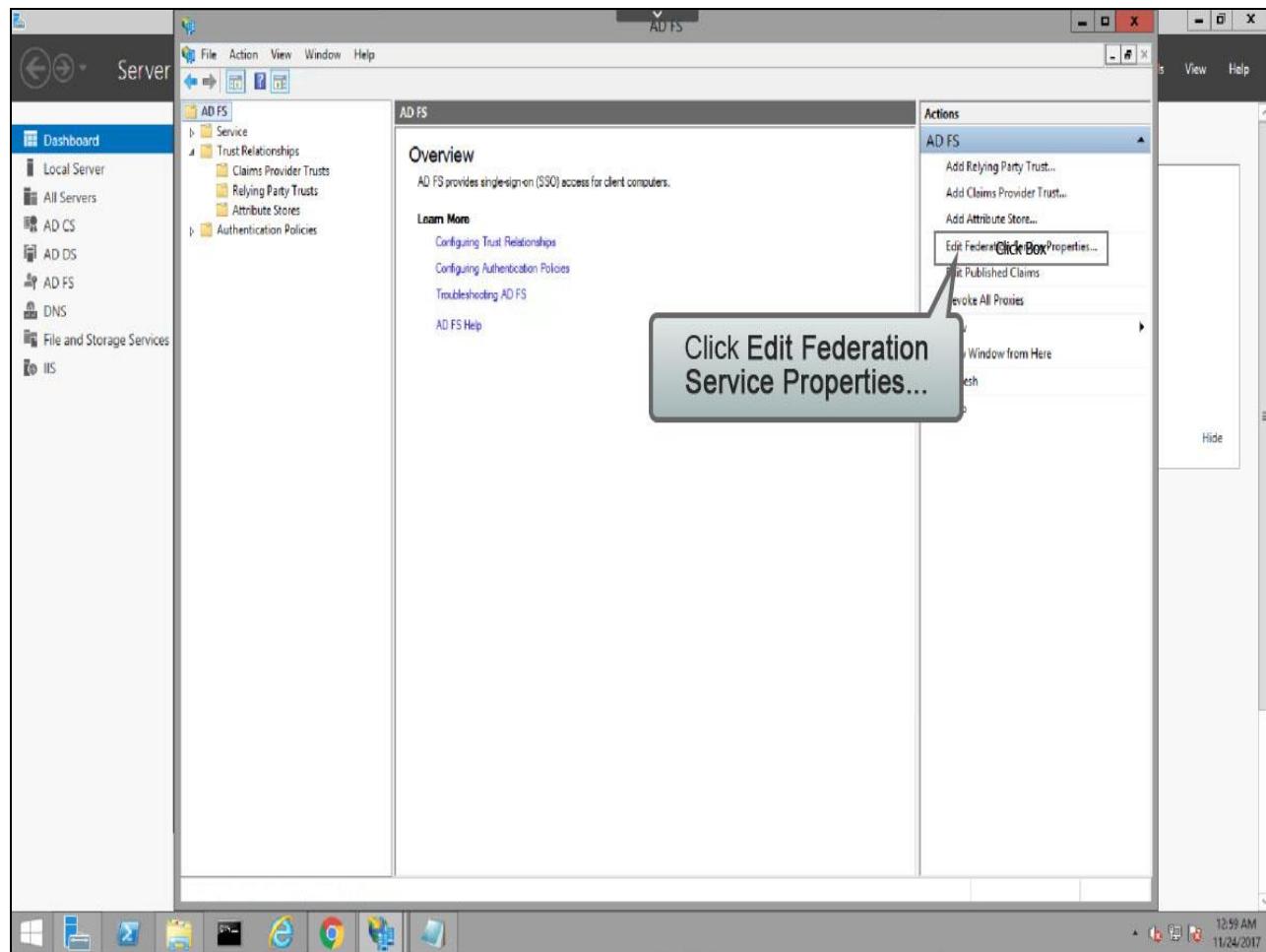
## Slide 86 - Slide 86



## Slide notes

To export the IdP metadata, in the ADFS Manager, in the left-hand navigation panel, select the top-level folder named **AD FS**, ...

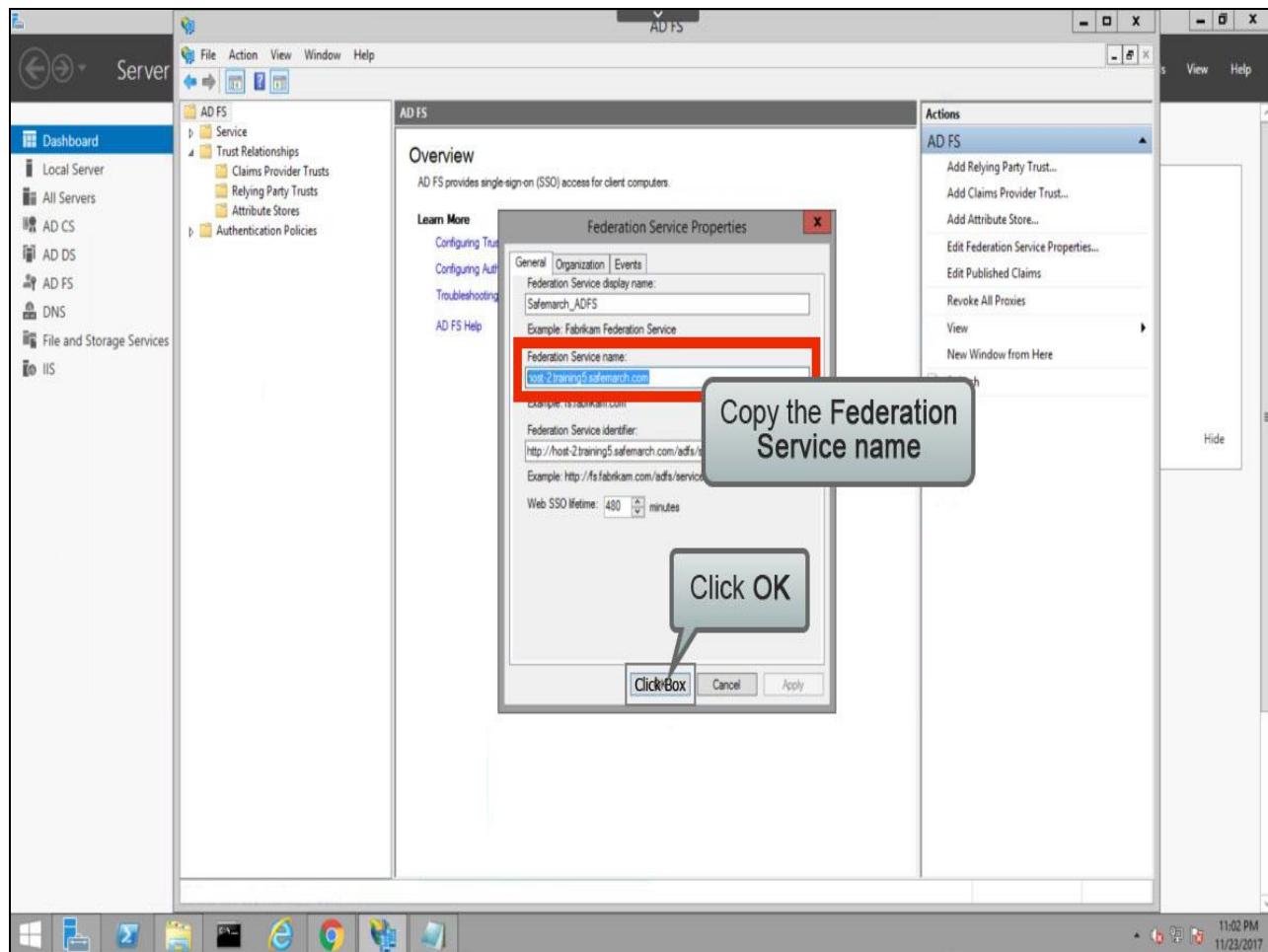
## Slide 87 - Slide 87



## Slide notes

...then in the Actions panel, click **Edit Federation Service Properties....**

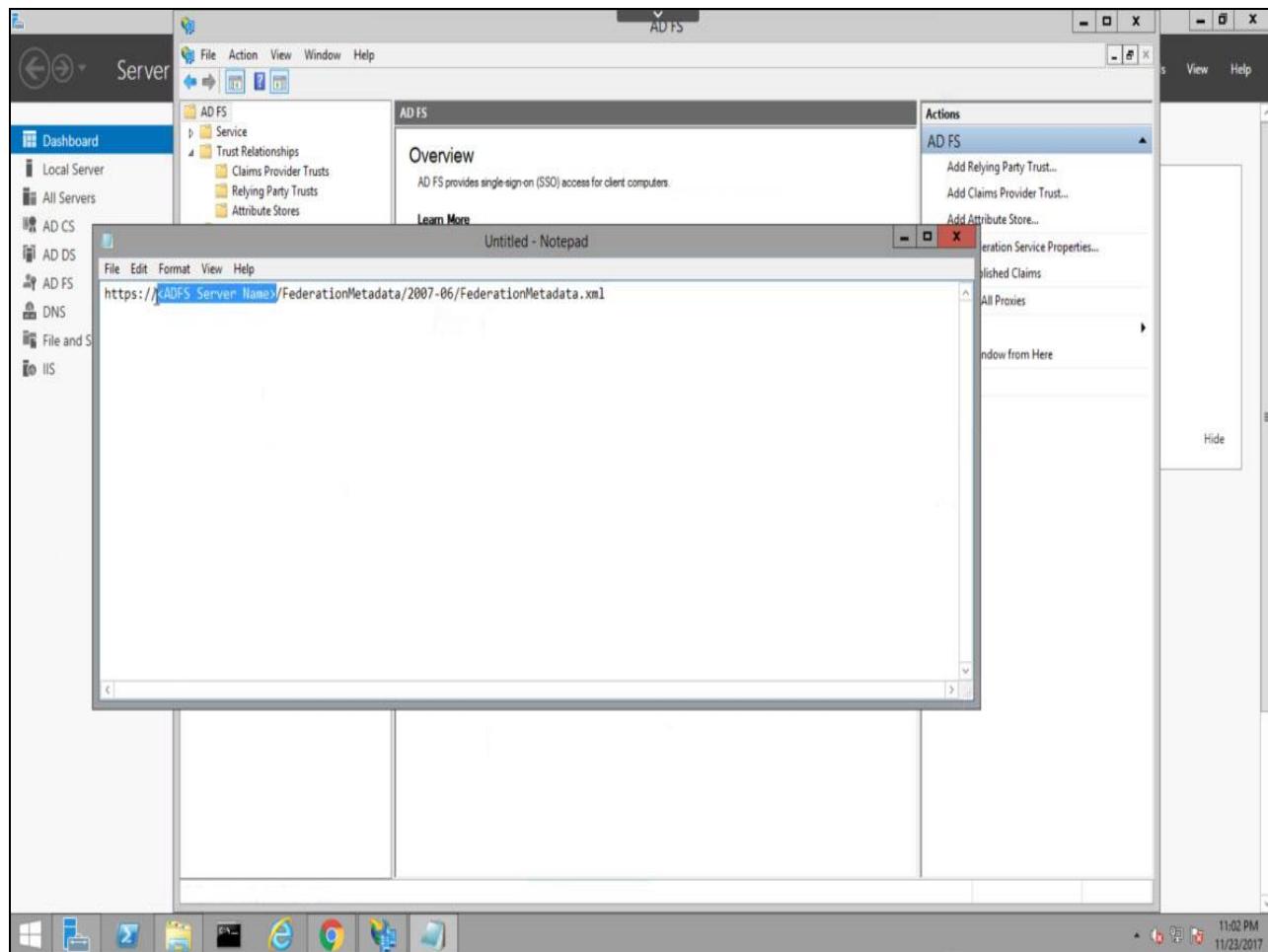
## Slide 88 - Slide 88



## Slide notes

On the **General** tab, copy the **Federation Service name** and click **OK** to close the dialog.

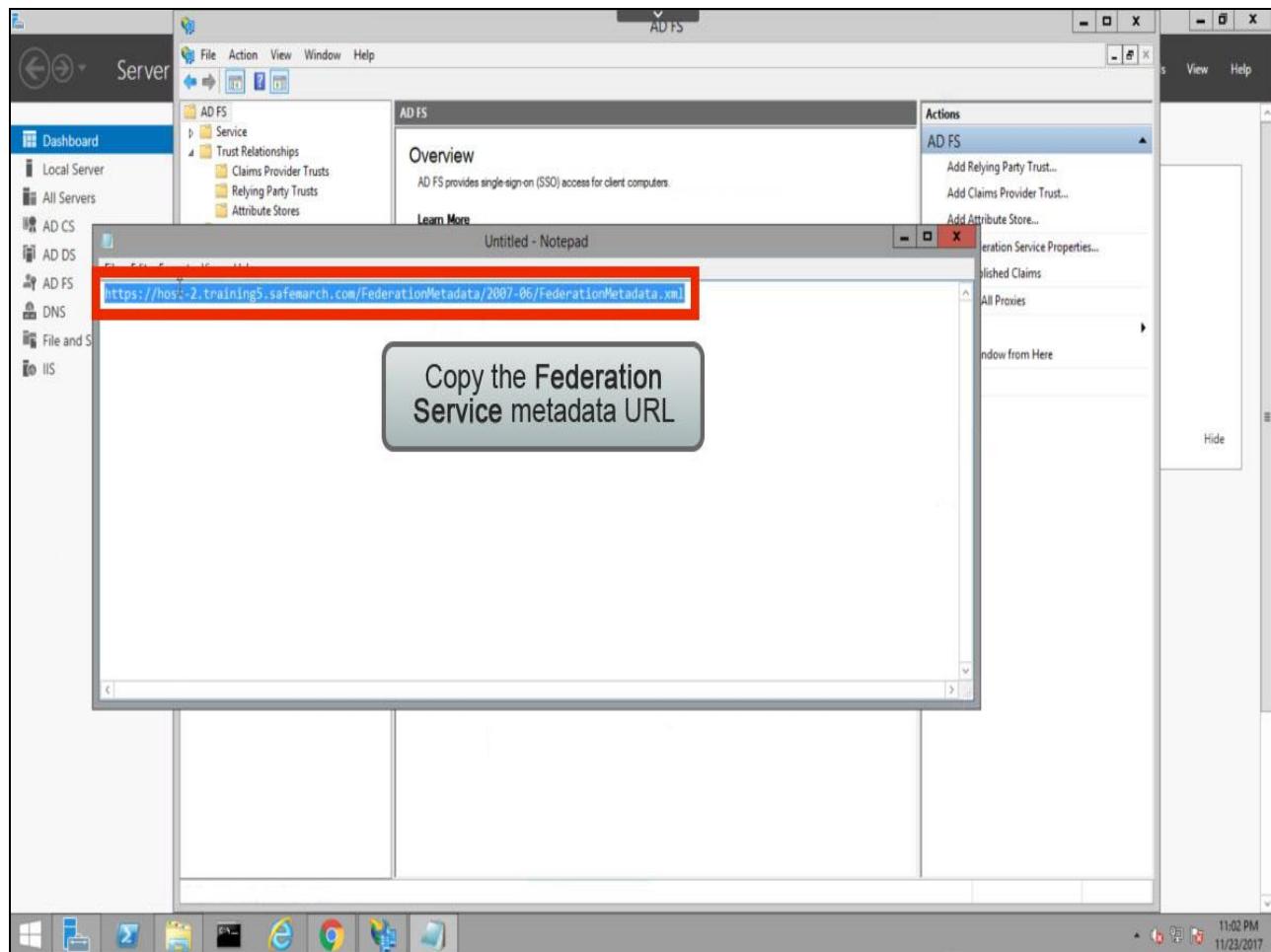
## Slide 89 - Slide 89



## Slide notes

You then need to paste the **Federation Server name** into the host portion of the URL shown here (<https://<ADFS Server Name>/FederationMetadata/2007-06/FederationMetadata.xml>)...

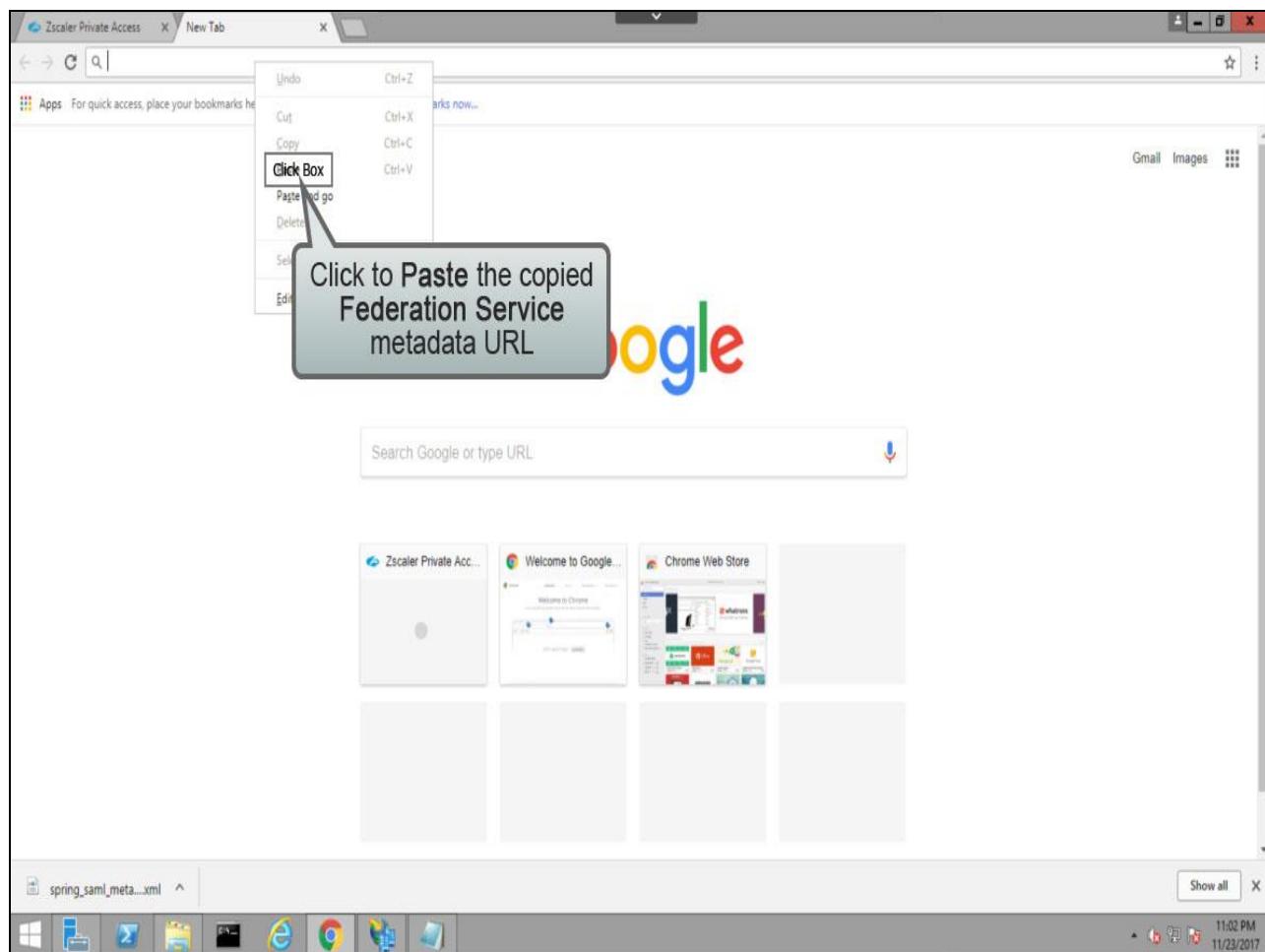
## Slide 90 - Slide 90



## Slide notes

...then copy the entire URL, ...

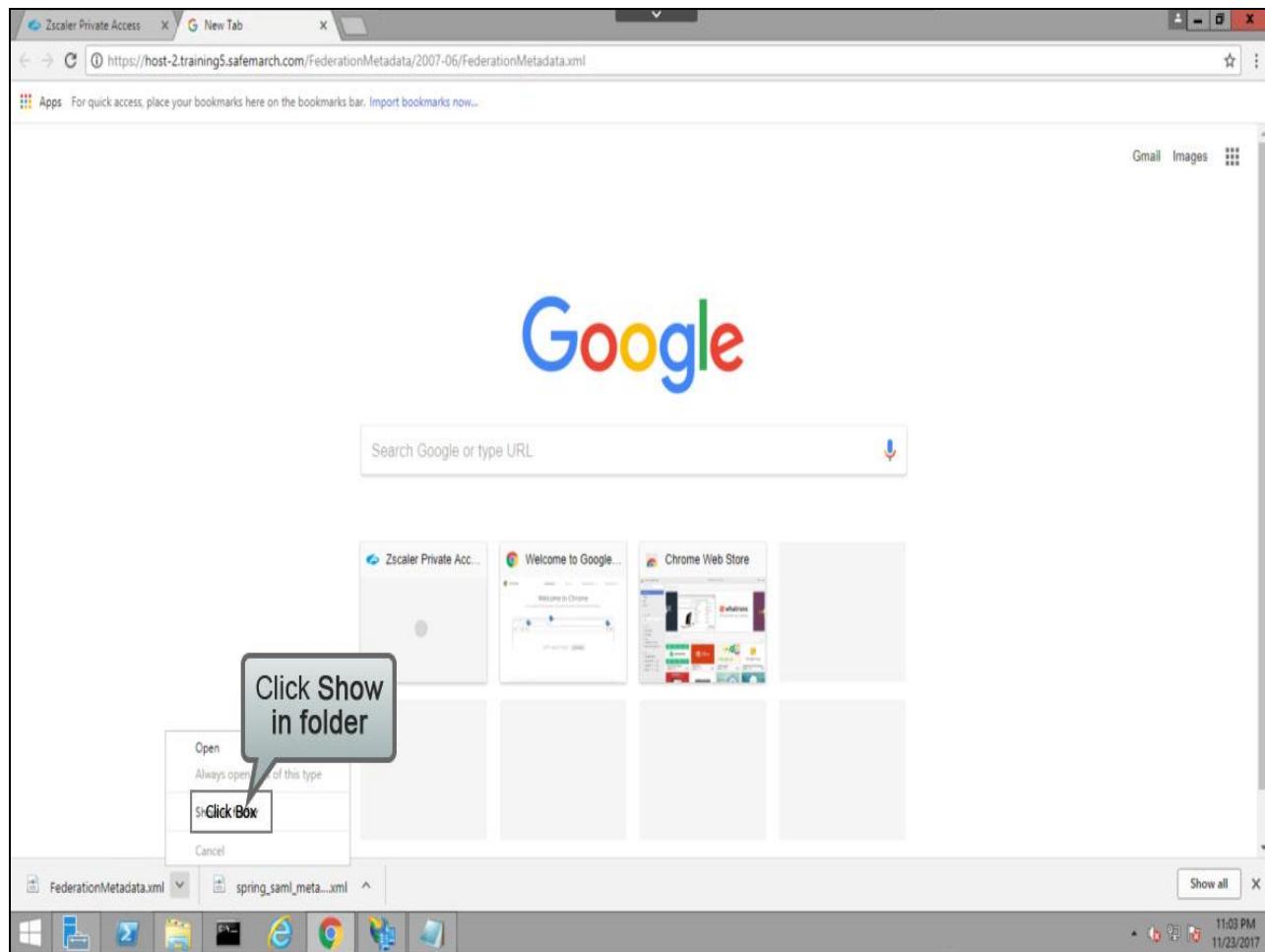
## Slide 91 - Slide 91



## Slide notes

...and paste it into the address bar of a Browser.

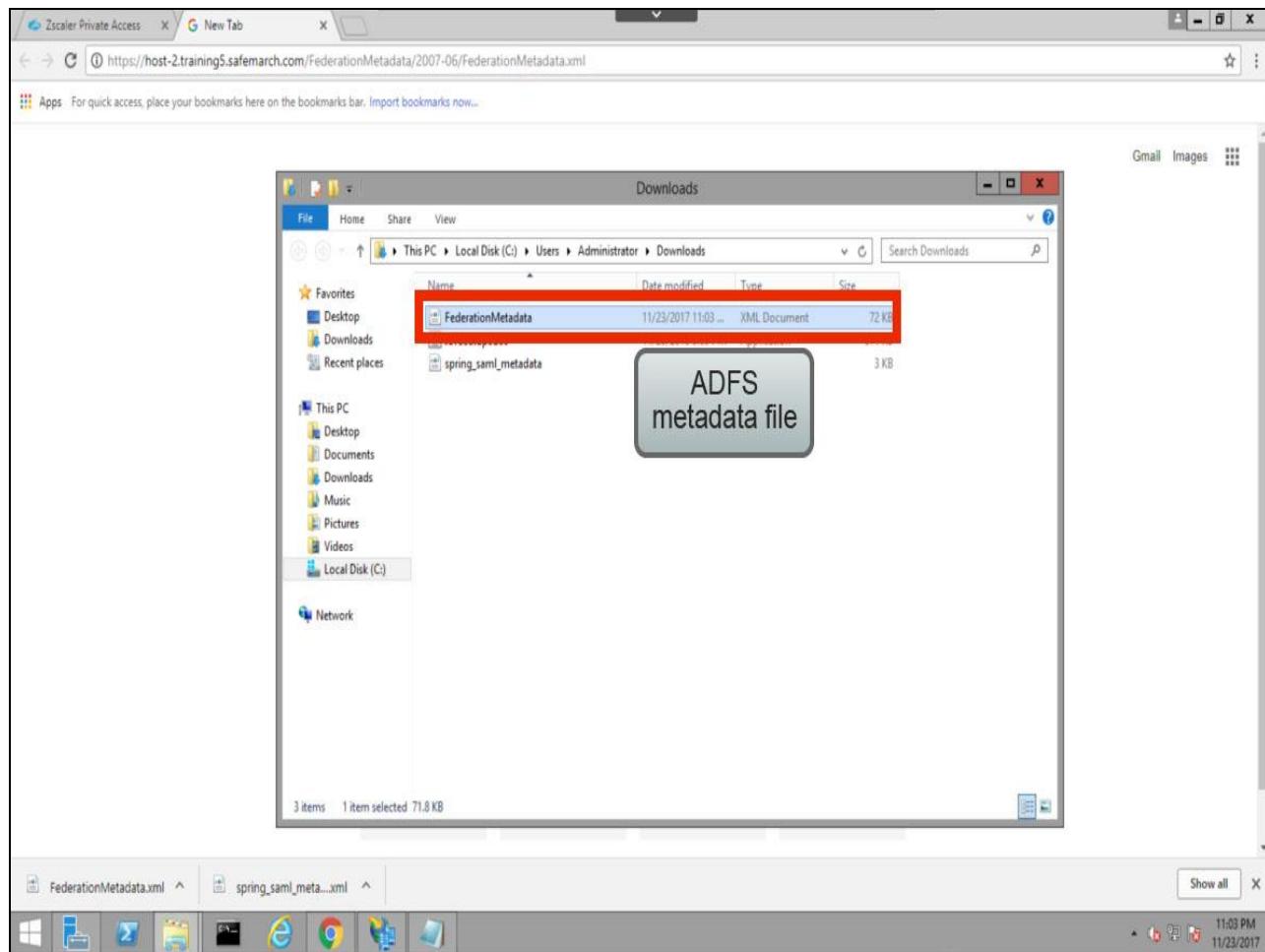
## Slide 92 - Slide 92



## Slide notes

In the Chrome Browser, click **Show in Folder** to see where the file has been saved.

## Slide 93 - Slide 93



### Slide notes

As before, make a note of where the file is located, and move it to a share accessible to the ZPA admin portal if necessary.

## Slide 94 - Configuring ZPA for ADFS Authentication



# Configuring ZPA for ADFS Authentication

E. Configuring IdP information in ZPA

**Slide notes**

Next, we'll look at how to import that metadata file, to add the IdP to the ZPA configuration.

## Slide 95 - Slide 95

The screenshot shows the Zscaler Admin Portal's navigation bar on the left with options like Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main content area is titled 'IdP Configuration' and contains a table with two entries:

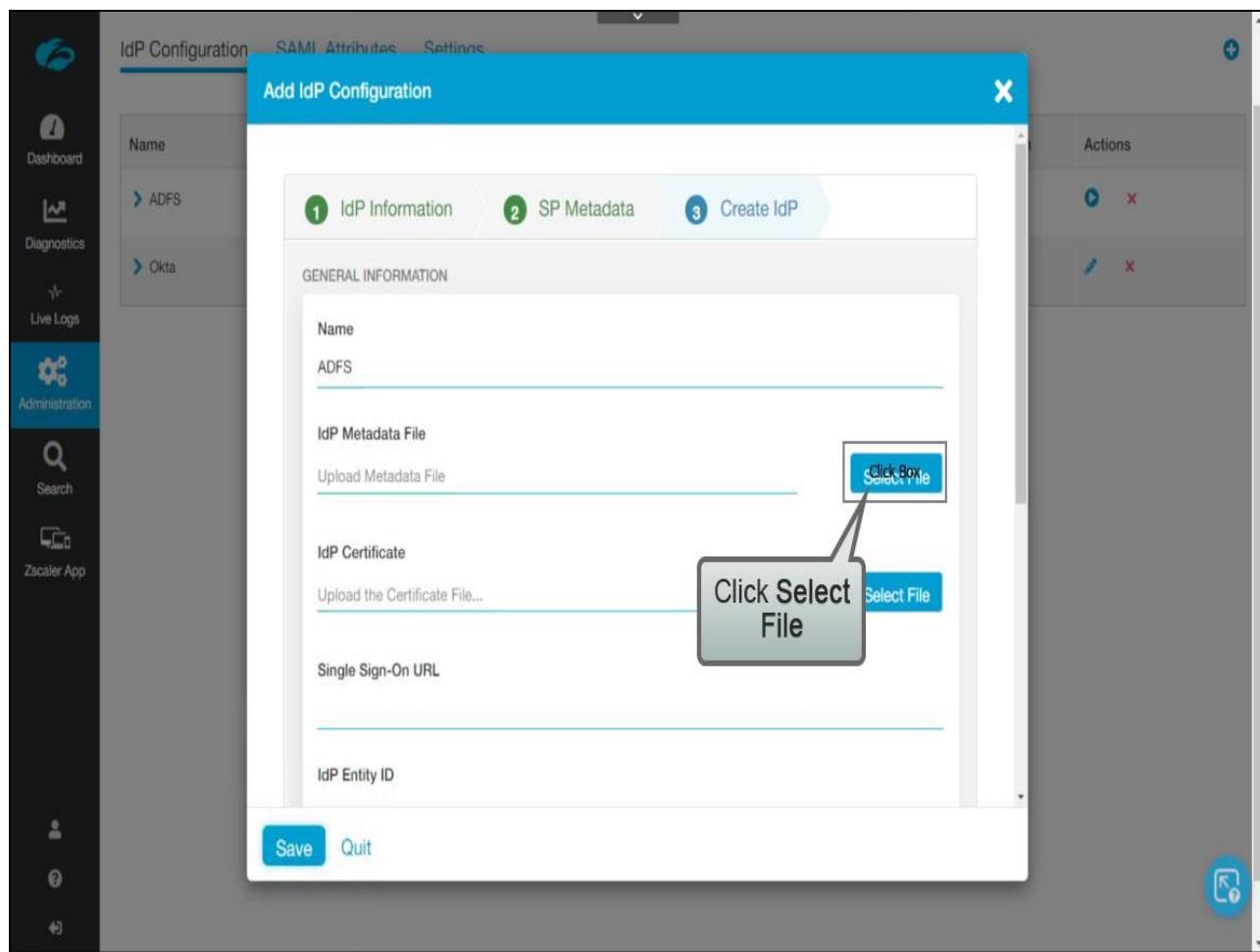
Name	Status	IdP Entity ID	Single Sign-On	Actions
ADFS	Paused		User	<span>Click Box</span> <span>X</span>
Okta	Active	http://www.okta.com/exkltqh8up9sQl2z90h7	User	<span>X</span>

A callout box with the text 'Click to Resume configuration' points to the 'Click Box' button next to the ADFS entry.

## Slide notes

In the ZPA Admin Portal, on the **Administration > AUTHENTICATION > IdP Configuration** page, click to **Resume** configuration of the ADFS IdP that you paused previously.

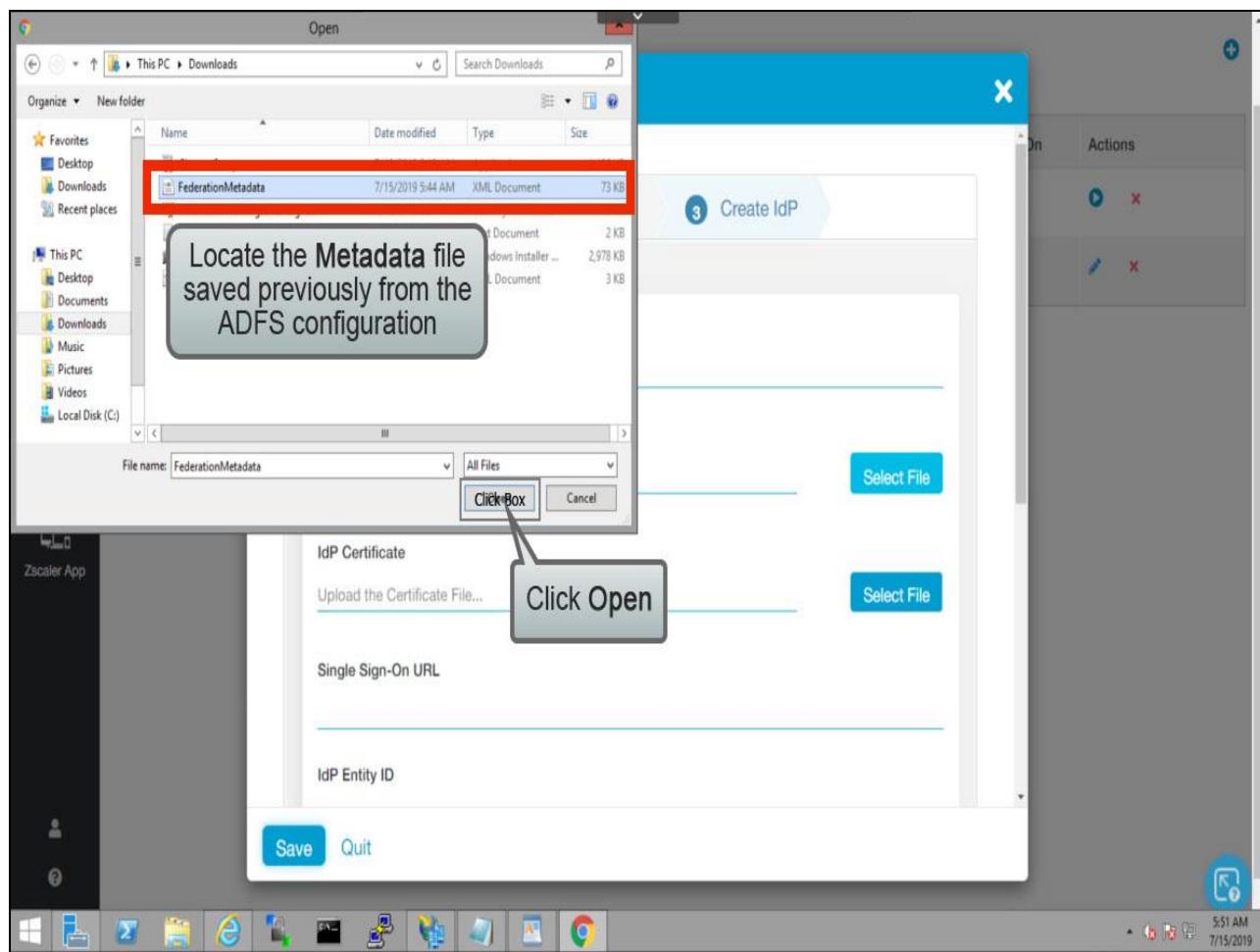
## Slide 96 - Slide 96



## Slide notes

To import the IdP metadata file we just saved from ADFS, click **Select File**.

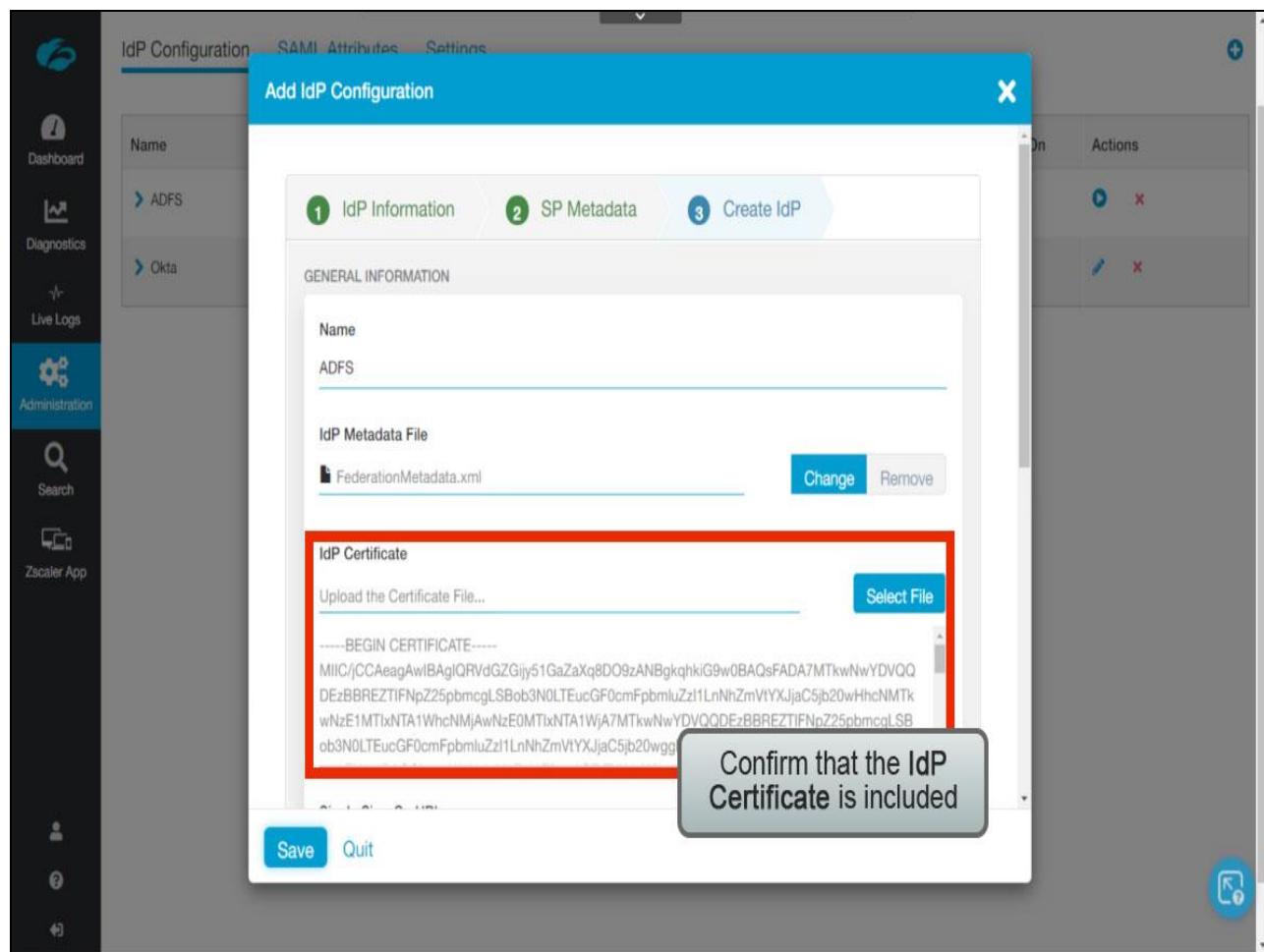
## Slide 97 - Slide 97



## Slide notes

Browse to the share and folder containing the ADFS metadata file, select it, and click **Open**.

## Slide 98 - Slide 98



## Slide notes

Confirm that the file imports successfully and that the **IdP Certificate** is included.

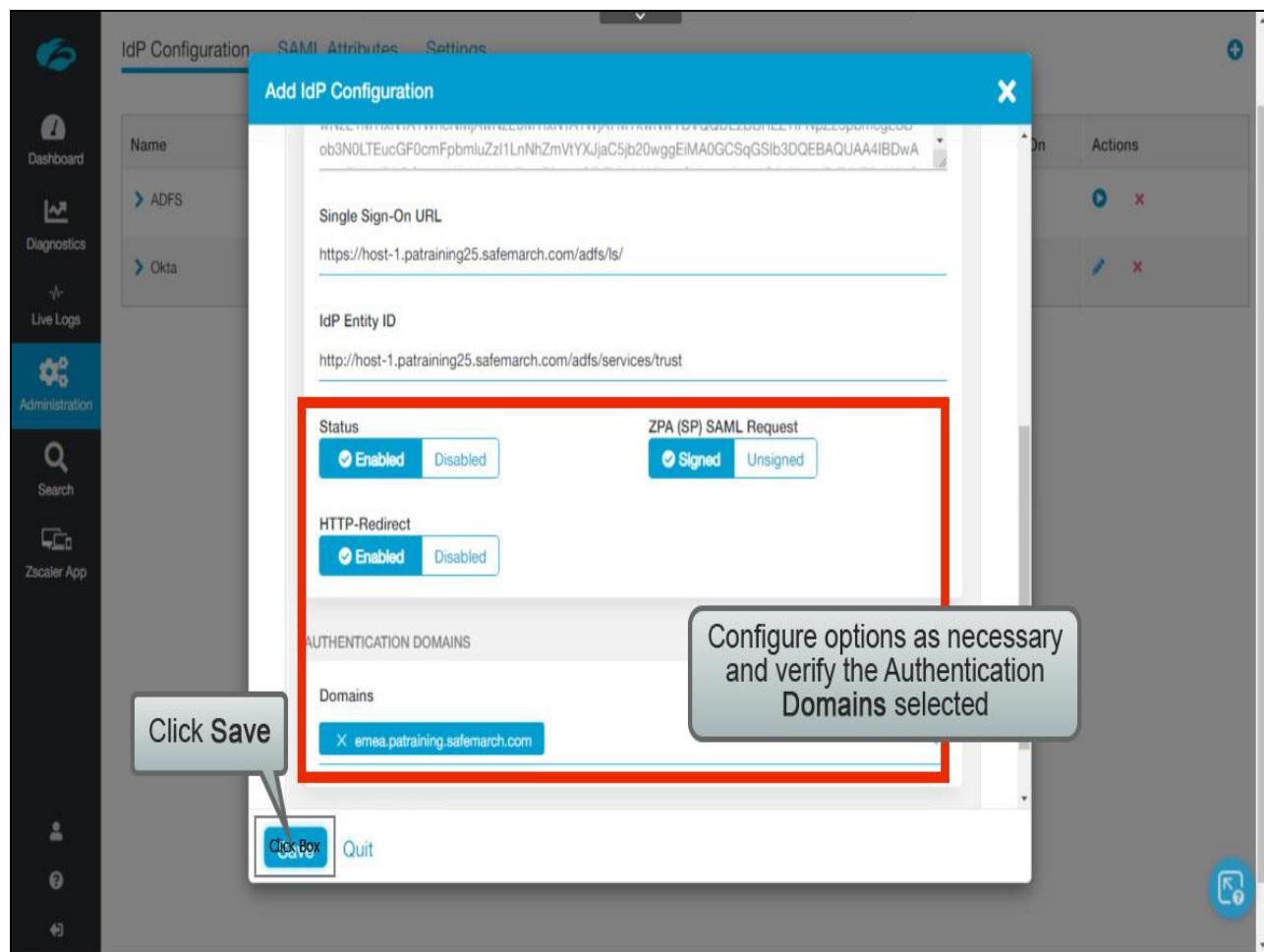
## Slide 99 - Slide 99

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal window titled 'Add IdP Configuration' is open, showing the 'ADFS' configuration. The 'GENERAL INFORMATION' section contains the name 'ADFS' and the metadata file 'FederationMetadata.xml'. Below this, there is a text area containing a certificate's BEGIN CERTIFICATE string, which is partially visible. A large gray box with the text 'Scroll down...' covers the bottom portion of this area. At the bottom of the modal are 'Save' and 'Quit' buttons.

## Slide notes

Scroll down, ...

## Slide 100 - Slide 100



## Slide notes

...configure IdP options as necessary and confirm the correct **Domains** are included, then click **Save**.

## Slide 101 - Slide 101

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. Two entries are listed: ADFS (Status: green checkmark, Entity ID: http://host-1.patraining25.safemarch.com/adfs/services/trust, Single Sign-On: User, Actions: edit, delete) and Okta (Status: green checkmark, Entity ID: http://www.okta.com/exkltqh8up9sQi2z90h7, Single Sign-On: User, Actions: edit, delete). A green notification bar at the bottom right says "IdP configuration saved" with a refresh icon.

Name	Status	IdP Entity ID	Single Sign-On	Actions
ADFS	✓	http://host-1.patraining25.safemarch.com/adfs/services/trust	User	
Okta	✓	http://www.okta.com/exkltqh8up9sQi2z90h7	User	

## Slide notes

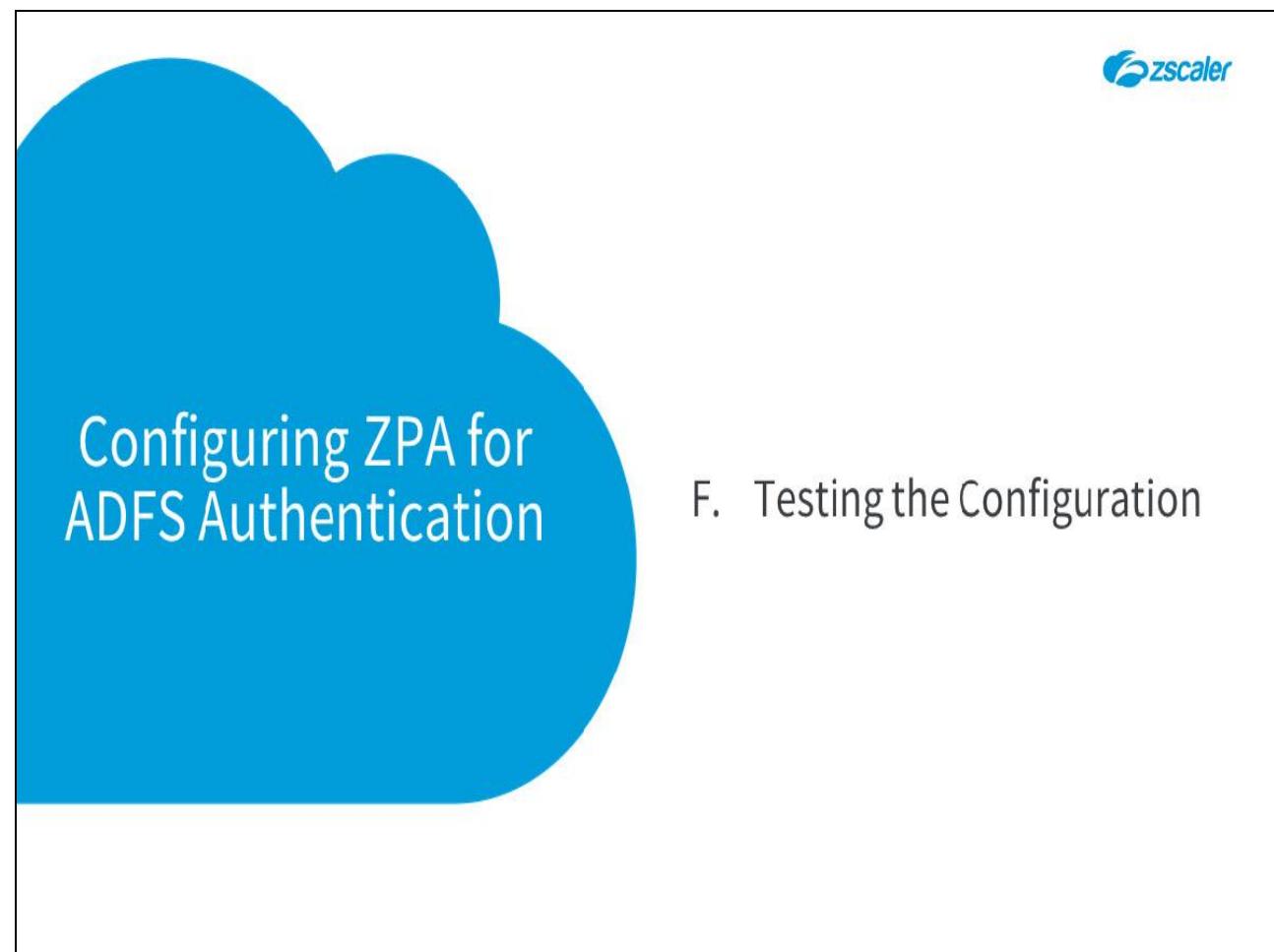
## Slide 102 - Slide 102

Name	Status	IdP Entity ID	Single Sign-On	Actions
ADFS	✓	http://host-1.patraining25.safemarch.com/adfs/services/trust	User	
Okta	✓	http://www.okta.com/exkltqh8up9sQi2z90h7	User	

## Slide notes

The IdP will be saved and is ready for use.

## Slide 103 - Configuring ZPA for ADFS Authentication



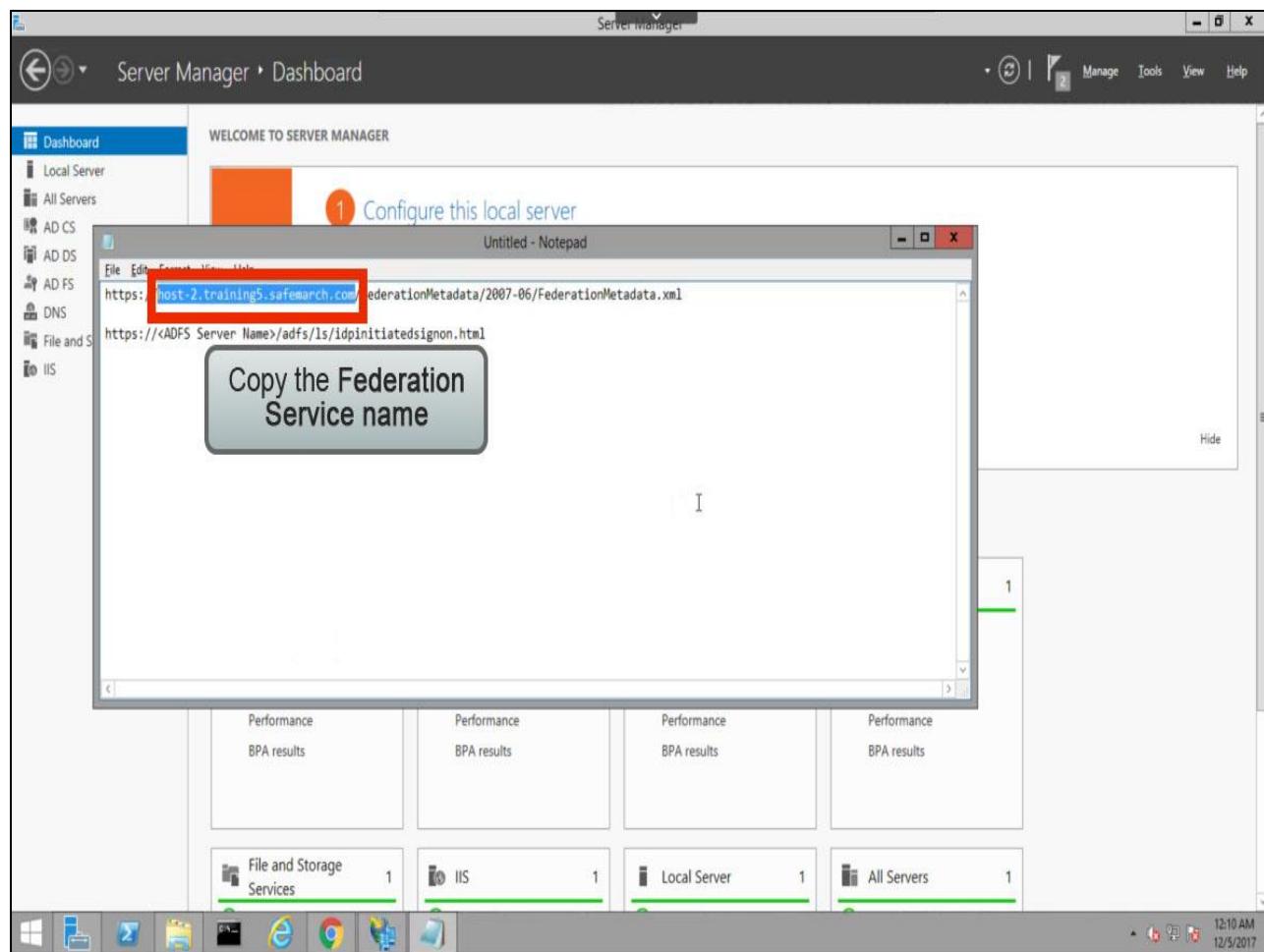
The slide features a large, semi-transparent blue cloud shape on the left side, containing the text "Configuring ZPA for ADFS Authentication". In the top right corner of the slide area, there is a small Zscaler logo.

F. Testing the Configuration

**Slide notes**

Finally, we'll look at how to test the IdP configuration, and import attributes if necessary.

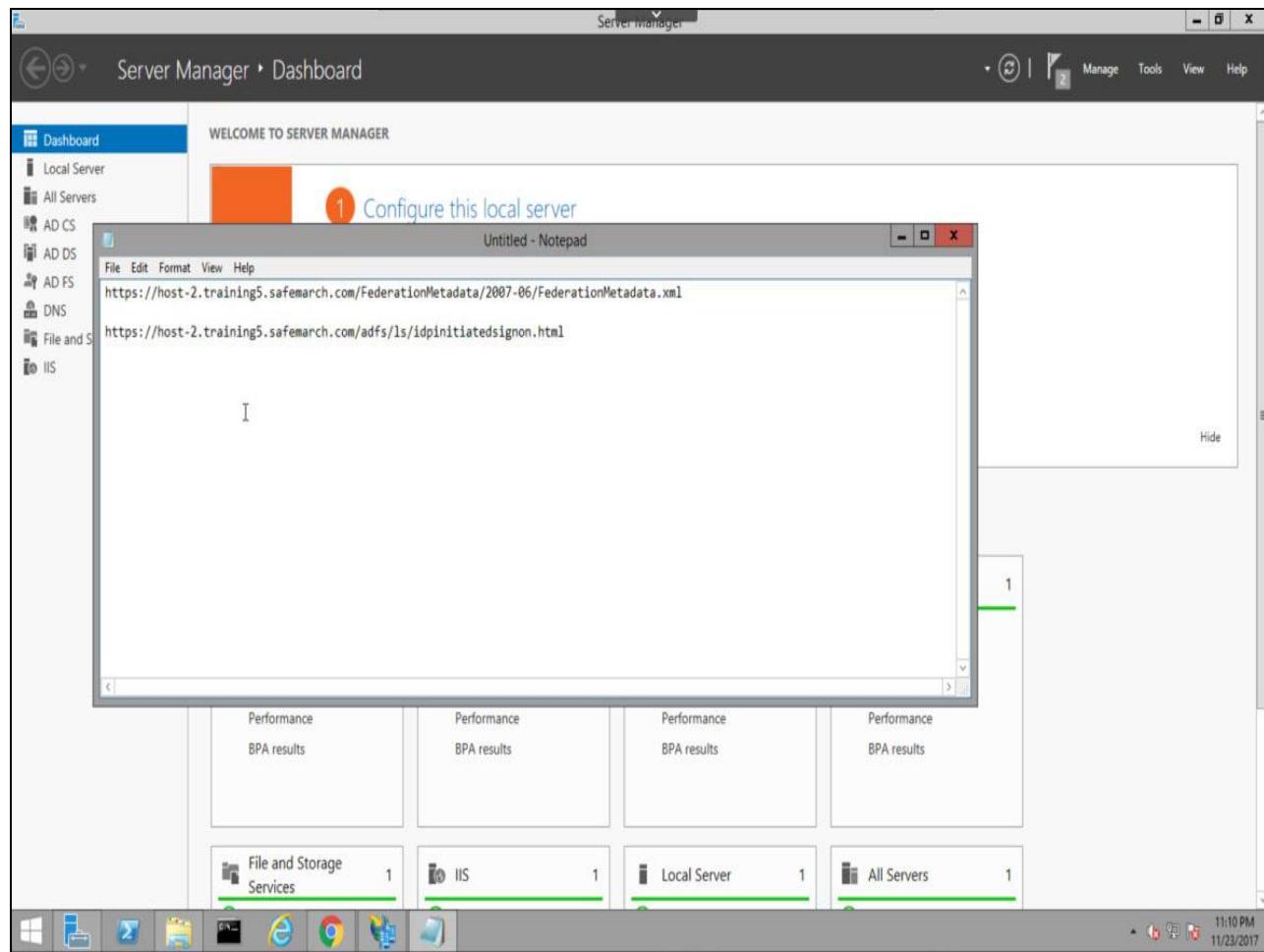
## Slide 104 - Slide 104



## Slide notes

Copy the Federation Service name once more, ...

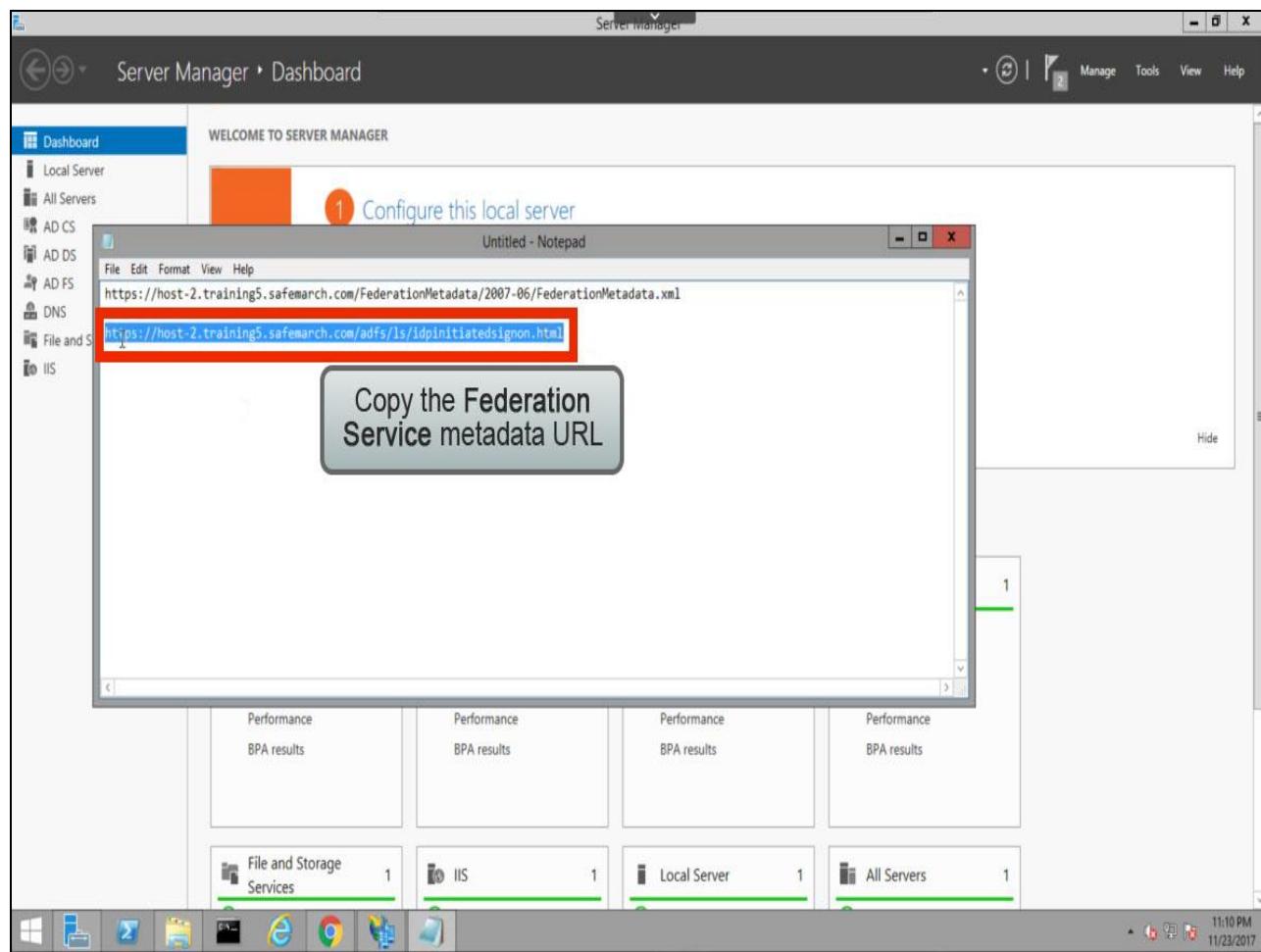
## Slide 105 - Slide 105



## Slide notes

...and paste it into the URL shown here (<https://<ADFS Server Name>/adfs/ls/idpinitiatedsignon.html>).

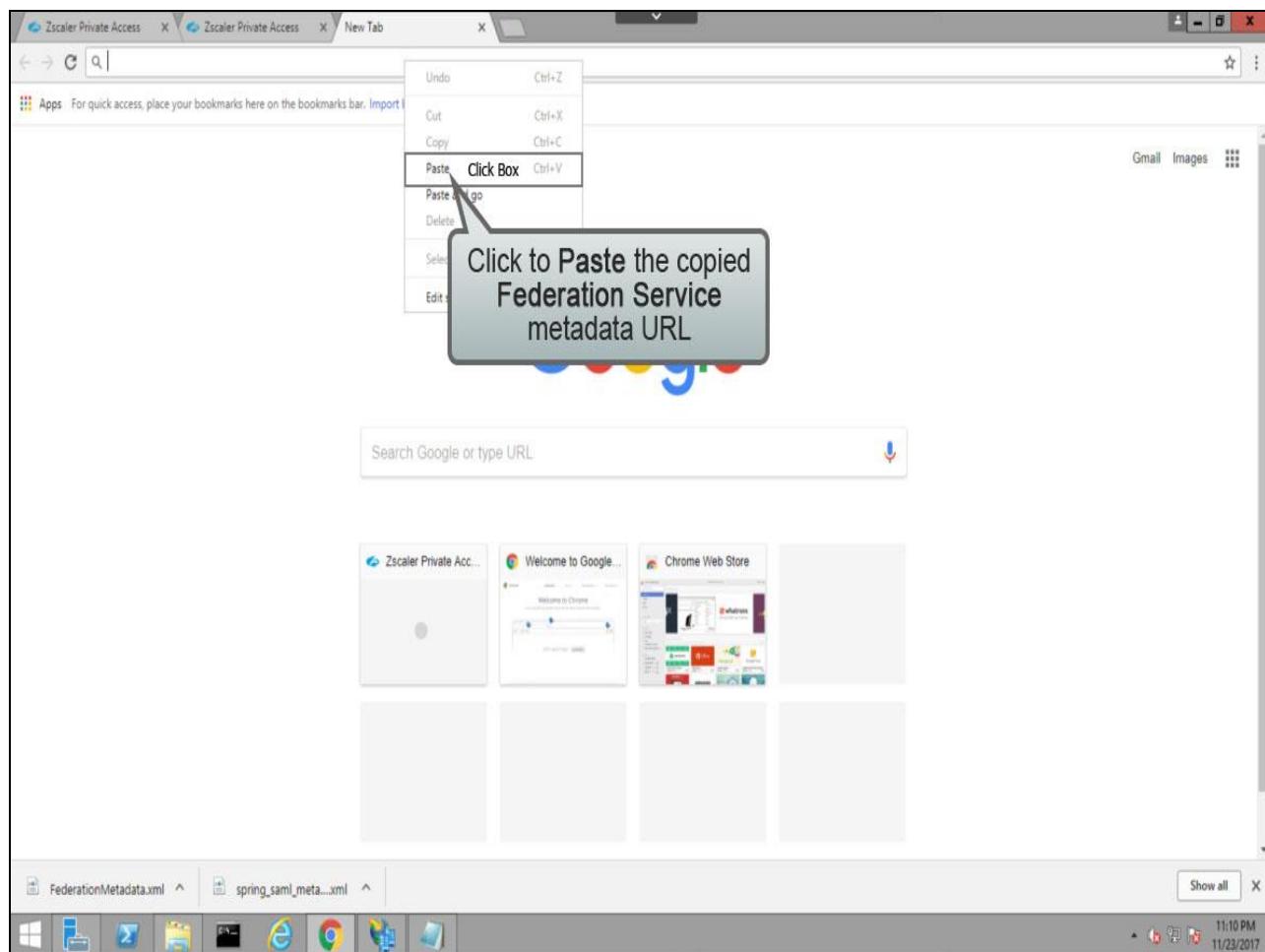
## Slide 106 - Slide 106



## Slide notes

Copy the entire URL, ...

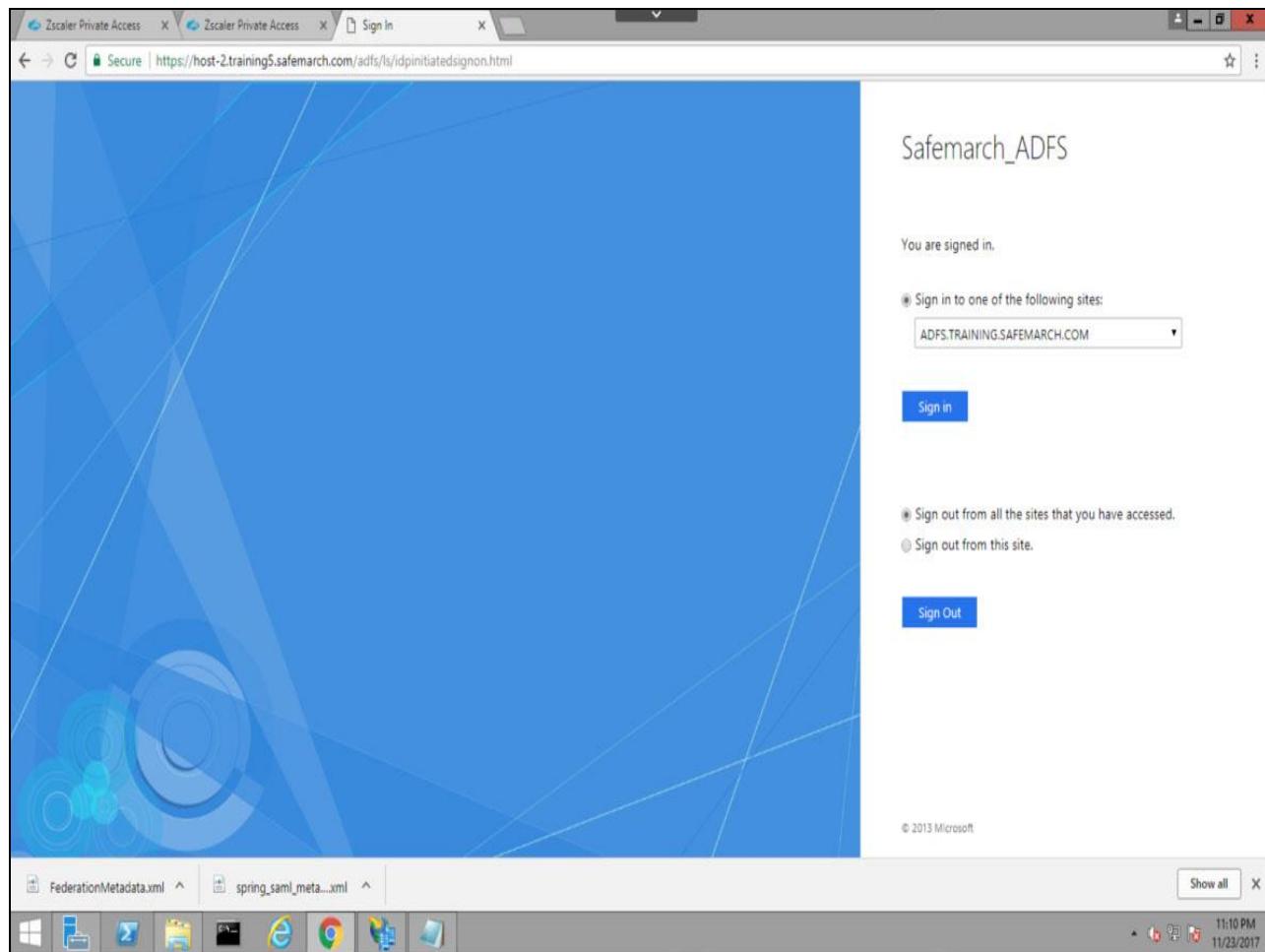
## Slide 107 - Slide 107



## Slide notes

...and paste it into a new Browser tab.

## Slide 108 - Slide 108



### Slide notes

Confirm that you are taken to the ADFS sign in page.

## Slide 109 - Slide 109

The screenshot shows the Zscaler Admin Portal interface. On the left is a dark sidebar with various icons and labels: Dashboard, Diagnostics, Live Logs, Administration (which is selected), 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 columns: Name, Status, IdP Entity ID, Single Sign-On, and Actions. There are two rows in the table. The first row has a status icon with a green checkmark, the URL <http://host-1.patraining25.safemarch.com/adfs/services/trust>, and the Single Sign-On status "User". The second row also has a green checkmark, the URL <http://www.okta.com/exkltqh8up9sQl2z90h7>, and the Single Sign-On status "User". To the right of the table is a blue circular icon with a white question mark. A callout box with a grey border and a black arrow points from the bottom-left towards the first row of the table. Inside the callout box is the text "Click to expand the IdP configuration".

Name	Status	IdP Entity ID	Single Sign-On	Actions
Click to expand the IdP configuration	✓	<a href="http://host-1.patraining25.safemarch.com/adfs/services/trust">http://host-1.patraining25.safemarch.com/adfs/services/trust</a>	User	
	✓	<a href="http://www.okta.com/exkltqh8up9sQl2z90h7">http://www.okta.com/exkltqh8up9sQl2z90h7</a>	User	

## Slide notes

In the ZPA admin portal, on the **Administration > AUTHENTICATION > IdP Configuration** page, expand the details for the ADFS IdP that you just added, ...

## Slide 110 - Slide 110

The screenshot shows the Zscaler Admin UI with the 'SAML Attributes' tab selected under 'IdP Configuration'. On the left sidebar, there are various navigation icons for Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help.

In the main content area, a table lists the configured IdPs:

Name	Status	IdP Entity ID	Single Sign-On	Actions
ADFS	✓	http://host-1.patraining25.safemarch.com/adfs/services/trust	User	<a href="#"></a> <a href="#"></a>

Below the table, detailed configuration settings are shown for the ADFS entry:

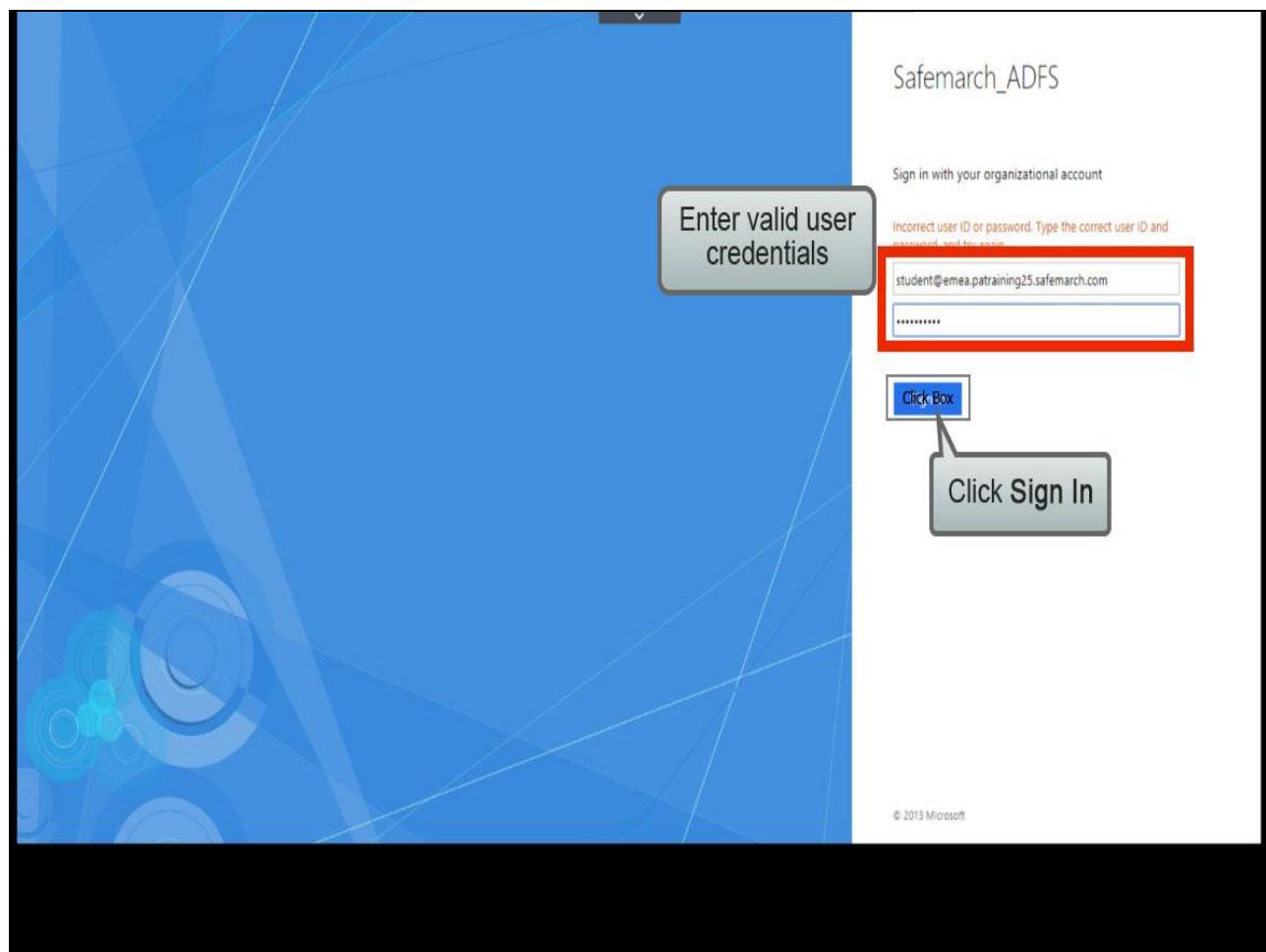
- Single Sign-On URL:** https://host-1.patraining25.safemarch.com/adfs/ls/
- ZPA (SP) SAML Request:** Signed (Enabled)
- HTTP-Redirect:** Enabled
- Authentication Domains:** emea.patraining.safemarch.com
- Import SAML Attributes:** emea.patraining.safemarch.com
- SAML Attributes:** [Show Attributes >](#)
- SERVICE PROVIDER SAML METADATA FOR USER SSO:**
  - Service Provider Metadata:** [Download Metadata](#)
  - Service Provider URL:** https://samlsp.private.zscaler.com/auth/144123139134062757/sso
- Service Provider Certificate:** [Download Certificate](#)
- Service Provider Entity ID:** https://samlsp.private.zscaler.com/auth/metadata/144123139134062757
- IdP CERTIFICATE:**
  - Common Name:** ADFS Signing - host-1.patraining25.safemarch.com
  - Serial Number:** 92169889259724689749033941848578641655
  - Created On:** Monday, July 15 2019 5:15:05 am
  - Expires On:** Tuesday, July 14 2020 5:15:05 am
- Okta:** ✓ [Edit](#) [Delete](#)

A callout box with the text "Click Box" points to the "Edit" icon in the "Actions" column for the Okta entry. Another callout box with the text "Click Import" points to the "Import" icon in the "Actions" column for the ADFS entry.

## Slide notes

...and click to Import SAML Attributes from the IdP.

## Slide 111 - Slide 111



## Slide notes

Verify that you are taken to the ADFS sign-in page, enter valid user credentials and click **Sign In**.

## Slide 112 - Slide 112

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 Help. The main area has a blue header 'Import SAML Attributes'. It contains a table with three rows:

Name	SAML Attribute Name
DisplayName_ADFS	DisplayName
memberOf_ADFS	memberOf
Department_ADFS	Department

Below the table is a JSON preview of user attributes:

```
{"nameid": "student@emea.patraining25.safemarch.com", "orgId": "144123139134062592", "idpEntityID": "http://host-1.patraining25.safemarch.com/adfs/services/trust", "idpID": "144123139134062757", "saml_attributes": [{"DisplayName": "student PATraining25", "memberOf": ["Domain Users", "Marketing"]}]}
```

A callout box with a blue arrow points to the 'Click Save' button at the bottom-left of the dialog.

## Slide notes

On a successful authentication, you will be shown the JSON script showing the returned attributes for the user. If you have not yet imported these, you can click **Save** to import any new attributes to the **ZPA SAML Attributes** configuration.

## Slide 113 - Slide 113

The screenshot shows the Zscaler Admin UI interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main content area has tabs for IdP Configuration, SAML Attributes (selected), and Settings. Under SAML Attributes, there is a table titled 'IdP Configuration' with a dropdown set to 'All'. The table lists three attributes: 'Department\_ADFS' (SAML Attribute: Department, IdP Name: ADFS), 'memberOf\_ADFS' (SAML Attribute: memberOf, IdP Name: ADFS), and 'DisplayName\_ADFS' (SAML Attribute: DisplayName, IdP Name: ADFS). Each row has edit and delete icons. A green notification bar at the bottom right says 'SAML attributes imported successfully' with a refresh icon.

Name	SAML Attribute	IdP Name	Actions
Department_ADFS	Department	ADFS	
memberOf_ADFS	memberOf	ADFS	
DisplayName_ADFS	DisplayName	ADFS	

## Slide notes

## Slide 114 - Slide 114

The screenshot shows the Zscaler Admin UI with the navigation bar on the left. The main content area is titled "SAML Attributes". At the top right of this area is a dropdown menu labeled "IdP Configuration" with "ADFS" selected. A red box highlights this dropdown. A callout bubble with a blue border and white text points to the "ADFS" option, containing the text "Filter SAML Attributes by IdP". Below the dropdown, there is a table with three rows, each representing a SAML attribute mapping:

Name	SAML Attribute	IdP Name
DisplayName_ADFS	DisplayName	ADFS
memberOf_ADFS	memberOf	ADFS
Department_ADFS	Department	ADFS

## Slide notes

On the **Administration > AUTHENTICATION > SAML Attributes** page, you have the option to filter the view to see only those attributes from the ADFS IdP that you just added.

Slide 115 - Thank You and Quiz



# Thank You and Quiz

**Slide notes**

This completes the SAML module. We hope this module has been useful to you and thank you for your time.

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