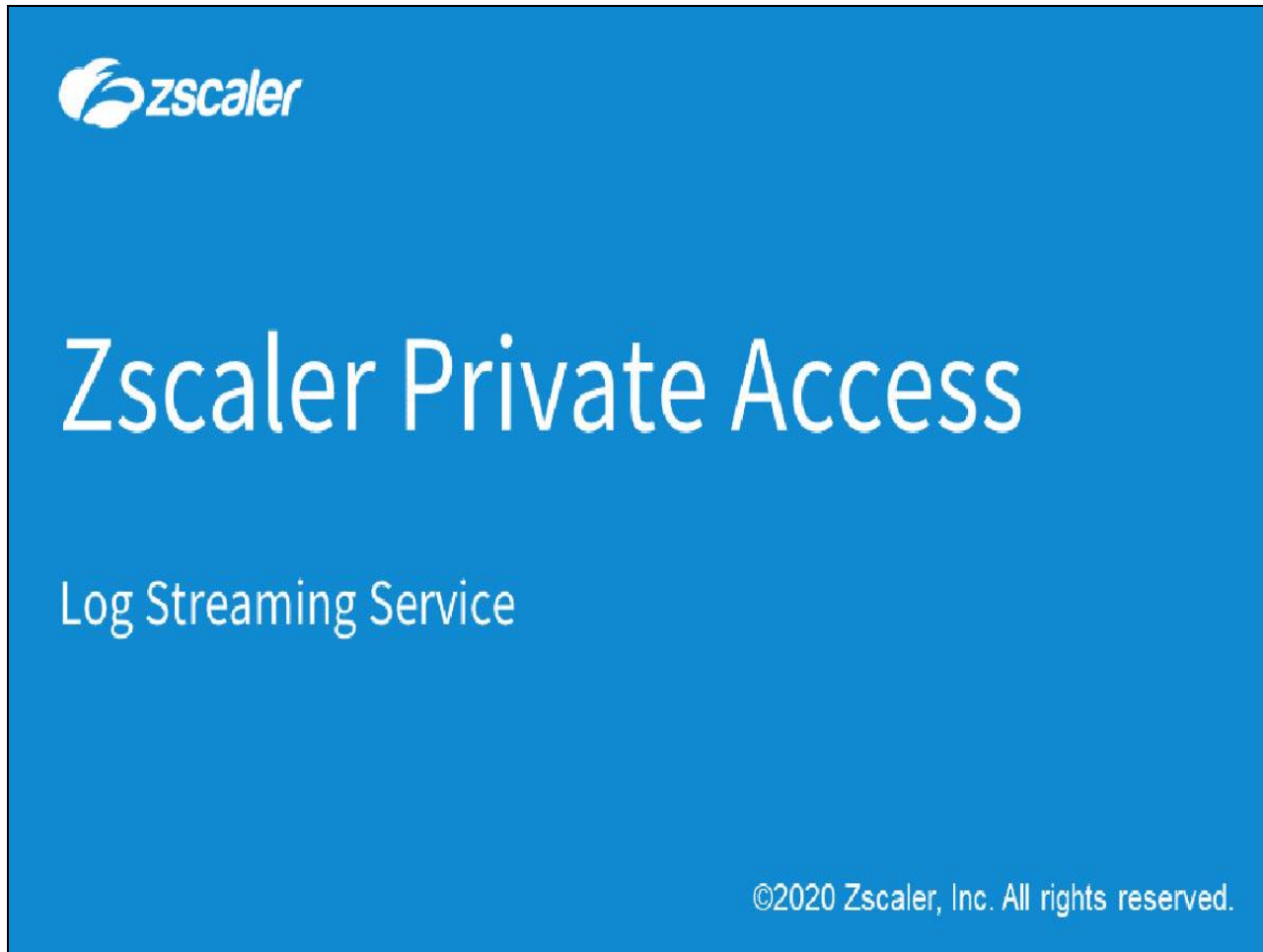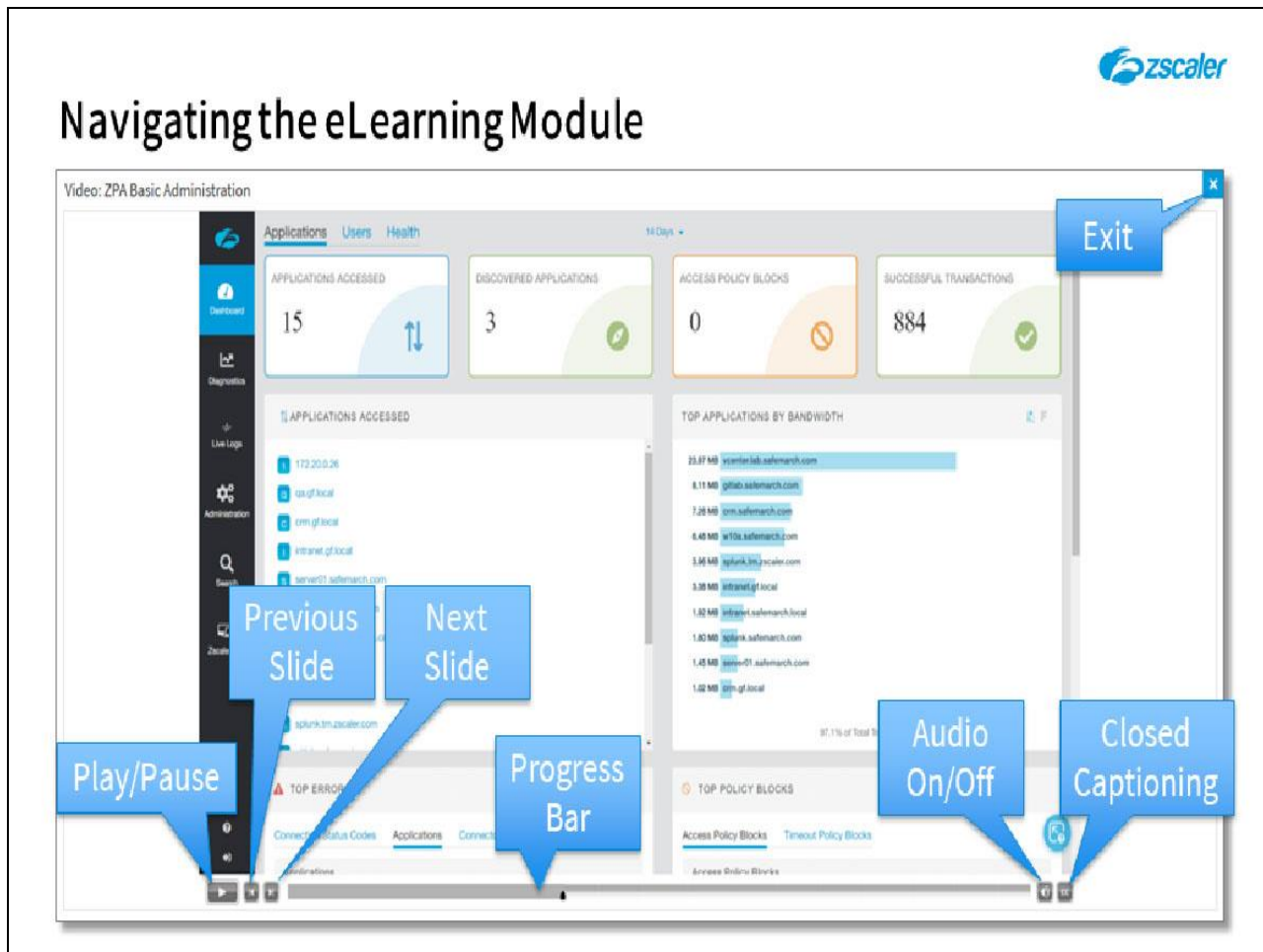Slide 1 - Zscaler Private Access

Slide notes

Welcome to this training module on the Zscaler Private Access Log Streaming Service (LSS).
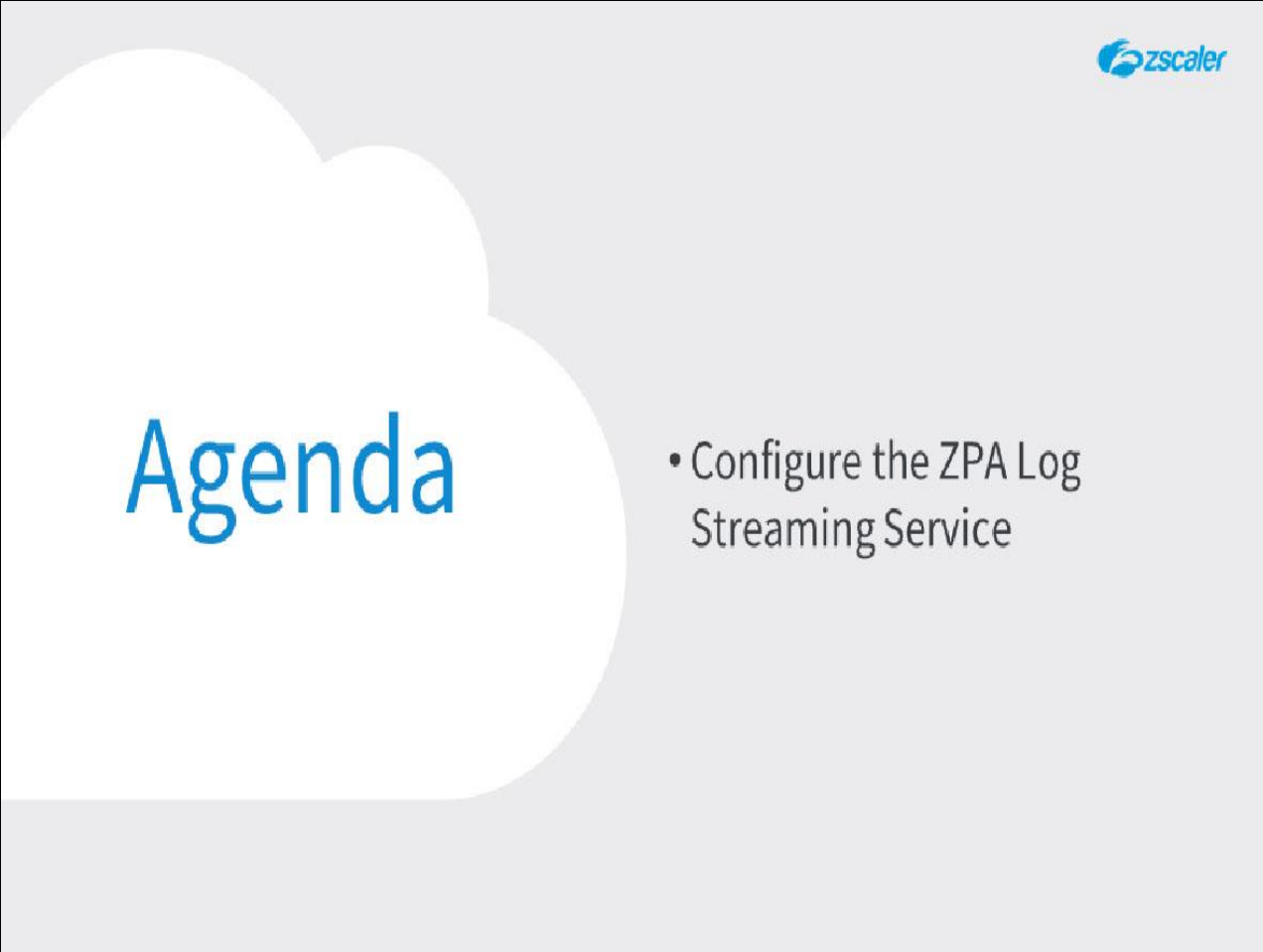
Slide 2 - Navigating the eLearning Module

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.
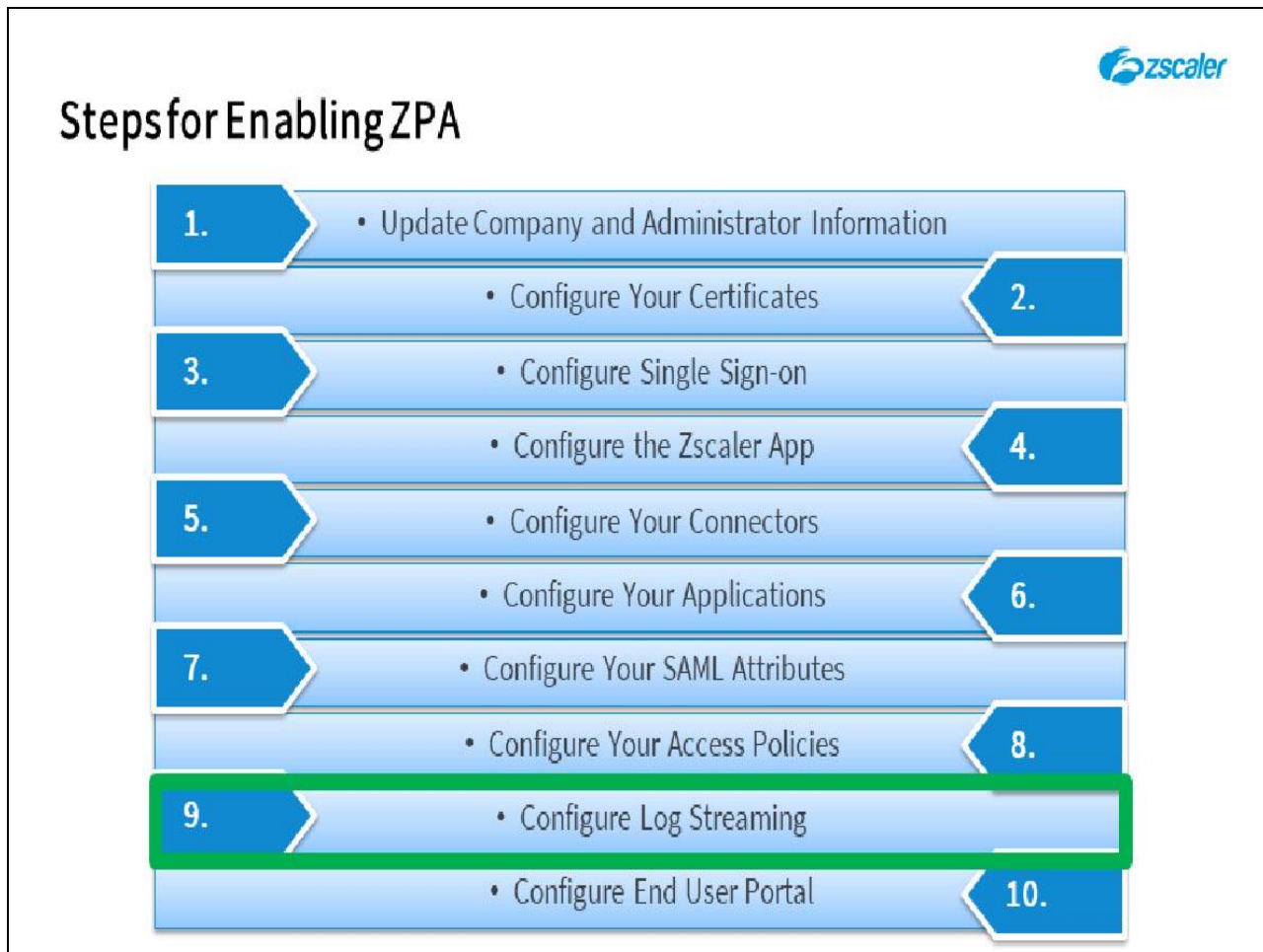
Slide 3 - Agenda

Slide notes

In this module, we will provide an overview of how to configure the ZPA Log Streaming Service (LSS).

Slide 4 - Steps for Enabling ZPA

Slide notes

Just as a reminder, this is where we are in the steps for enabling ZPA. In this module we will cover step 9, to enable and configure Log Streaming.

Slide 5 - Configuring LSS

Slide notes

The next topic that we will cover is how to configure the LSS.

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

Slide 6 - Slide 6

Slide notes

To enable and configure log streaming from your ZPA environment, from the **Administration** menu, click **Log Receivers**.

Slide 7 - Slide 7

Slide notes

Any existing Log Receivers will be displayed. To add a new one, click **Add Log Receiver**.

Slide 8 - Slide 8

Slide notes

Give the log receiver a **Name**, and optionally a **Description**, then specify the FQDN or IP address that logs are to be streamed to and specify the **TCP Port** number to use.

Logs are streamed through Connectors, ideally Connectors that are dedicated to the streaming service (to eliminate any possibility of contention with application data). Click to select the **Connector Group** to stream the logs through.

Slide 9 - Slide 9
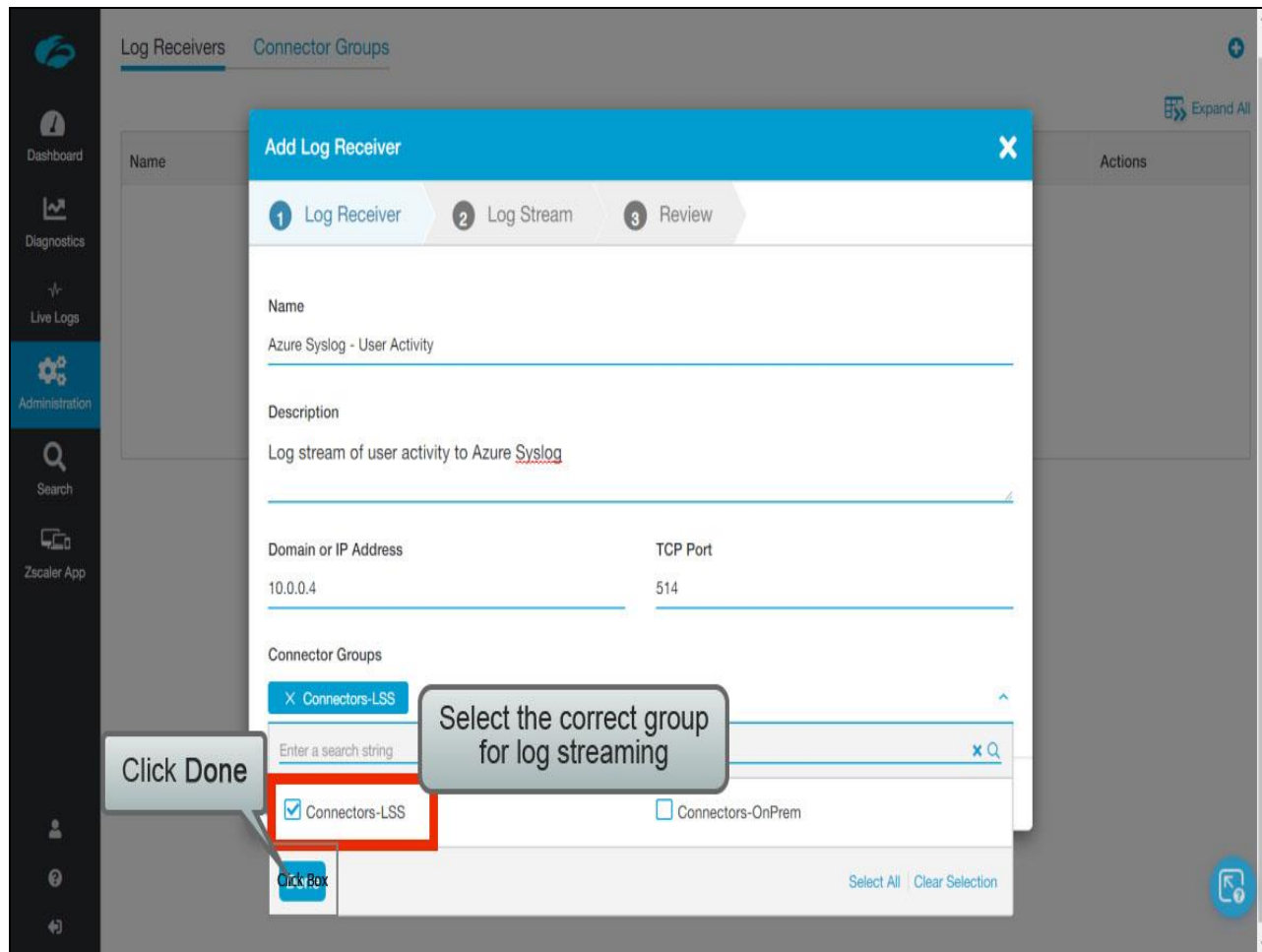
Slide notes

In this example, we have provided a Connector group just for log streaming, named **Connectors-LSS**. Click on the group to select it, then click **Done**, …

Slide 10 - Slide 10

Slide notes

…then click **Next** to proceed with the wizard.

Slide 11 - Slide 11

Slide notes

You now need to configure the **Log Type** to send, the options being: **User Activity**; **User Status**; **Connector Status**; and **Browser Access**. Note that you may only select one **Log Type** per log receiver, so if you wish to receive all log types you will need to set up 4 log receivers, one for each type. The destination can be the same for each, or you can stream each log type to a different system.

In this case we want to stream **User Activity**, so click on that, …

Slide 12 - Slide 12
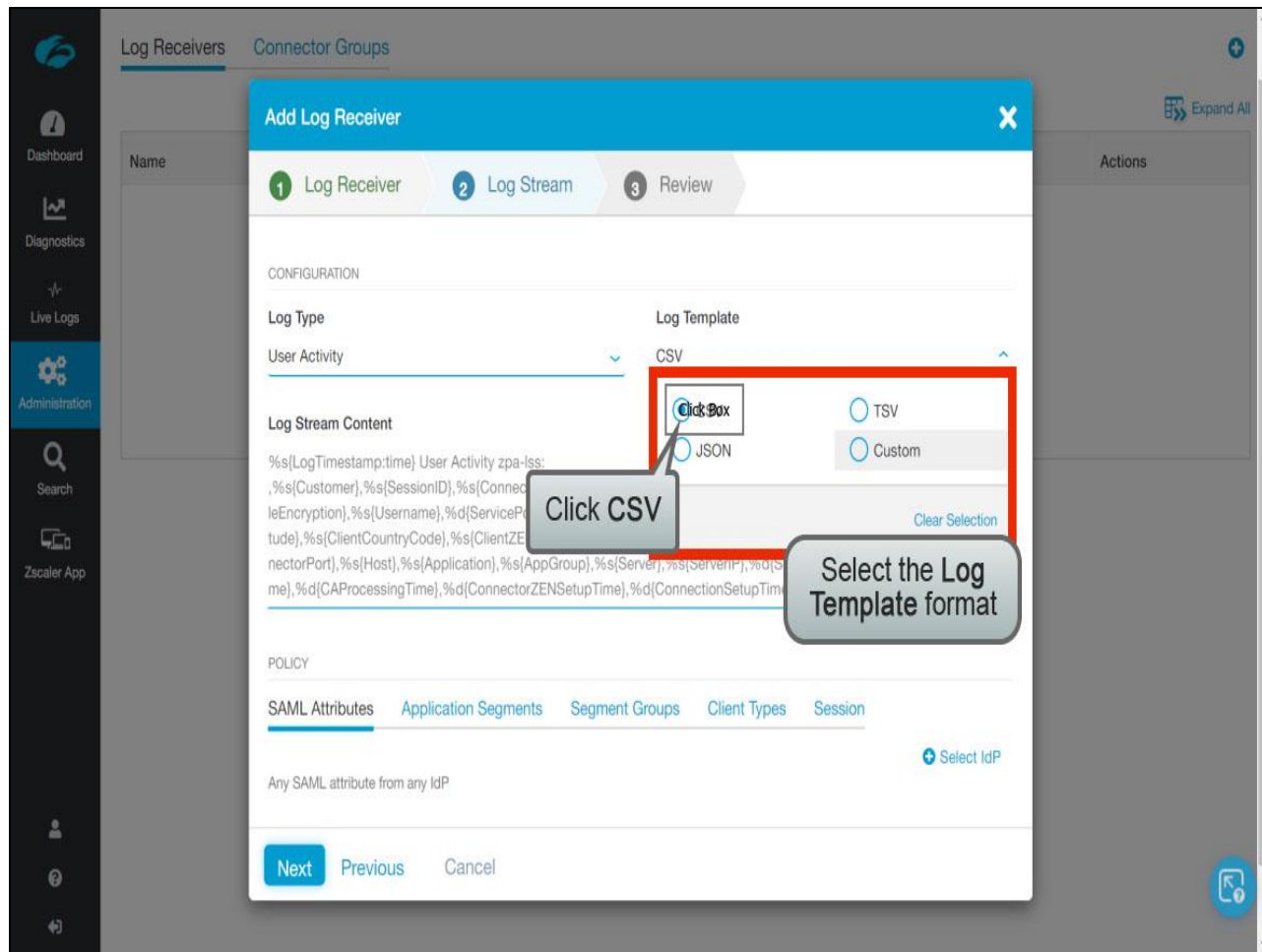
Slide notes

 …then select the **Log Template** to use, the options being; **CSV**, **TSV**, **JSON** and **Custom**. For this example, we will use the default **CSV** option, so click to select it.

Slide 13 - Slide 13

Slide notes

The next option you have is to edit the **Log Stream Content,** which is a comma-separated list of the fields available for the chosen **Log Type**, with format options. See the ZPA on-line help article **Understanding the Log Stream Content Format** for full details of what can be included here. By default, we include all the available fields for the selected **Log Type**.

Slide 14 - Slide 14

Slide notes

You can also configure a **POLICY** for the selected **Log Type**, the policy areas available for **User Activity** are; **SAML Attributes**, **Application Segments**, **Segment Groups**, **Client Types** and **Session**.

Configure each policy area as necessary, for example to configure a subset of **SAML Attributes** to include, you must first click **Select IdP** to choose the source IdP for the attributes of interest, ...

Slide 15 - Slide 15

Slide notes

...then, having selected the IdP, you can add the **SAML Attributes** of interest. We will not actually use SAML attributes in this example, ...

Slide 16 - Slide 16

Slide notes

…nor will we select a subset of the available **Application Segments** to include, …

Slide 17 - Slide 17

Slide notes

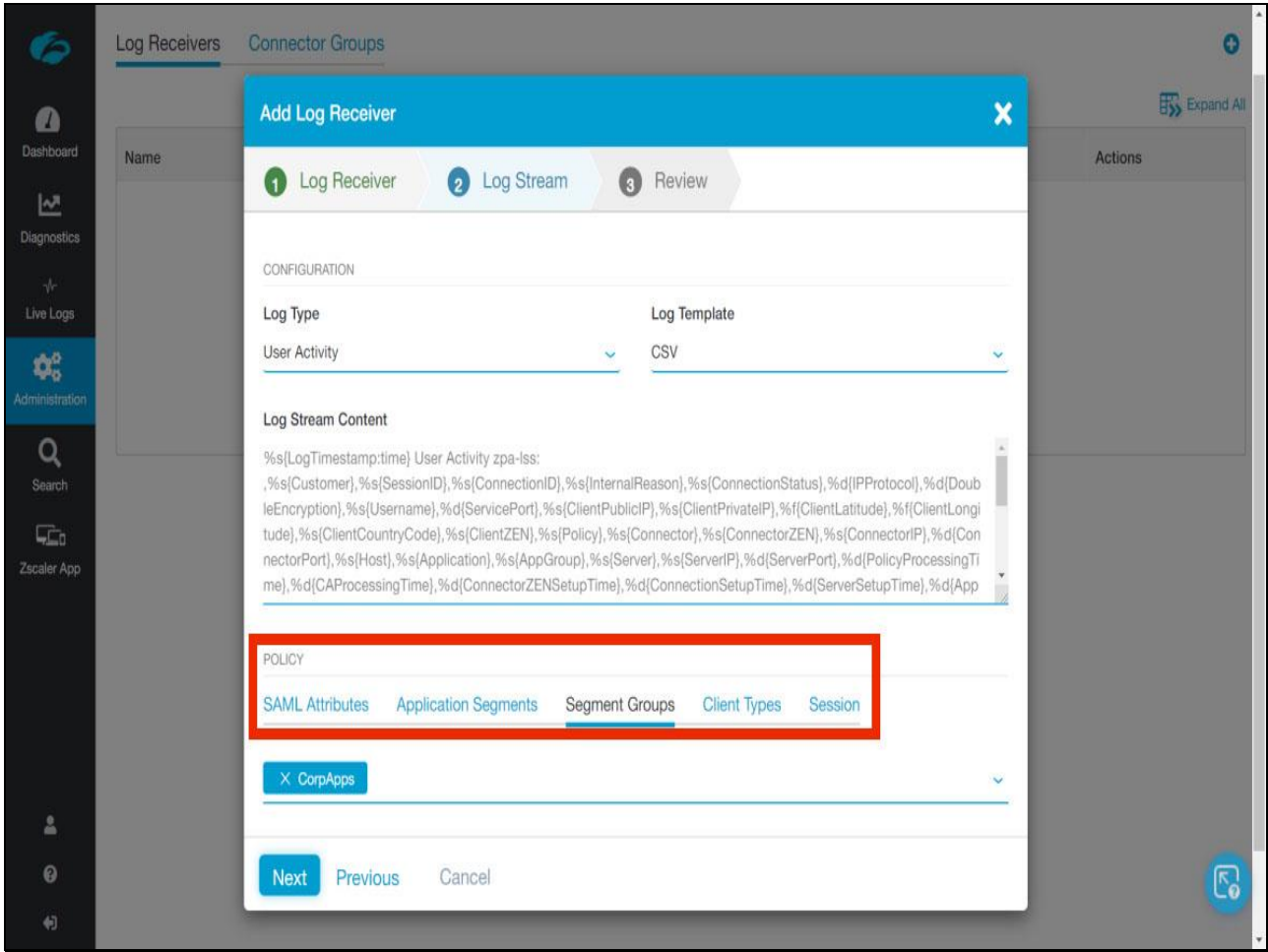…but we will add a **Segment Group** configuration, so click to choose the correct Segment Groups to include.

Slide 18 - Slide 18
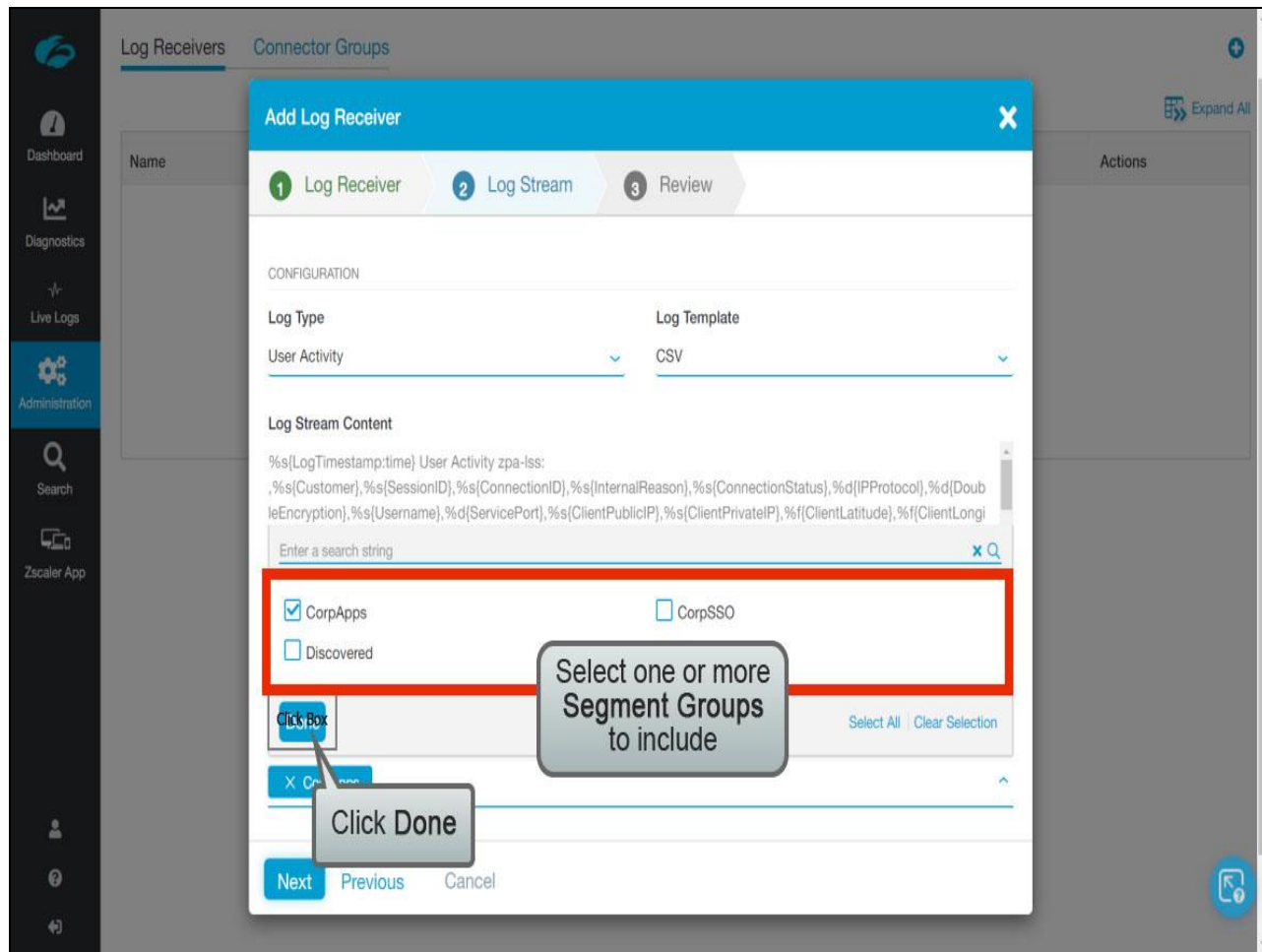
Slide notes

Here you may select one, or more of the defined **Segment Groups**. Having selected the correct groups, click **Done**.

Slide 19 - Slide 19

Slide notes

Slide 20 - Slide 20

Slide notes

If necessary, you may also specify the **Client Types** you wish to include. We include all types by default, to select a subset of them, click in the field, ...

Slide 21 - Slide 21

Slide notes

 ...then select one or more of the available types: **Zscaler App**; **Web Browser**; or even the **ZPA LSS** service itself. Although we will not use this criteria in this example.

Slide 22 - Slide 22

Slide notes

The final option here is to select one or more **Session** states to *exclude*. Click in the field to see what options are available, ...

Slide 23 - Slide 23
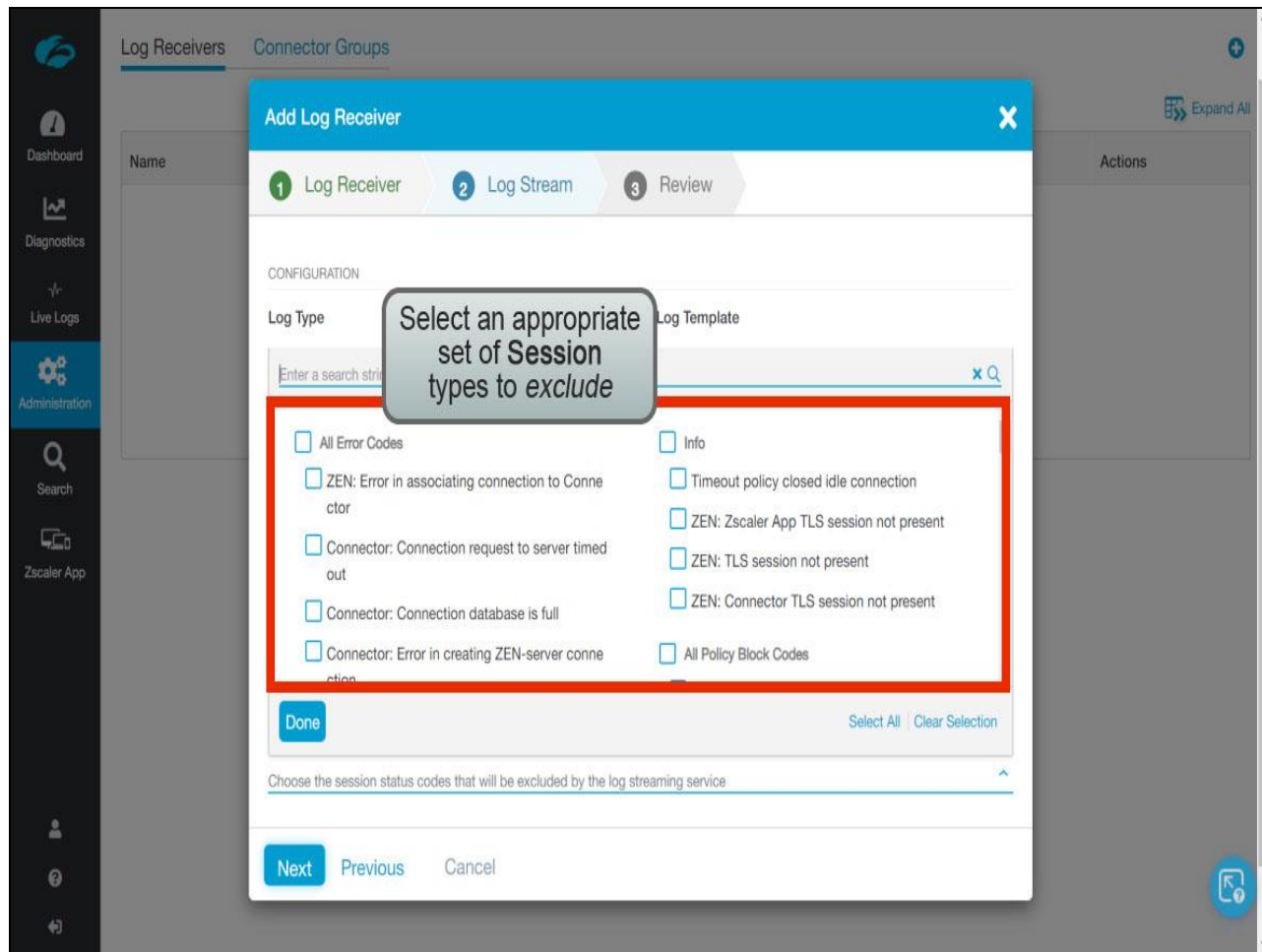
Slide notes

…and select individual, or complete blocks of status code messages.

Slide 24 - Slide 24

Slide notes

Having configured the log stream, click **Next**.

Slide 25 - Slide 25

Slide notes

Review your log receiver configuration, and once you are happy with it, click **Save**.

Slide 26 - Slide 26

Slide notes

Slide 27 - Slide 27

Slide notes

To add another **Log Receiver**, click the **Add Log Receiver** option, ...

Slide 28 - Slide 28

Slide notes

 ...and configure it as required. In this case we will stream **Connector Status** logs to the same Syslog server in Azure. Click **Next** to continue, ...
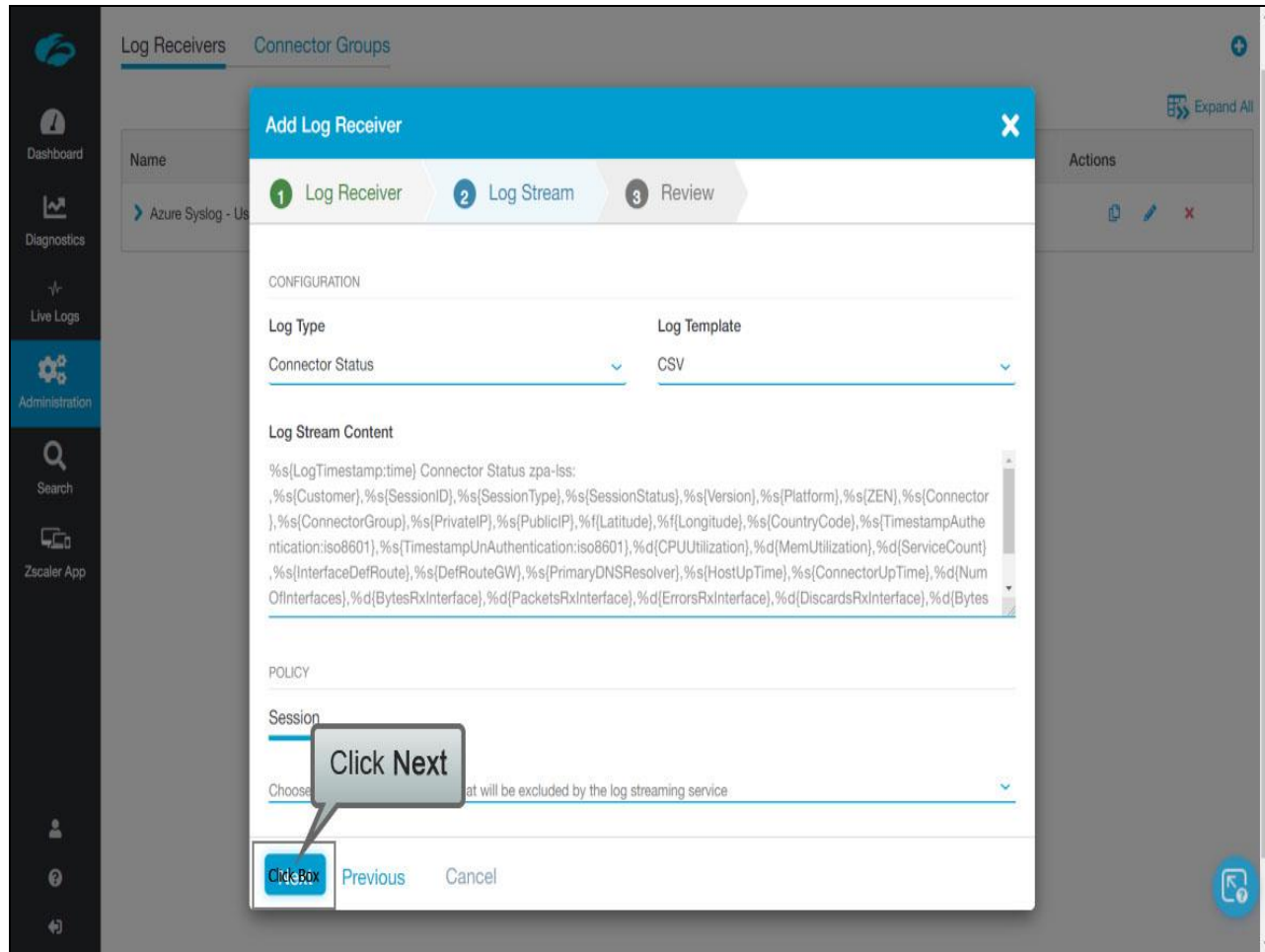
Slide 29 - Slide 29
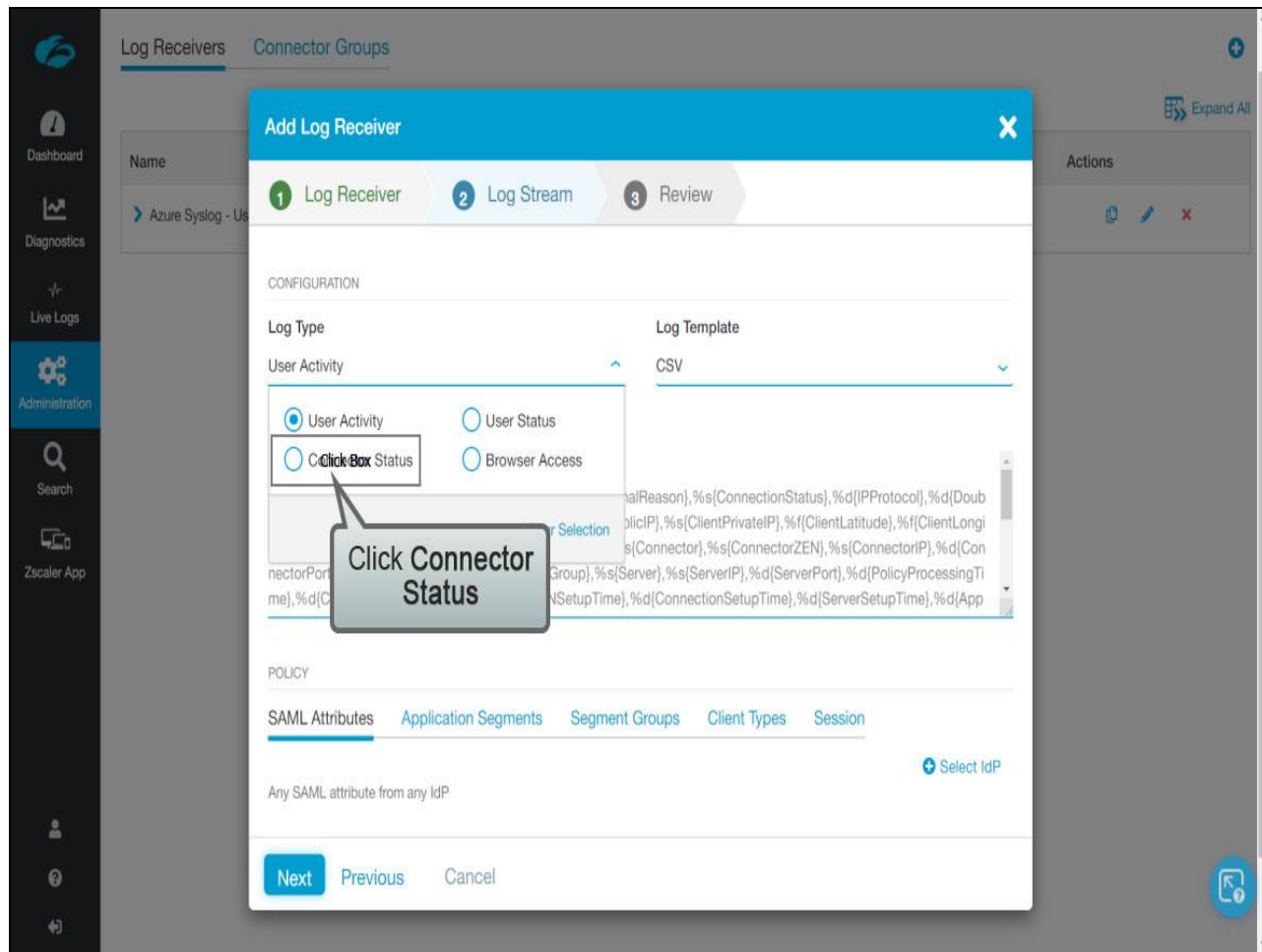
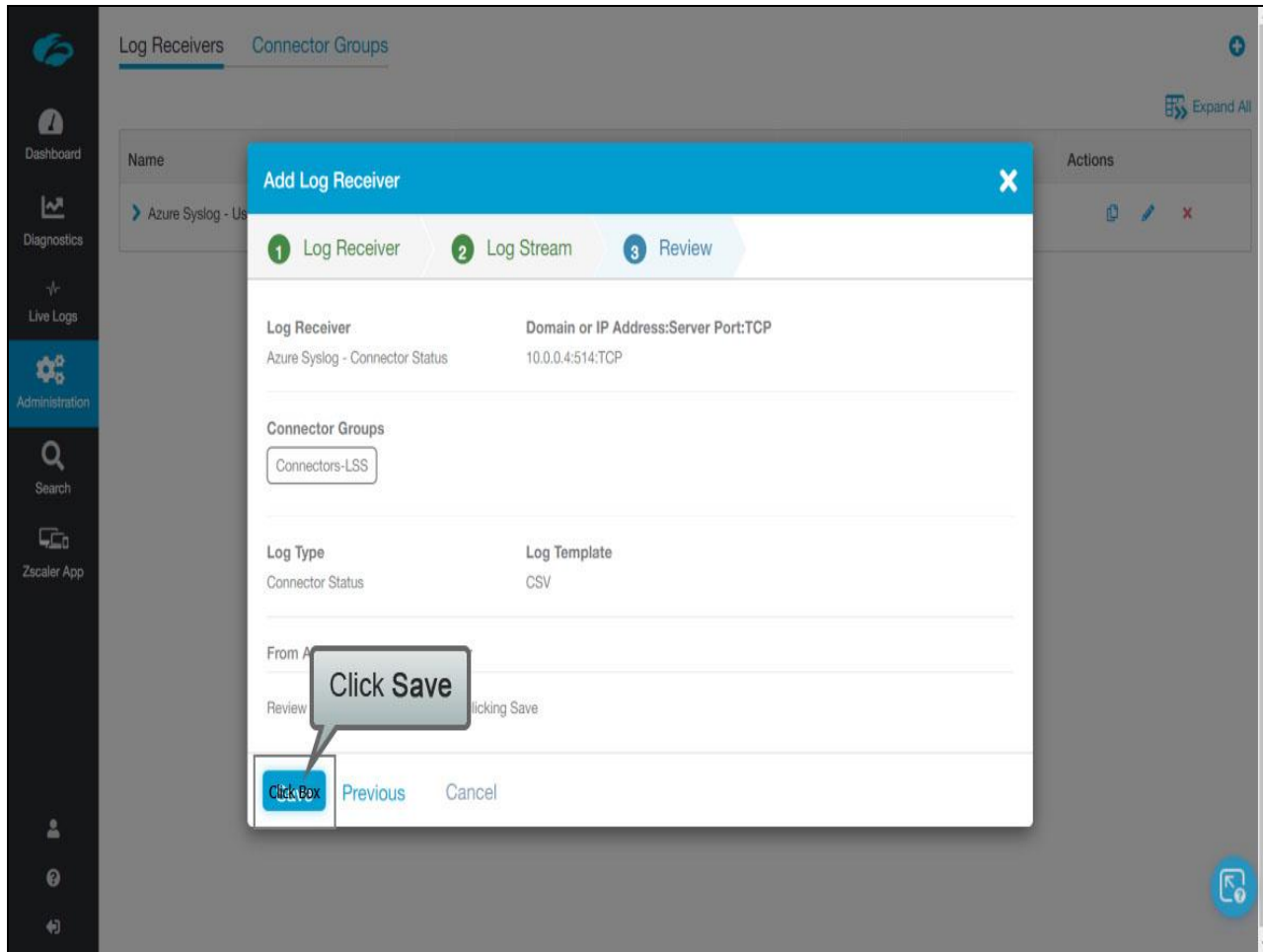**Slide notes**

...click to select **Connector Status**, ...

Slide 30 - Slide 30

Slide notes

 ...click **Next** once more, ...

Slide 31 - Slide 31

Slide notes

...then click **Save**.

Slide 32 - Slide 32

Slide notes

Slide 33 - Slide 33

Slide notes

You have the options to **Copy**, **Edit**, or **Delete** the added log receivers. To view details for any of them, click on the name.

Slide 34 - Slide 34

Slide notes

To review the Connector Groups associated with your log receivers, click **Connector Groups**.

Slide 35 - Slide 35

Slide notes

Here you have the option to **Edit** a group. To view details for any of the listed groups, click on the name.

Slide 36 - Slide 36

Slide notes

Slide 37 - Slide 37
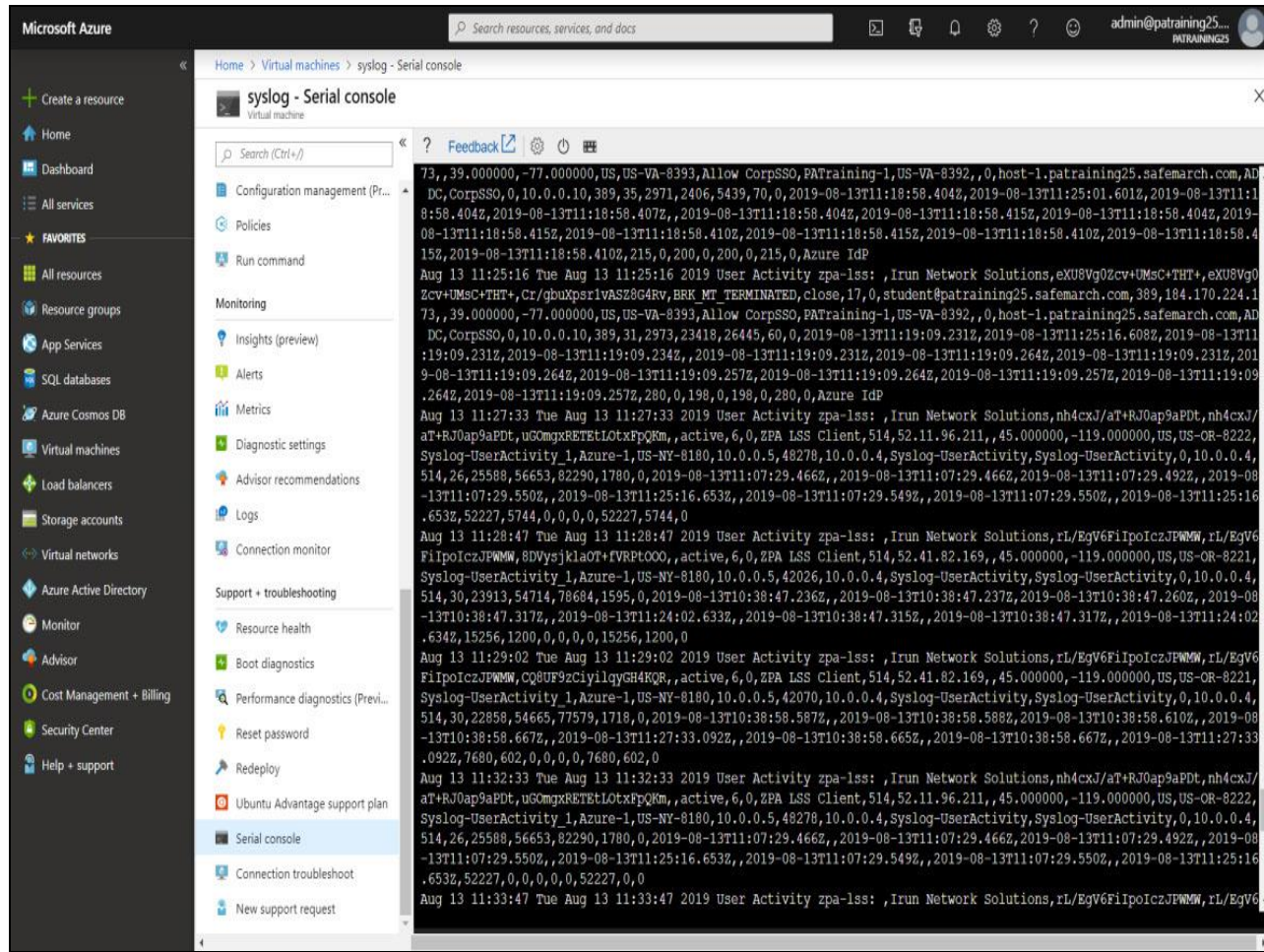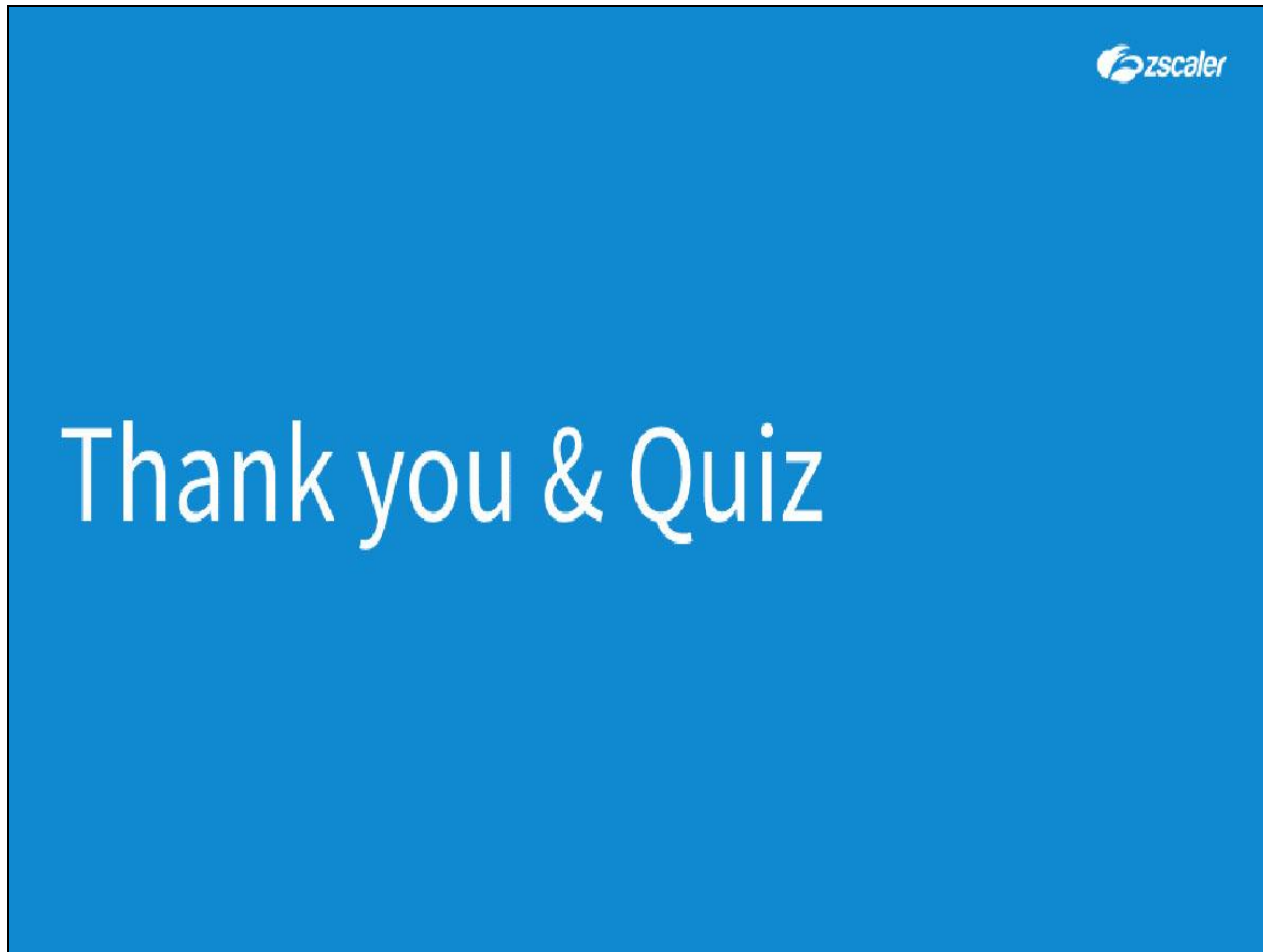

Slide notes

As soon as you save a **Log Receiver** configuration, logs will start to stream to your specified destination.

Slide 38 - Thank you & Quiz

Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

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