

Slide 1 - Zscaler Private Access



Zscaler Private Access

Policy-Based Application Access

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on configuring policy-based application access with ZPA.

Slide 2 - Navigating the eLearning Module

The screenshot shows a video player interface displaying a dashboard titled "Video: ZPA Basic Administration". The dashboard has a header with the Zscaler logo and a date range of "14 Days". It features several cards: "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "AVERAGE POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). Below these are sections for "TOP APPLICATIONS BY BANDWIDTH" and "TOP POLICY BLOCKS". At the bottom of the dashboard, there are tabs for "Access Policy Blocks" and "Timeout Policy Blocks". Overlaid on the video player are several blue callout boxes with white text, pointing to specific controls:

- Previous Slide
- Next Slide
- Play/Pause
- Progress Bar
- Audio On/Off
- Closed Captioning
- Exit

Slide notes

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

Slide 3 - Agenda

Agenda

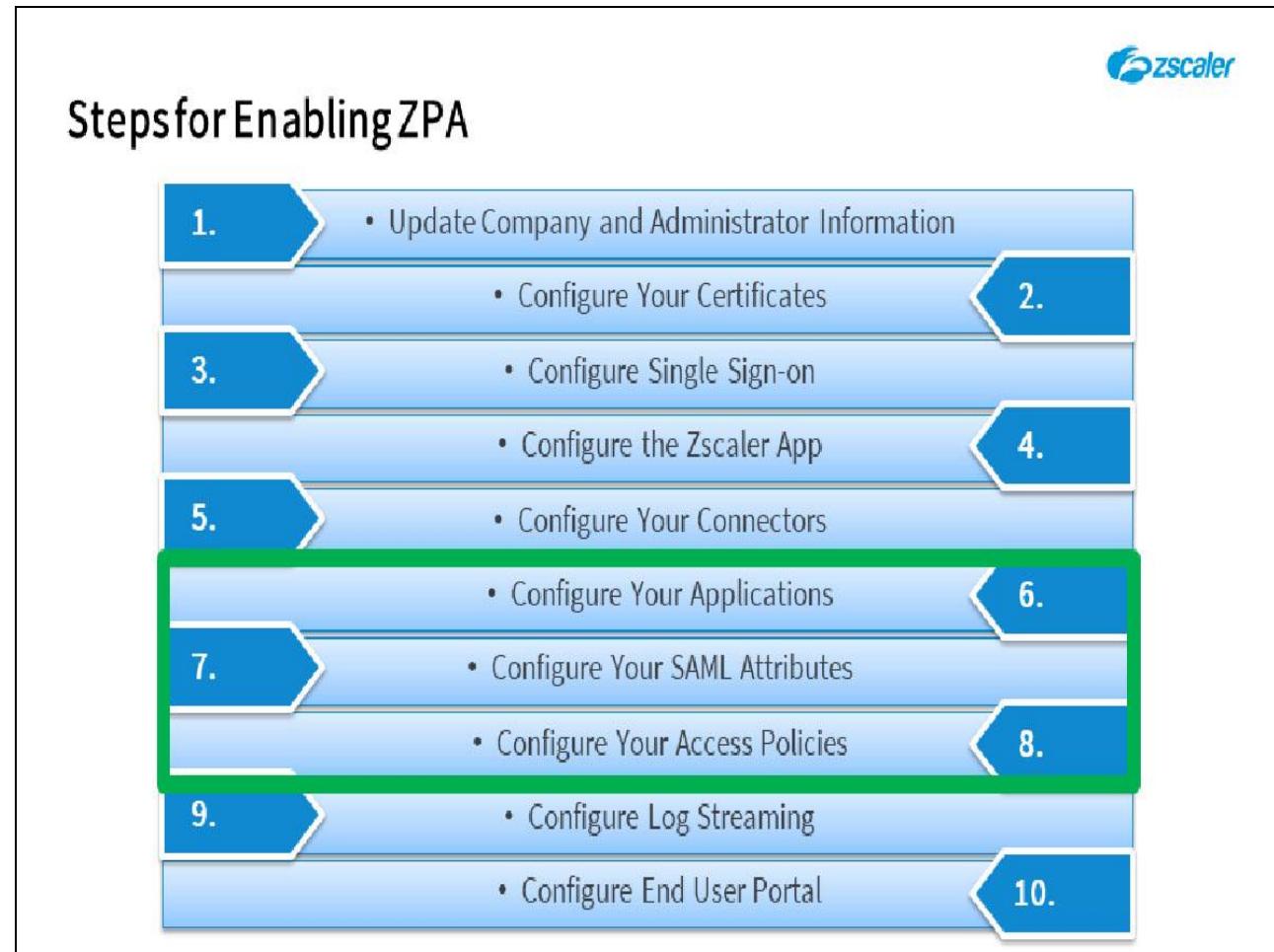


- Steps to Enabling ZPA
 - 6. Configure Applications
 - 7. Configure SAML Attributes
 - 8. Configure Access Policies

Slide notes

In this module, we will look at the steps necessary for enabling policy-based access to your private applications.

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 steps 6 through 8, which relate to adding applications and controlling access to them.

Slide 5 - 7. Configure Your Applications



Slide notes

In the first section, we will look at the configuration of Applications for ZPA.

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

The screenshot shows the Zscaler Admin Portal interface. On the left, there is a navigation sidebar with various menu items: Dashboard, Diagnostics, Live Logs, Administration, Zscaler App, and Settings. The 'Administration' menu is currently selected. Within the 'Administration' menu, the 'APPLICATION MANAGEMENT' section is expanded, showing 'Application Segments' (which is highlighted with a red box and a callout 'Click Application Segments'), 'Segment Groups', and 'Servers'. Below this, other sections like 'AUTHENTICATION', 'CERTIFICATE MANAGEMENT', 'CONNECTOR MANAGEMENT', 'LOG STREAMING SERVICE', 'POLICY MANAGEMENT', and 'SETTINGS' are listed. The main content area has a header '14 Days ▾'. It features three summary cards: 'APPLICATIONS' (green, 0), 'ACCESS POLICY BLOCKS' (orange, 0), and 'SUCCESSFUL TRANSACTIONS' (green, 968). Below these cards is a section titled 'TOP APPLICATIONS BY BANDWIDTH' with a horizontal bar chart. The data in the chart is as follows:

Bandwidth	Application
213.03 MB	server01.safemarch.com
28.50 MB	splunk.safemarch.com
15.11 MB	gitlab.safemarch.com
13.53 MB	crm.safemarch.com
1.80 MB	intranet.safemarch.local
1.31 MB	splunk.tm.zscaler.com
1.06 MB	nav.safemarch.com
510.61 KB	qa.safemarch.com
499.99 KB	safemarch.com
445.81 KB	172.20.0.26

At the bottom of the chart, it says '100% of Total Transactions'. There is also a 'TOP POLICY BLOCKS' section at the very bottom.

Slide notes

In the ZPA Admin Portal, from the **Administration** menu, click **Application Segments** in the **APPLICATION MANAGEMENT** section, ...

Slide 7 - Slide 7

The screenshot shows the 'Application Segments' tab selected in the top navigation bar. The main area displays a table of application segments with columns for Name, Applications, Status, Health Reporting, and Health Checks. A callout box with the text 'Click DNS Search Domains' points to the 'DNS Search Domains' icon in the top right corner of the interface.

Name	Applications	Status	Health Reporting	Health Checks
All Other Services	*.safemarch.com	Green checkmark	On Access	Green checkmark
DC Filesharing and RDP	server01.safemarch.com	Green checkmark	Continuous	Green checkmark
CF CRM Web Application	crm.gf.local	Green checkmark	Continuous	Green checkmark
GF Intranet Web App	intranet.gf.local	Green checkmark	Continuous	Green checkmark
GF QA Web App	qa.gf.local	Green checkmark	Continuous	Green checkmark
CF Research SSH App	research.gf.local	Green checkmark	Continuous	Green checkmark
IRC	irc.safemarch.com	Green checkmark	Continuous	Green checkmark
Microsoft Dynamics NAV	nav.safemarch.com	Green checkmark	On Access	Green checkmark
QA Application	qa.safemarch.com	Green checkmark	Continuous	Green checkmark
Research Server (IP) SSH	172.20.0.15	Green checkmark	On Access	Green checkmark
Safemarch GitLab	gitlab.safemarch.com	Green checkmark	Continuous	Green checkmark

Slide notes

...and the list of the currently defined **Application Segments** is shown.

If you would like your users to be able to access applications using just a short name rather than FQDN, you will need to add the relevant search domains that can be used to form a FQDN. To add search domains, click the **DNS Search Domains** icon at top right, ...

Slide 8 - Slide 8

The screenshot shows the Zscaler App interface with the 'Application Segments' tab selected. A modal dialog box titled 'DNS Search Domains' is open, prompting the user to enter a domain name: 'patraining.safemarch.com'. Below the input field is a checkbox labeled 'Domain Validation in Zscaler App'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. A callout bubble with the text 'Click Add More' points to the 'Save' button. The background list of search domains includes entries like 'All Other Services', 'DC Filesharing', 'GF CRM Web App', 'GF Intranet Web App', 'GF QA Web App', 'GF Research SSH App', 'IRC', 'Microsoft Dynamics NAV', 'QA Application', 'Research Server IP SSH', and 'Safemarch GitLab'. Each entry has a status icon, a name, a URL, a status indicator, and a 'Continuous' or 'On Access' access type. The 'Actions' column contains edit and delete icons.

Slide notes

...and the list of existing search domains will be shown. To add another, click **Add More**, ...

Slide 9 - Slide 9

The screenshot shows the Adobe Captivate interface with the 'Application Segments' tab selected. A modal dialog box titled 'DNS Search Domains' is open, listing two domains: 'patraining.safemarch.com' and 'safemarch.com'. Below the list are two checkboxes: 'Domain Validation in Zscaler App' and 'Domain Validation in Zscaler App'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. A callout bubble with the text 'Click Add More' points to a blue '+' icon located at the bottom right of the dialog. The background shows a list of other application segments, each with a status indicator (green checkmark or red X) and an edit/refresh icon.

Slide notes

...and specify the new Search Domain. Click **Add More** to add a new Search Domain.

Slide 10 - Slide 10

The screenshot shows the Zscaler App interface with the 'DNS Search Domains' configuration screen open. The left sidebar includes icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for Application Segments, Browser Access, Segment Groups, and a search bar. The 'DNS Search Domains' section lists several domains: patraining.safemarch.com, safemarch.com, engineering.safemarch.com, research.gf.local, irc.safemarch.com, nav.safemarch.com, qa.safemarch.com, 172.20.0.15, and gitlab.safemarch.com. For each domain, there is a checkbox labeled 'Domain Validation in Zscaler App'. A tooltip 'Click to enable Domain Validation in Zscaler App' points to one of these checkboxes. Another tooltip 'Domain Validation in Zscaler App option for each Search Domain added' points to the same checkbox. A 'Save' button is visible at the bottom left of the dialog.

Slide notes

Some Service Providers employ DNS optimization techniques which essentially hijack DNS responses, this can prevent the Zscaler App from correctly resolving the synthetic IP address for a ZPA application, making it apparently unreachable. Enabling the **Domain Validation in Zscaler App** option for each of the **Search Domains**, ensures that the Zscaler App will get first go at evaluating these domains and will always be able to resolve and reach ZPA applications on them.

Click to enable this option for all or a subset of your DNS Search Domains.

Slide 11 - Slide 11

The screenshot shows the 'DNS Search Domains' configuration screen. It lists several domains with validation checkboxes. A red box highlights the 'Add More' button. A callout bubble says 'Remove a Search Domain or Add More as required'. A blue box highlights the 'Click Save' button.

Name	Validation	Type	Continuous	Action
patraining.safemarch.com	<input checked="" type="checkbox"/>	Domain Validation in Zscaler App		
safemarch.com	<input checked="" type="checkbox"/>	Domain Validation in Zscaler App		
engineering.safemarch.com	<input checked="" type="checkbox"/>	Domain Validation in Zscaler App		
GF Research SSH App				
IRC				
Microsoft Dynamics NAV				
QA Application				
Research Server IP SSH				
Safemarch GitLab				

Slide notes

Having added Search Domains, you can subsequently remove them if necessary. Once the configuration is correct, click Save.

Slide 12 - Slide 12

The screenshot shows the Zscaler Application Firewall interface under the 'Application Segments' tab. The left sidebar includes icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help.

The main area displays a table of application segments:

Name	Applications	Status	Health Reporting	Health Check	Actions
All Other Services	*.safemarch.com	Green checkmark	On Access	Green checkmark	
DC Filesharing and RDP	server01.safemarch.com	Green checkmark	Continuous	Green checkmark	
GF CRM Web Application	crm.gf.local	Green checkmark	Continuous	Green checkmark	
GF Intranet Web App	intranet.gf.local	Green checkmark	Continuous	Green checkmark	
GF QA Web App	qa.gf.local	Green checkmark	Continuous	Green checkmark	
GF Research SSH App	research.gf.local	Green checkmark	Continuous	Green checkmark	
IRC	irc.safemarch.com	Green checkmark	Continuous	Green checkmark	
Microsoft Dynamics NAV	nav.safemarch.com	Green checkmark	On Access	Green checkmark	
QA Application	qa.safemarch.com	Green checkmark	Continuous	Green checkmark	
Research Server IP SSH	172.20.0.15	Green checkmark	On Access	Green checkmark	
Safemarch GitLab	gitlab.safemarch.com	Green checkmark	Continuous	Green checkmark	

A search bar at the top right contains 'search by name, domain or IP address' with a magnifying glass icon. A 'DNS' button and a '+' button are also present. A green banner at the bottom right says 'DNS search domains saved' with a circular refresh icon.

Slide notes

Slide 13 - Slide 13

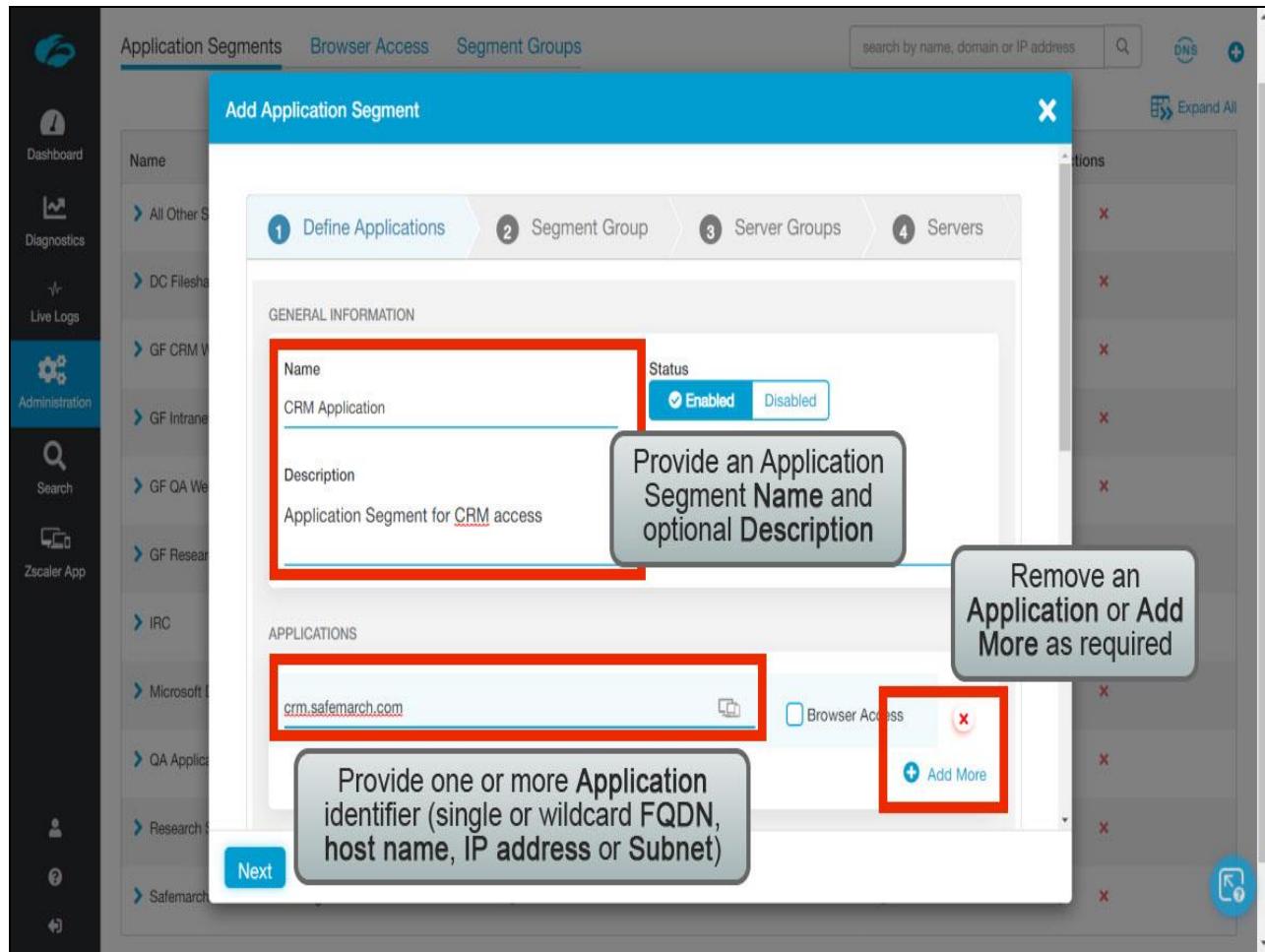
The screenshot shows the Adobe Application Insights dashboard. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main area has tabs for Application Segments (selected), Browser Access, and Segment Groups. A search bar and a 'Click Box' button are at the top right. The main content is a table of application segments:

Name	Applications	Status	Health Reporting	Health Checks	Action	Action
All Other Services	*.safemarch.com	Green checkmark	On Access	Green checkmark		
DC Filesharing and RDP	server01.safemarch.com	Green checkmark	Continuous	Green checkmark		
GF CRM Web Application	crm.gf.local	Green checkmark	Continuous	Green checkmark		
GF Intranet Web App	intranet.gf.local	Green checkmark	Continuous	Green checkmark		
GF QA Web App	qa.gf.local	Green checkmark	Continuous	Green checkmark		
GF Research SSH App	research.gf.local	Green checkmark	Continuous	Green checkmark		
IRC	irc.safemarch.com	Green checkmark	Continuous	Green checkmark		
Microsoft Dynamics NAV	nav.safemarch.com	Green checkmark	On Access	Green checkmark		
QA Application	qa.safemarch.com	Green checkmark	Continuous	Green checkmark		
Research Server IP SSH	172.20.0.15	Green checkmark	On Access	Green checkmark		
Safemarch GitLab	gitlab.safemarch.com	Green checkmark	Continuous	Green checkmark		

Slide notes

To open the wizard to create a new **Application Segment**, click the + icon at top right.

Slide 14 - Slide 14



Slide notes

Give the new Application Segment a **Name** and optionally add a **Description**. Add one or more **APPLICATIONS** by specifying the FQDN or IP address. Note that you may add multiple entries here, whether FQDNs or IPs, just use the **Add More** option to add additional names or addresses.

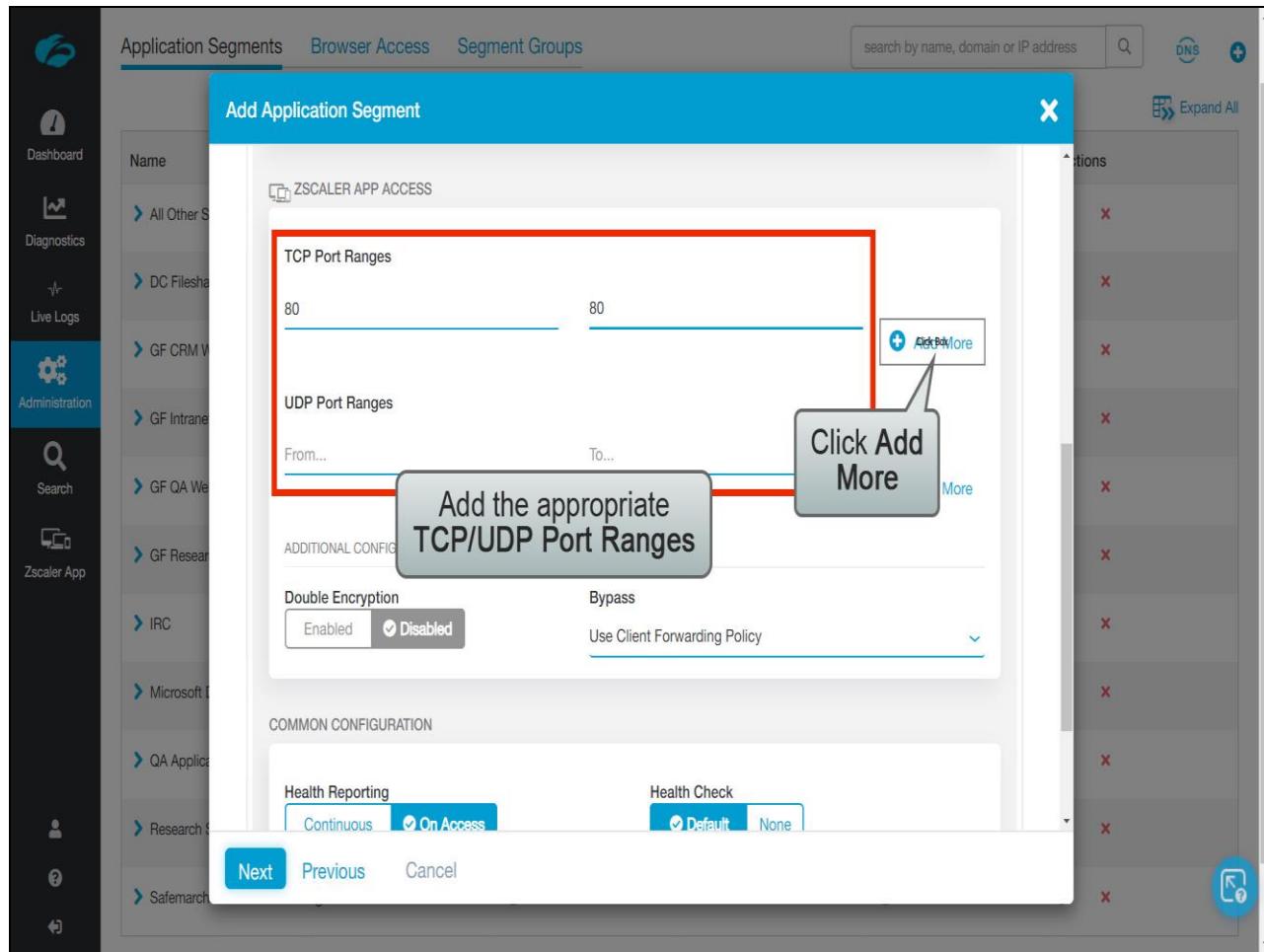
Slide 15 - Slide 15

The screenshot shows the Zscaler Admin interface with a sidebar containing various navigation links like Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area is titled 'Application Segments' and shows a search bar and a 'DNS' button. A modal window titled 'Add Application Segment' is open, divided into four steps: 1. Define Applications, 2. Segment Group, 3. Server Groups, and 4. Servers. Step 1 is active, showing 'GENERAL INFORMATION' with a 'Name' field containing 'CRM Application', a 'Status' dropdown set to 'Enabled', and a 'Description' field with the text 'Application Segment for CRM access'. Below this is the 'APPLICATIONS' section, which contains a single entry 'crm.safemarch.com' and a checkbox labeled 'Browser Access'. A 'Next' button is at the bottom left, and 'Previous' and 'Cancel' buttons are at the bottom right. A callout bubble with the text 'Scroll down...' points to the bottom of the application list.

Slide notes

Scroll down...

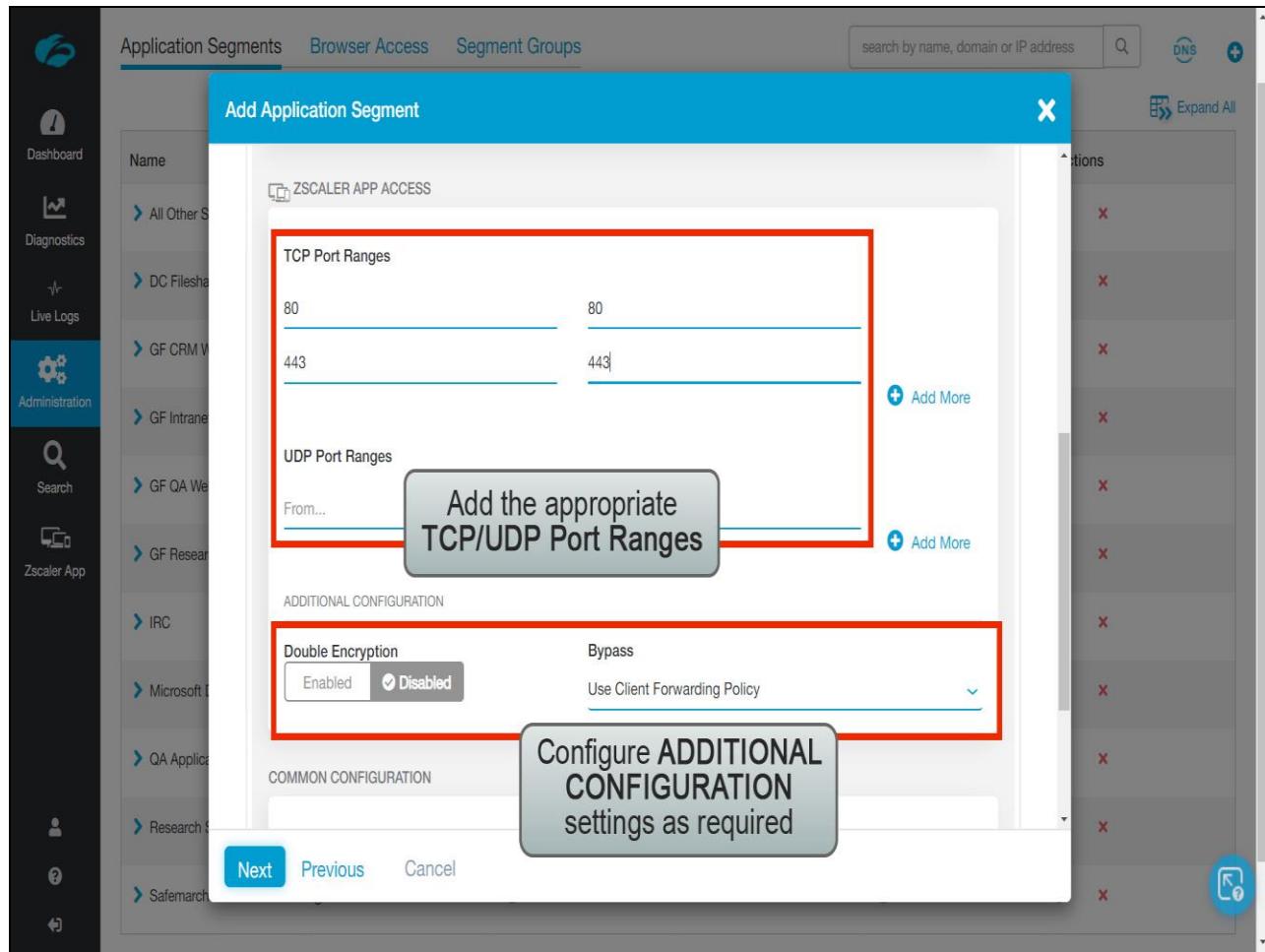
Slide 16 - Slide 16



Slide notes

...and add the appropriate **TCP Port Ranges** and if necessary, the valid **UDP Port Ranges**. If you need to add an additional port range, click **Add More**.

Slide 17 - Slide 17



Slide notes

In this instance we will add a Web-based CRM application accessible on TCP ports 80 and 443 only.

If necessary, enable the **Double Encryption** option and configure the **Bypass** option (**Use Client Forwarding Policy**, **Always** or **On Corporate Network**). Note, if the Client Forwarding Policy is left at default settings, then the **Use Client Forwarding Policy** equates to **Never**.

Slide 18 - Slide 18

The screenshot shows the 'Add Application Segment' dialog box over a background of the Zscaler dashboard. The dialog is titled 'Add Application Segment' and contains fields for defining port ranges and configuration options.

Port Ranges:

- TCP Port Ranges:** From 80 to 80
- UDP Port Ranges:** From... To... (fields are empty)

Additional Configuration:

- Double Encryption:** Enabled (radio button selected)
- Bypass:** Use Client Forwarding Policy

Common Configuration: (A large text input field is present but empty.)

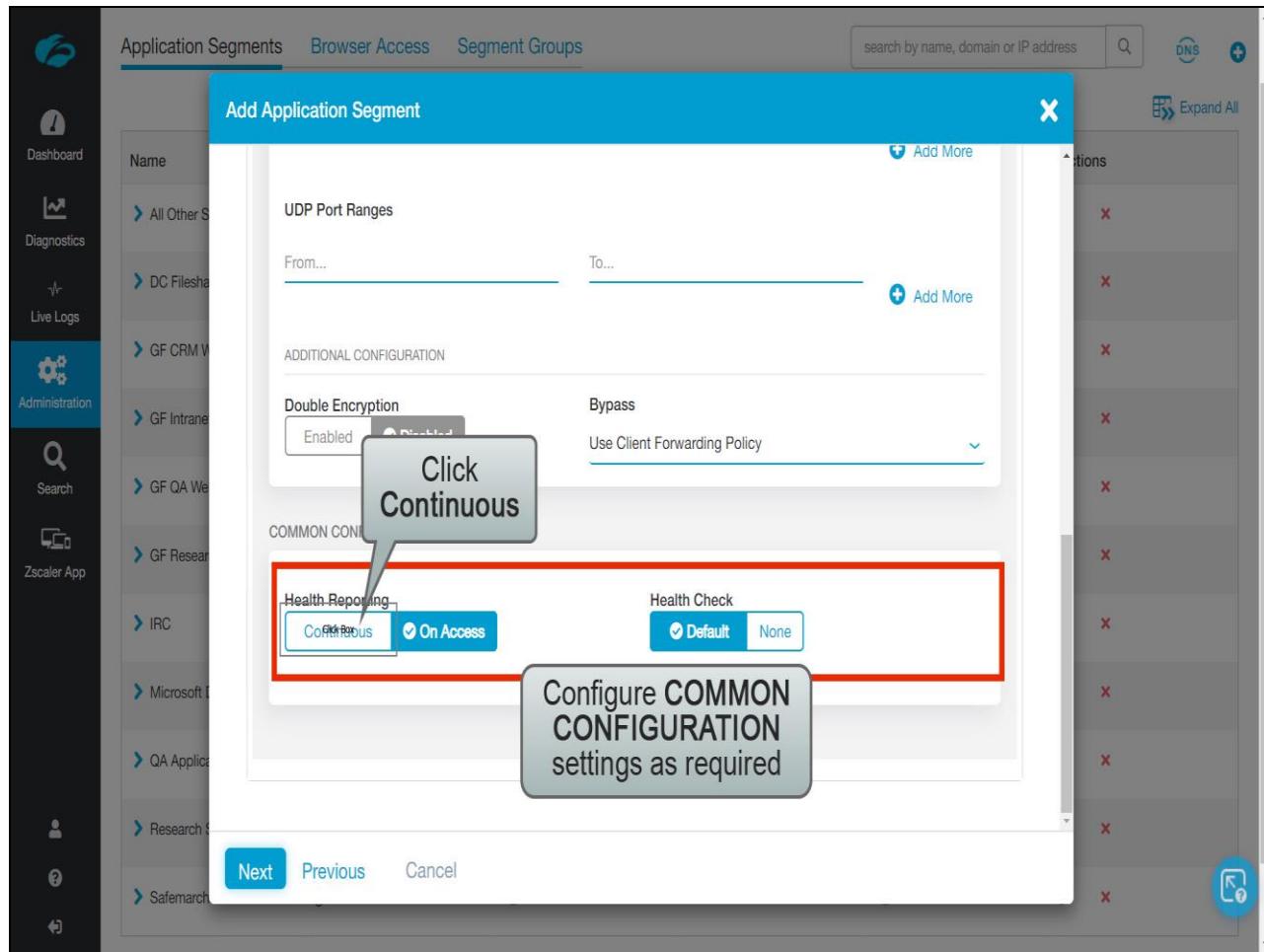
Buttons at the bottom: Next (highlighted in blue), Previous, Cancel.

A callout bubble with the text "Scroll down..." points to the bottom right corner of the dialog box, where there is a scroll-down arrow icon.

Slide notes

Scroll down...

Slide 19 - Slide 19



Slide notes

...and configure the **COMMON CONFIGURATION** settings: Set the **Health Reporting** option to **Continuous** or **On Access**; and the **Health Check** option to **Default** or **None**. In this case we want continuous health monitoring for this application, so click **Continuous**.

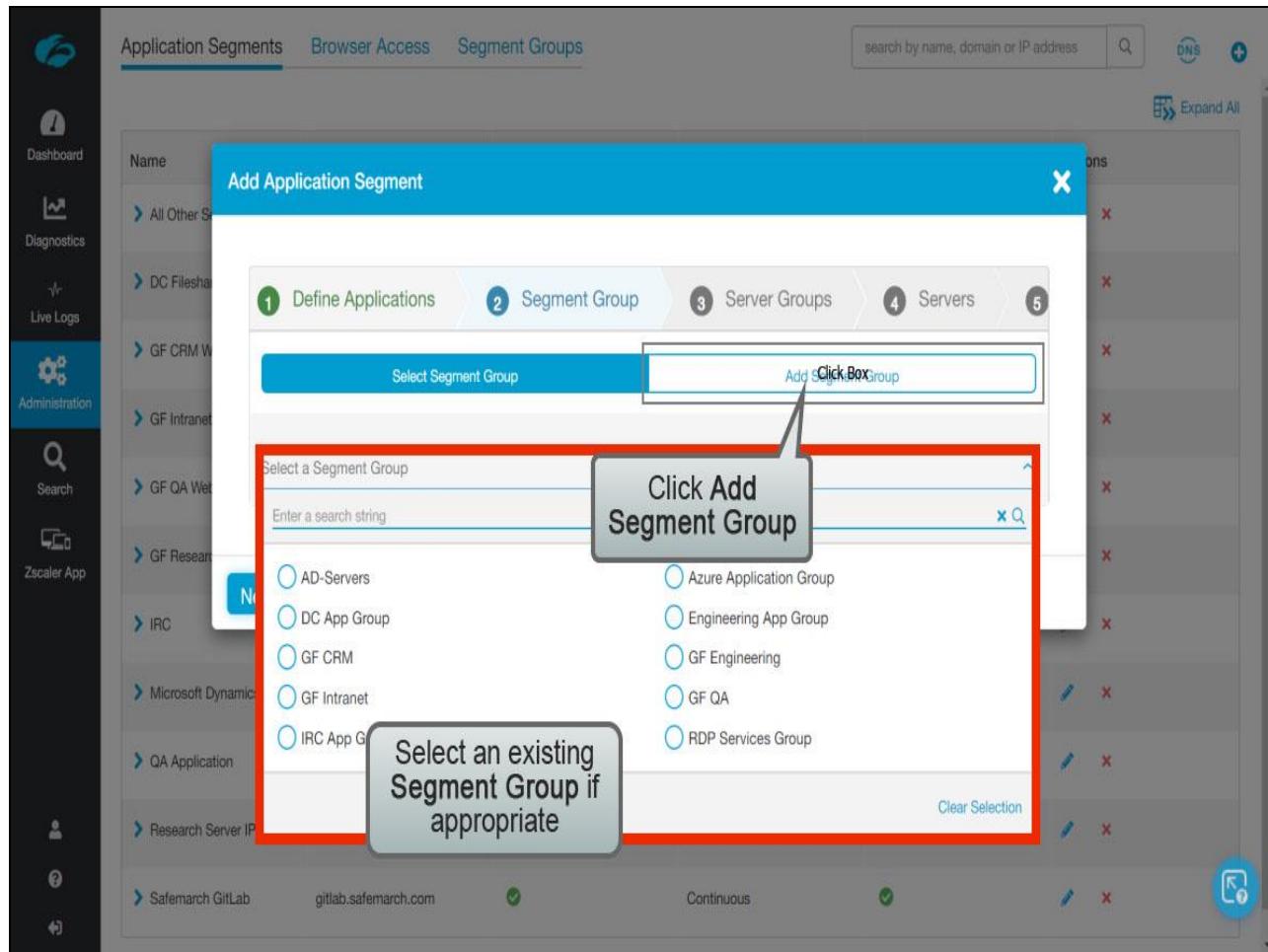
Slide 20 - Slide 20

The screenshot shows the Zscaler Application Segments configuration interface. On the left, there's a sidebar with various navigation options like Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and User Management. The main area is titled "Add Application Segment". It has tabs for "Application Segments", "Browser Access", and "Segment Groups". A search bar at the top right allows searching by name, domain or IP address. Below the tabs, there's a table with several rows, each with an "X" icon to delete. The main configuration area is titled "UDP Port Ranges" and includes fields for "From..." and "To...". There's also an "Add More" button. Under "ADDITIONAL CONFIGURATION", there are sections for "Double Encryption" (with "Enabled" and "Disabled" options) and "Bypass" (with "Use Client Forwarding Policy"). The "COMMON CONFIGURATION" section is highlighted with a red box and contains "Health Reporting" (with "Continuous" and "On Access" options) and "Health Check" (with "Default" and "None" options). A callout bubble points to the "On Access" and "Default" buttons with the text "Configure COMMON CONFIGURATION settings as required". At the bottom, there are "Next", "Previous", and "Cancel" buttons. A "Click Next" callout points to the "Next" button.

Slide notes

The **Health Check** option is set to **Default** already, so to continue with the wizard click **Next**.

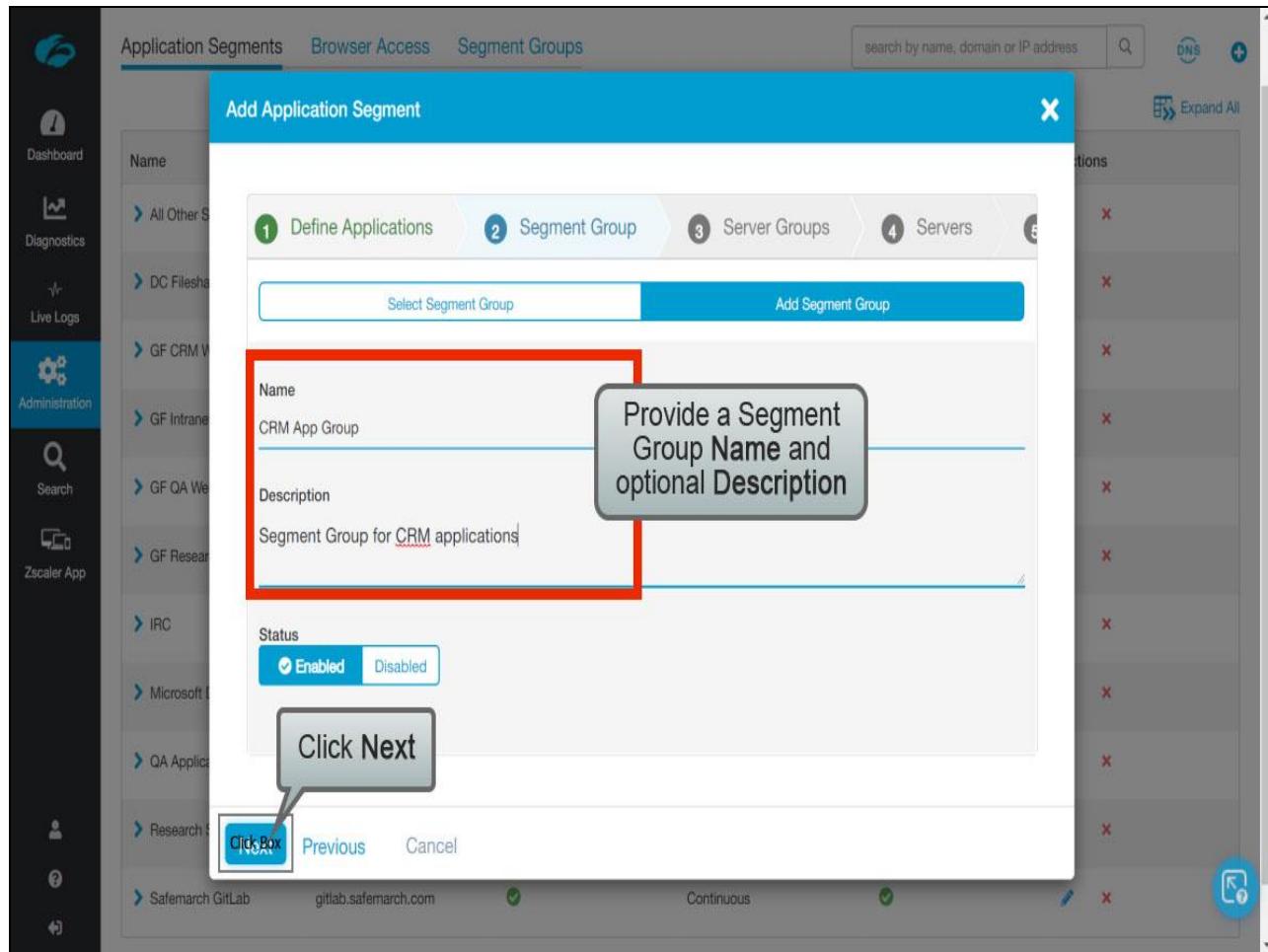
Slide 21 - Slide 21



Slide notes

If the correct Segment Group for this Application Segment already exists on the system, you can select it here. Alternatively, to create a new group, click **Add Segment Group**.

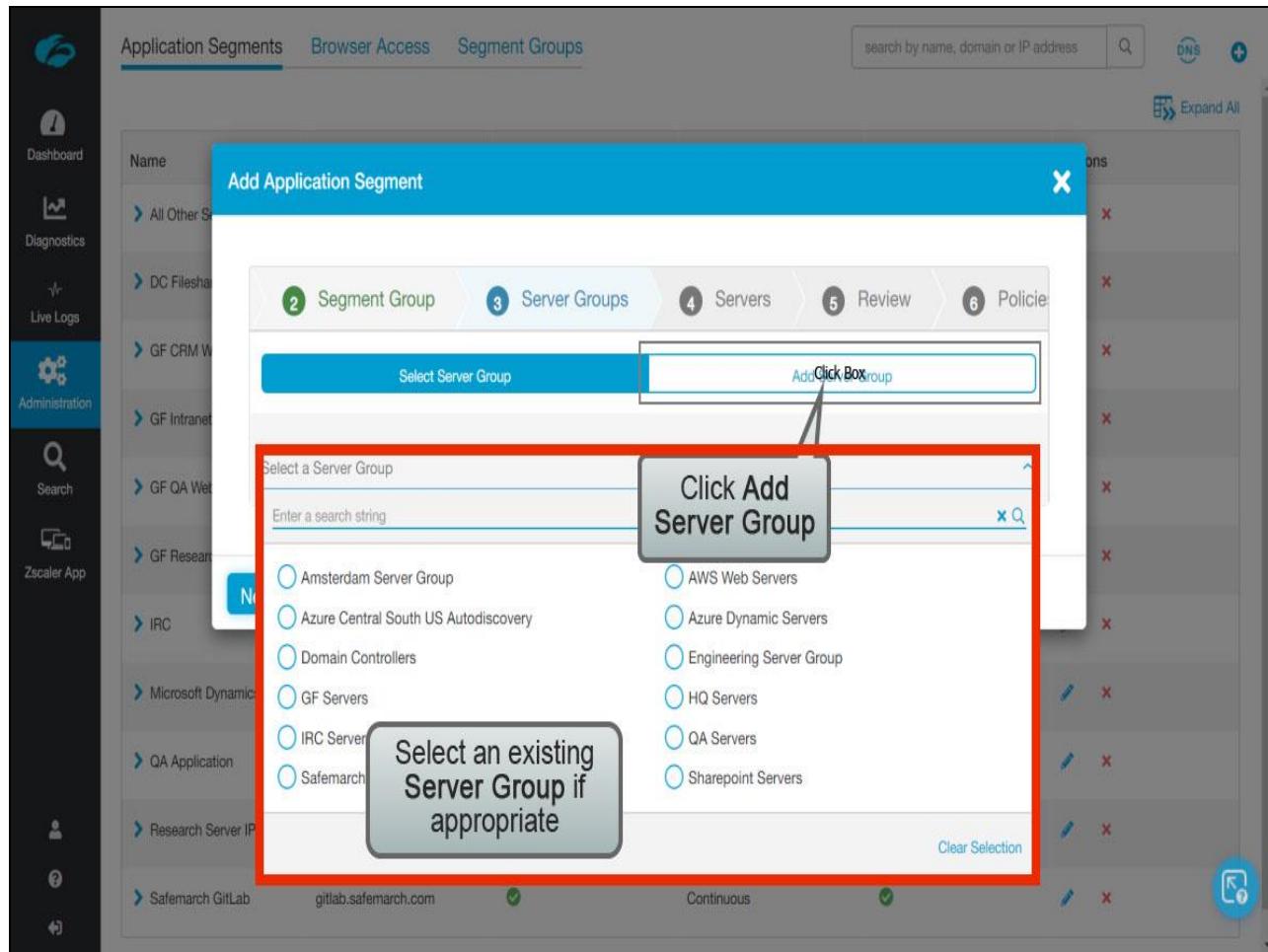
Slide 22 - Slide 22



Slide notes

Give the new Segment Group a **Name**, and optionally a **Description**, then click **Next** to continue with the wizard.

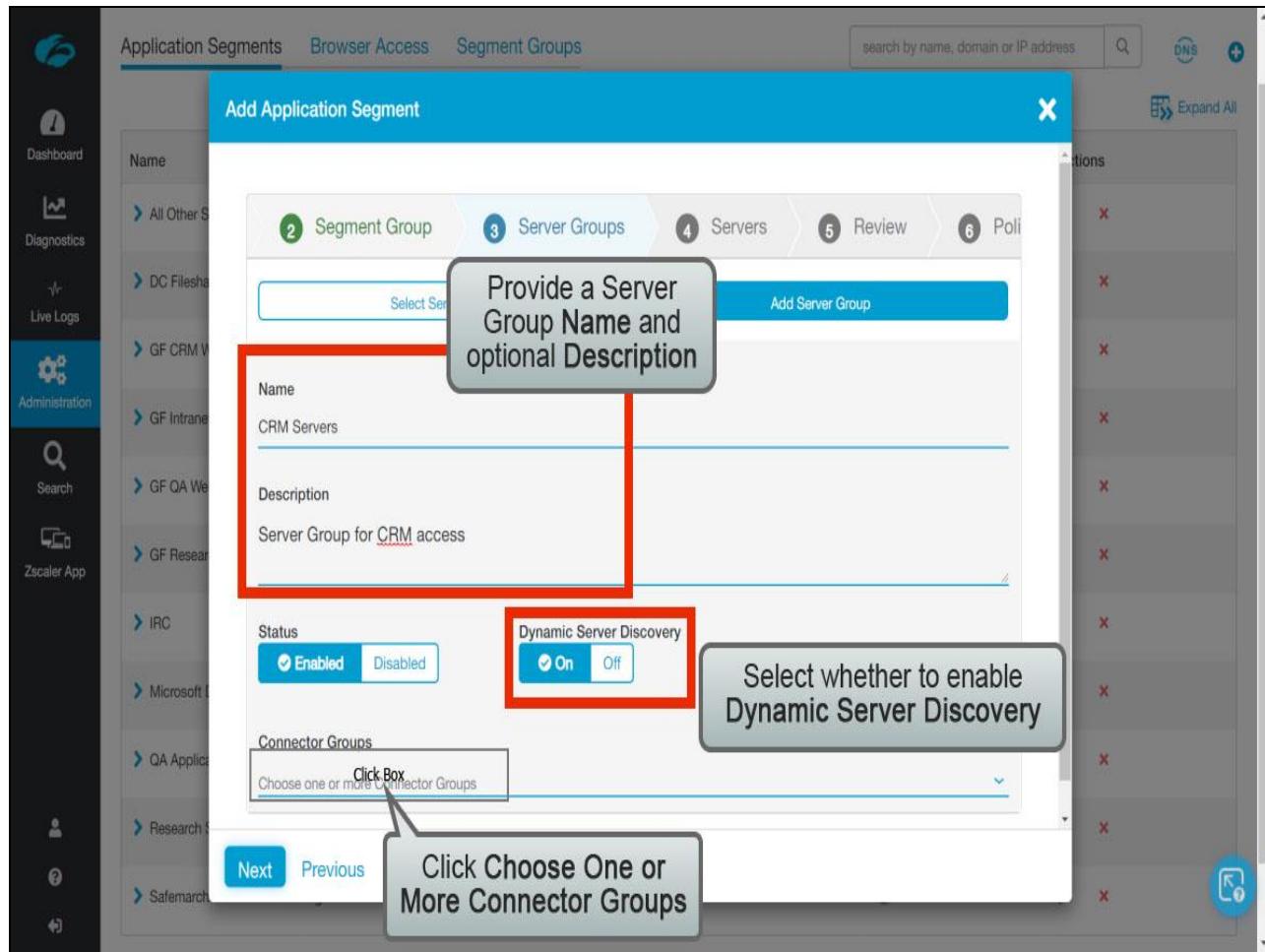
Slide 23 - Slide 23



Slide notes

If the correct Server Group for this Application Segment already exists on the system, you can select it here. Alternatively, to create a new group, click **Add Server Group**.

Slide 24 - Slide 24

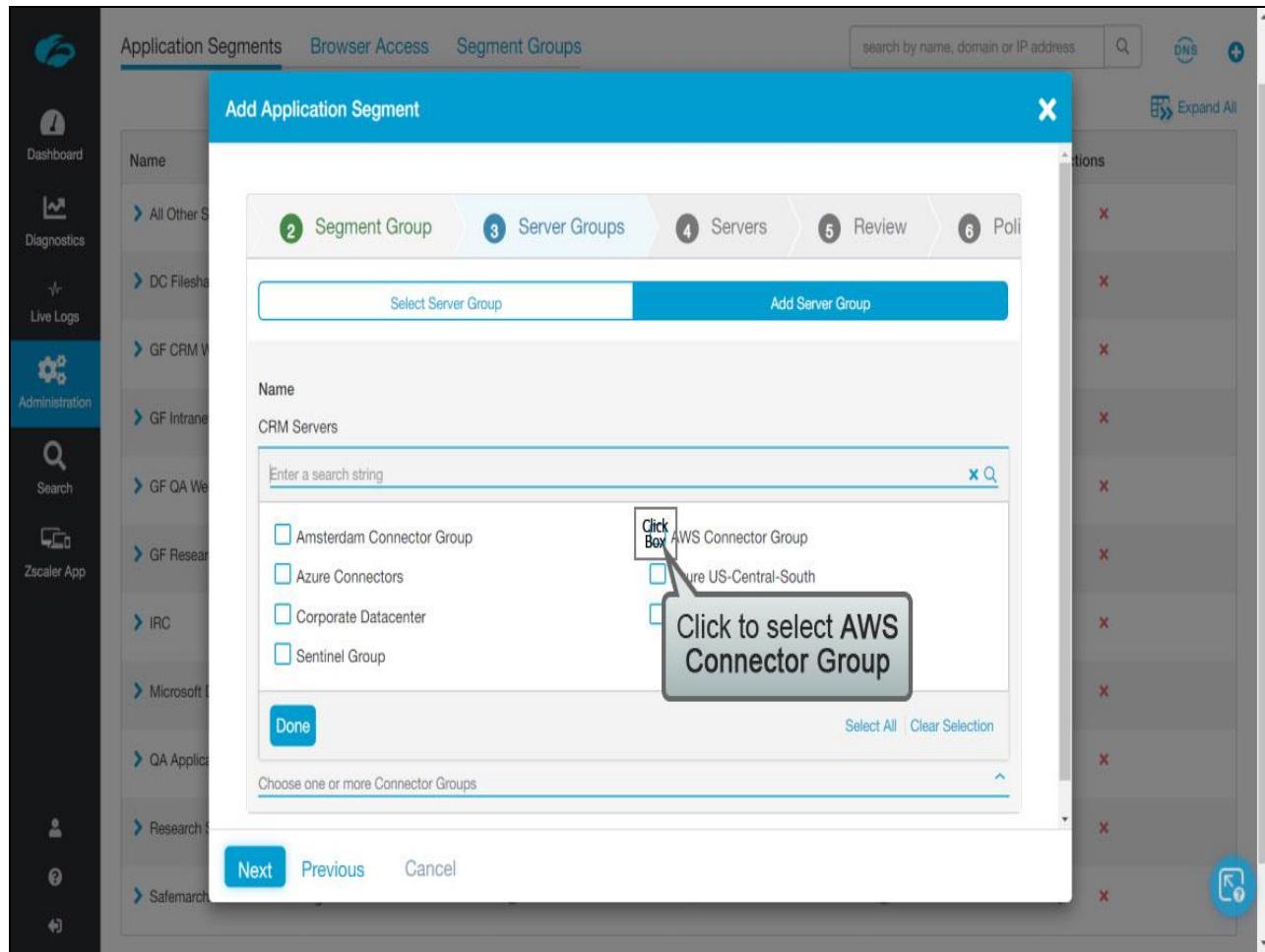


Slide notes

Give the new Server Group a **Name** and optionally a **Description**, then select whether or not to enable **Dynamic Server Discovery** (this is recommended and is enabled by default). Note that if **Dynamic Server Discovery** is disabled, an extra step is added to the wizard for you to add details of the Server hosting the application(s).

Then to match the new Server Group to one or more set of Connectors, click **Choose One or More Connector Groups**.

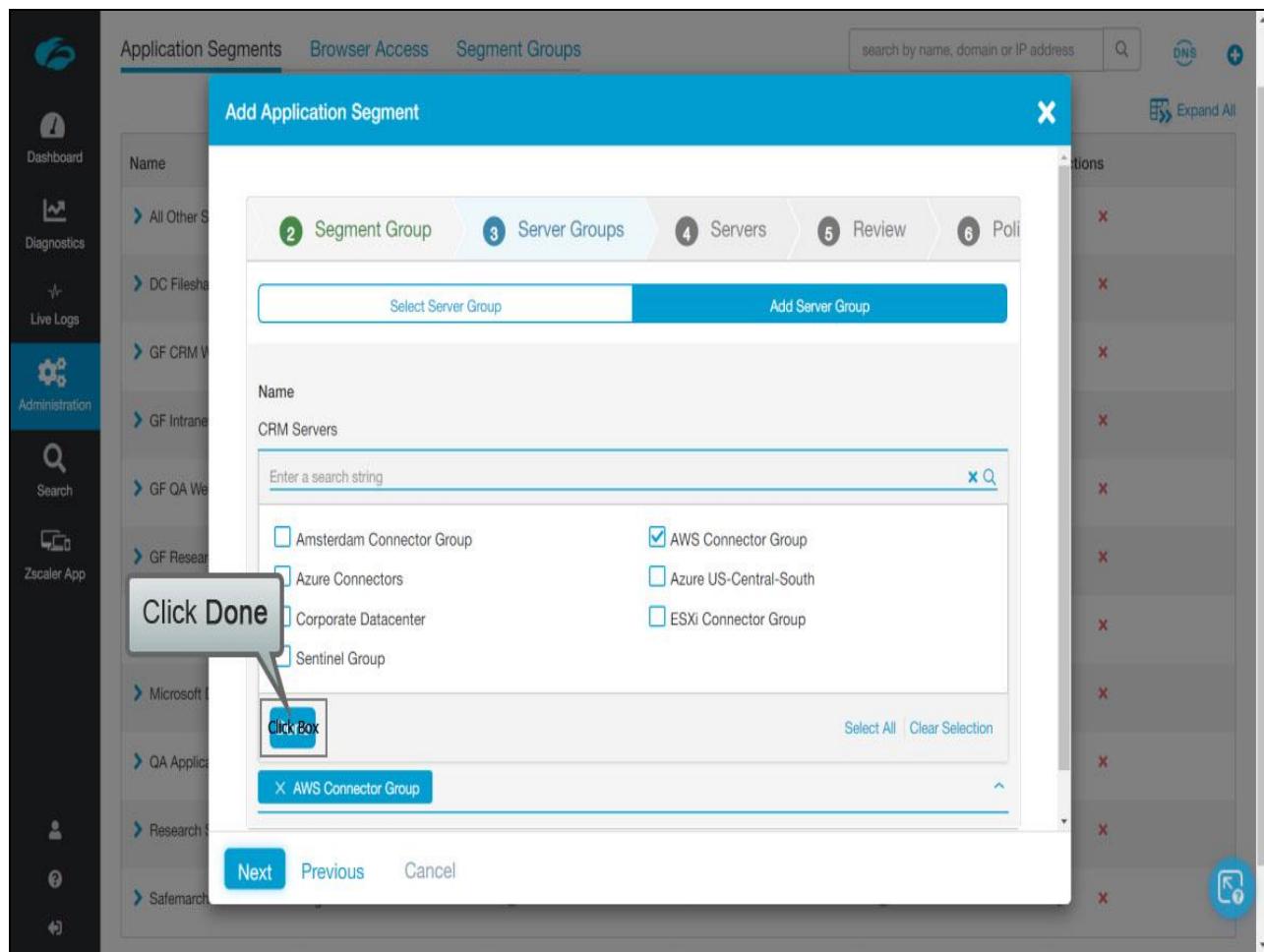
Slide 25 - Slide 25



Slide notes

Select the appropriate Connector Groups to match to this Server group, the Applications listed in this Application Segment will be reachable by any Connector that is a member of one of the Connector Groups that you select here. In this case we will add just the **AWS Connector Group**, ...

Slide 26 - Slide 26



Slide notes

...and click **Done**.

Slide 27 - Slide 27

The screenshot shows the Zscaler interface with the 'Add Application Segment' wizard open. The wizard has six steps: 2 Segment Group, 3 Server Groups, 4 Servers, 5 Review, and 6 Policy. Step 2 is active. The 'Name' field contains 'CRM Servers'. The 'Description' field contains 'Server Group for CRM access'. Under 'Status', 'Enabled' is selected. Under 'Dynamic Server Discovery', 'On' is selected. In the 'Connector Groups' section, 'AWS Connector Group' is listed. At the bottom, there are 'Previous' and 'Next' buttons, with 'Next' being highlighted. A callout box with the text 'Click Next' points to the 'Next' button.

Slide notes

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

Slide 28 - Slide 28

Application Segments Browser Access Segment Groups

search by name, domain or IP address

Add Application Segment

Applications 2 Segment Group 3 Server Groups 4 Review 5 Policies

Application Segment	Application Segment Status
CRM Application	Enabled

Segment Group	Segment Group Status
CRM App Group	Enabled

Server Group	Server Group Status
CRM Servers	Enabled

Servers	
AWS Connector Group	

Click Save

Click Box

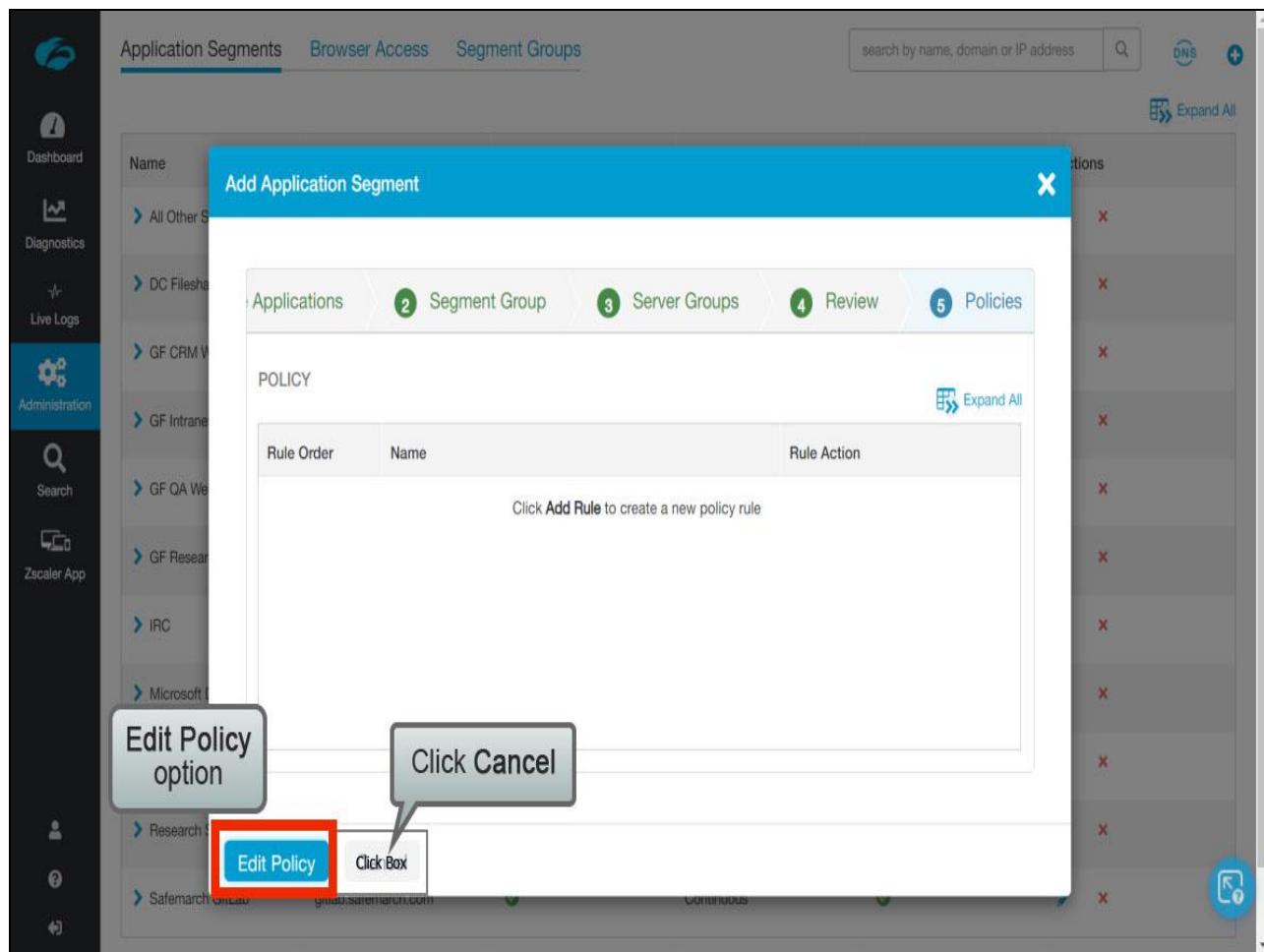
Previous Cancel

gitlab.safemarch.com	Continuous
✓	✓

Slide notes

Verify that all settings are correct, and if so click **Save** to add the new Application Segment (and if necessary the new Segment Group, Server, and Server Group).

Slide 29 - Slide 29



Slide notes

Once the Application Segment has been added you are given the option to **Edit Policy** for it, to properly control access to the new Application(s). To complete the creation of the application without configuring Policy click **Cancel**.

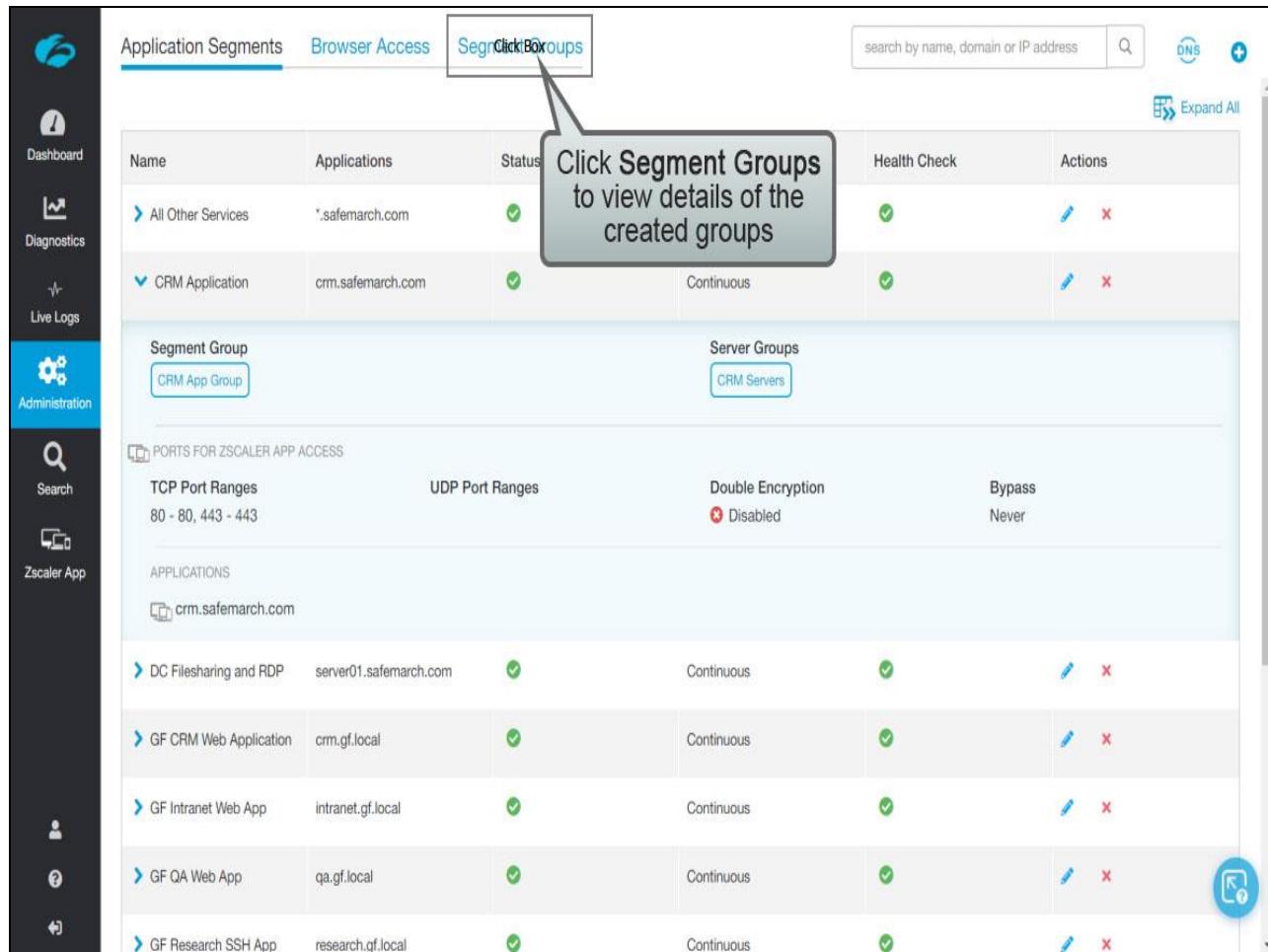
Slide 30 - Slide 30

Name	Applications	Status	Health Reporting	Health Check	Actions
All Other Services	*.safemarch.com	✓	On Access	✓	
CRM ClickBox	crm.safemarch.com	✓	Continuous	✓	
DC Fileshare and RDP	server01.safemarch.com	✓	Continuous	✓	
GF CRM		✓	Continuous	✓	
GF Intranet		✓	Continuous	✓	
GF QA Web App	qa.gf.local	✓	Continuous	✓	
GF Research SSH App	research.gf.local	✓	Continuous	✓	
IRC	irc.safemarch.com	✓	Continuous	✓	
Microsoft Dynamics NAV	nav.safemarch.com	✓	On Access		
QA Application	qa.safemarch.com	✓	Continuous		
Research Server IP SSH	172.20.0.15	✓	On Access	✓	

Slide notes

On the **Application Segments** page, you can see a list of all the defined Application Segments that have been added. You have the option to **Edit** or **Delete** any of these Application Segments (although you may have to unmap them from policies first). To view details for an Application Segment, click on its name.

Slide 31 - Slide 31



Click Segment Groups to view details of the created groups

Name	Applications	Status	Health Check	Actions
All Other Services	*.safemarch.com	Green	Green	
CRM Application	crm.safemarch.com	Green	Continuous	Green

Segment Group: CRM App Group

Server Groups: CRM Servers

PORTS FOR ZSCALER APP ACCESS

TCP Port Ranges	UDP Port Ranges	Double Encryption	Bypass
80 - 80, 443 - 443		Disabled	Never

APPLICATIONS

crm.safemarch.com					
DC Filesharing and RDP	server01.safemarch.com	Green	Continuous	Green	
GF CRM Web Application	crm.gf.local	Green	Continuous	Green	
GF Intranet Web App	intranet.gf.local	Green	Continuous	Green	
GF QA Web App	qa.gf.local	Green	Continuous	Green	
GF Research SSH App	research.gf.local	Green	Continuous	Green	

Slide notes

To view or manage the list of Segment Groups, click **Segment Groups**.

Slide 32 - Slide 32

The screenshot shows the 'Segment Groups' tab selected in the top navigation bar. The main area displays a table of segment groups with columns for Name, Status, and Actions. A red box highlights the Actions column. A callout bubble points to this column with the text 'Edit or Delete Segment Groups'. On the left sidebar, the 'Administration' section is active, showing options like Application Segments, Browser Access, and Segment Groups.

Name	Status	Actions
AD-Servers	✓	
Azure Application Group	✓	
CRM App Group	✓	
DC App Group	✓	
Engineering App Group	✓	
GF CRM	✓	
GF Engineering	✓	
GF Intranet	✓	
GF QA	✓	

Slide notes

On the Segment Groups page, you can see a list of all the Segment Groups that have been added. You have the option to **Edit** or **Delete** any of these Segment Groups (although you may have to unmap them from other objects first).

Slide 33 - Slide 33

The screenshot shows the Zscaler Admin UI interface. On the left, there is a navigation sidebar with various icons and sections: Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, Help, and Settings. The main content area has a header with 'Server Groups' and a search bar. Below the header is a table with columns for 'Status' and 'Actions'. A callout bubble points to the 'Server Groups' link in the sidebar with the text 'Click Server Groups'.

Slide notes

To view or manage the list of Server Groups, from the **Administration** menu click **Server Groups** in the **APPLICATION MANAGEMENT** section.

Slide 34 - Slide 34

The screenshot shows the Zscaler Admin interface with the 'Server Groups' tab selected. The main area displays a table of server groups, each with columns for Name, Status, Dynamic Server Discovery, Connector Groups, and Actions. A red box highlights the 'Actions' column. A callout bubble with the text 'Edit or Delete Server Groups' points to this column. The left sidebar includes links for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, and Zscaler App.

Name	Status	Dynamic Server Discovery	Connector Groups	Actions
Amsterdam Server Group	✓	✓	Amsterdam Connector Group	
AWS Web Servers	✓	✓	AWS Connector Group	
Azure Central South US Autodis...	✓	✓	Azure US-Central-South	
Azure Dynamic Servers	✓	✓	Azure Connectors	
CRM Servers	✓	✓	AWS Connector Group	

Description:
Server Group for CRM access

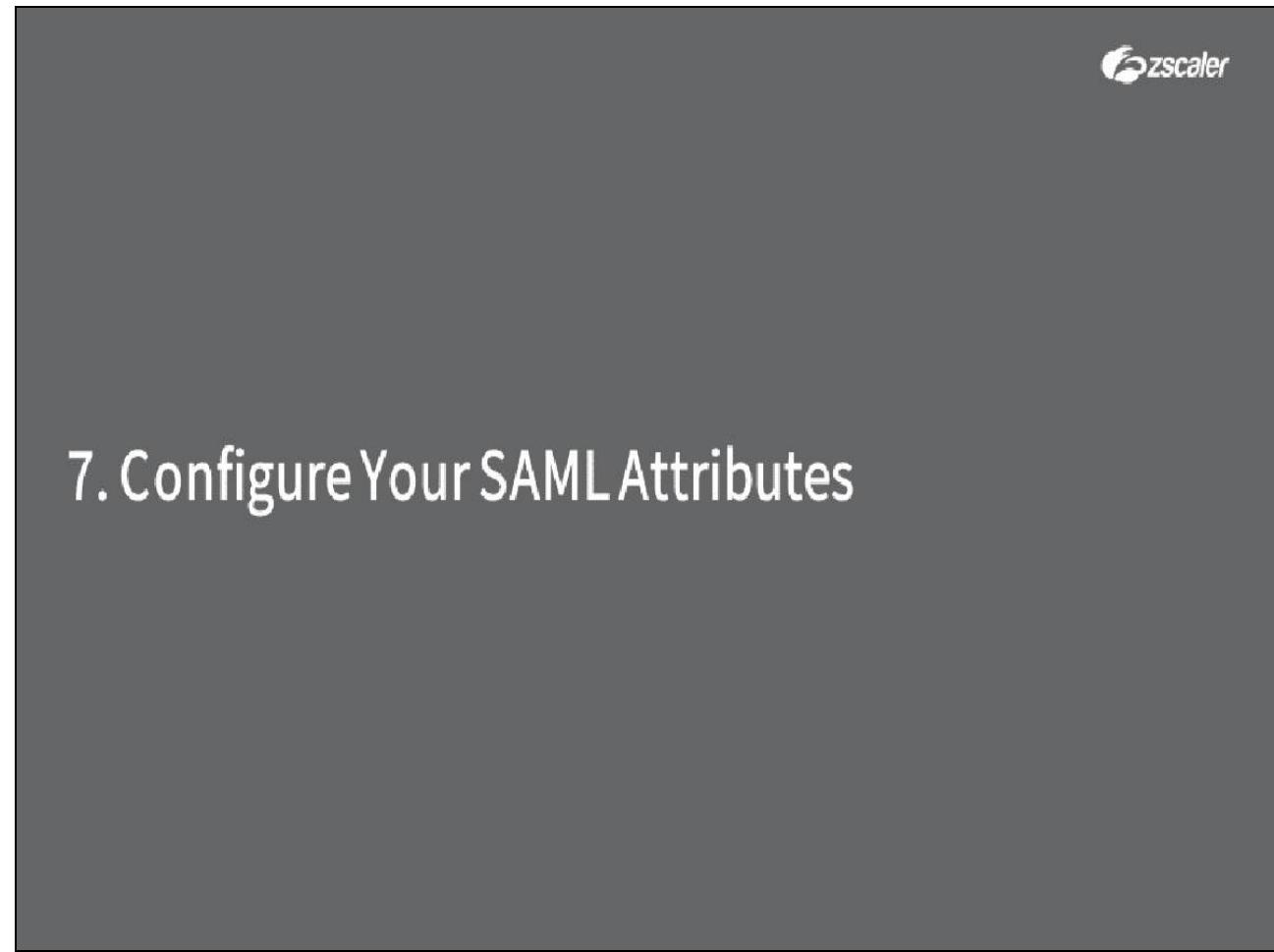
Servers:

Name	Status	Dynamic Server Discovery	Connector Groups	Actions
Domain Controllers	✓	✓	Corporate Datacenter	
Engineering Server Group	✓	✓	Corporate Datacenter	
GF Servers	✓	✓	ESXi Connector Group	
HQ Servers	✓	✓	Corporate Datacenter	

Slide notes

On the Server Groups page, you can see a list of all the Server Groups that have been added. You have the option to **Edit** or **Delete** any of these Server Groups (although you may have to unmap them from other objects first).

Slide 35 - 8. Configure Your SAML Attributes



7. Configure Your SAML Attributes

Slide notes

In the next section, we will look at the configuration of SAML Attributes for ZPA.

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 36 - Slide 36

The screenshot shows the Zscaler Admin Portal dashboard. On the left, there's a vertical navigation menu with sections like Application Management, Authentication, Certificate Management, Connector Management, Log Streaming Service, Policy Management, and Settings. A callout bubble points to the 'SAML Attributes' link under the Authentication section. The main dashboard area displays several cards: 'APPLICATION MANAGEMENT' (Application Segments, Segment Groups, Servers), 'AUTHENTICATION' (IdP Configuration, Settings, SAML Attributes), 'APPLICATIONS' (14 Days, 0), 'ACCESS POLICY BLOCKS' (0), 'SUCCESSFUL TRANSACTIONS' (968), 'TOP APPLICATIONS BY BANDWIDTH' (server01.safemarch.com, splunk.safemarch.com, gitlab.safemarch.com, crm.safemarch.com, intranet.safemarch.local, splunk.tm.zscaler.com, nav.safemarch.com, qa.safemarch.com, safemarch.com, 172.20.0.26), and 'TOP POLICY BLOCKS'.

Slide notes

SAML attributes can be used to create powerful policy controls for access to your private applications. You can create Access Policy rules targeted by any of the configured attributes, although note that your IdP must be configured to provide the attribute values in the assertions when users authenticate for ZPA access.

To manage SAML Attributes, from the **Administration** menu in the ZPA Admin Portal, click **SAML Attributes** in the **AUTHENTICATION** section.

Slide 37 - Slide 37

The screenshot shows the Zscaler Admin interface with the 'Administration' tab selected. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Search, and Zscaler App. The main area has tabs for 'IdP Configuration', 'SAML Attributes' (which is active), and 'Settings'. In the 'SAML Attributes' section, there's a table with columns: Name, SAML Attribute, IdP Name, and Actions. The table contains six rows corresponding to attributes provisioned from Okta and ADFS. A tooltip with the text 'Click ADFS' is overlaid on the 'IdP Configuration' dropdown menu, which is currently set to 'All'. The 'Actions' column for each row includes edit and delete icons.

Name	SAML Attribute	IdP Name	Actions
FirstName_Okta	FirstName	Okta	
DepartmentName_Okta	DepartmentName	Okta	
LastName_Okta	LastName	Okta	
Email_Okta	Email	Okta	
Department_ADFS	Department	ADFS	
memberOf_ADFS	memberOf	ADFS	
DisplayName_ADFS	DisplayName	ADFS	

Slide notes

The default view on the SAML Attributes page, is to show a list of **All** the known attributes, regardless from which IdP they were provisioned. To see only the attributes from a single IdP, select the IdP of interest from the **IdP Configuration** list. In this case click **ADFS**, ...

Slide 38 - Slide 38

The screenshot shows the Adobe Captivate interface with the 'SAML Attributes' tab selected for an 'ADFS' IdP Configuration. The table lists three attributes:

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

A tooltip labeled 'Click All' is overlaid on the first row's 'Actions' column, pointing to the edit icon.

Slide notes

...to see only the attributes provisioned from the ADFS IdP. Click to view All again, ...

Slide 39 - Slide 39

The screenshot shows the Adobe Captivate interface with the 'Administration' tab selected. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Zscaler App, and Help. The main area has tabs for 'IdP Configuration', 'SAML Attributes' (which is active), and 'Settings'. A sub-header 'IdP Configuration' with a dropdown menu is visible. The main content is a table of SAML attributes:

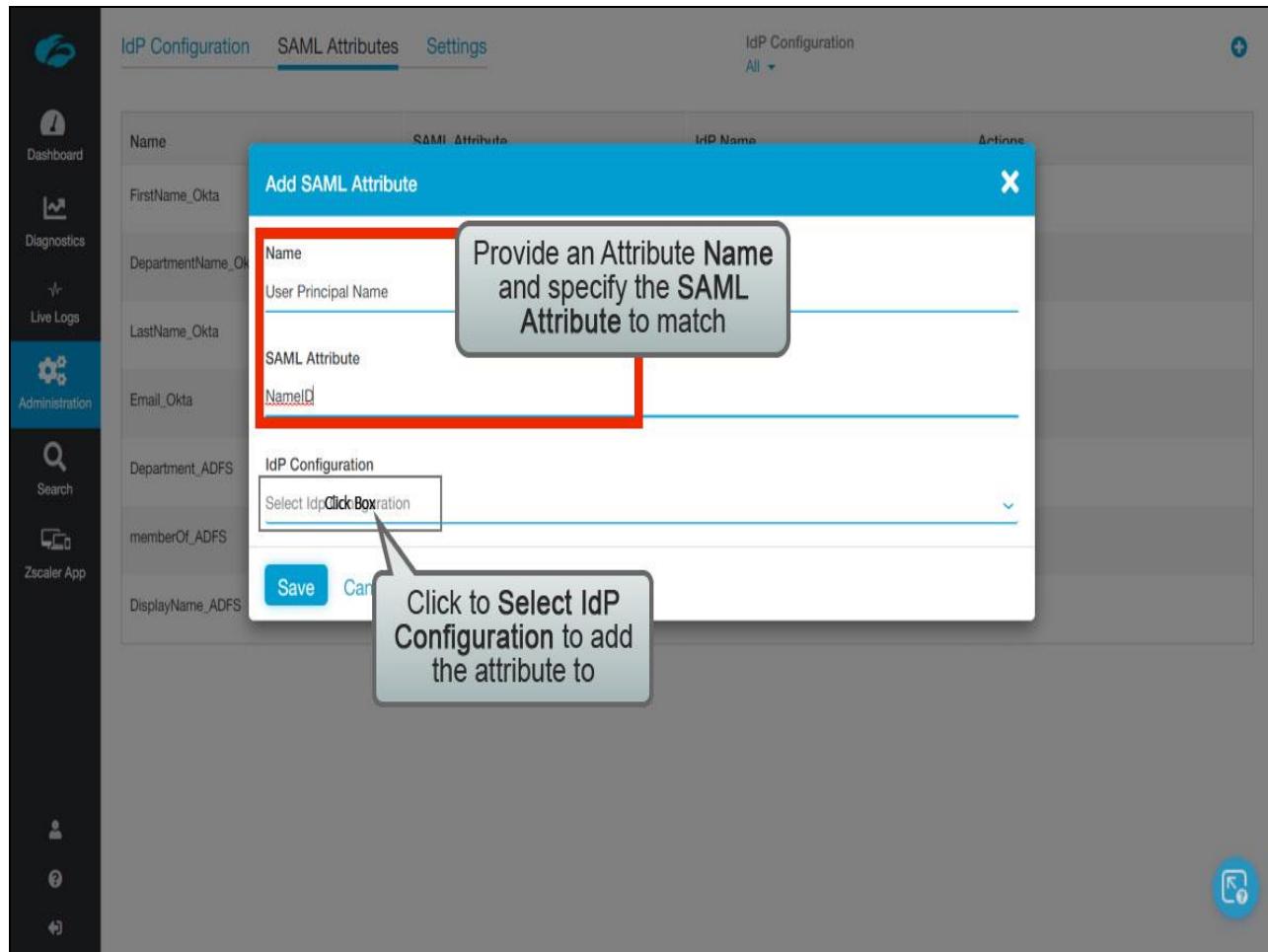
Name	SAML Attribute	IdP Name	Actions
FirstName_Okta	FirstName	Okta	
DepartmentName_Okta	DepartmentName	Okta	
LastName_Okta	LastName	Okta	
Email_Okta	Email	Okta	
Department_ADFS	Department	ADFS	
memberOf_ADFS	memberOf	ADFS	
DisplayName_ADFS	DisplayName	ADFS	

A callout box with a blue border and white background points to the top-right corner of the table area, containing the text 'Click + to add a new SAML Attribute'.

Slide notes

To manually add an attribute, click the + icon at top right.

Slide 40 - Slide 40



Slide notes

Give the new attribute a **Name** and specify the **SAML Attribute** to match. To specify the **IdP Configuration** to associate this attribute to, click **Select IdP Configuration**, ...

Slide 41 - Slide 41

The screenshot shows the Adobe Captivate interface with the 'SAML Attributes' tab selected. A modal window titled 'Add SAML Attribute' is open. Inside, there are fields for 'Name' (containing 'User Principal Name') and 'SAML Attribute' (containing 'NameID'). Below these, a 'Select IdP Configuration' dropdown is open, showing options like 'Click Box', 'Okta', and 'Clear Selection'. A callout box with the text 'Click to select ADFS' points to the 'Click Box' option in the dropdown.

Slide notes

...and select one of the available IdP Configurations, in this case click ADFS, ...

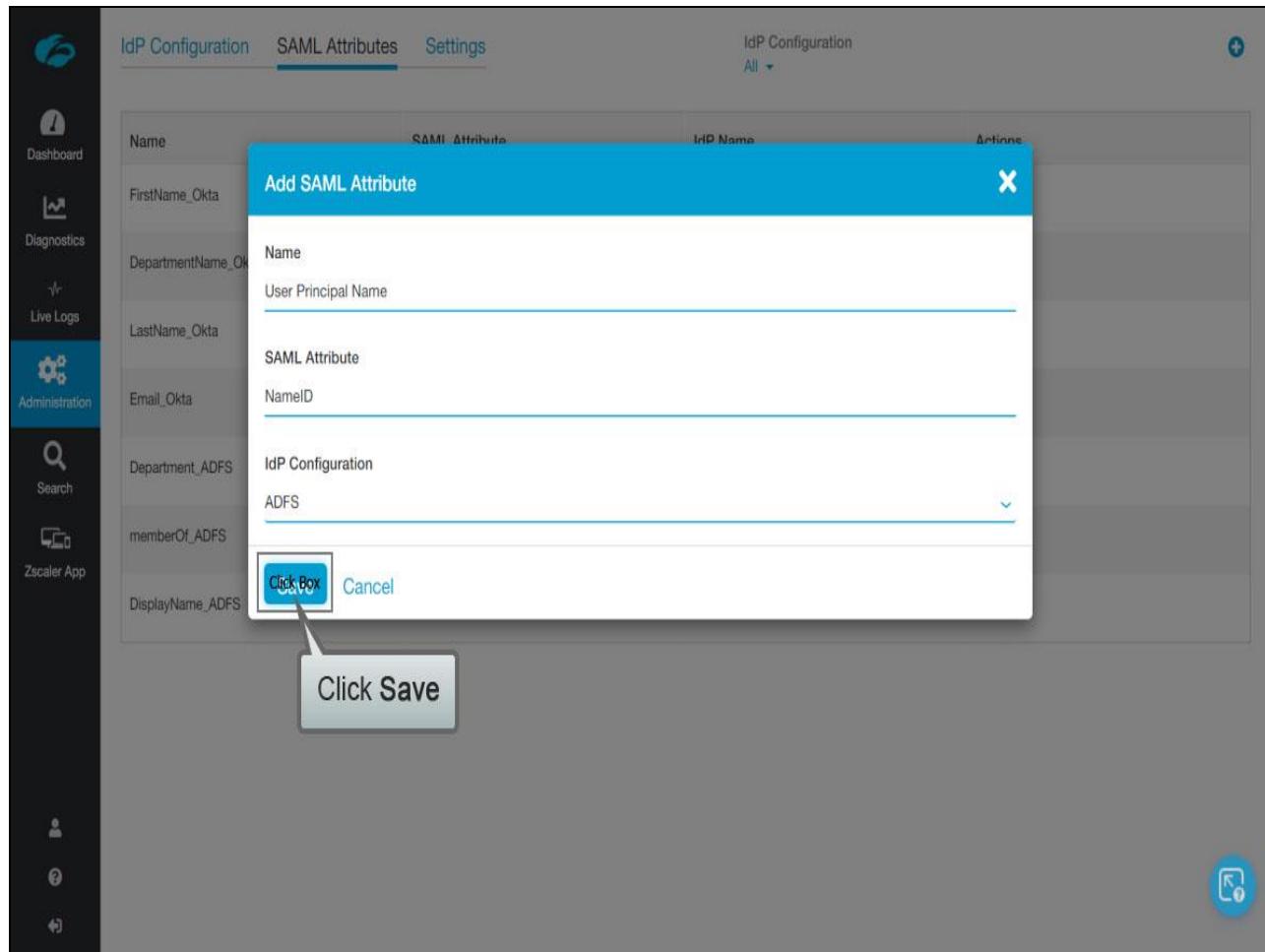
Slide 42 - Slide 42

The screenshot shows the Adobe Captivate interface with the "SAML Attributes" tab selected. A modal window titled "Add SAML Attribute" is open, prompting for a "Name" (User Principal Name) and a "SAML Attribute" (NameID). Below the modal, a dropdown menu lists "IdP Configuration" and "ADFS". The "ADFS" option is selected, indicated by a blue circle. The background table lists various SAML attributes, such as FirstName_Okta, DepartmentName_Okta, LastName_Okta, Email_Okta, Department_ADFS, memberOf_ADFS, and DisplayName_ADFS.

Name	SAML Attribute	IdP Name	Actions
FirstName_Okta			
DepartmentName_Okta			
LastName_Okta			
Email_Okta			
Department_ADFS			
memberOf_ADFS			
DisplayName_ADFS			

Slide notes

Slide 43 - Slide 43



Slide notes

...and click **Save**.

Slide 44 - Slide 44

The screenshot shows the Adobe Captivate interface with the "Administration" tab selected in the sidebar. The main area displays a table of SAML attributes for an Okta integration. The columns are "Name", "SAML Attribute", "IdP Name", and "Actions". The rows show mappings for FirstName_Okta, DepartmentName_Okta, LastName_Okta, User Principal Name, Email_Okta, Department_ADFS, memberOf_ADFS, and DisplayName_ADFS. Each row has edit and delete icons in the "Actions" column. A green notification bar at the bottom right indicates "SAML attribute saved" with a refresh icon.

Name	SAML Attribute	IdP Name	Actions
FirstName_Okta	FirstName	Okta	
DepartmentName_Okta	DepartmentName	Okta	
LastName_Okta	LastName	Okta	
User Principal Name	NameID	ADFS	
Email_Okta	Email	Okta	
Department_ADFS	Department	ADFS	
memberOf_ADFS	memberOf	ADFS	
DisplayName_ADFS	DisplayName	ADFS	

Slide notes

Slide 45 - Slide 45

The screenshot shows the 'SAML Attributes' tab of the IdP Configuration in Adobe Captivate. The table lists various SAML attributes with their names, SAML Attribute mappings, and IdP Names. A red box highlights the 'Actions' column, which contains edit and delete icons. A callout box labeled 'New SAML Attribute' points to the first row, which has been highlighted with a red border. Another callout box labeled 'Edit or Delete Attributes' points to the 'Actions' column.

Name	SAML Attribute	IdP Name	Actions
FirstName_Okta	FirstName	Okta	
DepartmentName_Okta	DepartmentName	Okta	
LastName_Okta	LastName	Okta	
User Principal Name	NameID	ADFS	
Email_Okta	Email	Okta	
Department_ADFS	Department	ADFS	
memberOf_ADFS	memberOf	ADFS	
DisplayName_ADFS	DisplayName	ADFS	

Slide notes

The new attribute will be added to the list of available SAML Attributes. You have the options to **Edit** or **Delete** any of the listed attributes.

Slide 46 - 9. Configure Your Access Policies

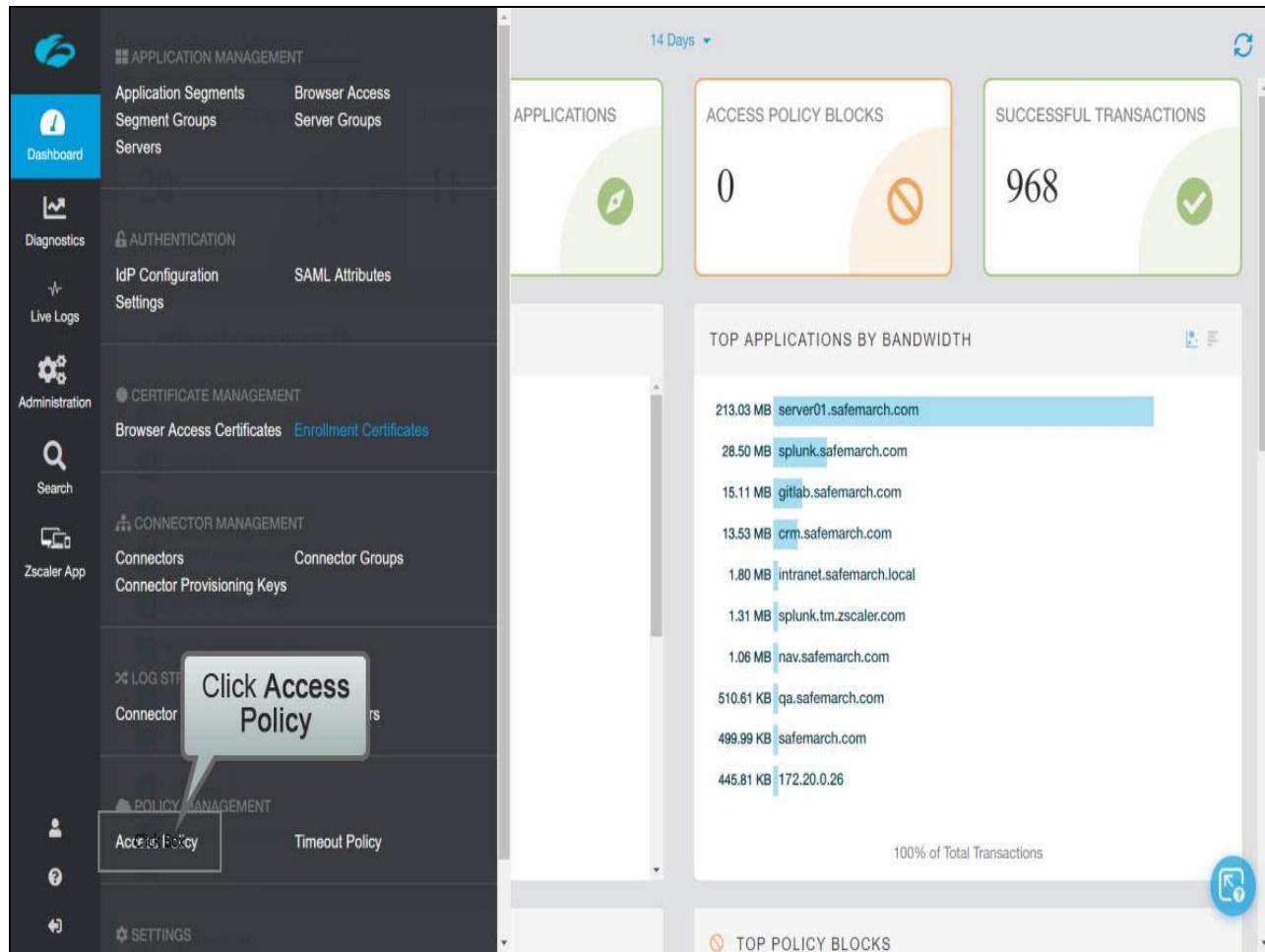
8. Configure Your Access Policies

Slide notes

In the final section, we will look at the configuration of Access Policies for ZPA.

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 47 - Slide 47



Slide notes

Until you configure access policies for applications your users will not be able to access any of the private applications that you've configured for ZPA, regardless of whether you explicitly define your applications or enable application discovery. You must explicitly **Allow** access to the applications using **Access Policy** rules. You also have the option to configure a default, or targeted **Timeout Policy** rules.

To create Access Policy rules, in the ZPA Admin Portal from the **Administration** menu click **Access Policy** in the **POLICY MANAGEMENT** section, ...

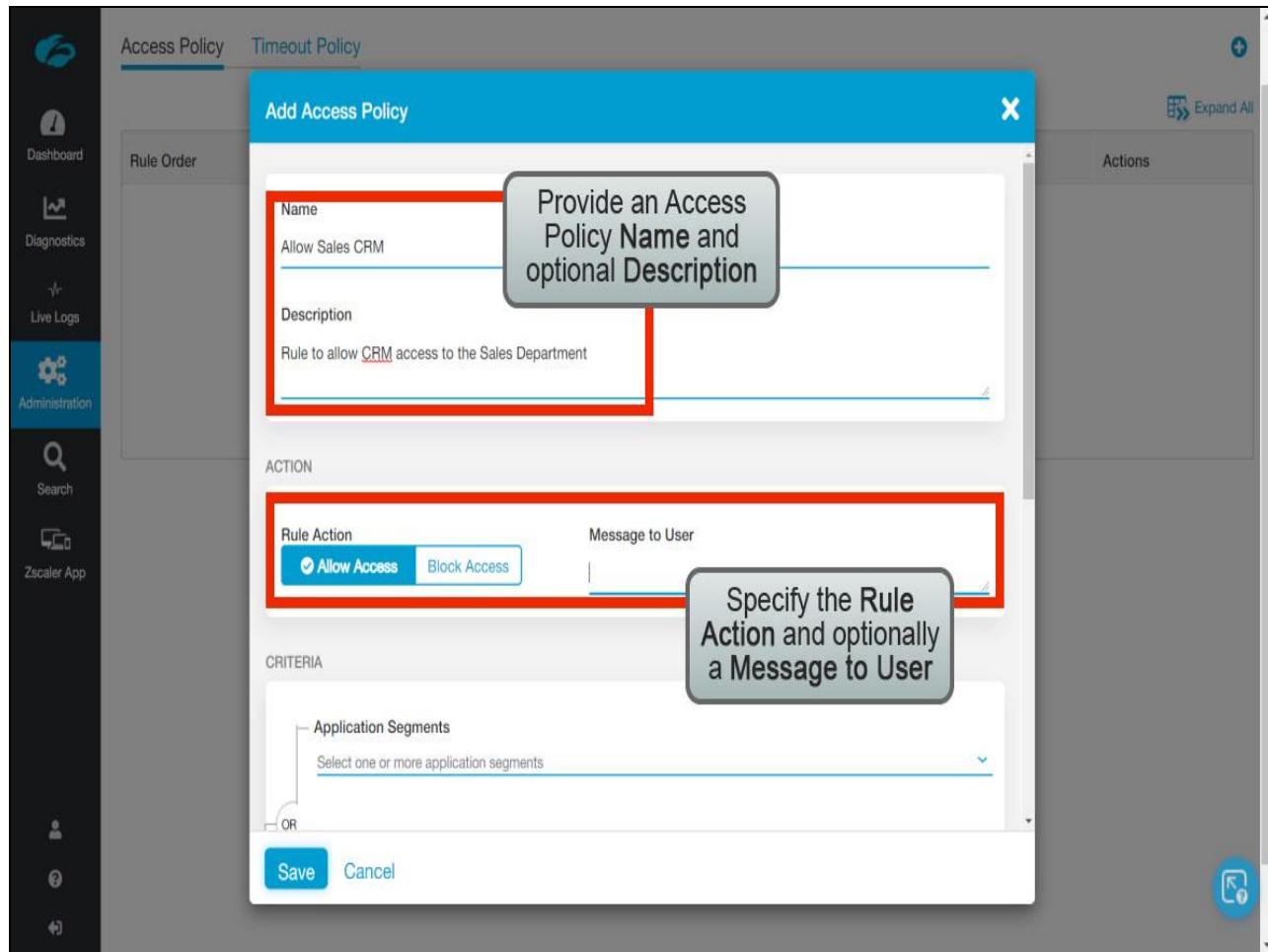
Slide 48 - Slide 48

The screenshot shows the ZPA interface with the 'Access Policy' tab selected. On the left is a vertical navigation bar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for 'Access Policy' (selected) and 'Timeout Policy'. Below the tabs is a table with columns 'Rule Order', 'Name', and 'Rule Action'. A message at the bottom of the table says 'Click Add Rule to create a new policy rule'. A large callout box with a grey border and white text points to the top-right corner of the table area, containing the text 'Click + to add a new rule'. Another callout box with a grey border and white text points to the center of the table area, containing the text 'By default ZPA denies access to applications for all users'. A blue circular icon with a white square and a question mark is located in the bottom right corner of the main area.

Slide notes

...and the list of existing **Access Policy** rules will be displayed. Note that by default ZPA denies access to applications for all users, you must create policy rules to explicitly **Allow** users access to specific **Application Segments** or **Segment Groups**. To create a new rule, click the + icon at top right.

Slide 49 - Slide 49



Slide notes

Give the rule a **Name** and optionally add a **Description**. To make this a rule to enable access, in the **Rule Action** field, select **Allow**.

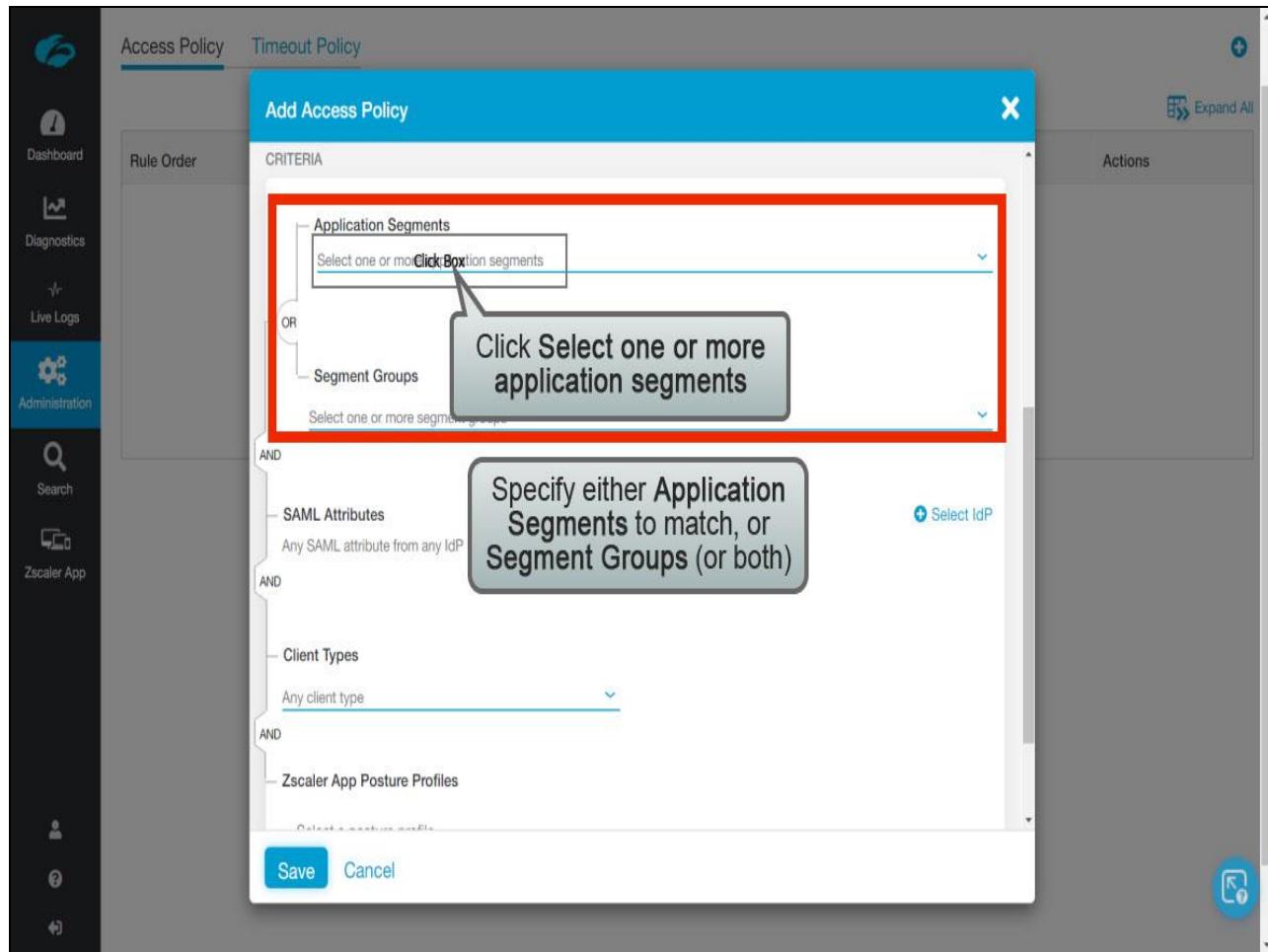
Slide 50 - Slide 50

The screenshot shows the Zscaler Access Policy configuration interface. The main window has tabs for 'Access Policy' and 'Timeout Policy', with 'Access Policy' selected. On the left, a sidebar lists various navigation options: Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and Help. The central area displays the 'Add Access Policy' dialog. The dialog has fields for 'Name' (set to 'Allow Sales CRM') and 'Description' (set to 'Rule to allow CRM access to the Sales Department'). Under the 'ACTION' section, there are two buttons: 'Allow Access' (which is checked) and 'Block Access'. A 'Message to User' field is also present. The 'CRITERIA' section contains a dropdown menu labeled 'Application Segments' with the sub-instruction 'Select one or more application segments'. A large button labeled 'Scroll down...' is overlaid on the right side of the dialog. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Slide notes

Scroll down...

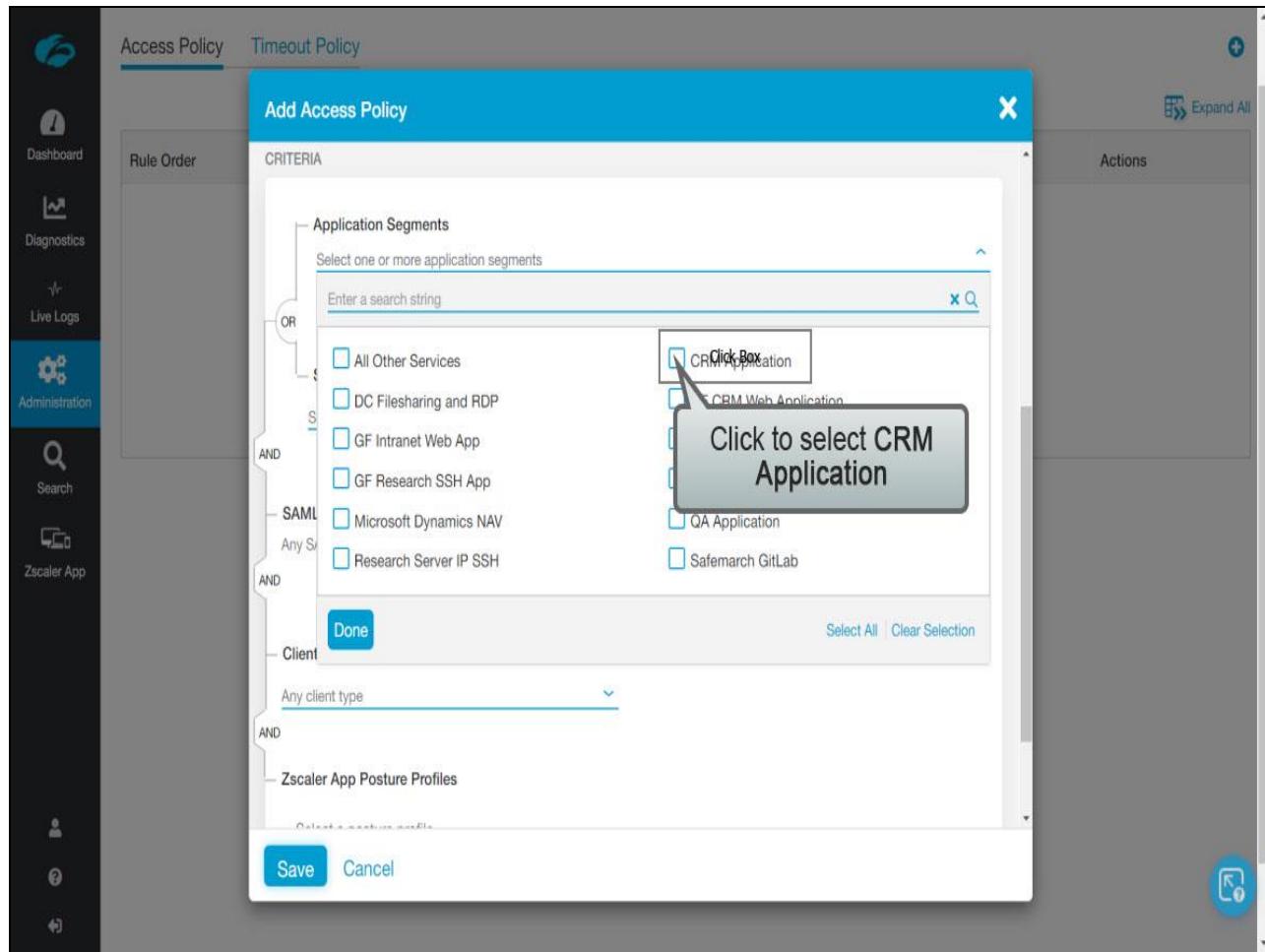
Slide 51 - Slide 51



Slide notes

In the **CRITERIA** section you have the option to target this rule against either Application Segments or Segment Groups, or both. Note that **Application Segments** and **Segment Groups** are logically matched using a Boolean **OR**. To add an Application Segment, click **Select one or more application segments**, ...

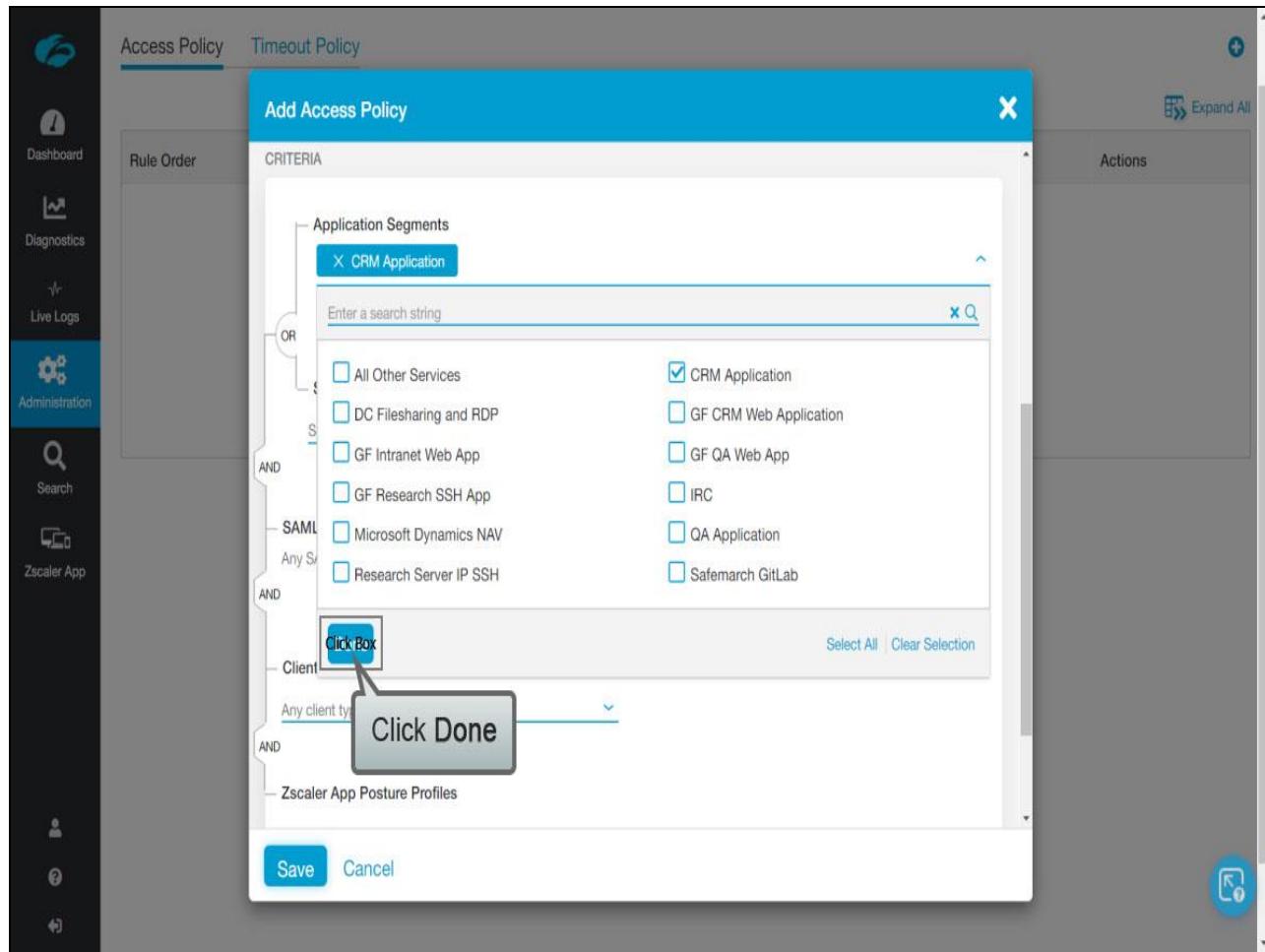
Slide 52 - Slide 52



Slide notes

...and select the **Application Segment or Segments** to target with this rule. In this case click to select the **CRM Application** you added earlier, ...

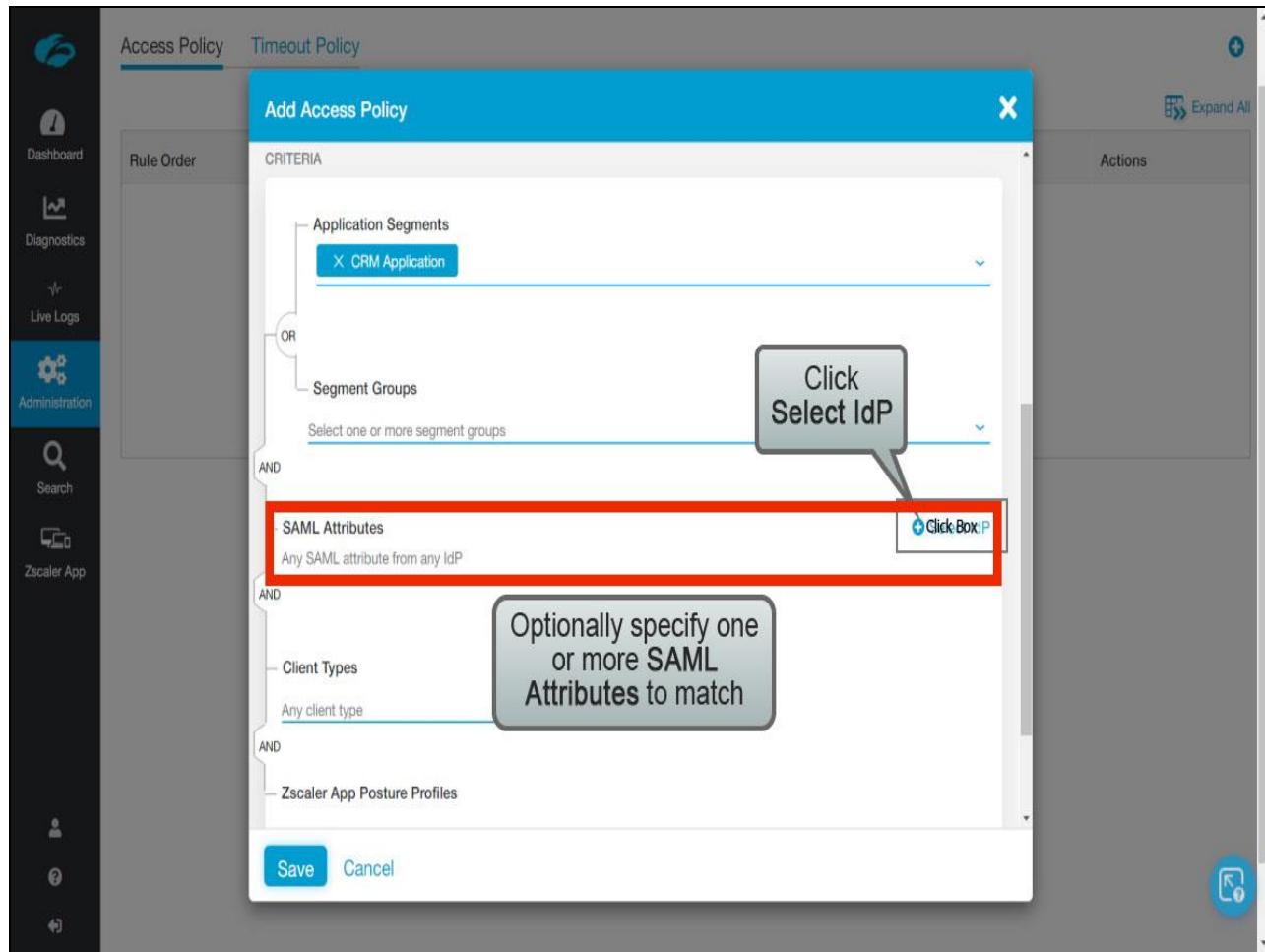
Slide 53 - Slide 53



Slide notes

...then click **Done**.

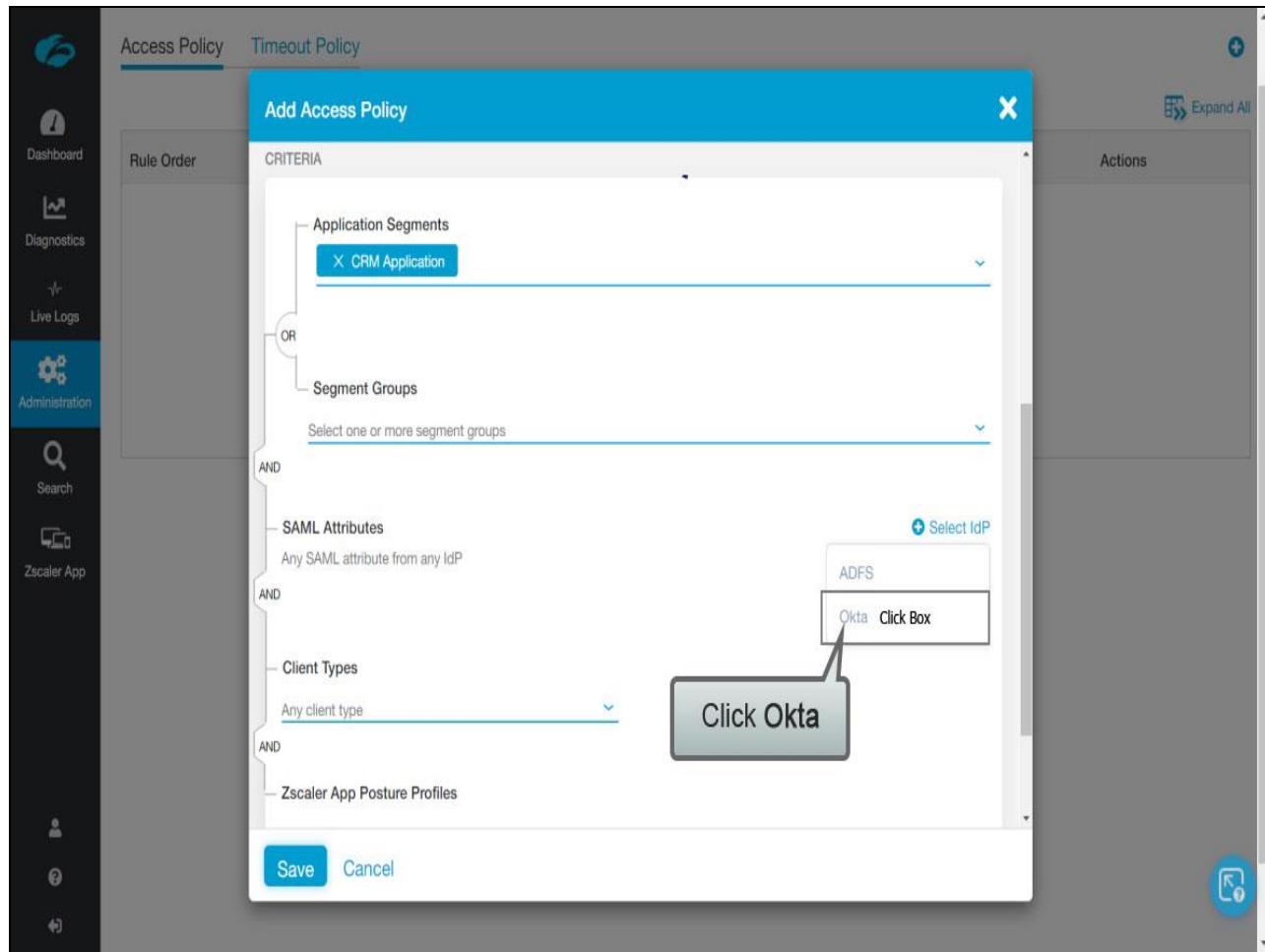
Slide 54 - Slide 54



Slide notes

Next, you have the option to target the policy to specific users by matching one or more of the available SAML Attributes. Note that this option (and all the subsequent ones) are matched using a logical Boolean **AND**. First you need to select the IdP Configuration the attribute belongs to, so click **Select IdP**, ...

Slide 55 - Slide 55



Slide notes

...and select the correct IdP, in this case click **Okta**.

Slide 56 - Slide 56

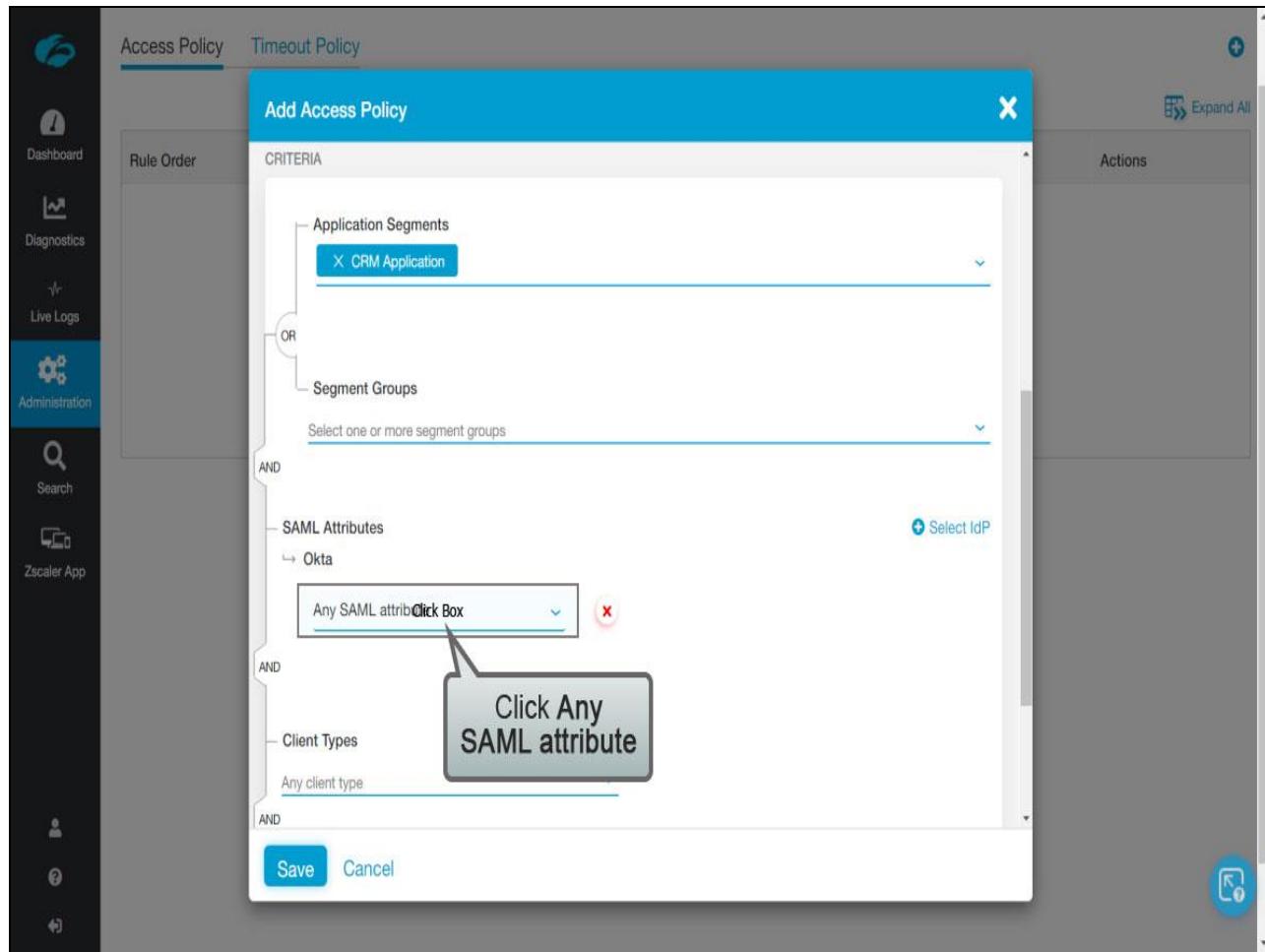
The screenshot shows the 'Add Access Policy' dialog box over a dark-themed Zscaler interface. The dialog has a blue header bar with the title 'Add Access Policy' and a close button. Below the header is a section titled 'CRITERIA' with a tree-like structure for defining policy rules:

- Application Segments:** Contains a single item: 'CRM Application'.
- Segment Groups:** A dropdown menu labeled 'Select one or more segment groups'.
- SAML Attributes:** A dropdown menu labeled 'Any SAML attribute from any IdP'.
- Client Types:** A dropdown menu labeled 'Any client type'.
- Zscaler App Posture Profiles:** A dropdown menu.

Below the criteria section are two buttons: 'Save' and 'Cancel'. To the right of the main dialog, there is a smaller, semi-transparent modal titled 'Select IdP' with two options: 'ADFS' and 'Okta', where 'Okta' is highlighted in blue.

Slide notes

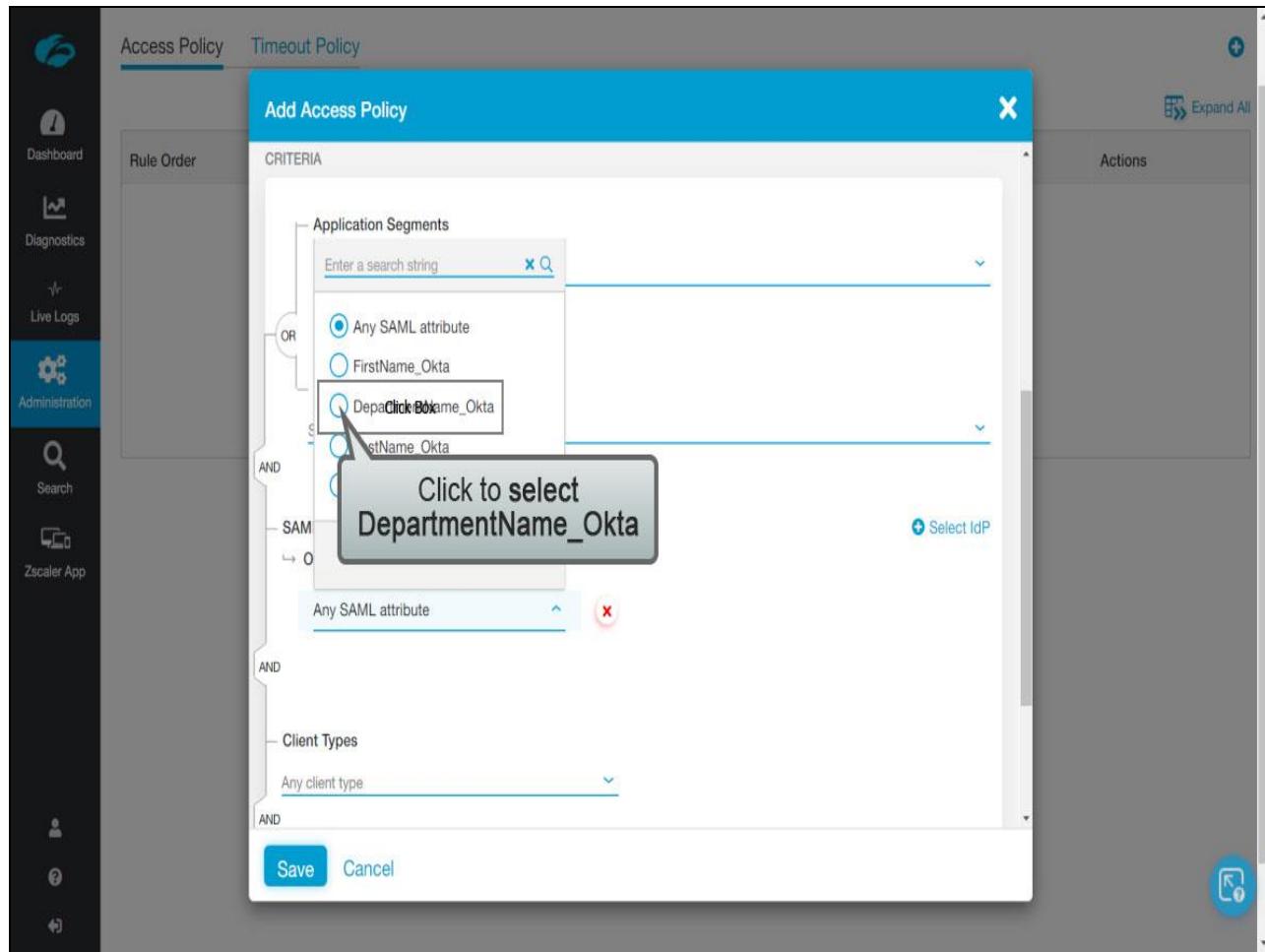
Slide 57 - Slide 57



Slide notes

Next, to select a specific attribute, click **Any SAML Attribute**, ...

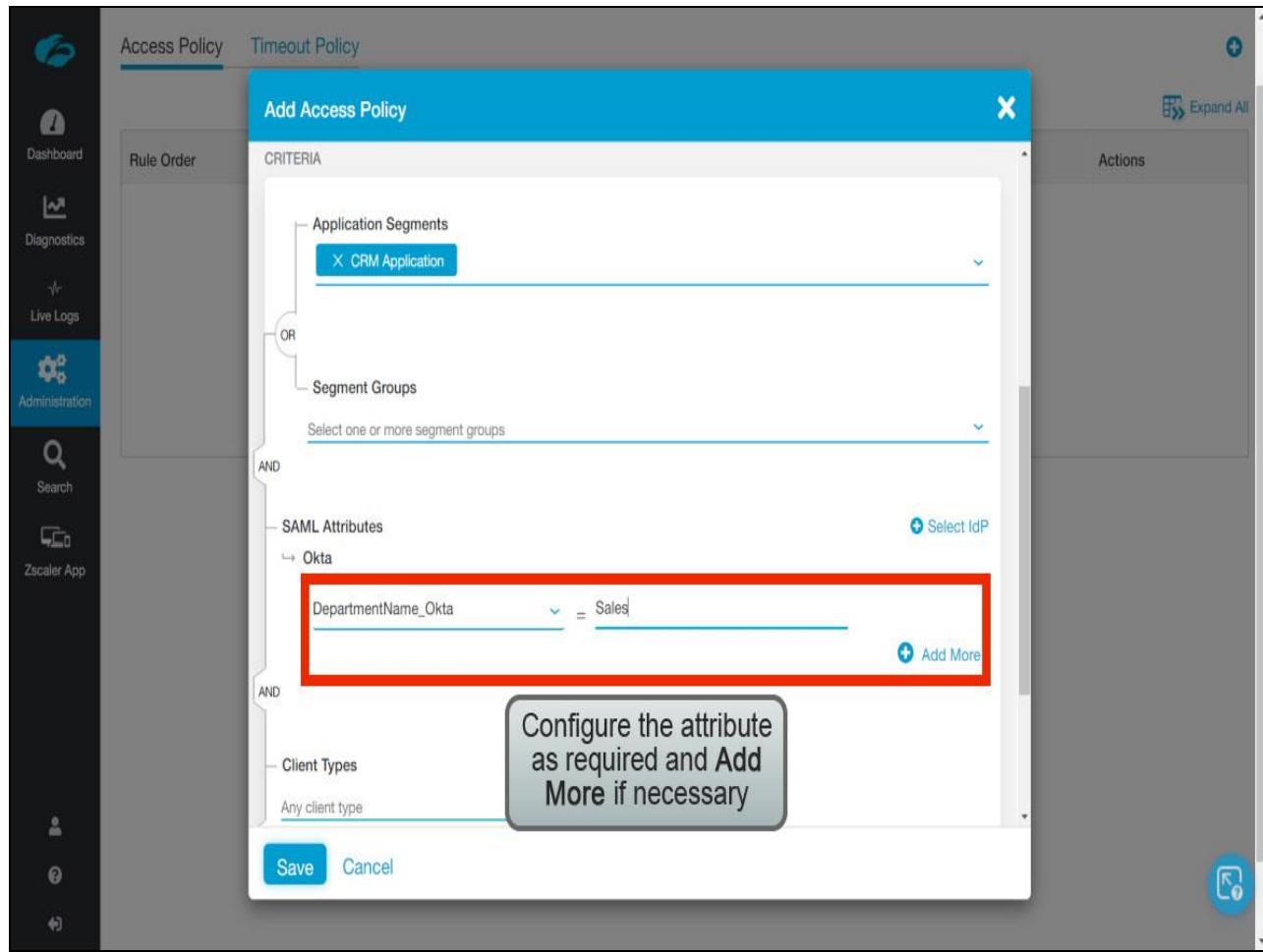
Slide 58 - Slide 58



Slide notes

...find and select the correct attribute, in this case click **DepartmentName_Okta**.

Slide 59 - Slide 59



Slide notes

Then, specify the appropriate attribute value to match. In this case the only users that will be allowed access to this application, are members of the **Sales** Department. There is an **Add More** option that allows you to add additional attributes if necessary.

Slide 60 - Slide 60

The screenshot shows the Zscaler Access Policy configuration interface. The main window has tabs for 'Access Policy' and 'Timeout Policy', with 'Access Policy' selected. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area is titled 'Add Access Policy' and contains a 'CRITERIA' section. The criteria are defined by a logical AND of two conditions:

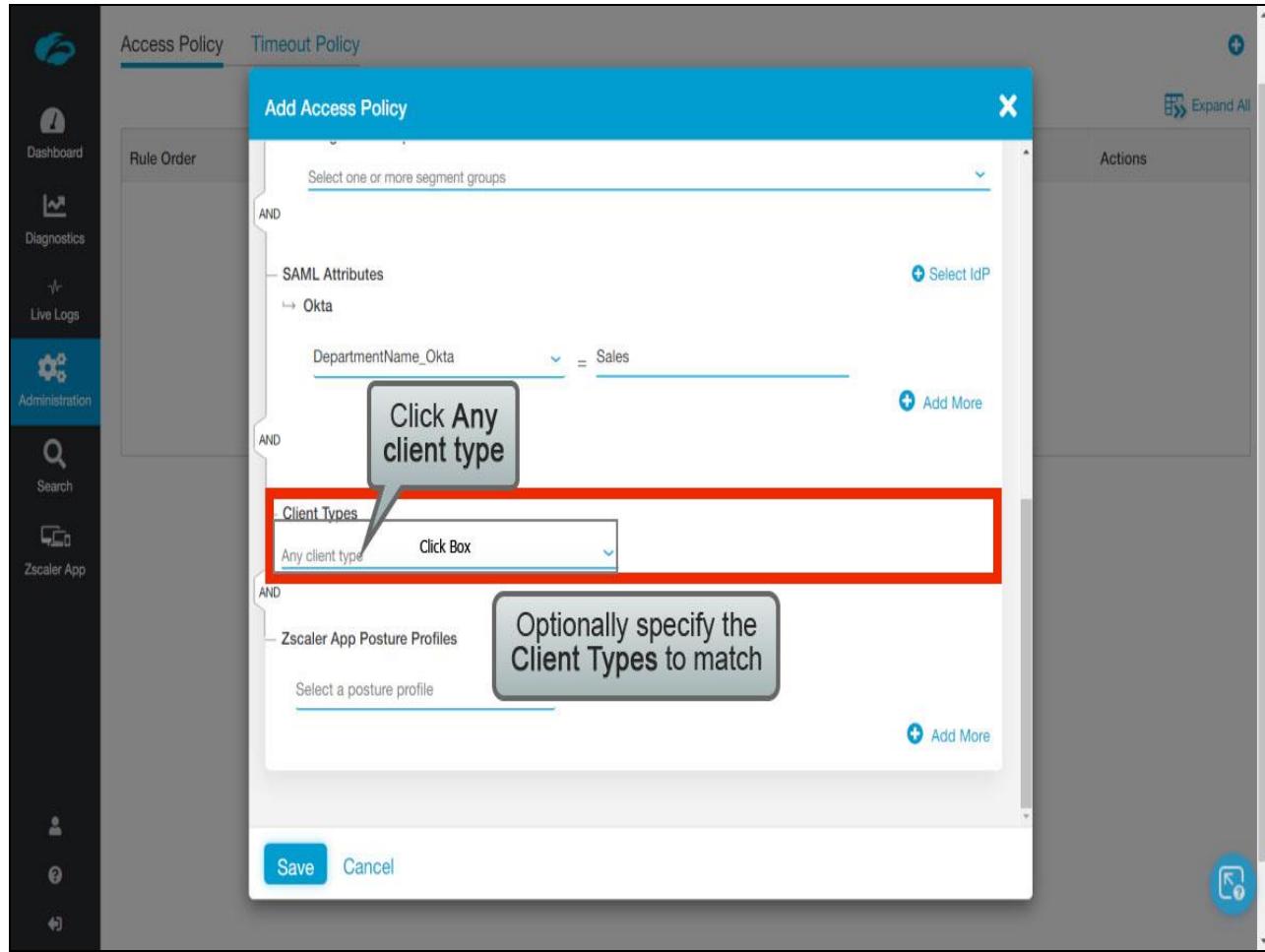
- Application Segments:** CRM Application
- AND:** SAML Attributes (Okta)
 - DepartmentName_Okta = Sales

Below the criteria, there's a 'Client Types' section with 'Any client type'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. A large button labeled 'Scroll down...' is overlaid on the right side of the dialog.

Slide notes

Scroll down...

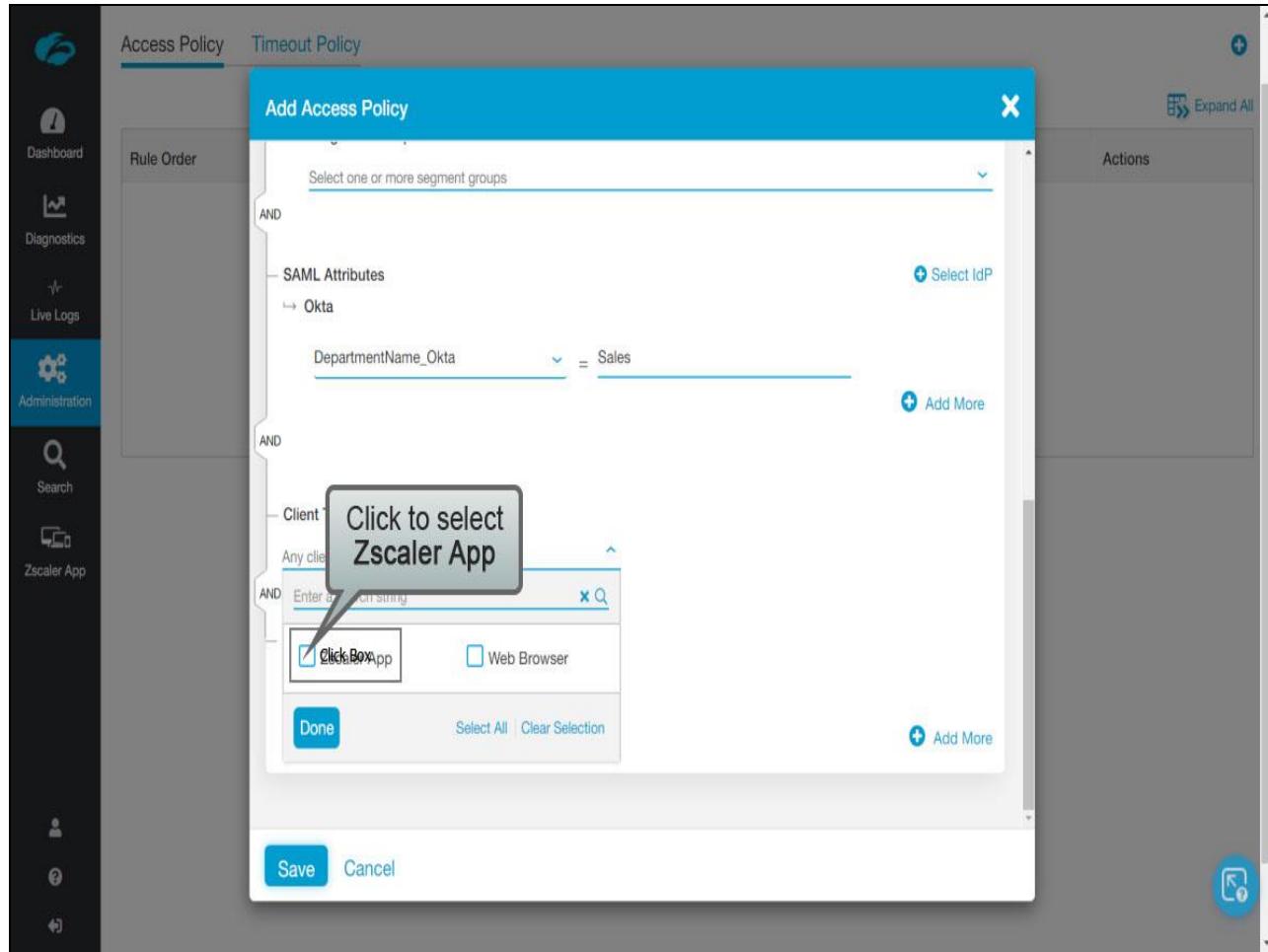
Slide 61 - Slide 61



Slide notes

The next option is to target the rule based on the **Client Type** (Zscaler App or Web Browser). To configure this, click **Any client type**, ...

Slide 62 - Slide 62



Slide notes

...then select the Client Types you wish to support on this rule. In this case click to enable **Zscaler App** only, ...

Slide 63 - Slide 63

The screenshot shows the Zscaler Access Policy configuration interface. The main window title is "Add Access Policy". The "Rule Order" dropdown is set to "Select one or more segment groups". The policy structure is defined by "AND" clauses:

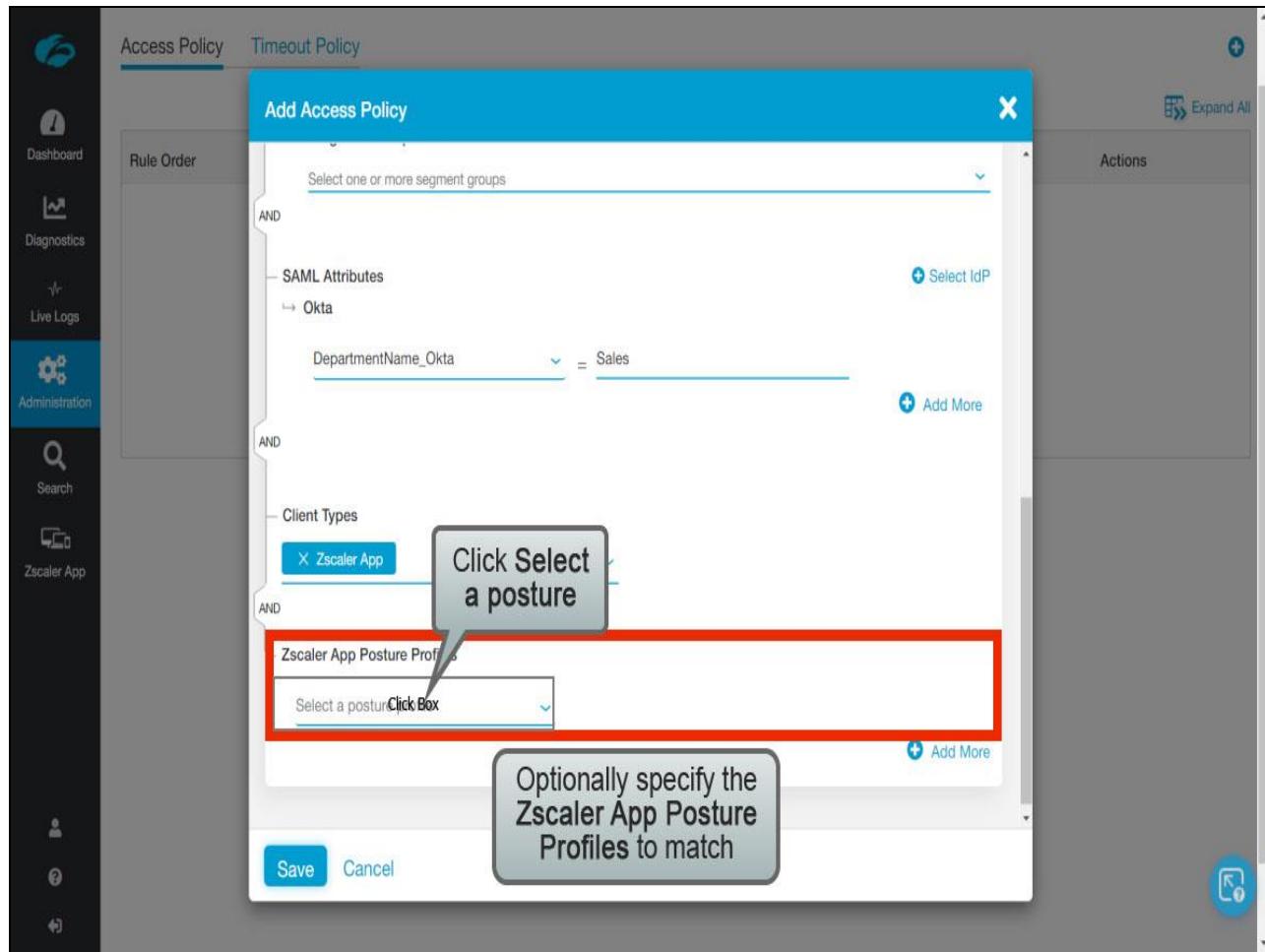
- The first clause is "SAML Attributes": "DepartmentName_Okta" = "Sales". A tooltip "Select IdP" is shown next to the "Select IdP" button.
- The second clause is "Client Types": "Zscaler App".
 - An "Enter a search string" input field is present.
 - A checkbox "Zscaler App" is checked.
 - A checkbox "Web Browser" is unchecked.
 - A "Click Box" button is highlighted with a callout bubble containing the text "Click Done".
 - Buttons "Select All" and "Clear Selection" are visible.
 - A "Save" button is at the bottom.

On the right side of the dialog, there is a "Actions" section with a "Select All" button and a "Clear Selection" button. The background of the main window shows a list of actions: "Expand All", "Actions", and a list of items starting with "Zscaler App".

Slide notes

...and click Done.

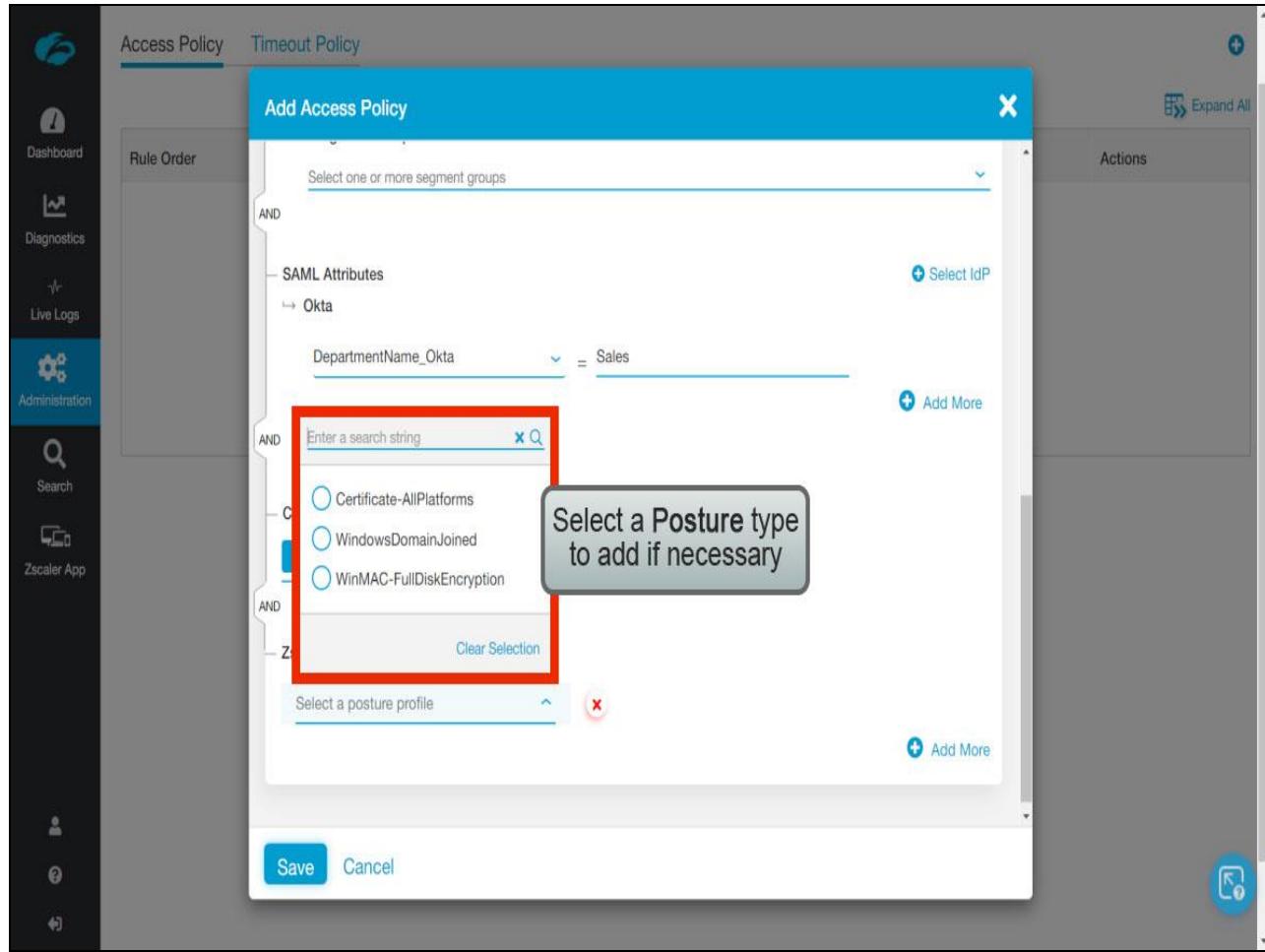
Slide 64 - Slide 64



Slide notes

Next, if you wish to enforce a device posture criteria for access to the application, you can select an appropriate **Zscaler App Posture Profile** here. Note that the Posture Profiles must already exist in the associated Zscaler App Portal in order for them to appear in this list for you to select. To add a posture criteria, click **Select a posture profile**, ...

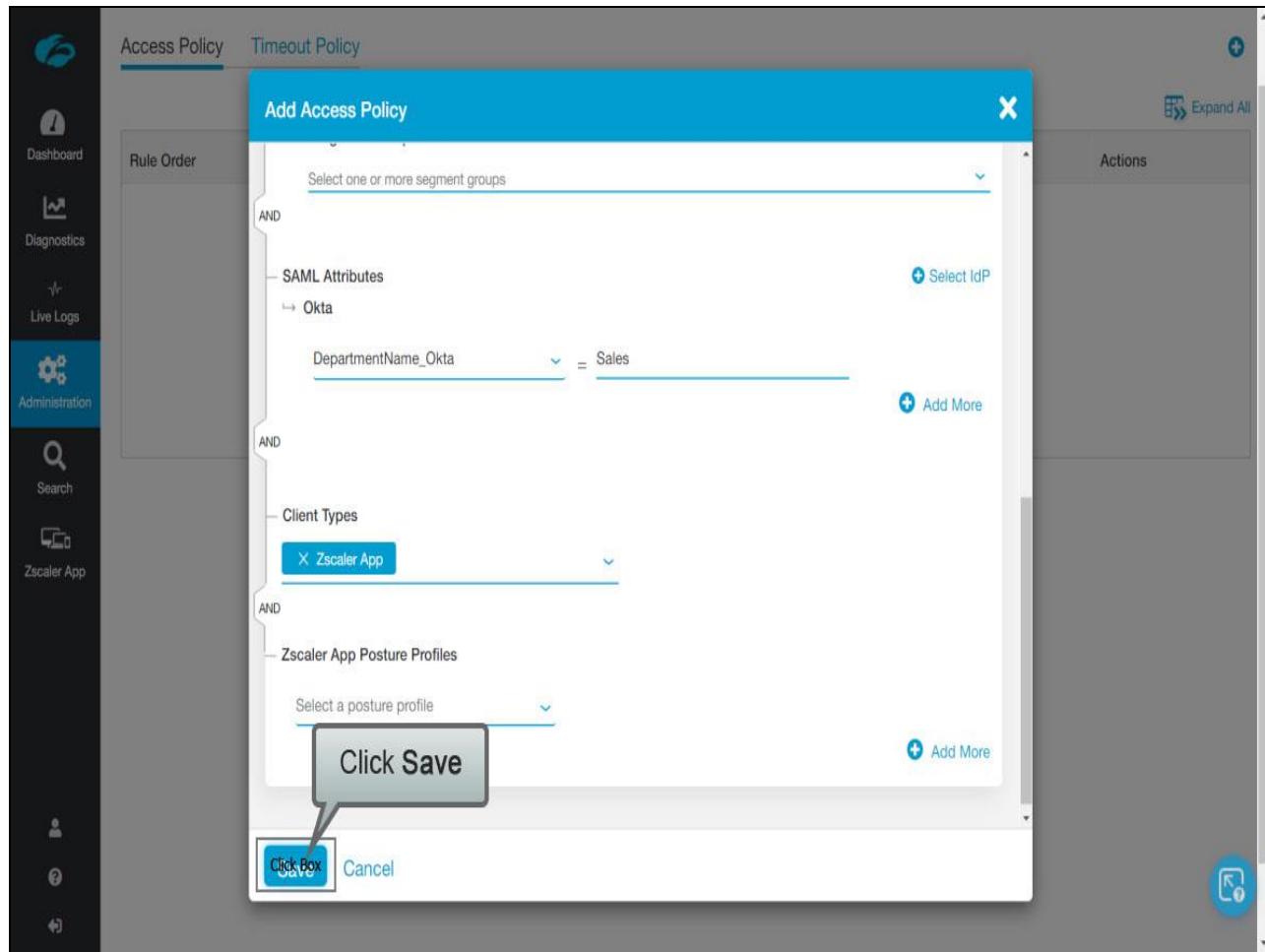
Slide 65 - Slide 65



Slide notes

...and select the Posture Profile to apply (although we will not use posture as a criteria on this rule).

Slide 66 - Slide 66



Slide notes

Having configured the policy rule as necessary, click **Save**.

Slide 67 - Slide 67

The screenshot shows the Zscaler Access Policy configuration screen. On the left is a dark sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main area has tabs for 'Access Policy' (selected) and 'Timeout Policy'. A table lists a single rule: 'Allow Sales CRM' with 'Allow Access' action. A green success message at the bottom right says 'Access policy saved'.

Rule Order	Name	Rule Action	Actions
1	Allow Sales CRM	Allow Access	

Access policy saved

Slide notes

Slide 68 - Slide 68

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left sidebar, there are icons for Dashboard, Diagnostics, Live Logs, Search, Zscaler App, and other administration settings. The main content area is titled 'Access Policy' and displays a single rule:

Rule Order	Name	Rule Action	Actions
1	Allow Sales CRM	Allow Access	

At the top right of the main content area, there is a 'Expand All' button and a '+' icon. A blue circular icon with a white square and a question mark is located in the bottom right corner of the main area.

Slide notes

Slide 69 - Slide 69

The screenshot shows the Zscaler Access Policy interface. On the left is a navigation sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, and Zscaler App. The main area has tabs for 'Access Policy' (selected) and 'Timeout Policy'. A table lists policy rules:

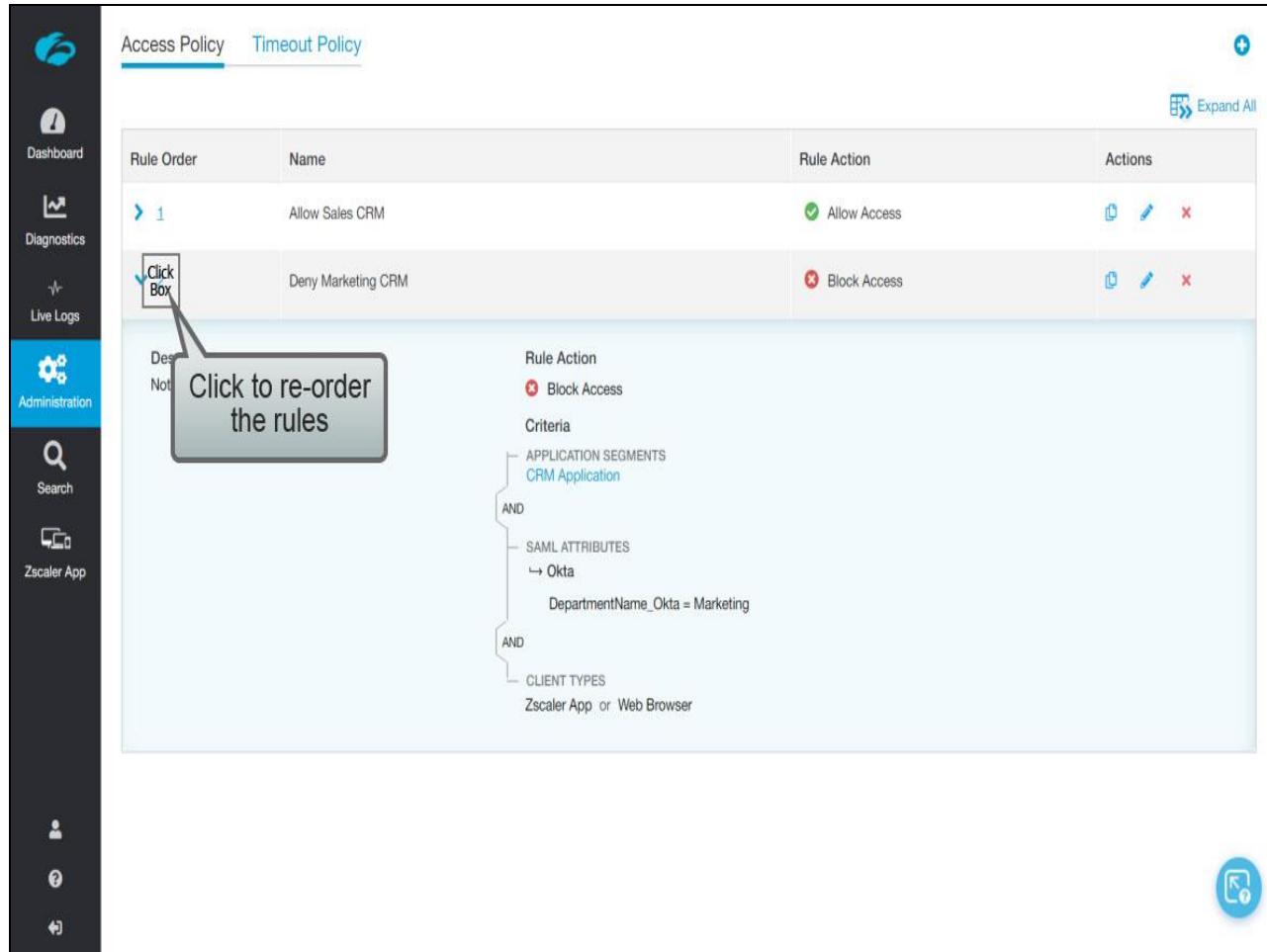
Rule Order	Name	Rule Action	Actions
1	Allow Sales CRM	Allow Access	
	Deny Marketing CRM	Block Access	

A red box highlights the 'Actions' column. A callout box with the text 'Edit or Delete Policy Rules' points to it. A grey box with the text 'Click to expand the Policy rule' points to the first rule's name.

Slide notes

The Access Policy rules are listed in the order that you created them, and each may be edited or deleted. Remember that rules are read from the top down with a first match, and that there is a default **Deny All** rule at the end of the list. To view details for a rule, click the name to expand it, ...

Slide 70 - Slide 70



Rule Order	Name	Rule Action	Actions
1	Allow Sales CRM	Allow Access	
2	Deny Marketing CRM	Block Access	

Des
Not

Click to re-order
the rules

Rule Action
Block Access

Criteria

APPLICATION SEGMENTS
CRM Application

AND

SAML ATTRIBUTES
Okta
DepartmentName_Okta = Marketing

AND

CLIENT TYPES
Zscaler App. or Web Browser

Slide notes

...and the details will be displayed. To change the order of the rules, click in the **Rule Order** field, ...

Slide 71 - Slide 71

The screenshot shows the Zscaler Access Policy configuration interface. The left sidebar includes icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, and Zscaler App. The main area has tabs for 'Access Policy' (selected) and 'Timeout Policy'. A table lists rules with columns for Rule Order, Name, Rule Action, and Actions. Two rules are present:

Rule Order	Name	Rule Action	Actions
1	Allow Sales CRM	Allow Access	
1	Deny Marketing CRM	Block Access	

The 'Deny Marketing CRM' rule is expanded to show its details:

- Description: Not Available
- Rule Action: Block Access
- Criteria:
 - APPLICATION SEGMENTS: CRM Application
 - AND
 - SAML ATTRIBUTES:
 - Okta
 - DepartmentName_Okta = Marketing
 - AND
 - CLIENT TYPES: Zscaler App or Web Browser

Slide notes

...and type the new rule order number for this rule (1 in this case).

Slide 72 - Slide 72

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left sidebar, there are icons for Dashboard, Diagnostics, Live Logs, Search, Zscaler App, and other navigation options. The main content area is titled 'Access Policy' and displays two rules in a table:

Rule Order	Name	Rule Action	Actions
1	Deny Marketing CRM	Block Access	Edit Delete
2	Allow Sales CRM	Allow Access	Edit Delete

A blue '+' button is located at the top right of the table. A green 'Expand All' button is also visible. At the bottom right, a green success message box contains the text 'Access policy rule order saved' next to a circular icon with a checkmark.

Slide notes

Slide 73 - Slide 73

The screenshot shows the Zscaler Admin interface. On the left, there's a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, Zscaler App, and Help. The main content area has a header 'Access Policy' with a sub-link 'Click Box Policy'. Below this is a table with columns: Rule Order, Name, Rule Action, and Actions. There are two rows: one for 'Deny Me' (Rule Order 1) with 'Block Access' and one for 'Allow Sales CRM' (Rule Order 2) with 'Allow Access'. An 'Expand All' button is in the top right of the table. A large callout box points to the 'Click Box Policy' link in the header.

Rule Order	Name	Rule Action	Actions
> 1	Deny Me	Block Access	
> 2	Allow Sales CRM	Allow Access	

<https://admin.private.zscaler.com/#authPolicy>

Slide notes

The rules will be re-ordered in the list to reflect the new order that you specified. As with other policy criteria, a best practice is to list the most specific rules at the top of the list.

To manage Timeout Policy rules, click **Timeout Policy**.

Slide 74 - Slide 74

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left sidebar, there are icons for Dashboard, Diagnostics, Live Logs, Search, and Zscaler App. The main content area is titled 'Timeout Policy'. It features a table with columns: Rule Order, Name, Timeouts, and Actions. A message at the top says 'Click Add Rule to create a new policy rule'. Below this, a section titled 'Default Rule' shows a single row with the following details:

Rule Order	Name	Timeouts	Actions
	Default_Rule	AUTHENTICATION TIMEOUT 7 Day(s) CRITERIA SEGMENT GROUPS Any Segment Group AND IDP CONFIGURATION Any SAML attribute from any IdP AND CLIENT TYPES Any Client Type	IDLE CONNECTION TIMEOUT Default Edit Click Box

A callout box with a blue border and white background points to the 'Edit' icon in the 'Actions' column of the first row. The callout box contains the text 'Click to Edit the Default Rule'.

Slide notes

There is a single, default Timeout Policy rule by default, which you can edit by clicking the **Edit** icon.

Slide 75 - Slide 75

The screenshot shows the 'Edit Timeout Policy' dialog box. In the 'GENERAL INFORMATION' section, the 'Name' is set to 'Default_Rule'. Under the 'TIMEOUTS' section, the 'Authentication Timeout' is configured to 'Specific interval' with a value of '7 Day(s)'. A message to the user is provided: 'Your access to internal Applications has expired'. A callout box highlights the 'Edit the TIMEOUTS configuration as necessary' text.

Slide notes

The default Timeout Policy rule applies to all users if no other rules have been created, and the default **Authentication Timeout** interval is **7 Days**. You can change this interval to the time you prefer, in **Day(s)**, **Hour(s)**, or even **Minute(s)**.

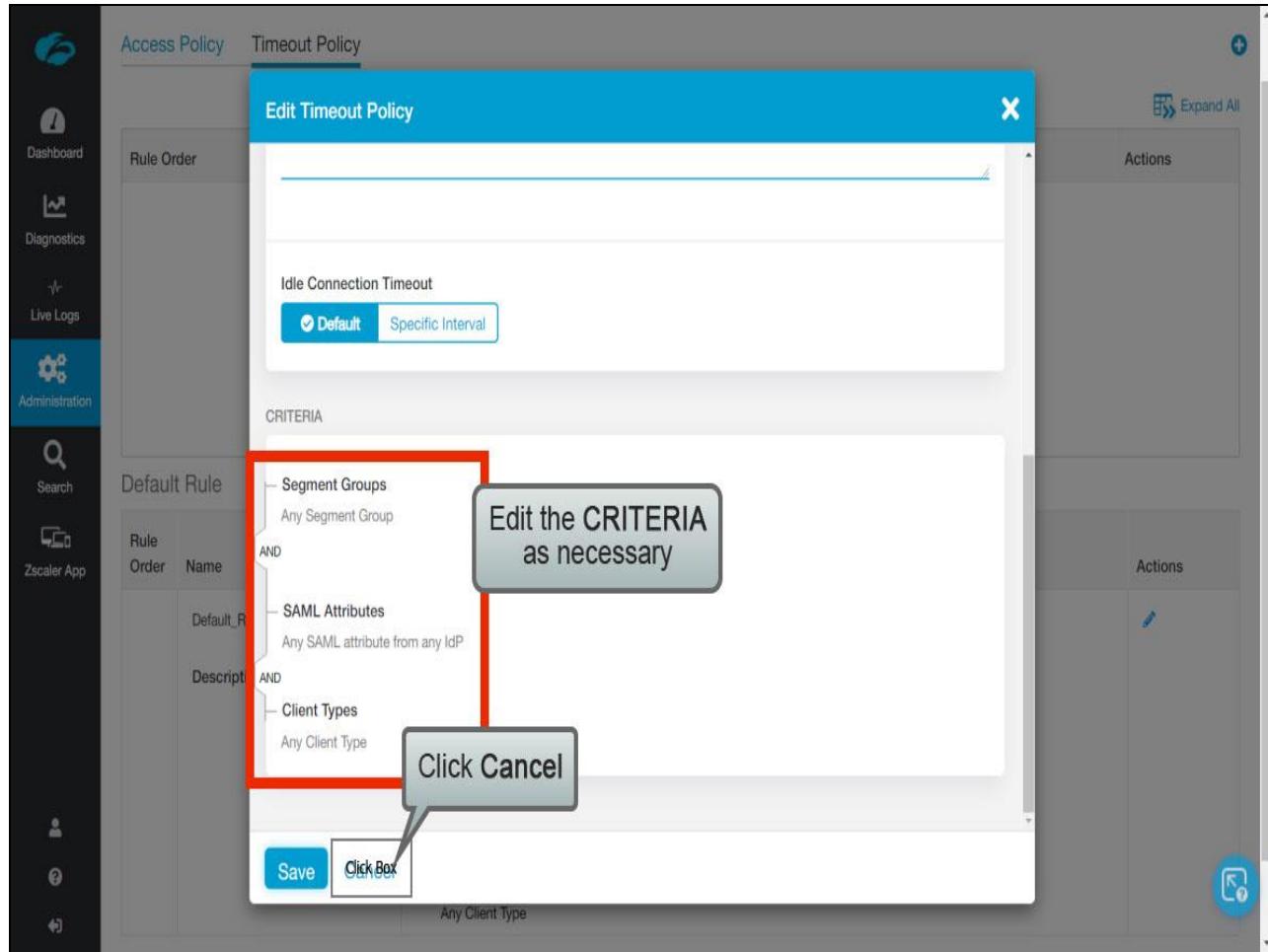
Slide 76 - Slide 76

The screenshot shows the Adobe Captivate interface with the 'Access Policy' tab selected. A modal window titled 'Edit Timeout Policy' is open. In the 'GENERAL INFORMATION' section, the 'Name' field contains 'Default_Rule'. The 'Description' field is empty. In the 'TIMEOUTS' section, the 'Authentication Timeout' dropdown is set to 'Never' (highlighted in blue) and 'Specific interval' is selected. The value '7' is entered in the 'Day(s)' field. Below this, a message to the user reads: 'Your access to internal Applications has expired'. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons. A grey box with the text 'Scroll down...' is overlaid on the right side of the dialog. The background shows a table with columns 'Rule Order', 'Name', and 'Actions'.

Slide notes

Scroll down...

Slide 77 - Slide 77



Slide notes

In the rule **CRITERIA** section, you have the option to adjust the available target criteria (**Segment Groups**, **SAML Attributes**, or **Client Types**).

If you changed the default rule, click **Save**, although in this case we will click **Cancel** to exit without saving any changes.

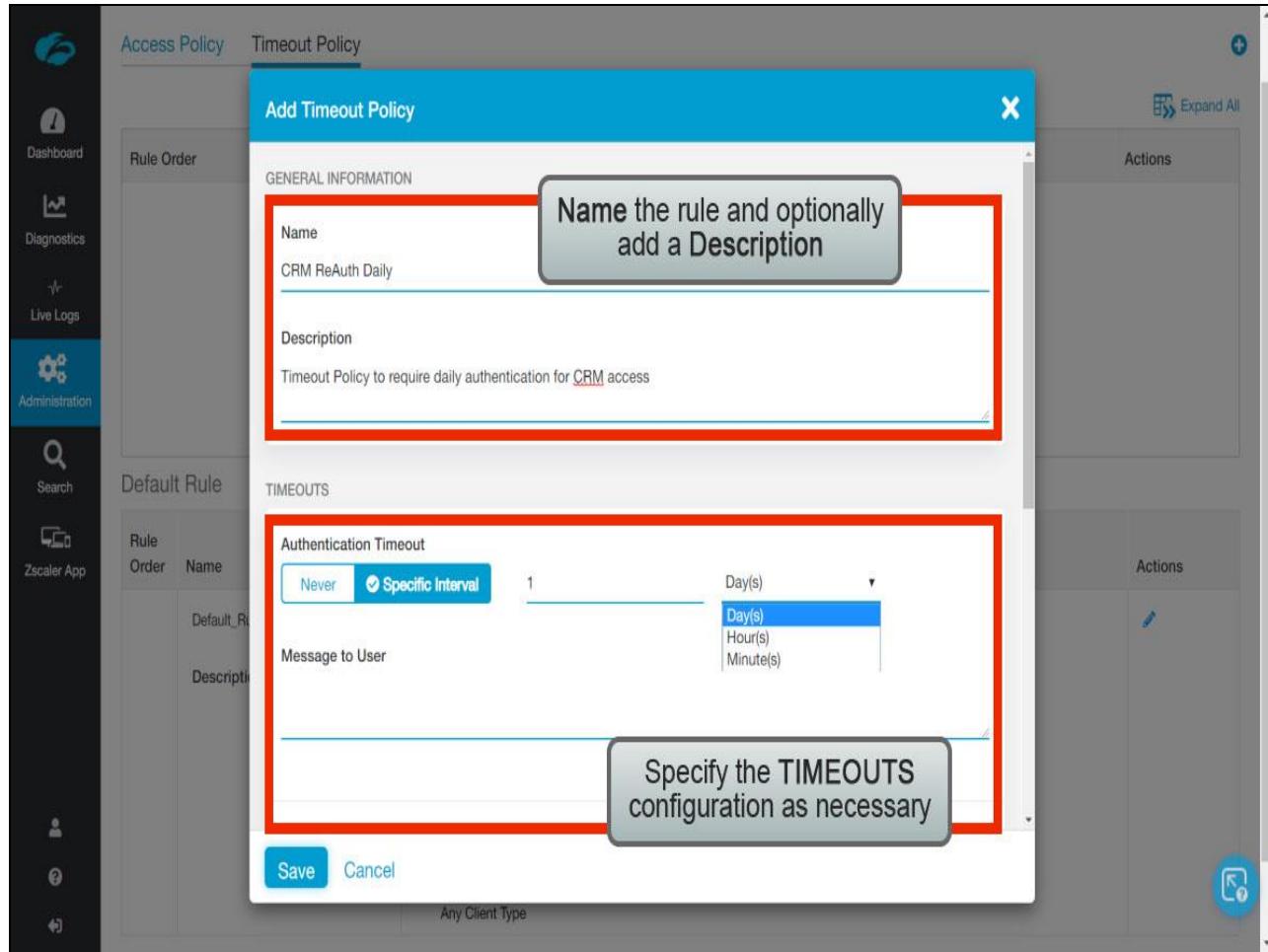
Slide 78 - Slide 78

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Search, and Zscaler App. The main area is titled 'Access Policy' and 'Timeout Policy'. It shows a table for 'Timeouts' with columns for 'Rule Order' and 'Name'. A message says 'Click Add Rule to create a new policy rule'. Below this is a 'Default Rule' section with a table for 'Timeouts' with columns for 'Rule Order', 'Name', and 'Actions'. The 'Description' column for the Default Rule shows the rule structure: AUTHENTICATION TIMEOUT (7 Day(s)), IDLE CONNECTION TIMEOUT (Default), CRITERIA (SEGMENT GROUPS: Any Segment Group, AND: IDP CONFIGURATION: Any SAML attribute from any IdP, AND: CLIENT TYPES: Any Client Type). A callout box with the text 'Click the + icon to add a custom rule' points to the '+' icon in the top right corner of the rule list area.

Slide notes

To add a new Timeout Policy rule, click the + icon at top right, ...

Slide 79 - Slide 79



Slide notes

...and configure the new rule as required. Give the rule a **Name** and optionally a **Description**, then in the **TIMEOUTS** section specify the **Authentication Timeout** value, ...

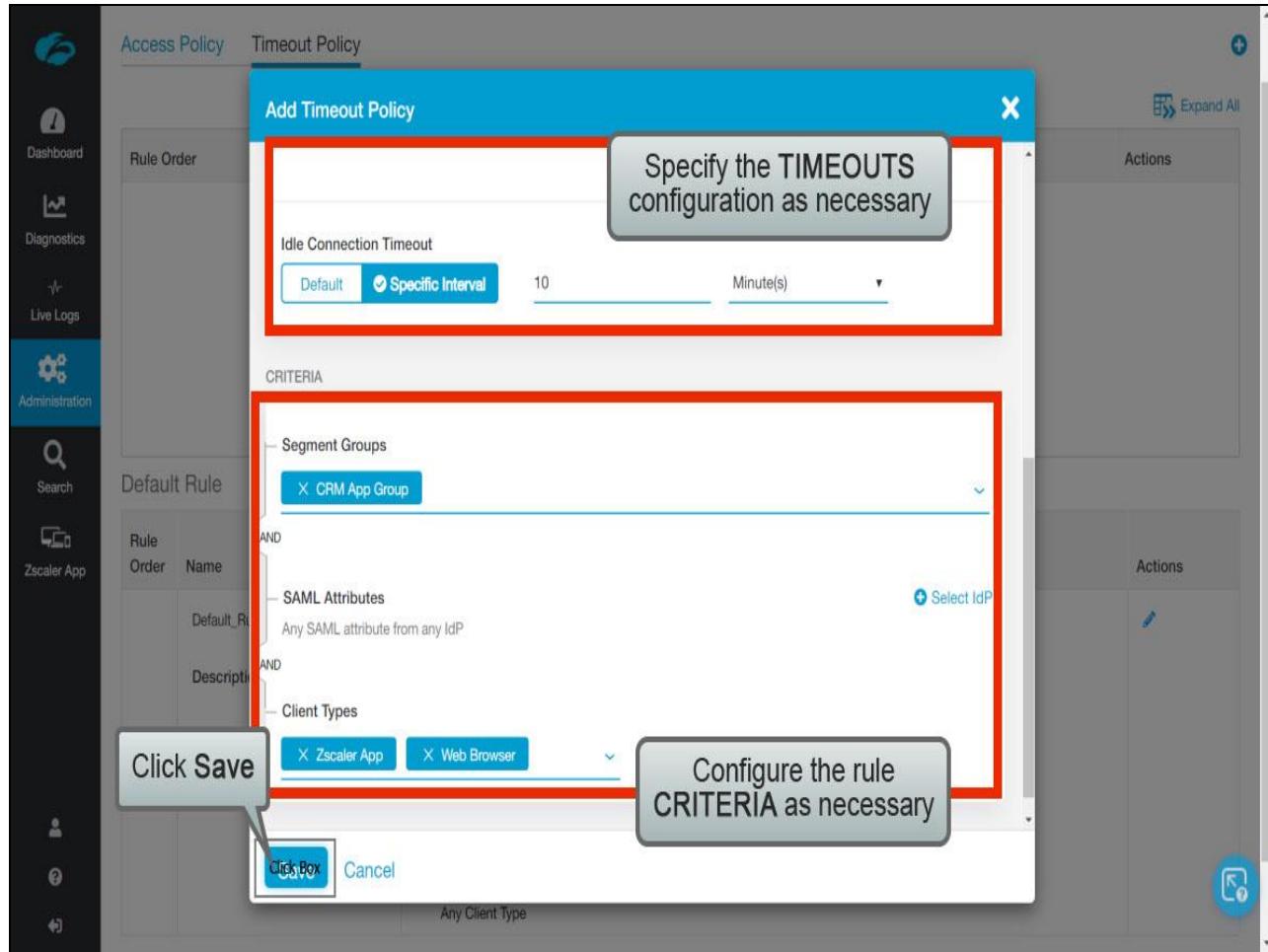
Slide 80 - Slide 80

The screenshot shows the Zscaler Access Policy interface. On the left, there's a sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for 'Access Policy' and 'Timeout Policy'. A modal window titled 'Add Timeout Policy' is open. It has a 'GENERAL INFORMATION' section with 'Name' set to 'CRM ReAuth Daily' and 'Description' set to 'Timeout Policy to require daily authentication for CRM access'. Below this is a 'TIMEOUTS' section with a red box around it. Inside the red box, there's an 'Authentication Timeout' field where 'Never' is selected and 'Specific Interval' is checked, with '1 Day(s)' entered. A callout bubble points to this field with the text 'Specify the TIMEOUTS configuration as necessary'. Another callout bubble points to a 'Message to User' field with the text 'Scroll down...'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

Slide notes

Scroll down...

Slide 81 - Slide 81



Slide notes

...and set a new **Idle Connection Timeout** value if necessary.

In the **CRITERIA** section, you can target the rule by; **Segment Groups**, **SAML Attributes**, or **Client Types**. Once the rule is configured, click **Save**.

Slide 82 - Slide 82

The screenshot shows the Adobe Captivate interface with the 'Timeout Policy' tab selected. On the left, a sidebar includes icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and user profile.

Access Policy **Timeout Policy**

Default Rule

Rule Order	Name	Timeouts	Actions
1	CRM ReAuth Daily	AUTHENTICATION TIMEOUT 1 Day(s) IDLE CONNECTION TIMEOUT 10 Minute(s)	

Default Rule

Rule Order	Name	Timeouts	Actions
	Default_Rule	AUTHENTICATION TIMEOUT 7 Day(s) IDLE CONNECTION TIMEOUT Default	

Description:

- SEGMENT GROUPS: Any Segment Group
- AND
- IDP CONFIGURATION: Any SAML attribute from any IdP
- AND
- CLIENT TYPES: Any Client Type

Timeout policy saved

Slide notes

Slide 83 - Slide 83

The screenshot shows the Zscaler Admin interface under the 'Administration' tab. On the left sidebar, there are icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, and Zscaler App.

The main content area is titled 'Timeout Policy'. It displays a table of rules:

Rule Order	Name	Timeouts	Actions	
1	CRM ReAuth Daily	AUTHENTICATION TIMEOUT 1 Day(s)	IDLE CONNECTION TIMEOUT 10 Minute(s)	

Below this is a 'Default Rule' section:

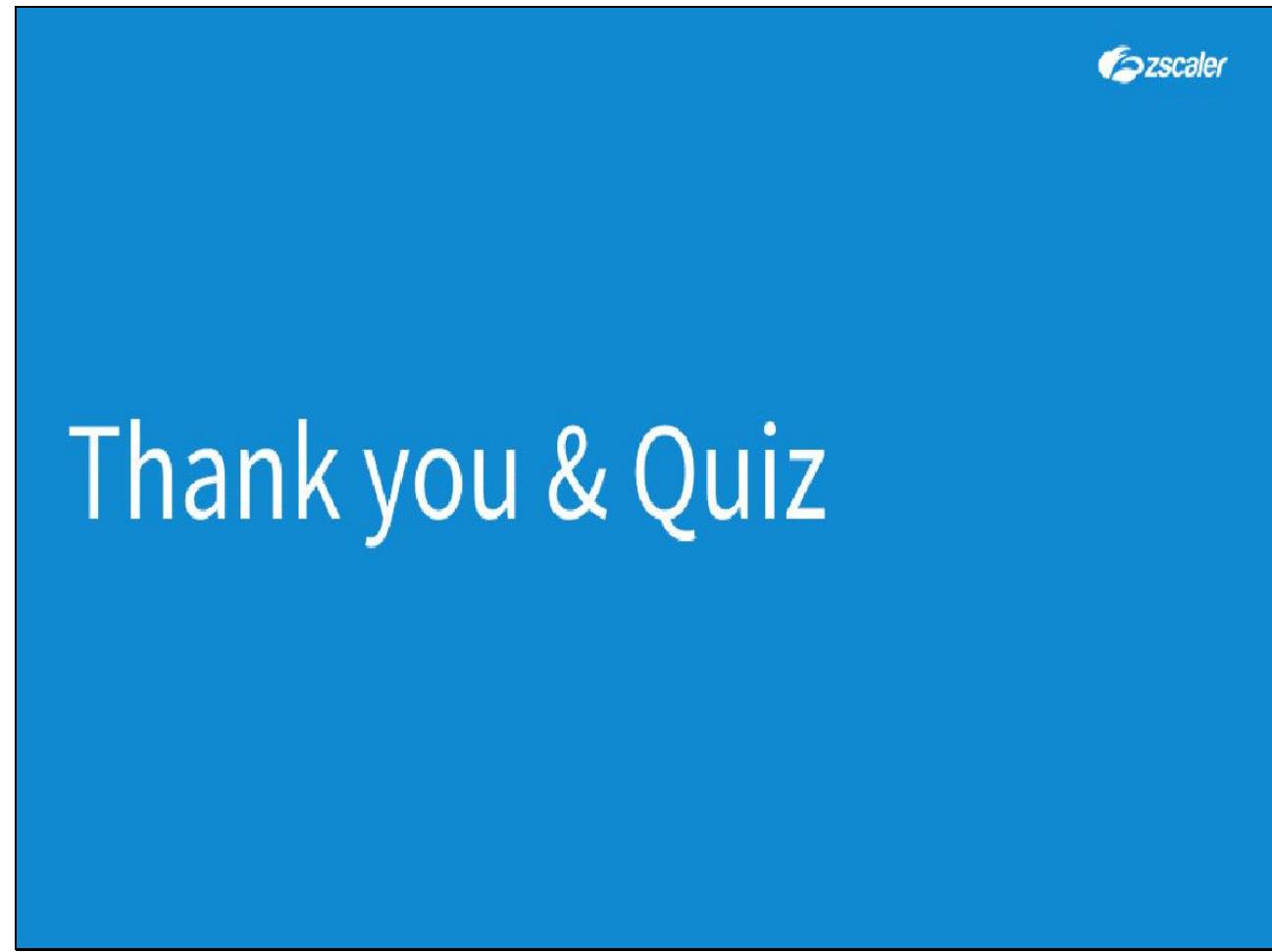
Rule Order	Name	Timeouts	Actions
	Default_Rule	AUTHENTICATION TIMEOUT 7 Day(s) IDLE CONNECTION TIMEOUT Default	
	Description	CRITERIA SEGMENT GROUPS Any Segment Group AND IDP CONFIGURATION Any SAML attribute from any IdP AND CLIENT TYPES Any Client Type	

A red box highlights the 'Actions' column in both tables. A callout bubble with a blue border and white text says 'Edit or Delete Policy Rules'. Another callout bubble with a blue border and white text points to the edit icon in the 'Actions' column of the detailed view table.

Slide notes

Any Timeout Policy rules that you add may be edited or deleted later.

Slide 84 - 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.