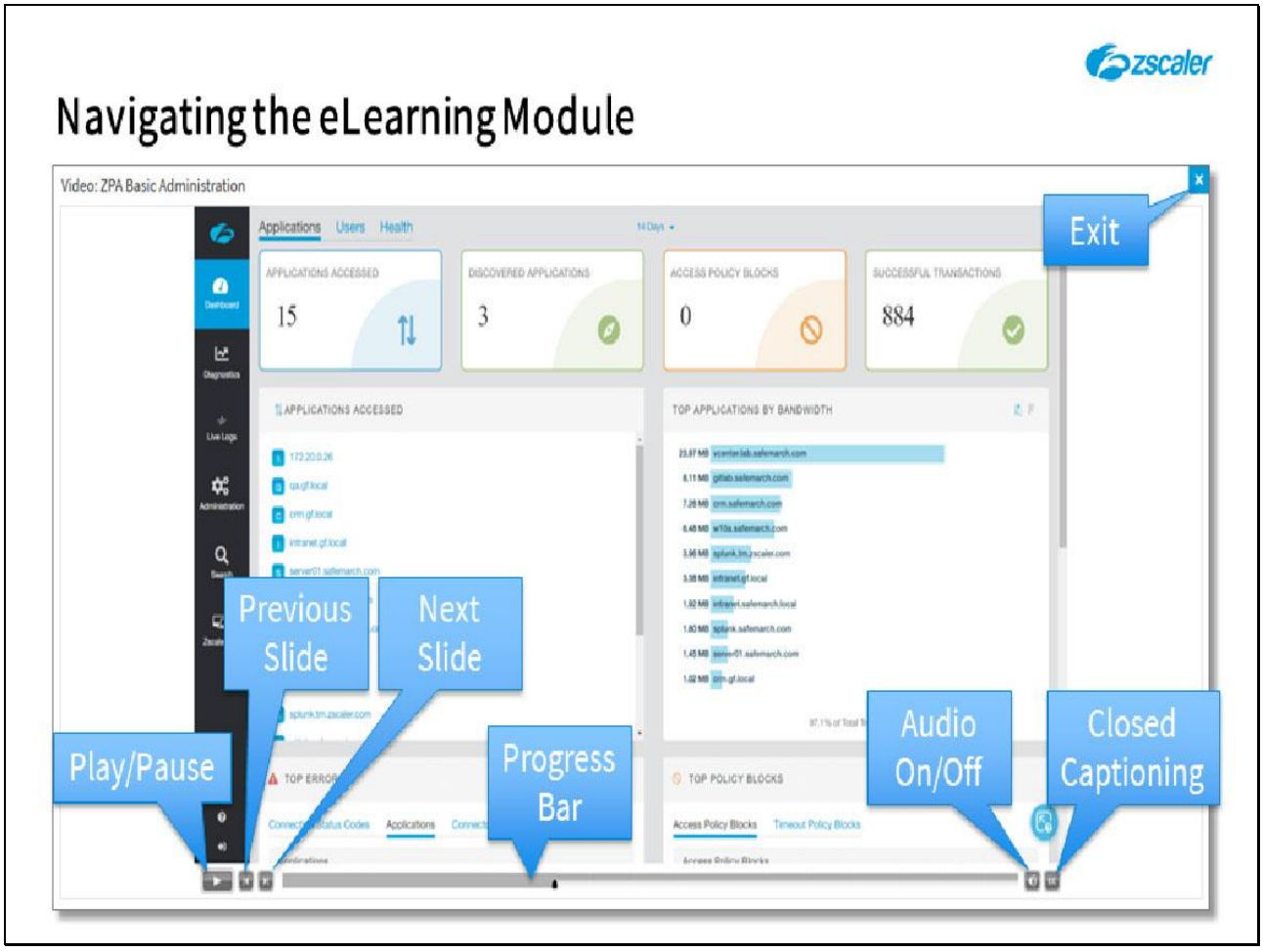
Slide 1 - Zscaler Private Access

Slide notes

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

Slide 2 - Navigating the eLearning Module



Slide notes

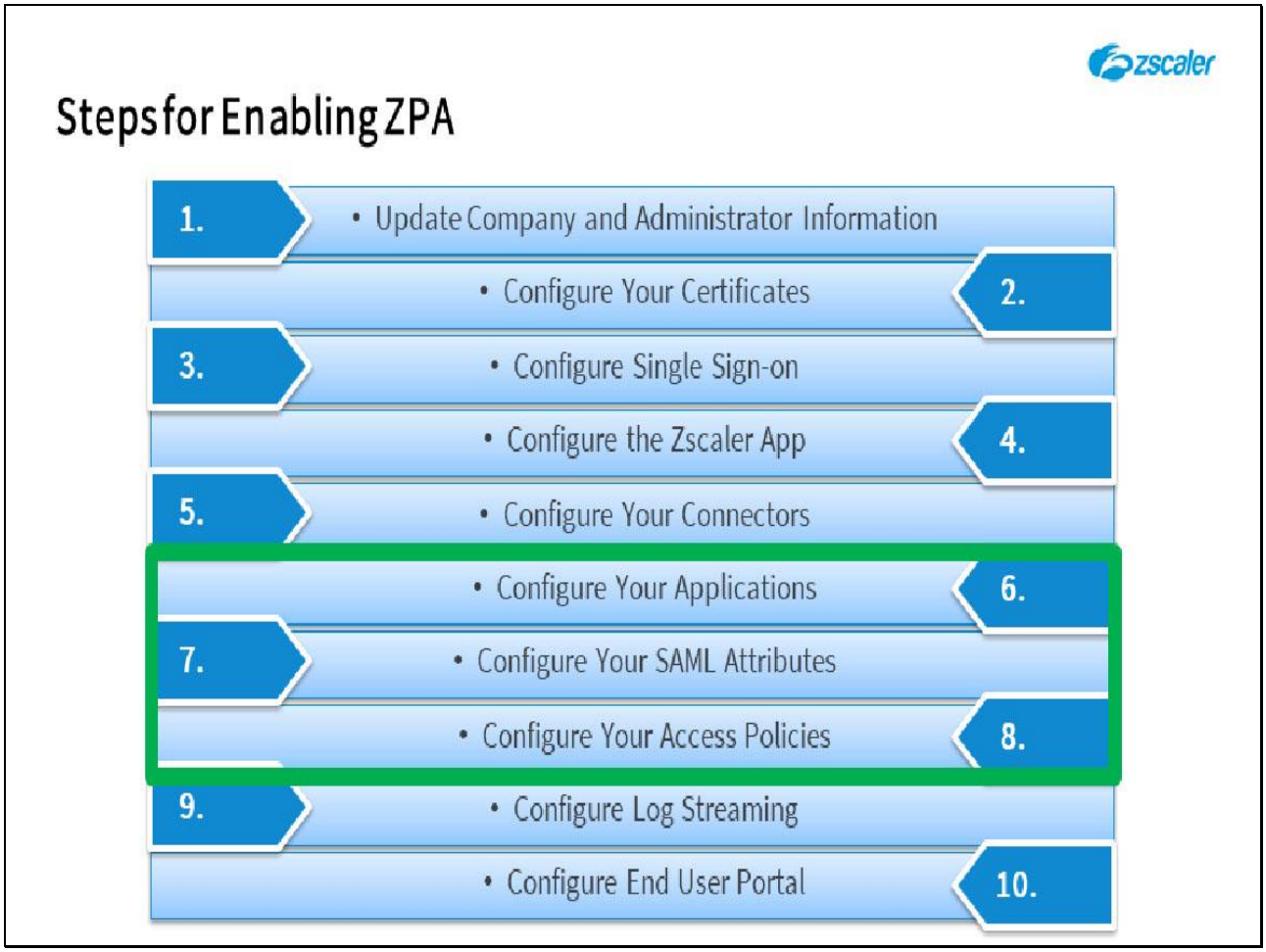
Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous**, and **Next** slide. You can also **Mute** the audio or enable **Closed Captioning** which will cause a transcript of the module to be displayed on the screen. Finally,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

Slide 3 - Agenda

Slide notes

In this module, we will 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.

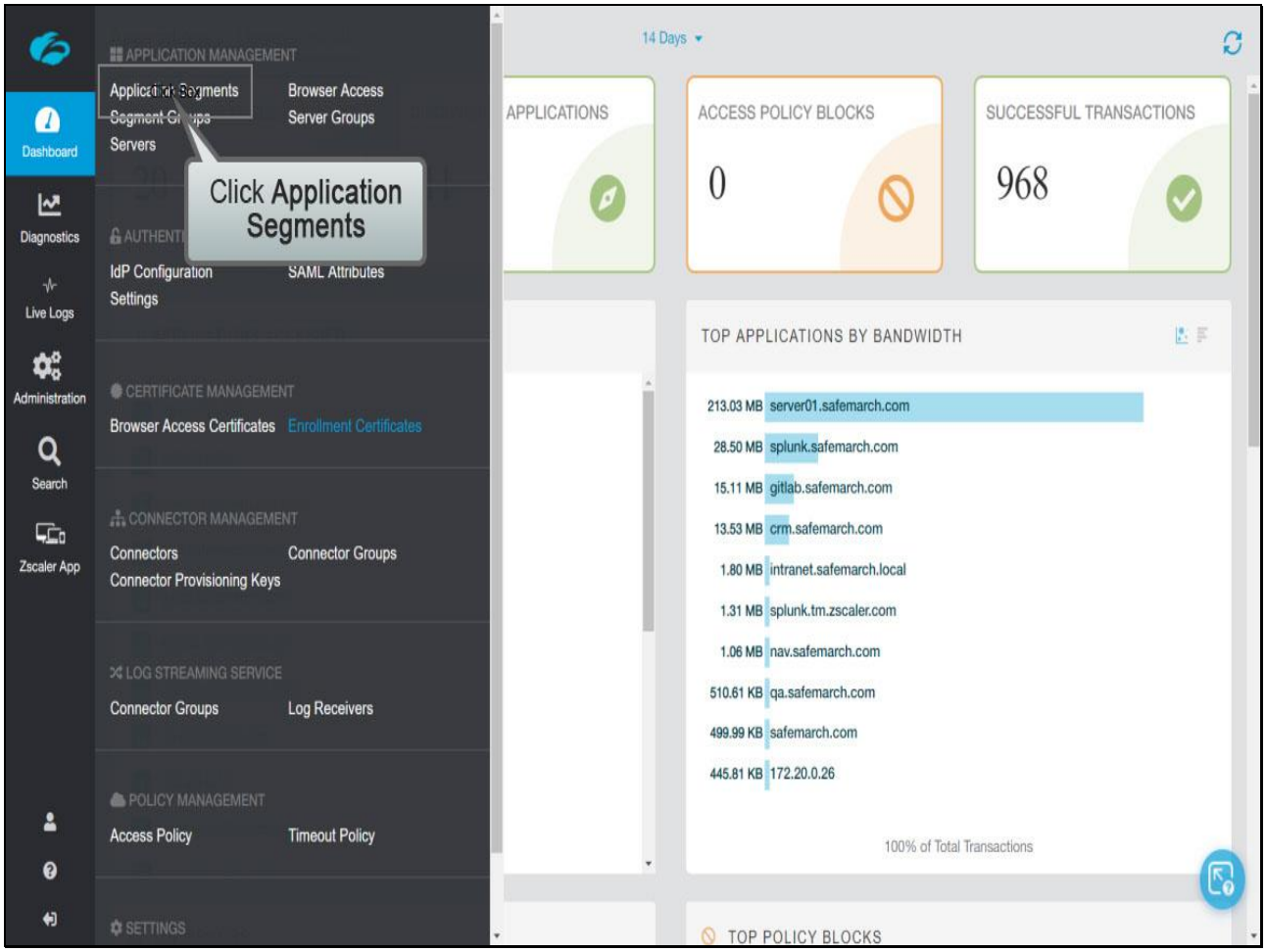
Slide 5 - 7. Configure Your Applications

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.

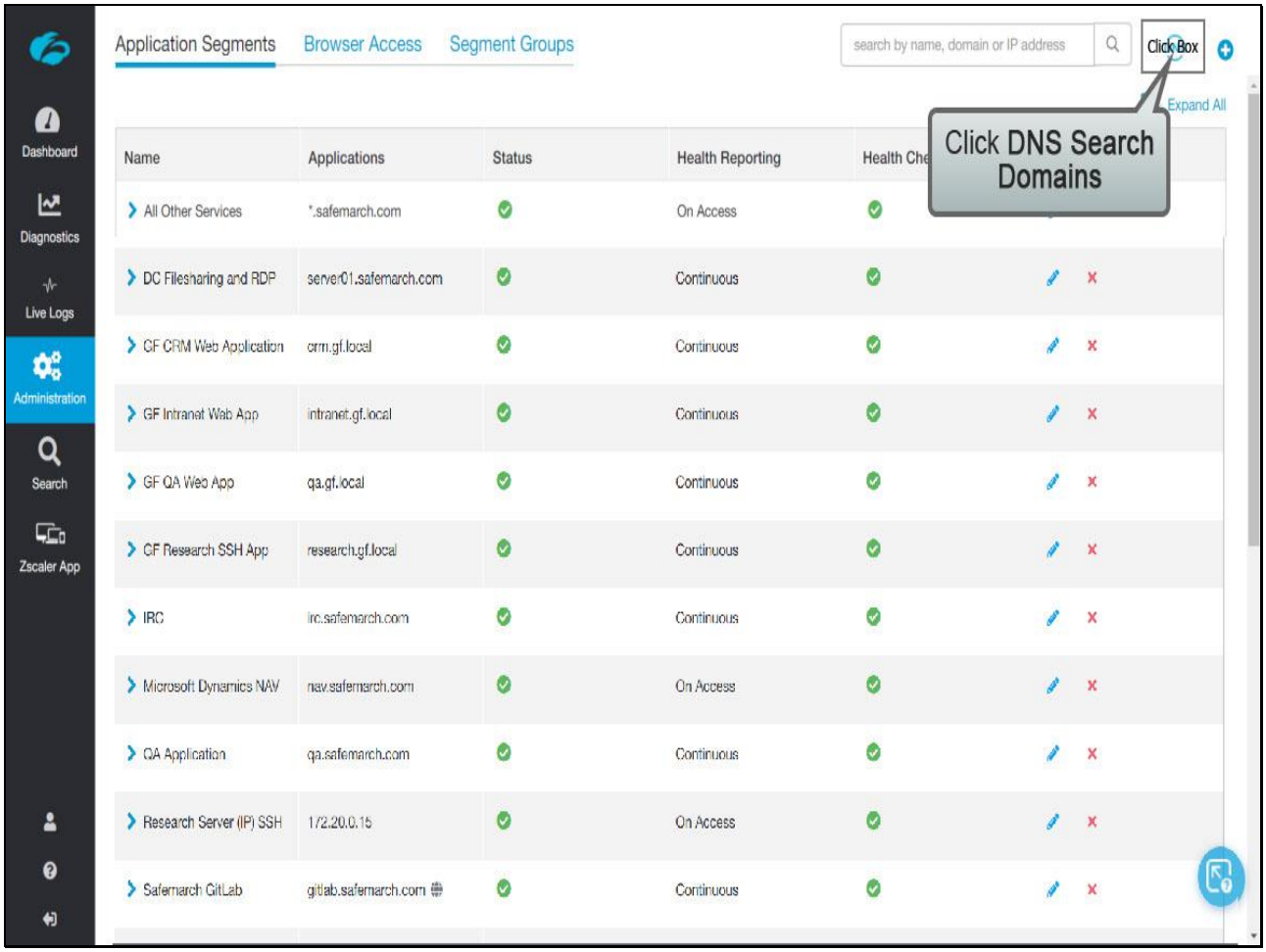
Slide 6 - Slide 6



Slide notes

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

Slide 7 - Slide 7

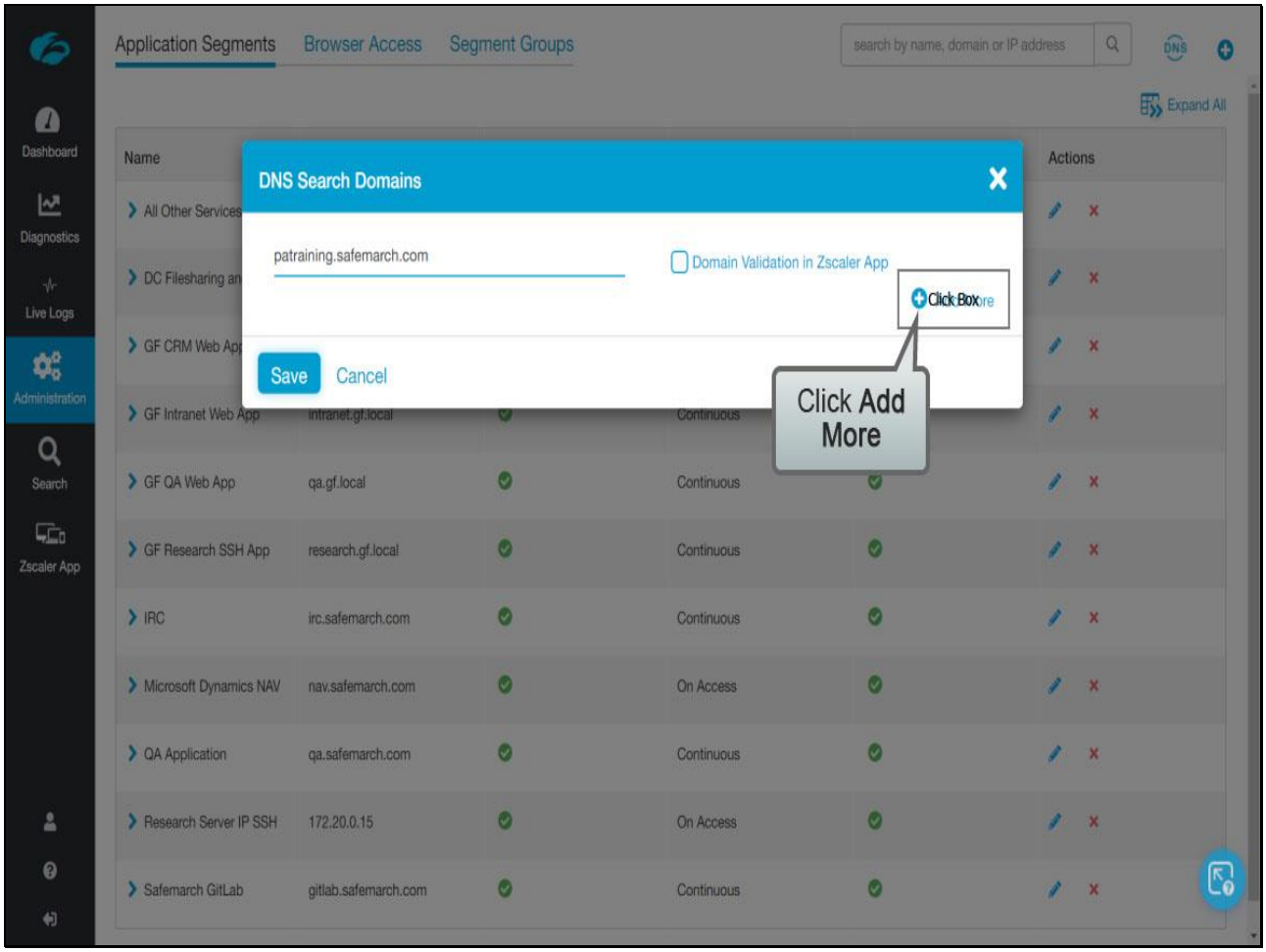


Slide notes

…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, ...

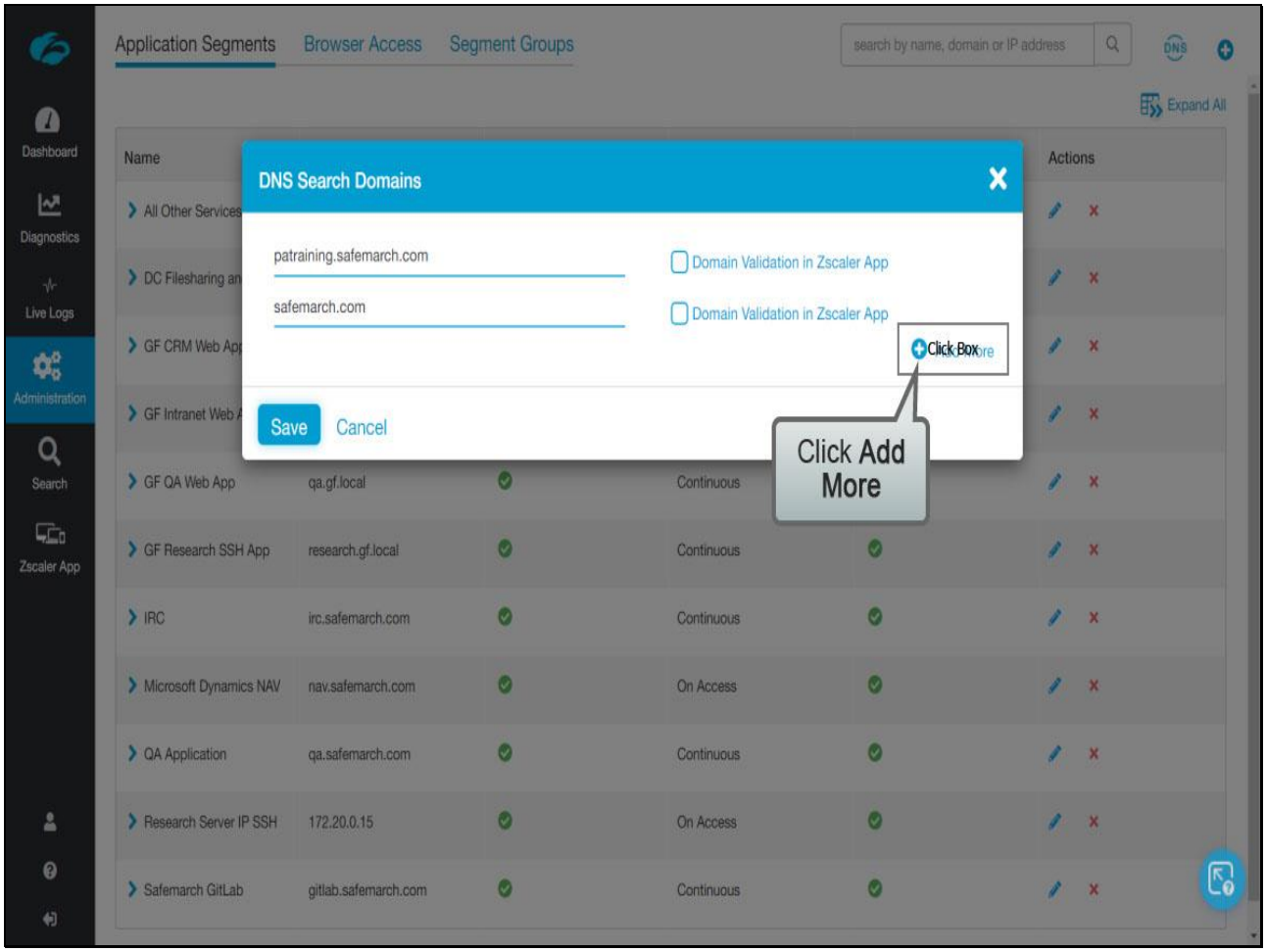
Slide 8 - Slide 8



Slide notes

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

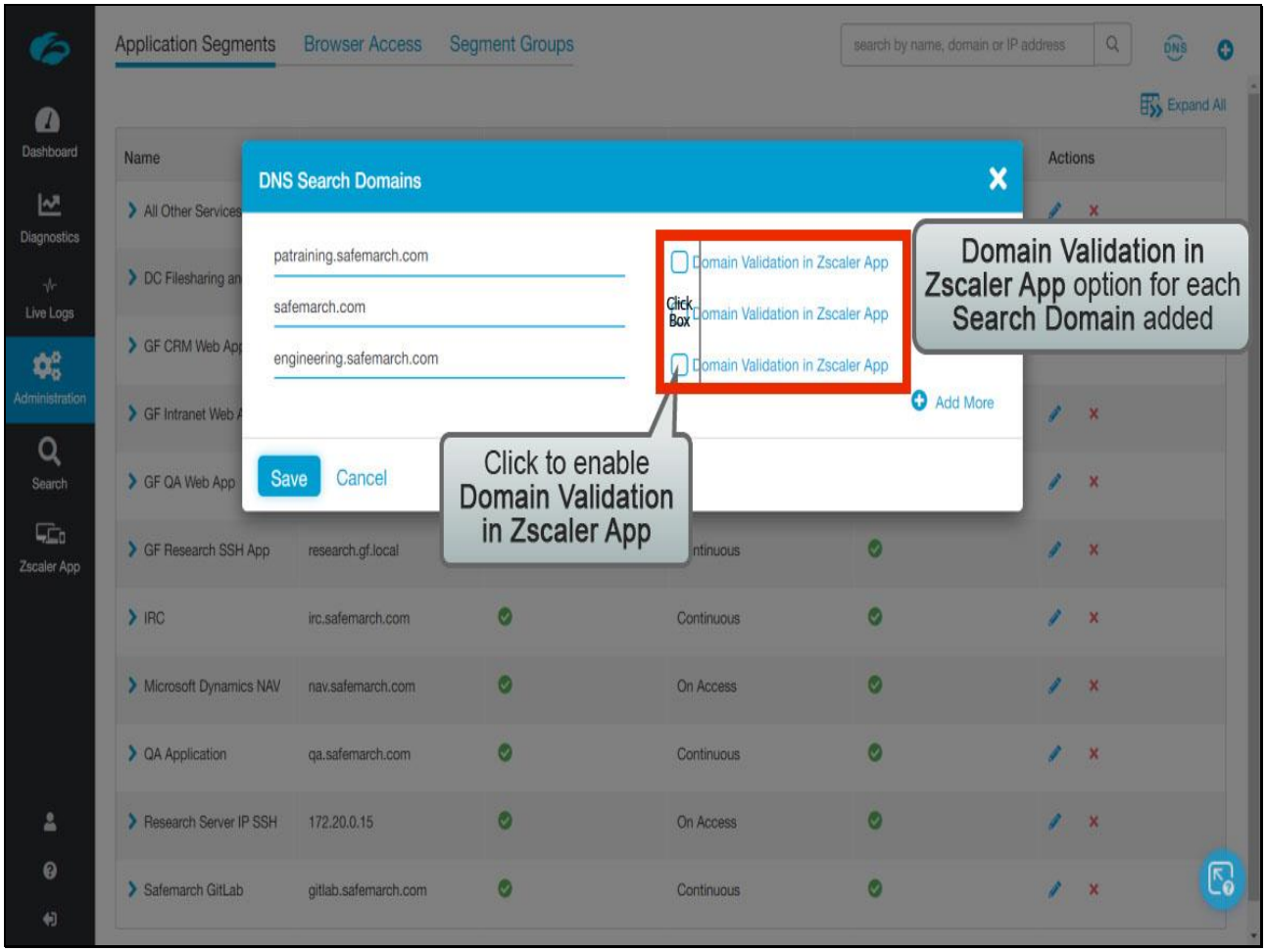
Slide 9 - Slide 9



Slide notes

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

Slide 10 - Slide 10

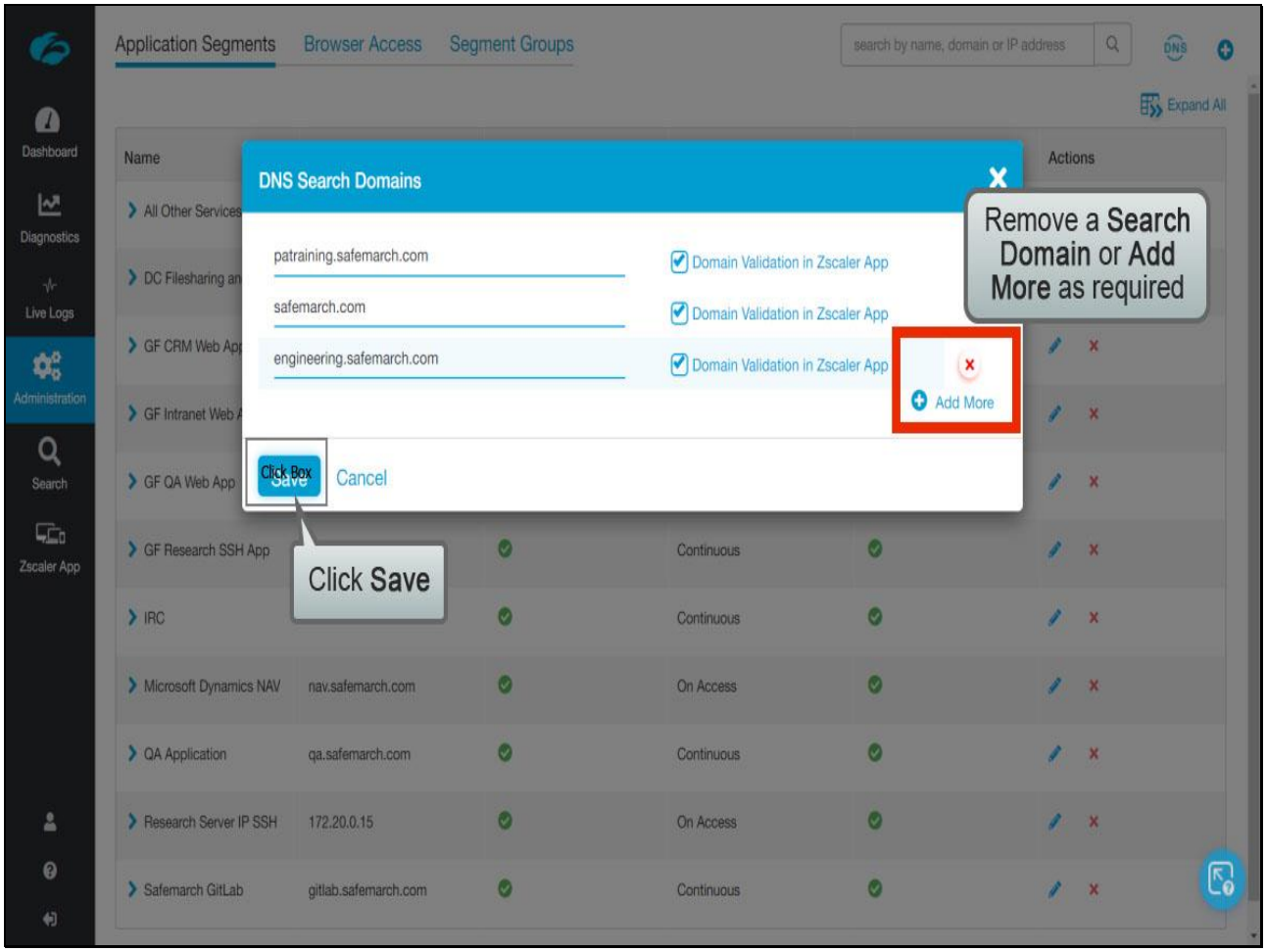


Slide notes

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.

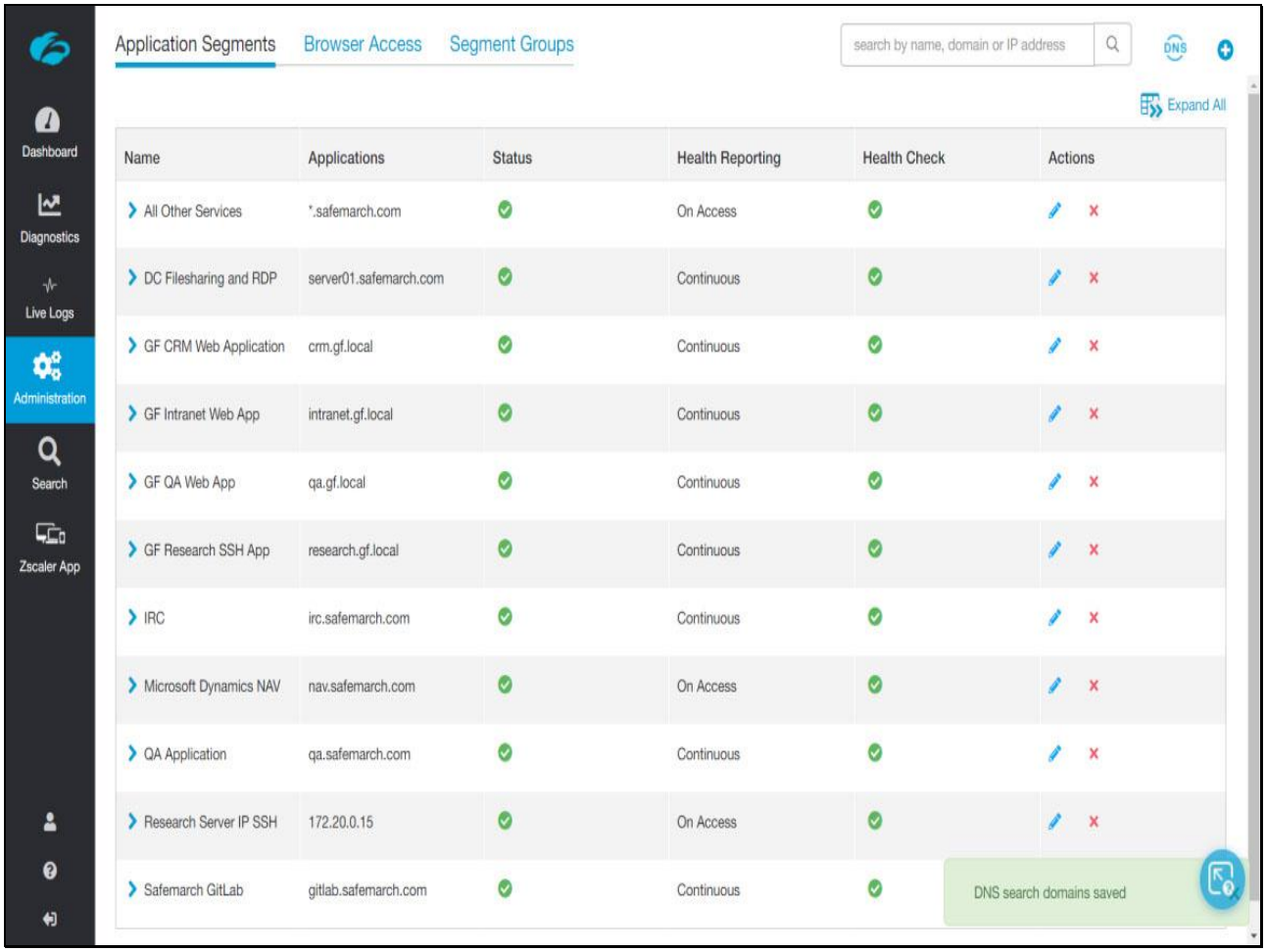
Slide 11 - Slide 11



Slide notes

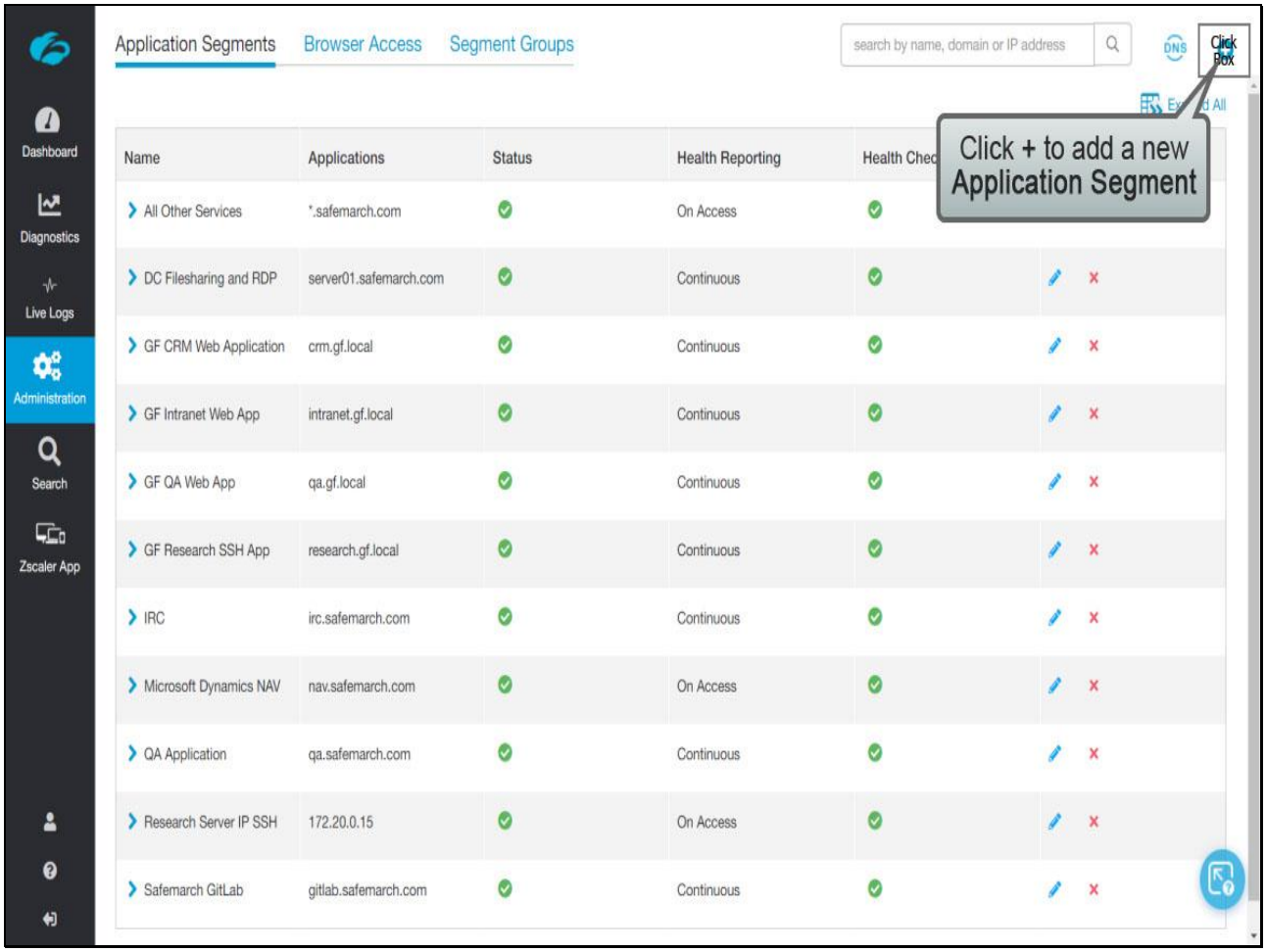
Having added Search Domains, you can subsequently remove them if necessary. Once the configuration is correct, click **Save**.

Slide 12 - Slide 12



Slide notes

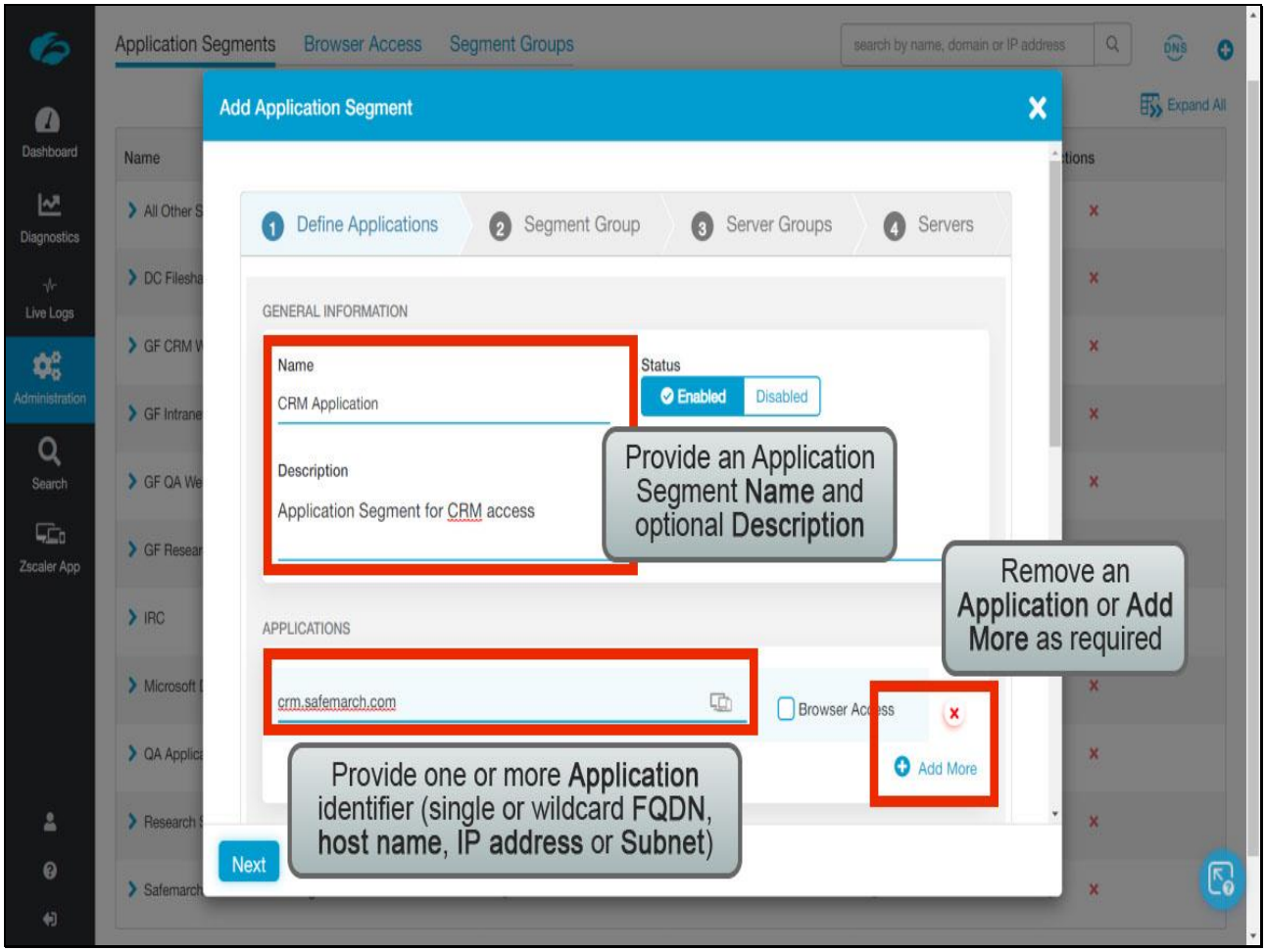
Slide 13 - Slide 13



Slide notes

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

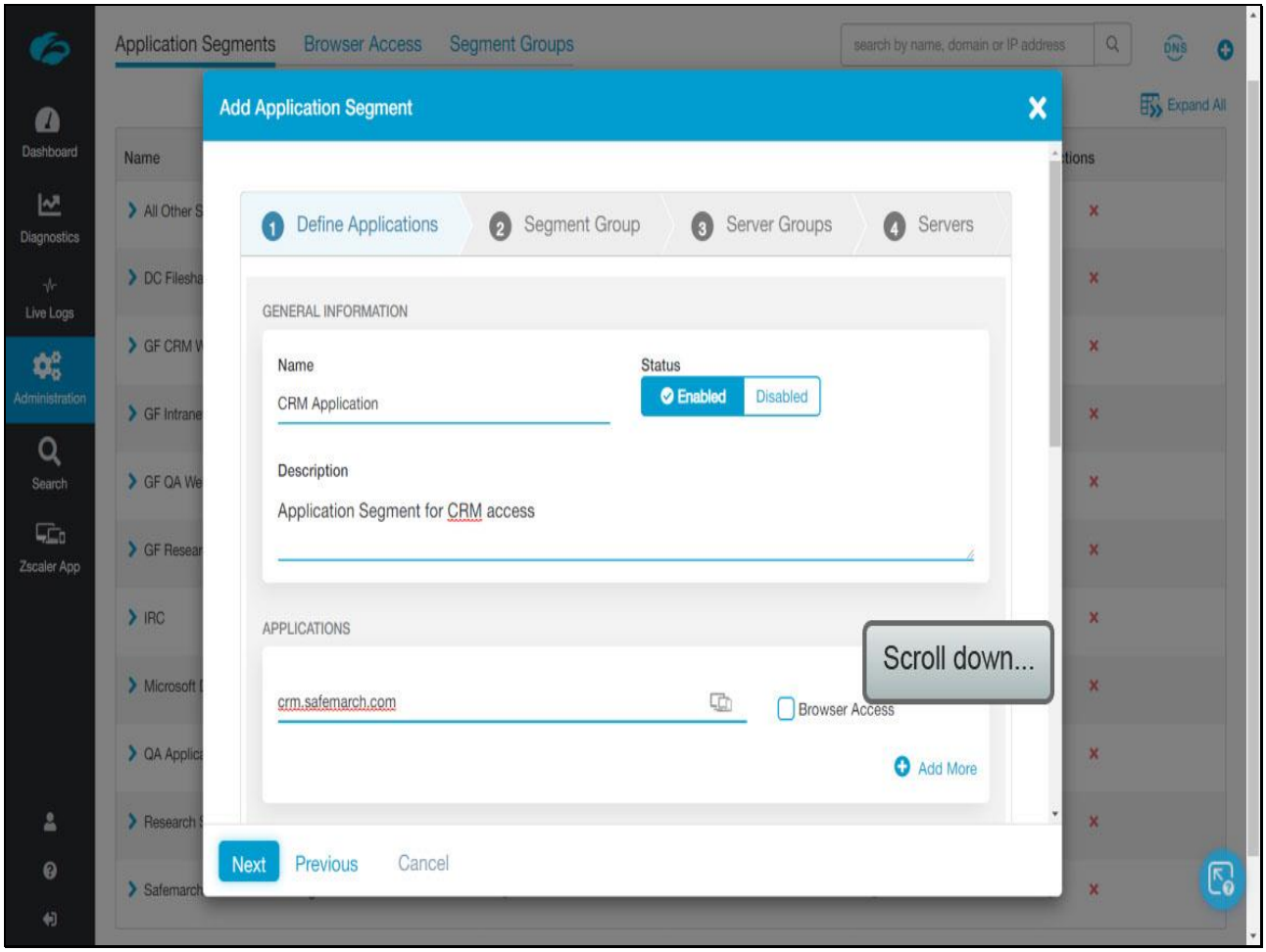
Slide 14 - Slide 14



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.

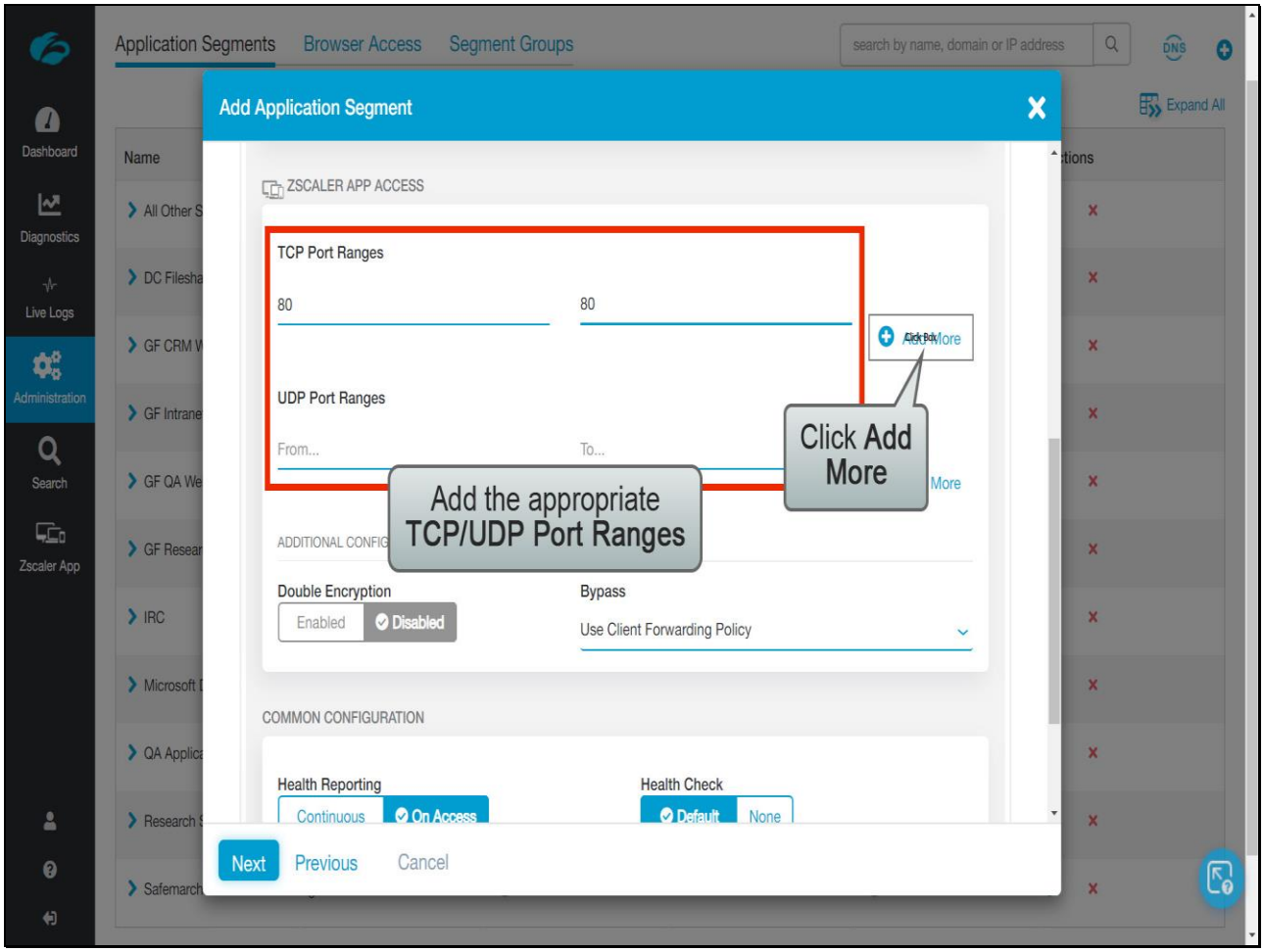
Slide 15 - Slide 15



Slide notes

Scroll down...

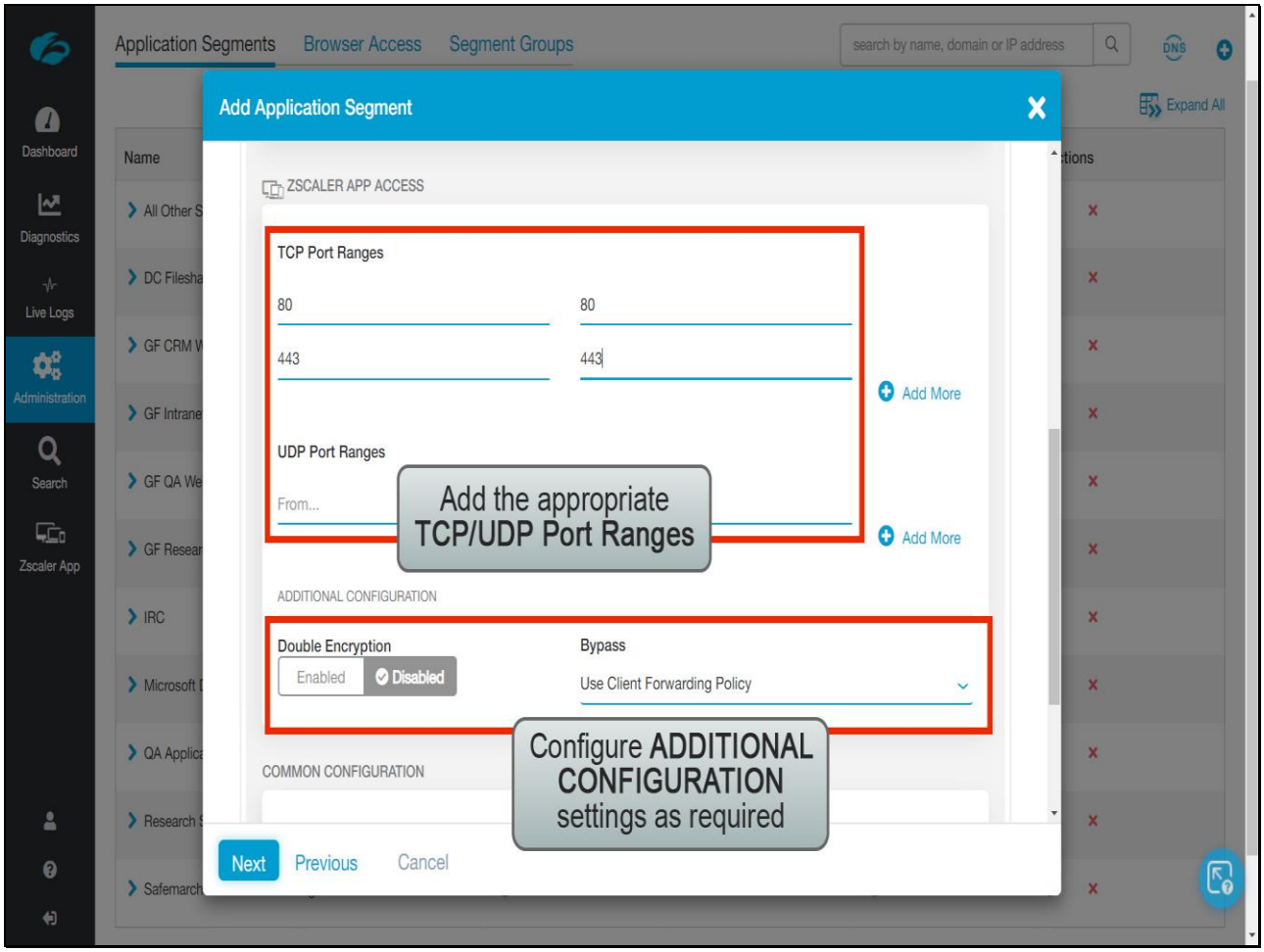
Slide 16 - Slide 16



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

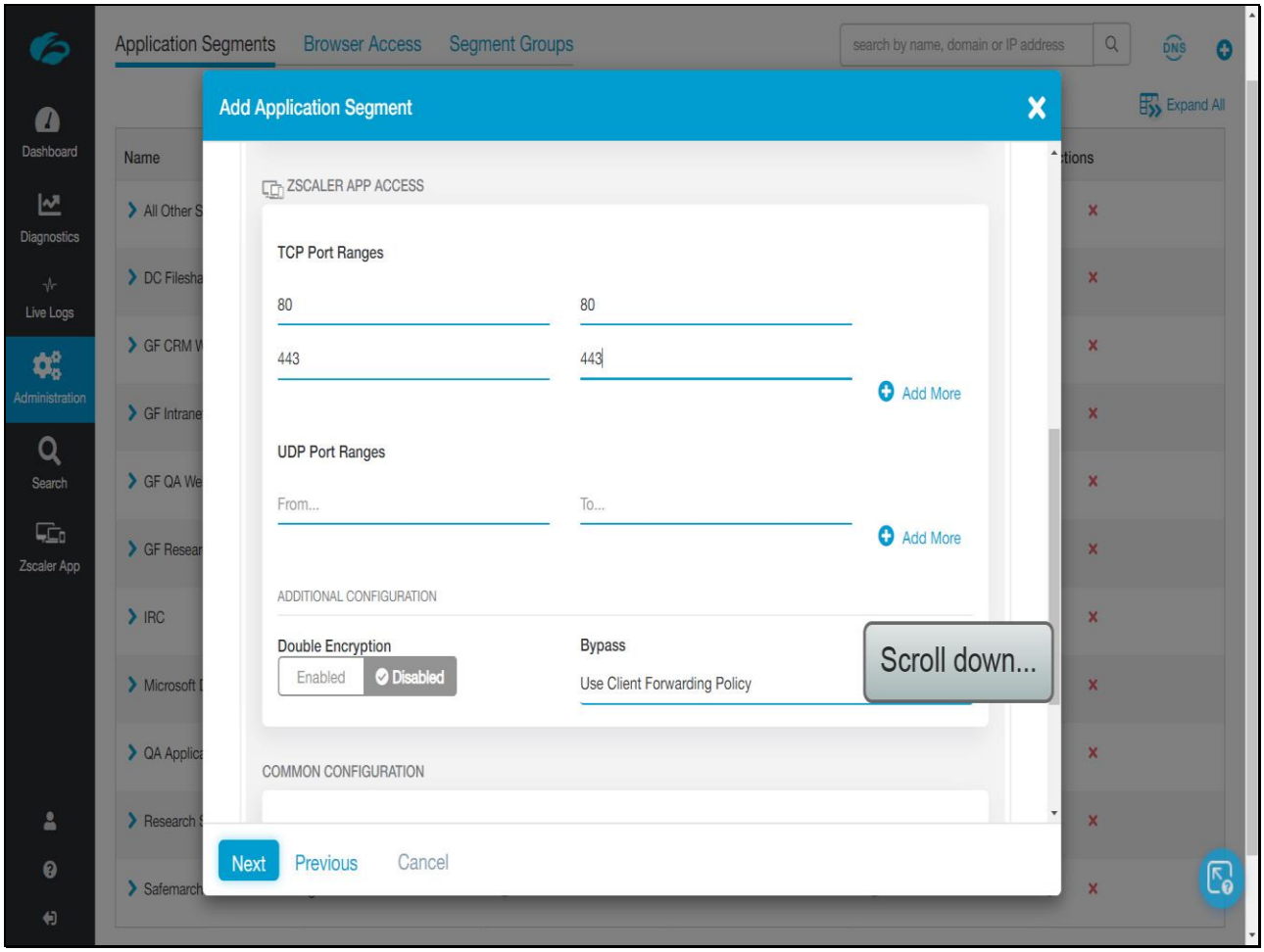


Slide notes

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**.

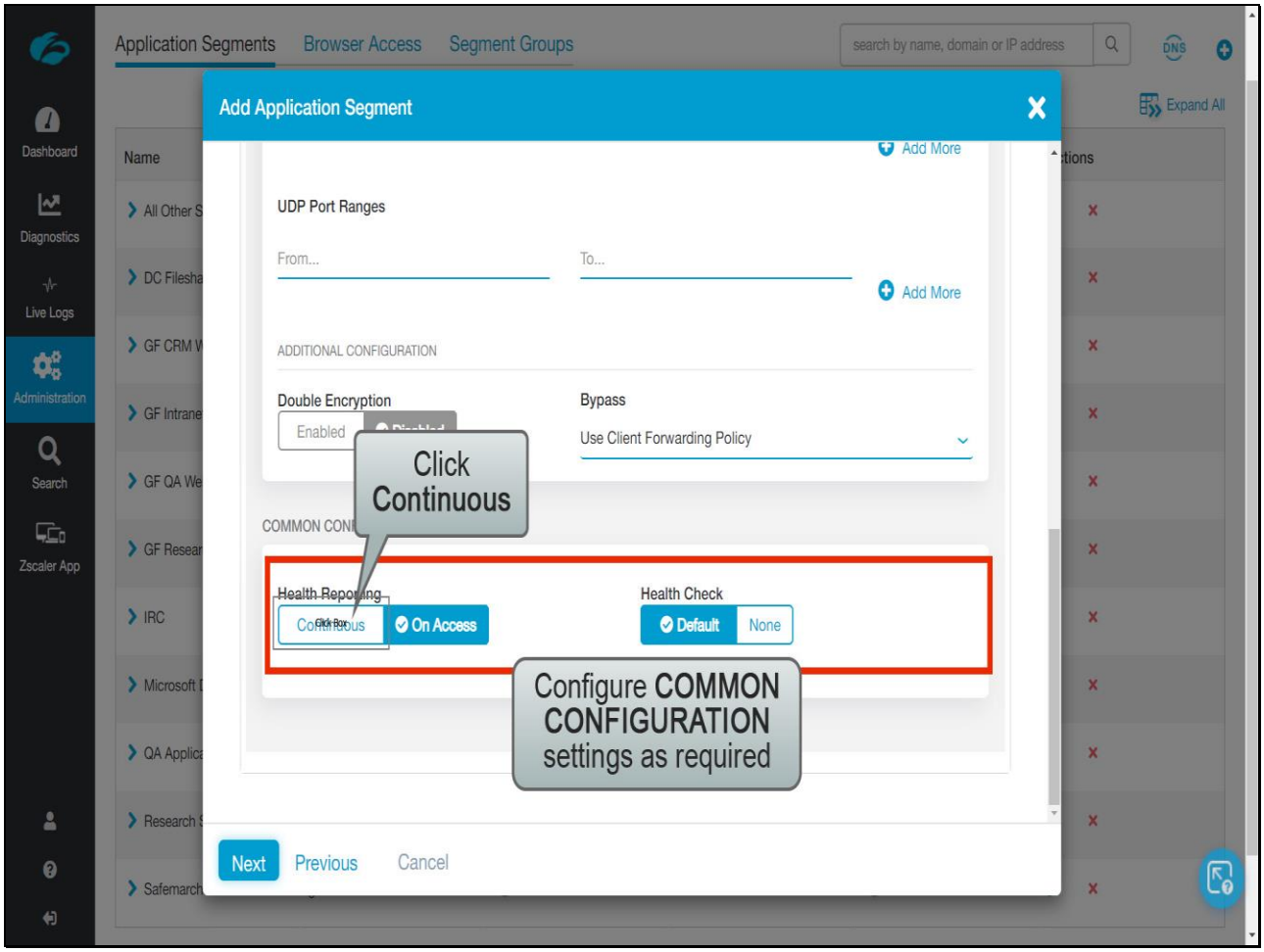
Slide 18 - Slide 18



Slide notes

Scroll down...

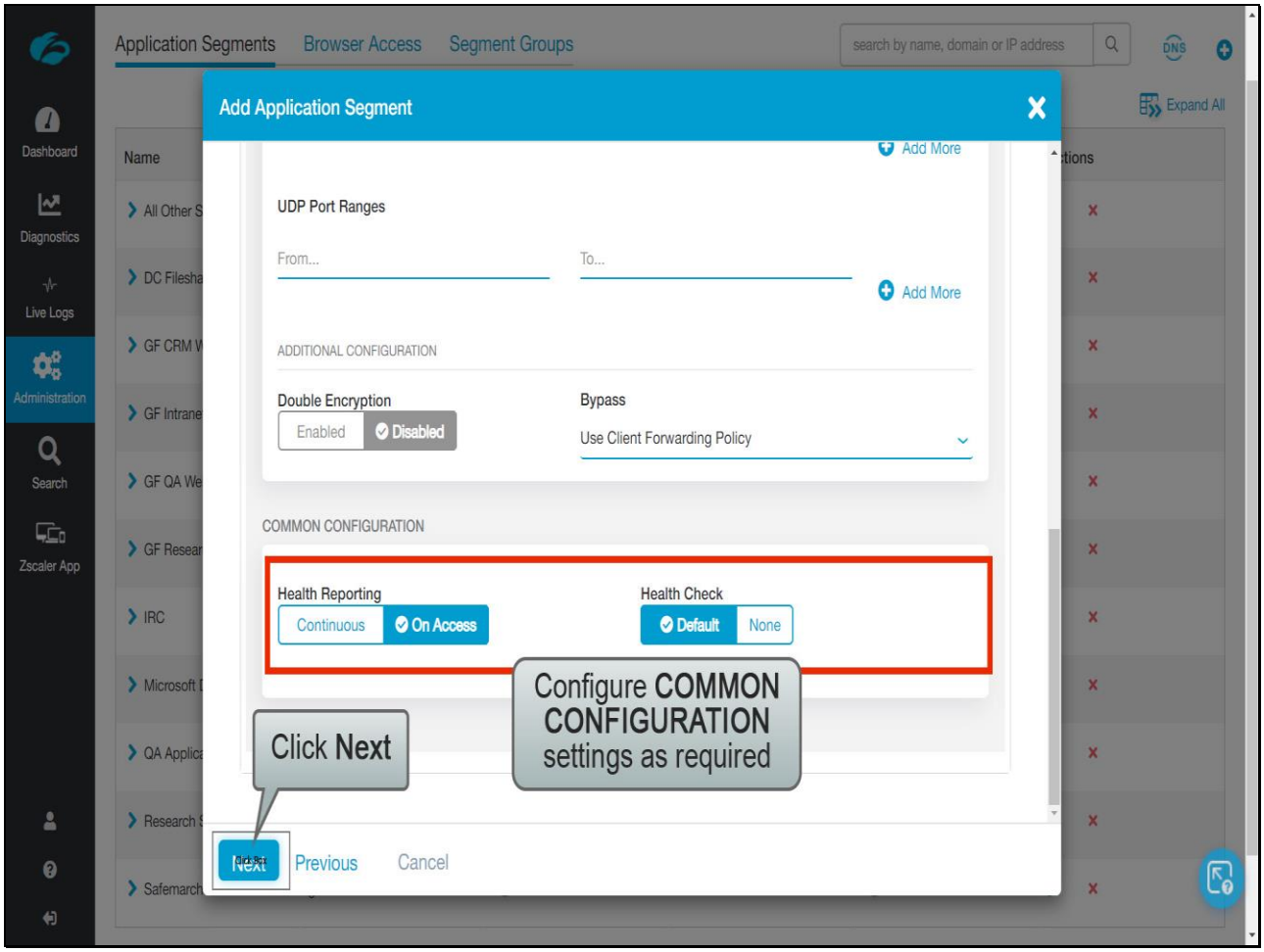
Slide 19 - Slide 19



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**.

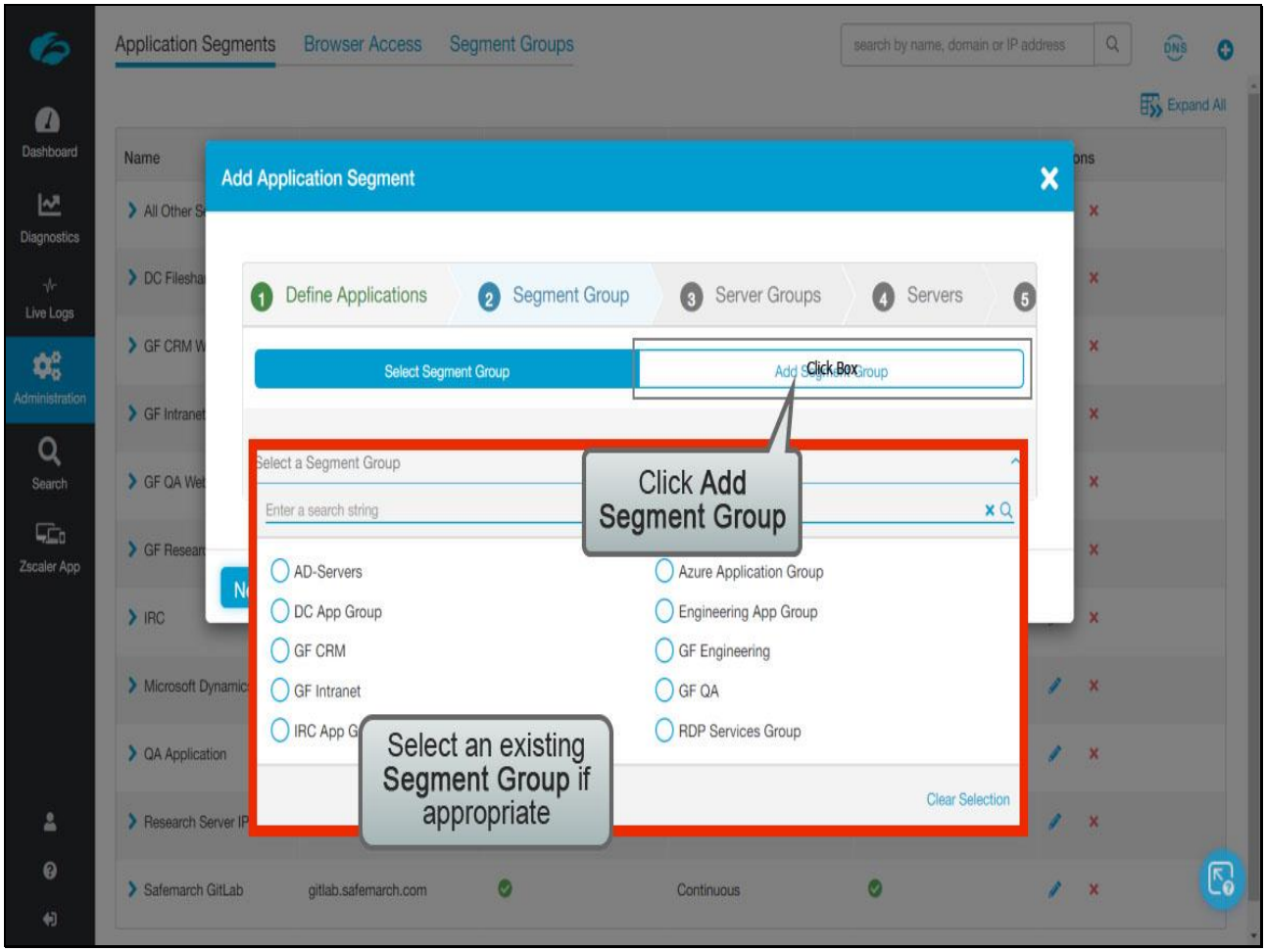
Slide 20 - Slide 20



Slide notes

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

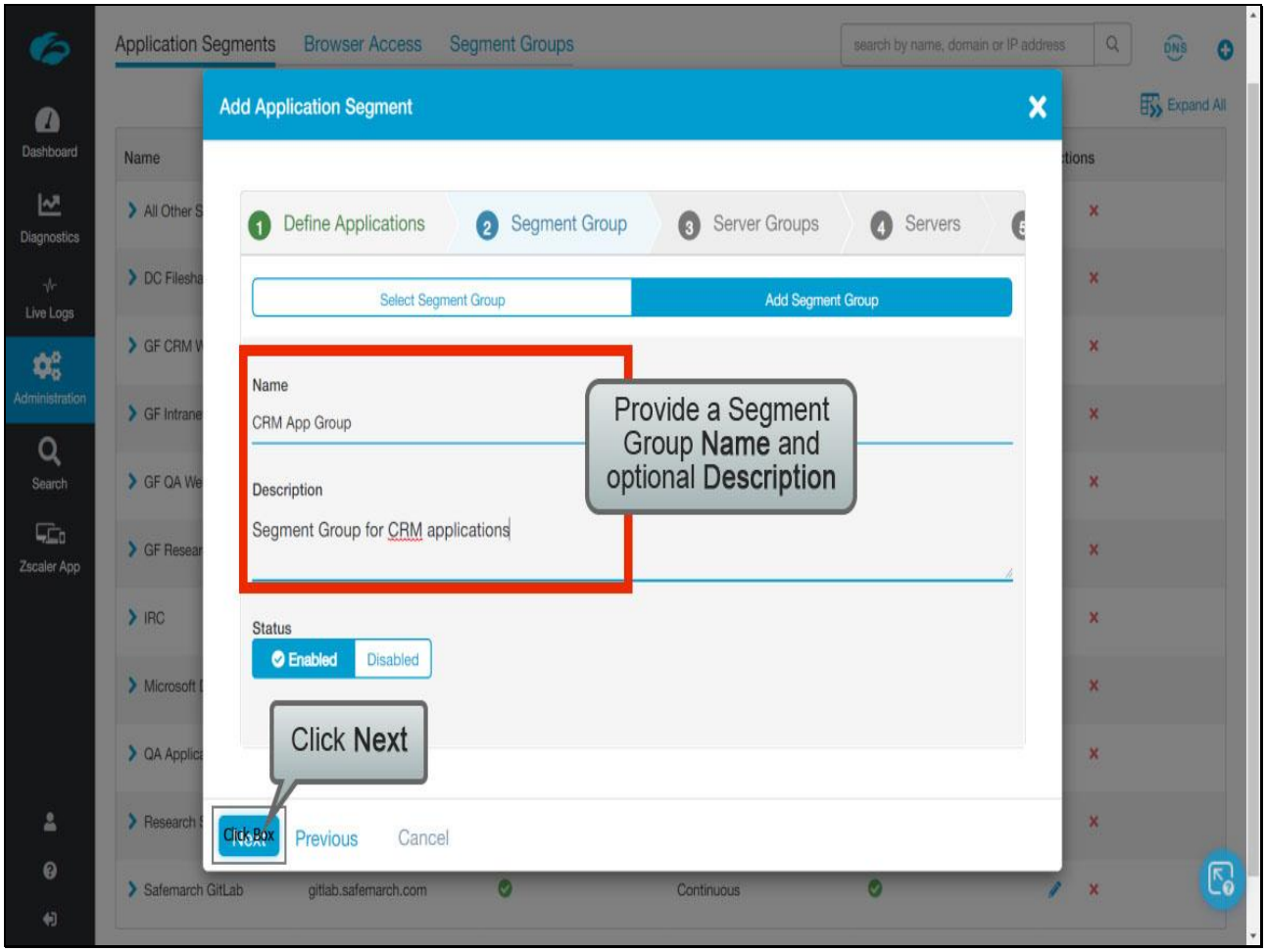
Slide 21 - Slide 21



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**.

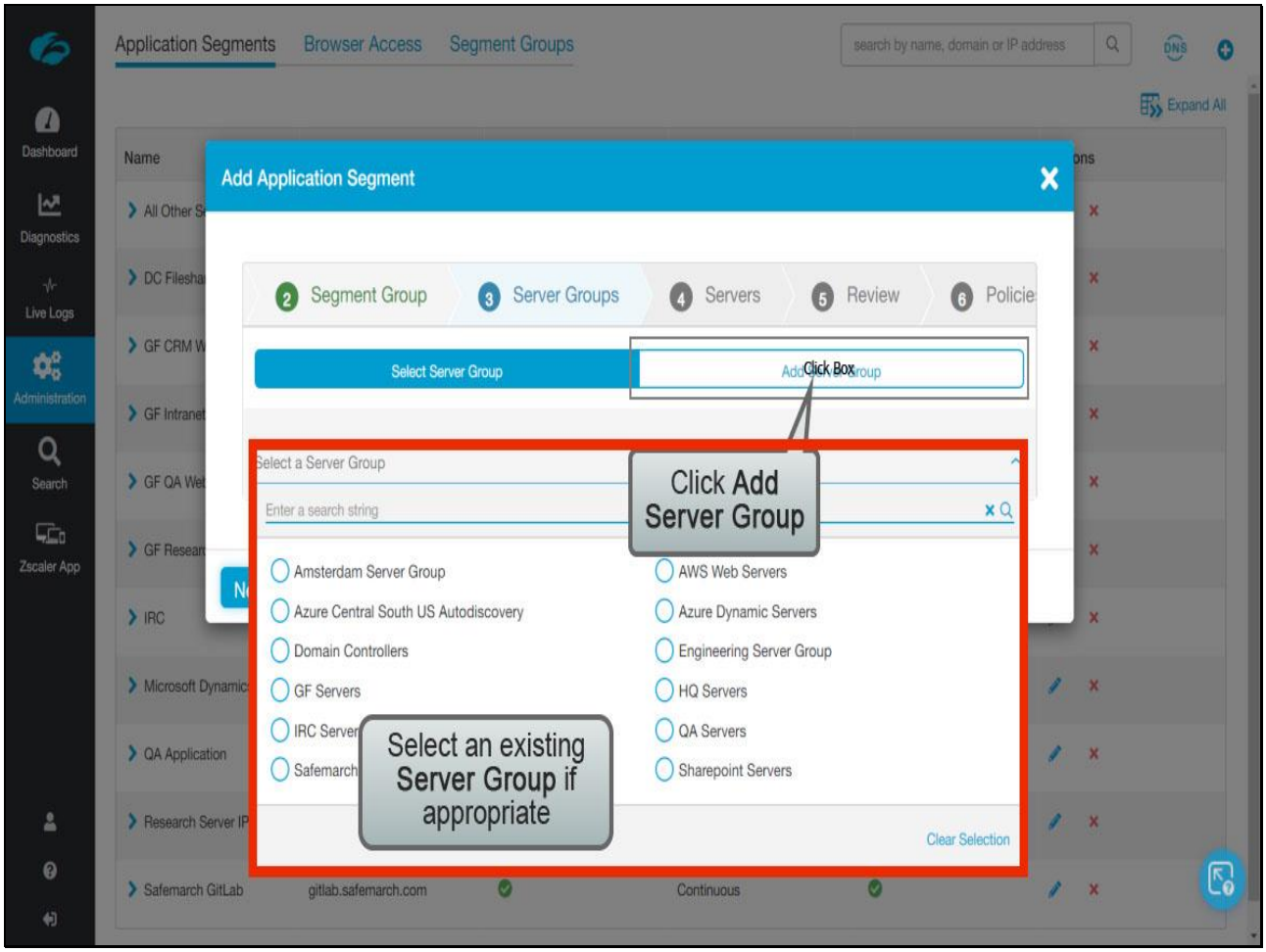
Slide 22 - Slide 22



Slide notes

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

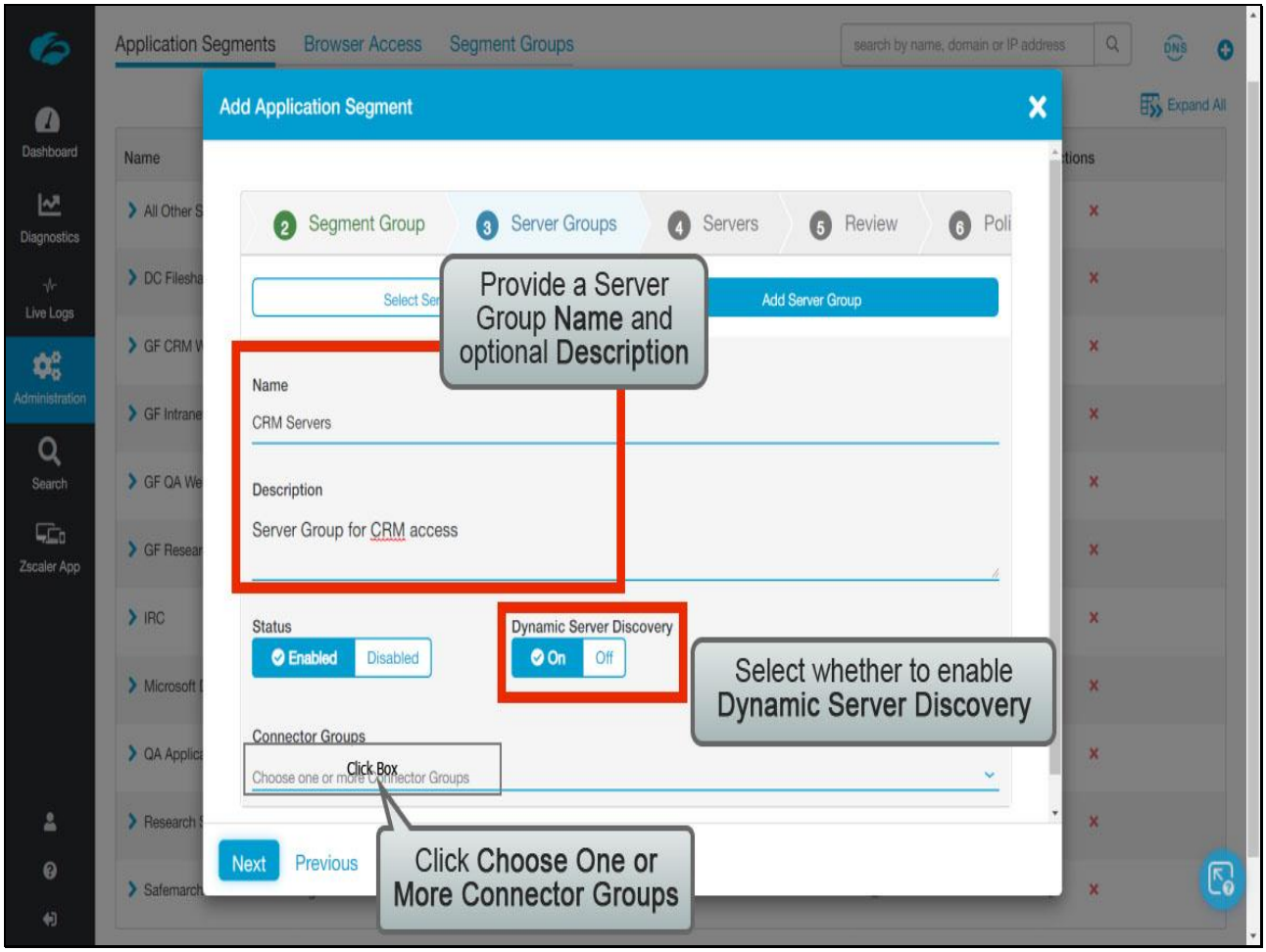
Slide 23 - Slide 23



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

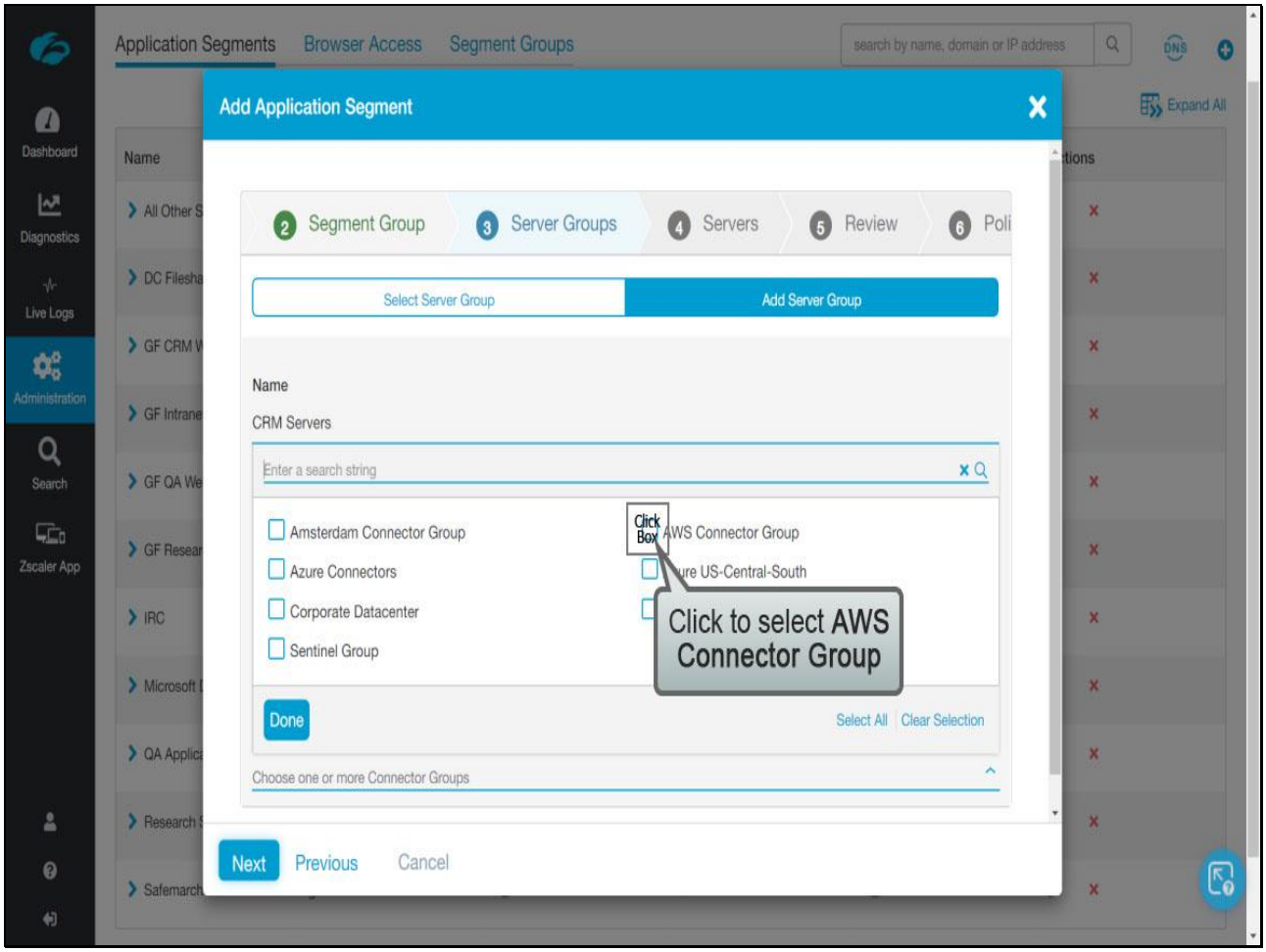


Slide notes

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**.

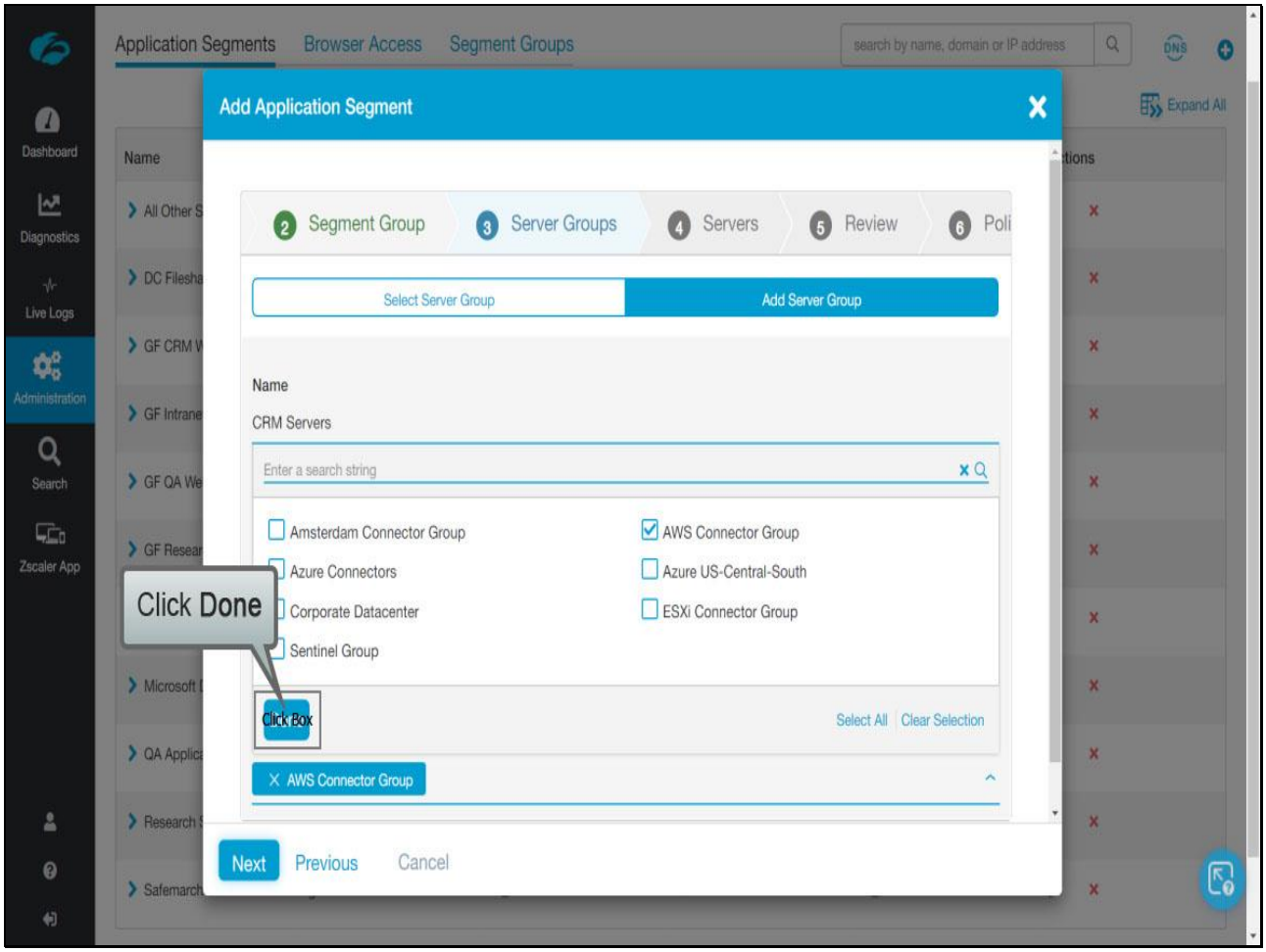
Slide 25 - Slide 25



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**, ...

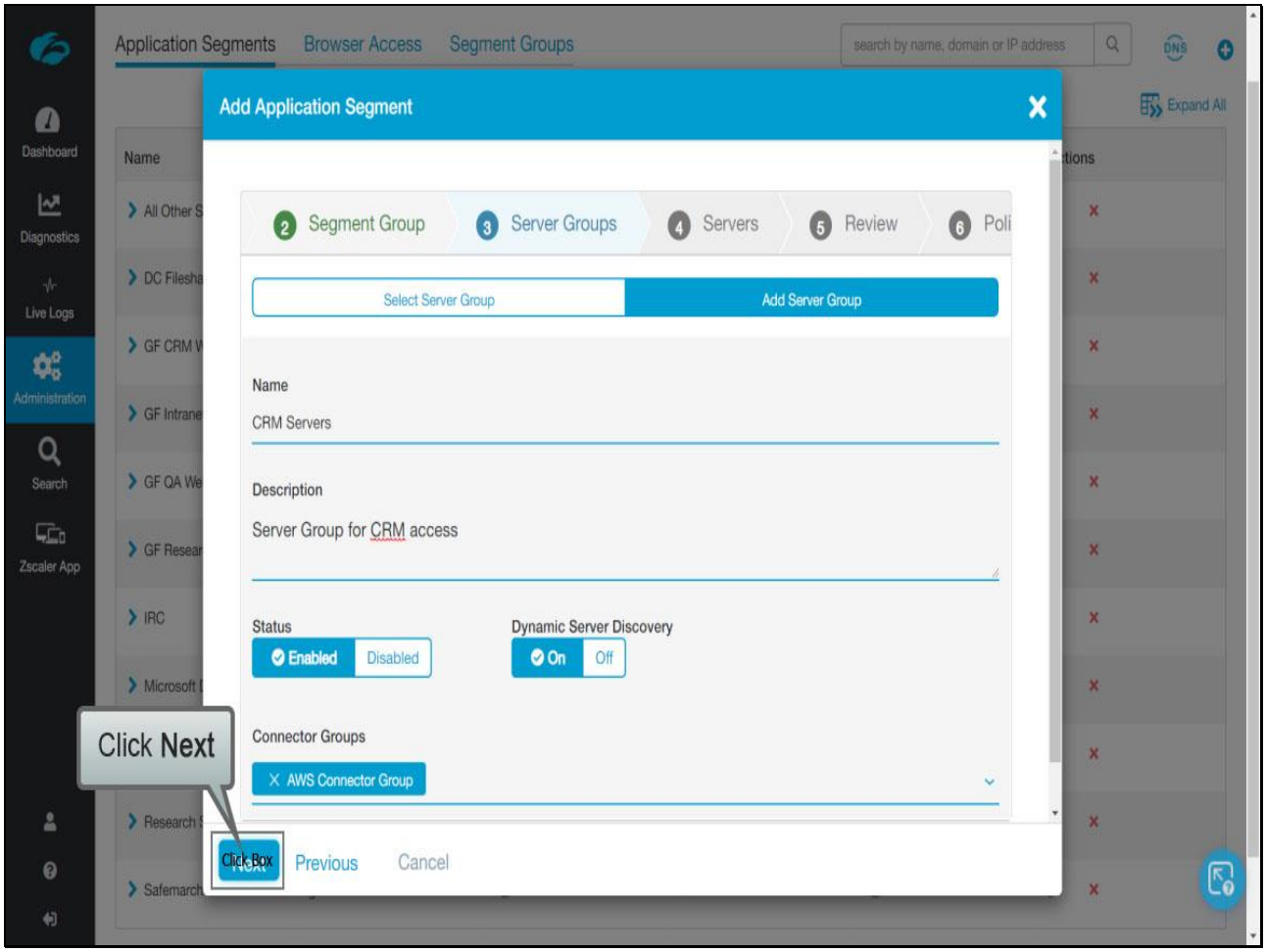
Slide 26 - Slide 26



Slide notes

...and click **Done**.

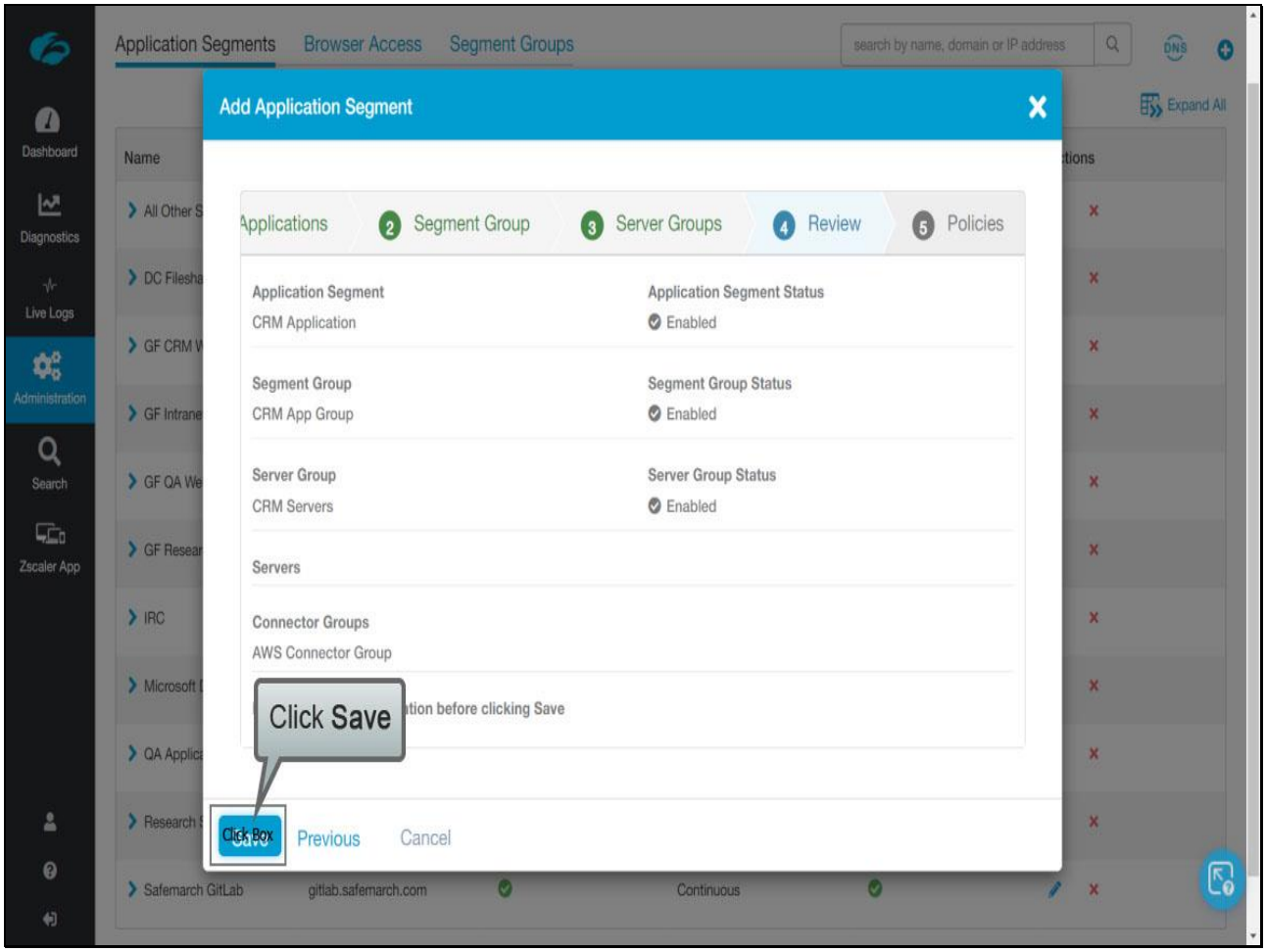
Slide 27 - Slide 27



Slide notes

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

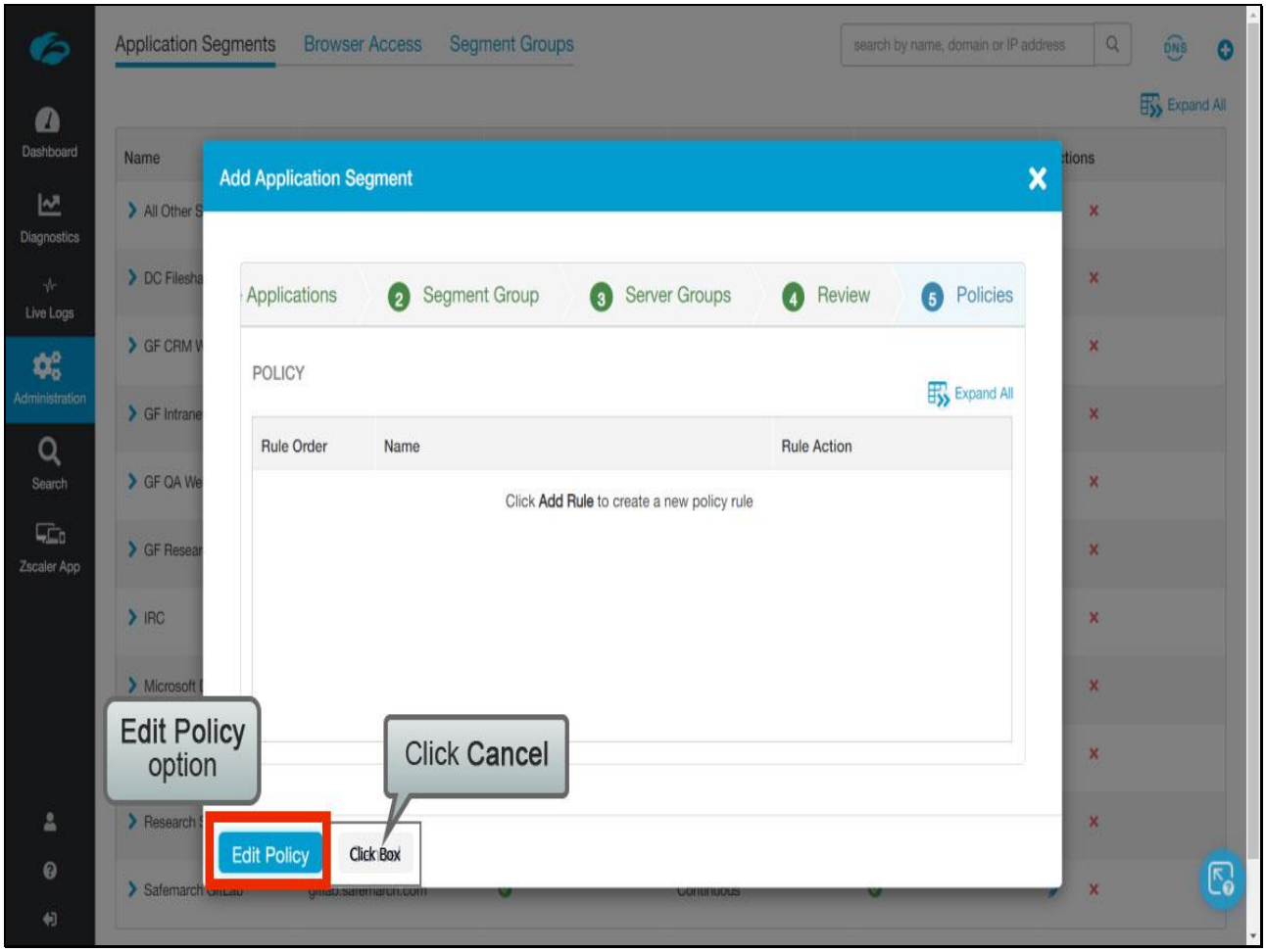
Slide 28 - Slide 28



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).

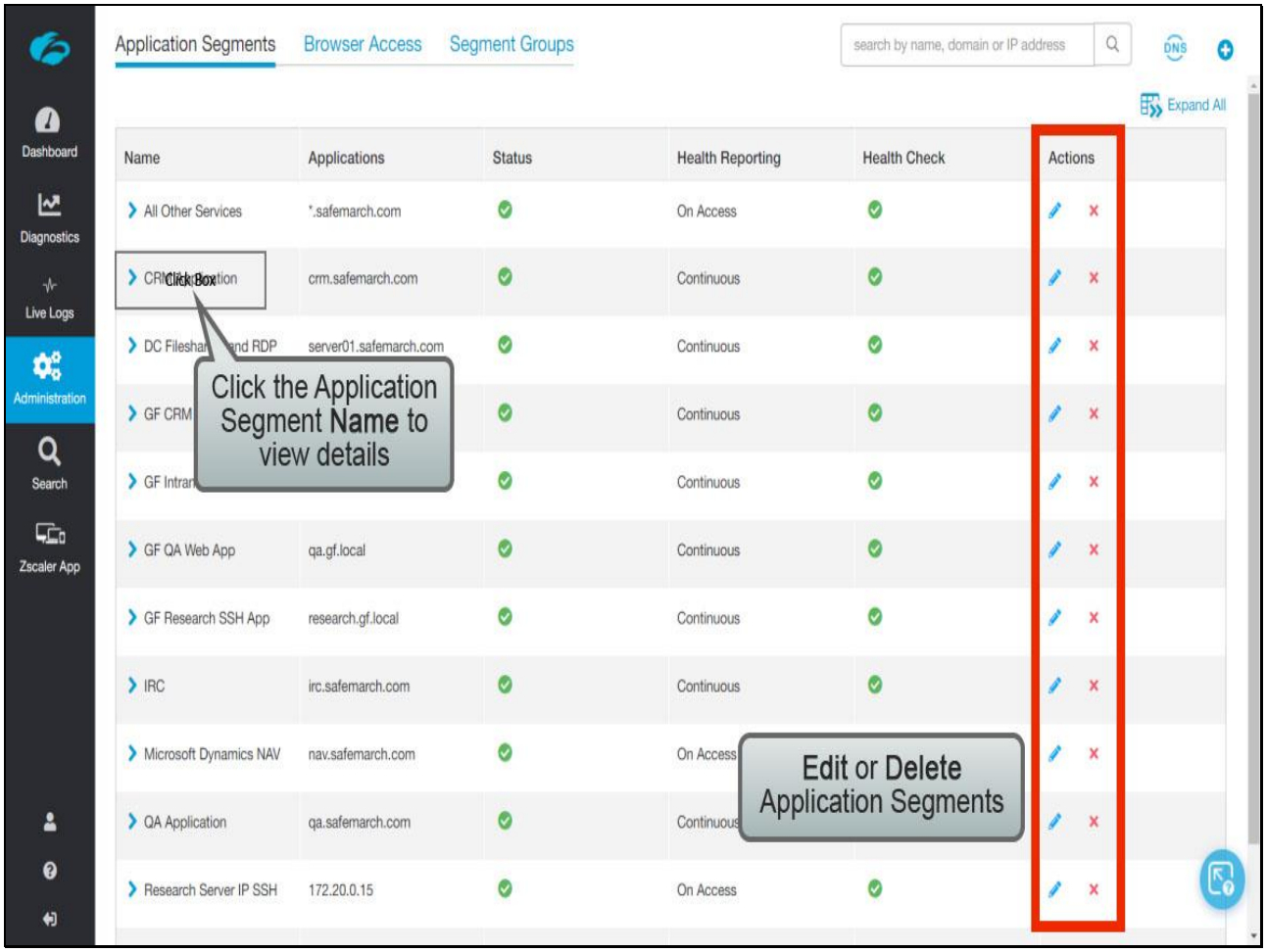
Slide 29 - Slide 29



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**.

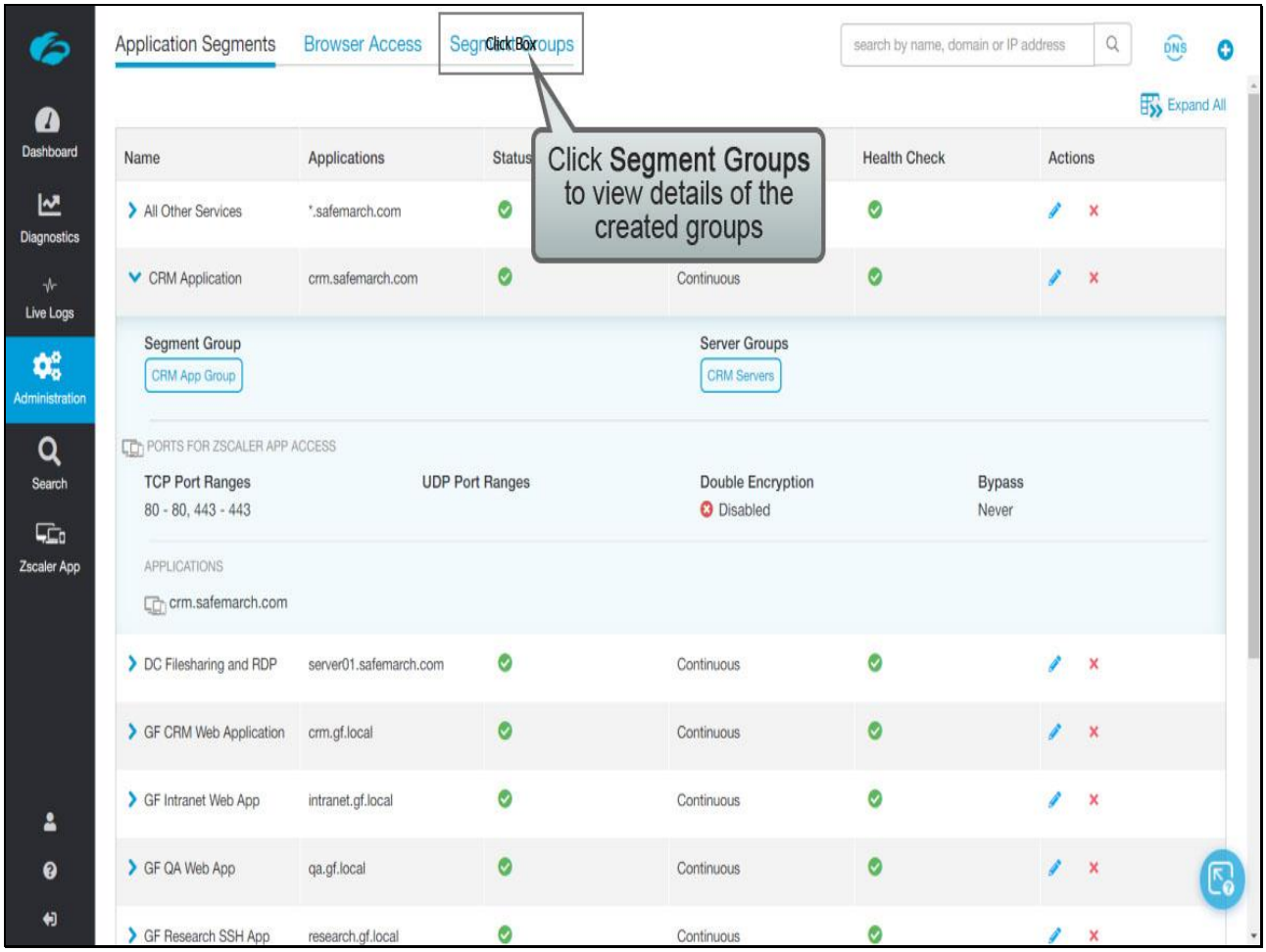
Slide 30 - Slide 30



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.

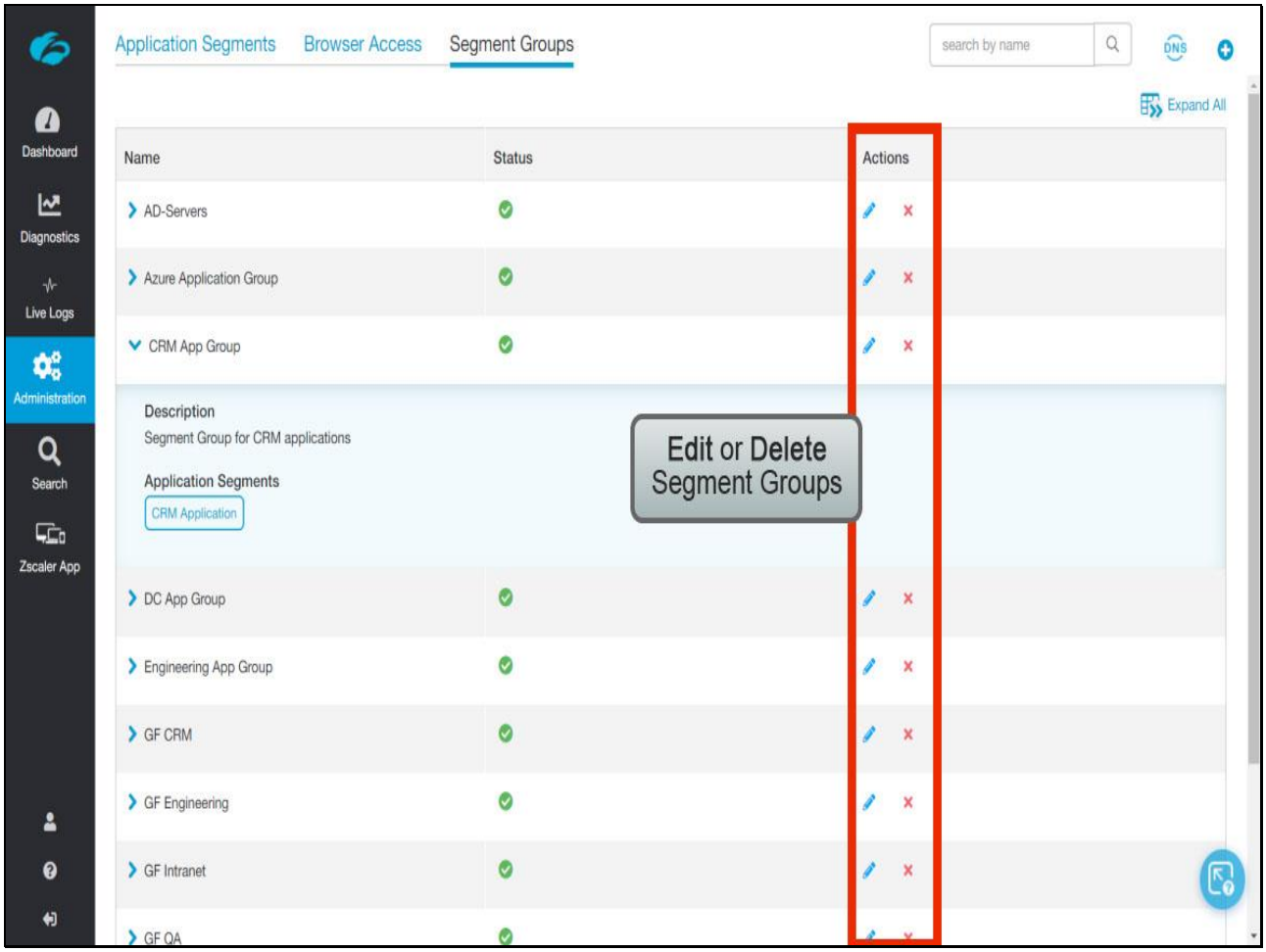
Slide 31 - Slide 31



Slide notes

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

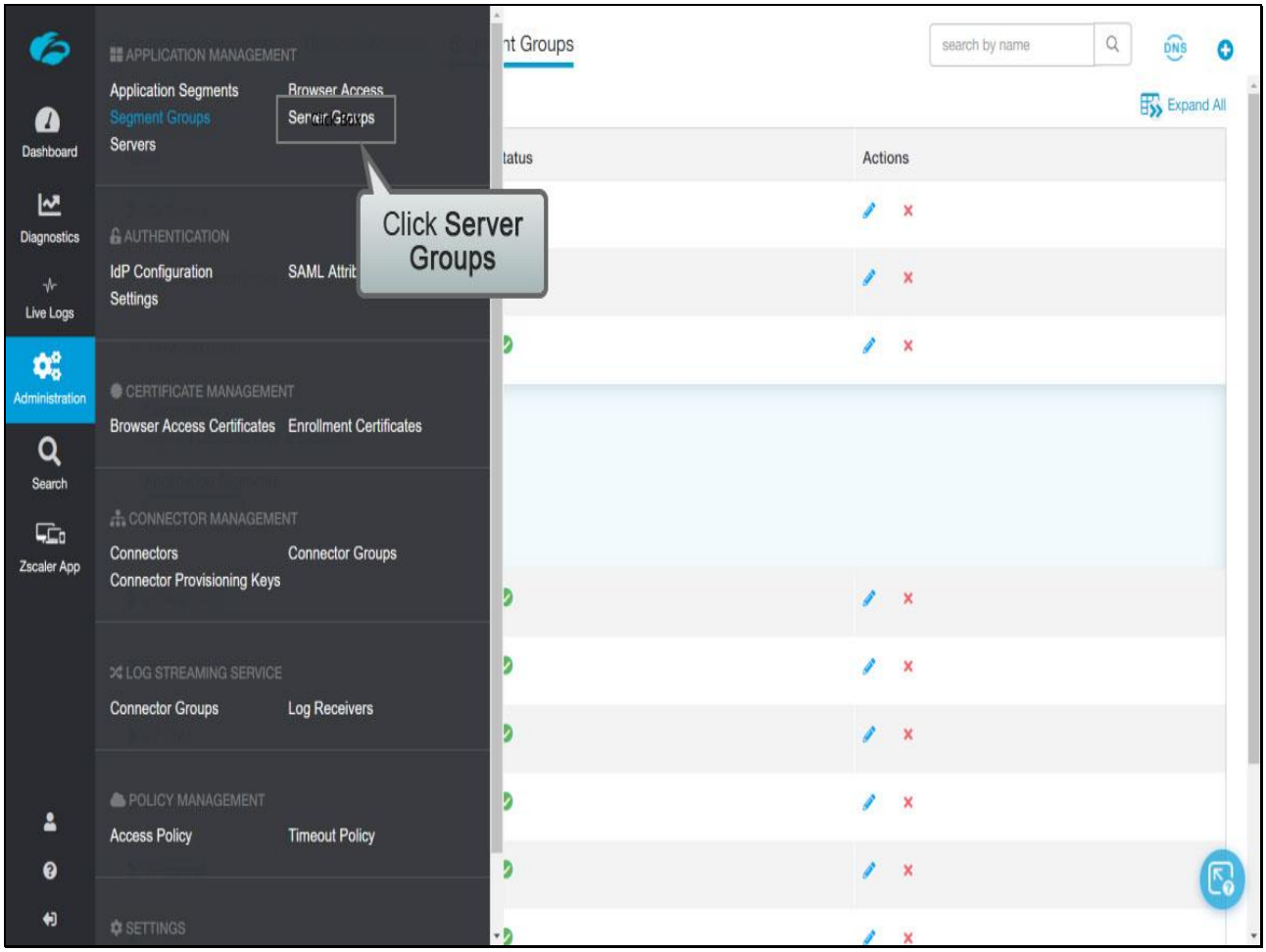
Slide 32 - Slide 32



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).

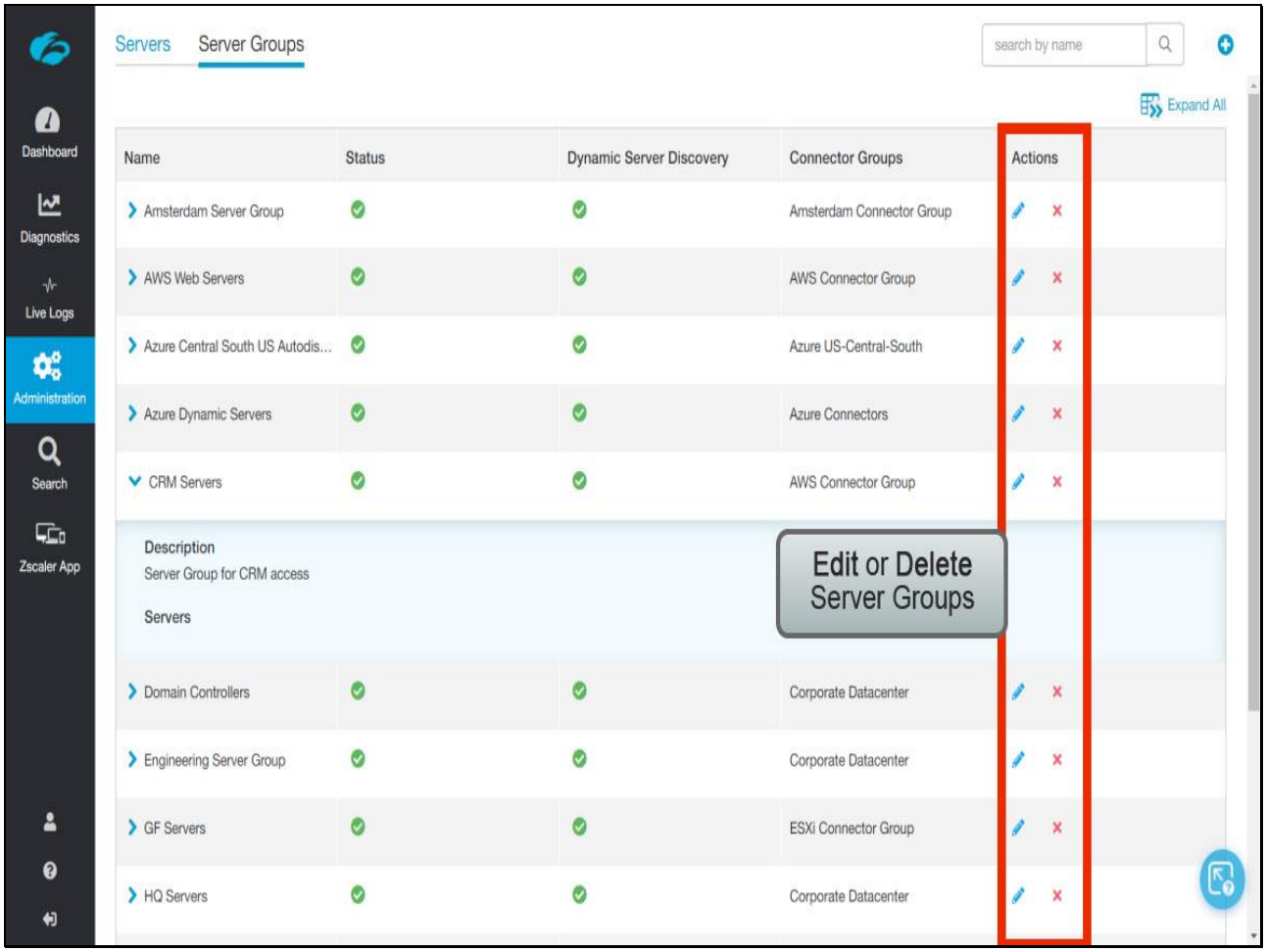
Slide 33 - Slide 33



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



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).

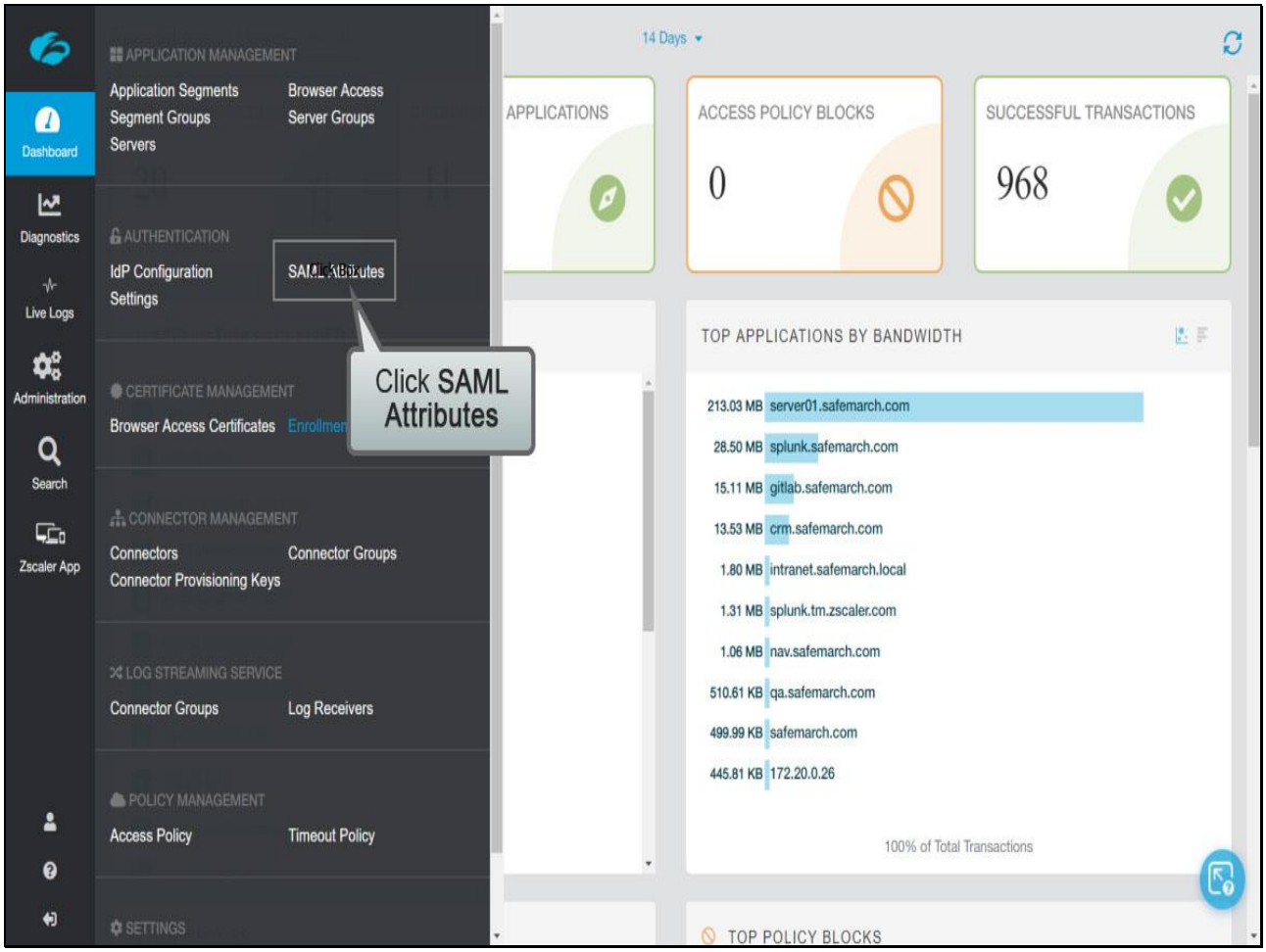
Slide 35 - 8. Configure Your SAML Attributes

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

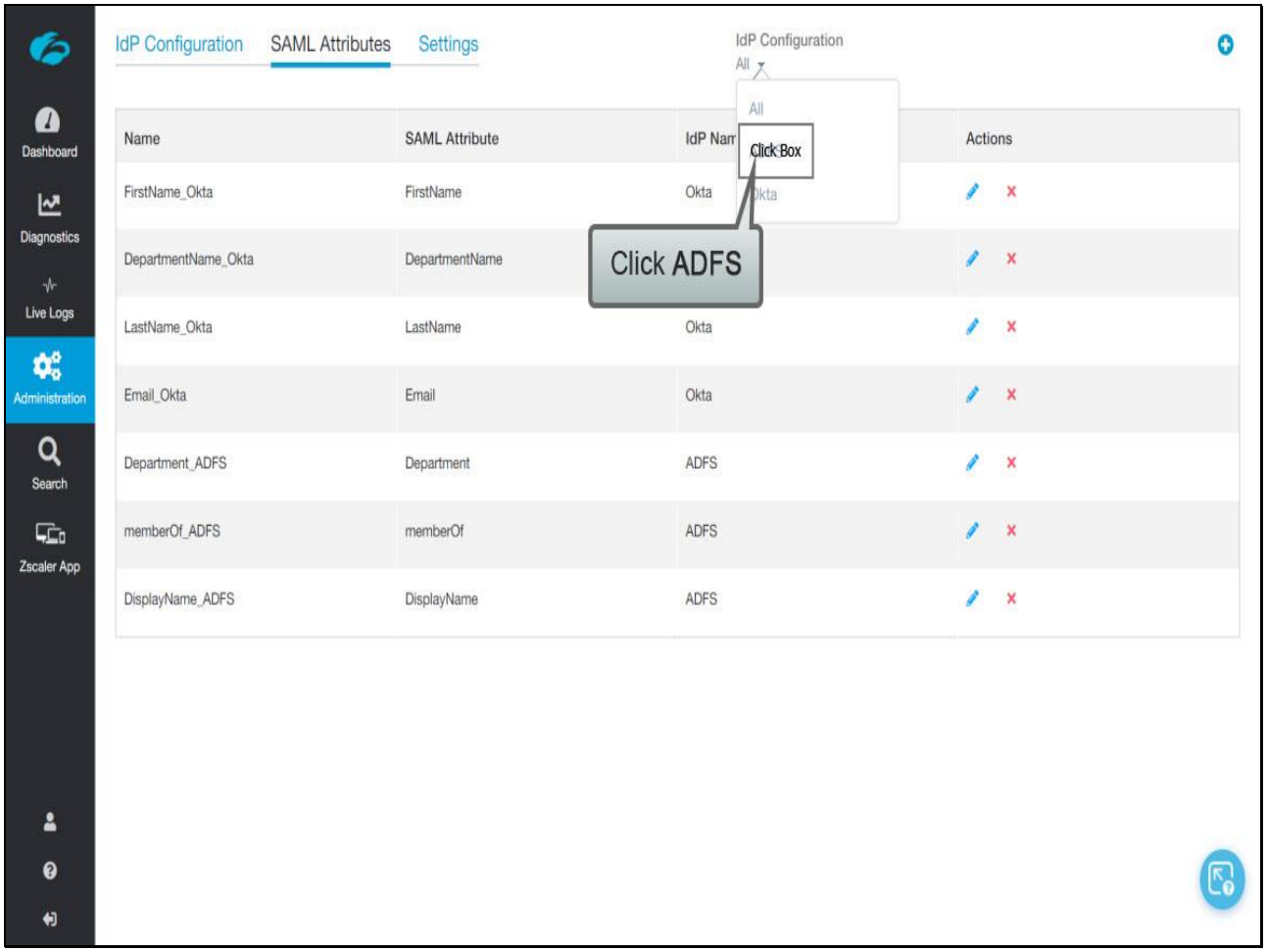


Slide notes

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.

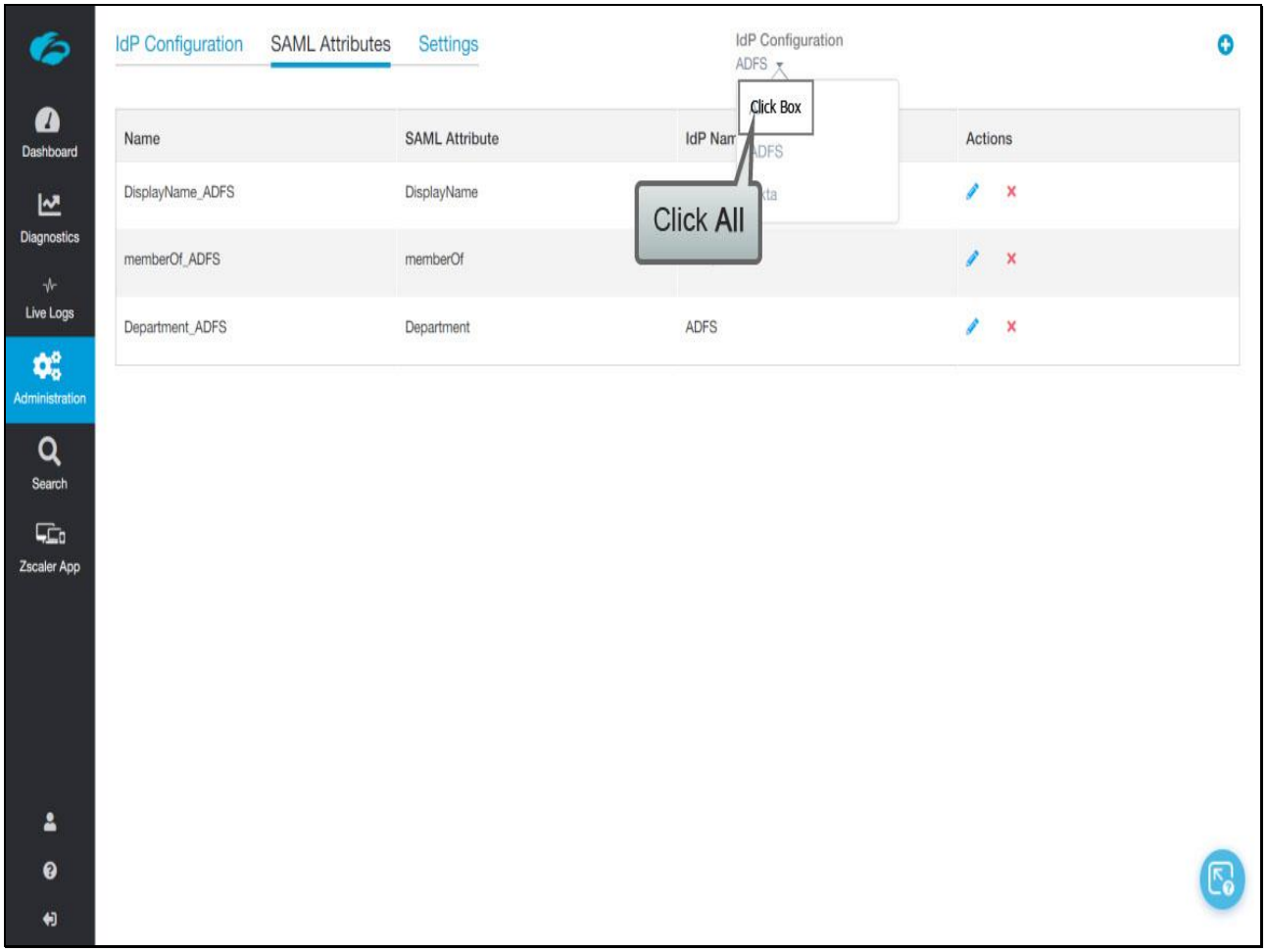
Slide 37 - Slide 37



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**, ...

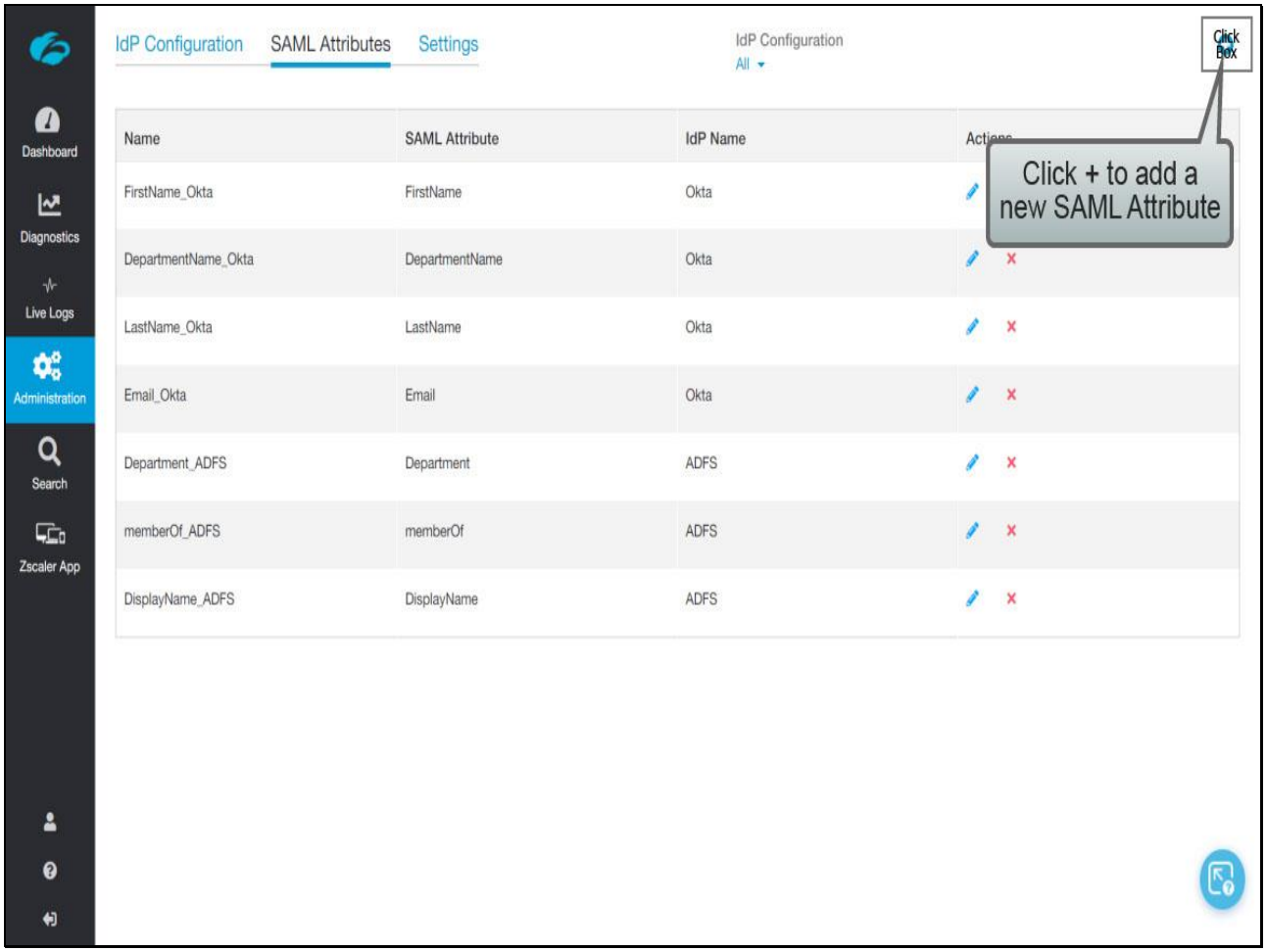
Slide 38 - Slide 38



Slide notes

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

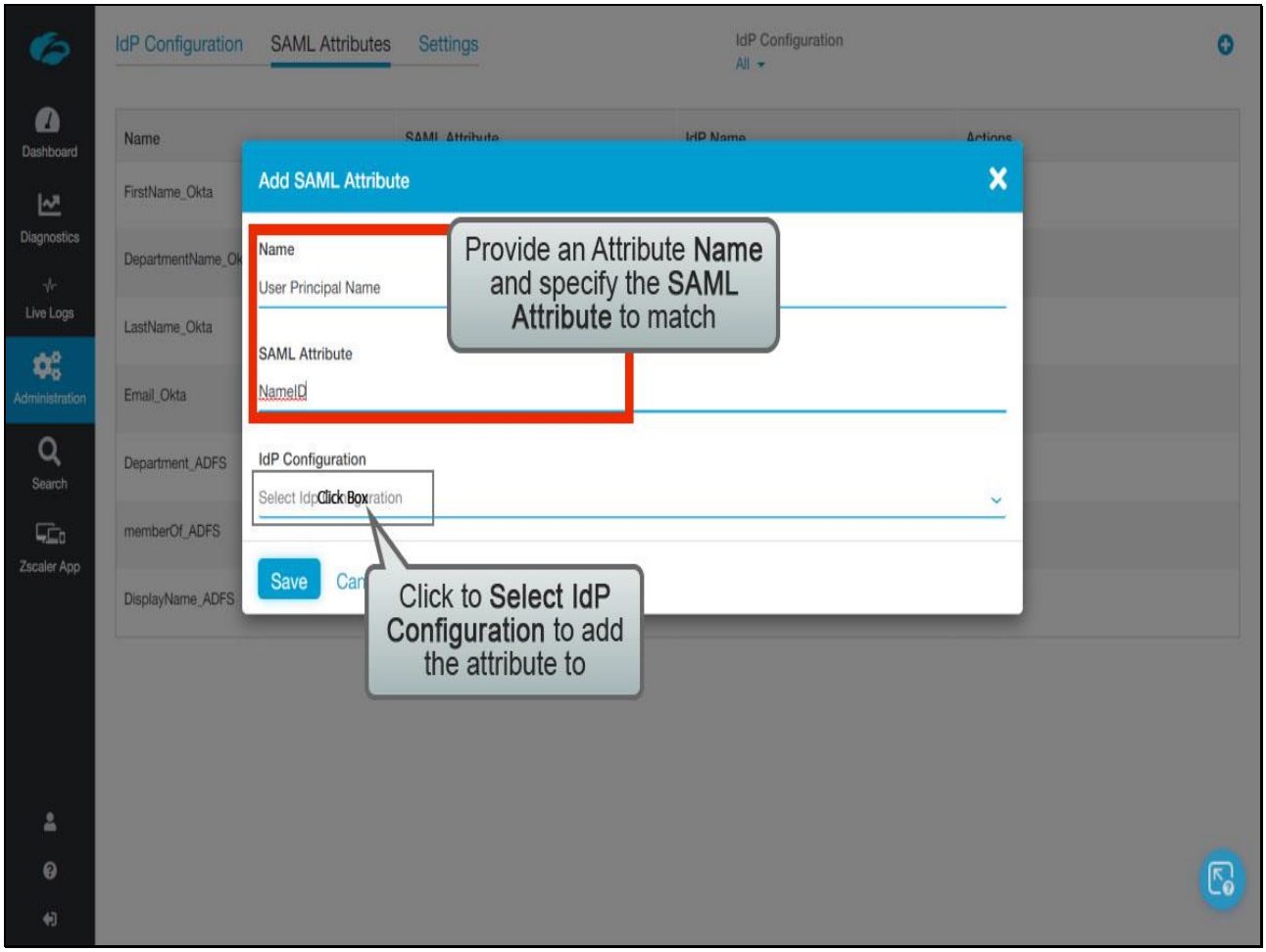
Slide 39 - Slide 39



Slide notes

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

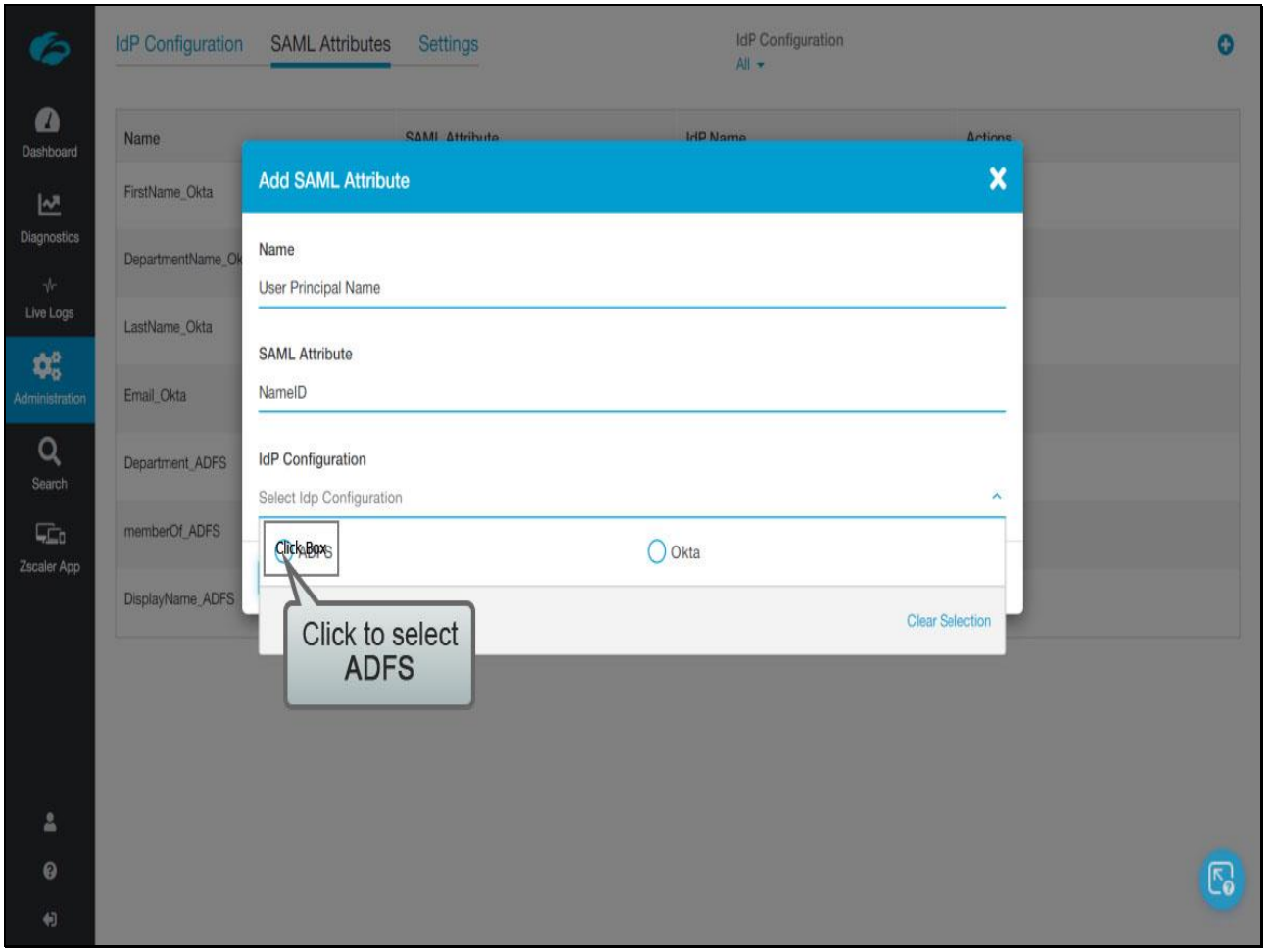
Slide 40 - Slide 40



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**, ...

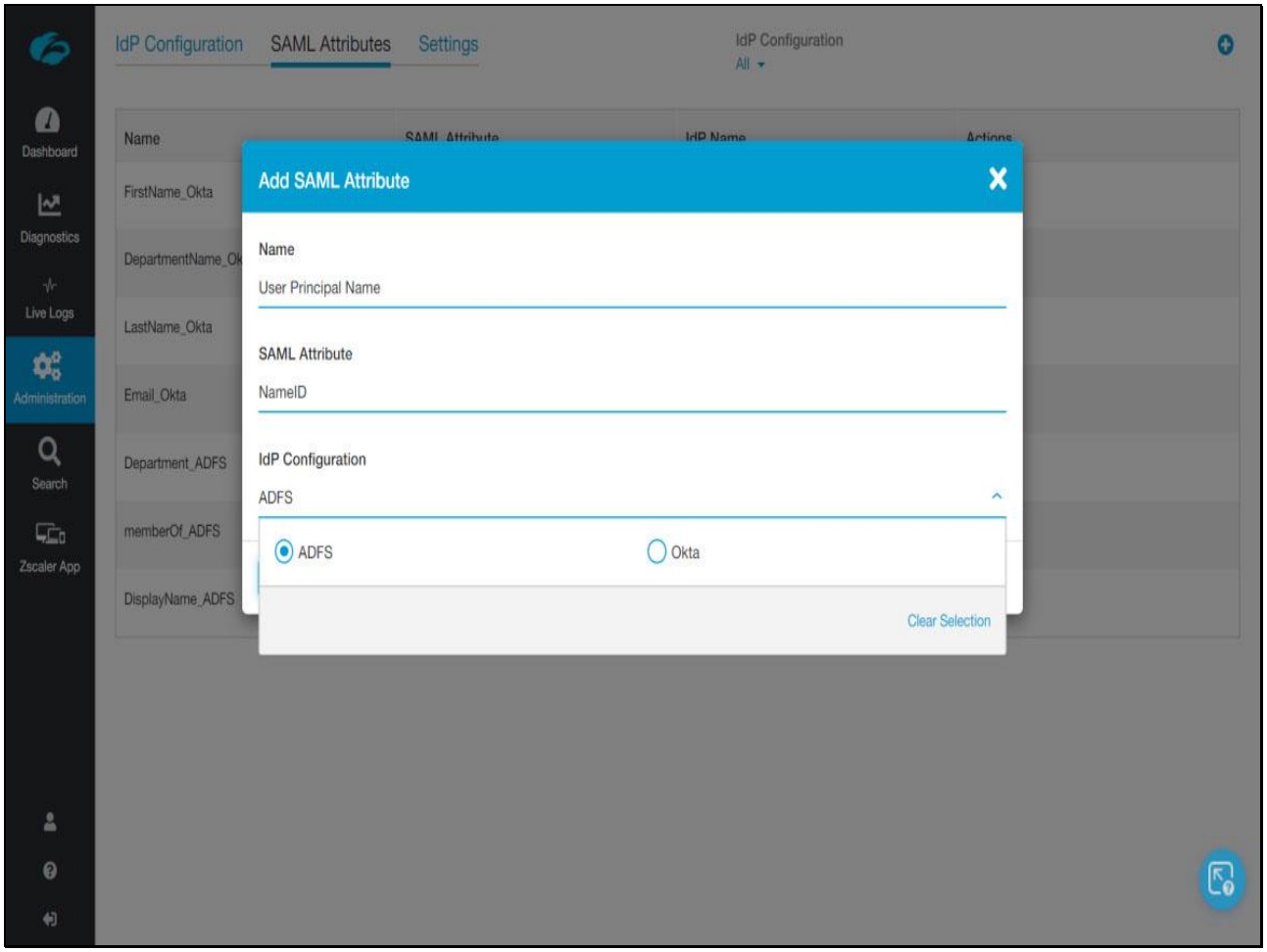
Slide 41 - Slide 41



Slide notes

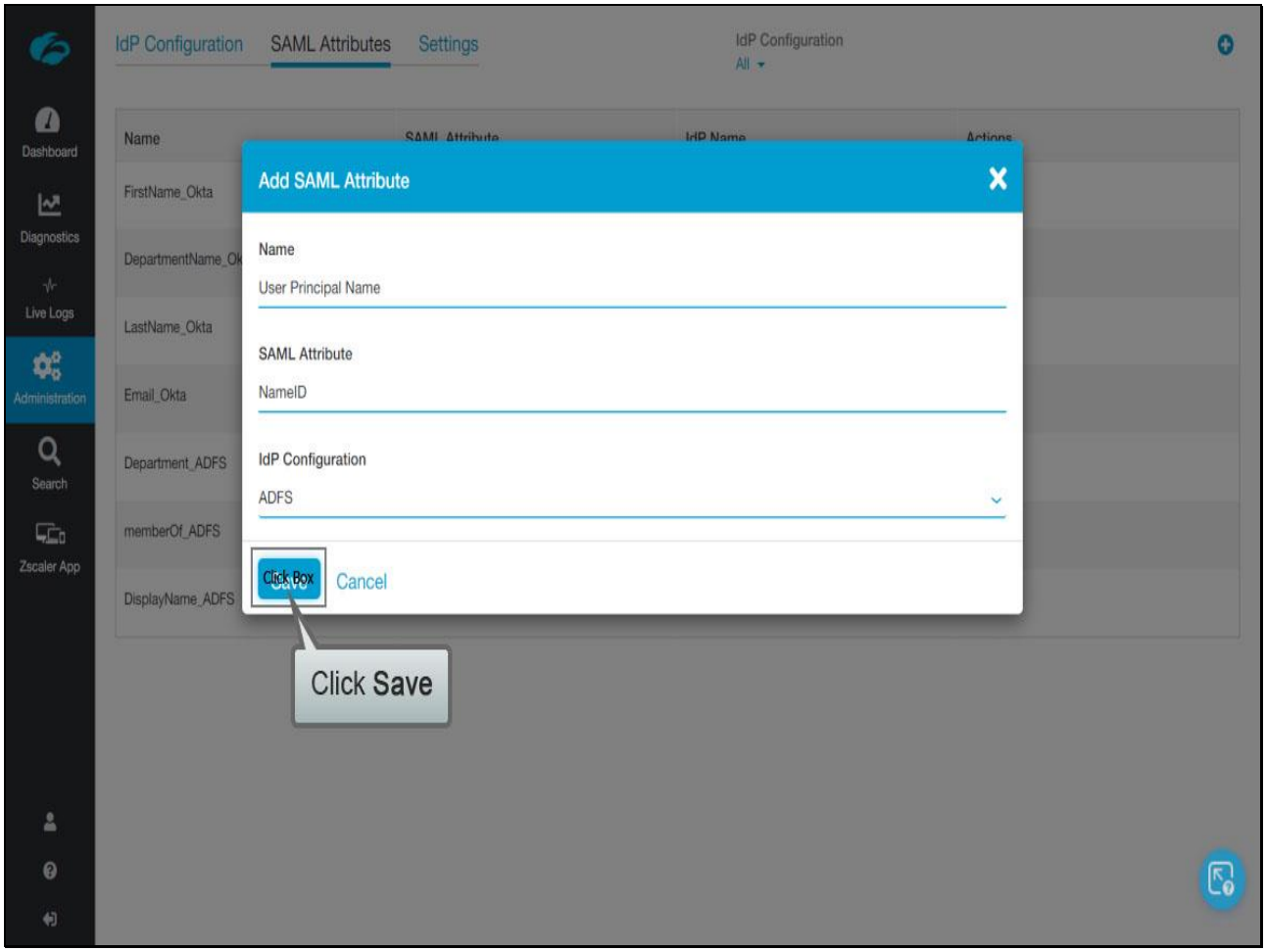
...and select one of the available IdP Configurations, in this case click **ADFS**, ...

Slide 42 - Slide 42



Slide notes

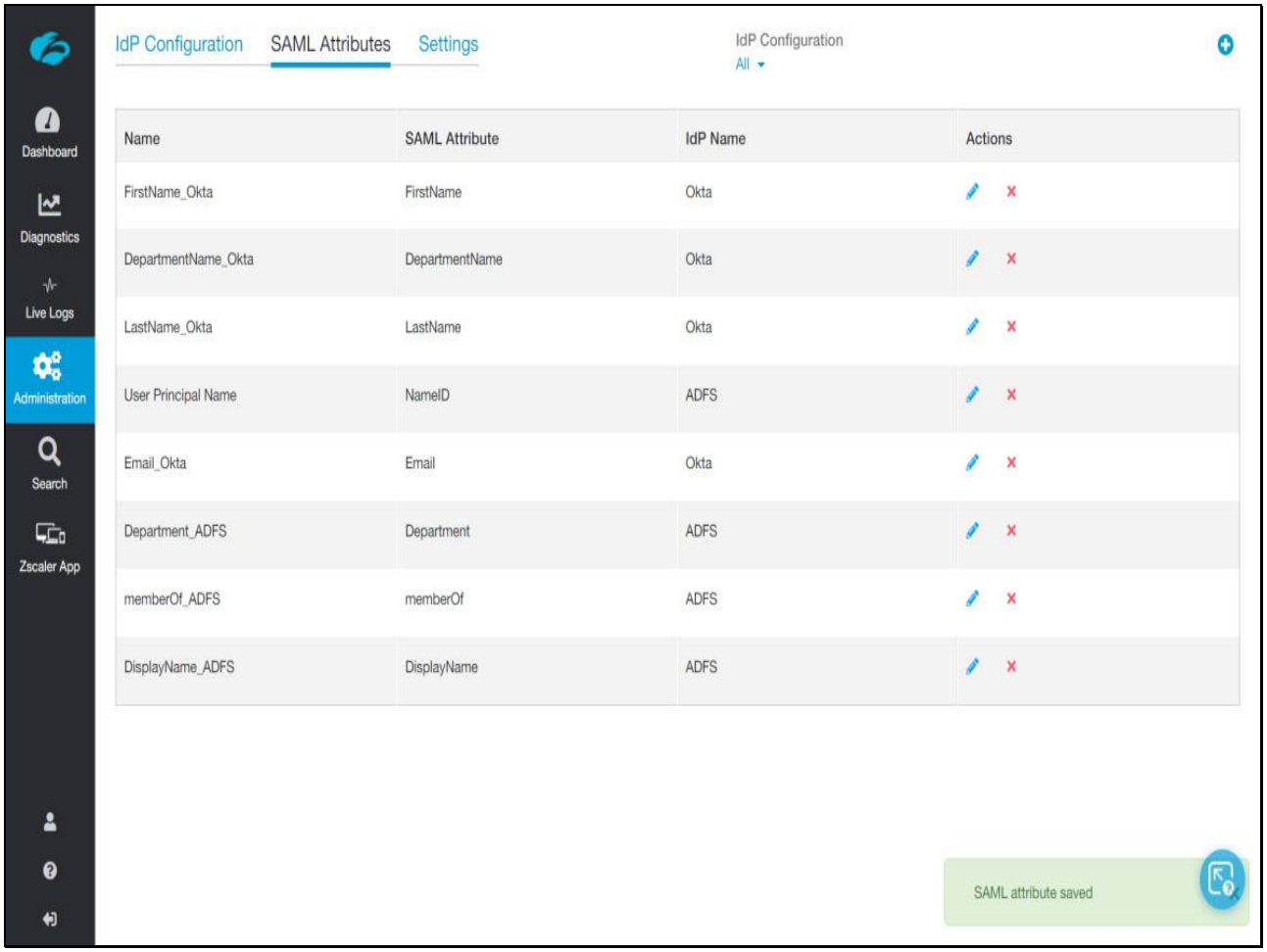
Slide 43 - Slide 43



Slide notes

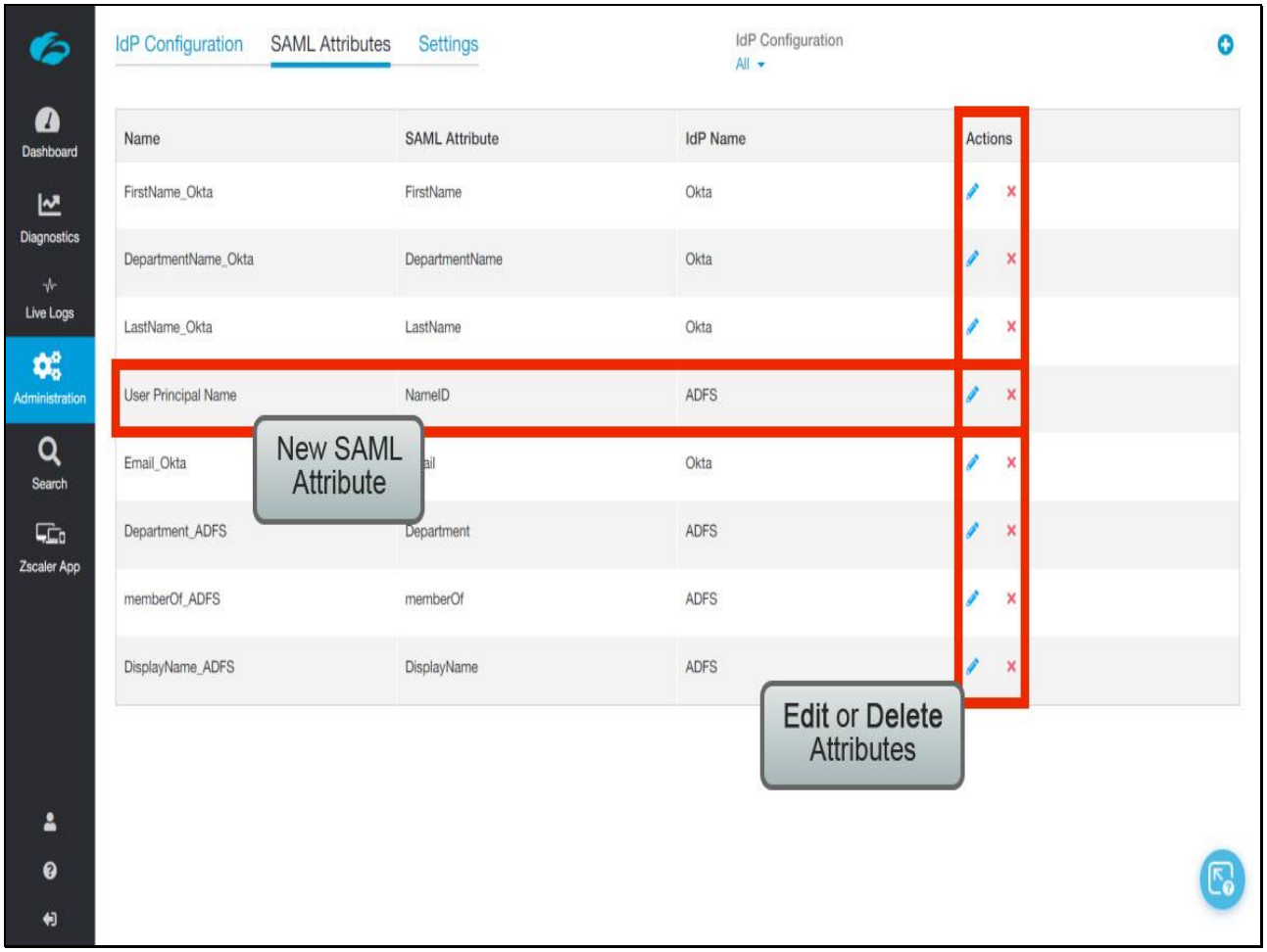
...and click **Save**.

Slide 44 - Slide 44



Slide notes

Slide 45 - Slide 45



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.

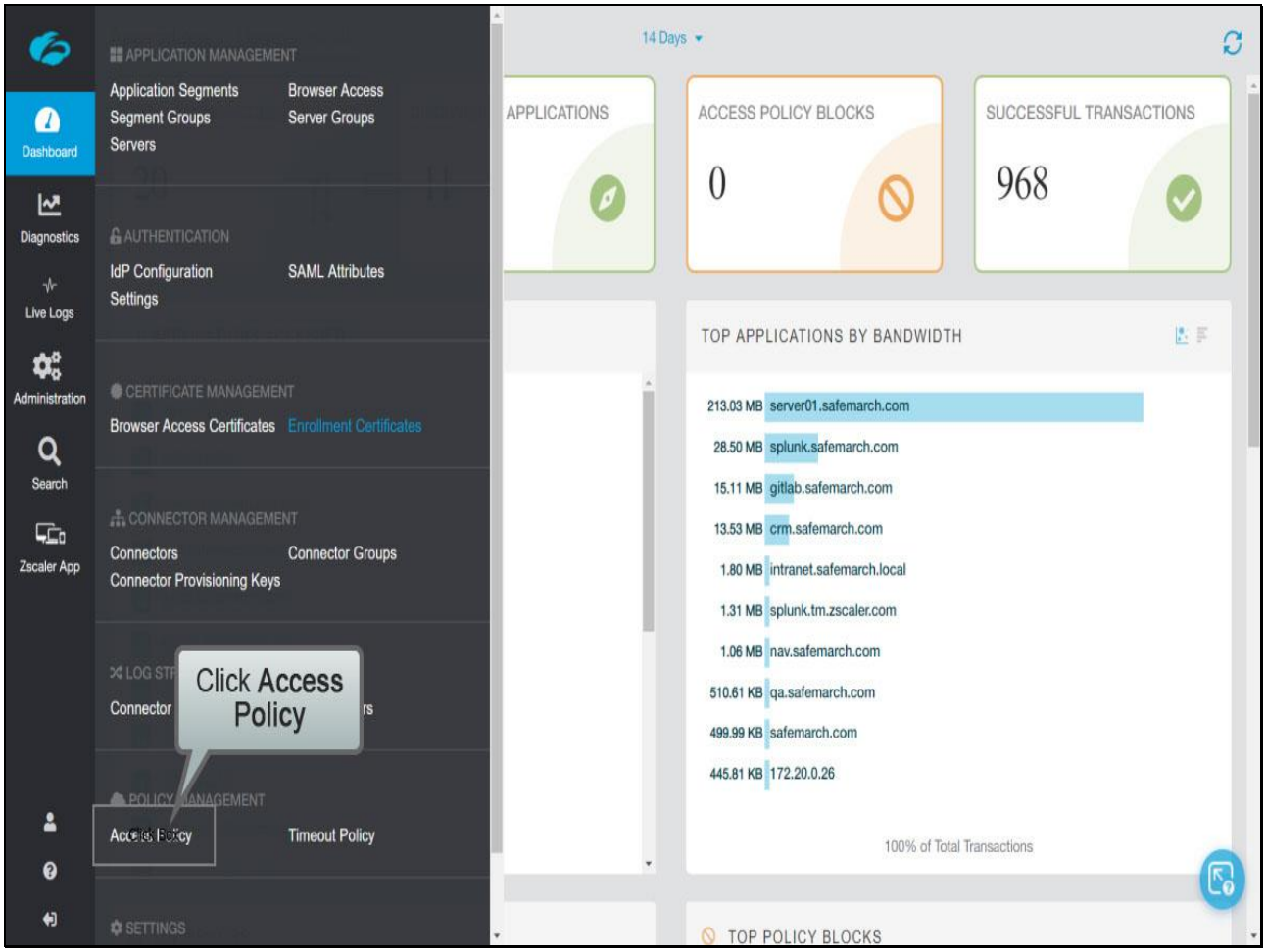
Slide 46 - 9. Configure Your Access Policies

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.

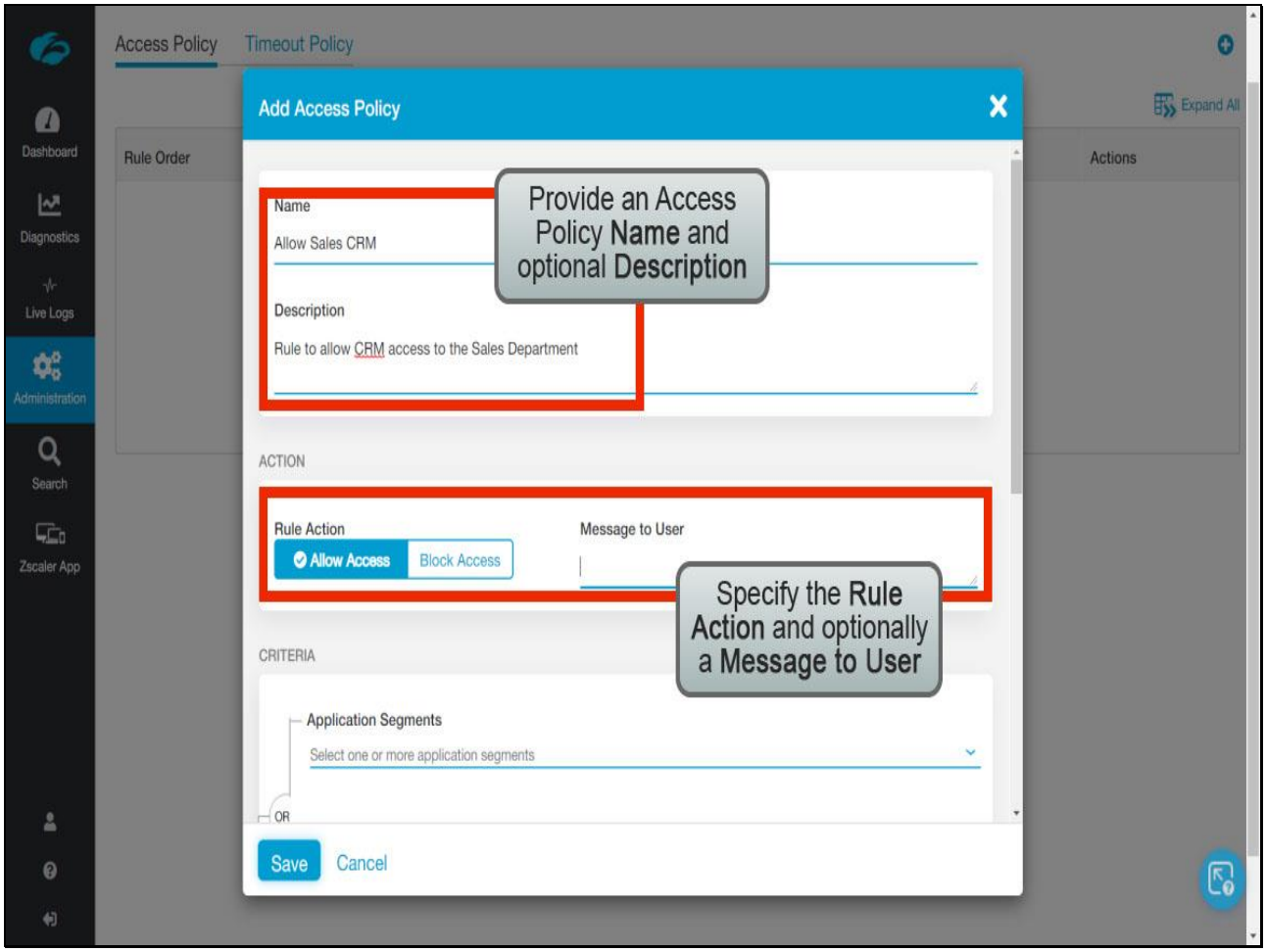
To create Access Policy rules, in the ZPA Admin Portal from the **Administration** menu click **Access Policy** in the **POLICY MANAGEMENT** section, ...

Slide 48 - Slide 48

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.

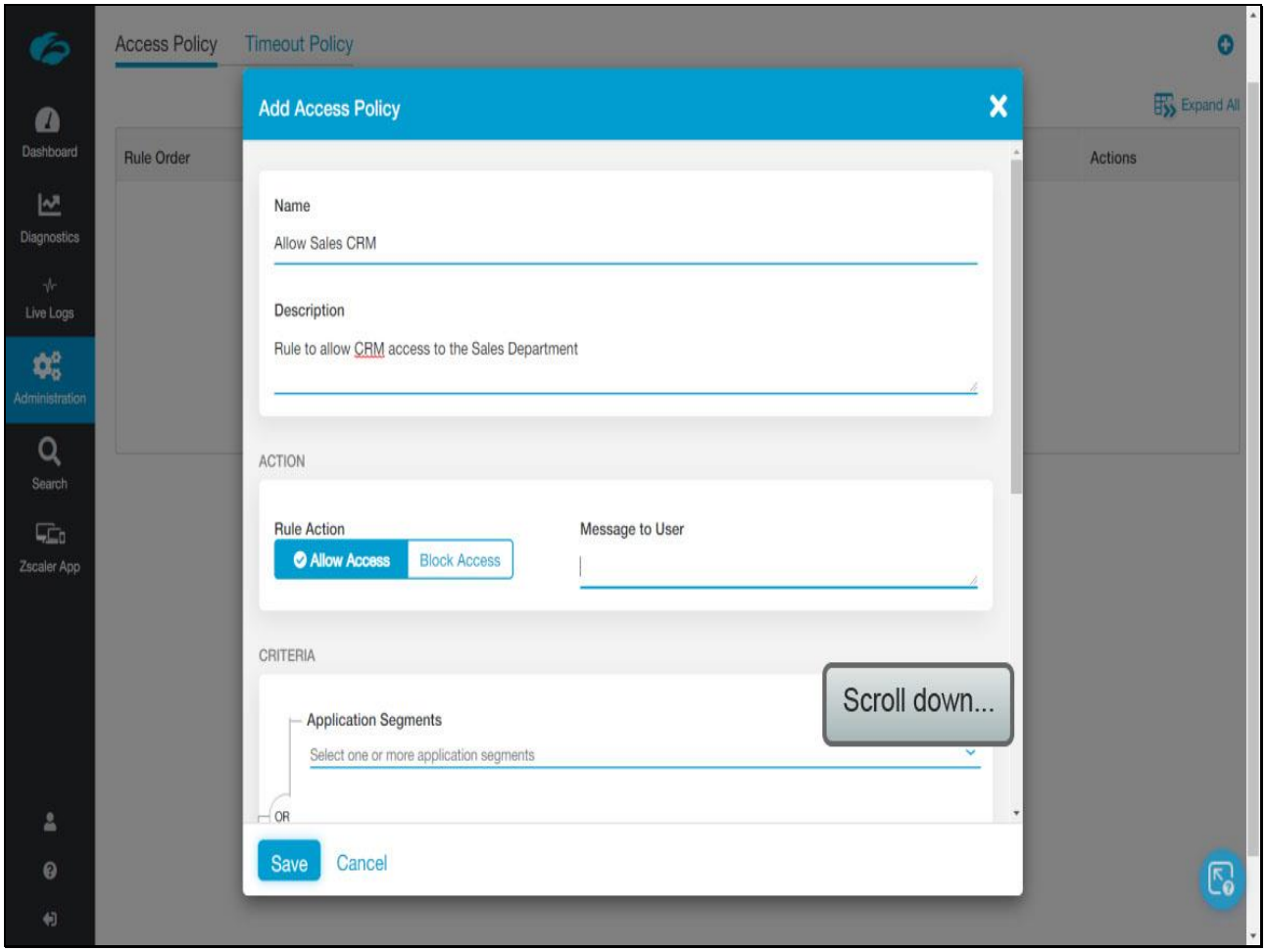
Slide 49 - Slide 49



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**.

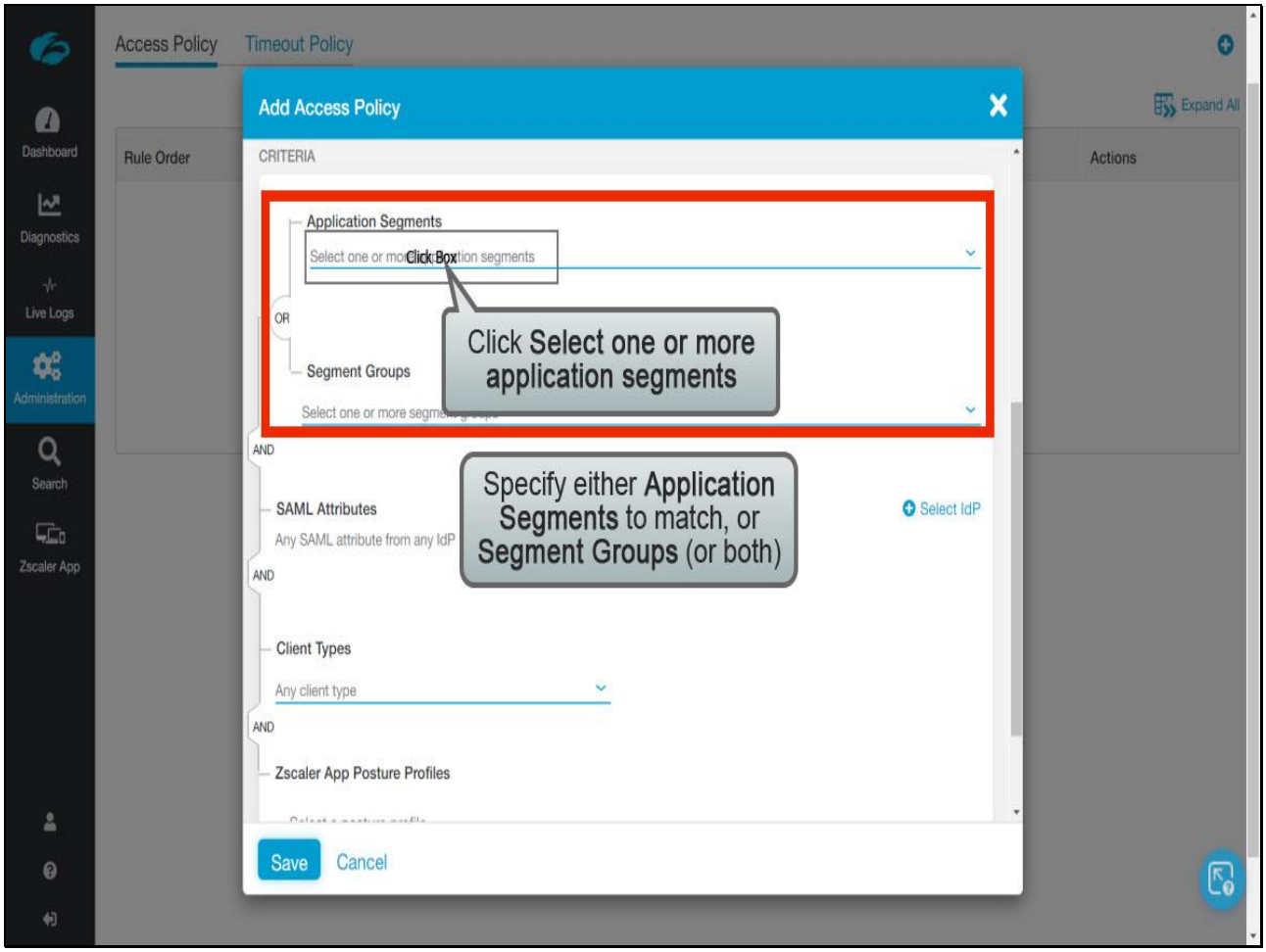
Slide 50 - Slide 50



Slide notes

Scroll down...

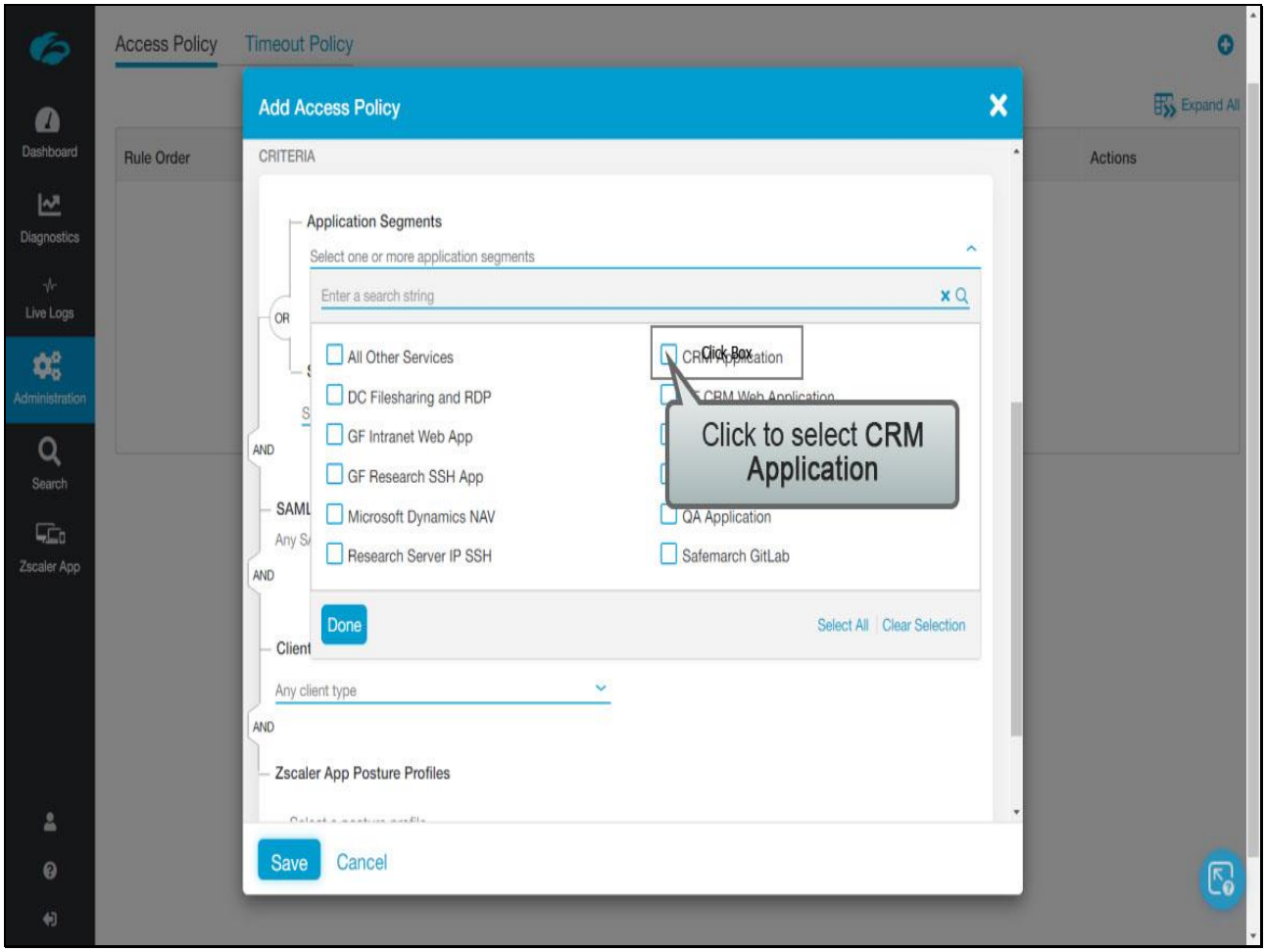
Slide 51 - Slide 51



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**, ...

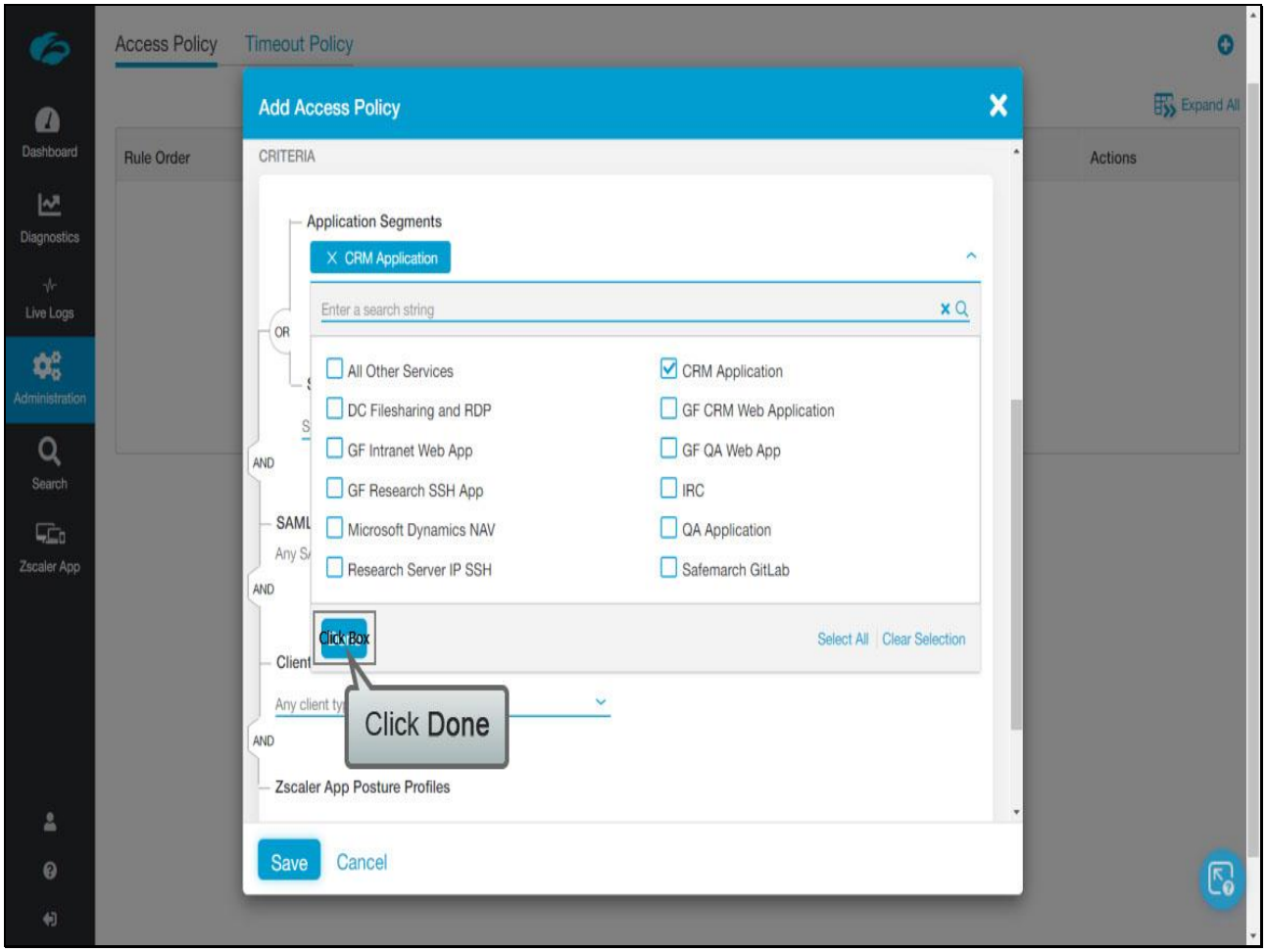
Slide 52 - Slide 52



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, ...

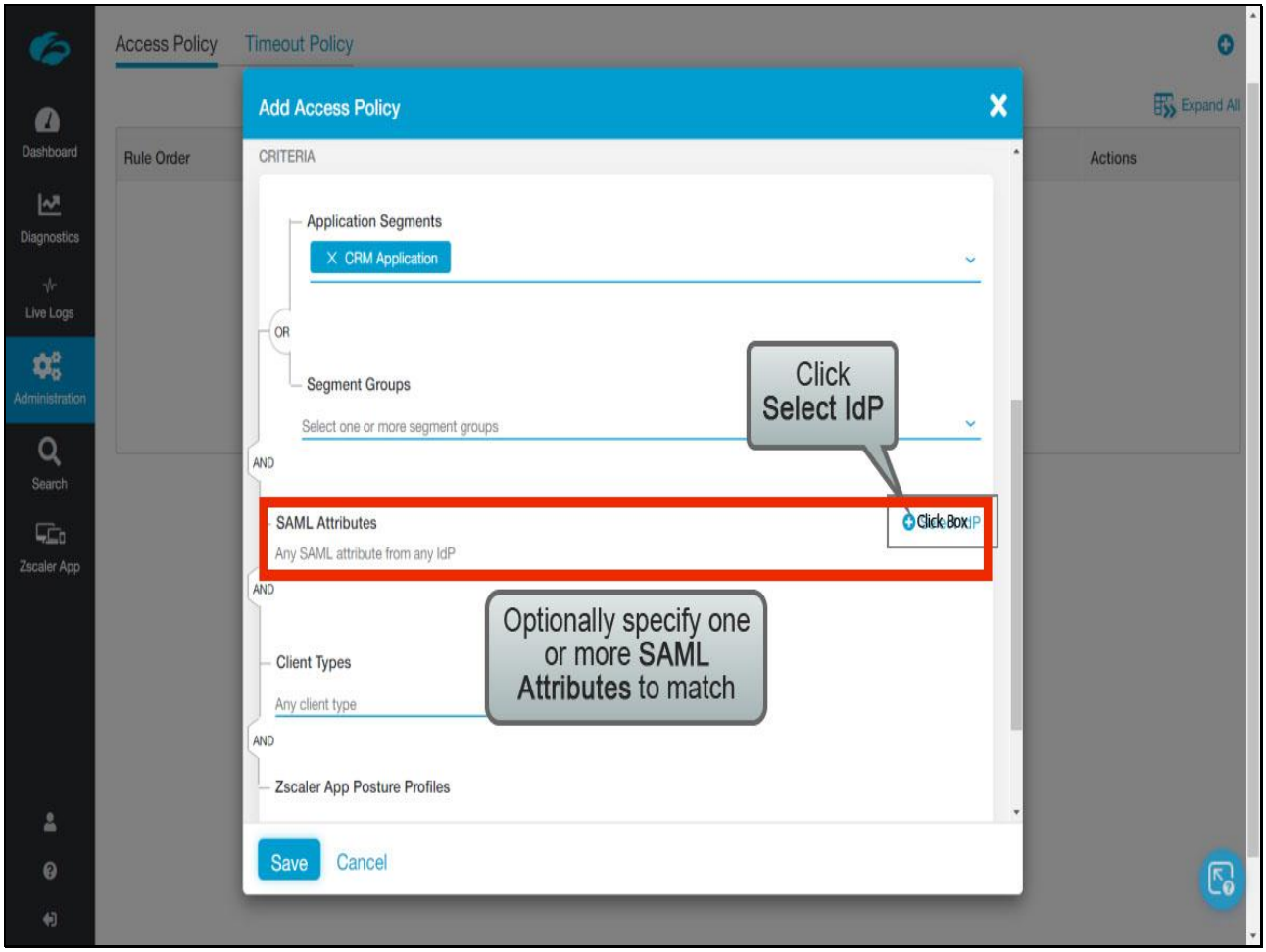
Slide 53 - Slide 53



Slide notes

...then click **Done**.

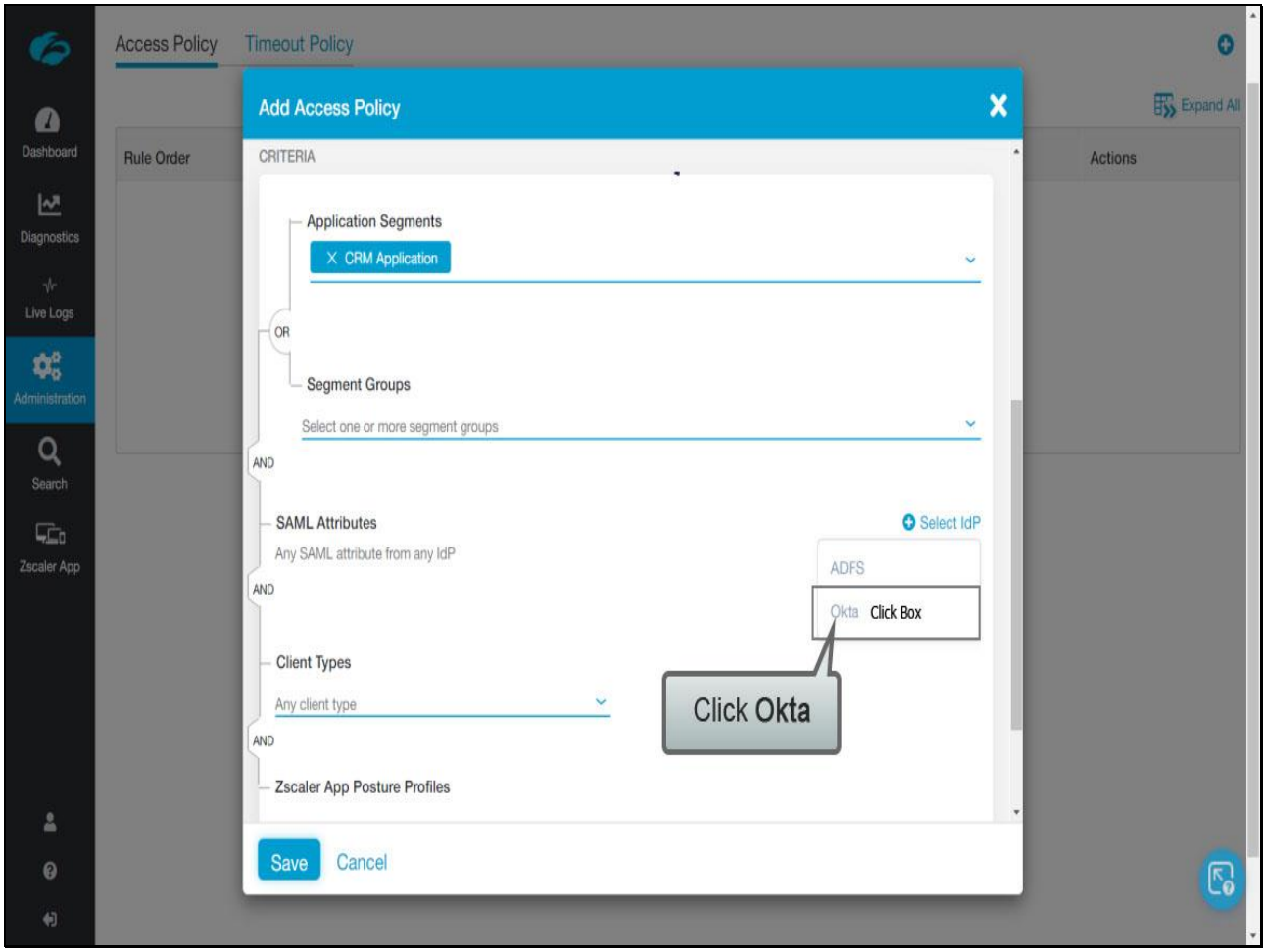
Slide 54 - Slide 54



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**, ...

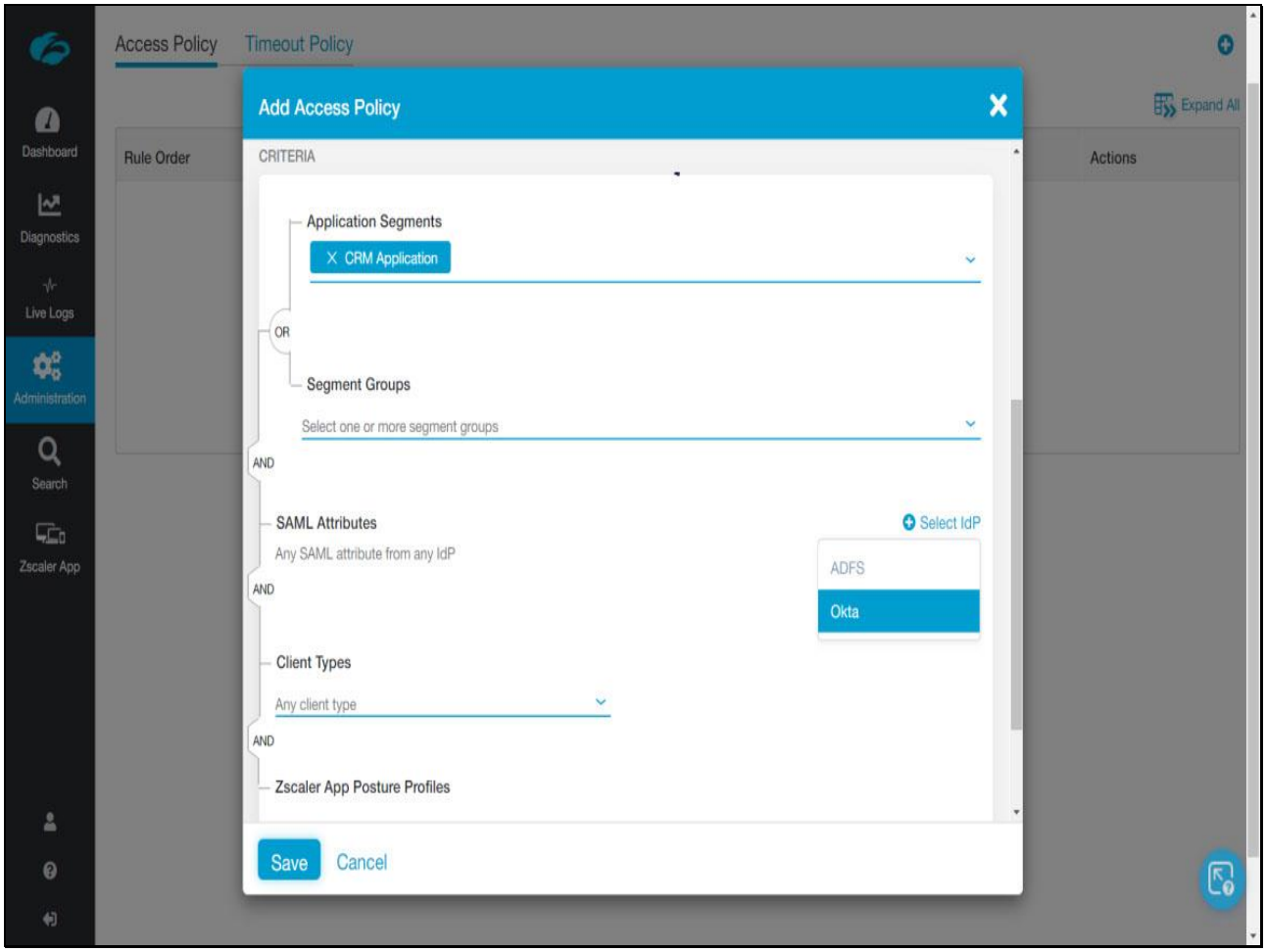
Slide 55 - Slide 55



Slide notes

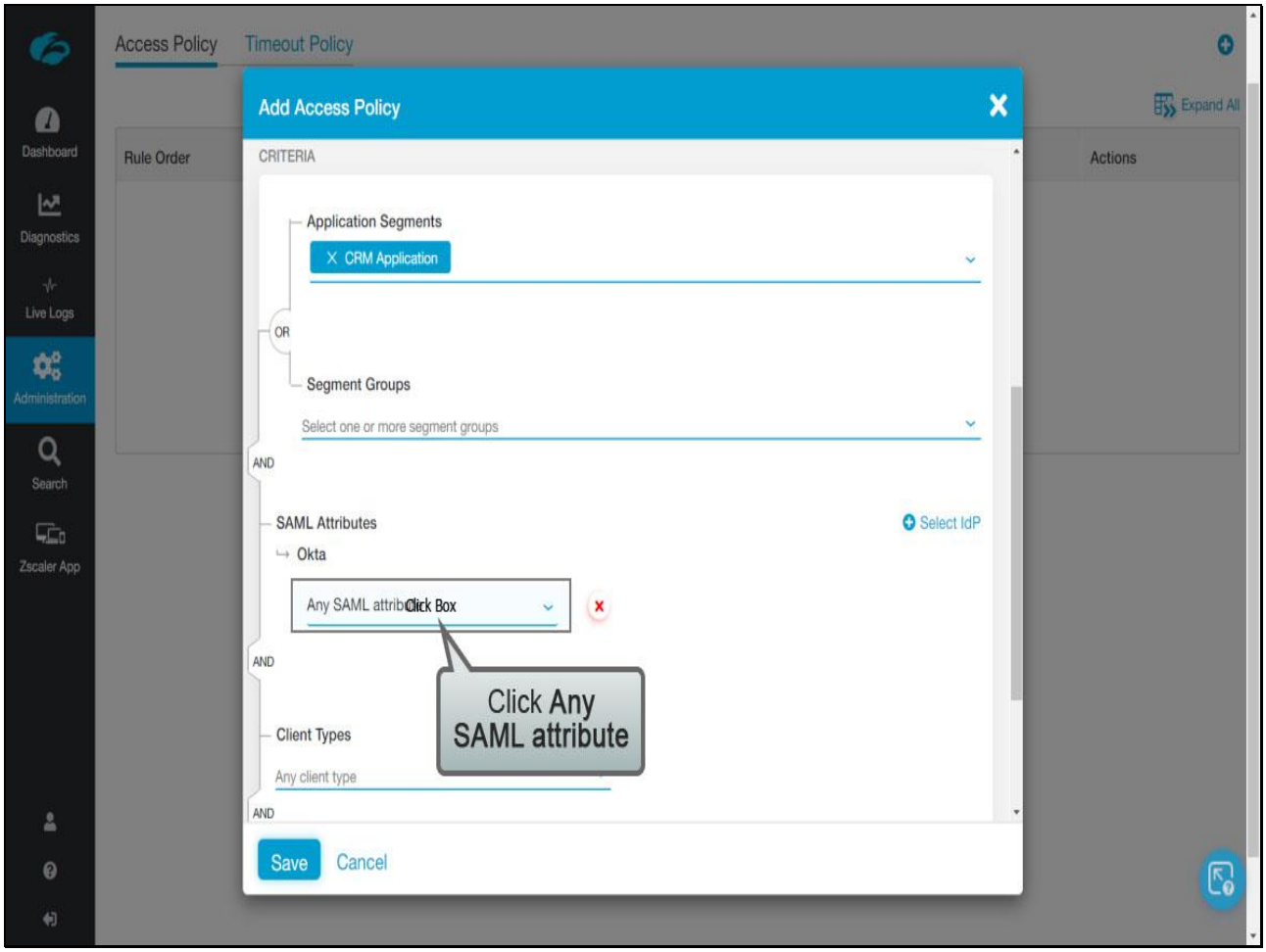
...and select the correct IdP, in this case click **Okta**.

Slide 56 - Slide 56



Slide notes

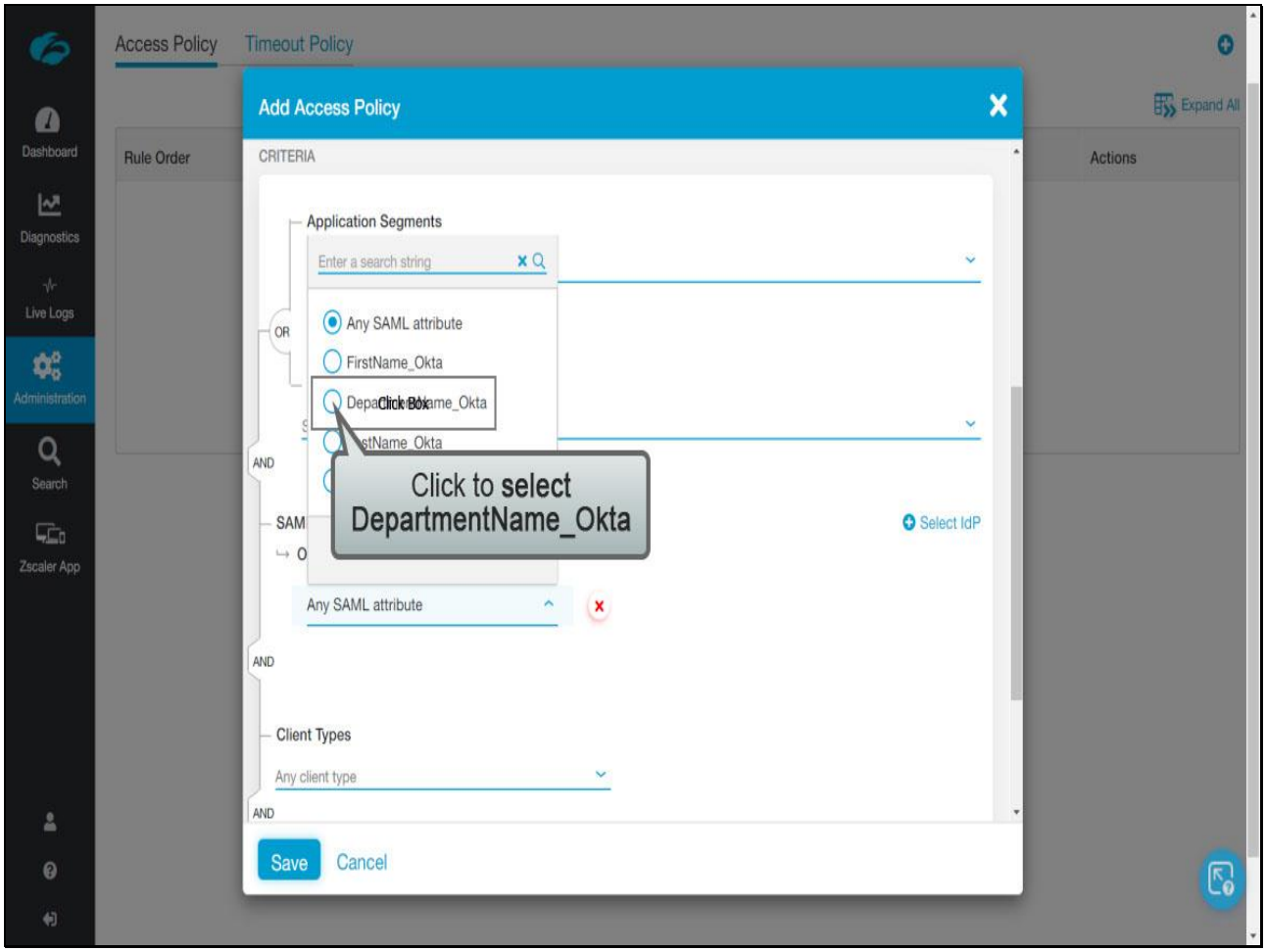
Slide 57 - Slide 57



Slide notes

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

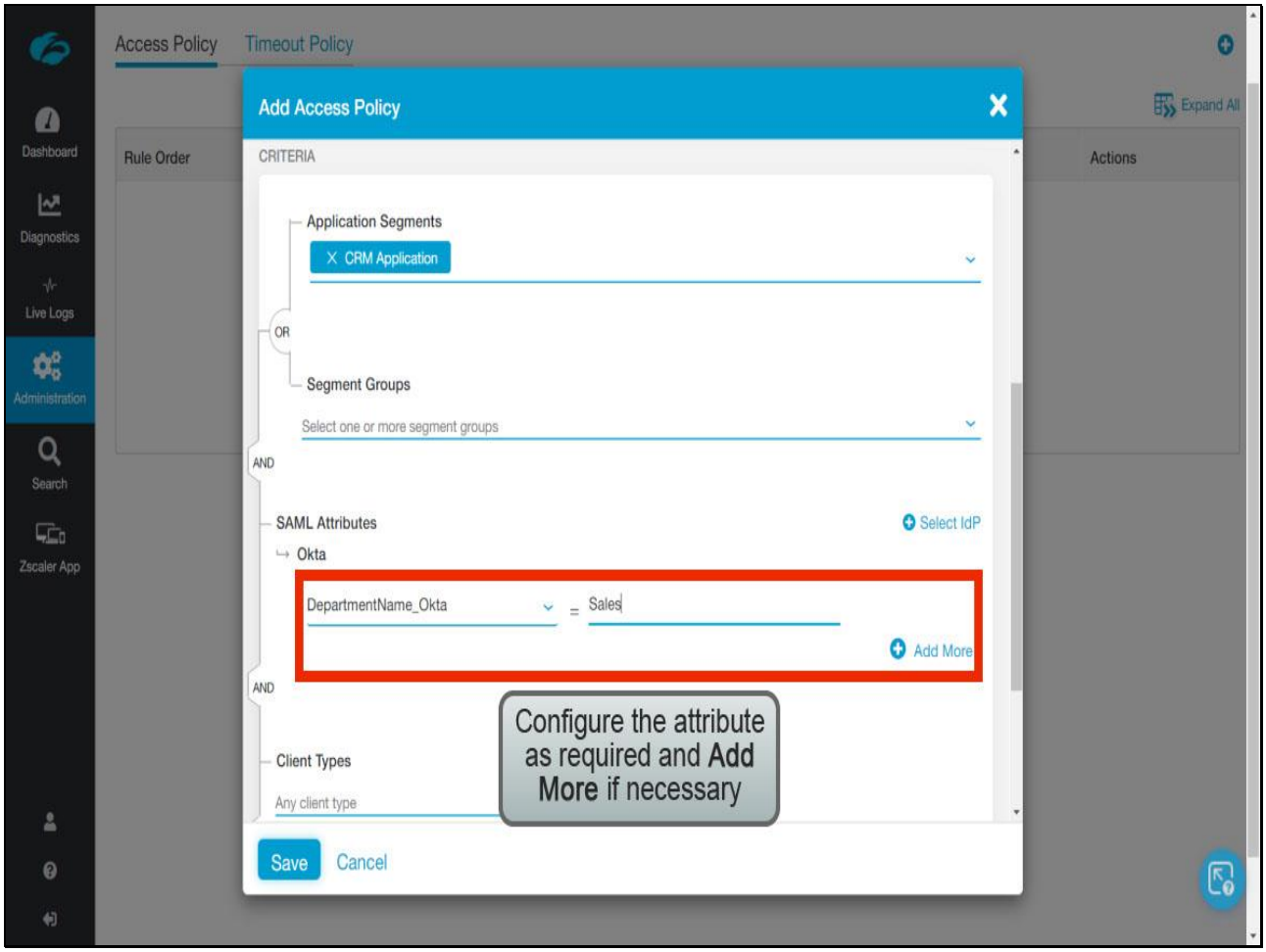
Slide 58 - Slide 58



Slide notes

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

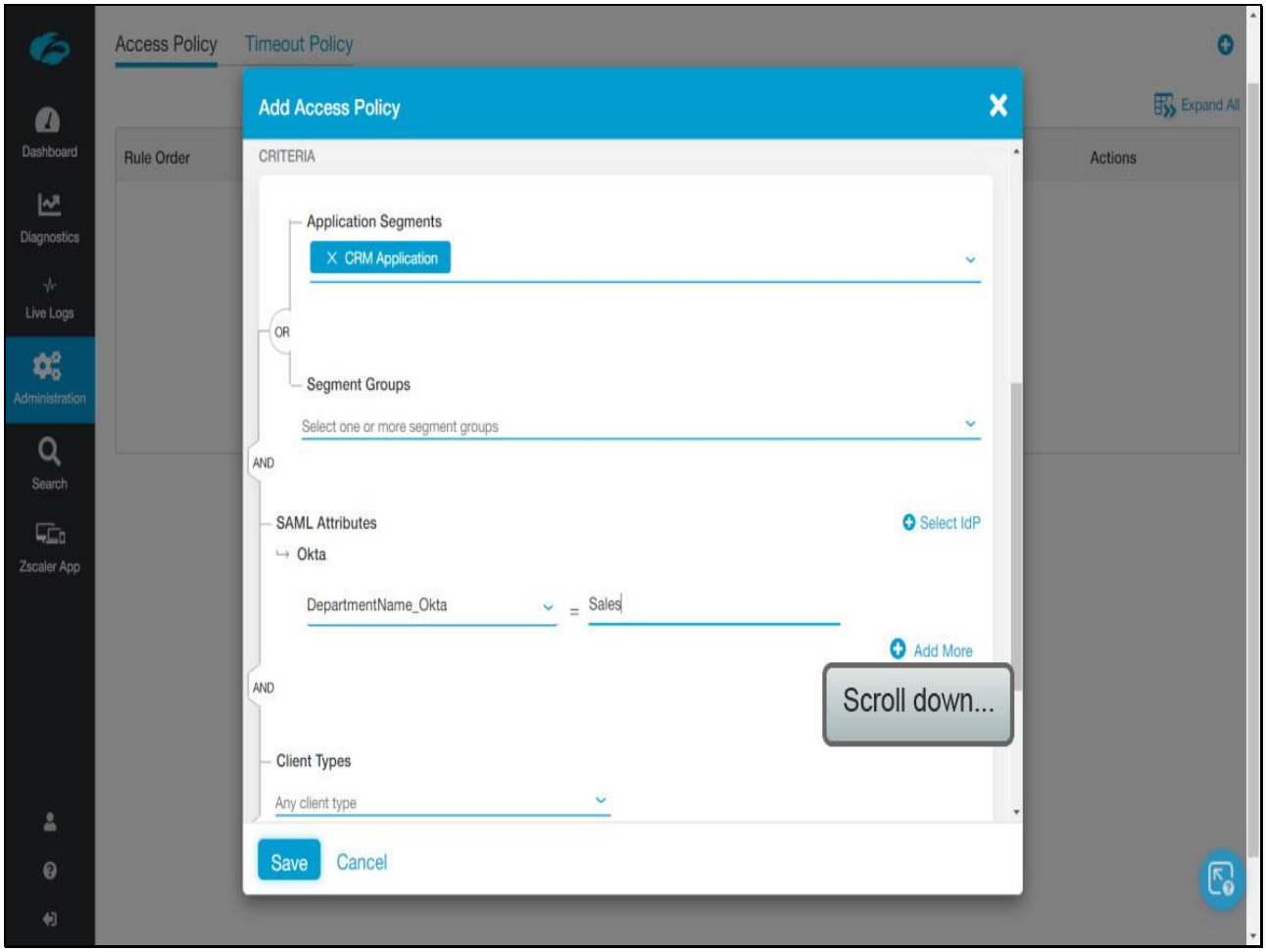
Slide 59 - Slide 59



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.

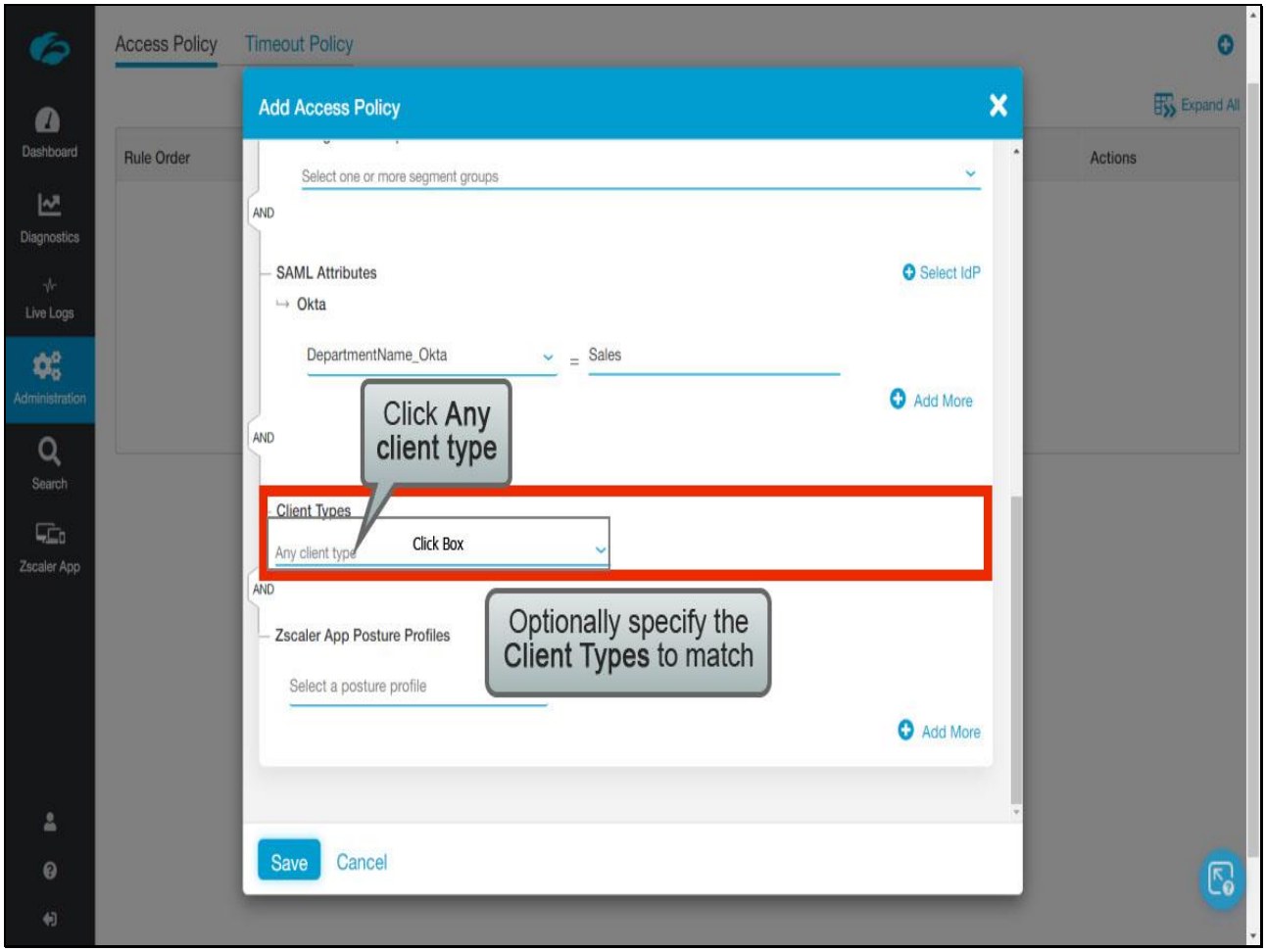
Slide 60 - Slide 60



Slide notes

Scroll down...

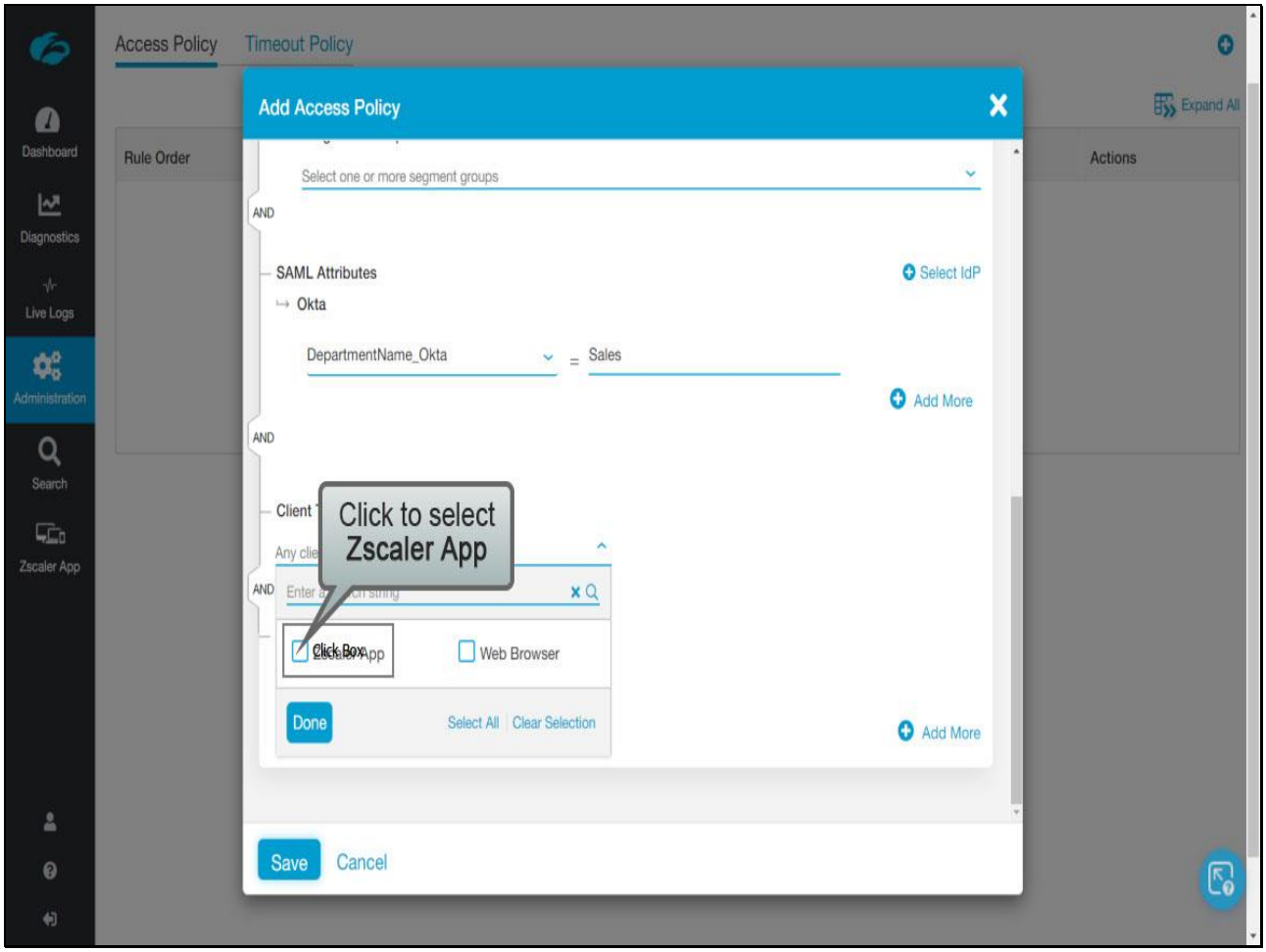
Slide 61 - Slide 61



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**, ...

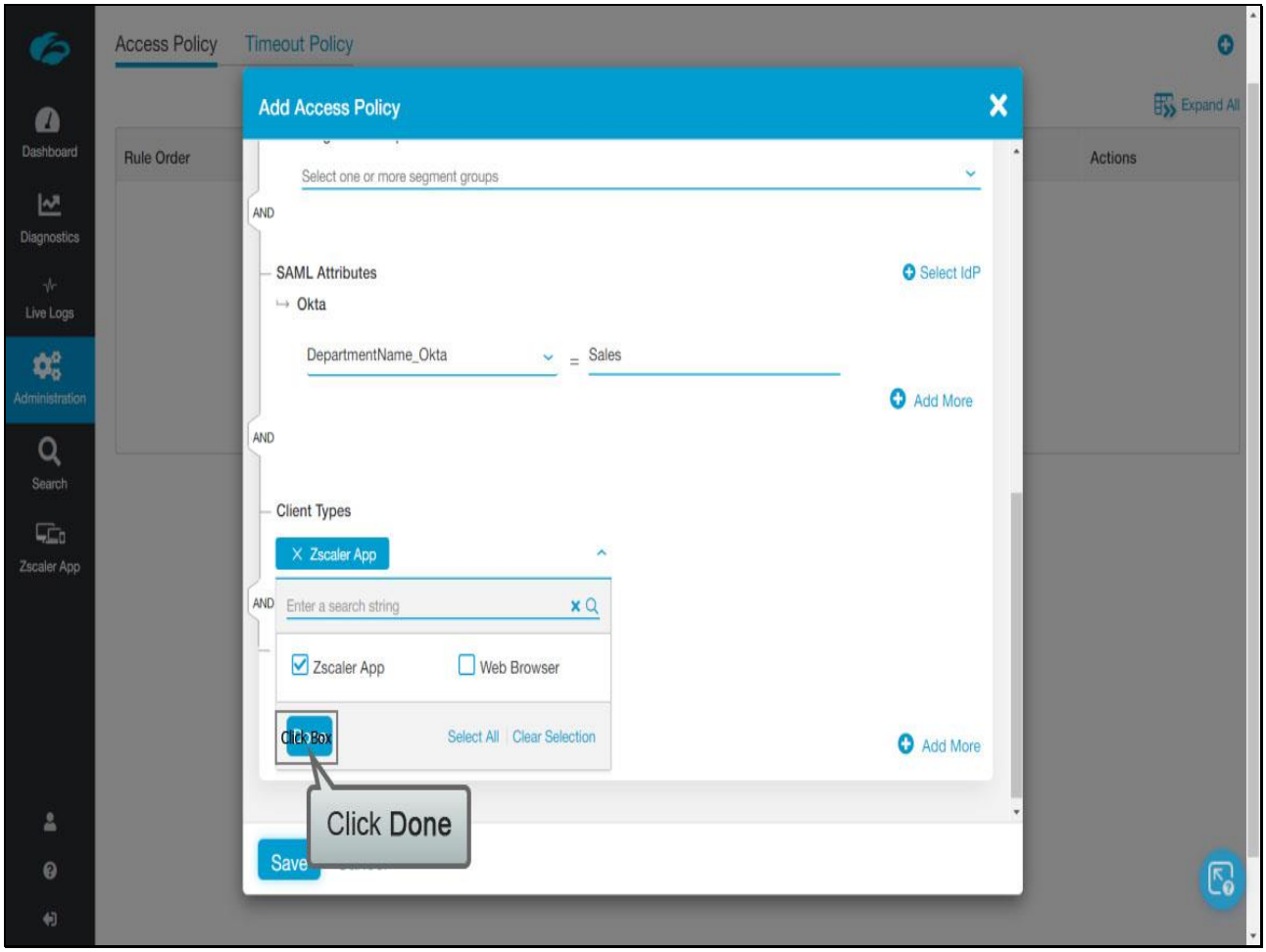
Slide 62 - Slide 62



Slide notes

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

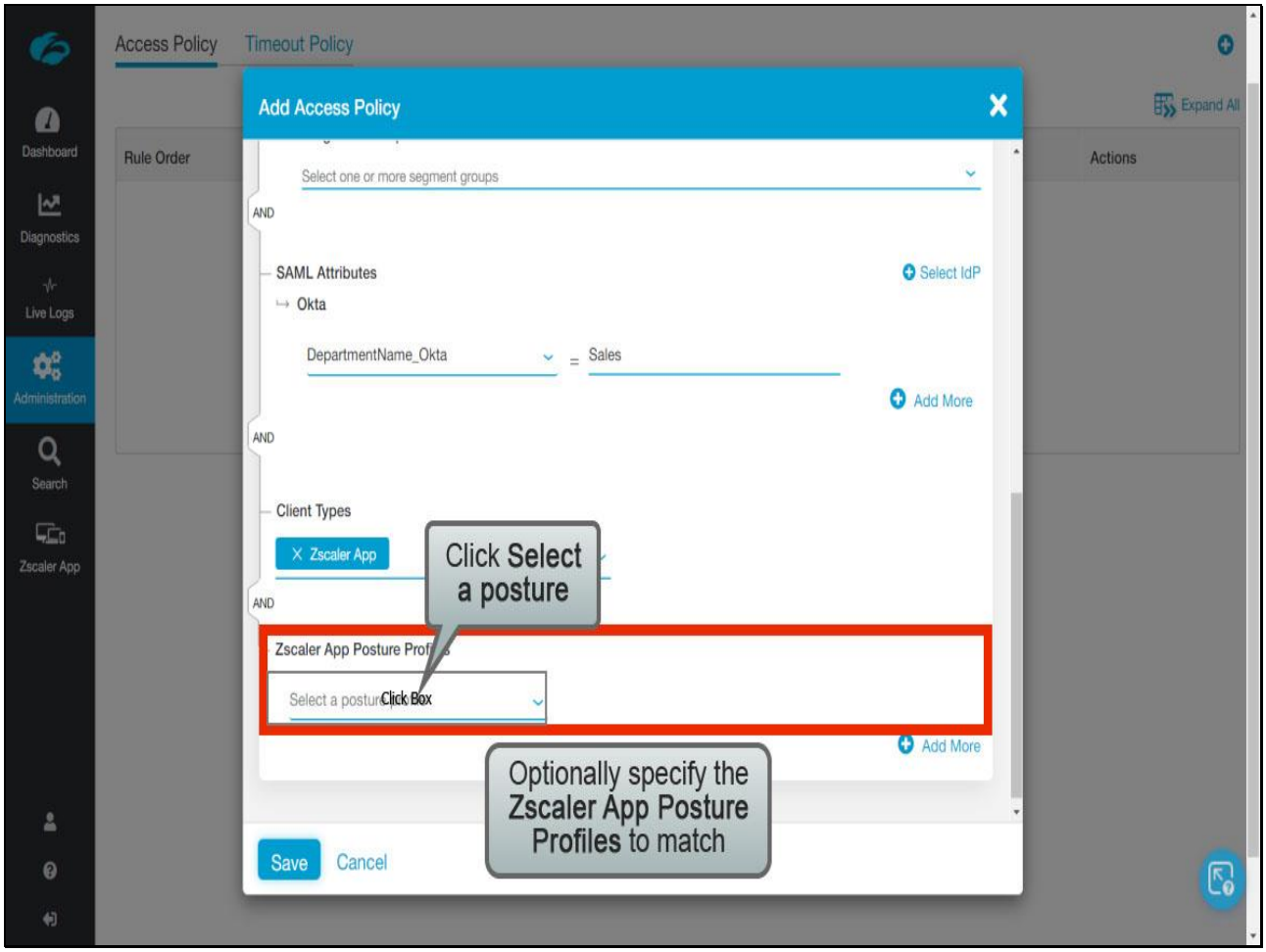
Slide 63 - Slide 63



Slide notes

...and click **Done**.

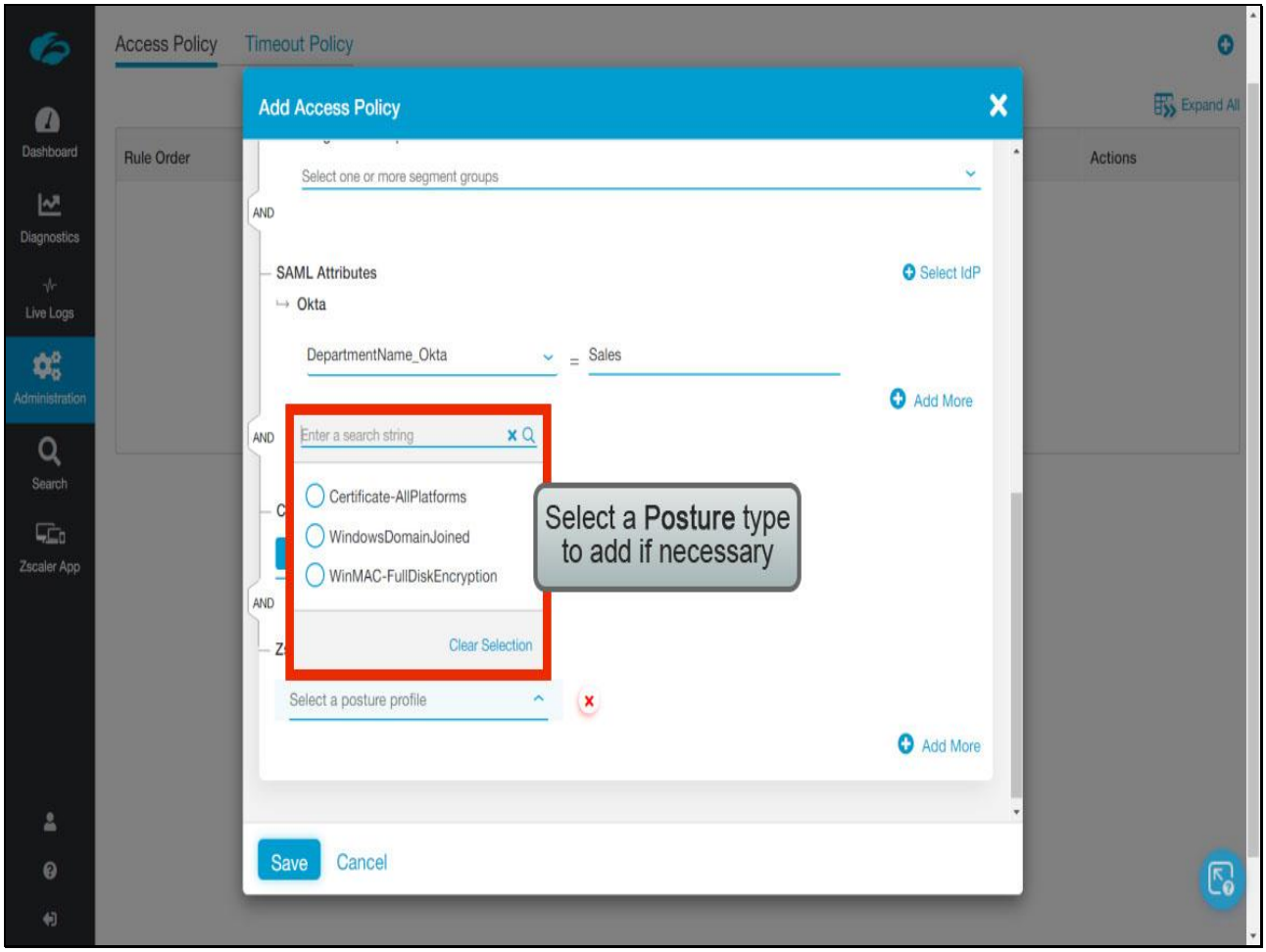
Slide 64 - Slide 64



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**, ...

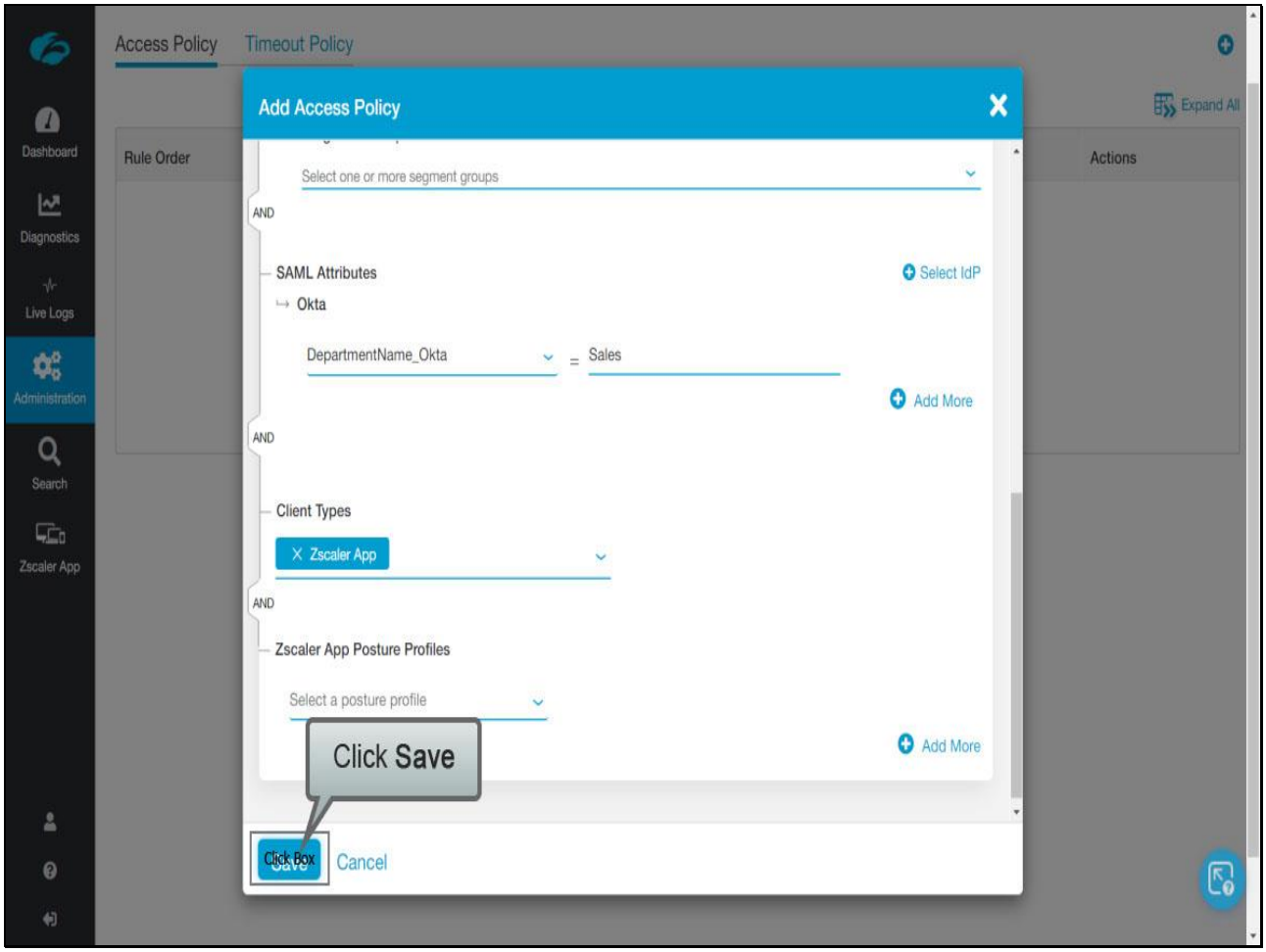
Slide 65 - Slide 65



Slide notes

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

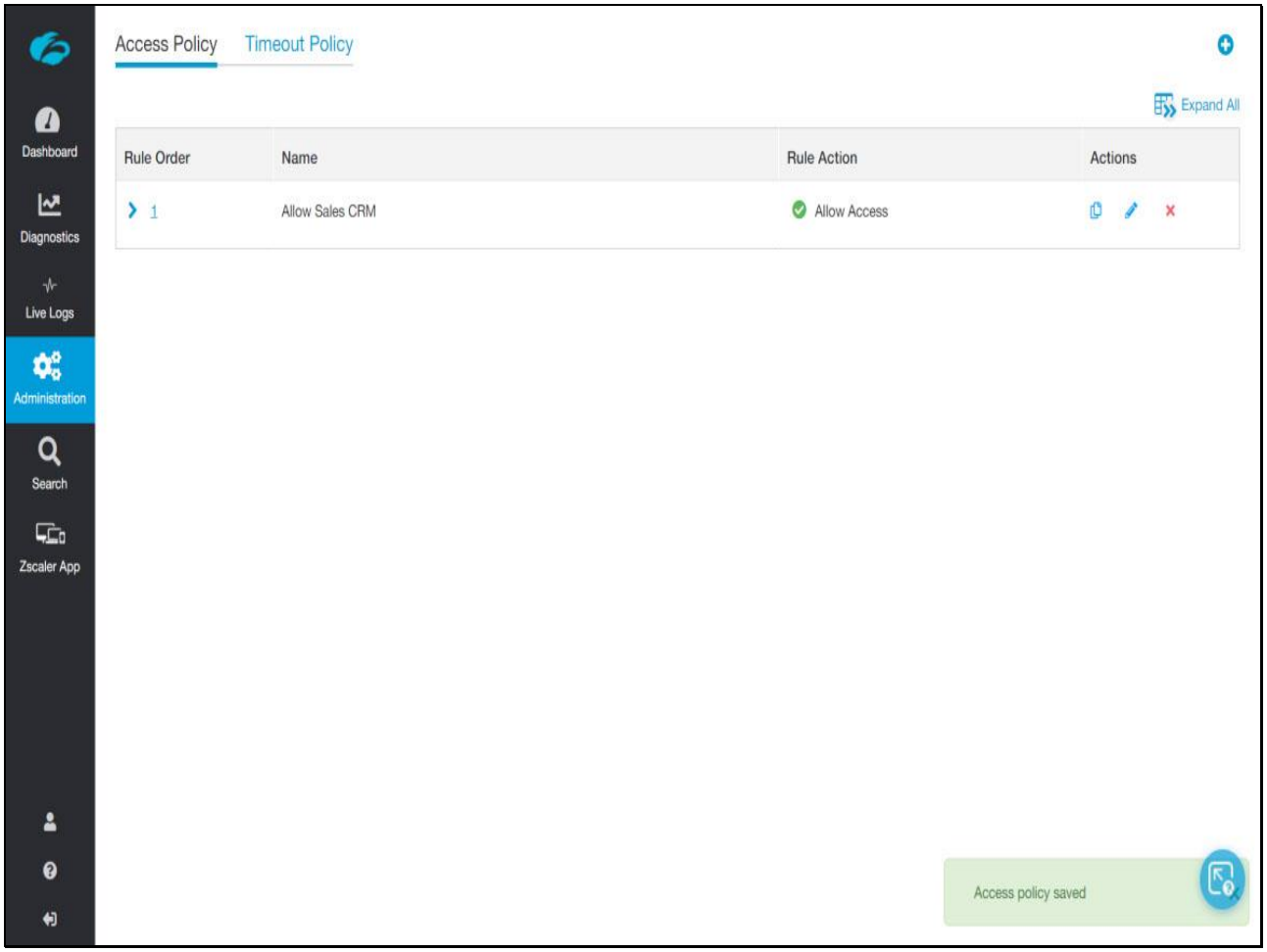
Slide 66 - Slide 66



Slide notes

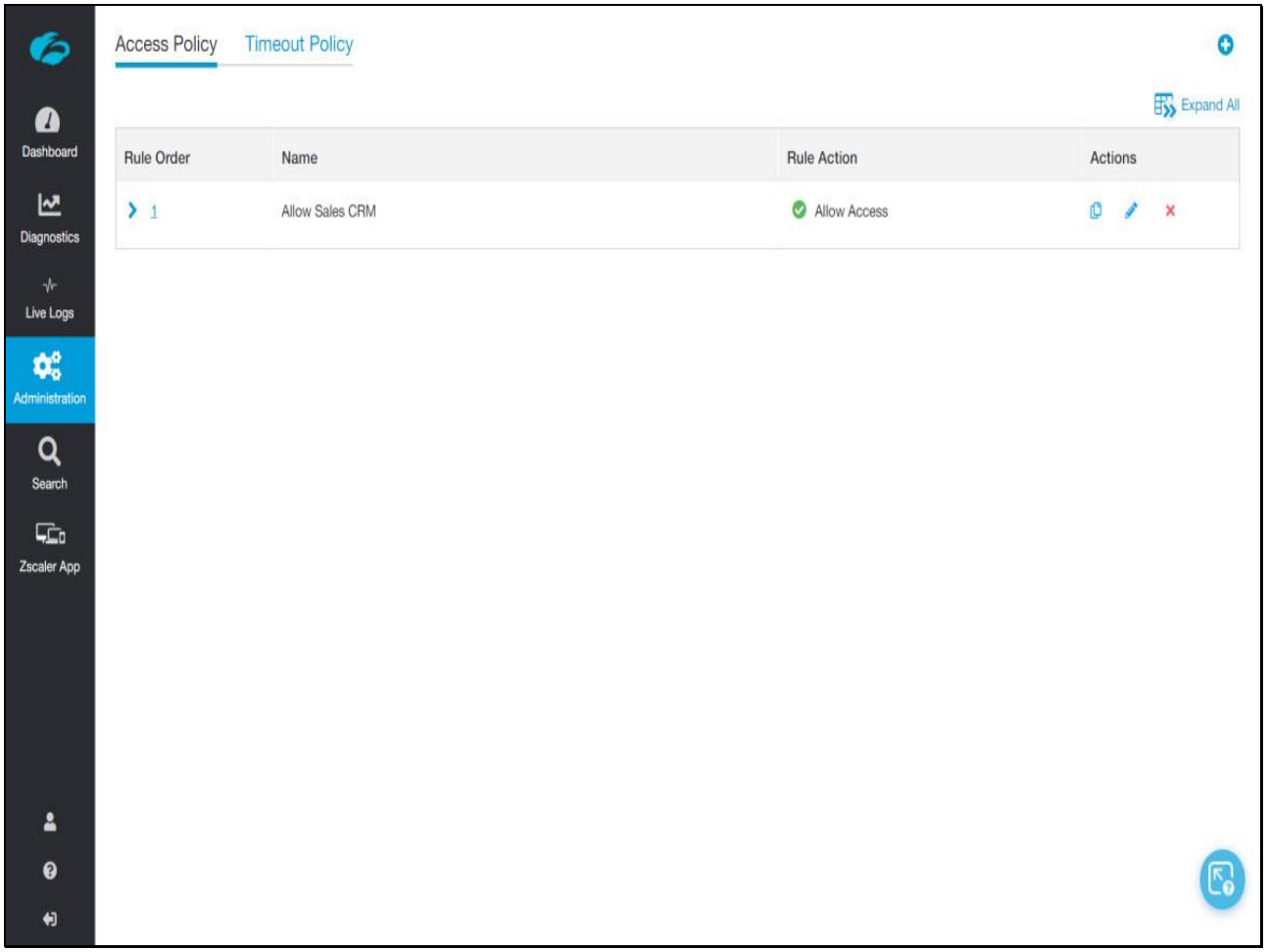
Having configured the policy rule as necessary, click **Save**.

Slide 67 - Slide 67



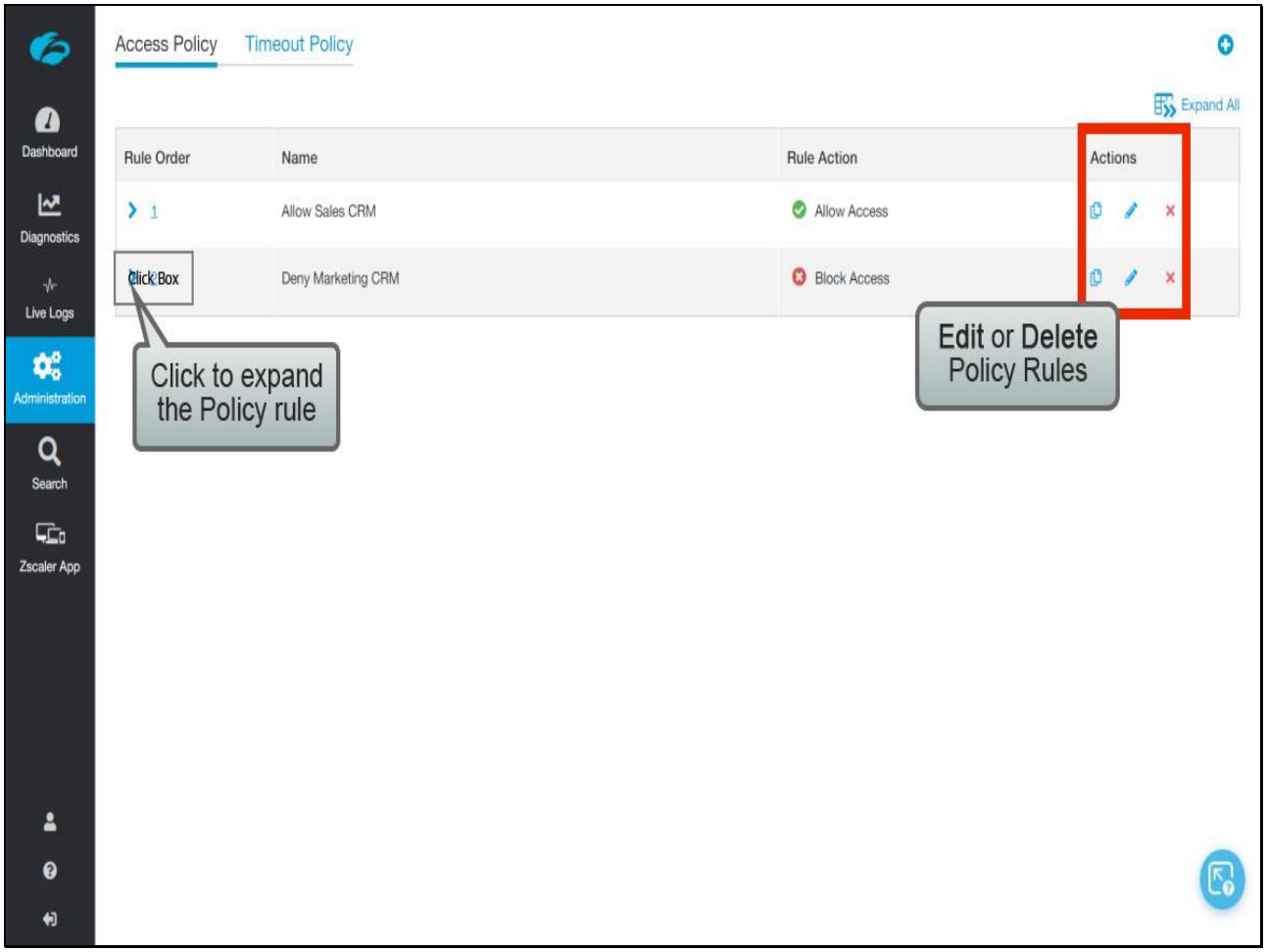
Slide notes

Slide 68 - Slide 68



Slide notes

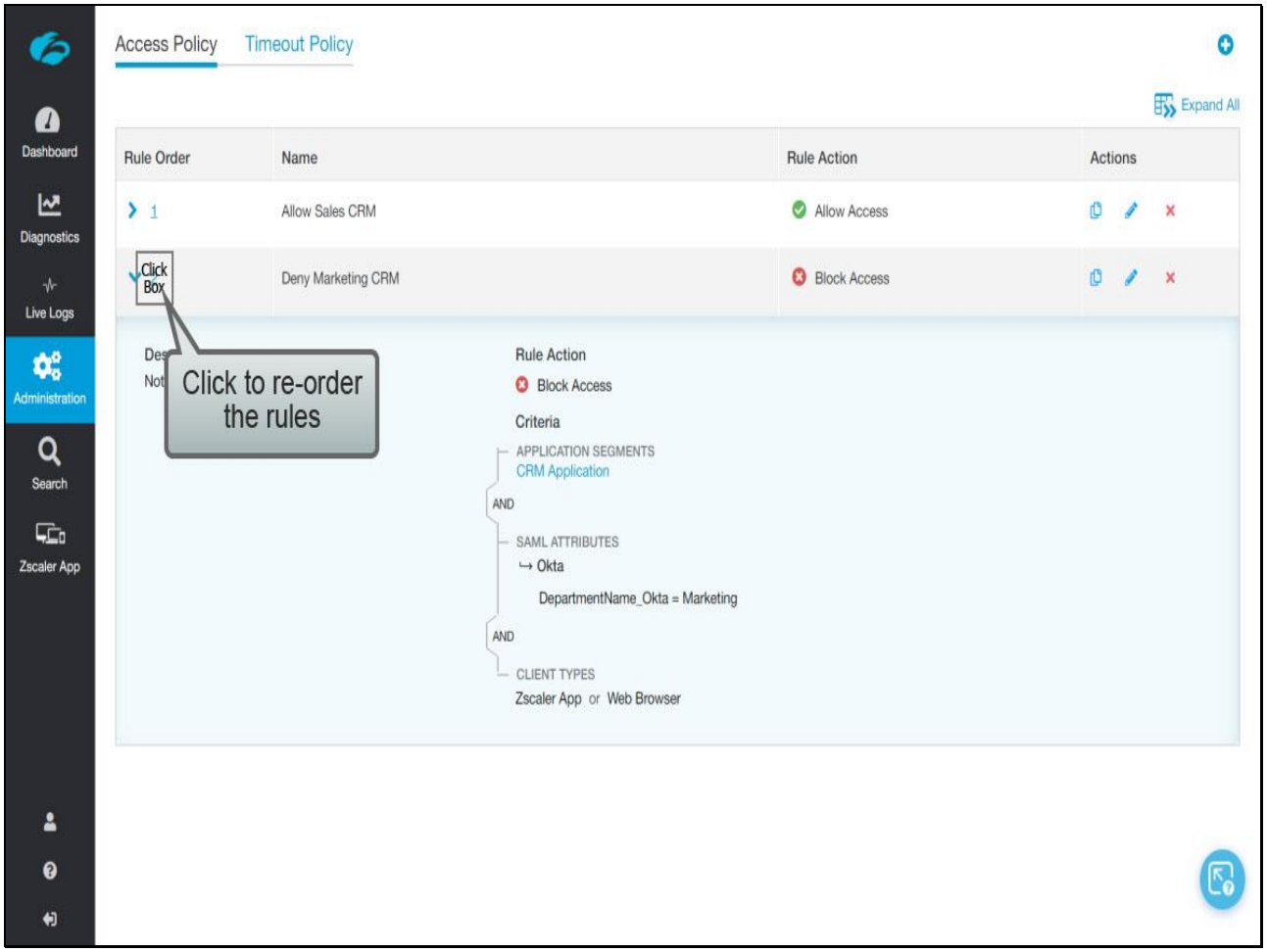
Slide 69 - Slide 69



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, ...

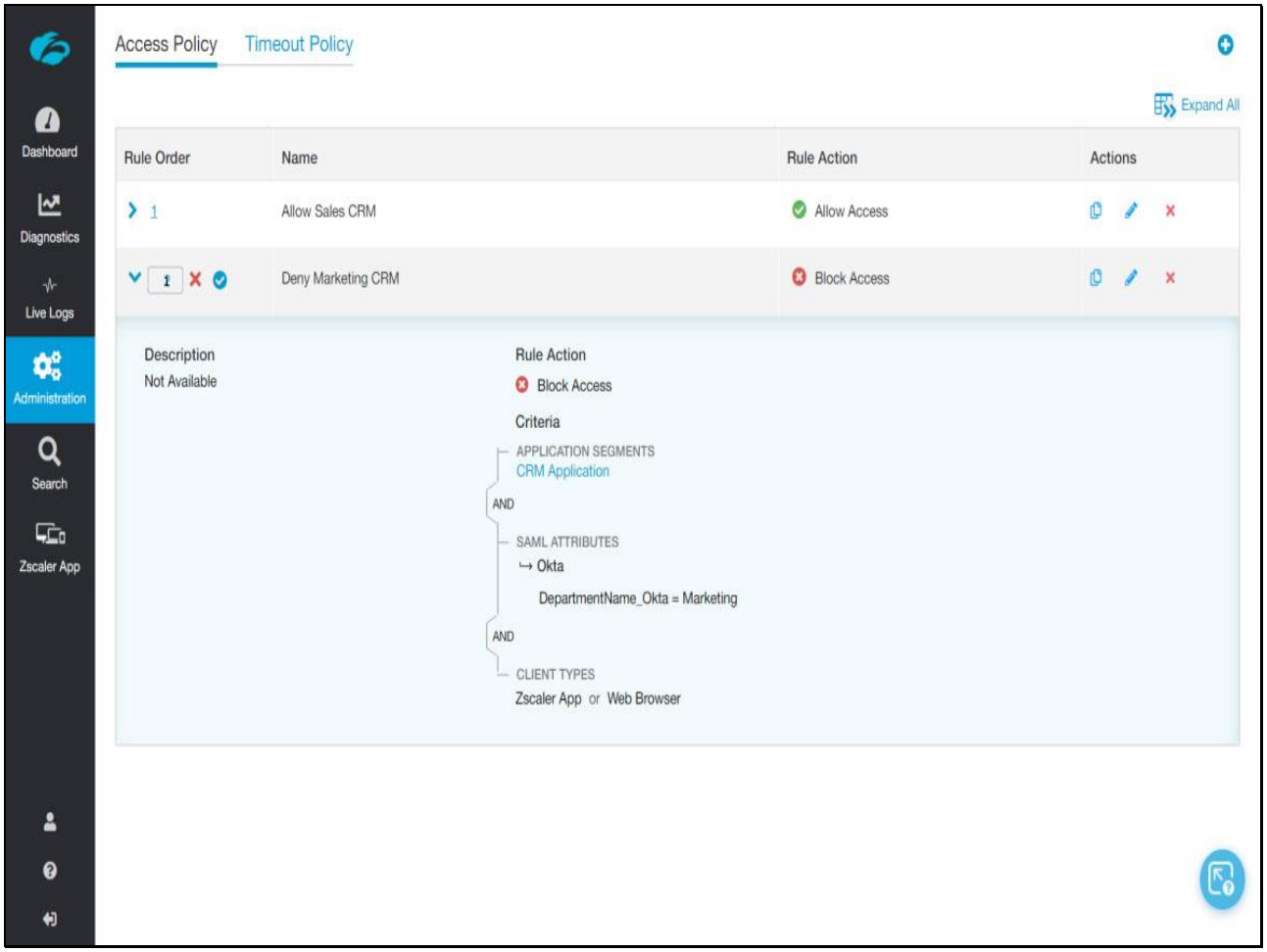
Slide 70 - Slide 70



Slide notes

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

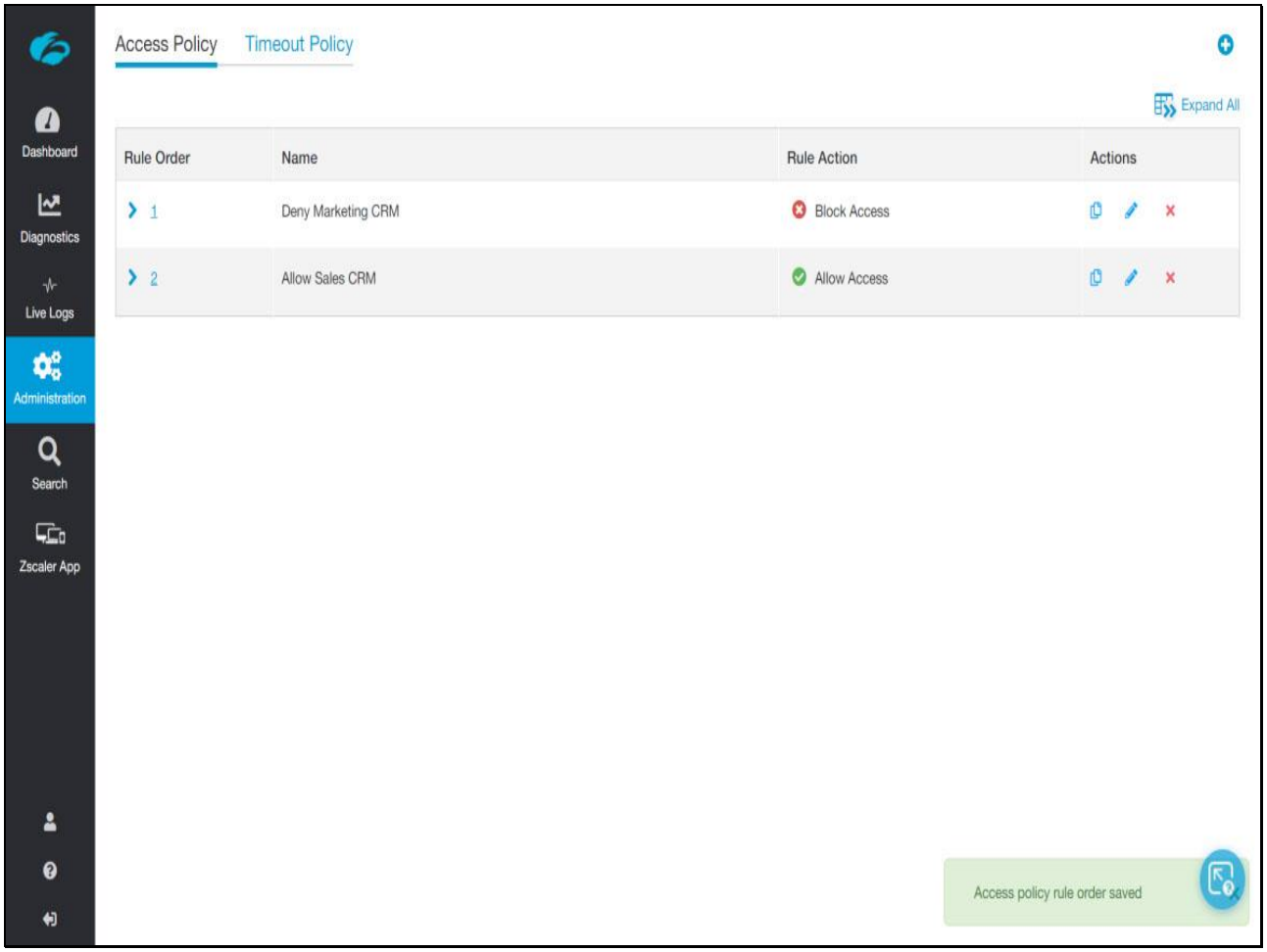
Slide 71 - Slide 71



Slide notes

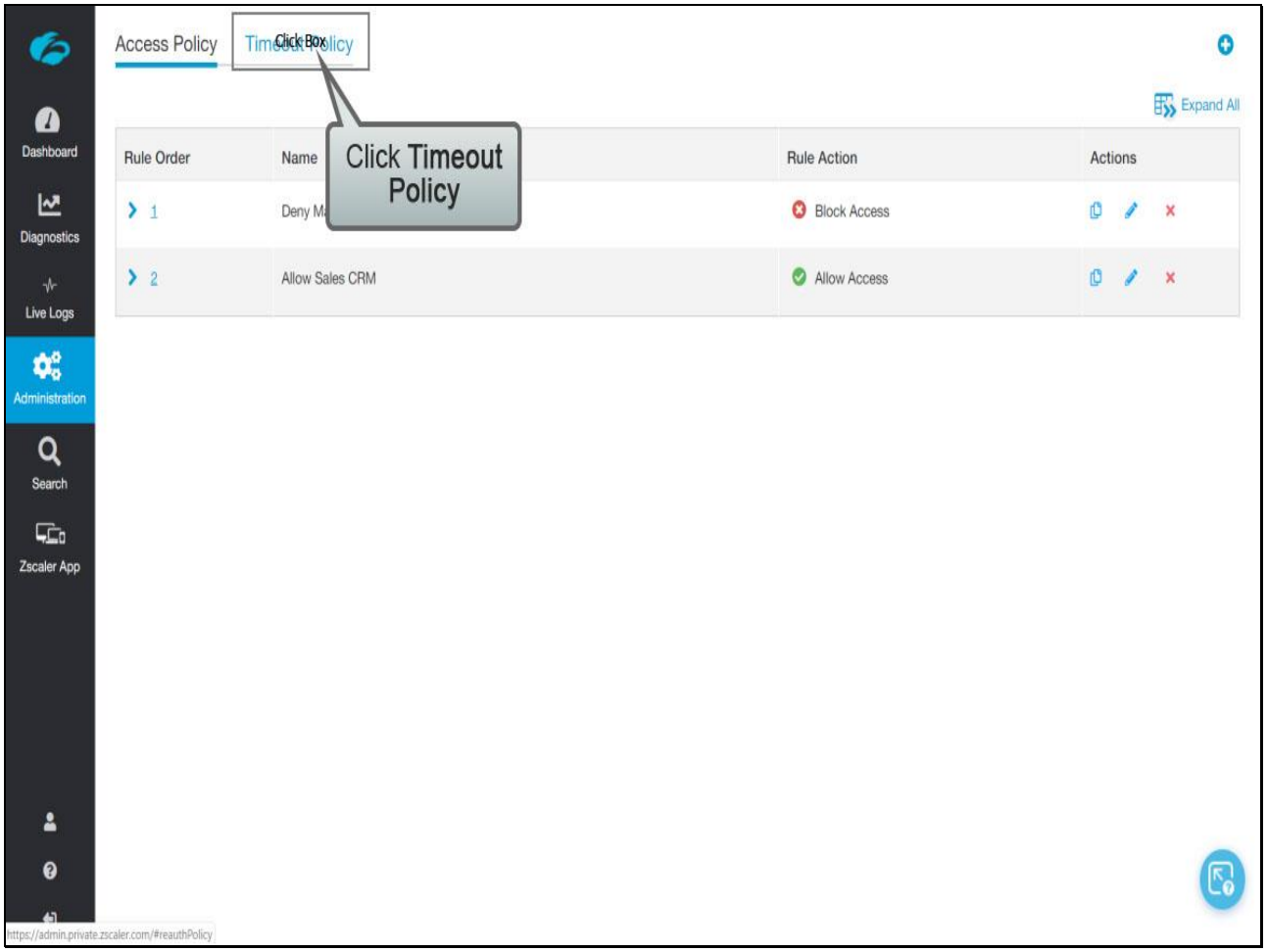
...and type the new rule order number for this rule (1 in this case).

Slide 72 - Slide 72



Slide notes

Slide 73 - Slide 73

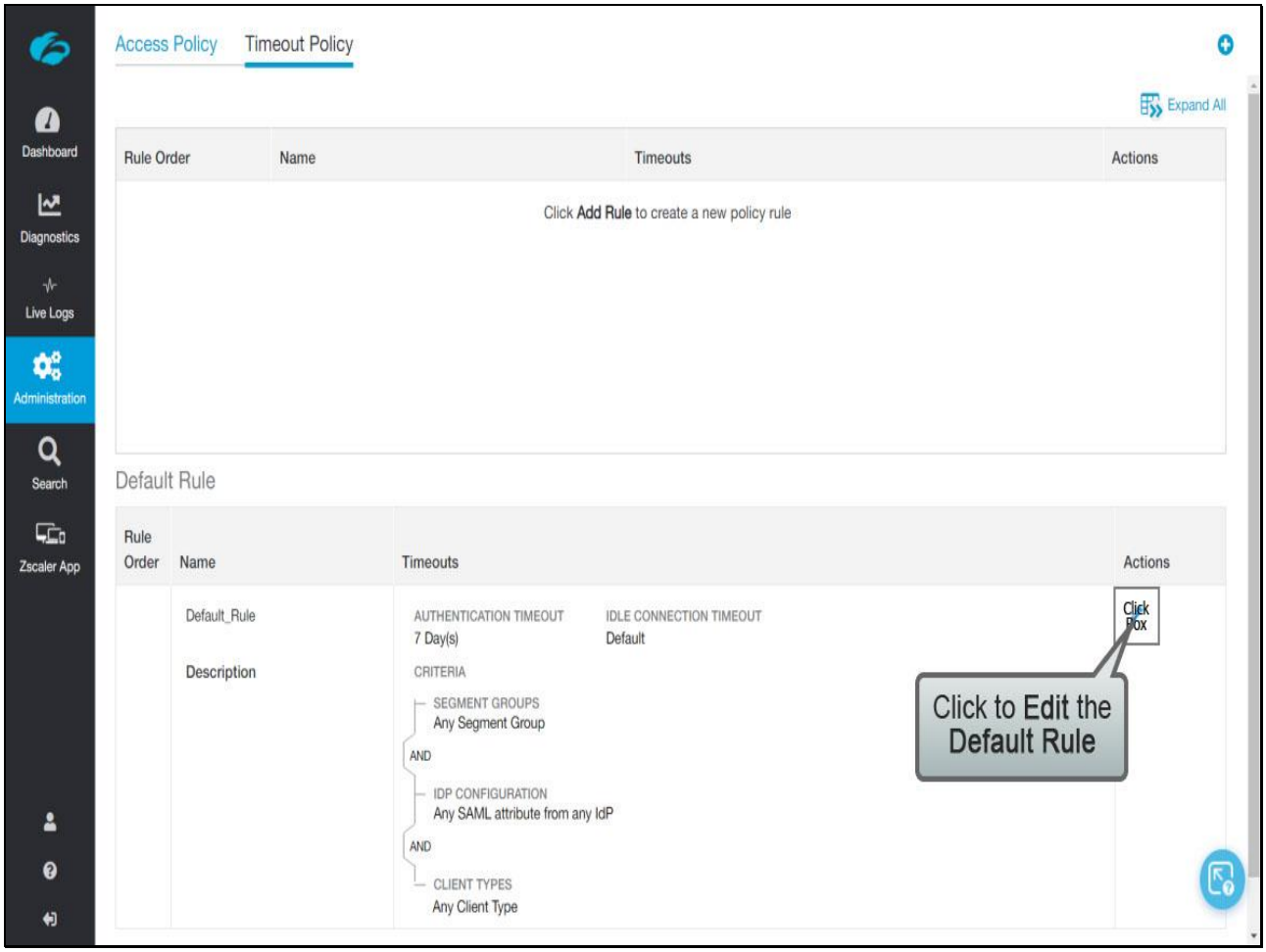


Slide notes

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**.

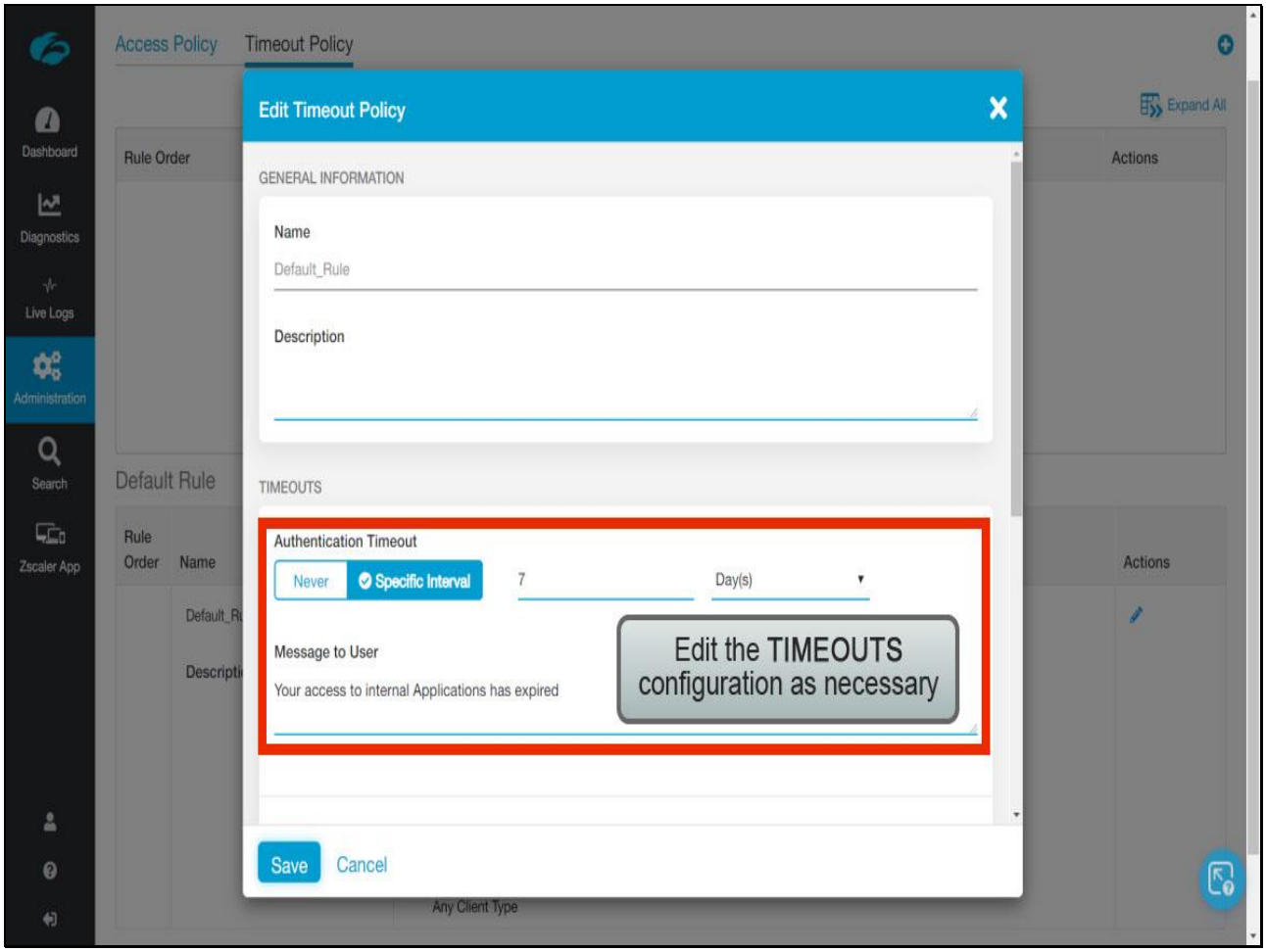
Slide 74 - Slide 74



Slide notes

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

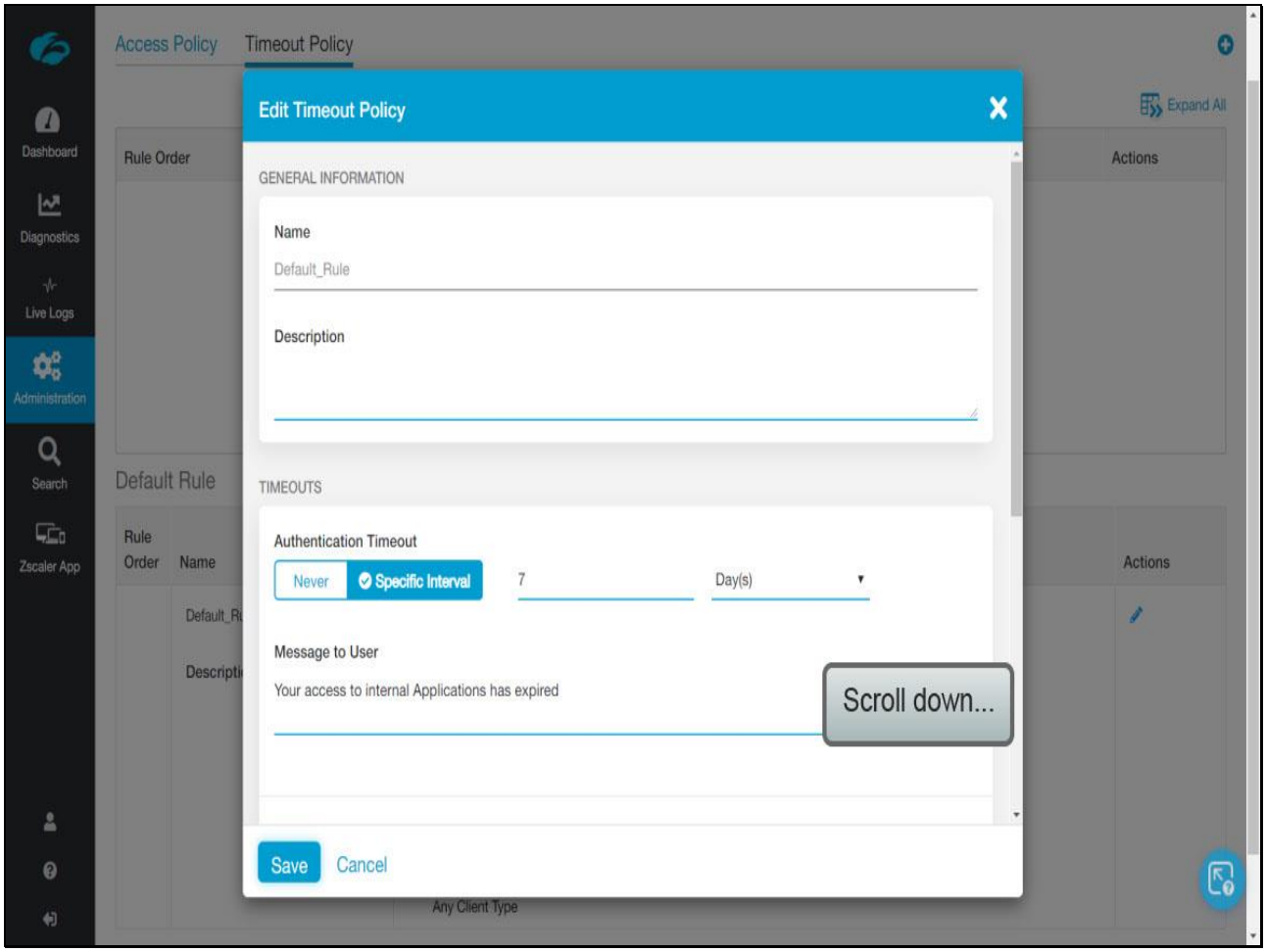
Slide 75 - Slide 75



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)**.

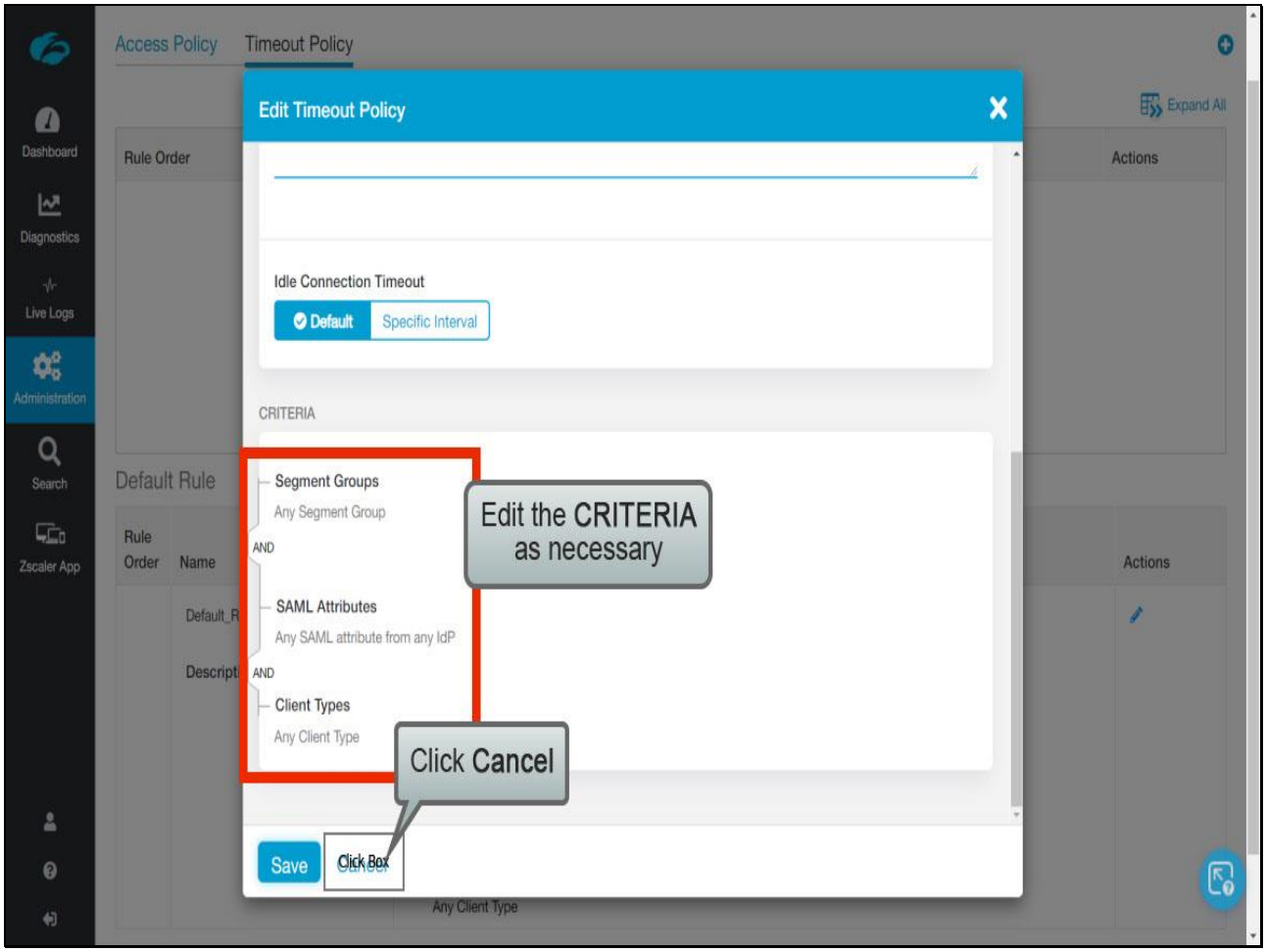
Slide 76 - Slide 76



Slide notes

Scroll down...

Slide 77 - Slide 77

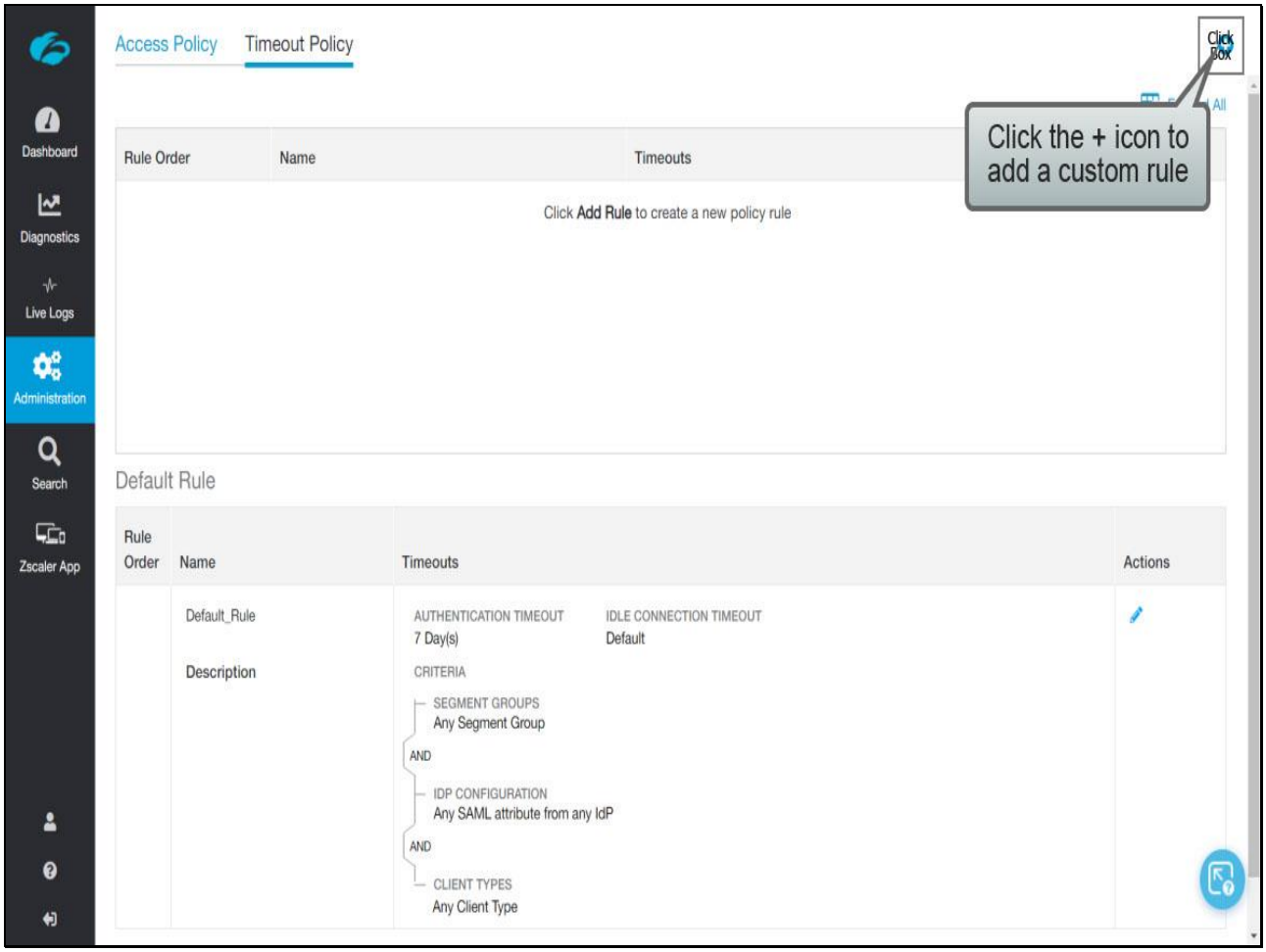


Slide notes

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.

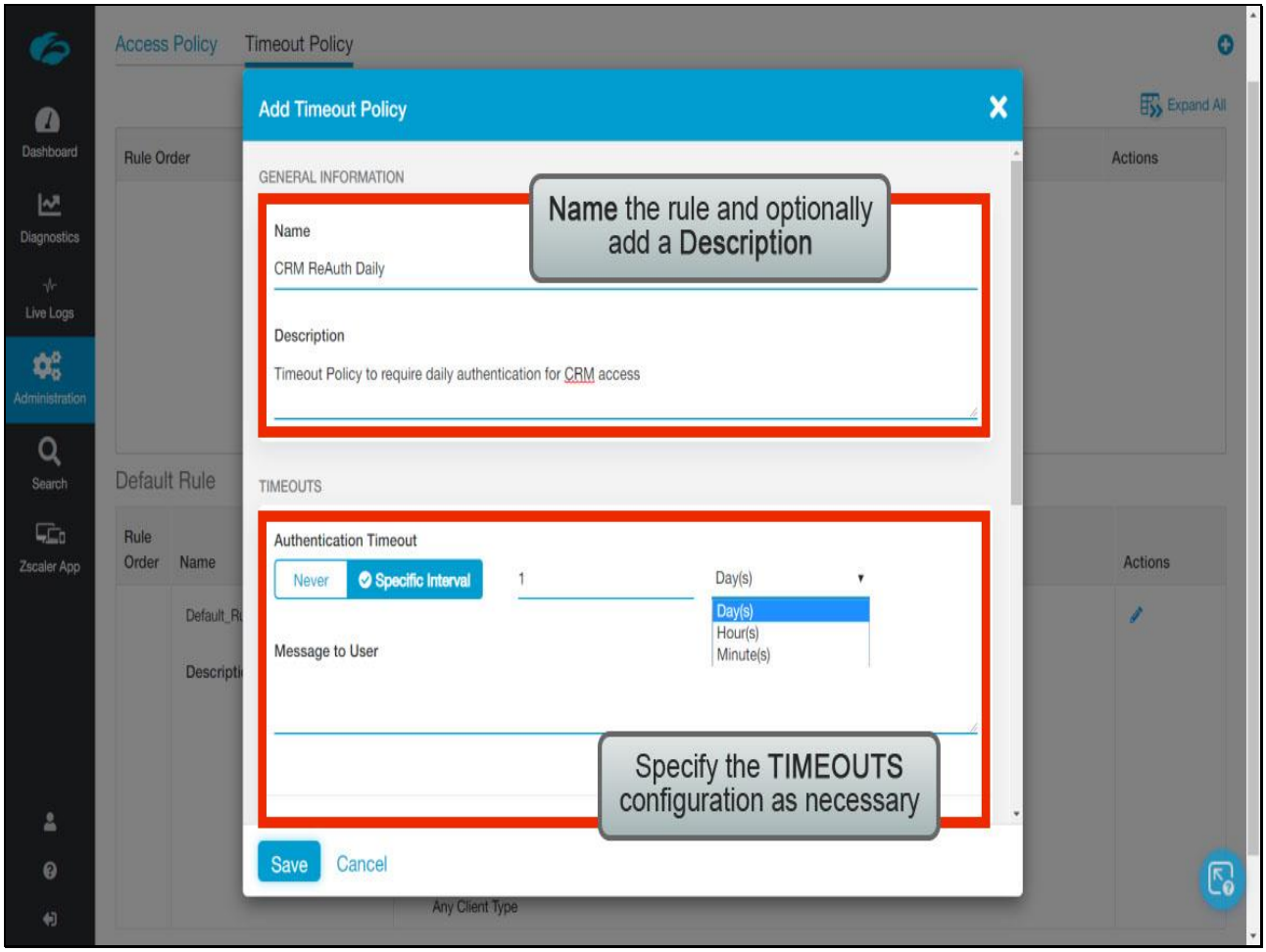
Slide 78 - Slide 78



Slide notes

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

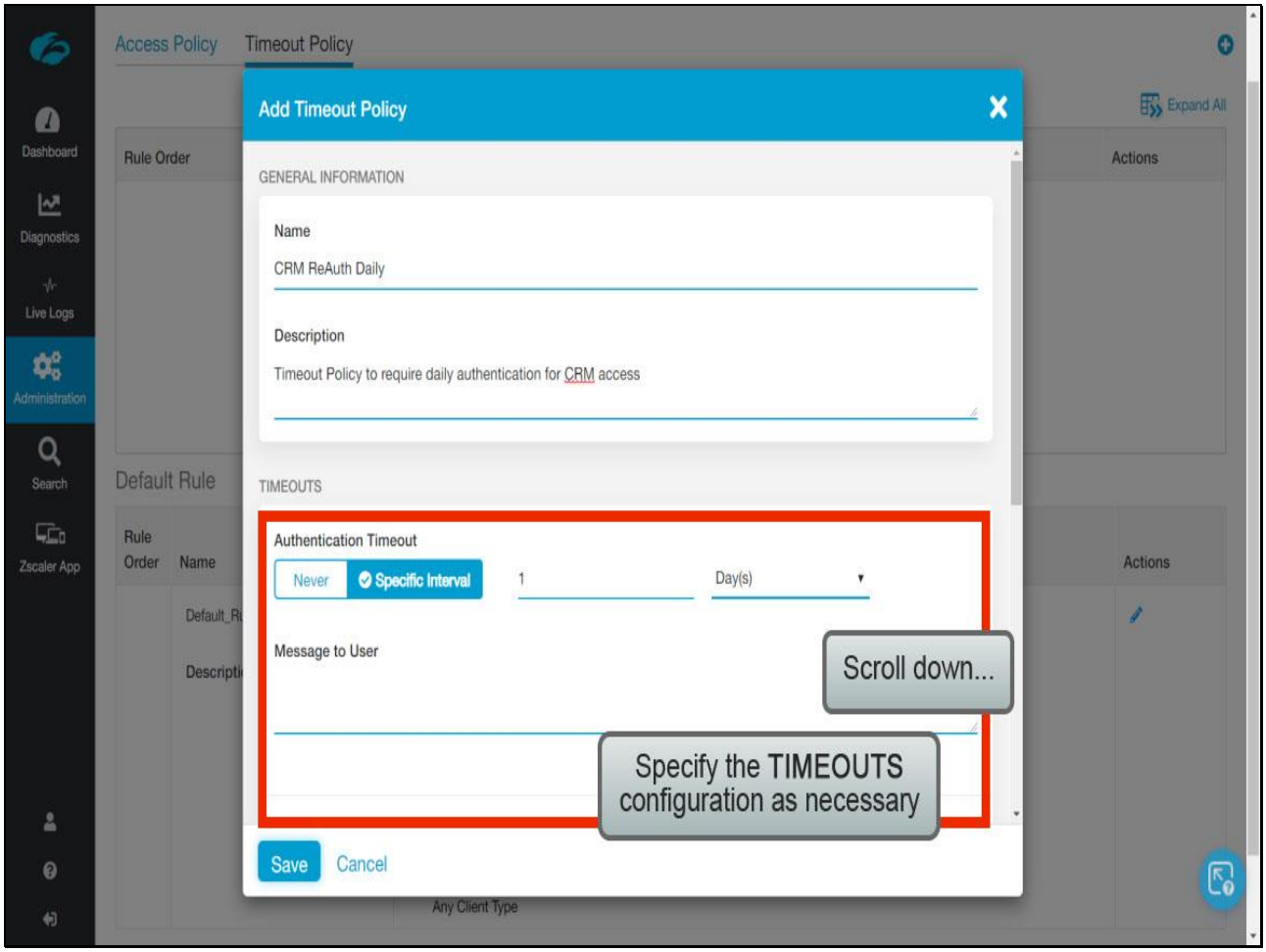
Slide 79 - Slide 79



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, ...

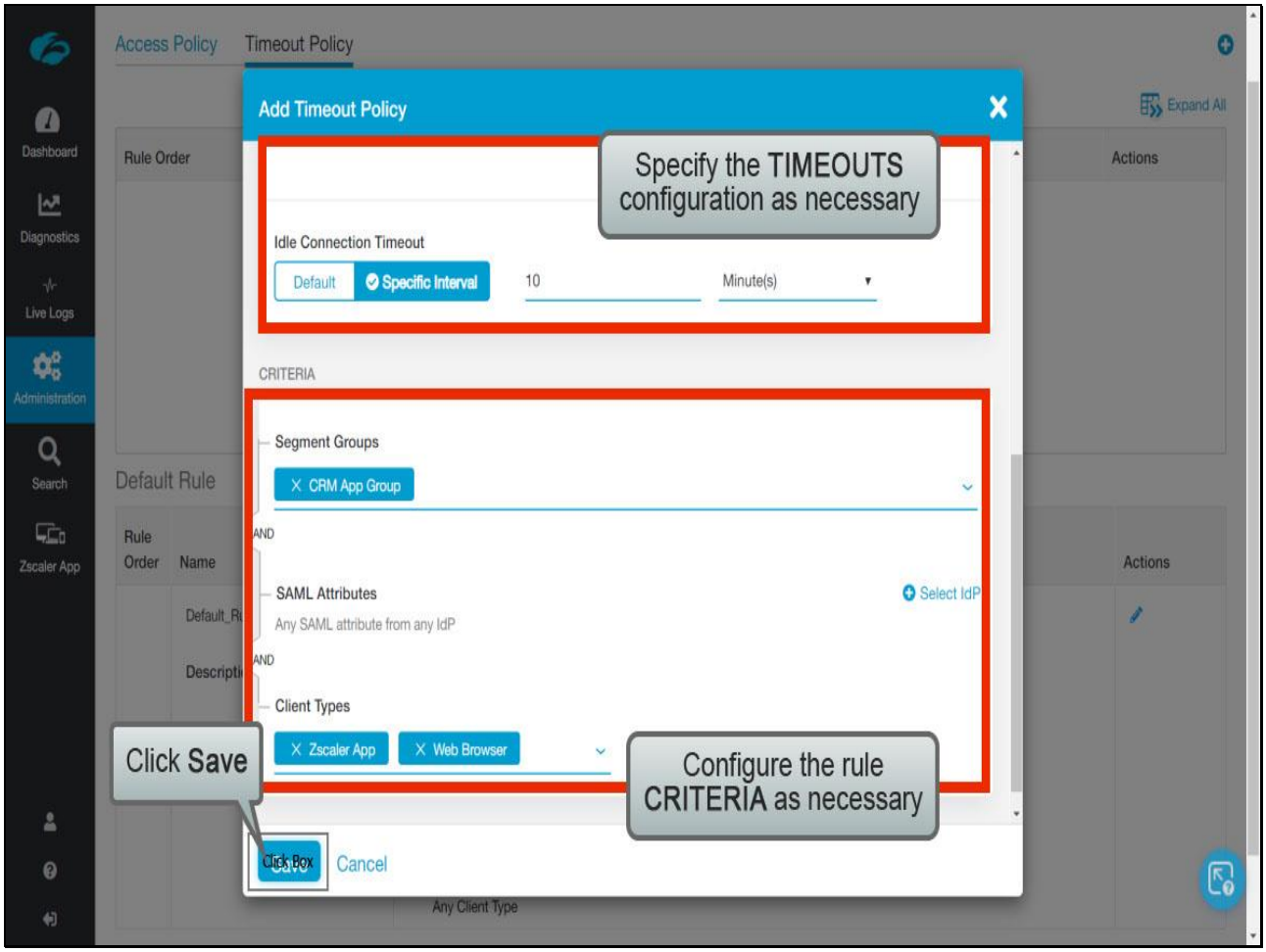
Slide 80 - Slide 80



Slide notes

Scroll down...

Slide 81 - Slide 81

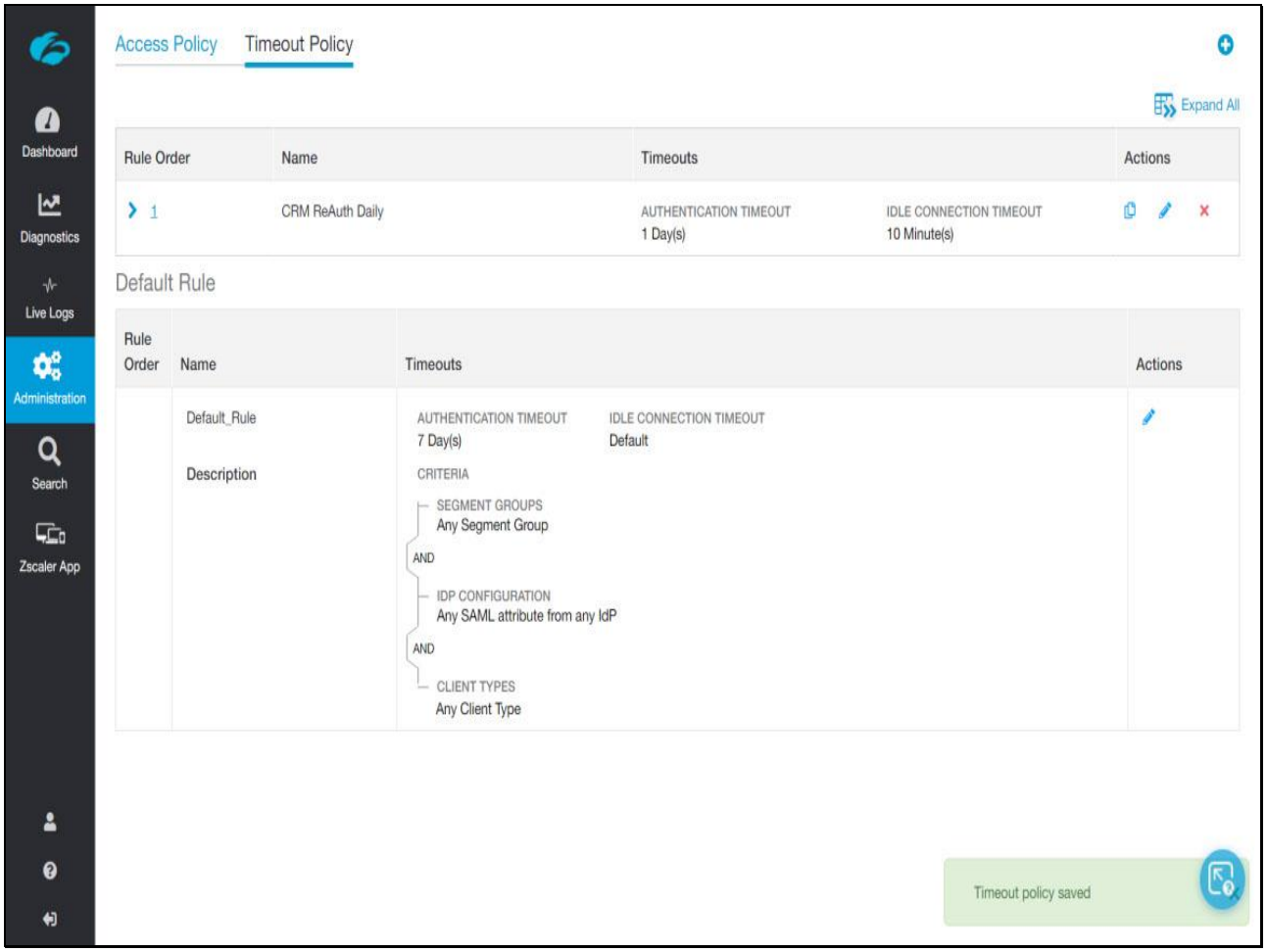


Slide notes

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

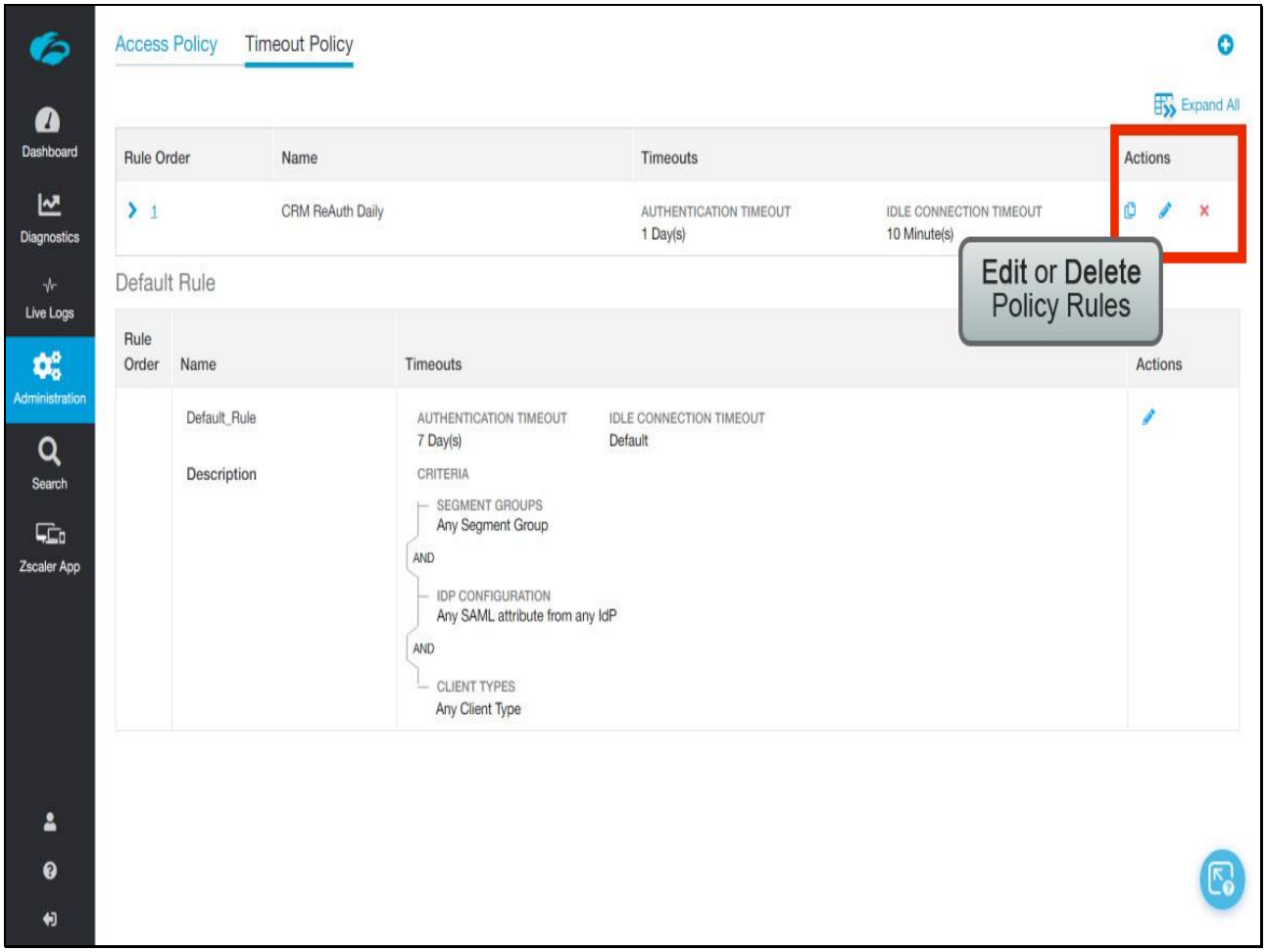
In the **CRITERIA** section, you can target the rule by; **Segment Groups**, **SAML Attributes**, or **Client Types**. Once the rule is configured, click **Save**.

Slide 82 - Slide 82



Slide notes

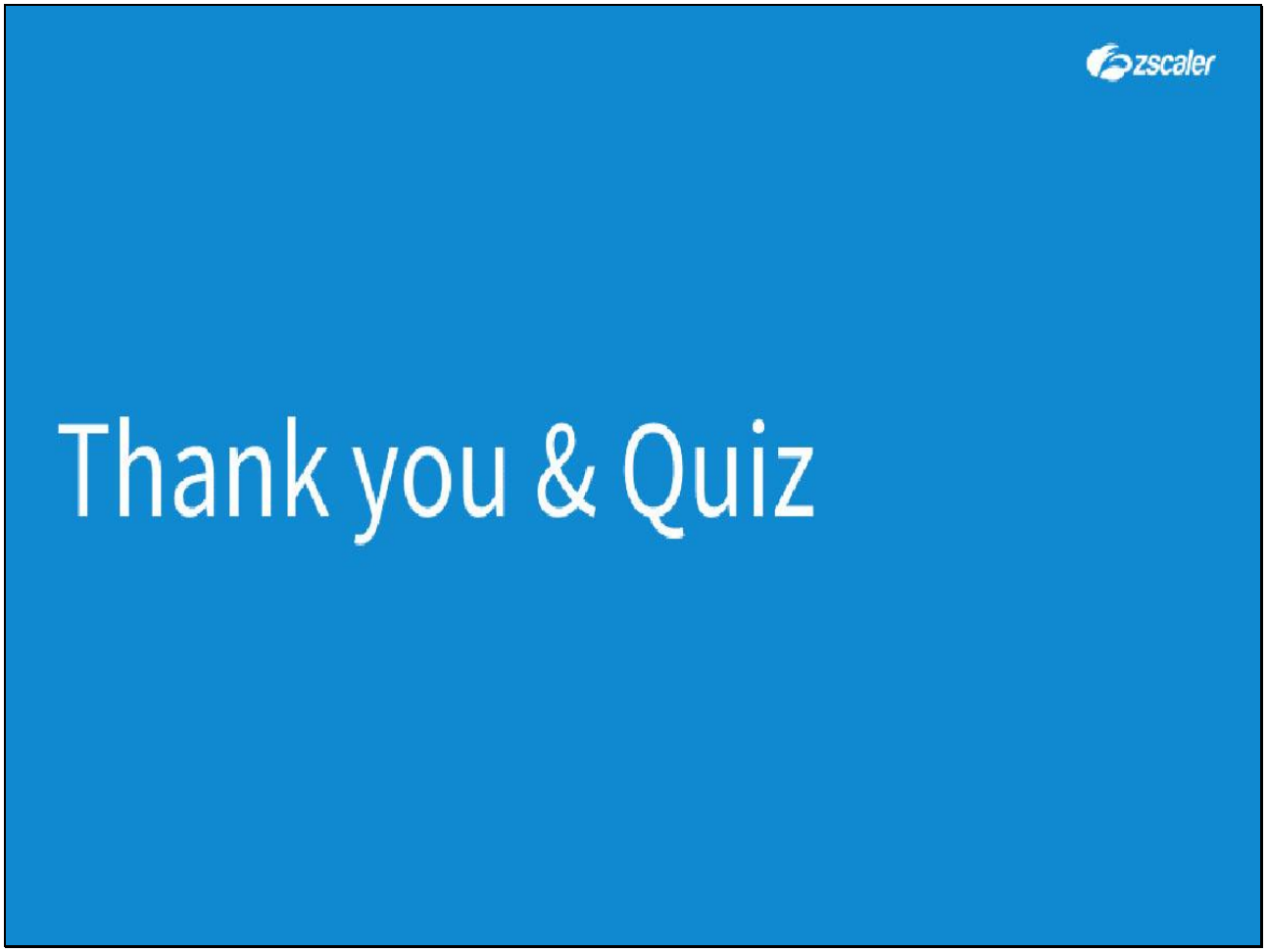
Slide 83 - Slide 83



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.