

Slide 1 – The Zscaler App: ZPA Specific Configurations



The Zscaler App

ZPA Specific Configurations

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on Zscaler App configurations that are specific to the ZPA service.

Slide 2 - Navigating the eLearning Module

The screenshot shows the Zscaler eLearning module dashboard. At the top right is the Zscaler logo. Below it, the title "Navigating the eLearning Module" is displayed. The dashboard has several sections: "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). On the left, there's a sidebar with "Dashboard", "Diagnostics", "Live Logs", "Administration", and a "Search" bar. The main content area includes a "TOP APPLICATIONS BY BANDWIDTH" chart and a "TOP POLICY BLOCKS" section. A progress bar at the bottom indicates "97.11% of Total Tr". Several blue callout boxes highlight specific controls: "Play/Pause" points to a video player control; "Previous Slide" and "Next Slide" point to navigation arrows; "Progress Bar" points to the progress bar at the bottom; "Audio On/Off" and "Closed Captioning" point to audio controls; and "Exit" points to the top-right exit button.

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



- Interactive Demos:
 - Configure Forwarding Profile Options
 - Zscaler Service Entitlement
 - Device Posture

Slide notes

In this module we will discuss the configuration of the following Zscaler App settings for ZPA: The available **Forwarding Profile** options; the **Zscaler Service Entitlement** option, for controlling which of your user groups have access to ZPA functionality; and at the available **Device Posture** options.

Slide 4 - Interactive Demo: Provisioning the Zscaler App

**Slide notes**

In the next section we will walk through the configuration of the Zscaler App.

This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler App Portal User Interface. 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 5 - Steps For Using the Zscaler App IdP



Forwarding Profile Options

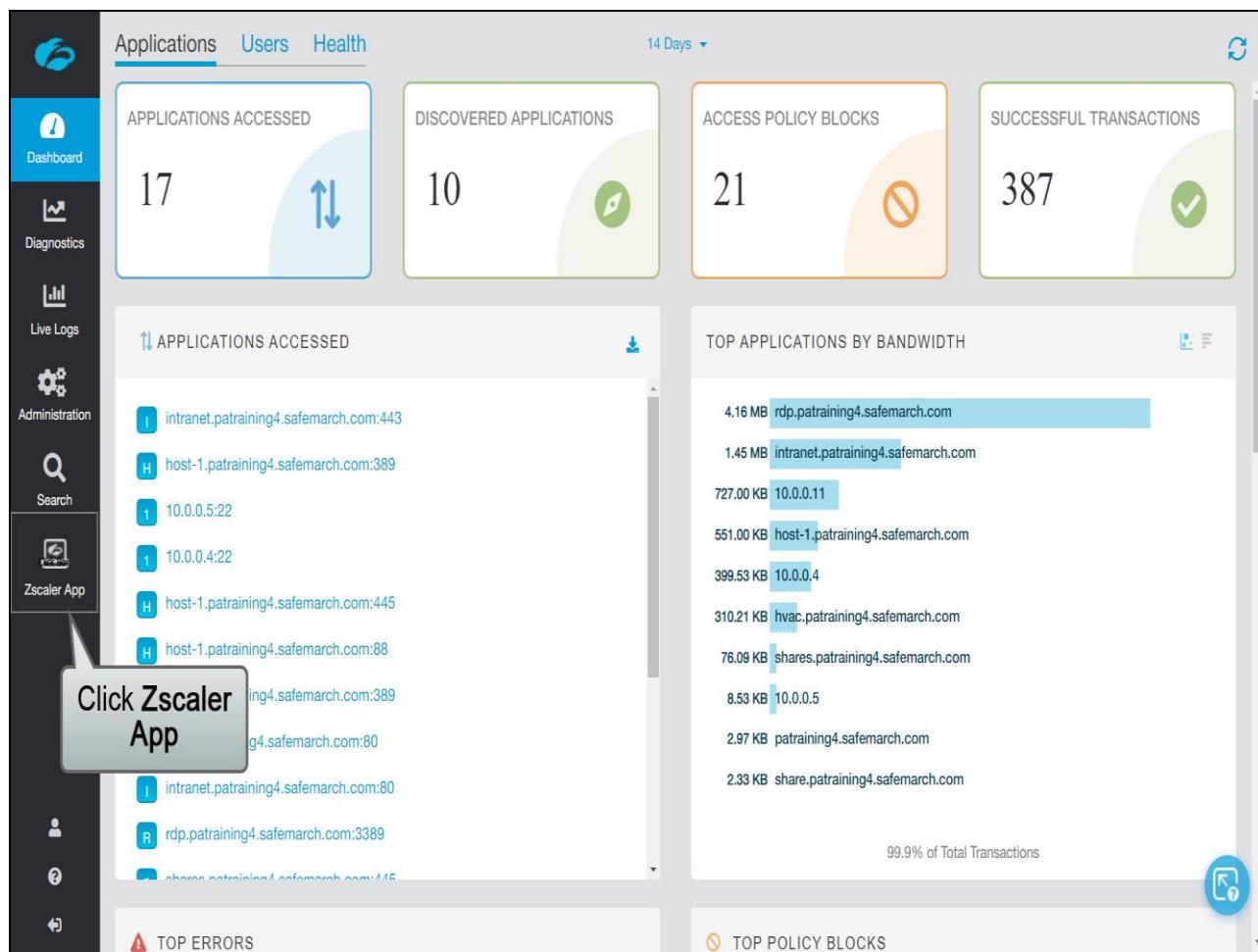
Identify the Network Using TRUSTED NETWORK CRITERIA

- On Trusted Network
- Off Trusted Network
- VPN Trusted Network

Slide notes

Forwarding Profiles can be used to control whether traffic is forwarded by the Zscaler App for Private access. The first key configuration options here are to allow the App to identify the network the device is currently connected to, whether it is **On Trusted Network**, **Off Trusted Network**, or **VPN Trusted Network**.

Slide 6 - Slide 6



Slide notes

To access the Zscaler App Portal from the ZPA Admin Portal, click the **Zscaler App** icon.

Slide 7 - Slide 7



Slide notes

To configure Forwarding Profiles, click on Administration, ...

Slide 8 - Slide 8

The screenshot shows the Zscaler App Store interface. On the left, a sidebar menu includes 'Settings', 'Zscaler App Store', 'Audit Logs', 'Forwarding Profile' (which is highlighted with a red box), 'Trusted Networks', 'Zscaler App Support', 'Zscaler Services', 'User Agents', 'Zscaler API', and 'Device Policies'. The main content area has tabs for 'PERSONAL COMPUTERS' and 'MOBILE DEVICES', with 'MOBILE DEVICES' selected. A modal window titled 'UPDATE SETTINGS' is open, showing options for 'Automatic Rollout': 'Always Latest Version', 'Specific Version', 'Group Based', and a 'Disable' button. Below the modal is a 'DEVICE SNAPSHOT' section with tables for 'Windows' and 'macOS'. The Windows table shows three rows: 2.1.2.71 (0 devices), 2.1.0.210 (0 devices), and 1.5.2.7 (1 device). The macOS table shows two rows: 2.1.0.190 (0 devices) and 1.5.2.6 (0 devices). At the bottom of the page are 'Help' and 'Versions' buttons, and the footer includes copyright information and a weblog time.

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1

Weblog Time: Wednesday, Apr 1, 2020 04:41:24 PM

Slide notes

...then click Forwarding Profile.

Slide 9 - Slide 9

The screenshot shows the Zscaler Administration interface. On the left, a sidebar lists various settings like Dashboard, Enrolled Devices, App Profiles, and Administration. Under 'Forwarding Profile', there's a list of profiles. The first profile is highlighted with a red box and labeled 'Default Forwarding Profile'. A callout box points to the 'Add Forwarding Profile' button with the text 'Click Add Forwarding Profile'.

Slide notes

You will find that there is a default **Forwarding Profile** (which cannot be edited), and the option to add a new one. The default profile configuration is as follows:

- **On and Off Trusted Network** - are both set to **Tunnel**;
- **VPN Trusted Network** - is set to the **None** option.

You can configure as many forwarding profiles as you need. For example, if you have multiple locations with different network information, you can configure different forwarding profiles so that the Zscaler App can recognize the known networks for different users and know how to respond upon detecting those networks.

To create a new profile, click **Add Forwarding Profile**.

Slide 10 - Slide 10

The screenshot shows the 'Add Forwarding Profile' dialog box over a dark-themed Zscaler dashboard. The dialog has a blue header bar with the title 'Add Forwarding Profile' and a close button. Below the header is a 'PROFILE DEFINITION' section with a 'Profile Name' field containing 'ZPA-ONLY'. A callout bubble highlights this field with the text 'Each Forwarding Profile must have a unique Profile Name'. The next section is 'TRUSTED NETWORK CRITERIA', which includes a 'Select' dropdown menu with 'Click Box' and an 'Add Condition' button. A callout bubble points to the 'Select' dropdown with the text 'Click Select to add a condition'. Below this is a 'WINDOWS DRIVER ACTION' section with 'Tunnel Driver Type' set to 'Route Based'. The main body of the dialog is 'FORWARDING PROFILE ACTION FOR ZPA', divided into three sections: 'On Trusted Network' (Tunnel selected), 'VPN Trusted Network' (None selected), and 'Off Trusted Network' (Tunnel selected). At the bottom are 'Save' and 'Cancel' buttons. The dashboard sidebar on the left lists various Zscaler services like Settings, App Store, and Audit Logs, with 'Forwarding Profile' currently selected. The footer of the dashboard shows copyright information and a timestamp.

Slide notes

Each **Forwarding Profile** must of course have a unique **Policy Name**, then you have the option to add **TRUSTED NETWORK CRITERIA**, to allow the App to recognize whether it is **On**, **Off**, or has a **VPN to a Trusted Network**.

To add a **TRUSTED NETWORK CRITERIA** condition, click in the **Add Condition** field, ...

Slide 11 - Slide 11

The screenshot shows the 'Add Forwarding Profile' dialog box. In the 'PROFILE DEFINITION' section, the 'Profile Name' is set to 'ZPA-ONLY'. Under 'TRUSTED NETWORK CRITERIA', there is a dropdown menu labeled 'Select' with options: 'DNS Server', 'DNS Search Domains', 'Hostname and IP', and 'Pre-defined Trusted Networks'. A red box highlights the 'Select' dropdown, and a callout bubble points to the 'Add Condition' button with the text 'Click Add Condition'. Below the dropdown, there are sections for 'VPN Trusted Network' and 'Off Trusted Network', each with a 'Same as "On Trusted Network"' checkbox and a 'Tunnel' radio button. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Select the Condition to add: **DNS Server, DNS Search Domains, Host Name and IP, Pre-defined Trusted Network**

Slide notes

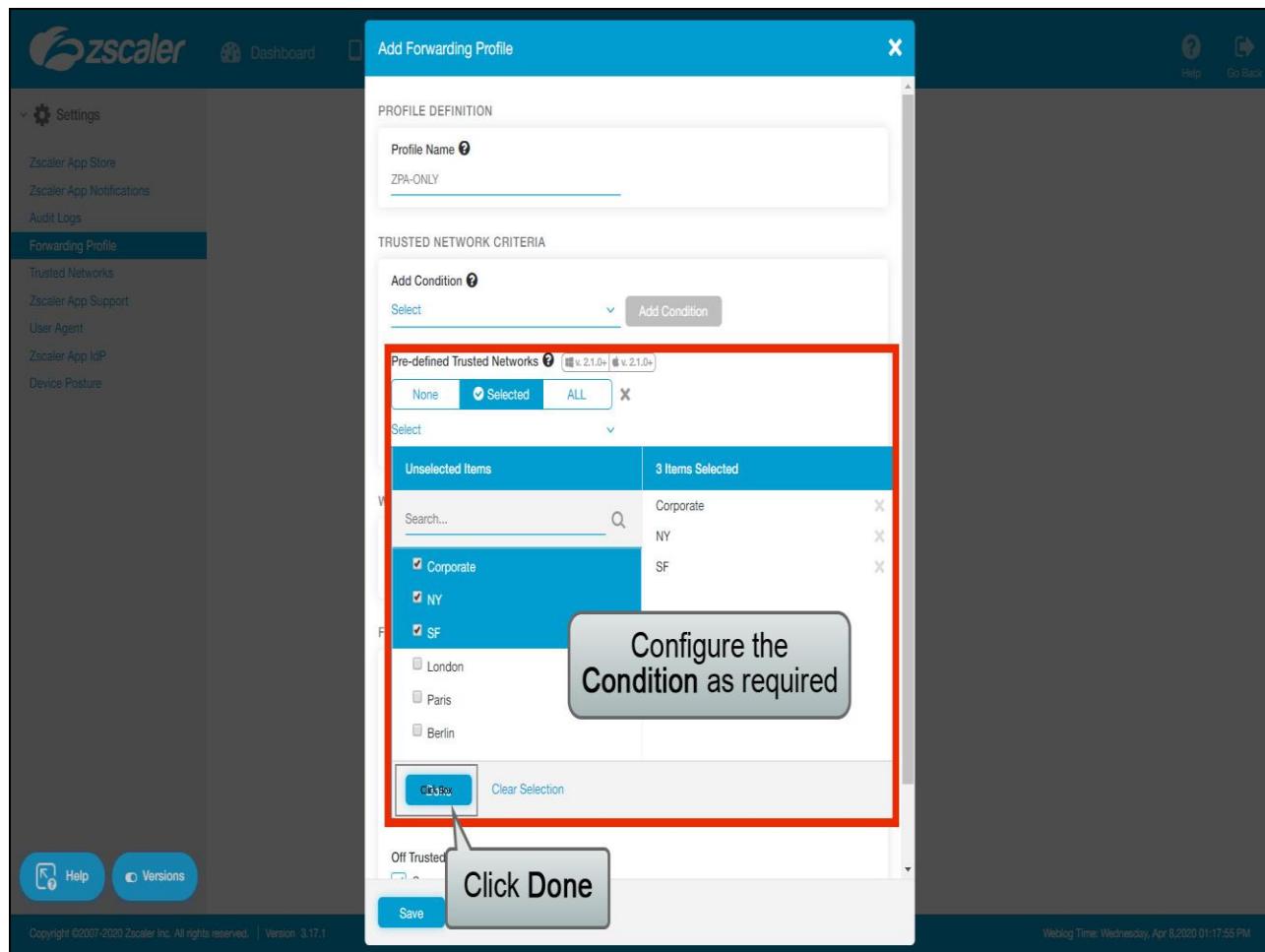
...and select the appropriate condition to be met. The conditions available are:

- **DNS Servers, DNS Search Domains, Host Name and IP** combinations;
- Or **Pre-defined Trusted Networks**.

You may add one instance of each of the first three conditions, OR you can add the **Pre-defined Trusted Network** condition. If you add a combination of the first three conditions, you can choose whether the App will verify any one condition (logical OR) or require that all conditions must be met (logical AND).

We already looked at how to configure the first three of these options in the **Common Configurations** module of this course, so for this example we will select the **Pre-defined Trusted Networks** option. Click the **Add Condition** button to add it to the profile, ...

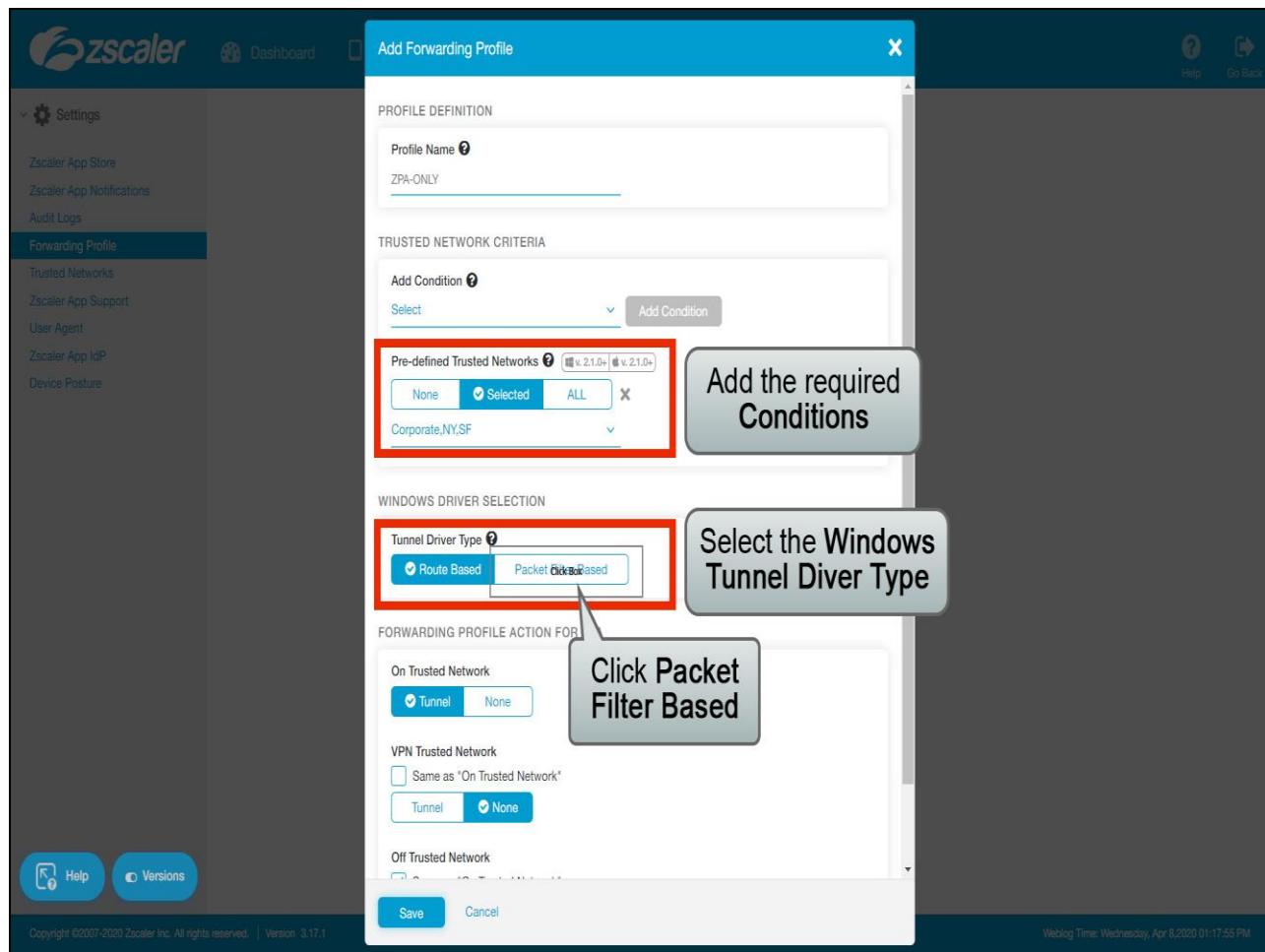
Slide 12 - Slide 12



Slide notes

...and the list of **Trusted Networks** that you defined earlier will be shown. Select the set of networks that you wish to use and click **Done**.

Slide 13 - Slide 13



Slide notes

Having configured the **TRUSTED NETWORK CRITERIA** as required, you then have the option to select the **Tunnel Driver Type** you wish to use for Windows devices. We generally recommend the **Packet Filter Based** driver as it gives better performance and enforcement.

By default this is set to the **Route Based** option, to use the recommended driver, click **Packet Filter Based**.

Slide 14 - Slide 14

The screenshot shows the 'Add Forwarding Profile' dialog box over a dark-themed Zscaler dashboard. The profile name is set to 'ZPA-ONLY'. Under 'Trusted Network Criteria', there is one condition selected: 'Selected' (v.2.1.0+). The 'Windows Driver Selection' section shows 'Route Based' is selected. In the 'Forwarding Profile Action for ZPA' section, 'Tunnel' is selected for both 'On Trusted Network' and 'VPN Trusted Network'. The 'Off Trusted Network' section is collapsed. At the bottom are 'Save' and 'Cancel' buttons.

Slide notes

Slide 15 - Forwarding Profile Options



Forwarding Profile Options

Identify the Network Using TRUSTED NETWORK CRITERIA

- On Trusted Network
- Off Trusted Network
- VPN Trusted Network

Configure ZIA Traffic Forwarding

- Tunnel
- None

Slide notes

The next part of the **Forwarding Profile** is all about traffic forwarding, with options for each of the three main scenarios (**On**, **Off**, or **VPN** to a trusted network). The ZPA forwarding options available are simply; **Tunnel** and **None**.

Note that the forwarding configurations available depend on the service that you are subscribed to:

- If you only use the ZIA service, you will only see ZIA forwarding configuration options;
- If you only subscribe to the ZPA service, then you will only see options for ZPA forwarding;
- If you subscribe to both services, then you will see both sets of forwarding configuration options.

Slide 16 - Slide 16

The screenshot shows the 'Add Forwarding Profile' dialog box over a dark background. The dialog has a blue header bar with the title 'Add Forwarding Profile'. Below it is a 'PROFILE DEFINITION' section with a 'Profile Name' field containing 'ZPA-ONLY'. In the 'TRUSTED NETWORK CRITERIA' section, there's a dropdown menu set to 'Select' with an 'Add Condition' button. Underneath is a 'Pre-defined Trusted Networks' dropdown showing 'v.2.1.0+' and 'v.2.1.0+', with 'Selected' checked. A 'Corporate,NY,SF' entry is listed below. The 'WINDOWS DRIVER SELECTION' section includes a 'Tunnel Driver Type' dropdown with 'Route Based' and 'Packet Filter Based' options, where 'Route Based' is selected. The 'FORWARDING PROFILE ACTION FOR ZPA' section is divided into three parts: 'On Trusted Network' (with 'Tunnel' selected), 'VPN Trusted Network' (with 'Same as "On Trusted Network"' checked and 'Tunnel' selected), and 'Off Trusted Network' (with 'None' selected). At the bottom are 'Save' and 'Cancel' buttons. A grey callout bubble with the text 'Scroll down...' points to the 'Forwarding Profile Action' section.

Slide notes

Scroll down if necessary, ...

Slide 17 - Slide 17

The screenshot shows the 'Add Forwarding Profile' dialog box over a dark-themed Zscaler dashboard. The dialog has a blue header bar with the title 'Add Forwarding Profile'. Below it, there's a section for 'ZPA-ONLY' and 'TRUSTED NETWORK CRITERIA'. Under 'TRUSTED NETWORK CRITERIA', there's a dropdown menu 'Add Condition' with 'Select' and 'Add Condition' buttons. A sub-section 'Pre-defined Trusted Networks' shows 'v. 2.1.0+' and 'v. 2.1.0-' with 'None', 'Selected', and 'ALL' buttons; 'Corporate,NY,SF' is listed under 'Selected'. The 'WINDOWS DRIVER SELECTION' section has a 'Tunnel Driver Type' dropdown with 'Route Based' and 'Packet Filter Based' options, where 'Route Based' is selected. The main configuration area is titled 'FORWARDING PROFILE ACTION FOR ZPA'. It contains three sections: 'On Trusted Network' (selected), 'VPN Trusted Network' (disabled), and 'Off Trusted Network' (disabled). Each section has a 'Tunnel' and 'None' button. A red box highlights the 'Tunnel' and 'None' buttons for the 'On Trusted Network' section. A callout bubble points to this highlighted area with the text: 'Configure FORWARDING PROFILE ACTION FOR ZPA as necessary'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Slide notes

If the App is to be used for Private Access only, configure the action to be taken when the App detects that it is **On Trusted Network**, or **Off Trusted Network** (based on the configured **TRUSTED NETWORK CRITERIA**), or that there is an active corporate **VPN Trusted Network**. The actions available for each scenario are; **Tunnel**, and **None**.

The **Tunnel** option enables ZPA connectivity using Z Tunnels and Microtunnels across the ZPA cloud to reach the available private applications. The **None** option disables ZPA functionality.

Slide 18 - Slide 18

The screenshot shows the 'Add Forwarding Profile' dialog box over a dark-themed Zscaler dashboard. The dialog has a blue header bar with the title 'Add Forwarding Profile'. Below it, a section titled 'ZPA-ONLY' is visible. The main area is titled 'TRUSTED NETWORK CRITERIA' and contains a 'Pre-defined Trusted Networks' dropdown set to 'Selected' with options 'v. 2.1.0+' and 'v. 2.1.0'. A dropdown below shows 'Corporate,NY,SF'. Under 'WINDOWS DRIVER SELECTION', the 'Tunnel Driver Type' is set to 'Route Based'. The 'FORWARDING PROFILE ACTION FOR ZPA' section is highlighted with a red box. It contains three sections: 'On Trusted Network' (set to 'None'), 'VPN Trusted Network' (checkbox checked, 'Same as "On Trusted Network"', set to 'None'), and 'Off Trusted Network' (checkbox checked, 'Same as "On Trusted Network"', set to 'Tunnel'). At the bottom right of the dialog is a 'Save' button. A callout bubble points to the 'Save' button with the text 'Click Save'. Another callout bubble points to the 'Tunnel' option under 'Off Trusted Network' with the text 'Configure FORWARDING PROFILE ACTION FOR ZPA as necessary'.

Slide notes

Once the **Forwarding Profile** configuration is complete, click **Save**.

Slide 19 - Slide 19

The screenshot shows the Zscaler dashboard with the 'Forwarding Profile' section selected in the sidebar. A success message 'All Changes have been saved successfully.' is displayed at the top. The main content area shows two forwarding profiles: 'ZPA-ONLY' and 'Default'. The 'ZPA-ONLY' profile uses 'PRE-DEFINED TRUSTED NETWORKS' criteria and has actions for 'ON TRUSTED NETWORK' (None) and 'VPN TRUSTED NETWORK' (None). The 'Default' profile uses 'CRITERIA' (None) and has actions for 'ON TRUSTED NETWORK' (Tunnel) and 'VPN TRUSTED NETWORK' (None). The bottom of the screen shows copyright information and a timestamp.

#	Profile Name	Trusted Network Criteria	Forwarding Profile Action
1	ZPA-ONLY	PRE-DEFINED TRUSTED NETWORKS Selected	ON TRUSTED NETWORK None VPN TRUSTED NETWORK None OFF TRUSTED NETWORK Tunnel
2	Default	CRITERIA None	ON TRUSTED NETWORK Tunnel VPN TRUSTED NETWORK None OFF TRUSTED NETWORK Tunnel

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 8, 2020 01:17:55 PM

Slide notes

Slide 20 - Slide 20

The screenshot shows the Zscaler web interface for managing Forwarding Profiles. The left sidebar is titled 'Settings' and includes links for Zscaler App Store, App Notifications, Audit Logs, Forwarding Profile (which is selected), Trusted Networks, Zscaler App Support, User Agent, Zscaler App IdP, and Device Posture. The main content area is titled 'Add Forwarding Profile' and displays two profiles: 'ZPA-ONLY' and 'Default'. The 'ZPA-ONLY' profile is set to 'PRE-DEFINED TRUSTED NETWORKS' with 'Selected' criteria, and its actions are 'ON TRUSTED NETWORK' (None) and 'VPN TRUSTED NETWORK' (None). The 'Default' profile is set to 'CRITERIA' with 'None' criteria, and its actions are 'ON TRUSTED NETWORK' (Tunnel) and 'VPN TRUSTED NETWORK' (None). The bottom of the screen shows copyright information (Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1) and a timestamp (Weblog Time: Wednesday, Apr 8, 2020 01:17:55 PM).

#	Profile Name	Trusted Network Criteria	Forwarding Profile Action
1	ZPA-ONLY	PRE-DEFINED TRUSTED NETWORKS Selected	ON TRUSTED NETWORK None VPN TRUSTED NETWORK None OFF TRUSTED NETWORK Tunnel
2	Default	CRITERIA None	ON TRUSTED NETWORK Tunnel VPN TRUSTED NETWORK None OFF TRUSTED NETWORK Tunnel

Slide notes

Slide 21 - Enabling SSL Inspection for Zscaler App Users



Zscaler Service Entitlement for ZPA

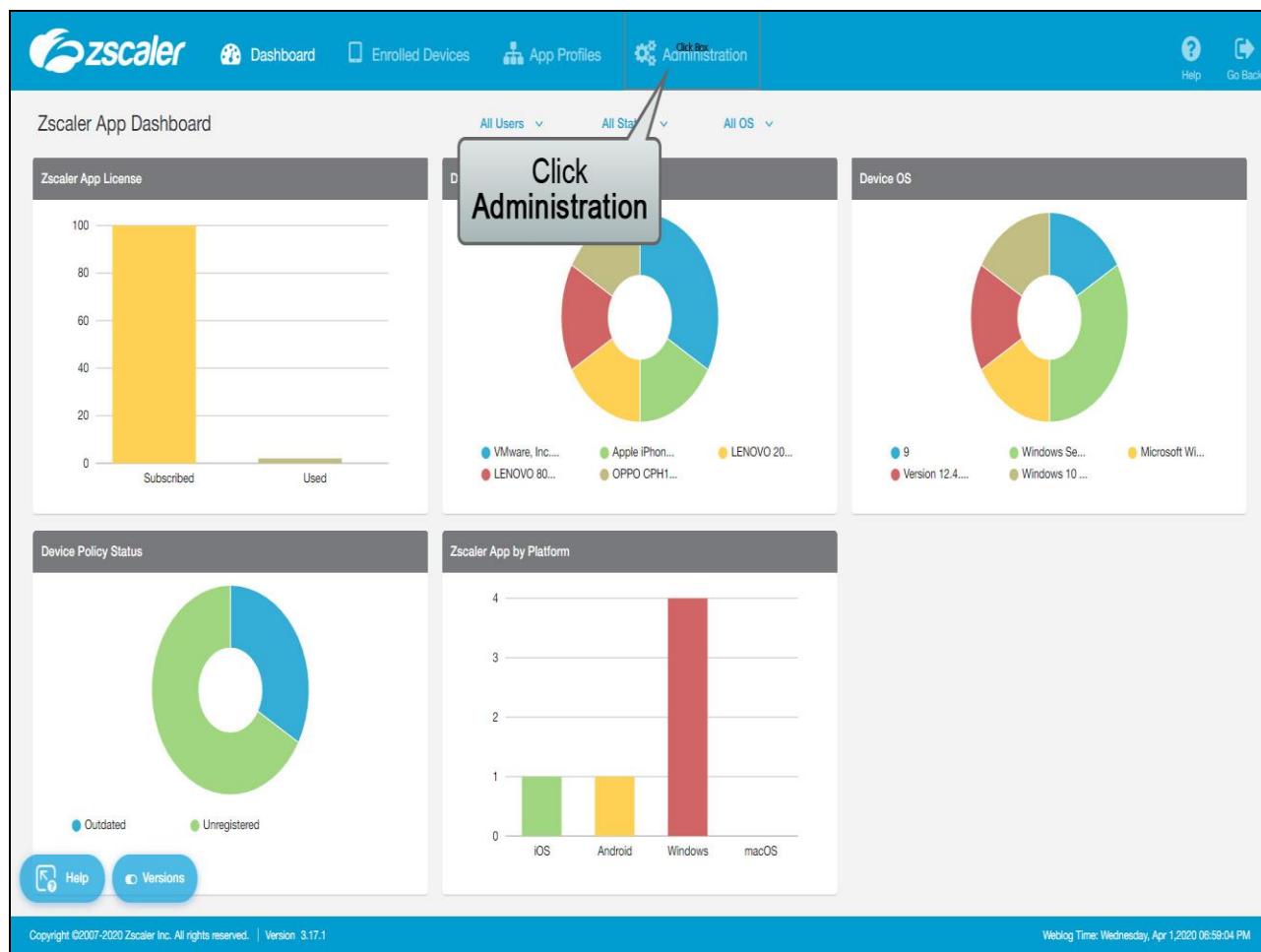
For ZPA Subscribers

- If you have subscriptions to BOTH ZIA and ZPA
- Identify which users are entitled to use ZPA features (by group)

Slide notes

If you subscribe to both the ZIA and ZPA services, but you only want to deploy ZPA to a subset of your users, you can use the **Zscaler Service Entitlement** configuration in the Zscaler App Portal. This feature allows you to select user groups from the ZIA Hosted DB, that are to have ZPA functionality enabled.

Slide 22 - Slide 22



Slide notes

In the Zscaler App Portal, click **Administration**.

Slide 23 - Slide 23

The screenshot shows the Zscaler App Store interface. On the left, a sidebar lists various settings and services, including 'Zscaler Service Entitlement'. A callout bubble points to this option with the text 'Click Zscaler Service Entitlement'. The main content area has tabs for 'PERSONAL COMPUTERS' and 'MOBILE DEVICES', with 'MOBILE DEVICES' selected. A sub-section titled 'UPDATE SETTINGS' contains an 'Automatic Rollout' section with options: 'Always Latest Version', 'Specific Version', 'Group Based', and a 'Disable' button. Below this are 'Save' and 'Cancel' buttons. The central part of the screen displays two tables: one for 'Windows' and one for 'macOS'. Both tables have columns for 'Application Version', 'Registered Devices', 'Release Notes', 'Download EXE', and 'Download MSI'. The Windows table shows versions 2.1.2.71, 2.1.0.210, and 1.5.2.7. The macOS table shows versions 2.1.2.38, 2.1.0.190, and 1.5.2.6. At the bottom of the page, there are 'Help' and 'Versions' buttons, and a footer note: 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1'.

Slide notes

The **Zscaler Service Entitlement** feature is relevant only if your organization is using the Zscaler App for BOTH Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), and you will only be able to see this menu option or access this page if you have subscriptions to both services.

To configure which of your users have access to the Private Access features of the Zscaler App, click **Zscaler Service Entitlement**.

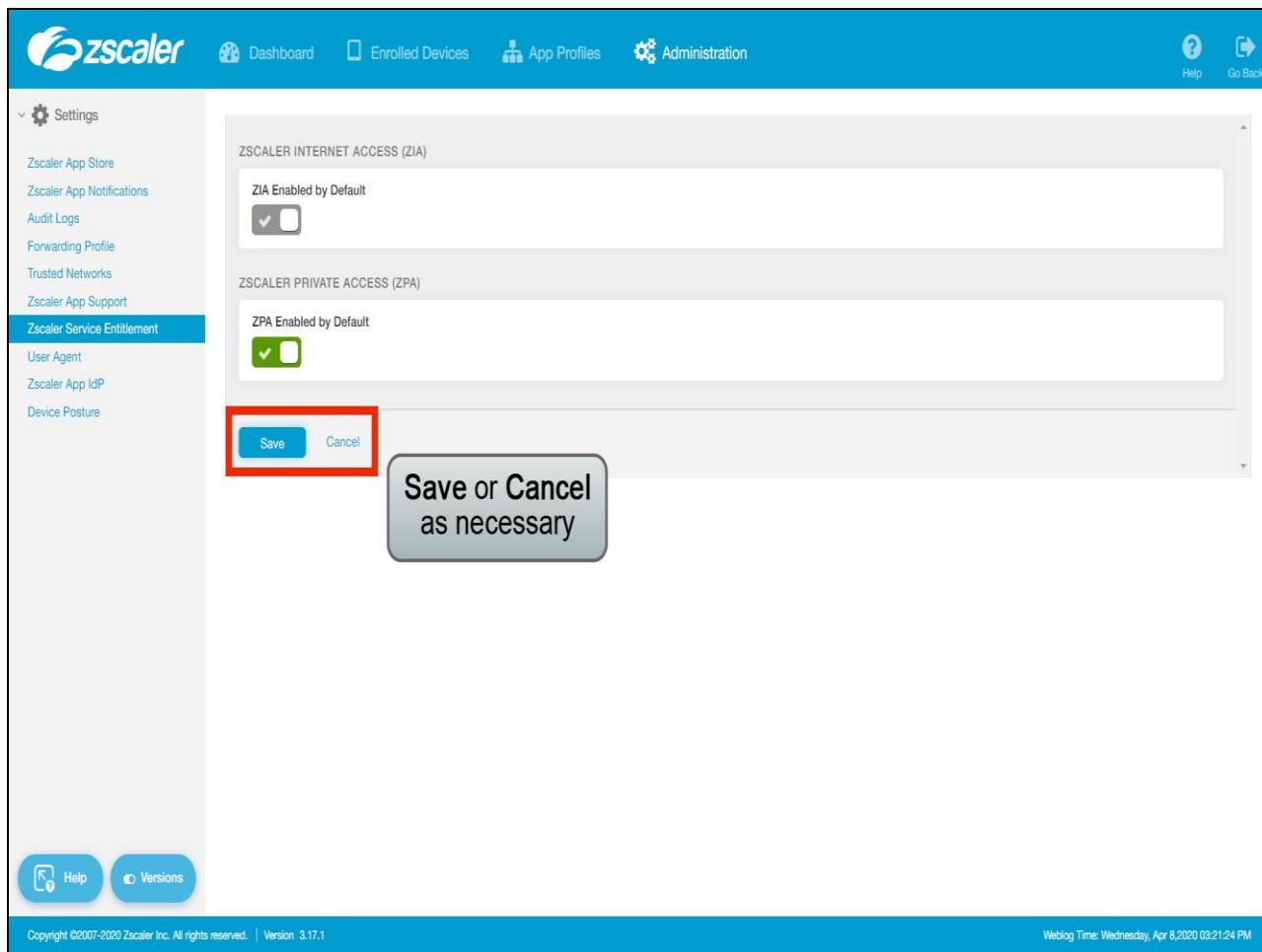
Slide 24 - Slide 24

The screenshot shows the Zscaler Administration interface. On the left, there's a sidebar with 'Settings' expanded, showing options like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, and Zscaler Service Entitlement. Under 'Zscaler Service Entitlement', 'User Agent' is selected. The main content area has two sections: 'ZSCALER INTERNET ACCESS (ZIA)' where 'ZIA Enabled by Default' is checked, and 'ZSCALER PRIVATE ACCESS (ZPA)' where 'ZPA Enabled by Default' is currently unchecked (disabled). A callout bubble points to this checkbox with the text 'Click to enable the ZPA Enabled by Default option'. At the bottom of the page, there are 'Help' and 'Versions' buttons, and a footer with copyright information and a timestamp.

Slide notes

ZPA access is disabled by default, to make ZPA functionality available to ALL of your users, click the **ZPA Enabled by Default** option.

Slide 25 - Slide 25



The screenshot shows the Zscaler Administration interface. On the left, there's a sidebar with a gear icon labeled 'Settings' and a list of options: Zscaler App Store, Zscaler App Notifications, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, and **Zscaler Service Entitlement**. Under 'Zscaler Service Entitlement', there are four items: User Agent, Zscaler App IdP, Device Posture, and another 'Settings' item which is expanded to show 'ZIA Enabled by Default' (with a checked checkbox) and 'ZPA Enabled by Default' (with a checked checkbox). At the bottom of this expanded section are two buttons: 'Save' and 'Cancel'. A red box highlights the 'Save' button. A callout bubble points to this red box with the text 'Save or Cancel as necessary'. At the very bottom of the interface, there are 'Help' and 'Versions' buttons, and a footer bar with copyright information: 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1' and 'Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM'.

Slide notes

You would then need to **Save** that configuration.

Slide 26 - Slide 26

The screenshot shows the Zscaler Admin interface. On the left, a sidebar lists various settings like Zscaler App Store, Audit Logs, and Zscaler Service Entitlement. The main panel is titled 'ZSCALER INTERNET ACCESS (ZIA)' and contains a checkbox for 'ZIA Enabled by Default' which is checked. Below it is another section titled 'ZSCALER PRIVATE ACCESS (ZPA)' with a checkbox for 'ZPA Enabled by Default' which is unchecked. A callout box points to a dropdown menu labeled 'Groups Enabled' which has two options: 'NONE' and 'Click Box'. At the bottom of the main panel are 'Save' and 'Cancel' buttons.

Slide notes

Otherwise, to select the specific user groups that are to have ZPA functionality, click in the **Groups Enabled** field, ...

Slide 27 - Slide 27

The screenshot shows the Zscaler Administration interface under the 'Zscaler Service Entitlement' section. In the 'ZSCALER PRIVATE ACCESS (ZPA)' section, there is a 'Groups Enabled' dropdown set to 'NONE'. Below it is a list of groups categorized into 'Unselected Items' and '6 Items Selected'. The 'Unselected Items' list includes Maintenance, Americas, EMEA, APAC, and ANZ. The '6 Items Selected' list includes Marketing, Sales, EMEA, APAC, Americas, and ANZ. A callout bubble with the text 'Click Done' points to the 'Done Row' button at the bottom left of the selection pane. The bottom of the screen shows standard navigation buttons for Help, Versions, and a copyright notice.

ZSCALER INTERNET ACCESS (ZIA)

ZIA Enabled by Default

ZSCALER PRIVATE ACCESS (ZPA)

ZPA Enabled by Default

Groups Enabled: NONE

Unselected Items	6 Items Selected
Search... <input type="text"/>	Marketing
Maintenance	Sales
<input checked="" type="checkbox"/> Americas	EMEA
<input checked="" type="checkbox"/> EMEA	APAC
<input checked="" type="checkbox"/> APAC	Americas
<input checked="" type="checkbox"/> ANZ	ANZ

Click Done

Done Row

Clear Selection

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1

Help

Versions

Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

...select the appropriate groups and click **Done**, ...

Slide 28 - Slide 28

The screenshot shows the Zscaler Settings interface. On the left, there's a sidebar with various options like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, and Zscaler Service Entitlement. Under Zscaler Service Entitlement, 'User Agent', 'Zscaler App IdP', and 'Device Posture' are listed. The main content area has two sections: 'ZSCALER INTERNET ACCESS (ZIA)' and 'ZSCALER PRIVATE ACCESS (ZPA)'. In the ZIA section, 'ZIA Enabled by Default' is checked. In the ZPA section, 'ZPA Enabled by Default' is unchecked. Below these sections, there's a 'Groups Enabled' dropdown with 'Marketing' selected. At the bottom of the main content area are 'Save' and 'Cancel' buttons. A callout bubble with the text 'Click Save' points to the 'Save' button.

Slide notes

...then click **Save**.

Slide 29 - Slide 29

The screenshot shows the Zscaler Settings interface. The left sidebar includes options like Settings, Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, and Zscaler Service Entitlement (which is selected). The main content area displays two sections: ZSCALER INTERNET ACCESS (ZIA) and ZSCALER PRIVATE ACCESS (ZPA). Under ZIA, 'ZIA Enabled by Default' is checked. Under ZPA, 'ZPA Enabled by Default' is unchecked. A dropdown menu labeled 'Groups Enabled' lists 'ANZ, APAC, Americas, EMEA, Marketing, S...'. At the bottom are 'Save' and 'Cancel' buttons. A message bar at the top right says 'All Changes have been saved successfully.' The footer contains copyright information and a timestamp.

All Changes have been saved successfully.

ZIA Enabled by Default

ZPA Enabled by Default

Groups Enabled

ANZ, APAC, Americas, EMEA, Marketing, S...

Save Cancel

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1

Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

Slide 30 - Slide 30

The screenshot shows the Zscaler Admin Portal interface. The top navigation bar includes links for Dashboard, Enrolled Devices, App Profiles, Administration, Help, and Go Back. On the left, a sidebar titled 'Settings' lists various options: Zscaler App Store, Zscaler App Notifications, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, and Zscaler Service Entitlement (which is currently selected). Under 'Zscaler Service Entitlement', there are links for User Agent, Zscaler App IdP, and Device Posture. At the bottom of the sidebar are 'Help' and 'Versions' buttons. The main content area displays two configuration sections: 'ZSCALER INTERNET ACCESS (ZIA)' and 'ZSCALER PRIVATE ACCESS (ZPA)'. In the ZIA section, 'ZIA Enabled by Default' is checked. In the ZPA section, 'ZPA Enabled by Default' is unchecked. Below these sections is a 'Groups Enabled' dropdown menu containing 'ANZ, APAC, Americas, EMEA, Marketing, S...'. At the bottom of the configuration panel are 'Save' and 'Cancel' buttons.

Slide notes

Note that these groups must be populated through configuration in the ZIA Admin Portal, see the inline help for detailed instructions.

Slide 31 - Device Posture Options for ZPA



Device Posture Options for ZPA

Platform Dependent Posture Criteria

- For PCs
 - Certificate Trust
 - Client Certificate
 - Domain-joined
 - End Point Agent:
 - Carbon Black
 - CrowdStrike
 - SentinelOne
 - File Path
 - Firewall
 - Process Check
 - Registry Key (Windows)
 - Full Disk Encryption
- For Android
 - Certificate Trust
 - Client Certificate
 - Full Disk Encryption
 - Unauthorized Modification
- For iOS
 - Certificate Trust
 - Unauthorized Modification

Slide notes

For ZPA users, posture criteria are available to ensure that ZPA access is only given to devices that are compliant with the specified posture conditions. The posture criteria available depend on the platform type:

- For the PC platforms (**Windows** and **MacOS**) the profiles you can add are; **Certificate Trust**, **File Path**, **Registry Key** (Windows only of course); **Client Certificate**, **Firewall**, **Full Disk Encryption**, **Domain-joined**, **Process Check**, plus the option to check for an active end point agent (the agents available being **Carbon Black**, **CrowdStrike** or **SentinelOne**).
- For **Android** you can add the **Certificate Trust**, **Client Certificate**, **Full Disk Encryption** and **Unauthorized Modification** conditions.
- For **iOS** only the **Certificate Trust** and **Unauthorized Modification** conditions are available.

Slide 32 - Slide 32

The screenshot shows the Zscaler Admin interface. The top navigation bar includes links for Dashboard, Enrolled Devices, App Profiles, Administration, Help, and Go Back. On the left, a sidebar menu lists Settings, Zscaler App Store, Zscaler App Notifications, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, and Zscaler Service Entitlement. Under Zscaler Service Entitlement, 'User Agent' and 'Zscaler App IdP' are listed, with 'Device Posture' highlighted and a callout box pointing to it. The main content area displays two sections: 'ZSCALER INTERNET ACCESS (ZIA)' with a 'ZIA Enabled by Default' toggle switch set to 'On' (indicated by a checkmark), and 'ZSCALER PRIVATE ACCESS (ZPA)' with a 'ZPA Enabled by Default' toggle switch set to 'Off' (indicated by a red 'X'). Below these sections, a 'Groups Enabled' dropdown menu lists 'ANZ, APAC, Americas, EMEA, Marketing, S...'. At the bottom of the content area are 'Save' and 'Cancel' buttons. The footer contains copyright information ('Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1') and a timestamp ('Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM').

Slide notes

The posture profiles feature is relevant only if your organization is using the Zscaler App for Zscaler Private Access (ZPA), and you will only be able to see this menu option or access this page if you have a subscription to ZPA.

To create and manage posture profiles, click **Device Posture**.

Slide 33 - Slide 33

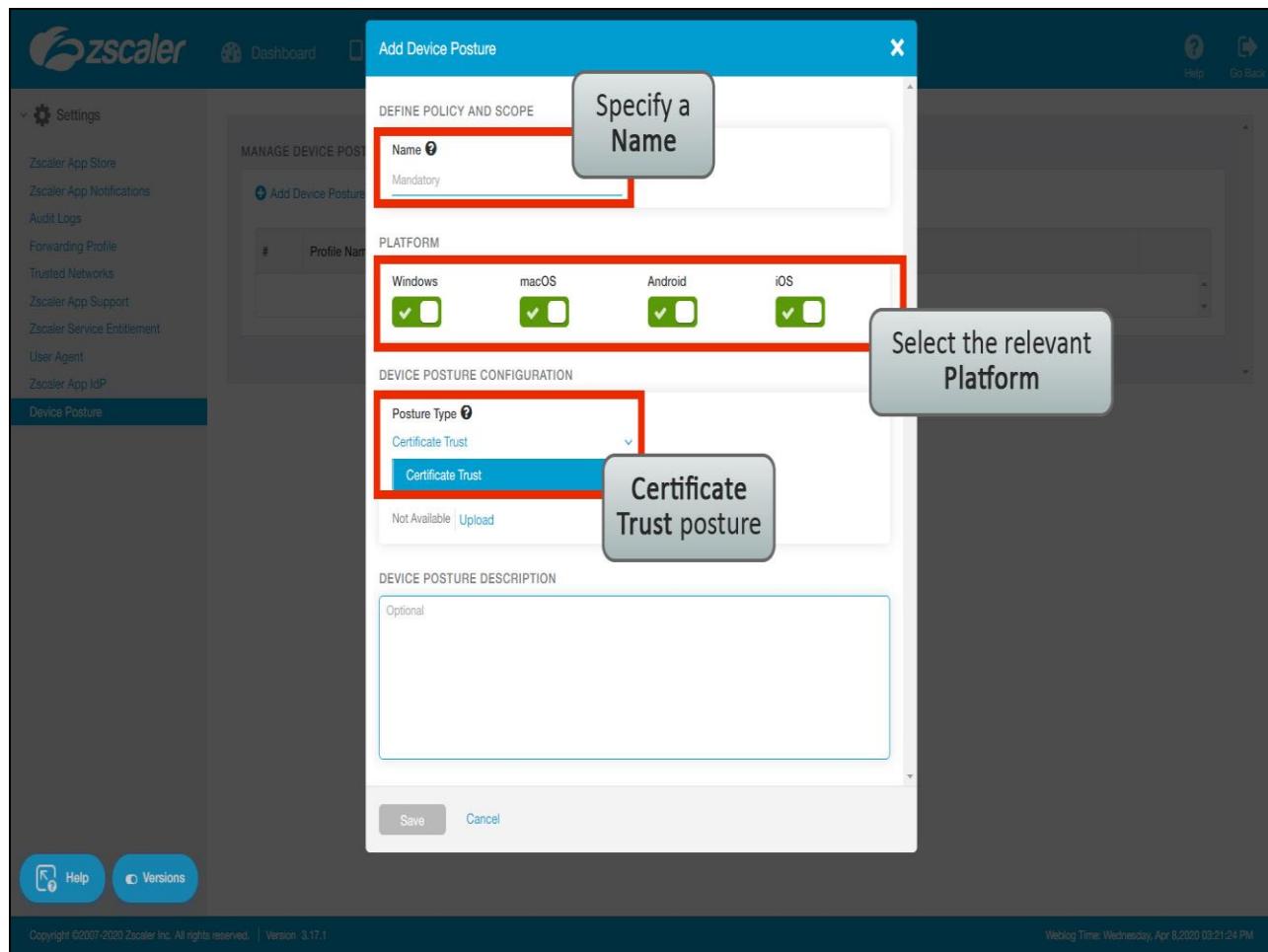
The screenshot shows the Zscaler App Portal interface. The top navigation bar includes links for Dashboard, Enrolled Devices, App Profiles, Administration, Help, and Go Back. On the left, a sidebar menu under 'Settings' lists various options like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IdP, and Device Posture (which is selected). The main content area is titled 'MANAGE DEVICE POSTURES' and contains a table with columns for '#', 'Profile Name', and 'Description'. A callout box with the text 'Click Add Device Posture Profile' points to the 'Add Device Posture Profile' button in the top-left corner of the table area. At the bottom, there are 'Help' and 'Versions' buttons, and a footer note about copyright and version information.

Slide notes

A **Device Posture** profile is a set of criteria that a user's device must meet in order to access applications with ZPA. You must create the posture profiles here in the Zscaler App Portal, then they are available for you to select when configuring **Access Policies** in the ZPA Admin Portal.

To add a new posture profile, click **Add Device Posture Profile**.

Slide 34 - Slide 34



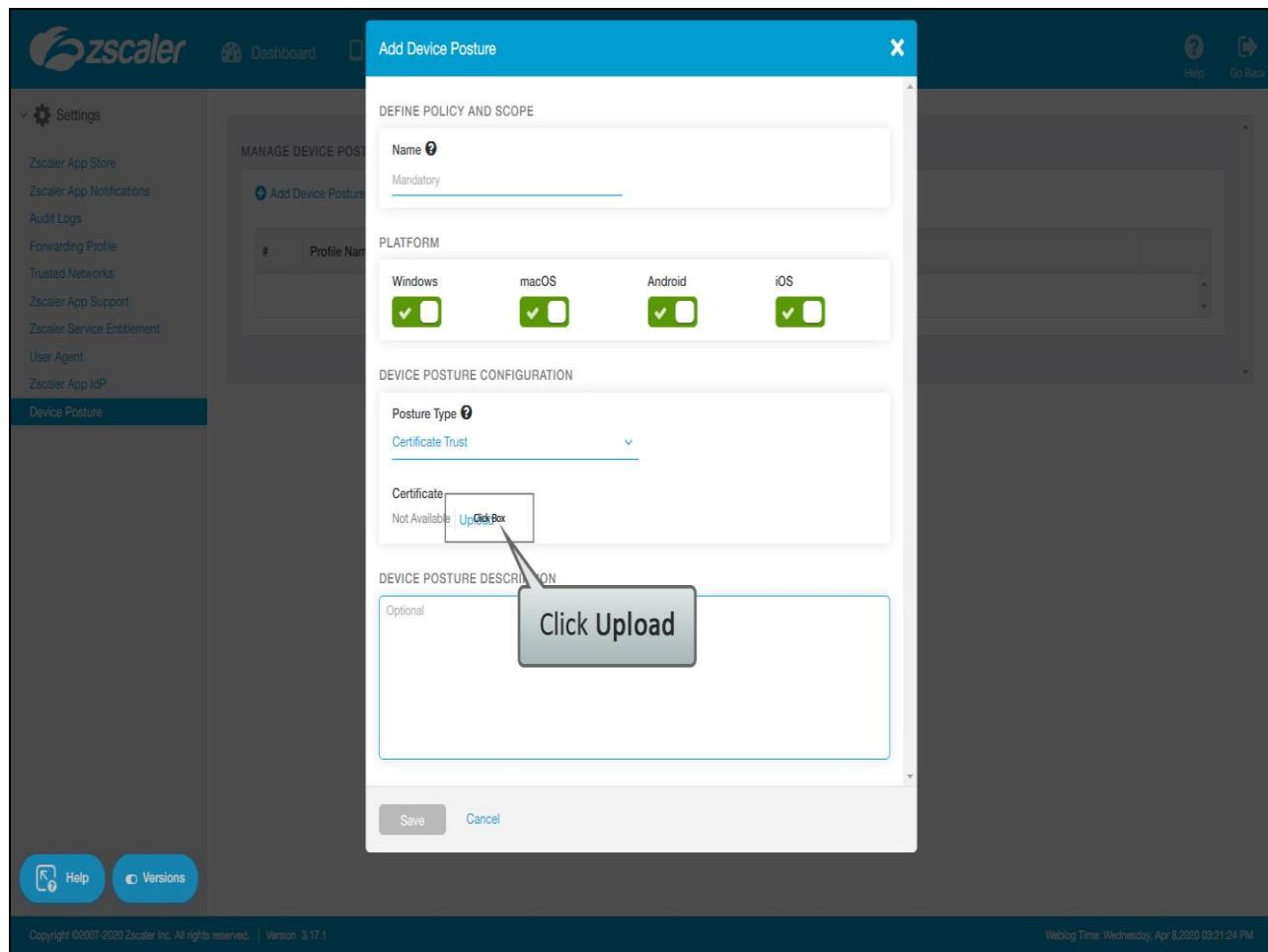
Slide notes

A posture profile must of course have a **Name**, then you must select what **PLATFORMS** it is to be applied to; **Windows**, **macOS**, **Android**, or **iOS**. Depending on which **PLATFORMS** you select in the profile configuration, this will control which conditions you can add and configure, you will only see the options that are common to all the selected platforms. Note that you can only add the one **Posture Type** per profile.

The only condition that is applicable across all platforms is the **Certificate Trust** condition, which allows you to upload a certificate issued by an internal root CA trusted by your organization's users (a root CA certificate, an intermediate certificate or a client certificate). The certificate must be in Base-64 encoded **.PEM** or **.CER** format.

Note that, with this condition, Zscaler App only checks the default certificate store on the user's system. After you have identified the default certificate store, you must ensure the issuer of the posture certificate is both present in it, and trusted. The posture certificate should be issued by an internal CA, not a public CA which would be trusted by most devices anyway.

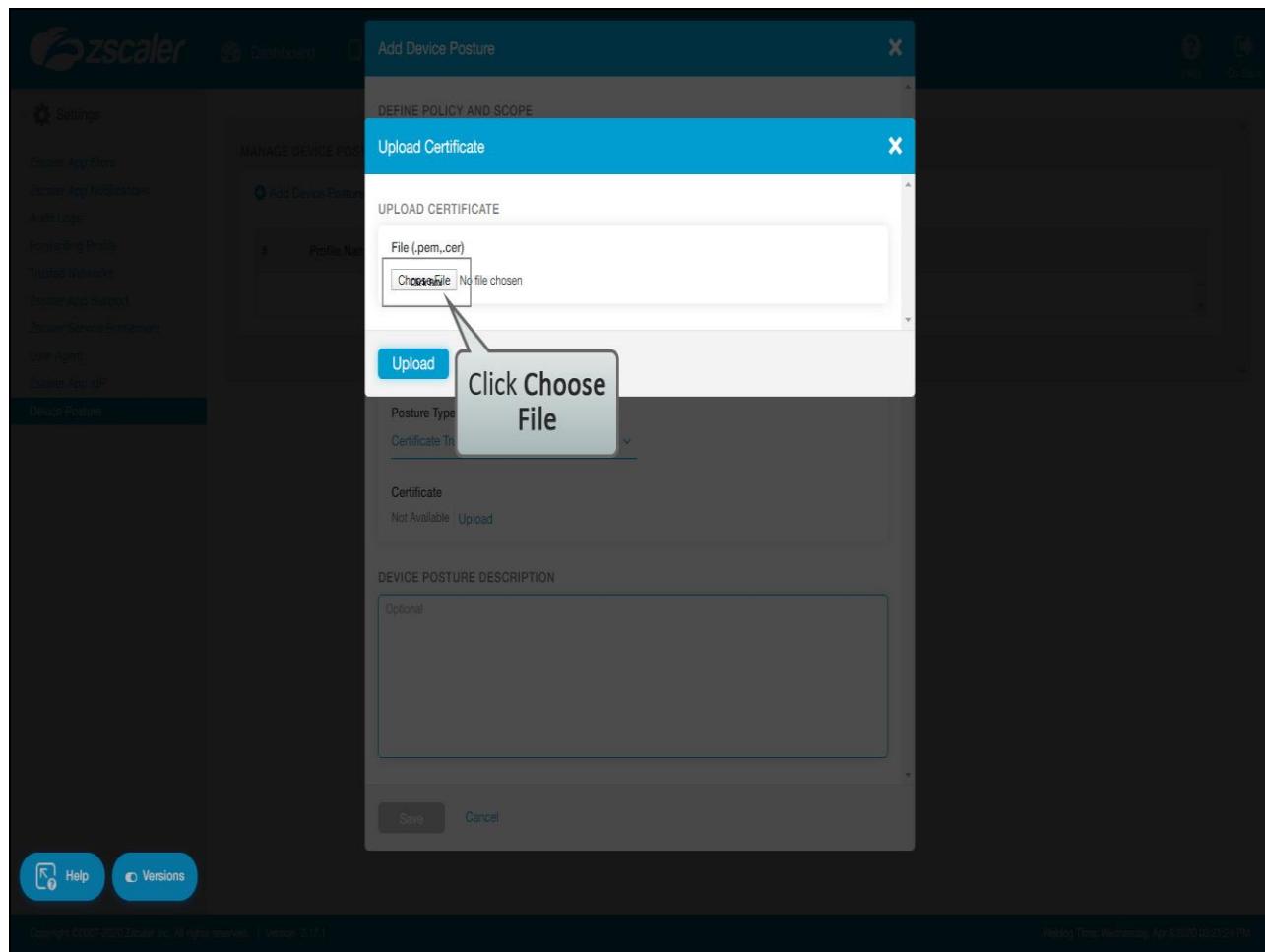
Slide 35 - Slide 35



Slide notes

While we're here, let's create a profile to deploy a **Certificate Trust** condition to all platforms. Click to **Upload** a certificate, ...

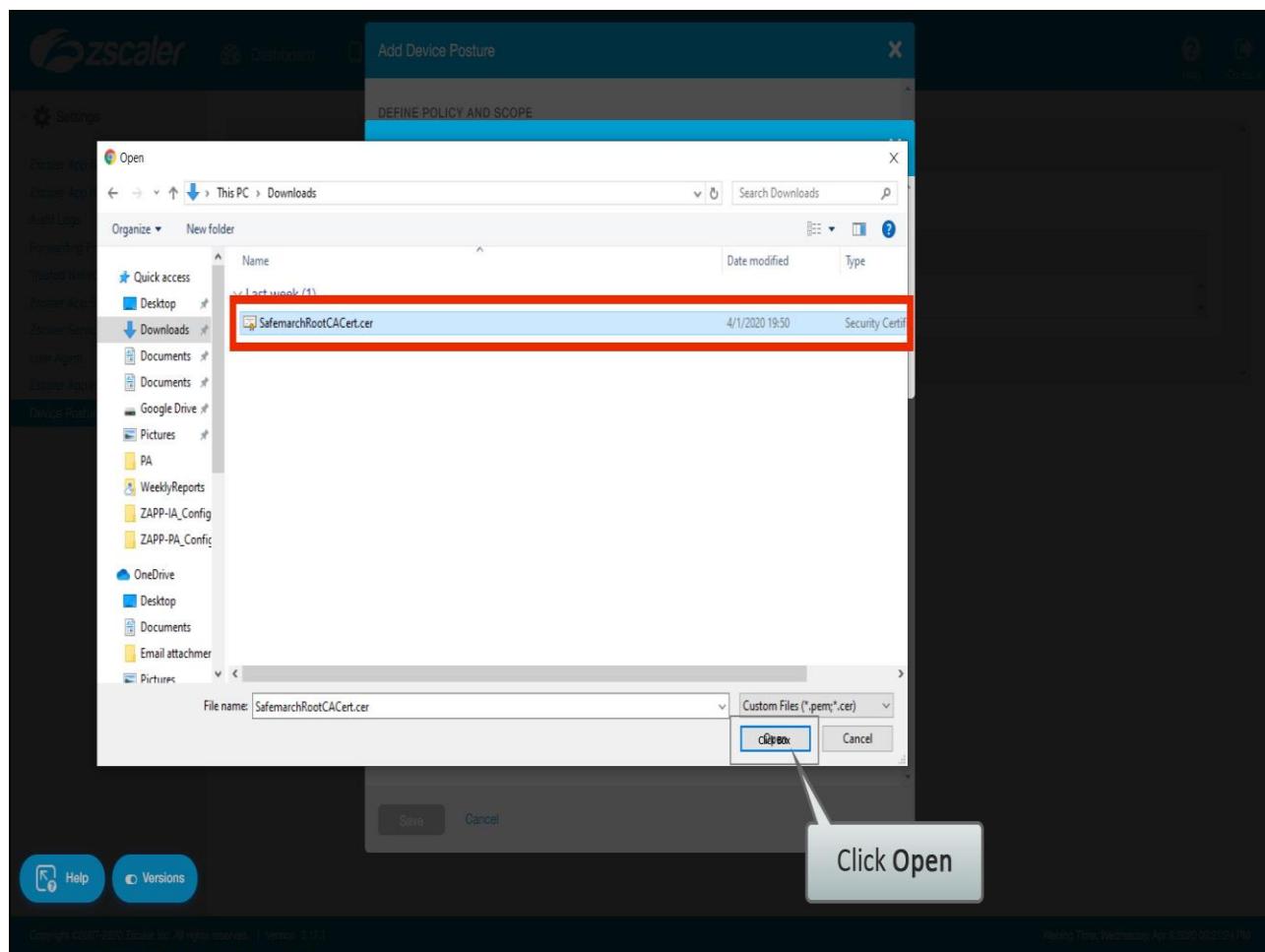
Slide 36 - Slide 36



Slide notes

...then click Choose File, ...

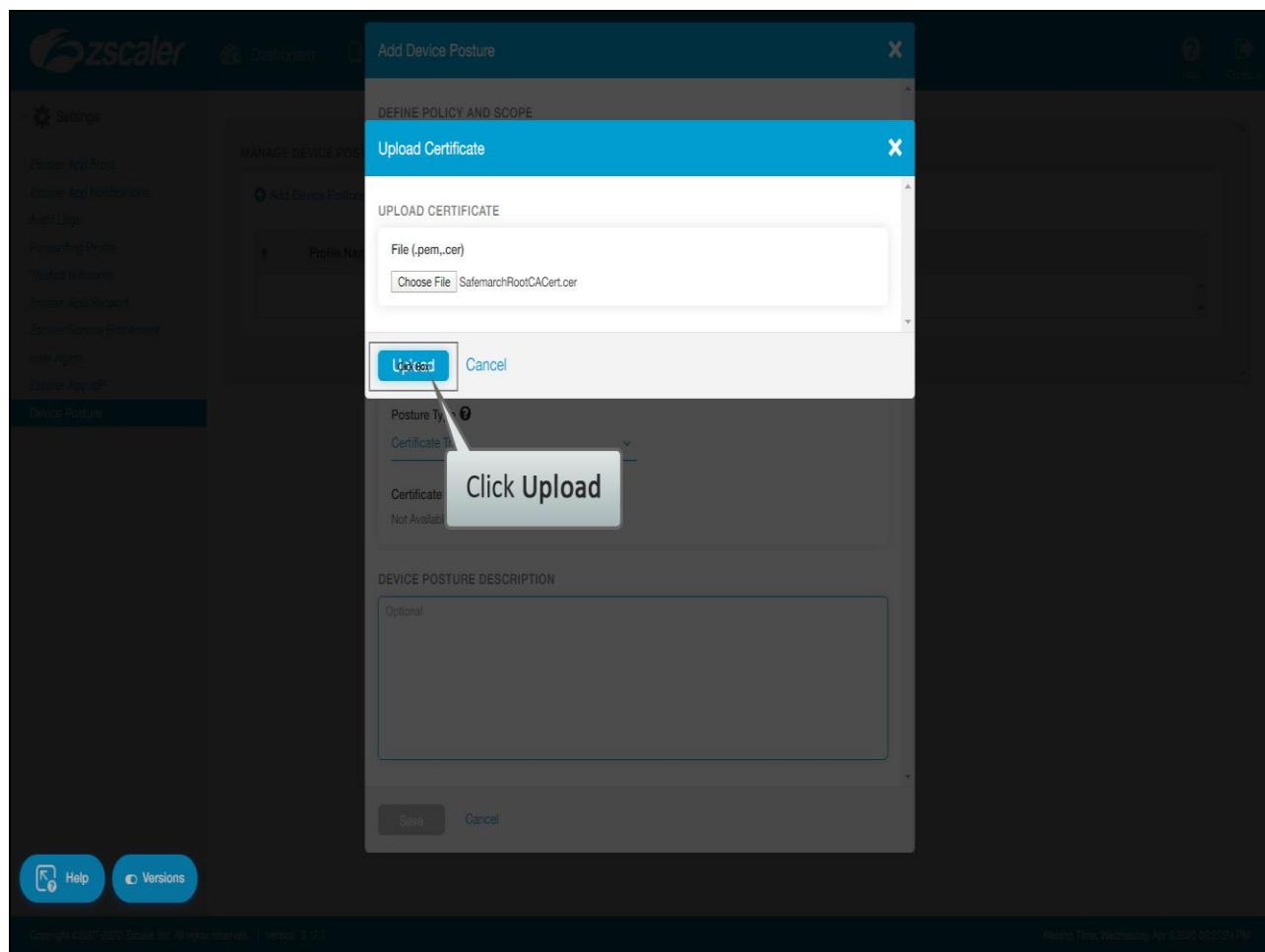
Slide 37 - Slide 37



Slide notes

...find the correct certificate file, select it and click Open, ...

Slide 38 - Slide 38



Slide notes

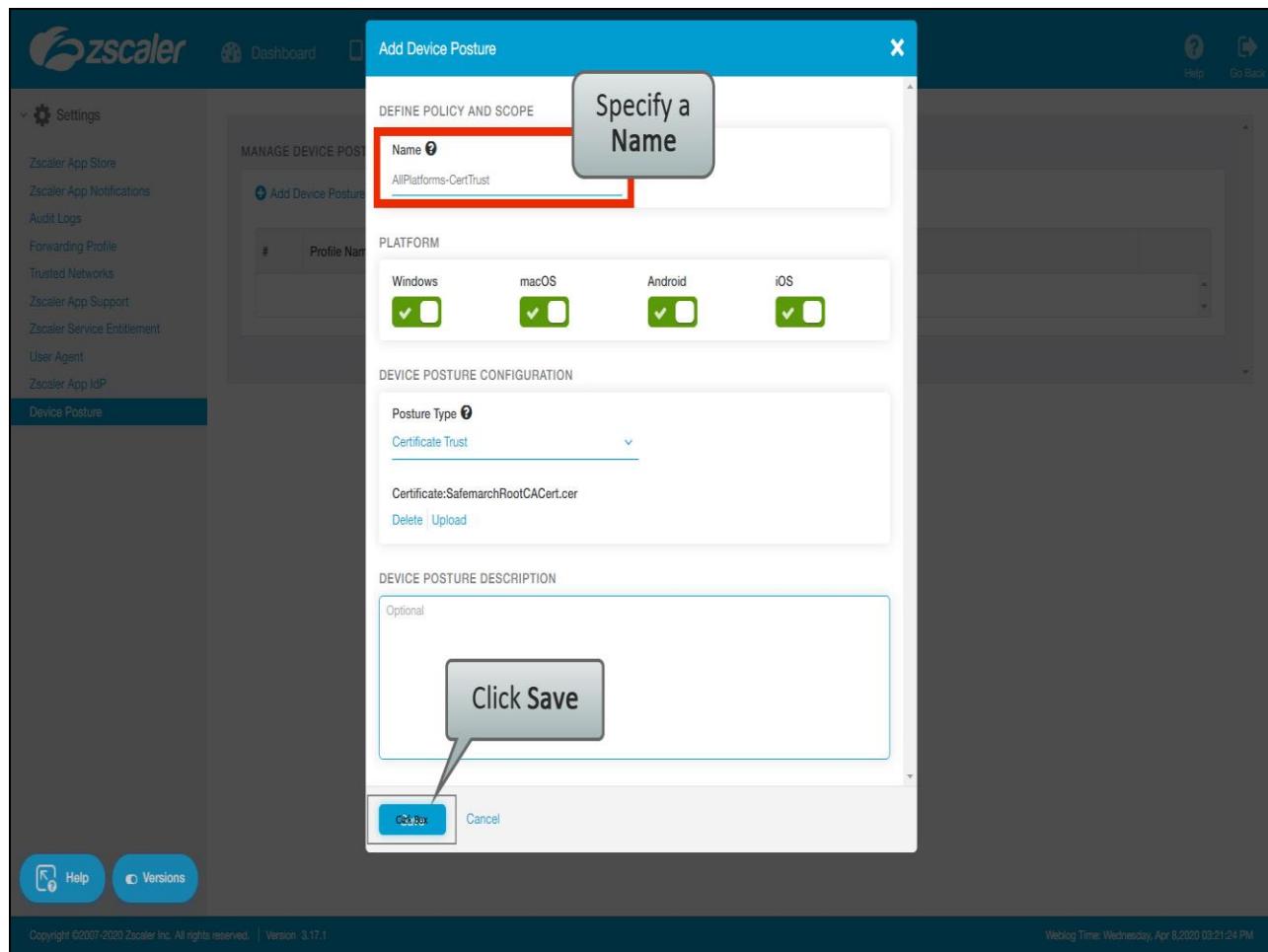
...then click Upload.

Slide 39 - Slide 39

The screenshot shows the Zscaler Device Posture configuration interface. A modal window is open, indicating that the device certificate 'SafemarchRootCACert.cer' has been uploaded successfully. The main configuration window is titled 'DEFINE POLICY AND SCOPE' and includes sections for 'Name' (set to 'Mandatory'), 'PLATFORM' (Windows, macOS, Android selected, iOS not selected), 'DEVICE POSTURE CONFIGURATION' (Posture Type set to 'Certificate Trust', with a certificate file 'SafemarchRootCACert.cer' listed), and 'DEVICE POSTURE DESCRIPTION' (Optional). At the bottom are 'Save' and 'Cancel' buttons.

Slide notes

Slide 40 - Slide 40



Slide notes

Once the condition is correctly configured, click **Save**.

Slide 41 - Slide 41

The screenshot shows the Zscaler Settings interface. The left sidebar has a 'Settings' section with various options like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IdP, and Device Posture (which is selected). The main content area is titled 'MANAGE DEVICE POSTURES' and contains a table with one row. The table has columns for '#', 'Profile Name', and 'Description'. The single row shows '# 1' and 'Profile Name: AllPlatforms-CertTrust'. There are edit and delete icons next to the profile name. A message at the top says 'All Changes have been saved successfully.' and there are 'Help' and 'Go Back' buttons in the top right.

#	Profile Name	Description
1	AllPlatforms-CertTrust	

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

Slide 42 - Slide 42

The screenshot shows the Zscaler Device Posture management interface. The left sidebar has a 'Device Posture' section selected. The main area is titled 'MANAGE DEVICE POSTURES' and contains a table with one row. The table columns are '#', 'Profile Name', and 'Description'. The single entry is '1 AllPlatforms-Cent...'. A callout box with the text 'Click Add Device Posture Profile' points to the 'Add Device Posture Profile' button in the top-left corner of the table area.

#	Profile Name	Description
1	AllPlatforms-Cent...	

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

In general, it is recommended that you create and configure platform specific posture profiles, although (as we have just seen) if you wish to test for presence of a **Certificate Trust**, that can be configured for all platforms in a single profile. In fact, that is the ONLY condition that is configurable across all platform types.

Let's go through the conditions available on a per-platform basis, click **Add Device Posture Profile**.

Slide 43 - Slide 43

Conditions available for Windows

Slide notes

For the **Windows** platform, you may configure:

- **Certificate Trust** - which we have just seen;
- **File Path** - the full path to a file that must exist on the system;
- **Registry Key** - the **Path** or **Value** of a key that must exist on the system;
- **Client Certificate** - which checks for a public/private key pair for a certificate issued by an internal root CA trusted by your organization's users;
- **Firewall** - which check for an active firewall on the public, private, and domain firewall profiles;

Slide 44 - Slide 44

The screenshot shows the 'Add Device Posture' dialog box over a dark-themed Zscaler dashboard. The dialog has two main sections: 'DEFINE POLICY AND SCOPE' and 'DEVICE POSTURE CONFIGURATION'. In the 'SCOPE' section, 'Name' is set to 'Mandatory' and 'Platform' is set to 'Windows' (indicated by a green checkmark). The 'DEVICE POSTURE CONFIGURATION' section contains a dropdown menu titled 'Posture Type' which lists several conditions: 'Certificate Trust', 'Firewall', 'Full Disk Encryption', 'Domain Joined', 'Process Check (v.2.1.2+, v.2.1.2+)', and 'Detect Carbon Black (v.2.1.2+, v.2.1.2+)'. A red box highlights the 'Process Check' option. A callout bubble points to this box with the text 'Conditions available for Windows'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Slide notes

- **Full Disk Encryption** - which checks that disk encryption is enabled;
- **Domain-joined** - which checks that the device is joined to the specified domain;
- **Process Check** - which checks for the specified process (full path) and signer certificate thumbprint;

Slide 45 - Slide 45

The screenshot shows the 'Add Device Posture' dialog box over a dark background dashboard. The dialog has a blue header 'Add Device Posture'. Under 'DEFINE POLICY AND SCOPE', the 'Name' is set to 'Mandatory'. In the 'PLATFORM' section, 'Windows' is selected with a green checkmark, while 'macOS', 'Android', and 'iOS' are unselected with red X's. The 'DEVICE POSTURE CONFIGURATION' section contains a 'Posture Type' dropdown menu with the following options:

- Certificate Trust
- Process Check (v.2.12+)
- Detect Carbon Black (v.2.12+)
- Detect CrowdStrike (v.2.12+)
- Detect SentinelOne (v.2.12+)

A red box highlights the 'Process Check' option. A gray callout box labeled 'Conditions available for Windows' points to the 'Process Check' option. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Slide notes

- plus there are options to check for an active end point agent (**Carbon Black**, **CrowdStrike** or **SentinelOne**).

Slide 46 - Slide 46

The screenshot shows the Zscaler Device Posture configuration interface. A modal window titled "Add Device Posture" is open, overlaid on a dark background. The modal has three main sections: "DEFINE POLICY AND SCOPE", "PLATFROM", and "DEVICE POSTURE CONFIGURATION".

- DEFINE POLICY AND SCOPE:** Contains a "Name" field with "Mandatory" typed in.
- PLATFORM:** Shows checkboxes for Windows (unchecked), macOS (checked), Android (unchecked), and iOS (unchecked).
- DEVICE POSTURE CONFIGURATION:** Contains a "Posture Type" dropdown menu. The "Certificate Trust" option is selected and highlighted with a red border. A callout bubble to the right of this menu says "Conditions available for MacOS". Below the dropdown are other options: "File Path", "Client Certificate", "Firewall", and "Full Disk Encryption".

At the bottom of the modal are "Save" and "Cancel" buttons. The background of the main interface shows a "MANAGE DEVICE POSTURE" section with a table and some status indicators.

Slide notes

For **macOS**, you have the same options as for Windows, although without the **Registry Key** one of course.

Slide 47 - Slide 47

The screenshot shows the Zscaler Device Posture configuration interface. A modal window titled 'Add Device Posture' is open. In the 'DEFINE POLICY AND SCOPE' section, the 'Name' is set to 'Mandatory'. Under 'PLATFORM', 'Windows' and 'macOS' are disabled (red), while 'Android' is enabled (green). In the 'DEVICE POSTURE CONFIGURATION' section, the 'Posture Type' dropdown is set to 'Certificate Trust', which is highlighted with a red box. To the right of this box, a callout bubble says 'Conditions available for Android'. Below the posture type, there are four options: 'Client Certificate', 'Full Disk Encryption', and 'Unauthorized Modification' (both in blue), and 'Certificate Trust' (in red, matching the dropdown). At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows a dark dashboard with various settings and audit logs.

Slide notes

For **Android**, you have the **Certificate Trust**, **Client Certificate** and **Full Disk Encryption** options, plus an **Unauthorized Modification** condition, which checks to see if the device has been 'rooted'.

Slide 48 - Slide 48

The screenshot shows the Zscaler Device Posture configuration interface. A modal window titled "Add Device Posture" is open, overlaid on a dark background. The modal has several sections:

- DEFINE POLICY AND SCOPE**:
 - Name: Mandatory
- PLATFORM**:
 - Windows: Off (red)
 - macOS: Off (red)
 - Android: Off (red)
 - iOS: On (green)
- DEVICE POSTURE CONFIGURATION**:
 - Posture Type: Certificate Trust (selected, highlighted with a red border)
 - Conditions available for iOS: Unauthorized Modification
- DEVICE POSTURE DESCRIPTION**:
 - Optional: (Text area)

At the bottom of the modal are "Save" and "Cancel" buttons. The background of the main interface shows a "MANAGE DEVICE POSTURE" section with a table and some status indicators.

Slide notes

For iOS you only have the **Certificate Trust** and **Unauthorized Modification** conditions, the latter checking for 'Jailbreaking'.

Slide 49 - Slide 49

The screenshot shows the Zscaler Device Posture management interface. The left sidebar has a 'Device Posture' tab selected. The main area is titled 'MANAGE DEVICE POSTURES' and contains a table with one row. The table columns are '#', 'Profile Name', and 'Description'. The single entry is '1 AllPlatforms-Cent...'. A callout box with the text 'Click Add Device Posture Profile' points to the 'Add Device Posture Profile' button in the top-left corner of the table area.

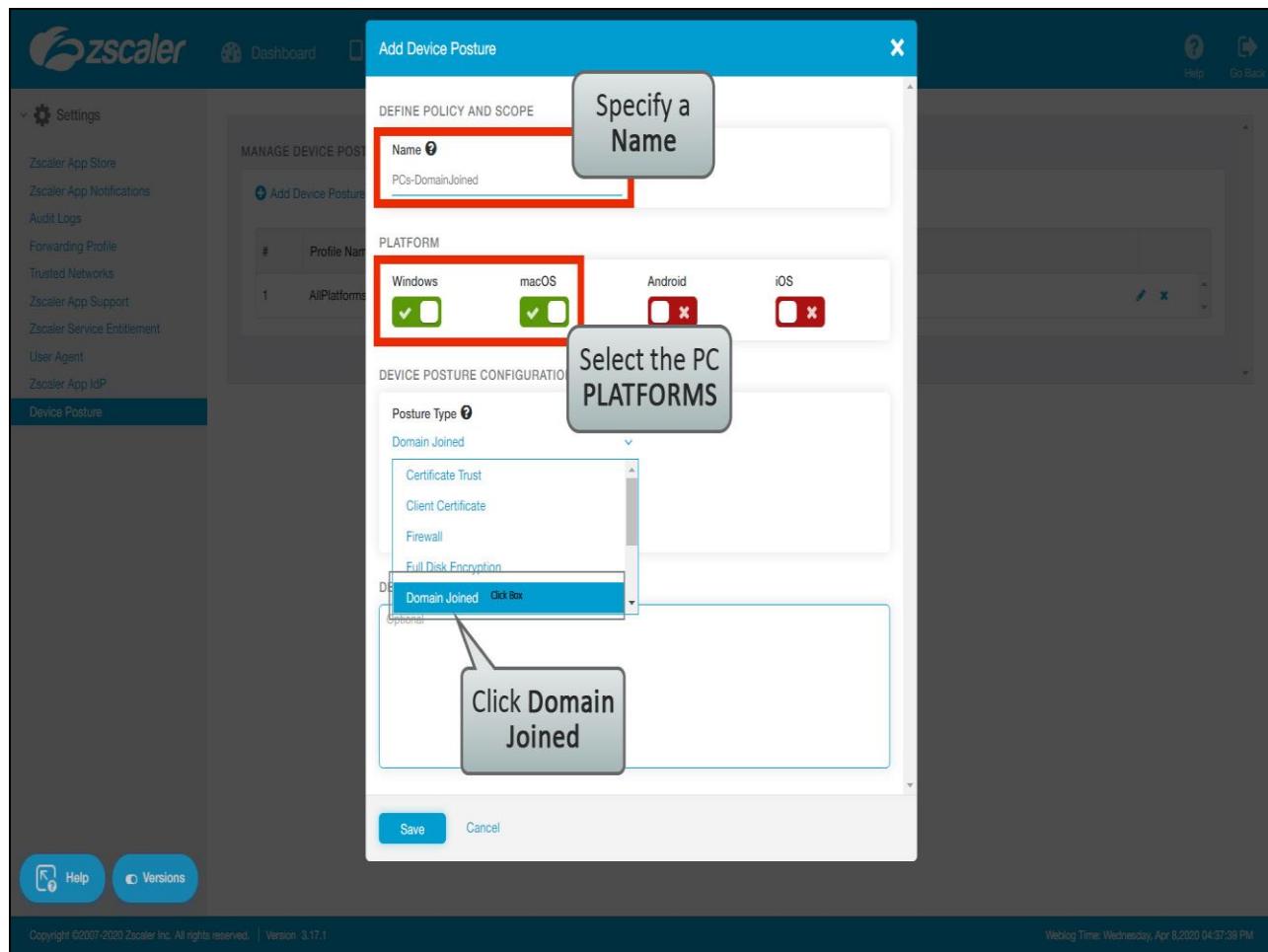
#	Profile Name	Description
1	AllPlatforms-Cent...	

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

To add a condition for PCs, click **Add Device Posture Profile**.

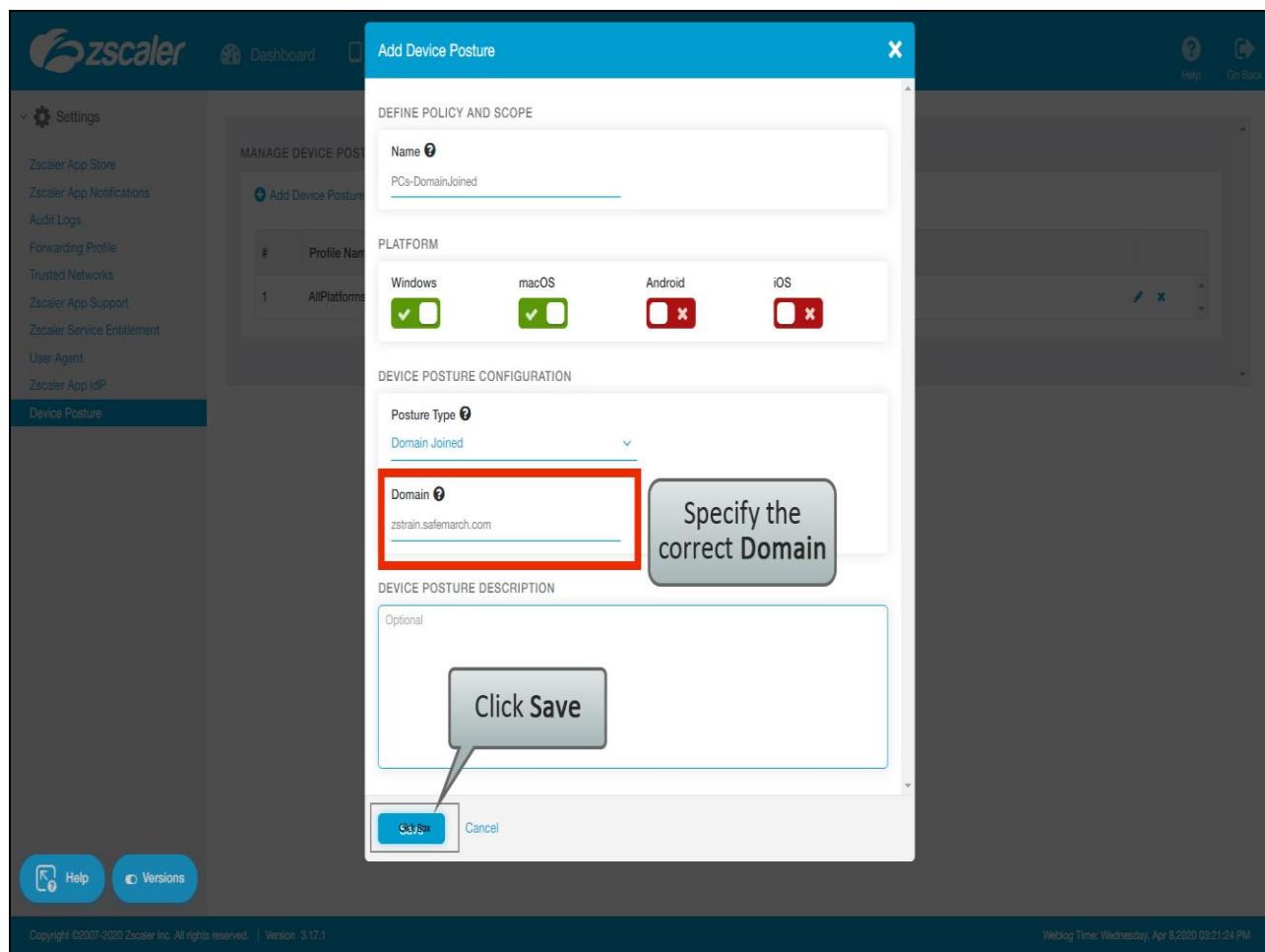
Slide 50 - Slide 50



Slide notes

Give the profile a **Name**, select just the PC platforms (**Windows** and **macOS**), then select a **Posture Type**. For this example, click **Domain Joined**, ...

Slide 51 - Slide 51



Slide notes

...specify the **Domain** to match and click **Save**.

Slide 52 - Slide 52

The screenshot shows the Zscaler Device Posture management interface. At the top, there is a success message: "All Changes have been saved successfully." In the top right corner, there are "Help" and "Go Back" buttons. On the left, a sidebar menu includes "Settings", "Zscaler App Store", "Zscaler App Notifications", "Audit Logs", "Forwarding Profile", "Trusted Networks", "Zscaler App Support", "Zscaler Service Entitlement", "User Agent", "Zscaler App IdP", and "Device Posture", which is highlighted with a blue bar. The main content area is titled "MANAGE DEVICE POSTURES" and contains a table with two rows:

#	Profile Name	Description
1	AllPlatforms-CertTrust	(Edit, Delete)
2	PCs-DomainJoined	(Edit, Delete)

At the bottom left, there are "Help" and "Versions" buttons. The bottom right corner displays the "Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM".

Slide notes

Slide 53 - Slide 53

The screenshot shows the Zscaler Device Posture management interface. The left sidebar has a 'Device Posture' tab selected. The main area is titled 'MANAGE DEVICE POSTURES' and contains a table with two rows:

#	Profile Name	Description
1	AllPlatforms-Cent	(edit) (x)
2	PCs-DomainJoin	(edit) (x)

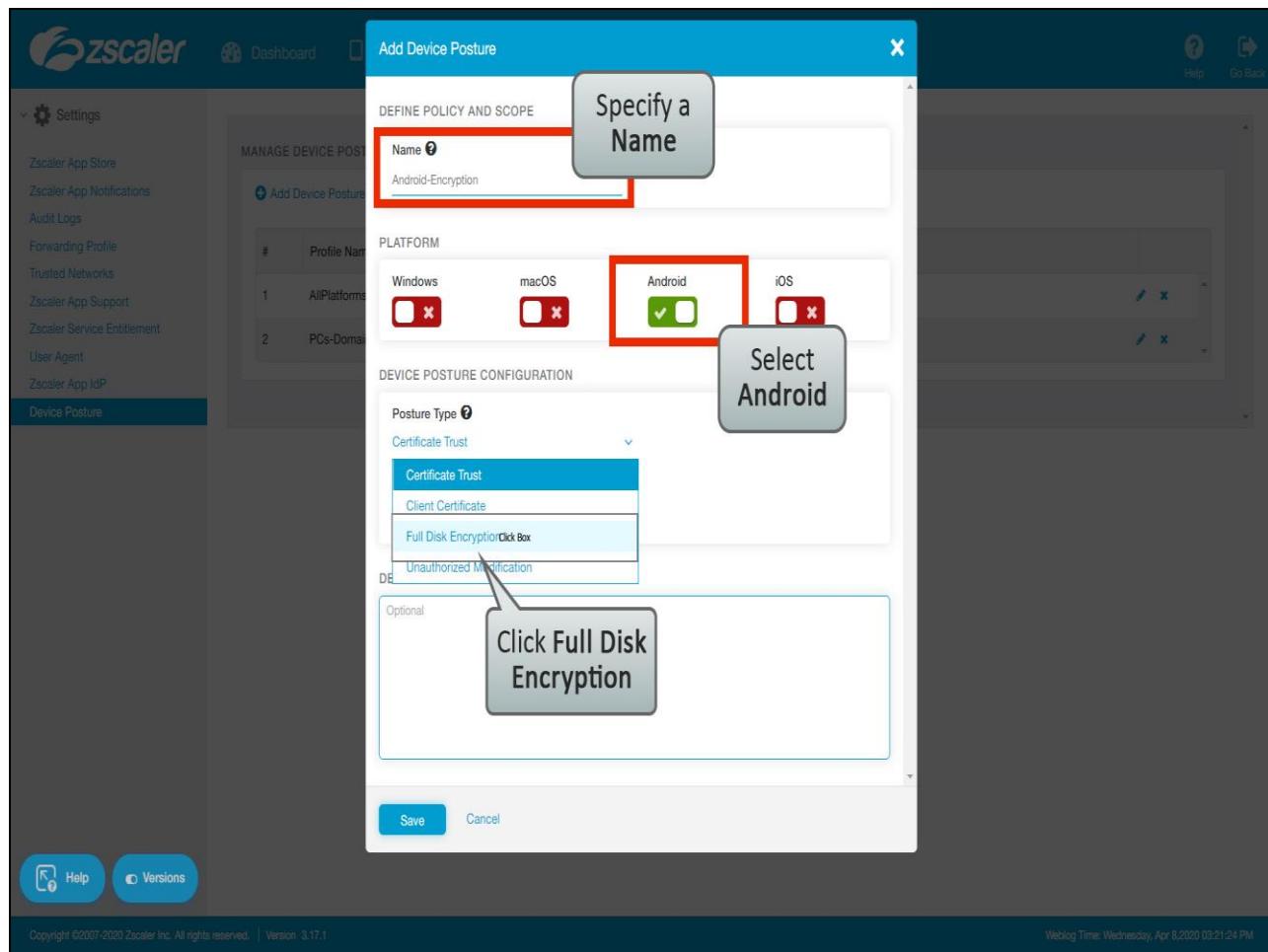
A callout box with the text 'Click Add Device Posture Profile' points to the 'Add Device Posture Profile' button in the top-left corner of the table header.

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

To add an **Android** profile, click **Add Device Posture Profile**, ...

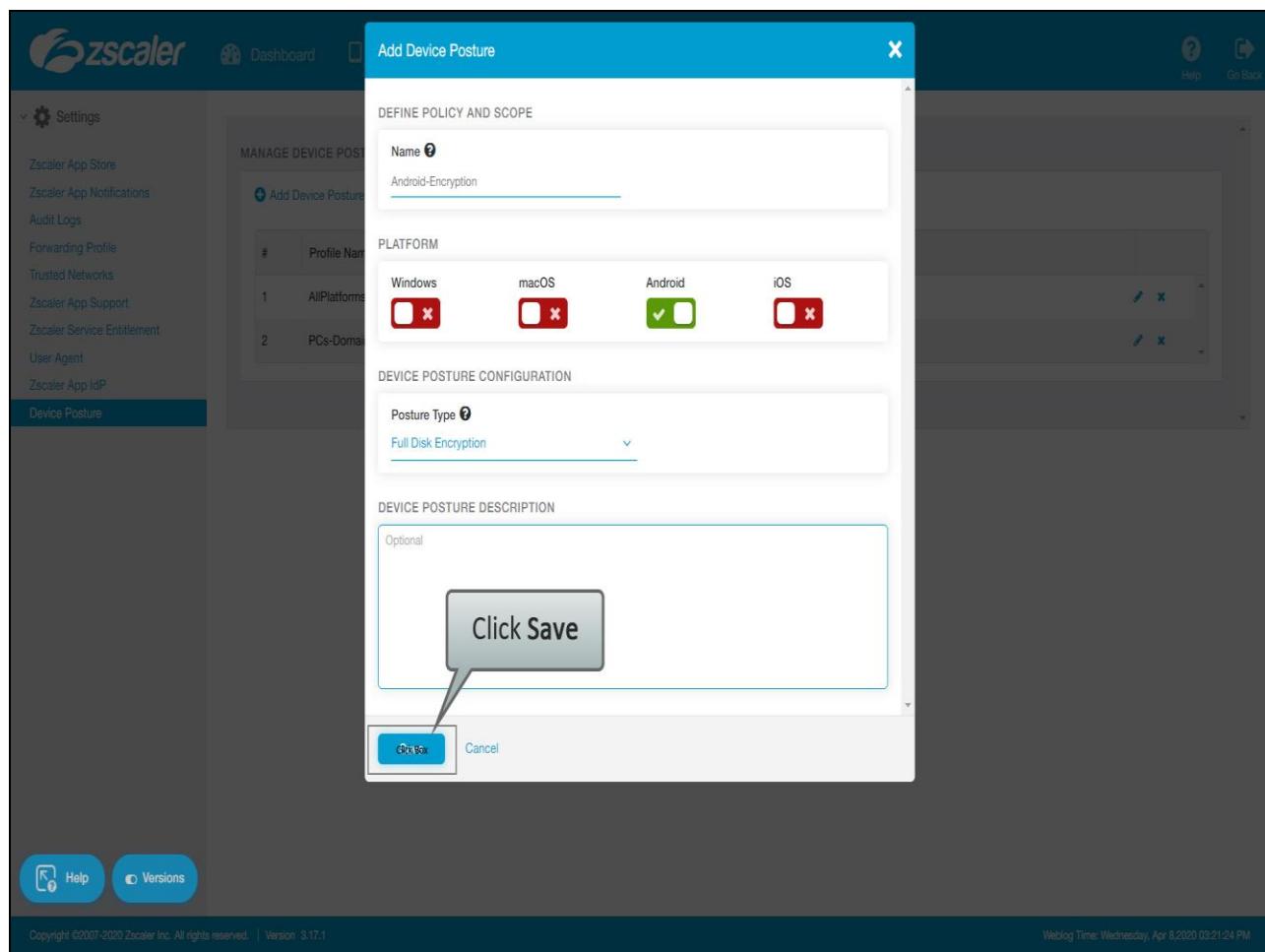
Slide 54 - Slide 54



Slide notes

Give the profile a **Name**, select **Android**, then select a **Posture Type**. For this example, click **Full Disk Encryption**, ...

Slide 55 - Slide 55



Slide notes

...and click **Save**.

Slide 56 - Slide 56

The screenshot shows the Zscaler Device Posture management interface. At the top, there is a blue header bar with the Zscaler logo, a 'Dashboard' button, and a message 'All Changes have been saved successfully.' In the top right corner, there are 'Help' and 'Go Back' buttons. On the left, a sidebar titled 'Settings' contains links for Zscaler App Store, Zscaler App Notifications, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IdP, and 'Device Posture' (which is highlighted in blue). The main content area is titled 'MANAGE DEVICE POSTURES' and features a table with three rows:

#	Profile Name	Description
1	AllPlatforms-CertTrust	(Edit, Delete)
2	PCs-DomainJoined	(Edit, Delete)
3	Android-Encryption	(Edit, Delete)

At the bottom of the interface, there are 'Help' and 'Versions' buttons, and a footer bar with copyright information: 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1' and 'Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM'.

Slide notes

Slide 57 - Slide 57

The screenshot shows the Zscaler Device Posture management interface. The left sidebar has a 'Device Posture' tab selected. The main area is titled 'MANAGE DEVICE POSTURES' and contains a table with three rows:

#	Profile Name	Description
1	AllPlatforms-Cent	
2	PCs-DomainJoin	
3	Android-Encrypt	

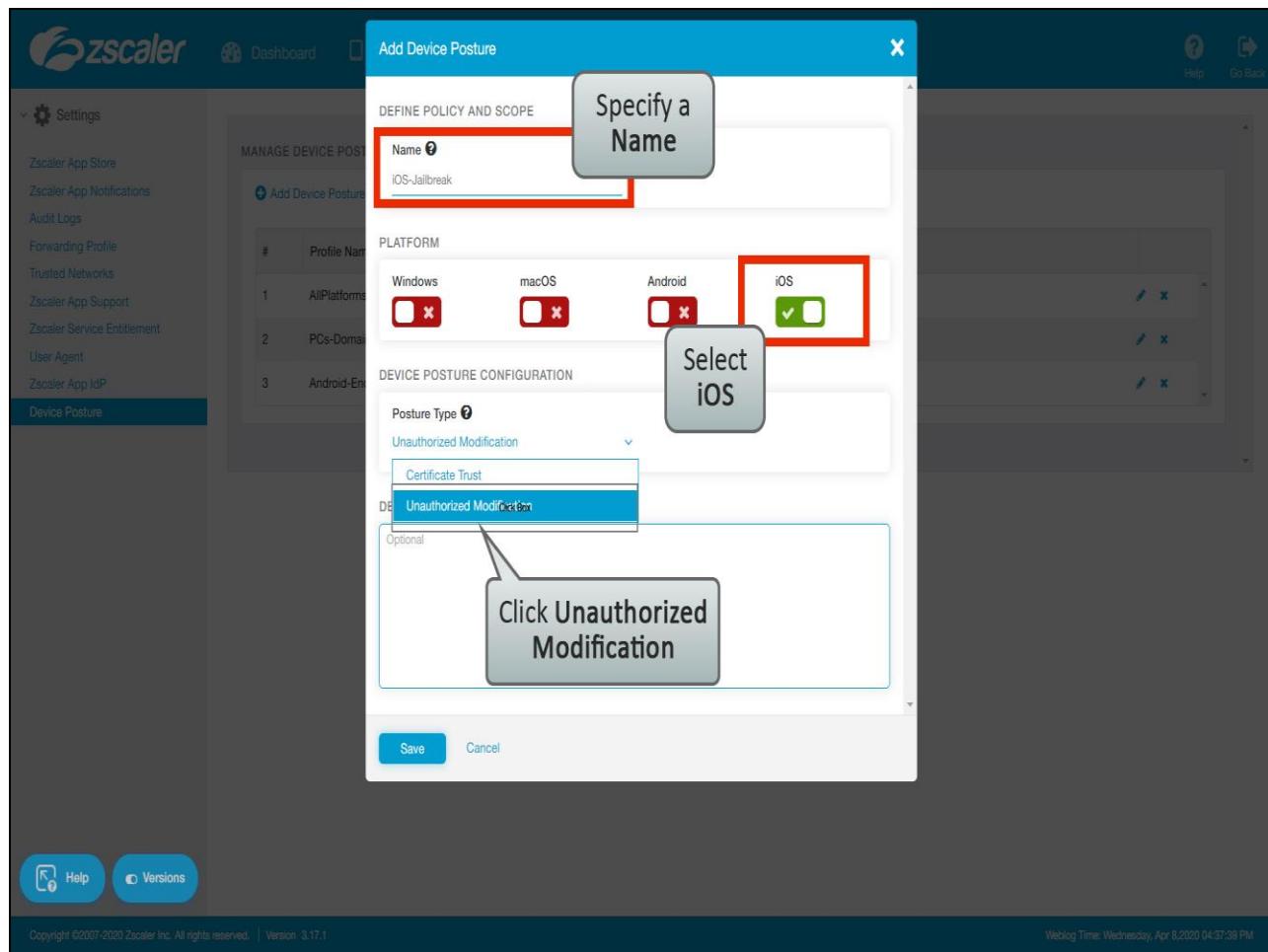
A callout box with the text 'Click Add Device Posture Profile' points to the 'Add Device Posture Profile' button in the top-left corner of the table header.

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM

Slide notes

Finally, to add an iOS profile, click **Add Device Posture Profile**, ...

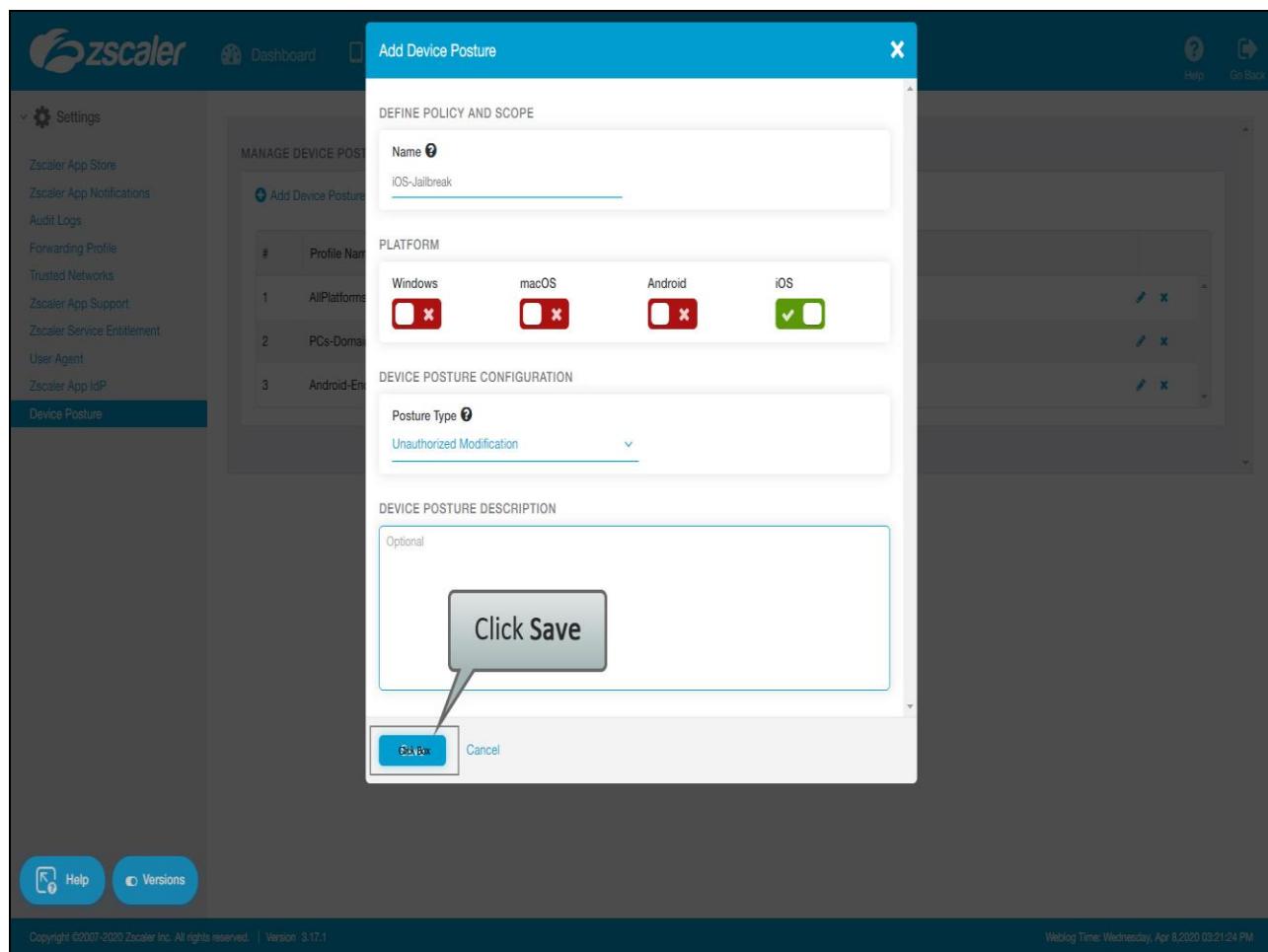
Slide 58 - Slide 58



Slide notes

Give the profile a **Name**, select **iOS** only, then select a **Posture Type**. For this example, click **Unauthorized Modification**, ...

Slide 59 - Slide 59



Slide notes

...and click **Save**.

Slide 60 - Slide 60

The screenshot shows the Zscaler Settings interface with a blue header bar. The header includes the Zscaler logo, a Dashboard link, and a message box stating "All Changes have been saved successfully." with a close button. On the right side of the header are "Help" and "Go Back" buttons.

The left sidebar contains a "Settings" section with the following options: Zscaler App Store, Zscaler App Notifications, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IdP, and **Device Posture**, which is highlighted with a blue background.

The main content area is titled "MANAGE DEVICE POSTURES" and features a table with the following data:

#	Profile Name	Description
1	AllPlatforms-CertTrust	
2	PCs-DomainJoined	
3	Android-Encryption	
4	iOS-Jailbreak	

At the bottom of the page are two buttons: "Help" and "Versions". The footer contains copyright information: "Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1" and a timestamp: "Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM".

Slide notes

Slide 61 - Slide 61

The screenshot shows the Zscaler Admin Portal interface. The top navigation bar includes links for Dashboard, Enrolled Devices, App Profiles, Administration, Help, and Go Back. On the left, a sidebar under 'Settings' lists various options like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IdP, and Device Posture, with 'Device Posture' being the active tab. The main content area is titled 'MANAGE DEVICE POSTURES' and contains a table with four rows of device posture profiles:

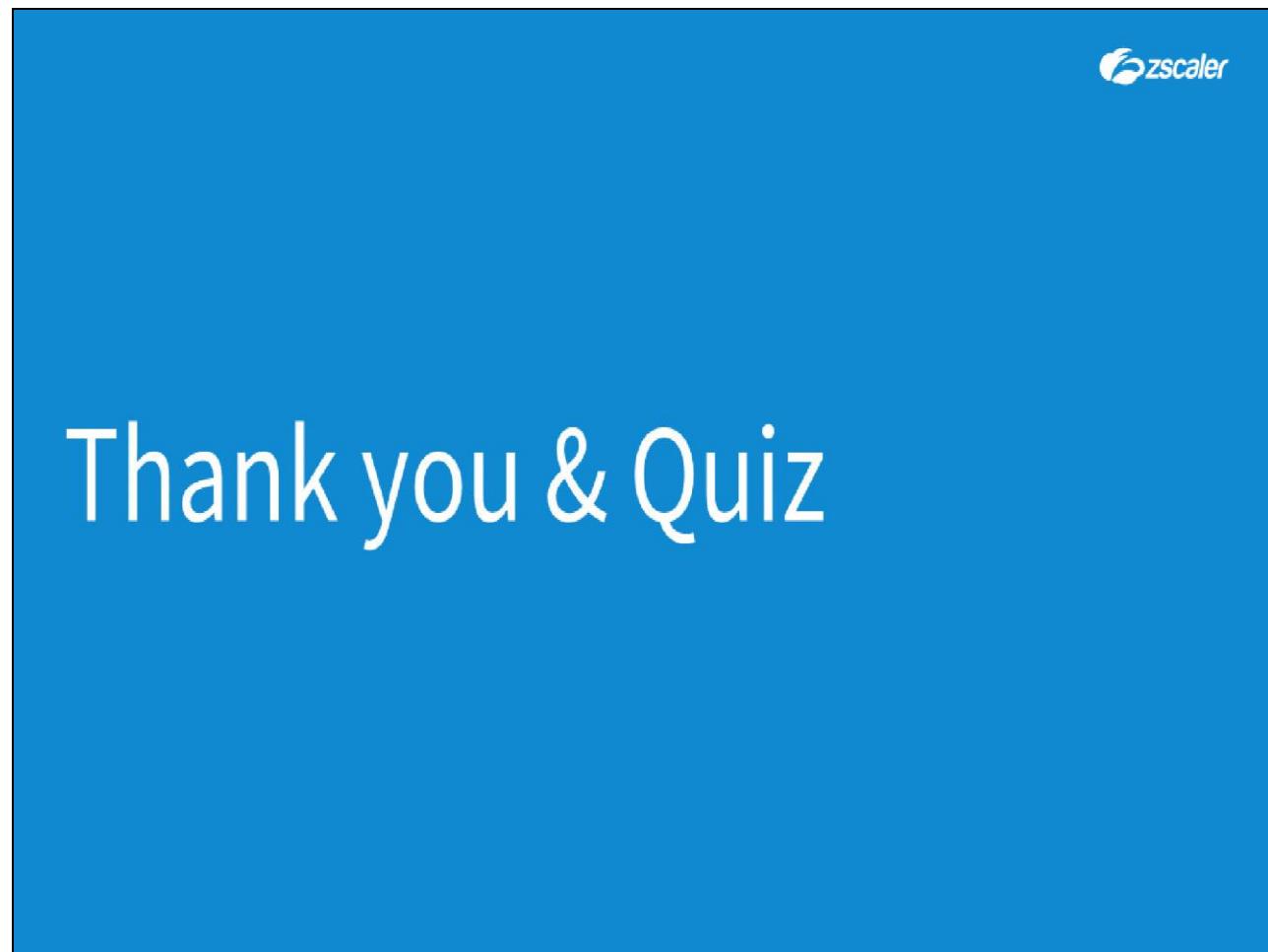
#	Profile Name	Description
1	AllPlatforms-CertTrust	
2	PCs-DomainJoined	
3	Android-Encryption	
4	iOS-Jailbreak	

At the bottom of the portal, there are 'Help' and 'Versions' buttons, and a footer note: 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1'. The timestamp in the footer is 'Weblog Time: Wednesday, Apr 8, 2020 03:21:24 PM'.

Slide notes

Having added several **Device Posture** profiles, these are now available from the ZPA Admin Portal to select in an **Access Policy**, to control access to private applications.

Slide 62 - 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.

Click the X at top right to close this interface, then launch the quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.