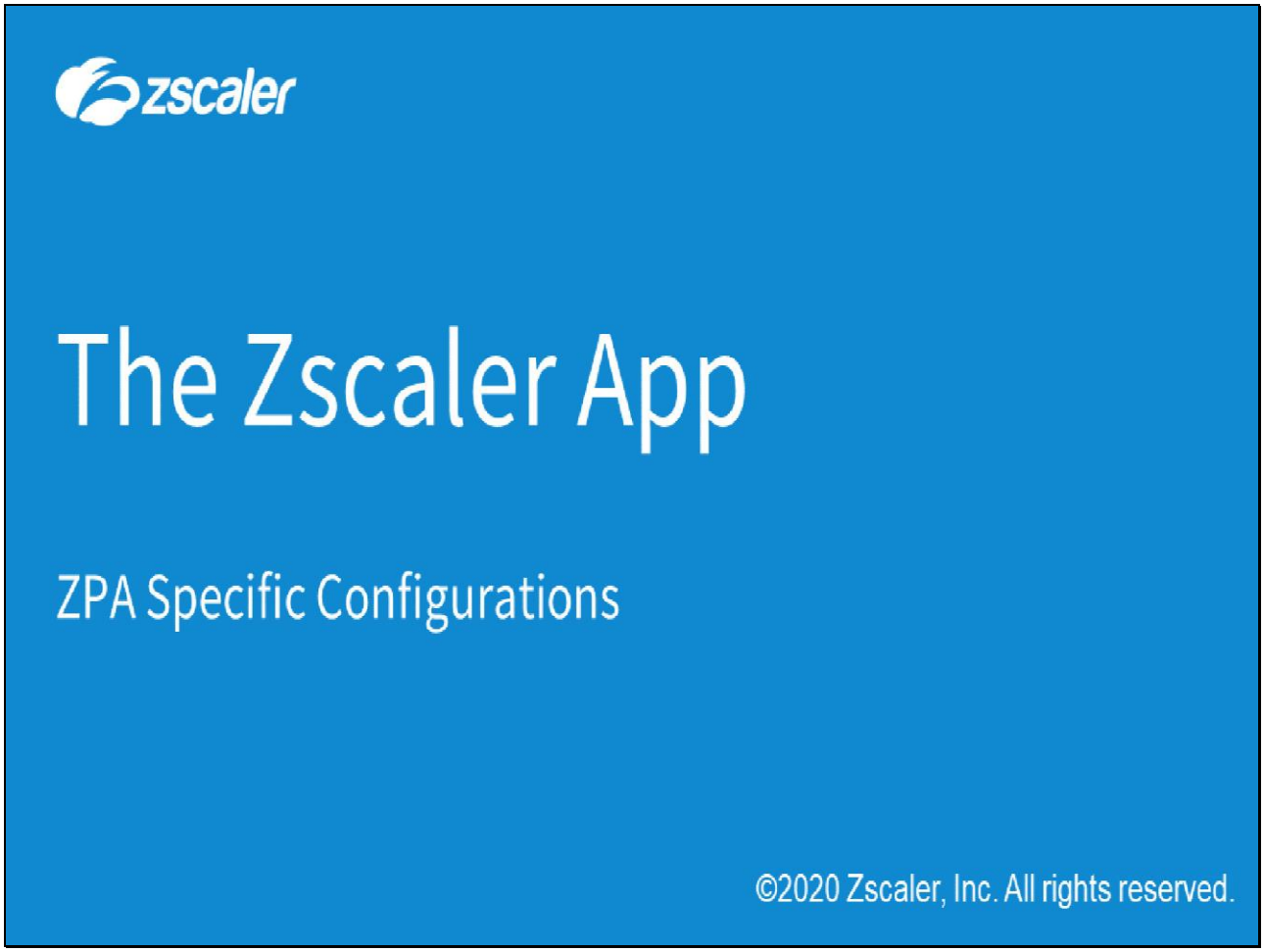
Slide 1 – The Zscaler App: ZPA Specific Configurations



Slide notes

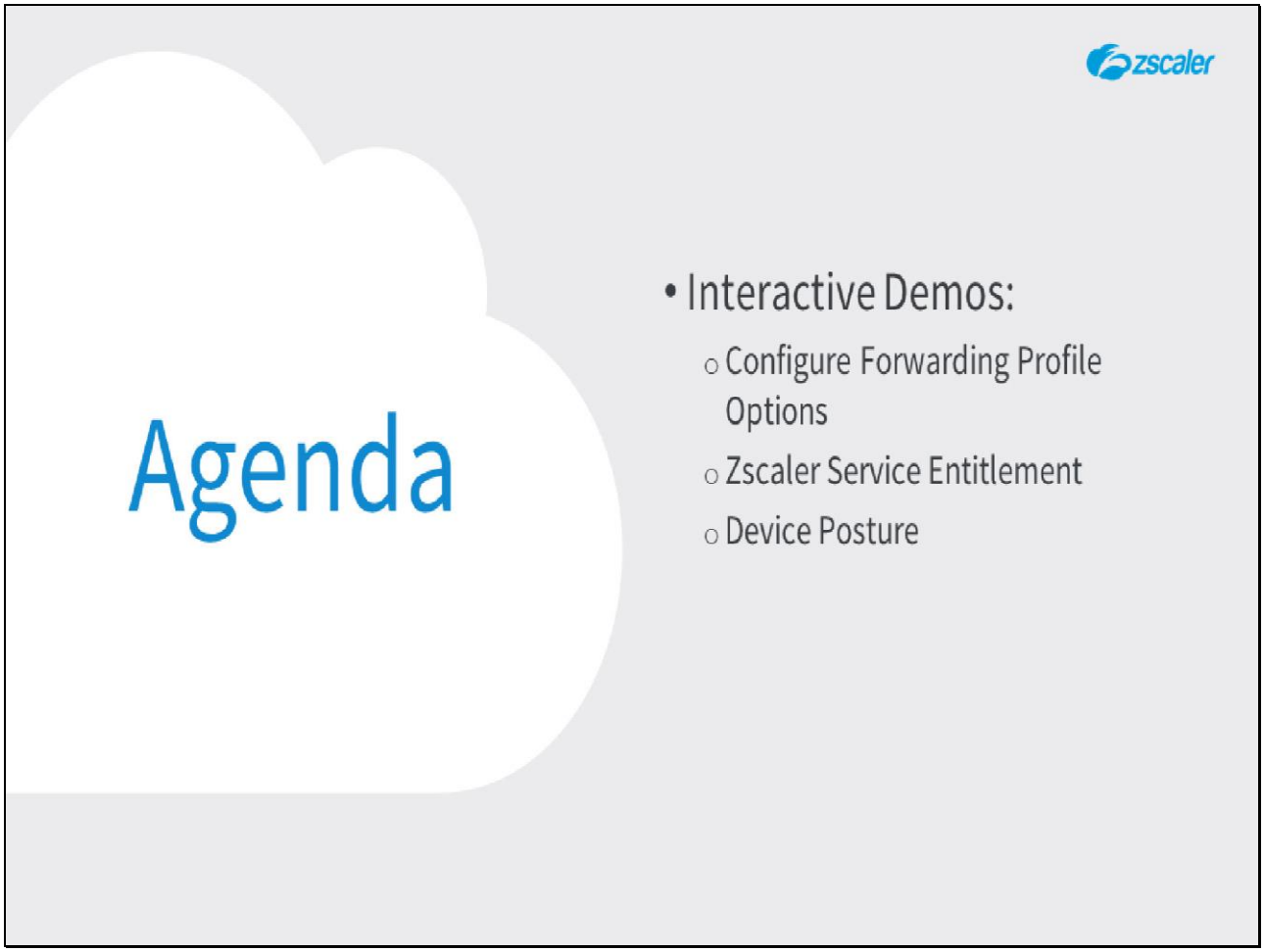
Welcome to this training module on Zscaler App configurations that are specific to the ZPA service.

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 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.

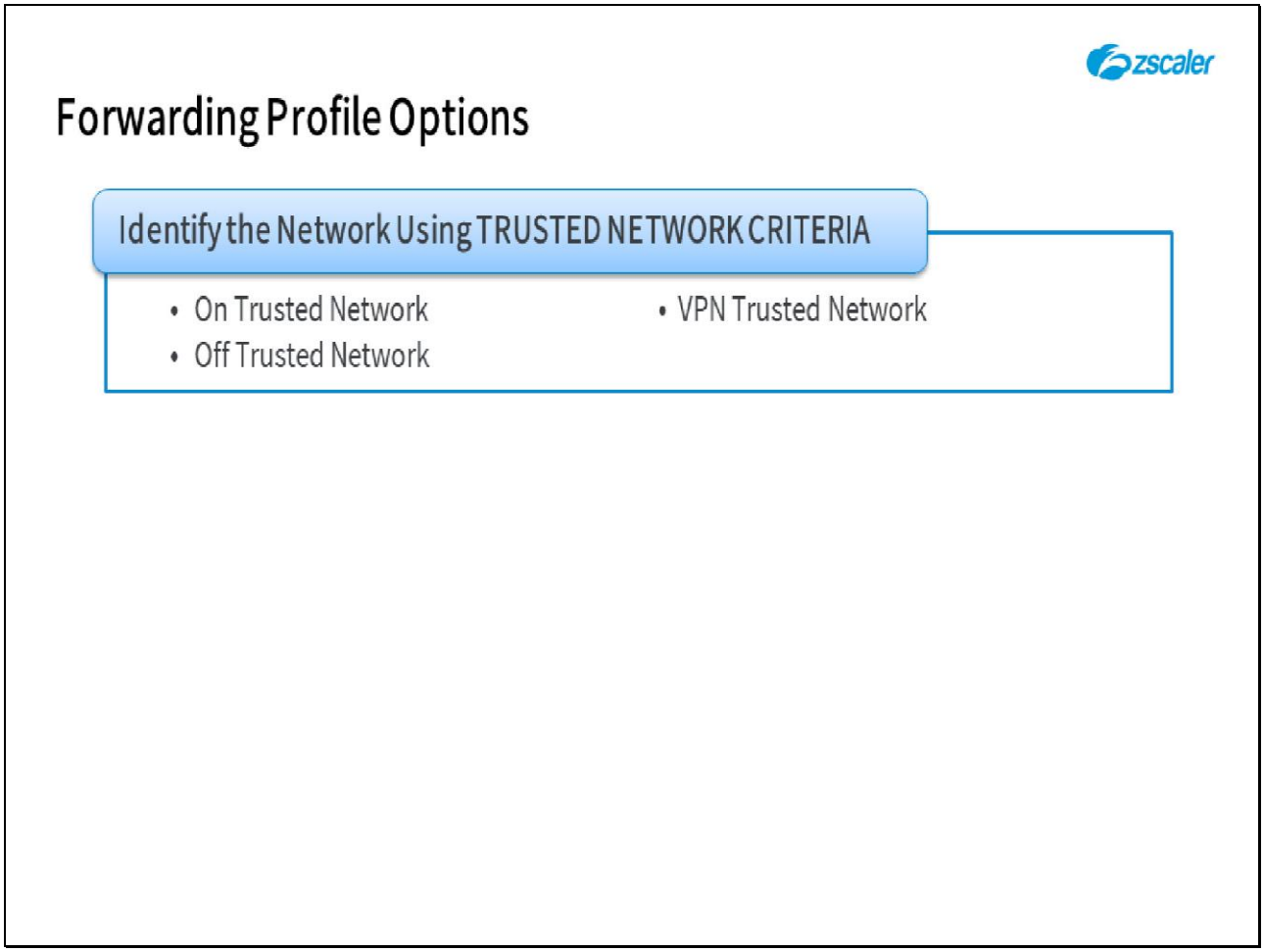
Slide 4 - Interactive Demo: Provisioning the Zscaler App

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.

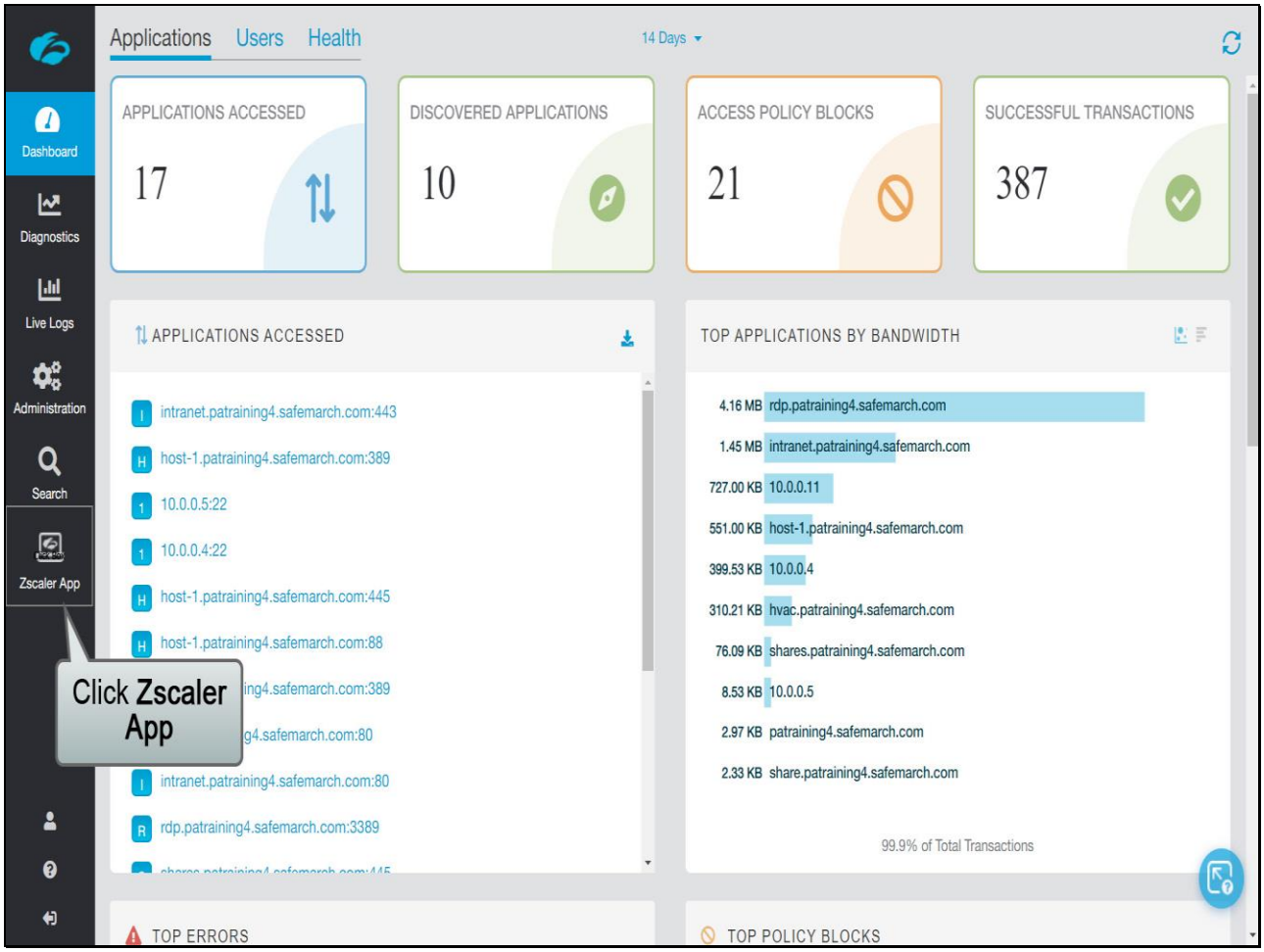
Slide 5 - Steps For Using the Zscaler App IdP



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

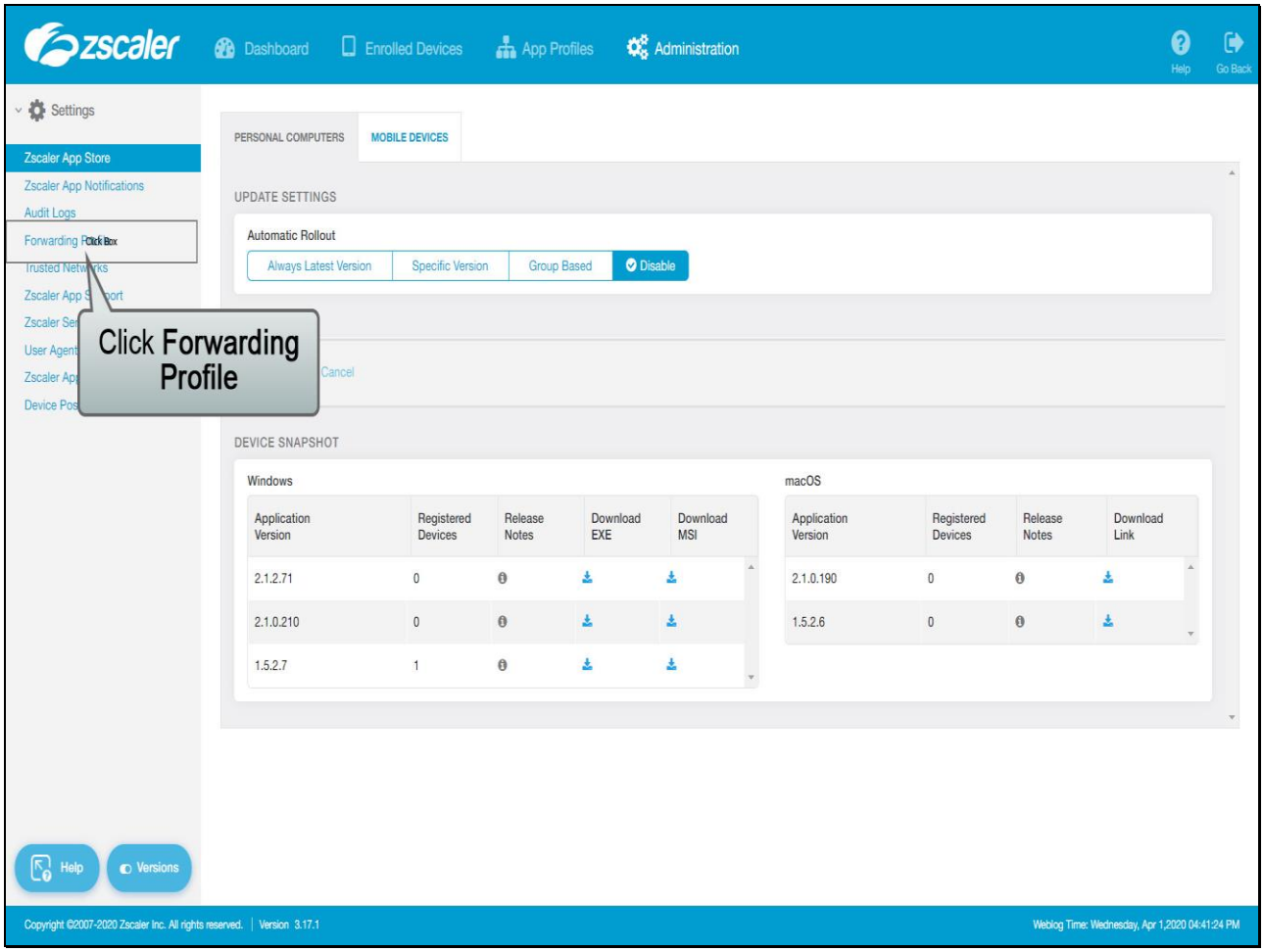
To access the Zscaler App Portal from the ZPA Admin Portal, click the **Zscaler App** icon.

Slide 7 - Slide 7

Slide notes

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

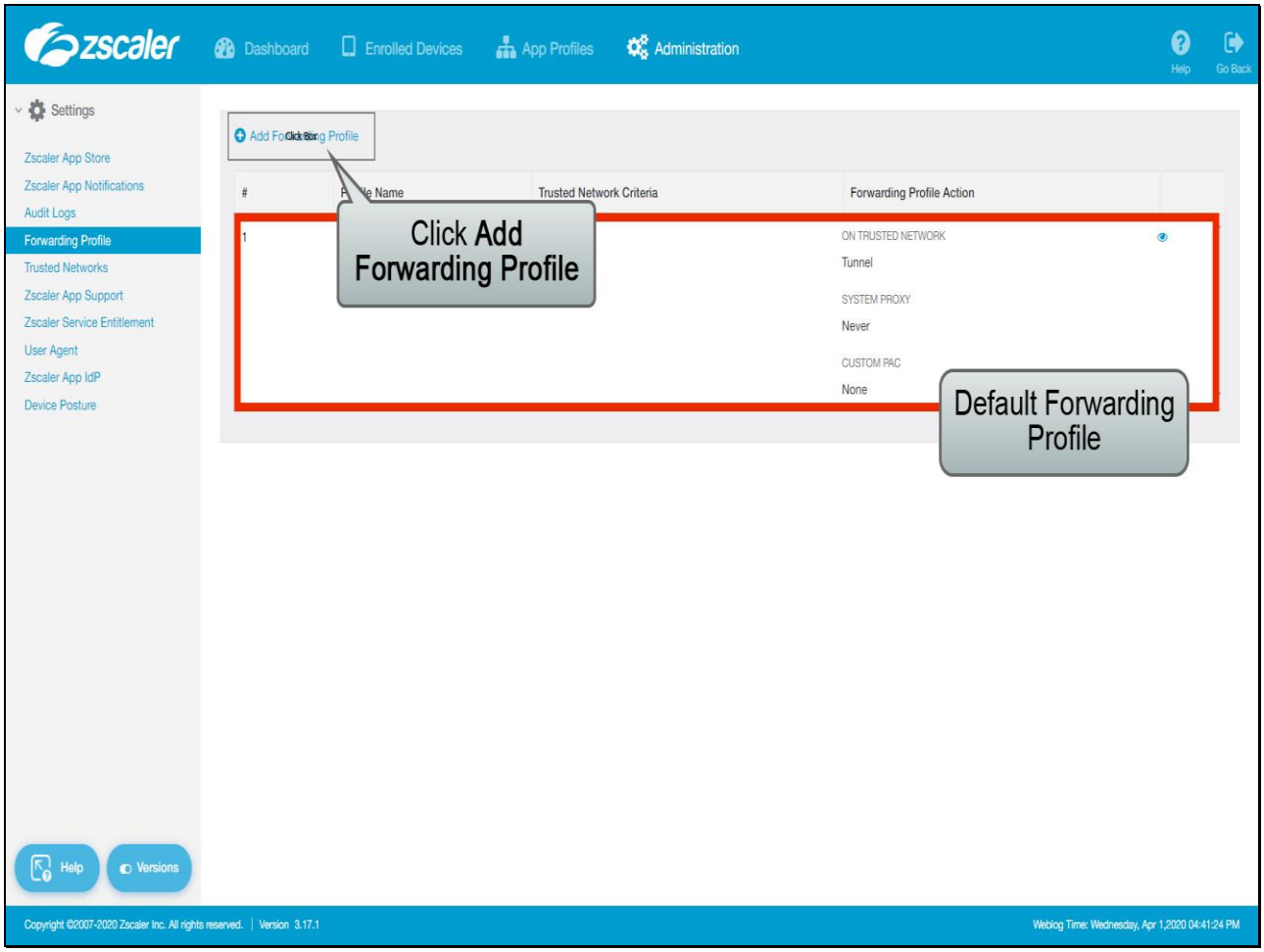
Slide 8 - Slide 8



Slide notes

...then click **Forwarding Profile**.

Slide 9 - Slide 9



Slide notes

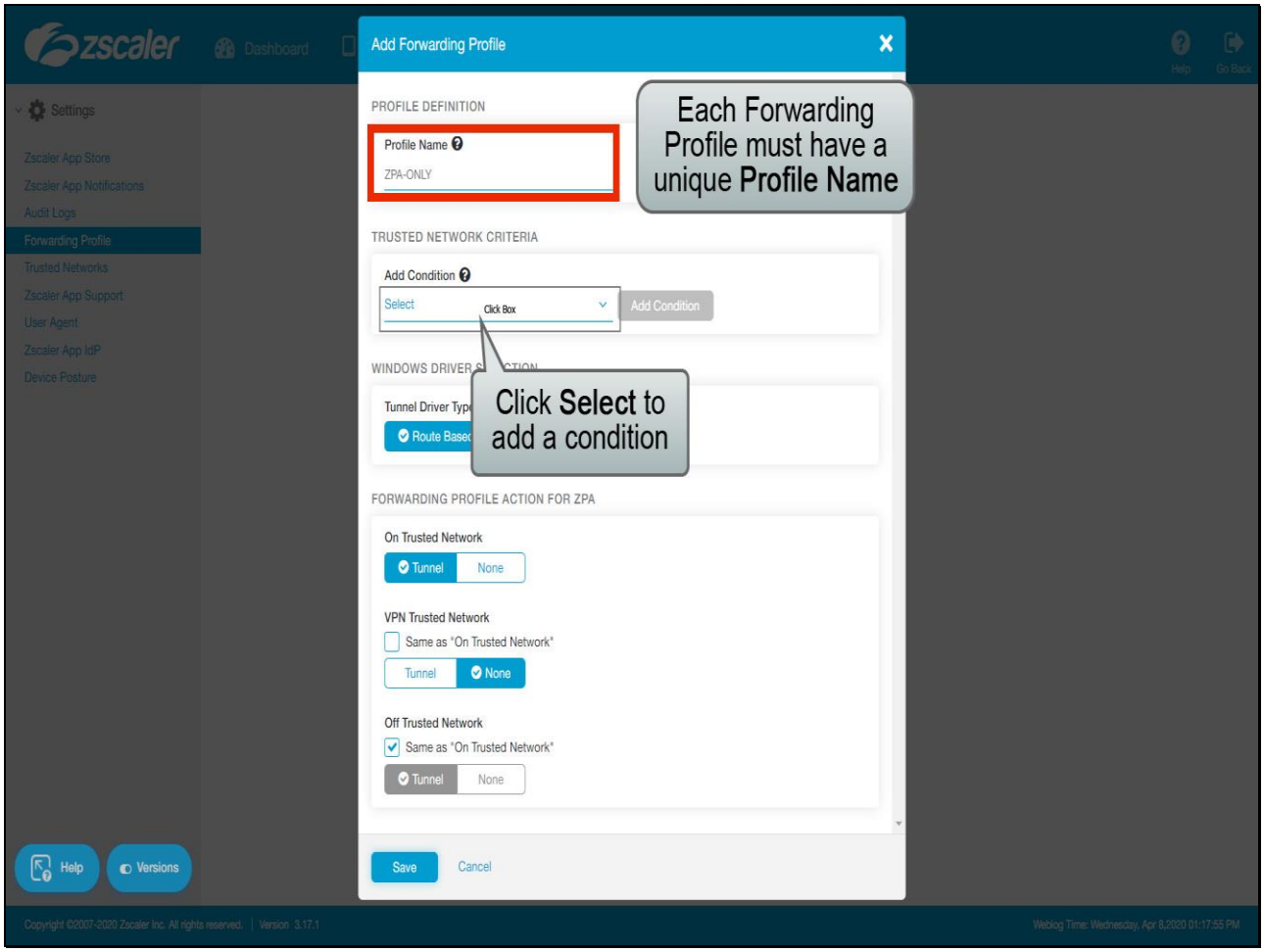
You will find that there is a default **Forwarding Profile** (which cannot be edited), and the option to add a new one. The default profile configuration is as follows:

- **On and Off Tusted 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

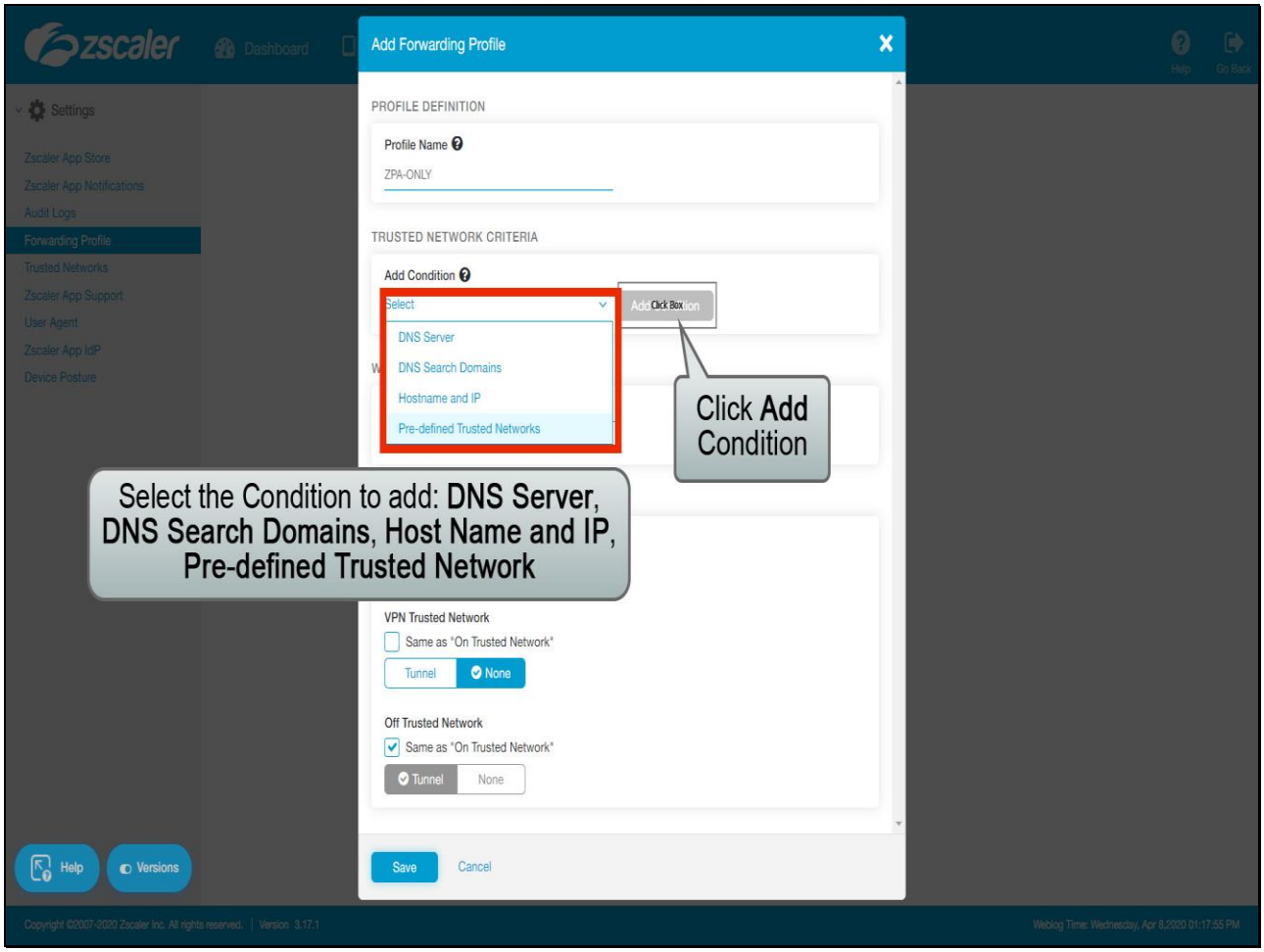


Slide notes

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



Slide notes

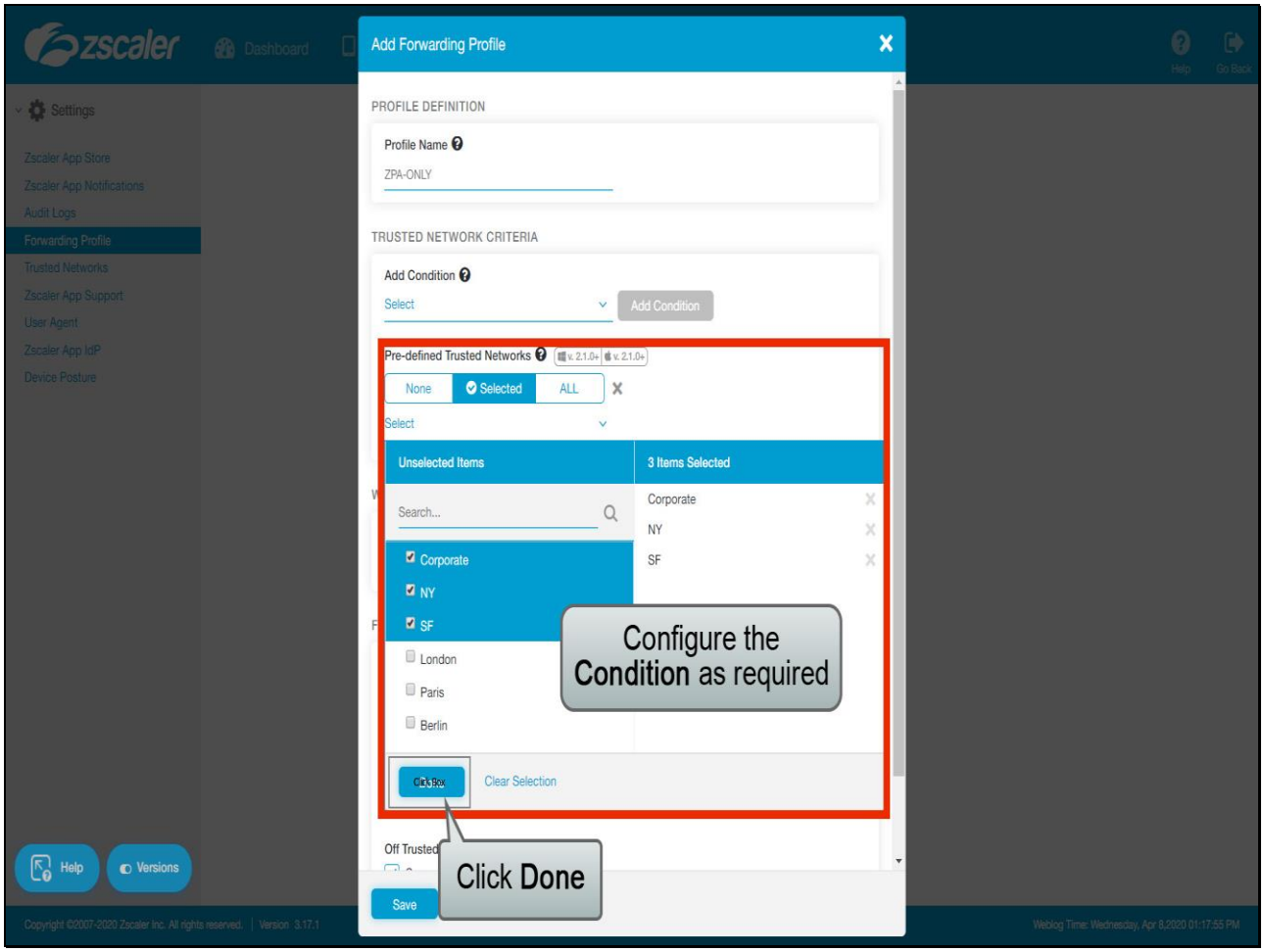
...and select the appropriate condition to be met. The conditions available are:

- **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, …

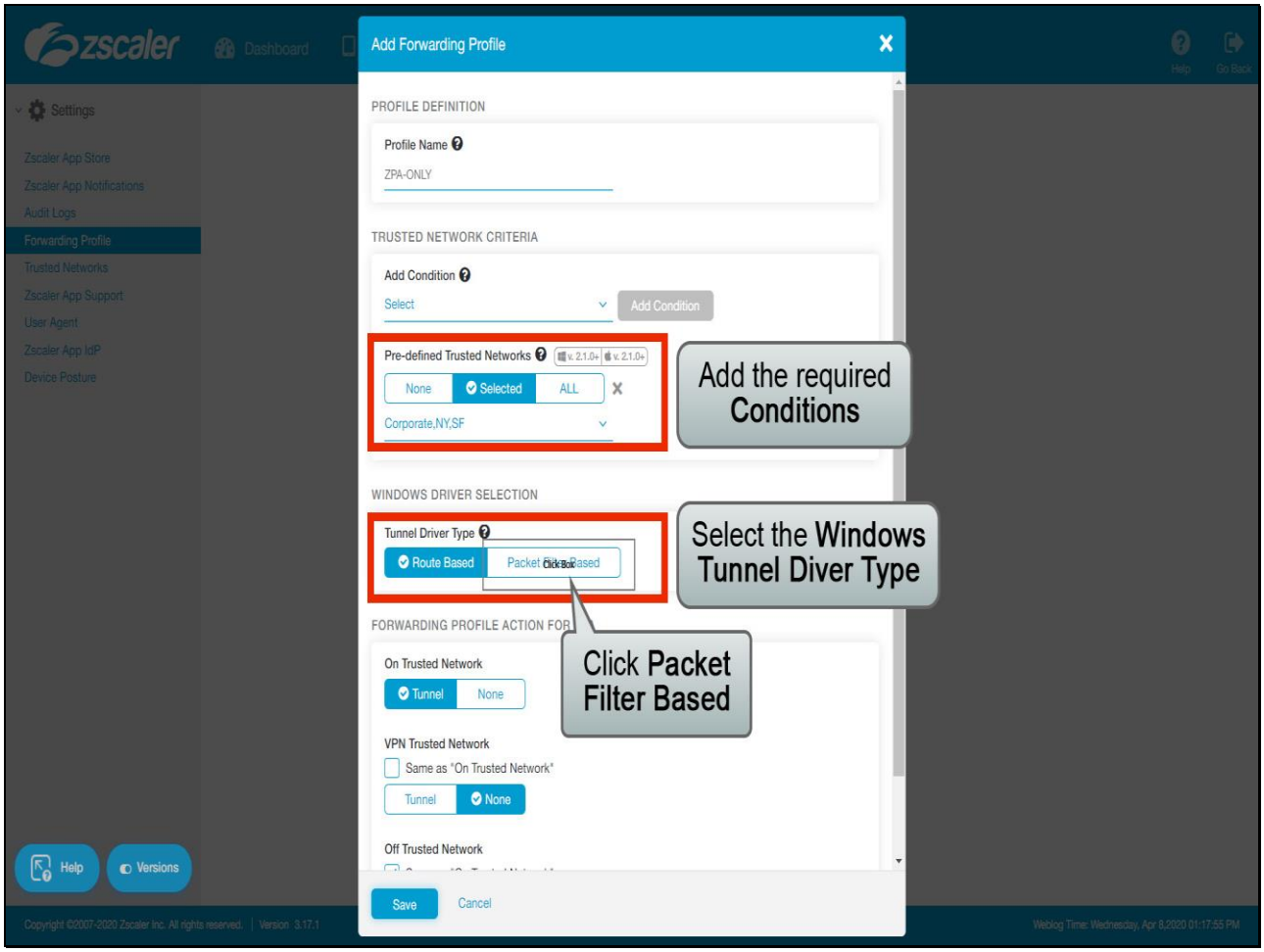
Slide 12 - Slide 12



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

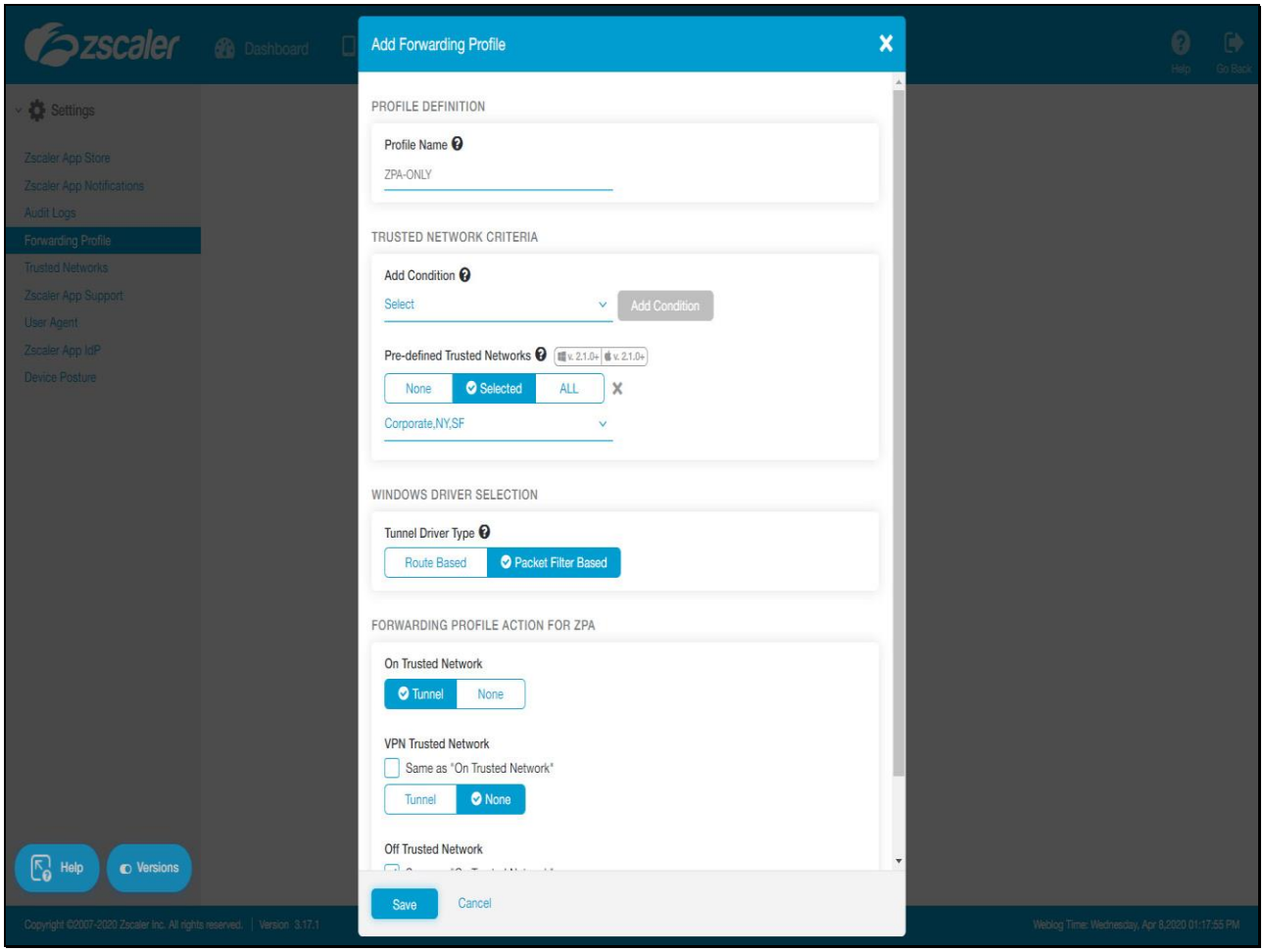


Slide notes

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.

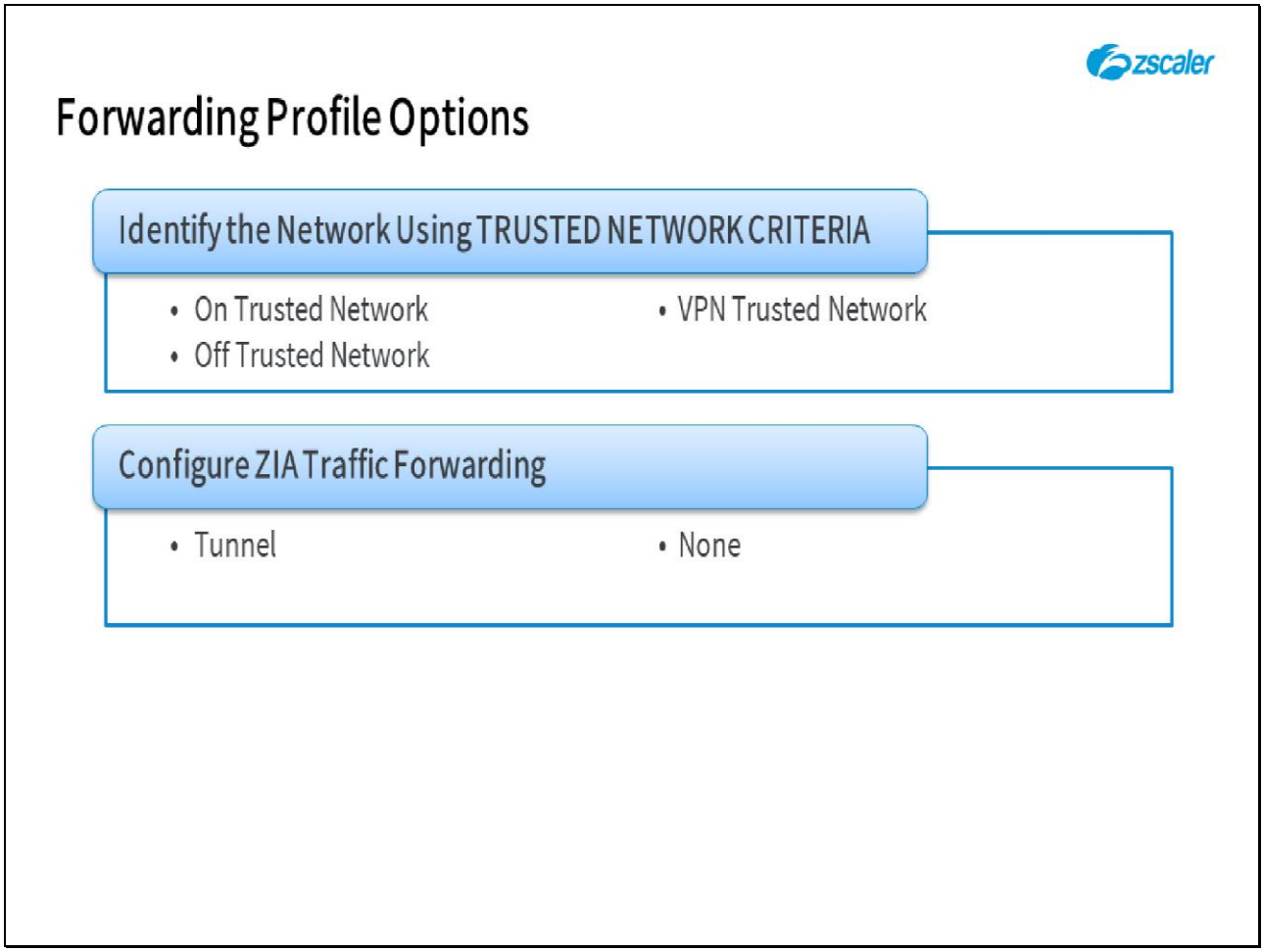
By default this is set to the **Route Based** option, to use the recommended driver, click **Packet Filter Based**.

Slide 14 - Slide 14



Slide notes

Slide 15 - Forwarding Profile Options



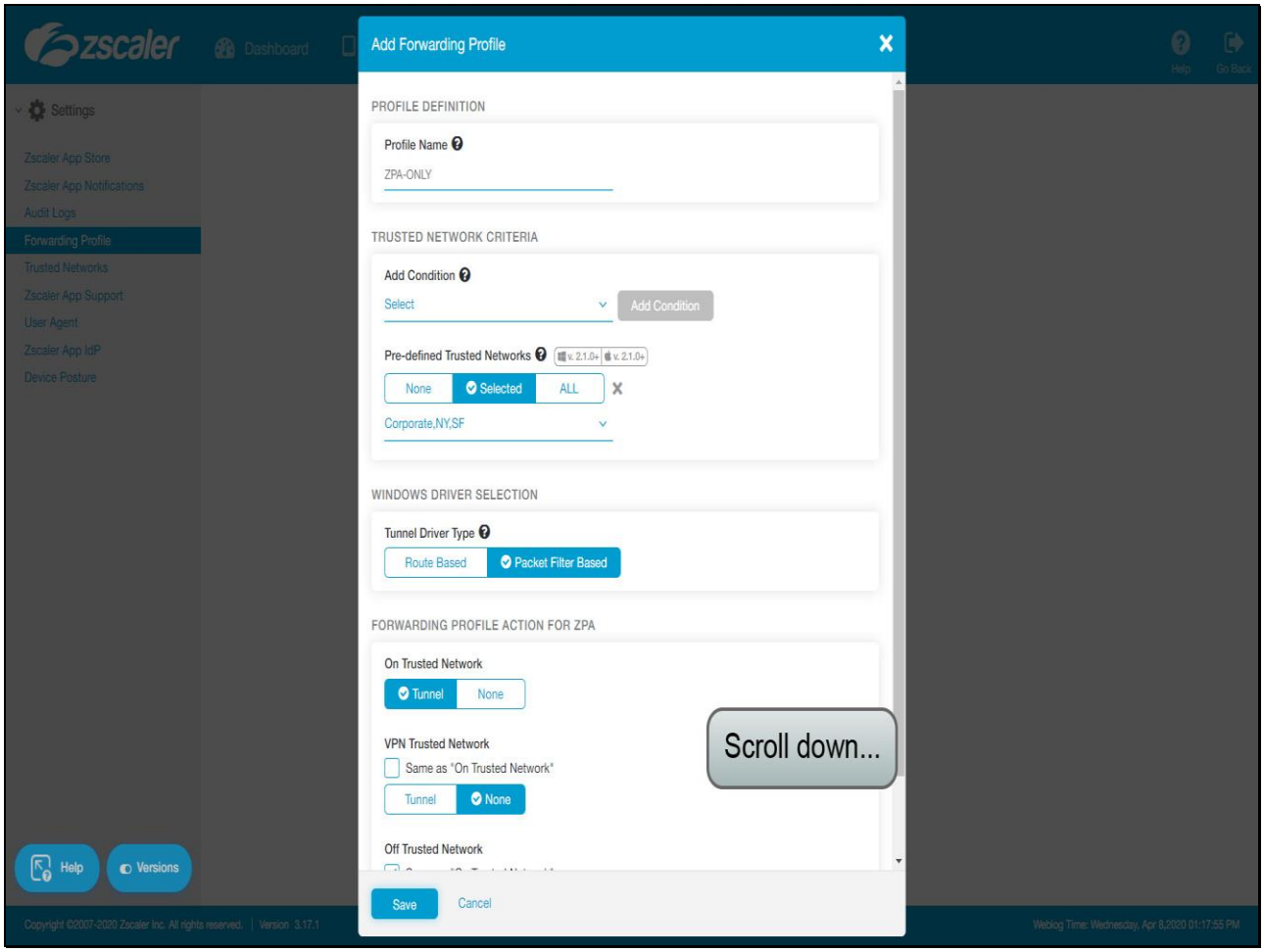
Slide notes

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.

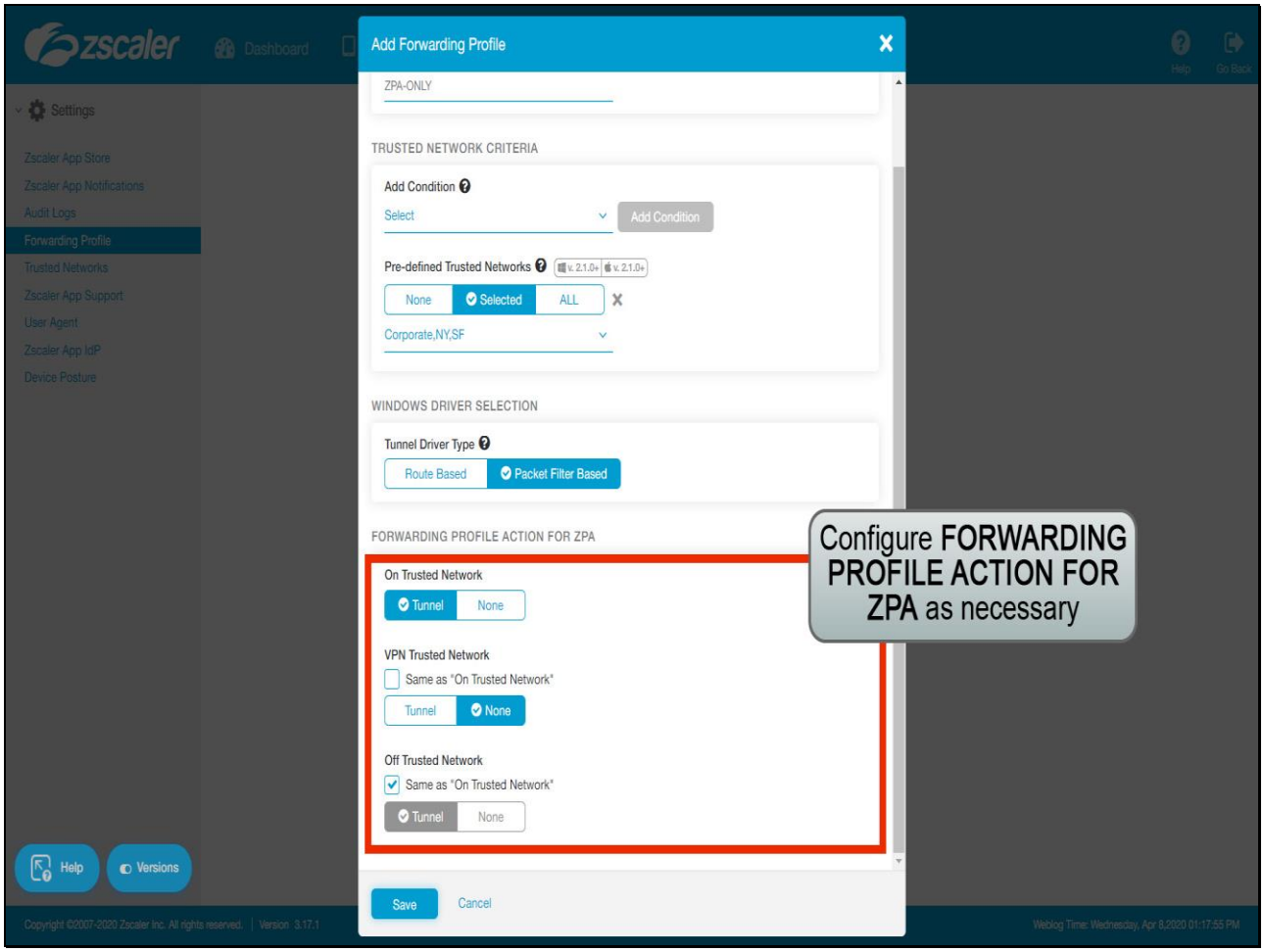
Slide 16 - Slide 16



Slide notes

Scroll down if necessary, ...

Slide 17 - Slide 17

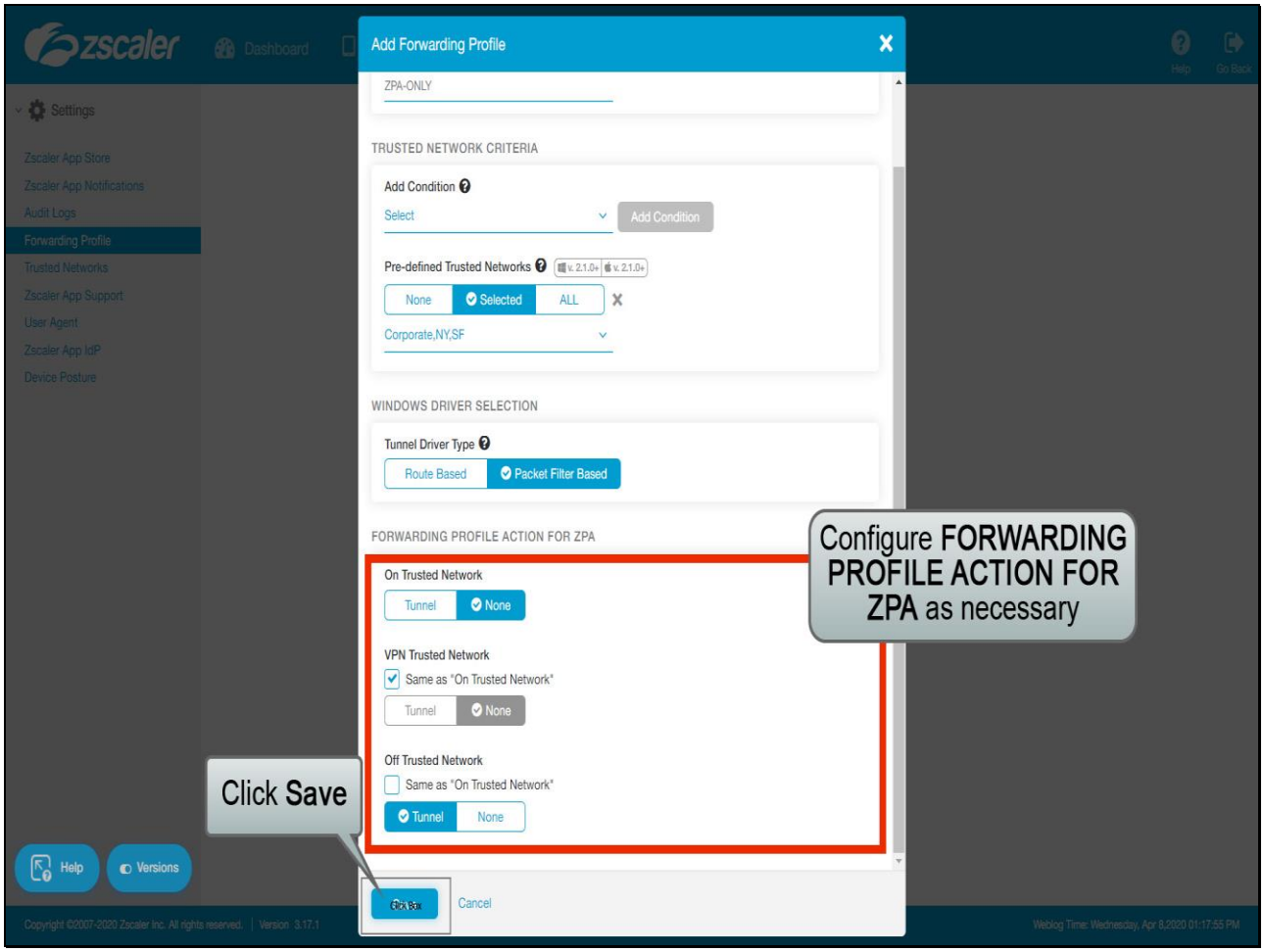


Slide notes

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.

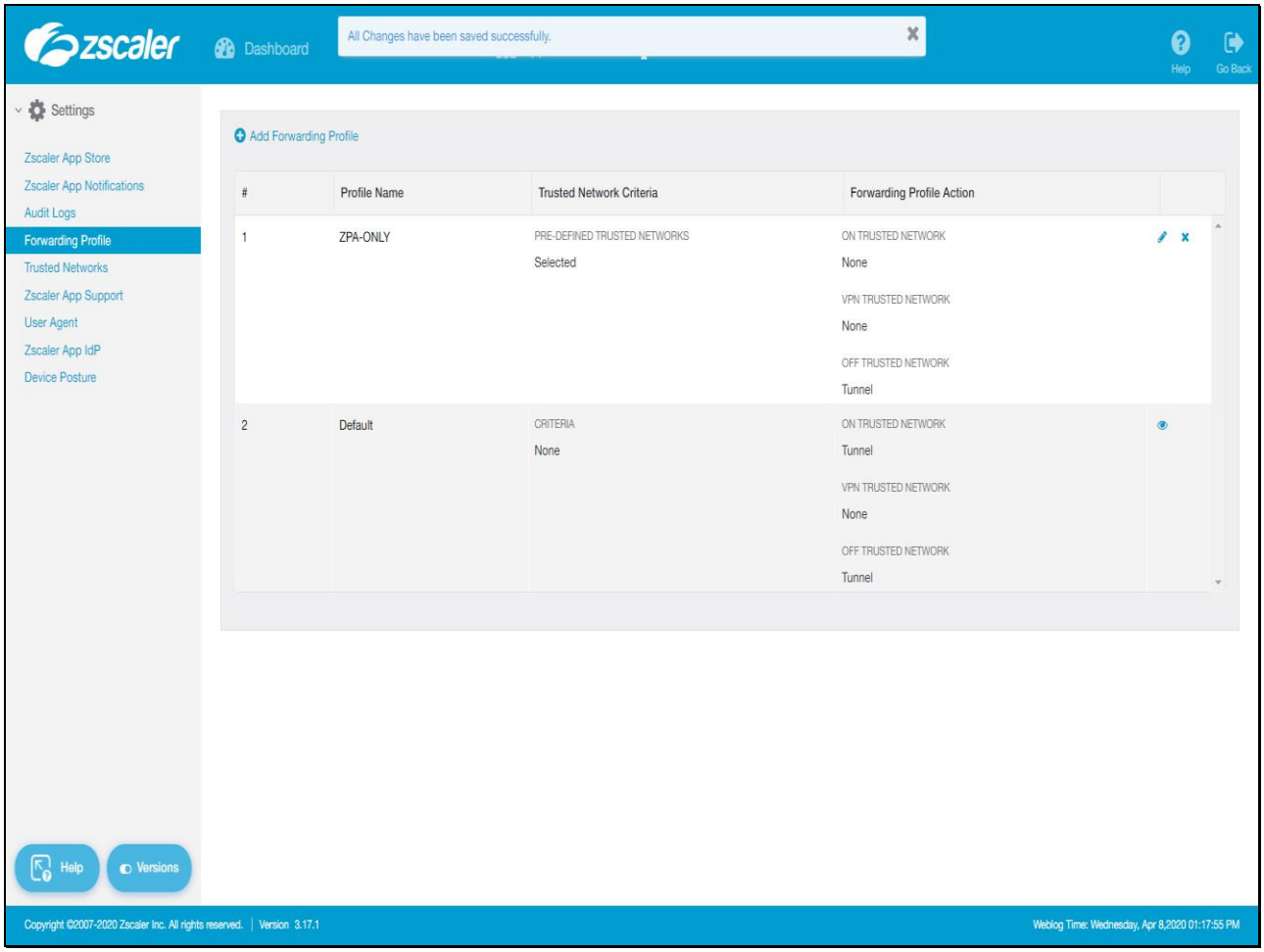
Slide 18 - Slide 18



Slide notes

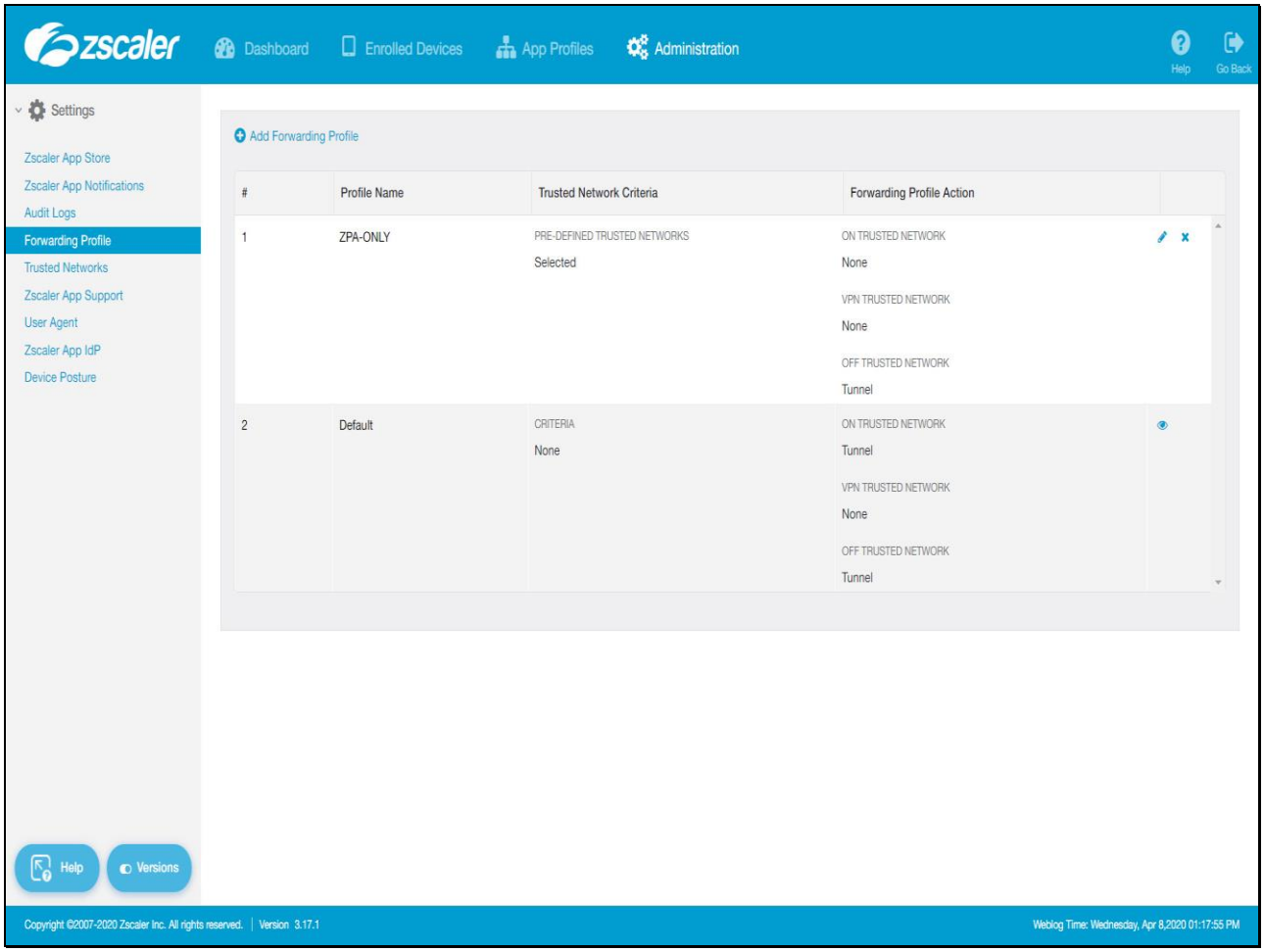
Once the **Forwarding Profile** configuration is complete, click **Save**.

Slide 19 - Slide 19



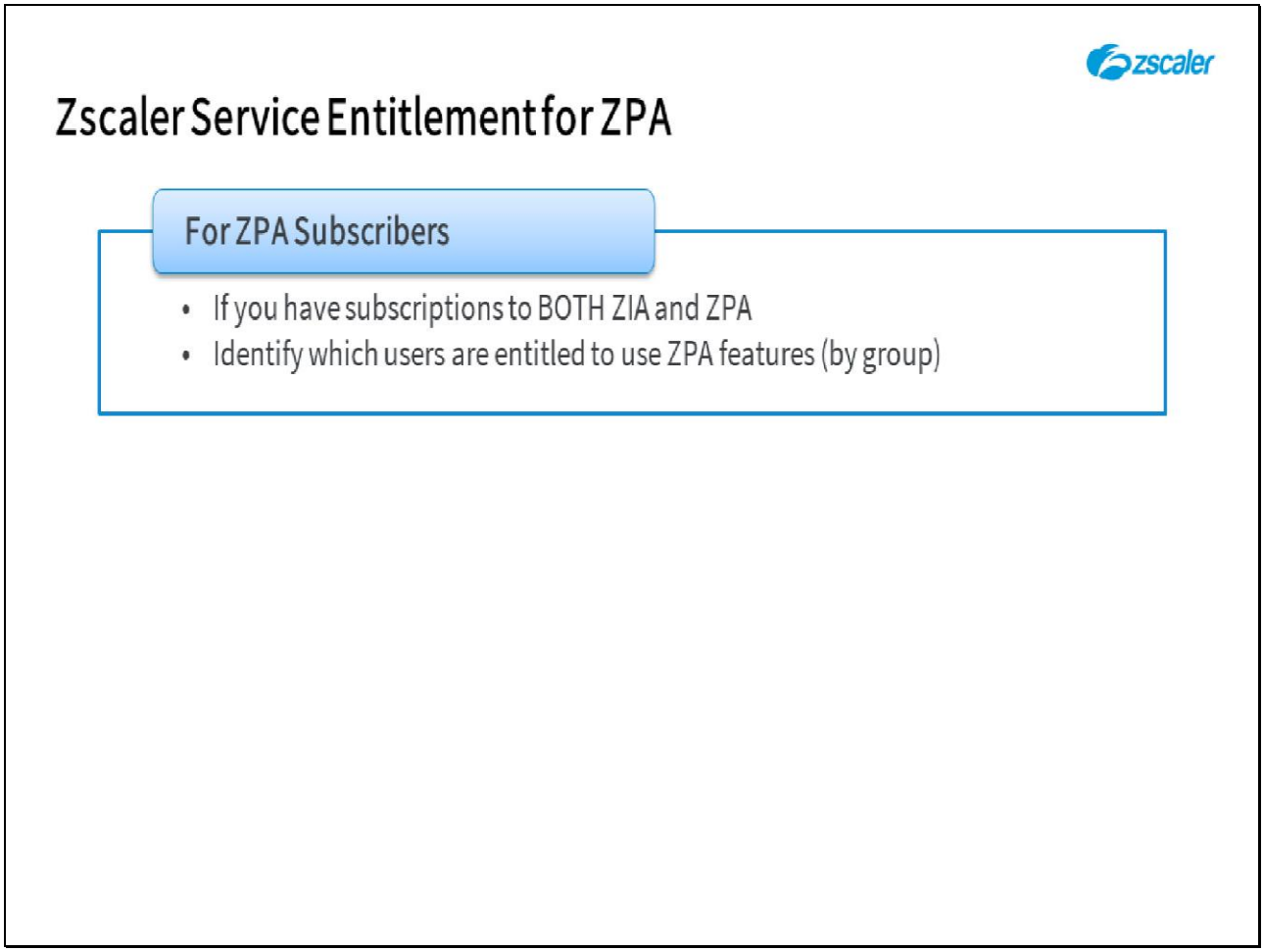
Slide notes

Slide 20 - Slide 20



Slide notes

Slide 21 - Enabling SSL Inspection for Zscaler App Users



Slide notes

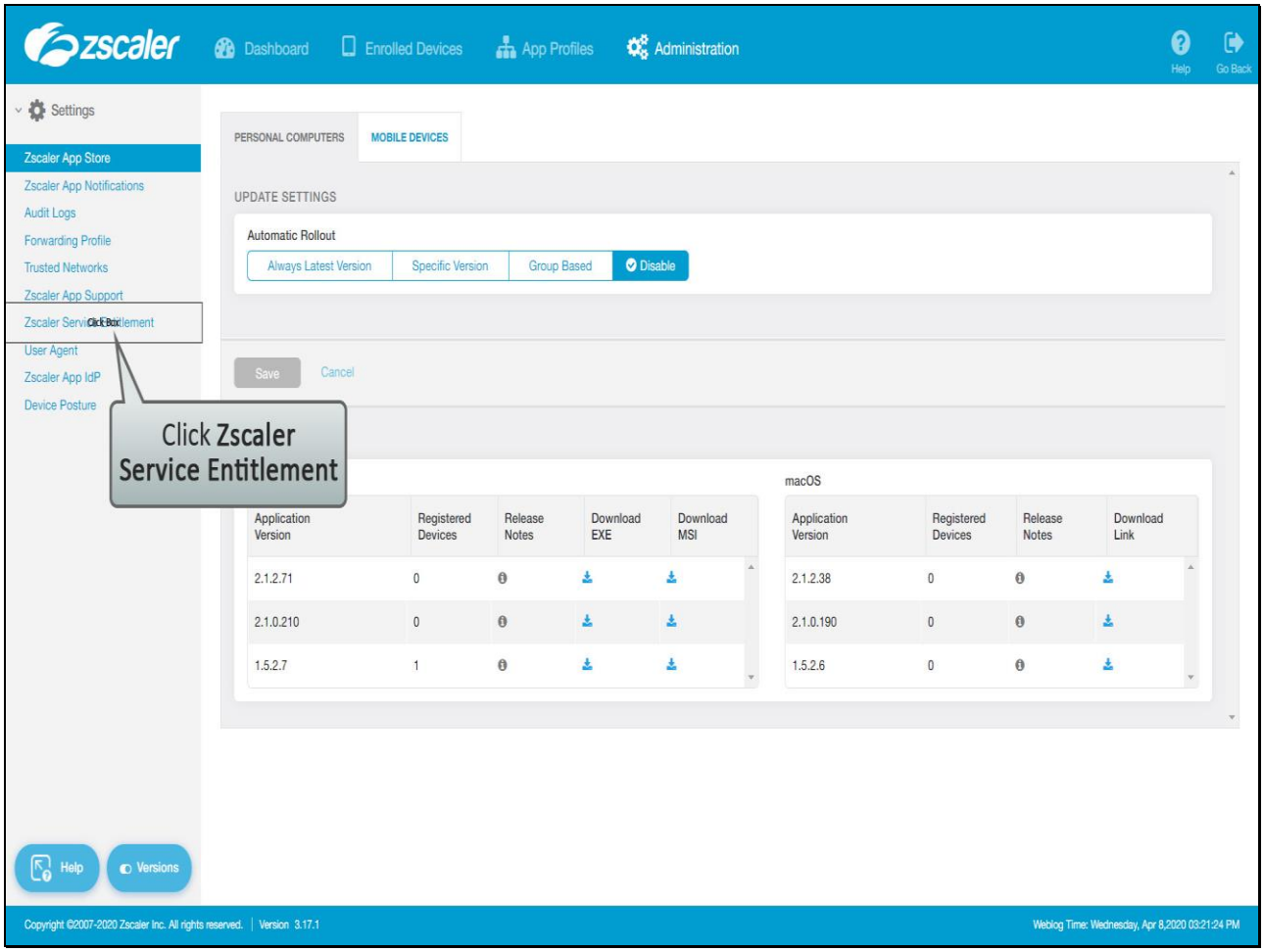
If you subscribe to both the ZIA and ZPA services, but you only want to deploy ZPA to a subset of your users, you can use the **Zscaler Service Entitlement** configuration in the Zscaler App Portal. This feature allows you to select user groups from the ZIA Hosted DB, that are to have ZPA functionality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

Slide 22 - Slide 22

Slide notes

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

Slide 23 - Slide 23

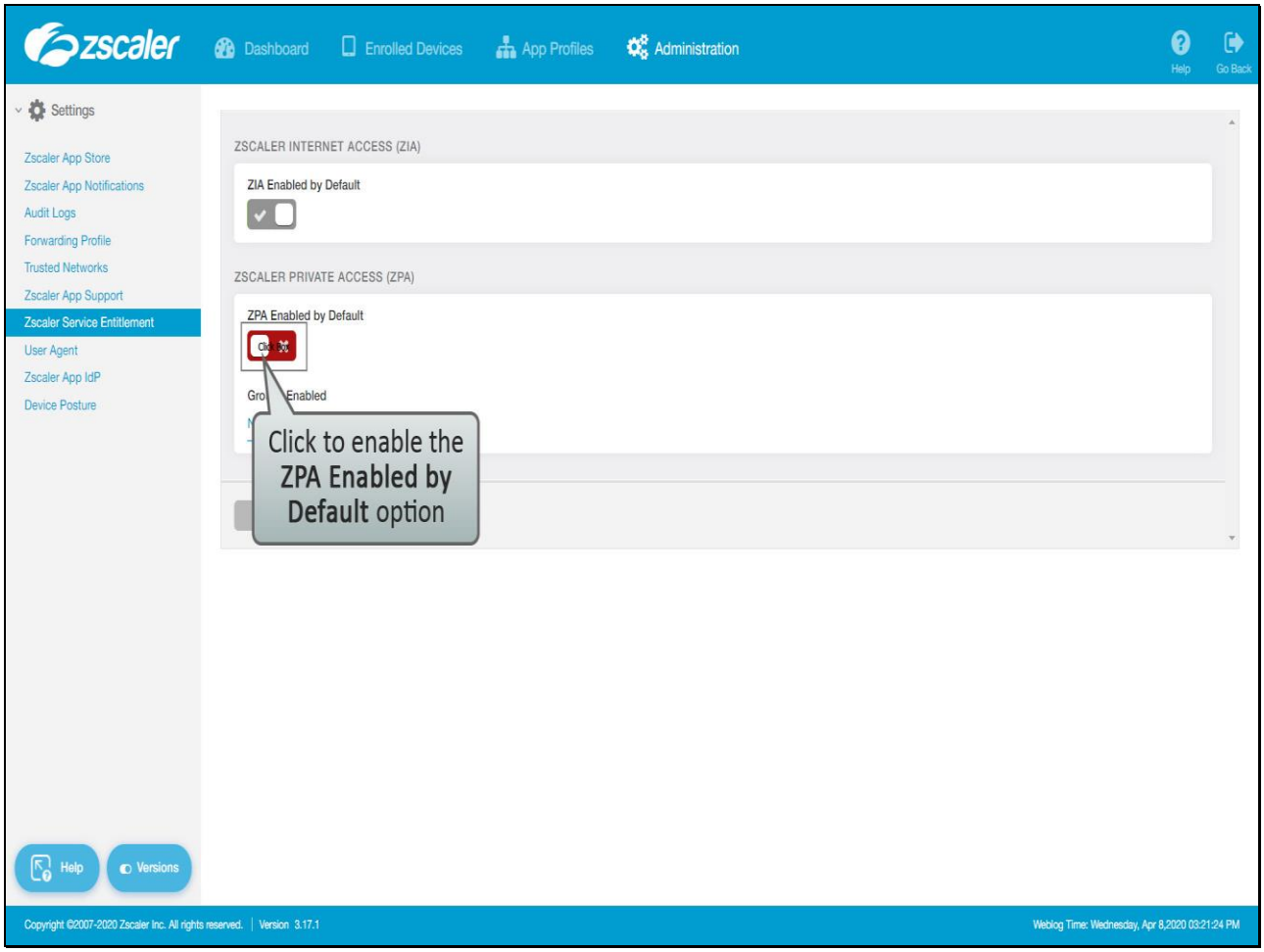


Slide notes

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**.

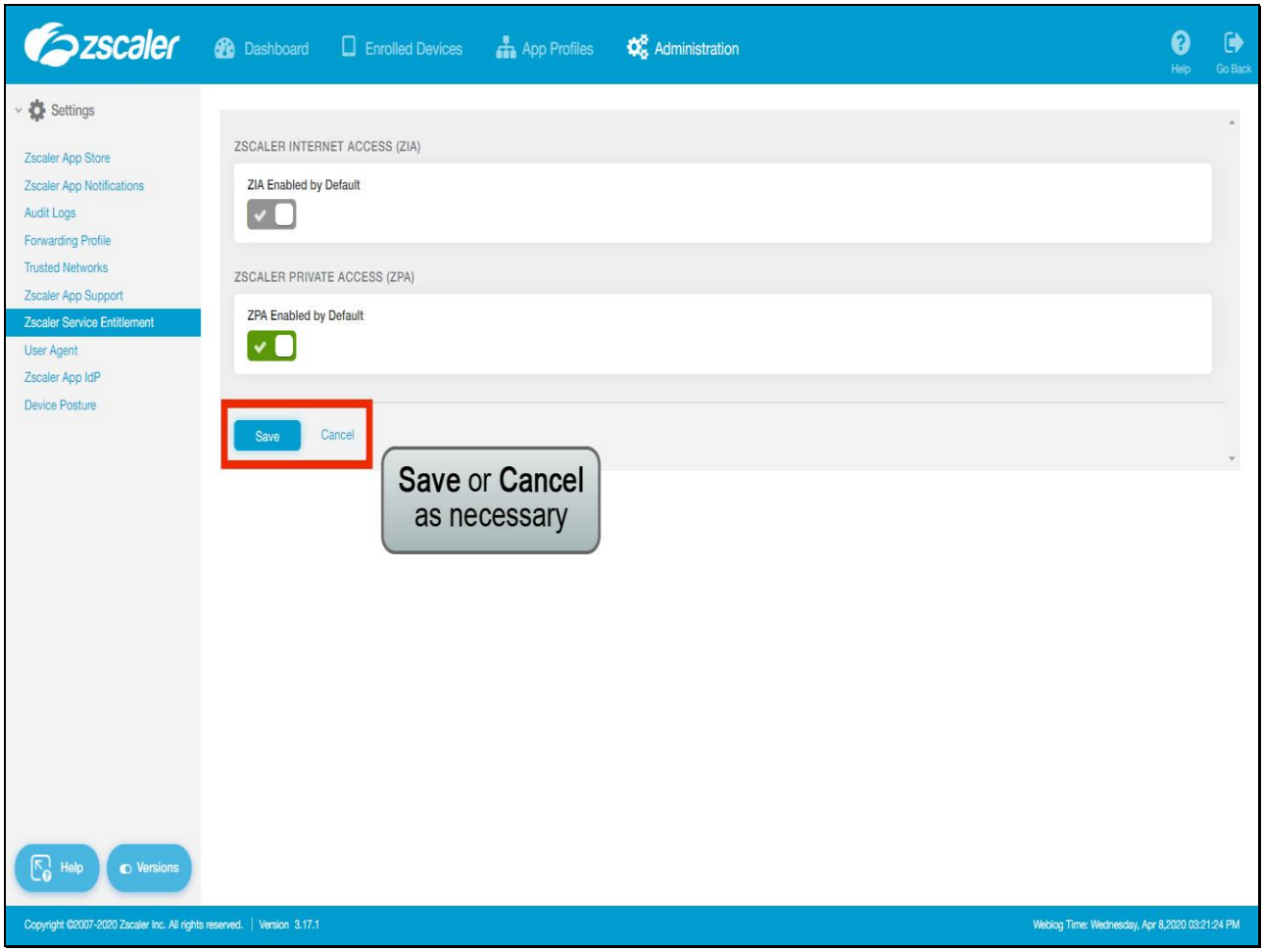
Slide 24 - Slide 24



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.

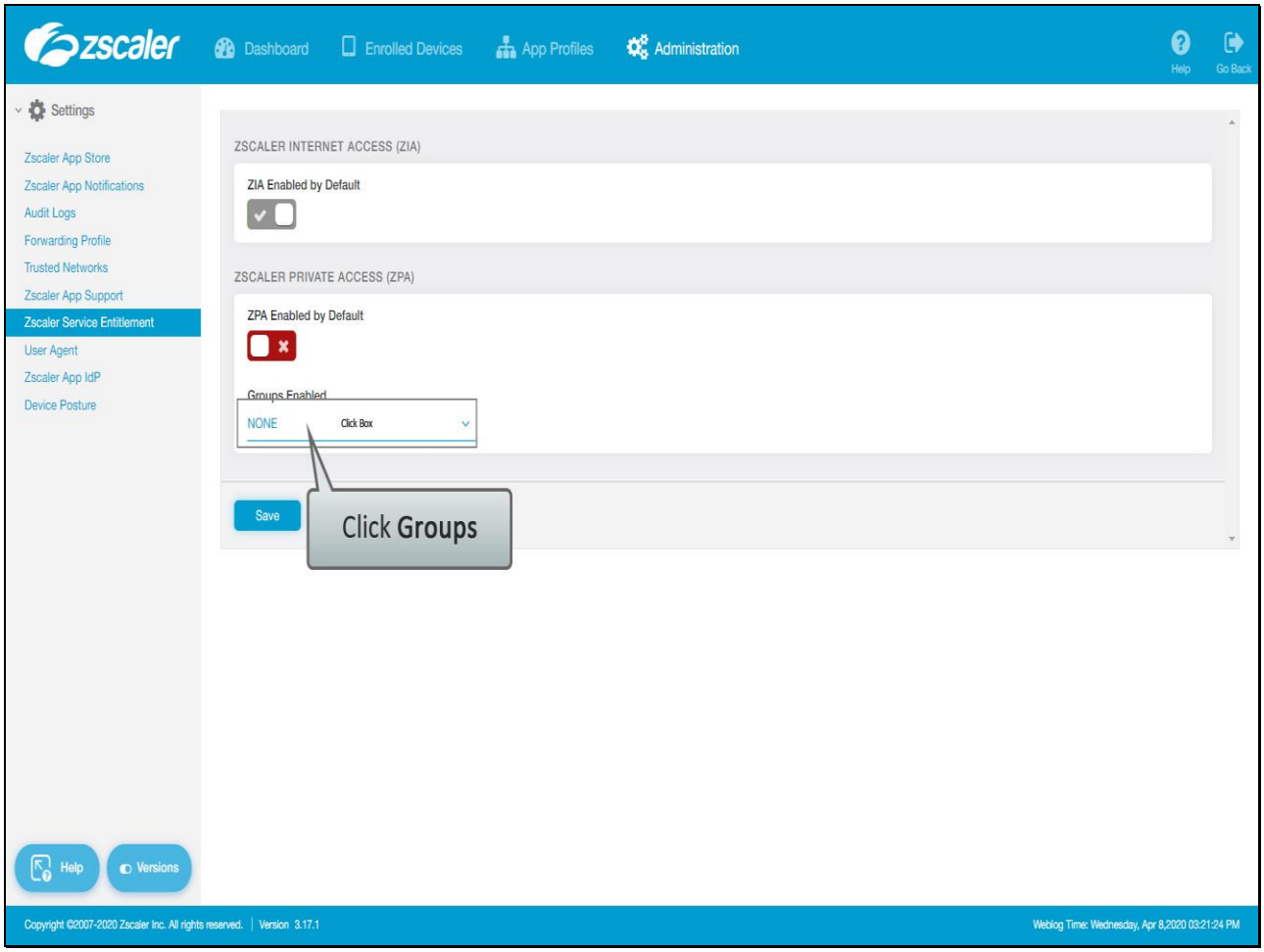
Slide 25 - Slide 25



Slide notes

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

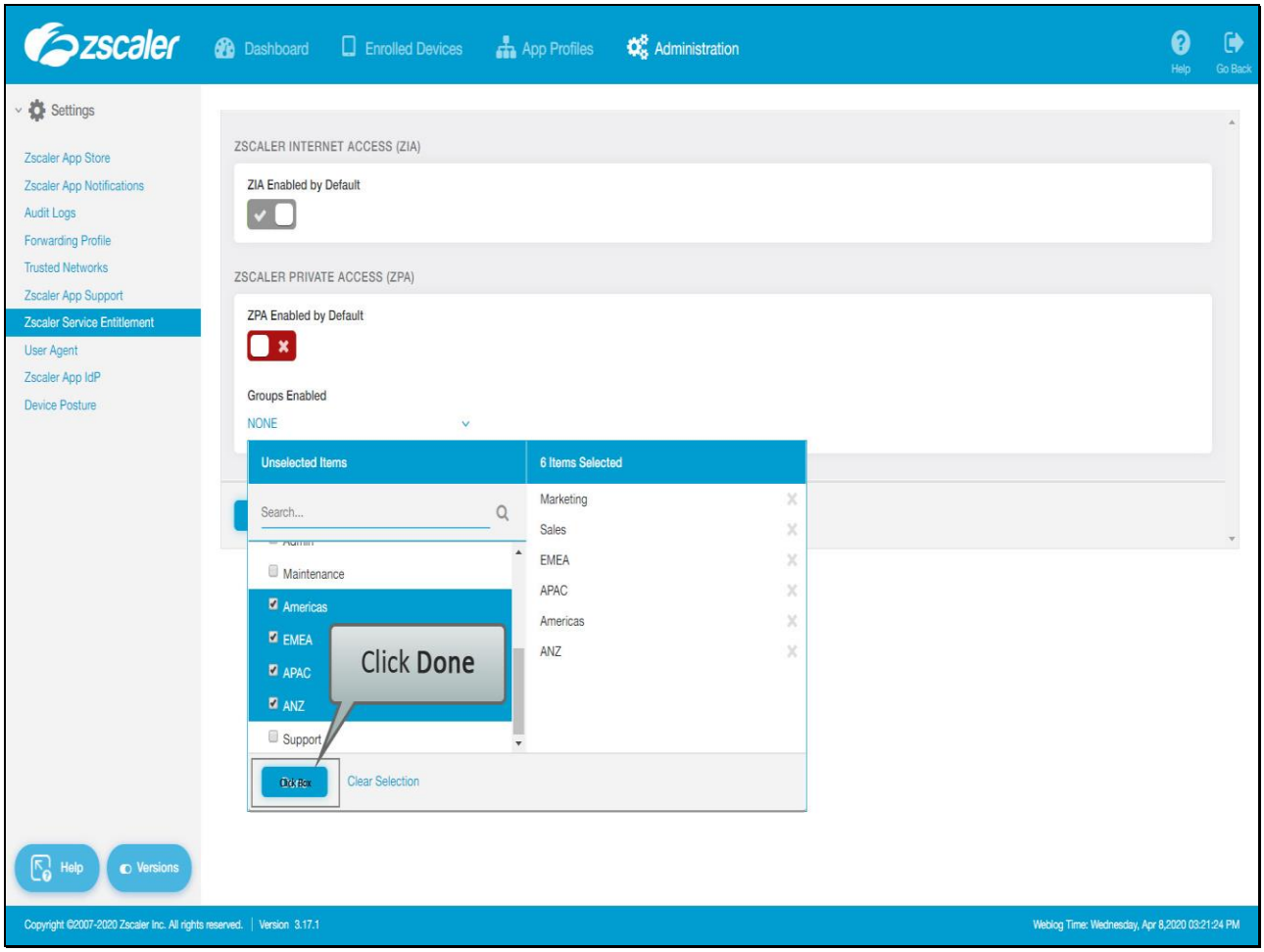
Slide 26 - Slide 26



Slide notes

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

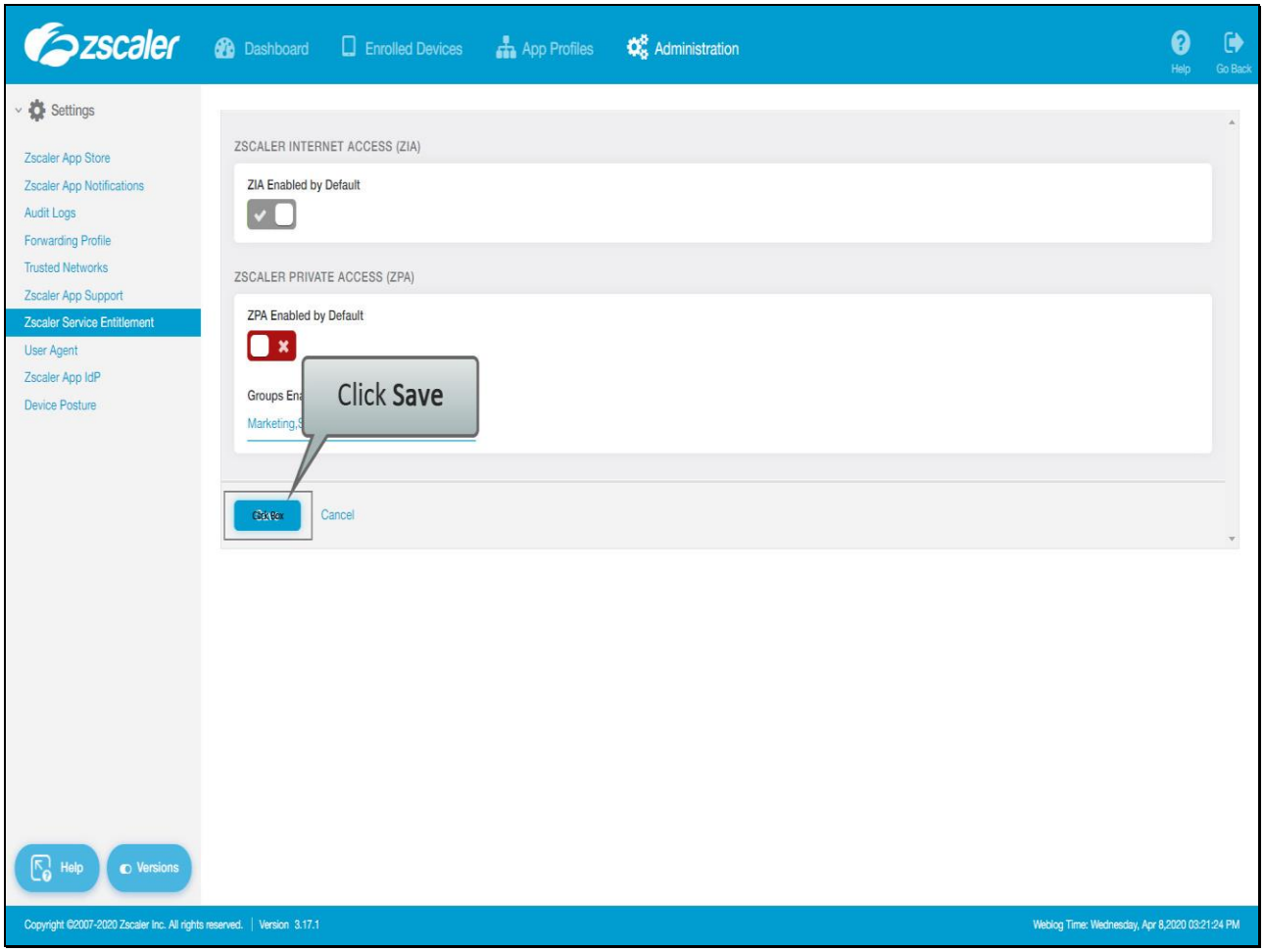
Slide 27 - Slide 27



Slide notes

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

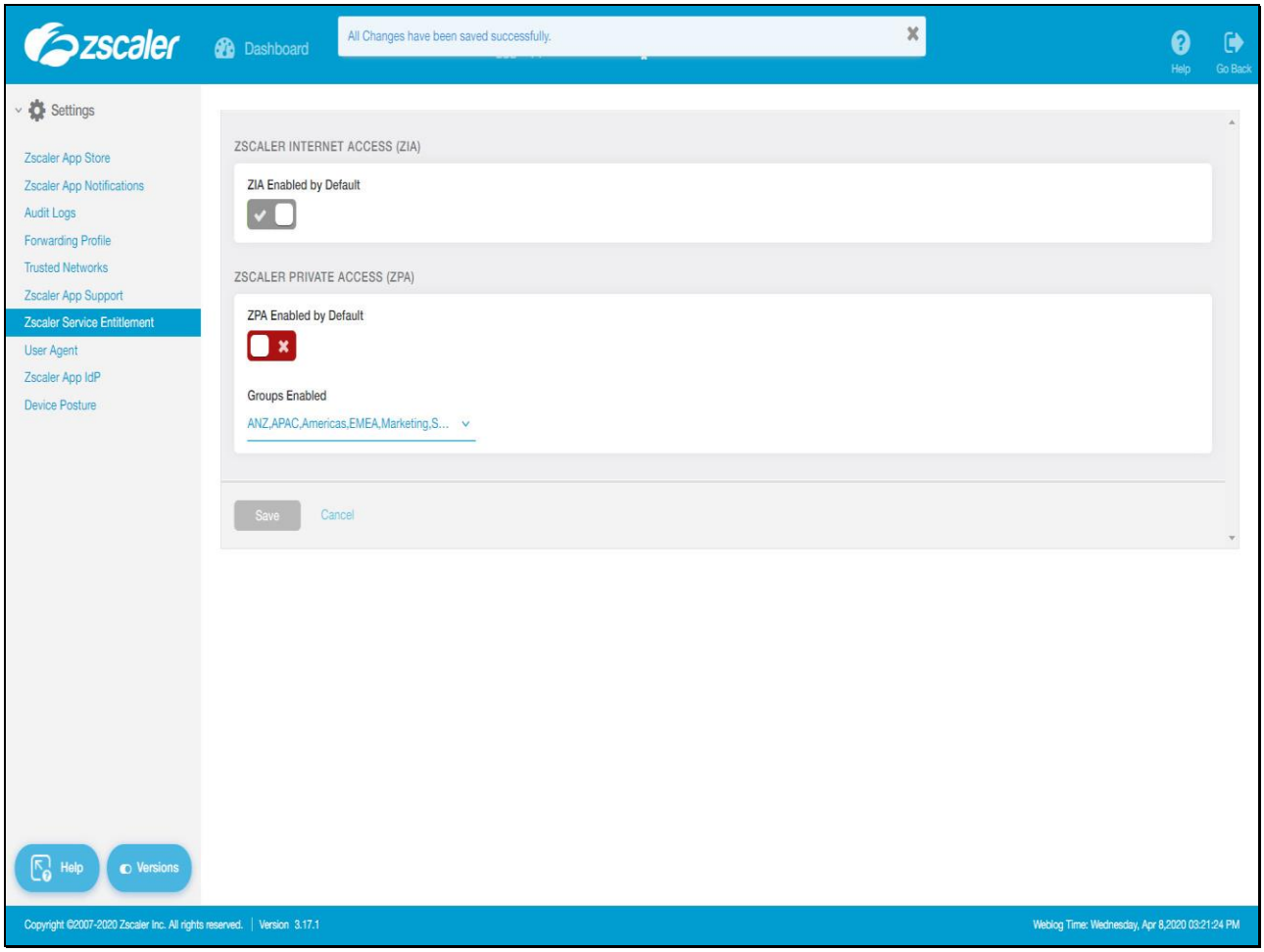
Slide 28 - Slide 28



Slide notes

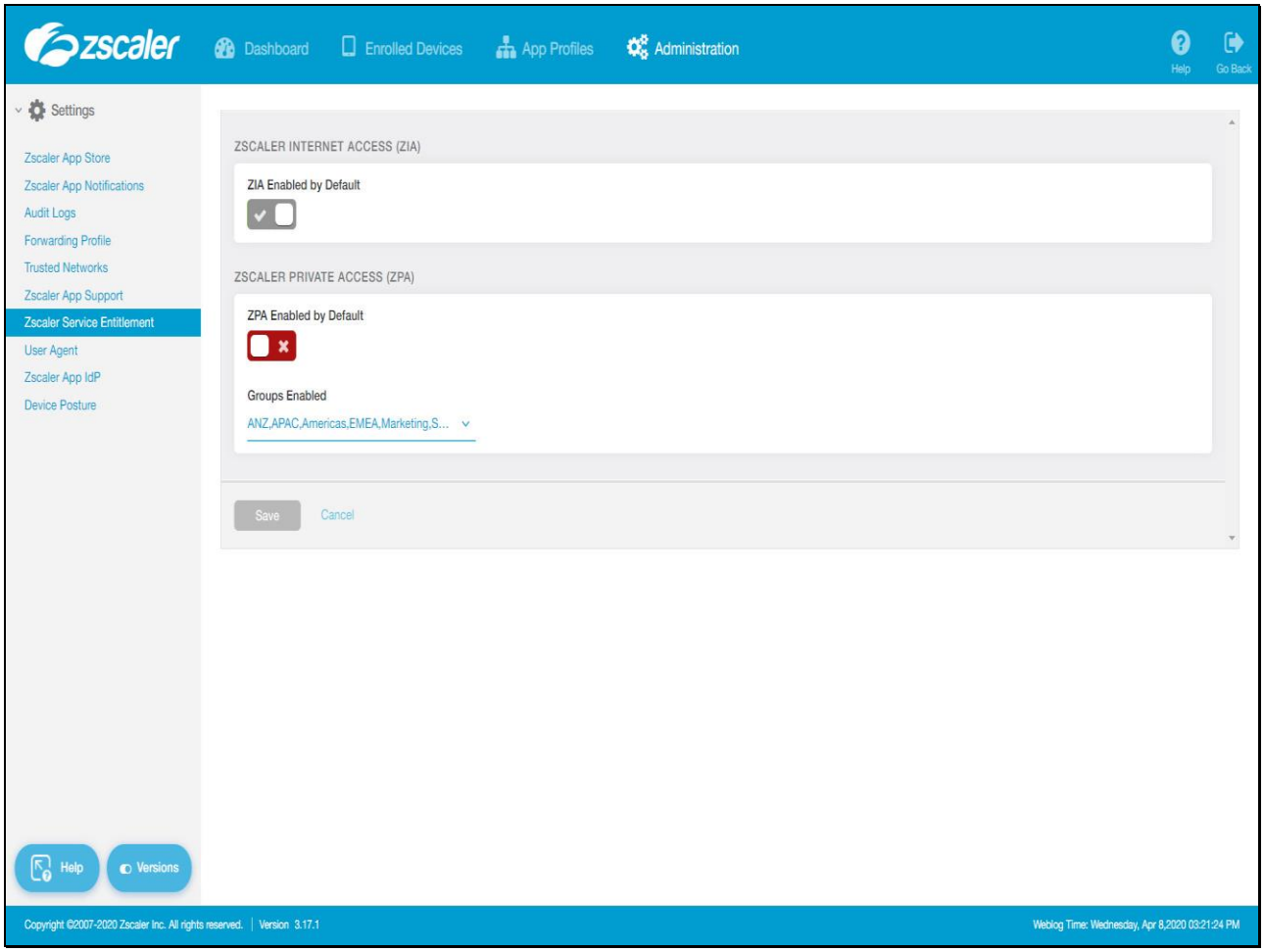
...then click **Save**.

Slide 29 - Slide 29



Slide notes

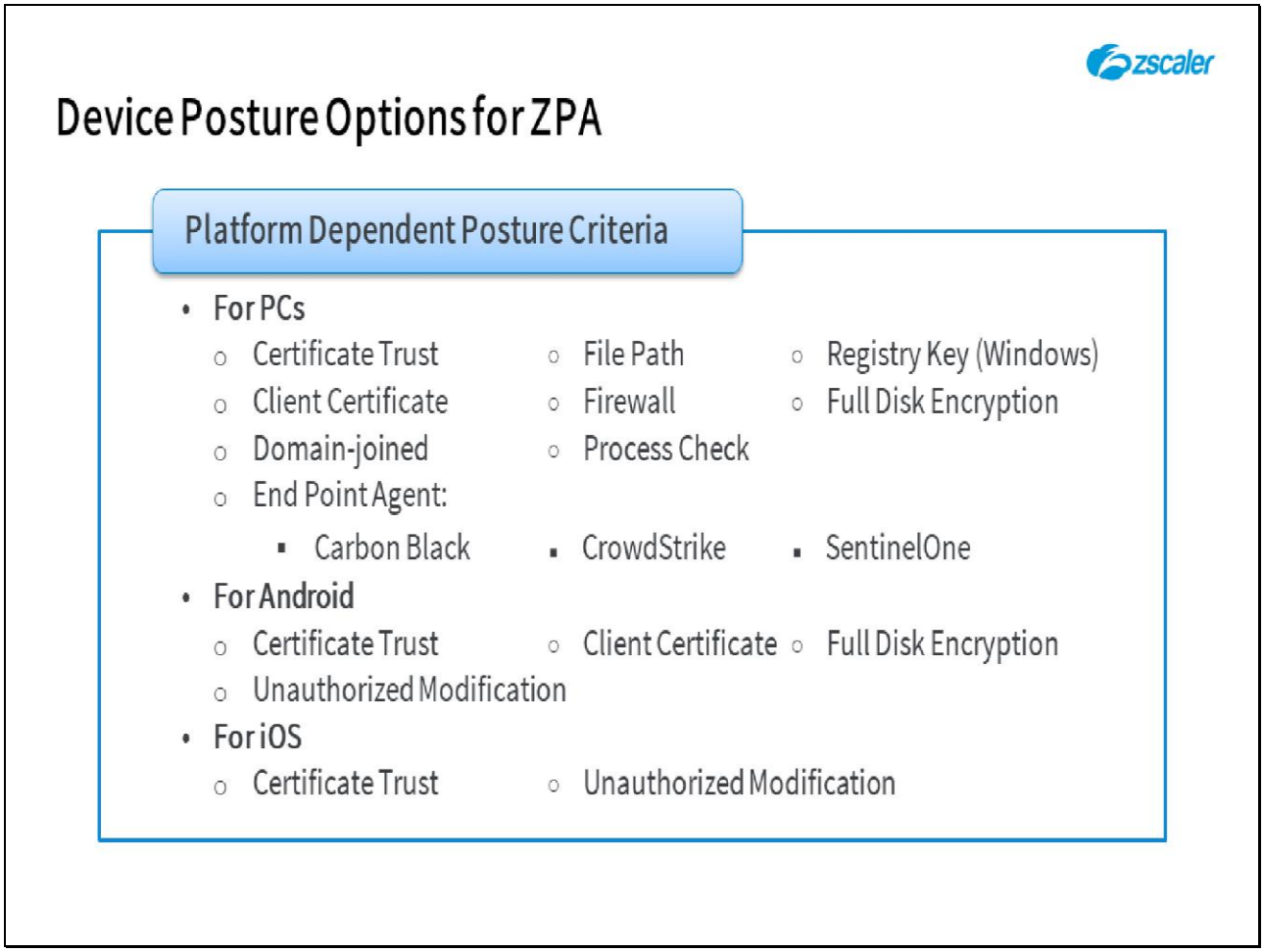
Slide 30 - Slide 30



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

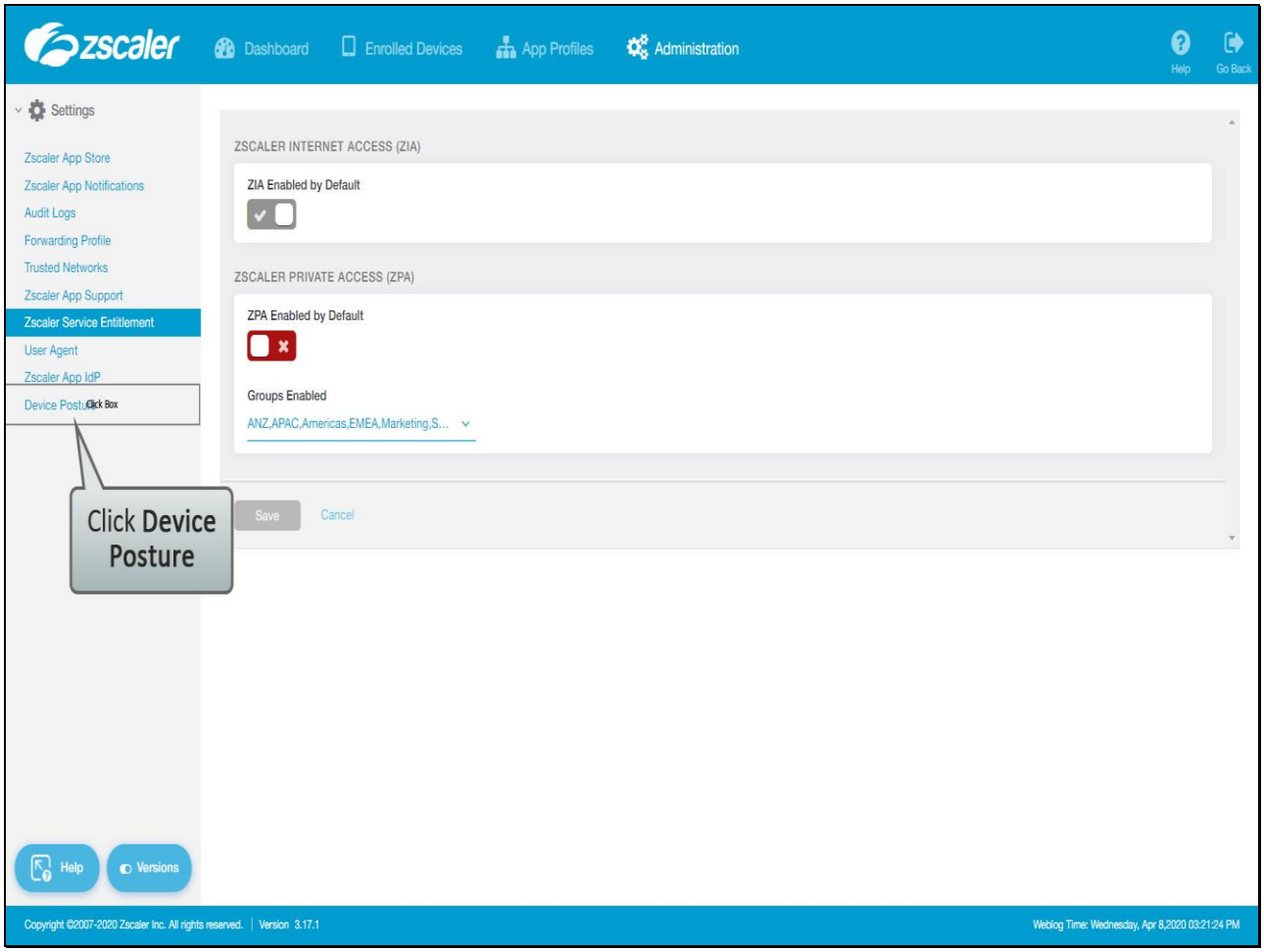


Slide notes

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

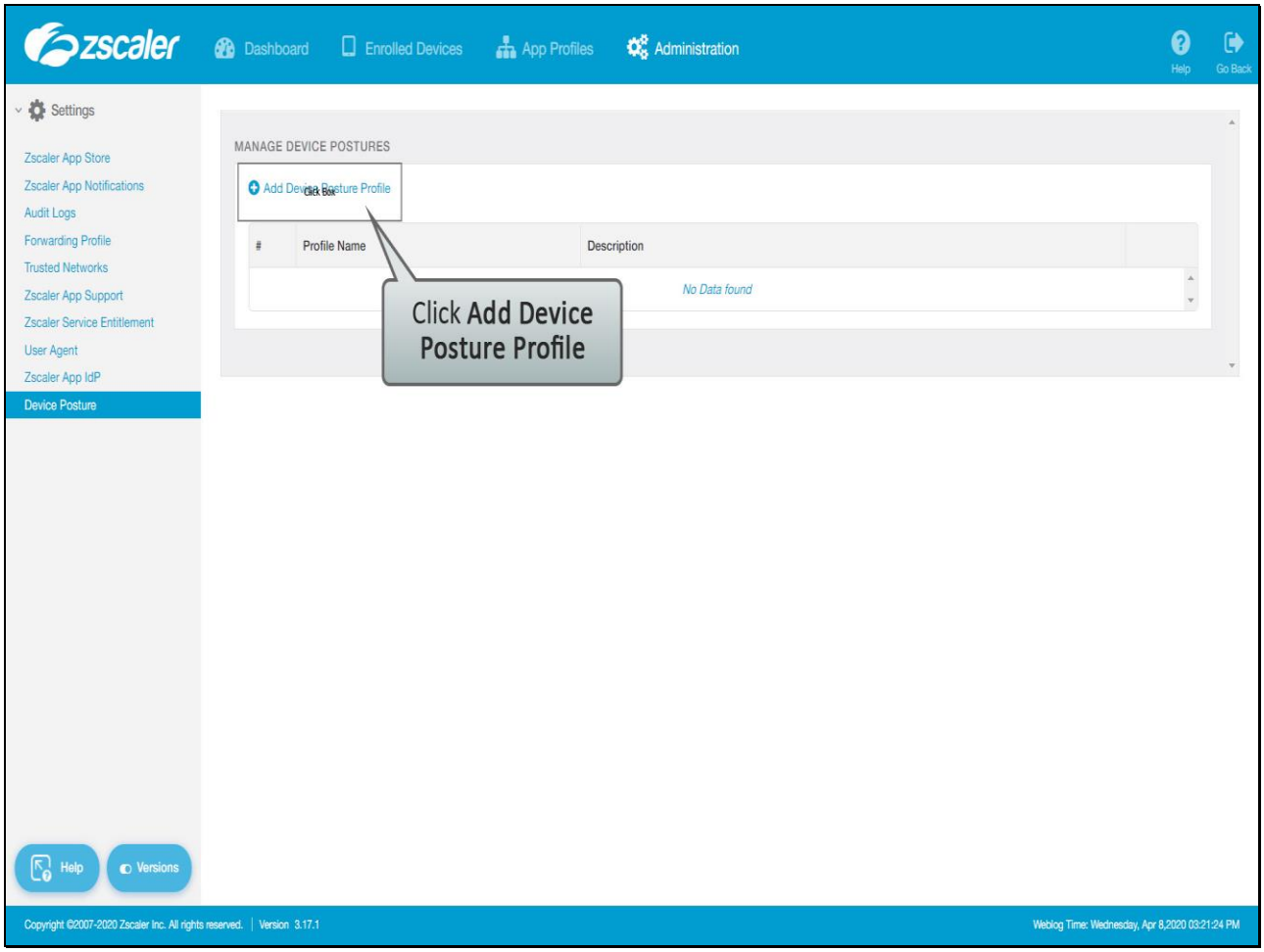


Slide notes

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

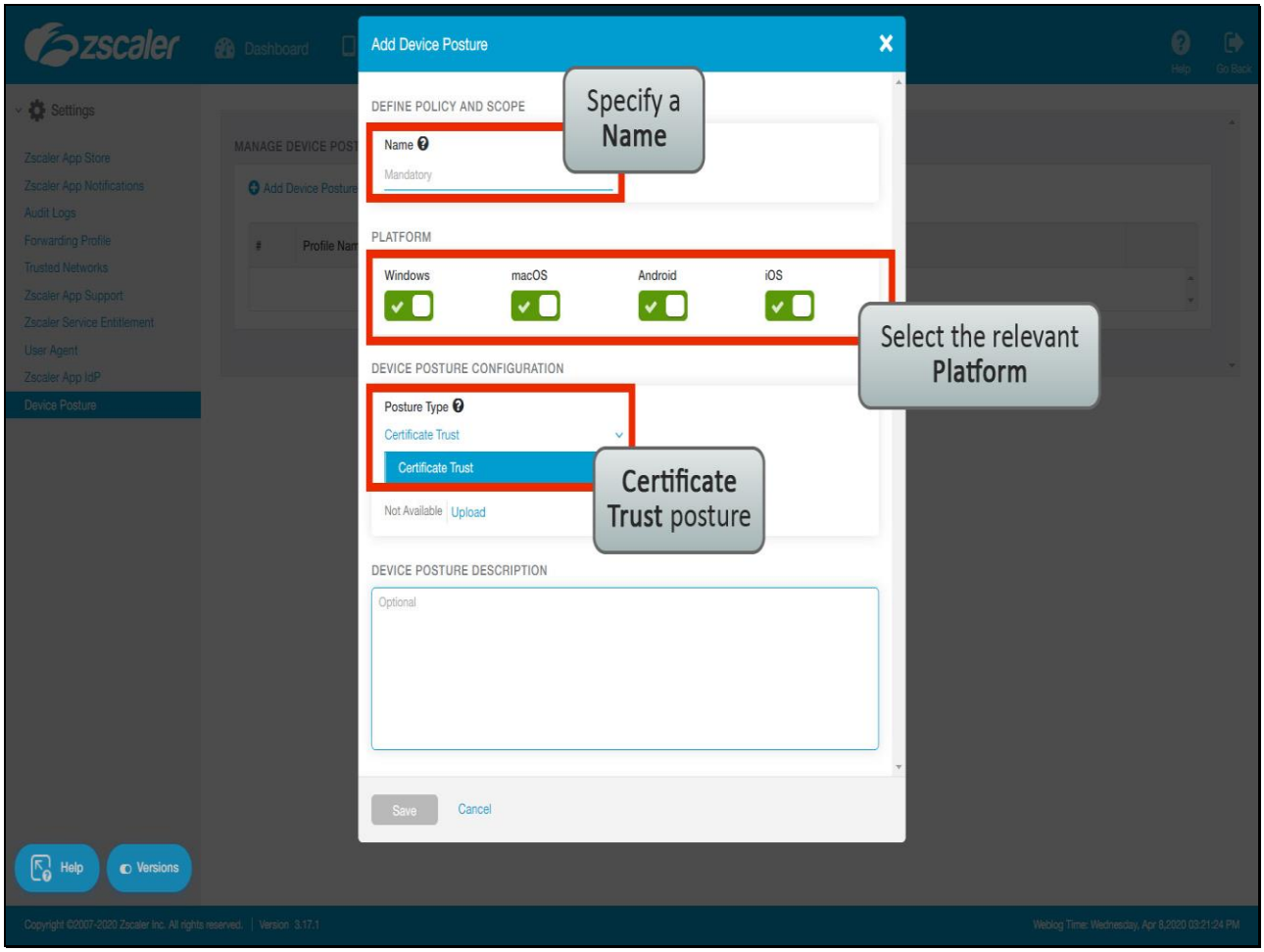


Slide notes

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



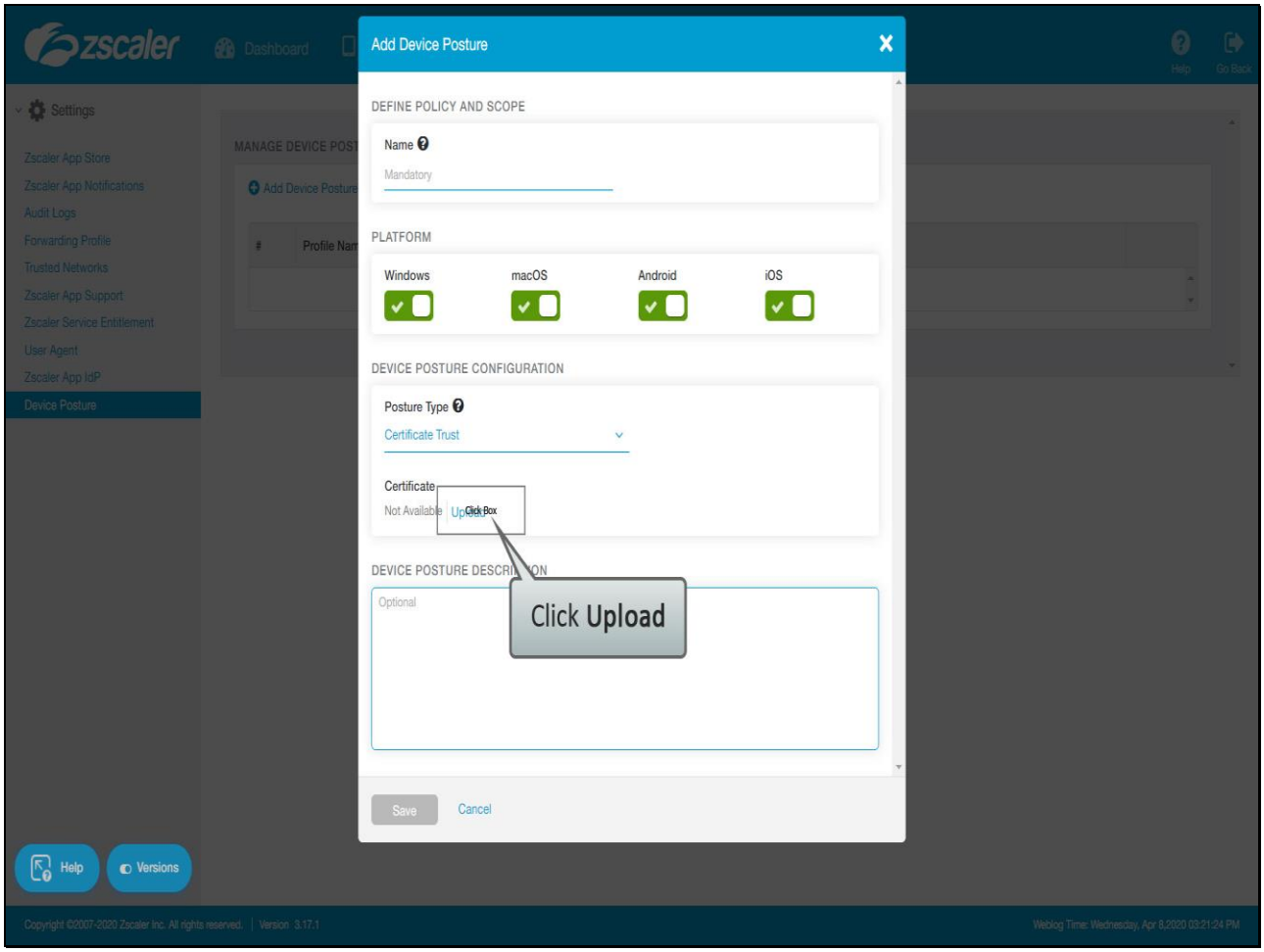
Slide notes

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.

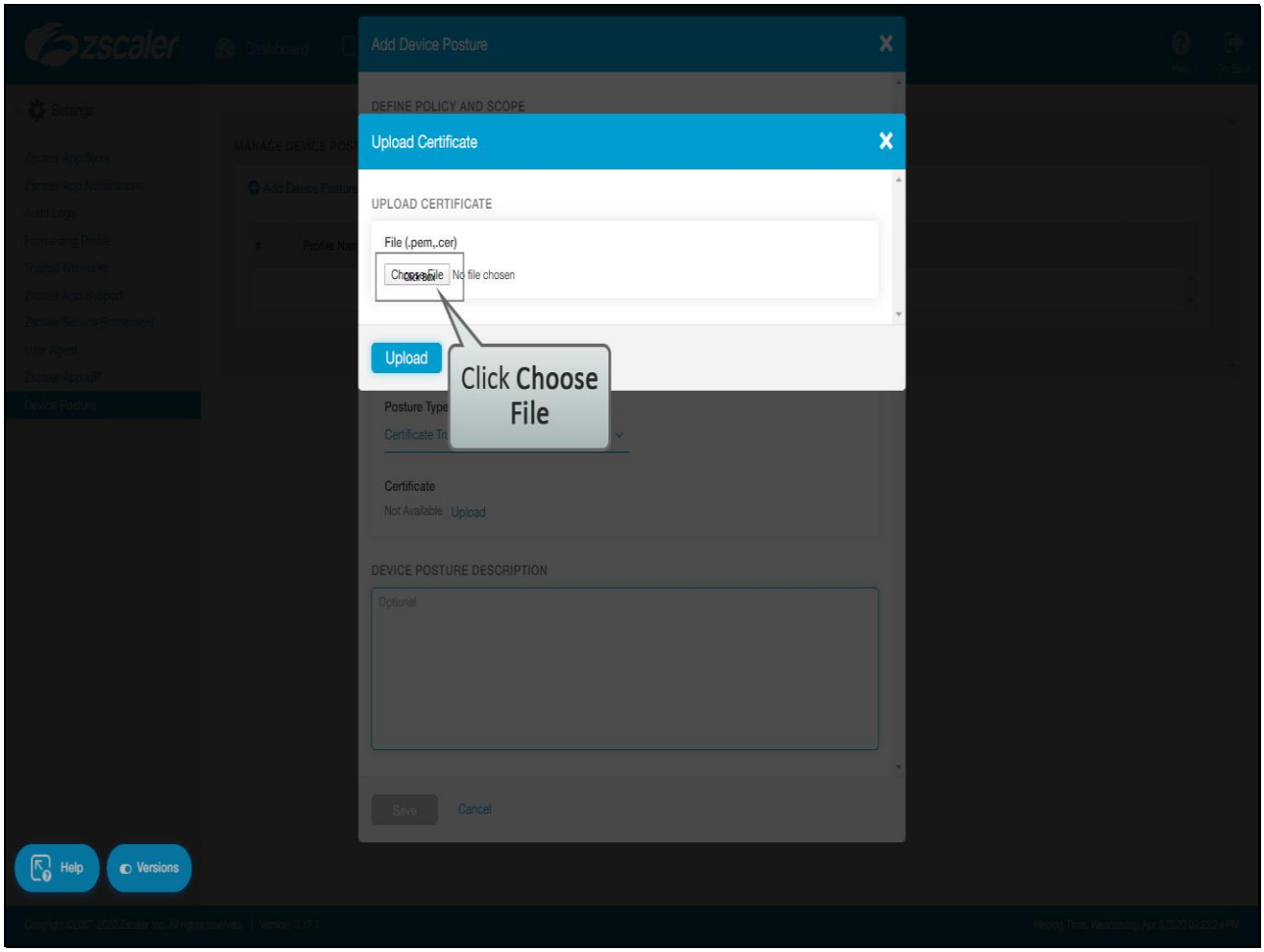
Slide 35 - Slide 35



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, ...

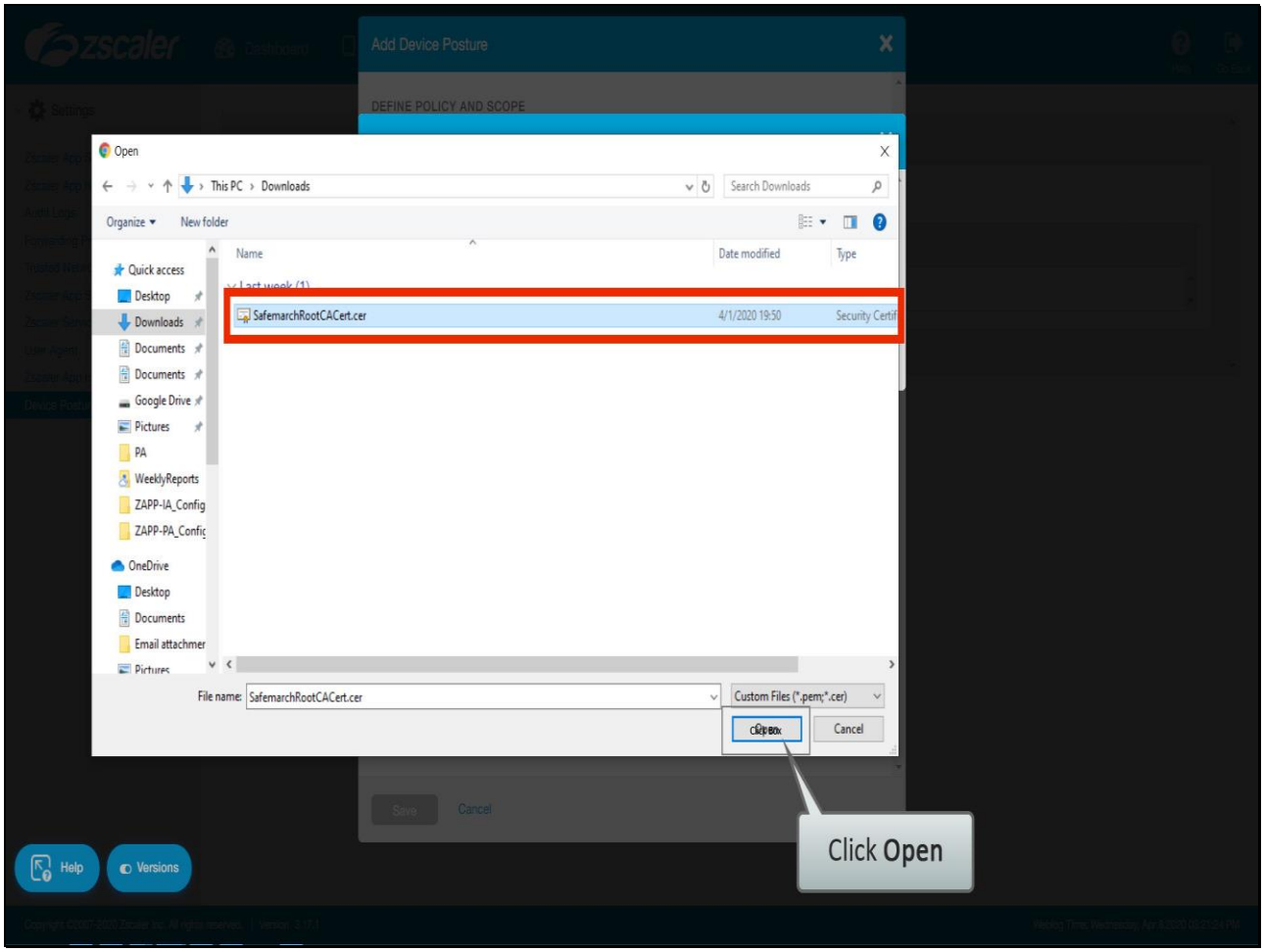
Slide 36 - Slide 36



Slide notes

...then click **Choose File**, ...

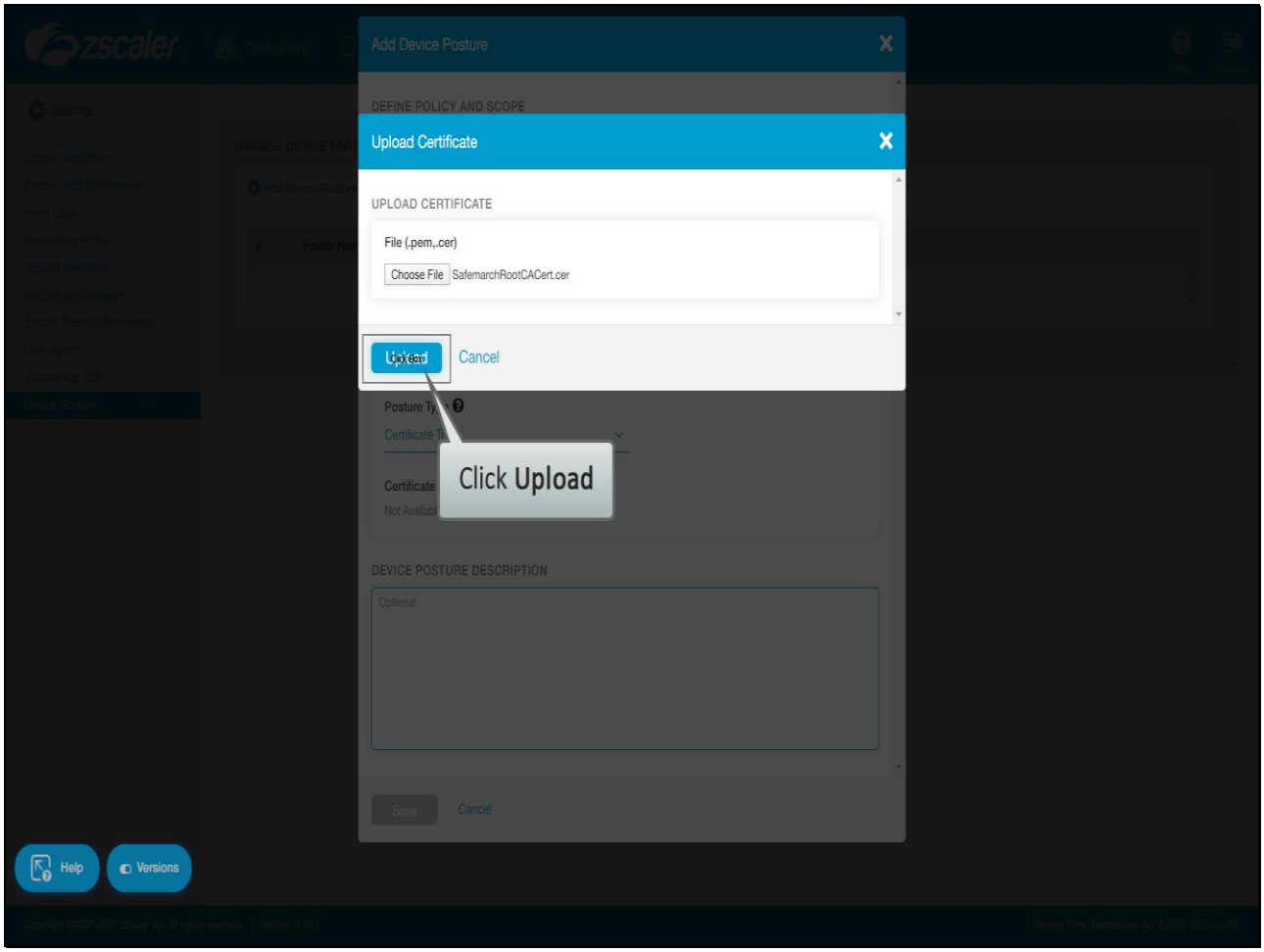
Slide 37 - Slide 37



Slide notes

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

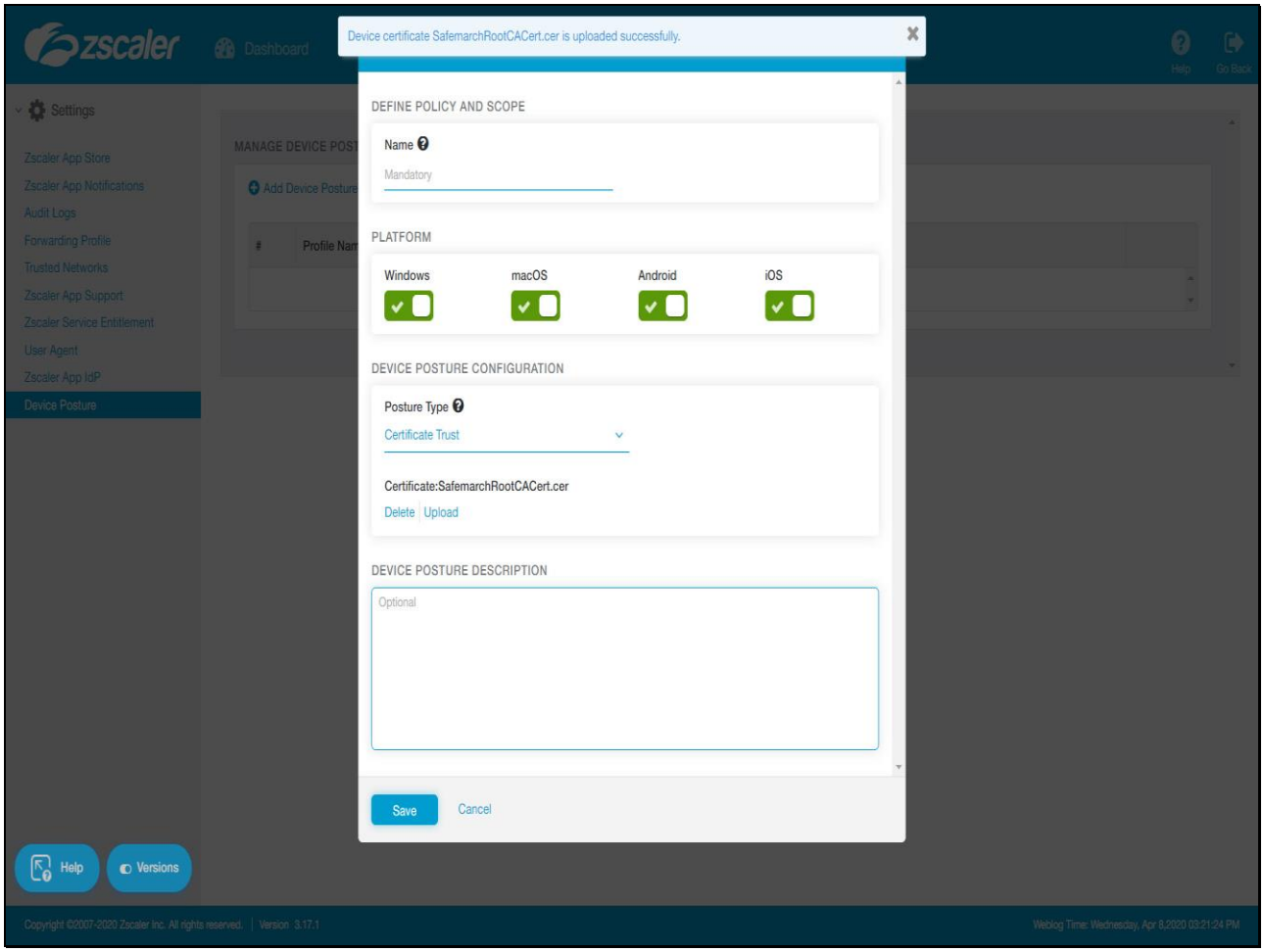
Slide 38 - Slide 38



Slide notes

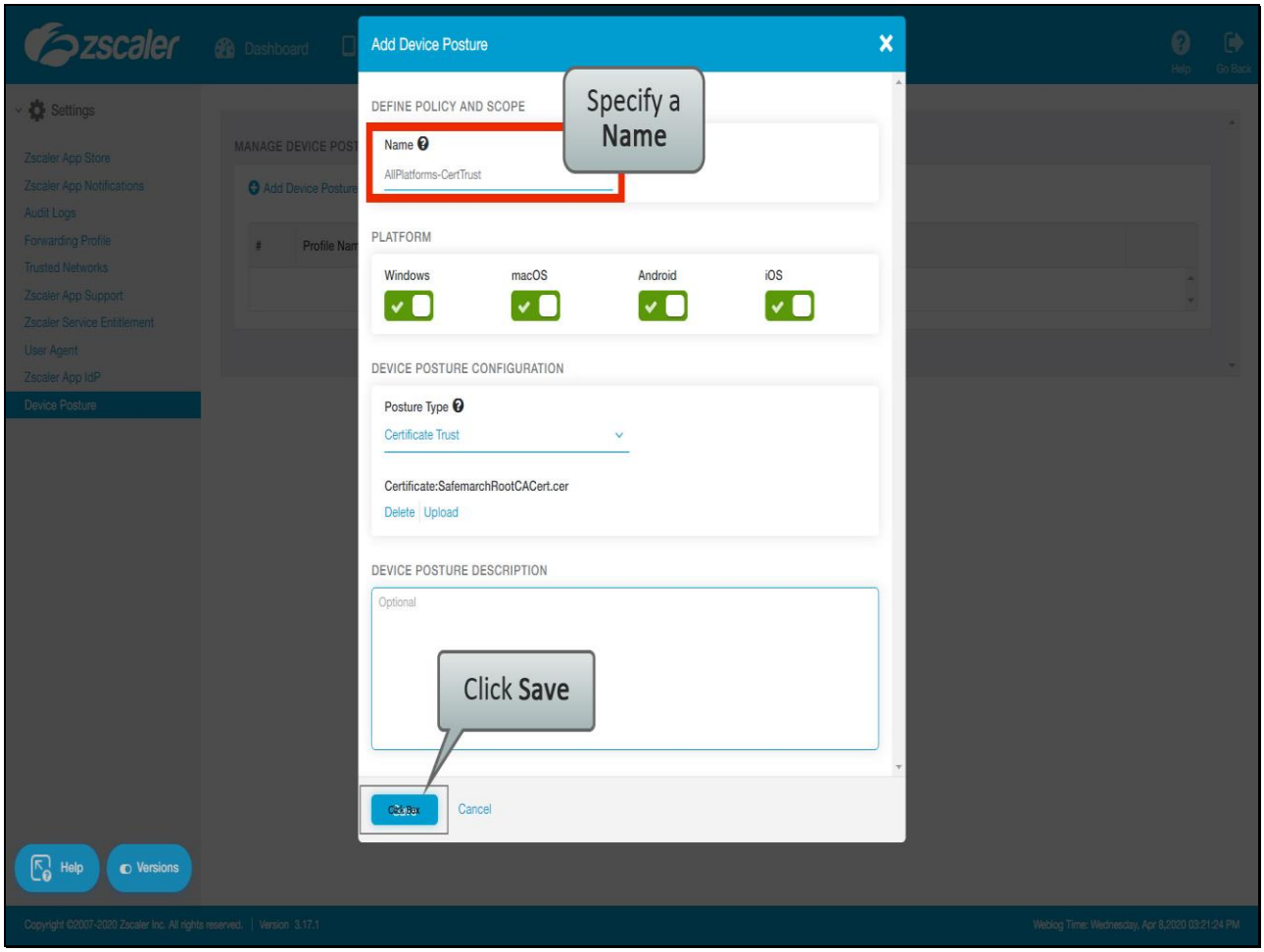
…then click **Upload**.

Slide 39 - Slide 39



Slide notes

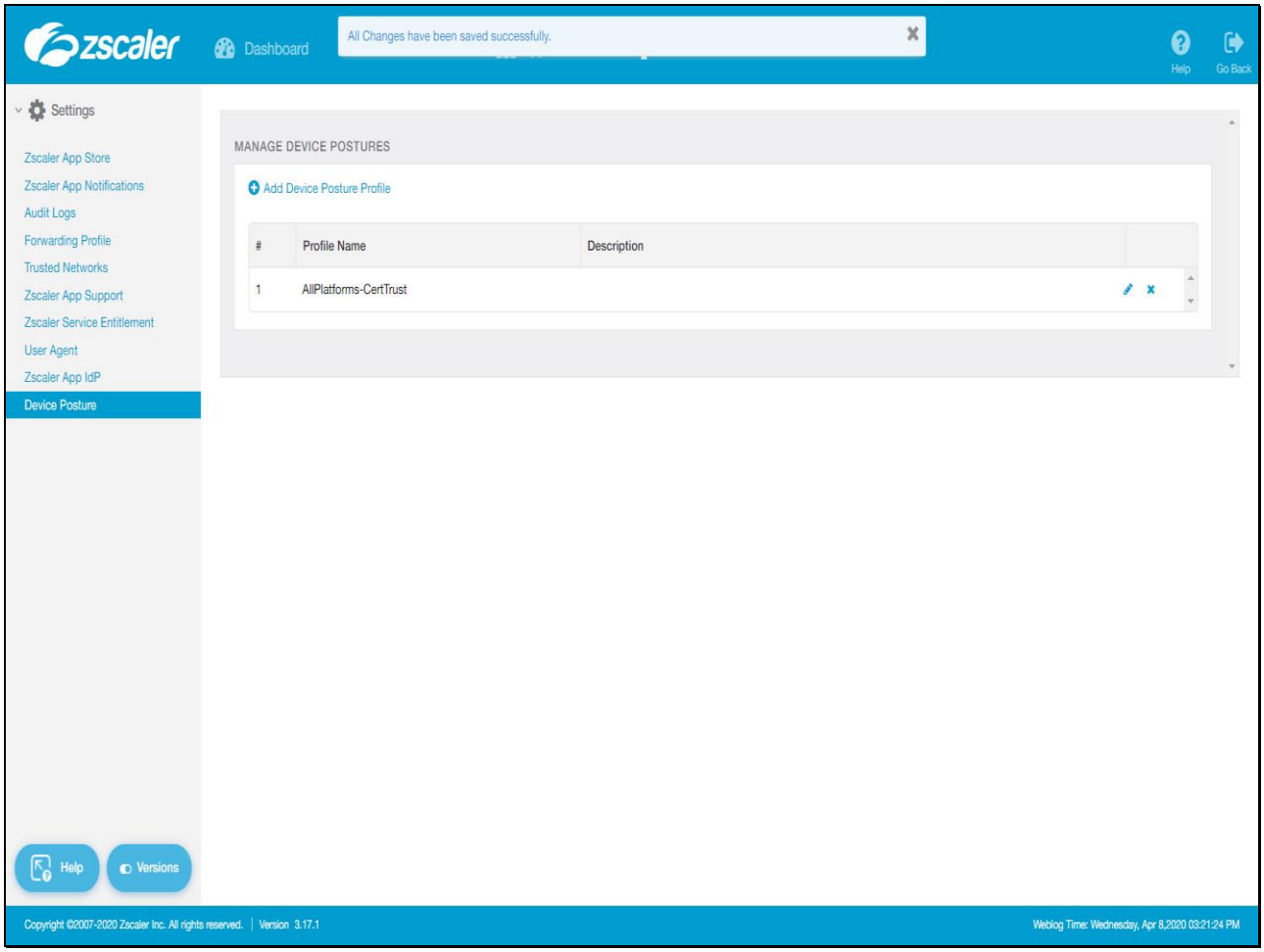
Slide 40 - Slide 40



Slide notes

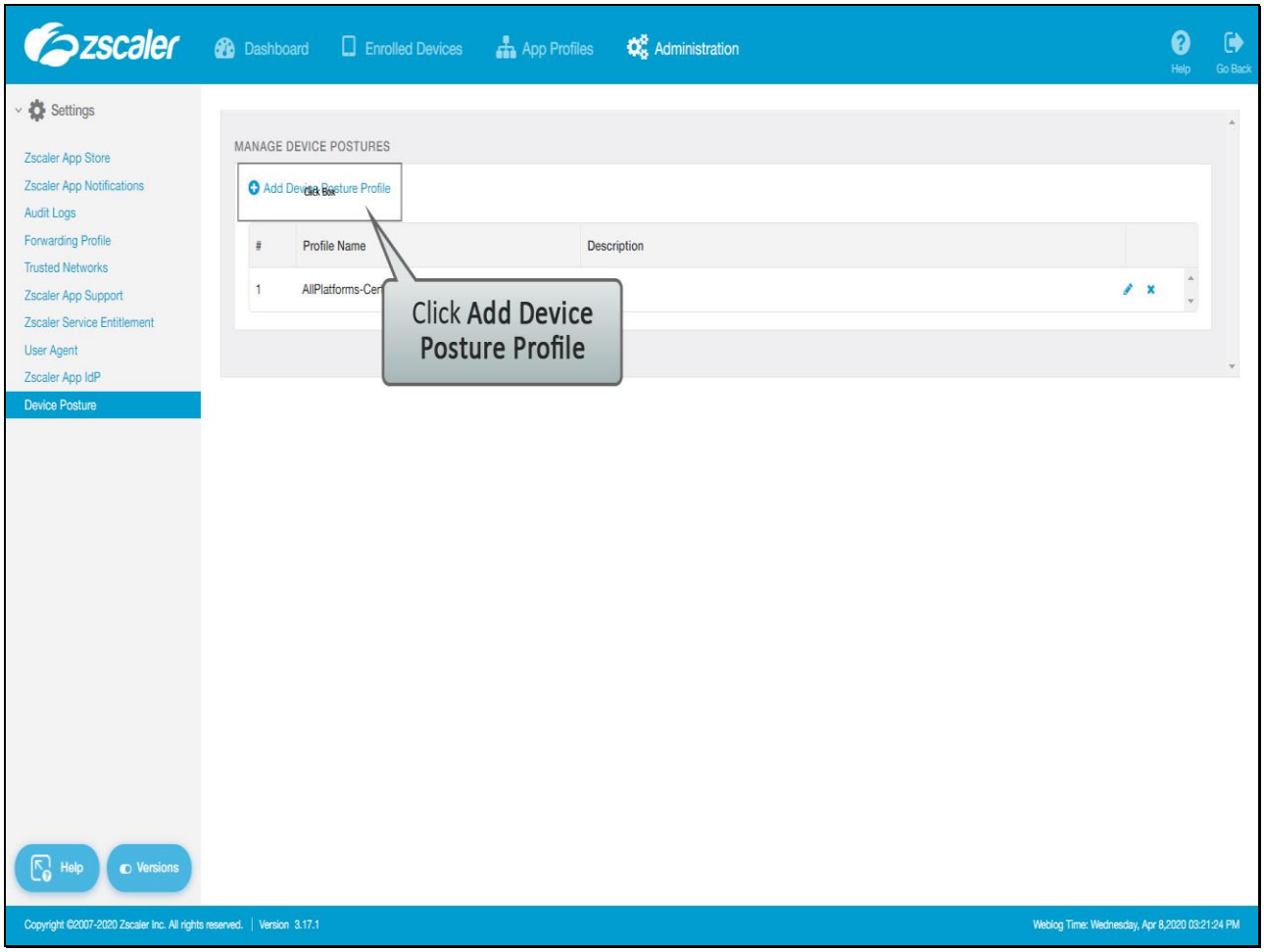
Once the condition is correctly configured, click **Save**.

Slide 41 - Slide 41



Slide notes

Slide 42 - Slide 42

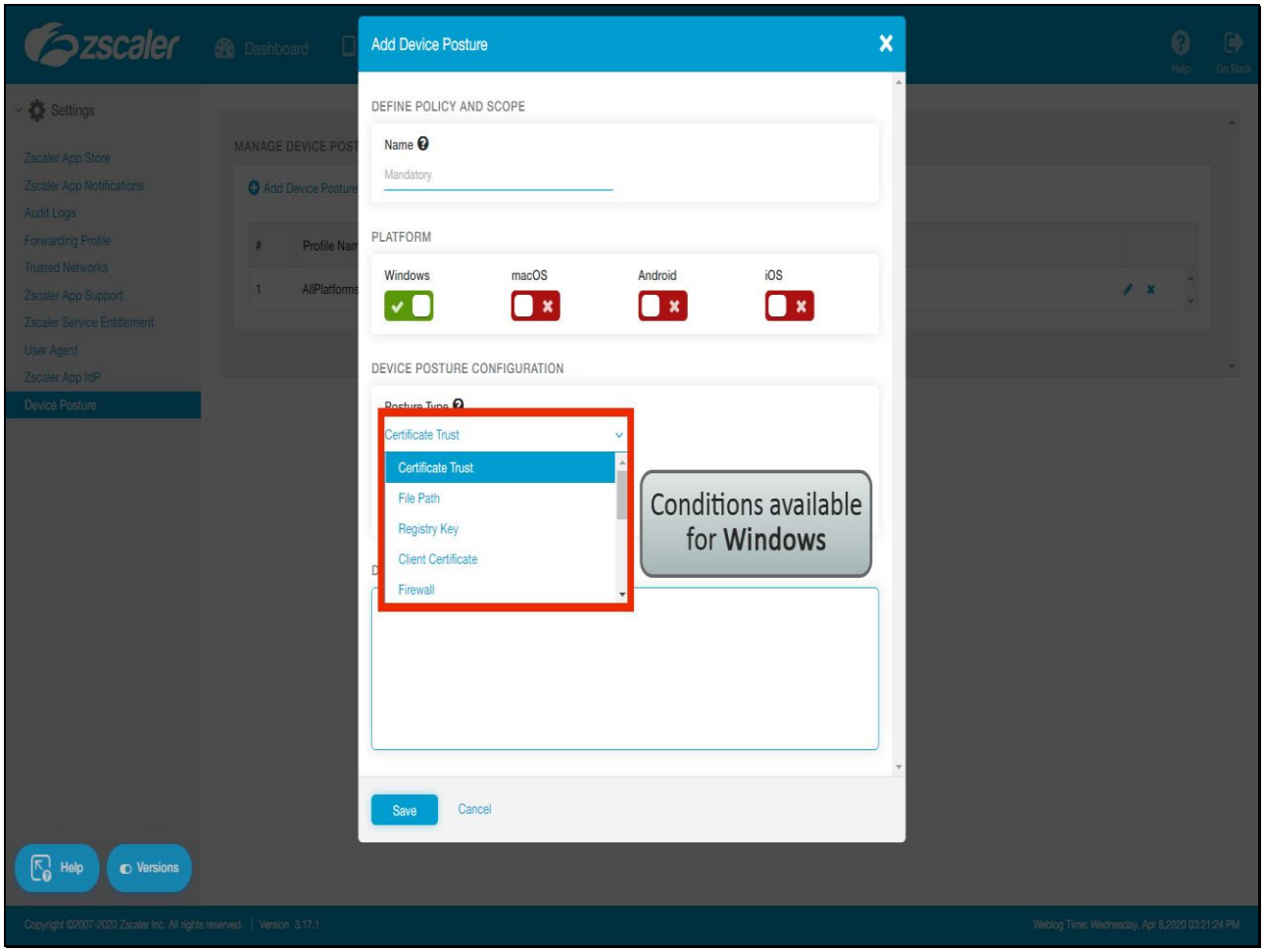


Slide notes

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

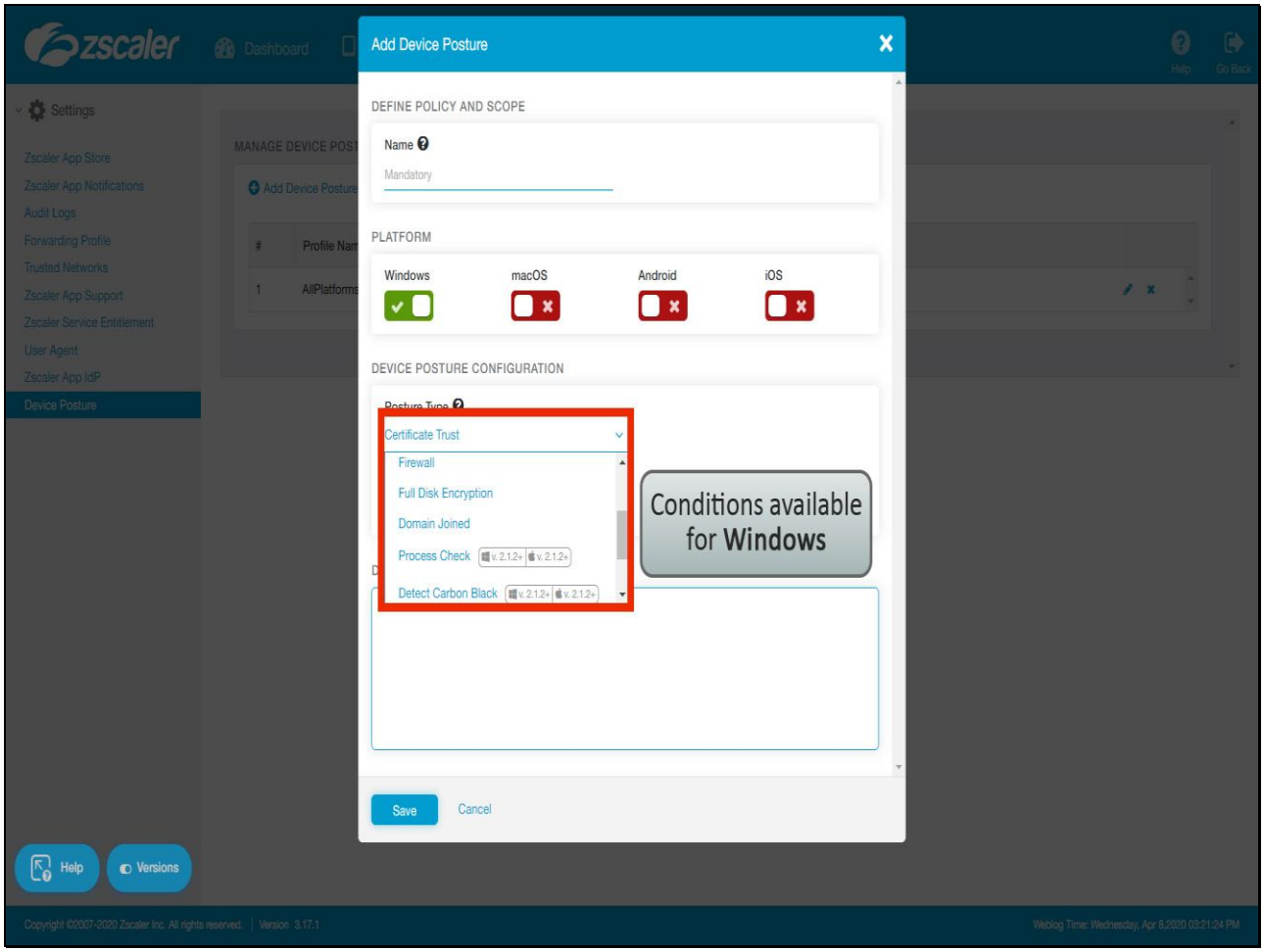


Slide notes

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;

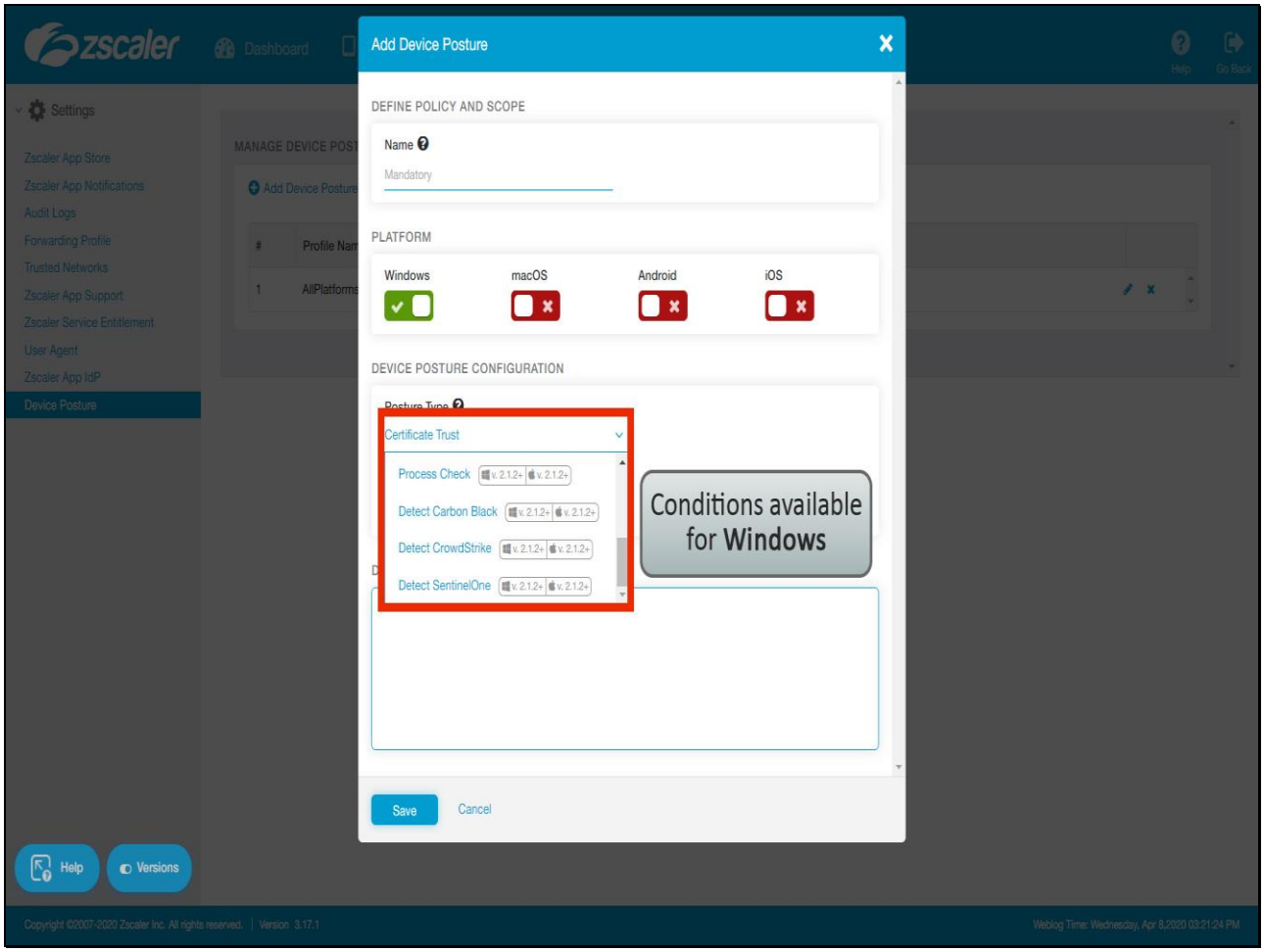
Slide 44 - Slide 44



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;

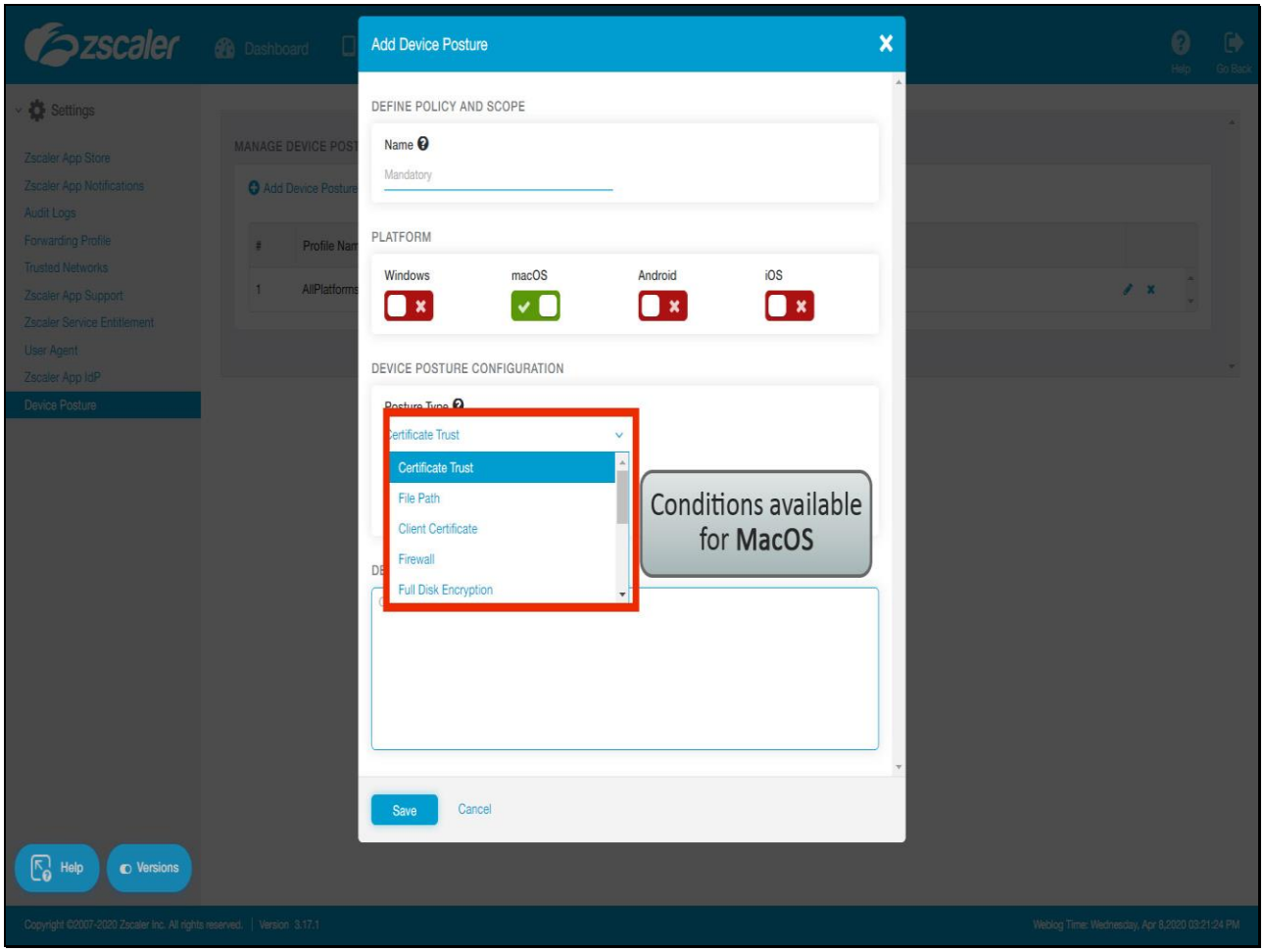
Slide 45 - Slide 45



Slide notes

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

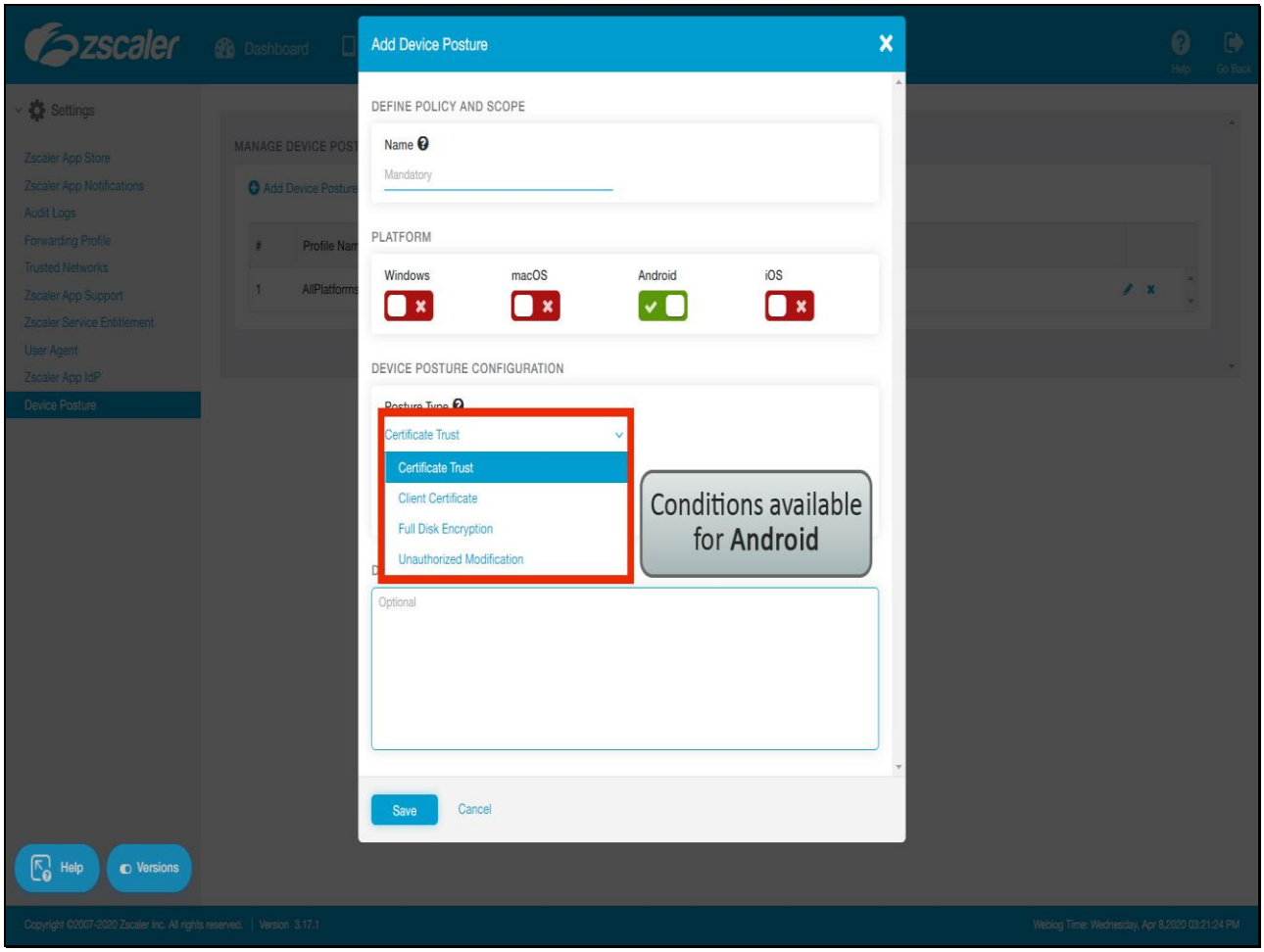
Slide 46 - Slide 46



Slide notes

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

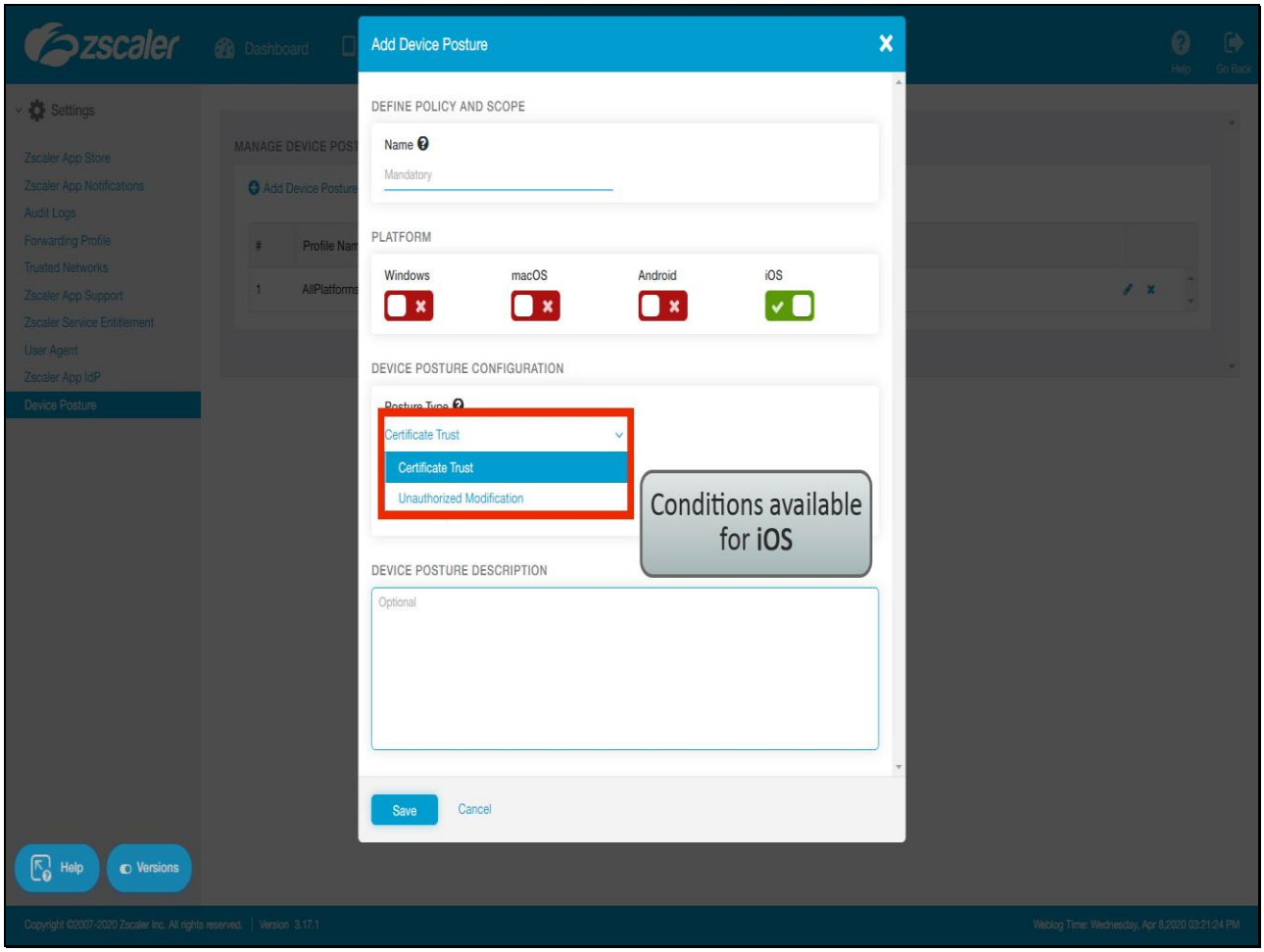
Slide 47 - Slide 47



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'.

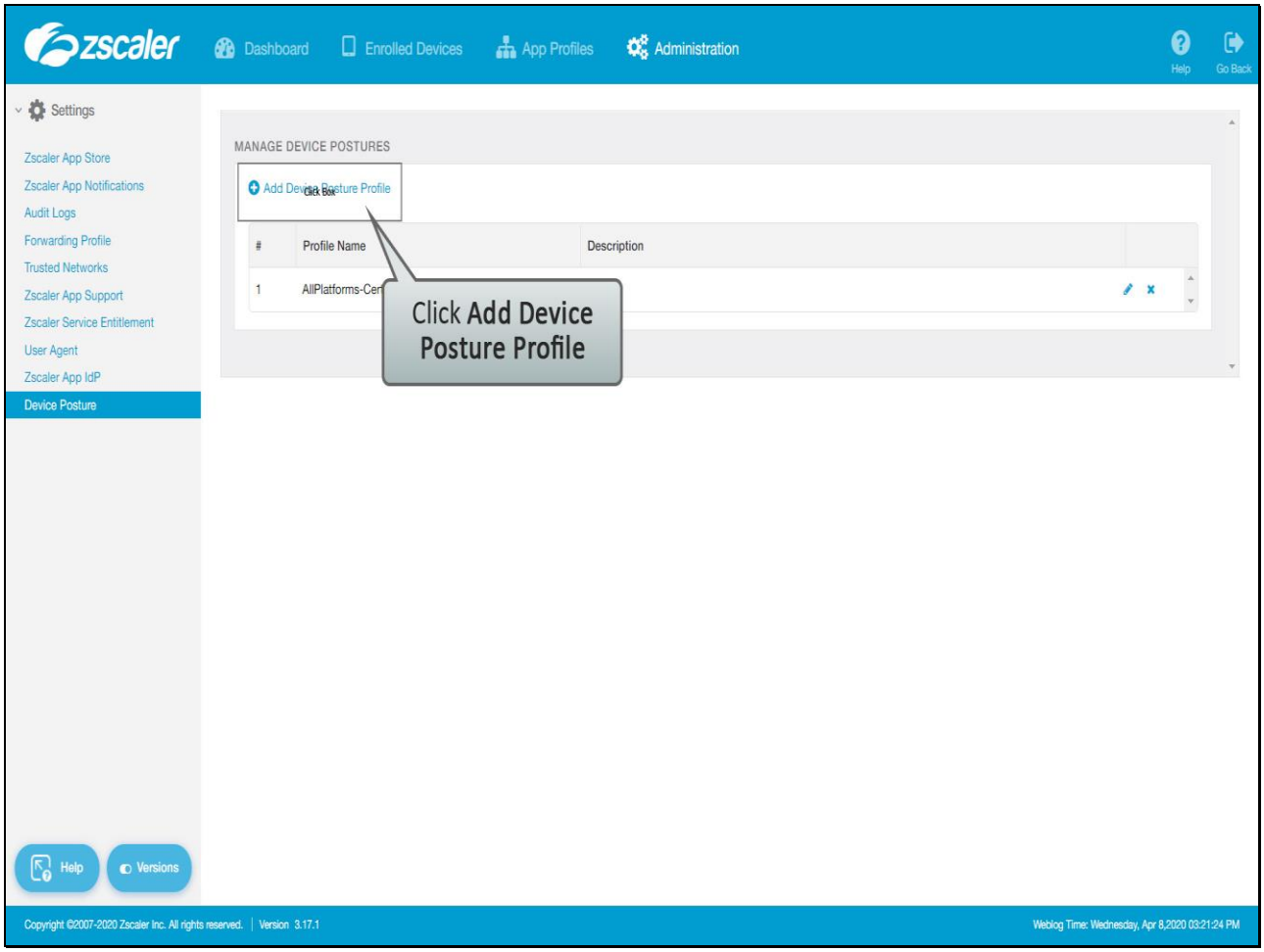
Slide 48 - Slide 48



Slide notes

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

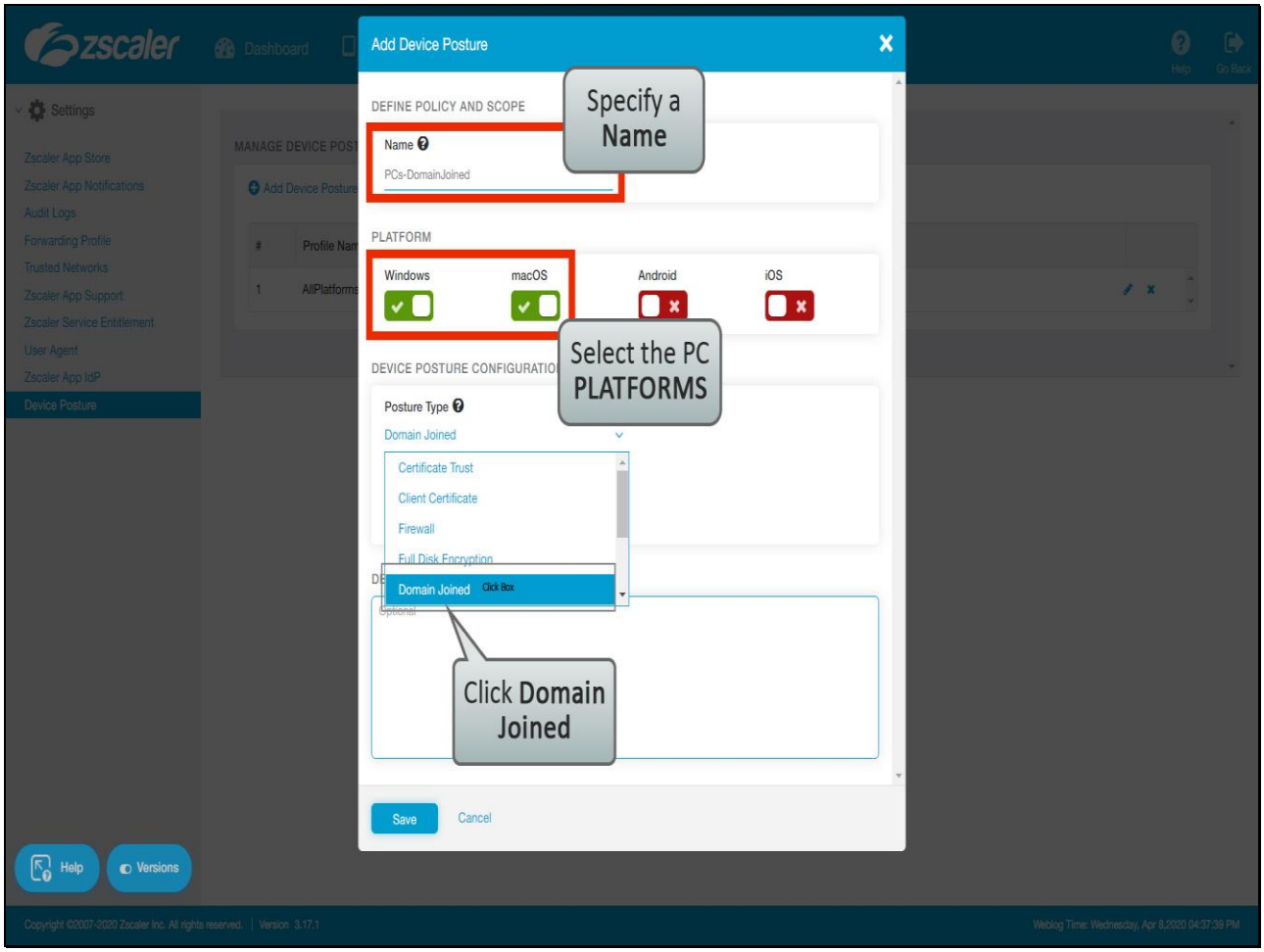
Slide 49 - Slide 49



Slide notes

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

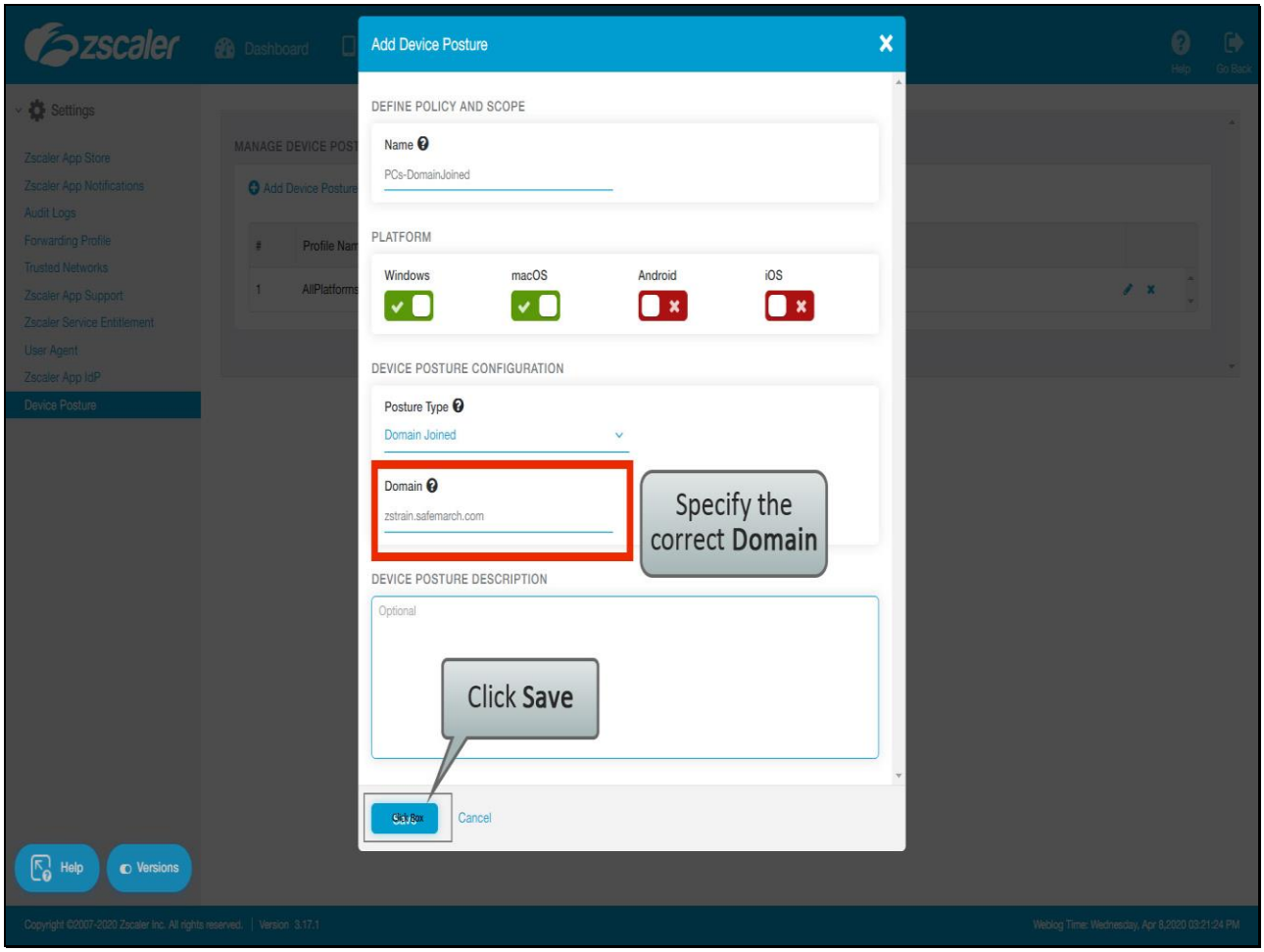
Slide 50 - Slide 50



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**, ...

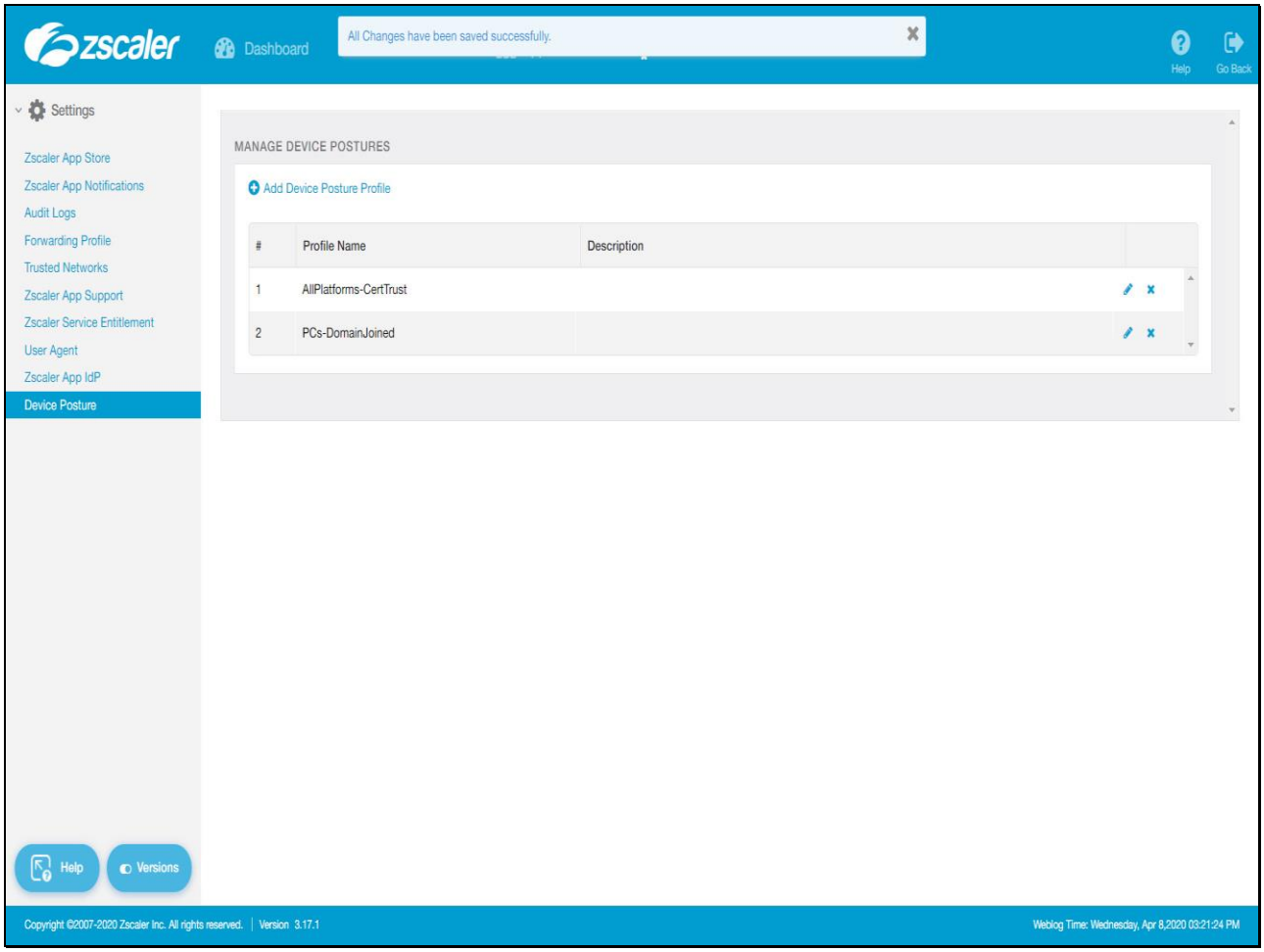
Slide 51 - Slide 51



Slide notes

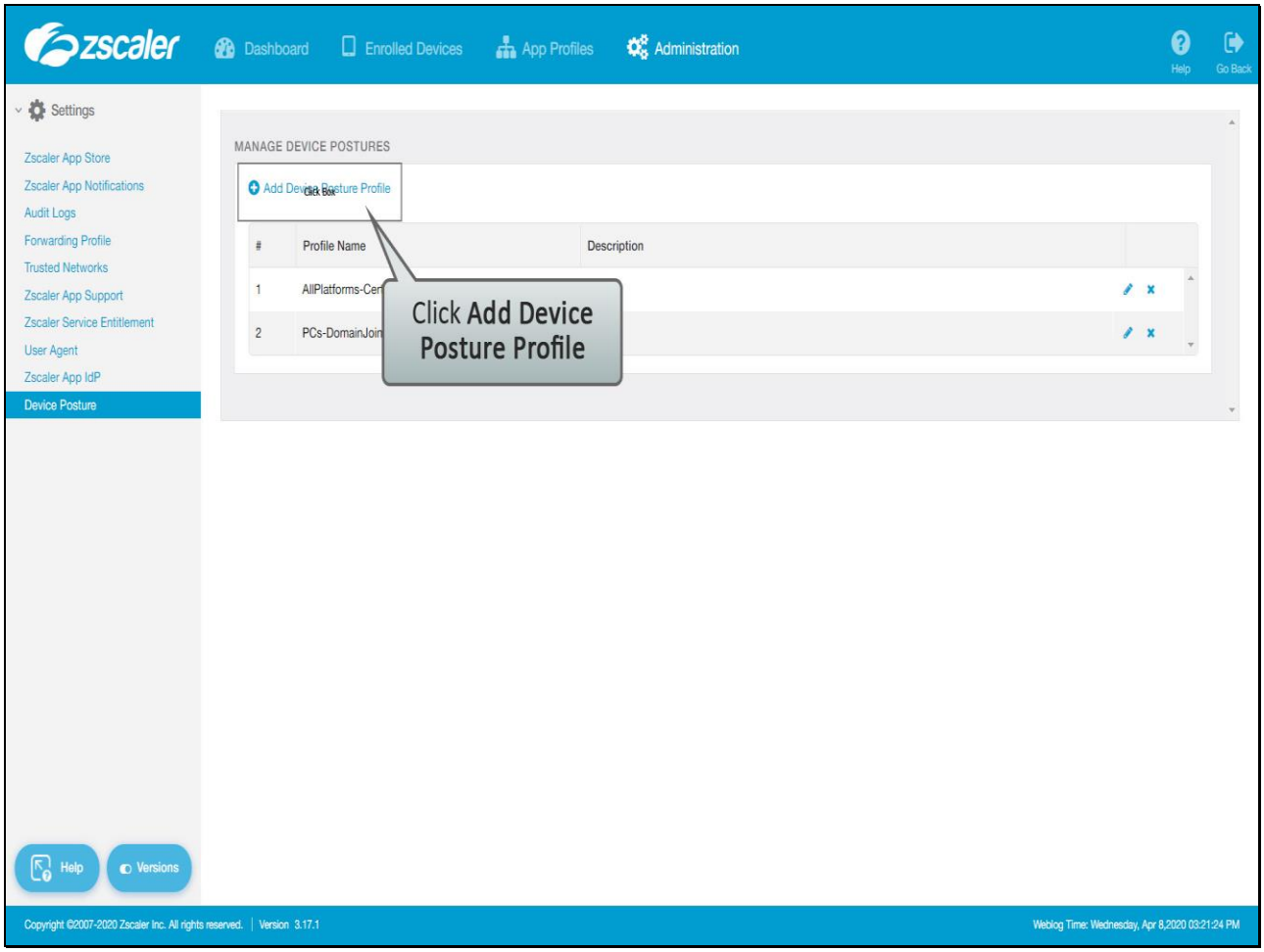
…specify the **Domain** to match and click **Save**.

Slide 52 - Slide 52



Slide notes

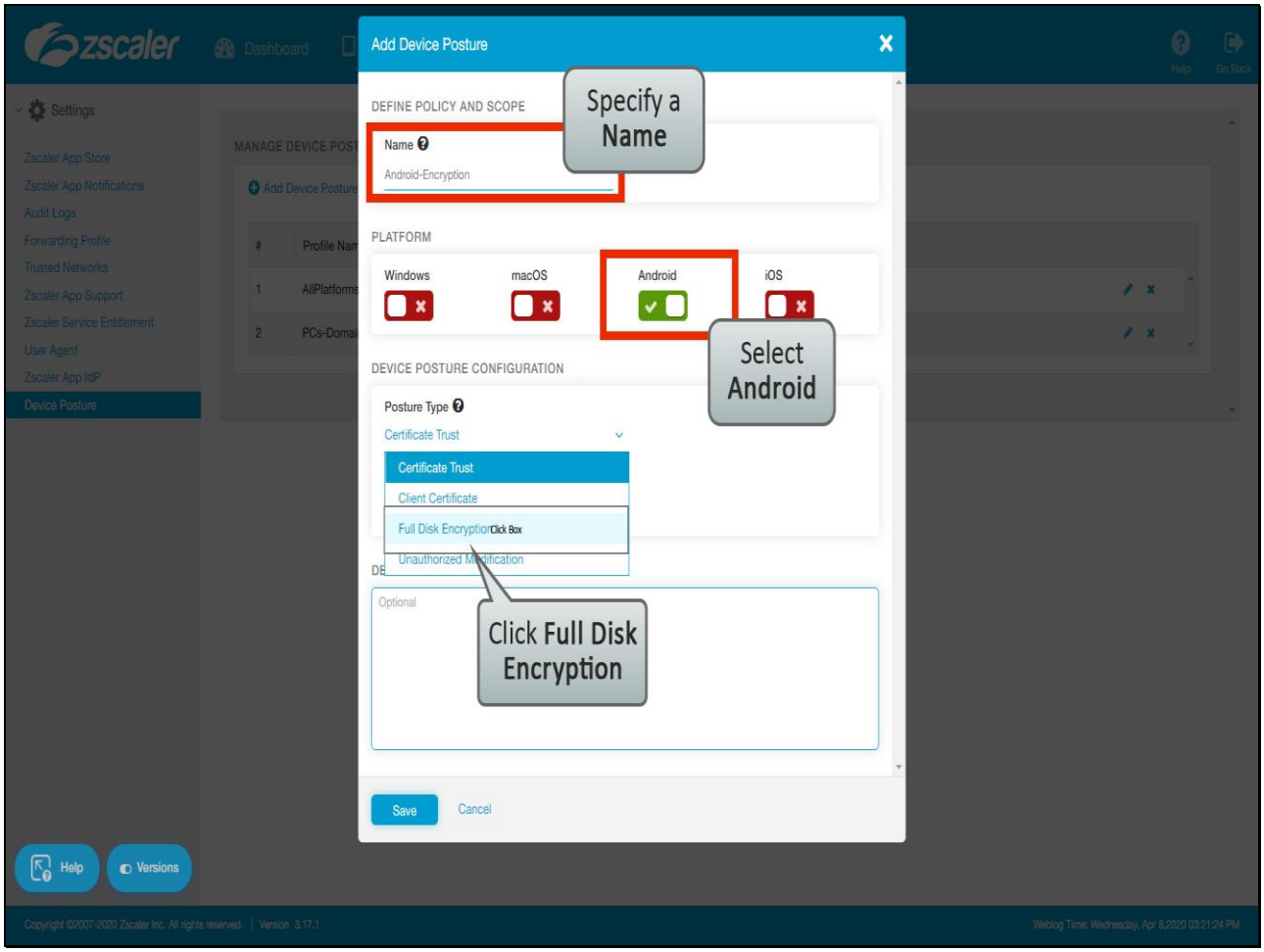
Slide 53 - Slide 53



Slide notes

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

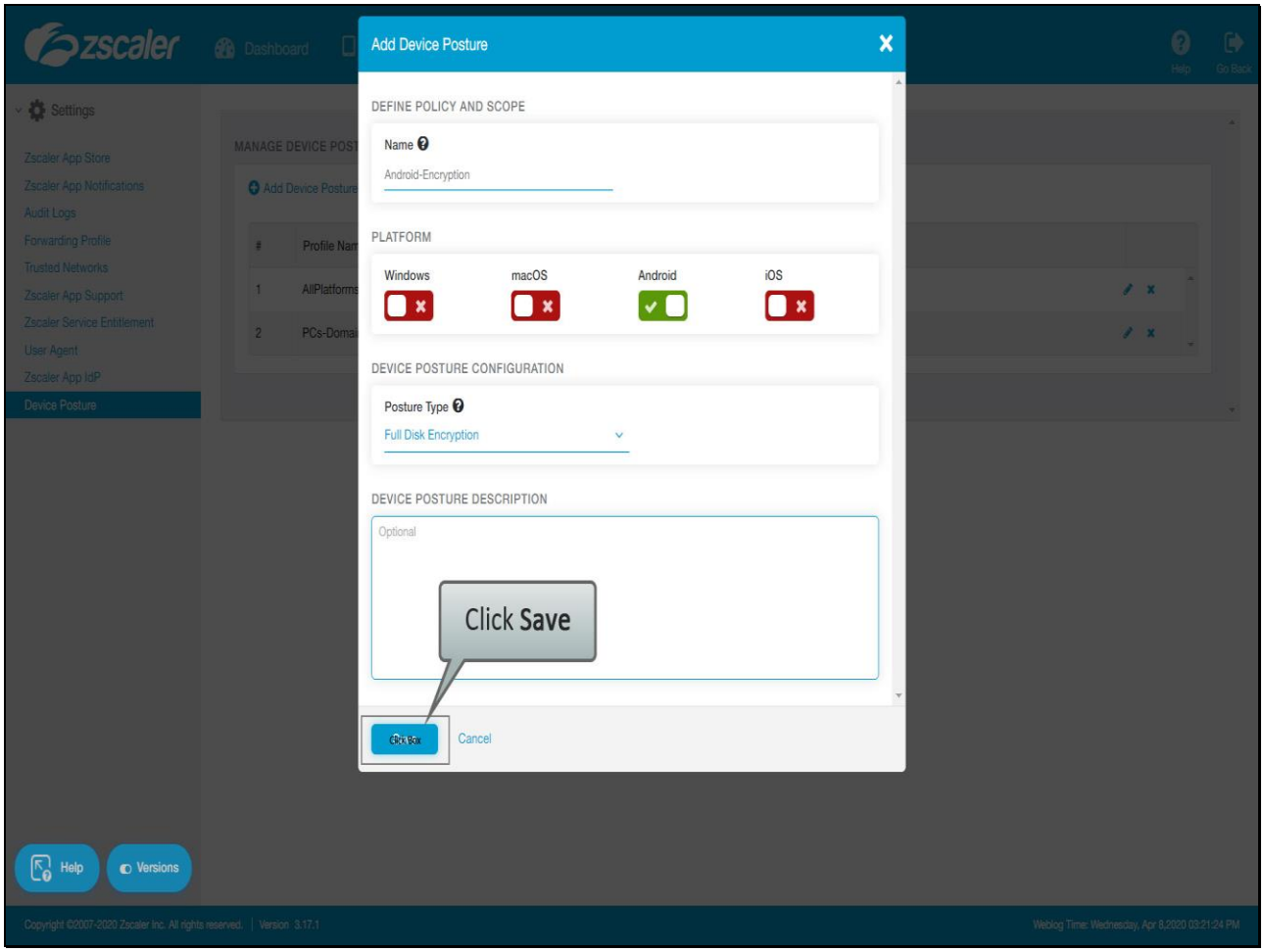
Slide 54 - Slide 54



Slide notes

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

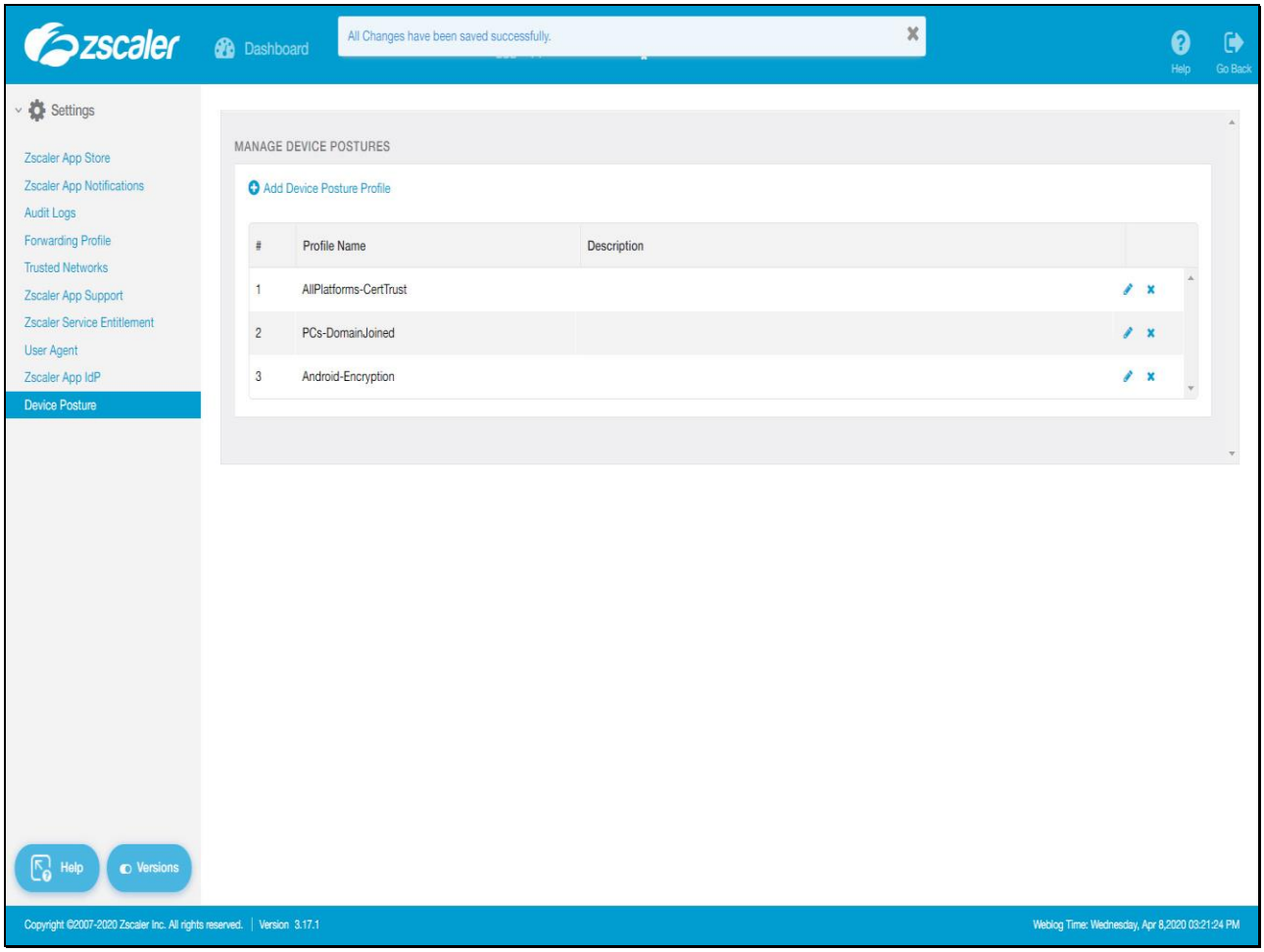
Slide 55 - Slide 55



Slide notes

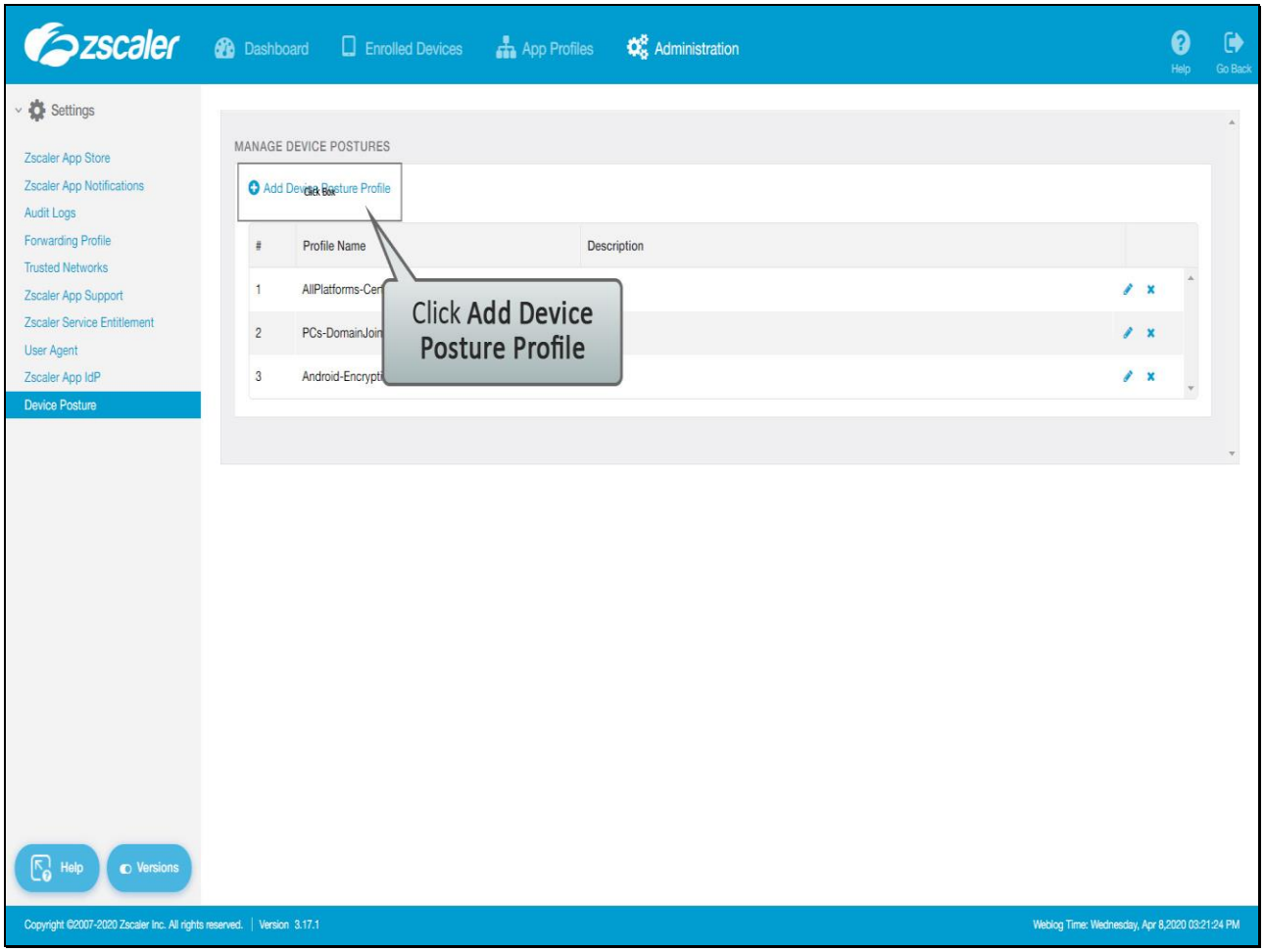
…and click **Save**.

Slide 56 - Slide 56



Slide notes

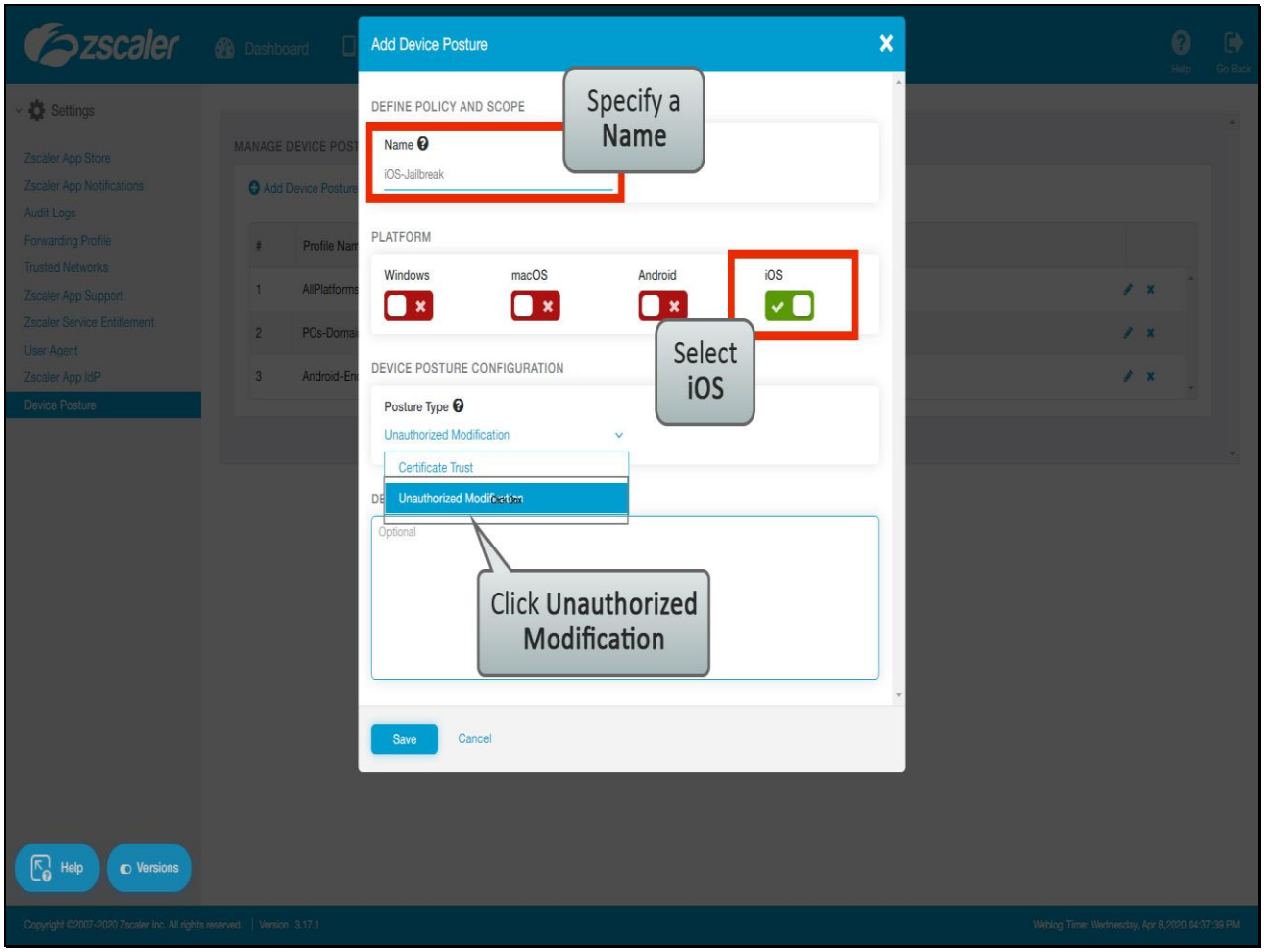
Slide 57 - Slide 57



Slide notes

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

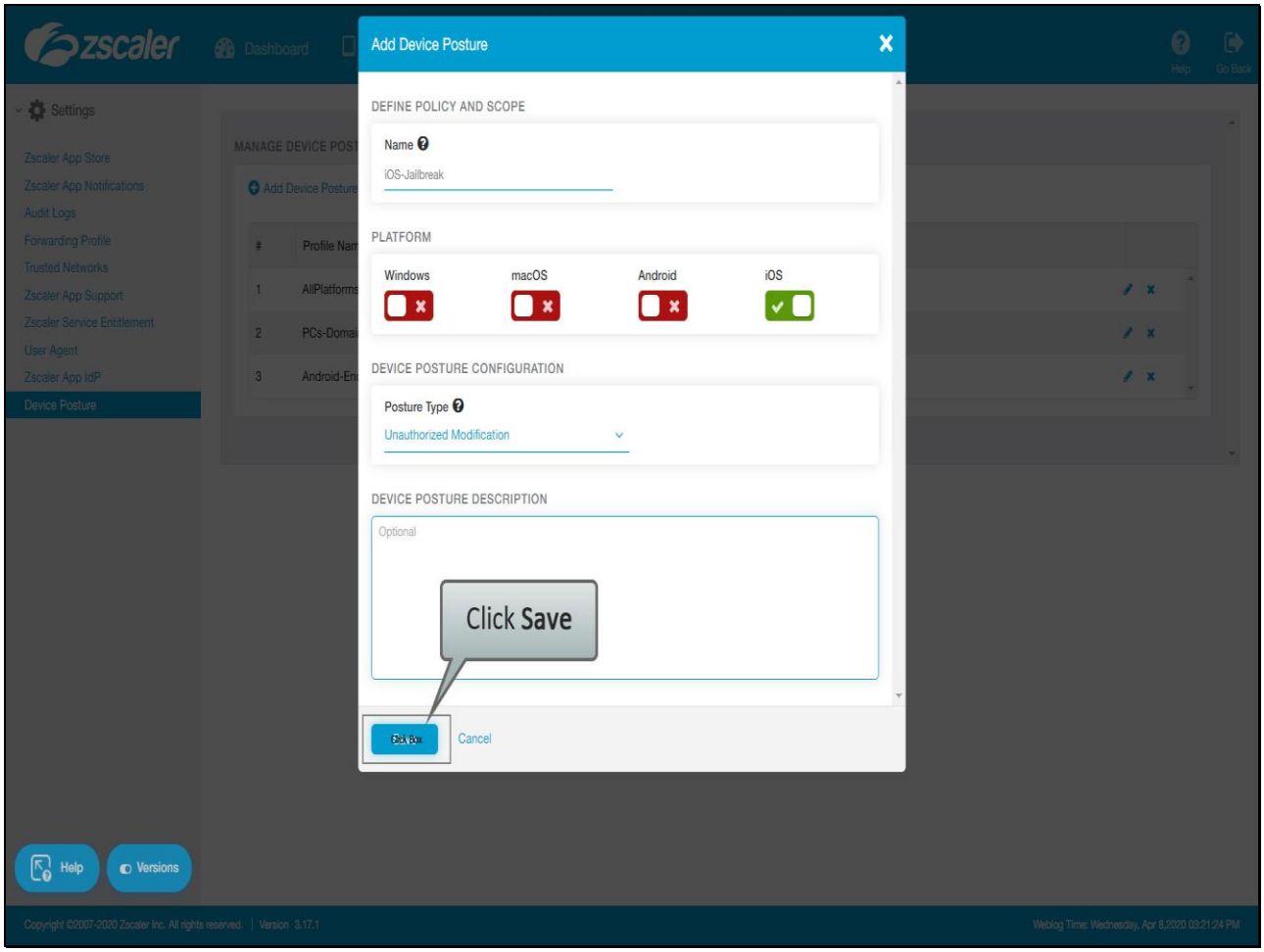
Slide 58 - Slide 58



Slide notes

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

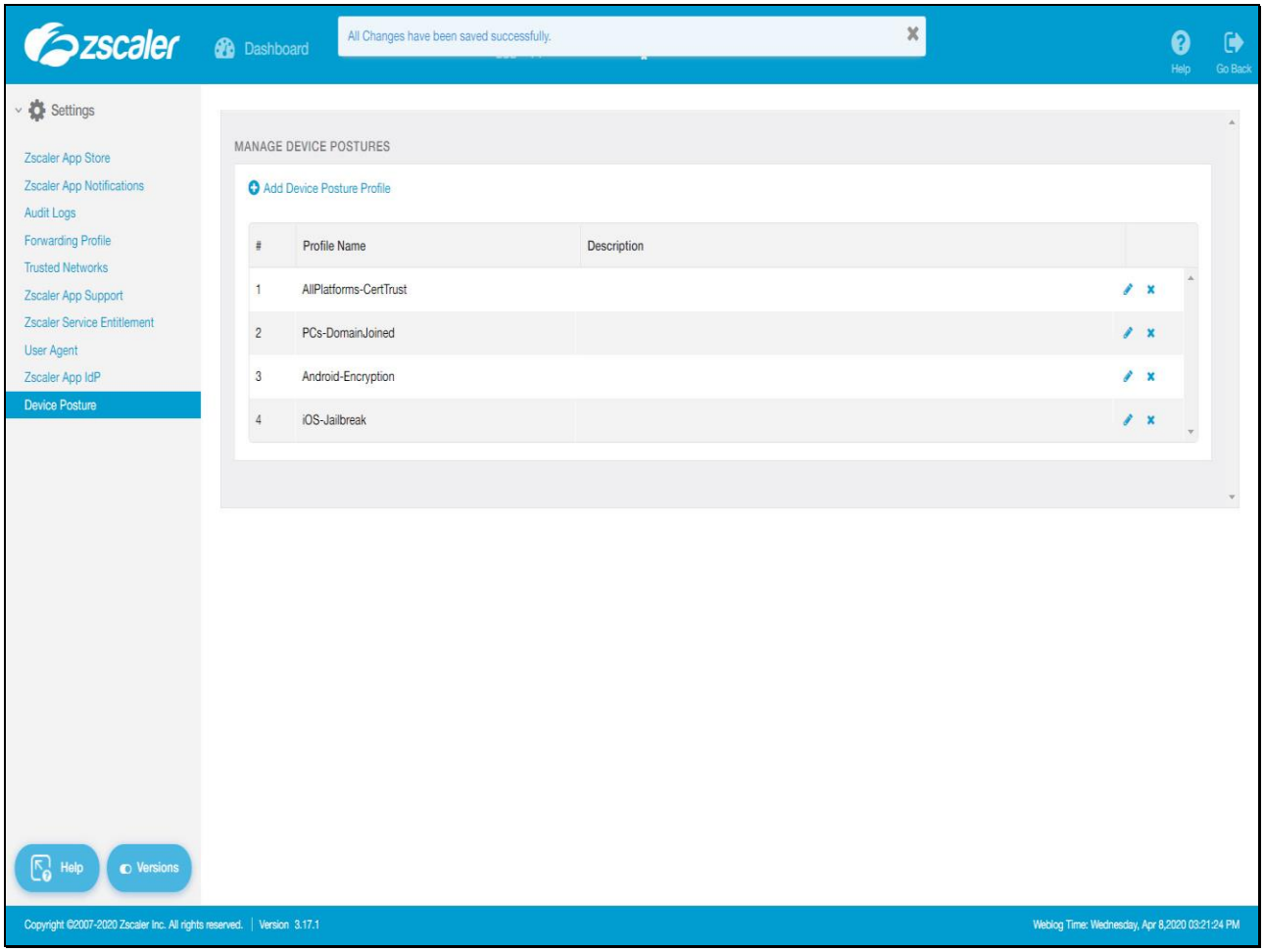
Slide 59 - Slide 59



Slide notes

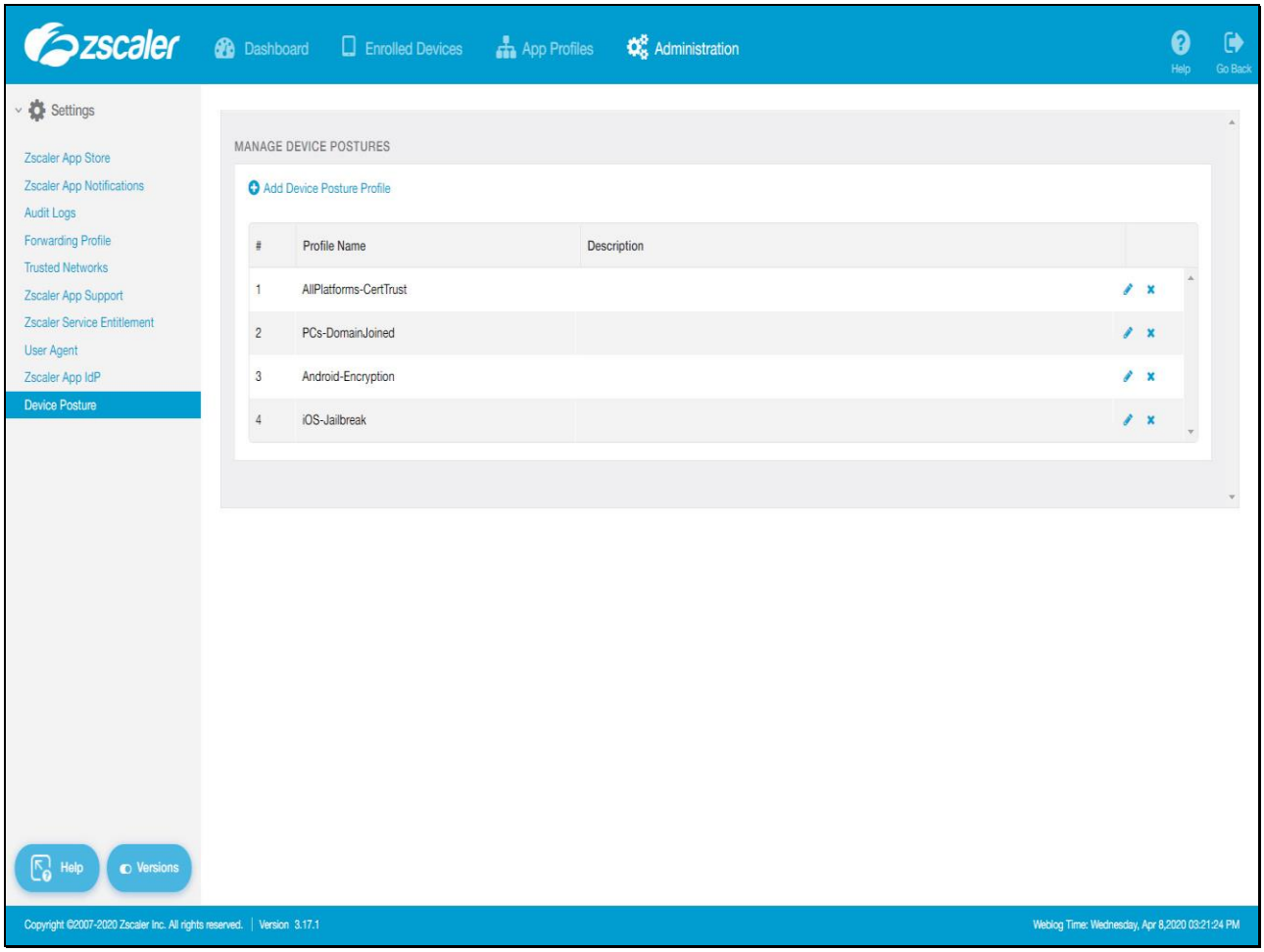
...and click **Save**.

Slide 60 - Slide 60



Slide notes

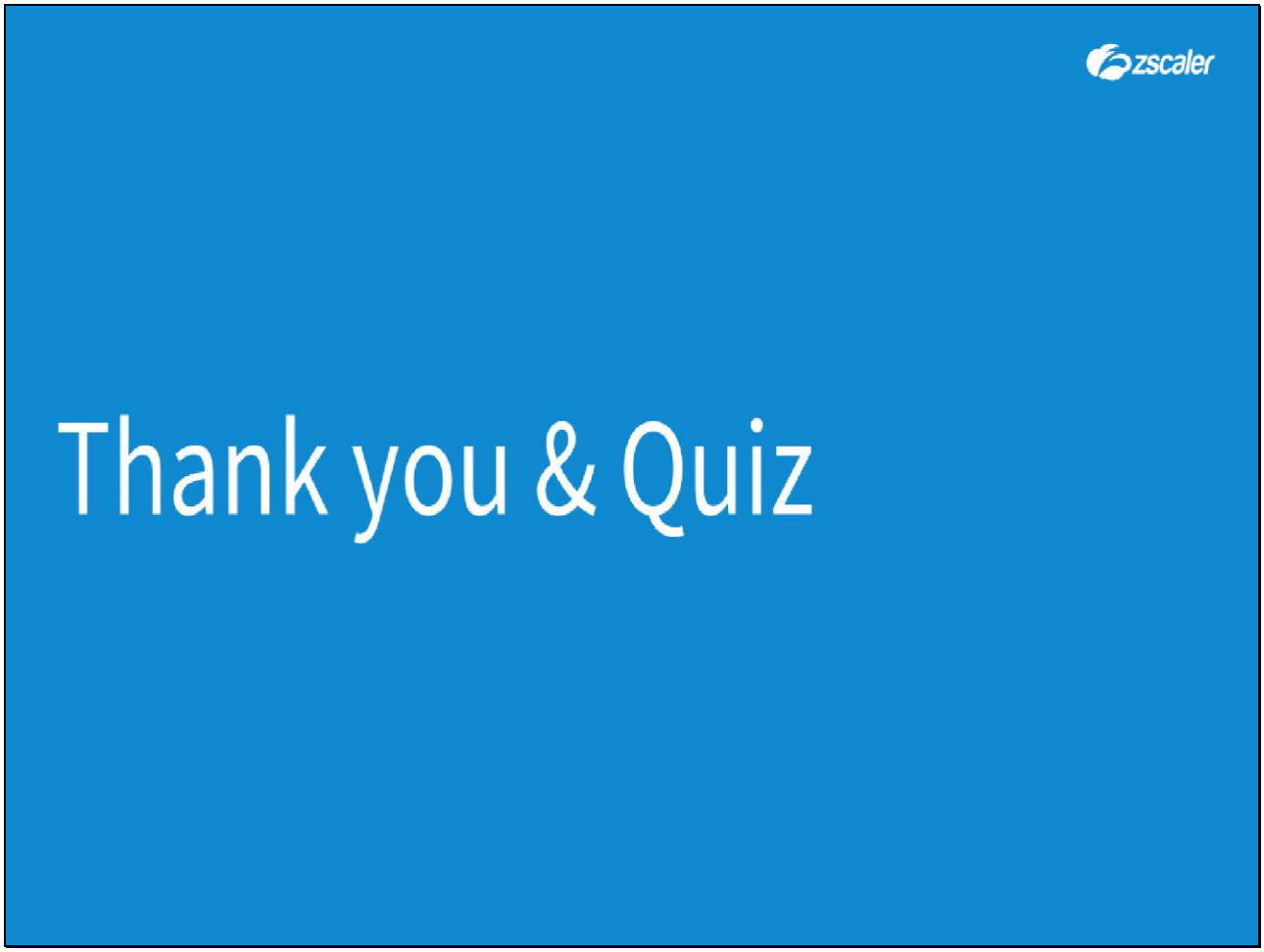
Slide 61 - Slide 61



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.