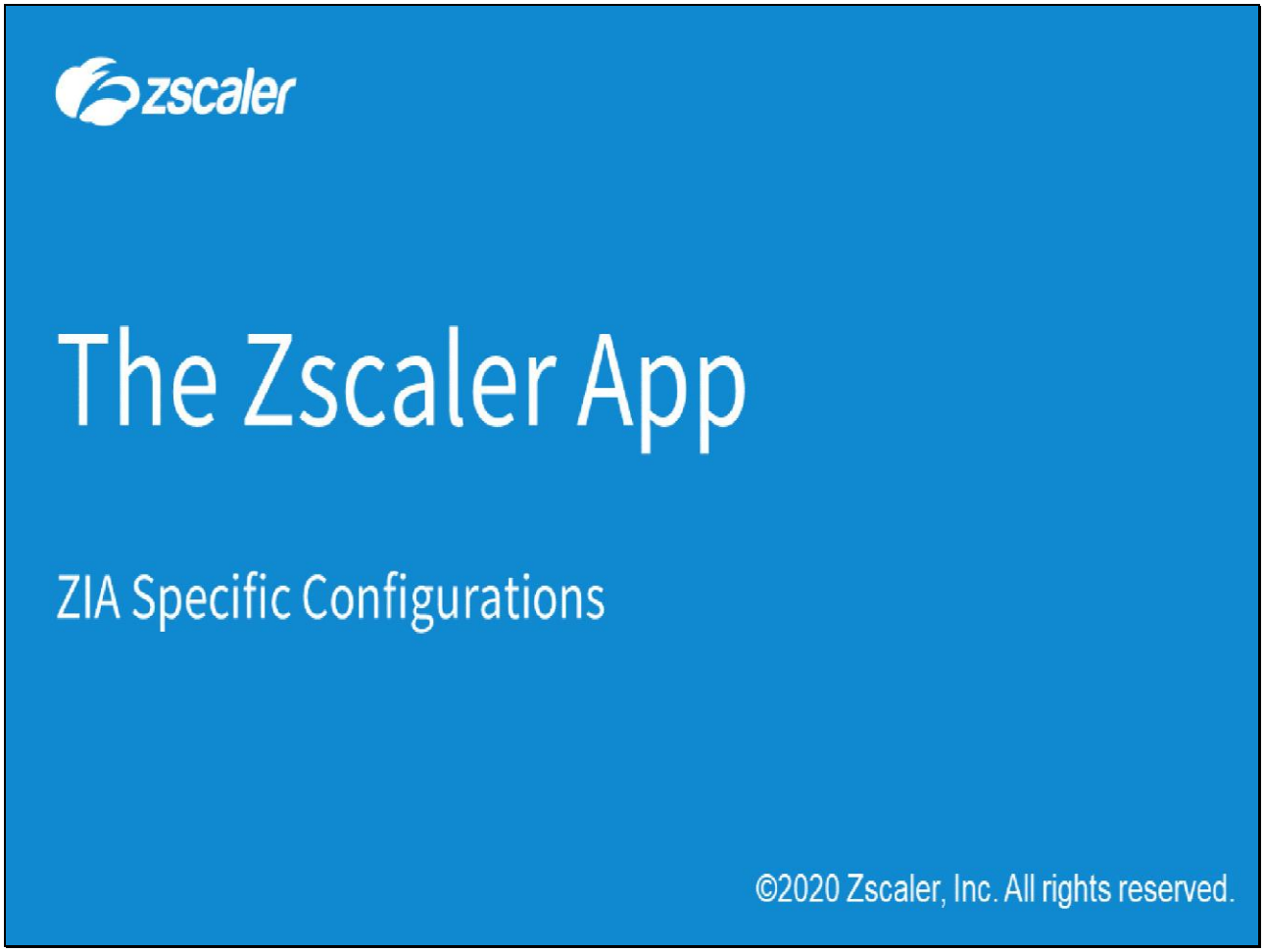
Slide 1 – The Zscaler App: ZIA Specific Configurations



Slide notes

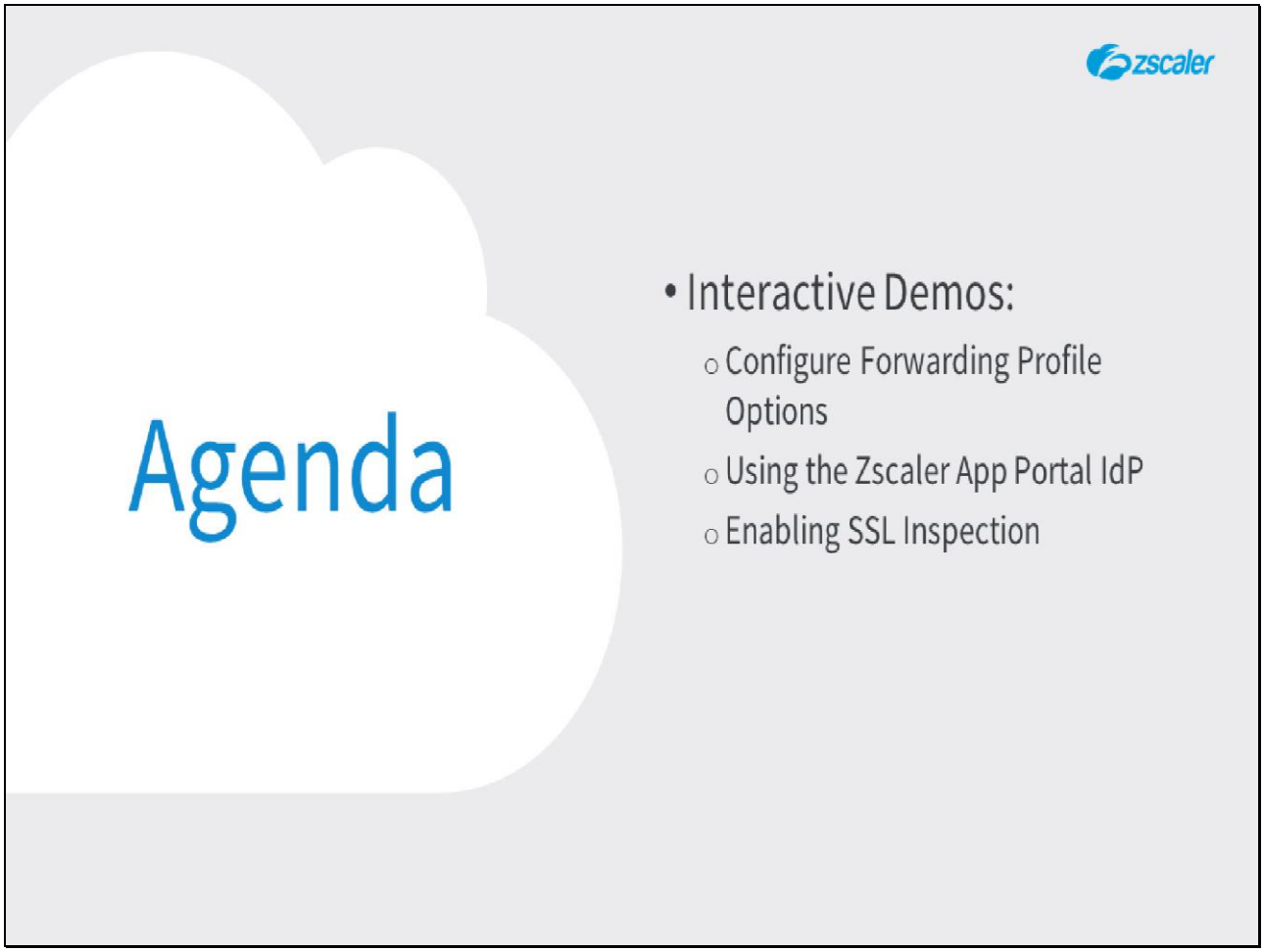
Welcome to this training module on Zscaler App configurations that are specific to the ZIA service.

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 ZIA: The available **Forwarding Profile** options; using the **Zscaler App Portal IdP** for silent ZIA end user enrollment; and at how to enable **SSL Inspection** for Zscaler App users.

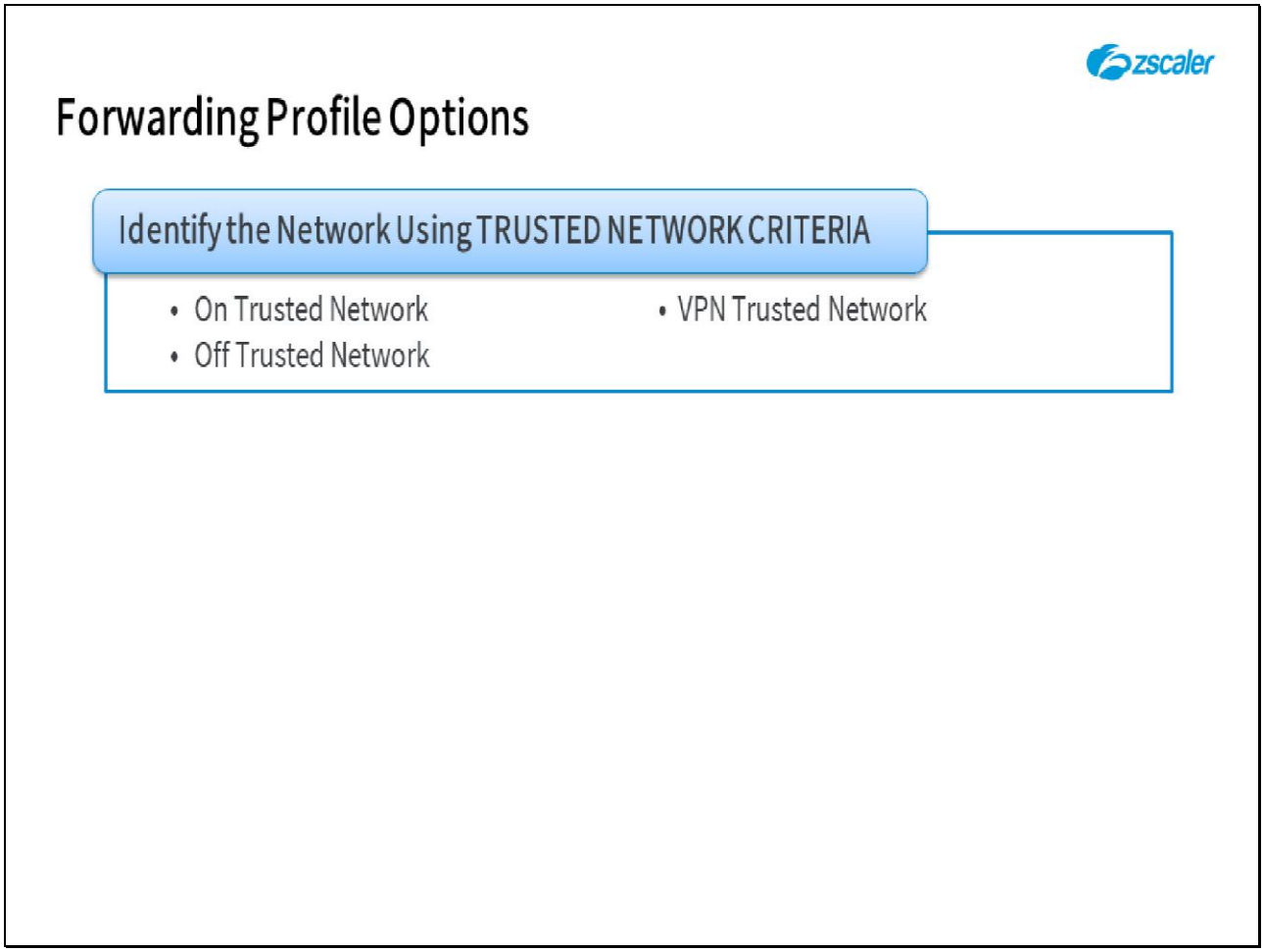
Slide 4 - Interactive Demo: Provisioning the Zscaler App

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.

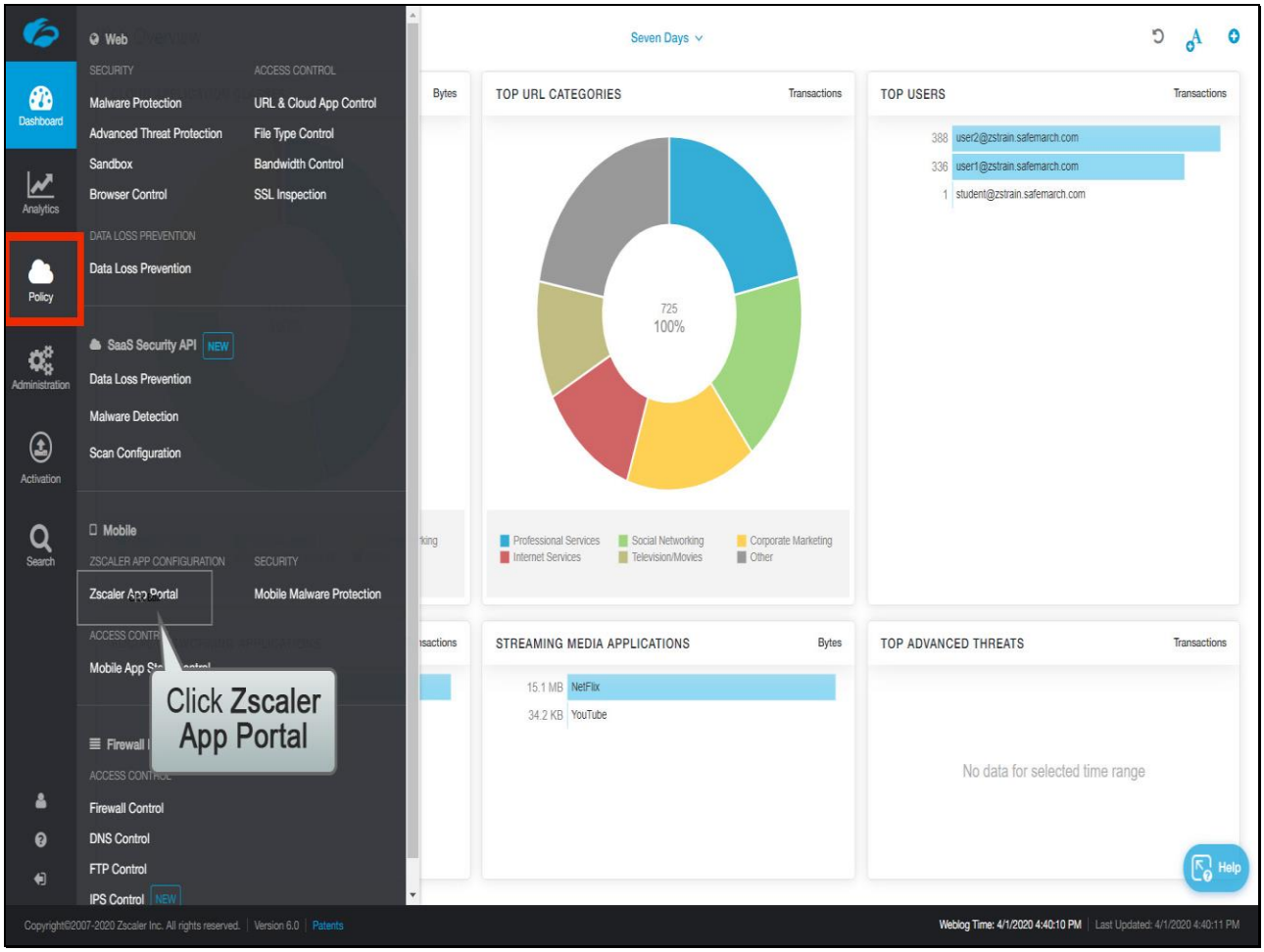
Slide 5 - Forwarding Profile Options



Slide notes

Forwarding Profiles can be used to control whether and how traffic is forwarded by the Zscaler App for Internet 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

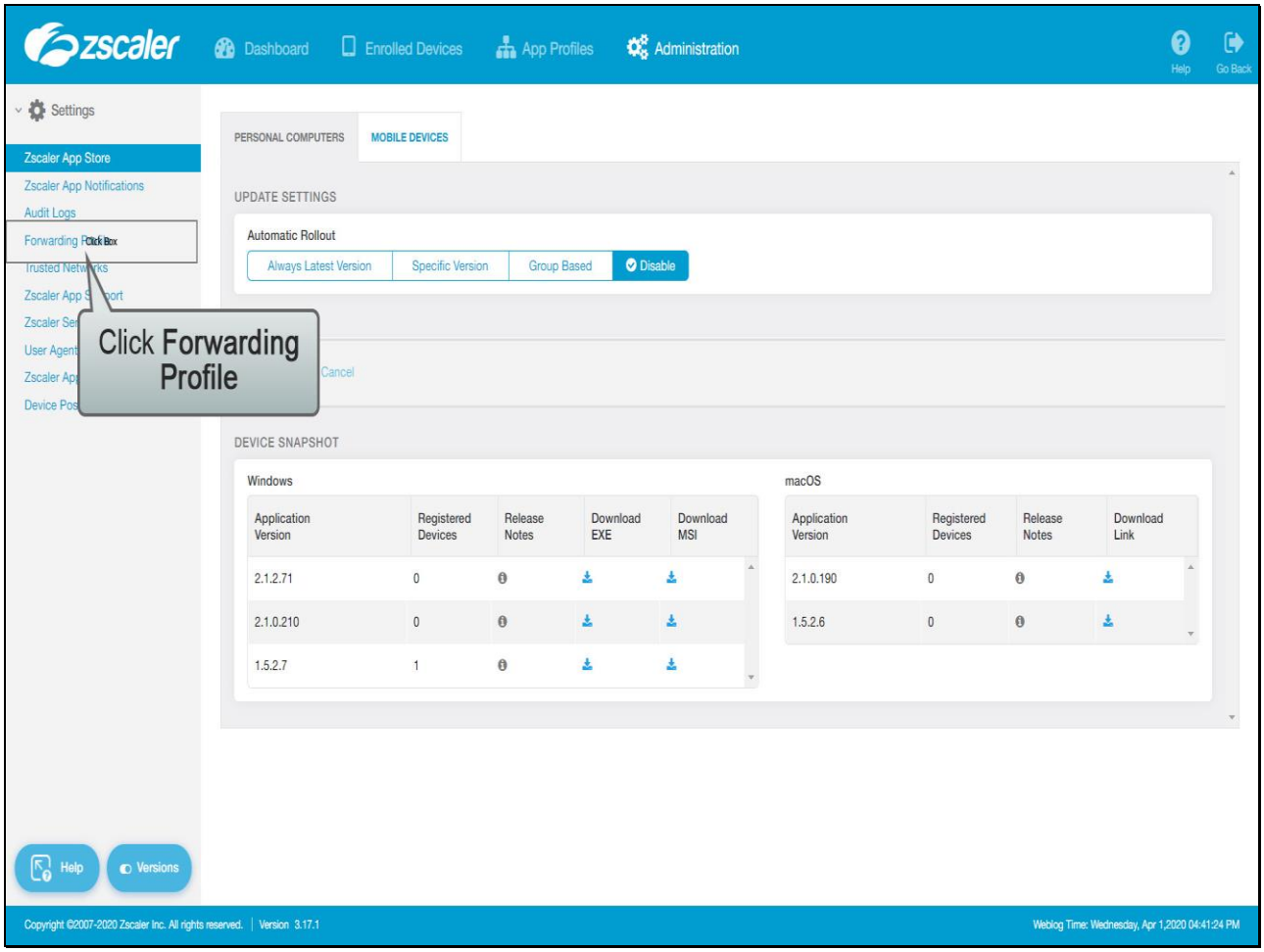
To access the Zscaler App Portal from the ZIA Admin Portal, click **Policy**, then **Zscaler App Portal**.

Slide 7 - Slide 7

Slide notes

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

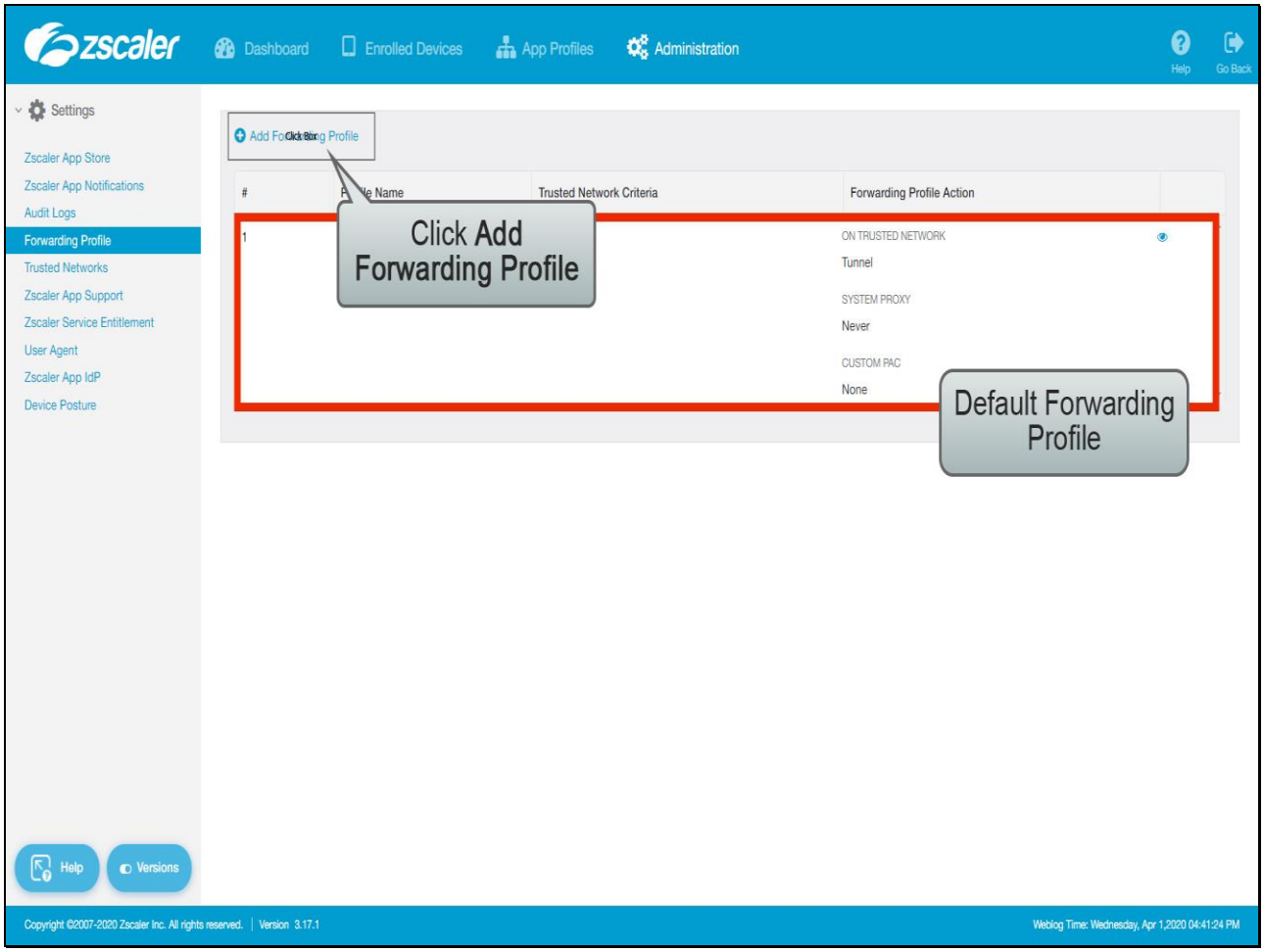
Slide 8 - Slide 8



Slide notes

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

Slide 9 - Slide 9



Slide notes

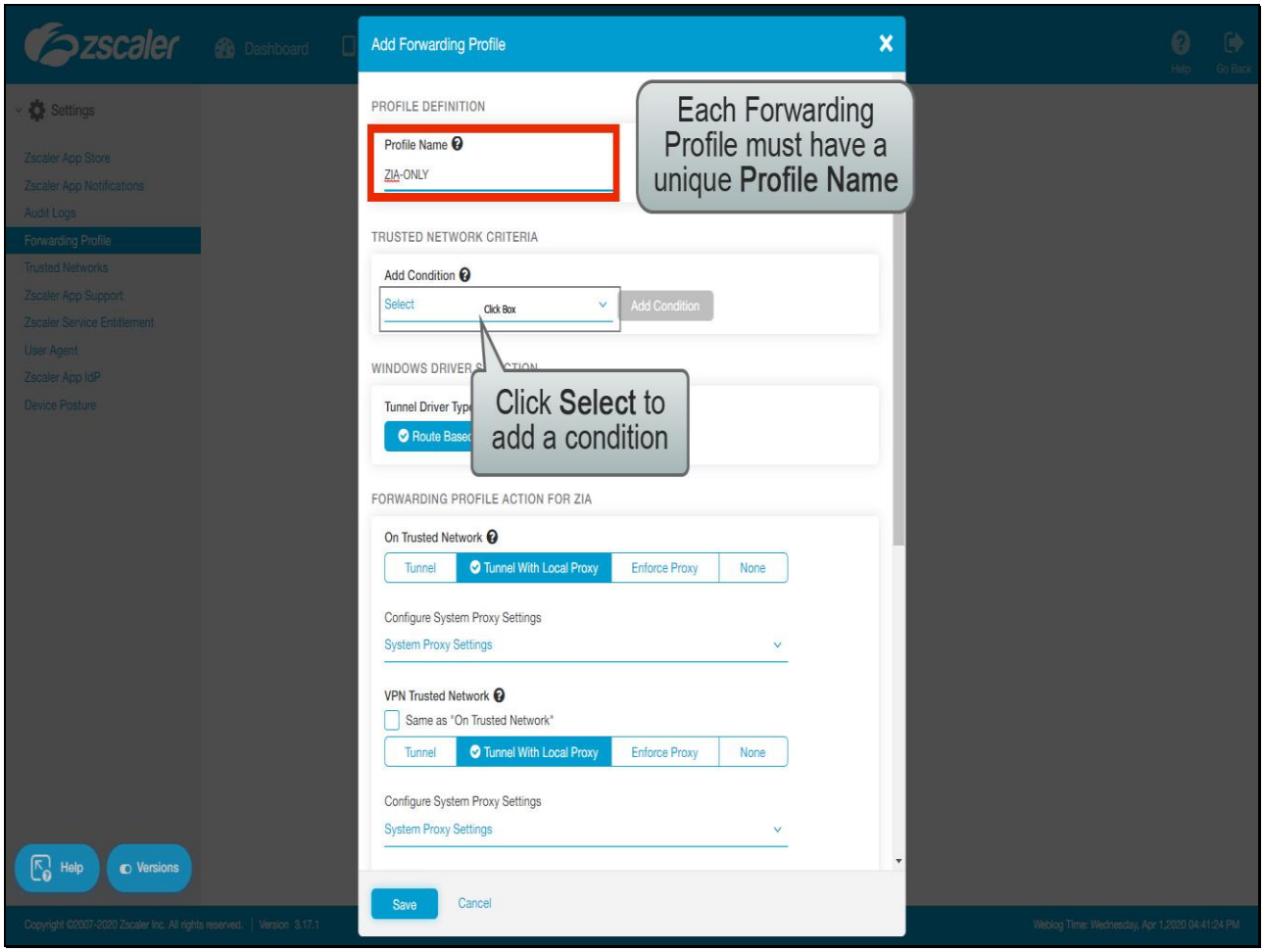
You will find that there is a default **Forwarding Profile** (which cannot be edited), and the option to add a new one. The default profile configuration is as follows:

- **On and Off Tusted Network** - are both set to use **Tunnel 1.0** with **Proxy Action Type** set to **Never**;
- **VPN Trusted Network** - uses the **Enforce Proxy** 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

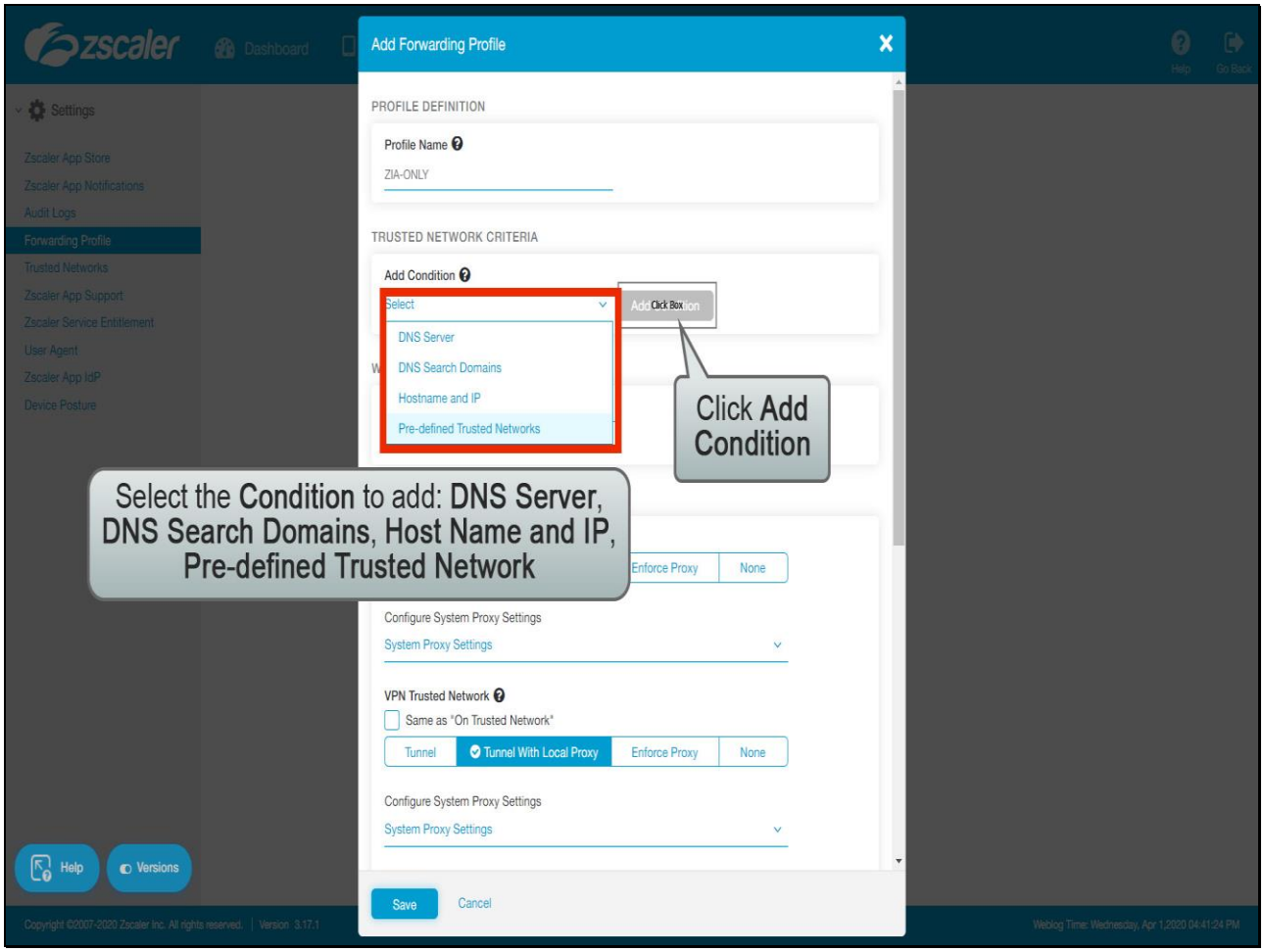


Slide notes

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

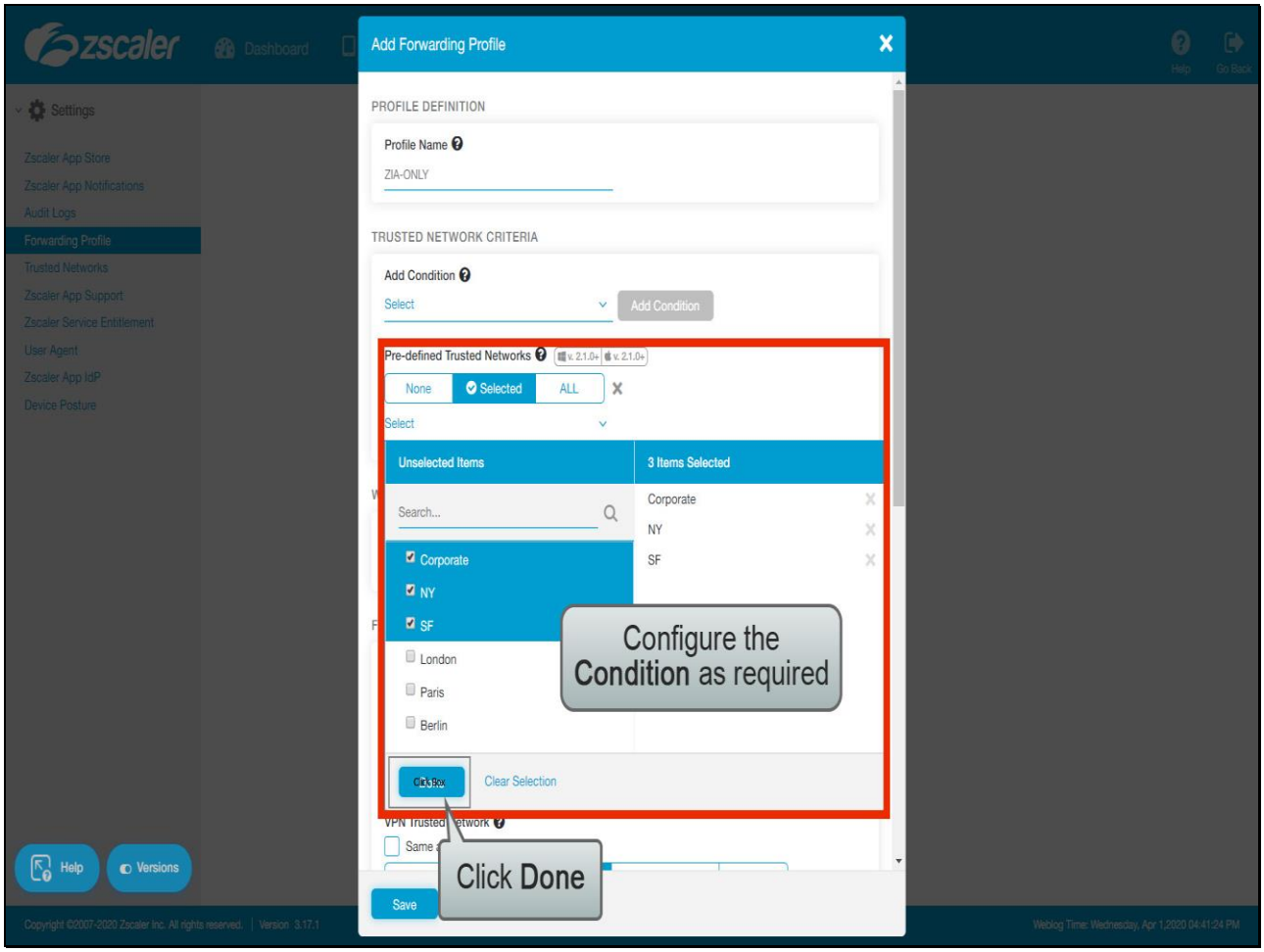
...and select the appropriate condition to be met. The conditions available are:

- **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, …

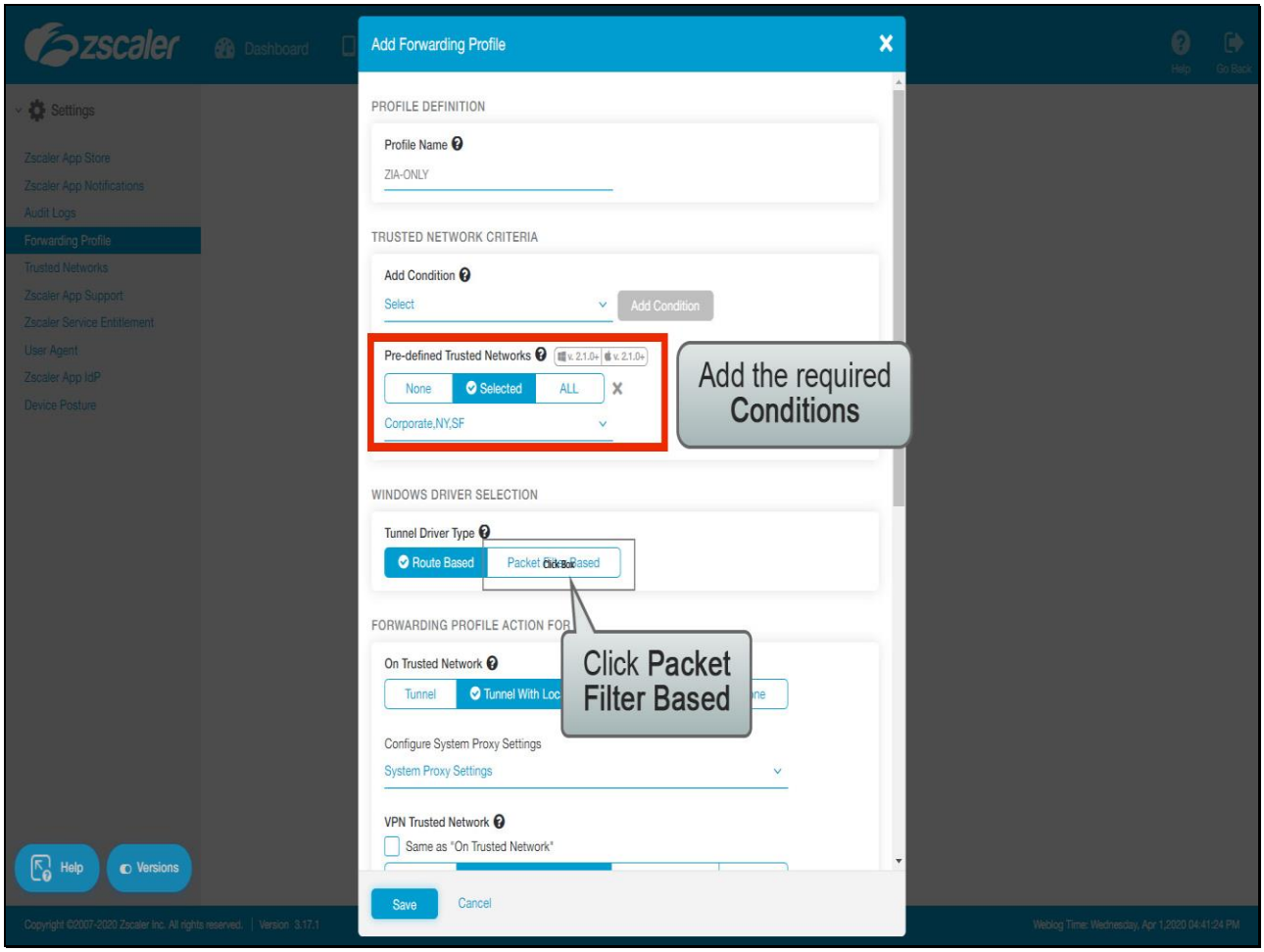
Slide 12 - Slide 12



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

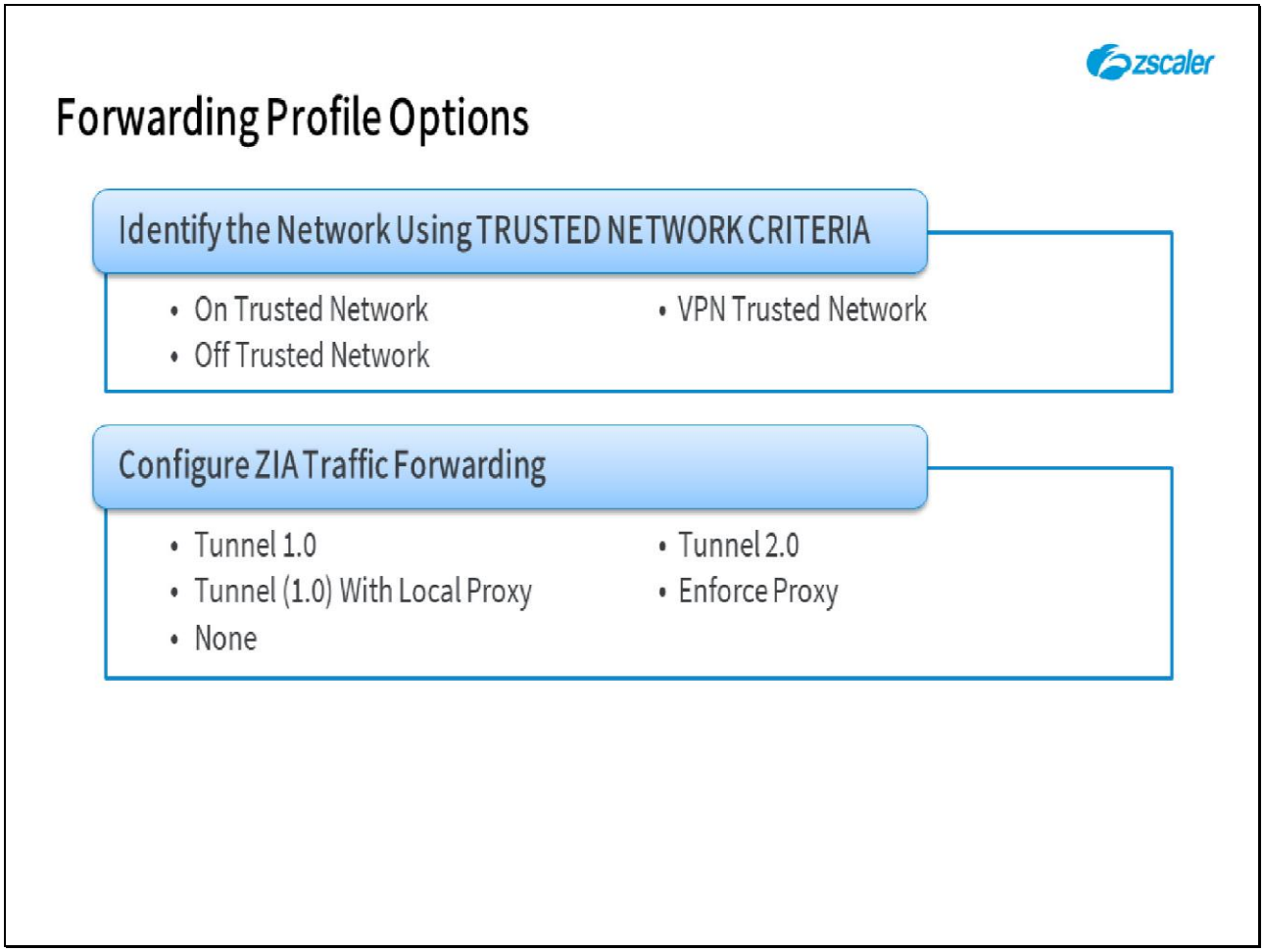


Slide notes

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 Lightweight Filter (LWF) 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 - Forwarding Profile Options



Slide notes

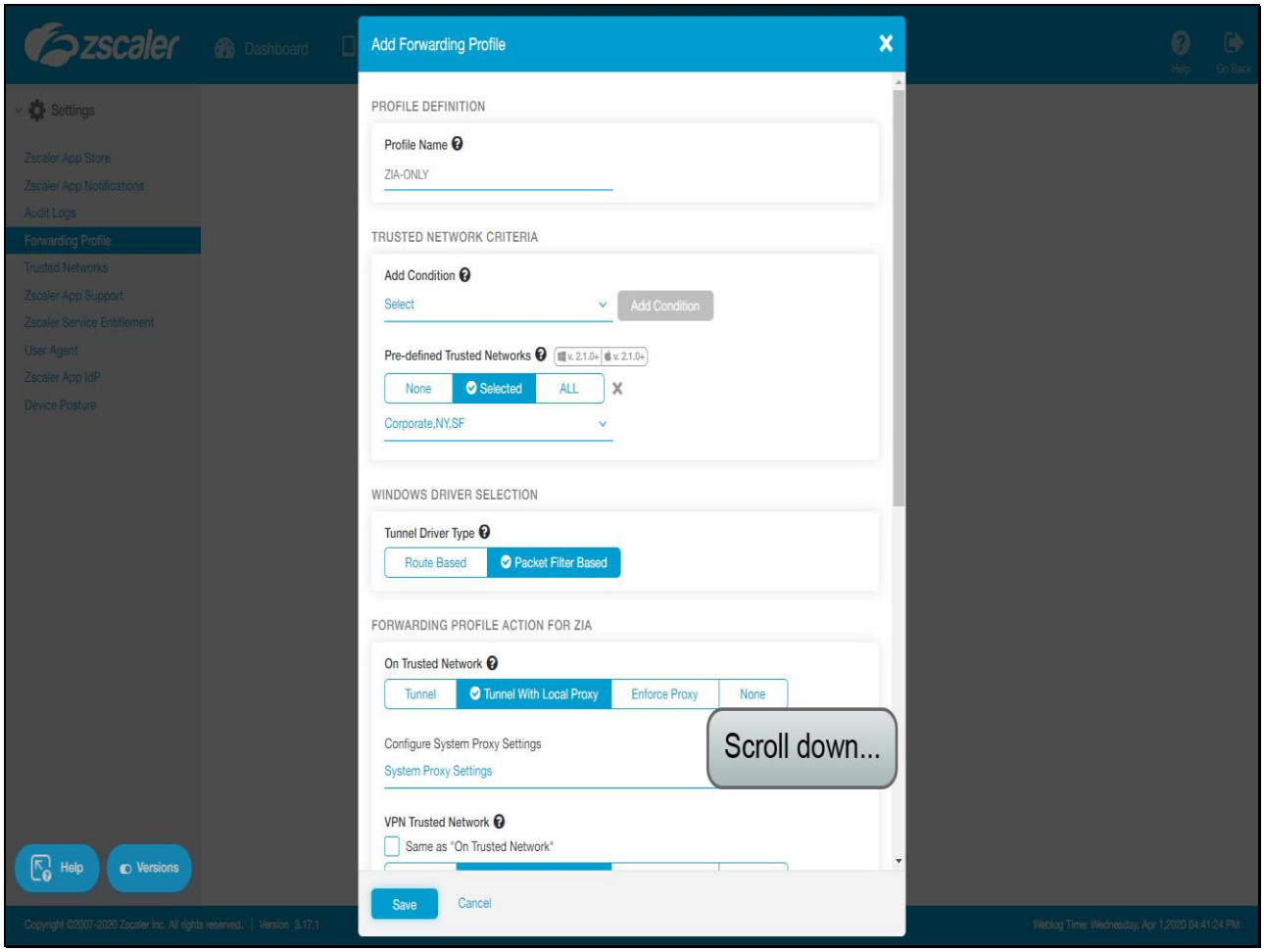
The next part of the **Forwarding Profile** is all about traffic forwarding, with options for each of the three main scenarios (**On**, **Off**, or **VPN to** a trusted network). The ZIA forwarding options available are:

- **Tunnel 1.0**;
- **Tunnel 2.0**;
- **Tunnel (1.0) with Local Proxy**;
- **Enforce Proxy**;
- Or **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.

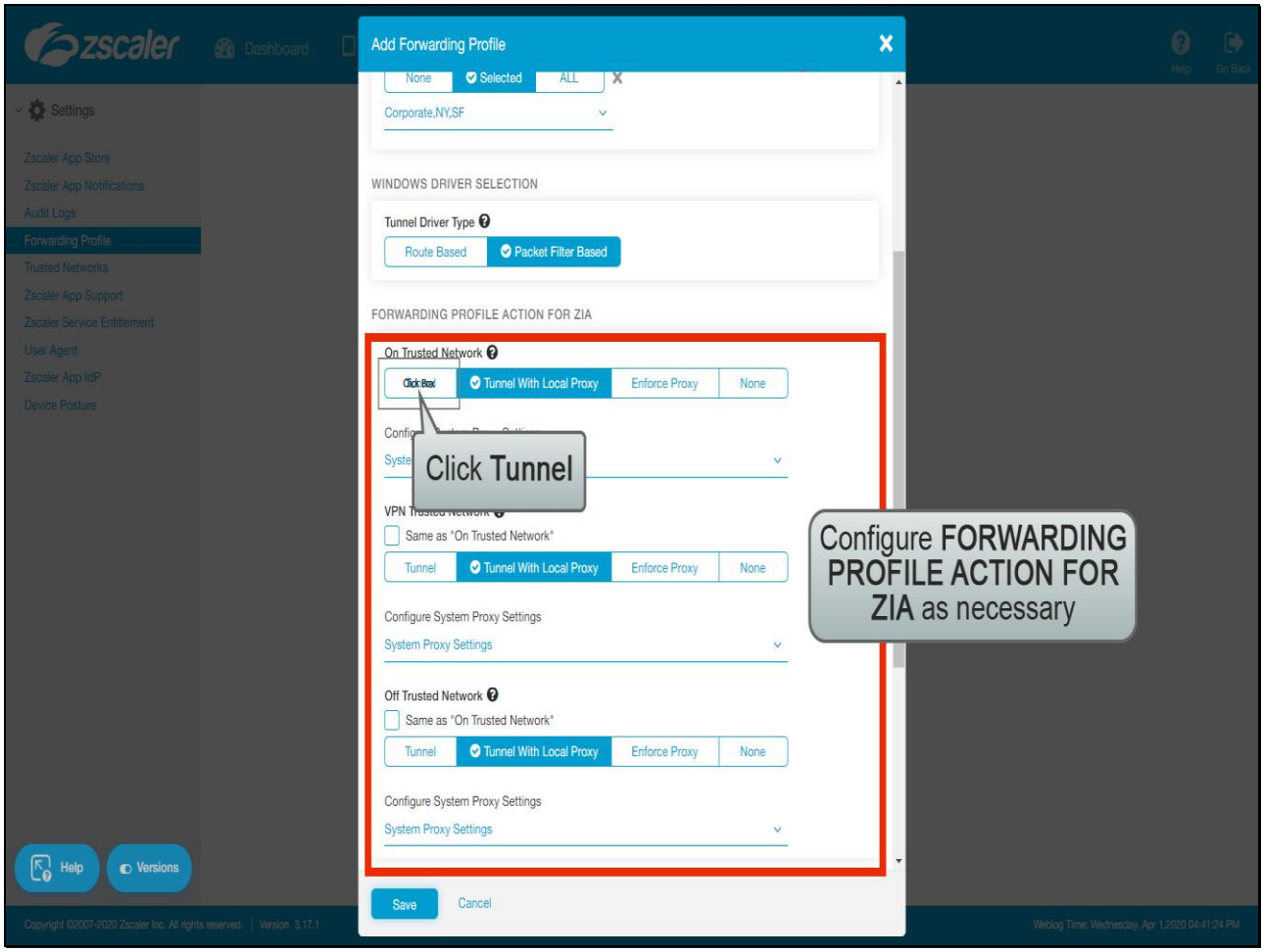
Slide 15 - Slide 15



Slide notes

Scroll down if necessary...

Slide 16 - Slide 16



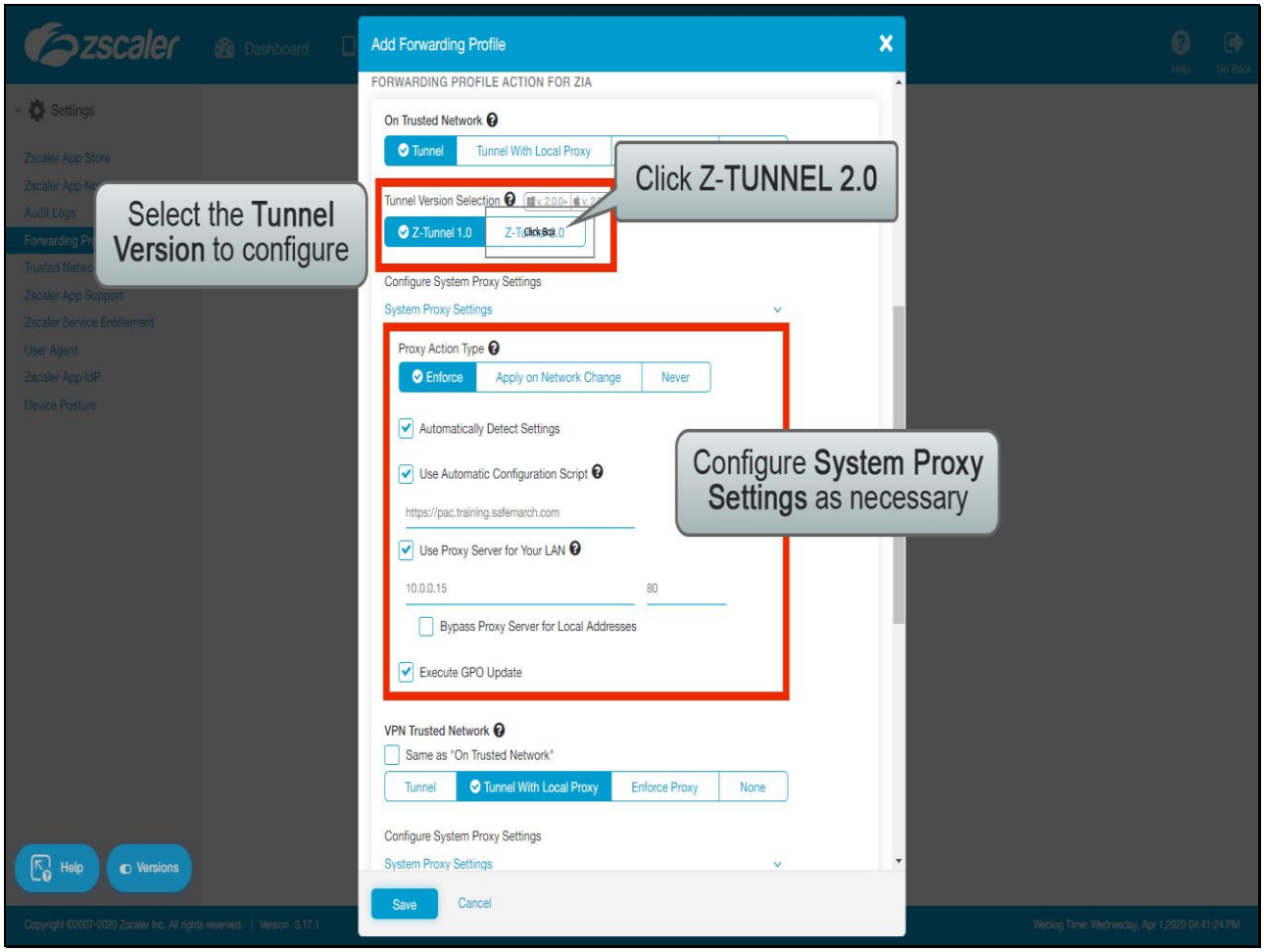
Slide notes

If the App is to be used for Internet Access, 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 1.0**;
- **Tunnel 2.0**;
- **Tunnel (1.0) with Local Proxy**;
- **Enforce Proxy**;
- And **None**.

We will look at the configuration for each option in turn. For the **On Trusted Network** configuration, click **Tunnel**, ...

Slide 17 - Slide 17



Slide notes

The first decision here is which version of tunneling to use, **Z-TUNNEL 1.0** (lightweight HTTP CONNECT tunnels), or **Z-TUNNEL 2.0** (DTLS or TLS tunnels). For a **Tunnel 1.0** configuration, you have a number of options for also configuring **System Proxy Settings**, whether to:

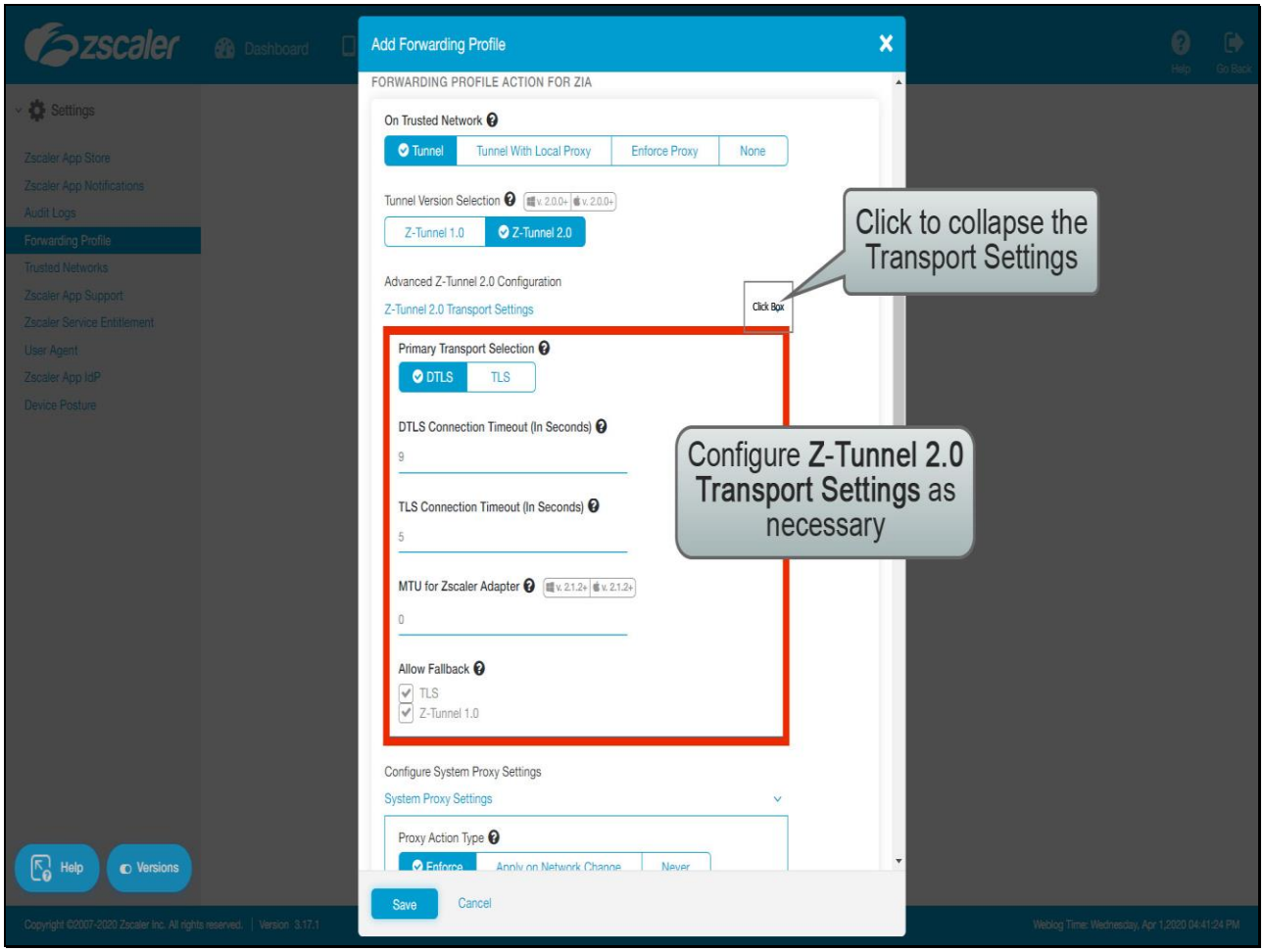
- **Enforce**;
- **Apply on Network Change**;
- Or **Never**.

With the **Enforce** and **Apply on Network Change** options, you can also control how the proxy settings should be delivered using a combination of:

- **Automatically Detect Settings**;
- **Use Automatic Configuration Script** with the URL of the PAC file to use;
- **Use Proxy Server for Your LAN**, with the server configuration;
- And/or **Execute GPO Update**.

If you need to support traffic types beyond simple HTTP/S, click **Z-TUNNEL 2.0**, ...

Slide 18 - Slide 18



Slide notes

...**Tunnel 2.0** supports the transport of just about any unicast IPv4 traffic, regardless of protocol and port. In order to provide integrity while maximizing capacity, the goal is to carry **Tunnel 2.0** traffic wherever possible in null-encrypted DTLS tunnels to the ZPA infrastructure, with a fallback to TLS tunnels if connection-oriented transport proves to be necessary. If absolutely necessary, **Tunnel 2.0** can fallback to the **Tunnel 1.0** method.

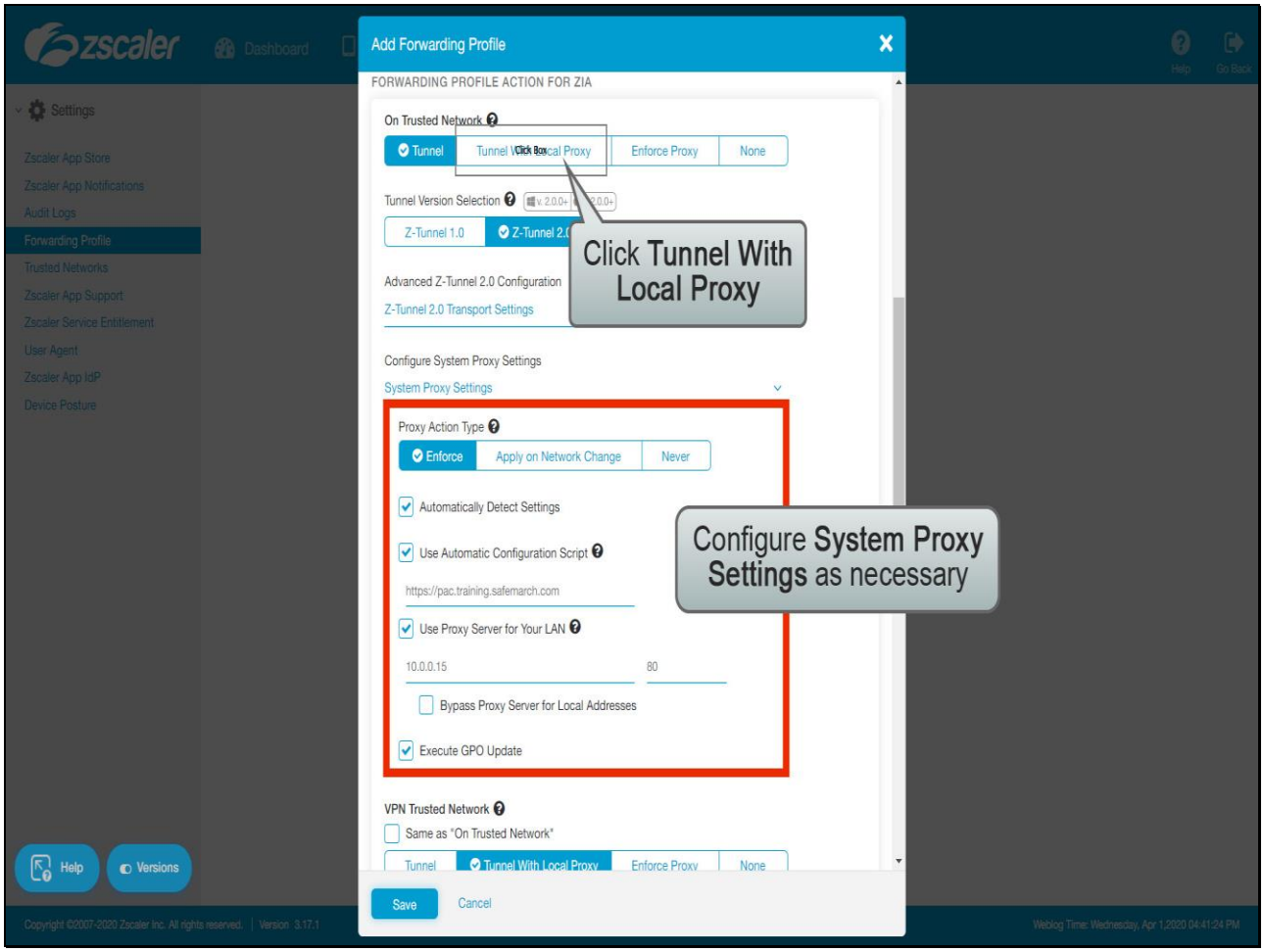
In the **Z-Tunnel 2.0 Transport Selection** settings, you can:

- Select the primary protocol for the tunnels (**DTLS** by default, or **TLS**);
- Control **Connection Timeout** settings for **DTLS** and **TLS**, plus you can set an **MTU for Zscaler Adapter**;
- You can also specify whether to Allow Fallback to **TLS** and/or **Z-Tunnel 1.0**.

Under most circumstances the default settings here should be fine, we would not recommend changing the defaults unless under special circumstances.

Click to collapse the **Z-Tunnel 2.0 Transport Selection** section, ...

Slide 19 - Slide 19

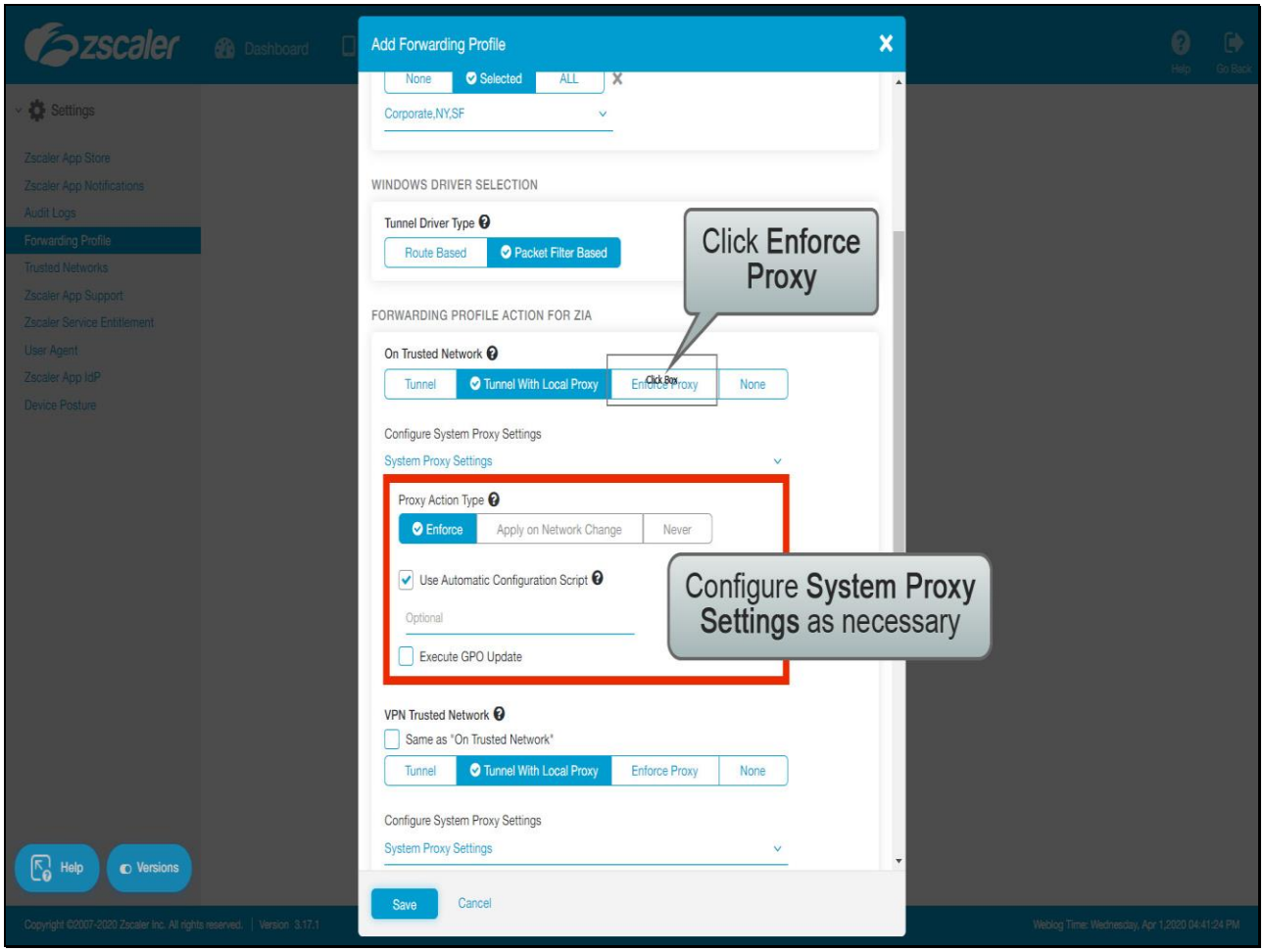


Slide notes

...and configure the **System Proxy Settings** as necessary, these are identical to the **Tunnel 1.0** settings.

If you want to have Zscaler App listen on a local proxy port for the traffic to send into an HTTP CONNECT tunnel, click the **Tunnel With Local Proxy** option.

Slide 20 - Slide 20



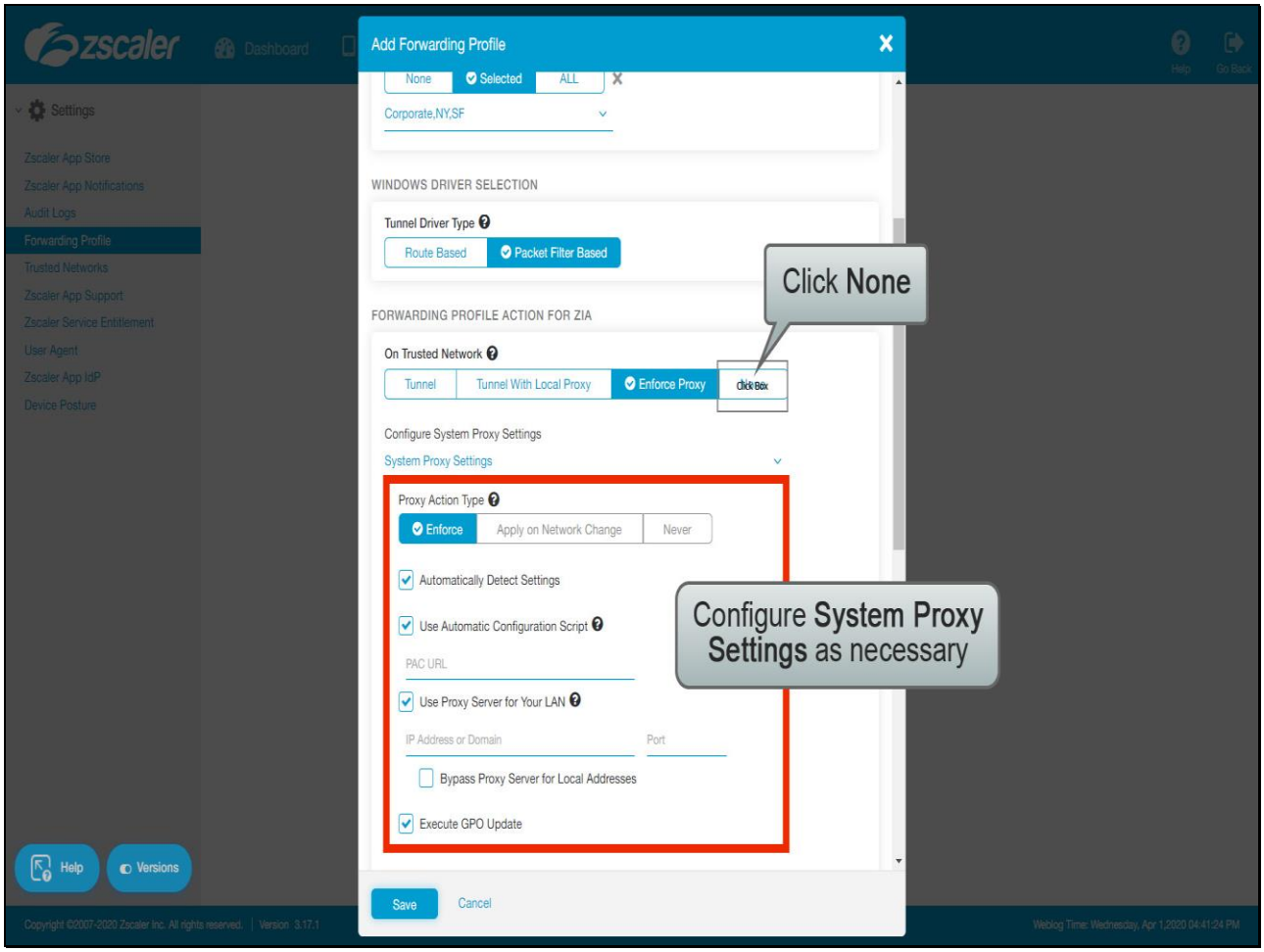
Slide notes

With this option, traffic that follows the proxy definition (which means primarily HTTP and HTTPS) will be forwarded to the loopback address, on port **9000** by default (although this can be changed if necessary). Zscaler App will listen for traffic on the configured port and will tunnel it using the **Tunnel 1.0** method to the closest ZEN, or to the ZEN specified in the **App Profile** PAC file. Note that **Tunnel 2.0** is not supported for this method.

The only **System Proxy Settings** available for this mode is the **Enforce** option, either with the default or a custom **Configuration Script** (PAC file), or with the **Execute GPO Update** option. Any PAC file used for this mode must contain the **${ZAPP_LOCAL_PROXY}** macro as the destination. The default PAC file contains this automatically, any custom file that you apply must also contain this macro.

To forward traffic to Zscaler without any tunnels, click the **Enforce Proxy** option.

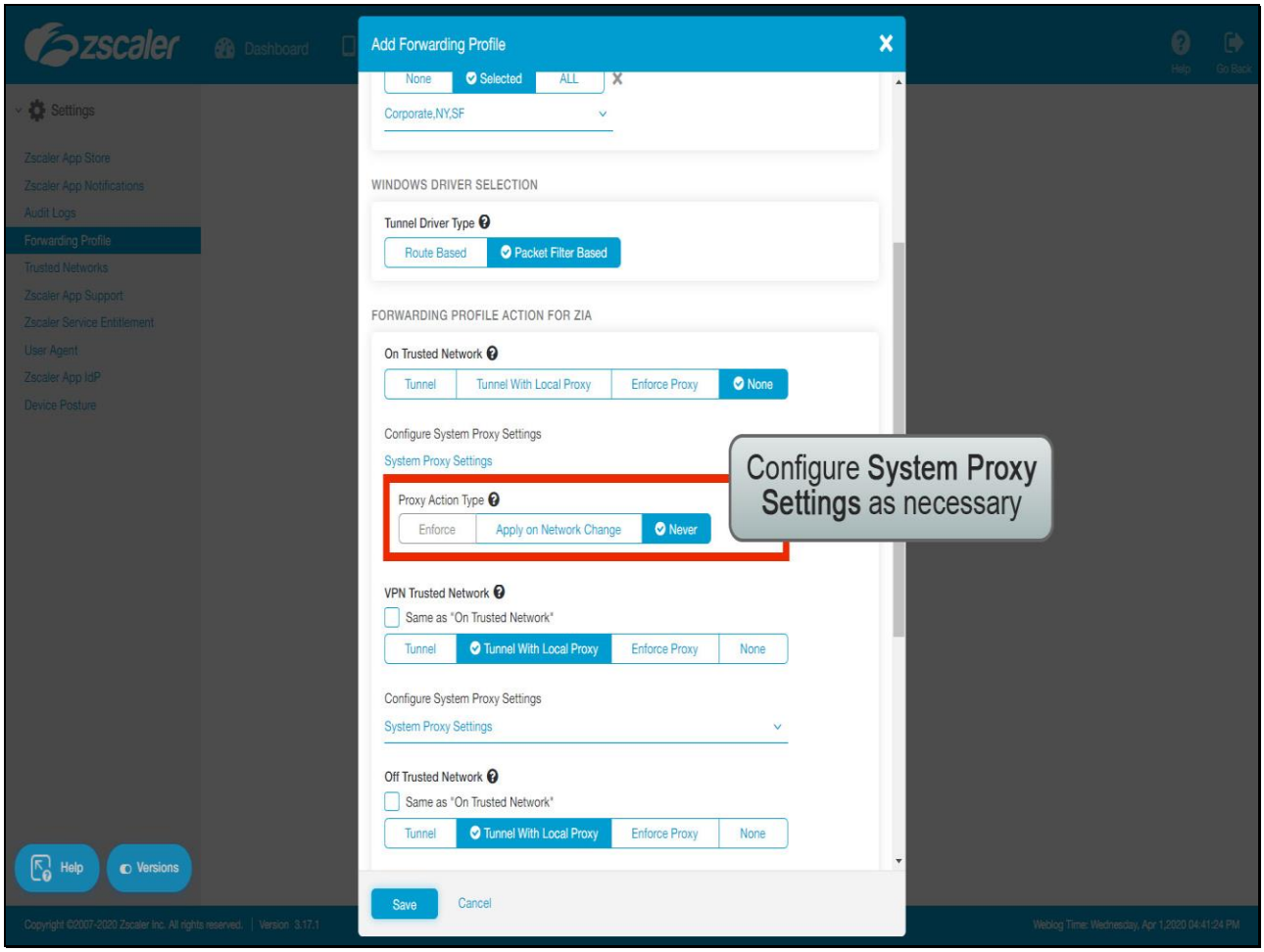
Slide 21 - Slide 21



Slide notes

Once again, the only **System Proxy Settings** available for this mode is the **Enforce** option, however this time with full range of proxy configuration options (as discussed for **Tunnel 1.0**). To turn off forwarding to Zscaler completely, click the **None** option.

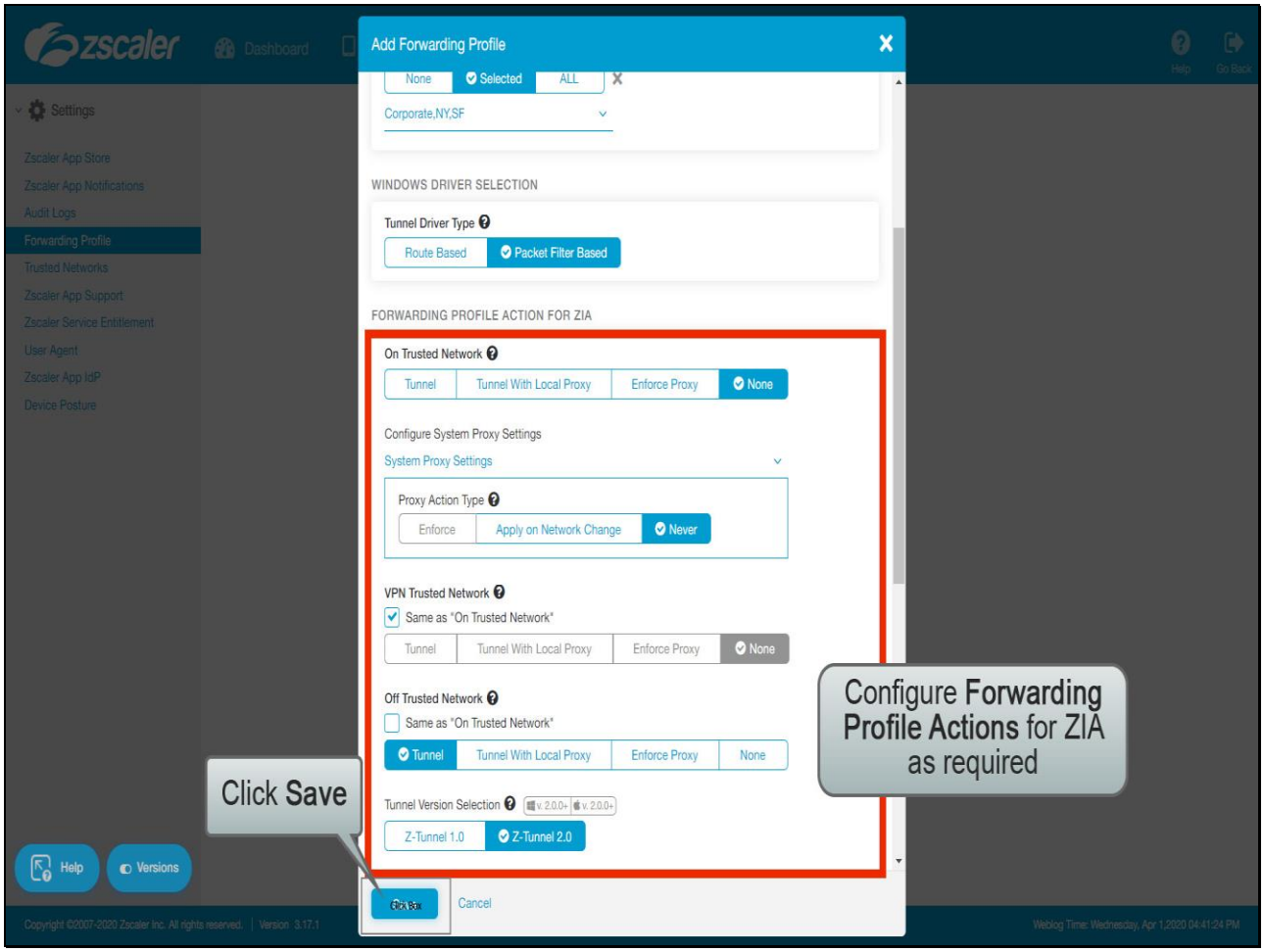
Slide 22 - Slide 22



Slide notes

In this case, the **System Proxy Settings** available are **Apply on Network Change** and **Never** (the default option). If you select the **Apply on Network Change** option, this gives you the full range of proxy configuration options (as discussed for **Tunnel 1.0**).

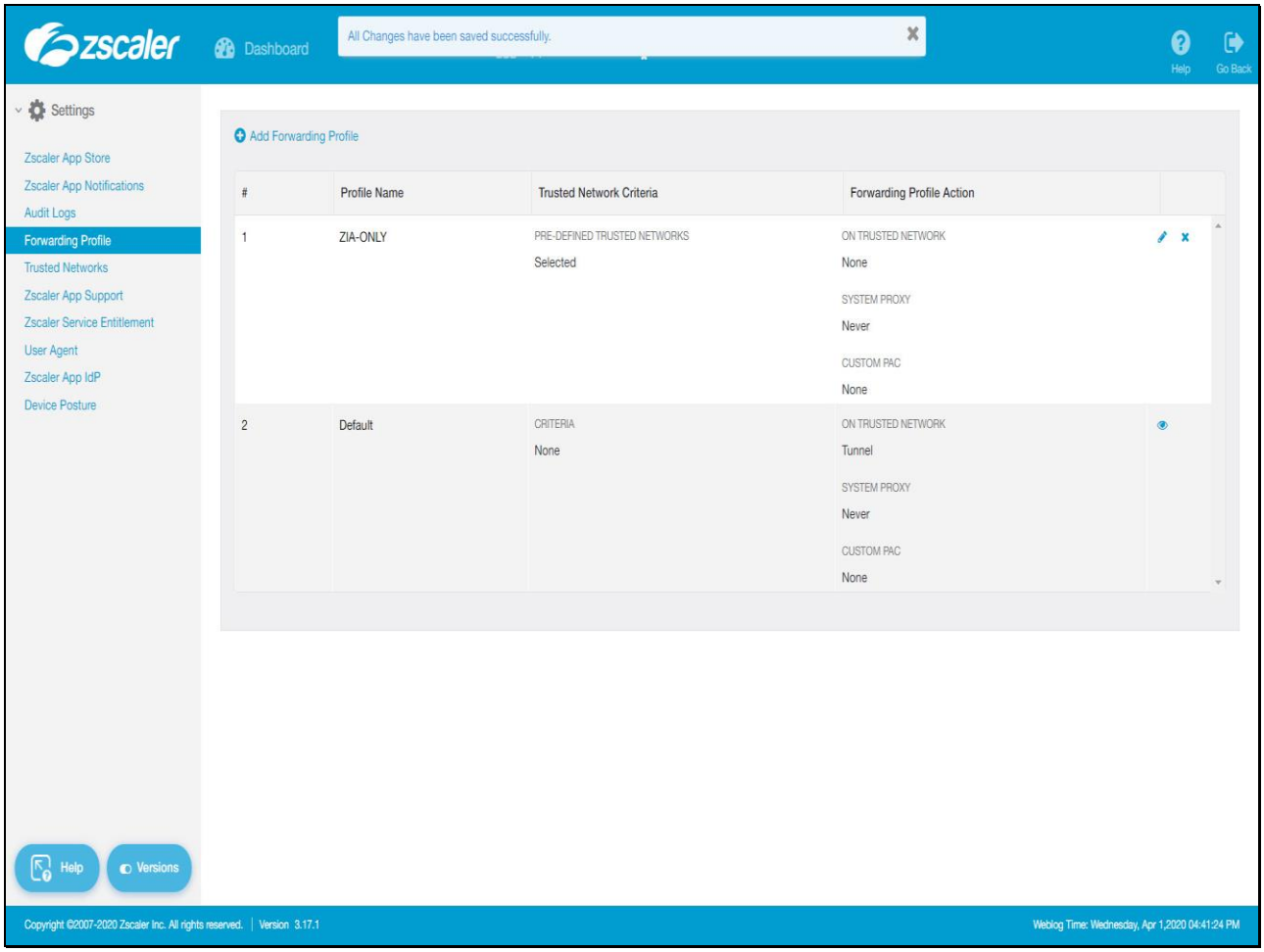
Slide 23 - Slide 23



Slide notes

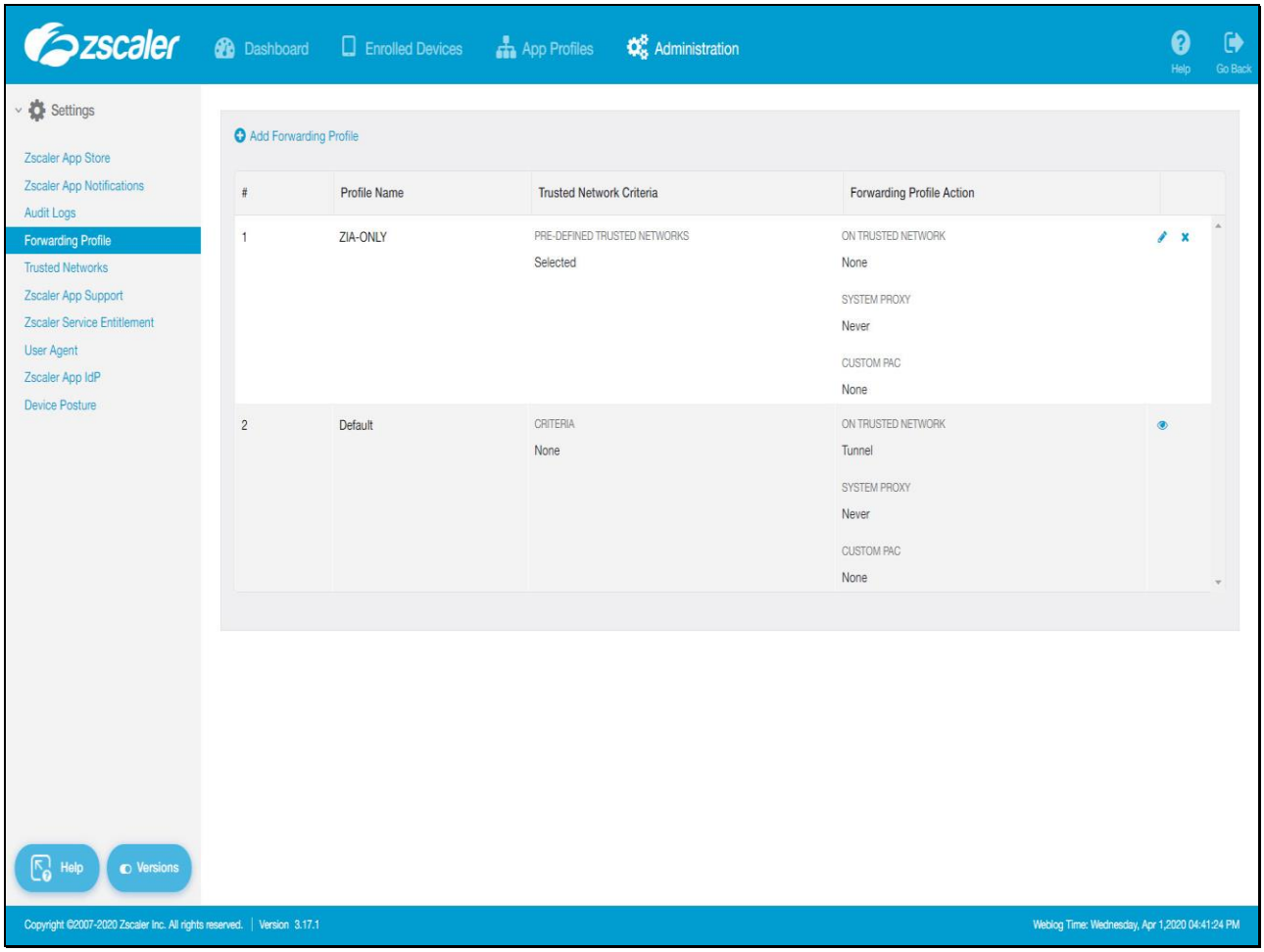
Set the forwarding options as required for your environment and click **Save**.

Slide 24 - Slide 24



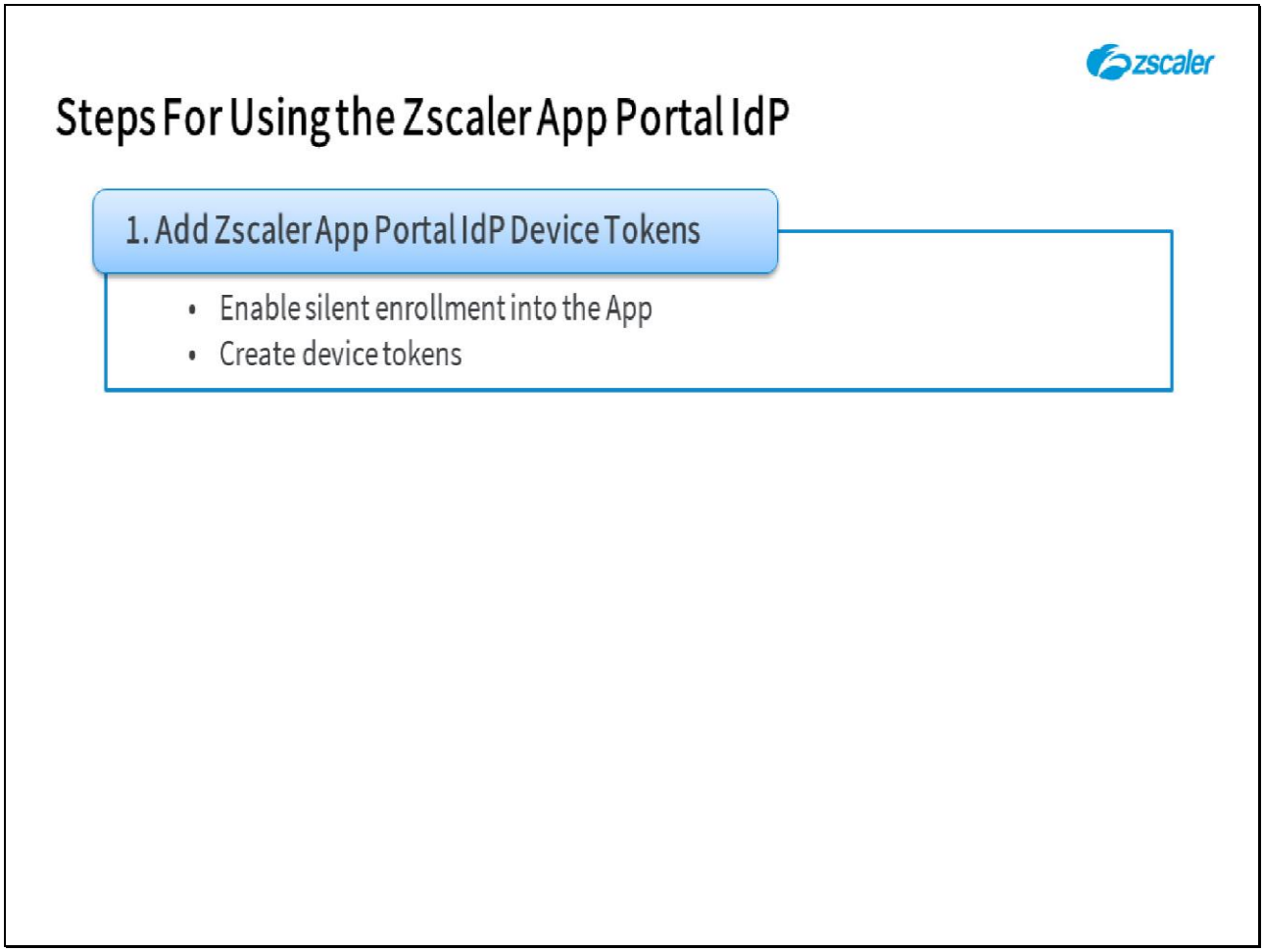
Slide notes

Slide 25 - Slide 25



Slide notes

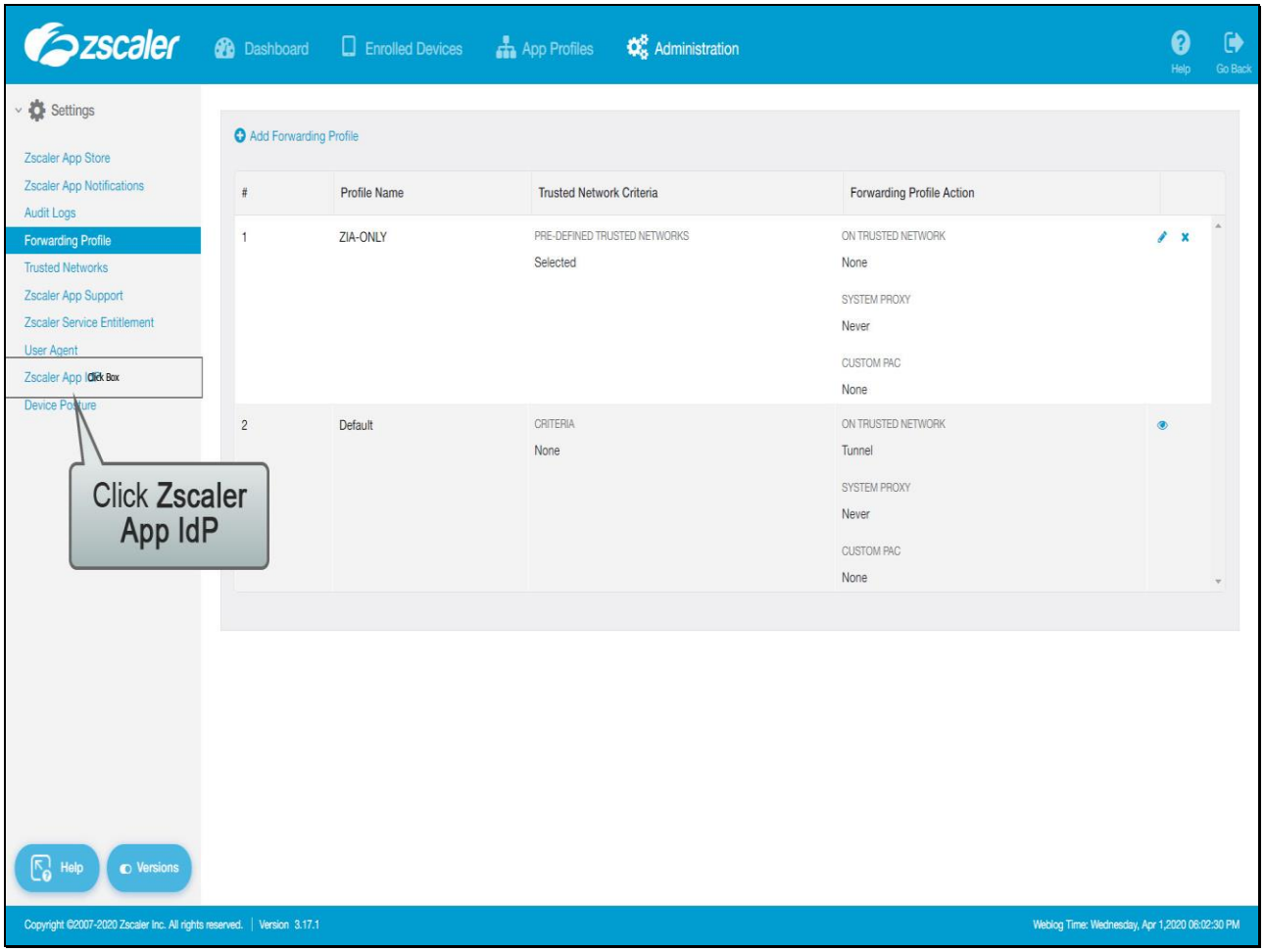
Slide 26 - Using the Zscaler App IdP for ZIA



Slide notes

The **Zscaler App Portal IdP** provides an option for silently enrolling ZIA users into the Zscaler App so that users are never prompted for login credentials. They are authenticated based on the **User ID** used to logon to the device itself and a **Device Token** created for that purpose. Note that this form of silent authentication is not supported to authenticate users for ZPA.

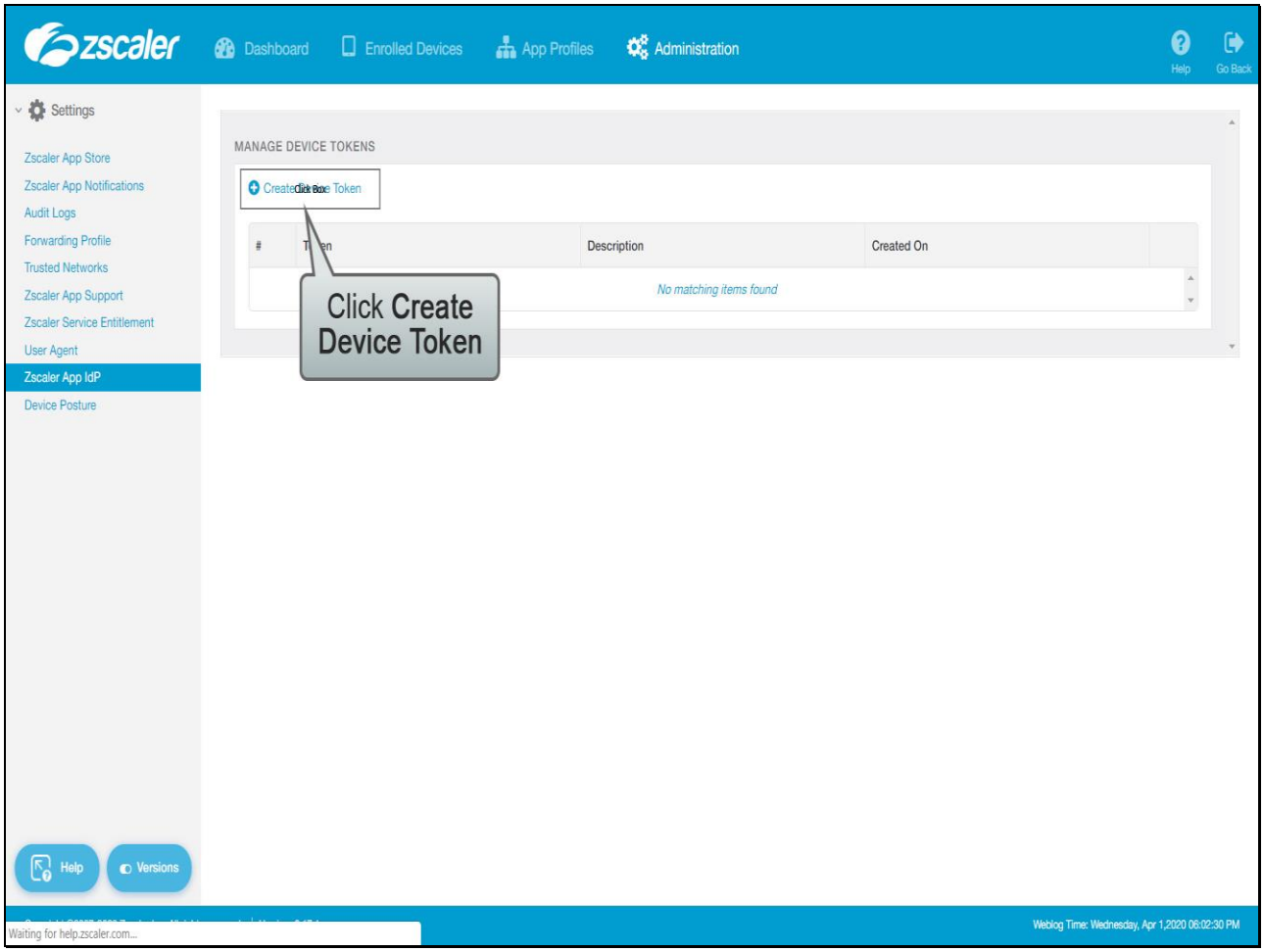
Slide 27 - Slide 27



Slide notes

To setup the Zscaler App Portal to act as a SAML Identity Provider (IdP), from the **Administration** page, click **Zscaler App IdP**.

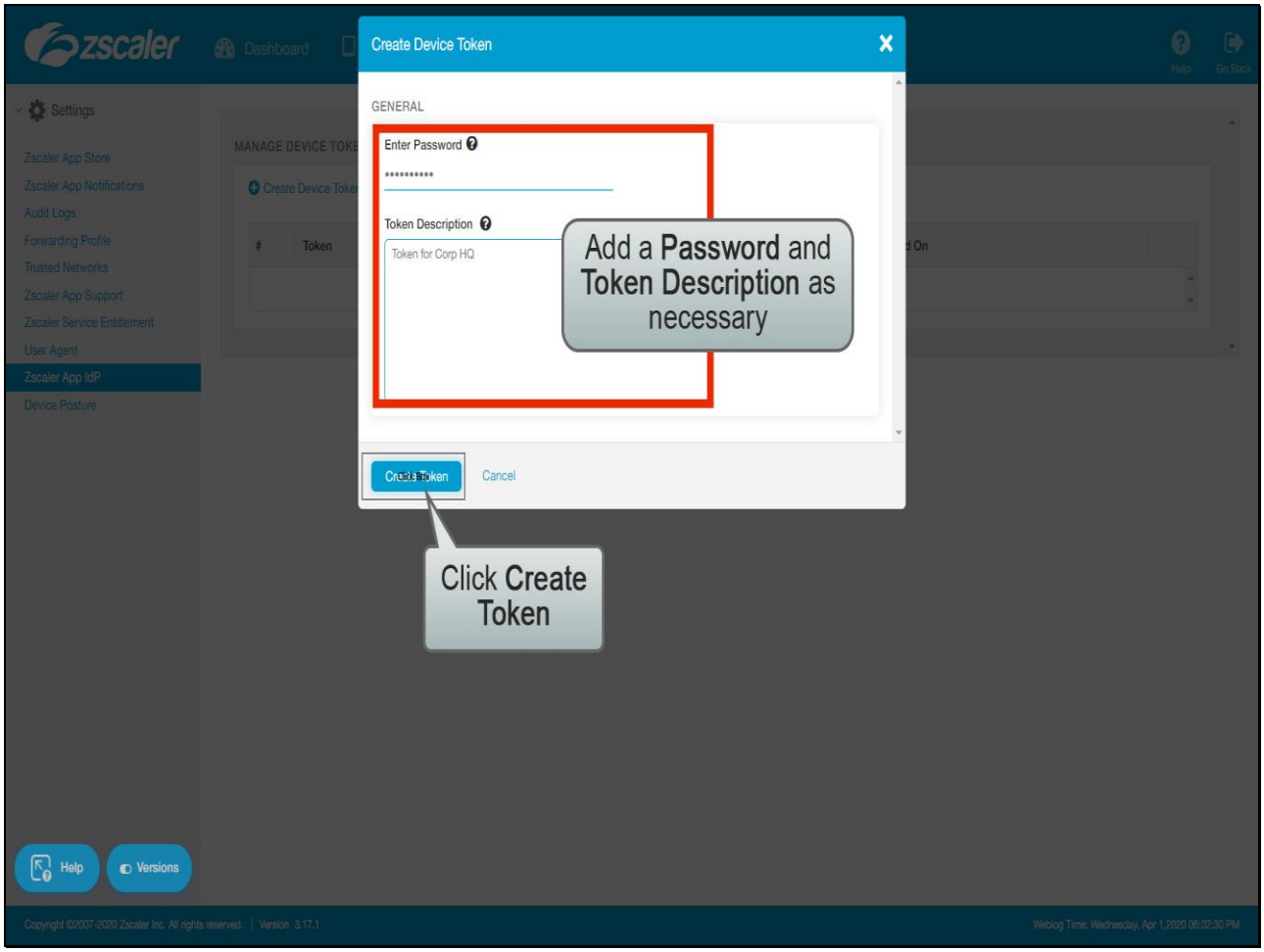
Slide 28 - Slide 28



Slide notes

To create a **Device Token**, to allow a device to authenticate silently to this IdP, click **Create Device Token**.

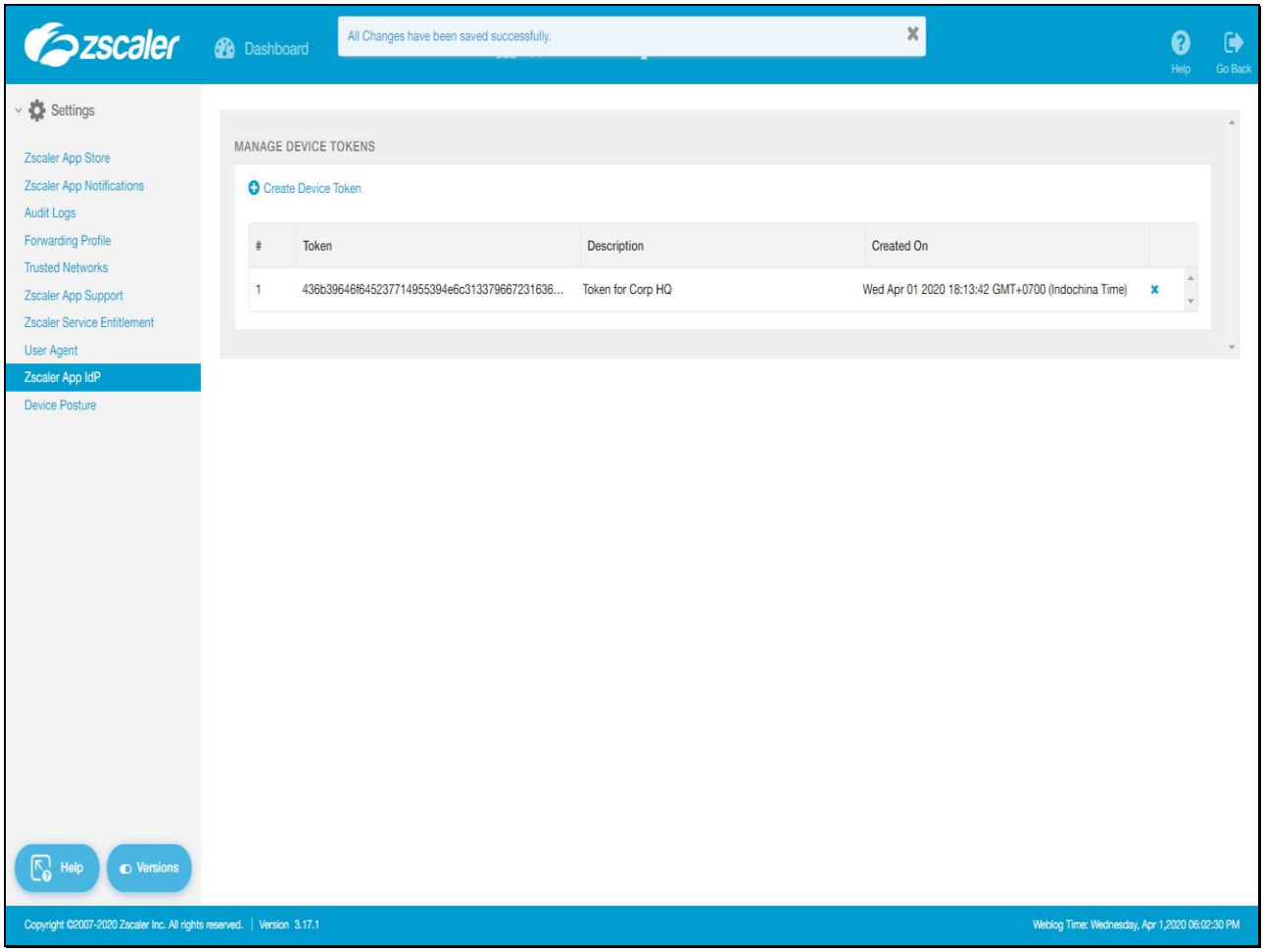
Slide 29 - Slide 29



Slide notes

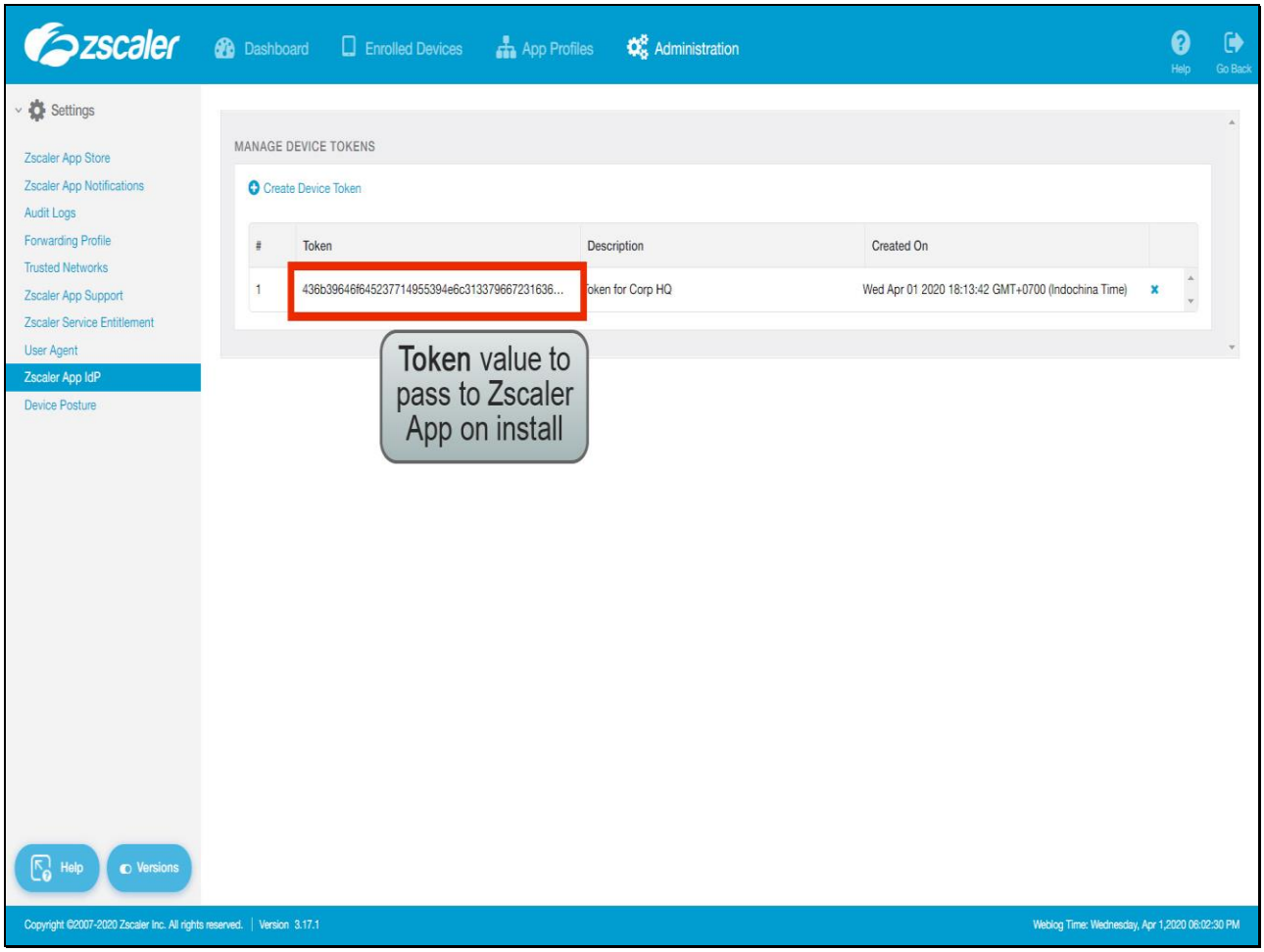
Specify a **Password** for the Token, add a description if necessary, then click **Create Token**.

Slide 30 - Slide 30



Slide notes

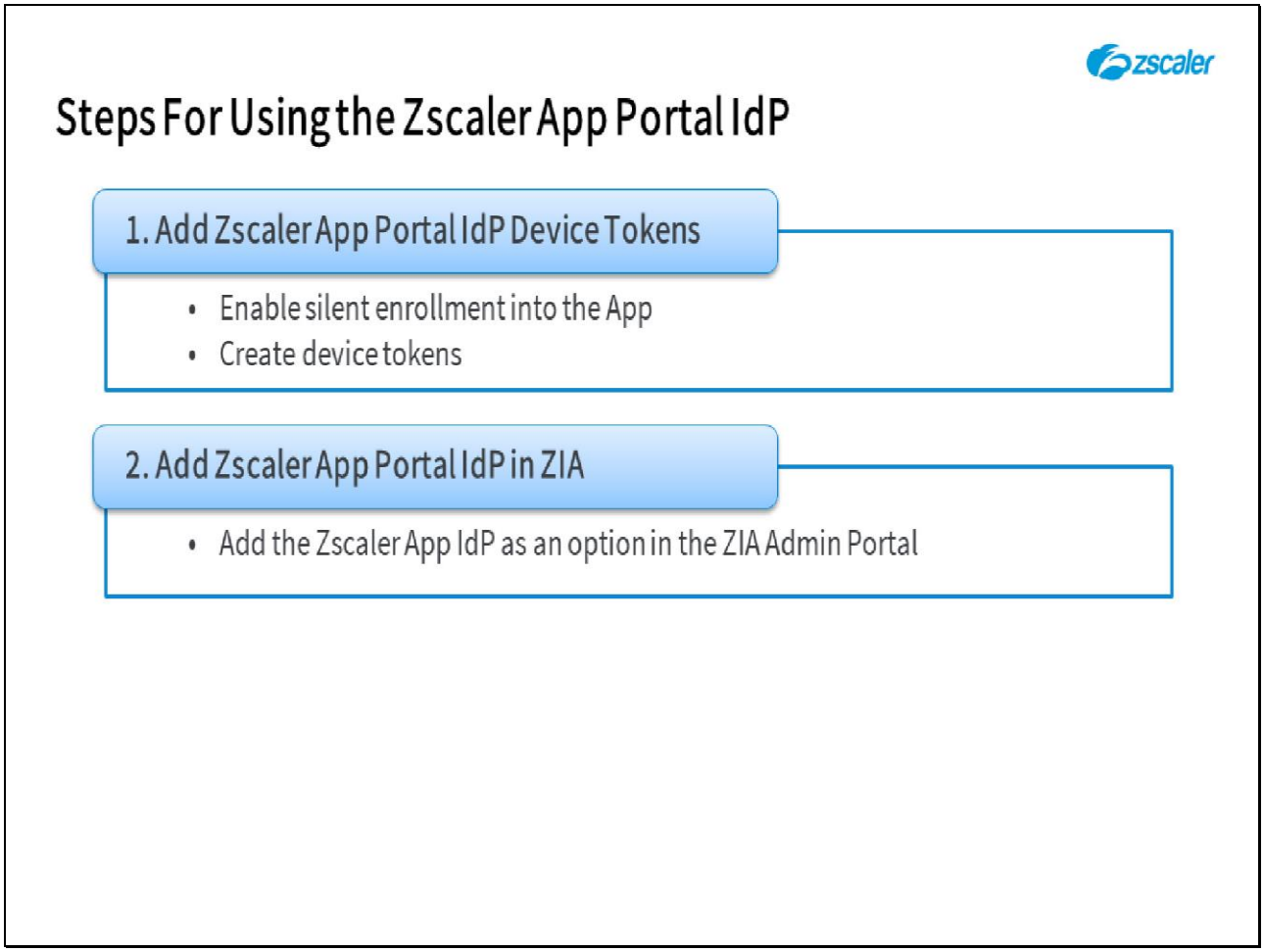
Slide 31 - Slide 31



Slide notes

Up to eight **Device Tokens** can be created, and the token values passed to the App during installation using the **--deviceToken** install option.

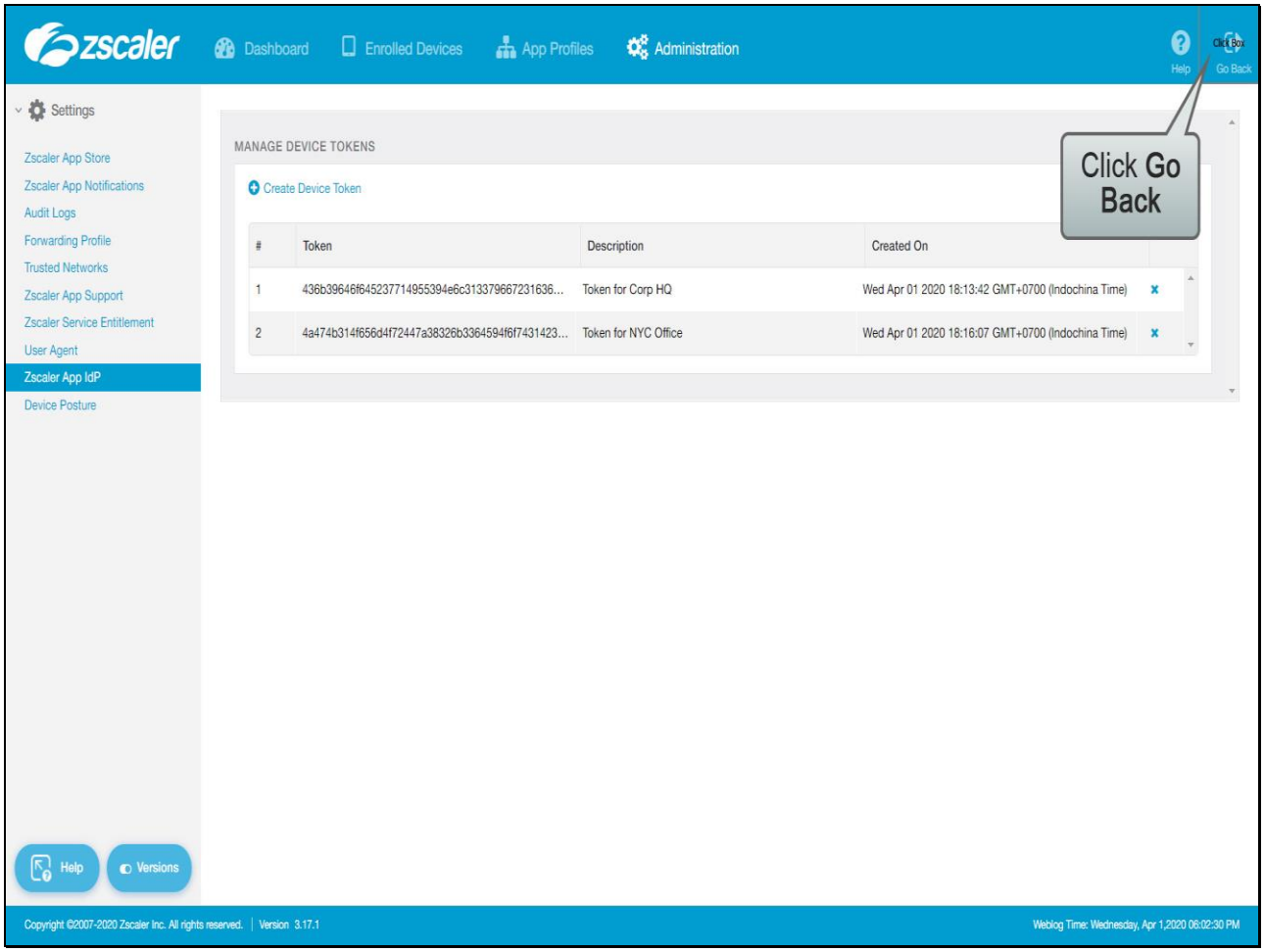
Slide 32 - Steps For Using the Zscaler App IdP



Slide notes

The ZIA Admin Portal must be configured correctly to authenticate users through this IdP.

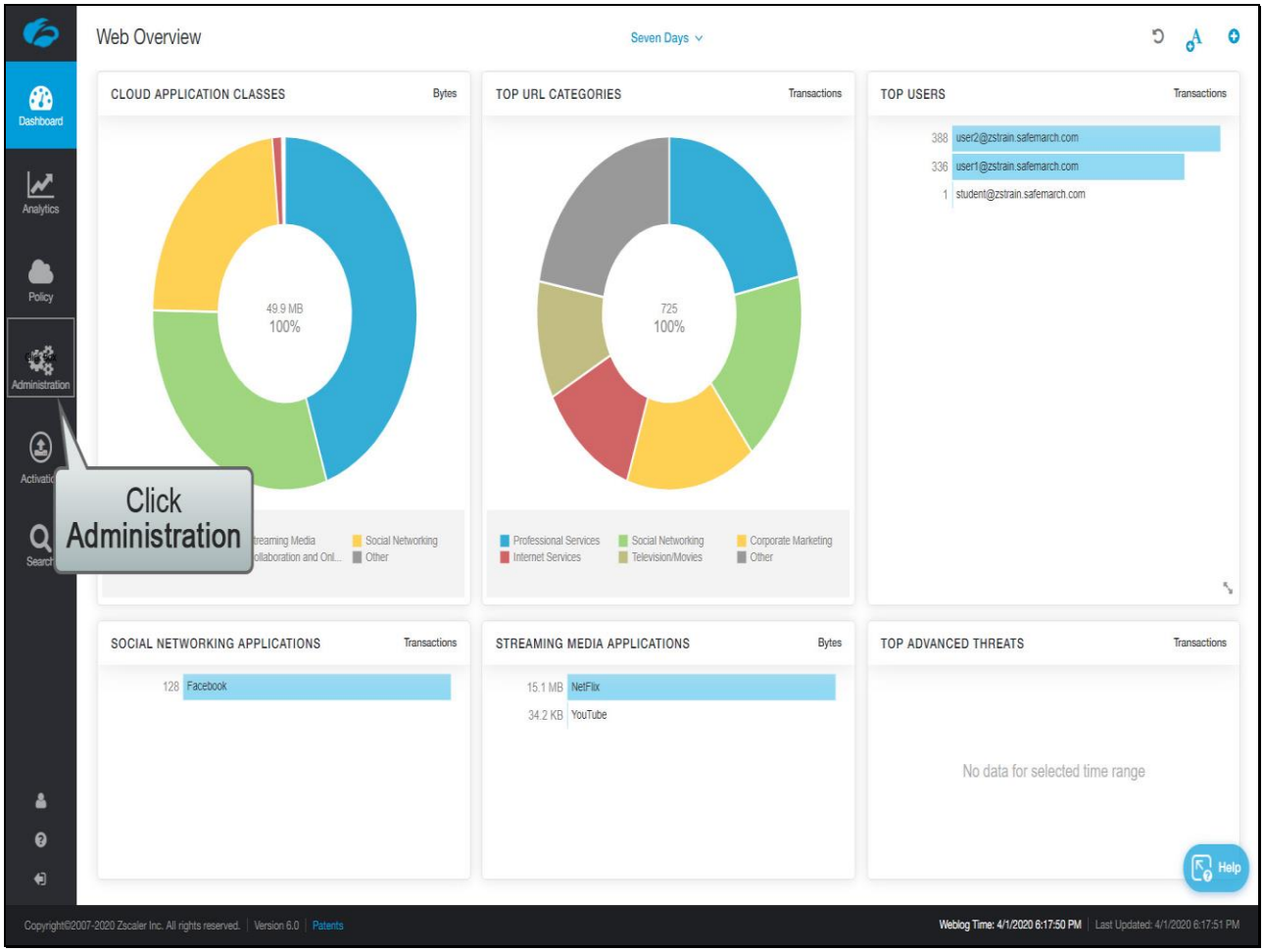
Slide 33 - Slide 33



Slide notes

To return to the ZIA Admin Portal, from the Zscaler App Portal, click **Go Back**.

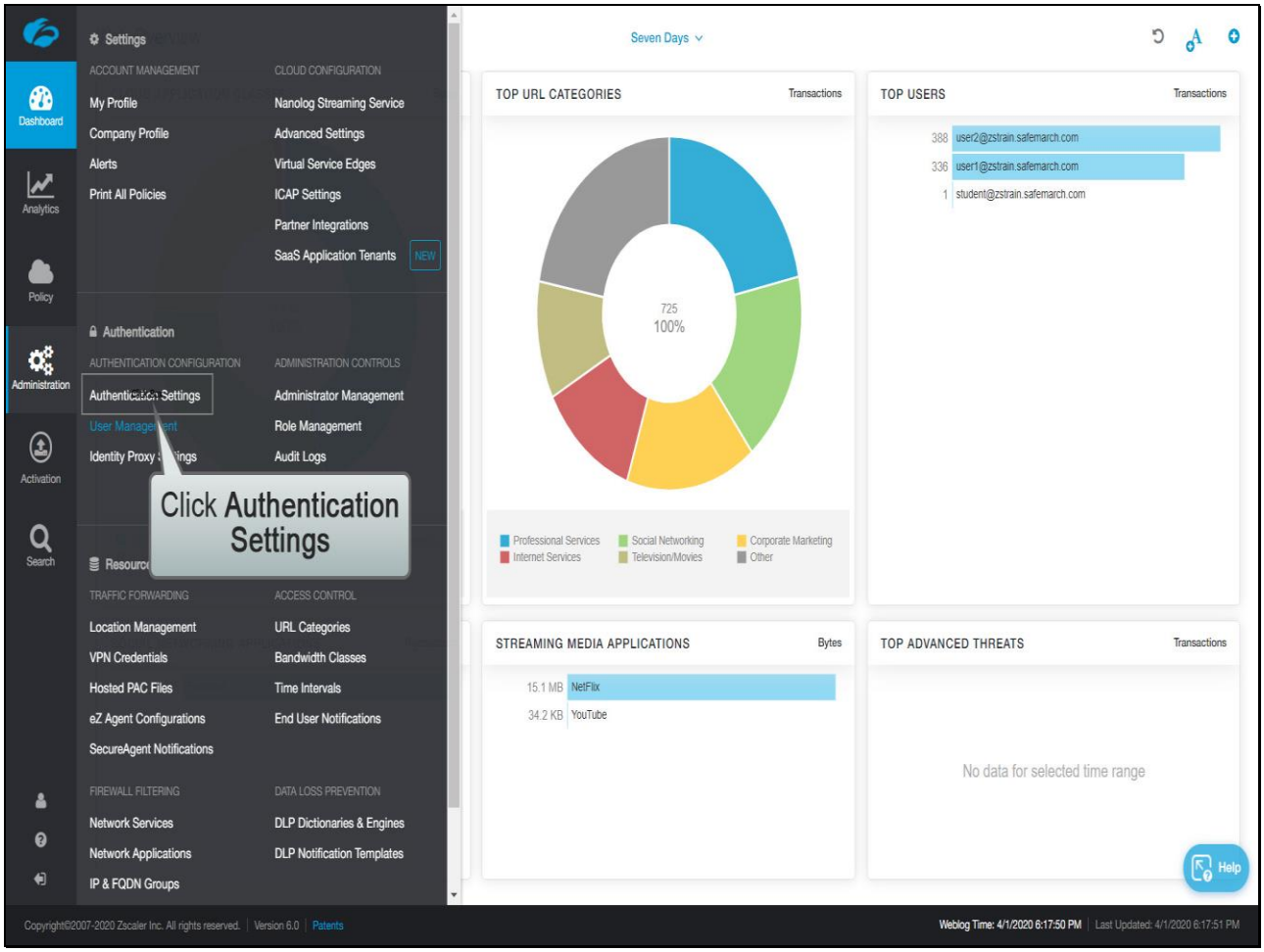
Slide 34 - Slide 34



Slide notes

To configure the Zscaler App Portal IdP, click **Administration**, ...

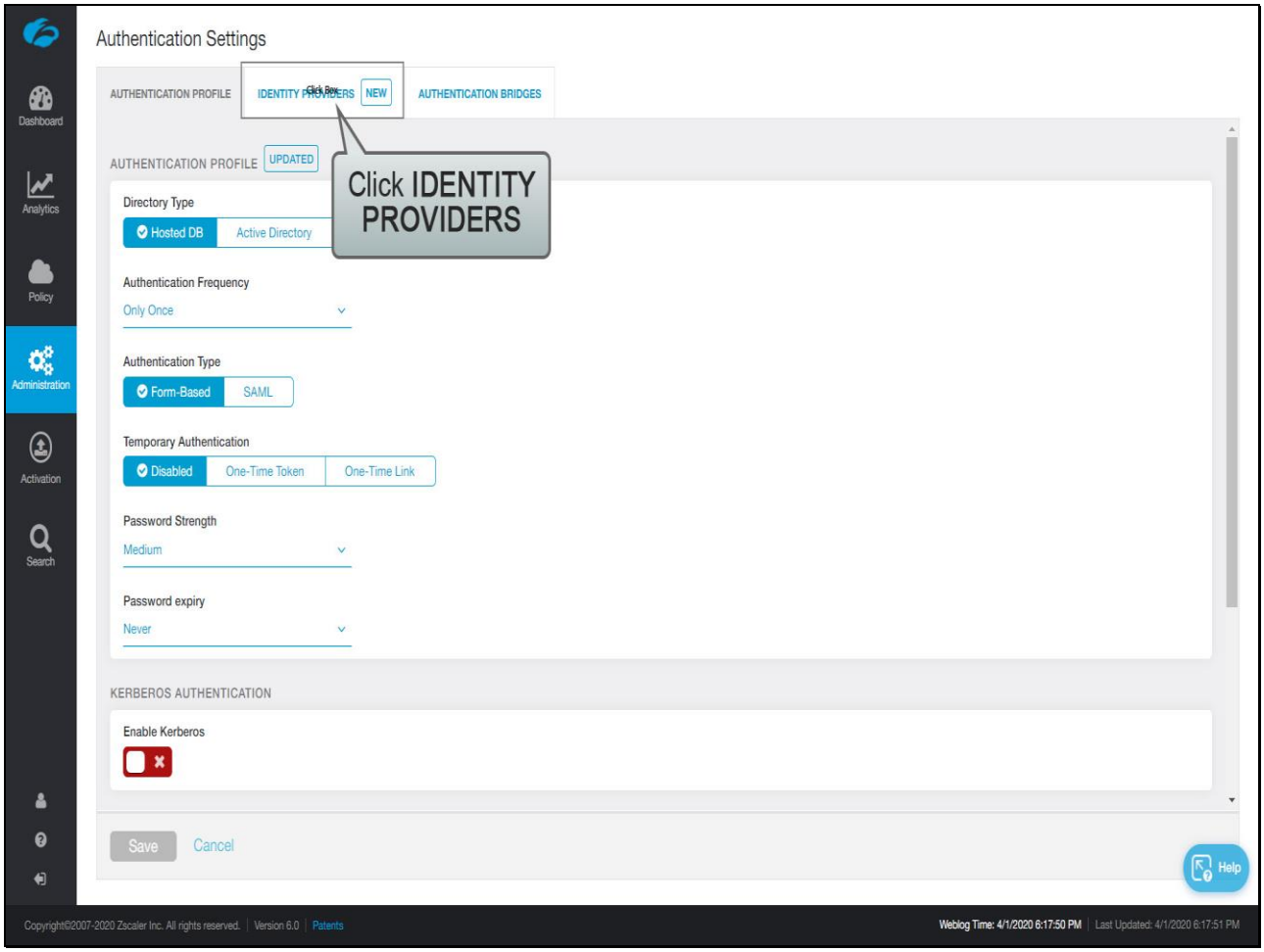
Slide 35 - Slide 35



Slide notes

...then **Authentication Settings**, ...

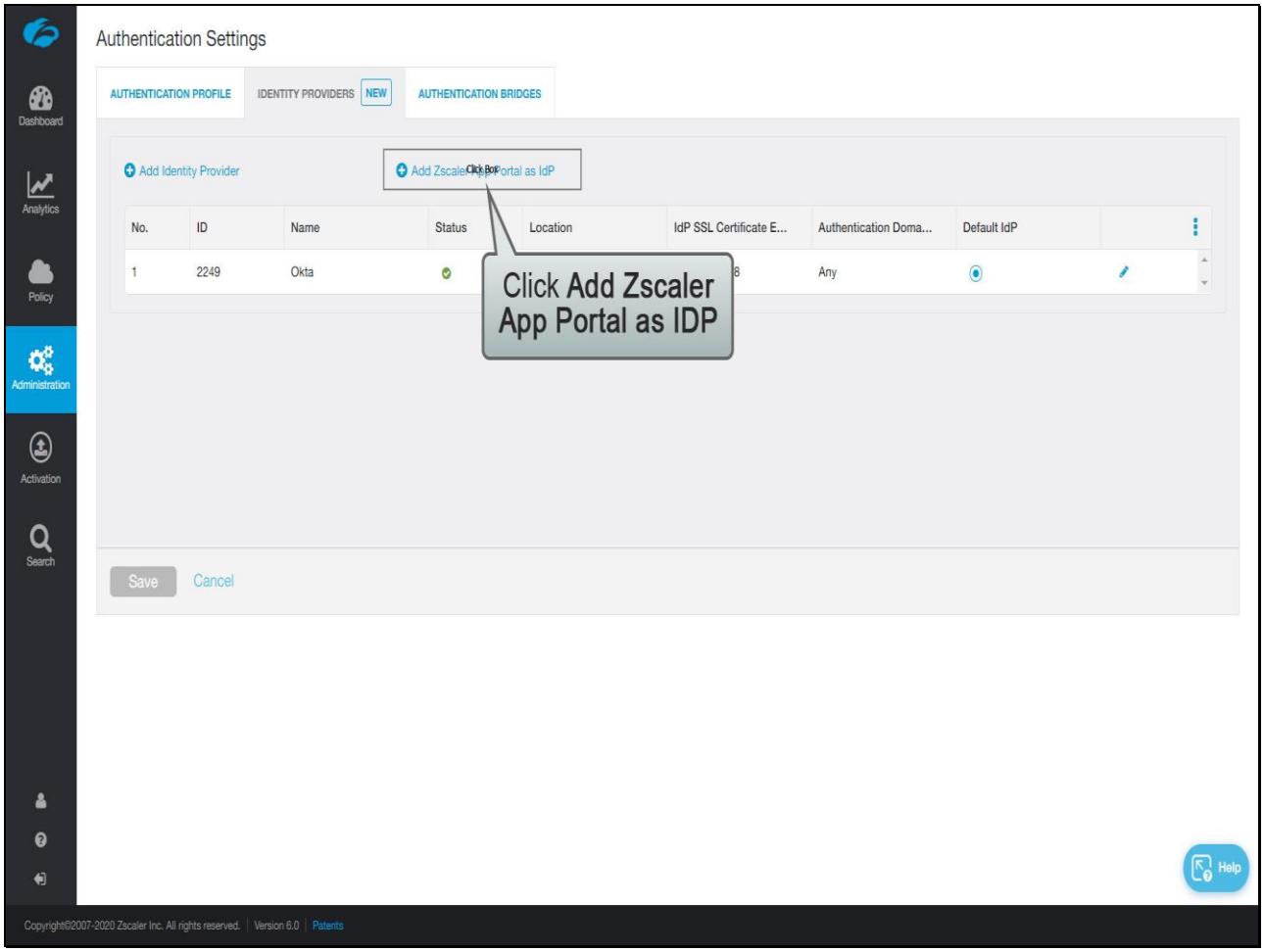
Slide 36 - Slide 36



Slide notes

...then click to open the **IDENTITY PROVIDERS** tab.

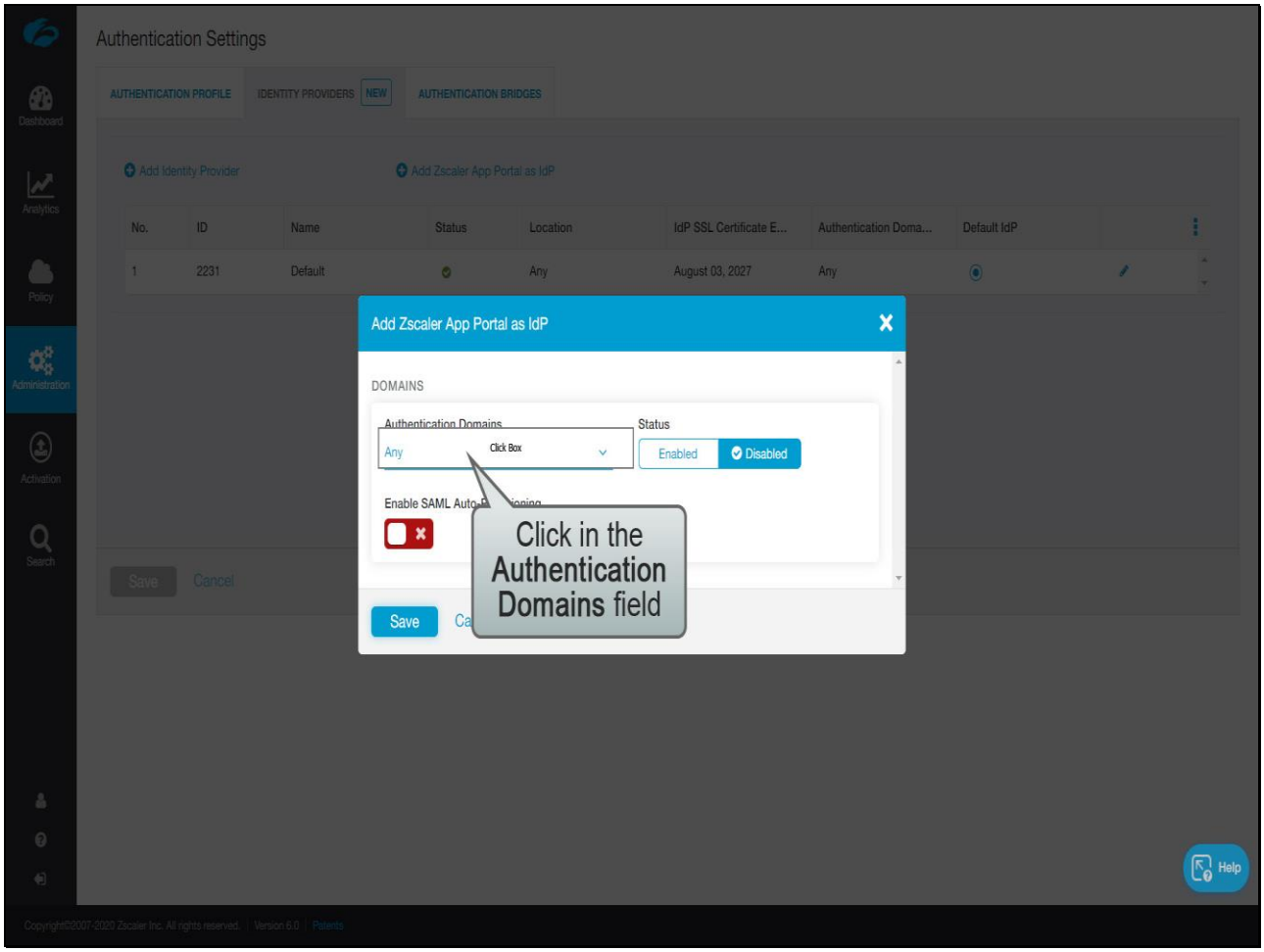
Slide 37 - Slide 37



Slide notes

Click the **Add Scaler App Portal as IdP** link.

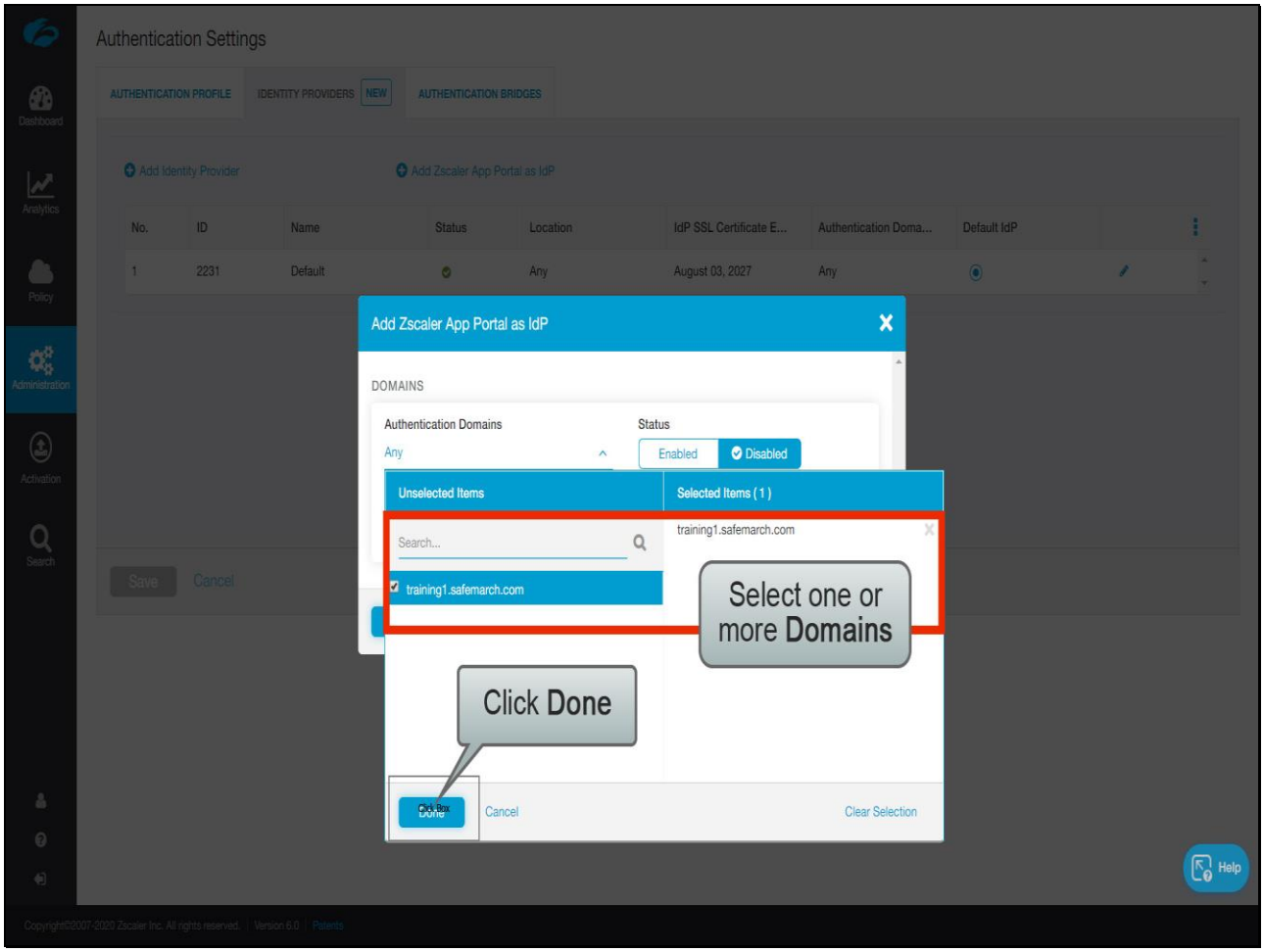
Slide 38 - Slide 38



Slide notes

If this is the only IdP on the system, you must leave the **Authentication Domains** setting at **Any**. Otherwise, click in the field, ...

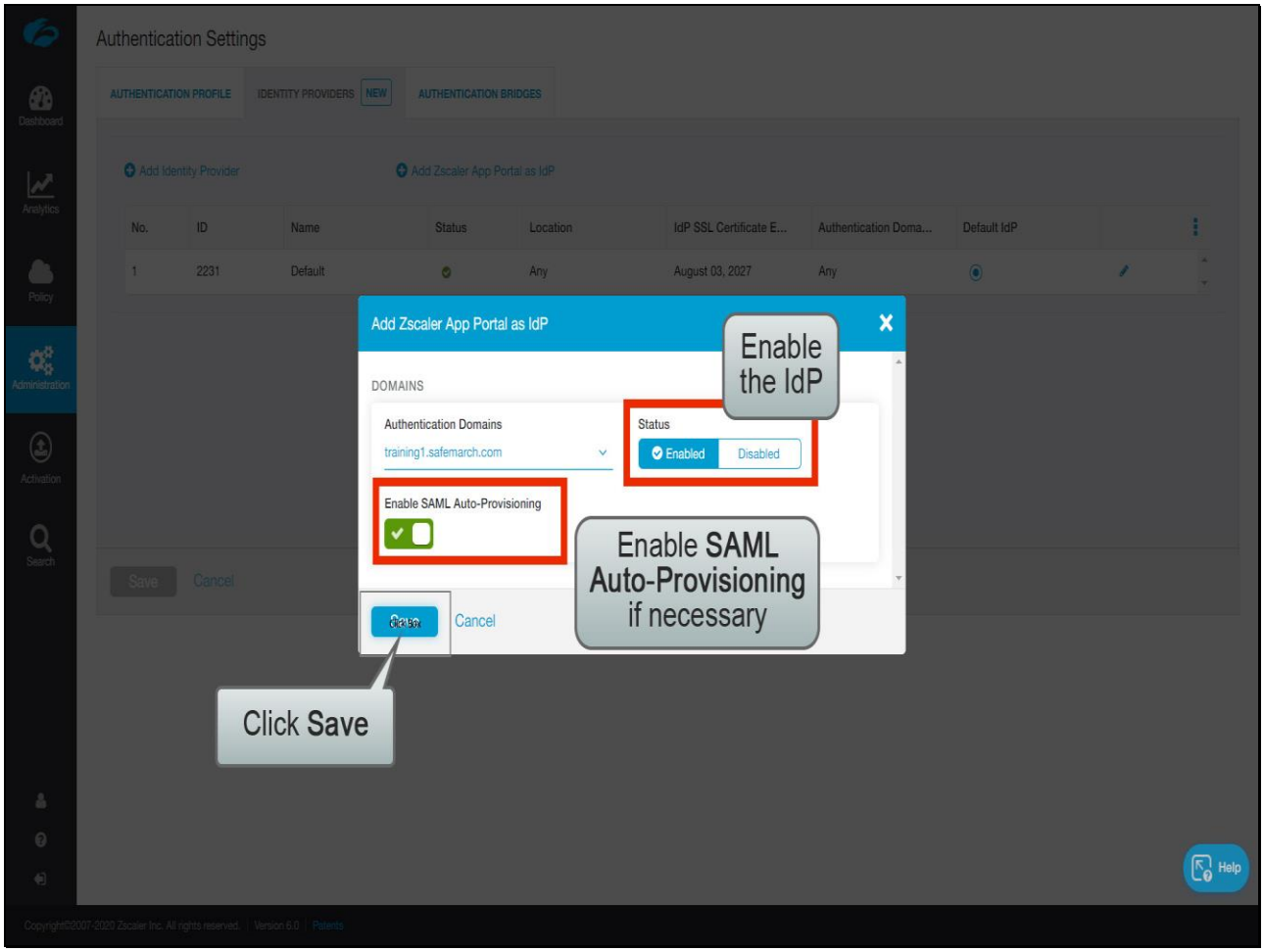
Slide 39 - Slide 39



Slide notes

...to select one or more **Domains**, then click **Done**.

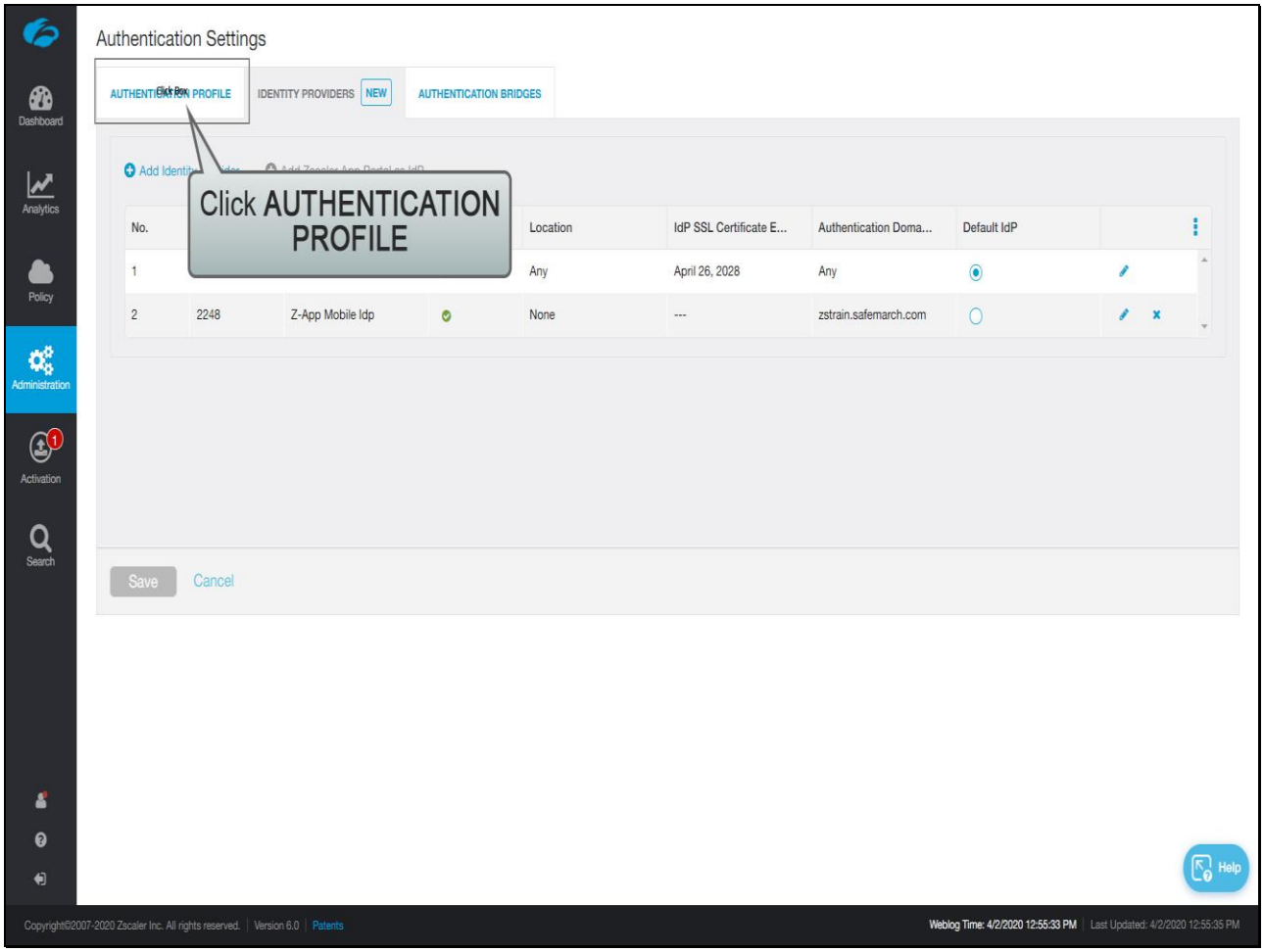
Slide 40 - Slide 40



Slide notes

If you need it, activate the **Enable SAML Auto-Provisioning** option (for example if your users are not yet populated to the ZIA user DB), also make sure that you set this configuration to **Enabled**, then click **Save**.

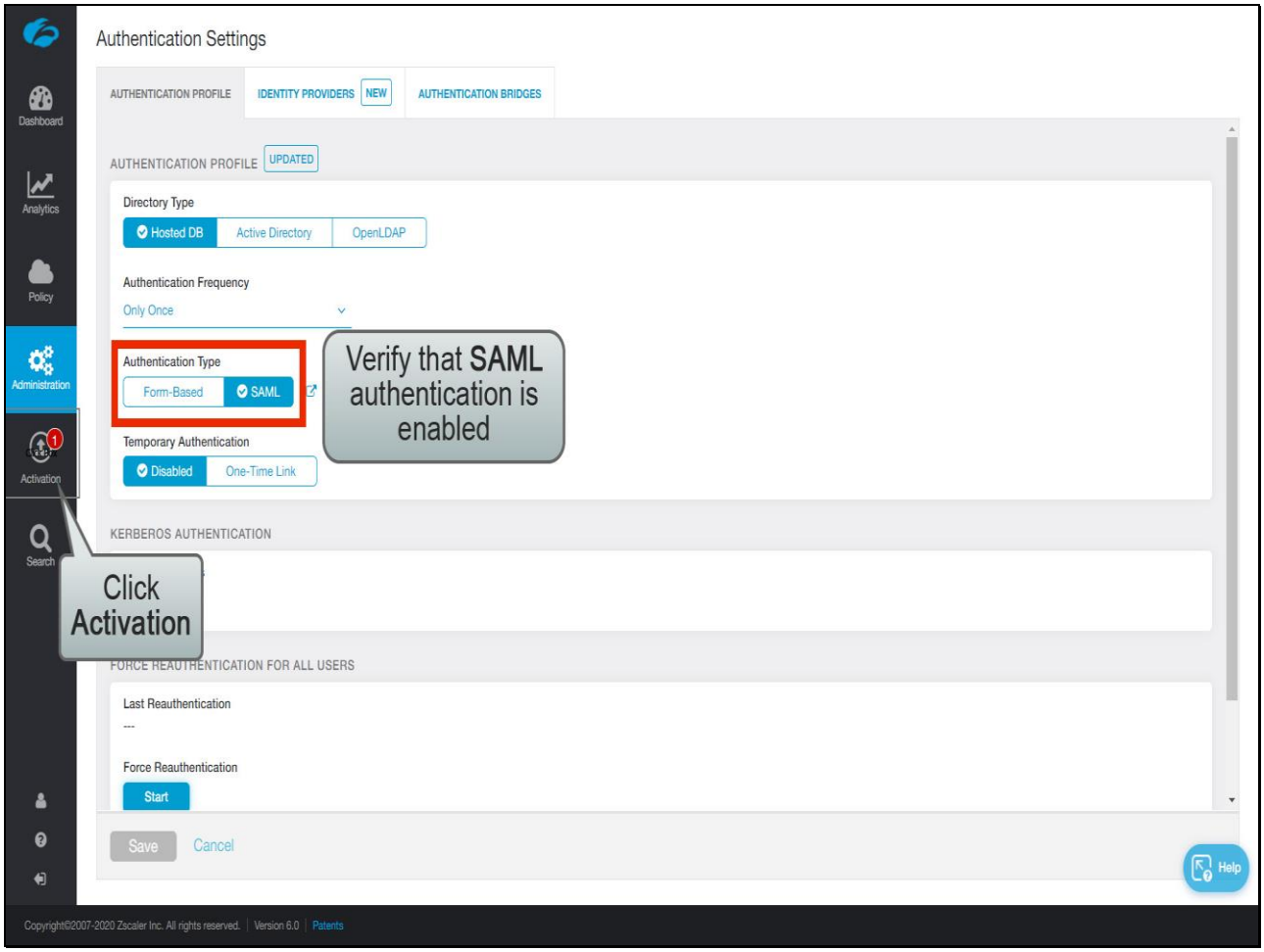
Slide 41 - Slide 41



Slide notes

Now that the IdP has been added, click the **AUTHENTICATION PROFILE** tab, ...

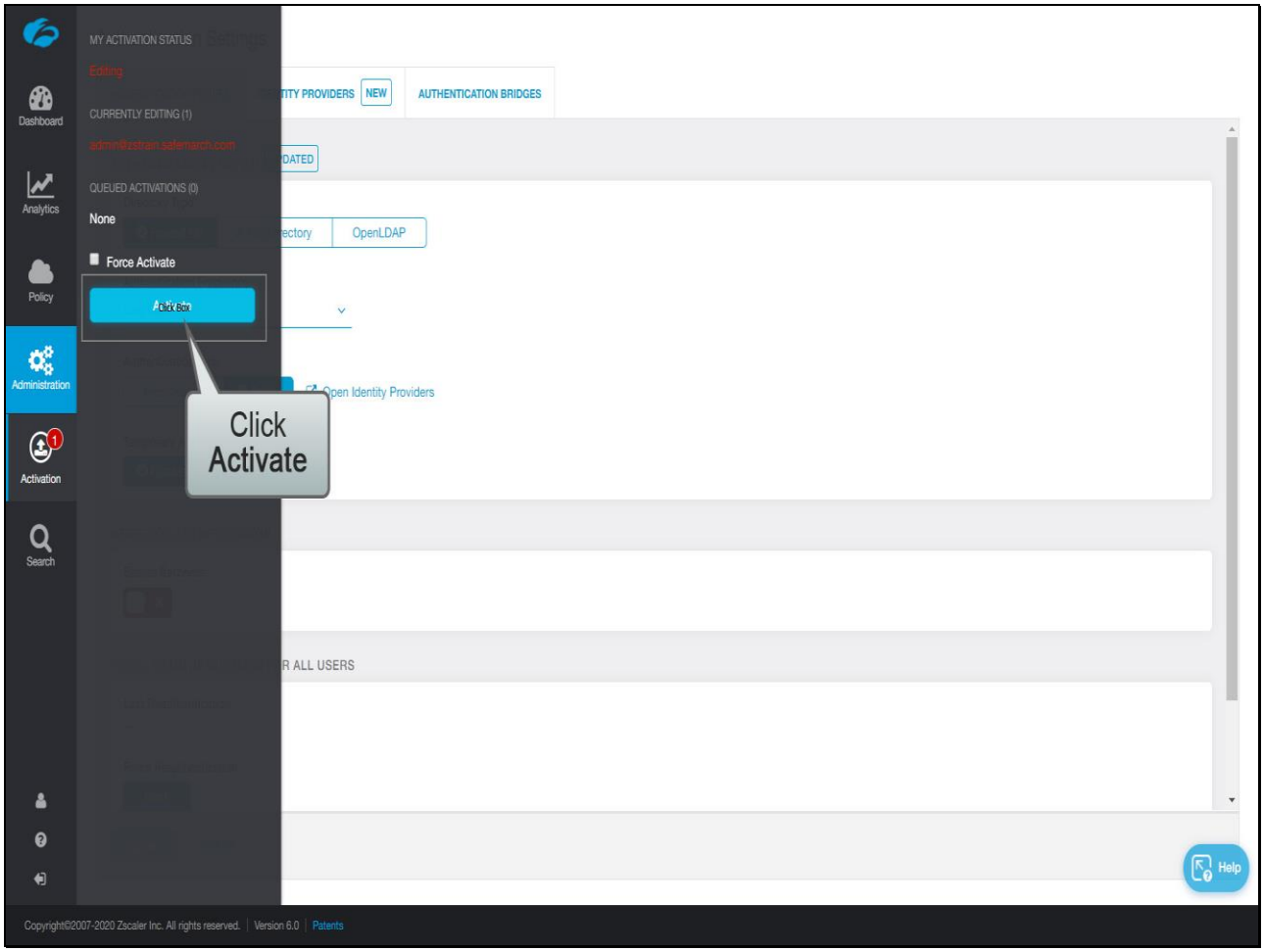
Slide 42 - Slide 42



Slide notes

...and verify that the **Authentication Type** has been set to **SAML**. Then to activate changes, click **Activation**, ...

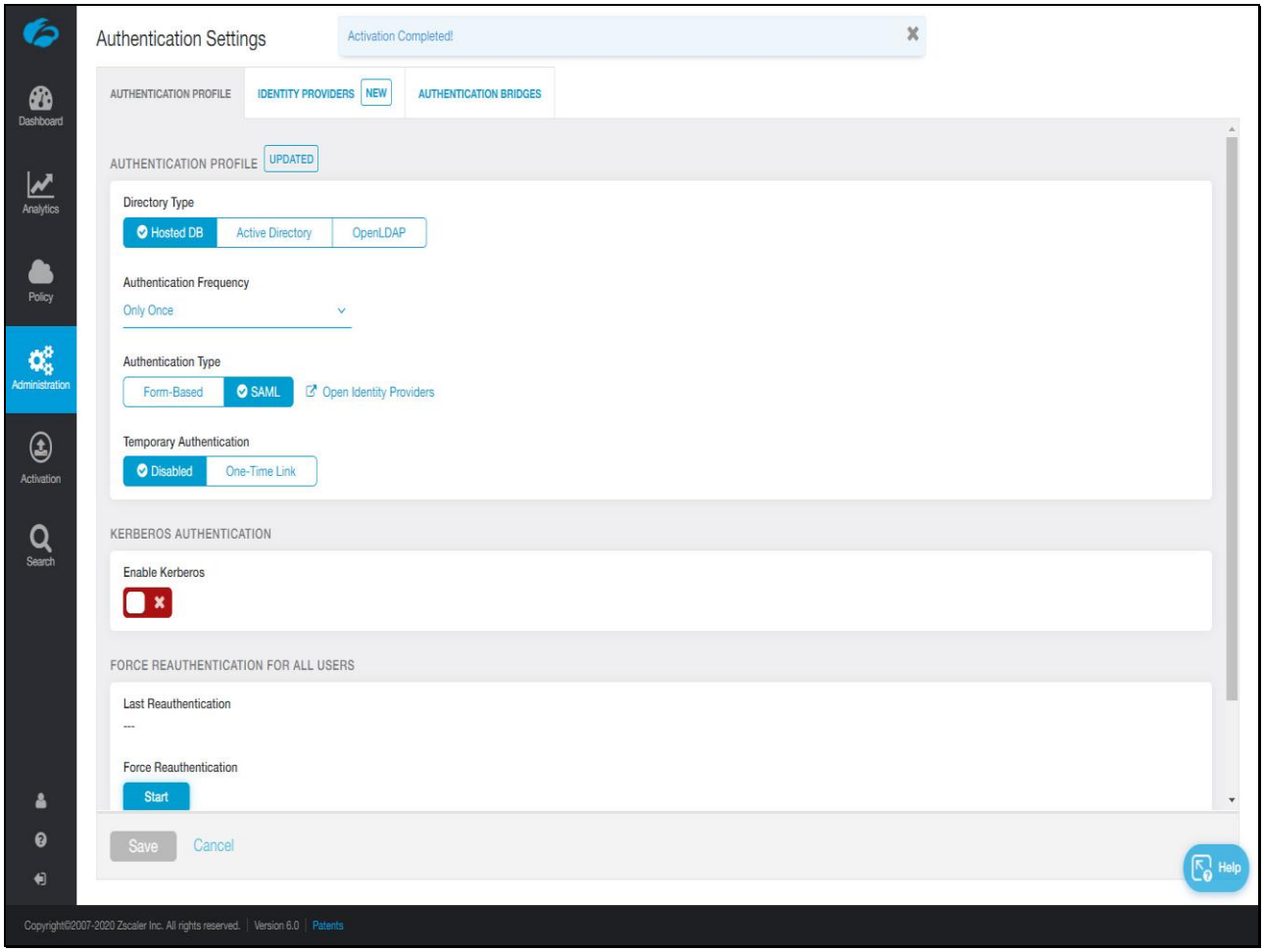
Slide 43 - Slide 43



Slide notes

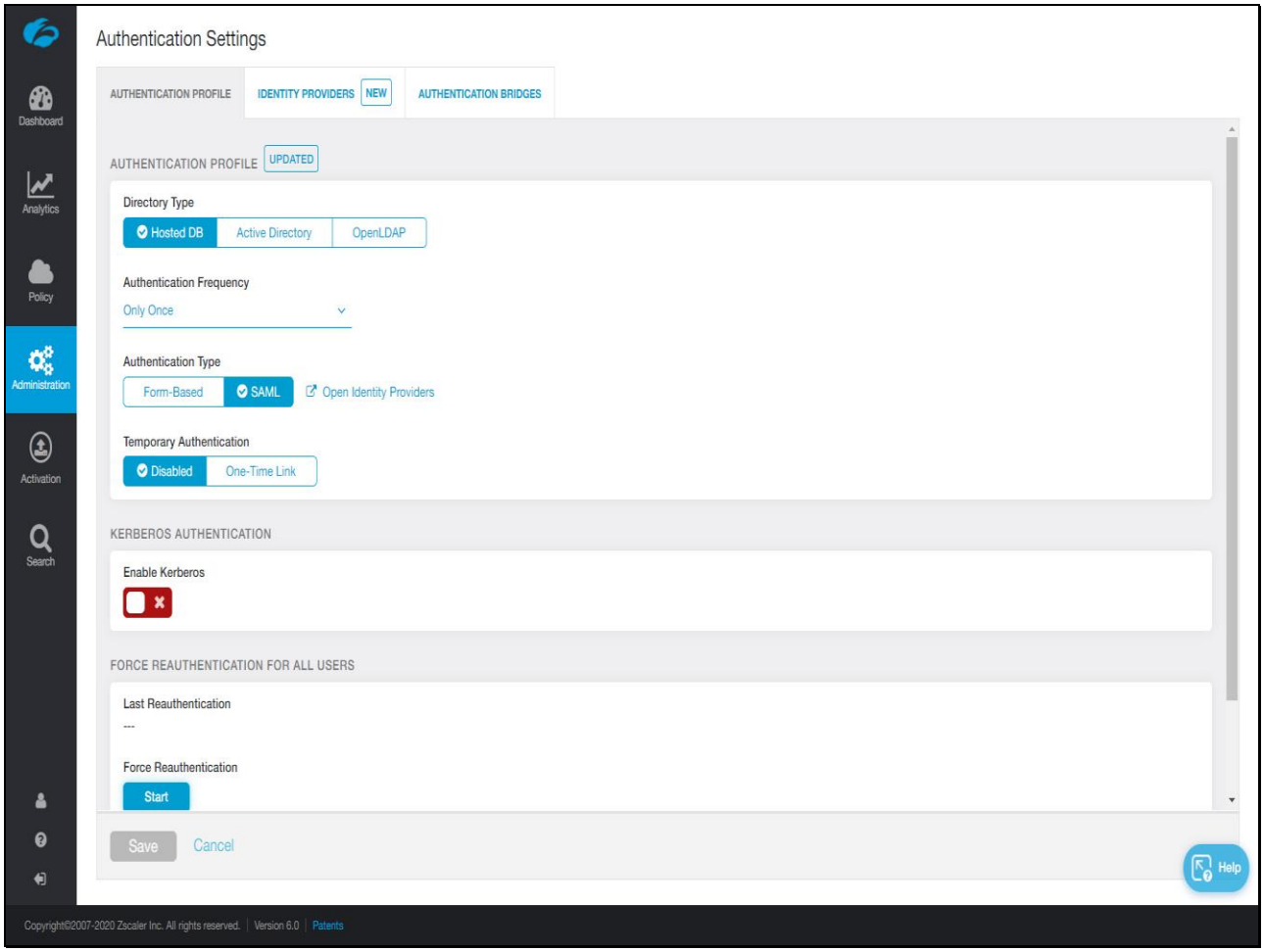
...then **Activate**.

Slide 44 - Slide 44



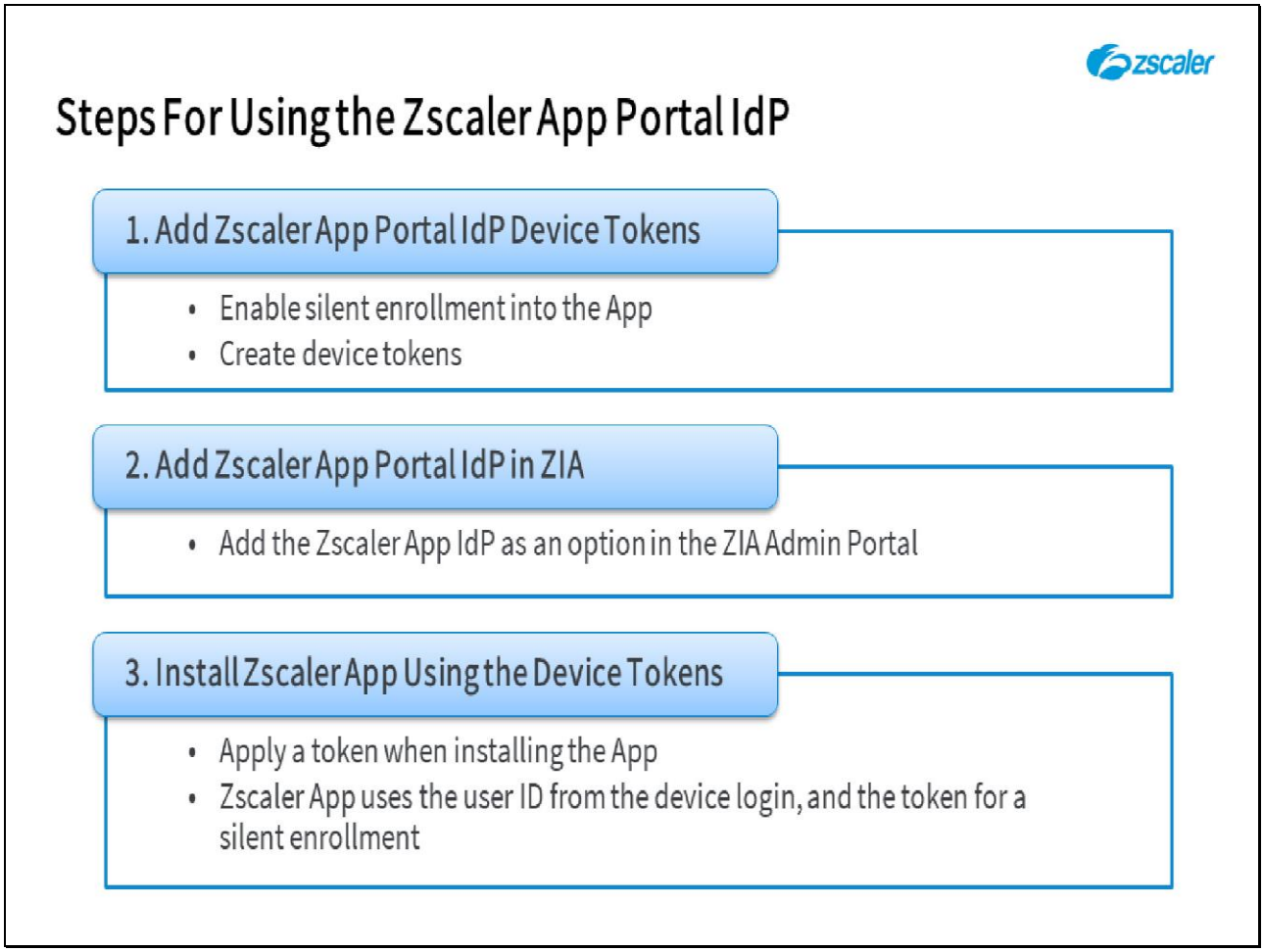
Slide notes

Slide 45 - Slide 45



Slide notes

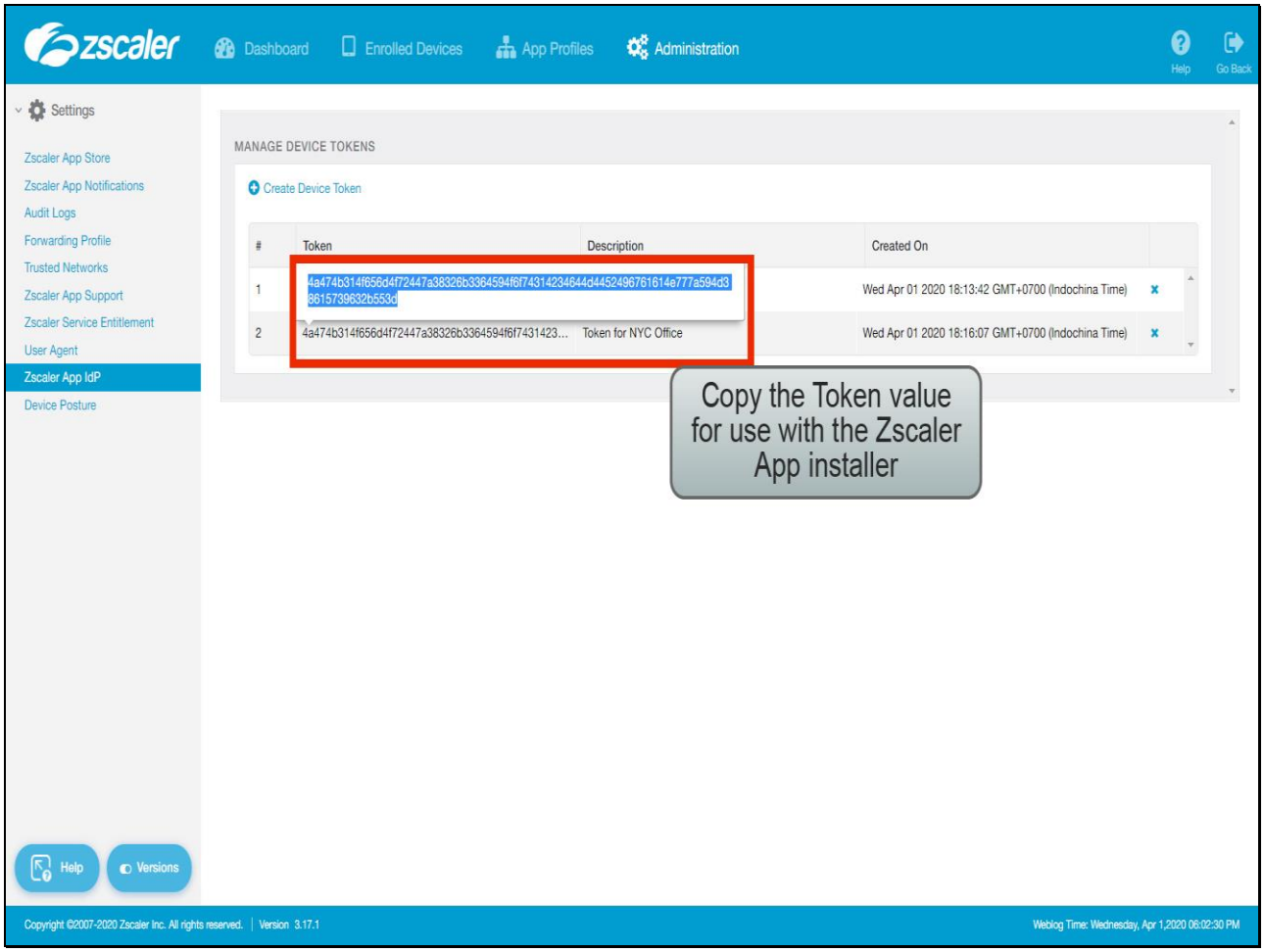
Slide 46 - Steps For Using the Zscaler App IdP



Slide notes

All you need to do now is apply one of those eight **Device Tokens** to the Zscaler App during installation, using the **--deviceToken** option. Note, you can use the one Token for multiple devices.

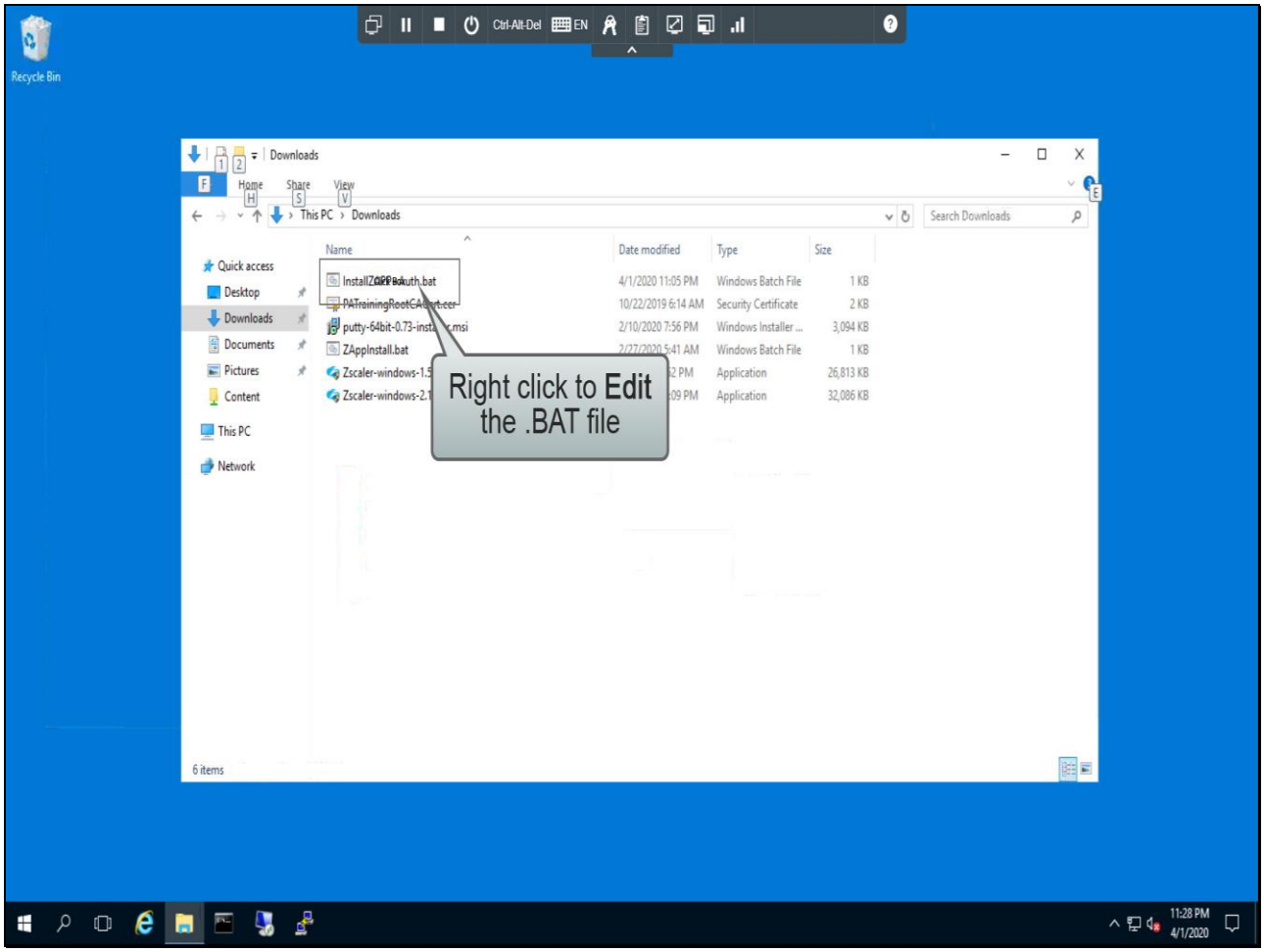
Slide 47 - Slide 47



Slide notes

In the Zscaler App Portal, on the **Administration > Zscaler App IdP** page, copy the value of the **Device Token** that you wish to use.

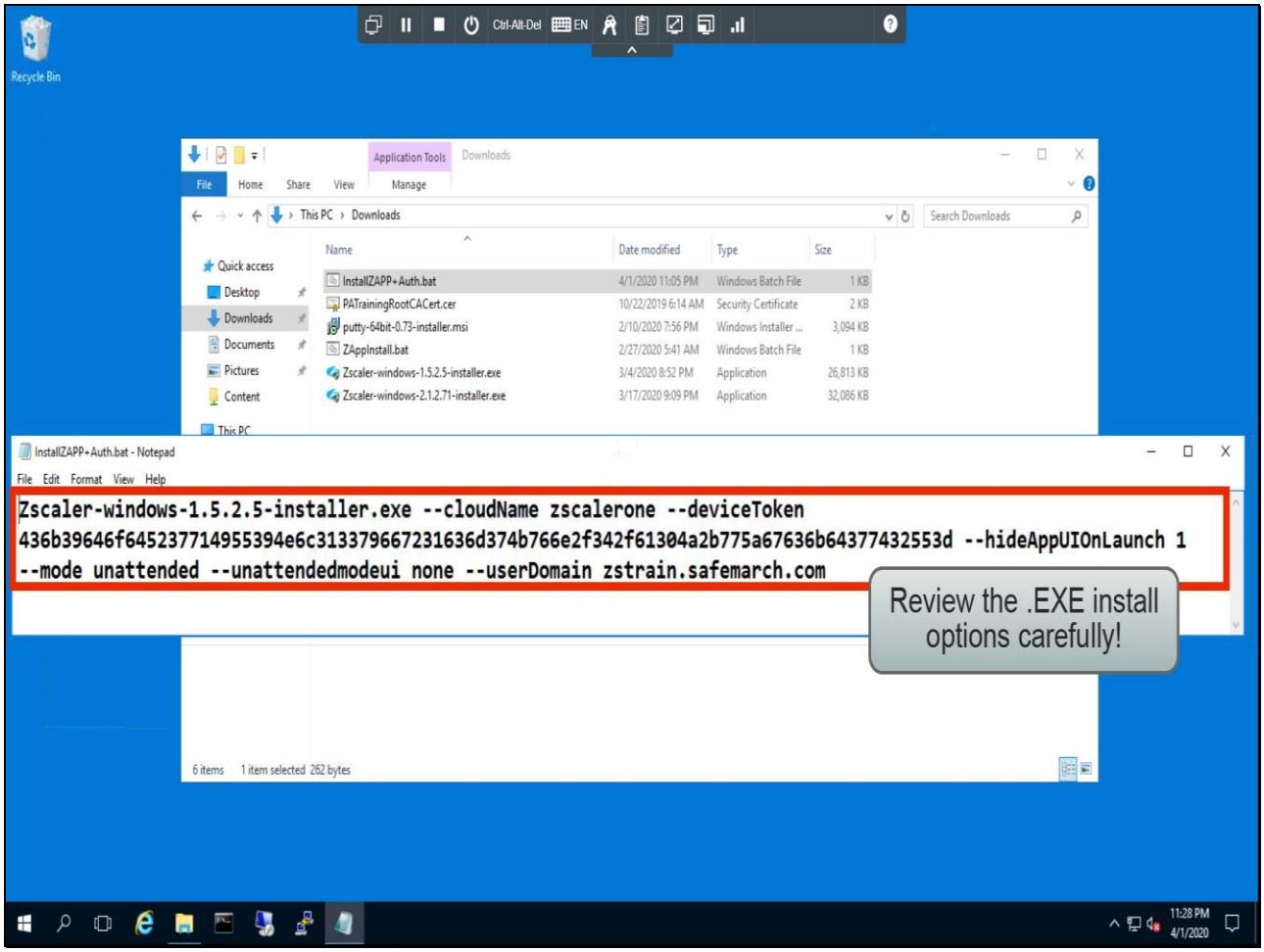
Slide 48 - Slide 48



Slide notes

On the end user's device, create a .BAT file to run the installer executable file with command line options. In this case, we have a Windows machine, so click to open the .BAT file, ...

Slide 49 - Slide 49

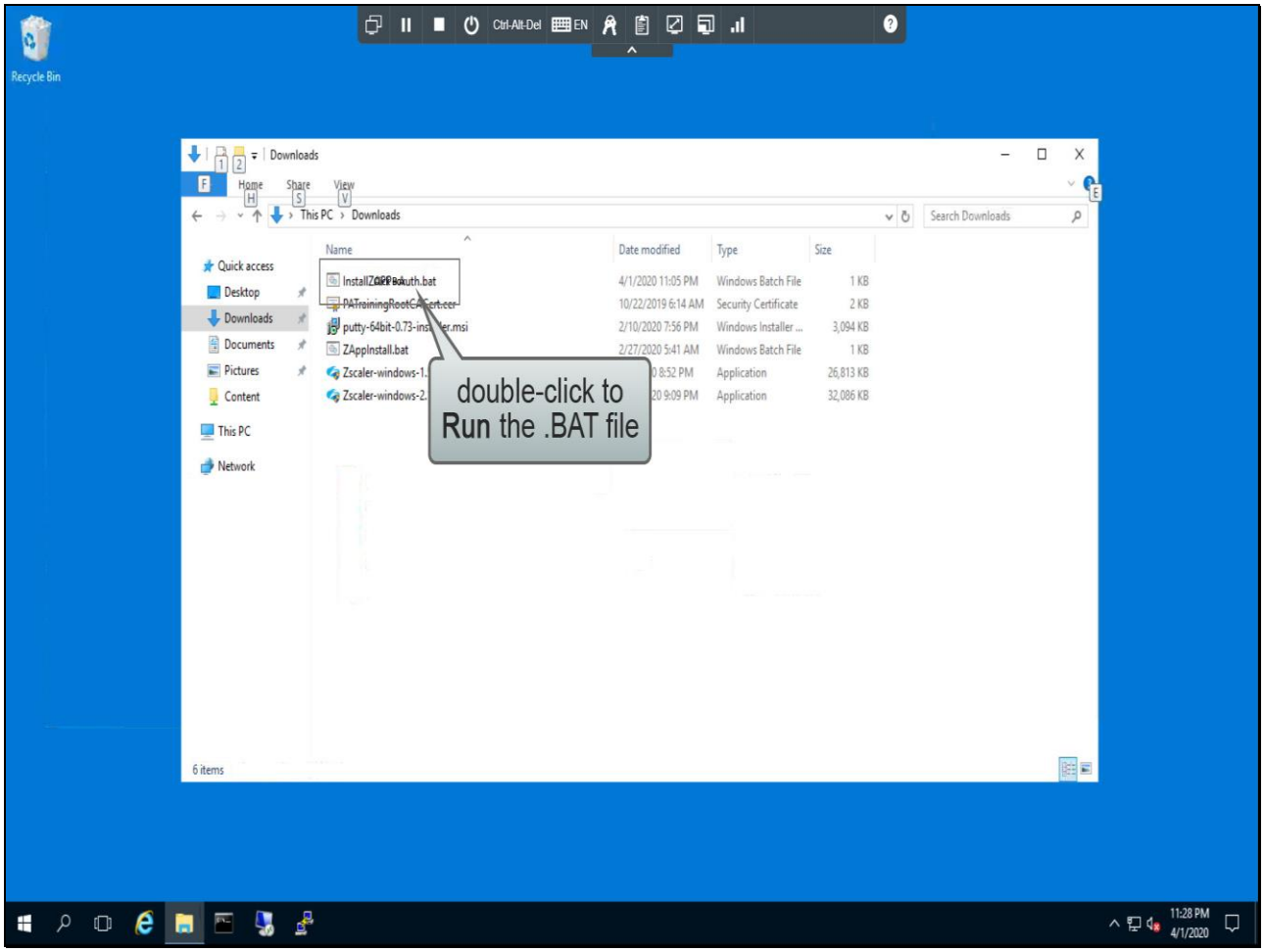


Slide notes

...and ensure that the file path to the .EXE and options are correct. The **--cloudName** option may be required, the **--deviceToken** option with the value for it from the Zscaler App Portal of course, plus the **--userDomain** option is required. Other options may also be used, for example to hide the installer from the end user.

Note, these options are also supported in a .MST file that you could push from AD using a GPO.

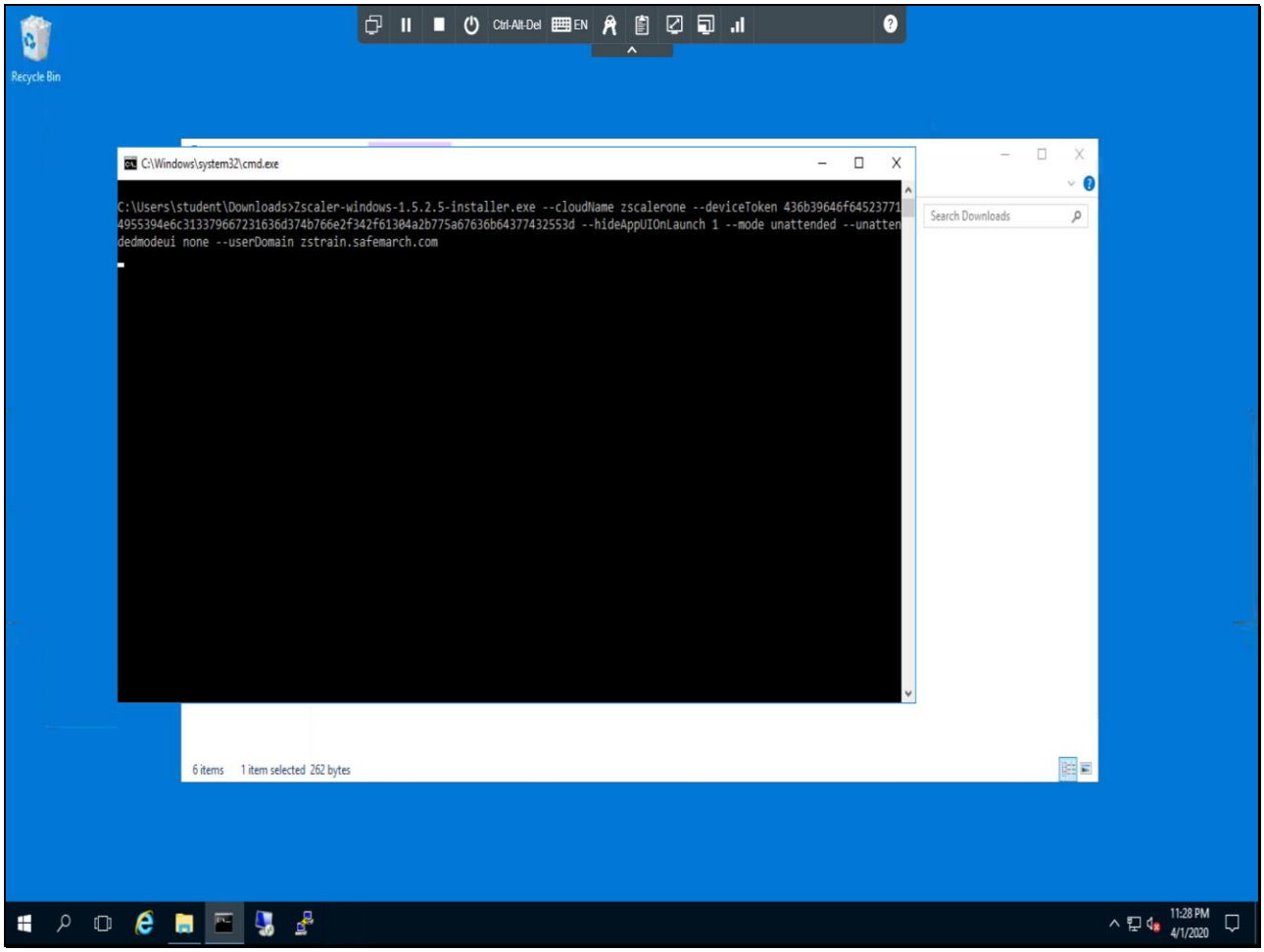
Slide 50 - Slide 50



Slide notes

Double-click the .BAT file to run it, ...

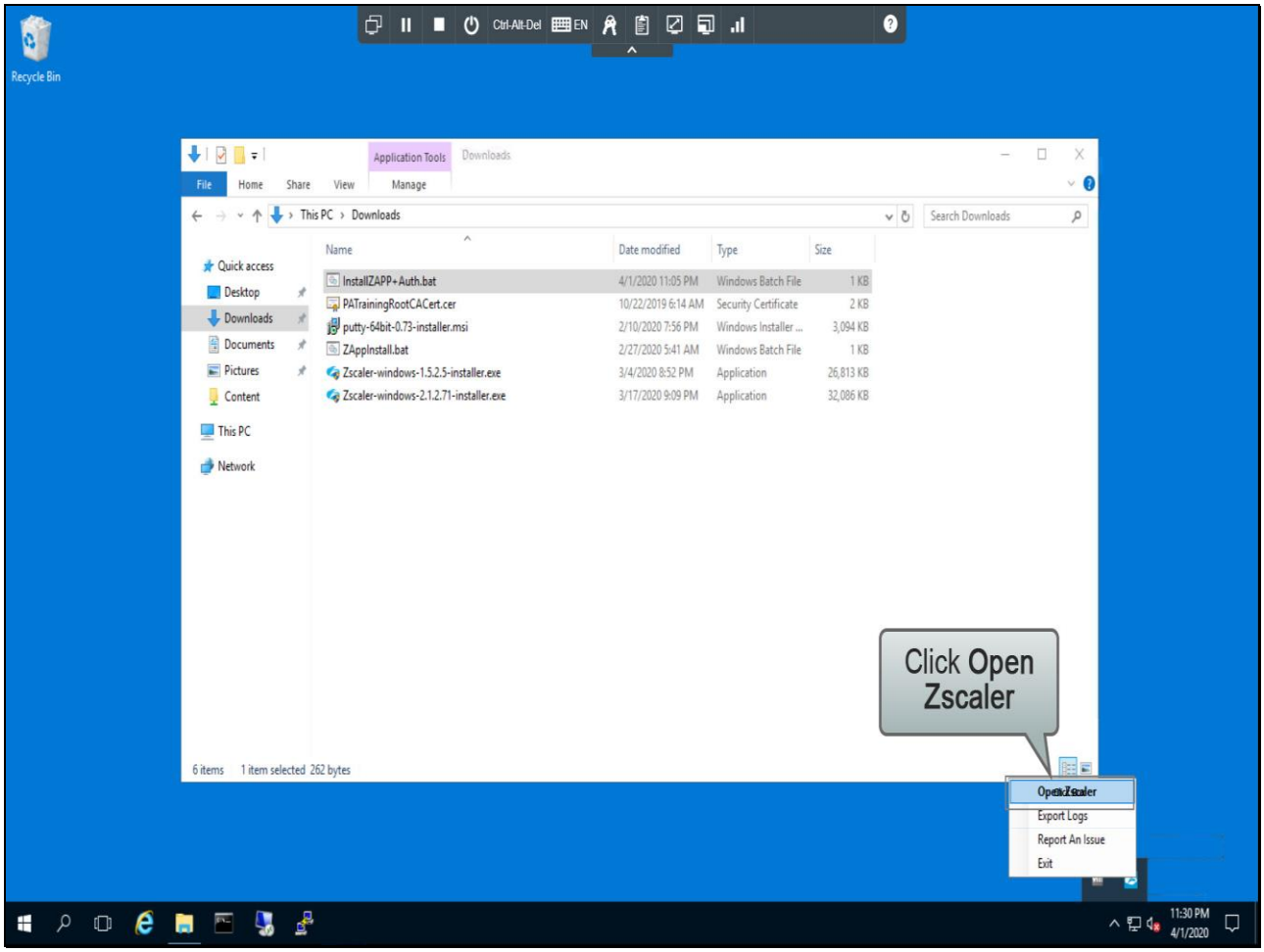
Slide 51 - Slide 51



Slide notes

...and just sit back and wait.

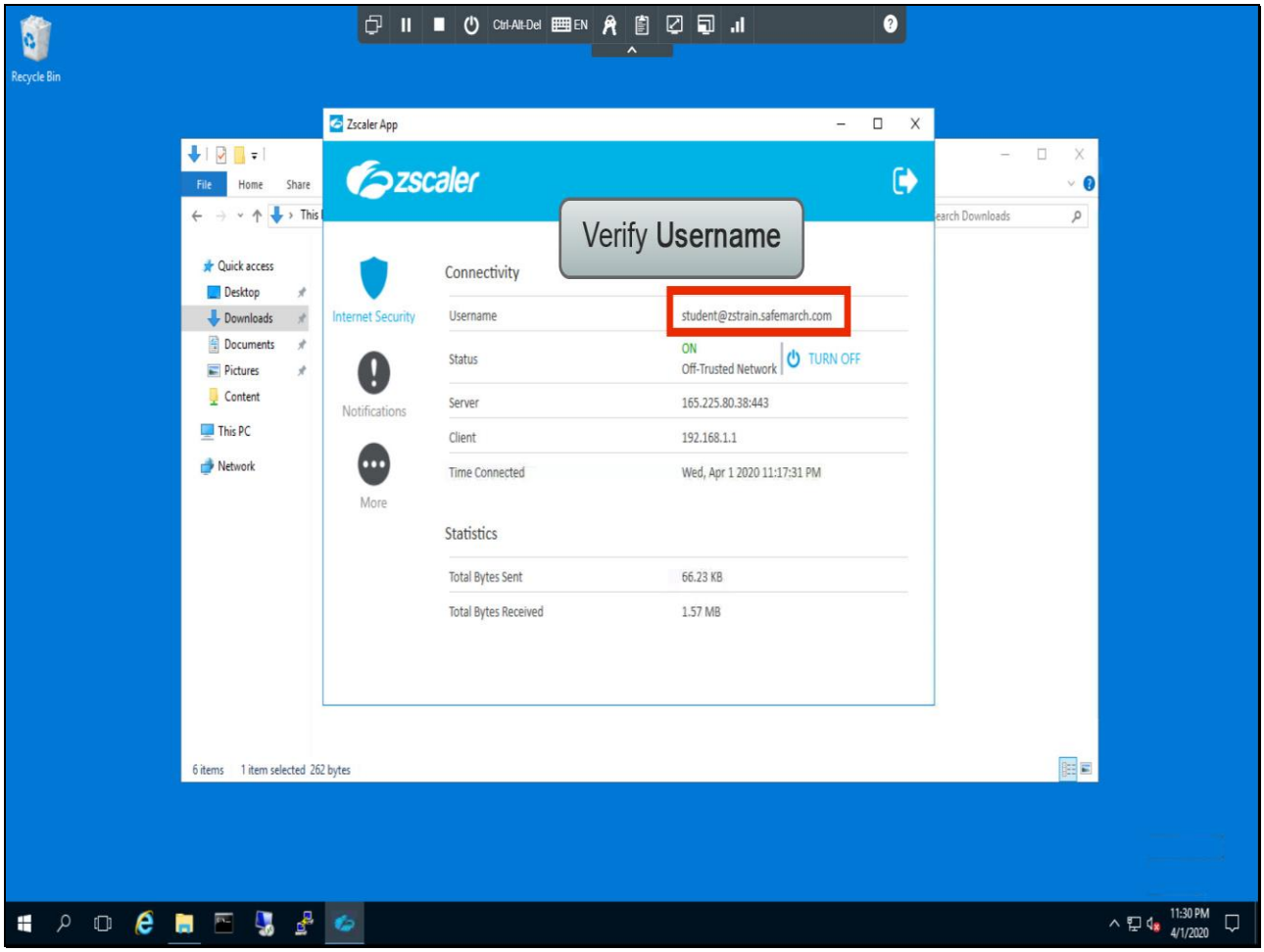
Slide 52 - Slide 52



Slide notes

Zscaler App will be installed and the end user automatically enrolled into it for access to the ZIA service. To verify, click to **Open Zscaler** from the **Task Bar**.

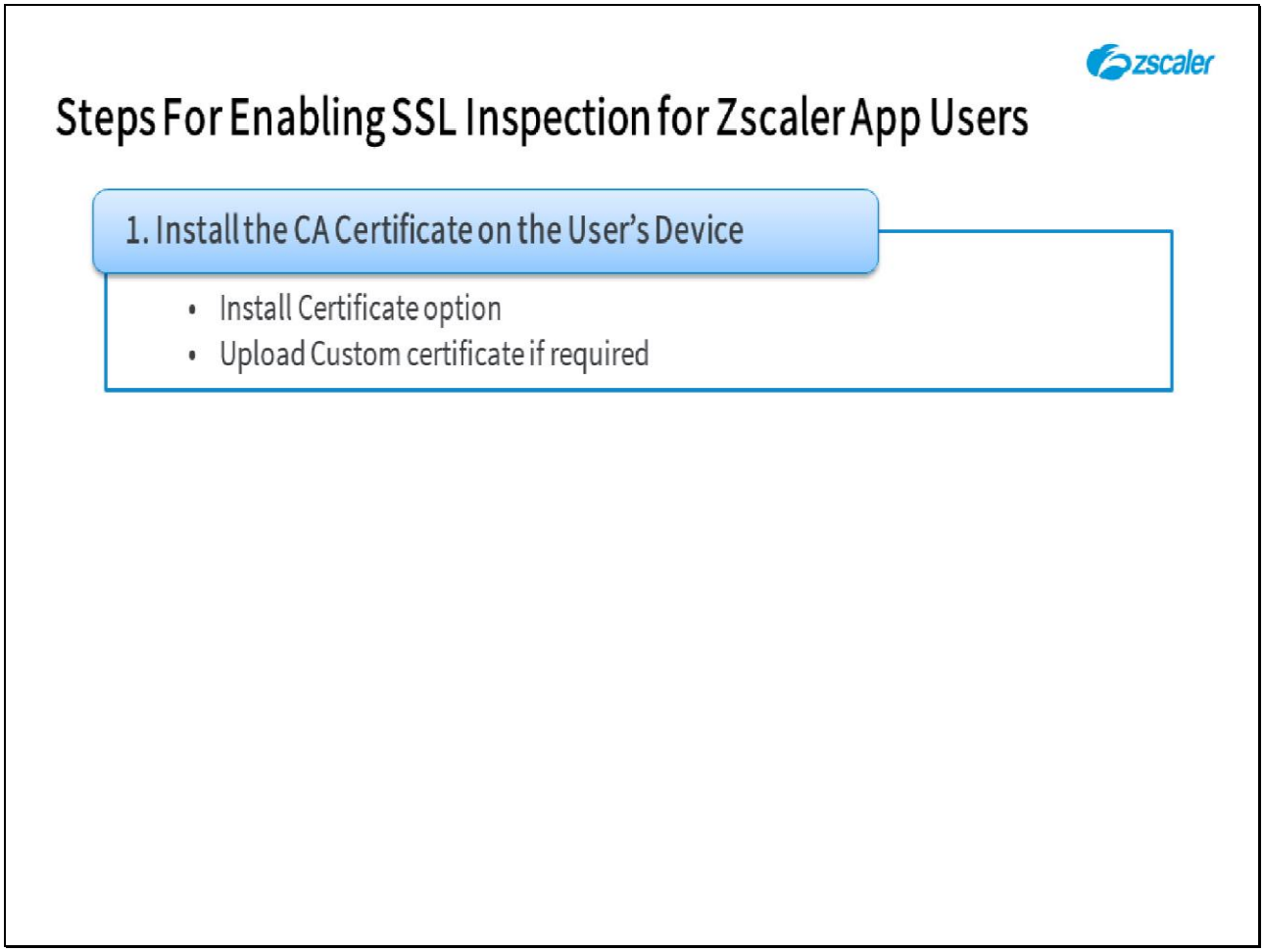
Slide 53 - Slide 53



Slide notes

You will find that the end user has been enrolled using the **Username** from the machine logon. The Zscaler **Internet Security** service should be active and traffic flowing based on the **App Profile** and **Forwarding Profile** assigned to this user.

Slide 54 - Enabling SSL Inspection for Zscaler App Users



Slide notes

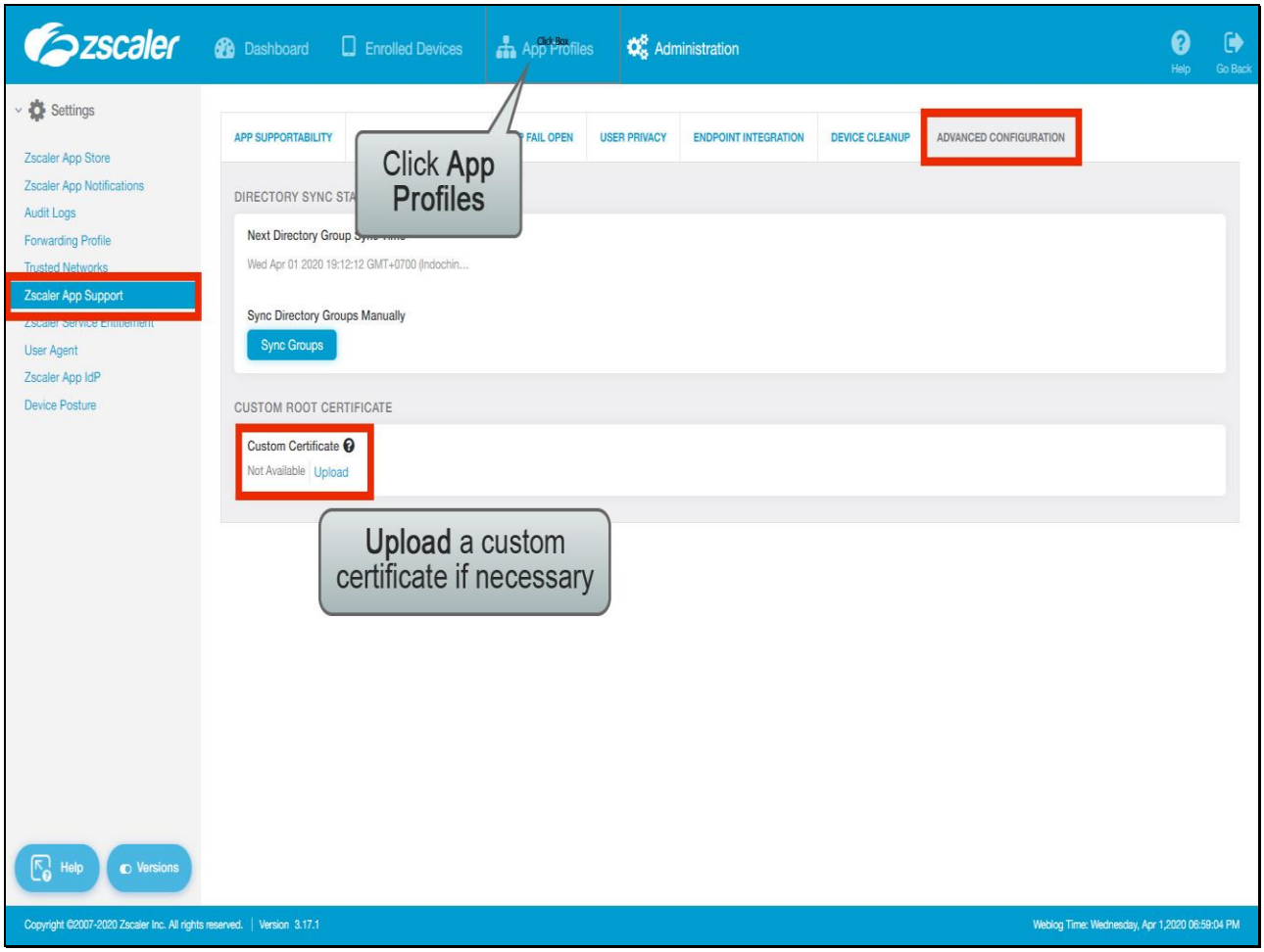
If you want to enable **SSL Inspection** for your Zscaler App users (which we would recommend), there are a couple of tasks required in the Zscaler App Portal.

Slide 55 - Slide 55

Slide notes

If you are using a custom certificate for the connection to Zscaler, you need to upload it to the Zscaler App Portal so we can deploy it to your end users. Click **Administration**, ...

Slide 56 - Slide 56

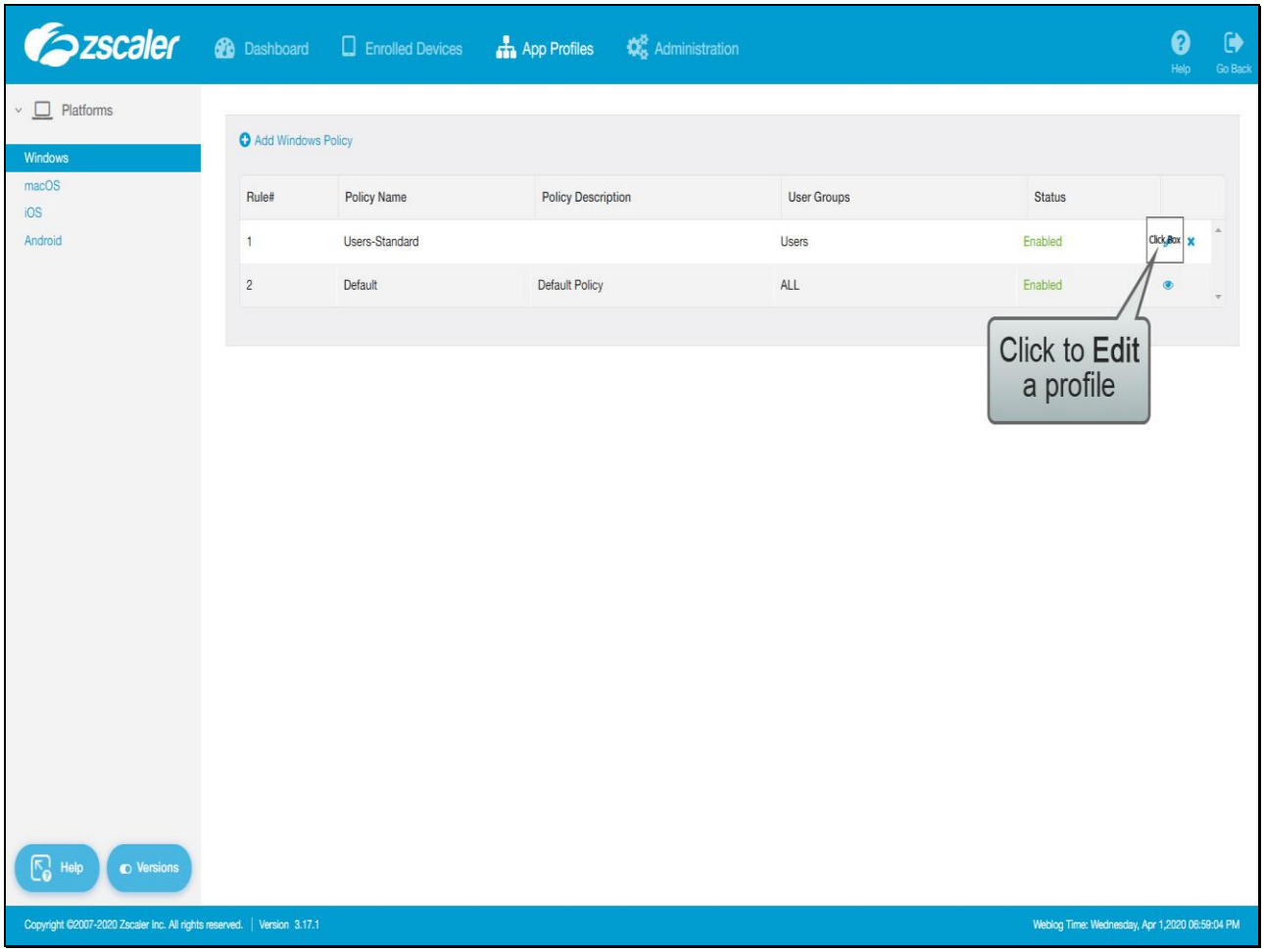


Slide notes

...go to the **Zscaler App Support > ADVANCED CONFIGURATION** page and **Upload** the root CA certificate from the CA that you used to create the web server certificate for Zscaler (the certificate that we will use to secure end user connections to the ZIA service). Note that, if you plan to use the default Zscaler certificate, there is nothing to be done here.

Click to go to your **App Profiles** configurations, ...

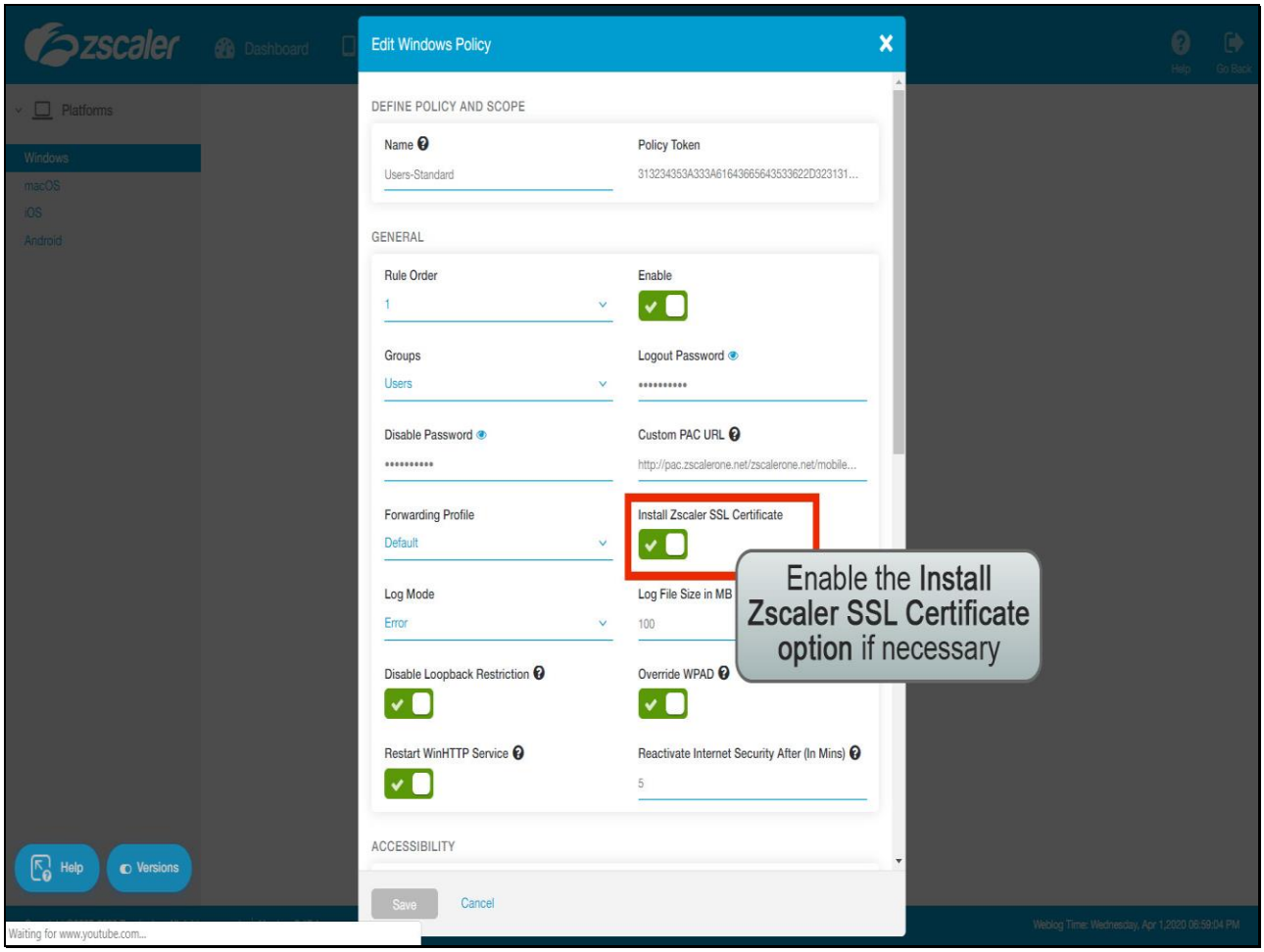
Slide 57 - Slide 57



Slide notes

...then click to **Edit** the relevant profiles, ...

Slide 58 - Slide 58

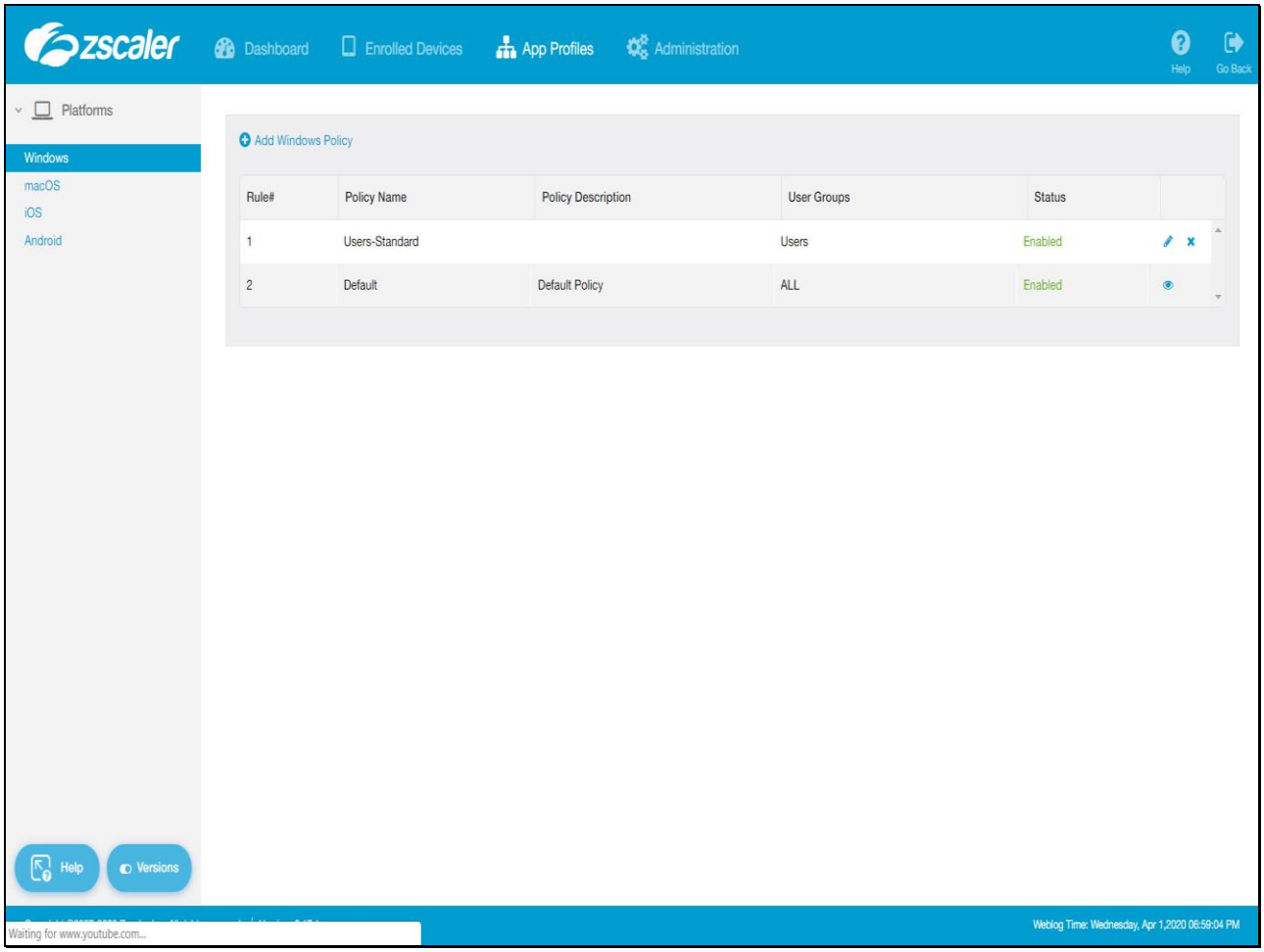


Slide notes

...and make sure that the **Install Zscaler SSL Certificate** option is enabled. This will install the Zscaler root CA certificate and, if there is one, the root CA certificate that you uploaded on the **ADVANCED CONFIGURATIONS** page.

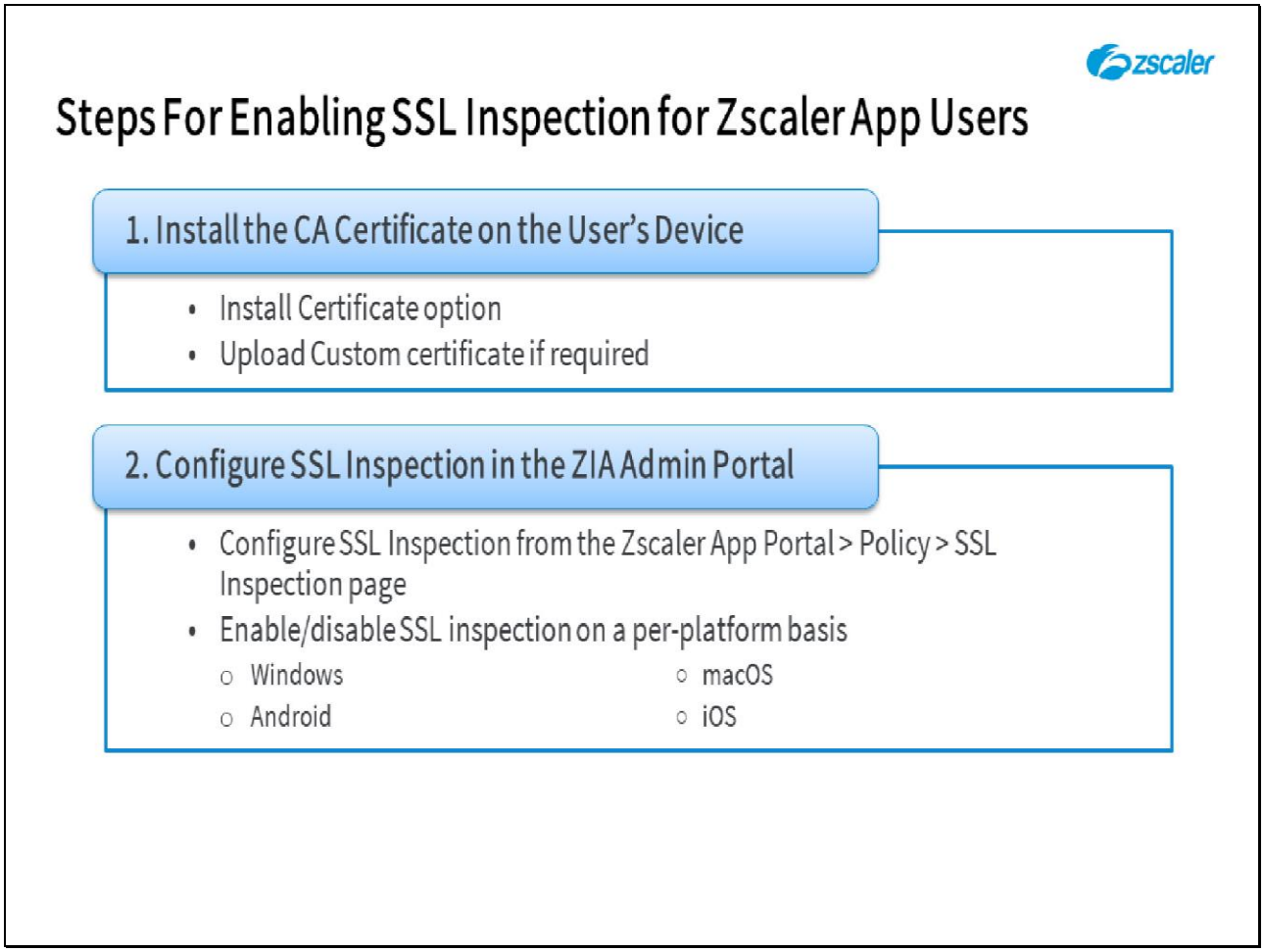
Note, we install the certificate(s) on enrollment into the App, so if you have users that are already using the App when you enable this option, they would need to **Log Out** of the App and enroll once more to receive the certificate(s).

Slide 59 - Slide 59



Slide notes

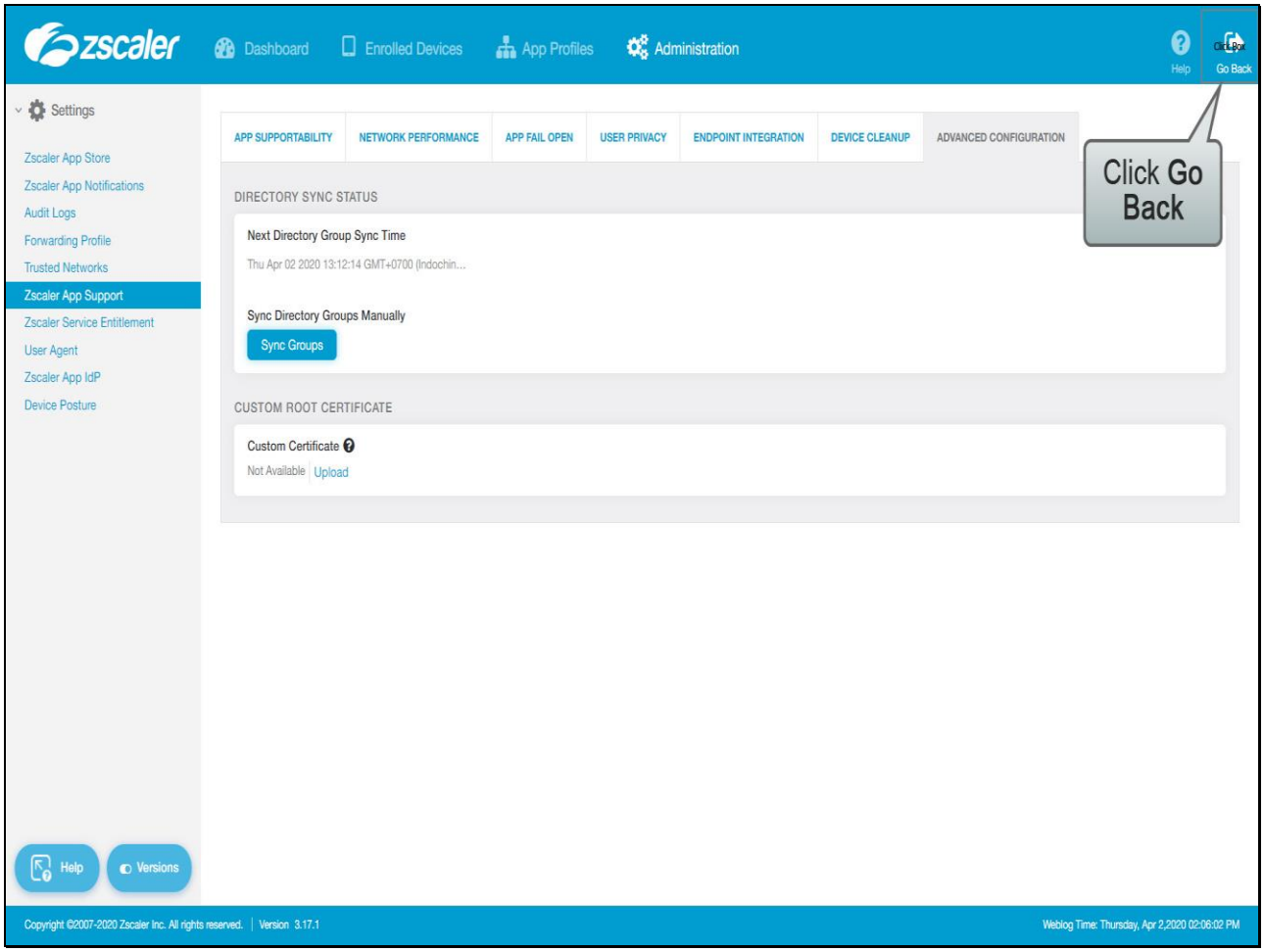
Slide 60 - Steps For Enabling SSL Inspection for Zscaler App Users



Slide notes

SSL inspection for Zscaler App devices is enabled from the ZIA Admin Portal, from the **Policy > SSL Inspection** page. You have the option to **Enable** or **Disable** SSL inspection on a per-platform basis, for; **Windows**, **macOS**, **Android**, and **iOS**.

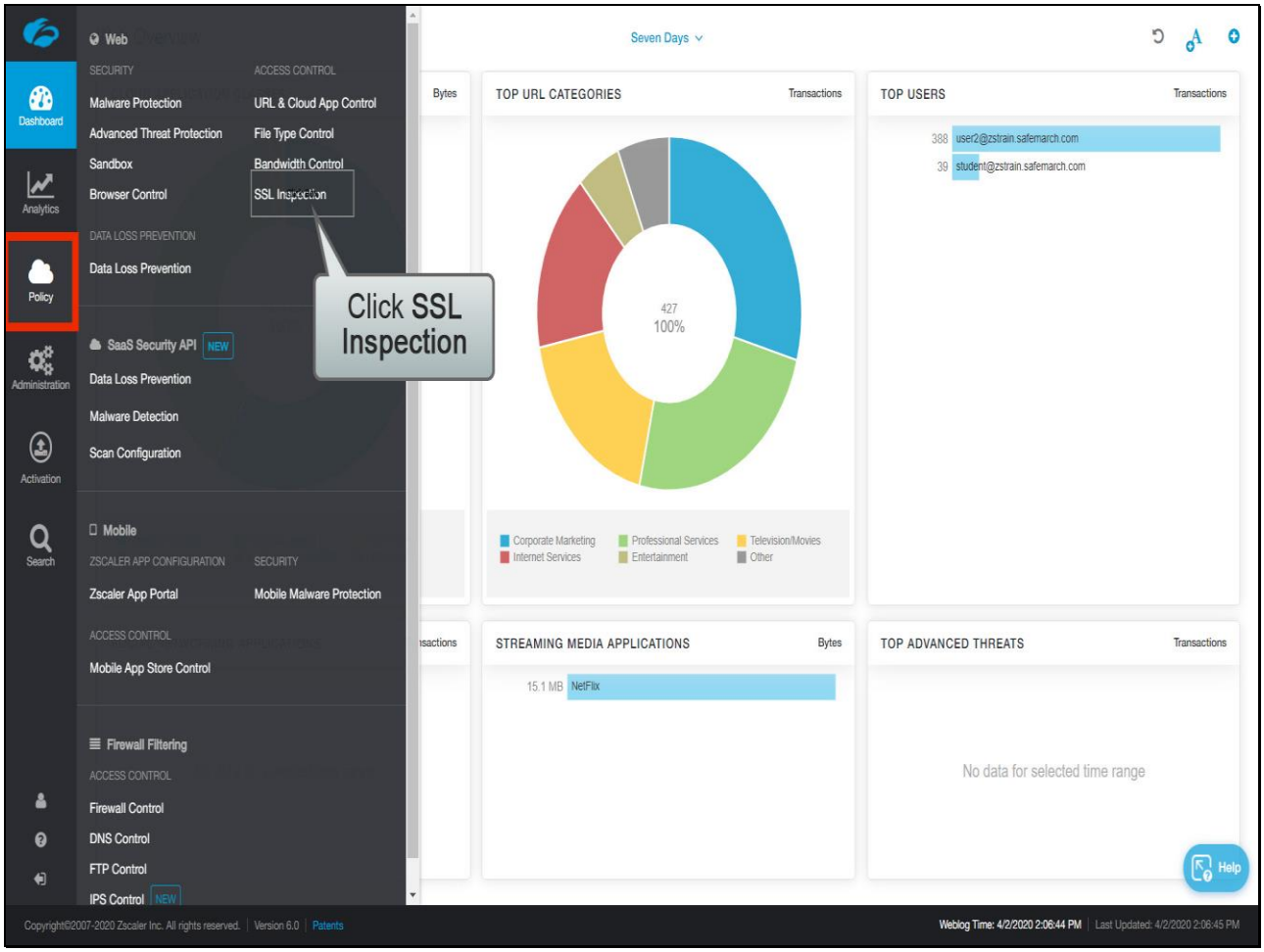
Slide 61 - Slide 61



Slide notes

To return to the ZIA Admin Portal, click the **Go Back** icon at top right.

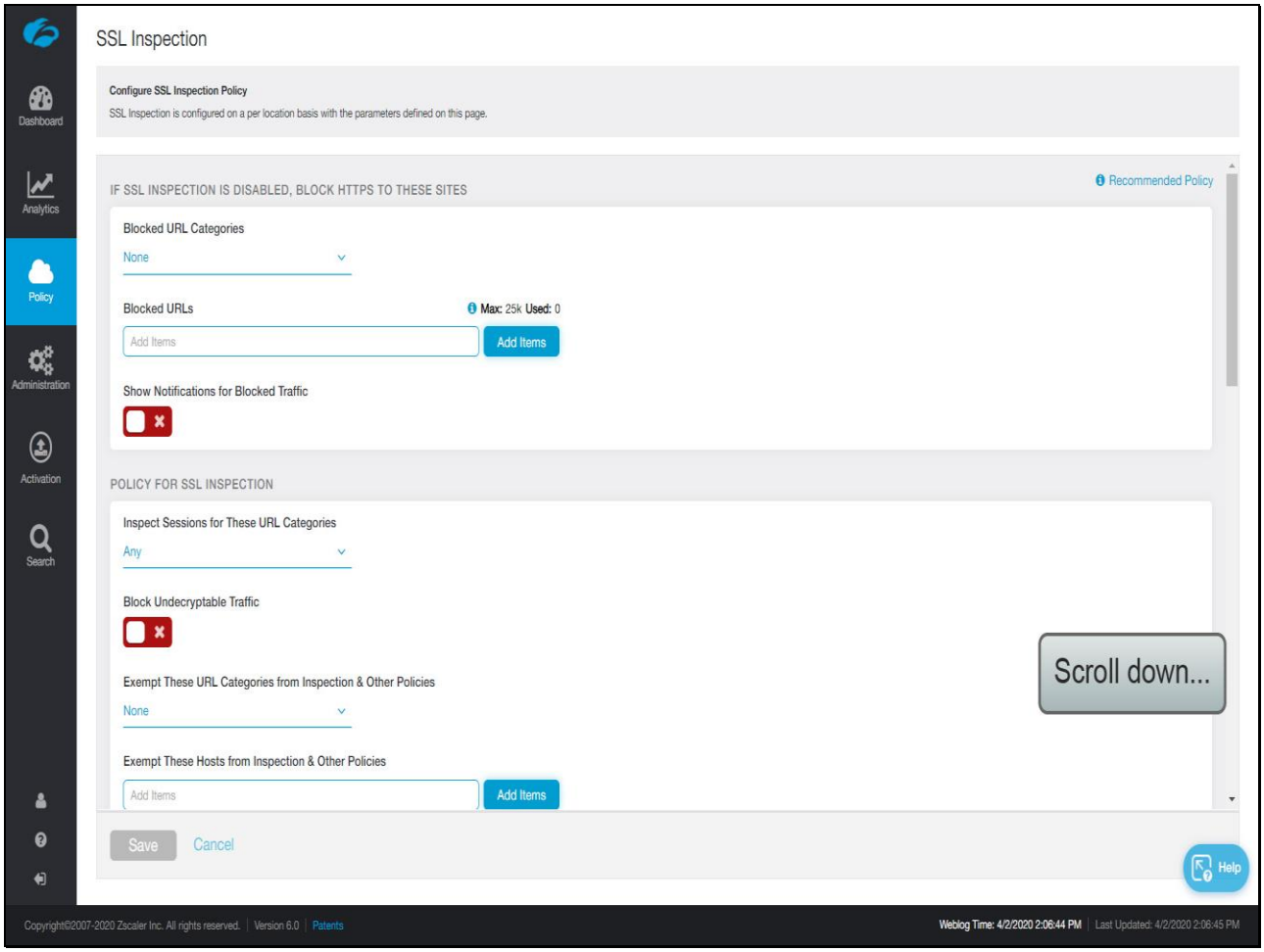
Slide 62 - Slide 62



Slide notes

To go to the SSL Inspection policy page, from the **Policy** menu click **SSL Inspection**.

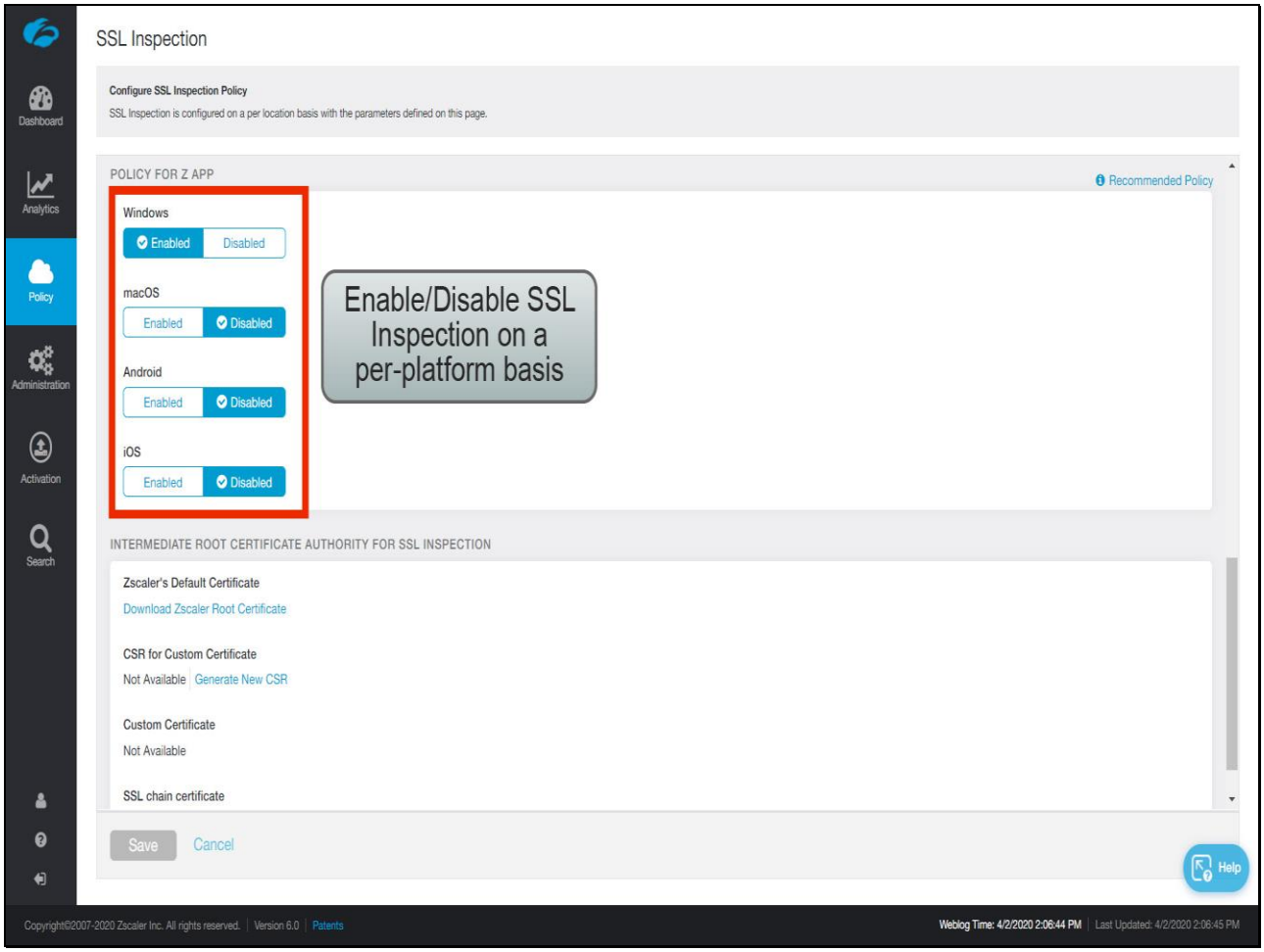
Slide 63 - Slide 63



Slide notes

Scroll down to the bottom of the page, …

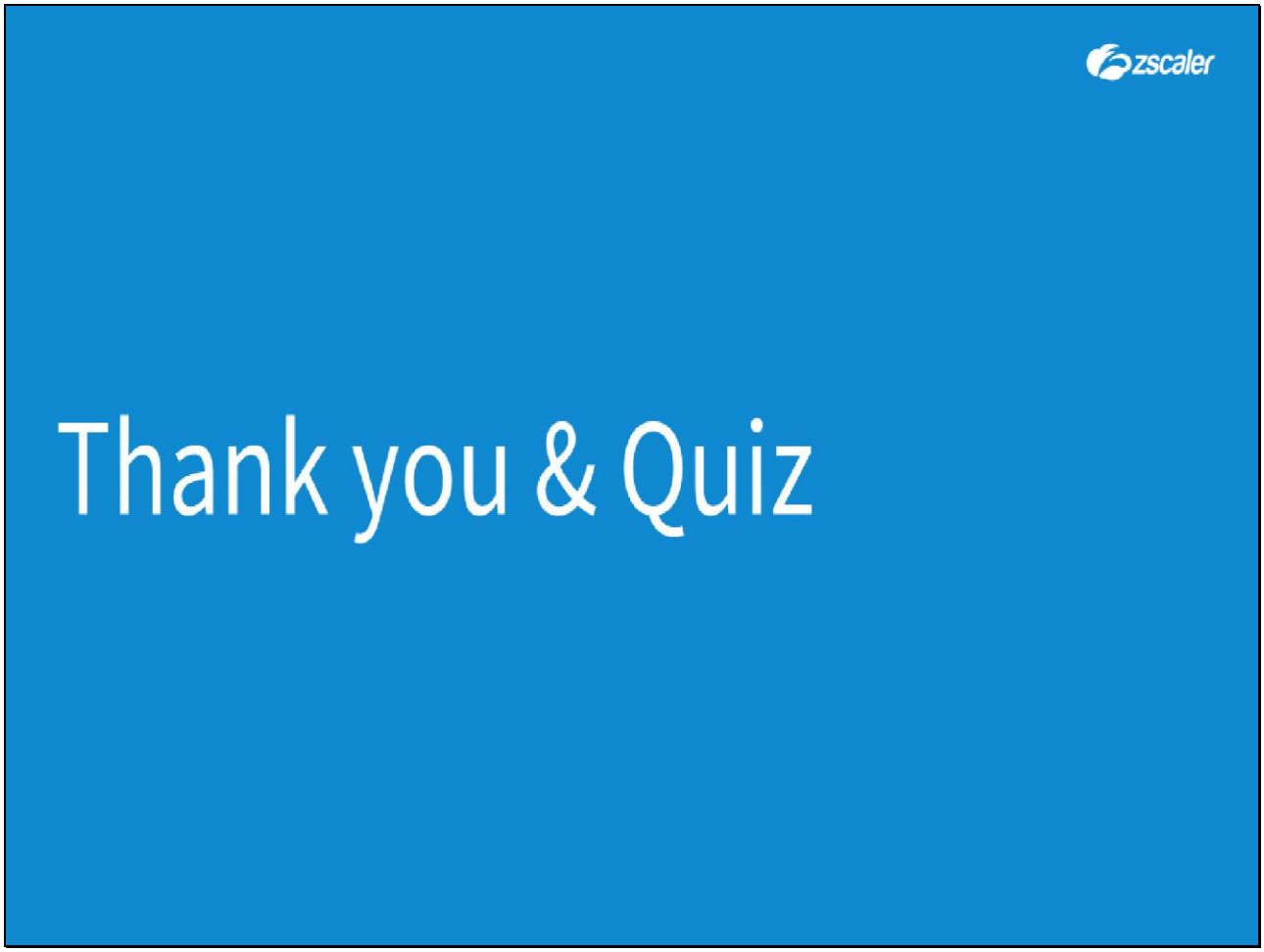
Slide 64 - Slide 64



Slide notes

…where you will find the per-platform controls to manage **SSL inspection** on Zscaler App devices. Configure these as necessary, then **Save** and **Activate** your changes.

Slide 65 - 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.