

Slide 1 – The Zscaler App: ZIA Specific Configurations



The Zscaler App

ZIA Specific Configurations

©2020 Zscaler, Inc. All rights reserved.

Slide notes

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

Slide 2 - Navigating the eLearning Module

The screenshot shows the Zscaler Basic Administration dashboard. At the top right is the Zscaler logo. Below it, the main title "Navigating the eLearning Module" is displayed. A large blue "Exit" button is positioned in the top right corner of the dashboard area. On the left side, there's a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration, and Search. The main content area has tabs for Applications, Users, and Health, with Applications selected. It displays metrics like "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). Below these are sections for "TOP APPLICATIONS BY BANDWIDTH" and "TOP POLICY BLOCKS". In the bottom left corner of the dashboard, there are four blue callout boxes with arrows pointing to specific controls: "Play/Pause" points to a play/pause button; "Previous Slide" and "Next Slide" point to previous/next slide buttons; "Progress Bar" points to a progress bar; and "Audio On/Off" and "Closed Captioning" point to audio control buttons.

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
 - Using the Zscaler App Portal IdP
 - Enabling SSL Inspection

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



Interactive Demo: Zscaler App - ZIA Specific Configurations

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



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 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

The screenshot shows the Zscaler Admin Portal interface. On the left sidebar, under the 'Policy' section, there is a button labeled 'Zscaler App Portal'. A large callout bubble with the text 'Click Zscaler App Portal' points to this button. The main dashboard area displays several charts and tables. One chart is a donut chart titled 'TOP URL CATEGORIES' showing data for 'Bytes' and 'Transactions'. The categories and their percentages are: Professional Services (blue, ~30%), Social Networking (green, ~25%), Corporate Marketing (yellow, ~15%), Television/Movies (light green, ~10%), Internet Services (red, ~5%), and Other (grey, ~10%). Below the chart is a table titled 'STREAMING MEDIA APPLICATIONS' showing bytes transferred. The data is as follows:

Application	Bytes
NetFlix	15.1 MB
YouTube	34.2 KB

Other sections visible include 'TOP USERS' (listing user2@zstrain.safemarch.com, user1@zstrain.safemarch.com, and student@zstrain.safemarch.com), 'TOP ADVANCED THREATS' (which shows 'No data for selected time range'), and various security controls like 'Malware Protection', 'URL & Cloud App Control', and 'Data Loss Prevention'.

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

The screenshot shows the Zscaler App Store interface. On the left, there's a sidebar with a 'Settings' icon and a list of options: Zscaler App Store, Zscaler App Notifications, 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.

In the main content area, there are two tabs: 'PERSONAL COMPUTERS' and 'MOBILE DEVICES'. The 'MOBILE DEVICES' tab is selected. Below it, there's a 'UPDATE SETTINGS' section with an 'Automatic Rollout' dropdown menu containing 'Always Latest Version', 'Specific Version', 'Group Based', and a 'Disable' option. A 'Cancel' button is also present.

Underneath, there's a 'DEVICE SNAPSHOT' section divided into 'Windows' and 'macOS' tables. The Windows table has three rows:

Application Version	Registered Devices	Release Notes	Download EXE	Download MSI
2.1.2.71	0	View	Download	Download
2.1.0.210	0	View	Download	Download

The macOS table has two rows:

Application Version	Registered Devices	Release Notes	Download Link
2.1.0.190	0	View	Download
1.5.2.6	0	View	Download

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 1, 2020 04:41:24 PM'.

Slide notes

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

Slide 9 - Slide 9

The screenshot shows the Zscaler Administration interface under the 'Forwarding Profile' section. On the left sidebar, 'Forwarding Profile' is selected. The main area displays a table of forwarding profiles. The first row, labeled '1', has a red border around its entire row. A callout box with the text 'Click Add Forwarding Profile' points to the 'Add Forwarding Profile' button at the top left of the table. Another callout box with the text 'Default Forwarding Profile' points to the first row of the table.

Slide notes

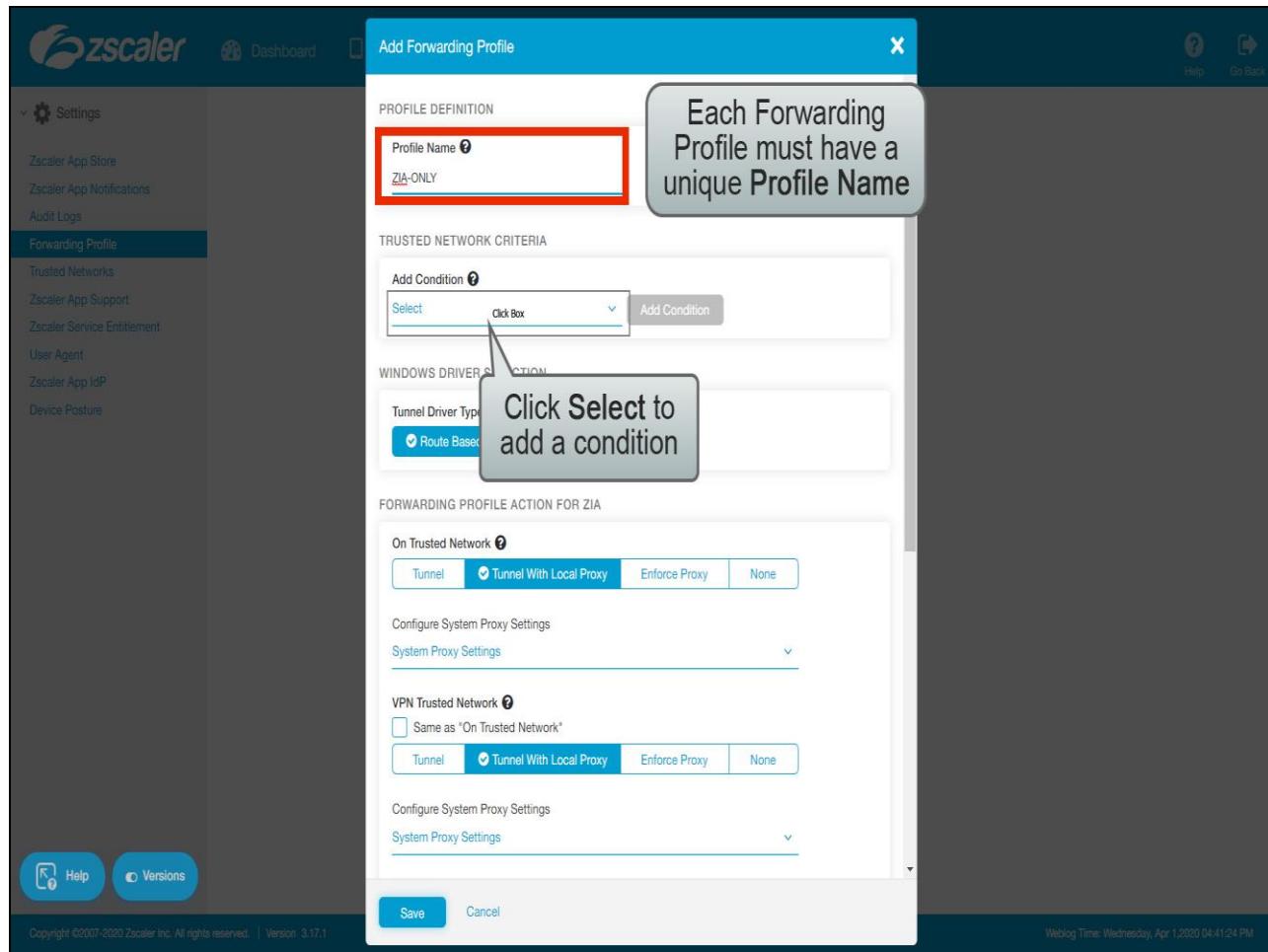
You will find that there is a default **Forwarding Profile** (which cannot be edited), and the option to add a new one. The default profile configuration is as follows:

- **On and Off Trusted Network** - are both set to 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

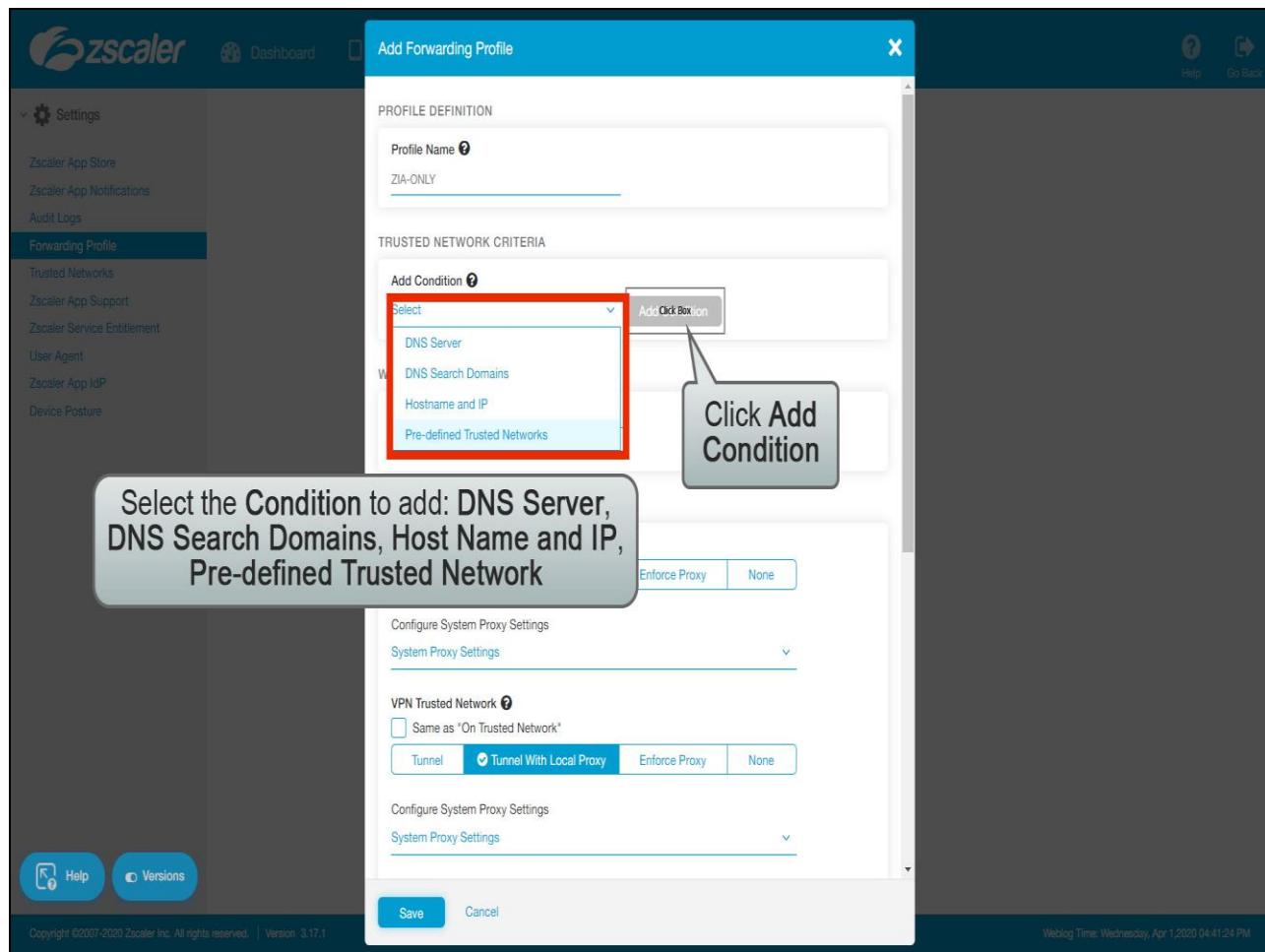


Slide notes

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

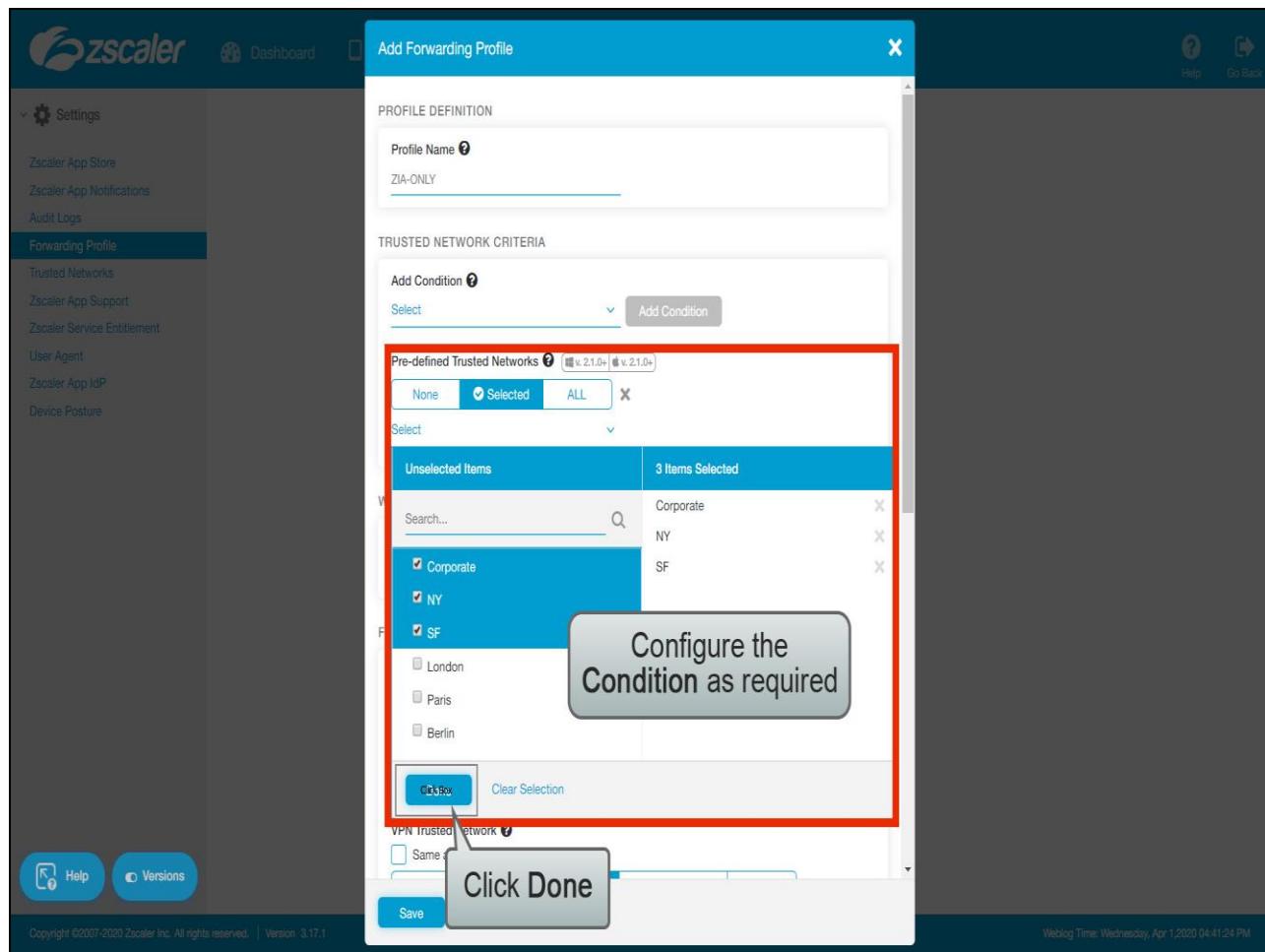
...and select the appropriate condition to be met. The conditions available are:

- 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, ...

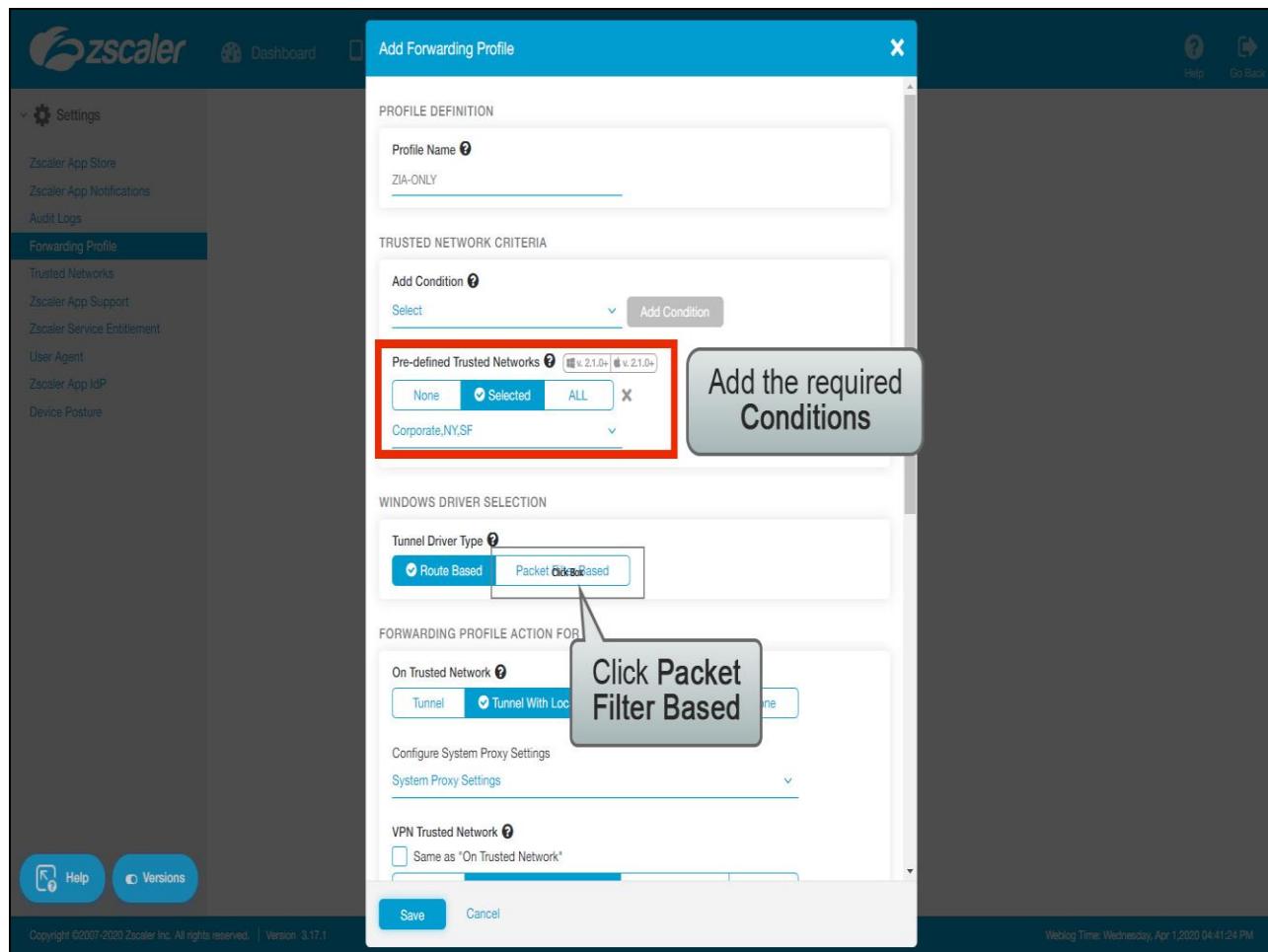
Slide 12 - Slide 12



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



Forwarding Profile Options

Identify the Network Using TRUSTED NETWORK CRITERIA

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

Configure ZIA Traffic Forwarding

- Tunnel 1.0
- Tunnel (1.0) With Local Proxy
- None
- Tunnel 2.0
- Enforce Proxy

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.

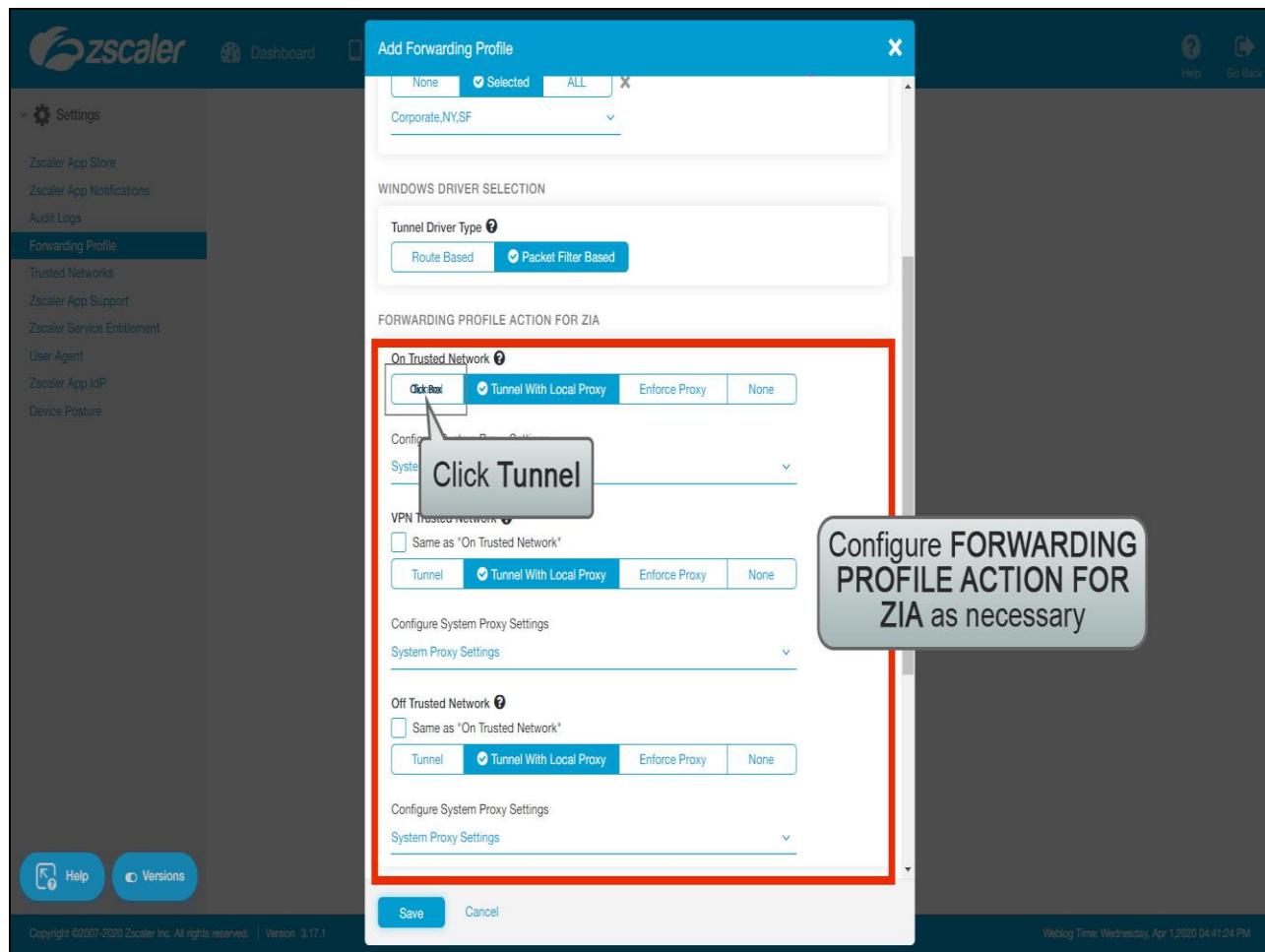
Slide 15 - Slide 15

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 'ZIA-ONLY'. In the 'TRUSTED NETWORK CRITERIA' section, there's a dropdown menu 'Select' and a 'Pre-defined Trusted Networks' dropdown showing 'v.2.1.0+' and 'v.2.1.0+'. A radio button 'Selected' is checked. Below these are dropdown menus for 'Corporate' and 'NY,SF'. The 'WINDOWS DRIVER SELECTION' section shows 'Tunnel Driver Type' with 'Route Based' selected. Under 'FORWARDING PROFILE ACTION FOR ZIA', the 'On Trusted Network' tab is active, showing 'Tunnel With Local Proxy' selected. A large gray callout bubble with the text 'Scroll down...' points to the bottom of this section. At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background of the slide shows the Zscaler dashboard with various navigation links like 'Dashboard', 'Forwarding Profile', and 'Audit Logs'.

Slide notes

Scroll down if necessary...

Slide 16 - Slide 16



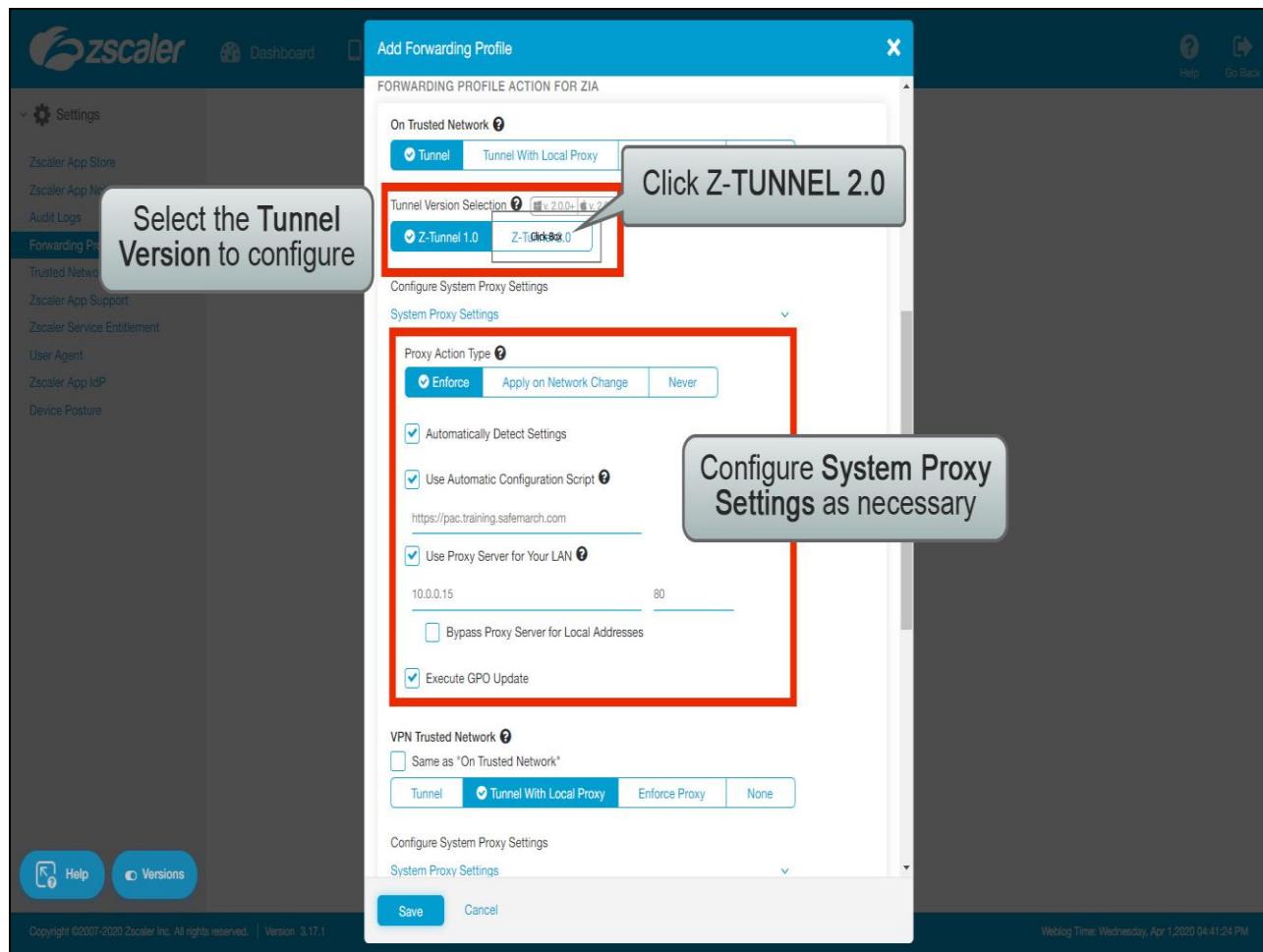
Slide notes

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

The screenshot shows the 'Add Forwarding Profile' dialog box for 'FORWARDING PROFILE ACTION FOR ZIA'. The 'On Trusted Network' tab is selected. Under 'Tunnel Version Selection', 'Z-Tunnel 2.0' is chosen. The 'Z-Tunnel 2.0 Transport Settings' section is highlighted with a red border. Inside this section, there are fields for 'Primary Transport Selection' (DTLS is checked), 'DTLS Connection Timeout (In Seconds)' (set to 9), 'TLS Connection Timeout (In Seconds)' (set to 5), 'MTU for Zscaler Adapter' (set to 0), and 'Allow Fallback' (TLS and Z-Tunnel 1.0 are checked). A callout bubble points to the 'Click Box' button in the top right corner of this section with the text 'Click to collapse the Transport Settings'. Another callout bubble points to the entire red-bordered area with the text 'Configure Z-Tunnel 2.0 Transport Settings as necessary'. At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

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.

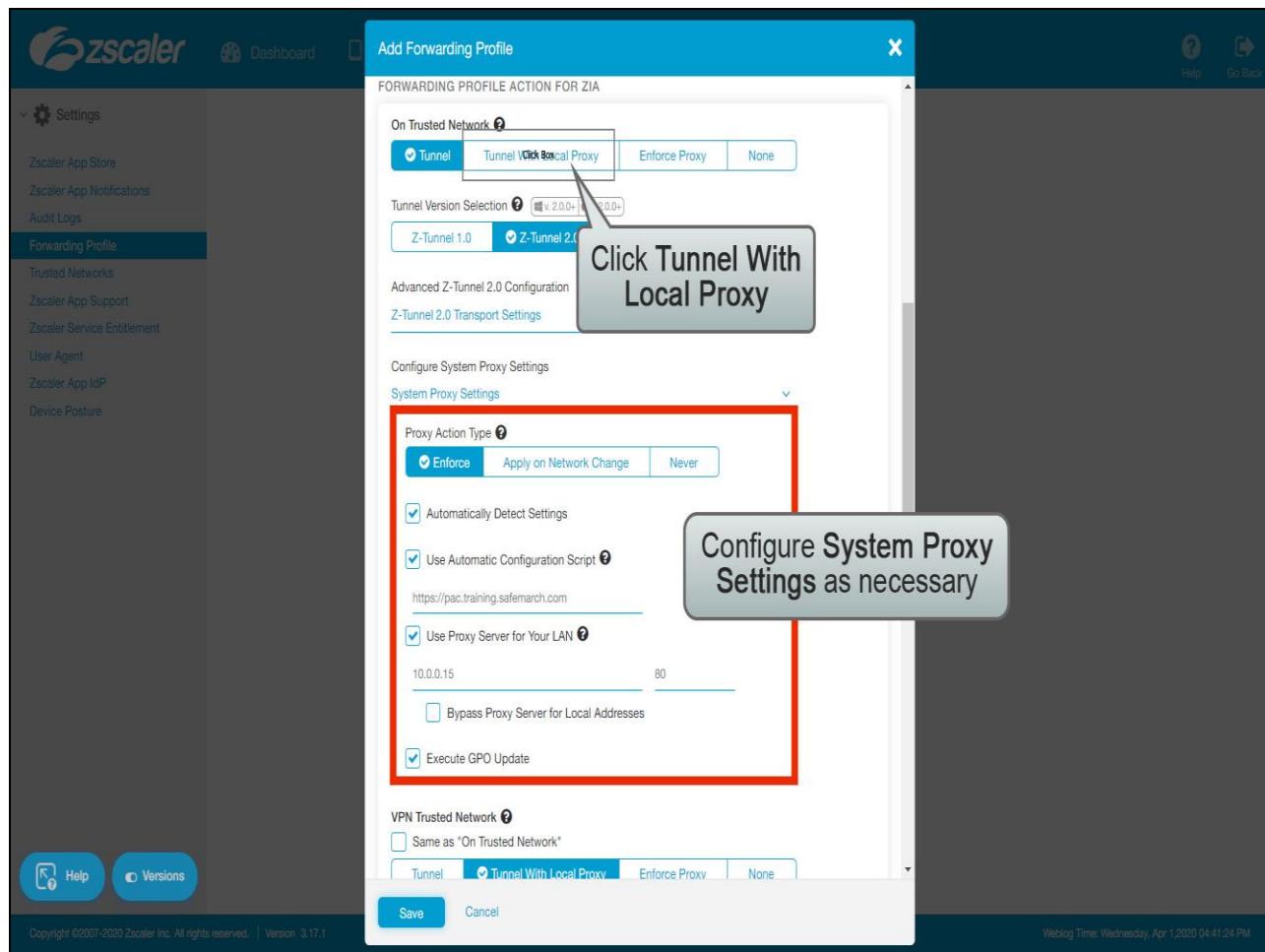
In the **Z-Tunnel 2.0 Transport Selection** settings, you can:

- 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

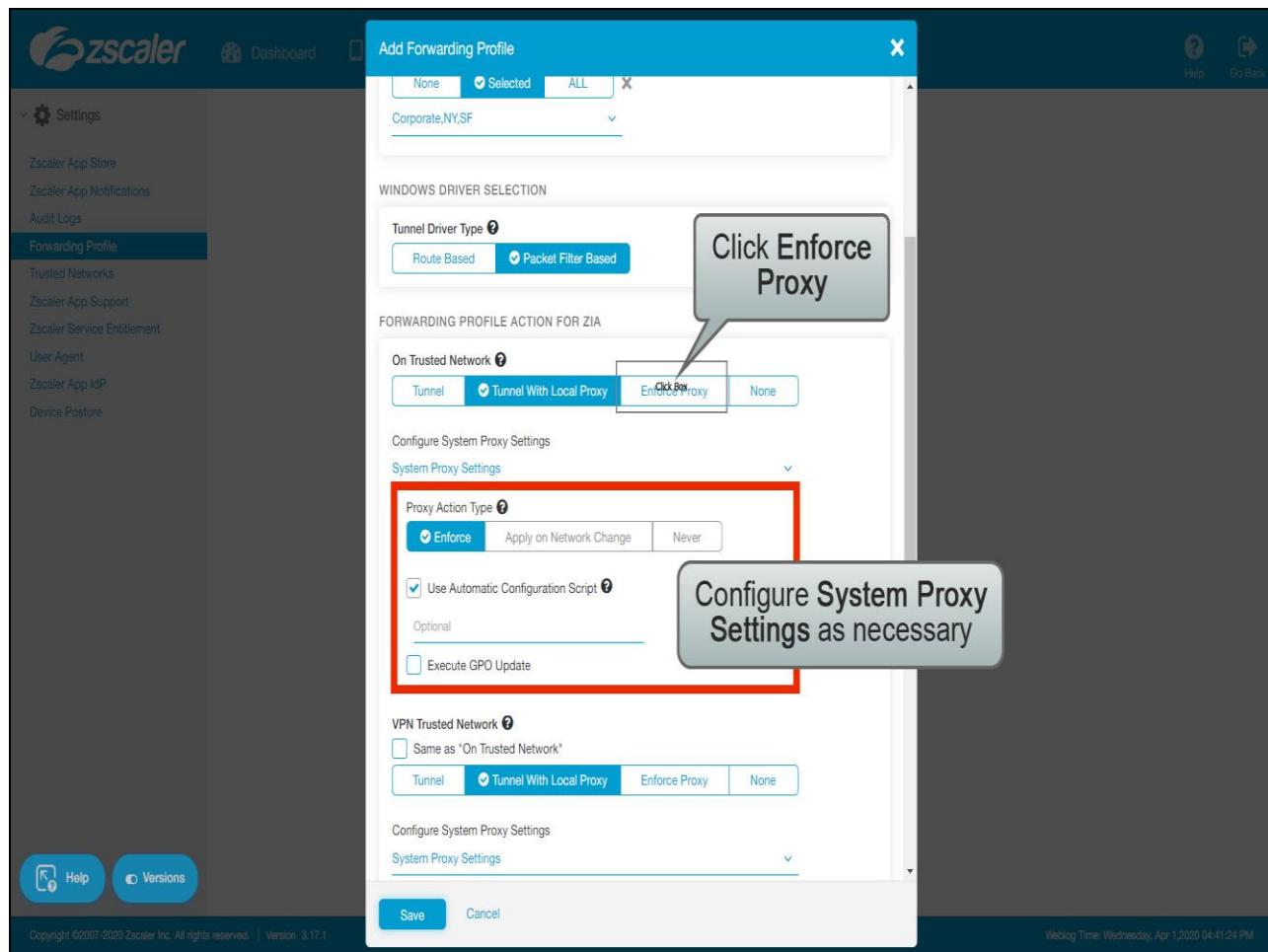


Slide notes

...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



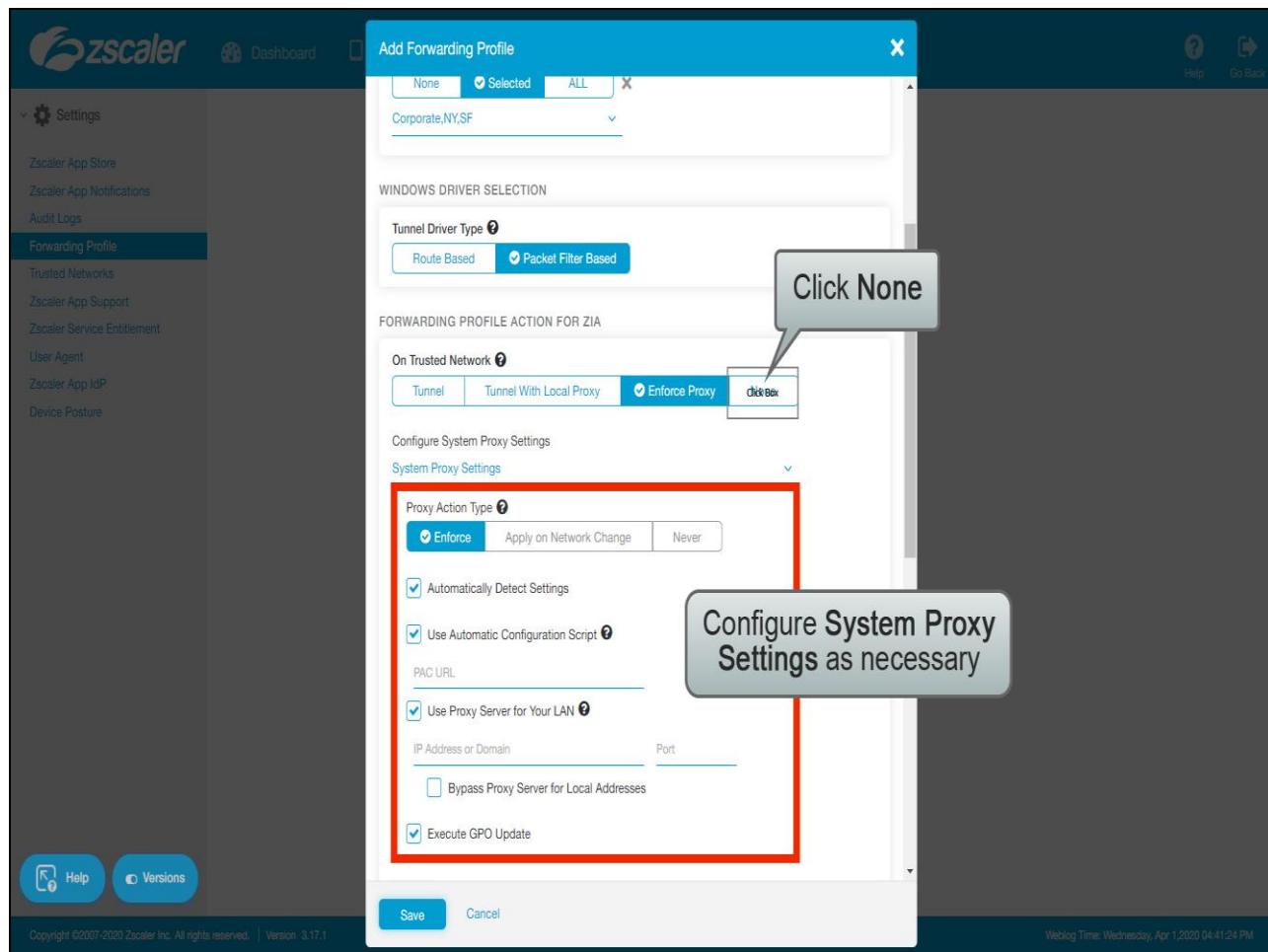
Slide notes

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.

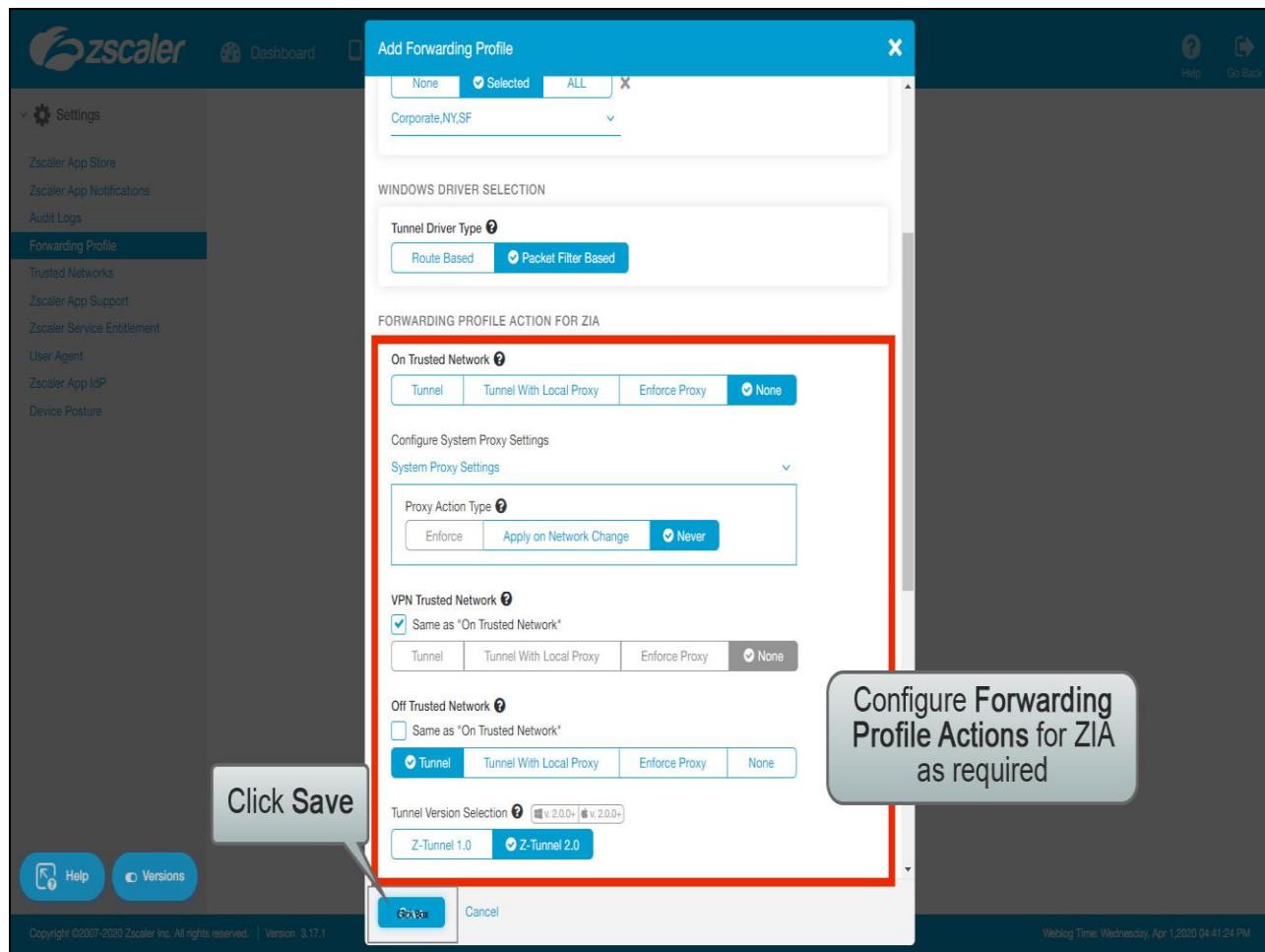
Slide 22 - Slide 22

The screenshot shows the 'Add Forwarding Profile' dialog box over a dark background. The dialog has a blue header bar with tabs for 'None', 'Selected', and 'ALL'. A dropdown menu shows 'Corporate,NY,SF'. Below this is a section for 'WINDOWS DRIVER SELECTION' with 'Tunnel Driver Type' set to 'Packet Filter Based'. Under 'FORWARDING PROFILE ACTION FOR ZIA', there are sections for 'On Trusted Network' (with 'Tunnel' selected), 'VPN Trusted Network' (with 'Tunnel With Local Proxy' selected), and 'Off Trusted Network' (with 'Tunnel With Local Proxy' selected). A callout bubble points to the 'Proxy Action Type' section, which includes 'Enforce', 'Apply on Network Change' (selected), and 'Never'. At the bottom are 'Save' and 'Cancel' buttons. The main interface background shows a sidebar with 'Forwarding Profile' selected and a list of other settings like 'Trusted Networks' and 'Audit Logs'. The footer includes 'Help', 'Versions', and copyright information.

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

The screenshot shows the Zscaler Forwarding Profile configuration interface. The left sidebar is titled 'Settings' and includes options like Zscaler App Store, Audit Logs, Forwarding Profile (selected), Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IdP, and Device Posture. The main content area displays a table of forwarding profiles:

#	Profile Name	Trusted Network Criteria	Forwarding Profile Action
1	ZIA-ONLY	PRE-DEFINED TRUSTED NETWORKS Selected	ON TRUSTED NETWORK None SYSTEM PROXY Never CUSTOM PAC None
2	Default	CRITERIA None	ON TRUSTED NETWORK Tunnel SYSTEM PROXY Never CUSTOM PAC None

A message at the top of the main area says 'All Changes have been saved successfully.' The top right has 'Help' and 'Go Back' buttons. The bottom navigation bar includes 'Help' and 'Versions' buttons. Copyright information at the bottom left reads 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1'. The bottom right shows 'Weblog Time: Wednesday, Apr 1, 2020 04:41:24 PM'.

Slide notes

Slide 25 - Slide 25

The screenshot shows the Zscaler interface for managing Forwarding Profiles. The left sidebar is titled 'Settings' and includes options like Zscaler App Store, Audit Logs, Forwarding Profile (which is selected), Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, Zscaler App IDP, and Device Posture. The main content area displays a table of forwarding profiles:

#	Profile Name	Trusted Network Criteria	Forwarding Profile Action
1	ZIA-ONLY	PRE-DEFINED TRUSTED NETWORKS Selected	ON TRUSTED NETWORK None SYSTEM PROXY Never CUSTOM PAC None
2	Default	CRITERIA None	ON TRUSTED NETWORK Tunnel SYSTEM PROXY Never CUSTOM PAC None

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'. The timestamp in the footer is 'Weblog Time: Wednesday, Apr 1, 2020 04:41:24 PM'.

Slide notes

Slide 26 - Using the Zscaler App IdP for ZIA



Steps For Using the Zscaler App Portal IdP

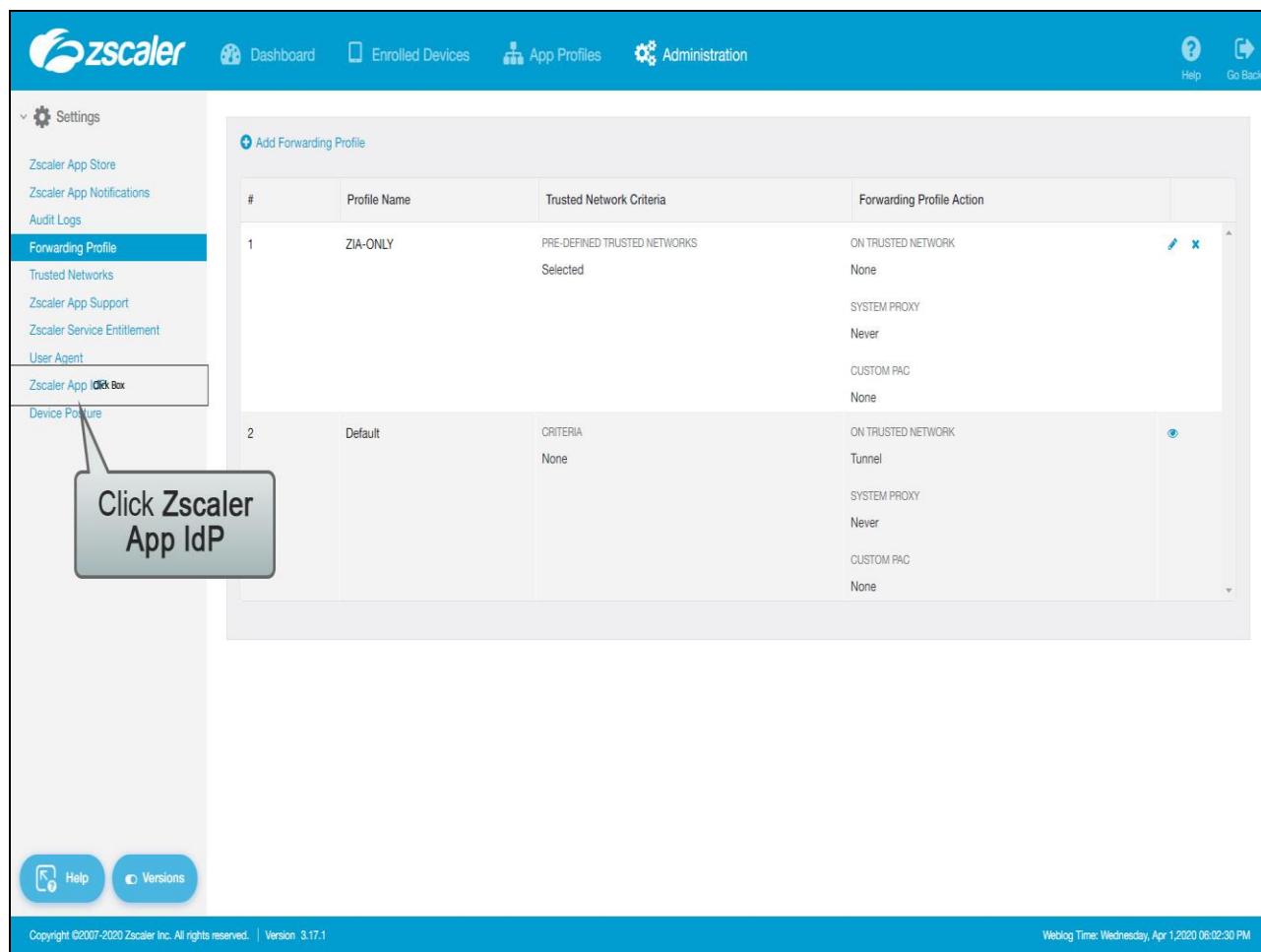
1. Add Zscaler App Portal IdP Device Tokens

- Enable silent enrollment into the App
- Create device tokens

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



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 is open under the 'Settings' section, listing options like Zscaler App Store, Audit Logs, Forwarding Profile (which is selected), Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, and Zscaler App IdP. A callout box with the text 'Click Zscaler App IdP' points to the 'Zscaler App IdP' link in the sidebar. The main content area displays a table titled 'Add Forwarding Profile' with two rows. Row 1 is for 'ZIA-ONLY' and Row 2 is for 'Default'. The table columns are '#', 'Profile Name', 'Trusted Network Criteria', and 'Forwarding Profile Action'. The 'Forwarding Profile Action' column contains sections for 'ON TRUSTED NETWORK', 'SYSTEM PROXY', and 'CUSTOM PAC'.

#	Profile Name	Trusted Network Criteria	Forwarding Profile Action
1	ZIA-ONLY	PRE-DEFINED TRUSTED NETWORKS Selected	ON TRUSTED NETWORK None SYSTEM PROXY Never CUSTOM PAC None
2	Default	CRITERIA None	ON TRUSTED NETWORK Tunnel SYSTEM PROXY Never CUSTOM PAC None

Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1 Weblog Time: Wednesday, Apr 1, 2020 06:02:30 PM

Slide notes

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

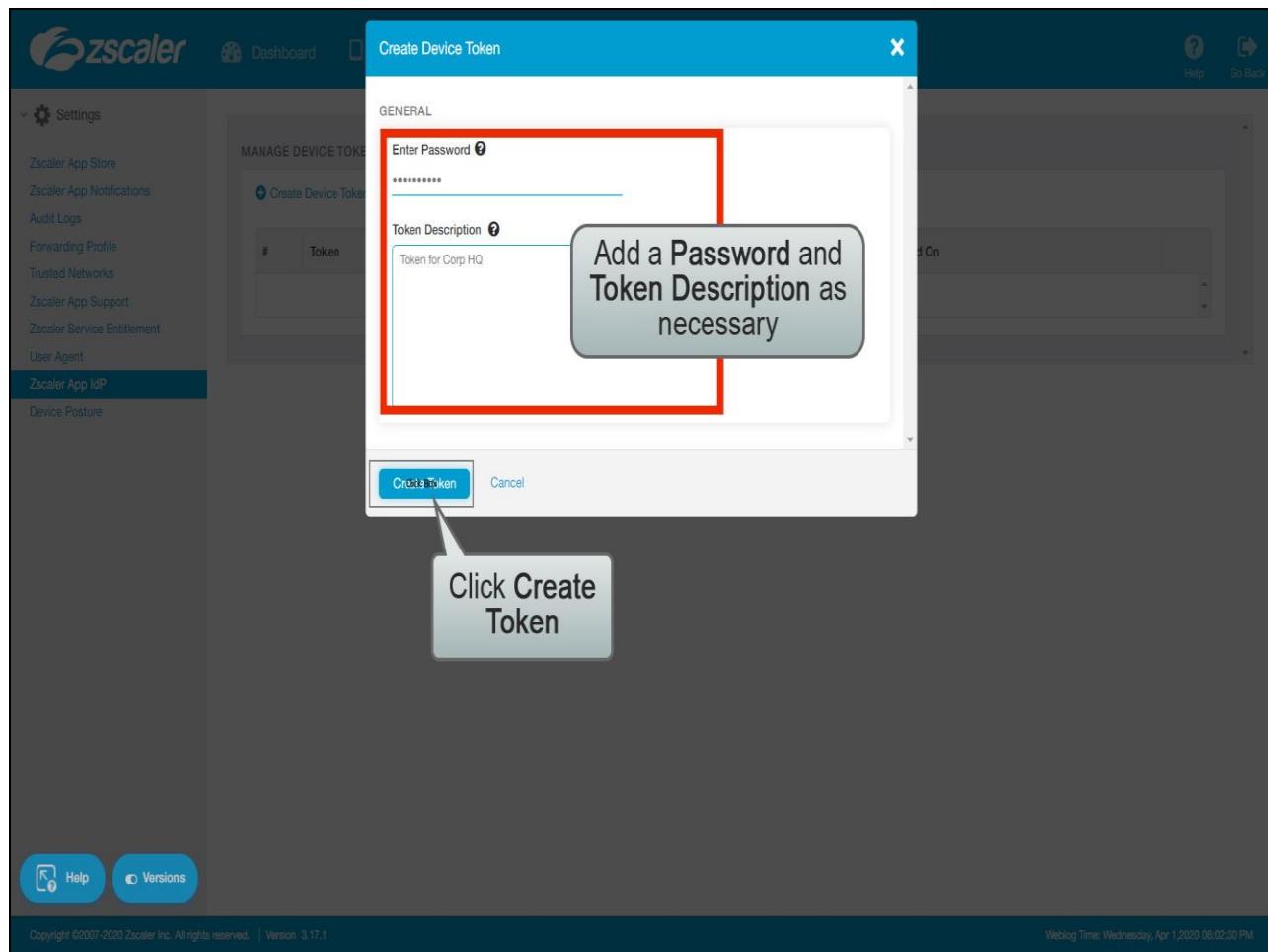
Slide 28 - Slide 28

The screenshot shows the Zscaler App IdP 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 various settings like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, and Zscaler App IdP, with Zscaler App IdP being the active tab. Below the sidebar is a message: "Waiting for help.zscaler.com...". The main content area is titled "MANAGE DEVICE TOKENS" and contains a table with columns for #, Token, Description, and Created On. A callout box points to the "Create Device Token" button, which is highlighted with a blue border. The message "No matching items found" is displayed below the table. At the bottom right, it says "Weblog Time: Wednesday, Apr 1, 2020 06:02:30 PM".

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

The screenshot shows the Zscaler App IDP interface. The top navigation bar includes the Zscaler logo, a dashboard icon, and a message stating "All Changes have been saved successfully." On the right side of the header are "Help" and "Go Back" buttons. The left sidebar contains a "Settings" section with various options like Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support, Zscaler Service Entitlement, User Agent, and Zscaler App IDP, which is currently selected and highlighted in blue. Below these are "Device Posture" and two buttons: "Help" and "Versions". The main content area is titled "MANAGE DEVICE TOKENS" and features a "Create Device Token" button. A table lists one device token: # 1, Token 436b39646f645237714955394e6c313379667231636..., Description "Token for Corp HQ", and Created On "Wed Apr 01 2020 18:13:42 GMT+0700 (Indochina Time)". The bottom of the screen displays copyright information "Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1" and a timestamp "Weblog Time: Wednesday, Apr 1, 2020 06:02:30 PM".

Slide notes

Slide 31 - Slide 31

The screenshot shows the Zscaler App Profiles interface with the 'Manage Device Tokens' page open. A specific token entry is highlighted with a red box, and a callout box points to it with the text: 'Token value to pass to Zscaler App on install'. The table in the interface includes columns for #, Token, Description, and Created On.

#	Token	Description	Created On
1	436b39646f645237714955394e6c313379667231636...	Token for Corp HQ	Wed Apr 01 2020 18:13:42 GMT+0700 (Indochina Time)

Annotations:

- A red box highlights the 'Token' column of the first row in the table.
- A callout box with a gray border and black text points to the highlighted token value, containing the text: 'Token value to pass to Zscaler App on install'.

Page footer:

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

Weblog Time: Wednesday, Apr 1, 2020 06:02:30 PM

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



Steps For Using the Zscaler App Portal IdP

1. Add Zscaler App Portal IdP Device Tokens

- Enable silent enrollment into the App
- Create device tokens

2. Add Zscaler App Portal IdP in ZIA

- Add the Zscaler App IdP as an option in the ZIA Admin Portal

Slide notes

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

Slide 33 - Slide 33

The screenshot shows the Zscaler App Portal interface. At the top, there's a navigation bar with links for Dashboard, Enrolled Devices, App Profiles, Administration, Help, ClickBox, and Go Back. 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 (which is highlighted), and Device Posture. Below the sidebar are two buttons: 'Help' and 'Versions'. The main content area is titled 'MANAGE DEVICE TOKENS' and includes a 'Create Device Token' button. A table lists two device tokens:

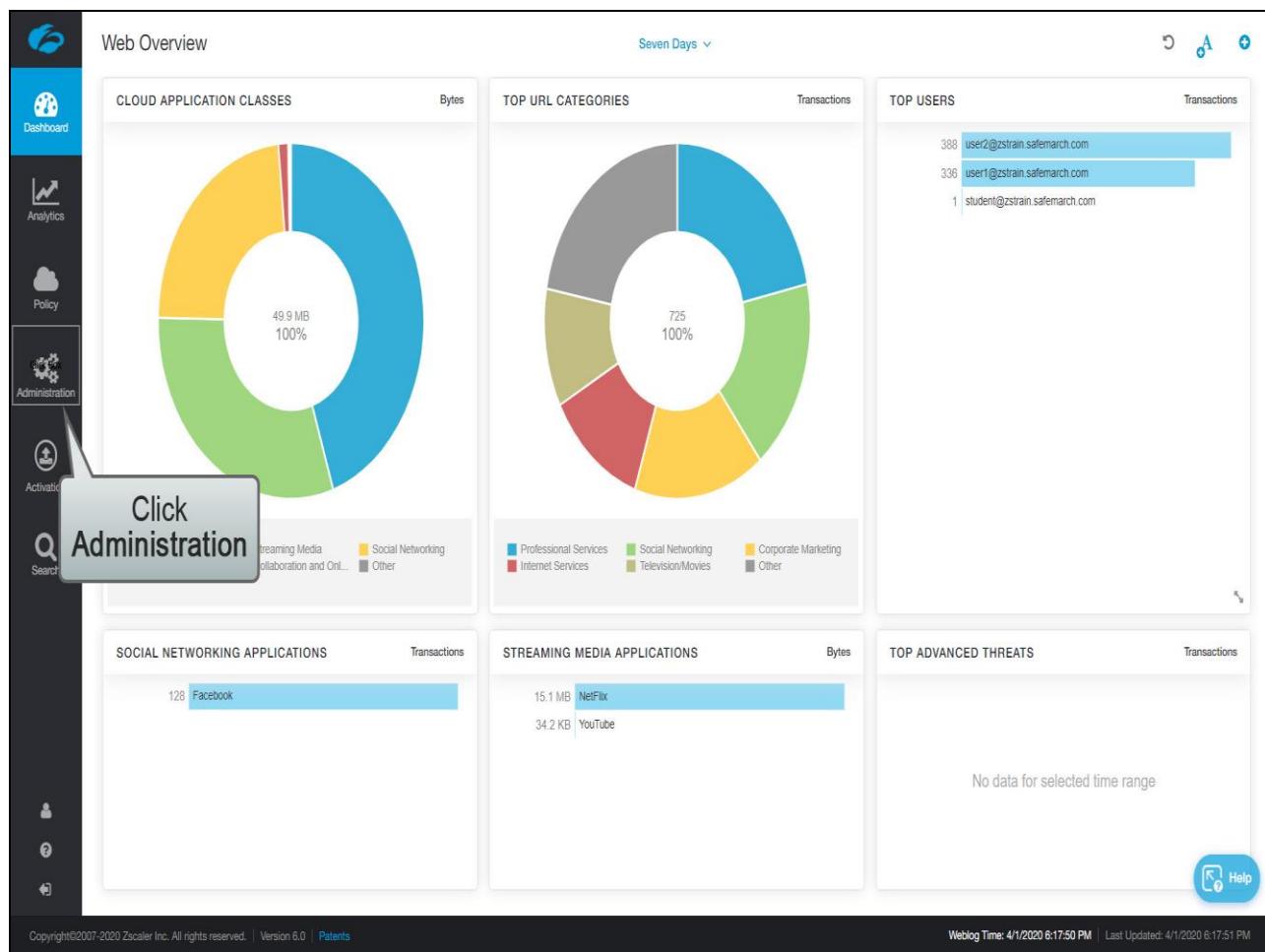
#	Token	Description	Created On
1	436b39646f645237714955394e6c313379667231636...	Token for Corp HQ	Wed Apr 01 2020 18:13:42 GMT+0700 (Indochina Time)
2	4a474b314f656d4f72447a38326b3364594f6f7431423...	Token for NYC Office	Wed Apr 01 2020 18:16:07 GMT+0700 (Indochina Time)

A callout box with the text 'Click Go Back' points to the 'Go Back' button in the top right corner of the main content area.

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

The screenshot shows the Zscaler Cloud interface. On the left, a sidebar lists various management sections: Account Management, Cloud Configuration, My Profile, Company Profile, Alerts, Print All Policies, SaaS Application Tenants, Authentication (with Authentication Settings highlighted), Administration (with User Management and Identity Proxy settings), Activation, Search, Traffic Forwarding, Location Management, VPN Credentials, Hosted PAC Files, eZ Agent Configurations, SecureAgent Notifications, Firewall Filtering, Network Services, Network Applications, and IP & FQDN Groups. A large callout box with the text "Click Authentication Settings" points to the highlighted section. The main content area has four panels: "TOP URL CATEGORIES" (a donut chart showing 725 transactions across six categories: Professional Services, Social Networking, Corporate Marketing, Television/Movies, Internet Services, and Other), "TOP USERS" (a list of three users with transaction counts: user2@zstrain.safemarch.com (388), user1@zstrain.safemarch.com (336), and student@zstrain.safemarch.com (1)), "STREAMING MEDIA APPLICATIONS" (a bar chart showing bytes transferred: Netflix (15.1 MB) and YouTube (34.2 KB)), and "TOP ADVANCED THREATS" (a panel stating "No data for selected time range"). The bottom of the screen shows copyright information ("Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 8.0 | Patents") and a timestamp ("Weblog Time: 4/1/2020 6:17:50 PM | Last Updated: 4/1/2020 6:17:51 PM").

Slide notes

...then Authentication Settings, ...

Slide 36 - Slide 36

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Authentication Settings' and contains several tabs: 'AUTHENTICATION PROFILE' (selected), 'IDENTITY PROVIDERS' (highlighted with a red box and a callout bubble saying 'Click IDENTITY PROVIDERS'), and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', there are sections for 'Directory Type' (Hosted DB selected), 'Authentication Frequency' (Only Once), 'Authentication Type' (Form-Based selected), and 'Temporary Authentication' (Disabled selected). Below these are sections for 'PASSWORD STRENGTH' (Medium) and 'PASSWORD EXPIRY' (Never). A 'KERBEROS AUTHENTICATION' section has an 'Enable Kerberos' checkbox (unchecked). At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' icon.

Slide notes

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

Slide 37 - Slide 37

The screenshot shows the 'Authentication Settings' page in the Zscaler App Portal. On the left is a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area has tabs for 'AUTHENTICATION PROFILE', 'IDENTITY PROVIDERS NEW', and 'AUTHENTICATION BRIDGES'. A sub-section titled 'Add Identity Provider' contains a button labeled 'Add Zscaler App Portal as IdP'. A callout box with the text 'Click Add Zscaler App Portal as IdP' points to this button. Below the sub-section are columns for No., ID, Name, Status, Location, IdP SSL Certificate E..., Authentication Domains, Default IdP, and a more options icon. A single row is listed: No. 1, ID 2249, Name Okta, Status green checkmark, Location Any, Authentication Domains 8, Default IdP. At the bottom are 'Save' and 'Cancel' buttons, and a 'Help' button on the right.

Slide notes

Click the Add Scaler App Portal as IdP link.

Slide 38 - Slide 38

The screenshot shows the Zscaler App Portal's 'Identity Providers' section. A modal window titled 'Add Zscaler App Portal as IdP' is open. Inside the modal, there is a 'DOMAINS' section with a dropdown menu set to 'Any'. A callout box with the text 'Click in the Authentication Domains field' points to this dropdown. The modal also contains other fields like 'Status' (Enabled/Disabled), 'Enable SAML Auto-Discovery' (disabled), and 'Save' and 'Cancel' buttons.

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, ...

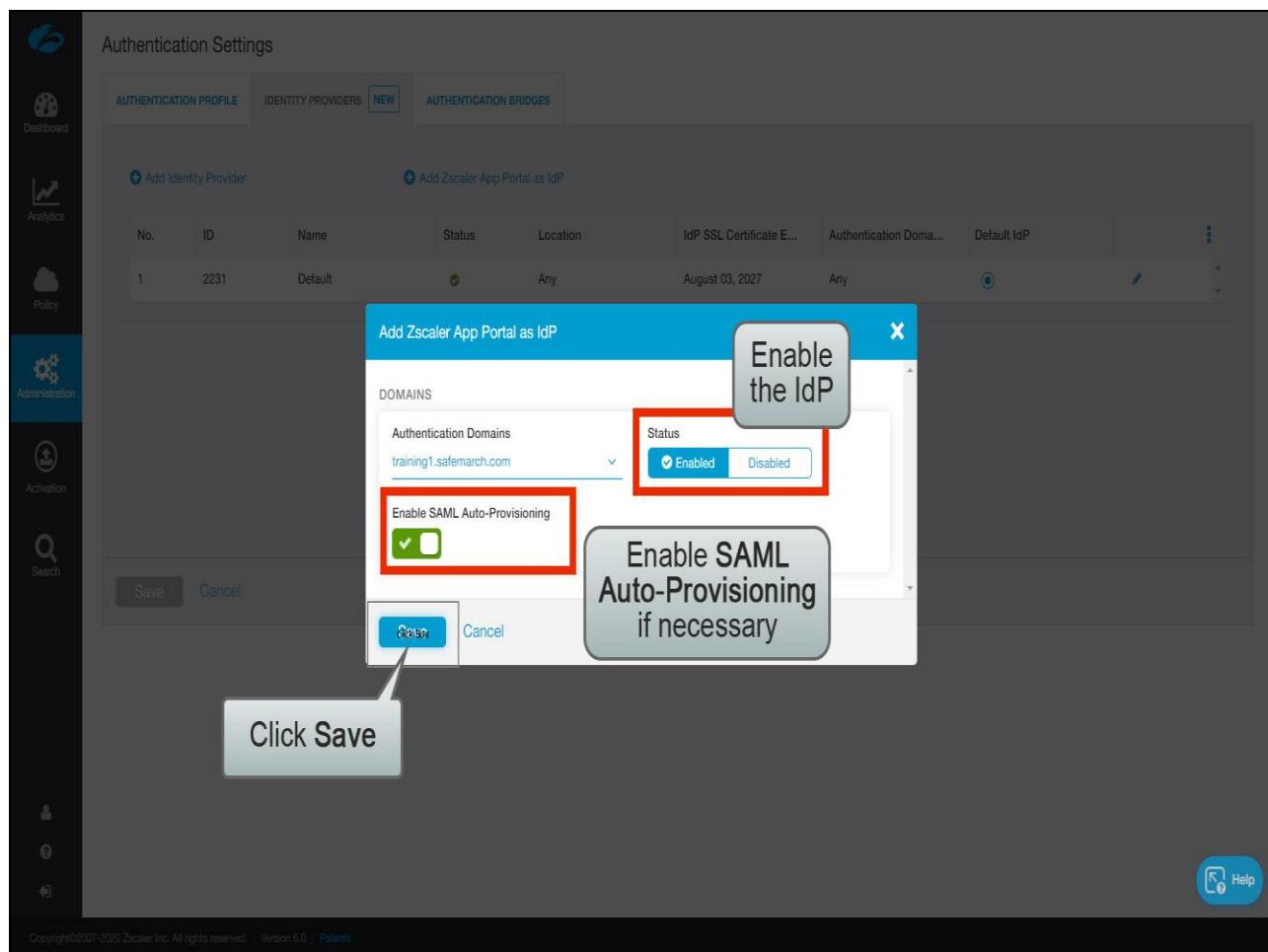
Slide 39 - Slide 39

The screenshot shows the Zscaler App Portal interface under 'Authentication Settings'. A modal window titled 'Add Zscaler App Portal as IdP' is open, specifically for adding domains. The modal has a 'DOMAINS' section with a search bar and two tabs: 'Unselected Items' and 'Selected Items (1)'. The item 'training1.safemarch.com' is selected, indicated by a red border around the checkbox. A callout bubble points to this selection with the text 'Select one or more Domains'. Another callout bubble points to the 'Done' button at the bottom left of the modal with the text 'Click Done'. The background shows a table of authentication profiles, with one row highlighted for profile ID 2231.

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

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with various icons: Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main content area has a title 'Authentication Settings' at the top. Below it are three tabs: 'AUTHENTICATION PROFILE' (which is highlighted with a red box and a blue arrow pointing to it), 'IDENTITY PROVIDERS' (with a 'NEW' button), and 'AUTHENTICATION BRIDGES'. A large central table lists authentication profiles. The first profile in the table is highlighted with a gray box and contains the text 'Click AUTHENTICATION PROFILE'. The table columns include 'No.', 'Location', 'IdP SSL Certificate E...', 'Authentication Domains', 'Default IdP', and a 'More' icon. At the bottom of the table are 'Save' and 'Cancel' buttons. In the bottom right corner of the main window is a 'Help' button.

No.	Location	IdP SSL Certificate E...	Authentication Domains	Default IdP	
1	Any	April 26, 2028	Any	<input checked="" type="radio"/>	<input type="button" value="Edit"/> <input type="button" value="X"/>
2	2248	Z-App Mobile Idp	None	<input type="radio"/>	<input type="button" value="Edit"/> <input type="button" value="X"/>

Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 8.0 | Patents

Weblog Time: 4/2/2020 12:55:33 PM | Last Updated: 4/2/2020 12:55:35 PM

Help

Slide notes

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

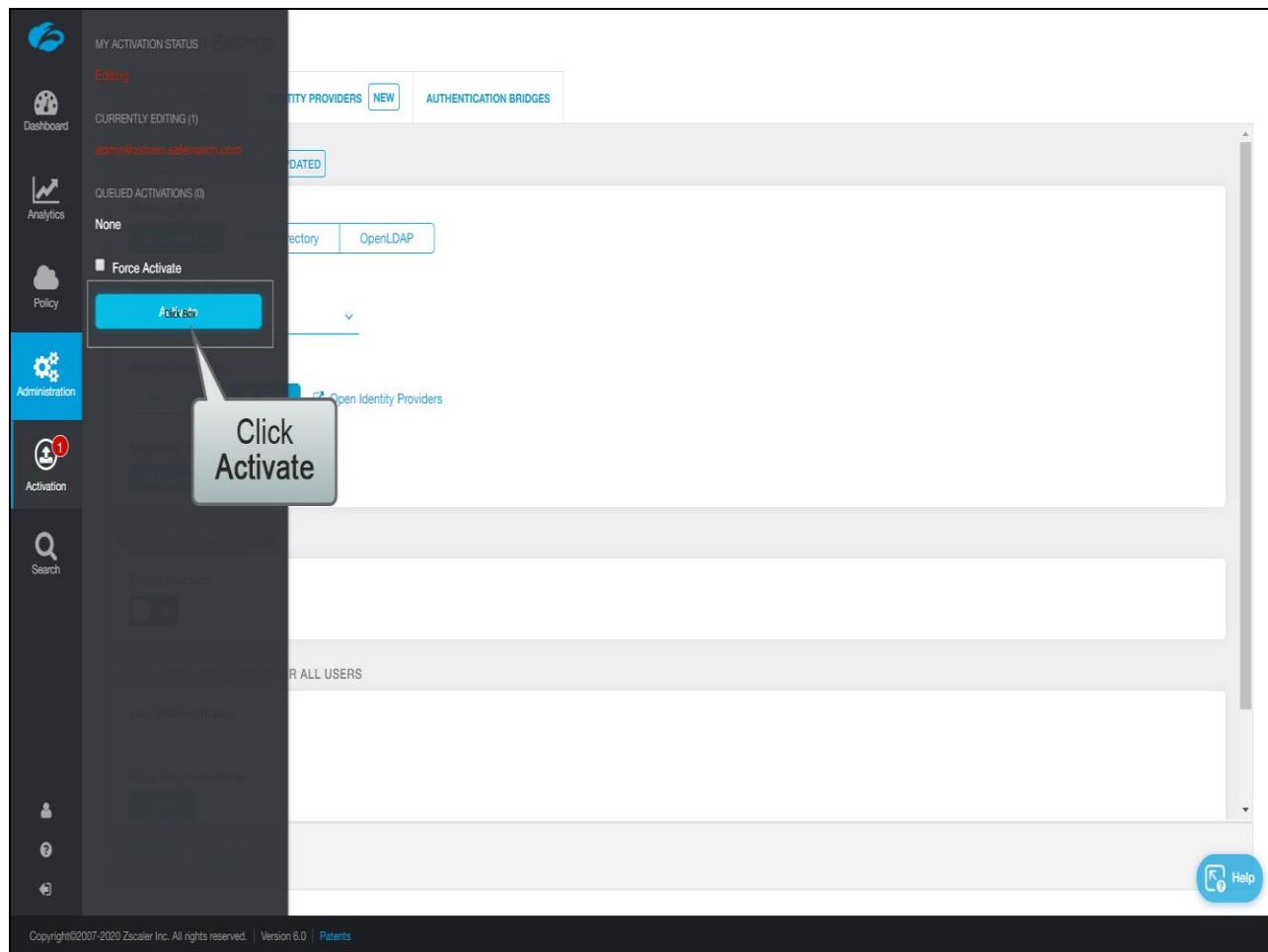
Slide 42 - Slide 42

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration (with a red notification badge), Activation (with a red notification badge), and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' (selected), 'IDENTITY PROVIDERS' (NEW), and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', the 'UPDATED' status is shown. The 'Directory Type' is set to 'Hosted DB'. The 'Authentication Frequency' is 'Only Once'. The 'Authentication Type' is set to 'SAML' (highlighted with a red box). The 'Temporary Authentication' option is 'Disabled'. A callout box points to the 'SAML' button with the text 'Verify that SAML authentication is enabled'. Below this, the 'KERBEROS AUTHENTICATION' section is visible. At the bottom, there's a 'FORCE REAUTENTICATION FOR ALL USERS' section with 'Last Reauthentication' and 'Force Reauthentication' buttons, and a 'Save' and 'Cancel' button. A 'Help' icon is also present.

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

The screenshot shows the Zscaler Authentication Settings interface. A prominent message at the top right says "Activation Completed!". Below this, there are three tabs: "AUTHENTICATION PROFILE" (selected), "IDENTITY PROVIDERS" (with a "NEW" button), and "AUTHENTICATION BRIDGES". Under the "AUTHENTICATION PROFILE" tab, the "Directory Type" section has "Hosted DB" selected. The "Authentication Frequency" dropdown is set to "Only Once". The "Authentication Type" section includes "Form-Based" (selected) and "SAML" options, with a link to "Open Identity Providers". The "Temporary Authentication" section has "Disabled" selected. In the "KERBEROS AUTHENTICATION" section, the "Enable Kerberos" checkbox is unchecked. The "FORCE REAUTHENTICATION FOR ALL USERS" section contains "Last Reauthentication" and "Force Reauthentication" fields, with a "Start" button. At the bottom are "Save" and "Cancel" buttons, and a "Help" icon.

Slide notes

Slide 45 - Slide 45

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for AUTHENTICATION PROFILE (selected), IDENTITY PROVIDERS (NEW), and AUTHENTICATION BRIDGES. Under AUTHENTICATION PROFILE, there are sections for Directory Type (Hosted DB selected), Authentication Frequency (Only Once), Authentication Type (Form-Based selected, SAML, Open Identity Providers), and Temporary Authentication (Disabled selected, One-Time Link). Below these are sections for KERBEROS AUTHENTICATION (Enable Kerberos is off) and FORCE REAUTHENTICATION FOR ALL USERS (Last Reauthentication and Force Reauthentication buttons, Start button). At the bottom are Save and Cancel buttons, and a Help icon.

Slide notes

Slide 46 - Steps For Using the Zscaler App IdP



Steps For Using the Zscaler App Portal IdP

1. Add Zscaler App Portal IdP Device Tokens

- Enable silent enrollment into the App
- Create device tokens

2. Add Zscaler App Portal IdP in ZIA

- Add the Zscaler App IdP as an option in the ZIA Admin Portal

3. Install Zscaler App Using the Device Tokens

- Apply a token when installing the App
- Zscaler App uses the user ID from the device login, and the token for a silent enrollment

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

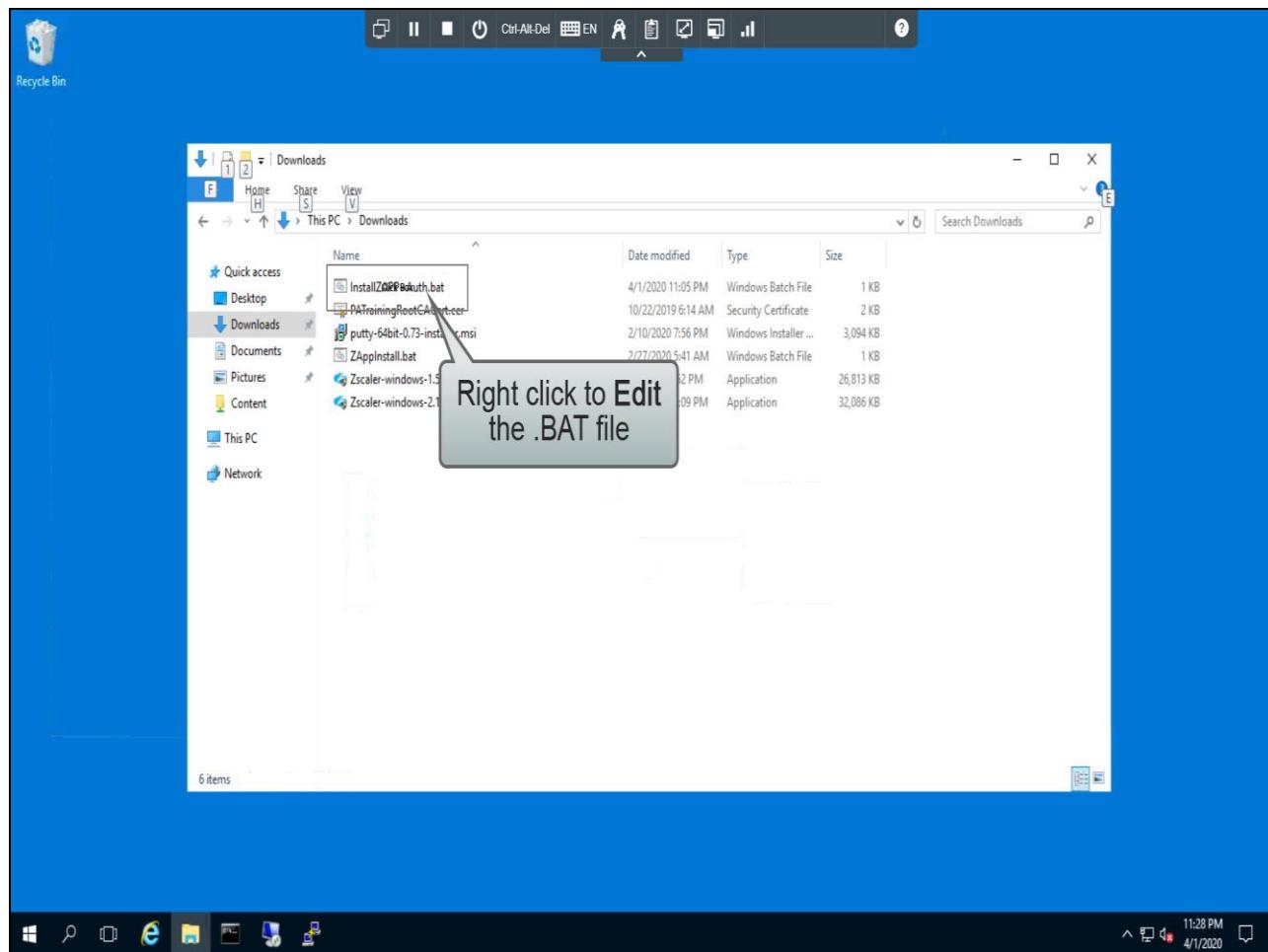
The screenshot shows the Zscaler App Portal interface. The left sidebar has a 'Zscaler App IdP' section selected. The main area is titled 'MANAGE DEVICE TOKENS' and contains a table with two rows. The first row's 'Token' column is highlighted with a red box. A callout bubble points to this row with the text: 'Copy the Token value for use with the Zscaler App installer'. The table columns are '#', 'Token', 'Description', and 'Created On'. The second row's 'Token' column starts with '4a474b314f656d4f72447a38326b3364594f6f74314234644d4452496761614e77a594d3...'. The 'Description' column for both rows is 'Token for NYC Office'. The 'Created On' column shows 'Wed Apr 01 2020 18:13:42 GMT+0700 (Indochina Time)' for the first row and 'Wed Apr 01 2020 18:16:07 GMT+0700 (Indochina Time)' for the second row.

#	Token	Description	Created On
1	4a474b314f656d4f72447a38326b3364594f6f74314234644d4452496761614e77a594d3... 8615739632b553d	Token for NYC Office	Wed Apr 01 2020 18:13:42 GMT+0700 (Indochina Time)
2	4a474b314f656d4f72447a38326b3364594f6f7431423...	Token for NYC Office	Wed Apr 01 2020 18:16:07 GMT+0700 (Indochina Time)

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.

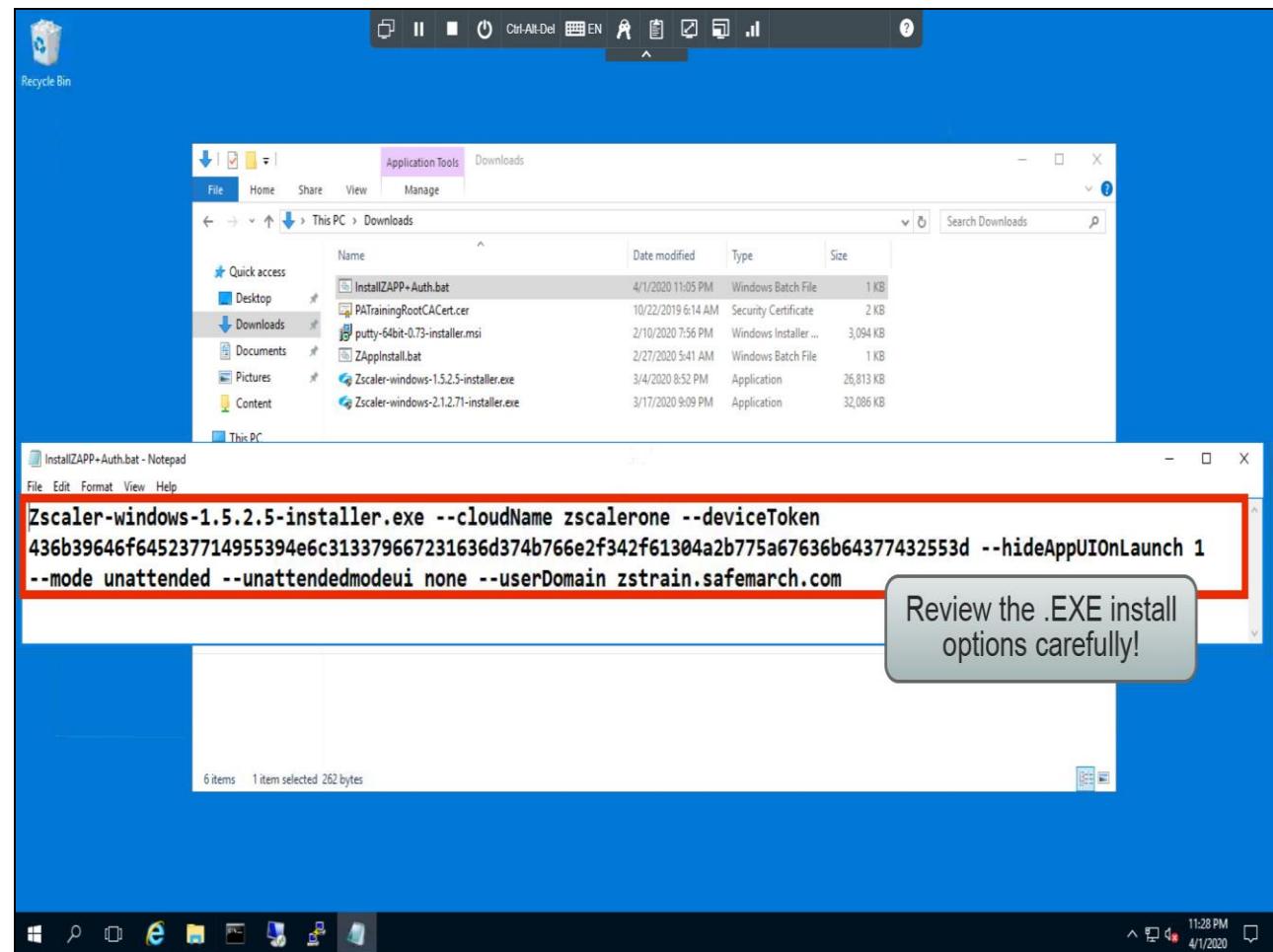
Slide 48 - Slide 48



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

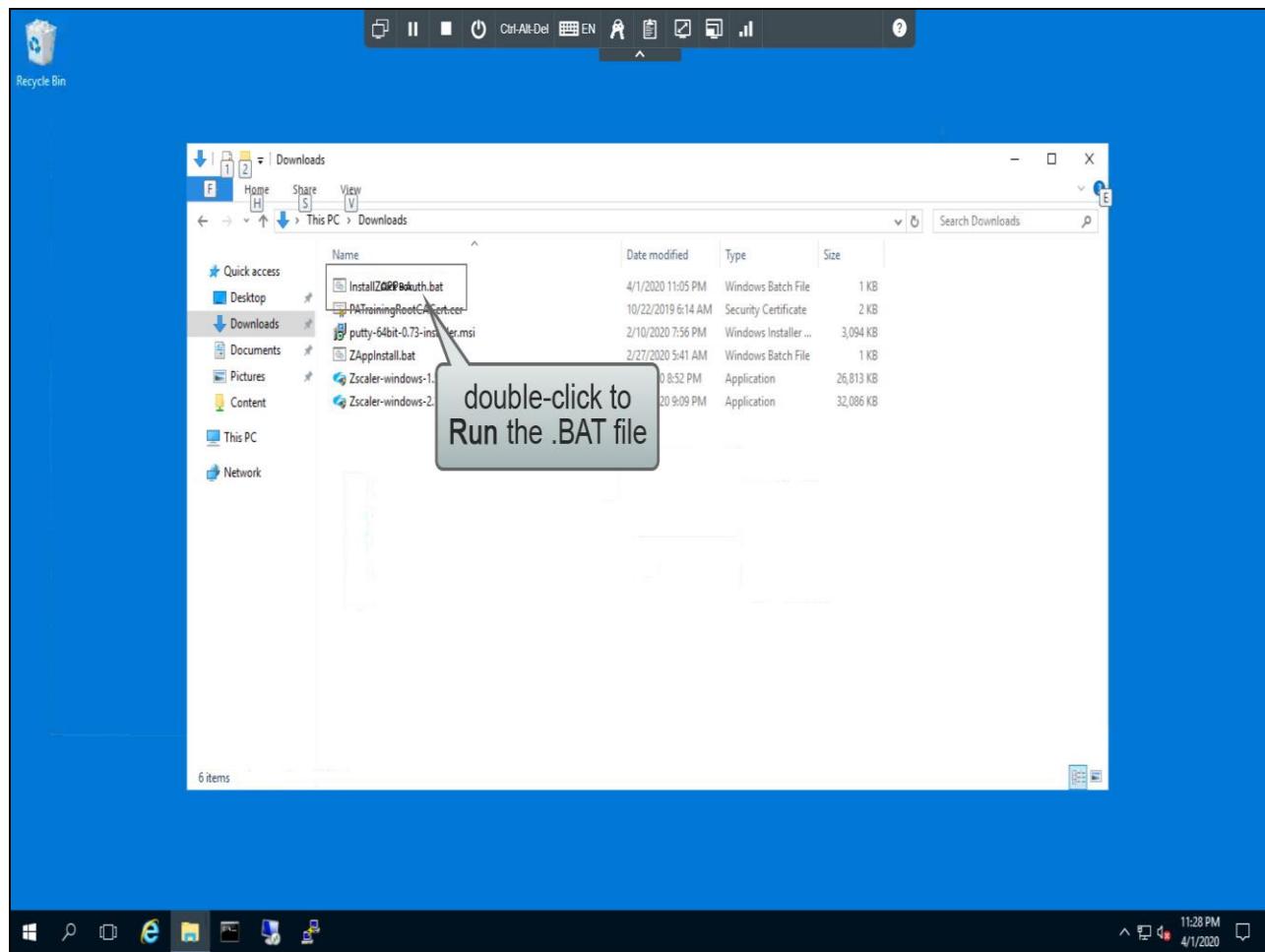


Slide notes

...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.

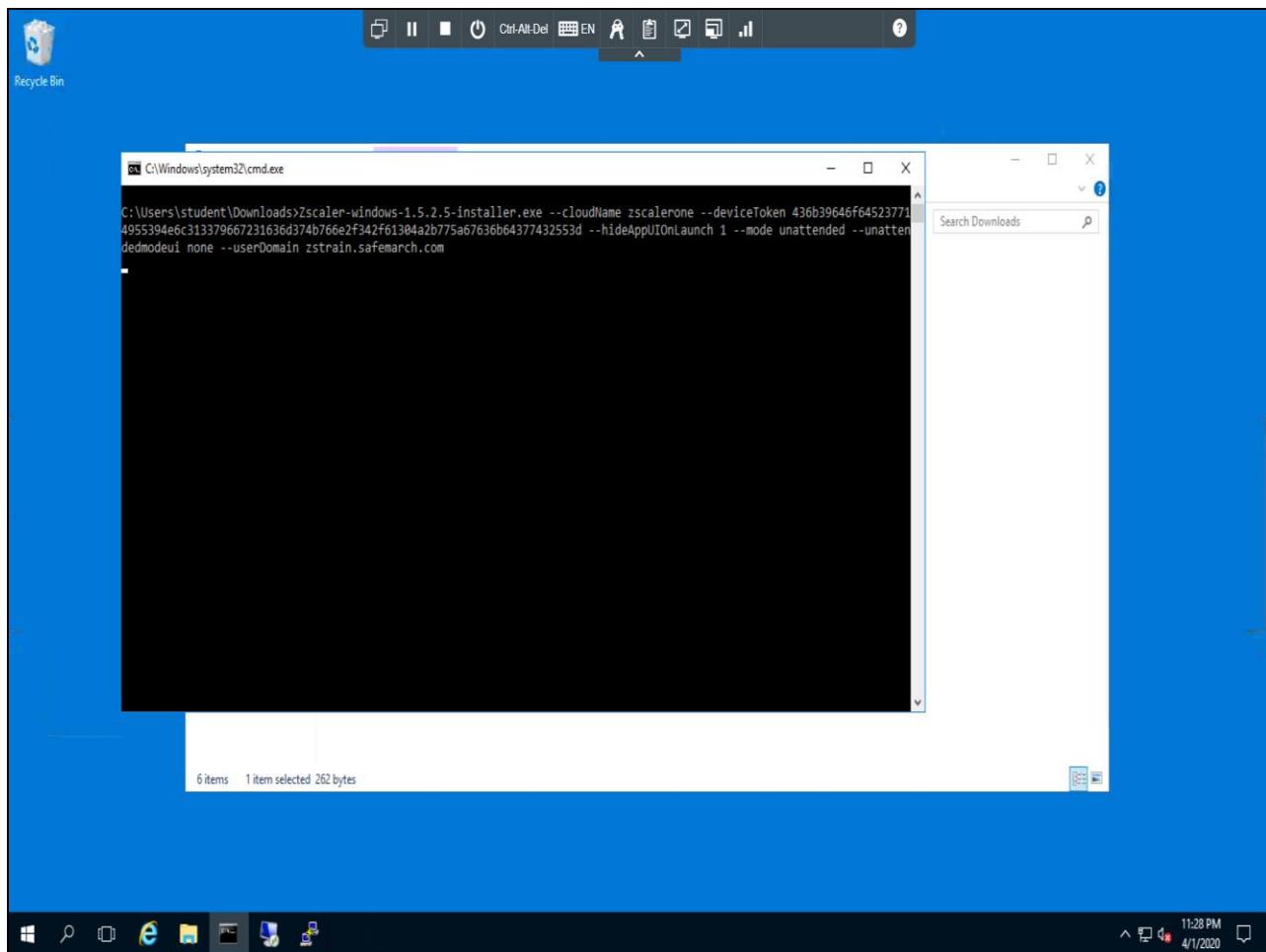
Slide 50 - Slide 50



Slide notes

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

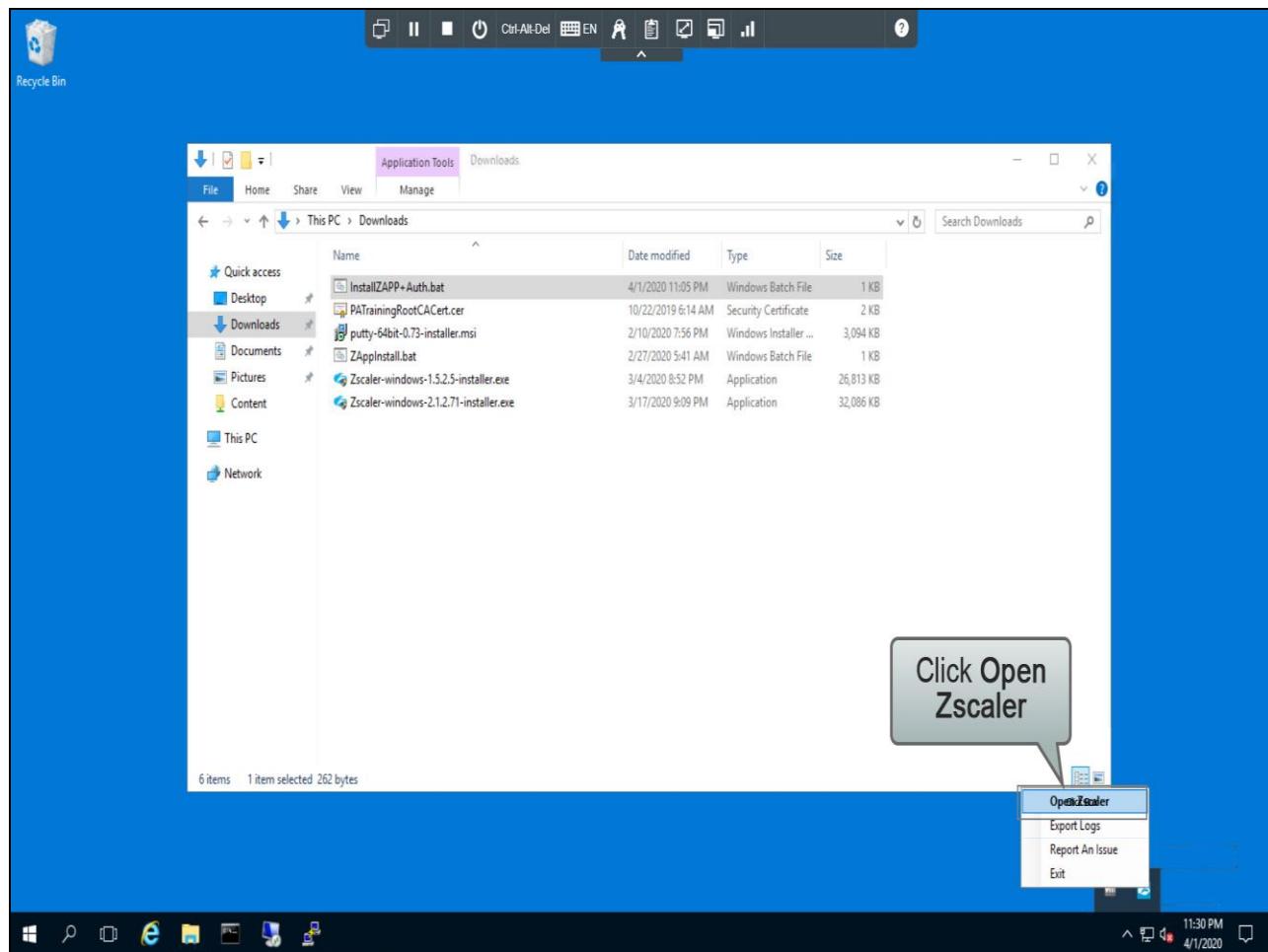
Slide 51 - Slide 51



Slide notes

...and just sit back and wait.

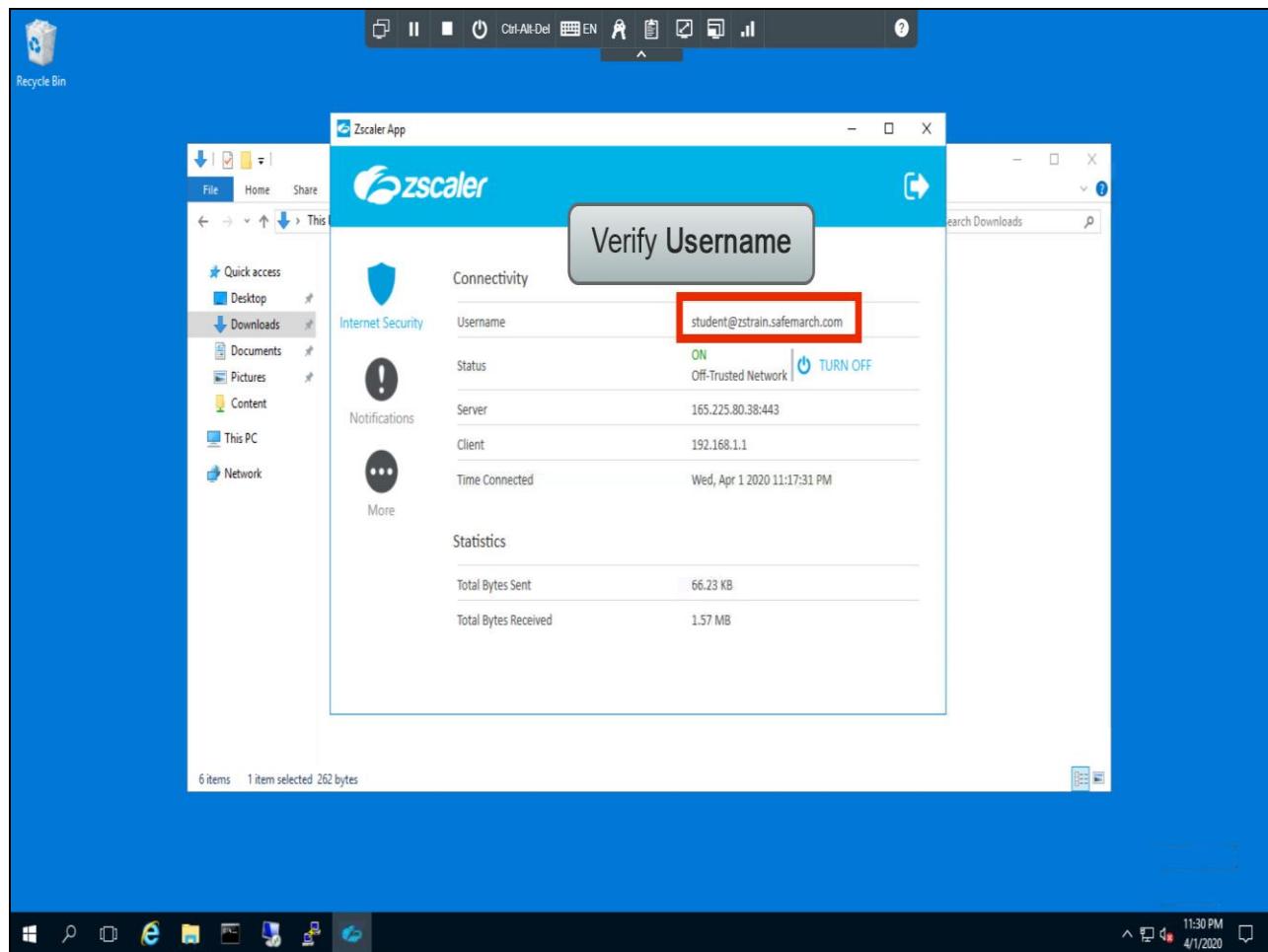
Slide 52 - Slide 52



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



Steps For Enabling SSL Inspection for Zscaler App Users

1. Install the CA Certificate on the User's Device

- Install Certificate option
- Upload Custom certificate if required

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

The screenshot shows the Zscaler App Support interface. The left sidebar includes options like Settings, Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, and Zscaler App Support (which is highlighted with a red box). The main content area has tabs for APP SUPPORTABILITY, FAIL OPEN, USER PRIVACY, ENDPOINT INTEGRATION, DEVICE CLEANUP, and ADVANCED CONFIGURATION (also highlighted with a red box). A callout box labeled 'Click App Profiles' points to the 'App Profiles' tab in the top navigation. Another callout box points to the 'Custom Certificate' section, which contains a 'Custom Certificate' link and an 'Upload' button.

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

The screenshot shows the Zscaler App Profiles interface. The left sidebar lists platforms: Windows (selected), macOS, iOS, and Android. The main area displays a table titled "Add Windows Policy". The table has columns: Rule#, Policy Name, Policy Description, User Groups, and Status. Two rows are present: Row 1 (Users-Standard) has User Groups set to "Users" and Status to "Enabled"; Row 2 (Default) has User Groups set to "ALL" and Status to "Enabled". In the top right corner of the table, there is an "Edit" icon represented by a small box with a "ClickBox" label and an "X". A callout box with the text "Click to Edit a profile" points to this icon. At the bottom of the interface, there are "Help" and "Versions" buttons, and a copyright notice: "Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1". The status bar at the bottom right shows "Weblog Time: Wednesday, Apr 1, 2020 06:59:04 PM".

Rule#	Policy Name	Policy Description	User Groups	Status
1	Users-Standard		Users	Enabled
2	Default	Default Policy	ALL	Enabled

Slide notes

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

Slide 58 - Slide 58

The screenshot shows the 'Edit Windows Policy' dialog box from the Zscaler interface. The 'GENERAL' section is visible, containing fields for Rule Order (set to 1), Groups (set to Users), Disable Password (set to *****), Forwarding Profile (set to Default), Log Mode (set to Error), and various other settings like Log File Size in MB (set to 100) and Override WPAD (set to checked). A specific checkbox, 'Install Zscaler SSL Certificate', is highlighted with a red rectangular border. A callout bubble with the text 'Enable the Install Zscaler SSL Certificate option if necessary' points to this checkbox. The bottom of the dialog box has 'Save' and 'Cancel' buttons.

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

The screenshot shows the Zscaler Admin UI interface. The top navigation bar includes links for Dashboard, Enrolled Devices, App Profiles, Administration, Help, and Go Back. On the left, a sidebar titled 'Platforms' lists 'Windows' (selected), 'macOS', 'iOS', and 'Android'. The main content area displays a table titled 'Add Windows Policy' with two rows:

Rule#	Policy Name	Policy Description	User Groups	Status	Action
1	Users-Standard		Users	Enabled	
2	Default	Default Policy	ALL	Enabled	

At the bottom of the screen, there are 'Help' and 'Versions' buttons, and a status message 'Waiting for www.youtube.com...'.

Slide notes

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



Steps For Enabling SSL Inspection for Zscaler App Users

1. Install the CA Certificate on the User's Device

- Install Certificate option
- Upload Custom certificate if required

2. Configure SSL Inspection in the ZIA Admin Portal

- Configure SSL Inspection from the Zscaler App Portal > Policy > SSL Inspection page
- Enable/disable SSL inspection on a per-platform basis
 - Windows
 - macOS
 - Android
 - iOS

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

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' contains links for Zscaler App Store, Audit Logs, Forwarding Profile, Trusted Networks, Zscaler App Support (which is currently selected), Zscaler Service Entitlement, User Agent, Zscaler App IdP, and Device Posture. The main content area displays 'DIRECTORY SYNC STATUS' with a note about the 'Next Directory Group Sync Time' (Thu Apr 02 2020 13:12:14 GMT+0700 (Indochin...)). It also includes a section for 'Sync Directory Groups Manually' with a 'Sync Groups' button, and a 'CUSTOM ROOT CERTIFICATE' section with a 'Custom Certificate' link and an 'Upload' button. At the bottom, there are 'Help' and 'Versions' buttons, and a footer noting 'Copyright ©2007-2020 Zscaler Inc. All rights reserved. | Version: 3.17.1' and 'Weblog Time: Thursday, Apr 2, 2020 02:06:02 PM'.

Slide notes

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

Slide 62 - Slide 62

The screenshot shows the Zscaler Cloud Security Platform dashboard. On the left sidebar, under the 'Policy' section, there is a red box highlighting the 'SSL Inspection' link. A gray callout bubble with the text 'Click SSL Inspection' points to this link. The main dashboard area displays several charts and tables. One chart is a donut chart titled 'TOP URL CATEGORIES' showing transactions over 'Seven Days'. The categories and their percentages are: Corporate Marketing (blue, 427), Internet Services (red, 100%), Professional Services (green, ~15%), Entertainment (yellow, ~10%), and Other (gray, ~5%). Below the chart is a legend: Corporate Marketing (blue), Internet Services (red), Professional Services (green), Entertainment (yellow), and Other (gray). Another chart titled 'STREAMING MEDIA APPLICATIONS' shows bytes transferred, with Netflix at 15.1 MB. A table titled 'TOP USERS' lists two users: user2@zstrainsafemarch.com (388 transactions) and student@zstrainsafemarch.com (39 transactions). A message at the bottom right says 'No data for selected time range'. The bottom of the screen shows copyright information and a help icon.

Slide notes

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

Slide 63 - Slide 63

The screenshot shows the 'SSL Inspection' configuration page. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy (highlighted in blue), Administration, Activation, and Search. The main content area is titled 'SSL Inspection' and contains the following sections:

- Configure SSL Inspection Policy:** A note stating "SSL Inspection is configured on a per location basis with the parameters defined on this page."
- IF SSL INSPECTION IS DISABLED, BLOCK HTTPS TO THESE SITES:**

 - Blocked URL Categories:** Set to "None".
 - Blocked URLs:** A table with one row showing "Add Items" and "Add Items" buttons. A note says "Max: 25k Used: 0".
 - Show Notifications for Blocked Traffic:** A toggle switch is turned off.

- POLICY FOR SSL INSPECTION:**

 - Inspect Sessions for These URL Categories:** Set to "Any".
 - Block Undecryptable Traffic:** A toggle switch is turned off.
 - Exempt These URL Categories from Inspection & Other Policies:** Set to "None".
 - Exempt These Hosts from Inspection & Other Policies:** A table with "Add Items" and "Add Items" buttons.

A large gray callout box with the text "Scroll down..." is positioned on the right side of the page, pointing towards the bottom.

At the bottom of the page, there are copyright information ("Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 8.0 | Patents") and a timestamp ("Weblog Time: 4/2/2020 2:06:44 PM | Last Updated: 4/2/2020 2:06:45 PM"). A "Help" button is also located at the bottom right.

Slide notes

Scroll down to the bottom of the page, ...

Slide 64 - Slide 64

SSL Inspection

Configure SSL Inspection Policy
SSL Inspection is configured on a per location basis with the parameters defined on this page.

POLICY FOR Z APP

Windows: Enabled (checked) / Disabled

macOS: Enabled / **Disabled** (checked)

Android: Enabled / **Disabled** (checked)

iOS: Enabled / **Disabled** (checked)

Enable/Disable SSL Inspection on a per-platform basis

INTERMEDIATE ROOT CERTIFICATE AUTHORITY FOR SSL INSPECTION

Zscaler's Default Certificate
Download Zscaler Root Certificate

CSR for Custom Certificate
Not Available | Generate New CSR

Custom Certificate
Not Available

SSL chain certificate

Save Cancel Help

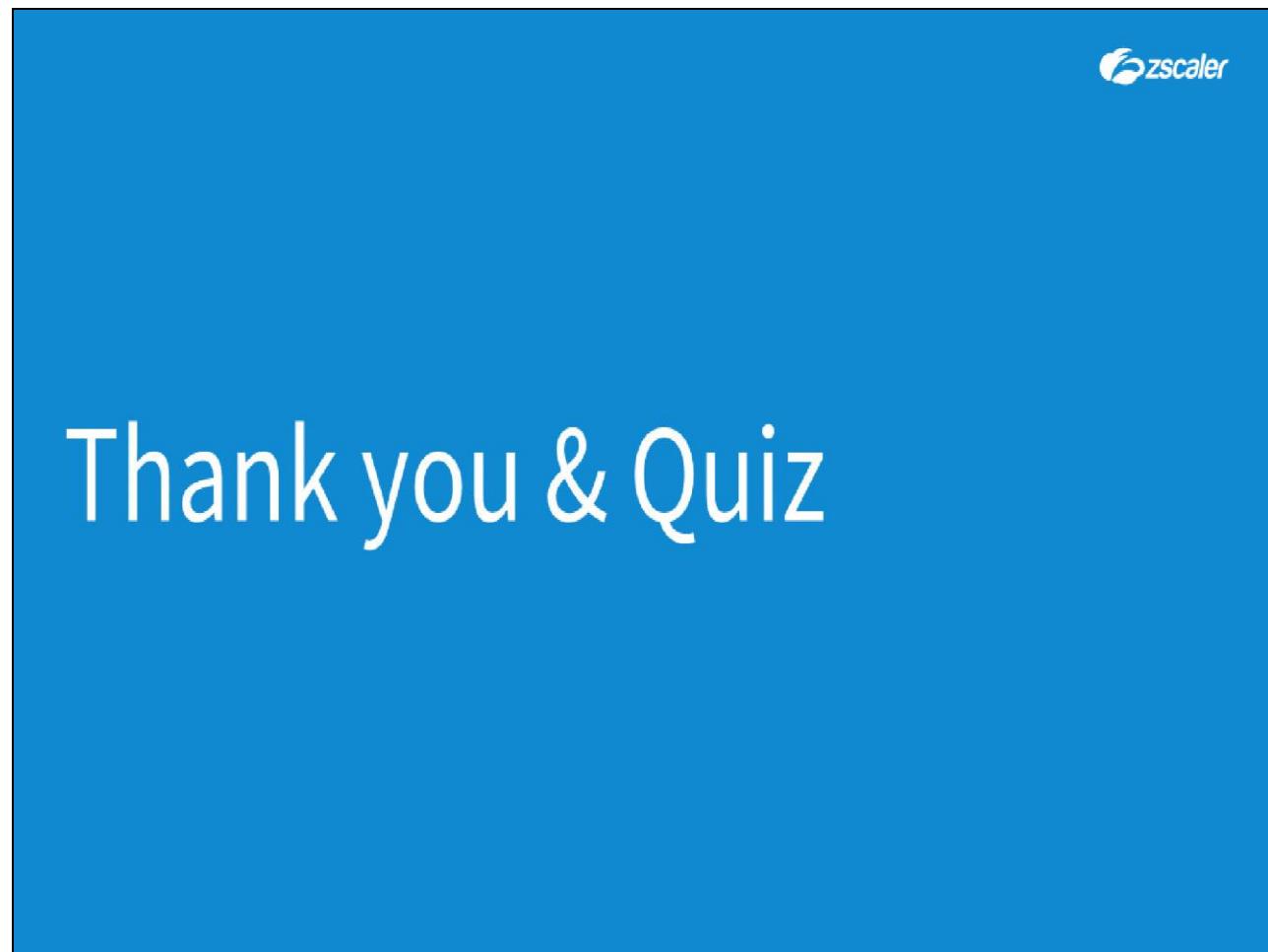
Copyright©2007-2020 Zscaler Inc. All rights reserved. | Version 8.0 | Patents

Weblog Time: 4/2/2020 2:06:44 PM | Last Updated: 4/2/2020 2:06:45 PM

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.