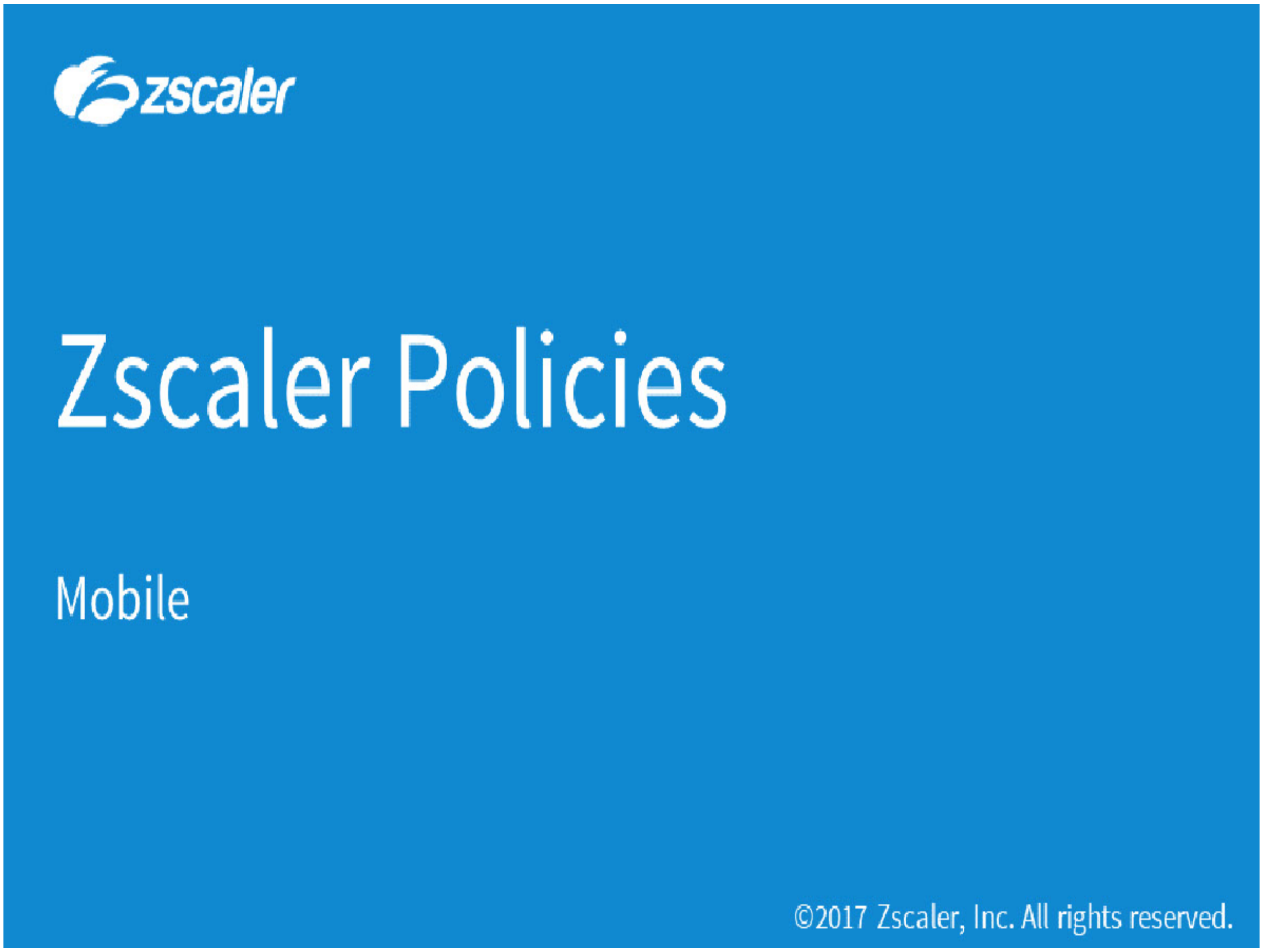
Slide 1 - Zscaler Policies



zscaler

Zscaler Policies

Mobile

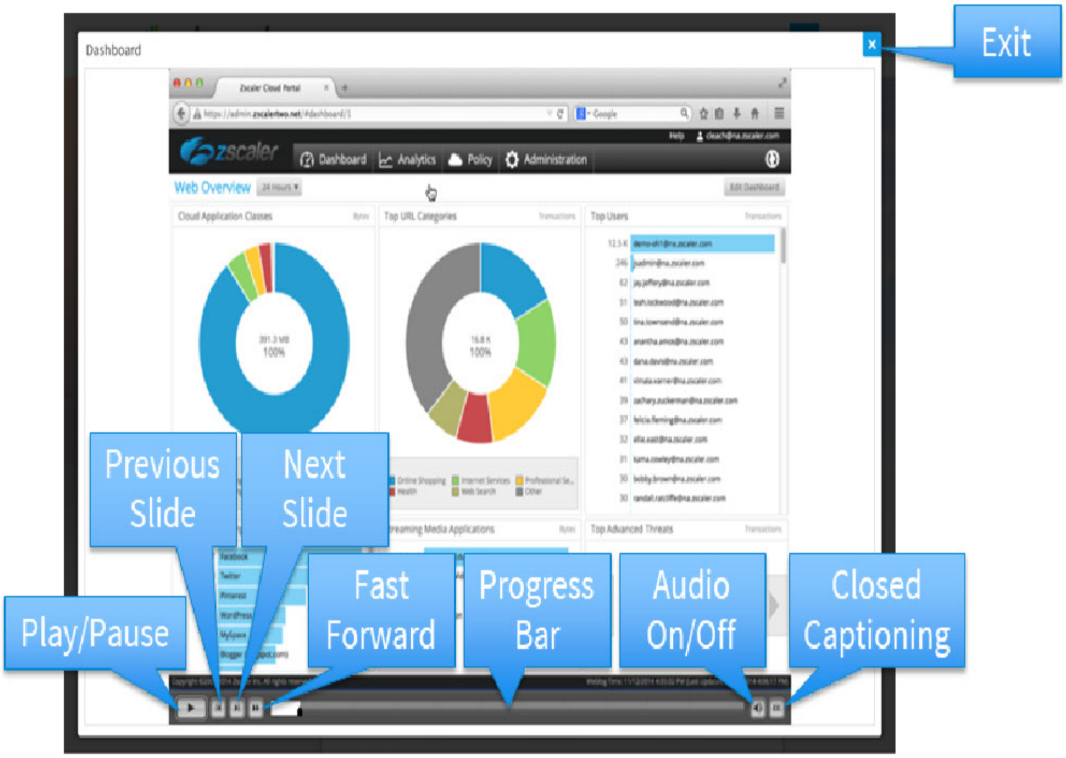
©2017 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to the Zscaler Mobile Policy Module.

Slide 2 - Navigating the eLearning Module

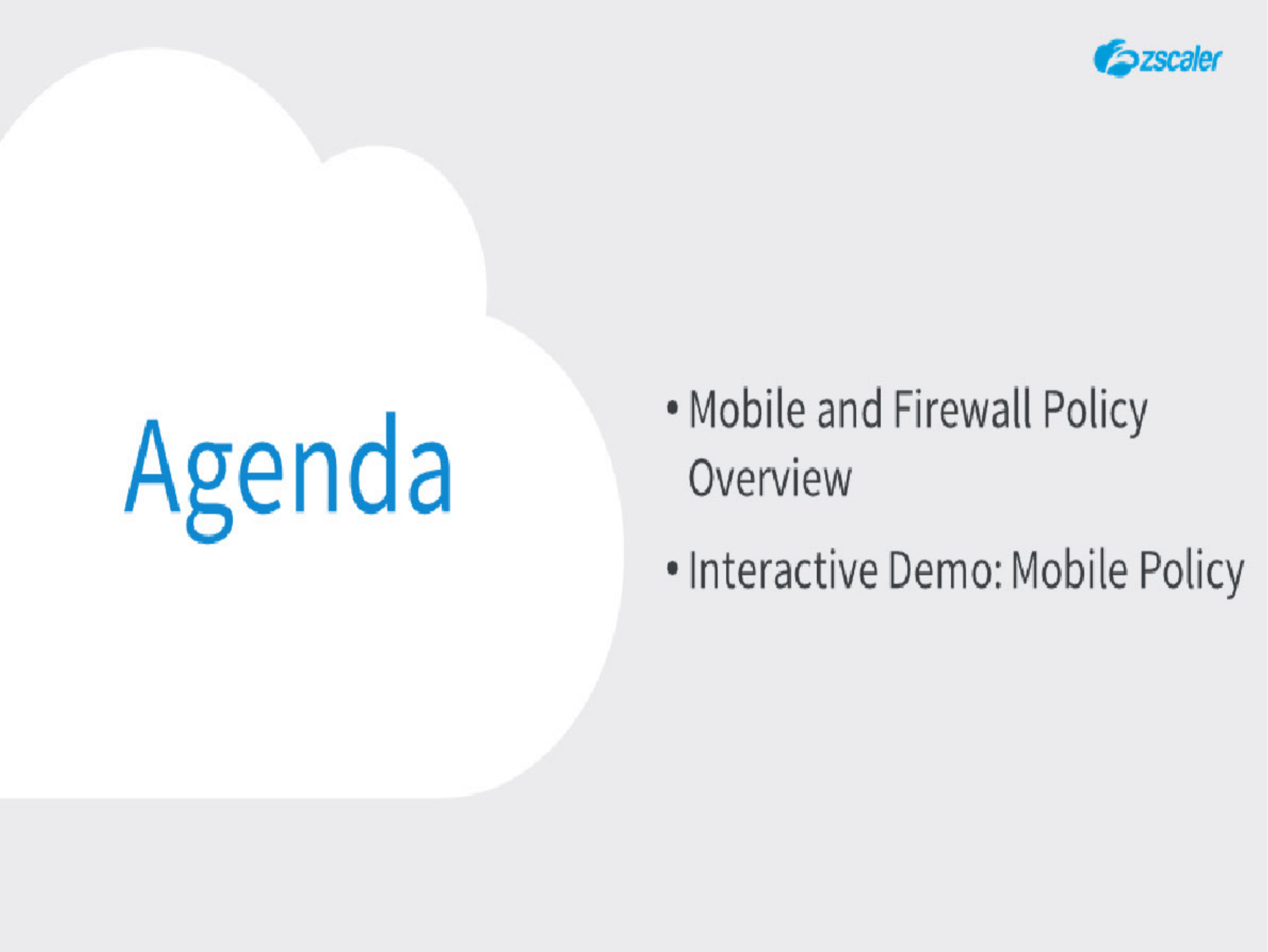
Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including play and pause, previous, next slide and fast forward. 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



zscaler

Agenda

- Mobile and Firewall Policy Overview
- Interactive Demo: Mobile Policy

Slide notes

In this module, we will provide an overview of the Mobile policies available.

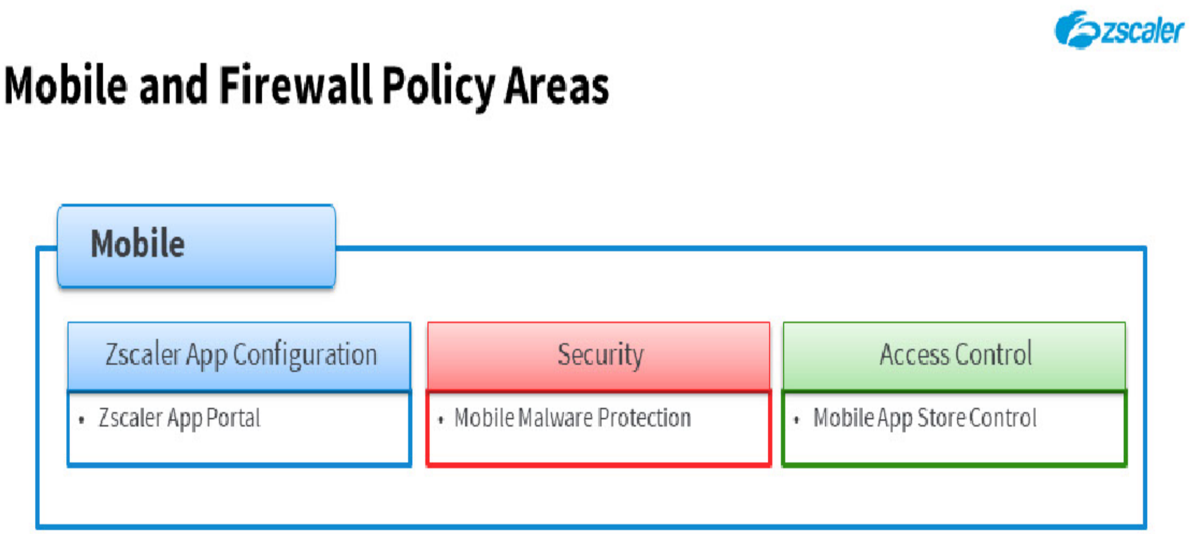
Slide 4 - Mobile and Firewall Policy Overview

Mobile Policy Overview

Slide notes

The first topic we will cover is to have a look at what Mobile policies are available.

Slide 5 - Mobile and Firewall Policy Areas



Mobile and Firewall Policy Areas

Mobile

Zscaler App Configuration
- Zscaler App Portal

Security
- Mobile Malware Protection

Access Control
- Mobile App Store Control

Slide notes

The Mobile policy area allows access to the **Zscaler App Portal**, and the configuration of **Security**, and **Access Control** policies for mobile users and devices.

Slide 6 - Interactive Demo: Mobile Policy

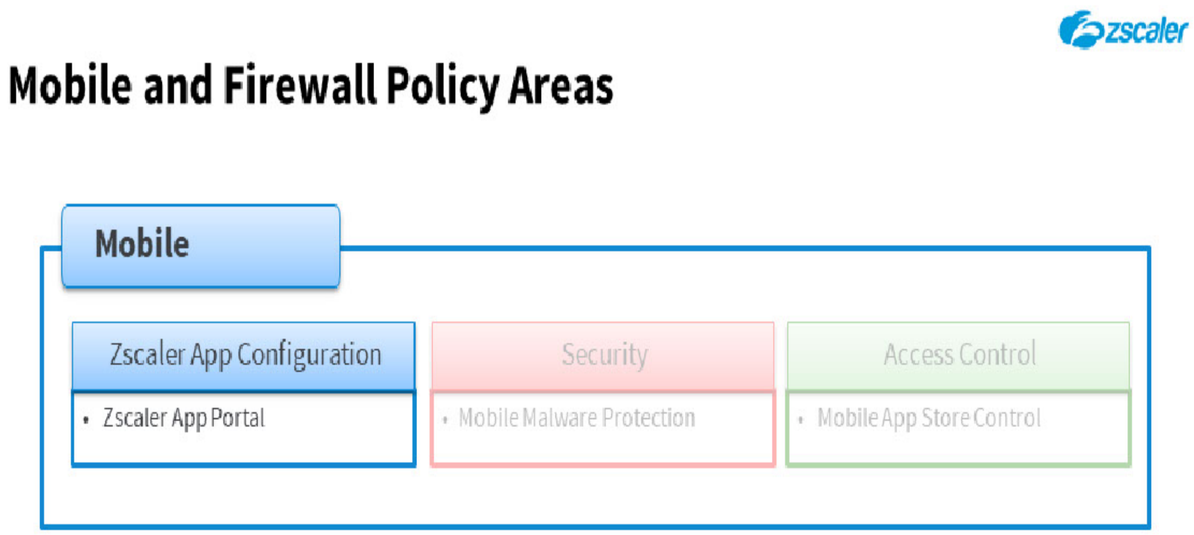
Interactive Demo: Mobile Policy

Slide notes

In the next section, we will have a detailed look at the Mobile Policies.

This section has been created as an interactive demo to give you a feel for the navigation of the Zscaler App Portal UI. 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 7 - Mobile and Firewall Policy Areas



Mobile and Firewall Policy Areas

Mobile

Zscaler App Configuration

- Zscaler App Portal

Security

- Mobile Malware Protection

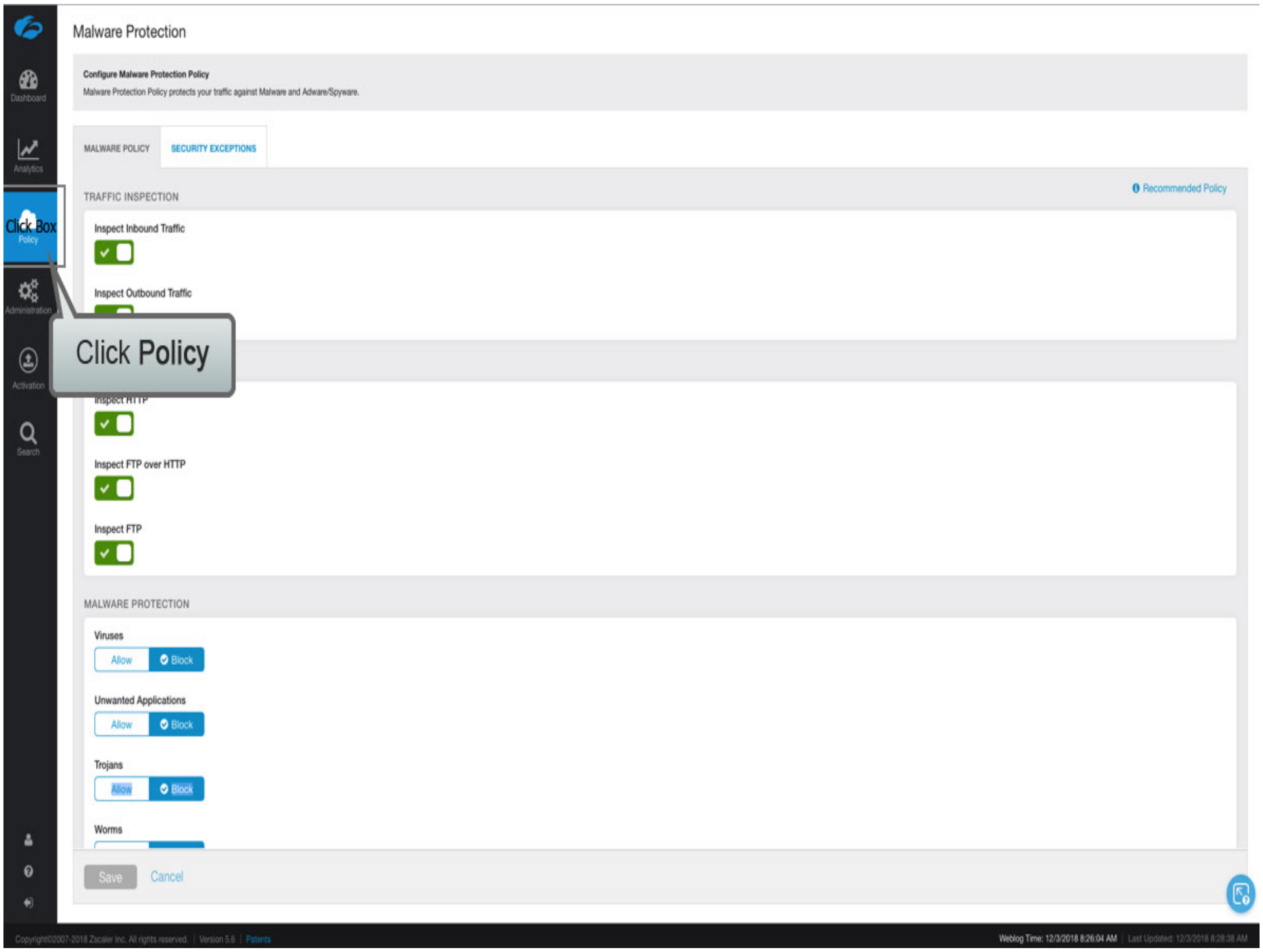
Access Control

- Mobile App Store Control

Slide notes

Firstly, we will look at the **Zscaler App Portal** option.

Slide 8 - Slide 8



Malware Protection

Configure Malware Protection Policy

Malware Protection Policy protects your traffic against Malware and Adware/Spyware.

TRAFFIC INSPECTION

Inspect Inbound Traffic ✓

Inspect Outbound Traffic

Inspect HTTP ✓

Inspect FTP over HTTP ✓

Inspect FTP ✓

MALWARE PROTECTION

Viruses: Allow [✓ Block]

Unwanted Applications: Allow [✓ Block]

Trojans: Allow [✓ Block]

Worms

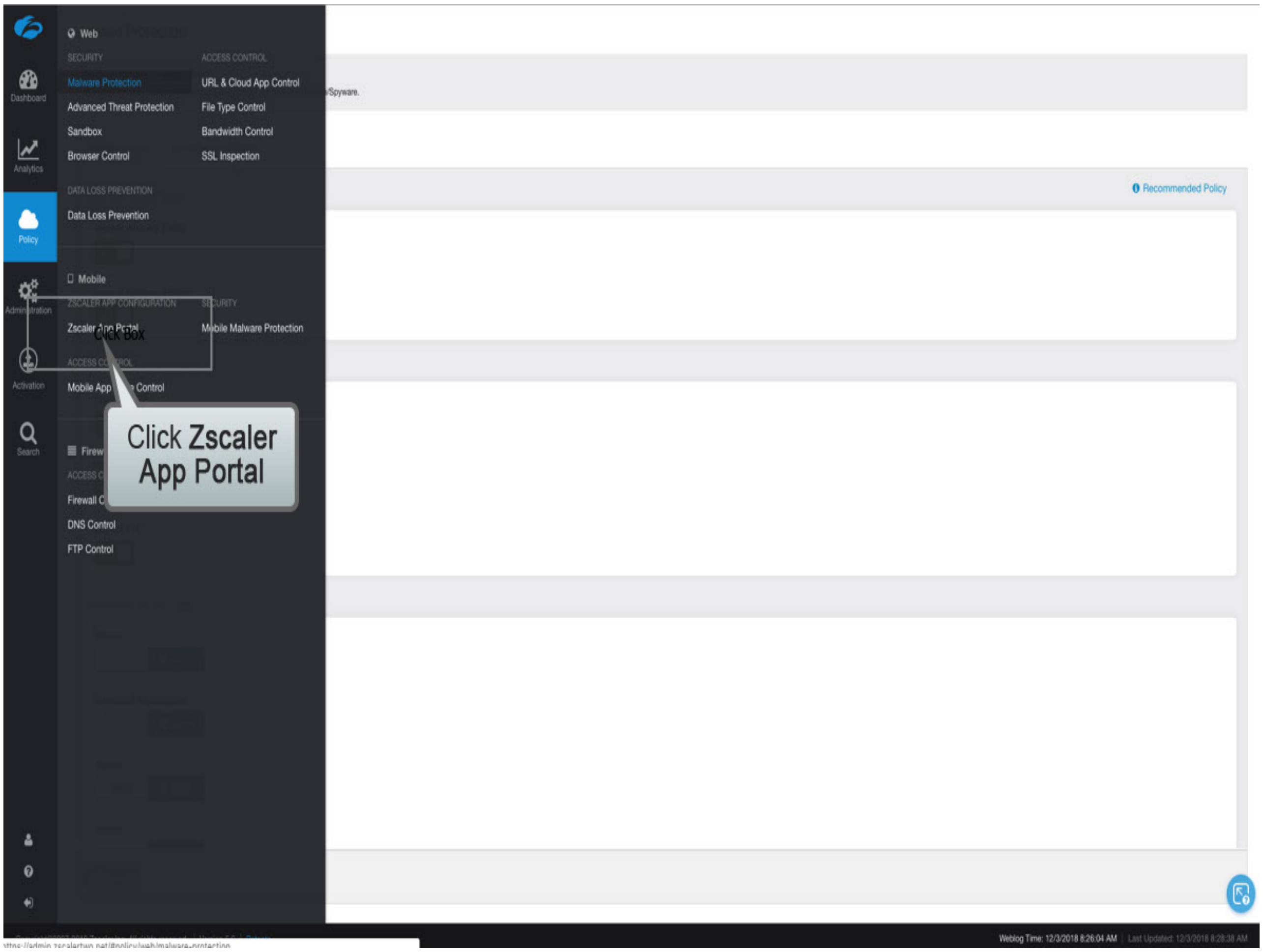
Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents

Weblog Time: 12/3/2018 8:26:04 AM | Last Updated: 12/3/2018 8:28:38 AM

Slide notes

Click on the **Policy** page to expand it.

Slide 9 - Slide 9



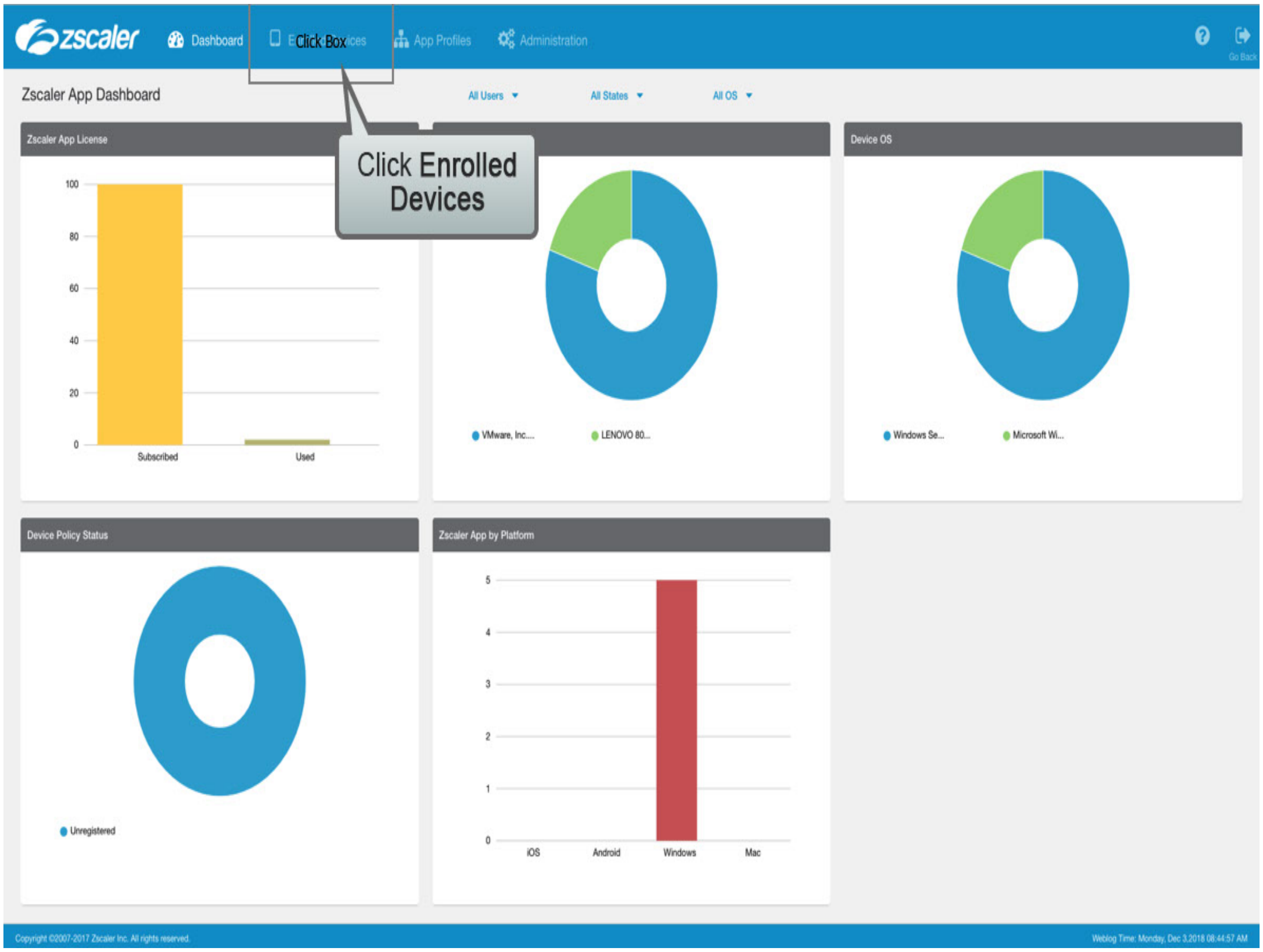
Click Box

Click Zscaler App Portal

Slide notes

To configure policy for the Zscaler App and eZAgent for mobile devices, click **Zscaler App Portal**.

Slide 10 - Slide 10



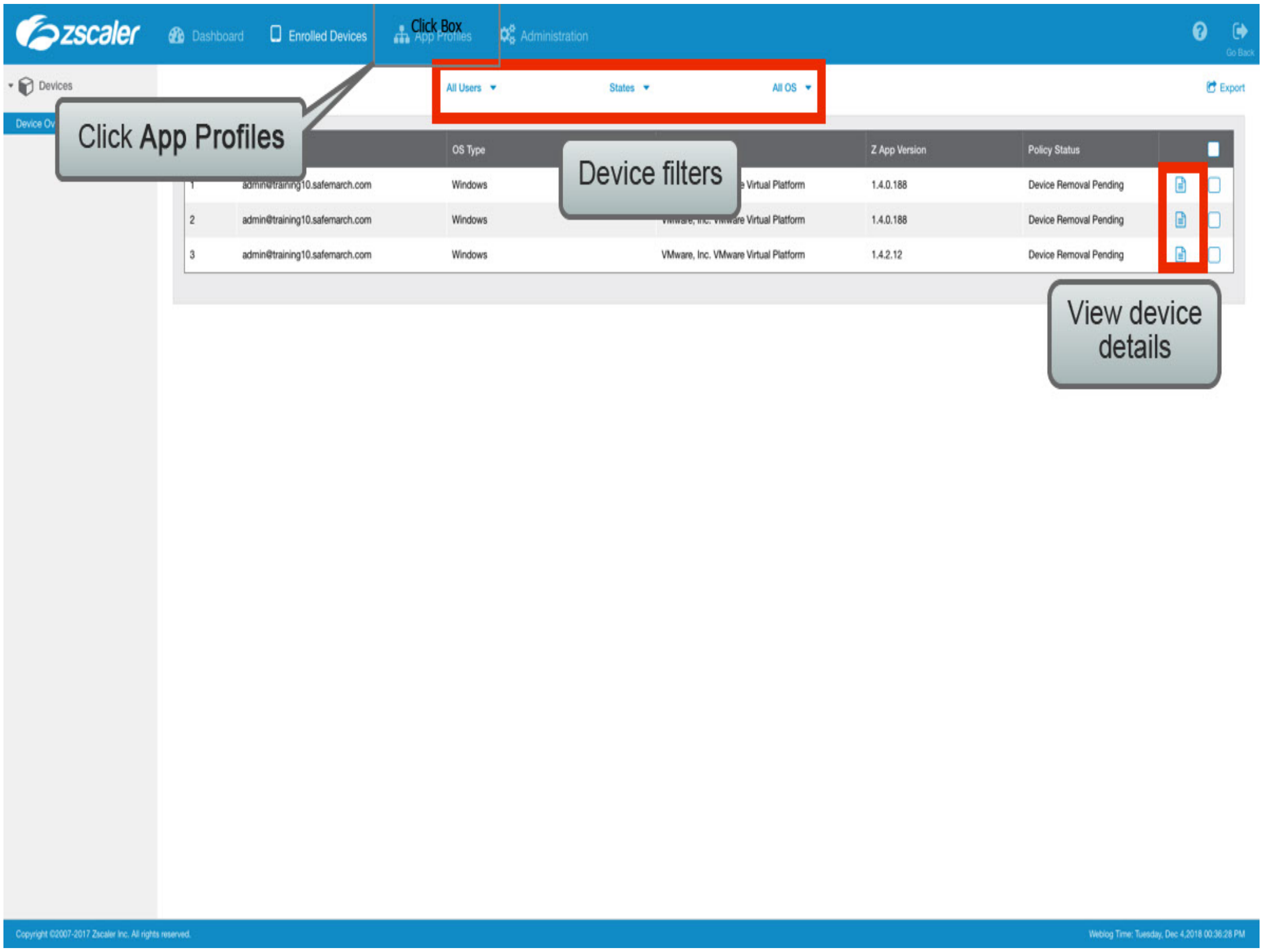
Click Box

Click Enrolled Devices

Slide notes

This will open the Mobile Portal, full screen, in the same Browser window. The **Dashboard** page will be shown. To see a list of the enrolled devices, click **Enrolled Devices**.

Slide 11 - Slide 11



Click App Profiles

Device filters

View device details

		OS Type		Z App Version	Policy Status	□
1	admin@training10.safemarch.com	Windows	e Virtual Platform	1.4.0.188	Device Removal Pending	□
2	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.0.188	Device Removal Pending	□
3	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.2.12	Device Removal Pending	□

Copyright ©2007-2017 Zscaler Inc. All rights reserved.

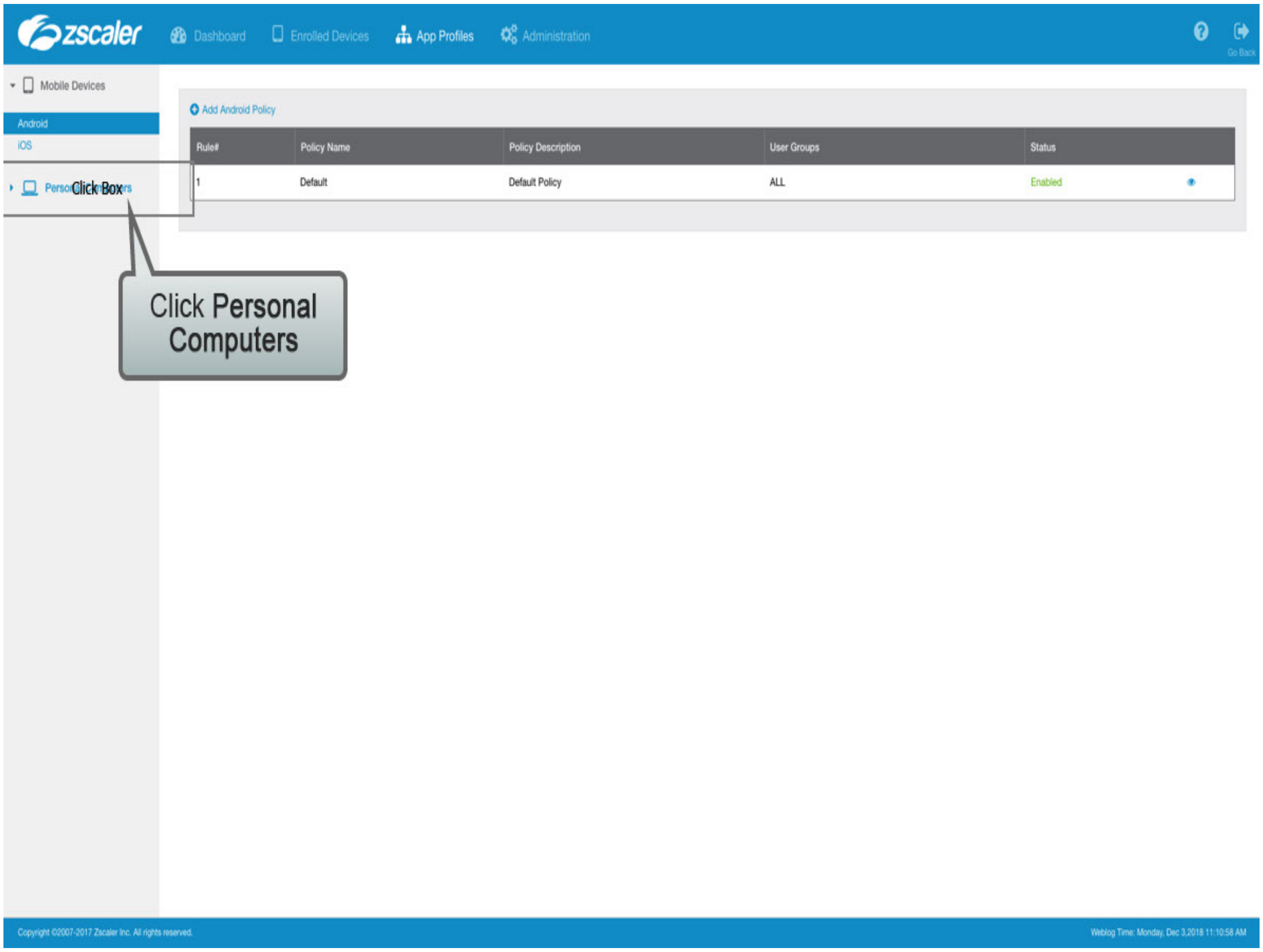
Weblog Time: Tuesday, Dec 4 2018 00:36:28 PM

Slide notes

A list of all the enrolled devices is available, and details for each may be viewed. You may filter the list by **User ID**, device **State**, and device **OS**.

To access and manage App Profiles, click **App Profiles**.

Slide 12 - Slide 12



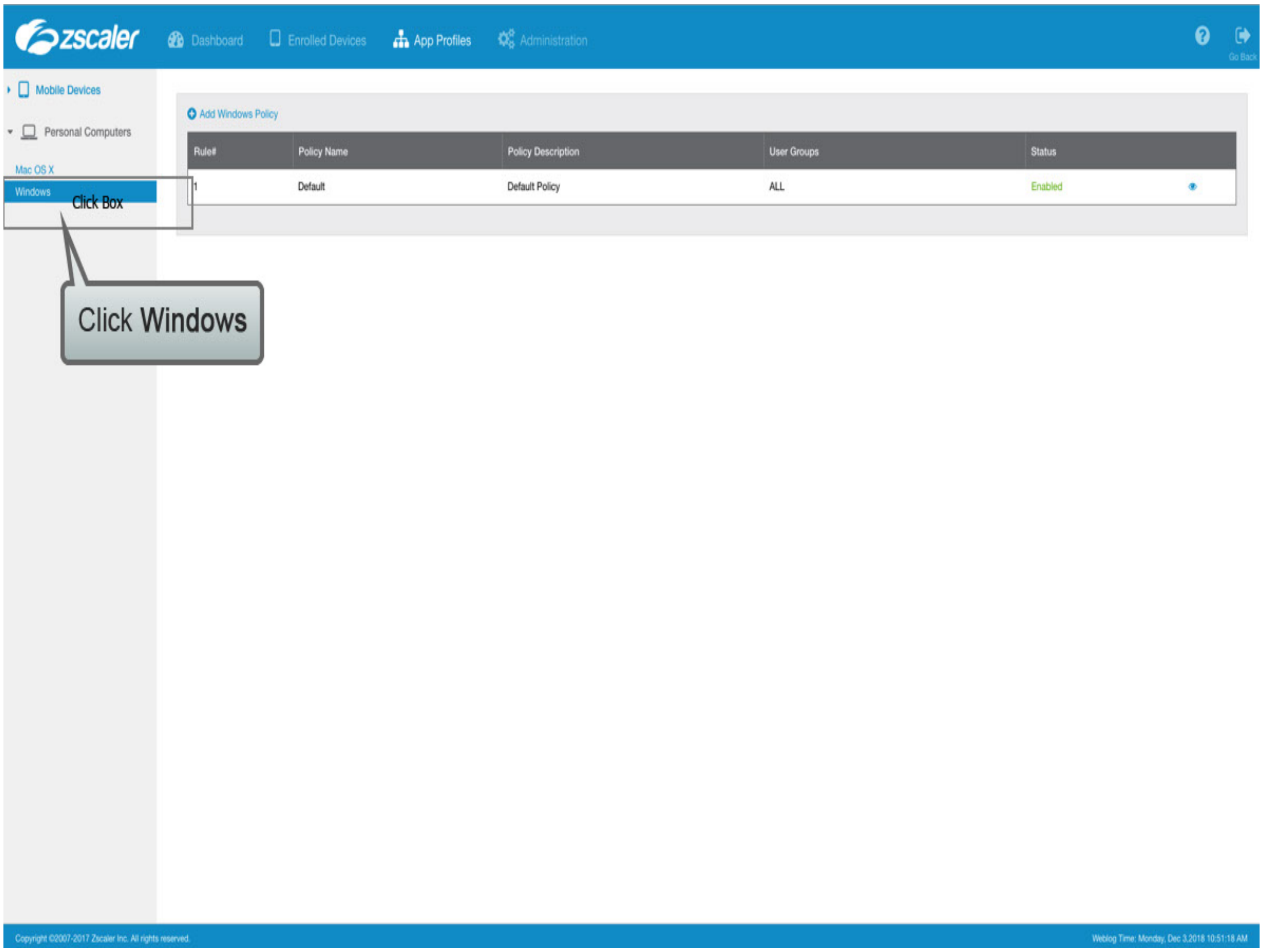
Rule#	Policy Name	Policy Description	User Groups	Status
1	Default	Default Policy	ALL	Enabled

Click Personal Computers

Slide notes

App Profiles allow the setting of policy and the configuration of the Zscaler App on PCs (Windows and Mac) and on Mobile devices (iOS and Android). To view and manage profiles for PCs, click **Personal Computers**.

Slide 13 - Slide 13



Rule#	Policy Name	Policy Description	User Groups	Status
1	Default	Default Policy	ALL	Enabled

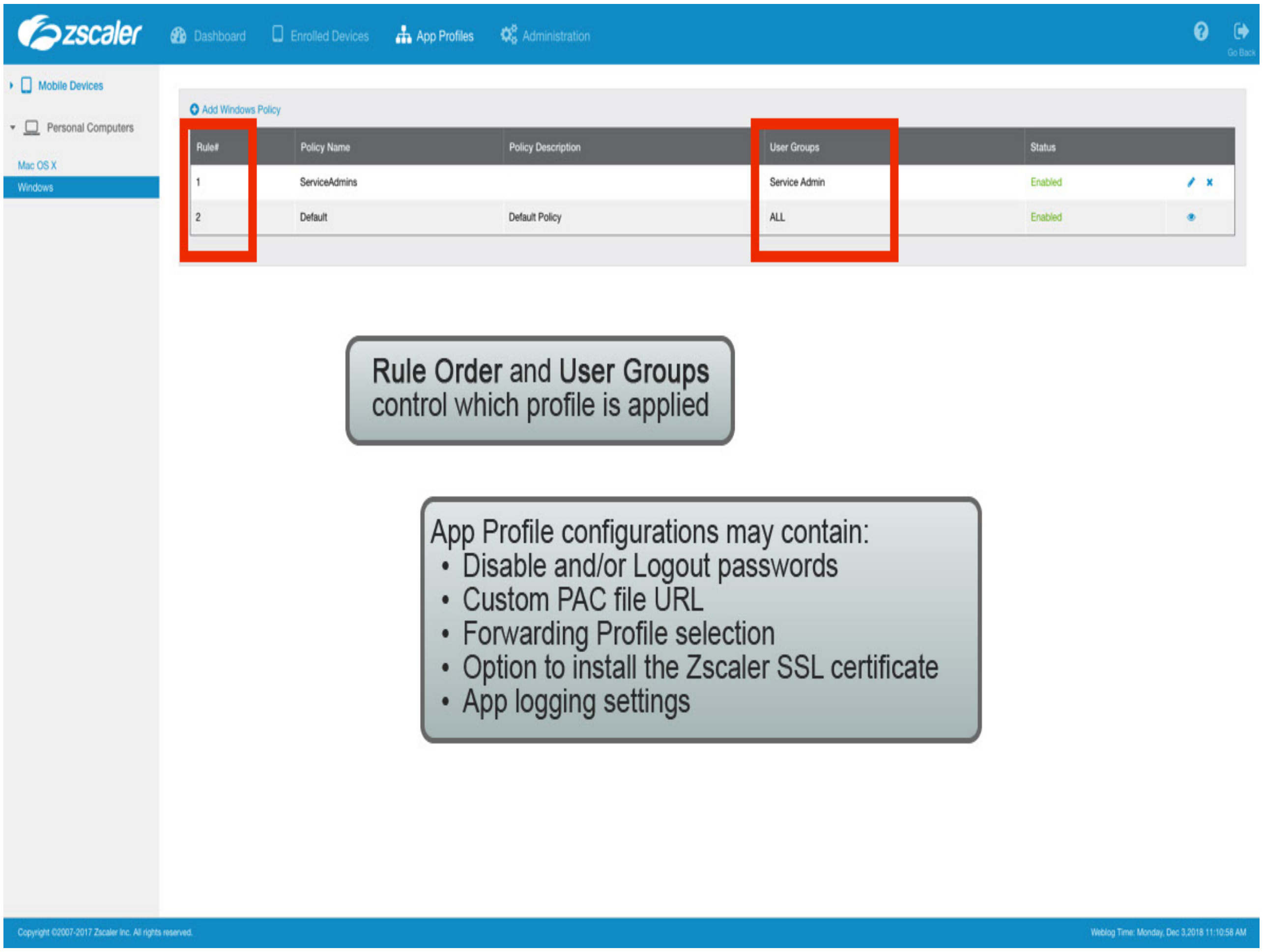
Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Monday, Dec 3,2018 10:51:18 AM

Slide notes

Both Mac OSX and Windows PCs are supported, click **Windows** to view and manage profiles for Windows PCs.

Slide 14 - Slide 14



Rule#	Policy Name	Policy Description	User Groups	Status
1	ServiceAdmins		Service Admin	Enabled
2	Default	Default Policy	ALL	Enabled

Rule Order and User Groups control which profile is applied

App Profile configurations may contain:
- Disable and/or Logout passwords
- Custom PAC file URL
- Forwarding Profile selection
- Option to install the Zscaler SSL certificate
- App logging settings

Copyright ©2007-2017 Zscaler Inc. All rights reserved.

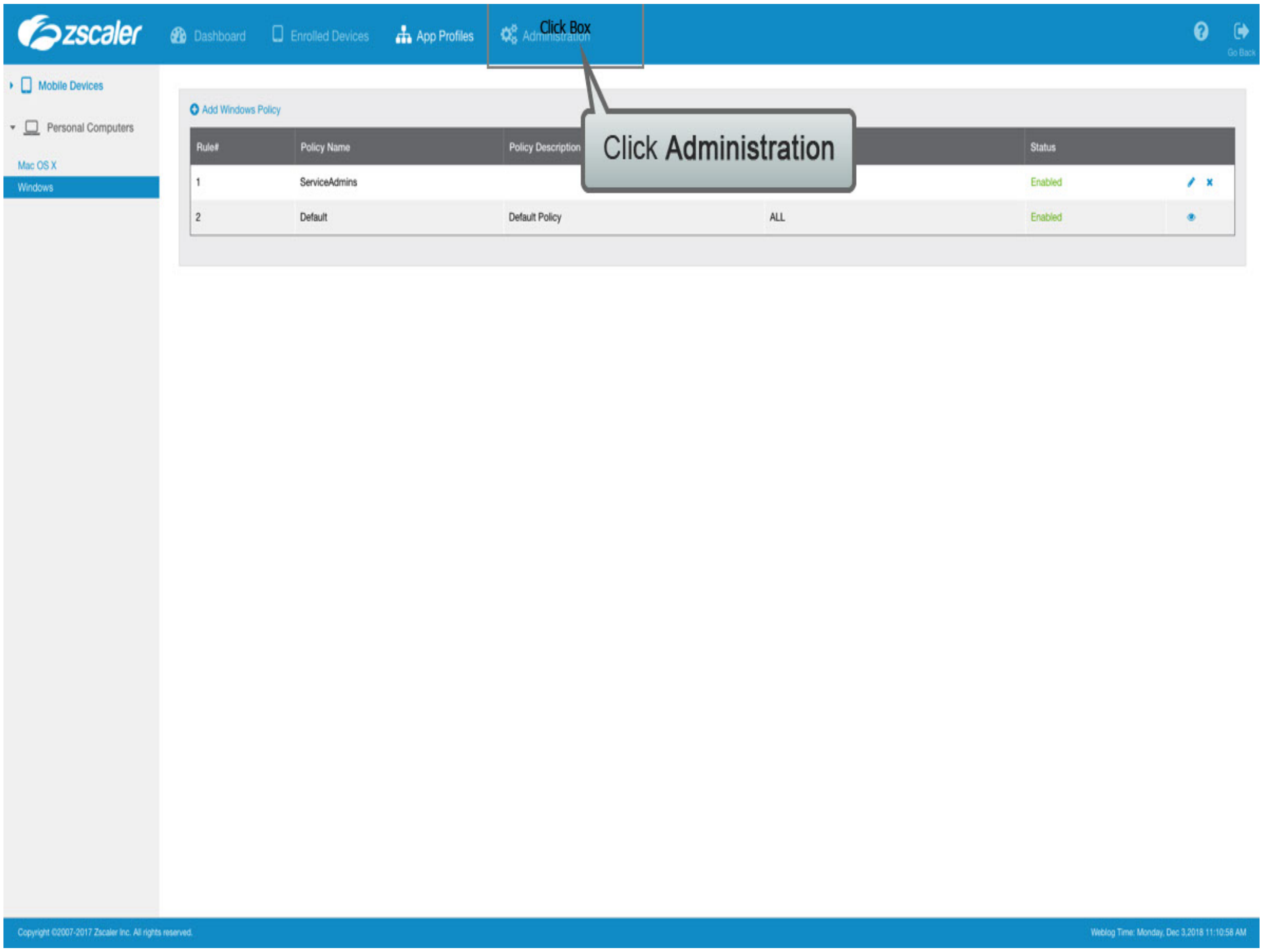
Weblog Time: Monday, Dec 3,2018 11:10:58 AM

Slide notes

An App Profile controls the following key App settings and behaviors: whether users must enter an admin-provided password in order to log out of, disable, or uninstall the app; The URL for a custom PAC file if one is required; how the App detects trusted networks and how it manages traffic forwarding when users are on, or off a trusted network; whether the App can install the Zscaler SSL certificate on user’s devices to allow SSL inspection of traffic forwarded by the app; also how the App generates logs, and the maximum size of its log files.

You can select the order of precedence among the profiles, and specify to whom each profile applies (by **Group**). When a user enrolls the App with Zscaler, the App takes into account this order of precedence and the identity of the user to download the App Profile containing the appropriate policy.

Slide 15 - Slide 15



Click Box

Click Administration

Rule#	Policy Name	Policy Description		Status	
1	ServiceAdmins			Enabled	
2	Default	Default Policy	ALL	Enabled	

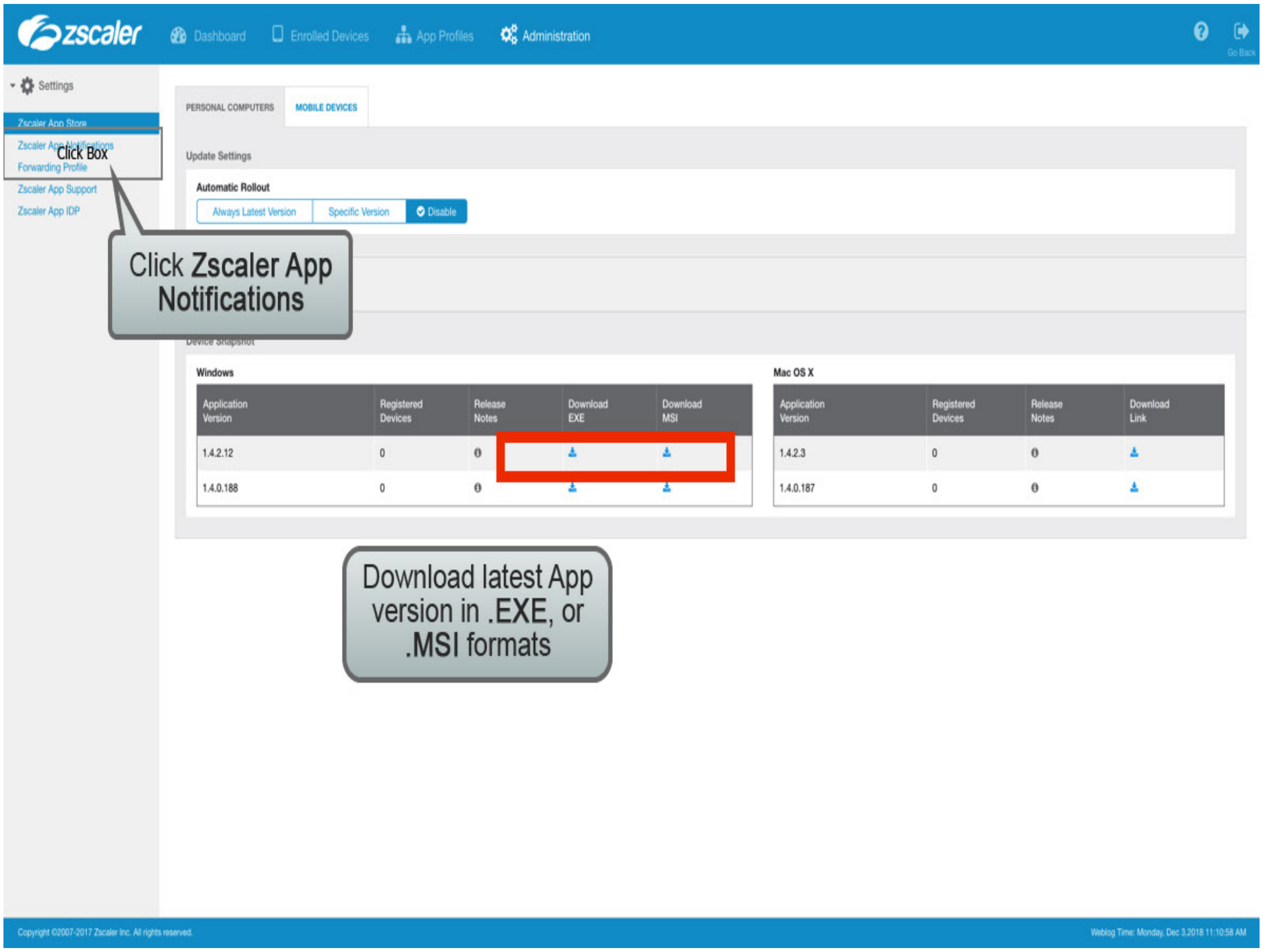
Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Monday, Dec 3,2018 11:10:58 AM

Slide notes

To manage other configuration settings, and policy, click **Administration**.

Slide 16 - Slide 16



Update Settings

Automatic Rollout: Always Latest Version | Specific Version | ● Disable

Click Zscaler App Notifications

Device Snapshot

Windows

Application Version	Registered Devices	Release Notes	Download EXE	Download MSI
1.4.2.12	0	ⓘ	⬇	⬇
1.4.0.188	0	ⓘ	⬇	⬇

Mac OS X

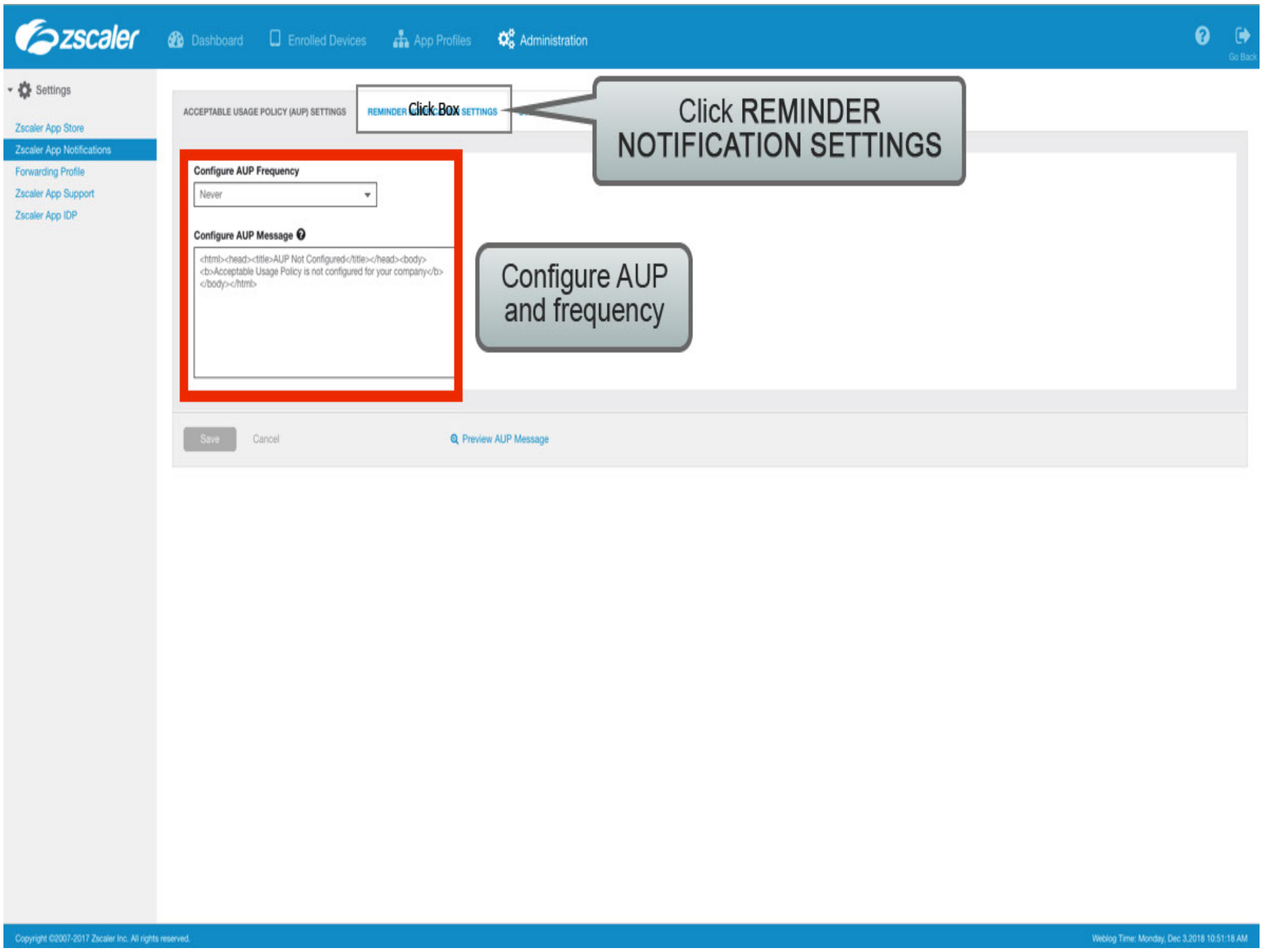
Application Version	Registered Devices	Release Notes	Download Link
1.4.2.3	0	ⓘ	⬇
1.4.0.187	0	ⓘ	⬇

Download latest App version in .EXE, or .MSI formats

Slide notes

On the **Zscaler App Store** page, you can download the latest version of the Zscaler App for your platform. For Windows PCs, the installer may be downloaded either as a .EXE, or as a .MSI file. You can also specify whether the App should be auto-updated. To configure end user notifications, click **Zscaler App Notifications**.

Slide 17 - Slide 17



Configure AUP Frequency: Never

Configure AUP Message:

```
<html><head><title>AUP Not Configured</title></head><body>
<b>Acceptable Usage Policy is not configured for your company</b>
</body></html>
```

Click REMINDER NOTIFICATION SETTINGS

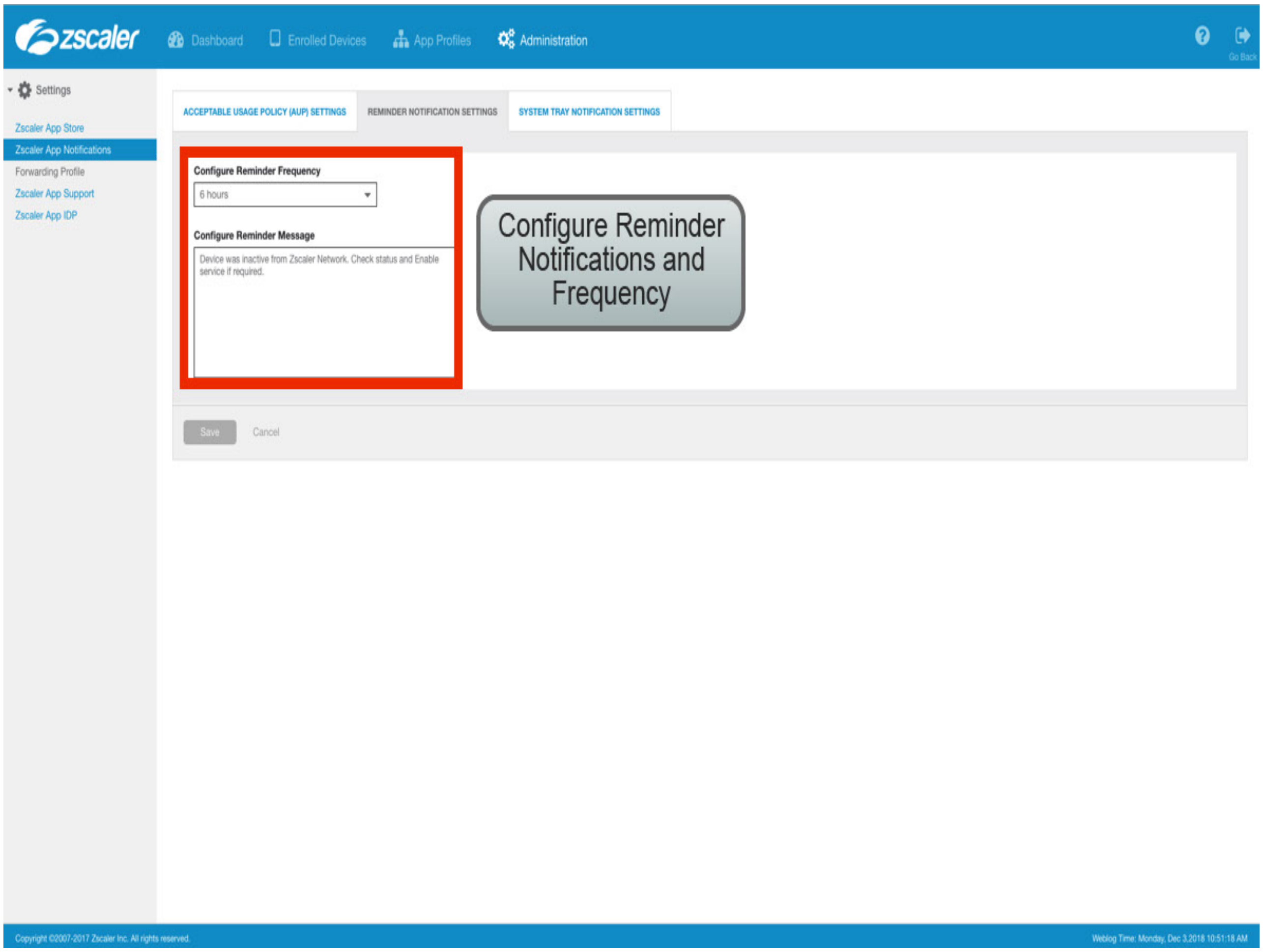
Configure AUP and frequency

Slide notes

You have the option to add an Acceptable Use Policy (AUP) that users must accept before they can use the App, and you can specify how often this should be displayed.

To configure reminder notifications, click the **REMINDER NOTIFICATION SETTINGS** tab.

Slide 18 - Slide 18


zscaler
Dashboard
Enrolled Devices
App Profiles
Administration
Go Back
Settings
Zscaler App Store
Zscaler App Notifications
Forwarding Profile
Zscaler App Support
Zscaler App IDP
ACCEPTABLE USAGE POLICY (AUP) SETTINGS
REMINDER NOTIFICATION SETTINGS
SYSTEM TRAY NOTIFICATION SETTINGS
Save
Cancel
Copyright ©2007-2017 Zscaler Inc. All rights reserved.
Weblog Time: Monday, Dec 3,2018 10:51:18 AM

Configure Reminder Frequency: 6 hours

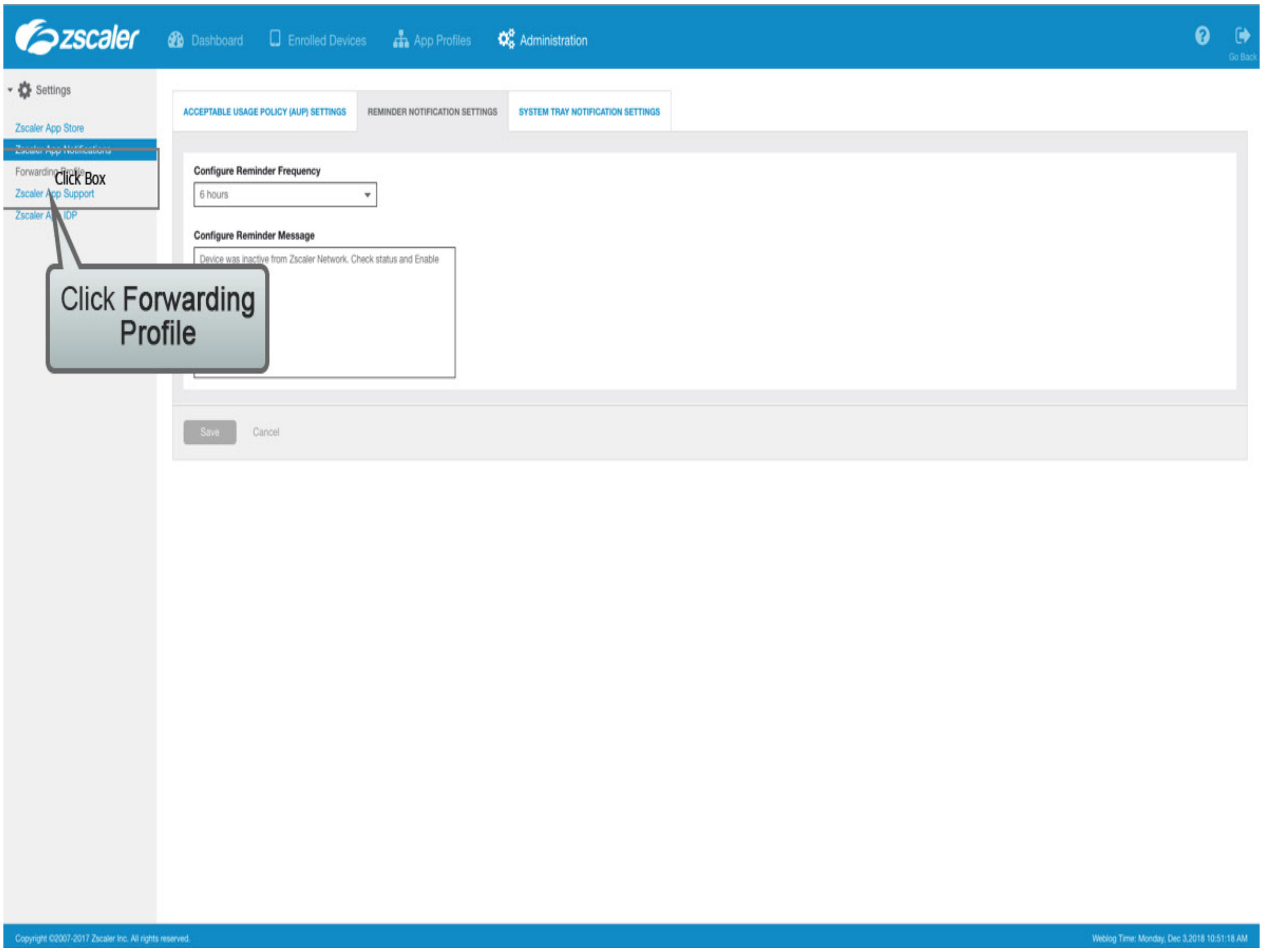
Configure Reminder Message: Device was inactive from Zscaler Network. Check status and Enable service if required.

Configure Reminder Notifications and Frequency

Slide notes

On the **REMINDER NOTIFICATION SETTINGS** tab, you can configure the security reminder displayed if the App is inactive, and the frequency to display it.

Slide 19 - Slide 19


zscaler
Dashboard
Enrolled Devices
App Profiles
Administration
Go Back
Settings
Zscaler App Store
Zscaler App Notifications
Forwarding Profile
Zscaler App Support
Zscaler App IDP
ACCEPTABLE USAGE POLICY (AUP) SETTINGS
REMINDER NOTIFICATION SETTINGS
SYSTEM TRAY NOTIFICATION SETTINGS
Save
Cancel
Click Box
Copyright ©2007-2017 Zscaler Inc. All rights reserved.
Weblog Time: Monday, Dec 3,2018 10:51:18 AM

Configure Reminder Frequency: 6 hours

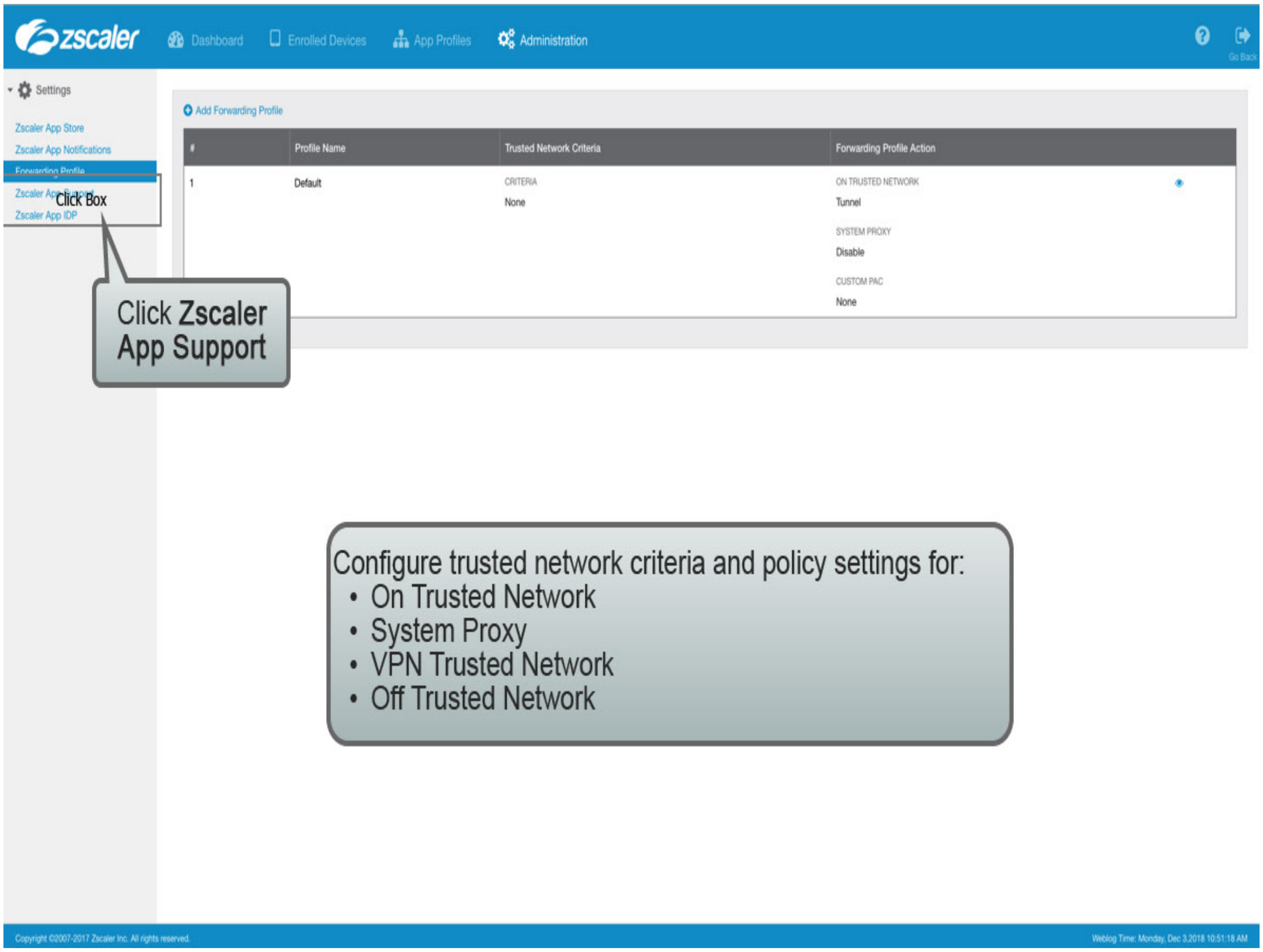
Configure Reminder Message: Device was inactive from Zscaler Network. Check status and Enable

Click Forwarding Profile

Slide notes

To manage how the App behaves when on a trusted network, click **Forwarding Profile**.

Slide 20 - Slide 20



#	Profile Name	Trusted Network Criteria	Forwarding Profile Action
1	Default	CRITERIA None	ON TRUSTED NETWORK Tunnel SYSTEM PROXY Disable CUSTOM PAC None

Click Zscaler App Support

Configure trusted network criteria and policy settings for:

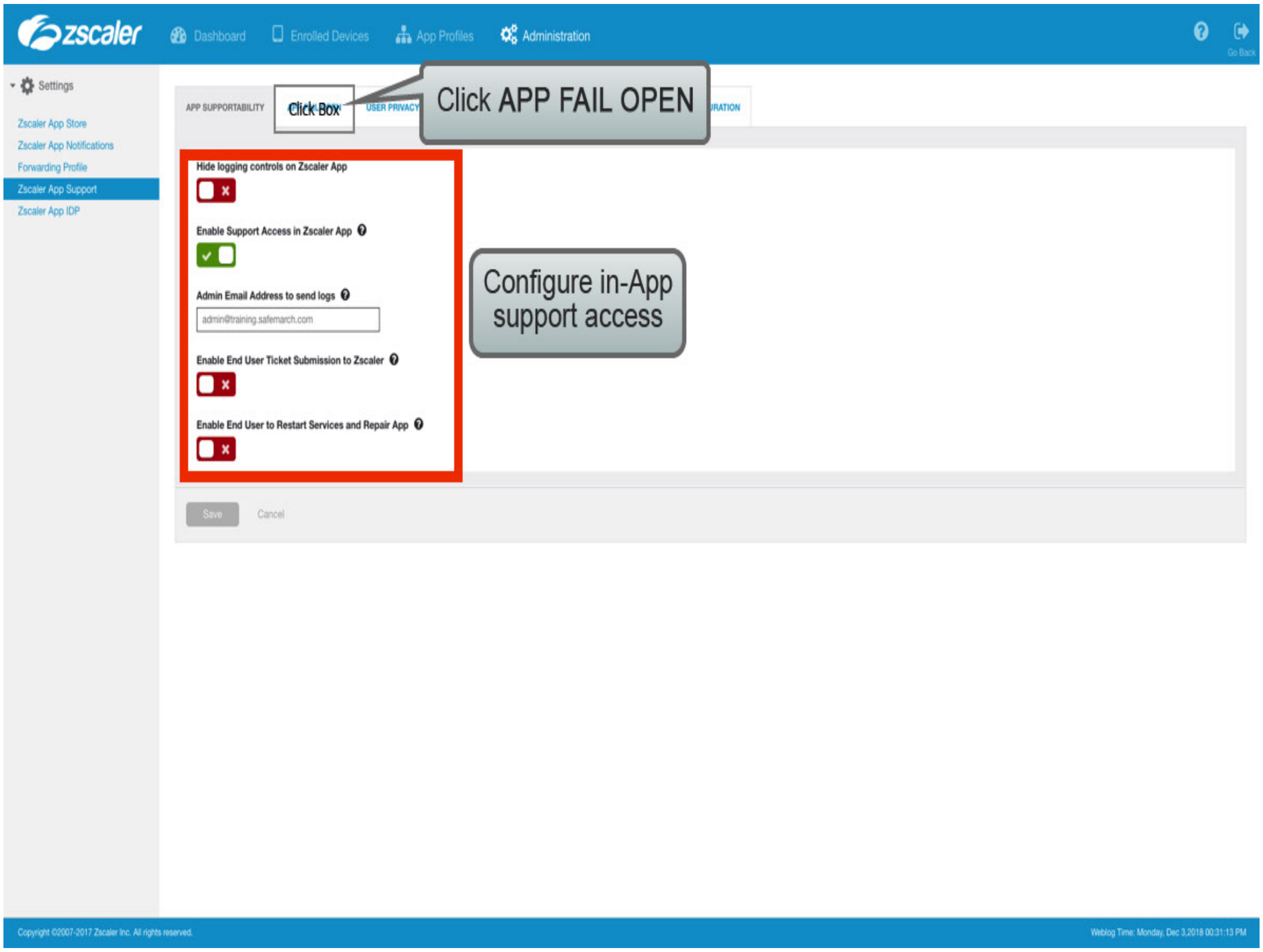
- On Trusted Network
- System Proxy
- VPN Trusted Network
- Off Trusted Network

Slide notes

When a user connects to a network, the Zscaler App can check the network to identify if it is one that you have designated as a trusted network (for example, your corporate network) and if so, may be configured to disable the Web security service. The app accomplishes this through the Forwarding Profiles, which are referred to from the App Profiles we looked at earlier.

To configure in-App access to the Helpdesk, click **Zscaler App Support**.

Slide 21 - Slide 21



Click APP FAIL OPEN

Hide logging controls on Zscaler App ☒

Enable Support Access in Zscaler App ☑

Admin Email Address to send logs: admin@training.safemarch.com

Enable End User Ticket Submission to Zscaler ☒

Enable End User to Restart Services and Repair App ☒

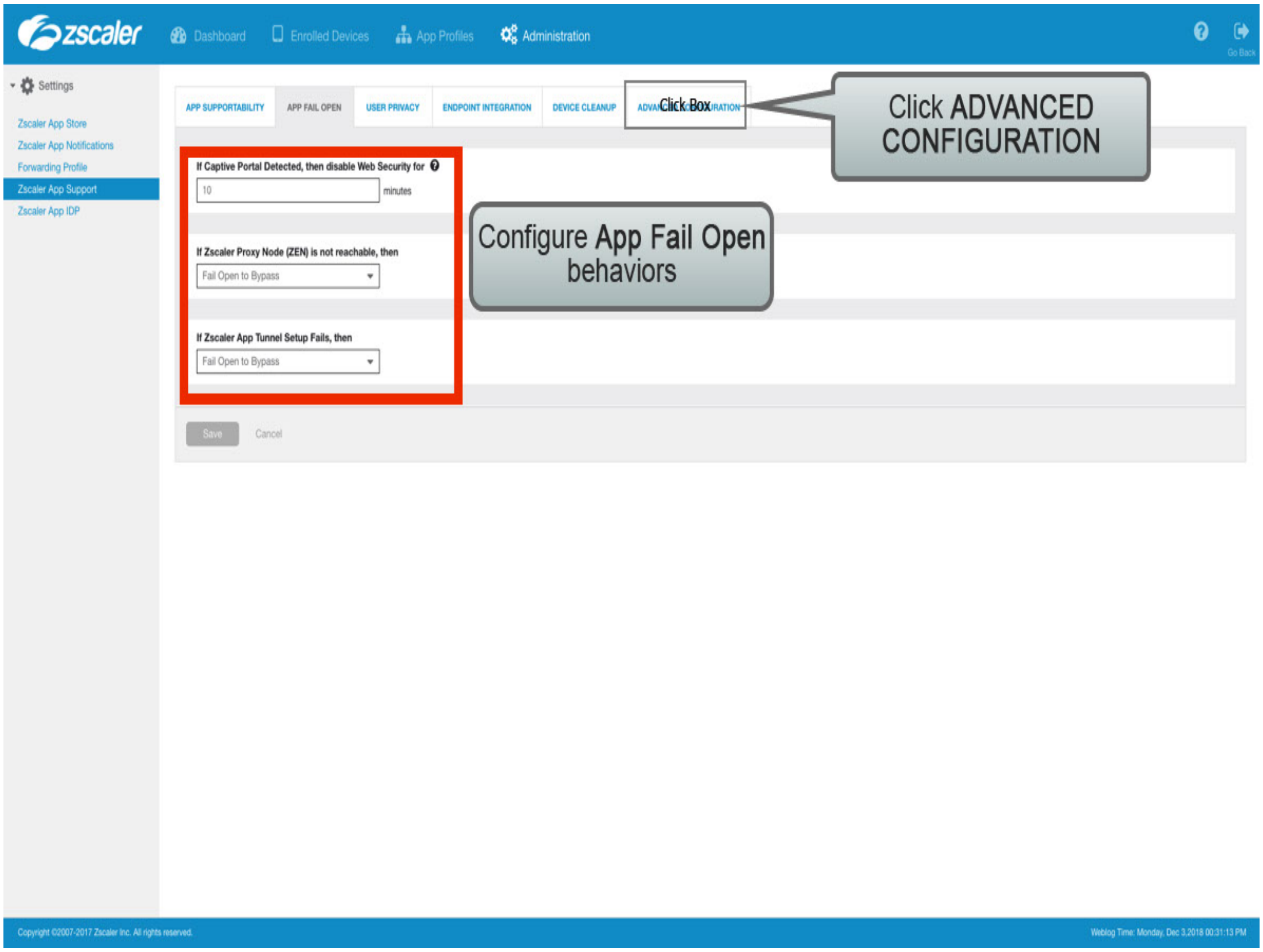
Configure in-App support access

Slide notes

Here you have the option to disable logging controls within the App, and you can decide whether to enable the raising of a support issue from within the App. You can specify the Helpdesk email address to send them to, and optionally allow cases to be raised with Zscaler directly.

To set Zscaler App fail open behavior, click on the **APP FAIL OPEN** tab.

Slide 22 - Slide 22



Click ADVANCED CONFIGURATION

Configure App Fail Open behaviors

If Captive Portal Detected, then disable Web Security for: 10 minutes

If Zscaler Proxy Node (ZEN) is not reachable, then: Fail Open to Bypass

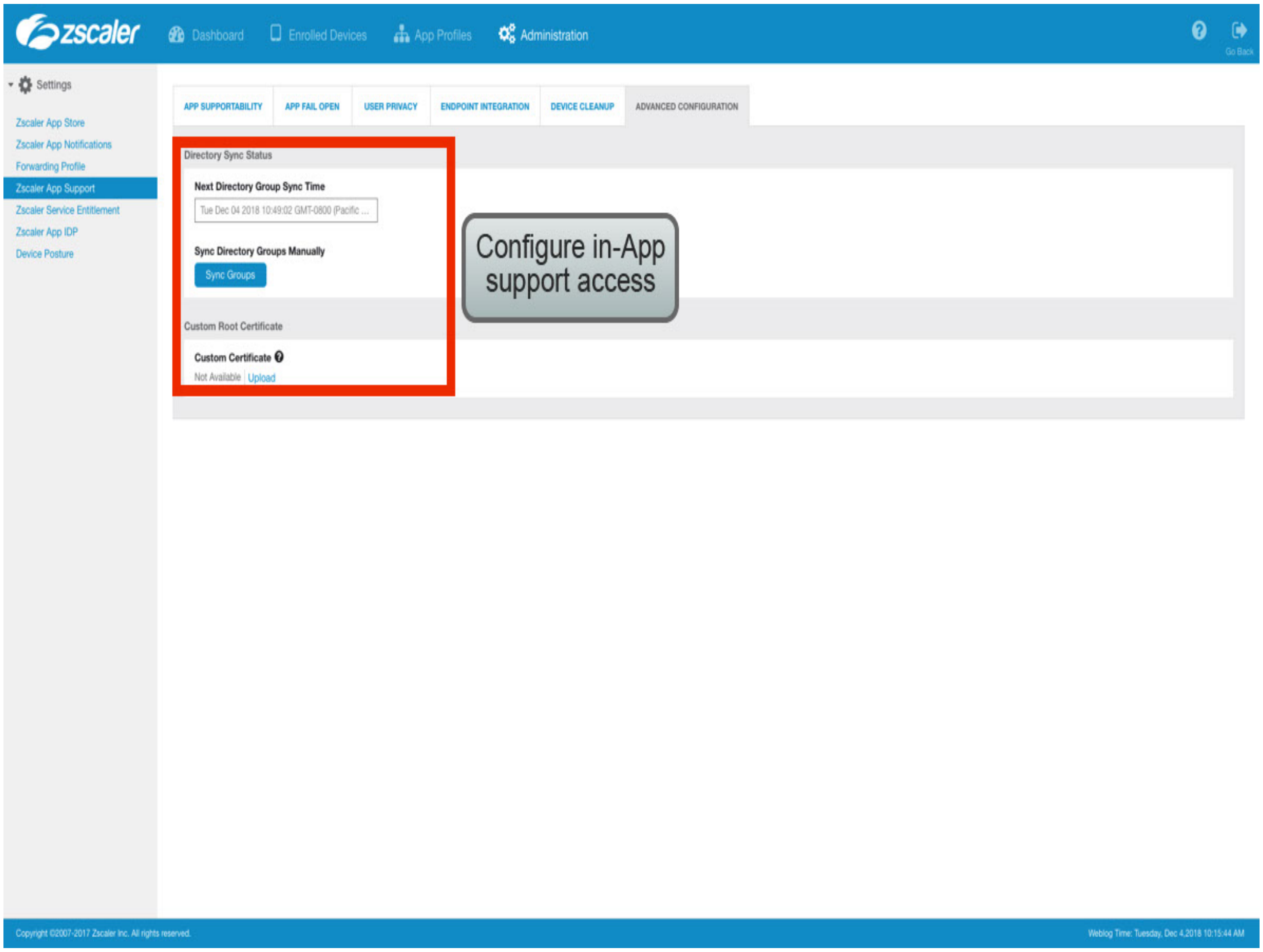
If Zscaler App Tunnel Setup Fails, then: Fail Open to Bypass

Slide notes

On the **APP FAIL OPEN** tab, you can specify what the App should do when it detects a Captive Portal, when it is unable to reach a ZEN, or when App Tunnel setup fails.

To set advanced settings, click on the **ADVANCED CONFIGURATION** tab.

Slide 23 - Slide 23



Directory Sync Status

Next Directory Group Sync Time: Tue Dec 04 2018 10:49:02 GMT-0800 (Pacific ...

Sync Directory Groups Manually

Custom Root Certificate

Custom Certificate: Not Available

Configure in-App support access

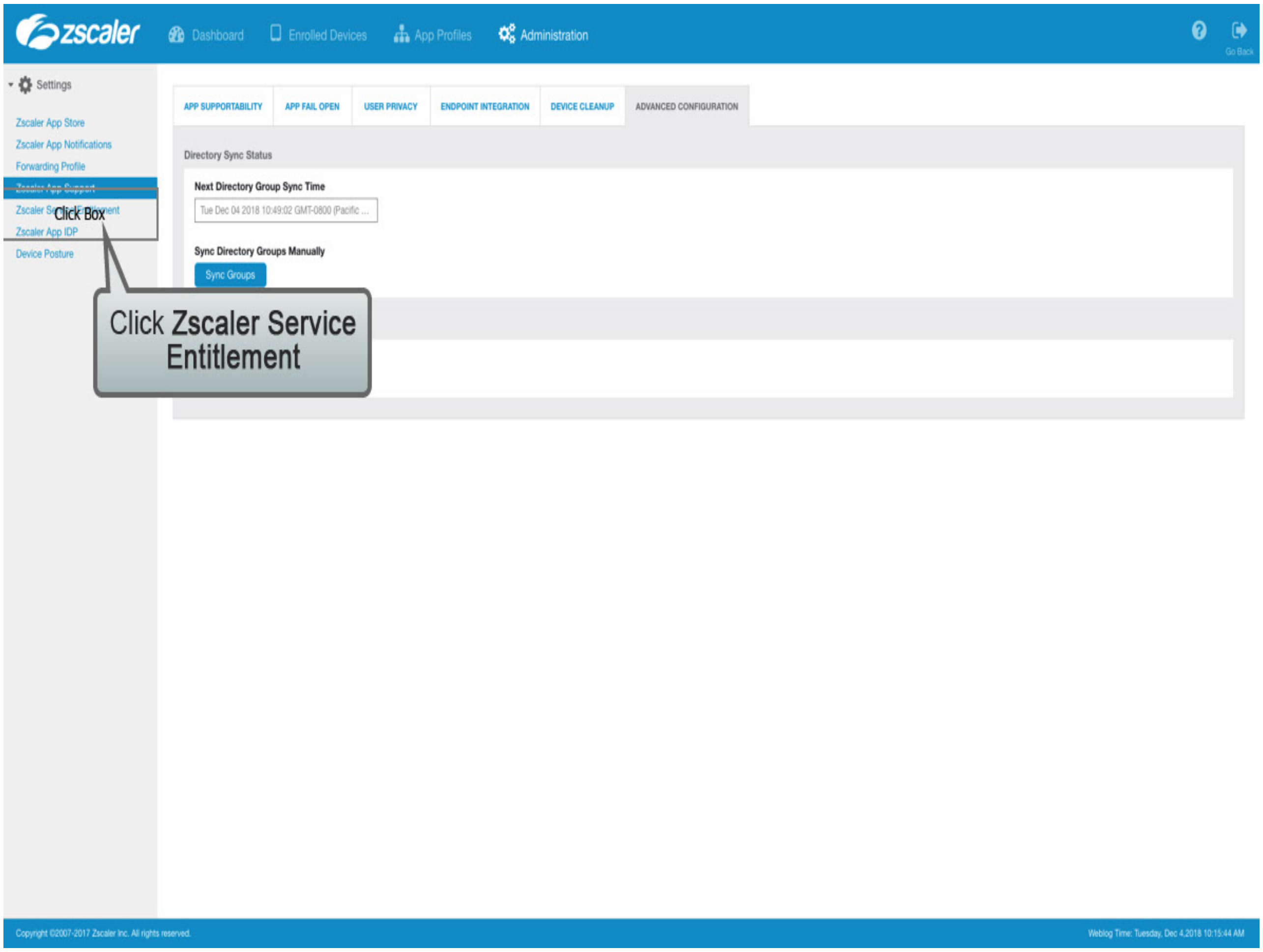
Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Tuesday, Dec 4,2018 10:15:44 AM

Slide notes

On the **ADVANCED CONFIGURATION** tab, you can configure some more advanced settings. **Directory Sync** settings are available, plus the ability to load an **Intermediate Root Certificate** to the Zscaler App host devices, to allow them to trust connections to servers with certificates from that CA.

Slide 24 - Slide 24



Directory Sync Status

Next Directory Group Sync Time: Tue Dec 04 2018 10:49:02 GMT-0800 (Pacific ...

Sync Directory Groups Manually

Click Zscaler Service Entitlement

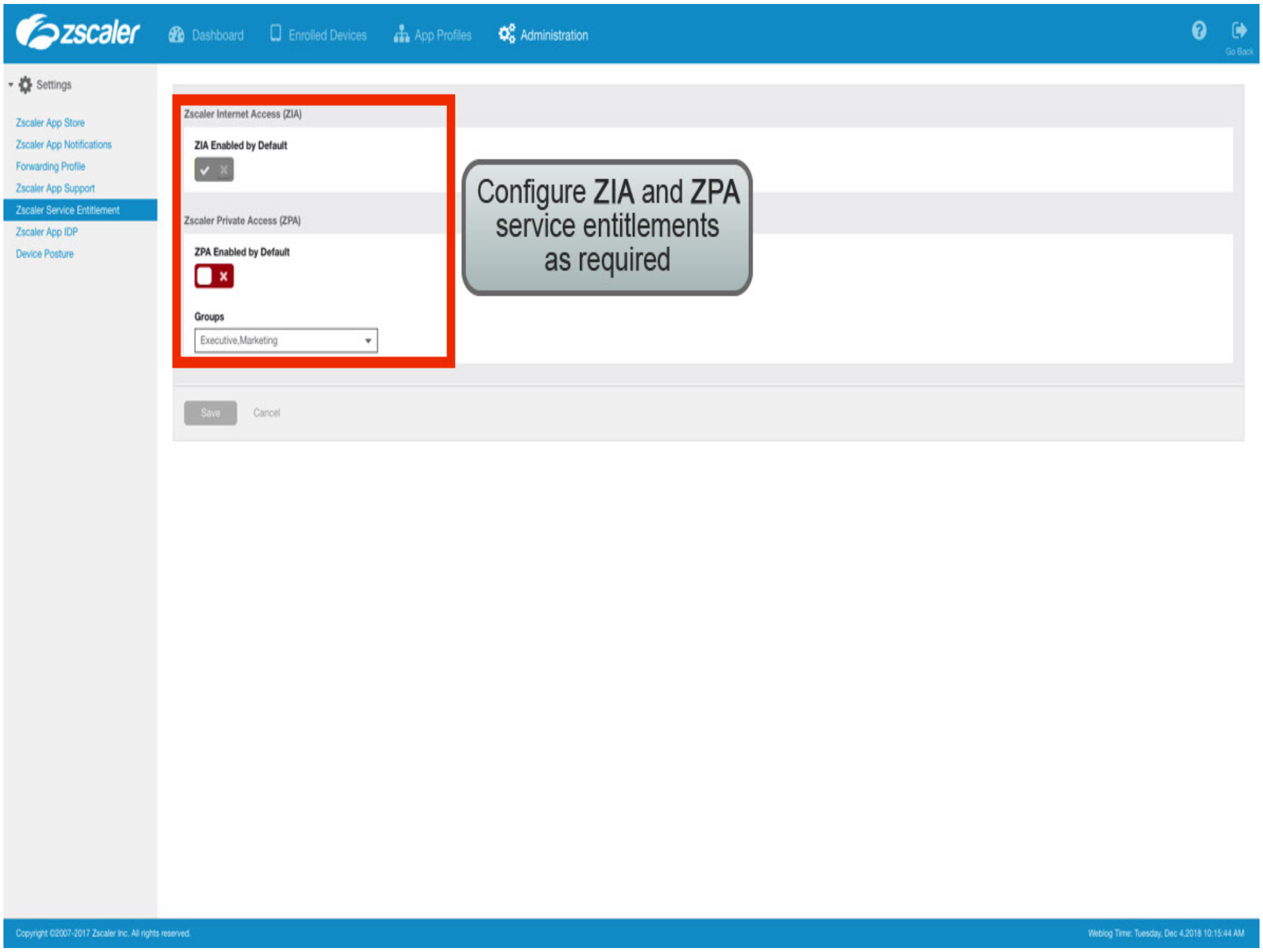
Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Tuesday, Dec 4 2018 10:15:44 AM

Slide notes

To configure service entitlements, click **Zscaler Service Entitlement**. Note that this option is only visible if you subscribe to the Zscaler Private Access (ZPA) service.

Slide 25 - Slide 25



Zscaler Internet Access (ZIA)

ZIA Enabled by Default ✓

Zscaler Private Access (ZPA)

ZPA Enabled by Default ✗

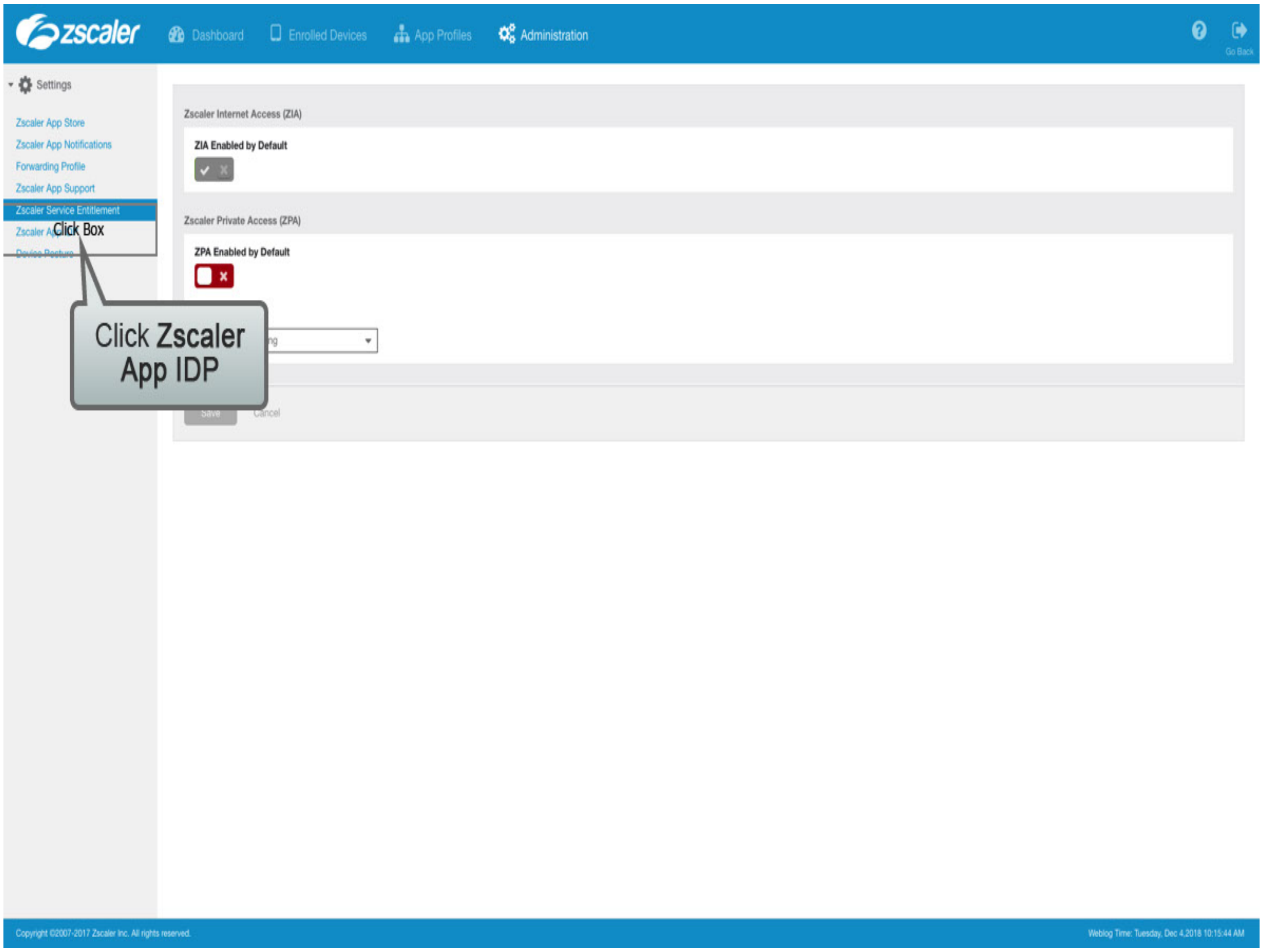
Groups: Executive,Marketing

Configure ZIA and ZPA service entitlements as required

Slide notes

For ZPA customers, all users have both Zscaler Internet Access (ZIA), and Zscaler Private Access functionality enabled by default. Here you have the option to restrict ZPA functionality to the members of a selected Group, or Groups.

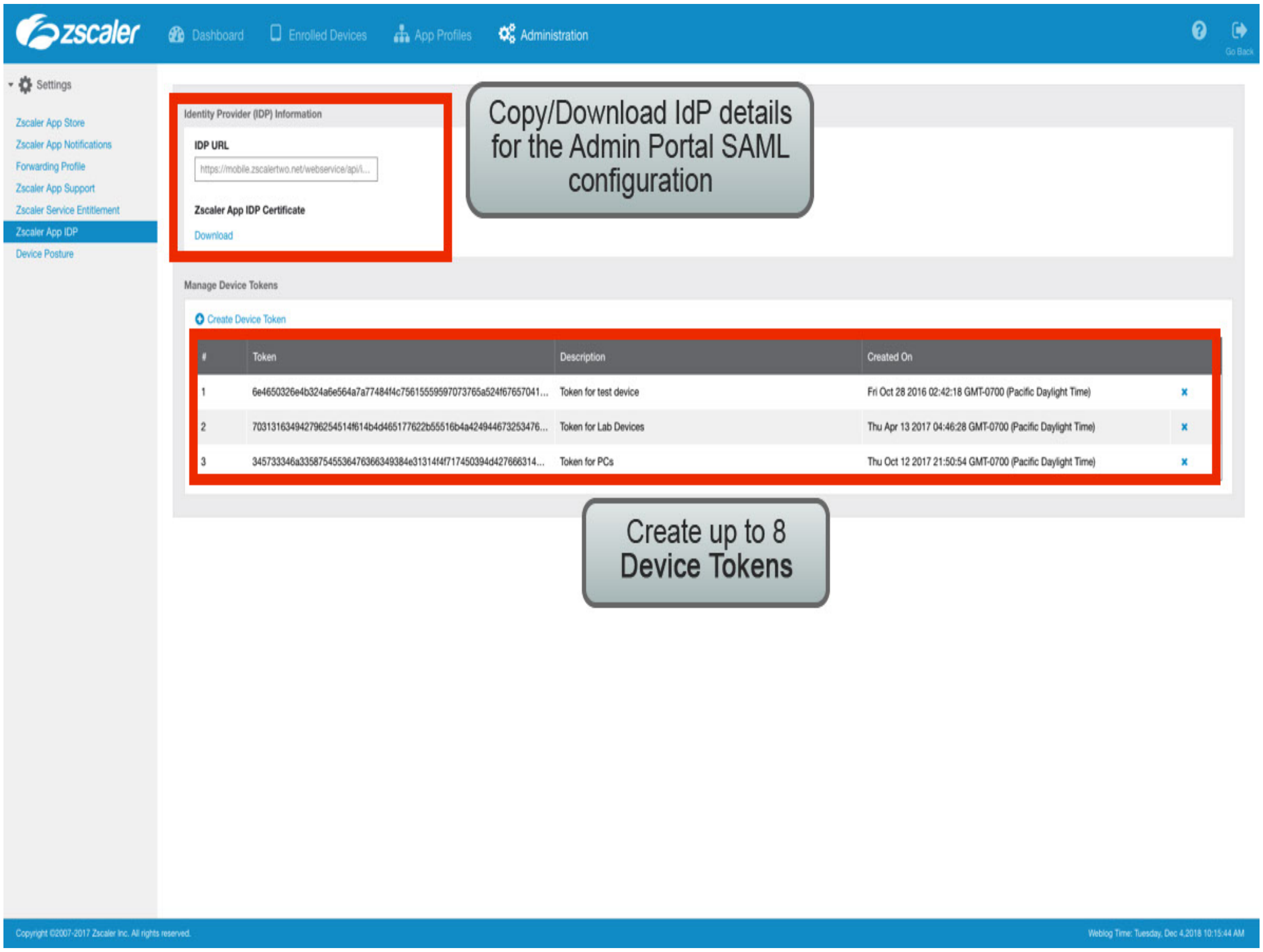
Slide 26 - Slide 26



Slide notes

To configure the Zscaler App Portal to act as a SAML IdP, click **Zscaler App IDP**.

Slide 27 - Slide 27



Identity Provider (IDP) Information

IDP URL: https://mobile.zscalertwo.net/webservice/api/i...

Zscaler App IDP Certificate

Download

Copy/Download IdP details for the Admin Portal SAML configuration

Manage Device Tokens

Create Device Token

#	Token	Description	Created On	
1	6e4650326e4b324a6e564a7a77484f4c756155595970737 65a524f67657041...	Token for test device	Fri Oct 28 2016 02:42:18 GMT-0700 (Pacific Daylight Time)	×
2	70313163494279625451 4f614b4d465177622b55516b4a424944673253476...	Token for Lab Devices	Thu Apr 13 2017 04:46:28 GMT-0700 (Pacific Daylight Time)	×
3	345733346a335875455364763666349384e31314f4f717450394d427666314...	Token for PCs	Thu Oct 12 2017 21:50:54 GMT-0700 (Pacific Daylight Time)	×

Create up to 8 Device Tokens

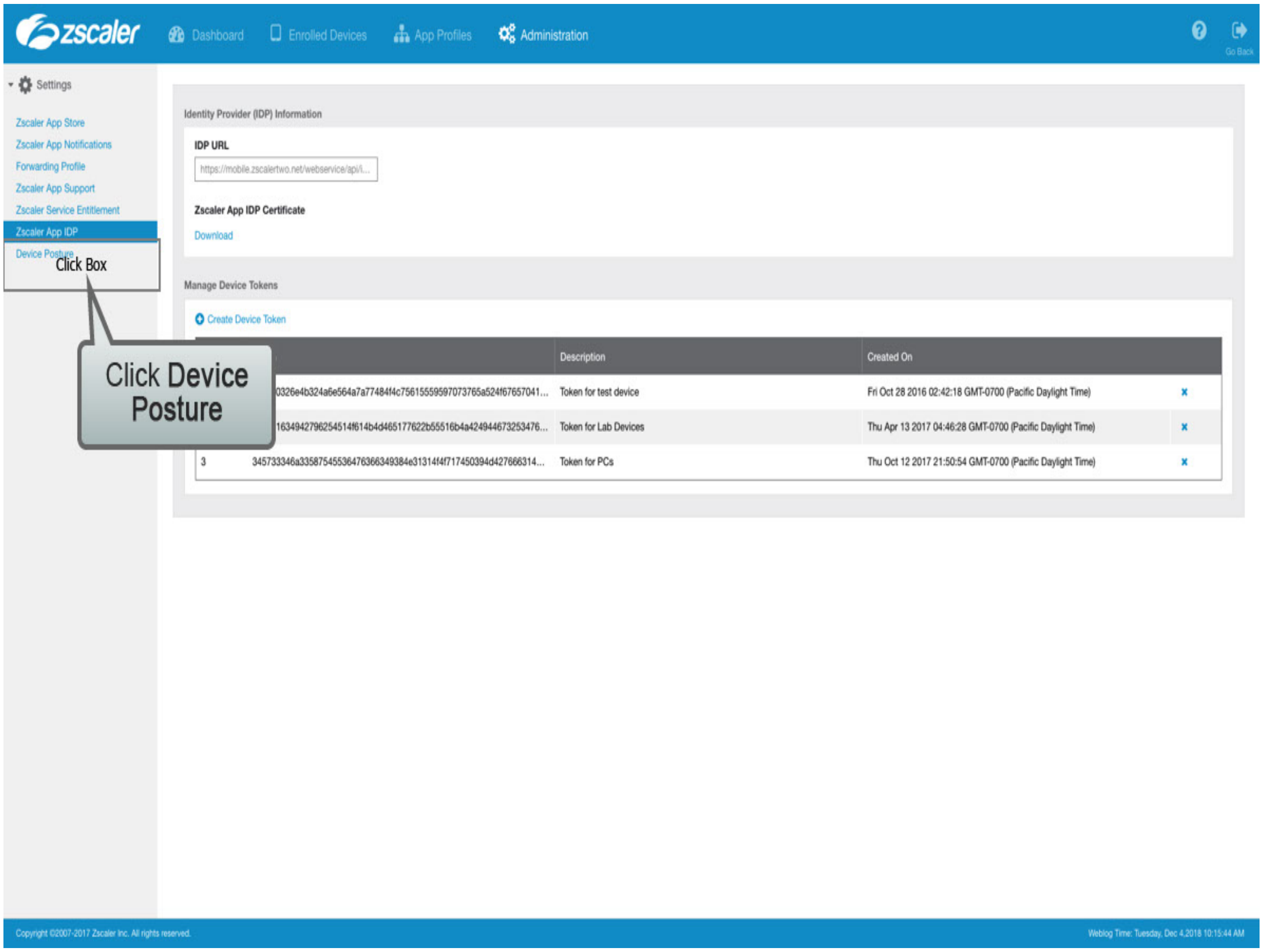
Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Tuesday, Dec 4,2018 10:15:44 AM

Slide notes

On this page, you may configure the Mobile Portal to act as a SAML IdP, to allow a silent authentication of the Zscaler App, based on the user identity from the device login. You may copy the **IdP URL**, and download the certificate required to integrate this IdP with the Zscaler Admin Portal, and create up to 8 **Device Tokens** for use during the install of the App on the client devices.

Slide 28 - Slide 28



Identity Provider (IDP) Information

IDP URL: https://mobile.zscalertwo.net/webservice/api/i...

Zscaler App IDP Certificate

Download

Manage Device Tokens

Create Device Token

		Description	Created On	
	0326e4b324a6e564a7a77484f4c756155595970737 65a524f67657041...	Token for test device	Fri Oct 28 2016 02:42:18 GMT-0700 (Pacific Daylight Time)	×
	16349427962545 14f614b4d465177622b55516b4a424944673253476...	Token for Lab Devices	Thu Apr 13 2017 04:46:28 GMT-0700 (Pacific Daylight Time)	×
3	345733346a33587545536476366349384e31314f4f717450394d427666314...	Token for PCs	Thu Oct 12 2017 21:50:54 GMT-0700 (Pacific Daylight Time)	×

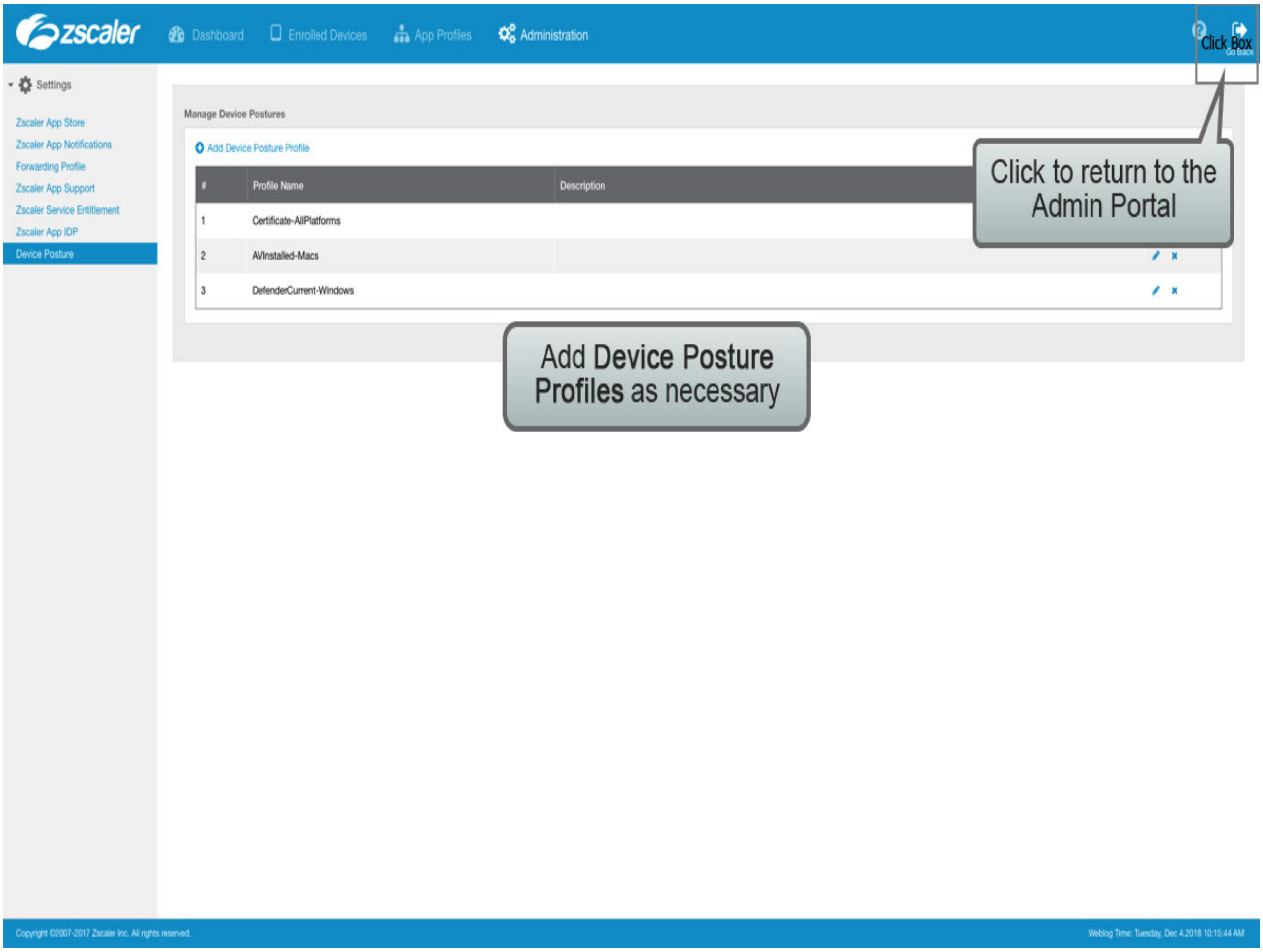
Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Tuesday, Dec 4,2018 10:15:44 AM

Slide notes

To configure Device Posture Profiles for Zscaler Private Access, click **Device Posture**. Note that this is another option that is only visible if you subscribe to the Zscaler Private Access (ZPA) service.

Slide 29 - Slide 29



Manage Device Postures

#	Profile Name	Description
1	Certificate-AllPlatforms	
2	AVInstalled-Macs	
3	DefenderCurrent-Windows	

Click to return to the Admin Portal

Add Device Posture Profiles as necessary

Copyright ©2007-2017 Zscaler Inc. All rights reserved.

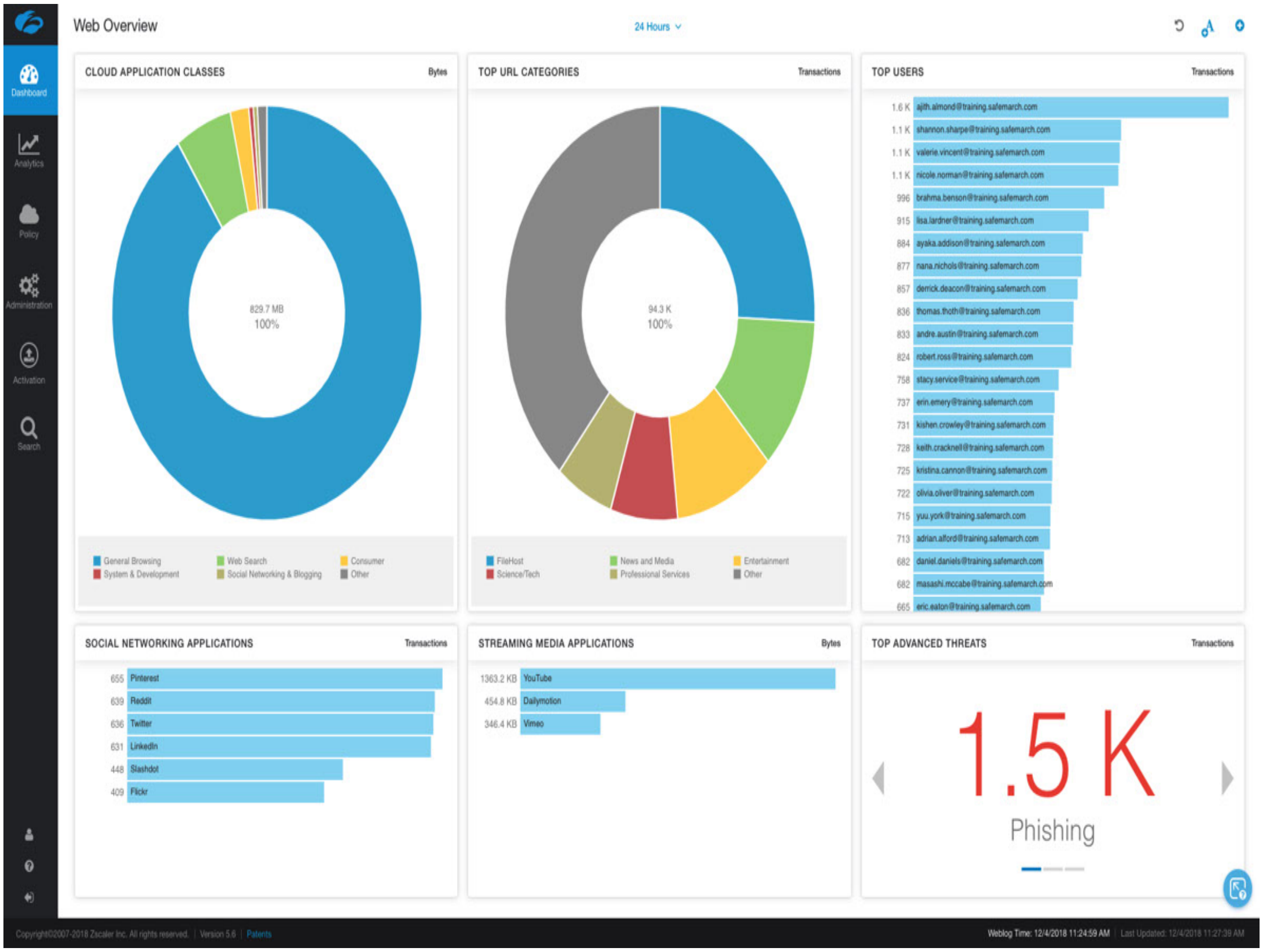
Weblog Time: Tuesday, Dec 4,2018 10:15:44 AM

Slide notes

The **Device Posture** feature is relevant only if your organization is using the Zscaler App for Private Access (ZPA). The **Device Posture** Profile is a set of criteria that a user's device must meet in order to access applications with ZPA.

For a full description of the profiles and configuration options at the Zscaler App Portal, see the Zscaler App module in the ZCCP certification content. To return to the Admin Portal, click the **Go Back** link at top right…

Slide 30 - Slide 30



TOP USERS — Transactions

1.6 K	ajith.almond@training.safemarch.com
1.1 K	shannon.sharpe@training.safemarch.com
1.1 K	valerie.vincent@training.safemarch.com
1.1 K	nicole.norman@training.safemarch.com
996	brahma.benson@training.safemarch.com
915	lisa.lardner@training.safemarch.com
884	ayaka.addison@training.safemarch.com
877	nana.nichols@training.safemarch.com
857	derrick.deacon@training.safemarch.com
836	thomas.thoth@training.safemarch.com
833	andre.austin@training.safemarch.com
824	robert.ross@training.safemarch.com
758	stacy.service@training.safemarch.com
737	erin.emery@training.safemarch.com
731	kishen.crowley@training.safemarch.com
728	keith.cracknell@training.safemarch.com
725	kristina.cannon@training.safemarch.com
722	olivia.oliver@training.safemarch.com
715	yuu.york@training.safemarch.com
713	adrian.alford@training.safemarch.com
682	daniel.daniels@training.safemarch.com
682	masashi.mccabe@training.safemarch.com
665	eric.eaton@training.safemarch.com

SOCIAL NETWORKING APPLICATIONS — Transactions

655	Pinterest
639	Reddit
636	Twitter
631	LinkedIn
448	Slashdot
409	Flickr

STREAMING MEDIA APPLICATIONS — Bytes

1363.2 KB	YouTube
454.8 KB	Dailymotion
346.4 KB	Vimeo

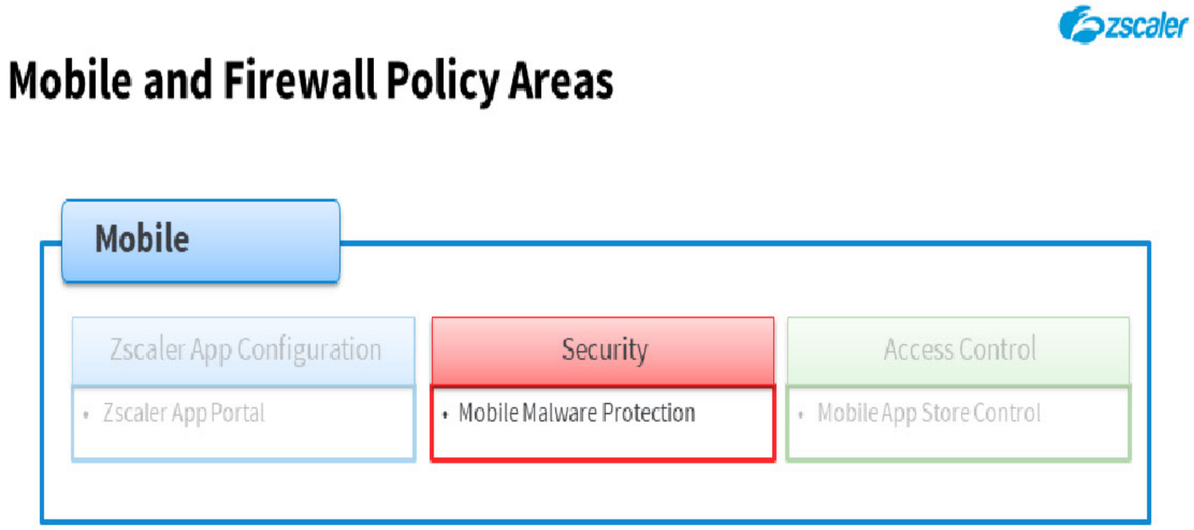
Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents

Weblog Time: 12/4/2018 11:24:59 AM | Last Updated: 12/4/2018 11:27:39 AM

Slide notes

...and you will be taken back to the **Dashboard** page.

Slide 31 - Mobile and Firewall Policy Areas



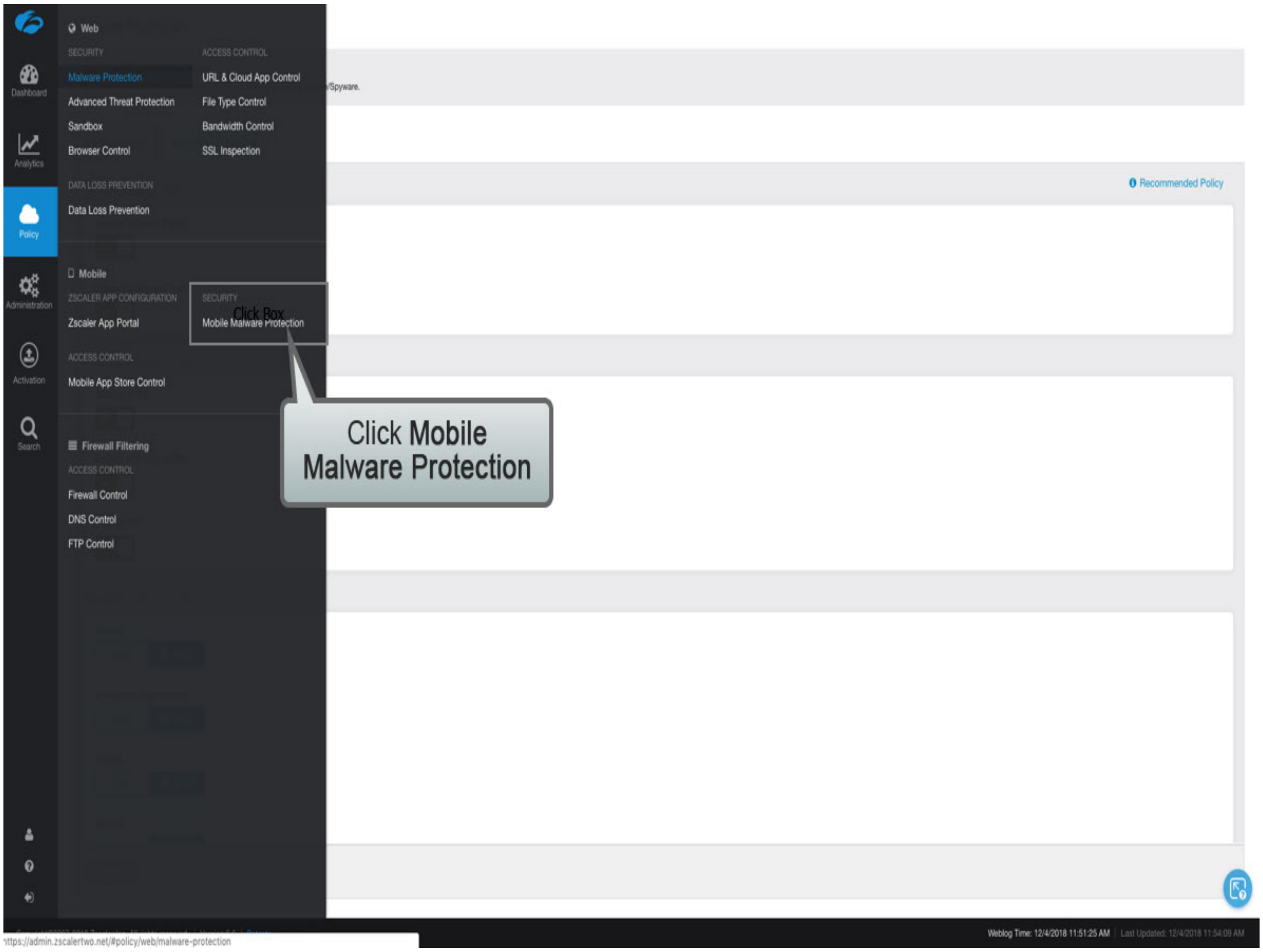
Mobile and Firewall Policy Areas

zscaler
Mobile
Zscaler App Configuration
• Zscaler App Portal
Security
• Mobile Malware Protection
Access Control
• Mobile App Store Control

Slide notes

Next, we will look at the **Mobile Malware Protection** options.

Slide 32 - Slide 32

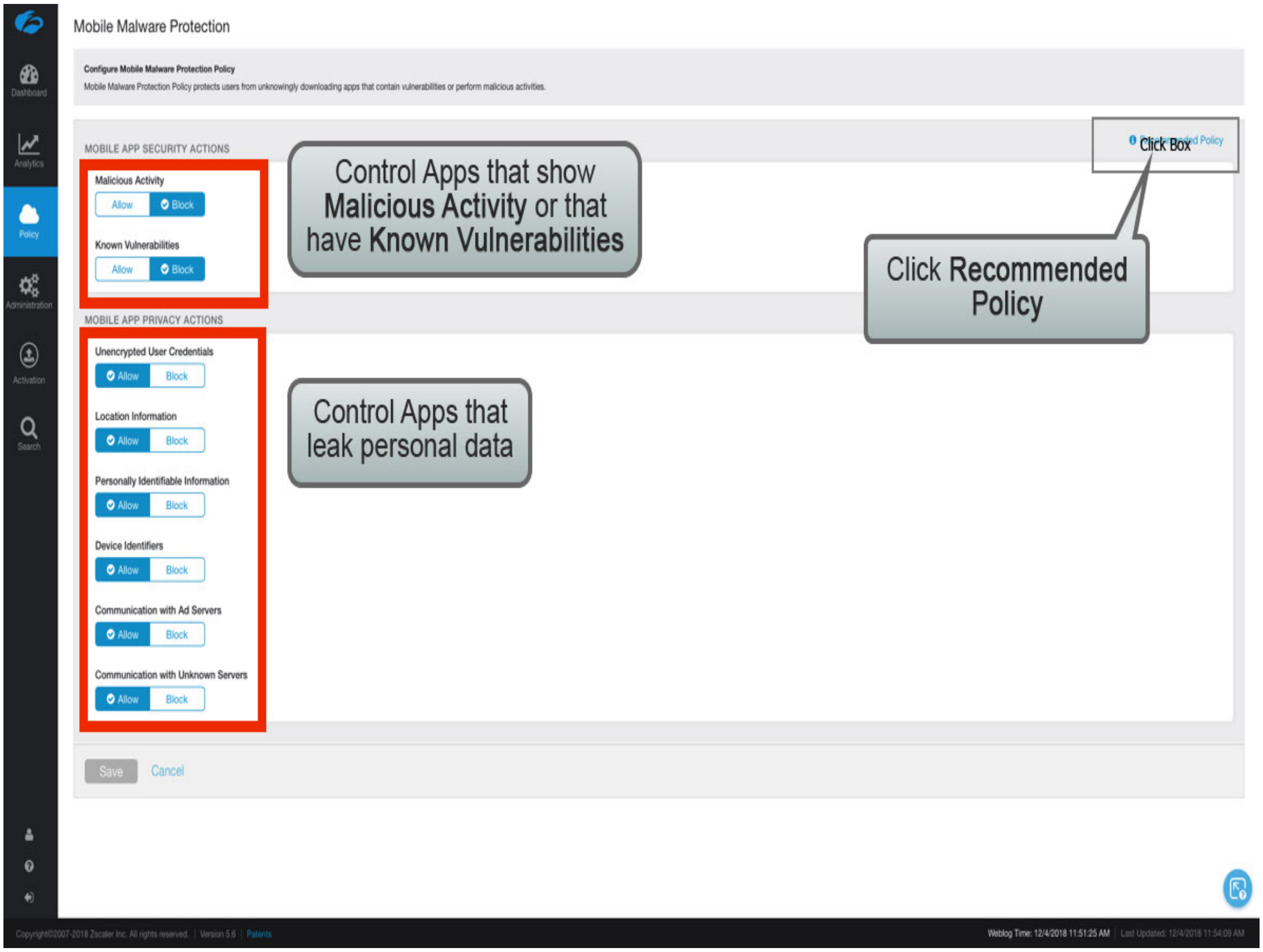


Click Mobile Malware Protection

Slide notes

From the **Policy** menu, select **Mobile Malware Protection**.

Slide 33 - Slide 33



Mobile Malware Protection

Configure Mobile Malware Protection Policy

Mobile Malware Protection Policy protects users from unknowingly downloading apps that contain vulnerabilities or perform malicious activities.

MOBILE APP SECURITY ACTIONS

Malicious Activity: Allow [✓ Block]

Known Vulnerabilities: Allow [✓ Block]

MOBILE APP PRIVACY ACTIONS

Unencrypted User Credentials: [✓ Allow] Block

Location Information: [✓ Allow] Block

Personally Identifiable Information: [✓ Allow] Block

Device Identifiers: [✓ Allow] Block

Communication with Ad Servers: [✓ Allow] Block

Communication with Unknown Servers: [✓ Allow] Block

Save Cancel

Click Box

Control Apps that show **Malicious Activity** or that have **Known Vulnerabilities**

Control Apps that leak personal data

Click **Recommended** Policy

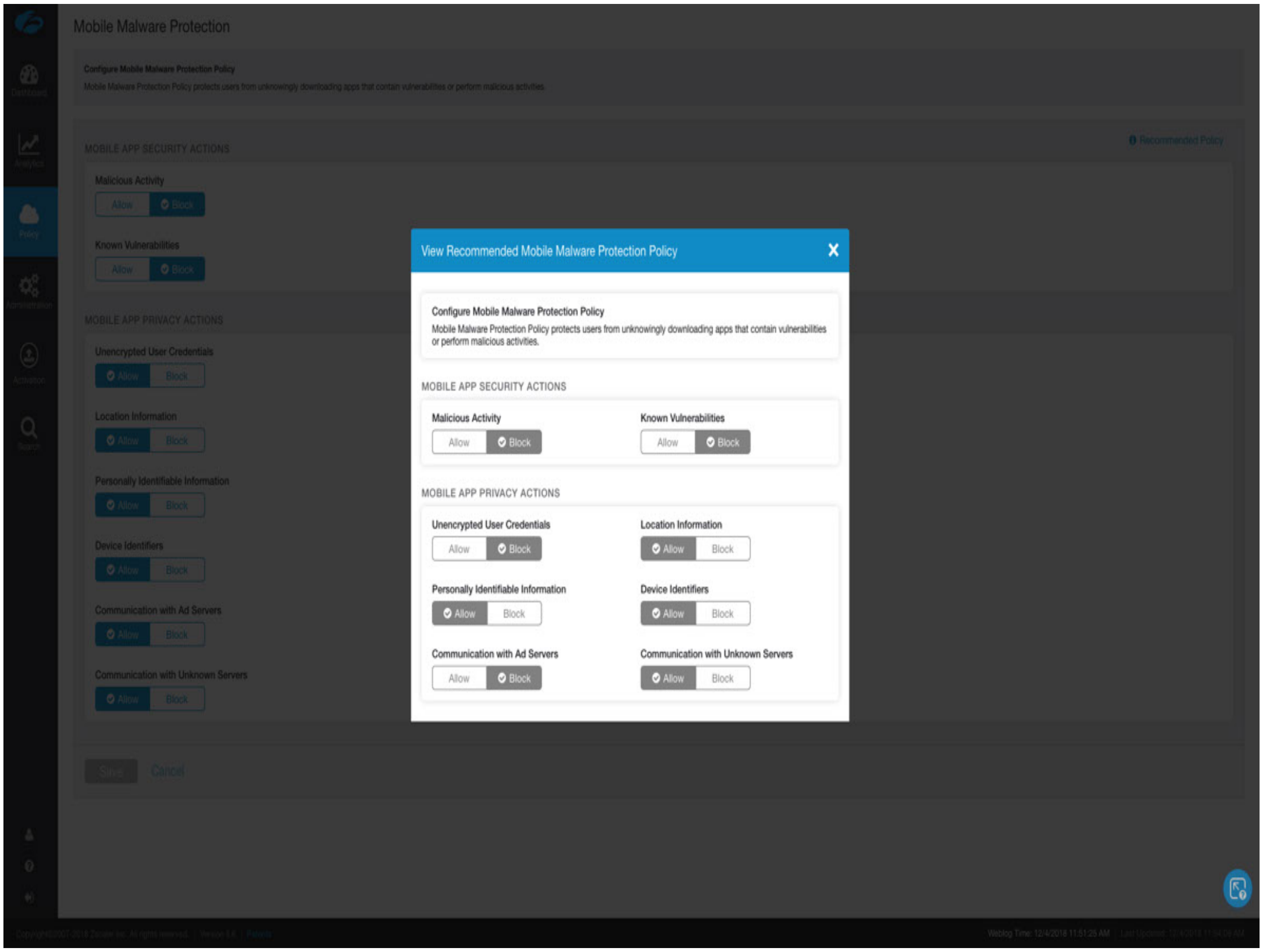
Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents

Weblog Time: 12/4/2018 11:51:25 AM | Last Updated: 12/4/2018 11:54:09 AM

Slide notes

Zscaler has a default policy that prevents users from unwittingly downloading apps to mobile devices that are known to contain vulnerabilities or perform malicious activities, but allows all other apps. You can also block apps that leak certain types of information. Adjust this policy as necessary to meet your mobile malware protection needs. To view Zscaler recommended settings for this policy, click the **Recommended Policy** link.

Slide 34 - Slide 34



View Recommended Mobile Malware Protection Policy

Configure Mobile Malware Protection Policy

Mobile Malware Protection Policy protects users from unknowingly downloading apps that contain vulnerabilities or perform malicious activities.

MOBILE APP SECURITY ACTIONS

- Malicious Activity: Allow [✓ Block]
- Known Vulnerabilities: Allow [✓ Block]

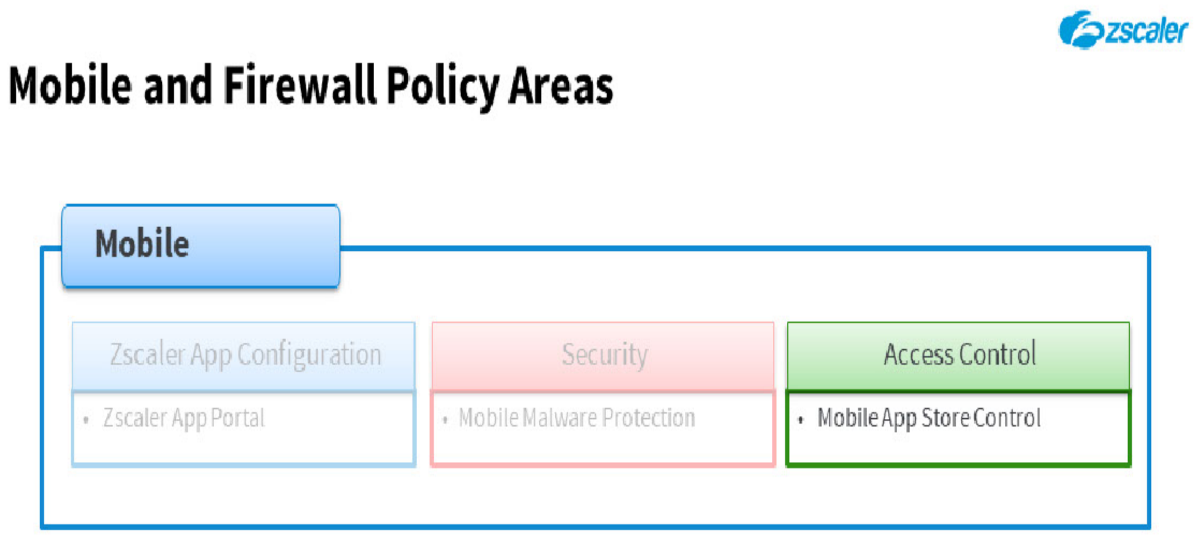
MOBILE APP PRIVACY ACTIONS

- Unencrypted User Credentials: Allow [✓ Block]
- Location Information: [✓ Allow] Block
- Personally Identifiable Information: [✓ Allow] Block
- Device Identifiers: [✓ Allow] Block
- Communication with Ad Servers: Allow [✓ Block]
- Communication with Unknown Servers: [✓ Allow] Block

Slide notes

For the **Mobile Malware Protection** Policy, Zscaler recommends that you block **Malicious Activity** and **Known Vulnerabilities** under the **Mobile App Security Actions** area. Then under **Mobile App Privacy Actions**, we recommend that you block **Unencrypted User Credentials** and **Communication with Ad Servers**.

Slide 35 - Interactive Demo: Creating NGFW Policy



Mobile and Firewall Policy Areas

Mobile

Zscaler App Configuration

- Zscaler App Portal

Security

- Mobile Malware Protection

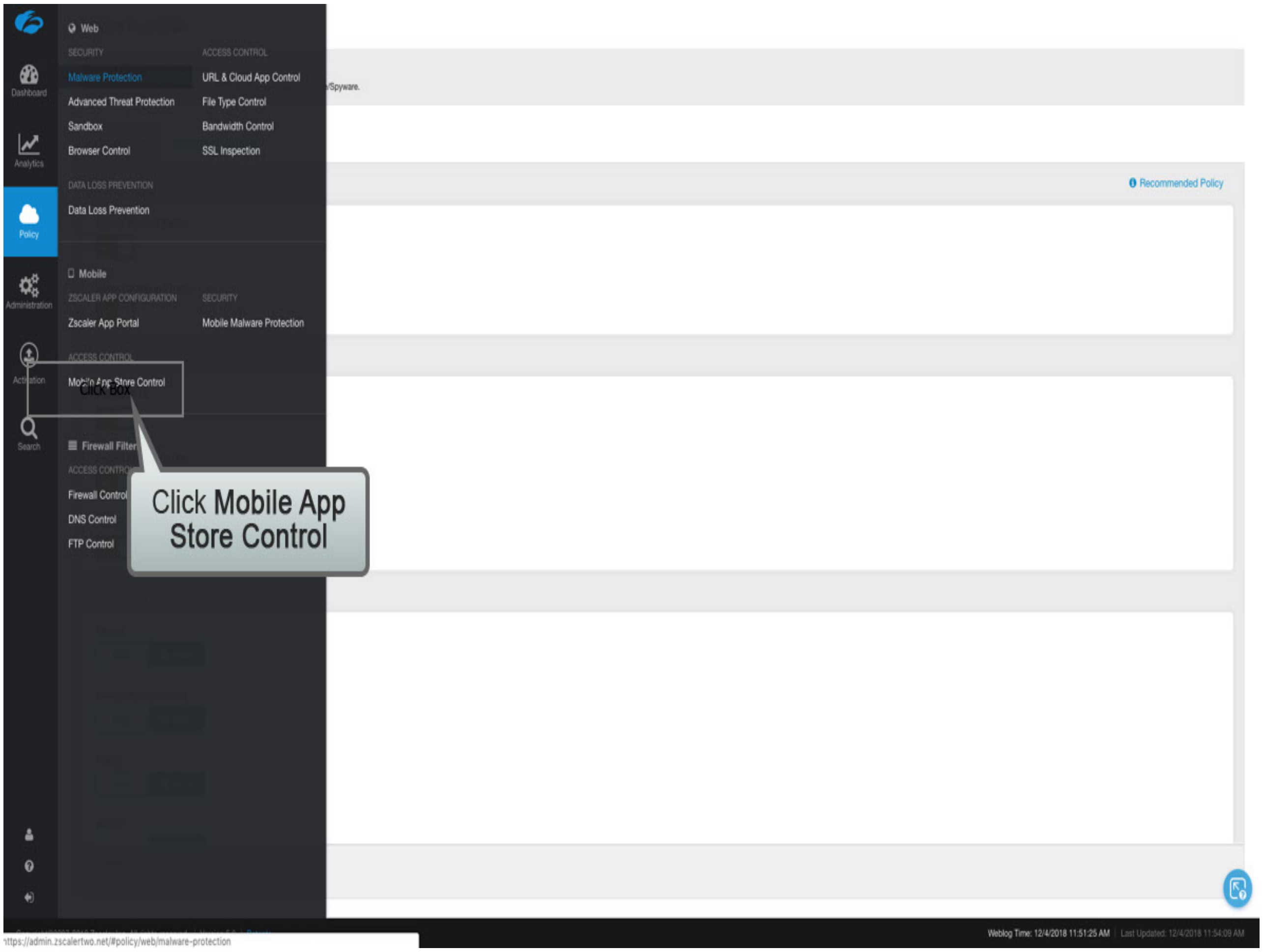
Access Control

- Mobile App Store Control

Slide notes

lastly, we will look at the **Mobile App Store Control** options.

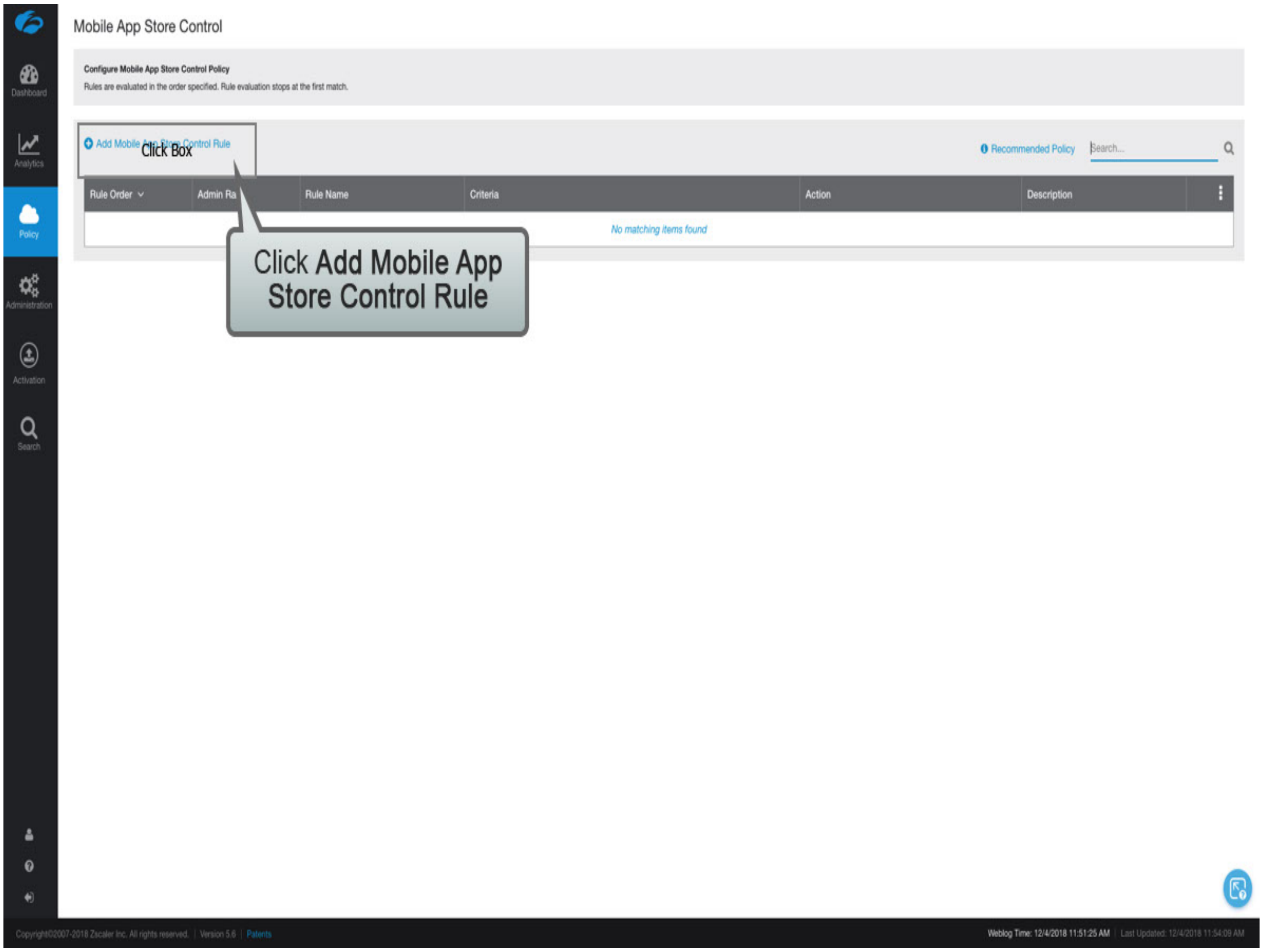
Slide 36 - Slide 36



Slide notes

To manage which App Stores users may download apps from, click **Mobile App Store Control**.

Slide 37 - Slide 37



Mobile App Store Control

Configure Mobile App Store Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Add Mobile App Store Control Rule

Click Box

Recommended Policy

Search...

Rule Order	Admin Ra	Rule Name	Criteria	Action	Description
No matching items found					

Click Add Mobile App Store Control Rule

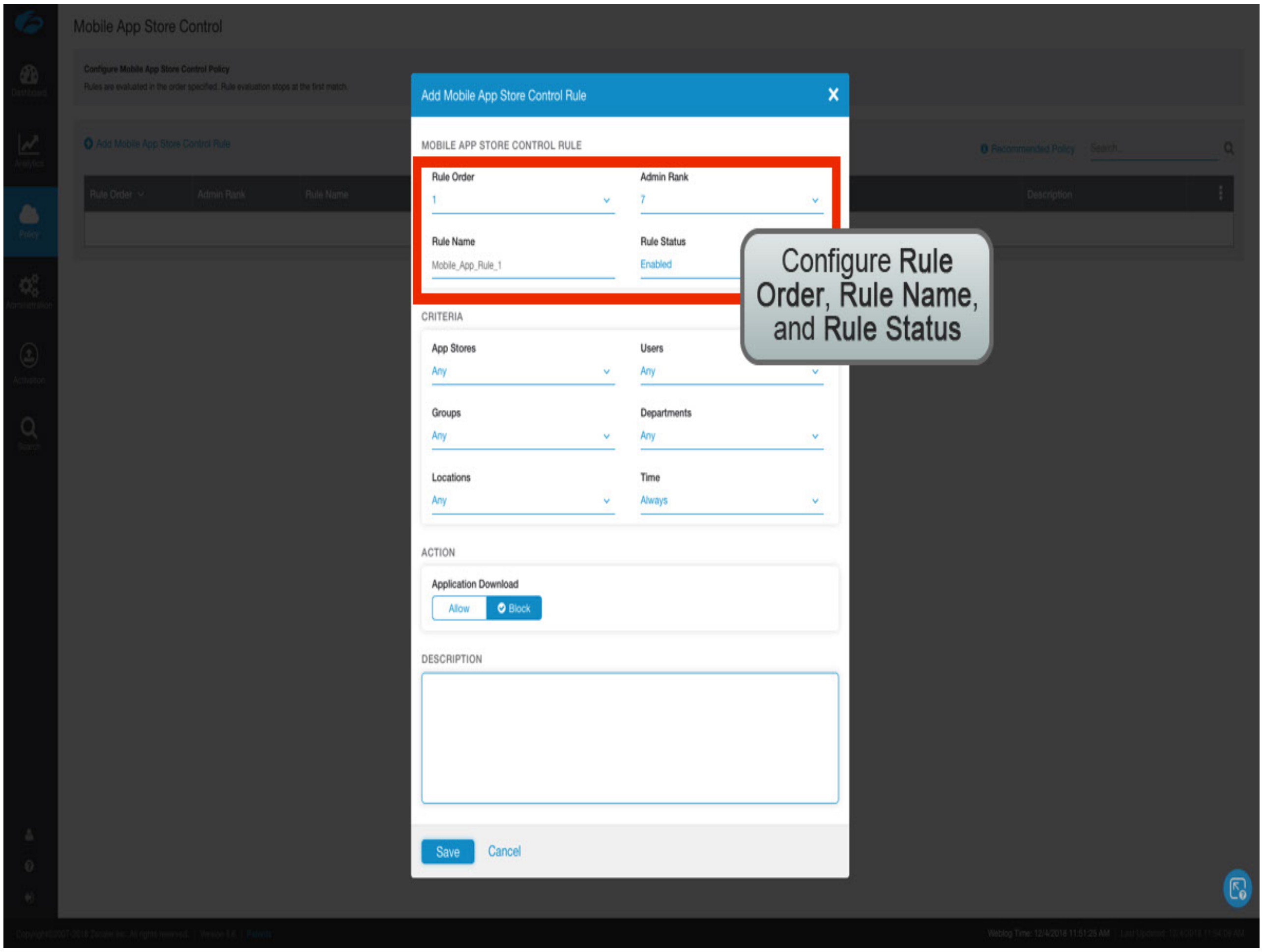
Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents

Weblog Time: 12/4/2018 11:51:25 AM | Last Updated: 12/4/2018 11:54:09 AM

Slide notes

The default action when no policy is configured is to allow App downloads from all App Stores. You have the option define a list of App Stores from which users are not allowed to download Apps, they will still be able to browse the App Stores in the list, but will be blocked from downloading Apps from those stores. To add a control rule, click the **Add Mobile App Store Control Rule** link.

Slide 38 - Slide 38



Add Mobile App Store Control Rule

MOBILE APP STORE CONTROL RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Mobile_App_Rule_1

Rule Status: Enabled

CRITERIA

App Stores: Any

Users: Any

Groups: Any

Departments: Any

Locations: Any

Time: Always

ACTION

Application Download: Allow / Block

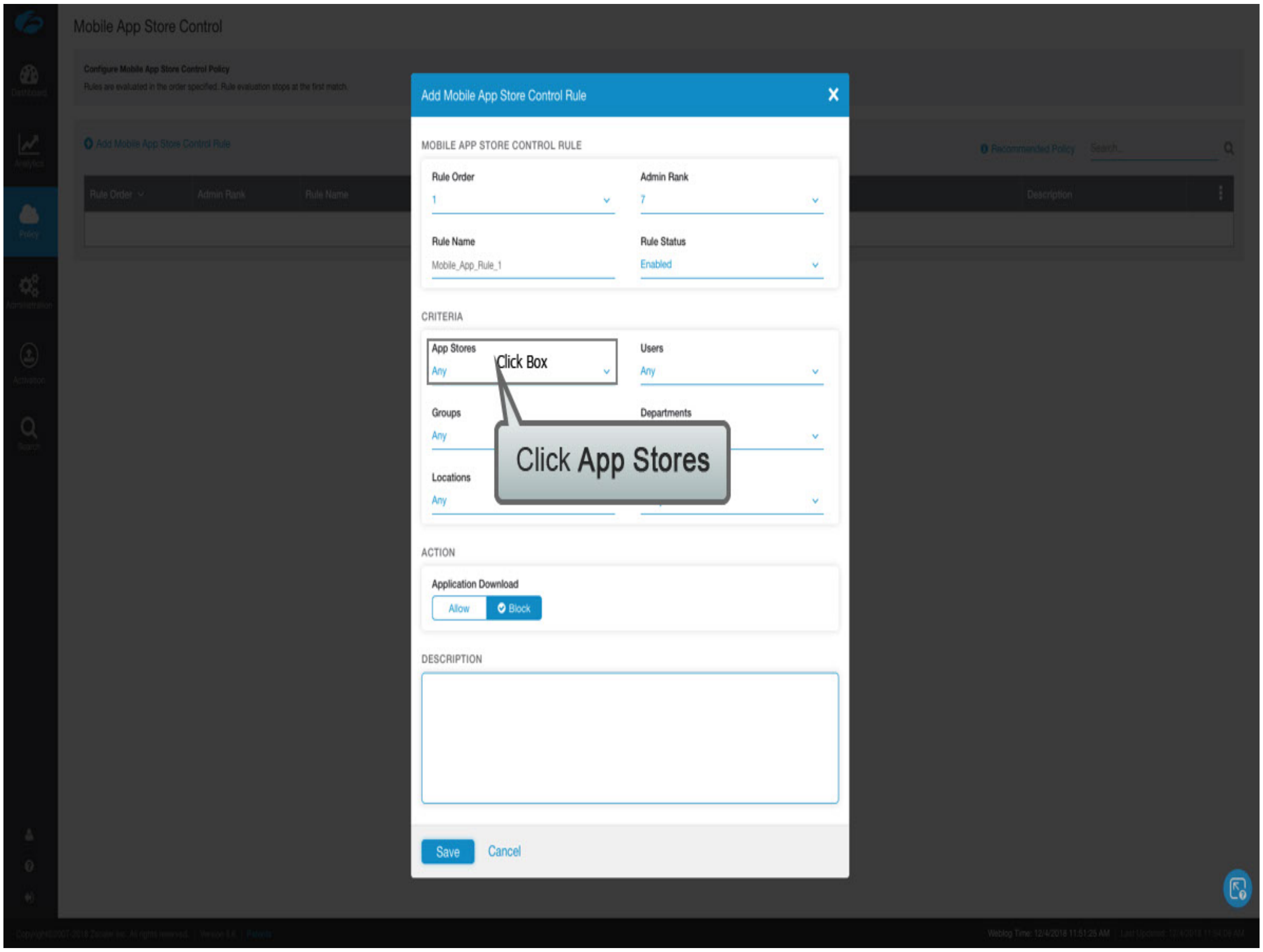
DESCRIPTION

Configure Rule Order, Rule Name, and Rule Status

Slide notes

As with the other rule types, you can manage the **Rule Order**, **Rule Name**, and **Rule Status**.

Slide 39 - Slide 39



Mobile App Store Control

Configure Mobile App Store Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Add Mobile App Store Control Rule

MOBILE APP STORE CONTROL RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Mobile_App_Rule_1

Rule Status: Enabled

CRITERIA

App Stores: Any

Users: Any

Groups: Any

Departments

Locations: Any

ACTION

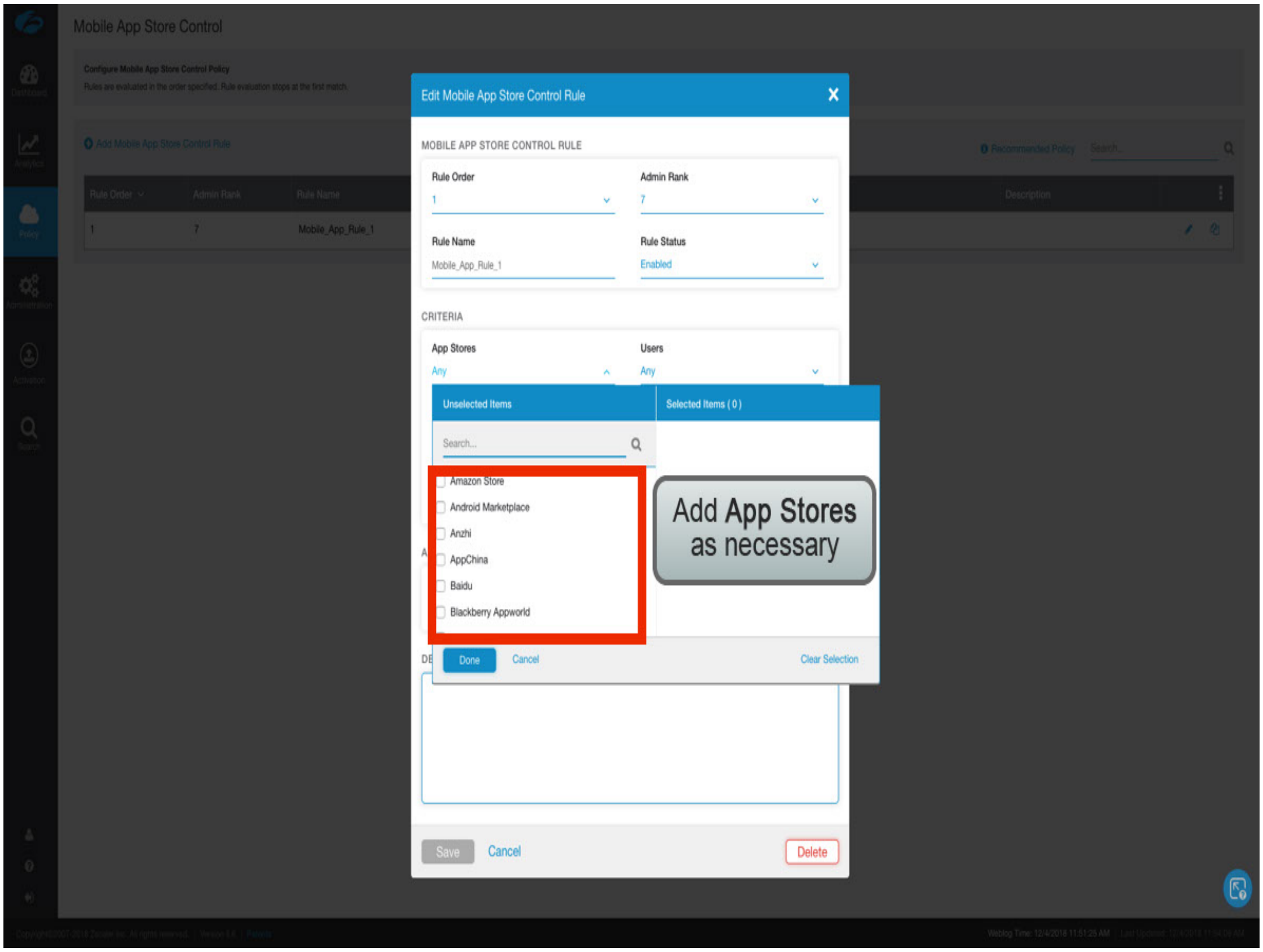
Application Download: Allow / Block

DESCRIPTION

Slide notes

To select which App Stores the rule is to apply to, click **App Stores**...

Slide 40 - Slide 40



Mobile App Store Control

Configure Mobile App Store Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Edit Mobile App Store Control Rule

MOBILE APP STORE CONTROL RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Mobile_App_Rule_1

Rule Status: Enabled

CRITERIA

App Stores: Any

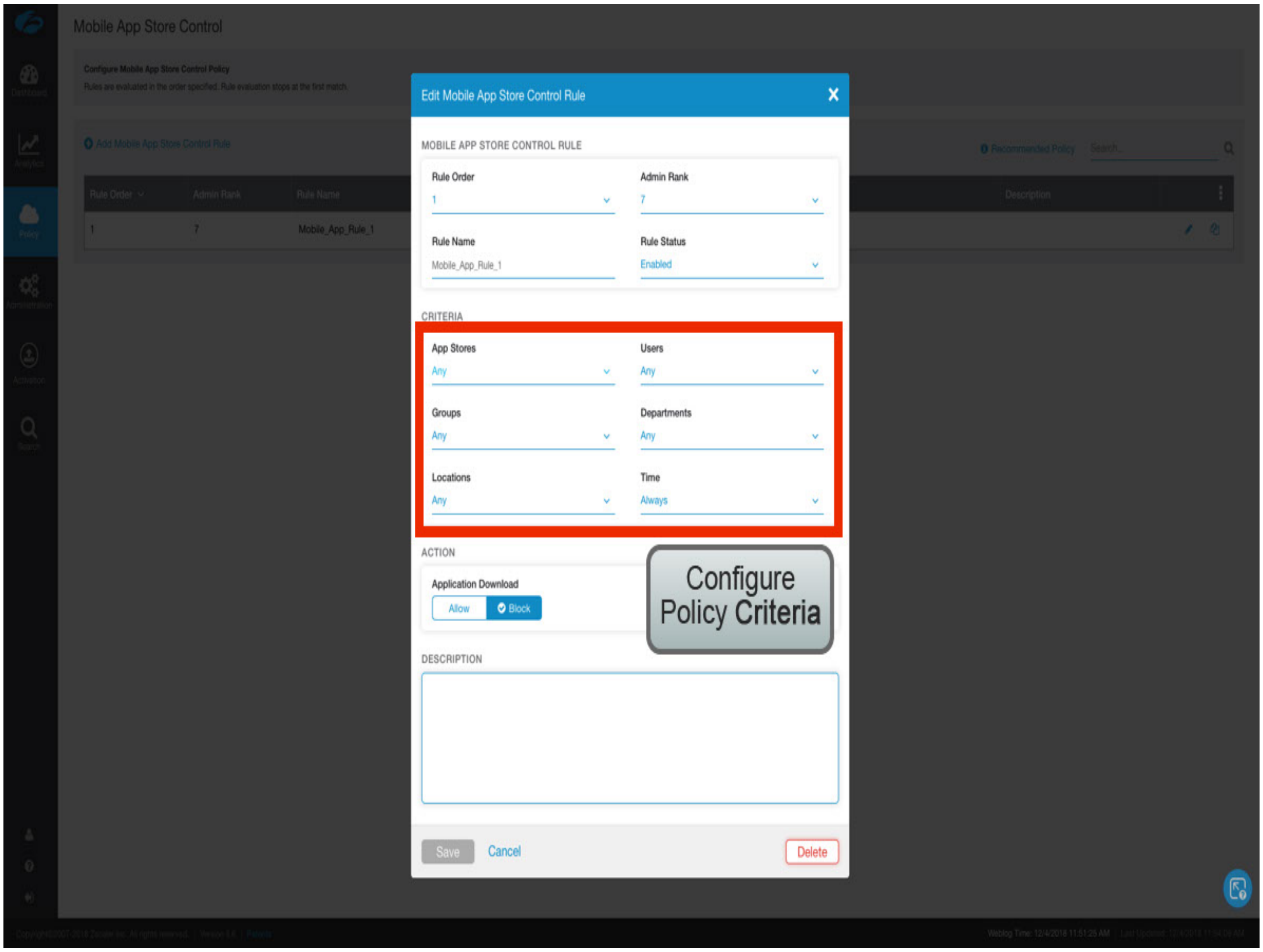
Users: Any

Add App Stores as necessary

Slide notes

...and select the App Sores to be included.

Slide 41 - Slide 41



Mobile App Store Control

Configure Mobile App Store Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Add Mobile App Store Control Rule

Rule Order	Admin Rank	Rule Name	Description
1	7	Mobile_App_Rule_1	

Edit Mobile App Store Control Rule

MOBILE APP STORE CONTROL RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Mobile_App_Rule_1

Rule Status: Enabled

CRITERIA

App Stores: Any

Users: Any

Groups: Any

Departments: Any

Locations: Any

Time: Always

ACTION

Application Download: Allow [✓ Block]

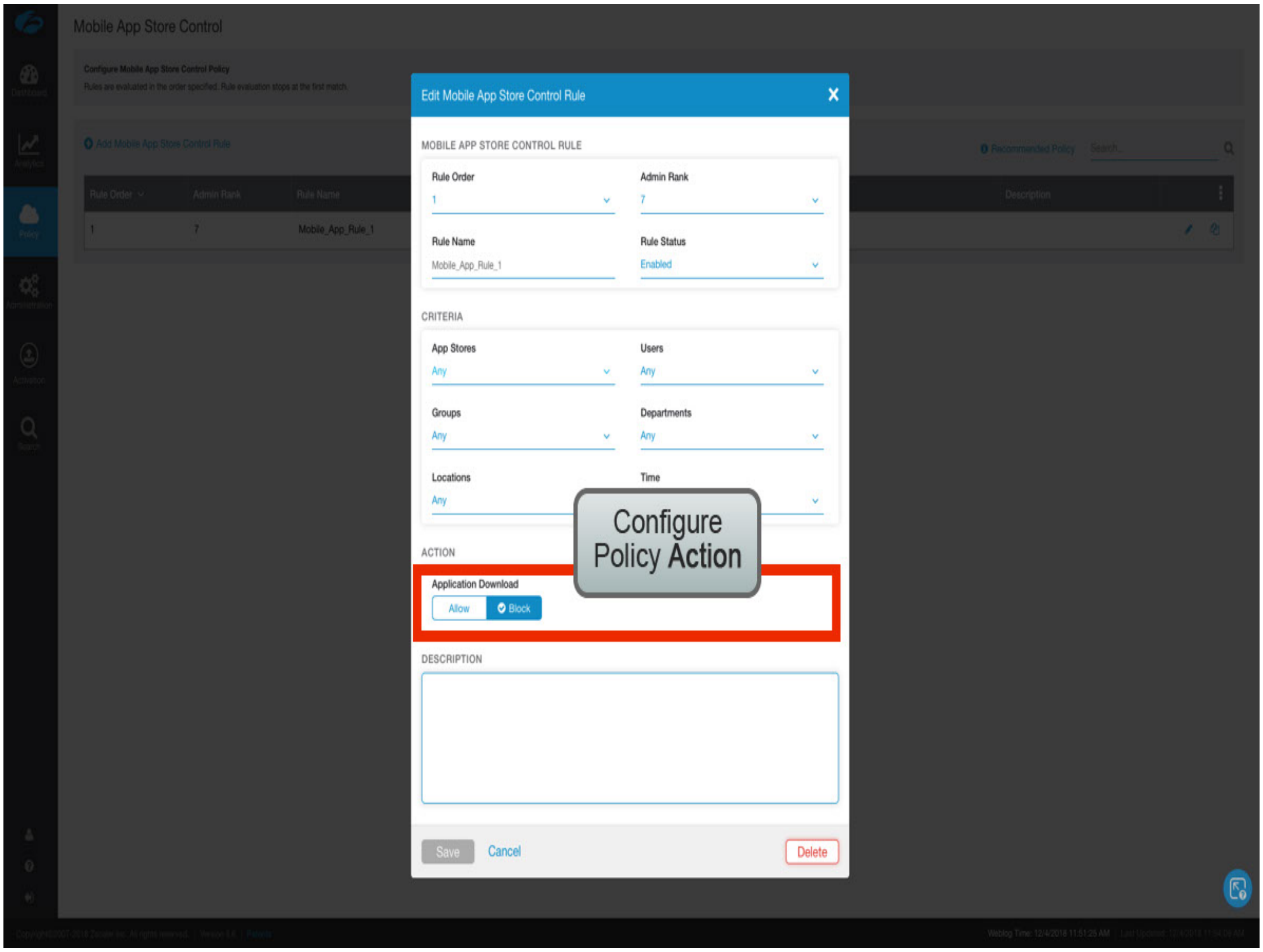
DESCRIPTION

Save Cancel Delete

Slide notes

Configure the rule as necessary for the standard **Criteria**, such as; **Users**, **Groups**, **Departments**, **Locations**, and **Time**.

Slide 42 - Slide 42



Mobile App Store Control

Configure Mobile App Store Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Rule Order	Admin Rank	Rule Name
1	7	Mobile_App_Rule_1

Edit Mobile App Store Control Rule

MOBILE APP STORE CONTROL RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Mobile_App_Rule_1

Rule Status: Enabled

CRITERIA

App Stores: Any

Users: Any

Groups: Any

Departments: Any

Locations: Any

Time

ACTION

Application Download: Allow [✓ Block]

DESCRIPTION

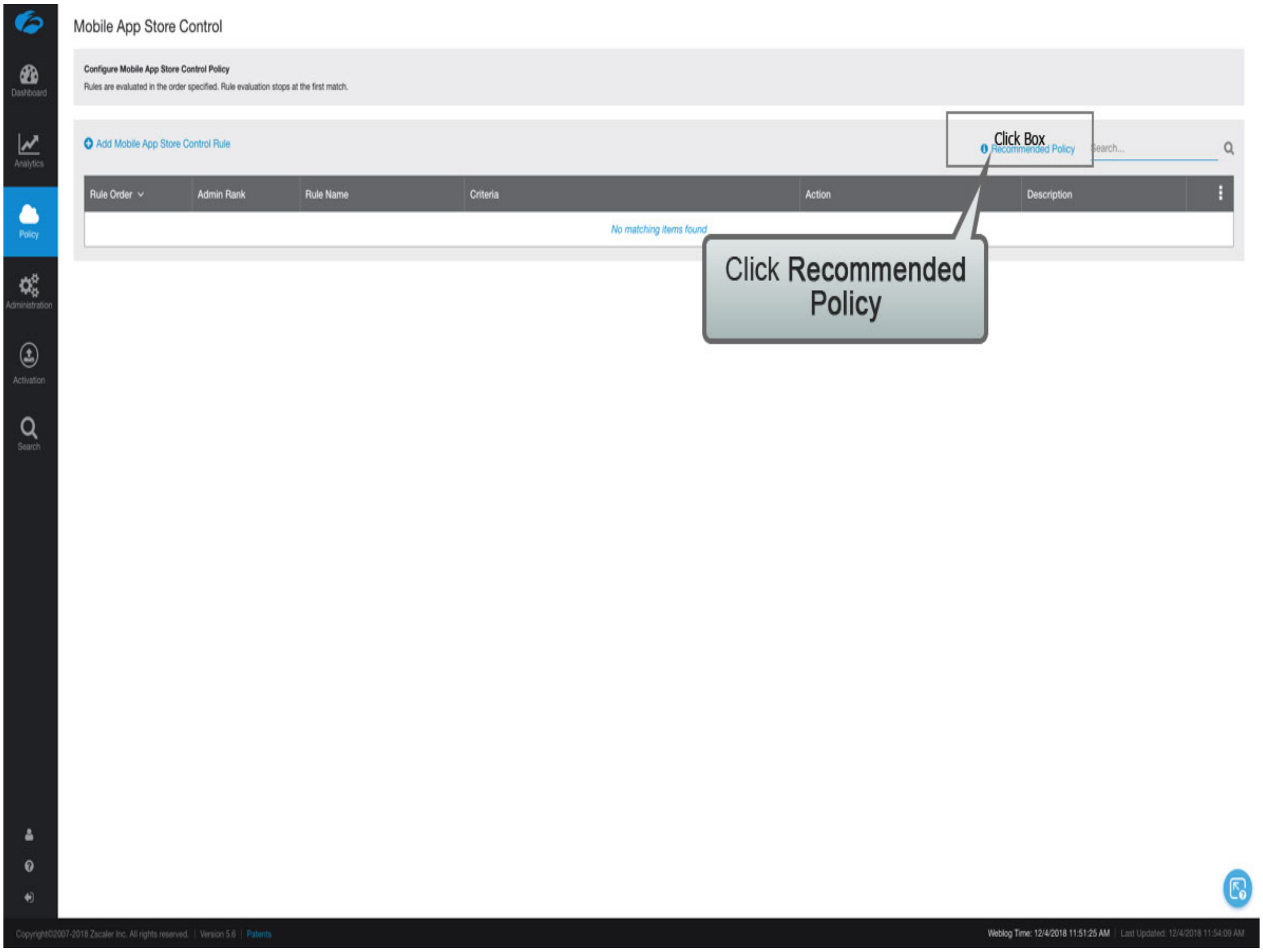
Configure Policy Action

Slide notes

Then specify whether **Application Downloads** are to be **Allowed**, or **Blocked**.

You would then need to **Save** the rule, and of course **Activate** your changes.

Slide 43 - Slide 43



Mobile App Store Control

Configure Mobile App Store Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description

No matching items found

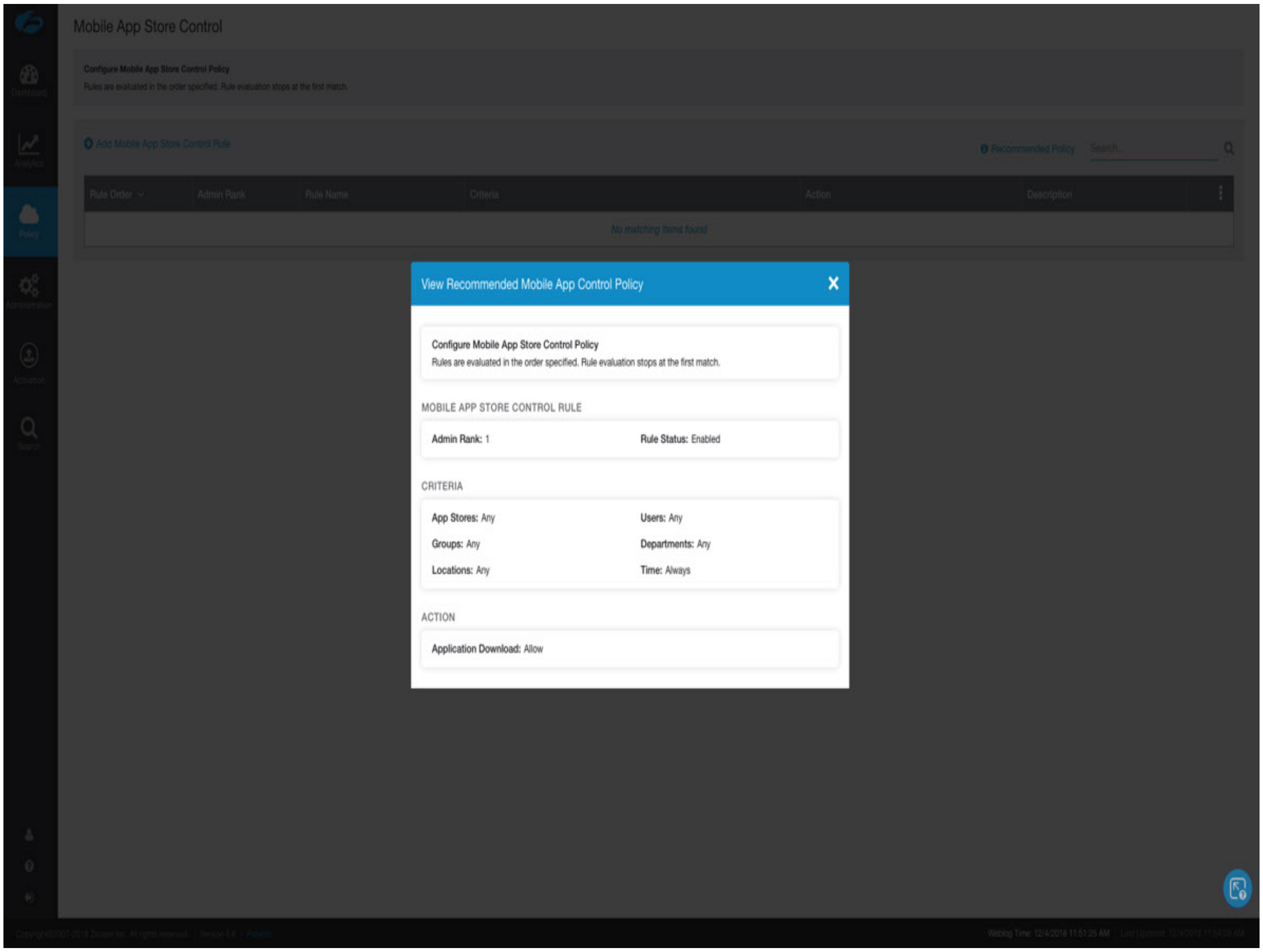
Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patents

Weblog Time: 12/4/2018 11:51:25 AM | Last Updated: 12/4/2018 11:54:09 AM

Slide notes

To see Zscaler recommended settings for this Policy, click the **Recommended Policy** link.

Slide 44 - Slide 44



Mobile App Store Control

Configure Mobile App Store Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

Add Mobile App Store Control Rule

Recommended Policy

Search...

Rule Order	Admin Rank	Rule Name	Criteria	Action	Description
No matching items found					

View Recommended Mobile App Control Policy ✕

Configure Mobile App Store Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at the first match.

MOBILE APP STORE CONTROL RULE

Admin Rank: 1 **Rule Status:** Enabled

CRITERIA

App Stores: Any **Users:** Any
Groups: Any **Departments:** Any
Locations: Any **Time:** Always

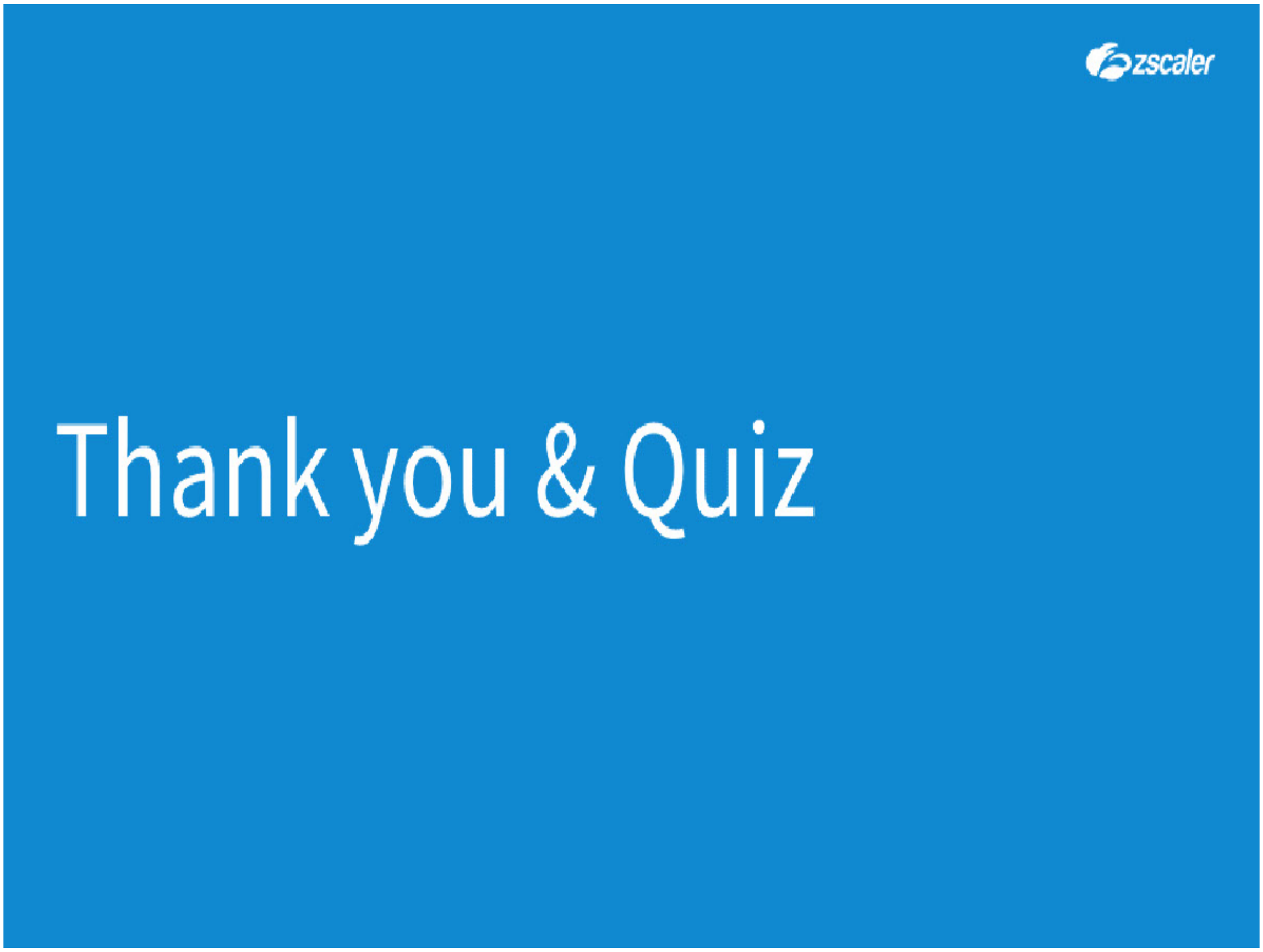
ACTION

Application Download: Allow

Slide notes

It is difficult for Zscaler to recommend specific settings for the **Mobile App Store Control** Policy, as every organization will have their own perspective. The default setting is to allow all known App Stores, and you should **Block** access depending on your corporate policy.

Slide 45 - Thank you & Quiz



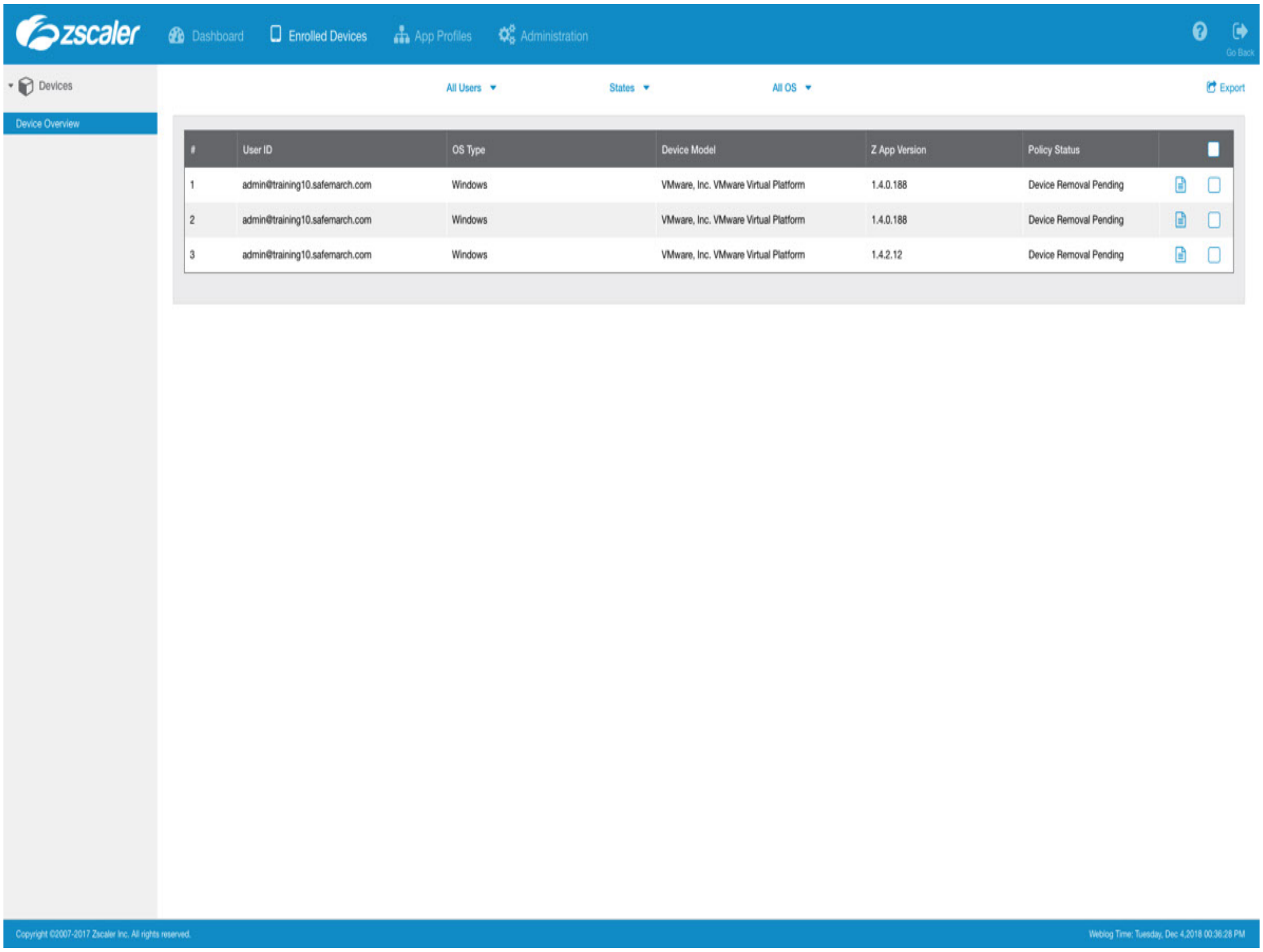
Thank you & Quiz

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.

Slide 46 - Slide 46



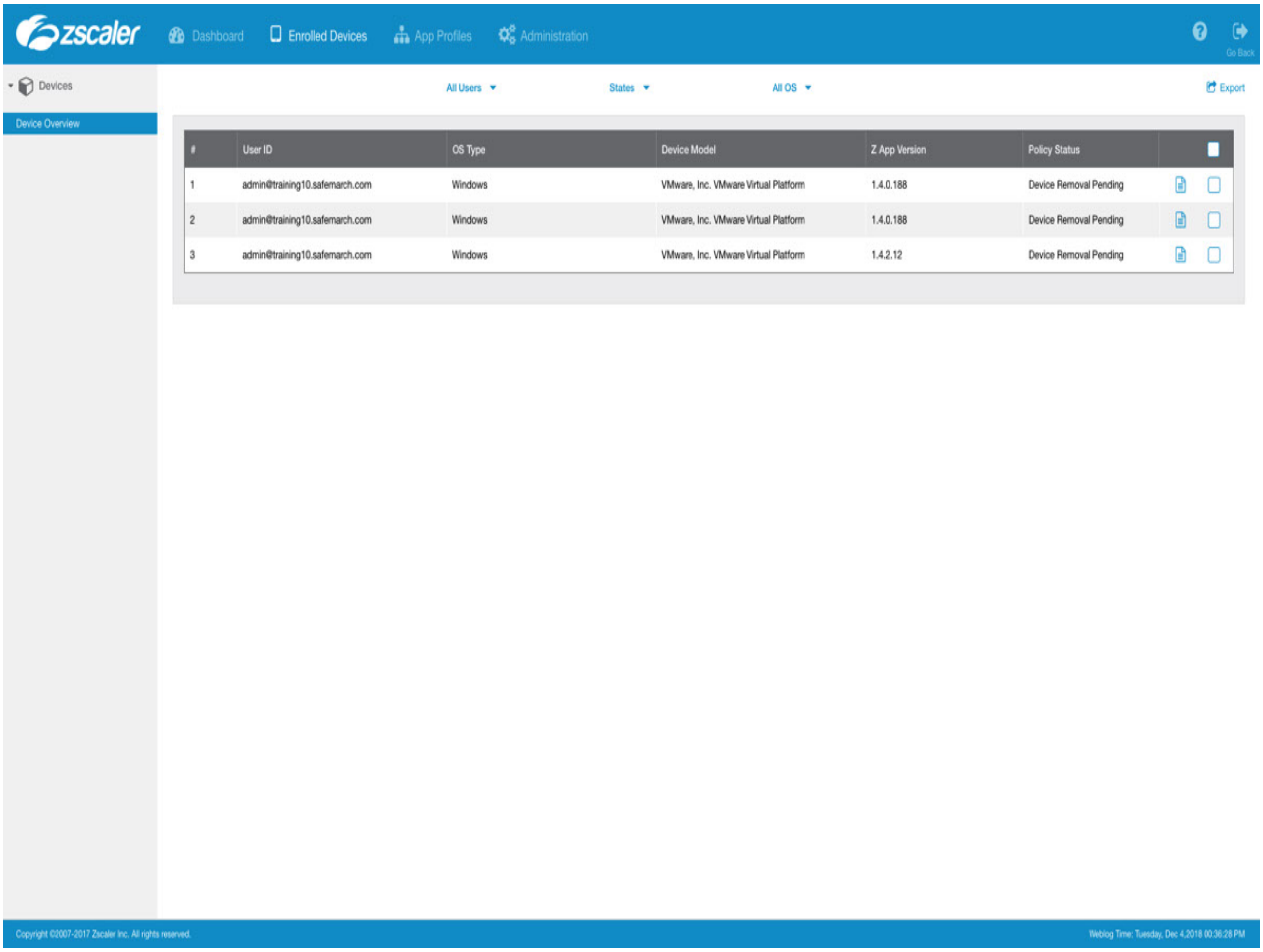
#	User ID	OS Type	Device Model	Z App Version	Policy Status		□
1	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.0.188	Device Removal Pending		□
2	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.0.188	Device Removal Pending		□
3	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.2.12	Device Removal Pending		□

Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Tuesday, Dec 4,2018 00:36:28 PM

Slide notes

Slide 47 - Slide 47



#	User ID	OS Type	Device Model	Z App Version	Policy Status		☐
1	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.0.188	Device Removal Pending		☐
2	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.0.188	Device Removal Pending		☐
3	admin@training10.safemarch.com	Windows	VMware, Inc. VMware Virtual Platform	1.4.2.12	Device Removal Pending		☐

Copyright ©2007-2017 Zscaler Inc. All rights reserved.

Weblog Time: Tuesday, Dec 4,2018 00:36:28 PM

Slide notes