


Slide 1 – Zscaler App: Best Practices for ZPA



The Zscaler App

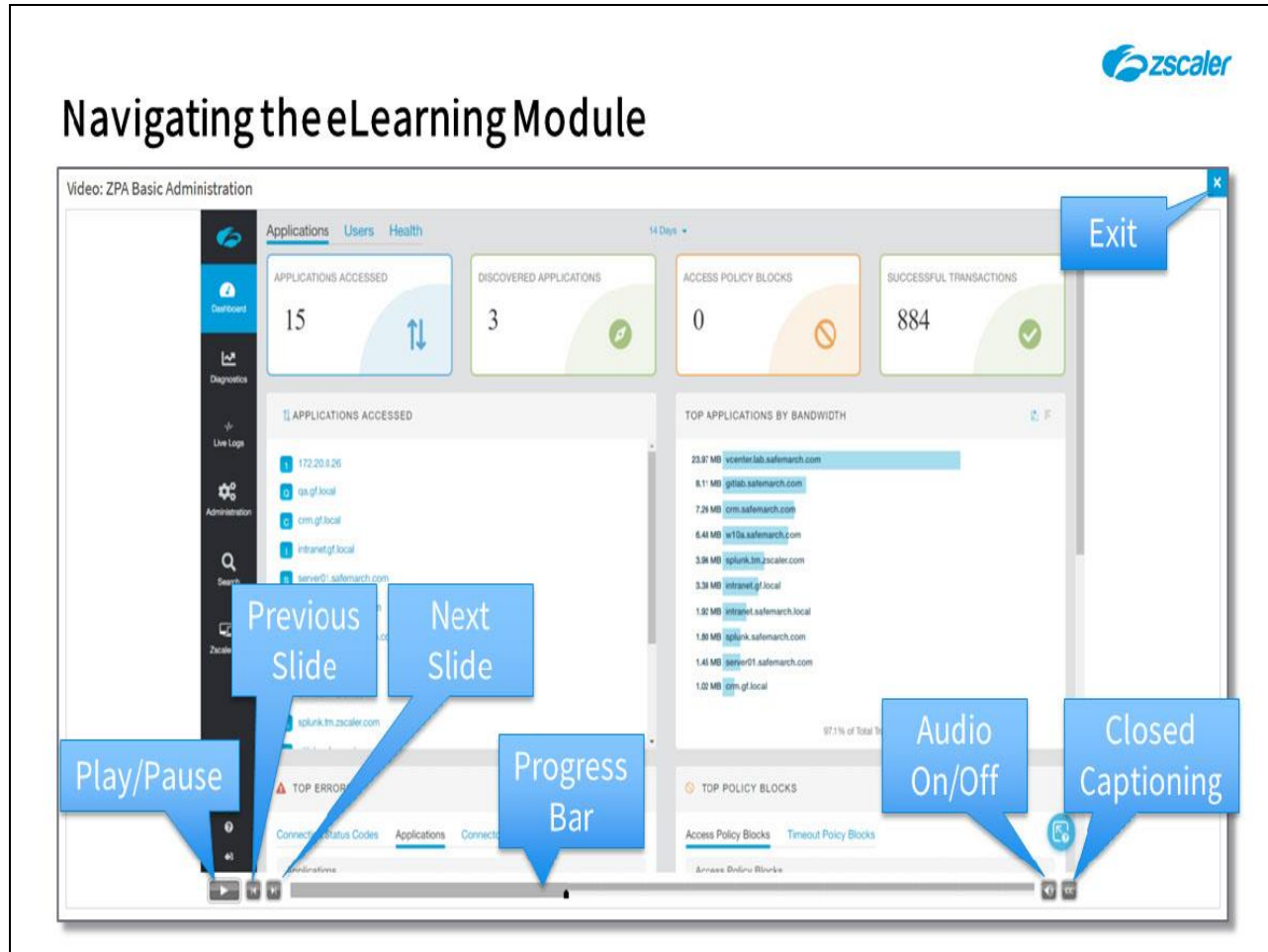
ZPA Best Practices

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module for a look some Zscaler App **Best Practices** for the ZPA service.

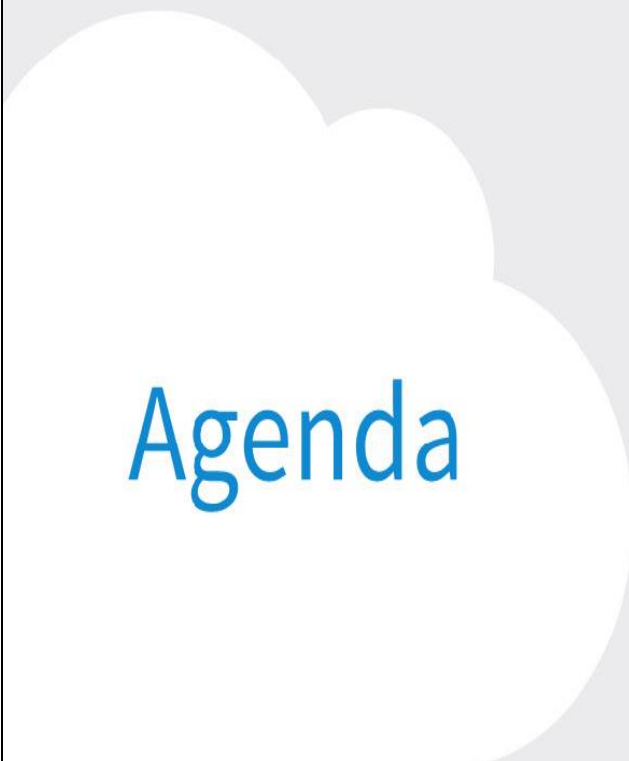

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous** and **Next** slide. You can also **Mute** the audio or enable **Closed Captioning** which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button at the top to exit.

Slide 3 - Agenda



Agenda

- Zscaler App Best Practices:
 - Deployment
 - Authentication
 - General Use

Slide notes

In this module, we will cover some Zscaler App **Best Practices**, in the areas of; Deployment, Authentication, and general usage guidelines.

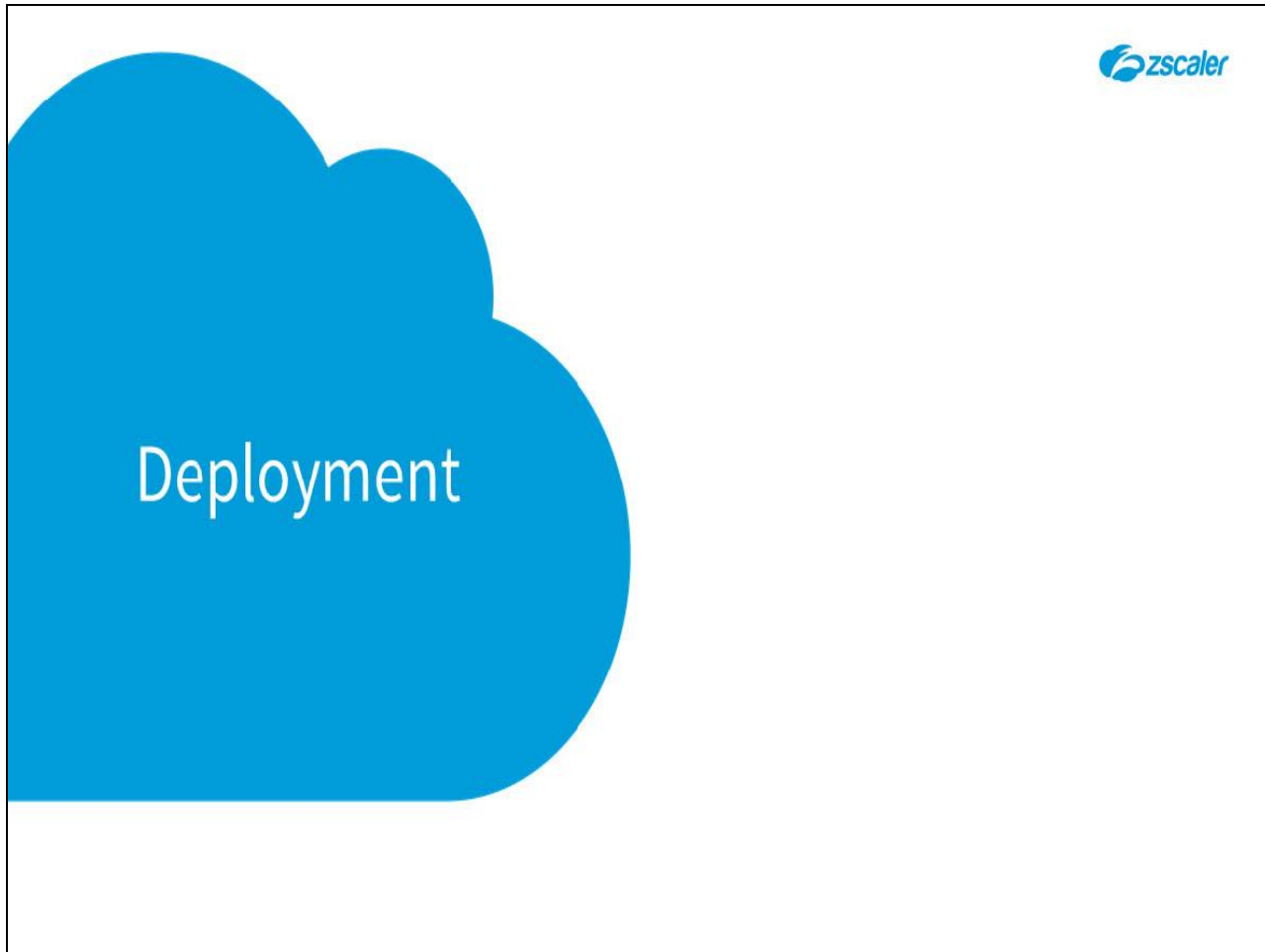
Slide 4 - Zscaler App Best Practices:



Slide notes

The first topic that we will cover is a look at some Zscaler App **Best Practices** when used to connect to the ZPA service.

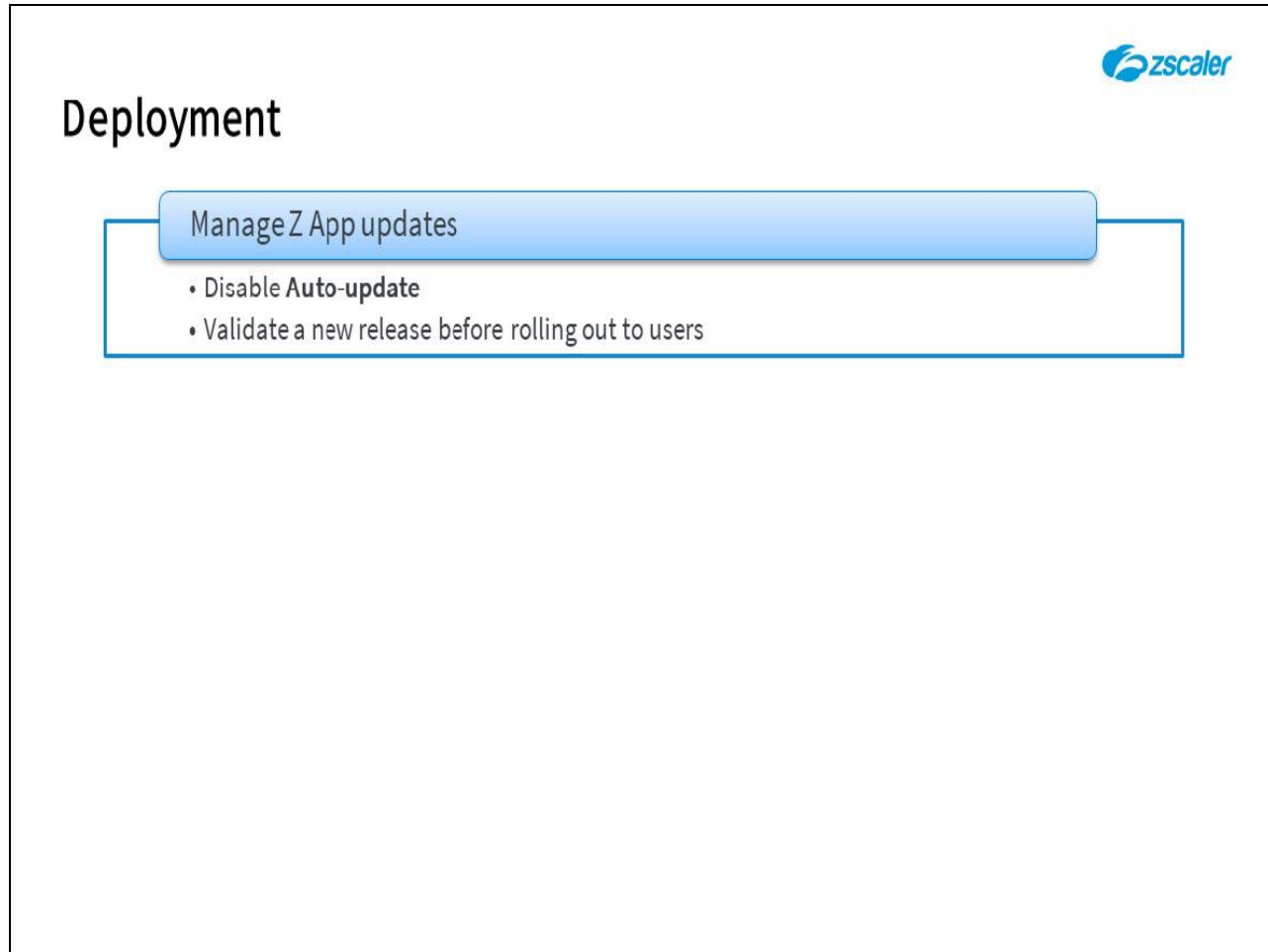
Slide 5 - Install



Slide notes

To start with, we'll look at some **Best Practices** for Z App deployment.

Slide 6 - Install



The slide is titled "Deployment" in a large, bold, black font. In the top right corner, there is a blue Zscaler logo. Below the title, there is a blue rounded rectangular box with the text "Manage Z App updates". To the right of this box, a blue line extends and then turns down to form a vertical line, which then turns left to form a horizontal line that encloses a list of two bullet points. The first bullet point is "• Disable Auto-update" and the second is "• Validate a new release before rolling out to users".

Deployment

Manage Z App updates


- Disable Auto-update
- Validate a new release before rolling out to users

Slide notes

First and foremost, you need to be sure to control exactly what version of the App gets installed to your end user's devices. Ideally, you would always like the latest version available, to be sure to have all the latest bug fixes and any new features. However, it is probably not a good idea to install the new version blindly. We would recommend that you turn off the automatic Z App updates and only ever deploy versions that are known to be good *in your environment*.

This may well mean that you need to test each new version of the App prior to pushing it to your installed end user base.

Slide 7 - Install




Deployment

- Manage Z App updates
 - Disable **Auto-update**
 - Validate a new release before rolling out to users
- Manage Z App Permissions, Processes and Firewall Rules
 - Use GPO if necessary to configure **Firewall Rules**

Slide notes

Be sure to review all the Z App requirements for the devices that you will be deploying it to, in terms of the **Permissions**, **Processes** and **Firewall Rules** required. If any of these are already under the control of some management system (e.g. AD GPO rules), be sure to update these rules to account for the Z App requirements.

Slide 8 - Install



Deployment

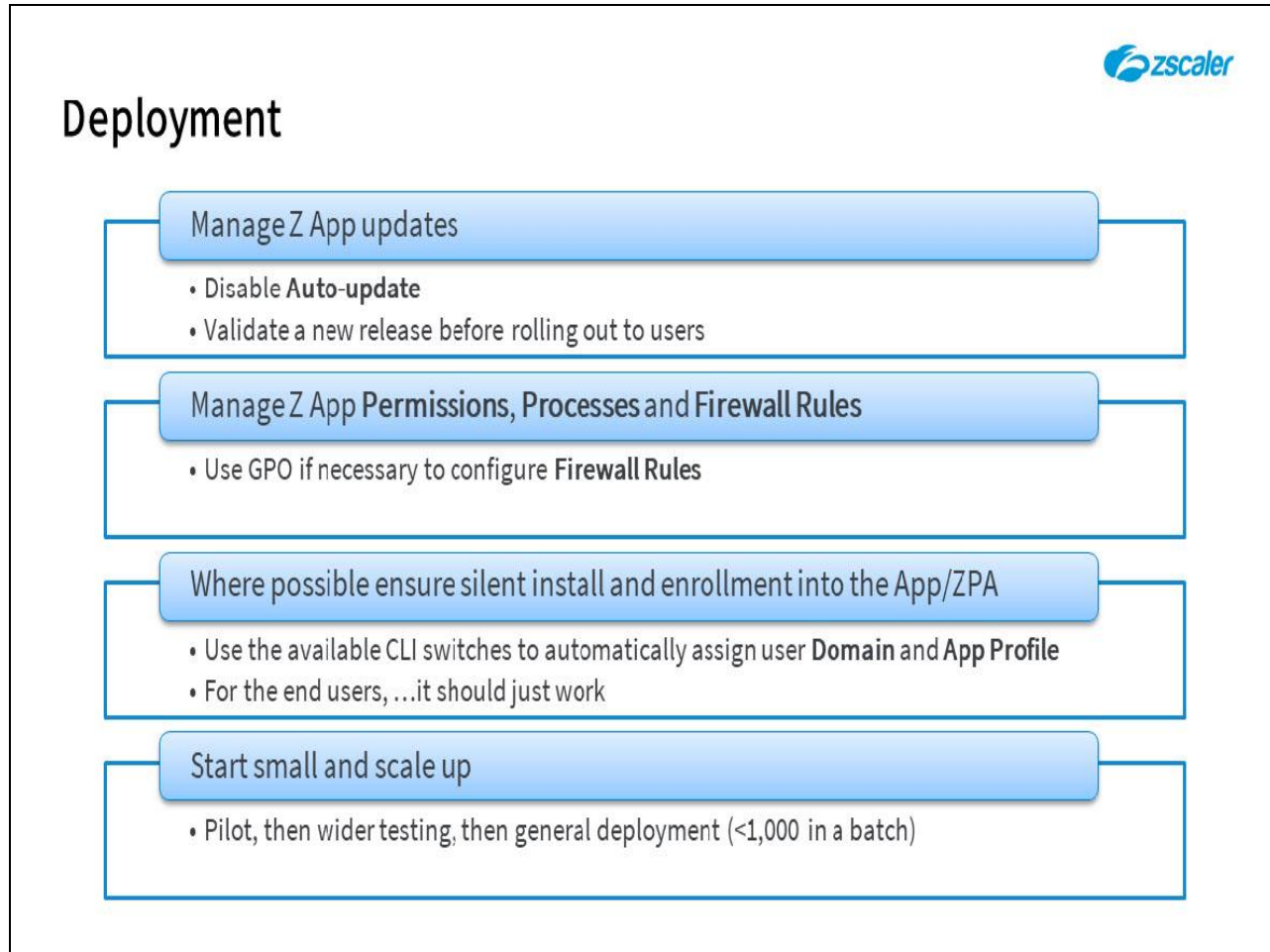
- Manage Z App updates
 - Disable **Auto-update**
 - Validate a new release before rolling out to users
- Manage Z App Permissions, Processes and Firewall Rules
 - Use GPO if necessary to configure **Firewall Rules**
- Where possible ensure silent install and enrollment into the App/ZPA
 - Use the available CLI switches to automatically assign user **Domain** and **App Profile**
 - For the end users, ...it should just work

Slide notes

Wherever possible, use the available command line switches when installing the App, such as **--userDomain** and **--policyToken**. This improves the end user enrollment experience as they will be immediately redirected to the appropriate SAML IdP. This also ties the Z App installation to your domain (so end users are unable to enter some other domain during enrollment) and automatically applies the appropriate **App Profile** (with all the correct App settings and the correct **Forwarding Profile** for the users).

Taking this a stage further, where possible configure a silent end user enrollment into the App and authentication into the ZPA service; from the end user perspective "it should just work". A silent enrollment and authentication for ZPA can often be achieved using the options available with your chosen SAML IdP.

Slide 9 - Install




Slide notes

Start your deployment small and scale up. Do a pilot deployment first, targeting a small group of ideally tech-savvy users. Once you have confirmed the configurations and methods you require, you can then start to do a wider deployment.

We would recommend that you enroll **no more than 1,000** Z App end users at a time.

Slide 10 - Install



Deployment


Use the .EXE installer during local testing

- To avoid SCCM/GPO version mismatches

Slide notes

When testing on a local machine, use the **.EXE** installer for preference. This will avoid any potential clashes with a SCCM or GPO pushed installer.

Slide 11 - Install



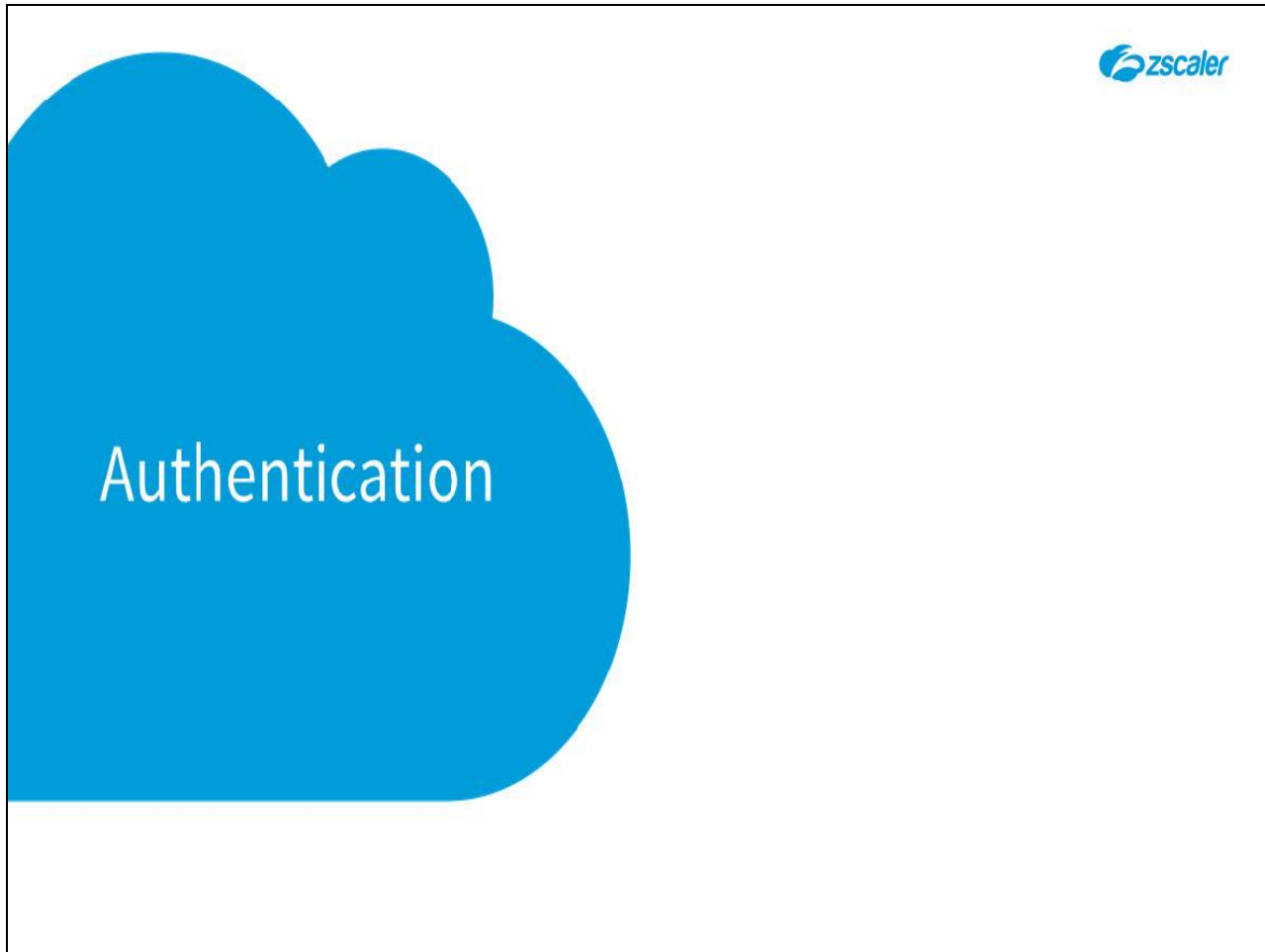
Deployment

- Use the .EXE installer during local testing
 - To avoid SCCM/GPO version mismatches
- Set Device Threshold to 8
 - Reduce the number of devices a single end user can enroll the App onto
 - Use the Device Cleanup option to enforce the limit

Slide notes

Set the **Device Threshold** to **8** and ensure it is enforced through the **Device Cleanup** configuration. This will ensure that users cannot install and enroll Z App on more than specified number of devices.


Slide 12 - Authentication



Slide notes

Now let's talk about some Authentication best practices.

Slide 13 - Authentication



Authentication

SAML is required for user authentication into the ZPA service


- Map the user email domains to the correct IdP

Slide notes

For the ZPA service, SAML authentication is required. Depending on your chosen IdP, you may also be able to use advanced authentication options (silent authentication, certificate-based authentication, or multi-factor authentication (MFA)).

You will need to map the necessary end user email domains to the appropriate SAML IdPs to ensure redirection to the correct IdP for ZPA authentication.

Slide 14 - Authentication




Authentication

- SAML is required for user authentication into the ZPA service
 - Map the user email domains to the correct IdP
- If required - Configure MFA on the SAML IdP
 - Be sure to test it

Slide notes

Configure and test MFA on your IdP, preferably before deploying Z App. Make sure this works prior to authenticating Z App users.

Slide 15 - Authentication



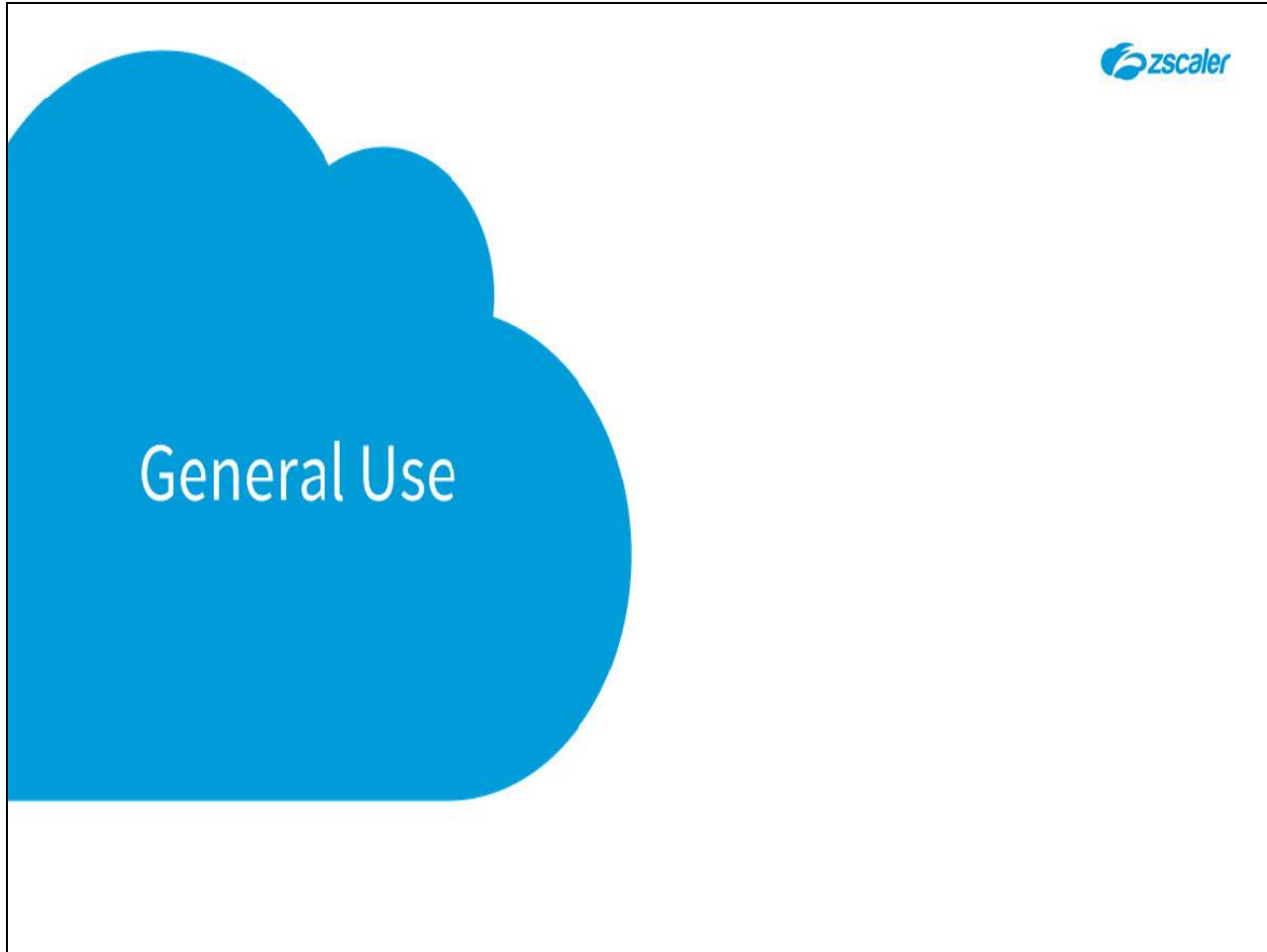
Authentication

- SAML is required for user authentication into the ZPA service
 - Map the user email domains to the correct IdP
- If required - Configure MFA on the SAML IdP
 - Be sure to test it
- Provisioning
 - Azure, Okta, PingOne - use SCIM for dynamic user attribute updates (limited scope)

Slide notes

For the dynamic update of end user attributes, you can use **Azure AD**, **Okta** or **PingOne** with a **SCIM** configuration. You will need to limit the scope of the attributes updated using **SCIM**, to avoid unnecessary synchronization traffic.


Slide 16 - General Use



Slide notes

Finally some general Z App best practices.

Slide 17 - General



General


Test application responses thoroughly before general roll-out

- Make sure it works for all required applications

Slide notes

Test access to all required applications through the ZPA service prior to a general roll-out. Make sure you can reach all the applications that you know your end users will need!

Slide 18 - General




General

- Test application responses thoroughly before general roll-out
 - Make sure it works for all required applications
- Use **Packet Filter Based** driver on Windows
 - For better performance, enforcement, interoperability, network functionality

Slide notes

Use the **Packet Filter Based** driver for the Windows platform, for better performance, enforcement, interoperability and network functionality.

Slide 19 - General




General

- Test application responses thoroughly before general roll-out
 - Make sure it works for all required applications
- Use **Packet Filter Based** driver on Windows
 - For better performance, enforcement, interoperability, network functionality
- Use the **Host Name > IP Address** matching for **Trusted Networks**
 - Other methods can be suspect

Slide notes

When configuring **Trusted Networks** in the Zscaler App Portal, use the **Host Name to IP Address** matching criteria for preference, as this can be a more reliable method of identifying the network.

Slide 20 - General



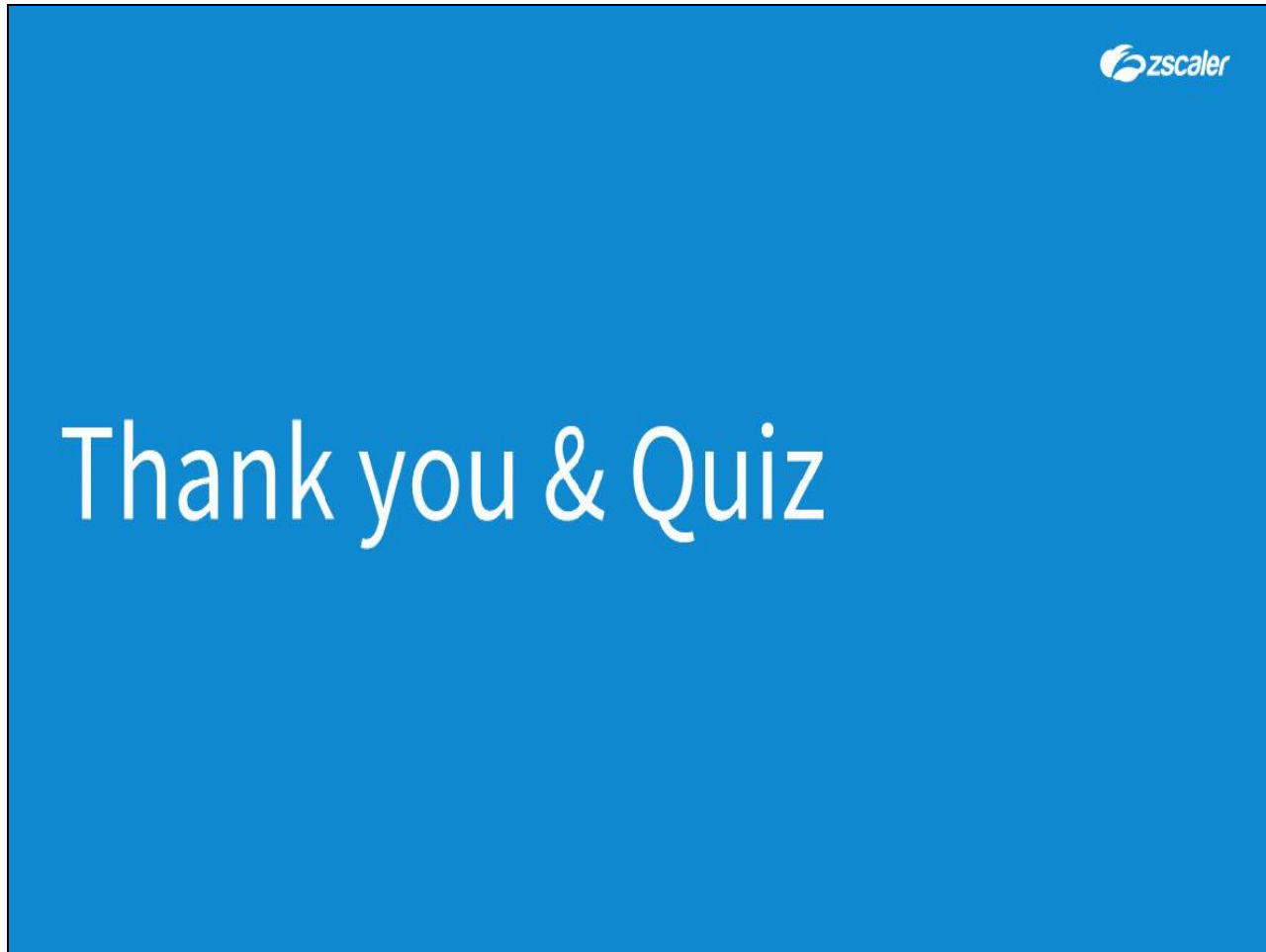
General

- Test application responses thoroughly before general roll-out
 - Make sure it works for all required applications
- Use Packet Filter Based driver on Windows
 - For better performance, enforcement, interoperability, network functionality
- Use the Host Name > IP Address matching for Trusted Networks
 - Other methods can be suspect
- Keep End User Control to a minimum
 - No user access to: **Logging, Support Access, Restart and Repair**
 - To minimize end user influence over the App environment

Slide notes

Try to keep end user controls within the App to a minimum, to avoid any opportunity for them to 'tinker' with the settings. You can hide the logging controls, disable support access in the App and prevent the end user from restarting or repairing the services.

Slide 21 - 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.