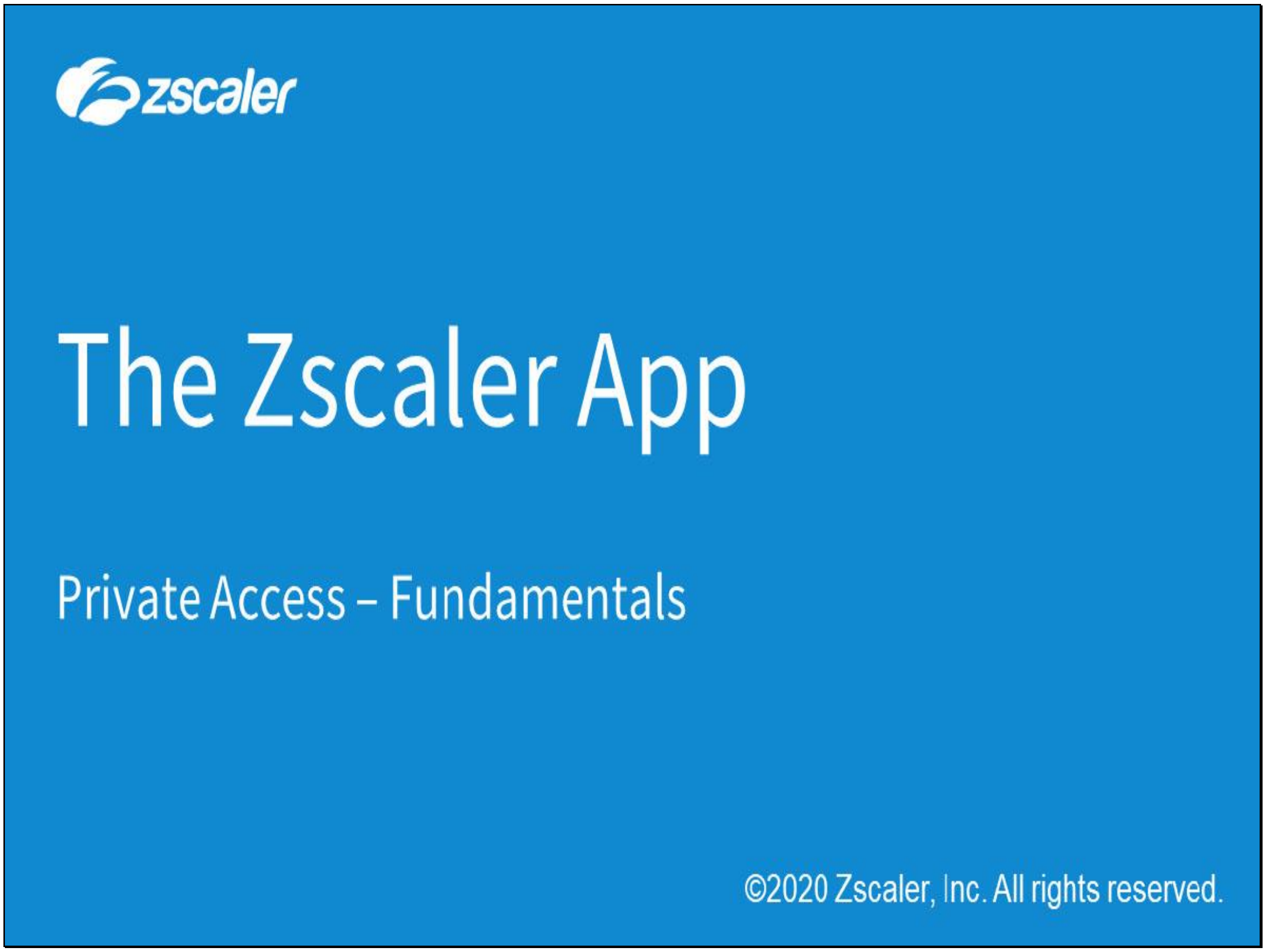
Slide 1 – The Zscaler App: Private Access Fundamentals



zscaler

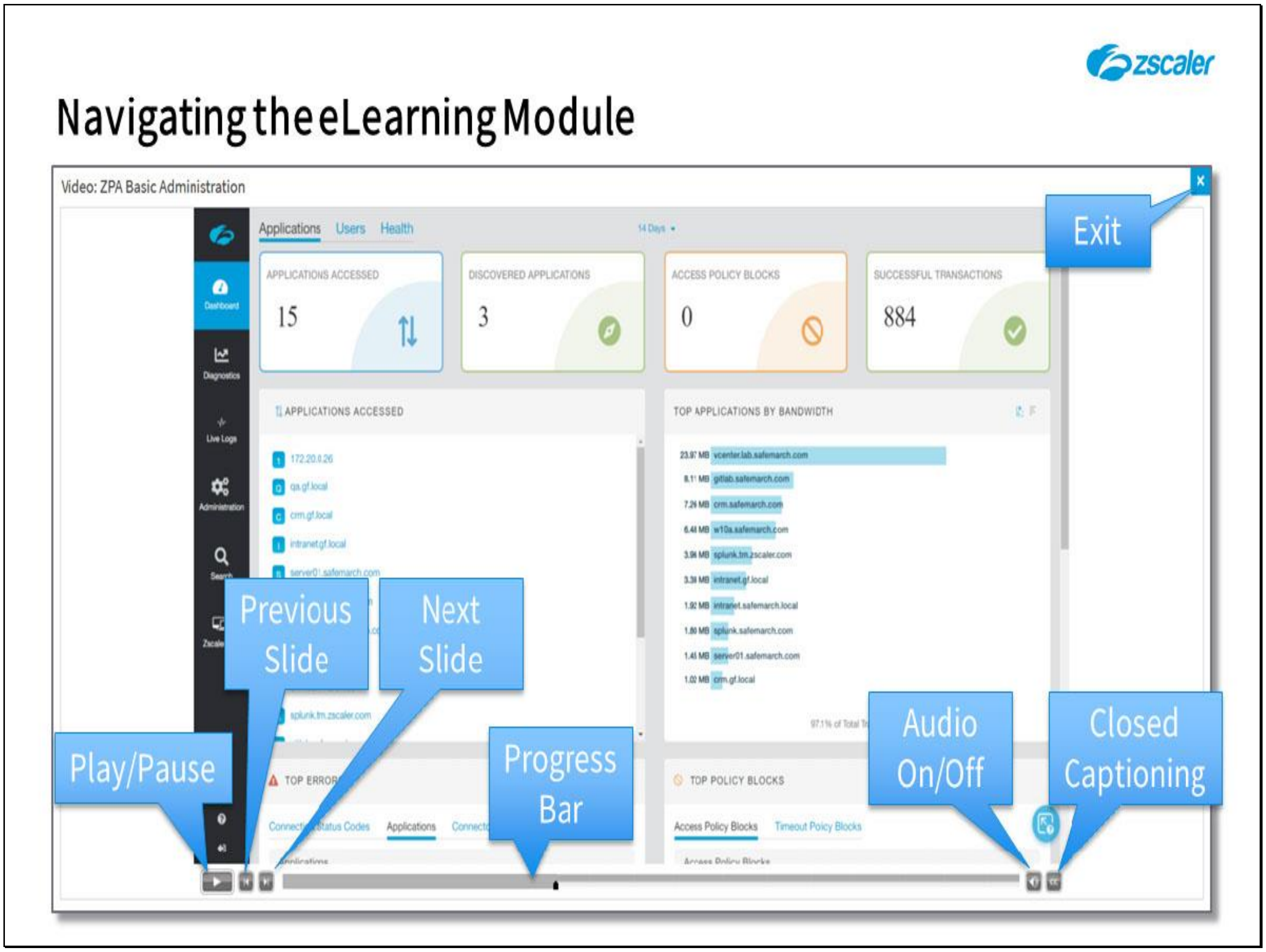
The Zscaler App

Private Access – Fundamentals

Slide notes

Welcome to this training module on the Zscaler App Private Access fundamentals.

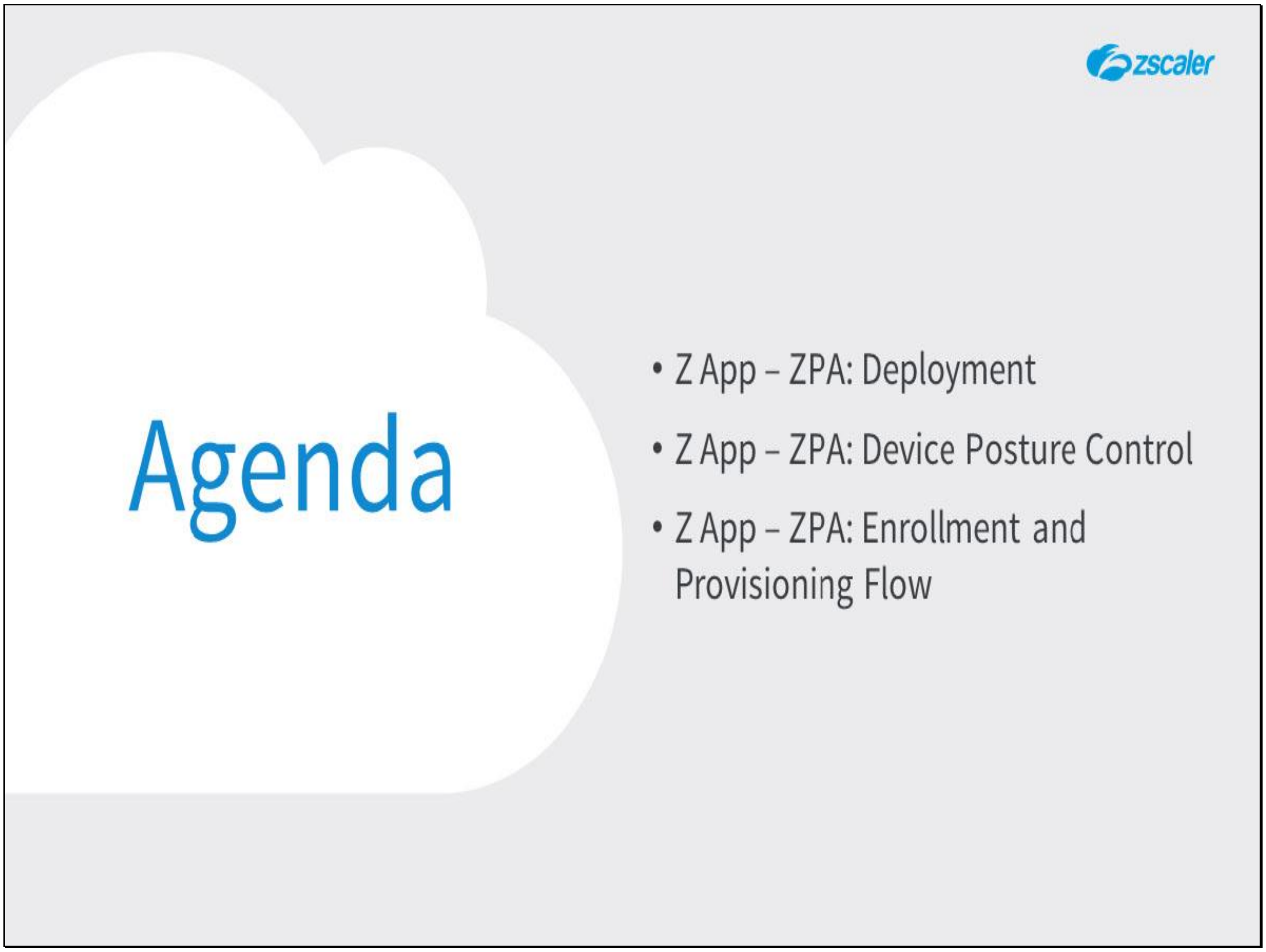
Slide 2 - Navigating the eLearning Module



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



zscaler

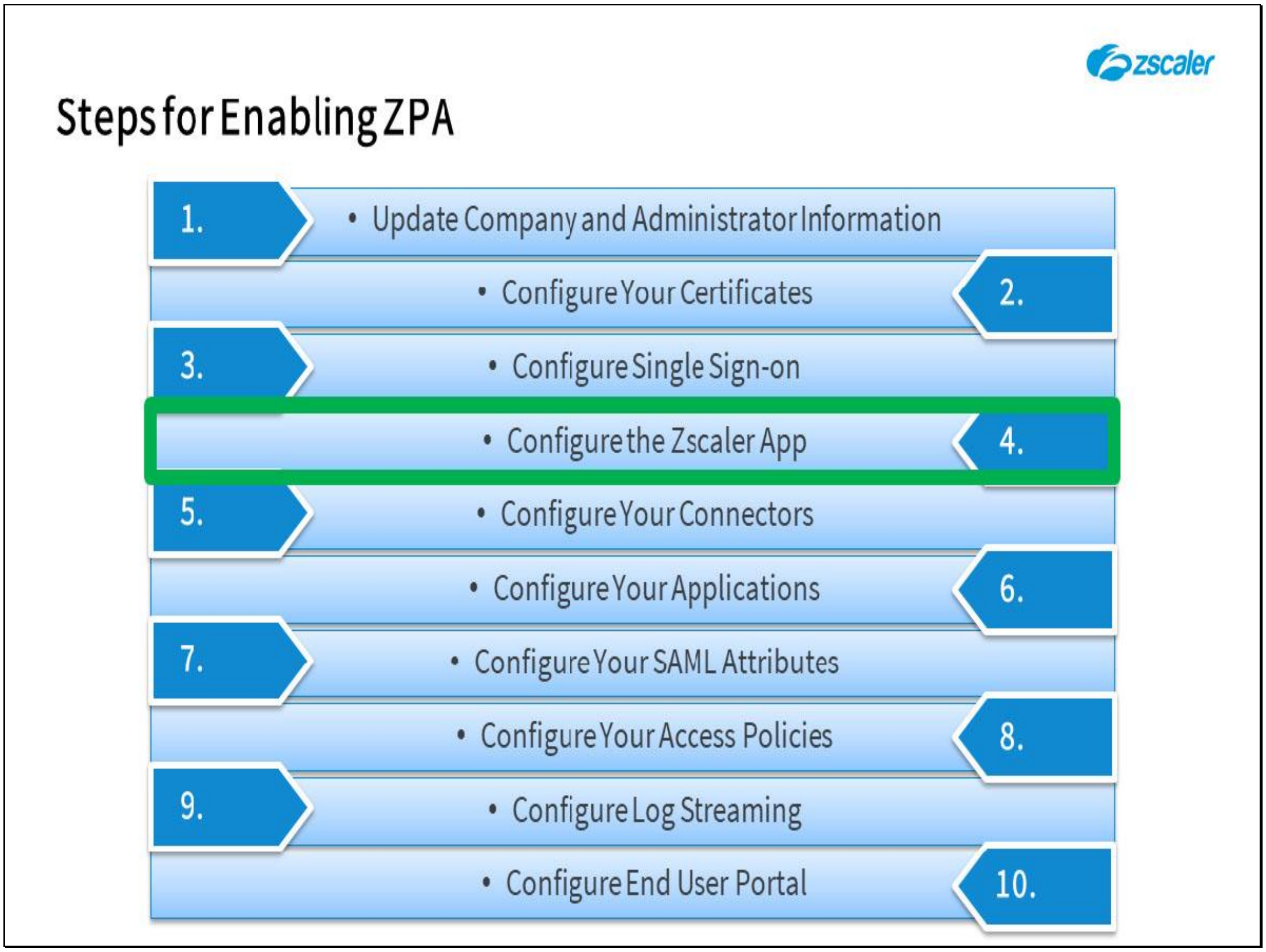
Agenda

- Z App – ZPA: Deployment
- Z App – ZPA: Device Posture Control
- Z App – ZPA: Enrollment and Provisioning Flow

Slide notes

In this module we will cover the following topics: The Zscaler App for Private Access deployment process; the methods available for verifying device posture; and the Zscaler App enrollment and provisioning flow for Private Access.

Slide 4 - Steps for Enabling ZPA



Steps for Enabling ZPA

1. • Update Company and Administrator Information
2. • Configure Your Certificates
3. • Configure Single Sign-on
4. • Configure the Zscaler App
5. • Configure Your Connectors
6. • Configure Your Applications
7. • Configure Your SAML Attributes
8. • Configure Your Access Policies
9. • Configure Log Streaming
10. • Configure End User Portal

Slide notes

Just as a reminder, this is where we are in the steps for enabling ZPA.

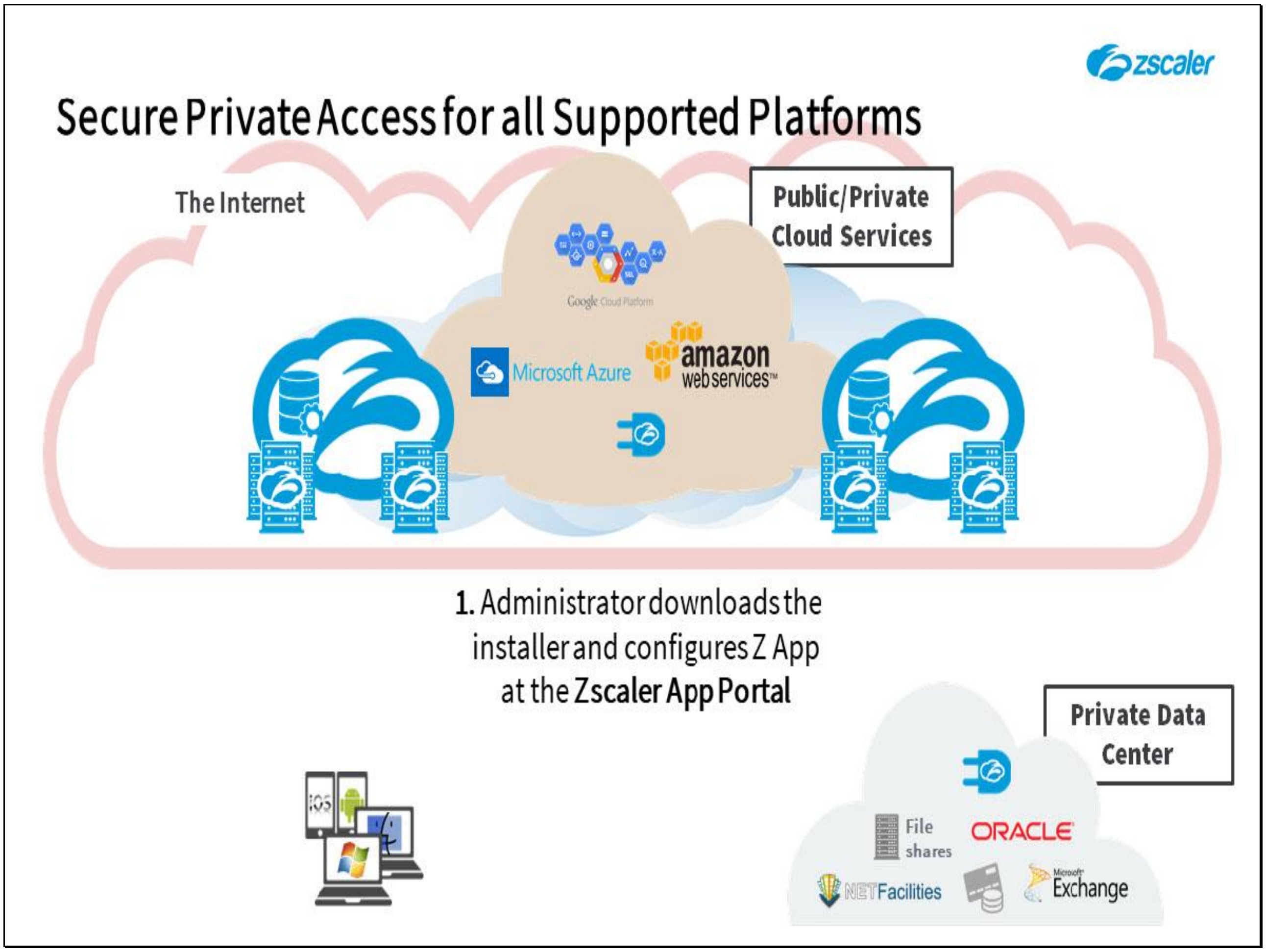
Slide 5 - Zscaler App for ZPA – Architecture

Z App – ZPA: Deployment

Slide notes

The first topic that we will cover is a look at the Zscaler App deployment process for the ZPA service.

Slide 6 - Secure Private Access for all Supported Platforms



Secure Private Access for all Supported Platforms

1. Administrator downloads the installer and configures Z App at the **Zscaler App Portal**

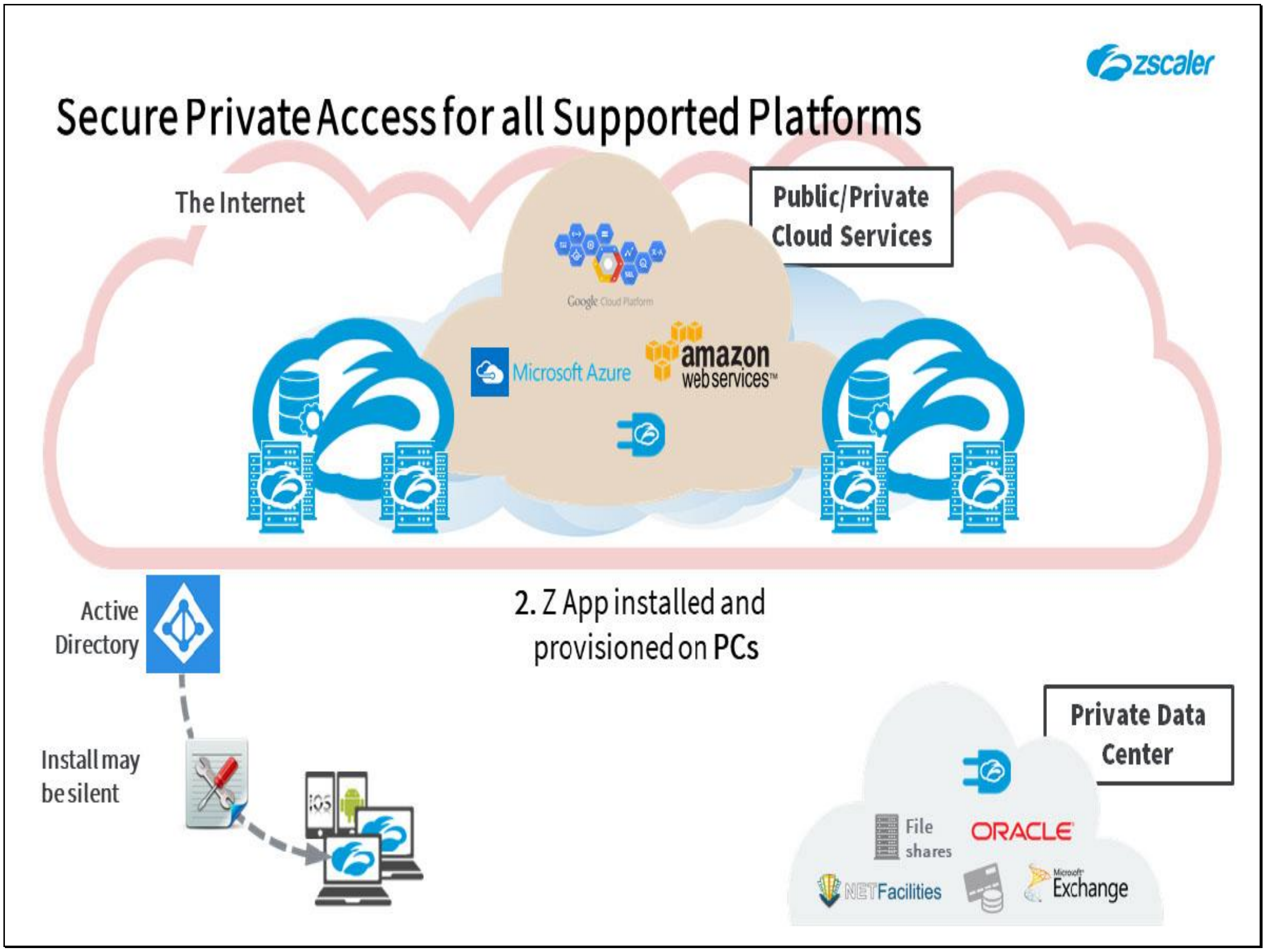
Slide notes

There are a number of steps to enabling secure access to private applications for your road warriors using the Zscaler App, as follows:

Step 1: An administrator must download the appropriate PC installation file for distribution and must configure appropriate App settings for the groups that will be using the App. For the ZPA service these include:

- **App Profile** and **Forwarding Profile** settings;
- **Notification** and **Support** settings;
- **Trusted Network** settings;
- **Zscaler Service Entitlement** and **User Agent** settings;
- And per-platform **Device Posture** configurations.

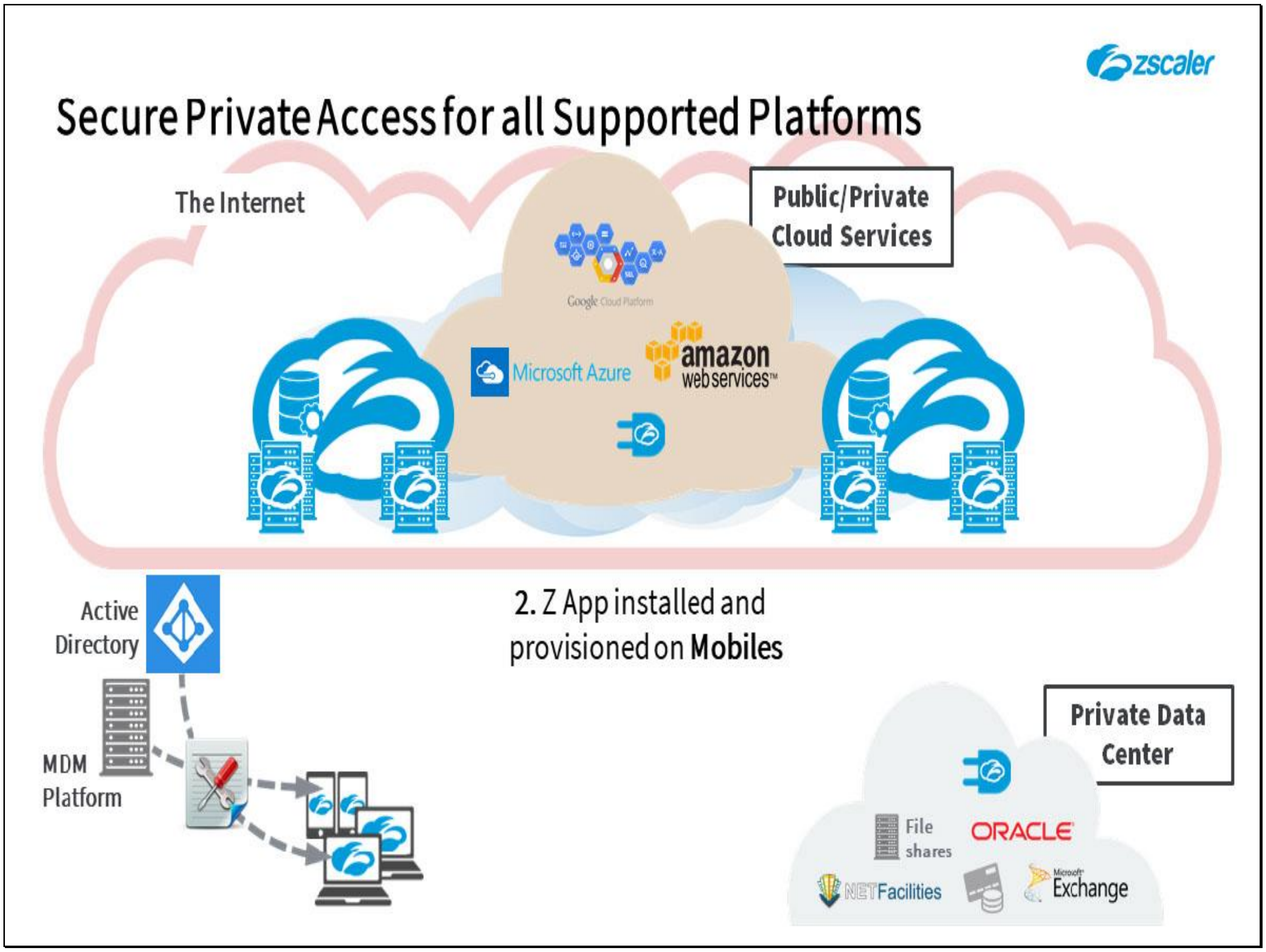
Slide 7 - Secure Private Access for all Supported Platforms



Slide notes

Step 2: The app must be distributed to the users that require it. For Windows users this can be done using an AD Group Policy Object (GPO) or Microsoft Intune, for Macs it can be done using Casper Suite or Tanium, or of course it can be installed manually. The install of the App can also be made silent, so the user is not aware that it is happening.

Slide 8 - Secure Private Access for all Supported Platforms



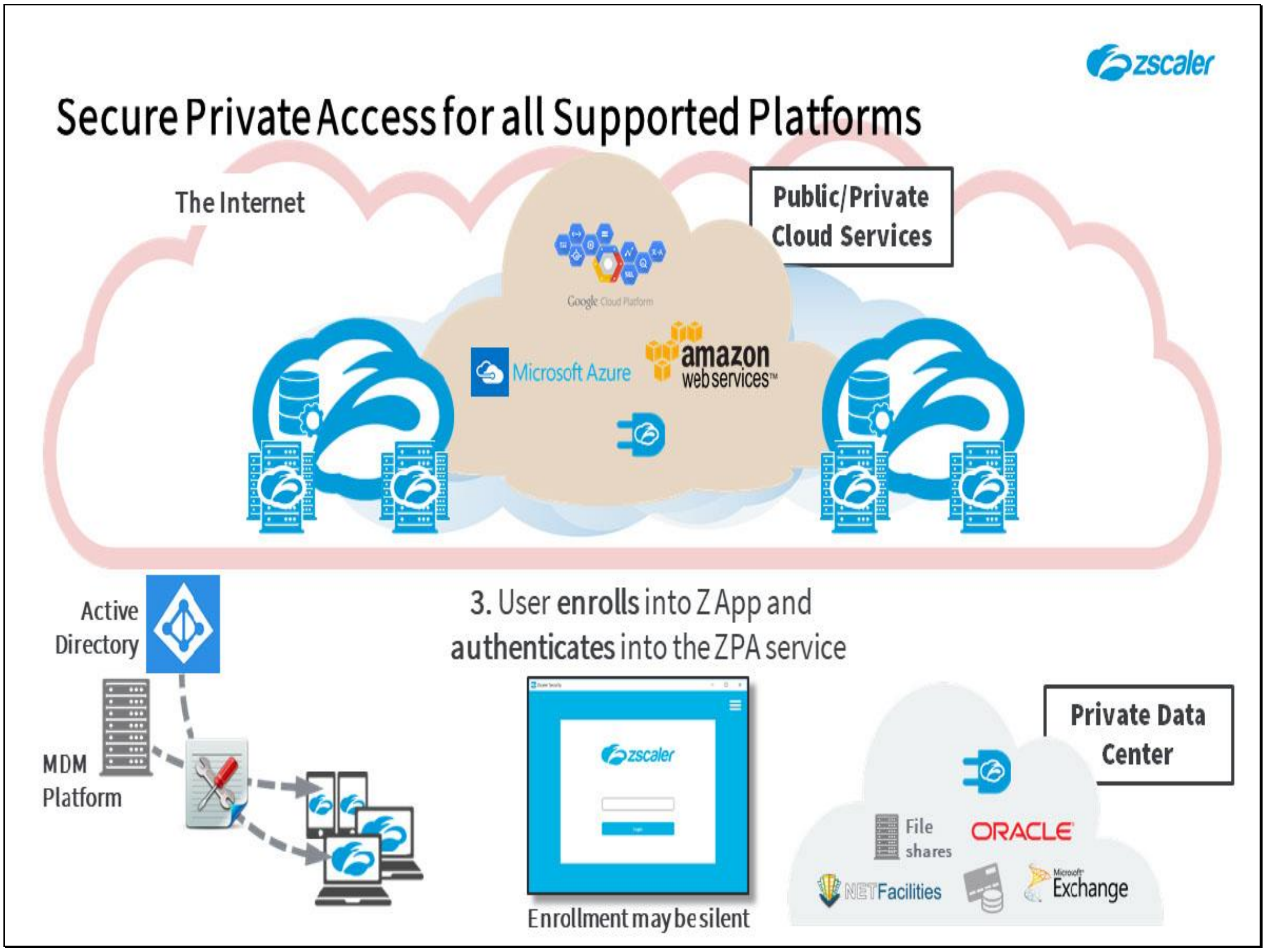
Secure Private Access for all Supported Platforms

2. Z App installed and provisioned on **Mobiles**

Slide notes

For Mobile devices, the installer is available on the public App Stores for your users to install themselves, or you can distribute it as a managed App using your preferred Mobile Device Management (MDM) platform, such as VMware's Workspace ONE (previously known as AirWatch), MobileIron, or Microsoft Intune. If you push the App from an MDM manager, you have more control over how it is installed and configured on the end user's device.

Slide 9 - Secure Private Access for all Supported Platforms

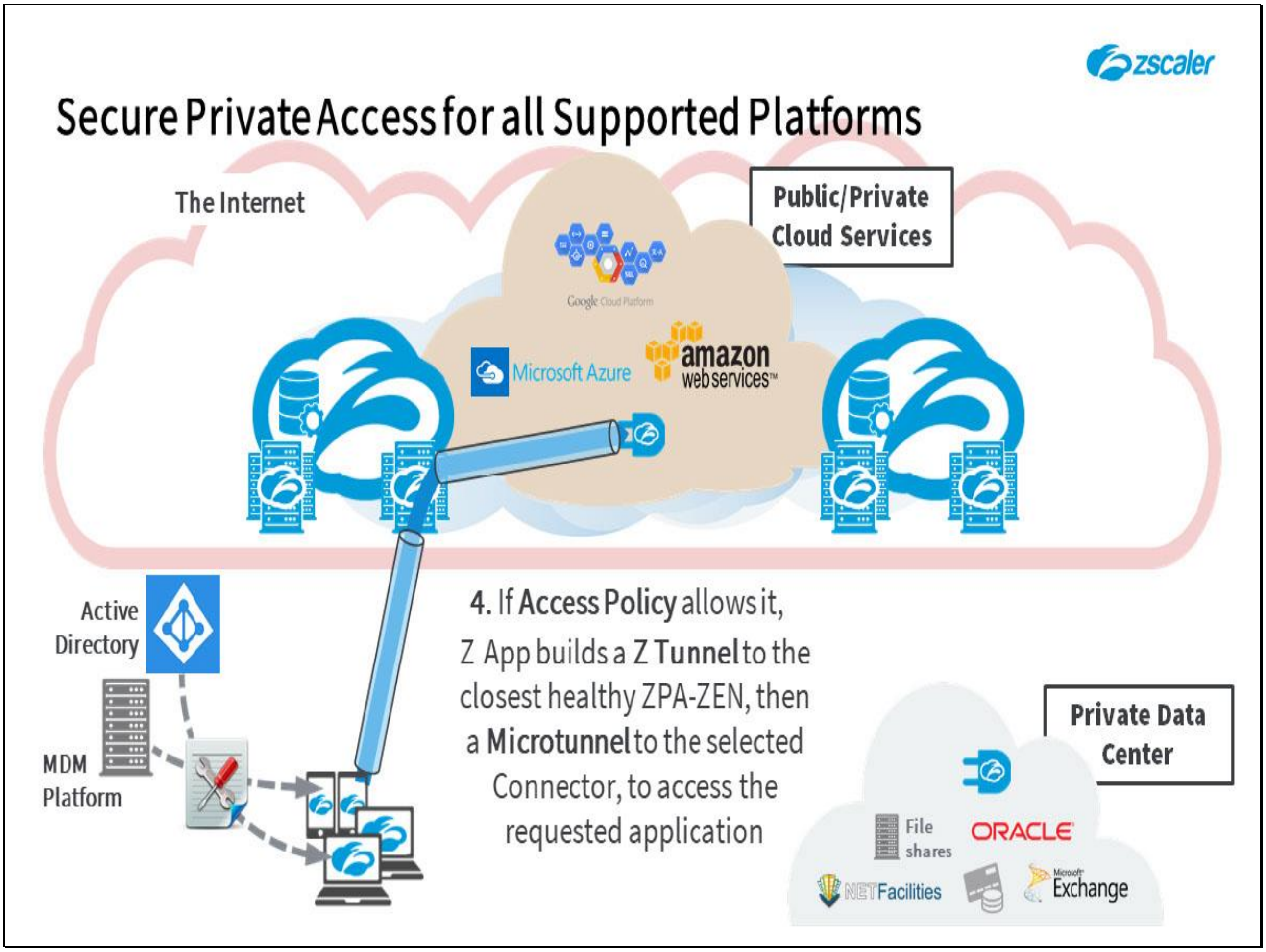


Slide notes

Step 3: After installation, the device user is prompted to enroll through the app; currently this is a one-time enrollment process using SAML. The end user will also be authenticated to the ZPA service at the same time and will be prompted to re-authenticate periodically (based on the ZPA **Timeout Policy** settings).

If the App is also to be used for Internet security with the ZIA service, we recommend that you use the same SAML IdP for App enrollment to avoid the end user having to login twice. It is also possible to enroll the user silently based on the user's device login, although this also requires SSO support on the chosen SAML IdP.

Slide 10 - Secure Private Access for all Supported Platforms



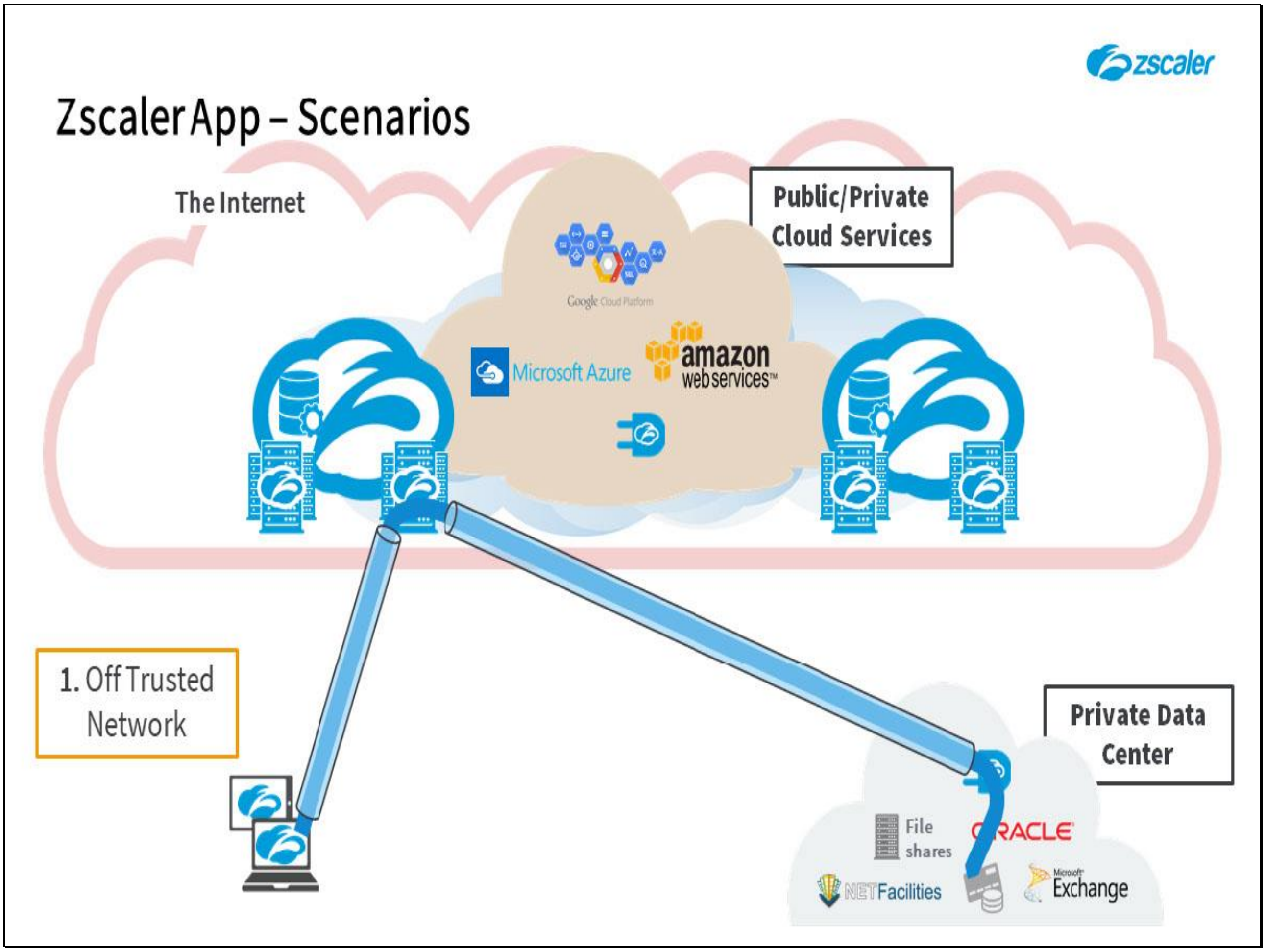
Secure Private Access for all Supported Platforms

4. If Access Policy allows it, Z App builds a Z Tunnel to the closest healthy ZPA-ZEN, then a Microtunnel to the selected Connector, to access the requested application

Slide notes

Step 4: After a successful enrollment, if used for accessing applications with the ZPA service, the App will establish an encrypted **Z Tunnel** to the closest healthy ZPA-ZEN when the user requests an application (if this is allowed by the **Access Policy**). Subsequently, an end-to-end **Microtunnel** will be put in place through the nominated App Connecter, that provides a data path for the end user to reach the application.

Slide 11 - Zscaler App – Scenarios



Zscaler App – Scenarios

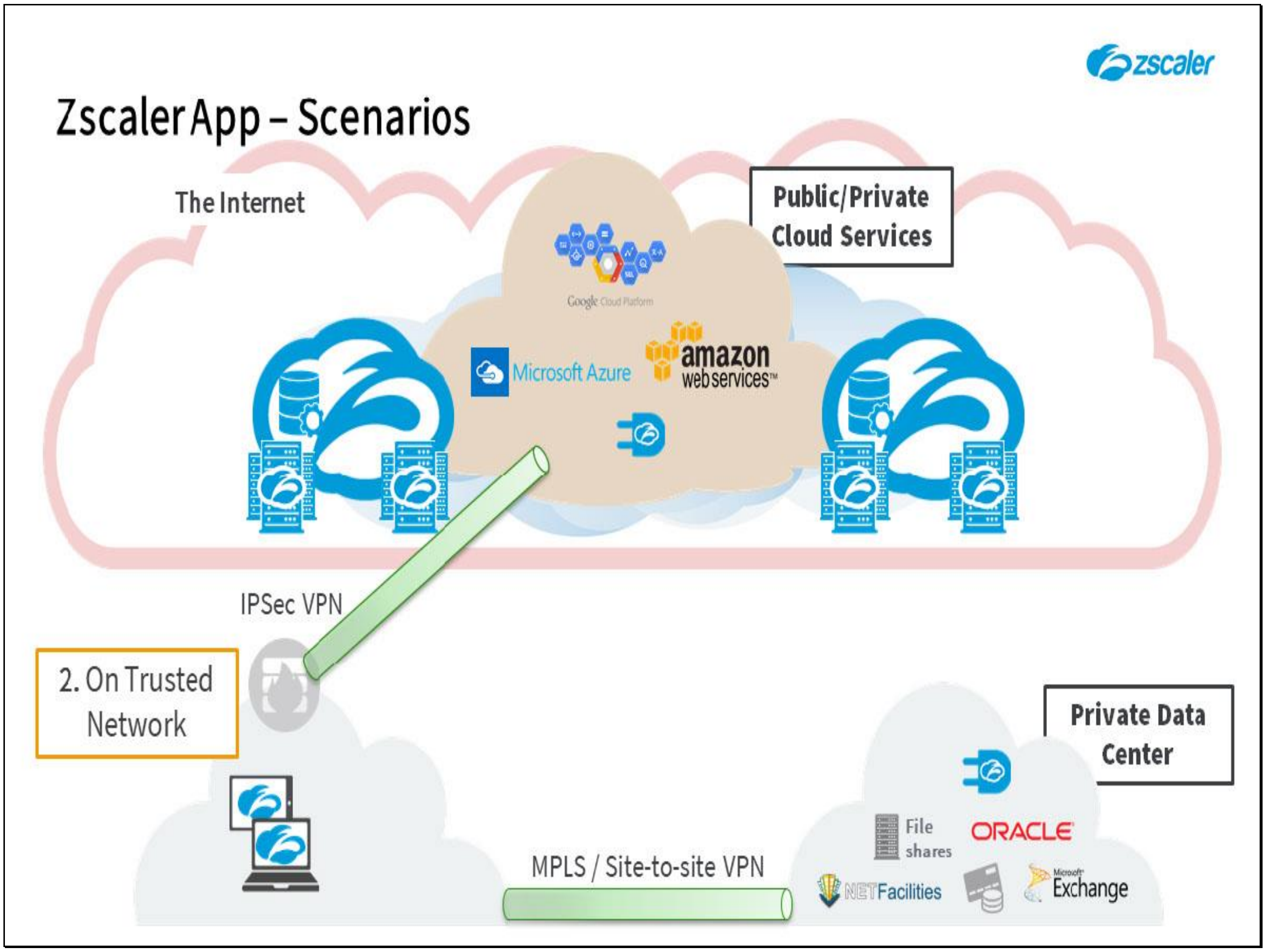
Slide notes

There are three primary forwarding scenarios for the Zscaler App:

1. And the first of these is the classic Road Warrior scenario, where an employee is connecting from outside any of your locations and is therefore not on a trusted network.

   It is for precisely this situation that the Zscaler App was developed, and it provides a secure channel through the ZPA Cloud to allow your Road Warrior's to connect to the private applications that they need. Enabling ZPA tunneling when users are **Off Trusted Network** allows the use of ZPA as a VPN replacement solution for remote access.

Slide 12 - Zscaler App – Scenarios

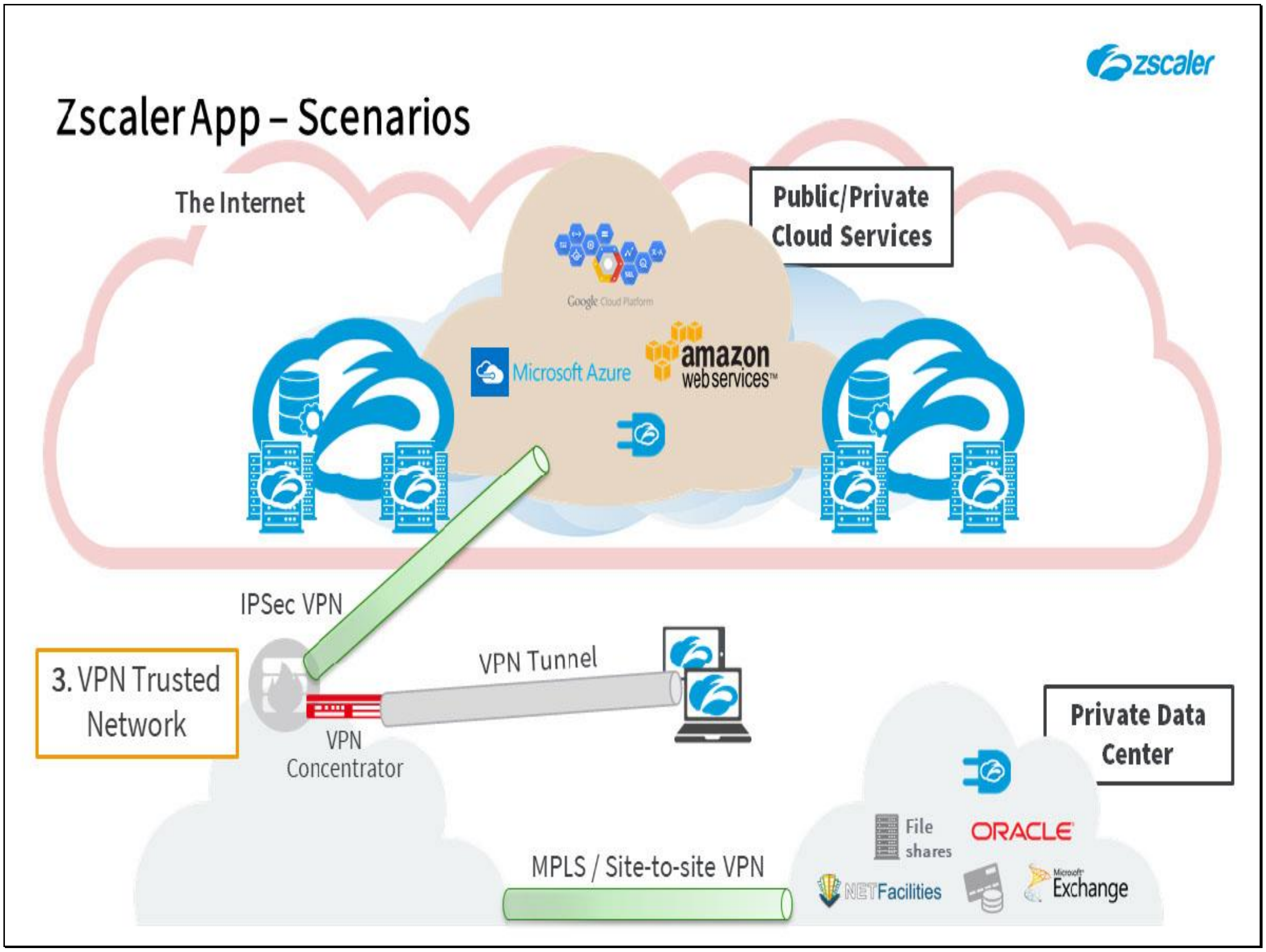


Slide notes

2. But what happens when your Road Warriors return to the office? If they connect to a trusted network at a location that has secure connectivity to the private applications anyway, is there any need for the app to tunnel traffic through Zscaler? Although, enabling ZPA tunneling when users are **On Trusted Network**, allows the use of ZPA to offload access to cloud-based applications which can help to reduce bandwidth consumption on the dedicated connections between your datacenter and the cloud applications.

   In addition, using ZPA tunneling for all applications (both datacenter hosted, and private cloud hosted) allows enterprises to shift user endpoints out of the corporate network even when on-premise, leveraging ZPA as a Software-Defined Perimeter solution (SDP) for complete access control and visibility

Slide 13 - Zscaler App – Scenarios



Zscaler App – Scenarios

Slide notes

3. The third main scenario is when a Road Warrior who is out of the office, chooses to establish a VPN connection to a trusted network. There are two main options here:
    - Full-tunnel VPN, where the VPN is established for all traffic;
    - Or split-tunnel VPN, where the VPN is established only for specific traffic.

   Note that ZPA is intended to replace the need for VPN and co-existence can take careful configuration of the two services to avoid conflicts. Zscaler best practice is to disconnect any VPN tunnels when ZPA is active.

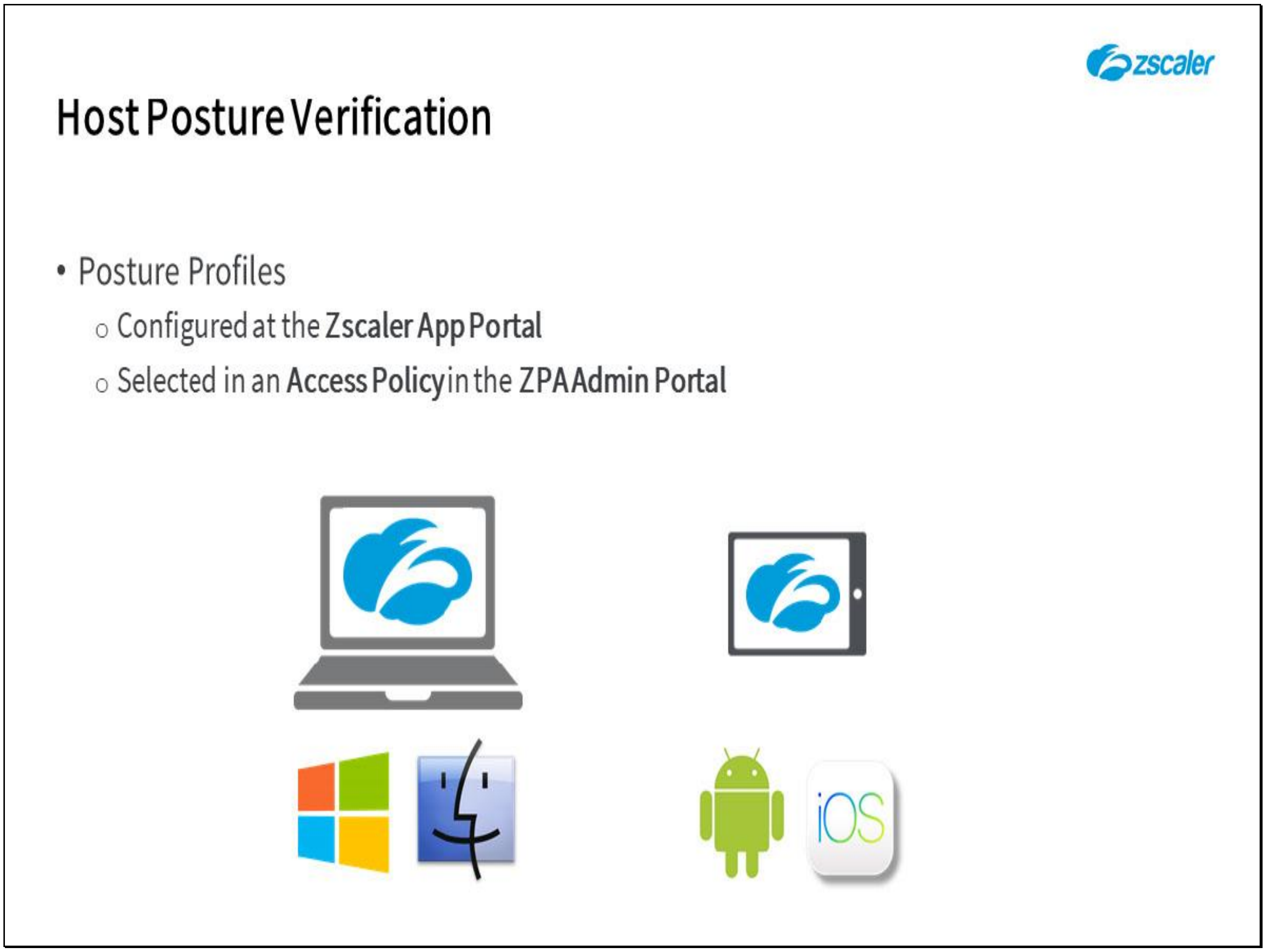
Slide 14 - Zscaler App for ZPA – Device Posture Control

Z App – ZPA: Device Posture Control

Slide notes

In the next section, we will look at the available Posture Profiles for end user devices.

Slide 15 - Host Posture Verification



Host Posture Verification

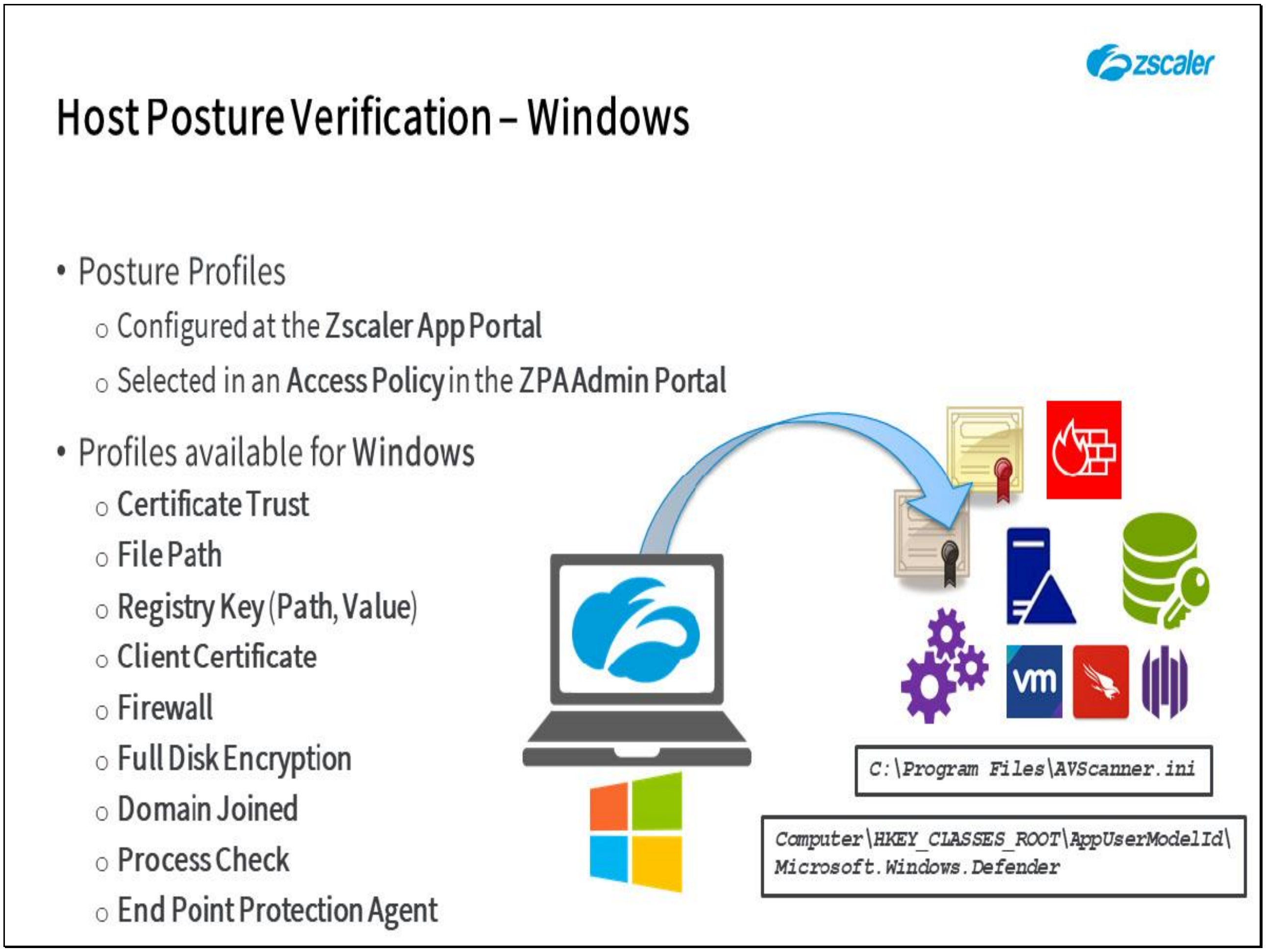
- Posture Profiles
  - Configured at the **Zscaler App Portal**
  - Selected in an **Access Policy** in the **ZPA Admin Portal**

zscaler
iOS

Slide notes

A device **Posture Profile** is a set of criteria that a user’s device must meet in order for it to be permitted to access applications with ZPA. Per platform **Posture Profiles** must be added and configured in the Zscaler App Portal to make them available for your access policies. Once they are available, you have the option to select one or more device **Posture Profile** when configuring access policies in the ZPA Admin Portal.

Slide 16 - Host Posture Verification – Windows



Host Posture Verification – Windows

- Posture Profiles
  - Configured at the **Zscaler App Portal**
  - Selected in an **Access Policy** in the **ZPA Admin Portal**
- Profiles available for **Windows**
  - **Certificate Trust**
  - **File Path**
  - **Registry Key** (Path, Value)
  - **Client Certificate**
  - **Firewall**
  - **Full Disk Encryption**
  - **Domain Joined**
  - **Process Check**
  - **End Point Protection Agent**

```
C:\Program Files\AVScanner.ini
```

```
Computer\HKEY_CLASSES_ROOT\AppUserModelId\
Microsoft.Windows.Defender
```

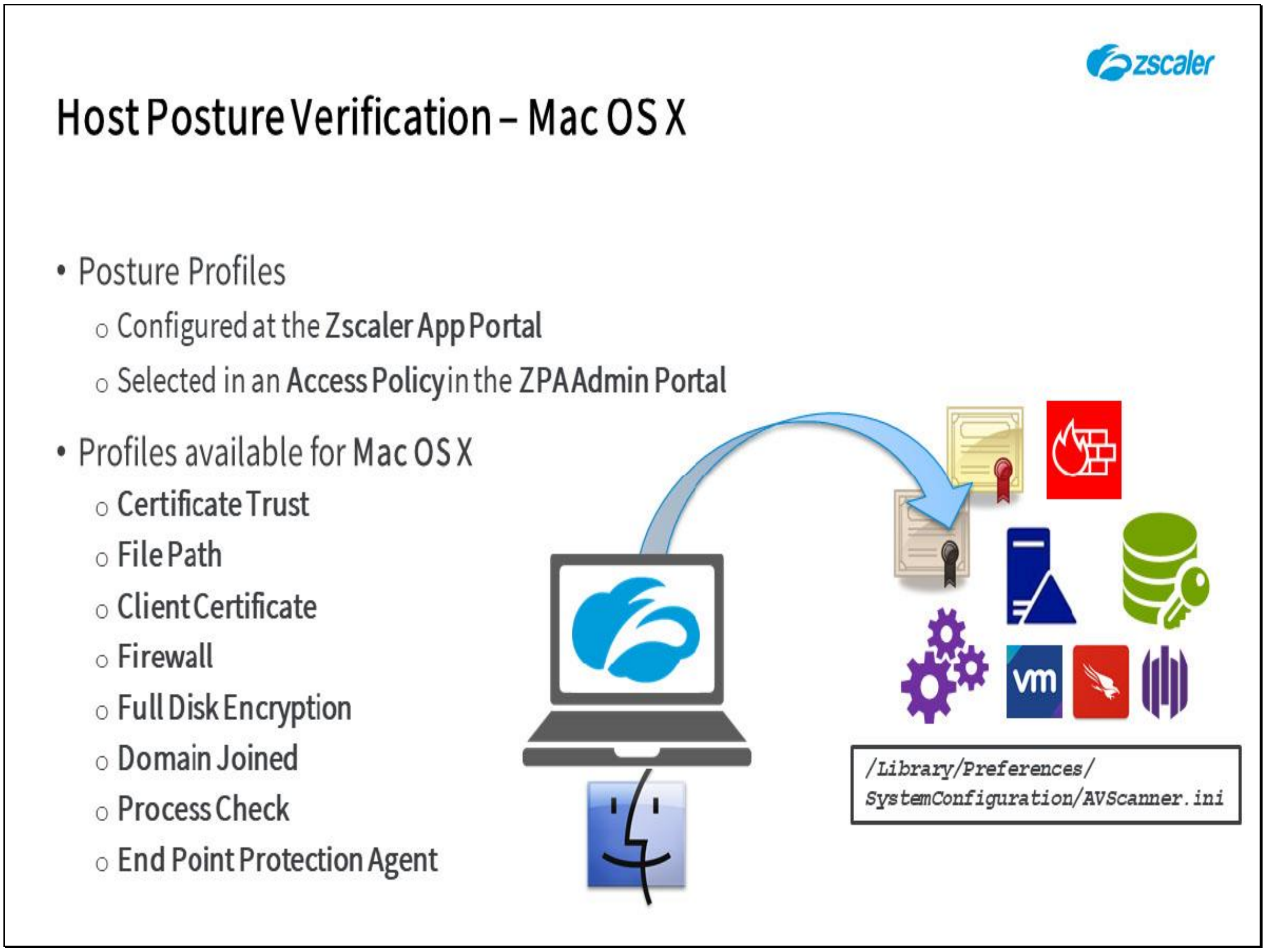
Slide notes

The Windows platform supports the most types of **Posture Profile**, the options available being:

- The **Certificate Trust** posture type, where a CA certificate can be uploaded to the device profile and the issuer of that certificate must be present and trusted on the end user device;
- For the **FilePath** posture type you must specify the path to a file that must exist on your user's device;
- The **Registry Key** posture criteria, can be used to specify either the path to a required key, or the key value to validate;
- For the **Client Certificate** type, you must upload a certificate signed by the same CA certificate (or chain) that signed the device's client cert (whether a root CA, intermediate CA, or client certificate);
- If you select the **Firewall** type, the firewall must be active on the device on either the public, private, or domain firewall profiles;
- With the **Full Disk Encryption** option, disk encryption must be enabled on the device;
- If you select the **Domain Joined** option, you must specify the domain that the device must be joined to;

- The **Process Check** option requires you to specify the path to the process and load the **Signer Certificate Thumbprint**;
- Finally you can also specify that one of the supported end point protection agents be installed and active (**Carbon Black**, **CrowdStrike**, or **SentinelOne**).

Slide 17 - Host Posture Verification – Windows, Mac



Host Posture Verification – Mac OS X

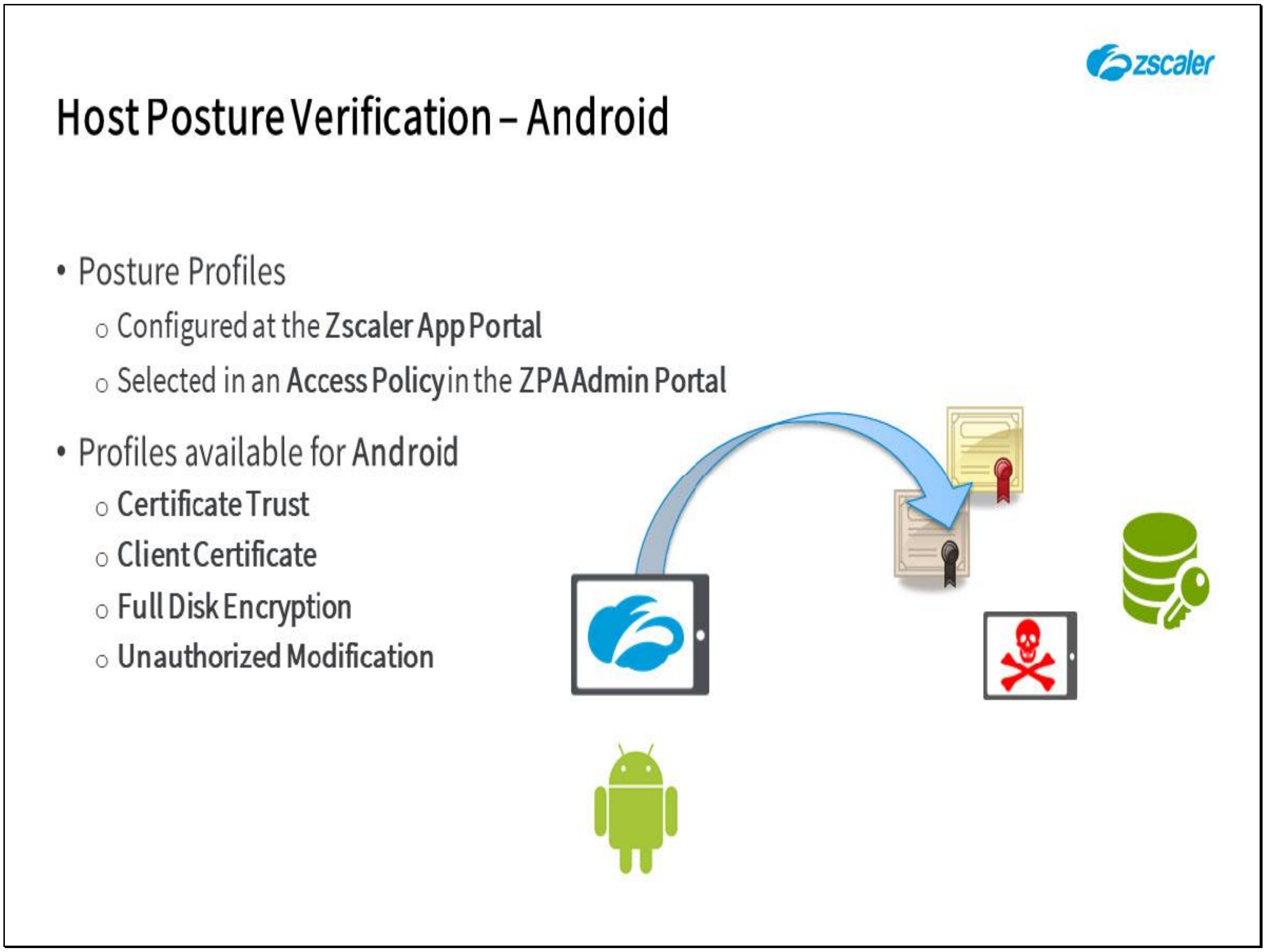
- Posture Profiles
  - Configured at the **Zscaler App Portal**
  - Selected in an **Access Policy** in the **ZPA Admin Portal**
- Profiles available for Mac OS X
  - **Certificate Trust**
  - **File Path**
  - **Client Certificate**
  - **Firewall**
  - **Full Disk Encryption**
  - **Domain Joined**
  - **Process Check**
  - **End Point Protection Agent**

```
/Library/Preferences/
SystemConfiguration/AVScanner.ini
```

Slide notes

For the Mac platform (OS X), the same **Posture Profile** options are available, with the exception of the **Registry Key** option of course.

Slide 18 - Host Posture Verification – Android



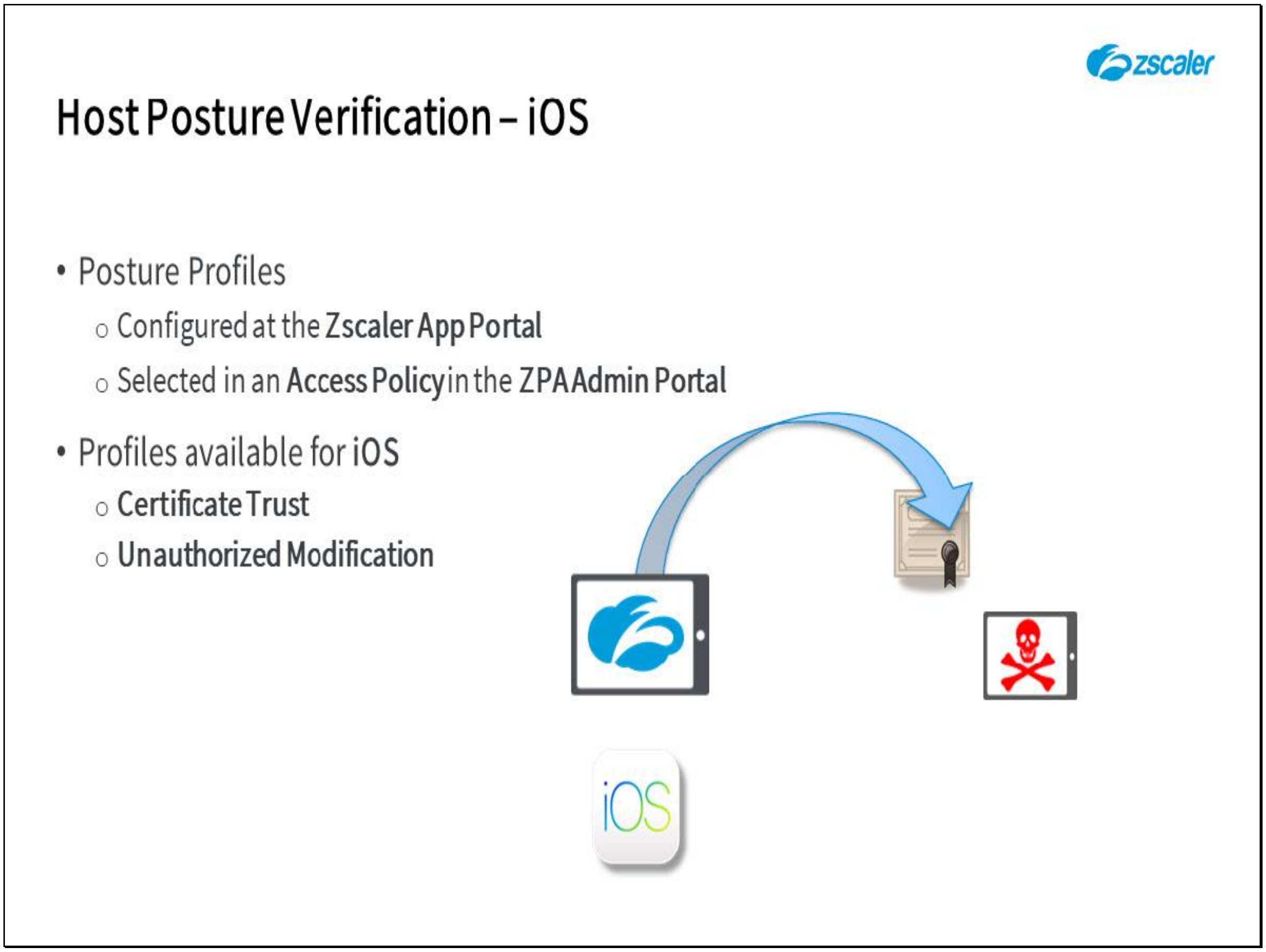
Host Posture Verification – Android

- Posture Profiles
  - Configured at the **Zscaler App Portal**
  - Selected in an **Access Policy** in the **ZPA Admin Portal**
- Profiles available for **Android**
  - **Certificate Trust**
  - **Client Certificate**
  - **Full Disk Encryption**
  - **Unauthorized Modification**

Slide notes

For the Android platform, a subset of these **Posture Profiles** is available: **Certificate Trust**; **Client Certificate**; and **Full Disk Encryption**. In addition to these there is also an **Unauthorized Modification** profile, which checks to see if the device has been ‘rooted’ and modified without authorization.

Slide 19 - Host Posture Verification – Windows



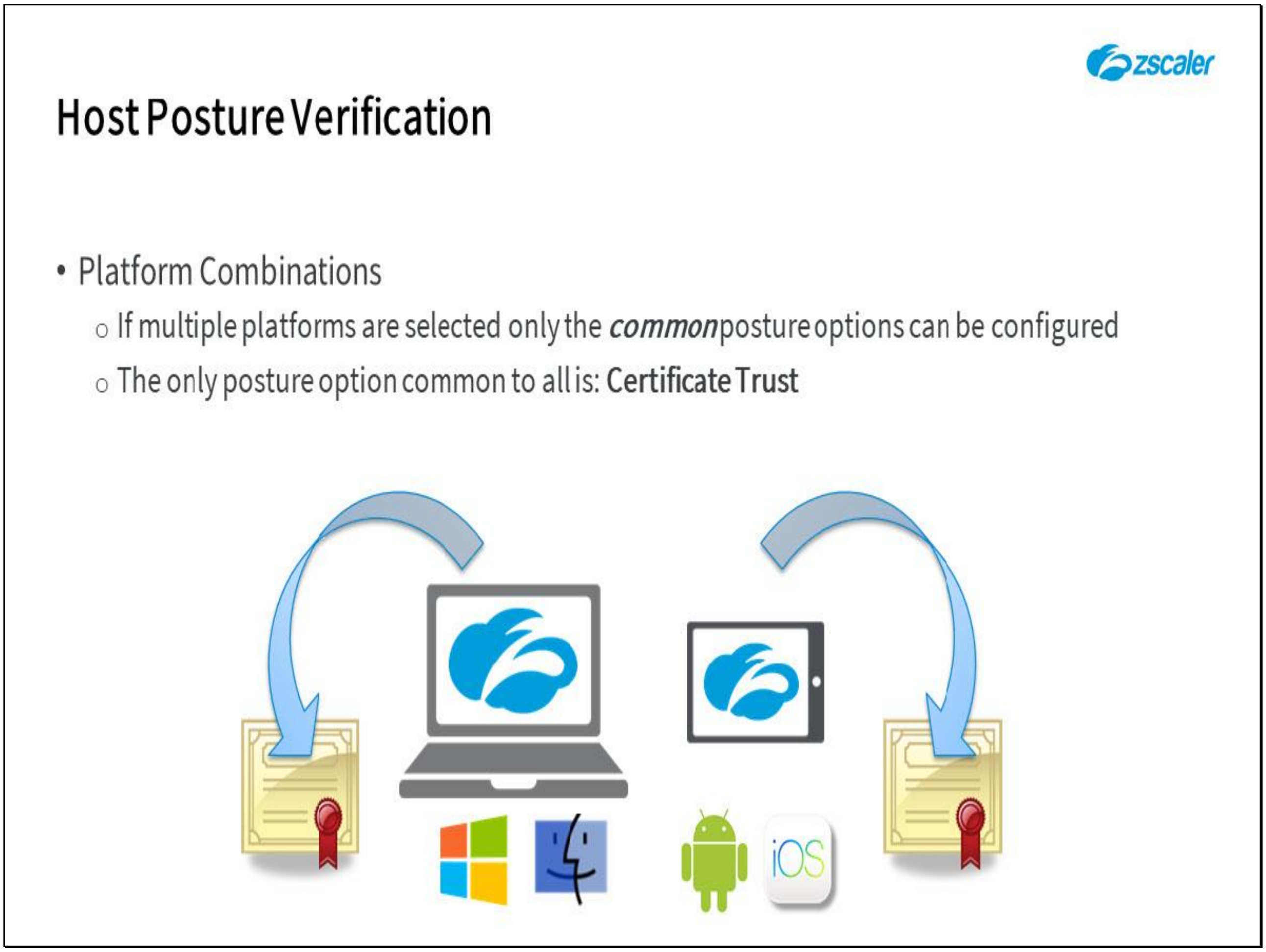
Host Posture Verification – iOS

- Posture Profiles
  - Configured at the **Zscaler App Portal**
  - Selected in an **Access Policy** in the **ZPA Admin Portal**
- Profiles available for **iOS**
  - **Certificate Trust**
  - **Unauthorized Modification**

Slide notes

For iOS, the only supported **Posture Profiles** currently are the **Certificate Trust** and **Unauthorized Modification** (which checks for jailbreaking).

Slide 20 - Host Posture Verification – Windows, Mac, Mobile



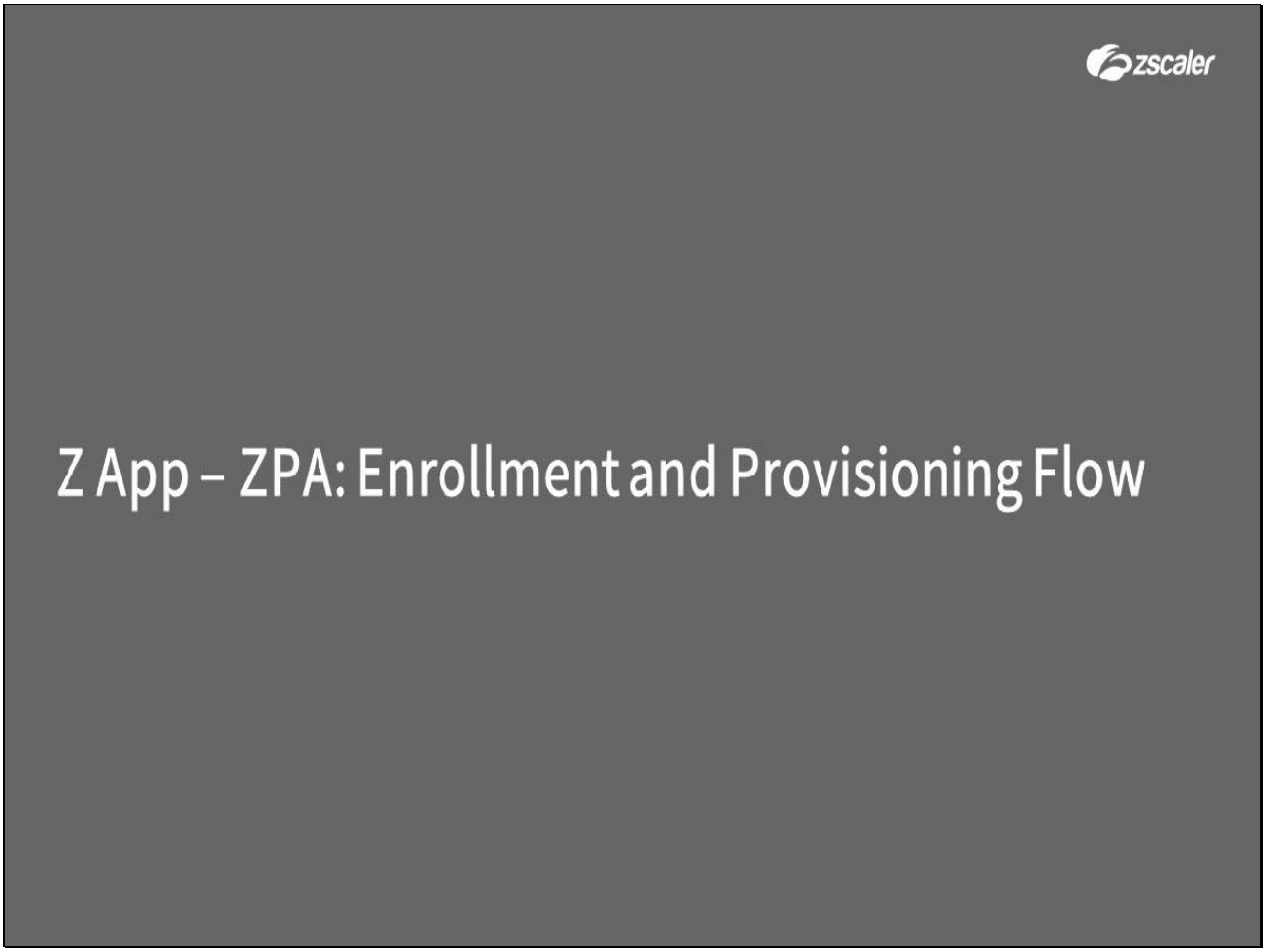
Host Posture Verification

- Platform Combinations
  - If multiple platforms are selected only the ***common*** posture options can be configured
  - The only posture option common to all is: **Certificate Trust**

Slide notes

Note that, if you select multiple platform types within a **Posture Profile** configuration, the only options that will be available to configure will be the profiles that are common across all of the selected platforms. For example, if you select all platforms the only common posture type is the **Certificate Trust** option.

Slide 21 - Zscaler App for ZPA – Provisioning and Enrollment Flow

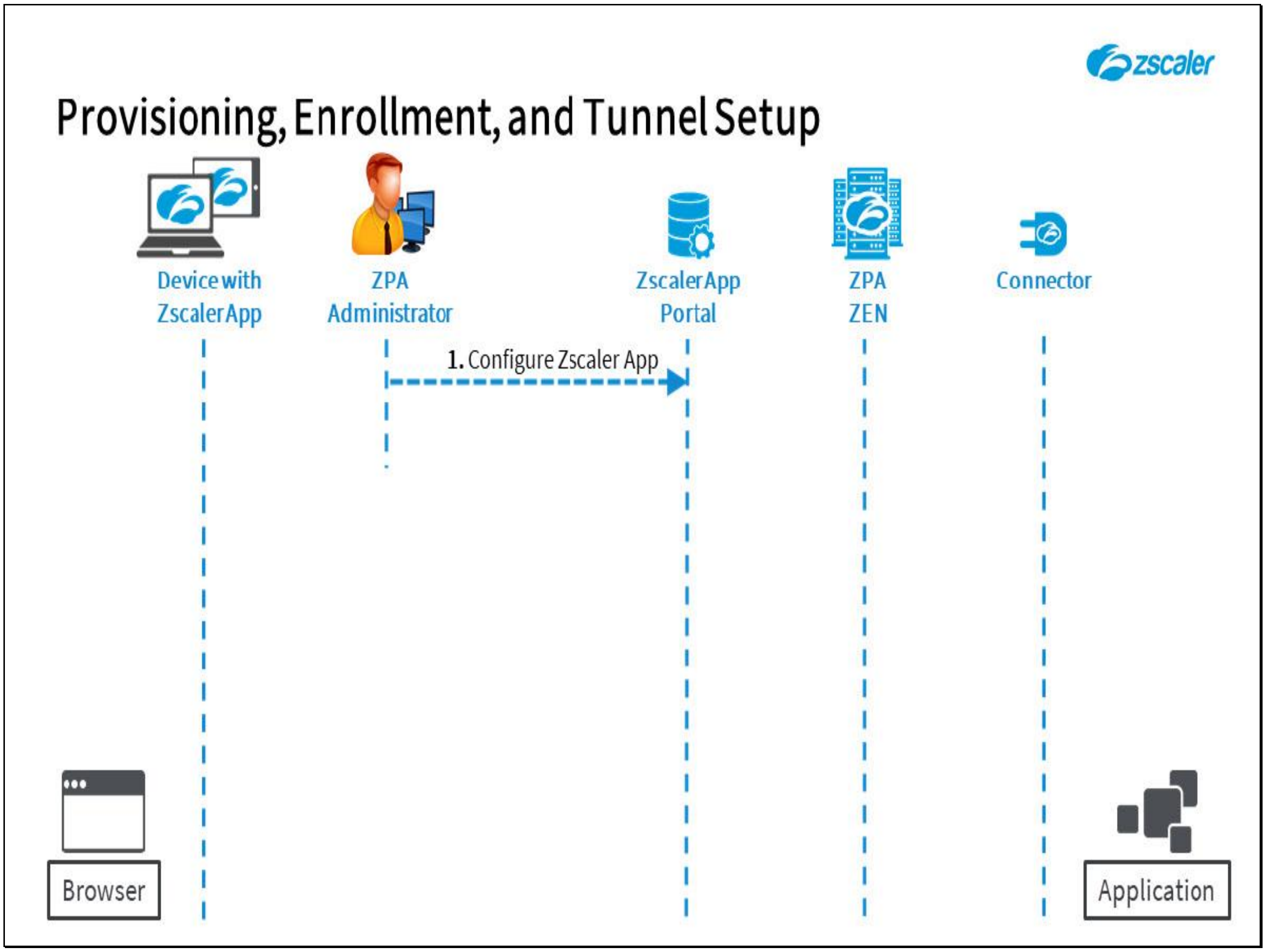


Z App – ZPA: Enrollment and Provisioning Flow

Slide notes

The final topic that we will cover is a look at the enrollment and provisioning flow for the Zscaler App used for ZPA.

Slide 22 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

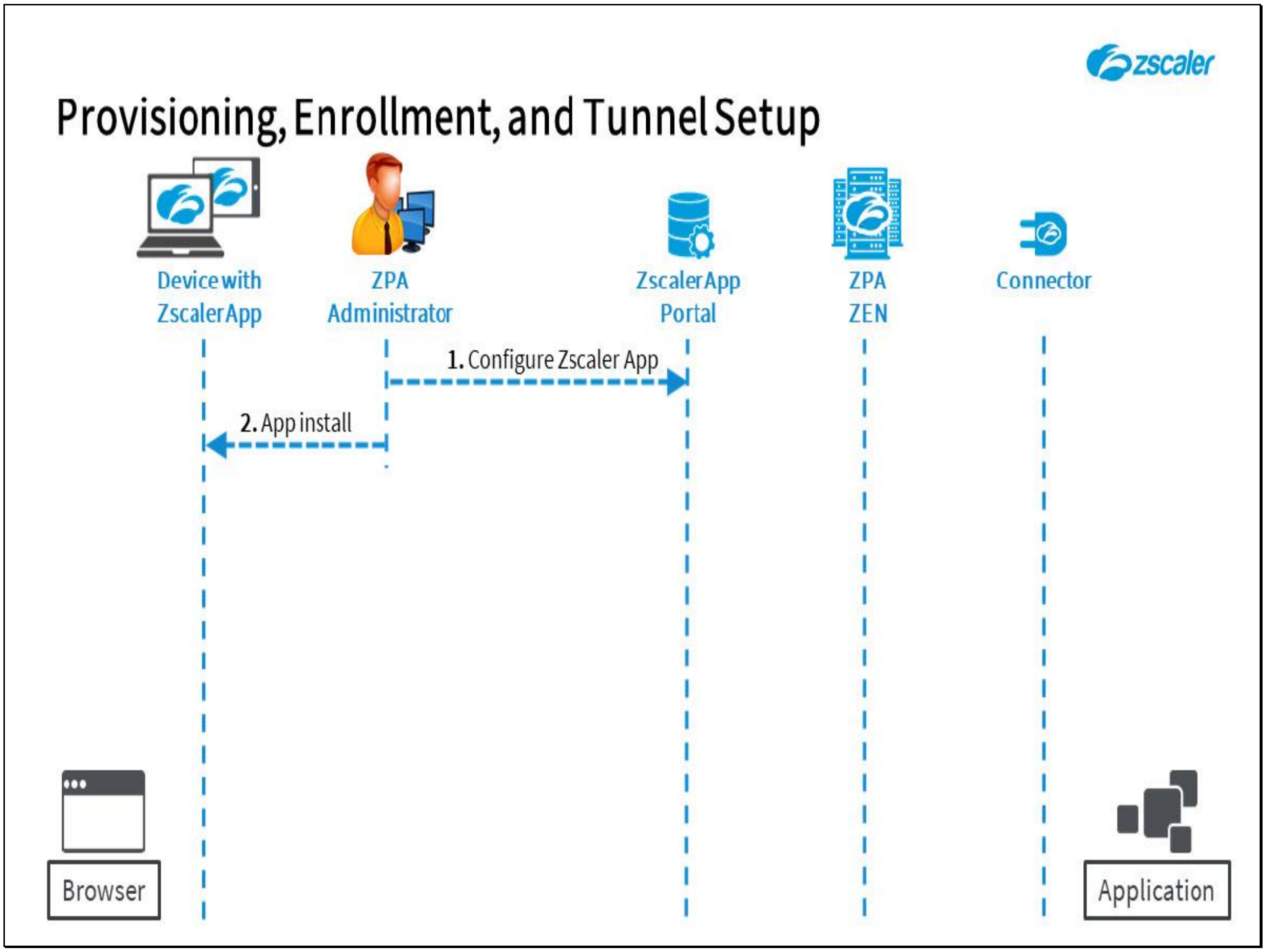
Slide notes

The enrollment and provisioning flow for the Zscaler App when used for ZPA is as follows:

Step 1: An administrator configures appropriate app settings for the users or groups in **App Profiles**, and optionally one or more **Forwarding Profiles**. There are additional miscellaneous configuration options, such as:

- **Zscaler App Notifications**;
- **Trusted Networks**;
- **Zscaler App Support**;
- **Zscaler Service Entitlement**;
- **User Agent**;
- And **Device Posture** options.

Slide 23 - Provisioning, Enrollment, and Tunnel Setup

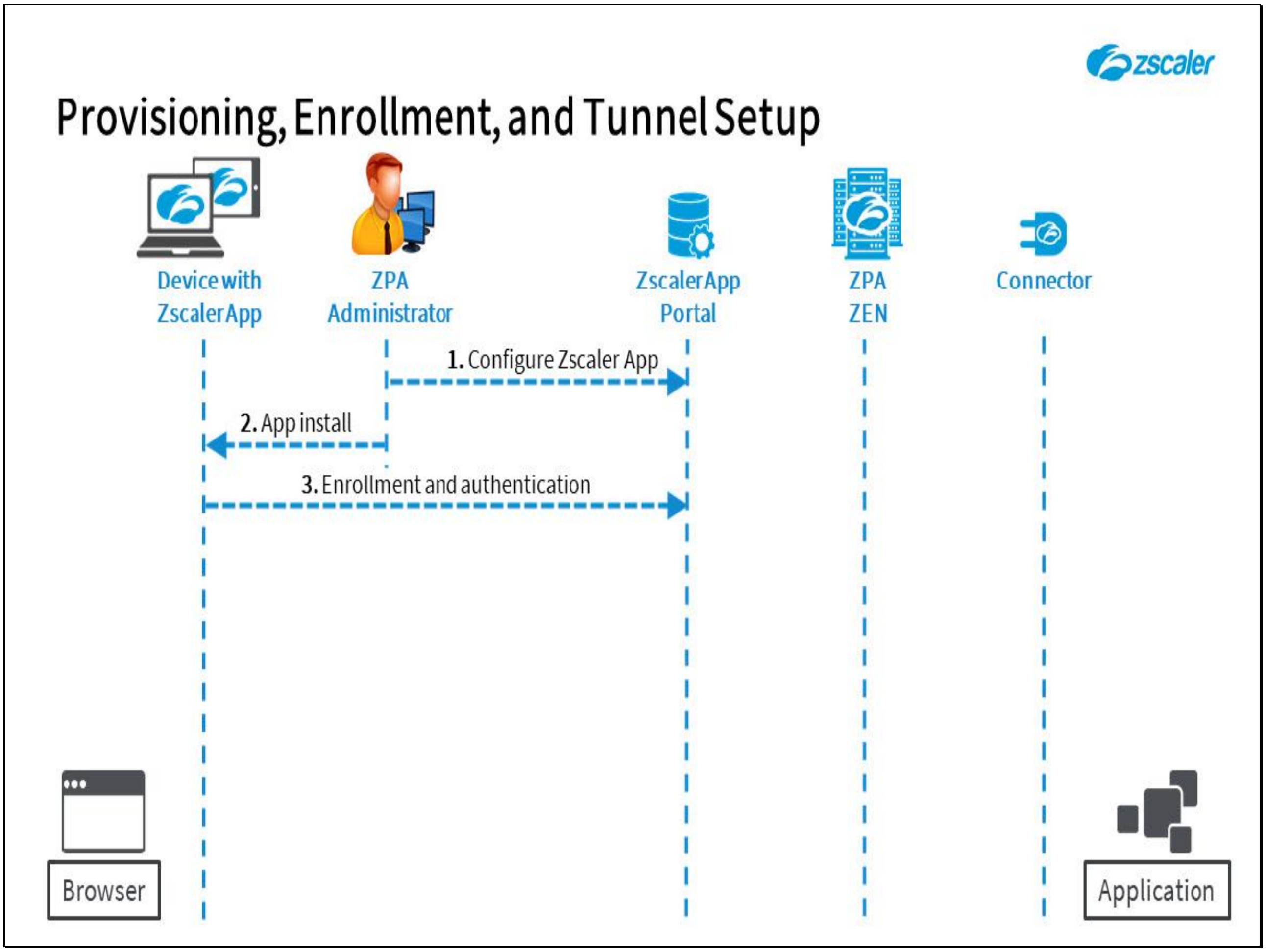


Provisioning, Enrollment, and Tunnel Setup

Slide notes

Step 2: The administrator ensures the distribution and installation of the App to those users that require it. This is often done by silently pushing the App using an AD Group Policy Object (or some other ESSM tool), or for mobile devices, by pushing the App as a 'managed' App from the MDM platform.

Slide 24 - Provisioning, Enrollment, and Tunnel Setup

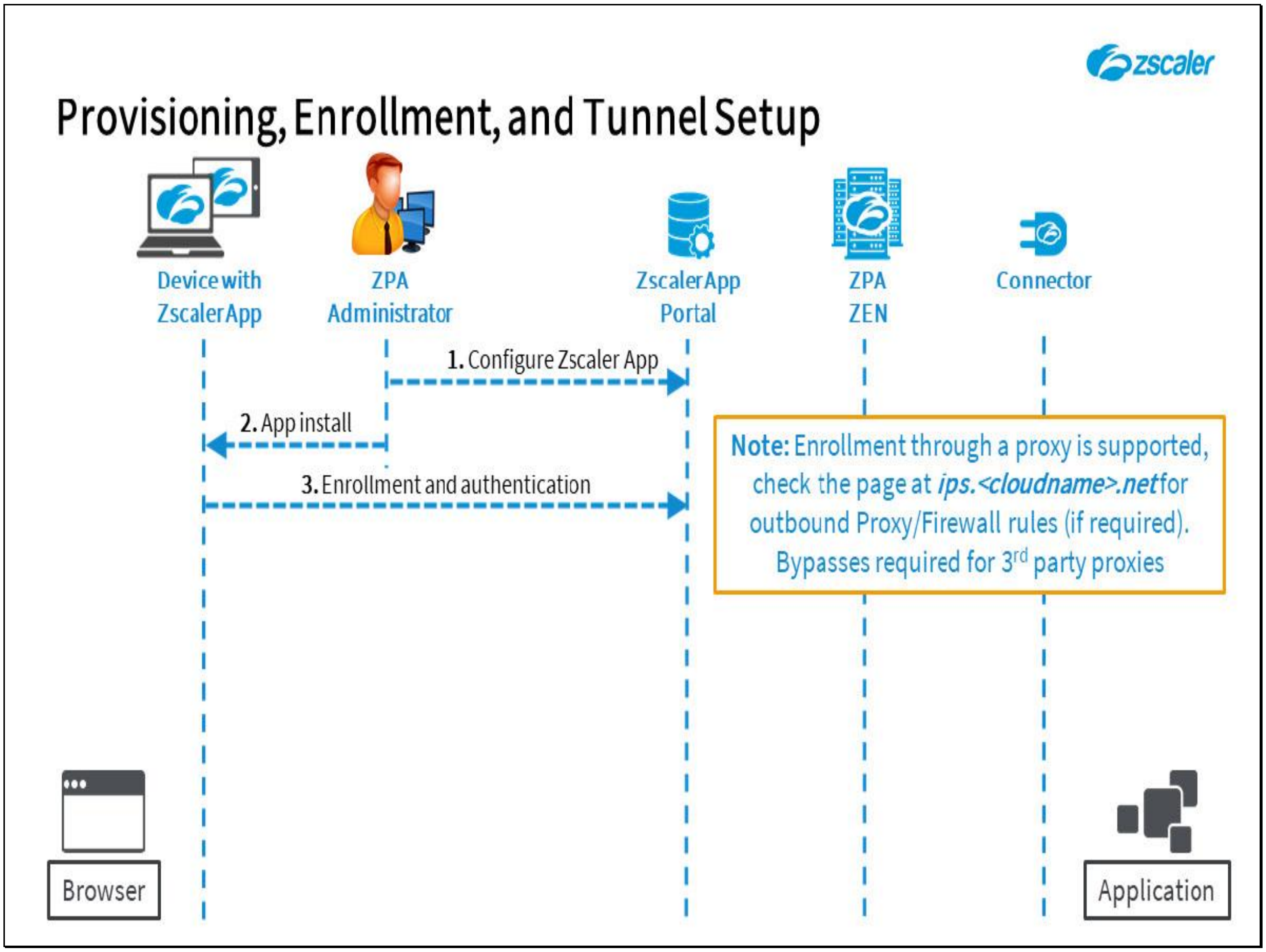


Provisioning, Enrollment, and Tunnel Setup

Slide notes

Step 3: The device user is prompted to enroll through the app. Authentication must use SAML and if the app is also to be used for Internet Access, enrollment to the ZIA cloud should also use SAML (and ideally the same IdP, to avoid the end user seeing 2 login prompts).

Slide 25 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

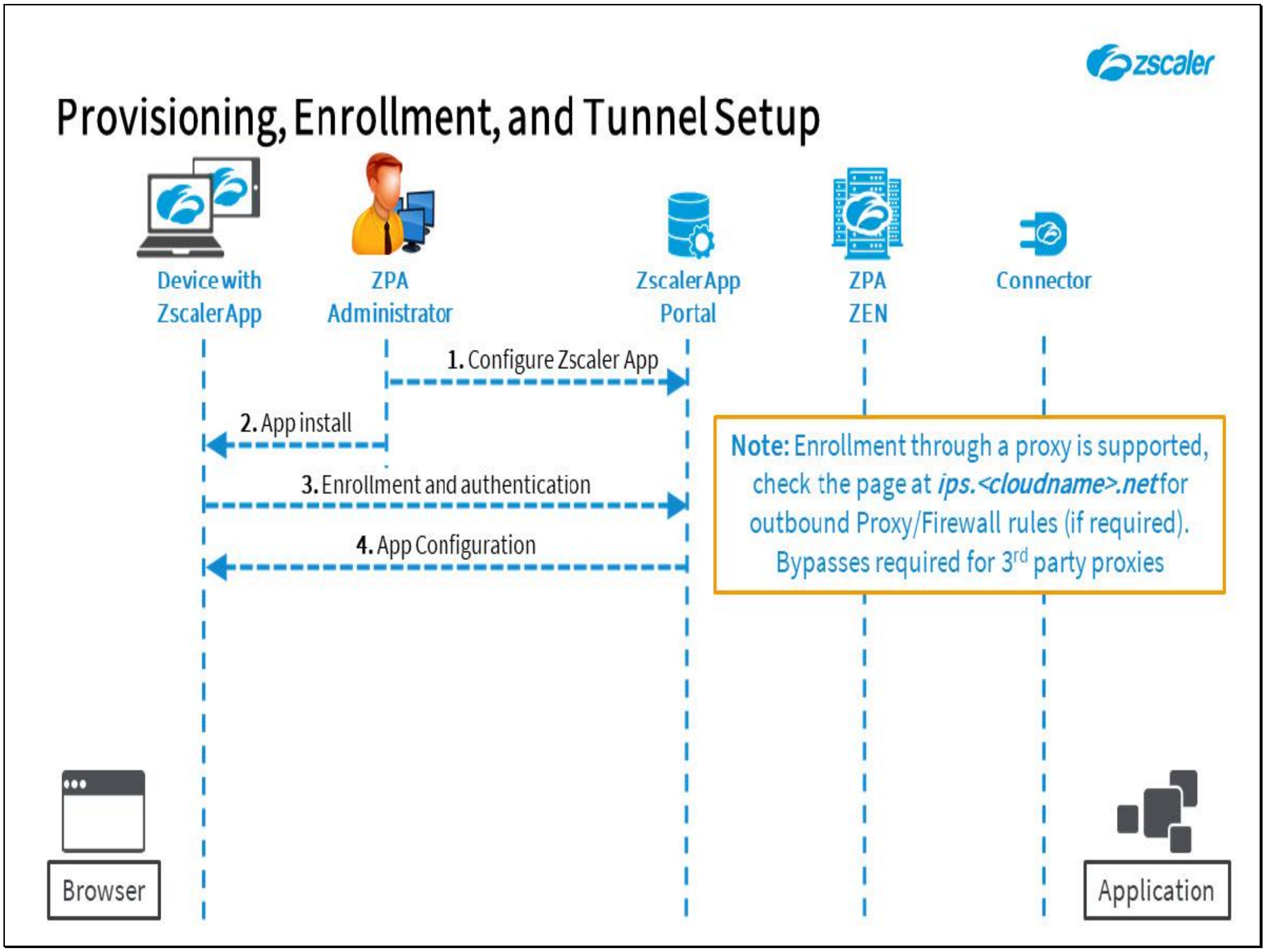
Note: Enrollment through a proxy is supported, check the page at ***ips.<cloudname>.net*** for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

Slide notes

Note that, the app tries to enroll direct first, if that fails it then tries using the system proxy settings. For enrollment through a Proxy, or from behind a Firewall there are some destinations that may need to be opened in the outbound direction including authentication bypasses.

Check the page at **https://ips.zscaler.net/zpa** for details. Also note that although registration through a proxy is possible, it is not recommended.

Slide 26 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

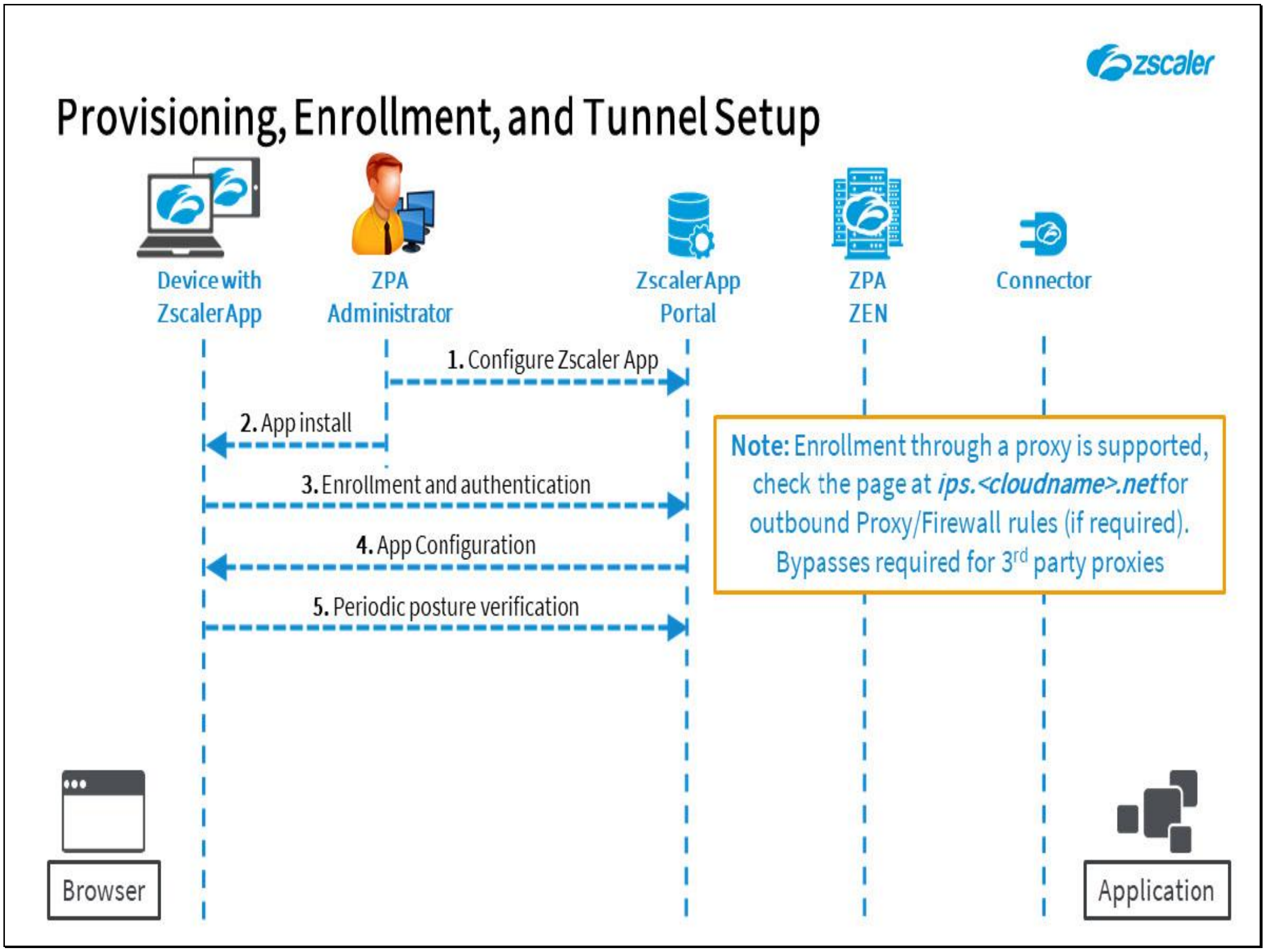
Slide notes

Step 4: On a successful enrollment, the App is provisioned and configured by the matching profiles, this includes the provisioning of the identity certificate required for authenticating **Z Tunnels**.

With ZPA, any number of authorization attributes may be provided by the IdP to the Zscaler App in the SAML assertion (unlike ZIA SAML assertions which are restricted to **User Identity**, **Group**, and **Department** attributes). The assertion is encrypted and stored locally by the Zscaler App to allow it to re-authenticate the user seamlessly for the duration of the current authentication session.

The App is also notified by the ZPA Central Authority of the private applications available, and of the applications that require **Double Encryption**.

Slide 27 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

1. Configure Zscaler App
2. App install
3. Enrollment and authentication
4. App Configuration
5. Periodic posture verification

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

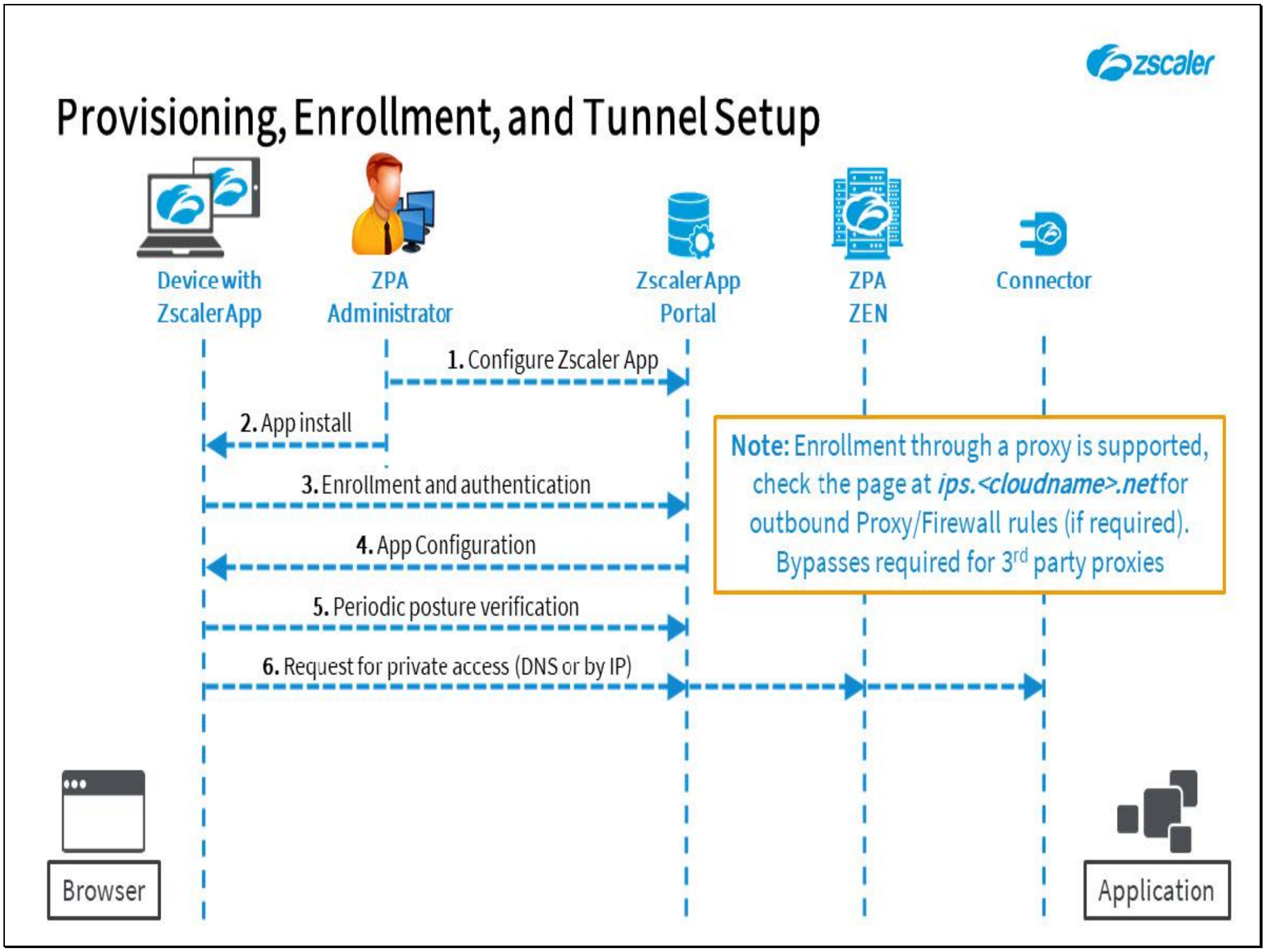
Slide notes

Step 5: The App sends device information to Zscaler that allows fingerprinting of the device for security and reporting purposes. The fingerprint contains key unique data from the host device, to prevent any possibility of cloning the machine for unauthorized access, for example; the CPU ID, the HD serial number, and the battery unique ID. The App checks in:

- Every 15 minutes to check for **App Profile** and **Forwarding Profile** PAC file updates;
- Every 60 minutes for profile/policy updates and to refresh the device fingerprint;
- And every 2 hours for new SW.

The user can also manually force a check in for Policy or PAC file updates from within the app, although note that this manual check only applies to Zscaler App profiles/policies (**App Profile** and **Forwarding Profile**), ZPA **Access Policies** to control application access are updated in real-time by the CA.

Slide 28 - Provisioning, Enrollment, and Tunnel Setup



zscaler

Provisioning, Enrollment, and Tunnel Setup

Device with ZscalerApp

ZPA Administrator

ZscalerApp Portal

ZPA ZEN

Connector

1. Configure Zscaler App

2. App install

3. Enrollment and authentication

4. App Configuration

5. Periodic posture verification

6. Request for private access (DNS or by IP)

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

Browser

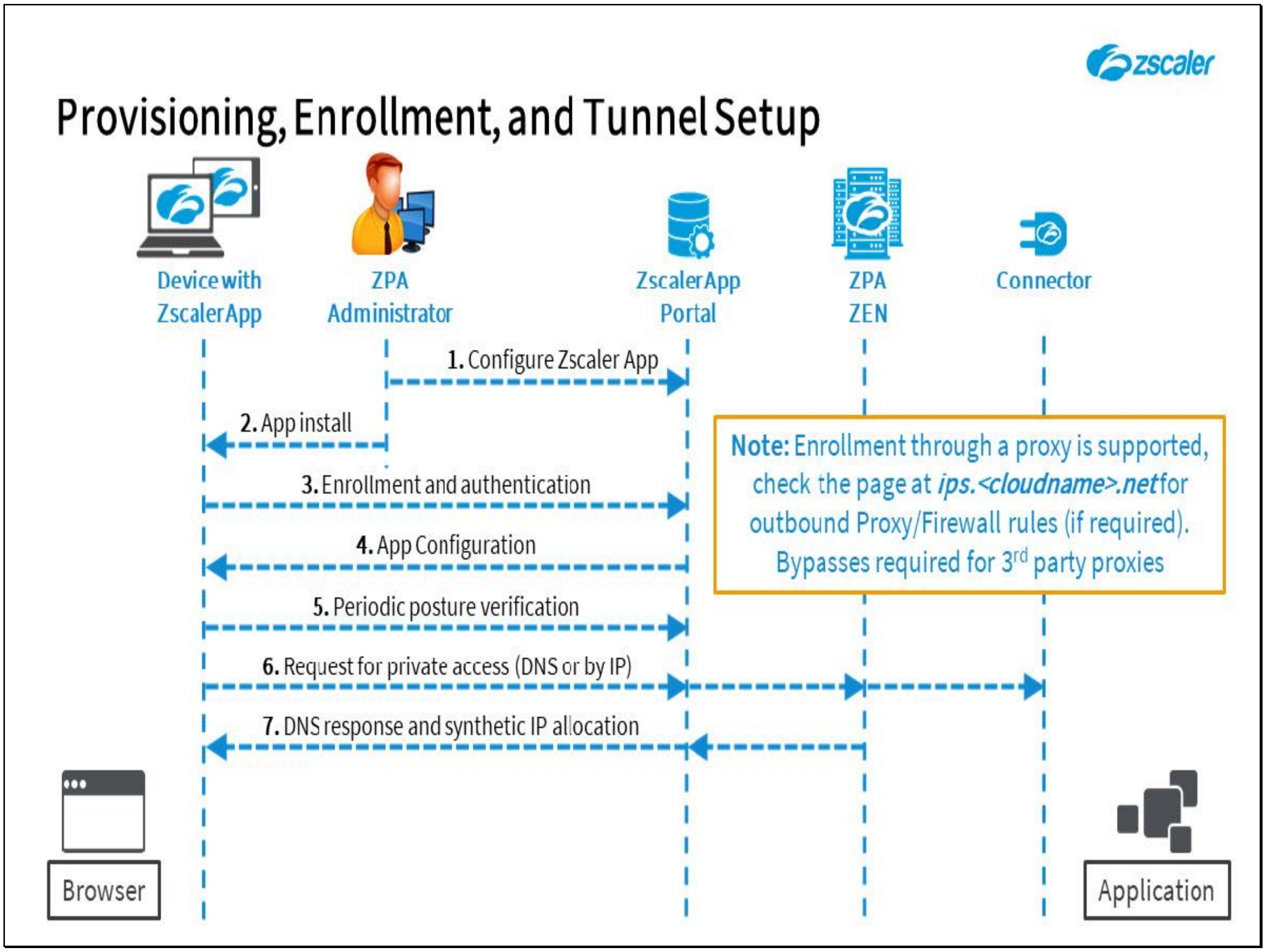
Application

Slide notes

Step 6: When a user requests access to a private application, the App sees the request and forwards it to the ZPA infrastructure through the ZPA-ZEN it is connected to. The ZPA CA will:

- Verify that the user meets all policy requirements to access the application;
- Confirm that the application is currently available;
- Identify the best instance of the application to connect to;
- And initiate establishing the end-to-end connection to the requested application, through the adjacent App Connector. The Connector is notified of the incoming connection through the TLS encrypted control channel that it established outbound to its nearest healthy ZPA-ZEN.

Slide 29 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

Device with Zscaler App

ZPA Administrator

Zscaler App Portal

ZPA ZEN

Connector

1. Configure Zscaler App

2. App install

3. Enrollment and authentication

4. App Configuration

5. Periodic posture verification

6. Request for private access (DNS or by IP)

7. DNS response and synthetic IP allocation

Note: Enrollment through a proxy is supported, check the page at ***ips.<cloudname>.net*** for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

Browser

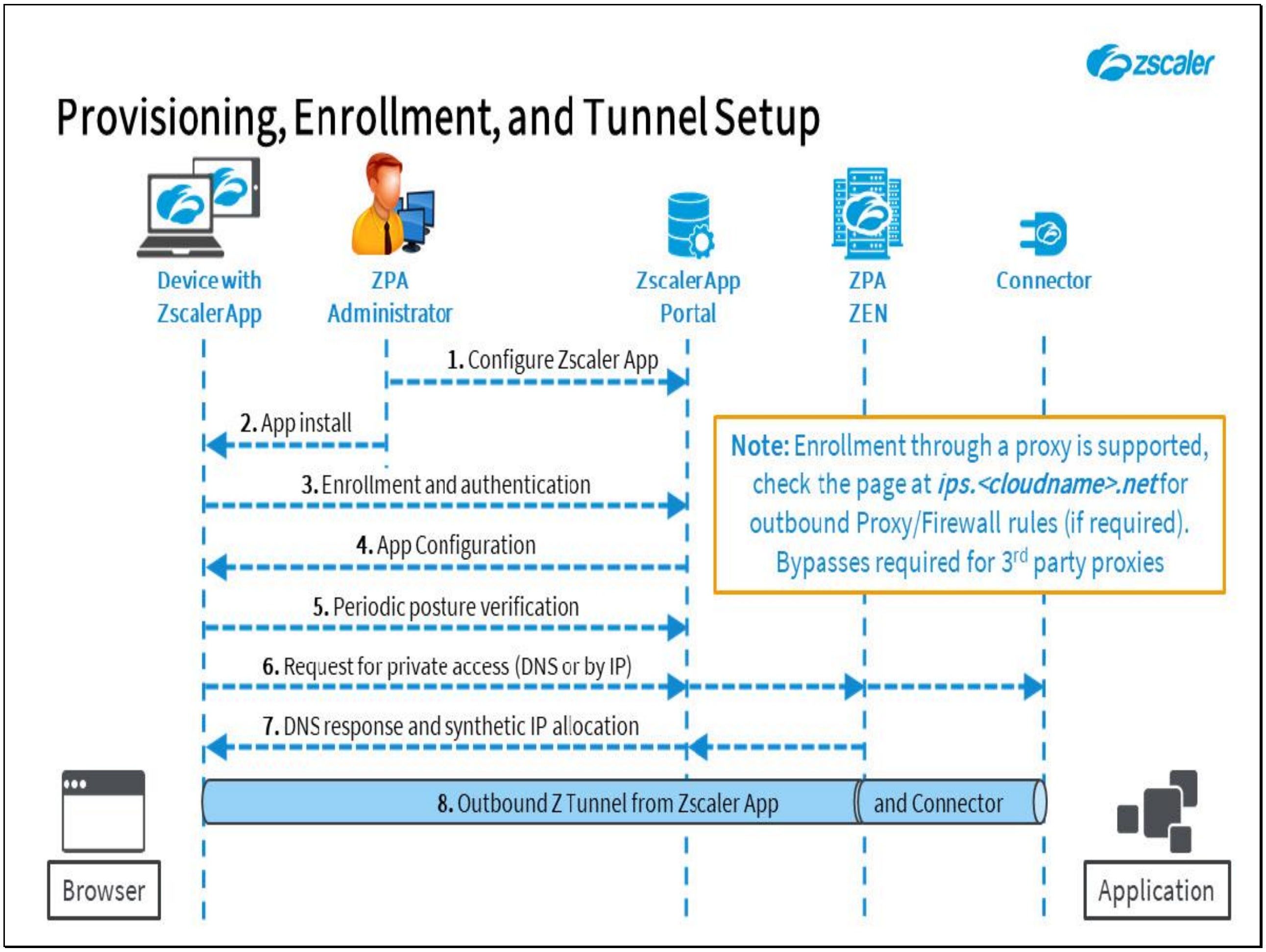
Application

Slide notes

Step 7: When it receives a response from the ZPA-ZEN, the Zscaler App will allocate a synthetic IP address from the **100.64.0.0/16** range for that application and return this to the browser (or other SW) that initiated the DNS request. Note that for applications that rely on DNS CNAME records (such as Kerberos), the app returns both the synthetic IP address and CNAME record for resolved ZPA domains.

Also note that, if the Zscaler App is also used for ZIA, then any custom PAC file applied in the **App Profile** needs to bypass the **100.64.0.0/16** address range. This bypass is defined in the Cloud service default PAC file, which is automatically applied if no custom PAC file URL is applied in the **App Profile**.

Slide 30 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

1. Configure Zscaler App

2. App install

3. Enrollment and authentication

4. App Configuration

5. Periodic posture verification

6. Request for private access (DNS or by IP)

7. DNS response and synthetic IP allocation

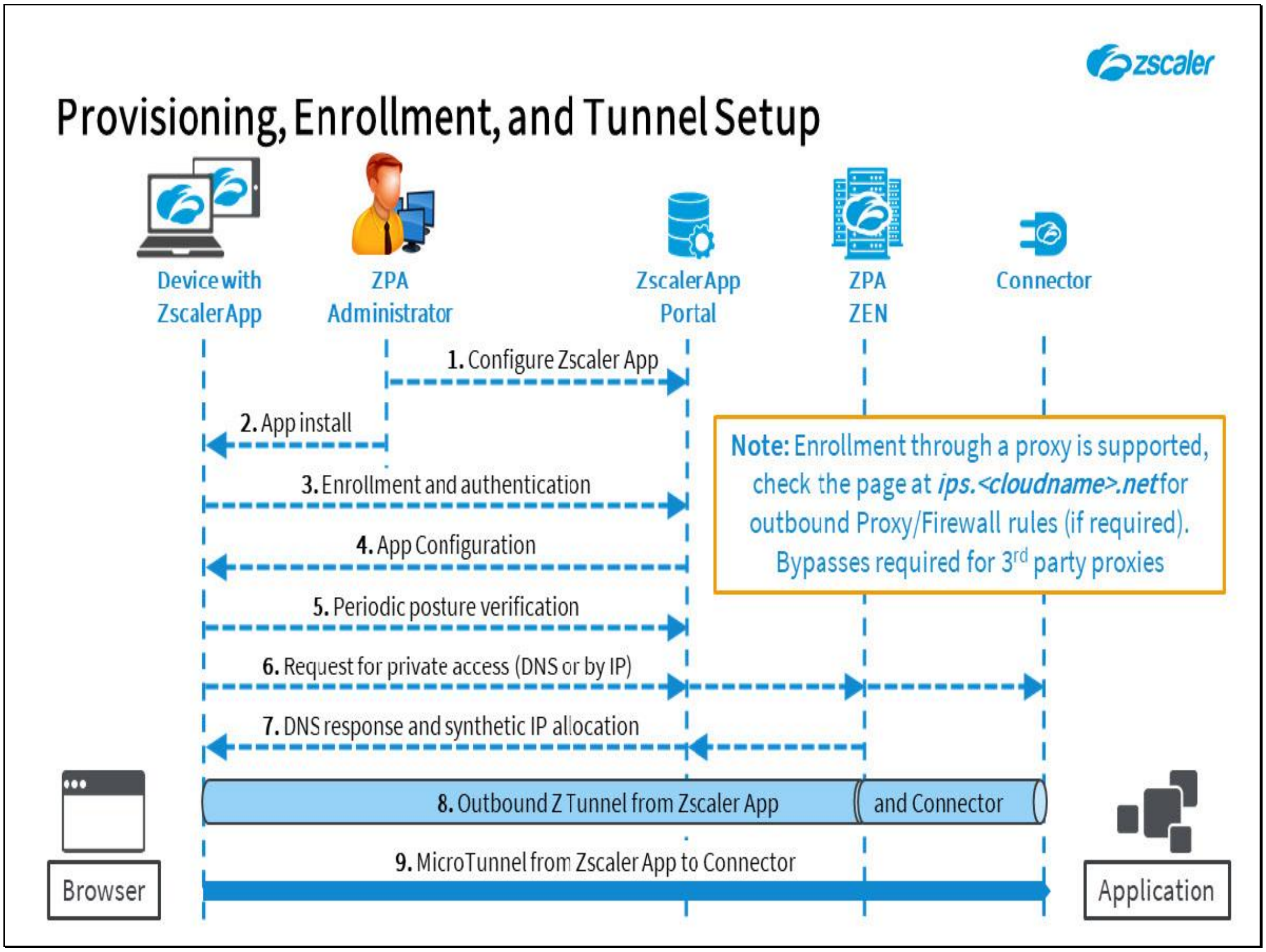
8. Outbound Z Tunnel from Zscaler App and Connector

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

Slide notes

Step 8: At this point, both the Zscaler App and the Connector adjacent to the selected application instance will establish outbound TLS 1.2 encrypted **Z Tunnels** to the nominated ZPA-ZEN (chosen to minimize end-to-end latency). The tunnels are mutually validated through the certificates installed at each end, and the user is authenticated through the SAML token from the last re-authentication.

Slide 31 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

Device with Zscaler App

ZPA Administrator

Zscaler App Portal

ZPA ZEN

Connector

1. Configure Zscaler App

2. App install

3. Enrollment and authentication

4. App Configuration

5. Periodic posture verification

6. Request for private access (DNS or by IP)

7. DNS response and synthetic IP allocation

8. Outbound Z Tunnel from Zscaler App and Connector

9. MicroTunnel from Zscaler App to Connector

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

Browser

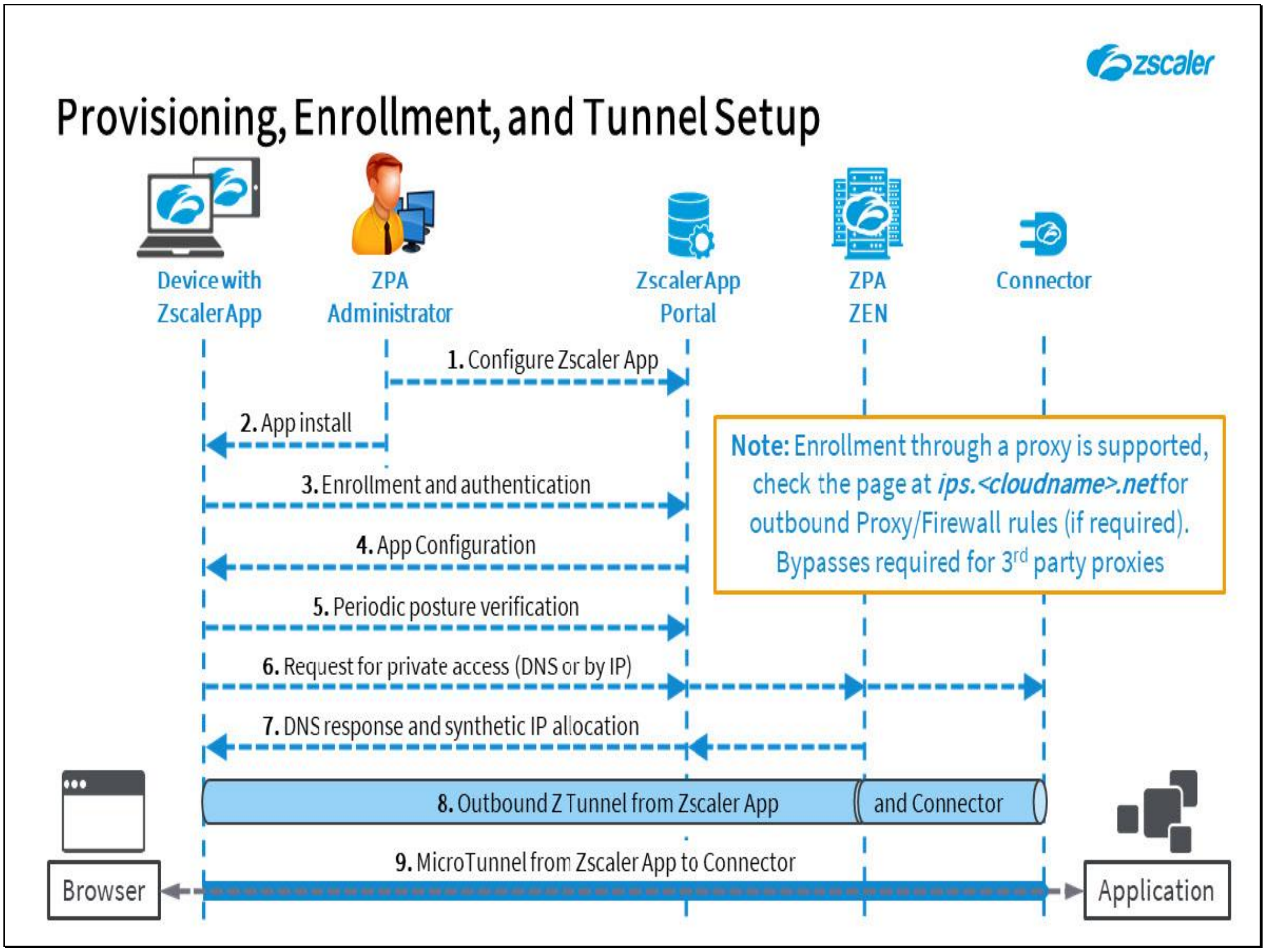
Application

Slide notes

Step 9: Once the **Z Tunnels** are in place, the App can send the byte stream from the source SW to the **Microtunnel** established for this connection and addressed using the unique tags allocated dynamically during the connection setup process. This **Microtunnel** connects at the ZPA-ZEN to the **Microtunnel** established to the Connector, to provide an end-to-end connection from Zscaler App to Connector.

Optionally, with the **Double Encryption** option, an additional end-to-end TLS tunnel may be established within the **Microtunnel**, based on the customer's custom PKI. This option prevents even Zscaler from intercepting or viewing the data transferred within the tunnel.

Slide 32 - Provisioning, Enrollment, and Tunnel Setup



Provisioning, Enrollment, and Tunnel Setup

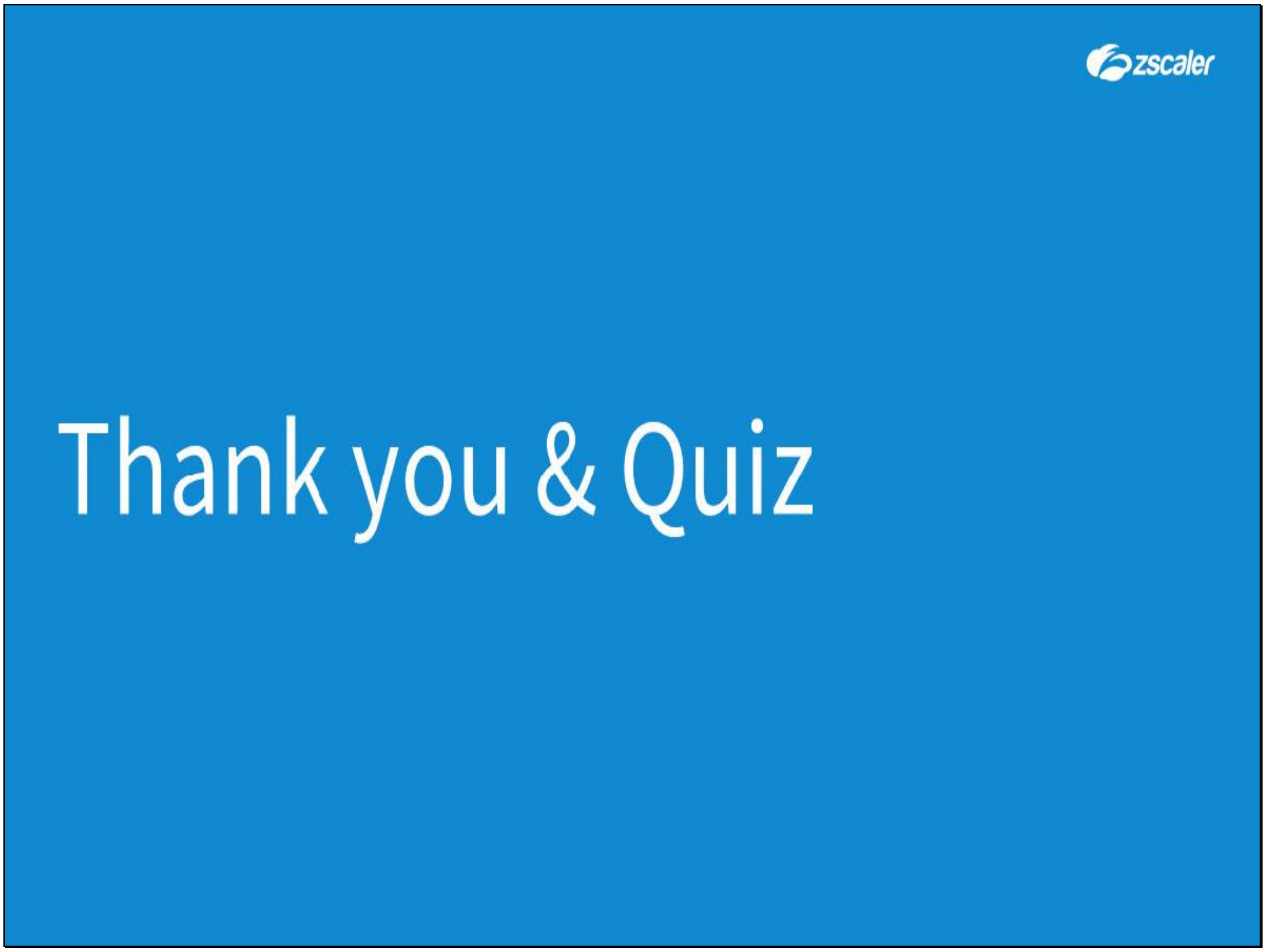
zscaler
Device with Zscaler App
ZPA Administrator
Zscaler App Portal
ZPA ZEN
Connector
1. Configure Zscaler App
2. App install
3. Enrollment and authentication
4. App Configuration
5. Periodic posture verification
6. Request for private access (DNS or by IP)
7. DNS response and synthetic IP allocation
8. Outbound Z Tunnel from Zscaler App
and Connector
9. MicroTunnel from Zscaler App to Connector
Browser
Application

Note: Enrollment through a proxy is supported, check the page at *ips.<cloudname>.net* for outbound Proxy/Firewall rules (if required). Bypasses required for 3rd party proxies

Slide notes

Once the **Z Tunnels** and **Microtunnel** are in place, the browser (or other SW agent on the host) can connect seamlessly to the private application in the data center. The browser believes it is talking directly to the Zscaler App on the assigned synthetic IP address, and the application believes it is talking directly to the Connector. The Zscaler App and Connector manage the flow of data between the end points.

Slide 33 - Thank you & Quiz



zscaler

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.

What follows is a short 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.