

Slide 1 - Zscaler Private Access



# Zscaler Private Access

## ZPA Connector Installation – Overview

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on Zscaler Private Access Connector installation.

## 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

- Connector Prerequisites
- Installation Process
- Connector Provisioning

## Slide notes

In this module, we will look at Connector prerequisites, at the installation process, and at how to provision a Connector in the ZPA Admin Portal.

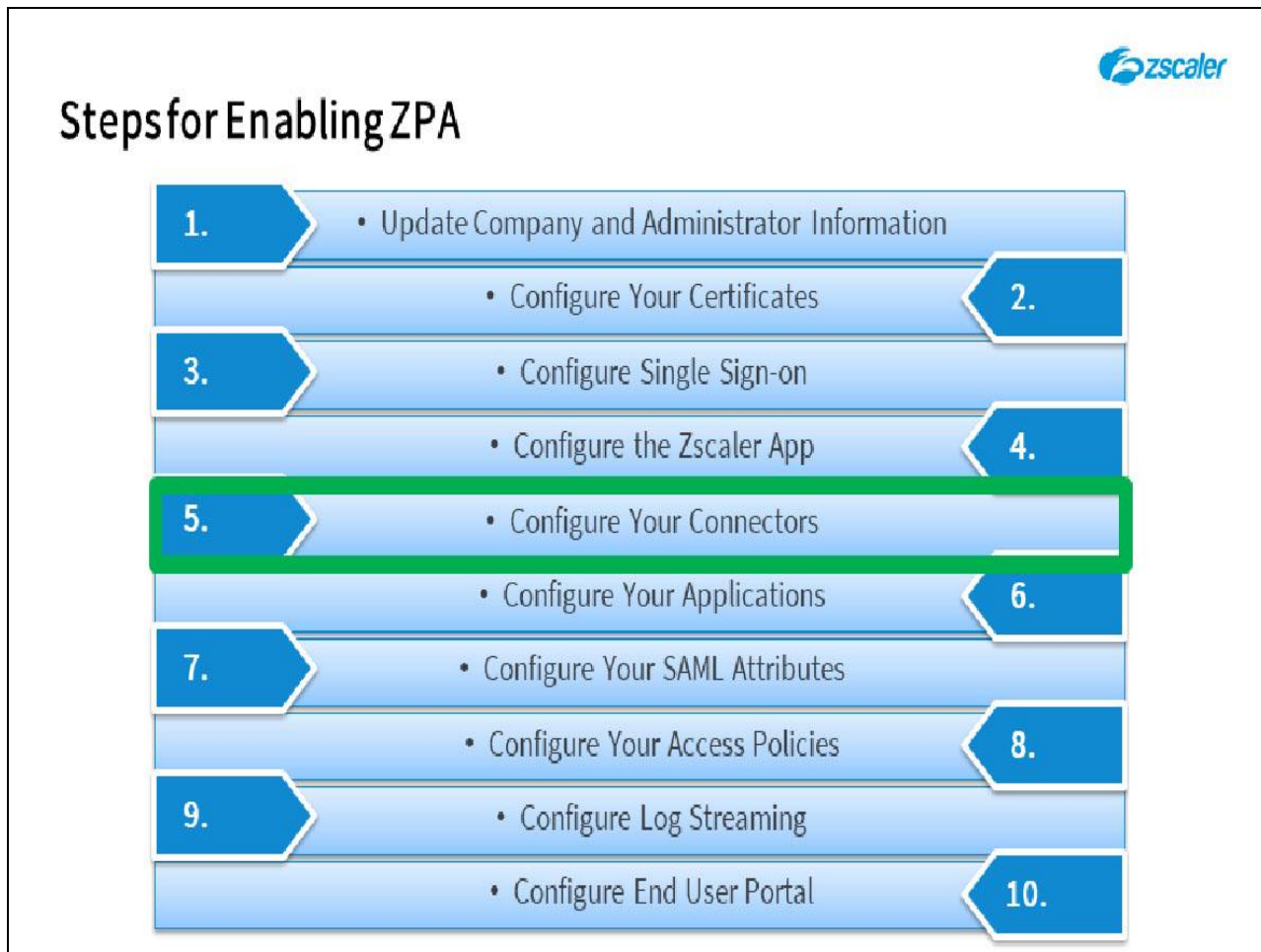
Slide 4 - ZPA Portal Overview



Slide notes

The first topic that we will cover is the prerequisites for a Connector installation.

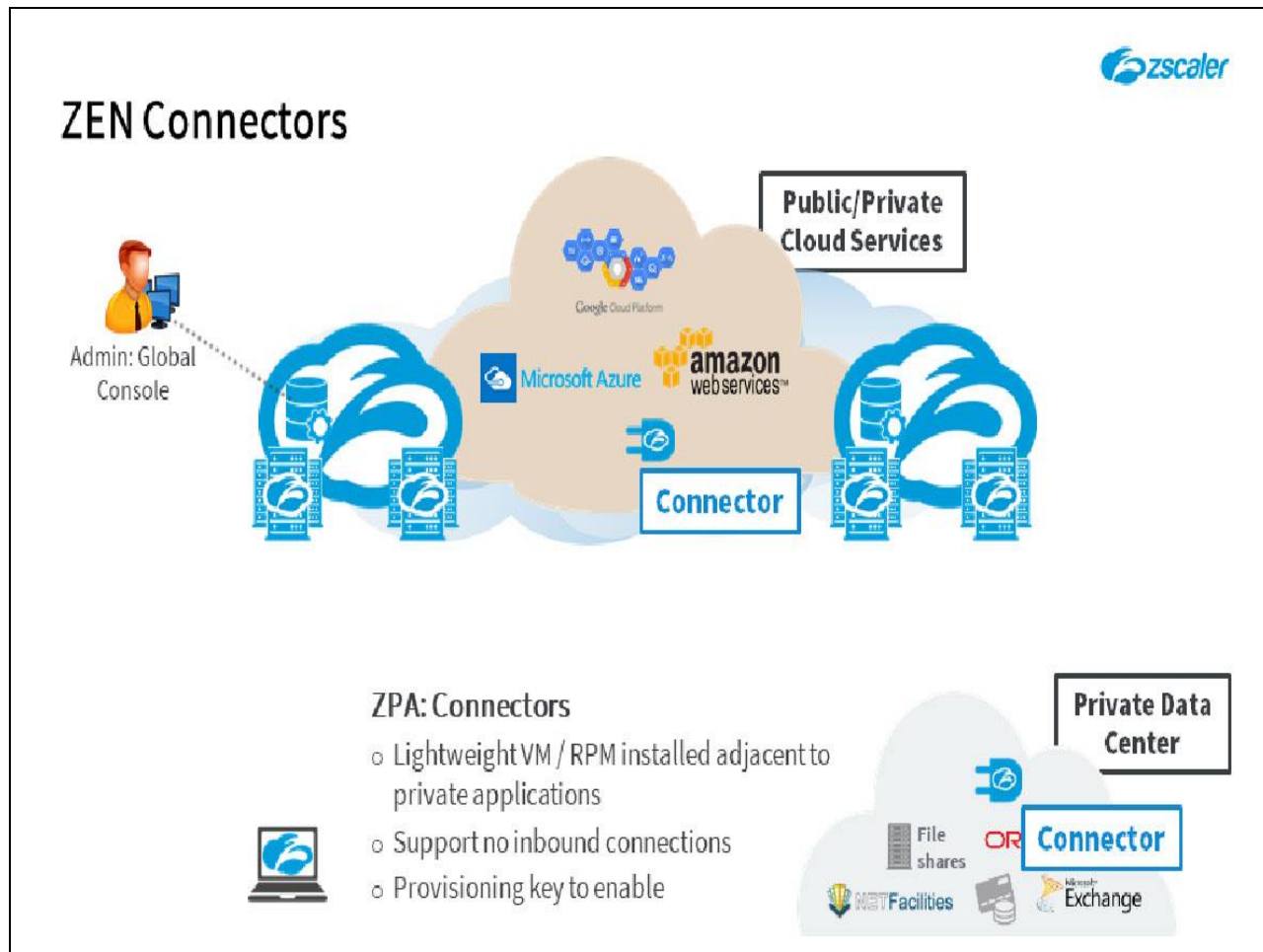
## Slide 5 - Steps for Enabling ZPA



## Slide notes

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

## Slide 6 - Virtual Appliance Requirements

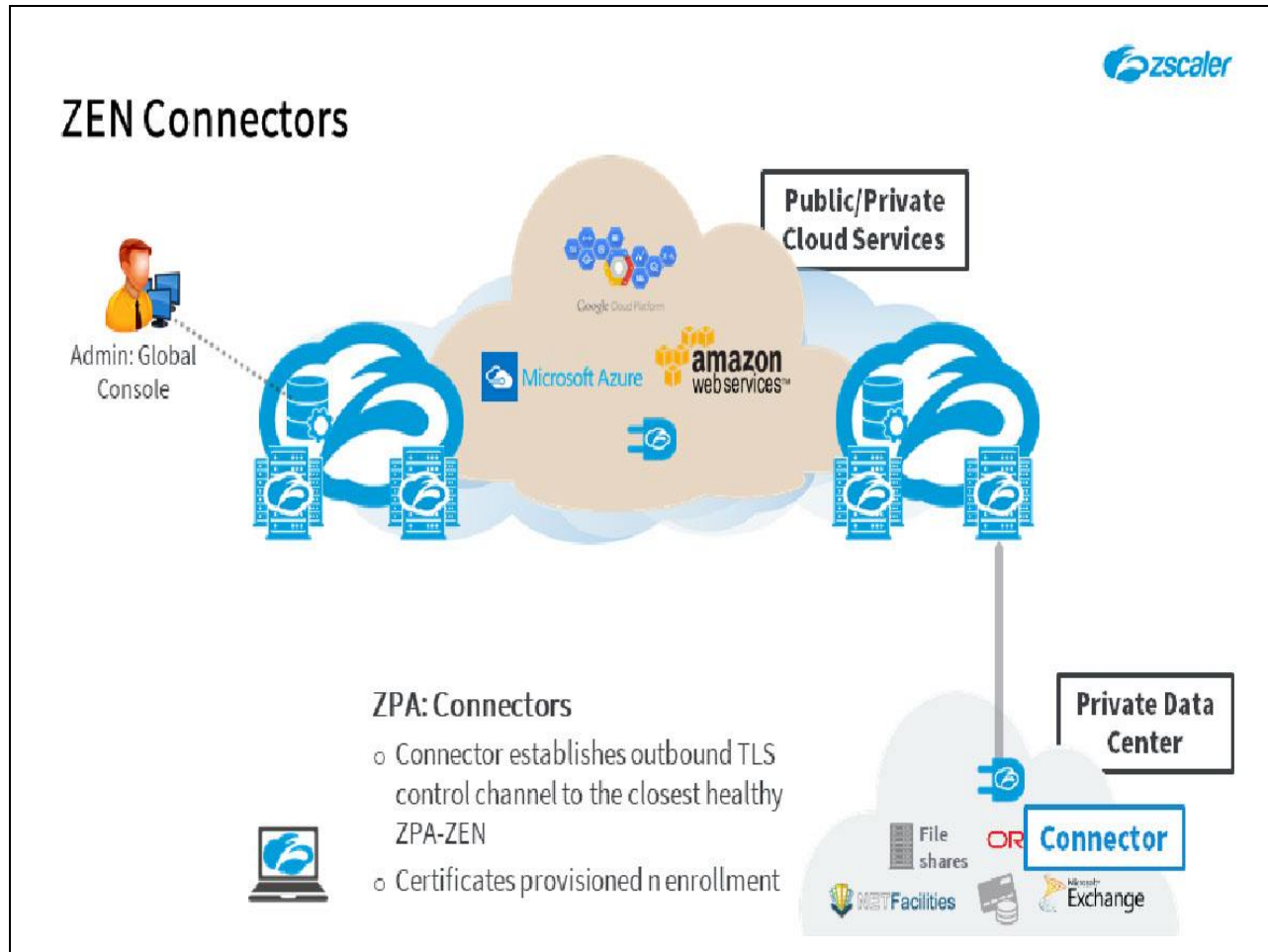


## Slide notes

As a reminder, the Connector is the only component of the ZPA solution that is connected to the customer's internal network, adjacent to the private applications that need to be shared. A Connector is a lightweight Linux implementation (VM / RPM) that boots extremely fast and is intended to sit adjacent to the private applications that you need to provide remote access to.

Connectors neither support, nor require any inbound connections, they only ever establish connections to the ZPA infrastructure in the outbound direction. A Provisioning Key is required in order to enroll a Connector to the ZPA infrastructure, after which they receive their configuration and certificates from the ZPA-CA. They may be updated or restarted from the CA as required.

## Slide 7 - Connectors

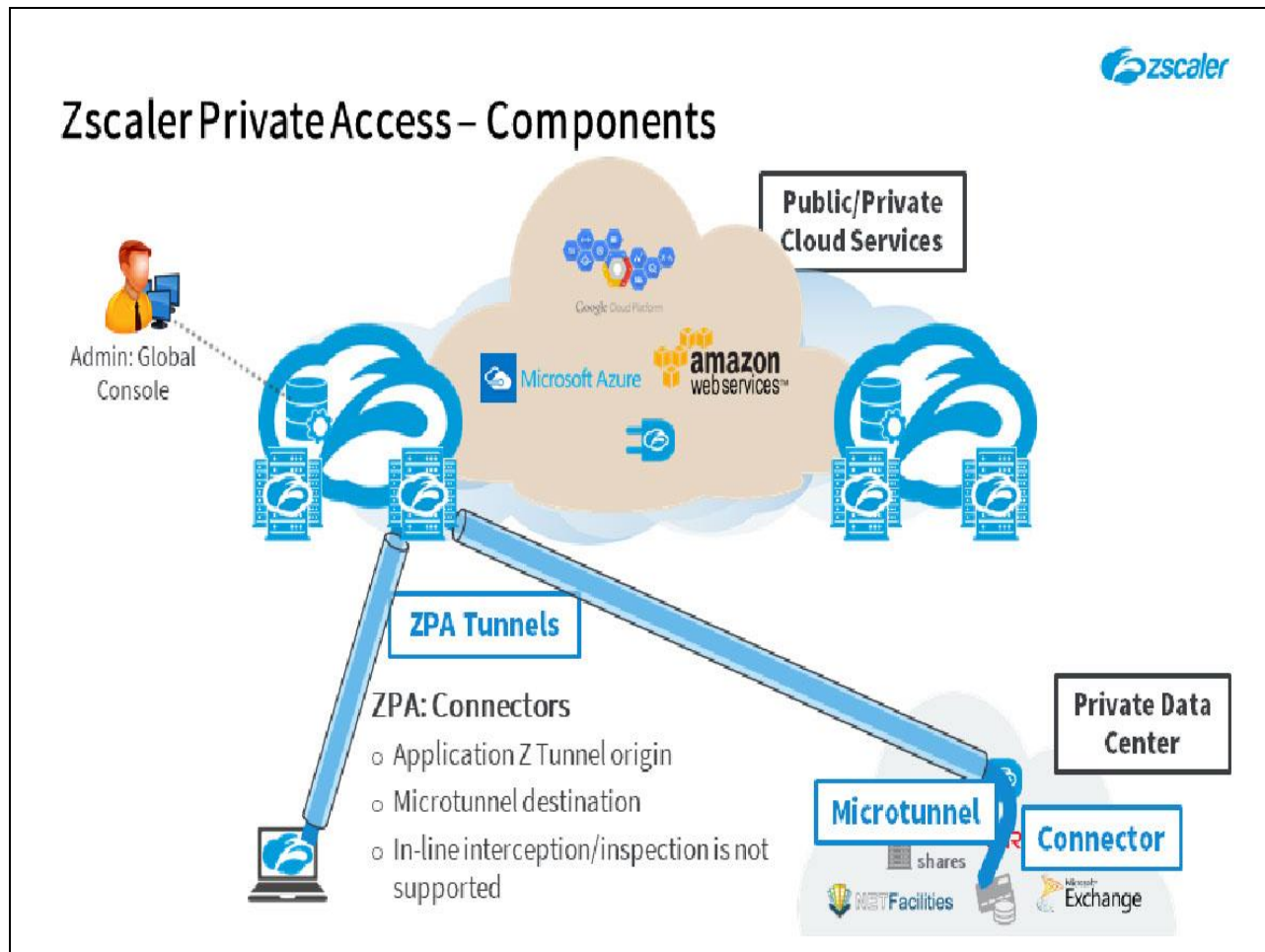


## Slide notes

When you deploy a Connector, as it boots onto the network, it “calls home” and establishes an outbound encrypted TLS connection to the closest healthy ZPA-ZEN. This connection is used as a control channel to allow enrollment and configuration of the Connector, and for it to notify the ZPA-CA of any discovered applications when required.

The enrollment of the Connector is secured through a Provisioning Key that is signed by the Intermediate CA on the ZPA instance. On enrollment, the Connector requests and receives both an identity certificate (used to authenticate itself to the ZPA infrastructure), and a server certificate issued by the intermediate CA (used to establish encrypted Microtunnels). Note that this enrollment can be done through a proxy, although this is not recommended.

## Slide 8 - Zscaler Private Access – Components



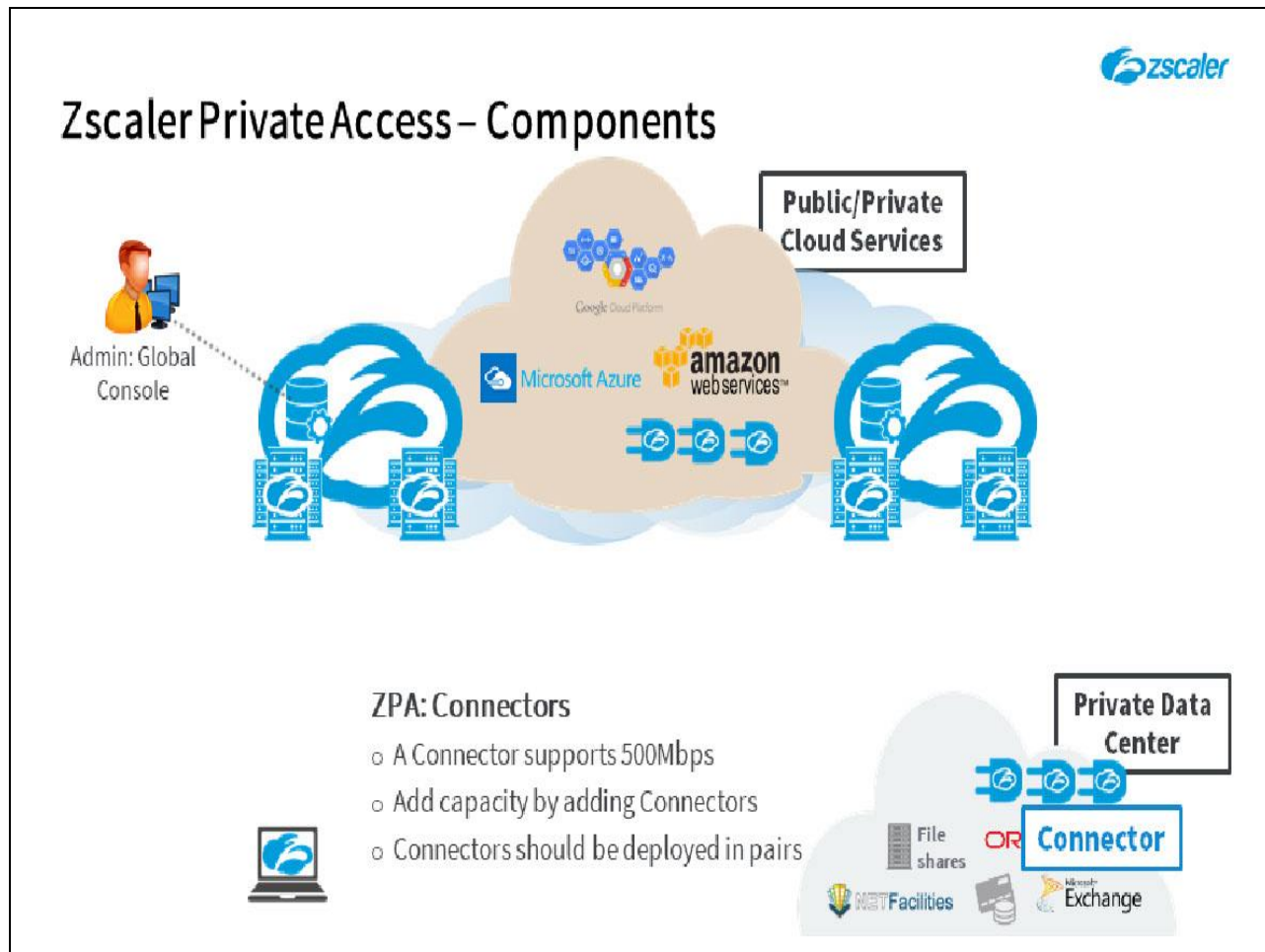
## Slide notes

Connectors are the origin point for the encrypted and doubly-pinned TLS 1.2 Z Tunnels to the ZPA-ZEN that provide access to the local applications. They are the destination for the end-to-end Microtunnels from the users that need and are authorized to access the applications.

Note that any attempt to do in-line SSL inspection of the outbound Z Tunnels from the Connectors will prevent the establishment of those tunnels, as the certificate validation will fail; this is by design.



## Slide 9 - Zscaler Private Access – Components

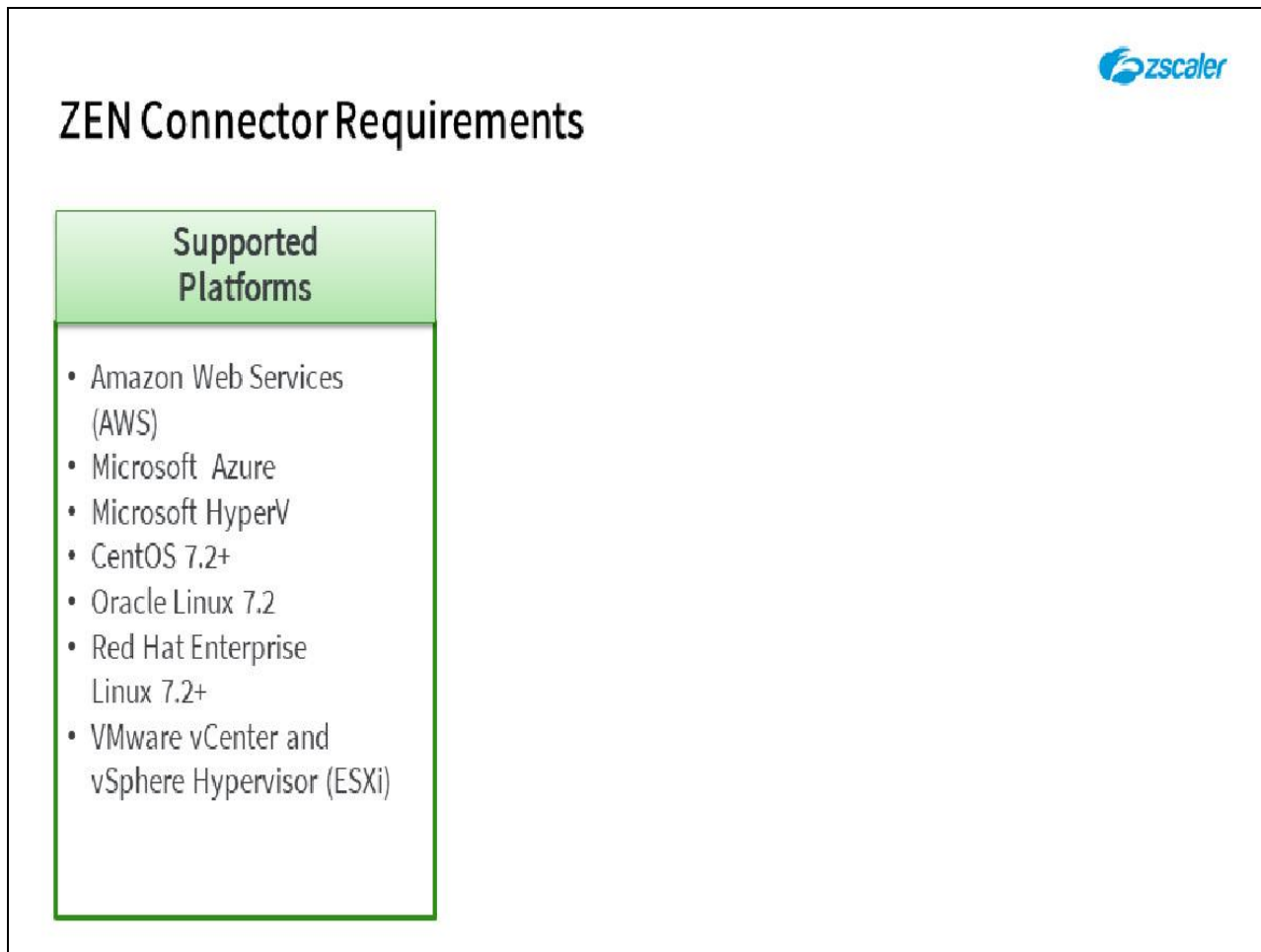


## Slide notes

Each Connector is provisioned to support up to 500Mbps of throughput, to add access capacity for your private applications simply add additional Connectors. Connectors are extremely lightweight VMs/RPMs, that boot extremely quickly, you can add one within about 15 minutes.

Note that Zscaler recommends that Connectors be deployed in pairs, to ensure continuous availability during software upgrades.

## Slide 10 - Connector Requirements



The slide features the Zscaler logo in the top right corner. The main title 'ZEN Connector Requirements' is positioned on the left. Below it, a green-bordered box titled 'Supported Platforms' contains a bulleted list of supported environments.

## ZEN Connector Requirements


**Supported Platforms**

- Amazon Web Services (AWS)
- Microsoft Azure
- Microsoft HyperV
- CentOS 7.2+
- Oracle Linux 7.2
- Red Hat Enterprise Linux 7.2+
- VMware vCenter and vSphere Hypervisor (ESXi)

## Slide notes

Check the ZPA Support Portal for current details of the supported platforms for Connector deployment. The current list includes virtual machine packages for a range of environments, including: Amazon Web Services (available as an App in the AWS EC2 Dashboard); Microsoft Azure (available within the Azure App Store), also Microsoft HyperV; CentOS 7.2+; Oracle Linux 7.2; Red Hat Enterprise Linux 7.2+; and VMware, whether as an Appliance with VMware vCenter, or a VMware Appliance with the vSphere Hypervisor (ESXi).

## Slide 11 - Connector Requirements



## ZEN Connector Requirements

Supported Platforms	Provisioning and Connectivity
<ul style="list-style-type: none"><li>• Amazon Web Services (AWS)</li><li>• Microsoft Azure</li><li>• Microsoft HyperV</li><li>• CentOS 7.2+</li><li>• Oracle Linux 7.2</li><li>• Red Hat Enterprise Linux 7.2+</li><li>• VMware vCenter and vSphere Hypervisor (ESXi)</li></ul>	<ul style="list-style-type: none"><li>• A Connector provisioning key from the ZPA Admin Portal</li><li>• DHCP or static IP configuration</li><li>• Static MAC address</li><li>• Internal connectivity on the LAN to the applications to be made available</li><li>• Outbound connectivity for TCP on port 443 (see <a href="https://ips.zscaler.net/zpa">ips.zscaler.net/zpa</a>)</li></ul>


## Slide notes

A valid Connector Provisioning Key is required, obtained from the ZPA Admin Portal.

Connectors must of course have network connectivity and may obtain their IP address and DNS Server configurations dynamically by DHCP, or they may be configured with static IPs if required. They must use static MAC addresses. The Connectors must also be able to DNS resolve both internal and external hosts. The Connectors must of course have connectivity across your internal network to the servers that host your applications.

If you choose to firewall or otherwise restrict outbound traffic to the Internet from your data center, your firewall must be configured to allow outbound communications on port 443, and to perform NAT for the source IP addresses of the Connectors. Details of the IP addresses that must be reachable can be found on the <https://ips.zscaler.net/zpa> page.

## Slide 12 - Connector Requirements



Supported Platforms	Provisioning and Connectivity	Interoperability Considerations
<ul style="list-style-type: none"><li>• Amazon Web Services (AWS)</li><li>• Microsoft Azure</li><li>• Microsoft HyperV</li><li>• CentOS 7.2+</li><li>• Oracle Linux 7.2</li><li>• Red Hat Enterprise Linux 7.2+</li><li>• VMware vCenter and vSphere Hypervisor (ESXi)</li></ul>	<ul style="list-style-type: none"><li>• A Connector provisioning key from the ZPA Admin Portal</li><li>• DHCP or static IP configuration</li><li>• Static MAC address</li><li>• Internal connectivity on the LAN to the applications to be made available</li><li>• Outbound connectivity for TCP on port 443 (see <a href="https://ips.zscaler.net/zpa">ips.zscaler.net/zpa</a>)</li></ul>	<ul style="list-style-type: none"><li>• Avoid any encapsulation (IPSec, GRE) that may interfere with the use of a standard 1500Byte MTU (including Zscaler Internet Access tunnels)</li><li>• Disable all forms of inline or man-in-the-middle TLS interception or inspection (default exemption on the ZIA service)</li></ul>


## Slide notes

In addition, to ensure interoperability with other security products and services (including the Zscaler Internet Access service), we recommend you do not send Connector traffic through an existing Zscaler tunnel (IPsec, GRE, etc.), or through any form of encapsulation that may interfere with the use of a standard **1500Byte MTU**.

Also, because the system enforces TLS certificate pinning for both client and server certificates, all forms of inline or man-in-the-middle TLS interception or inspection must be disabled. Connectors will not function at all if the TLS certificates presented by the ZPA-ZENs cannot be cryptographically verified against Zscaler-trusted public keys. The certificate verification process is not configurable by design in order to maintain the integrity of the system.

Note that when using the ZIA service and SSL Inspection, ZPA destinations are exempted by default.

## Slide 13 - Connector Sizing, Scaling, and Throughput



## Connector Sizing, Scaling, and Throughput


### ZEN Connector Sizing

- A Connector supports up to 500Mbps of data
- Connector VM sizing:
  - 4 GB RAM
  - 2 CPU cores (Xeon E5 class) or 4 cores with Hyperthreading for VMs
  - 8 GB Disk Space (thin provisioned)
  - 1 NIC

**Slide notes**

A single Connector can support up to 500Mbps of aggregate data, which includes overhead traffic and application connectivity. When implementing a Connector, plan for the following resources: 4GB RAM; 2 Xeon E5 class CPU cores (4 cores with Hyperthreading for VM Connectors); 8GB Disk Space (thin provisioned); and at least 1 NIC.

## Slide 14 - Connector Sizing, Scaling, and Throughput



## Connector Sizing, Scaling, and Throughput


ZEN Connector Sizing	ZEN Connector Scaling
<ul style="list-style-type: none"><li>• A Connector supports up to 500Mbps of data</li><li>• Connector VM sizing:<ul style="list-style-type: none"><li>◦ 4 GB RAM</li><li>◦ 2 CPU cores (Xeon E5 class) or 4 cores with Hyperthreading for VMs</li><li>◦ 8 GB Disk Space (thin provisioned)</li><li>◦ 1 NIC</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Scale access capacity by adding Connectors</li><li>• This also adds redundancy and resilience</li><li>• Use dedicated Connectors for Log Streaming</li></ul>

## Slide notes


While it would be possible to improve throughput for a single Connector by increasing the resources allocated to the VM, this is not recommended. We recommend that you have more Connectors with lower specifications, rather than fewer Connectors with higher specifications in order to horizontally scale your deployment. For example, if you have fewer, larger Connectors and one fails, you could adversely affect more user application traffic/sessions than for a smaller Connector that fails.

If you plan to use the ZPA **Log Streaming Service**, deploy additional Connectors adjacent to your SIEM just for this purpose. This avoids any possibility of contention between user traffic and log streaming.

## Slide 15 - Connector Sizing, Scaling, and Throughput



## Connector Sizing, Scaling, and Throughput


ZEN Connector Sizing	ZEN Connector Scaling
<ul style="list-style-type: none"><li>• A Connector supports up to 500Mbps of data</li><li>• Connector VM sizing:<ul style="list-style-type: none"><li>◦ 4 GB RAM</li><li>◦ 2 CPU cores (Xeon E5 class) or 4 cores with Hyperthreading for VMs</li><li>◦ 8 GB Disk Space (thin provisioned)</li><li>◦ 1 NIC</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Scale access capacity by adding Connectors</li><li>• This also adds redundancy and resilience</li><li>• Use dedicated Connectors for Log Streaming</li></ul>  <p>Deploy Connectors in pairs to allow seamless upgrades</p>

## Slide notes


Using more Connectors also adds redundancy and resilience, and we recommend that you deploy them at least in pairs, to ensure minimal disruption when Connector SW is being updated.



## Slide 16 - Connector Sizing, Scaling, and Throughput



## Connector Sizing, Scaling, and Throughput

ZEN Connector Sizing	ZEN Connector Scaling	ZEN Connector Throughput
<ul style="list-style-type: none"><li>• A Connector supports up to 500Mbps of data</li><li>• Connector VM sizing:<ul style="list-style-type: none"><li>◦ 4 GB RAM</li><li>◦ 2 CPU cores (Xeon E5 class) or 4 cores with Hyperthreading for VMs</li><li>◦ 8 GB Disk Space (thin provisioned)</li><li>◦ 1 NIC</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Scale access capacity by adding Connectors</li><li>• This also adds redundancy and resilience</li><li>• Use dedicated Connectors for Log Streaming</li></ul> <div style="text-align: center; margin-top: 20px;"><p style="margin: 0;"><b>Deploy Connectors in pairs to allow seamless upgrades</b></p></div>	<ul style="list-style-type: none"><li>• Background traffic:<ul style="list-style-type: none"><li>◦ Keepalives to the ZPA ZENs</li><li>◦ Application learning</li><li>◦ Application health reporting</li><li>◦ ZPA software upgrades (weekly)</li></ul></li><li>• Double encryption has an impact on Connector throughput<ul style="list-style-type: none"><li>◦ 50% of applications &gt; throughput is 375Mbps</li><li>◦ 100% of applications &gt; throughput is 250Mbps</li></ul></li></ul>


**Slide notes**

The available Connector throughput is also used for some background, system-related traffic, such as: Periodic Keepalives to ZPA-ZENs; application learning; application health reporting; Connector software upgrades (which happens weekly).

The double encryption feature does have an impact on throughput, depending on the percentage of your private applications that it is enabled for. It is a linear relationship, and if all of your applications use it, then Connector throughput is reduced to 250Mbps.



## Slide 17 - Connector Provisioning



## Connector Provisioning

### Provisioning Keys

- A text string generated when you provision a new Connector
- When deploying a Connector, you are prompted to enter this key
- Allows the ZPA Cloud to verify the Connector's authenticity
- The Provisioning Key identifies the Connector Group
- Configurable max use count


## Slide notes

The Connector **Provisioning Key** is a text string that is generated when you provision a new Connector at the Admin Portal. When deploying the Connector VM, you are prompted to enter this key. The Provisioning Key functions like an ID for the Connector, enabling the ZPA cloud to verify the Connector's authenticity and complete the deployment process.

Provisioning Keys are designed to enable auto-scaling so that you can easily deploy additional Connectors and respond quickly to increases in your available capacity. When generating a Provisioning Key, you can specify the number of times it can be used to deploy Connectors, and once you reach this limit you cannot use the key any more, although it is possible to edit this number at any time. ZPA tracks the number of times a key is used to deploy a Connector and displays this information on the **Connector Provisioning Keys** page.

Note that, provisioning keys are considered confidential information and must be kept in a safe place. For each provisioning key, a **COPY KEY** option is provided so that you can copy the key to your clipboard.

## Slide 18 - Connector Provisioning



## Connector Provisioning

### Provisioning Keys

- A text string generated when you provision a new Connector
- When deploying a Connector, you are prompted to enter this key
- Allows the ZPA Cloud to verify the Connector's authenticity
- The Provisioning Key identifies the Connector Group
- Configurable max use count

### Connector Group

- Each Provisioning Key must be associated to a Connector Group
- A Connector Group may have multiple Provisioning Keys associated
- Edit Connector update schedule

## Slide notes

Each key is associated to a specific Connector group, so the key also allows the ZPA Cloud to identify the Connector group to which a Connector must be deployed. Note that it is possible to associate multiple Provisioning Keys to a single Connector group. One of the configuration settings available on a Connector group, is the schedule for updating the associated Connectors. Connectors within a group are updated on a round robin basis, to ensure that not all Connectors will be down for a SW update at the same time.

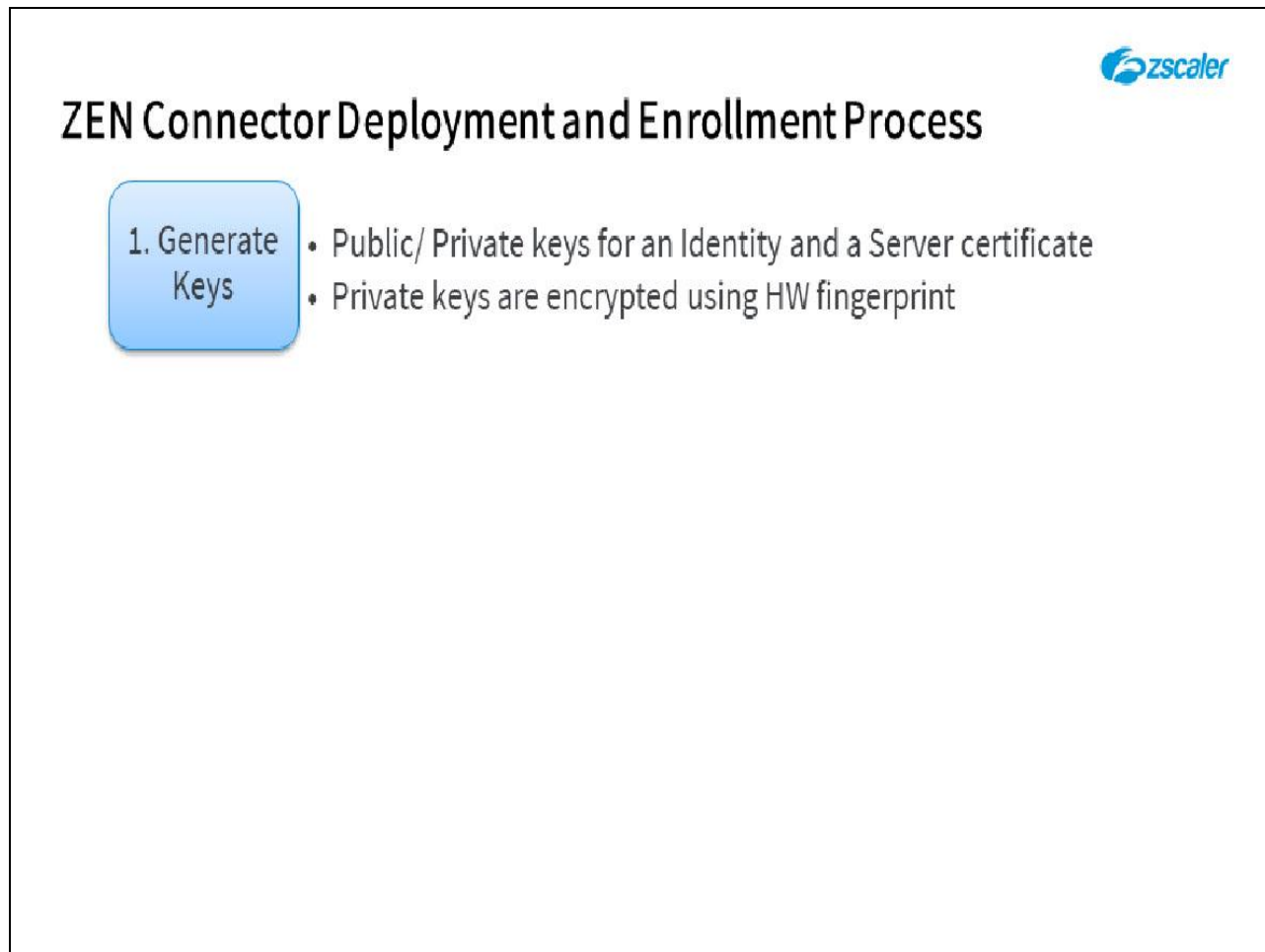
Slide 19 - Virtual Appliance Requirements



Slide notes


The next topic that we will cover is the Connector installation and provisioning process.

## Slide 20 - Connector Deployment and Enrollment Process



The slide features the Zscaler logo in the top right corner. The main title is "ZEN Connector Deployment and Enrollment Process". Below the title, there is a blue rounded rectangle containing the text "1. Generate Keys". To the right of this rectangle, there is a bulleted list: "• Public/ Private keys for an Identity and a Server certificate" and "• Private keys are encrypted using HW fingerprint".

## ZEN Connector Deployment and Enrollment Process



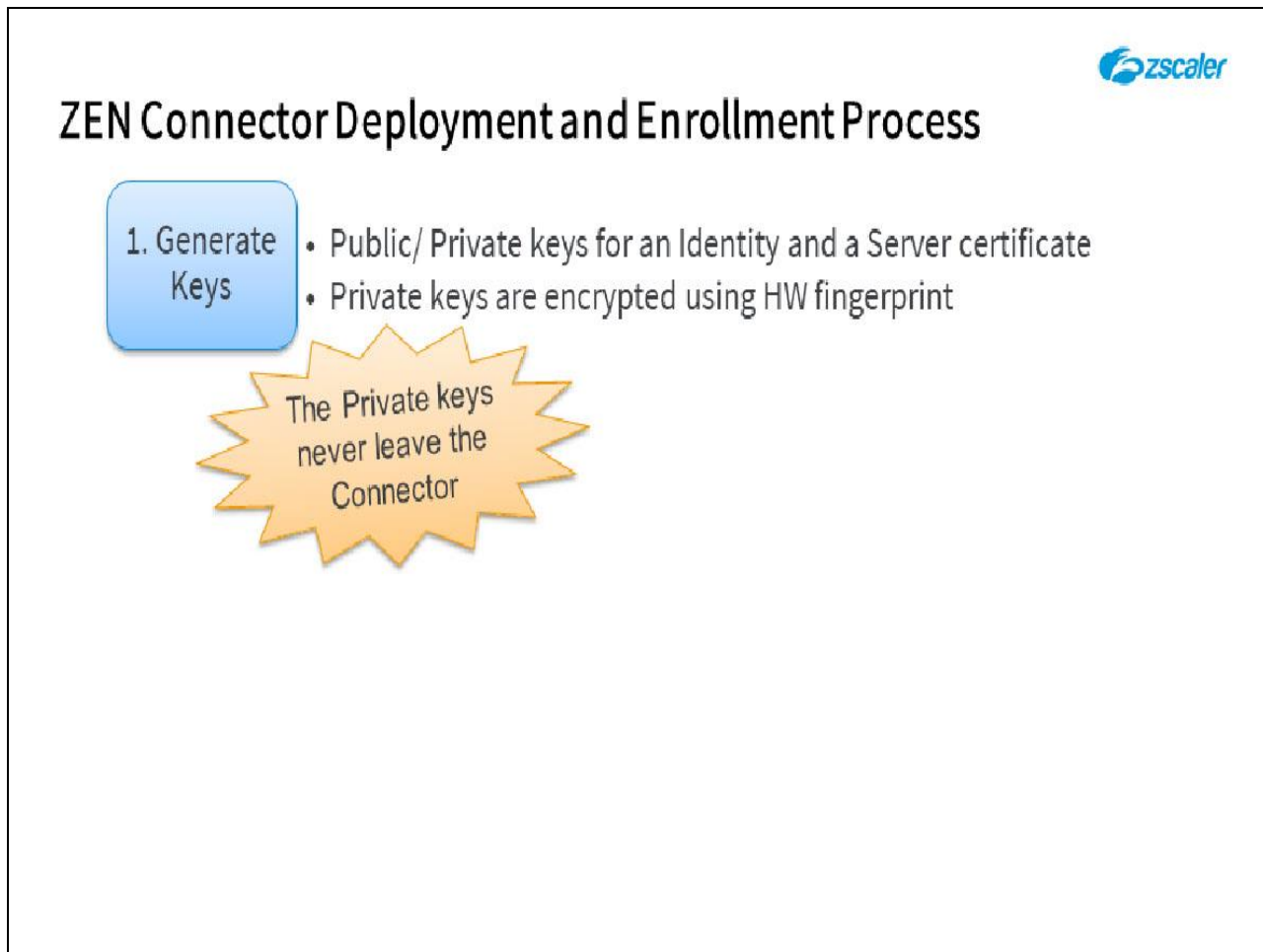
1. Generate Keys
  - Public/ Private keys for an Identity and a Server certificate
  - Private keys are encrypted using HW fingerprint

**Slide notes**

Deploying a Connector consists of installing the Connector SW or image then enrolling the Connector with the correct ZPA instance, which then allows the Connector to obtain the TLS client certificate that it must use to authenticate itself to the ZPA cloud. The Connector also receives a server certificate on enrollment to allow it to establish the end-to-end Microtunnels when double encryption is required. After deployment, the Connector is ready to securely connect users to applications.

When the Connector is powered up for the first time, it does not yet have either of the key pairs that it requires, so the first thing it does is to generate its own public/private key pairs. The private keys are encrypted using a hardware fingerprint and stored locally.

## Slide 21 - Connector Deployment and Enrollment Process



The slide features the Zscaler logo in the top right corner. The main title is "ZEN Connector Deployment and Enrollment Process". Below the title, a blue rounded rectangle contains the text "1. Generate Keys". To the right of this rectangle is a bulleted list: "• Public/ Private keys for an Identity and a Server certificate" and "• Private keys are encrypted using HW fingerprint". Below the list is a yellow starburst shape containing the text "The Private keys never leave the Connector".

## ZEN Connector Deployment and Enrollment Process

1. Generate Keys

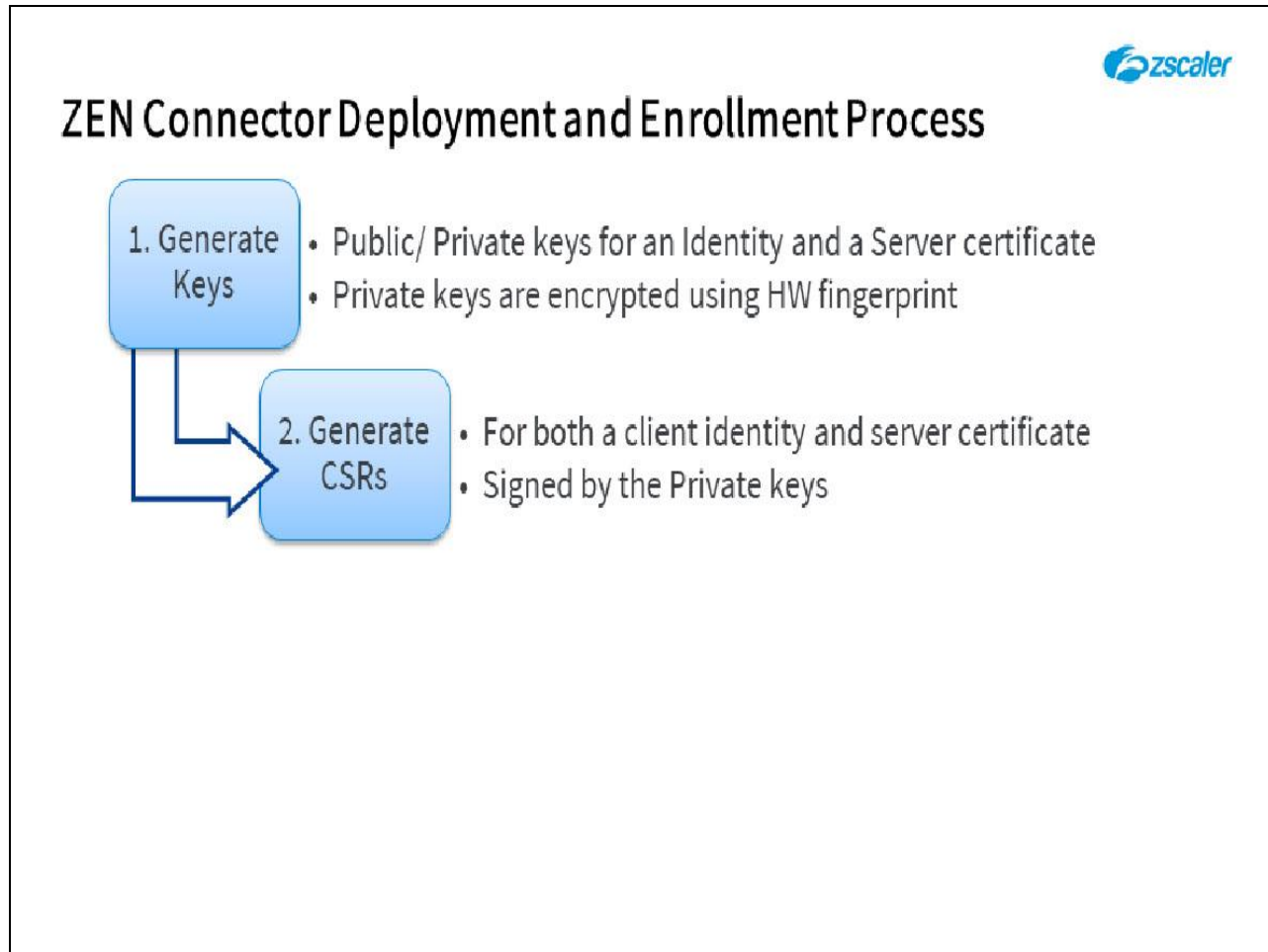
- Public/ Private keys for an Identity and a Server certificate
- Private keys are encrypted using HW fingerprint

The Private keys never leave the Connector

## Slide notes

Note that, in accordance with industry best practices, the Connector generates its own keys, and that the private key is encrypted and stored locally on the Connector. It is never shared with any other network entity.

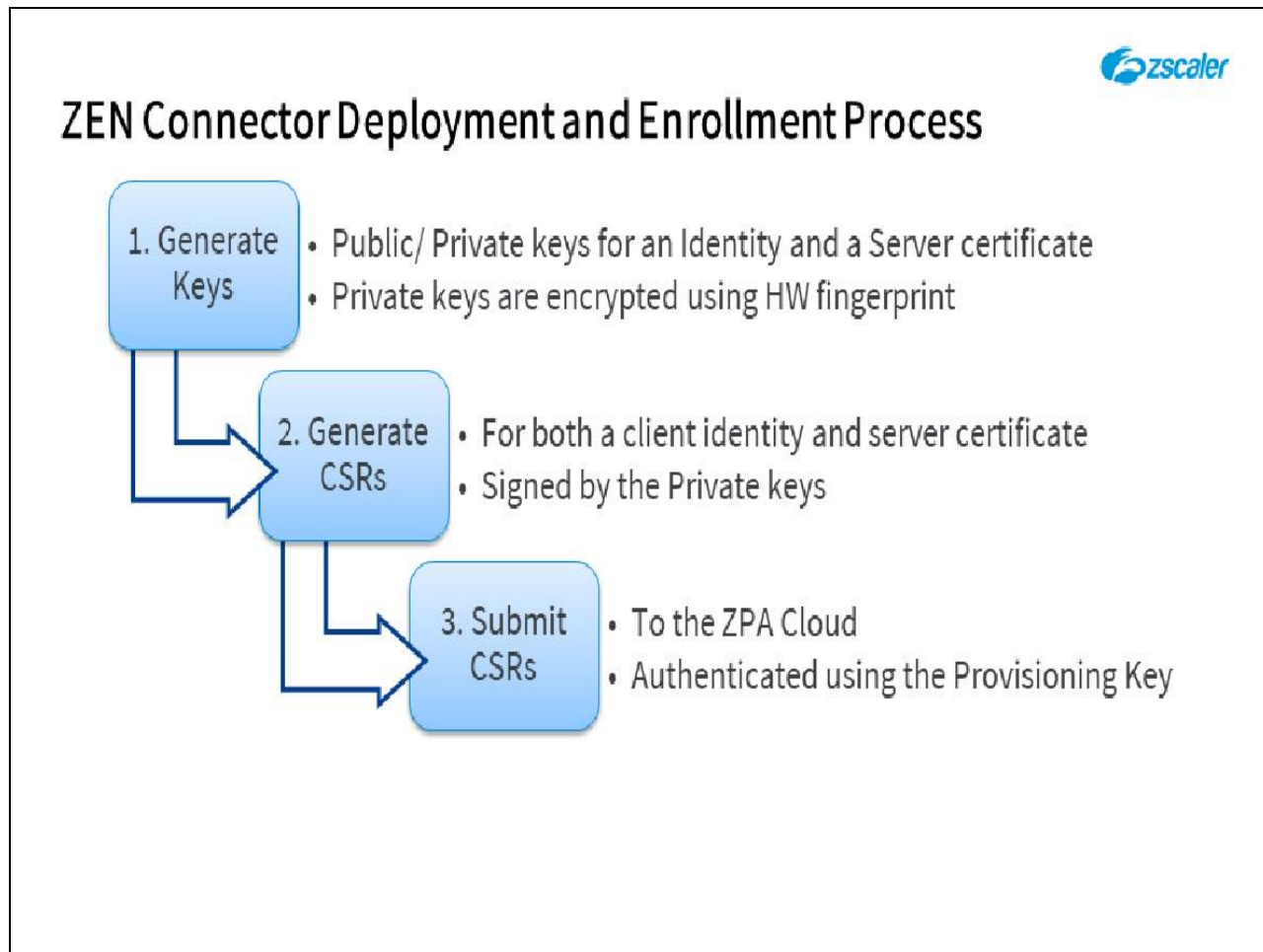
## Slide 22 - Connector Deployment and Enrollment Process



## Slide notes

The Connector must then obtain a TLS client identity certificate, and a server certificate through an enrollment process, the first step of which is to use its local private key to generate Certificate Signing Requests (CSR).

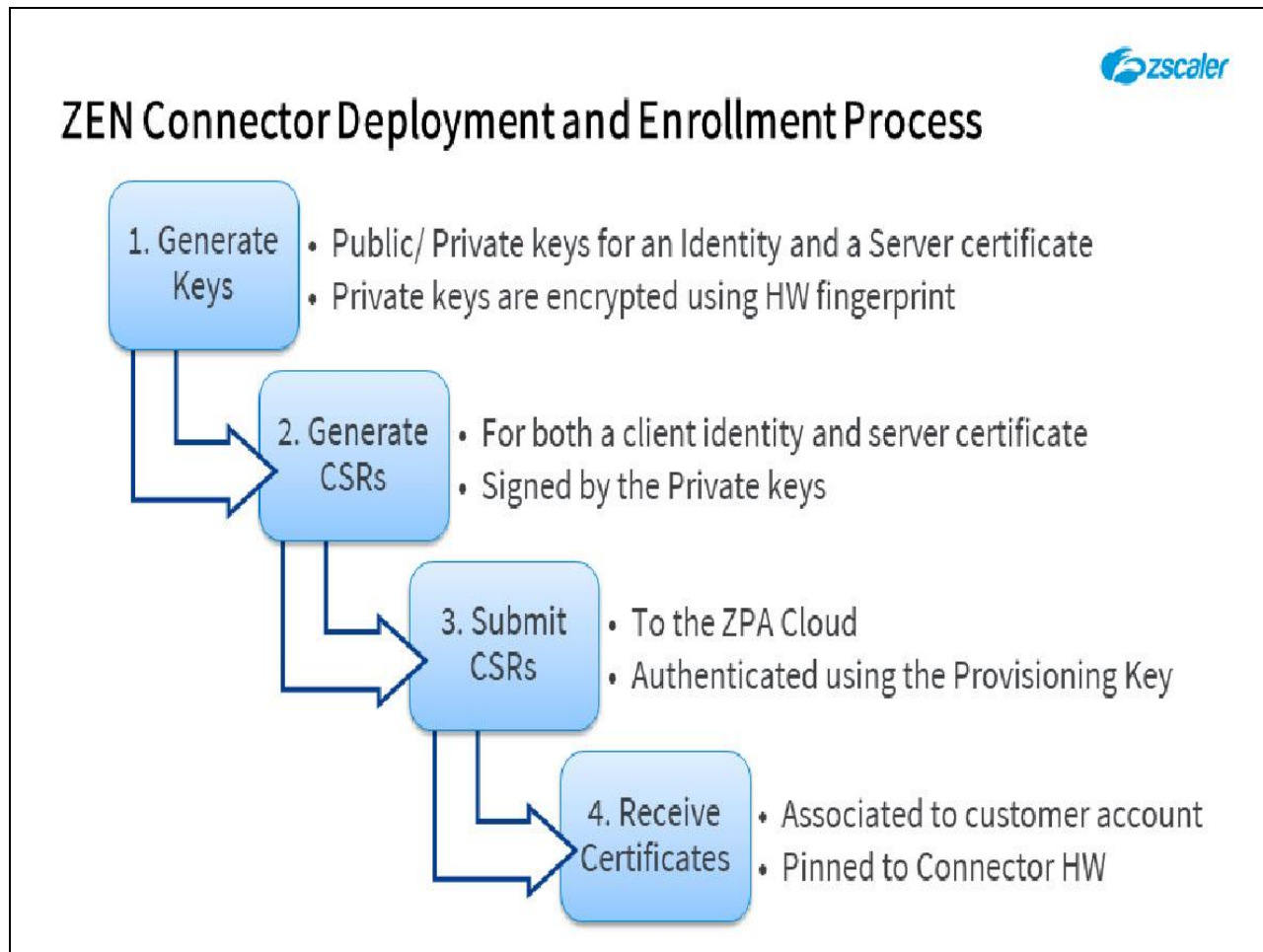
## Slide 23 - Connector Deployment and Enrollment Process



## Slide notes

It then uses its Provisioning Key to authenticate the CSR to the ZPA Cloud (this is the Provisioning Key which you generated in the ZPA Admin Portal and provided for the Connector during installation). The Provisioning Key was signed by the intermediate CA on the ZPA instance and can be validated by the ZPA Cloud Central Authority.

## Slide 24 - Connector Deployment and Enrollment Process




## Slide notes

Finally, it receives both a signed TLS client identity certificate, and a signed server certificate from the ZPA Cloud. The certificates are pinned to the Connector's hardware fingerprint and are paired with a single customer account.

Connectors that are running in virtual machine environments cannot be cloned, as the keys will no longer match the virtual hardware fingerprints.



## Slide 25 - Connector SW Update



## Connector SW Update

### Automatic SW Updates


- Managed at the Connector Group level
  - Updates occur within a 4 hour window
  - Start time for the update window is specified on the Connector Group
- Process:
  - Random Connector selected for update
    - Connector stops receiving new connections
    - Connector waits 5 minutes
  - Once upgrade is complete another Connector is selected for update
  - Repeat until all Connectors have been updated

**Slide notes**

Automatic Connector SW updates are managed at the Connector Group level. A configuration option for a Connector Group is the start time for a 4-hour update window within which the Connectors will each be updated. A Connector from the group is selected at random for update. It stops accepting any new connections and waits 5 minutes for existing connections to timeout. Once the update is complete (a few minutes only) another Connector is chosen and updated, and so on until all Connectors in the group have been updated.

Note that, during an update the Connector must restart and becomes unavailable for a short interval. During this interval, any new application access request is redirected to the other Connectors in the Connector Group.

## Slide 26 - Connector SW Update



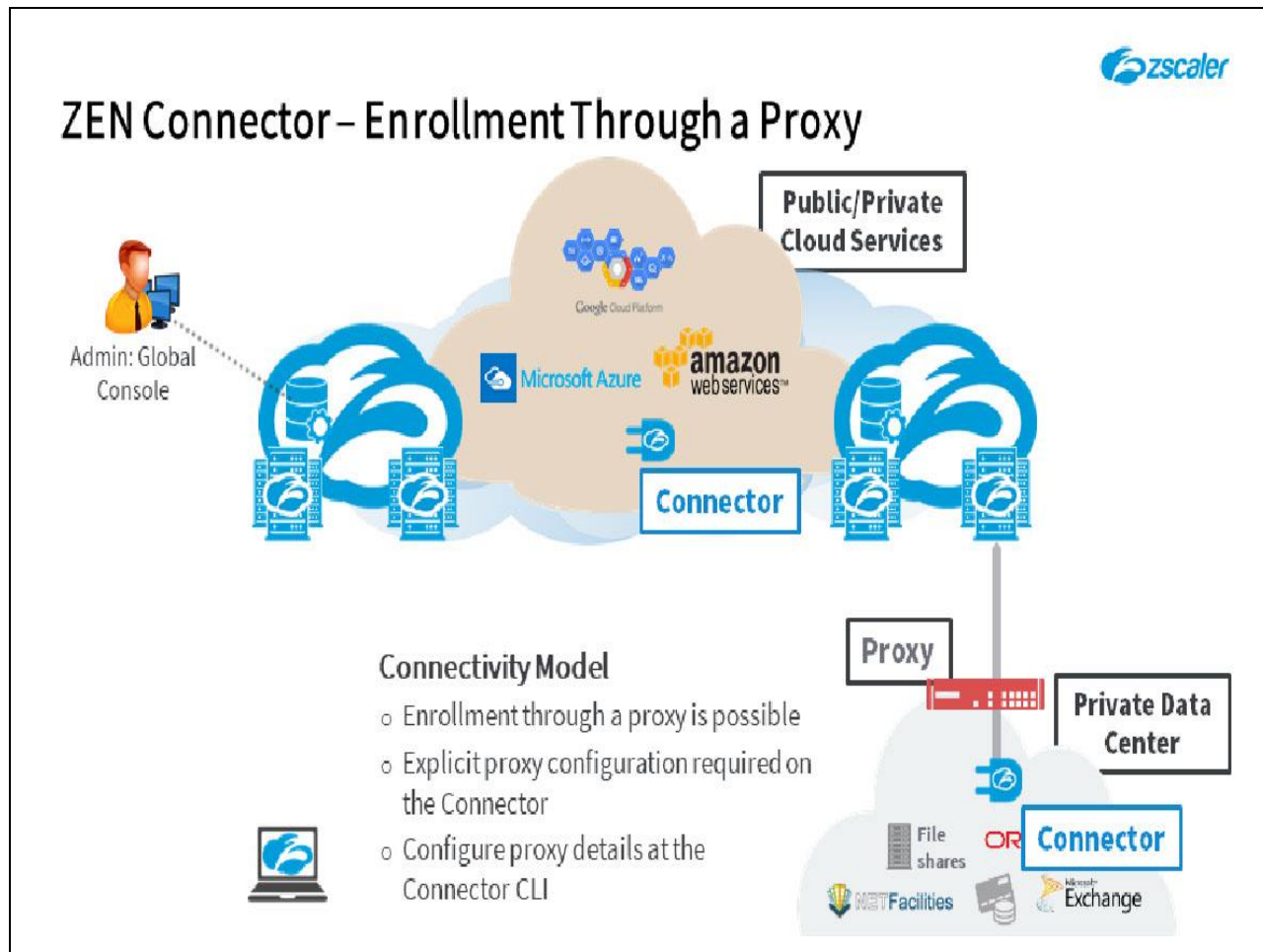
## Connector SW Update

Automatic SW Updates	Manual SW Update
<ul style="list-style-type: none"><li>• Managed at the Connector Group level<ul style="list-style-type: none"><li>◦ Updates occur within a 4 hour window</li><li>◦ Start time for the update window is specified on the Connector Group</li></ul></li><li>• Process:<ul style="list-style-type: none"><li>◦ Random Connector selected for update<ul style="list-style-type: none"><li>▪ Connector stops receiving new connections</li><li>▪ Connector waits 5 minutes</li></ul></li><li>◦ Once upgrade is complete another Connector is selected for update</li><li>◦ Repeat until all Connectors have been updated</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Recommended following Connector installation</li><li>• From the UI:<ul style="list-style-type: none"><li>◦ Connector must be <b>Scheduled</b> for an update</li><li>◦ Use the <b>Update Now</b> option</li></ul></li><li>• From the CLI:<ul style="list-style-type: none"><li>◦ When accessing the Connector CLI, use the commands <code>sudo yum update -y</code> <code>Sudo reboot</code></li></ul></li></ul>

## Slide notes

The Connectors can also be updated manually, and it is recommended that you do this as soon as possible after deploying a new Connector. This can be done from the Admin Portal (as long as the Connector indicates that it is **Scheduled** for an update), by using the **Update Now** option. From the Connector CLI, you can force an immediate SW update using the commands: **sudo yum update -y**, followed by **sudo reboot**.

## Slide 27 - Connector – Enrollment Through a Proxy



## Slide notes

Note that Connector enrollment through a proxy although not recommended, can be done when necessary, for example in a “no default route” environment. Although note that the proxy must not authenticate requests from the Connectors and any form of in-line inspection will prevent the Connector enrolling and establishing Z Tunnels to the ZPA public infrastructure. The details for the proxy must be explicitly configured at the Connector CLI.

## Slide 28 - Connector Enrollment Through a Proxy



## Connector Enrollment Through a Proxy

- To configure the Connector to work through an explicit proxy:
  1. Log in to the Connector console
  2. Create a file named `/opt/zscaler/var/proxy`
  3. Add to the file an entry of the form:  
`<Proxy Hostname>:<Proxy Port> or <Proxy IP Address>:<Proxy Port>`
  1. Restart the Connector with the following command:  
`sudo systemctl restart zpa-connector`
- The Connector attempts to create a TLS session through the proxy specified in step 3

### Slide notes

To configure the Connector to work through an explicit proxy, log in to the Connector console and create a file named `/opt/zscaler/var/proxy`. Add an entry to the file of the form `<Proxy Hostname>:<Proxy Port>` or `<Proxy IP Address>:<Proxy Port>` and save the file. Restart the Connector with the command `sudo systemctl restart zpa-connector`, and the Connector will reboot and attempt to establish a TLS connection to the closest healthy ZPA-ZEN through the proxy specified in the file.

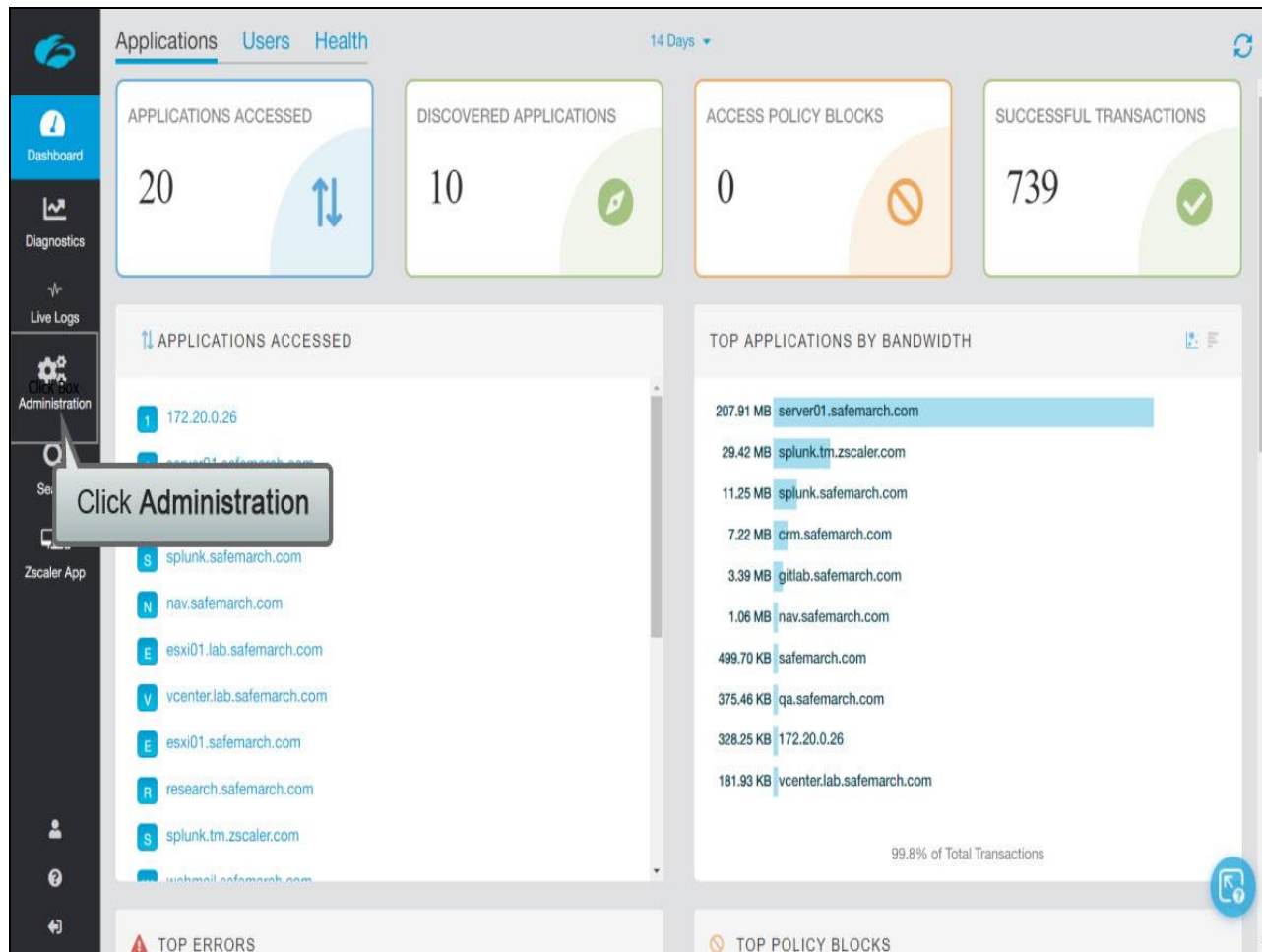
## Slide 29 - Connector Provisioning

**Slide notes**

The final topic that we will cover is how to provision a Connector in the ZPA Admin Portal.

This section has been created as an interactive demo to give you a feel for the navigation of the ZPA Admin Portal. 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 30 - Slide 30



## Slide notes

To expand the configuration menu options, click **Administration**, ...

## Slide 31 - Slide 31

The screenshot displays the Adobe Captivate console interface. On the left is a dark sidebar with navigation options: Dashboard, Diagnostics, Live Logs, Administration, Search, Zscaler App, and a bottom section with user and settings icons. The main content area is divided into several sections. The top section, 'APPLICATION MANAGEMENT', includes 'Application Segments', 'Segment Groups', 'Servers', 'Browser Access', and 'Server Groups'. Below this is the 'AUTHENTICATION' section with 'IdP Configuration' and 'SAML Attributes Settings'. The 'CERTIFICATE MANAGEMENT' section includes 'Browser Access Certificates' and 'Enrollment Certificates'. The 'CONNECTOR MANAGEMENT' section is highlighted, showing 'Connectors', 'Connector Groups', and 'Connector Provisioning Keys'. A callout box with the text 'Click Connectors' points to the 'Connectors' link. Below this are 'Connector Groups' and 'Log Receivers'. The 'POLICY MANAGEMENT' section includes 'Access Policy' and 'Timeout Policy'. The 'SETTINGS' section is at the bottom. The main content area also features a top summary bar with '14 Days' and a refresh icon. Below this are three summary cards: 'APPLICATIONS' (0), 'ACCESS POLICY BLOCKS' (0), and 'SUCCESSFUL TRANSACTIONS' (739). The 'TOP APPLICATIONS BY BANDWIDTH' section lists various domains and their bandwidth usage, with 'server01.safemarch.com' at the top (207.91 MB). The bottom of the main content area shows 'TOP POLICY BLOCKS'.

Click Connectors

## Slide notes

...then to add a new Connector, click **Connectors**.

## Slide 32 - Slide 32

The screenshot shows the Adobe Captivate interface with the 'Connectors' tab selected. The table lists various connectors and their status. A callout box highlights the '+ icon' at the top right of the table, indicating where to click to add a new connector.

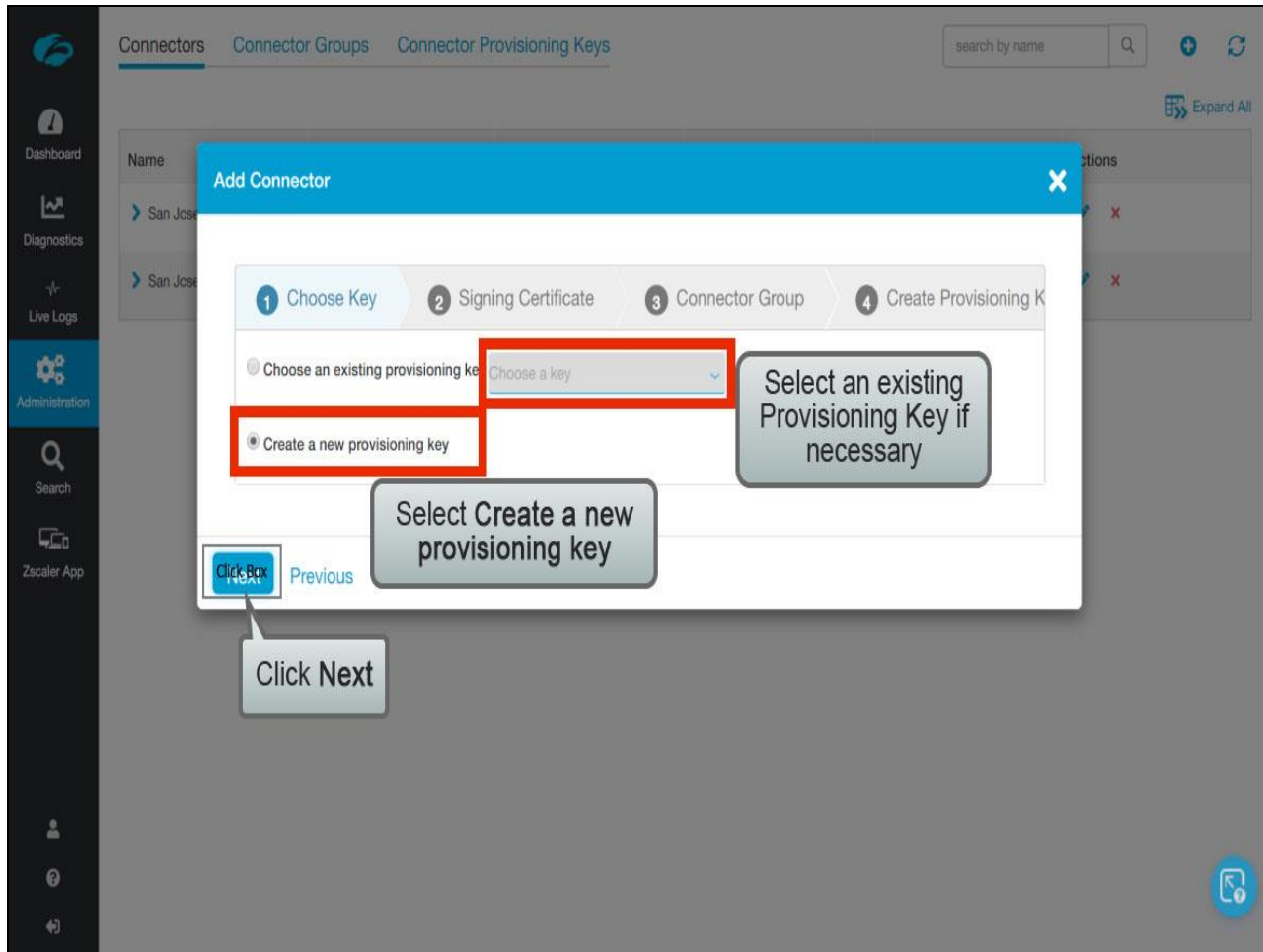
Name	Status	Session	Update Status	Current Software
Amsterdam Connector 1	✖	Disconnected	Success ⓘ	16.86.1
AWS Prov-4	✔	Disconnected		
AWS US-West Connector 1	✔	Authenticated	Success ⓘ	19.20.3
AWS US-West Connector 2	✔	Authenticated	Success ⓘ	19.20.3
Azure East-US-1	✔	Authenticated	Success ⓘ	19.20.3
Azure US-Central-South-1	✔	Authenticated	Success ⓘ	19.20.3
Log Streaming Service-1	✖	Disconnected	Success ⓘ	17.62.2
Log Streaming Service San Jose-1	✔	Authenticated	Success ⓘ	19.20.3
San Francisco Connector 1	✖ ⓘ	Disconnected		
San Jose Connector 3	✔	Authenticated	Success ⓘ	19.20.3
San Jose Connector 4	✔	Authenticated	Success ⓘ	19.20.3

## Slide notes

The **Connectors** page lists only the Connectors that have been successfully activated. To add a new Connector, click the + icon at top right.



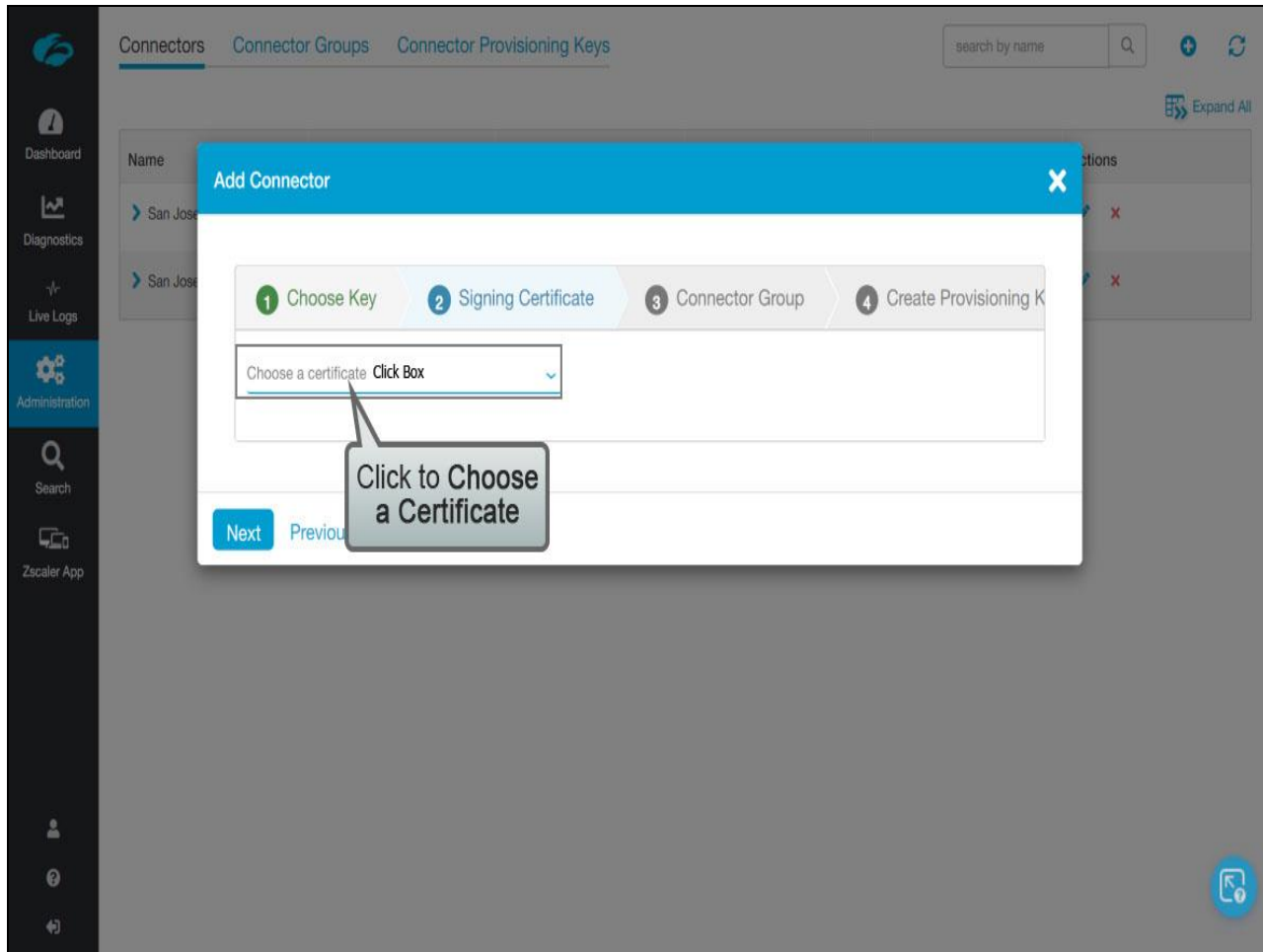
## Slide 33 - Slide 33



## Slide notes

At Step 1 of the **Add Connector** wizard, if you previously created a Connector provisioning key and wish to re-use it, select the key here. Alternatively, select the **Create a new provisioning key** option, then click **Next**.

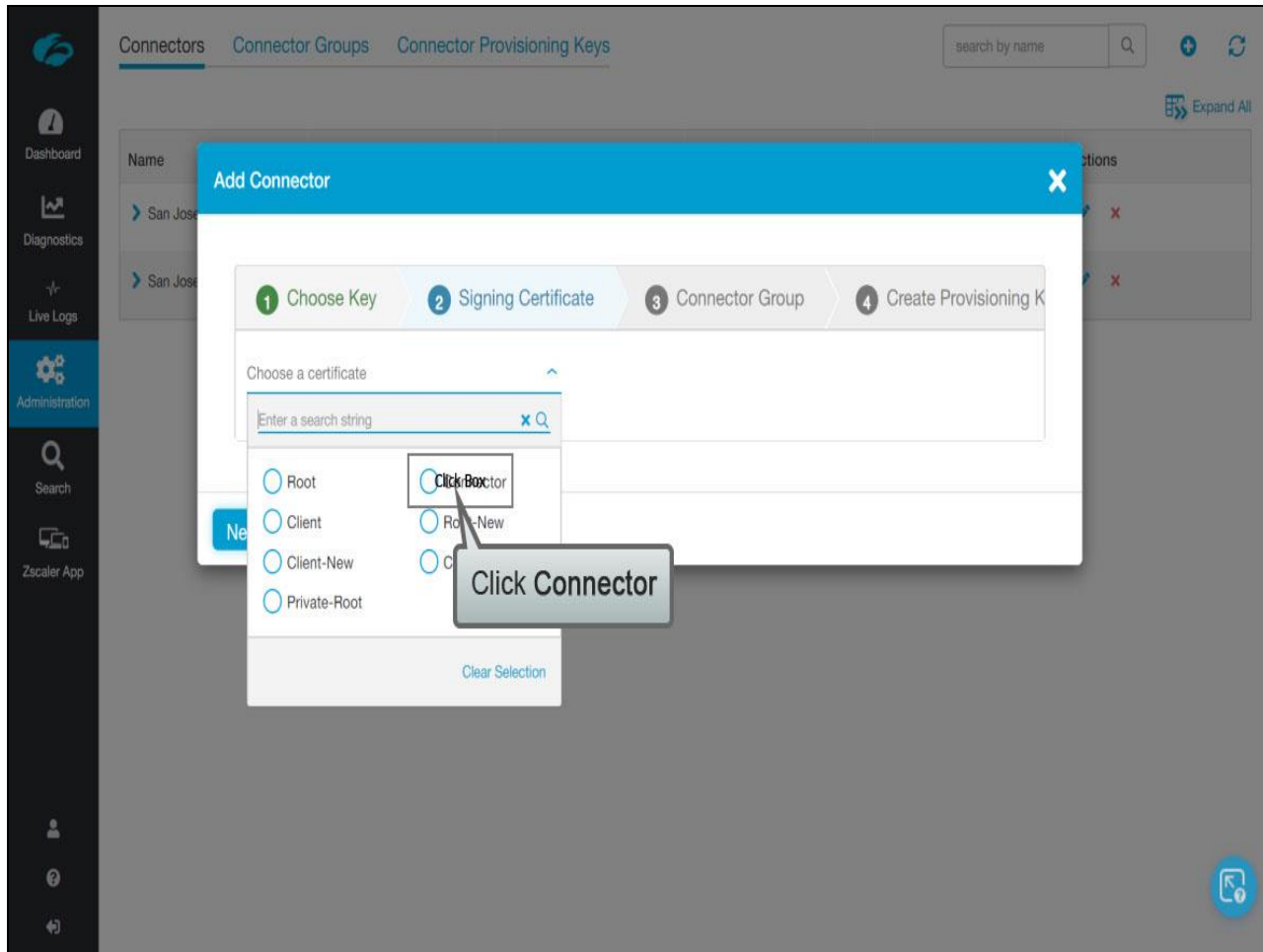
## Slide 34 - Slide 34



## Slide notes

To select the Intermediate CA to issue certificates to this Connector on enrollment, click **Choose a Certificate**, ...

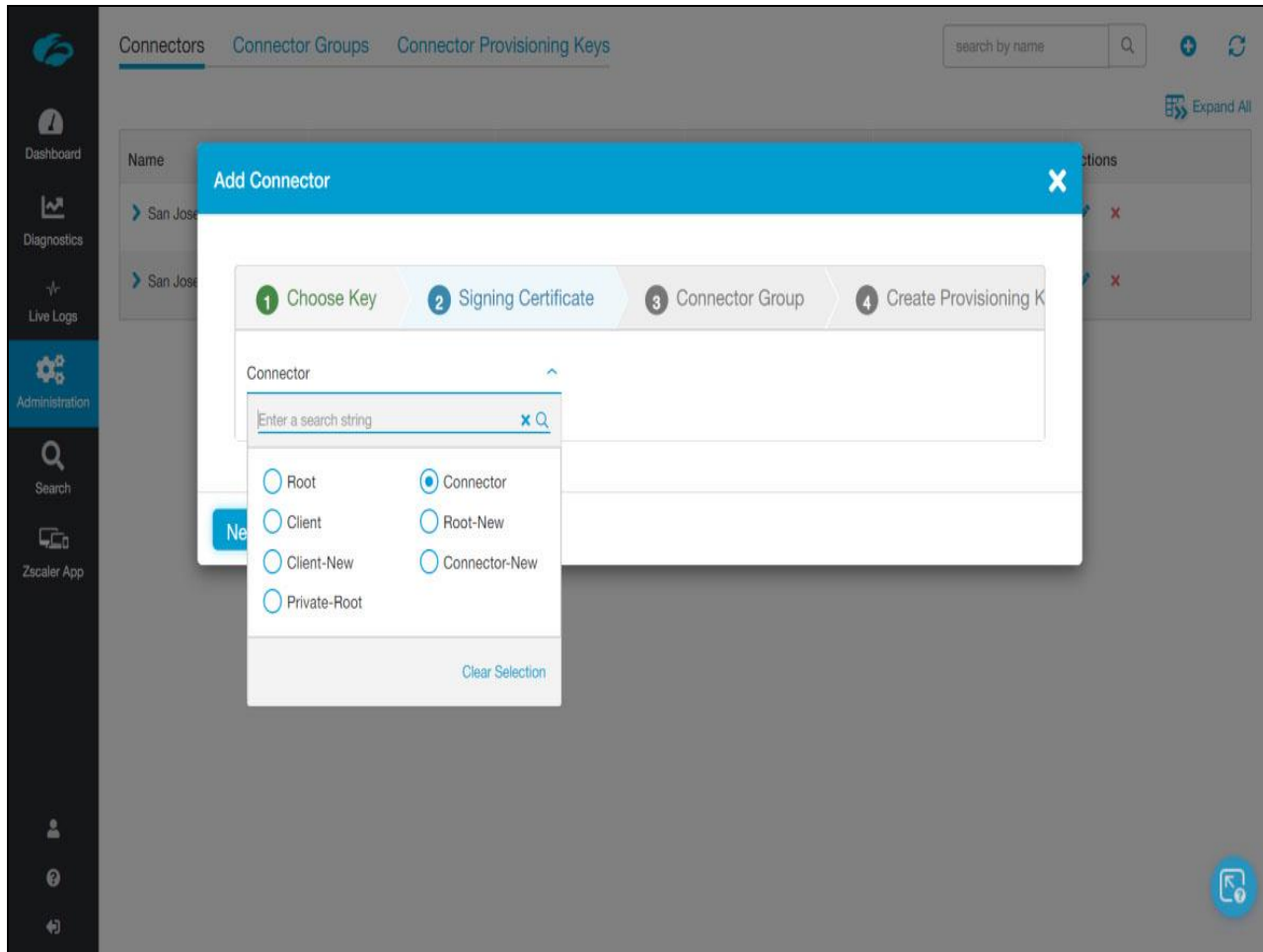
## Slide 35 - Slide 35



## Slide notes

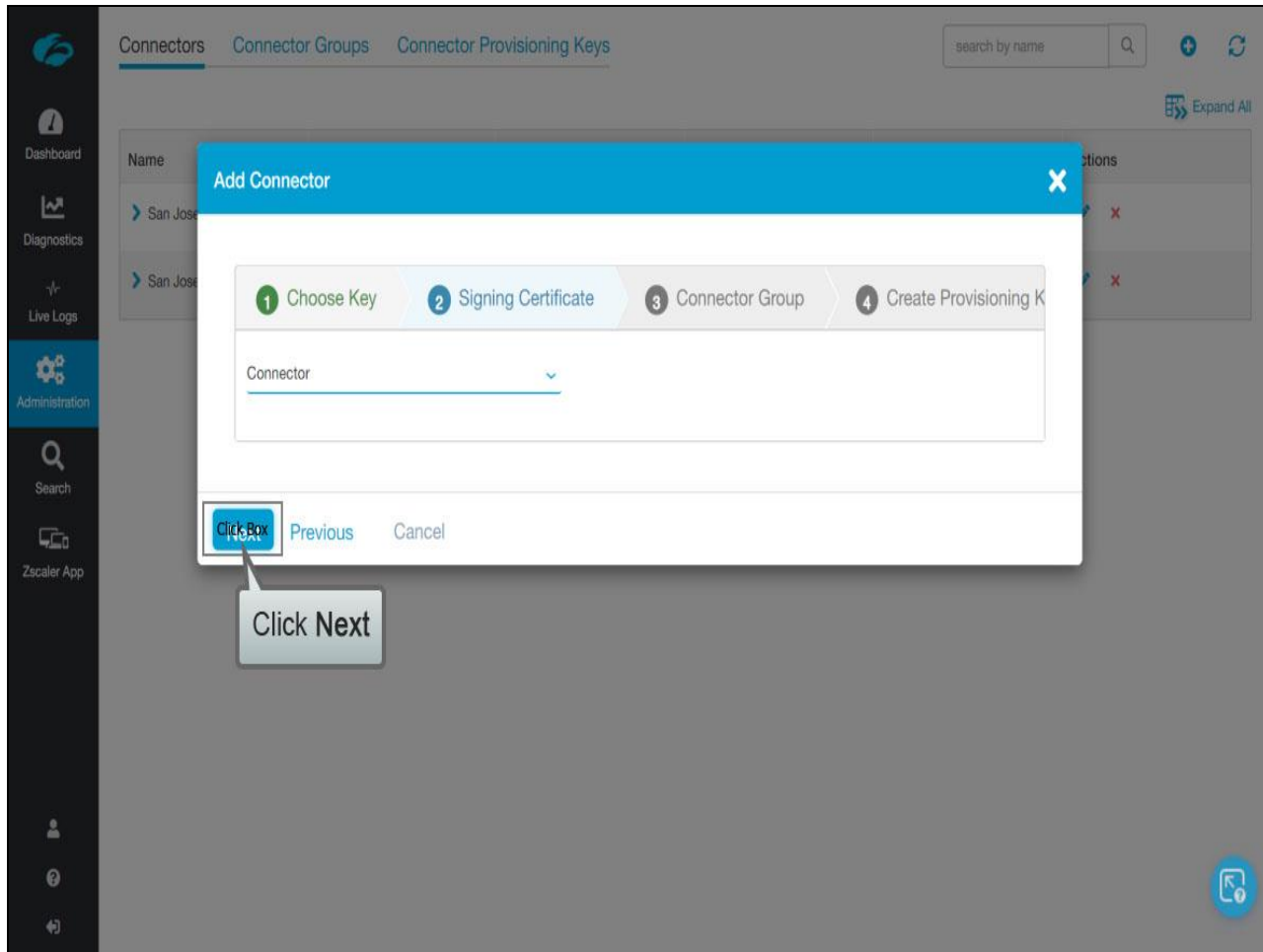
...and select the certificate to be used for this Connector, from the list of certificates available by default or that you created.

## Slide 36 - Slide 36



## Slide notes

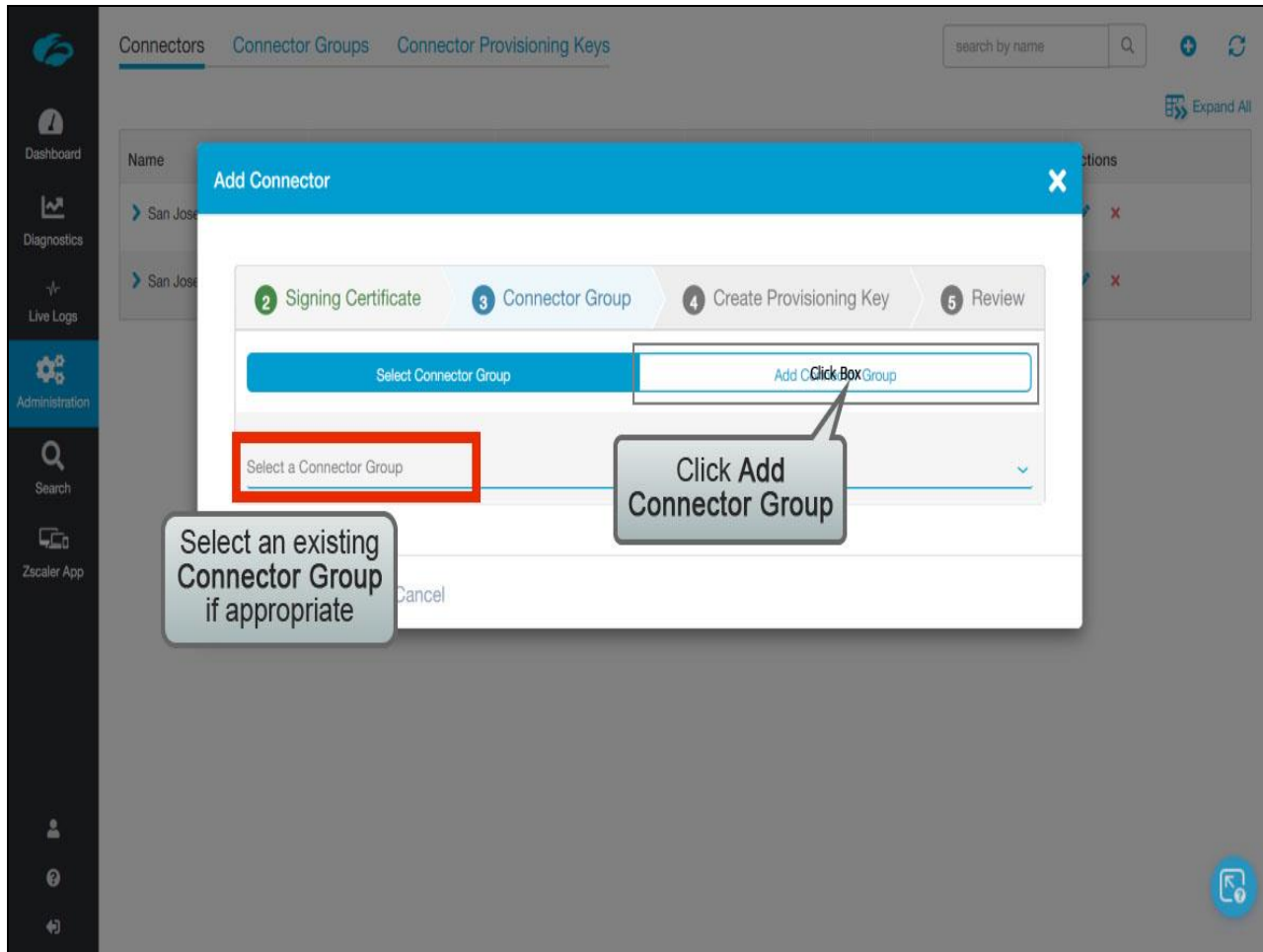
## Slide 37 - Slide 37



## Slide notes

Having selected the appropriate certificate, click **Next** to continue with the Connector provisioning wizard.

## Slide 38 - Slide 38



## Slide notes

If you have previously created a **Connector Group**, select it here; or click **Add Connector Group**.

## Slide 39 - Slide 39

**Add Connector**

2 Signing Certificate 3 Connector Group 4 Create Provisioning Key 5 Review

Select Connector Group Add Connector Group

**Name**  
Sentinel Group

**Description**  
Group for Sentinel Connectors

**Status**  
☒ Enabled ☐ Disabled

**Connectors**

Next Previous Cancel

Provide a Name and optional Description

## Slide notes

Configure the Connector Group as necessary.

## Slide 40 - Slide 40

The screenshot shows the 'Add Connector' dialog box in Adobe Captivate, specifically the 'Connector Group' step (step 3 of 5). The dialog box is overlaid on the main interface, which includes a sidebar with navigation options like Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main interface also shows a search bar and a table of connectors.

The 'Add Connector' dialog box has a blue header with the title 'Add Connector' and a close button (X). Below the header is a progress bar with five steps: 1. Signing Certificate, 2. Connector Group (current step), 3. Create Provisioning Key, 4. Review, and 5. Review. The current step is highlighted with a blue background.

The 'Connector Group' step contains the following fields and controls:

- Select Connector Group:** A dropdown menu with the text 'Select Connector Group' and a blue button labeled 'Add Connector Group'.
- Name:** A text input field with the value 'Sentinel Group'.
- Description:** A text input field with the value 'Group for Sentinel Connectors'.
- Status:** A toggle switch with 'Enabled' selected (indicated by a checkmark) and 'Disabled' as an option.
- Connectors:** A list box for adding connectors, currently empty.

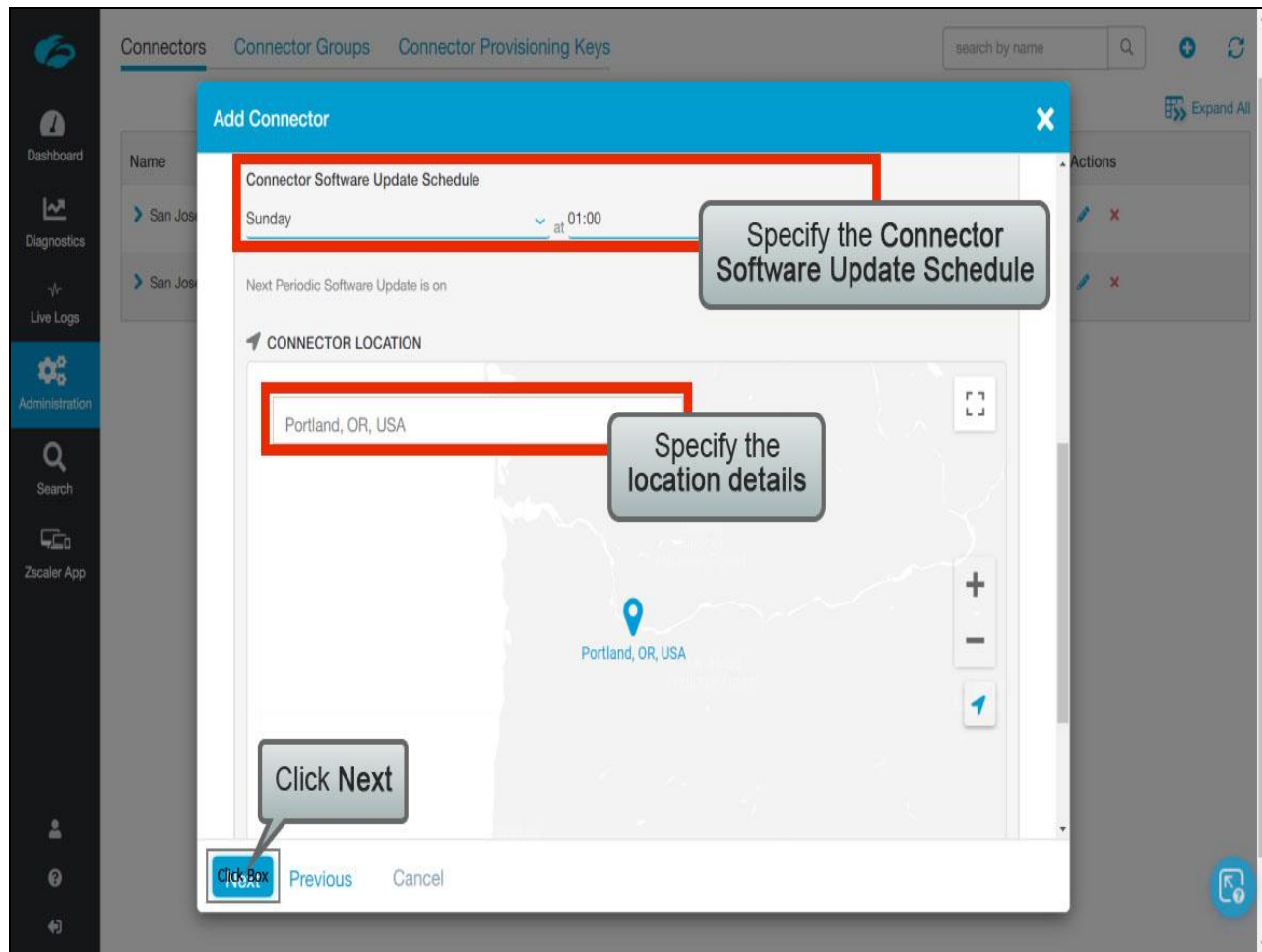
At the bottom of the dialog box are three buttons: 'Next' (blue), 'Previous' (gray), and 'Cancel' (gray). A gray callout box with the text 'Scroll down...' is positioned over the 'Connectors' list box.

## Slide notes

Scroll down...



## Slide 41 - Slide 41



## Slide notes

...the configuration includes the **Day** and **Time** for periodic updates of the Connectors, and their geographic location.

Click **Next** once you are done.

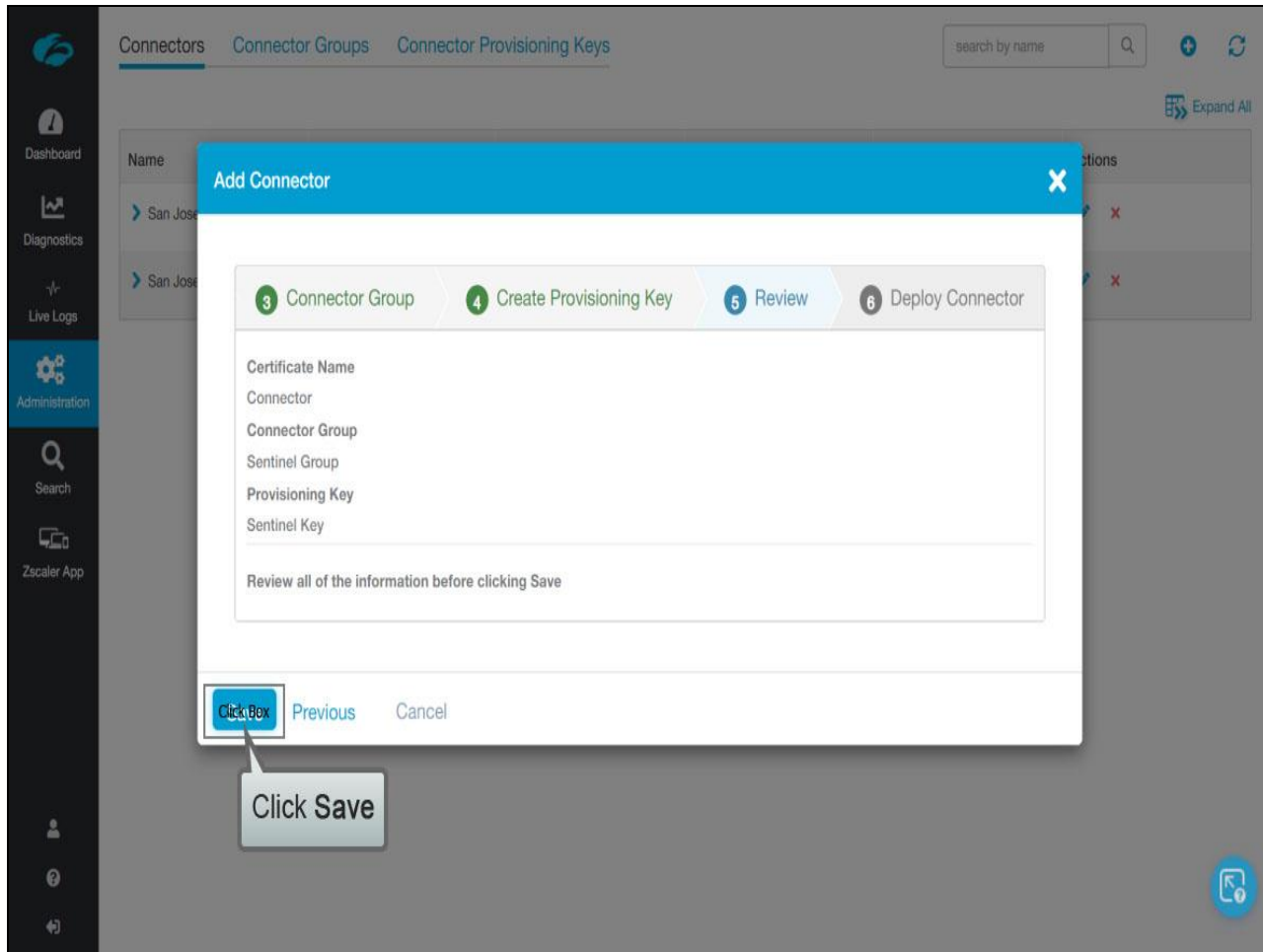
## Slide 42 - Slide 42

The screenshot shows the 'Add Connector' dialog box in Adobe Captivate, specifically the 'Create Provisioning Key' step. The dialog has a blue header with a close button. Below the header is a progress bar with four steps: 3 Connector Group, 4 Create Provisioning Key (current step), 5 Review, and 6 Deploy Connector. The main form area contains three input fields: 'Name' (with 'Sentinel Key' entered), 'Maximum Reuse of Provisioning Key' (with '10' entered), and 'Instances of Provisioning Key Reuse'. A red rectangular box highlights the 'Name' and 'Maximum Reuse of Provisioning Key' fields. A grey callout box with a blue border points to these fields, containing the text 'Give the Provisioning Key a Name and set the Maximum Reuse of Provisioning Key'. At the bottom of the dialog are three buttons: 'Click Next' (highlighted with a blue box and a callout), 'Previous', and 'Cancel'. The background shows the Adobe Captivate interface with a sidebar on the left and a search bar at the top.

## Slide notes

Configure a **Provisioning Key** as necessary. Note that the configuration includes the maximum number of times the key may be used. This limit is not encoded in the key itself, rather the database and API enforce it, which means that it can be changed at a later date if necessary. Click **Next** once you are done.

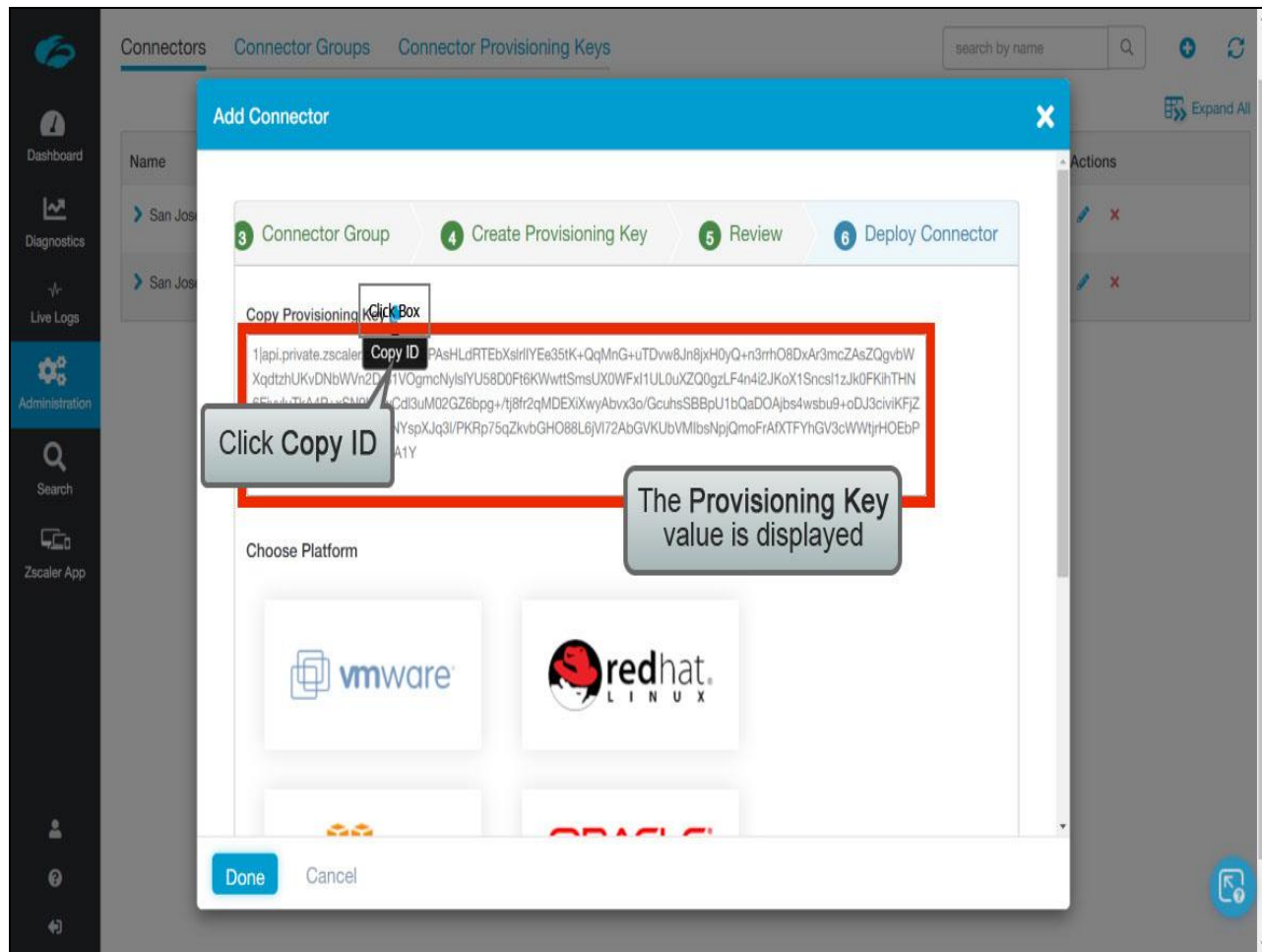
## Slide 43 - Slide 43



## Slide notes

Review the new Connector configuration and once you are happy with it click **Save**.

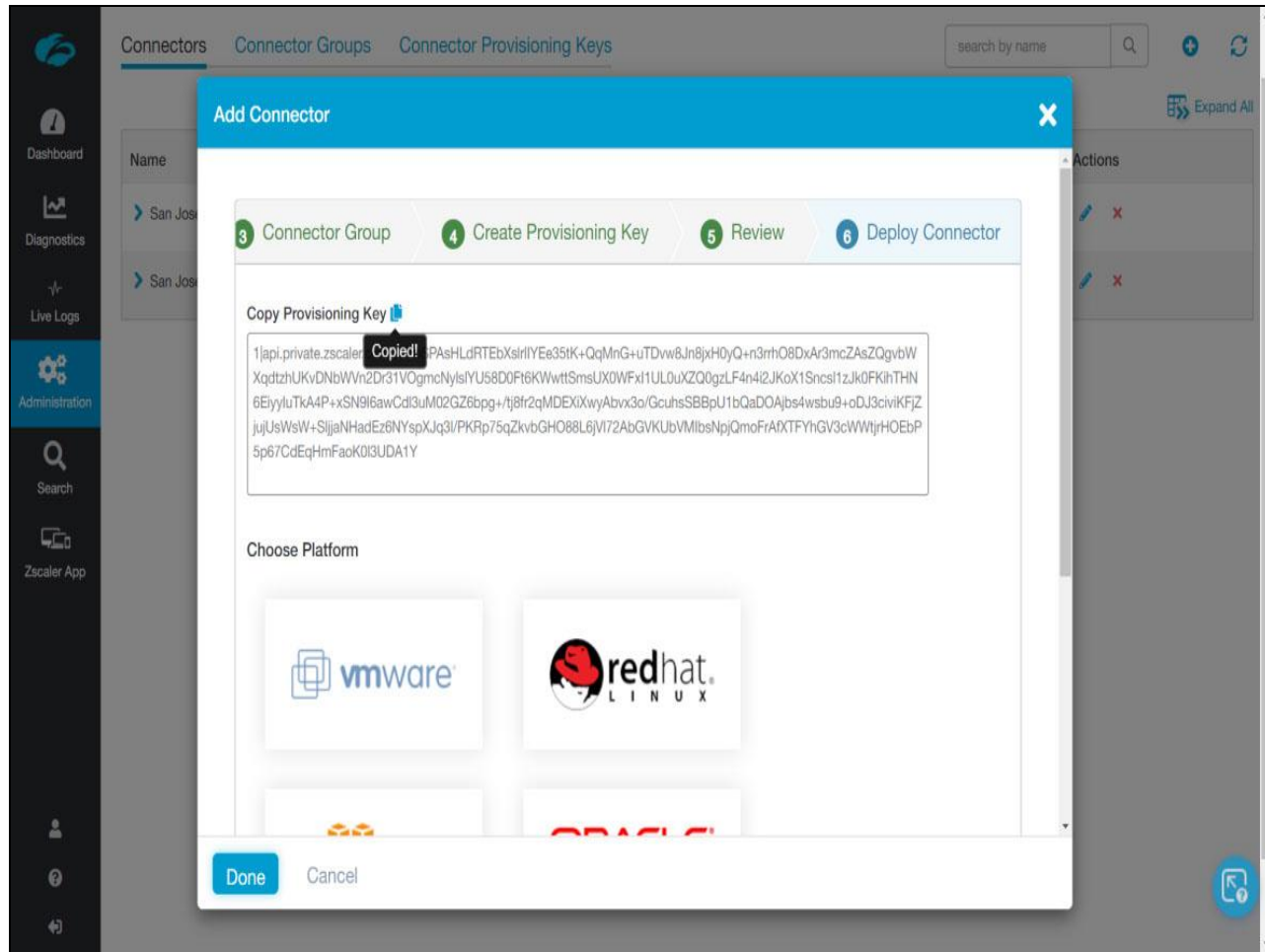
## Slide 44 - Slide 44



## Slide notes

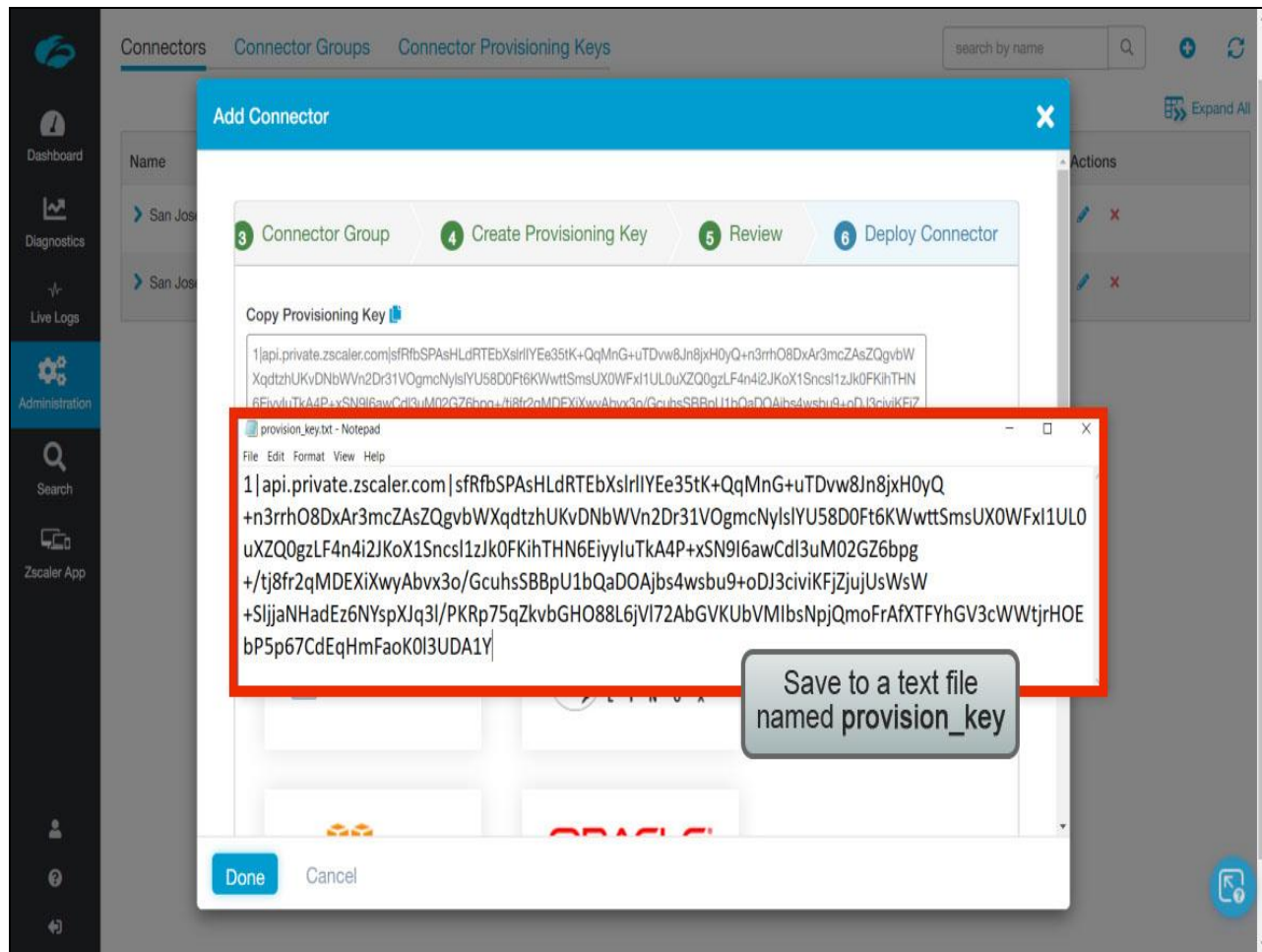
The data for the new key will be displayed. Note that provisioning keys are considered confidential information and must be kept in a safe place. Click the **Copy ID** option to copy the key value to your clipboard, ...

## Slide 45 - Slide 45



## Slide notes

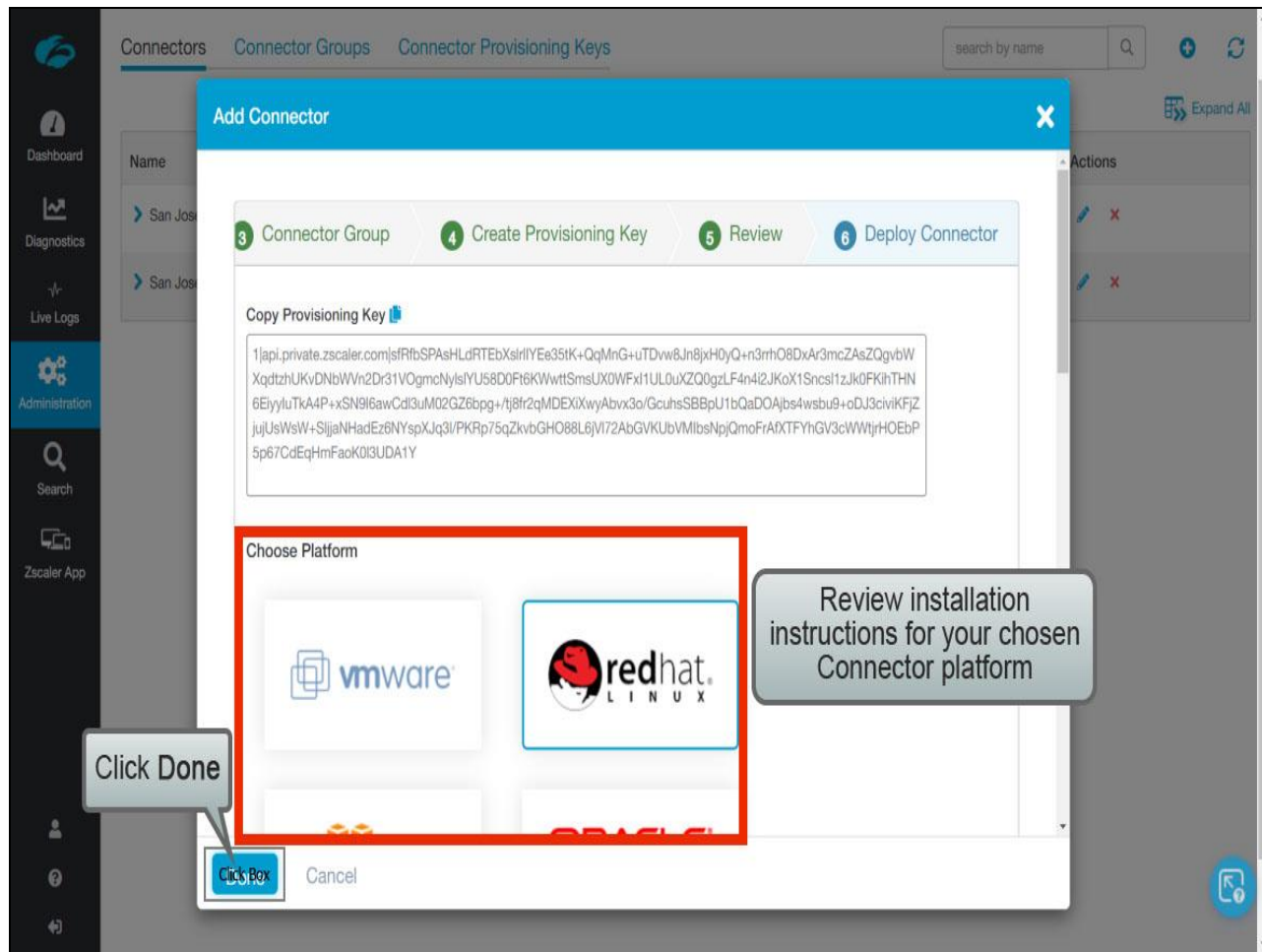
## Slide 46 - Slide 46



## Slide notes

...then paste it to a file as a record of the provisioning key value. Ideally you should save the file with the name **provision\_key**, all lower case and with no file extension.

## Slide 47 - Slide 47



## Slide notes

Links are provided for you within the wizard for per-platform installation instructions. Click **Done** to exit the **Add Connector** wizard.

## Slide 48 - Slide 48

Click Connector Groups

Click or

Edit or Delete

Status	Session	Update Status	Current Software Version	Actions
✖	Disconnected	Success ⓘ	16.86.1	
✔	Disconnected			
✔	Authenticated	Success ⓘ	19.20.3	
✔	Authenticated	Success ⓘ	19.20.3	
✔	Authenticated	Success ⓘ	19.20.3	
✔	Authenticated	Success ⓘ	19.20.3	
✖	Disconnected	Success ⓘ	17.62.2	
✔	Authenticated	Success ⓘ	19.20.3	
✖ ⓘ	Disconnected			
✔	Authenticated	Success ⓘ	19.20.3	
✔	Authenticated	Success ⓘ	19.20.3	

## Slide notes

The new Connector will not yet be visible in the **Connectors** list, as it is not yet installed and active. You have the option to **Edit** or **Delete** any of the active Connectors.

To view the list of available Connector Groups, click the **Connector Groups** tab.



Slide 49 - Slide 49

Dashboard

Diagnostics

Live Logs

Administration

Search

Zscaler App

Connectors

Connector Groups

Connector Provisioning Keys

search by name

Expand All

Name	Status	Next Periodic Software Update	Actions
AWS Connector Group		Jul 22 between 0:00 - 4:00 (Indochina Time)	
ESXi Connector Group		Jul 22 between 6:00 - 10:00 (Indochina Time)	
Log-Streaming-Connectors		Jul 22 between 6:00 - 10:00 (Indochina Time)	
SanJose		Jul 20 between 15:00 - 19:00 (Indochina Time)	
Santa Clara		Jul 20 between 15:00 - 19:00 (Indochina Time)	
Sentinel Group		Jul 21 between 1:00 - 5:00 (Indochina Time)	

Slide notes

You also have the option to **Edit** or **Delete** any of the Connector Groups. To view a list of Provisioning Keys that have been created, click the **Connector Provisioning Keys** tab.

## Slide 50 - Slide 50

Connectors Connector Groups Connector Provisioning Keys search by name Q

Expand All

Name	Maximum # of Connectors	# of Enrolled Connectors	Connector Group	Provisioning Key	Actions
> AWS Key	10	0	AWS Connector Group	COPY KEY	
> ESXi Connector Key	5	0	ESXi Connector Group	COPY KEY	
> Log-Streaming-Key	12	0	Log-Streaming-Connectors	COPY KEY	
> San Jose Connector - 1	5	4	SanJose	COPY KEY	
> Santa Clara Key	5	1	Santa Clara	COPY KEY	
> Sentinel Key	10	0	Sentinel Group	COPY KEY	

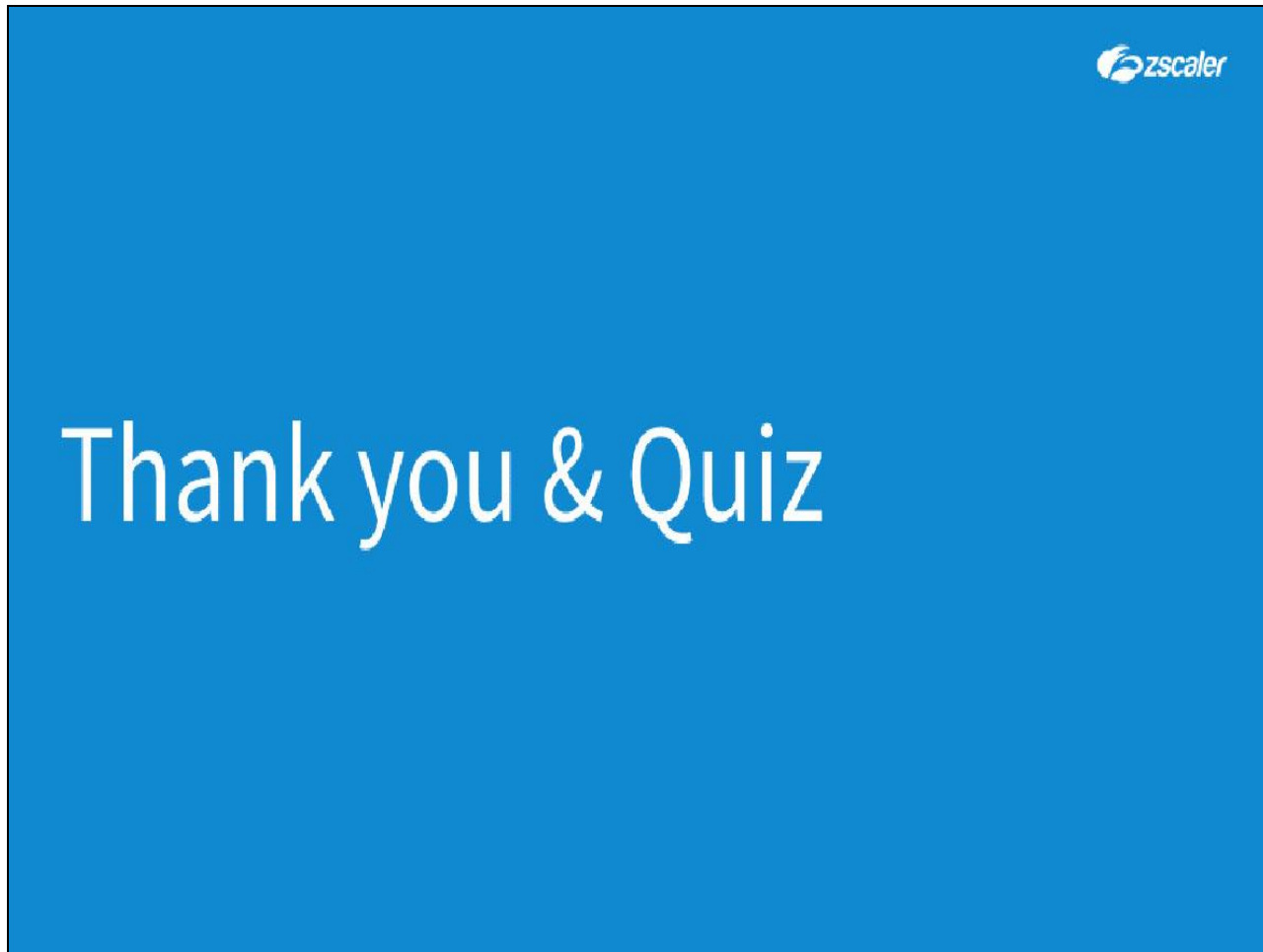
Copy Key option

Edit or Delete

## Slide notes

Once again you have the options to **Edit** or **Delete** Provisioning Keys, and note that for each of the provisioning keys there is a **COPY KEY** option, to allow you to access the Provisioning Key value for the Connector.

## Slide 51 - Thank you &amp; 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.