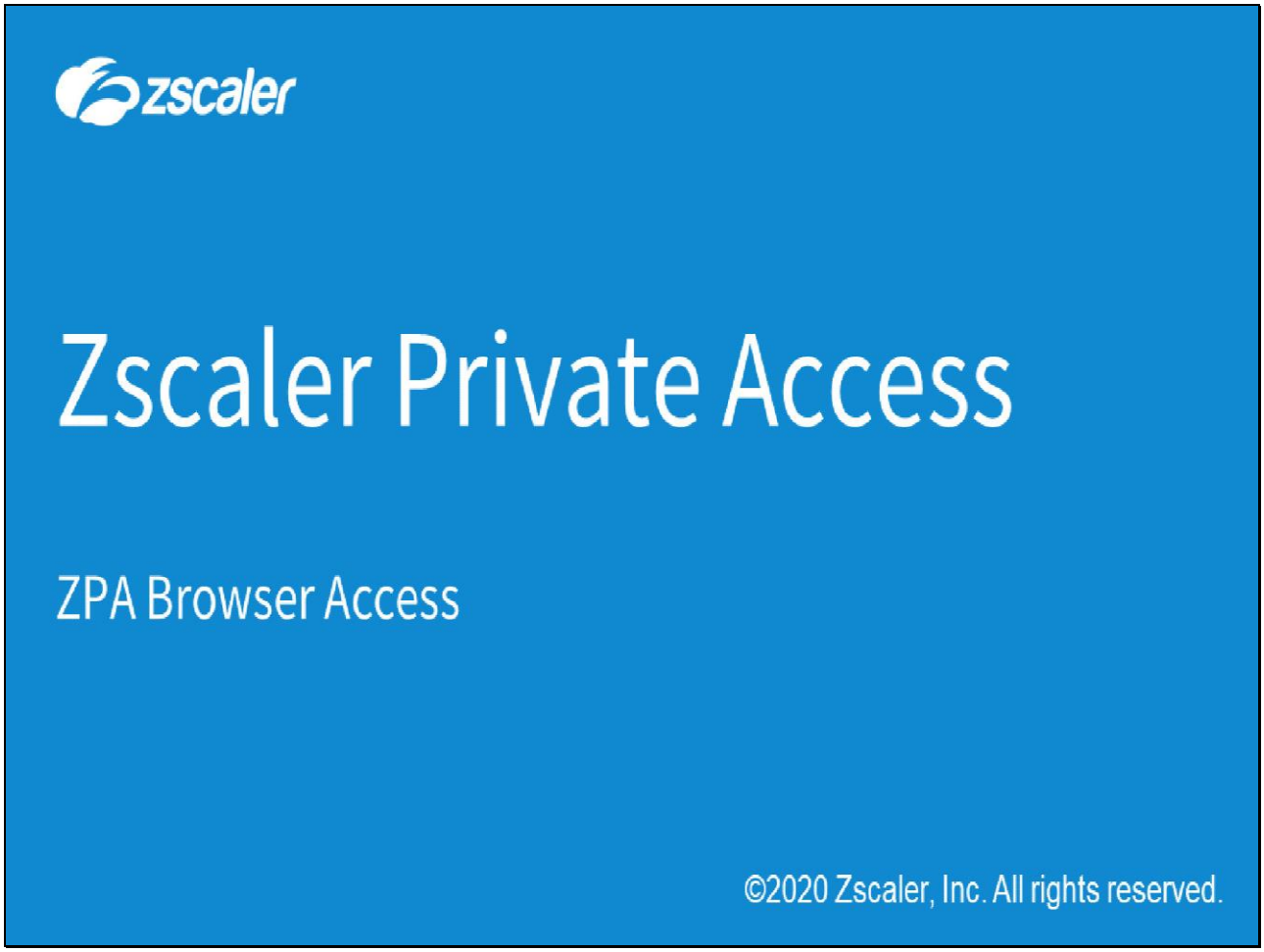
Slide 1 - Zscaler Private Access



Slide notes

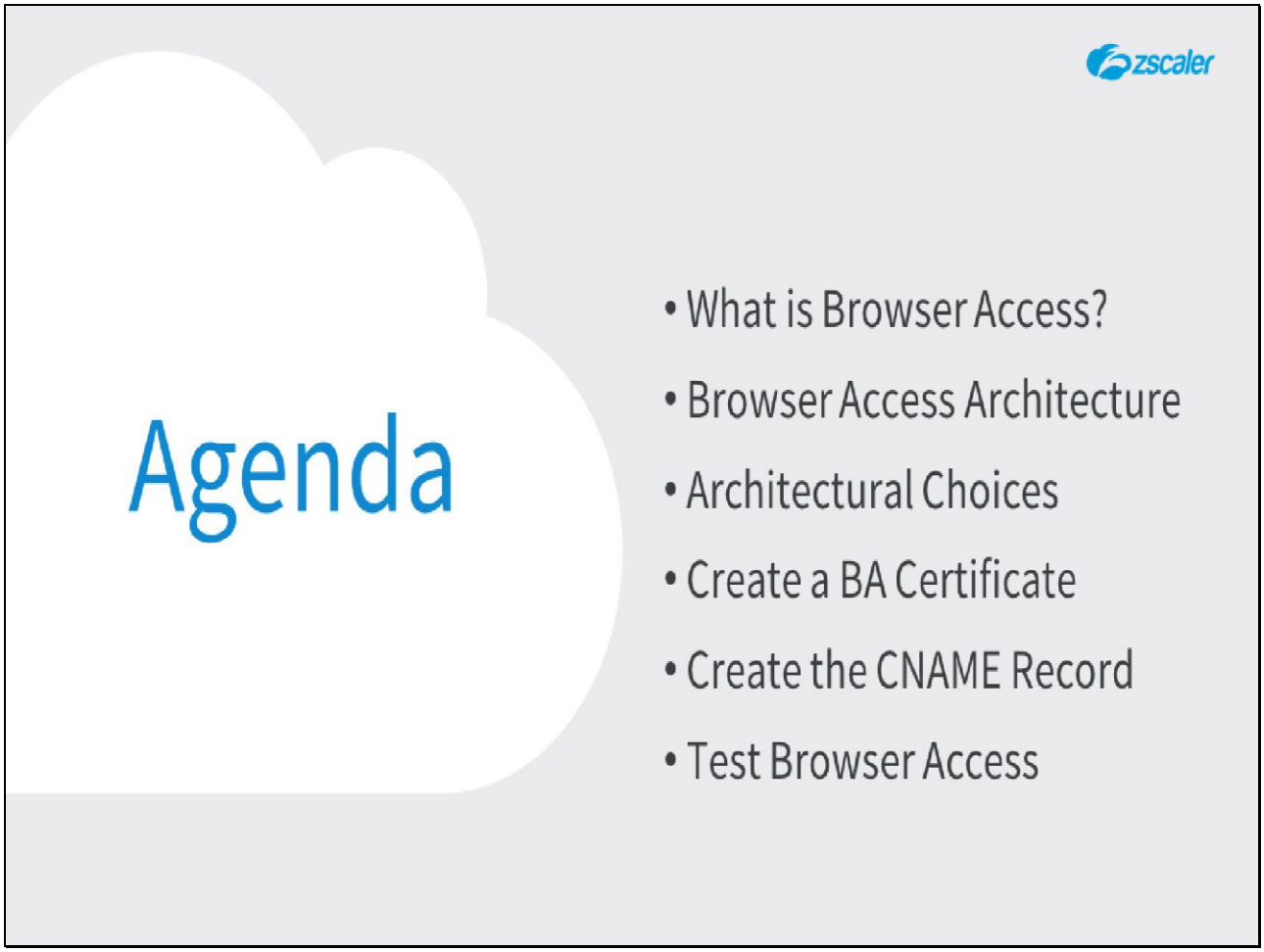
Welcome to this training module on ZPA Browser Access (BA).

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



Slide notes

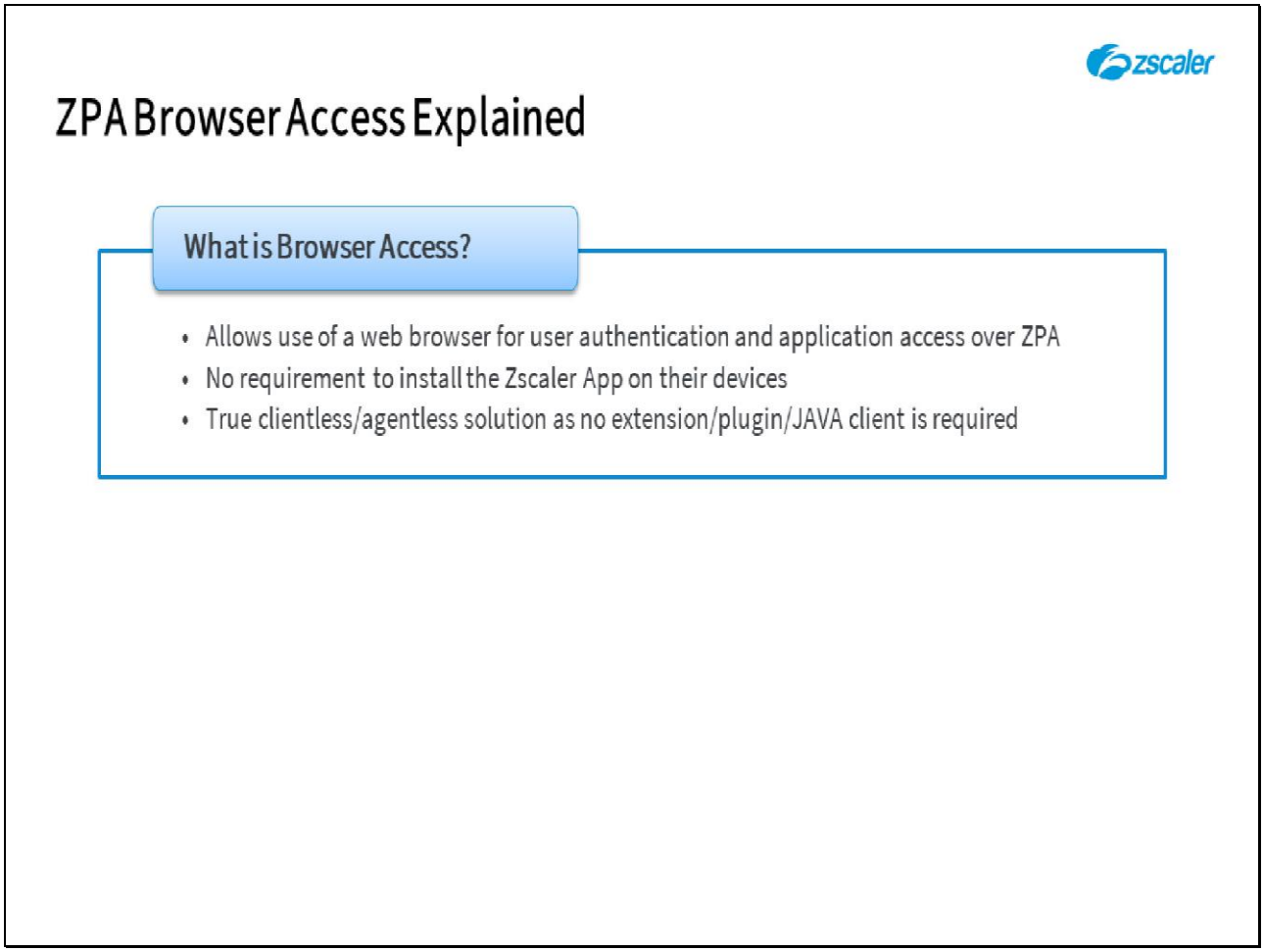
In this module we will: describe what BA is; have a look at the BA architecture; look at some of the architectural choices that you have with BA; step through the process of creating a certificate for a BA Application Segment; look at how to create the necessary CNAME record on the DNS; then look at the end user experience.

Slide 4 - What is Browser Access

Slide notes

In the first section, we will describe what BA is.

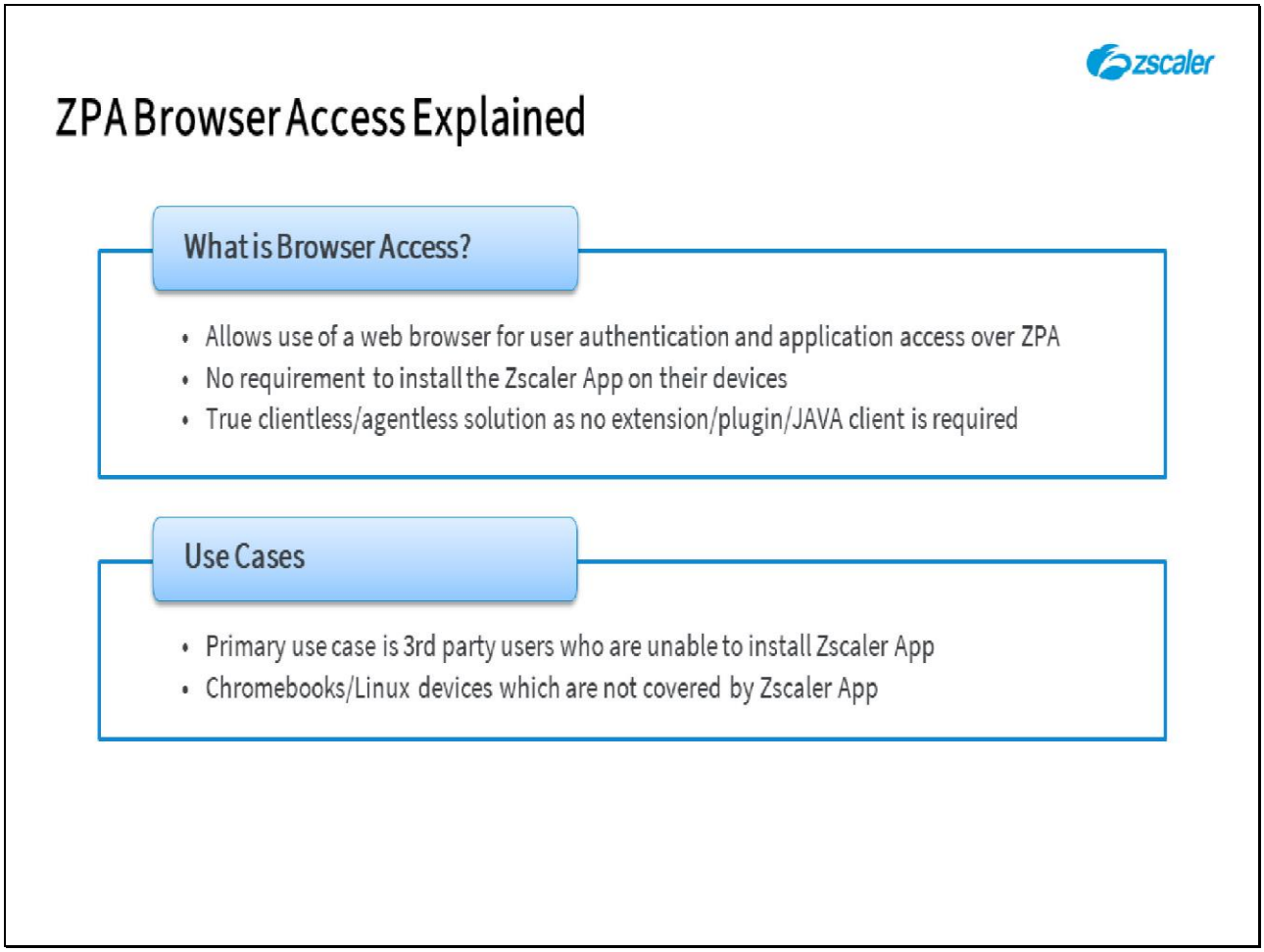
Slide 5 - ZPA Browser Access Explained



Slide notes

At its simplest, BA allows access to ZPA Applications from a web browser, with no need to install the Zscaler App. BA allows the use of a standard, modern web browser (that supports TLS1.2) for user authentication and application access over ZPA, without requiring users to install the Zscaler App on their devices. BA is truly a clientless/agentless solution for accessing your private applications, in that no browser extension, plugin, or Java client is required on the browser.

Slide 6 - ZPA Browser Access Explained



Slide notes

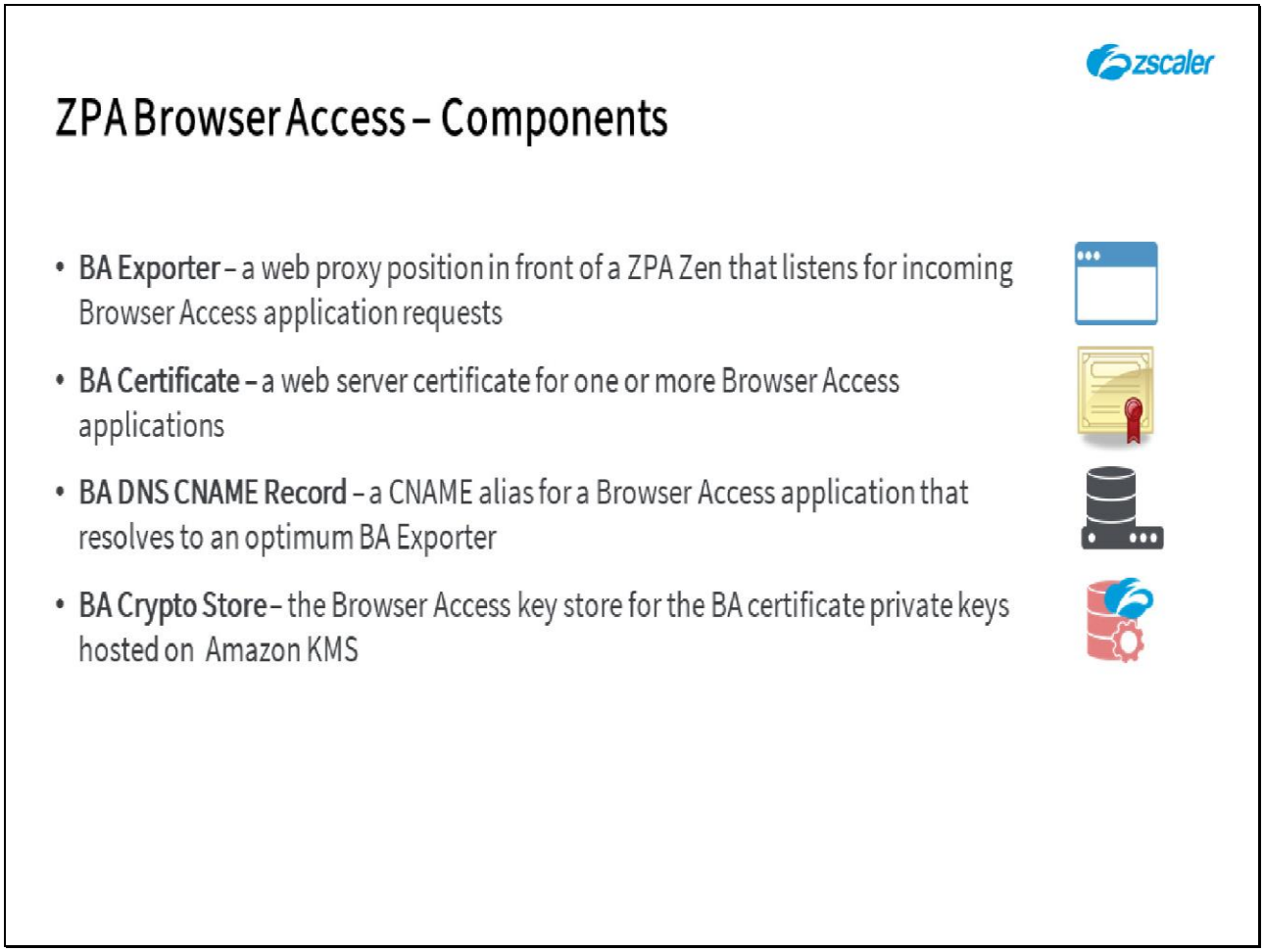
The primary use case for BA is for 3rd party users (contractors or consultants) who are unable to install Zscaler App on the client device for whatever reason. In addition, BA is useful to provide ZPA connectivity for those devices for which there is no Zscaler App installer, such as Chromebooks, or Linux devices.

Slide 7 - Browser Access Architecture

Slide notes

In the next section, we will provide an overview of the ZPA BA architecture.

Slide 8 - ZPA Browser Access – Components

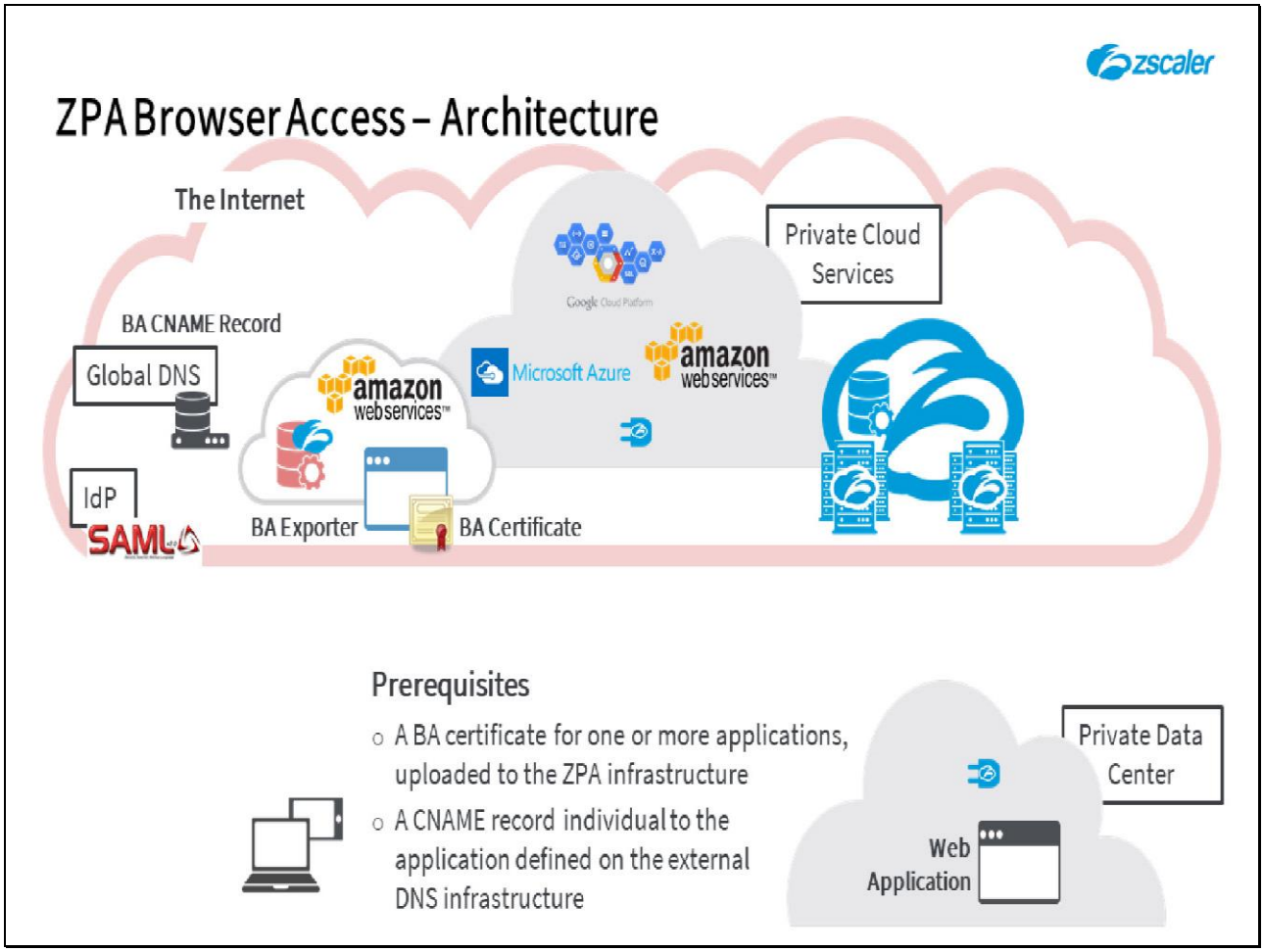


Slide notes

In addition to the regular ZPA architectural elements, BA introduces some new components as listed and described here:

- **BA Exporter** - this is a secure web proxy sitting in front of a ZPA ZEN that listens for incoming BA application requests. It responds with the necessary BA certificate and on a successful end user authentication, establishes a Z Tunnel to the local ZPA-ZEN;
- **BA Certificate** - a web server certificate for one or more Browser Access applications (may be a wildcard certificate);
- **BA DNS CNAME Record** - a CNAME alias for a Browser Access application that resolves to an optimum BA Exporter;
- **BA Crypto Store** - the Browser Access key store for the BA certificate private keys hosted on the Amazon Key Management Service (KMS).

Slide 9 - ZPA Browser Access – Architecture

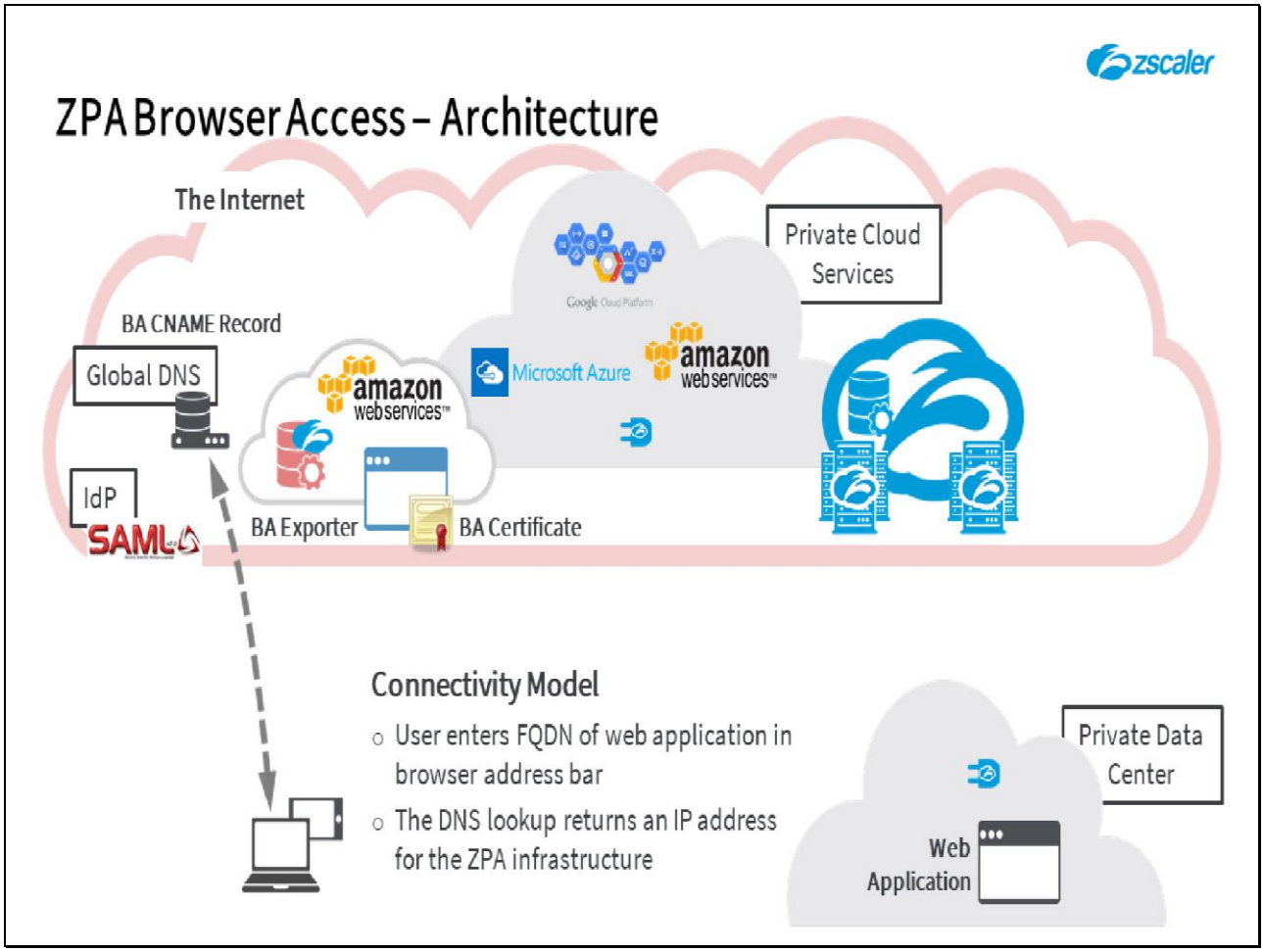


Slide notes

Prerequisite steps that are required to enable BA for an application are as follows:

1. A **BA certificate** for one (or more) applications must be uploaded to the ZPA infrastructure.
2. A **CNAME** record for each individual BA application must be defined on the DNS infrastructure (usually on the external public DNS), to allow the resolution of the FQDN for an application to the ZPA infrastructure.

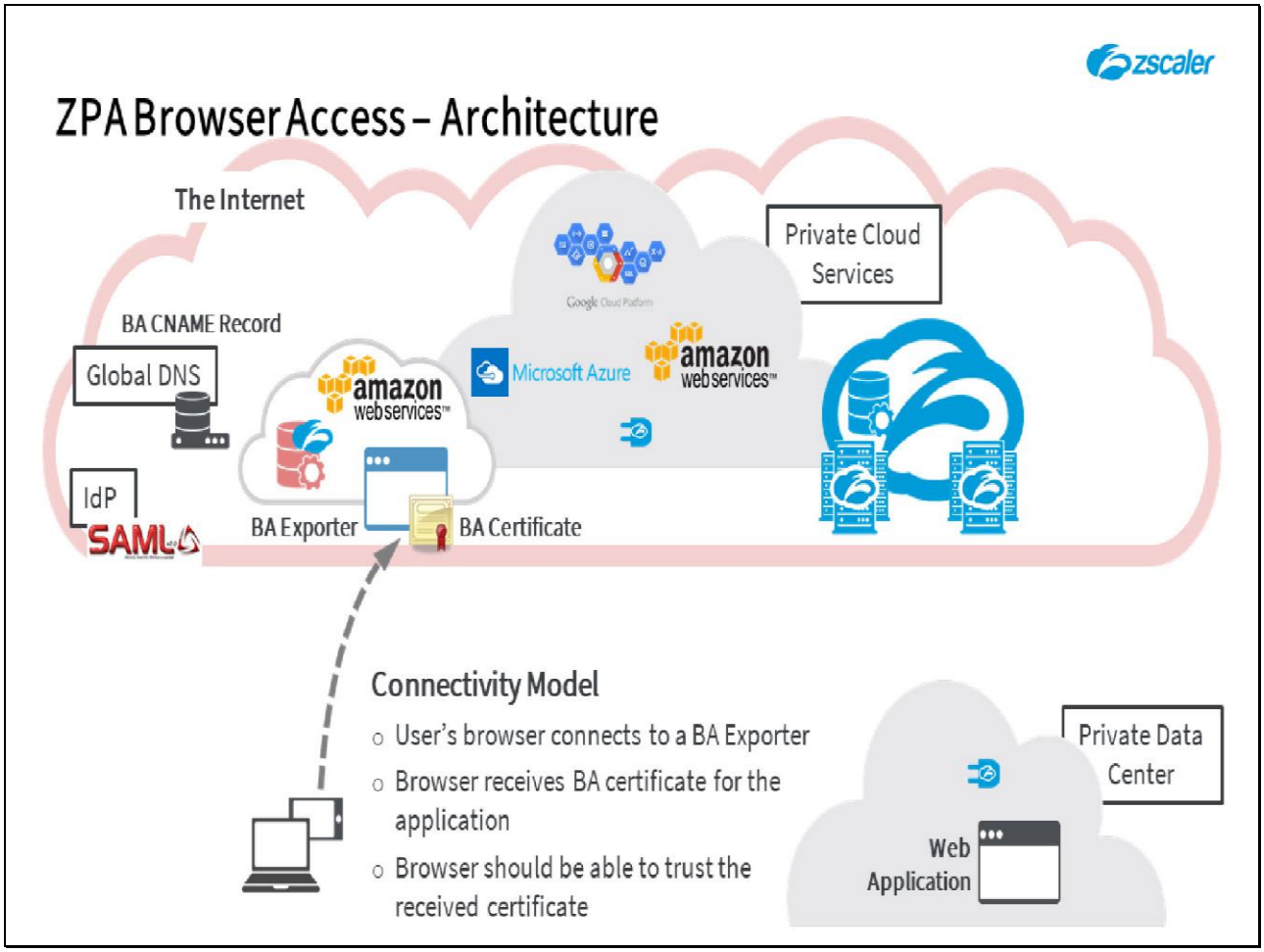
Slide 10 - ZPA Browser Access – Architecture



Slide notes

The user requests access to the private web application, by entering the FQDN for it in the browser address bar. The user's system will do a DNS lookup which will resolve to the **CNAME**, at which point the DNS server will look up the matching **A** record, then resolve that to an IP address. Ultimately, the user's system will receive an IP for the optimum **BA Exporter** to use to access the requested application.

Slide 11 - ZPA Browser Access – Architecture

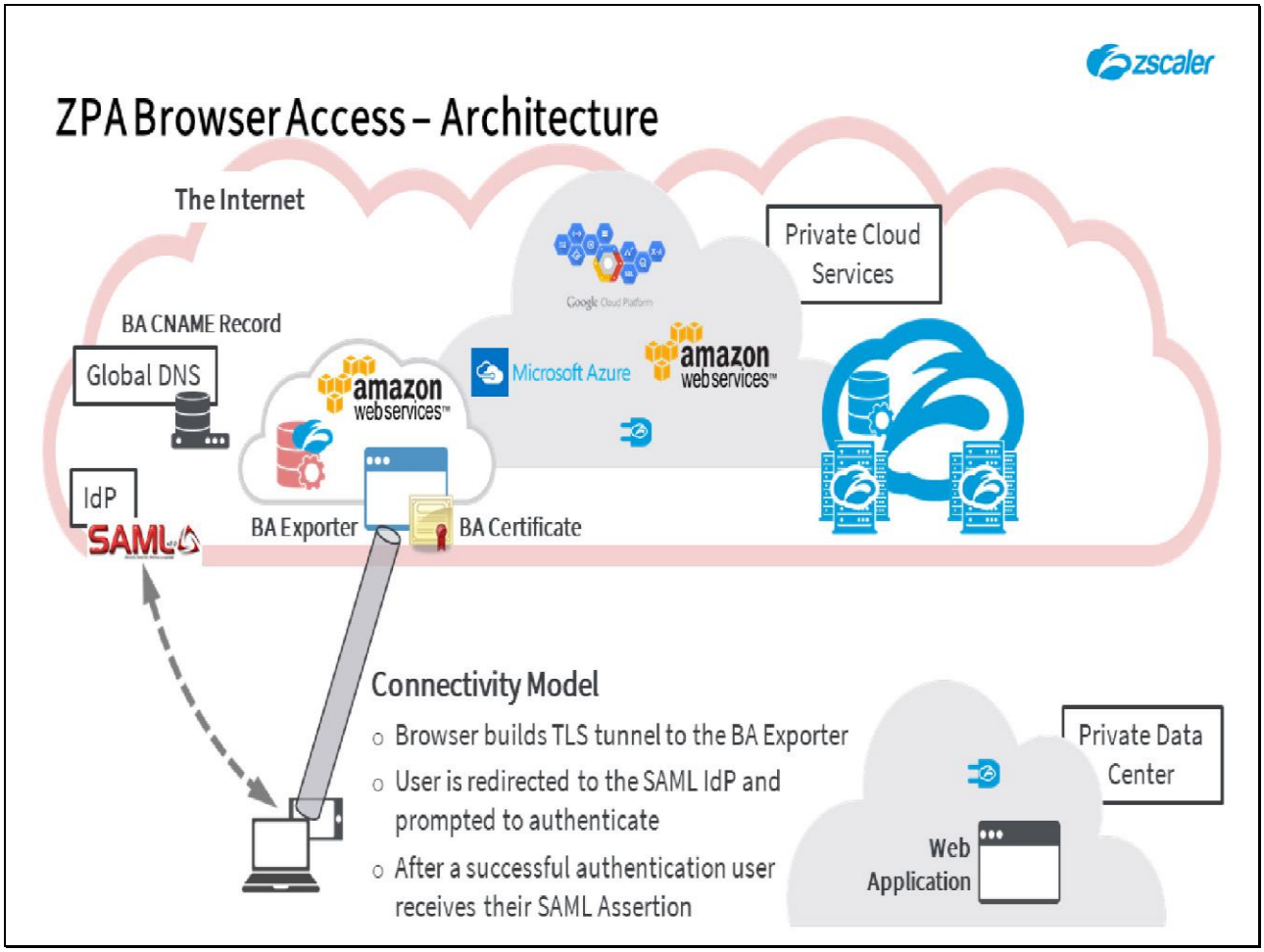


Slide notes

The user's browser connects to the **BA Exporter** that the DNS record resolves to and if necessary is redirected to **HTTPS**. It then receives the **BA certificate** for the requested application. The user's device should be in possession of the appropriate root CA certificate to allow it to trust the connection to the Exporter.

Note: Under most circumstances the root CA will be public, and the device will already have the required root CA certificate.

Slide 12 - ZPA Browser Access – Architecture

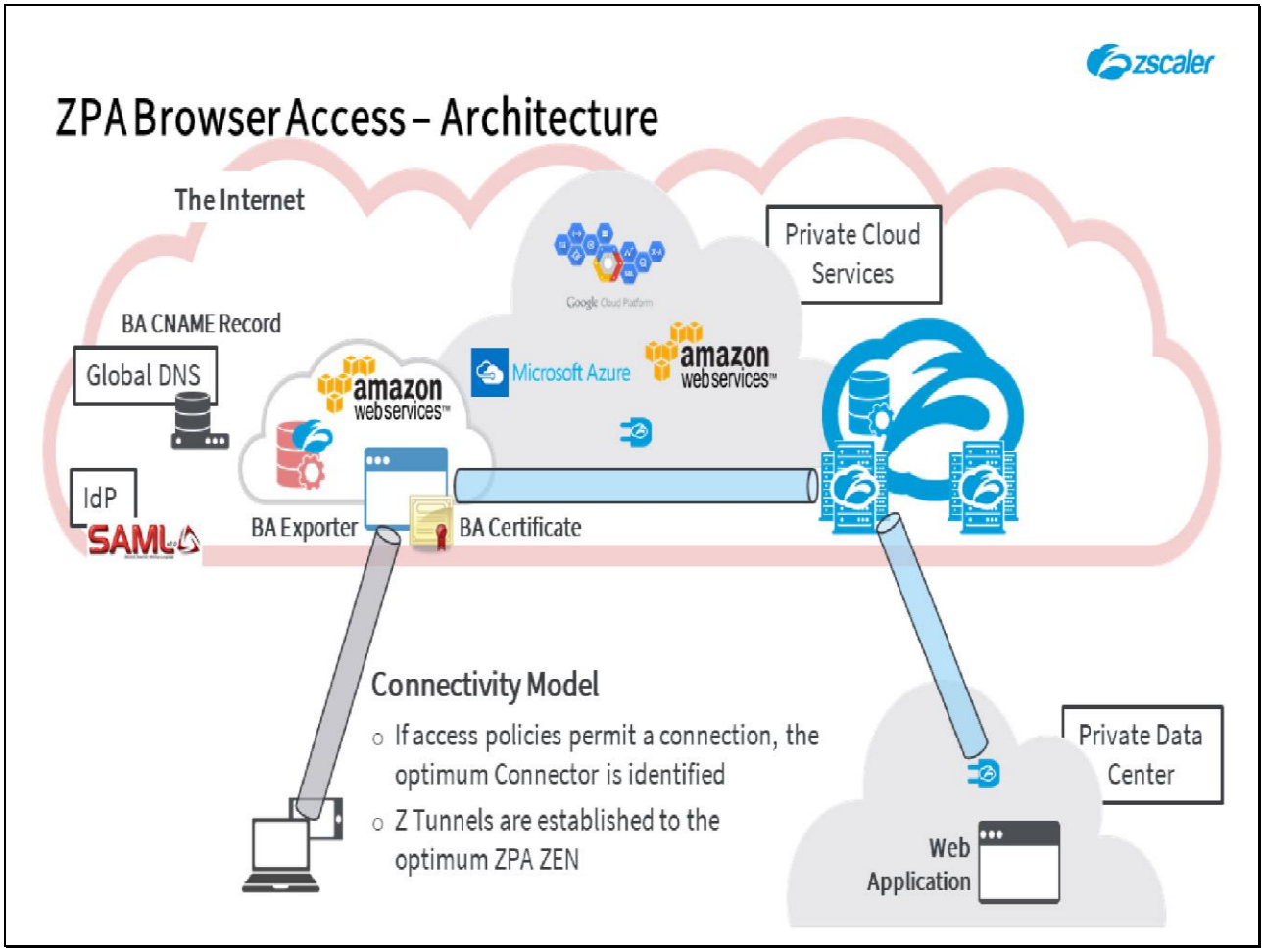


Slide notes

The browser establishes a TLS connection to the **BA Exporter**, which then triggers a user authentication using SAML and the configured IdP. The user will be prompted to login at this point and, after a successful authentication, will receive a SAML assertion.

Note: This is the exact same authentication and authorization process as for ZPA with the Zscaler App, using the exact same SAML configuration.

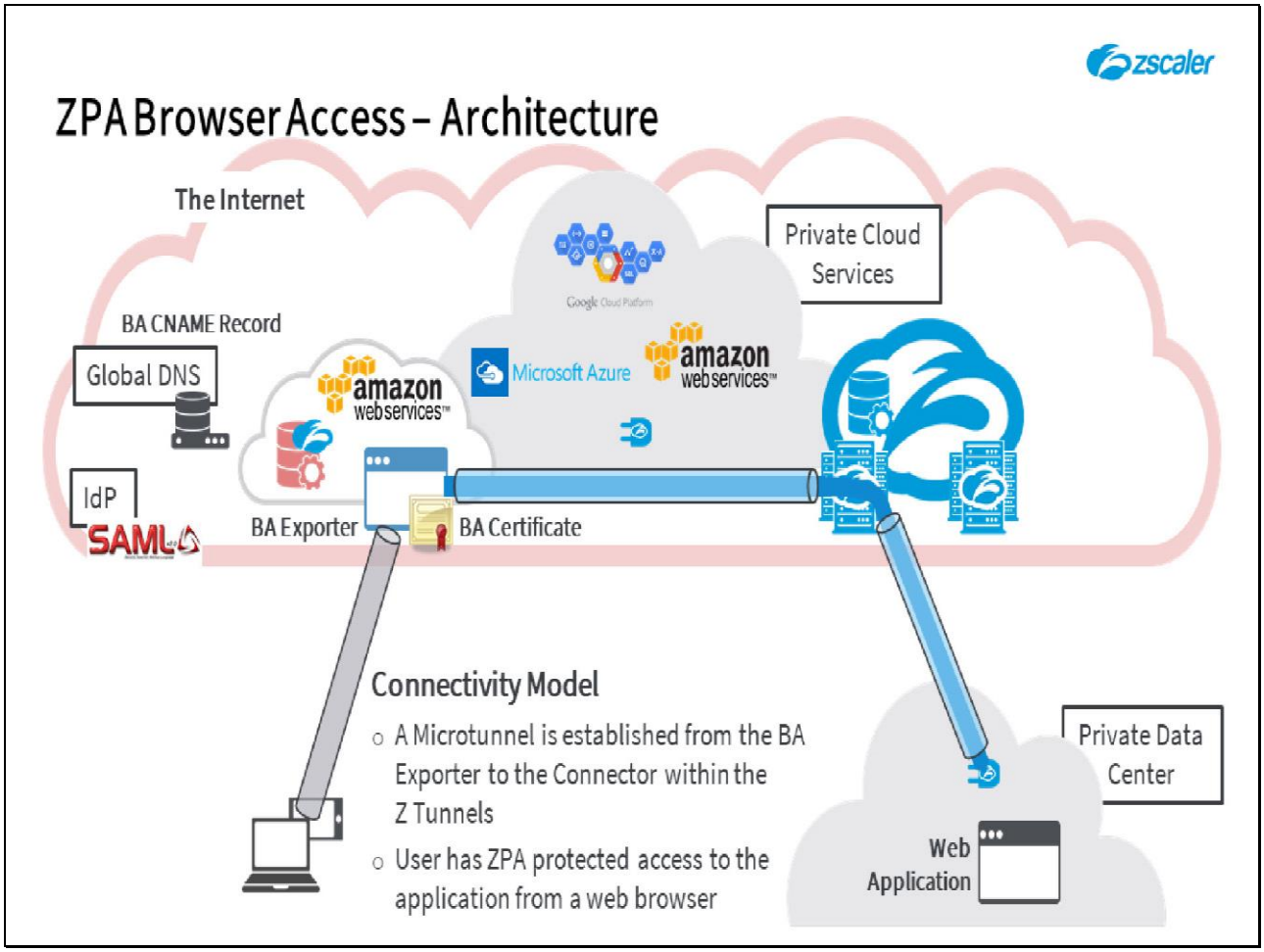
Slide 13 - ZPA Browser Access – Architecture



Slide notes

If the access policy configuration permits this user to connect to the requested application, ZPA identifies the optimum ZPA-ZEN and the best-path Connector to access it. Z Tunnels are established from the **BA Exporter** and the chosen Connector to the ZPA-ZEN. Note that the ZPA-ZEN will in most cases be immediately adjacent to the **BA Exporter**.

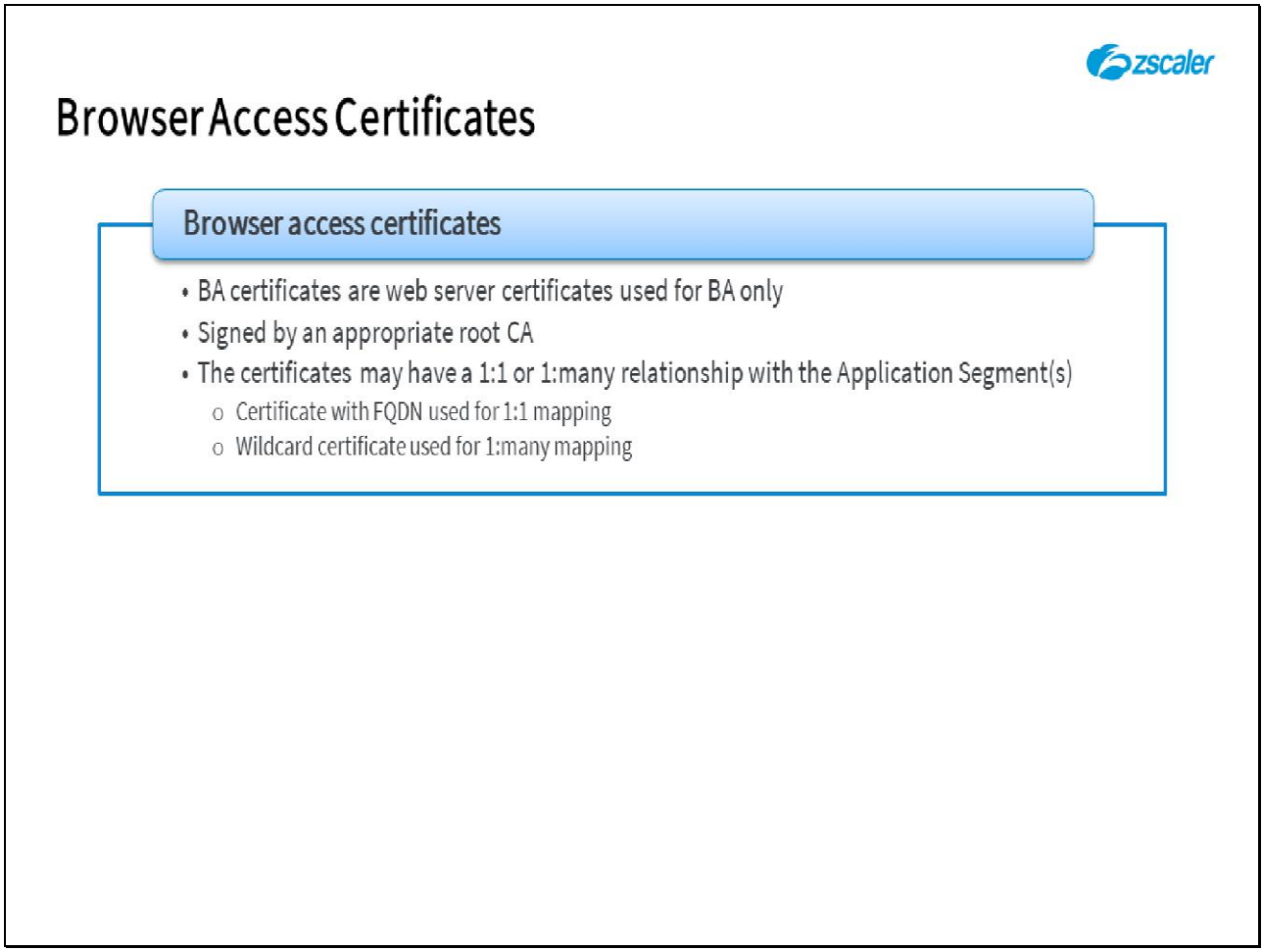
Slide 14 - ZPA Browser Access – Architecture



Slide notes

Subsequently a Microtunnel is established through the Z Tunnels to provide an encrypted end-to-end data path for the user to access the private web-based application. Data is encrypted between the user's browser and the **BA Exporter** using **HTTPS**, then it is again protected by TLS in the Z Tunnels within the ZPA infrastructure. As is always the case, the Microtunnel is established on a per-user and per-application basis; it cannot be used by another user, nor for accessing some other application.

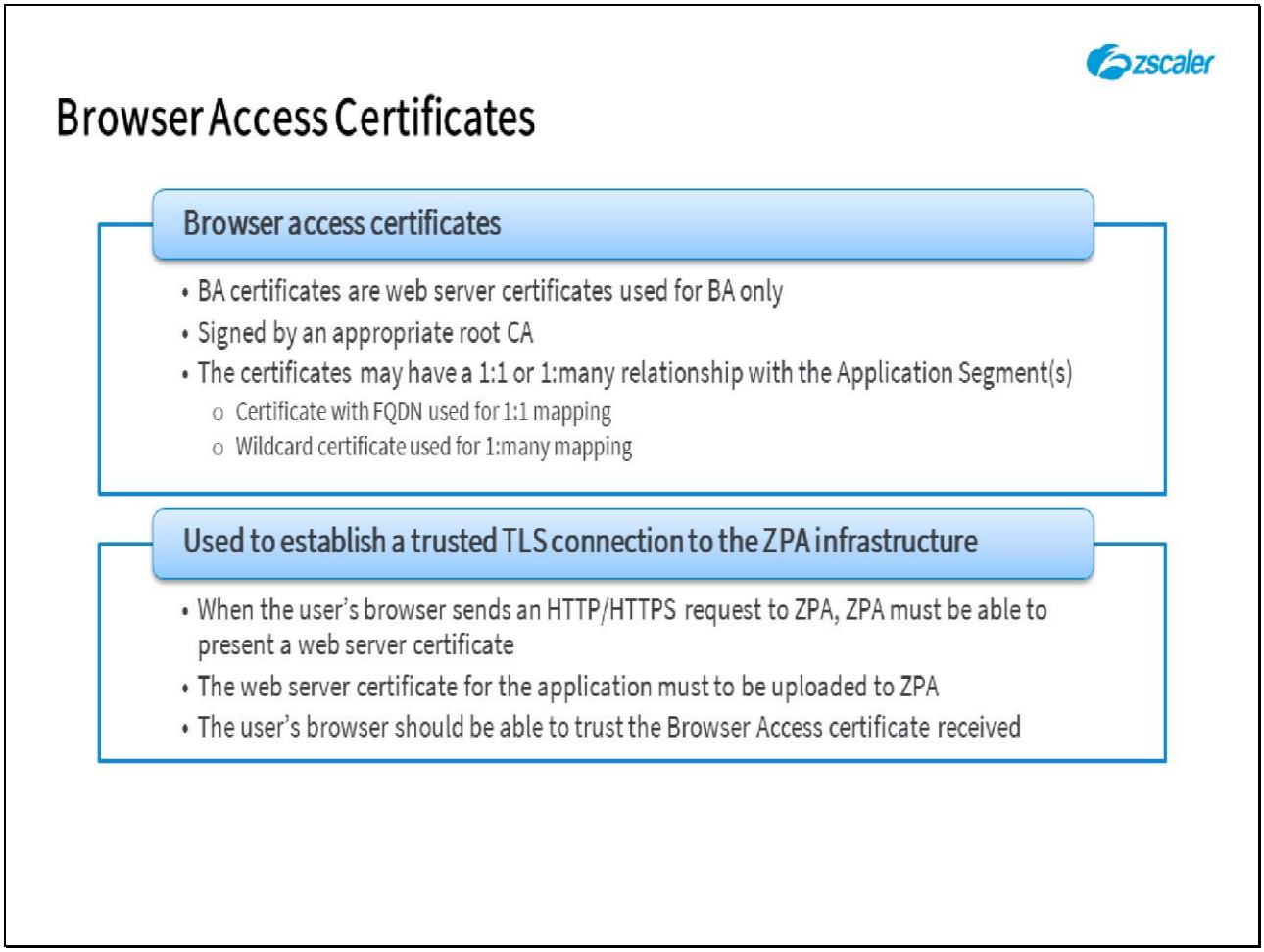
Slide 15 - Browser Access Certificates



Slide notes

The **BA certificates** are essentially web server certificates signed by an appropriate root CA, which are used only to enable Browser Access. The certificate used for BA may have either a **1:1** or **1:many** relationship with BA Application Segments. If the certificate is generated for a FQDN, then the mapping is **1:1**; a wildcard certificate may be used for a **1:many** mapping.

Slide 16 - Browser Access Certificates

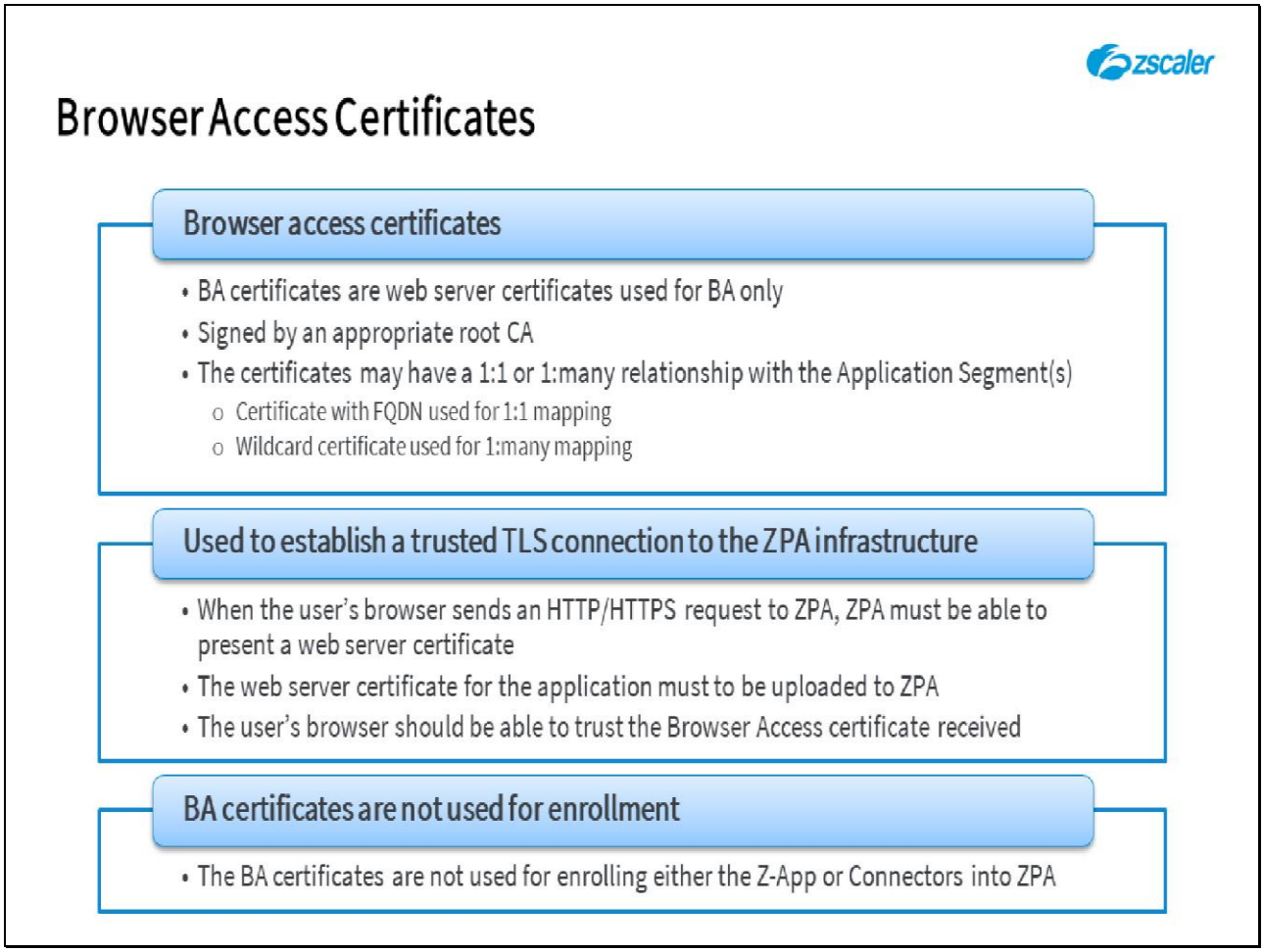


Slide notes

The **BA certificates** are used to allow the user's device to establish a trusted and encrypted TLS 1.2 connection to the ZPA infrastructure. When the user's browser sends an **HTTP** or **HTTPS** request to the **BA Exporter**, ZPA will automatically present the **BA certificate** to enforce a secure connection. Hence the prerequisite to upload the **BA certificate** to the infrastructure in order to enable BA connectivity.

BA certificates may be signed by any root CA that the client device is able to trust, although under most circumstances they will be signed by a public CA. Note that both the signed certificate and the private key must be uploaded to the ZPA infrastructure, the private key being securely stored in the Amazon KMS.

Slide 17 - Browser Access Certificates



Slide notes

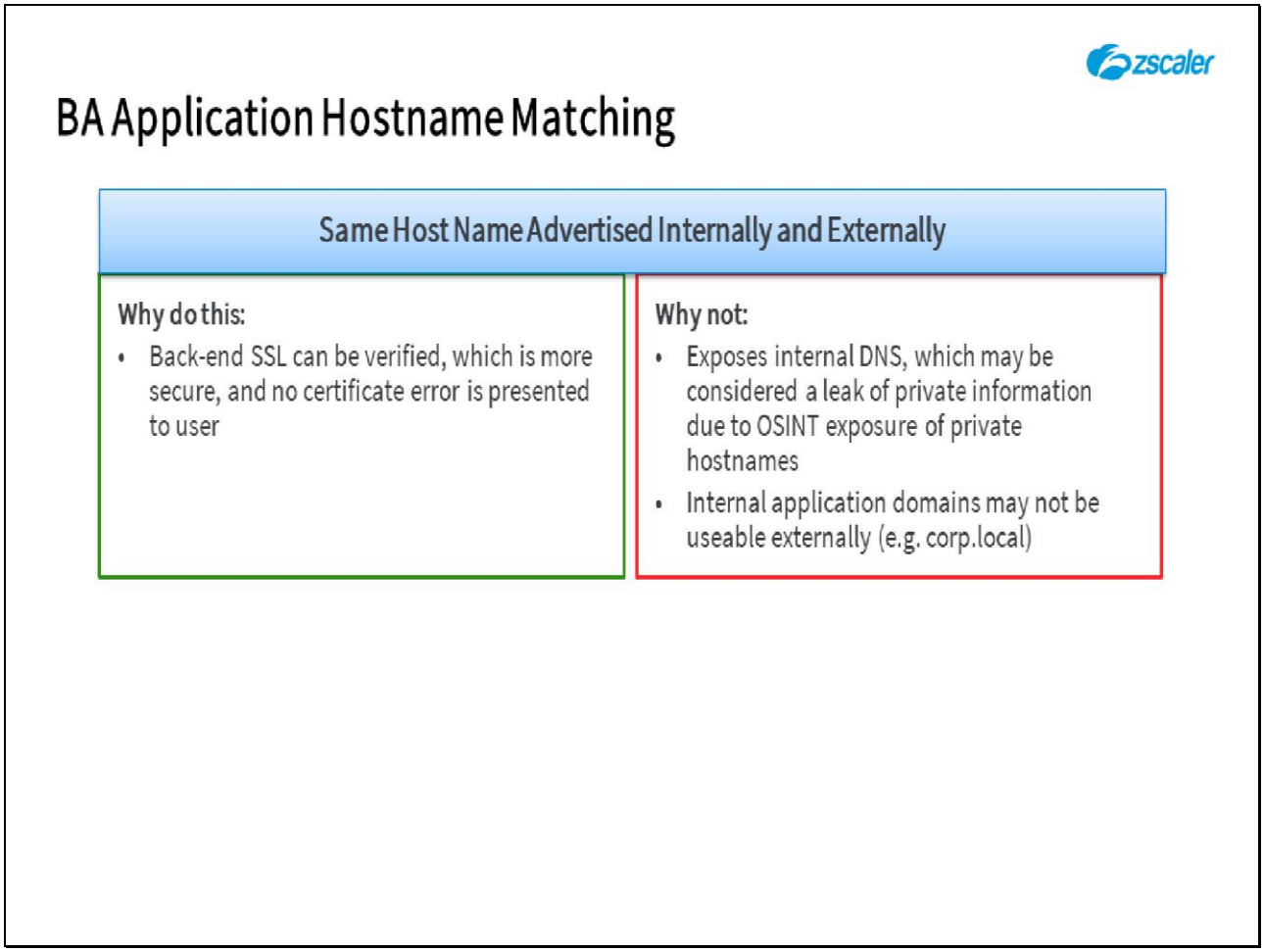
BA certificates are not suitable for and cannot be used for enrolling either the Zscaler App, or a Connector into the ZPA service.

Slide 18 - Architectural Choices

Slide notes

In the next section, we will look at some architectural choices for Browser Access, and at their implications.

Slide 19 - BA Application Hostname Matching

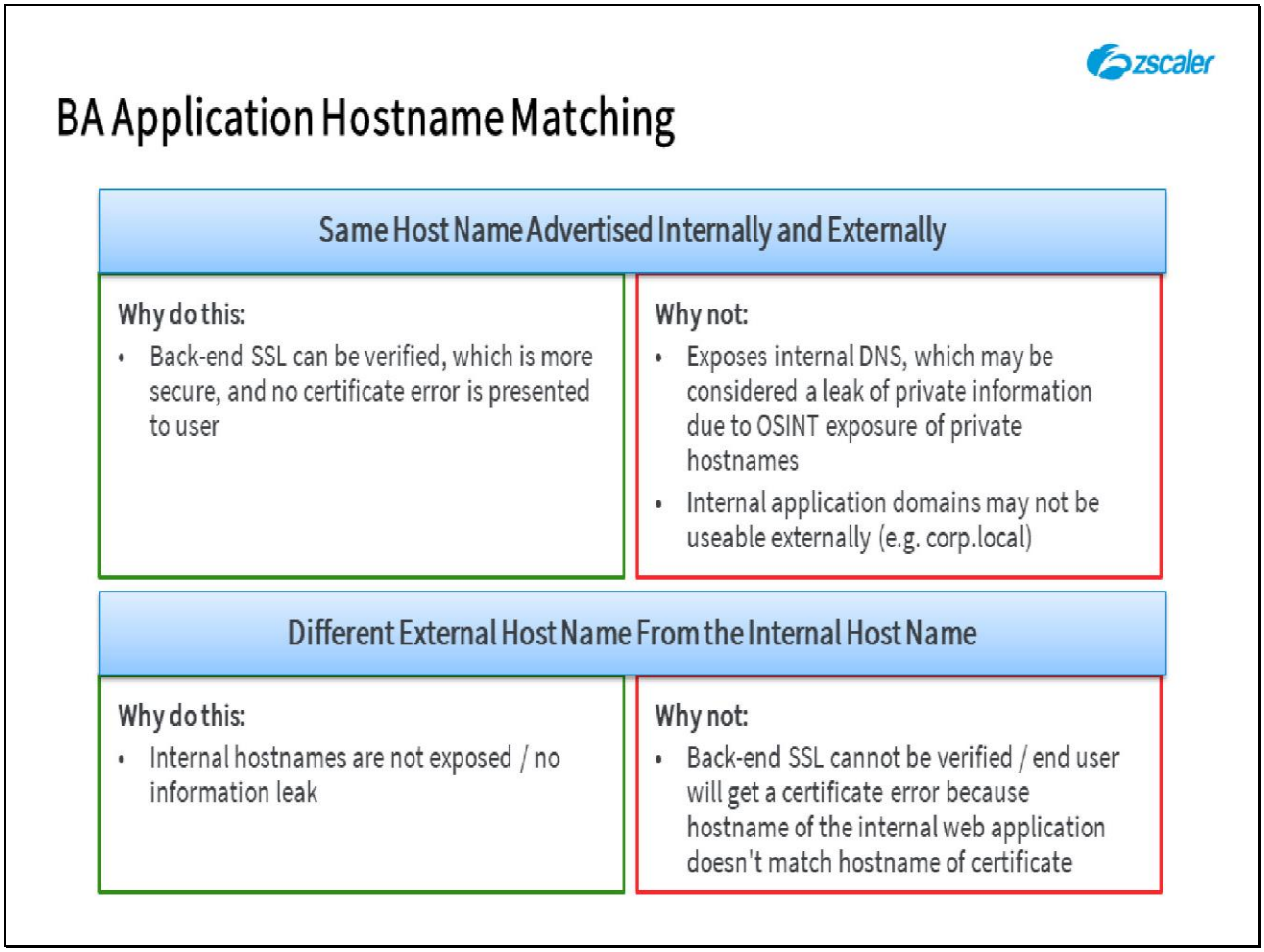


Slide notes

It is not strictly necessary to advertise the same application hostnames externally as you do within your network (and in the ZPA application configuration). The only requirement is that the hostname advertised externally must match the **BA certificate** that you upload to ZPA, so the user's browser can trust the initial connection to the **BA Exporter**.

Using the same app hostnames externally as you use internally is the simplest option and allows the client browser to fully validate the certificate presented by the application itself. The downside is that by doing this you expose your internal DNS structure, which could be considered a leak of private information through 'Open Source Intelligence' (OSINT) exposure of your private hostnames.

Slide 20 - BA Application Hostname Matching



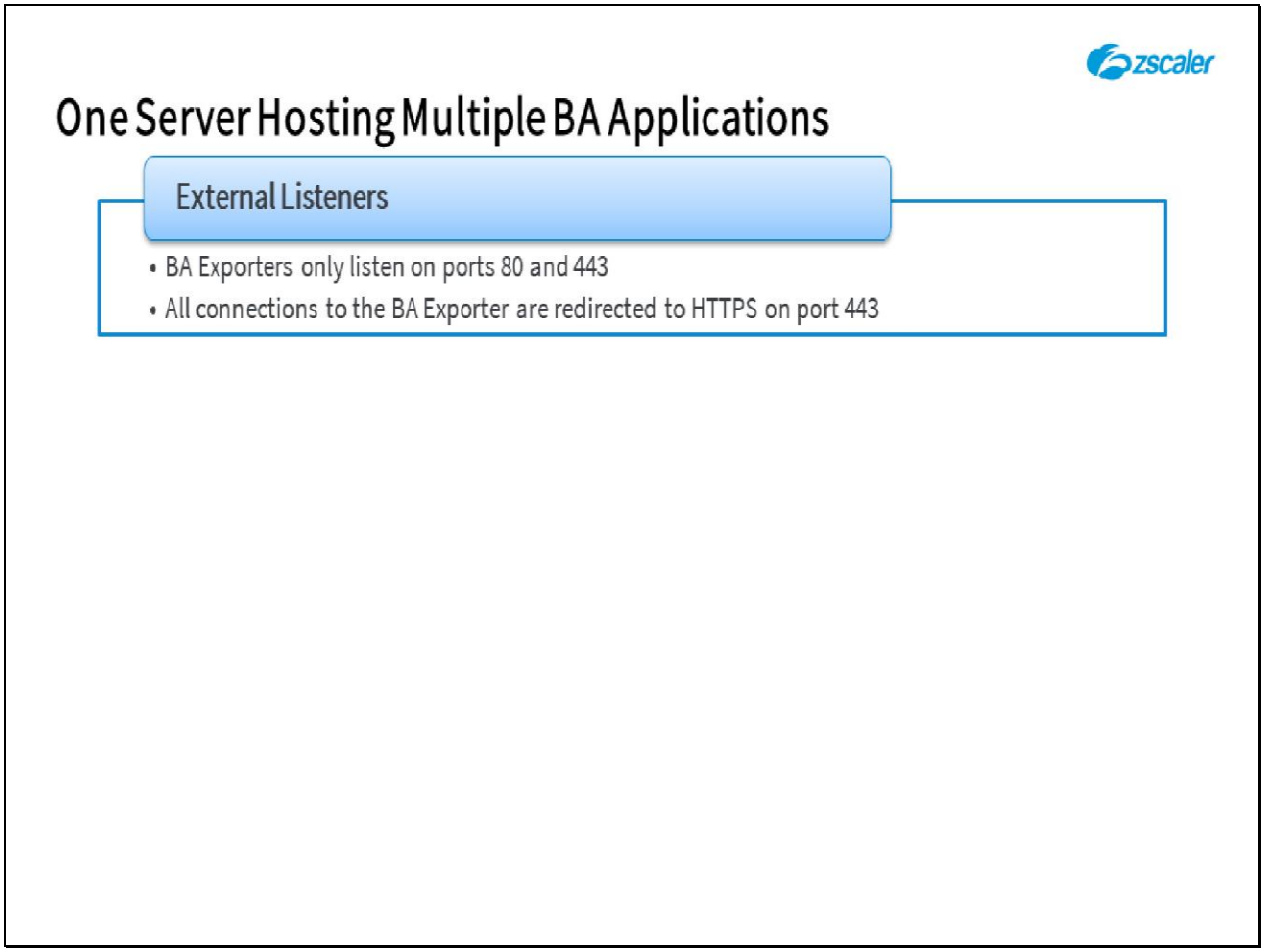
Slide notes

You may elect to use different external hostnames than the existing internal hostnames (e.g. for the internal application **financeapp.corp.com** you might use the external hostname **webapp1.corp.com**), which means you no longer expose your internal DNS structure to the outside world. The disadvantage of this is that on the back-end SSL cannot be verified, and the end user will get a certificate error because the hostname of the internal web application will not match the hostname of the certificate.

In addition, if the web server is multi-tenant (host-header) or doing any cookie domain checking, then the website will most likely break. Unless the web application is coded to take requests irrespective of the FQDN or cookie, avoid hostname rewrite, or place some re-write (WAF/RPROXY) between the connector and the web application. Another consideration is that some internal application domains cannot be used externally (e.g. **corp.local**).

Note that there is no single correct answer here, the best choice will depend on your circumstances, priorities and preferences.

Slide 21 - One Server Hosting Multiple BA Applications

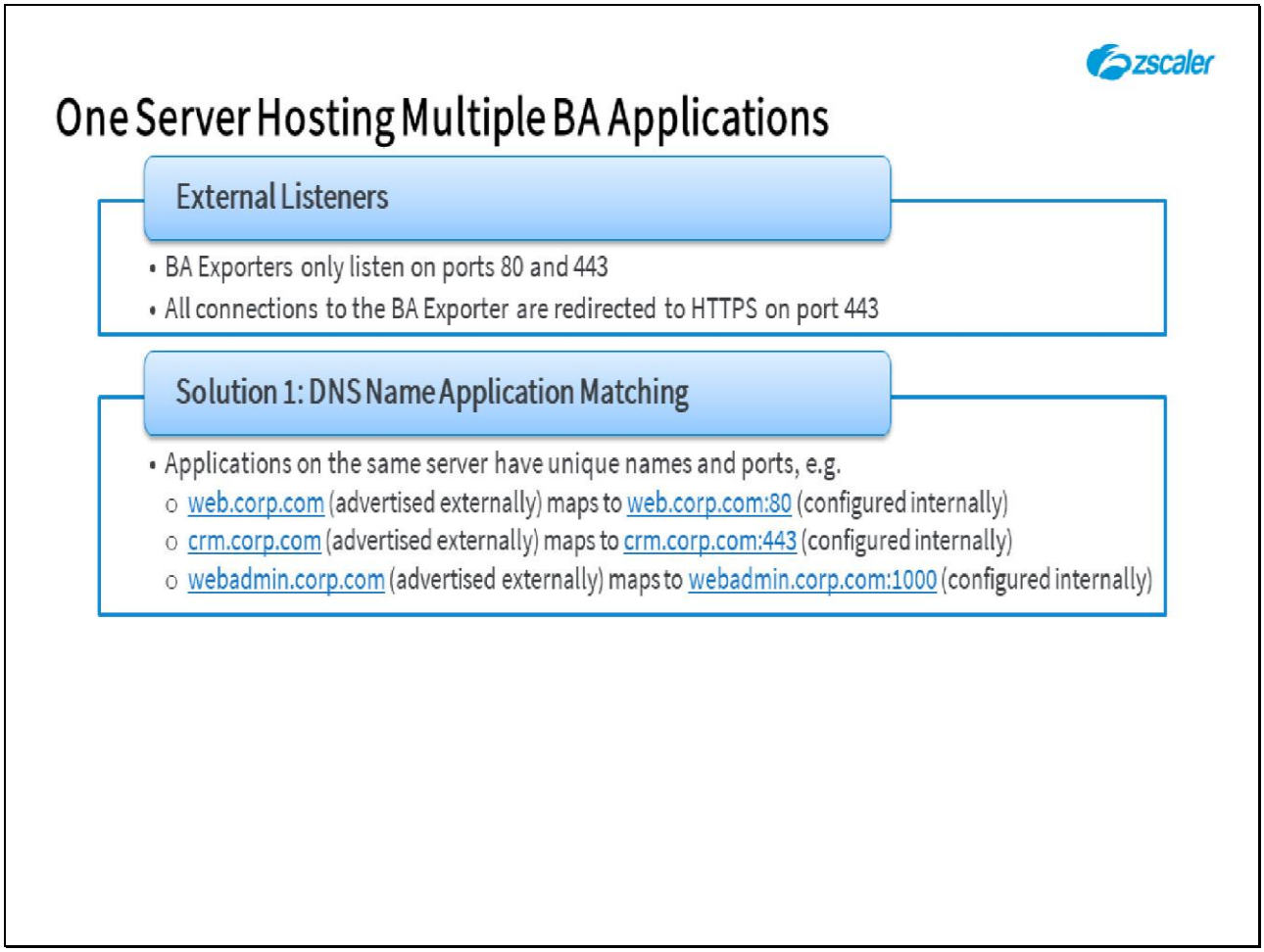


Slide notes

In many cases the applications you wish to make available using BA will be running on a single web server. Since it is not necessary for the externally advertised DNS hostnames to match the internal ones, unmatched hostnames can be used to handle scenarios with one host serving web applications on multiple ports. For Browser Access enabled applications, **BA Exporters** only listen on ports **80** and **443** for inbound connections from web browsers.

A port **80** connection will be automatically redirected to port **443**, while a port **443** connection does domain virtualization though the provided SNI. As a consequence, ZPA only receives one domain name and one port, and mapping that one domain + port combination to multiple ports is not possible. However, you can map ports through multiple domain names using one of the following methods:

Slide 22 - One Server Hosting Multiple BA Applications



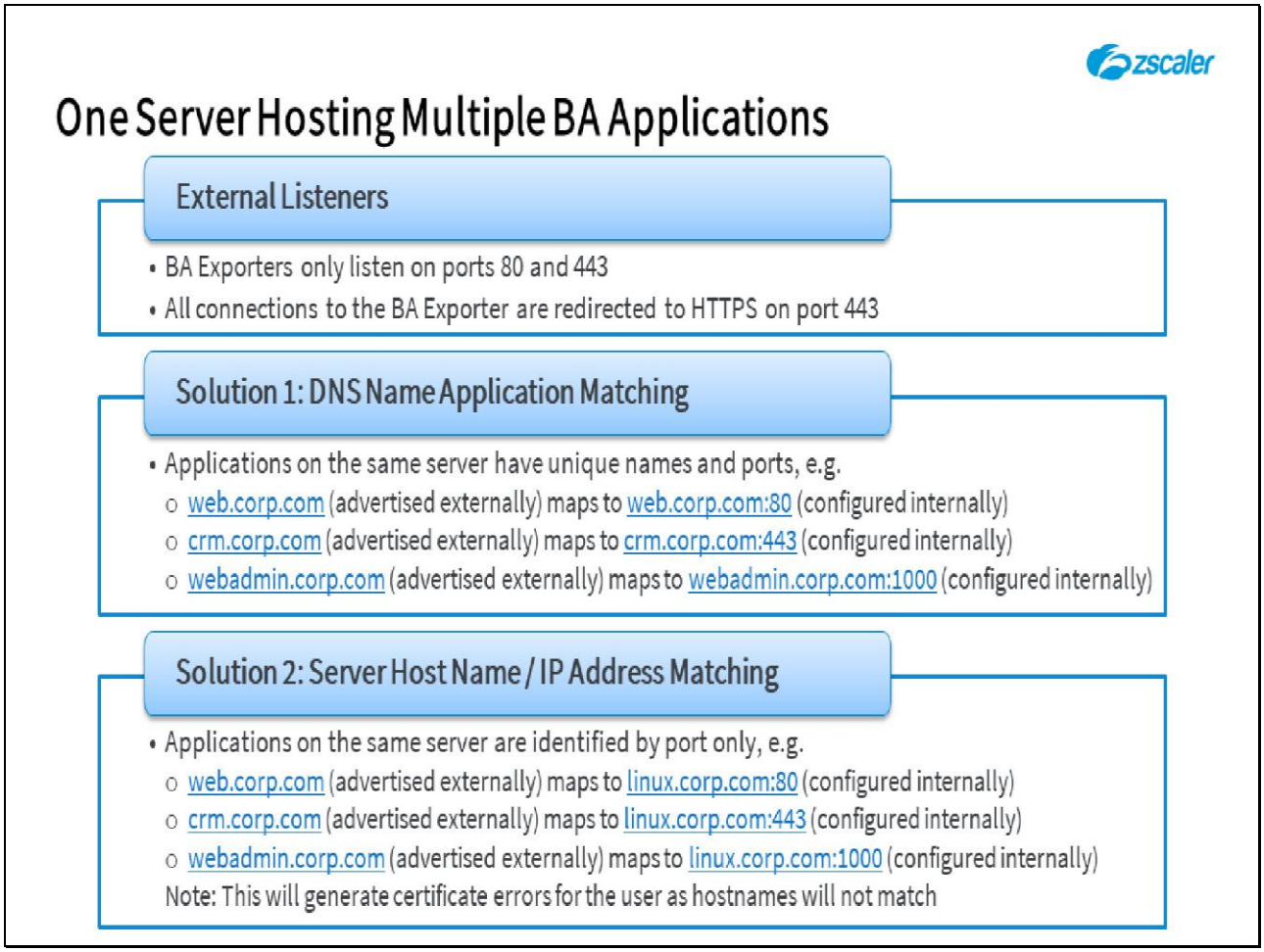
Slide notes

Method 1: Use unique hostnames per application by using your internal DNS or by explicitly defining static servers in ZPA. This will allow the advertising of a unique external hostname, that matches an internal hostname and port combination, for example:

- The host name **web.corp.com** (advertised externally), maps to **web.corp.com:80** (configured internally);
- The host name **crm.corp.com** (advertised externally), maps to **crm.corp.com:443** (configured internally);
- The host name **webadmin.corp.com** (advertised externally), maps to **webadmin.corp.com:1000** (configured internally).

This configuration will work directly, as dynamic server discovery for all three applications will work as long as internal DNS for those 3 host names is configured. If internal DNS doesn't exist for those three hostnames, then you would have to explicitly define static servers within the ZPA Admin Portal for them.

Slide 23 - One Server Hosting Multiple BA Applications



Slide notes

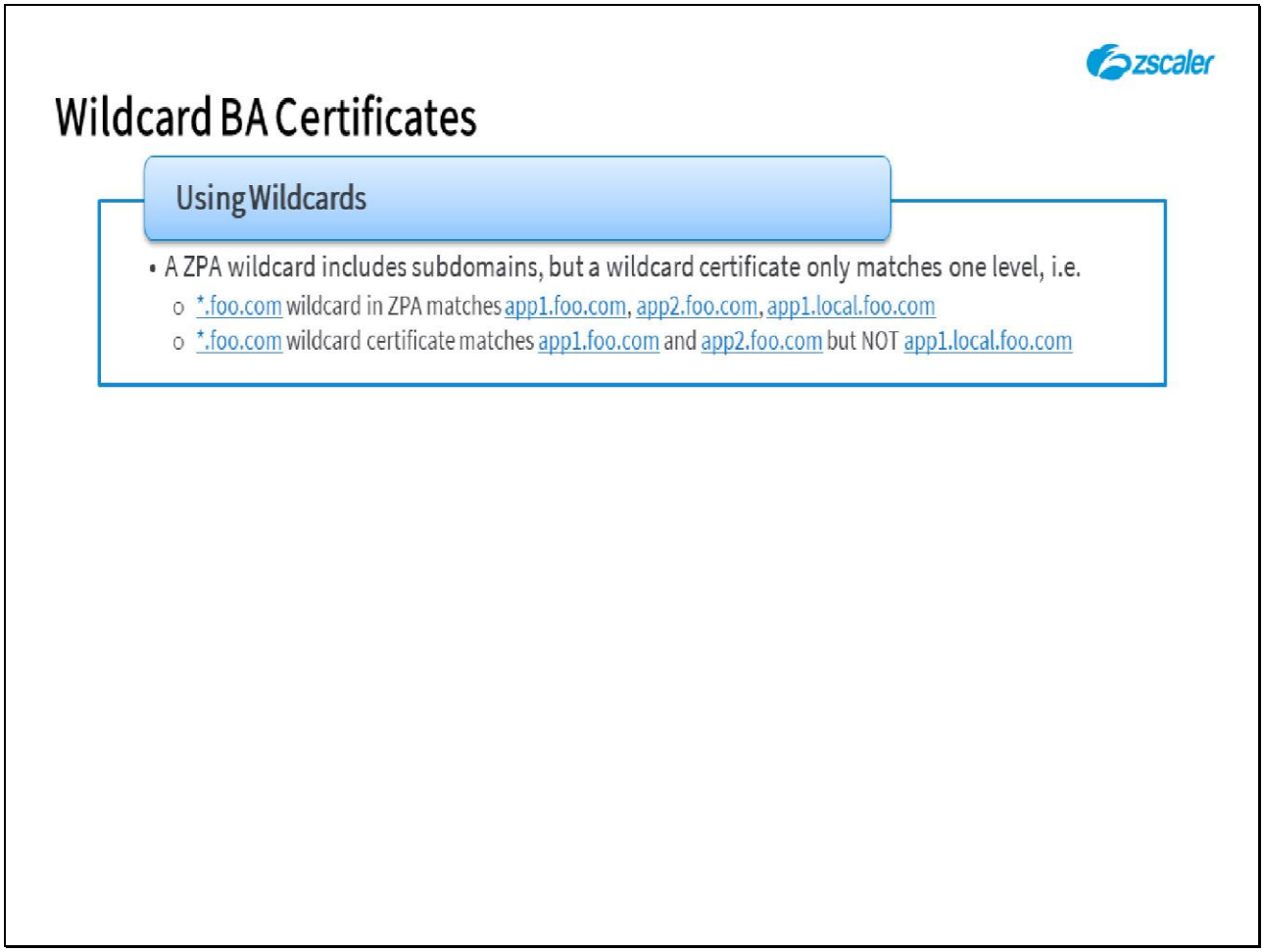
Method 2: You can define the applications within an application segment internally to point to a specific hostname or IP address. However, this will cause certificate validation problems because the hostname check will fail, so users will see web server certificate errors when connecting to the applications. In this case you might configure:

- The host name **web.corp.com** (advertised externally) maps to **linux.corp.com:80** (configured internally);
- The host name **crm.corp.com** (advertised externally) maps to **linux.corp.com:443** (configured internally);
- The host name **webadmin.corp.com** (advertised externally) maps to **linux.corp.com:1000** (configured internally).

Note: You would need to manually add a server in the ZPA Admin Portal and map it to the appropriate Server Group (e.g., Server Group **linux.corp.com** has server **linux.corp.com**), with multiple Connector Groups as necessary. Or the server might be specified by IP address instead. Then you can have all three applications use the same Server Group, but you would not be able to verify web server certificates.

Zscaler recommends using Method 1 as Method 2 does not provide a satisfactory usability experience for your end users.

Slide 24 - Wildcard BA Certificates



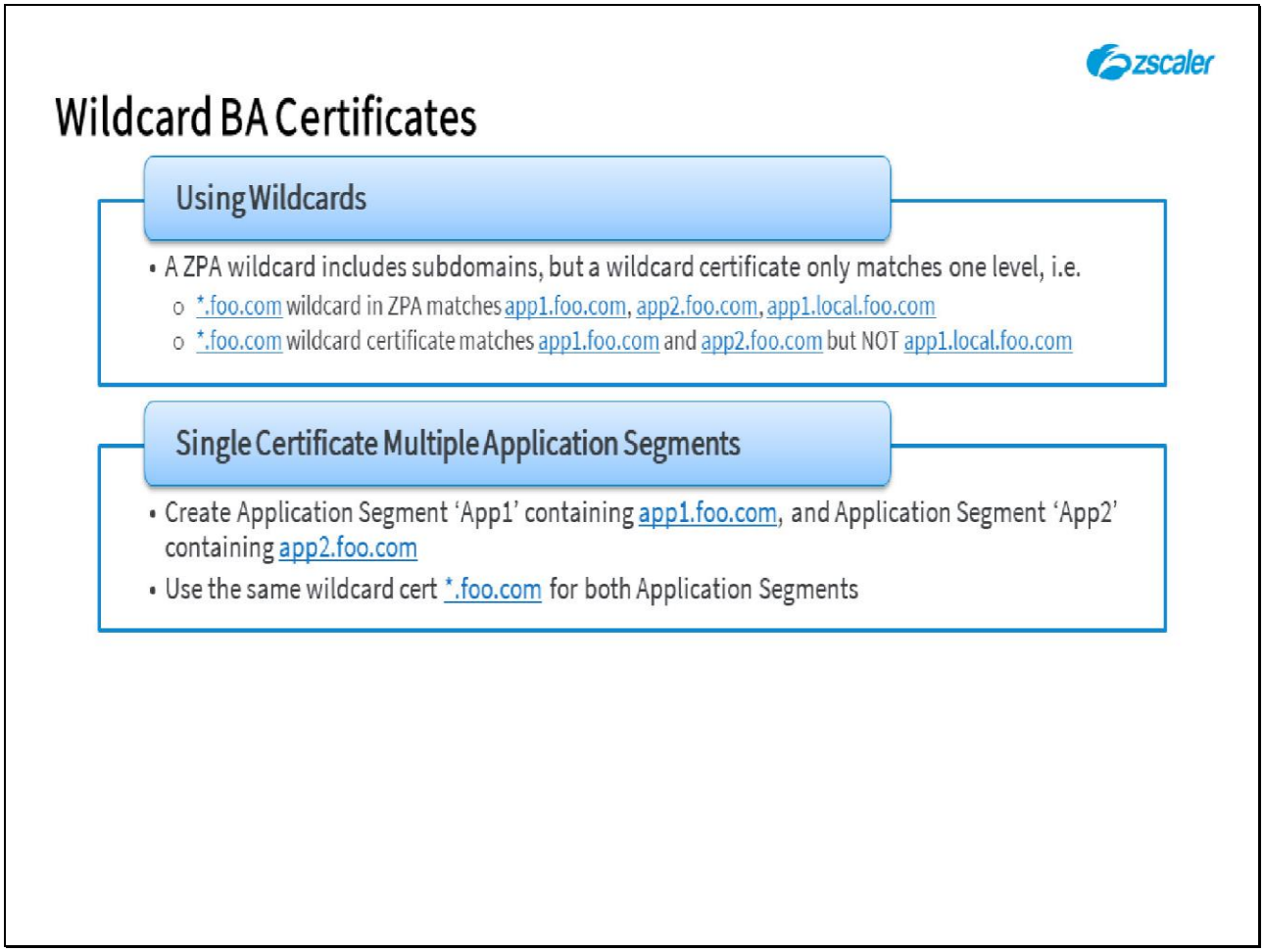
Slide notes

You can use a wildcard certificate for multiple FQDNs in the one application Segment, or for multiple FQDNs in multiple application Segments, for example, you may create application Segment **App1** containing **app1.foo.com**, and application Segment **App2** containing **app2.foo.com**, and use the same wildcard certificate ***.foo.com** within both Application Segments for those applications.

However, there is a complication here, namely that a ZPA wildcard application includes subdomains, but a wildcard certificate will only match a single level, i.e.:

- The ***.foo.com** wildcard application in ZPA will match all three of **app1.foo.com**, **app2.foo.com**, **app1.local.foo.com**;
- The ***.foo.com** wildcard certificate will match **app1.foo.com** and **app2.foo.com** but will NOT match **app1.local.foo.com**, so the browser will reject the certificate as not trusted for **app1.local.foo.com**.

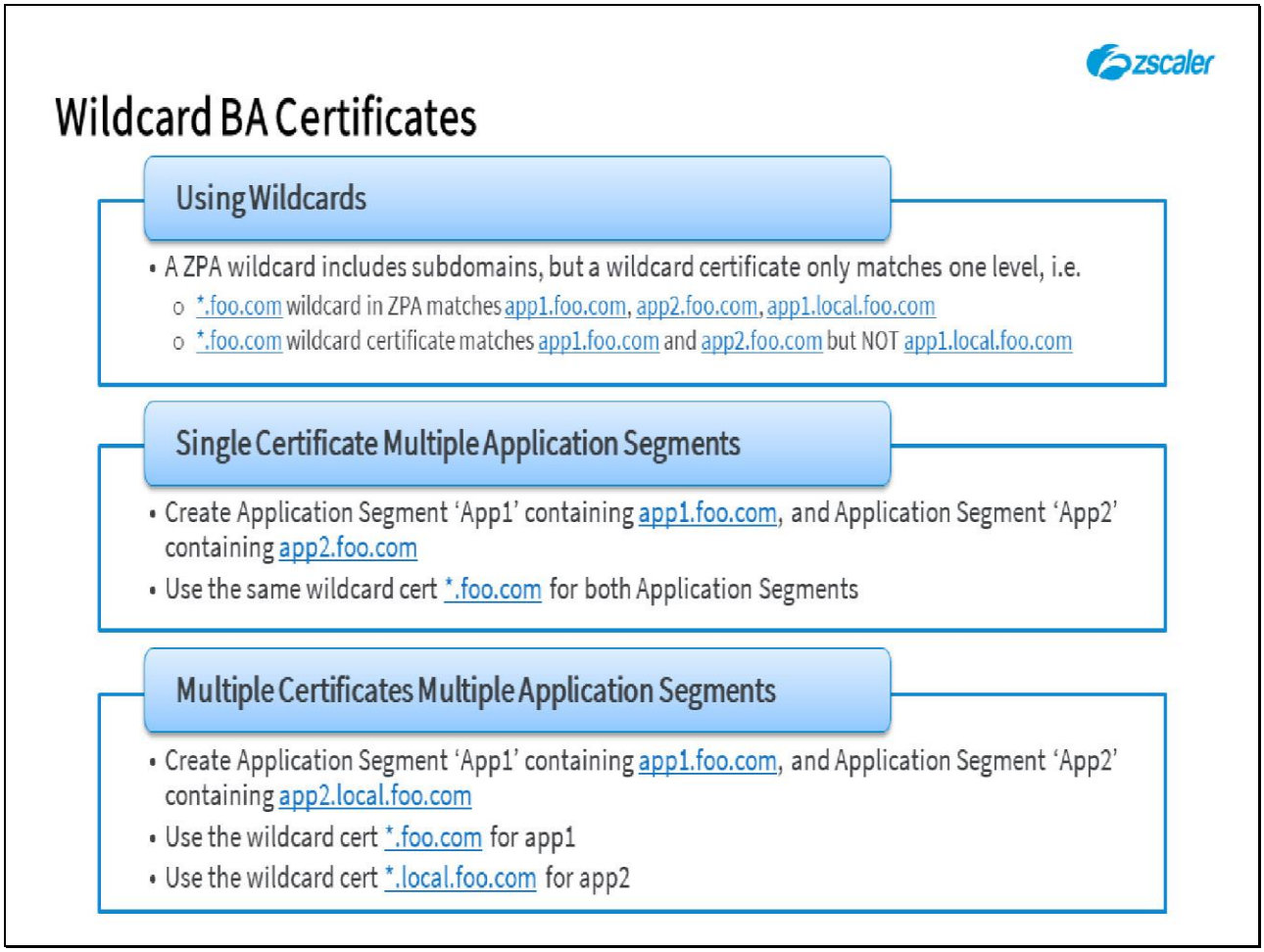
Slide 25 - Wildcard BA Certificates



Slide notes

If you want to use wildcard access for applications on the one subdomain, you can add a single wildcard application. For example, the wildcard ***.foo.com**, with an equivalent wildcard certificate.

Slide 26 - Wildcard BA Certificates



Slide notes

If you want wildcard access for several subdomains, then you should add separate wildcard applications. For example, the wildcard applications ***.foo.com** and ***.local.foo.com**, with equivalent wildcard certificates.

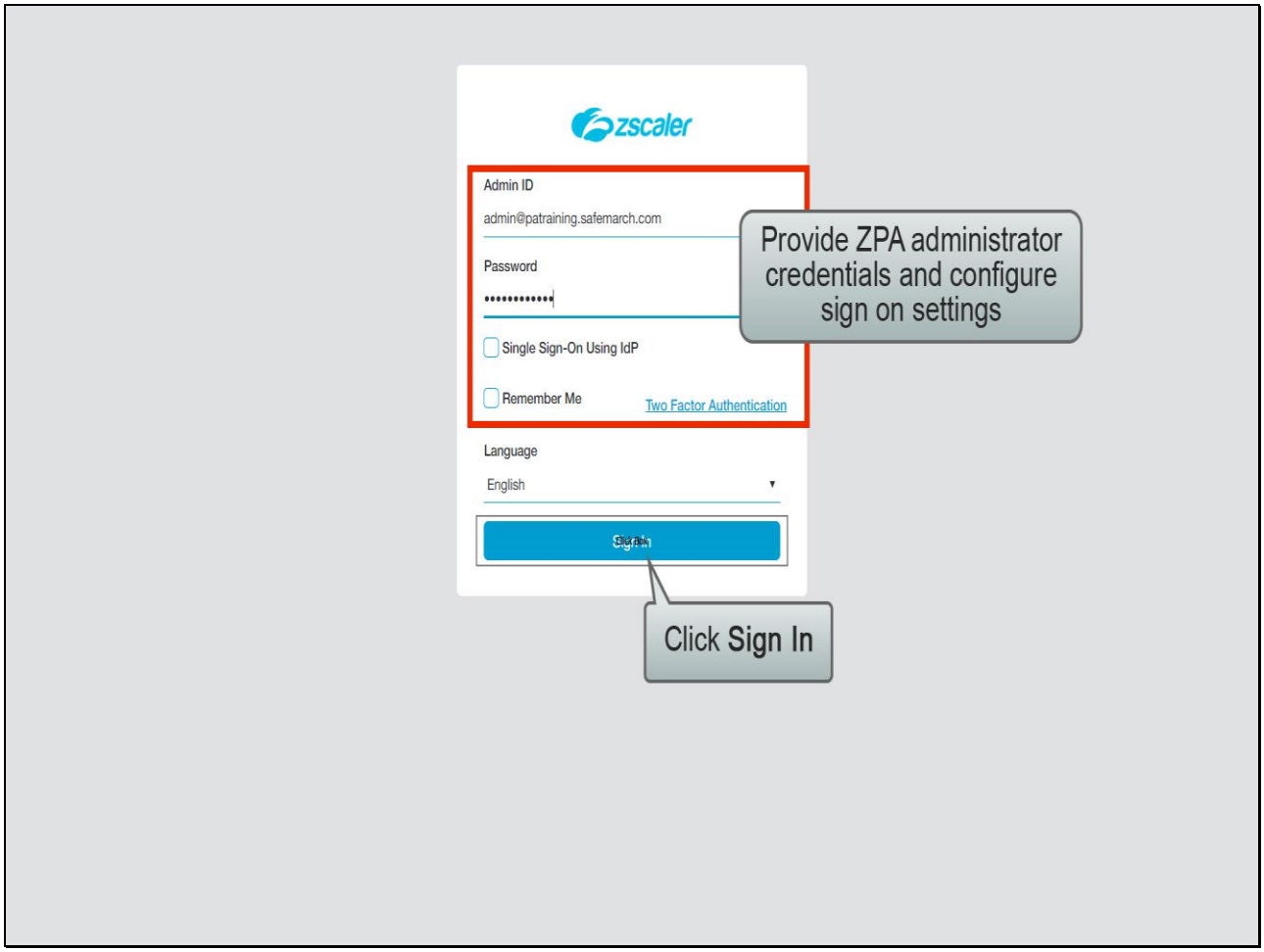
Slide 27 - Browser Access Configuration

Slide notes

In the next section, we will step through the process to create a Browser Access certificate.

This section has been created as an interactive demo to give you a feel for the navigation of the ZPA Admin 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 28 - Slide 28

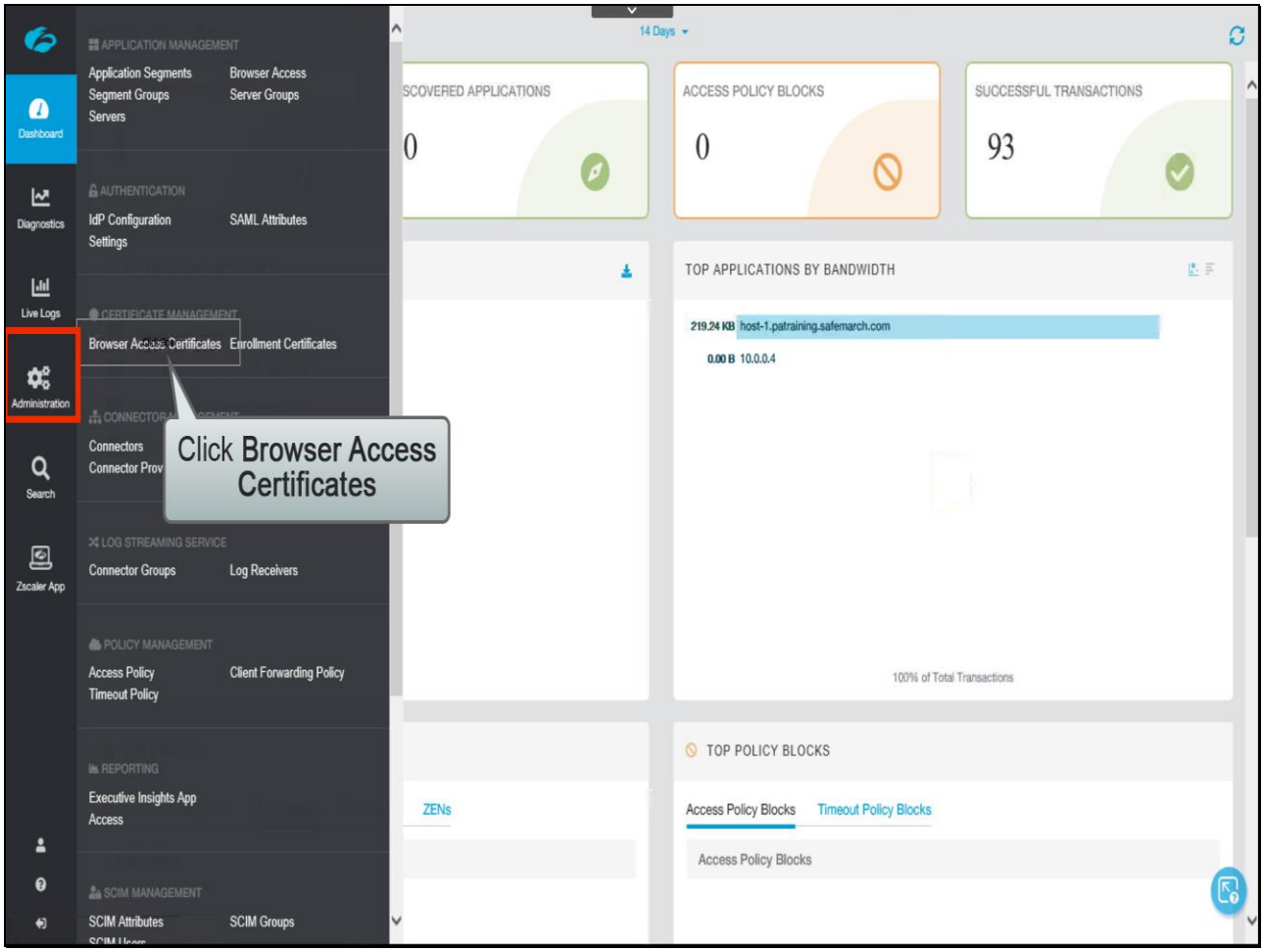


Slide notes

For this example, we will request a web certificate from an enterprise private CA, that our end user is able to trust. Under most circumstances you would request a certificate from a public CA.

Open the ZPA Admin Portal in a browser on a machine with access to your corporate Certificate Services web enrollment pages. Enter valid admin user credentials, configure sign on options as necessary and click **Sign In**.

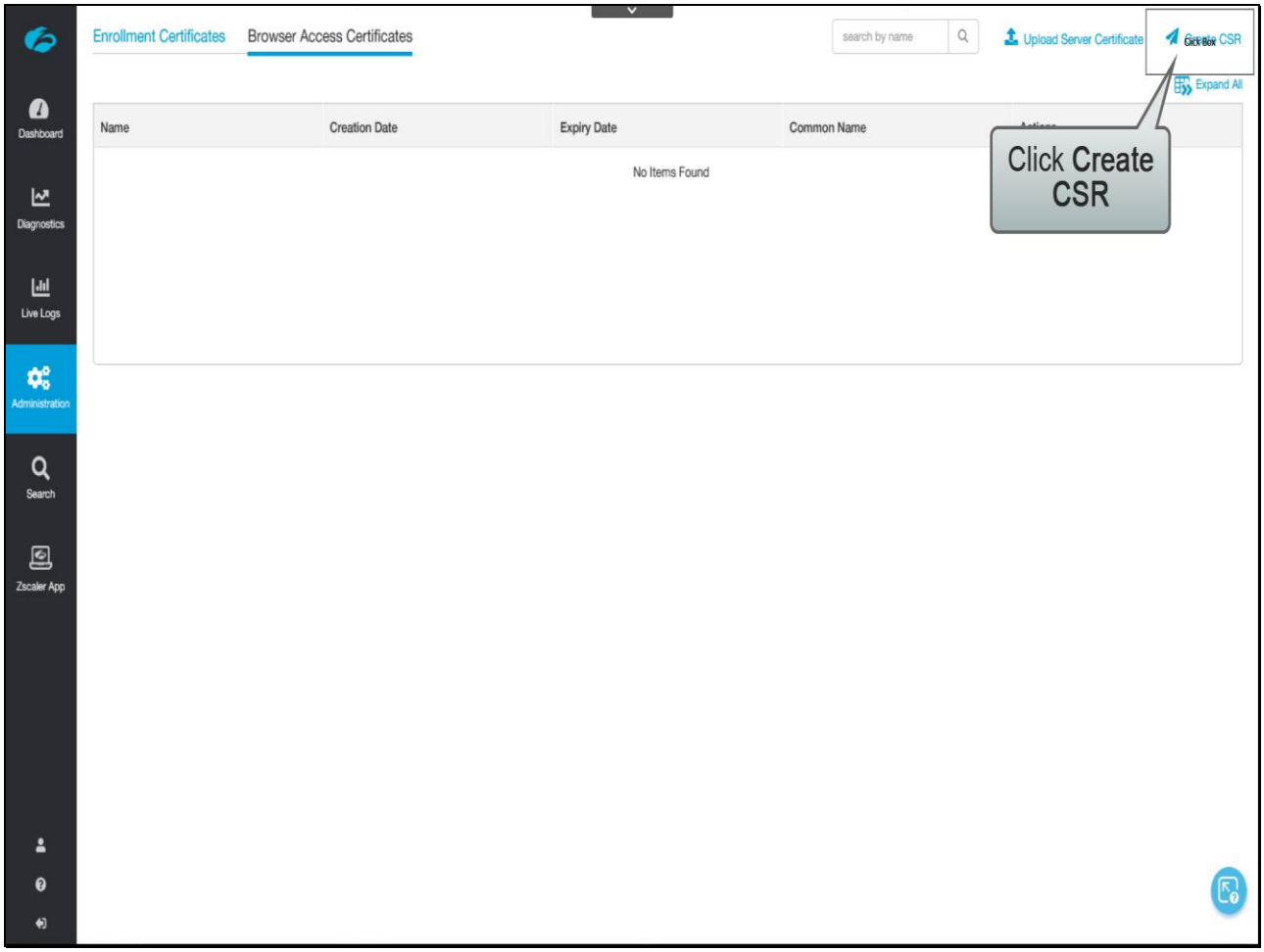
Slide 29 - Slide 29



Slide notes

From the **Administration** menu, under **CERTIFICATE MANAGEMENT**, click **Browser Access Certificates**.

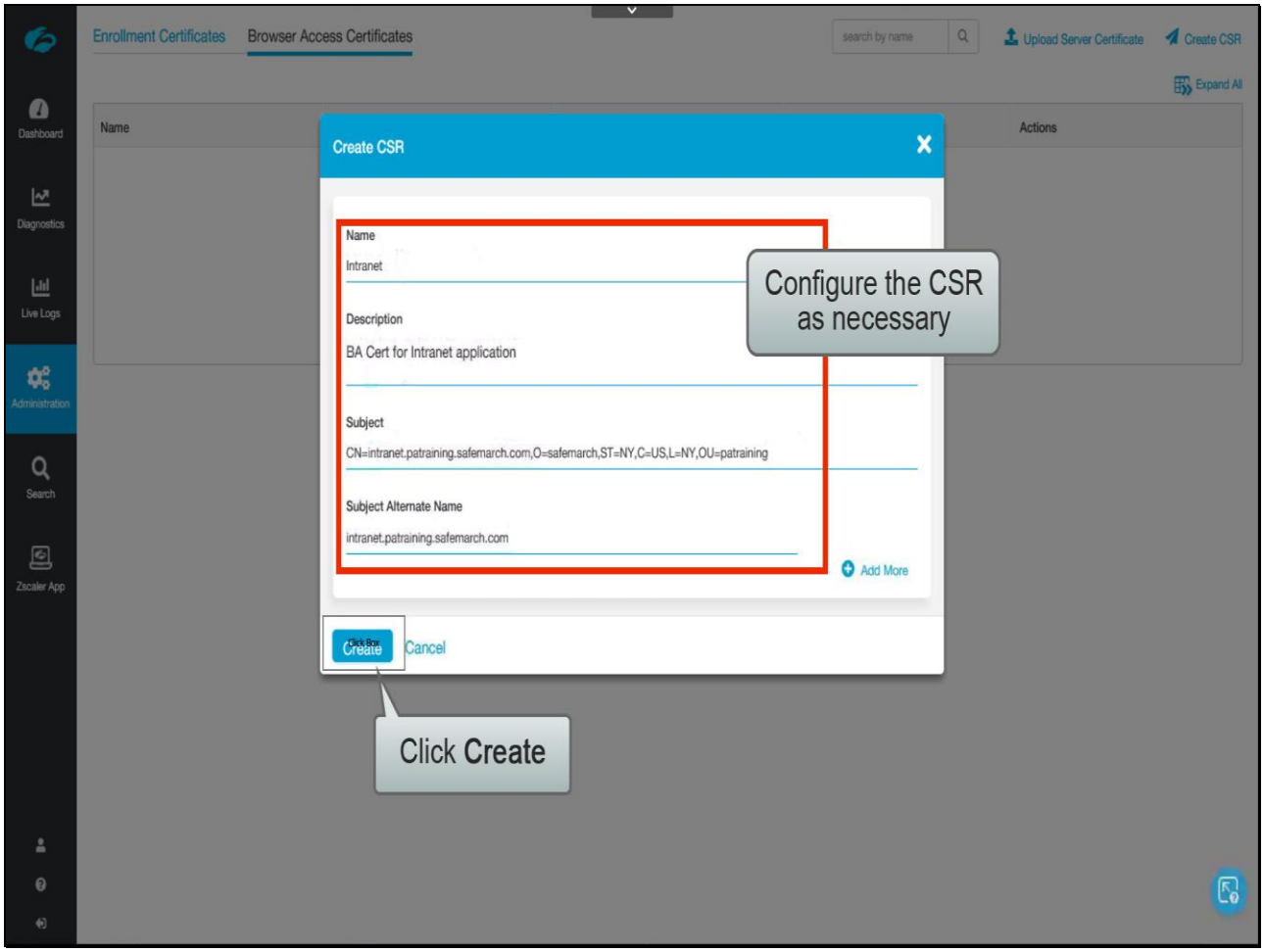
Slide 30 - Slide 30



Slide notes

To create a Certificate Signing Request (CSR) for a new Browser Access certificate, click **Create CSR**.

Slide 31 - Slide 31



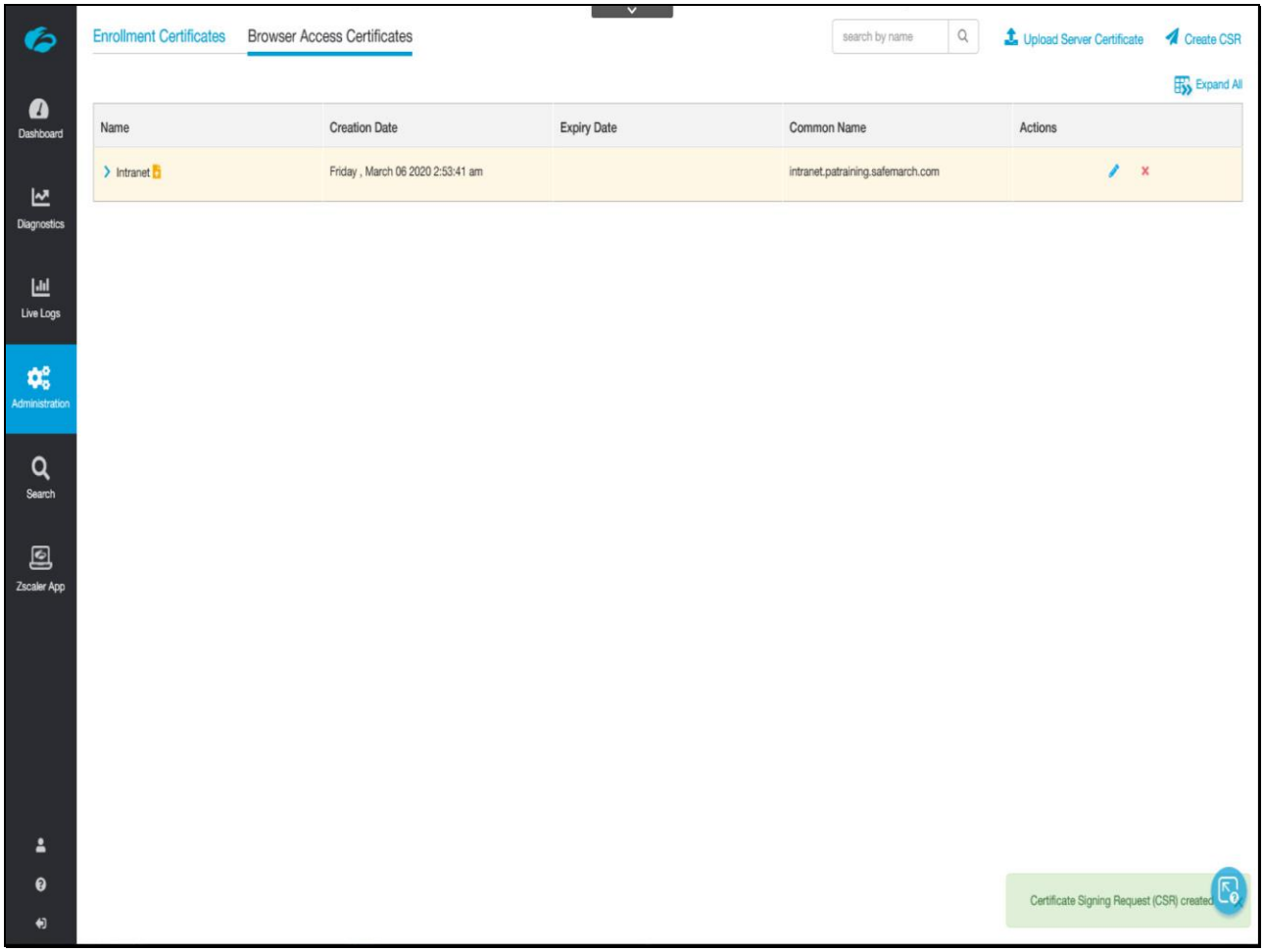
Slide notes

Name the certificate, optionally provide a description, then configure the **Subject** using the X.520 syntax for Relative Distinguished Names (RDN), where:

- **C** = Country,
- **ST** = State,
- **L** = Locale,
- **O** = Organization,
- **OU** = Organizational Unit,
- **A**nd **CN** = Common Name (note that the **CN** attribute must be listed first).

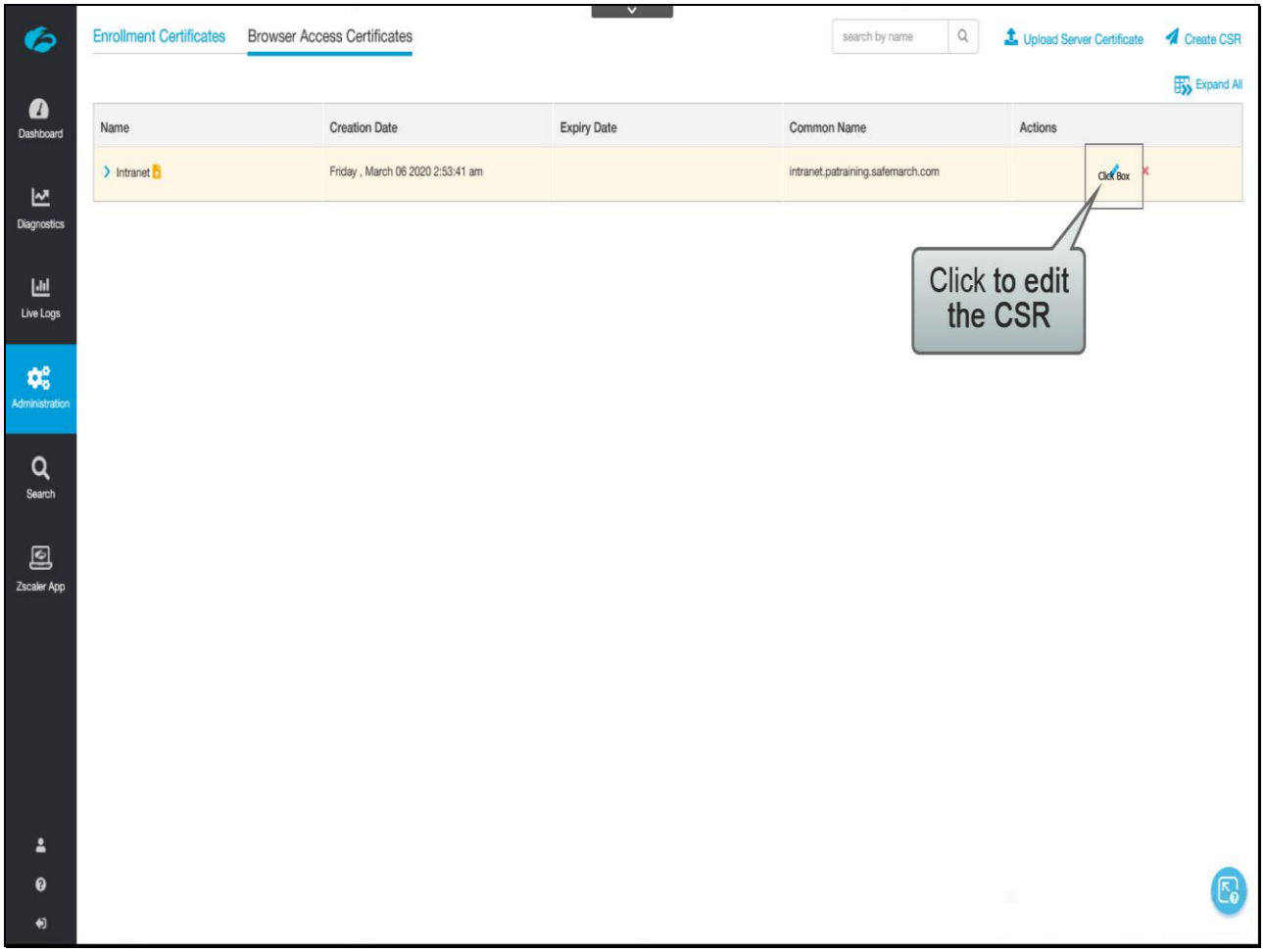
Add a **Subject Alternate Name** if required (this should match the **CN** of the **Subject** field) and click **Create**.

Slide 32 - Slide 32



Slide notes

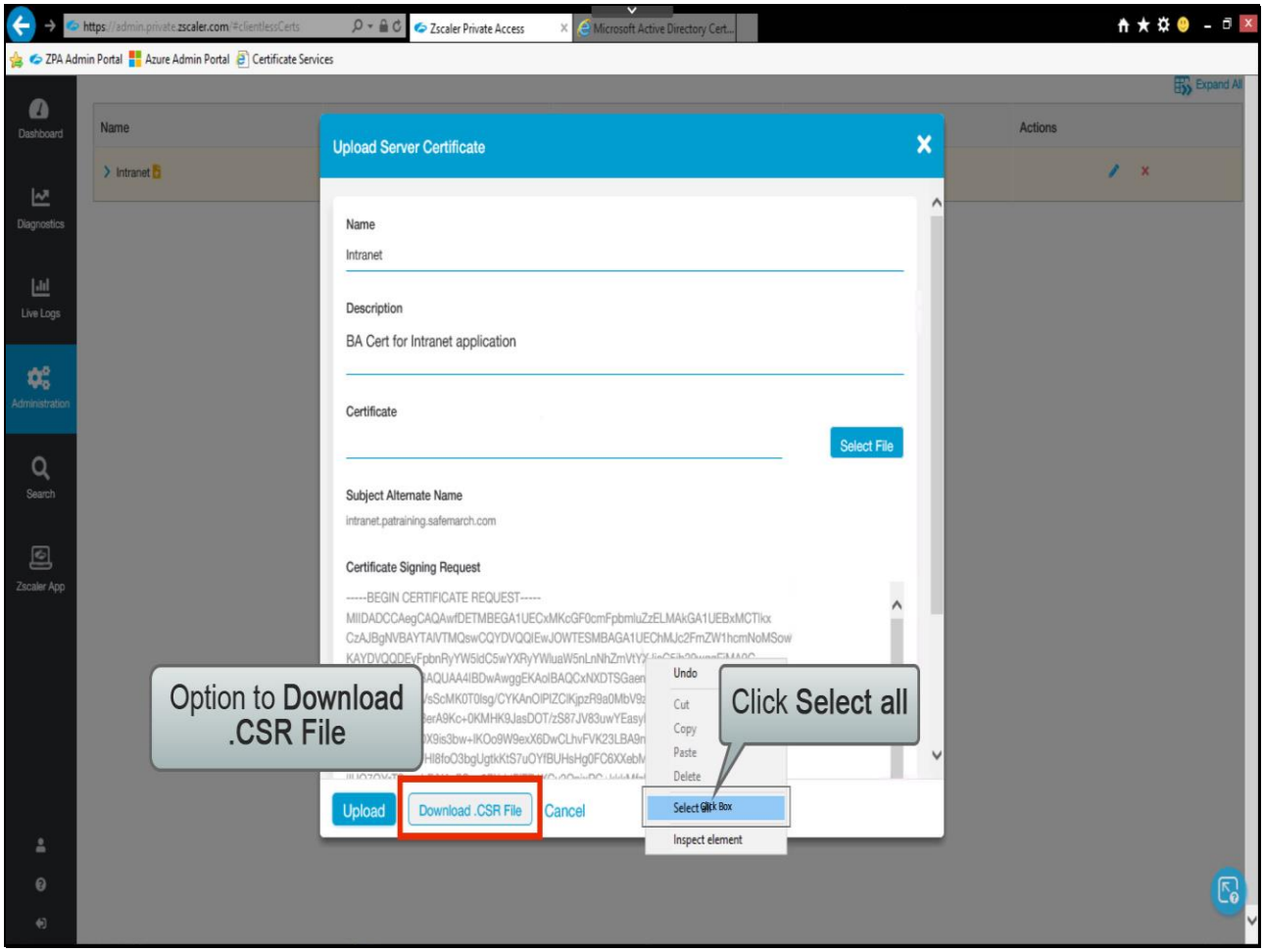
Slide 33 - Slide 33



Slide notes

Click to edit the new CSR, …

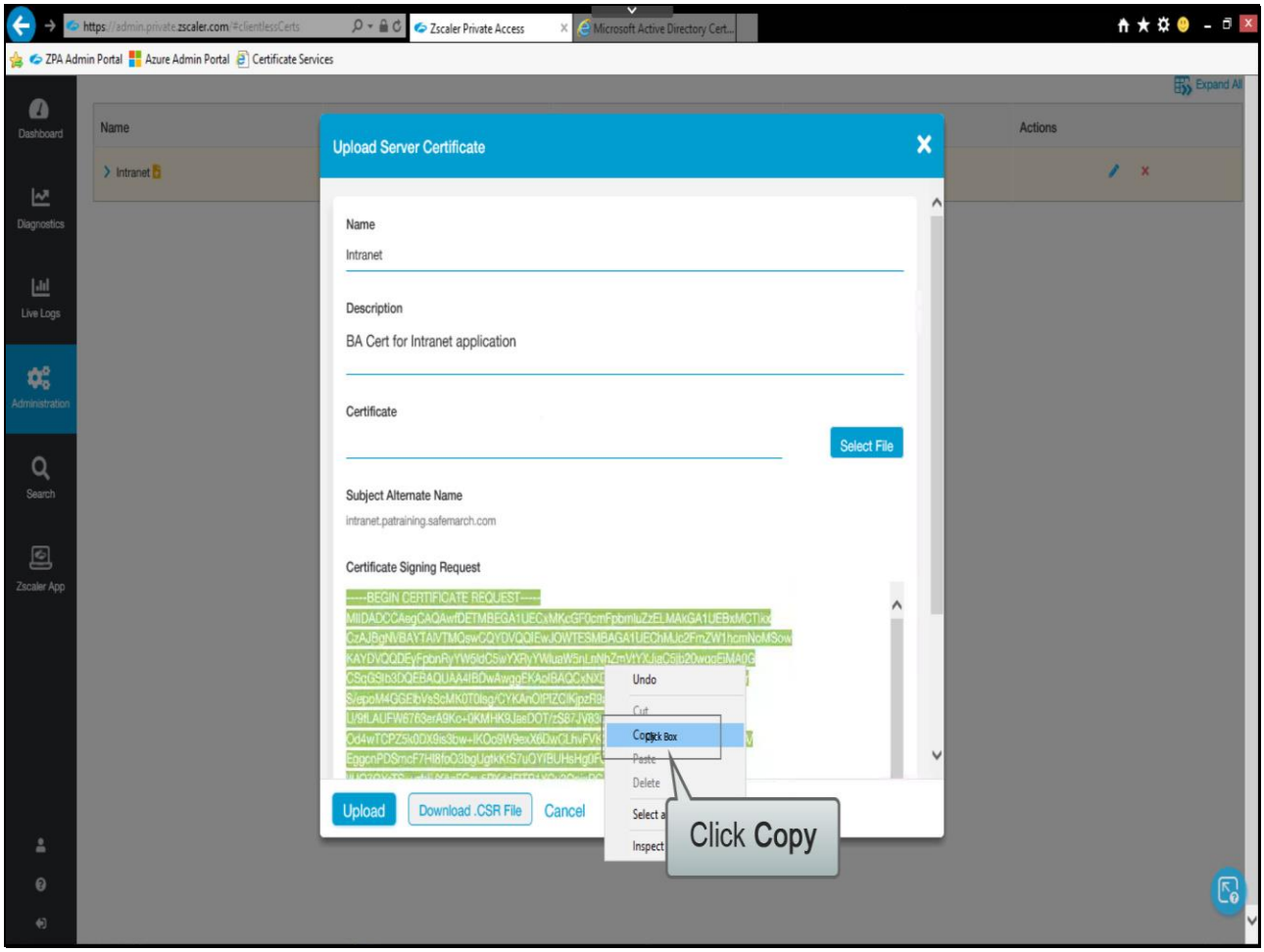
Slide 34 - Slide 34



Slide notes

As with the CSRs for the **Enrollment Certificates**, you have the option here to save the CSR data to file. We will do this in memory however, so right-click in the data for the **Certificate Signing Request** and click **Select All**, …

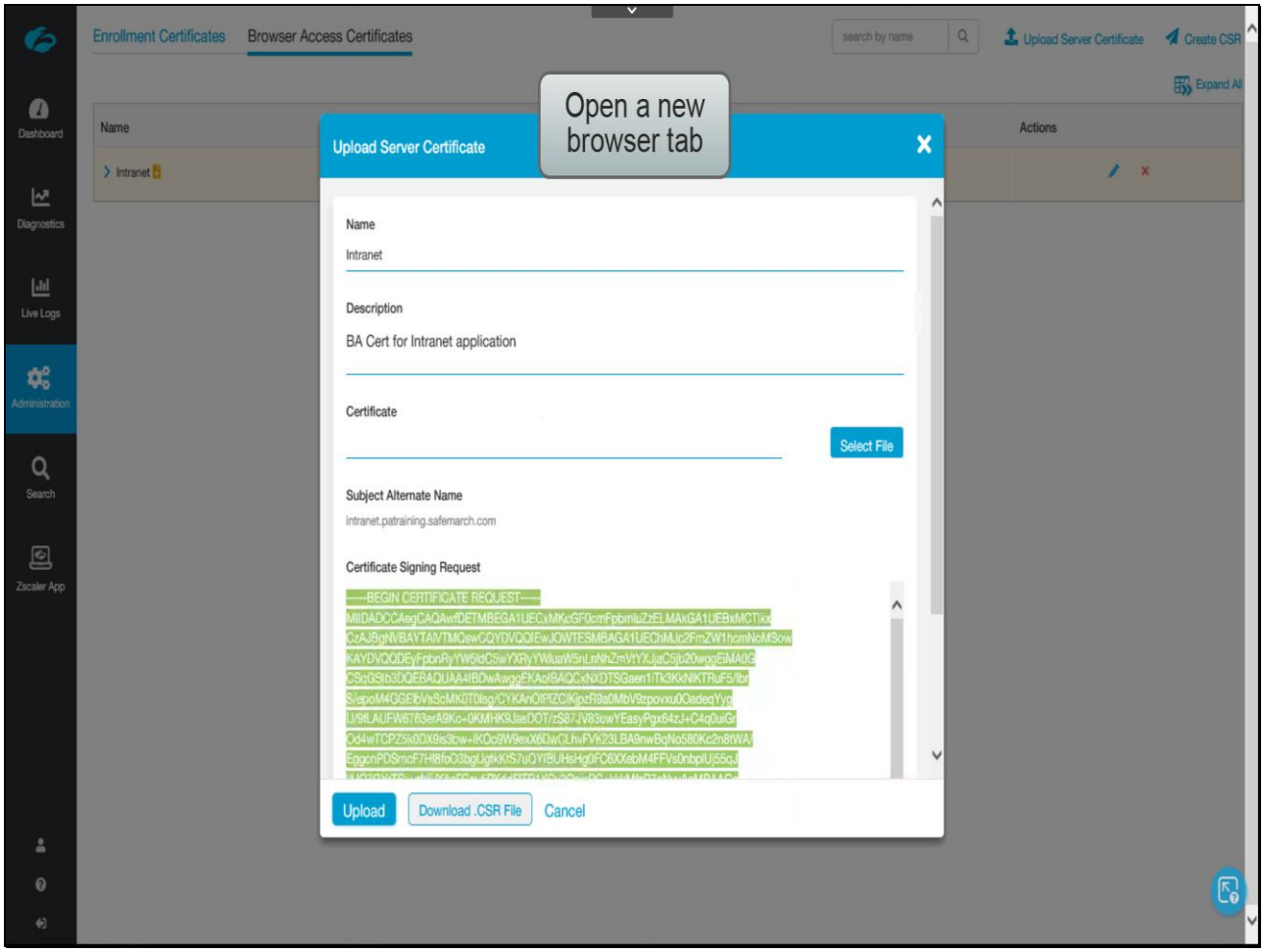
Slide 35 - Slide 35



Slide notes

…then right-click and click **Copy**.

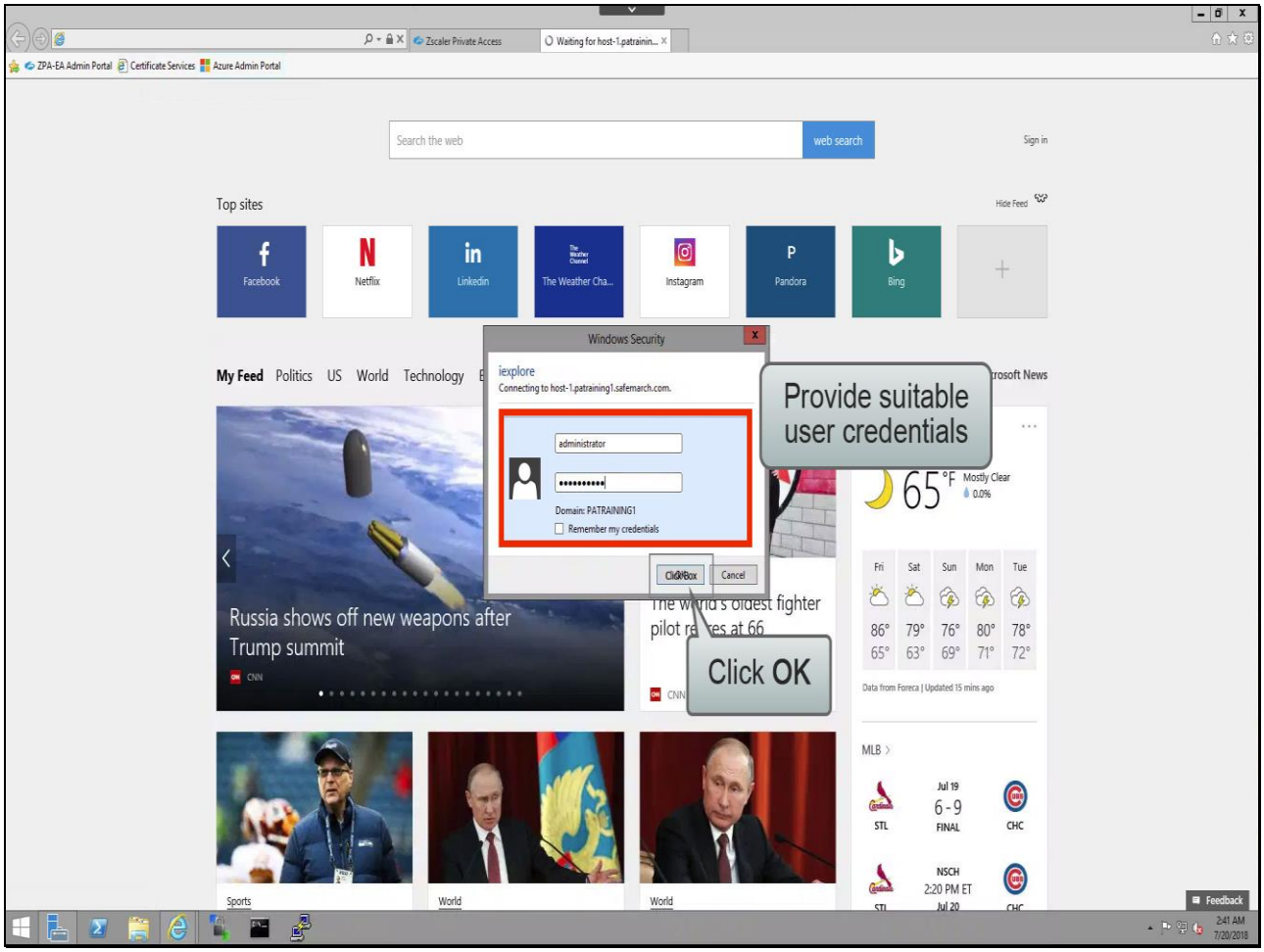
Slide 36 - Slide 36



Slide notes

Click to open a new browser tab, …

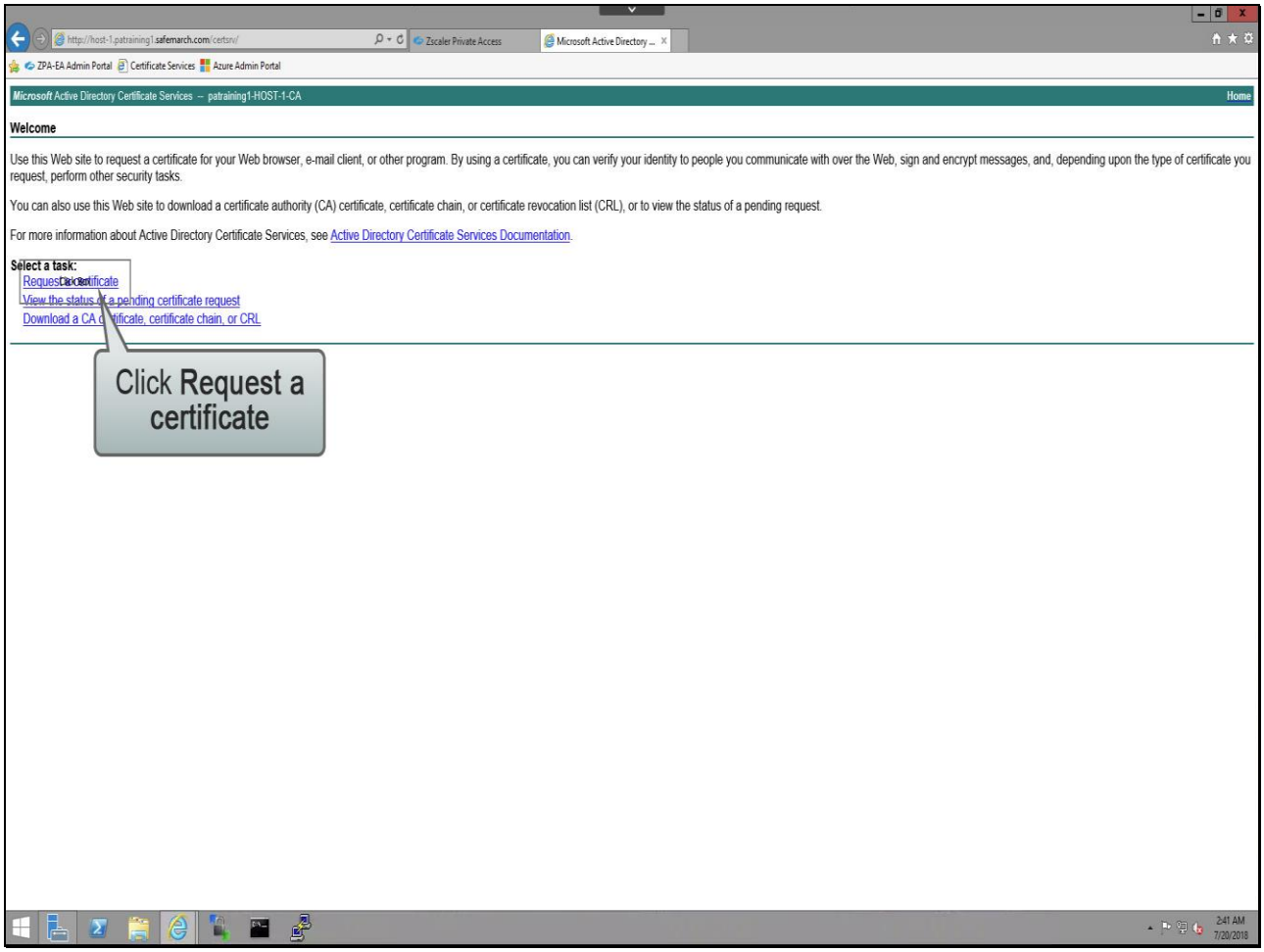
Slide 37 - Slide 37



Slide notes

…navigate to your corporate Certificate Services home page, provide credentials for a user with permissions to generate web server certificates and click **OK**.

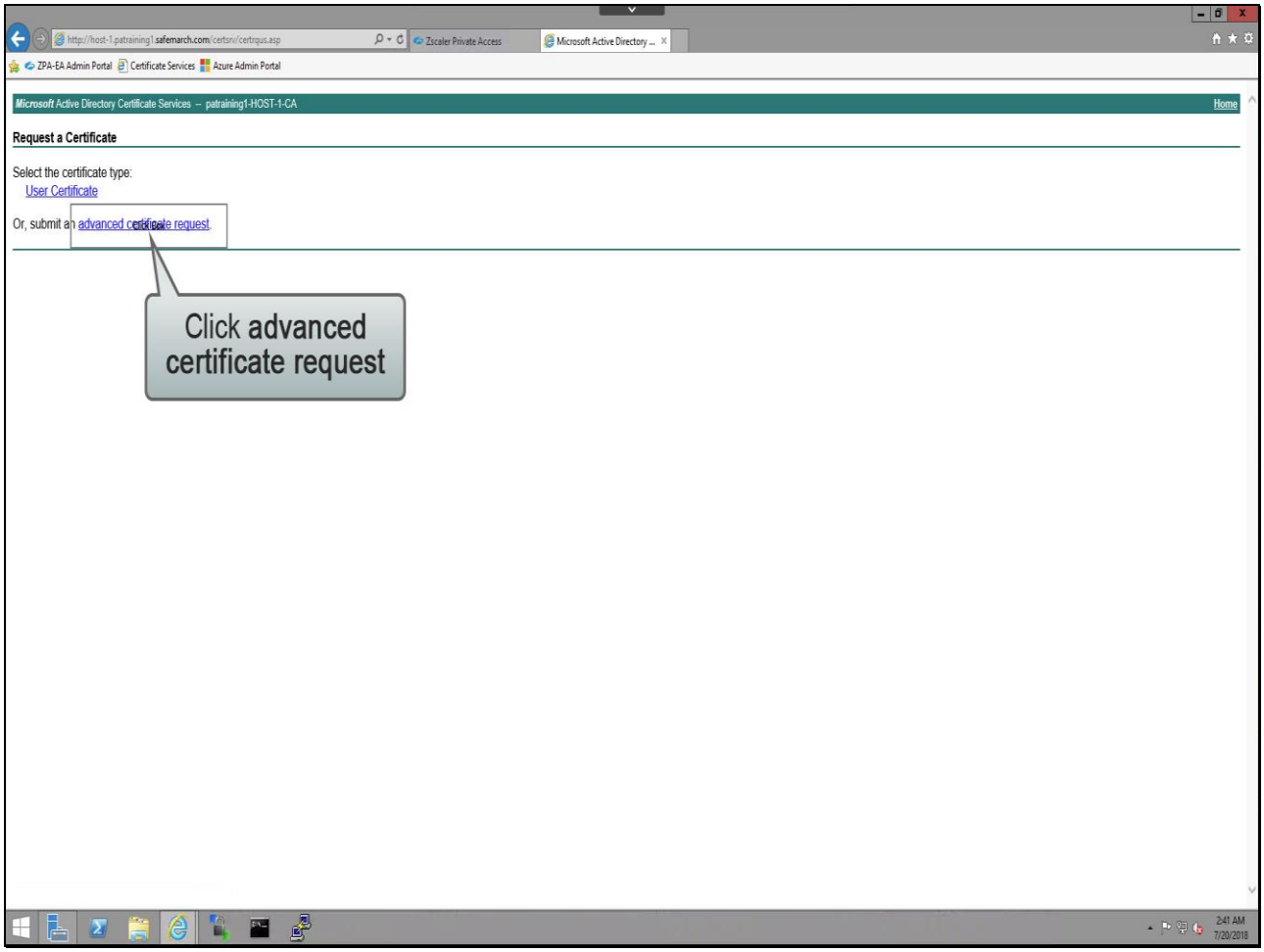
Slide 38 - Slide 38



Slide notes

Click **Request a certificate**, …

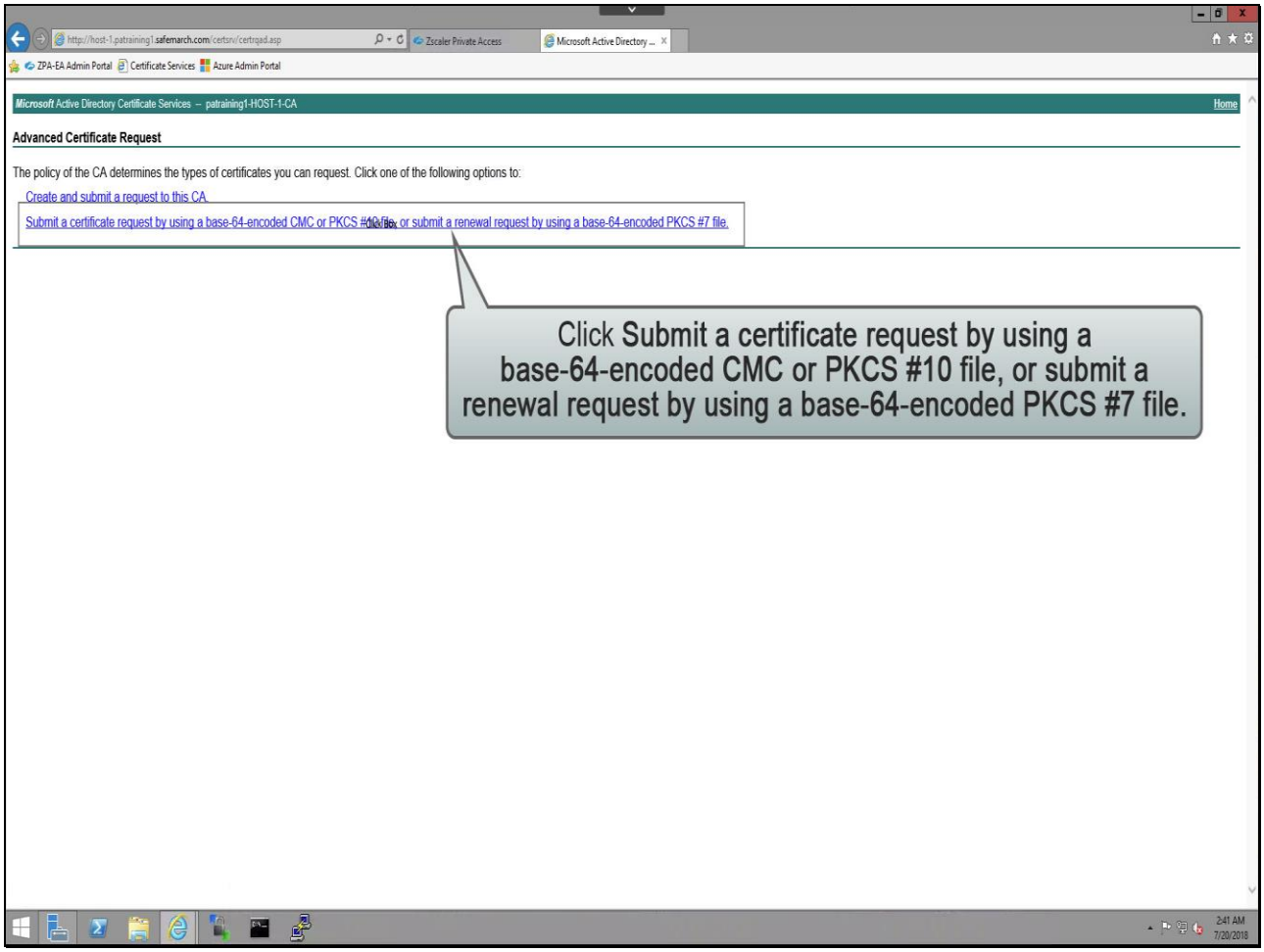
Slide 39 - Slide 39



Slide notes

…then click **advanced certificate request**, …

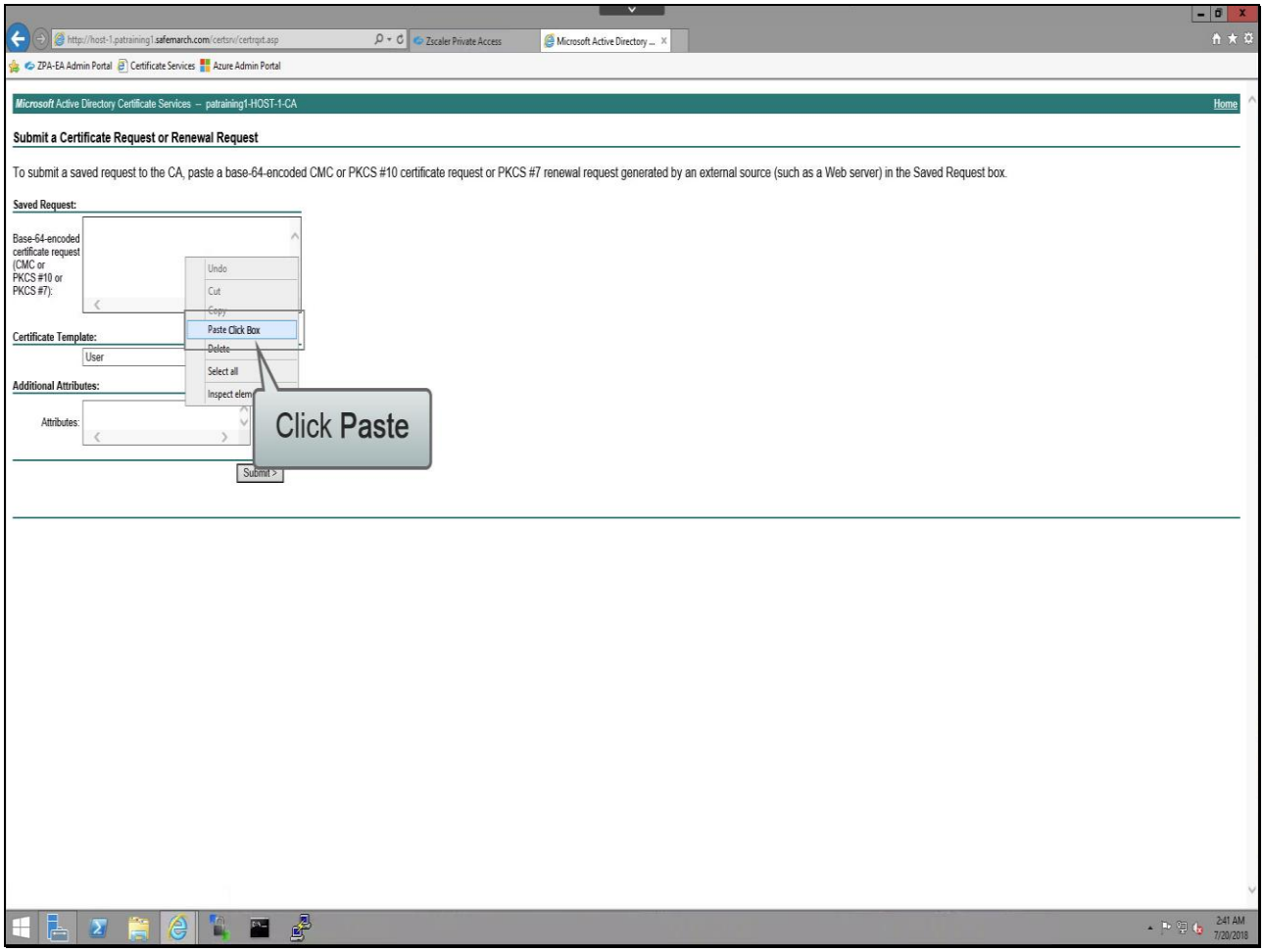
Slide 40 - Slide 40



Slide notes

…then click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS #7 file.**

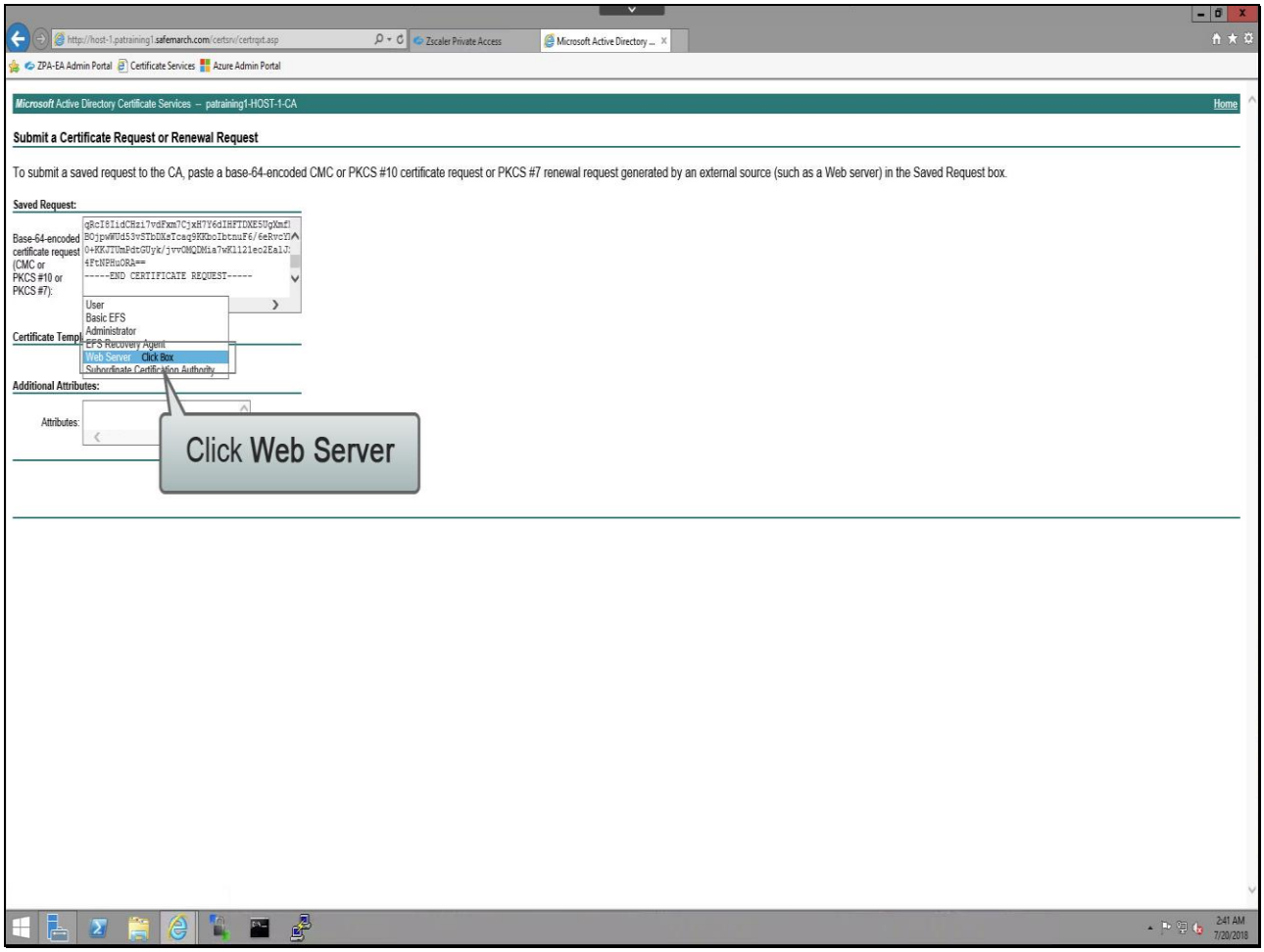
Slide 41 - Slide 41



Slide notes

Right-click in the **Saved Request** field and click **Paste**.

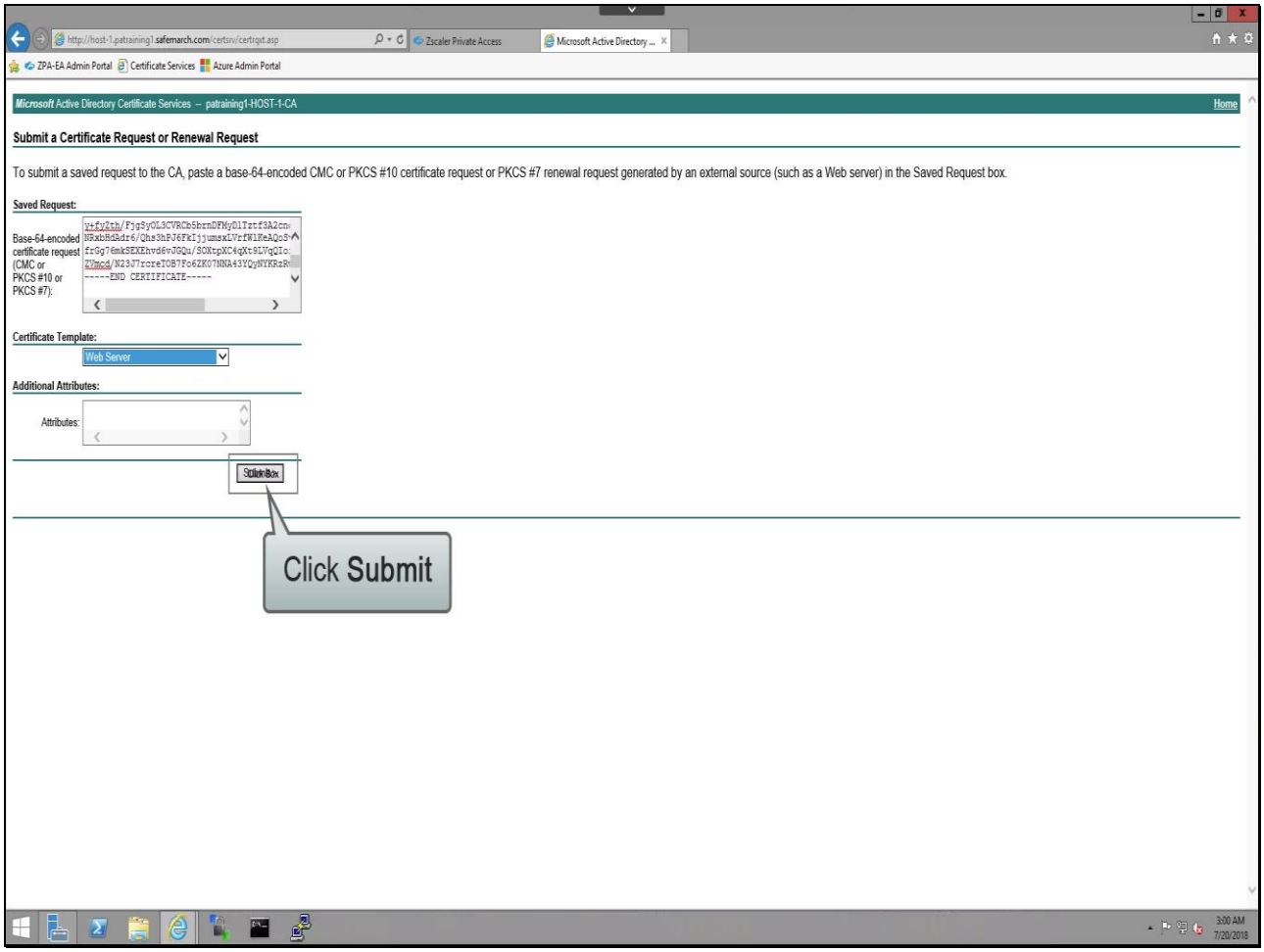
Slide 42 - Slide 42



Slide notes

Click on **Web server** in the **Certificate Template** drop-down list, …

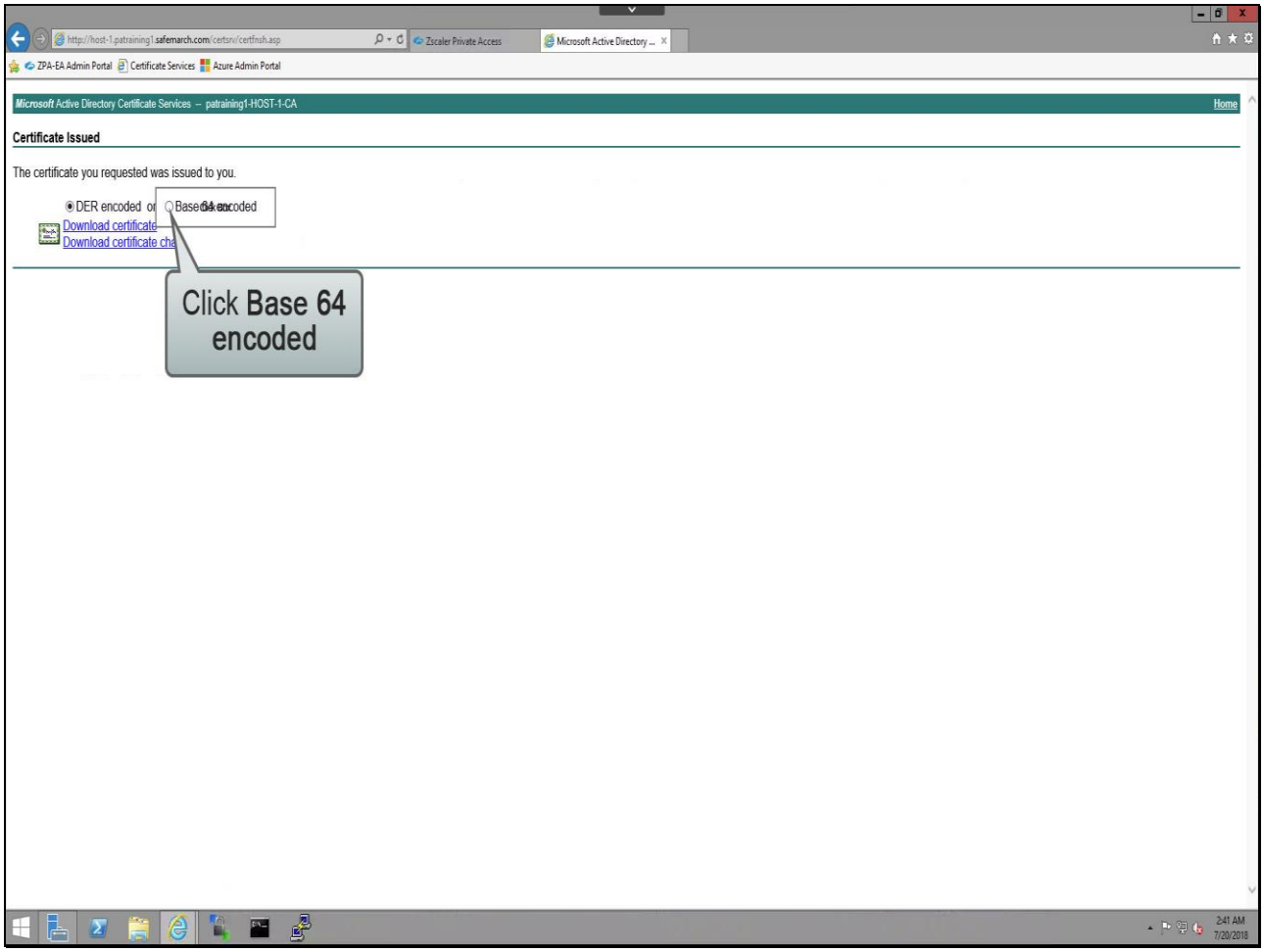
Slide 43 - Slide 43



Slide notes

…then click **Submit**.

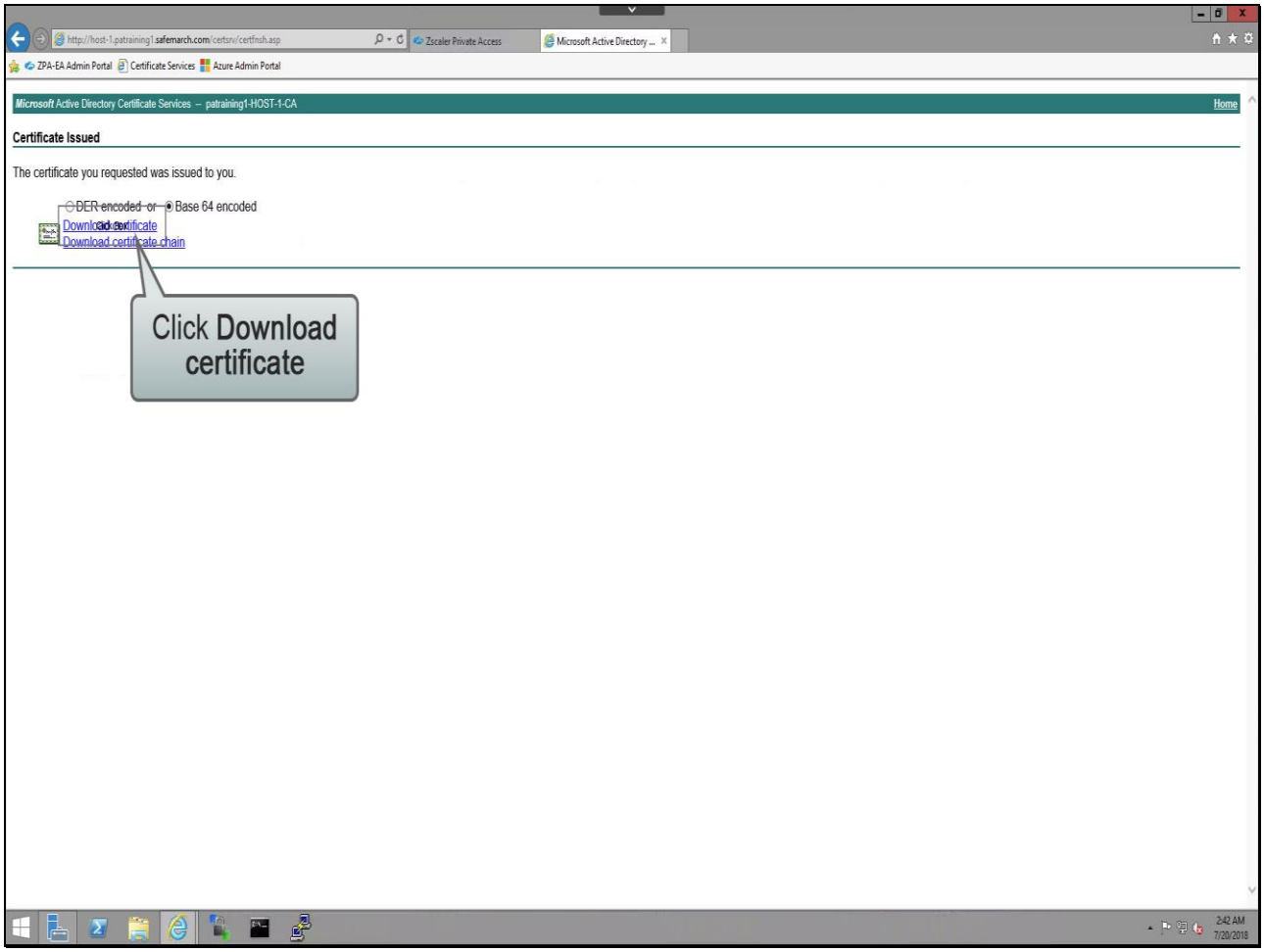
Slide 44 - Slide 44



Slide notes

Click to select the **Base 64 encoded** format option, …

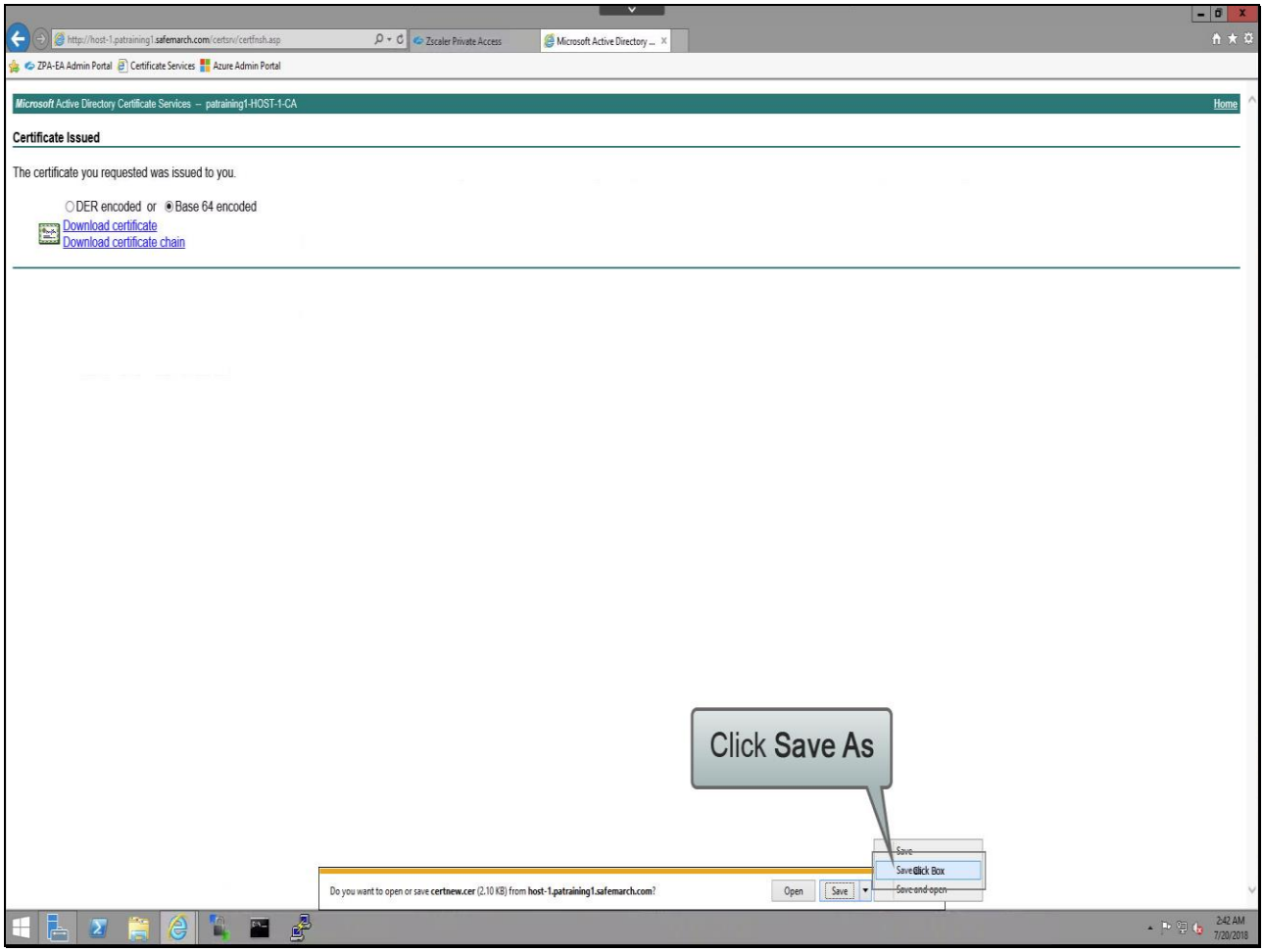
Slide 45 - Slide 45



Slide notes

…click **Download certificate**, …

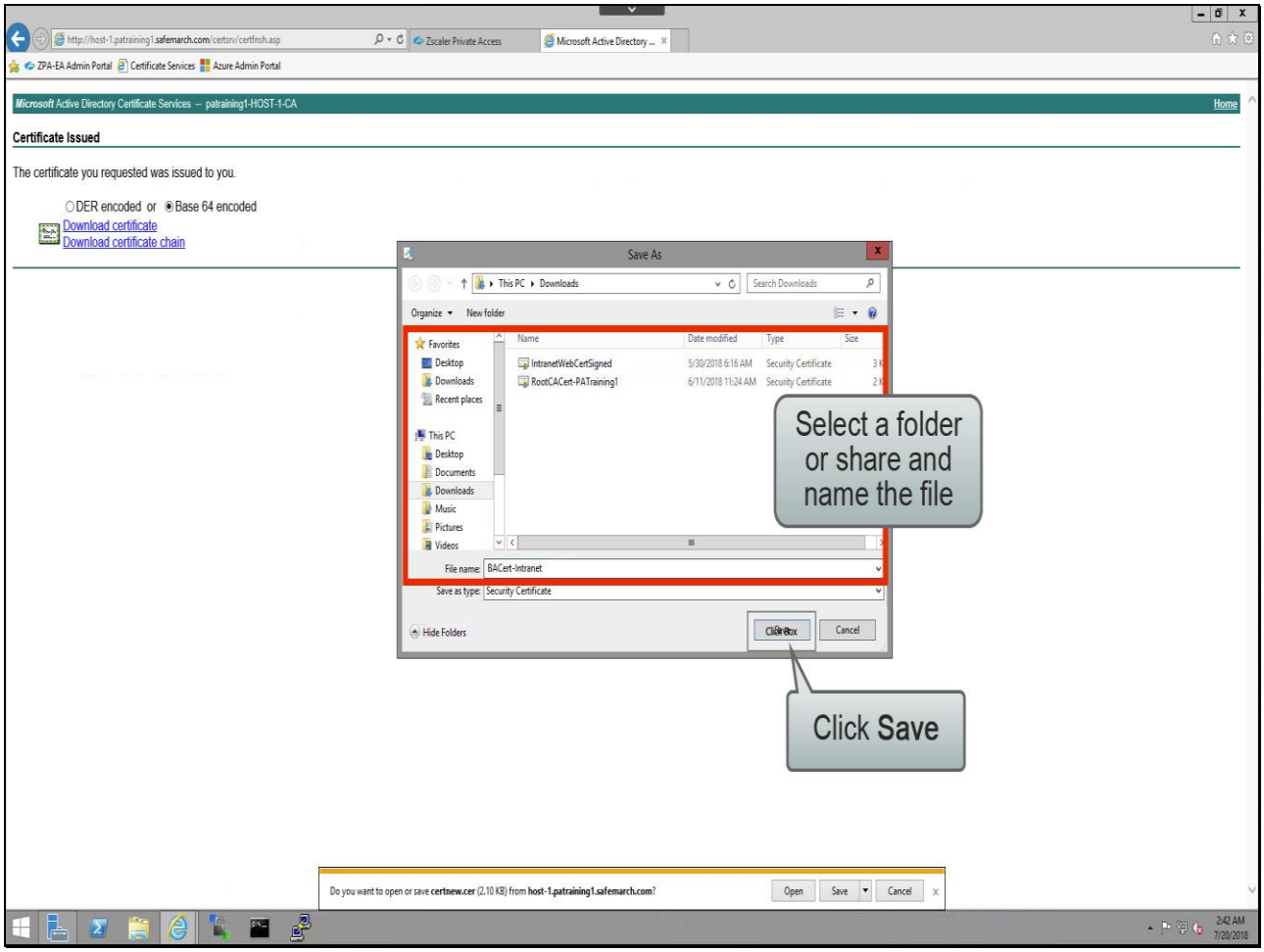
Slide 46 - Slide 46



Slide notes

…click the **Save As** option, …

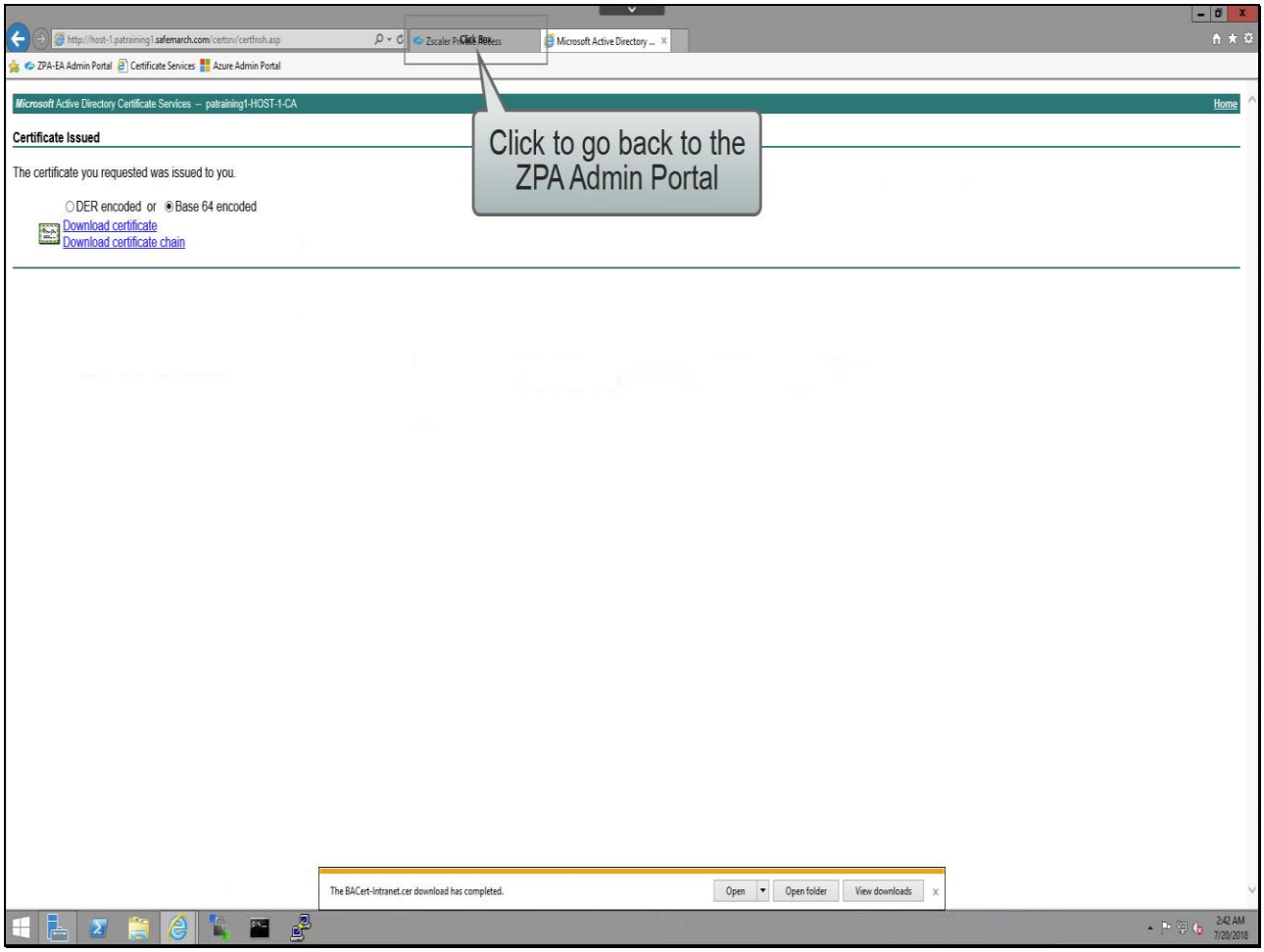
Slide 47 - Slide 47



Slide notes

…navigate to a suitable folder or share, give the certificate an appropriate name and click **Save**.

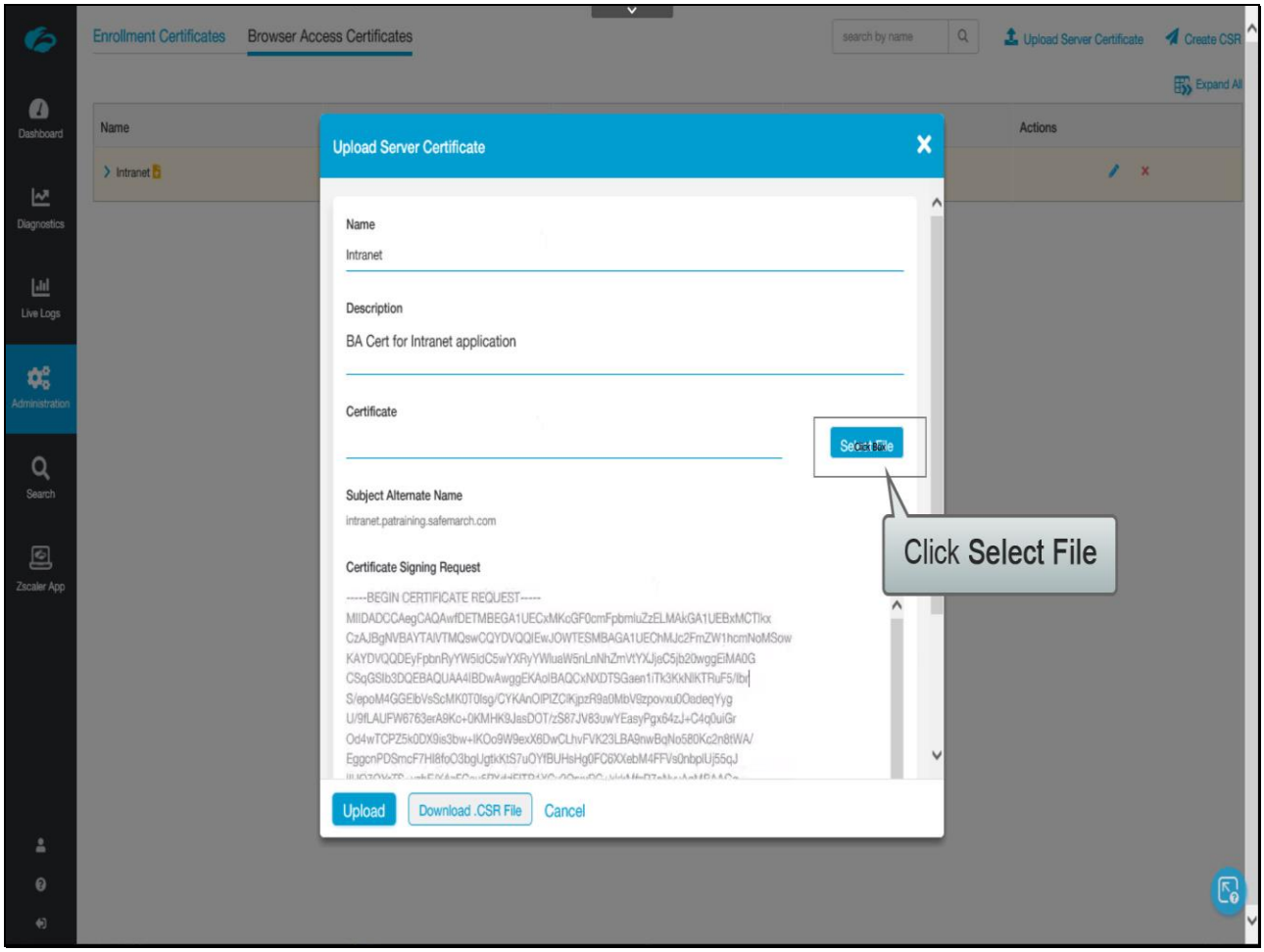
Slide 48 - Slide 48



Slide notes

Click to go back to the browser tab with the ZPA Admin Portal.

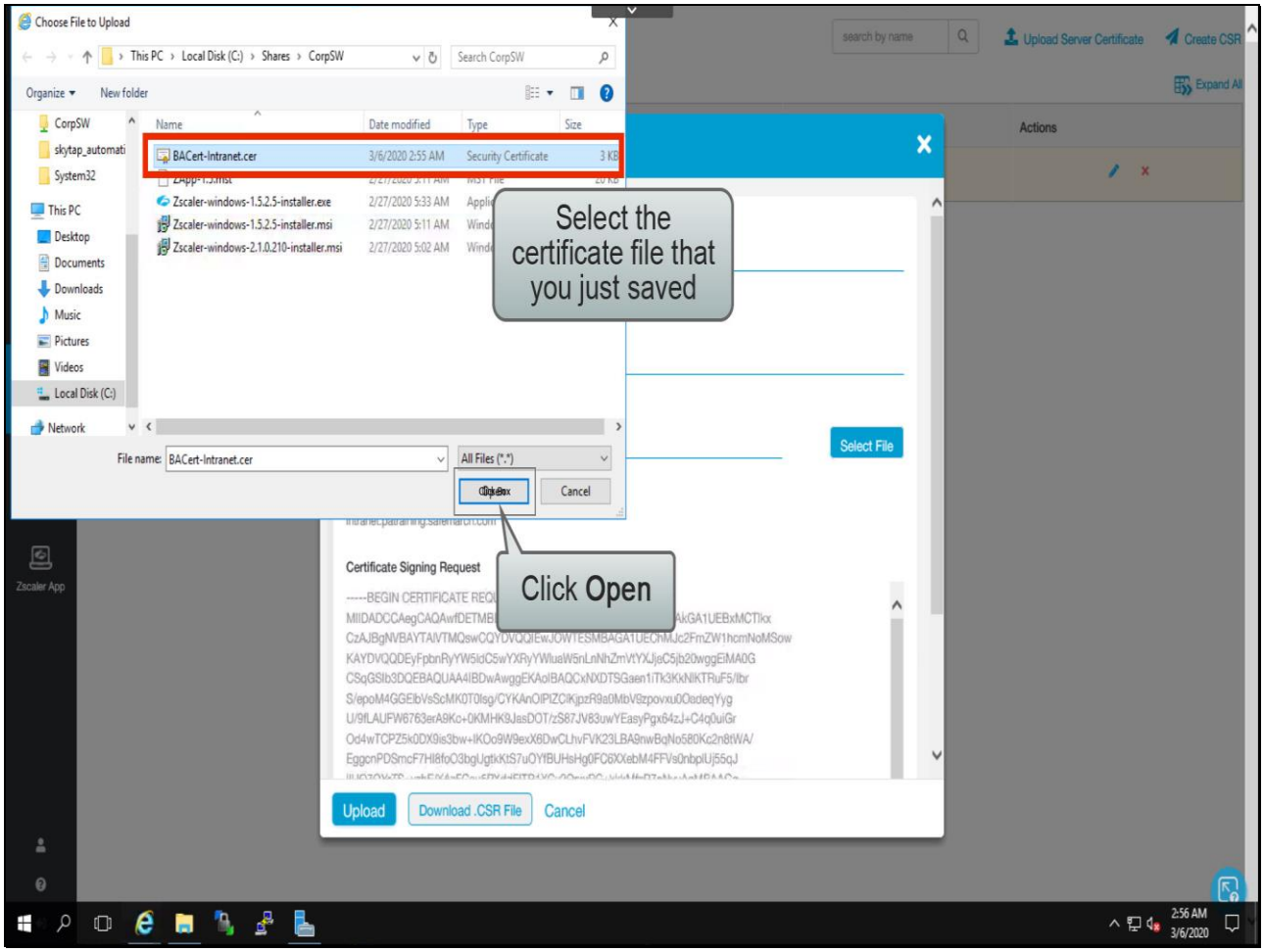
Slide 49 - Slide 49



Slide notes

In the **Upload Server Certificate** window, click **Select File**, …

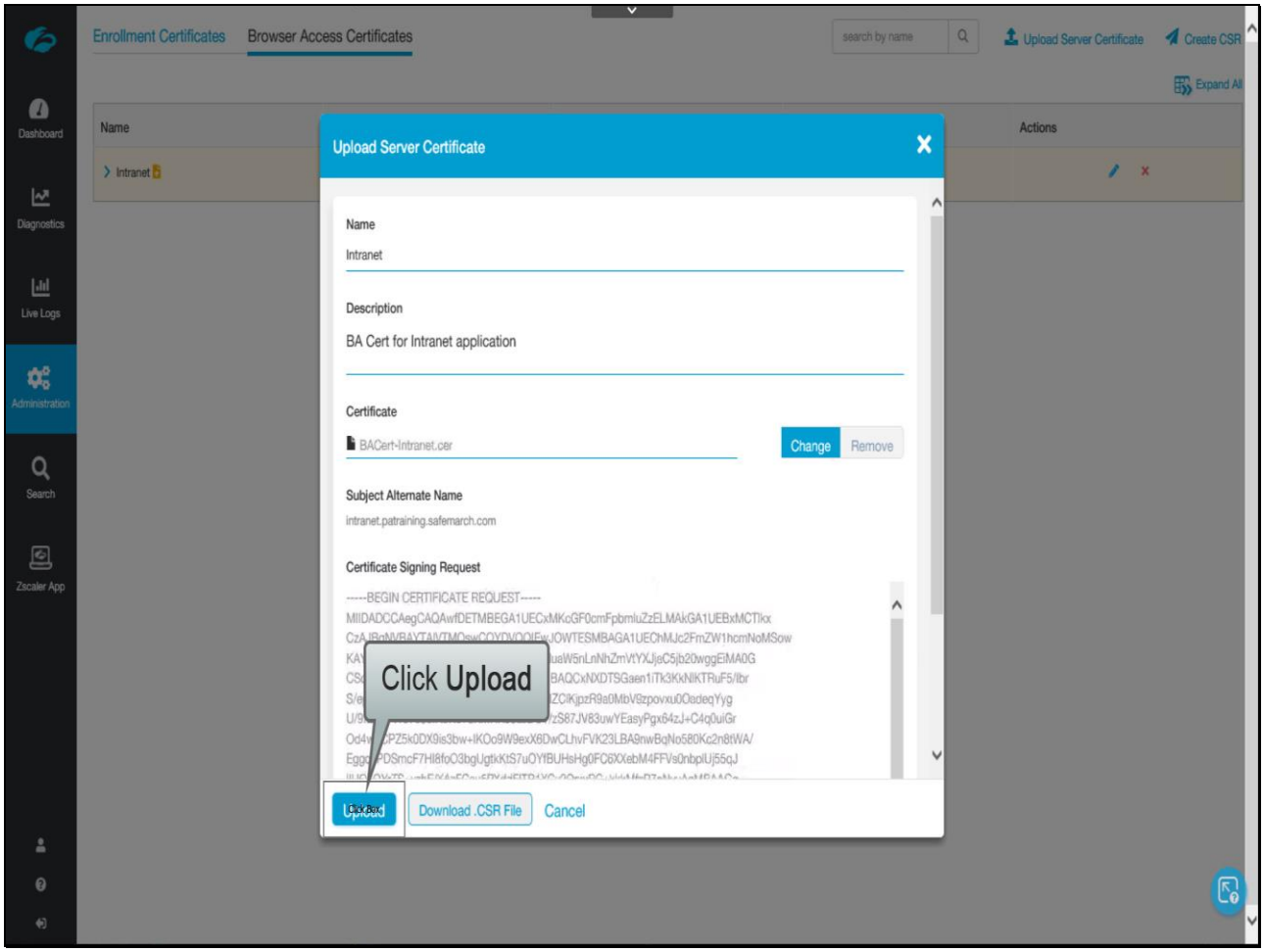
Slide 50 - Slide 50



Slide notes

…find the certificate file that you just saved, select it and click **Open**, …

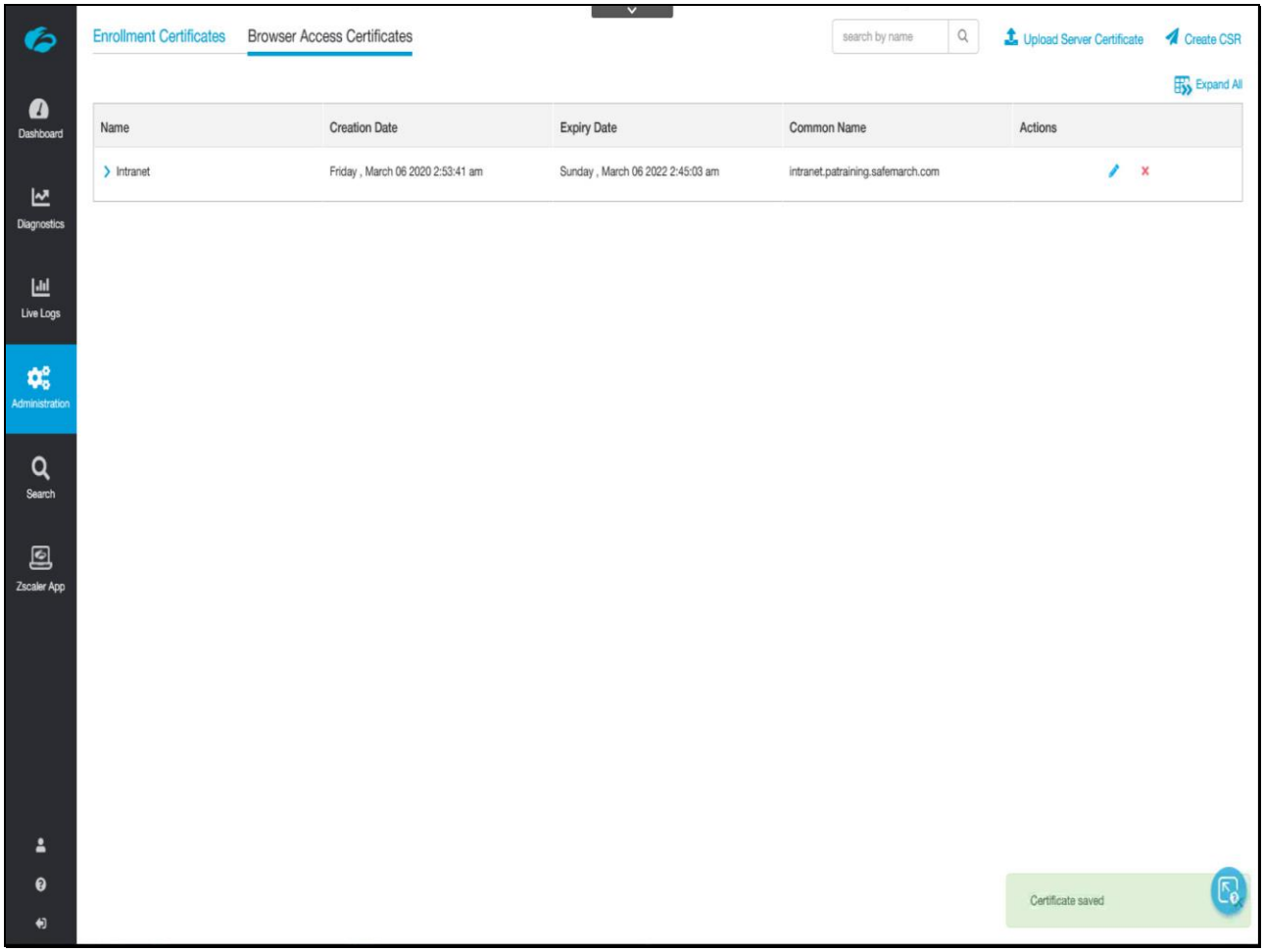
Slide 51 - Slide 51



Slide notes

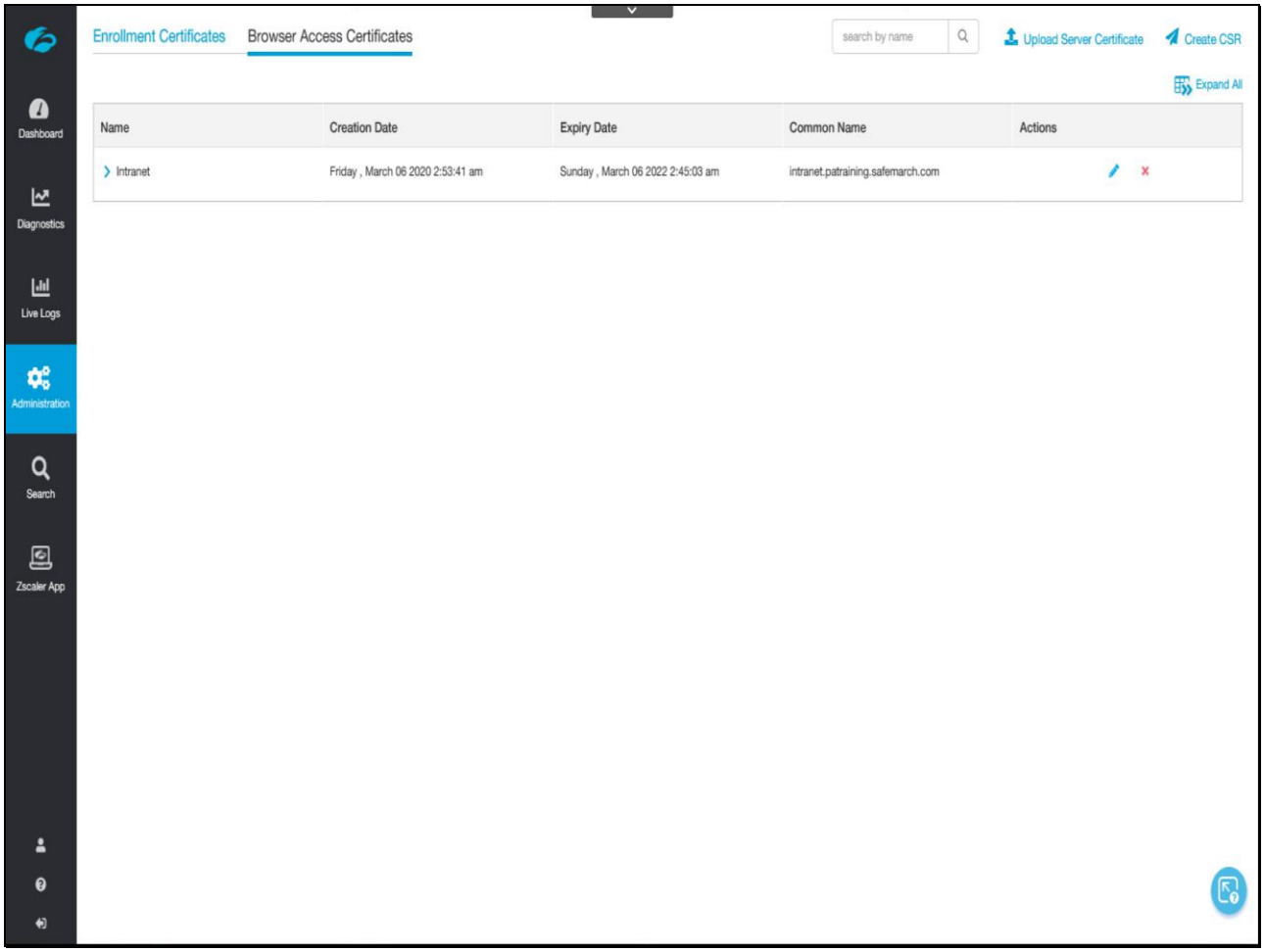
…then click **Upload**.

Slide 52 - Slide 52



Slide notes

Slide 53 - Slide 53



Slide notes

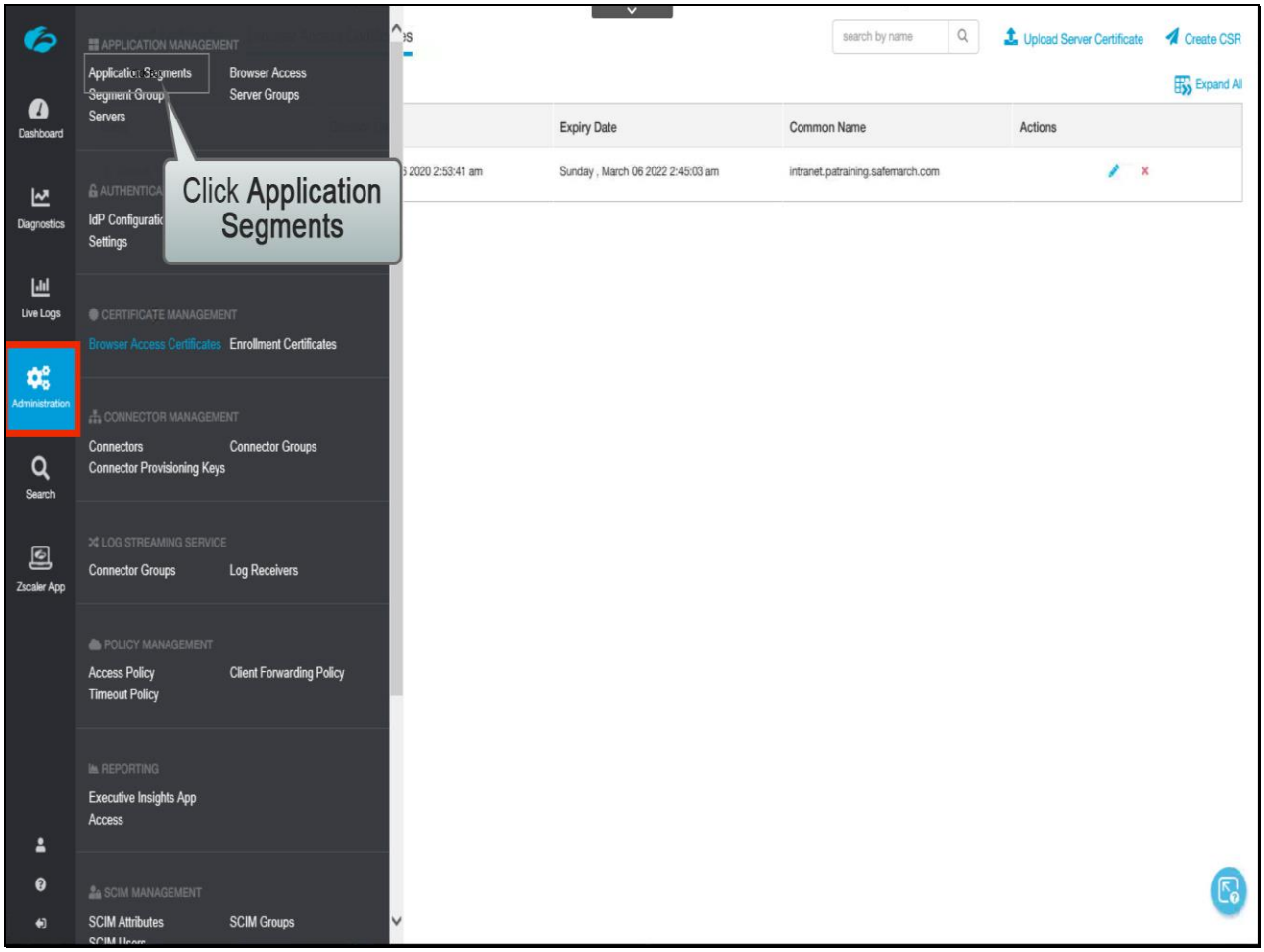
Slide 54 - Create the CNAME Record

Slide notes

In the next section, we will step through the process for adding a DNS CNAME record for the application.

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

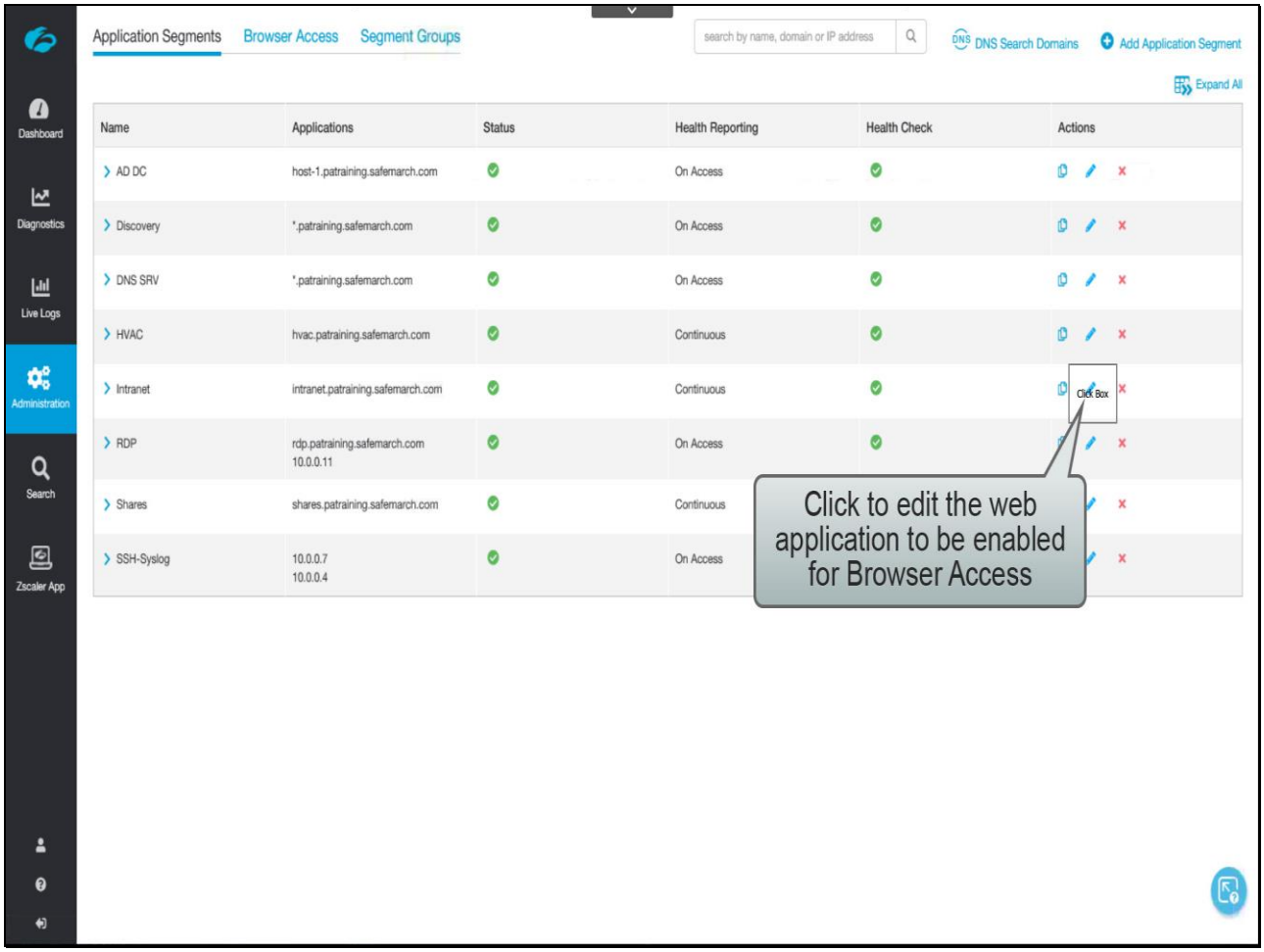
Slide 55 - Slide 55



Slide notes

In the ZPA Admin Portal, from the **Administration** menu under **APPLICATION MANAGEMENT**, click **Application Segments**.

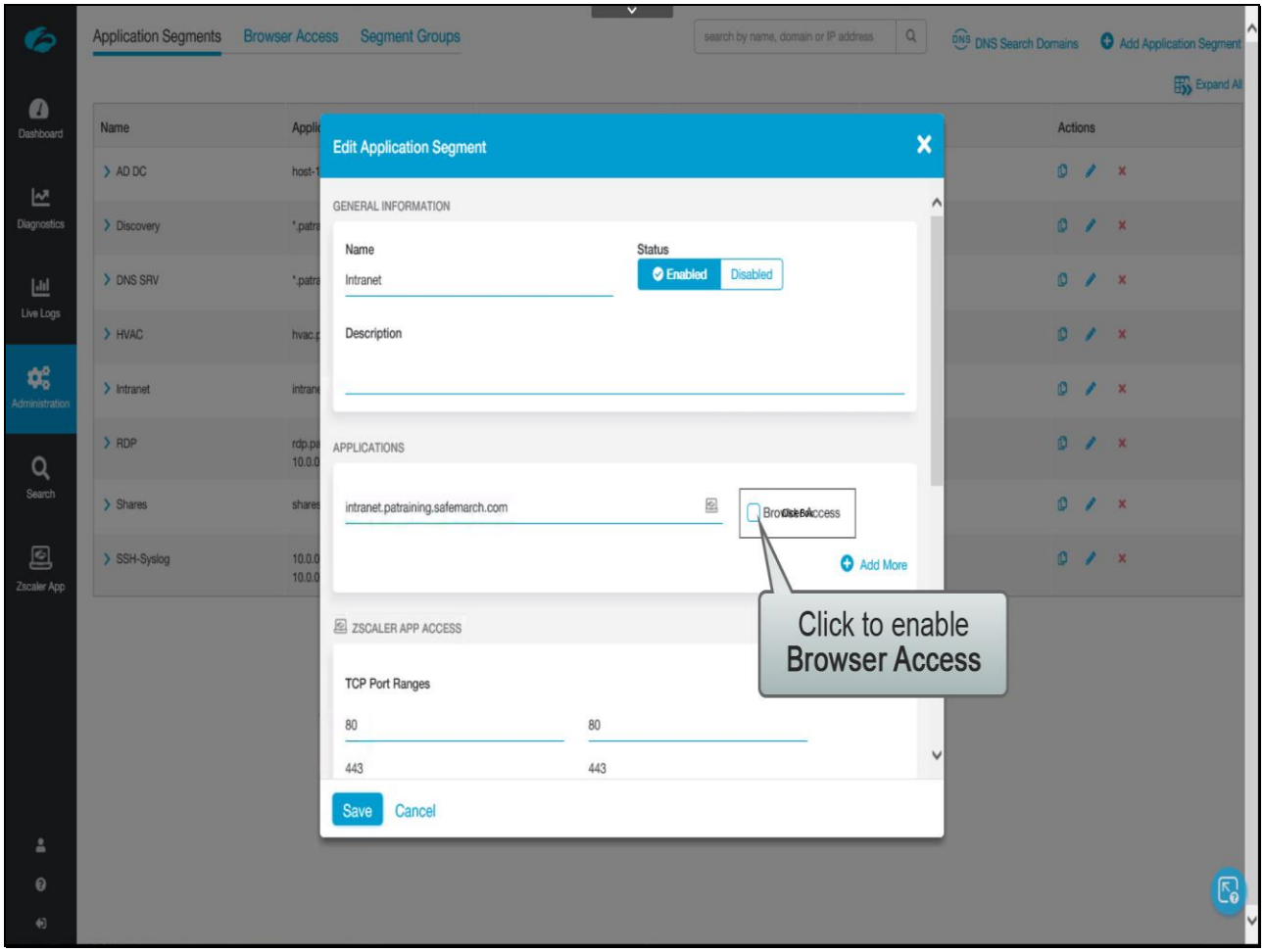
Slide 56 - Slide 56



Slide notes

Click to edit the web application that you also want to make available in a web browser.

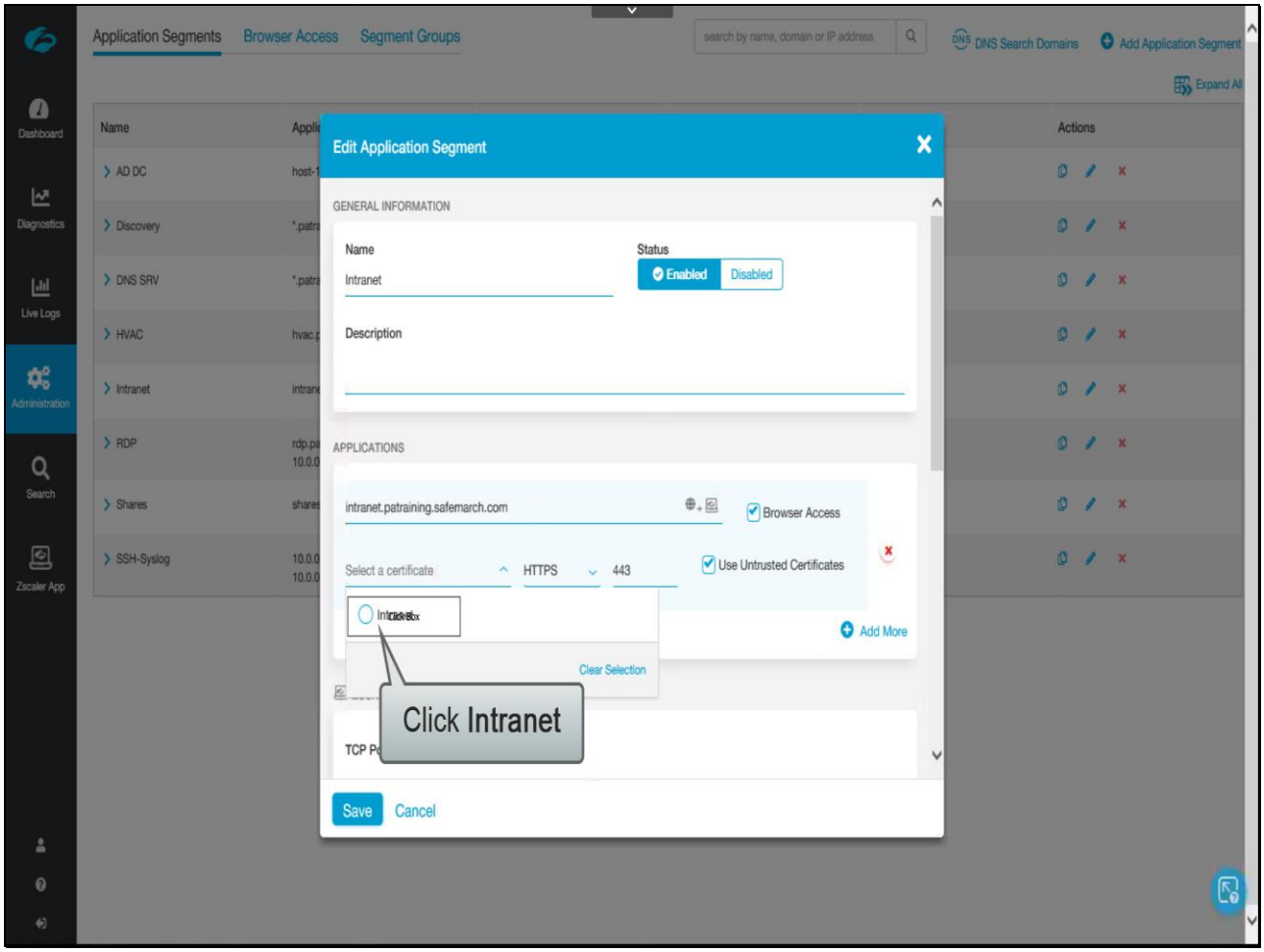
Slide 57 - Slide 57



Slide notes

In the **APPLICATIONS** section, click to enable the **Browser Access** option.

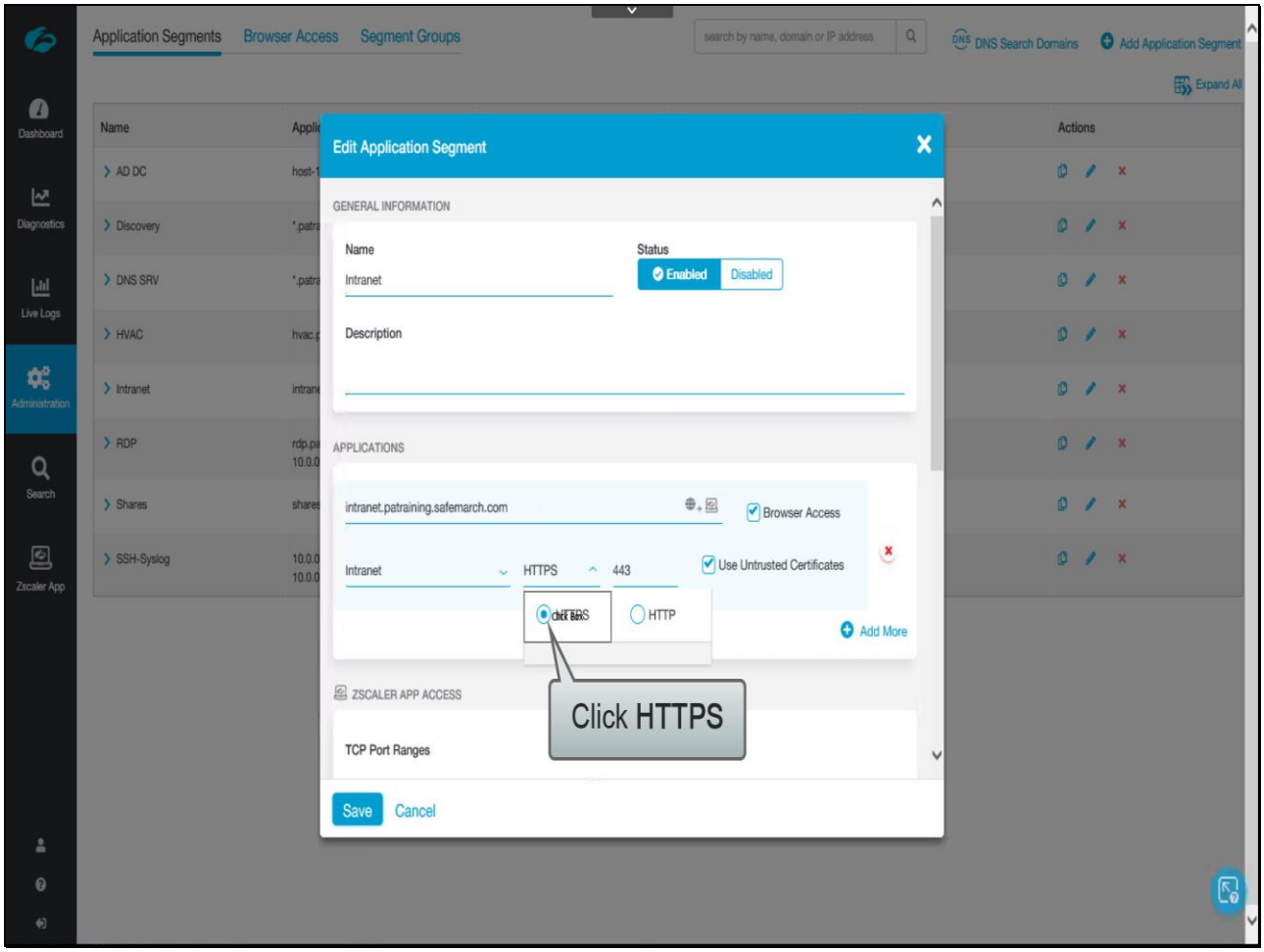
Slide 58 - Slide 58



Slide notes

In the **Select certificate** field, click to select the **Intranet** Browser Access certificate that you created earlier.

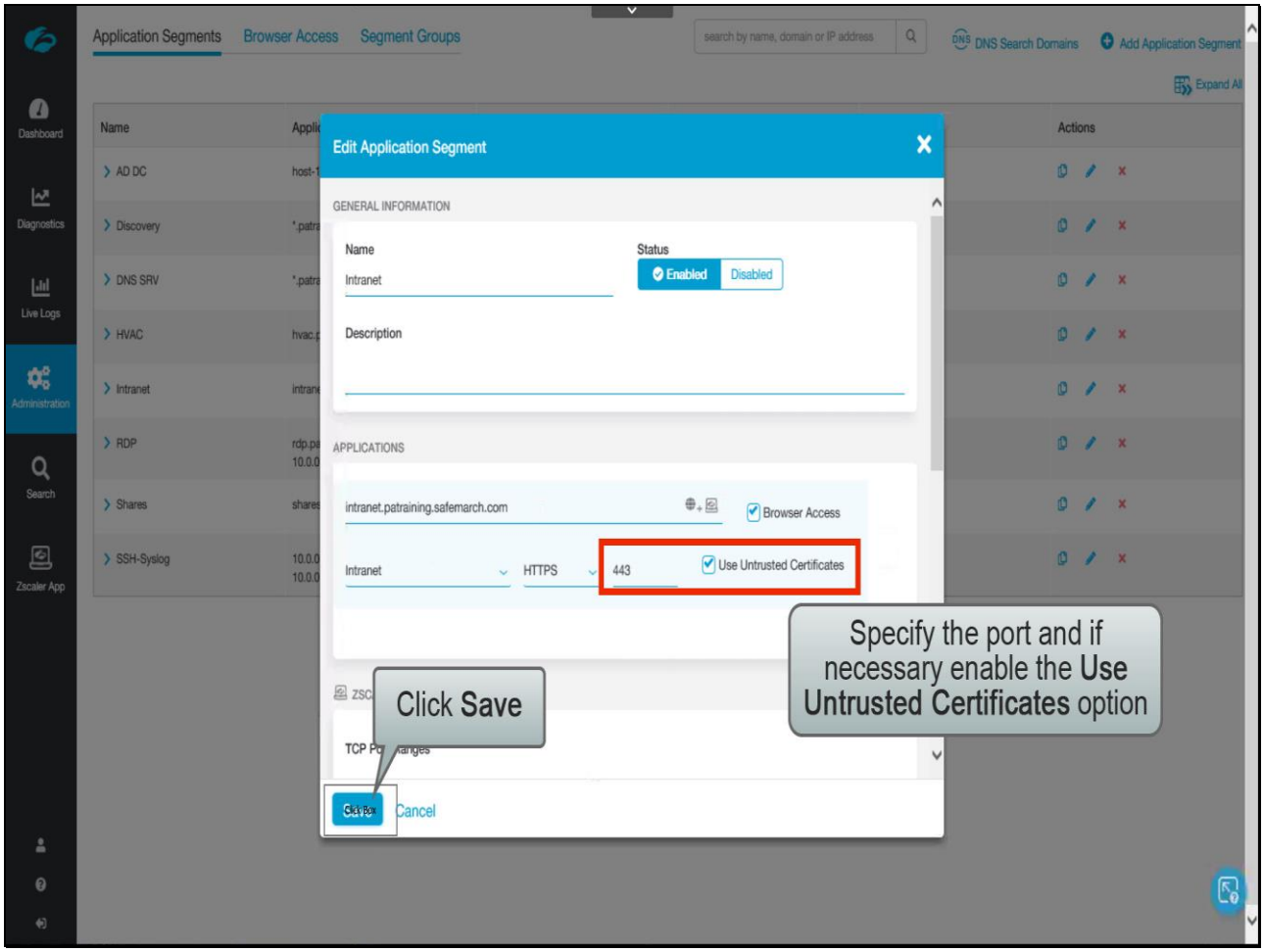
Slide 59 - Slide 59



Slide notes

Click to select **HTTPS** as the protocol that ZPA is to use on the 'back end' to request the application (this is the protocol that will be used by the BA Exporter when connecting to the application).

Slide 60 - Slide 60

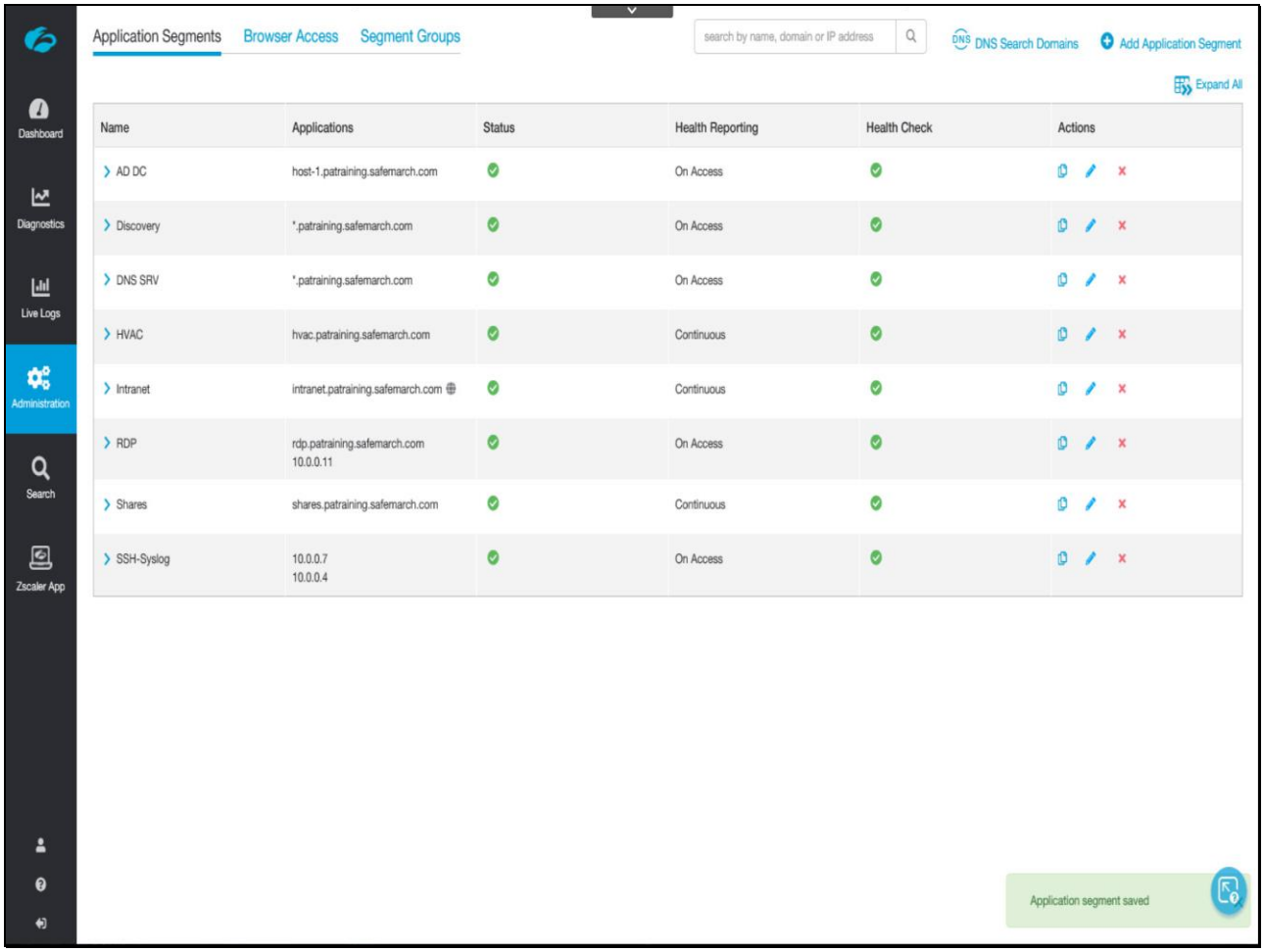


Slide notes

You may also set the port to use for the connection to the application, if it is different from the default. In addition, there is the option to **Use Untrusted Certificates** if the application server certificate cannot be validated by the BA Exporter (for example because it was issued by an enterprise private CA - this option is enabled by default).

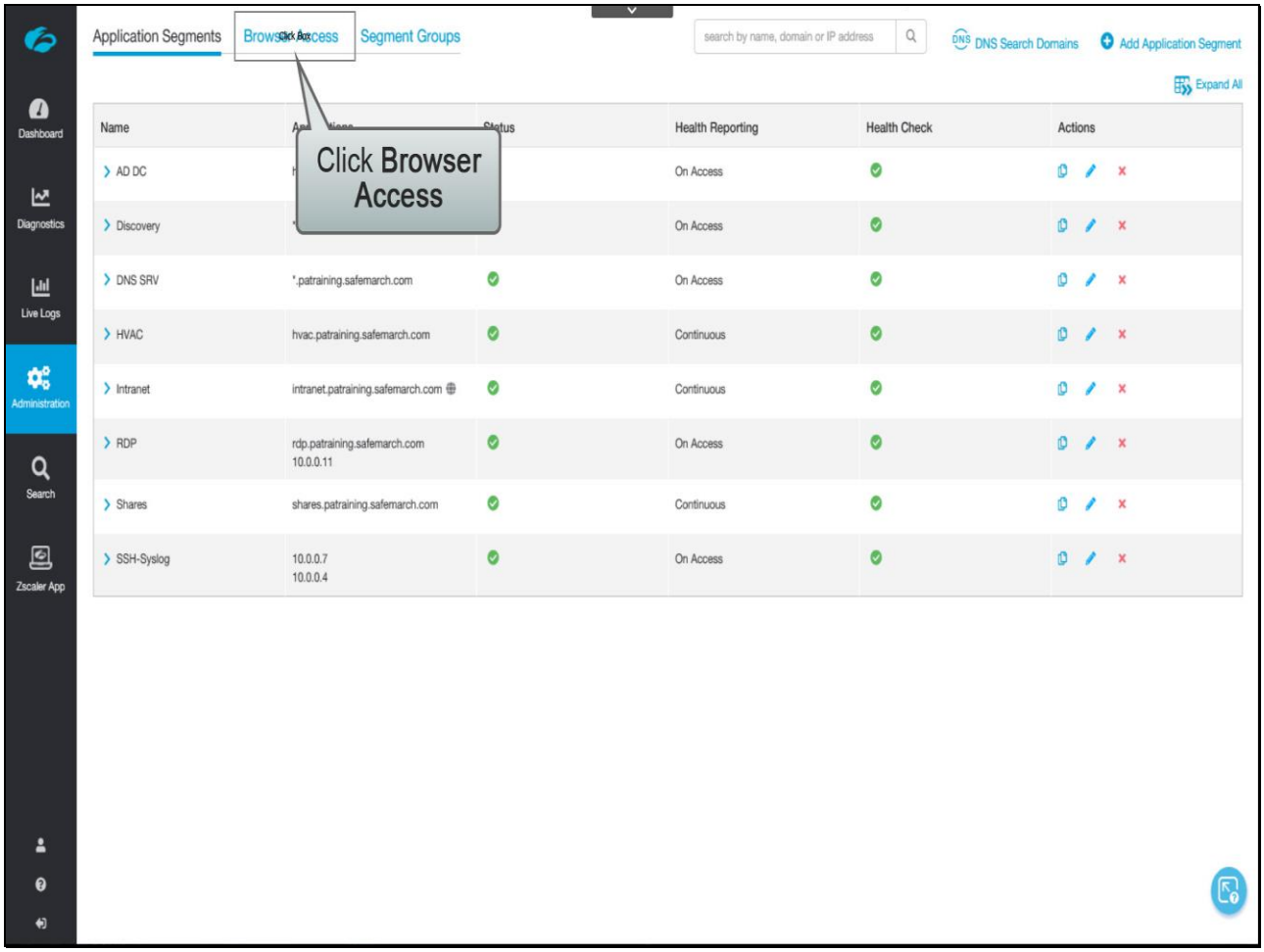
Click **Save** once the BA configuration is complete.

Slide 61 - Slide 61



Slide notes

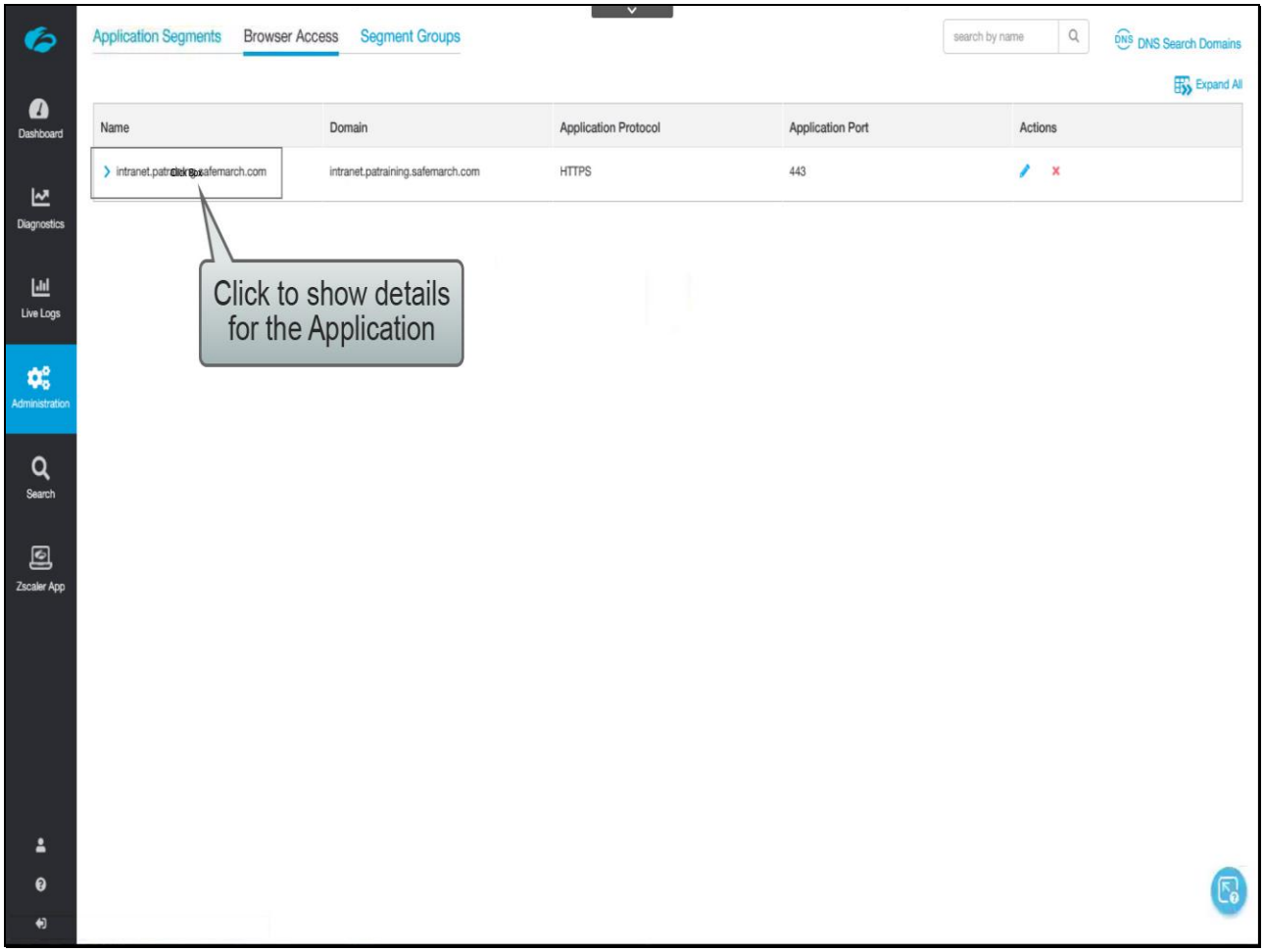
Slide 62 - Slide 62



Slide notes

To review your Browser Access applications, click **Browser Access**, ...

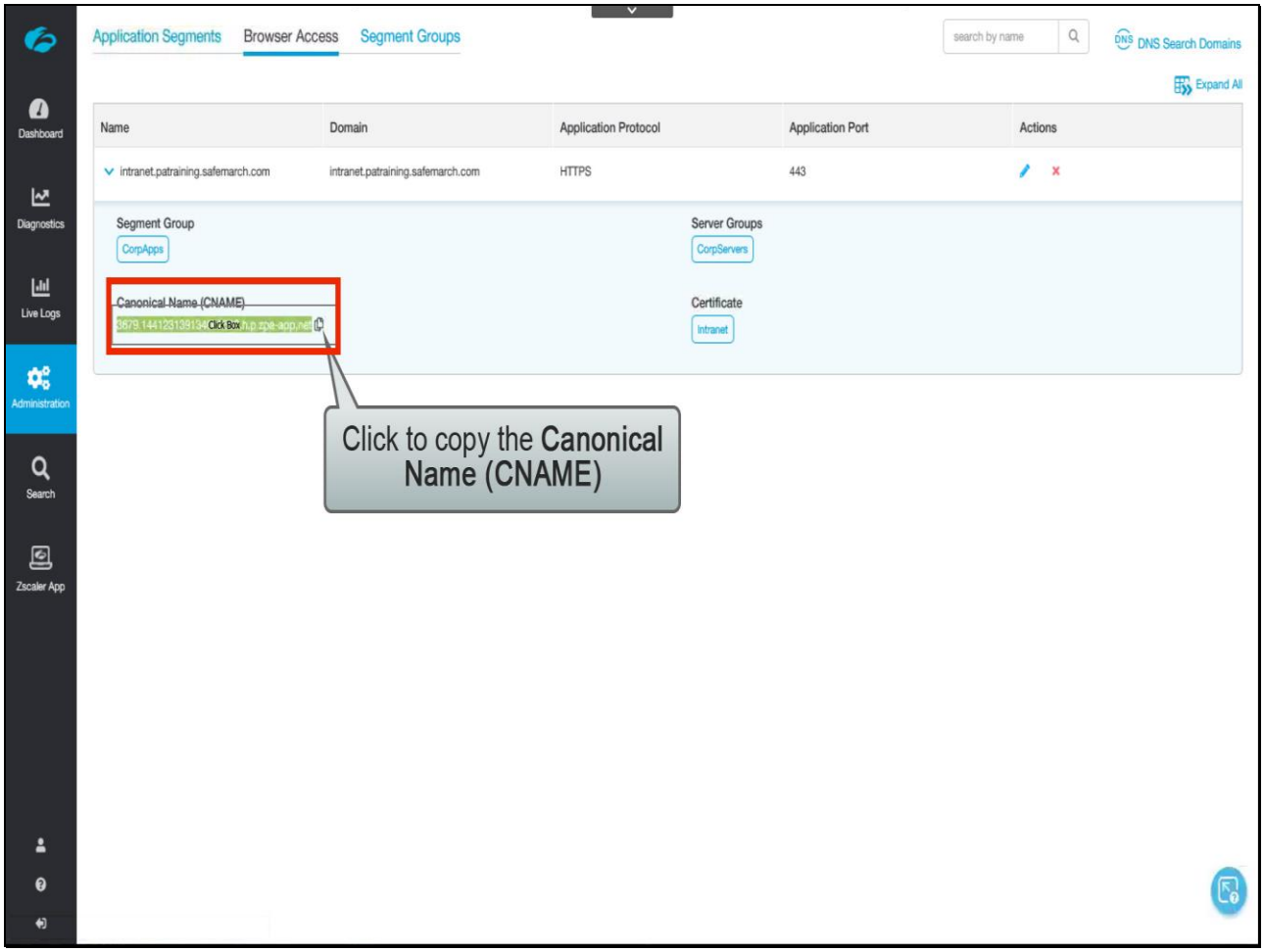
Slide 63 - Slide 63



Slide notes

…then to view details for an application, click on the name.

Slide 64 - Slide 64

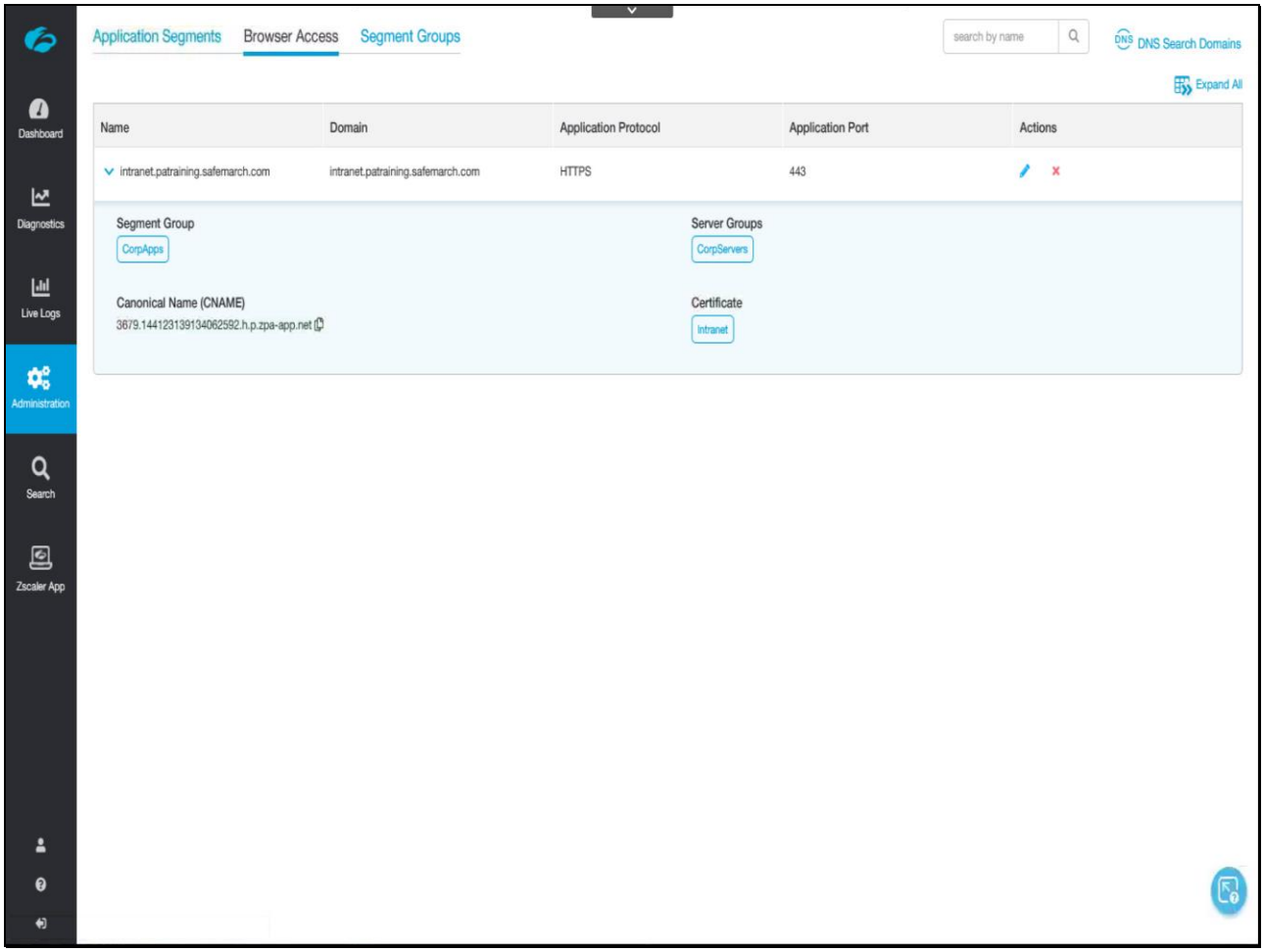


Slide notes

The **Canonical Name (CNAME)** for a BA application will be shown, this CNAME must be defined on the DNS environment used by the users of this BA application (normally this means on the public, internet DNS).

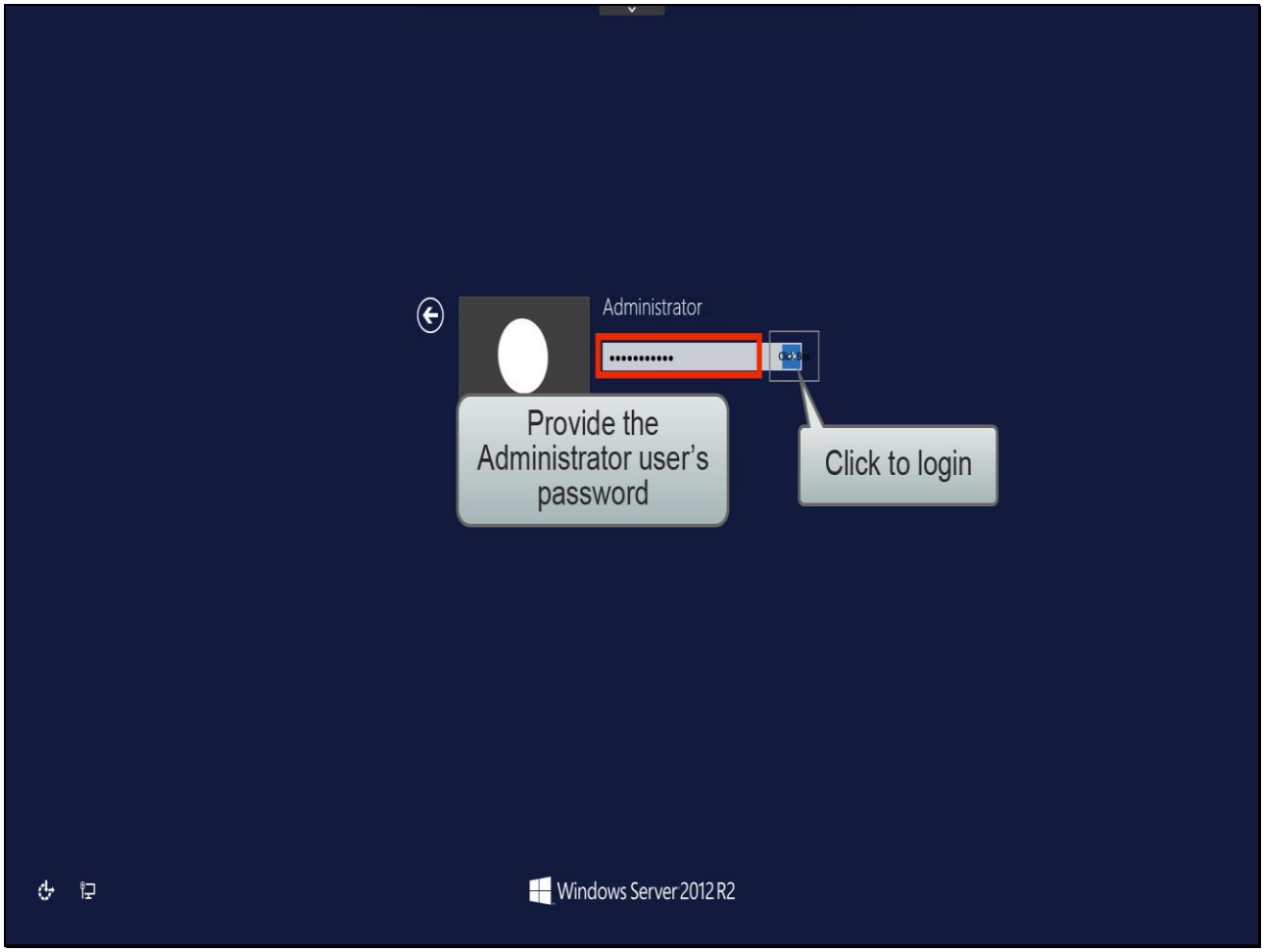
To copy the value for the alias, click **Copy**.

Slide 65 - Slide 65



Slide notes

Slide 66 - Slide 66

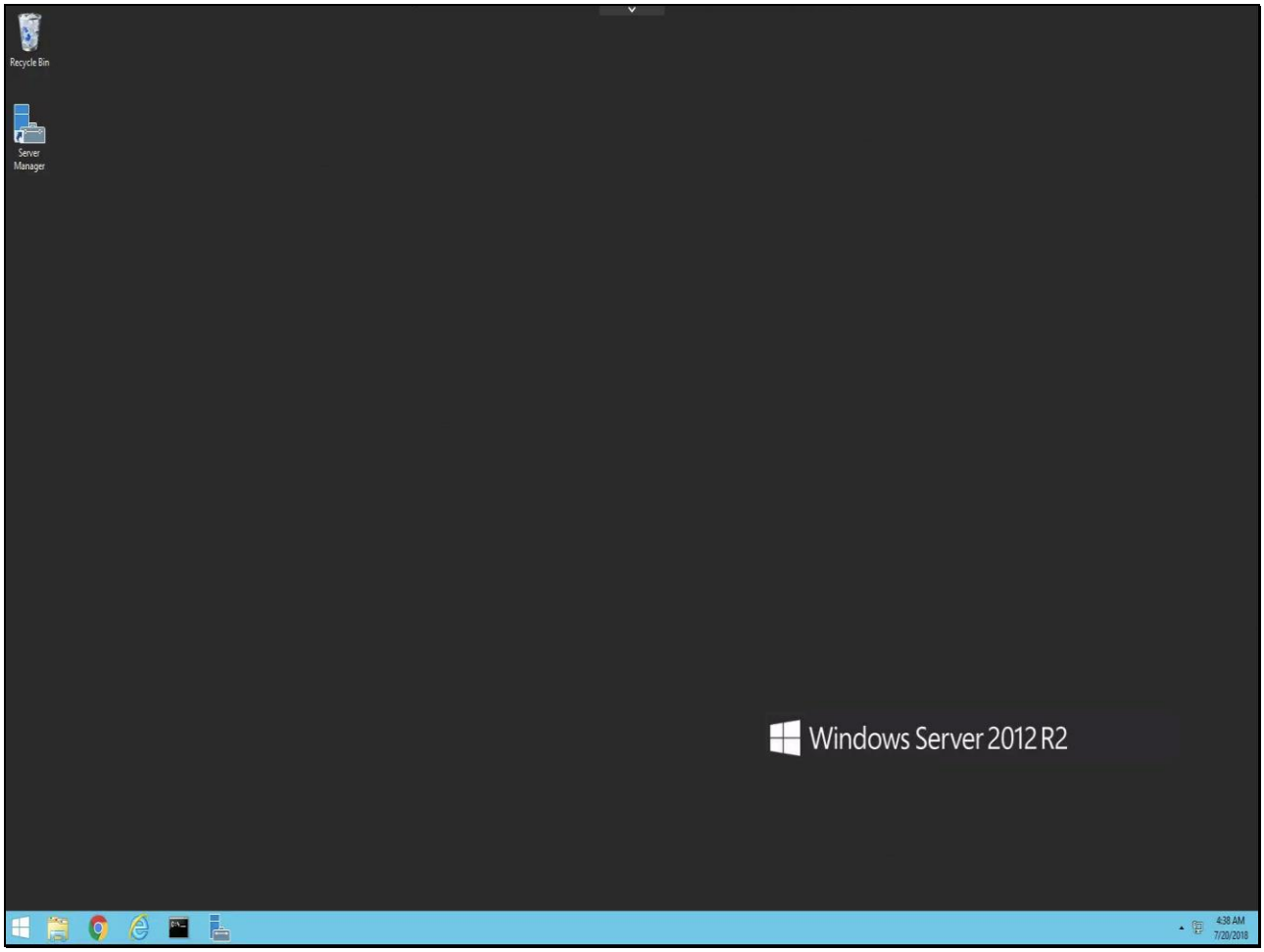


Slide notes

The CNAME record needs to be defined on the appropriate DNS server, in this case we will use a local server.

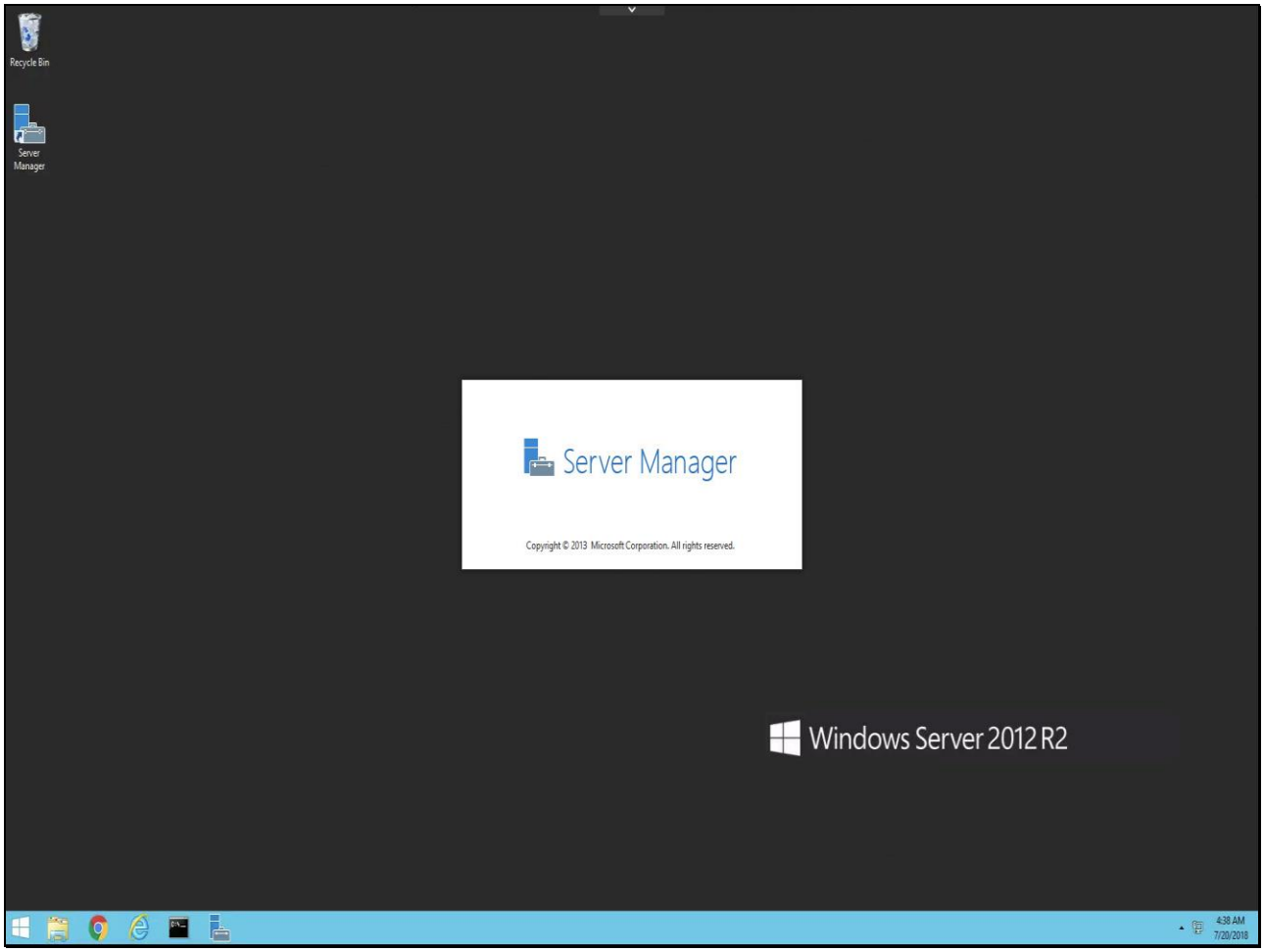
Provide the admin password and click to login.

Slide 67 - Slide 67



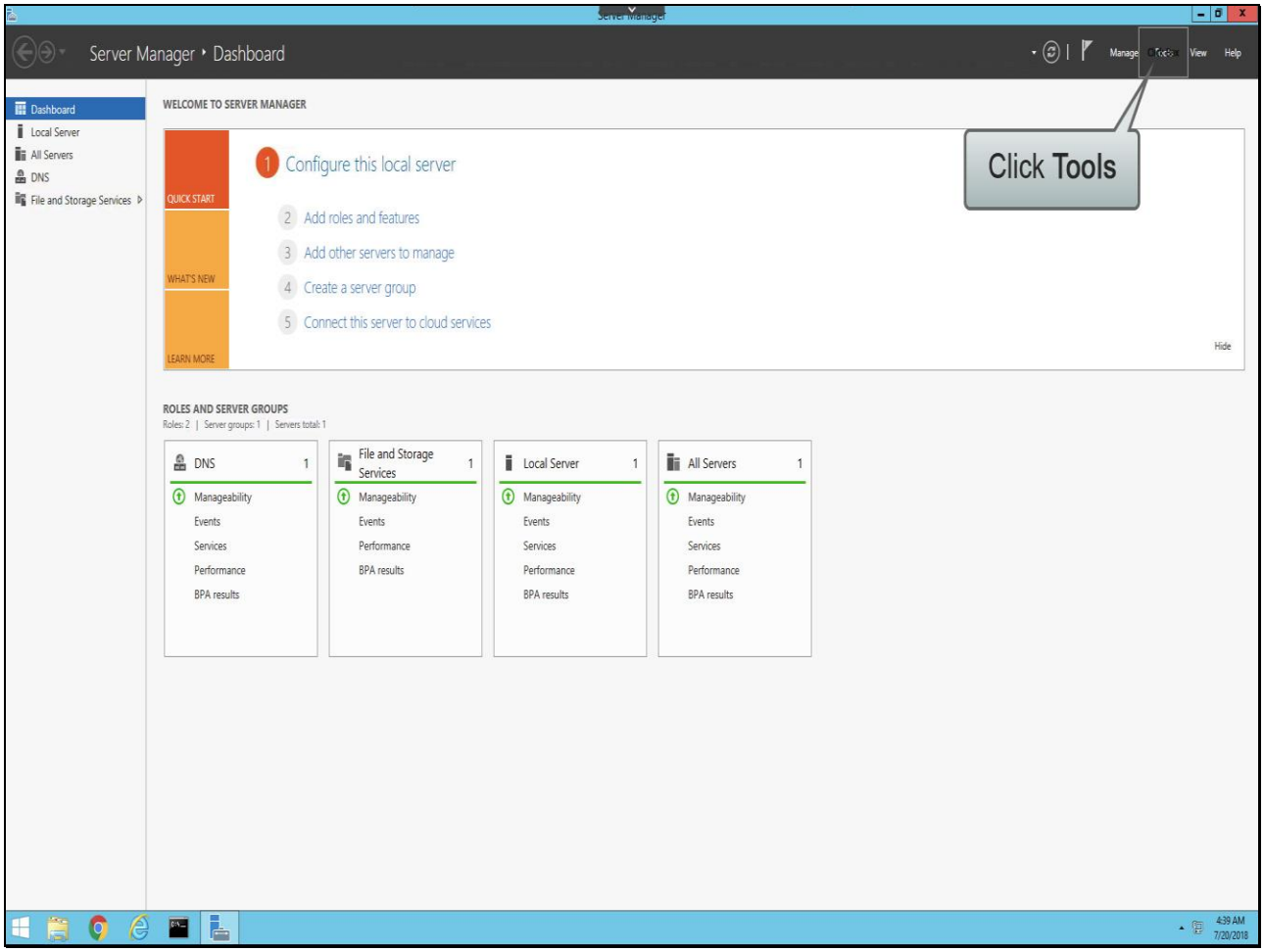
Slide notes

Slide 68 - Slide 68



Slide notes

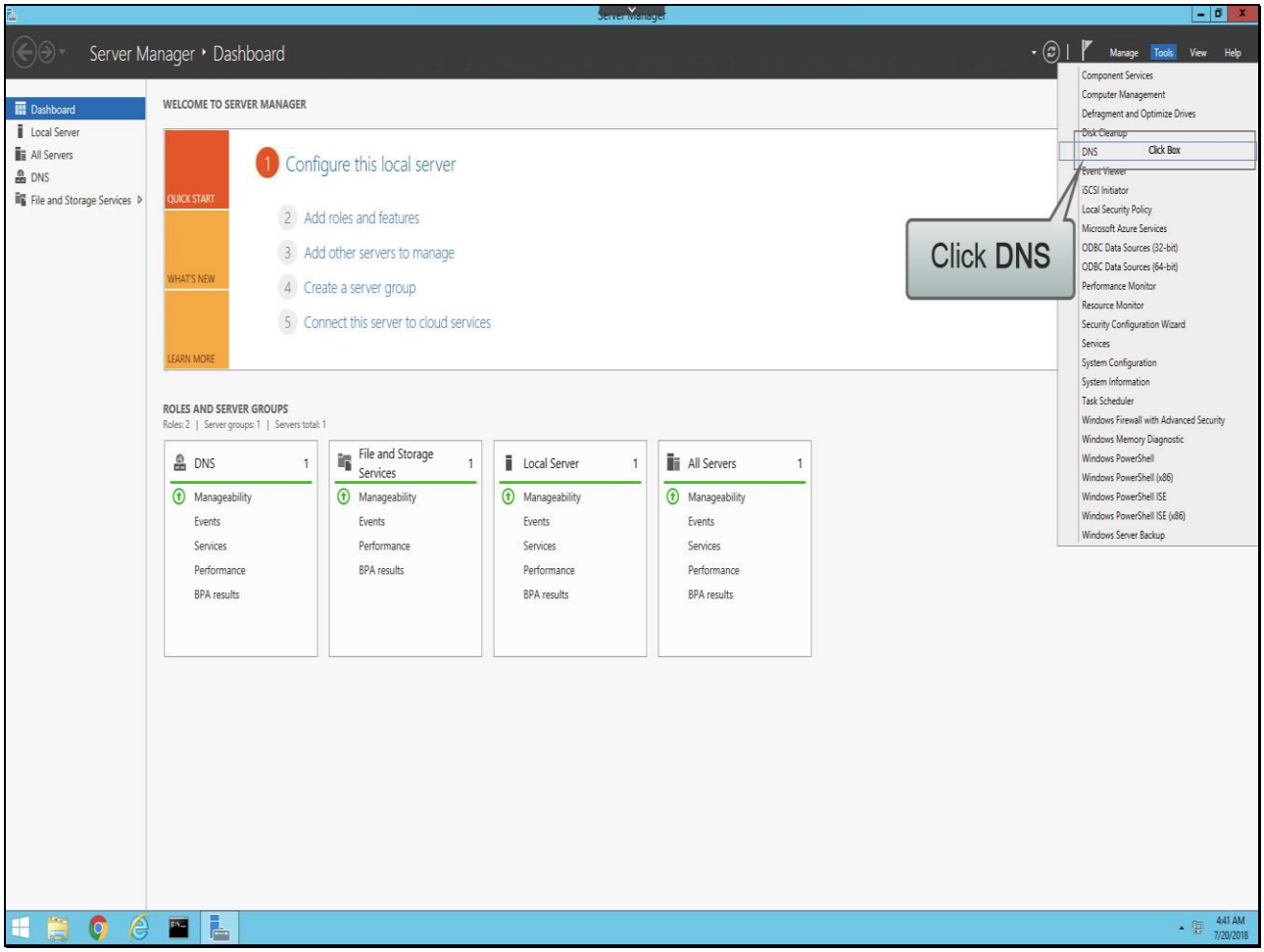
Slide 69 - Slide 69



Slide notes

In the Server Manager, click on the **Tools** menu, …

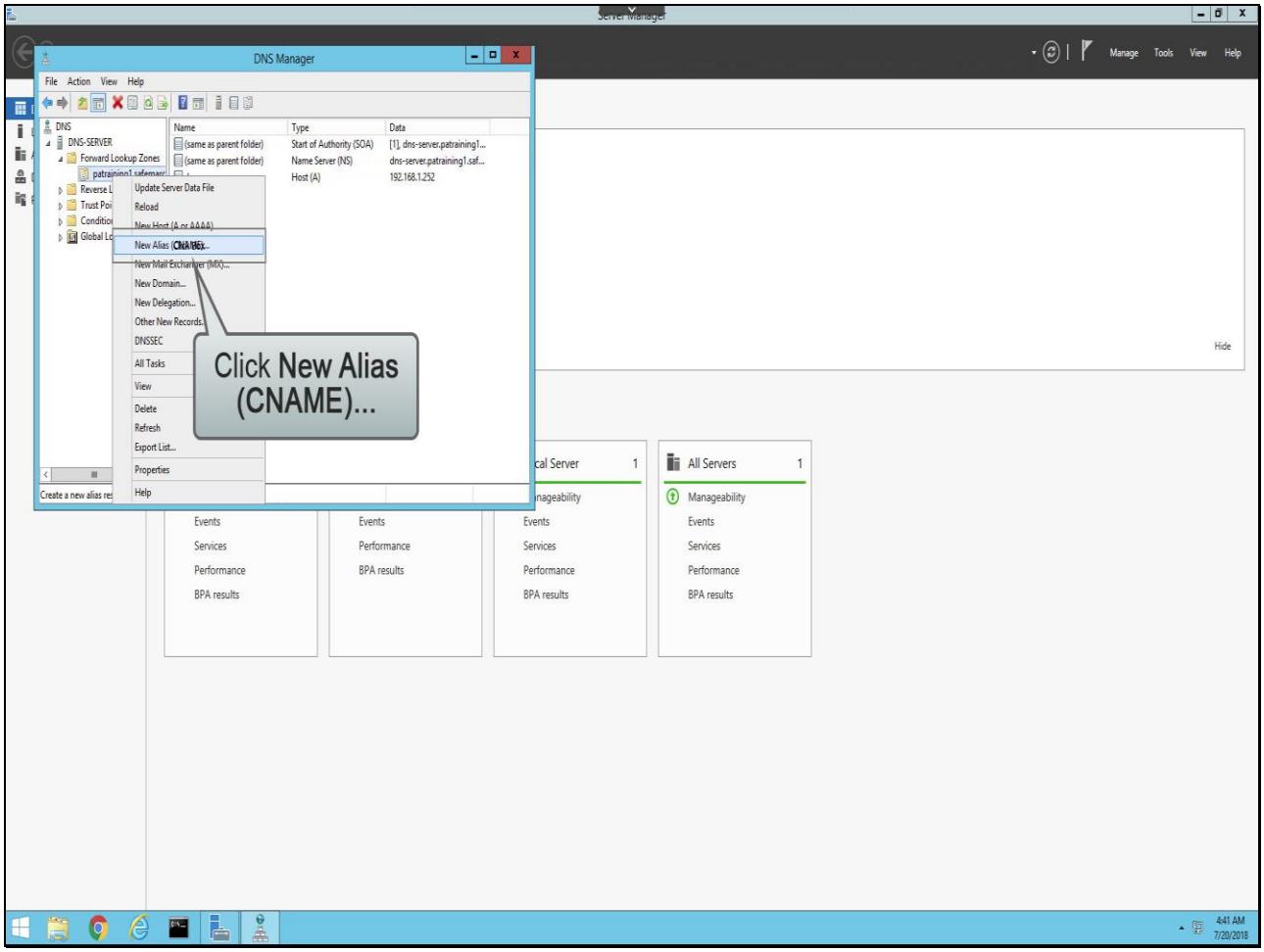
Slide 70 - Slide 70



Slide notes

…then click **DNS**.

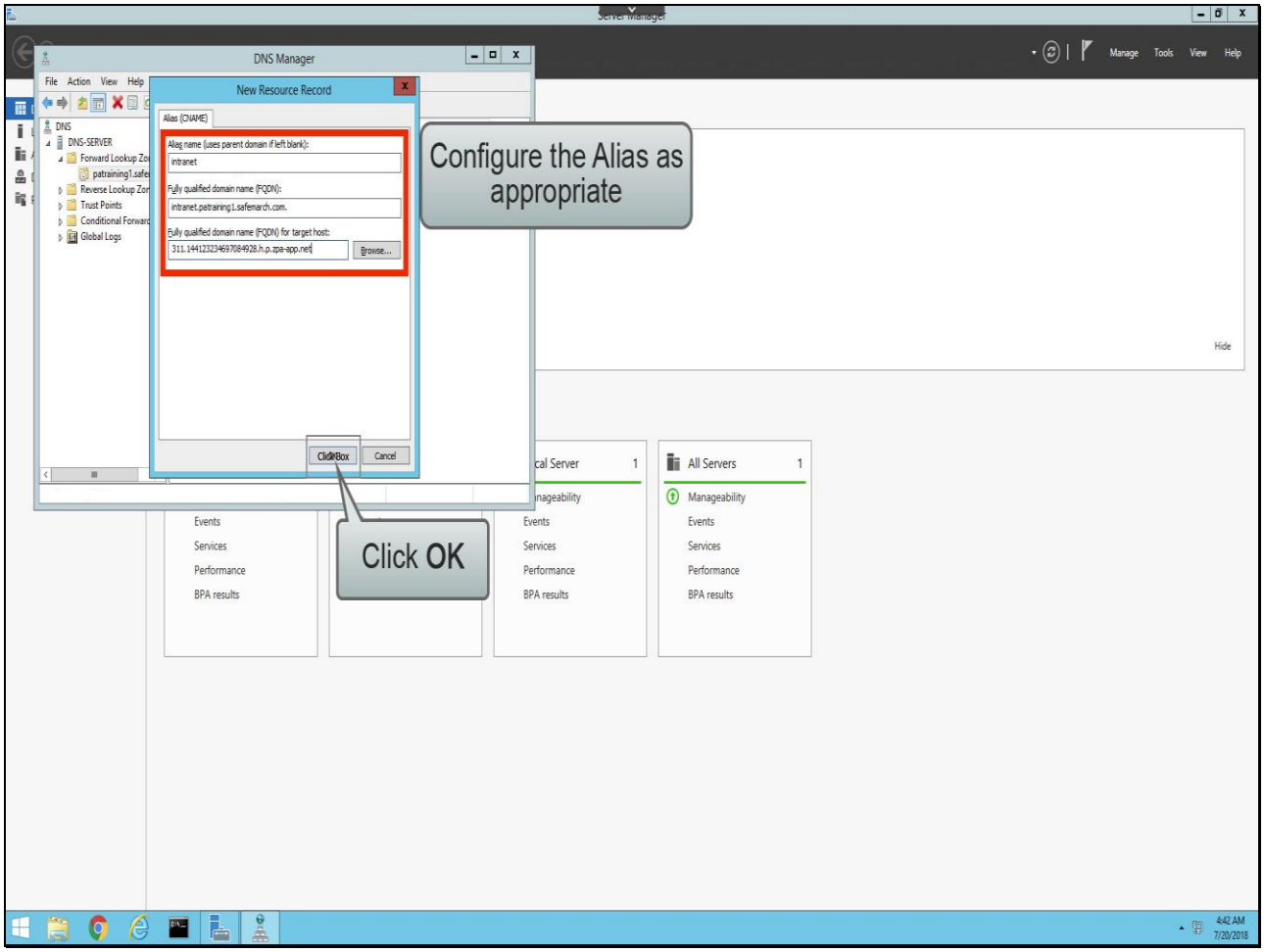
Slide 71 - Slide 71



Slide notes

Expand the appropriate **Forward Lookup Zone**, right-click, then click on the **New Alias (CNAME)** option.

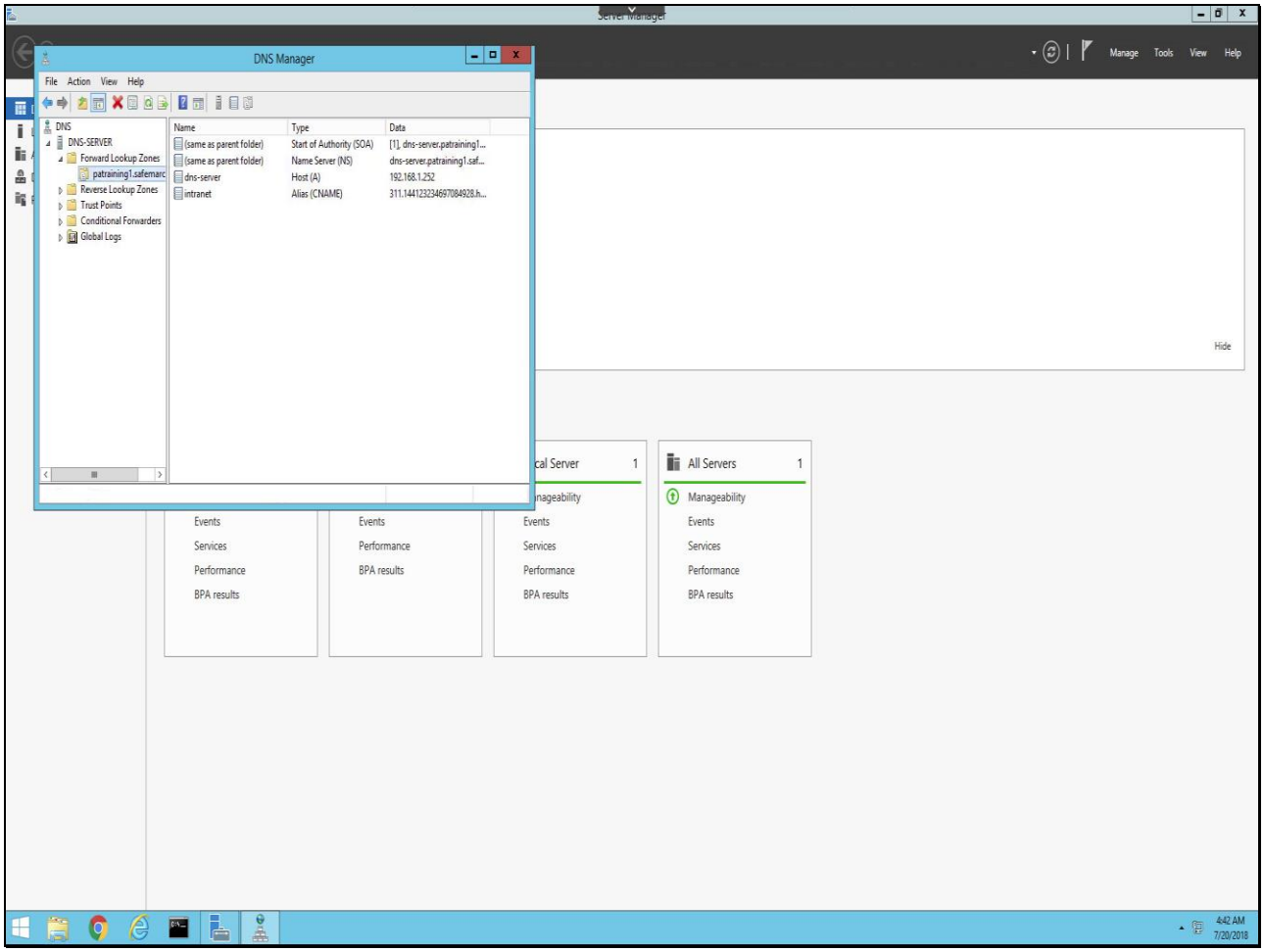
Slide 72 - Slide 72



Slide notes

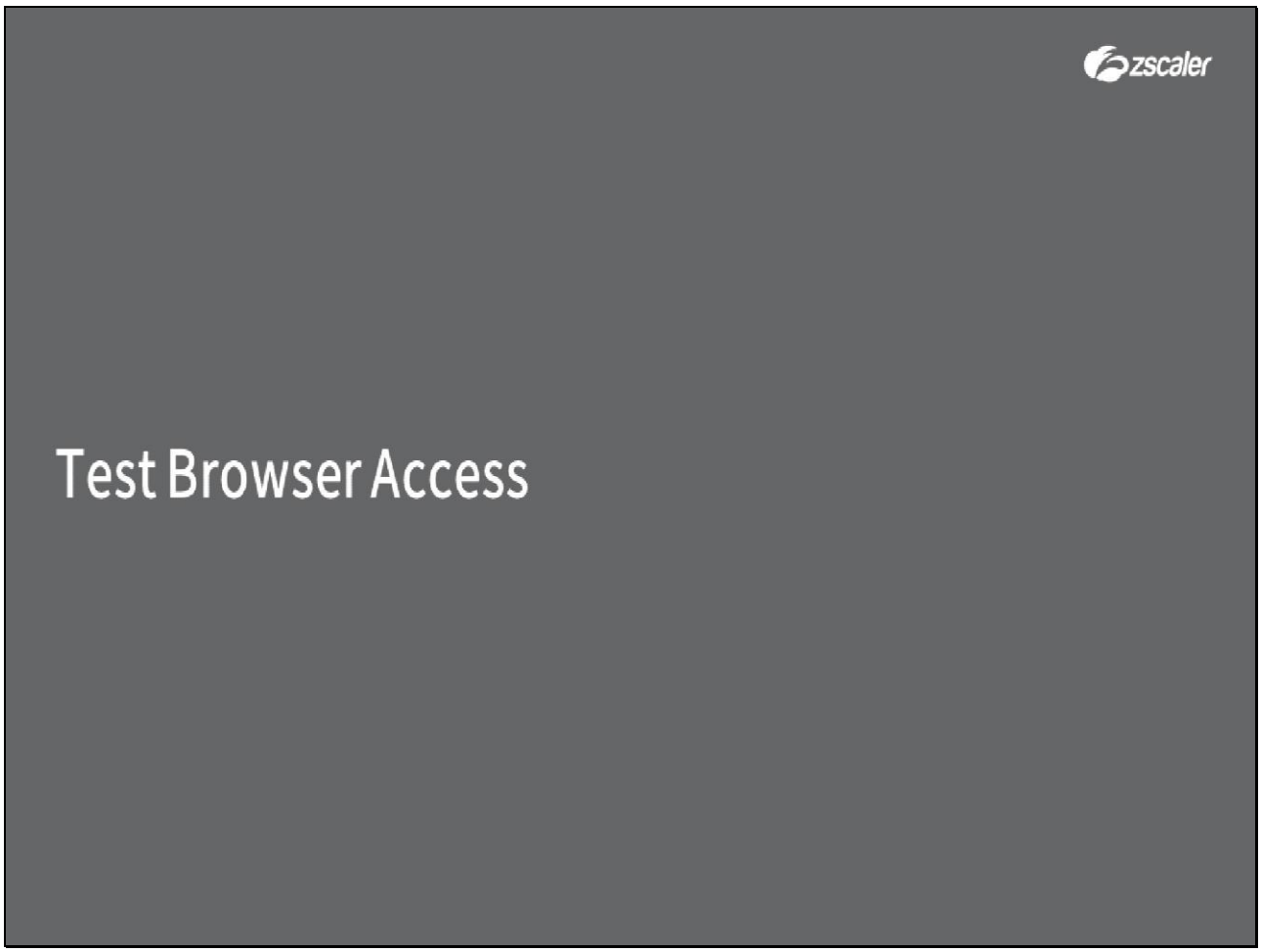
Specify the **Alias name** (the name of the application), verify that the **FQDN** generated for it is correct, paste in the value for the alias to the **Fully qualified domain name (FQDN) for target host** field (this is the CNAME value that you copied from the ZPA Admin Portal), then click **OK**.

Slide 73 - Slide 73



Slide notes

Slide 74 - Test Browser Access

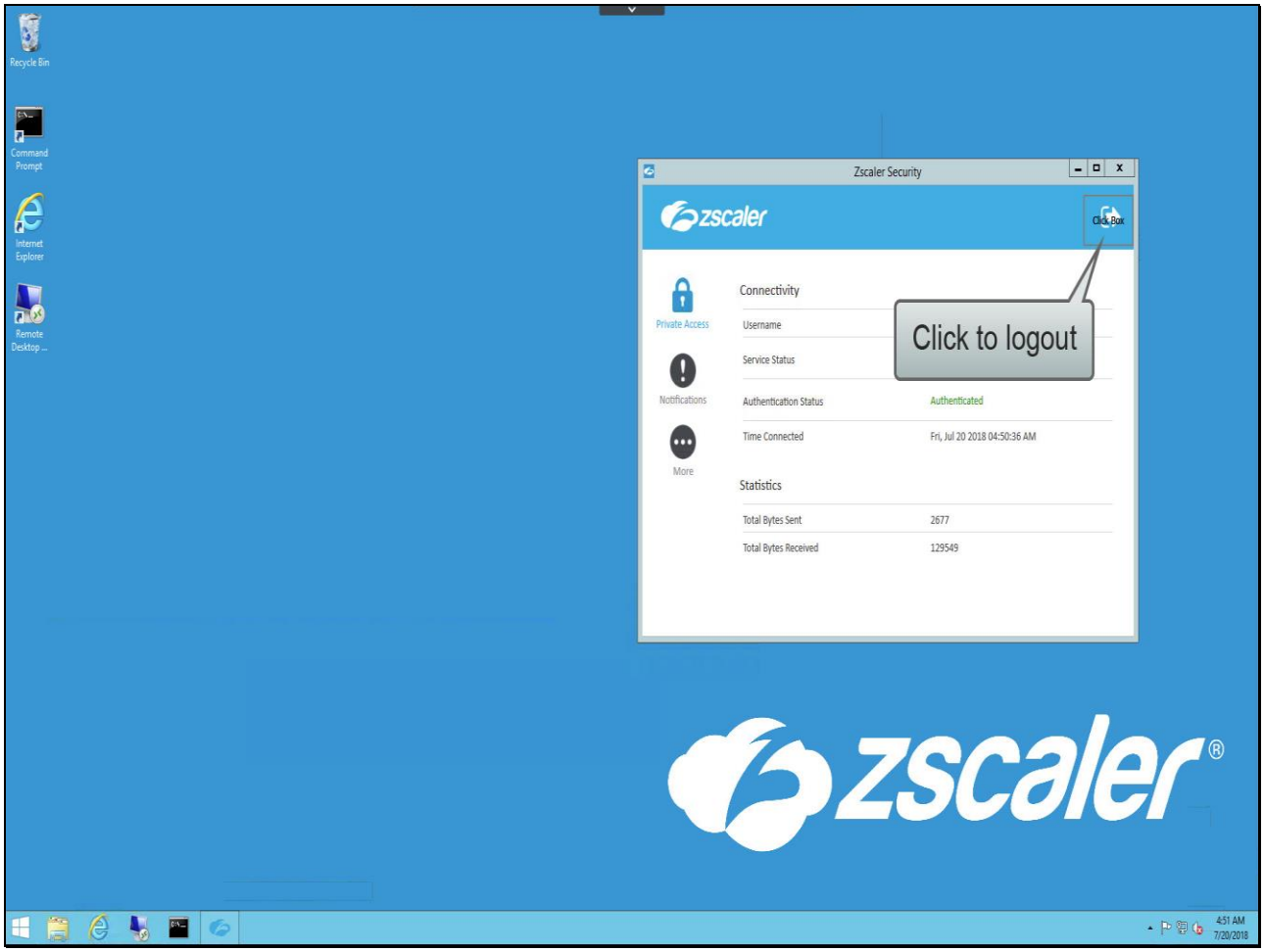


Slide notes

In the final section, we test Browser Access connectivity from an end user's device.

This section has been created as an interactive demo to give you a feel for the use of Zscaler Browser Access as an end user. 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.

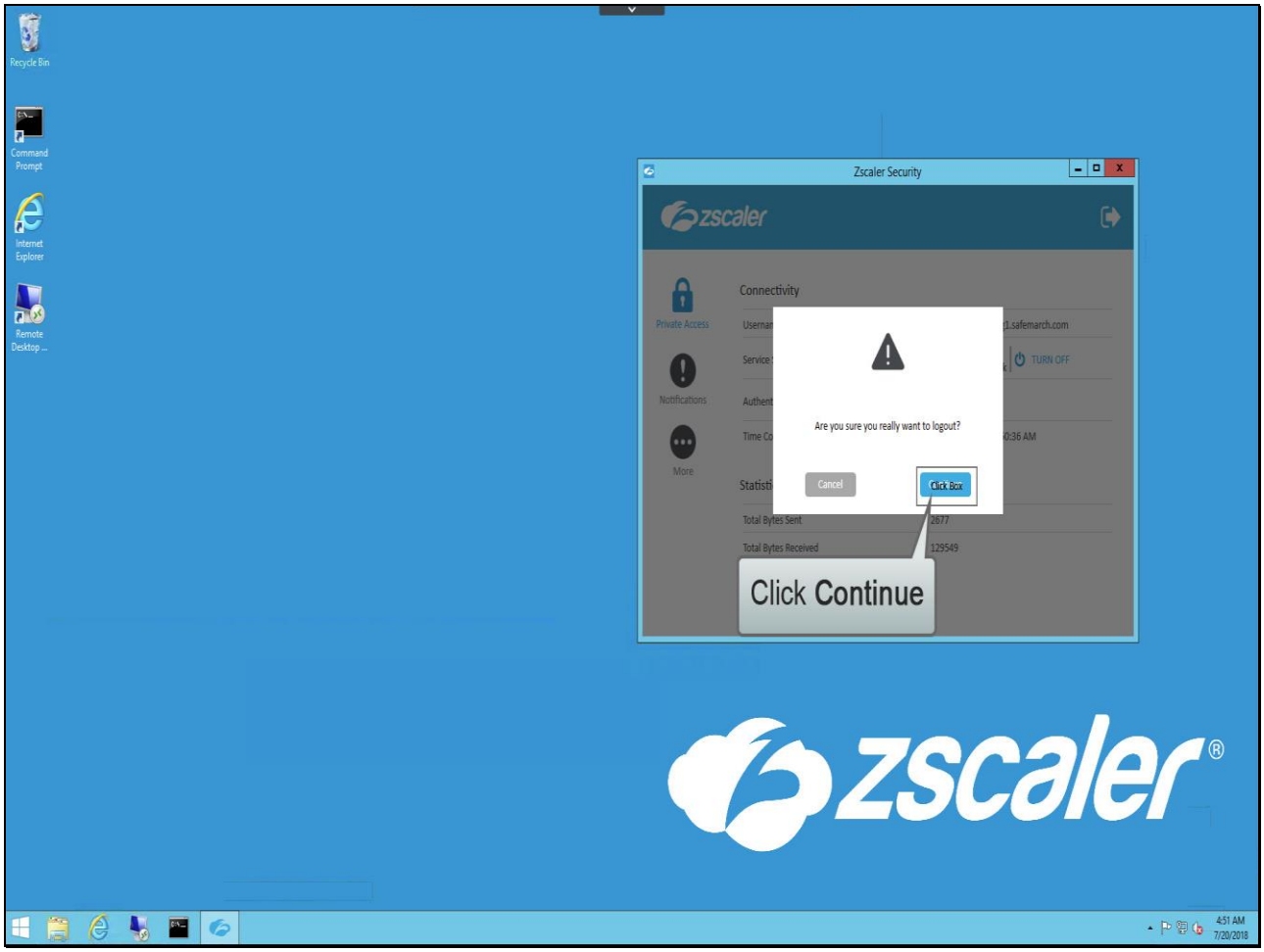
Slide 75 - Slide 75



Slide notes

On an end user's device (in this case a Windows PC), if the Zscaler App is installed and operative, open it and click to logout, …

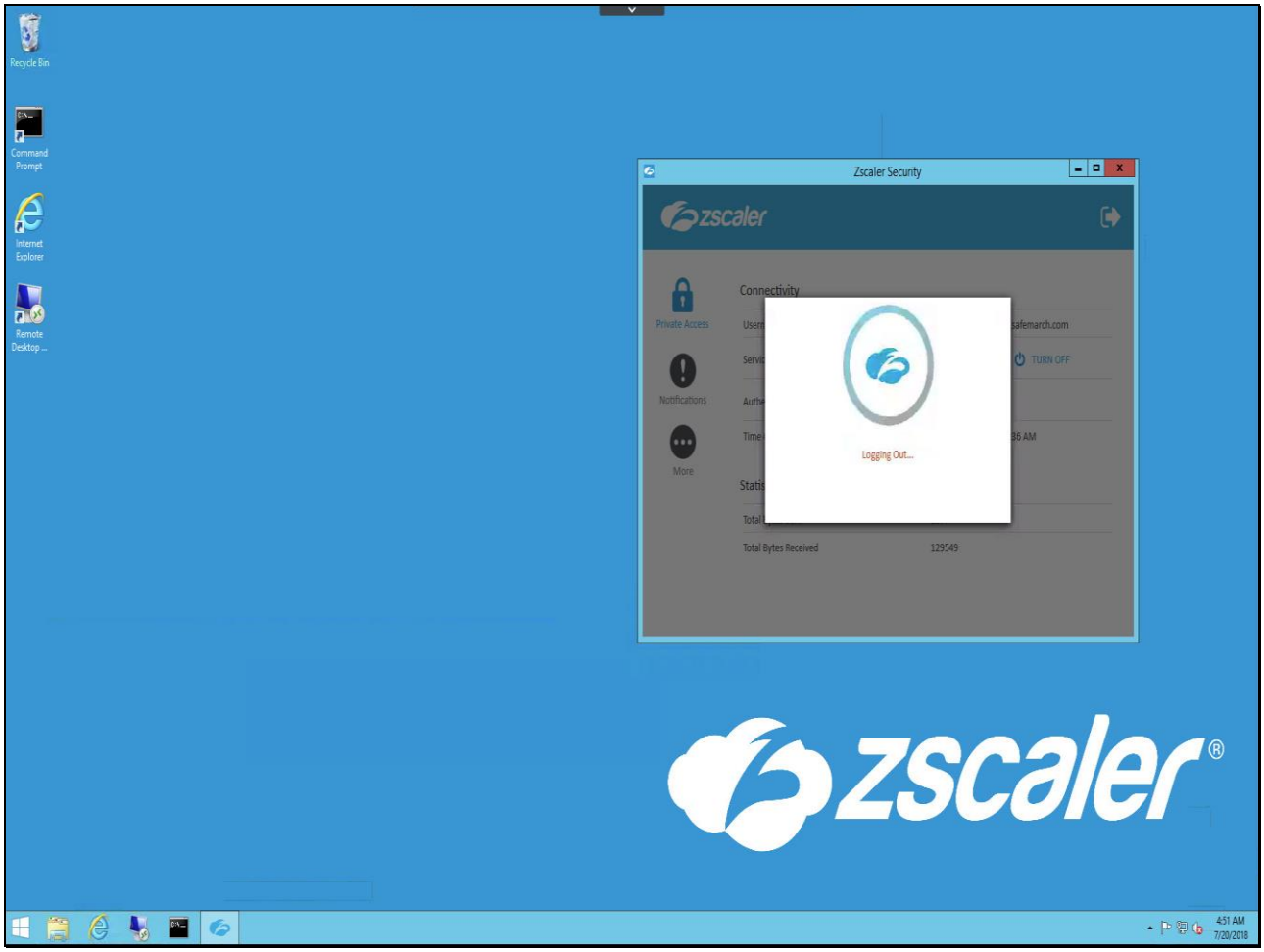
Slide 76 - Slide 76



Slide notes

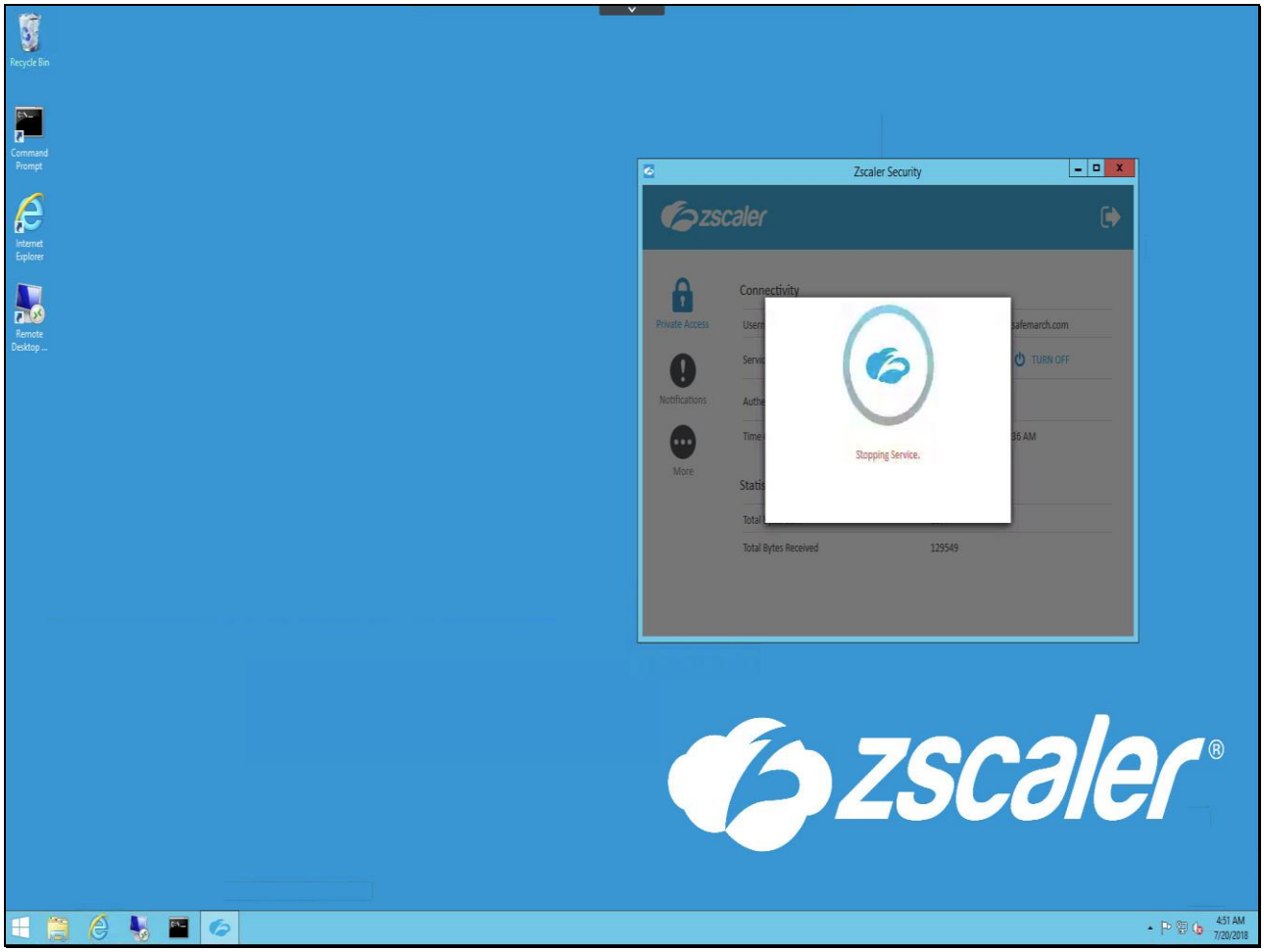
…then click **Continue** (you may need to provide the logout password if one has been set).

Slide 77 - Slide 77



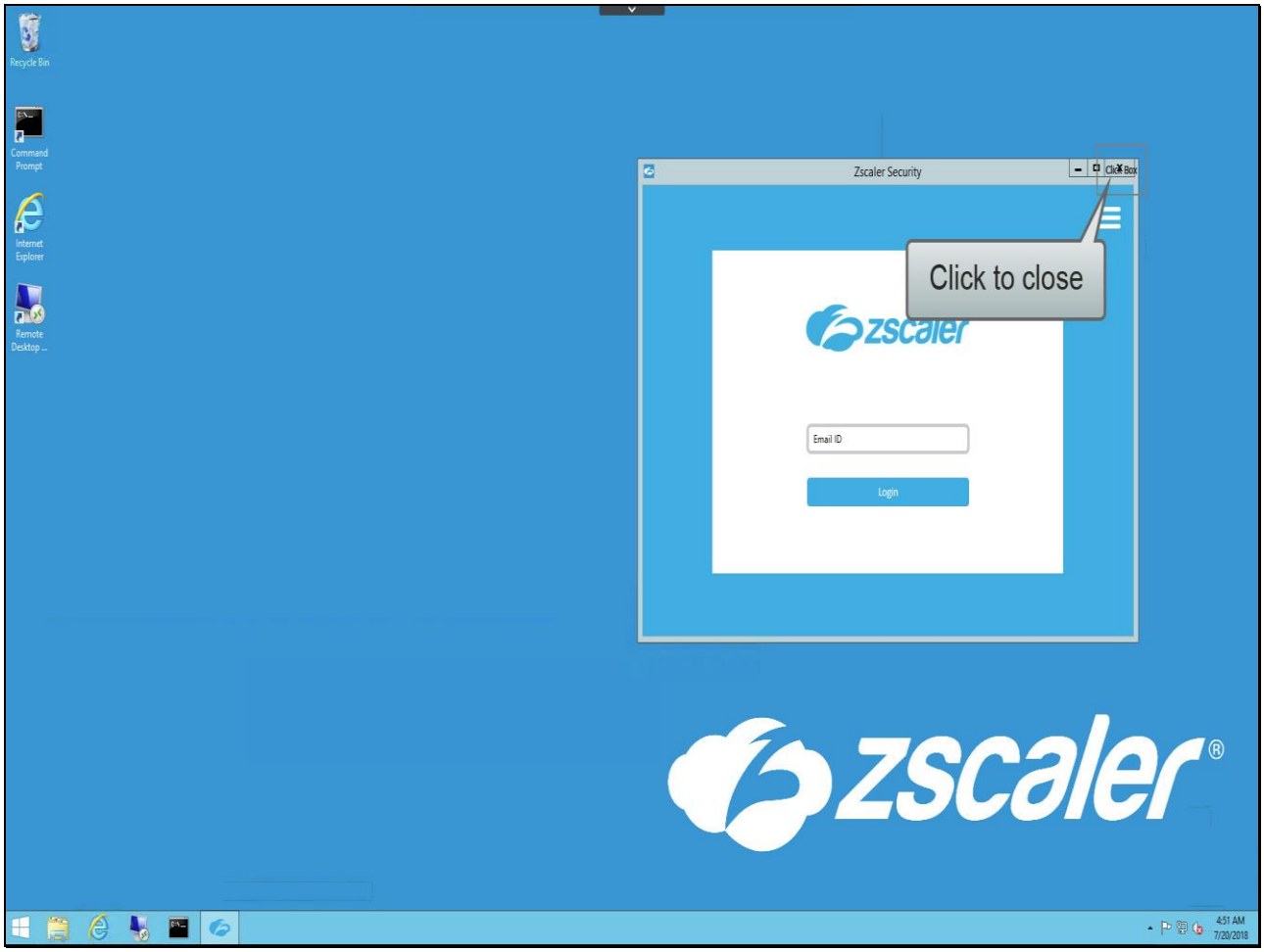
Slide notes

Slide 78 - Slide 78



Slide notes

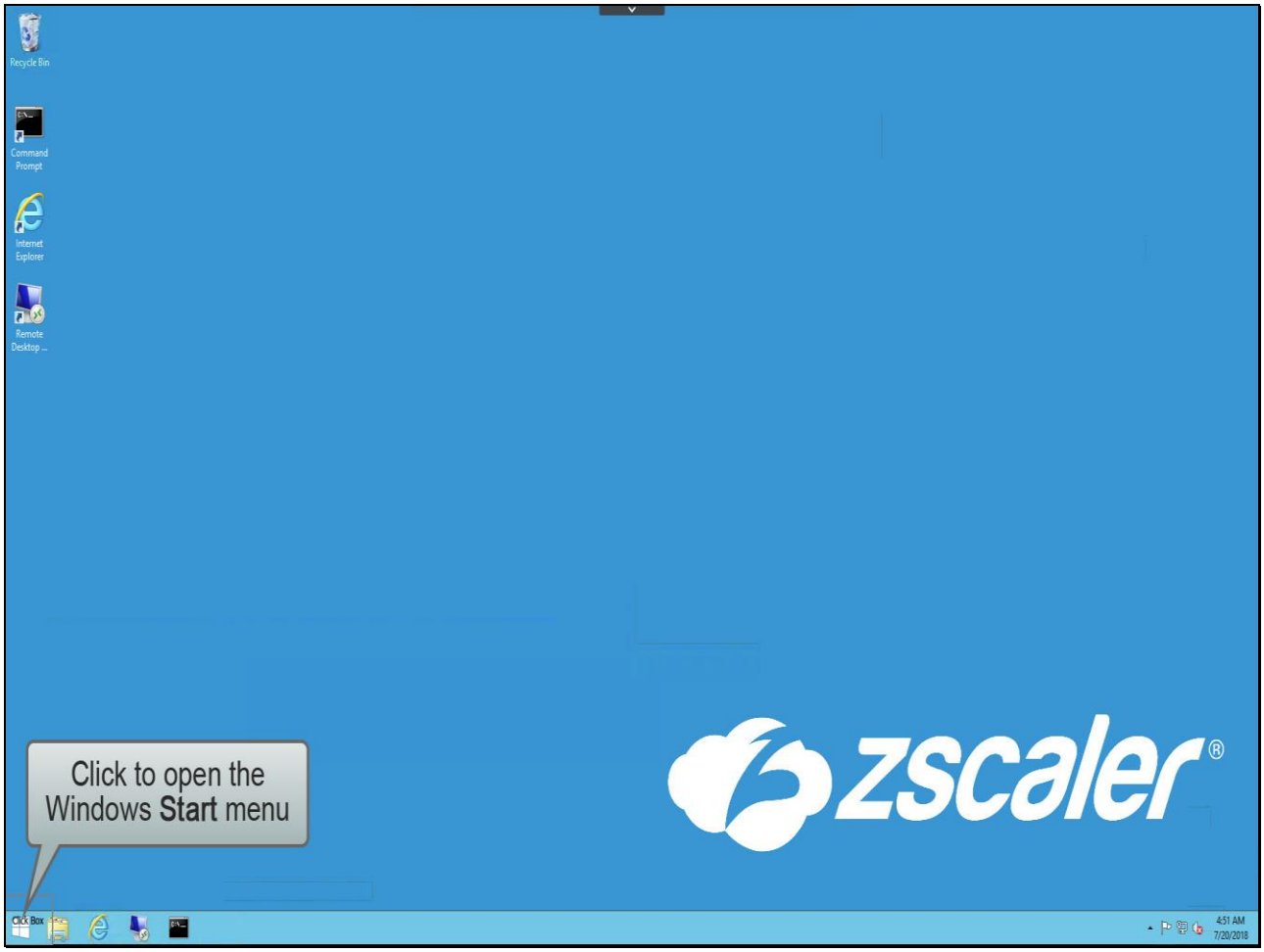
Slide 79 - Slide 79



Slide notes

Click to close the Zscaler App.

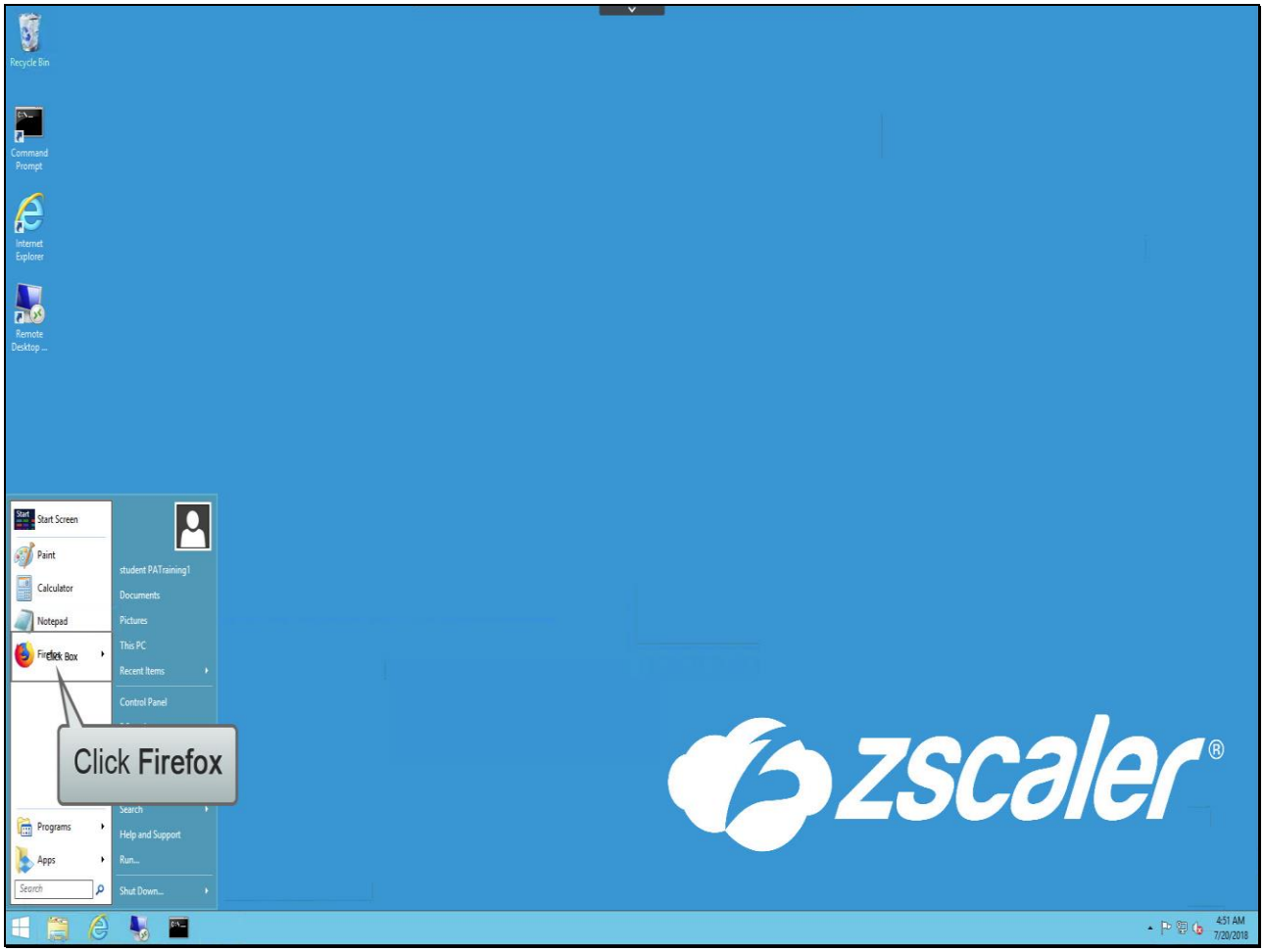
Slide 80 - Slide 80



Slide notes

Click on the Windows **Start** menu, …

Slide 81 - Slide 81

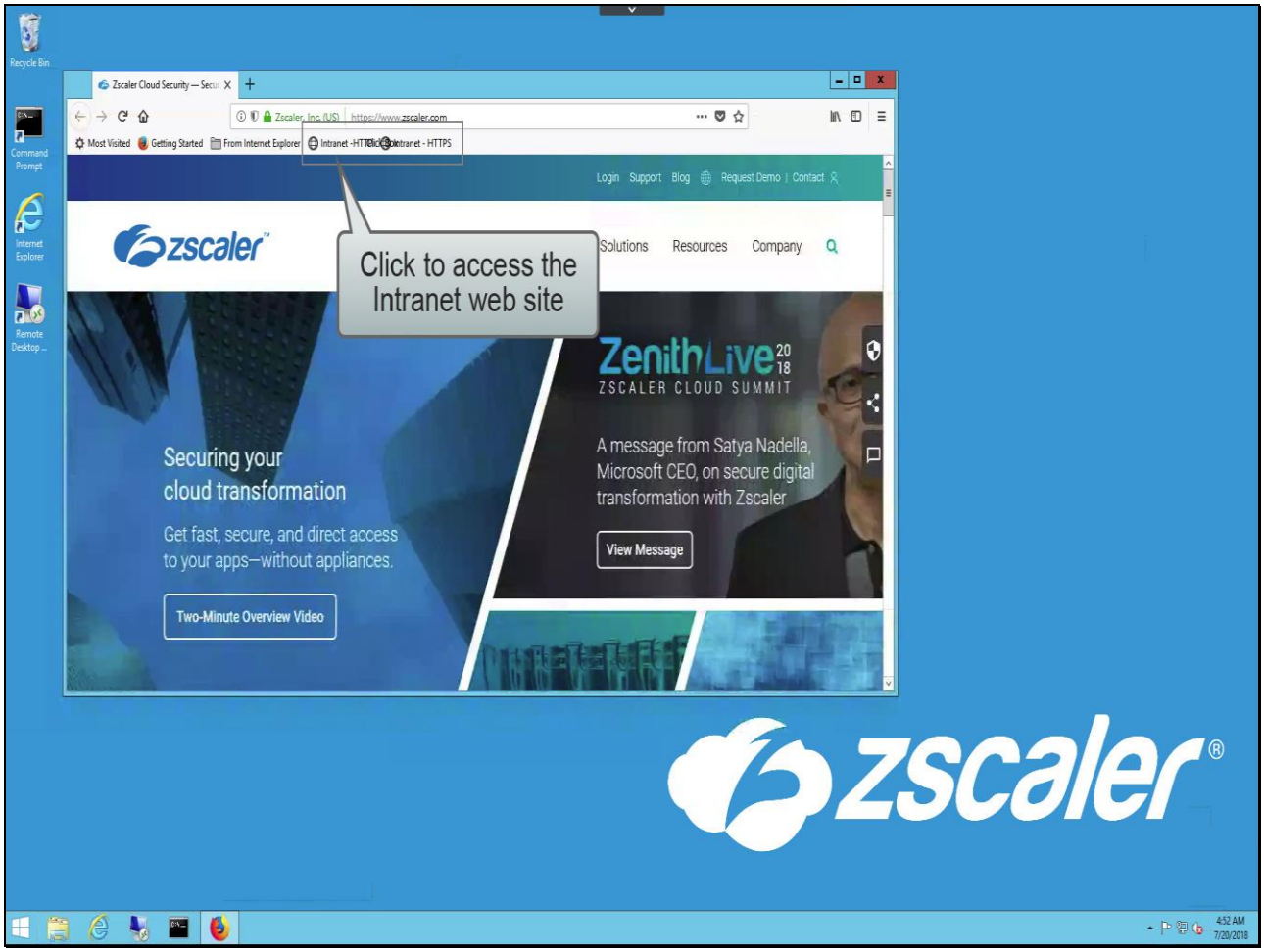


Slide notes

…and open a web browser, in this case click on **Firefox**.

The browser must support TLS1.2 with a specific cipher suite, for details check the Support page at: **https://help.zscaler.com/zpa/about-browser-access**.

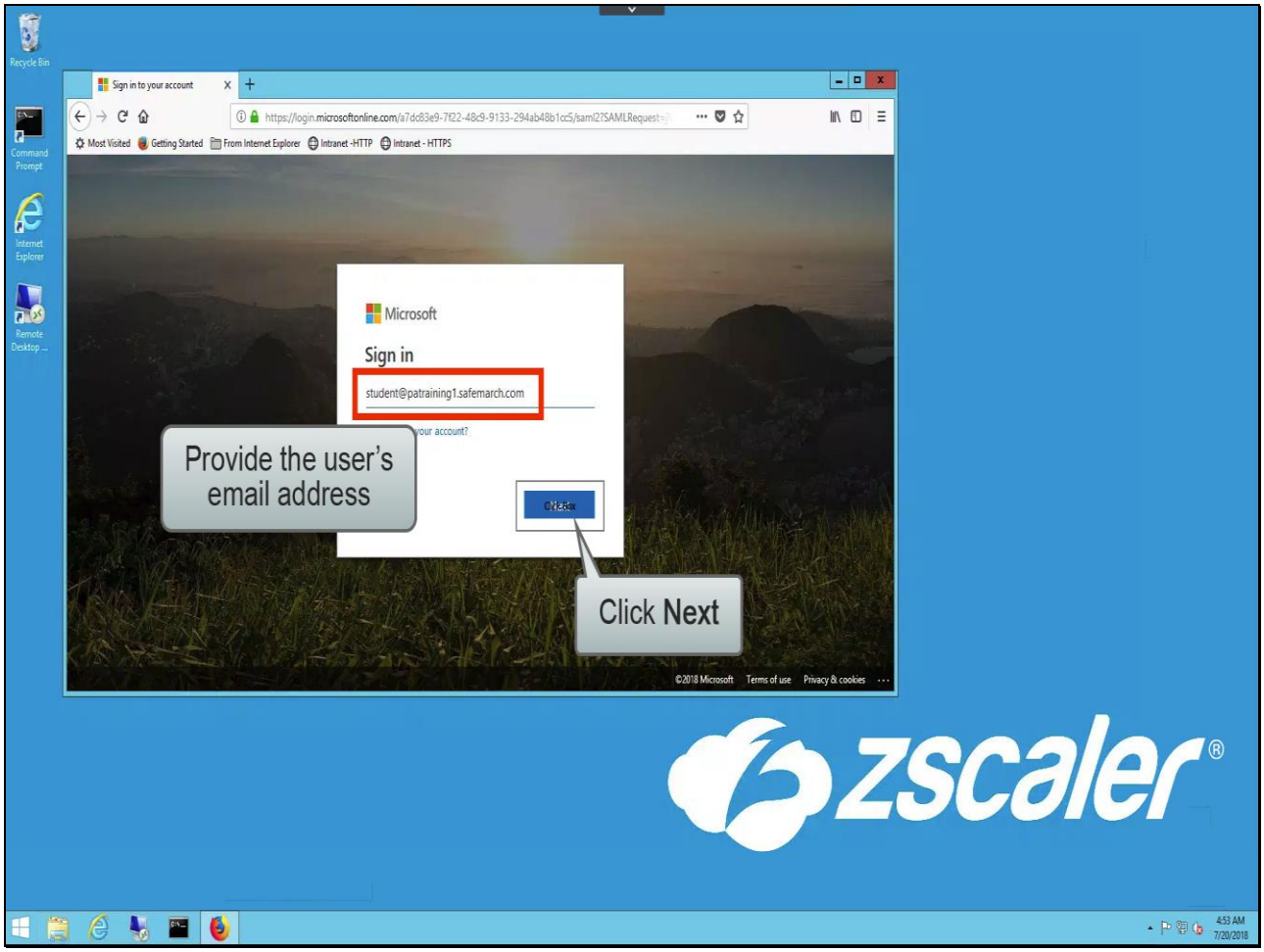
Slide 82 - Slide 82



Slide notes

Navigate to the web application by FQDN, in this case you can click on the saved bookmark.

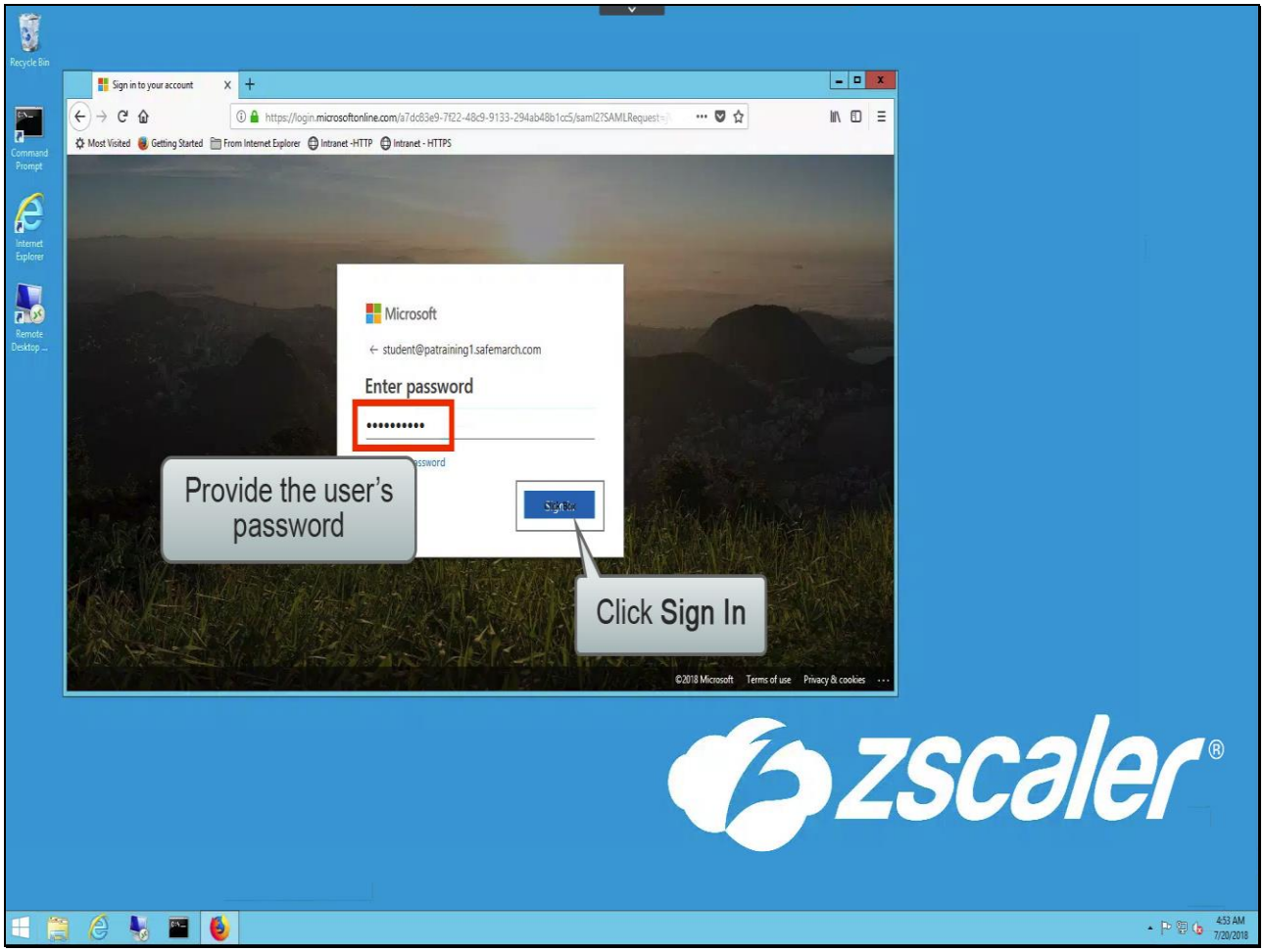
Slide 83 - Slide 83



Slide notes

The request will be re-directed to a nearby BA Exporter and you will be prompted to authenticate. Provide your username and click **Next**, …

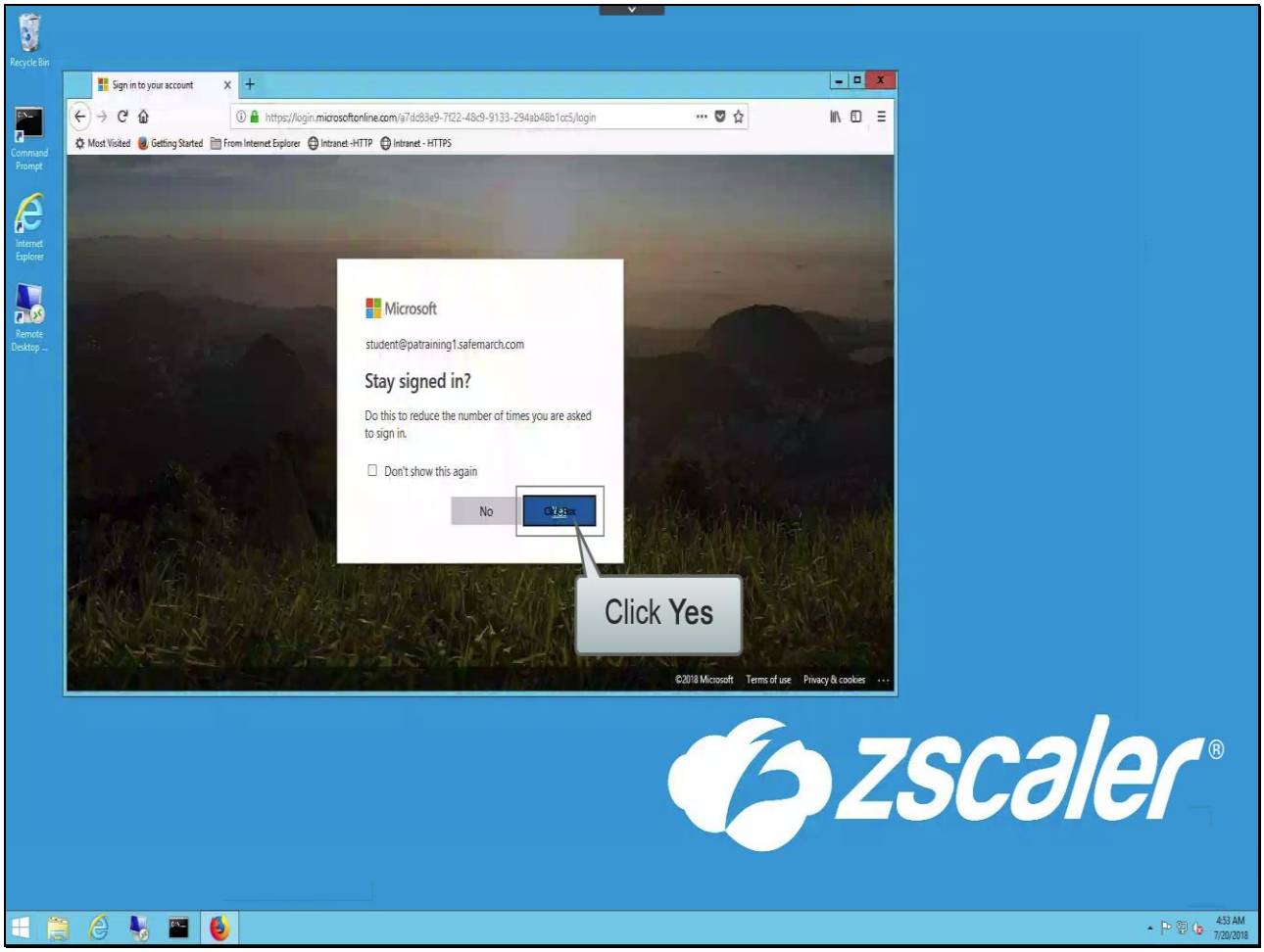
Slide 84 - Slide 84



Slide notes

…key in your password and click **Sign In**, …

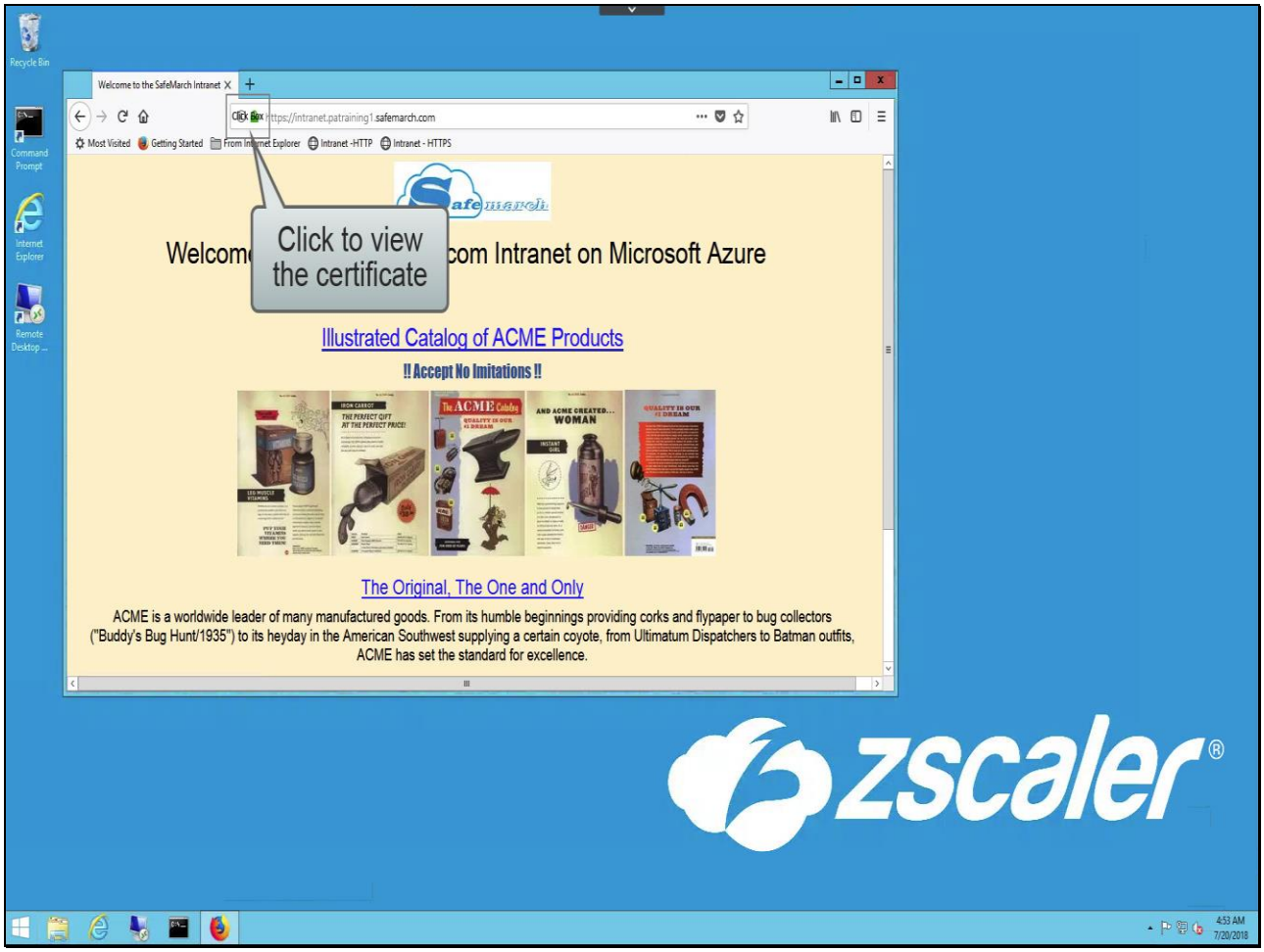
Slide 85 - Slide 85



Slide notes

…elect whether or not to stay signed in, in this case click **Yes**.

Slide 86 - Slide 86

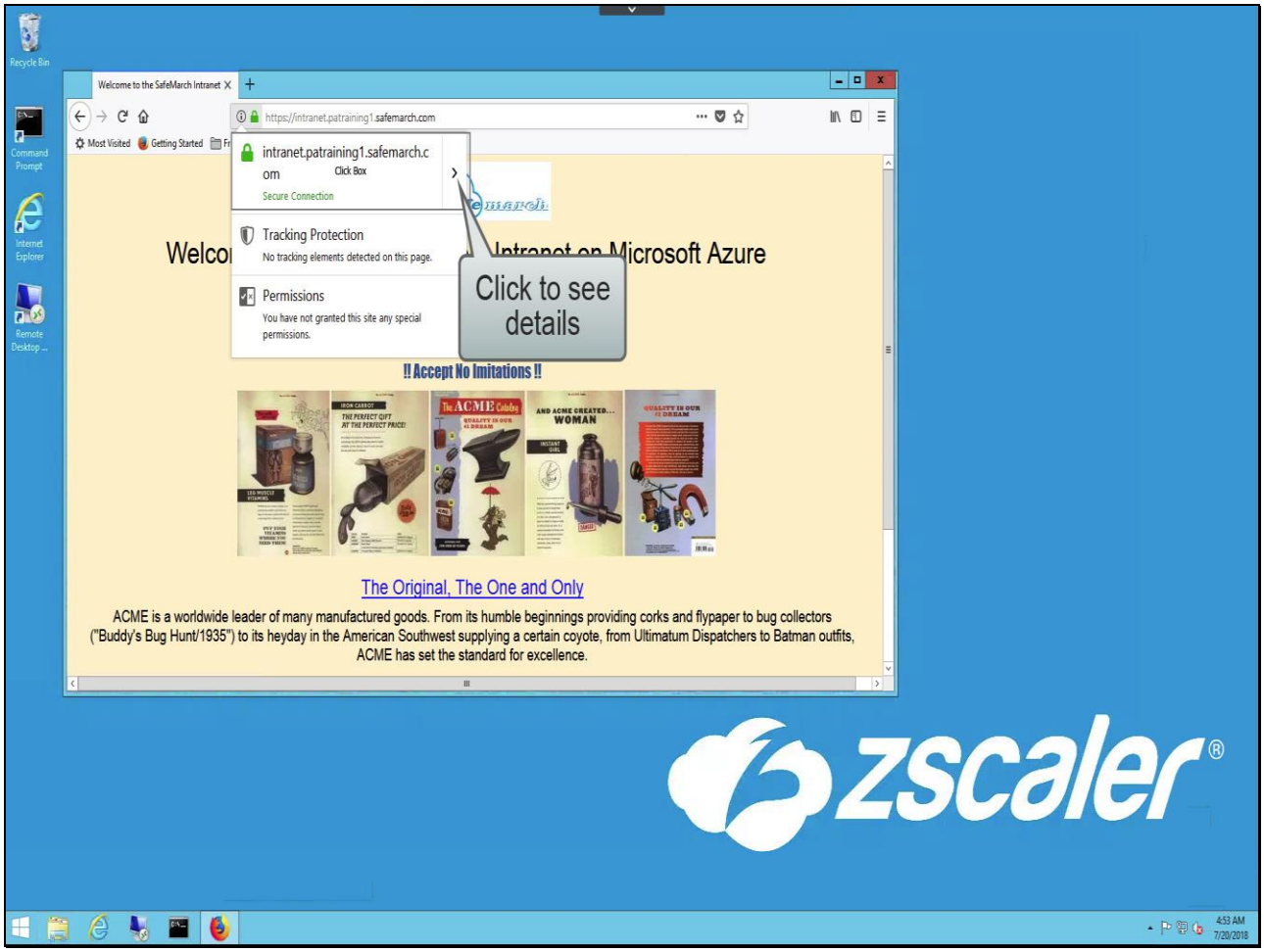


Slide notes

The web application will be displayed.

To view the certificate presented by the ZPA Infrastructure, click on the padlock icon in the browser address bar, …

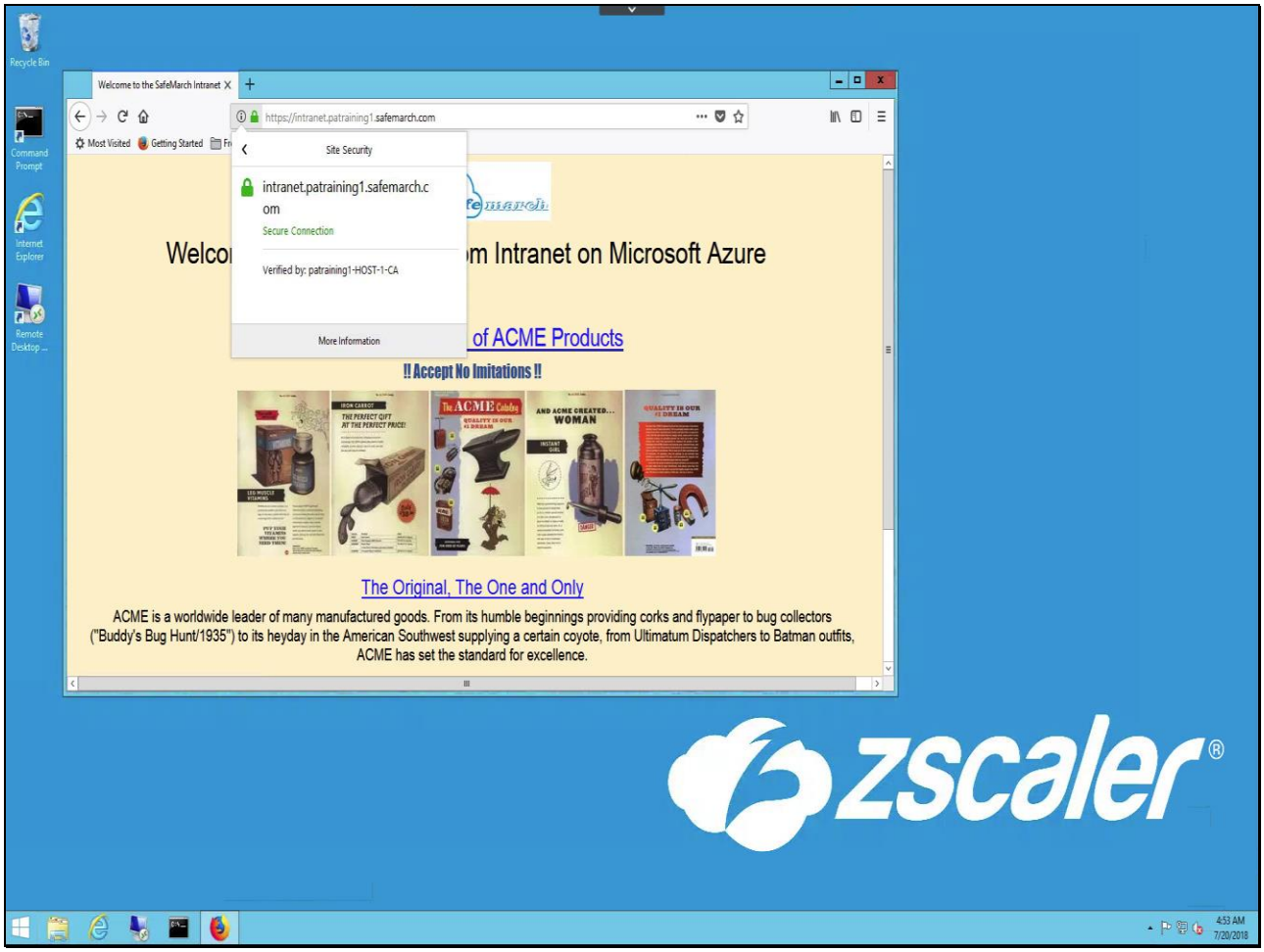
Slide 87 - Slide 87



Slide notes

…and click to view details.

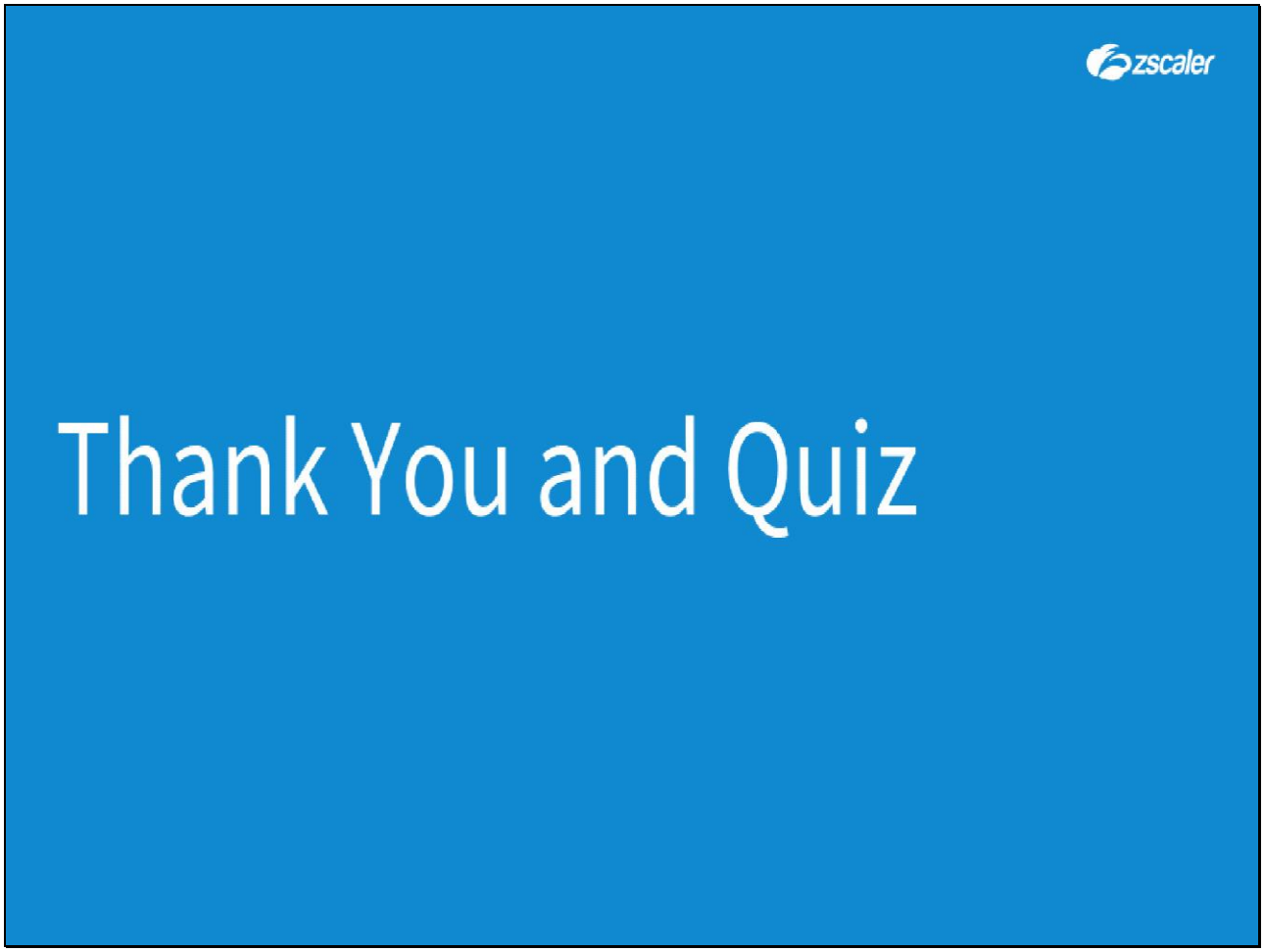
Slide 88 - Slide 88



Slide notes

In this case we can see that the certificate is verified by your internal CA and is fully trusted.

Slide 89 - Thank You and 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.