Slide 1 - ZCCP-IA

Slide notes

Hello and welcome to this eLearning module on the Zscaler Authentication Bridge (ZAB).

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, next slide and fast forward. You can also mute the audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button at the top to exit.

Slide 3 - Agenda

Slide notes

During this session we will look at use-cases for the Authentication bridge (ZAB), cover the pre-requisites for installing the ZAB, examine the configuration and troubleshooting, then move into an interactive demo.

Slide 4 - ZAB Use Cases

Slide notes

Slide 5 - Feature Highlights

Slide notes

The Zscaler Authentication Bridge is a virtual appliance that you can use to provision as well as authenticate users. You can use the ZAB to automatically import user information from an Active Directory Server, or LDAP server, to the Zscaler database without requiring inbound connections to your directory server. The ZAB can be used solely as a provisioning tool in conjunction with another authentication mechanism such as SAML or Kerberos.

Alternatively, it can be used for authentication as well using LDAP with SSL client certificates. The ZAB scales to hundreds of thousands of users; it requires minimal administration. After you deploy it you can configure the service to automatically synchronize users: on-demand, daily, weekly, monthly, or custom time period.

Slide 6 - ZAB Explained

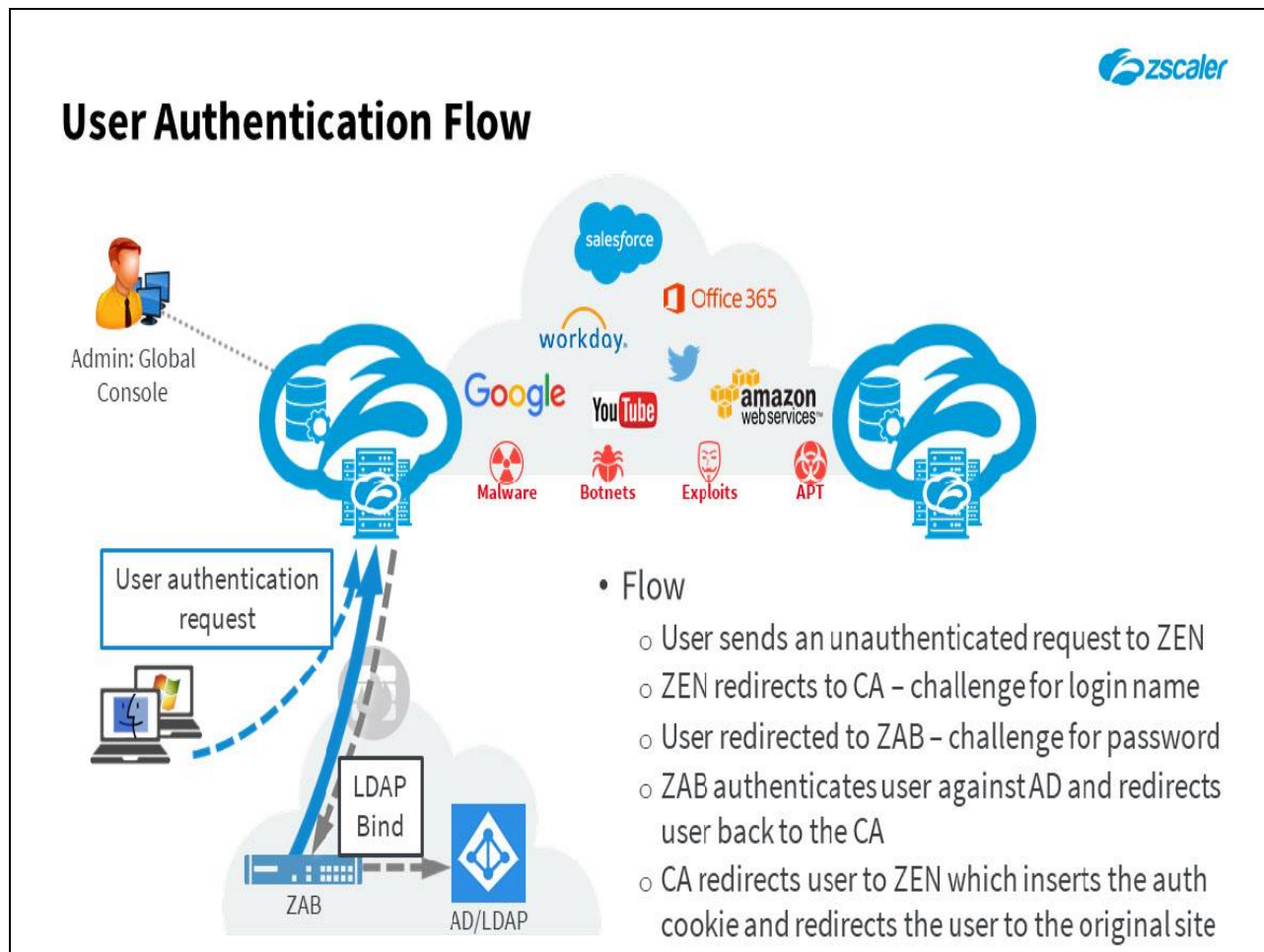**Slide notes**

Slide 7 - User Provisioning Flow
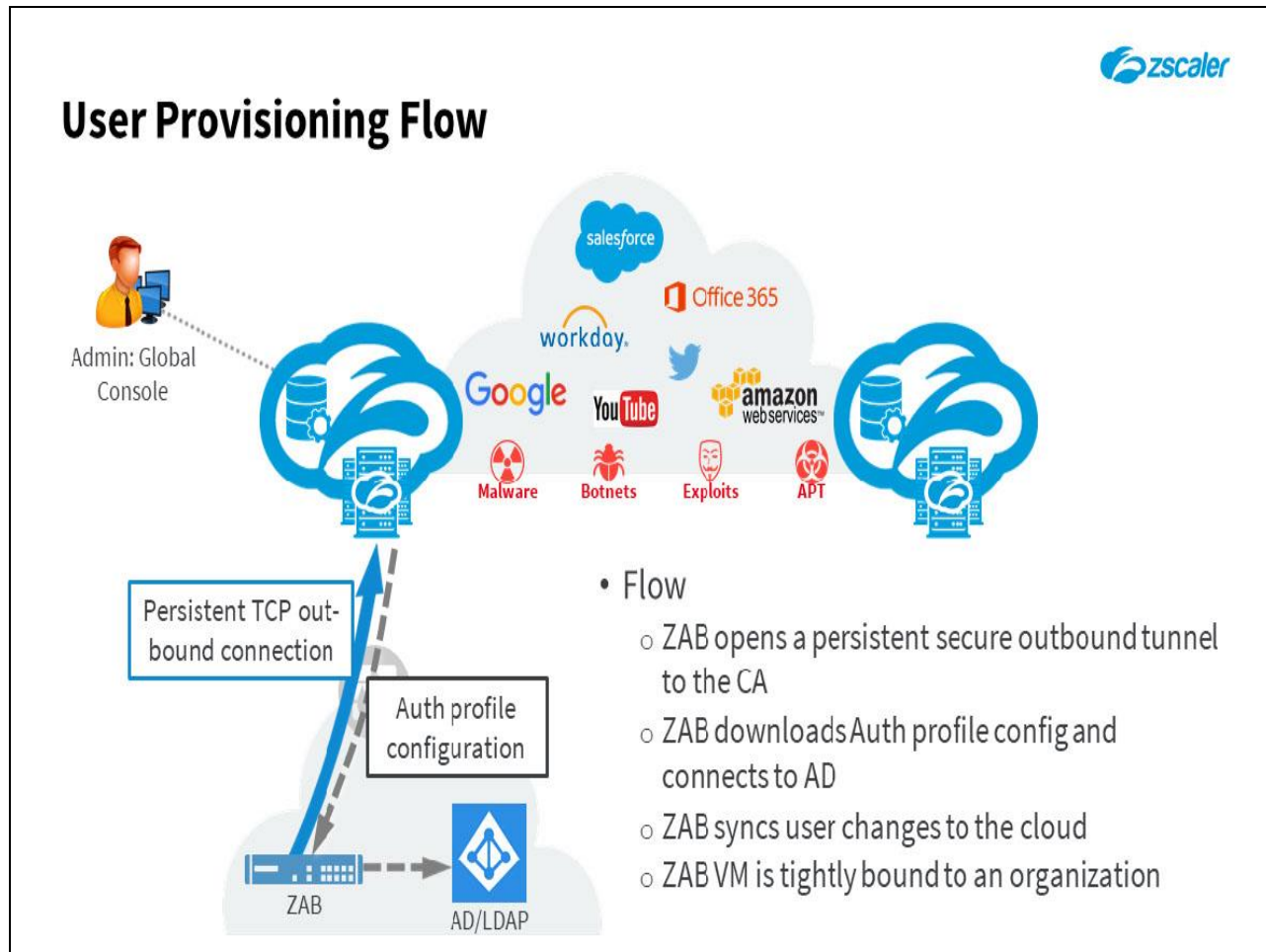
Slide notes

As shown in the diagram the ZAB sits behind the Firewall with the directory server. The ZAB opens a long lived, secure, outbound tunnel to the Zscaler cloud. The ZAB downloads the auth-profile config and connects to Active Directory. When the administrator forces a manual sync, via the Admin Portal, or at the configured auto-sync time, the ZAB will synchronize the user information changes to the cloud. Configurable auto sync times are: daily, weekly, monthly, or a custom time period.

A ZAB VM is tightly bound to the organization so a ZAB can only sync users for that organization and no other.

Slide 8 - User Authentication Flow

Slide notes
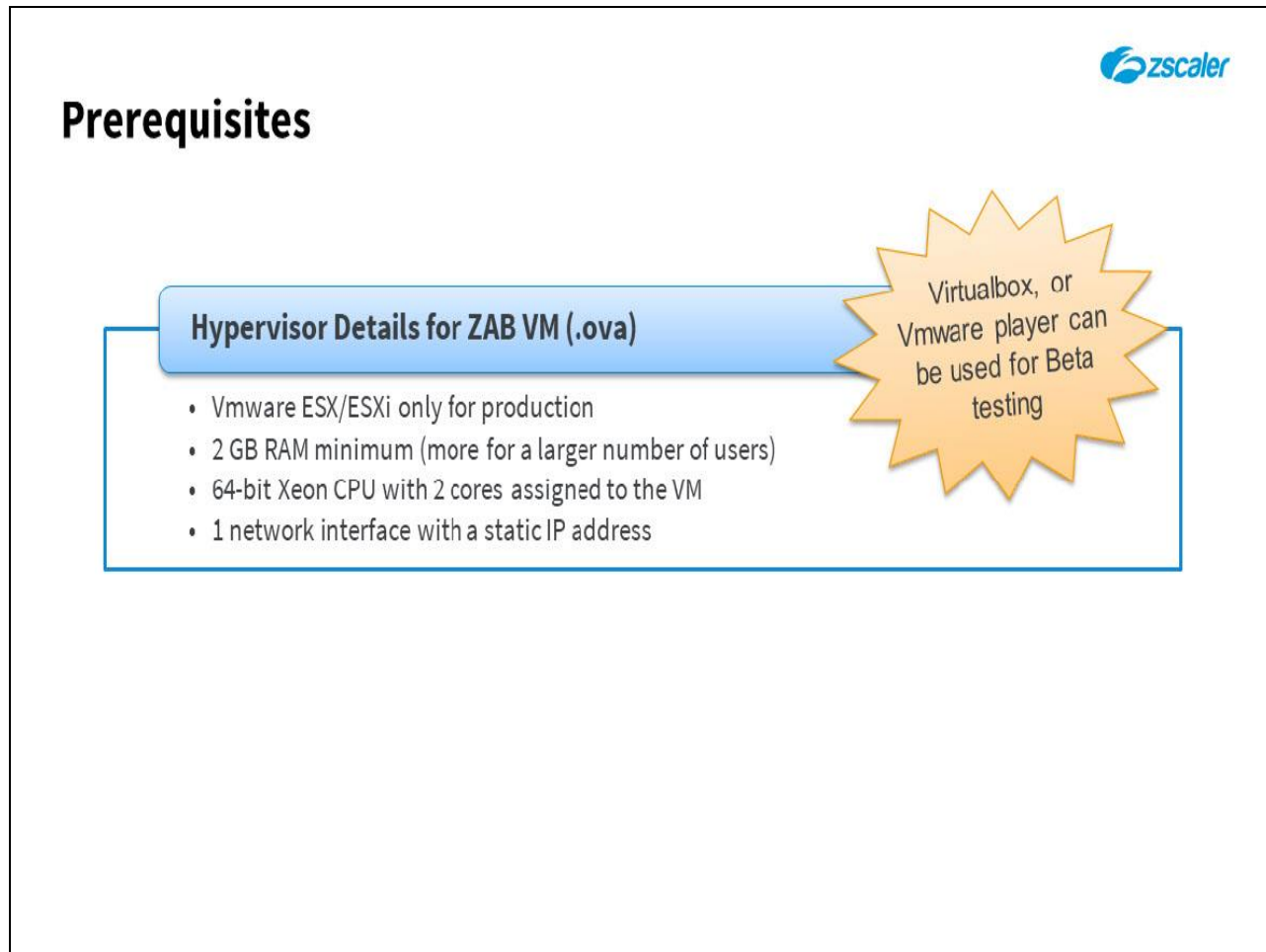
Now let's examine the user authentication flow:
- When an unauthenticated user tries to browse to a website the ZEN sees that the user is unauthenticated;
- The ZEN redirects the user to the CA which challenges the user for the login name;
- The user specifies the login name;
- And is redirected to the ZAB which challenges the user for the password;
- The ZAB authenticates the user against Active Directory;
- And then redirects the user back to the CA;
- The CA redirects the user to the ZEN which inserts the authentication cookie and redirects the user to the original destination.

Slide 9 - Prerequisites

Slide notes

Slide 10 - Prerequisites

Slide notes

The ZAB VM must be run on ESXi for production environments. VM player or workstation may be used but for proof of concept or for Beta testing only. There must be a minimum of 2GB of memory allocated and this will increase with the number of users. The Admin UI calculates the server hardware requirements based on the number of users authenticating against the ZAB. You will see this as part of the interactive demo.

Slide 11 - Prerequisites

Prerequisites

Hypervisor Details for ZAB VM (.ova)

- Vmware ESX/ESXi only for production
- 2 GB RAM minimum (more for a larger number of users)
- 64-bit Xeon CPU with 2 cores assigned to the VM
- 1 network interface with a static IP address

Virtualbox, or Vmware player can be used for Beta testing

Network readiness for ZAB

- Host name entry for the ZAB for both the internal, and public IP of the ZAB
- Use Authentication Exemption for the Public IP of the ZAB (or configure a bypass in the PAC file / proxy settings)
- Server Certificate for an issuing authority if using the ZAB for user authentication

Slide notes

To prepare the network for the ZAB you should have an entry for the hostname of the ZAB for both the internal IP as well as the public facing IP of the ZAB. You should also enable authentication bypass for the public IP of the ZAB or set an exception in the PAC file or proxy settings if using the ZAB for authentication.

A server certificate from an issuing authority should also be used if using the ZAB for user authentication. This will prevent the user from seeing a server certificate warning in the browser.

Slide 12 - Configure Outbound Firewall rules for user provisioning

Configure Outbound Firewall Rules for User Provisioning

Source IP	Dest IP	Service Port	Description
ZAB IP Address	Zscaler Hub IP	9422 (TCP)	Connection to Zscaler Central Authority for authentication, user sync, and Policy Retrieval. Network configuration download
ZAB IP Address	Zscaler Hub IP	443 (TCP)	Connection to the Zscaler Central Authority for master CA resolution Connection to the update server for software download
ZAB IP Address	Remote Support IP	12002 (TCP)	Reverse Tunnel for remote support assistance. This feature is optional and must be explicitly enabled by the customer
ZAB IP Address	Local Name server IP	53 (UDP/TCP)	For domain resolution. This may be an internal name server
ZAB IP Address	NTP Server IP	123 (UDP)	Time sync with NTP Servers. The ZAB is extremely sensitive to VM and the cloud times being in sync. Please refer to the latest ZAB Guide for configuring sync with local NTP Server.
ZAB IP Address	LDAP or AD	LDAP/AD Listening Port (TCP)Typically: 389, 636, 3268, 3269	Connection to the LDAP or AD Server for synchronizing and/or authenticating users. Zscaler strongly recommends secure LDAP connections

o For an up to date and complete list of Zscaler IP addresses for your Firewall policies go to:
https://ips.*<cloud_name>*.net/zab

For example: **https://ips.zscalerone.net/zab**

https://ips.zscalertwo.net/zab

Slide notes

No inbound connections from Zscaler to the ZAB are required to be opened in your firewall. You do, however, need to ensure that the ZAB can communicate out to the Zscaler service on the ports you see listed here. Port 12002 is optional and is only needed for Zscaler TAC to remotely access your ZAB for troubleshooting. This feature is disabled by default.

For a list of the Zscaler IP addresses your ZAB must be able to reach see the URL at the end of this slide for a complete and up to date list. The URL is **https://ips.<your assigned cloud name>.net/zab**. So, for example **https://ips.zscalertwo.net/zab**.

Slide 13 - ZAB for Authentication as Well as User provisioning

Slide notes

If using the ZAB for both provisioning and user authentication, then you will need to open an inbound connection to your ZAB on port **443**.

Slide 14 - Configuration Overview

Slide notes

Let's now examine the steps involved with setting up a ZAB for authentication.

Slide 15 - Overview of the Steps

Slide notes

1. The Zscaler Authentication Bridge is offered on subscription. You must first purchase the option then it will appear in your subscription list in the Admin Portal then the options to configure the ZAB will appear in the Admin Portal as well.

Slide 16 - Overview of the Steps

Slide notes

2. Once subscribed you register, or create, a new ZAB instance in the Admin Portal, …

Slide 17 - Overview of the Steps

Slide notes

3. …which then allows you to download of the ZAB VM and SSL client certificate.

Slide 18 - Overview of the Steps
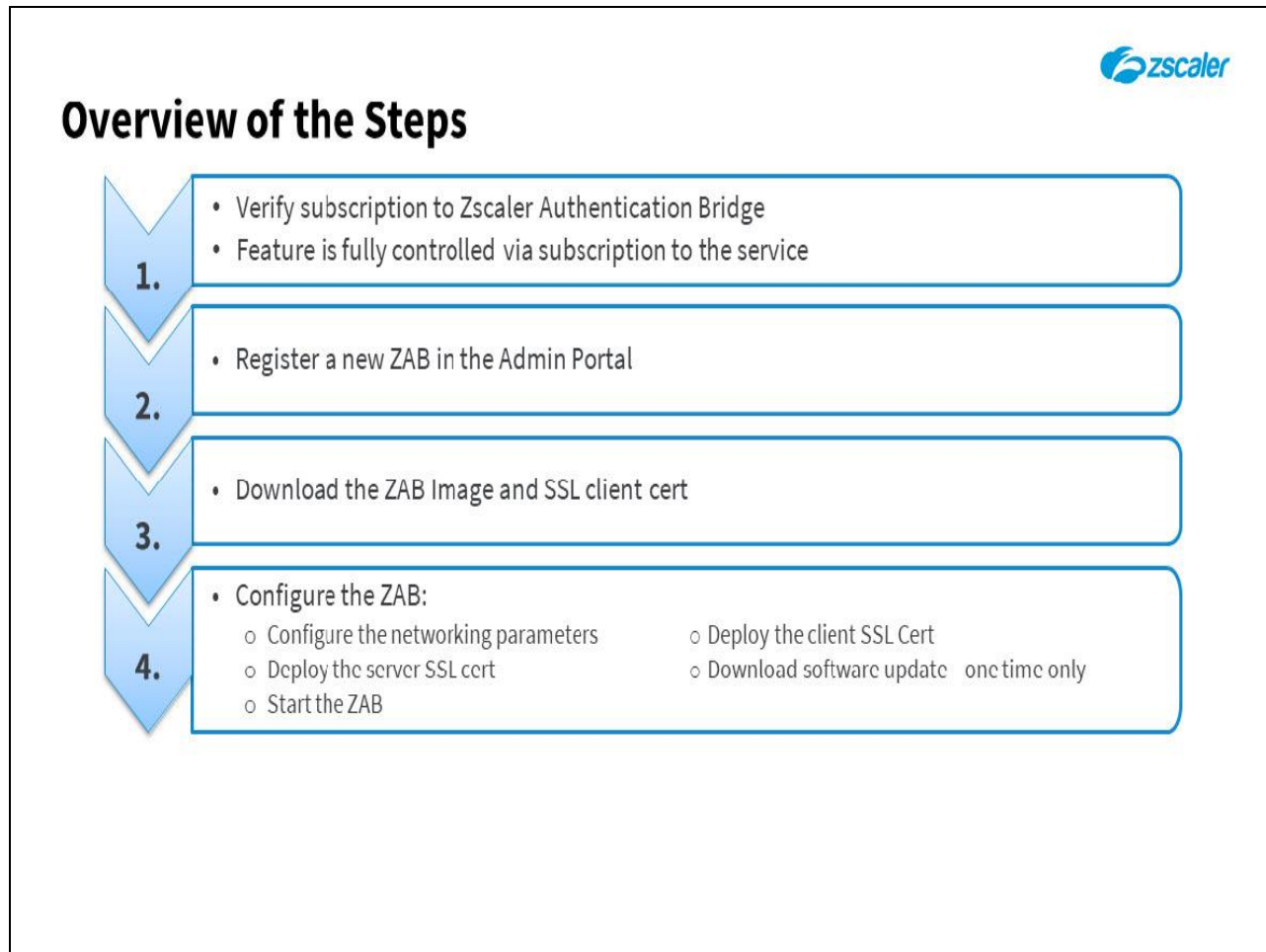
Slide notes

4. To configure the ZAB itself you will: launch the VM, configure the network parameters, deploy the client certificate and server certificate, perform a one-time software update, then start the ZAB.

Slide 19 - Overview of the Steps
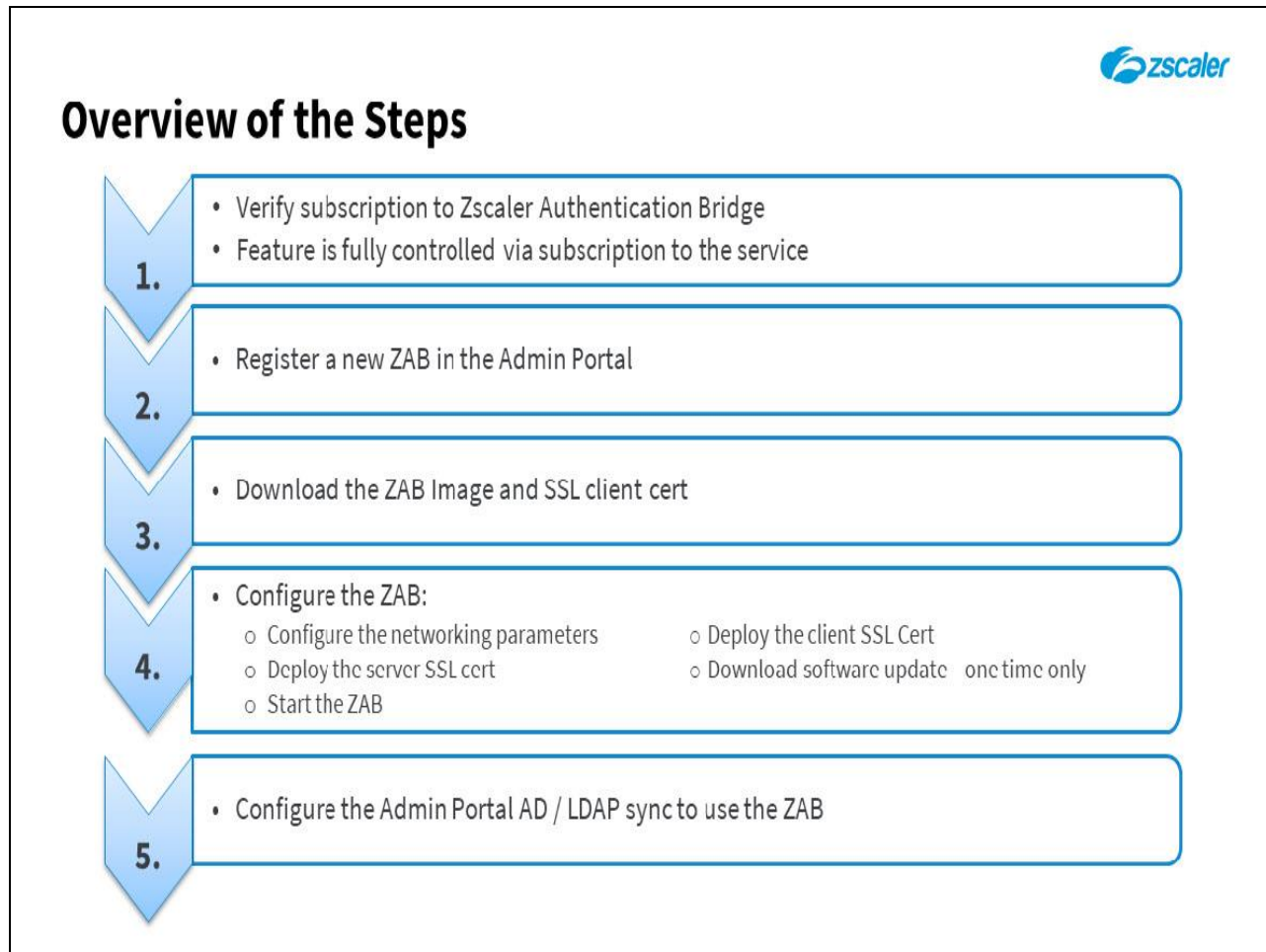
Slide notes

5. There are a few additional steps for configuration in the Admin Portal. All of which will be covered later during the interactive demo.

Slide 20 - ZAB Config Step Summary / Cliff Notes

ZAB Configuration Steps Overview

1. Start ZAB VM
2. Take option 1 for the OS or just let the default timer expire and auto-start
3. Login using **zsroot / zsroot**
4. Switch to super-user: **sudo su –**
5. Login with **zsroot**
6. **zab configure**
   a) **Nameserver**
   b) **IP address / mask** e.g. 192.168.1.25/24
   c) **Default GW**
7. **zab dump-config** to verify config
8. Download the **ZabCert.zip** from the AdminUI under Authbridge page
9. Use SCP to copy **ZABCert.zip** to the VM
10. Install the cert **zab install-client-cert /<path>/ZabCert.zip**
11. **zab dump-config** to verify cert is installed and recognizes the right cloud

12. Install the server cert **zab install-server-cert** (can be by CA- or self-signed). Just hit enter for self signed and provide key string and verify
13. **zab update-now** to download the current build
14. **zab start**
15. **zab enable auto-start**
16. Verify the ZAB is running **zab status**
17. Verify connectivity **sockstat** should show connections to ZEN / CA and AD
18. **zab test-firewall** to ensure connectivity to all necessary

AdminUI step summary
1. Run setup wizard
   a. **Auth Agent hosting = Enterprise** (for ZAB use)
   b. **Directory server IP = AD**
   c. **Auth Agent Address = ZAB Host Name**

Slide notes

Here is a summarization of the steps involved with configuring the ZAB. This slide is for your reference only and you will see these steps in the interactive demo.

Slide 21 - Interactive Demo
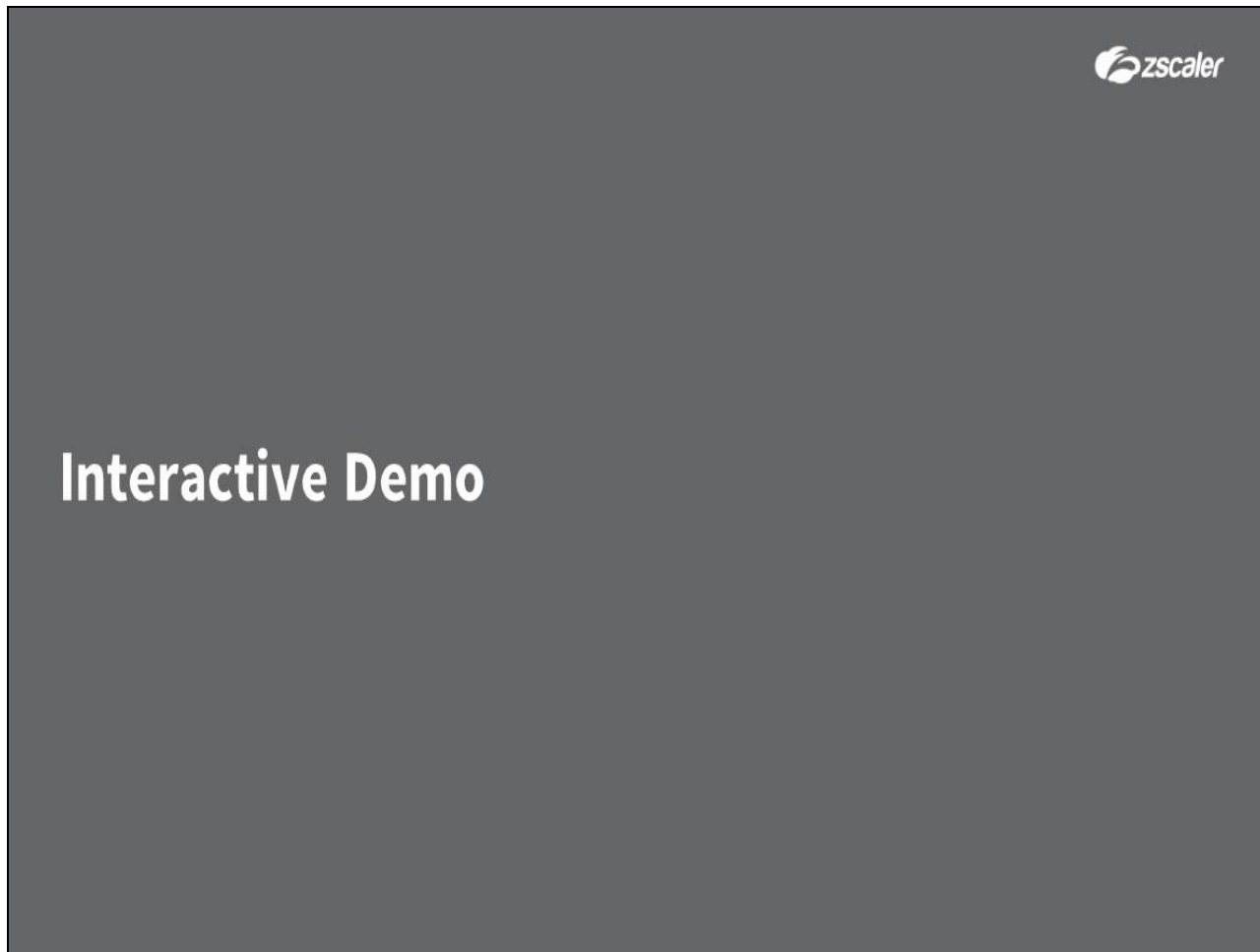
Slide notes

Now let's walk through the configuration of the Zscaler Authentication bridge. Your participation is required during the configuration of the Admin Portal. The configuration of the ZAB will be a demo only.

Slide 22 - Slide 22
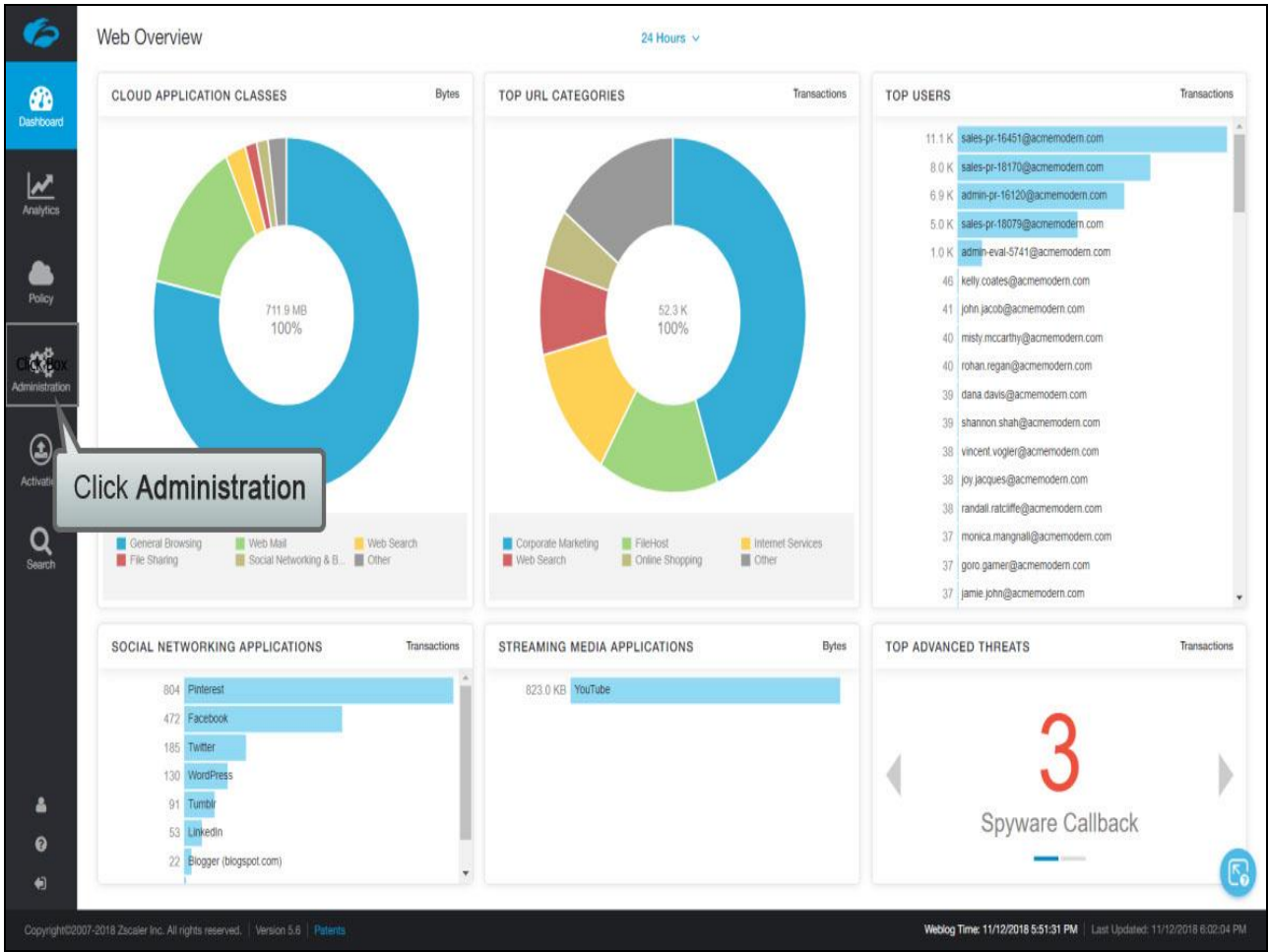
Slide notes

Begin in the Zscaler Admin Portal by going to **Administration**, …

Slide 23 - Slide 23
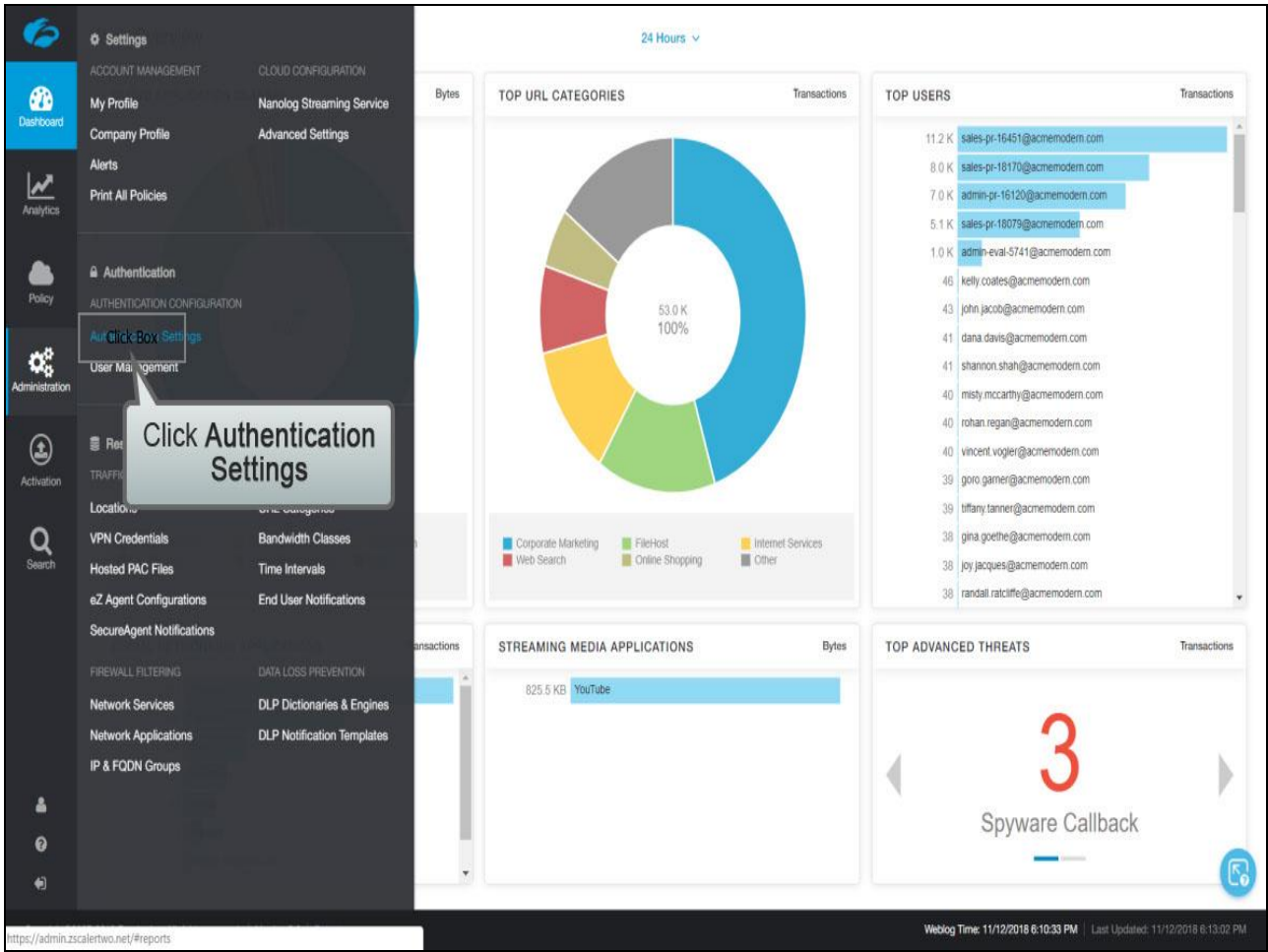
Slide notes

…then **Authentication Settings**.

Slide 24 - Slide 24

Slide notes

Then click on the **Authentication Bridges** tab.

Slide 25 - Slide 25

Slide notes

Click **Add Authentication Bridge** to add a new Authentication Bridge.

Slide 26 - Slide 26

Slide notes

Then enter the name of your Authentication Bridge.

Slide 27 - Slide 27
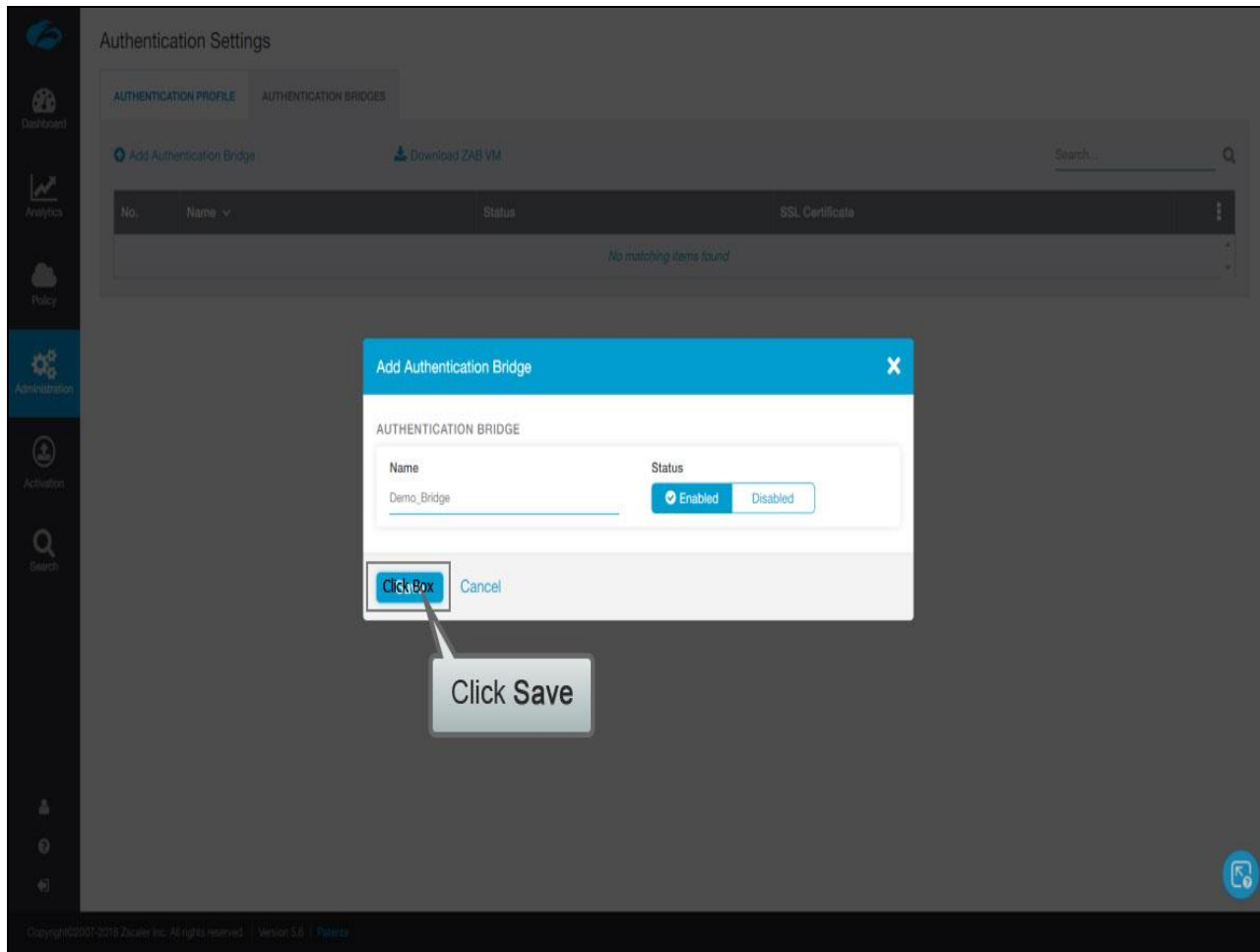
Slide notes

Then click **Save**.

Slide 28 - Slide 28

Slide notes

Slide 29 - Slide 29

Slide notes

And **Activate** your changes.

Slide 30 - Slide 30
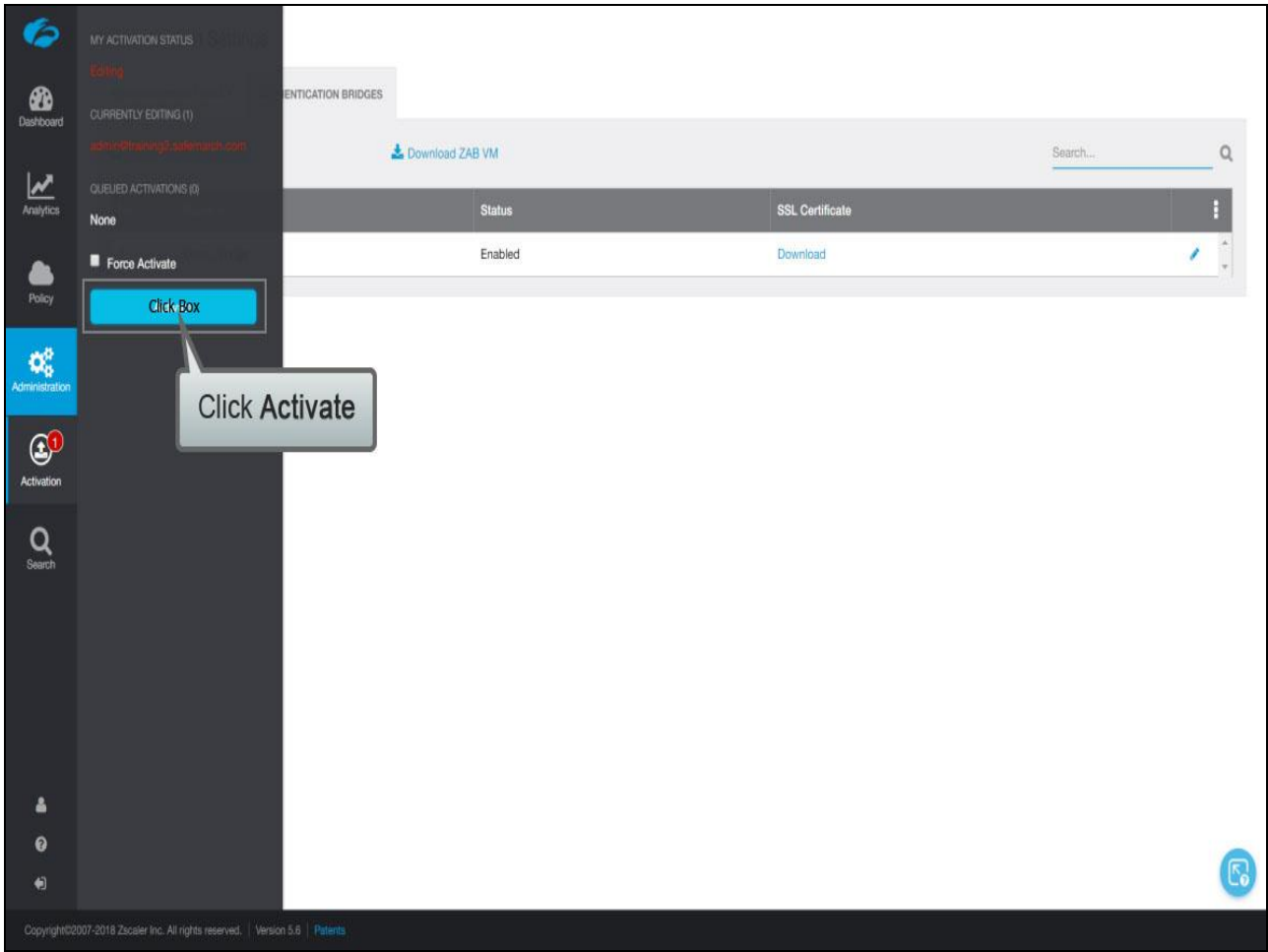
Slide notes

Slide 31 - Slide 31

Slide notes

Slide 32 - Slide 32

Slide notes

In the **SSL Certificate** column, under your new ZAB instance, click the **Download** button to download the client certificate. You will use this later as part of the ZAB configuration.

Slide 33 - Slide 33

Slide notes

Slide 34 - Slide 34

Slide notes

Download a copy of the ZAB virtual machine by clicking on the **Download ZAB VM** button.

Slide 35 - Slide 35

Slide notes

The system will compute the minimum required hardware for the ZAB based on the number of users that will be authenticating through the ZAB. Type the number of users and click **Compute**.

Slide 36 - Slide 36
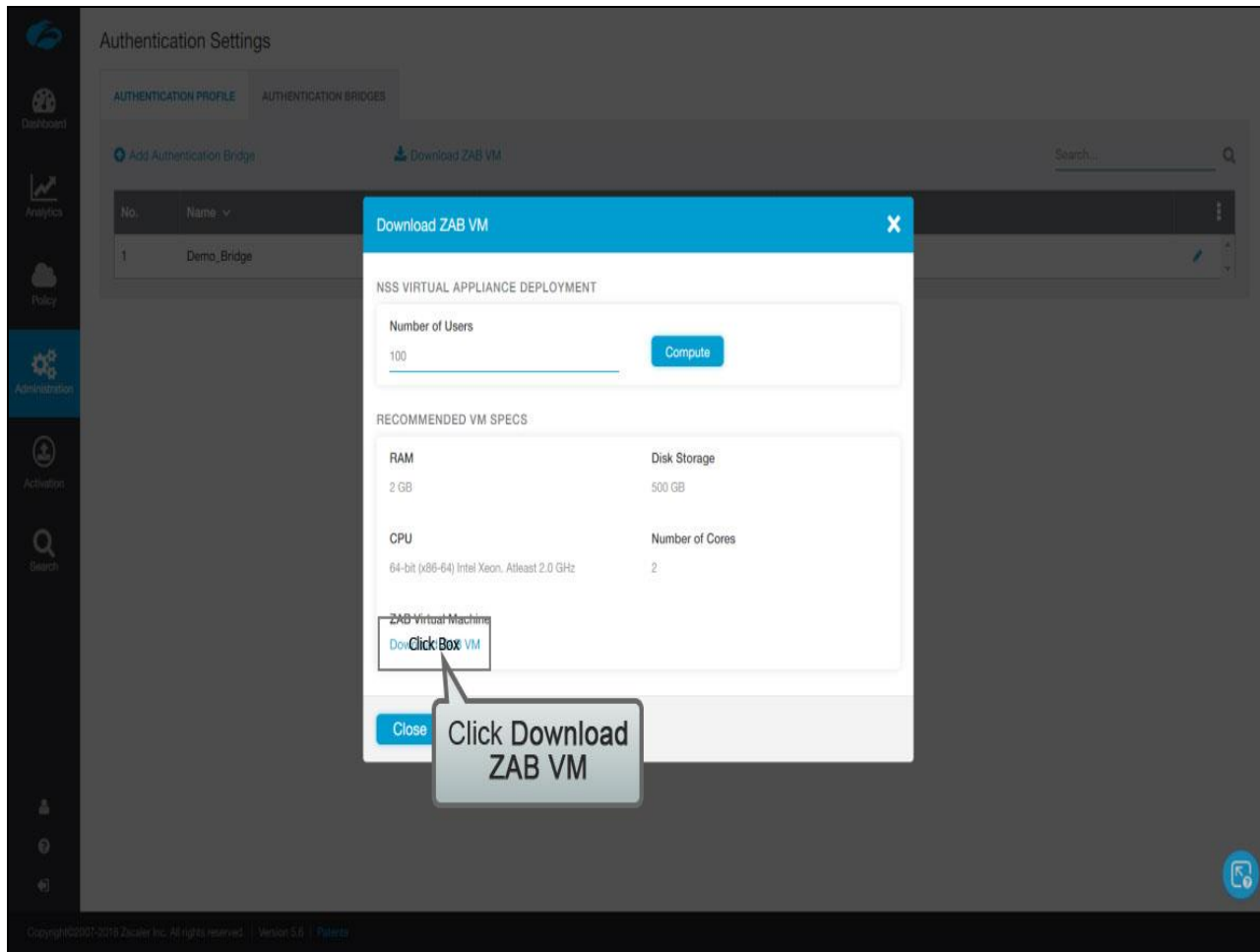
Slide notes

Just beneath the heading **ZAB Virtual Machine**, click **Download ZAB VM**.

Slide 37 - Slide 37

Slide notes

Slide 38 - Slide 38
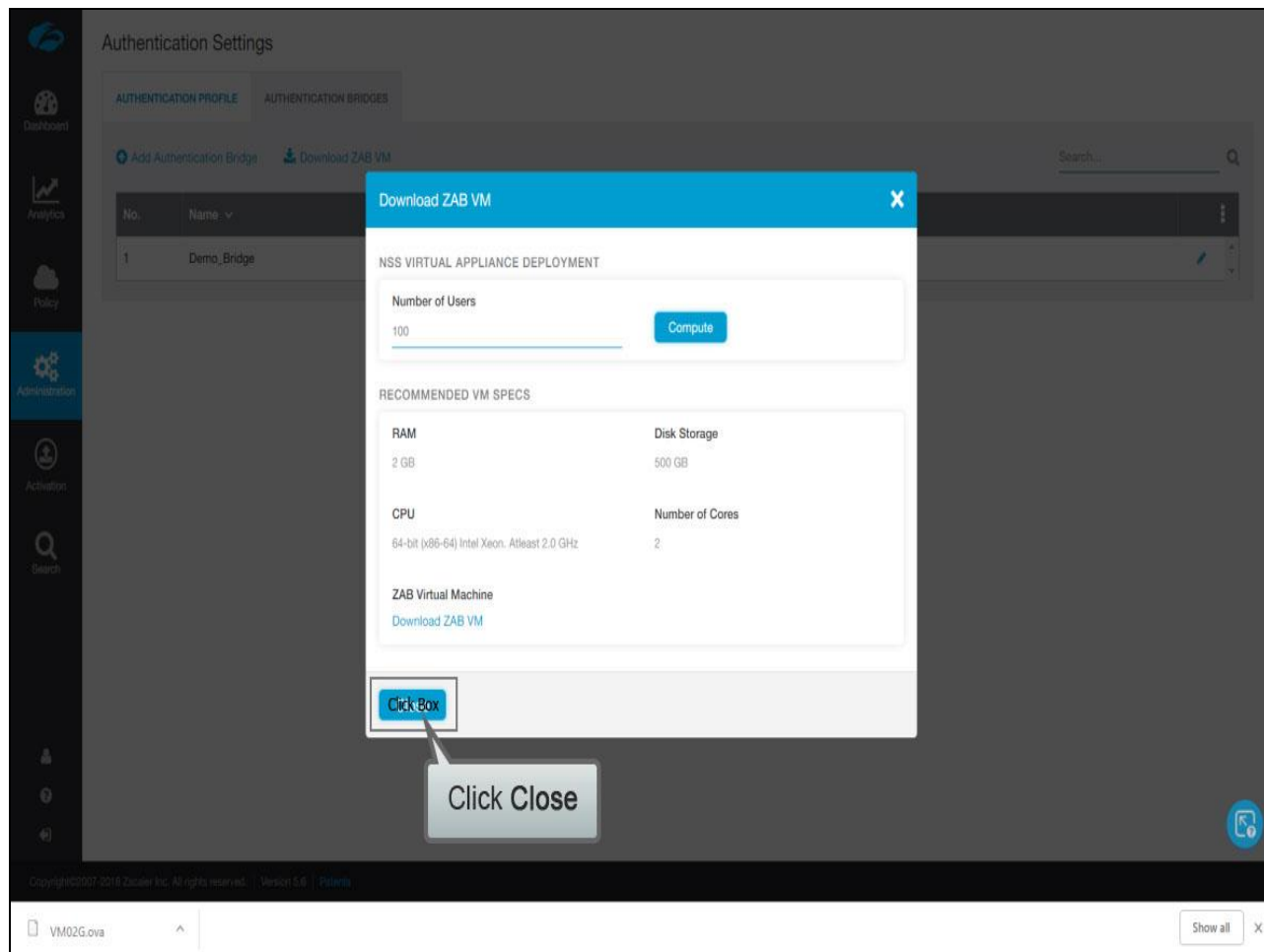
Slide notes

And save the file. The file is approximately 475MB. Next, you will launch the ZAB VM in VMWare ESXi which is required for production environments or, for testing purposes, you can use VM Player. Loading and launching the .ova file will not be part of the demonstration. We will now move on into configuring the ZAB once started.

Slide 39 - Slide 39

Slide notes

Slide 40 - Slide 40

Slide notes

1. Now let's take a look at configuring the ZAB. For the demo I've already installed and launched the ZAB VM in Workstation; however, for production environments you want to launch this in VM ESXi. Let's go ahead and log in using the login of **zsroot** and password of **zsroot**. Next, switch to **superuser** by typing the command **sudo su** and login in with **zsroot**. Now we want to configure our network settings by typing the command **zab configure**.

2. Enter the IP address of the name server. For the purpose of the demo we will use Google. No, I don't want to add a secondary name server for this demo. Enter the IP address of the ZAB itself. And the default gateway.

3. Type **zab dump-config** to verify your settings. And you can see we have the name server, the IP address, and the default route configured. And you do see **CloudName: Failed to read SSL Certificate**. We have not installed an SSL certificate and at this point you want to use Secure Copy to copy the client certificate, that you downloaded previously from the Zscaler Admin Portal, and copy that into the VM. Won't do that as part of the demo for time savings.

4. To install the certificate, type the command **zab install-client-cert** then provide the path and the filename. Again, type **zab dump-config** to verify the certificate is installed and recognizes the right cloud. And now you see the cloud is recognized as **zscalertwo** and it also displays our company ID. The company ID is what you can find in the Admin Portal under **Administration** then **Company Profile**.

5. Next, install the server cert by typing **zab install-server-cert**. This cert can be obtained from a Certificate Authority or be self-signed. For the demo we will use a self-signed cert. Simply hit **Enter** to generate that self-signed certificate. Enter your **domain name** and enter a **passphrase** for generating the certificate - this can be anything you like.

6. Type **zab update-now** to download and install the current build. This is only required during the initial installation. Start the ZAB by typing **zab start**. Enable auto-start by typing **zab enable-autostart**. And verify the ZAB is running by typing **zab status** and you can see that the service is running.

7. Next, we want to verify that the ZAB has initiated an outbound connection to both the Zscaler service and your Active Directory server by typing the command **sockstat**. You can see we have established two connections to the Zscaler service. This is a persistent outbound tunnel and we have also established a connection to our Active Directory server.

8. Another helpful diagnostic command is **zab test-firewall** which ensures that the ZAB has connectivity to all necessary services. Additionally, if you encounter any trouble you can allow remote access to Zscaler TAC for remote diagnostics. There are two commands you can run. The first is **zab enable-remote-debugging**. And another command allows SSH access to your ZAB by typing **zab support-access-start**.

9. Lastly, there is a command called **zab collect-diagnostics** which will automatically collect all the required logs and put them in a .zip file that you can then use Secure Copy to copy the file off and send to TAC. And now that diagnostics have completed you can see the path to the file that he ZAB generated.

10. And this concludes our configuration demonstration of the ZAB. We will now move back to the Zscaler Admin Portal to finish off our configuration there.

Slide 41 - Slide 41
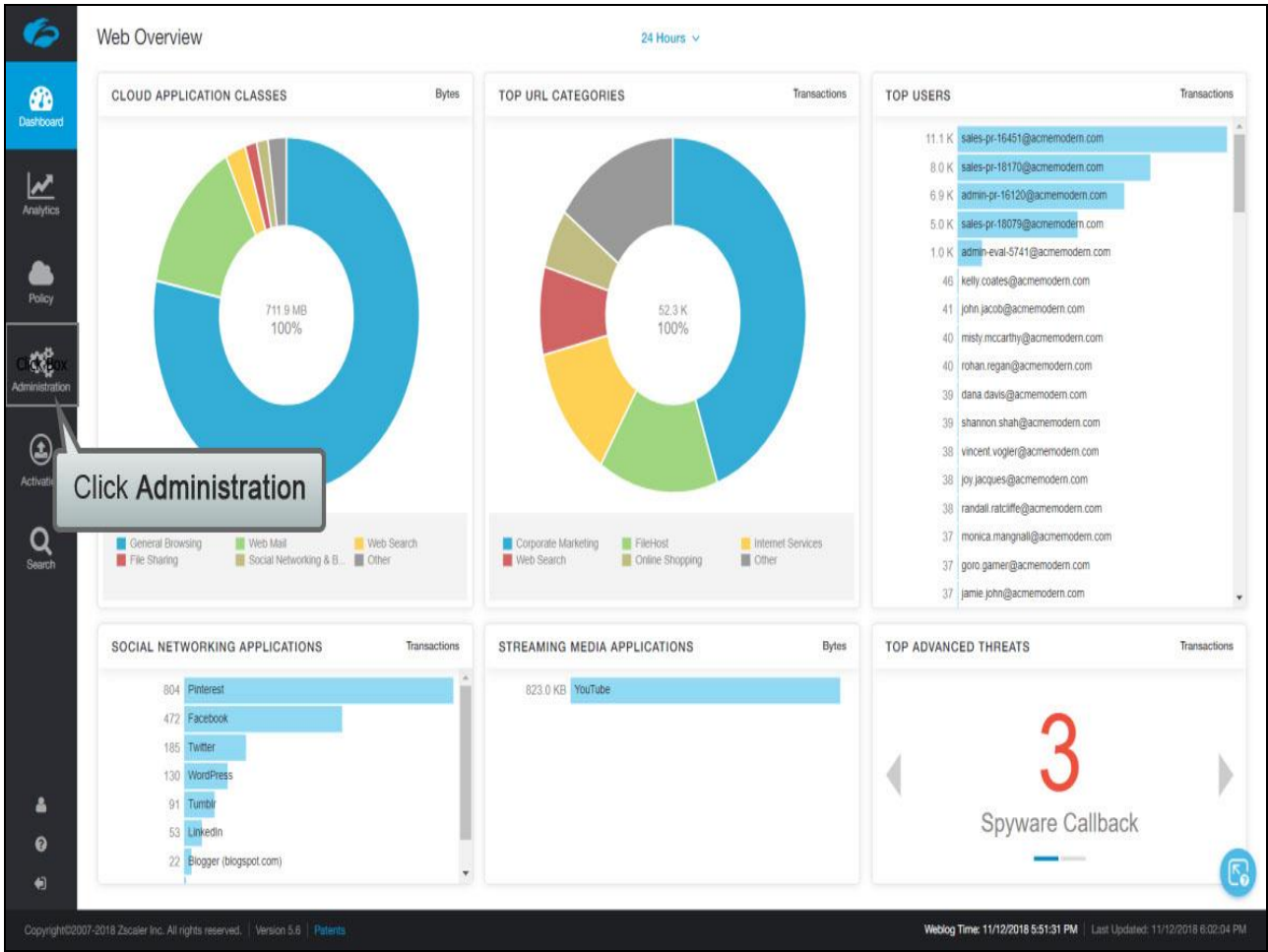
Slide notes

Begin in the Zscaler Admin Portal by going to **Administration**, …

Slide 42 - Slide 42
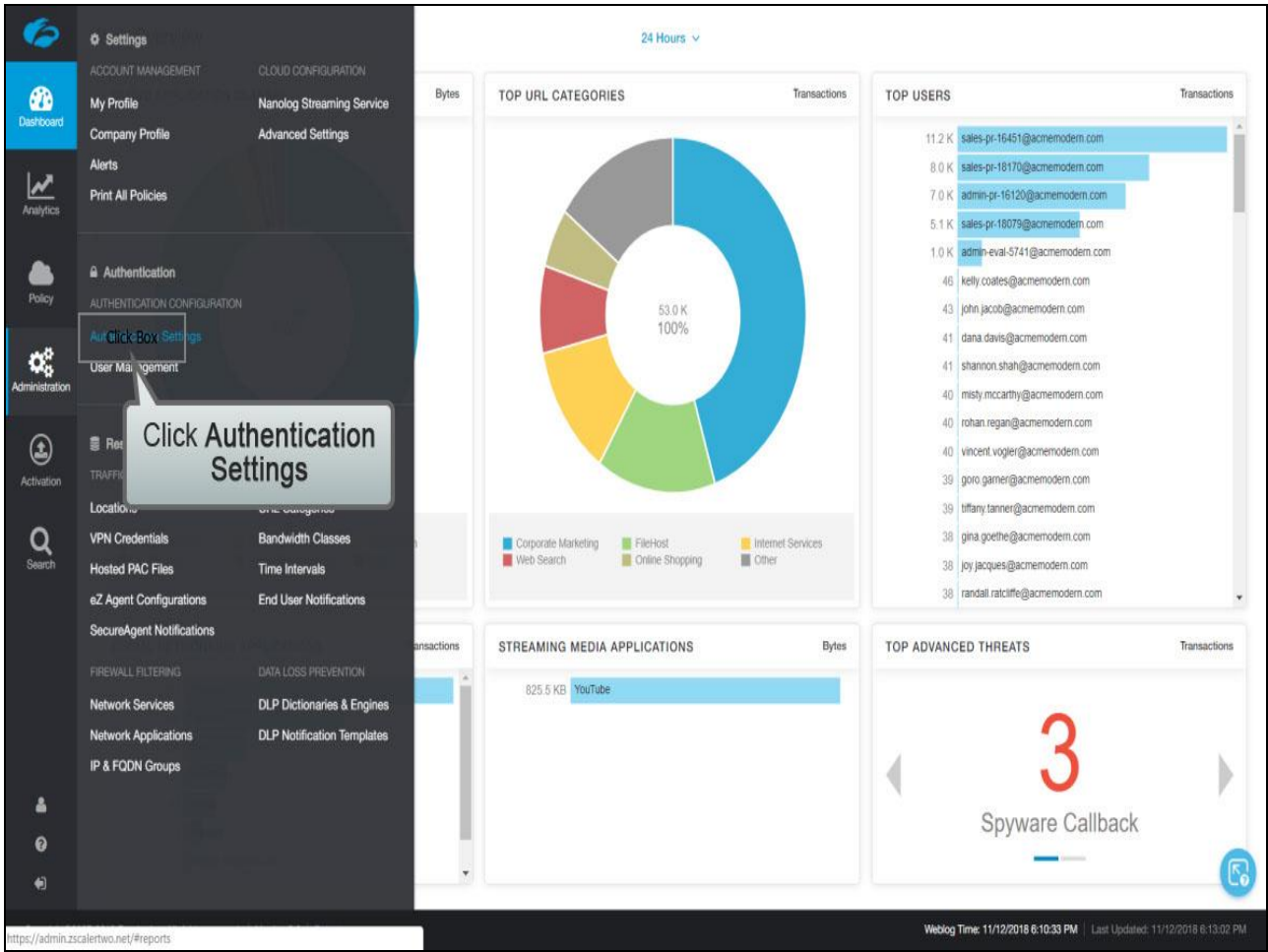
Slide notes

…then **Authentication Settings**.

Slide 43 - Slide 43
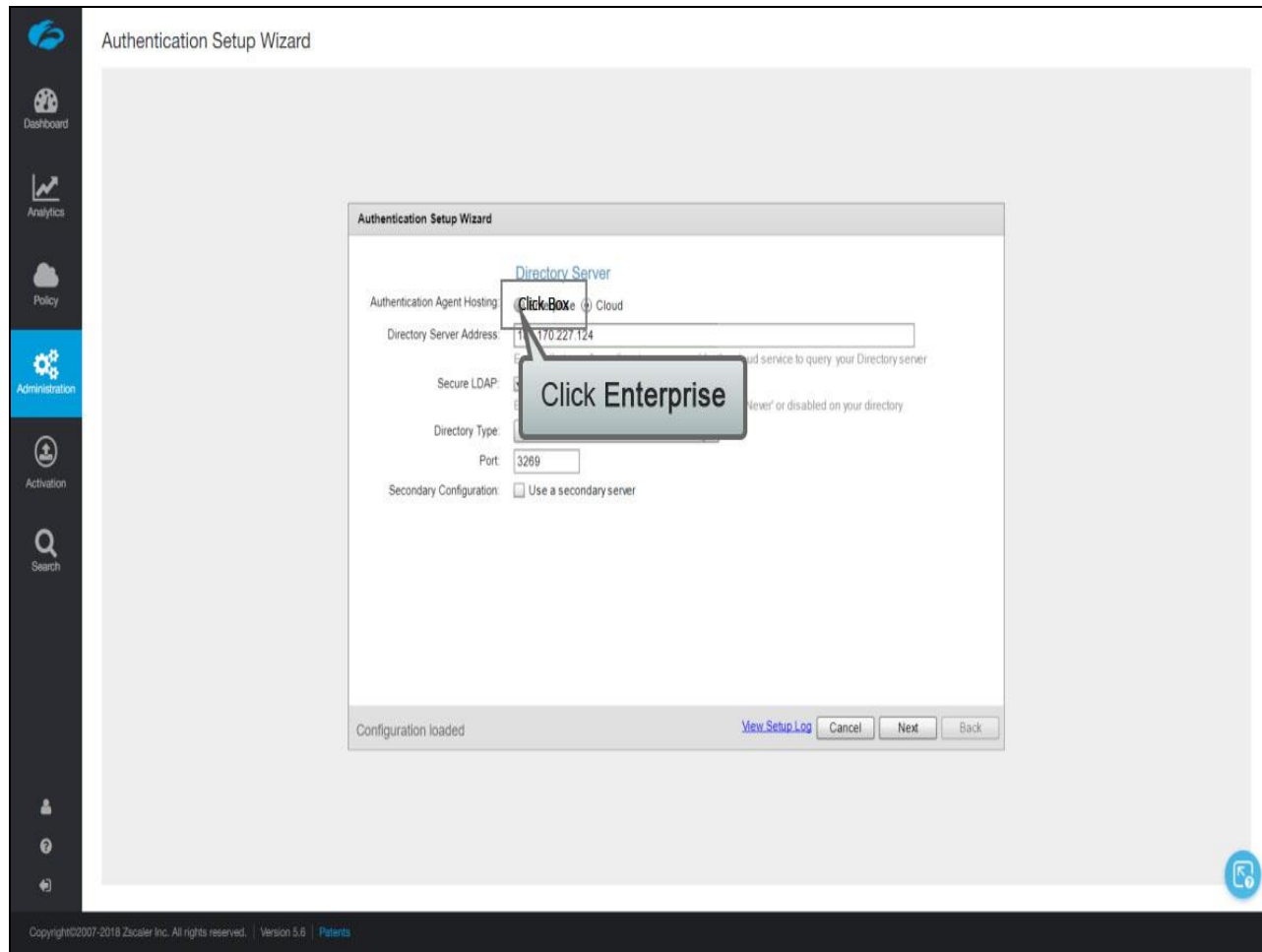

Slide notes

And run the **Setup Wizard**.

Slide 44 - Slide 44

Slide notes

For **Authentication Agent Hosting** select **Enterprise**. This tells Zscaler to talk to the ZAB instead of talking directly to your Active Directory server.

Slide 45 - Slide 45

Slide notes

Then click **Next**.

Slide 46 - Slide 46

Slide notes

We are going to skip some of these settings as the Setup Wizard was discussed in detail in the Active Directory eLearning module. The settings you see reflect what we configured during the Active Directory module.

Slide 47 - Slide 47
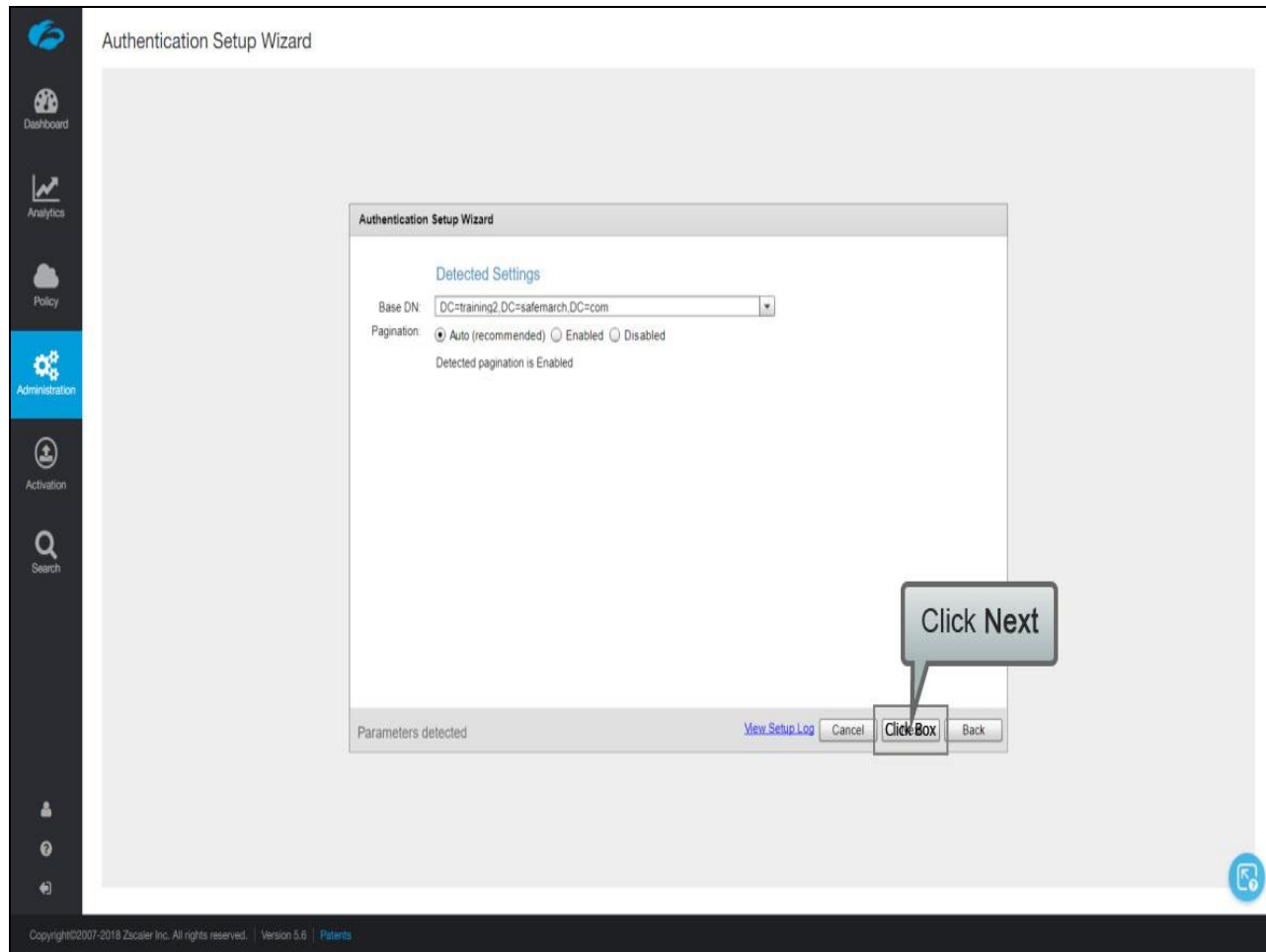
Slide notes

Slide 48 - Slide 48

Slide notes

Slide 49 - Slide 49

Slide notes

Slide 50 - Slide 50

Slide notes

For **Authentication Agent Address**, type in the host name of your ZAB then click **Next**.

Slide 51 - Slide 51
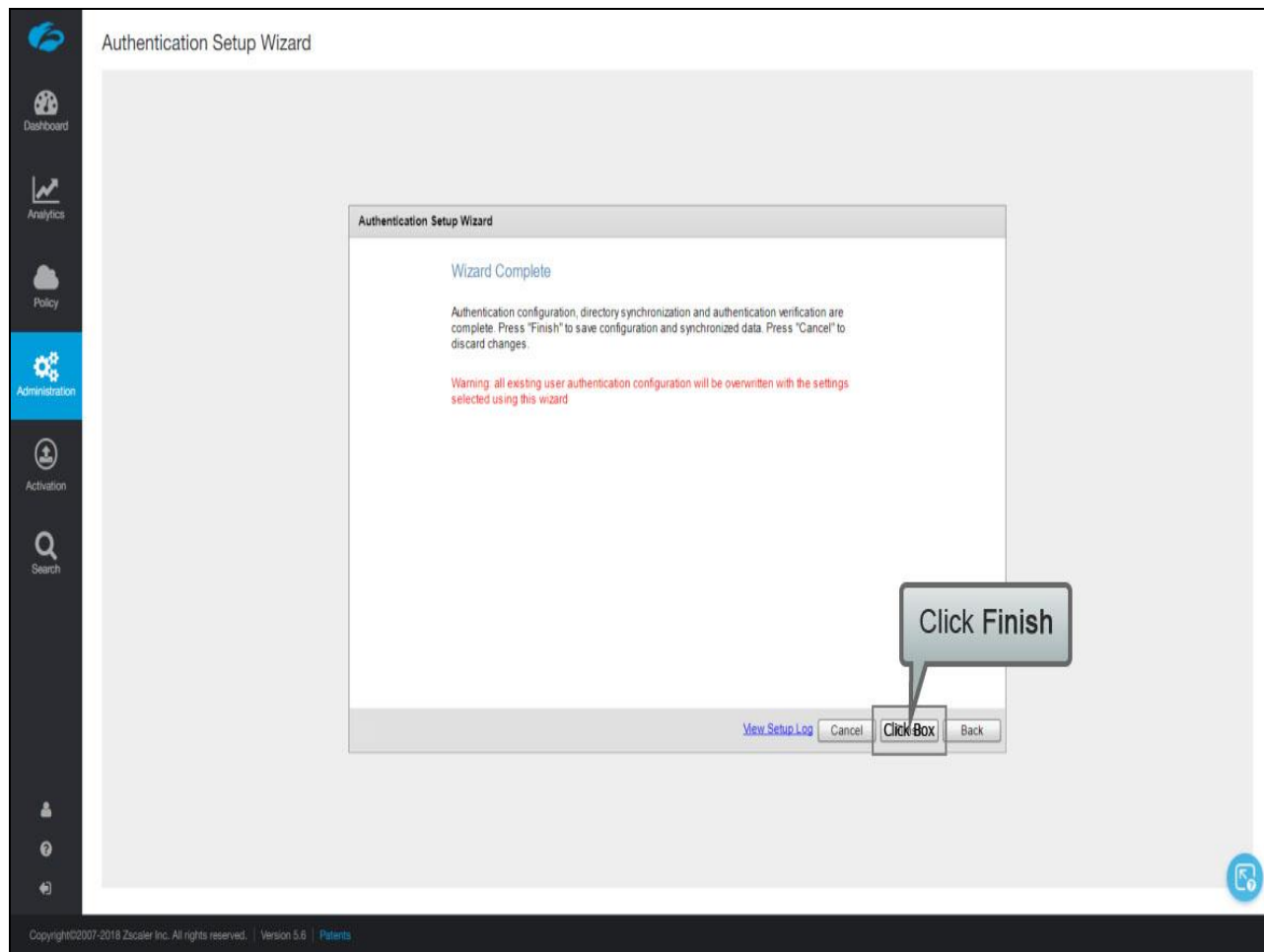
Slide notes

Then close the Setup Wizard by clicking **Finish**.

Slide 52 - Slide 52

Slide notes

Then **Activate** your changes.

Slide 53 - Slide 53
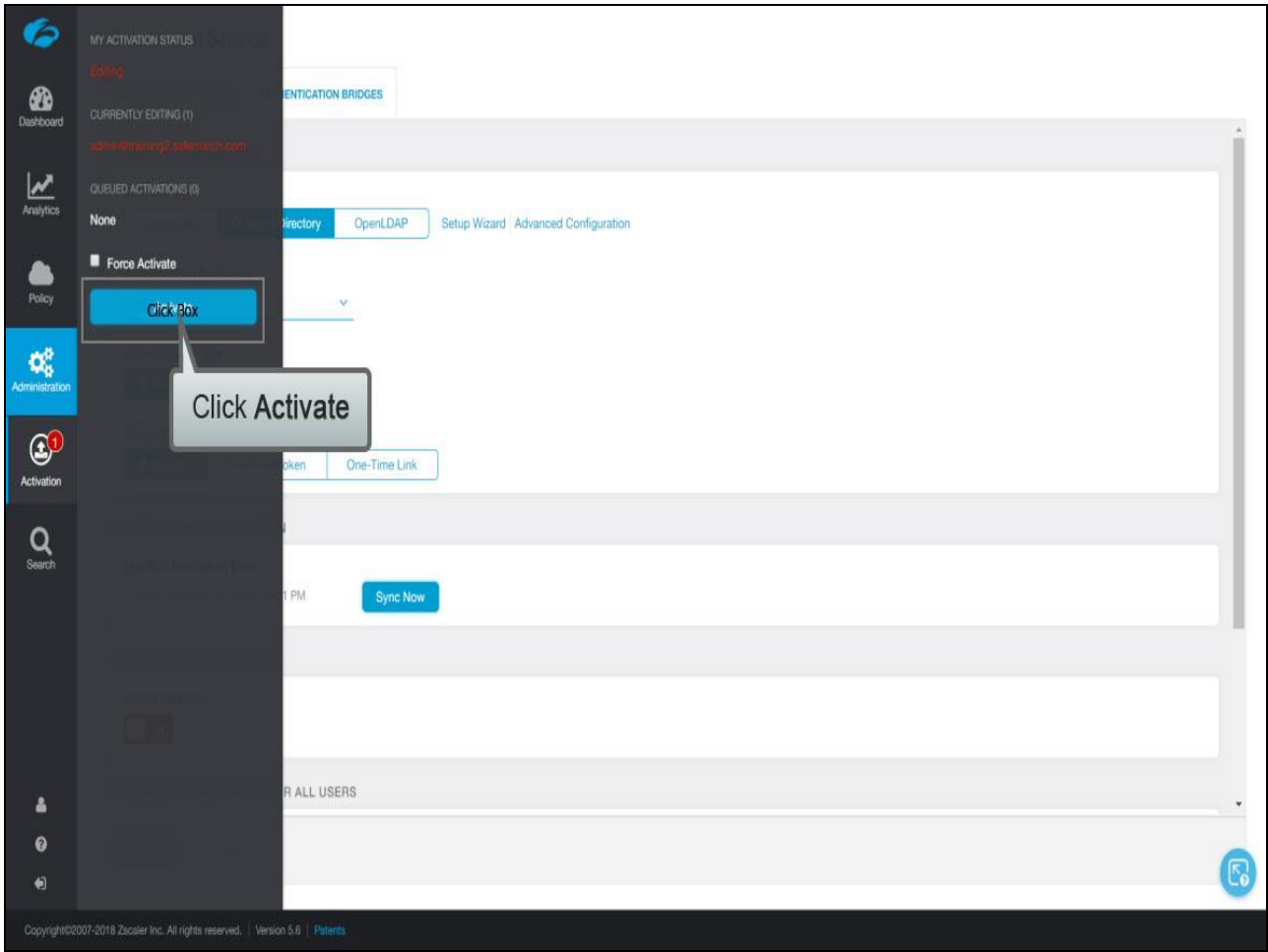
Slide notes

Slide 54 - Slide 54
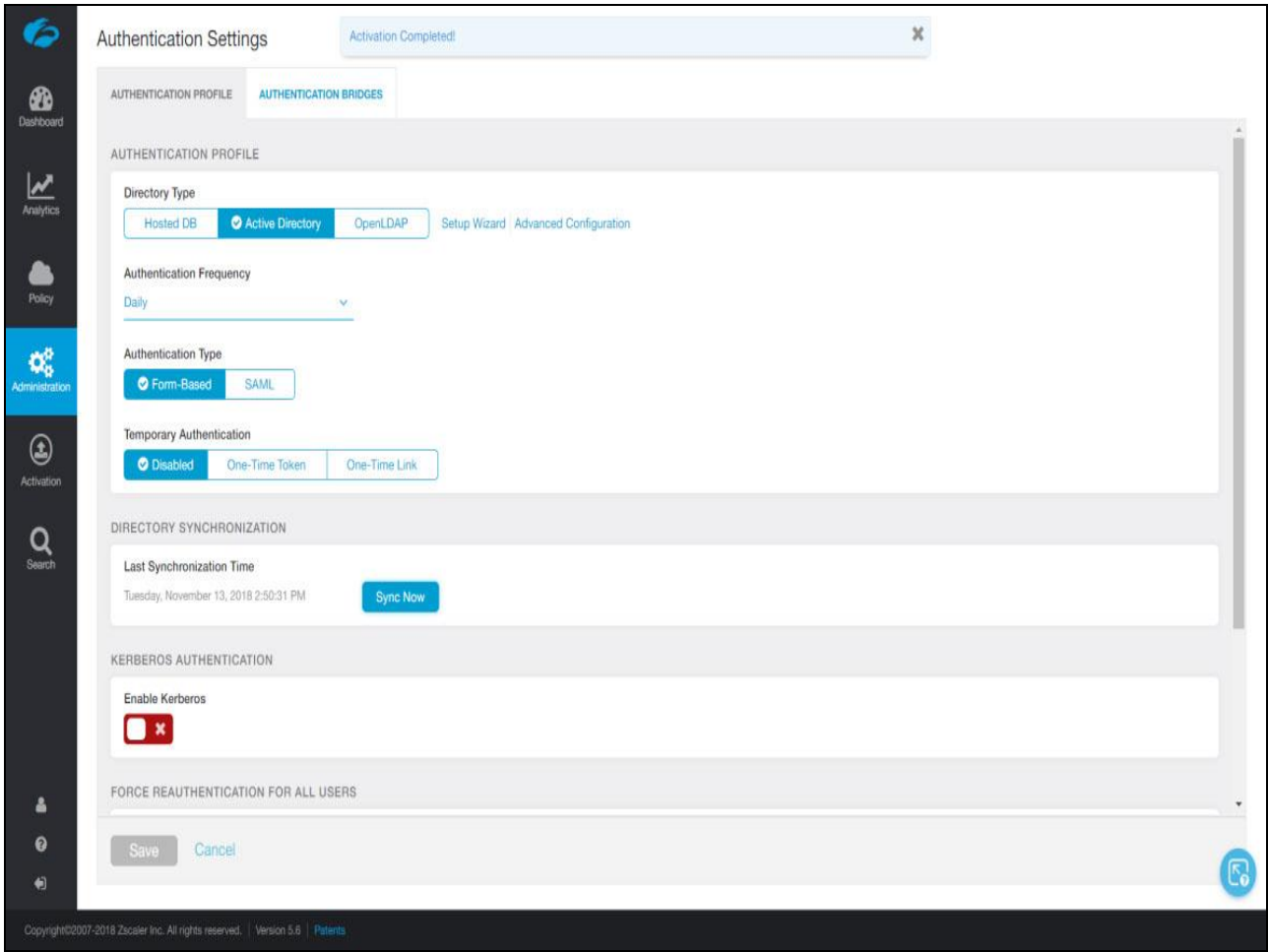
Slide notes

Slide 55 - Slide 55

Slide notes

Slide 56 - Troubleshooting
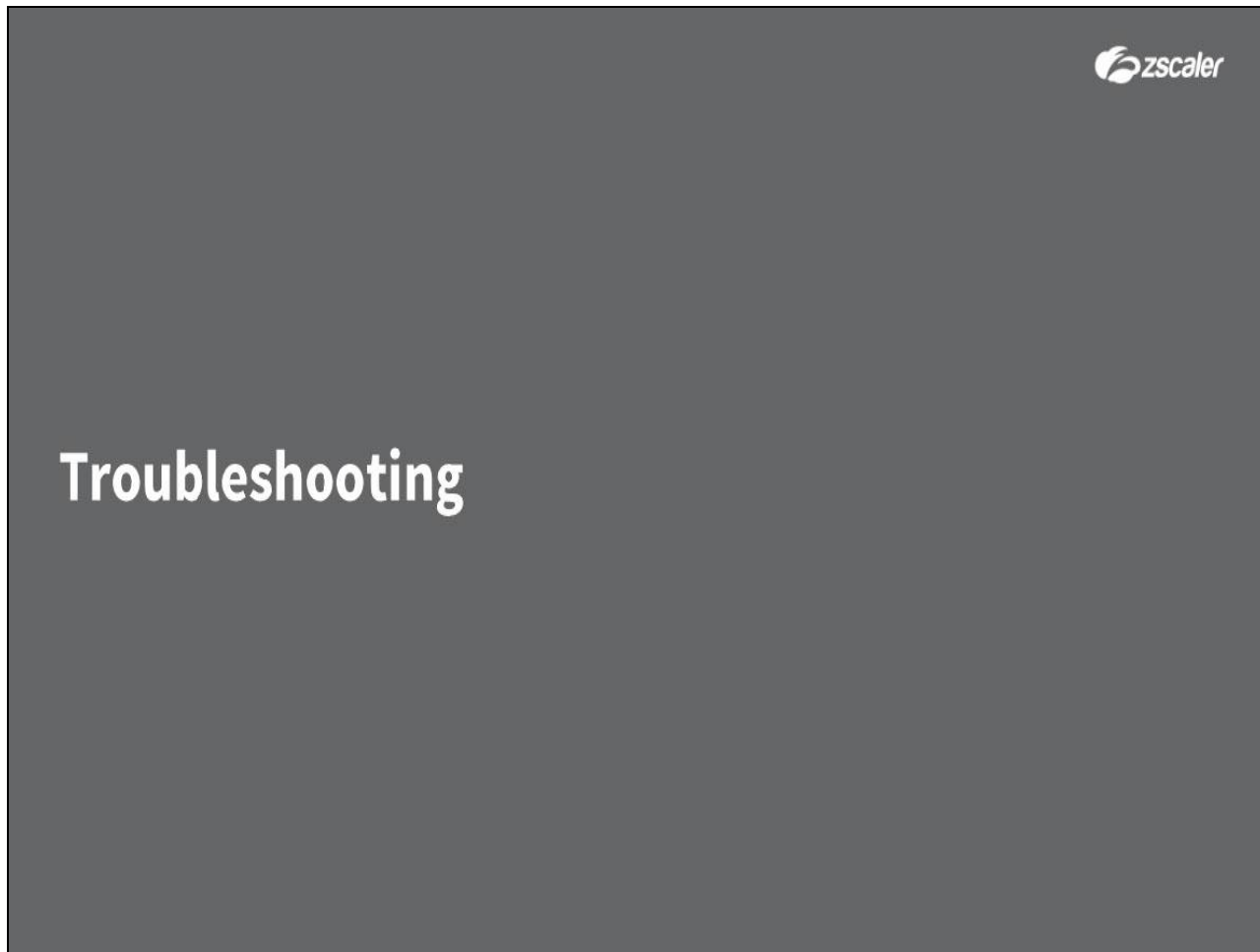
Slide notes

You have already seen the ZAB troubleshooting tools as part of the interactive demo but let's do a quick recap as a refresher.

Slide 57 - Troubleshooting on the ZAB CLI

Slide notes

There are only a few troubleshooting commands needed for the ZAB. These are as follows: **zab status** - this should show that the process is running;

Slide 58 - Troubleshooting on the ZAB CLI

Slide notes

zab test-firewall - which runs a script to test outbound firewall access;

Slide 59 - Troubleshooting on the ZAB CLI

Slide notes

zab collect-diagnostics - this automatically collects all the relevant log files and config files and places them in a .zip file which you can copy off, via Secure Copy, and provide to Technical Support;

Slide 60 - Troubleshooting on the ZAB CLI

Slide notes

zab enable-remote-debugging - allows Zscaler Support to run a limited set of commands from the Cloud for debugging (this is disabled by default and must be enabled by the user);

Slide 61 - Troubleshooting on the ZAB CLI

Slide notes

zab support-access-start - allows Zscaler support to SSH log into the VM for remote assistance (this is disabled by default and must be enabled by the user as well).
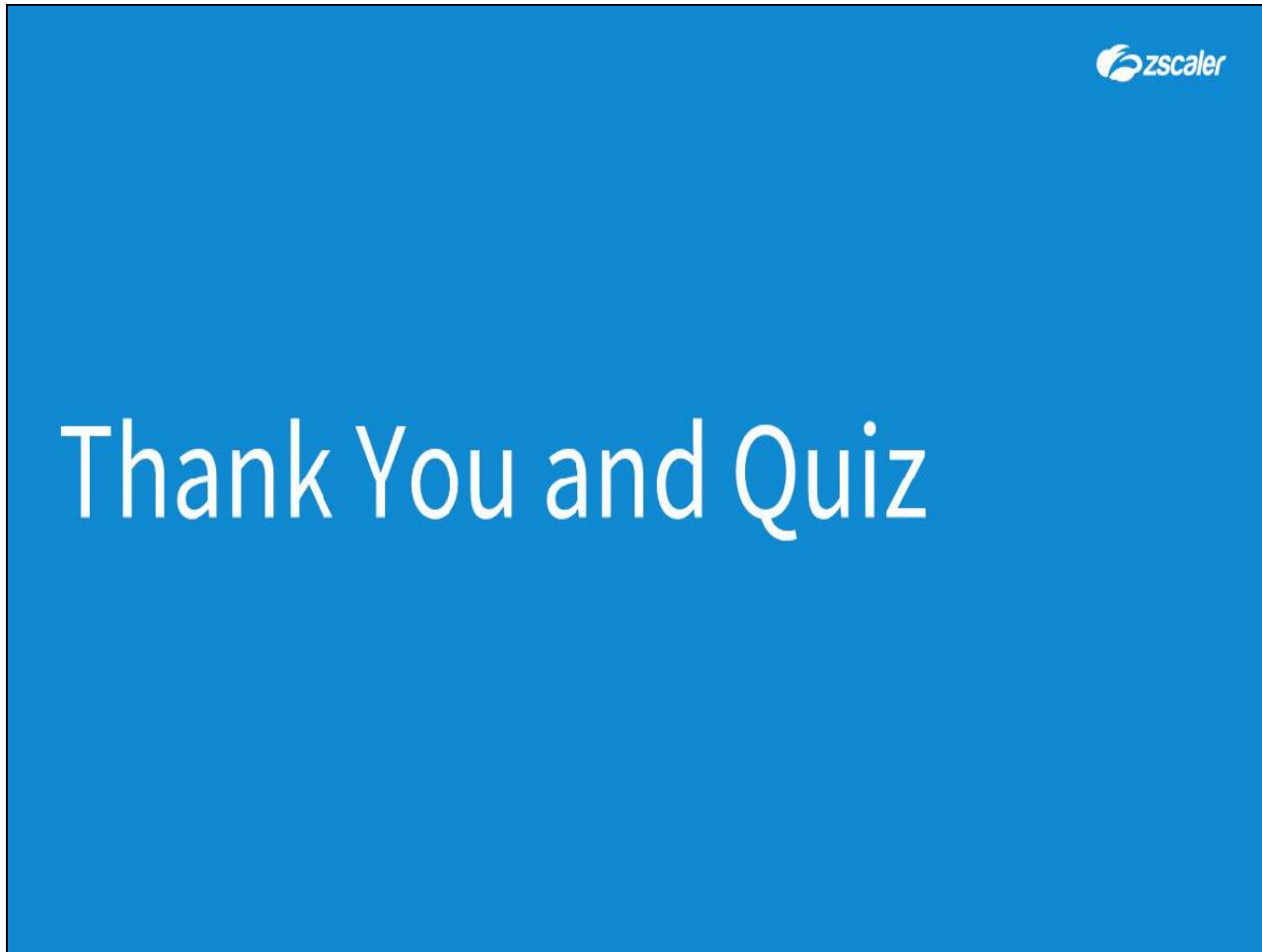
Slide 62 - Troubleshooting

Slide notes

The command **sockstat** will show open connections from the ZAB. This should show two connections to the Zscaler service and a connection to your Active Directory server.

Slide 63 - Thank You and Quiz

Slide notes

Thank you for participating in this eLearning module on configuring the Zscaler Authentication Bridge.

What will follow is a short quiz to test your knowledge. You can retake the quiz as many times as necessary to pass.