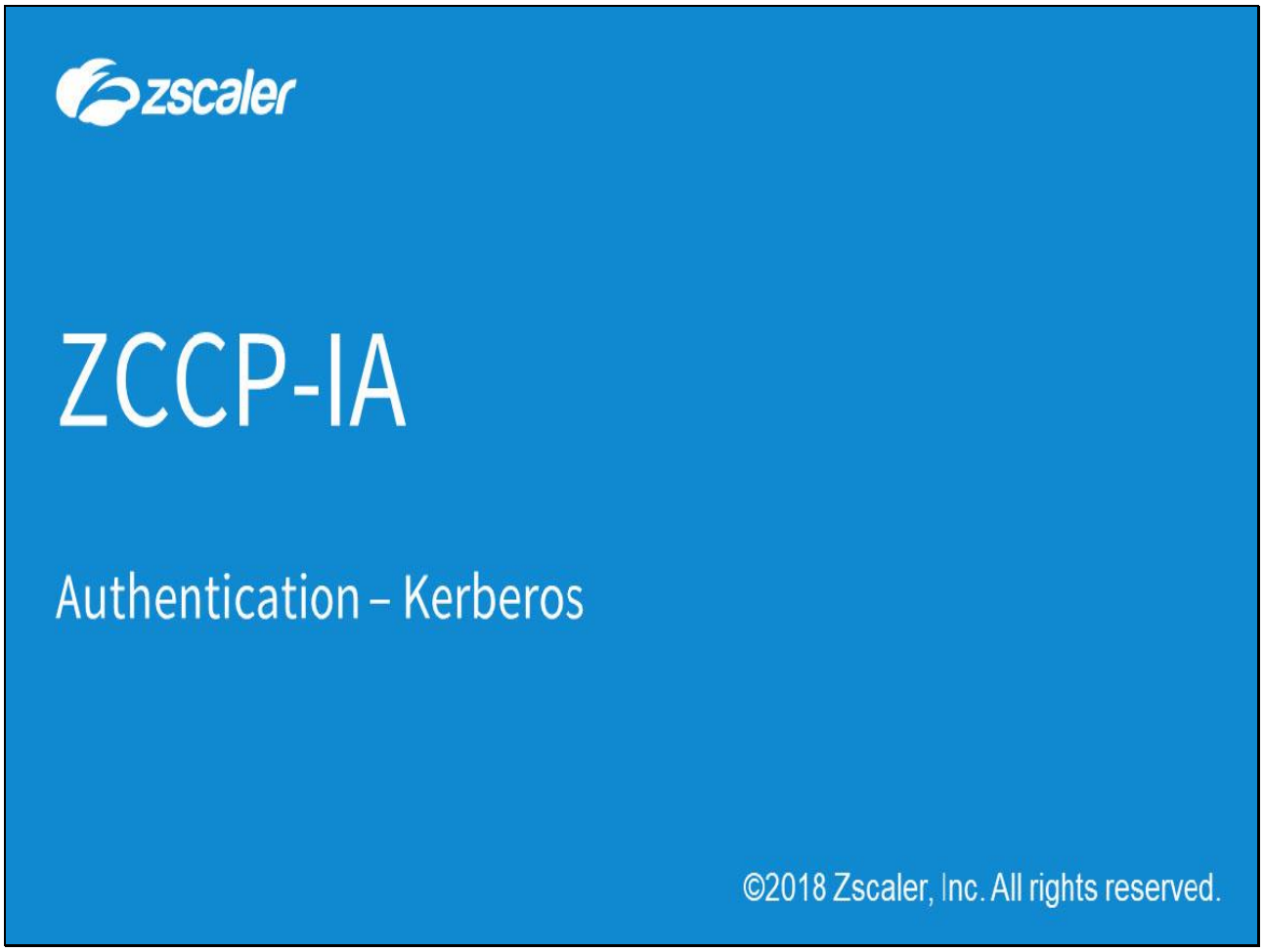
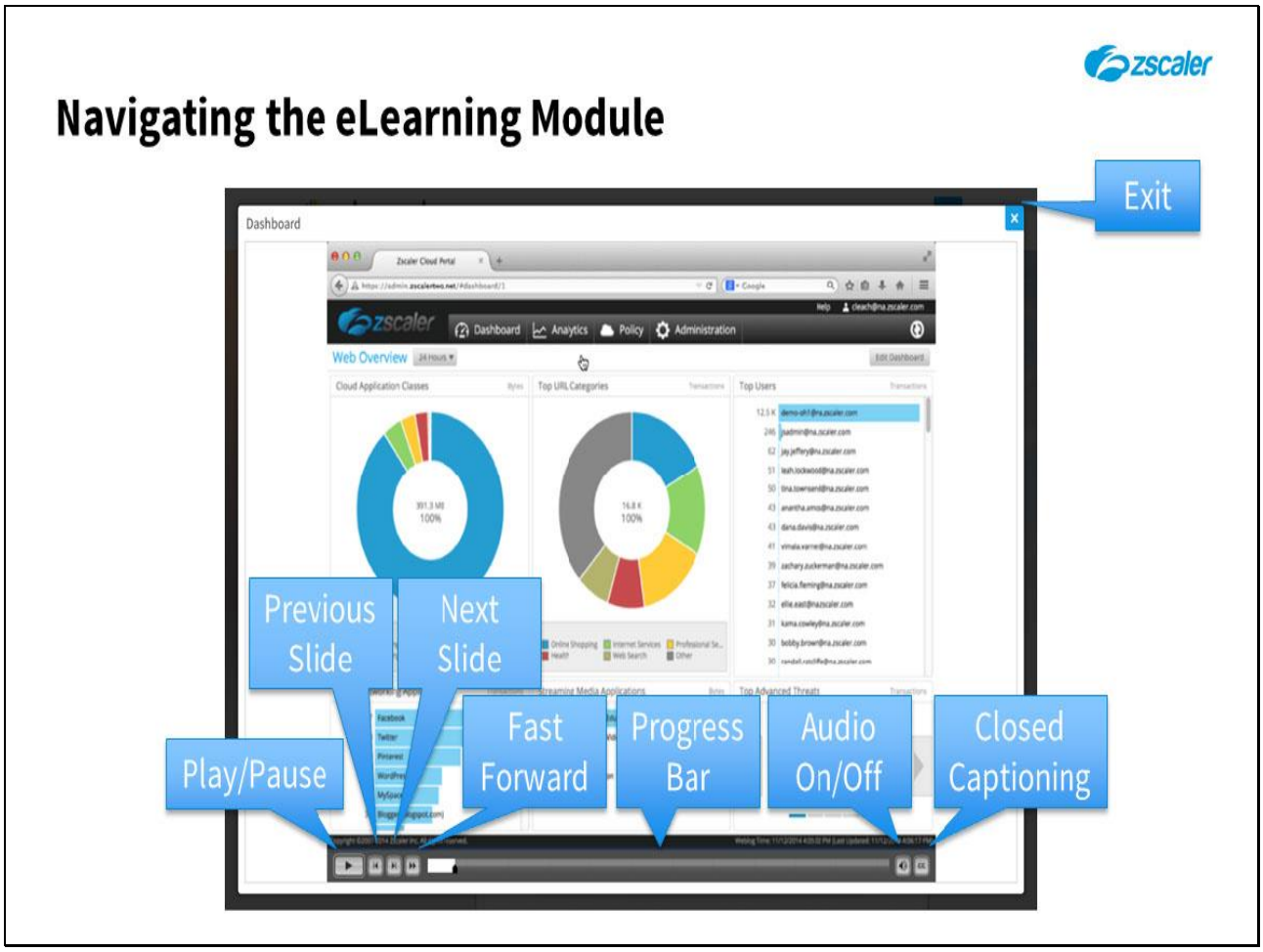
Slide 1 - ZCCP-IA



Slide notes

Thank you for viewing this elearning module on Kerberos Authentication with Zscaler.

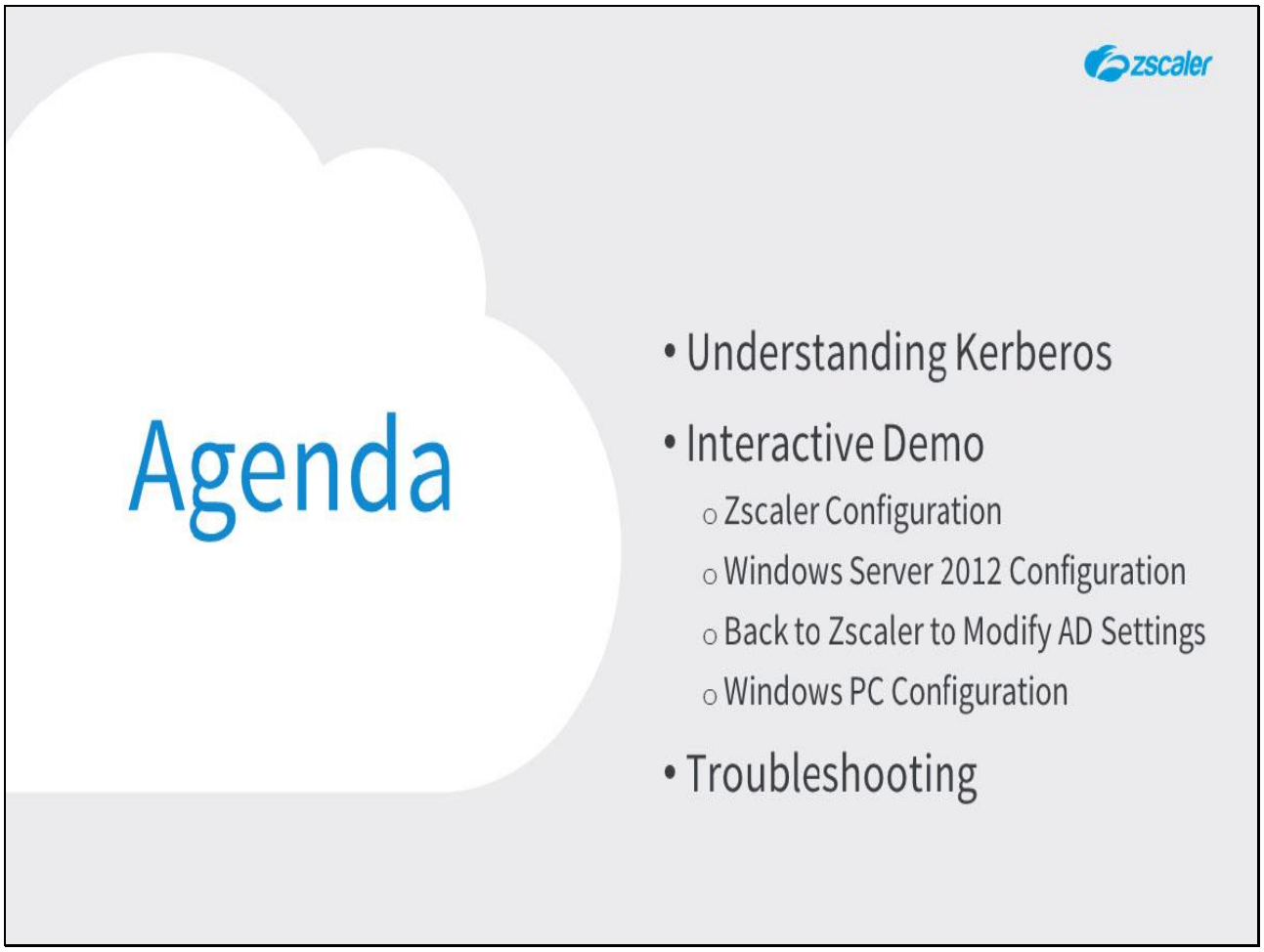
Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this eLearning module. There are various controls for playback including Play/Pause, Previous and 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 if you wish to exit.

Slide 3 - Agenda



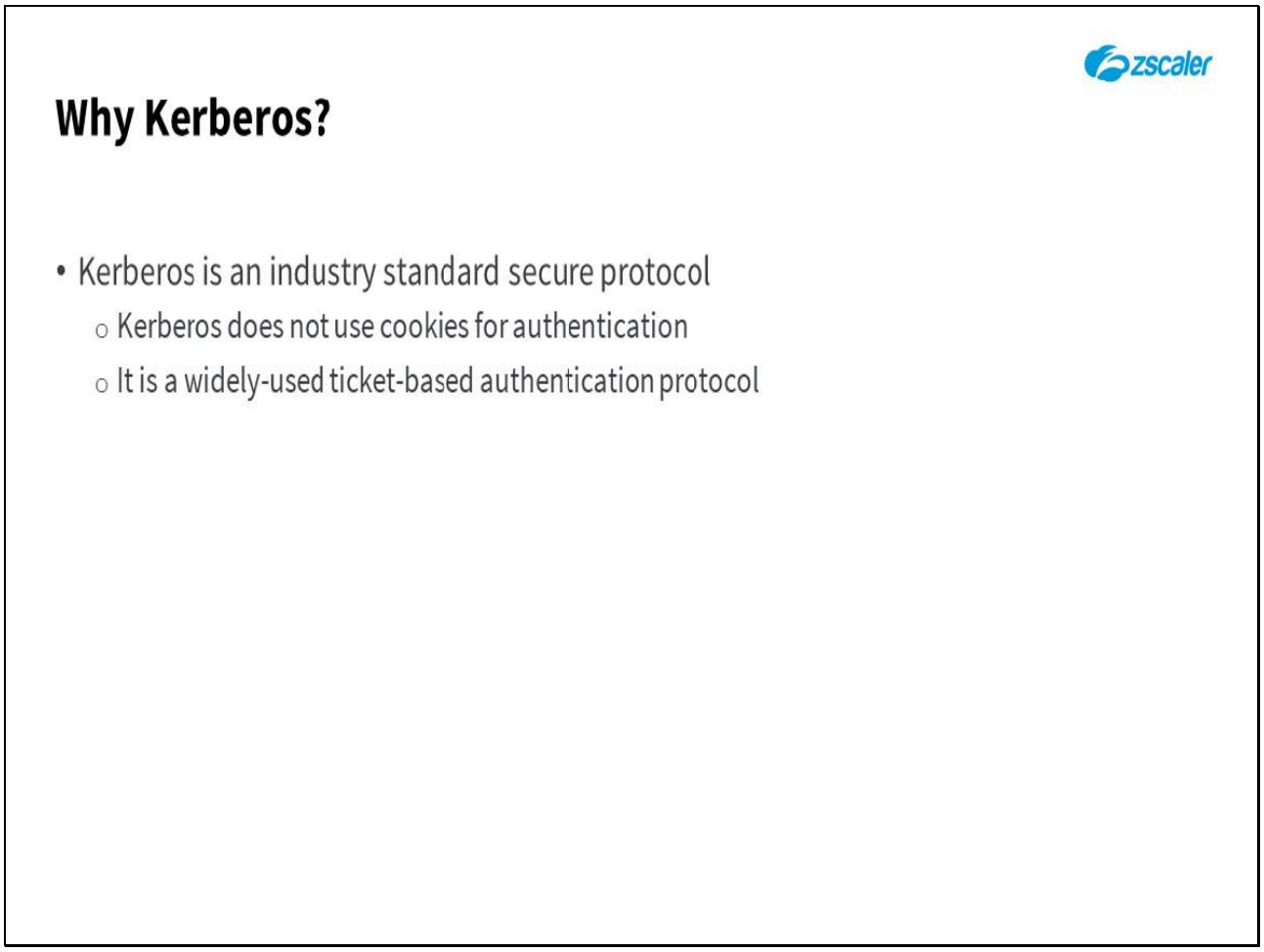
Slide notes

During this session we will look at use cases for Kerberos Authentication. We will look at the components of Kerberos and the authentication flow. We will also discuss user provisioning when using Kerberos, followed by an interactive configuration demonstration.

Slide 4 - Understanding Kerberos

Slide notes

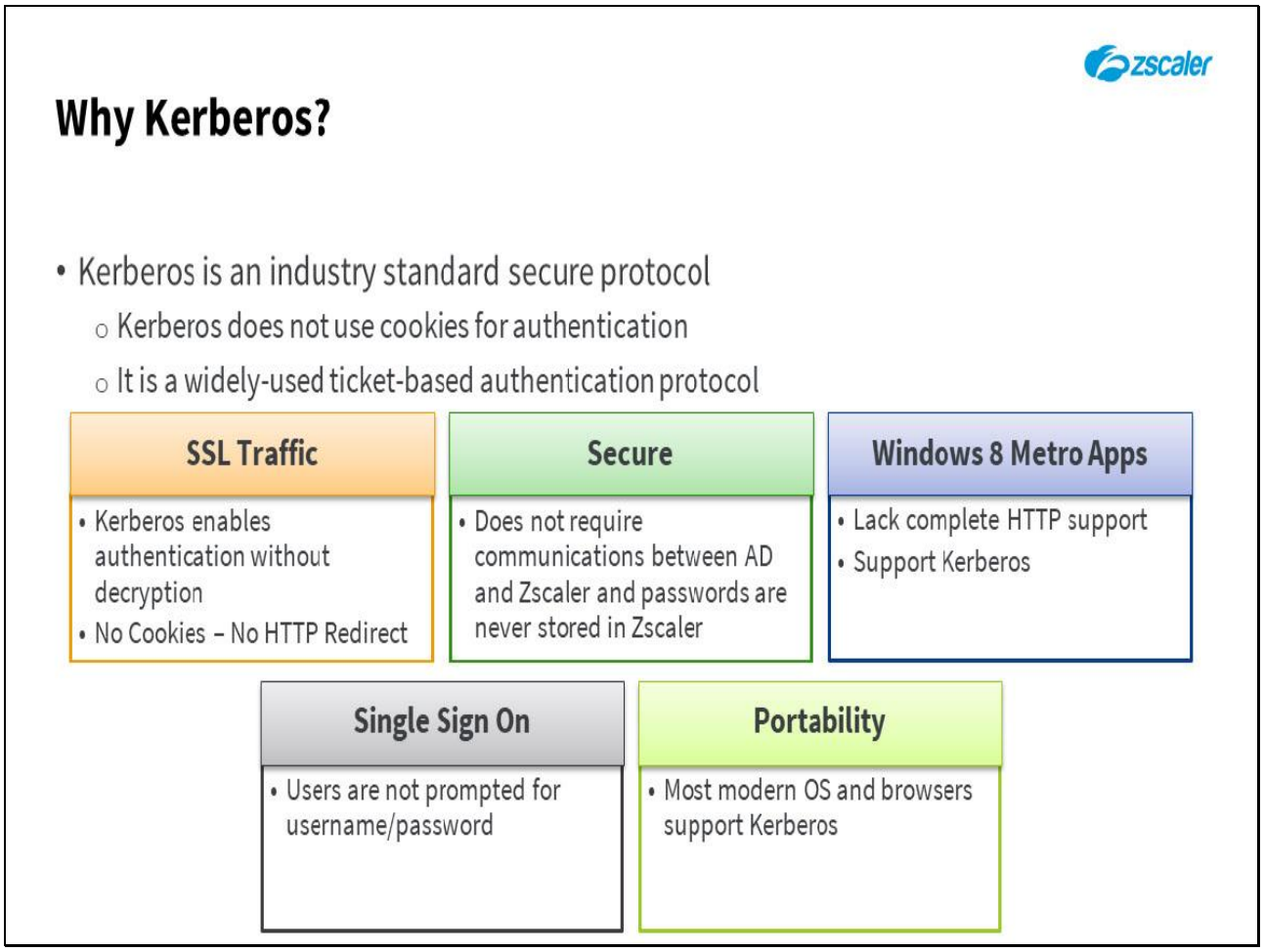
Slide 5 - Why Kerberos?



Slide notes

Zscaler supports authentication using Kerberos, an industry standard secure protocol. Unlike the other supported authentication mechanisms, Kerberos does not use cookies for authentication. It is a ticket-based authentication protocol that is widely used to authenticate users to network services.

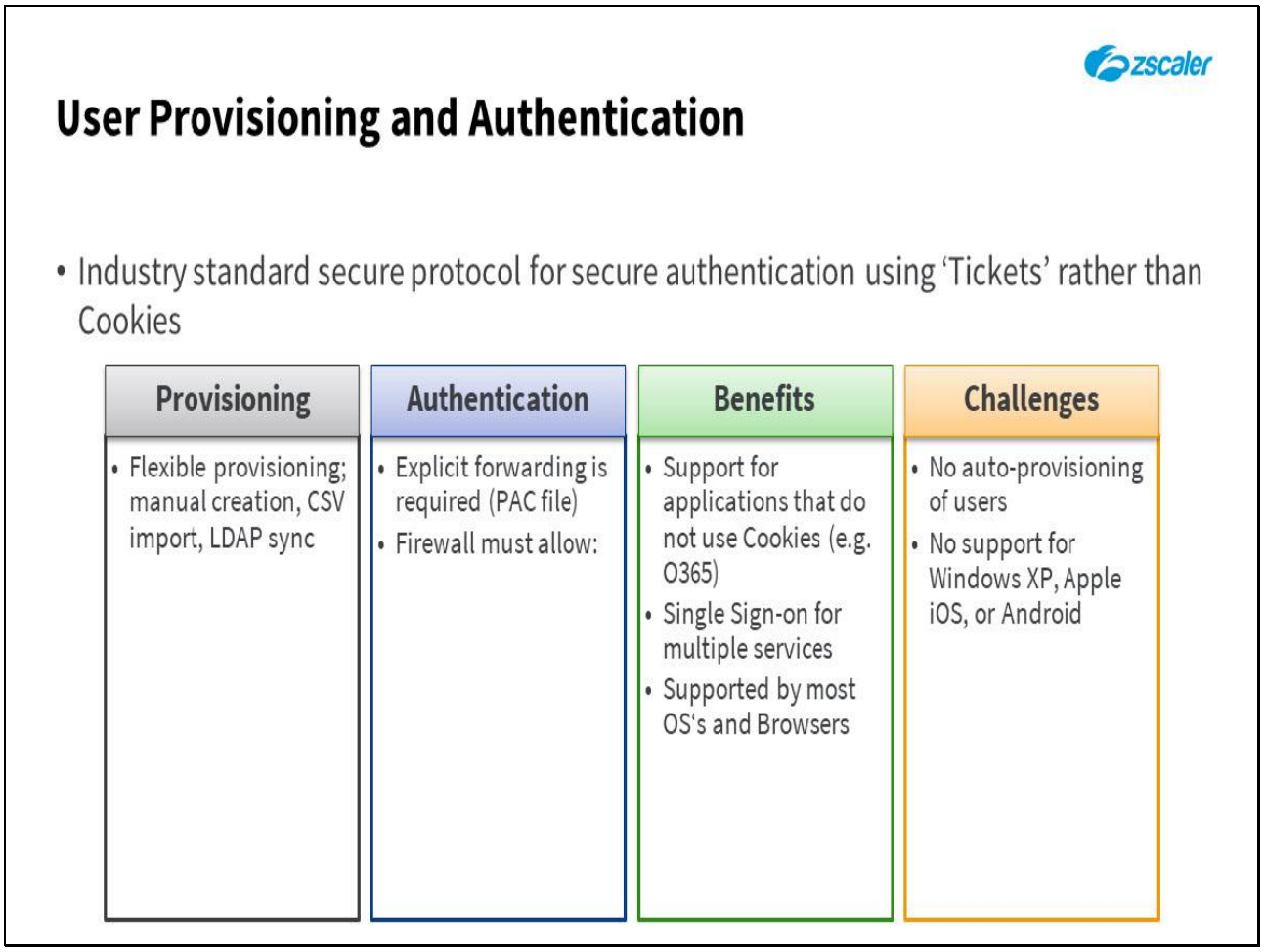
Slide 6 - Why Kerberos?



Slide notes

SSL traffic can be authenticated without decryption and there are no cookies or HTTP redirection as with other supported authentication methods. Kerberos provides support for Windows8 Metro apps and Office365. Kerberos provides a seamless user authentication experience - the user simply logs into their PC on the Windows domain then Kerberos authenticates the user to Zscaler with no user interaction. And most current operating systems and current browsers support Kerberos. Plus, it does not require any connectivity directly from Active Directory to Zscaler.

Slide 7 - User Provisioning and Authentication

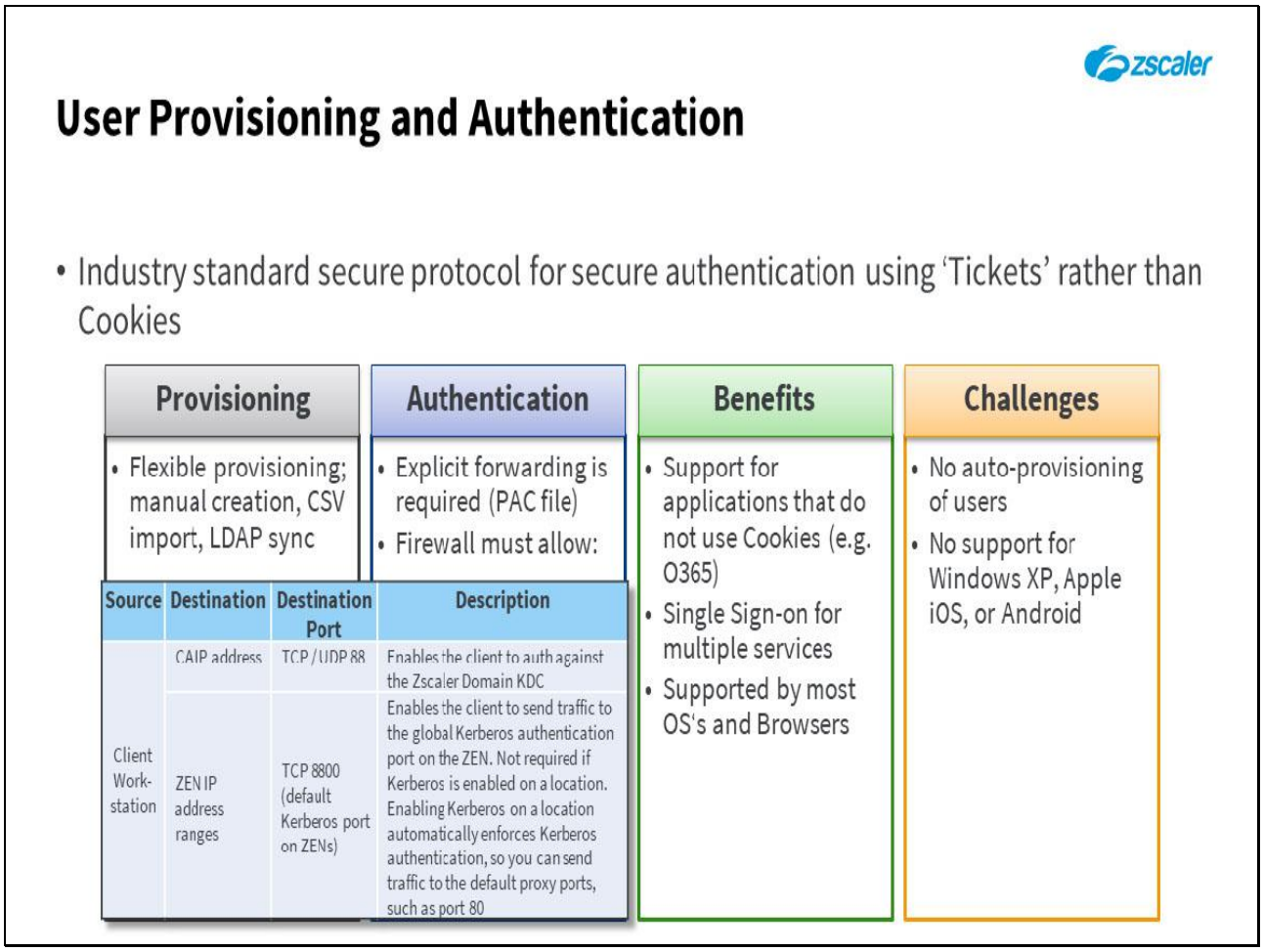


Slide notes

Kerberos provides for user authentication only. Unlike SAML there is no concept of user auto-provisioning or auto-sync as with Active directory. As such, Kerberos must be combined with one of the supported forms of user provisioning such as a manual CSV import as discussed in the Hosted DB training module, SAML auto-provisioning, Active directory sync, or the Zscaler Authentication bridge.

When using Kerberos authentication traffic to be authenticated by Kerberos must be forwarded in Explicit mode via a PAC file, which is covered in an earlier training module, or by manual proxy config in the browser. The use of the PAC file is considered to be best practice where the manual proxy config is a quick way to run a test or proof-of-concept.

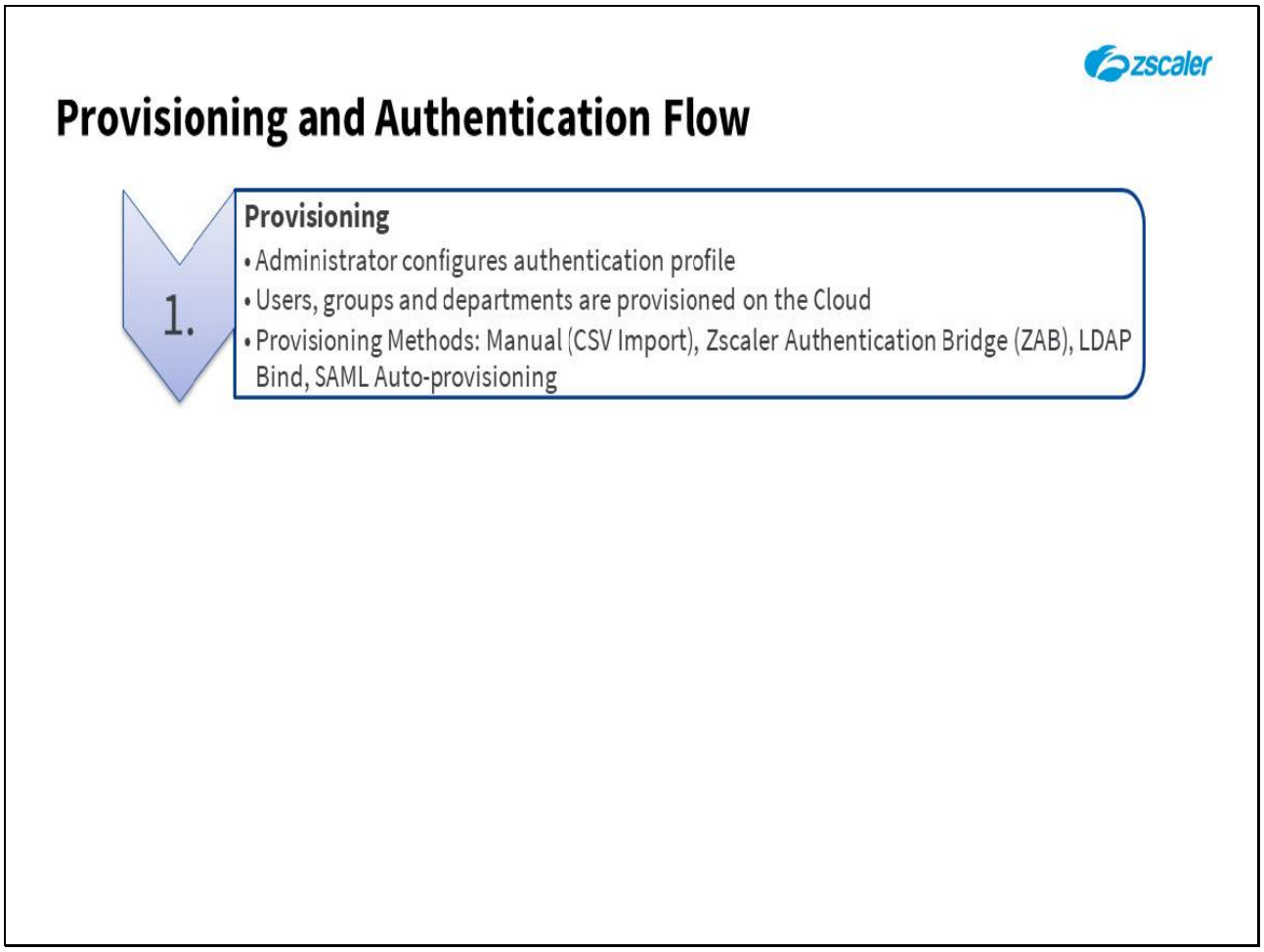
Slide 8 - User Provisioning and Authentication



Slide notes

As Zscaler does not need to talk directly to the Domain controller or Active directory there is no need to open inbound ports on your firewall. You only to ensure that the client workstation can open outbound connections to the Zscaler cloud.

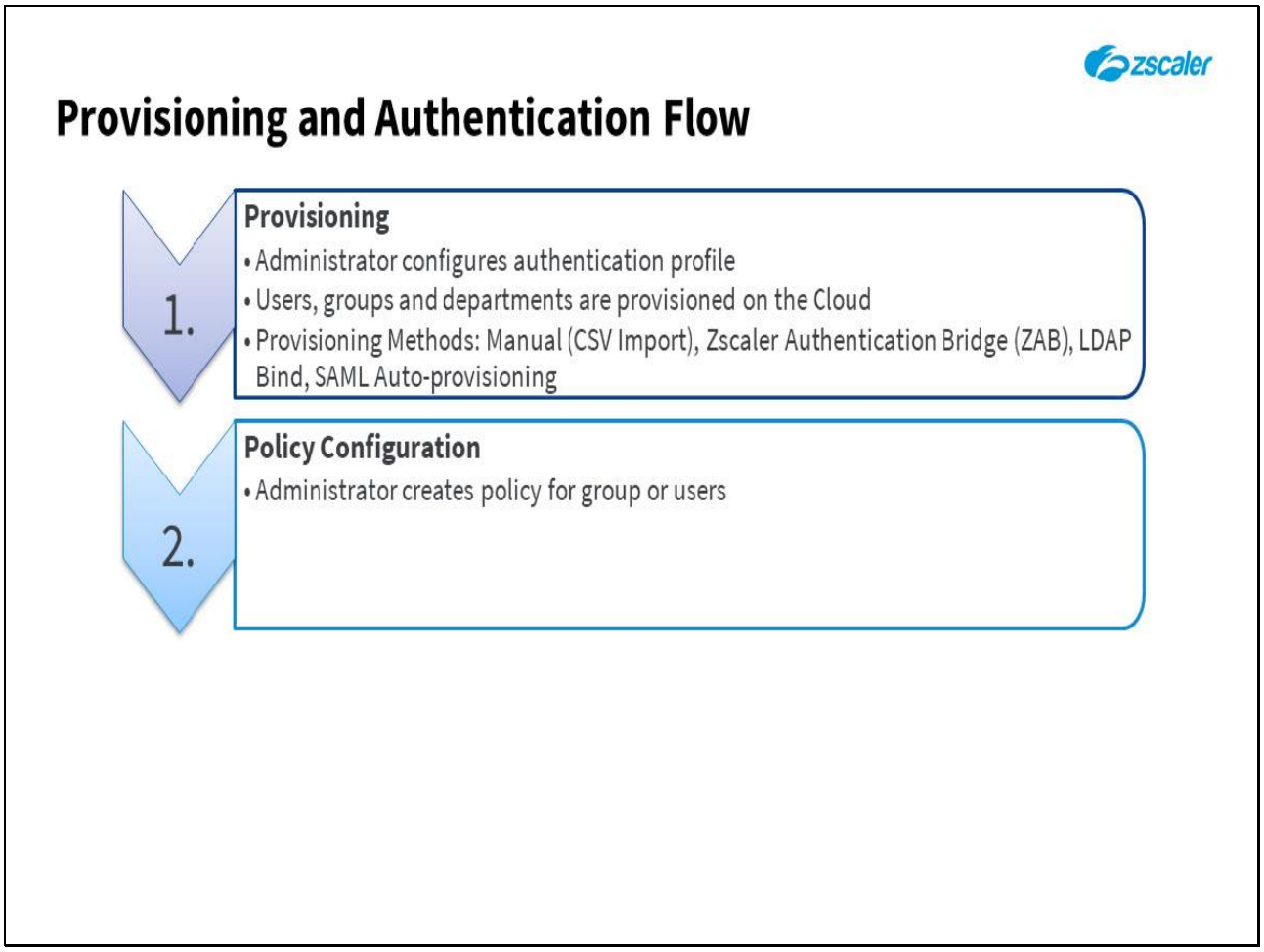
Slide 9 - Provisioning and Authentication Flow



Slide notes

It is important to understand that users must be provisioned in the Zscaler system and then they are authenticated against a User database. How you populate the Zscaler database varies based on the authentication mechanism you employ for your organization. Provisioning methods include: Manual via the Admin Portal, CSV import, LDAP BIND which you will see during the demonstration, or SAML auto-provisioning, or SAML auto-provisioning.

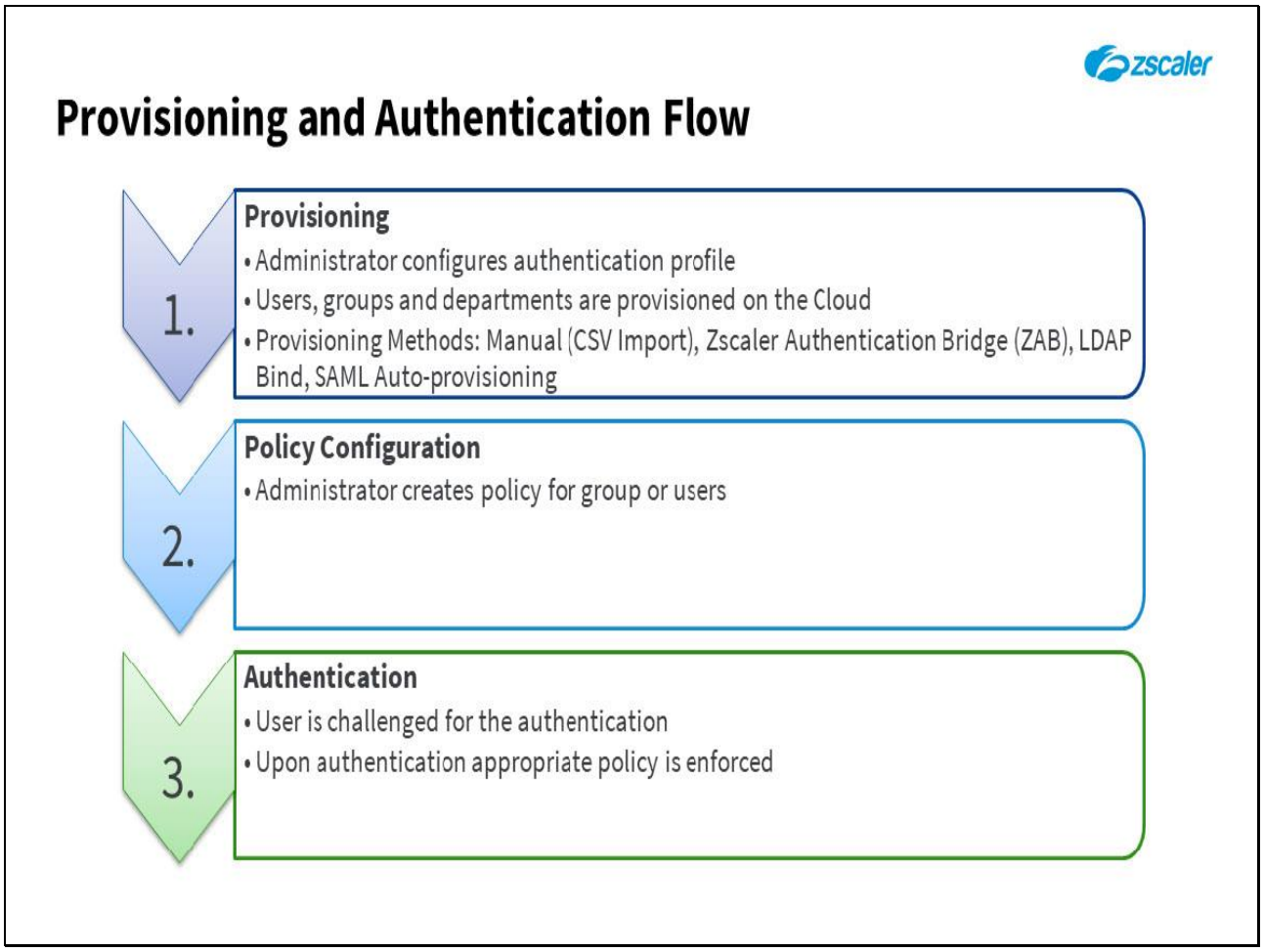
Slide 10 - Provisioning and Authentication Flow



Slide notes

Once the user is created in the system the user should also be tied to a policy (covered in another module), or multiple policies, that determine levels of access. The user is also tied to a department for reporting.

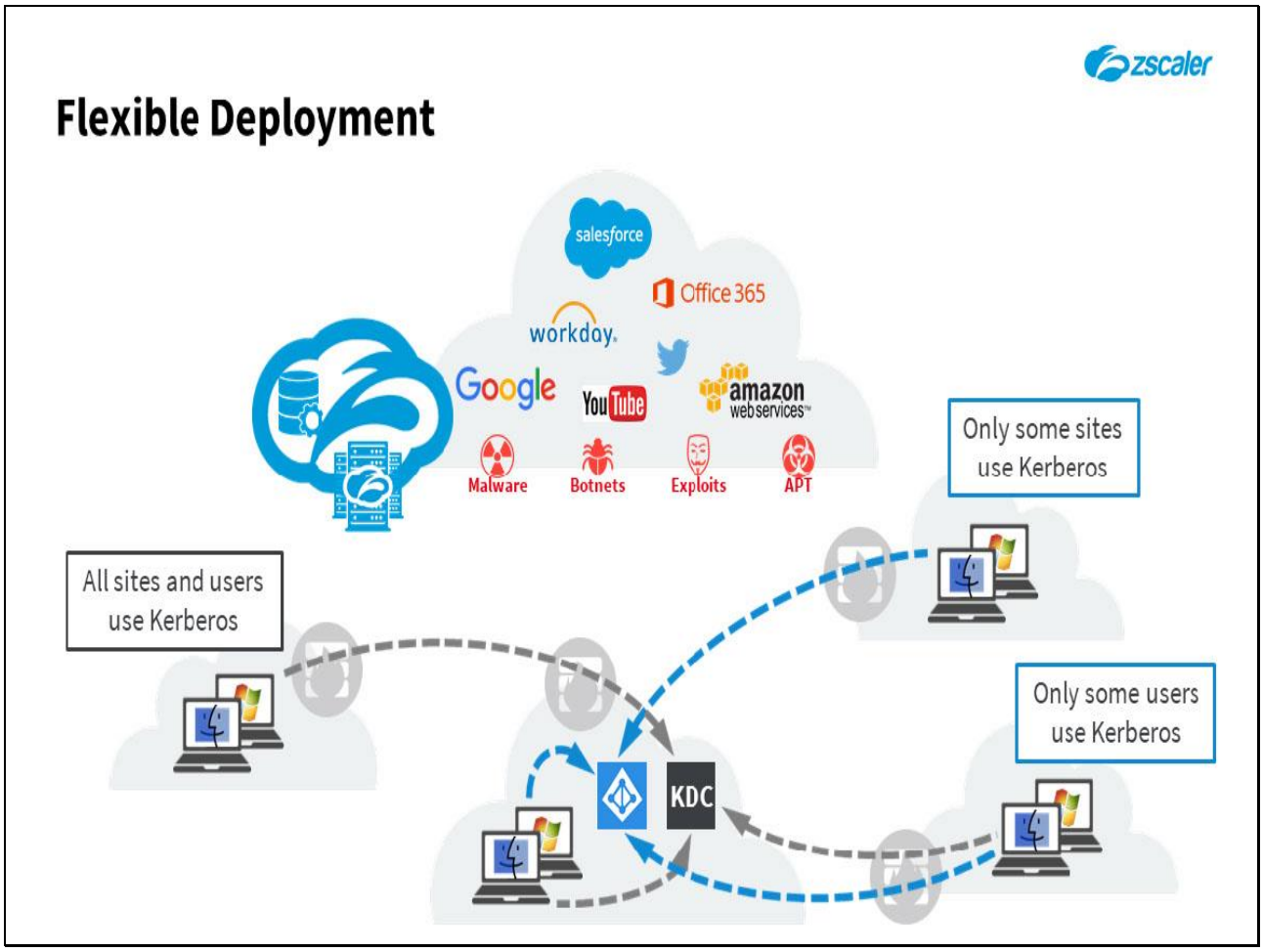
Slide 11 - Provisioning and Authentication Flow



Slide notes

When the user is authenticated the system sees the policy that has been assigned to the user, either directly or via a group, which then determines access privileges.

Slide 12 - Flexible Deployment

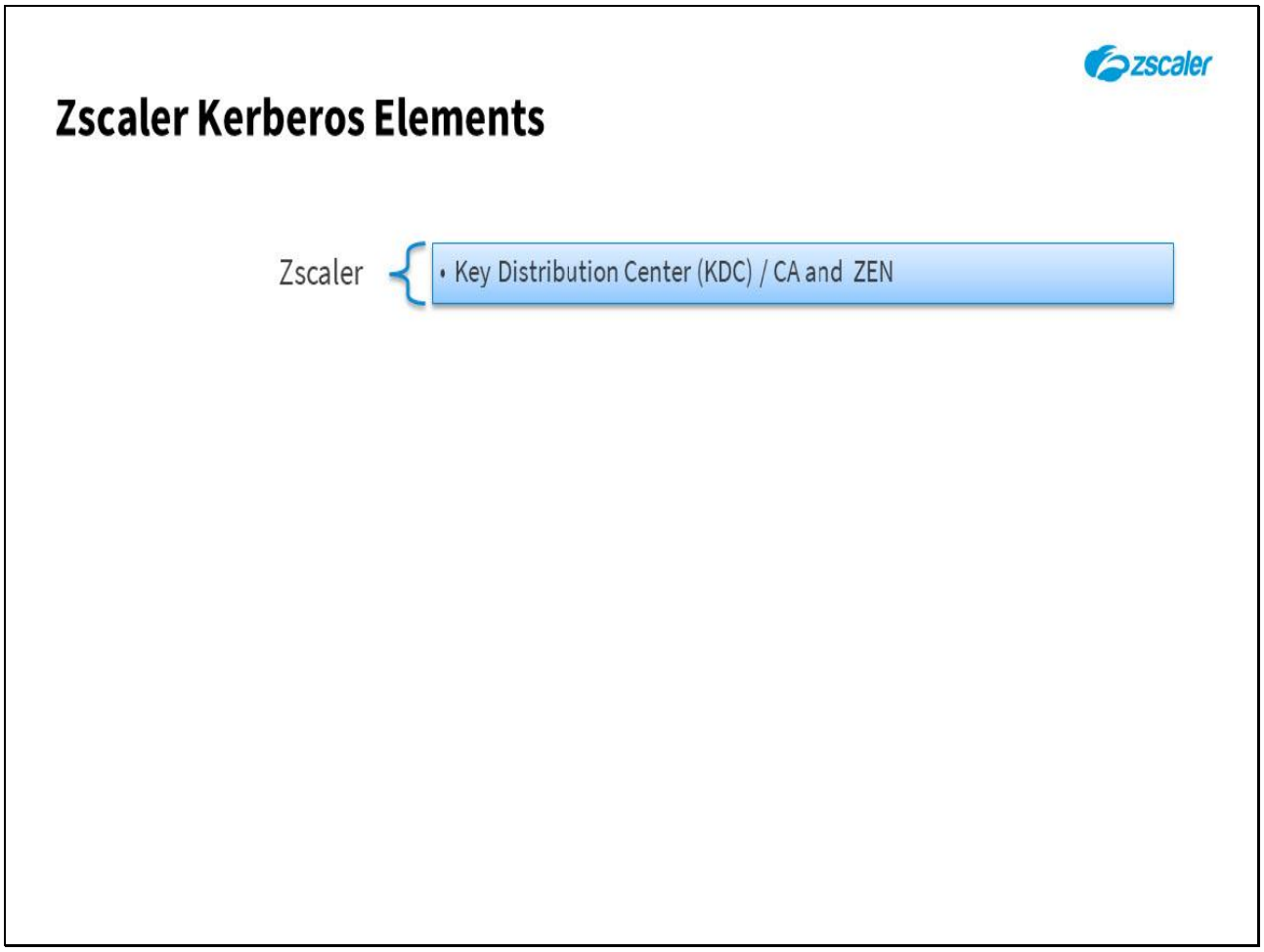


Slide notes

Kerberos provides flexibility in who authenticates via Kerberos or other authentication options.

- In the first example on the left all sites and users are authenticated using Kerberos.
- In the middle, we see that one branch and HQ use Kerberos while another branch uses SAML or LDAP;
- And to the right we see an example where only some users in the branch, or the same location, use Kerberos while others in the same branch use SAML or LDAP.

Slide 13 - Zscaler Kerberos Elements

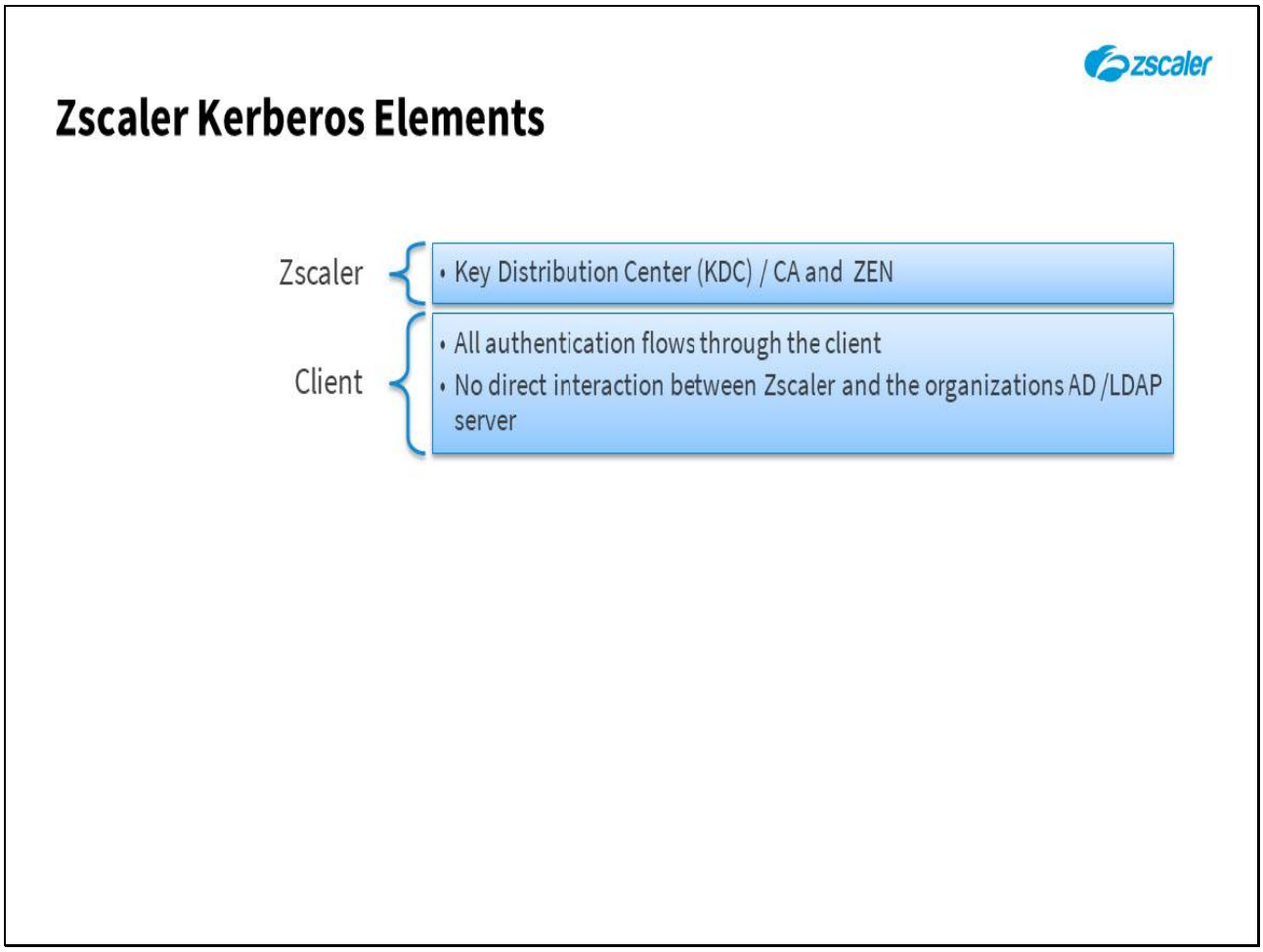


Slide notes

There are several elements that participate in Kerberos Authentication.

1. First is the Zscaler Key Distribution Center (KDC) which is on the CA and ZEN.

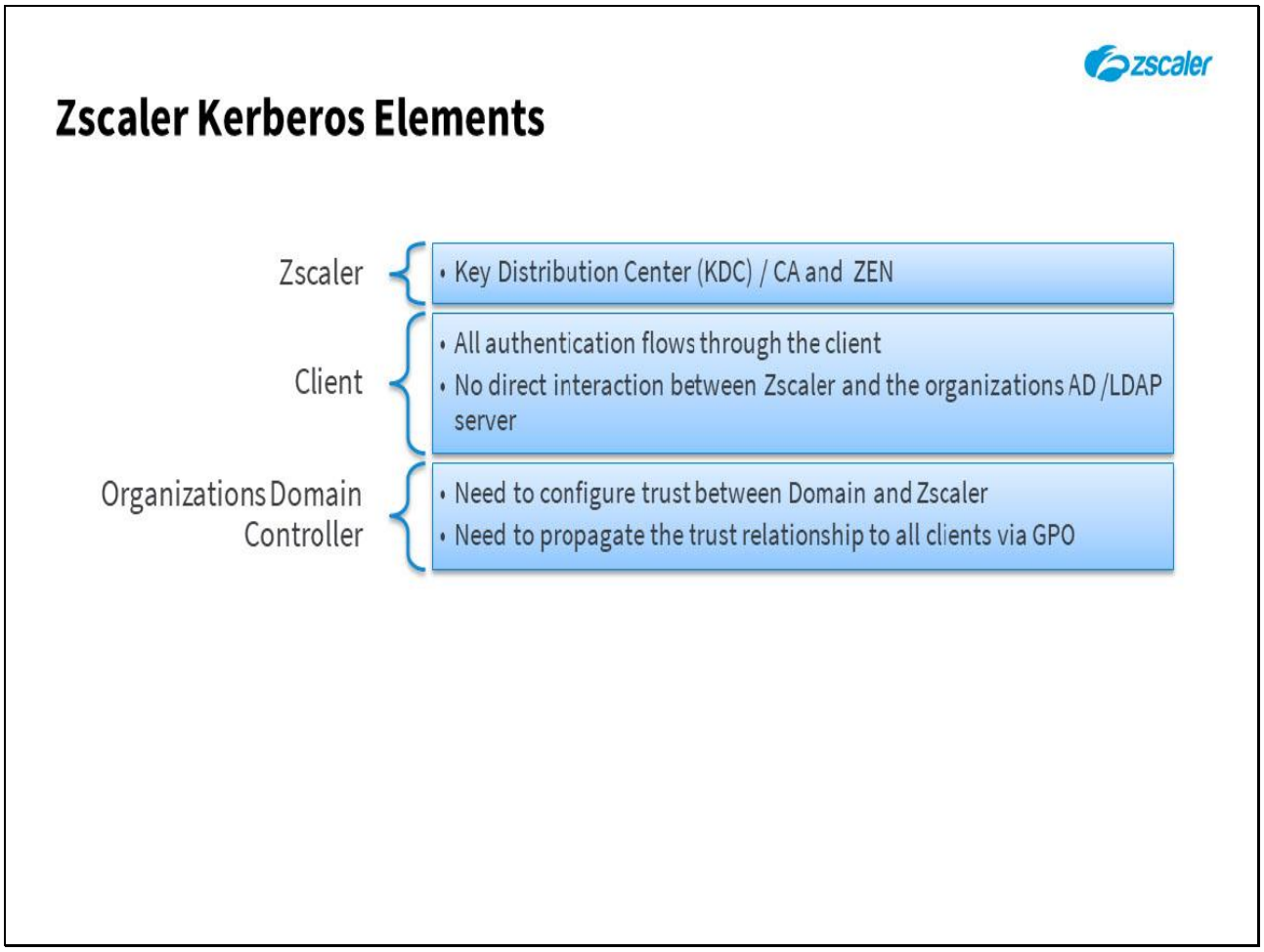
Slide 14 - Zscaler Kerberos Elements



Slide notes

2. Next is the client. All authentication flows through the client. There is no direct interaction between Zscaler and the organizations AD / LDAP server.

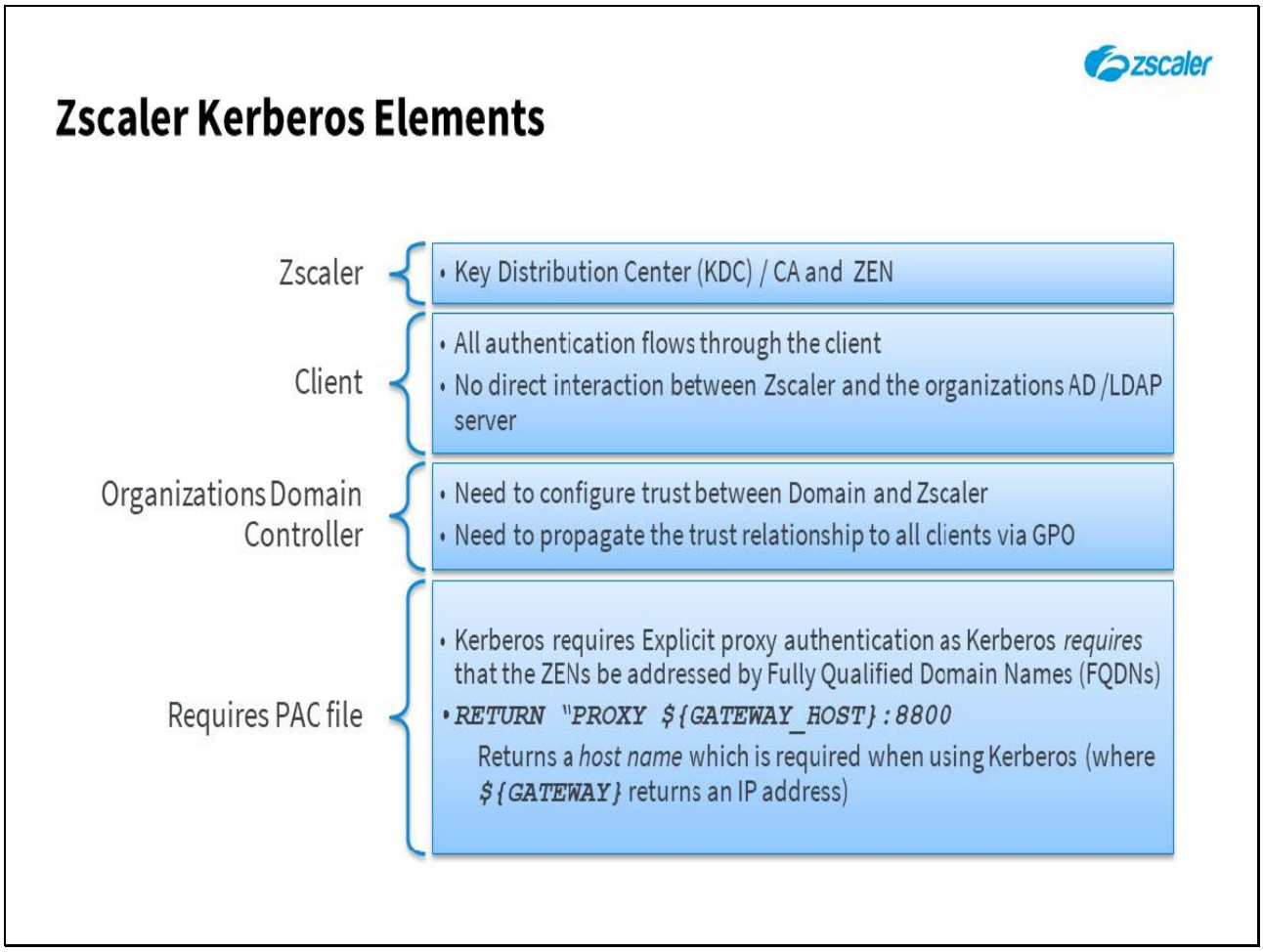
Slide 15 - Zscaler Kerberos Elements



Slide notes

3. Next is the Organizations Domain Controller. A trust must be configured between Domain and Zscaler. The trust relationship must be propagated to all the clients via GPO or manual registry edits.

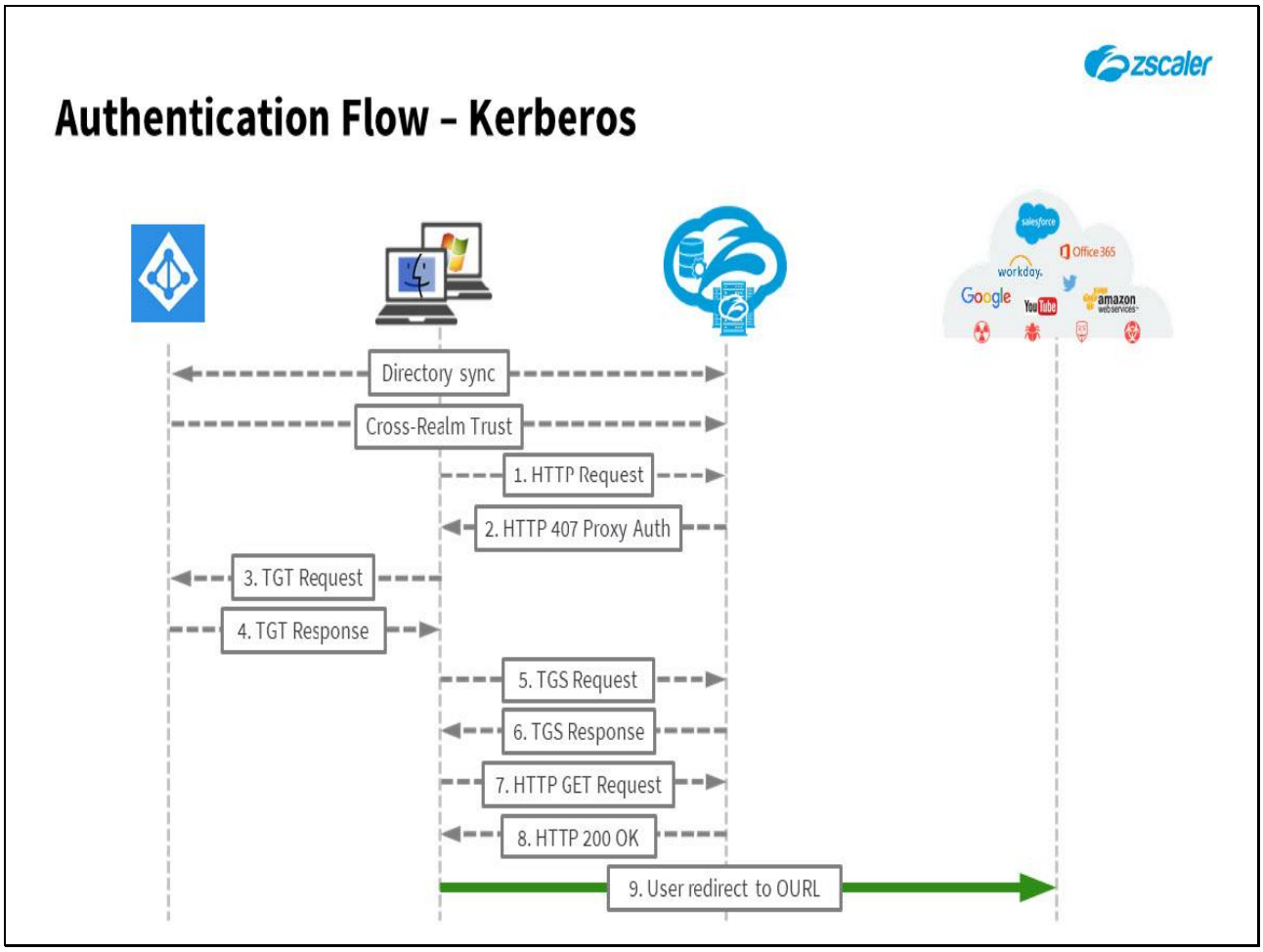
Slide 16 - Zscaler Kerberos Elements



Slide notes

4. Next is the Kerberos PAC file. Kerberos requires Explicit proxy authentication as Kerberos requires that the Zscaler Enforcement Nodes (ZENs) be addressed as Fully Qualified Domain Names (FQDNs).

Slide 17 - Authentication Flow – Kerberos



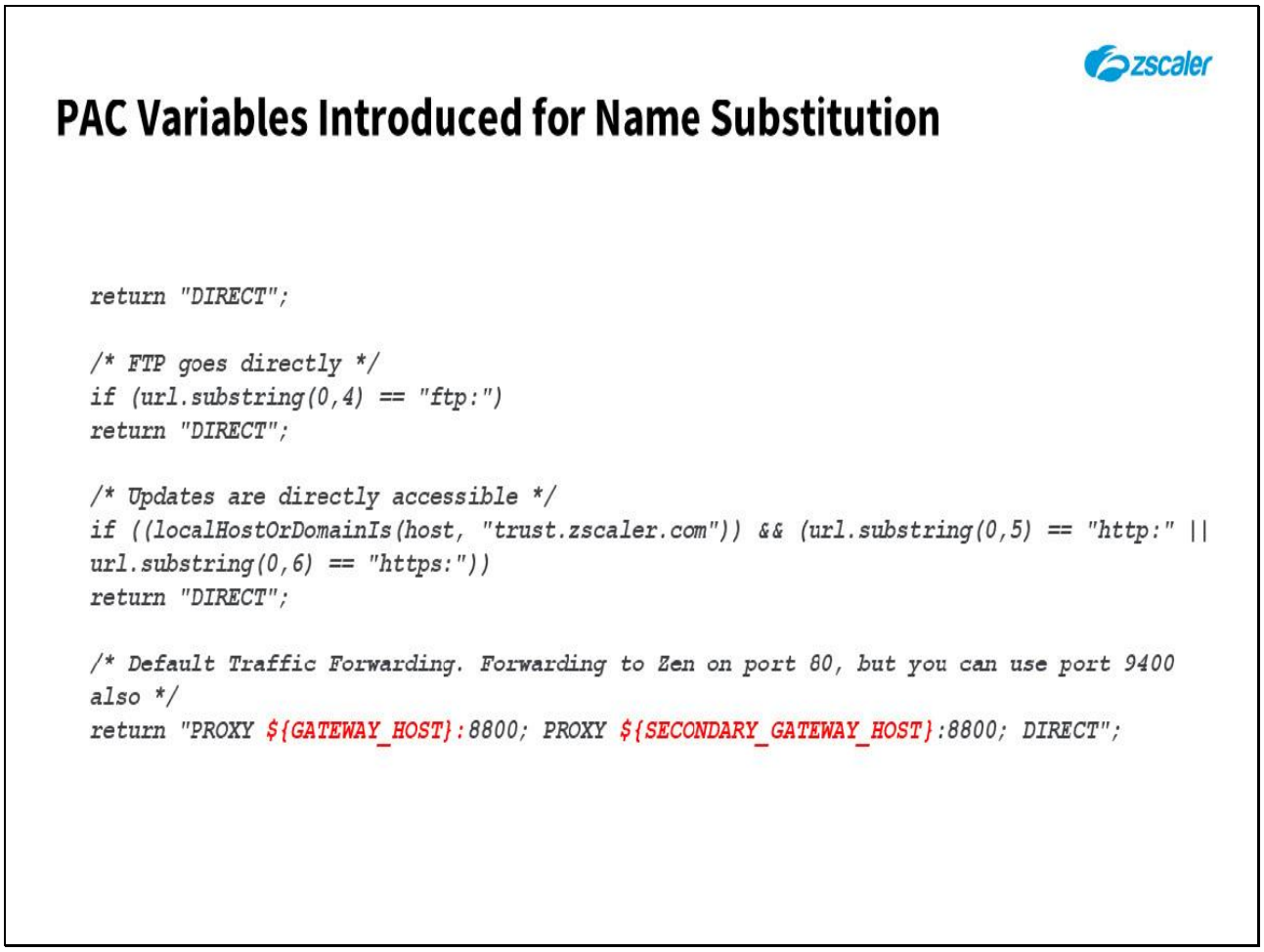
Slide notes

Now let's take a high-level look at the Kerberos authentication process.

- First, an incoming trust relationship is created on the Customer KDC by registering the Zscaler Realm and the Zscaler KDC. This is propagated to the clients via GPO update, or manual Registry changes.
- Next, the client authenticates to the KDC using username and password. If successful, client is sent a Ticket-Granting-Ticket.

1. Next, the user tries to browse through the proxy,
2. Which issues 407 Negotiate challenge.
3. Next, the client contacts the KDC with the server name,
4. And the KDC issues a cross-realm ticket.
5. Next, the client contacts the Zscaler KDC with the cross-realm ticket and the proxy name.
6. The Zscaler KDC issues a ticket for the Zscaler proxy.
7. 8. 9. And last, the client contacts the proxy with the ticket.

Slide 18 - PAC Variables Introduced for Name Substitution

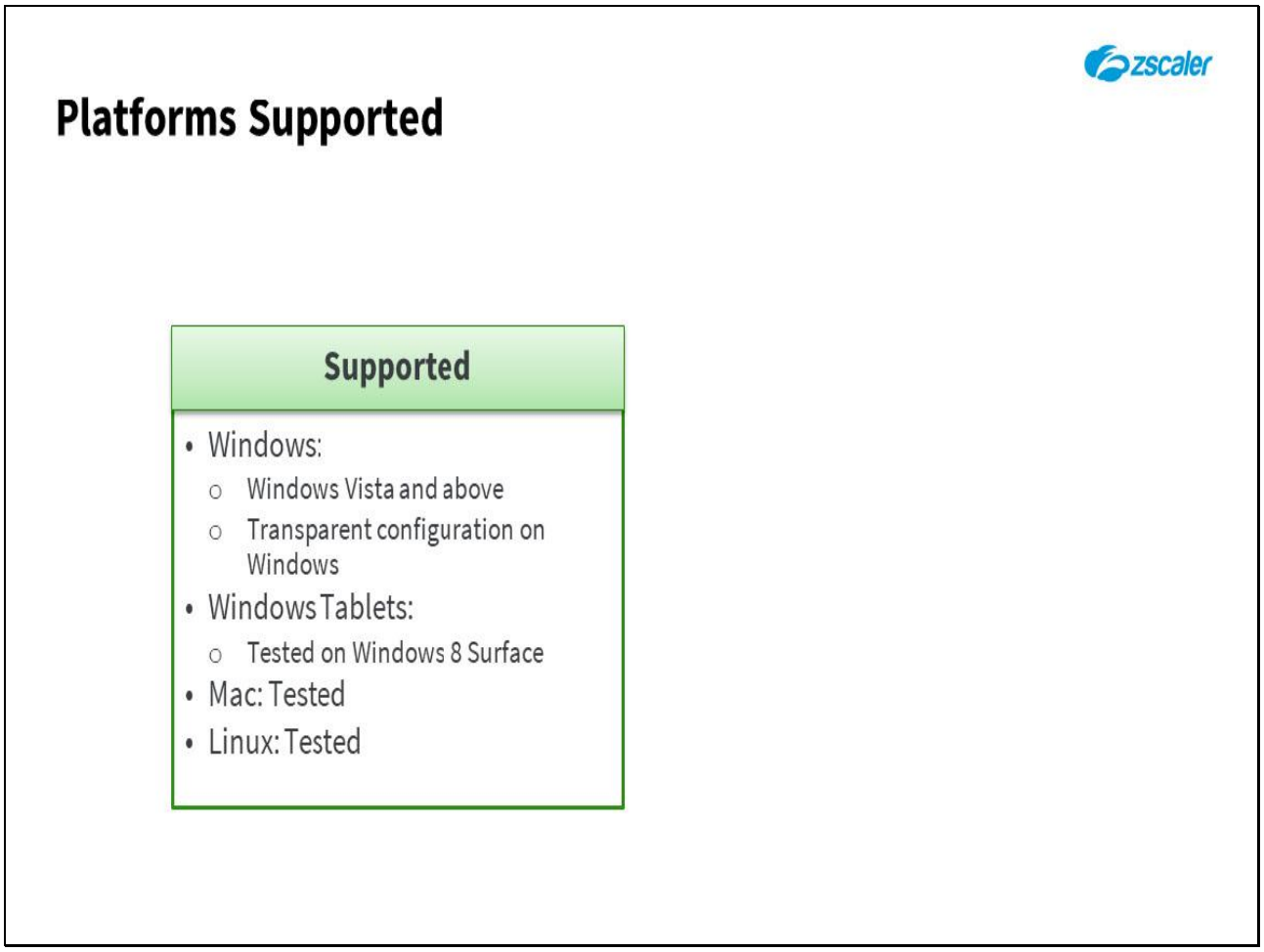


Slide notes

The Zscaler Kerberos default PAC file specifies the following:

- Kerberos requires that the Zscaler Enforcement Nodes (ZENs) be addressed as Fully Qualified Domain Names (FQDNs). To accommodate this requirement, the Kerberos PAC file contains the variables ${GATEWAY_HOST} and ${SECONDARY_GATEWAY_HOST}, which the service substitutes with the domain names of the primary and secondary ZENs as shown here.
- It forwards web traffic to port 8800 of the ZEN. ZENs challenge all traffic that it receives on port 8800 for a Kerberos Negotiate Authentication ticket for the Zscaler service.
- If the location has Kerberos enabled, then traffic can be forwarded to the proxy ports, port 80, 443, 9400, 9443, or to the dedicated proxy port associated with that location if available. The service automatically challenges all explicitly forwarded proxy traffic from that location for a Kerberos ticket for the Zscaler domain.

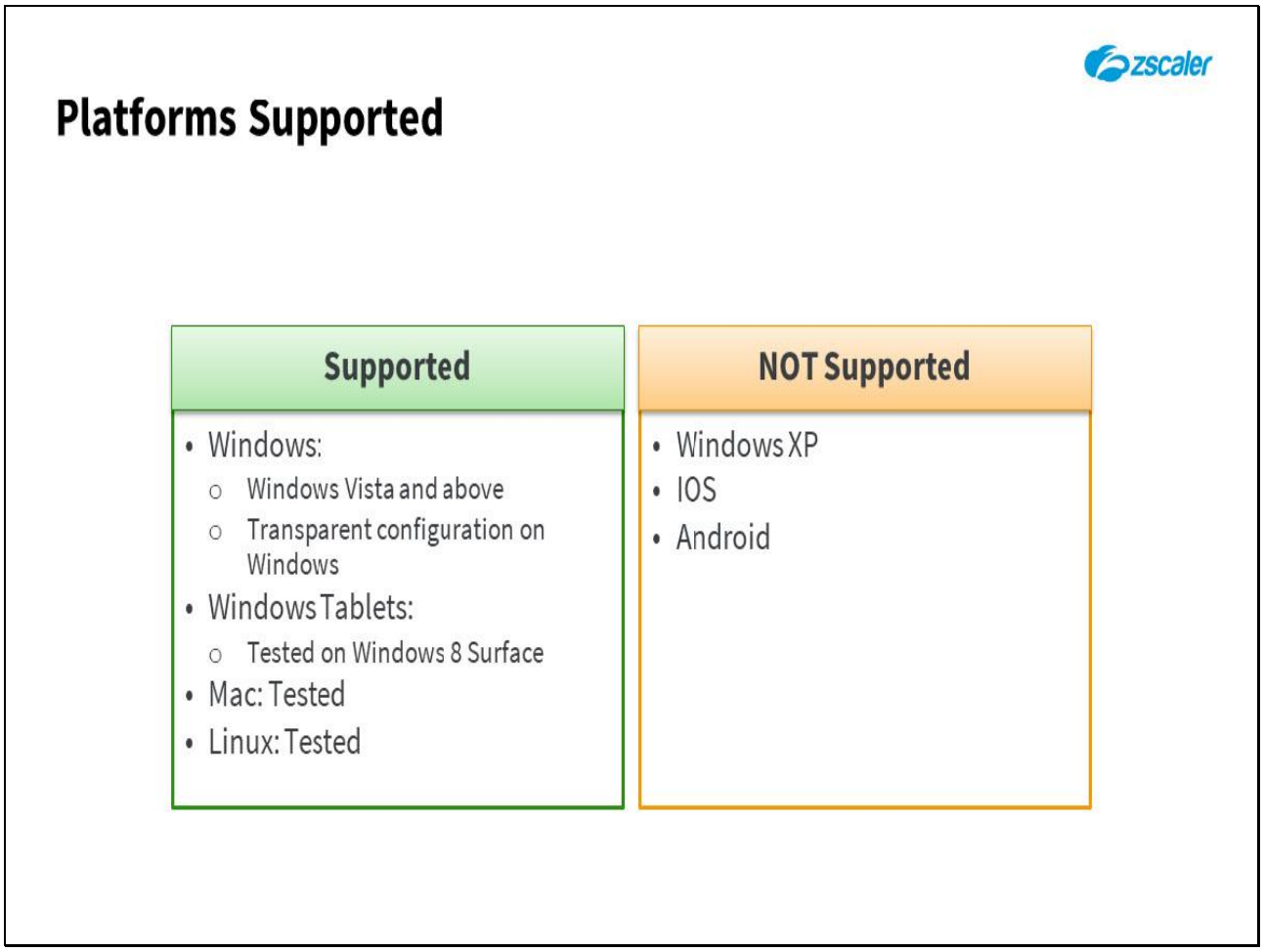
Slide 19 - Platforms Supported



Slide notes

Windows Vista and above support Kerberos where Windows XP does not. Kerberos authentication is transparent to the user once on the domain.

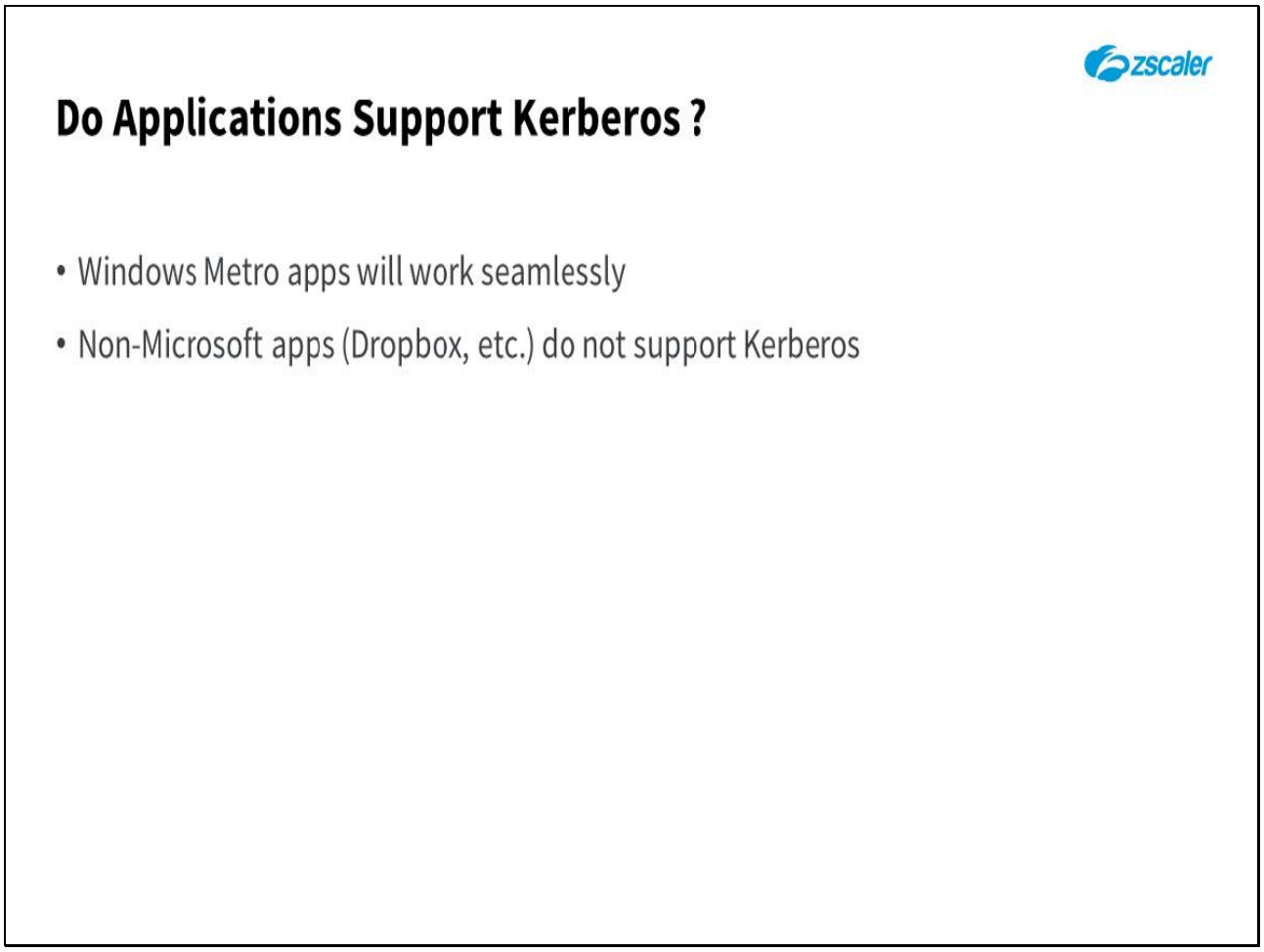
Slide 20 - Platforms Supported



Slide notes

Windows tablets on Windows 8 are also supported. MacOS and Linux have been tested though IOS and Android are not supported.

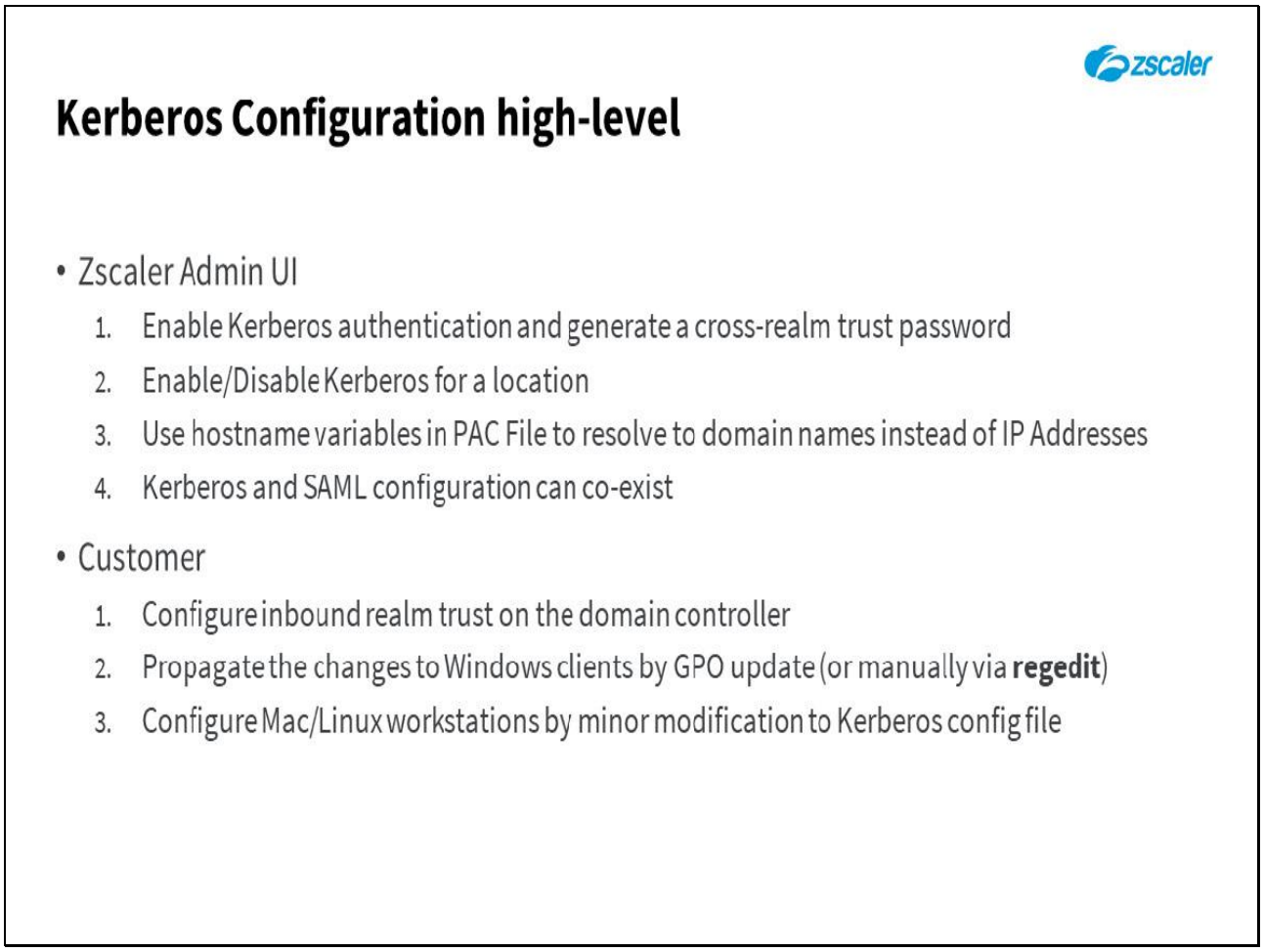
Slide 21 - Do Applications Support Kerberos ?



Slide notes

Regarding specific application support of Kerberos Windows metro apps will work seamlessly where non-Microsoft apps, such as Dropbox, don’t support Kerberos.

Slide 22 - Kerberos Configuration high-level



Slide notes

Let's go over the configuration process at a high level before going into the interactive demo. There are configuration elements in three places - the Zscaler cloud, the Domain controller, and the windows workstation.

On Zscaler you will need to enable Kerberos authentication globally then generate a cross-realm trust password. You will then, optionally, enable Kerberos on a location. Do this if you want to use Kerberos to authenticate all devices at that location. Use the hostname variables in your PAC file to resolve to domain names instead of IP addresses. Zscaler provides a default PAC file that can be used as a starting point in building your own PAC file. This is covered in the PAC file module separately.

Alternatively, for testing purposes or quick deployments manual proxy configuration can be used. Lastly, as mentioned previously, Kerberos does not provide for user provisioning. You can use SAML for auto-provisioning or use one of the other methods.

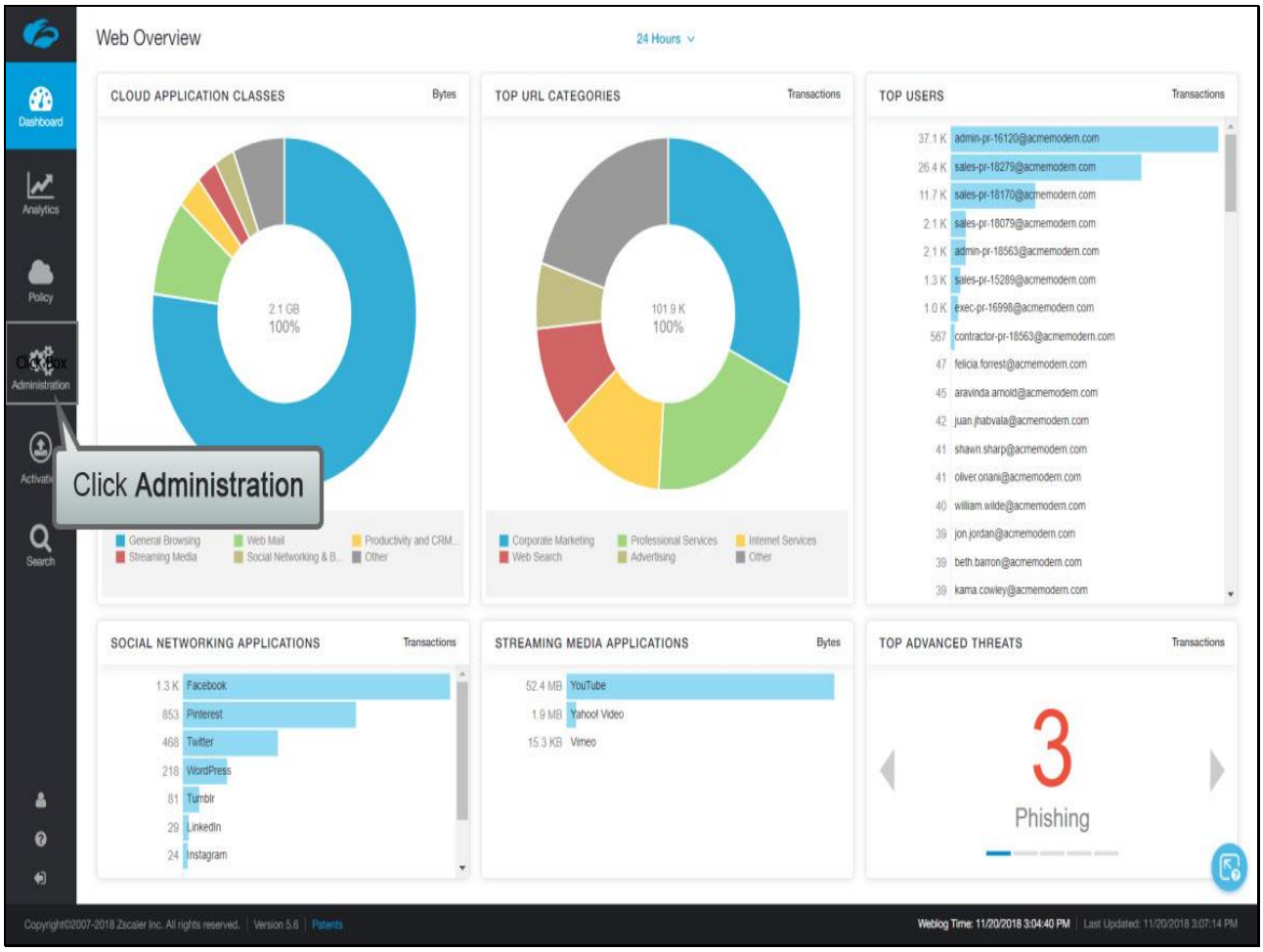
Some configuration on the Domain Controller and clients are required as well to enable Kerberos. On the Windows PC registry changes are required. These can be done manually on an individual workstation using regedit, or more commonly using GPO.

Slide 23 - Zscaler Configuration

Slide notes

Now let’s walk through the configuration process for Kerberos authentication.

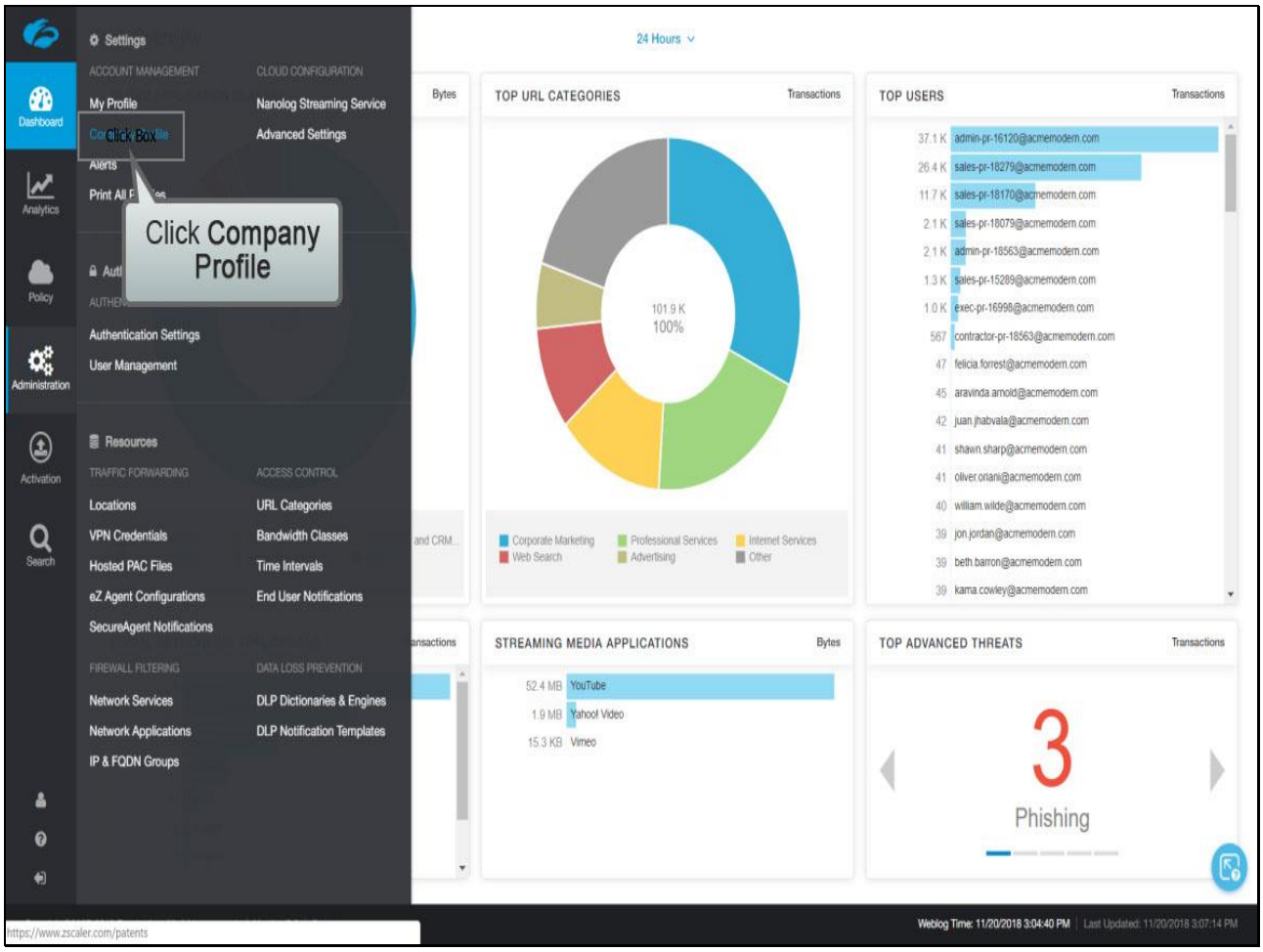
Slide 24 - Slide 24



Slide notes

Begin by checking that the Domain name you have registered on the Zscaler service is the same that you will use for your Kerberos Realm name. To check this on Zscaler go to **Administration**.

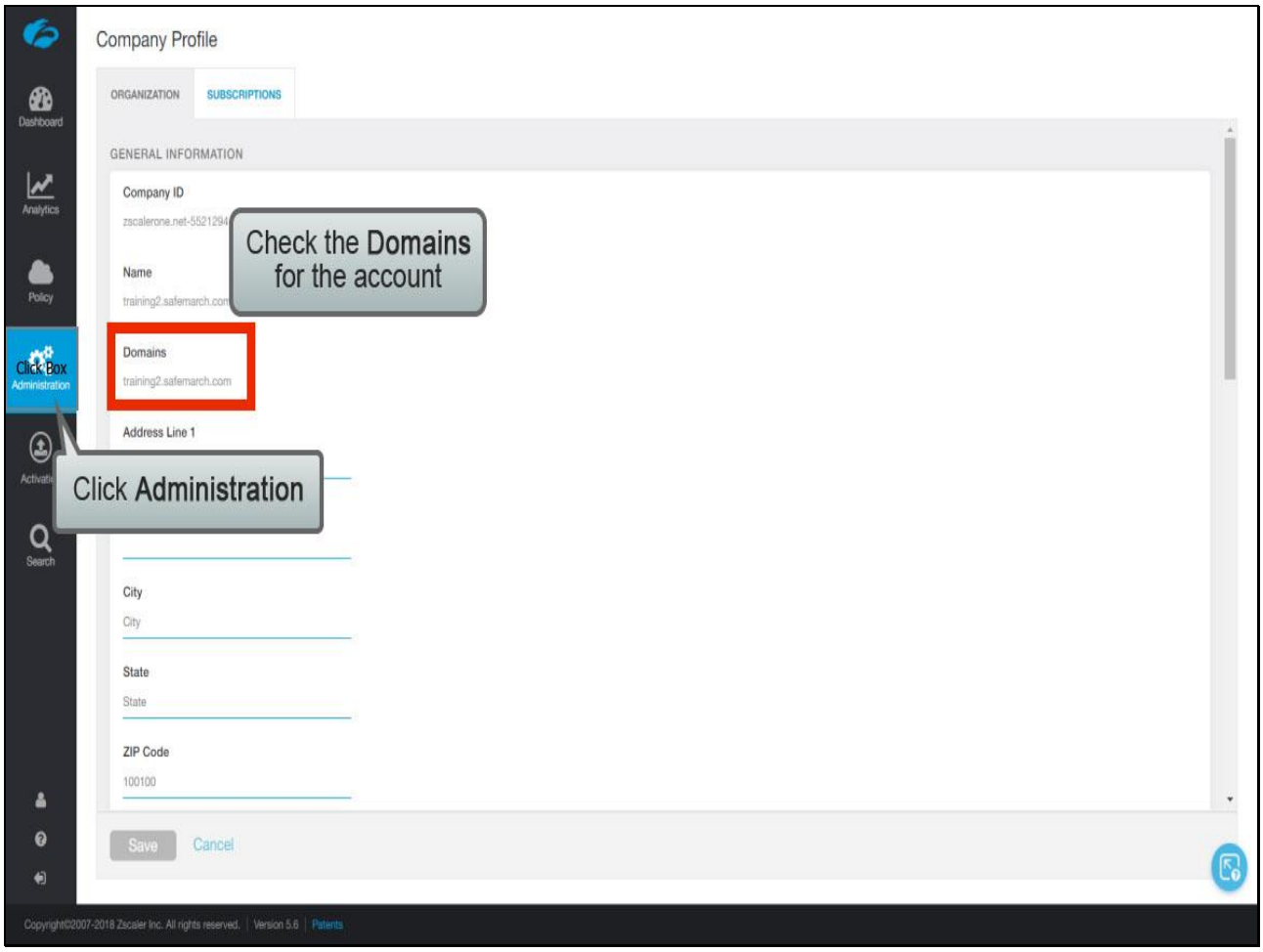
Slide 25 - Slide 25



Slide notes

Then **Company Profile**.

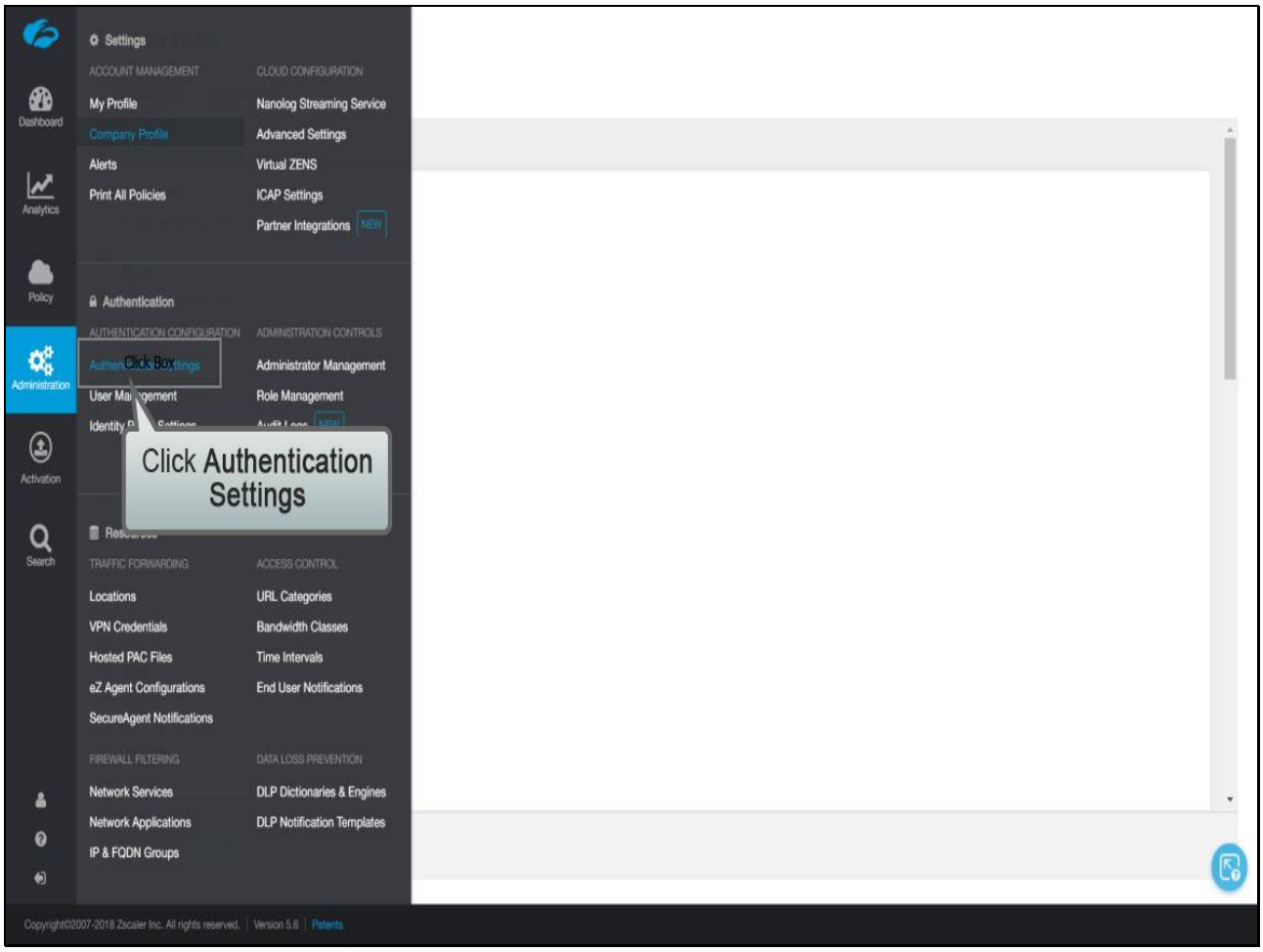
Slide 26 - Slide 26



Slide notes

You can see in the **GENERAL INFORMATION** box there is a listing for **Domains**. Make sure this Domain matches what you are configuring for the Kerberos Realm Domain. Next, go to **Administration**.

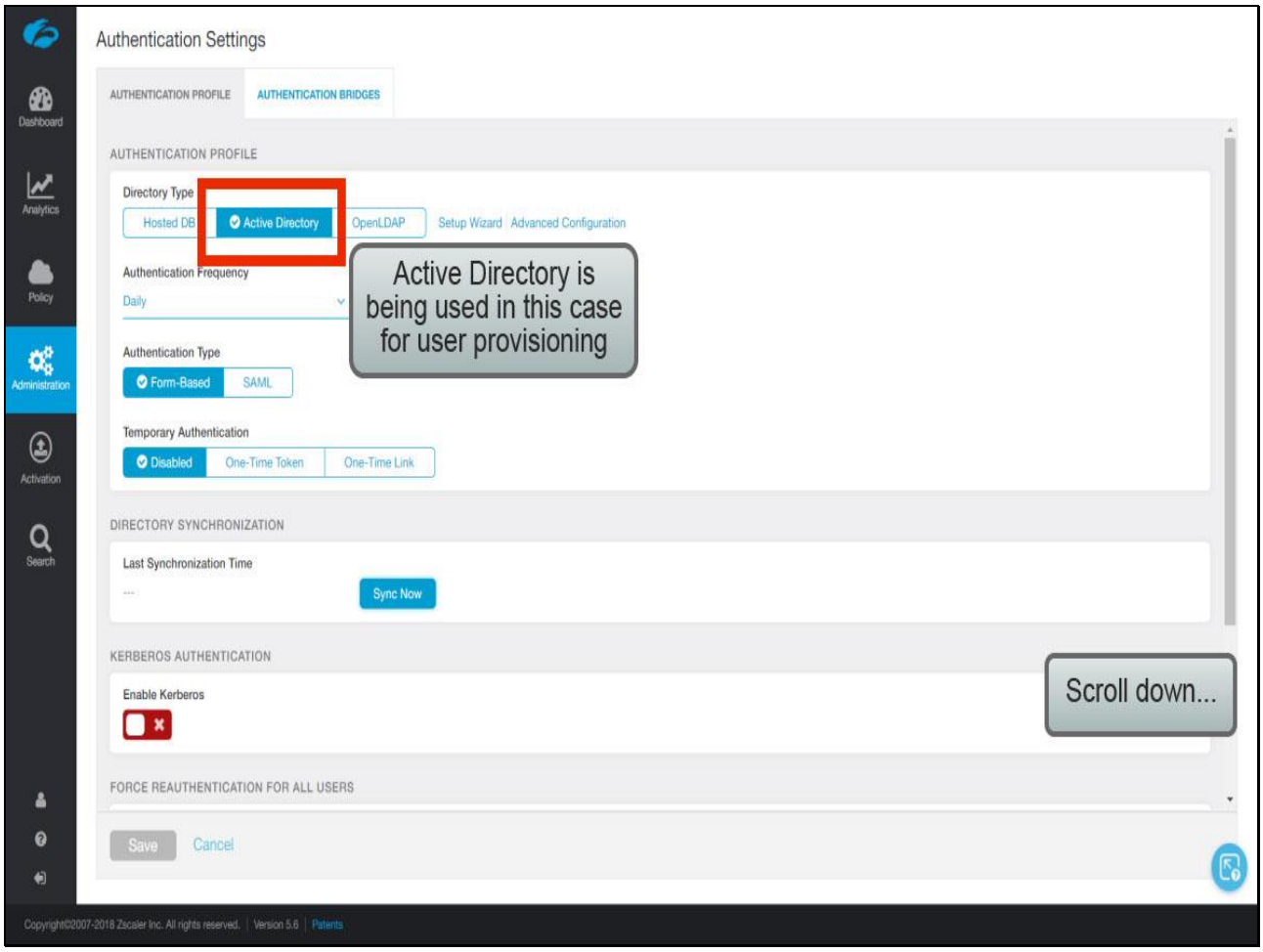
Slide 27 - Slide 27



Slide notes

Then **Authentication Settings**.

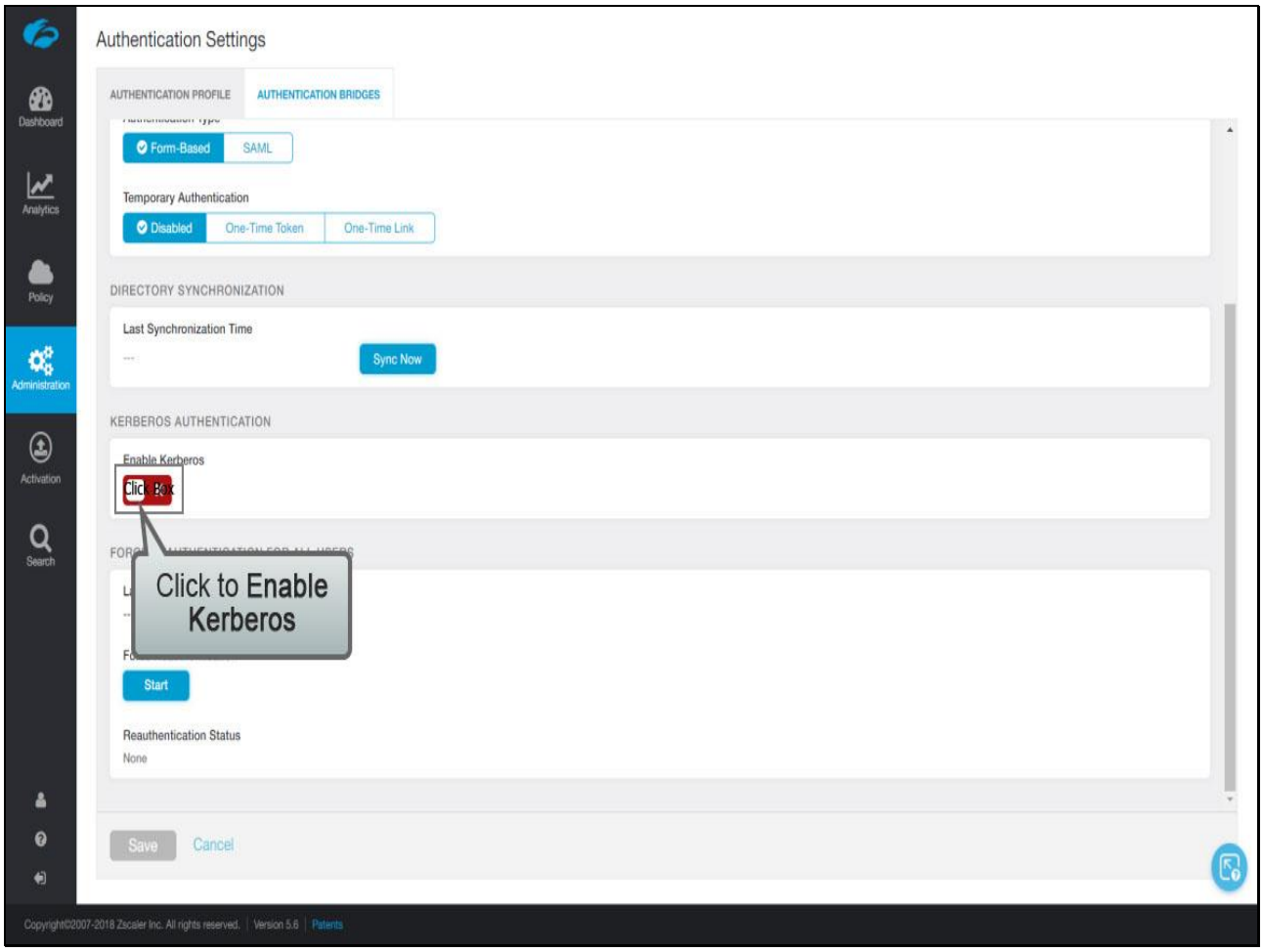
Slide 28 - Slide 28



Slide notes

As discussed in the slides, Kerberos provides for Authentication only and does not provide for User Provisioning. User provisioning is not part of this demonstration and has been covered in the previous authentication modules for Hosted DB, Active Directory, and SAML. For this example, I am using Active Directory Sync for User provisioning.

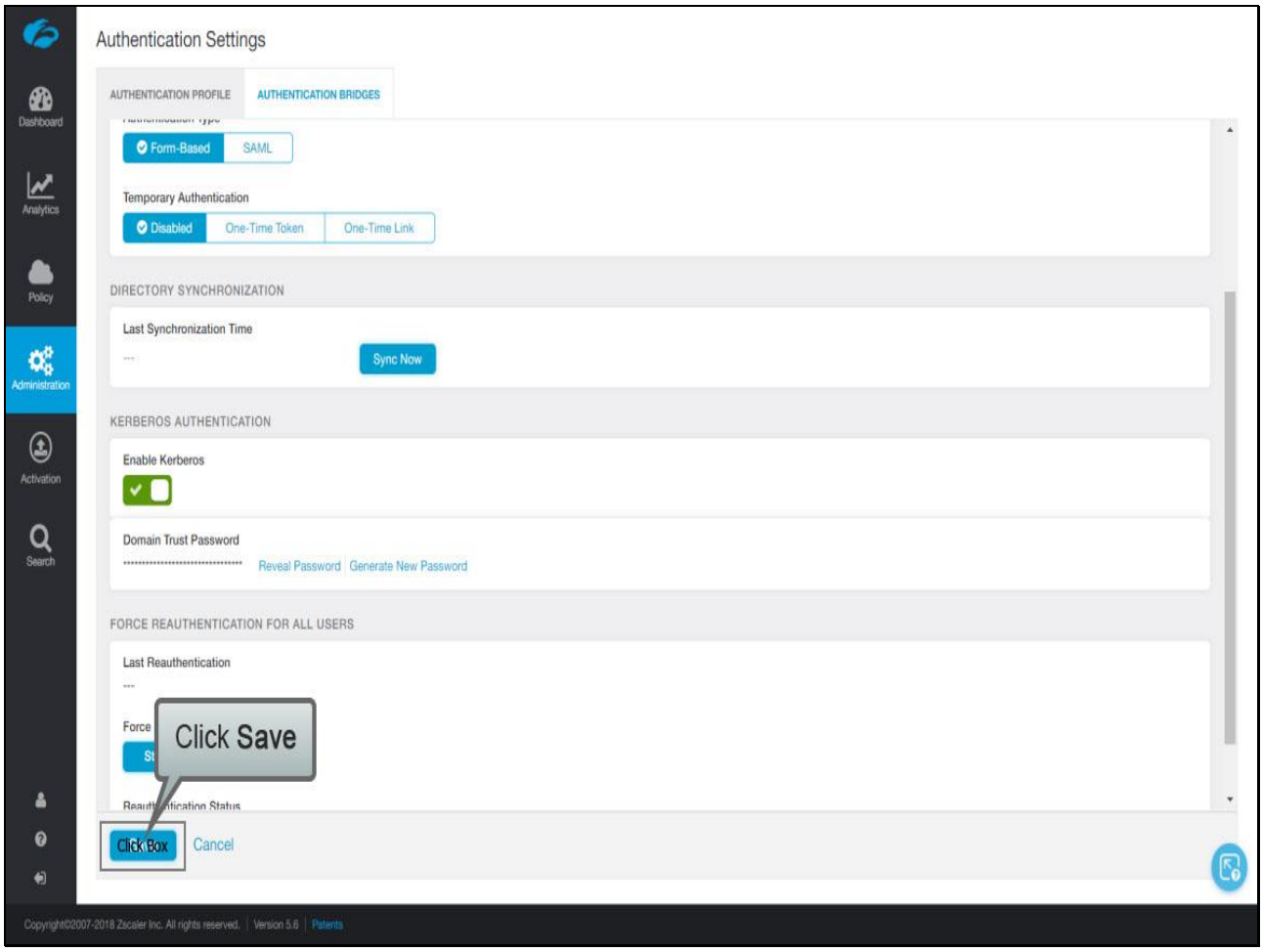
Slide 29 - Slide 29



Slide notes

Check **Enable Kerberos**.

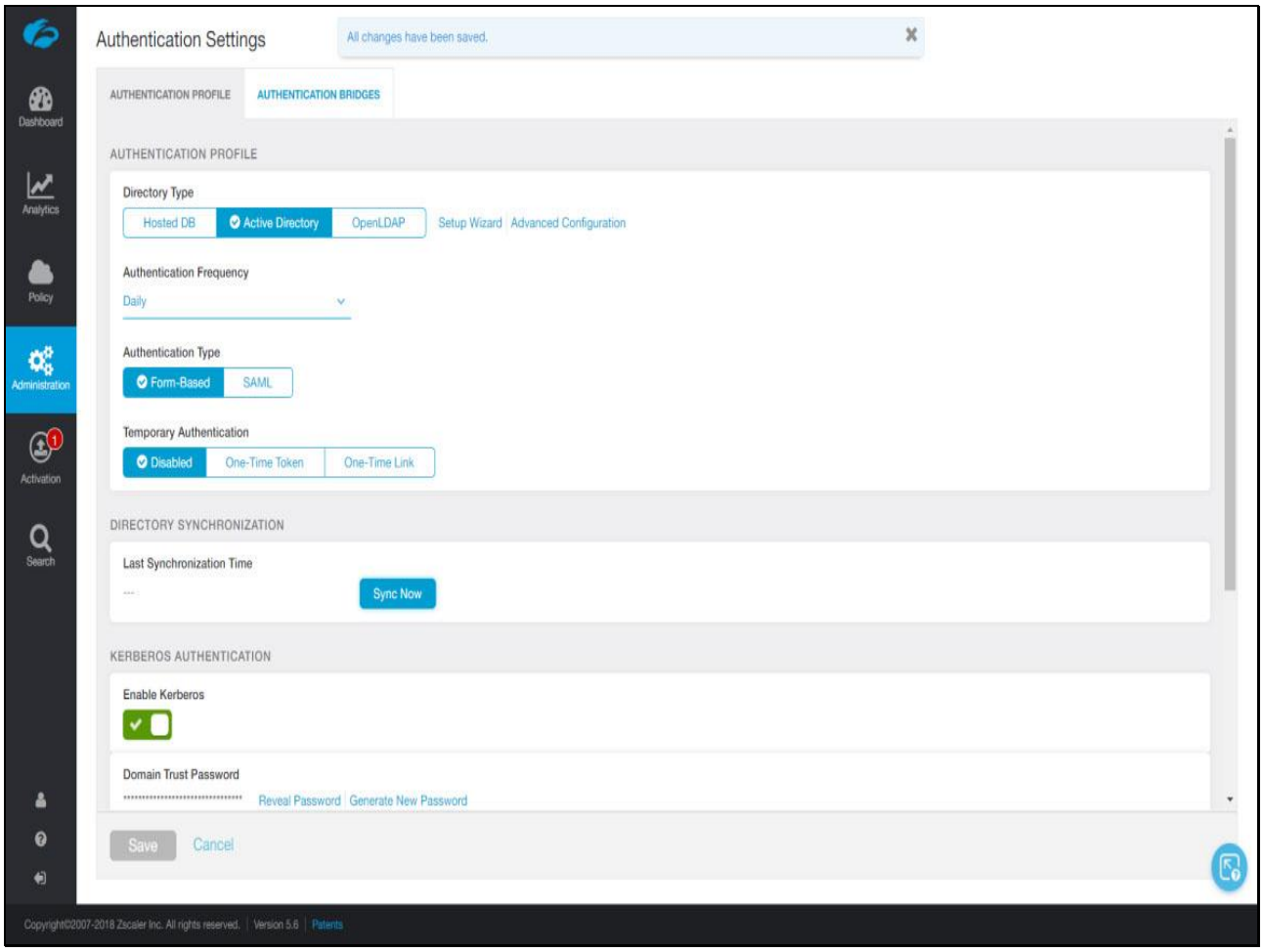
Slide 30 - Slide 30



Slide notes

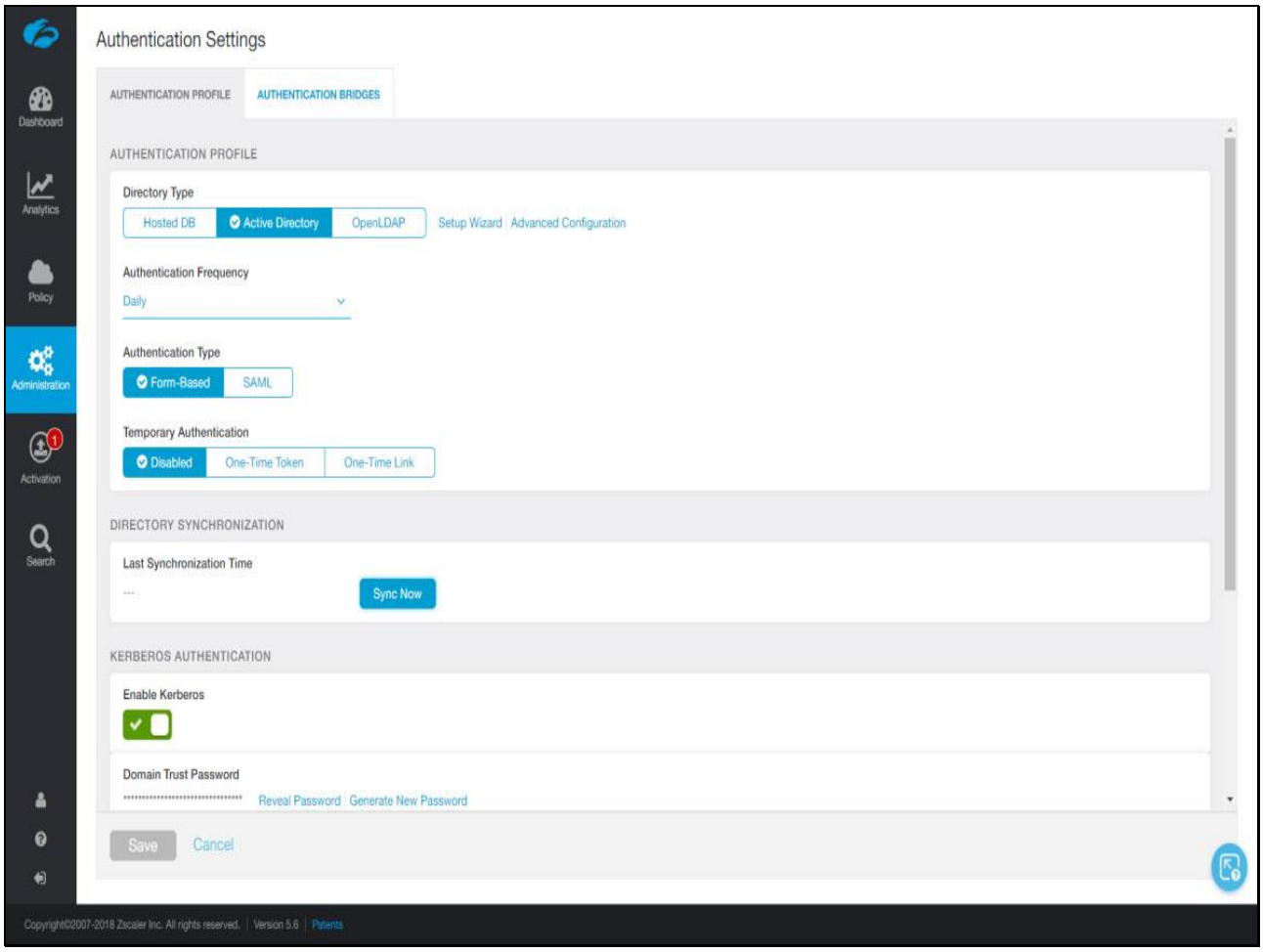
Then **Save**.

Slide 31 - Slide 31



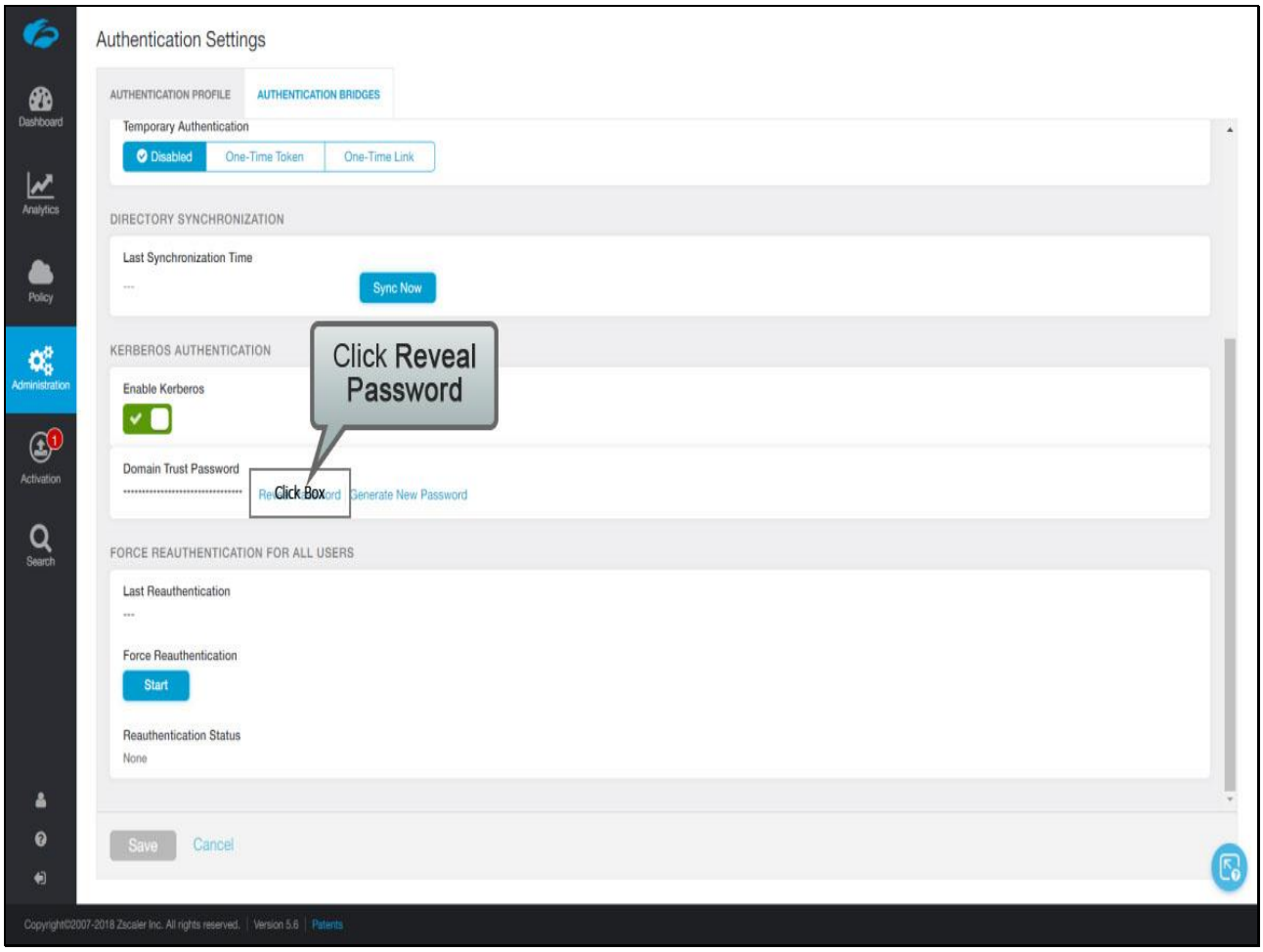
Slide notes

Slide 32 - Slide 32



Slide notes

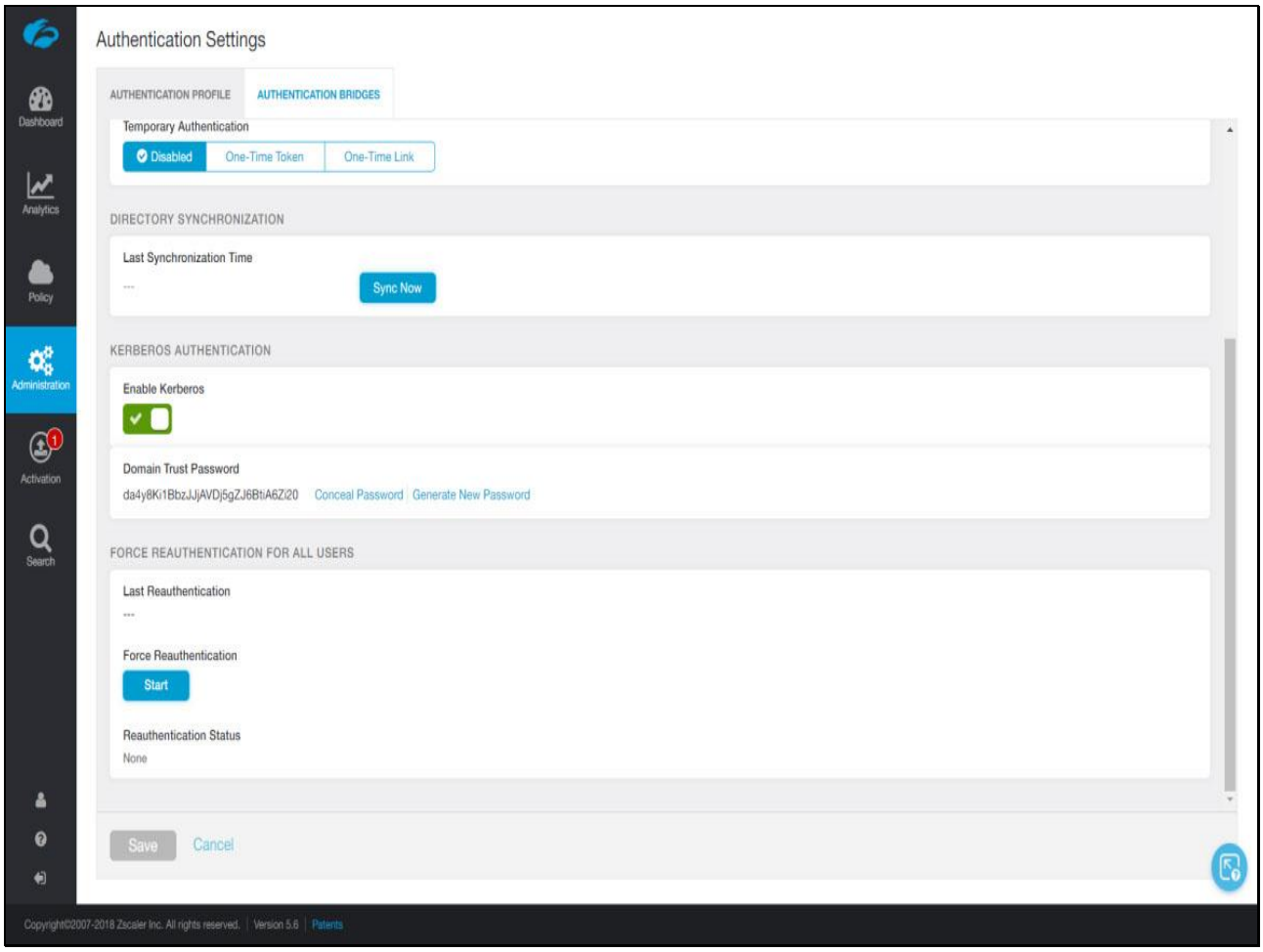
Slide 33 - Slide 33



Slide notes

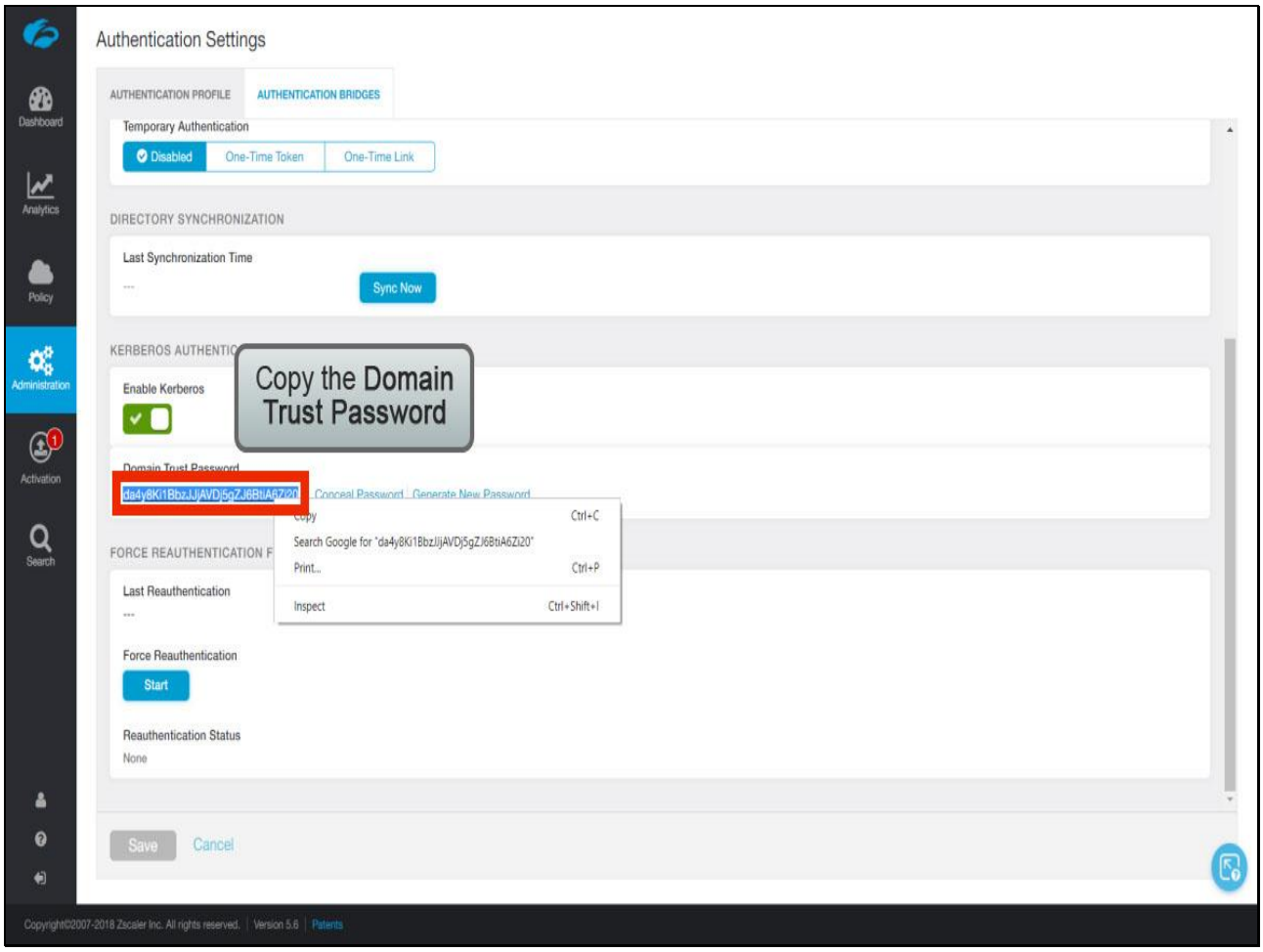
Next to the **Domain Trust Password** click on **Reveal Password**.

Slide 34 - Slide 34



Slide notes

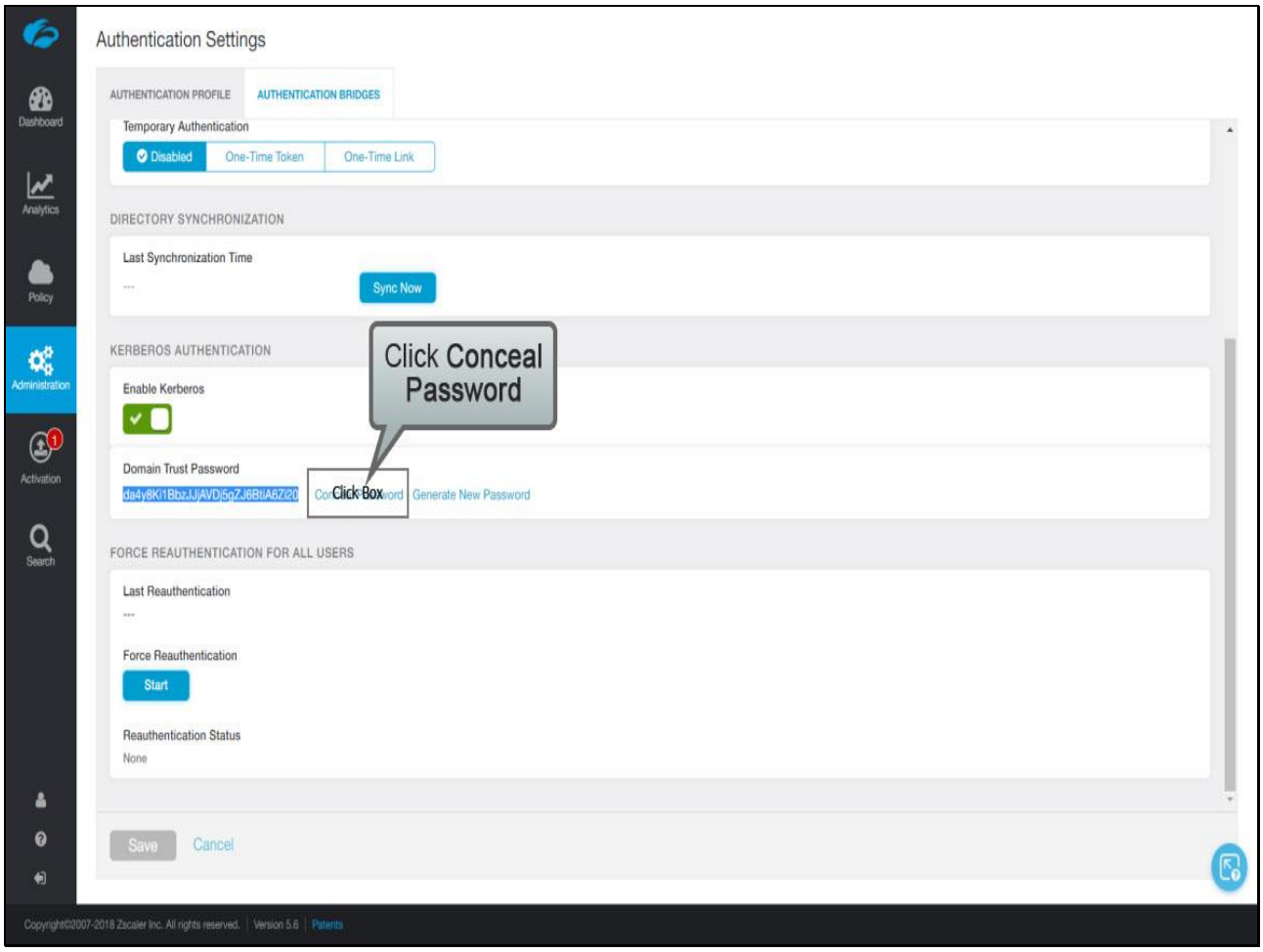
Slide 35 - Slide 35



Slide notes

This will show the Trust password. Copy this for use later when you configure the Domain controller.

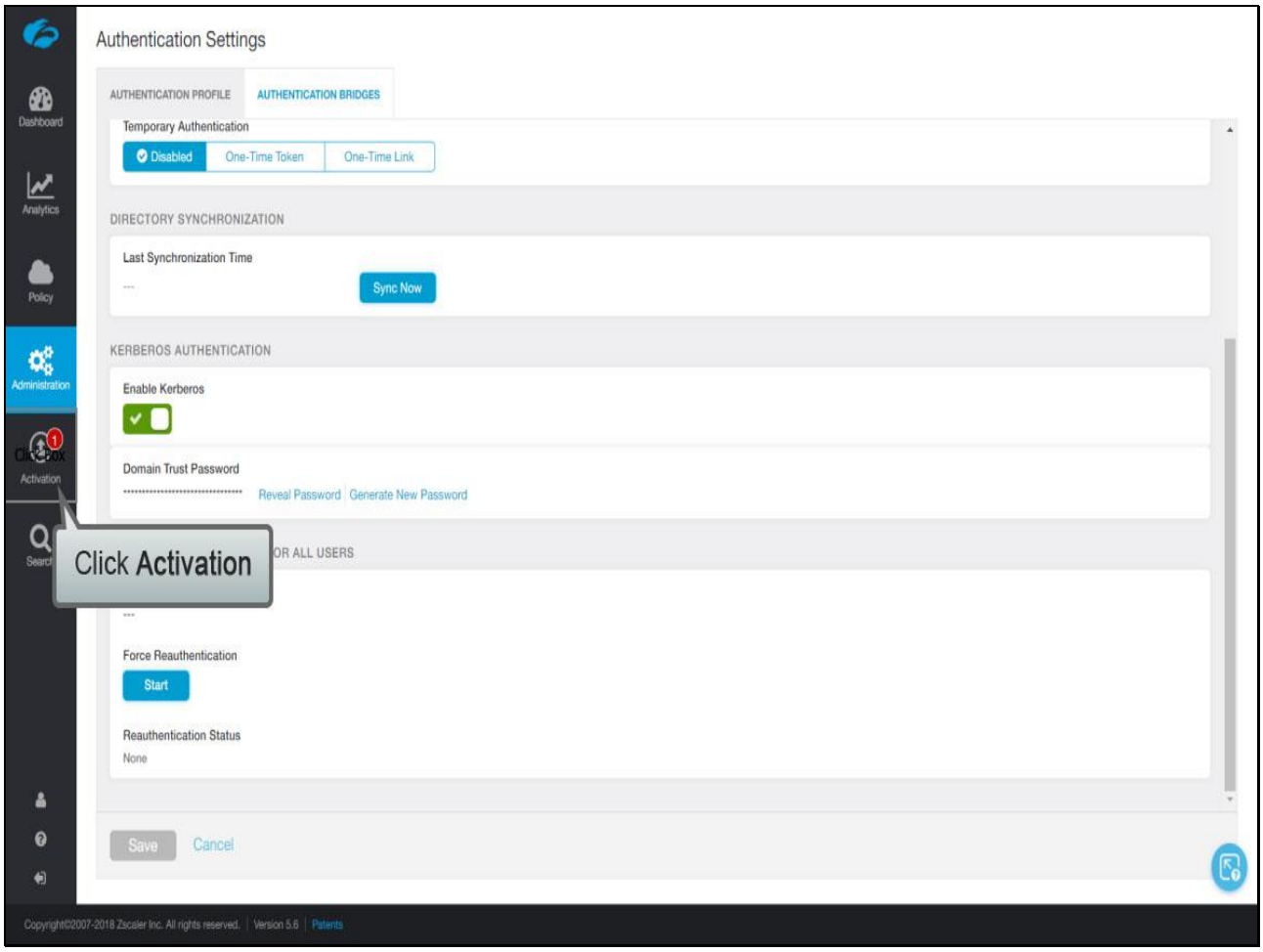
Slide 36 - Slide 36



Slide notes

Click **Conceal Password**, …

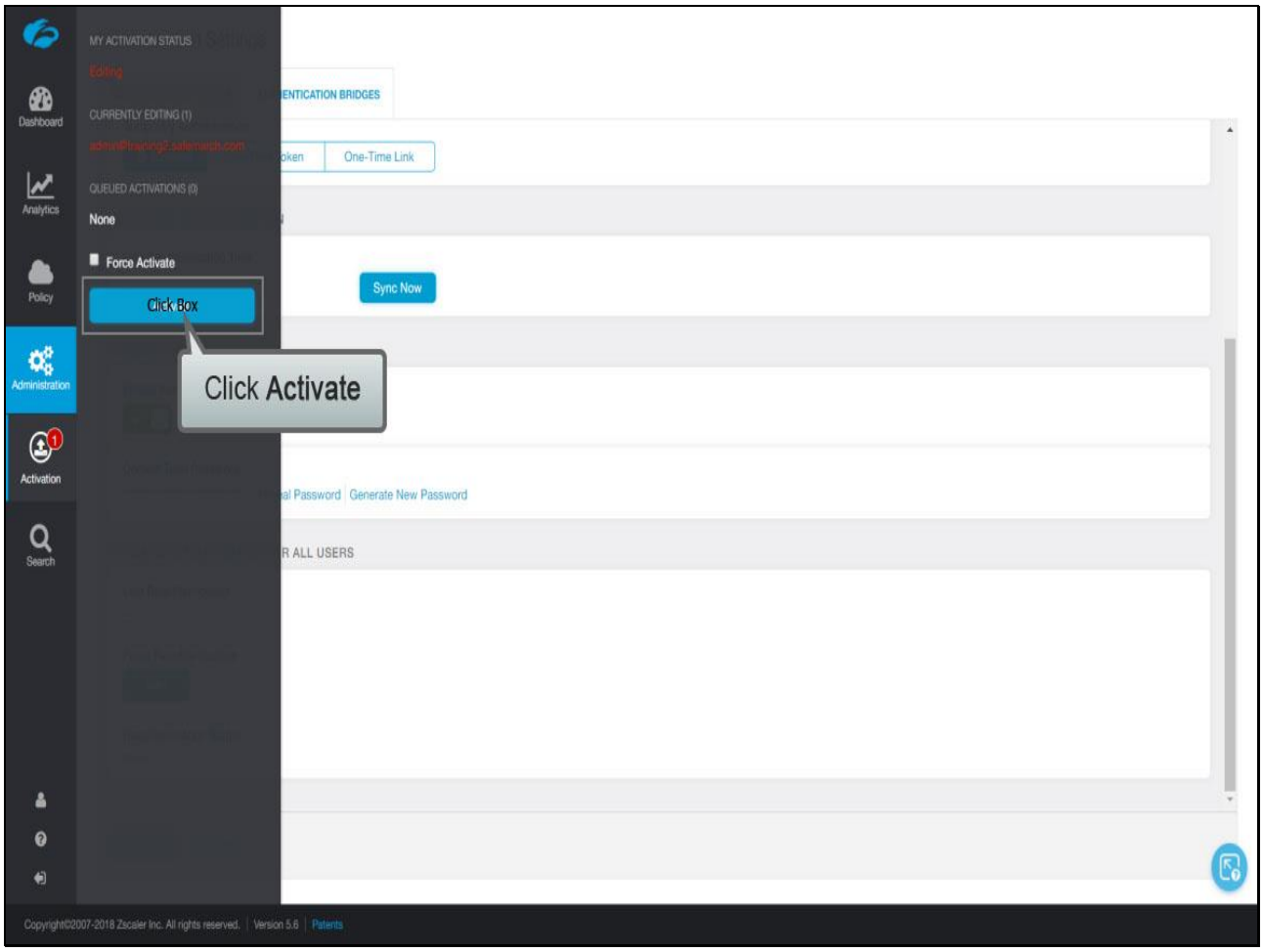
Slide 37 - Slide 37



Slide notes

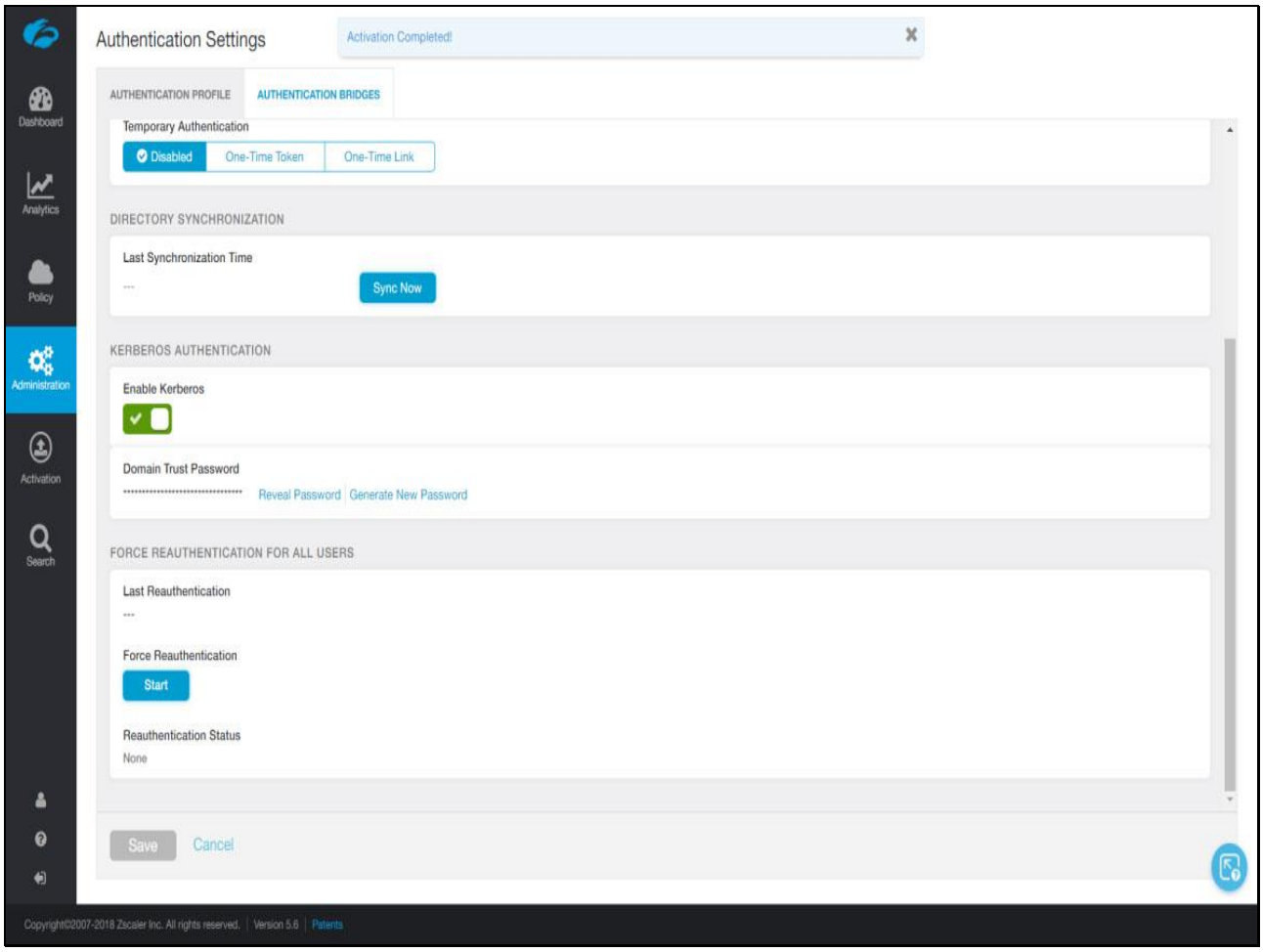
…and **Activate** your changes.

Slide 38 - Slide 38



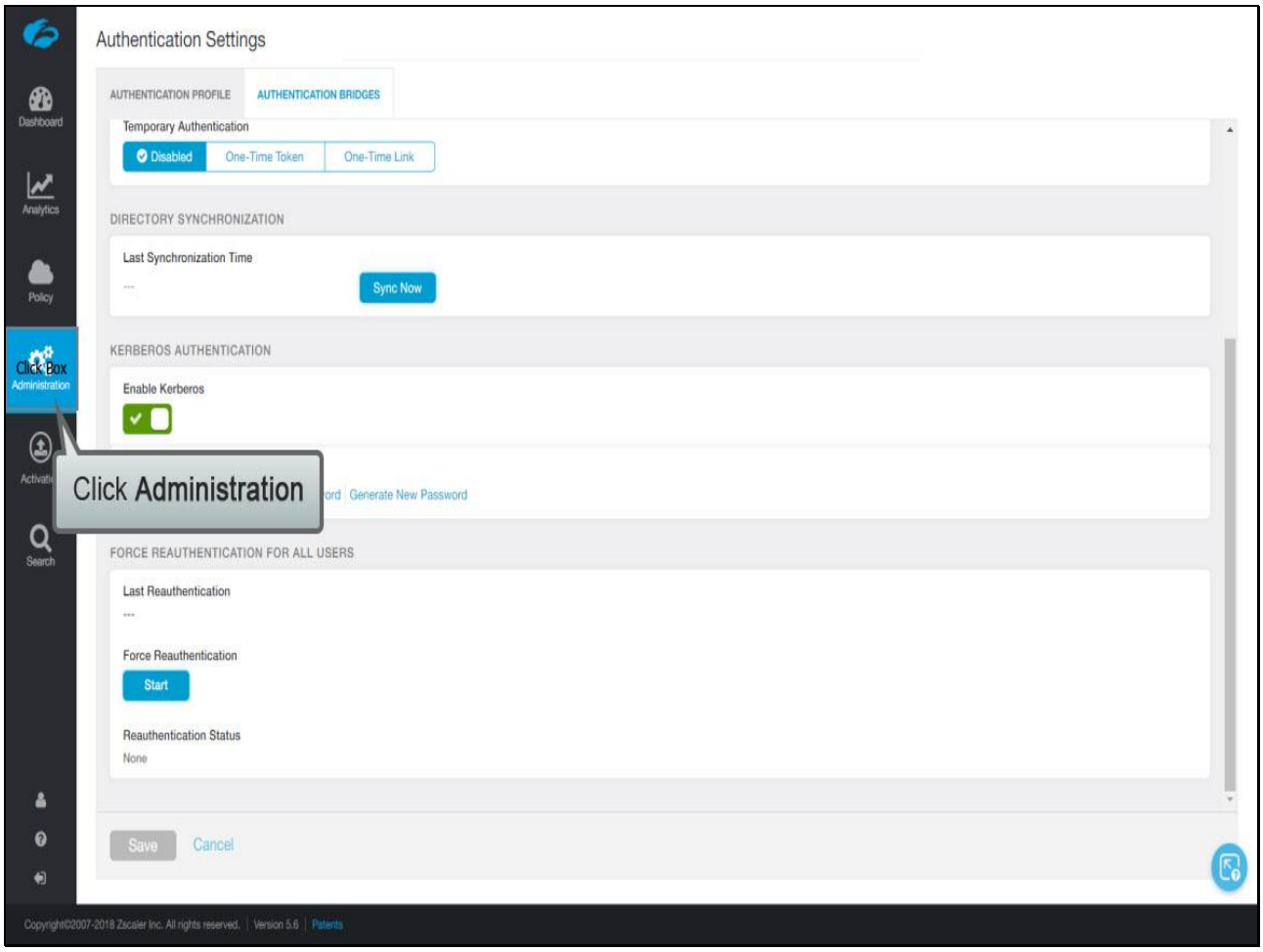
Slide notes

Slide 39 - Slide 39



Slide notes

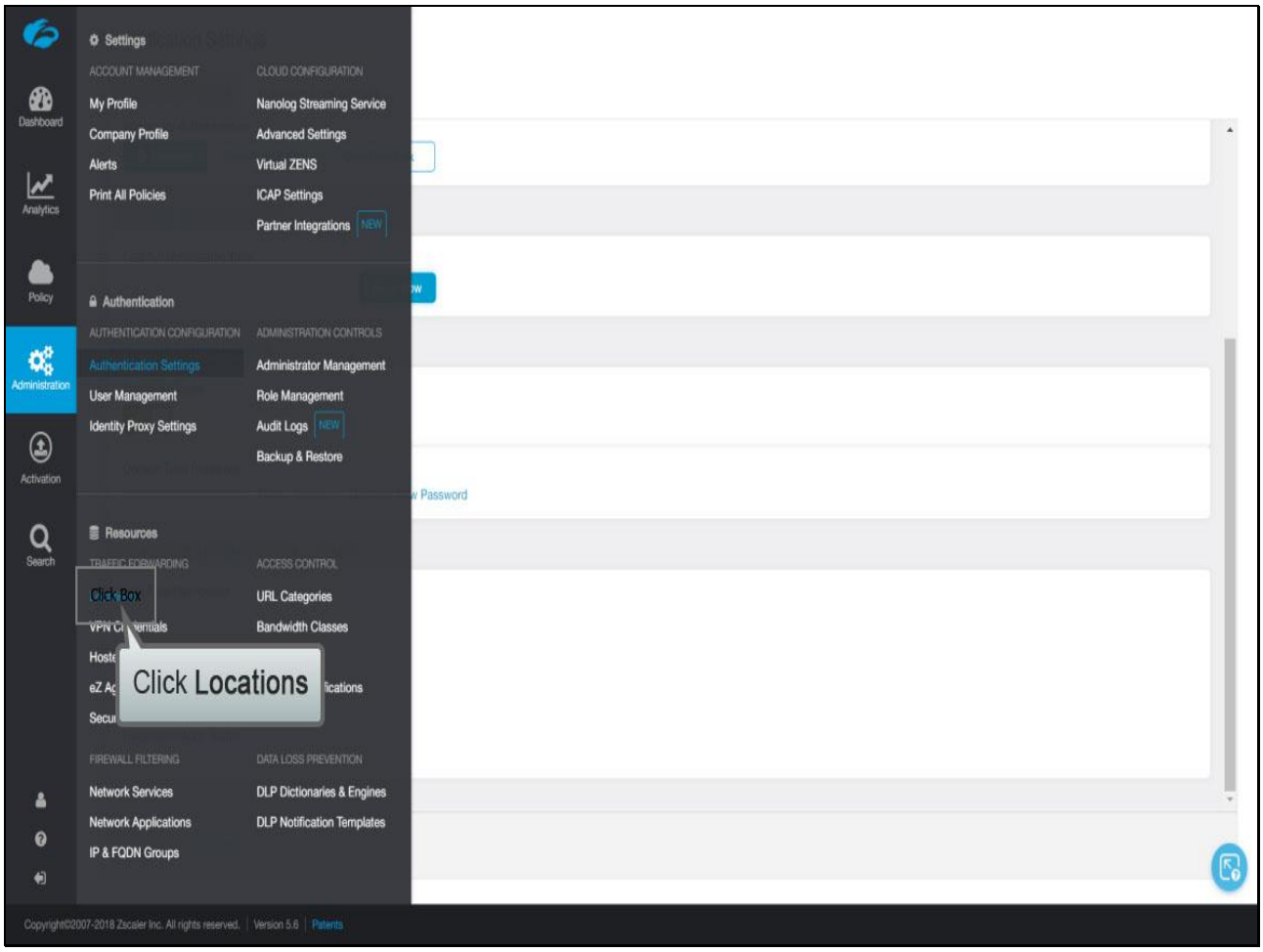
Slide 40 - Slide 40



Slide notes

Optionally, we can enable Kerberos on a location. Perform this task if you want to enforce Kerberos authentication for all web traffic from a location. Skip this step if you want to use Kerberos only for specific users and not others. Go to **Administration**.

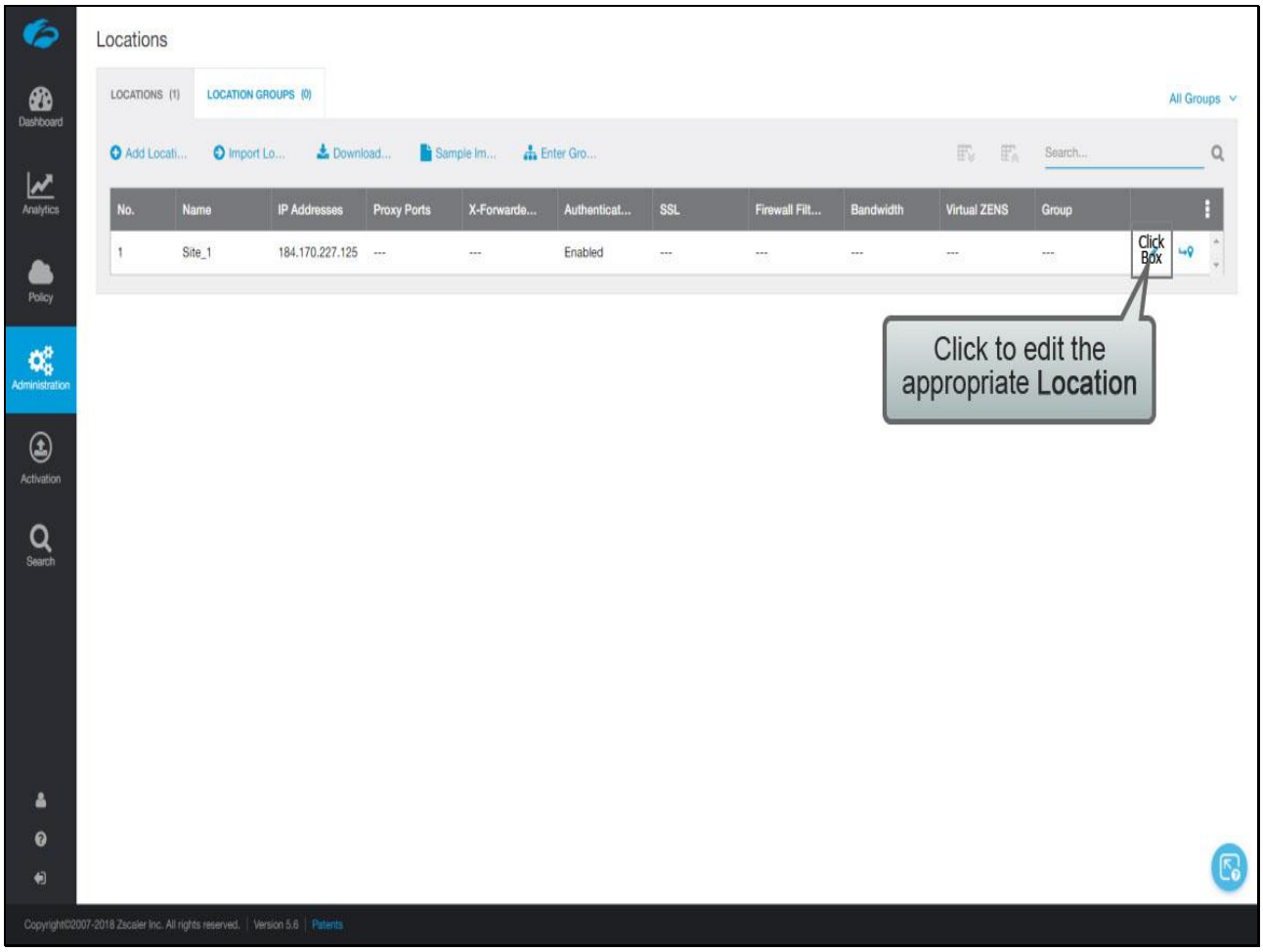
Slide 41 - Slide 41



Slide notes

Click on **Locations**, …

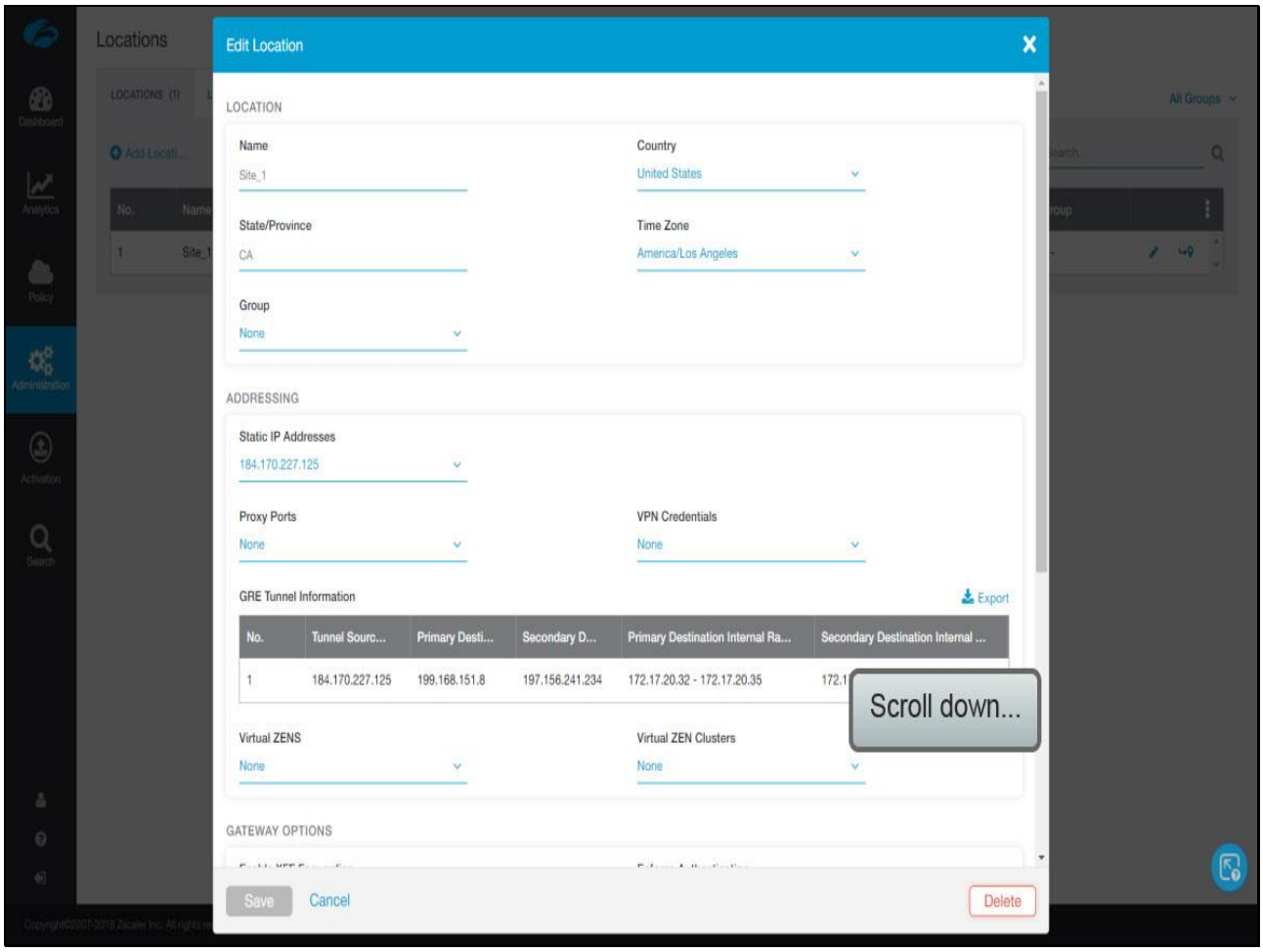
Slide 42 - Slide 42



Slide notes

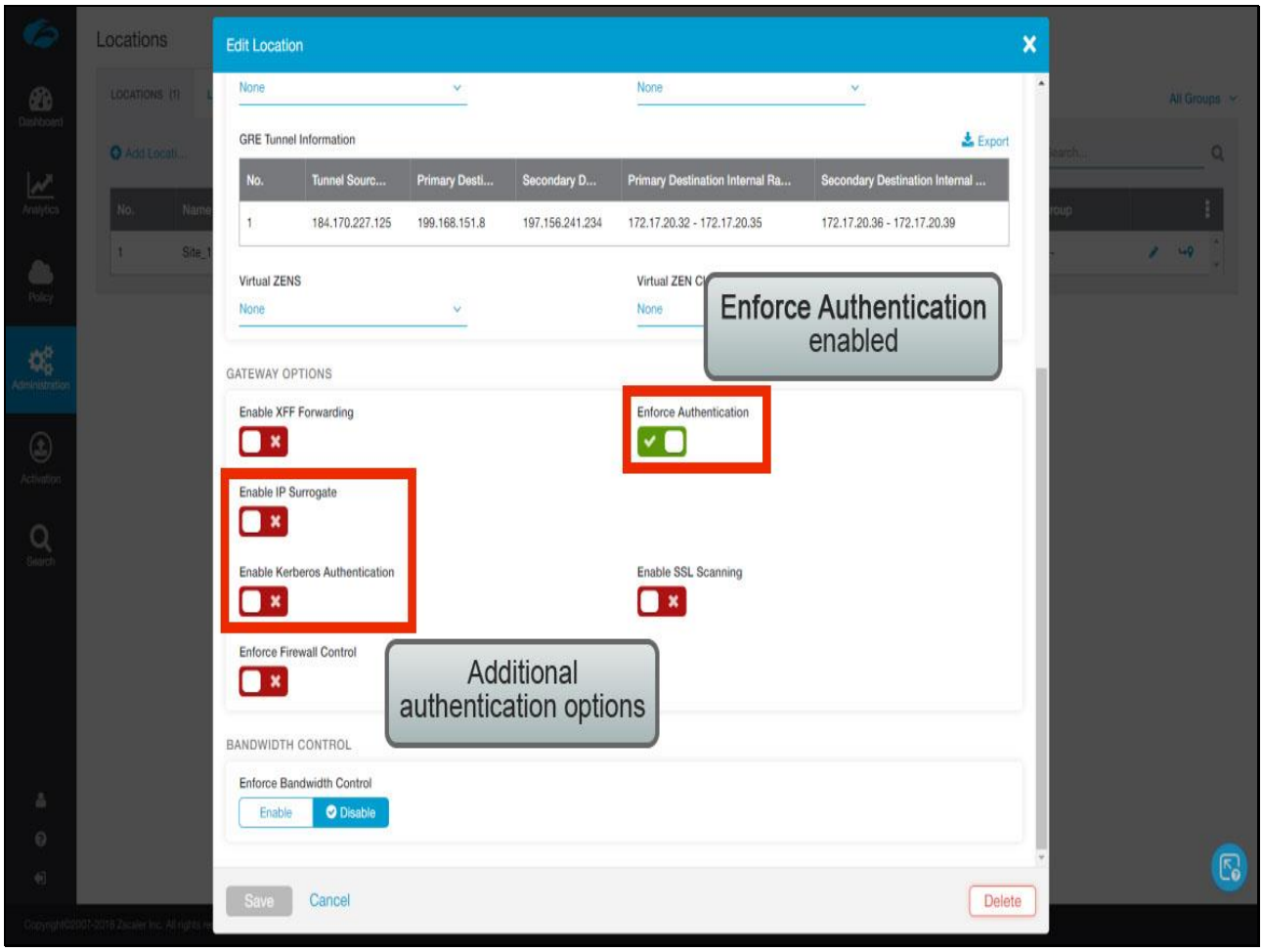
…then click **Edit**.

Slide 43 - Slide 43



Slide notes

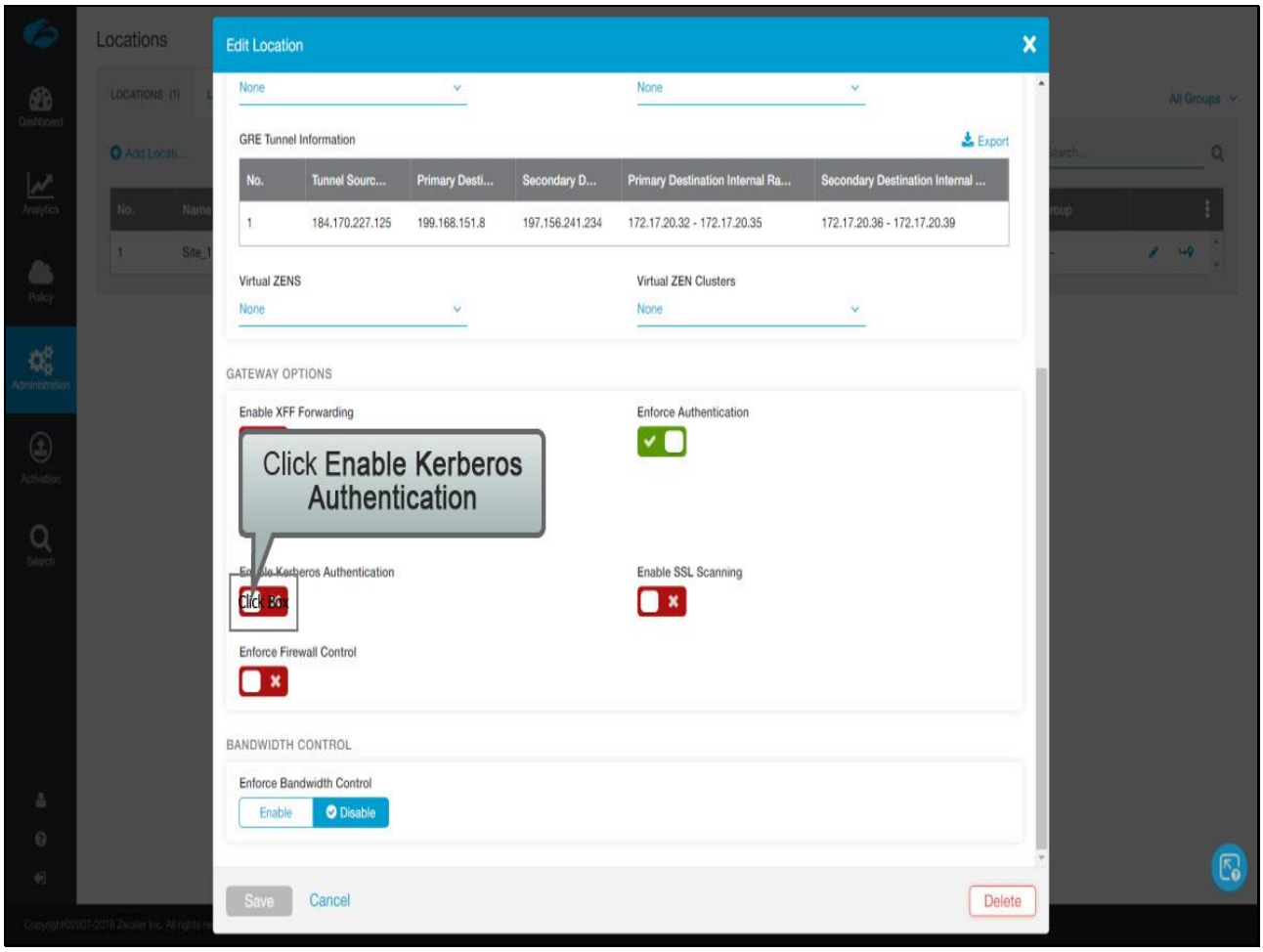
Slide 44 - Slide 44



Slide notes

Check **Enforce Authentication** if it is not already enabled. This will show additional configurables once selected.

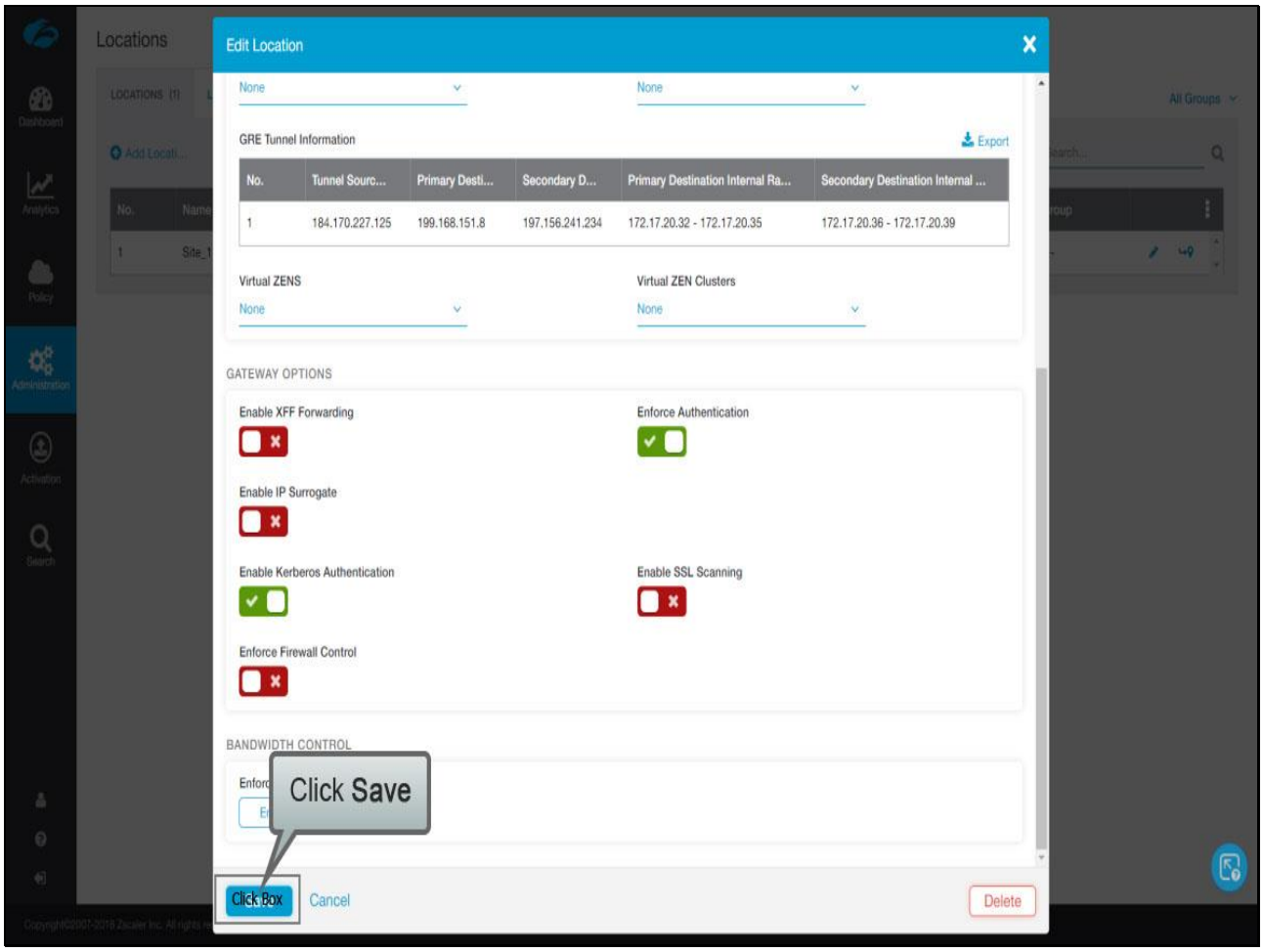
Slide 45 - Slide 45



Slide notes

Check **Enable Kerberos Authentication**, …

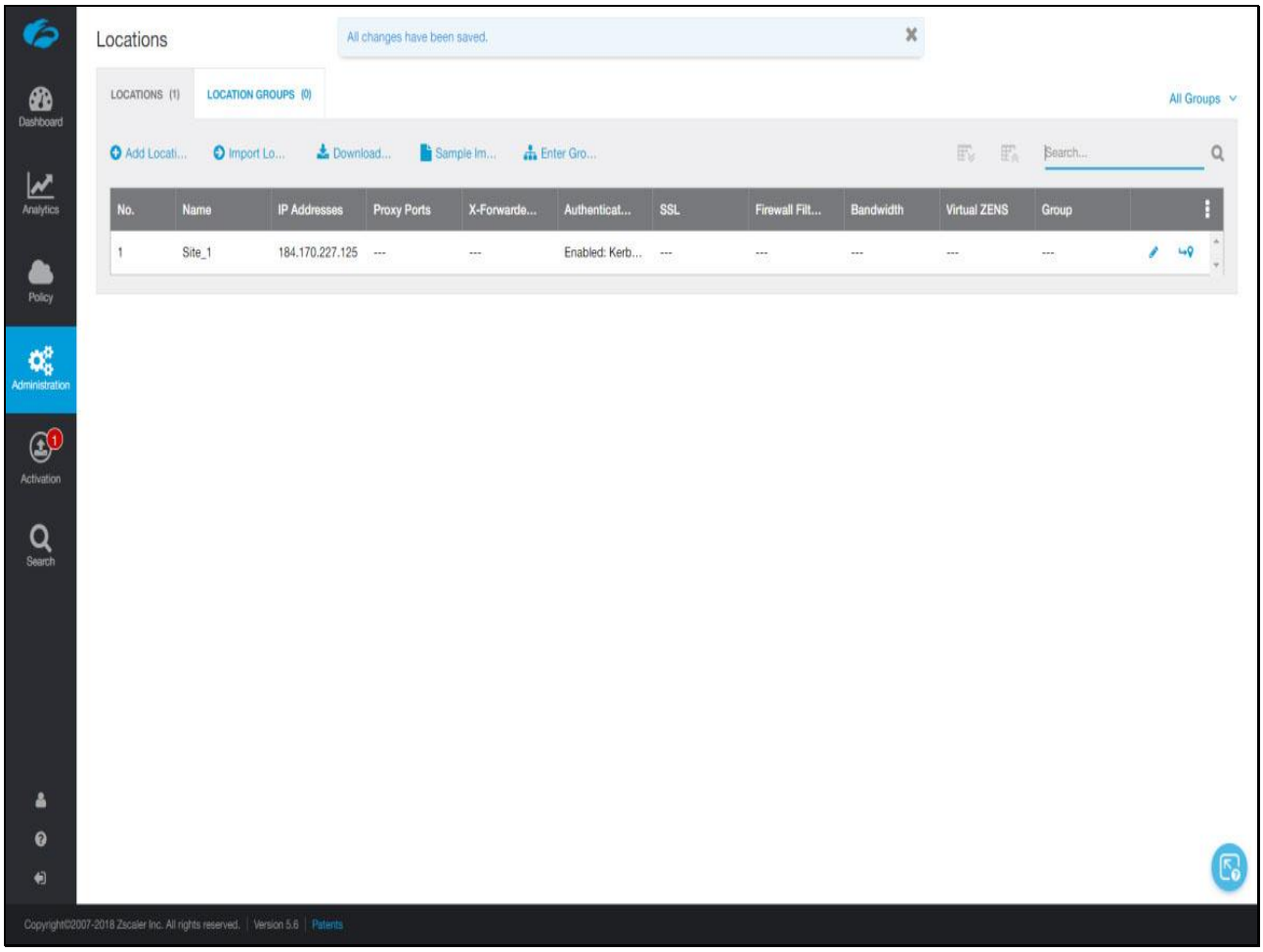
Slide 46 - Slide 46



Slide notes

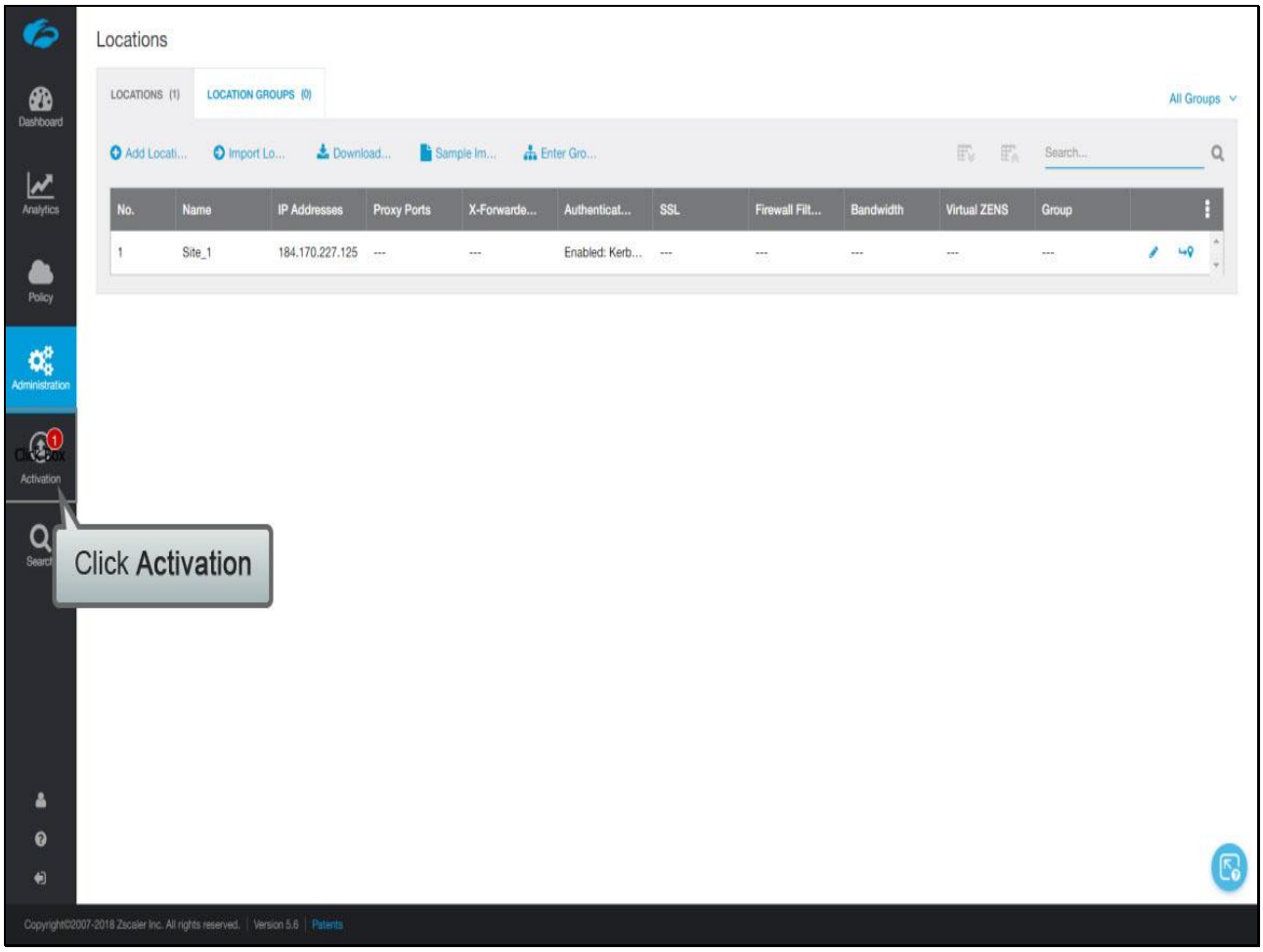
…then **Save** and **Activate** your changes.

Slide 47 - Slide 47



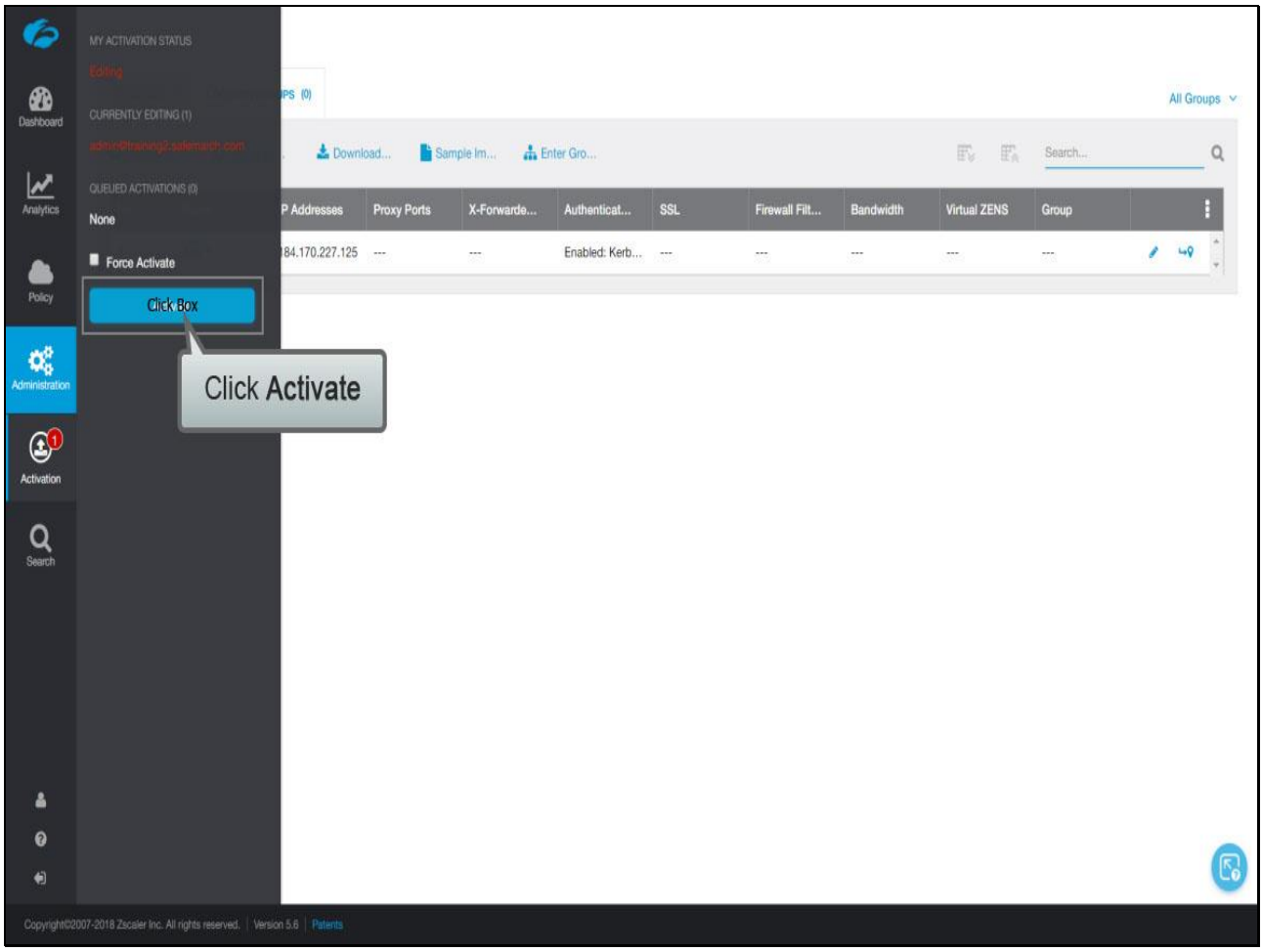
Slide notes

Slide 48 - Slide 48



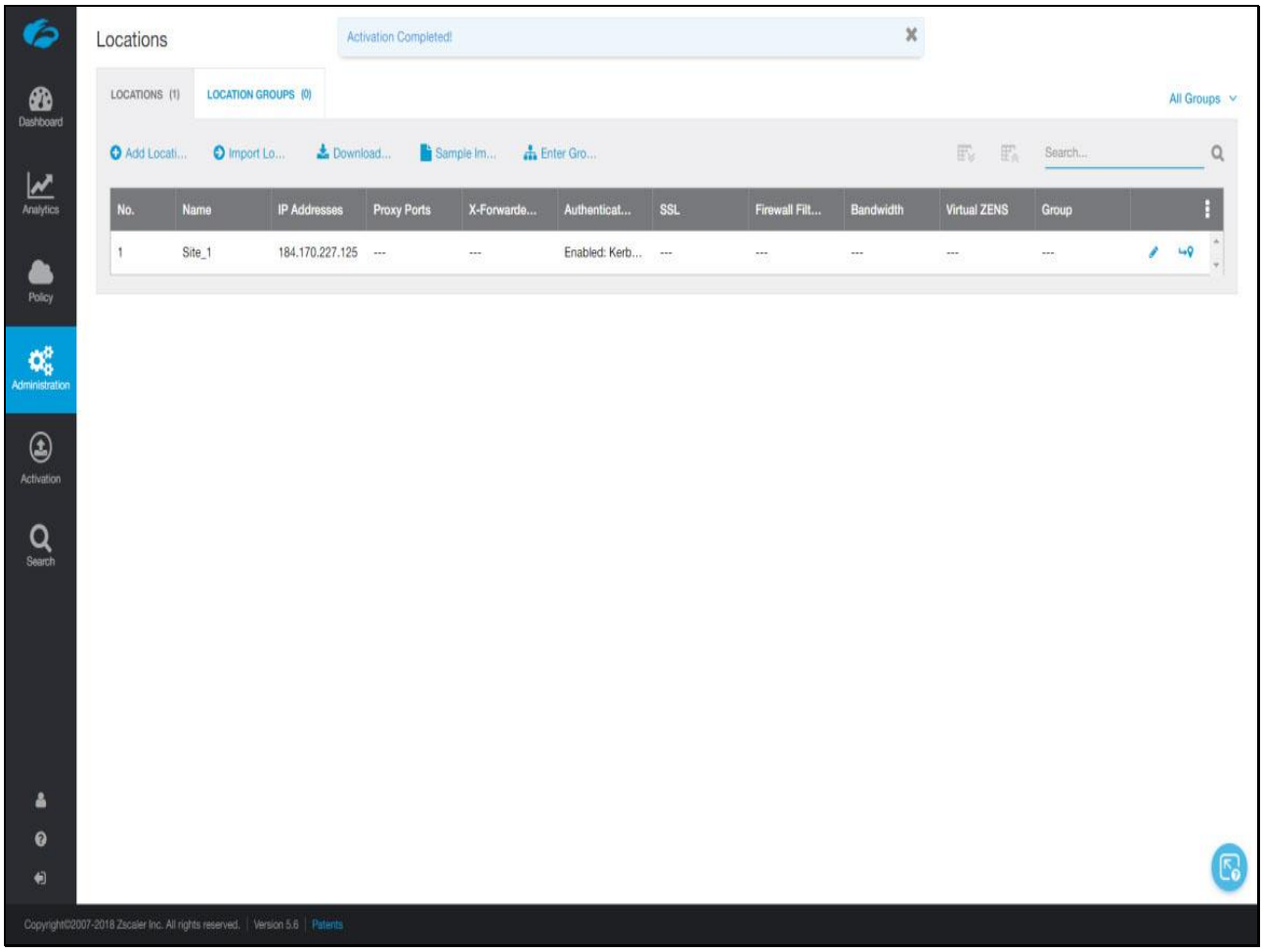
Slide notes

Slide 49 - Slide 49



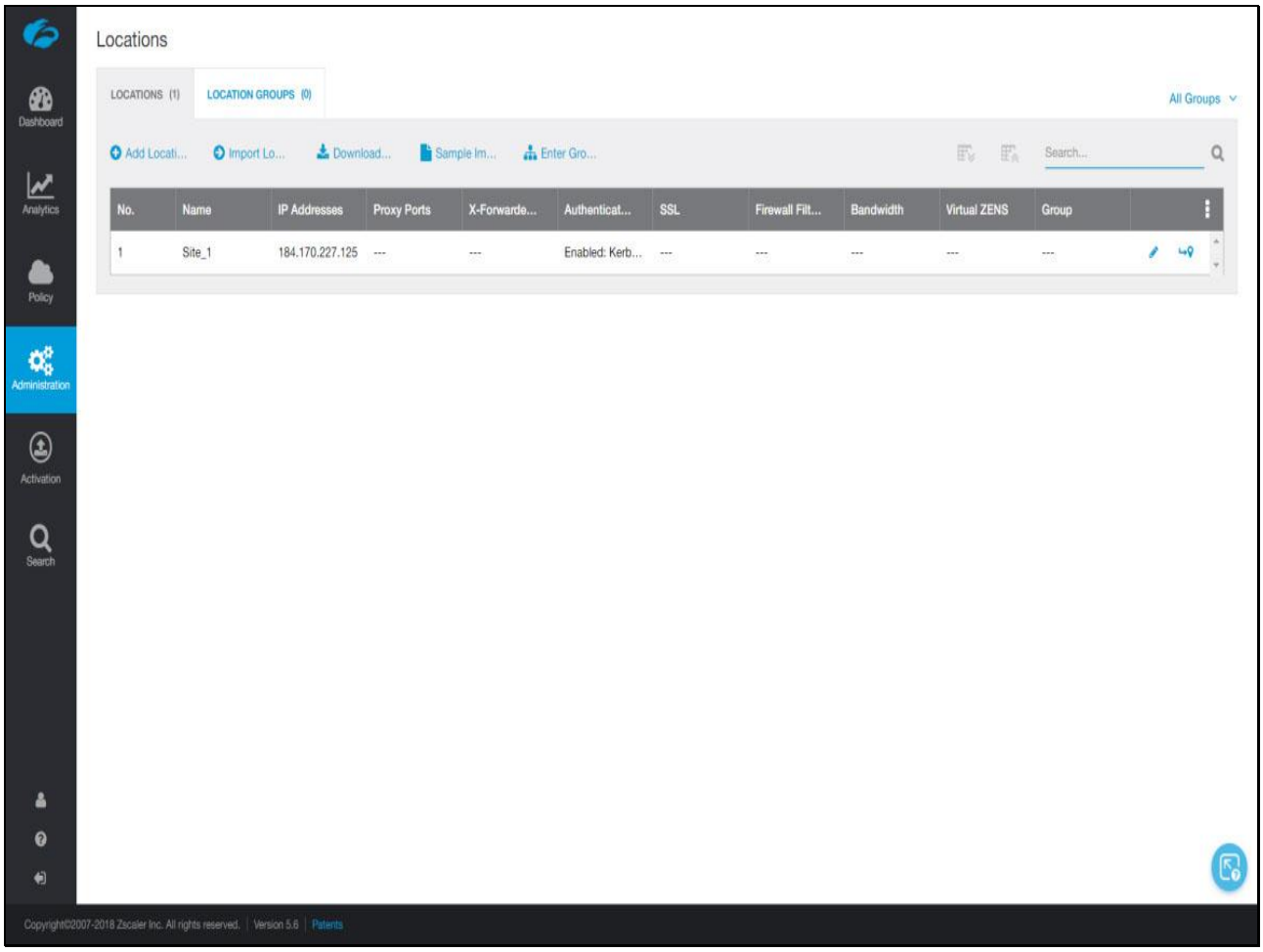
Slide notes

Slide 50 - Slide 50



Slide notes

Slide 51 - Slide 51



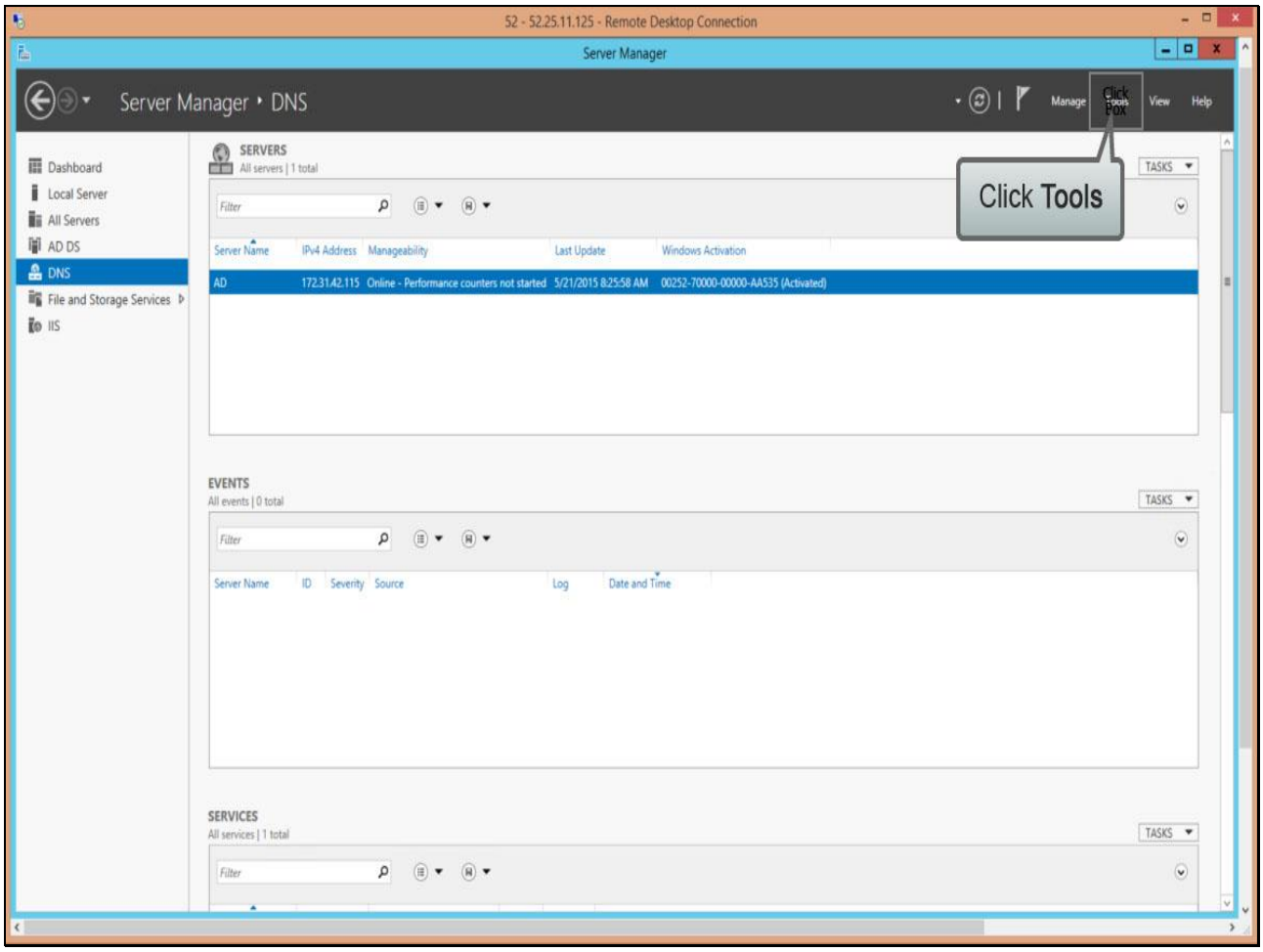
Slide notes

Slide 52 - Windows Server 2012 Configuration

Slide notes

This configuration example will illustrate how to establish a one-way cross-realm trust from your organization to the Zscaler service on Windows Server 2012. This one-way trust enables Zscaler to trust the authenticated users of the domain and NOT the reverse.

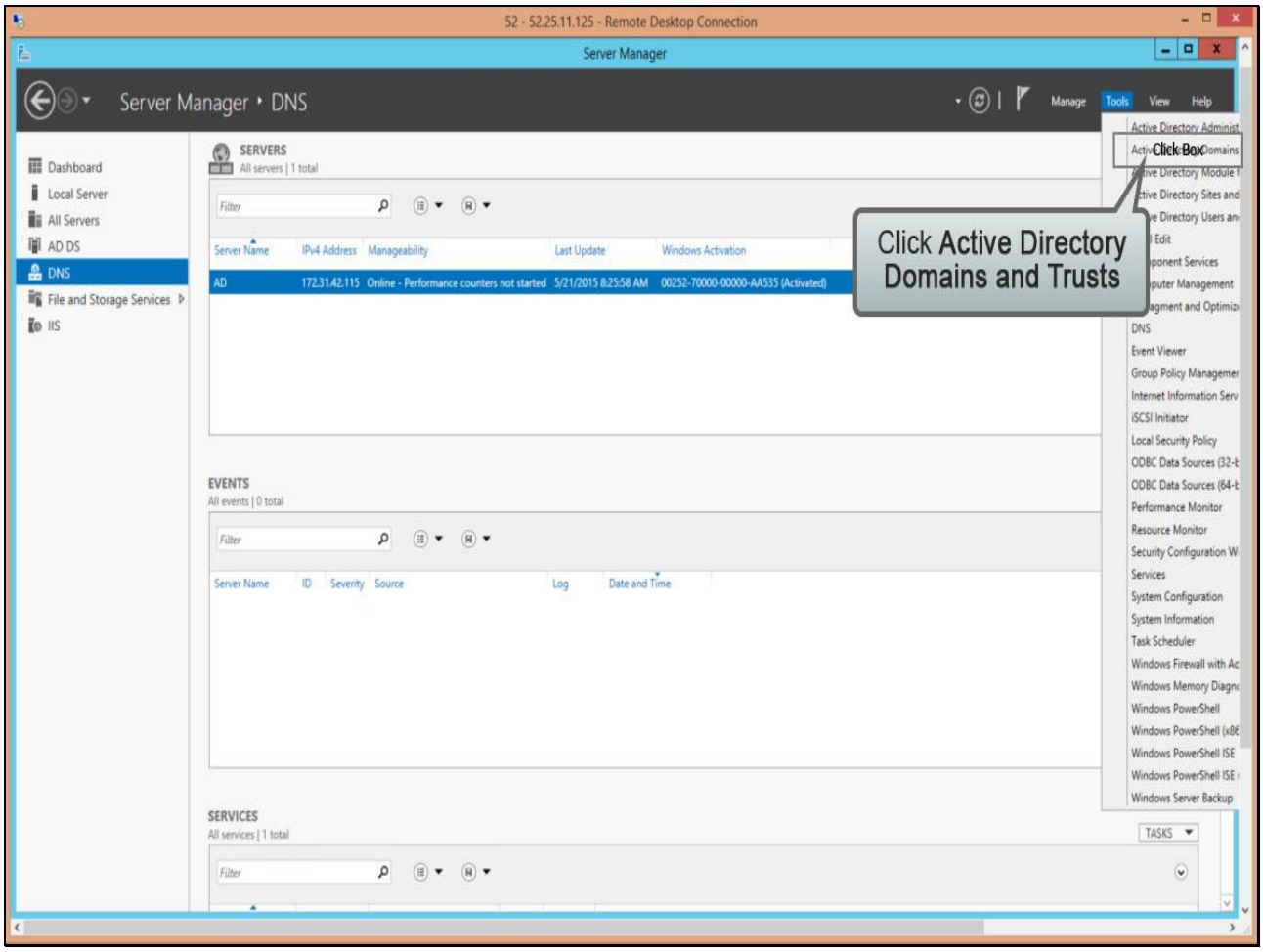
Slide 53 - Slide 53



Slide notes

Begin in the Server Manager then click on **Tools** in the upper right corner.

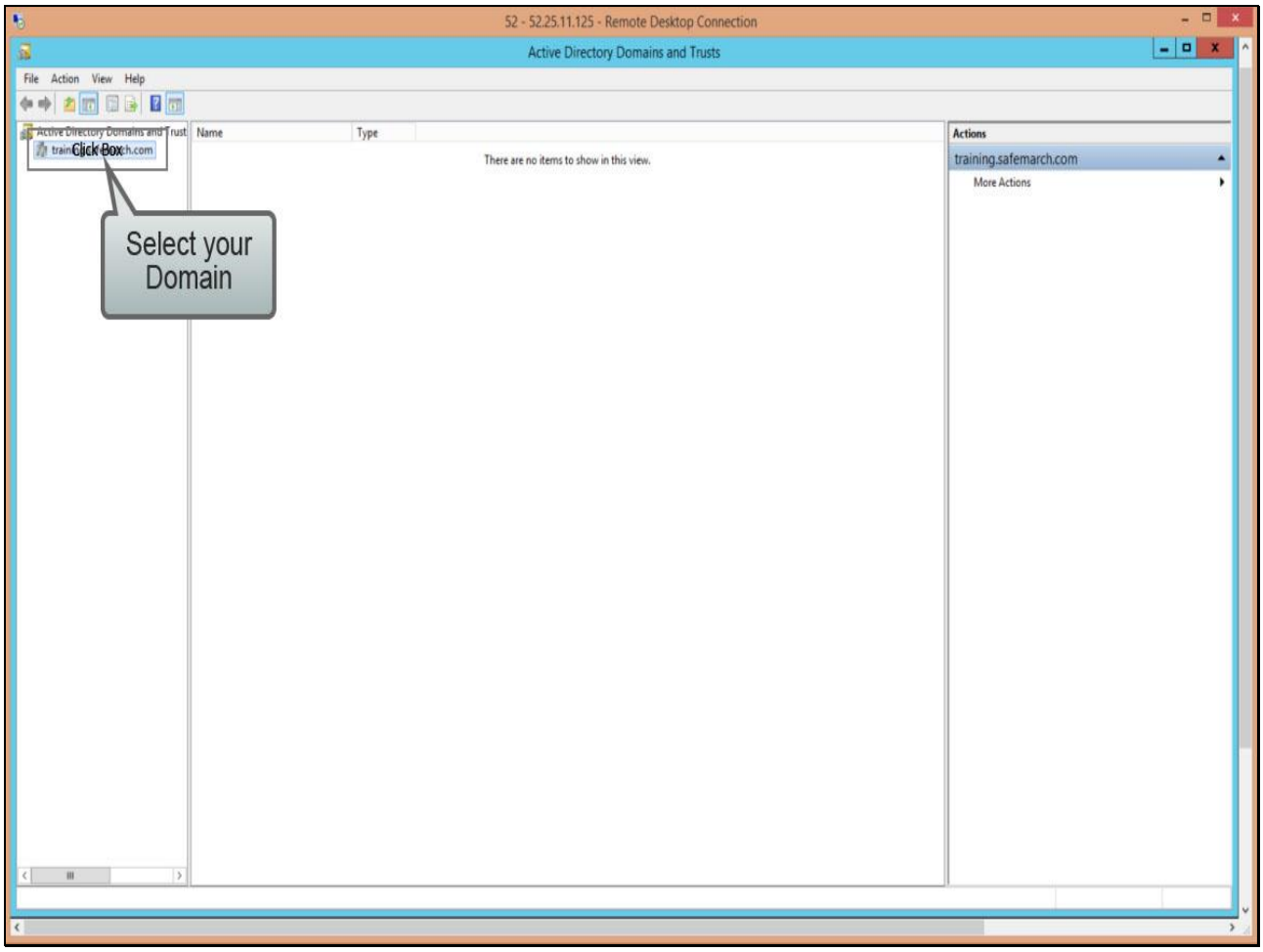
Slide 54 - Slide 54



Slide notes

Select **Active Directory Domains and Trusts**.

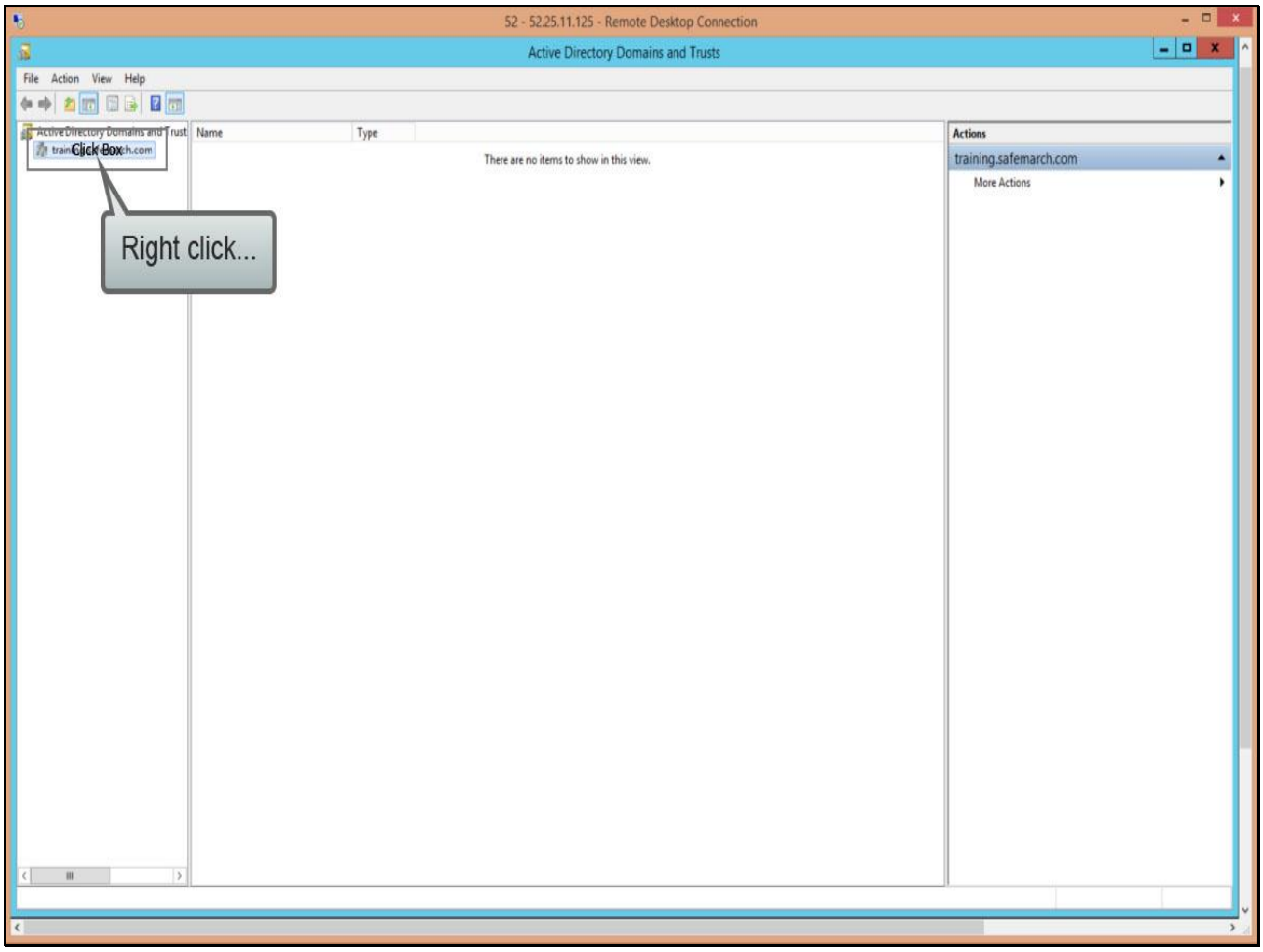
Slide 55 - Slide 55



Slide notes

Highlight your Domain, …

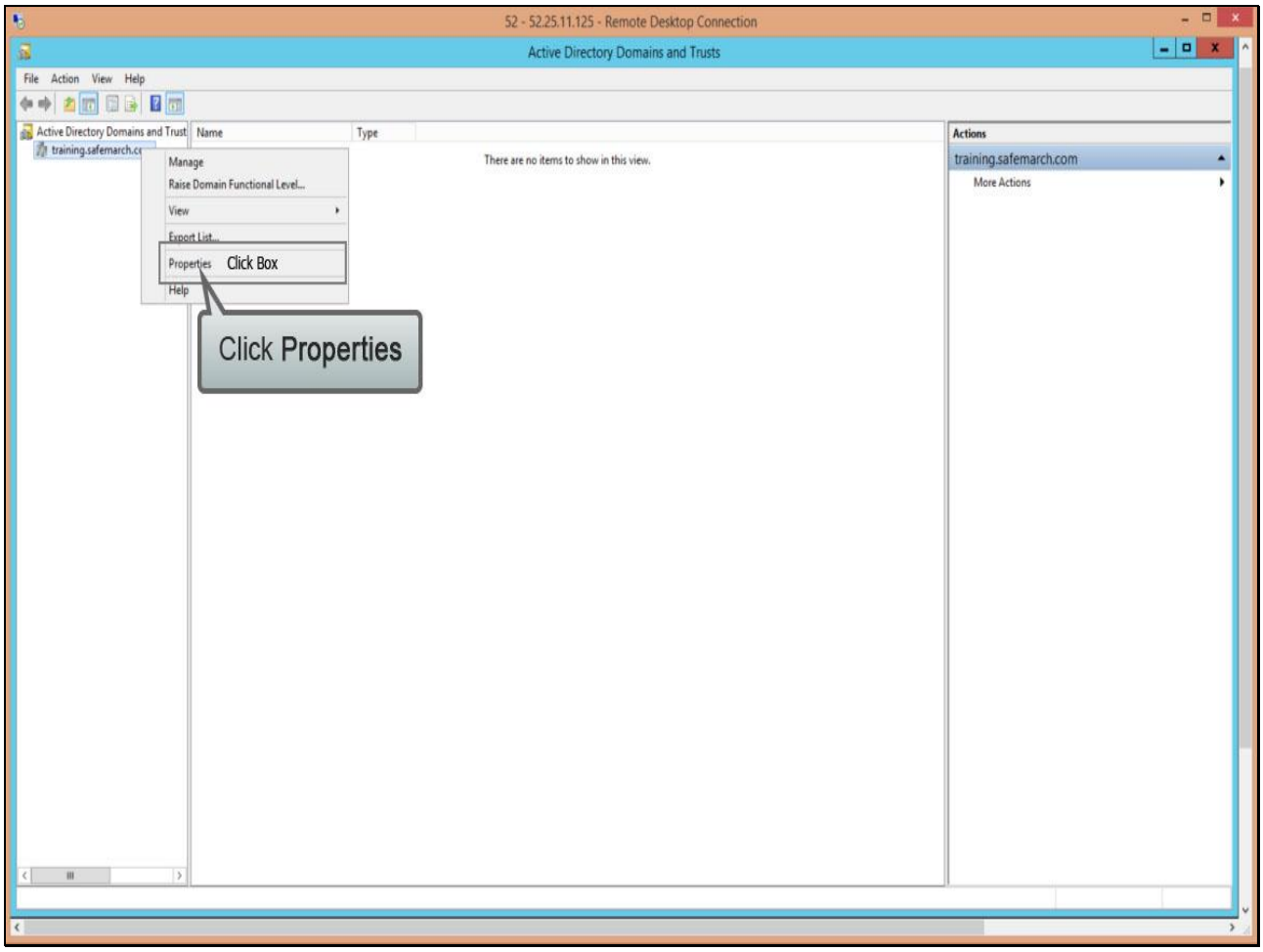
Slide 56 - Slide 56



Slide notes

…right-click, …

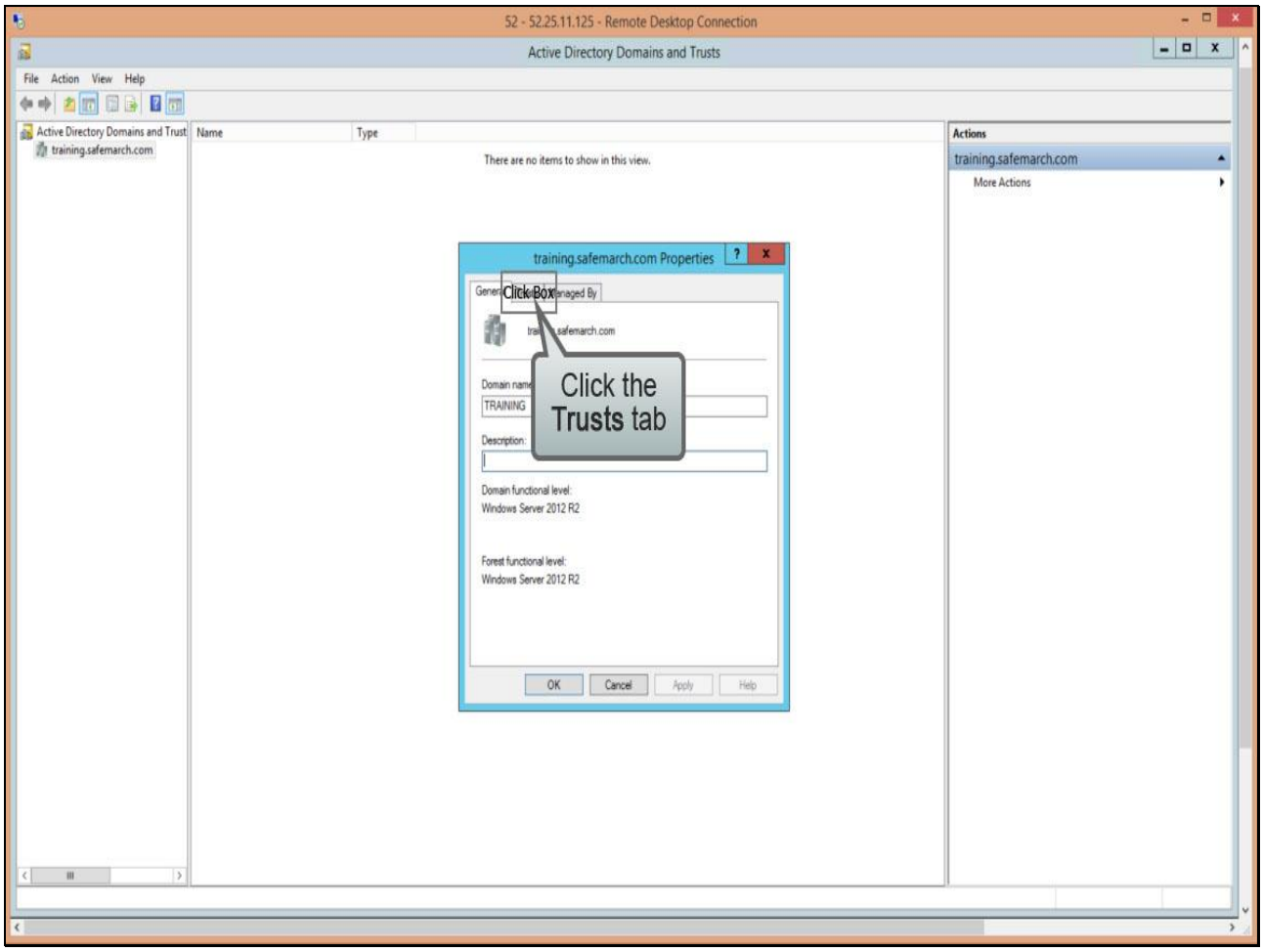
Slide 57 - Slide 57



Slide notes

…and select **Properties**.

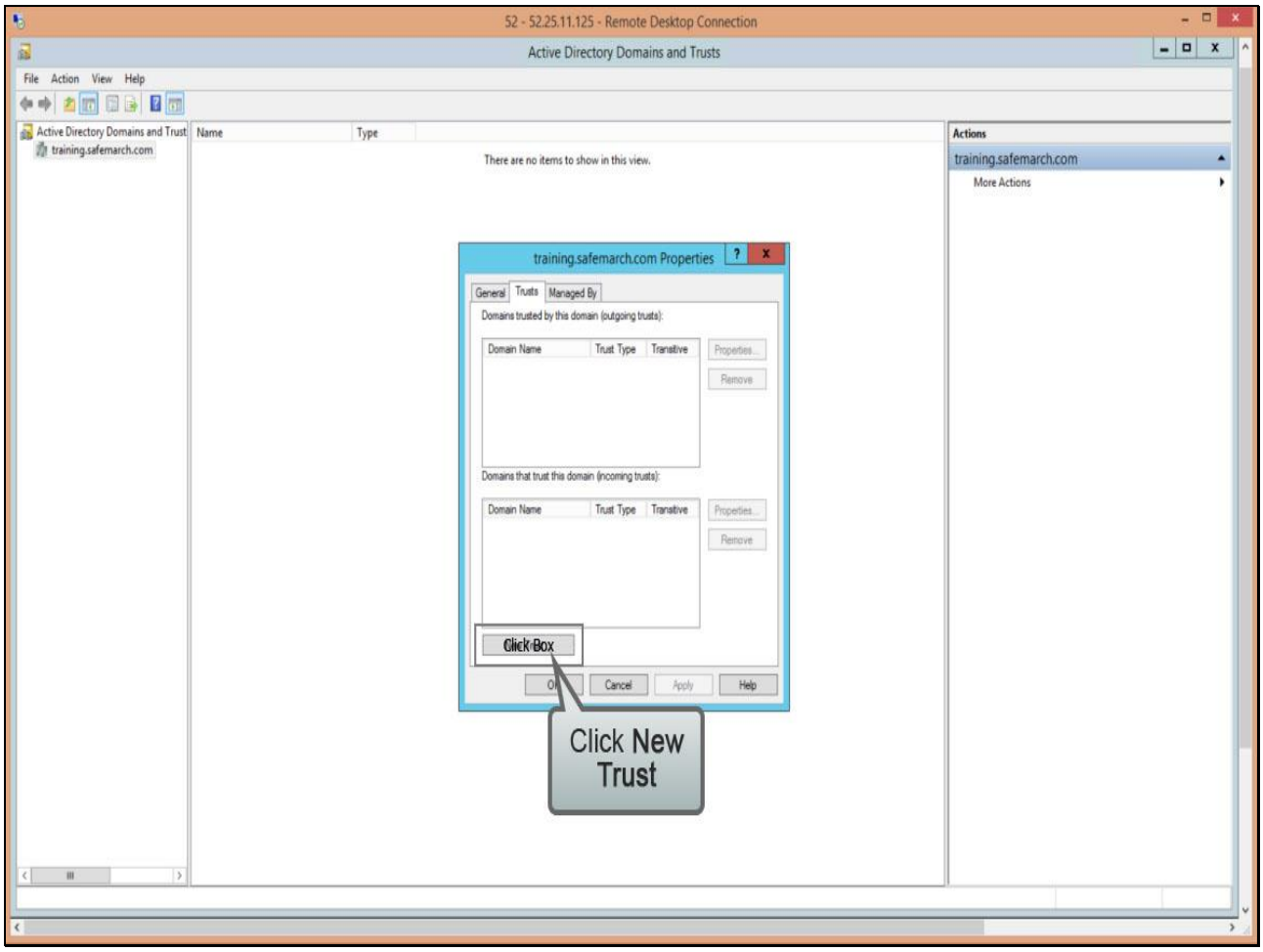
Slide 58 - Slide 58



Slide notes

In the properties window go to the **Trusts** tab.

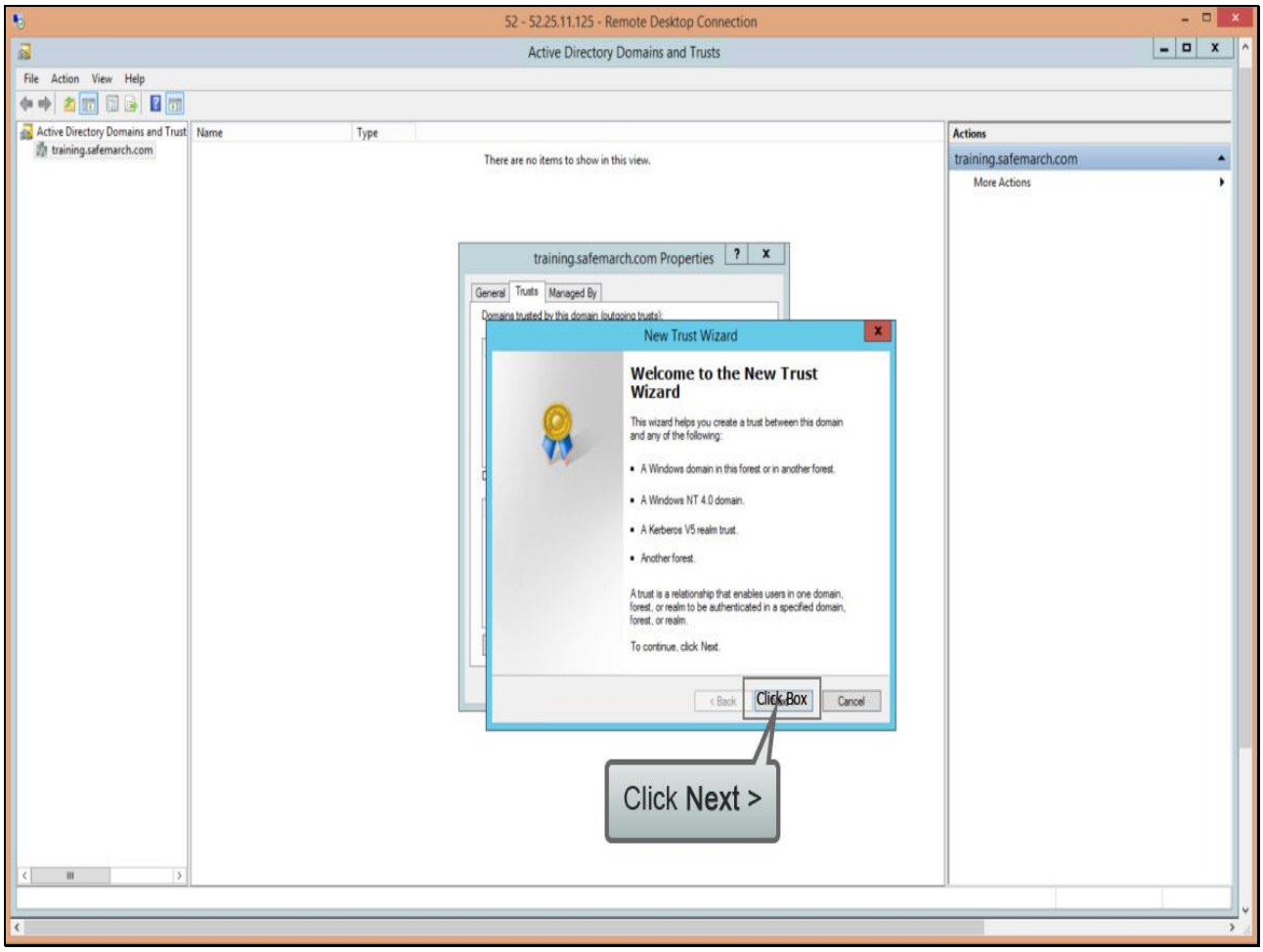
Slide 59 - Slide 59



Slide notes

Click **New Trust**, …

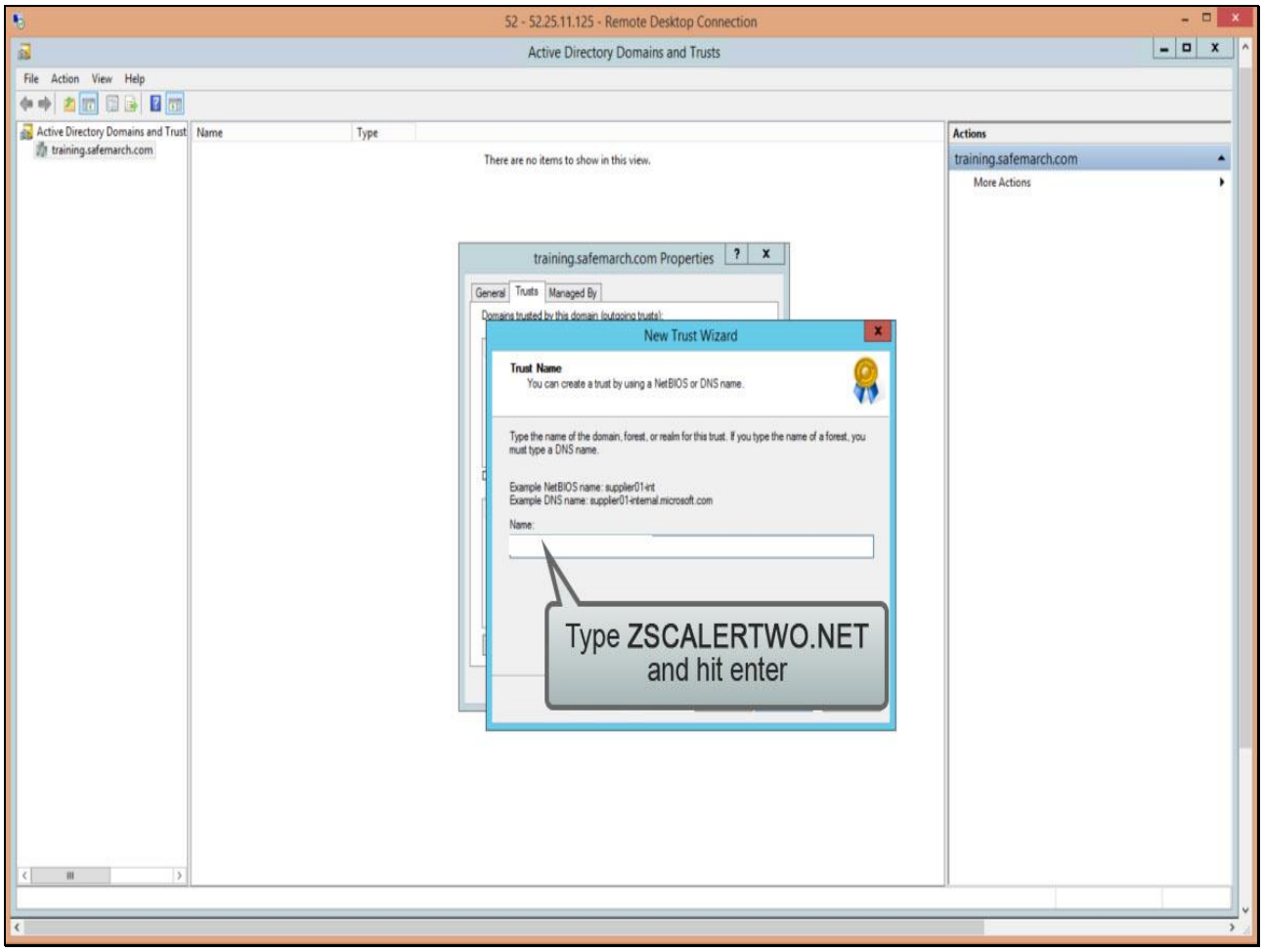
Slide 60 - Slide 60



Slide notes

…this starts the **New Trust Wizard**. Click **Next**.

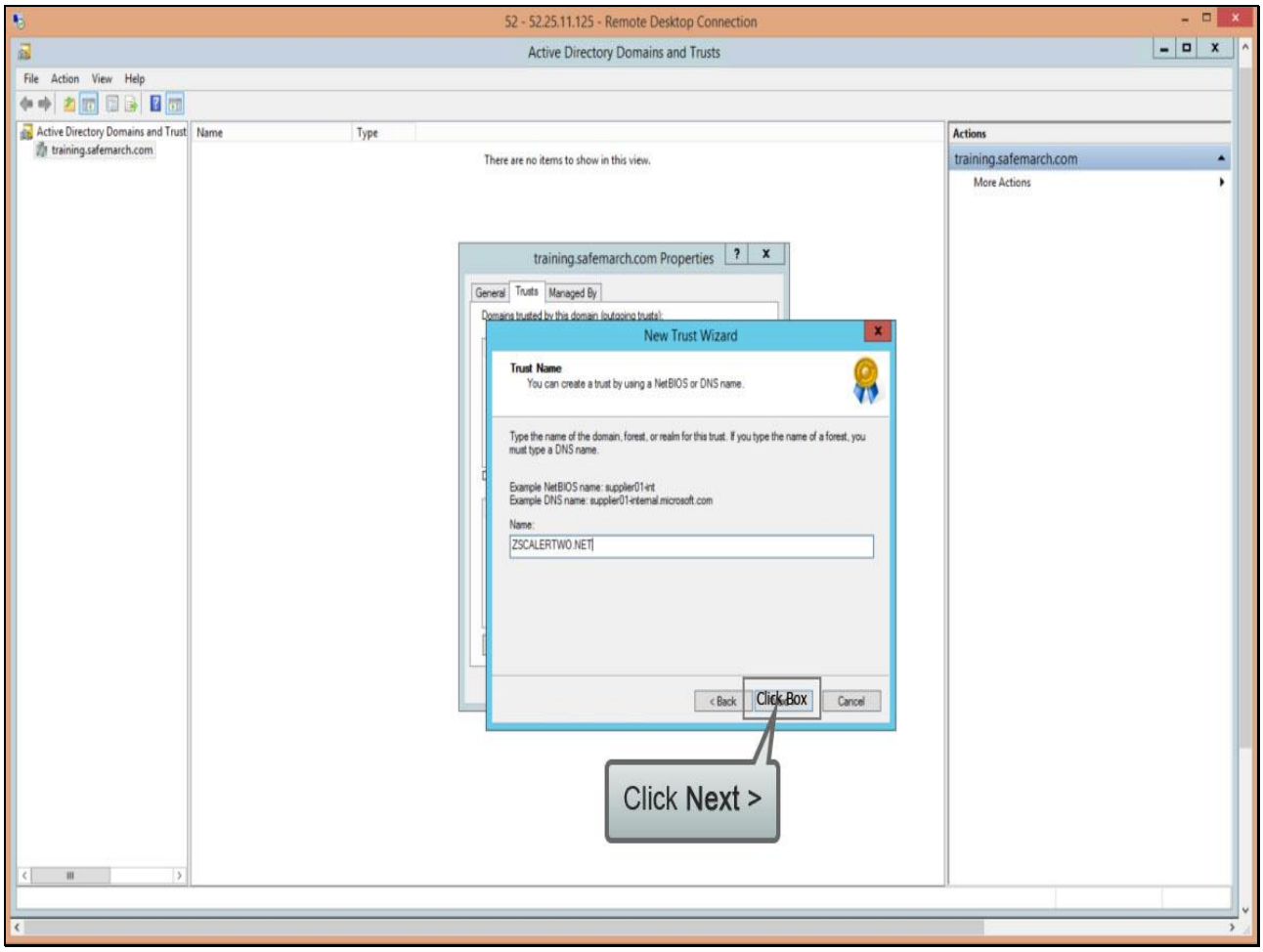
Slide 61 - Slide 61



Slide notes

For the trust **Name** enter the Zscaler cloud name you are assigned to in all UPPER CASE. In this example this account is provisioned on the **ZSCALERTWO.NET** cloud.

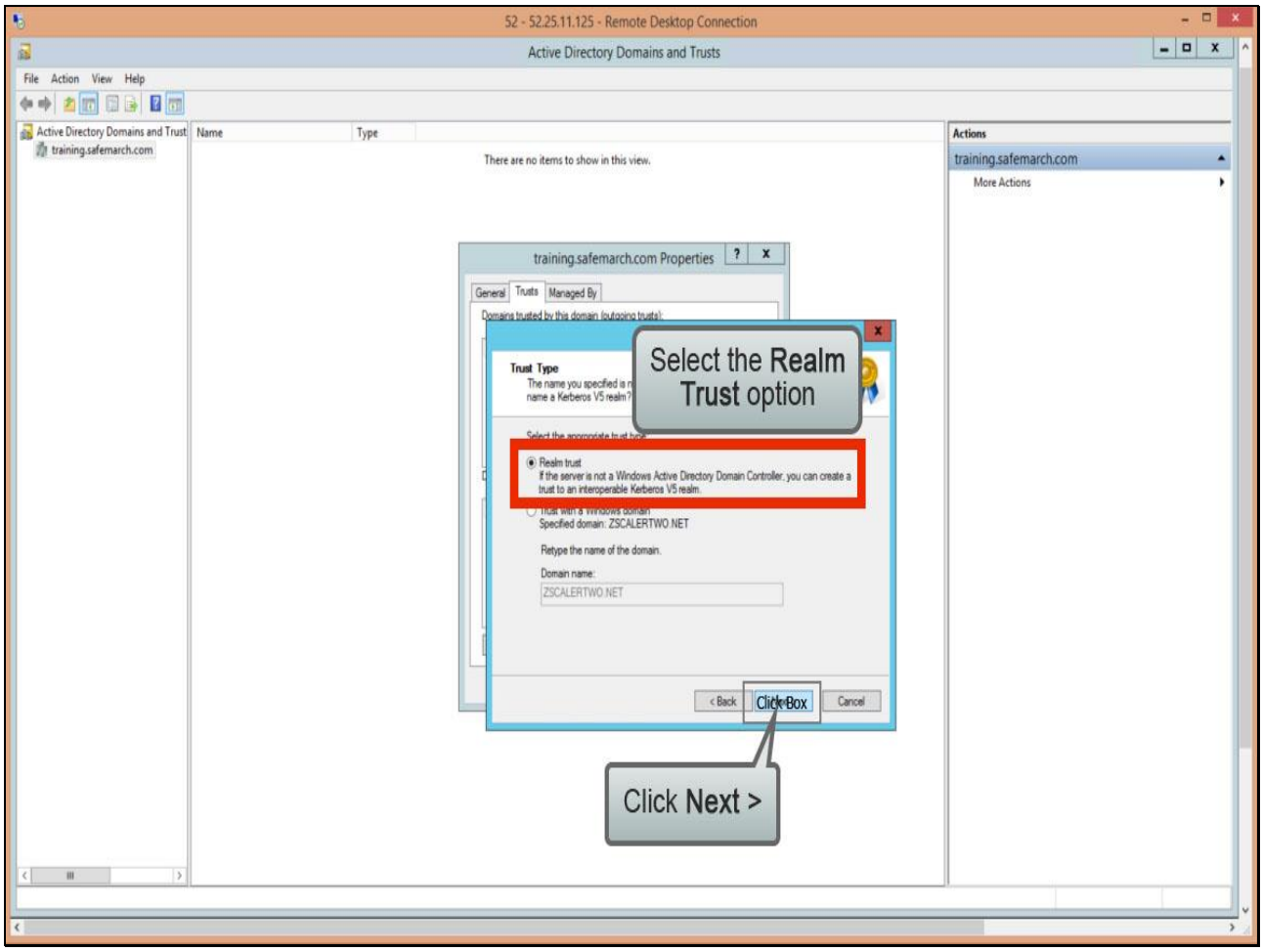
Slide 62 - Slide 62



Slide notes

Click **Next**, …

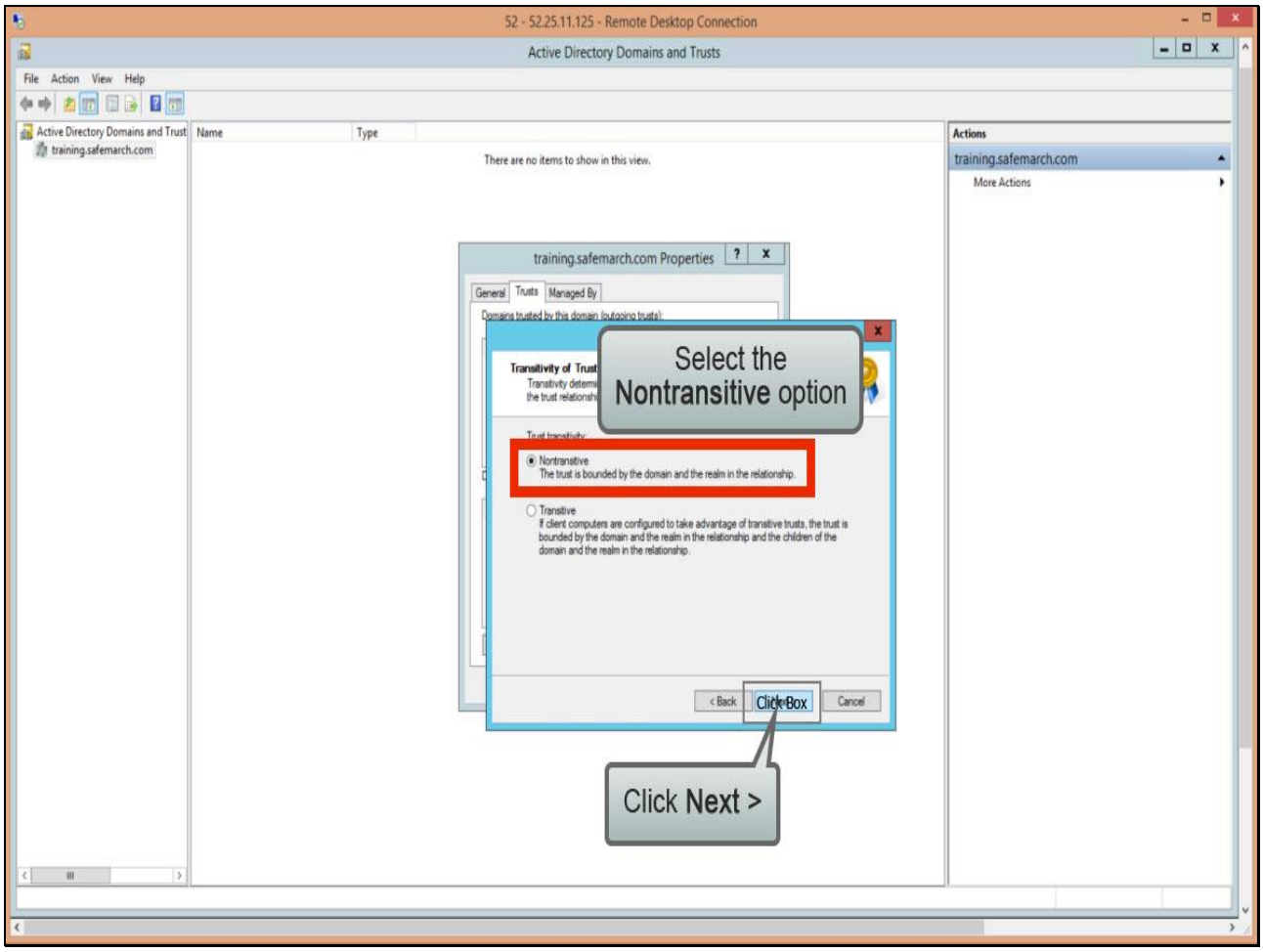
Slide 63 - Slide 63



Slide notes

…for the **Trust Type** select **Realm Trust** and click **Next**.

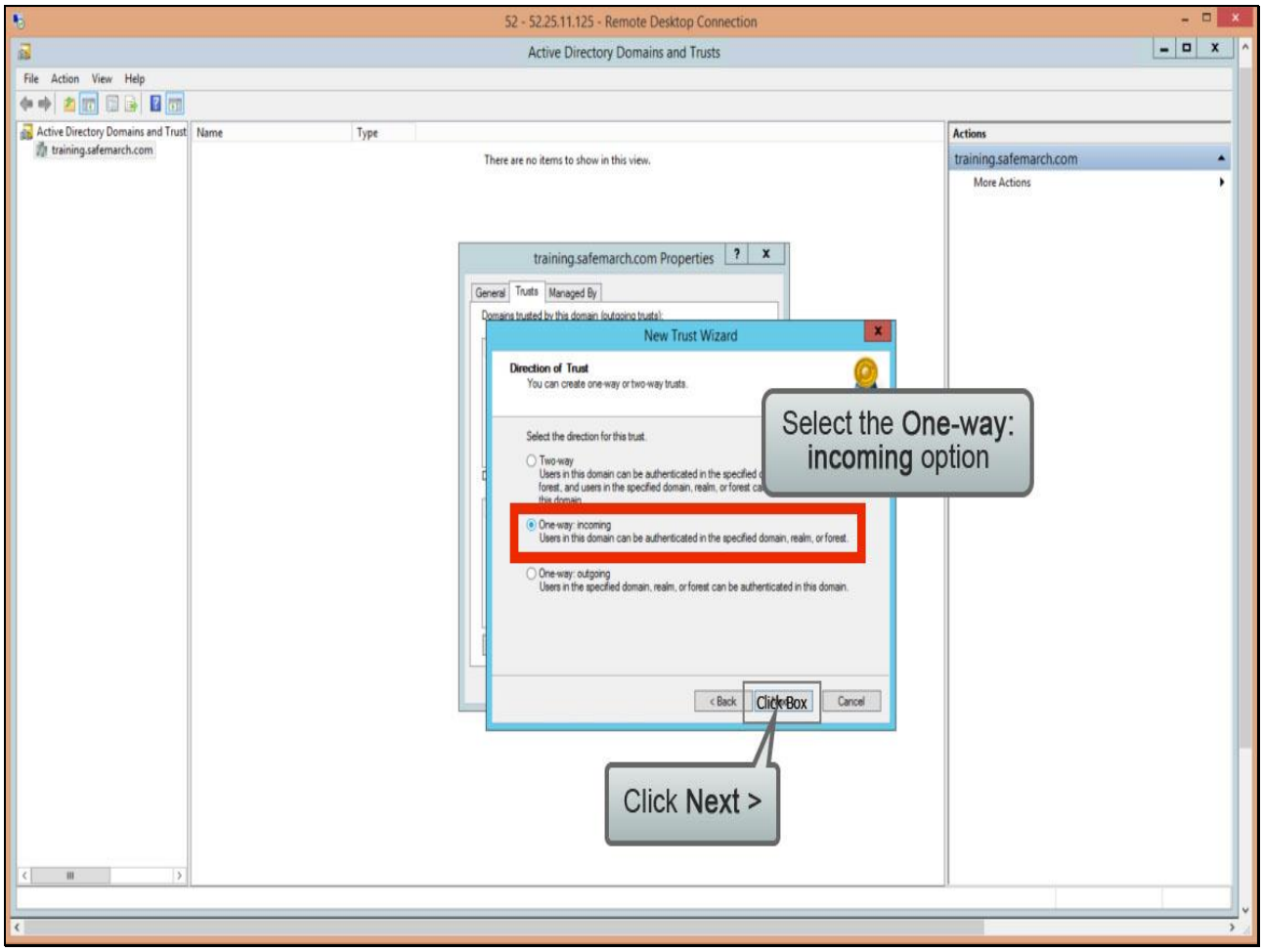
Slide 64 - Slide 64



Slide notes

Select **Nontransitive** and click **Next**.

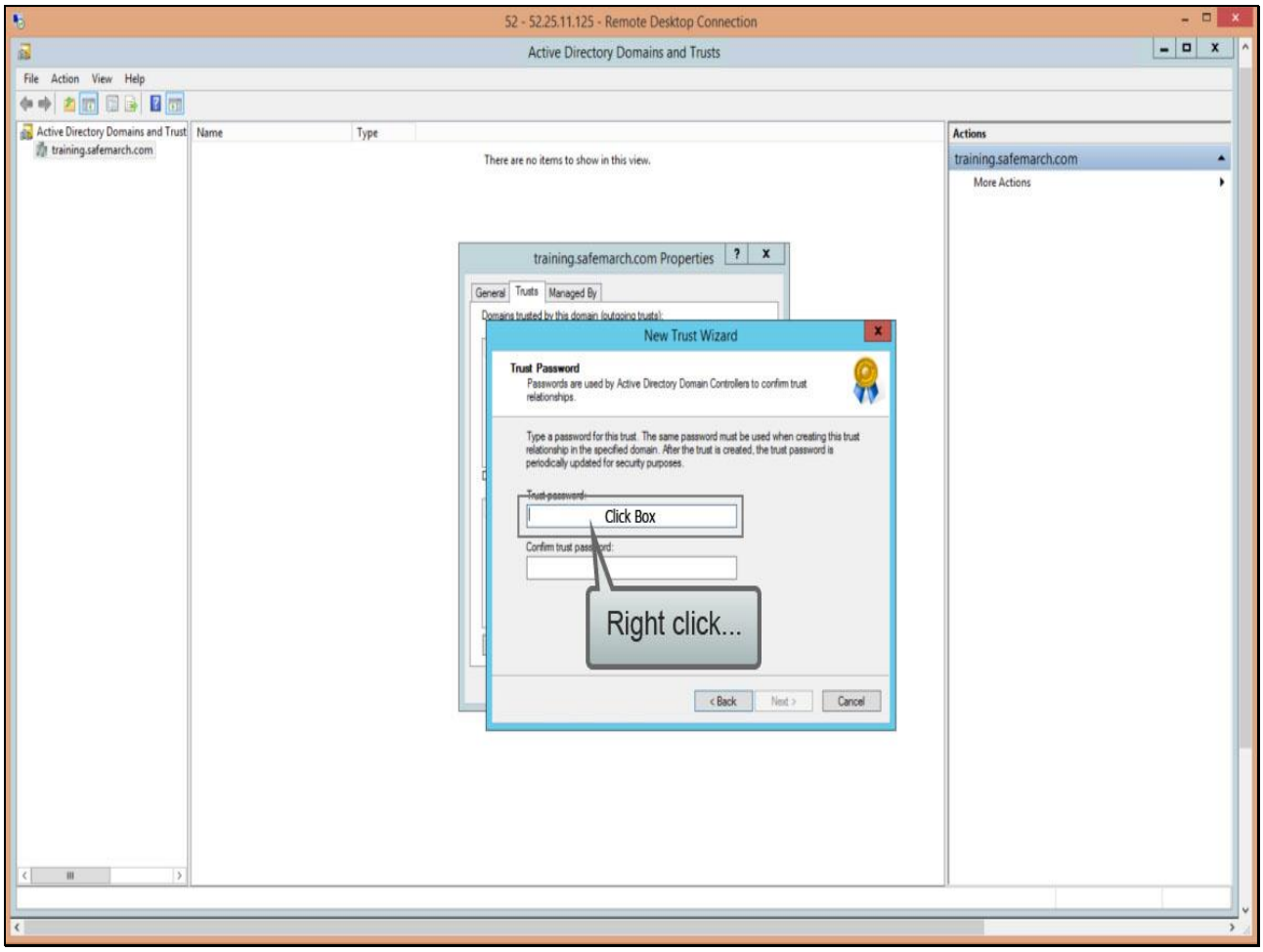
Slide 65 - Slide 65



Slide notes

For the **Direction of Trust** select **One-way Incoming** and click **Next**.

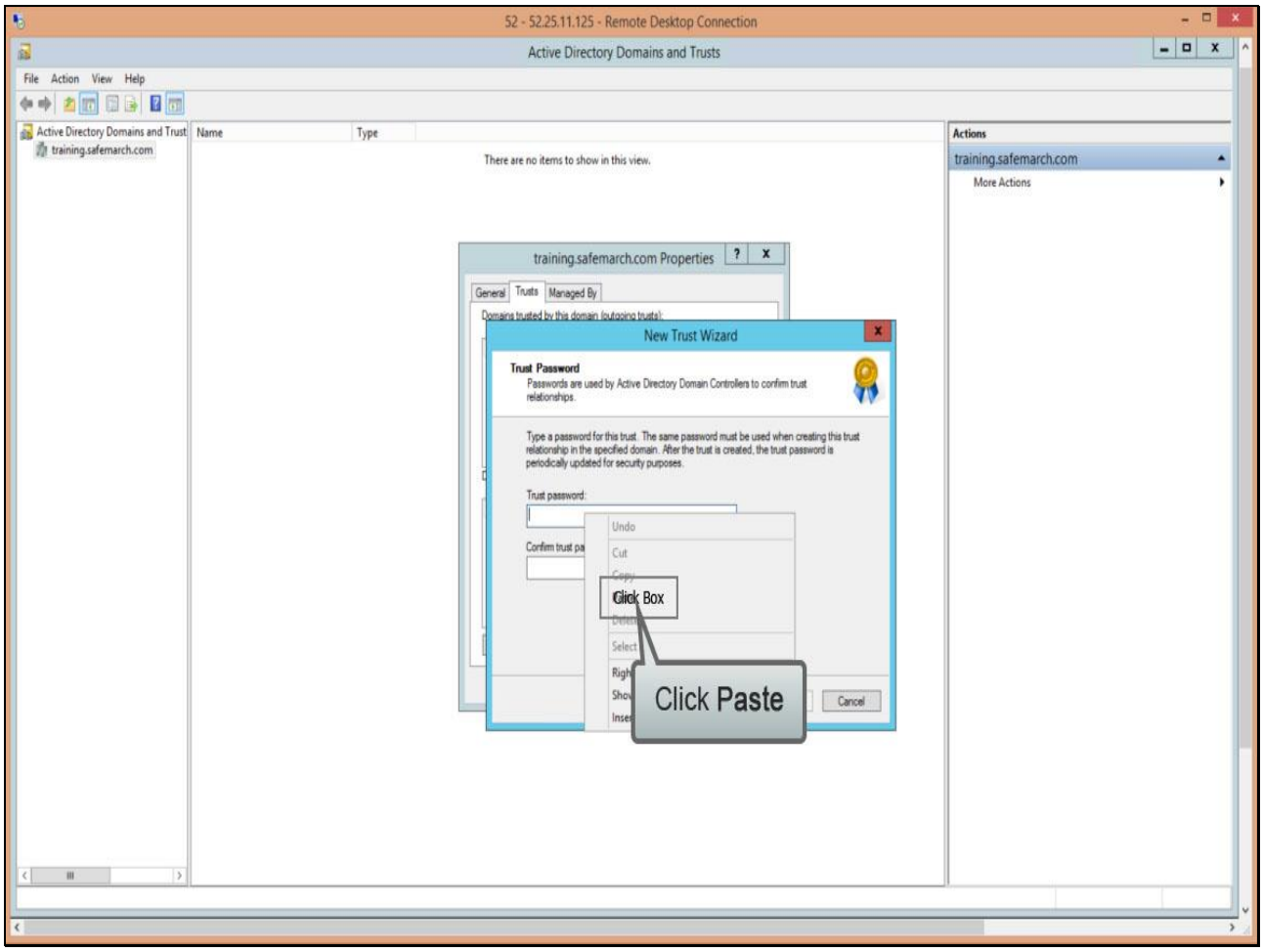
Slide 66 - Slide 66



Slide notes

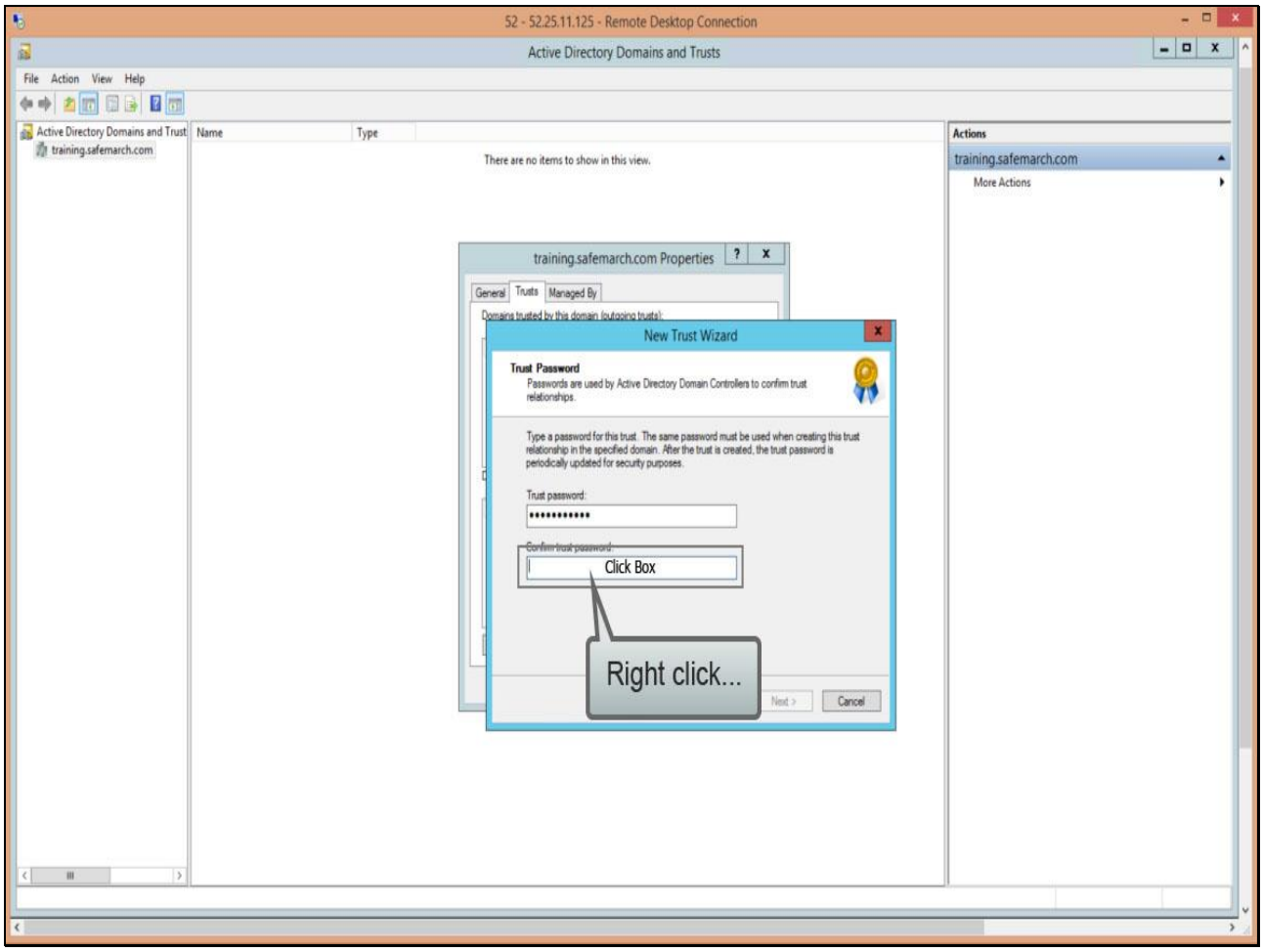
For the **Trust Password** paste in the Trust password that was copied earlier from the Zscaler Admin Portal.

Slide 67 - Slide 67



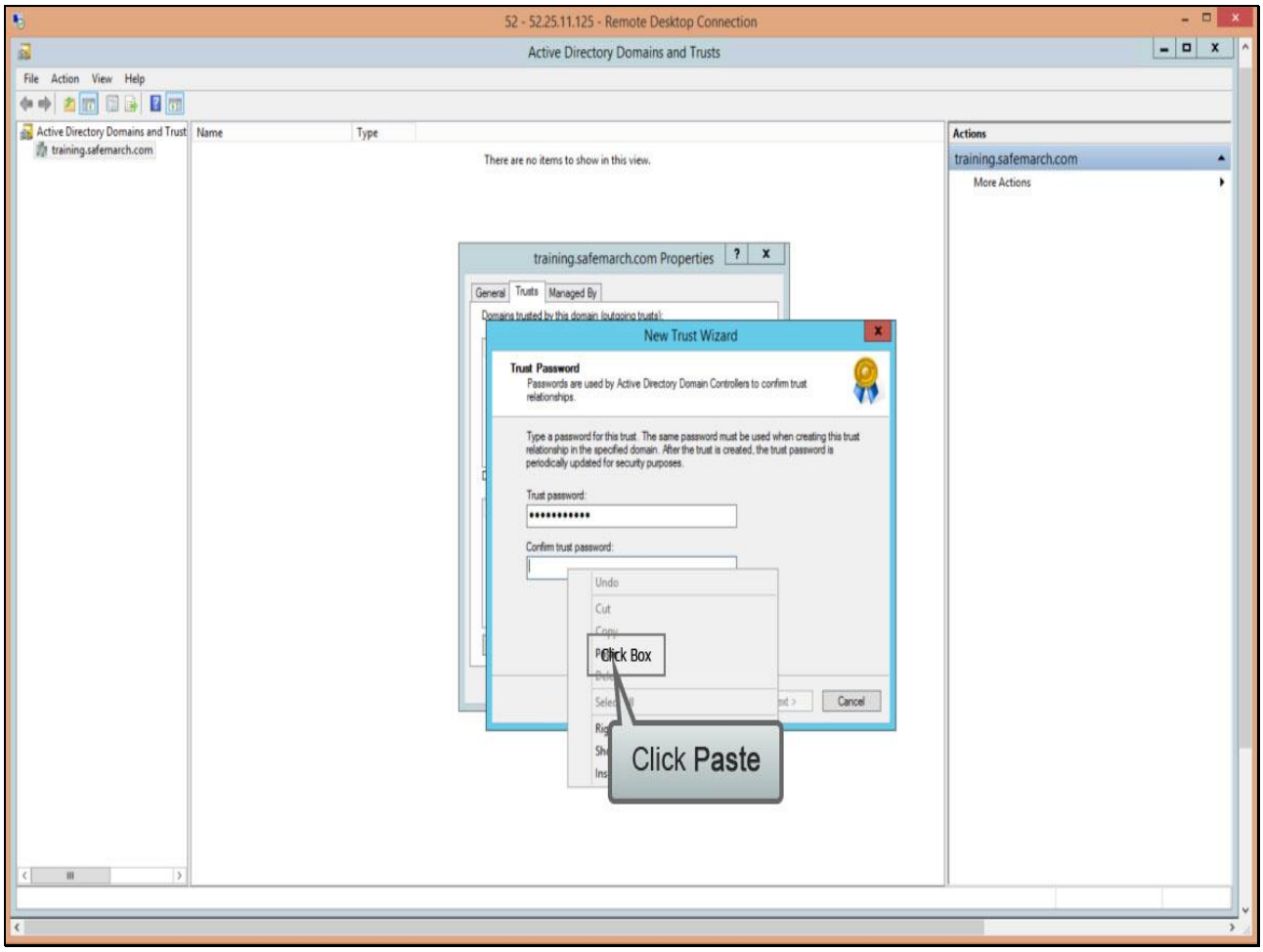
Slide notes

Slide 68 - Slide 68



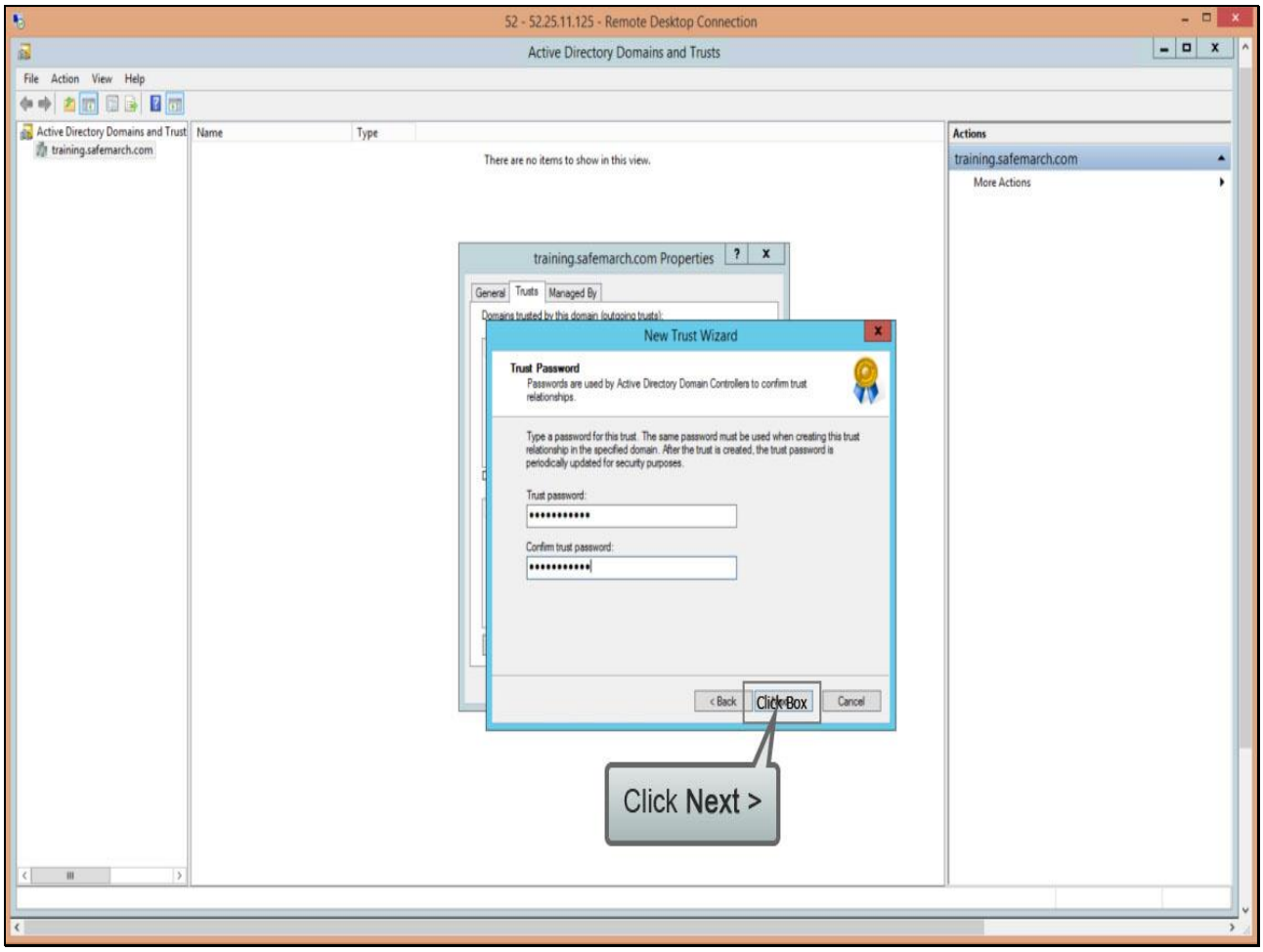
Slide notes

Slide 69 - Slide 69



Slide notes

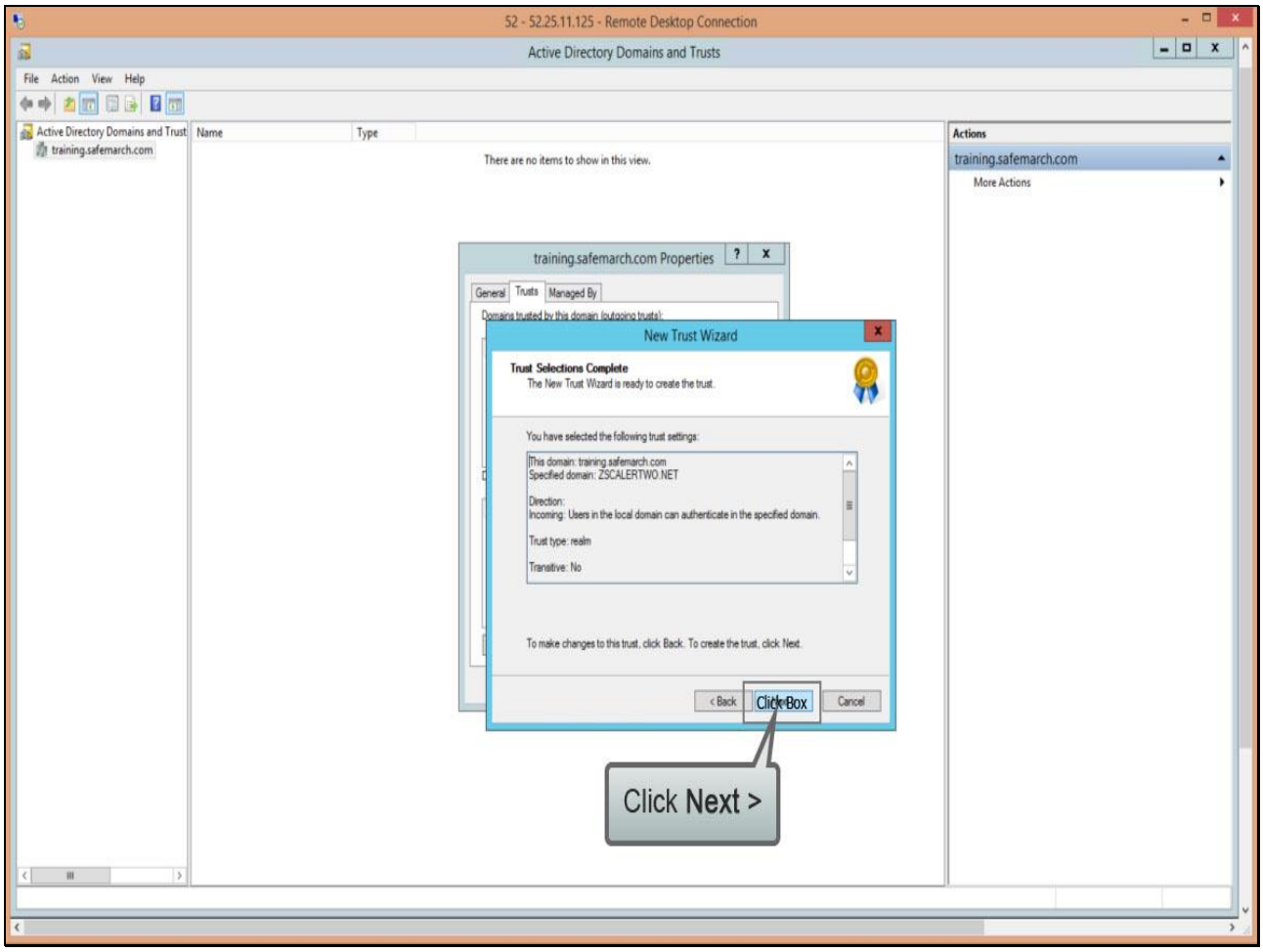
Slide 70 - Slide 70



Slide notes

Click **Next**, …

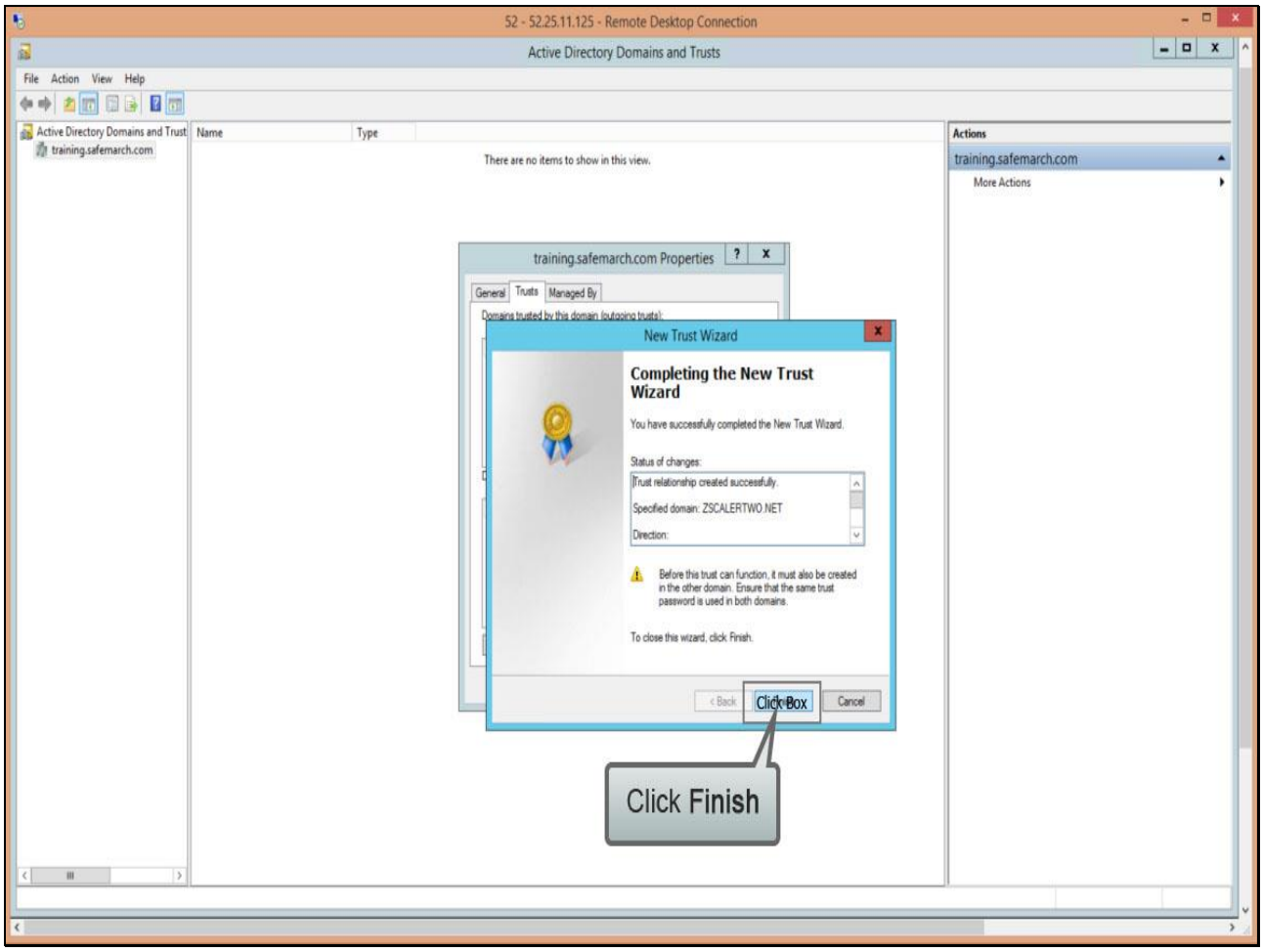
Slide 71 - Slide 71



Slide notes

…verify your settings then click **Next**.

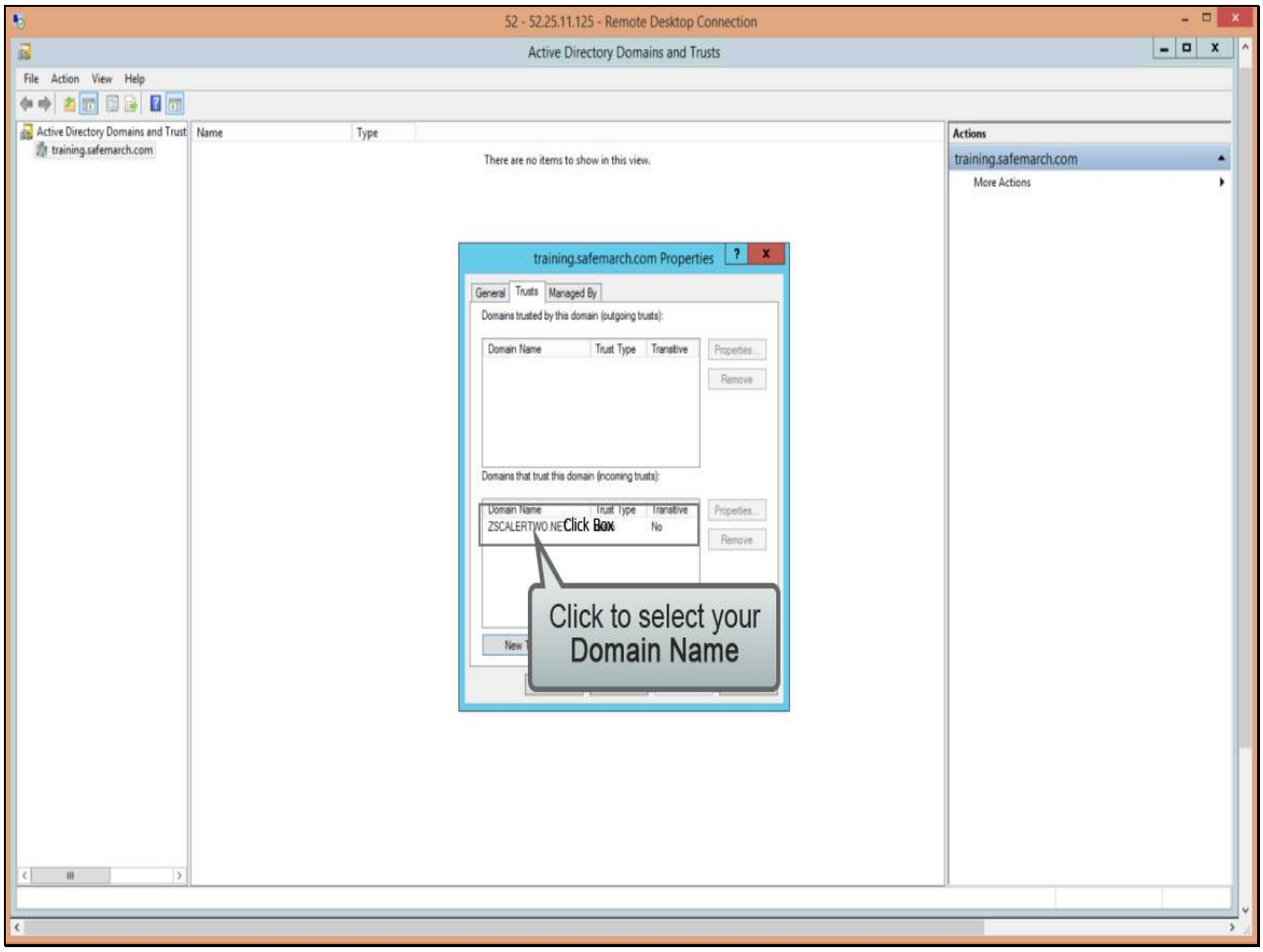
Slide 72 - Slide 72



Slide notes

Click **Finish** to close the Wizard.

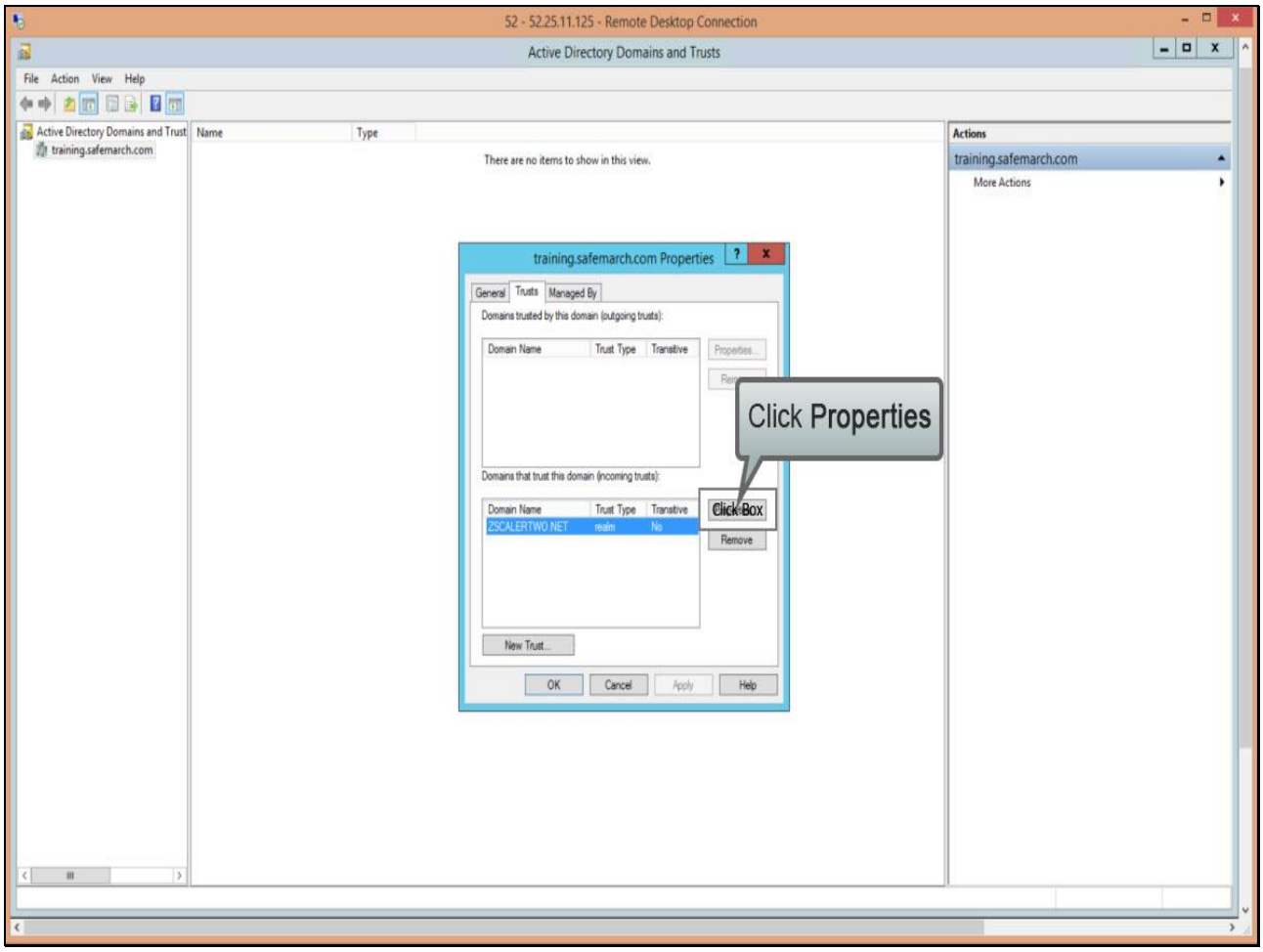
Slide 73 - Slide 73



Slide notes

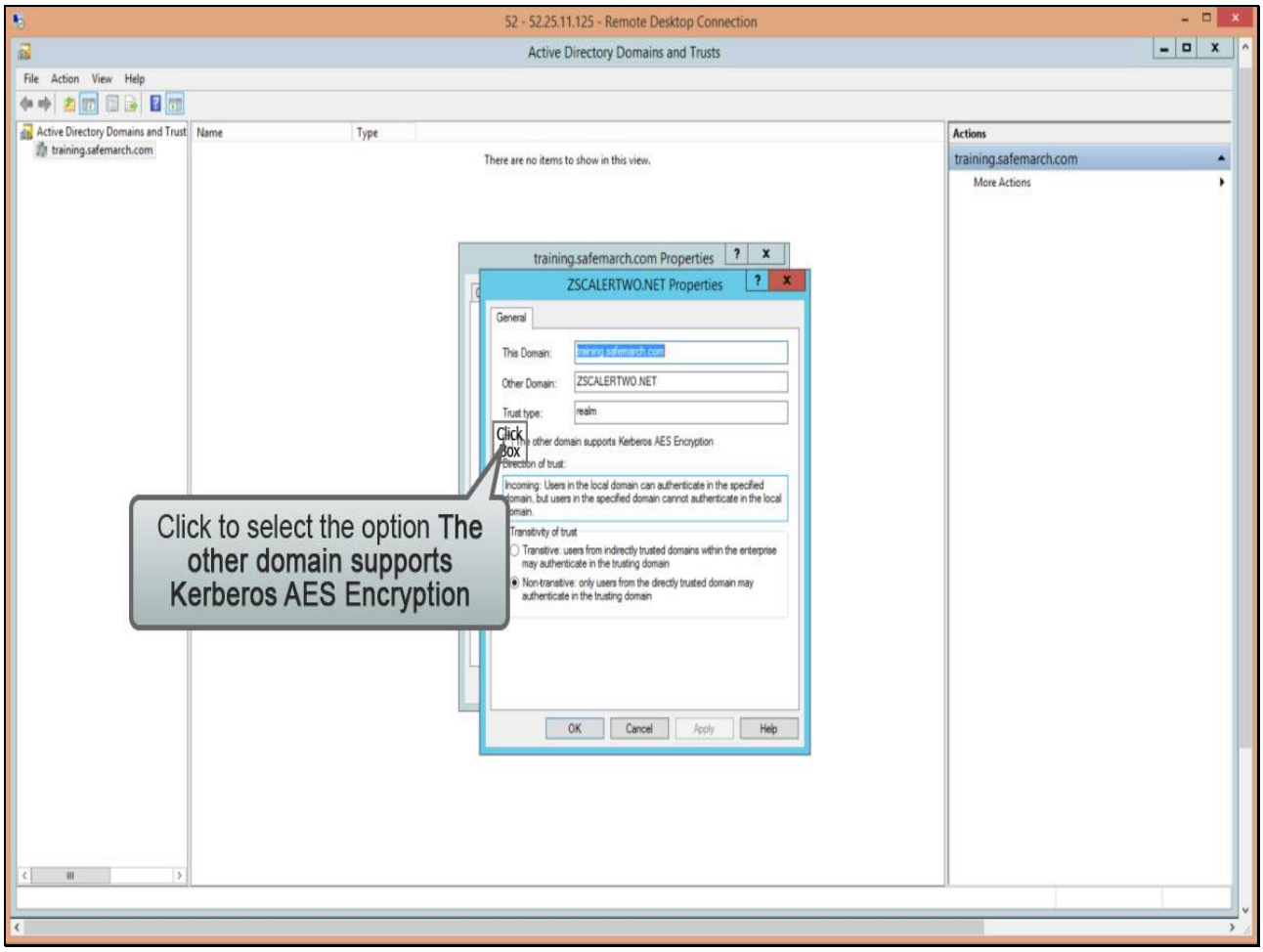
Highlight the trust you just created then click **Properties**.

Slide 74 - Slide 74



Slide notes

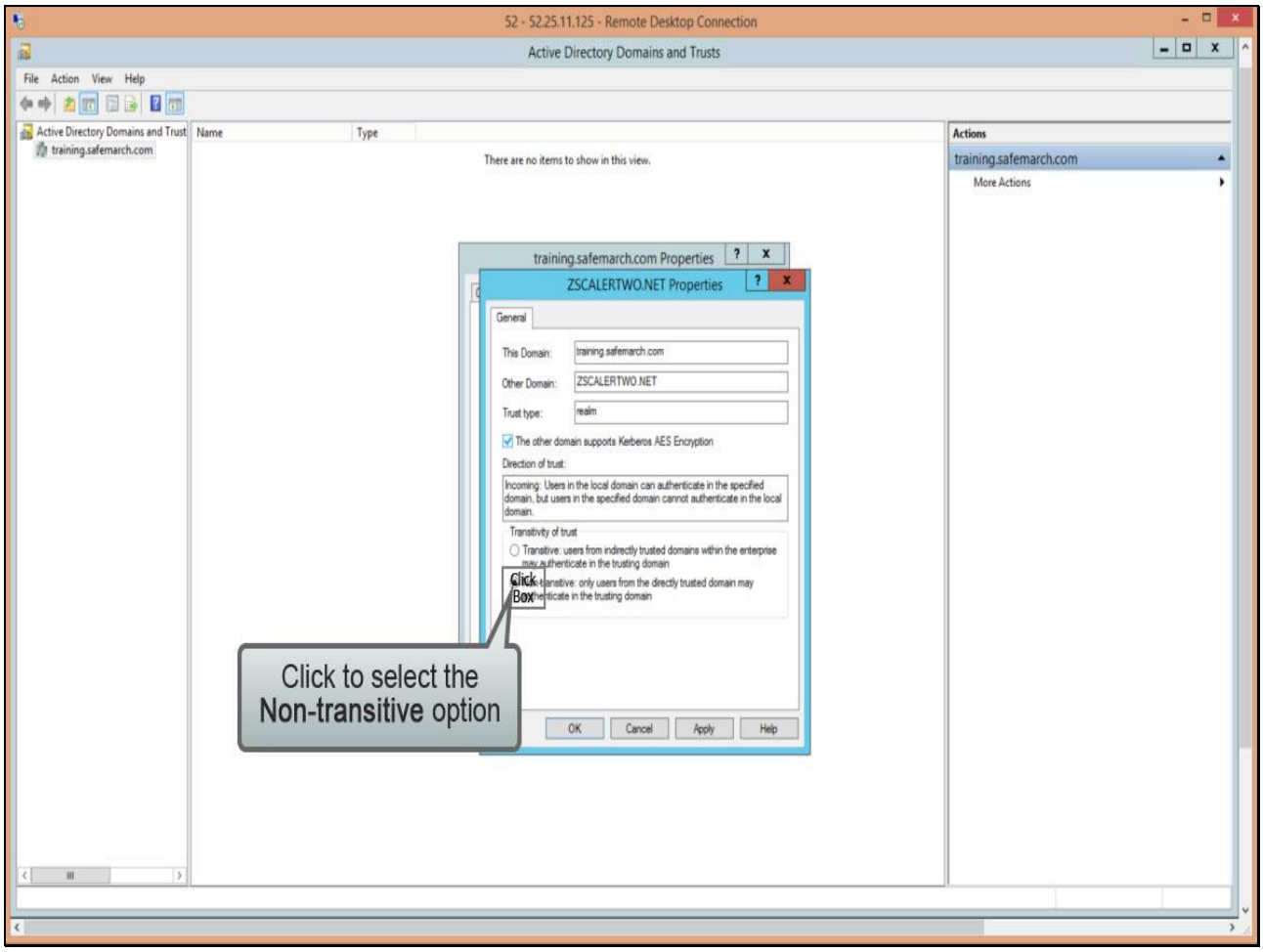
Slide 75 - Slide 75



Slide notes

Check **The other domain supports Kerberos AES encryption**, …

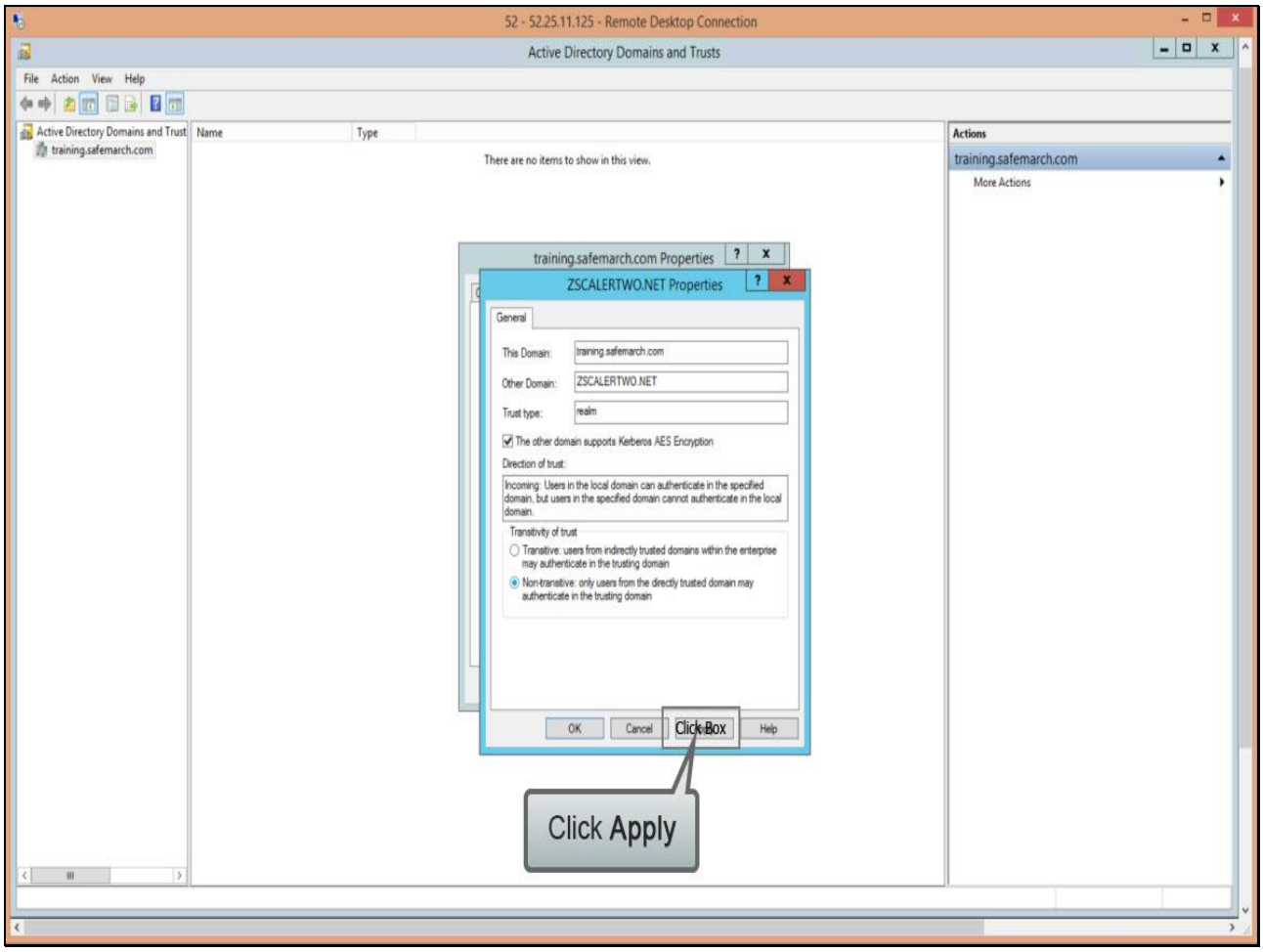
Slide 76 - Slide 76



Slide notes

…and select **Non-transitive**, …

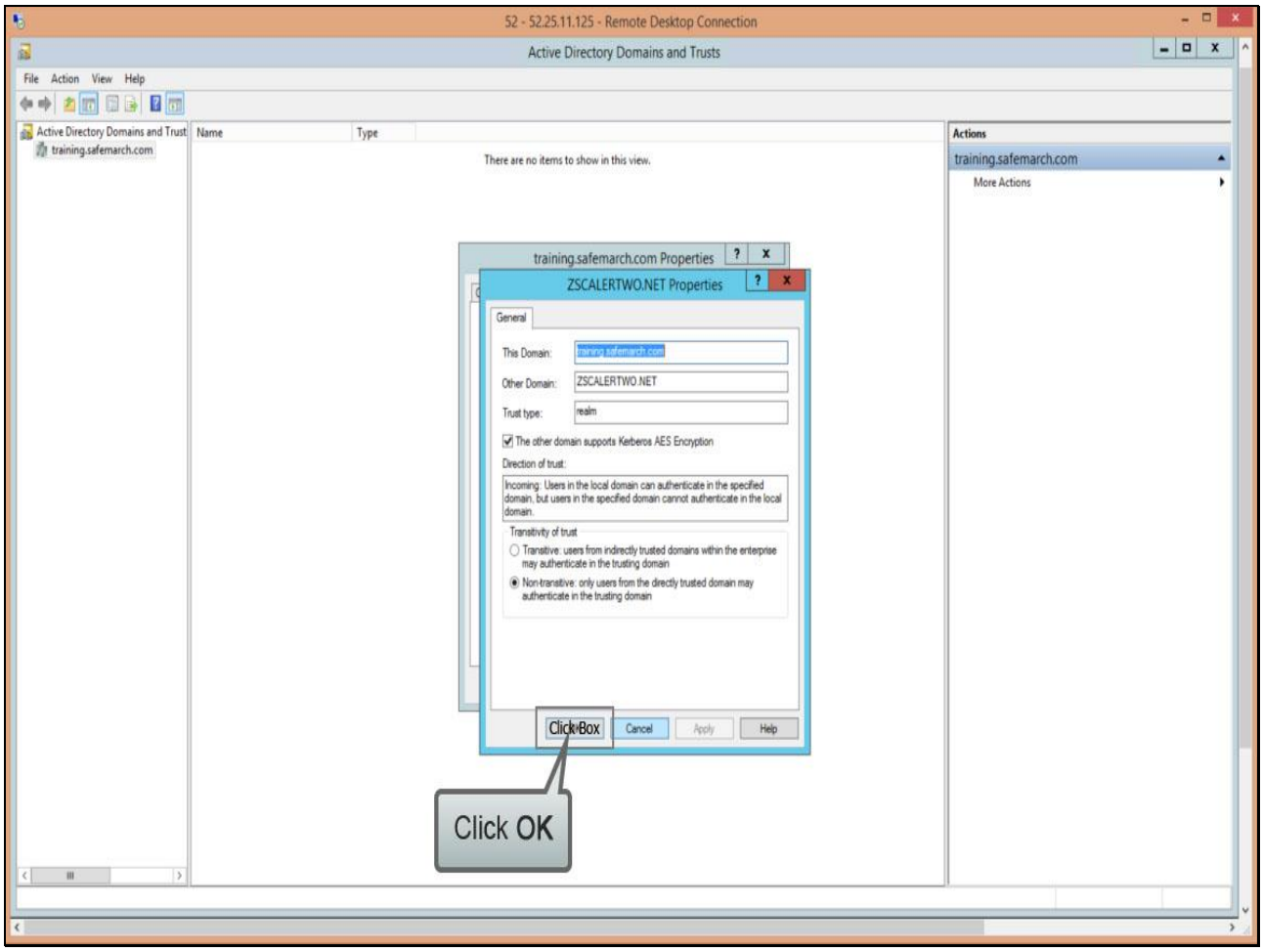
Slide 77 - Slide 77



Slide notes

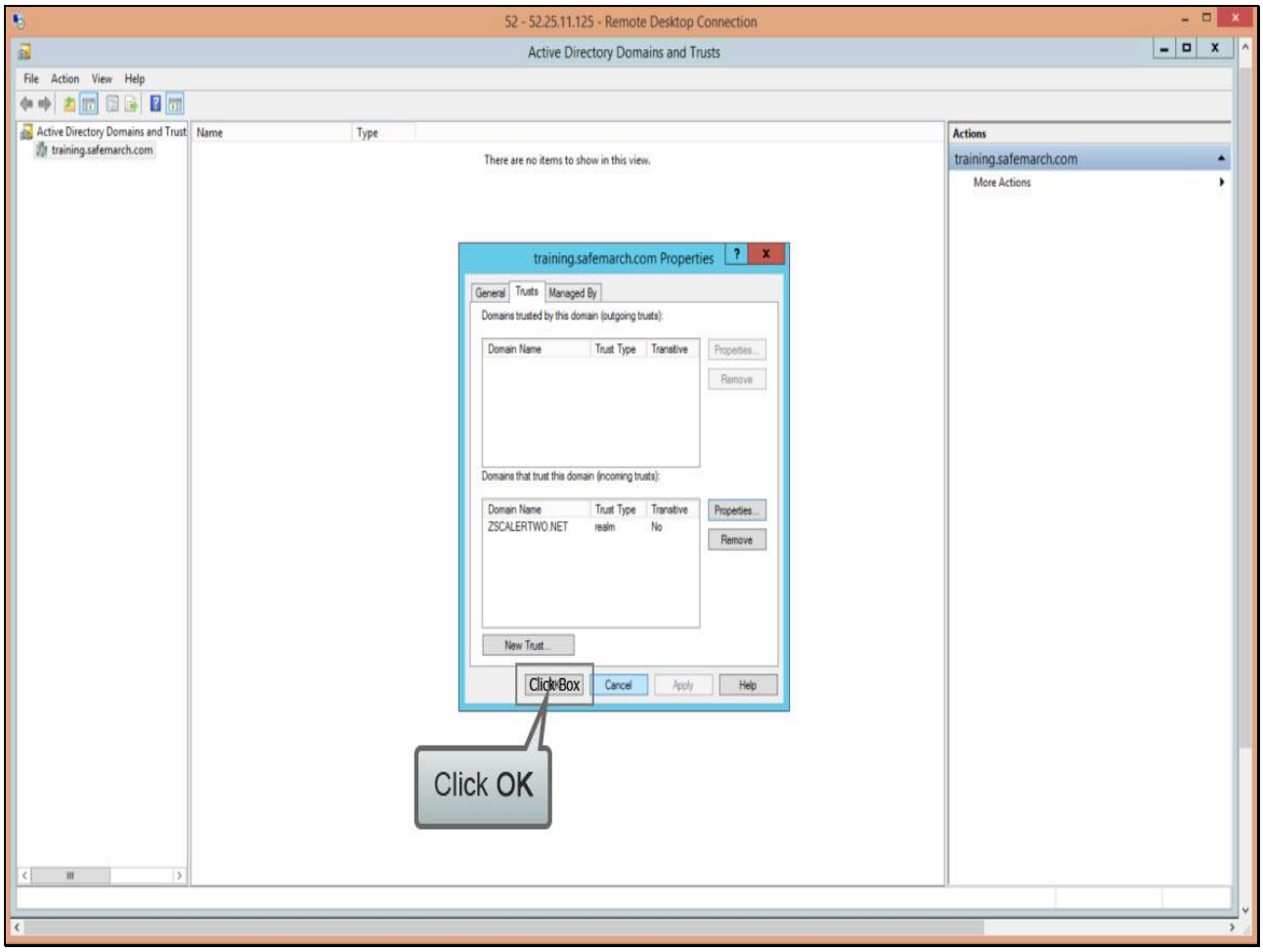
…then click **Apply**.

Slide 78 - Slide 78



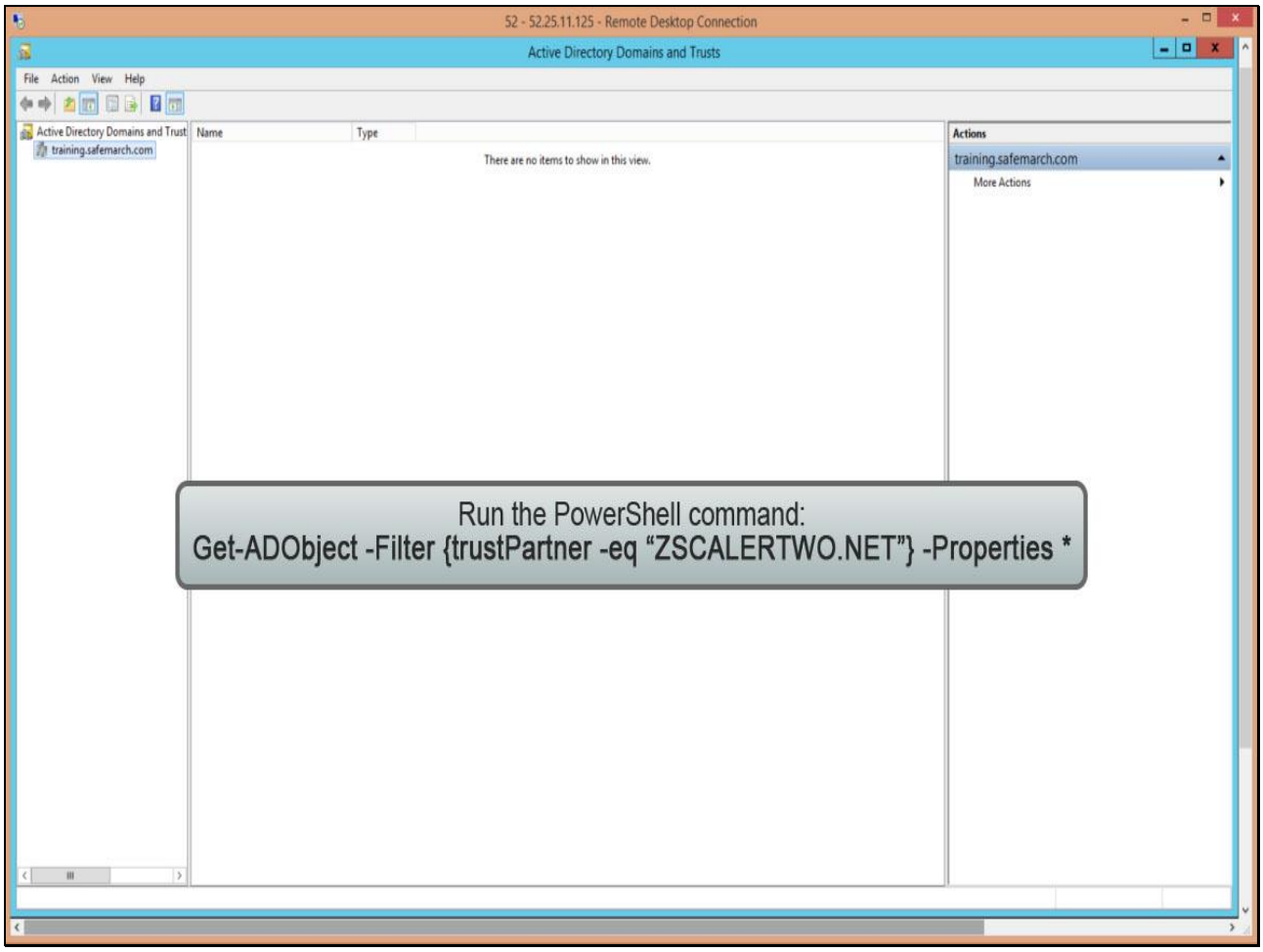
Slide notes

Slide 79 - Slide 79



Slide notes

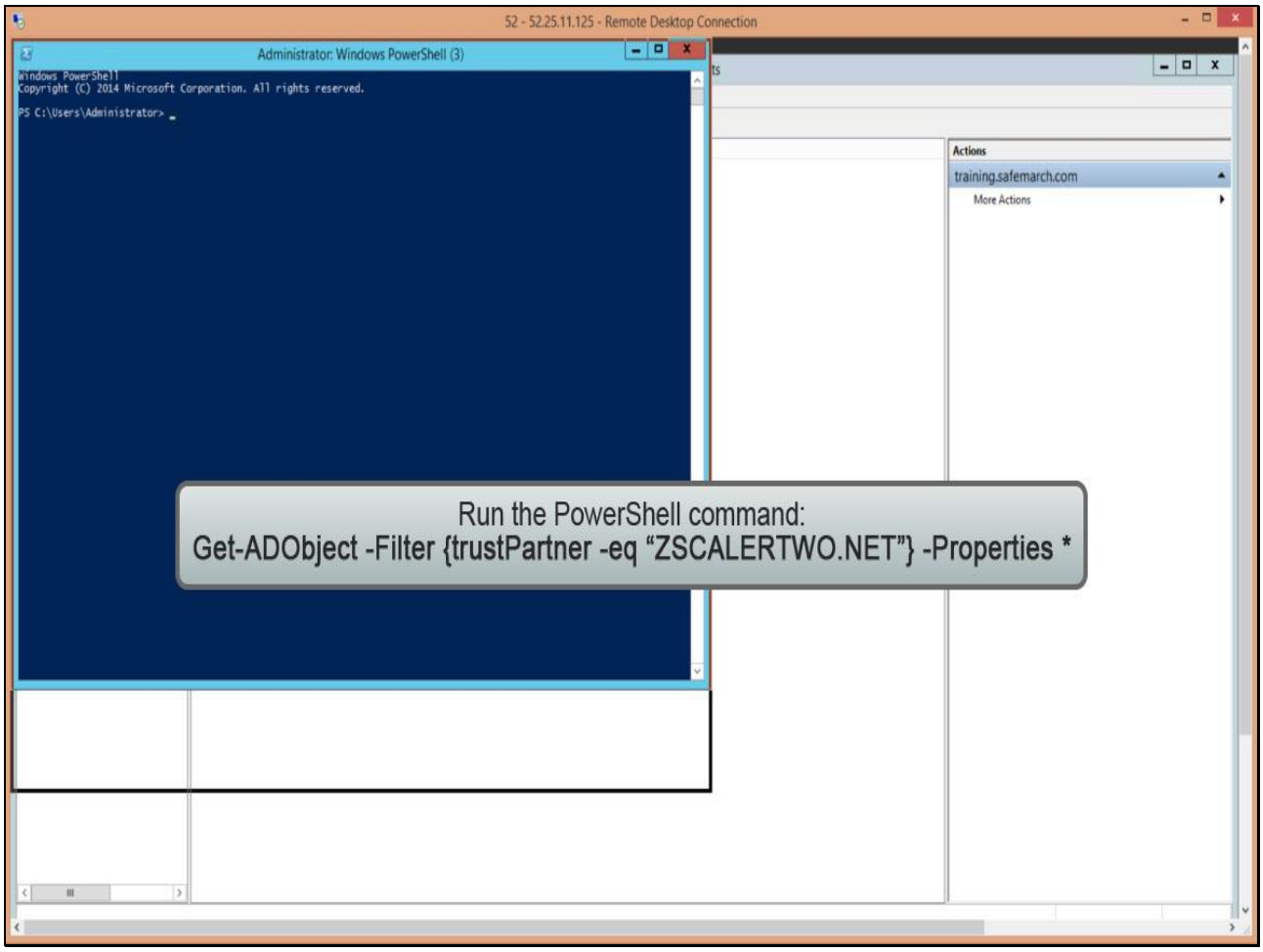
Slide 80 - Slide 80



Slide notes

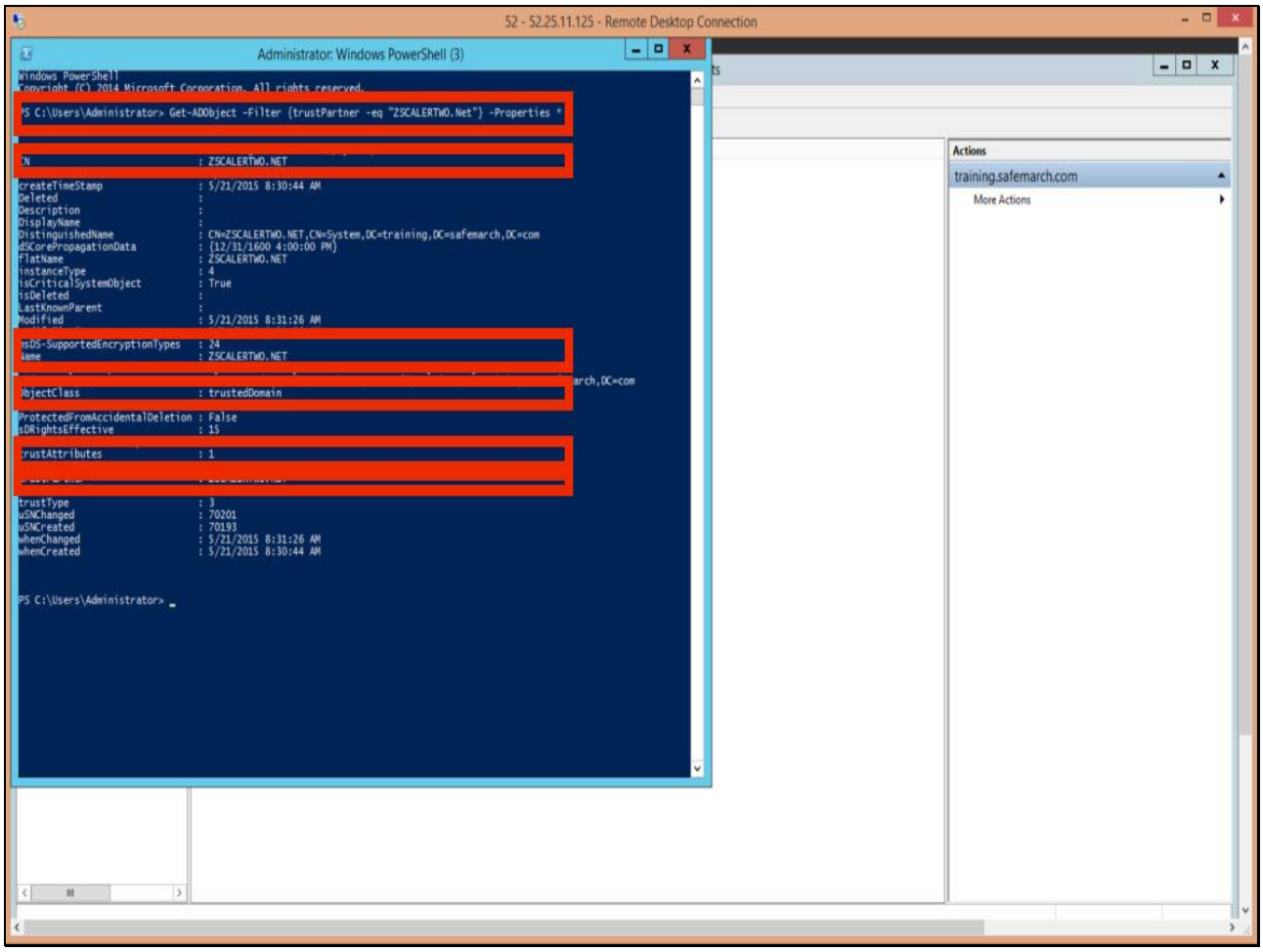
Validate your settings on the CLI under Windows PowerShell using the command **Get-ADObject -Filter {trustPartner -eq "ZSCALERTWO.NET"} -Properties ***

Slide 81 - Slide 81



Slide notes

Slide 82 - Slide 82

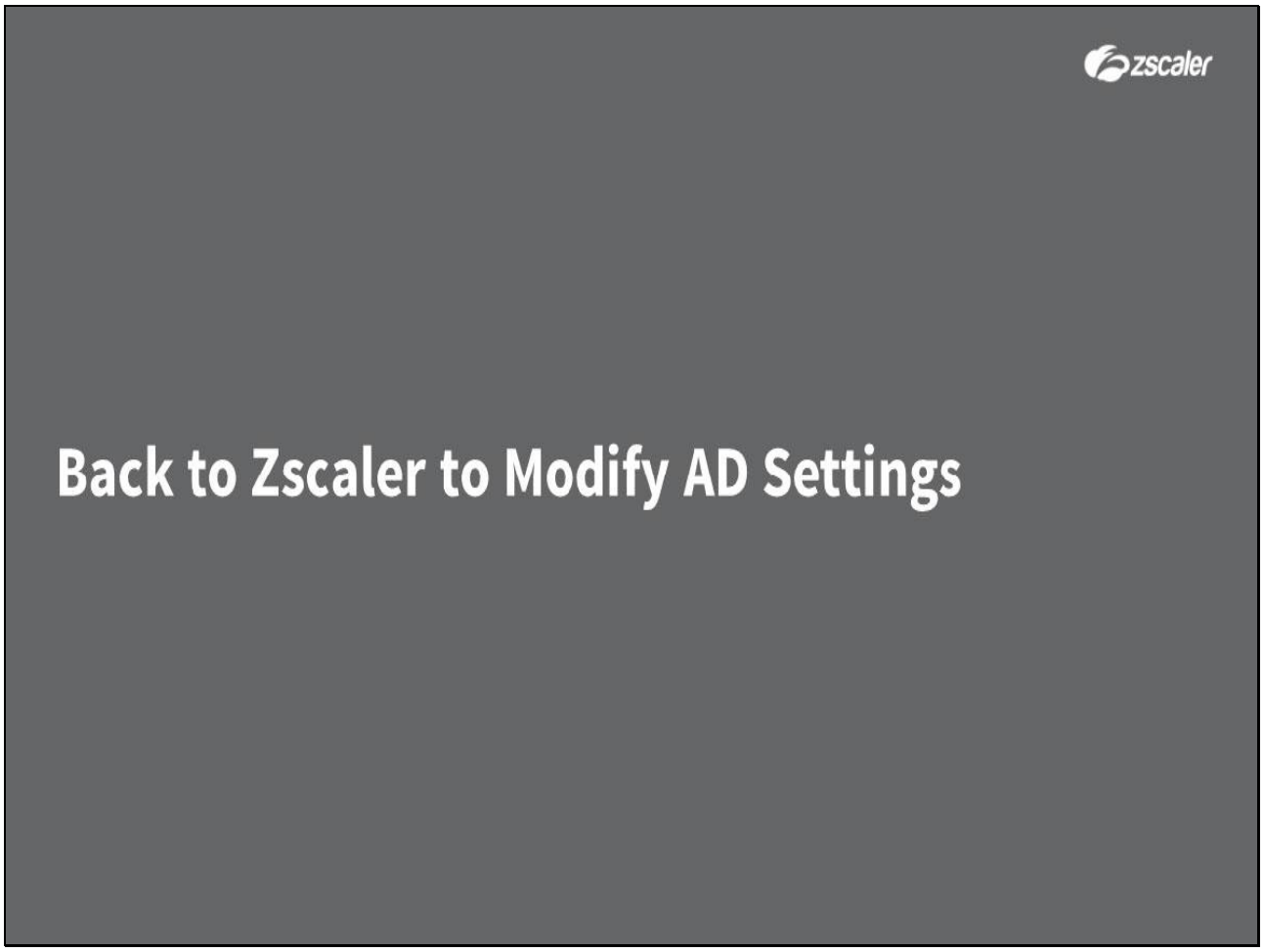


Slide notes

Check the output and look specifically at:

- **CN** to see that it matches the Zscaler cloud domain you are on;
- **msDS-SupportedEncryptionTypes Name** should also show the Zscaler cloud you are on;
- **ObjectClass** should show **trusted Domain**;
- **trustAttributes** and **trustDirection** should show **1**;
- And the **trustPartner**, again, is your Zscaler cloud.

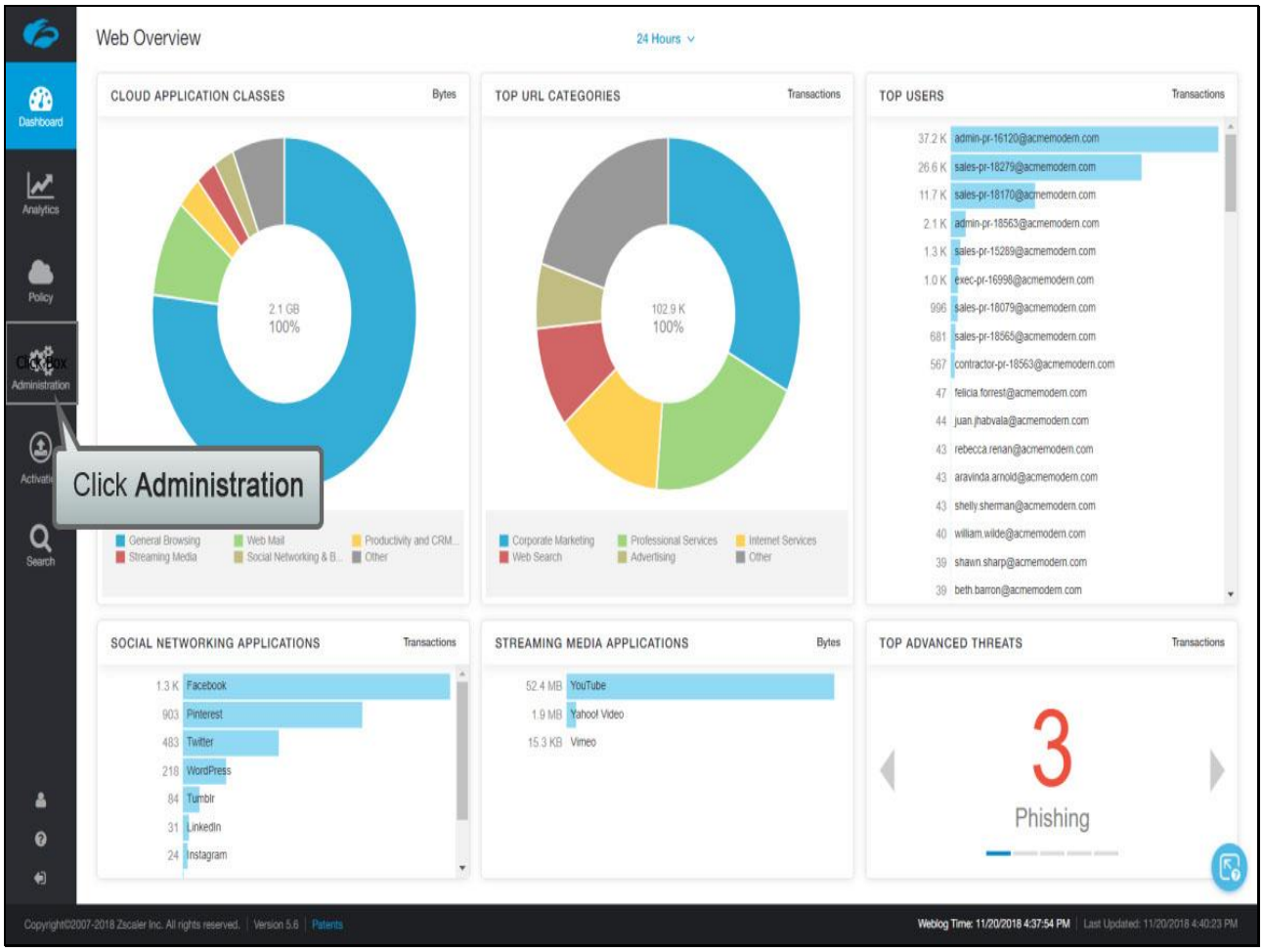
Slide 83 - Back to Zscaler to Modify AD Settings



Slide notes

Let’s return to the Zscaler Admin Portal to make a minor modification to the Active Directory configuration for use with Kerberos.

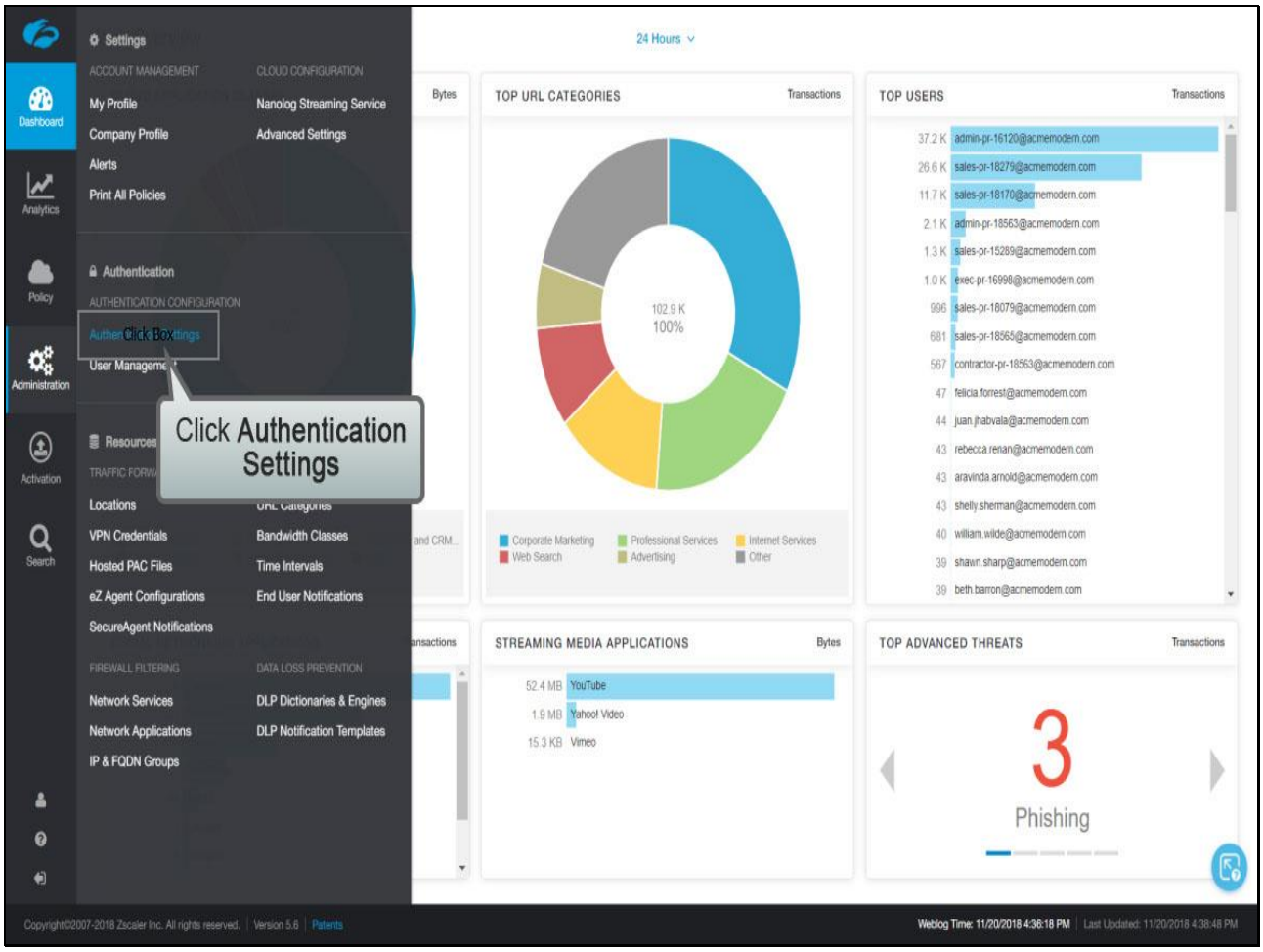
Slide 84 - Slide 84



Slide notes

Go to **Administration**, …

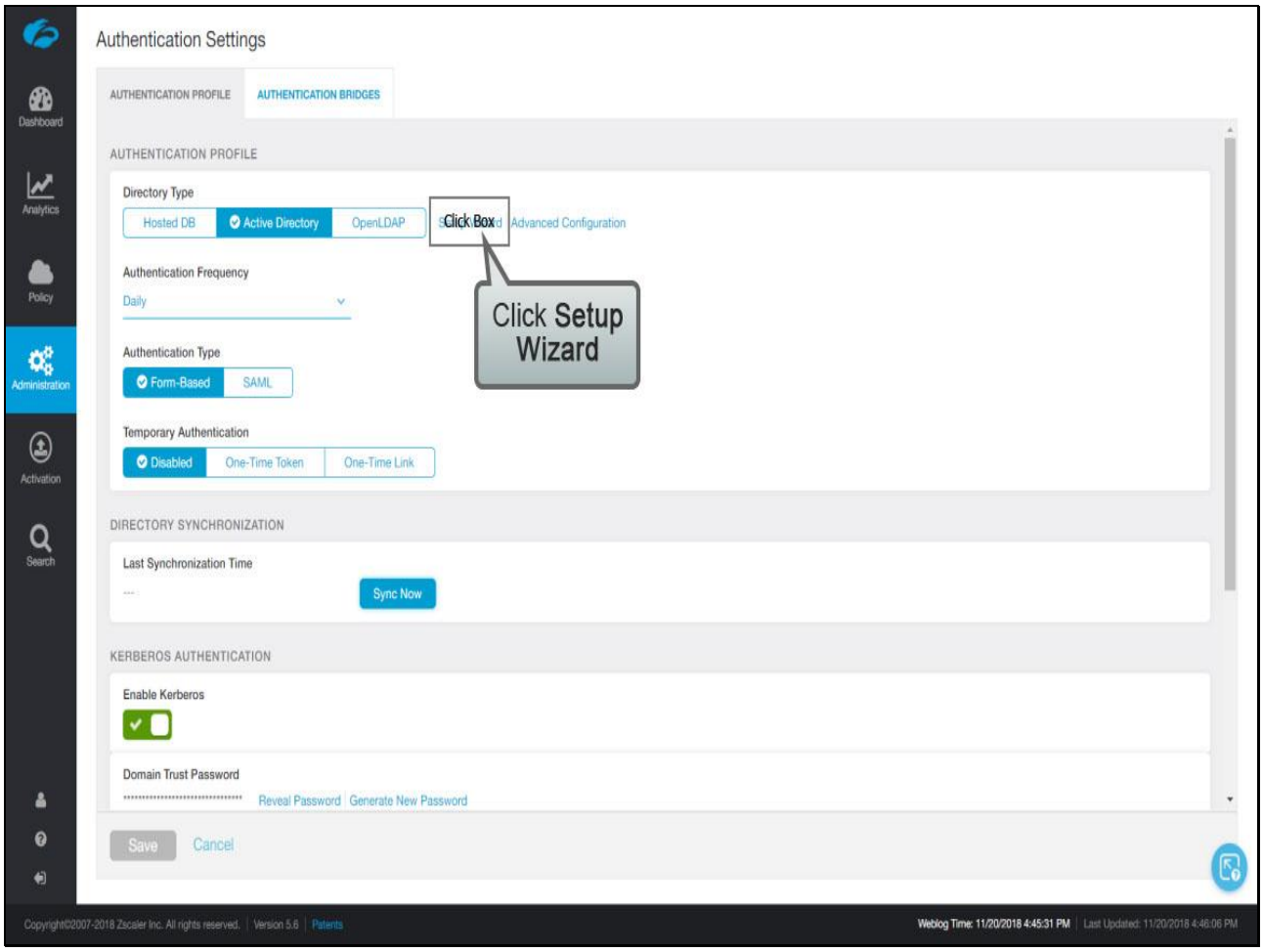
Slide 85 - Slide 85



Slide notes

…then **Authentication Settings**.

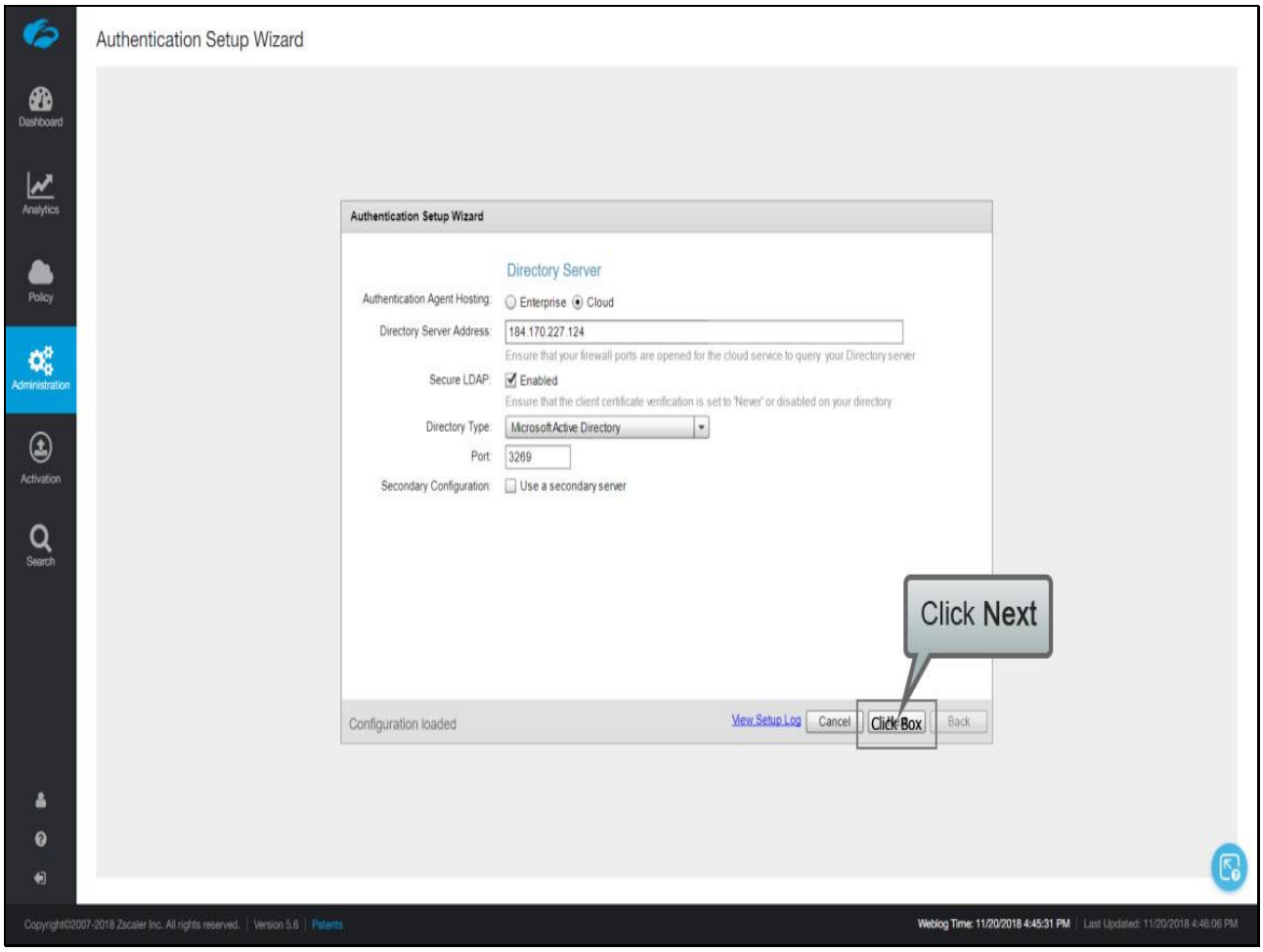
Slide 86 - Slide 86



Slide notes

Click on **Setup Wizard**.

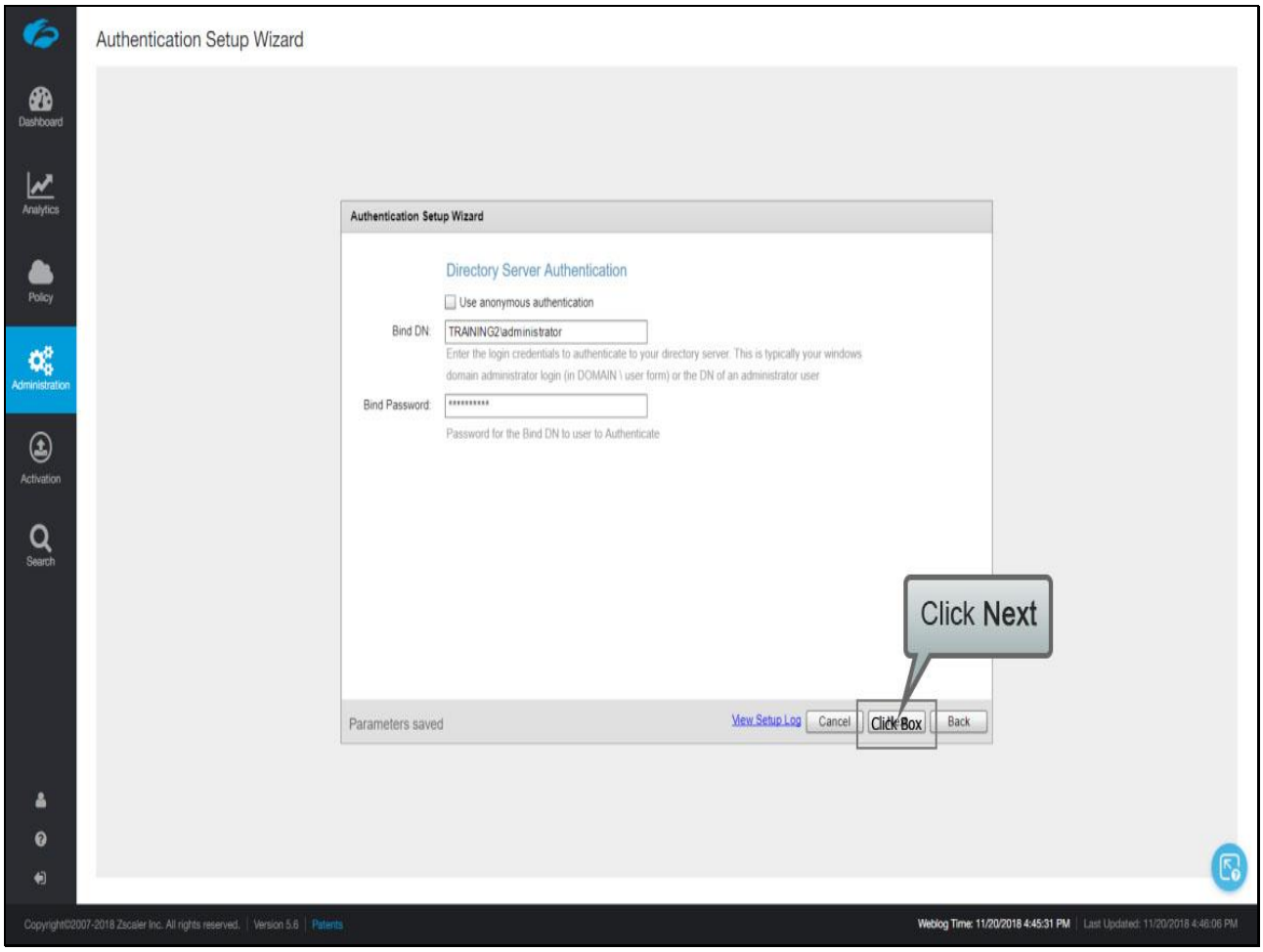
Slide 87 - Slide 87



Slide notes

Please note that Active Directory has already been configured per the Active Directory training module. Just go ahead and click **Next**.

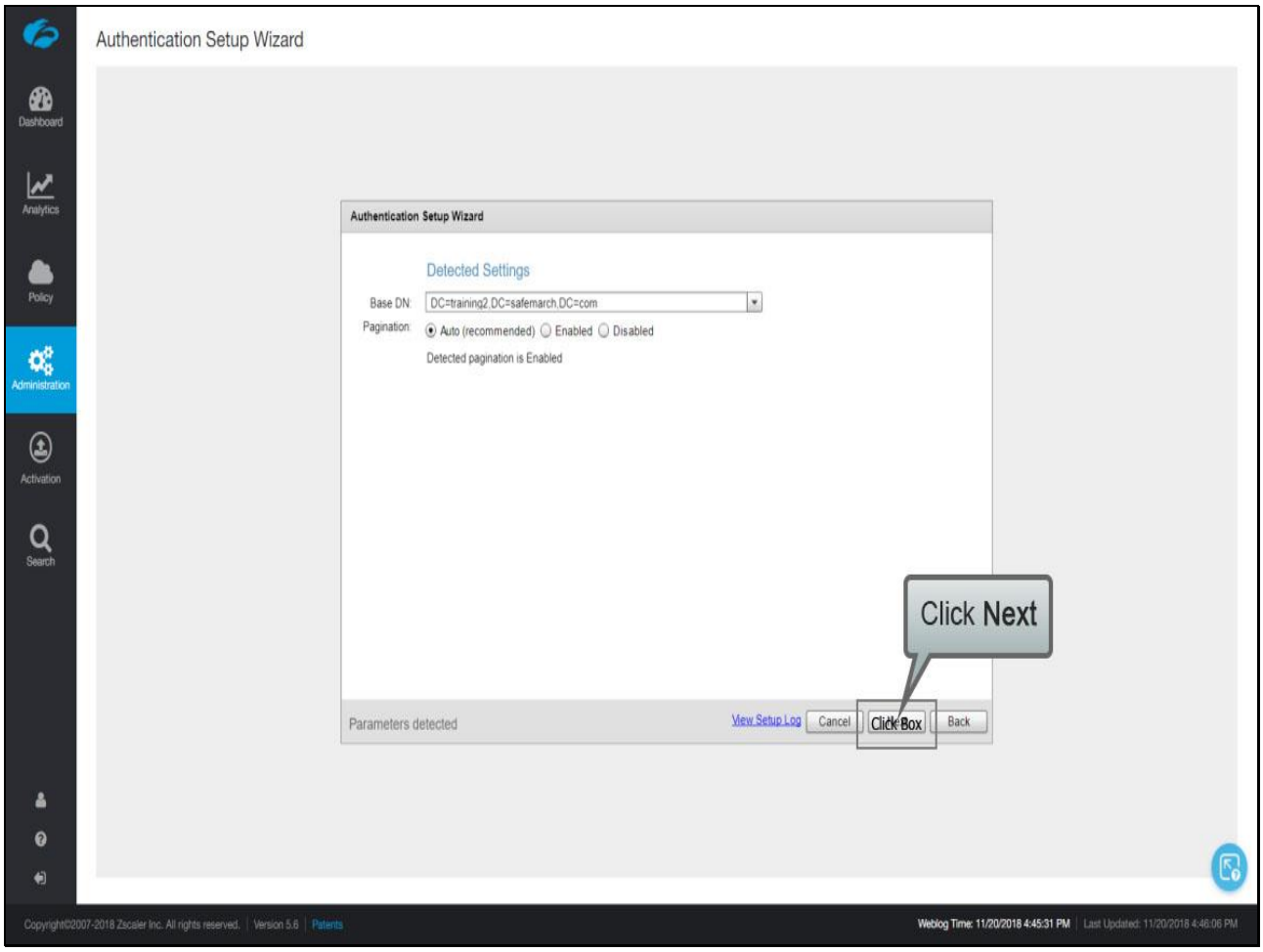
Slide 88 - Slide 88



Slide notes

Click **Next**, …

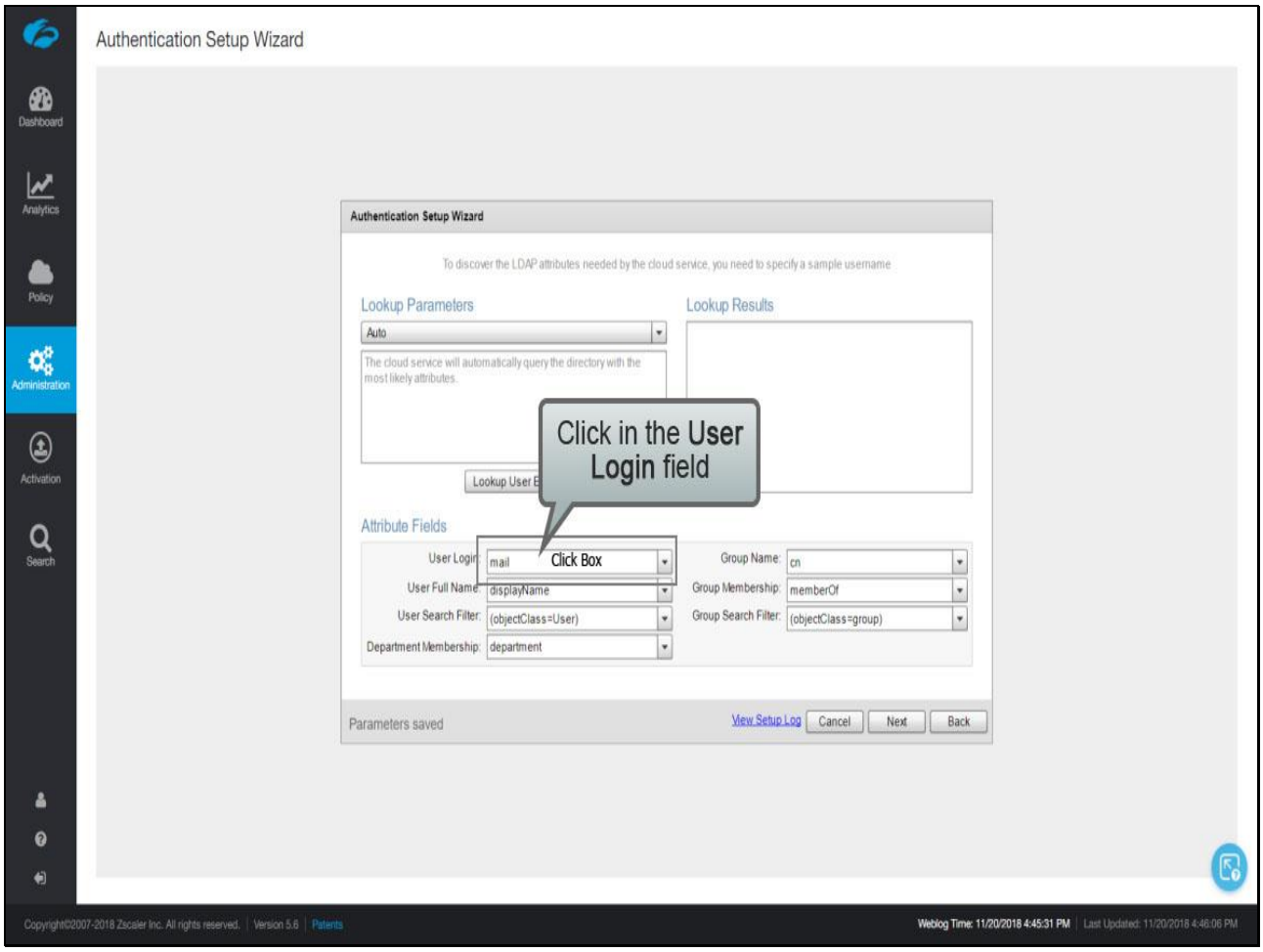
Slide 89 - Slide 89



Slide notes

Click **Next**, …

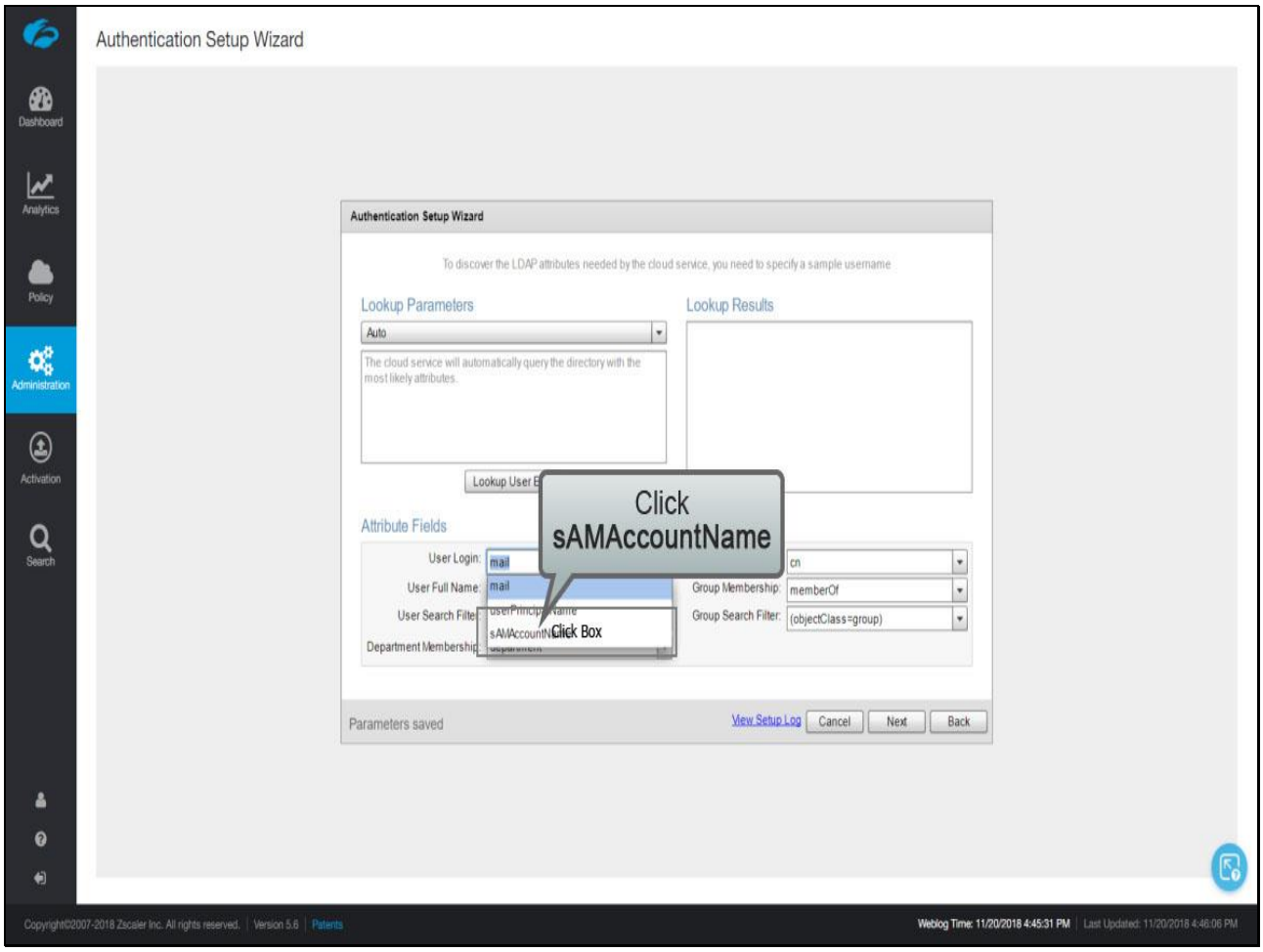
Slide 90 - Slide 90



Slide notes

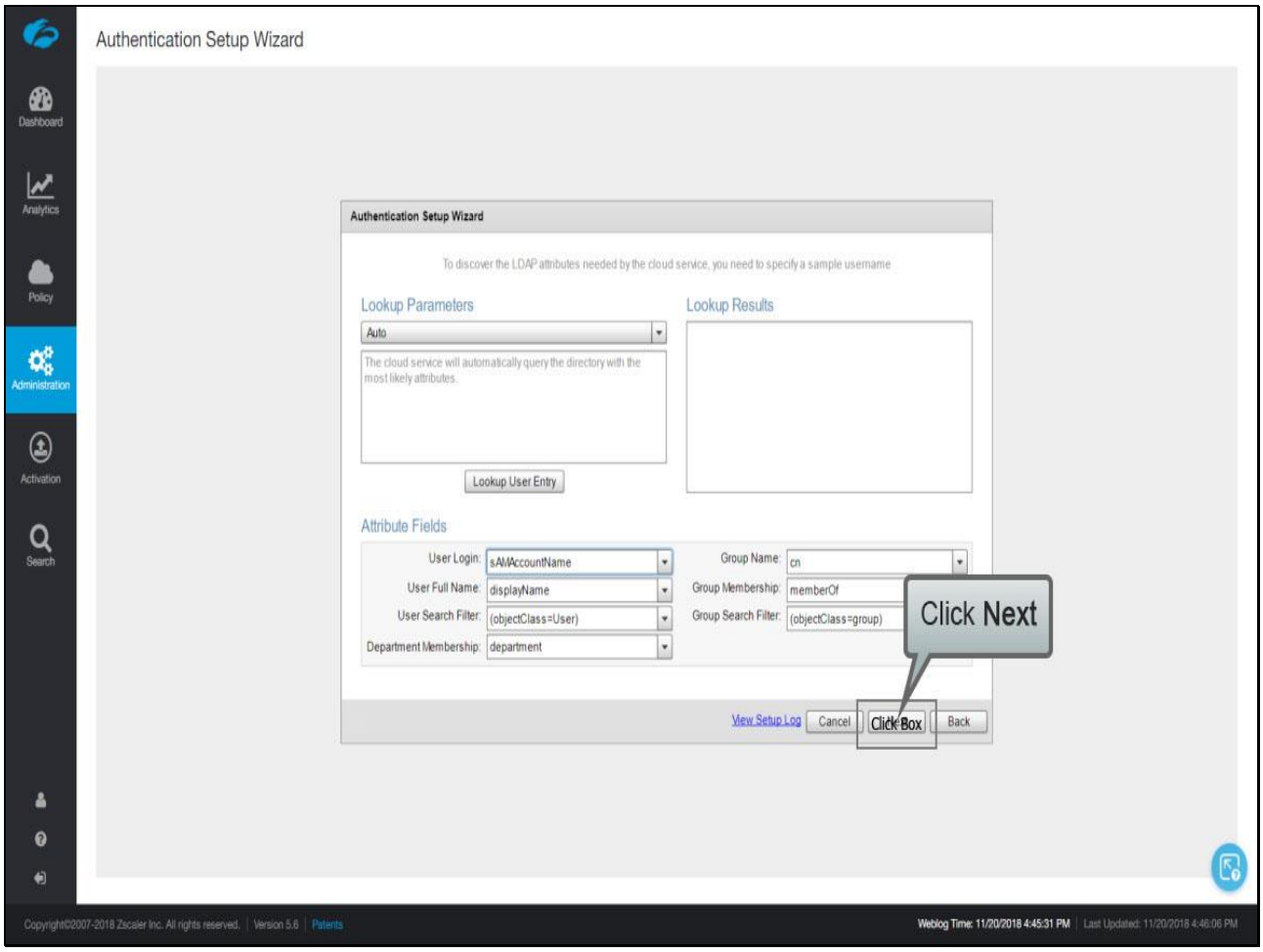
Under the **Attribute Fields** section change **User login** from **email** to **sAMAccountName** then click **Next**.

Slide 91 - Slide 91



Slide notes

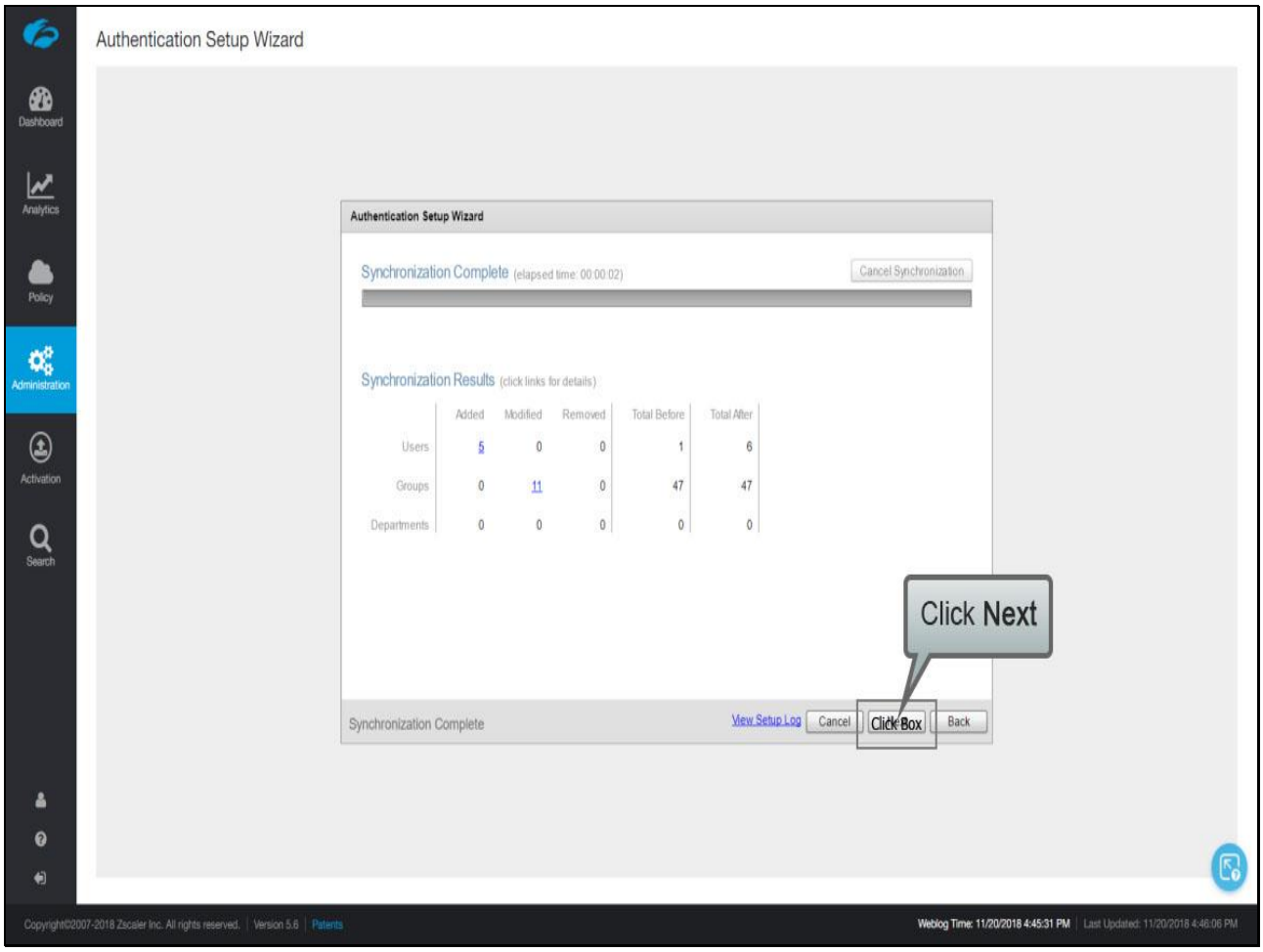
Slide 92 - Slide 92



Slide notes

Click **Next**, …

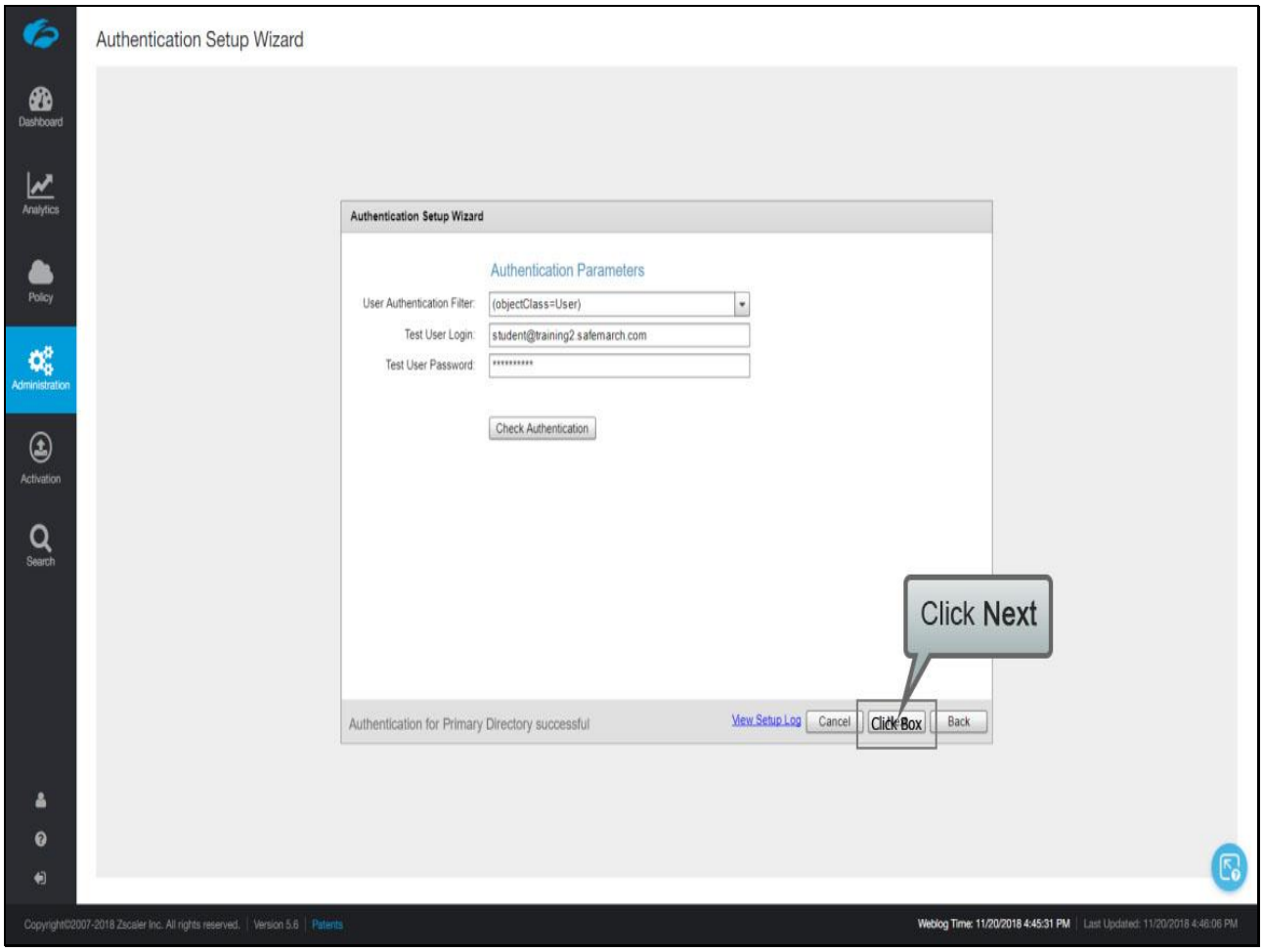
Slide 93 - Slide 93



Slide notes

Click **Next**, …

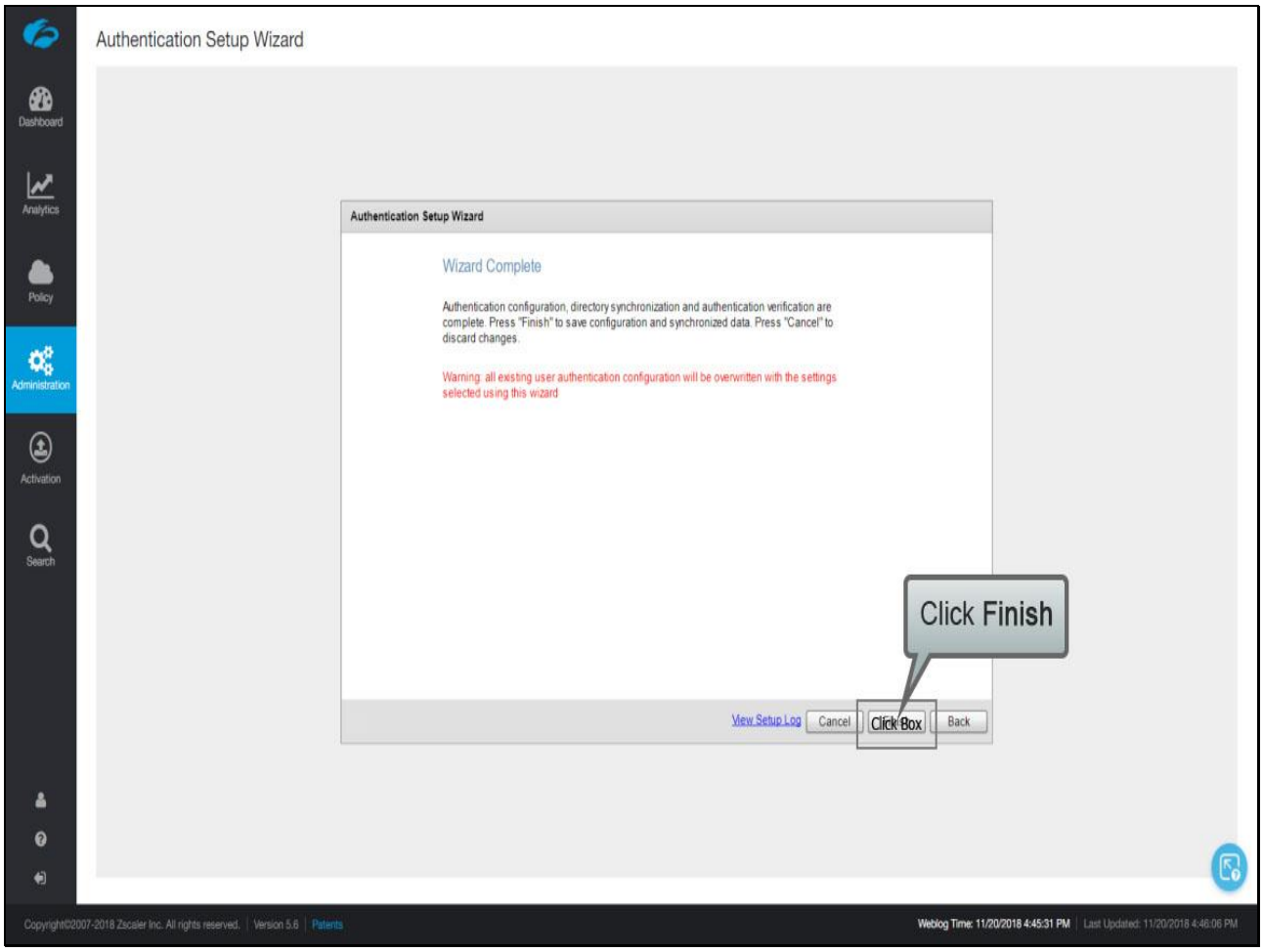
Slide 94 - Slide 94



Slide notes

Click **Next**, …

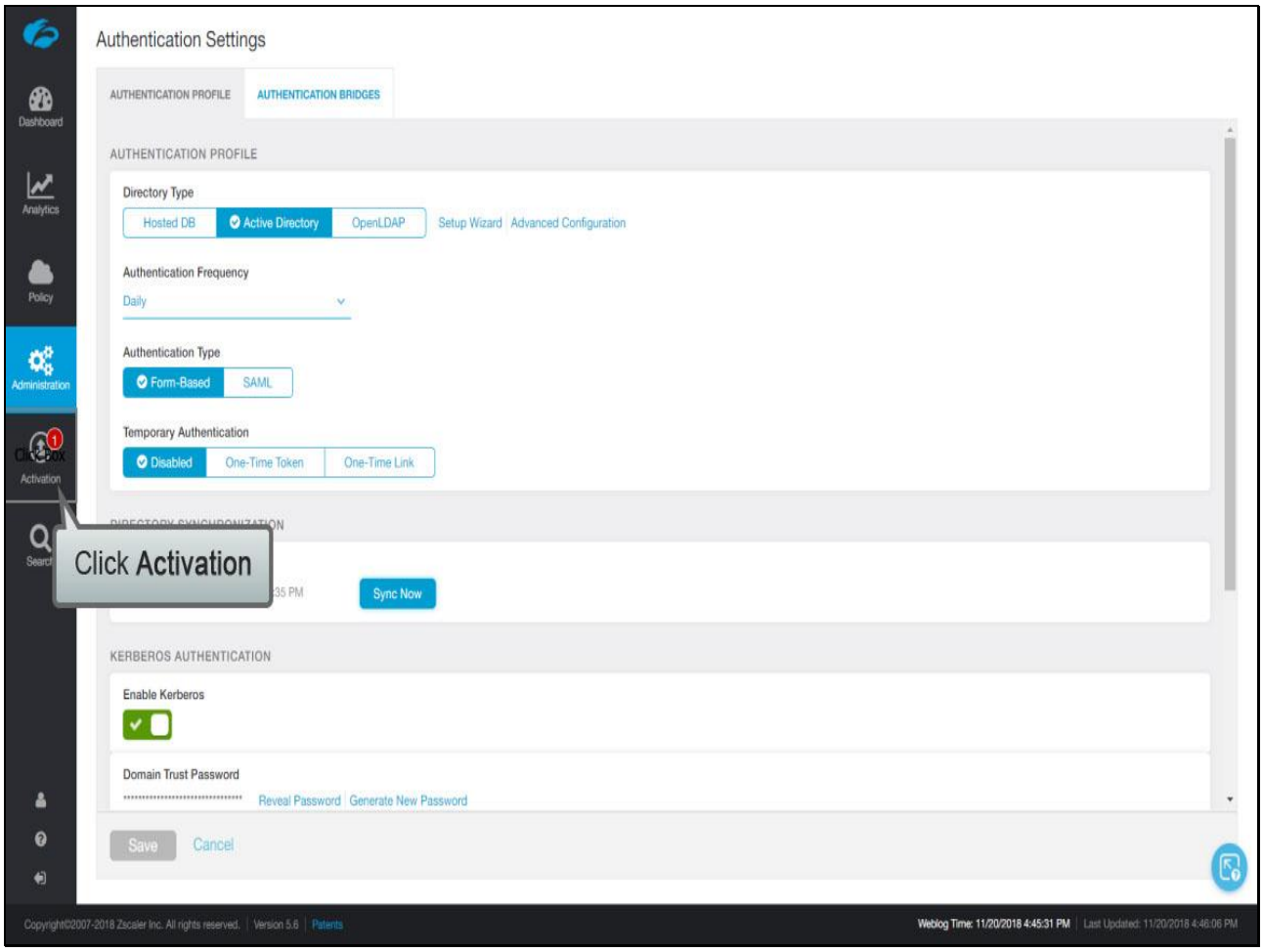
Slide 95 - Slide 95



Slide notes

Then click **Finish**.

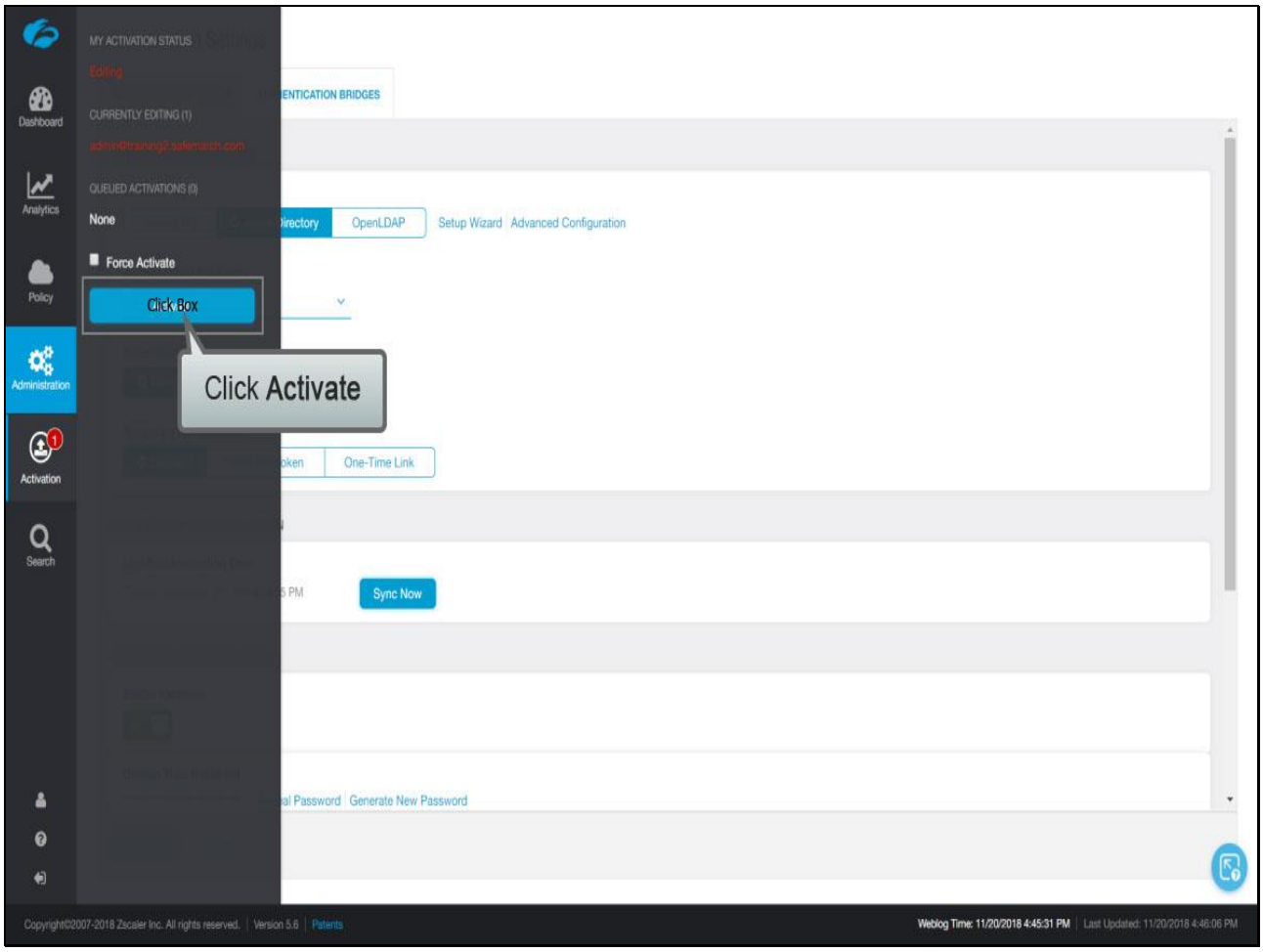
Slide 96 - Slide 96



Slide notes

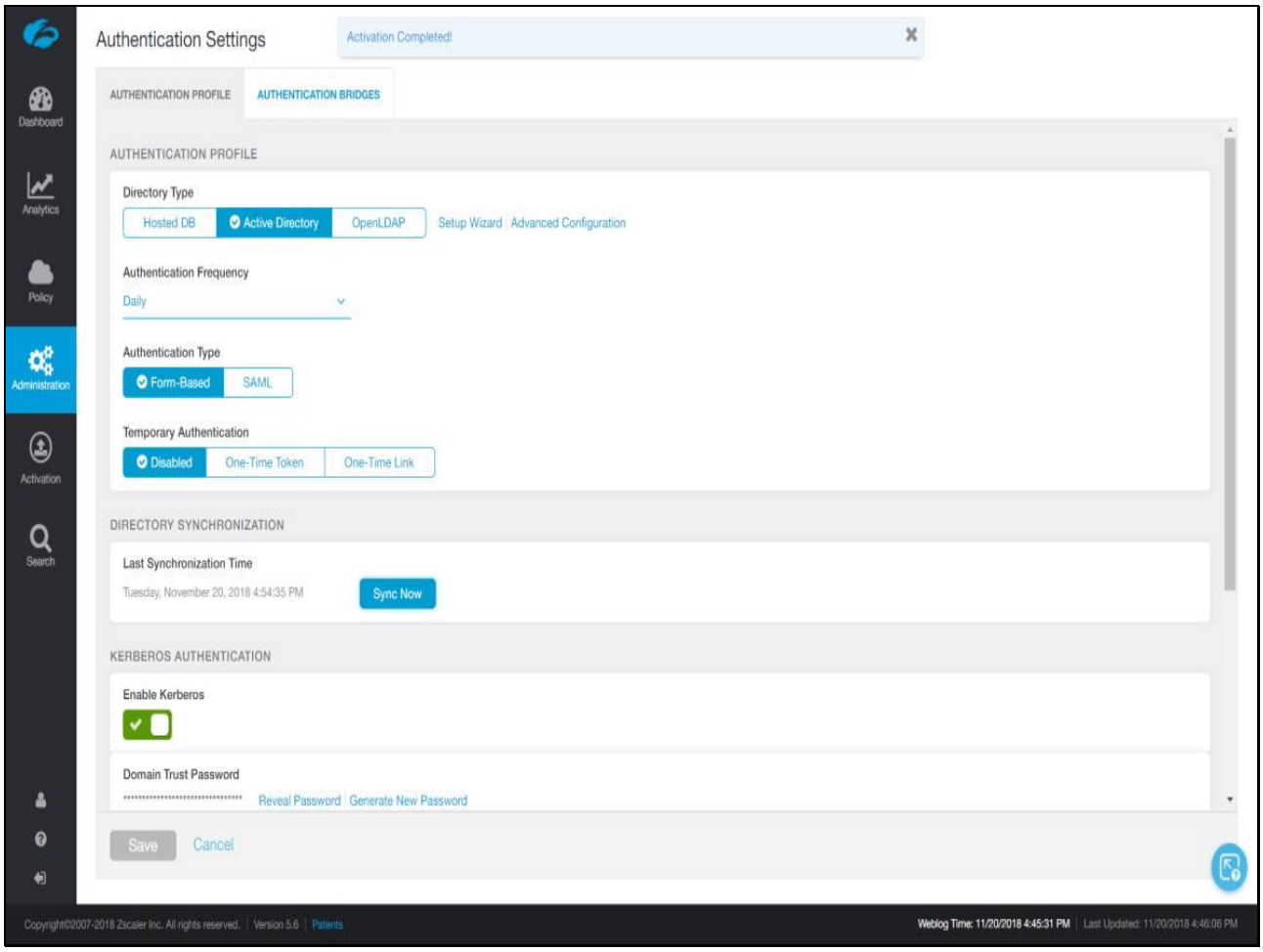
Then **Activate** your changes.

Slide 97 - Slide 97



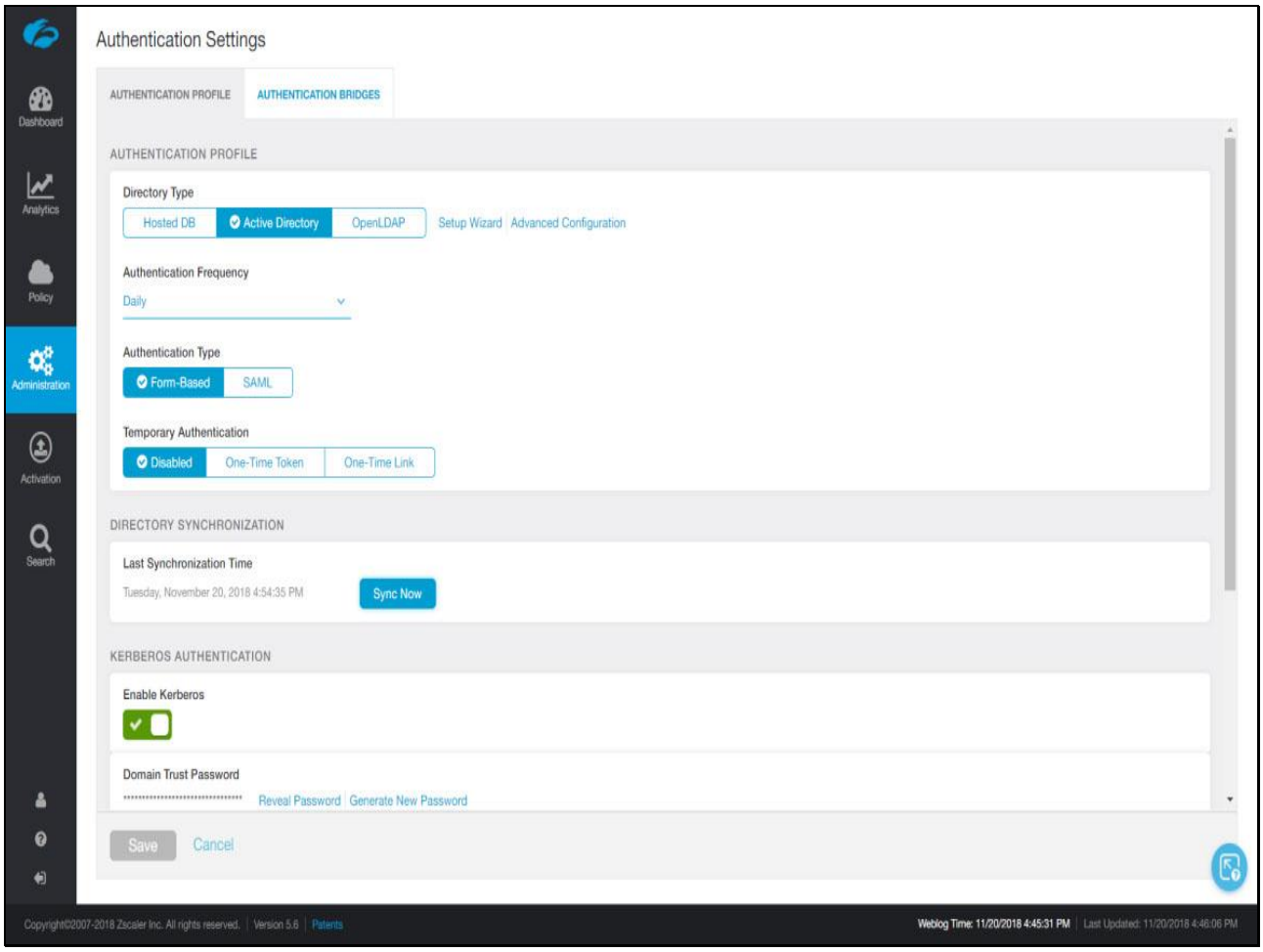
Slide notes

Slide 98 - Slide 98



Slide notes

Slide 99 - Slide 99



Slide notes

Slide 100 - Windows PC Configuration

Slide notes

The PC must be already configured to join the Windows Domain when using Kerberos. Once joined the PC also needs to be configured to use Kerberos Authentication for Web traffic which requires registry changes on the PC. This can be done directly in the registry using the regedit command or be configured and pushed via GPO which is best practice. For steps on configuring GPO please refer to the Zscaler Kerberos Configuration Guide. On the next slide I will illustrate the registry keys that need to be changed using Regedit.

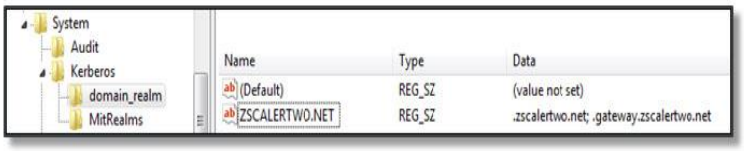
Slide 101 - PC registry changes

PC registry changes

- To enable Kerberos authentication on Windows the following registry changes must be made (manually via **regedit** or pushed via GPO which is best practice)

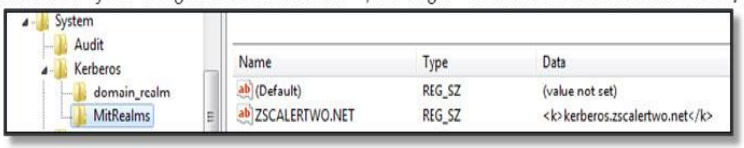
Computer\HKEY_LOCAL_MACHINSOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Kerberos\domain_realm

- Create a registry entry with the Value Name of <your assigned Zscaler cloud> in Upper Case. E.g.: **ZSCALERTWO.NET** and Value data of .<your assigned Zscaler cloud>; .gateway. <your assigned Zscaler cloud> . E.g.: **.zscalertwo.net; .gateway.zscalertwo.net**



Computer\HKEY_LOCAL_MACHINSOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Kerberos\MitRealms

- Create a registry entry with the Value Name of <your assigned Zscaler cloud> in Upper Case. E.g.: **ZSCALERTWO.NET** and Value data of <k>Kerberos. <your assigned Zscaler cloud> </k>. E.g.: **<k>Kerberos.zscalertwo.net</k>**



Slide notes

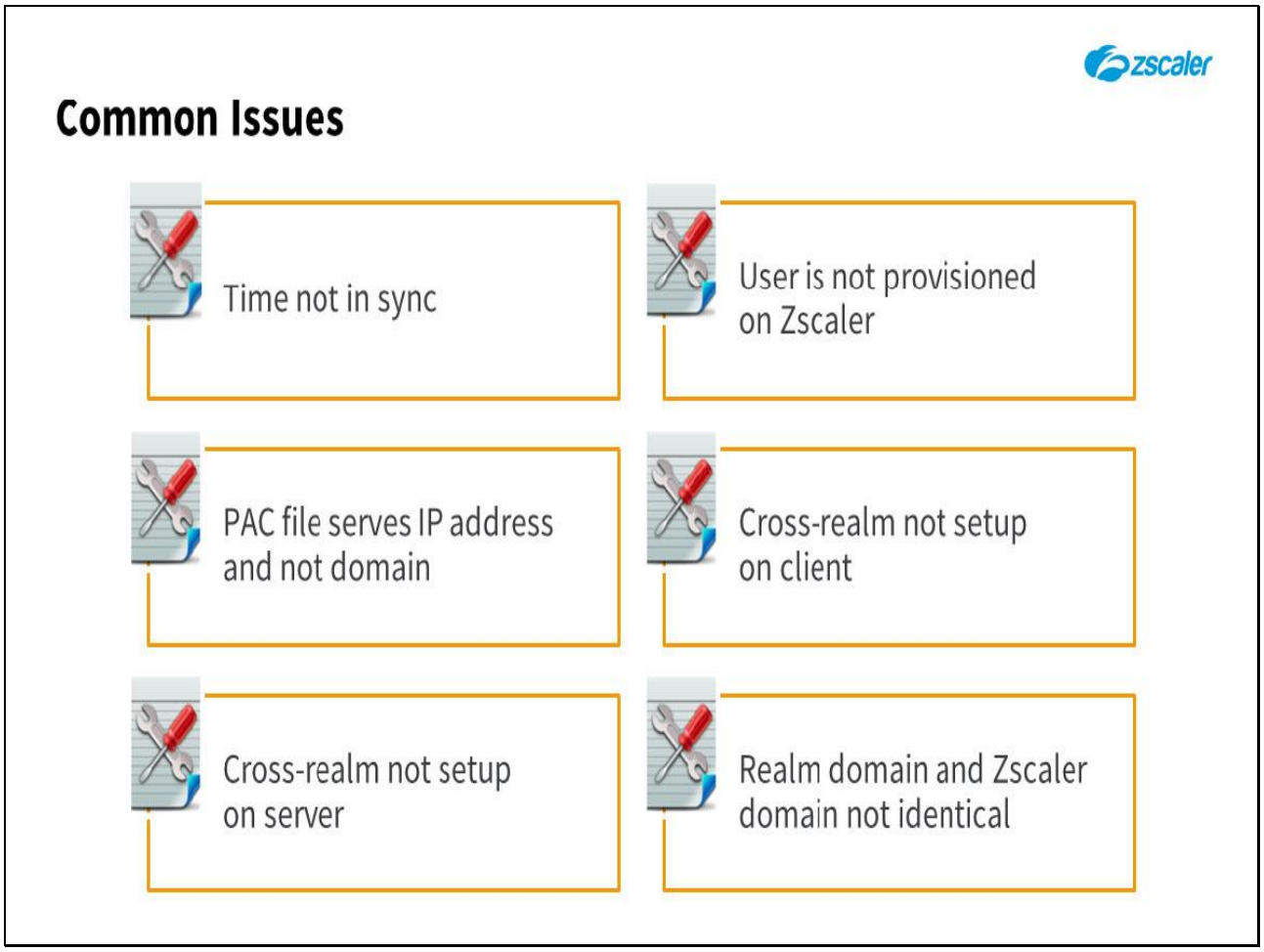
On the Windows PC first make sure it has joined the Domain then make the following registry changes. These can be made manually via Regedit or via GPO which is Best Practice. This concludes the configuration of Kerberos in the Zscaler solution. At this point your client workstations should be joined to the Domain and should be able to browse the internet with seamless authentication.

Slide 102 - Troubleshooting

Slide notes

Now that we have seen how to configure Kerberos let’s take a look at few moments to examine troubleshooting.

Slide 103 - Common Issues

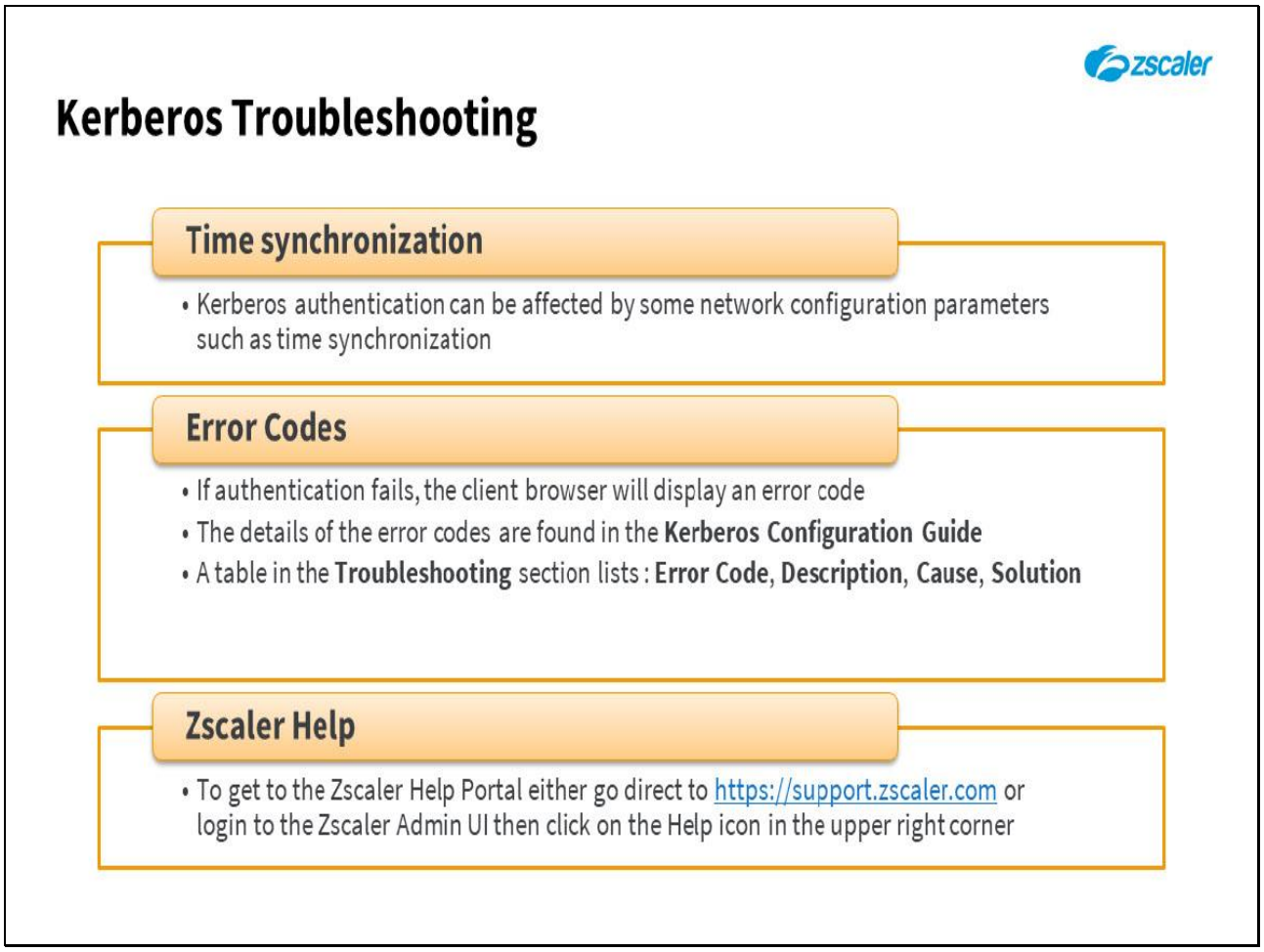


Slide notes

Some common issues of users being unable to authenticate are:

- Time not in sync. If the time between the PC and Domain controller are off by 5 to 10 minutes authentication errors will result. All workstations should synchronize with the Domain controller then the Domain controller will use NTP to set its own time.
- A user will fail to authenticate if the user account information is not in the Zscaler database. Remember, Kerberos does not provide provisioning services and users must be provisioned with one of the supported methods.
- A misconfiguration of the PAC file stating IP addresses will cause Kerberos to fail. All references must be to the domain and not the IP.
- The cross-realm trust was not properly setup on the server,
- …or client.
- And lastly if the domain name and Zscaler domain do not match authentication will also fail.

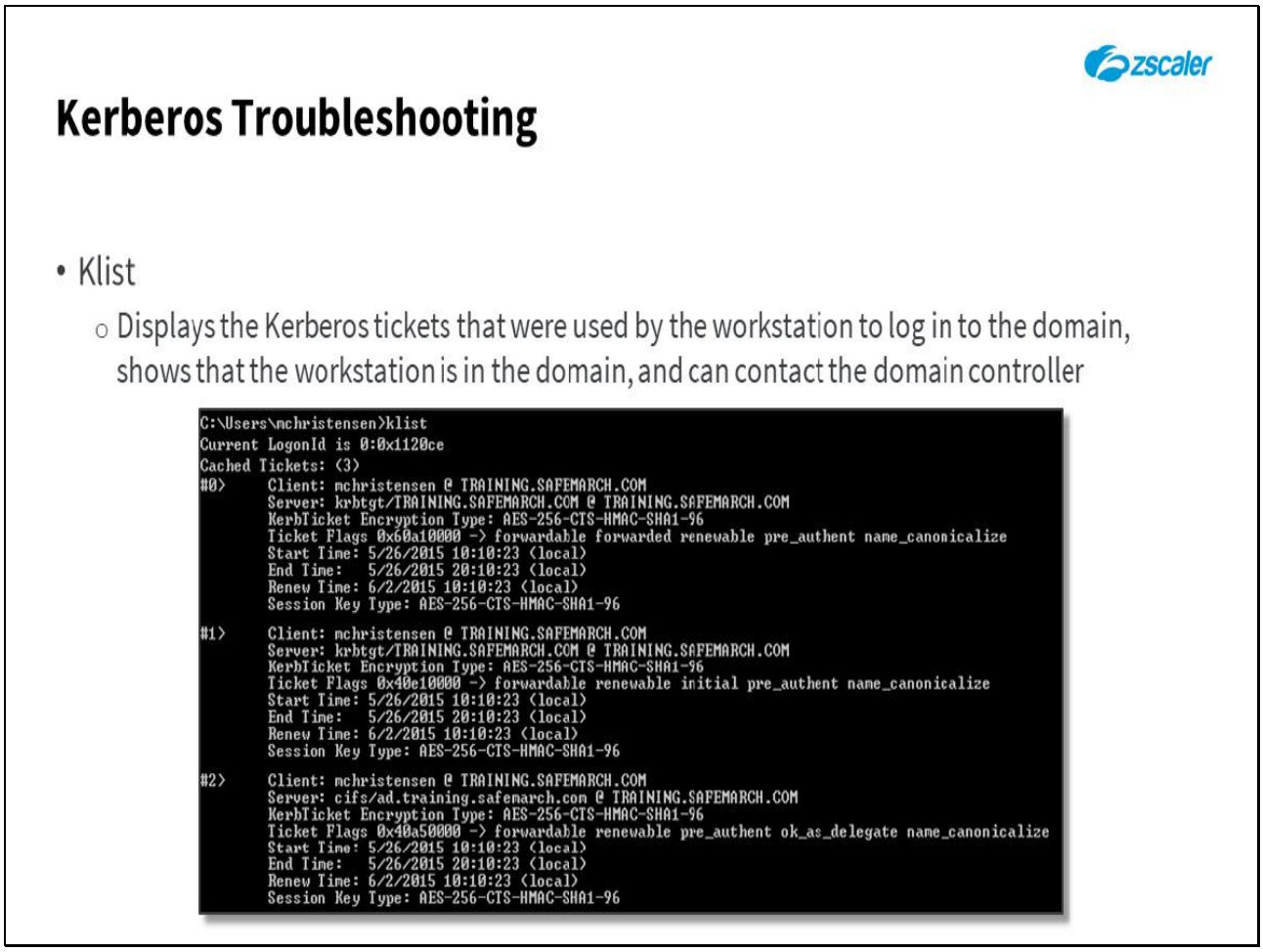
Slide 104 - Kerberos Troubleshooting



Slide notes

Kerberos authentication can be affected by some network configuration parameters such as time synchronization. If authentication fails, the client browser displays an error code. The details of the error codes are found in the Troubleshooting section of the Kerberos Configuration Guide. A table in the Troubleshooting section lists the following: error code, description, cause, solution.

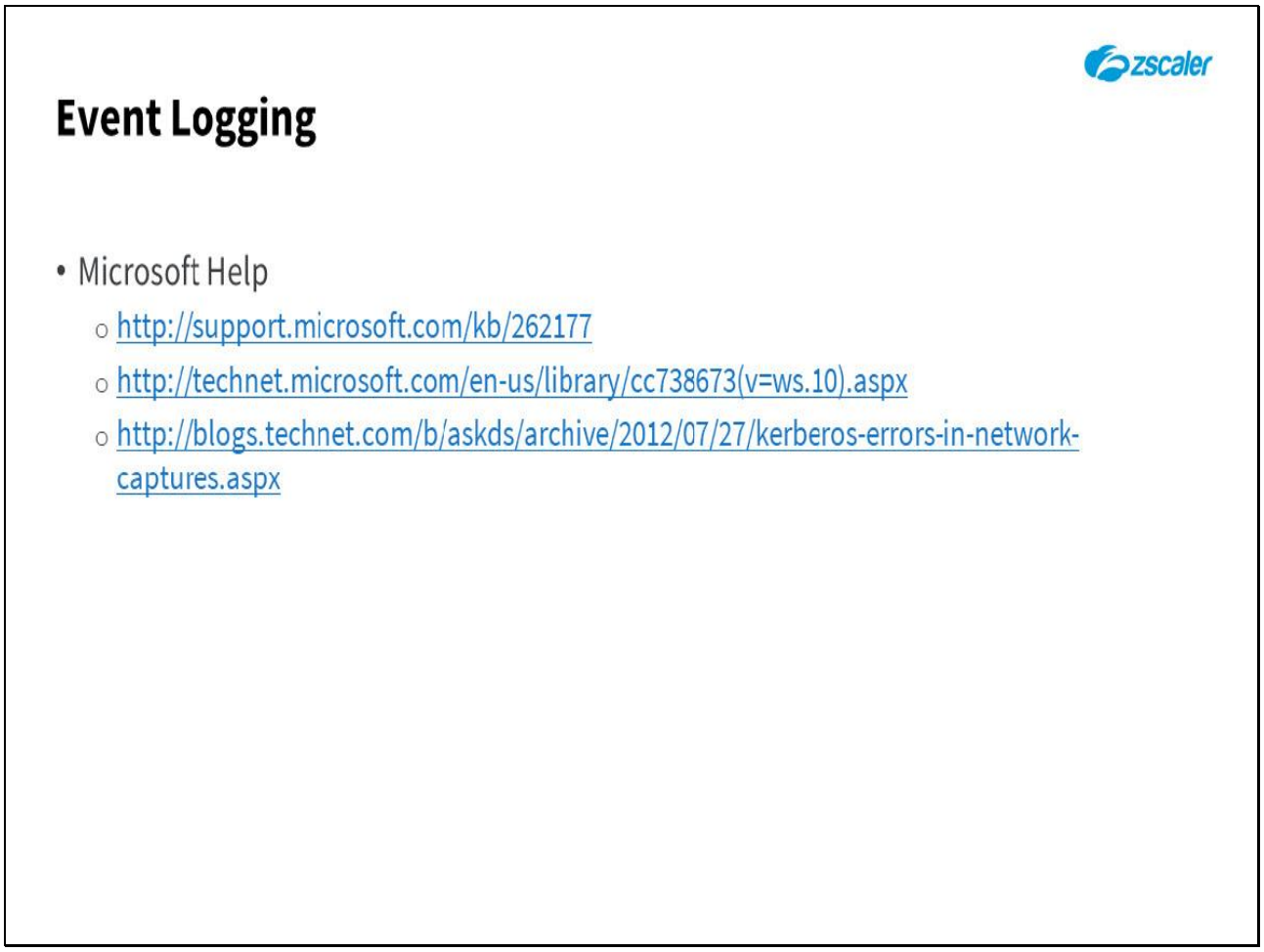
Slide 105 - Kerberos Troubleshooting



Slide notes

klist displays the Kerberos tickets that were used by the workstation to log in to the domain and shows that the workstation is in to the domain and can contact the domain controller. If, when you run **klist**, the Kerberos tickets are not displayed, then there is an inherent domain or workstation configuration issue that must be resolved before you proceed.

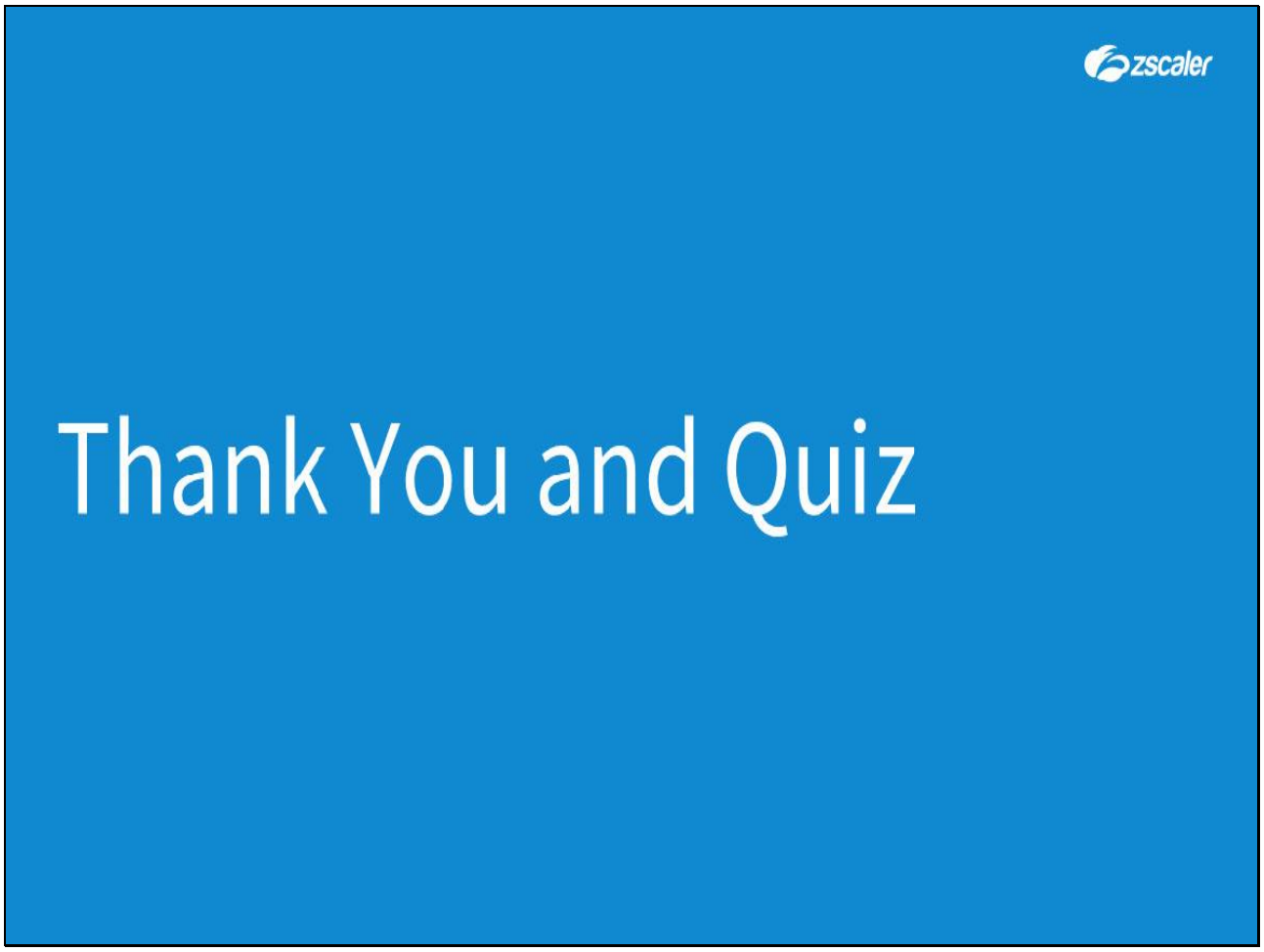
Slide 106 - Event Logging



Slide notes

For more information on Kerberos troubleshooting see the following Microsoft knowledgebase articles and the links shown on this slide.

Slide 107 - Thank You and Quiz



Slide notes

Thank you for participting in this eLearning module on Kerberos authentication.

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