

Slide 1 - ZCCP-IA



ZCCP-IA

Authentication – Kerberos

©2018 Zscaler, Inc. All rights reserved.

Slide notes

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

Slide 2 - Navigating the eLearning Module

Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. At the top right is the Zscaler logo. In the bottom right corner of the dashboard, there is an 'Exit' button. Along the bottom edge of the dashboard, several control buttons are overlaid with blue callout boxes:

- Previous Slide
- Next Slide
- Play/Pause
- Fast Forward
- Progress Bar
- Audio On/Off
- Closed Captioning

The dashboard itself displays various metrics and charts, including a large donut chart showing 391.3 MB and 16.8 K, and a list of top users.

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

Agenda



- Understanding Kerberos
- Interactive Demo
 - Zscaler Configuration
 - Windows Server 2012 Configuration
 - Back to Zscaler to Modify AD Settings
 - Windows PC Configuration
- Troubleshooting

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



Understanding Kerberos

Slide notes

Slide 5 - Why Kerberos?

Why Kerberos?



- Kerberos is an industry standard secure protocol
 - Kerberos does not use cookies for authentication
 - It is a widely-used ticket-based authentication protocol

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?

Why Kerberos?

- Kerberos is an industry standard secure protocol
 - Kerberos does not use cookies for authentication
 - It is a widely-used ticket-based authentication protocol

SSL Traffic	Secure	Windows 8 Metro Apps
<ul style="list-style-type: none">• Kerberos enables authentication without decryption• No Cookies - No HTTP Redirect	<ul style="list-style-type: none">• Does not require communications between AD and Zscaler and passwords are never stored in Zscaler	<ul style="list-style-type: none">• Lack complete HTTP support• Support Kerberos
Single Sign On		Portability
<ul style="list-style-type: none">• Users are not prompted for username/password		<ul style="list-style-type: none">• Most modern OS and browsers support 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

User Provisioning and Authentication

- Industry standard secure protocol for secure authentication using 'Tickets' rather than Cookies

Provisioning	Authentication	Benefits	Challenges
<ul style="list-style-type: none">• Flexible provisioning; manual creation, CSV import, LDAP sync	<ul style="list-style-type: none">• Explicit forwarding is required (PAC file)• Firewall must allow:	<ul style="list-style-type: none">• Support for applications that do not use Cookies (e.g. O365)• Single Sign-on for multiple services• Supported by most OS's and Browsers	<ul style="list-style-type: none">• No auto-provisioning of users• No support for Windows XP, Apple iOS, or Android

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



User Provisioning and Authentication

- Industry standard secure protocol for secure authentication using 'Tickets' rather than Cookies

Provisioning			Authentication		Benefits		Challenges	
Source	Destination	Destination Port	Description					
Client Workstation	CAIP address ZEN IP address ranges	TCP / UDP 88 TCP 8800 (default Kerberos port on ZENs)	Enables the client to auth against the Zscaler Domain KDC	Enables the client to send traffic to the global Kerberos authentication port on the ZEN. Not required if Kerberos is enabled on a location. Enabling Kerberos on a location automatically enforces Kerberos authentication, so you can send traffic to the default proxy ports, such as port 80	Support for applications that do not use Cookies (e.g. O365)	Single Sign-on for multiple services	Supported by most OS's and Browsers	No auto-provisioning of users No support for Windows XP, Apple iOS, or Android

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 need to ensure that the client workstation can open outbound connections to the Zscaler cloud.

Slide 9 - Provisioning and Authentication Flow

Provisioning and Authentication Flow

1.

Provisioning

- Administrator configures authentication profile
- Users, groups and departments are provisioned on the Cloud
- Provisioning Methods: Manual (CSV Import), Zscaler Authentication Bridge (ZAB), LDAP Bind, SAML Auto-provisioning

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

Provisioning and Authentication Flow

1.

Provisioning

- Administrator configures authentication profile
- Users, groups and departments are provisioned on the Cloud
- Provisioning Methods: Manual (CSV Import), Zscaler Authentication Bridge (ZAB), LDAP Bind, SAML Auto-provisioning

2.

Policy Configuration

- Administrator creates policy for group or users

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

Provisioning and Authentication Flow

1.

Provisioning

- Administrator configures authentication profile
- Users, groups and departments are provisioned on the Cloud
- Provisioning Methods: Manual (CSV Import), Zscaler Authentication Bridge (ZAB), LDAP Bind, SAML Auto-provisioning

2.

Policy Configuration

- Administrator creates policy for group or users

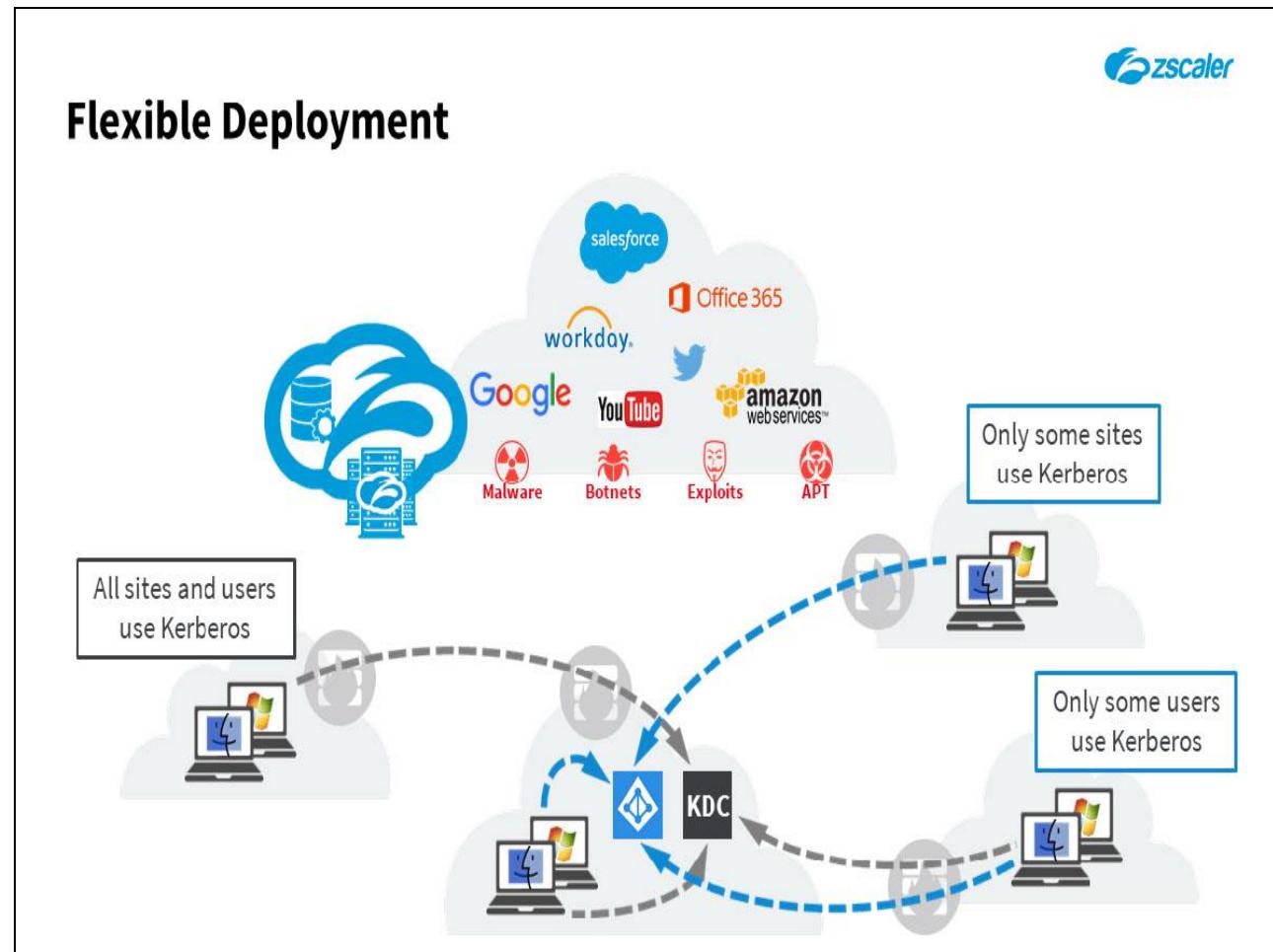
3.

Authentication

- User is challenged for the authentication
- Upon authentication appropriate policy is enforced

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

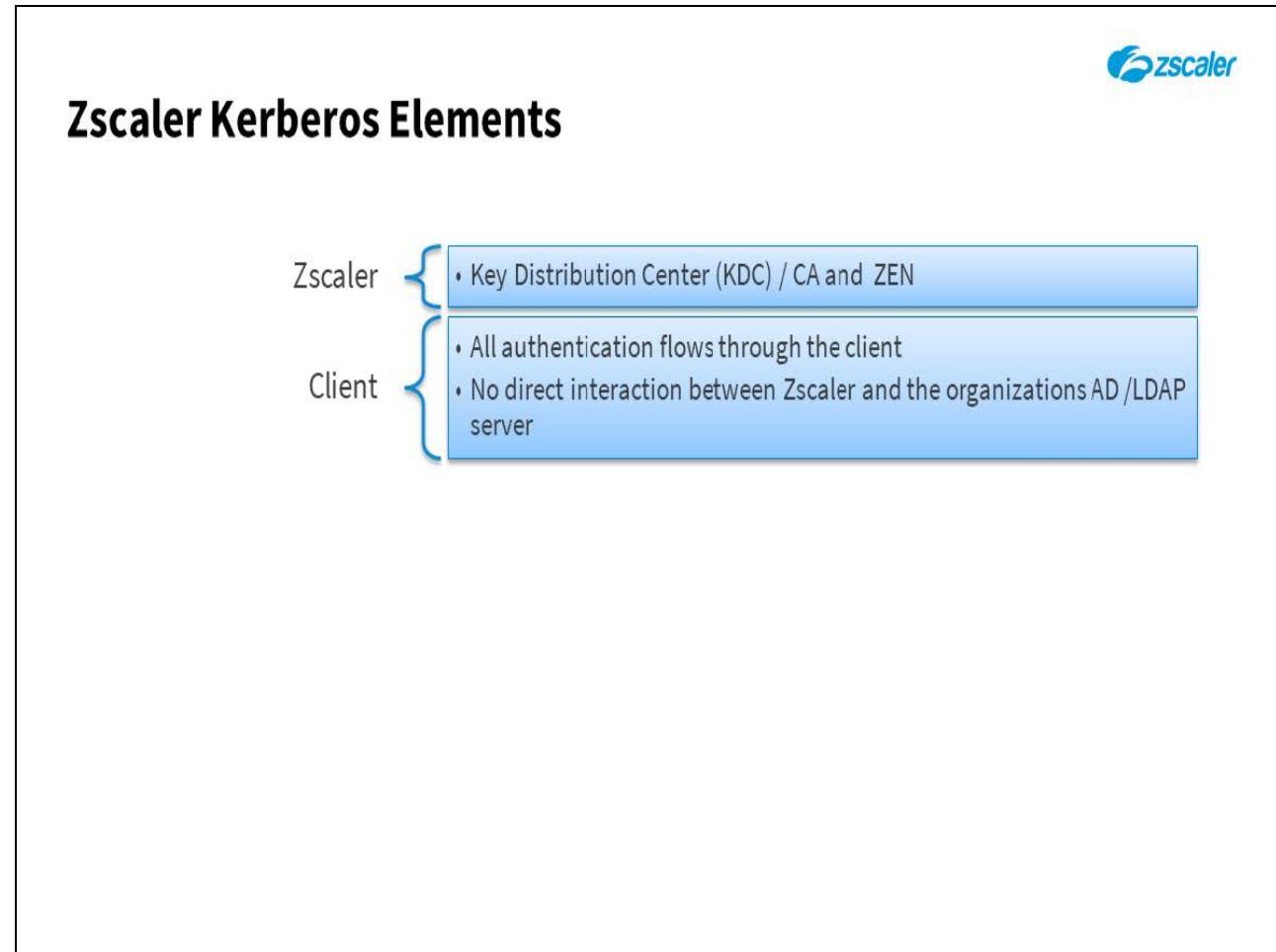
Zscaler Kerberos Elements

Zscaler { • Key Distribution Center (KDC) / CA and ZEN

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.

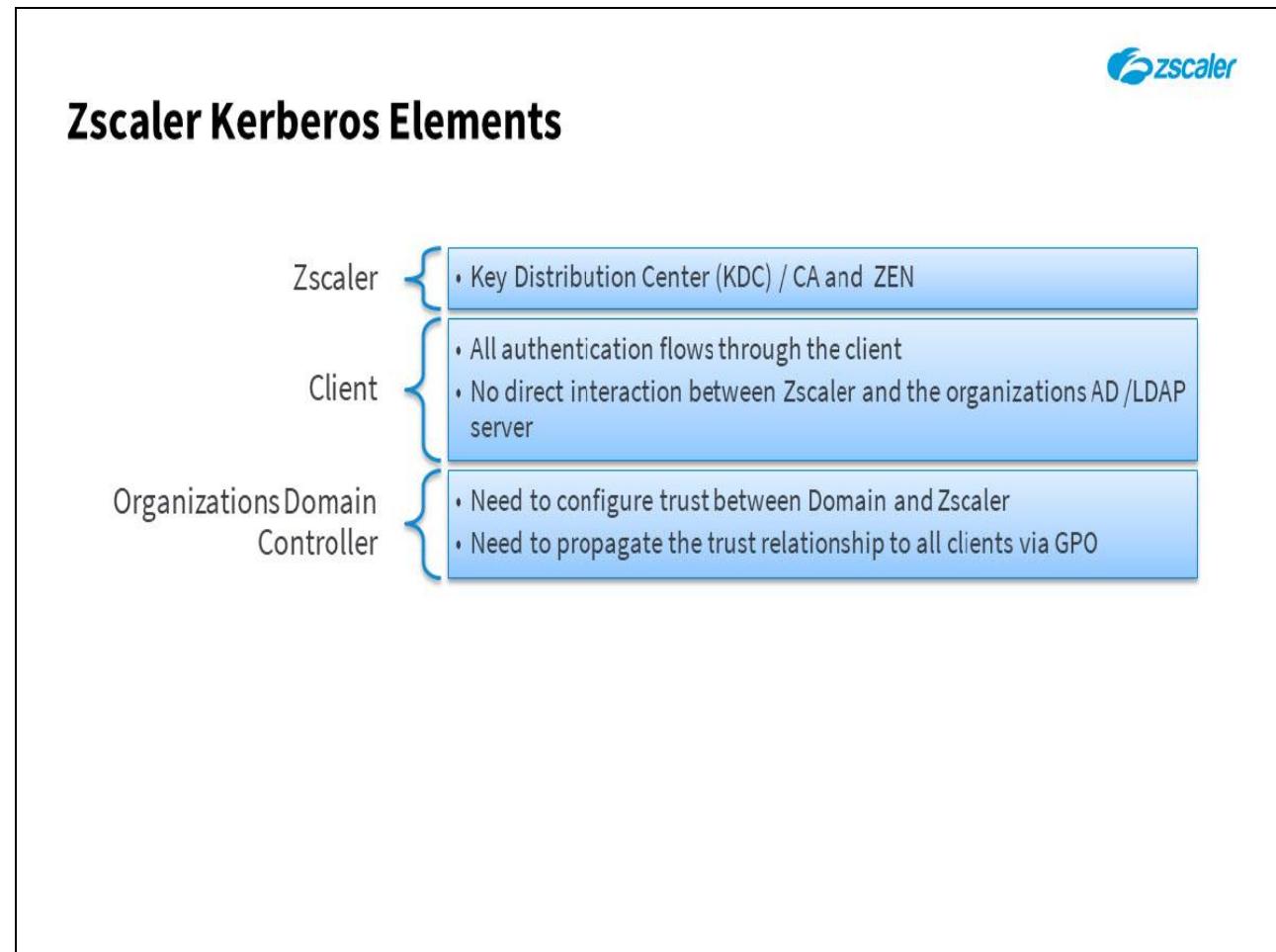
Slide 14 - Zscaler Kerberos Elements

The slide features the Zscaler logo in the top right corner. The main title "Zscaler Kerberos Elements" is centered at the top. Below the title, there are two columns: "Zscaler" and "Client". A curly brace groups the two columns. To the right of the brace is a blue box containing three bullet points. The Zscaler column has one bullet point, and the Client column has two.

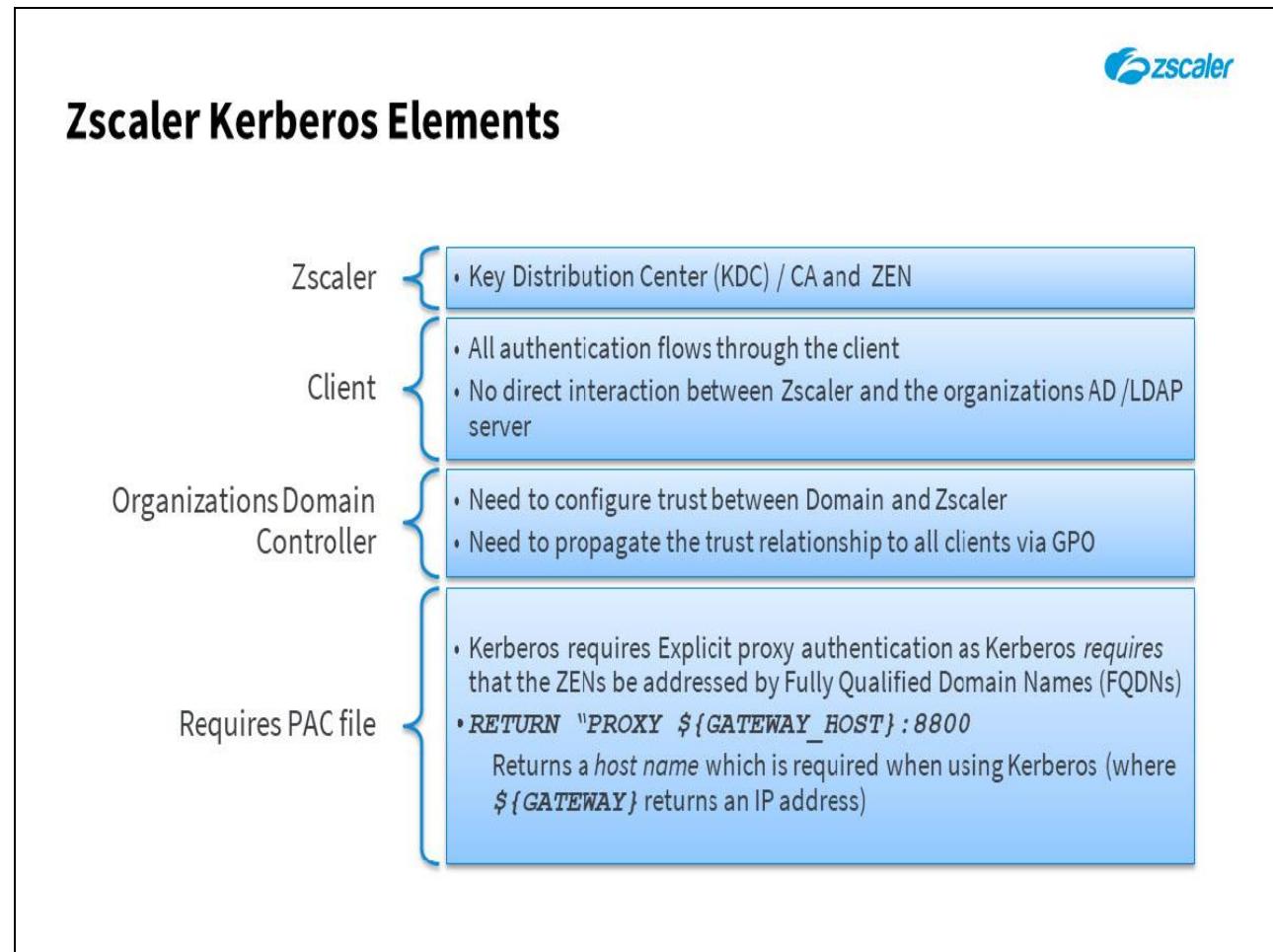
Zscaler	<ul style="list-style-type: none">• Key Distribution Center (KDC) / CA and ZEN
Client	<ul style="list-style-type: none">• All authentication flows through the client• No direct interaction between Zscaler and the organizations AD /LDAP server

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.

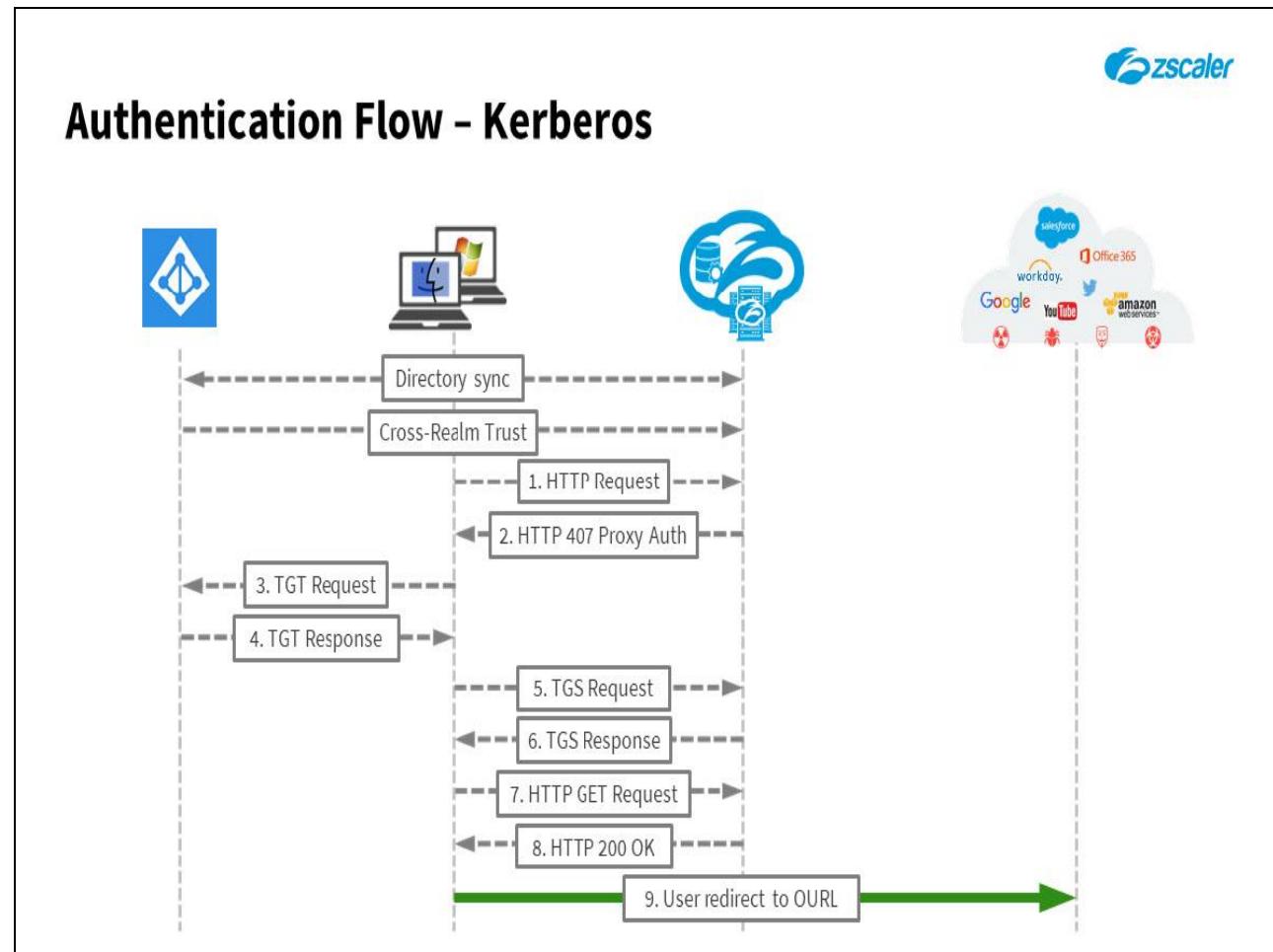
Slide 15 - Zscaler Kerberos Elements**Slide notes**

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

PAC Variables Introduced for Name Substitution

```
return "DIRECT";

/* FTP goes directly */
if (url.substring(0,4) == "ftp:")
return "DIRECT";

/* Updates are directly accessible */
if ((localHostOrDomainIs(host, "trust.zscaler.com")) && (url.substring(0,5) == "http:" || url.substring(0,6) == "https:"))
return "DIRECT";

/* Default Traffic Forwarding. Forwarding to Zen on port 80, but you can use port 9400 also */
return "PROXY ${GATEWAY_HOST}:8800; PROXY ${SECONDARY_GATEWAY_HOST}:8800; DIRECT";
```

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

Platforms Supported

Supported

- Windows:
 - Windows Vista and above
 - Transparent configuration on Windows
- Windows Tablets:
 - Tested on Windows 8 Surface
- Mac: Tested
- Linux: Tested

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

Platforms Supported

Supported	NOT Supported
<ul style="list-style-type: none">• Windows:<ul style="list-style-type: none">◦ Windows Vista and above◦ Transparent configuration on Windows• Windows Tablets:<ul style="list-style-type: none">◦ Tested on Windows 8 Surface• Mac: Tested• Linux: Tested	<ul style="list-style-type: none">• Windows XP• IOS• Android

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 ?

Do Applications Support Kerberos ?

- Windows Metro apps will work seamlessly
- Non-Microsoft apps (Dropbox, etc.) do not 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

Kerberos Configuration high-level

- Zscaler Admin UI
 - 1. Enable Kerberos authentication and generate a cross-realm trust password
 - 2. Enable/Disable Kerberos for a location
 - 3. Use hostname variables in PAC File to resolve to domain names instead of IP Addresses
 - 4. Kerberos and SAML configuration can co-exist
- Customer
 - 1. Configure inbound realm trust on the domain controller
 - 2. Propagate the changes to Windows clients by GPO update (or manually via **regedit**)
 - 3. Configure Mac/Linux workstations by minor modification to Kerberos config file

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.

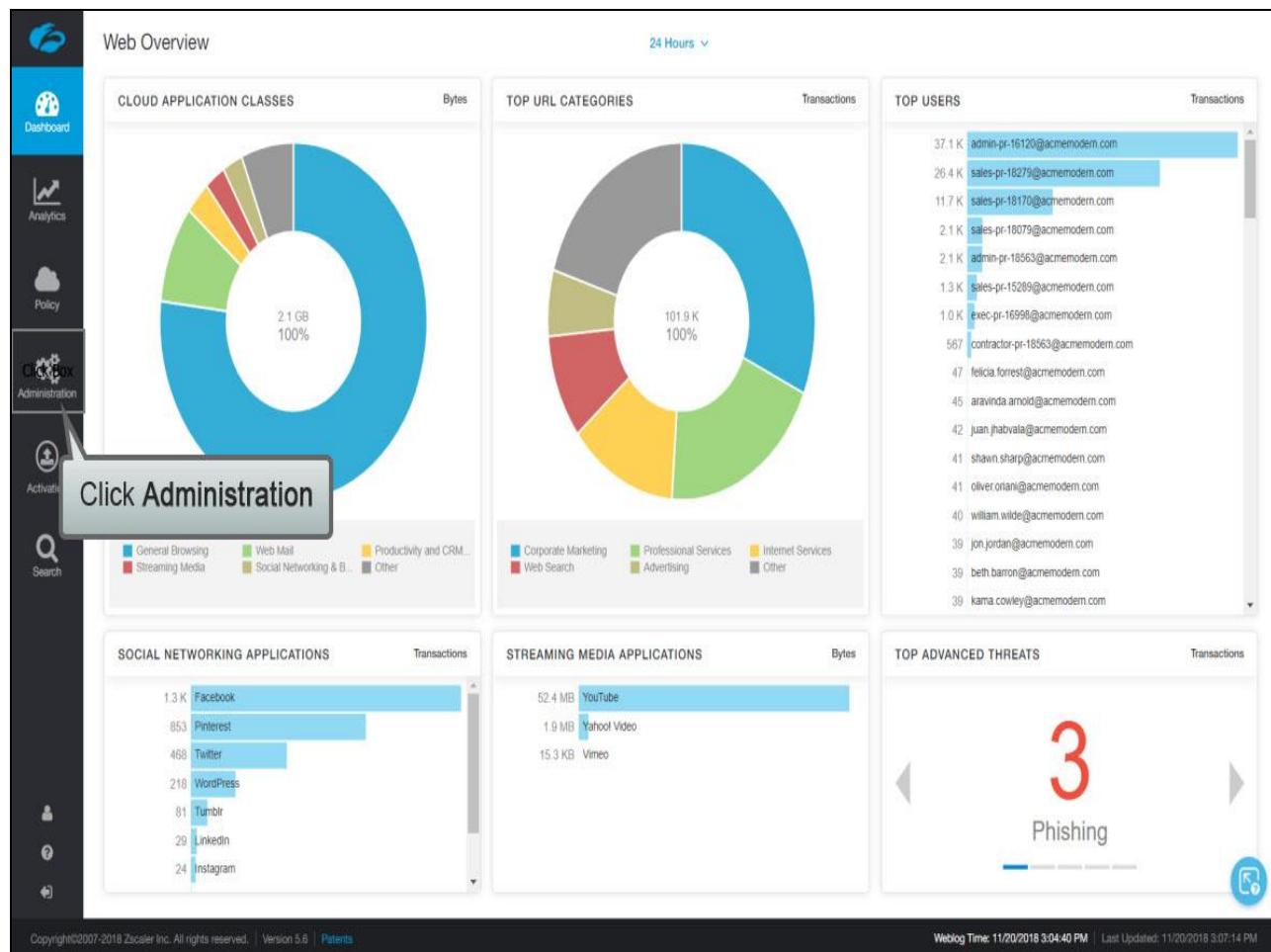
Slide 23 - Zscaler Configuration



Slide notes

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

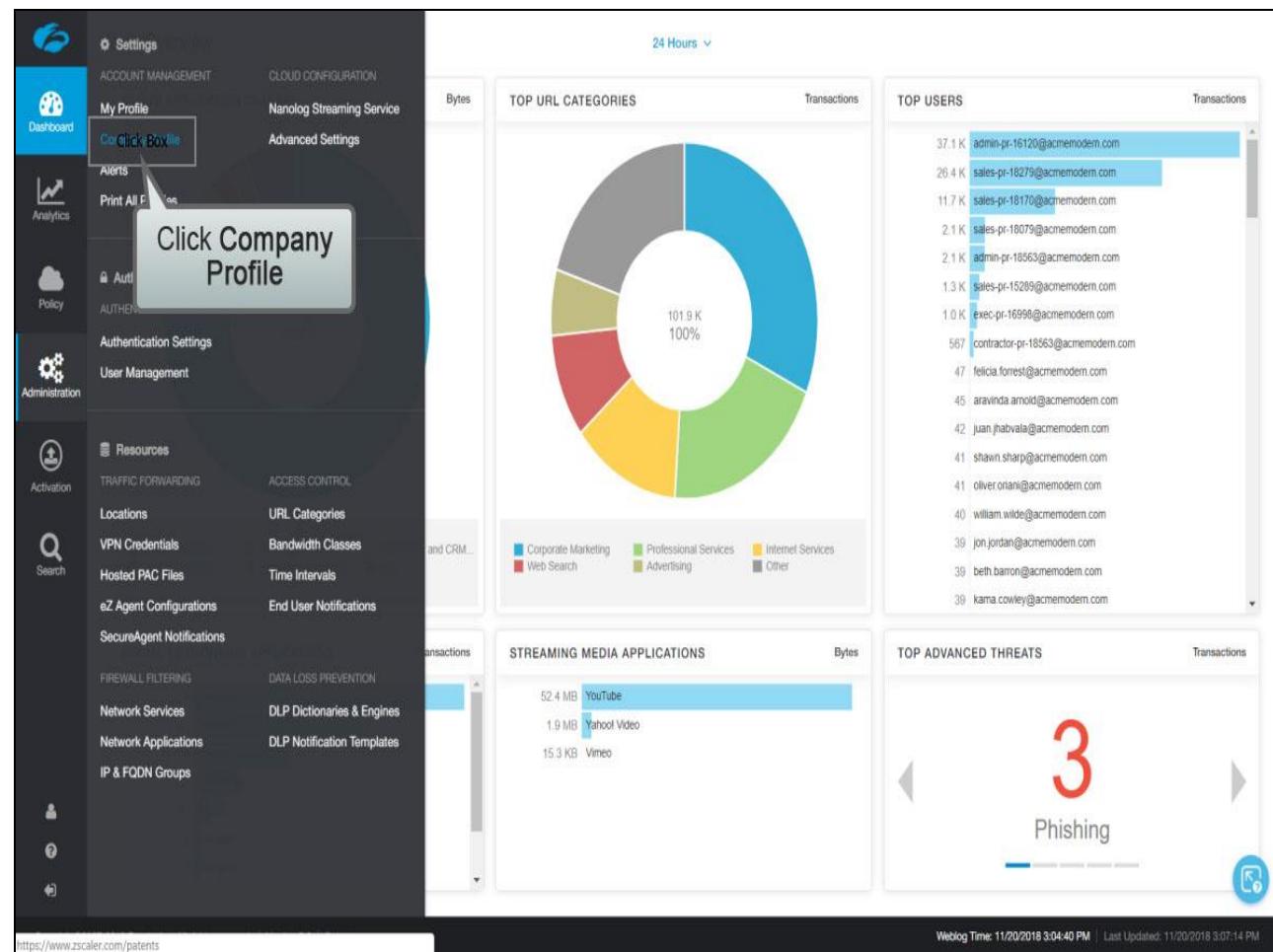
Slide 24 - Slide 24



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

The screenshot shows the Zscaler Click Administration interface. On the left is a dark sidebar with various icons: a gear, a bar chart, a cloud, a person, a magnifying glass, and a gear labeled "Click Box Administration". The main area is titled "Company Profile" and has tabs for "ORGANIZATION" and "SUBSCRIPTIONS". Under "GENERAL INFORMATION", there is a "Company ID" field containing "zscalerone.net-551294", a "Name" field containing "training2.safemarch.com", and a "Domains" field also containing "training2.safemarch.com". A callout box with a red border highlights the "Domains" field with the text "Check the Domains for the account". Below these fields are "Address Line 1", "City", "State", and "ZIP Code" input fields, each with their respective values. At the bottom are "Save" and "Cancel" buttons, and a "Print" icon.

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

The screenshot shows the Zscaler Admin UI interface. On the left, there is a vertical navigation menu with several sections: Dashboard, Analytics, Policy, Administration (which is currently selected), Activation, Search, and Reference. Under the Administration section, there are links for Account Management, Cloud Configuration, My Profile, Company Profile, Alerts, Print All Policies, Partner Integrations (with a 'NEW' badge), Authentication Configuration, Administration Controls, User Management, Role Management, Identity (with a 'CONTINUE' button), Audit Logs (with a 'NEW' badge), Traffic Forwarding, Access Control, Locations, URL Categories, VPN Credentials, Bandwidth Classes, Hosted PAC Files, Time Intervals, eZ Agent Configurations, End User Notifications, SecureAgent Notifications, Firewall Filtering, Data Loss Prevention, Network Services, DLP Dictionaries & Engines, Network Applications, DLP Notification Templates, and IP & FQDN Groups. A large callout box with a blue border and white text is overlaid on the screen, pointing to the 'Authentication Settings' link under the Administration section. The callout box contains the text 'Click Authentication Settings'. At the bottom of the page, there is a copyright notice: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'.

Slide notes

Then **Authentication Settings**.

Slide 28 - Slide 28

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Authentication Settings' and has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', there's a section for 'Directory Type' where 'Active Directory' is selected (highlighted with a red box). A callout bubble says 'Active Directory is being used in this case for user provisioning'. Other options in this section include 'Hosted DB', 'OpenLDAP', 'Setup Wizard', and 'Advanced Configuration'. Below this are sections for 'Authentication Frequency' (set to 'Daily'), 'Authentication Type' (set to 'Form-Based'), and 'Temporary Authentication' (disabled). In the 'DIRECTORY SYNCHRONIZATION' section, there's a 'Sync Now' button. The 'KERBEROS AUTHENTICATION' section has a 'Enable Kerberos' toggle switch that is off. A callout bubble says 'Scroll down...'. At the bottom, there are 'Save' and 'Cancel' buttons, and a copyright notice: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'.

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

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration (which is selected), Activation, and Search. The main content area is titled 'Authentication Settings' and contains several tabs: AUTHENTICATION PROFILE (selected), AUTHENTICATION BRIDGES, and TEMPORARY AUTHENTICATION. Under AUTHENTICATION PROFILE, 'Form-Based' is selected over 'SAML'. Under TEMPORARY AUTHENTICATION, 'Disabled' is selected over 'One-Time Token' and 'One-Time Link'. The 'KERBEROS AUTHENTICATION' section includes a checkbox labeled 'Enable Kerberos' with a red 'Click Box' overlay. A large gray callout box with the text 'Click to Enable Kerberos' points to this checkbox. Below the checkbox are buttons for 'Start' and 'Save' (disabled) or 'Cancel'. At the bottom of the page, a footer notes 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'.

Slide notes

Check **Enable Kerberos**.

Slide 30 - Slide 30

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', there are sections for 'Temporary Authentication' (disabled), 'DIRECTORY SYNCHRONIZATION' (last synchronization time is '...'), and 'KERBEROS AUTHENTICATION'. In the 'KERBEROS AUTHENTICATION' section, 'Enable Kerberos' is checked. Below it is a 'Domain Trust Password' field with options to 'Reveal Password' or 'Generate New Password'. At the bottom, there's a 'FORCE REAUTHENTICATION FOR ALL USERS' section with a 'Last Reauthentication' field and a 'Force' button. A callout bubble points to the 'Save' button in this section. At the very bottom, there are 'Click Box' and 'Cancel' buttons. The footer contains copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'.

Slide notes

Then **Save**.

Slide 31 - Slide 31

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Authentication Settings' with a message 'All changes have been saved.' A header bar includes tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', 'Directory Type' is set to 'Active Directory' (selected). 'Authentication Frequency' is set to 'Daily'. 'Authentication Type' is set to 'Form-Based' (selected). 'Temporary Authentication' is set to 'Disabled'. Under 'DIRECTORY SYNCHRONIZATION', there is a 'Sync Now' button. Under 'KERBEROS AUTHENTICATION', 'Enable Kerberos' is checked. A 'Domain Trust Password' field is present with 'Reveal Password' and 'Generate New Password' links. At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon.

Slide notes

Slide 32 - Slide 32

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Authentication Settings' and has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', 'Directory Type' is set to 'Active Directory' (selected). 'Authentication Frequency' is set to 'Daily'. 'Authentication Type' is set to 'Form-Based' (selected). 'Temporary Authentication' is set to 'Disabled'. Under 'DIRECTORY SYNCHRONIZATION', there is a 'Last Synchronization Time' section with a 'Sync Now' button. Under 'KERBEROS AUTHENTICATION', 'Enable Kerberos' is checked. A 'Domain Trust Password' field is present with 'Reveal Password' and 'Generate New Password' options. At the bottom are 'Save' and 'Cancel' buttons, and a 'Logout' icon.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

Slide 33 - Slide 33

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' and 'AUTHENTICATION BRIDGES', with 'AUTHENTICATION BRIDGES' selected. Under 'Temporary Authentication', 'One-Time Token' is highlighted. The 'KERBEROS AUTHENTICATION' section contains a checked checkbox for 'Enable Kerberos'. Below it, the 'Domain Trust Password' field is shown with a 'Reveal Password' link. A callout bubble points to this link with the text 'Click Reveal Password'. At the bottom, there are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 34 - Slide 34

The screenshot shows the 'Authentication Settings' page in the Zscaler Admin UI. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'Temporary Authentication', 'One-Time Token' is selected. 'DIRECTORY SYNCHRONIZATION' shows a 'Sync Now' button. 'KERBEROS AUTHENTICATION' has an 'Enable Kerberos' checkbox checked. 'Domain Trust Password' is listed as da4y0Ki1BbzJjAVD|5gZJ6BtA6Z20. 'FORCE REAUTHENTICATION FOR ALL USERS' includes a 'Start' button and a status message 'Reauthentication Status: None'. At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

Slide 35 - Slide 35

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left is a sidebar with icons for Dashboard, Analytics, Policy, Administration (selected), Activation, and Search. The main area has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'Temporary Authentication', 'One-Time Token' is selected. In the 'KERBEROS AUTHENTICATION' section, 'Enable Kerberos' is checked. A large callout box with the text 'Copy the Domain Trust Password' is overlaid on the 'Domain Trust Password' field, which contains the value 'da4y8K1BbzUjAVD5gZj6BtiA6Zl20'. A context menu is open over this field with options: Copy (highlighted with a red box), Conceal Password, Generate New Password, Search Google for 'da4y8K1BbzUjAVD5gZj6BtiA6Zl20', Print..., Ctrl+C, Inspect, and Ctrl+Shift+I. At the bottom are 'Save' and 'Cancel' buttons.

Slide notes

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

Slide 36 - Slide 36

The screenshot shows the 'Authentication Settings' page in the Zscaler Admin UI. The left sidebar has icons for Dashboard, Analytics, Policy, Administration (selected), Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' and 'AUTHENTICATION BRIDGES' (selected). Under 'Temporary Authentication', 'One-Time Token' is selected. 'DIRECTORY SYNCHRONIZATION' shows 'Last Synchronization Time' and a 'Sync Now' button. In the 'KERBEROS AUTHENTICATION' section, 'Enable Kerberos' is checked. A callout box with the text 'Click Conceal Password' points to the 'Conceal Password' button next to the 'Domain Trust Password' input field, which contains the value 'da4y@K1Bbz.UJAVD5gZj6BtA8z20'. Below this, there's a 'Click Box' button and a 'Generate New Password' link. The 'FORCE REAUTHENTICATION FOR ALL USERS' section includes a 'Start' button and a 'Reauthentication Status' field showing 'None'. At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon with a refresh symbol.

Slide notes

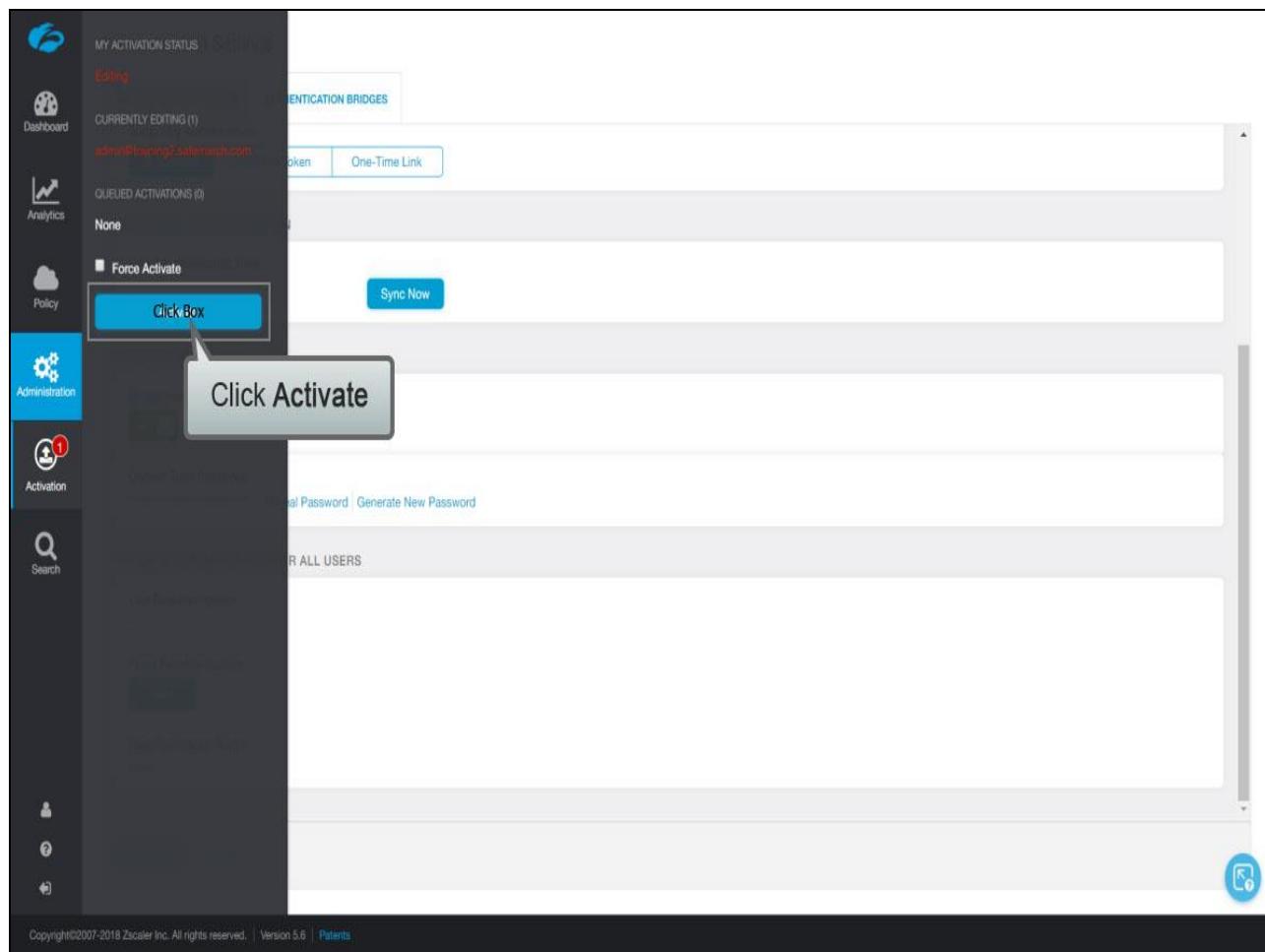
Click Conceal Password, ...

Slide 37 - Slide 37

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left, a vertical sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation (with a red '1' notification), and a Search bar. The main content area is titled 'Authentication Settings' and contains three tabs: 'AUTHENTICATION PROFILE' (selected), 'AUTHENTICATION BRIDGES', and 'TEMPORARY AUTHENTICATION'. Under 'TEMPORARY AUTHENTICATION', there are three options: 'Disabled' (selected), 'One-Time Token', and 'One-Time Link'. Below this is a 'DIRECTORY SYNCHRONIZATION' section with a 'Last Synchronization Time' field showing '---' and a 'Sync Now' button. The 'KERBEROS AUTHENTICATION' section includes an 'Enable Kerberos' checkbox (checked) and a 'Domain Trust Password' field with 'Reveal Password' and 'Generate New Password' links. A large callout box with the text 'Click Activation' is overlaid on the 'Enable Kerberos' section. At the bottom, there are 'Save' and 'Cancel' buttons, and a blue circular icon with a white 'K'.

Slide notes

...and **Activate** your changes.

Slide 38 - Slide 38**Slide notes**

Slide 39 - Slide 39

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'Temporary Authentication', 'One-Time Token' is selected. The 'DIRECTORY SYNCHRONIZATION' section shows 'Last Synchronization Time' and a 'Sync Now' button. The 'KERBEROS AUTHENTICATION' section has an 'Enable Kerberos' toggle switch (checked), a 'Domain Trust Password' field with 'Reveal Password' and 'Generate New Password' links, and a 'FORCE REAUTHENTICATION FOR ALL USERS' section with a 'Start' button and 'Reauthentication Status' (None). At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon.

Activation Completed!

AUTHENTICATION PROFILE AUTHENTICATION BRIDGES

Temporary Authentication

Disabled One-Time Token One-Time Link

DIRECTORY SYNCHRONIZATION

Last Synchronization Time Sync Now

KERBEROS AUTHENTICATION

Enable Kerberos

Domain Trust Password Reveal Password Generate New Password

FORCE REAUTHENTICATION FOR ALL USERS

Last Reauthentication

Force Reauthentication Start

Reauthentication Status None

Save Cancel

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Slide notes

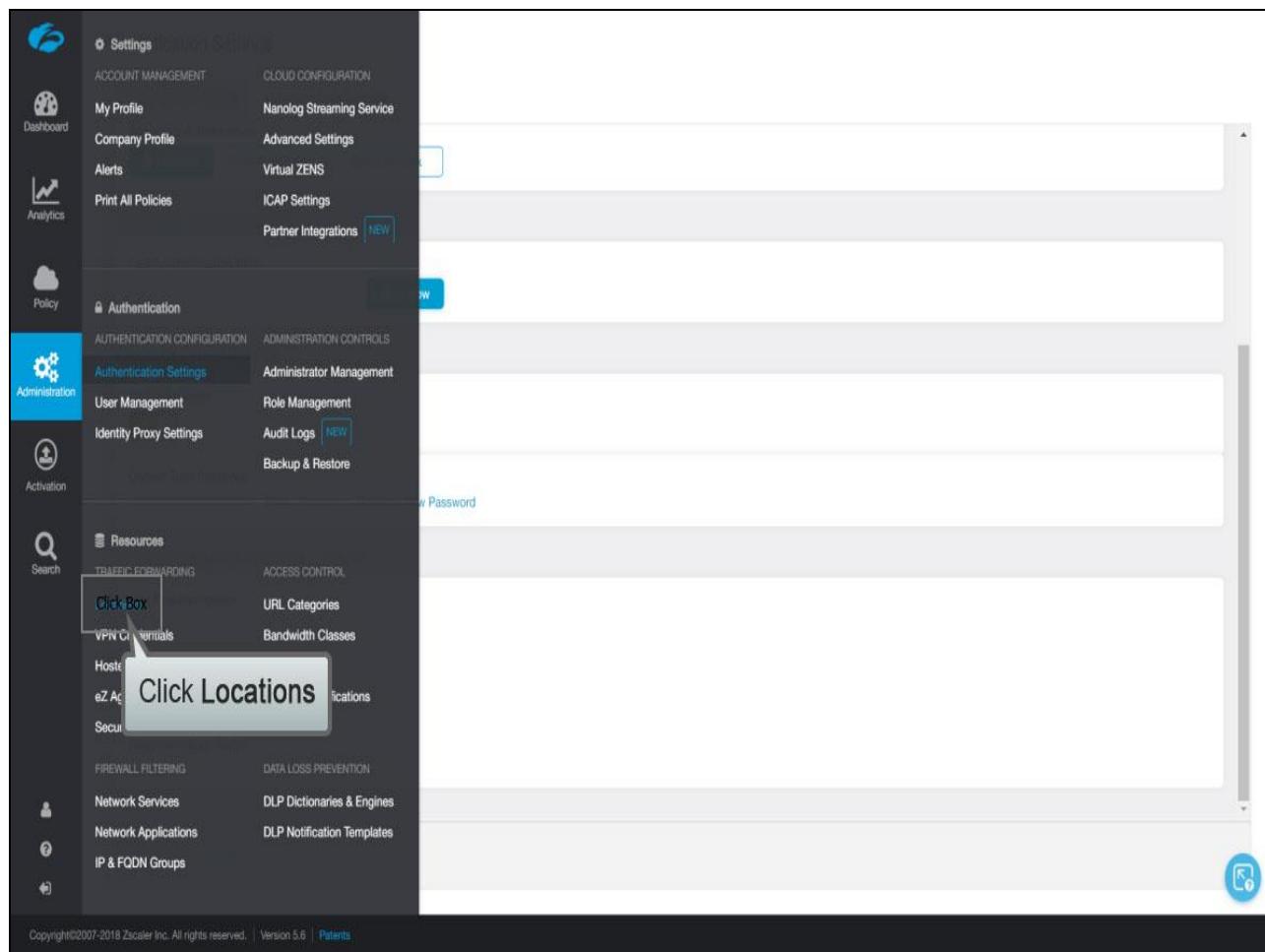
Slide 40 - Slide 40

The screenshot shows the Click Administration interface with a sidebar on the left containing icons for Dashboard, Analytics, Policy, Click Box Administration, Activation, and Search. The main content area is titled "Authentication Settings". It includes tabs for "AUTHENTICATION PROFILE" and "AUTHENTICATION BRIDGES" (which is selected). Under "Temporary Authentication", the "One-Time Token" option is highlighted. The "DIRECTORY SYNCHRONIZATION" section shows a "Last Synchronization Time" field with a "Sync Now" button. The "KERBEROS AUTHENTICATION" section has a checked checkbox for "Enable Kerberos". A modal window titled "Click Administration" is overlaid on the page, containing fields for "Old Password" and "Generate New Password", along with "Save" and "Cancel" buttons. At the bottom of the main content area, there is a "FORCE REAUTHENTICATION FOR ALL USERS" section with a "Start" button and a "Reauthentication Status" field showing "None". The footer of the page includes copyright information: "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients".

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

The screenshot shows the Zscaler Admin UI with the 'Locations' page selected. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area displays a table of locations. The first row, labeled 'Site_1', has a 'Click Box' callout pointing to the edit icon in the last column. The table columns are: No., Name, IP Addresses, Proxy Ports, X-Forwards..., Authentication..., SSL, Firewall Filter..., Bandwidth, Virtual ZENS, Group, and an edit icon.

No.	Name	IP Addresses	Proxy Ports	X-Forwards...	Authentication...	SSL	Firewall Filter...	Bandwidth	Virtual ZENS	Group	Edit
1	Site_1	184.170.227.125	---	---	Enabled	---	---	---	---	---	

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

...then click **Edit**.

Slide 43 - Slide 43

The screenshot shows the Zimbra Admin interface with the 'Locations' module selected. A modal window titled 'Edit Location' is open, displaying configuration for 'Site_1'. The 'LOCATION' section includes fields for Name (Site_1), Country (United States), State/Province (CA), and Time Zone (America/Los Angeles). The 'Group' field is set to 'None'. The 'ADDRESSING' section contains fields for Static IP Addresses (184.170.227.125), Proxy Ports (None), and VPN Credentials (None). The 'GRE Tunnel Information' section shows one entry with the following details:

No.	Tunnel Sourc...	Primary Desti...	Secondary D...	Primary Destination Internal Ra...	Secondary Destination Internal ...
1	184.170.227.125	199.168.151.8	197.156.241.234	172.17.20.32 - 172.17.20.35	172.1...

The 'Virtual ZENS' and 'Virtual ZEN Clusters' fields are both set to 'None'. At the bottom of the dialog are 'Save' and 'Cancel' buttons, and a 'Delete' button is located in the bottom right corner. A large gray callout box with the text 'Scroll down...' is overlaid on the right side of the dialog.

Slide notes

Slide 44 - Slide 44

The screenshot shows the 'Edit Location' dialog in the Zscaler Admin UI. The 'Enforce Authentication' checkbox is checked and highlighted with a red box. A callout box labeled 'Additional authentication options' points to the 'Enable IP Surrogate' and 'Enable Kerberos Authentication' checkboxes, which are also highlighted with a red box.

GRE Tunnel Information

No.	Tunnel Source...	Primary Destin...	Secondary D...	Primary Destination Internal Ra...	Secondary Destination Internal ...
1	184.170.227.125	199.168.151.8	197.156.241.234	172.17.20.32 - 172.17.20.35	172.17.20.36 - 172.17.20.39

Virtual ZENS

GATEWAY OPTIONS

- Enable XFF Forwarding (unchecked)
- Enforce Authentication** (checked)
- Enable IP Surrogate (unchecked)
- Enable Kerberos Authentication (unchecked)
- Enable Firewall Control (unchecked)
- Enable SSL Scanning (unchecked)

BANDWIDTH CONTROL

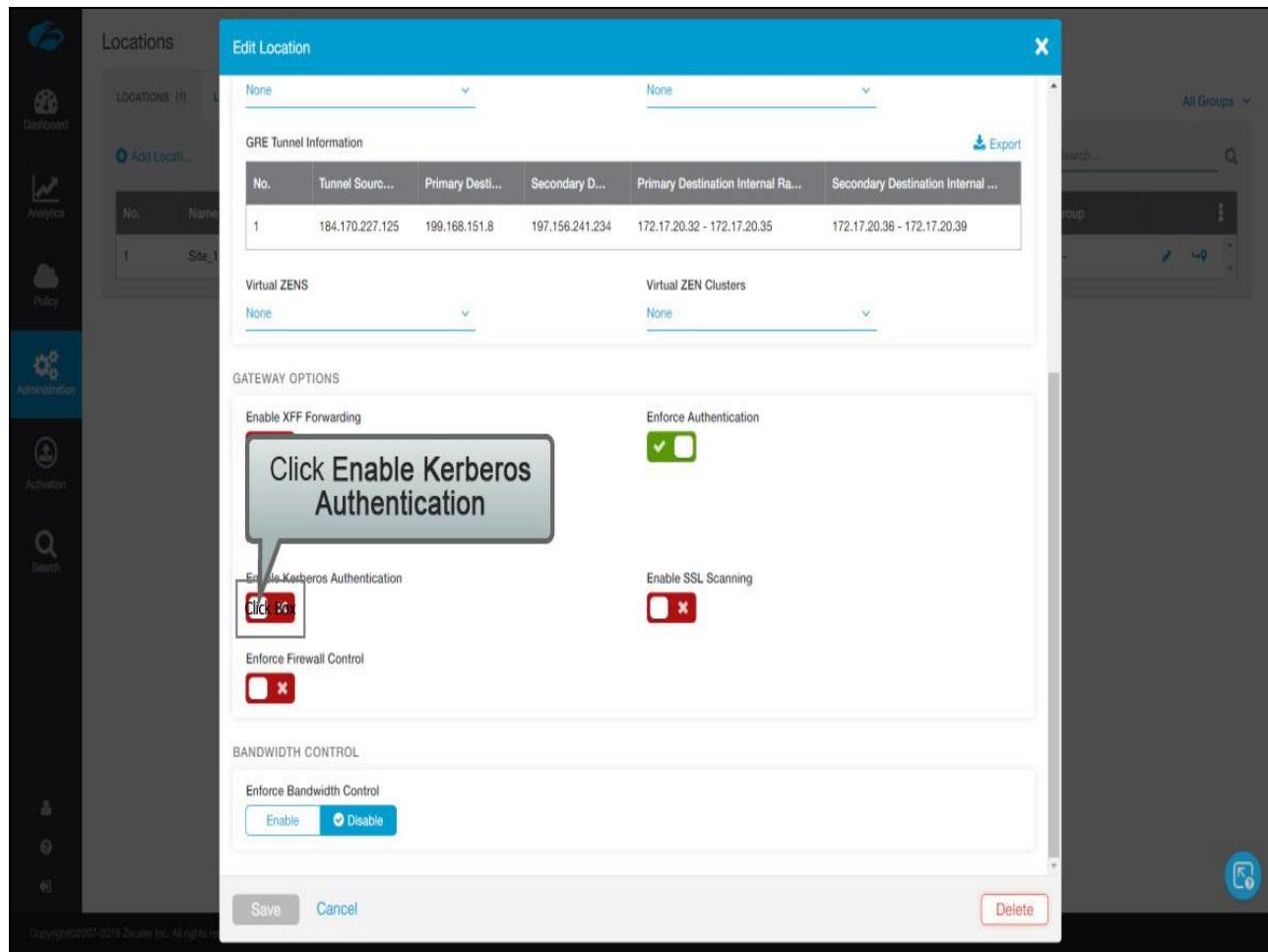
Enforce Bandwidth Control: Enable Disable

Save **Delete**

Slide notes

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

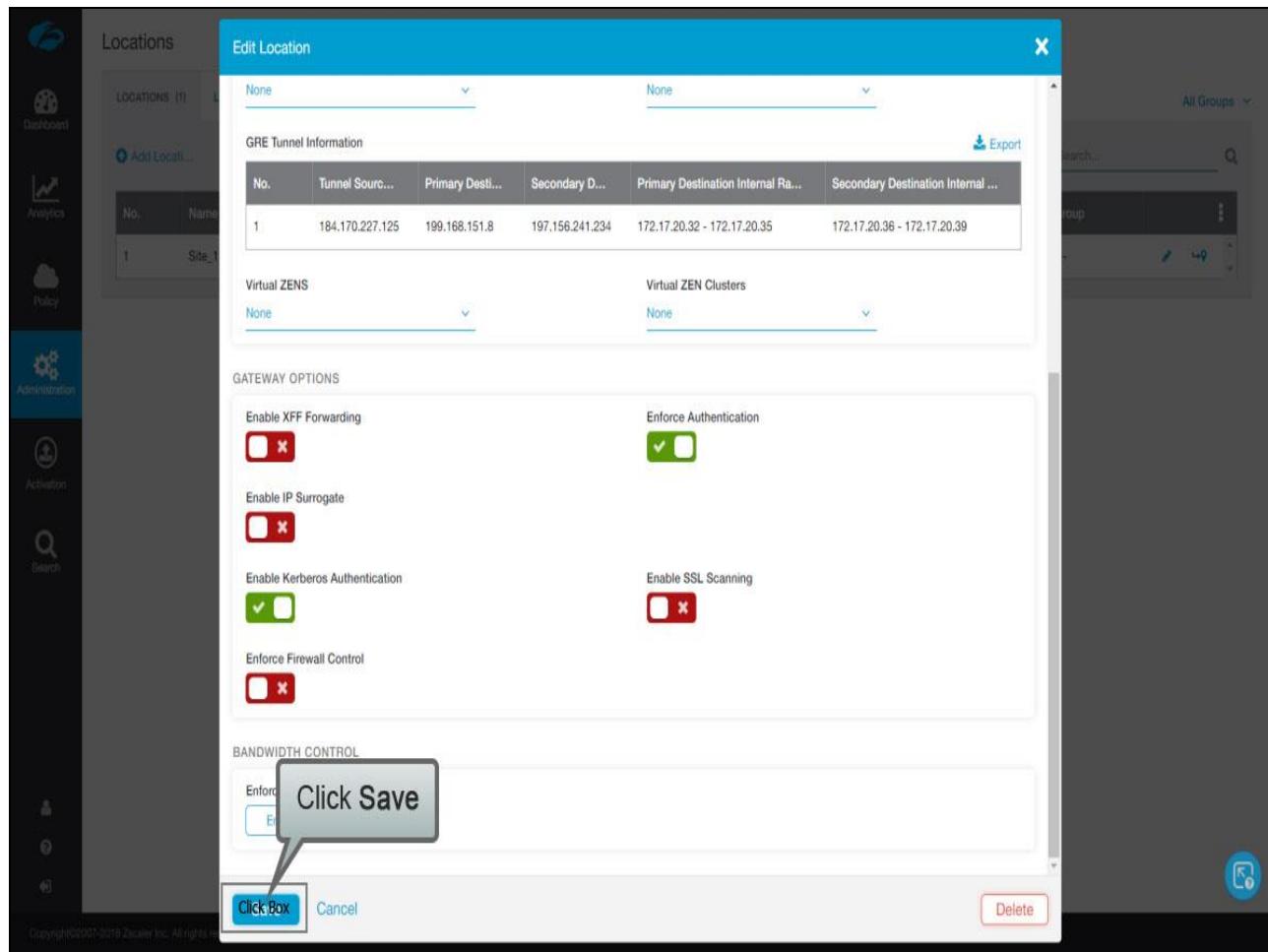
Slide 45 - Slide 45



Slide notes

Check **Enable Kerberos Authentication**, ...

Slide 46 - Slide 46



Slide notes

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

Slide 47 - Slide 47

The screenshot shows the Zscaler Admin UI with the 'Locations' page open. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a header 'Locations' with a save message 'All changes have been saved.' and a close button. Below is a table with columns: No., Name, IP Addresses, Proxy Ports, X-Forwards..., Authentication, SSL, Firewall Filter, Bandwidth, Virtual ZENS, Group, and actions. One row is shown: Site_1, 184.170.227.125, ---, ---, Enabled: Kerb..., ---, ---, ---, ---, ---, and actions. There are tabs for 'LOCATIONS (1)' and 'LOCATION GROUPS (0)'. A search bar and a 'All Groups' dropdown are at the top right.

No.	Name	IP Addresses	Proxy Ports	X-Forwards...	Authentication	SSL	Firewall Filter	Bandwidth	Virtual ZENS	Group	Actions
1	Site_1	184.170.227.125	---	---	Enabled: Kerb...	---	---	---	---	---	Edit Delete

Slide notes

Slide 48 - Slide 48

The screenshot shows the Zscaler Cloud interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation (which has a red notification badge), and Search. The main content area is titled 'Locations' and displays a table with one row. The table columns are: No., Name, IP Addresses, Proxy Ports, X-Forwards..., Authentication, SSL, Firewall Filter, Bandwidth, Virtual ZENS, Group, and Actions. The single entry is Site_1 with IP 184.170.227.125. Below the table are buttons for Add Location, Import Location, Download, Sample Import, Enter Group, and a search bar. A callout box with the text 'Click Activation' points to the Activation icon in the sidebar.

No.	Name	IP Addresses	Proxy Ports	X-Forwards...	Authentication	SSL	Firewall Filter	Bandwidth	Virtual ZENS	Group	Actions
1	Site_1	184.170.227.125	---	---	Enabled: Kerb...	---	---	---	---	---	Edit Delete

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | [Patents](#)

Slide notes

Slide 49 - Slide 49

The screenshot shows the Zscaler interface with the following details:

- Left Sidebar:** Includes icons for Dashboard, Analytics, Policy, Administration, Activation (with a red notification badge), and Search.
- Header:** Shows "MY ACTIVATION STATUS" and "CURRENTLY EDITING (1)" with the URL "admin@zscaler-test.com".
- Content Area:** Displays a table with one row:

	IP Addresses	Proxy Ports	X-Forwards...	Authentical...	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	...
	64.170.227.125	---	---	Enabled: Kerb...	---	---	---	---	---	Edit
- Annotations:** A blue rectangular box surrounds the "Force Activate" checkbox in the table header. A grey callout bubble with the text "Click Box" points to this area. Another grey callout bubble with the text "Click Activate" points to the "Edit" link in the table's last column.
- Footer:** Shows "Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients".

Slide notes

Slide 50 - Slide 50

The screenshot shows the Zscaler Admin UI with the 'Locations' page open. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has a header 'Activation Completed!' with a close button. Below it, there are tabs for 'LOCATIONS (1)' and 'LOCATION GROUPS (0)'. A toolbar includes 'Add Location...', 'Import Location...', 'Download...', 'Sample Import...', 'Enter Group...', and search/filter options. A table lists one location: Site_1 with IP 184.170.227.125, SSL status Enabled: Kerb..., and other columns like X-Forwards..., Authentication, Firewall Filter, Bandwidth, Virtual ZENS, and Group. A blue circular icon with a white question mark is in the bottom right corner.

No.	Name	IP Addresses	Proxy Ports	X-Forwards...	Authenticatio...	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	⋮
1	Site_1	184.170.227.125	---	---	Enabled: Kerb...	---	---	---	---	---	

Slide notes

Slide 51 - Slide 51

The screenshot shows the Zscaler Admin UI with the 'Locations' page open. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for 'LOCATIONS (1)' and 'LOCATION GROUPS (0)'. Below are buttons for 'Add Location...', 'Import Location...', 'Download...', 'Sample Import...', 'Enter Group...', and a search bar. A table lists one location: Site_1 with IP 184.170.227.125, X-Forwarded-For: ---, Authentication: Enabled: Kerb..., SSL: ---, Firewall Filter: ---, Bandwidth: ---, Virtual ZENS: ---, and Group: ---. There are edit and delete icons for Site_1.

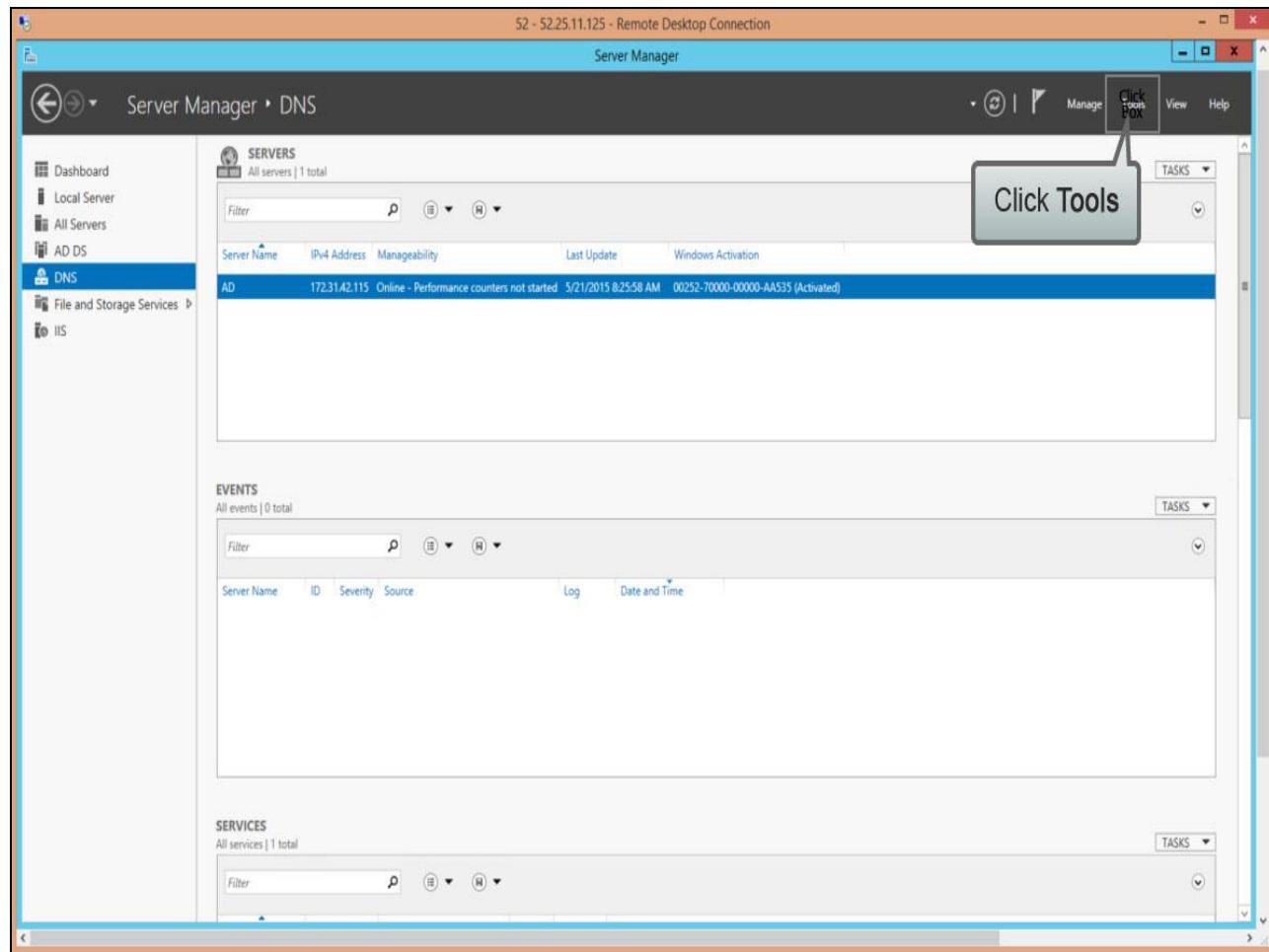
No.	Name	IP Addresses	Proxy Ports	X-Forwards...	Authenticatio...	SSL	Firewall Fil...	Bandwidth	Virtual ZENS	Group	Actions
1	Site_1	184.170.227.125	---	---	Enabled: Kerb...	---	---	---	---	---	

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.

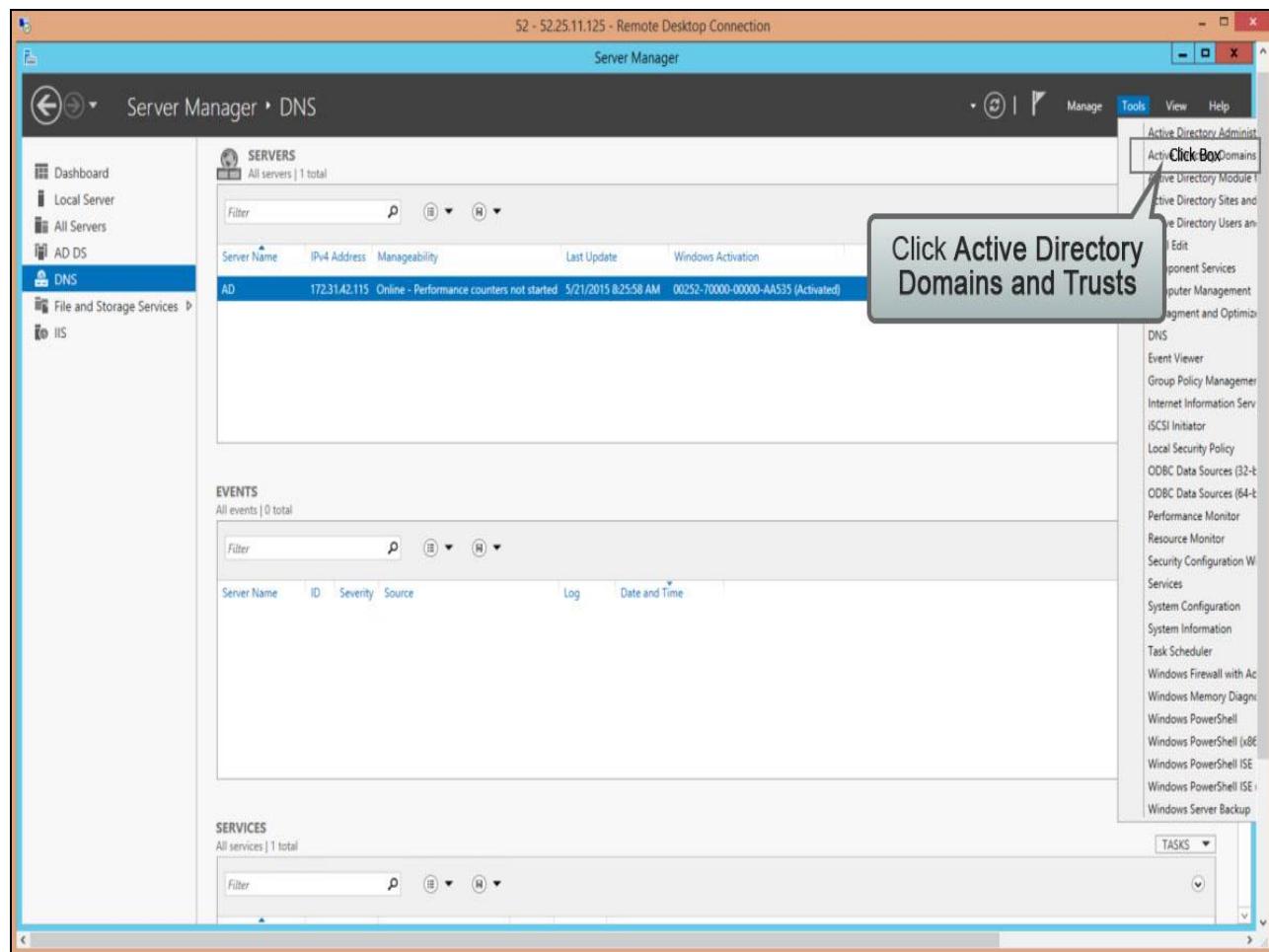
Slide 53 - Slide 53



Slide notes

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

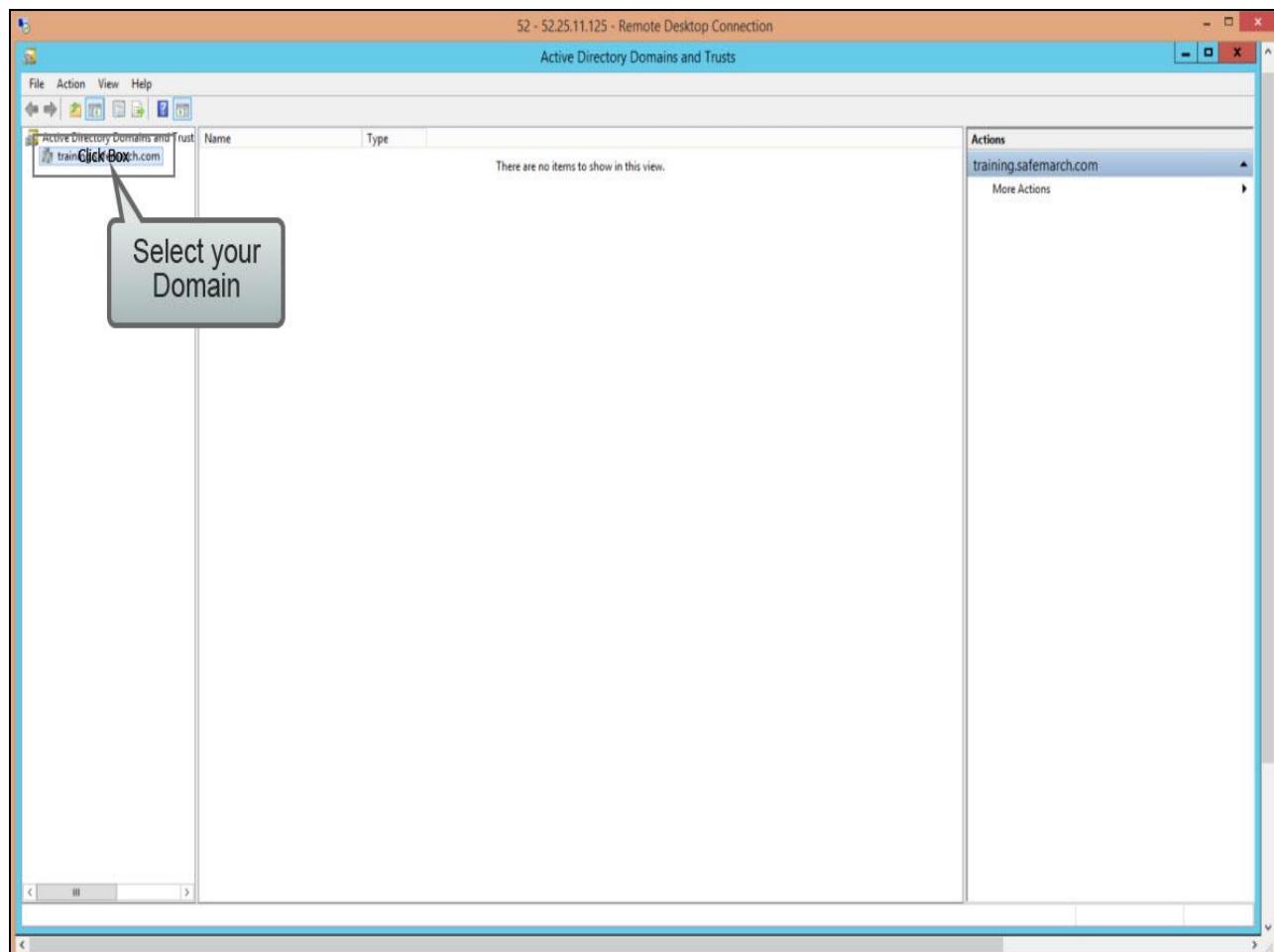
Slide 54 - Slide 54



Slide notes

Select **Active Directory Domains and Trusts**.

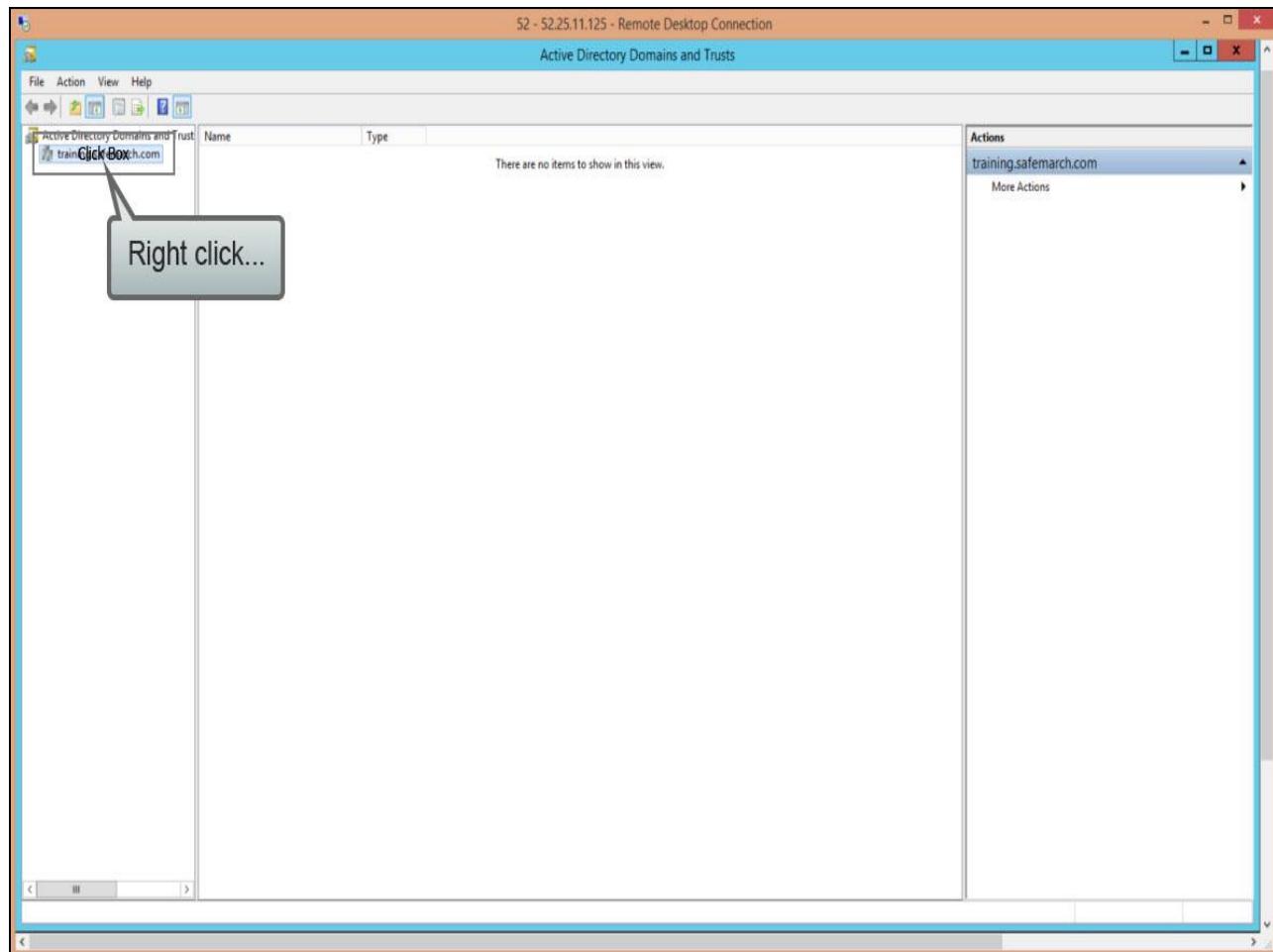
Slide 55 - Slide 55



Slide notes

Highlight your Domain, ...

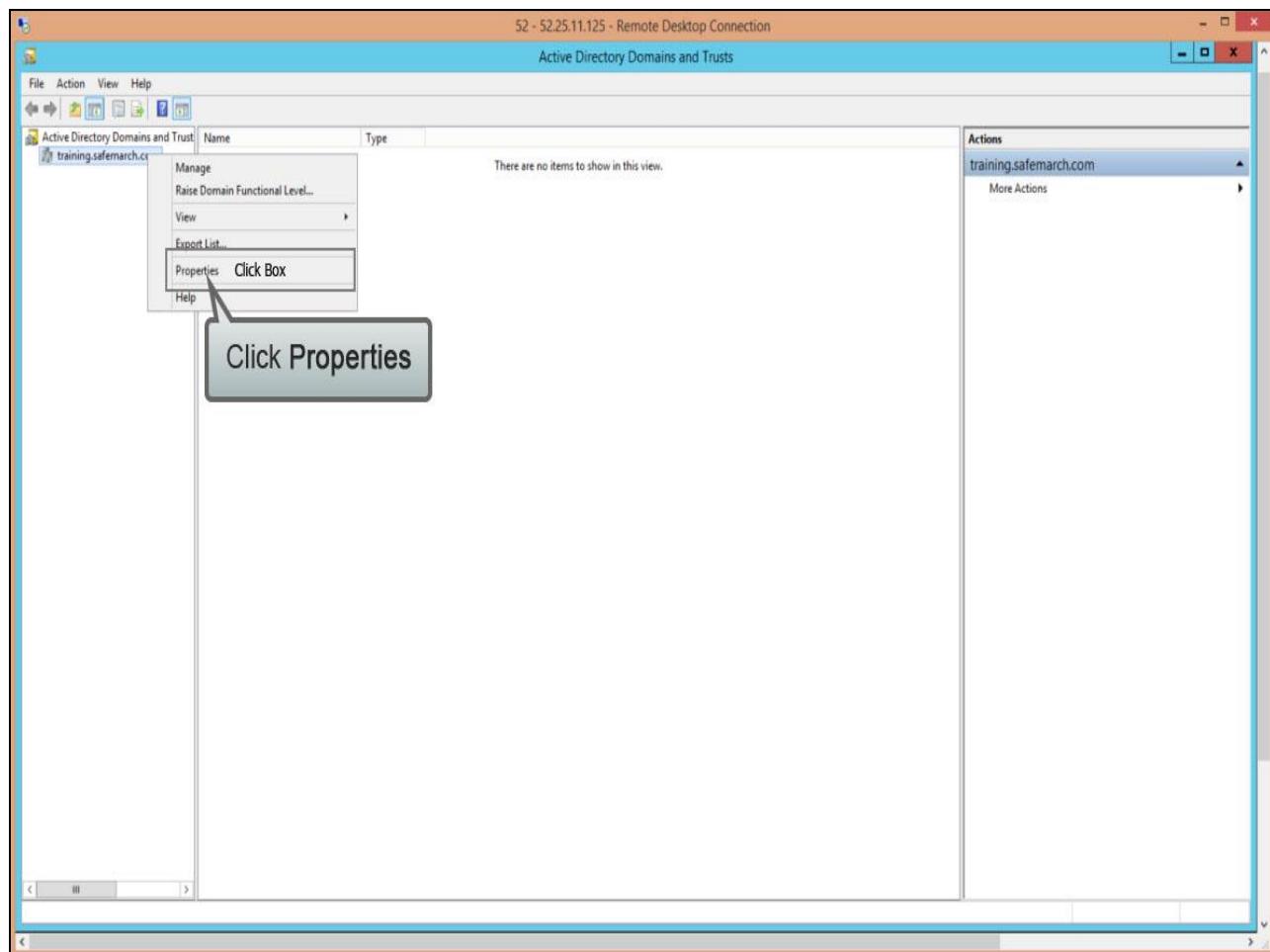
Slide 56 - Slide 56



Slide notes

...right-click, ...

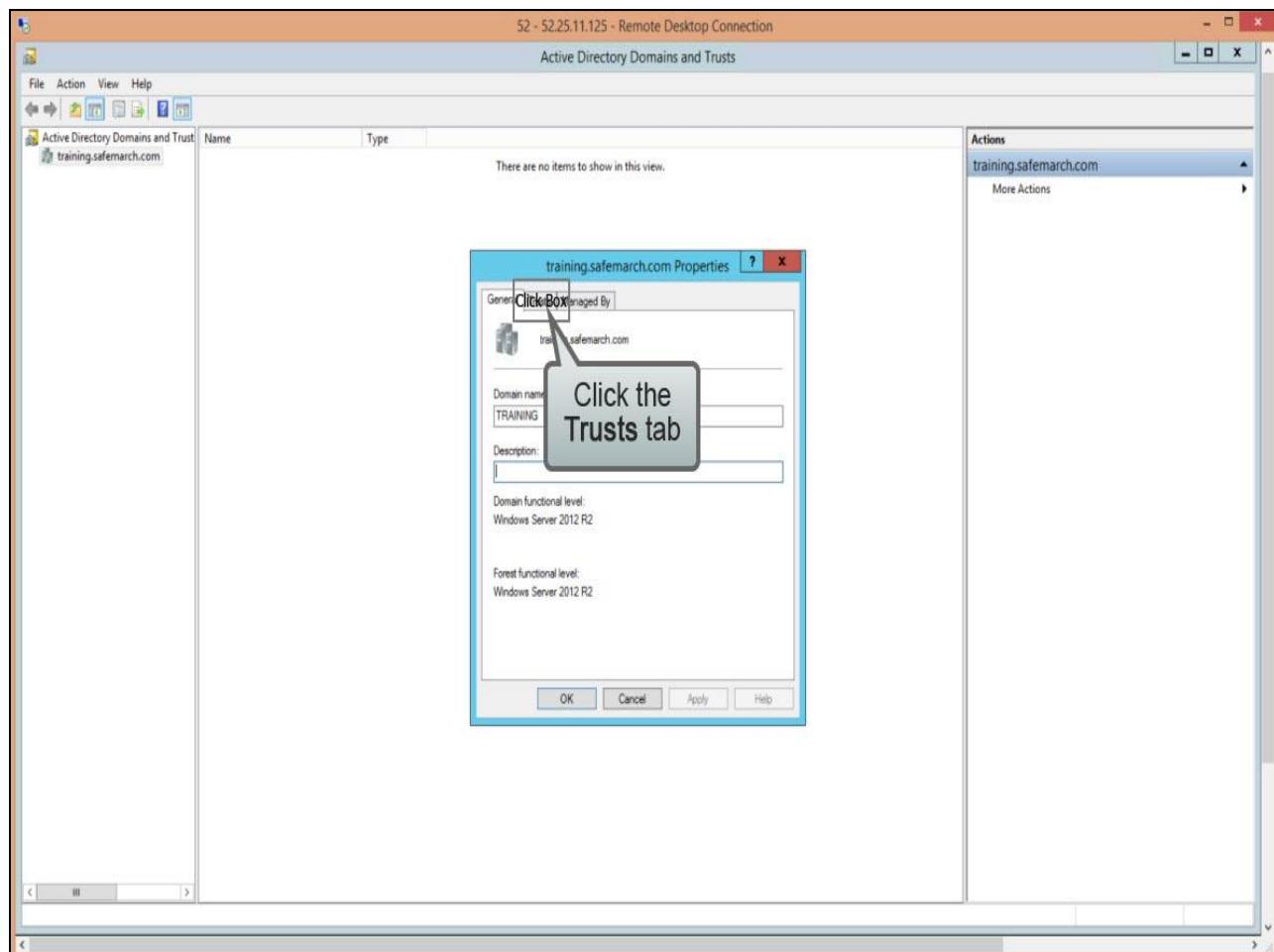
Slide 57 - Slide 57



Slide notes

...and select **Properties**.

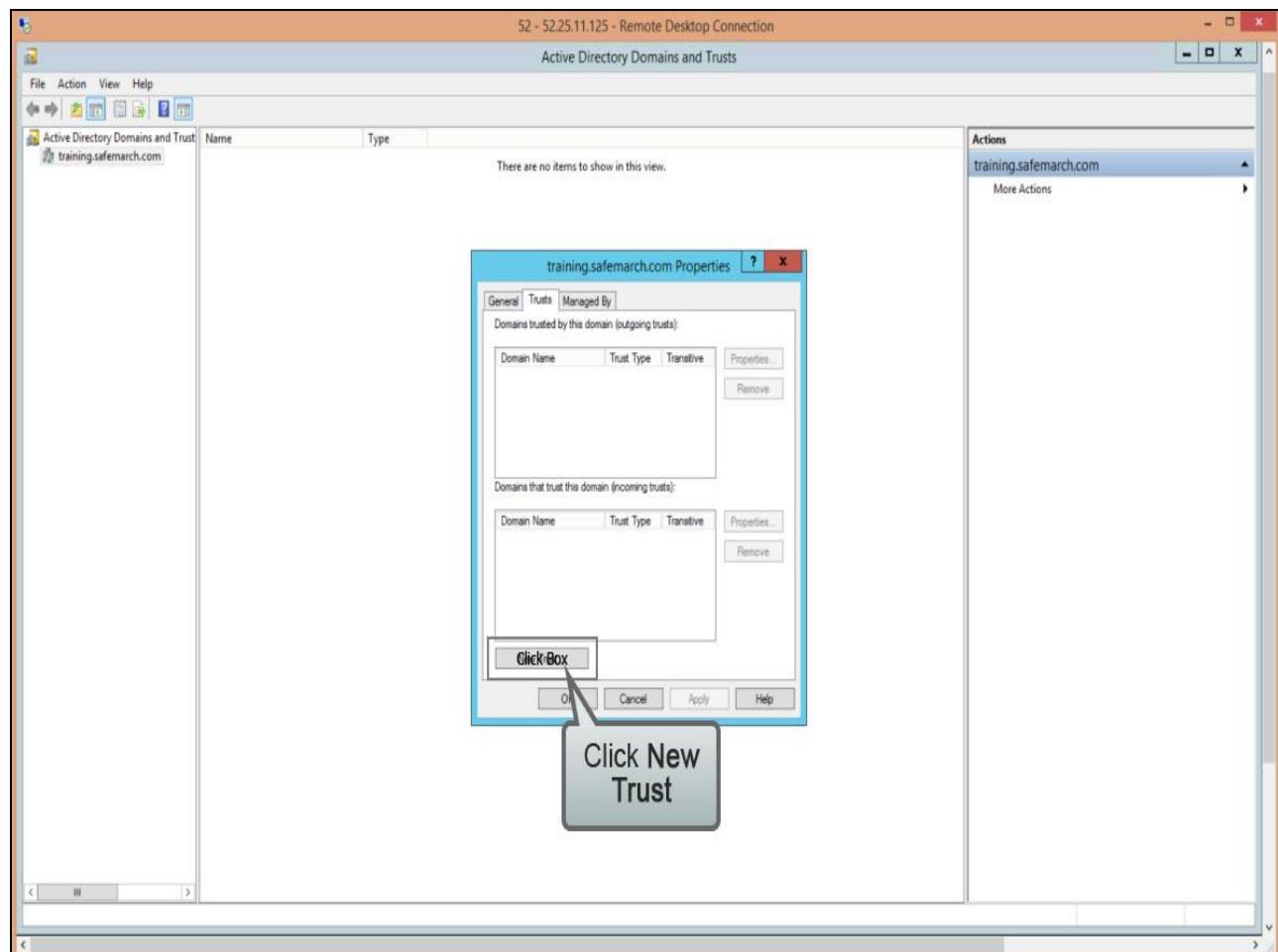
Slide 58 - Slide 58



Slide notes

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

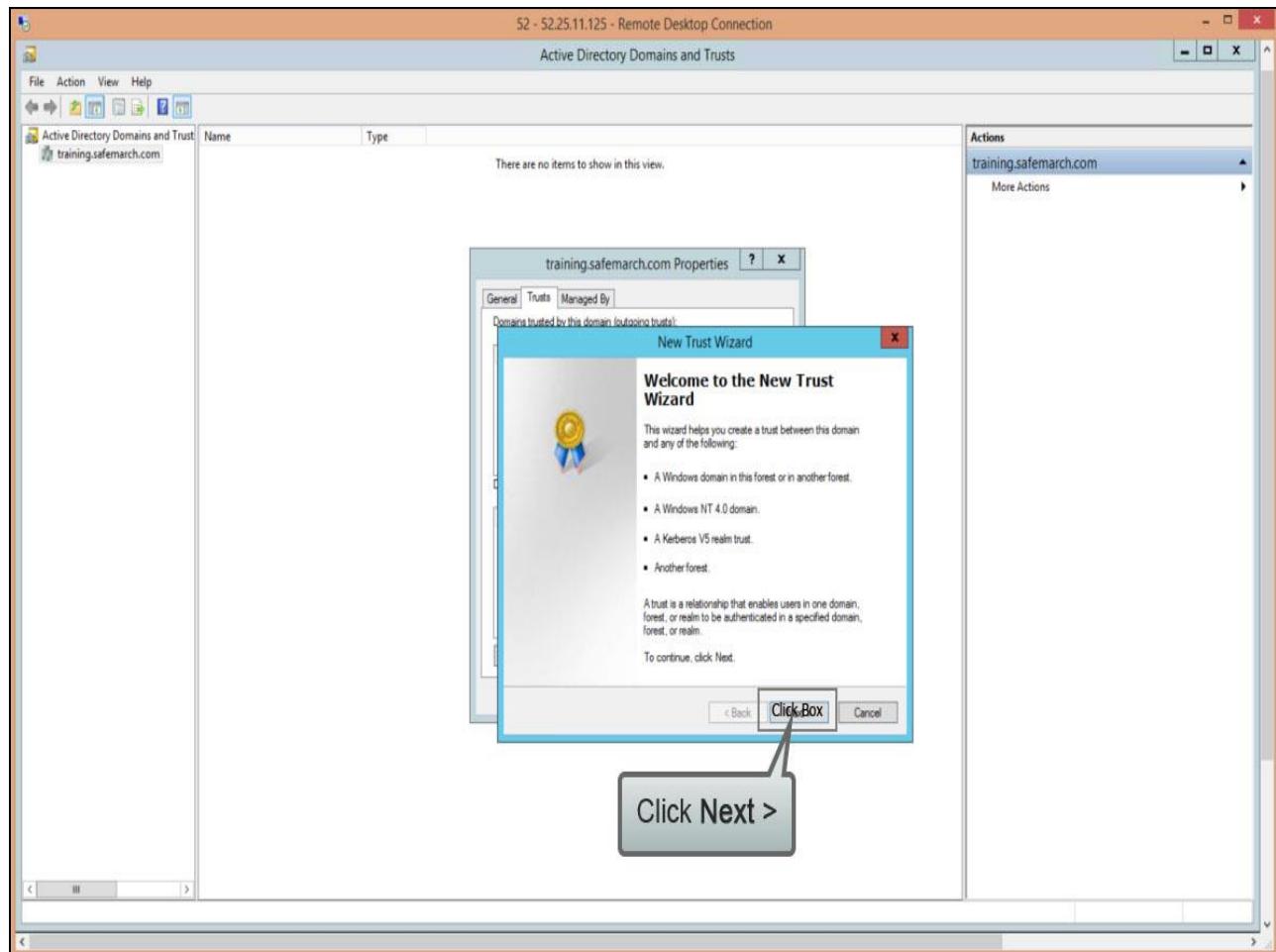
Slide 59 - Slide 59



Slide notes

Click New Trust, ...

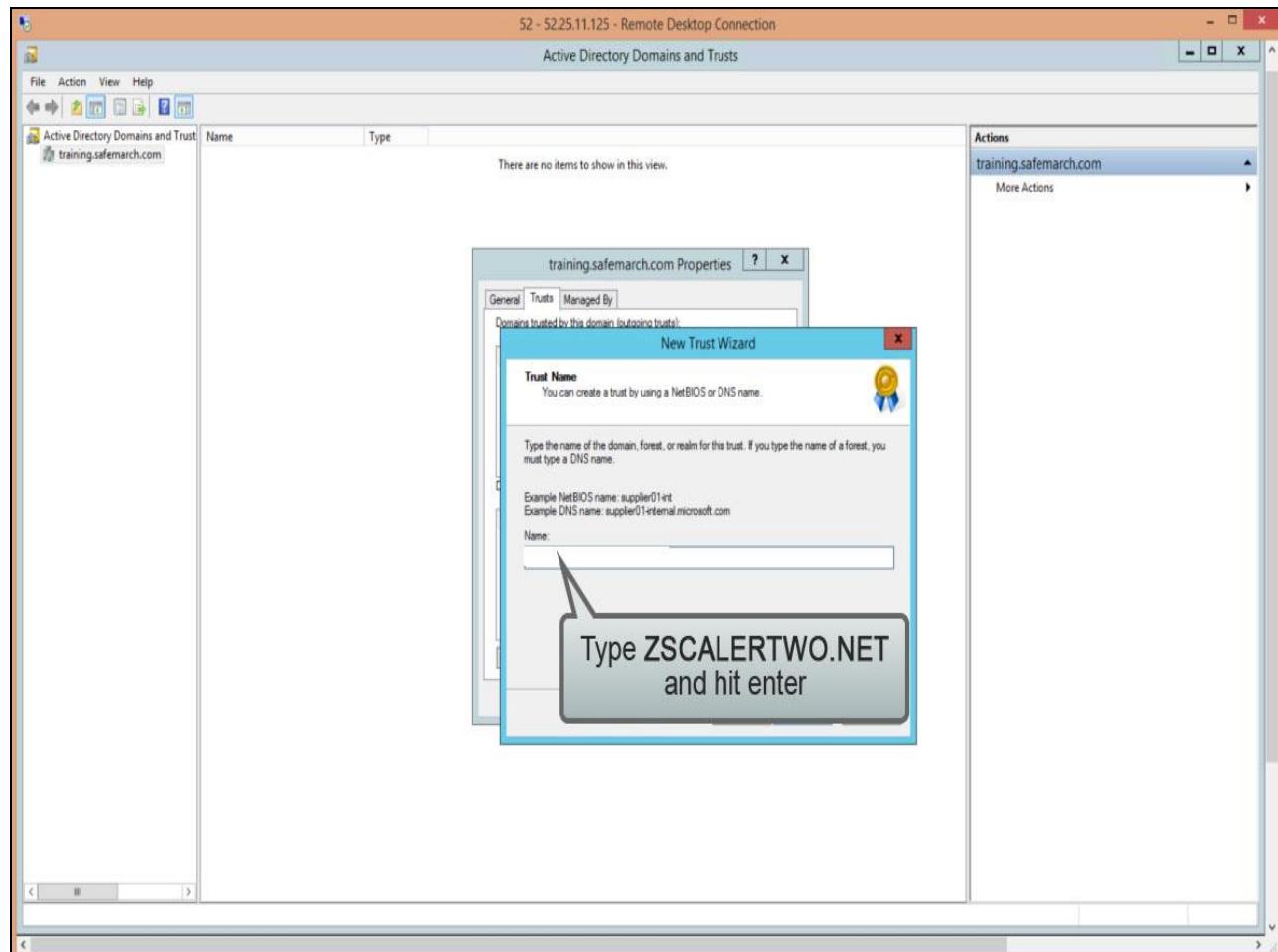
Slide 60 - Slide 60



Slide notes

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

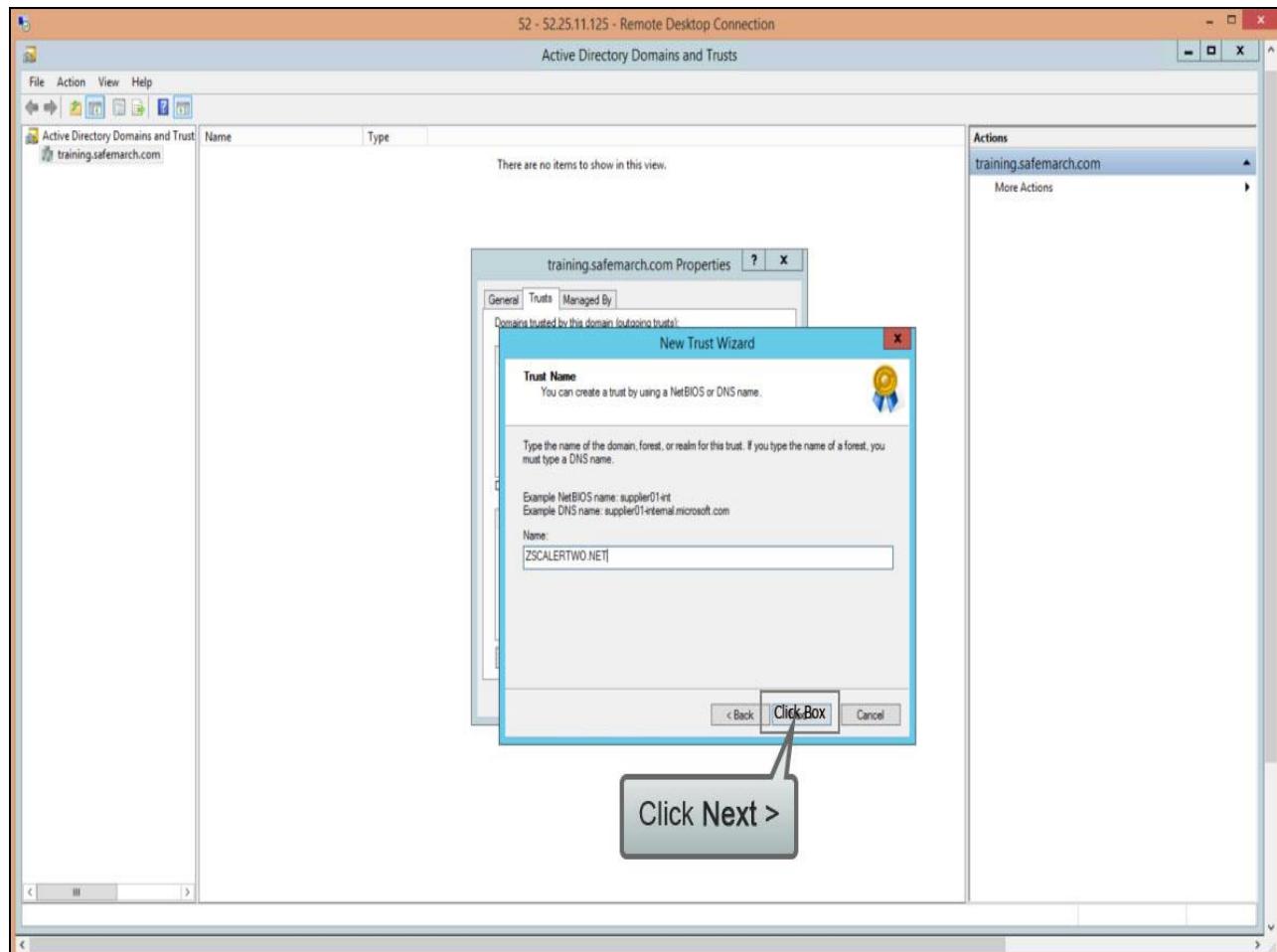
Slide 61 - Slide 61



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.

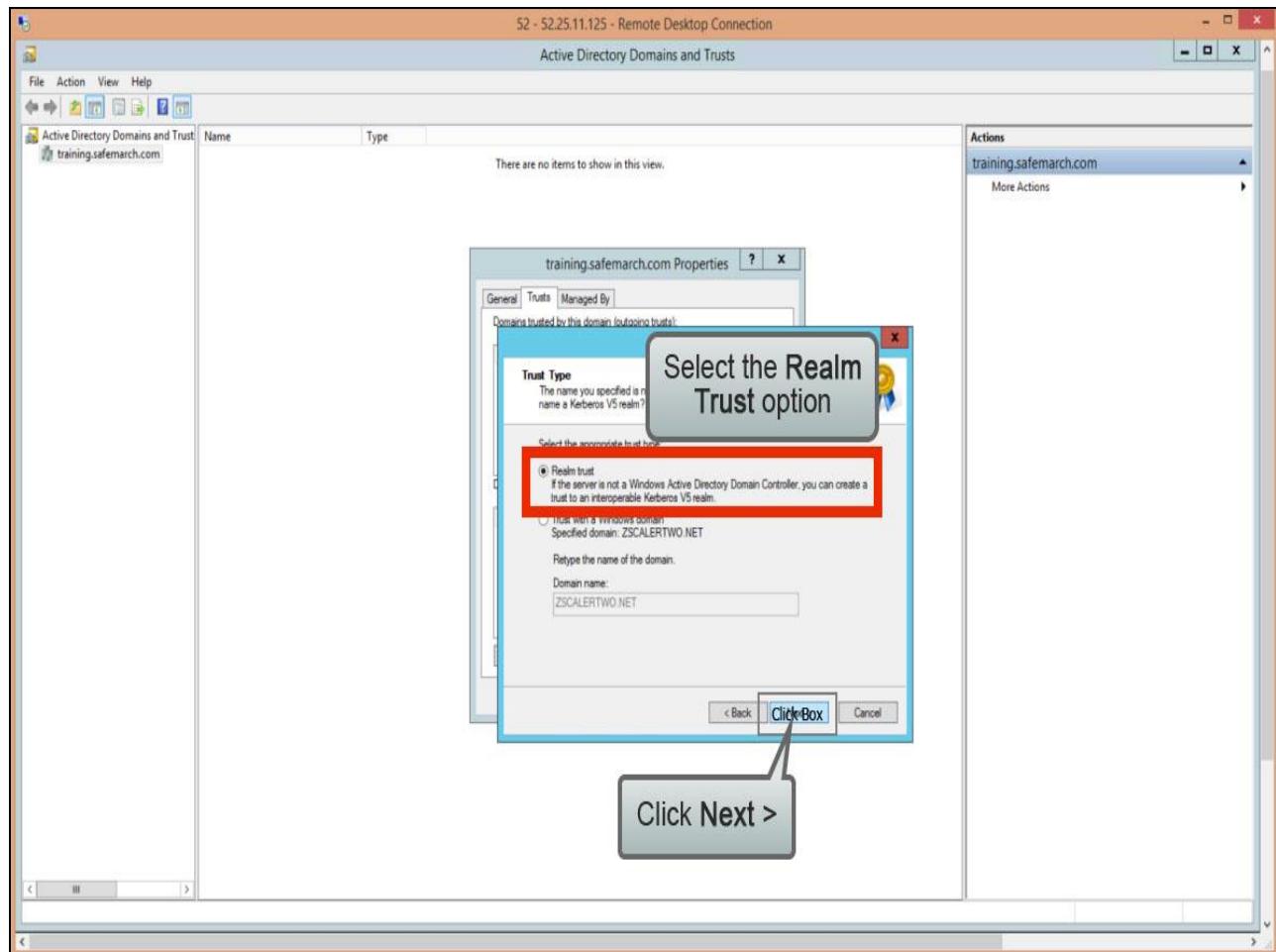
Slide 62 - Slide 62



Slide notes

Click **Next**, ...

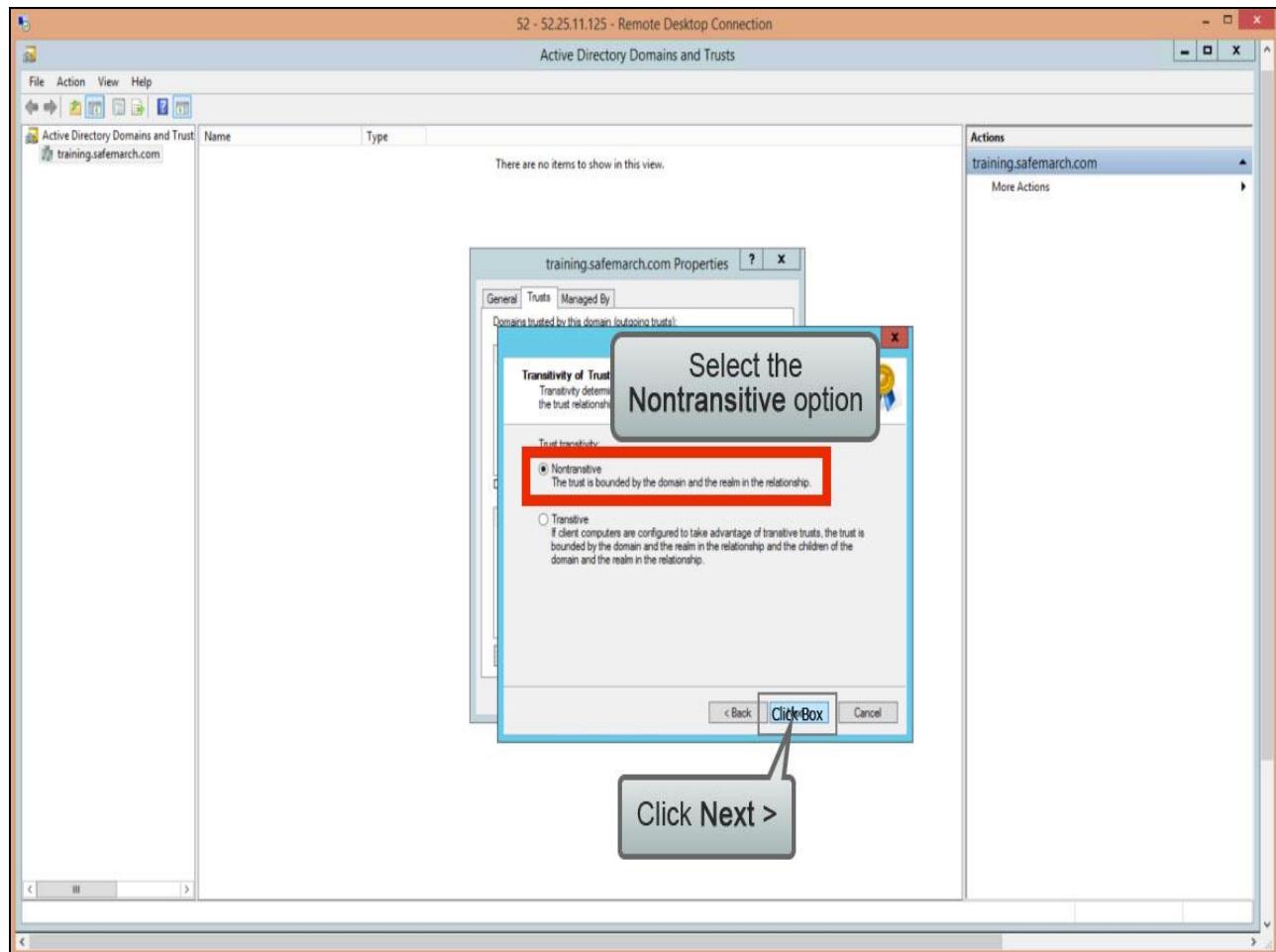
Slide 63 - Slide 63



Slide notes

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

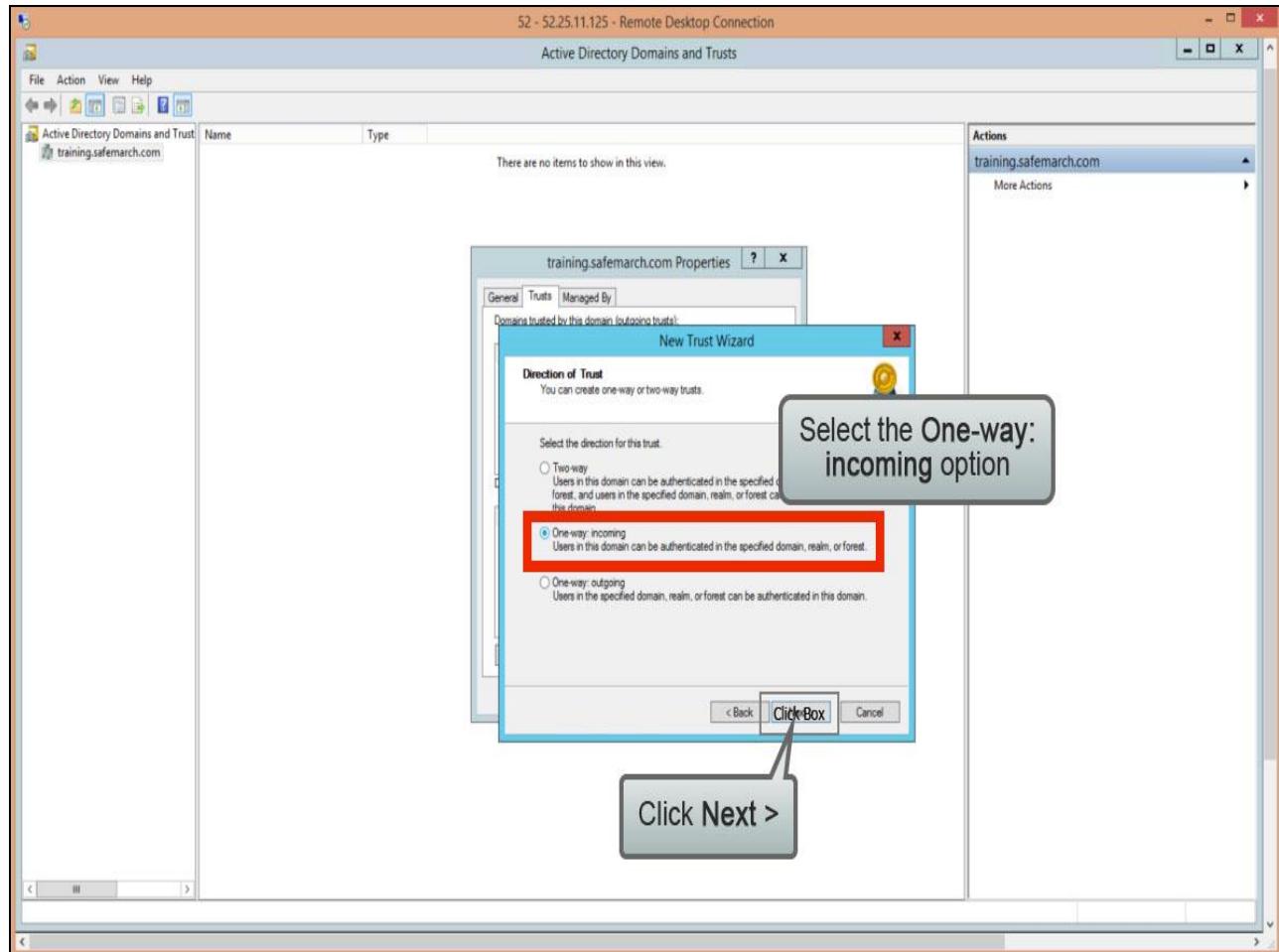
Slide 64 - Slide 64



Slide notes

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

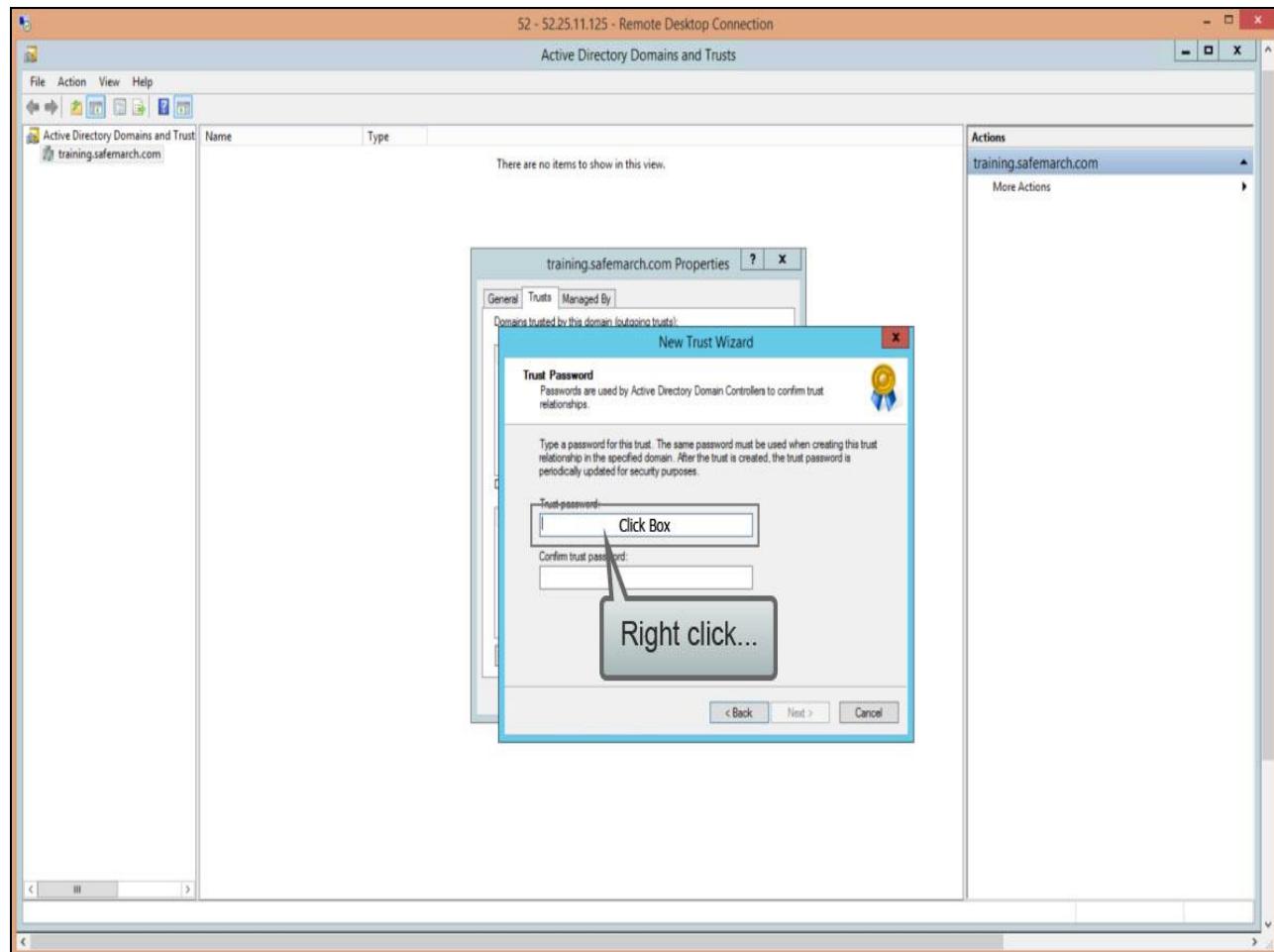
Slide 65 - Slide 65



Slide notes

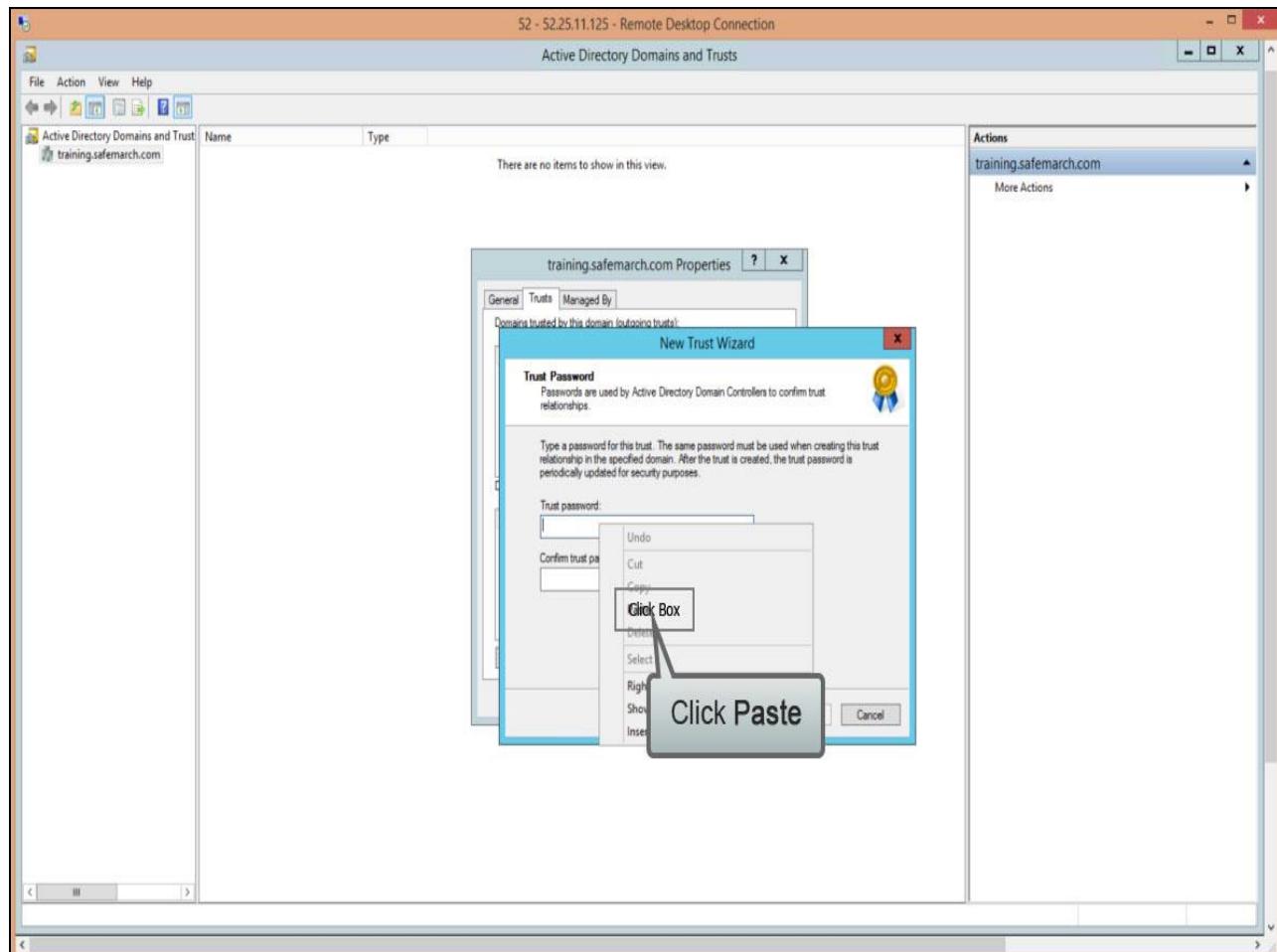
For the **Direction of Trust** select **One-way Incoming** and click **Next**.

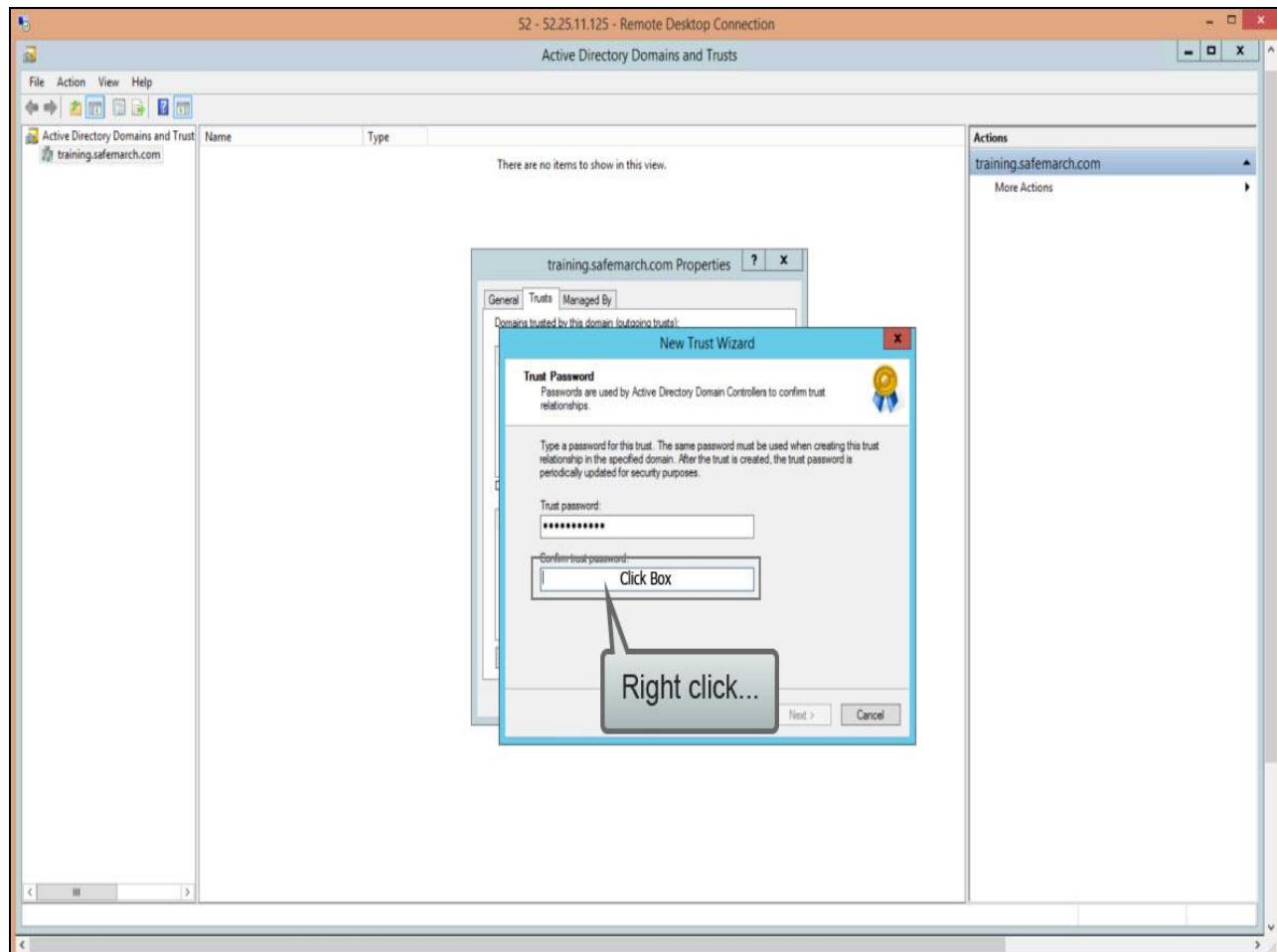
Slide 66 - Slide 66

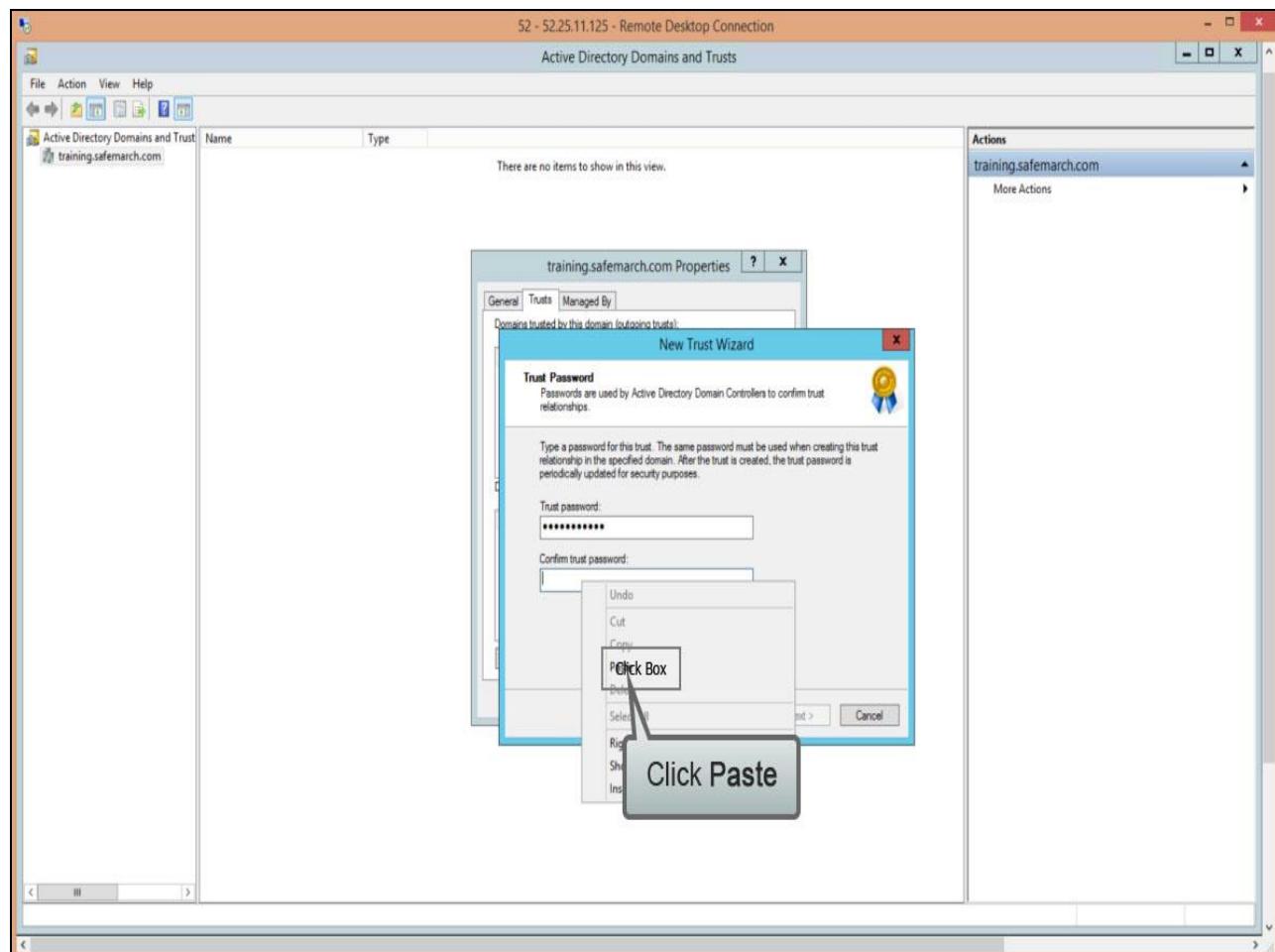


Slide notes

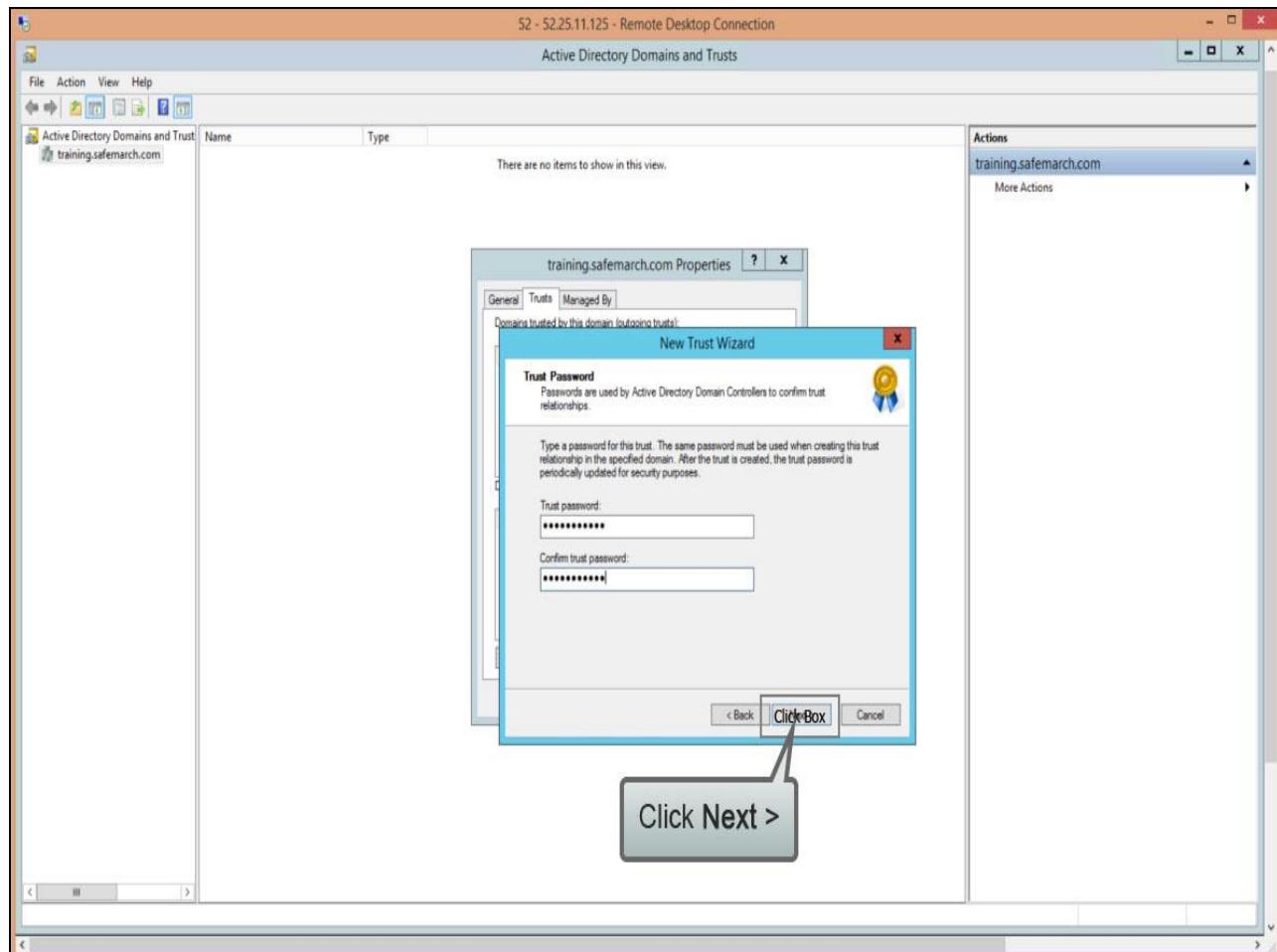
For the **Trust Password** paste in the Trust password that was copied earlier from the Zscaler Admin Portal.

Slide 67 - Slide 67**Slide notes**

Slide 68 - Slide 68**Slide notes**

Slide 69 - Slide 69**Slide notes**

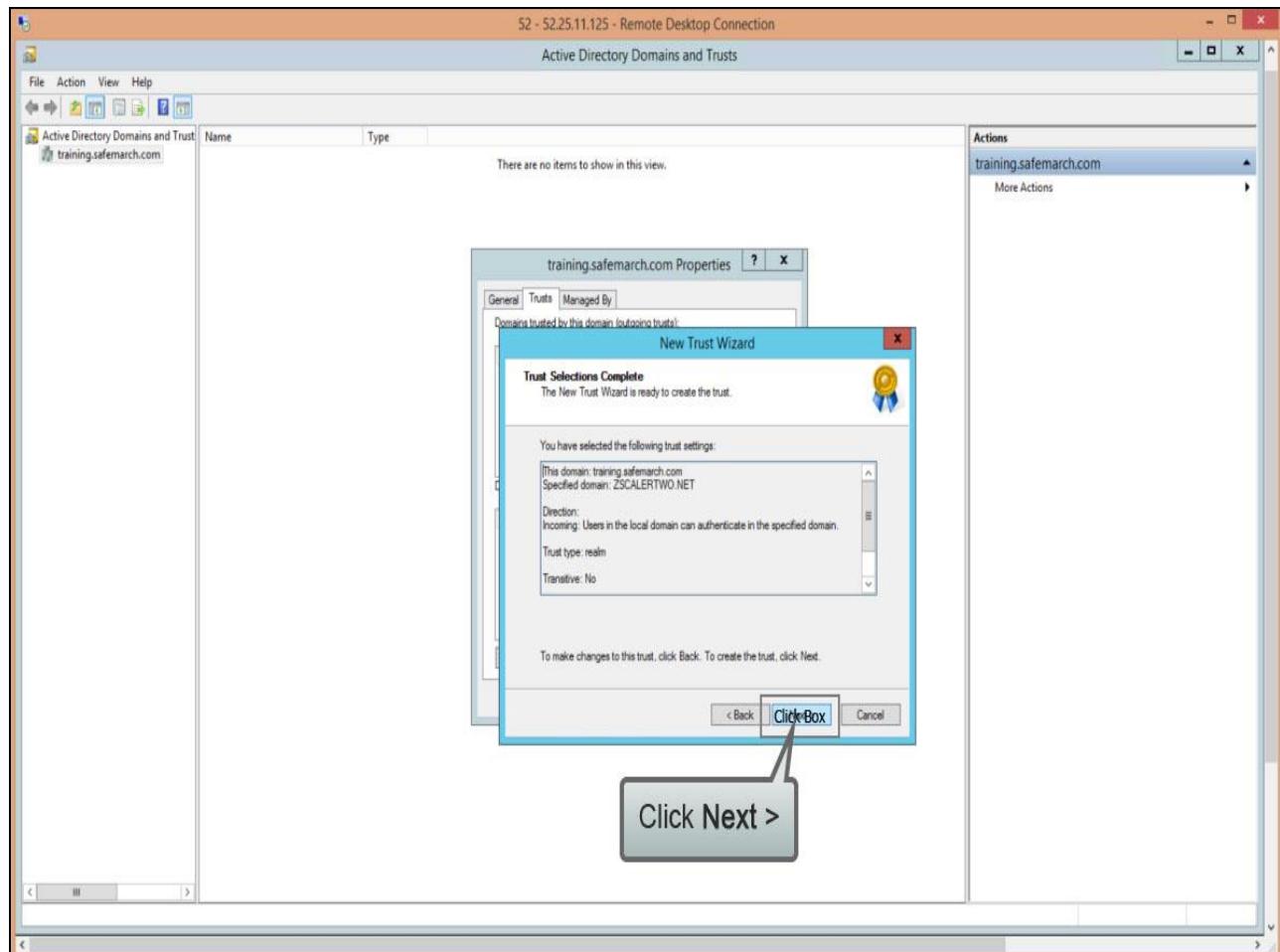
Slide 70 - Slide 70



Slide notes

Click **Next**, ...

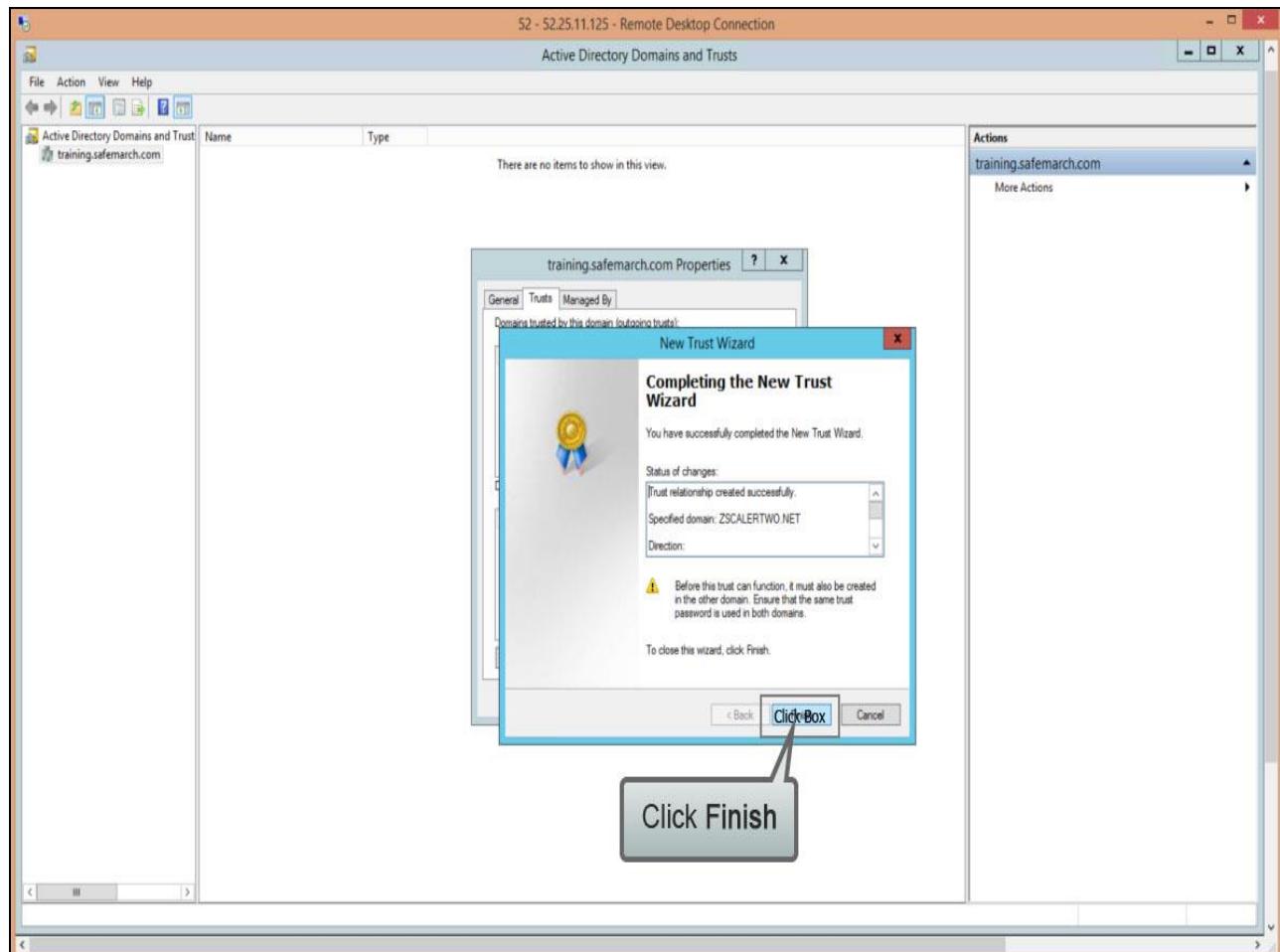
Slide 71 - Slide 71



Slide notes

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

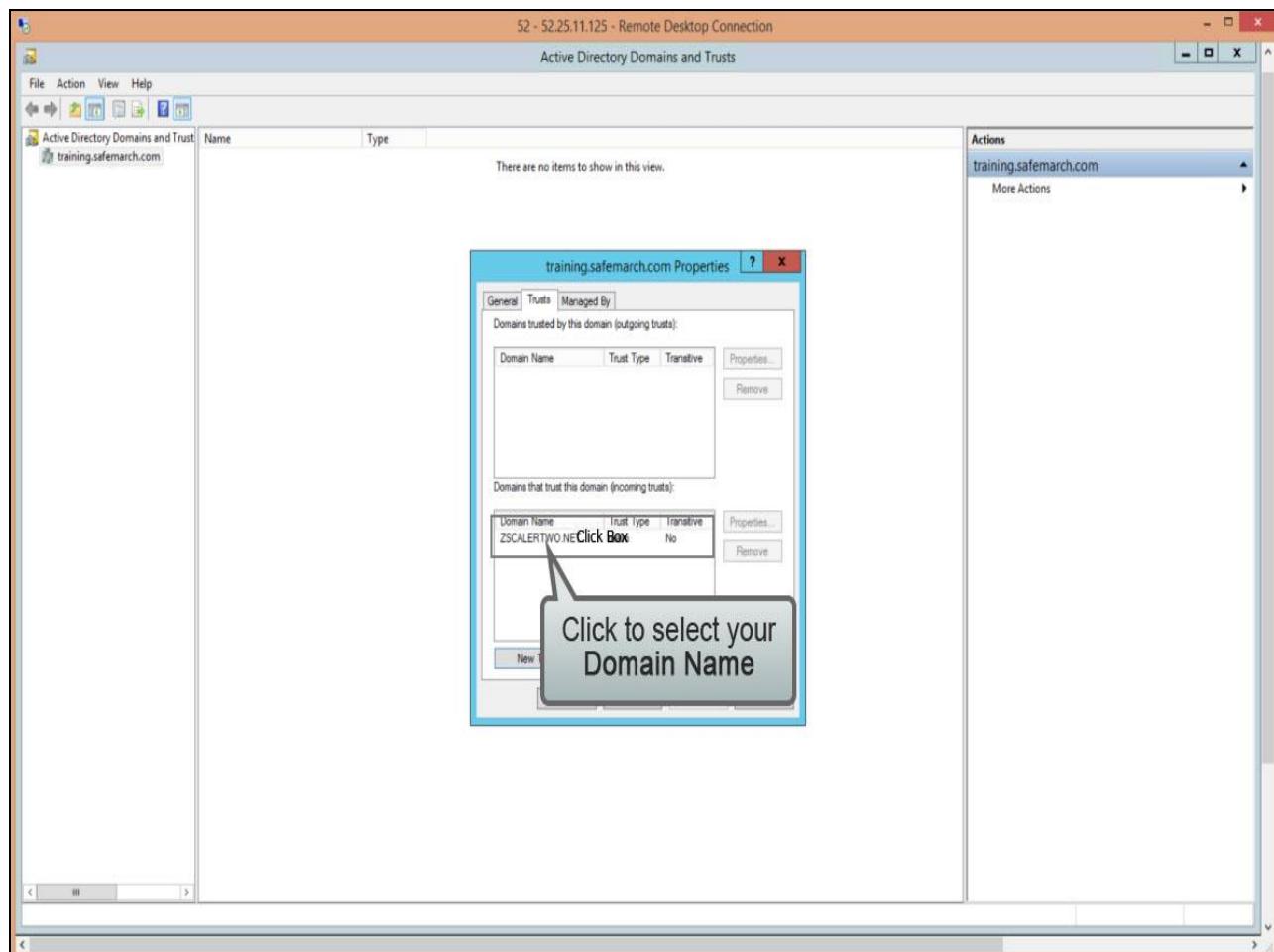
Slide 72 - Slide 72



Slide notes

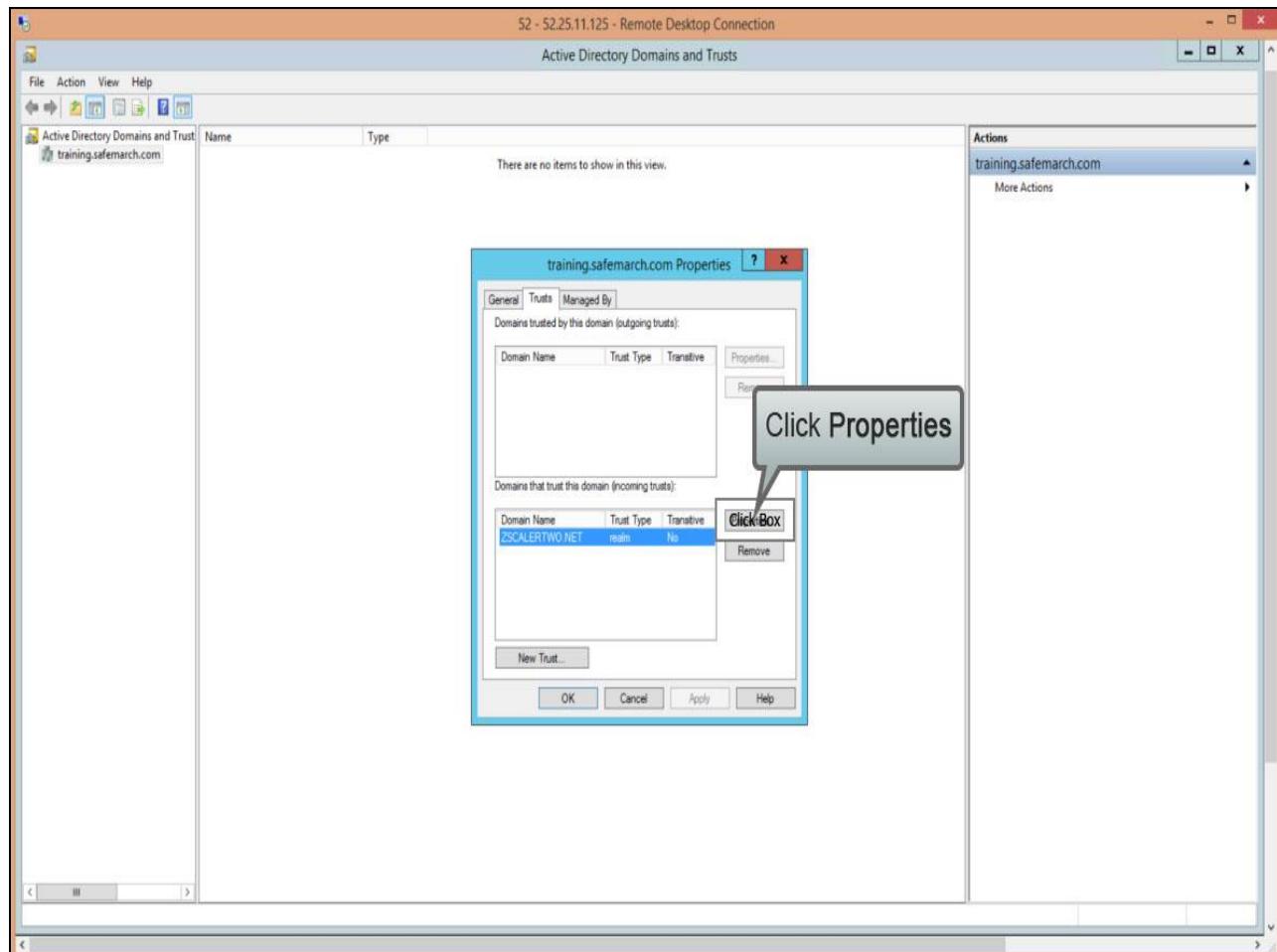
Click **Finish** to close the Wizard.

Slide 73 - Slide 73

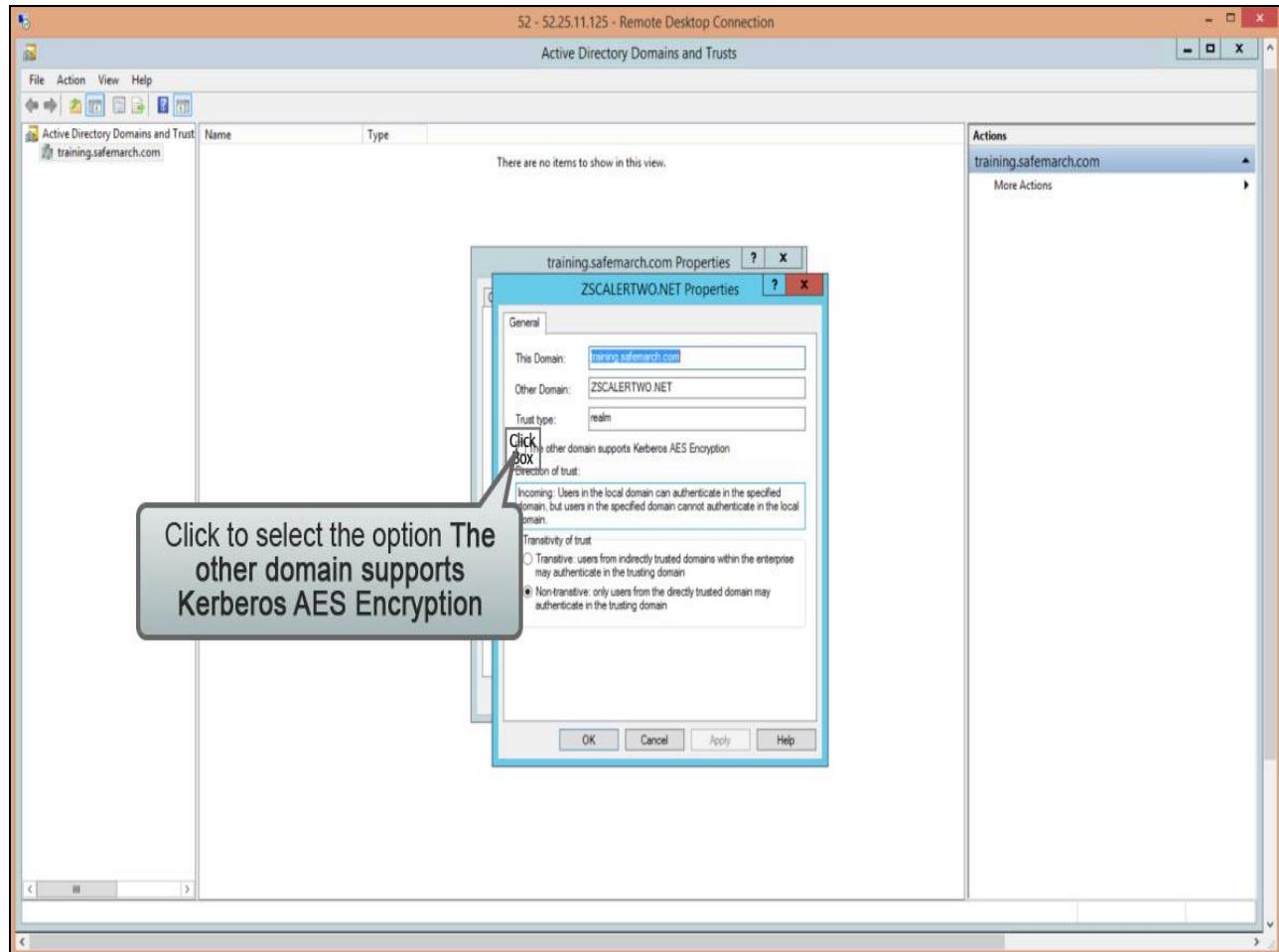


Slide notes

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

Slide 74 - Slide 74**Slide notes**

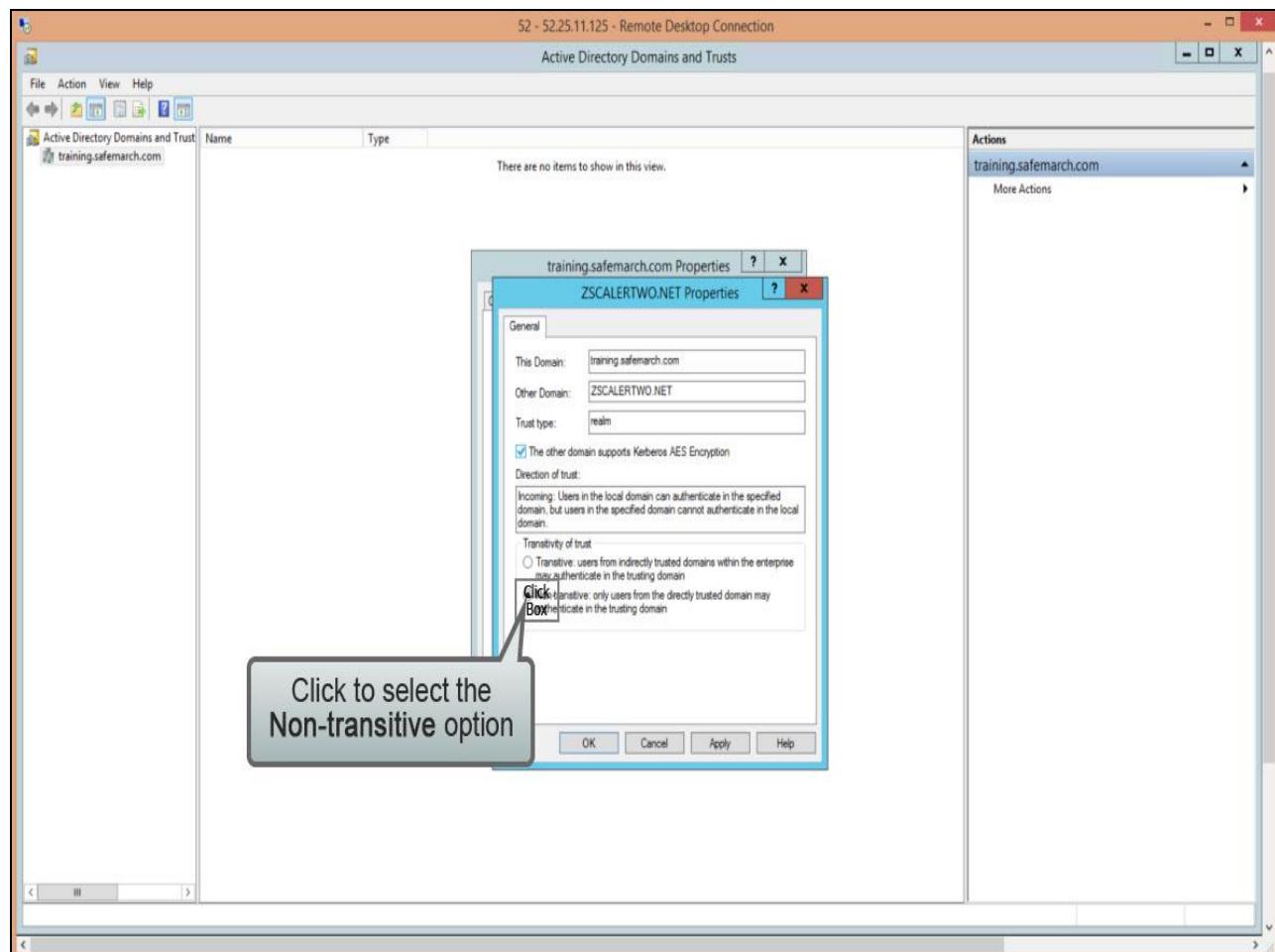
Slide 75 - Slide 75



Slide notes

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

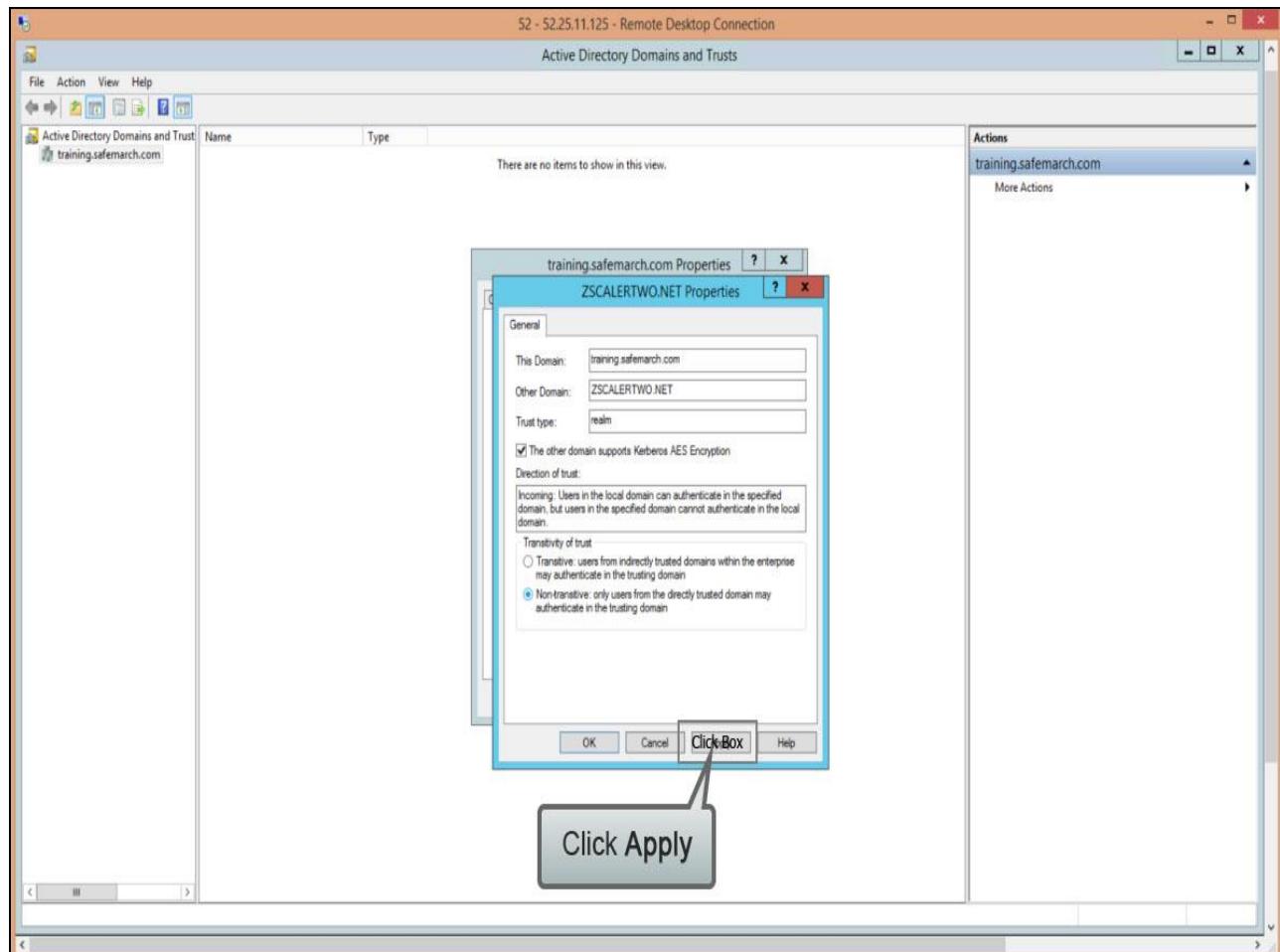
Slide 76 - Slide 76



Slide notes

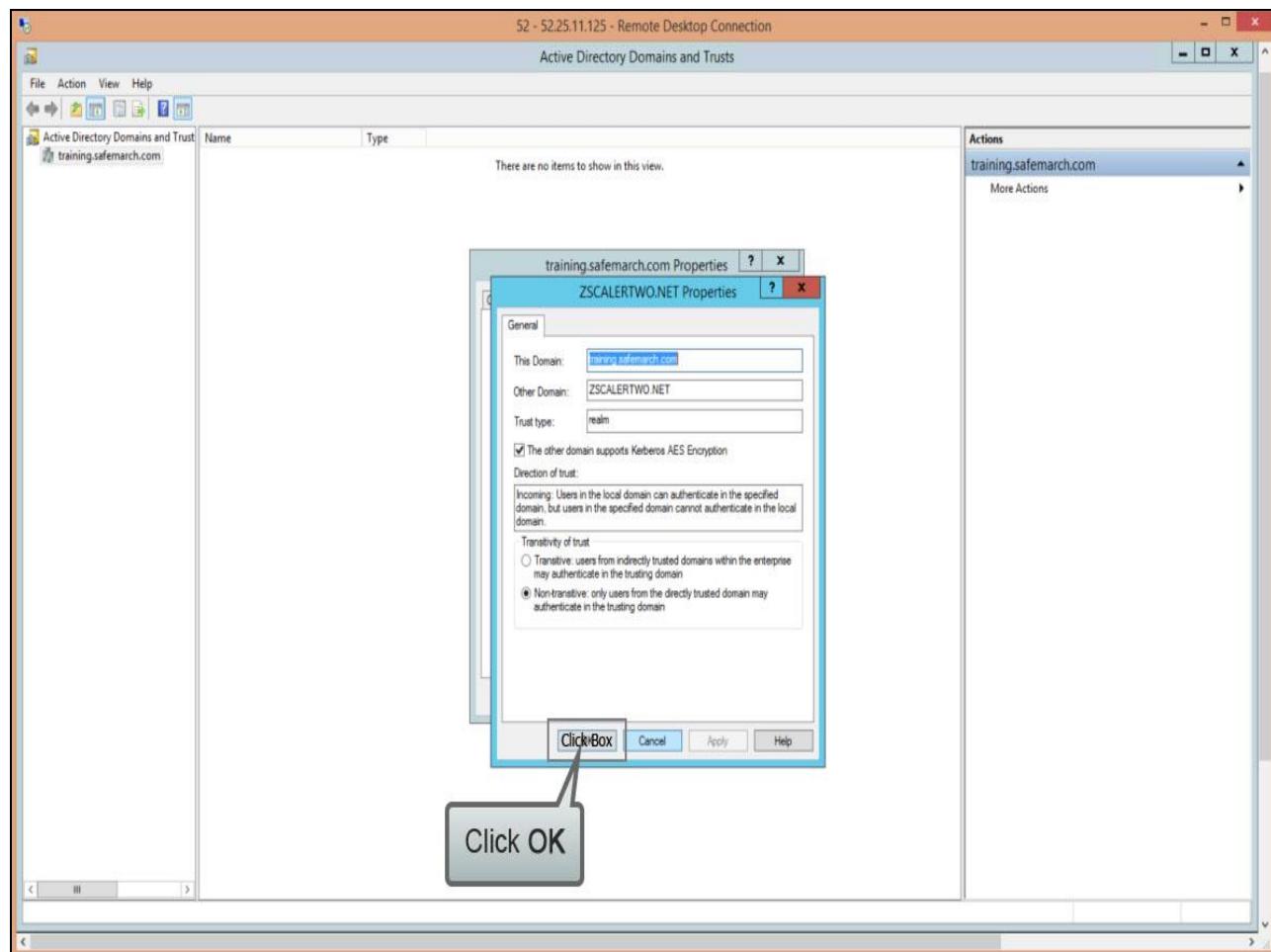
...and select **Non-transitive**, ...

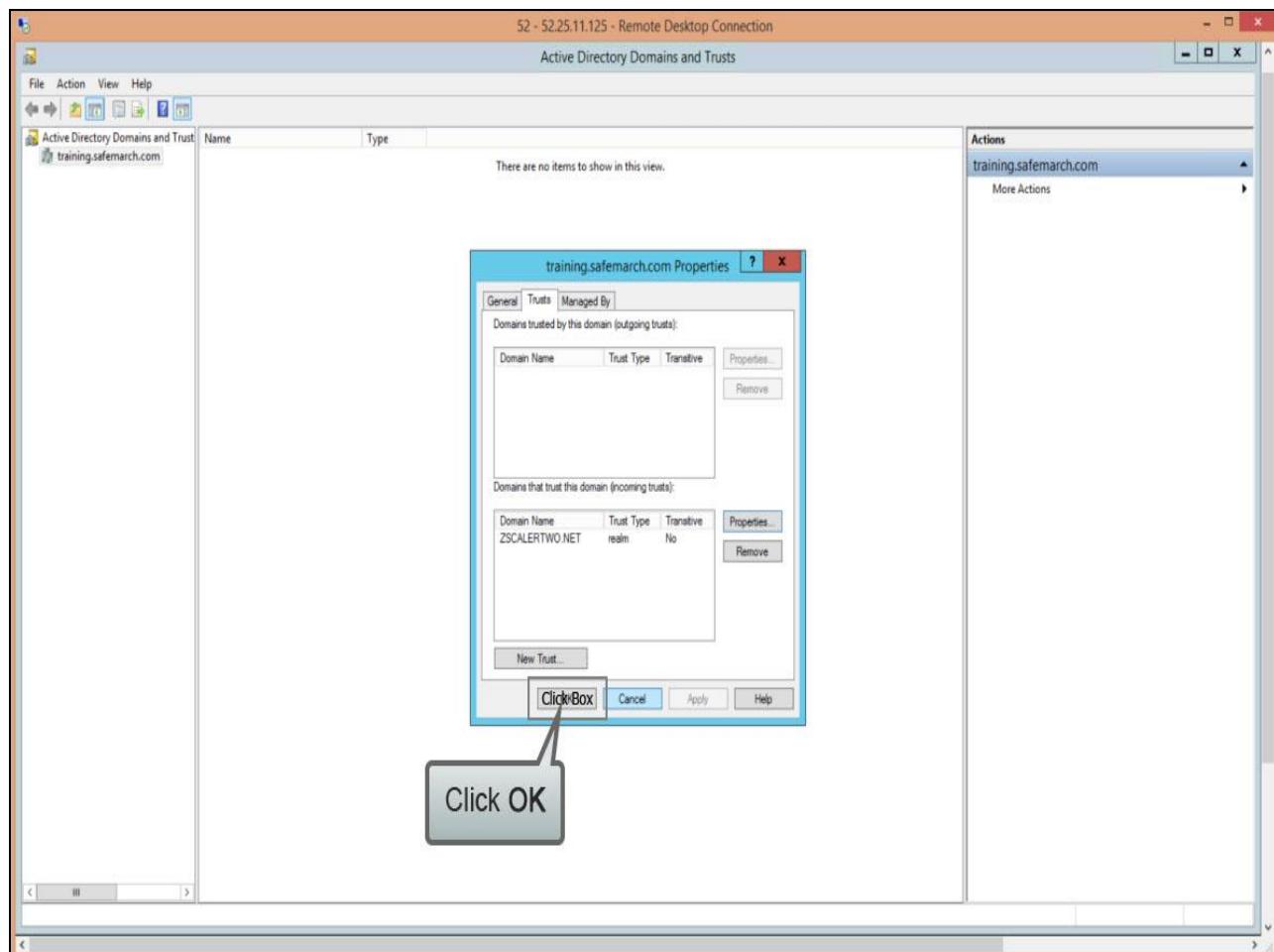
Slide 77 - Slide 77



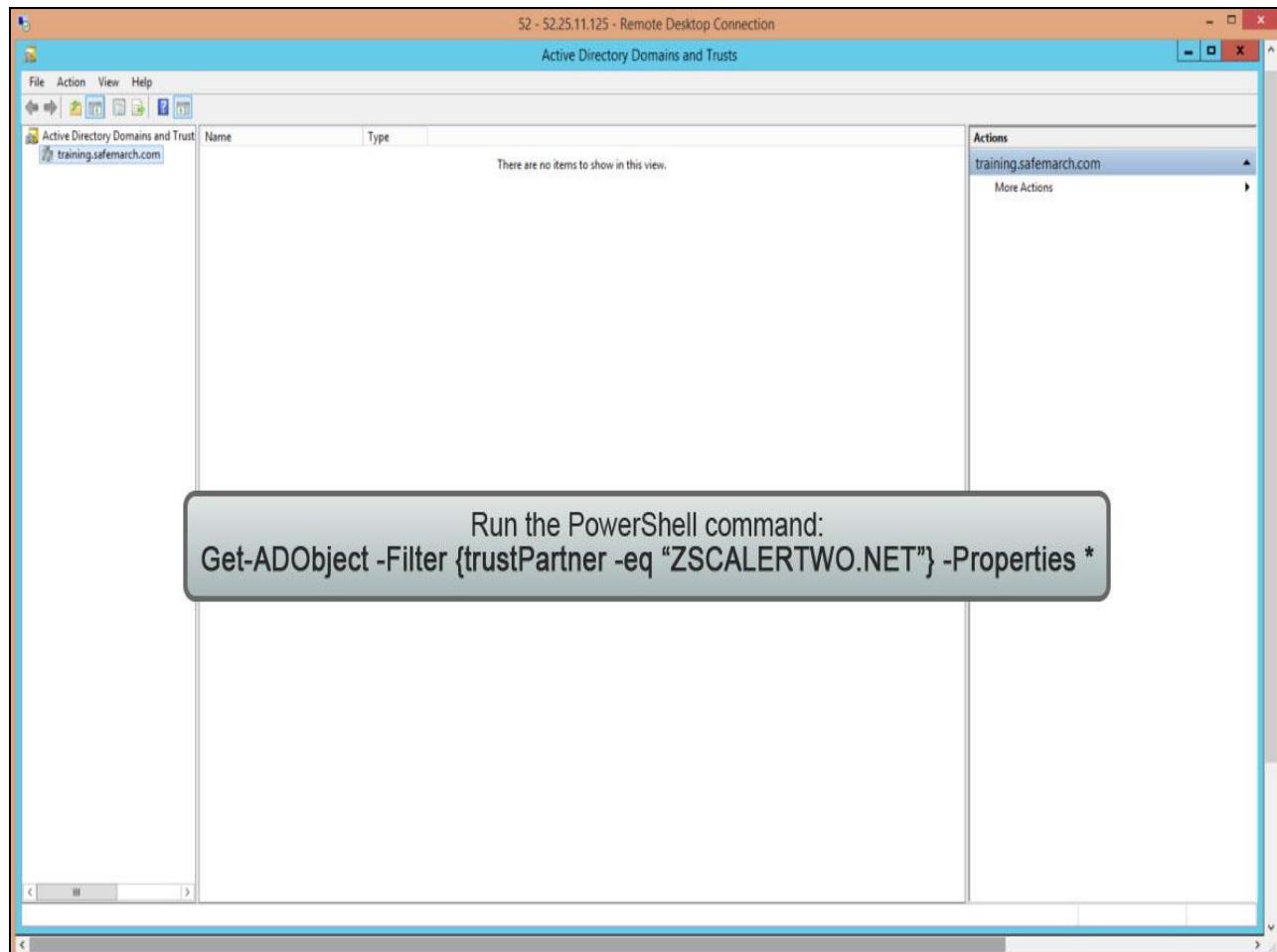
Slide notes

...then click **Apply**.

Slide 78 - Slide 78**Slide notes**

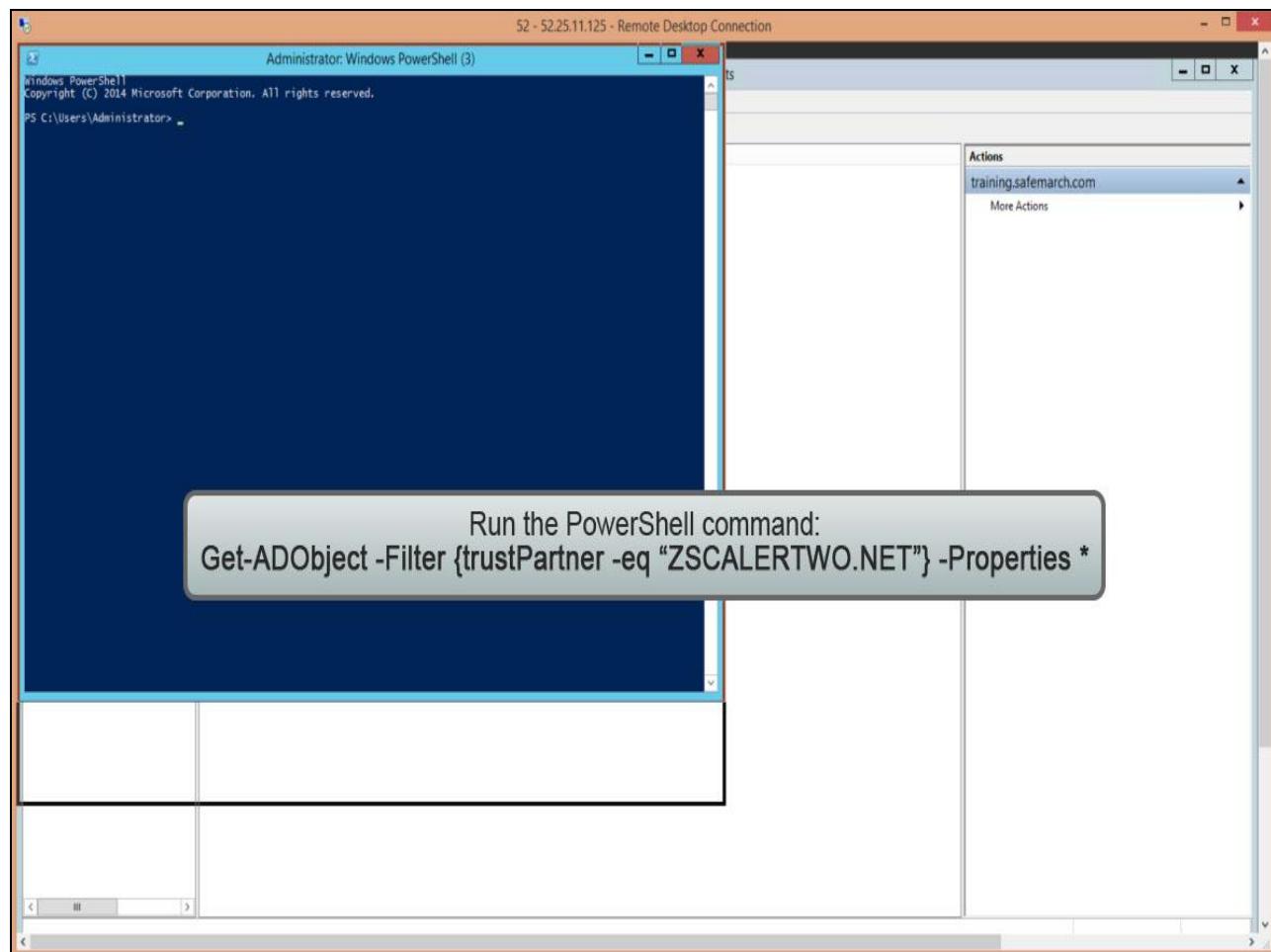
Slide 79 - Slide 79**Slide notes**

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

The screenshot shows a Windows Remote Desktop Connection window with two visible panes:

- Administrator: Windows PowerShell (3)**: A terminal window displaying PowerShell commands and their output. The command run is:

```
PS C:\Users\Administrator> Get-ADObject -Filter {trustPartner -eq "ZSCALER TWO.NET"} -Properties *
```

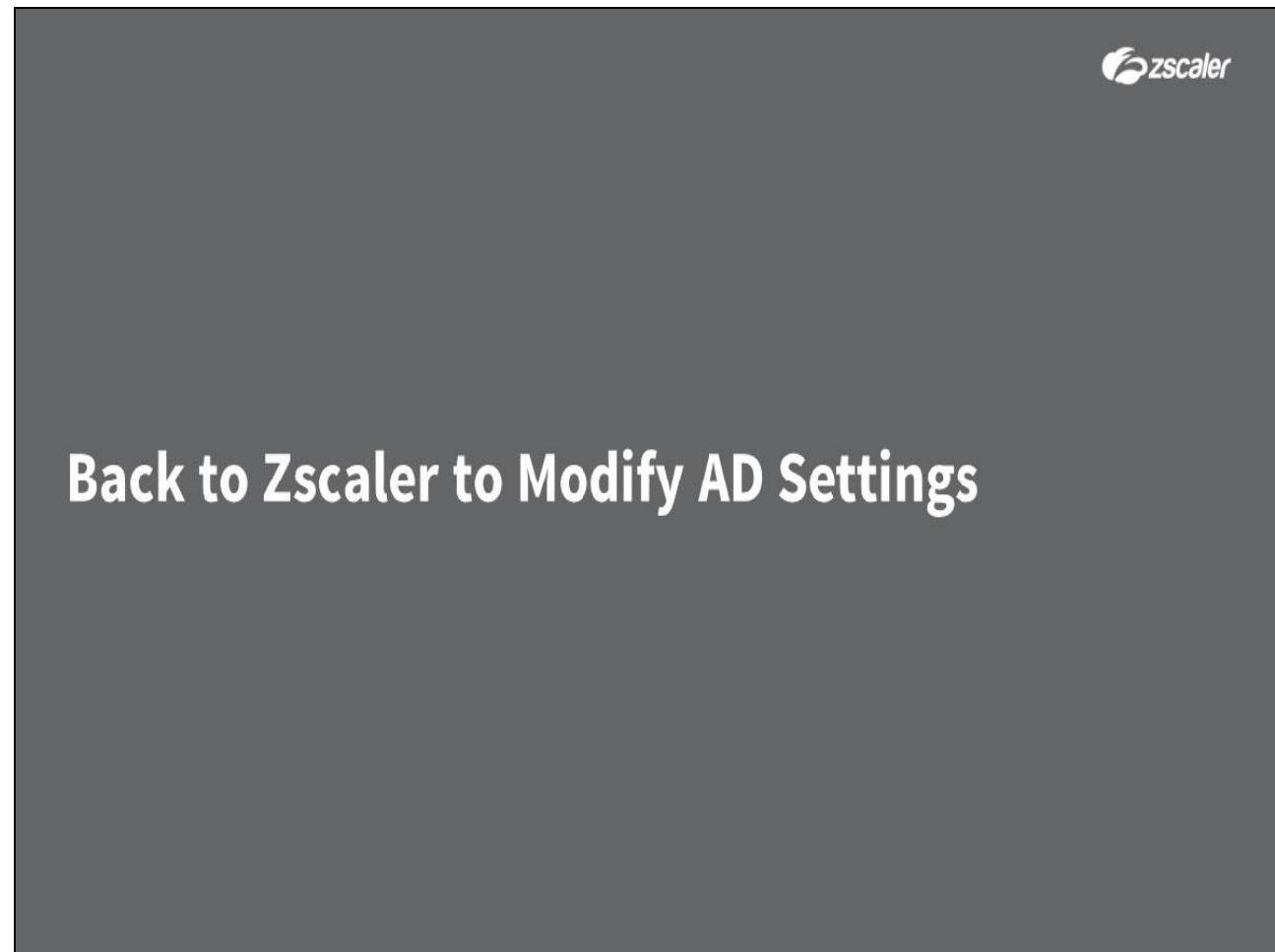
The output shows various attributes for the object, including:
 - CN**: ZSCALER TWO.NET
 - createTimeStamp**: 5/21/2015 8:30:44 AM
 - Deleted**: False
 - Description**:
 - DisplayName**:
 - distinguishedName**: CN=ZSCALER TWO.NET,CN=System,DC=training,DC=safemarch,DC=com
 - dsCorePropagationData**: [12/31/1600 4:00:00 PM]
 - FlatName**: ZSCALER TWO.NET
 - instanceType**: 4
 - isCriticalSystemObject**: True
 - isDeleted**: False
 - LastKnownParent**:
 - Modified**: 5/21/2015 8:31:26 AM
 - msDS-SupportedEncryptionTypes**: 24
 - Name**: ZSCALER TWO.NET
 - objectClass**: trustedDomain
 - ProtectedFromAccidentalDeletion**: False
 - rightsEffective**: 15
 - trustAttributes**: 1
 - trustDirection**: 1
 - trustType**: 3
 - usNChanged**: 70201
 - usNCreated**: 70193
 - whenChanged**: 5/21/2015 8:31:26 AM
 - whenCreated**: 5/21/2015 8:30:44 AM
- Actions**: A browser window showing the URL training.safemarch.com. The page content is mostly blank or illegible.

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

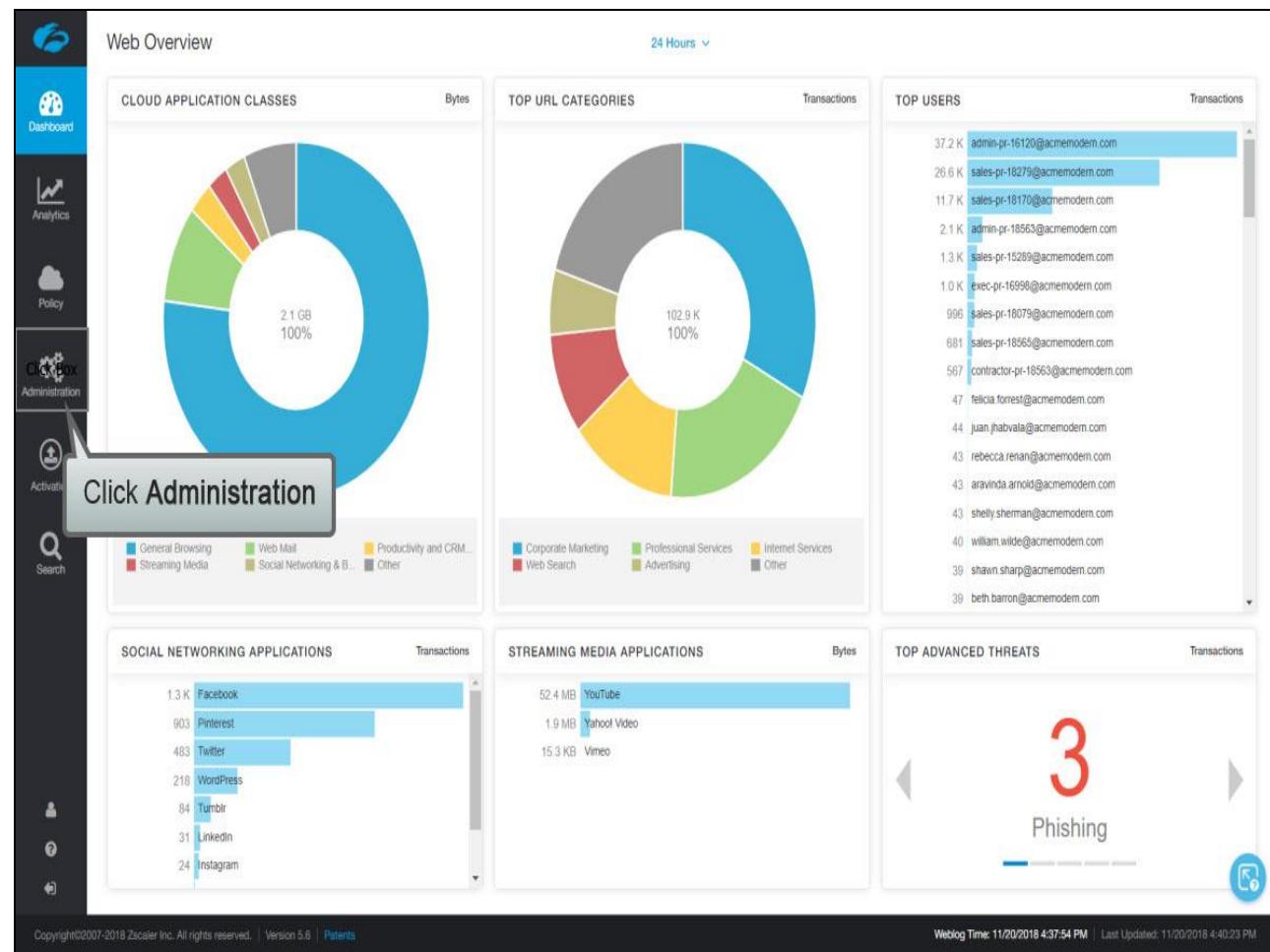


Back to Zscaler to Modify AD Settings

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

The screenshot shows the Zscaler Cloud interface. On the left, a sidebar menu is open under the 'Administration' section, specifically the 'Authentication' sub-section. A callout box with the text 'Click Authentication Settings' points to the 'Authentication' link in the sidebar. The main content area displays several dashboards:

- TOP URL CATEGORIES:** A donut chart showing traffic distribution across categories. The chart is divided into four segments: Corporate Marketing (blue), Web Search (red), Advertising (green), and Internet Services (yellow). The total value is 102.9 K.
- STREAMING MEDIA APPLICATIONS:** A bar chart showing bytes transferred for different media applications. YouTube leads with 52.4 MB, followed by Yahoo Video (1.9 MB) and Vimeo (15.3 KB).
- TOP USERS:** A list of users ranked by transactions. The top user is admin-pr-16120@acmemodern.com with 37.2 K transactions.
- TOP ADVANCED THREATS:** A summary card indicating 3 Phishing threats.

At the bottom of the interface, there are copyright and update information: Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients. Weblog Time: 11/20/2018 4:36:18 PM | Last Updated: 11/20/2018 4:38:48 PM

Slide notes

...then **Authentication Settings**.

Slide 86 - Slide 86

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'AUTHENTICATION PROFILE'. It includes tabs for 'HOSTED DB', 'Active Directory' (which is selected), and 'OpenLDAP'. Below these are sections for 'Authentication Frequency' (set to 'Daily'), 'Authentication Type' (set to 'Form-Based'), and 'Temporary Authentication' (set to 'Disabled'). A large callout box with the text 'Click Setup Wizard' points to the 'Click Box' button located in the top right corner of the main content area. The bottom of the page shows copyright information ('Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients') and a timestamp ('Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM').

Slide notes

Click on **Setup Wizard**.

Slide 87 - Slide 87

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a navigation sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area displays the 'Authentication Setup Wizard' configuration screen for a 'Directory Server'. The configuration includes:

- Authentication Agent Hosting:** Radio buttons for 'Enterprise' (selected) and 'Cloud'.
- Directory Server Address:** Input field containing '184.170.227.124'.
- Secure LDAP:** Checkboxes for 'Enabled' (selected) and 'TLS 1.2'.
- Directory Type:** Dropdown menu set to 'Microsoft Active Directory'.
- Port:** Input field containing '3269'.
- Secondary Configuration:** Checkbox for 'Use a secondary server'.

A large callout bubble points to the 'Next' button at the bottom right of the configuration panel, which is labeled 'Click Box'.

At the bottom of the configuration panel, it says 'Configuration loaded'. Below the configuration panel are buttons for 'View Setup Log', 'Cancel', 'Click Box' (highlighted with a red box), and 'Back'.

At the very bottom of the page, there is footer text: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM'.

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

Authentication Setup Wizard

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a navigation sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The 'Administration' icon is highlighted in blue. The main window title is 'Authentication Setup Wizard'. The current step is 'Directory Server Authentication'. It includes fields for 'Bind DN' (set to 'TRAINING2\administrator') and 'Bind Password' (redacted). Below these fields is a note: 'Enter the login credentials to authenticate to your directory server. This is typically your windows domain administrator login (in DOMAIN\user form) or the DN of an administrator user'. At the bottom of the wizard window, there are buttons for 'View Setup Log', 'Cancel', 'Click Box' (which is highlighted with a gray box and a callout bubble containing the text 'Click Next'), and 'Back'.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM

Slide notes

Click **Next**, ...

Slide 89 - Slide 89

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, Search, and other unlabelled items. The main window displays 'Detected Settings' with a dropdown for 'Base DN' set to 'DC=training2,DC=safemarch,DC=com'. Under 'Pagination', the 'Auto (recommended)' radio button is selected. A note says 'Detected pagination is Enabled'. At the bottom, there's a message 'Parameters detected' and buttons for 'View Setup Log', 'Cancel', 'Click Box' (which is highlighted with a red box and a callout saying 'Click Next'), and 'Back'.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM

Slide notes

Click **Next**, ...

Slide 90 - Slide 90

The screenshot shows the 'Authentication Setup Wizard' interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration (which is selected), Activation, Search, and other icons. The main window title is 'Authentication Setup Wizard'. It displays a message: 'To discover the LDAP attributes needed by the cloud service, you need to specify a sample username.' Below this are two sections: 'Lookup Parameters' (set to 'Auto') and 'Lookup Results' (empty). A callout bubble points to the 'User Login' dropdown in the 'Attribute Fields' section, which currently contains 'mail'. The 'Attribute Fields' section also includes fields for User Full Name ('displayName'), User Search Filter ('(objectClass=User)'), Group Name ('cn'), Group Membership ('memberOf'), Group Search Filter ('(objectClass=group)'), and Department Membership ('department'). At the bottom, a message says 'Parameters saved' and includes buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The footer contains copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM'.

Slide notes

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

Slide 91 - Slide 91

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main window title is 'Authentication Setup Wizard'. It displays a message: 'To discover the LDAP attributes needed by the cloud service, you need to specify a sample username.' Below this are two sections: 'Lookup Parameters' (set to 'Auto') and 'Lookup Results' (empty). In the 'Attribute Fields' section, there are four fields: 'User Login' (set to 'mail'), 'User Full Name' (set to 'mail'), 'User Search Filter' (set to 'sAMAccountName'), and 'Group Membership' (set to 'memberOf'). A callout box with the text 'Click sAMAccountName' points to the 'User Search Filter' field. At the bottom, a message says 'Parameters saved' and includes buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The footer contains copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM'.

Slide notes

Slide 92 - Slide 92

The screenshot shows the 'Authentication Setup Wizard' window. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main window has a title bar 'Authentication Setup Wizard'. It contains two sections: 'Lookup Parameters' and 'Lookup Results'. In 'Lookup Parameters', there is a dropdown set to 'Auto' with a note: 'The cloud service will automatically query the directory with the most likely attributes.' Below it is a 'Lookup User Entry' button. In 'Attribute Fields', there are dropdown menus for User Login ('sAMAccountName'), Group Name ('cn'), User Full Name ('displayName'), Group Membership ('memberOf'), User Search Filter ('(objectClass=User)'), Group Search Filter ('(objectClass=group)'), and Department Membership ('department'). At the bottom of the wizard window are buttons for 'View Setup Log', 'Cancel', 'Click Box' (which is highlighted with a callout bubble), and 'Back'.

Slide notes

Click **Next**, ...

Slide 93 - Slide 93

Authentication Setup Wizard

Dashboard

Analytics

Policy

Administration

Activation

Search

Help

Logout

The screenshot shows the 'Authentication Setup Wizard' interface. At the top, it displays 'Synchronization Complete' (elapsed time: 00:00:02) and a 'Cancel Synchronization' button. Below this is a 'Synchronization Results' table:

	Added	Modified	Removed	Total Before	Total After
Users	5	0	0	1	6
Groups	0	11	0	47	47
Departments	0	0	0	0	0

At the bottom, there are buttons for 'View Setup Log', 'Cancel', 'Click Box' (which is highlighted with a red box), and 'Back'. A speech bubble points to the 'Click Box' button with the text 'Click Next'.

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM

Slide notes

Click **Next**, ...

Slide 94 - Slide 94

The screenshot shows the 'Authentication Setup Wizard' window. On the left is a vertical navigation bar with icons for Dashboard, Analytics, Policy, Administration, Activation, Search, and other system status indicators. The main window title is 'Authentication Setup Wizard'. It contains a form for 'Authentication Parameters' with fields for 'User Authentication Filter' (set to '(objectClass=User)'), 'Test User Login' (set to 'student@training2.safemarch.com'), and 'Test User Password' (set to '*****'). A 'Check Authentication' button is present. Below the form, a message says 'Authentication for Primary Directory successful'. At the bottom right of the window are buttons for 'View Setup Log', 'Cancel', 'Click Box' (which is highlighted with a red box and a callout bubble saying 'Click Next'), and 'Back'. The status bar at the bottom of the screen displays 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM'.

Slide notes

Click **Next**, ...

Slide 95 - Slide 95

The screenshot shows a software interface with a left sidebar containing icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled "Authentication Setup Wizard" and displays the "Wizard Complete" screen. The screen includes a message about configuration being complete, a warning about overwriting existing user authentication configuration, and three buttons at the bottom: "View Setup Log", "Cancel", and "Finish". A callout bubble points to the "Finish" button with the text "Click Finish".

Authentication Setup Wizard

Dashboard

Analytics

Policy

Administration

Activation

Search

Wizard Complete

Authentication configuration, directory synchronization and authentication verification are complete. Press "Finish" to save configuration and synchronized data. Press "Cancel" to discard changes.

Warning: all existing user authentication configuration will be overwritten with the settings selected using this wizard.

View Setup Log Cancel Click Box Back

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM

Slide notes

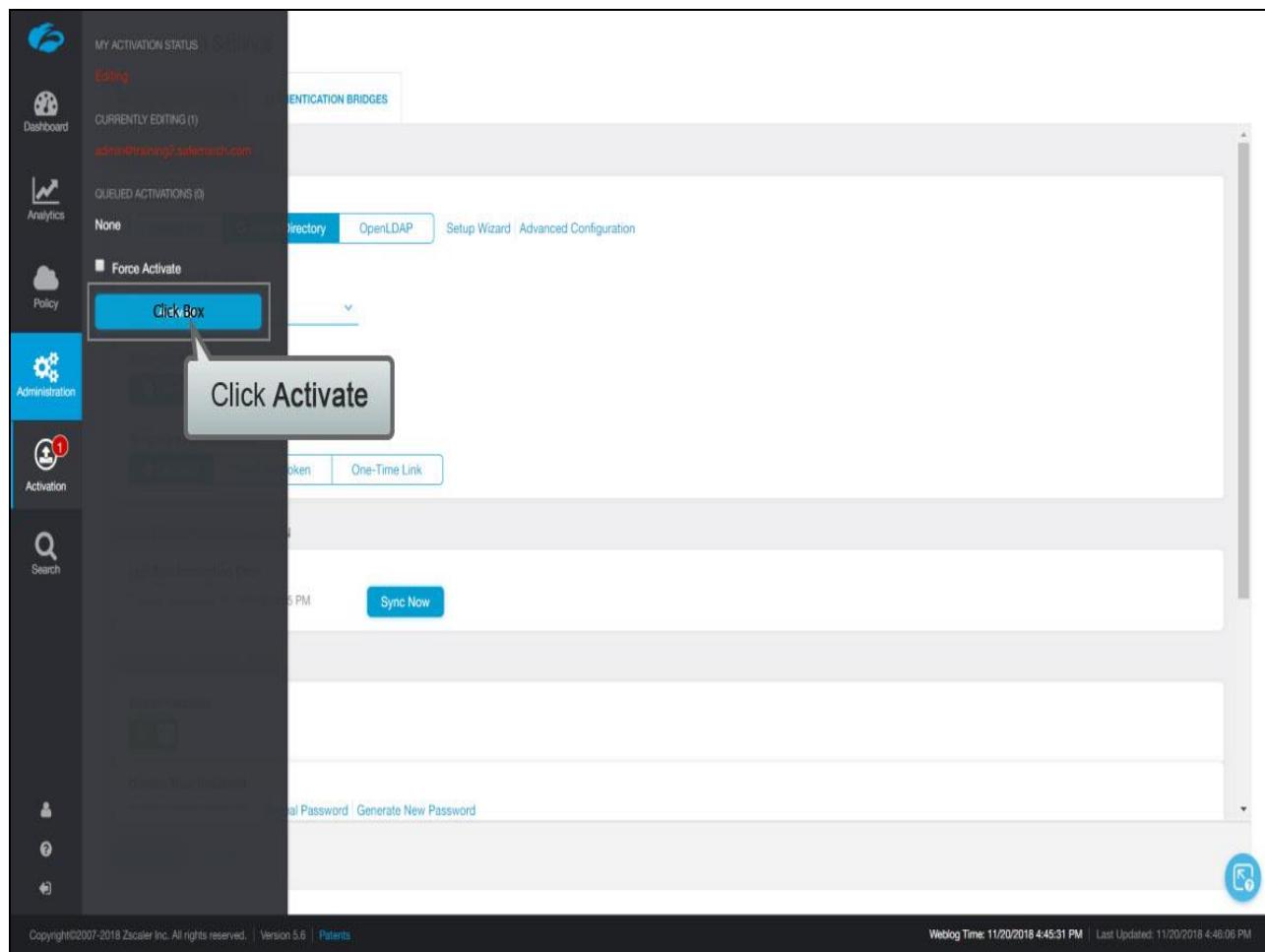
Then click **Finish**.

Slide 96 - Slide 96

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Authentication Settings' and has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', it shows 'Directory Type' set to 'Active Directory', 'Authentication Frequency' set to 'Daily', 'Authentication Type' set to 'Form-Based', and 'Temporary Authentication' set to 'Disabled'. A large callout box highlights the 'Sync Now' button under 'DIRECTORY SYNCHRONIZATION'. Below this, the 'KERBEROS AUTHENTICATION' section has 'Enable Kerberos' checked and a 'Domain Trust Password' field with 'Reveal Password' and 'Generate New Password' options. At the bottom, there are 'Save' and 'Cancel' buttons, and a copyright notice: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'. The status bar at the bottom right shows 'Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM'.

Slide notes

Then **Activate** your changes.

Slide 97 - Slide 97**Slide notes**

Slide 98 - Slide 98

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', 'Directory Type' is set to 'Active Directory'. 'Authentication Frequency' is set to 'Daily'. 'Authentication Type' is set to 'Form-Based'. 'Temporary Authentication' is set to 'Disabled'. Under 'DIRECTORY SYNCHRONIZATION', the 'Last Synchronization Time' is listed as 'Tuesday, November 20, 2018 4:54:35 PM' with a 'Sync Now' button. Under 'KERBEROS AUTHENTICATION', 'Enable Kerberos' is checked. A 'Domain Trust Password' field is present with 'Reveal Password' and 'Generate New Password' options. At the bottom are 'Save' and 'Cancel' buttons, and a refresh icon.

Activation Completed!

AUTHENTICATION PROFILE AUTHENTICATION BRIDGES

DASHBOARD ANALYTICS POLICY ADMINISTRATION ACTIVATION SEARCH

AUTHENTICATION PROFILE

Directory Type: Active Directory

Authentication Frequency: Daily

Authentication Type: Form-Based

Temporary Authentication: Disabled

DIRECTORY SYNCHRONIZATION

Last Synchronization Time: Tuesday, November 20, 2018 4:54:35 PM Sync Now

KERBEROS AUTHENTICATION

Enable Kerberos:

Domain Trust Password: Reveal Password | Generate New Password

Save Cancel

Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients

Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM

Slide notes

Slide 99 - Slide 99

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar has icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'Authentication Settings' and contains several sections:

- AUTHENTICATION PROFILE**: Sub-sections include 'Directory Type' (Active Directory selected), 'Authentication Frequency' (Daily), 'Authentication Type' (Form-Based selected), and 'Temporary Authentication' (Disabled selected).
- DIRECTORY SYNCHRONIZATION**: Shows 'Last Synchronization Time' as Tuesday, November 20, 2018 4:54:35 PM, with a 'Sync Now' button.
- KERBEROS AUTHENTICATION**: Includes 'Enable Kerberos' (checked), 'Domain Trust Password' (input field with 'Reveal Password' and 'Generate New Password' links), and 'Save' and 'Cancel' buttons.

At the bottom, there are copyright notices: 'Copyright©2007-2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Patients'. On the right, it says 'Weblog Time: 11/20/2018 4:45:31 PM | Last Updated: 11/20/2018 4:46:06 PM'.

Slide notes

Slide 100 - Windows PC Configuration

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_MACHINE\Software\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**

Name	Type	Data
(Default)	REG_SZ	(value not set)
ZSCALERTWO.NET	REG_SZ	.zscalertwo.net;.gateway.zscalertwo.net

Computer\HKEY_LOCAL_MACHINE\Software\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>**

Name	Type	Data
(Default)	REG_SZ	(value not set)
ZSCALERTWO.NET	REG_SZ	<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

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

Common Issues

 Time not in sync	 User is not provisioned on Zscaler
 PAC file serves IP address and not domain	 Cross-realm not setup on client
 Cross-realm not setup on server	 Realm domain and Zscaler domain not identical

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

Kerberos Troubleshooting

Time synchronization

- Kerberos authentication can be affected by some network configuration parameters such as time synchronization

Error Codes

- If authentication fails, the client browser will display an error code
- The details of the error codes are found in the **Kerberos Configuration Guide**
- A table in the **Troubleshooting** section lists : **Error Code, Description, Cause, Solution**

Zscaler Help

- To get to the Zscaler Help Portal either go direct to <https://support.zscaler.com> or login to the Zscaler Admin UI then click on the Help icon in the upper right corner

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



Kerberos Troubleshooting

- Klist

- Displays the Kerberos tickets that were used by the workstation to log in to the domain, shows that the workstation is in the domain, and can contact the domain controller

```
C:\Users\mchristensen>klist
Current LogonId is 0x01120ce
Cached Tickets: (3)
#0>    Client: mchristensen @ TRAINING.SAFEMARCH.COM
        Server: krbtgt/TRAINING.SAFEMARCH.COM @ TRAINING.SAFEMARCH.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 5/26/2015 10:10:23 <local>
        End Time: 5/26/2015 20:10:23 <local>
        Renew Time: 6/2/2015 10:10:23 <local>
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#1>    Client: mchristensen @ TRAINING.SAFEMARCH.COM
        Server: krbtgt/TRAINING.SAFEMARCH.COM @ TRAINING.SAFEMARCH.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 5/26/2015 10:10:23 <local>
        End Time: 5/26/2015 20:10:23 <local>
        Renew Time: 6/2/2015 10:10:23 <local>
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#2>    Client: mchristensen @ TRAINING.SAFEMARCH.COM
        Server: cifs/ad.training.safemarch.com @ TRAINING.SAFEMARCH.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 5/26/2015 10:10:23 <local>
        End Time: 5/26/2015 20:10:23 <local>
        Renew Time: 6/2/2015 10:10:23 <local>
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

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

Event Logging

- Microsoft Help
 - <http://support.microsoft.com/kb/262177>
 - [http://technet.microsoft.com/en-us/library/cc738673\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc738673(v=ws.10).aspx)
 - <http://blogs.technet.com/b/askds/archive/2012/07/27/kerberos-errors-in-network-captures.aspx>

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



Thank You and Quiz

Slide notes

Thank you for participating 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.