

**Slide 1 - ZCCP-IA**



# ZCCP-IA

## Authentication – AD / LDAP

©2018 Zscaler, Inc. All rights reserved.

**Slide notes**

Hello and welcome to this eLearning module on Authentication with Active Directory and Lightweight Directory Access Protocol (LDAP).

## 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. Below it is a large blue button labeled "Exit". On the left side, there are two blue callout boxes: "Previous Slide" and "Next Slide". In the center, there are four blue callout boxes: "Play/Pause", "Fast Forward", "Progress Bar", and "Audio On/Off". On the right side, there is one blue callout box labeled "Closed Captioning". The dashboard itself displays various charts and lists, including a pie 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 - Authentication with AD / LDAP**

# Agenda

- AD / LDAP
- User Provisioning
- User Authentication
- LDAP Setup Wizard
- Demo

**Slide notes**

During this session we will look at Active Directory Integration, User Provisioning, User authentication, and run through an interactive configuration demonstration.

**Slide 4 - AD / LDAP**

**AD / LDAP**



**Slide notes**

**Slide 5 - 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.

**Slide 6 - 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 7 - 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

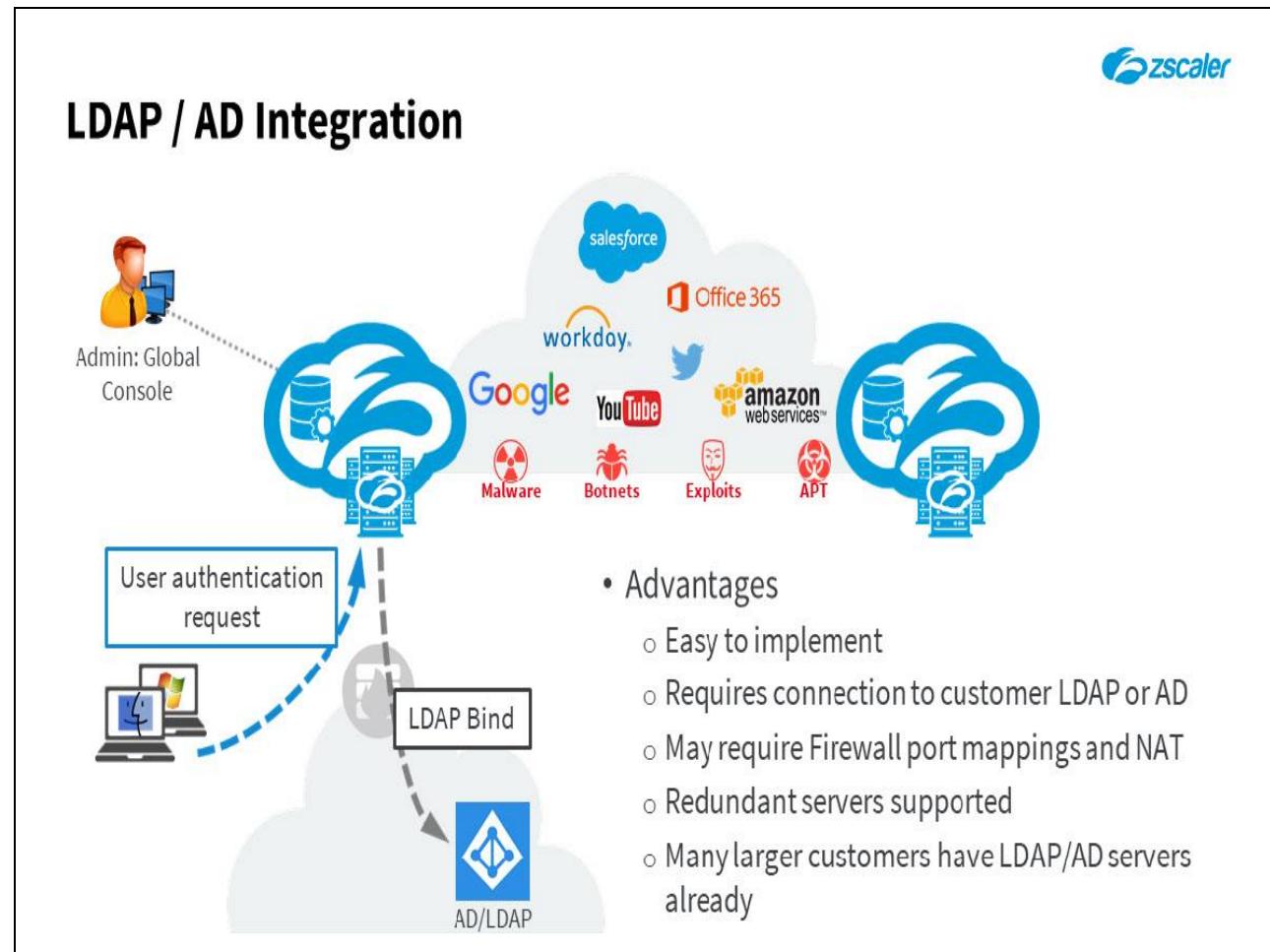
3.

### 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 8 - LDAP / AD Integration****Slide notes**

Active Directory or LDAP is simple to implement with Zscaler via a simple configuration wizard. There is no hardware or software to deploy other than the customers' own existing directory infrastructure which most customers already have in place. Integration, in its most basic form does require that the customer open communication between Zscaler and their Directory servers through the firewall. Server redundancy is also supported.

**Slide 9 - Customer Concerns With AD Integration**

## Customer Concerns With AD Integration

- Does not want to open a 'security hole' into their LDAP/AD server
- Does not permit connections from 'insecure' networks to secure ones
- Afraid Zscaler will augment utilization on LDAP/AD environment

**Slide notes**

Customers may be concerned that they have to open holes to their Directory server and they may also be concerned that Zscaler can somehow modify their Directories.

**Slide 10 - Customer Concerns With AD Integration – Response In short**

## Customer Concerns With AD Integration – Response In short



- Does not want to open a ‘security hole’ into their LDAP/AD server
  - Connecting to the customer LDAP or AD is secure
    - firewall rules required for authentication limit access.
    - Secure LDAP (LDAPS) is used
    - The bind account does not require privileged access over the directory
- Does not permit connections from ‘insecure’ networks to secure ones
  - Passwords are not sent over the Internet
  - Zscaler does not ‘pull’ the entire account list and passwords down from the customer directory, only validates the user input via an LDAP query
- Afraid Zscaler will augment utilization on LDAP/AD environment
  - Authentication is only required to install the authentication cookie – very low overhead if authentication is set to ‘onetime only’ – no more authentication once cookie is present

**Slide notes**

AD Integration, however, is very secure. Secure LDAP is recommended for LDAP over SSL. Strict firewall policies are configured to allow communication between the Zscaler cloud and the customers Directory server over a specific port. Zscaler does not import user passwords - only username, group, and department information is copied.

Lastly, authentication requires the insertion of an authentication cookie into the user’s browser. The cookie has an expiration time built in which can be: per session, daily, only once, or a custom time period.

**Slide 11 - Zscaler- Firewall Rules**

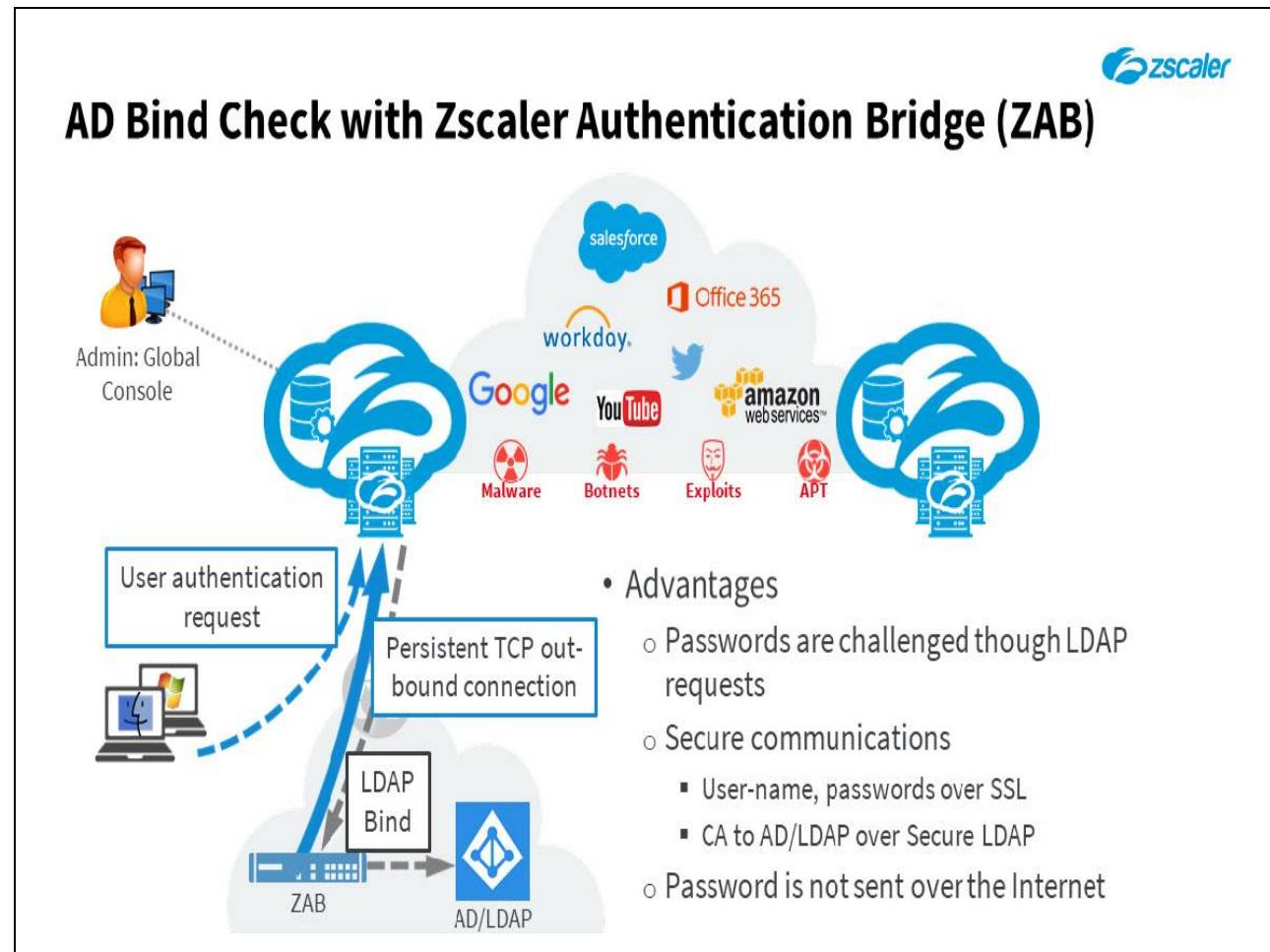
## Zscaler - Firewall Rules

Port	From	To	Reason
TCP 80 TCP 443	Customer Network	Zscaler Nodes IP's	Client Web Usage
TCP 80 TCP 443	Customer Network	Zscaler Node IP's	Client access to Hosted Authentication Agent Service
TCP 389, TCP 636, TCP 3268, OR TCP 3269 Depending on Directory Server Type and if SSL is used	Zscaler Node IP's	Customer Directory Server	Authentication verification requests from Zscaler Hosted Authentication Agent to customer directory server

- For an up to date and complete list of Zscaler IP addresses for your Firewall policies go to: [https://ips.<cloud\\_name>.net](https://ips.<cloud_name>.net)  
For example: <https://ips.zscalerone.net>  
<https://ips.zscalertwo.net>

**Slide notes**

As mentioned previously some Firewall configuration is required to allow communications between the Zscaler cloud and the Directory server behind the Firewall; a summary of rules is shown here. For a complete list of Zscaler IP addresses for your Firewall policies go to [https://ips.<cloud\\_name>.net](https://ips.<cloud_name>.net) (which is the cloud you are assigned when signed up for the Zscaler service). For example, [ips.zscalertwo.net](https://ips.zscalertwo.net).

**Slide 12 - AD Bind Check with Zscaler Authentication Bridge (ZAB)****Slide notes**

An option to opening holes in your firewall to allow Zscaler to communicate with your directory server is to install a Zscaler Authentication Bridge, or ZAB, in your network behind the firewall. The ZAB is a VM that is installed on your own hardware.

The ZAB then communicates directly with your Directory Server thus eliminating the need for opening ports on the firewall. The ZAB periodically initiates an outbound connection to the Zscaler service in the cloud. The Zscaler Authentication Bridge will be discussed in more detail in another eLearning module later.

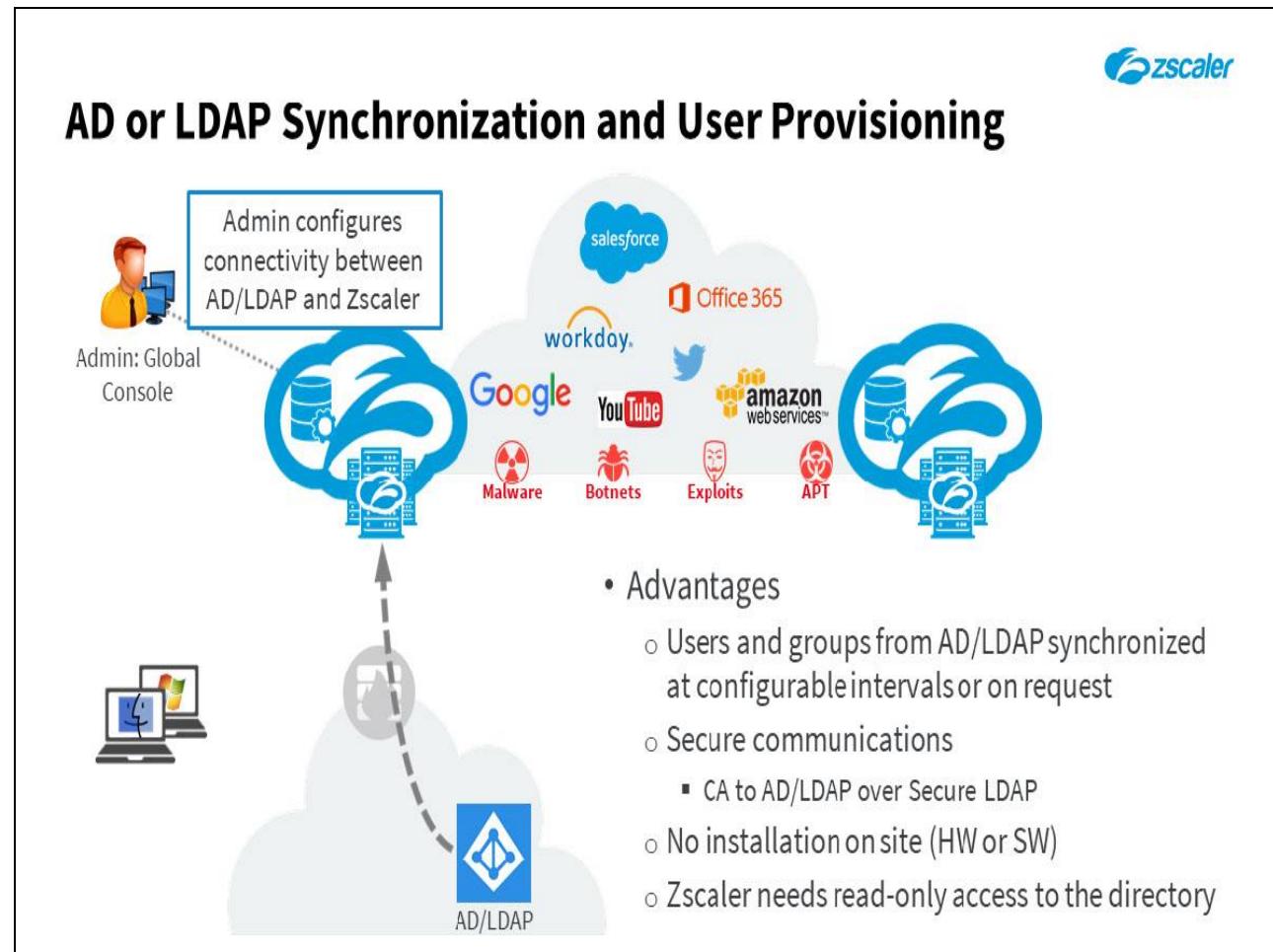
**Slide 13 - User Provisioning**



# User Provisioning

**Slide notes**

Let's take a look at how Zscaler synchronizes with AD and imports user names, groups, and department membership.

**Slide 14 - AD or LDAP Synchronization and User Provisioning****Slide notes**

Even though the user accounts exist on the directory server the Zscaler system must also know the user names, so they can be tied to the proper policies. As stated previously, there are several ways to get the user information into Zscaler from manual processes to automatic processes.

When integrating with AD Zscaler can be configured to synchronize with AD on regular configurable intervals or even manually anytime desired.

**Slide 15 - LDAP Sync Process - detailed**

## LDAP Sync Process - Detailed

- Zscaler authenticates to LDAP using Bind DN and password...

### Retrieve list of users

- Eliminate unwanted Users (printers, computers, etc) by applying LDAP User filter
  - Eliminate Users whose email address doesn't belong to Zscaler registered domains
- Retrieve **Group** mappings
  - Eliminate unwanted Groups (printer access etc.) by applying LDAP Group Filter
- Retrieve **Department** mapping

**Slide notes**

Zscaler authenticates to the Directory server using the BIND DN and password and retrieves the user list. Which entries in the Directory server database are copied in to Zscaler can be controlled using filters such as group mappings and user filters.

**Slide 16 - LDAP Sync Process – Detailed**

## LDAP Sync Process – Detailed

- Zscaler authenticates to LDAP using Bind DN and password...

### Retrieve list of users

- Eliminate unwanted Users (printers, computers, etc) by applying LDAP User filter
  - Eliminate Users whose email address doesn't belong to Zscaler registered domains
- Retrieve **Group** mappings
  - Eliminate unwanted Groups (printer access etc.) by applying LDAP Group Filter
- Retrieve **Department** mapping

### Compare list to Zscaler Cloud

- If User (or Group, or Department) exists on LDAP, but not on Zscaler:
  - Add User/Group/Department on Zscaler
- If User (or Group or Department) exists on Zscaler but not on LDAP:
  - Delete User/Group/Department on Zscaler
- If User exists on both Zscaler and LDAP:
  - Update Group/Department attributes on Zscaler mirroring that of LDAP
- If User belongs to a Group or Department not on Zscaler:
  - Create the Group/Department and add user to it

**Slide notes**

Entries are added or deleted based on the following rules:

- If user (or group or dept) exists on LDAP, but not on Zscaler: User (or Group or Dept) was added newly, add the user (or group or dept) on Zscaler
- If user (or group or dept) exists on Zscaler but not on LDAP: User (or Group or Dept) was deleted, delete the user (or group or dept) on Zscaler
- If user exists on both Zscaler and LDAP: Update group/department/name attributes on Zscaler mirroring that of LDAP
- If user belongs to a group (or dept) not on Zscaler: Create the group (or dept) and add user to it

**Slide 17 - LDAP Sync Configuration Parameters**

<b>LDAP Sync Configuration Parameters</b>		
LDAP Address	LDAP Login Credentials	Attribute Mapping
<ul style="list-style-type: none"><li>• IP Address</li><li>• Clear-text or SSL Port</li></ul> <p><b>Passwords are never synchronized to the cloud</b></p>	<ul style="list-style-type: none"><li>• Login (Bind DN, Domain Logon)</li><li>• Bind Password (stored encrypted in the cloud)</li><li>• Base DN</li></ul>	<ul style="list-style-type: none"><li>• Login Name (UPN, Proxy addresses, sAMAccountName)</li><li>• Group (memberOf)</li><li>• Department (Department, Country)</li><li>• Full Name (displayname, cn)</li><li>• User/Group Filter</li></ul>
<ul style="list-style-type: none"><li>• <b>Login Name:</b> email address format, must be unique, email Domain must be registered, concatenatesAMAccountName(if used) with Domain</li><li>• <b>Groups:</b> Used to set policy, 128 groups per user, unlimited users per group, Group Filters</li><li>• <b>Departments:</b> used for reporting, 1 department per user, unlimited users per department</li></ul>		

**Slide notes**

Zscaler is configured with the following parameters so it can communicate with the Directory Server: Directory server IP address and port and we choose whether to send in the clear or via SSL.

Zscaler needs the LDAP login credentials so it can log in and synchronize the Directory Servers information to Zscaler --- this is a one-way operation.

And we need to define the format of the login name, group, department, full name, and user and group filters.

**Slide 18 - LDAP Sync Methods**

## LDAP Sync Methods

Setup Wizard	LDAP Manual Sync	LDAP Auto Sync
<ul style="list-style-type: none"><li>Interactive mode wizard to setup LDAP Configuration</li><li>Validation of every step</li><li>Parameters are saved only if they are correct</li><li>Running Progress Display</li><li>Strongly recommended for any configuration change</li><li>Auto-probe of BaseDN and Pagination</li></ul>	<ul style="list-style-type: none"><li>On-demand</li><li>Running Progress Display</li></ul>	<ul style="list-style-type: none"><li>Automatic background synchronization</li><li>Frequency: Daily, Weekly, Monthly</li><li>Generates email alerts to indicate success or failure</li><li>Provides safeguards against mass-deletion due to bad config change</li></ul>

**Slide notes**

Several methods can be used to trigger synchronization. For example, if you use the Setup wizard synchronization occurs as part of the wizard as you will see later in the demo. Synchronization can also be done on-demand in the Admin Portal and it can also be configured to synchronize automatically on a configured interval.

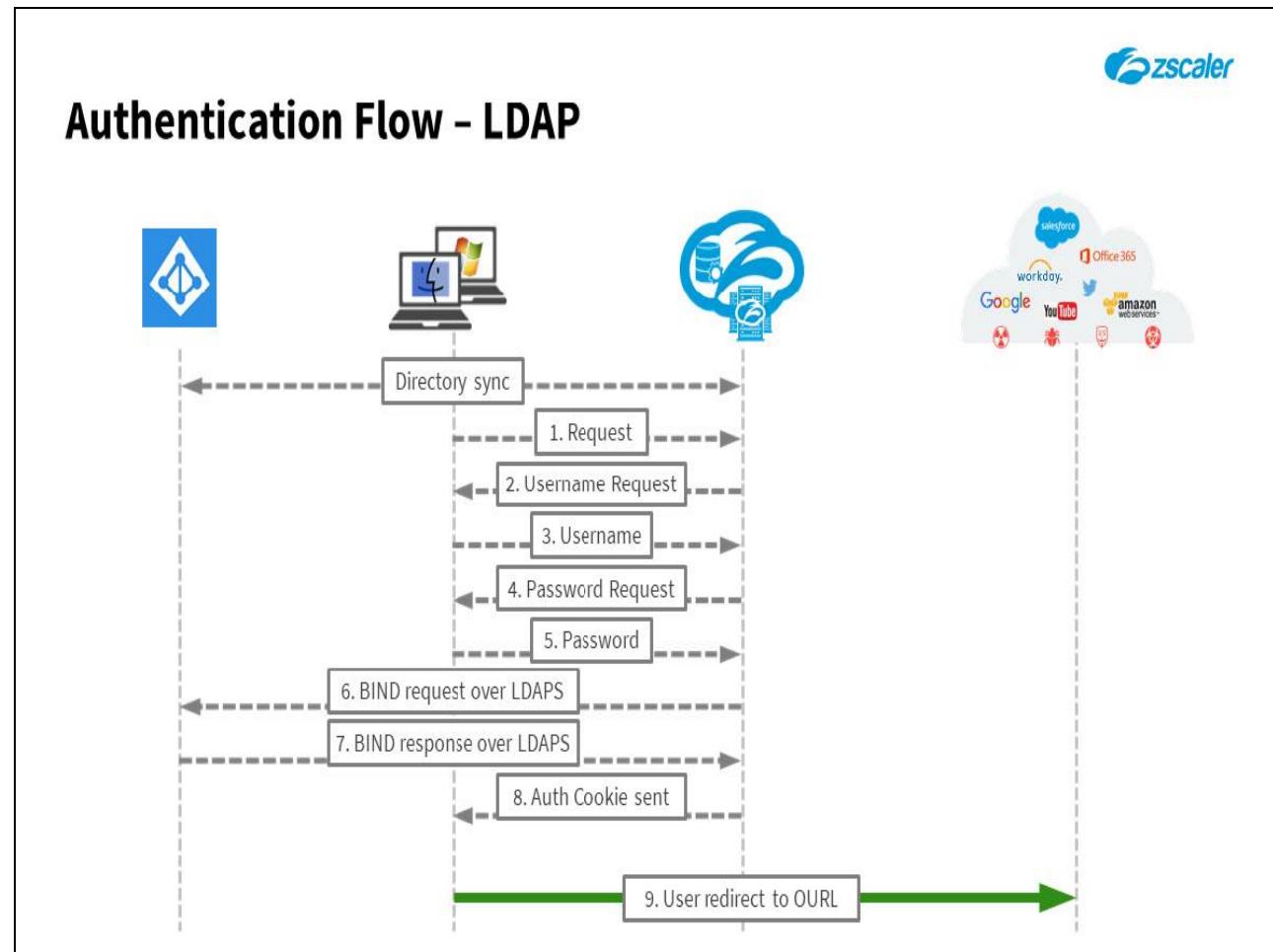
**Slide 19 - User Authentication**



# User Authentication

**Slide notes**

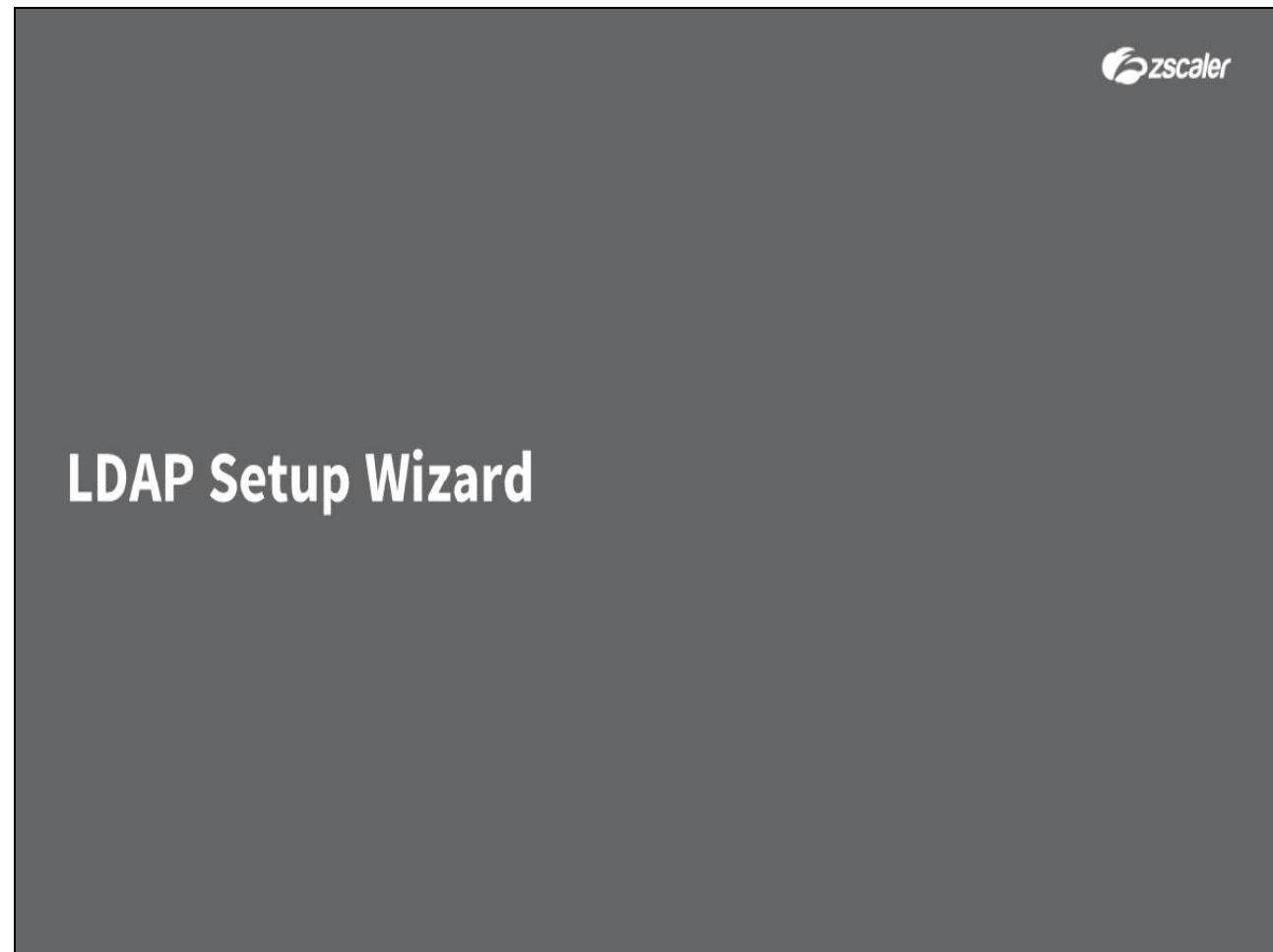
Let's now take a look at the authentication process.

**Slide 20 - Authentication Flow – LDAP****Slide notes**

Now that provisioning is complete via AD Sync when an unauthenticated user is seen by Zscaler as it attempts to browse to a website it will trigger the following authentication process:

- The ZEN recognizes an unauthenticated client and redirects it to the Central Authority (CA) for authentication.
- The CA challenges the browser with username and password, and the browser sends its authentication credentials to the CA.
- The CA verifies the provided credentials with the customers directory server (LDAP, Active Directory).
- If successful, the CA inserts a cookie and redirects the browser to the original site. The ZEN intercepts the request, and recognizes the cookie and allows it to pass through

**Slide 21 - LDAP Setup Wizard**



**Slide notes**

The LDAP setup wizard should always be used. You can configure all the settings, but the wizard automates most of these tasks.

## Slide 22 - Slide 22

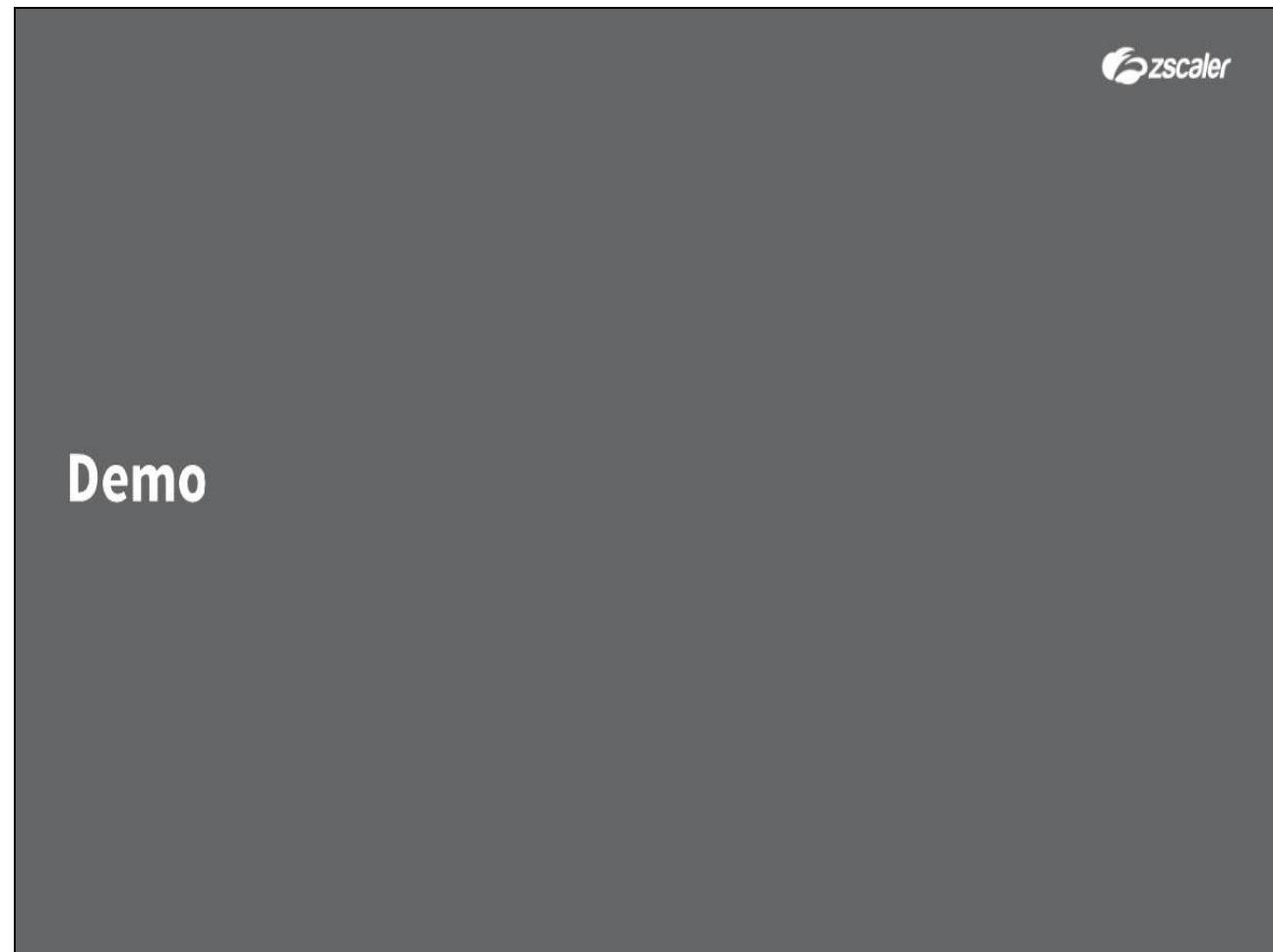
The screenshot shows the Zscaler Admin Portal interface. On the left, there's a vertical sidebar with icons for Dashboard, Analytics, Policy, and Administration. The main area has a title 'AD / LDAP Setup Wizard' at the top. Below it, there's a sub-header 'Authentication Settings' and tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', there's a section for 'Directory Type' with options 'Hosted DB', 'Active Directory', 'OpenLDAP' (selected), and 'Setup Wizard | Advanced Configuration' (which is circled in red). Other settings include 'Authentication Frequency' (Once Per Session) and 'Authentication Type' (Form-Based selected, SAML). To the right, a modal window titled 'Authentication Setup Wizard' is open, showing fields for 'Directory Server' (Authenticator Agent Hosting: Enterprise selected, Cloud), 'Directory Name', 'Directory Server IP Address', 'Secure LDAP' (checkbox checked), 'Warning: LDAP data will be transmitted over clear text', 'Directory Type' (dropdown), 'Port' (input field), and 'Secondary Configuration' (checkbox). At the bottom of the modal, there's an 'I/O problem' message, a 'View Setup Log' link, and 'Cancel', 'Next', and 'Back' buttons.

- **LDAP Setup Wizard**
  - Configure all AD related items
  - Displays AD sync status / results
  - Test user authentication
  - Recommended for configuring AD / LDAP
  - Use **Advanced Configuration** option to configure manually

## Slide notes

The setup wizard option appears in the Admin Portal when the Directory Type is set to **Active Directory** or **Open LDAP**. It is used to configure all AD related items, display synchronization status and results, test user authentication and is considered Best Practice. Should you desire you can always click on **Advanced Configuration** and config all items manually.

**Slide 23 - Demo**



**Slide notes**

During this interactive demo you will participate in configuring AD integration with Zscaler.

**Slide 24 - Assumptions and tasks**

## Assumptions and tasks

- Assumptions
  - Focus on Microsoft Active Directory
  - Assumed that Active Directory is already installed and configured, and users created
  - Assumed the appropriate Firewall policies are configured to allow communication from Zscaler to your AD
- Tasks
  1. Configure Zscaler for AD Integration
  2. Set the Synchronization frequency
  3. Use the Setup Wizard to configure:
    - Server IP
    - Server type
    - User information
    - Test user authentication

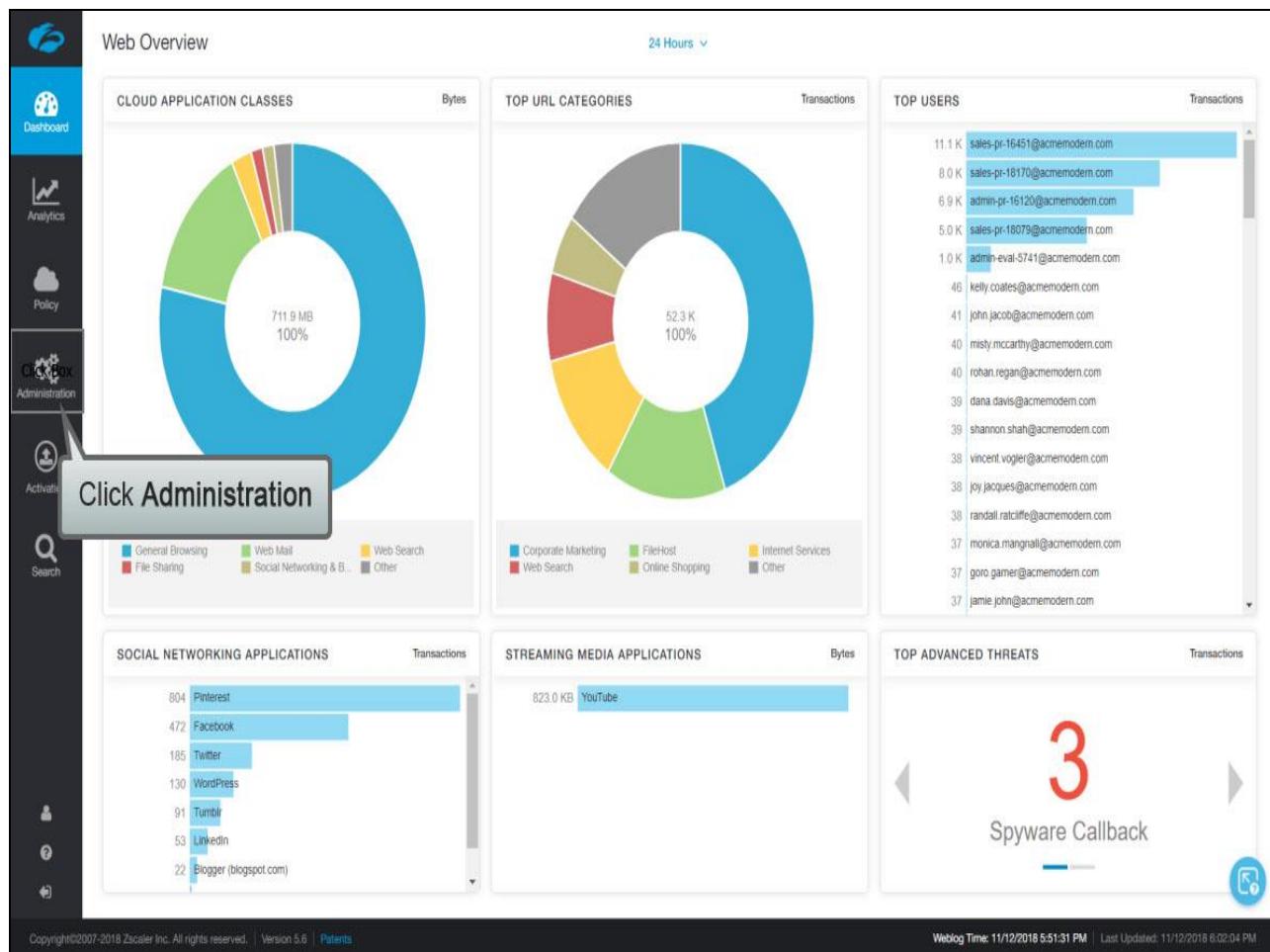
**Slide notes**

This demonstration focuses on Microsoft Active Directory. It is assumed that you already have Active Directory installed and configured and users created in your own environment. You have already configured the appropriate Firewall policies to allow communication from the Zscaler service to your AD.

The tasks that will be demonstrated are:

1. Configure Zscaler for AD Integration,
2. Set the Synchronization frequency,
3. Use the Setup Wizard to configure the following:
  - a. Server IP,
  - b. Server type,
  - c. User information,
  - d. And test user authentication.

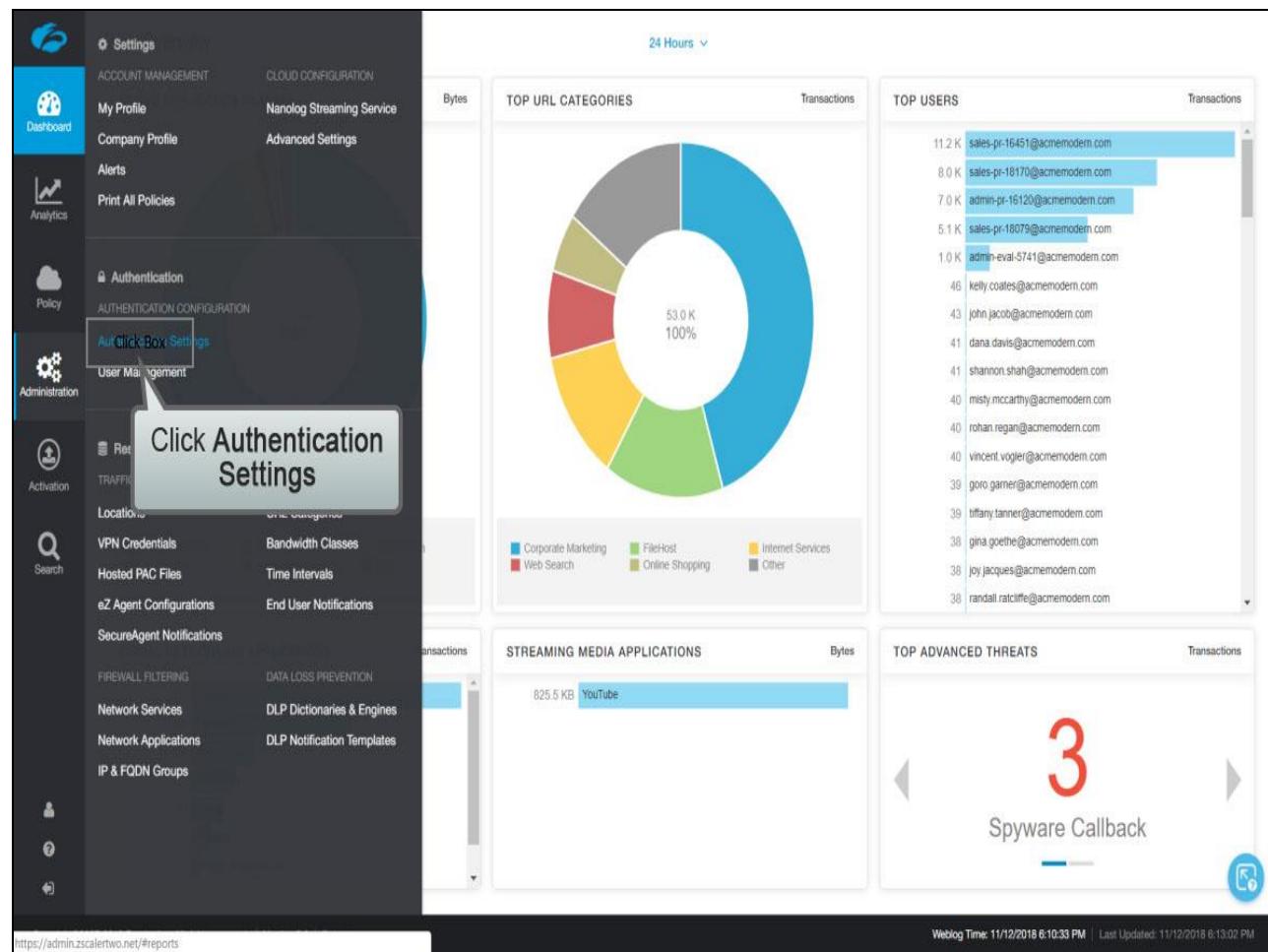
## Slide 25 - Slide 25



## Slide notes

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

## Slide 26 - Slide 26



## Slide notes

...then **Authentication Settings**.

## Slide 27 - Slide 27

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 are sections for 'Directory Type' (with 'Hosted DB' checked), 'Authentication Frequency' (set to 'Only Once'), 'Authentication Type' (with 'Form-Based' checked), and 'Temporary Authentication' (with 'Disabled' checked). A large callout box with the text 'Click Active Directory' points to the 'Active Directory' button in the 'Directory Type' section. Below these are sections for 'KERBEROS AUTHENTICATION' (with 'Enable Kerberos' checked) and 'FORCE REAUTHENTICATION FOR ALL USERS'. At the bottom are 'Save' and 'Cancel' buttons, and a status message: 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

## Slide notes

Set the Directory Type to **Active Directory**, ...

## Slide 28 - Slide 28

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 is titled 'AUTHENTICATION PROFILE' and contains tabs for 'HOSTED DB', 'Active Directory' (which is selected and highlighted with a blue border), and 'OpenLDAP'. Below these tabs are sections for 'Authentication Frequency' (set to 'Only Once'), 'Authentication Type' (set to 'Form-Based'), and certificate expiration dates for IDP and SP SSL. A callout bubble with the text 'Click Setup Wizard' points to the 'Click Box' button located in the bottom right corner of the main content area. At the bottom, there are 'Save' and 'Cancel' buttons.

## Slide notes

...then click on **Setup Wizard**.

## Slide 29 - Slide 29

The screenshot shows the Zimbra Admin interface with the 'Authentication Settings' page open. The 'AUTHENTICATION PROFILE' tab is selected. In the center, there's a 'Confirm' dialog box with the message: 'You have unsaved changes that you will lose if you navigate away from this page. Are you sure you want to leave this page?'. Two buttons are visible: 'Click Box' (highlighted with a callout) and 'Cancel'. The background shows various configuration options like 'Authentication Type' (Form-Based, SAML), 'SSL Certificate Expiration Dates', and 'Temporary Authentication' settings.

## Slide notes

## Slide 30 - Slide 30

The screenshot shows the Zscaler Authentication Setup Wizard interface. On the left is a navigation sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main area is titled 'Authentication Setup Wizard'. A callout box with the text 'Click to select Cloud' points to the 'Enterprise' radio button under 'Authentication Agent Hosting'. The 'Cloud' radio button is also visible. Other fields include 'Directory Name', 'Directory Server Address', 'Secure LDAP' (checkbox), 'Directory Type', 'Port', and 'Secondary Configuration' (checkbox). At the bottom are 'View Setup Log', 'Cancel', 'Next', and 'Back' buttons.

## Slide notes

For the **Authentication Agent Hosting** select **Cloud** if Zscaler will query your Active Directory server or **Enterprise** if the Zscaler Authentication Bridge is used. For the purpose of this demo select **Cloud**.

**Slide 31 - Slide 31**

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 'Administration' icon is highlighted in blue. The main window title is 'Authentication Setup Wizard'. The current step is 'Directory Server'. The configuration options are as follows:

- Authentication Agent Hosting:** Radio button selected for 'Cloud'.
- Directory Server Address:** An empty text input field.
- Secure LDAP:** A checkbox labeled 'Enabled' is checked.
- Warning:** A message states, 'Ensure that your firewall ports are opened for the cloud service to query your Directory server'. Below it, another message says, 'Warning: LDAP data will be transmitted over clear text.'
- Directory Type:** A dropdown menu set to 'Microsoft Active Directory'.
- Port:** A text input field containing '3268'.
- Secondary Configuration:** A checkbox labeled 'Use a secondary server' is unchecked.

At the bottom of the wizard window are buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'.

At the very bottom of the screen, there is footer text: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

**Slide notes**

**Slide 32 - Slide 32**

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 'Administration' icon is highlighted in blue. The main window title is 'Authentication Setup Wizard'. A callout box highlights the 'Directory Server' section with the text 'Enter the Directory Server Address'. The 'Directory Server Address' input field contains the value '184.170.227.124' and is also highlighted with a red box. Other fields in this section include 'Authentication Agent Hosting' (radio buttons for 'Enterprise' and 'Cloud'), 'Secure LDAP' (checkbox 'Enabled' checked), 'Warning: LDAP data will be transmitted over clear text.', 'Directory Type' (dropdown menu set to 'Microsoft Active Directory'), 'Port' (text input '3268'), and 'Secondary Configuration' (checkbox 'Use a secondary server'). At the bottom of the window are buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The footer of the page includes copyright information 'Copyright©2007-2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Patients', as well as a timestamp 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

**Slide notes**

Remember, your Firewall must be configured to allow communication between Zscaler and your Active Directory server as described previously during the slides. Specify the public IP address of your Active Directory server.

## Slide 33 - Slide 33

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 'Administration' icon is highlighted in blue. The main window title is 'Authentication Setup Wizard'. The current step is 'Directory Server'. It includes fields for 'Authentication Agent Hosting' (Enterprise selected), 'Directory Server Address' (184.170.227.124), 'Secure LDAP' (checkbox checked, with a note about clear text transmission), 'Directory Type' (Active Directory selected), 'Port' (389), and 'Secondary Configuration'. A large callout box points to the 'Secure LDAP' checkbox with the text 'Click to select Secure LDAP'. At the bottom are buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'.

## Slide notes

Select **Secure LDAP**. This checkbox enables SSL encryption for the LDAP communications.

## Slide 34 - Slide 34

Authentication Setup Wizard

Directory Server

Authentication Agent Hosting:  Enterprise  Cloud

Directory Server Address: 184.170.227.124  
Ensure that your firewall ports are open.

Secure LDAP:  Enabled  
Ensure that the client certificate verification is disabled or trusted on your directory.

Directory Type: Microsoft Active Directory

Port: 3269

Secondary Configuration:  Use a secondary server

Click Next

View Setup Log Cancel ClickBox Back

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

Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM

## Slide notes

Choose your **Directory Type**. For this demonstration we will use **Microsoft Active Directory**.

The **Port** number will be auto-populate depending on the option selected previously. Port **3268** is for communications with Active Directory without SSL and **3269** is used with SSL.

Enable a secondary server to synchronize with two servers that have different sets of user data. Do not use this option to synchronize the service with two directory servers that have duplicate information. We will not use this option for this demo. Click **Next**.

## Slide 35 - Slide 35

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration (which is selected), Activation, and Search. The main area is titled 'Authentication Setup Wizard' and shows the 'Directory Server Authentication' step. It has fields for 'Bind DN' (containing 'TRAINING2\administrator') and 'Bind Password'. A red box highlights the 'Bind DN' field. A callout bubble says 'Specify and administrator account for the Bind DN'. Another callout bubble says 'Click Next' pointing to the 'Next' button in the bottom right. At the bottom are buttons for 'View Setup Log', 'Cancel', 'ClickBox' (which is highlighted with a blue box), and 'Back'.

## Slide notes

Enter the **BIND DN** name of an administrator account that has permission to query the directory server. For example, **TRAINING\Administrator**, then type the admin password and click **Next**.

## Slide 36 - Slide 36

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 window title is 'Authentication Setup Wizard'. It displays 'Detected Settings' with a dropdown for 'Base DN' set to 'DC=training2,DC=safemarch,DC=com'. Below it is a 'Pagination' section with three radio button options: 'Auto (recommended)' (selected), 'Enabled', and 'Disabled'. A callout box points to the 'Auto (recommended)' option with the text 'Click to select Auto (recommended)'. At the bottom, there's a note 'Parameters detected', buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back', and a copyright notice at the bottom left.

## Slide notes

At this point the Wizard has successfully connected to the directory server and pre-populated the **Base DN** field. The **Base DN** specifies the location or branch of the directory where service will begin searching for users, groups, and departments. The service only retrieves objects from the branch that is specified in the **Base DN** field. The information that was auto-populated may be all that you need though you can modify this if needed.

Ensure **Pagination** is set to **Auto** or **Enabled**. This is enabled by default and will allow the server to send user information in 1,000 user blocks. If disabled, the server will only send the first 1,000.

**Slide 37 - Slide 37**

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation, Search, and other less visible options. The main window title is 'Authentication Setup Wizard'. It displays 'Detected Settings' with a dropdown for 'Base DN' set to 'DC=training2,DC=safemarch,DC=com'. Under 'Pagination', it shows 'Auto (recommended)' is selected. A note says 'Detected pagination is Enabled'. At the bottom, there's a message 'Parameters detected' and a row of buttons: 'View Setup Log', 'Cancel', a large central button labeled 'ClickBox' (which is highlighted with a red box), and 'Back'. A speech bubble points to the 'ClickBox' button with the text 'Click Next'. The footer contains copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved.' and 'Version 5.6 | Patients'. It also shows 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

**Slide notes**

**Click Next.**

## Slide 38 - Slide 38

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'. A callout bubble points to the 'Lookup Parameters' section, which contains a dropdown menu set to 'Auto' and a text input field containing 'student@training2.safemarch.com'. Below this is a 'Lookup User Entry' button. The 'Attribute Fields' section includes dropdown menus for User Login ('mail'), 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 are 'View Setup Log', 'Cancel', 'Next', and 'Back' buttons. A watermark 'Safemarch' is visible in the bottom right corner.

## Slide notes

Under **Lookup Parameters** leave the default **Auto** then enter the email address of one of the users in your Active Directory.

## Slide 39 - Slide 39

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'. A message at the top says, 'To discover the LDAP attributes needed by the cloud service, you need to specify a sample username.' Below this is a 'Lookup Parameters' section with a dropdown set to 'Auto' and an input field containing 'student@training2.safemarch.com'. To the right is a 'Lookup Results' section which is currently empty. Below these sections is an 'Attribute Fields' group with several dropdown menus: 'User Login' (mail), 'User Full Name' (displayName), 'User Search Filter' (objectClass), 'Group Name' (cn), 'Membership' (memberOf), and 'Search Filter' (objectClass=group). A large callout box with the text 'Click Lookup User Entry' points to the 'Lookup' button in the 'Lookup Parameters' section. At the bottom of the window are buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The footer of the page includes copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and a timestamp: 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

## Slide notes

Then click **Lookup User Entry** to confirm connectivity.

## Slide 40 - Slide 40

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' with a sub-section 'Verify the Lookup Results'. A large callout box highlights the 'Lookup Results' section. Inside, a red box highlights the list of attributes for the user 'student@training2.safemarch.com': dn, CN=student, OU=DeployZAPPDC=training2, DC=safemarch, DC=com, objectClass: top, objectClass: person, objectClass: organizationalPerson, objectClass: user, cn: student, sn: test, givenName: student, distinguishedName: ...'. Below this is the 'Attribute Fields' section with dropdowns for User Login (mail), 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, it says 'User lookup complete' and has buttons for View Setup Log, Cancel, Next, and Back.

## Slide notes

Confirm the lookup in the **Lookup Results** box.

## Slide 41 - Slide 41

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, 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' and 'Lookup Results'. In 'Lookup Parameters', the dropdown is set to 'Auto' and the input field contains 'student@training2.safemarch.com'. The 'Lookup Results' section shows a list of LDAP attributes for this user, including 'dn', 'cn', 'objectClass', and various 'labeledName' entries. A large callout box with the text 'Review and configure as necessary the Attribute Fields' points to the 'Attribute Fields' section at the bottom. This section contains five dropdown menus: 'User Login' (set to 'mail'), 'Group Name' (set to 'cn'), 'User Full Name' (set to 'displayName'), 'Group Membership' (set to 'memberOf'), 'User Search Filter' (set to '(objectClass=User)'), and 'Group Search Filter' (set to '(objectClass=group)'). The 'User Search Filter' and 'Group Search Filter' dropdowns are highlighted with a red border. At the bottom of the wizard window, it says 'User lookup complete' and includes buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The footer of the page includes copyright information: 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and a timestamp: 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

## Slide notes

In the **Attribute Fields** section specify the names of the attributes that represent the users email address, full name, group, and department, and define filters as well. Zscaler provides granular filters so you can synchronize only the relevant users, groups, and departments to the service. Use the **Group Search Filter** and **User Search Filter** to narrow down the user and group objects that are returned.

Here, you can define a filter string that will locate only the users and groups that you need such as users that belong to specific groups. For username, specify the attribute that represents the user name that users enter when logging into the service. This attribute is used to verify the login name that a user enters when logging in to the Zscaler service for authentication. We will use **mail** for the demo.

## Slide 42 - Slide 42

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a dark sidebar 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input field contains 'student@training2.safemarch.com'. A button labeled 'Lookup User Entry' is present. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various names like student, test, and student. Below these sections is a 'Attribute Fields' group. It includes fields for 'User Login' (set to 'mail'), 'User Full Name' (set to 'displayName'), 'User Search Filter' (set to '(objectClass=)', and 'Department Membership' (set to 'department'). To the right of these fields are 'Group Name' (set to 'cn'), 'Group Membership' (set to 'memberOf'), and 'Group Search Filter' (set to '(objectClass=group)'). A large callout box with the text 'Click in the User Login field' points to the 'User Login' dropdown. At the bottom of the wizard window, there are buttons for 'Skip Logon', 'Cancel', 'Next', and 'Back'. The status bar at the bottom of the screen shows 'User lookup complete', 'Weblog Time: 11/12/2018 6:16:56 PM', and 'Last Updated: 11/12/2018 6:17:13 PM'.

## Slide notes

**Slide 43 - Slide 43**

The screenshot shows the 'Authentication Setup Wizard' window. In the 'Lookup Parameters' section, 'Auto' is selected and 'student@training2.safemarch.com' is entered. Below it is a 'Lookup User Entry' button. To the right, the 'Lookup Results' pane displays the following LDAP entry details:

```
dn : CN=student,OU=DeployZAPPDC=training2,DC=safemarch,DC=com
objectClass : top
objectClass : person
objectClass : organizationalPerson
objectClass : user
cn : student
sn : test
givenName : student
distinguishedName : ...
```

In the 'Attribute Fields' section, there are several dropdown menus and input fields. A 'User Login' dropdown has 'mail' selected. A 'Click Box' is overlaid on the 'User Full Name' dropdown, which also contains 'mail'. Other fields include 'User Search Filter' (usePrincipalName) and 'Department Membership' (sAMAccountName). To the right, 'Group Name' is set to 'cn', 'Group Membership' to 'memberOf', and 'Group Search Filter' to '(objectClass=group)'. A large 'Click Email' button is overlaid on the 'User lookup complete' message at the bottom.

At the bottom of the wizard window are buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The status bar at the bottom of the screen shows 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

**Slide notes**

## Slide 44 - Slide 44

The screenshot shows the 'Authentication Setup Wizard' interface. On the left, a vertical sidebar contains 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input field contains 'student@training2.safemarch.com'. A button labeled 'Lookup User Entry' is below it. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various person-related fields. Below these sections is 'Attribute Fields'. This section includes dropdowns for 'User Login' (set to 'mail'), 'User Full Name' (set to 'displayName', with a callout box pointing here), 'Group Name' (set to 'cn'), 'Group Membership' (set to 'memberOf'), 'User Search Filter' (set to '(objectClass=person)'), 'Group Search Filter' (set to '(objectClass=group)'), and 'Department Membership' (set to 'department'). At the bottom of the wizard are buttons for 'Up Log', 'Cancel', 'Next', and 'Back'. A watermark 'Zscaler' is visible in the bottom right corner.

## Slide notes

For **User Full Name** specify the attribute that represents user names. For example: **cn** or **displayName**.

**Slide 45 - Slide 45**

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a dark sidebar 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and contains the value 'student@training2.safemarch.com'. A button labeled 'Lookup User Entry' is present. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various names like student, test, givenName, and distinguishedName. Below these sections is 'Attribute Fields' where 'User Login' is set to 'mail' and 'User Full Name' is set to 'displayName'. A 'Click Box' is overlaid on the 'displayName' field. To the right, 'Group Name' is set to 'cn', 'Group Membership' is set to 'memberOf', and 'Group Search Filter' is set to '(objectClass=group)'. A 'Click displayName' callout box points to the 'displayName' field in the 'User Full Name' section. At the bottom are buttons for 'setup Log', 'Cancel', 'Next', and 'Back'.

**Slide notes**

## Slide 46 - Slide 46

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 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input contains 'student@training2.safemarch.com'. A button labeled 'Lookup User Entry' is present. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and sn. Below these sections is 'Attribute Fields' with fields for User Login (mail), User Full Name (displayName), Group Name (cn), Group Membership (memberOf), User Search Filter (objectClass), and Group Search Filter ((objectClass=group)). A callout box with the text 'Click in the User Search Filter field' points to the 'User Search Filter' dropdown, which contains '(objectClass=Click Box)'. At the bottom right are 'Cancel', 'Next', and 'Back' buttons.

## Slide notes

Use the **User Search Filter** to narrow down the user objects that the service returns after the synchronization. You can enter a filter string to locate specific users only, such as users who belong to a specific group. For example, enter **objectClass=person** to narrow down the data to persons and not computers. In our case we will set it to **User**.

## Slide 47 - Slide 47

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 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input field contains 'student@training2.safemarch.com'. A button labeled 'Lookup User Entry' is present. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various names like student, test, and givenName. Below these sections is 'Attribute Fields' with fields for User Login (mail), User Full Name (displayName), User Search Filter (objectClass=User), Group Name (cn), Group Membership (memberOf), and Group Search Filter (objectClass=group). A tooltip 'Click Box' points to the 'User Search Filter' dropdown, which is currently expanded to show '(objectClass=User)'. At the bottom right are 'Next' and 'Back' buttons.

Authentication Setup Wizard

Lookup Parameters

Lookup Results

Attribute Fields

User Login: mail

User Full Name: displayName

User Search Filter: **(objectClass=User)**

Group Name: cn

Group Membership: memberOf

Group Search Filter: (objectClass=group)

Click Box

Next Back

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

Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM

## Slide notes

## Slide 48 - Slide 48

The screenshot shows the 'Authentication Setup Wizard' interface. On the left, a vertical sidebar contains icons for Dashboard, Analytics, Policy, Administration, Activation, and Search. The main window displays the 'Authentication Setup Wizard' dialog box. In the 'Lookup Parameters' section, 'Auto' is selected and 'student@training2.safemarch.com' is entered. The 'Lookup Results' section shows LDAP attributes for this user. In the 'Attribute Fields' section, several fields are configured: 'User Login' is set to 'mail', 'Group Name' is 'cn', 'User Full Name' is 'displayName', 'Group Membership' is 'memberOf', 'User Search Filter' is '(objectClass=User)', and 'Group Search Filter' is '(objectClass=group)'. The 'Department Membership' field is highlighted with a red box and a callout bubble containing the text 'Click in the Department Membership field'. At the bottom right of the dialog are 'Next' and 'Back' buttons.

## Slide notes

The **Department Membership** field is used to populate the **Department** field in the reports produced by the Zscaler service. You can specify any attribute that identifies the information that should appear in the **Department** field. For example, you can use **department** or **ou**.

**Slide 49 - Slide 49**

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 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input field contains 'student@training2.safemarch.com'. A 'Lookup User Entry' button is below. To the right is a scrollable list of LDAP attributes with their values. In 'Attribute Fields', several dropdowns are shown: 'User Login' (mail), 'Group Name' (cn), 'User Full Name' (displayName), 'Group Membership' (memberOf), 'User Search Filter' (objectClass=User), 'Group Search Filter' ((objectClass=group)), and 'Department Membership' (department). A callout box with the text 'Click department' points to the 'department' dropdown. At the bottom are 'Cancel', 'Next', and 'Back' buttons.

**Slide notes**

## Slide 50 - Slide 50

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 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input contains 'student@training2.safemarch.com'. A 'Lookup User Entry' button is below. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and sn. Below these sections is 'Attribute Fields' with fields for User Login ('mail'), User Full Name ('displayName'), User Search Filter ('(objectClass=User)'), and Department Membership ('department'). To the right of these fields is a 'Group Name' dropdown with 'cn' selected. A callout box with the text 'Click in the Department Membership field' points to the 'Group Name' dropdown. At the bottom are 'View Setup Log', 'Cancel', and 'Next Step' buttons.

## Slide notes

For **Group Name**, specify the attribute that represents group names. Select **cn**.

## Slide 51 - Slide 51

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 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' and 'Lookup Results'. In 'Lookup Parameters', the dropdown is set to 'Auto' and the input field contains 'student@training2.safemarch.com'. A 'Lookup User Entry' button is present. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various names like student, test, givenName, and distinguishedName. Below these sections is 'Attribute Fields' where various fields like User Login, User Full Name, User Search Filter, Department Membership, Group Name, Group Membership, and Group Search Filter are mapped. A callout box points to the 'cn' entry in the 'Group Name' dropdown with the instruction 'Click cn'. At the bottom are 'View Setup Log' and 'Cancel' buttons.

## Slide notes

## Slide 52 - Slide 52

The screenshot shows the 'Authentication Setup Wizard' interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main window displays the 'Authentication Setup Wizard' dialog. In the 'Lookup Parameters' section, 'Auto' is selected and 'student@training2.safemarch.com' is entered. The 'Lookup Results' pane shows LDAP attributes for this user. In the 'Attribute Fields' section, several fields are configured: User Login (mail), User Full Name (displayName), User Search Filter (objectClass=User), and Department Membership (department). The 'Group Membership' field is highlighted with a red box and a callout bubble containing the text 'Click in the Group Membership field'. At the bottom of the dialog are 'View Setup Log' and 'Cancel' buttons.

## Slide notes

For **Group Membership**, specify the attribute that identifies the group membership. For example, **memberOf**.

**Slide 53 - Slide 53**

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 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input field contains 'student@training2.safemarch.com'. A 'Lookup User Entry' button is below. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various name, sn, givenName, and distinguishedName entries. Below these sections is 'Attribute Fields'. It includes fields for 'User Login' (set to 'mail'), 'User Full Name' (set to 'displayName'), 'User Search Filter' (set to '(objectClass=User)'), and 'Department Membership' (set to 'department'). To the right of these fields are 'Group Name' (set to 'cn'), 'Group Membership' (set to 'memberOf'), and 'Group Search Filter' (set to 'memberOf'). A callout bubble points to the 'memberOf' dropdown with the text 'Click memberOf'. At the bottom are 'View Setup Log' and 'Cancel' buttons.

**Slide notes**

## Slide 54 - Slide 54

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 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input contains 'student@training2.safemarch.com'. A 'Lookup User Entry' button is below. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various names like student, test, givenName, and distinguishedName. Below these sections is 'Attribute Fields' with dropdowns for User Login ('mail'), User Full Name ('displayName'), User Search Filter ('(objectClass=User)'), Group Name ('cn'), Group Membership ('memberOf'), and Group Search Filter ('(objectClass=Click-Box)'). A callout box with the text 'Click in the Group Search Filter field' points to the 'Group Search Filter' dropdown. At the bottom are 'View Setup Log' and 'Cancel' buttons.

## Slide notes

Use the **Group Search Filter** to narrow down the group objects that the service returns after the synchronization. Define filters to narrow down the results to only the groups to which you want to apply policies.

## Slide 55 - Slide 55

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 window displays the 'Authentication Setup Wizard' dialog box. In the 'Lookup Parameters' section, 'Auto' is selected and 'student@training2.safemarch.com' is entered. Below it is a 'Lookup User Entry' button. To the right, the 'Lookup Results' pane shows detailed LDAP attributes for the user: dn, cn, objectClass, and various person-related attributes like top, person, organizationalPerson, user, student, test, student, givenName, and distinguishedName. Under 'Attribute Fields', there are dropdown menus for User Login (set to mail), Group Name (set to cn), User Full Name (set to displayName), Group Membership (set to memberOf), User Search Filter (set to (objectClass=User)), Group Search Filter (set to (objectClass=group)), and Department Membership (set to department). A callout box points to the 'Group Search Filter' dropdown with the text 'Click (objectClass=group)'. At the bottom of the dialog are 'View Setup Log' and 'Cancel' buttons.

## Slide notes

## Slide 56 - Slide 56

The screenshot shows the 'Authentication Setup Wizard' interface. On the left is a dark sidebar 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' and 'Lookup Results'. In 'Lookup Parameters', a dropdown is set to 'Auto' and a text input field contains 'student@training2.safemarch.com'. A 'Lookup User Entry' button is below. In 'Lookup Results', a list of LDAP attributes is shown, including dn, cn, objectClass, and various names like student, test, and student. Below these sections is 'Attribute Fields' with dropdowns for User Login ('mail'), 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 are buttons for 'View Setup Log', 'Cancel', 'ClickBox' (which is highlighted with a red box), and 'Back'.

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

Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM

## Slide notes

Click Next.

**Slide 57 - Slide 57**

The screenshot shows the 'Authentication Setup Wizard' interface. At the top, it displays 'Synchronization Complete' with an elapsed time of '00:00:02'. Below this is a table titled 'Synchronization Results' showing the count of users, groups, and departments added, modified, removed, and total before and after synchronization.

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

A callout bubble points to the 'Click Next' button at the bottom right of the wizard window. The bottom bar includes buttons for 'View Setup Log', 'Cancel', 'ClickBox' (which is highlighted with a red box), and 'Back'.

Left sidebar navigation icons include: Dashboard, Analytics, Policy, Administration, Activation, Search, and other unlabelled icons.

Bottom footer: Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients | Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM

**Slide notes**

You should see the Synchronization process and **Synchronization Results**. Click **Next**.

**Slide 58 - Slide 58**

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 titled 'Authentication Parameters' with three fields: 'User Authentication Filter' set to '(objectClass=User)', 'Test User Login' set to 'student@training2.safemarch.com', and 'Test User Password' set to '\*\*\*\*\*'. Below the form is a 'Check Authentication' button. At the bottom of the window are buttons for 'View Setup Log', 'Cancel', 'Next', and 'Back'. The footer of the page includes copyright information ('Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients'), a timestamp ('Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'), and a Zscaler logo.

**Slide notes**

Now you can test an individual's credentials to confirm that the Zscaler service is able to talk to AD and validate a user's password. Type a user's name and password.

## Slide 59 - Slide 59

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 'Administration' icon is highlighted in blue. The main window title is 'Authentication Setup Wizard'. It contains fields for 'User Authentication Filter' (set to '(objectClass=User)'), 'Test User Login' (set to 'student@training2.safemarch.com'), and 'Test User Password' (set to '\*\*\*\*\*'). Below these fields is a checkbox labeled 'Click Box'. A callout box with a grey border and white text 'Click Check Authentication' has an arrow pointing to the 'Click Box' checkbox. At the bottom of the window are buttons for 'View Setup Log', 'Cancel', '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' on the left and 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM' on the right.

## Slide notes

And click **Check Authentication**.

**Slide 60 - Slide 60**

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 'Administration' icon is highlighted in blue. The main window title is 'Authentication Setup Wizard'. It contains an 'Authentication Parameters' section 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 '\*\*\*\*\*'). Below these fields is a 'Check Authentication' button. At the bottom of the window, there are buttons for 'View Setup Log', 'Cancel', 'ClickBox' (which is highlighted with a red box), and 'Back'. A callout bubble points to the 'ClickBox' button with the text 'Click Next'. Another callout bubble points to the 'ClickBox' button with the text 'Verify that authentication was successful'. The status message 'Authentication for Primary Directory successful' is displayed at the bottom of the window.

**Slide notes**

You should see **Authentication Successful** at the bottom of the window. Click **Next**.

## Slide 61 - Slide 61

The screenshot shows the Zscaler interface with a sidebar containing icons for Dashboard, Analytics, Policy, Administration, Activation, Search, and other management functions. The main window displays the 'Authentication Setup Wizard' with the title 'Wizard Complete'. It informs the user that authentication configuration, directory synchronization, and authentication verification are complete. A warning message states that all existing user authentication configuration will be overwritten with the settings selected using this wizard. At the bottom, there are buttons for 'View Setup Log', 'Cancel', 'ClickBox' (which is highlighted with a red box), and 'Back'. A callout bubble points to the 'ClickBox' button with the instruction 'Click Finish'.

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

Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM

## Slide notes

Click **Finish**.

## Slide 62 - Slide 62

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 has tabs for 'AUTHENTICATION PROFILE' and 'AUTHENTICATION BRIDGES', with 'AUTHENTICATION PROFILE' selected. Under 'AUTHENTICATION PROFILE', there's a 'Directory Type' section with 'Hosted DB', 'Active Directory' (which is checked), 'OpenLDAP', 'Setup Wizard', and 'Advanced Configuration'. Below that is an 'Authentication Frequency' dropdown with 'Only Once' and 'Click Box' options. A callout box with a grey background and a blue border highlights the 'Click Box' option. Other sections include 'DIRECTORY SYNCHRONIZATION' (Last Synchronization Time: Monday, November 12, 2018 6:45:45 PM, Sync Now button) and 'KERBEROS AUTHENTICATION' (Enable Kerberos checkbox, which is unchecked). At the bottom are 'Save' and 'Cancel' buttons, and a refresh icon.

## Slide notes

Next, set the desired authentication frequency for the user. For the purpose of this demo we will select **Daily**.

## Slide 63 - Slide 63

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', the 'Directory Type' is set to 'Active Directory'. The 'Authentication Frequency' dropdown is open, showing options: 'Only Once' (selected), 'Daily', 'Once Per Session', 'Custom', and 'Disabled'. A large 'Click Daily' button is overlaid on the 'Only Once' option. Other sections include 'DIRECTORY SYNCHRONIZATION' (Last Synchronization Time: Monday, November 12, 2018 6:45:45 PM, Sync Now button) and 'KERBEROS AUTHENTICATION' (Enable Kerberos checkbox). At the bottom are 'Save' and 'Cancel' buttons, and a refresh icon.

## Slide notes

## Slide 64 - Slide 64

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 (with a red '1' notification), Activation, and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', it shows 'Directory Type' with 'Active Directory' selected (indicated by a blue border). Below that is 'Authentication Frequency' set to 'Daily'. The 'Authentication Type' section has two options: 'Click Boxed' (selected, highlighted with a blue box and a callout 'Click Forms Based') and 'SAML'. Under 'DIRECTORY SYNCHRONIZATION', it shows 'Last Synchronization Time' as 'Monday, November 12, 2018 6:45:45 PM' with a 'Sync Now' button. In the 'KERBEROS AUTHENTICATION' section, there's a 'Enable Kerberos' toggle switch that is off (red). At the bottom, there are 'Save' and 'Cancel' buttons, and a small circular icon with a 'K'.

## Slide notes

For **Authentication Type** set this to **Form Based**.

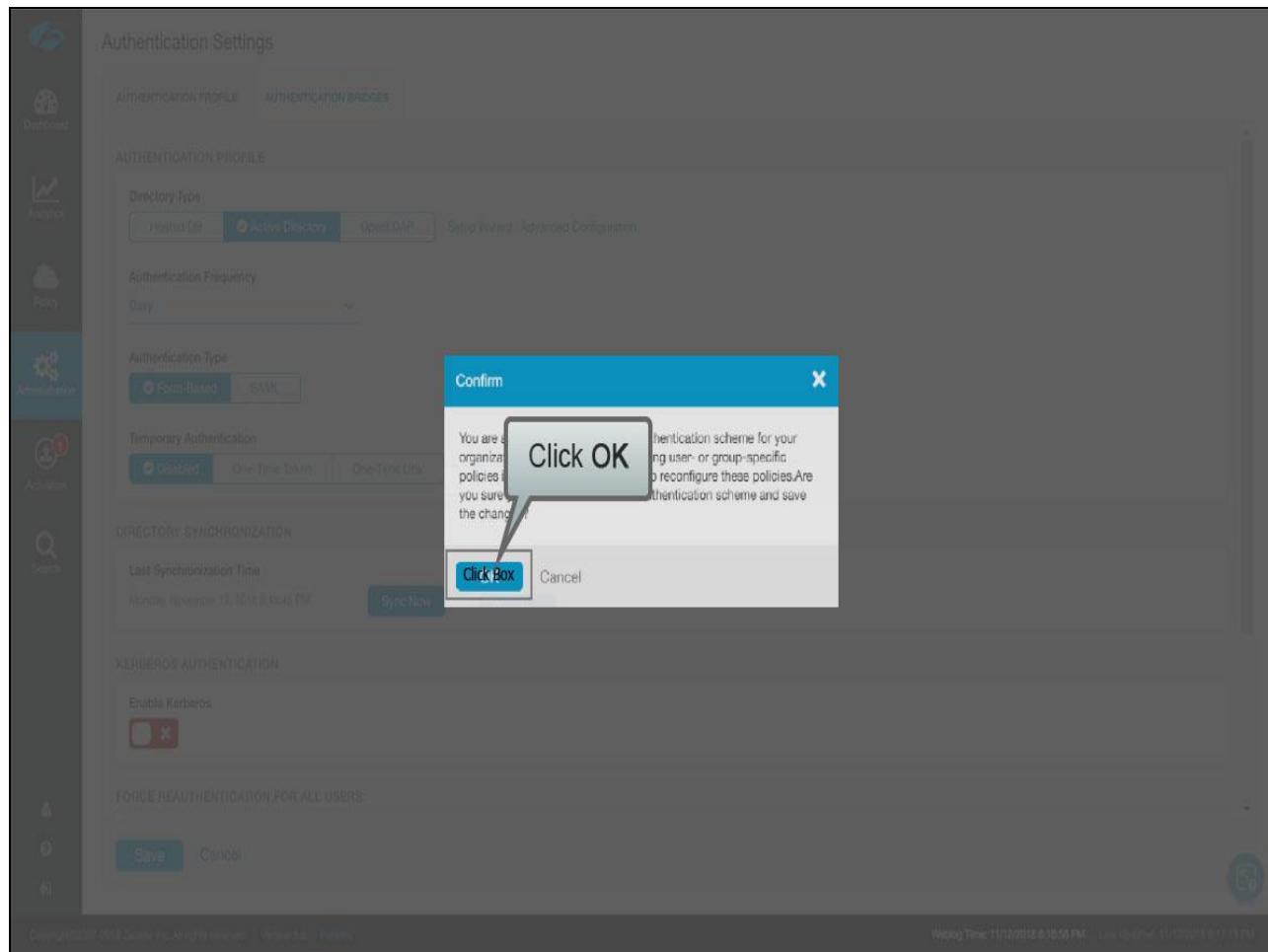
## Slide 65 - Slide 65

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Policy, Administration, Activation, and Search. The main content area is titled 'AUTHENTICATION PROFILE' and shows the 'Active Directory' tab selected under 'Directory Type'. Other tabs include 'Hosted DB', 'OpenLDAP', 'Setup Wizard', and 'Advanced Configuration'. Under 'Authentication Frequency', 'Daily' is selected. Under 'Authentication Type', 'Form-Based' is checked. Under 'Temporary Authentication', 'Disabled' is selected. In the 'DIRECTORY SYNCHRONIZATION' section, the last synchronization time is listed as 'Monday, November 12, 2018 6:45:45 PM' with a 'Sync Now' button. The 'KERBEROS AUTHENTICATION' section contains an 'Enable' checkbox (which is checked) and a 'Click Save' callout bubble pointing to it. Below this is a 'FORCE REAUTHENTICATION FOR ALL USERS' section with a 'Click Box' button and a 'Cancel' button. At the bottom of the page, copyright information reads 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and a footer note says 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

## Slide notes

Then click **Save**.

## Slide 66 - Slide 66



## Slide notes

Then click **OK** on the dialog box warning you that you are about to change the authentication scheme for the entire company.

## Slide 67 - Slide 67

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). Under 'TEMPORARY AUTHENTICATION', 'Disabled' is selected. Under 'DIRECTORY SYNCHRONIZATION', the 'Last Synchronization Time' is 'Monday, November 12, 2018 6:45:45 PM' with a 'Sync Now' button. Under 'KERBEROS AUTHENTICATION', 'Enable Kerberos' is turned off. At the bottom are 'Save' and 'Cancel' buttons, and a blue circular icon.

## Slide notes

## Slide 68 - Slide 68

The screenshot shows the 'Authentication Settings' page in the Zscaler interface. The left sidebar includes icons for Dashboard, Analytics, Policy, Administration, Click Activation (with a red notification dot), and Search. The main content area has tabs for 'AUTHENTICATION PROFILE' and 'AUTHENTICATION BRIDGES', with 'AUTHENTICATION PROFILE' selected. Under 'AUTHENTICATION PROFILE', 'Active Directory' is chosen from a list (Hosted DB, Active Directory, OpenLDAP). Other settings include 'Authentication Frequency' (Daily), 'Authentication Type' (Form-Based checked, SAML), and 'Temporary Authentication' (Disabled checked, One-Time Token, One-Time Link). A 'Click Activation' button is visible. Below these are sections for 'KERBEROS AUTHENTICATION' (Enable Kerberos checked) and 'FORCE REAUTHENTICATION FOR ALL USERS' (Save, Cancel buttons). The bottom footer includes copyright information (Copyright 2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients) and a timestamp (Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM).

## Slide notes

Then **Activate** your changes.

**Slide 69 - Slide 69**

The screenshot shows the Zscaler Activation interface. On the left is a dark sidebar with icons for Dashboard, Analytics, Policy, Administration, Activation (with a red notification dot), and Search. The main area has a light gray background. At the top, it says "MY ACTIVATION STATUS" and "Editing". Below that is a section titled "CURRENTLY EDITING (1)" with the email "admin@training.zadematch.com". Under "QUEUED ACTIVATIONS (0)", it says "None". There are three tabs: "Directory" (selected), "OpenLDAP", "Setup Wizard", and "Advanced Configuration". A checkbox labeled "Force Activate" is checked, and a blue button labeled "Click Box" is highlighted with a white arrow pointing to it from a callout bubble containing the text "Click Activate". Below this is a "Sync Now" button. At the bottom, there's a "Sync All Users" button 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: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM".

**Slide notes**

## Slide 70 - Slide 70

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 has tabs for 'AUTHENTICATION PROFILE' (selected) and 'AUTHENTICATION BRIDGES'. Under 'AUTHENTICATION PROFILE', 'Active Directory' is selected from a list (Hosted DB, Active Directory, OpenLDAP). Other sections include 'Authentication Frequency' (Daily), 'Authentication Type' (Form-Based selected), 'Temporary Authentication' (Disabled selected), 'DIRECTORY SYNCHRONIZATION' (Last Synchronization Time: Monday, November 12, 2018 6:45:45 PM, Sync Now button), 'KERBEROS AUTHENTICATION' (Enable Kerberos checkbox is unchecked), and 'FORCE REAUTHENTICATION FOR ALL USERS' (Save and Cancel buttons). A 'Activation Completed!' message is at the top right.

## Slide notes

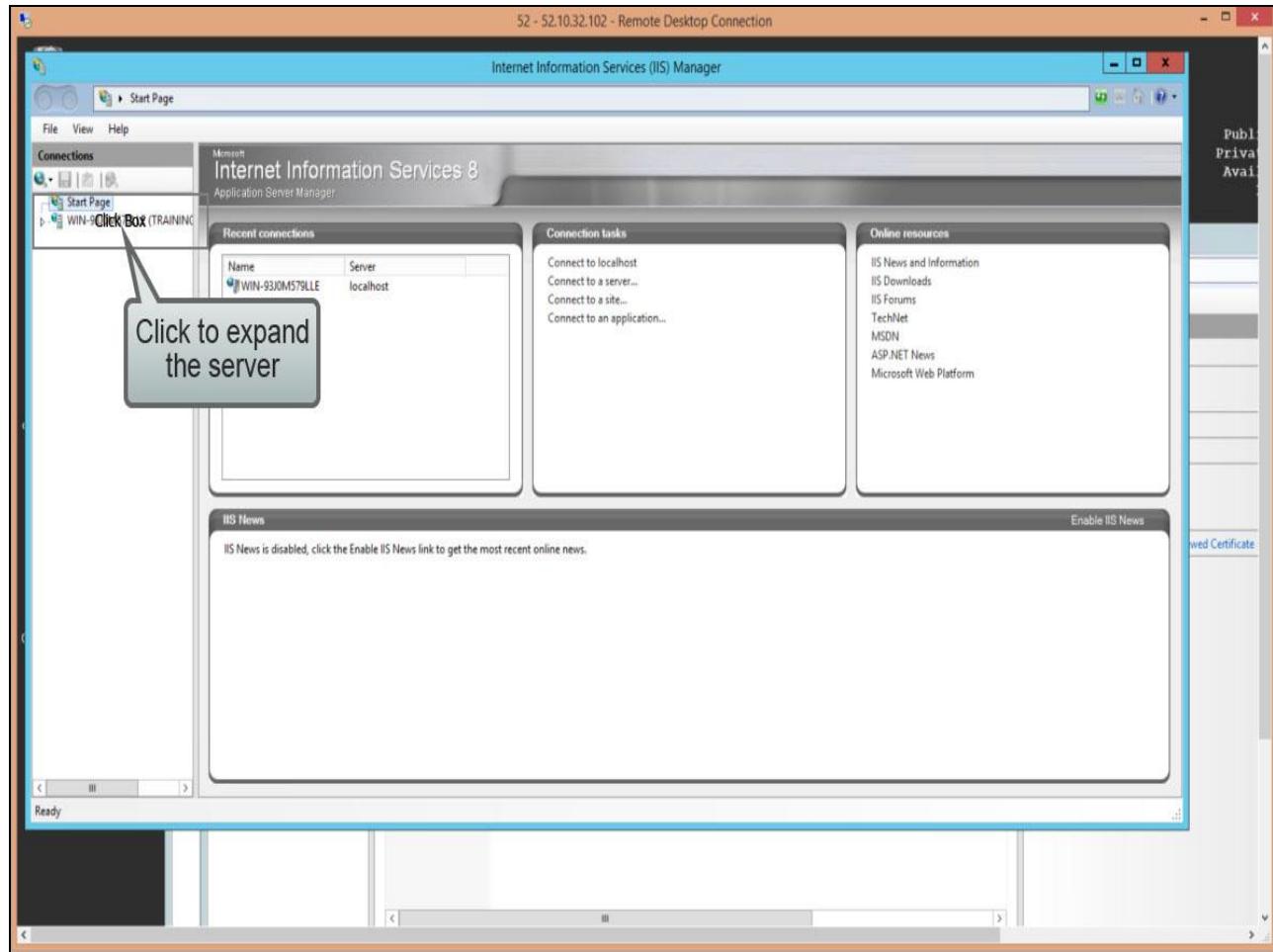
## Slide 71 - Slide 71

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', 'Last Synchronization Time' is 'Monday, November 12, 2018 6:45:45 PM' with a 'Sync Now' button. Under 'KERBEROS AUTHENTICATION', 'Enable Kerberos' is turned off. Under 'FORCE REAUTHENTICATION FOR ALL USERS', there are 'Save' and 'Cancel' buttons. A blue circular icon with a white 'K' is in the bottom right. At the bottom, it says 'Copyright©2007-2018 Zscaler Inc. All rights reserved. | Version 5.6 | Patients' and 'Weblog Time: 11/12/2018 6:16:56 PM | Last Updated: 11/12/2018 6:17:13 PM'.

## Slide notes

We have now completed the configuration of the Zscaler service. Now let's take a quick look at configuring Active Directory.

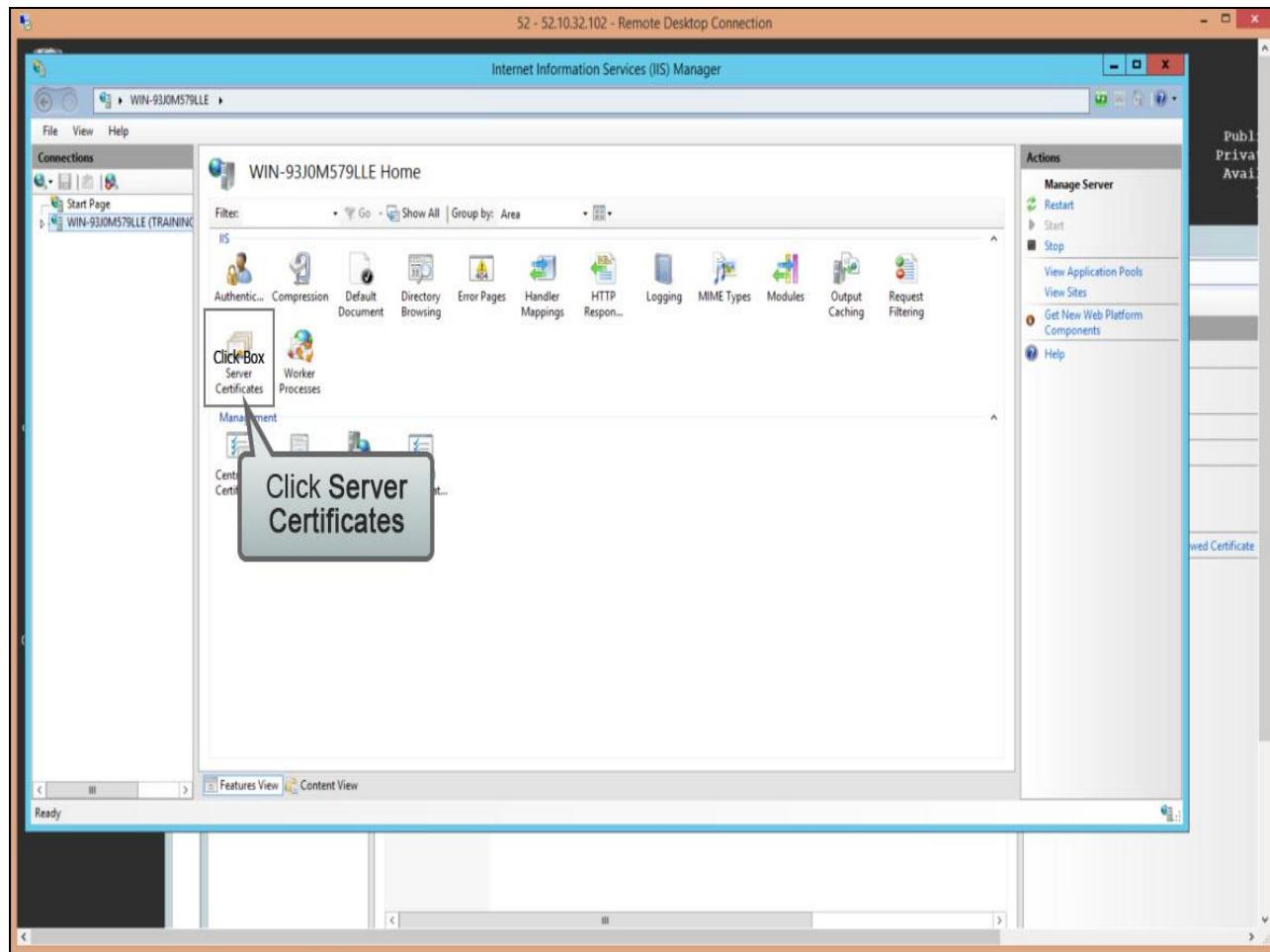
## Slide 72 - Slide 72



## Slide notes

As we have enabled Secure LDAP in the Zscaler Service we need to configure Active Directory with either a self-signed SSL certificate or use one from a 3rd party CA such as Verisign or GoDaddy. For the purpose of this demo I pre-installed a self-signed certificate such that when we went through the Zscaler Setup Wizard synchronization would pass. Let's take a quick look at IIS, specifically the IIS Manager in Windows server and create a self-signed certificate. Start by clicking on the server name on the left.

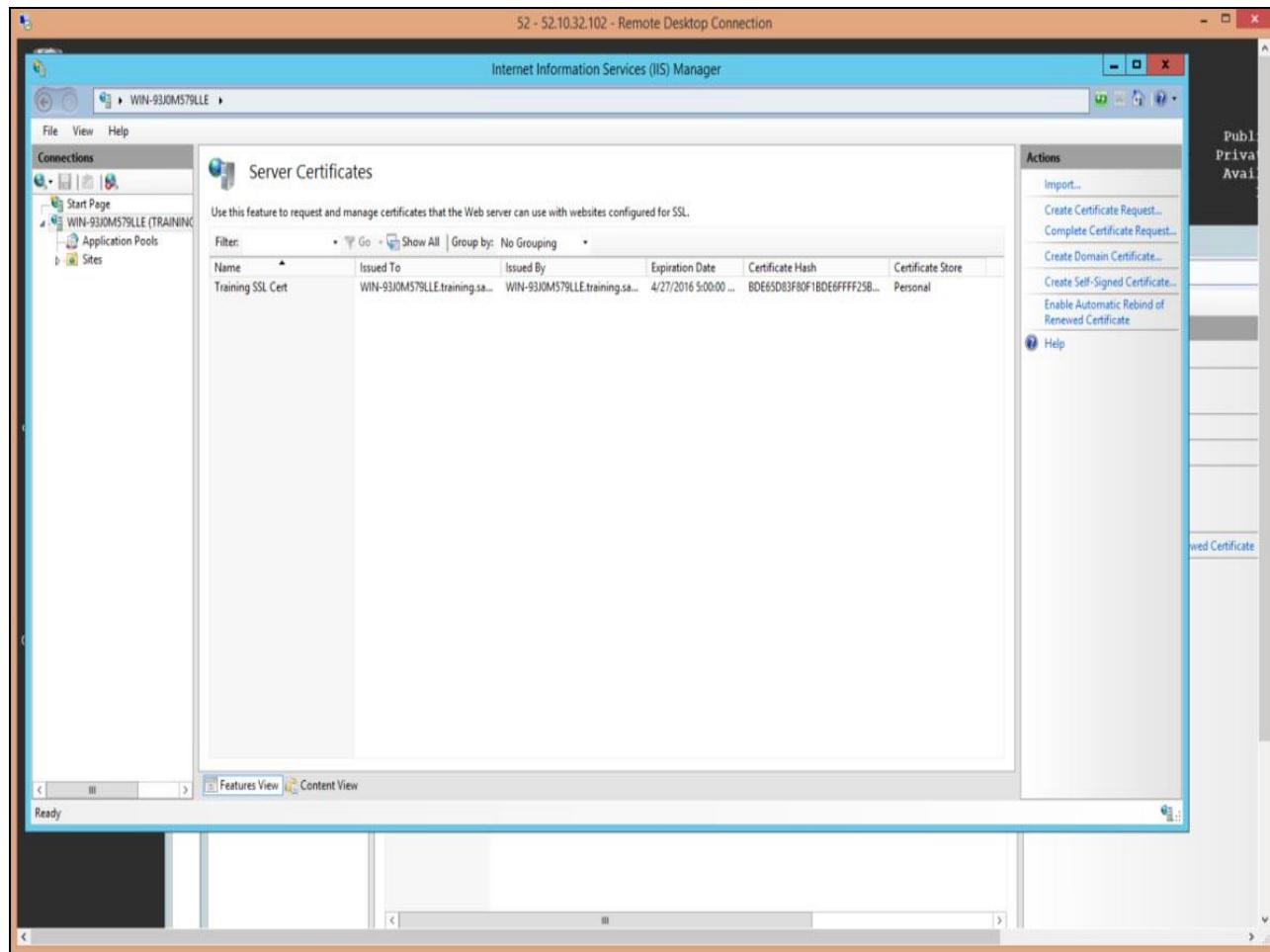
## Slide 73 - Slide 73



## Slide notes

Click on **Server Certificates**.

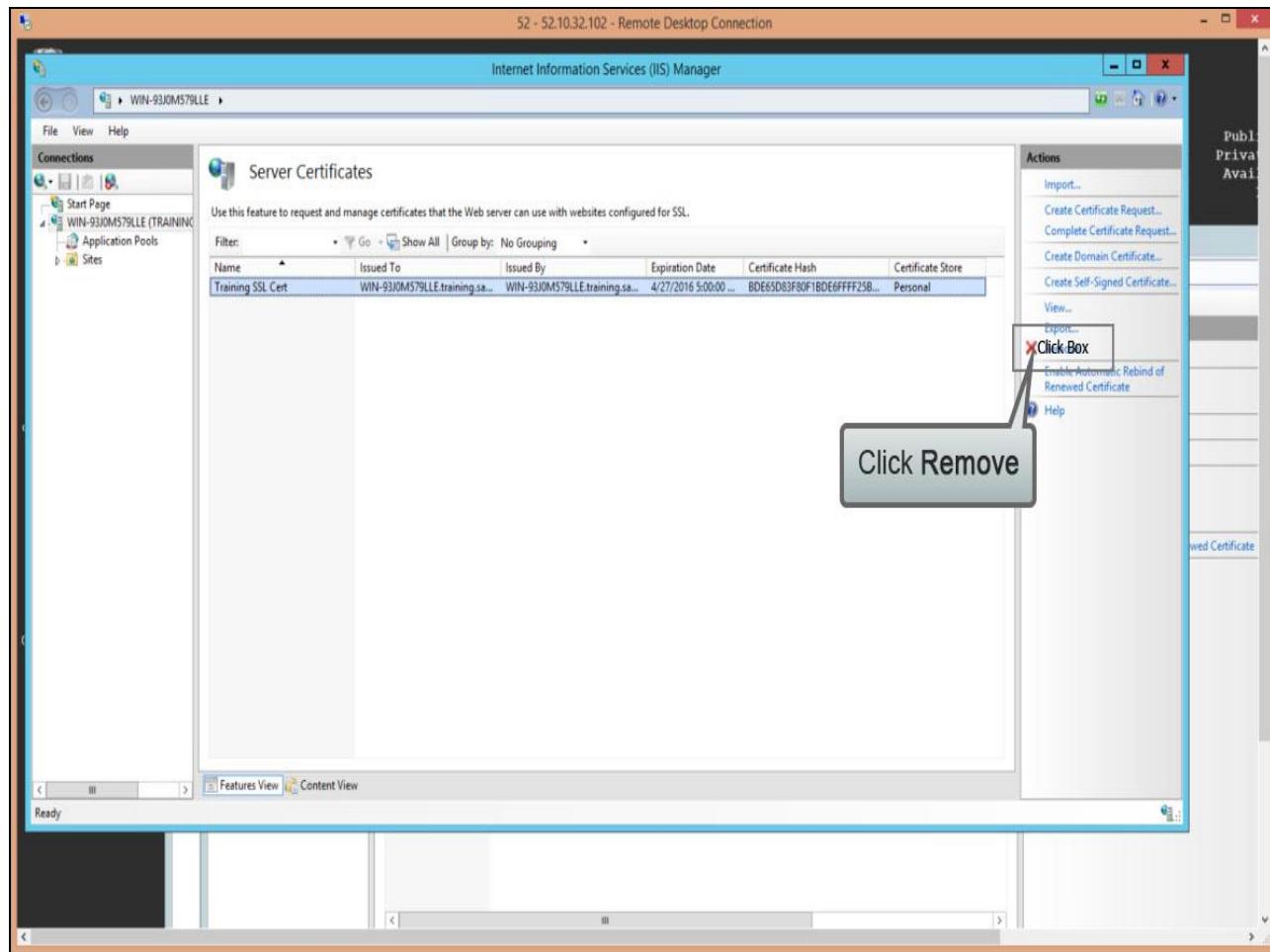
## Slide 74 - Slide 74



## Slide notes

You can see that I already have a server certificate, ...

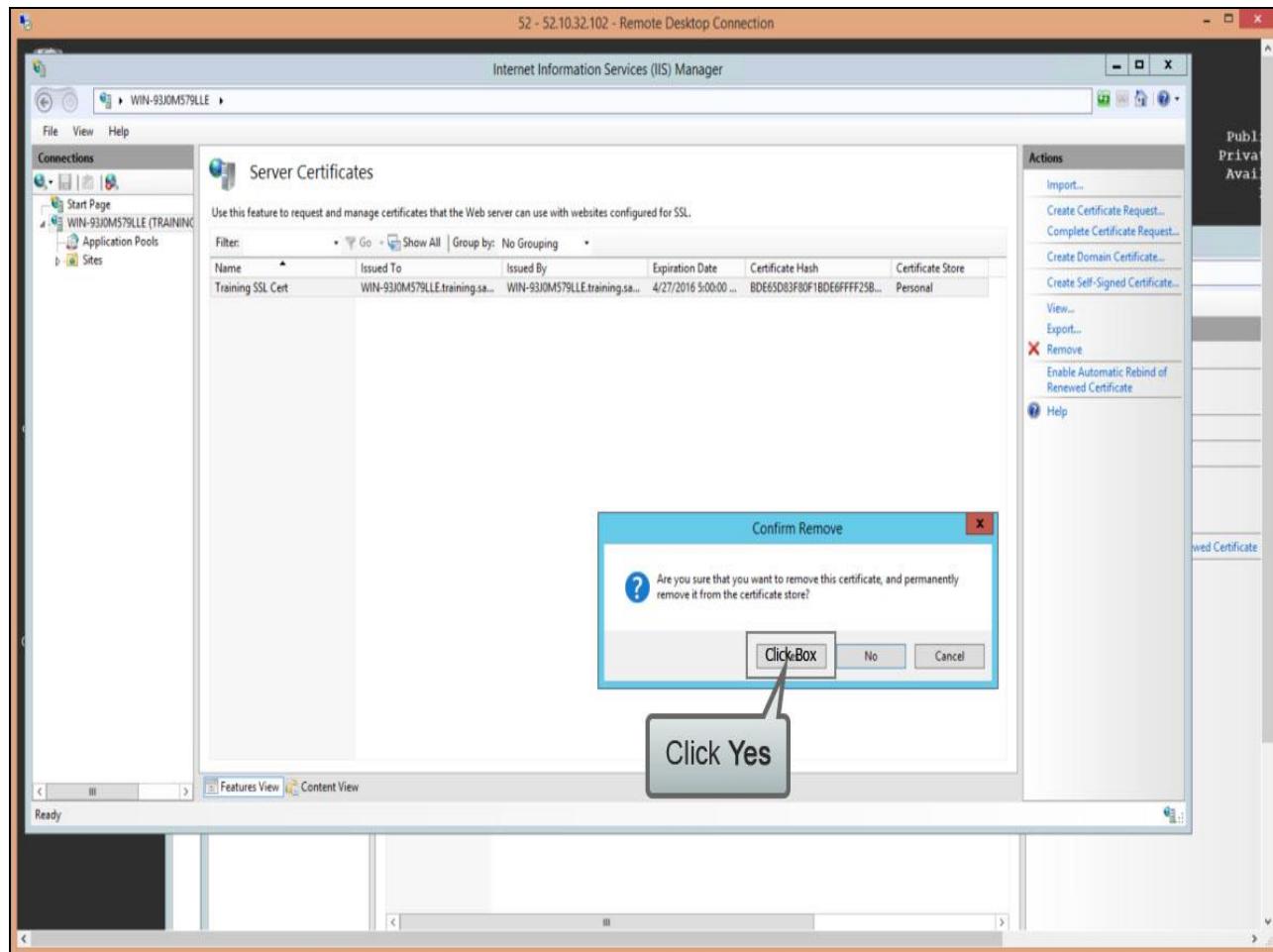
## Slide 75 - Slide 75



## Slide notes

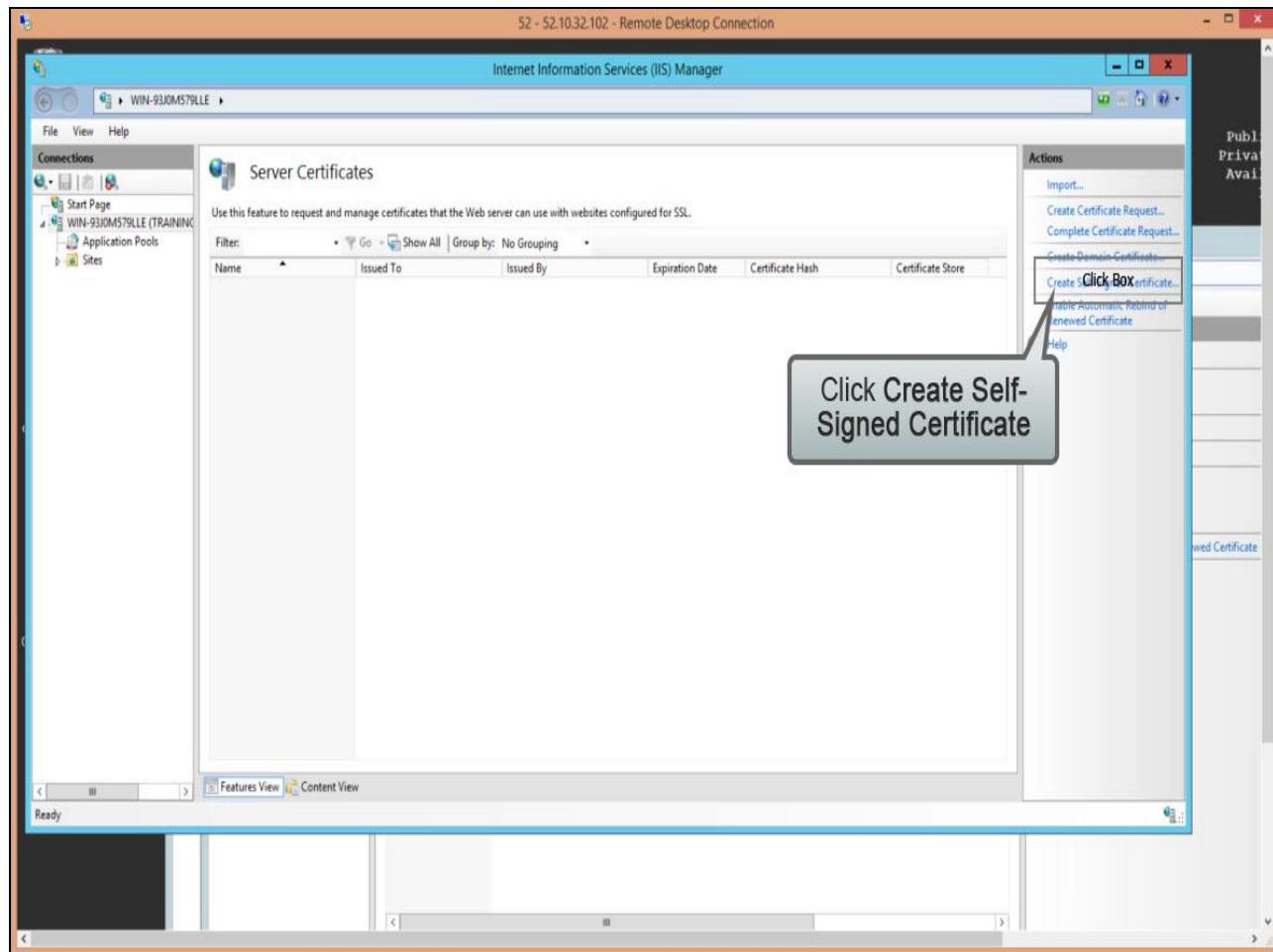
...installed but let's go ahead and remove that.

## Slide 76 - Slide 76



## Slide notes

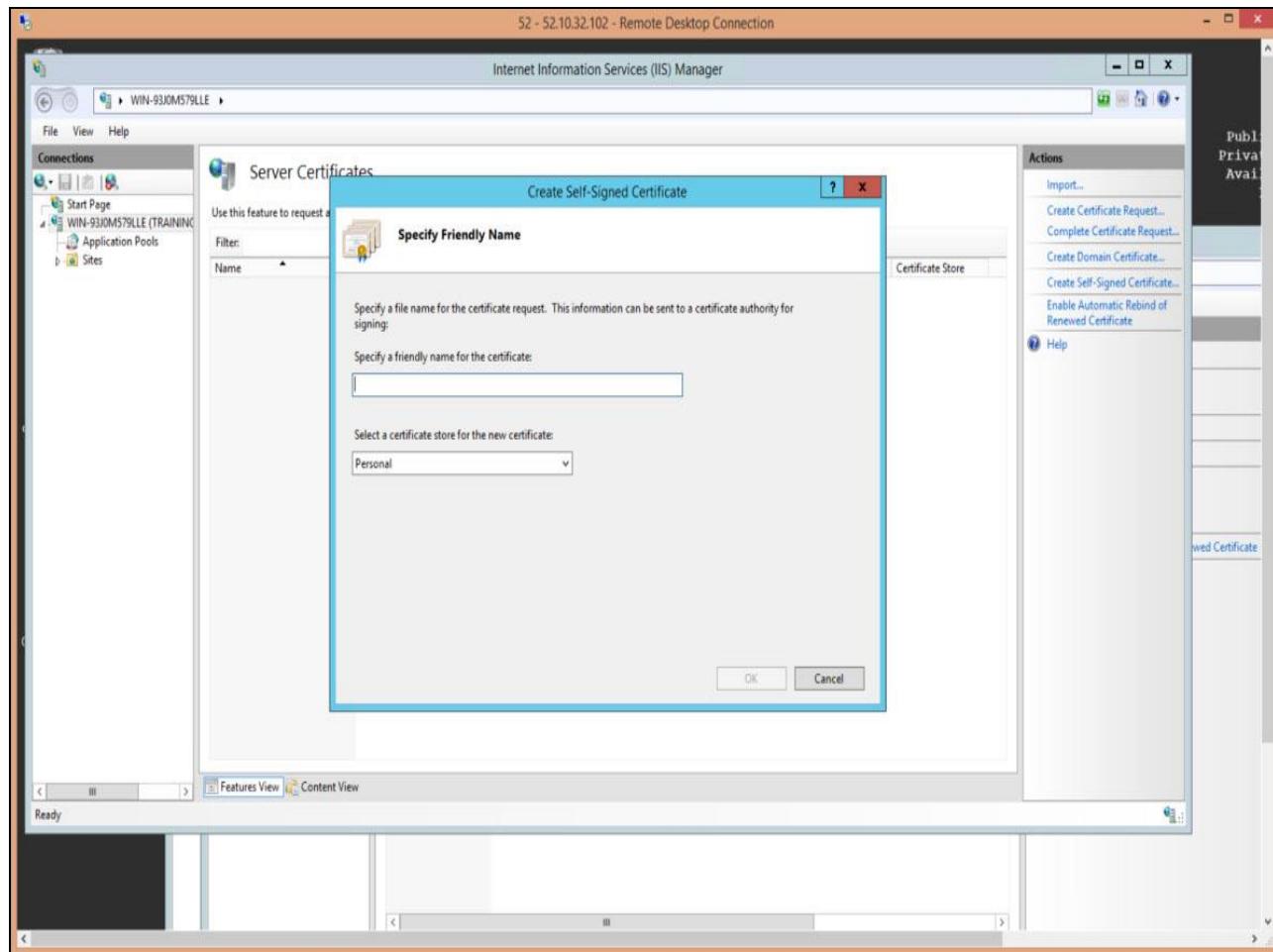
## Slide 77 - Slide 77



## Slide notes

And let's create a self-signed certificate.

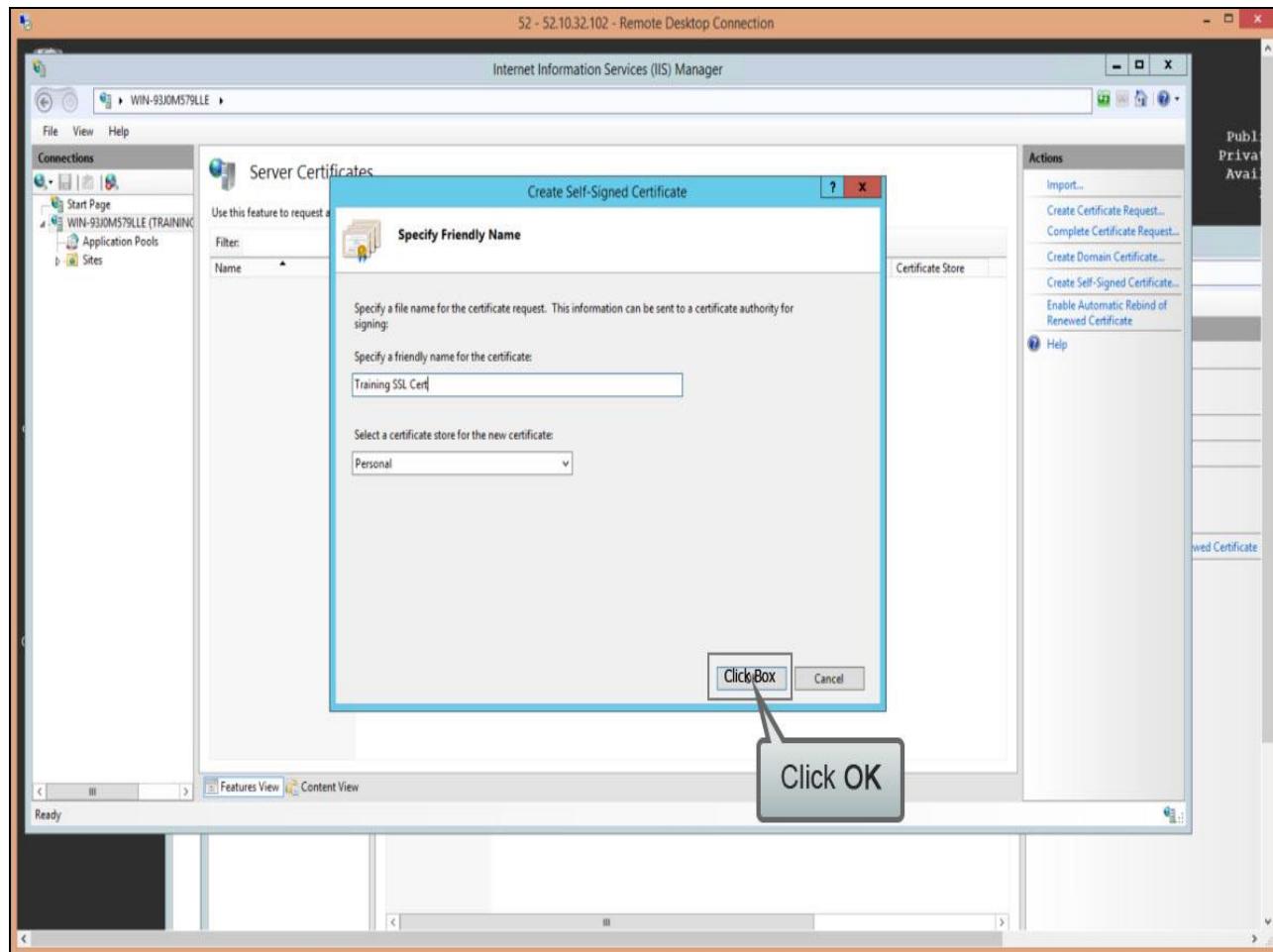
## Slide 78 - Slide 78



## Slide notes

Provide a friendly name for the certificate.

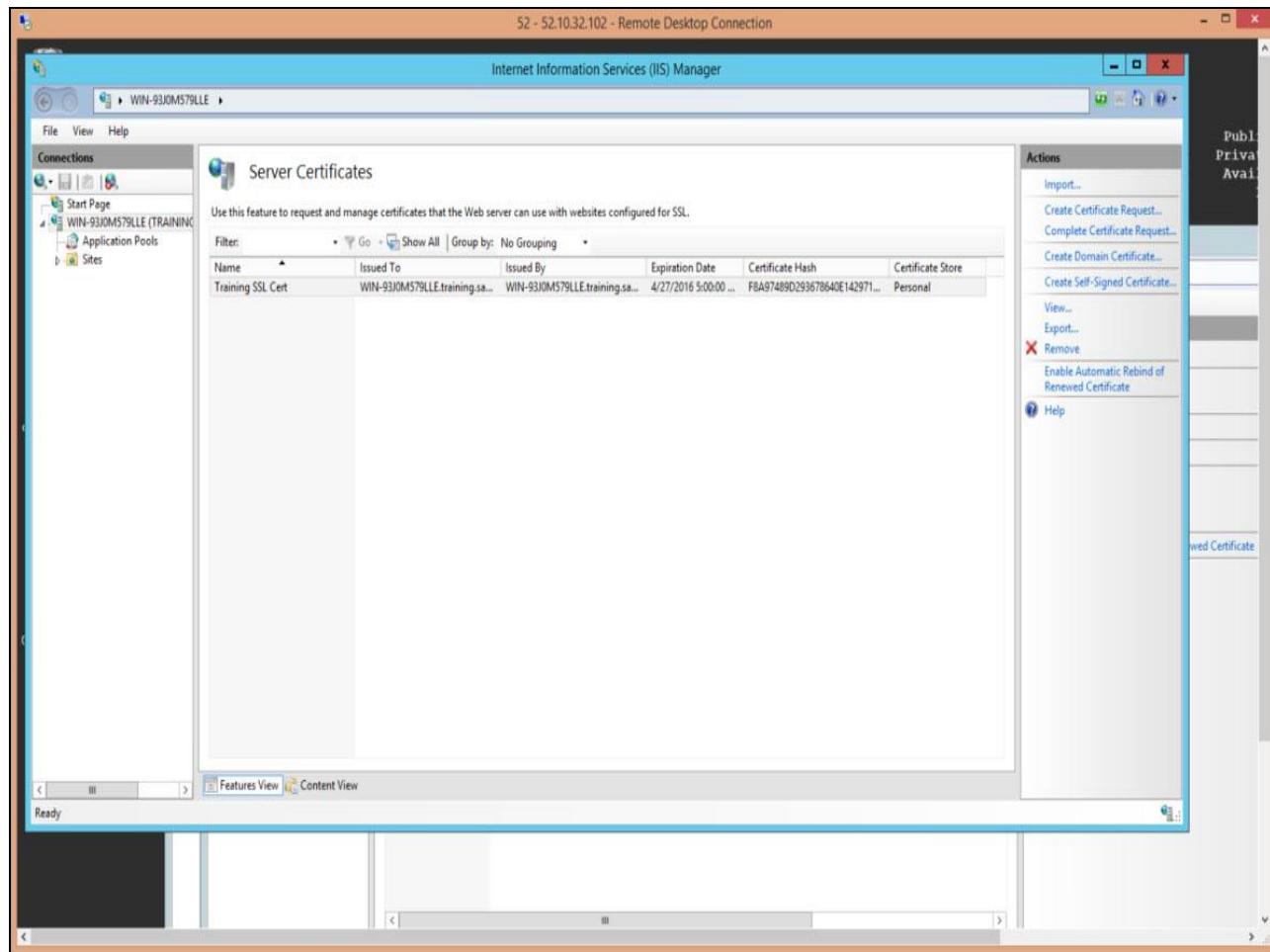
## Slide 79 - Slide 79



## Slide notes

And hit **OK**.

## Slide 80 - Slide 80



## Slide notes

And that concludes the demonstration of configuring Active Directory with the Zscaler service.

**Slide 81 - Thank You and Quiz**



# Thank You and Quiz

**Slide notes**

This completes the LDAP module. We hope this module has been useful to you and thank you for your time.

What will follow is a short quiz to test your knowledge of the material presented during this module. You may take the quiz as many times as necessary to pass.