

Slide 1 - Zscaler Private Access



# Zscaler Private Access

## Authentication – SCIM With Azure AD

©2020 Zscaler, Inc. All rights reserved.

### Slide notes

Welcome to this training module on integrating ZPA with Azure AD for System for Cross-domain Identity Management functionality (SCIM).

## Slide 2 - Navigating the eLearning Module

The screenshot shows the Zscaler eLearning module dashboard. At the top right is the Zscaler logo. Below it, the title "Navigating the eLearning Module" is displayed. On the left, there's a sidebar with "Dashboard", "Diagnostics", "Live Logs", "Administration", and a "Search" bar. The main area has tabs for "Applications", "Users", and "Health". A date range selector shows "14 Days". Key statistics include "APPLICATIONS ACCESSED" (15), "DISCOVERED APPLICATIONS" (3), "ACCESS POLICY BLOCKS" (0), and "SUCCESSFUL TRANSACTIONS" (884). A large blue callout box highlights the "Exit" button in the top right corner. Another blue callout box points to the "Previous Slide" and "Next Slide" buttons. A third blue callout box points to the "Play/Pause" button. A fourth blue callout box points to the "Progress Bar". A fifth blue callout box points to the "Audio On/Off" and "Closed Captioning" buttons.

## Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play and Pause**, **Previous** and **Next** slide. You can also **Mute** the audio or enable **Closed Captioning** which will cause a transcript of the module to be displayed on the screen. Finally, you can click the X button at the top to exit.

## Slide 3 - Agenda

# Agenda

- SCIM Overview
- Enabling SCIM on Azure AD
- Verifying SCIM Functionality

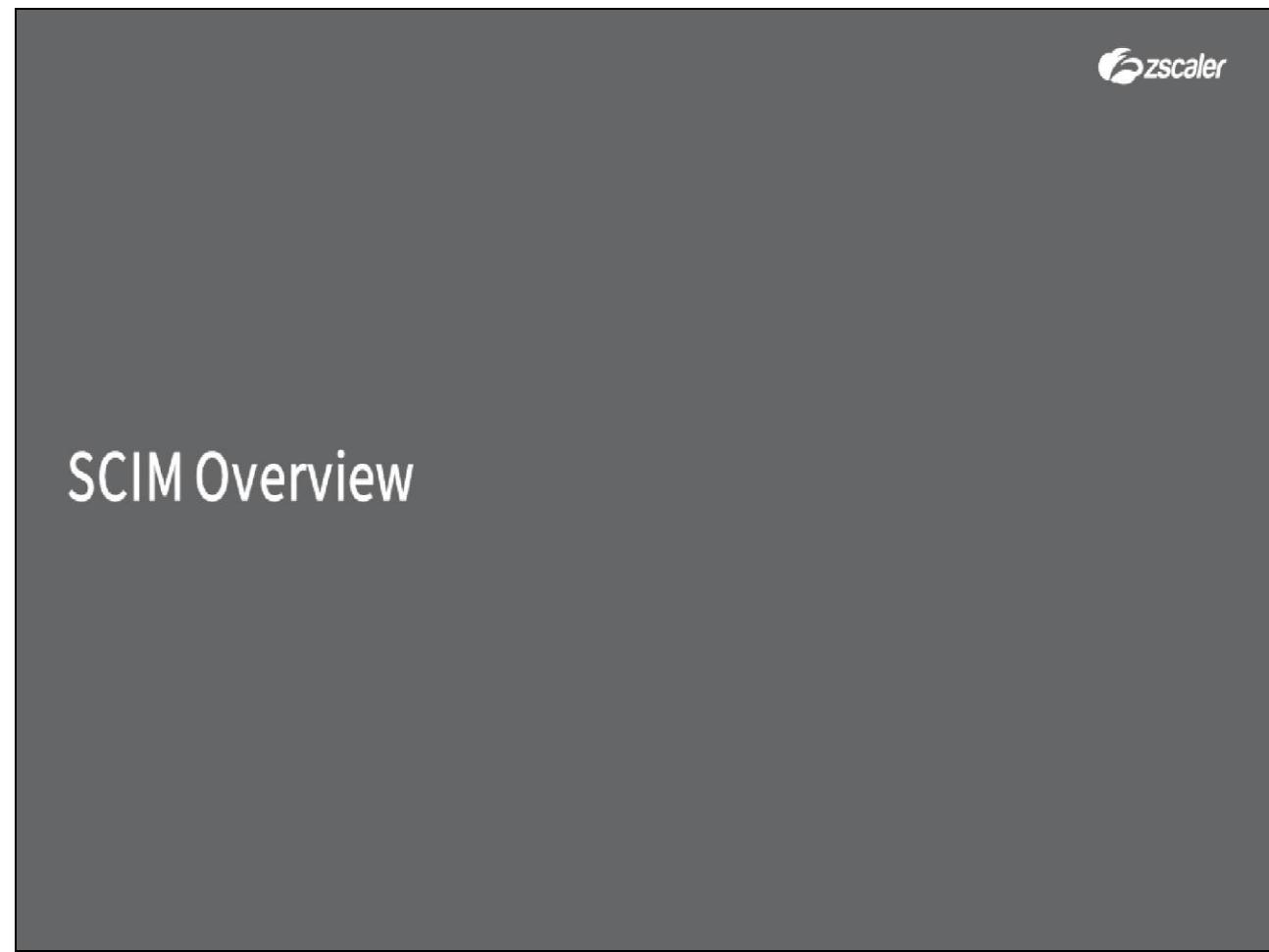


## Slide notes

In this module, we will:

- Have a quick look at what SCIM is and what it can be used for;
- Look at how to enable SCIM in ZPA for use with an Azure AD account;
- And look at how to verify that SCIM is actually working.

Slide 4 - SCIM Overview



**Slide notes**

The first topic that we will cover is an overview of the System for Cross-domain Identity Management (SCIM).

## Slide 5 - What is SCIM?



# What is SCIM?



- System for Cross-domain Identity Management (SCIM)
  - Standard for automating the exchange of user identity information between identity domains
  - Automatic API driven updates to user attributes on a change in the home directory, e.g. automatic update to group memberships, or automatic user removal (to deny service)

### Slide notes

SCIM is a standard for automating the exchange of user identity information between identity domains or IT systems, for example:

- As a company hires or dismisses employees, the user accounts must be created on, or deleted from the company directory server;
- But there may be other directory services where these users also need to be added or removed (e.g. a SAML IdP for Web SSO, Google, Office 365 or Salesforce.com accounts, etc.) – SCIM allows for the automatic exchange of end user information between directory servers.

It may also be used to update a user's details should they move between groups or departments. The major advantage of SCIM is that you only need to manage user accounts in the one place, from there they will be automatically updated wherever else their accounts exist.

The whole idea behind SCIM is to make it fast, cheap, and easy to move users into, out of, and around the cloud.

## Slide 6 - What is SCIM?



## What is SCIM?



- System for Cross-domain Identity Management (SCIM)
  - Standard for automating the exchange of user identity information between identity domains
  - Automatic API driven updates to user attributes on a change in the home directory, e.g. automatic update to group memberships, or automatic user removal (to deny service)

**Resource Model**

- Standard schemas for defining resources, e.g. Users, Groups
- Complex resource types are supported, e.g. with attributes, sub-attributes, multivalued attributes
- Resources are encoded as SCIM objects in JSON

## Slide notes

SCIM 2.0 is built on an object model where a SCIM Resource is the common denominator and all SCIM objects are derived from it. A SCIM **Resource** is a collection of SCIM **Attributes** identified by one or more SCIM **Schemas** (much like an LDAP Entry is a collection of AttributeTypes identified by one or more ObjectClass).

- At a minimum, a SCIM **Attribute** consists of the attribute name and at least one simple or complex value, either of which may be multi-valued.
- For each attribute, a SCIM **Schema** defines the data type, plurality, mutability, and other distinguishing features of the attribute.
- Each SCIM **Resource** is encoded as a JSON object that defines both the type of resource and the attributes it comprises.

## Slide 7 - What is SCIM?



## What is SCIM?



- System for Cross-domain Identity Management (SCIM)
  - Standard for automating the exchange of user identity information between identity domains
  - Automatic API driven updates to user attributes on a change in the home directory, e.g. automatic update to group memberships, or automatic user removal (to deny service)

Resource Model	REST API - Operations
<ul style="list-style-type: none"><li>• Standard schemas for defining resources, e.g. Users, Groups</li><li>• Complex resource types are supported, e.g. with attributes, sub-attributes, multivalued attributes</li><li>• Resources are encoded as SCIM objects in JSON</li></ul>	<ul style="list-style-type: none"><li>• <b>Create:</b> Add a resource (e.g. user, group)</li><li>• <b>Read:</b> Get information about a resource</li><li>• <b>Update:</b> Update the attributes of a resource</li><li>• <b>Delete:</b> Remove a resource</li><li>• <b>SSO:</b> Trigger Create/Update to a 3<sup>rd</sup> party</li><li>• <b>Replace:</b> Change a resource</li><li>• <b>Search:</b> Find a resource</li><li>• <b>Bulk:</b> Operations on multiple resources</li></ul>

## Slide notes

For the manipulation of resources, SCIM provides a REST API with a rich but simple set of operations, which support everything from patching a specific attribute on a specific user, to doing massive bulk updates. The available operations are the traditional CRUD set (Create, Read, Update, Delete), with some important additions:

- **Create** - use a POST operation to add a resource;
- **Read** - use a GET operation to retrieve information about a resource;
- **Update** - use a PATCH operation to change one or more attributes on a resource;
- **Delete** - use a DELETE operation to remove a resource;
- **SSO** - Trigger a Create or Update operation on a 3rd party system;
- **Replace** - Use a PUT operation to change the attributes on a resource;
- **Search** - Use a GET operation to find a specific resource;
- **Bulk** - use POST operations to update multiple resources.

## Slide 8 - ZPA Support for SCIM (Fall 2020)



## ZPA Support for SCIM (September 2020)

Directories Supported



Azure  
Active Directory



Ping  
identity.

PingFederate®

- For the current list of supported IdPs, see the page at:  
<https://help.zscaler.com/zpa/about-scim>
- API Integration required to allow push notifications from these services

### Slide notes

As at the time this module was created (September 2020), the only directories that ZPA integrates with for SCIM functionality are:

- Microsoft's **Azure Active Directory**;
- And the **Pingfederate** product from Ping Identity.

For the current list of supported directory service providers that support SCIM integration, see the page at:  
<https://help.zscaler.com/zpa/about-scim>

The directory services must be provided with the Service Provider URL for the ZPA instance to be updated, and a Secret Key (Bearer Token) to secure their API access. Synchronization is in one direction only; it is a data push from the directory service to ZPA.

## Slide 9 - ZPA Support for SCIM (Fall 2020)

## ZPA Support for SCIM (September 2020)

 zscaler

**Directories Supported**



Azure  
Active Directory



Ping  
identity.

PingFederate®

- For the current list of supported IdPs, see the page at:  
<https://help.zscaler.com/zpa/about-scim>
- API Integration required to allow push notifications from these services

**Operations Supported**

- Add users – As they are assigned to the ZPA SP in the source IdP (individually or as part of a group)
- Delete Users – Remove ZPA access for users that are either removed from the ZPA SP in the source IdP, or are removed from the directory completely

### Slide notes

Again, at the time that this module was created, the only functions supported by ZPA with SCIM are:

- The automated addition of users as they are assigned to the ZPA Service Provider in the source directory product (whether AAD or PingFederate);
- And the automated removal of users if they are removed from the ZPA SP configuration in the source directory, or if they are removed from the directory completely.

## Slide 10 - ZPA Support for SCIM (Fall 2020)



## ZPA Support for SCIM (Fall 2020)

### ZPA User Management

- With SCIM enabled a list of the users assigned to the ZPA SP in the IdP is created in ZPA
- Users can only be managed in the source directory (AAD or Ping Federate)
- The list remains in sync with the source directory (AAD or Ping Federate) as changes are made
- Update interval of 40 Minutes

### Slide notes

Once SCIM has been enabled in ZPA and integrated with the chosen directory, ZPA provides a list of the end user accounts that have been synchronized using SCIM. With SCIM enabled, end user's that are changed in the source directory (whether added or deleted) will automatically be synchronized with ZPA within a reasonable time interval (40 minutes currently). Users can only be managed in the source directory, although those that have been synchronized with ZPA can be viewed in the list in the ZPA Admin Portal. The ZPA list will stay in sync with the source directory, as end users are managed.

The advantage of this is that there is no longer any need to separately manage an end user's access to ZPA, their permissions to use the system will be automatically updated as their account is changed in the source directory. If an end user is terminated and removed from the corporate directory, their access to private applications using ZPA will automatically be removed.

## Slide 11 - ZPA Support for SCIM (Fall 2020)



## ZPA Support for SCIM (Fall 2020)

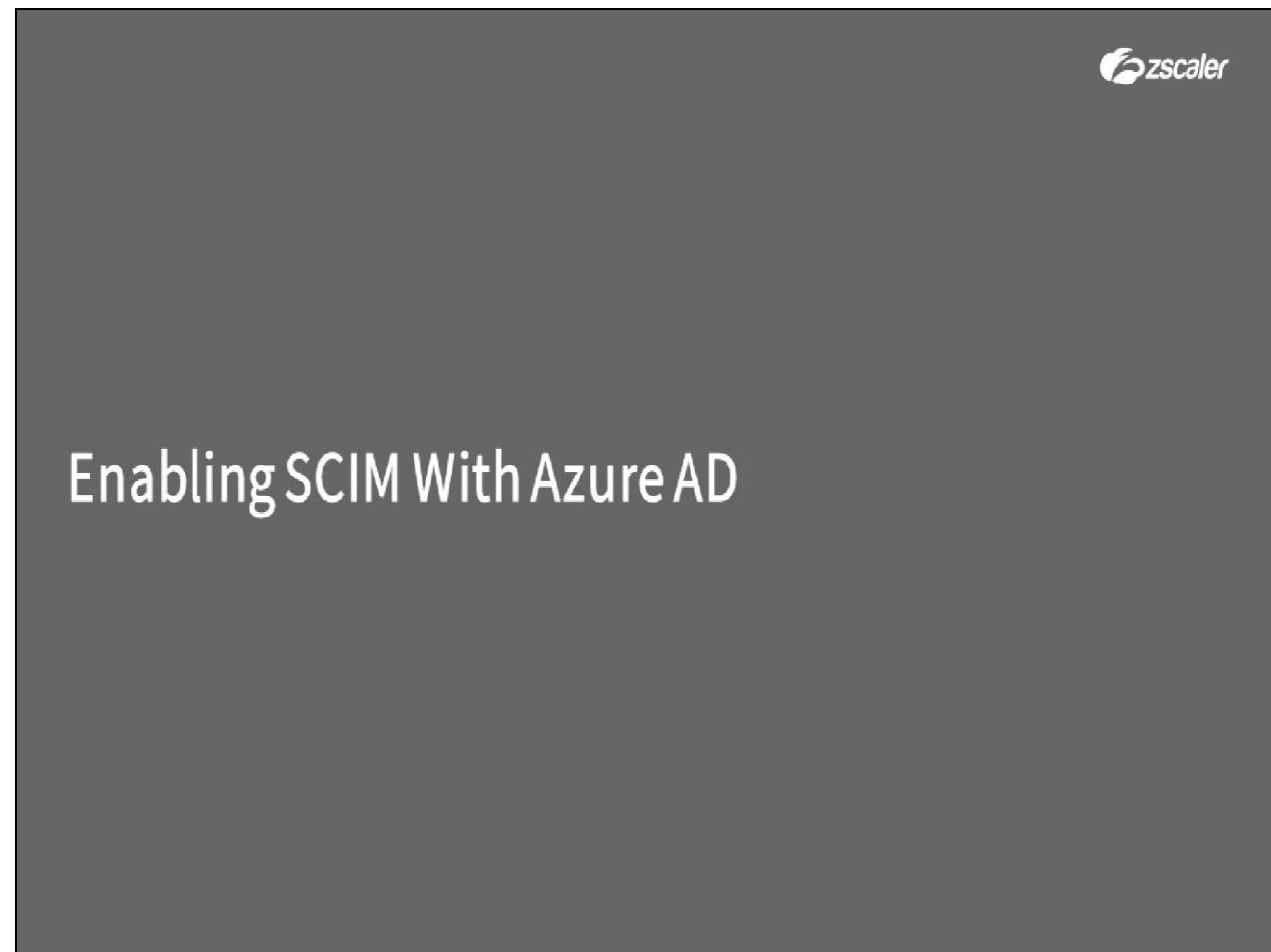
ZPA User Management	User Operations
<ul style="list-style-type: none"><li>With SCIM enabled a list of the users assigned to the ZPA SP in the IdP is created in ZPA</li><li>Users can only be managed in the source directory (AAD or Ping Federate)</li><li>The list remains in sync with the source directory (AAD or Ping Federate) as changes are made</li><li>Update interval of 40 Minutes</li></ul>	<ul style="list-style-type: none"><li>Synchronized happens when:<ol style="list-style-type: none"><li>Users are added/removed to/from a group that is mapped to the ZPA SP in the IdP</li><li>Users are individually assigned or removed from the ZPA SP in the IdP</li><li>Users are removed from the source directory entirely</li></ol></li></ul>

### Slide notes

The operations currently supported are:

- Automatically add or remove users for ZPA access if they are added/removed from a directory group that is assigned to the ZPA SP configuration in the IdP;
- Automatically add or remove users for ZPA access if they are individually assigned to, or removed from the ZPA SP configuration in the IdP;
- Or automatically remove ZPA access for any user removed completely from the source IdP.

## Slide 12 - Enabling SCIM With Azure AD



### Slide notes

The next topic that we will cover is how to enable SCIM with Azure AD.

This section has been created as an interactive demo to give you a feel for the navigation of the ZPA and Azure AD Admin Portals. You will be asked to select the appropriate menu options to navigate the UI. You may also use the **Play** control to proceed to the next step.

## Slide 13 - Slide 13

The screenshot shows the Zscaler Admin Portal dashboard. On the left, there's a sidebar with several menu items: Application Management (Application Segments, Segment Groups, Servers), Authentication (IdP Configuration, Settings), Certificate Management (Browser Access, Certificates), Connector Management (Connectors, Connector Groups, Connector Provisioning Keys), Log Streaming Service (Connector Groups, Log Receivers), and Policy Management (Access Policy, Client Forwarding Policy, Timeout Policy). A callout bubble points to the 'IdP Configuration' link in the Authentication section with the text 'Click IdP Configuration'. The main dashboard area has three cards: 'APPLICATIONS' (13), 'ACCESS POLICY BLOCKS' (13, with a red exclamation mark), and 'SUCCESSFUL TRANSACTIONS' (279, with a green checkmark). Below these is a chart titled 'TOP APPLICATIONS BY BANDWIDTH' showing traffic volumes for shares.patraining.safemarch.com, host-1.patraining.safemarch.com, rdp.patraining.safemarch.com, and intranet.patraining.safemarch.com. At the bottom right is a 'Help' button.

## Slide notes

To enable SCIM functionality on an IdP Configuration in the ZPA Admin Portal, from the **Administration** menu click **IdP Configuration**.

## Slide 14 - Slide 14

The screenshot shows the Zscaler Admin UI interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and other navigation links. The main content area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with the following data:

Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure	✓	https://sts.windows.net/457d09b0-86e3-49d8-9ffd-14e6ec0a12a1/	User	<a href="#">Edit Box</a> <a href="#">X</a>

A callout bubble points to the 'Edit Box' link in the Actions column of the Azure row, containing the text: 'Click to Edit the Azure IdP Configuration'. In the bottom right corner of the main area, there is a 'Help' button.

## Slide notes

Click to **Edit** the Azure IdP Configuration.

## Slide 15 - Slide 15

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal window titled 'Edit IdP Configuration' is open, showing the configuration for the 'Azure' provider. The 'Name' field is set to 'Azure'. Under 'Authentication Domains', there is a dropdown menu with 'patraining26.safermarch.com' listed. The 'SAML ATTRIBUTES' section contains fields for 'IdP Metadata File' (with a 'Select File' button) and 'IdP Certificate' (with a 'Select File' button). The 'Single Sign-On URL' field contains the value 'https://login.microsoftonline.com/457d09b0-86e3-49d8-9ffd-14e6ec0a12a1/saml2'. A large gray box covers the bottom half of the modal window, containing the text 'Scroll down...'. At the bottom of the modal are 'Save' and 'Cancel' buttons, and a 'Help' link is visible on the right.

## Slide notes

Scroll down, ...

## Slide 16 - Slide 16

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. The main panel displays the 'Edit IdP Configuration' dialog for the 'Azure' provider. The configuration includes:

- Single Sign-On URL:** https://login.microsoftonline.com/457d09b0-86e3-49d8-9ffd-14e6ec0a12a1/saml2
- IdP Entity ID:** https://sts.windows.net/457d09b0-86e3-49d8-9ffd-14e6ec0a12a1/
- Status:** Enabled (radio button selected)
- Single Sign-On:** User (radio button selected)
- ZPA (SP) SAML Request:** Signed (radio button selected)
- HTTP-Redirect:** Enabled (radio button selected)
- SCIM Sync:** Enabled (radio button selected)

A gray callout bubble with the text "Click to Enable the SCIM Sync option" points to the "Enabled" radio button under the "SCIM Sync" section. At the bottom of the dialog are "Save" and "Cancel" buttons.

## Slide notes

...and click to enable **SCIM Sync**.

## Slide 17 - Slide 17

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. Under the 'SCIM' section, the 'SCIM Sync' status is set to 'Enabled'. The 'SCIM Service Provider Endpoint URL' field is highlighted with a red box and contains the URL <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>. A callout box with the text 'Click Generate New Token' points to the 'Generate New Token' button below the URL field. The 'Save' and 'Cancel' buttons are also visible at the bottom.

## Slide notes

Once this is enabled, the **SCIM Service Provider Endpoint** URL will be shown. To generate a new secret key for the API integration with Azure AD, click **Generate New Token**.

## Slide 18 - Slide 18

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal dialog titled 'Edit IdP Configuration' is open, specifically for the 'Azure' provider. The dialog contains several configuration sections:

- Status:** Single Sign-On options include 'Enabled' (selected), 'Disabled', 'Admin', 'User' (selected), and 'Both'.
- ZPA (SP) SAML Request:** Options include 'Signed' (selected) and 'Unsigned'.
- HTTP-Redirect:** Options include 'Enabled' and 'Disabled'.
- SCIM:**
  - SCIM Sync:** Options include 'Enabled' (selected) and 'Disabled'.
  - SCIM Service Provider Endpoint:** URL: <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>
  - Bearer Token:** A long token value: qZYRXiFVH08j0lhWY-eXBqJh70FH0DcroXj7cW-7pI4SQuA\_1\_3hmbi79j9xrUGgWQxMj5yDSBlyiFbxA
  - Generate New Token:** A blue button.

At the bottom of the dialog are 'Save' and 'Cancel' buttons, and a 'Help' link on the right.

## Slide notes

Note, this token value will only be displayed the one time, as soon as you save this configuration it will no longer be accessible. You can create a new token of course, but that would then need to be updated in the linked IdP configuration.

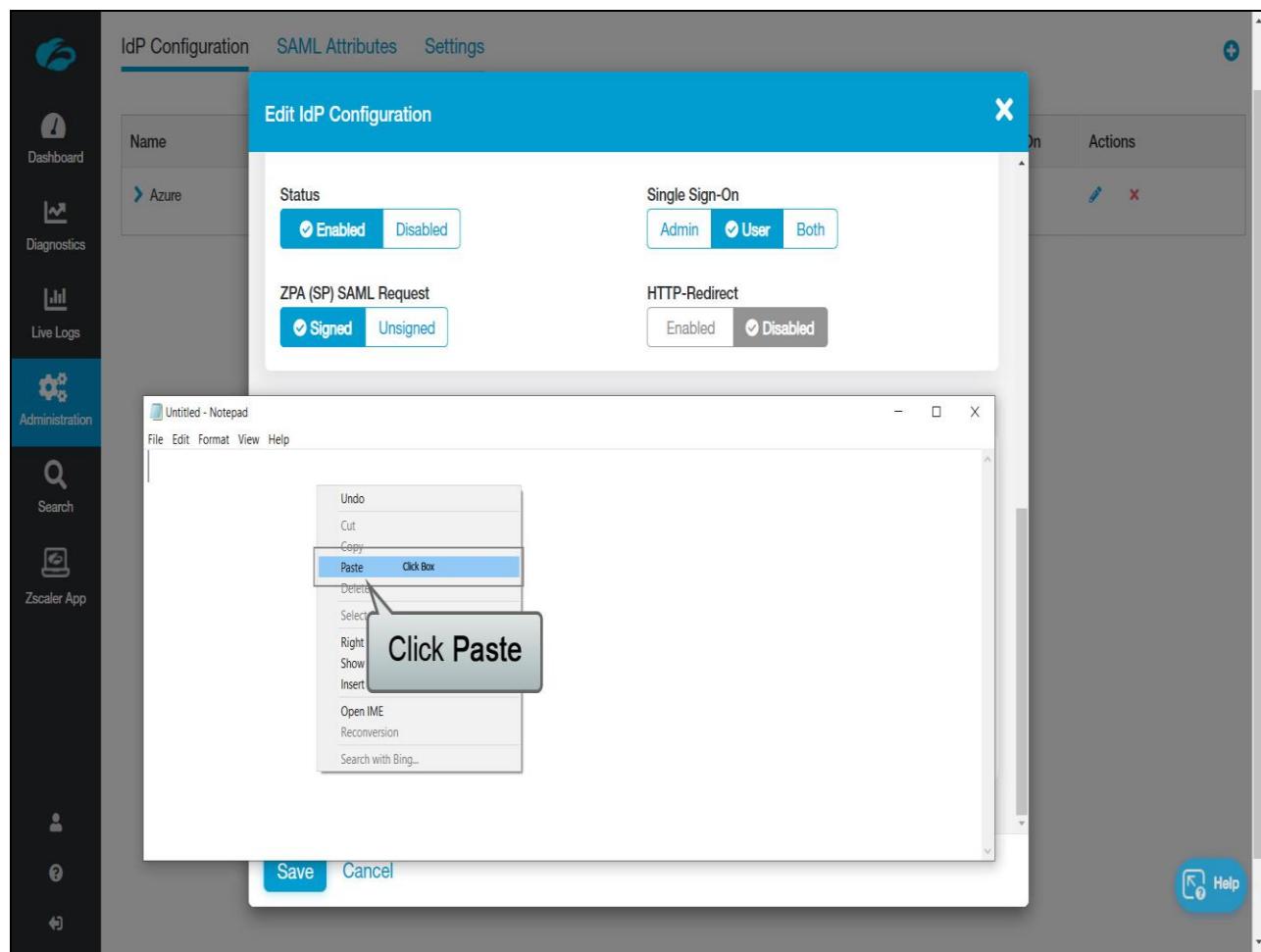
## Slide 19 - Slide 19

The screenshot shows the Zscaler Admin UI with the 'Edit IdP Configuration' dialog open for the 'Azure' provider. The dialog contains sections for 'Status' (Enabled), 'Single Sign-On' (User selected), 'ZPA (SP) SAML Request' (Signed selected), 'HTTP-Redirect' (Disabled), and 'SCIM' (Sync Enabled). In the 'SCIM' section, the 'SCIM Service Provider Endpoint' URL is highlighted and a context menu is open, showing options like 'Copy', 'Go to', 'Print', and 'Inspect'. The 'Copy' option is highlighted with a red box and a tooltip 'Click Copy'.

## Slide notes

Both the **SCIM Service Provider Endpoint** URL and the **Bearer Token** must be transferred to the directory services provider, so highlight the URL, right-click and select **Copy**, ...

## Slide 20 - Slide 20



## Slide notes

...open a text editor (e.g. Notepad on Windows), right-click and select **Paste**.

## Slide 21 - Slide 21

The screenshot shows the Zscaler Admin UI interface. On the left, there's a sidebar with various icons for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. The main area has tabs for IdP Configuration, SAML Attributes, and Settings, with IdP Configuration selected. A modal window titled "Edit IdP Configuration" is open, showing configuration for "Azure". The "Status" section has "Enabled" checked. The "Single Sign-On" section has "User" checked. The "ZPA (SP) SAML Request" section has "Signed" checked. The "HTTP-Redirect" section has "Enabled" checked. Below the modal, a Notepad window is open with the URL <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>. At the bottom of the modal, there are "Save" and "Cancel" buttons.

## Slide notes

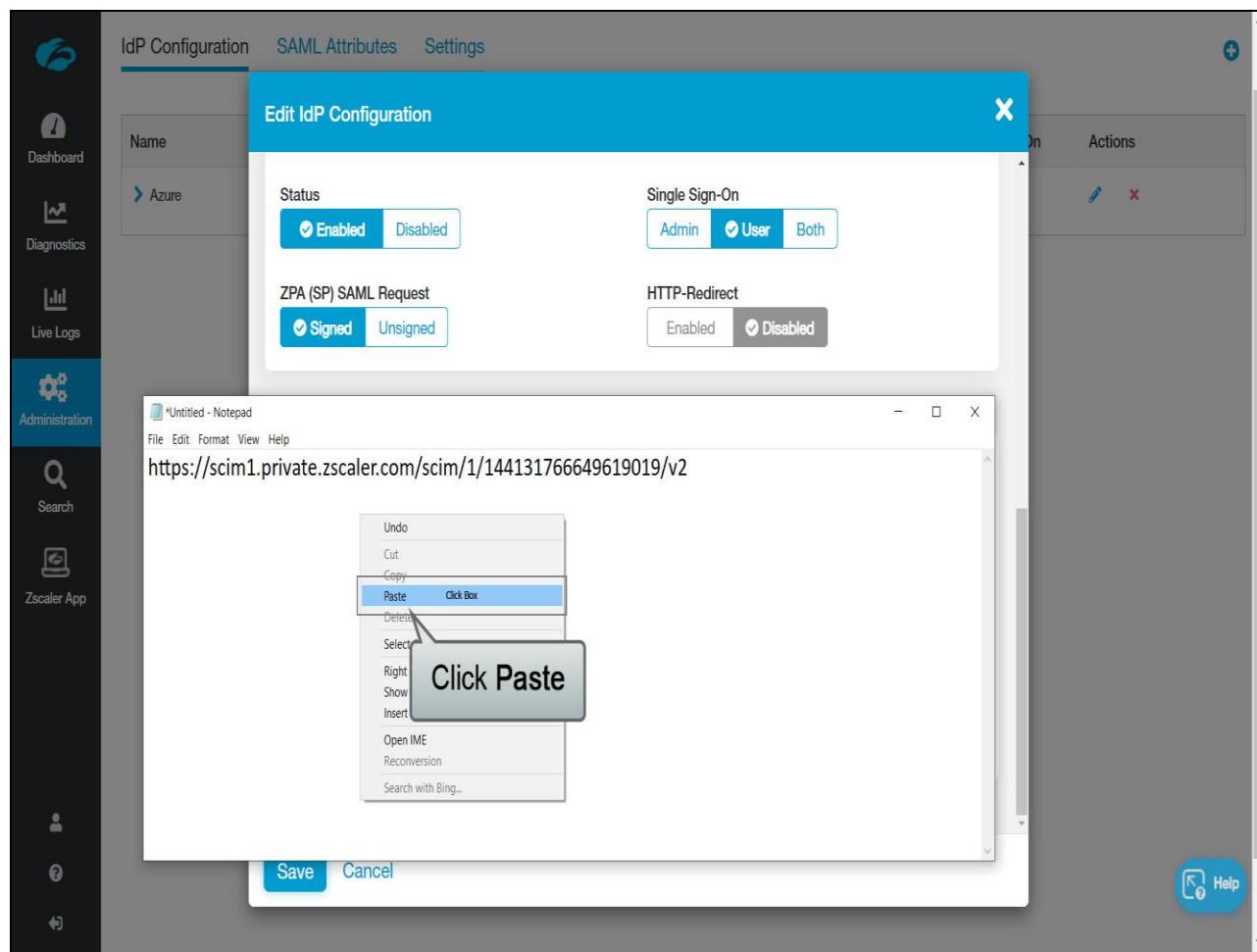
## Slide 22 - Slide 22

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal window titled 'Edit IdP Configuration' is open for the 'Azure' provider. Inside the modal, there are sections for 'Status' (Enabled), 'Single Sign-On' (Admin, User, Both), 'ZPA (SP) SAML Request' (Signed), 'HTTP-Redirect' (Enabled, Disabled), and 'SCIM' (Sync Enabled). In the 'SCIM' section, there is a 'Bearer Token' field containing a long string of characters. A context menu is open over this token field, with the option 'Click Copy' highlighted. At the bottom of the modal, there are 'Save' and 'Cancel' buttons.

## Slide notes

Repeat this process for the **Bearer Token**, select it, right-click and select **Copy**, ...

## Slide 23 - Slide 23



## Slide notes

...then back in Notepad, right-click and select **Paste**.

## Slide 24 - Slide 24

The screenshot shows the Zscaler Admin UI interface. On the left is a sidebar with various icons: Dashboard, Diagnostics, Live Logs, Administration (selected), Search, and Zscaler App. The main area has tabs for IdP Configuration, SAML Attributes, and Settings. A modal window titled "Edit IdP Configuration" is open, showing configuration for "Azure". The "Status" section has "Enabled" checked. The "Single Sign-On" section has "User" checked. The "ZPA (SP) SAML Request" section has "Signed" checked. The "HTTP-Redirect" section has "Enabled" checked. Below the modal is a Notepad window titled "Untitled - Notepad" containing the URL: <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2> qZYRXIFVH08jx0lhWY-eXBqJh70FH0DcroXj7cVv-7phgeY4C8u1zWHue-erKXY5UCxQq-LIUH7RZYott-FCg. At the bottom of the modal are "Save" and "Cancel" buttons.

## Slide notes

## Slide 25 - Slide 25

The screenshot shows the Zscaler Admin UI with the 'IdP Configuration' tab selected. A modal window titled 'Edit IdP Configuration' is open, specifically for the 'Azure' provider. The modal contains several configuration sections:

- Status:** Enabled (selected)
- Single Sign-On:** User (selected)
- ZPA (SP) SAML Request:** Signed (selected)
- HTTP-Redirect:** Disabled
- SCIM Sync:** Enabled (selected)
- SCIM Service Provider Endpoint:** https://scim1.private.zscaler.com/scim/1/144131766649619019/v2
- Bearer Token:** A long token string is displayed.

A callout bubble with the text "Click Save" points to the blue "Save" button at the bottom left of the modal. Other buttons include "Generate New Token" and "Cancel".

## Slide notes

Click to **Save** the configuration.

## Slide 26 - Slide 26

The screenshot shows the Zscaler Admin UI interface. On the left is a dark sidebar with various icons and labels: Dashboard, Diagnostics, Live Logs, Administration (which is selected and highlighted in blue), Search, Zscaler App, and three icons at the bottom. The main content area has a header with tabs: IdP Configuration (selected), SAML Attributes, and Settings. Below the header is a table with the following data:

Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure	✓	https://sts.windows.net/457d09b0-86e3-49d8-9ffd-14e6ec0a12a1/	User	<span>(Edit)</span> <span>(Delete)</span>

In the bottom right corner of the main area, there is a green notification box with the text "IdP configuration saved" and a small "Help" icon.

## Slide notes

## Slide 27 - Slide 27

## Slide notes

You now need to configure Azure AD, ...

## Slide 28 - Slide 28

The screenshot shows the Microsoft Azure Portal homepage. On the left, there's a sidebar with various service icons and names. The main area is titled 'Azure services' and contains several buttons: 'Create a resource' (with a plus sign icon), 'Azure Active Directory' (with a blue box icon, highlighted with a gray callout box and the text 'Click Azure Active Directory'), 'Enterprise applications', 'Virtual machines', 'Resource groups', 'All resources', and 'Subscriptions'. Below this is a section titled 'Recent resources' with a table:

Name	Type	Last Viewed
PATRAINING26	Resource group	6 months ago
syslog	Virtual machine	8 months ago
Host-1	Virtual machine	8 months ago
patraining26	Subscription	11 months ago

At the bottom, there's a 'Navigate' section with links for 'Subscriptions', 'Resource groups', and 'All resources'.

## Slide notes

...so open the Microsoft Azure Portal and click **Azure Active Directory**.

## Slide 29 - Slide 29

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled 'patraining26 | Overview' under 'Azure Active Directory'. It includes sections for Overview, Getting started, Preview hub, Diagnose and solve problems, Manage (with links for Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registration, Identity Governance, Application proxy, and Licenses), Tenant information (showing Your role as Global administrator, License as Azure AD Free, and Tenant ID as 457d09b0-86e3-49d8-9ffd-14e6...), and Azure AD Connect (Status: Not enabled, Last sync: Sync has never run). A callout box with the text 'Click Enterprise Applications' points to the 'Enterprise applications' link in the Manage section of the sidebar.

## Slide notes

Click Enterprise Applications, ...

## Slide 30 - Slide 30

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons such as Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Enterprise applications | All applications" under "patraining26 - Azure Active Directory". The left navigation pane has sections for Overview, Manage, Security, and Activity, with "All applications" currently selected. The main pane displays a table of applications with columns for Name, Homepage URL, Object ID, and Application ID. A specific row for "Zscaler Private Access" is highlighted with a callout bubble containing the text "Click Zscaler Private Access (ZPA)".

## Slide notes

...then click to open the application named **Zscaler Private Access (ZPA)**.

## Slide 31 - Slide 31

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation bar with various service icons like Create a resource, Home, Dashboard, etc. The main content area is titled "Zscaler Private Access (ZPA) | Overview" and is categorized as an "Enterprise Application".  
On the right, under the "Properties" section, there are fields for Name (Zscaler Private Access (ZPA)), Application ID (85f2856c-f062-4e85-b61e-...), and Object ID (79190bd0-3730-466f-863d...). Below these fields is a "Copy to clipboard" button.  
In the center, under the "Getting Started" heading, there are two boxes:

- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Azure AD credentials

A large callout box with a blue border and white text points to the "Users and groups" link in the sidebar. Another callout box with a blue border and white text points to the "Copy to clipboard" button.

## Slide notes

The first thing to check, is that the correct set of users and/or groups is assigned to this application, so click **Users and groups**, ...

## Slide 32 - Slide 32

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation bar includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', and 'Security Center'. The main content area displays the 'Zscaler Private Access (ZPA) | Users and groups' page under 'Enterprise Application'. The left sidebar under 'Manage' lists 'Properties', 'Owners', 'Roles and administrators (Previous)', 'Users and groups' (which is selected), 'Single sign-on', 'Provisioning' (with a callout 'Click Provisioning'), 'Self-service', 'Conditional Access', 'Permissions', and 'Token encryption'. The right pane shows a table with three users:

Display Name	Object Type	Role assigned
HT hvac test	User	User
ST smadmin test	User	User
ST student test	User	

A callout box over the table contains the text 'Verify the users that are to be sync'd using SCIM'.

[https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/ManagedAppMenuBlade/ManageProvisioning/appId/85f2856c-f062-4e85-b61e-d303db15f221/objectId/79190bd0-3730-466f-863d-1c7174114c00](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/ManageProvisioning/appId/85f2856c-f062-4e85-b61e-d303db15f221/objectId/79190bd0-3730-466f-863d-1c7174114c00)

## Slide notes

...and verify that the correct users and groups are listed.

To enable SCIM synchronization to ZPA, click **Provisioning**, ...

## Slide 33 - Slide 33

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning" and is described as an "Enterprise Application". A navigation bar at the top includes Home, Enterprise applications, Zscaler Private Access (ZPA), Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service), Security (Conditional Access, Permissions, Token encryption), and Help. A message bar at the top right says "Got a second? We would love your feedback on user provisioning. →". Below the navigation bar is a central panel with a cloud icon and the text "Automate identity lifecycle management with Azure Active Directory". It explains that accounts are automatically created, updated, and deleted when users join, leave, and move within the organization, with a link to "Learn more". A prominent blue "Get started" button is highlighted with a callout bubble containing the text "Click Get started". Other links in the panel include "What is provisioning?", "Configure automatic provisioning.", and "application deployment".

## Slide notes

...then click **Get started**.

## Slide 34 - Slide 34

The screenshot shows the Microsoft Azure portal interface. On the left is a sidebar with various service icons. The main area is titled "Provisioning" under "Enterprise applications > Zscaler Private Access (ZPA)". A dropdown menu for "Provisioning Mode" is open, showing "Manual" and "Automatic". A large callout box with the text "Click Automatic" points to the "Automatic" option.

## Slide notes

To push updates to ZPA automatically using the API, for the **Provisioning Mode** option select **Automatic**.

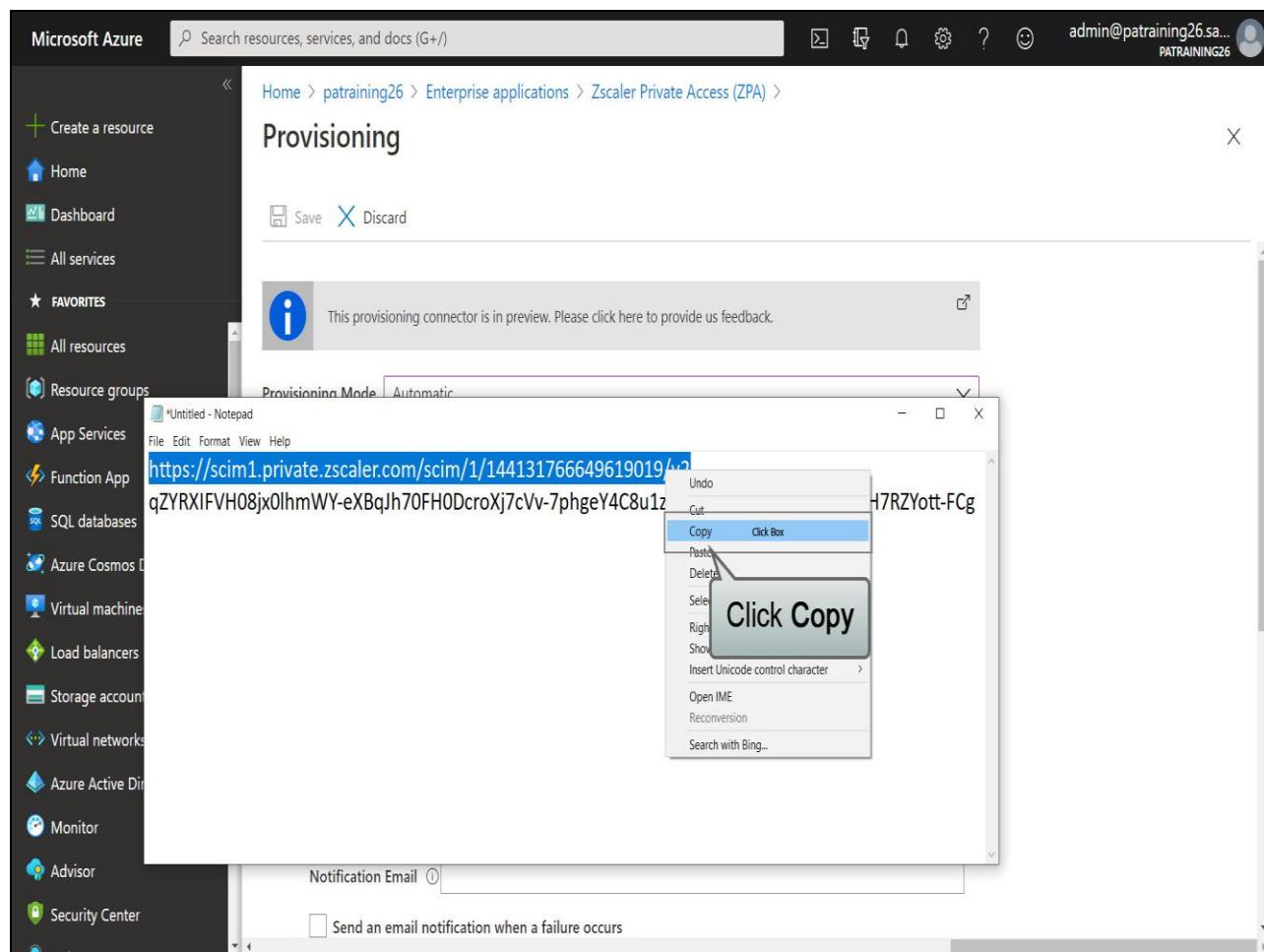
## Slide 35 - Slide 35

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area is titled "Provisioning" and shows the "Enterprise applications > Zscaler Private Access (ZPA)" path. A message at the top says "This provisioning connector is in preview. Please click here to provide us feedback." Below it, "Provisioning Mode" is set to "Automatic". A descriptive text explains that Azure AD manages user account creation and synchronization based on user and group assignment. Under "Admin Credentials", there are fields for "Tenant URL" (with a placeholder "https://zpa.zscaler.net"), "Secret Token" (with a placeholder "XXXXXXXXXX"), "Test Connection" (a button), "Notification Email" (with a placeholder "admin@patraining26.sa..."), and a checkbox for "Send an email notification when a failure occurs".

## Slide notes

This is where you need to provide that URL and the secret key, so switch back to Notepad, ...

## Slide 36 - Slide 36



## Slide notes

...select and right-click on the URL and select **Copy**, ...

## Slide 37 - Slide 37

The screenshot shows the 'Provisioning' configuration page for Zscaler Private Access (ZPA) in the Microsoft Azure portal. The 'Provisioning Mode' is set to 'Automatic'. The 'Admin Credentials' section requires a 'Tenant URL' (which is highlighted with a red box) and a 'Secret Token' (containing 'training-team@zscaler.com'). A context menu is open over the 'Tenant URL' field, showing options like Undo, Redo, Cut, Copy, Paste, Paste plain text, Select, Spell, Write, Inspect, and Test Connection. A callout bubble with the text 'Click Paste' points to the 'Paste' option in the menu.

## Slide notes

...back in Azure, right-click in the Tenant URL field and click Paste.

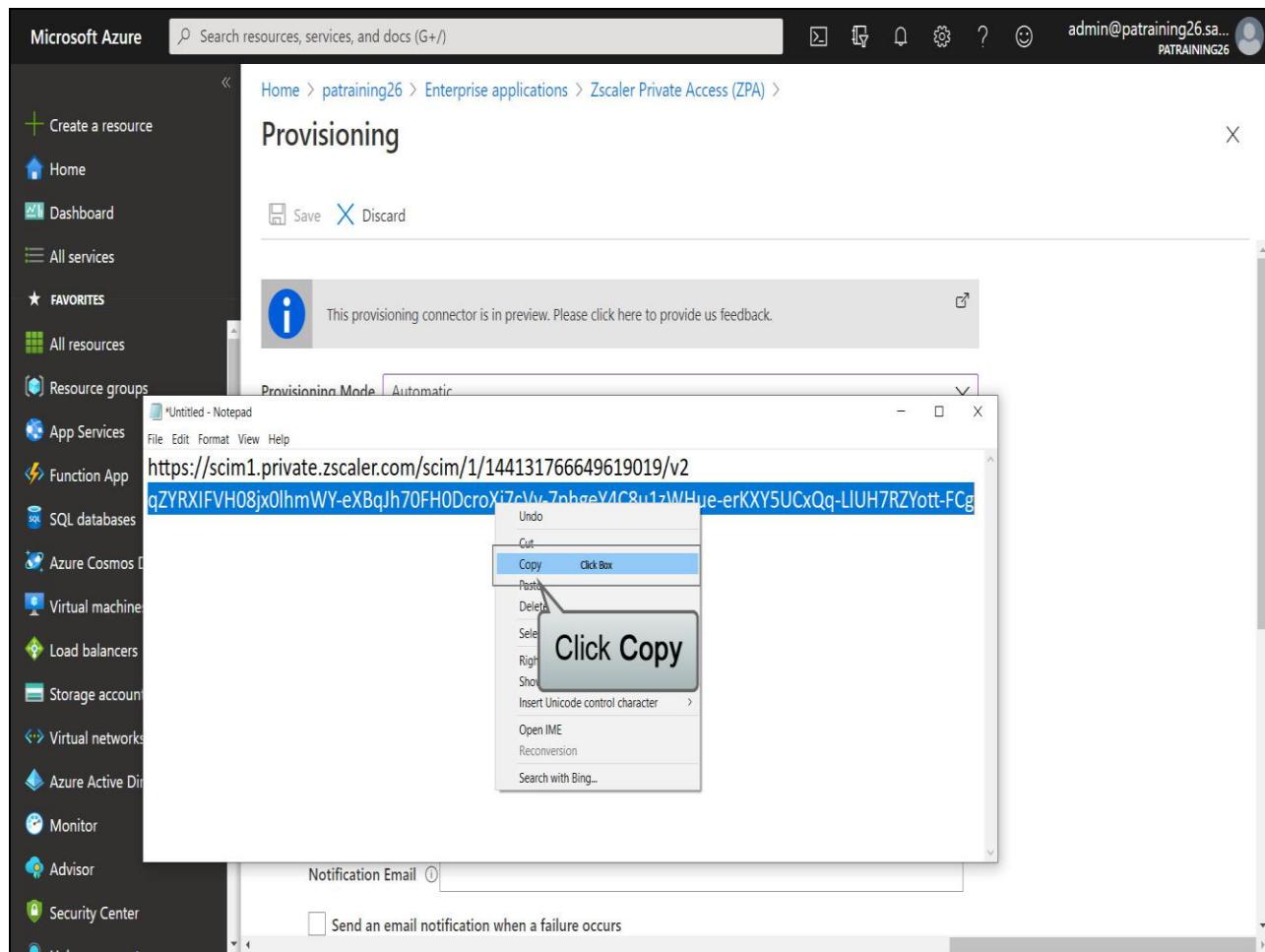
## Slide 38 - Slide 38

The screenshot shows the Microsoft Azure portal interface for provisioning. The left sidebar lists various services like Home, Dashboard, and Resource groups. The main content area is titled 'Provisioning' under 'Enterprise applications > Zscaler Private Access (ZPA)'. A message indicates the connector is in preview. The 'Provisioning Mode' is set to 'Automatic'. Under 'Admin Credentials', the 'Tenant URL' field contains 'https://scim1.private.zscaler.com/scim/1/144131766649619019/v2' and has a validation error message: 'This field is required.' The 'Secret Token' field is empty and also has a validation error message: 'This field is required.' Other fields shown include 'Notification Email' and a checkbox for 'Send an email notification when a failure occurs'.

## Slide notes

Repeat this process for the **Secret (Bearer) Token**, ...

## Slide 39 - Slide 39



## Slide notes

...click to **Copy** the **Bearer Token** from Notepad, ...

## Slide 40 - Slide 40

The screenshot shows the 'Provisioning' page for Zscaler Private Access (ZPA) in the Microsoft Azure portal. The left sidebar lists various Azure services. The main area shows the provisioning configuration for ZPA. A context menu is open over the 'Secret Token' input field, with the 'Paste' option highlighted. The 'Secret Token' field is also highlighted with a red box.

## Slide notes

...then right-click and **Paste** the value into the **Secret Token** field.

## Slide 41 - Slide 41

The screenshot shows the 'Provisioning' page in the Microsoft Azure portal. The URL in the browser is [Home > patraining26 > Enterprise applications > Zscaler Private Access \(ZPA\) >](#). The left sidebar lists various Azure services. The main content area is titled 'Provisioning' and contains a message: 'This provisioning connector is in preview. Please click here to provide us feedback.' Below this is a section for 'Admin Credentials' with fields for 'URL' (containing 'https://scim1.private.zscaler.com/scim/1/144131766649619019/v2') and 'Secret Token' (containing a redacted token). A 'Test Connection' button is present. At the bottom, there are options for 'Notification Email' and 'Send an email notification when a failure occurs'. A callout bubble with the text 'Click Test Connection' points to the 'Test Connection' button.

## Slide notes

To test that the API connection has been established, click the **Test Connection** option, ...

## Slide 42 - Slide 42

The screenshot shows the Microsoft Azure portal interface. On the left, the sidebar lists various services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area is titled "Provisioning" under "Enterprise applications > Zscaler Private Access (ZPA)". A message box at the top right says "Testing connection to Zscaler Private Access... 5:44 PM" and "One moment while we confirm the supplied credentials can be used for provisioning". Below this, there's a note: "This provisioning connector is in preview. Please click here to provide us feedback." A "Save" and "Discard" button are present. The "Provisioning Mode" dropdown is set to "Automatic". A descriptive text block explains: "Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Private Access (ZPA) based on user and group assignment." Under "Admin Credentials", there are fields for "Tenant URL" (set to <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>), "Secret Token" (redacted), "Test Connection" button, "Notification Email" field, and a checkbox for "Send an email notification when a failure occurs".

## Slide notes

## Slide 43 - Slide 43

The screenshot shows the Microsoft Azure portal interface for managing enterprise applications. The left sidebar lists various services, and the main content area shows the 'Provisioning' configuration for the 'Zscaler Private Access (ZPA)' application under 'Enterprise applications'. A success message at the top right indicates a successful test connection. The 'Admin Credentials' section is expanded, showing fields for 'Tenant URL' (set to <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>) and 'Secret Token' (a masked value). A 'Test Connection' button is present, along with options for 'Notification Email' and 'Send an email notification when a failure occurs'.

## Slide notes

...and verify that the test is successful. If not, you may need to generate a new **Bearer Token** in the ZPA Admin Portal and copy/paste it to the **Secret Token** field and try the test once more.

## Slide 44 - Slide 44

This provisioning connector is in preview. Please click here to provide us feedback.

Provisioning Mode: Automatic

Use Azure AD to manage the creation and synchronization of user accounts in Zscaler Private Access (ZPA) based on user and group assignment.

Admin Credentials

Admin Credentials  
Azure AD needs the following information to connect to Zscaler Private Access (ZPA)'s API and synchronize user data.

Tenant URL \*

Secret Token \*

Notification Email

Send an email notification when a failure occurs

Scroll down...

## Slide notes

Scroll down if necessary, ...

## Slide 45 - Slide 45

The screenshot shows the 'Provisioning' page in the Microsoft Azure portal for Zscaler Private Access (ZPA). The left sidebar lists various Azure services. The main content area shows the 'Admin Credentials' section, which requires a Tenant URL (https://scim1.private.zscaler.com/scim/1/144131766649619019/v2) and a Secret Token. A 'Notification Email' field contains 'training-team@zscaler.com'. A callout bubble points to the 'Send an email notification when a failure occurs' checkbox, which is currently unchecked. The entire 'Notification Email' input field is highlighted with a red border.

## Slide notes

...and add a suitable **Notification Email** address for alerts, then enable the **Send an email notification when a failure occurs** option.

Note, this is an optional step, although we would recommend that you do this.

## Slide 46 - Slide 46

The screenshot shows the 'Provisioning' configuration page in the Microsoft Azure portal. The left sidebar lists various services like Home, Dashboard, and Azure Active Directory. The main pane shows the 'Admin Credentials' section for connecting to Zscaler Private Access. It includes fields for 'Tenant URL' (set to <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>) and 'Secret Token' (redacted), both marked as required (\*). A 'Test Connection' button is present below these fields. Below the credentials, there's a checkbox for 'Send an email notification when a failure occurs' which is checked. At the bottom of the page, there are sections for 'Mappings' and 'Settings'. The top right corner shows the user's email (admin@patraining26.sa...) and the tenant name (PATRNING26). A large gray box with the text 'Click Save' is overlaid on the 'Save' button in the top right corner of the configuration area.

## Slide notes

Click to **Save** the configuration, ...

## Slide 47 - Slide 47

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a list of services: Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area is titled "Provisioning" under "Enterprise applications > Zscaler Private Access (ZPA)". A sub-section titled "Admin Credentials" is displayed, with a note stating: "Azure AD needs the following information to connect to Zscaler Private Access (ZPA)'s API and synchronize user data." It includes fields for "Tenant URL" (set to <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>), "Secret Token" (redacted), and "Notification Email" (set to training-team@zscaler.com). A checkbox labeled "Send an email notification when a failure occurs" is checked. Below this section is a "Mappings" section, which is currently collapsed. At the bottom of the page is a "Settings" section.

## Slide notes

## Slide 48 - Slide 48

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons such as Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Provisioning" under "Enterprise applications > Zscaler Private Access (ZPA)". A success message box is displayed at the top right: "Updating user provisioning settings" and "Successfully updated Zscaler Private Access (ZPA)" at 5:45 PM. The "Admin Credentials" section is expanded, showing fields for "Tenant URL" (https://scim1.private.zscaler.com/scim/1/144131766649619019/v2) and "Secret Token" (redacted). A "Test Connection" button is present. Below this, a "Notification Email" field contains training-team@zscaler.com, and a checked checkbox indicates "Send an email notification when a failure occurs". The "Mappings" section is collapsed. At the bottom, there is a "Settings" link.

## Slide notes

## Slide 49 - Slide 49

The screenshot shows the Azure portal interface for managing Zscaler Private Access (ZPA) provisioning. On the left is the navigation sidebar with various service icons. The main content area shows the 'Provisioning' configuration page for ZPA. It includes fields for 'Tenant URL' (set to <https://scim1.private.zscaler.com/scim/1/144131766649619019/v2>) and 'Secret Token' (redacted). There's a 'Test Connection' button and a checkbox for 'Send an email notification when a failure occurs' (which is checked). Below these are sections for 'Mappings' and 'Settings'. In the top right corner of the main content area, there is a small modal window with a red 'Close' button. A grey callout bubble with the text 'Click Close' points to this button.

## Slide notes

...then click to **Close** it.

## Slide 50 - Slide 50

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning" under "Enterprise Application". It features a toolbar with "Start provisioning" (highlighted with a callout box), Stop provisioning, Restart provisioning, Edit provisioning, and more. A message box says "Got a second? We would love your feedback on user provisioning. →". Below the toolbar, it says "Current cycle" and "Incremental cycle stopped. 0% complete". Under "Manage", sections include Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning (which is selected and highlighted with a callout box), Self-service, and Security. Under "Statistics to date", there are links for View provisioning details and View technical information. A "View provisioning logs" link is also present. In the "Manage provisioning" section, there are links for Update credentials, Edit attribute mappings, Add scoping filters, and Provision on demand.

## Slide notes

To start synchronizing users across to the ZPA Admin Portal, click **Start provisioning**, ...

## Slide 51 - Slide 51

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons such as Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning" and shows the following details:

- Current cycle status:** Incremental cycle stopped. 0% complete.
- Statistics to date:**
  - View provisioning details
  - View technical information
- Manage provisioning:**
  - Update credentials
  - Edit attribute mappings
  - Add scoping filters
  - Provision on demand

A modal window at the top right says "Start provisioning" and "Please wait while provisioning begins." The timestamp is 5:45 PM.

## Slide notes

## Slide 52 - Slide 52

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons such as Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning" under "Enterprise Application". The top navigation bar includes a search bar, account information for "admin@patraining26.sa... PATRNING26", and a notification bubble indicating "Provisioning is scheduled to start." Below the title, there are tabs for Overview, Deployment Plan, and Diagnose and solve problems. The "Manage" section is expanded, showing sub-options like Properties, Owners, Roles and administrators (Previous), Users and groups, Single sign-on, Provisioning (which is selected), Self-service, Conditional Access, Permissions, and Token encryption. The "Current cycle status" section indicates "Initial cycle not run." The "Statistics to date" section has two collapsed items: "View provisioning details" and "View technical information". A link "View provisioning logs" is also present. The "Manage provisioning" section includes links for Update credentials, Edit attribute mappings, Add scoping filters, and Provision on demand.

## Slide notes

...and verify that the process starts successfully.

## Slide 53 - Slide 53

The screenshot shows the Azure portal interface for managing an Enterprise Application named "Zscaler Private Access (ZPA) | Provisioning". The left sidebar lists various Azure services. The main content area displays the provisioning status for this application. A red box highlights the "Current cycle status" section, which indicates an "Incremental cycle completed." with a progress bar showing "100% complete". A grey callout box labeled "SCIM provisioning Current cycle status" points to this section. Another grey callout box labeled "Click View provisioning details" points to the "View provisioning details" link under the "Statistics to date" heading.

## Slide notes

The status of the current provisioning cycle will be displayed. To view details, click **View provisioning details**.

## Slide 54 - Slide 54

The screenshot shows the Microsoft Azure portal interface for managing an Enterprise Application named "Zscaler Private Access (ZPA) | Provisioning".

**Current cycle status:** Incremental cycle completed. 100% complete.

**Statistics to date:**

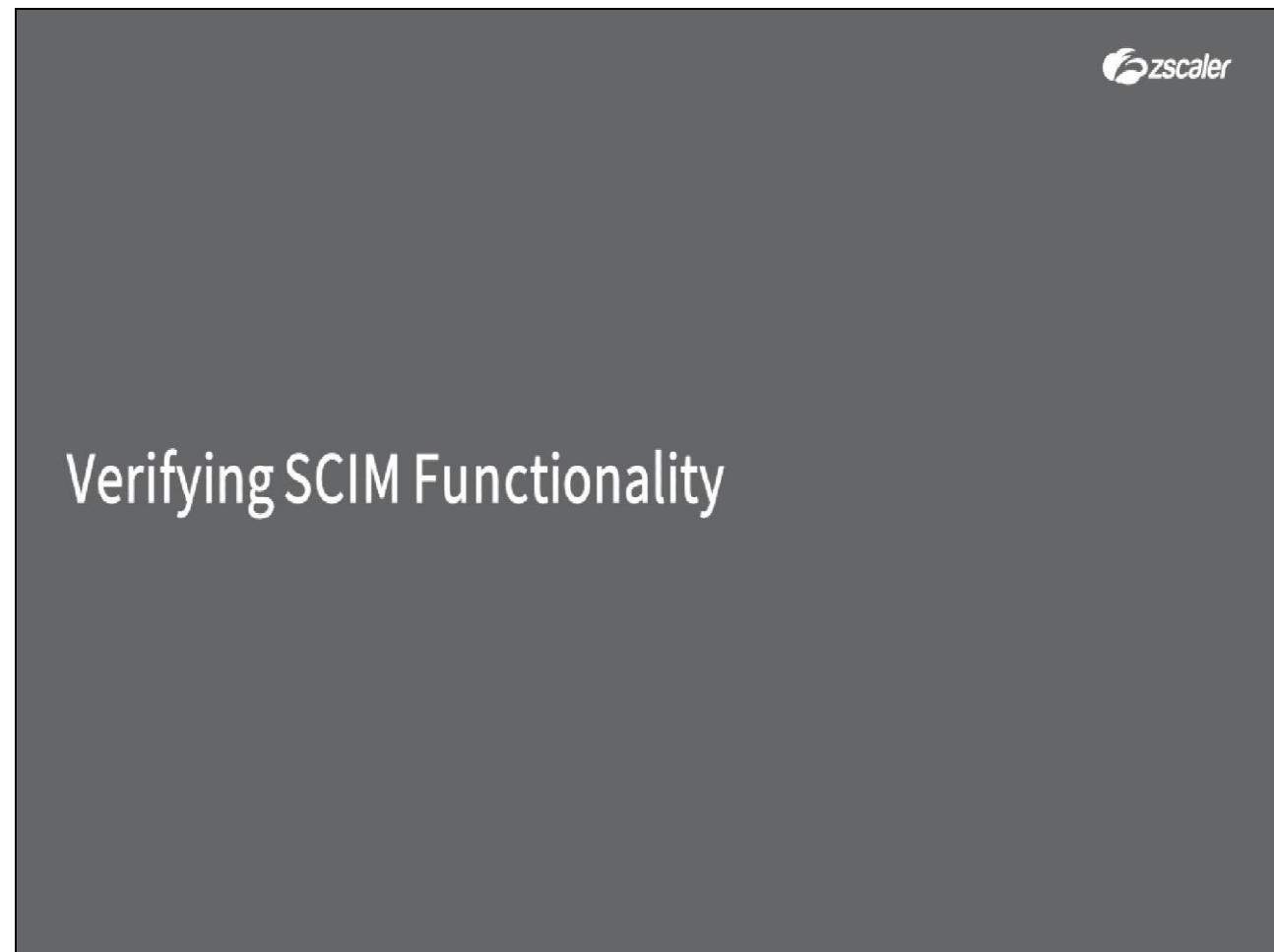
- Completed: 9/24/2020, 11:33:44 AM
- Duration: 1.954 seconds
- Steady state achieved: 9/24/2020, 11:33:44 AM
- Provisioning interval: 40 minutes

A callout box highlights the "Provisioning interval: 40 minutes" entry in the statistics table.

## Slide notes

Details will be displayed, including the hard-coded **Provisioning interval** (which is currently set to **40 minutes**).

## Slide 55 - Verifying SCIM Functionality

**Slide notes**

The final topic that we will cover is how to verify that SCIM is working.

This section has been created as an interactive demo to give you a feel for the navigation of the ZPA and Azure AD Admin Portals. You will be asked to select the appropriate menu options to navigate the UI. You may also use the **Play** control to proceed to the next step.

## Slide 56 - Slide 56

The screenshot shows the ZPA Admin Portal interface. On the left, there is a navigation sidebar with various icons and sections: LOG STREAMING SERVICE, Dashboard, Diagnostics, Live Logs, Administration (which is selected and highlighted in blue), Search, Zscaler App, and SETTINGS. Under the Administration section, there are links for Connector Groups, Log Receivers, POLICY MANAGEMENT (Access Policy, Client Forwarding Policy, Timeout Policy), REPORTING (Executive Insights App, Access), SCIM MANAGEMENT (SCIM Attributes, SCIM Groups, SCIM Users, SERVICE Keys), and SETTINGS (Administrators, Company, User Portal AUP). A callout bubble with the text "Click SCIM Users" points to the SCIM Users link under SCIM MANAGEMENT. On the right, there is a table titled "IdP Entity ID" with one row containing "https://sts.windows.net/457d09b0-86e3-49d8-9ffd-14e6ec0a12a1/" and "User". There are edit and delete icons next to the row.

## Slide notes

To verify that the SCIM synchronization is working, in the ZPA Admin Portal, from the **Administration** menu under **SCIM MANAGEMENT**, click **SCIM Users**.

## Slide 57 - Slide 57

The screenshot shows the ZPA Admin interface with the 'SCIM Users' tab selected. On the left sidebar, there are navigation links: Dashboard, Diagnostics, Live Logs, Administration (selected), Search, and Zscaler App. The main content area has a header with 'SCIM Attributes' (highlighted with a red box and a callout 'Click SCIM Attributes'), 'SCIM Users' (selected), and 'SCIM Groups'. Below the header are sections for 'SCIM ENDPOINT' (set to Azure), 'TIME RANGE' (set to Mar 22, 2020 +07 - Sep 22, 2020 +07), and 'Update' button. There are also search fields for 'SCIM USER NAME', 'IDP SCIM USER ID', and 'SCIM GROUP NAME'. The main table lists SCIM users with columns: Last Updated, UTC, Internal User ID, SCIM User Name, and IDP SCIM User ID. The table shows three rows of data:

Last Updated	UTC	Internal User ID	SCIM User Name	IDP SCIM User ID
Sep 22nd, 17:46 (+07)		884221	student@patraining26.safemarch.com	14eccf4b-b0c0-4e03-b49b-7320f8cf6aa5
Sep 22nd, 17:46 (+07)		884222	smadmin@patraining26.safemarch.com	68b22640-b78d-4aee-88b6-91f363a0e2c5
Sep 22nd, 17:46 (+07)		884220	hvac@patraining26.safemarch.com	9c01d6de-071c-447b-b8e3-e88110971190

A callout box points to the user list with the text 'Verify that the list of active SCIM users is correct'.

## Slide notes

Verify that the list of users that you saw in the ZPA Enterprise Application in Azure AD, is also visible here.

Note, you have a set of filtering and search options here to help find an individual user and an **Update** option, however there are no management controls. Remember, SCIM synchronization only occurs in a single direction, it is a push of data from the directory service to the ZPA Tenant. There is no ability to update users in ZPA and synchronize them back to the directory service.

To view the attributes assigned to SCIM users, click **SCIM Attributes**.

## Slide 58 - Slide 58

The screenshot shows the Zscaler SCIM interface. On the left is a vertical sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main content area has a header with tabs: SCIM Attributes (blue underline), SCIM Users, and SCIM Groups (highlighted with a red box). Below the header is a search bar with 'Azure' selected and a 'Search' input field. To the right of the search bar is a blue 'Update' button. The main table lists SCIM attributes with columns: SCIM Attribute Name, SCIM Attribute, Required Attribute, and Unique Attribute. Each row contains a small blue edit icon. A blue help icon is located in the bottom right corner of the table area.

SCIM Attribute Name	SCIM Attribute	Required Attribute	Unique Attribute
Active	active	No	No
Cost Center	costCenter	No	No
Department	department	No	No
Display Name	displayName	No	No
Division	division	No	No
Email	emails.value	No	No
Last Name	name.familyName	No	No
Formatted Name	name.formatted	No	No
First Name	name.givenName	No	No
Nickname	nickName	No	No

## Slide notes

Once again, you have some filtering and search options here to help find a particular attribute and an **Update** option, however there are no management controls.

To view the groups that SCIM users are assigned to, click **SCIM Groups**.

## Slide 59 - Slide 59

The screenshot shows the Zscaler SCIM Groups interface. On the left is a vertical navigation bar with icons for Dashboard, Diagnostics, Live Logs, Administration (selected), Search, Zscaler App, and Help. The main area has tabs for SCIM Attributes, SCIM Users, and SCIM Groups (selected). A red box highlights the top search/filter section. Inside this box are fields for SCIM ENABLED IDENTITY PROVIDERS (set to Azure), SCIM GROUP NAME (Search), IDP SCIM GROUP ID (Search), and SCIM USER NAME (None). Below this is a TIME RANGE dropdown set to Mar 24, 2020 +07 - Sep 24, 2020 +07, and an Update button. A callout bubble labeled "List filter and search options" points to this section. The main table below has columns for Last Updated (UTC), Internal Group ID, SCIM Group Name, and IdP SCIM Group ID. It displays the message "No Items Found". A blue "Help" button is located in the bottom right corner.

## Slide notes

A similar set of filtering and search options are available here to help find a particular group or user, plus the **Update** option.

Note that in this example, no Azure AD groups have been synchronized using SCIM, hence this list is empty.

## Slide 60 - Slide 60

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning" and is described as an Enterprise Application. It has sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups), Statistics to date (View provisioning details, View technical information, View provisioning logs), and Manage provisioning (Update credentials, Edit attribute mappings, Add scoping filters, Provision on demand). A callout bubble points to the "Users and groups" link under the Manage section. The URL in the browser bar is [https://portal.azure.com/#blade/Microsoft\\_AAD\\_IAM/ManagedAppMenuBlade/Users/appId/05f2056c-f062-4e85-b61e-d303db15f221/objectId/79190bd0-3730-466f-863d-1c7174114c00](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/Users/appId/05f2056c-f062-4e85-b61e-d303db15f221/objectId/79190bd0-3730-466f-863d-1c7174114c00).

## Slide notes

To actively verify that SCIM synchronization is working, open the Azure Admin Portal, navigate to the **Zscaler Private Access (ZPA)** Enterprise Application in Azure AD and click **Users and groups**.

## Slide 61 - Slide 61

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Users and groups" and shows the following details:

- Overview, Deployment Plan, Diagnose and solve problems.
- Manage section with options: Properties, Owners, Roles and administrators (Previous), **Users and groups** (which is selected and highlighted in blue), Single sign-on, Provisioning, Self-service.
- Security section with Conditional Access, Permissions, Token encryption.

At the top right, there are buttons for Add user, Edit, Remove, Update Credentials, Columns, and Got feedback?.

A message box states: "The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this." Below it is a search bar: "First 100 shown, to search all users & groups, enter a display name." A table lists users:

Display Name	Object Type	Role assigned
HT hvac test	User	User
smadmin test	User	User
	User	User

A callout box with a pink border and white text points to the user "hvac test": "Click to select the user named hvac test".

## Slide notes

You need to force an update of the list of users assigned to this application, in this case we will remove a user, although we could just as easily add a test user to the list. Click to select the user named **hvac test**, ...

## Slide 62 - Slide 62

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Zscaler Private Access (ZPA) | Users and groups" and is described as an Enterprise Application. It has a breadcrumb trail: Home > patraining26 > Enterprise applications > Zscaler Private Access (ZPA). Below the title, there are buttons for Add user, Edit, Remove, Update Credentials, Columns, and Got feedback? A tooltip for the Remove button says: "The application will appear on the user's dashboard. Set 'visible to users?' to no in properties to prevent this." A large callout box with the text "Click Remove" points to the Remove button. The main table lists three users:

Display Name	Object Type	Role assigned
HT hvac test	User	User
ST smadmin test	User	User
ST student test	User	User

## Slide notes

...click Remove, ...

## Slide 63 - Slide 63

The screenshot shows the Microsoft Azure portal interface. On the left is the navigation sidebar with various service icons. The main area displays the 'Enterprise applications' section under 'patraining26'. A specific application, 'Zscaler Private Access (ZPA)', is selected. The 'Users and groups' tab is active, showing a list of users assigned to the application. A modal dialog box is overlaid on the page, prompting the user to confirm the removal of these assignments. The dialog has two buttons: 'Yes' (highlighted with a pink circle and a callout bubble) and 'No'. A tooltip-like callout bubble points to the 'Yes' button with the text 'Click Yes to confirm'.

## Slide notes

...click Yes to confirm, ...

## Slide 64 - Slide 64

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area displays the 'Zscaler Private Access (ZPA) | Users and groups' page for an Enterprise Application. The 'Manage' section on the left lists Properties, Owners, Roles and administrators (Preview), Users and groups (selected), Single sign-on, Provisioning, and Self-service. The 'Users and groups' table lists three users:

Display Name	Object Type	Role assigned
HT hvac test	User	User
ST smadmin test	User	User
ST student test	User	User

A modal window at the top right shows a progress bar and the message: "Application removal in progress" and "Removing access to 1 application assignments". The status bar at the bottom right shows "6:25 PM".

## Slide notes

## Slide 65 - Slide 65

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', and 'Security Center'. The main content area displays the 'Enterprise applications' section under 'patraining26'. A specific application, 'Zscaler Private Access (ZPA)', is selected. The 'Users and groups' tab is active. A success message at the top right states 'Application assignments removed' at 6:25 PM, indicating one assignment was removed. Below this, a note says 'The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this.' A search bar allows searching for users and groups by display name. A table lists the assigned users:

Display Name	Object Type	Role assigned
smadmin test	User	User
student test	User	User

## Slide notes

...and verify that the user is removed.

Note, the user still exists in Azure AD, we have just removed the assignment to the ZPA application.

## Slide 66 - Slide 66

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation bar includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', 'Advisor', and 'Security Center'. The main content area displays the 'Zscaler Private Access (ZPA) | Users and groups' page under 'Enterprise Application'. The 'Manage' section on the left lists 'Properties', 'Owners', 'Roles and administrators (Previous)', 'Users and groups' (which is selected), 'Single sign-on', 'Provisioning' (with a callout box labeled 'Click Provisioning'), 'Self-service', 'Conditional Access', 'Permissions', and 'Token encryption'. The 'Users and groups' table shows two entries: 'smadmin test' and 'student test', both listed as 'User' type with 'User' assigned. At the top right, there are buttons for 'Add user', 'Edit', 'Remove', 'Update Credentials', 'Columns', and 'Got feedback?'. A message at the top states: 'The application will appear on the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this.' A search bar at the top says 'First 100 shown, to search all users & groups, enter a display name.'

## Slide notes

To open the SCIM configuration page, click **Provisioning**.

## Slide 67 - Slide 67

The screenshot shows the Microsoft Azure portal interface for managing Zscaler Private Access (ZPA) provisioning. The left sidebar lists various Azure services. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning". It displays the "Current cycle status" as "Incremental cycle stopped" with a progress bar at 0% complete. Below this is a section for "Statistics to date" with two collapsed dropdowns: "View provisioning details" and "View technical information". A "View provisioning logs" link is also present. In the bottom-left corner of the main content area, there is a red-bordered box containing a list of management options under the heading "Manage provisioning": "Update credentials", "Edit attribute mappings", "Add scoping filters", and "Provision on demand". A callout box labeled "Click to access More options" points to the "Edit provisioning" button at the top right of the page. Another callout box labeled "Additional management options" points to the "Manage provisioning" section.

## Slide notes

There are a number of options on this page that allow you to view configuration details or manage the configuration. One of the management options is to **Provision on demand**, which will force an immediate synchronization for a selected user.

This option is also available in the menu at the top, click on the **Ellipsis, ...**

## Slide 68 - Slide 68

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled 'Zscaler Private Access (ZPA) | Provisioning' under 'Enterprise Application'. It has tabs for Overview, Deployment Plan, and Diagnose and solve problems. Under 'Manage', there are sections for Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning (which is selected), Self-service, Conditional Access, Permissions, and Token encryption. A callout box points to the 'Provision on demand' button in the top right corner of the main content area. The status bar at the bottom shows '0% complete'.

## Slide notes

...then click **Provision on demand**.

## Slide 69 - Slide 69

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area is titled "Provision on demand" under "Enterprise applications > Zscaler Private Access (ZPA)". It includes a "Learn More" link and a "Got feedback?" button. A section titled "Select a user to" lists three options: "Quickly create or update the user's account in the target application based on your provisioning configuration", "Provision a user on demand", and "Validate provisioning with a subset of users before rolling out broadly in your organization". Below this is a search bar with the placeholder "Search for user by name, userPrincipalName or mail". A callout box with the text "Click in the Search field" points to this search bar. At the bottom, there's a "Provision" button.

## Slide notes

Click in the Search field, ...

## Slide 70 - Slide 70

The screenshot shows the Microsoft Azure portal interface. On the left is the classic navigation menu. The main content area is titled "Provision on demand" under "Enterprise applications > Zscaler Private Access (ZPA)". A search bar at the top says "Search resources, services, and docs (G+/" followed by a magnifying glass icon. To the right of the search bar are several small icons: a square, a gear, a question mark, a smiley face, and a user profile. The user profile shows "admin@patraining26.sa..." and "PATRNING26".  
  
The main content area has a heading "Select a user to" and a list of three bullet points:

- Quickly create or update the user's account in the target application based on your provisioning configuration
- Provision a user on demand
- Validate provisioning with a subset of users before rolling out broadly in your organization

A search bar contains the text "hvac". Below it, a dropdown menu shows a single result: "hvac test" with the email "hvac@patraining26.safemarch.com". A callout box with a grey border and black text points to this dropdown, containing the instruction "Click to select the user hvac test".  
  
At the bottom of the main content area is a "Provision" button.

## Slide notes

...start to type the name of the user that you wish to synchronize (in this case the user named **hvac test**) and click to select the correct user, ...

## Slide 71 - Slide 71

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area has a header 'Provision on demand' and a sub-header 'Home > patraining26 > Enterprise applications > Zscaler Private Access (ZPA) >'. Below this, there's a 'Learn More' link and a 'Got feedback?' button. A section titled 'Select a user to' lists three options: 'Quickly create or update the user's account in the target application based on your provisioning configuration', 'Provision a user on demand', and 'Validate provisioning with a subset of users before rolling out broadly in your organization'. There's also a search bar 'Search for user by name, userPrincipalName or mail'. Under 'Selected user', it shows 'hvac test' with the email 'hvac@patraining26.safemarch.com'. At the bottom, there's a large 'Provision' button with a callout bubble pointing to it that says 'Click Provision'.

## Slide notes

...then click **Provision**.

## Slide 72 - Slide 72

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains various service icons such as Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main content area is titled "Provision on demand". It displays a user selection interface with a purple circular icon containing a green "C" and a blue "Z". Below it, the text "Select a user to" is followed by a bulleted list: "• Quickly create or update the user's account in the target application based on your provisioning configuration", "• Provision a user on demand", and "• Validate provisioning with a subset of users before rolling out broadly in your organization". A search bar below the list contains the placeholder text "Search for user by name, userPrincipalName or mail". Under the heading "Selected user", there is a list item: "hvac test hvac@patraining26.safemarch.com". At the bottom of the page, a progress bar indicates "Validating..." with a circular loading icon.

## Slide notes

## Slide 73 - Slide 73

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area has a header 'Provision on demand' with a back arrow, a search bar, and a user profile. Below the header, there's a section titled 'Select a user to' with a list of options: 'Quickly create or update the user's account in the target application based on your provisioning configuration', 'Provision a user on demand', and 'Validate provisioning with a subset of users before rolling out broadly in your organization'. A search bar below this says 'Search for user by name, userPrincipalName or mail'. Under 'Selected user', there's a list with one item: 'hvac test' (represented by a pink circle icon) and 'hvac@patraining26.safemarch.com'. At the bottom, a progress bar indicates 'Validating...' with three small squares.

## Slide notes

## Slide 74 - Slide 74

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons: Create a resource, Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, and more. The main content area has a header 'Provision on demand' with a back arrow, a search bar, and a user profile. Below the header, there's a section titled 'Select a user to' with a list of provisioning options. A user 'hvac test' is selected, shown with a pink profile icon and the email 'hvac@patraining26.safemarch.com'. At the bottom, a progress bar indicates 'Validating...'.

## Slide notes

## Slide 75 - Slide 75

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Create a resource, Home, Dashboard, etc. The main area shows a 'Scoping details' page for provisioning. A message at the top says: 'The User 'hvac@patraining26.safemarch.com' will be skipped due to the following reasons: 1) This object is not a user or group. If you do not expect the object to be skipped, assign the object to the application or change your scoping filter to include it in scope for provisioning. 2) This object does not have required entitlement for provisioning. If you did not skip this object, update provisioning scope to 'Sync all users and groups' or assign the object to the application with entitlements. Click Close'. Below this, there's a table with columns 'Attribute name' and 'Attribute value'. The table contains four rows: SkipReason (NotEffectivelyEntitled), IsActive (True), Assigned to the application (False), and IsInProvisioningScope (True). A red box highlights this table. A callout bubble points to the 'Click Close' button with the text 'Check the result of the on-demand provisioning'.

Attribute name	Attribute value
SkipReason	NotEffectivelyEntitled
IsActive	True
Assigned to the application	False
IsInProvisioningScope	True

## Slide notes

Check the results of the provisioning, they may indicate that:

- The end user has been added to;
- Or removed from the ZPA list;
- In this case the manual provisioning was unnecessary as the end user was removed just about immediately, so is no longer available in the ZPA instance to be updated.

Click to Close the Scoping details message.

## Slide 76 - Slide 76

Microsoft Azure Search resources, services, and docs (G+)

Home > patraining26 > Enterprise applications > Zscaler Private Access (ZPA) >

## Provision on demand

Learn More Technical details Got feedback?

**Import user** (Success)  
Successfully imported user  
View details

**Determine if user is in scope** (Information)  
User is not in scope  
View details

Click to return to the Enterprise Application

Options to Retry or to Provision another user

**Retry** **Provision another user**

## Slide notes

You have options on this page to **Retry** the provisioning, or to **Provision another user**. Alternatively, you can click to return to the **Provisioning** page of the Enterprise Application.

## Slide 77 - Slide 77

The screenshot shows the Microsoft Azure portal interface. On the left is the navigation sidebar with various service icons. The main content area is titled "Zscaler Private Access (ZPA) | Provisioning". The top navigation bar includes "Search resources, services, and docs (G+)", user info, and settings. A red box highlights the top right controls: "Start provisioning" (disabled), "Stop provisioning", "Restart provisioning", "Edit provisioning", and more. A callout bubble contains the text: "Verify that provisioning is started, if necessary Start provisioning or Restart provisioning". The left sidebar has sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning - which is selected), Self-service, Security (Conditional Access, Permissions, Token encryption), and Statistics to date (View provisioning details, View technical information, View provisioning logs). The bottom section is titled "Manage provisioning" with a "Update credentials" link.

## Slide notes

On this page, be sure to check that provisioning is enabled:

- The **Start provisioning** option should be greyed out;
- The **Stop provisioning** and **Restart provisioning** options should both be available to activate.

## Slide 78 - Slide 78

The screenshot shows the Zscaler Admin Portal's SCIM Management interface. On the left is a navigation sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected), Search, and Zscaler App. The main content area has tabs for SCIM Attributes, SCIM Users (selected), and SCIM Groups. It includes filters for SCIM Enabled Identity Providers (Azure), SCIM User Name, IDP SCIM User ID, and SCIM Group Name, along with a Time Range selector (Mar 22, 2020 +07 - Sep 22, 2020 +07) and an Update button. The main table lists users with columns for Last Updated (UTC), SCIM User Name, and IDP SCIM User ID. A context menu is open over the second row, with a callout box containing the text "Click to Reload the page" pointing to the "Click Box" option in the menu. The menu also includes options like Reload, Back, Forward, Save as, Print, Cast, Trans, View page, Inspect, and Help.

Last Updated (UTC)	SCIM User Name	IDP SCIM User ID
Sep 22nd, 17:46 (+07)	student@patraining26.safemarch.com	14eccf4b-b0c0-4e03-b49b-7320f8cf6aa5
Sep 22nd, 17:46 (+07)	smadmin@patraining26.safemarch.com	68b22640-b78d-4aee-88b6-91f363a0e2c5
Sep 22nd, 17:46 (+07)	hvac@patraining26.safemarch.com	9c01d6de-071c-447b-b8e3-e88110971190

## Slide notes

Back in the ZPA Admin Portal, on the **Administration > SCIM MANAGEMENT > SCIM Users** page, reload the page to update the list, ...

## Slide 79 - Slide 79

The screenshot shows the Zscaler SCIM interface with the 'SCIM Users' tab selected. On the left sidebar, there are icons for Dashboard, Diagnostics, Live Logs, Administration (which is highlighted in blue), Search, and Zscaler App. The main area displays a table of SCIM users with the following columns: Last Updated, UTC, Internal User ID, SCIM User Name, and IdP SCIM User ID. Two rows are visible, both of which have been highlighted with a red box. A callout bubble points to these rows with the text: 'Verify that the list of active SCIM users has been updated'. The rows are as follows:

Last Updated	UTC	Internal User ID	SCIM User Name	IdP SCIM User ID
Sep 22nd, 17:46 (+07)	884221		student@patraining26.safemarch.com	14eccf4b-b0c0-4e03-b49b-7320f8cf6aa5
Sep 22nd, 17:46 (+07)	884222		smadmin@patraining26.safemarch.com	68b22640-b78d-4aee-88b6-91f363a0e2c5

## Slide notes

...and verify that the user in question has been updated. In this case, the user named **hvac test** has been removed.

Slide 80 - Thank you & Quiz



# Thank you & Quiz

## Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

What follows is a short quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.