

# Zscaler Certified Cloud Professional – Private Access (ZCCP-PA)

## Hands-on Lab Guide





## Copyright

©2020 Zscaler, Inc. All rights reserved. This document is protected by the United States copyright laws, and is proprietary to Zscaler Inc. Copying, reproducing, integrating, translating, modifying, enhancing, recording by any information storage or retrieval system or any other use of this document, in whole or in part, by anyone other than the authorized employees, customers, users or partners (licensees) of Zscaler, Inc. without the prior written permission from Zscaler, Inc. is prohibited.

## Trademark Statements

Zscaler™, Zscaler Internet Access™, Zscaler Private Access™, ZIA™ and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the property of their respective owners.

## ZCCP-PA Lab Guide

Summer 2020, Rev. 3.2a

## Contents

About the ZCCP-PA Hands-on Lab .....	4
Lab Diagram .....	5
Product Name Changes.....	6
Lab 1: Configure Basic Settings .....	7
Lab 2: Enable Zscaler Client Connector User Authentication .....	12
Lab 3: Provision ZPA Infrastructure.....	22
Lab 4: Add an Application.....	30
Lab 5: Discover Corporate Applications .....	34
Lab 6: Configure Corporate Applications .....	39
Lab 7: Browser Access for 3 <sup>rd</sup> Parties .....	47
Lab 8: Configure Advanced Access Policy .....	55
Lab 9: Configure LSS.....	61

## About the ZCCP-PA Hands-on Lab

Welcome to the Zscaler Certified Cloud Professional – Private Access (ZCCP-PA) Hands-on Lab that showcases the Zscaler Private Access (ZPA) service. During this lab you will practice fundamental and advanced skills that you require to implement ZPA including the support of 3<sup>rd</sup> party users. You will complete several tasks designed to increase your proficiency in configuring the ZPA solution.

### Connecting to the Virtual Lab

The ZCCP-PA Hands-on Lab uses cloud-based lab resources hosted on the Skytap service. Each student has access to an account on the ZPA service, an account for the Microsoft Azure service and access to a Skytap ‘Pod’ that contains two networks (Corporate and Public) and the following virtual machines (VMs):

- A Windows Client PC;
- A Windows 2016 Active Directory server and domain controller;
- A CentOS-based ZPA App Connector;
- A Windows 2012 R2 DNS server;
- A Linux Client PC.

### Login Details

Details to allow you to access the lab infrastructure will be provided prior to the start of the lab session, including:

- Your student number;
- The access URL for your Skytap Pod;
- Your login name and password for the ZPA Admin Portal;
- Your login name and password for the Microsoft Azure portal.

### Username Format

The Lab Guide includes instructions on how to login to the various portals and systems. The username format used throughout is of the form **[username]@patraining[1-N].safemarch.com**. The **[1-N]** portion indicates that you need to plug in your student number, which can be found in the login details provided to you prior to the session.

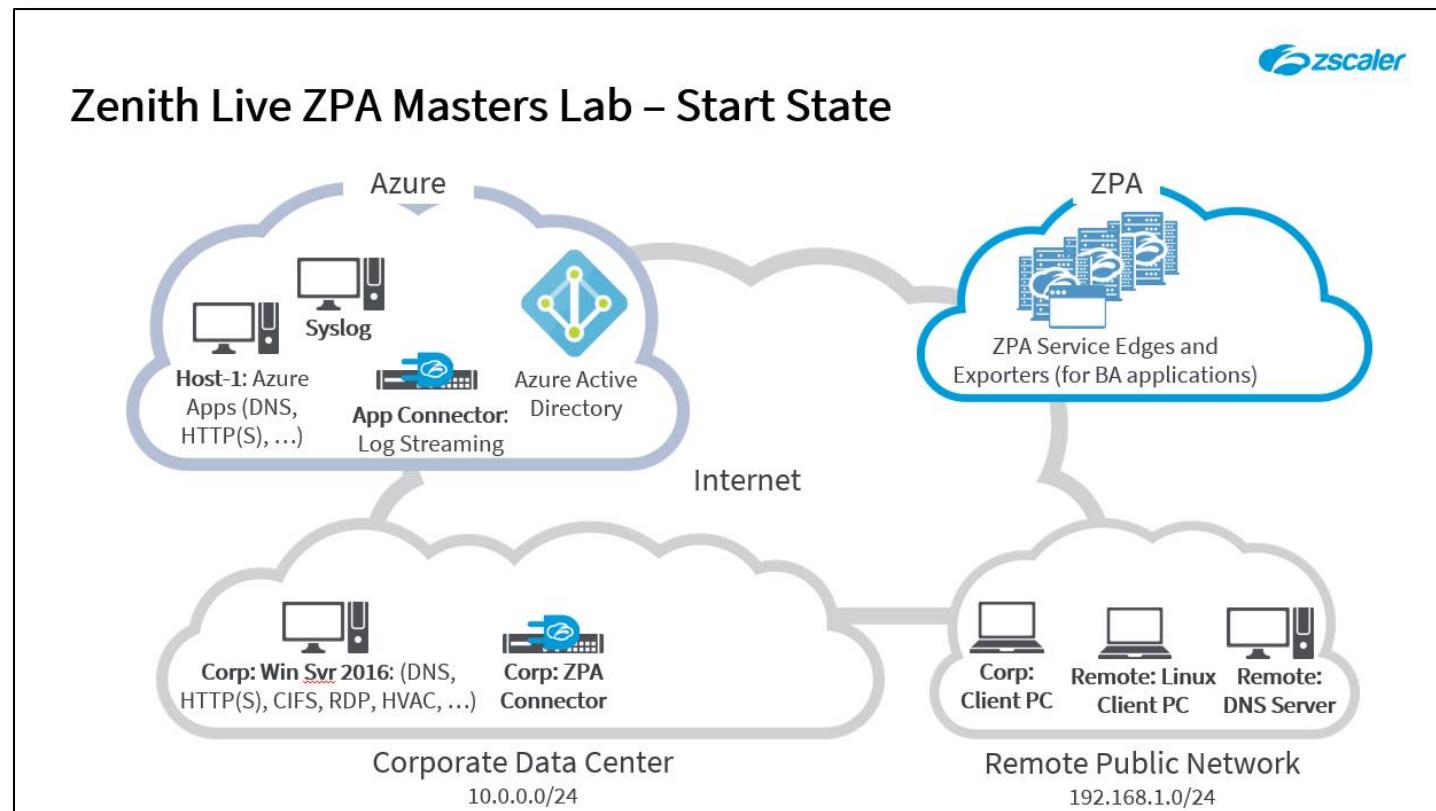
### Admin Portal Access

You can access the ZPA and Azure portals from the machine/browser of your choice. These are cloud services accessible from any machine with an Internet connection. In some labs you should access the Admin Portal from a specific VM in order to download a file or configuration to the VM.

## Lab Diagram

For your lab exercises, you will be configuring the ZPA service and an Azure environment including Azure AD as your IdP to authenticate Zscaler Client Connector and Browser Access users, allowing them access to a range of corporate applications through the ZPA App Connectors on the corporate network and in Azure.

- The **Corp: Win Svr 2016** server provides local directory services through Active Directory, and hosts Intranet applications.
- The **Corp: Client PC** is a client machine only and is equipped with 2 network adapters, so that it can be connected to the corporate network or to a remote public network (simulating a hotspot, home, or customer network).
- The **Corp: ZPA Connector** is a CentOS VM with the App Connector RPM already installed, although it must still be activated for the ZPA service.
- The **Remote: DNS Server** provides DNS services on the remote network. This will also host the CNAME records for Browser Access applications.
- The **Remote: Linux Client PC** is a Linux client machine with Firefox installed, for access to ZPA Browser Access applications.



## Product Name Changes

Note that we are in the process of changing the names of some of our products. This Lab Guide has been updated to indicate the new product names where possible, however named locations with the Admin Portal UI may still refer to the old nomenclature.

Please refer to the image below for the mapping of old names to new...

	Current Product Name	New Product Name
Connectors		
	Zscaler App	Client Connector
	Mobile Admin	Client Connector Portal
	ZPA/B2B Connectors	App Connector
Zscaler Service Edge		
	ZPA	
	ZPA Broker	ZPA Public Service Edge
	Private Brokers	ZPA Private Service Edge
	ZIA	
	ZEN/SME	ZIA Public Service Edge
	Private/Virtual ZEN	ZIA Private Service Edge
Other Services		
	Remote Browser Isolation	Cloud Browser Isolation

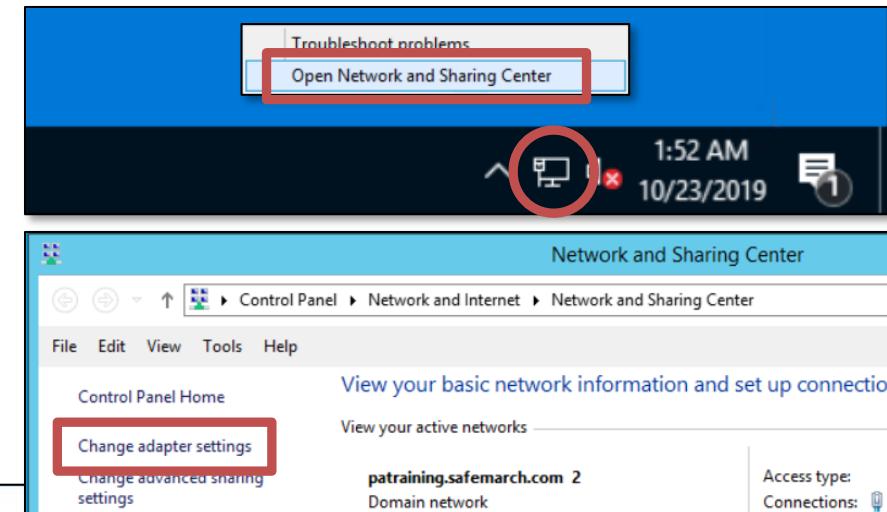
## Lab 1: Configure Basic Settings

Your ZPA environment has been newly created and contains no configurations beyond the default settings, you must add your basic settings at the ZPA Admin Portal. In this lab you will confirm the connectivity of the client PC and add some basic configuration settings, including; a 'Helpdesk' administrator with restricted permissions, and basic Company data.

### Confirm Client PC Connectivity

**The Corp:** Client PC in your environment is equipped with two network interfaces, one on the corporate network, and one on a remote network (that has no connectivity to the corporate network). The remote network simulates a connection from some external network, such as a hotspot, customer, partner, or home network. In this section you will confirm that only the network adapter on the remote network is enabled and that you have access to applications on the corporate network.

1. On the VM labelled **Corp: Client PC**, from the VM tools bar at the top, send the **Ctrl-Alt-Del** command and login to the PC with username **Student** and password **Admin-123!**
2. From the Windows Status Bar at bottom right, right-click on the network interface icon and click **Open Network and Sharing Center**.
3. In the left-hand navigation menu, click **Change adapter settings**.
4. Check that interface named **Corporate** is **Disabled** and that the interface named **Public** is **Enabled**. If necessary, disable **Corporate** and enable **Public** (use the **Administrator** account with password **Admin-123!** when prompted).
5. Right-click the adapter labelled **Public** and click **Status**, then click **Details**. Confirm that this adapter has an IP address on the **192.168.1.0** subnet.



6. Start a web browser and confirm that you have connectivity to the Internet by navigating to your preferred public web page.

## Lab 1: Configure Basic Settings

### Add a ZPA 'Helpdesk' User

In this section you will create a new role for Helpdesk users with a subset of the management functionality, then create a new Helpdesk user with restricted access to the ZPA Admin Portal suitable for your Helpdesk personnel.

7. Open a browser and access the **ZPA Admin Portal** using the URL <https://admin.private.zscaler.com> and credentials supplied in the joining instructions email.

**Note:** You may access the Admin Portal direct from your own PC in your preferred browser.

8. From the **Administration** menu under **SETTINGS**, select **Roles**, then click the **+ Add Role** link at top right and create a new role for Helpdesk users as follows:
    - a. Name the new role **Helpdesk** and optionally add a description;
    - b. Enable the following **ACCESS CONTROL** options and accept the default configuration for each:
      - **Dashboard**;
      - **Diagnostics**;
      - **Policies**;
      - And **Zscaler App Portal**;
    - c. Click **Save** to create the new role.
- Note:** In your own deployments, you will need to create and assign a suitable set of roles that meets the needs of your user population.

The screenshot shows the 'Add Role' dialog box. The 'Name' field is set to 'Helpdesk'. The 'Description' field contains 'Role for Internal Helpdesk User'. The 'ACCESS CONTROL' section is expanded, showing settings for 'Dashboard', 'Diagnostics', 'Log Streaming', 'Policies', and 'Zscaler App Portal'. Each of these sections has an 'Enable' checkbox checked and highlighted with a red box. At the bottom left of the dialog box, there is a 'Save' button, which is also highlighted with a red box.

## Lab 1: Configure Basic Settings

9. From the **Administration** menu under **SETTINGS**, select **Administrators**, then click the **Add Administrator** link at top right and create a new admin as follows:
  - a. **Admin ID:** Specify **helpdesk@patraining[1-N].safemarch.com**
  - b. **Password:** Set **Admin-123!** (and confirm);
  - c. **Role:** Select the **Helpdesk** role that you just created;
  - d. **Status:** Set to **Enabled**
  - e. **Two Factor Authentication:** Set to **Off**
  - f. **Force Password Reset:** Set to **No**
  - g. **Email:** Add your own email address;
  - h. **Phone:** Add your own phone number;
  - i. **Time Zone:** Select your own time zone;
  - j. Click **Save** to create the new **Administrator**.

**Edit Administrator**

Admin ID  
helpdesk@patraining.safemarch.com

Password  
\*\*\*\*\*

Confirm Password  
\*\*\*\*\*

Role  
Helpdesk

Status <input checked="" type="button"/> Enabled <input type="button"/> Disabled	Two Factor Authentication <input checked="" type="button"/> On <input type="button"/> Off	Force Password Reset <input type="button"/> Yes <input checked="" type="button"/> No
---	--	---

Email  
helpdesk@patraining.safemarch.com

**Save** **Cancel**

10. Log out of the Admin Portal using the using the **Logout** arrow in the navigation bar at bottom left.



11. Log in with the **Helpdesk** user that you just created.
12. Try to navigate back to the **Administration > Administrators** page.  
**Note:** This should fail, as the helpdesk user does not have sufficient permissions to access this page.
13. Log out of the Admin Portal, then log back in as the **administrator** with credentials supplied in the joining instructions email.

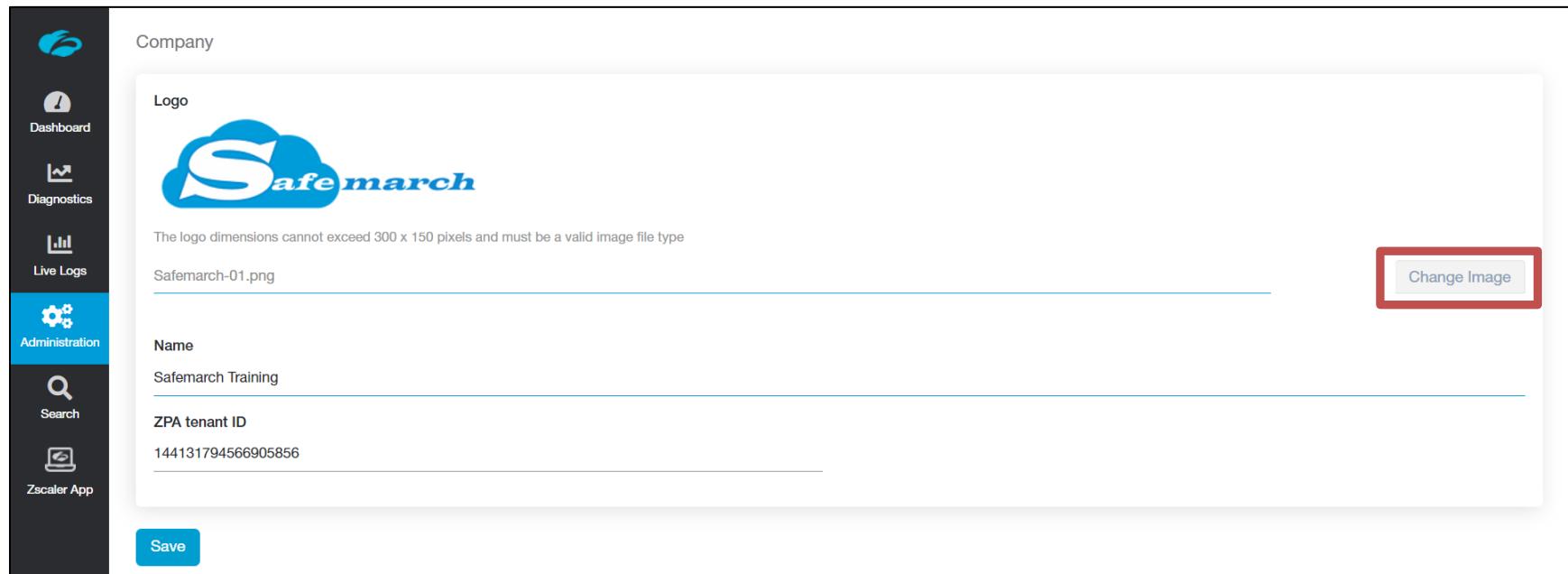
## Lab 1: Configure Basic Settings

### Update Company Data

In this section you will review and configure your Company data.

14. From the **Administration** menu under **SETTINGS**, select **Company**.
15. Click **Select Image**, upload a new image of your choice (maximum dimensions 300 x 150 pixels), and click **Save**.

**Note:** Safemarch and Zscaler image files are available in the \Pictures folder on the Windows VMs, or just pick a suitable image.



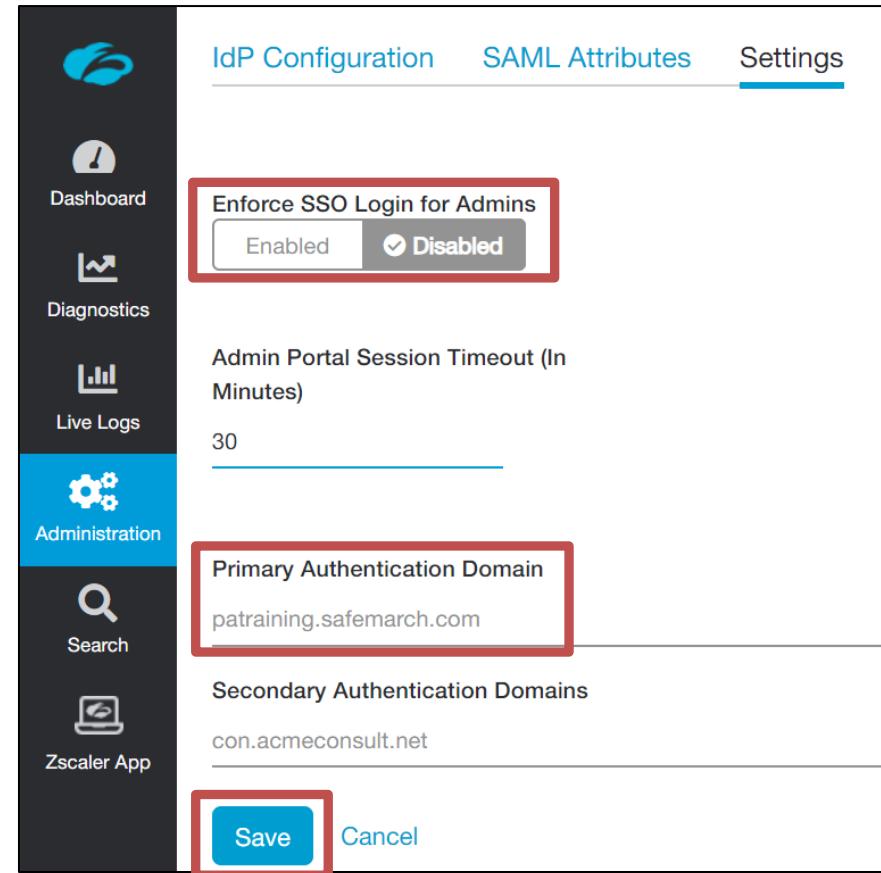
The screenshot shows the 'Company' configuration page in the Zscaler interface. On the left is a dark sidebar with icons for Home, Dashboard, Diagnostics, Live Logs, Administration (which is selected and highlighted in blue), Search, and Zscaler App. The main content area has a light gray header 'Company'. Below it, there's a 'Logo' section featuring a blue cloud icon with the word 'Safemarch' in white. A note says 'The logo dimensions cannot exceed 300 x 150 pixels and must be a valid image file type'. Below the logo is a file input field containing 'Safemarch-01.png'. To the right of the input field is a red-bordered button labeled 'Change Image'. Further down, there are fields for 'Name' (containing 'Safemarch Training') and 'ZPA tenant ID' (containing '144131794566905856'). At the bottom left is a blue 'Save' button.

## Lab 1: Configure Basic Settings

### Manage Settings

In this section you will review SSO settings for administrators and verify your primary authentication domain.

16. From the **Administration** menu under **AUTHENTICATION**, select **Settings**.
17. Verify that the **Enforce SSO Login for Admins** option is set to **Disabled**.
18. Verify your **Primary Authentication Domain** (should be **patraining[1-N].safemarch.com**) and click **Save**.



The screenshot shows the Zscaler Admin UI. On the left is a dark sidebar with icons for Dashboard, Diagnostics, Live Logs, Administration (which is selected and highlighted in blue), Search, and Zscaler App. The main content area has tabs at the top: IdP Configuration, SAML Attributes, and Settings (the latter is selected). Under the Settings tab, there are two sections: 'Enforce SSO Login for Admins' (with a radio button set to 'Disabled') and 'Primary Authentication Domain' (set to 'patraining.safemarch.com'). At the bottom are 'Save' and 'Cancel' buttons, with 'Save' being highlighted by a red box.

## Lab 2: Enable Zscaler Client Connector User Authentication

PATraining users of the Safemarch corporation need to be authenticated against the corporate directory before they are permitted to access internal applications using ZPA. The SAML IdP chosen to authenticate Safemarch users is Azure AD, it has been pre-configured with the users required.

### Verify AAD User Accounts

In this section you will confirm that the AAD accounts you require are available for you.

1. Open a browser and navigate to the Azure portal page at <https://portal.azure.com> and login with the credentials supplied in the joining instructions email.  
**Note:** You can access the Azure portal direct from your own PC using your preferred browser.
2. Navigate to the **Azure Active Directory > Users > All Users** page and verify that the users you will require exist in the directory (the users; **student**, **HVAC** and **smadmin**).

Name	User name	User type	Source
CD	cleach@zscaler.co	Member	Microsoft Account
HV	HVAC	HVAC@patraining21.safe...	Member
PA	patraining21	admin@patraining21.saf...	Member
PE	Paul Ellis	pellis@zscaler.com	Guest
SM	smadmin	smadmin@patraining21....	Member
ST	student	student@patraining21.sa...	Member

## Lab 2: Enable Zscaler Client Connector User Authentication

### Create the unique SP Metadata for the IdP.

With the introduction of the Multi-IdP feature, we now create per-IdP metadata for the ZPA Service Provider (SP). As a result, you must now first begin the process of adding an IdP at the ZPA Admin Portal in order to generate the SP metadata for the IdP, then move to the IdP to add the ZPA SP.

3. In a browser, load the ZPA Admin Portal at <https://admin.private.zscaler.com>, navigate to the page at **Administration > AUTHENTICATION > IdP Configuration** and click **+ Add IdP Configuration** at top right to add a new IdP.

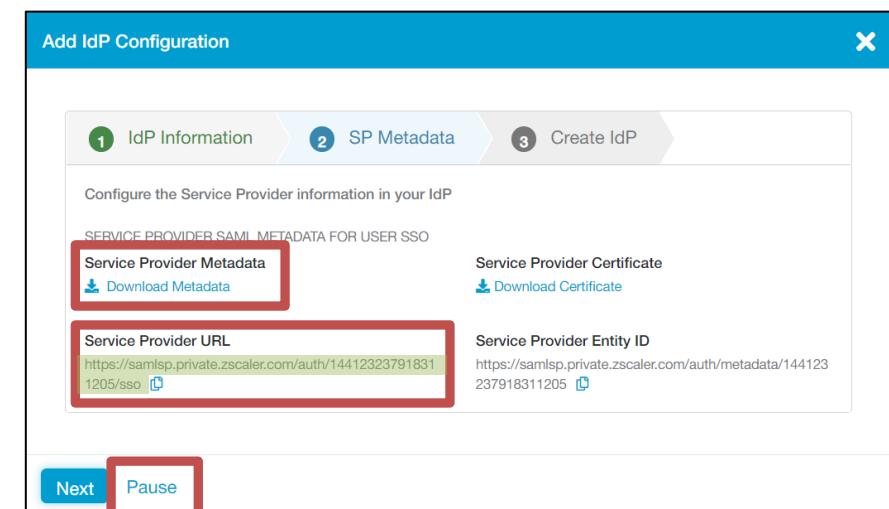
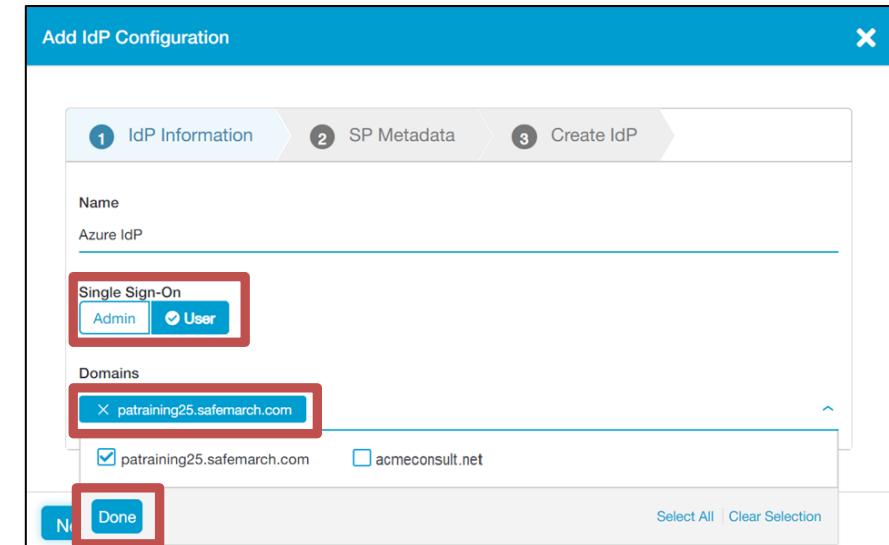
**Note:** You may access the Admin Portal direct from your own PC using your preferred browser.

4. Name the IdP (e.g. Azure), verify that the **Single Sign-On** option is set to **User**.
5. Click **Select a value** in the **Domains** field and select the primary authentication domain for your tenant (**patraining[1-N].safemarch.com**) and click **Done**, then **Next**.

6. At Step 2 of the wizard, the unique SP metadata for the IdP is made available. Click the **Download Metadata** link and save the file to the \Downloads folder with the name **azure\_sp\_metadata.xml**.

7. Highlight and **Copy** the **Service Provider URL** value.

**Note:** You now need to step across to the Azure Portal, you may just leave this wizard open, or you could also click the **Pause** option, which will add the IdP in an incomplete state, to be completed later.



## Lab 2: Enable Zscaler Client Connector User Authentication

### Configure Azure IdP for ZPA

In this section you will configure Azure AD to act as a SAML IdP to allow Zscaler Client Connector user authentication for ZPA access. To do this you will import the SP metadata file that you just downloaded for this IdP from the ZPA Admin Portal.

8. Open a browser and navigate to the Azure portal page at <https://portal.azure.com> and login with the credentials supplied in the joining instructions email.

**Note:** You may access the Azure Admin Portal direct from your own PC in your preferred browser.

9. From the Azure portal, in the left-hand navigation menu click **Azure Active Directory**, then **Enterprise Applications**.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes 'Create a resource', 'All services', 'FAVORITES' (with 'Dashboard' selected), 'All resources', 'Resource groups', 'App Services', and 'Azure Active Directory'. The main content area is titled 'Enterprise applications - All applications' under 'patraining1 - Azure Active Directory'. It shows an 'Overview' card with 'MANAGE' options for 'All applications', 'Application proxy', and 'User settings'. A red box highlights the '+ New application' button in the top right corner.

10. Click **New application**, then type ZPA into the search field under the heading **Add from the gallery**.
11. Click the Zscaler Private Access (ZPA) entry to select it, then click **Add** at bottom right.
12. Select **Users and Groups** and click **Add User**.

**Note:** This step is to authorize a user or group to make use of the ZPA application.

13. Click **Users - None Selected**.
14. Select the three users; **student@patraining[1-N]**, **smadmin@patraining[1-N]** and **hvac@patraining[1-N].safemarch.com**, then click **Select**.
15. Verify that the page indicates **3 users selected**, then click **Assign**.

The screenshot shows the 'Zscaler Private Access (ZPA) - Users and groups' page. The left sidebar includes 'Create a resource', 'All services', 'FAVORITES' (with 'Dashboard' selected), 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Azure Cosmos DB', and 'Virtual machines'. The main content area shows an 'Overview' card with 'Getting started', 'Deployment Plan', 'Manage' (Properties, Owners, Users and groups, Single sign-on), and 'DISPLAY NAME' and 'OBJECT TYPE' fields. A red box highlights the '+ Add user' button in the top right and the 'Users and groups' tab in the sidebar.

The screenshot shows the 'Add Assignment' dialog box. The left sidebar is identical to the previous screenshot. The main content area shows an 'Add Assignment' card with 'Groups are not available for assignment due to your Active Directory plan level.' A red box highlights the 'Users' dropdown set to 'None Selected' and the 'Select' button at the bottom right.

## Lab 2: Enable Zscaler Client Connector User Authentication

16. Click the **Single sign-on** link.

The screenshot shows the Microsoft Azure portal interface. On the left sidebar, under the 'Manage' section, the 'Single sign-on' link is highlighted with a red box. The main content area displays the 'Zscaler Private Access (ZPA) - Single sign-on' configuration page. It includes sections for 'Disabled' (User must manually enter their username and password) and 'SAML' (Rich and secure authentication to applications using SAML). The 'SAML' section is also highlighted with a red box.

17. In the **Select a single sign-on method** list click the **SAML** option.

18. Above the box labelled **1 Basic SAML Configuration**, click the link **Upload metadata file**, browse to find the file **azure\_sp\_metadata.xml** that you saved earlier, select it, click **Open**, then click **Add**.

The screenshot shows the 'Basic SAML Configuration' step of the ZPA Admin Portal. At the top, there is a link labeled 'Upload metadata file' which is highlighted with a red box. Below it, there is a section titled 'Set up Single Sign-On with SAML' with a note to 'Read the [configuration guide](#) for help integrating Zscaler Private Access (ZPA)'. The configuration details are listed in a table:

<b>1 Basic SAML Configuration</b>	<b>Identifier (Entity ID)</b> <small>Required</small>	<b>Reply URL (Assertion Consumer Service URL)</b> <small>Required</small>
	https://samisp.private.zscaler.com/auth/sso	
	<b>Sign on URL</b> <small>Optional</small>	
	<b>Relay State</b> <small>Optional</small>	
	<b>Logout Url</b> <small>Optional</small>	

19. The **Identifier (Entity ID)** URL and the **Reply URL** will be populated automatically, however you will need to correctly configure the **Sign on URL** field. Paste the **Service Provider URL** value that you copied from the **Add IdP Configuration** wizard in the ZPA Admin Portal.

The screenshot shows the 'Sign on URL' field in the 'Basic SAML Configuration' step. The URL 'https://samisp.private.zscaler.com/auth/144123237918311205/sso' is pasted into the input field and is highlighted with a red box. Below the input field, there is a note: 'Patterns: https://samisp.private.zscaler.com/auth/login:domain=EXAMPLE'.

20. Click **Save** at the very top left and close the **Basic SAML Configuration** window. When prompted to **Test single sign-on with Zscaler Private Access (ZPA)** click **No, I'll test later**.

The screenshot shows the 'Basic SAML Configuration' step again. The 'Save' button is highlighted with a red box. Below it, there is a note: 'Identifier (Entity ID) The default identifier will be the audience of the SAML response for IDP-initiated SSO'.

## Lab 2: Enable Zscaler Client Connector User Authentication

21. In the box labelled **② User Attributes & Claims**, click to **Edit** the settings.
22. Verify that the **Unique User Identifier (Name ID)** variable is set to **user.userprincipalname [nameid-format:emailAddress]**. If necessary, **Edit** that variable to ensure that it is correctly mapped to the **user.userprincipalname** attribute.

**Note:** Zscaler best practice here is to use the **UPN** option.

**User Attributes & Claims**

CLAIM NAME	VALUE
Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

**SAML Signing Certificate**

**User Attributes & Claims**

**Add new claim**

CLAIM NAME	VALUE
Unique User Identifier (Name ID)	user.userprincipalname [nameid-format:emailAddress]

**Additional claims**

**Manage claim**

**Save**

<b>Name</b>	Department
Namespace	Enter a namespace URI
<b>Source</b>	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation
<b>Source attribute</b>	user.department
<b>Claim conditions</b>	user.department

**User Attributes & Claims**

**Add new claim**

Name identifier value: **user.userprincipalname**

CLAIM NAME	VALUE
Department	user.department
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail

23. To add a new claim mapping, click **Add new claim**.

24. **Name** the claim **Department**, then from the **Source attribute** drop down list, select **user.department** and click **Save**.

25. Click to close the **User Attributes & Claims** window.

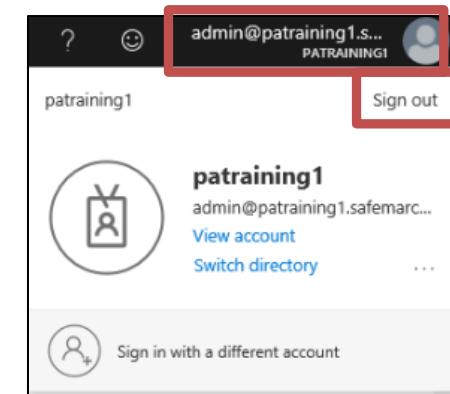
## Lab 2: Enable Zscaler Client Connector User Authentication

26. In the box labelled ③ SAML Signing Certificate, click to Download the Federation Metadata XML and save the file to the \Downloads folder as the file Zscaler Private Access (ZPA).XML. Also download the Certificate (Base64).

The screenshot shows the Azure portal's application registration interface. A specific application is selected, and its configuration details are displayed. Step 3 is highlighted over the 'Download' button next to the 'Federation Metadata XML' link. Step 4 is highlighted over the 'Set up Zscaler Private Access (ZPA)' link at the bottom of the page.

27. Sign out of the Azure portal (top right) and close the browser tab.

**Note:** You need to sign out so that when later testing the configuration from the ZPA Admin Portal you can authenticate with one of the user accounts that you assigned to ZPA in Azure AD. The **admin@** user has not been assigned to the ZPA application in Azure.



### Complete the IdP Configuration in the ZPA Admin Portal

Having configured the IdP to add ZPA as a valid SP, you need to complete the configuration in the ZPA Admin Portal by adding the IdP metadata and (if necessary) the certificate.

28. Go back to the browser tab with the **ZPA Admin Portal** or log back into the Admin Portal. If the **Add IdP Configuration** wizard is still open at **Step 2**, click **Next**. If the IdP configuration was closed, click the **Resume** button.

The screenshot shows the ZPA Admin Portal's IdP Configuration table. The table lists a single entry for 'Azure IdP'. The 'Actions' column for this entry contains a blue circular icon with a white plus sign and a red 'x' icon. This row is circled with a red circle.

Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure IdP	Idle		User	<span style="color: blue;">+</span> Add IdP Configuration <span style="color: red;">x</span>

## Lab 2: Enable Zscaler Client Connector User Authentication

29. Next to the **IdP Metadata File** field click **Select File**, navigate to and select the IdP metadata file named **Zscaler Private Access (ZPA).XML** that you just saved out of Azure and click **Open**.

Add IdP Configuration

1 IdP Information    2 SP Metadata    3 Create IdP

GENERAL INFORMATION

Name  
Azure IdP

IdP Metadata File  
Upload Metadata File

IdP Certificate  
Upload the Certificate File...

30. Scroll down and verify that the configuration is complete and includes the **IdP certificate**.

**Note:** If the certificate details are blank or show **Undefined**, you will also need to upload the **Certificate (Base64)** file that you previously downloaded from Azure. The IE browser on the server VM does not always parse the metadata file correctly and read in the certificate.

31. Configure the settings as follows:

- Domains** (at the top): Verify that your primary authentication domain is selected (**patraining[1-N].safemarch.com**);
- Status**: Set to **Enabled**;
- ZPA (SP) SAML Request**: Set to **Signed**;
- HTTP-Redirect**: Set to **Enabled**.

32. Click **Save** to finalize the configuration of the IdP.

Add IdP Configuration

1 IdP Information    2 SP Metadata    3 Create IdP

IdP Certificate  
Upload the Certificate File...

-----BEGIN CERTIFICATE-----  
MIIC8DCCAdigAwIBAgIQbxetcru97mrBFCMJE120lRjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD  
EyNaWNyb3NvZnQgQxptcmUgRmVkJhdGVkIjNTyBDZXJ0aWZpY2F0ZTAeFwoxOTA2MjQwO  
Dj3MzFaFw0yMjA2MjQwODI3MzFaMDQzMjAwBgNVBAMTKU1pY3Jvc29mdCBvBenzYzSBGZWRIc  
mF0ZWQgU1NPtENlcRpZmljYXRIMIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmnXLj

Single Sign-On URL  
<https://login.microsoftonline.com/1b85b0ba-9372-4582-a1dc-5b264ab307c4/saml2>

IdP Entity ID  
<https://sts.windows.net/1b85b0ba-9372-4582-a1dc-5b264ab307c4/>

Status  Enabled  Disabled    ZPA (SP) SAML Request  Signed  Unsigned

HTTP-Redirect  Enabled  Disabled

## Lab 2: Enable Zscaler Client Connector User Authentication

33. Click the name of the IdP that you just added, to expand the details for it and next to the Import SAML Attributes item click Import.

Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure IdP	<span style="color: green;">✓</span>	https://sts.windows.net/1b85b0ba-9372-4582-a1dc-5b264ab307c4/	User	<span style="color: blue;">Edit</span> <span style="color: red;">Delete</span>

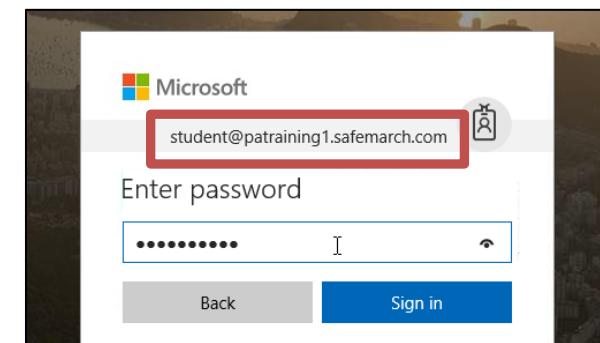
Single Sign-On URL: https://login.microsoftonline.com/1b85b0ba-9372-4582-a1dc-5b264ab307c4/saml2  
 Authentication Domains: patraining4.safemarch.com  
 Import SAML Attributes: patraining4.safemarch.com Import

SERVICE PROVIDER SAML METADATA FOR USER SSO  
 Service Provider Metadata: [Download Metadata](#)  
 Service Provider URL: https://samlsp.private.zscaler.com/auth/144123237918311206/sso [Edit](#)

IdP CERTIFICATE  
 Common Name: Microsoft Azure Federated SSO Certificate  
 Created On: Monday , June 24 2019 3:27:31 pm  
 Serial Number: 147686379388806261393120480617086920006  
 Expires On: Friday , June 24 2022 3:27:31 pm

34. A new browser tab will open and take you to the Azure login page, click Use another account and login with the student credentials:

- Username: student@patraining[1-N].safemarch.com
- Password: Admin-123!



## Lab 2: Enable Zscaler Client Connector User Authentication

35. You should be logged into Azure and taken to the ZPA Admin Portal **Import SAML Attributes** page where a list of the attributes provided by Azure is shown.

**Note:** Only new attributes will be listed, if an attribute is already configured in the ZPA Admin Portal it will not be shown.

36. We recommend that you change the names of these attributes, to remove the Microsoft protocol and schema prefixes. To change the names of the attributes to make them shorter and easier to find in the Access Policy configuration interface, simply click in each of the **Name** fields and enter the **Name** value that you prefer.

**Note:** This step is optional, although it makes it much easier to find the attribute you need when creating Access Policy rules.

Name	SAML Attribute Name
TenantID_Azure	http://schemas.microsoft.com/identity/claims/tenantid
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/objectidentifier
http__schemas__microsoft__com__identity__claims__displayname_Azure	http://schemas.microsoft.com/identity/claims/displayname
http__schemas__microsoft__com__ws__2008__06__identity__claims__groups_Azure	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
http__schemas__microsoft__com__identity__claims__identityprovider_Azure	http://schemas.microsoft.com/identity/claims/identityprovider

37. Also included on this page (at the bottom), is a JSON listing of the attribute values returned by AAD for the user that you authenticated as.

**Note:** This list is for informational purposes only, it can also be used for troubleshooting purposes, to identify exactly what attribute **values** have been applied to this user.

```
{
  "nameid": "student@patraining8.safemarch.com",
  "orgId": "144123242213277696",
  "idpEntityID": "https://sts.windows.net/d26680f9-be1c-4246-a4e4-be4e7cb090e1",
  "idpId": "144123242213278253",
  "saml_attributes": {
    "http://schemas.microsoft.com/identity/claims/tenantid": "d26680f9-be1c-4246-a4e4-be4e7cb090e1",
    "http://schemas.microsoft.com/identity/claims/objectidentifier": "96076a21-fbdc-4f2b-b4ce-35bc16aa99b4",
    "http://schemas.microsoft.com/identity/claims/displayname": "student PATraining8",
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/groups": "b47d244d-c5ac-47f4-9712-b3f06002e9b5",
    "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/d26680f9-be1c-4246-a4e4-be4e7cb090e1",
    "http://schemas.microsoft.com/claims/authnmethodreferences": "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "student",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "PATraining8",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress": "student@patraining8.safemarch.com",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "student@patraining8.safemarch.com",
    "Department": "Marketing"
  }
}
```

## Lab 2: Enable Zscaler Client Connector User Authentication

38. Once you have changed the names for the attributes, to import them and make them available for use in Access Policy configurations, click **Save**.

Surname_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
EmailAddress_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name_Azure	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Department_Azure	Department

**Save** **Cancel**

39. You will be taken to the **SAML Attributes** page, where the full list of attributes available for ZPA (that have either been imported or created) will be shown.

**Note:** The actual attributes sent can be customized within your Azure AD admin portal. Zscaler can use any of the attributes provided by this or any other IdP that you add to control access to applications in your Access Policy rules. You have the option to filter this list to see only the attributes provided by Azure AD. If you delete the Azure IdP Configuration, all these Attributes will also be removed.

Name	SAML Attribute	IdP Name	Actions
AuthnMethodsReferences_Azure	http://schemas.microsoft.com/claims/authnme...	Azure	
ObjectIdentifier_Azure	http://schemas.microsoft.com/identity/claims/...	Azure	
TenantID_Azure	http://schemas.microsoft.com/identity/claims/t...	Azure	
Department_Azure	Department	Azure	

40. Close the new browser tab, go back to the Azure Admin Portal, reload the page and **Sign Out** as the user **student@patraining[1-N].safemarch.com**.

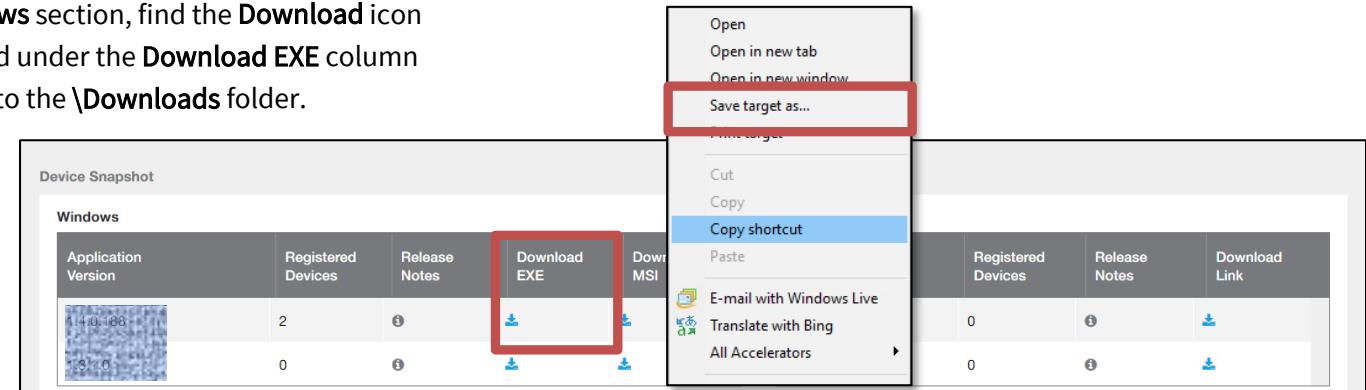
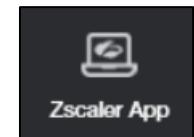
## Lab 3: Provision ZPA Infrastructure

The Safemarch users will connect to applications using the Zscaler Client Connector, so that must be installed on their domain-joined PCs. Applications are hosted on the Windows server in the Datacenter, so an on-premise App Connector is required.

### Install Zscaler Client Connector

The Zscaler Client Connector is required on the domain-joined corporate client PCs. In this section you will simply download the .EXE file directly from the Zscaler Client Connector Portal and run the install executable.

1. Go to the VM named **Corp: Client PC** and login to Windows as the user **Student test**, with password **Admin-123!**
2. Load a browser and login to the ZPA Admin Portal (<https://admin.private.zscaler.com>), login as the admin user then click the **Zscaler Client Connector** icon in the left-hand navigation menu to open the Zscaler Client Connector Portal in a new browser tab.  
**Note:** You need to access the Admin Portal from the Windows Client PC, to download and run the installer executable.
3. Navigate to the **Administration > Zscaler App Store** page and check that you are on the **PERSONAL COMPUTERS** tab.
4. Under **Device Snapshot**, in the **Windows** section, find the **Download** icon for the *latest version* of the App listed under the **Download EXE** column (should be **>2.1.2**). Download the file to the **\Downloads** folder.

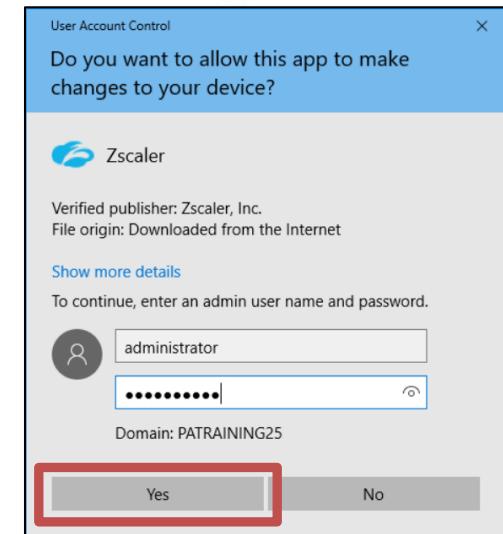
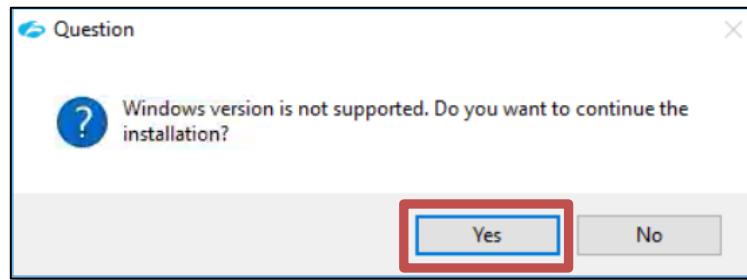


A screenshot of the Zscaler App Store interface. On the left, there's a table titled "Device Snapshot" for the "Windows" section. It shows two rows of data. The first row has Application Version 1.4.0.188, Registered Devices 2, Release Notes, and a "Download EXE" button with a red box around it. The second row has Application Version 1.3.1.6, Registered Devices 0, Release Notes, and a "Download EXE" button. To the right of the table is another table with columns: Registered Devices, Release Notes, and Download Link. A context menu is open over the "Download EXE" button in the first row. The menu options are: Open, Open in new tab, Open in new window, Save target as... (which is highlighted with a red box), Print target, Cut, Copy, Copy shortcut (which is blue), Paste, E-mail with Windows Live, Translate with Bing, and All Accelerators.

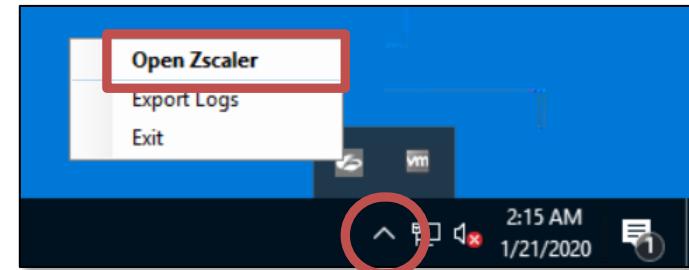
5. In Windows **File Explorer**, open the **\Downloads** folder and find the downloaded installer file.
6. Double-click on the installer file to start the install process.

### Lab 3: Provision ZPA Infrastructure

7. Login in as the user **Administrator** with password **Admin-123!** and follow the prompts to install the App.
8. At the unsupported Windows version prompt, click **Yes** to continue the installation.

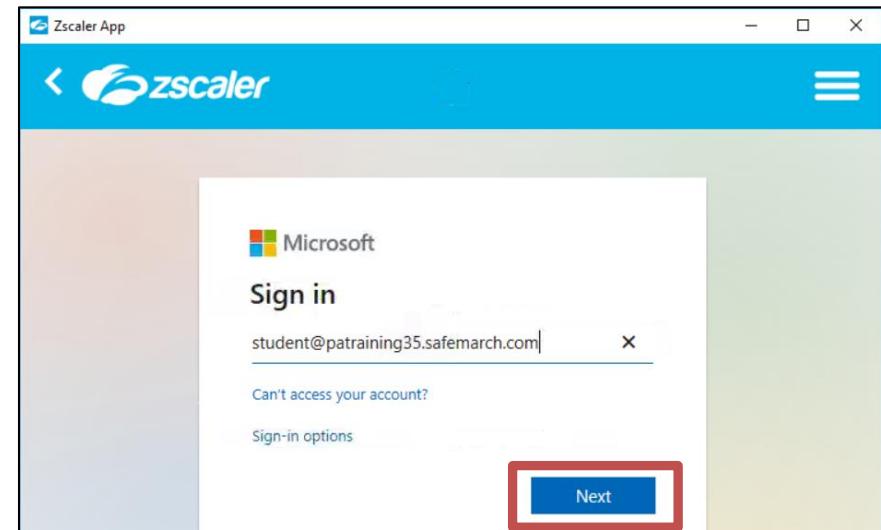


9. If necessary, from the Windows Status Bar, click to **Show hidden icons**, click on the **Zscaler Client Connector**, then click **Open Zscaler**.



10. When the Zscaler Client Connector UI opens, enter the username **student@patraining[1-N].safemarch.com** and click **Login**.
11. When you are redirected to Azure to authenticate, login with the username **student@patraining[1-N].safemarch.com** and password **Admin-123!**
12. **When Azure prompts you to stay logged in, click No!**

**Caution:** It is the system browser that does the SAML authentication. If you tell the browser to 'remember' the user, then that is exactly what the browser will do! You can log out of Z App and try to log in as someone else, but the browser will just log you straight back in as the user you told it to remember. For a single user device this is no problem, however in the Lab you will be logging to Z App with other user IDs.

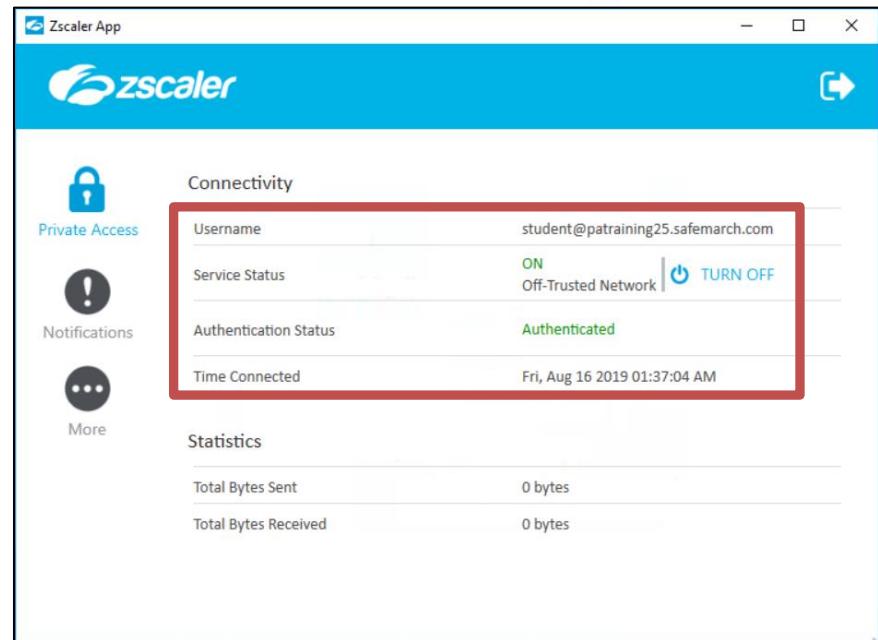


### Lab 3: Provision ZPA Infrastructure

13. Open the Zscaler Client Connector and on the **Private Access** page, confirm that **Service Status** indicates **ON**, that **Authentication Status** indicates **Authenticated**, and that the username is correct.

14. Open a **Command** prompt and try to ping the host **intranet.patraining[1-N].safemarch.com**. Also try to access that page in a browser.

**Note:** Both the ping and the browser request should fail as, although the ZPA service is active, that application is not yet configured as being available over ZPA.



### Provision an App Connector

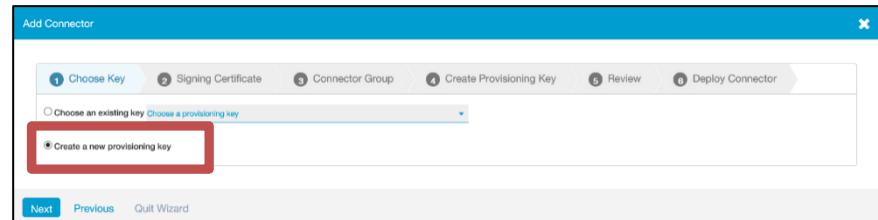
A CentOS-based App Connector has already been installed on the corporate network for you, configured with appropriate network, DNS, and NTP settings. In this section, you will activate it by providing a valid provisioning key created at the ZPA Admin Portal.

15. On the VM labelled **Corp: Win Svr 2016**, open a browser and go to the URL <http://admin.private.zscaler.com>.
  16. Log into the **ZPA Admin Portal** using the credentials assigned to you in the student access information that you received (**admin@patraining[1-N].safemarch.com**).
- Note:** For this lab, you must access the ZPA Admin Portal in a browser on the Windows 2016 server, as you need to download a provisioning key to install to the App Connector VM.
17. From the **Administration** menu under **CONNECTOR MANAGEMENT**, select **Connectors**.

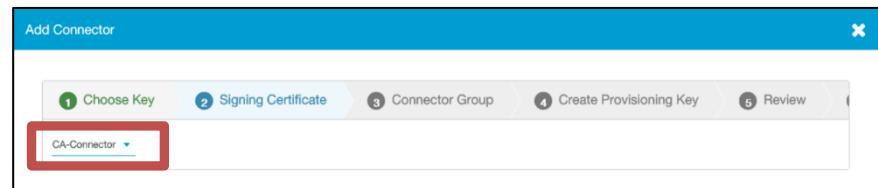
### Lab 3: Provision ZPA Infrastructure

18. Click the Add Connector icon at top right to add a new App Connector and step through the wizard as follows:

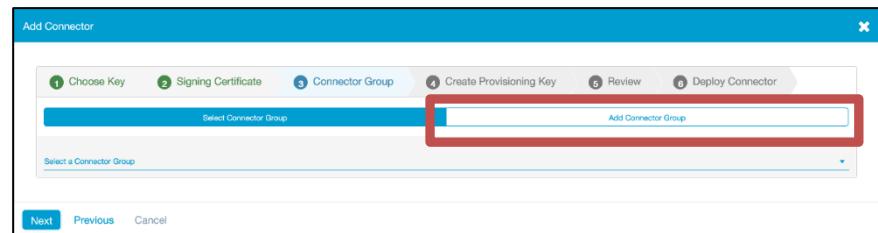
a. Select Create a new provisioning key and click Next.



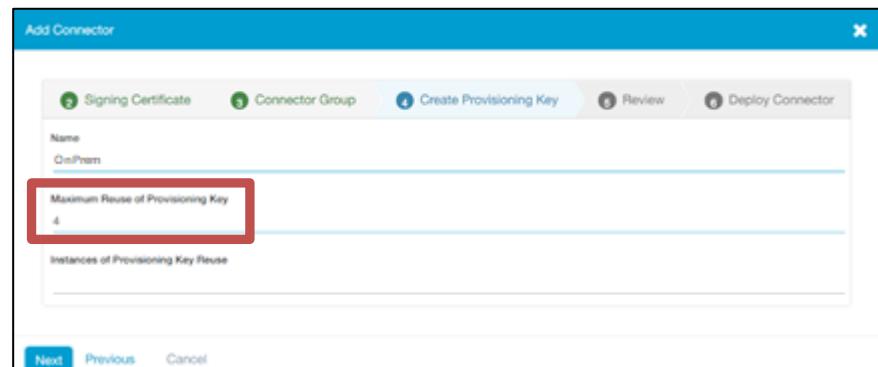
b. Click Choose a certificate and select the certificate named **Connector**, then click Next;



c. Click Add Connector Group;



d. Name the group **OnPrem**, add a description if you wish, set the **Connector Software Update Schedule** to occur on **Sundays at 00:30**, and specify the location as **NYC, NY, USA**, then click Next;

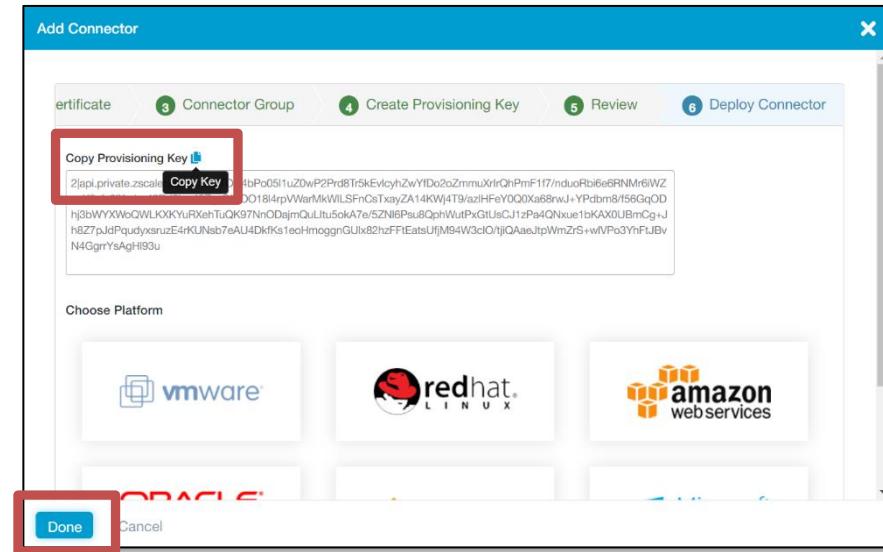


e. Name the Provisioning Key **OnPrem** and specify a **Maximum Reuse of Provisioning Key** of **4**, then click Next;

f. Review the App Connector settings and click Save;

### Lab 3: Provision ZPA Infrastructure

- g. By the **Copy Provisioning Key** text, click the **Copy ID** icon (it should show the caption **Copied**);  
**Note:** Alternatively, you can right click and **Select all** data in the Provisioning Key field, then right click again and select **Copy**.
- h. Click the Windows **Start** menu, type **Notepad** and open that application, right-click and select **Paste** to paste the Provisioning Key text into the file;
- i. Save the file to the desktop with the name **provision\_key.txt** and close Notepad.
- j. Click **Done**.



19. Open Windows **File Explorer** and navigate to the provisioning key that you just saved. If necessary, from the **View** menu enable the **file name extensions** option, then rename the file to remove the extension, so the name is just **provision\_key**. Confirm the change to the file extension.
20. In the **ZPA Admin Portal**, click **Connector Groups** to confirm that the group has been created, click on the name of the group to review details.
21. Click **Connector Provisioning Keys** to confirm that a key has been created to support a maximum of 4 App Connectors.

### Activate the App Connector

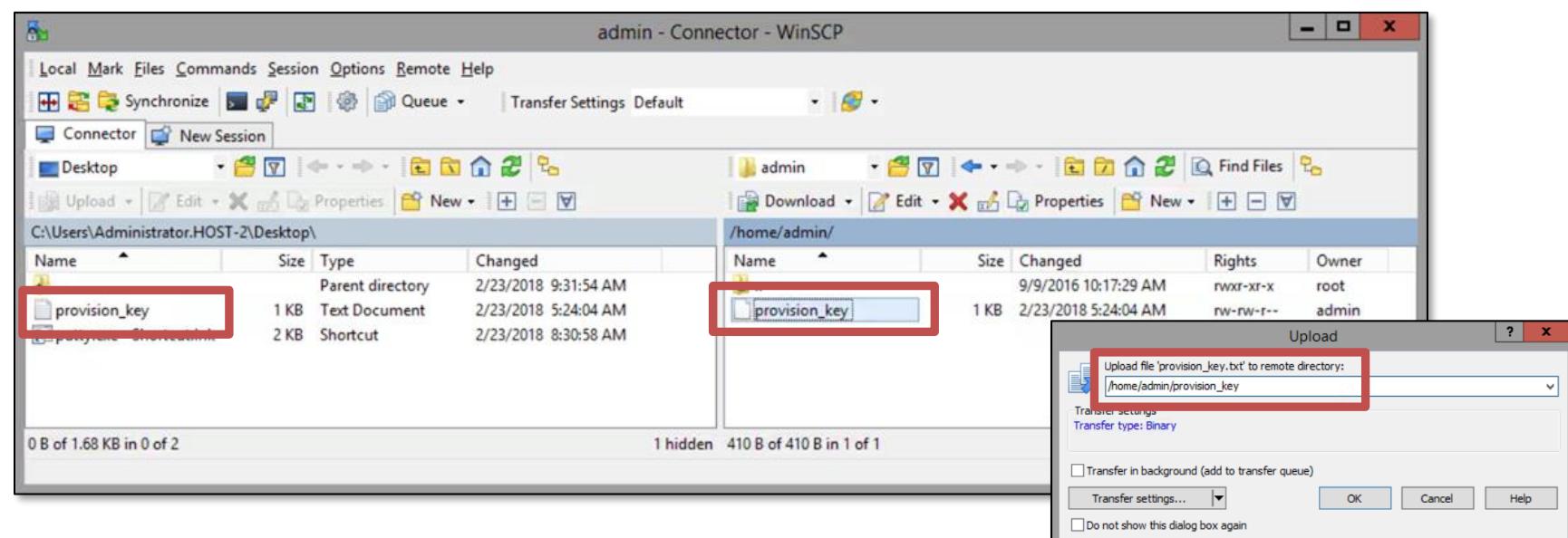
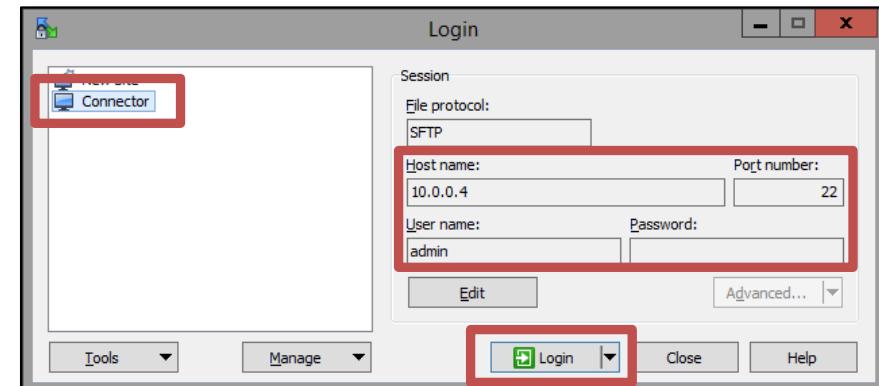
A prebuilt App Connector VM has been provided, with basic networking, DNS, and NTP configured. You need to activate the App Connector software on this VM and provide the provisioning key value that you saved to the Windows server. You must first enable the SSH Daemon on the App Connector to allow the transfer of the provisioning key file from the Windows server. Finally, the App Connector is still set to use the default password, so you will change it to a more secure value.

22. On the VM labelled **Corp: ZPA Connector**, login with the default username / password (**admin / zscaler**).
23. Start the **SSH Daemon** on the App Connector by entering the command: **sudo systemctl start sshd** (enter the password **zscaler** when prompted).
24. Verify that the **SSHD Daemon** has started using the command **sudo systemctl status sshd**, confirm that status is **active (running)**.

### Lab 3: Provision ZPA Infrastructure

25. On the VM labelled **Corp: Win Svr 2016**, copy the provisioning key file to the Connector:

- Start **WinSCP** using the icon on the desktop or in the taskbar;
- Load the saved session named **Connector** (IP address **10.0.0.4**, Port **22**) and click **Login**;
- Login to the App Connector using the default user password (**zscaler**), accept the certificate if necessary;
- In the left-hand panel of WinSCP (the local Windows server), navigate to the **Desktop** folder and select the file **provision\_key**;
- Right-click on the file and select **Upload**;
- Specify the path on the App Connector as **/home/admin/provision\_key** and click **OK**;



26. Verify that the file is uploaded and close WinSCP.
27. On the VM labelled **Corp: ZPA Connector**, stop the **SSH Daemon** on the App Connector by entering the command: **sudo systemctl stop sshd** (enter the password **zscaler** if prompted). Check that the **SSHD Daemon** has stopped using the command **sudo systemctl status sshd**.

**Note:** Under most circumstances, for security reasons it is not recommended that you start the SSH Daemon and just leave it running.

### Lab 3: Provision ZPA Infrastructure

28. Activate the App Connector with the new provisioning key file:

- First identify the current directory with the command `pwd` (you should be in `/home/admin`);
- List the contents of the directory with the command `ls` and confirm that the file `provision_key` is there;
- Stop the App Connector service with the command `sudo systemctl stop zpa-connector` (enter the password `zscaler` if prompted);
- Copy the file to the correct Zscaler directory using the command `sudo cp provision_key /opt/zscaler/var/provision_key`

**Caution:** The name of the file is critical to the correct loading of the provisioning key; *it is case sensitive!*

- Check that the file is there using the command `sudo ls /opt/zscaler/var/`
- Now restart the App Connector service with the command `sudo systemctl start zpa-connector`
- Wait about 10s, then check the status of the App Connector service using the command `sudo systemctl status zpa-connector`
- Verify that it is active and has established a connection to the ZPA infrastructure.
- Run the command `sudo ls /opt/zscaler/var` again and review the contents of that folder now that the App Connector has enrolled.

**Note:** You should now see a set of key and certificate `.pem` files.

```
[admin@zpa-connector ~]$ 
[admin@zpa-connector ~]$ systemctl status zpa-connector
● zpa-connector.service - Zscaler Private Access Connector
  Loaded: loaded (/usr/lib/systemd/system/zpa-connector.service; enabled; vendor preset: enabled)
  Active: active (running) since Tue 2018-02-27 02:07:20 PST; 14min ago
    Main PID: 1152 (zpa-connector)
   CGroup: /system.slice/zpa-connector.service
           └─1152 /opt/zscaler/bin/zpa-connector
             ├─1735 zpa-connector-child

Feb 27 02:20:24 zpa-connector zpa-connector-child[1735]: Time skew: - 0.005375s
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: ----- Connector Status:ID=144123139134062609;Name=Training-1;Ver=17.81.2 -----
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Certificate will expire in 374 days, 14 hours, 32 minutes, 42 seconds
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Control connection state: foeh_connection_connected, [10.0.0.41]:50038:broker1.nyc3.prod.zpat...2541:443
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: RPC Messages: BrkRq = 0, BrkRqAck = 0, BindReq = 0, BindReqAck = 0, AppRtDisc = 0, AppRtReq ...tChk = 0
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Broker data connection count = 0, backed_off connections = 0
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Data Transfer: Total ToBroker = 0 bytes, Total FromBroker = 0 bytes
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Mtnnells: Total Created = 0, Total Freed = 0, Current Active = 0, Alloc = 0, Free_q_cnt = 0
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Registered apps count = 0, alive app = 0, passive_health = 0, service_count = 0, target_coun...rget = 0
Feb 27 02:21:24 zpa-connector zpa-connector-child[1735]: Time skew: - 0.005760s
Hint: Some lines were ellipsized, use -l to show in full.
[admin@zpa-connector ~]$ pwd
```

29. On the VM labelled **Corp: Win Svr 2016**, in a browser, login to the ZPA Admin Portal, navigate to the **Administration > CONNECTOR MANAGEMENT > Connectors** page and confirm that the App Connector is listed.

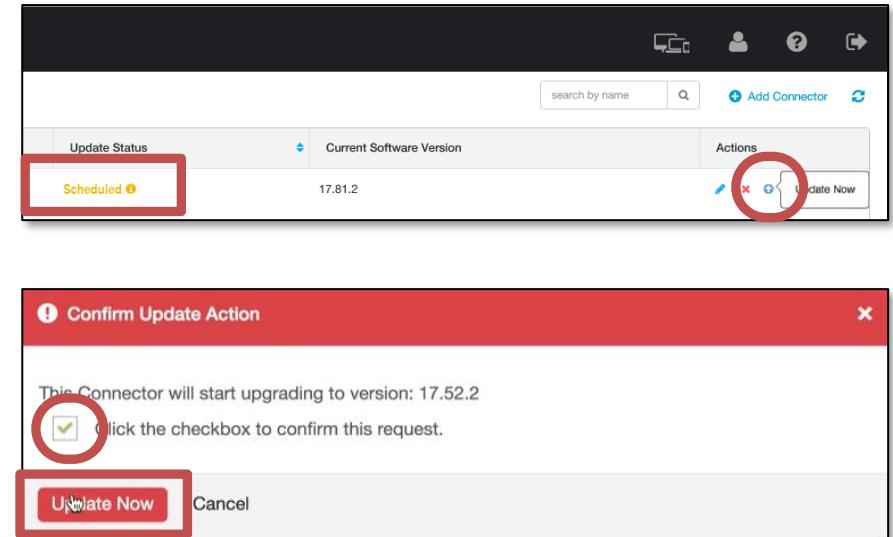
Name	Status	Session	Update Status	Current Software Version	Actions
OnPrem-1	✓	Authenticated	Success	19.60.1	

### Lab 3: Provision ZPA Infrastructure

30. Check the **Update Status** field for the App Connector. If it is blank, or indicates **Failure**, refresh the page, or navigate away from the page and come back to it, the status should change to either **Success** or **Scheduled**:

- If it indicates **Success**, this means that the App Connector is at the latest version of software and no update is necessary.
- If it indicates **Scheduled**, this means that a software update is required and will take place automatically at the next scheduled update interval for the App Connector Group.
  - To manually start the update immediately, click the **Update Now** control for the App Connector, in the pop-up window click in the check box to confirm the request, then click **Update Now**.
  - Return to the **Connector** page in a few minutes to verify that the update is complete.

**Note:** There is no need to wait for the App Connector to update, continue with the lab and check back in a few minutes.



31. On the VM labelled **Corp: ZPA Connector**, it is recommended that you change the admin user password on the App Connector to a more secure value:

- Enter the command **passwd**;
- Enter the current password (**zscaler**);
- Enter the new password **Zscaler-123!**
- Re-enter the new password;
- Enter the command **exit**;
- Log back into the App Connector VM using the new password.
- Once you have confirmed that you can log in successfully with the new password, log back out using the command **exit**.

## Lab 4: Add an Application

The ZPA infrastructure components are all now in place (SAML IdP, Zscaler App and Zscaler Client Connectors). You now need to add applications for the end users to connect to. Remember ZPA will not give *anyone* access to *anything* unless an application is defined (or discovered), AND there is an Access Policy rule that allows access. In this lab you will manually add the **Intranet** application and create a specific Access Policy Allow rule for it.

### Add the Intranet Application

In this section you will manually add an Application Segment and Access Rule for access to the corporate Intranet server on TCP ports 80 and 443.

1. In a browser, open and login to the **ZPA Admin Portal**. From the **Administration** menu under **APPLICATION MANAGEMENT**, go to the **Application Segments** page.  
**Note:** You can also access the Admin Portal directly, in a browser on your own PC.
2. Click the **Add Application Segment** link at top right to add a new **Application Segment** and add an **HTTP/S** application for access to the corporate intranet. At the **Define Application** step of the wizard, configure the following:
  - a. In the **General Information** section, set the **Name** for the application to **Intranet**, set the **Status** to **Enabled** and add a suitable description;
  - b. In the **Applications** section, click in the **Enter a domain or IP address** field and specify **intranet.patraining[1-N].safemarch.com**;
  - c. In the **Zscaler App Access** section, specify a **TCP Port Range** from **80** to **80**. Click **Add More** and add the range from **443** to **443**;
  - d. Do not add a **UDP Port Range**;

**GENERAL INFORMATION**

**Name:** Intranet **Status:** Enabled

**APPLICATIONS**

intranet.patraining1.safemarch.com  Browser Access

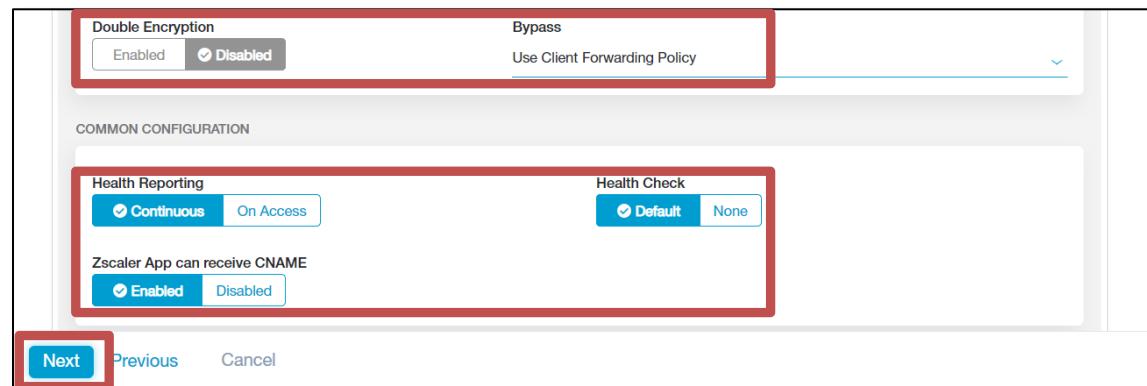
**ZSCALER APP ACCESS**

**TCP Port Ranges:** 80 80

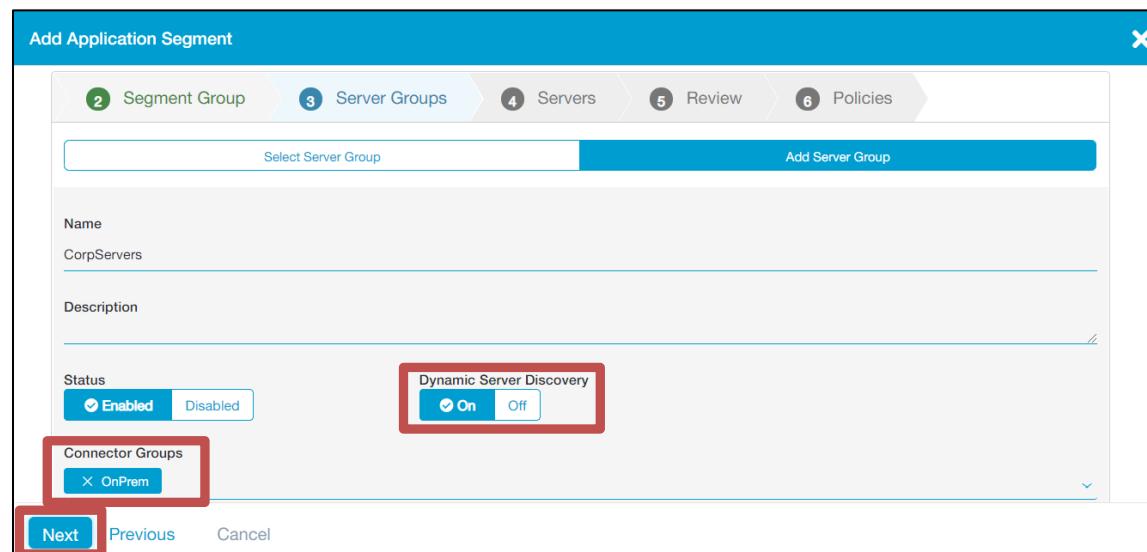
**UDP Port Ranges:** From... To...

## Lab 4: Add an Application

- e. In the ADDITIONAL CONFIGURATION section, set Double Encryption to Disabled and Bypass to Use Client Forwarding Policy;

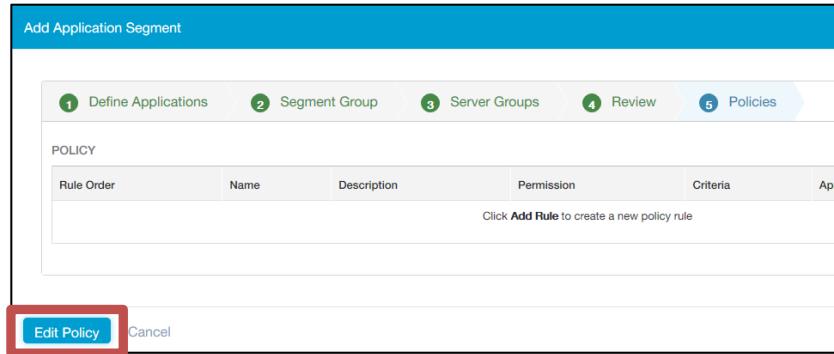


- f. In the COMMON CONFIGURATION section, set Health Reporting to Continuous, Health Check to Default and Zscaler App can receive CNAME to Enabled, then click Next;
3. At the Segment Group step of the wizard, click Add Segment Group, name the group CorpApps, optionally add a description, verify that the Status is set to Enabled, and click Next.
  4. At the Server Groups step of the wizard, click Add Server Group, name the group CorpServers, optionally add a description, verify that the Status is set to Enabled, set Dynamic Server Discovery to On, select the App Connector group OnPrem that you created earlier, click Done then click Next.



## Lab 4: Add an Application

5. At the **Review** step click **Save**.
6. To add an Access Policy rule for this application, click **Edit Policy**.



The screenshot shows the 'Add Access Policy' dialog box. It includes fields for 'Name' (Allow Intranet) and 'Description' (Allow rule for access to Safemarch Training Intranet pages). The 'ACTION' section has a 'Rule Action' dropdown set to 'Allow Access' (highlighted by a red box), with 'Block Access' as an option. The 'CRITERIA' section contains several AND/OR conditions: 
 

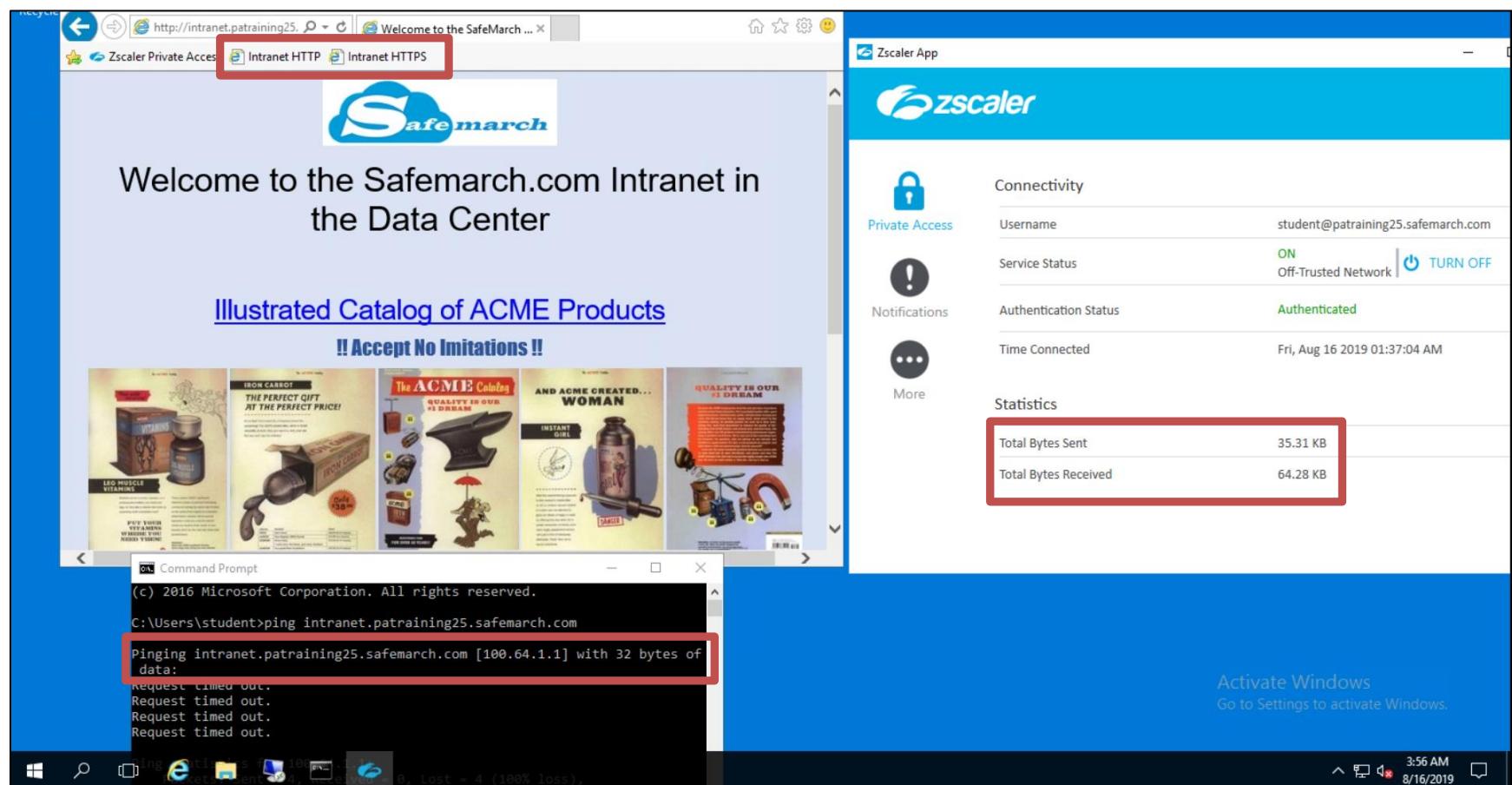
- Application Segments:** An 'Intranet' segment is selected (highlighted by a red box).
- SAML Attributes:** 'Azure' is selected under 'Any SAML attribute' (highlighted by a red box). A 'Select IdP' button is shown to its right.
- Client Types:** 'Any client type' is selected (highlighted by a red box).
- Zscaler App Posture Profiles:** 'Select a posture profile' is shown.
- Zscaler App Trusted Networks:** 'Select one or more trusted networks' is shown.

 There are also 'Add More' and 'Save' (highlighted by a red box) buttons at the bottom.

7. Add a policy rule to allow access to this application as follows:
  - a. On the **Access Policy** page, click **+ Add Rule**;
  - b. Name the rule **Allow Intranet** and optionally add a description;
  - c. Set the **Action** to **Allow Access**;
  - d. In the **Application Segments** field, select the **Intranet** application segment that you just created and click **Done**;
  - e. Click **Select IdP** and select the **Azure** IdP you added in Lab 2, set the **SAML Attributes** to **Any SAML Attribute**;
  - f. Set the **Client Types** to **Any client type**;
  - g. Do not select any **Zscaler App Posture Profiles**;
  - h. Do not select any **Zscaler App Trusted Networks**;
  - i. Click **Save**.

## Lab 4: Add an Application

8. Login to the VM labelled **Corp: Client PC**, open a web browser in a window and open the **Zscaler Client Connector** adjacent to it, so you can see the traffic counters as you load web pages.
9. Try to access the intranet page at **HTTP://intranet.patraining[1-N].safemarch.com** (a bookmark is provided) and confirm that the intranet page loads.
10. Also try to access the intranet page using **HTTPS** (a bookmark is provided) and confirm that the intranet page loads.
11. From the Windows **Start** menu, open a **Command** prompt and ping the host name at **intranet.patraining[1-N].safemarch.com**. Verify that it resolves to a **100.64.1.x** IP address (indicating that it is reachable using ZPA), but that it does not respond to pings.
12. In the browser, refresh the page and view the **Total Bytes Sent** and **Total Bytes Received** counters in the Zscaler Client Connector and confirm that they are now incrementing.



## Lab 5: Discover Corporate Applications

The ZPA service is now active and the end user has access to the one defined application. But what about the other domain applications that they may need access to? A useful way to find the applications that end users actually need, is to configure ZPA for application discovery.

### Configure Application Discovery

In this section you will add an Application Segment in the ZPA Admin Portal, configured to allow application discovery. You will also add a DNS Search Domain to allow application discovery using short names (rather than FQDNs).

1. On the VM labelled **Corp: Win Svr 2016**, open a browser, navigate to and login to the **ZPA Admin Portal**. From the **Administration** menu under **APPLICATION MANAGEMENT**, go to the **Application Segments** page.

**Note:** You can also access the Admin Portal directly, in a browser on your own PC.

2. Click the **DNS Search Domains** icon at top right to add a new **Search Domain**:

- a. Add the domain **patraining[1-N].safemarch.com**;
- b. Enable the **Domain Validation in Zscaler App** option and click **Save**.

**Note:** This will allow the discovery of applications on this domain requested using a short name only. The **Domain Validation** option gives Zscaler Client Connector first go at resolving these derived FQDNs (and is a recommended best practice).

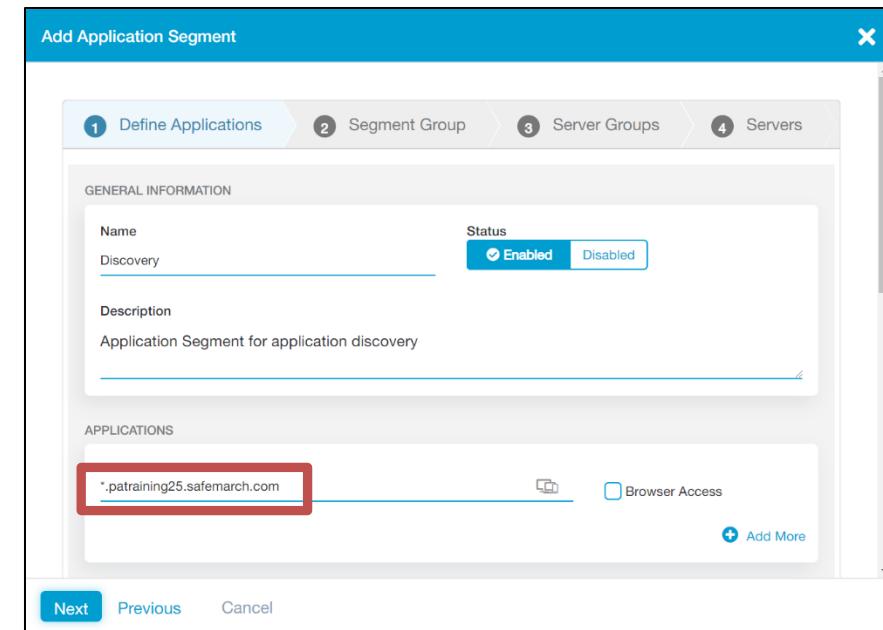


3. Click the **Add Application Segment** icon at top right to add a new **Application Segment**.

**Note:** Here you will configure an Application Segment for application discovery using a wildcard domain on just about all TCP and UDP ports.

4. At the **Define Applications** step of the wizard, configure the following:

- a. In the **GENERAL INFORMATION** section, set the **Name** for the application to **Discovery**, set the **Status** to **Enabled** and add a suitable **Description**;



## Lab 5: Discover Corporate Applications

- c. Scroll down, and in the **ZSCALER APP ACCESS** section, specify a **TCP Port Range** from **2** to **52**, click **Add More** and add the range **54** to **65535**;

**Note:** We will need to use TCP port 1 with this FQDN in another rule later.

- d. Add a **UDP Port Range** of **1** to **52**, click **Add More** and add the range **54** to **65535**;

**Note:** Zscaler recommends that you exclude TCP and UDP port 53 so as not to interfere with the operation of DNS.

- e. Leave the **Double Encryption** option at **Disabled**, and the **Bypass** option at **Use Client Forwarding Policy**;

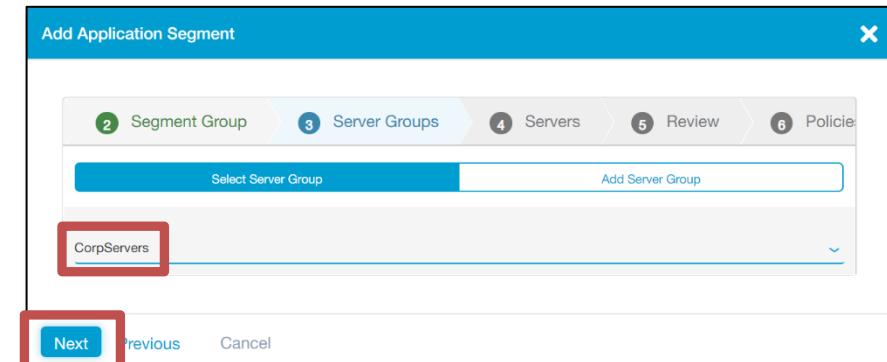
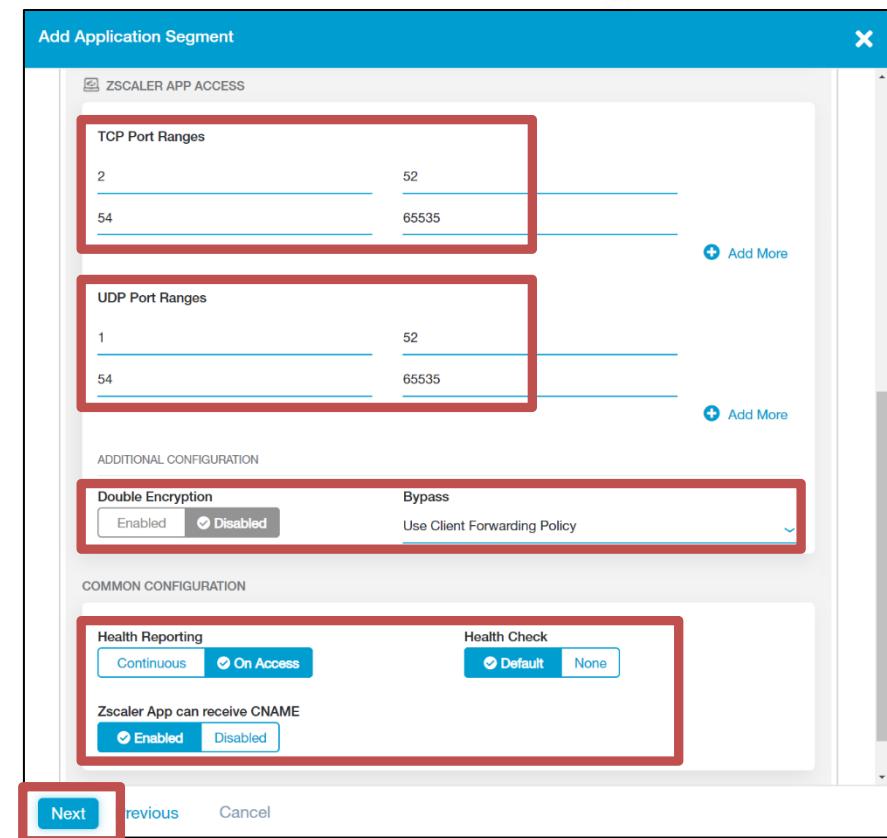
- f. Scroll down and in the **COMMON CONFIGURATION** section, set **Health Reporting** to **On Access**, **Health Check** to **Default** and **Zscaler App can receive CNAME** to **Enabled**;

- g. Then click **Next**;

5. At the **Segment Group** step of the wizard, click **Add Segment Group**, name the group **Discovered**, optionally add a description, verify that the **Status** is set to **Enabled**, and click **Next**.

6. At the **Server Groups** step, select the group **CorpServers** group that you added previously, click **Done** then **Next**.

7. At the **Review** step click **Save**.



## Lab 5: Discover Corporate Applications

8. To add an access policy rule for this application, click **Edit Policy**.

Add a policy rule to allow access to this application as follows:

- a. On the **Access Policy** page, click **+ Add Rule**;
  - b. Name the rule **Allow Discovered** and optionally add a description;
  - c. Set the **Action** to **Allow Access**;
  - d. In the **Segment Groups** field, select the **Discovered** Segment Group that you just created and click **Done**;
  - e. Leave the **SAML Attribute** option set to **Any SAML attribute from any IdP**;
  - f. Leave the **Client Types** option set to **Any client type**;
  - g. Do not select any **Zscaler App Posture Profiles**;
  - h. Do not select any **Zscaler App Trusted Networks**;
  - i. Click **Save**.
9. This rule will be added at the bottom of the list of Access Policy rules. However, as this is a very general rule, that is a good position for it.

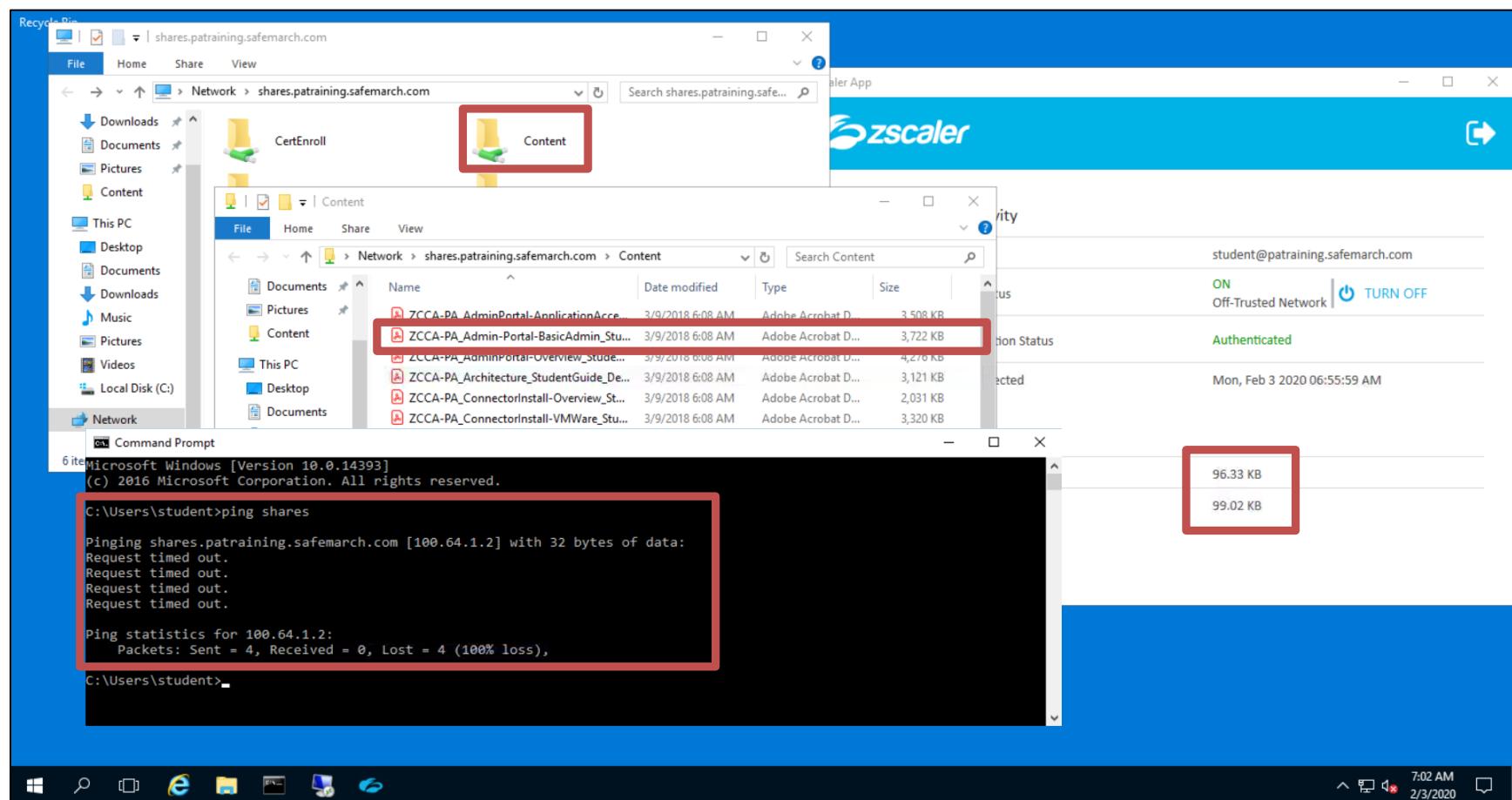
The screenshot shows the 'Add Application Segment' dialog with the 'Edit Policy' step selected. The 'ACTION' section has 'Rule Action' set to 'Allow Access'. The 'CRITERIA' section shows 'Segment Groups' set to 'Discovered'. The 'Save' button at the bottom is highlighted with a red box.

## Lab 5: Discover Corporate Applications

### Discover Applications

In this section you will attempt to access the various corporate applications available by both FQDN and short names.

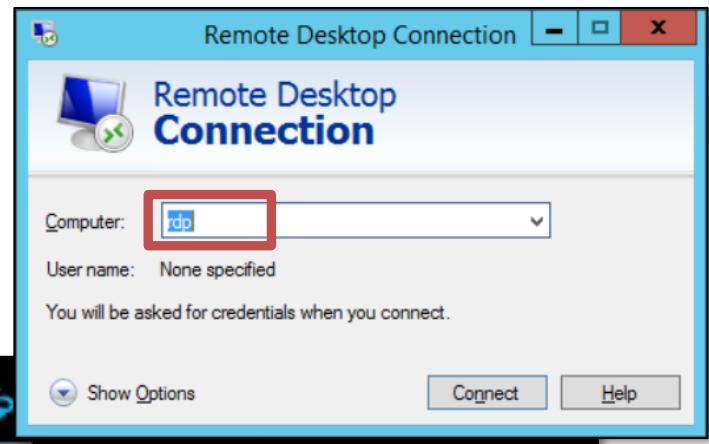
10. On the VM named **Corp: Client PC**, click the **Search Windows** icon in the Status Bar (next to the Windows Start icon) and in the **Search** field, type **\shares**. Confirm that the available shares are shown, that you can access the share named **Content** and open one of the PDFs; also, that the Zscaler Client Connector traffic counters increment.
- Note:** You do not need to specify the FQDN for the application, as you added the **DNS Search Domain** configuration earlier.
11. From the Windows **Start** menu, open a **Command** prompt and ping the host name at **shares**. Verify that it resolves to a **100.64.1.x** IP address (indicating that it is reachable using ZPA), and that it does not respond to pings.



## Lab 5: Discover Corporate Applications

12. In the Windows Status bar, click on the RDP icon and try to connect to the server using just the application short name **rdp**. Try to login with the username **student@patraining[1-N].safemarch.com** and accept the certificate.
13. Close the RDP connection to the server.

**Note:** The RDP Command bar may be obscured by the Skytap Tools bar, collapse the Skytap Tools bar, then use the close control on the RDP Command bar.



14. Go back to the ZPA Admin Portal and navigate to the **Dashboard** page. Scroll down to view the **DISCOVERED APPLICATIONS** widget, check that the applications that you have accessed are all listed. If necessary, click on the **Refresh** icon to update the contents of the widget.

15. Navigate to the **Diagnostics** page and review the list of **User Activity**. Look for entries that match your **Allow Intranet** and **Allow Discovered** Access Policy rules. Expand an entry and review the data available.

## Lab 6: Configure Corporate Applications

Access to corporate applications is now available, however it is indiscriminate, any user can pretty much connect to any application on the domain. You now need to convert the discovered applications to defined applications, so that you can start building systematic Access Policy controls. Plus, two additional Application Segments are required to ensure background Domain Services traffic is carried over ZPA to the AD Server, to allow seamless application discovery and SSO.

### Add defined Applications

In this section you will specifically define Application Segments, to enable granular control of access to individual app. Applications to be added are:

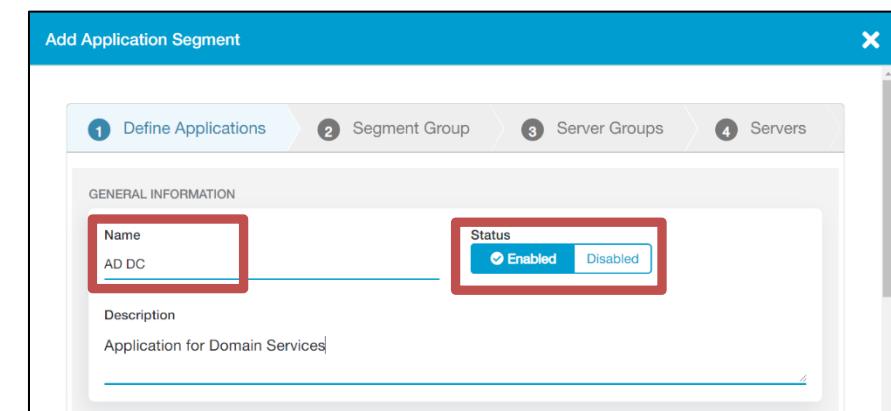
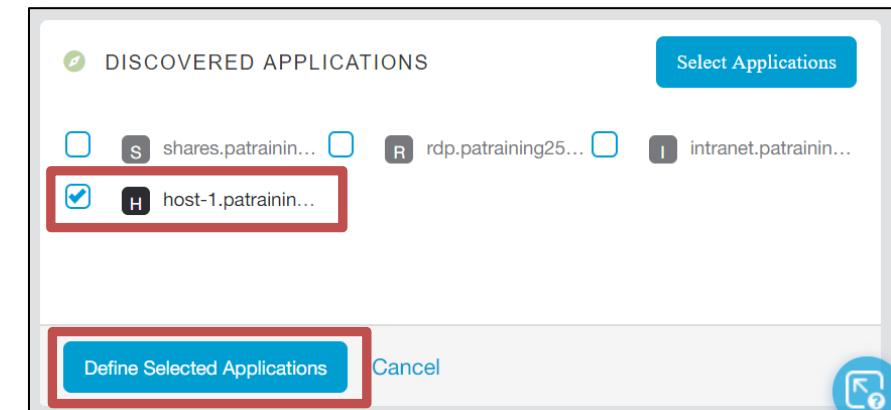
- The AD Domain Controller (for seamless user application SSO – Kerberos and Domain SRV);
- The corporate file share (CIFS);
- RDP access to the AD server.

1. In a browser, navigate to and login to the **ZPA Admin Portal**. Navigate to the **Dashboard** page and scroll down to the **DISCOVERED APPLICATIONS** widget.

**Note:** You can also access the Portal direct from a browser on your own PC.

2. Click **Add Application Segment** and select the application named **host-1.patrainin...** and at the bottom of the widget click **Define Selected Applications**.

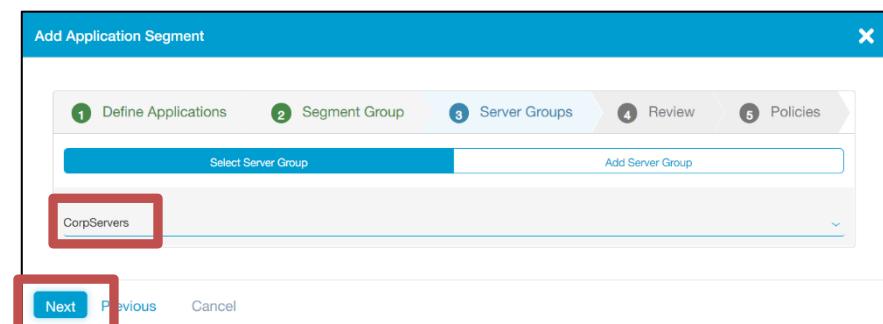
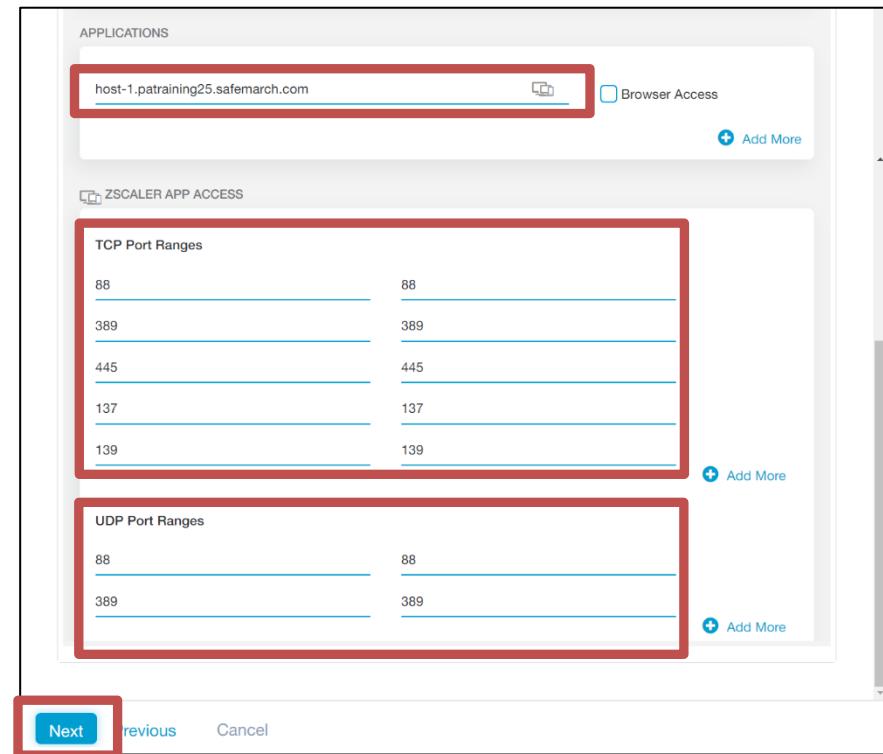
**Note:** If there are multiple entries, just pick one and configure it as a defined application. All of the entries of the same application in the **DISCOVERED APPLICATIONS** widget will have the same FQDN anyway.



3. Add an **Application Segment** for AD Domain Controller access for seamless end user SSO, domain services and application discovery. At the **Define Applications** step of the wizard, configure the following:
  - a. In the **GENERAL INFORMATION** section, set the **Name** to **AD DC**;
  - b. **Status:** Set to **Enabled**;

## Lab 6: Configure Corporate Applications

- c. **APPLICATIONS:** This has already been discovered for you, verify the FQDN is set to **host-1.patraining25.safemarch.com**;
  - d. Scroll down and in the **ZSCALER APP ACCESS** section, set the following **TCP Port Ranges**:
    - From **88** to **88**;
    - From **389** to **389**;
    - From **445** to **445**;
    - From **137** to **137**;
    - From **139** to **139**.
  - e. **UDP Port Range:** Add the following ranges:
    - From **88** to **88**;
    - From **389** to **389**;
  - f. Leave the **Double Encryption** option at **Disabled** and the **Bypass** option at **Use Client Forwarding Policy**;
  - g. Scroll down and in the **COMMON CONFIGURATION** section, set **Health Reporting** to **On Access**, **Health Check** to **Default** and the **Zscaler App can receive CNAME** option at **Enabled**;
  - h. Then click **Next**;
- 
4. At the **Segment Group** step of the wizard, click **Add Segment Group**, name the group **CorpSSO**, optionally add a description, verify that the **Status** is set to **Enabled**, and click **Next**.
  5. At the **Server Groups** step of the wizard, click **Select a Server Group** and select the group named **CorpServers**, you created earlier, and click **Next**.
  6. At the **Review** step click **Save**.



## Lab 6: Configure Corporate Applications

7. To add an access policy rule for this application, click **Edit Policy**.

The screenshot shows the 'Add Application Segment' dialog box. At the top, there are five tabs: 1 Define Applications, 2 Segment Group, 3 Server Groups, 4 Review, and 5 Policies. The 5 Policies tab is selected. Below the tabs is a table titled 'POLICY' with columns 'Rule Order', 'Name', and 'Rule Action'. There are two rows: 'Allow Intranet' (Rule Order 1, Allow Access) and 'Allow Discovered' (Rule Order 2, Allow Access). At the bottom of the dialog are 'Edit Policy' and 'Cancel' buttons, with 'Edit Policy' being highlighted by a red box.

8. Add a policy rule to allow access to this application as follows:
- On the **Access Policy** page, click **+ Add Rule**;
  - Name the rule **Allow CorpSSO** and optionally add a description;
  - Set the **Action** to **Allow Access**;
  - In the **Segment Groups** field, select the **CorpSSO** Segment Group that you just created and click **Done**;
  - Leave the **SAML Attribute** option set to **Any SAML attribute from any IdP**;
  - Leave the **Client Types** option set to **Any client type**;
  - Do not select any **Zscaler App Posture Profiles**;
  - Do not select any **Zscaler App Trusted Networks**;
  - Click **Save**.
9. Click the **Rule Order** number for this new rule (should be **3**) and type in the number **1** and press Enter. Verify that this rule is re-positioned to the top of the list, above the **Allow Discovered** rule.
- Note:** This rule is for background domain service traffic, so should be positioned at the very top of the Access Policy rule list.

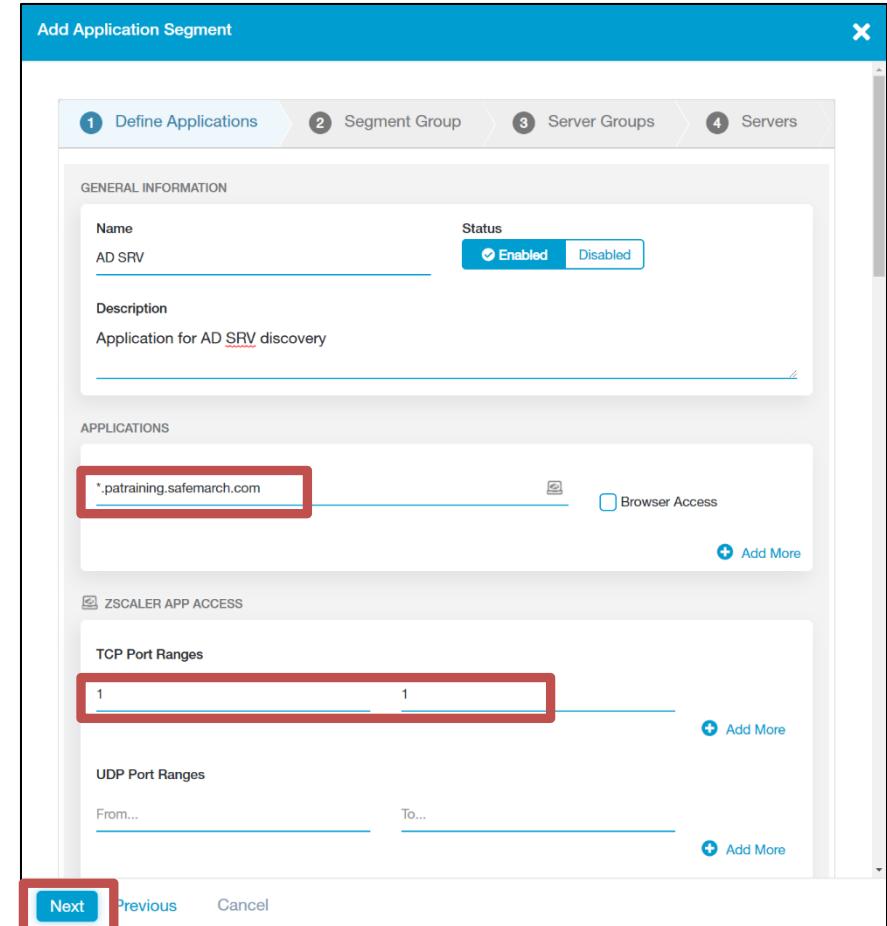
The screenshot shows the 'Edit Access Policy' dialog box. It has sections for 'Name' (Allow CorpSSO), 'Description' (Allow rule for DNS SRV discovery), 'ACTION' (Rule Action: Allow Access selected), 'CRITERIA' (Application Segments: Select one or more application segments, Segment Groups: CorpSSO selected), and 'Message to User' (empty). The 'Rule Action' section and the 'CorpSSO' segment group selection are highlighted by red boxes.

## Lab 6: Configure Corporate Applications

10. An additional Application Segment is required for seamless domain application discovery, which must be added manually. In the ZPA Admin Portal, navigate to the **Administration > APPLICATION MANAGEMENT > Application Segments** page.
11. Click the **+ Add Application Segment** icon at top right to add a new **Application Segment**. Configure an **Application Segment** for AD SRV discovery, using a wildcard domain for the Application on the TCP port of your choice.
12. At the **Define Application** step of the wizard, configure the following:
  - a. Set the **Name** to **AD SRV**, set the **Status** to **Enabled** and add a suitable **Description**;
  - b. In the **APPLICATIONS** section, click in the **Enter a domain or IP address** field and specify **\*.patraining[1-N].safemarch.com**;
  - c. Scroll down, and in the **ZSCALER APP ACCESS** section, specify a **TCP Port Range** from **1** to **1**, with no **UDP Port Range**, leave the **Double Encryption** option at **Disabled**, the **Bypass** option at **Use Client Forwarding Policy**;

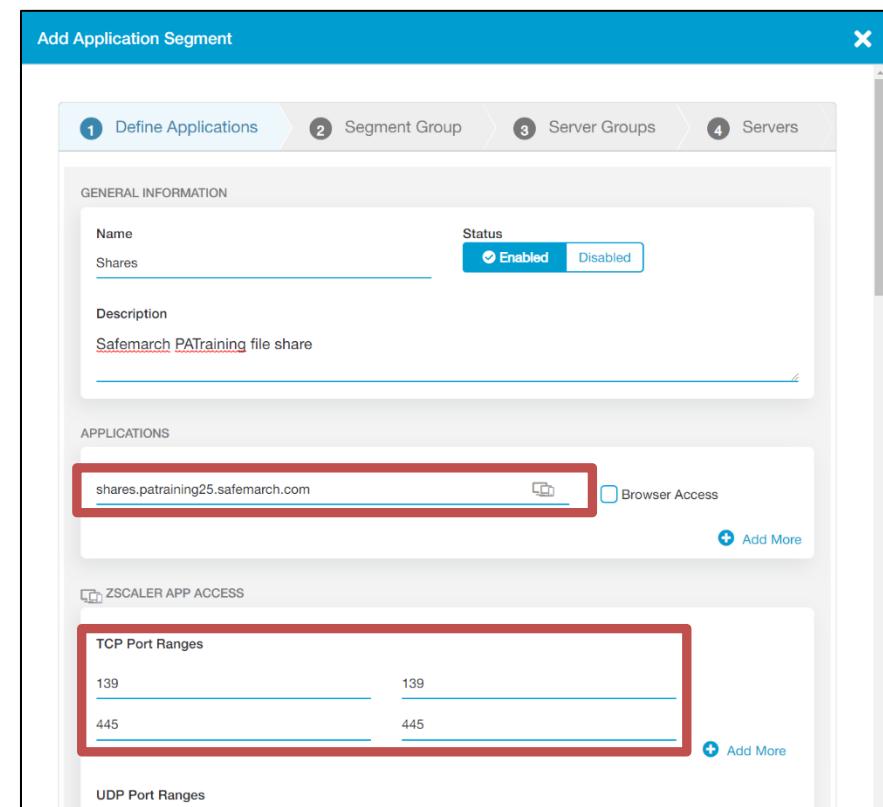
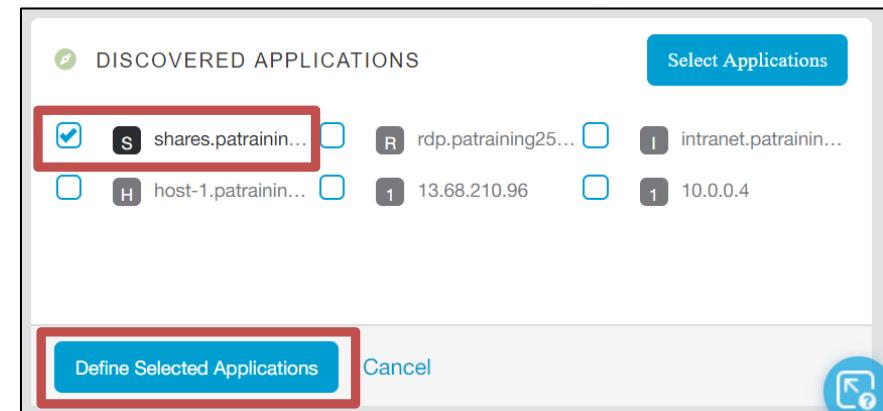
**Note:** You can specify any port number you like here. For the lab, for the sake of simplicity we will use port 1, although this is actually the port reserved for the tcpmux service.

  - d. Scroll down and in the **COMMON CONFIGURATION** section, set **Health Reporting** to **On Access**, **Health Check** to **Default** and the **Zscaler App can receive CNAME** set to **Enabled**;
  - e. Then click **Next**;
13. At the **Segment Group** step of the wizard, click **Select a Segment Group**, select the group **CorpSSO** that you created earlier and click **Next**.
14. At the **Server Groups** step of the wizard, click **Select a Server Group**, select the group **CorpServers** that you created earlier and click **Next**.
15. At the **Review** step click **Save**.
16. There is no need to add an Access Policy rule for this application, as it is a member of the **CorpSSO** Segment Group that is used in the allow policy you created above, so click **Cancel** to exit the wizard.



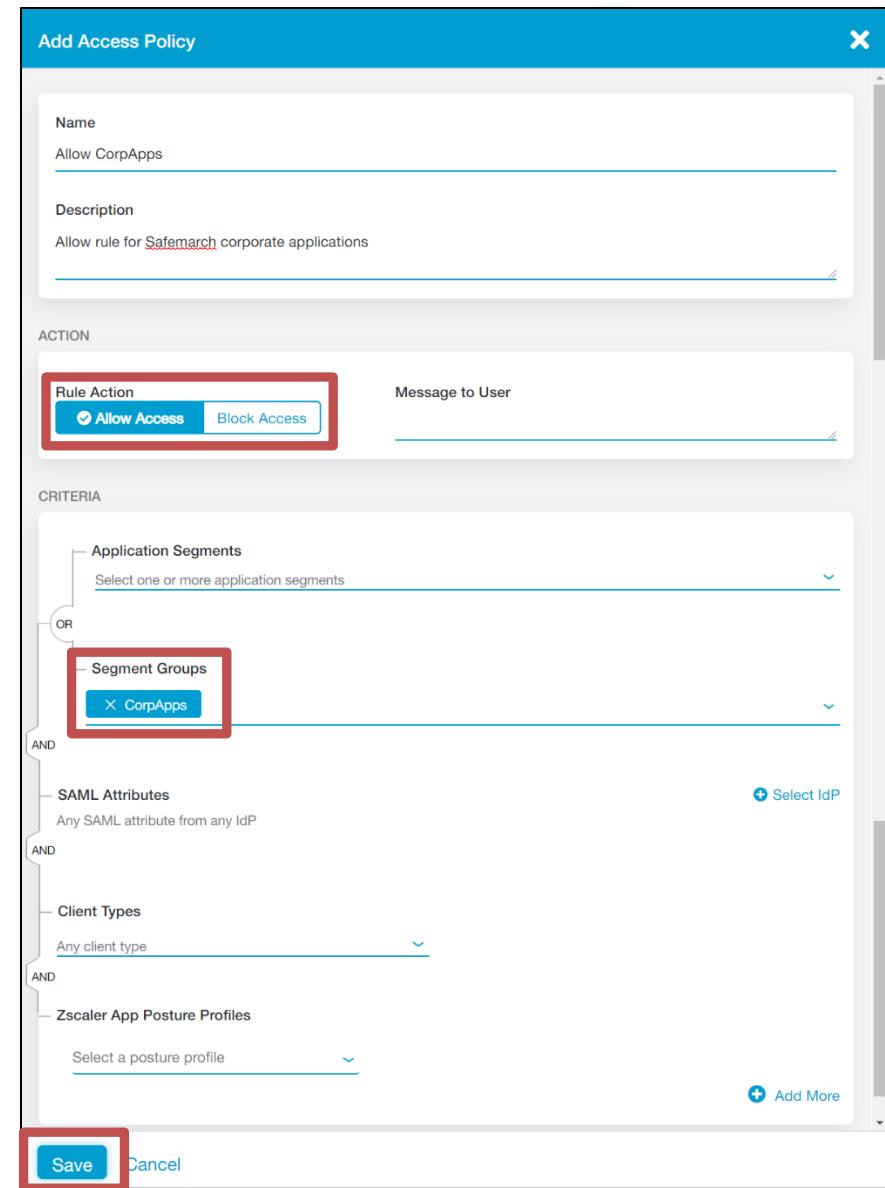
## Lab 6: Configure Corporate Applications

17. In the **ZPA Admin Portal**, navigate to the **Dashboard** page and scroll down to the **DISCOVERED APPLICATIONS** widget.
18. Click **Add Application Segment** and select the application named **shares.patrainin...** and at the bottom of the widget click **Define Selected Applications**.  
**Note:** If there are multiple entries, just pick one and configure it as a defined application. All of the entries of an application in the **DISCOVERED APPLICATIONS** widget should have the same FQDN anyway.
19. Add an **Application Segment** for the corporate file share. At the **Define Application** step of the wizard, configure the following:
  - a. **Name:** Set to **Shares**;
  - b. **Status:** Set to **Enabled**;
  - c. **APPLICATIONS:** Verify it is already set to **shares.patrainin[1-N].safemarch.com**;
  - d. **TCP Port Range:** Add the following ranges:
    - From **139** to **139**;
    - From **445** to **445**.
  - e. **UDP Port Range:** Leave blank;
  - f. **Double Encryption:** Set to **Disabled**;
  - g. **Bypass:** Set to **Use Client Forwarding Policy**;
  - h. **Health Reporting:** Set to **Continuous**;
  - i. **Health Check:** Set to **Default**;
  - j. **Zscaler App can receive CNAME:** Set to **Enabled**;
  - k. Click **Next**.
20. At the **Segment Group** step of the wizard, click **Select a Segment Group** and select the group **CorpApps** that you added previously.
21. At the **Server Groups** step of the wizard, click **Select a Server Group** and select the group **CorpServers** that you added previously.
22. At the **Review** step click **Save**.
23. To add an access policy rule for this application, click **Edit Policy**.



## Lab 6: Configure Corporate Applications

24. Add a policy rule to allow access to this application as follows:
- On the Access Policy page, click **Add Rule**;
  - Name the rule **Allow CorpApps** and optionally add a description;
  - Set the **Action** to **Allow Access**;
  - In the **Segments Groups** field, select the **CorpApps** Segment Group that you just created and click **Done**;
  - Leave the **SAML Attribute** option set to **Any SAML attribute from any IdP**;
  - Leave the **Client Types** option set to **Any client type**;
  - Do not select any **Zscaler App Posture Profiles**;
  - Do not select any **Zscaler App Trusted Networks**;
  - Click **Save**.
25. Click the **Rule Order** number for this new rule (should be **4**) and type in the number **3** and press Enter. Verify that this rule is re-positioned above the **Allow Discovered** rule.
- Note:** This rule is more specific than the rule for application discovery, so should be positioned higher up on the Access Policy rule list.
26. Click to **Delete** the rule named **Allow Intranet**, as this rule is now redundant.



## Lab 6: Configure Corporate Applications

27. In the **ZPA Admin Portal**, navigate to the **Dashboard** page and scroll down to the **DISCOVERED APPLICATIONS** widget.
28. Click **Add Application Segment** and select the application named **rdp.patrainin...**, then at the bottom, click **Define Selected Applications**.

**Note:** If there are multiple entries, just pick one and configure it as a defined application. All of the entries of an application in the **DISCOVERED APPLICATIONS** widget should have the same FQDN anyway.

29. Add an Application Segment for RDP access to the corporate AD server.

At the **Define Application** step of the wizard, configure the following:

- a. **Name:** Set to **RDP**;
- b. **Status:** Set to **Enabled**;
- c. **APPLICATIONS:** Verify it is already set to **rdp.patrainin[1-25].safemarch.com**;
- d. Click **Add More** and add the IP address **10.0.0.11**;
- e. **TCP Port Range:** Add the range: From **3389** to **3389**.
- f. **UDP Port Range:** Add the range: From **3389** to **3389**.
- g. **UDP Port Range:** Leave blank;
- h. **Double Encryption:** Set to **Disabled**;
- i. **Bypass:** Set to **Use Client Forwarding Profile**;
- j. **Health Reporting:** Set to **On Access**;
- k. **Health Check:** Set to **Default**;
- l. **Zscaler App can receive CNAME:** Set to **Enabled**, then click **Next**.

30. At the **Segment Group** step of the wizard, click **Select a Segment Group** and select the group **CorpApps** that you added previously.
31. At the **Server Groups** step of the wizard, click **Select a Server Group** and select the group **CorpServers** that you added previously.
32. At the **Review** step click **Save**.
33. There is no need to add an Access Policy rule for this application, as it is a member of the **CorpApps** Segment Group, so click **Cancel** to exit the wizard.

## Lab 6: Configure Corporate Applications

### Test Remote Application Access

In this section you will test connectivity to the corporate applications with the client PC connected to a remote network.

34. On the VM named **Corp: Client PC**, try to ping each of the applications loaded previously (**intranet**, **shares** and **rdp**) and confirm that they resolve to a **100.64.1.x** IP address, but that they do not respond to pings.
35. Test application access:
  - a. Open a web browser in a window again, and open the **Zscaler Client Connector** adjacent to it, so you can see the traffic counters as you load web pages.
  - b. Try to access the page at [http://intranet.patraining\[1-N\].safemarch.com](http://intranet.patraining[1-N].safemarch.com) and confirm that the intranet page loads. Confirm that you are able to navigate the **Intranet** pages using HTTP or HTTPS and that the Zscaler Client Connector traffic counters increment as you do so.
  - c. Click the Windows **Search Windows** icon and type **\shares**. Confirm that the share named **Content** from the Windows 2016 server is accessible and that the Zscaler Client Connector traffic counters increment.
  - d. Click the **RDP** icon again and try to connect to the server on the short name **rdp**. Verify that you can login and receive the server certificate. Then close the RDP connection.

36. To verify the routing of AD domain SRV traffic, open a **Command prompt** window and enter the command **nslookup**:

- a. At the **nslookup** prompt, type the command: **set type=srv**
- b. Then enter the command: **\_kerberos.\_tcp.patraining[1-N].safemarch.com**
- c. Review the output.

**Note:** The service location should indicate the FQDN of the AD server on the corporate network, however the address resolved should be a ZPA assigned **100.64.x.x** address.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\student.PATRINING>nslookup
Default Server: dns-server.patraining25.safemarch.com
Address: 192.168.1.252

> set type=srv
> _kerberos._tcp.patraining25.safemarch.com
Address: 192.168.1.252

Non-authoritative answer:
_kerberos._tcp.patraining25.safemarch.com SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = host-1.patraining25.safemarch.com
host-1.patraining25.safemarch.com internet address = 100.64.1.1
```

37. In the ZPA Admin Portal, navigate to the **Diagnostics** page and view **User Activity**. Click in the **Connection** field of an entry to expand details for it and review the contents. Check the latest few entries, you should see successful access attempts for **Corp SSO** and **CorpApps**;

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

In this Lab you will create an Application Segment for Vendor access to an internal HVAC control application and configure it for Browser Access.

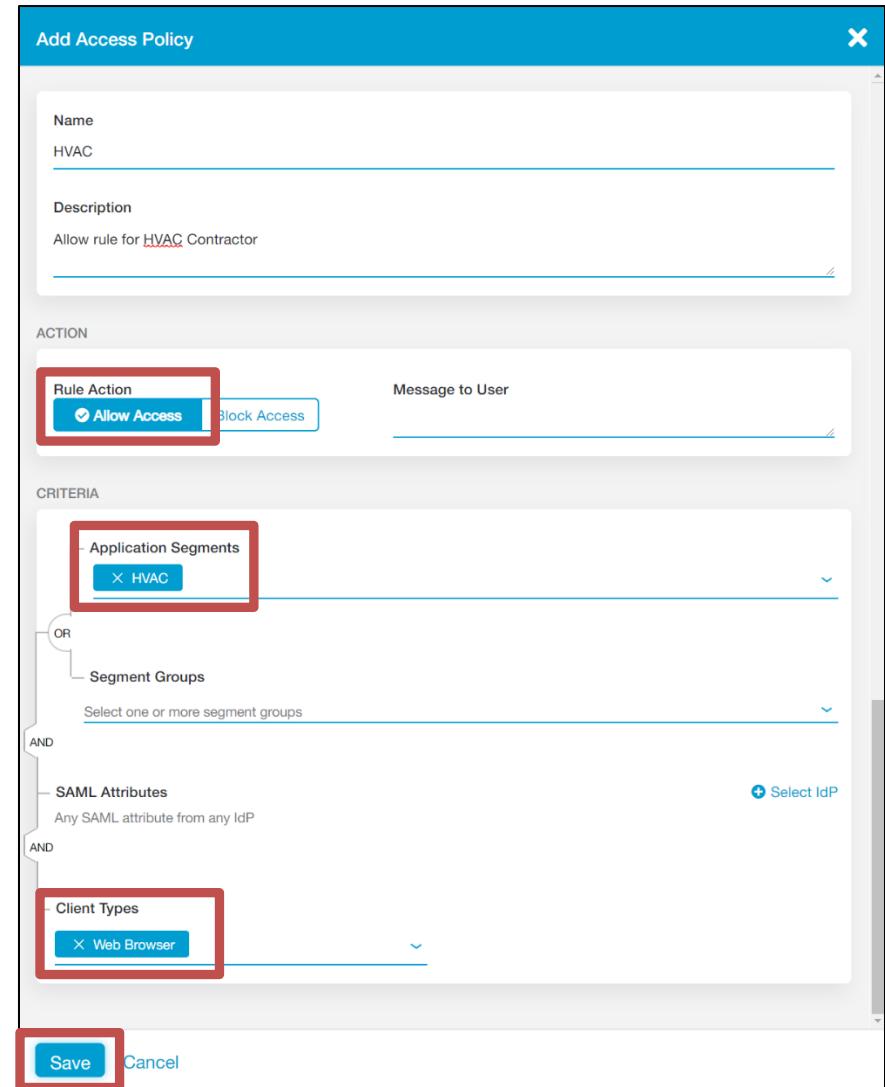
### Create HVAC Application for BA

In this section you will add the Safemarch HVAC application that the 3<sup>rd</sup> party Vendor is to access using BA.

1. In the ZPA Admin Portal, navigate to the **Administration > APPLICATION MANAGEMENT > Application Segments** page and click the **+ Add Application Segment** icon at top right.
2. At the **Define Application** step of the wizard, configure the following:
  - a. **Name:** Set to **HVAC**;
  - b. **Description:** Optionally add a description;
  - c. **Status:** Set to **Enabled**;
  - d. **APPLICATIONS:** Specify the application **hvac.patraining[1-N].safemarch.com**;
  - e. **TCP Port Range:** Add the ranges from **80** to **80**.
  - f. **UDP Port Range:** Leave blank;
  - g. **Double Encryption:** Set to **Disabled**;
  - h. **Bypass:** Set to **Use Client Forwarding Policy**;
  - i. **Health Reporting:** Set to **Continuous**;
  - j. **Health Check:** Set to **Default**;
  - k. **Zscaler App can receive CNAME:** Set to **Enabled**;
  - l. Click **Next**.
3. At the **Segment Group** step of the wizard, click **Add Segment Group**, name the group **Maint**, optionally add a description, verify that the **Status** is set to **Enabled**, and click **Next**.
4. At the **Server Groups** step of the wizard, click **Select Server Group** and select the group **CorpServers** that you added previously.
5. At the **Review** step click **Save**.
6. To add an access policy rule for this application, click **Edit Policy**.

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

7. Add a policy rule to allow access to this application as follows:
- On the **Access Policy** page, click **Add Rule**;
  - Name the rule **Allow HVAC** and optionally add a description;
  - Set the **Action** to **Allow Access**;
  - In the **Application Segments** field, select the HVAC Application Segment that you just created and click **Done**;
  - Leave the **SAML Attribute** option set to **Any SAML attribute from any IdP**;
  - Set the **Client Types** option set to **Web Browser** and click **Done**;
  - Click **Save**.



8. Click the **Rule Order** number for this new rule (should be **4**) and type in the number **2** and press Enter. Verify that this rule is re-positioned above the **Allow CorpApps** rule.

**Note:** This rule is more specific than the rule for access to corporate applications, so should be positioned higher up on the Access Policy rule list.

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

### Create HVAC Web Server Certificate

Create a Browser Access Certificate for the HVAC application and have it signed by the PATraining enterprise private CA.

**Note:** Normally these certificates would be signed by a public CA, so they can be trusted by any browser/device anywhere.

- On the VM labelled **Corp: Win Svr 2016**, open a browser, navigate to and login to the **ZPA Admin Portal** for your organization on the URL <https://admin.private.zscaler.com> and login with your normal administrator credentials.

**Note:** You must access the Admin Portal from the Windows 2016 server, as that is where the corporate certificate services must be accessed.

The screenshot shows the Zscaler Admin Portal interface. On the left is a sidebar with icons for Dashboard, Diagnostics, Live Logs, and Administration. The main area has tabs for 'Enrollment Certificates' and 'Browser Access Certificates', with 'Browser Access Certificates' highlighted and surrounded by a red box. A search bar and a refresh/circular arrow icon are at the top right. Below is a table with columns: Name, Creation Date, Expiry Date, Common Name, and Actions. A message 'No Items Found' is displayed. To the right, a modal window titled 'Create CSR' is open. It has fields for 'Name' (set to 'HVAC'), 'Description' (set to 'BA certificate for the HVAC application'), 'Subject' (set to 'CN=hvac.patraining[1-N].safemarch.com,O=safemarch,ST=NY,C=US,L=NY,OU=patraining[1-N]'), and 'Subject Alternate Name' (set to 'hvac.patraining25.safemarch.com'). At the bottom are 'Create' and 'Cancel' buttons, with 'Create' also highlighted by a red box.

- From the **Administration** menu, under **CERTIFICATE MANAGEMENT** select **Browser Access Certificates**, then click the icon to create a CSR.
- Name the CSR **HVAC** and add a **Description** as necessary.
- Enter the **Subject** value:  
**CN=hvac.patraining[1-N].safemarch.com,O=safemarch,ST=NY,C=US,L=NY,OU=patraining[1-N]**
- Enter the **Subject Alternate Name** value **hvac.patraining[1-N].safemarch.com** and click **Create**.

**Note:** Under normal circumstances, the Common Name (CN) must match the external FQDN you have chosen. However, if your external FQDN is different from the internal setting the SAN to the value of the internal FQDN will allow the user to access the web application without getting a certificate mismatch warning.

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

14. Click the **Download .CSR File** button adjacent to the CSR that you just created and save the file to the \Downloads folder with the file name HVAC.csr.

The screenshot shows the 'Enrollment Certificates' section of the Zscaler interface. A table lists a single entry for 'HVAC'. The 'Actions' column contains three icons: a person icon (highlighted with a red circle), a group icon, and a delete icon. The 'Name' column shows 'HVAC', 'Creation Date' shows 'Tuesday, June 23 2020 1:56:24 am', and 'Common Name' shows 'hvac.patraining25.safemarch.com'.

15. Go to the \Downloads folder, find the file that you just saved, right click and select **Open**.

**Note:** if necessary, choose **Open With**, then select the **Notepad** application.

16. Now take this data to your internal corporate root CA to generate a signed certificate, as follows:

- In a new browser window or tab, navigate to the corporate certificate services page at <http://10.0.0.9/certsrv> (a bookmark is provided);
- Log in with the **Administrator** user and password **Admin-123!**
- Click the **Request a certificate** link, then the **advanced certificate request** link;
- Click the link **Submit a certificate request by using a base-64-encoded, CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**;
- Go back to the Notepad file, select all the text in it, right-click and select **Copy**;
- Back in the web browser, paste the text into the **Saved Request** field;
- For the **Certificate Template** option, select **Web Server**;
- Click **Submit >**;
- Select the **Base 64 encoded** option, then click the **Download certificate** link and save the file to the desktop as **HVAC-BA-Signed.cer**.

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page. The 'Saved Request' field contains a large amount of base-64 encoded certificate request data. The 'Certificate Template' dropdown is set to 'Web Server'. The 'Submit' button is highlighted with a red box.

The screenshot shows the 'Certificate Issued' page. It displays a message stating 'The certificate you requested was issued to you.' Below this, there are two download links: 'Download certificate' (highlighted with a red box) and 'Download certificate chain'.

**Note:** If an error message is shown when submitting the request, **restart the server and try again**.

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

17. Go back to the ZPA Admin Portal in the web browser and on the Administration > CERTIFICATE MANAGEMENT > Browser Access Certificates page click the Upload Certificate button adjacent to the CSR that you just created.

Name	Creation Date	Expiry Date	Common Name	Actions
> HVAC	Tuesday , June 23 2020 1:56:24 am		hvac.patraining25.safemarch.com	

18. In the Upload Server Certificate dialog, in the Certificate field click Select File, navigate to the \Downloads folder and select the file named HVAC-BA-Signed.cer that you just saved, click Open then click Upload.

Upload Server Certificate

Name  
HVAC

Description  
BA certificate for the HVAC application

Certificate

Select File

Subject Alternate Name  
hvac.patraining25.safemarch.com

Certificate Signing Request  
-----BEGIN CERTIFICATE REQUEST-----  
MIIC/jCCAEyCAQAwfDEVMBMGA1UECxMMcGF0cmFpbmluZzI1MQswCQYDVQQHEwJ...  
-----END CERTIFICATE REQUEST-----

19. Confirm that the certificate is uploaded successfully.

Name	Creation Date	Expiry Date	Common Name	Actions
> HVAC	Tuesday , June 23 2020 12:56:24 pm	Thursday , June 23 2022 12:53:08 pm	hvac.patraining25.safemarch.com	

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

### Create DNS CNAME Record for the HVAC Application

In this section, you will reconfigure the Safemarch HVAC application for Browser Access, which will give you the details for the DNS CNAME record that you need to create. You will then create that record on the DNS server of the network the client PC is connected to.

**Note:** For the purposes of the lab you will create a CNAME record on the DNS Server on the remote network that the client is attached to, normally you would create this on the public DNS infrastructure.

20. In a web browser, access the **ZPA Admin Portal** for your organization and navigate to the **Administration > APPLICATION MANAGEMENT > Application Segments** page.

**Note:** You can access the Admin Portal from any convenient browser.

21. Click the **Edit** icon by the application named **HVAC**.

Name	Applications	Status	Health Reporting	Health Check	Actions
Discovery	*.patraining.safemarch.com	✓	On Access	✓	<a href="#">Edit</a> <a href="#">Preview</a> <a href="#">Delete</a>
HVAC	hvac.patraining25.safemarch.com	✓	Continuous	✓	<a href="#">Edit</a> <a href="#">Preview</a> <a href="#">Delete</a>

22. In the **Edit Application Segment** wizard, at the **General Information** page, click **Next**.

23. At the **Application And Ports Configuration** page, configure the **Applications** for **Browser Access**:

- Click the check box to enable the **Browser Access** option;
- In the **Select a certificate** field select the certificate named **HVAC** that you uploaded earlier;
- Select **HTTP**;
- Click **Next**, then click **Save**.

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

24. Get the **CNAME** value for the HVAC application:

- Go to the **Browser Access** tab, then click the name of the HVAC application to expand it to see the details;
- Select and copy the **value** of the **Canonical Name (CNAME)** for the application.

**Note:** If you use the **Copy** tool, paste the data into Notepad then copy **only the value for the CNAME** to configure on the DNS Server.

Name	Domain	Application Protocol	Application Port	Actions
hvac.patraining25.safemarch.com	hvac.patraining25.safemarch.com	HTTP	80	<span style="color: blue;">Edit</span> <span style="color: red;">Delete</span>
Segment Group		Server Groups		
<span style="border: 1px solid blue; padding: 2px;">Maint</span>		<span style="border: 1px solid blue; padding: 2px;">CorpServers</span>		
Canonical Name (CNAME)		Certificate		
5141.144131794566905856.h.p.zpa-app.net		<span style="border: 1px solid blue; padding: 2px;">HVAC</span>		
<span style="border: 1px solid blue; padding: 2px;">Copy</span> <span style="margin-left: 10px;">Ctrl+C</span> <span style="border: 1px solid blue; padding: 2px;">Go to 5141.144131794566905856.h.p.zpa-app.net</span> <span style="margin-left: 10px;">Ctrl+P</span> <span style="border: 1px solid blue; padding: 2px;">Print...</span> <span style="margin-left: 10px;">Ctrl+P</span>				

25. Open the VM named **Remote: DNS Server**, from the VM tools bar send the **Ctrl-Alt-Del**, and login to the PC with username **Administrator** and password **Zscaler123!**

26. Wait for the **Server Manager Dashboard** to open, then from the **Tools** menu, select **DNS** and add a **CNAME** record:

- Expand the DNS server named **DNS-SERVER**;
- Expand the **Forward Lookup Zones** and select the zone for the pod (**patraining[1-N].safemarch.com**);
- Right-click and select the option **New Alias (CNAME)...**;
- Enter the **Alias name** value **hvac**;
- Paste only the **CNAME value** into the field labelled **fully qualified domain name (FQDN) for target host** and click **OK**.

**Note:** It is best practice to add a single trailing dot character.

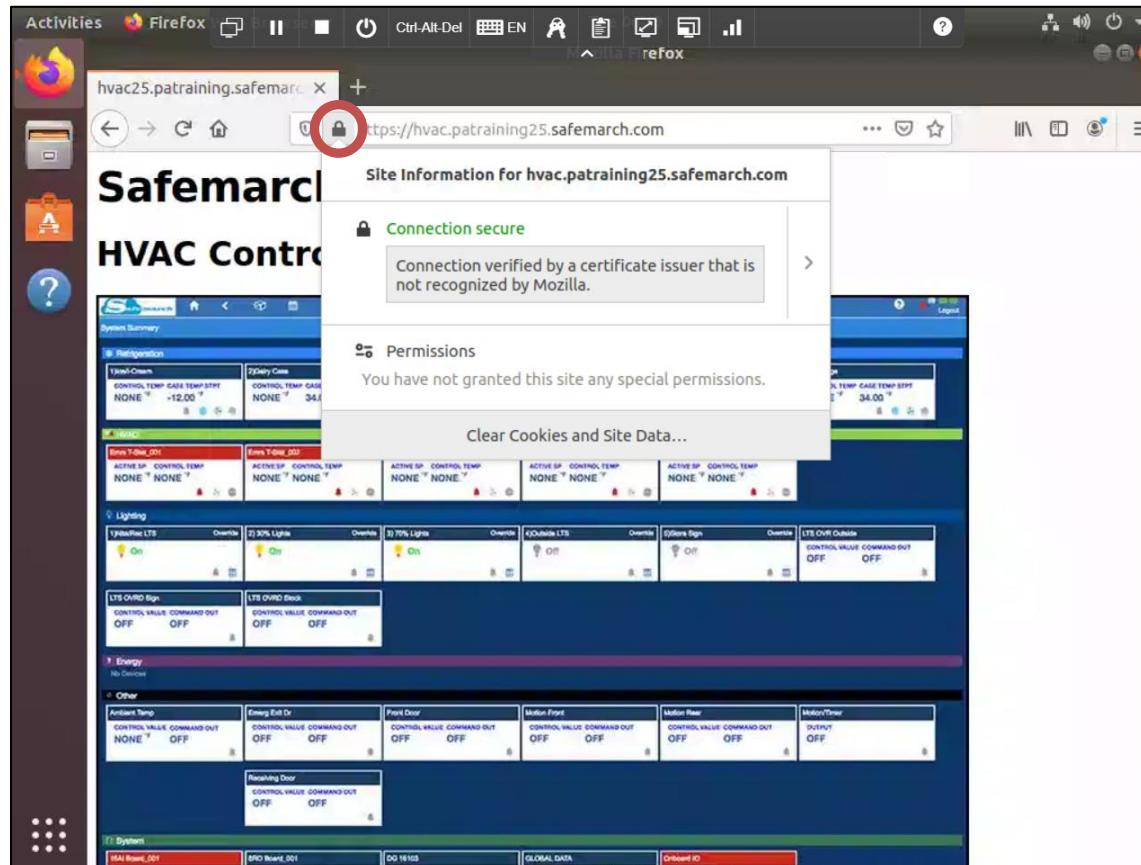
**Tip:** Use the Clipboard tool in the VM Control Panel to copy/paste the value between VMs.

## Lab 7: Browser Access for 3<sup>rd</sup> Parties

### Test Browser Access to the HVAC Application

In this section you will attempt to access the HVAC application in a web browser from the Linux Client PC on the remote network.

27. Open the VM named **Remote: Linux Client PC**, click to login as the user **Admin** with password **Admin-123!** ...then click to open **Firefox**.
28. Try to navigate to the **HVAC** application using **HTTP**, on the URL [http://hvac.patraining\[1-N\].safemarch.com](http://hvac.patraining[1-N].safemarch.com).
29. When prompted, login through the **Azure SAML IdP** with the username **hvac@patraining[1-N].safemarch.com** and password **Admin-123!**
30. Confirm that you can reach the **Safemarch HVAC Control** page. Click the padlock icon in the address bar and review the certificate details.  
**Note:** The browser has been re-directed to **HTTPS**, you will see details for the Web server certificate that you created for the application.
31. Close the browser.

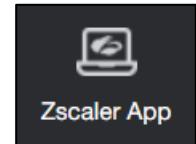


## Lab 8: Configure Advanced Access Policy

In this Lab you will create posture profile criteria for use in Access Policy rules, then configure the rules to ensure only authorized users have access to the various applications, using compliant access method (Zscaler Client Connector or Browser Access) and from compliant devices.

### Create Posture Profiles

In this section you will create posture profiles in the Zscaler Client Connector Portal to test: Whether a Windows client machine is domain joined or not; whether a client certificate is installed from the Safemarch enterprise private CA.



1. On the VM named **Corp: Win Svr 2016** in the ZPA Admin Portal, click the **Zscaler Client Connector** icon in the left-hand navigation bar.

**Note:** You need to do this from the Windows 2016R2 Server VM, as you will need to upload a certificate from that machine.

2. In the Zscaler Client Connector Portal, navigate to the **Administration > Device Posture** page and click the **+ Add Device Posture Profile** link.
3. Configure the new Posture Profile as follows:

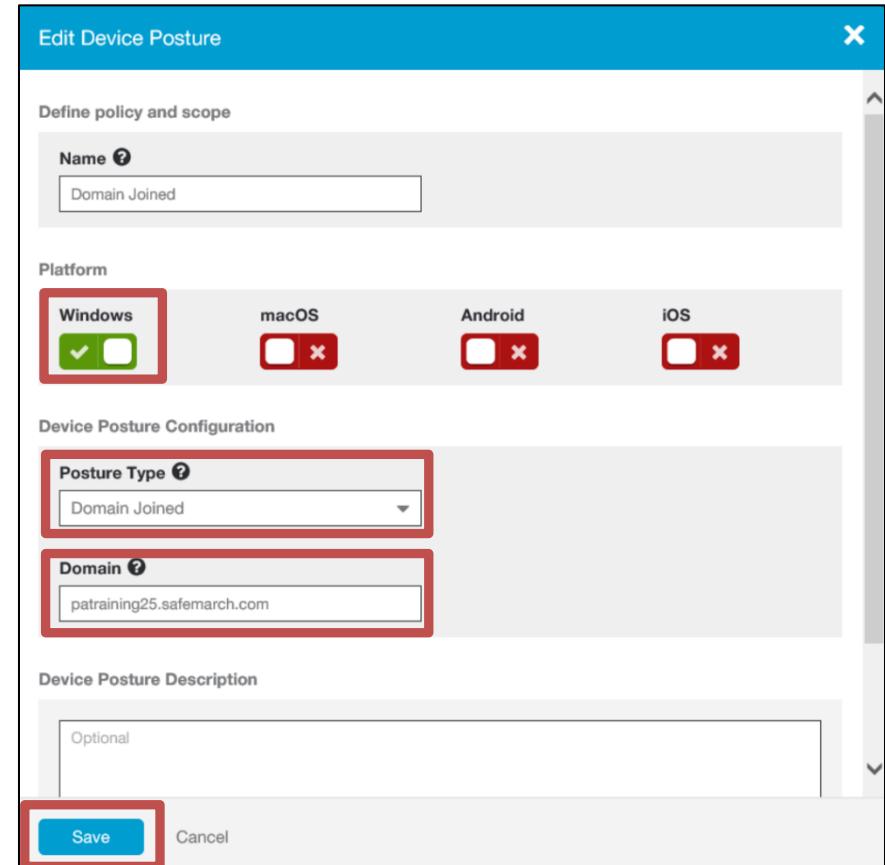
a. **Name:** Domain Joined;

b. **Platform:** Enable only Windows;

c. **Posture Type:** Domain Joined;

d. **Domain:** Set it to your domain (**patraining[1-N].safemarch.com**);

e. Click **Save**.



The screenshot shows the 'Edit Device Posture' dialog box. The 'Name' field is set to 'Domain Joined'. Under 'Platform', the 'Windows' checkbox is selected (indicated by a green checkmark). The 'macOS', 'Android', and 'iOS' checkboxes are unselected (indicated by a red 'X'). In the 'Device Posture Configuration' section, the 'Posture Type' dropdown is set to 'Domain Joined' and the 'Domain' input field contains 'patraining25.safemarch.com'. The 'Device Posture Description' section has an optional text area with the word 'Optional'. At the bottom, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted with a red border.

## Lab 8: Configure Advanced Access Policy

4. In the Zscaler Client Connector Portal, navigate to the **Administration > Device Posture** page and click the **+ Add Device Posture Profile** link.

5. Configure the new Posture Profile as follows:

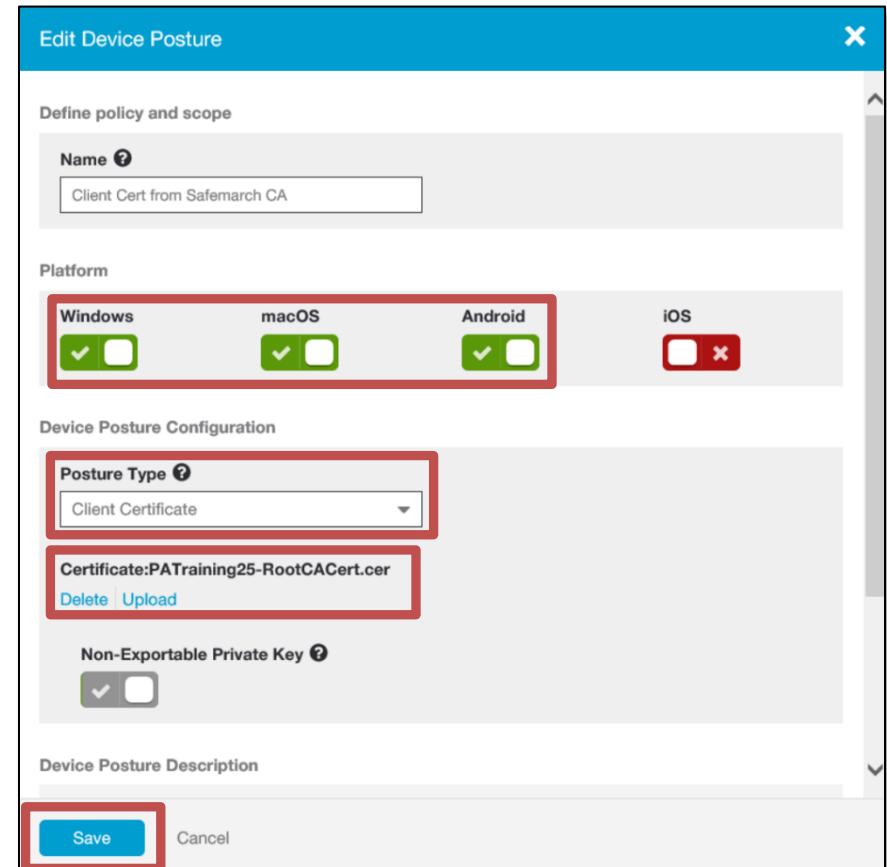
a. **Name:** Client Cert from Safemarch CA;

b. **Platform:** Enable for Windows, macOS, Android;

c. **Posture Type:** Client Certificate;

d. Click the **Upload** link and navigate to the \Downloads folder. Select the file named **PATraining[1-N]-RootCACert**, click **Open**, then **Upload**.

e. Click **Save**.



6. Close the browser tab with the Zscaler Client Connector Portal.

## Lab 8: Configure Advanced Access Policy

### Manage Access Policy

In this section you will create and manage a set of Access Policies to meet the access needs of the Safemarch corporation, which are:

- Corporate users (targeted by AD Department) are to have access to corporate file shares and the Intranet from domain-joined Windows PCs and other devices (macOS, Android) that possess a client certificate from the corporate PKI.
- The HVAC Vendor is to have access to the HVAC application only, using Browser Access only.
- Only corporate admins can access the server using RDP.

First, we will look at Access Policy for internal Safemarch users.

7. In the ZPA Admin Portal, go to the **Administration > POLICY MANAGEMENT > Access Policy** page and click to **Edit** the rule named **Allow CorpApps**.

Rule Order	Name	Rule Action	Actions
> 1	Allow Corp SSO	Allow Access	
> 2	Allow HVAC	Allow Access	
> 3	Allow CorpApps	Allow Access	
> 4	Allow Discovered	Allow Access	

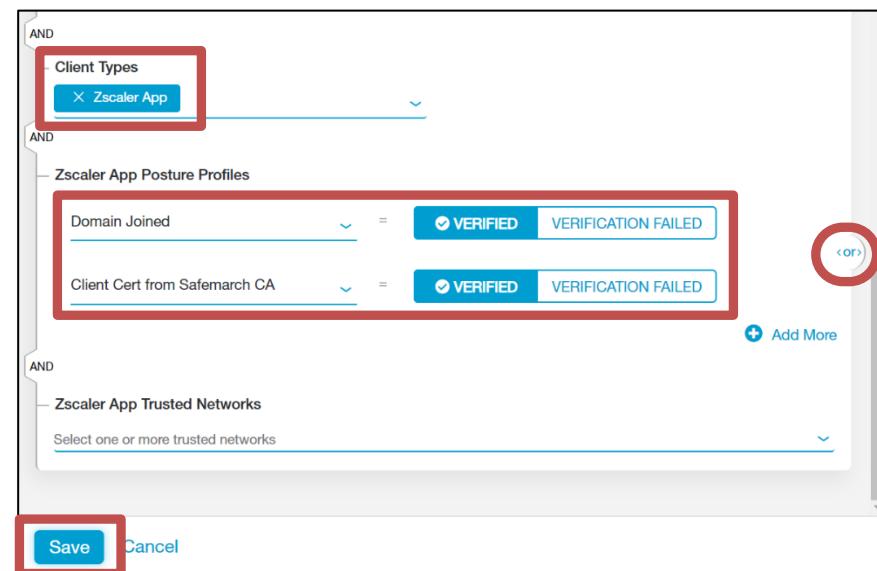
8. Edit the rule to target corporate users only (by Department) and to restrict access to either domain-joined Windows PCs, or other devices that have a client certificate from the Safemarch PKI:

- a. Click **Select IdP** then click on **Azure IdP**;
- b. Click **Any SAML attribute** and select the attribute named **Department\_Azure IdP**;
- c. **Note:** There is a search option to find the Department attribute.
- d. Specify the value to match as **Marketing**.

**Note:** We could add additional departments here, but for the lab we will just use the Marketing department.

## Lab 8: Configure Advanced Access Policy

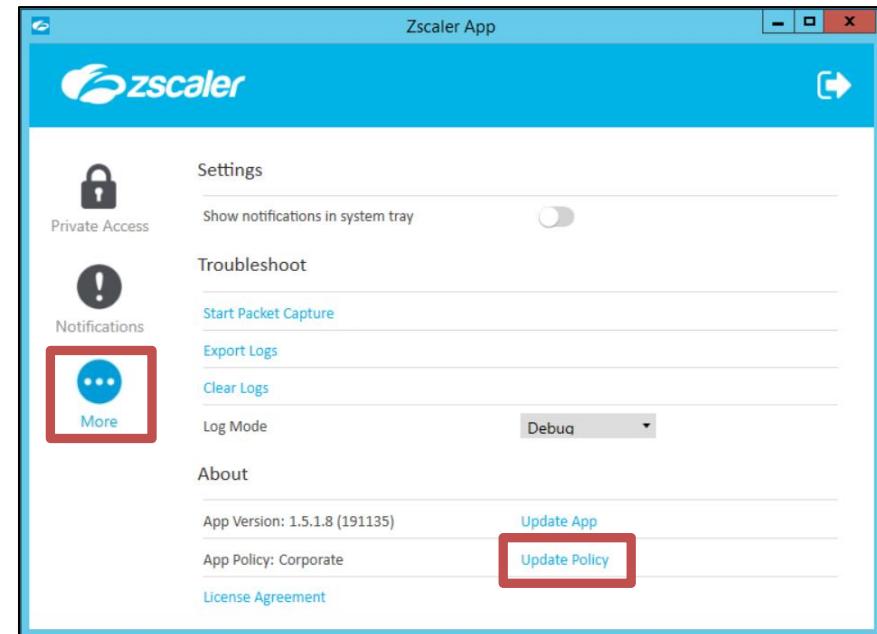
- e. Click in the **Client Types** field and select the **Zscaler App** option only, then click **Done**;
- f. Scroll down and click in the **Zscaler App Posture Profiles** field.
  - Select the profile named **Domain Joined** and enable the **VERIFIED** option;
  - Click **Add More**, then select the profile named **Client Cert from Safemarch CA** and ensure it is also set to **VERIFIED**;
  - Verify that the selector (at right) is set to a logical **<or>**.
- g. Click **Save**.



9. To test the rule, go to the VM named **Corp: Client PC** and login to Windows:
  - a. Open the Zscaler Client Connector, go to the **More** page and click **Update Policy**;
 

**Note:** This is only required as you have only just added the Posture Profiles at the Zscaler Client Connector Portal.
  - b. Open a browser and confirm that you can access the Intranet pages;
  - c. Confirm that you can access the corporate file share at **\shares.patraining[1-N].safemarch.com\Content**.
 

**Note:** These tests confirm that corporate Windows PCs that are domain-joined OR have a client certificate from the corporate PKI AND are using the Zscaler Client Connector and can successfully access the corporate applications.

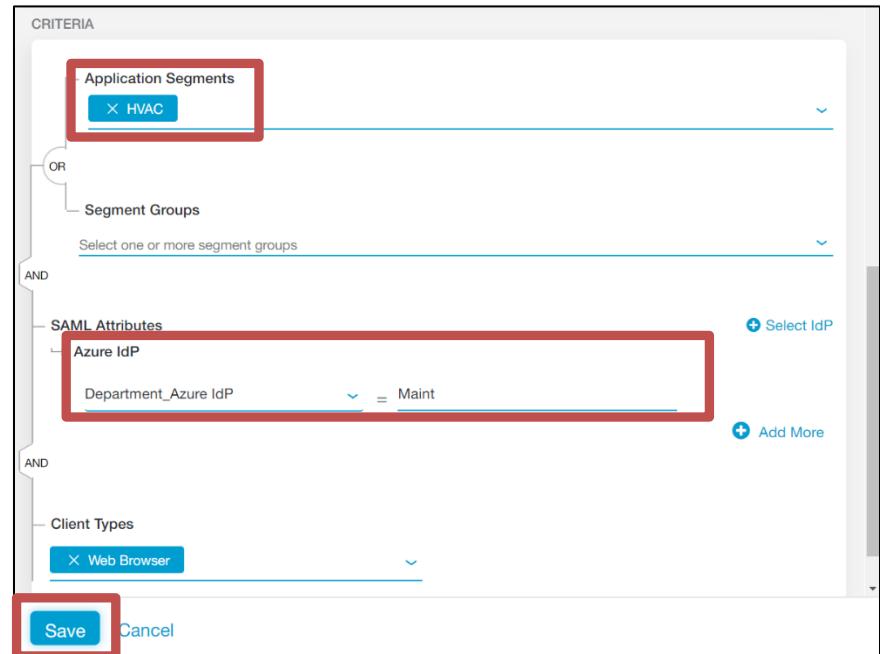


## Lab 8: Configure Advanced Access Policy

### Manage Vendor Access

In this section you will manage the Access Policy to control access for the HVAC vendor.

10. In the ZPA Admin Portal, go to the **Administration > POLICY MANAGEMENT > Access Policy** page and click to **Edit** the rule named **Allow HVAC**.
11. This rule is already targeted only against the **HVAC Application Segment** and is already configured for Browser Access only, the only remaining configuration required is to target it against the **Maint Department** using a SAML attribute:
  - a. Click **Select IdP** and select **Azure IdP**.
  - b. Click in the **Select a SAML Attribute** field, select the attribute named **Department\_Azure IdP** and configure the value to match as **Maint**.
  - c. Click **Save**.



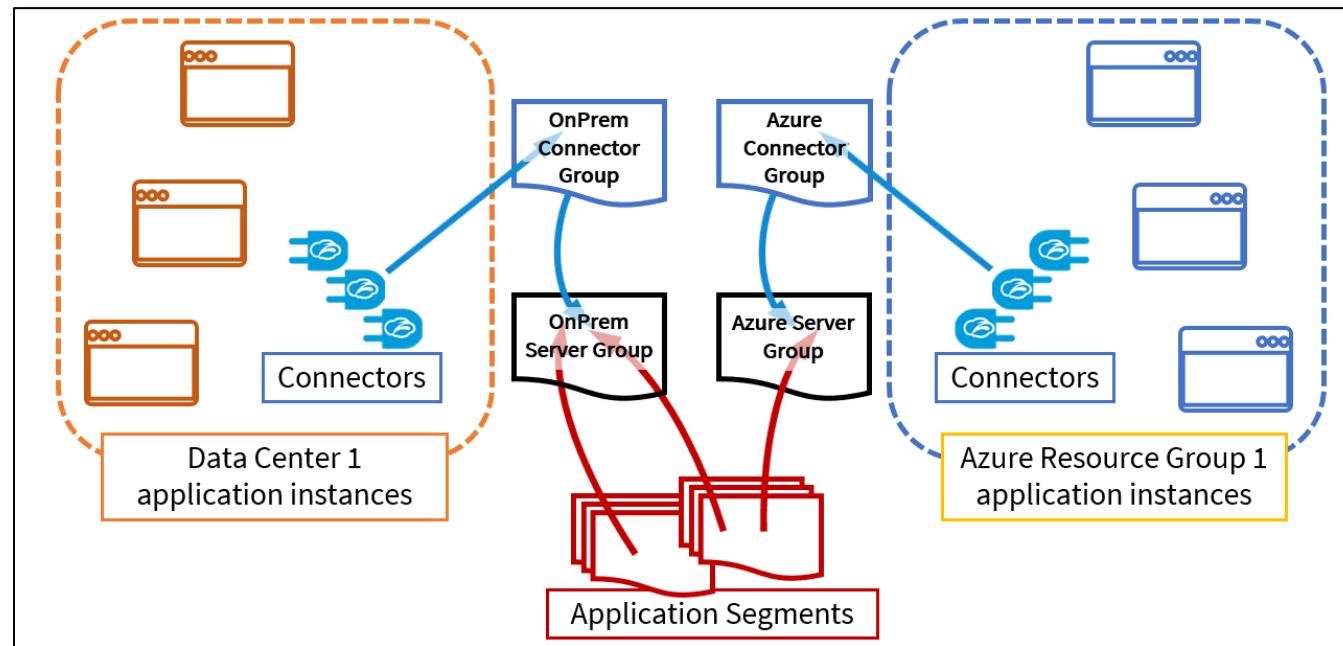
12. From the VM named **Remote: Linux Client PC** test connectivity to the **HVAC** application when logged in as the **hvac@patraining[1-N].safemarch.com** user.
13. Also test if the **student@patraining[1-N].safemarch.com** user can access the application in a browser.  
**Note:** This should fail, as the student user is not a member of the department named **Maint**. If necessary open a new Private tab in Firefox to log in as the new user.
14. In the ZPA Admin Portal, check the **Diagnostics** page for recent activity.

## Lab 8: Configure Advanced Access Policy

15. Lastly, manage access using RDP to restrict non-admin users from using that application:
    - a. Remove the Application Segment named **RDP** from the Segment Group named **CorpApps**;
    - b. Add a new Segment Group named **Admin**, with only the Application Segment named **RDP**;
    - c. Add an Access Policy rule to allow the **Admin** Segment Group for **Azure** users that are members of the Department named **Admin**, using **Zscaler Client Connector** only, with either the **Domain Joined** or **Client Cert from Safemarch CA** Posture Profiles verified.
    - d. Move this rule above the **Allow CorpApps** rule;
    - e. On the **Corp: Client PC**, logout of Zscaler Client Connector, log back in as **student@patraining[1-N].safemarch.com** and test whether you can now access the server using RDP;
    - f. Login to Zscaler Client Connector as the user **smadmin@patraining[1-N].safemarch.com** with password **Admin-123!** and test whether you can access the server using RDP.
- Note:** If you do not see entries in the Diagnostics for the **smadmin@patraining[1-N].safemarch.com** user, on the **Corp: Client PC** logout out of the Zscaler Client Connector, open IE and clear all cache settings and close the browser. Then log back into Z App as that user.
- g. Test whether the user **smadmin@patraining[1-N].safemarch.com** can access the Intranet web pages or the corporate file share.
- Note:** These should both fail, as access to them has been restricted to members of the Department named **Marketing**.

## Lab 9: Configure LSS

In this Lab you will activate a Syslog server in Azure, add an App Connector in Azure and configure log streaming to the Syslog server. To access the Syslog server, you will use ZPA through the same App Connector. To achieve this, you need to add an App Connector Group and Server Group, which allows you to map the Application Segments to their correct logical destinations (on-premise App Connectors or Azure App Connectors), as indicated in the diagram.



**Note:** Best Practice is to use separate App Connector Groups for application access and LSS; for convenience in the Lab, we will use one App Connector Group for both.

### Activate the LSS Infrastructure

In this section you will activate the Syslog server in Azure, then add and activate an App Connector in a new App Connector Group adjacent to it.

1. Open a browser and navigate to the Azure portal page at <https://portal.azure.com> and login with the credentials supplied in the joining instructions.

**Note:** You can access the Admin Portal direct from your own PC.

2. In the left-hand navigation menu click **Virtual machines**, then select only the VM named **Host-1** and click **Start** and confirm.

Name	Type	Status	Resource Group
Host-1	Virtual machine	Stopped (deallocated)	patrain
syslog	Virtual machine	Stopped (deallocated)	patrain

## Lab 9: Configure LSS

3. Wait until **host-1** status shows that it is **Running** (it has the DNS server for this subnet), then select only the VM named **syslog**, click **Start** and confirm.

**Note:** It may take a few minutes for each of the VMs to start.

The screenshot shows the Microsoft Azure portal's Virtual Machines page. The top navigation bar includes 'Home', 'Virtual machines', 'patraining1', 'Subscriptions: patraining1', and a search bar. On the left, there's a sidebar with 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main area is titled 'Virtual machines' with 'patraining1' listed. A red box highlights the '+ Add' button in the top right corner of the main content area.

4. In the Azure Portal on the **Virtual Machines** page, click **Add** to add a ZPA App Connector virtual machine, and configure the **Basics**:

- a. Configure the virtual machine **Project details** so that the App

Connector will be on the same subnet as the **host-1** server:

- Subscription: **patraining[1-N]**;
- Resource group: **patraining[1-N]ResourceGroup** or **PATRNING[1-N]RESOURCEGROUP**.

**Note:** For some pods the **Resource Group** may be named **patraining[1-N]**. Do *NOT* create a new Resource group, use the one that already exists!

The screenshot shows the 'Project details' step in the Azure VM creation wizard. It asks to select a subscription and resource group. The 'Subscription' dropdown is set to 'patraining8' and the 'Resource group' dropdown is set to 'patraining8ResourceGroup'. Both are highlighted with red boxes. A 'Create new' link is also visible.

- b. Configure the virtual machine **Instance Details** as a ZPA App Connector for Azure Compute of a Standard B2s size in East US:

- Virtual machine name: **ZPAConector**;
- Region: **East US**;
- Image: Click **Browse all public and private images**, search for and select **Zscaler Private Access Connector for Azure Compute**;
- Azure Spot instance: Set to **No**;
- Size: Click **Change size** and scroll down to the **B2s** option (2 x VCPUs, LOCAL SSD), click to highlight it and click **Select**.

The screenshot shows the 'Instance details' step in the Azure VM creation wizard. It includes fields for 'Virtual machine name' (set to 'ZPAConector'), 'Region' (set to '(US) East US'), 'Image' (set to 'Zscaler Private Access Connector for Azure Compute' with a red box around it and 'Browse all public and private images' link), 'Azure Spot instance' (set to 'No'), and 'Size' (set to 'Standard B2s' with a red box around it and 'Change size' link). Other options like 'Availability options' and 'No infrastructure redundancy required' are also shown.

## Lab 9: Configure LSS

- c. Configure the **Administrator Account**:
  - **Authentication type:** Password;
  - **Username:** to patraining;
  - **Password:** to Zscaler-123!
  
- d. Configure the **INBOUND PORT RULES** to allow SSH connections:
  - Select the **Allow selected ports** option;
  - In the **Select inbound ports** field select **SSH (22)**.
  - At the bottom, click **Next : Disks >**
  
- 5. Specify to use **Unmanaged** disks:
  - a. Leave the **OS disk type** at the default setting (should be **Premium SSD**);
  - b. **Scroll down** and click to expand the **Advanced** settings;
  - c. For the **Use managed disks** option, select the **No**;
  - d. At the bottom, click **Next : Networking >**
  
- 6. Verify that the ZPA Connect virtual machine will be configured on the same subnet as the **host-1** application server and verify:
  - **Virtual network:** patraining[1-N]ResourceGroup-vnet;
  - **Subnet:** (10.0.0.0/24);
  - **Public IP:** (new) ZPAConector-ip;
  - **Select inbound ports:** Confirm SSH is shown.

**Caution:** Check the IP subnet! Be sure it is 10.0.0.0/24!

**Administrator account**

Authentication type  Password  SSH public key

\* Username

\* Password

\* Confirm password

**INBOUND PORT RULES**

Select which virtual machine network ports are accessible from the public internet. You can specify network access on the Networking tab.

\* Public inbound ports  None  Allow selected ports

\* Select inbound ports  SSH

**Review + create** **< Previous** **Next : Disks >**

**Advanced**

Use managed disks  No  Yes

Storage account \*  [Create new](#)

**Review + create** **< Previous** **Next : Networking >**

**Network interface**

When creating a virtual machine, a network interface will be created for you.

\* Virtual network  [Create new](#)

\* Subnet  [Manage subnet configuration](#)

Public IP

## Lab 9: Configure LSS

7. Review the settings and create the virtual machine:
- Click the **Review + create** button at the bottom of the window;
  - Verify that **Validation passed** is displayed;  
**Note:** If the **Preferred phone number** is not configured, enter **+11234567890**.
  - Review the settings and click **Create**;
  - If prompted that **unsaved edits will be discarded**, just click **OK**;
  - Verify that after a few seconds the page refreshes and displays **...Your deployment is underway**.  
**Note:** Creating the VM may take several minutes.

8. After **Your deployment is complete** is displayed, record the public IP address of the **ZPAConector**:
- Click the **Go to resource** button;
  - Record the **Public IP address** of the VM (it will be needed later).

**Note:** We suggest you copy the IP address and paste it into Notepad for later use.

The screenshot shows the Azure portal interface for creating a virtual machine. The 'Create' button is highlighted with a red box. The Public IP address (40.121.59.165) is also highlighted with a red box. The portal shows the following details:

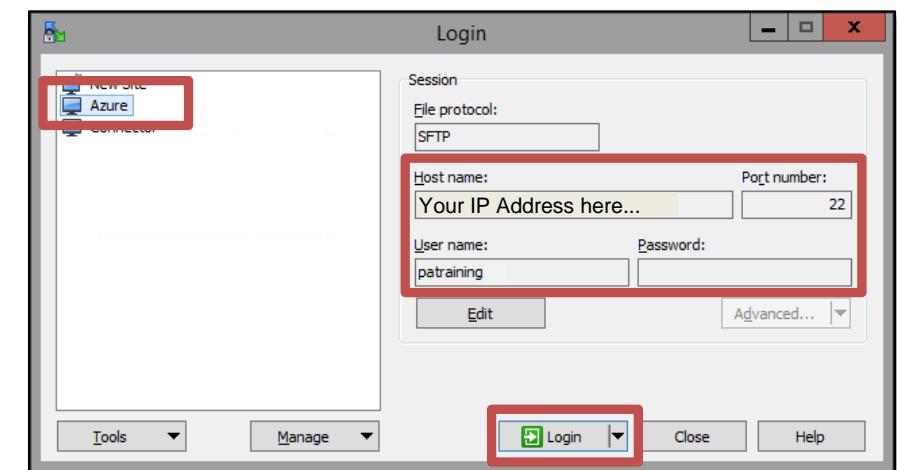
Name	pa training
* Preferred e-mail address	admin@patraining1.safemarch.com
* Preferred phone number	+11234567890
<b>BASICS</b>	
Subscription	patraining1
Resource group	patraining1ResourceGroup
Virtual machine name	ZPAConector
Region	East US
Availability options	No infrastructure redundancy required
Authentication type	Password
Username	patraining1
Public inbound ports	SSH

## Lab 9: Configure LSS

### Activate the Azure App Connector

In this section, you will activate the App Connector software on the Azure VM and provide the provisioning key in exactly the same way that you did for the on-premise App Connector.

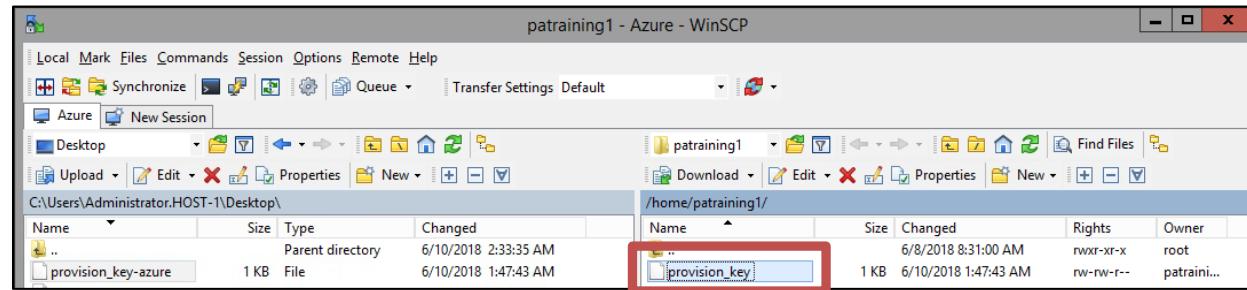
9. On the VM labelled **Corp: Win Svr 2016**, open a browser and access the **ZPA Admin Portal** using the URL <https://admin.private.zscaler.com> and credentials supplied in the joining instructions.  
**Note:** You need to do this from the Windows 2016R2 Server VM, as you will need to upload a file to Azure from that machine.
10. From the **Administration** menu under **CONNECTOR MANAGEMENT**, select **Connectors**, Click the icon at top right and run through the wizard as before to add a new App Connector with the following details:
  - a. Use the **Create a new provisioning key** option;
  - b. Use the certificate named **Connector**;
  - c. Use the **Add Connector Group** option to create a group named **Connectors-LSS**, with an update schedule of **Monday at 00:00**, located in **NYC, NY, USA**;
  - d. Name the new provisioning key **Azure** and specify a Maximum Reuse of Provisioning Key of **4**.
  - e. Click **Next** and **Save**.
11. Copy the provisioning key, paste it to **Notepad** and save it to a file on the Windows **Desktop** named **provision\_key-azure.txt**. Click **Done** to complete the **Add Connector** wizard.
12. Start **WinSCP** using the icon on the desktop or in the taskbar;
  - a. Click **New Site** in the navigation panel at top left and specify an **SFTP** connection to the **public IP address** for the App Connector VM in Azure that you recorded earlier, with the username **patraining** and password **Zscaler-123!**
  - b. Save this connection as the site named **Azure**;
  - c. Select the new site, click **Login** and connect to the Azure App Connector, accept the certificate if necessary, and provide the password **Zscaler-123!** when prompted;
  - d. In the left-hand panel of **WinSCP** (the local Windows server), from the **Desktop** folder select the file **provision\_key-azure.txt**;
  - e. Right-click on the file and select **Upload**;



## Lab 9: Configure LSS

- f. Once the file has been uploaded, right-click on it in the right-hand panel of WinSCP, select the **Rename** option and change the file name to just **provision\_key**.

**Caution:** The file name on the App Connector VM MUST be just **provision\_key** ! ALL in lowercase, with NO file extension.



13. Open **PuTTY** from the server desktop or Task Bar and connect using **SSH** to the Azure App Connector VM **public IP address** that you recorded earlier. Accept the certificate and login using the username **patraining** and password **Zscaler-123!**

**Note:** Alternatively, in Azure there is a **Serial Console** app for the App Connector at the bottom of the list of available apps, in the **Support + troubleshooting** section.

14. Repeat the CLI commands on the Azure App Connector that you used to bring up the App Connector in Skytap:
- First identify the current directory with the command **pwd** (you should be in **/home/patraining**);
  - List the contents of the directory with the command **ls** and confirm that the file **provision\_key** is there and has the correct file name;
  - Stop the App Connector service with the command **sudo systemctl stop zpa-connector** (enter the password **Zscaler-123!** when prompted);
  - Move the file to the correct Zscaler directory using the command **sudo cp provision\_key /opt/zscaler/var/provision\_key**
- Caution:** The name of the file is critical to the correct loading of the provisioning key; *it is case sensitive!*
- Check that the file is there using the command **sudo ls /opt/zscaler/var**
  - Now restart the App Connector service with the command **sudo systemctl start zpa-connector**
  - After 10s or so, check the status of the App Connector using the command **sudo systemctl status zpa-connector**
  - Verify that the App Connector is active and has established a connection to the ZPA infrastructure.
15. In a browser, login to the **ZPA Admin Portal**, navigate to the **Administration > CONNECTOR MANAGEMENT > Connectors** page, and confirm that the App Connector is listed. You have the options as before to review and manage the installed software version.

## Lab 9: Configure LSS

### Add an Application Segment for the Syslog Server

In this section, you will create an Application Segment for the Syslog server, with a separate Segment Group (to allow flexibility in targeting policy), and a new Server Group (to allow segregation of applications by logical location). You will map the new Server Group to the **Connectors-LSS** App Connector Group that you have just created, so that ONLY the App Connector in Azure will attempt to find the Syslog server.

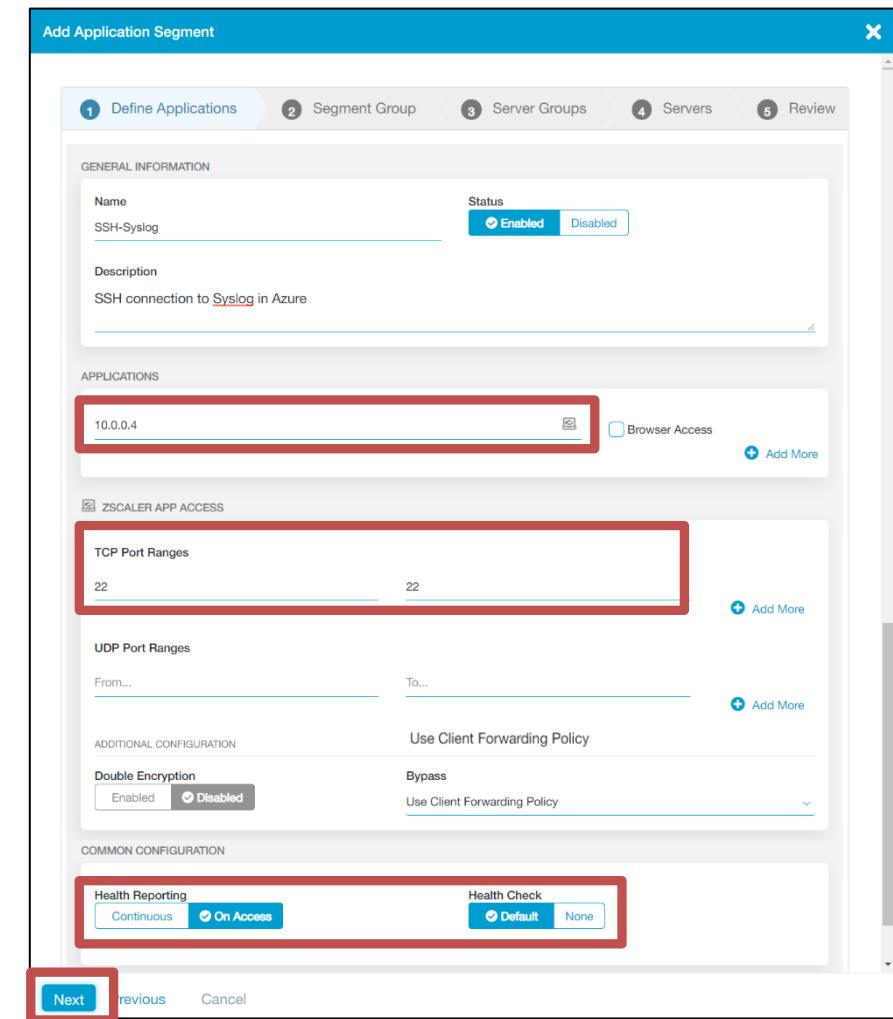
**Note:** Best Practice is to use separate App Connector Groups for application access and LSS; for convenience in the Lab, we will use one App Connector Group for both.

16. In the ZPA Admin Portal, navigate to the **Administration > APPLICATION MANAGEMENT > Application Segments** page and click the **+ Add Application Segment** icon at top right.

17. At the **Define Application** step of the wizard, configure the following:
  - a. **Name:** Set to **SSH-Syslog**;
  - b. **Status:** Set to **Enabled**;
  - c. **APPLICATIONS:** Specify IP Address **10.0.0.4**;
  - d. **TCP Port Range:** Add range from **22** to **22**.
  - e. **UDP Port Range:** Leave blank;
  - f. **Double Encryption:** Set to **Disabled**;
  - g. **Bypass:** Set to **Use Client Forwarding Policy**;
  - h. **Health Reporting:** Set to **On Access**;
  - i. **Health Check:** Set to **Default**;
  - j. **Zscaler App can receive CNAME:** Set to **Enabled**;
  - k. Click **Next**.

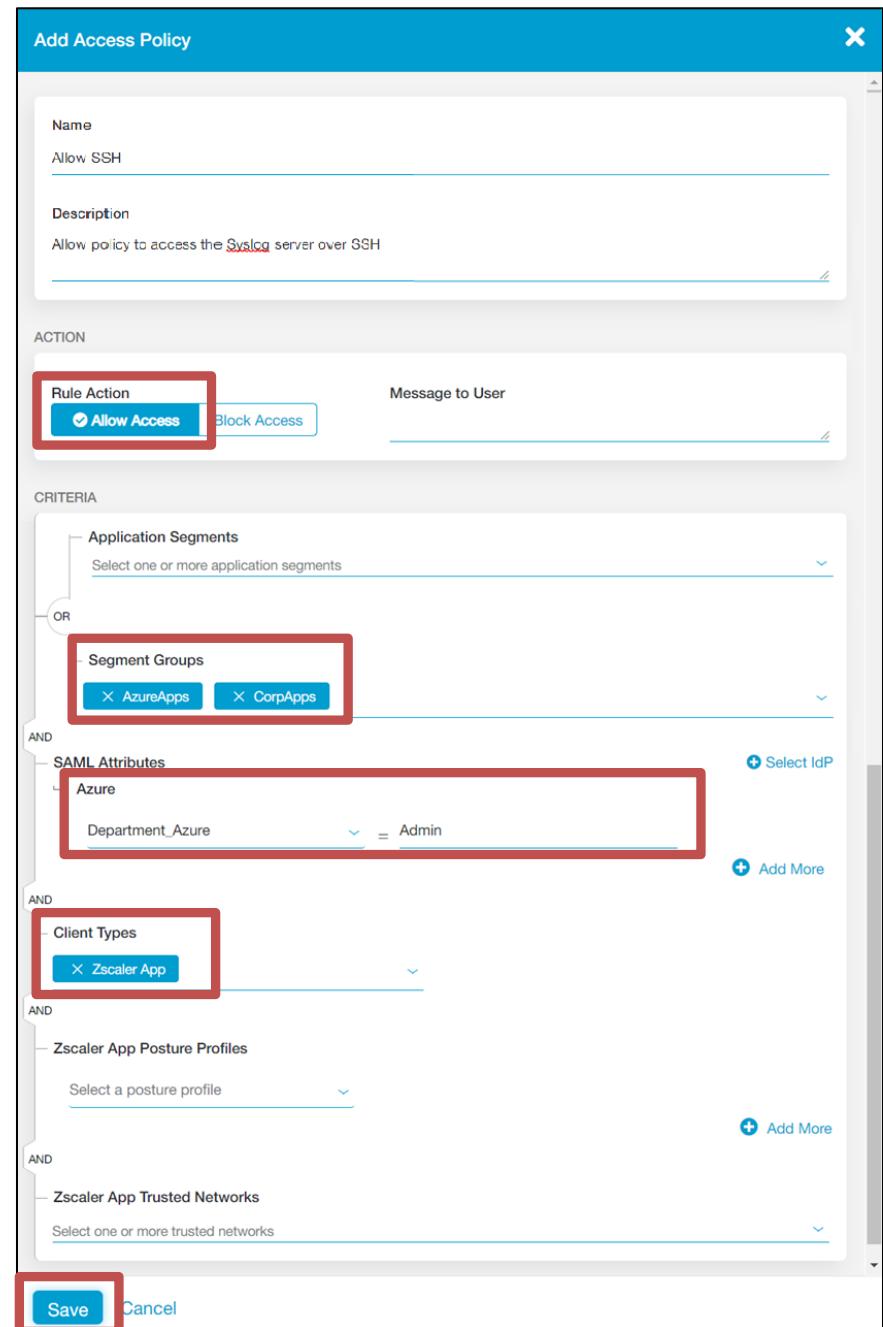
18. At the **Segment Group** step of the wizard, click **Add Segment Group**, name the group **AzureApps**, optionally add a description, verify that the **Status** is set to **Enabled**, and click **Next**.

19. At the **Server Groups** step of the wizard, click **Add Server Group** as follows:
  - a. **Name:** Set to **AzureServers**;
  - b. **Status:** Set to **Enabled**;
  - c. **Dynamic Server Discovery:** Set to **On**;
  - d. **Connector Groups:** Add ONLY the group named **Connectors-LSS**;
  - e. Click **Next**.



## Lab 9: Configure LSS

20. At the **Review** step click **Save**.
  21. To add an access policy rule for this application, click **Edit Policy**.
  22. Add a policy rule to allow access to this application as follows:
    - a. On the **Access Policy** page, click **Add Rule**;
    - b. Name the rule **Allow SSH** and optionally add a description;
    - c. Set the **Action** to **Allow Access**;
    - d. In the **Segment Groups** field, select both the **AzureApps** and **CorpApps** Segment Groups and click **Done**;
    - e. Under **SAML Attributes**, add the **Azure** attribute named **Department** with the value **Admin**;
    - f. Set the **Client Types** option set to **Zscaler App** and click **Done**;
    - g. Click **Save**.
  23. Click the **Rule Order** number for this new rule and type in the number **2** and press Enter.
- Note:** This is a very specific rule and should be positioned high up on the Access Policy rule list.

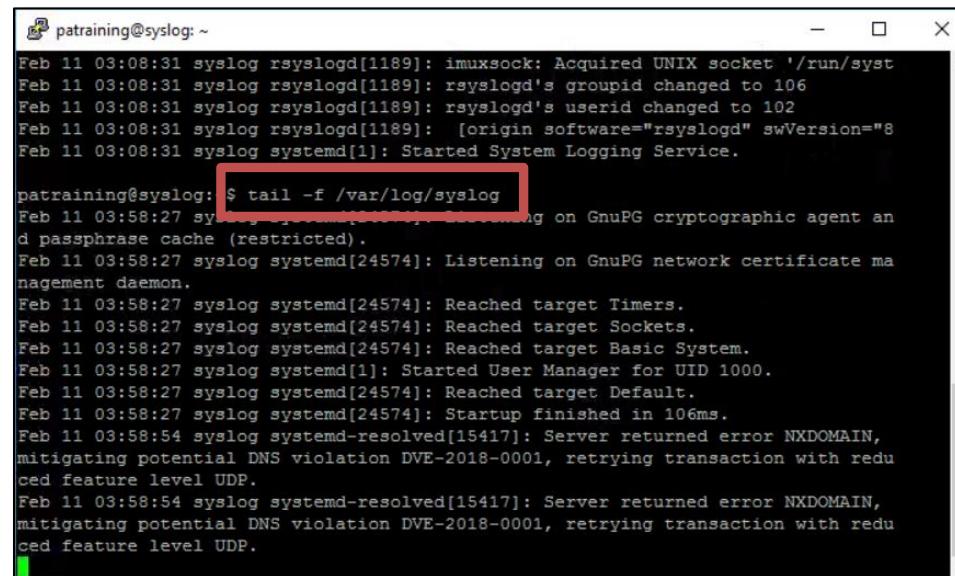


## Lab 9: Configure LSS

### Activate the Syslog Server

In this section, you access the Syslog server in Azure over ZPA from the Windows Client PC. You will activate the Syslog it to listen for log traffic on port 514.

24. Go to the VM named **Corp: Client PC**, open the Zscaler Client Connector and logout, then login as the user **smadmin@patraining[1-N].safemarch.com**.
25. Open the web browser and try to navigate to the Intranet web pages (be sure to refresh the page). Verify that Intranet access is available to this user.  
**Note:** If you do not see entries in the Diagnostics for the **smadmin@patraining[1-N].safemarch.com** user, on the **Corp: Client PC** logout out of the Zscaler Client Connector, open IE and clear all cache settings and close the browser. Then log back into Z App as that user.
26. From the Windows **Status Bar**, click the icon to open **PuTTY**.
27. Enter the IP address **10.0.0.4**, verify that the Port is set to **22** and click **Connect**. Accept the certificate, then login to the Syslog VM with the username **patraining** and password **Zscaler-123!**
28. Start the Syslog service using the command **sudo systemctl start rsyslog**
29. Check the status using the command **sudo systemctl status rsyslog** (use the **Ctl C** combination to exit the status display).
30. To view Syslog entries as they are received, enter the command **tail -f /var/log/syslog**
31. Leave the console open so you can come back and check for Syslog activity once LSS is configured.



```
patraining@syslog: ~
Feb 11 03:08:31 syslog rsyslogd[1189]: imuxsock: Acquired UNIX socket '/run/syslogd'
Feb 11 03:08:31 syslog rsyslogd[1189]: rsyslogd's groupid changed to 106
Feb 11 03:08:31 syslog rsyslogd[1189]: rsyslogd's userid changed to 102
Feb 11 03:08:31 syslog rsyslogd[1189]: [origin software="rsyslogd" swVersion="8"]
Feb 11 03:08:31 syslog systemd[1]: Started System Logging Service.

patraining@syslog: $ tail -f /var/log/syslog
Feb 11 03:58:27 syslog systemd[1]: Listening on GnuPG cryptographic agent and passphrase cache (restricted).
Feb 11 03:58:27 syslog systemd[24574]: Listening on GnuPG network certificate management daemon.
Feb 11 03:58:27 syslog systemd[24574]: Reached target Timers.
Feb 11 03:58:27 syslog systemd[24574]: Reached target Sockets.
Feb 11 03:58:27 syslog systemd[24574]: Reached target Basic System.
Feb 11 03:58:27 syslog systemd[1]: Started User Manager for UID 1000.
Feb 11 03:58:27 syslog systemd[24574]: Reached target Default.
Feb 11 03:58:27 syslog systemd[24574]: Startup finished in 106ms.
Feb 11 03:58:54 syslog systemd-resolved[15417]: Server returned error NXDOMAIN, mitigating potential DNS violation DVE-2018-0001, retrying transaction with reduced feature level UDP.
Feb 11 03:58:54 syslog systemd-resolved[15417]: Server returned error NXDOMAIN, mitigating potential DNS violation DVE-2018-0001, retrying transaction with reduced feature level UDP.
```

## Lab 9: Configure LSS

### Add Log receivers

In this section, you will create two Log Receivers to separately stream App Connector Status and User logs. In this case the destination for both streams will be the Syslog server in Azure.

32. In the **ZPA Admin Portal** navigate to the **Administration > LOG STREAMING SERVICE > Log Receivers** page and click the **+ Add Log Receiver** link to add a new Log Receiver.
33. Configure a log stream for **Connector Status** as follows:
  - a. **Name:** Syslog-Connectors;
  - b. **Description:** as preferred;
  - c. **Domain or IP Address:** The private IP address of the Syslog server on the VLAN in Azure (**10.0.0.4**);
  - d. **TCP Port:** 514;
  - e. **Connector Groups:** Select the group **Connectors-LSS** that you just created and click **Done**;
  - f. Click **Next**;
  - g. **Log Type:** Select **Connector Status**;
  - h. **Log Template:** Leave it set to **CSV**;
  - i. **Log Stream Content:** Leave it at the default values;
  - j. **Session:** Leave all options at the default setting;
  - k. Click **Next**, review the configuration and click **Save**.

## Lab 9: Configure LSS

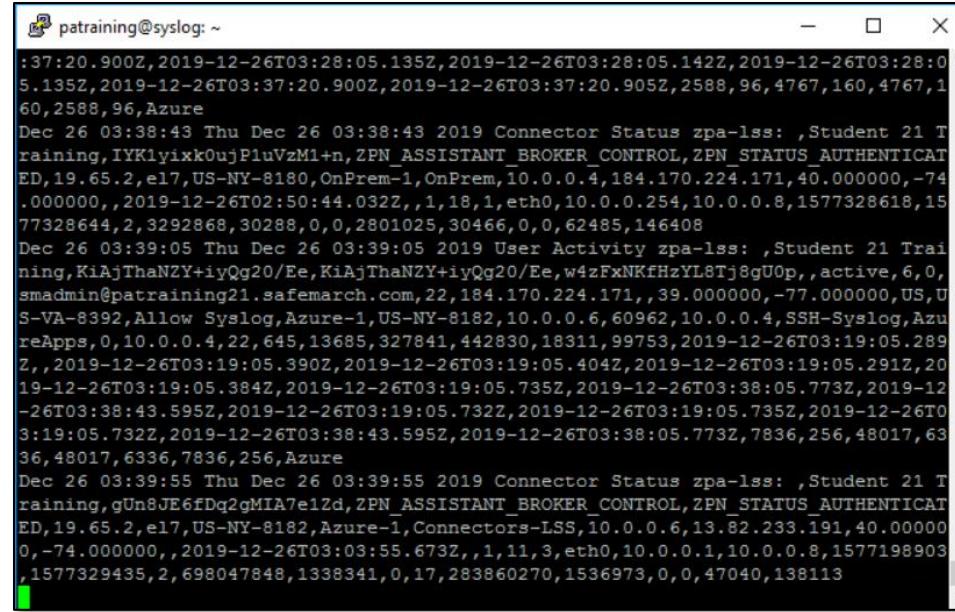
34. In the **ZPA Admin Portal** navigate to the **Administration > LOG STREAMING SERVICE > Log Receivers** page and click the **+ Add Log Receiver** link to add a new Log Receiver.

35. Configure a log stream for **User Activity** as follows:

- a. **Name:** Syslog-UserActivity;
- b. **Description:** as preferred;
- c. **Domain or IP Address:** The private IP address of the Syslog server on the VLAN in Azure (**10.0.0.4**);
- d. **TCP Port:** 514;
- e. **Connector Groups:** Select the group **Connectors-LSS** that you just created and click **Done**;
- f. Click **Next**;
- g. **Log Type:** Select **User Activity**;
- h. **Log Template:** Leave it set to **CSV**;
- i. **Log Stream Content:** Leave it at the default values;
- j. **POLICY:** Leave all options at their default settings (all **Attributes**, all **Application Segments**, all **Segment Groups**, all **Client Types**, all **Sessions**);
- k. Click **Next**;
- l. Review the configuration and click **Save**.

## Lab 9: Configure LSS

36. Generate some traffic over ZPA from the Client PC (open the Intranet pages and/or the file share).
37. Go back to PuTTY session for the **syslog** VM and watch for log messages from ZPA.



```

patraining@syslog: ~
:37:20.900Z,2019-12-26T03:28:05.135Z,2019-12-26T03:28:05.142Z,2019-12-26T03:28:05.135Z,2019-12-26T03:37:20.900Z,2019-12-26T03:37:20.905Z,2588,96,4767,160,4767,160,2588,96,Azure
Dec 26 03:38:43 Thu Dec 26 03:38:43 2019 Connector Status zpa-lss: ,Student 21 Training,IYK1yixk0ujPluVzM1+n,ZPN_ASSISTANT_BROKER_CONTROL,ZPN_STATUS_AUTHENTICATED,19.65.2.e17,US-NY-8180,OnPrem-1,OnPrem,10.0.0.4,184.170.224.171,40.000000,-74.000000,,2019-12-26T02:50:44.032Z,,1,18,1,eth0,10.0.0.254,10.0.0.8,1577328618,1577328644,2,3292868,30288,0,0,2801025,30466,0,0,62485,146408
Dec 26 03:39:05 Thu Dec 26 03:39:05 2019 User Activity zpa-lss: ,Student 21 Training,KiAjThaNZY+iyQg20/Ee,KiAjThaNZY+iyQg20/Ee,w4zFxNkfHzYL8Tj8gUOp,,active,6,0,smadmin@patraining21.safemarch.com,22,184.170.224.171,,39.000000,-77.000000,US,U-S-VA-8392,Allow Syslog,Azure-1,US-NY-8182,10.0.0.6,60962,10.0.0.4,SSH-Syslog,AzureApps,0,10.0.0.4,22,645,13685,327841,442830,18311,99753,2019-12-26T03:19:05.289Z,,2019-12-26T03:19:05.390Z,2019-12-26T03:19:05.404Z,2019-12-26T03:19:05.291Z,2019-12-26T03:19:05.384Z,2019-12-26T03:19:05.735Z,2019-12-26T03:38:05.773Z,2019-12-26T03:38:43.595Z,2019-12-26T03:19:05.732Z,2019-12-26T03:19:05.735Z,2019-12-26T03:19:05.732Z,2019-12-26T03:38:43.595Z,2019-12-26T03:38:05.773Z,7836,256,48017,6336,48017,6336,7836,256,Azure
Dec 26 03:39:55 Thu Dec 26 03:39:55 2019 Connector Status zpa-lss: ,Student 21 Training,gUn8JE6fDq2gMIA7e1Zd,ZPN_ASSISTANT_BROKER_CONTROL,ZPN_STATUS_AUTHENTICATED,19.65.2.e17,US-NY-8182,Azure-1,Connectors-LSS,10.0.0.6,13.82.233.191,40.000000,-74.000000,,2019-12-26T03:03:55.673Z,,1,11,3,eth0,10.0.0.1,10.0.0.8,1577198903,1577329435,2,698047848,1338341,0,17,283860270,1536973,0,0,47040,138113

```

## Make the Azure Resource Group go Dark

In this section, you will also configure and test SSH access to the Azure App Connector over ZPA. This would allow you to remove the public IP addresses for the Syslog and App Connector VMs and block inbound access to the Azure Resource Group on TCP port 22.

38. In the ZPA Admin Portal, navigate to the **Administration > APPLICATION MANAGEMENT > Application Segments** page and click to edit the entry for the Syslog server that you just added (SSH-Syslog). At the **General Information** step, click **Next**.
39. At the **Applications And Ports Configuration** step, in the **Applications** section (where the IP address **10.0.0.4** is listed), scroll down if necessary and click **+ Add More**. Add the **private IP address** of the Azure App Connector VM (should be **10.0.0.5** or **10.0.0.6** (check in the settings for that VM in Azure if necessary)). Then click **Next** and **Save**.
40. On the Windows Client PC, open another PuTTY instance and enter the private IP address of the Azure App Connector VM for a port 22 connection and click **Open**.

## *Lab 9: Configure LSS*

41. Accept the certificate warning and login to the App Connector VM.

```
[patraining@zpaconnector:~]$ ./hMMMMMMMMMMMMMMMMMMMMMMMMMMMMNhs0+//://`  
..+hMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNhs0+//://`  
` ``,-://:-hMMMMMMMMMMMMMMMMMMNds/-`  
` -+ydnMMMMMMMMMMMMMMMMMMMMMMMMNdo:`  
-smMMMMMMMMMMMMMMMMMMMMMMMMMMMMN+:/oyhdmmdyo-  
:hMMMMMMMMMMMMMMMMMMMMMMMMMMNNdNMMMMNmho:..`  
` yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNho-` ..:+yhdNMMMMMMMMMMNNhs/..`  
-mMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNMny/. ..:/ydNMMMMMMMMMMMMMMMMMMMd+`  
.mMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNMny/+ ..:+dNMNNDnhyysoosyhdNMMMMMMMMNs+`  
hMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNMMMo. -sddy+:-.` ..:/yMMMMMMMMMs  
.MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMd+` ..:-` ..:+nMMMMMMMM/  
+MMMMMMMMMMMMMMMMMMMMMMMMMMMMNs+` ..:-` ..:nMMMMMMNh  
:MMMMMMMMMMMMMMMMMMMMMMMMMMMMMs. ..:-` ..:nMMMMMMMd  
.MMMMMMMMMMMMMMMMMMMMMMMMNm: ..:-` ..:+osyyysso+/-.` ..:hMMMMMMMM/  
/MMMMMMMMMMMMMMMMMMMd. ..:+ohdNMMMMMMMMMMMMNNmdysoosyNMMMMMMNs+`  
/NMMMMMMMMMMMMMMMMNs. ..:/yNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNs. `:  
.hMMMMMMMMMMMMMMMd` ..:+dNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNNho:.`  
:yNMMMMMMMMMMMN. ..:/hNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNs/-`.  
.+hNMMMMMMMM/ ..:+mMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNs`  
`-/oyhhhs :mMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMNs`  
`/hNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMd+.`  
`-/+++++sdNMMMMMMMMMMMMMMMMMMMMMMMMMMMMNs/`  
.:/+osyyysso+/-`  
[patraining@zpaconnector ~]$
```

**Note:** You have now configured application access (SSH to Syslog and App Connector VMs) **AND** log streaming through the same App Connector in Azure. In the real-world, best practice is to have **separate** App Connector Groups (each with at least 2 App Connectors), one for application access and one for LSS.