Zscaler Private Access Workshop

Getting ZPA Working

Hands-on Lab Guide

Copyright

Trademark Statements

ZPA Workshop Lab Guide
2020, Rev. 1.0c

Contents

About the ZPA Workshop

Welcome to the ZPA Workshop that showcases the Zscaler Private Access (ZPA) service. During this workshop you will practice the fundamental skills that you require to get ZPA working. You will complete several tasks designed to increase your proficiency in configuring the ZPA solution.

Connecting to the Virtual Lab

The ZPA Workshop 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 Remote) and the following virtual machines (VMs):

- A Windows Client PC;
- A Windows 2016 Active Directory server and domain controller;
- A CentOS-based ZPA Connector;

Login Details

Details to allow you to access the lab infrastructure will be provided prior to the start of the workshop, 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 **admin@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 instruction provided to you prior to the session.

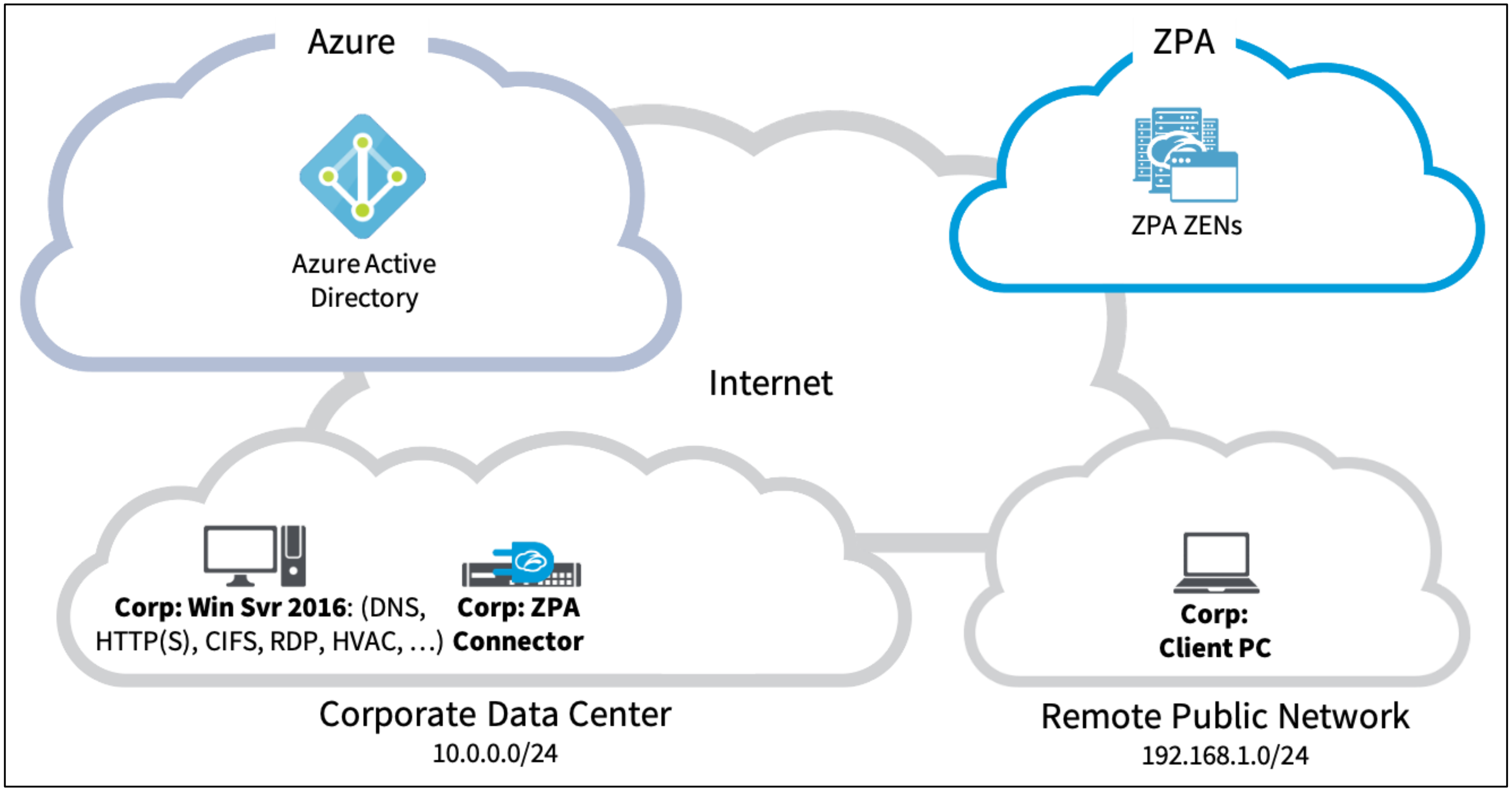
Admin Portal Access

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, an Azure environment including Azure AD as your primary IdP to authenticate Zscaler App users, allowing them access to a range of corporate applications through the local ZPA Connector.

- 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, connected to the remote public network (simulating a hotspot, home, or customer network).
- The **Corp: ZPA Connector** is a CentOS VM with the Connector RPM already installed. It must still be activated as an App Connector for ZPA service.



Lab 1: Enable Zscaler App 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.

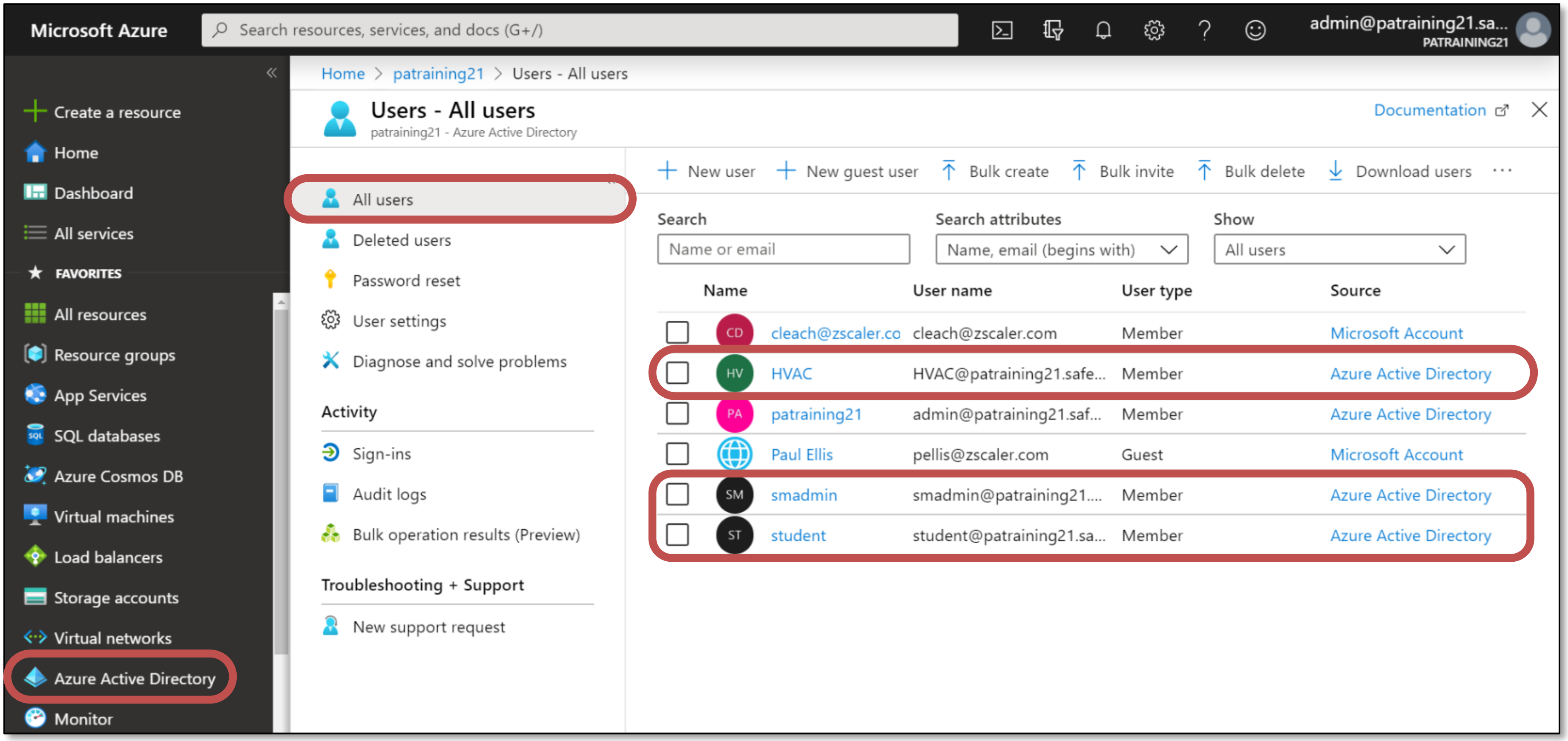
Verify AAD User Accounts

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.

   Note: You can access the Azure portal directly 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 (**student**, **hvac** and **smadmin**).



Search: Name or email

Search attributes: Name, email (begins with)

Show: All users

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

Create the unique SP Metadata for the IdP.

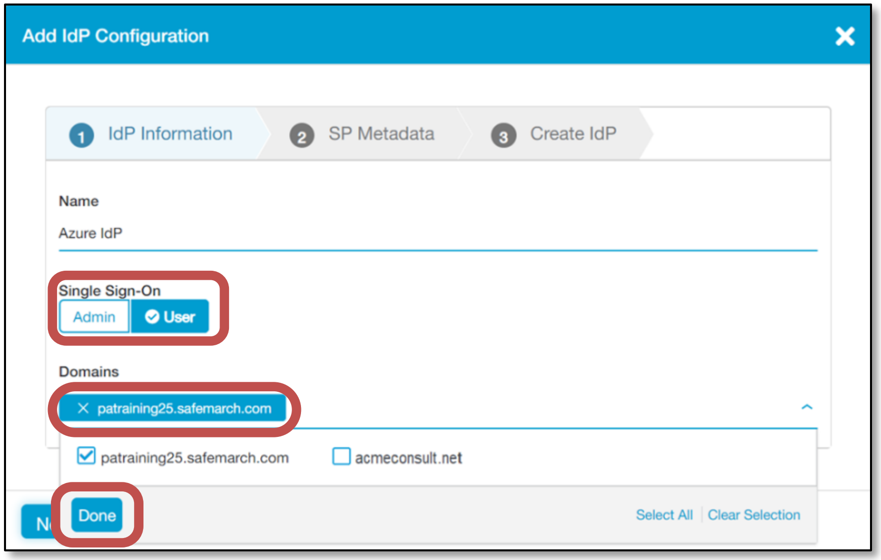
Configuring Azure as the IdP for ZPA is done in a sequence that involves configuration at both the ZPA Admin Portal and the Azure Portal. It begins at the ZPA Admin Portal with the generation of SP metadata for the IdP which will be then uploaded into Azure.

3. In a browser, load the ZPA Admin Portal at **https://admin.private.zscaler.com**, login with the credentials supplied in the joining instructions and 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 directly 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**.



Name: Azure IdP

Single Sign-On: Admin [✓ User]

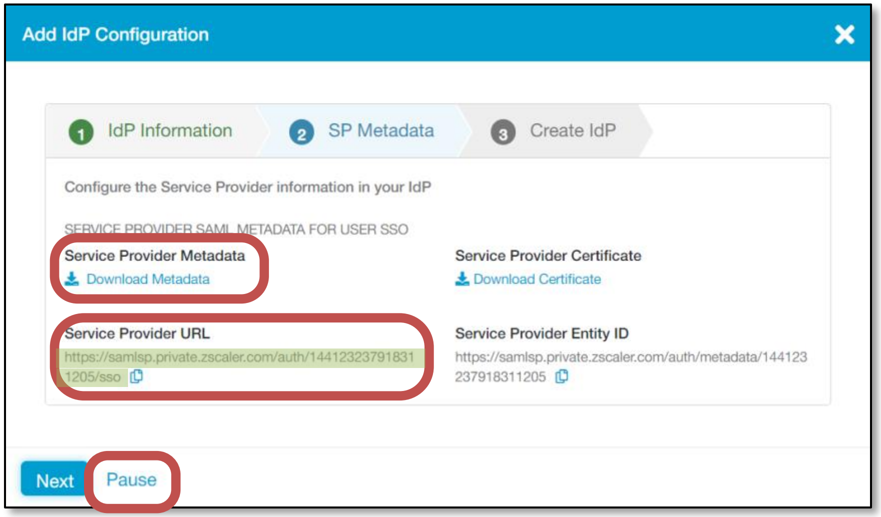
Domains: ✕ patraining25.safemarch.com

☑ patraining25.safemarch.com
□ acmeconsult.net

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.



Configure the Service Provider information in your IdP

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata

Service Provider Certificate

Service Provider URL: https://samlsp.private.zscaler.com/auth/144123237918311205/sso

Service Provider Entity ID: https://samlsp.private.zscaler.com/auth/metadata/144123237918311205

Configure Azure IdP for ZPA

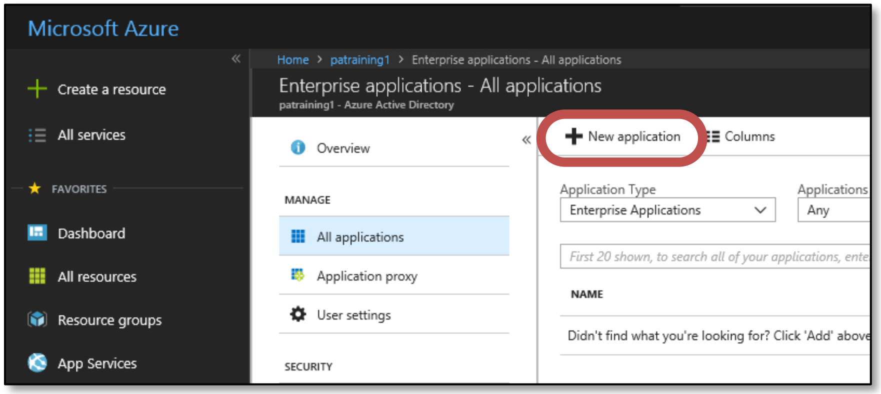
In this section, you will configure Azure AD to act as a SAML IdP to allow Zscaler App user authentication for ZPA access. Import the SP metadata file that was downloaded for this IdP from the ZPA Admin Portal.

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.

   Note: You may access the Azure Admin Portal directly 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**.

10. Click **New application**, then type **ZPA** into the search field under the heading **Add from the gallery**.

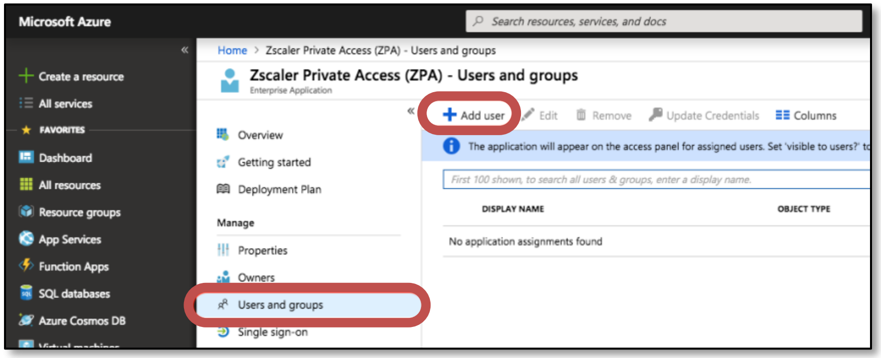


Didn't find what you're looking for? Click 'Add' above

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: Only the user or group authorized at this step will be able to authenticate to access the ZPA service.



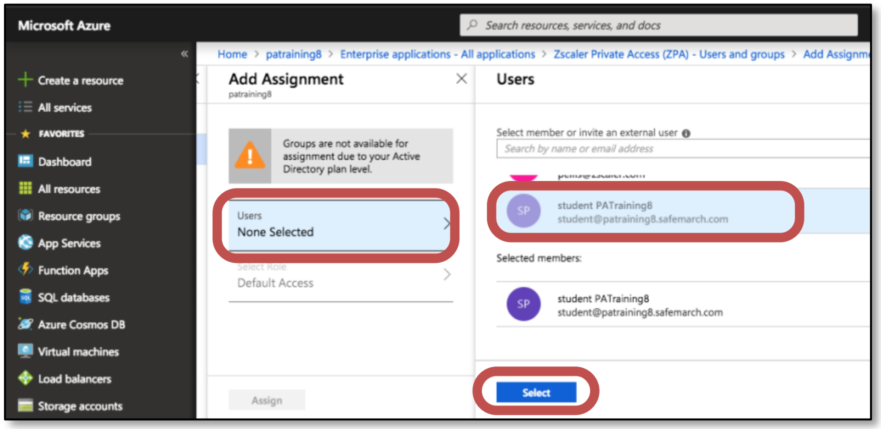
The application will appear on the access panel for assigned users. Set 'visible to users?' to

No application assignments found

13. Click **Users - None Selected**.

14. Select the user **student@patraining[1-N].safemarch.com**, then click **Select**.

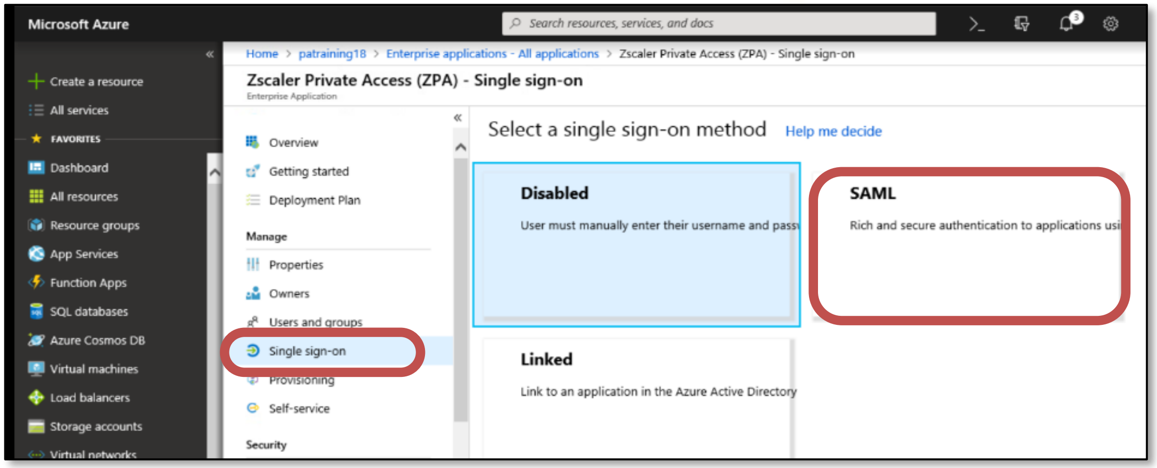
15. Verify that the page indicates **1 user selected**, then click **Assign**.



Groups are not available for assignment due to your Active Directory plan level.

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

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



Zscaler Private Access (ZPA) - Single sign-on
Enterprise Application

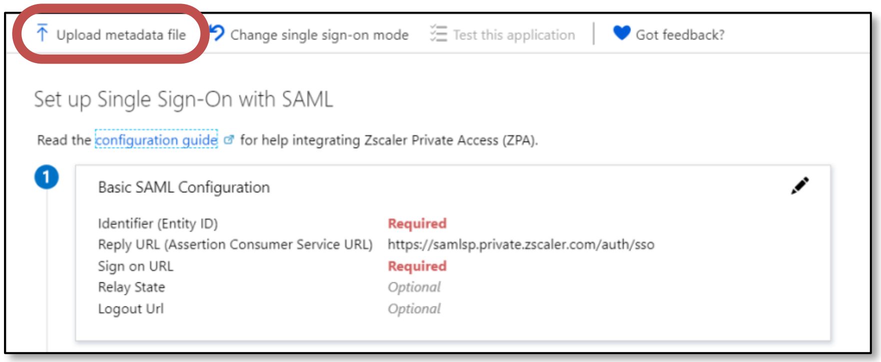
Select a single sign-on method Help me decide

Disabled
User must manually enter their username and pass

SAML
Rich and secure authentication to applications usi

Linked
Link to an application in the Azure Active Directory

18. Above the box labelled ❶ **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**.



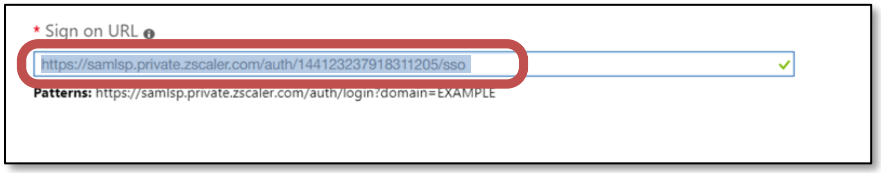
Set up Single Sign-On with SAML

Read the configuration guide for help integrating Zscaler Private Access (ZPA).

❶ Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	https://samlsp.private.zscaler.com/auth/sso
Sign on URL	Required
Relay State	Optional
Logout Url	Optional

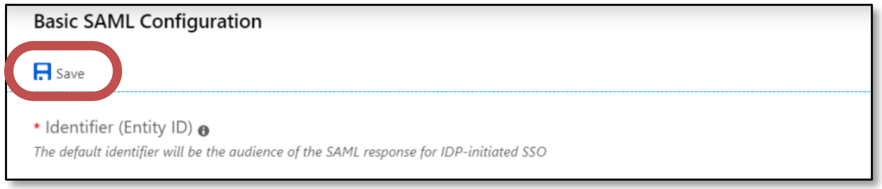
19. The **Identifier (Entity ID)** URL and the **Reply URL** will be populated automatically. However, you will need to correctly configure the **Sign on URL** field. Paste the **Service Provider URL** value that you copied from the **Add IdP Configuration** wizard in the ZPA Admin Portal.


* Sign on URL

https://samlsp.private.zscaler.com/auth/144123237918311205/sso ✓

Patterns: https://samlsp.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**.


Basic SAML Configuration

* Identifier (Entity ID)

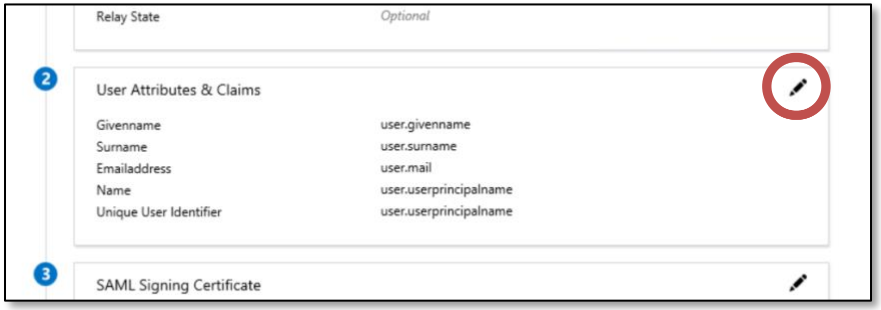
The default identifier will be the audience of the SAML response for IDP-initiated SSO

Lab 1: Enable Zscaler App 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.



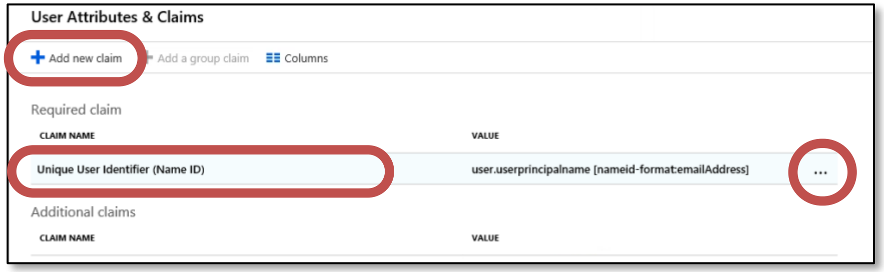
Relay State	Optional

2 User Attributes & Claims

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

3 SAML Signing Certificate

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



User Attributes & Claims

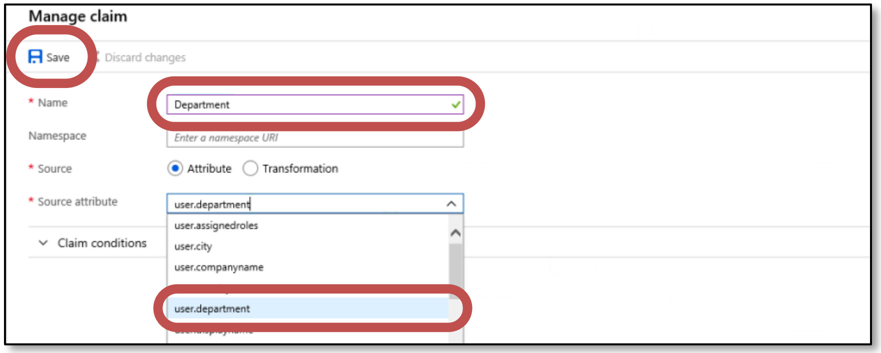
Required claim

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

Additional claims

CLAIM NAME	VALUE

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



Manage claim

* Name: Department

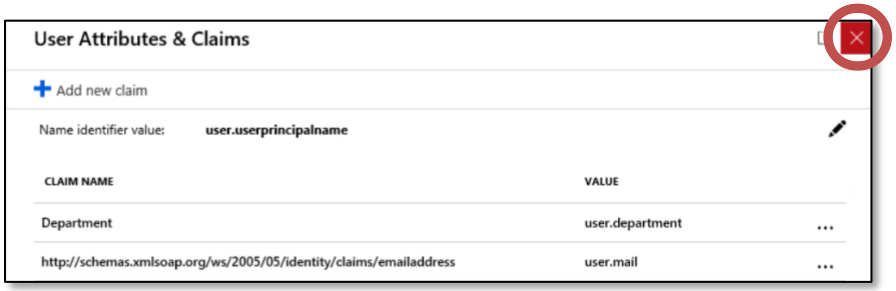
Namespace: Enter a namespace URI

* Source: ● Attribute ○ Transformation

* Source attribute: user.department

Claim conditions

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

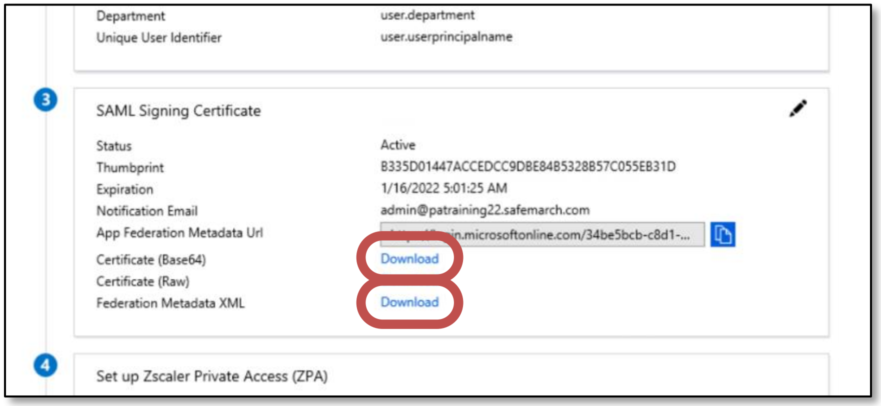


User Attributes & Claims

Name identifier value: **user.userprincipalname**

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

26. In the box labelled ❸ **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)**.



Department	user.department
Unique User Identifier	user.userprincipalname

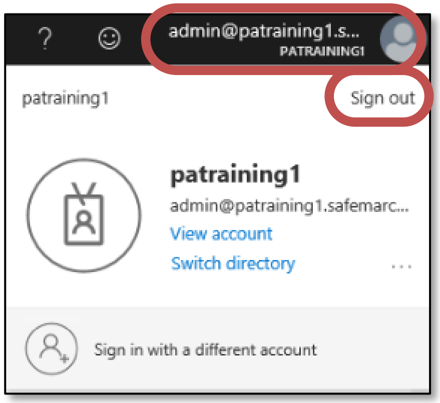
3 SAML Signing Certificate

Status	Active
Thumbprint	B335D01447ACCEDCC9DBE84B5328B57C055EB31D
Expiration	1/16/2022 5:01:25 AM
Notification Email	admin@patraining22.safemarch.com
App Federation Metadata Url	in.microsoftonline.com/34be5bcb-c8d1-...
Certificate (Base64)	Download
Certificate (Raw)	
Federation Metadata XML	Download

4 Set up Zscaler Private Access (ZPA)

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

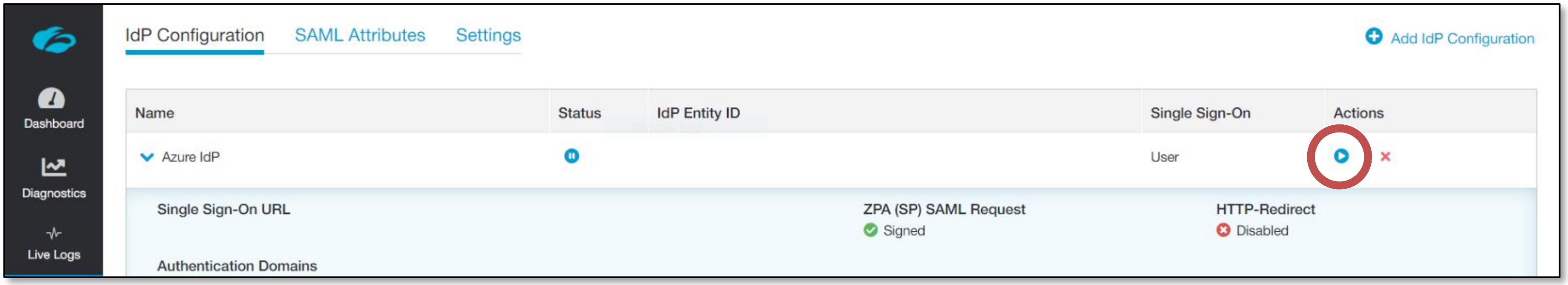
    Note: You need to sign out so that when later configuring the ZPA Admin Portal, it will prompt for authentication by a user assigned to ZPA in Azure AD. The **admin** user has not been assigned to the ZPA application in Azure.



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.

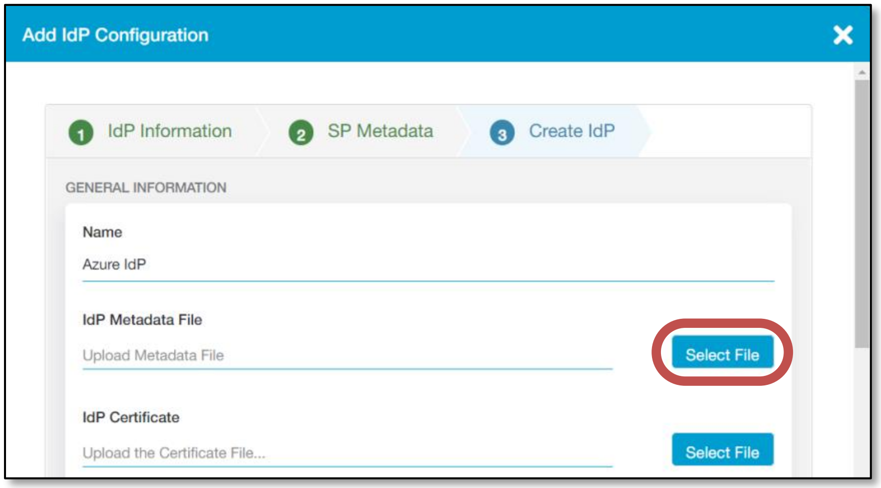


Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure IdP	●		User	▶ ✕

Single Sign-On URL	ZPA (SP) SAML Request	HTTP-Redirect
	✓ Signed	✕ Disabled

Authentication Domains

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

GENERAL INFORMATION

Name: Azure IdP

IdP Metadata File: Upload Metadata File — Select File

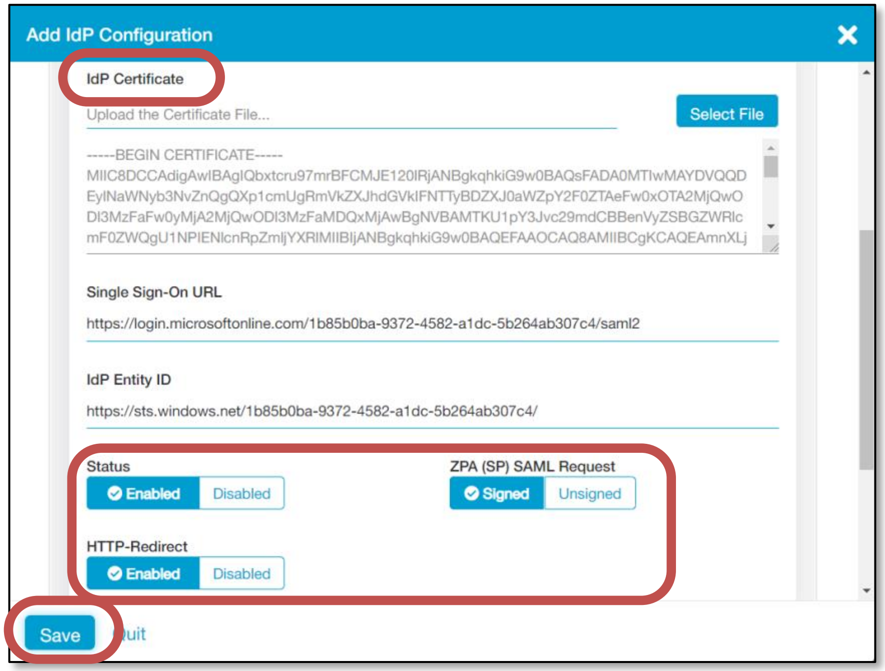
IdP Certificate: Upload the Certificate File... — Select File

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

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



Add IdP Configuration

IdP Certificate: Upload the Certificate File... — Select File

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQbxtcru97mrBFCMJE120IRjANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
EyINaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0xOTA2MjQwO
DI3MzFaFw0yMjA2MjQwODI3MzFaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlc
mF0ZWQgU1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmnXLj
```

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

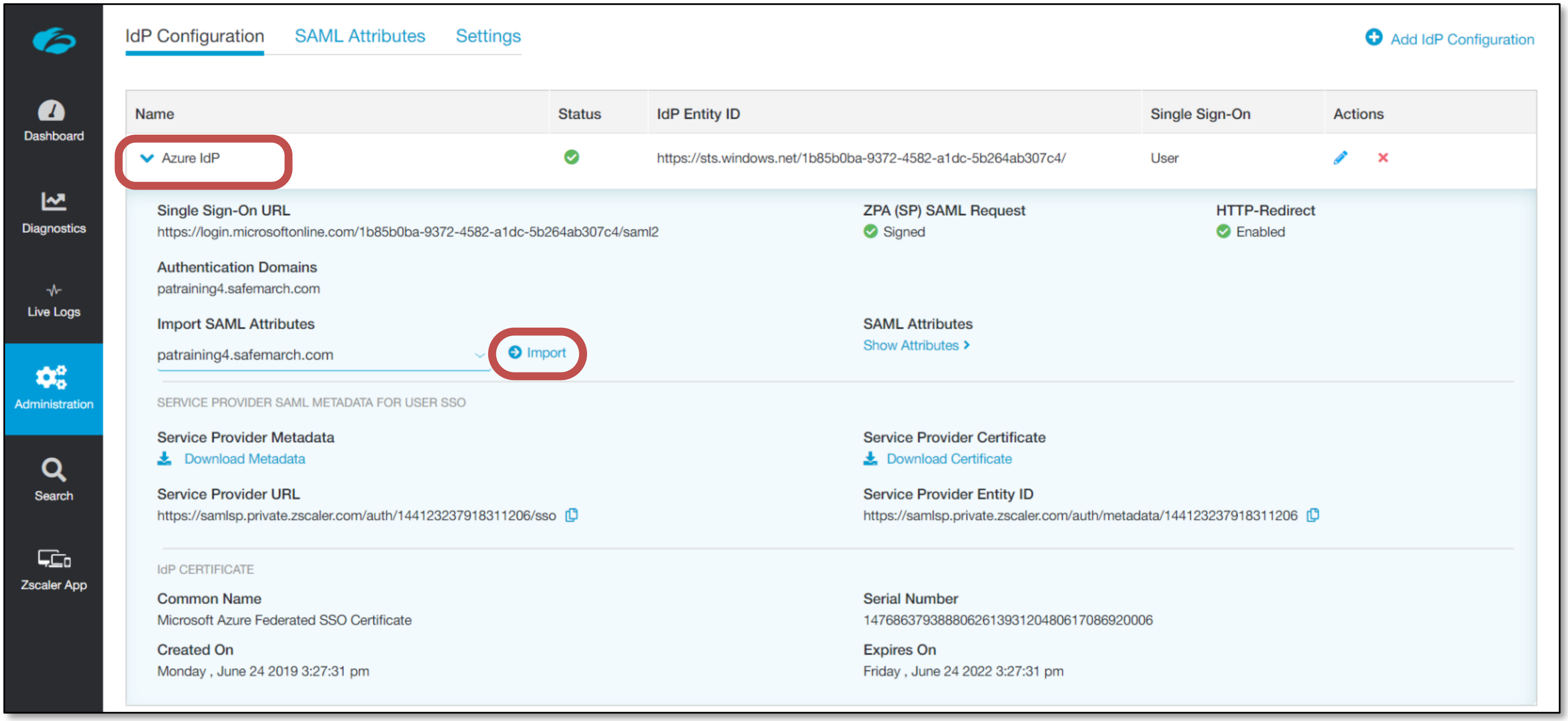
IdP Entity ID: https://sts.windows.net/1b85b0ba-9372-4582-a1dc-5b264ab307c4/

Status: [✓ Enabled] Disabled

ZPA (SP) SAML Request: [✓ Signed] Unsigned

HTTP-Redirect: [✓ Enabled] Disabled

33. Click the name of the IdP that just added, to expand to see the details. Next to the **Import SAML Attributes** item, click **Import**.



Name	Status	IdP Entity ID	Single Sign-On	Actions
Azure IdP	✓	https://sts.windows.net/1b85b0ba-9372-4582-a1dc-5b264ab307c4/	User	

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

ZPA (SP) SAML Request
✓ Signed

HTTP-Redirect
✓ Enabled

Authentication Domains
patraining4.safemarch.com

Import SAML Attributes
patraining4.safemarch.com

SAML Attributes
Show Attributes ›

SERVICE PROVIDER SAML METADATA FOR USER SSO

Service Provider Metadata
Download Metadata

Service Provider Certificate
Download Certificate

Service Provider URL
https://samlsp.private.zscaler.com/auth/144123237918311206/sso

Service Provider Entity ID
https://samlsp.private.zscaler.com/auth/metadata/144123237918311206

IdP CERTIFICATE

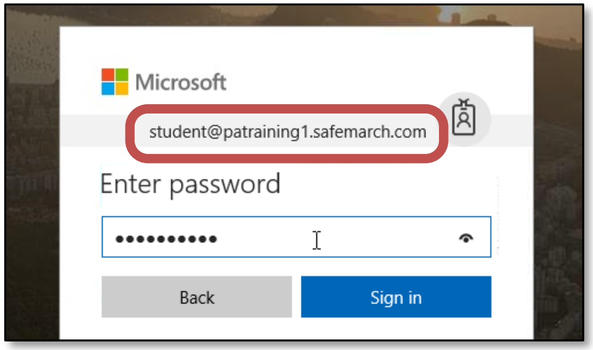
Common Name
Microsoft Azure Federated SSO Certificate

Serial Number
147686379388806261393120480617086920006

Created On
Monday , June 24 2019 3:27:31 pm

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



student@patraining1.safemarch.com

Enter password

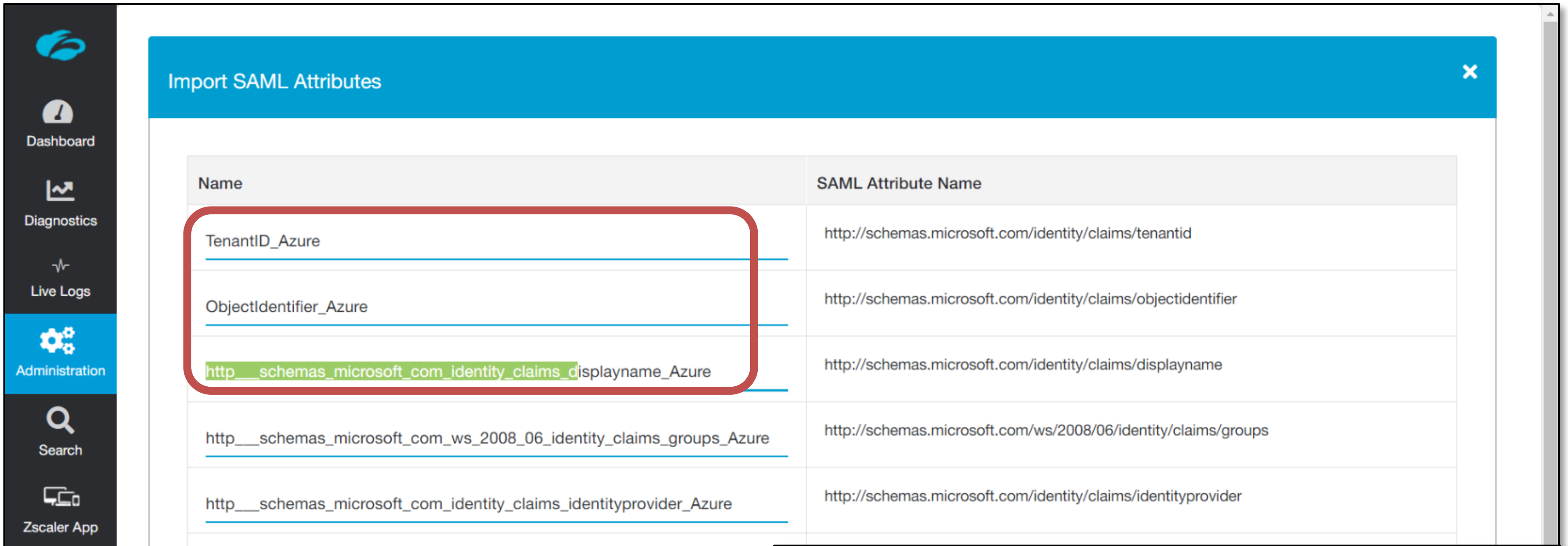
••••••••••

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. It is recommended to change the names of these attributes, to remove the Microsoft protocol and schema prefixes to make them shorter and easier to find in the Access Policy configuration interface. Click in each of the **Name** fields and enter the **Name** value that you prefer.

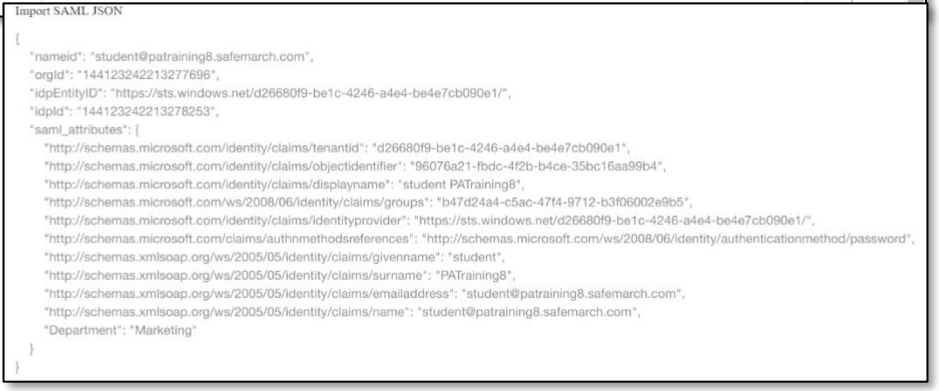
    Note: This step is optional, although using short names makes it much easier to find the attribute you need when later creating Access Policy rules.



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

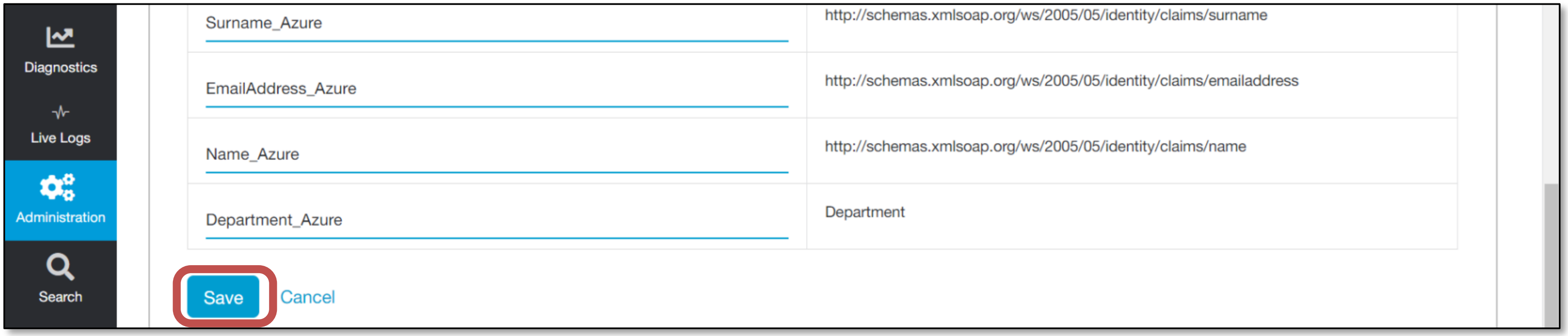
37. Also included on this page (at the bottom), is a JSON listing of the attribute values returned by AAD for the user that you authenticated as.

    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.


Import SAML JSON

```
{
  "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": "b47d24a4-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/authnmethodsreferences": "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"
  }
}
```

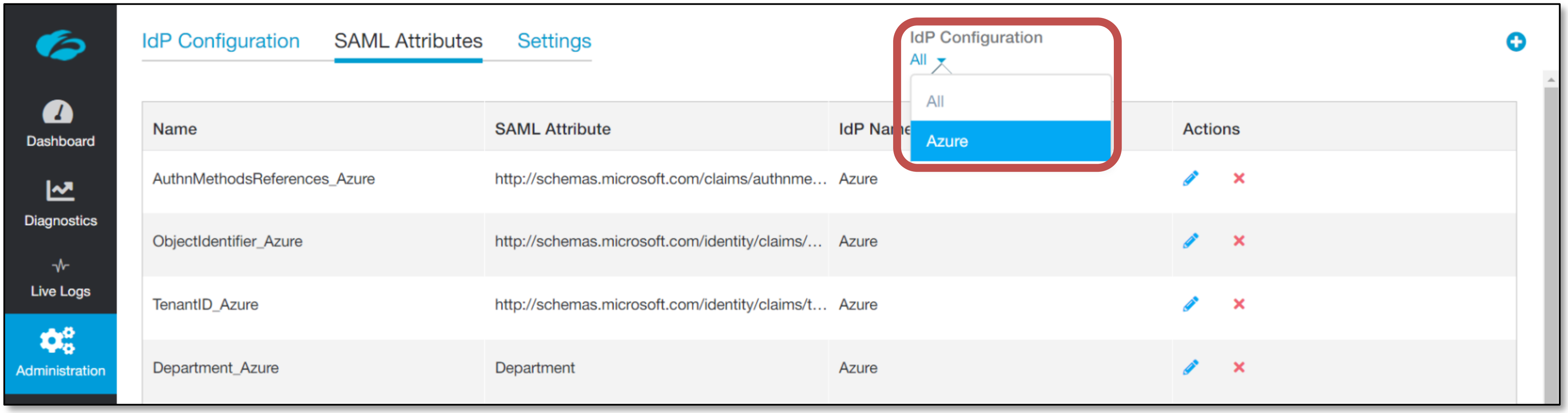
38. Once the names are set for the attributes make them available for use in Access Policy configurations by clicking **Save**.



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

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 Azure browser tab. Open a new browser tab, go to the Azure Admin Portal, and **Sign out** as the user **student@patraining[1-N].safemarch.com**.

Lab 2: Provision ZPA Infrastructure

End users will use the Zscaler App to access applications, which must be installed on their PCs. Applications are hosted on the Windows server in the Datacenter, so an on-premise Connector is required.

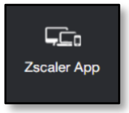
Install Zscaler App

The Zscaler App is required on the corporate client PCs. In this section, you will simply download the .EXE file directly from the Zscaler App Portal and run the executable.

Note: For this lab, you will download and run the .EXE installer for quick setup and testing. Real deployments would use options available to automate the deployment such as with an .MST file to specify installation options that is pushed from AD using a Group Policy Object (GPO).

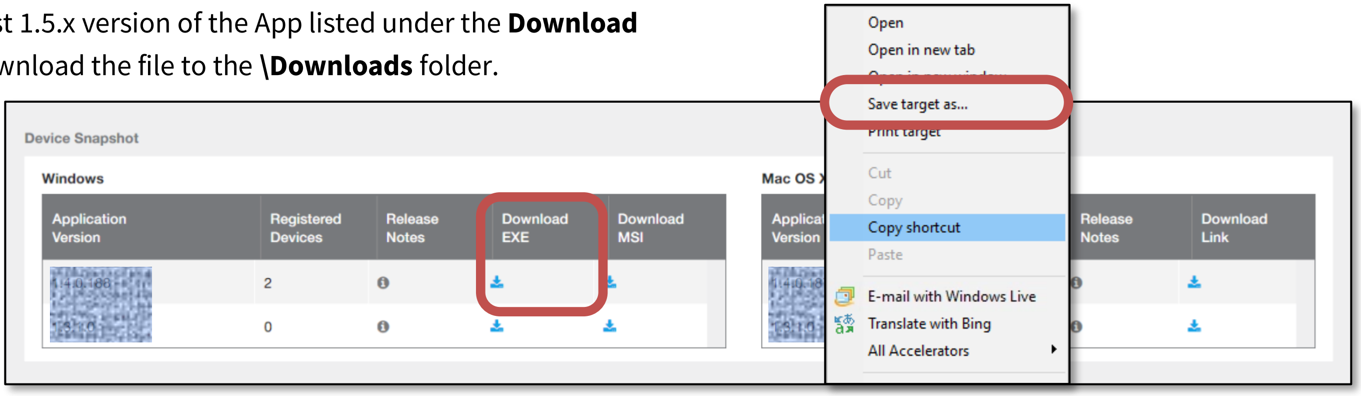
1. Go to the VM named **Corp: Client PC** and login to Windows as the user **student test**, with password **Admin-123!**

2. Launch a browser and login to the ZPA Admin Portal (https://admin.private.zscaler.com). Login as the **admin** user, then click the **Zscaler App** icon in the left-hand navigation menu to open the Zscaler App Portal in a new browser tab.



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 1.5.x version of the App listed under the **Download EXE** column. Download the file to the **\Downloads** folder.



Device Snapshot

Windows

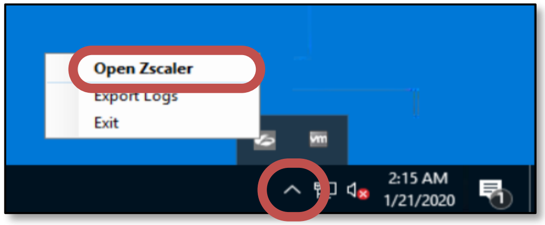
Application Version	Registered Devices	Release Notes	Download EXE	Download MSI
[redacted]	2	ⓘ	⬇	⬇
[redacted]	0	ⓘ	⬇	⬇

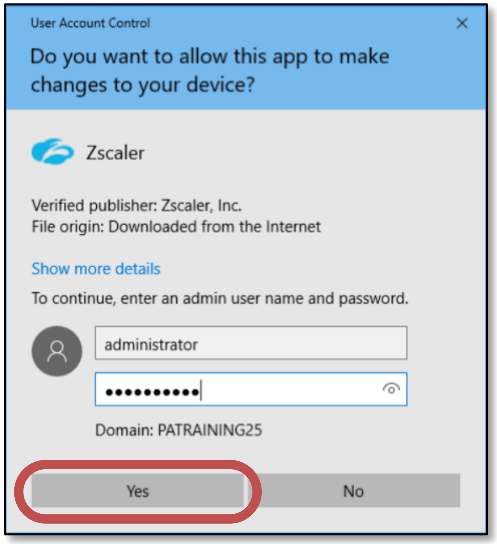
Mac OS X

Application Version	Release Notes	Download Link
[redacted]	ⓘ	⬇
[redacted]	ⓘ	⬇

5. In Windows **File Explorer**, open the **\Downloads** folder and run the installer file.

6. Authenticate as **Administrator** with password **Admin-123!** to allow the app installer to make changes and follow the prompts to install the App.
7. Close the **File Explorer** windows and the **browser**.
8. If necessary, from the Windows Status Bar, click to **Show hidden icons**, click on the **Zscaler App**, then click **Open Zscaler**.
9. When the Zscaler App UI opens, it should be immediately redirected to Azure to authenticate. Login with the username **student@patraining[1-N].safemarch.com** and password **Admin-123!**
10. When Azure prompts to stay logged in, click **No**.




User Account Control

Do you want to allow this app to make changes to your device?

Zscaler

Verified publisher: Zscaler, Inc.
File origin: Downloaded from the Internet

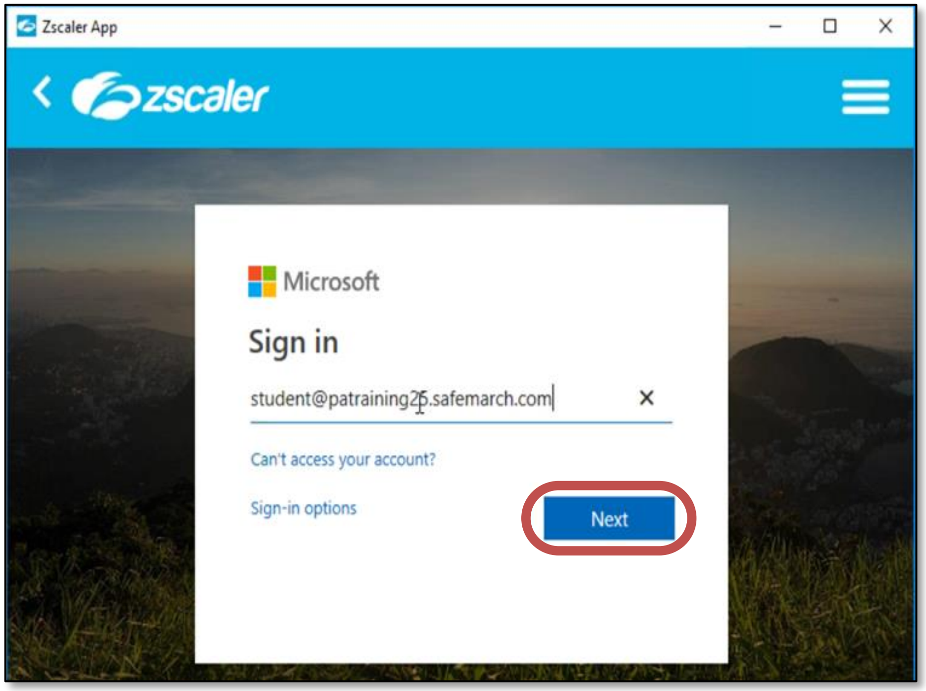
Show more details

To continue, enter an admin user name and password.

administrator

••••••••••

Domain: PATRAINING25


Zscaler App

Microsoft

Sign in

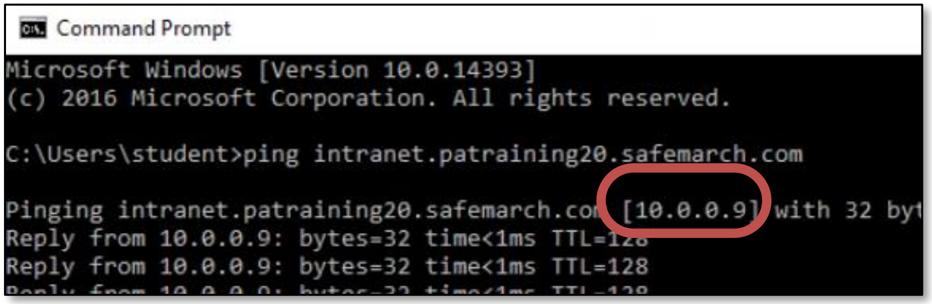
student@patraining25.safemarch.com

Can't access your account?

Sign-in options

11. Open the Zscaler App **Private Access** page. Confirm that **Service Status** indicates **ON**, that **Authentication Status** indicates **Authenticated**, and that the **Username** is correct.

12. Open a **Command** prompt and use ping to resolve the IP for the FQDN **intranet.patraining[1-N].safemarch.com**. Verify that the name resolves to an IP on the Corporate Data Center network (10.0.0.0/24).

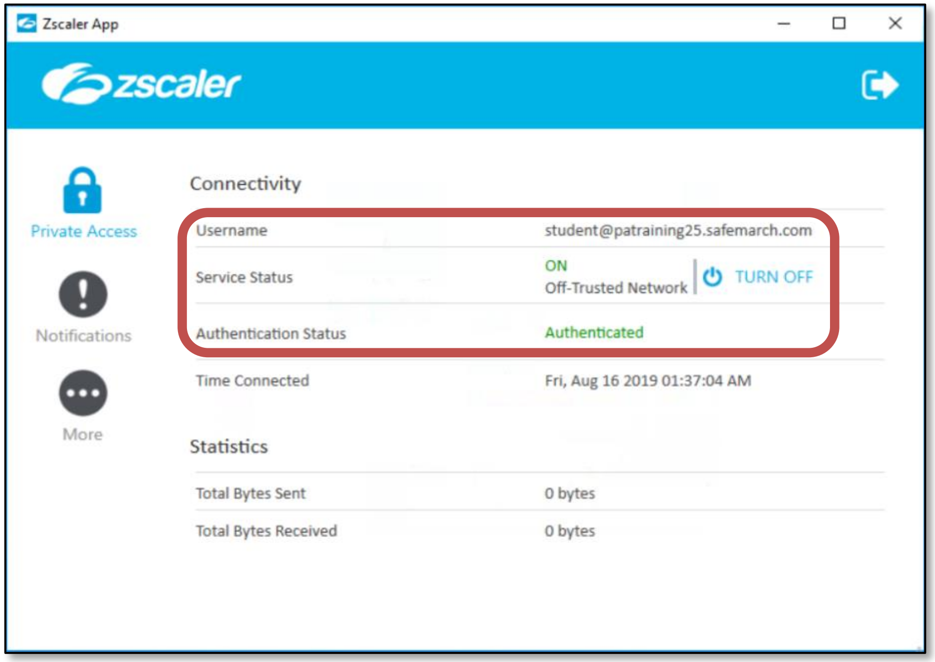


Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\student>ping intranet.patraining20.safemarch.com

Pinging intranet.patraining20.safemarch.com [10.0.0.9] with 32 byt
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128
```



Zscaler App

Connectivity

Username: student@patraining25.safemarch.com

Service Status: ON
Off-Trusted Network | TURN OFF

Authentication Status: Authenticated

Time Connected: Fri, Aug 16 2019 01:37:04 AM

Statistics

Total Bytes Sent: 0 bytes

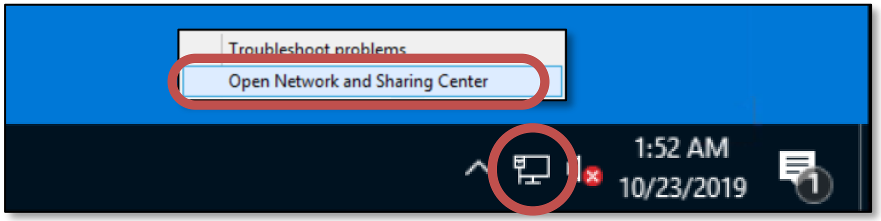
Total Bytes Received: 0 bytes

***Note**:* In the lab the Corp: Client PC initially has a NIC connected to the Corporate Data Center. This NIC will be disabled in the next step to ensure it is not able to reach the private applications in the Corporate Data Center until ZPA is configured.

Switch the Client PC to the Remote Network

Disconnect the client PC from the corporate network to use it to test from a remote network.

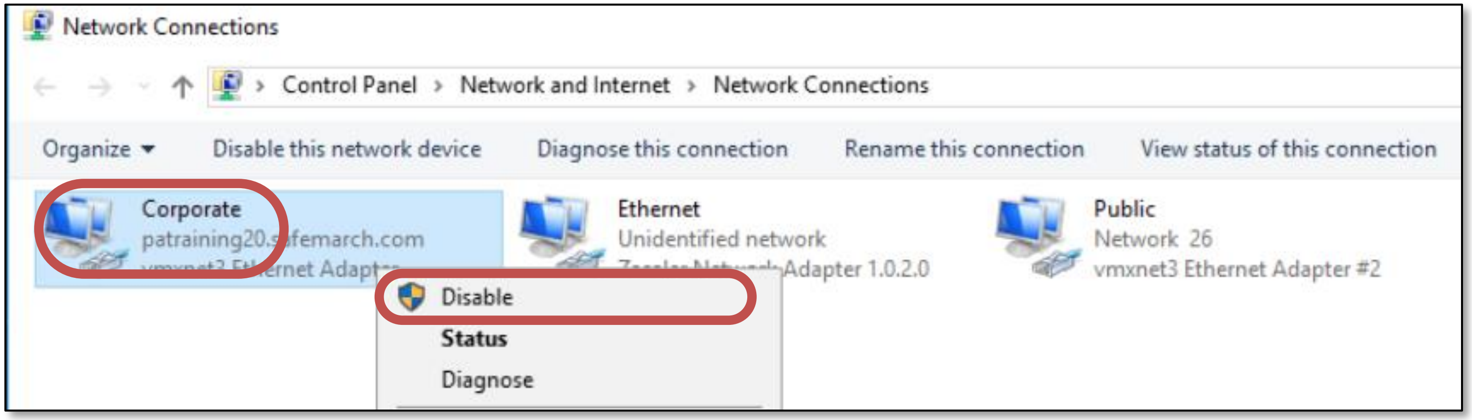
13. On the **Corp: Client PC**, from the **Windows Status Bar**, in the lower right corner, right-click on the network interface icon and click **Open Network and Sharing Center**.



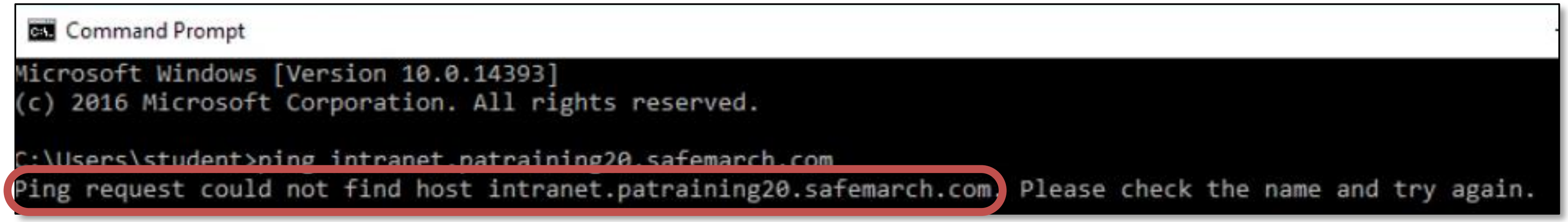
14. In the left-hand navigation menu, click **Change adapter settings**.

15. Right-click the interface named **Corporate** and select **Disable**; enter the administrator credentials when prompted (**Administrator** / **Admin-123!**).

    Note: This PC is now only connected to the Public network, which simulates being off the corporate network, and at some other location such as a coffee shop, customer, partner, or home network.


Network Connections
Control Panel › Network and Internet › Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Corporate
patraining20.safemarch.com
vmxnet3 Ethernet Adapter
Ethernet
Unidentified network
Zscaler Network Adapter 1.0.2.0
Public
Network 26
vmxnet3 Ethernet Adapter #2
Disable
Status
Diagnose

16. Open a **Command** prompt and verify that the FQDN **intranet.patraining[1-N].safemarch.com**. is no longer reachable.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\student>ping intranet.patraining20.safemarch.com
Ping request could not find host intranet.patraining20.safemarch.com. Please check the name and try again.
```

***Note**:* Even though the user is enrolled in the ZPA service through the Zscaler App, application access will not be available until the connector is deployed and the application segments and access policies are configured.

Provision a Connector

A CentOS-based 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 in the ZPA Admin Portal.

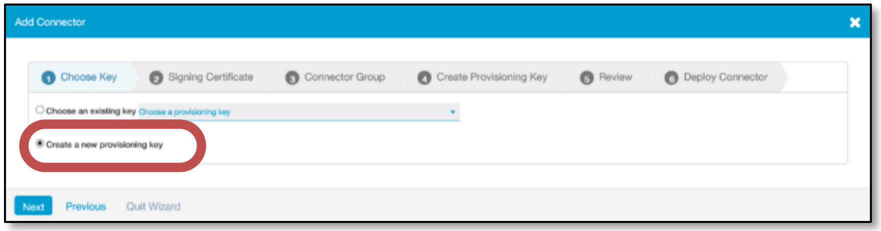
17. On the VM labelled **Corp: Win Svr 2016**, open a browser and go to the URL **http://admin.private.zscaler.com**.

18. Log into the **ZPA Admin Portal** using the credentials assigned to you (**admin@patraining[1-N].safemarch.com**).

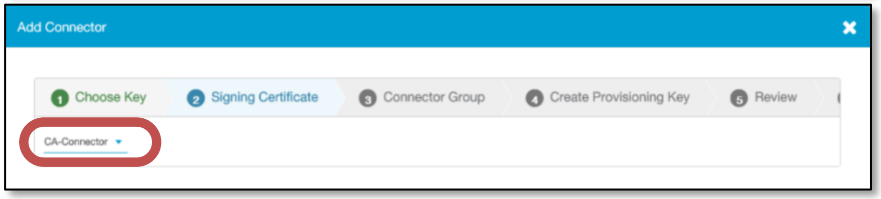
    Note: For this lab, you must access the ZPA Admin Portal in a browser on the Windows 2016 server, as you need to download a provisioning key to install on the Connector VM.

19. From the **Administration** menu under **CONNECTOR MANAGEMENT**, select **Connectors**.

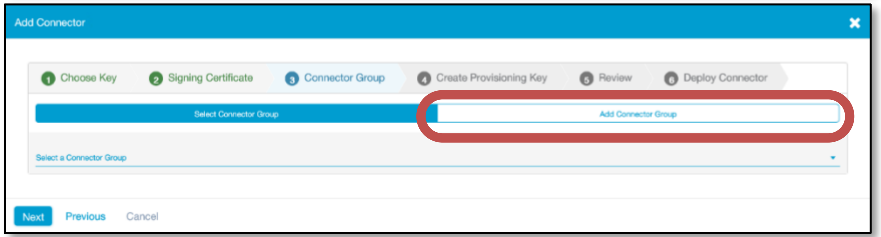
20. Click the ⊕ **Add Connector** icon at top right to add a new Connector and step through the wizard as follows:
    a. Select **Create a new provisioning key** and click **Next**.
    b. Click **Choose a certificate** and select the certificate named **Connector**, then click **Next**;
    c. Click **Add Connector Group**;
    d. Name the group **OnPrem**, add a description if you wish, **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 Connector settings and click **Save**;



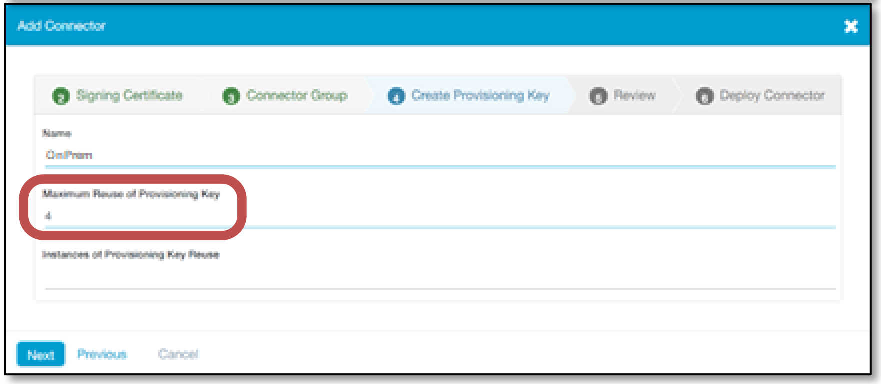
○ Choose an existing key Choose a provisioning key
● Create a new provisioning key



CA-Connector



Select a Connector Group



Name
OnPrem

Maximum Reuse of Provisioning Key
4

Instances of Provisioning Key Reuse

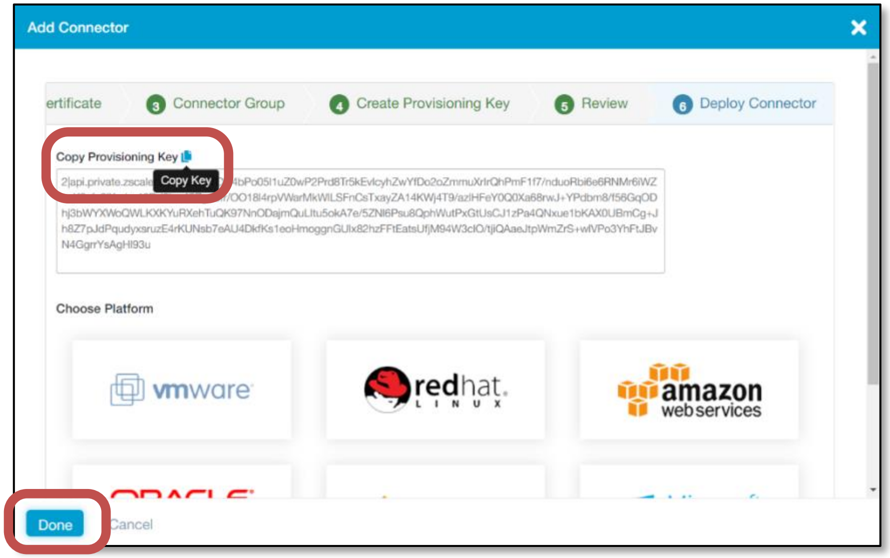
g. By the **Copy Provisioning Key** text, click the **Copy ID** icon (it should show the caption **Copied**);

   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**.



Copy Provisioning Key

```
2|api.private.zscale                    4bPo05l1uZ0wP2Prd8Tr5kEvlcyhZwYfDo2oZmmuXrIrQhPmF1f7/nduoRbi6e6RNMr6iWZ
                                       /OO18l4rpVWarMkWILSFnCsTxayZA14KWj4T9/azlHFeY0Q0Xa68rwJ+YPdbm8/f56GqOD
hj3bWYXWoQWLKXKYuRXehTuQK97NnODajmQuLltu5okA7e/5ZNl6Psu8QphWutPxGtUsCJ1zPa4QNxue1bKAX0UBmCg+J
h8Z7pJdPqudyxsruzE4rKUNsb7eAU4DkfKs1eoHmoggnGUlx82hzFFtEatsUfjM94W3clO/tjiQAaeJtpWmZrS+wlVPo3YhFtJBv
N4GgrrYsAgHl93u
```

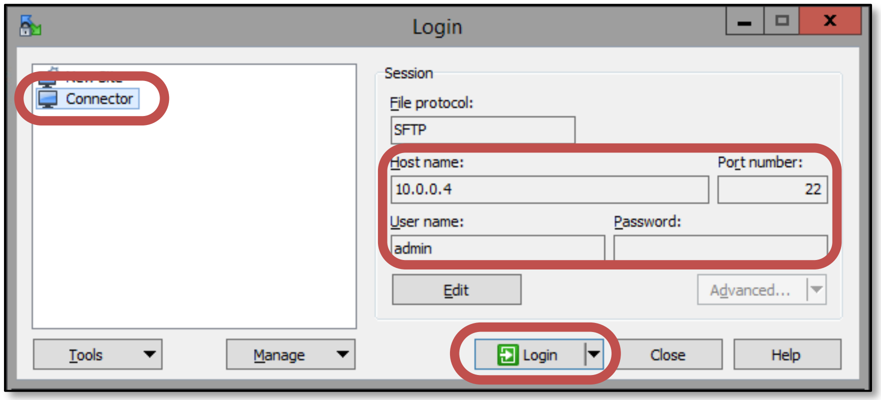
21. Open Windows **File Explorer** and navigate to the provisioning key that you just saved. If necessary, from the **View** menu enable the **file name extensions** option. Then rename the file to remove the extension, so the name is just **provision_key**. Confirm the change to the file extension.
22. 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.
23. Click **Connector Provisioning Keys** to confirm that a key has been created to support a maximum of 4 Connecters.

Activate the Connector

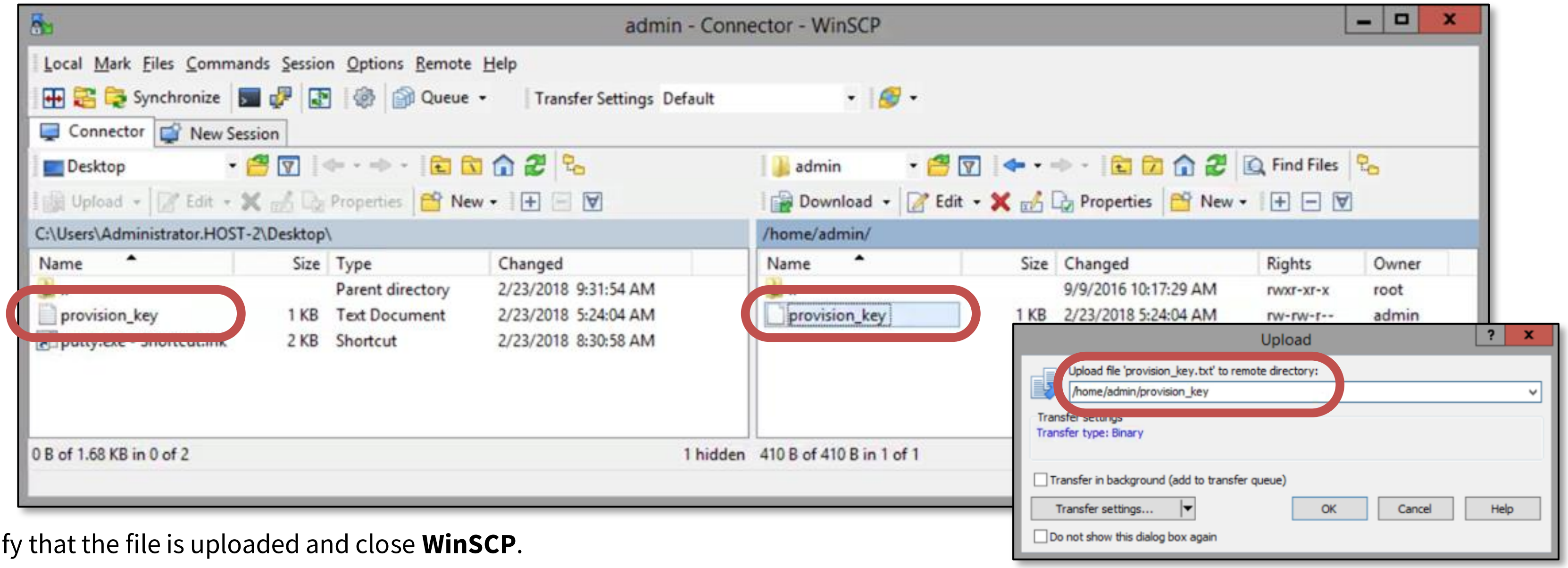
A prebuilt Connector VM has been provided, with basic networking, DNS, and NTP configured. You need to activate the Connector software on this VM and provide the provisioning key value that you saved to the Windows server. You must first enable the SSH Daemon on the Connector to allow the transfer of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

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

27. On the VM labelled **Corp: Win Svr 2016**, copy the provisioning key file to the Connecter:
    a. Start **WinSCP** using the icon on the desktop or in the taskbar:
    b. Load the saved session named **Connector** (IP address **10.0.0.4**, Port **22**) and click **Login**;
    c. Login to the Connector using the default user password (**zscaler**), accept the certificate if necessary;
    d. In the left-hand panel of WinSCP (the local Windows server), navigate to the **Desktop** folder and select the file **provision_key**;
    e. Right-click on the file and select **Upload**;
    f. Specify the path on the Connector as **/home/admin/provision_key** and click **OK**;



Session
File protocol: SFTP
Host name: 10.0.0.4
Port number: 22
User name: admin
Password:



Transfer Settings Default

C:\Users\Administrator.HOST-2\Desktop\

Name	Size	Type	Changed
..		Parent directory	2/23/2018 9:31:54 AM
provision_key	1 KB	Text Document	2/23/2018 5:24:04 AM
putty.exe - Shortcut.lnk	2 KB	Shortcut	2/23/2018 8:30:58 AM

0 B of 1.68 KB in 0 of 2 — 1 hidden

/home/admin/

Name	Size	Changed	Rights	Owner
..		9/9/2016 10:17:29 AM	rwxr-xr-x	root
provision_key	1 KB	2/23/2018 5:24:04 AM	rw-rw-r--	admin

410 B of 410 B in 1 of 1

Upload file 'provision_key.txt' to remote directory: /home/admin/provision_key

Transfer settings
Transfer type: Binary

□ Transfer in background (add to transfer queue)

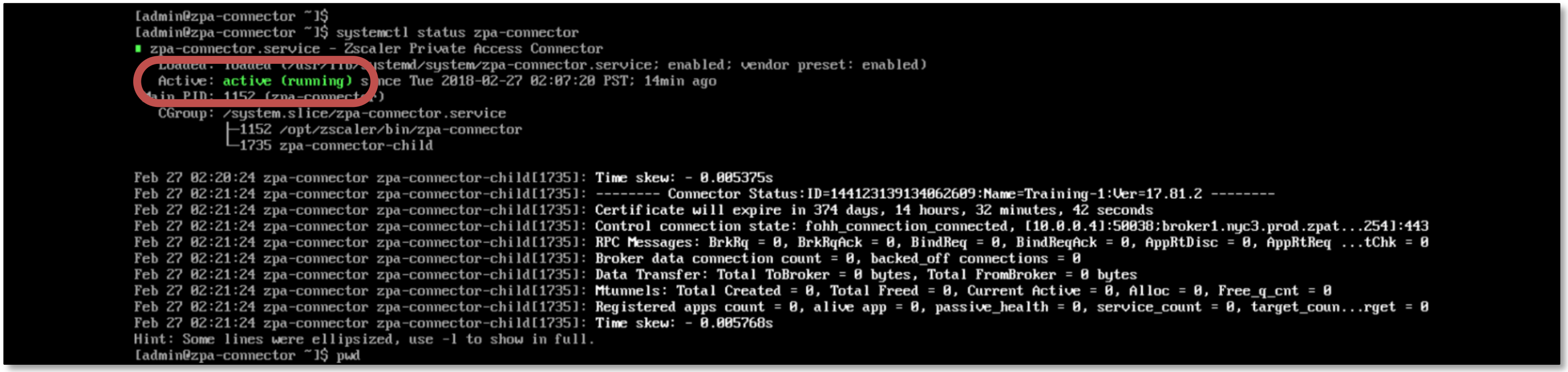
□ Do not show this dialog box again

28. Verify that the file is uploaded and close **WinSCP**.

29. Activate the Connector with the new provisioning key file:
    a. First identify the current directory with the command **`pwd`** (you should be in **`/home/admin`**);
    b. List the contents of the directory with the command **`ls`** and confirm that the file **provision_key** is there;
    c. Stop the **Connector** service with the command **`sudo systemctl stop zpa-connector`** (enter the password **zscaler** if prompted);
    d. 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!
    e. Check that the file is there using the command **`sudo ls /opt/zscaler/var/`**
    f. Now restart the **Connector** service with the command **`sudo systemctl start zpa-connector`**
    g. Wait about 30s, then check the status of the **Connector** service using the command **`sudo systemctl status zpa-connector`**
    h. Verify that it is active and has established a connection to the ZPA infrastructure.
    i. Run the command **`sudo ls /opt/zscaler/var`** again and review the contents of that folder now that the Connector has enrolled.

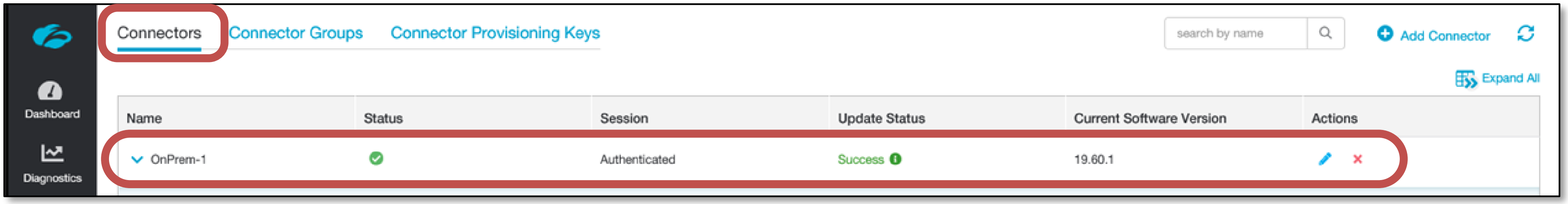
       Note: You should now see a set of key and certificate **.pem** files.



```
[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: fohh_connection_connected, [10.0.0.4]:50038;broker1.nyc3.prod.zpat...254]: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]: Mtunnels: 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: - 0.005768s
Hint: Some lines were ellipsized, use -l to show in full.
[admin@zpa-connector ~]$ pwd
```

30. 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 Connector is listed.



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

Lab 3: Add an Application

The ZPA infrastructure components are all now in place (SAML IdP, Connector, Zscaler App). It is now needed to add applications for the end users to connect to. ZPA will not give *anyone* access to *anything* unless; the 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.

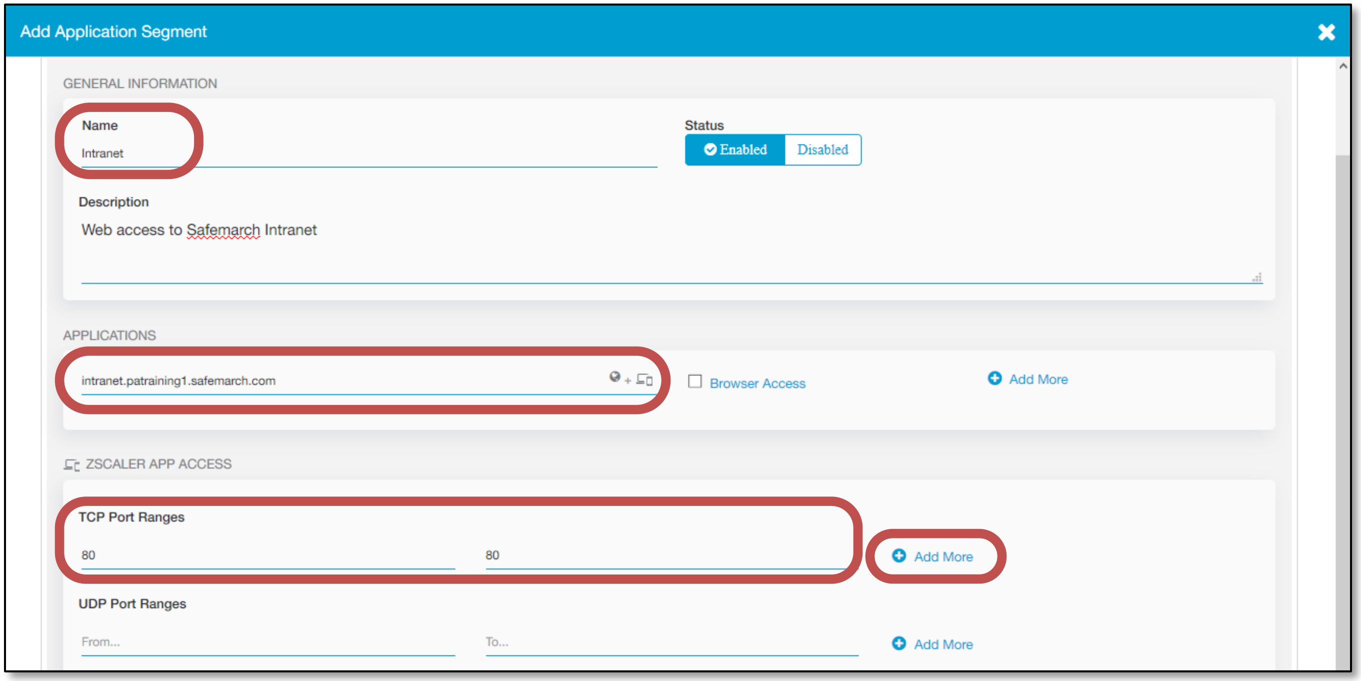
Add the Intranet Application

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**;



Add Application Segment

GENERAL INFORMATION

Name: Intranet

Status: ● Enabled | Disabled

Description: Web access to Safemarch Intranet

APPLICATIONS

intranet.patraining1.safemarch.com

□ Browser Access

ZSCALER APP ACCESS

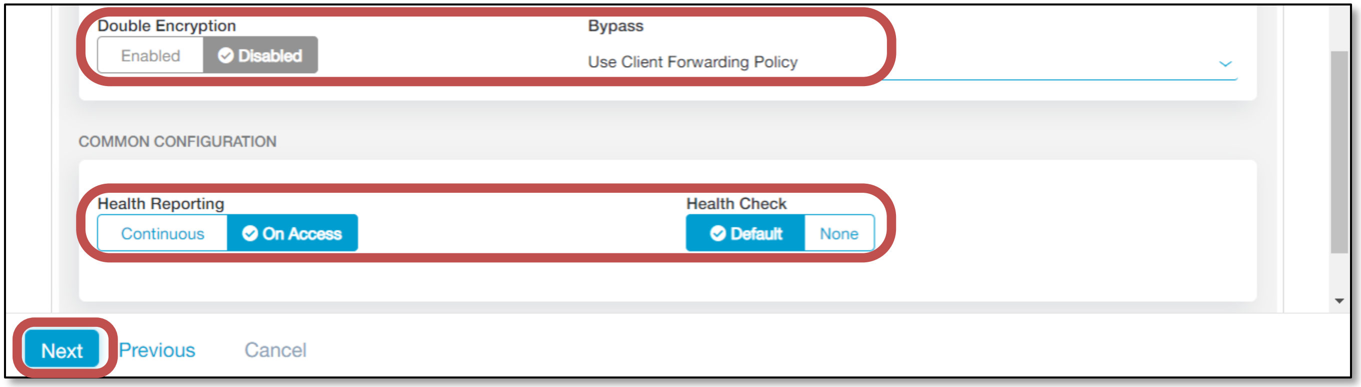
TCP Port Ranges: 80 – 80

UDP Port Ranges: From... – To...

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** and **Health Check** to **Default**;

g. Then click **Next**;



Double Encryption: Enabled / Disabled

Bypass: Use Client Forwarding Policy

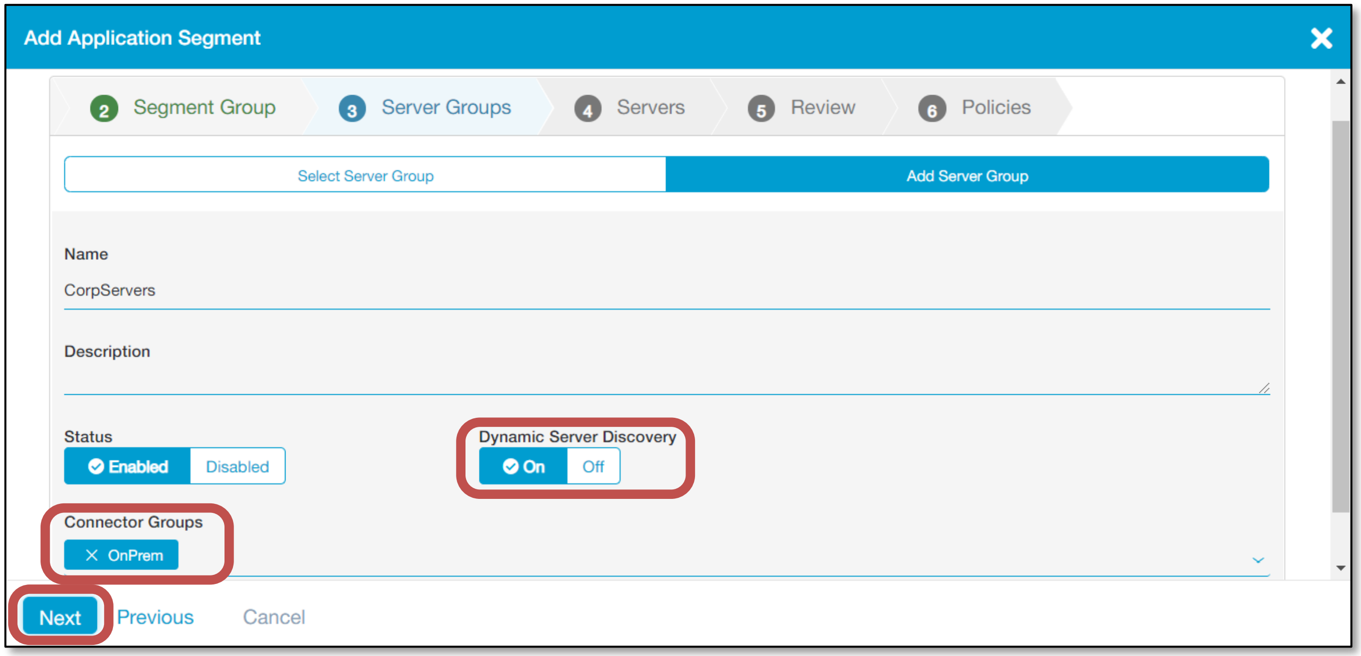
COMMON CONFIGURATION

Health Reporting: Continuous / On Access

Health Check: Default / None

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 Connector group **OnPrem** that you created earlier. Click **Done**, then click **Next**.



Add Application Segment

Name: CorpServers

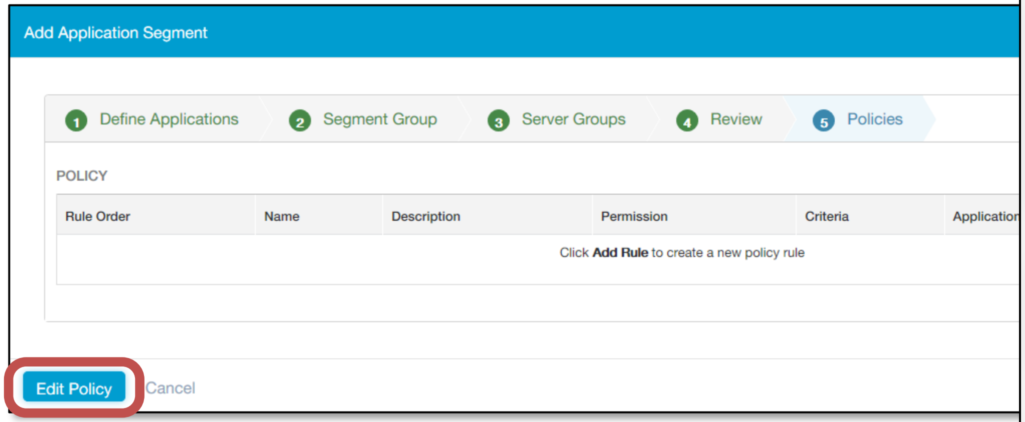
Description

Status: Enabled / Disabled

Dynamic Server Discovery: On / Off

Connector Groups: OnPrem

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



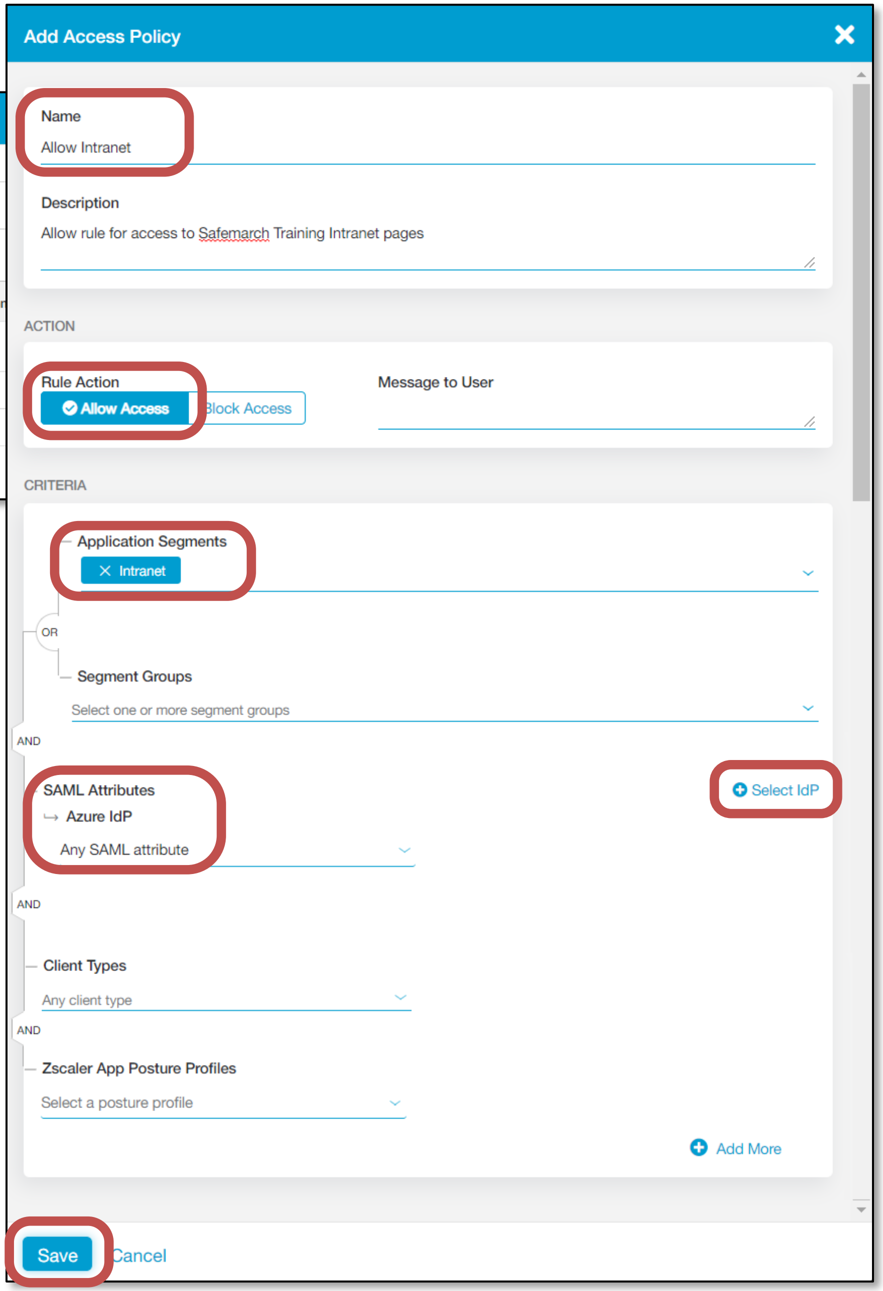
Add Application Segment

1 Define Applications — 2 Segment Group — 3 Server Groups — 4 Review — 5 Policies

POLICY

Rule Order	Name	Description	Permission	Criteria	Application
Click **Add Rule** to create a new policy rule					

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 1, 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**.



Add Access Policy

Name: Allow Intranet

Description: Allow rule for access to Safemarch Training Intranet pages

ACTION

Rule Action: Allow Access | Block Access

Message to User:

CRITERIA

Application Segments: Intranet

OR

Segment Groups: Select one or more segment groups

AND

SAML Attributes
→ Azure IdP
Any SAML attribute

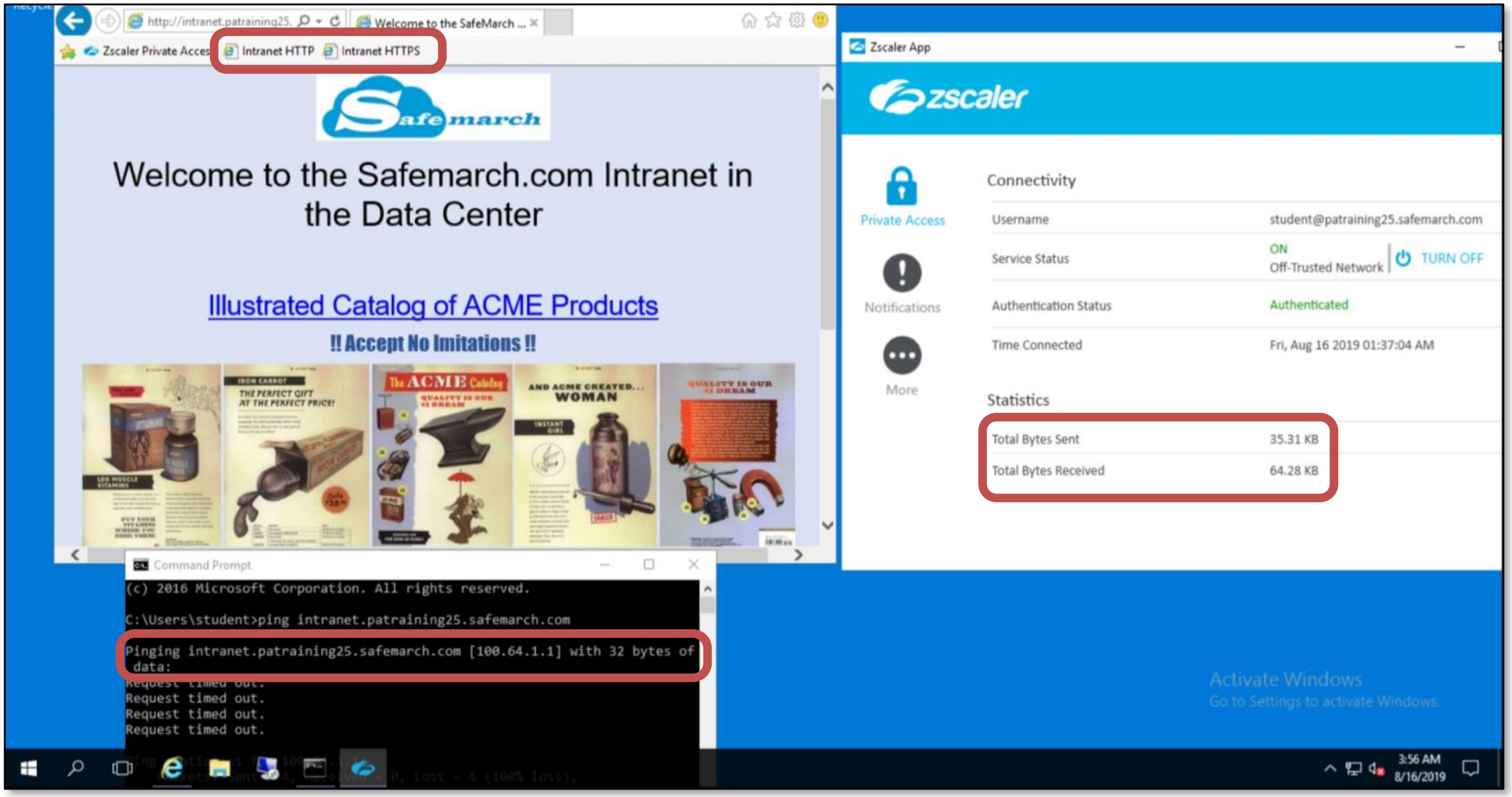
AND

Client Types: Any client type

AND

Zscaler App Posture Profiles: Select a posture profile

8. Login to the VM labelled **Corp: Client PC**, open a web browser in a window and open the **Zscaler App** 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).
    ***Note**:* Since the application segment is only configured for TCP ports 80 and 443, ping (ICMP) will not reach the intranet server and will show a timeout.
12. In the browser, refresh the page and view the **Total Bytes Sent** and **Total Bytes Received** counters in the Zscaler App and confirm that they are now incrementing.


http://intranet.patraining25.
Welcome to the SafeMarch ...
Zscaler Private Acces
Intranet HTTP
Intranet HTTPS
Safemarch
Welcome to the Safemarch.com Intranet in the Data Center
Illustrated Catalog of ACME Products
!! Accept No Imitations !!
Zscaler App
zscaler
Private Access
Notifications
More
Activate Windows
Go to Settings to activate Windows.
3:56 AM
8/16/2019

Connectivity

Username	student@patraining25.safemarch.com
Service Status	ON Off-Trusted Network ⏻ TURN OFF
Authentication Status	Authenticated
Time Connected	Fri, Aug 16 2019 01:37:04 AM

Statistics

Total Bytes Sent	35.31 KB
Total Bytes Received	64.28 KB

Command Prompt

```
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\student>ping intranet.patraining25.safemarch.com

Pinging intranet.patraining25.safemarch.com [100.64.1.1] with 32 bytes of
 data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.64.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Lab 4: Discover Applications

The ZPA service is now active and end users have 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

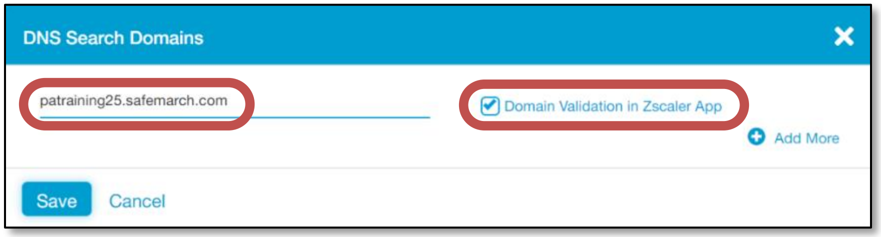
In this section, you will add an Application Segment in the ZPA Admin Portal, configured to allow application discovery. You will also add a DNS Search Domain to allow application discovery using short names (rather than FQDNs).

1. Open a browser and login to the **ZPA Admin Portal**. From the **Administration** menu under **APPLICATION MANAGEMENT**, go to the **Application Segments** page.

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

2. Click the DNS **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 using a short name only. The **Domain Validation** option gives Zscaler App first go at resolving these derived FQDNs (and is a recommended best practice).



DNS Search Domains

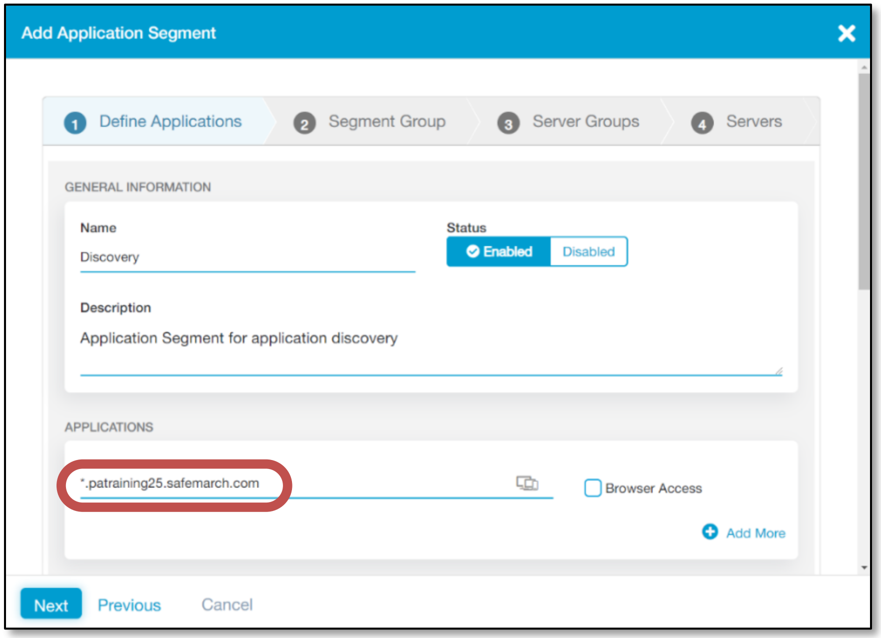
patraining25.safemarch.com

☑ Domain Validation in Zscaler App

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**;



Add Application Segment

1 Define Applications 2 Segment Group 3 Server Groups 4 Servers

GENERAL INFORMATION

Name: Discovery

Status: [✓ Enabled] Disabled

Description: Application Segment for application discovery

APPLICATIONS

*.patraining25.safemarch.com

□ Browser Access

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 **52**, click **Add More** and add the range **54** to **65535**;

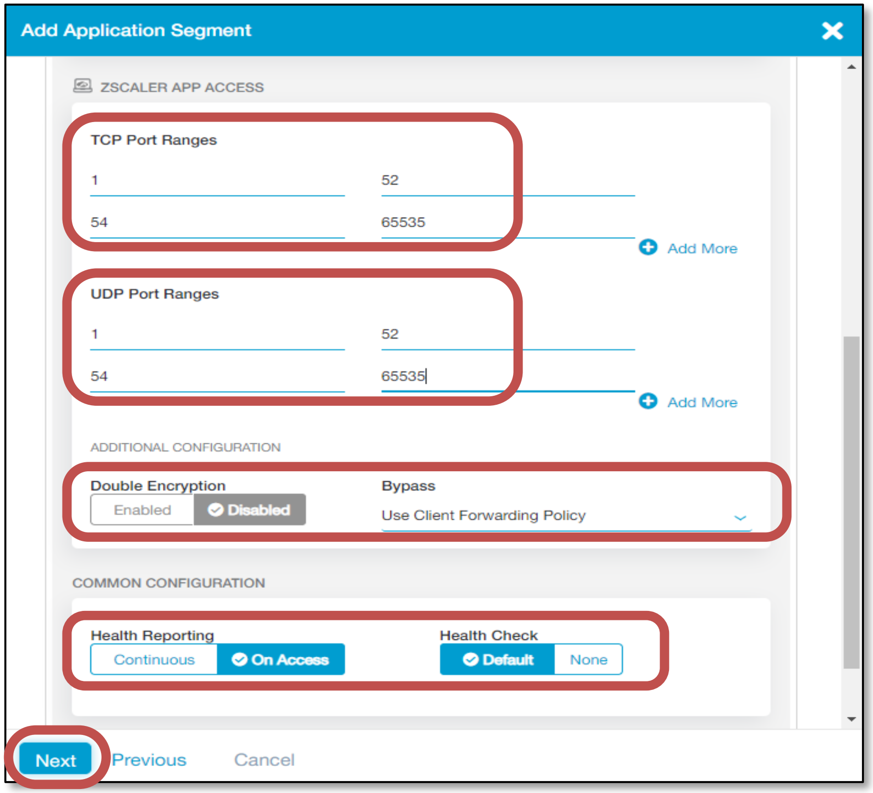
d. Add a **UDP Port Range** of **1** to **52**, click **Add More** and add the range **54** to **65535**;

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** and **Health Check** to **Default**;

g. Then click **Next**;



Add Application Segment

ZSCALER APP ACCESS

TCP Port Ranges

1	52
54	65535

UDP Port Ranges

1	52
54	65535

ADDITIONAL CONFIGURATION

Double Encryption: Enabled [✓ Disabled]

Bypass: Use Client Forwarding Policy

COMMON CONFIGURATION

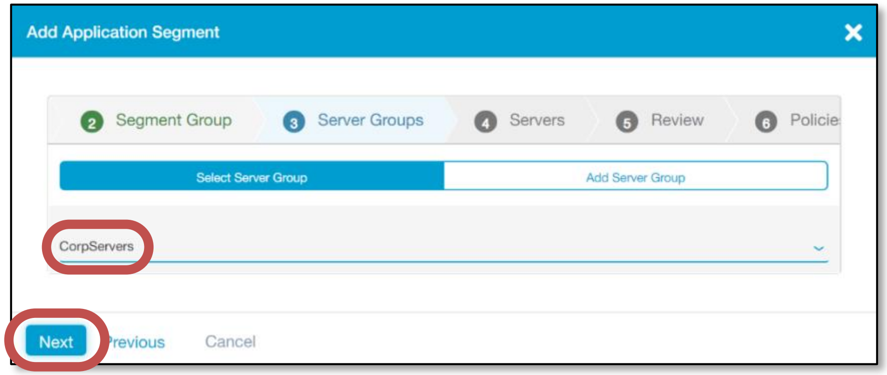
Health Reporting: Continuous [✓ On Access]

Health Check: [✓ Default] None

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 **CorpServers** group that you added previously, click **Done** then **Next**.

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

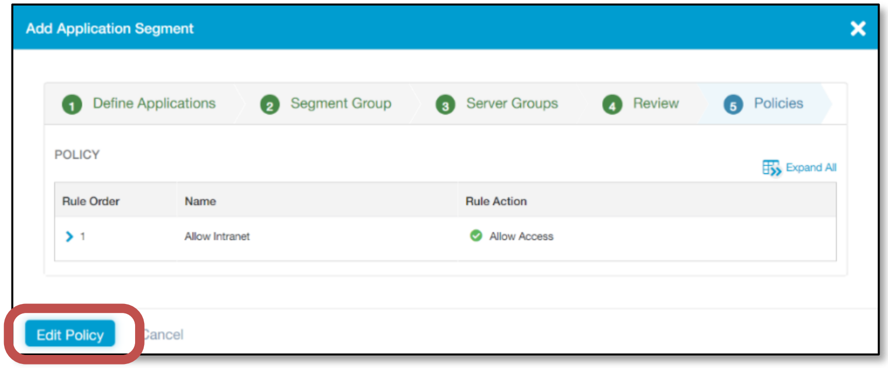


Add Application Segment

CorpServers

Lab 4: Discover Corporate Applications

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



9. 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**;

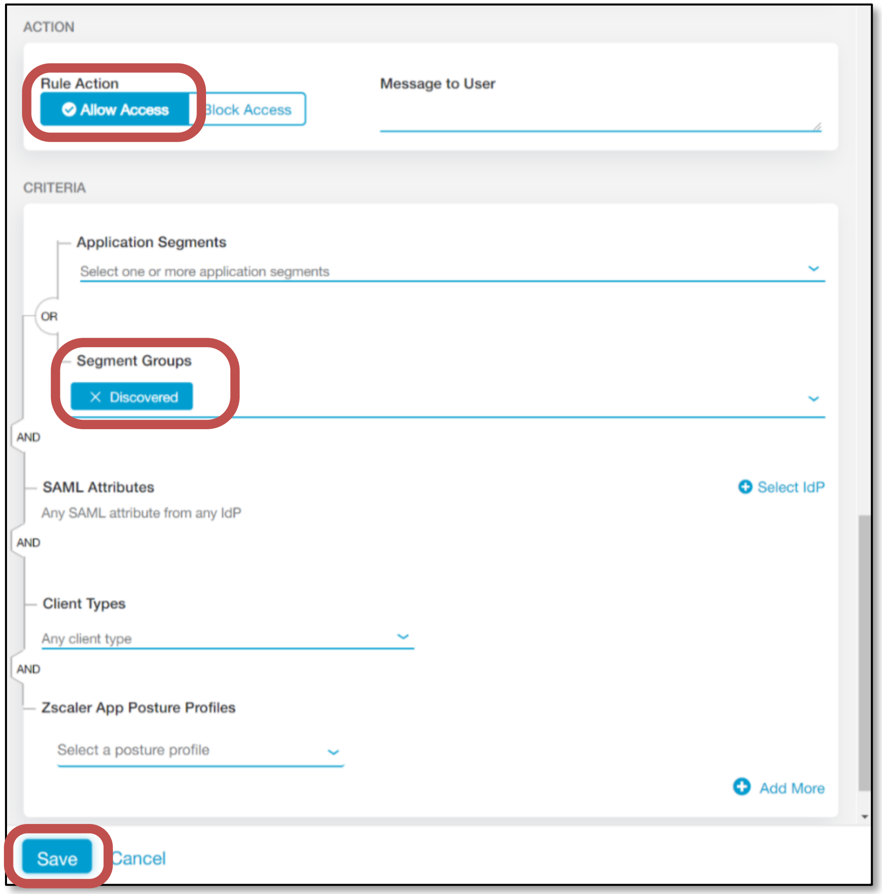
   e. Leave the **SAML Attribute** option set to **Any SAML attribute from any IdP**;

   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**.



10. 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.

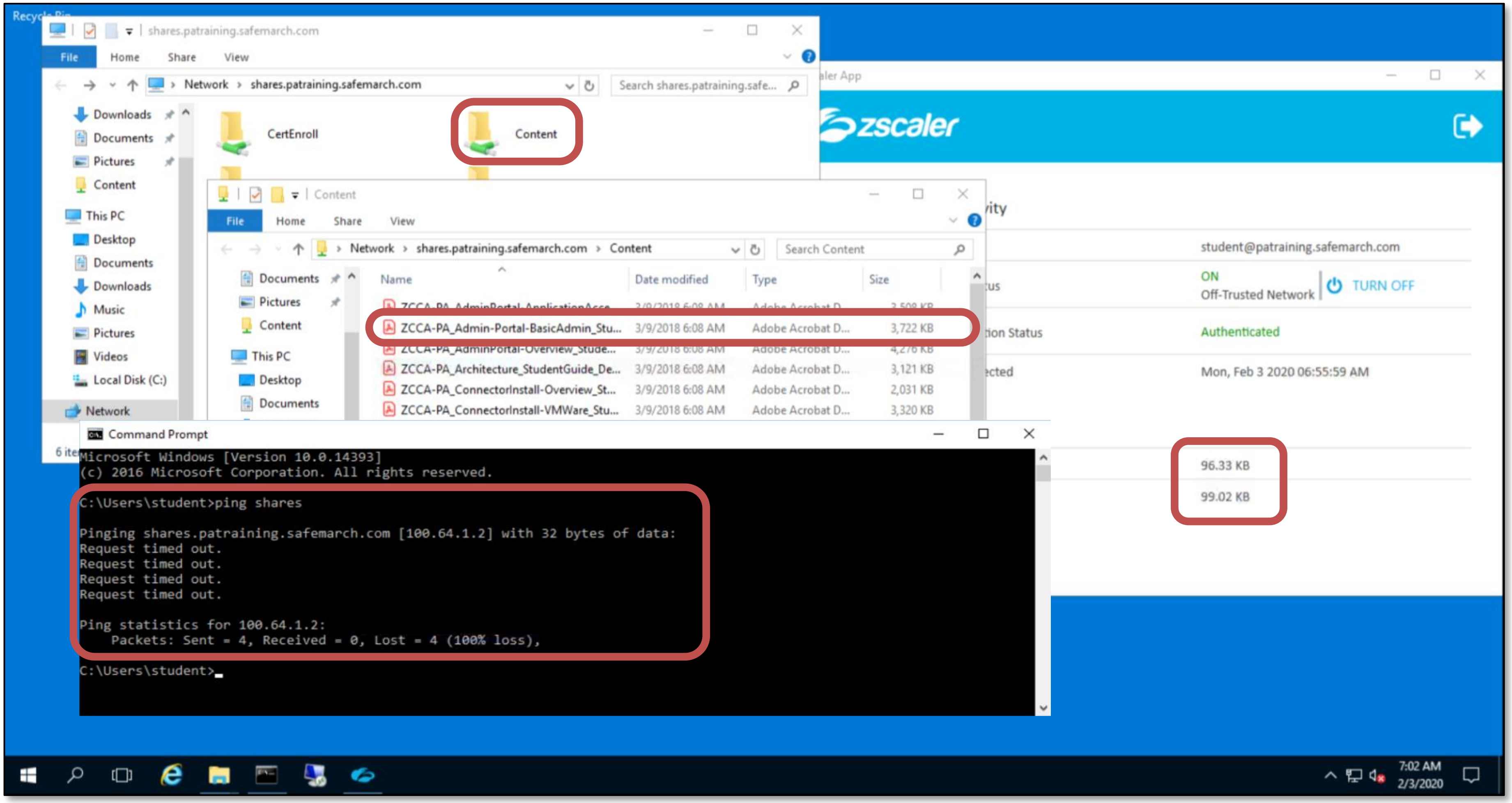
Discover Applications

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

11. 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, verify that the Zscaler App traffic counters increment.

    Note: You do not need to specify the FQDN for the application, as you added the **DNS Search Domain** configuration earlier.

12. 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.



Network › shares.patraining.safemarch.com › Content

Name	Date modified	Type	Size
ZCCA-PA_AdminPortal-ApplicationAcce...	3/9/2018 6:08 AM	Adobe Acrobat D...	3,508 KB
ZCCA-PA_Admin-Portal-BasicAdmin_Stu...	3/9/2018 6:08 AM	Adobe Acrobat D...	3,722 KB
ZCCA-PA_AdminPortal-Overview_Stude...	3/9/2018 6:08 AM	Adobe Acrobat D...	4,276 KB
ZCCA-PA_Architecture_StudentGuide_De...	3/9/2018 6:08 AM	Adobe Acrobat D...	3,121 KB
ZCCA-PA_ConnectorInstall-Overview_St...	3/9/2018 6:08 AM	Adobe Acrobat D...	2,031 KB
ZCCA-PA_ConnectorInstall-VMWare_Stu...	3/9/2018 6:08 AM	Adobe Acrobat D...	3,320 KB

Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\student>ping shares

Pinging shares.patraining.safemarch.com [100.64.1.2] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.64.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\student>_
```

zscaler

student@patraining.safemarch.com

us: ON Off-Trusted Network | TURN OFF

ion Status: Authenticated

ected: Mon, Feb 3 2020 06:55:59 AM

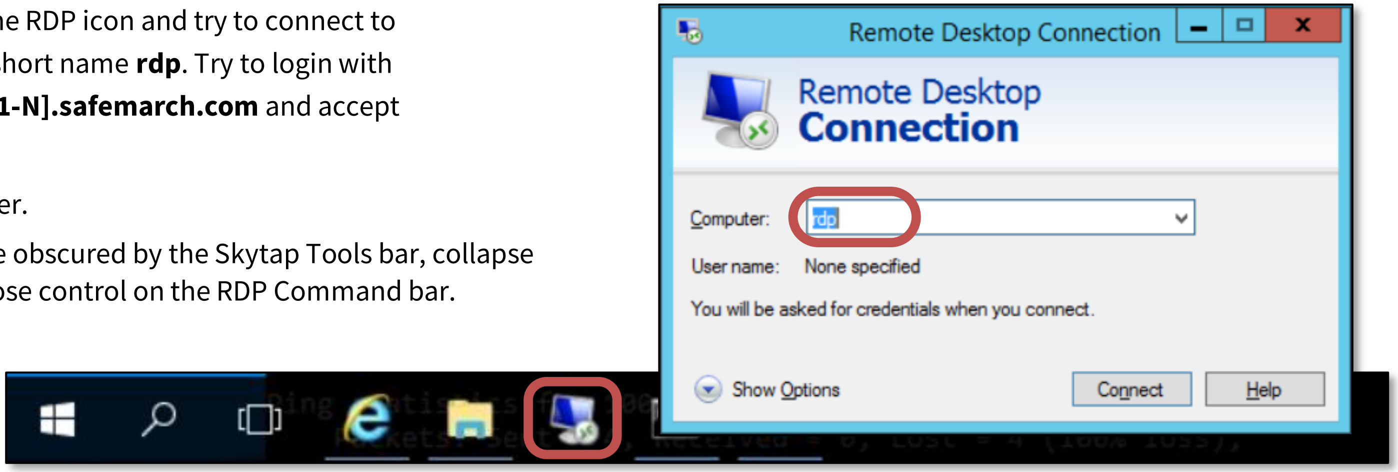
96.33 KB

99.02 KB

13. 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.

14. 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.



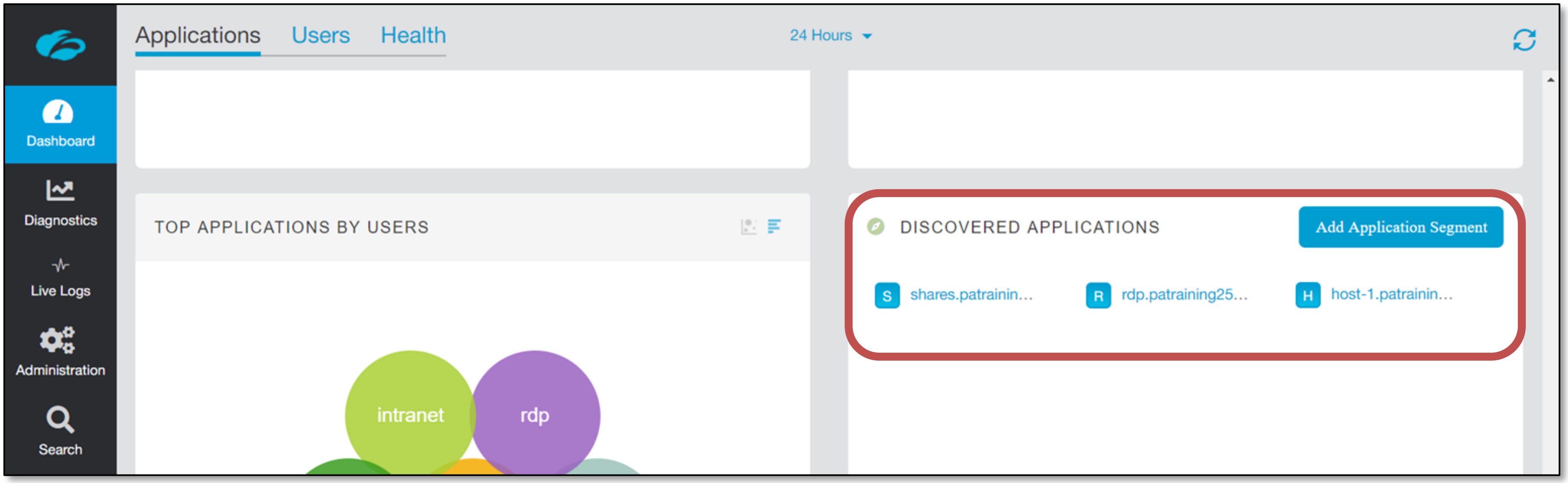
Remote Desktop Connection

Computer: rdp

User name: None specified

You will be asked for credentials when you connect.

15. 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.



16. 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.