Zscaler Certified Cloud Professional – Internet Access (ZCCP-IA)

Hands-on Lab Guide

ZCCP-IA Lab Guide

July 2020, Rev. 6.0k

Contents

About the ZCCP-IA Hands-on Labs

Welcome to the Zscaler Certified Cloud Professional (ZCCP-IA) Hands-on Lab. During this portion of the ZCCP-IA course you will practice the skills you learned during the interactive demo's using the Zscaler remote lab. The pre-requisite for the hands-on portion of the ZCCP-IA course is the completion of the ZCCP-IA eLearning modules and passing grade of each quiz in ZCCP-IA. During this course, you will complete a number of labs designed to increase proficiency in configuring the Zscaler Internet Access solution.

Connecting to the Virtual Lab

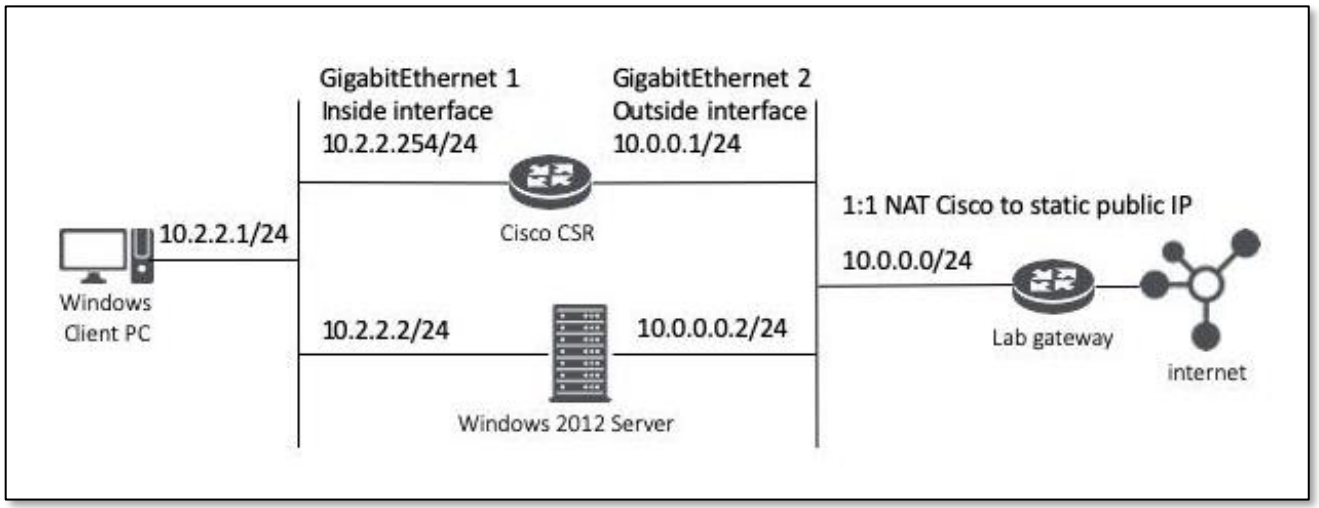
The Zscaler Certified Cloud Professional (ZCCP-IA) Hands-on Lab is a remote lab hosted in the cloud. Each student has access to a 'Pod' that contains the following: Windows Client PC; Windows 2012 Server; Cisco CSR1000; and an account in the Zscaler service. Each service will be used as you progress through the labs.

Registration Emails

Upon registering for the ZCCP-IA Lab, and within 24hrs of the class start, you will receive an email from Zscaler with your login name and password for the Zscaler Admin Portal, and instructions on connecting to your assigned Pod.

Lab diagram

For your lab exercises you will be configuring an IPSec tunnel and then a GRE tunnel from the Cisco router to Zscaler in the cloud. The Windows 2012 server is providing directory services via Active Directory. The Windows Client PC is a client only and is used for verification of connectivity and authentication.



Lab 1: Verify No Protection

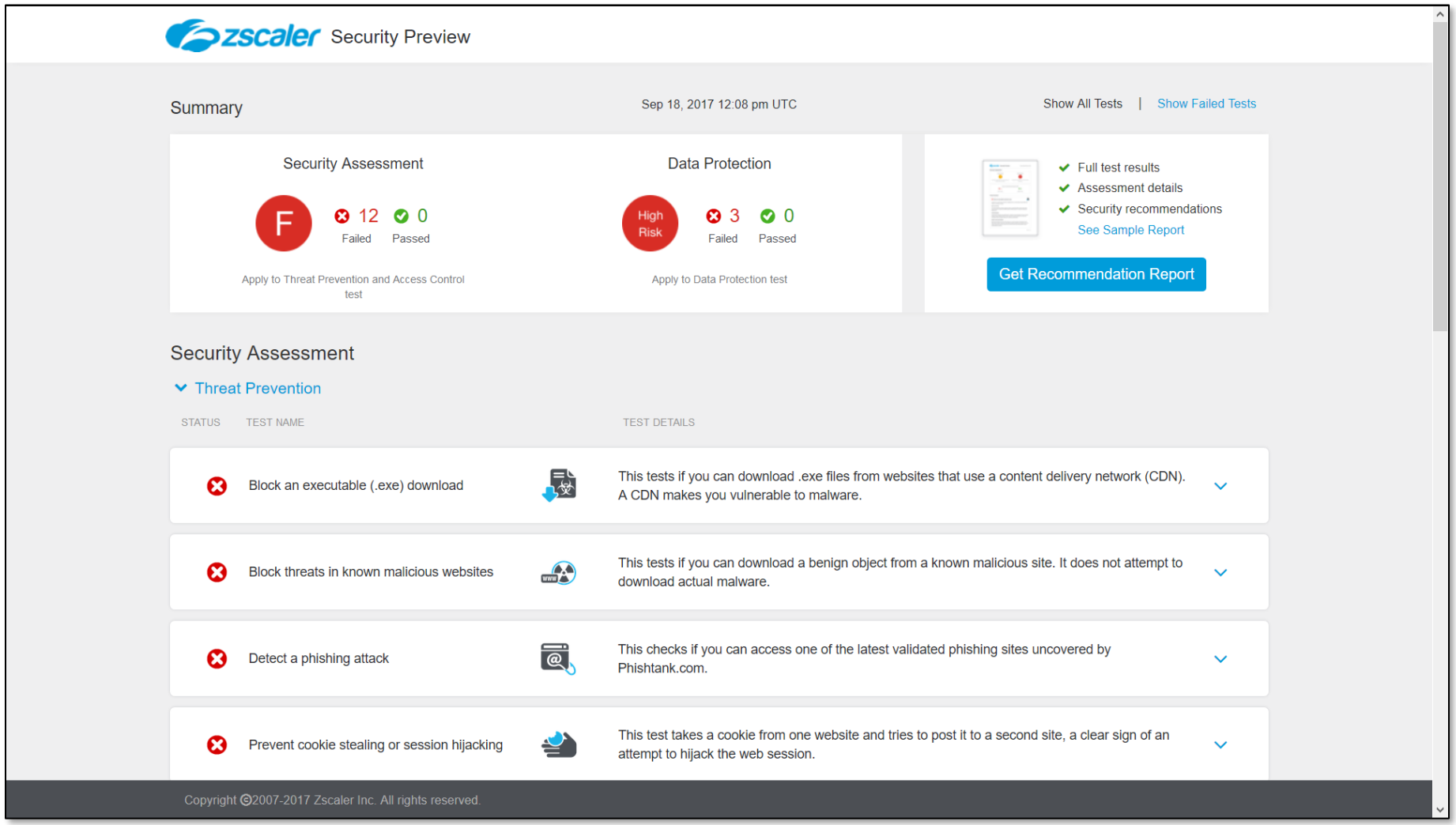
Your lab environment has been pre-configured with network settings including NAT on the Cisco such that only the Public IP is visible externally. No tunneling to Zscaler and no authentication have been configured. To demonstrate that no protection is in place you will visit a couple of websites.

1. On the **Windows Client PC**, from the VM tools bar send the **Ctrl-Alt-Del**, and login to the Domain with username **student** and password **Admin-123!**
2. Open a browser browser and go to **http://ip.zscaler.com**. This page will identify the source IP address, indicate if the traffic is flowing through Zscaler and providing protection, and if the user is authenticated. You will notice that your **Public IP** for your **Cisco** router is displayed, and that the system is stating that the traffic is not going through Zscaler. The space in the middle of the page is for the authentication status which should appear blank as no protection nor any authentication is happening currently.

3. Next, browse to the gaming website at **http://www.thebigfarmgame.com**. You should have access to this site, as Zscaler is not inspecting and protecting user traffic yet.

4. Run **Zscaler's Security Preview** by visiting **http://securitypreview.zscaler.com** and clicking the **Test your cyber risk posture**. After a few moments, you will receive a vulnerability assessment report. A complete report can be generated, and the site also provides descriptions of each of the tests performed and how they are performed. These are industry standard tests with no marketing gimmickry. This will show how vulnerable this network is. Later, after connecting through the Zscaler Global Security cloud you will execute the test again and compare results.

   Note: Security Preview will not run in the IE browser.



Note: There may be some tests that pass due to OS protective measures, however the overall assessment should fail.

Lab 2: Traffic Forwarding: Zscaler App

As you learned during the ZCCP-IA eLearning course user traffic must be forwarded to the Zscaler cloud for inspection and protection. Traffic forwarding is straight forward enough for a fixed location using IPSec or GRE tunnels, a solution is also required for your Road Warriors however. Traffic forwarding from an end device can be enabled using a PAC file, or the Zscaler App. In this Lab, you will practice the installation, management, and use of the Zscaler App.

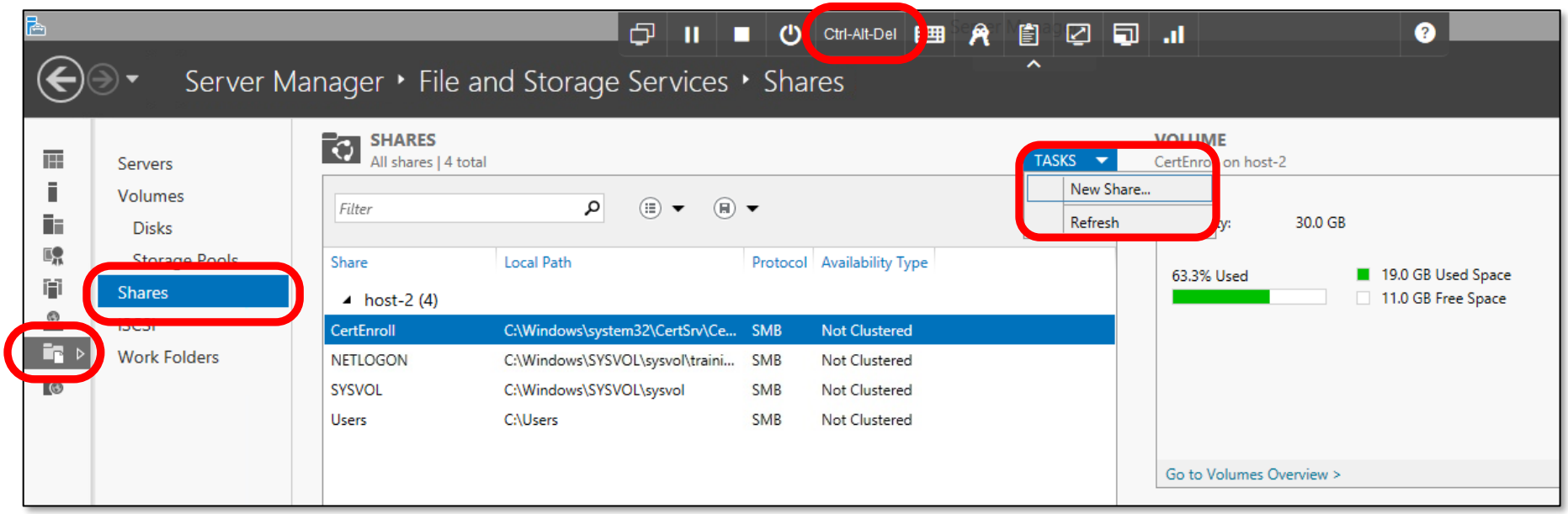
The Zscaler App can be installed on your users' computers to protect their web traffic even when they are outside your corporate network. The app forwards user traffic to the Zscaler service (tunneled or proxied) and ensures that the security and access policies in the Zscaler Admin Portal are enforced wherever the users may be accessing the Internet.

The recommended way to distribute the App to your end user's computers, is to use a Microsoft Active Directory (AD) 'Group Policy Object' (GPO) configuration, to push the install file silently – and that is how you will deploy the App in this Lab.

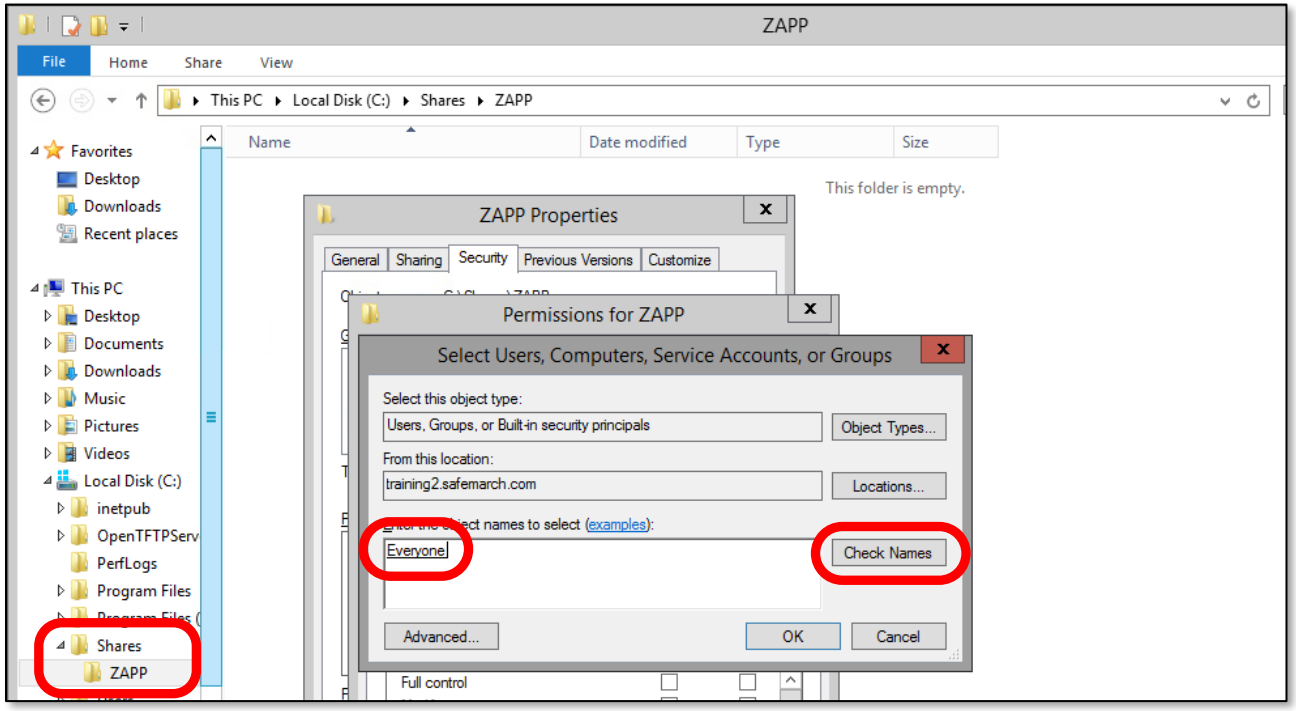
Create a Network Share for the Zscaler App Install Files

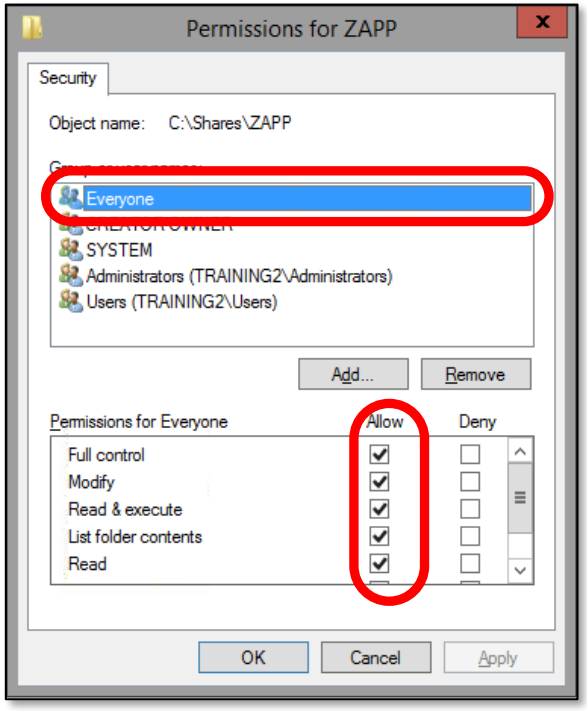
In this section, you will create a network share accessible to your users. This is where your users will install the Zscaler App from.

1. On the **Windows 2012 Server**, from the VM tools bar send the **Ctrl-Alt-Del**, and login to the server with username **Administrator** and password **Admin-123!**
2. Open the **Server Manager**, and in the side bar navigation menu at left, click on **File and Storage Services**.
3. Click on **Shares**, then on **TASKS** and select **New Share…**.



4. To configure the new share, in the **New Share Wizard**:
    a. At the **Select Profile** step, accept the default **SMB Share – Quick** and click **Next >**;
    b. At the **Select the server and path for this share** step, ensure that the server **host-2** is selected, and click **Next >**.
    c. At the **Specify share name** step, enter **ZAPP** as the **Share name:**, make a note of the Local and Remote paths and click **Next**
    d. At the **Configure share settings** step, click **Next >**.
    e. At the **Specify permissions to control access** step, click **Next >**.
    f. At the **Confirm selections** step, click **Create**, then click **Close**.
5. Run **File Explorer** and navigate to the folder at **C:\Shares**. Right-click on the **ZAPP** share you just created, select **Properties**, then go to the **Security** tab.
6. Under the **Group or user names:** box, click **Edit…**, then click **Add…**. In the **Enter the object names to select** field, type **every**, and click **Check Names**. Verify that the object **Everyone** is listed and click **OK**.
7. With the object **Everyone** selected, enable all permissions *except* **Special permissions**, click **Apply**, then **OK**, then **OK** again to close the **Properties** dialog for the share.

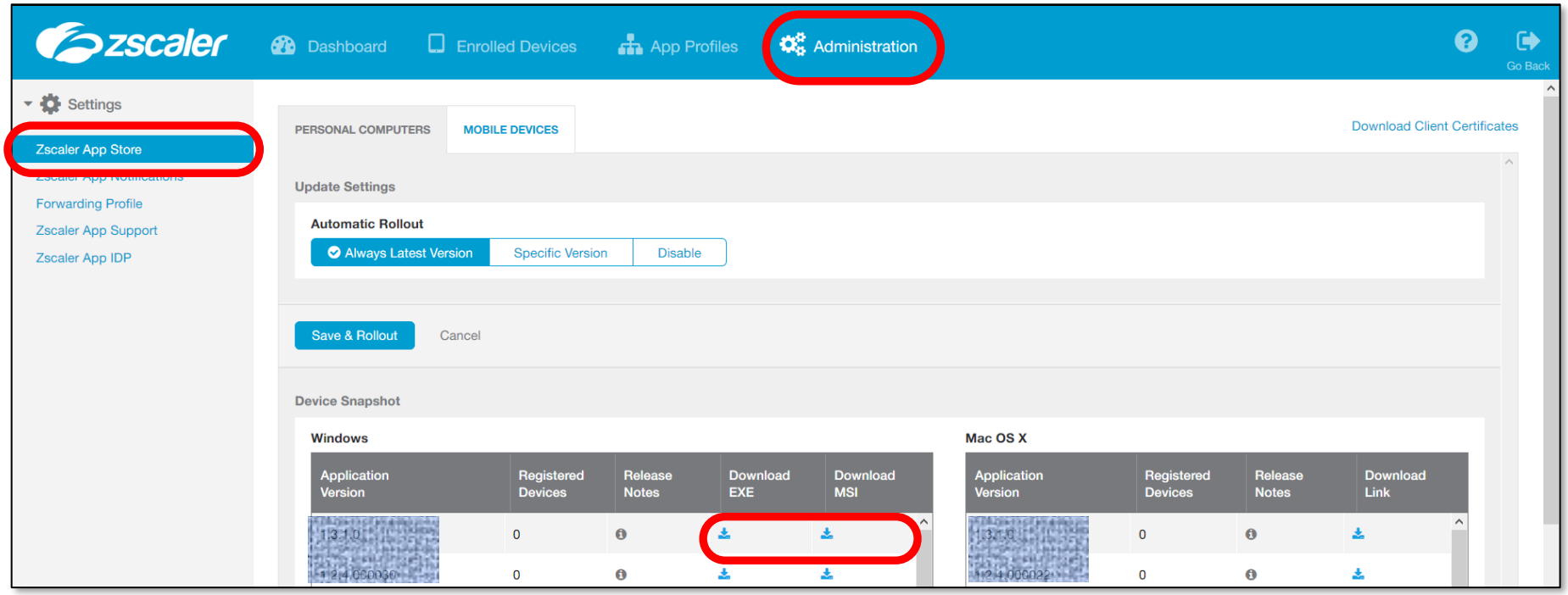




Download the Zscaler App

In this section, you will download the Zscaler App installers to the network share that you just created.

8. On the **Windows 2012 Server**, open a browser and go to the **Zscaler Admin Portal URL** (provided in your lab access instructions).
   Note: You must access the Admin Portal from the **Windows 2012 Server**, as you will need to download the install fle to a share on this machine.
9. Log into the **Zscaler Admin Portal** with the username and password assigned to you in the student access email that you received before the Lab session (**admin@training[1-N].safemarch.com**).
10. From the **Policy** menu, in the **Mobile** section under **ZSCALER APP CONFIGURATION** select **Zscaler App Portal**.
11. Within the **Zscaler App Portal**, navigate to the **Administration > Zscaler App Store** page and verify that you are on the **PERSONAL COMPUTERS** tab.
12. Under **Device Snapshot**, go to the **Windows** section and click on the **Download** link for the *latest version* of the App listed under the **Download EXE** column.



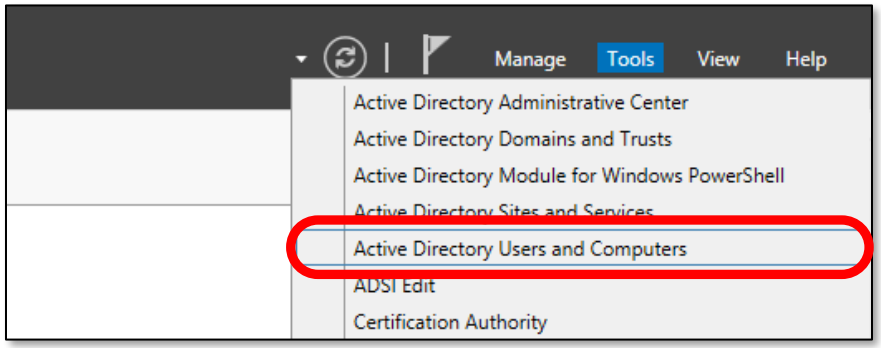
13. From the **Save** options select **Save as** and browse to the folder **C:\Shares\ZAPP** and click **Save**.
14. Repeat these steps to save the **.MSI installer** to the same folder.
15. Open **File Explorer**, navigate to the folder **C:\Shares\ZAPP**, and verify that both files are in there.

Create an Organizational Unit (OU)

In this section, you will create an OU on the AD server, and move the Windows Client PC, and a user into it. This OU will be used to specify who the Zscaler App GPO is to be assigned to.

Note: that a prerequisite to do this is that the Client PC be Domain-joined. This has already been taken care of for you.

16. On the **Windows 2012 Server**, from the **Server Manager Dashboard**, select the **Tools** menu at top right, then select **Active Directory Users and Computers**.



17. Expand the Directory tree and select your Domain **training[1-N].safemarch.com**.

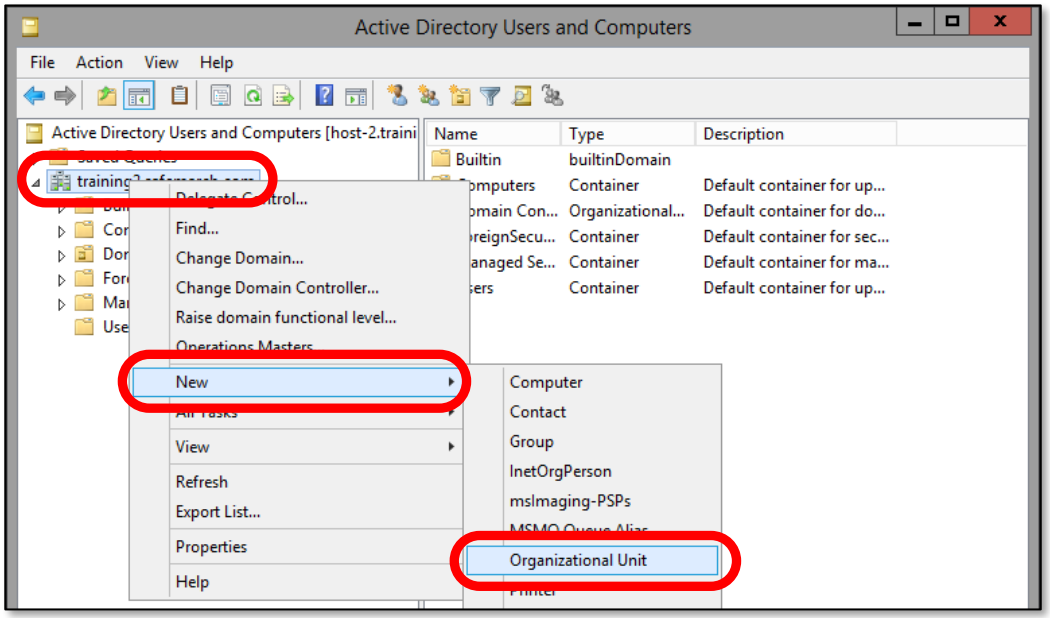
18. Right-click on the Domain, then select **New > Organizational Unit**.

19. Name the new OU **DeployZAPP** and click **OK**.

20. Expand your Domain if necessary and select **Computers**.

21. Right-click on the Computer named **CLIENT** and select **Move**. Select the new OU named **DeployZAPP** and click **OK**.

22. Under your Domain, select **Users**, then find and right-click on the User named **student** and select **Move...**. Select the new OU named **DeployZAPP** and click **OK**.



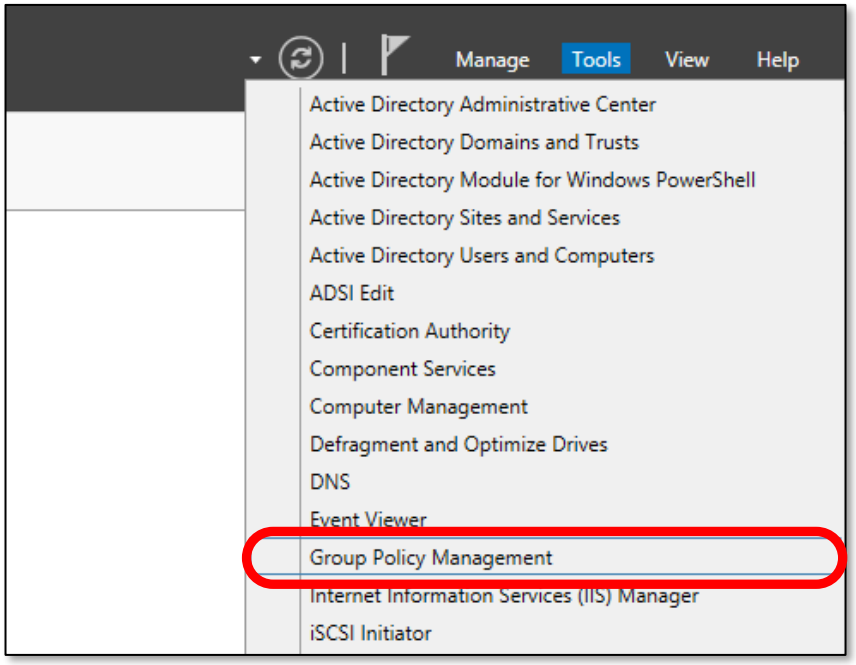
23. Under your Domain, select the new OU **DeployZAPP** and verify that it contains both the Computer named **CLIENT**, and the User named **student**.

24. Close the **Active Directory Users and Computers** window.

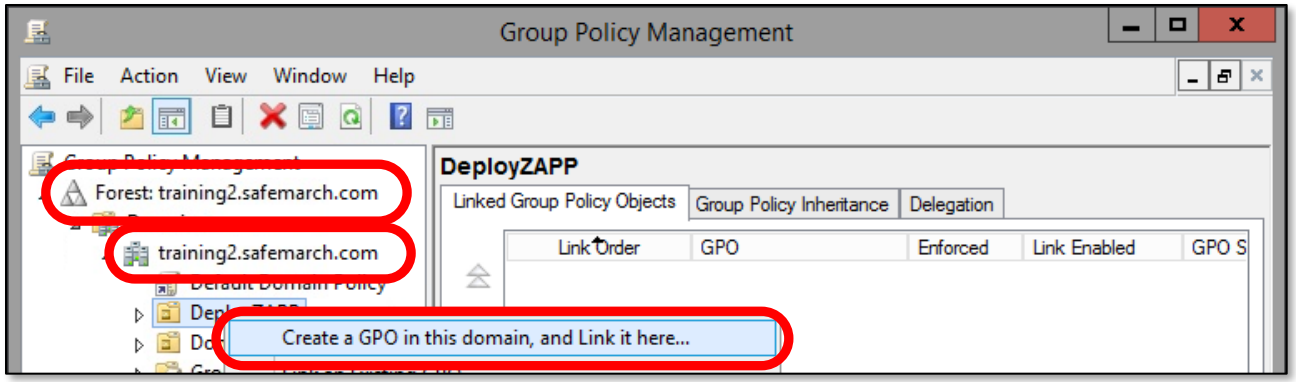
Create a GPO and Install the Zscaler App

In this section, you will create an AD GPO to push the Zscaler App to client PCs for silent installation.

25. On the **Windows 2012 Server**, from the **Server Manager Dashboard**, select the **Tools** menu at top right, then select **Group Policy Management**.

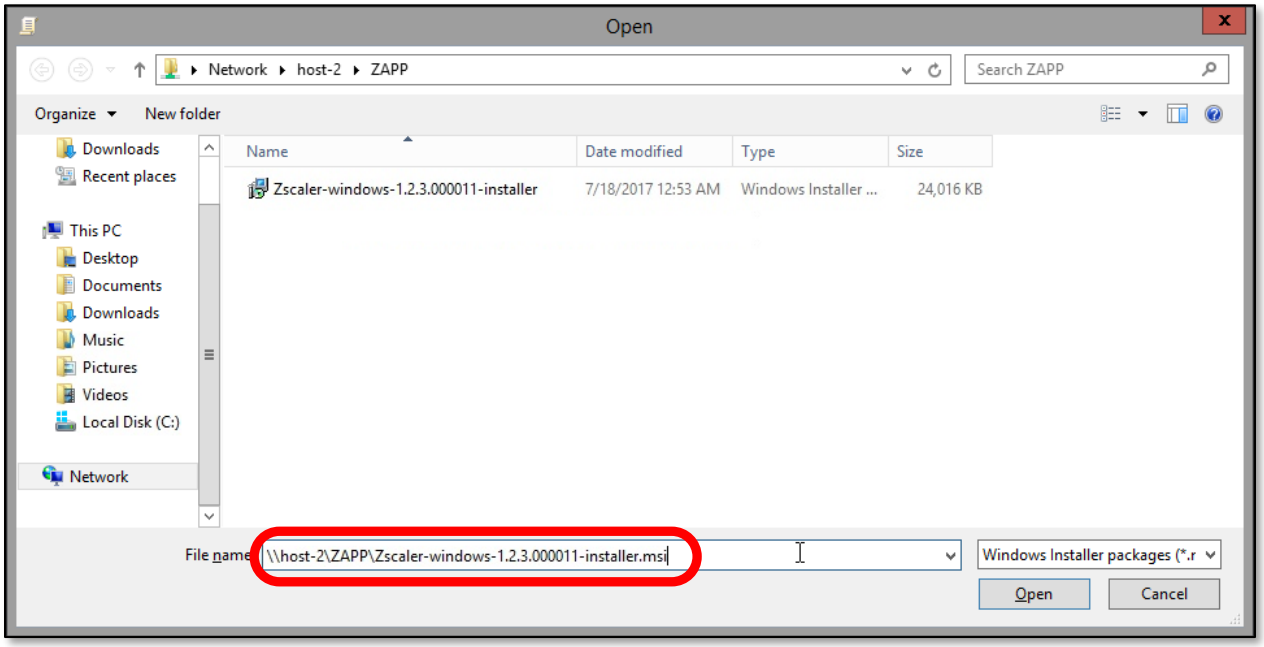


26. Expand the Forest named **training[1-N].safemarch.com**, expand the **Domains**, then expand your Domain. Right-click on the OU named **DeployZAPP** and select **Create a GPO in this domain, and link it here…**. Name the GPO **InstallZAPP** and click **OK**.



27. Expand the **DeployZAPP** OU, right-click on the new GPO named **InstallZAPP** and select **Edit**.
28. In the **Group Policy Management Editor**, under **Computer Configuration** expand the **Policies** item, then expand **Software Settings**.

    Note: we will deploy to the computer rather than to a specific user, so Zscaler App will be available for all users of the PCs it is installed to.
29. Right-click **Software Installation** and select **New > Package**. Navigate to the share with the Zscaler App installer files (**C:\Shares\ZAPP**) and select (***single click***) the **.msi file**.
30. In the **File name:** field add the full path to the server and share, so the location reads **\\host-2\ZAPP\Zscaler-windows-[Zscaler App version number]-installer.msi**, then click **Open**.



Note: It is critical to specify a path to the install file that the end user device can reach, this may be a relative path using a mapped drive, or an absolute path using the uniform naming convention (UNC) notation. UNC paths are generally a better option, and this is what we will use in this lab.

31. In the **Deploy Software** pop-up, select **Advanced** and click **OK**, then in the **Zscaler Properties** dialog, click **OK**. Verify that the file path is correct in the GPO, then close the **Group Policy Management** and **Group Policy Management Editor** windows.
32. On the **Windows Client PC** VM, from the Windows **Start** menu, expand the **Shut Down** menu and click **Restart**.
33. Once the **Windows Client PC** has restarted, on the VM tools bar click **Ctrl-Alt-Del**, and login to the Domain with username **student** and password **Admin-123!** Confirm that the Zscaler App runs and prompts you to enroll.

    Note: It may take a few minutes for the Zscaler App to be installed during reboot.

Login to the Zscaler App and Verify Protection

In this section, you will enroll into the Zscaler App, and confirm that the Windows Client PC is now being protected by the App.

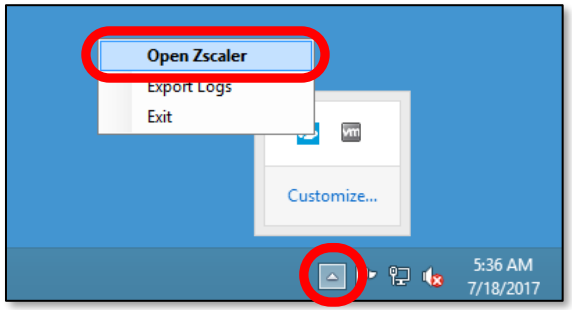
34. On the **Windows Client PC**, at the Zscaler App login screen enter your Zscaler Admin Portal **Username** from the student access email that you received (**admin@training[1-N].safemarch.com**) and click **Login**.

    Note: In a real-World deployment, you would log in with valid end user credentials, for the purposes of this Lab we are using the **admin** username as it is currently the only user defined on the Admin Portal.

35. If you are prompted to select a **Cloud**, select your assigned cloud name.

    Note: During this lab, **your assigned cloud name** is the name in the URL to access the Zscaler Admin UI. For example:

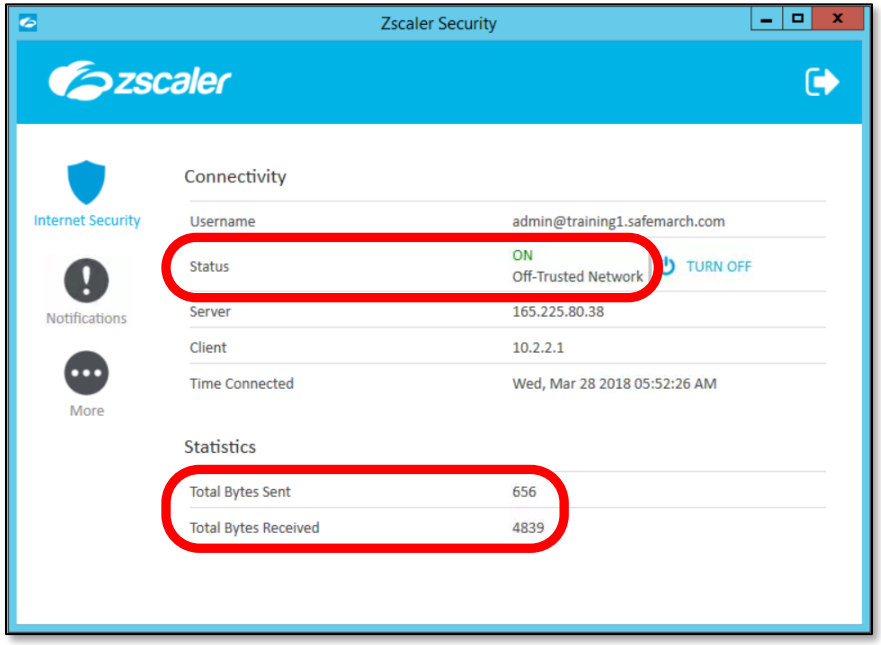
    - **https://admin.zscalerone.net** equates to the **zscalerone** cloud;
    - **https://admin.zscalertwo.net** equates to the **zscalertwo** cloud.



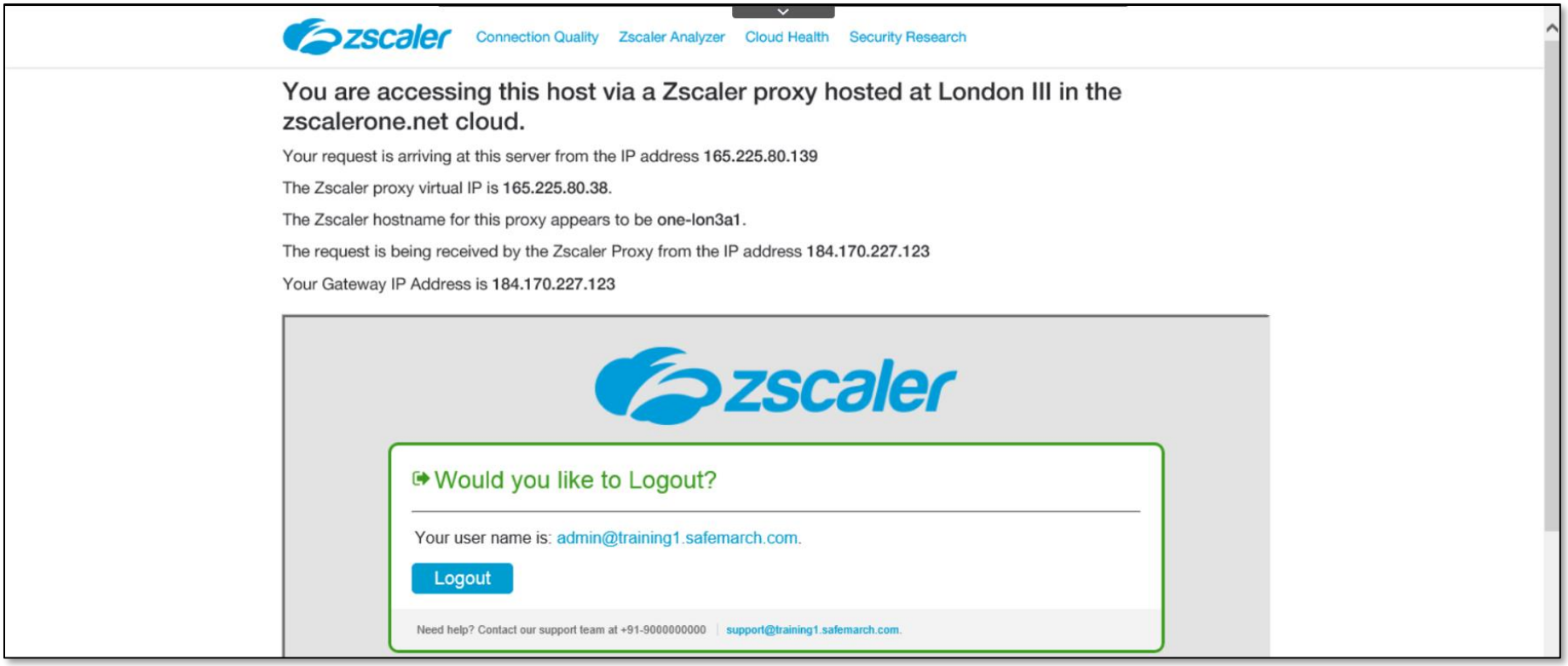
36. Enter the correct user **Password** (from the student access email) and click **Login**.

37. In the **Windows Task Bar**, at bottom right, click to **Show hidden icons**, click on the **Zscaler App** icon, then click **Open Zscaler**.

38. On the **Internet Security** page, confirm that **Status** indicates **ON**, that the **Username** is correct and that the **Total Bytes Sent** and **Total Bytes Received** increment when you load web pages.

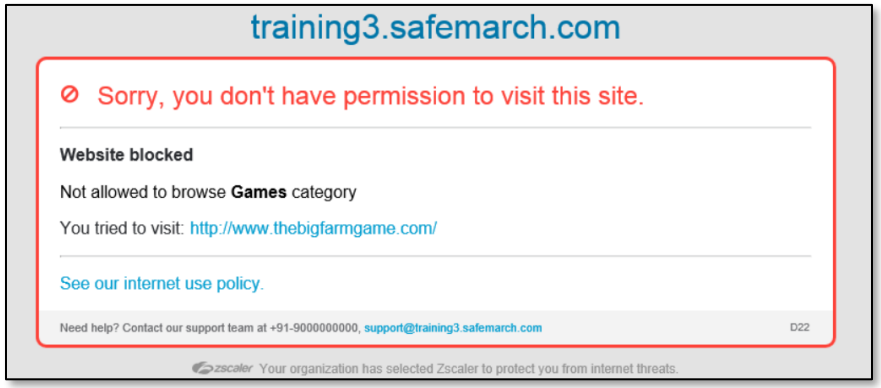


39. In a browser, navigate to the page at **http://ip.zscaler.com**, and review the information displayed.

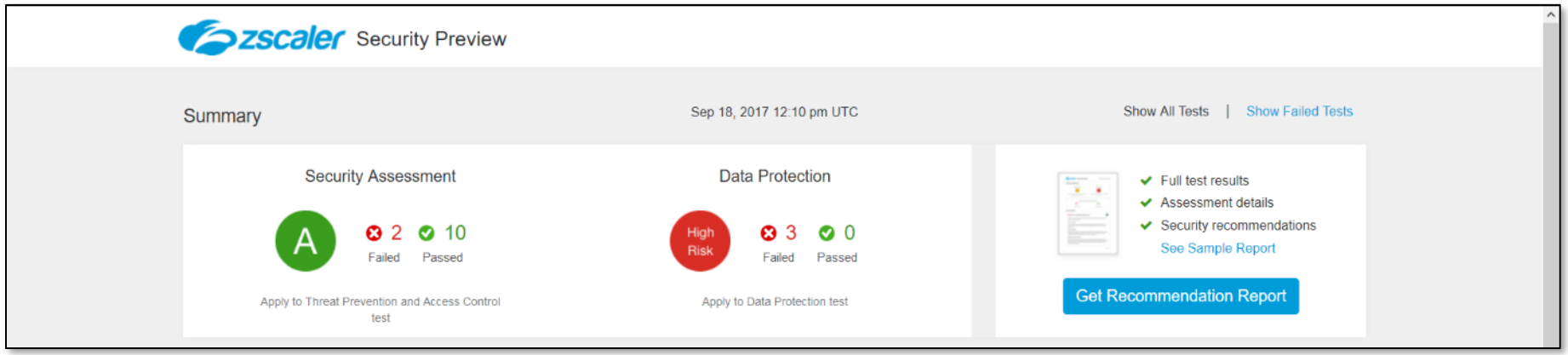


40. Browse to the gaming website at **http://www.thebigfarmgame.com**. You should see an End User Message (EUN) stating that you are not permitted to visit the site.

    Note: As the user is authenticating to Zscaler through the App, we can apply policies on any traffic coming through the system. In this case, a policy has been pre-defined for the lab blocking adult and gaming-oriented URLs.



41. Run Zscaler's **Security Preview** by visiting **http://securitypreview.zscaler.com** then clicking **Test your cyber risk posture**. Compare the results of this report to those from Lab 1.



Note: Currently only the default set of policies are being applied, at their default settings. This score can be improved further by customizing the policies applied to the users, and by adding the policies that are not applied by default.

Configuring Forwarding Options

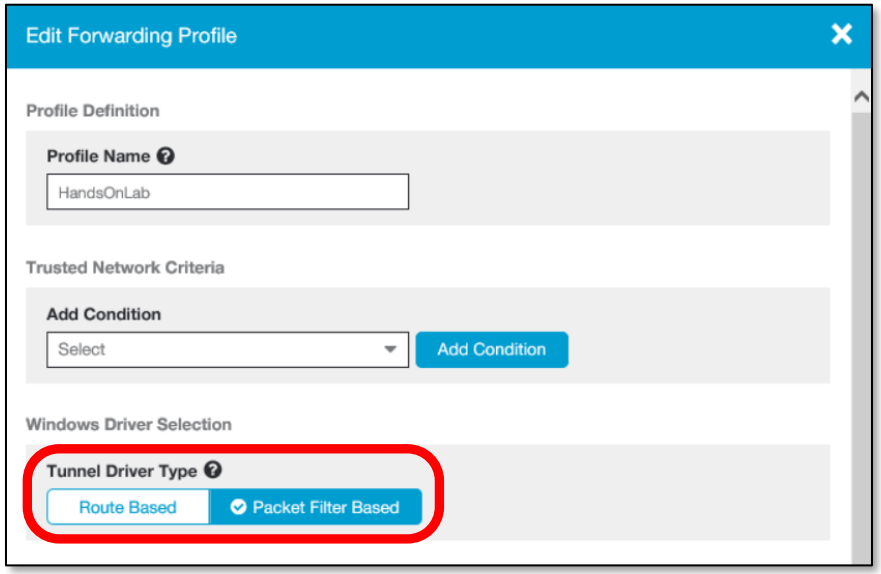
In this section, you will create a Forwarding Profile and configure the forwarding actions to be taken when a trusted network is detected, when a VPN to a trusted network is detected, or when the App recognizes that it is on an untrusted network.

42. On the **Windows 2012 Server**, in the **Zscaler App Portal**, navigate to the **Administration > Forwarding Profile** page.

    Note: You may also access the Admin Portal in a browser directly from your own PC.

43. To create and configure a **Forwarding Profile**, click **Add Forwarding Profile** and configure the policy as shown below:
    a. Name the profile **HandsOnLab**;
    b. In the **Windows Driver Selection** section, select **Packet Filter Based**.

    Note: The Packet Filter Based driver is recommended on the Windows platform, as it has improved performance, enforcement and integration. The driver (Route Based or Packet Filter Based) is only used in Tunnel mode.



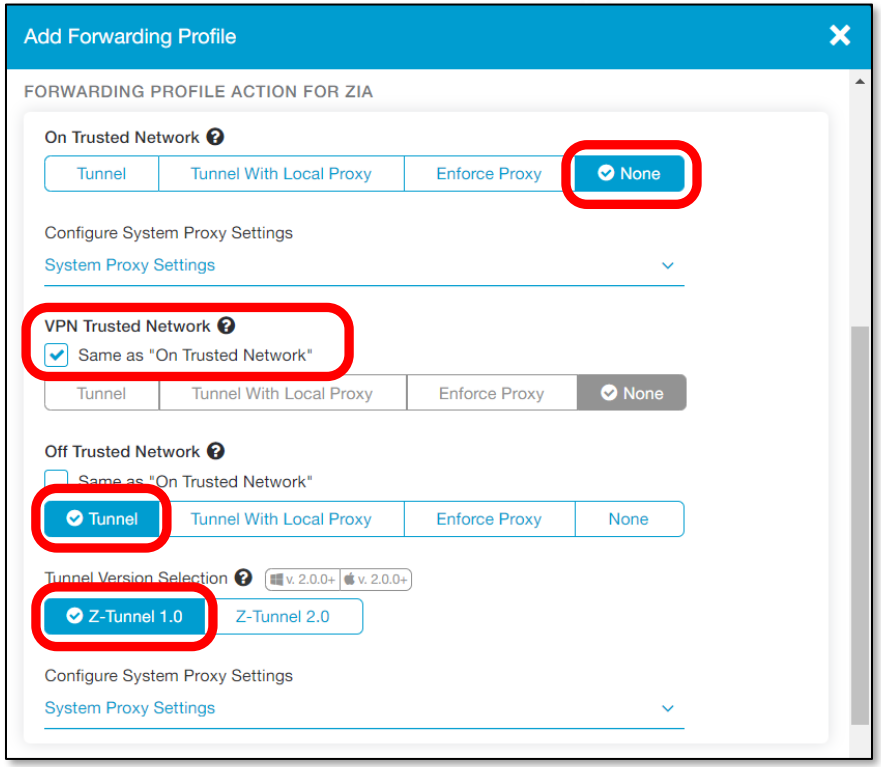
c. In the **Forwarding Profile Action** section under **On Trusted Network**, select **None**;

d. Under **VPN Trusted Network**, use the **Same as "On Trusted Network"** option;

e. Under **Off Trusted Network** select **Tunnel**.

f. Fot the **Tunnel Version Selection** use **Z.Tunnel 1.0**;

g. Click **Save**.

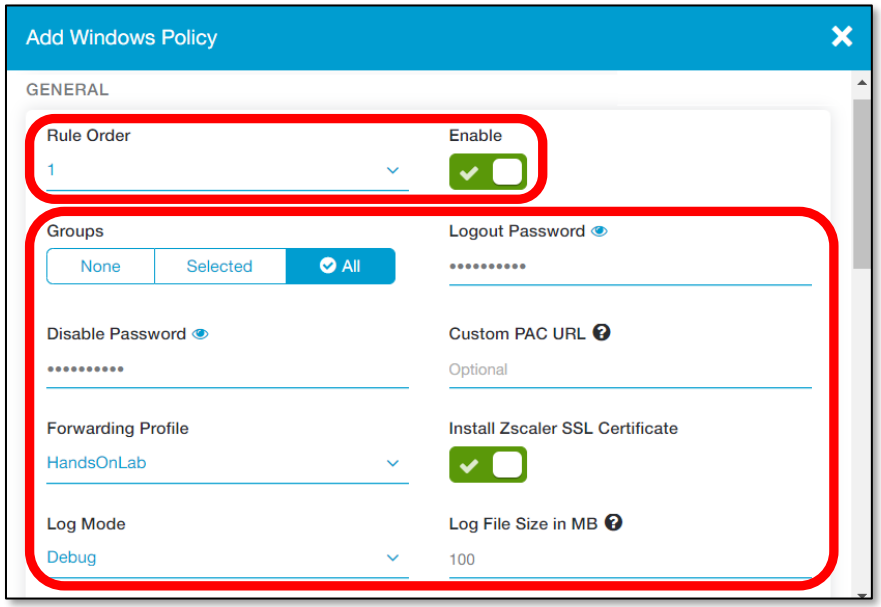


44. Navigate to the **App Profiles > Platforms > Windows** page, and delete any existing profiles except the one named **Default**.

45. To add and configure a new **App Profile** for a Windows machine, click **Add Windows Policy**, and configure the policy as shown below (any field not mentioned leave at default settings):
    a. **Name**: **HandsOnLab**;
    b. **Rule Order**: **1**;
    c. **Enabled**;
    d. **Groups**: Select **ALL**;
    e. **Logout Password** and **Disable Password**: **Admin-123!**
    f. **Install Zscaler SSL Certificate**: **Enable**;

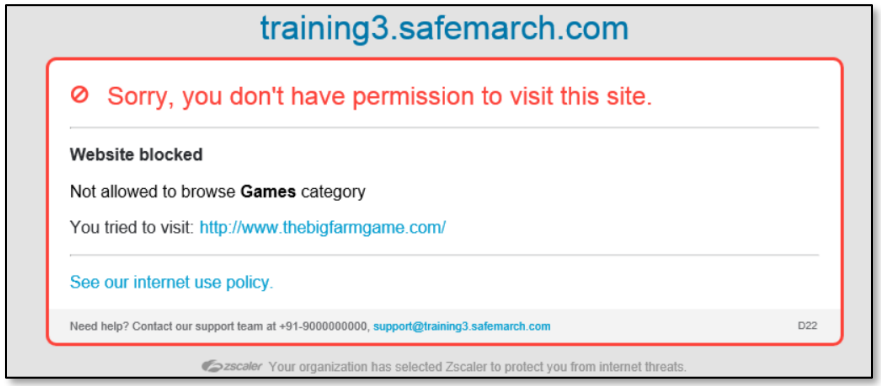
    Note: This will install the Zscaler Root CA Certificate to the client PC. If you have configured Zscaler for SSL Inspection, a best practice is to enable this option for your Zscaler App users.

    g. **Forwarding Profile**: select the profile named **HandsOnLab** that you created earlier;
    h. Click **Save**.



46. On the **Windows Client PC**, open the Zscaler App and navigate to the **More** page, then click **Update Policy**.

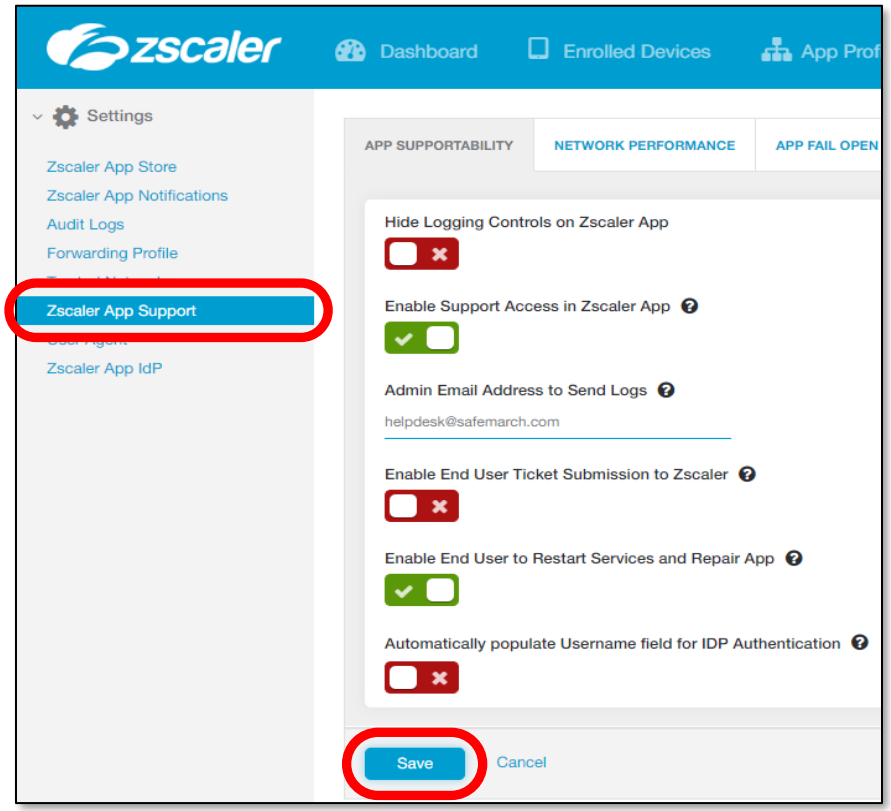
47. Confirm that you are still connecting through Zscaler by loading the page at **http://ip.zscaler.com**. Try to load **http://www.thebigfarmgame.com** and verify that you still receive an End User Notification.



Zscaler App Supportability and User Tools

In this section, you will explore some of the supportability tools available for the Zscaler App and some of the user tools available within the App.

48. Go back to the browser with the **Zscaler App Portal**, navigate to the **Administration > Zscaler App Support** page and on the **APP SUPPORTABILITY** tab:
    a. Enable the **Enable Support Access in Zscaler App** option;
    b. Enter your own email address in the **Admin Email Address to send logs** field;
       Note: In a real-world deployment, you would enter your helpdesk email address. For this Lab environment, do *NOT* enable the ***Enable End User Ticket Submission to Zscaler*** option.
    c. Enable the **Enable End User to Restart Services and Repair App** option;
    d. Disable the **Automatically populate Username field for IdP Authentication** option;
    e. Click **Save**.

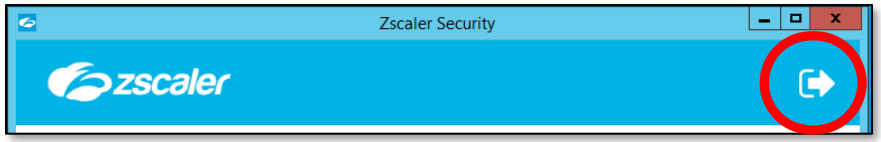


49. Navigate to the **Administration > Zscaler App Notifications** page, enable and create an **Acceptable Use Policy** statement.
    a. Set the **Configure AUP Frequency** option to **After each login**;
    b. Copy the text below and paste it into the **Configure AUP Message** field between the **** and **** tags (use the **Clipboard** option from the VM tools bar), replacing the text **Acceptable Usage Policy is not configured for your company**, then click **Save**.

    Infosecs intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the company's established culture of openness, trust and integrity. Infosec is committed to protecting company employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

    Note: in a real-World deployment, you would paste your genuine AUP and conditions into this field.

50. On the **Windows Client PC**, open the Zscaler App and click the **Logout** icon at top right, enter the logout password that you set earlier (should be **Admin-123!**) then click **Continue** to disable the App completely on the **Windows Client PC**.



51. Log back into the App using the same credentials as before, and verify that you are now prompted with, and must accept the **Acceptable Use Policy** before the App will load.

52. To explore some of the options available to end users within the App, navigate to the **More** page:
    a. Enable the **Show notifications in system** tray option;
    b. Check for a newer version of the App using the **Update App** option, watch for the system tray notifications.
    c. Restart the Zscaler service using the **Restart Service** option and confirm. Watch for the system tray notifications;
    d. Repair the App using the **Repair App** option and confirm. Watch for the system tray notifications;

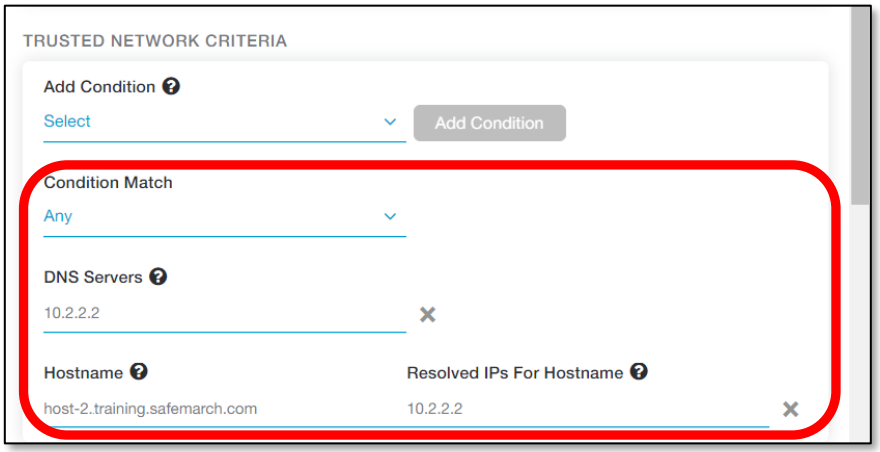
53. Within the App, navigate to the **Notifications** page and review the listed notifications.

Configuring Forwarding Options

In this section, you will modify the Forwarding Profile with criteria to detect a 'trusted' network (a network that is configured to tunnel traffic to Zscaler anyway).

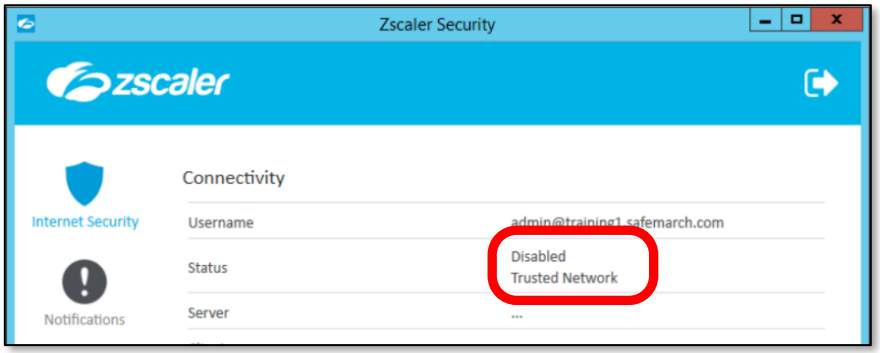
54. In the **Zscaler App Portal**, go back to the **Administration > Forwarding Profile** page and click to edit the Forwarding Profile that you created earlier (**HandsOnLab**).

55. Configure the policy as shown below:
    a. In the **Trusted Network Criteria** section select the **Add Condition** drop-down list, select **DNS Server**, then click **Add Condition**;
    b. Select the **Conditional Match** drop-down and select **Any**;
    c. In the **DNS Servers** field enter the IP address **10.2.2.2**;
    d. Click the **Add Condition** drop-down list again and select **Hostname and IP**, then click **Add Condition**;
    e. In the **Hostname** field enter **host-2.training[1-N]. safemarch.com**, in the **Resolved IPs For Hostname** field add the IP address **10.2.2.2**;
    f. Click **Save**.



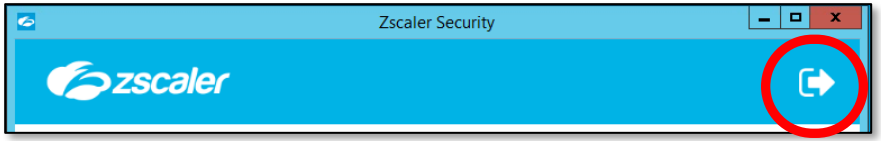
56. On the **Windows Client PC**, open the Zscaler App and navigate to the **More** page, then click **Update Policy**.

57. Navigate back to the **Internet Security** page and verify that the App indicates that it is in **Disabled** status, due to being on a **Trusted Network**.



58. Within the App, click the **Logout** icon at top right to disable the App completely on the **Windows Client PC**. Provide the password **Admin-123!** that you specified earlier.

59. Close the App once you have been logged out.



60. Confirm that the App is inactive by re-loading the page at **http://ip.zscaler.com**.

Lab 3: Traffic Forwarding: PAC Files

As you learned during the ZCCP-IA eLearning course, user traffic must be forwarded to the Zscaler cloud for inspection and protection. Traffic forwarding is straightforward enough for a fixed location using IPSec or GRE tunnels, a solution is also required for your Road Warriors, however. Traffic forwarding from an end device can be enabled using a PAC file, or the Zscaler App. In this Lab, you practice the use of PAC files.

Creating a Custom PAC File

Custom PAC files can be created at the Zscaler Admin Portal, and configured to proxy traffic through the Zscaler service, or to bypass Zscaler and go direct for specific destinations. In this section, you will create a simple custom PAC file to manage the forwarding of HTTP traffic.

1. On the **Windows Client PC**, open a browser (IE or Chrome) and go to the **Zscaler Admin Portal URL** (provided in your lab access instructions).

   Note: We recommend you do this from the Windows Client PC in the Lab to allow a simple copy/paste of the PAC file URL.

2. Log into the **Zscaler Admin Portal** using the username and password assigned to you in the student access email that you received (**admin@training[1-N].safemarch.com**).

3. From the **Administration** menu, in the **Resources > TRAFFIC FORWARDING** section, select **Hosted PAC Files**. Delete any PAC files other than the default read-only files.

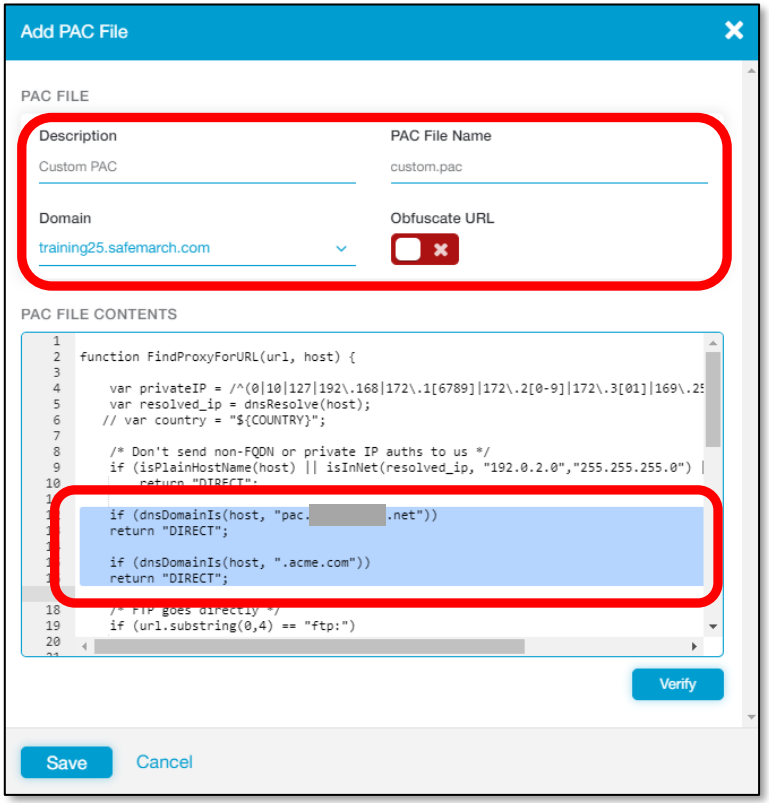
4. To add a custom PAC file, click **Add PAC File**:
   a. In the **Description** field, type **Custom PAC File**;
   b. In the **PAC File Name** field, type **custom.pac**;
   c. In the **Domain** field, select the domain for your pod (**training[1-N].safemarch.com**);
   d. **Disable** the **Obfuscate URL** option;
   e. In the **PAC FILE CONTENTS** section, at **line 11**, before the **`/* FTP goes directly */`** statement, paste in the lines shown below (use the **Clipboard** in the VM tools bar):

```
if (dnsDomainIs(host, "pac.<your_assigned_cloud>.net"))
return "DIRECT";

if (dnsDomainIs(host, ".acme.com"))
return "DIRECT";
```

   Note: During this lab, **<your_assigned_cloud>** is the name in the URL to access Zscaler Admin UI. For example:

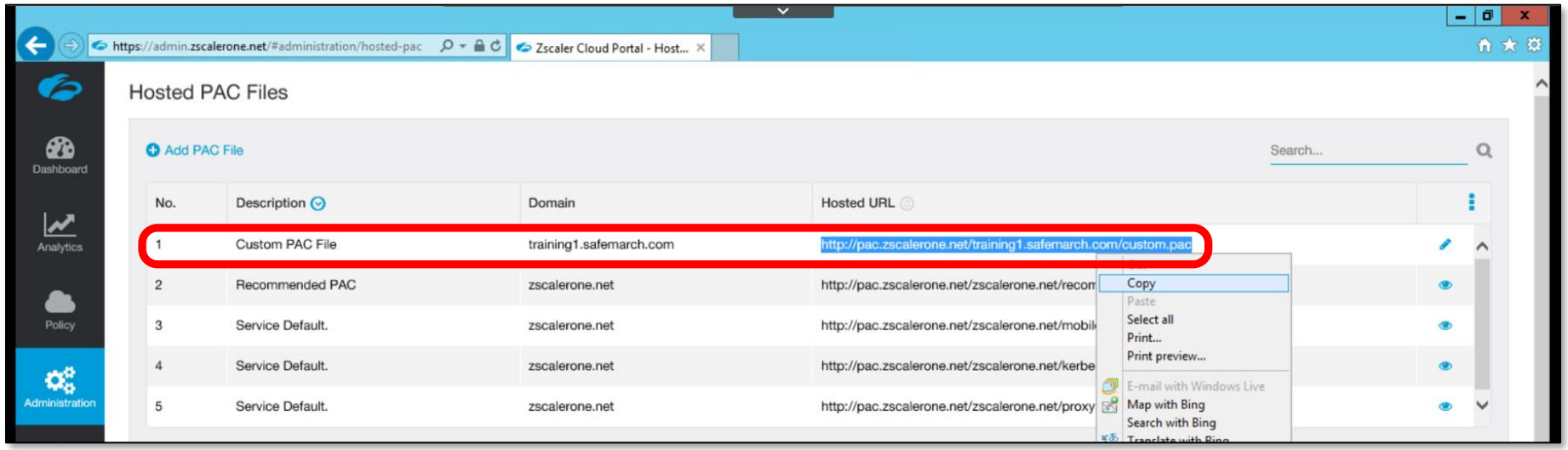
   - https://admin.**zscalerone**.net -> **zscalerone**;
   - https://admin.**zscalertwo**.net -> **zscalertwo**.



Note: Be sure to match the line format of previous and following entries, with the preceding tabs and leave a blank line before and after the new entries. This adds a bypass for the PAC file itself (which is a recommended best practice) and for the **.acme.com** domain, so that access attempts to them will go direct, i.e. they are bypassed by the PAC file.

f. Scroll down and click **Verify** to check the syntax of the new file;
g. Click **Save**, then **Activate** your changes.

5. Highlight the **URL** for the **Custom PAC File** that you just created, right-click and select **Copy**.



Applying and Testing the Custom PAC File

In this section, you will apply the file to your Client PC, and test connectivity in a browser.

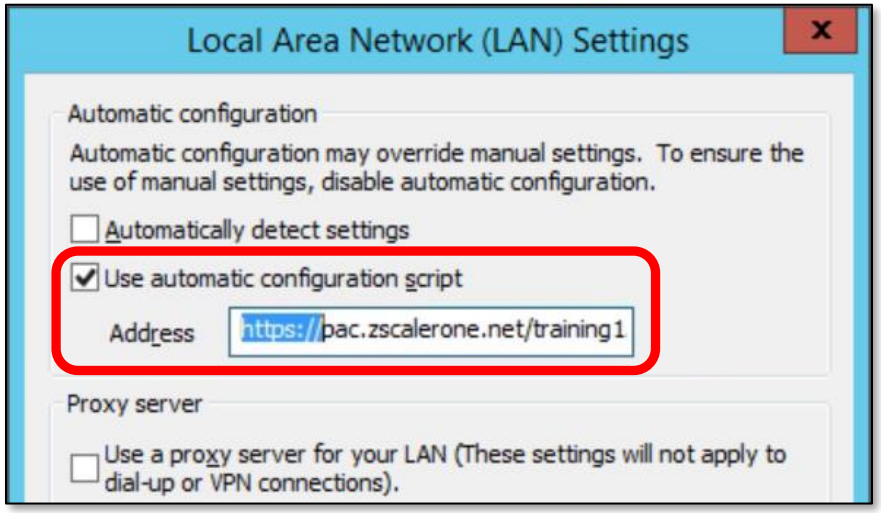
6. Close all browsers on the Client PC.
7. From the Windows **Start** menu, select **Control Panel > Internet Options**.
8. In the **Internet Properties** dialog, on the **Connections** tab, click **LAN Settings**.

9. Enable the option **Use automatic configuration script**, and paste the URL copied from the Zscaler Admin Portal into the **Address** field.
10. Change the URL's protocol definition to **https://**;

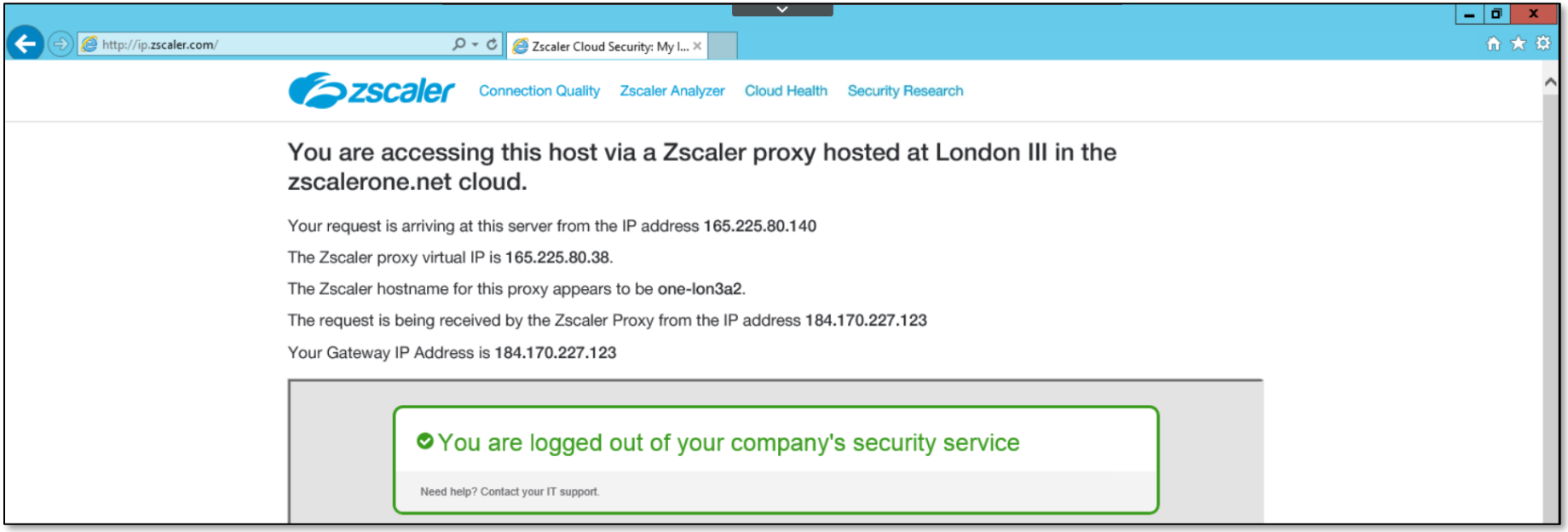
    Note: Zscaler best practice is to use HTTPS to retrieve PAC files, to ensure that they cannot be viewed or manipulated in transit to the user's browser.
11. Click **OK** and **OK** again to exit the **Internet Properties** dialog.

    Note: that both the Chrome and Firefox browsers pick up the system proxy configuration by default, although Firefox can be configured independently to other browsers on the system if necessary.
12. From the Windows **Start** menu restart the **Windows Client PC**.

    Note: Do NOT log back in to Zscaler App after the restart!

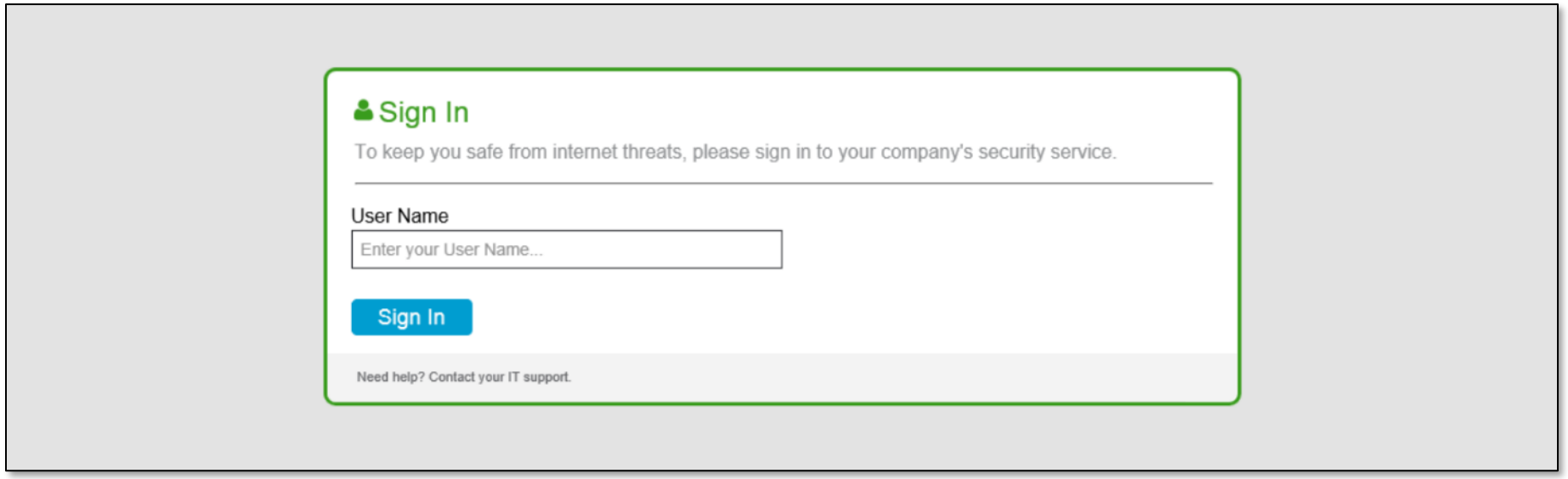


13. In a browser that follows the system settings (IE or Chrome), navigate to **http://ip.zscaler.com**, and review the information displayed.

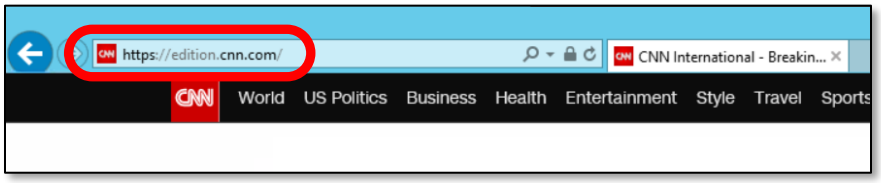


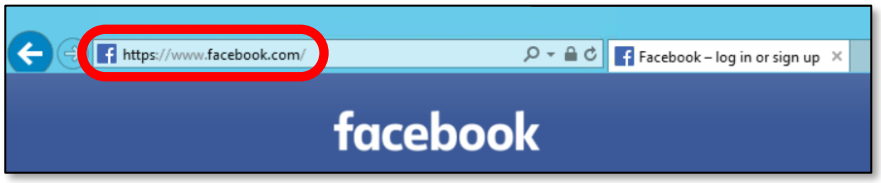
14. Confirm that you are connecting through the Zscaler service and are currently logged out.

15. Test network connectivity using a browser that follows the system settings (IE or Chrome):
    a. Open the browser and try to navigate to **http://www.google.com/**. The access request should be blocked and a **Sign In** page displayed, as you must now use the Zscaler proxy service to access the Internet and have not yet authenticated to Zscaler.



    b. Try to navigate to some other Web page, e.g. **www.cnn.com**, or **www.facebook .com**, these pages *will most likely load*. This is because the pages are redirected to HTTPS and we do not yet have SSL Inspection enabled.





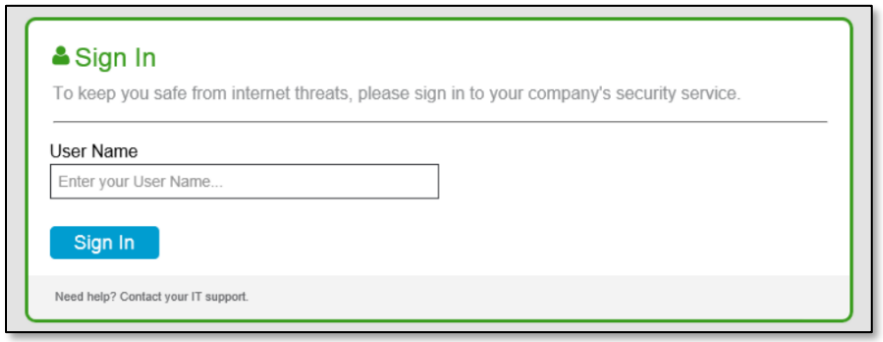
Reconfigure the Custom PAC File to activate SSL Inspection

In this section, you will reconfigure the PAC file to forward traffic on port 9443. This has the effect of turning on SSL Inspection for all traffic forwarded by the PAC file to Zscaler. This will ensure that the PAC file forwarding rules are correctly applied, whether for HTTP or HTTPS destinations.

16. On the **Windows Client PC**, open a browser once more, log back in to the **Zscaler Admin Portal**, go back to the **Administration > Resources > TRAFFIC FORWARDING > Hosted PAC Files** page and click to **Edit** the PAC file you created earlier.
17. Scroll to the bottom of the file and change the port numbers in the final **return** statement (below **/* Default Traffic Forwarding.**) to **9443** for both the **${GATEWAY}** and **${SECONDARY_GATEWAY}**.
18. **Save** and **Activate** the file changes.
19. Open the Windows **Internet Properties** dialog once more, go the **Connections > LAN Settings** and verify that the **use automatic configuration script** option is still enabled, and that the PAC file **Address** is correct. Click **OK** to exit.
20. From the Windows **Start** menu, restart the **Windows Client PC**.

    Note: Do NOT log back in to Zscaler App after the restart!

21. Open the browser and verify your connectivity:
    a. Navigate to the page at **http://ip.zscaler.com**, and review the information displayed.
    b. Try to navigate to any page, e.g. **www.cnn.com**, or **www.facebook.com**. You should now be redirected to the Zscaler login page as (according to the PAC file) most destinations must be proxied by Zscaler, however as we are not an open proxy, we will not forward traffic until we know who the user is.



c. In a new tab, navigate to the page at **https://trust.zscaler.com**. You should find that this is possible, as we bypass the **.zscaler.com** domain automatically.
d. Try to navigate to **http://www.acme.com/catalog**. This page should also load OK, as you configured a bypass for the **.acme.com** domain in the custom PAC file.

Note: The PAC file is now able to correctly redirect traffic to the Zscaler service, as all traffic proxied to Zscaler on port 9443 is SSL inspected. This means that we can reliably identify the primary site requested and any referred sites that may be included in the loaded page. The SSL inspection feature works correctly as the Zscaler App installed the Zscaler root CA certificate for you in Lab 2.

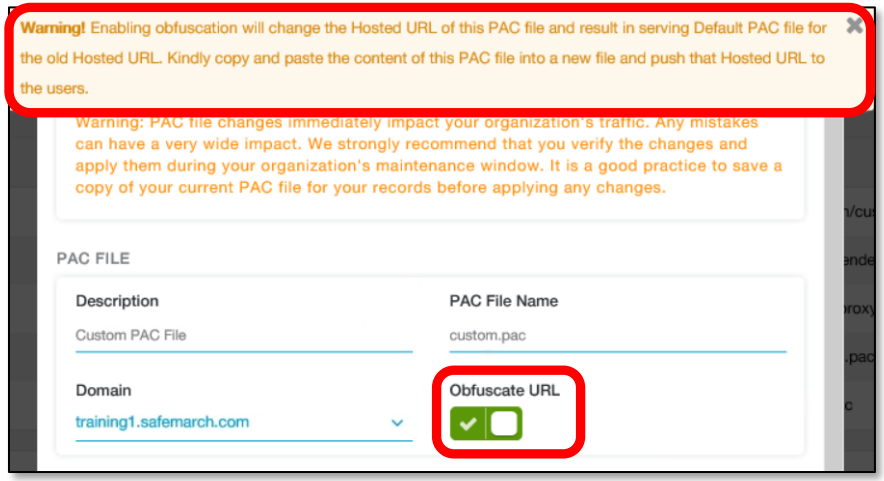
Obfuscating the domain portion of the PAC File URL

In this section you will enable the obfuscation of the domain portion of the PAC file URL, to help to conceal the organization that owns the PAC file.

22. Open the browser once more, log back in to the Zscaler Admin Portal, go back to the **Administration > Resources > TRAFFIC FORWARDING > Hosted PAC Files** page and click to **Edit** the PAC file you created earlier.
23. Enable the **Obfuscate URL** option and note the warning message displayed.

    Note: Having enabled the obfuscation of the URL, the updated PAC file URL must be configured in the Internet Properties of all users that need it. If not, the default PAC file for the Cloud will be delivered to them.
24. **Save** the change and **Activate** it.
25. Highlight the new obfuscated **URL** for the **Custom PAC File** that you just created, right-click and select **Copy**.

    Note: The domain part of the URL for the organization is now obfuscated, so nobody can identify the owner of the PAC file just from the URL.



26. On the Windows Client PC**,** close all browsers windows then open the Windows **Internet Properties** once more and go back to the **Connections > LAN Settings** page. Paste the new, obfuscated URL into the **Address** field to replace the URL you pasted previously. Change the URL's protocol definition to **https://** and save the configuration.
27. From the Windows **Start** menu, restart the **Windows Client PC**.

    Note: Do NOT log back in to Zscaler App after the restart!
28. Launch the browser once more and verify that the PAC functionality is as before.

29. In the browser, go to a tab showing the **Sign In** page (or try to load some Web page to trigger presentation of the **Sign In** page), enter the admin credentials for your instance (**admin@training[1-N].safemarch.com**) in the **User Name** field and click **Sign In**. When prompted for the **Password** enter the admin password from the student access email that you received and click **Sign In**.
30. Verify that you are authenticated successfully and are taken to the original URL that you requested. Confirm that you can browse the Internet at will.
31. Try to load the page at **http://thebigfarmgame.com** and confirm you see the Block EUN message.
32. Navigate to the page at **http://ip.zscaler.com**, and click **Logout**, then close all browsers and all tabs.

    Note: It is essential to logout after this Lab so as not to adversely impact the subsequent Labs. Also note that Zscaler provides a PAC file review tool at **https://tools.zscaler.com/pac/**, you can paste the PAC file URL into this page to see a review of the file and recommendations for improving it.

Disable the PAC configuration in the Browser and logout of the Zscaler service

You are done with the PAC file lab. Before moving on we want to disable the PAC file usage on the Windows Client PC. Continued use of the PAC file can mask configuration issues in the following Tunneling labs.

33. From the Windows **Start** menu, select **Control Panel > Internet Options**.
34. In the **Internet Properties** dialog, on the **Connections** tab, click **LAN Settings**.
35. Un-check the **Use Automatic Configuration Script** option, click **Ok** then **Ok** again to close the dialog box.
36. In a browser that follows the system settings (IE or Chrome) go to **http://ip.zscaler.com**.
37. If the service shows your admin account logged in click the **Logout** button to logout.
38. Clear the browser history then close ALL browser windows.

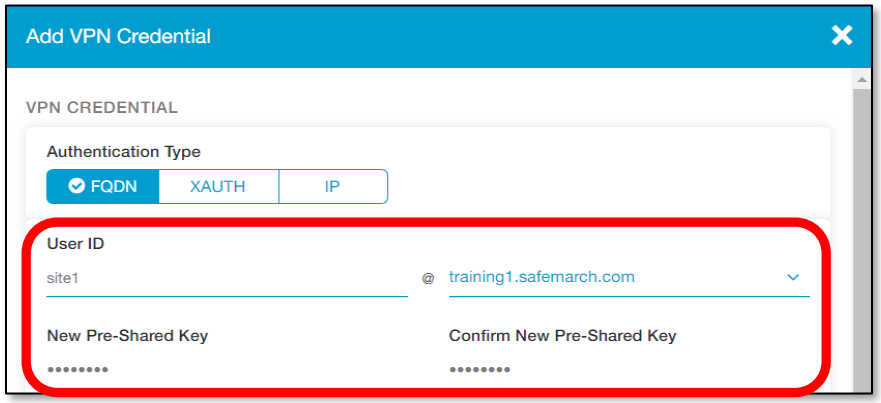
Lab 4: Traffic Forwarding: IPsec

As you learned during the ZCCP-IA eLearning course, user traffic must be forwarded to the Zscaler cloud for inspection and protection. Traffic forwarding can be accomplished in a number of ways, including: GRE Tunnel or IPsec Tunnel from a fixed location (GRE is recommended); The use of PAC files; Or the use of Zscaler App.
For the tunneling forwarding methods, the locations identify the various networks from which your organization sends its Internet traffic. When an organization forwards its traffic to the Zscaler service through a GRE or IPsec tunnel, Zscaler checks whether the traffic is from a known location (a location that is configured on the Admin Portal) and applies any applicable policies.

Zscaler Admin Portal Configuration
In this section, you will create the required VPN credentials to authenticate an IPSec VPN tunnel. If dynamic IP addressing is used on the IPSec VPN, these credentials also identify the customer to Zscaler (through the specified domain), so we know what policies to apply to any received traffic. You will also create the Location in the Zscaler Admin Portal.

1. Log into the **Zscaler Admin Portal** using the information from the student access email that you received and go to **Administration > Resources > TRAFFIC FORWARDING > VPN Credentials** page.

2. To create a new set of VPN credentials, click **Add VPN Credential**:
    a. Set the **Authentication Type** to **FQDN**;
    b. In **User ID** specify **site1** and confirm the domain is set to **@training[1-50]. safemarch.com**;
    c. For the **Pre-Shared Key** enter **site1key** and retype **site1key** to confirm;
    d. Click **Save**.



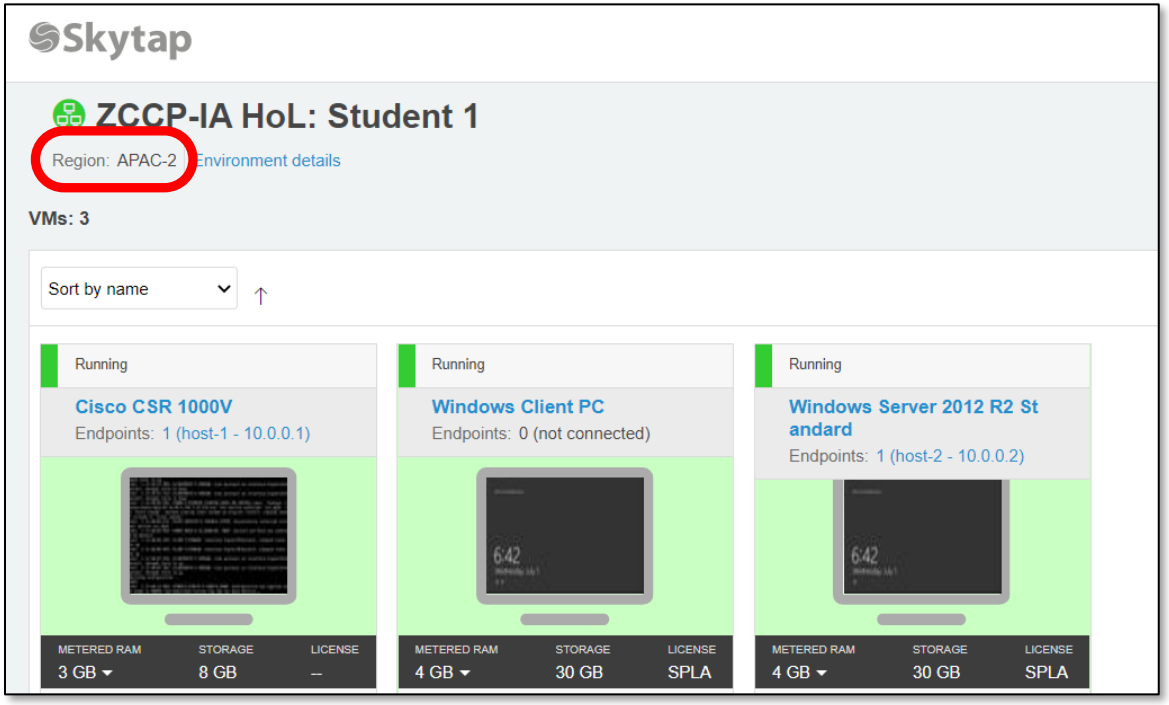
3. Go to the **Administration > Resources > TRAFFIC FORWARDING > Location Management** page.

4. To create a new Location, click **Add Location**:
    a. In the **Location** section provide the name for the location (e.g. **Site_1_IPSEC**);
    b. Select the **Country**, **State/Province**, and **Time Zone** as appropriate;
    Note: These fields are informational only.
    c. In the **Addressing** section select the **VPN Credentials** drop-down. Select the **email address** you provided in **an earlier step**, and click **Done**;
    Note: This will be used in combination with the **Pre-Shared key** when bringing up the IPsec Tunnel between the **Cisco** and Zscaler.
    d. Click **Save** and **Activate** your changes.

Cisco CSR1000 Configuration

In this section, you will configure the router for a primary and secondary IPsec tunnel to a Cloud Enforcement Node. The configuration is in a text file that resides on the desktop on your Windows Client VM. You will need to edit the file to input the proper VPN Host Name and VPN Credentials.

5. Find the region that your training environment is hosted in. Go to your Skytap access URL to see the **Region** listed at the top of the portal.



6. Depending on your Region, use the **Primary/Secondary VPN Locations** listed in the table below:

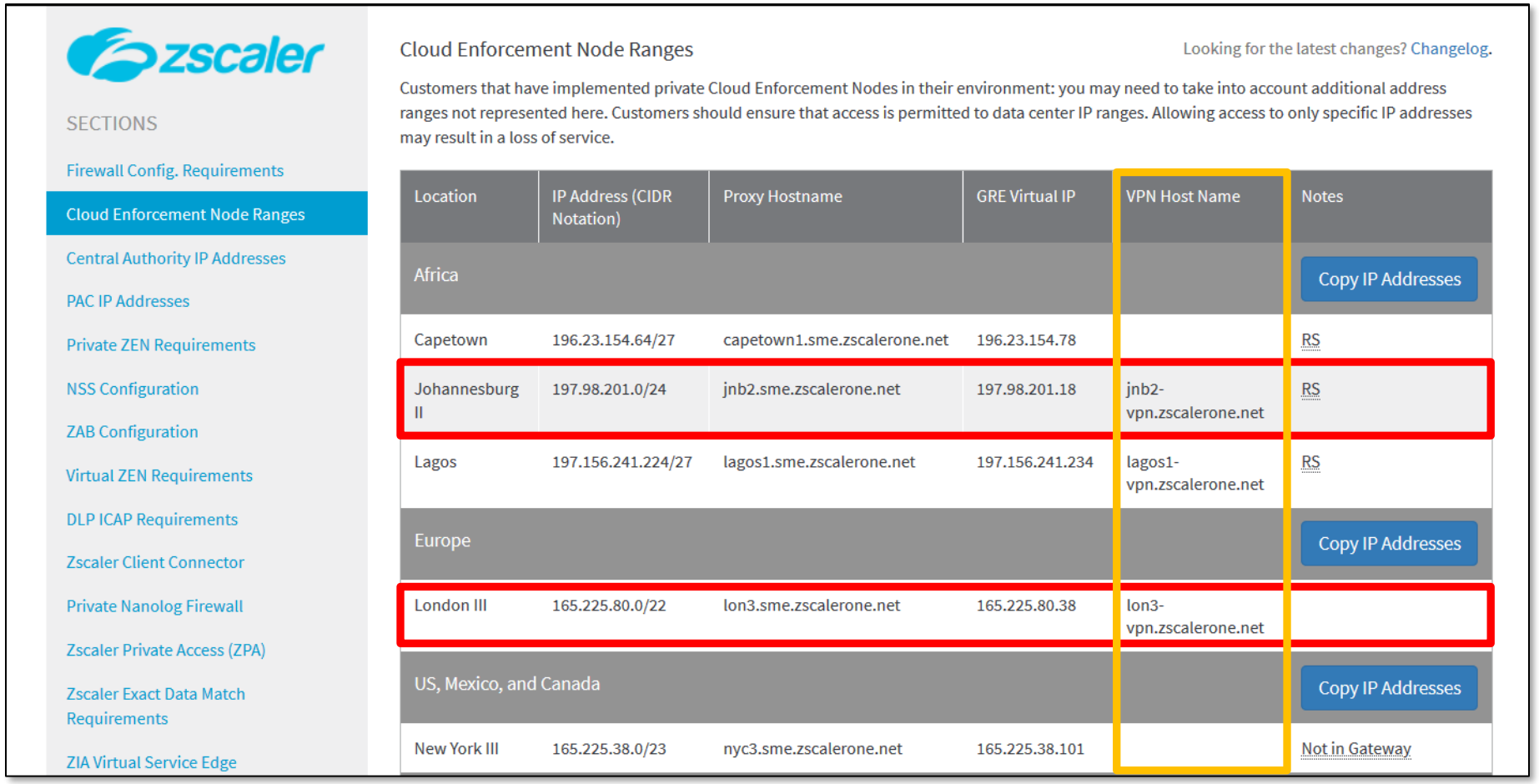
Training Data Center Location	Primary VPN Location	Secondary VPN Location
US East	London III	Johannesburg II
APAC-2	Singapore	Tokyo

Note: In production environments Zscaler Customer Service Team can advise on the lowest latency location reachable from your location. For this exercise use the training data center location assigned for your training session.

7. On the **Windows Client PC**, open a browser and visit **https://ips.<your_assigned_cloud_name>.net** then click on the **Cloud Enforcement Node Ranges** link in the left hand menu.

   Note: You need to do this on the Client PC, so you can copy/paste the **VPN Host Names** into the configuration file.

8. Make a note of the **VPN Host Name** for your ***primary*** connection (London III or Singapore).
9. Make a note of the **VPN Host Name** for your ***secondary*** connection (Johannesburg II or Tokyo).



SECTIONS

- Firewall Config. Requirements
- Cloud Enforcement Node Ranges
- Central Authority IP Addresses
- PAC IP Addresses
- Private ZEN Requirements
- NSS Configuration
- ZAB Configuration
- Virtual ZEN Requirements
- DLP ICAP Requirements
- Zscaler Client Connector
- Private Nanolog Firewall
- Zscaler Private Access (ZPA)
- Zscaler Exact Data Match Requirements
- ZIA Virtual Service Edge

Cloud Enforcement Node Ranges

Looking for the latest changes? Changelog.

Customers that have implemented private Cloud Enforcement Nodes in their environment: you may need to take into account additional address ranges not represented here. Customers should ensure that access is permitted to data center IP ranges. Allowing access to only specific IP addresses may result in a loss of service.

Location	IP Address (CIDR Notation)	Proxy Hostname	GRE Virtual IP	VPN Host Name	Notes
Africa					Copy IP Addresses
Capetown	196.23.154.64/27	capetown1.sme.zscalerone.net	196.23.154.78		RS
Johannesburg II	197.98.201.0/24	jnb2.sme.zscalerone.net	197.98.201.18	jnb2-vpn.zscalerone.net	RS
Lagos	197.156.241.224/27	lagos1.sme.zscalerone.net	197.156.241.234	lagos1-vpn.zscalerone.net	RS
Europe					Copy IP Addresses
London III	165.225.80.0/22	lon3.sme.zscalerone.net	165.225.80.38	lon3-vpn.zscalerone.net	
US, Mexico, and Canada					Copy IP Addresses
New York III	165.225.38.0/23	nyc3.sme.zscalerone.net	165.225.38.101		Not in Gateway

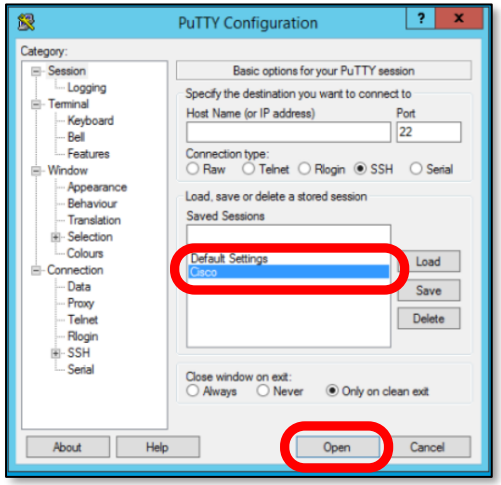
Caution! Be careful NOT to use either the **GRE Virtual IP** or the the **Proxy Hostname** from the adjacent columns!

10. On the desktop of the **Windows Client PC**, open the folder named **Student_X**. Open the file named **IPSEC_config**, review the contents and keep the file open for editing.
11. Replace the **PRIMARY VPN HOSTNAME** placeholder with the **VPN Host Name** for your ***primary*** connection.

    Note: You may need to scroll down, there will be two placeholders to change in the file.
12. Replace the **SECONDARY VPN HOSTNAME** placeholder the **VPN Host Name** for your ***secondary*** connection.

    Note: You may need to scroll down, there will be two placeholders to change in the file.
13. Edit the **site1@training[1-50].safemarch.com** placeholders with the correct **VPN Credentials** for this pod.

    Note: There will be two placeholders to change in the text file.
14. While in the IPSec configuration file, use **CTRL-A** to select ALL, and then **CTRL-C** to copy.
15. On the **Windows Client PC**, locate **PuTTY** on the desktop and open the Application.
16. Click to highlight and select the preconfigured **Cisco** connection.
17. Click **Open** to open the telnet session. A terminal window should open.
18. In the PuTTY terminal window, Enter the **Telnet password** from the **student access sheet**.




```
crypto isakmp policy 1
encryption aes
authentication pre-share
group 2
exit

crypto isakmp keepalive 10 periodic
crypto isakmp nat keepalive 20
crypto isakmp peer address PRIMARY VPN HOSTNAME
set aggressive-mode password site1key
set aggressive-mode client-endpoint user-fqdn site1@training[1-50].safemarch.com
exit

crypto isakmp peer address SECONDARY VPN HOSTNAME
set aggressive-mode password site1key
set aggressive-mode client-endpoint user-fqdn site1@training[1-50].safemarch.com
exit

crypto ipsec transform-set MYSET esp-null esp-md5-hmac
mode tunnel
exit

crypto ipsec fragmentation after-encryption
crypto ipsec profile VTI
set security-association lifetime seconds 14400
set security-association idle-time 14400
set transform-set MYSET
exit

interface tunnel 10
ip unnumbered GigabitEthernet 2
ip mtu 1400
ip tcp adjust-mss 1300
tunnel source GigabitEthernet 2
tunnel mode ipsec ipv4
tunnel destination PRIMARY VPN HOSTNAME
tunnel protection ipsec profile VTI
exit

interface tunnel 20
ip unnumbered GigabitEthernet 2
ip mtu 1400
ip tcp adjust-mss 1300
tunnel source GigabitEthernet 2
tunnel mode ipsec ipv4
tunnel destination SECONDARY VPN HOSTNAME
tunnel protection ipsec profile VTI
exit
```

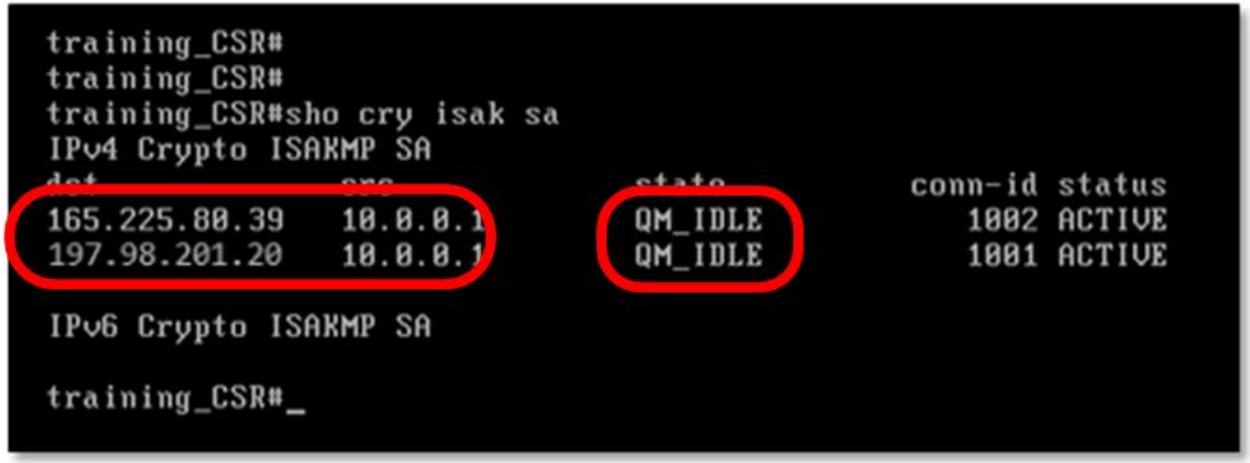
19. Enter **`enable`** mode by typing **`enable`**, and then enter the **enable password** from the student access sheet.
20. Type **`show ip interface brief`**. You will see that two interfaces have been created for your use.
    `GigabitEthernet 1` = this is the interior LAN interface.
    `GigabitEthernet 2` = this is the exterior WAN interface.

```
training_CSR#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.2.2.254      YES NVRAM  up                    up
GigabitEthernet2       10.0.0.1        YES NVRAM  up                    up
training_CSR#
```

21. **Right-click** in the PuTTY terminal window to paste the IPSEC config.
    Note: If you see any error messages, double check you IPsec text file for errors and try the process again. Exit **`conf t`** mode if needed by typing **`exit`**.
22. Once the configuration has been applied succesfully, enter the command **`write mem`**.

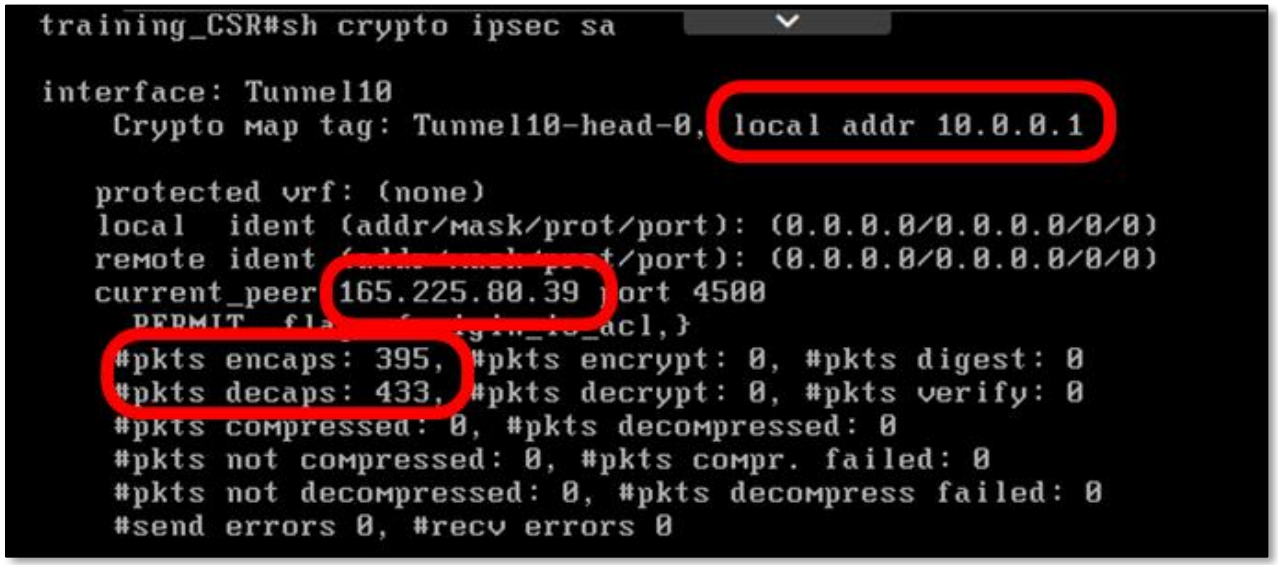
```
training_CSR(config-ext-nacl)#exit
training_CSR(config)#!
training_CSR(config)#$from the inside LAN network into the IPsec Tunnel.
training_CSR(config)#!
training_CSR(config)#route-map ZRM_IPsec permit 20
training_CSR(config-route-map)#match ip address ZSCALER_IPsec
training_CSR(config-route-map)#set interface tunnel 10 tunnel 20
training_CSR(config-route-map)#exit
training_CSR(config)#!
training_CSR(config)#! Tie the Route-Map to GigabitEthernet 1
training_CSR(config)#!
training_CSR(config)#interface GigabitEthernet 1
training_CSR(config-if)#ip policy route-map ZRM_IPsec
training_CSR(config-if)#exit
training_CSR(config)#exit
training_CSR#wr mem
Building configuration...
[OK]
training_CSR#
```

23. At this point the IPsec Tunnel should be active and traffic from the Windows PC should be flowing through the primary tunnel to Zscaler. Confirm this on the **Cisco** router with the command **`show crypto isakmp sa`**. Verify that the source and destination IP addresses are correct, and the state is shown as **`QM_IDLE`**.

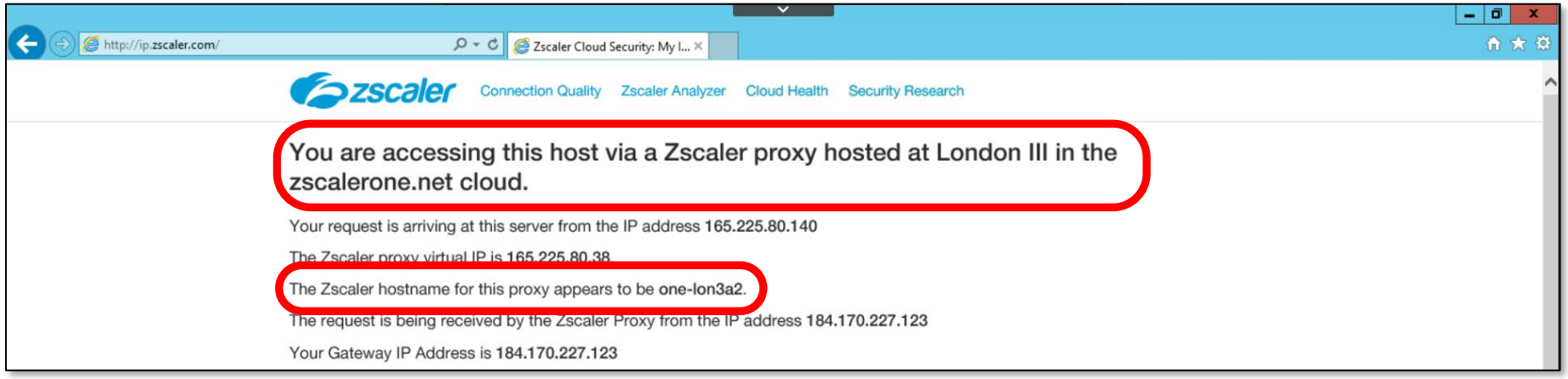


24. Use the command **`show crypto ipsec sa`**. Once again, check that the source and destination IPs are correct, that traffic is being encapsulated into the tunnel, and decapsulated out of the tunnel.

    Note: You will need to generate traffic in the tunnel from the **Windows Client PC** before the **encap**/**decap** values will increase.



25. To confirm that the tunnels are working, open a browser on the **Windows Client PC** then navigate to **http://ip.zscaler. com**. There are two IP addresses to look for on this page:
    - The line **Your request is arriving at this server from the IP address x.x.x.x** indicates the Zscaler node you are connected to;
    - Further down is a line **The request is being received by the Zscaler proxy from the IP address x.x.x.x**, where this is your public facing IP address from the lab environment.



26. The authentication status window (in red) shows that traffic is being received, but that authentication is **disabled** for the location. Which is correct, as authentication has not yet been configured. As such, you will not be prompted to authenticate when accessing the Internet, but we can still verify that traffic is flowing through the tunnels.

27. To verify that traffic flowing through the tunnels is now being protected by Zscaler, in the browser on the **Windows Client PC** browse to **http://www. thebigfarmgame.com** again.

Note: Even though the student account is not authenticating yet (so we cannot apply granular user-/group-based policies), Zscaler can still apply policies on any traffic coming through from known locations. In this case, a policy has been pre-defined for the lab blocking adult and gaming-oriented URLs.

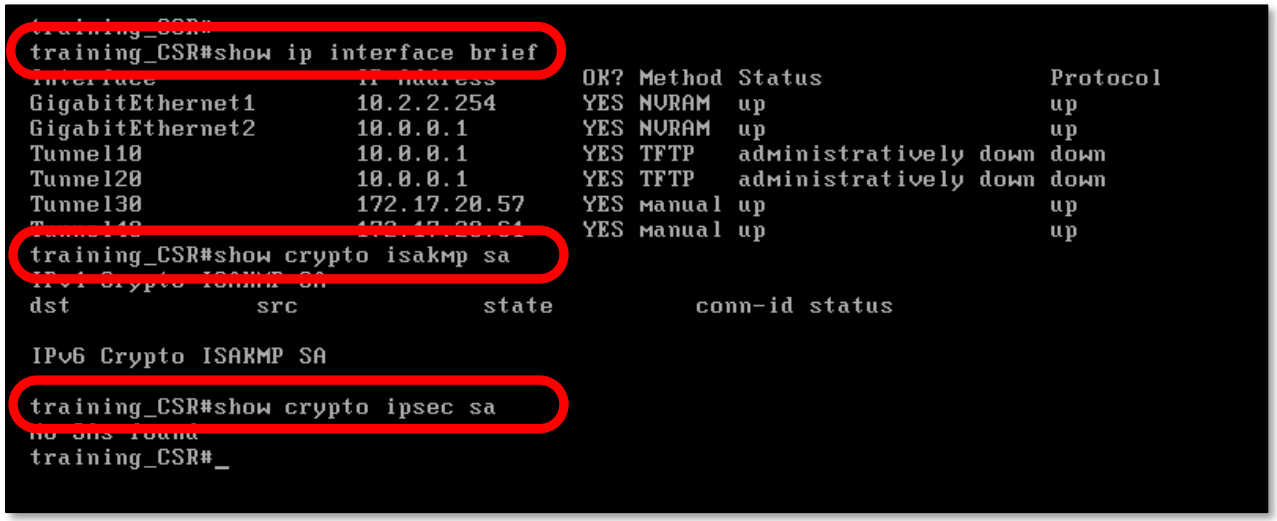
Router Cleanup

Now that we have successfully tested the IPsec deployment, we will clean up the IPsec configuration from the router.

28. Close the file named **IPSEC_config** and save changes.
29. Open or return to the PuTTY terminal session.
30. Enter **`enable`** mode by typing **`enable`**, and then enter the **enable password** from the **student access sheet.**
31. Type **`conf t`** to enter **`config terminal`** mode.
32. Shut down the existing IPSec tunnels using the commands:

```
interface tunnel 10
    shutdown
    exit
interface tunnel 20
    shutdown
    exit
exit
```

33. Verify that tunnels 10 and 20 are now down using the commands: **`show ip interface brief`**; **`show crypto isakmp sa`**; and **`show crypto IPsec sa`**. Confirm that the tunnels are inactive.



34. To save the running configuration to the boot configuration, enter the command **`write mem`**.

Lab 5: Traffic Forwarding: GRE Tunnel

As you learned during the ZCCP-IA eLearning course user traffic must be forwarded to the Zscaler cloud for inspection and protection. Traffic forwarding can be accomplished in a number of ways including: GRE Tunnel or IPsec Tunnel from a fixed location (GRE is recommended); The use of PAC files; Or the use of the Zscaler App.

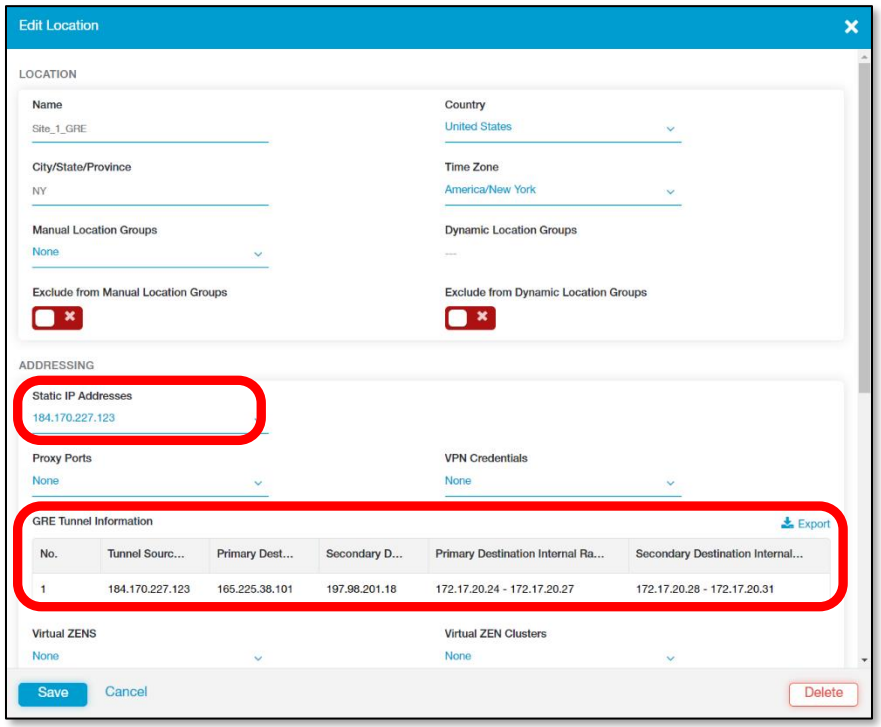
Zscaler Admin Portal

For this lab, you will create a new location and configure it for GRE tunnels.

1. Log into the **Zscaler Admin Portal** using the information from the student access email that you received, then go to the **Administration > Resources > TRAFFIC FORWARDING > Locations** page.

   Note: You may also access the Admin Portal in a browser direct from your PC.
2. Go to the **Administration > Resources > TRAFFIC FORWARDING > Location Management** page.
3. To create a new Location, click **Add Location**.
4. In the **Location** section provide the name for the location (e.g. **Site_1_GRE**).
5. Select the **Country**, **State/Province**, and **Time Zone** as appropriate.

   Note: These fields are informational only.
6. In the **Addressing** section select the **Static IP Addresses** drop-down box.
7. Select the **IP address** listed (this is your **Cisco**'s Public IP and was pre-configured for you) and click **Done**.
8. Scroll to view the **GRE Tunnel Information** in the GRE Tunnel Information section.
9. Record the following information from the **GRE Tunnel Information**:
   a. **Primary Destination**;
   b. **Primary Destination Internal Range**;
   c. **Secondary Destination**;
   d. **Secondary Destination Internal Range**.



10. Use the example below to record the **GRE Tunnel Source IP** and **GRE Tunnel Destination IP**. The Internal IP address range for your GRE tunnel configuration will be similar to **172.17.99.232 – 172.17.99.235 / 30**. Each IP address in the subnet is as follows:
    - **172.17.99.232** **Subnet Address** (cannot be assigned to any host);
    - **172.17.99.233** **Primary/Secondary GRE Tunnel Source IP** – 1st usable host address (customer on-premise Router);
    - **172.17.99.234** **Primary/Secondary GRE Tunnel Destination IP** – 2nd usable host address (Zscaler data center Router);
    - **172.17.99.235** **Broadcast Address** (cannot be assigned to any host).

    Note: ***This is an example only***, you need to read the IP address and subnet values from the GRE Location ***that you just created***.
11. In the **Zscaler Admin Portal**, click **Save**, then **Activate** your changes.

Cisco CSR1000 Configuration

In this section, you will configure the router for a primary and secondary GRE tunnel to a Cloud Enforcement Node. The configuration is in a text file that resides on the desktop on your Windows Client VM. You will need to edit the file to input the correct GRE primary / secondary and destination addresses.

12. On the **Windows Client PC**, find and open the folder named **Student_X** that is located on the desktop.
13. Open the file named **GRE_config**, review the contents and keep the file open for editing.

    Note: Notice the fields in red. The configuration file must be edited to include the GRE Tunnel information for your pod before applying to the router.

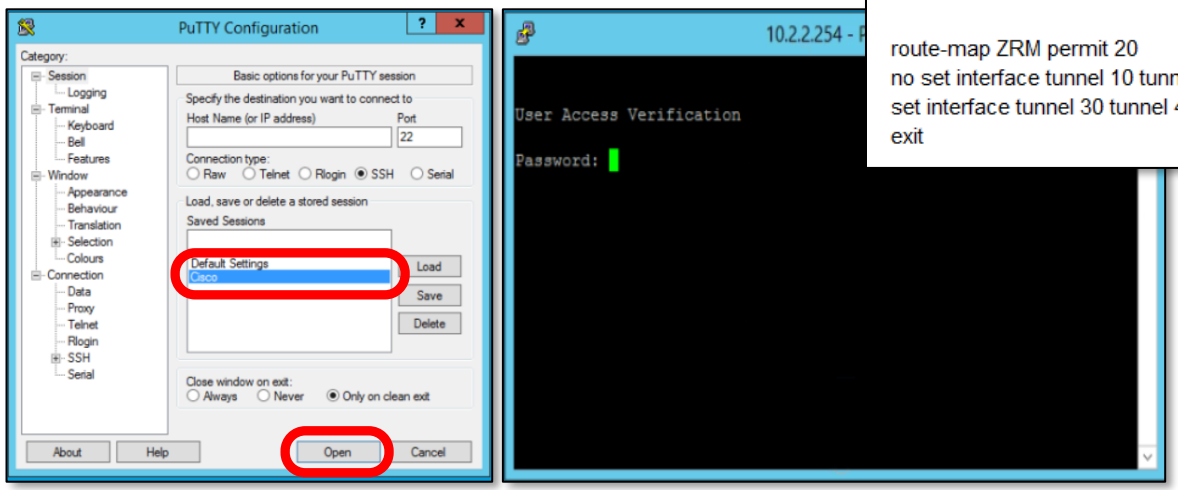
14. Edit the **GRE** file using the IP information you recorded in an earlier step:
    a. Replace the **<Primary Tunnel Source IP address - INTERNAL>** placeholder with your **Primary GRE Tunnel Source IP** address;
    b. Replace the **<Primary Destination IP>** placeholder with your **Primary Destination** IP address;
    c. Replace the **<Secondary Tunnel Source IP Address - INTERNAL>** placeholder with your **Secondary GRE Tunnel Source IP** address;
    d. Replace the **<Secondary Destination IP>** placeholder with your **Secondary Destination** IP address;
    e. Use **CTRL-A** to select ALL, and then **CTRL-C** to copy.
15. On the **Windows Client PC**, locate **PuTTY** on the desktop and open it.
16. Click to highlight and select the preconfigured **Cisco** connection.
17. Click **Open** to open the telnet session. A terminal window should open.

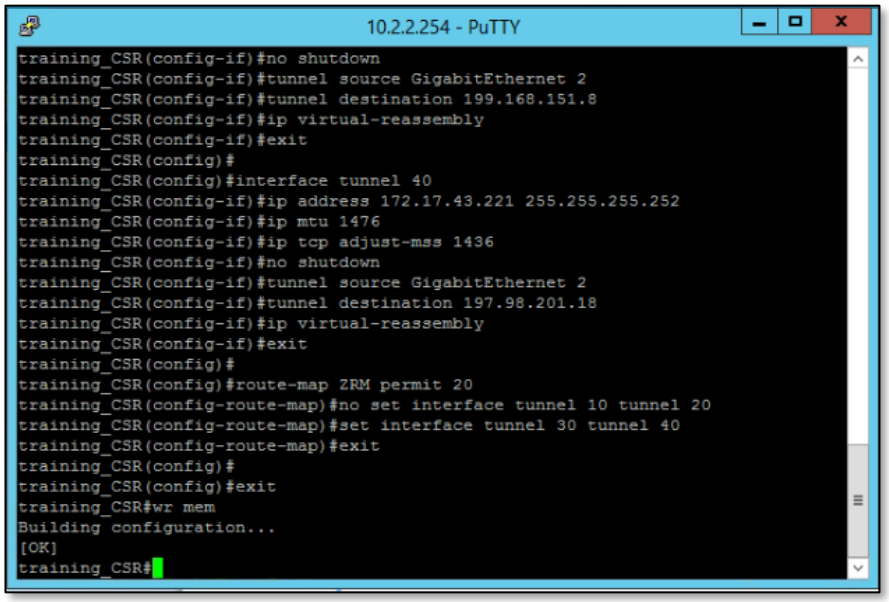
```
conf t
interface tunnel 10
shutdown
exit
interface tunnel 20
shutdown
exit

interface tunnel 30
ip address <Primary Tunnel Source IP address - INTERNAL> 255.255.255.252
ip mtu 1476
ip tcp adjust-mss 1436
no shutdown
tunnel source GigabitEthernet 2
tunnel destination <Primary Destination IP>
ip virtual-reassembly
exit

interface tunnel 40
ip address <Secondary Tunnel Source IP Address - INTERNAL> 255.255.255.252
ip mtu 1476
ip tcp adjust-mss 1436
no shutdown
tunnel source GigabitEthernet 2
tunnel destination <Secondary Destination IP>
ip virtual-reassembly
exit

route-map ZRM permit 20
no set interface tunnel 10 tunnel 20
set interface tunnel 30 tunnel 40
exit
```

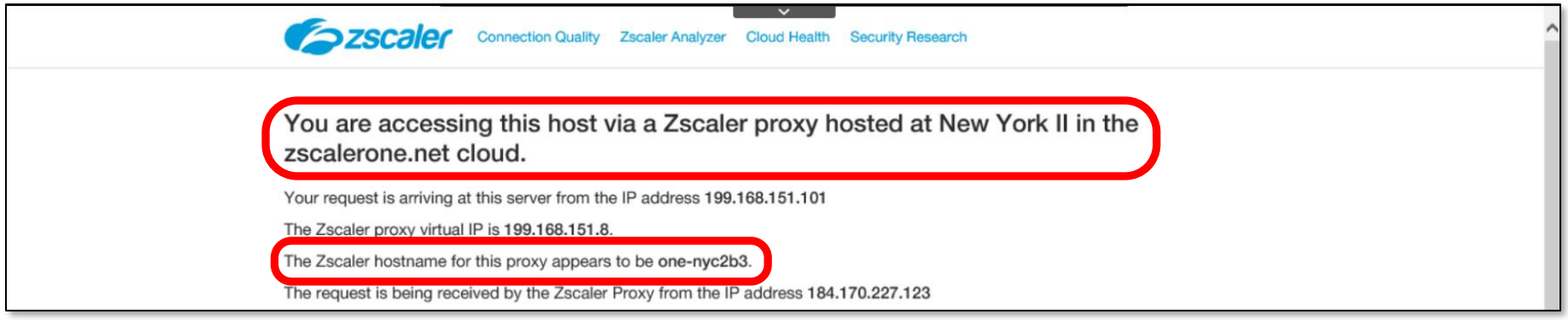




18. In the PuTTY terminal window, Enter the **Telnet password** from the **student access sheet**.
19. Enter **`enable`** mode by typing **`enable`**, and then enter the **enable password** from the **student access sheet.**
20. Right-click in the PuTTY terminal window to paste the GRE config.

    Note: If you see any error messages, double check your GRE file for errors and try the process again.
21. Exit **`Config terminal`** mode if needed by typing **`exit`**.
22. To save the running configuration to the boot configuration, enter the command **`write mem`**.
23. At this point the GRE Tunnels should be active and traffic from the Windows PC should be flowing through tunnel 30 to Zscaler. Authentication, however, has not yet been enabled. As such, you will not be prompted to authenticate but we can still verify that the traffic is flowing through the tunnel.
24. To confirm open a browser on the **Windows Client PC** then navigate to **http://ip.zscaler. com**. As before, there are two IP addresses to look for on this page:
    - The line **Your request is arriving at this server from the IP address x.x.x.x** indicates the Zscaler node you are connected to;
    - Further down is a line **The request is being received by the Zscaler proxy from the IP address x.x.x.x**, where this is your public facing IP address from the lab environment.

      Note: As before, the authentication status window (in red) shows that traffic is being received but that authentication is disabled for the location.
25. Make a note of the **Zscaler host name** for the proxy you are connected to.



26. Back on the **Cisco** use the command **`show interface tunnel 30`** and confirm the tunnel is up and you see the traffic in the counters.

```
training_CSR#show interface tunnel 30
Tunnel30 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.17.20.57/30
  MTU 9976 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 10.0.0.1 (GigabitEthernet2), destination 199.168.151.8
   Tunnel Subblocks:
      src-track:
         Tunnel30 source tracking subblock associated with GigabitEthernet2
          Set of tunnels with source GigabitEthernet2, 4 members (includes itera
tors), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:20:16
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     981 packets input, 708517 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runs, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     974 packets output, 131130 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
```

Note: You will need to generate traffic in the tunnel from the Windows Client PC before you will see traffic values.

27. On the **Cisco** shut down tunnel 30, using the commands:

```
conf t
interface tunnel 30
    shut
    exit
```

28. Traffic should fail over to tunnel 40. To check this, refresh the **Windows Client PC** browser while on **http://ip.zscaler.com**. After the refresh take note of the **Zscaler host name**, you should see that it has changed.
29. On the **Cisco** bring tunnel 30 back up, using the commands:

```
Conf t
interface tunnel 30
    no shut
    exit
exit
```

30. Traffic should fail back to tunnel 30.
31. Save your **Cisco** configuration by typing **`write mem`**.
32. Close the file named **GRE_config** and save changes.

Lab 6: Traffic Forwarding: IPSLA Monitoring for Tunnels

Tunnel redundancy is a key configuration to ensure continuous access for end users through the Zscaler cloud, although redundancy on its own is not enough. What is also required is a method for monitoring the health of the tunnels, and of automatically triggering a fail-over to the secondary tunnel if the primary stops responding. Cisco's 'Internet protocol service level agreement' (IPSLA) is a powerful and flexible tool, that can be configured to provide the continuous monitoring of your tunnels (IPsec or GRE) and the dynamic fail-over capability.

Adding IP SLA monitoring to GRE tunnels

Cisco's IPSLA is an additional layer of network monitoring that can be layered on top of existing tunnel heartbeats to not only be sure that your tunnels (in this case your GRE tunnels) are up, but that traffic is actually able to traverse the tunnel. IPSLA can be implemented in many different ways. The solution presented in this lab is designed to test reachability of a web site beyond the tunnel and out on the internet. If a response is not received within the configured intervals IPSLA will deem that there is a problem with the tunnel and force a failover from the primary tunnel to the secondary tunnel. This can occur regardless of the fact that the tunnel heartbeat mechanism says that the tunnel is healthy.

1. On the **Windows Client PC**, find and open the folder named **Student_X** that is located on the desktop.

2. Open the file named **IPSLA_config**, review the cntents and keep the file open for editing.

   Note: Notice the fields in red and blue. The configuration file must be edited to include the GRE Tunnel information and the cloud name for your pod before applying to the router.

```
conf t
track 1 ip sla 1 reachability
delay down 120 up 180
ip sla 1
http raw http://<Primary GRE Tunnel destination IP>
http-raw-request
GET http://gateway.<your_cloud_name>.net/vpntest HTTP/1.0\r\n
User-Agent: Cisco IP SLA\r\n
end\r\n
\r\n
exit
```

3. You will need to refer to Lab 5 for the **Primary/Secondary GRE Tunnel Destination IP Addresses**. This is the 2nd usable host address on the subnet, in the example we used in Lab 5:
   - 172.17.99.232 Subnet Address (cannot be assigned to any host);
   - 172.17.99.233 Primary/Secondary GRE Tunnel Source IP – 1st usable host address (customer on-premise Router);
   - **172.17.99.234** **Primary/Secondary GRE Tunnel Destination IP** – 2nd usable host address (Zscaler data center Router);
   - 172.17.99.235 Broadcast Address (cannot be assigned to any host).

   Note: ***This is an example only***, you need to read the IP addresses from the GRE Location that you created.

4. Make the following changes to the IPSLA config file:

   a. In the first **http raw** line, replace **<Primary GRE Tunnel destination IP>** with the **Primary GRE Tunnel Destination** address.

      Note: There should not be any spaces in the URL.

   b. Edit the **GET** request and replace **<your_cloud_name>** with your training pod Zscaler Cloud name.

      Note: There should not be any spaces in the URL. There should be a single space separating the URL from **HTTP/1.0\r\n**.

   c. In the second **http raw** line, replace **<Secondary GRE Tunnel destination IP>** the **Secondary GRE Tunnel Destination** address.

      Note: There should not be any spaces in the URL.

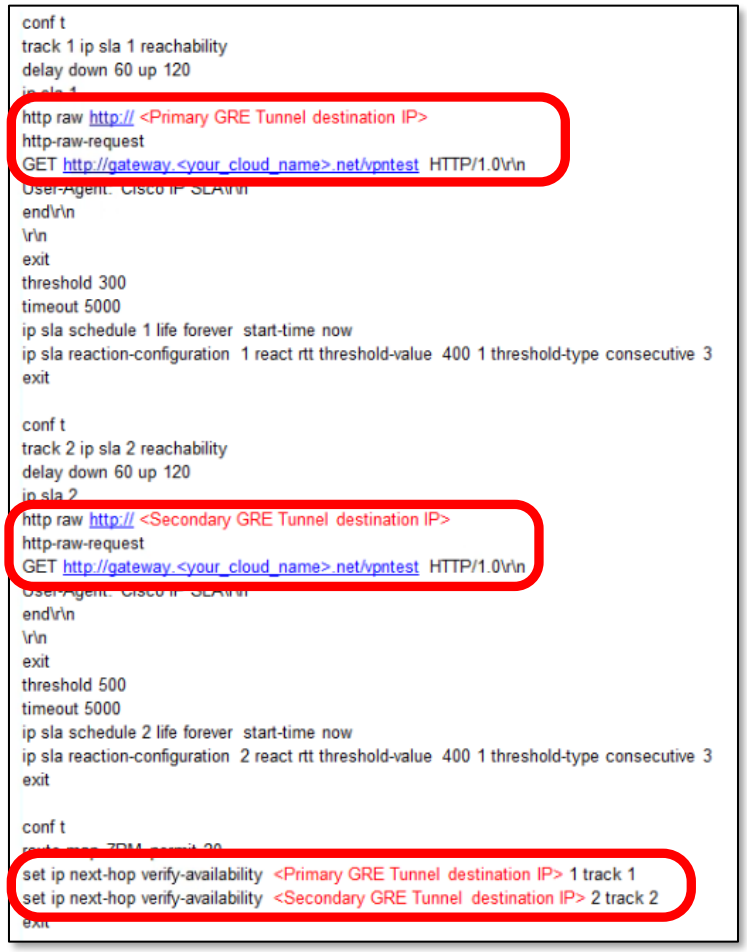
   d. Edit the **GET** request and replace **<your_cloud_name>** with your training pod Zscaler Cloud name.

      Note: There should not be any spaces in the URL. There should be a single space separating the URL from **HTTP/1.0\r\n**.

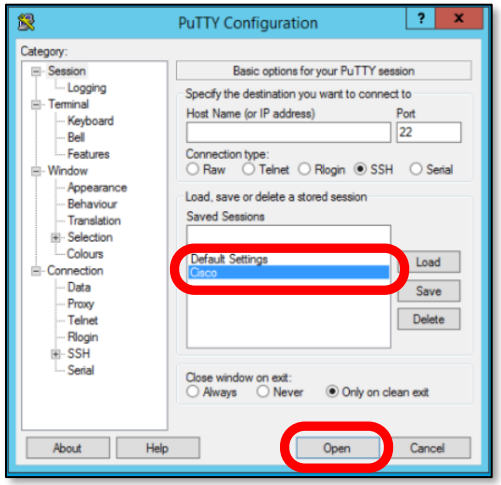
   e. In the first **set ip next-hop** line, replace **<Primary GRE Tunnel destination IP>** with the **Primary GRE Tunnel Destination** address.

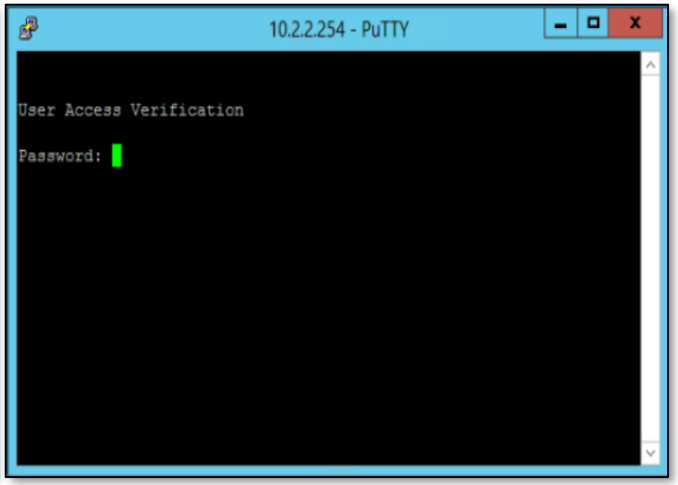
   f. In the second **set ip next-hop** line, replace **<Secondary GRE Tunnel destination IP>** with the **Secondary GRE Tunnel Destination** address.

   g. Use **CTRL-A** to select ALL, and then **CTRL-C** to copy.

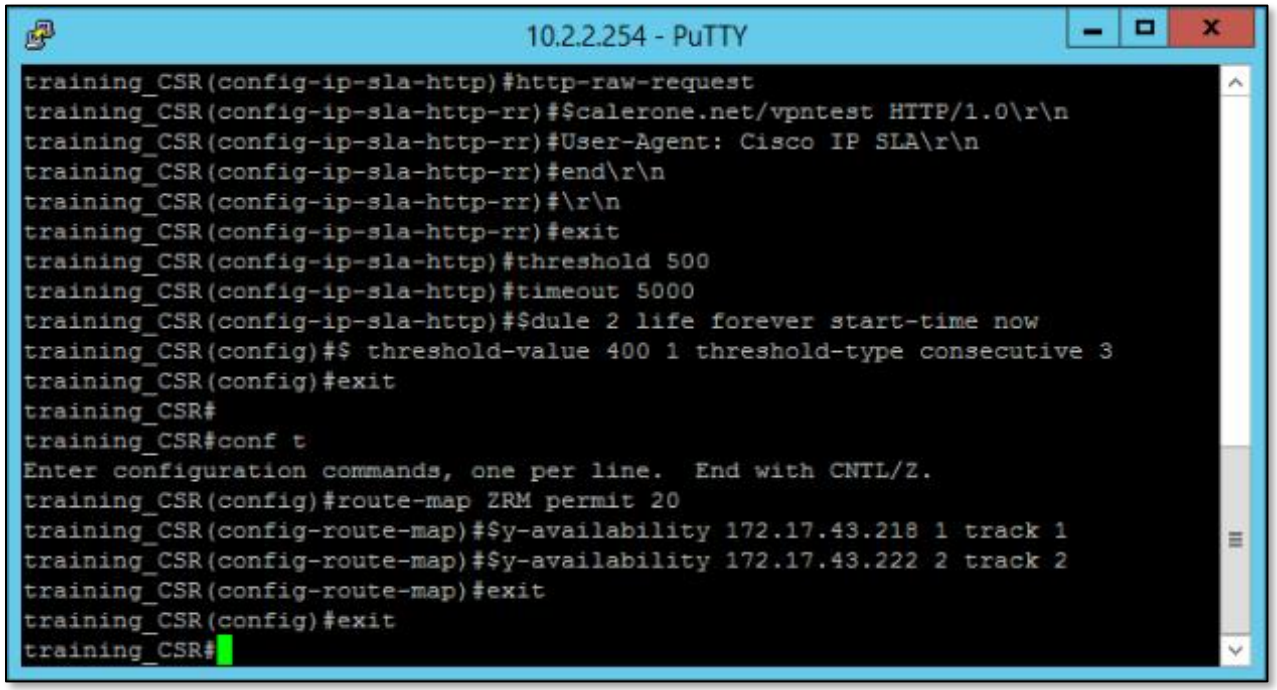


5. On the **Windows Client PC**, locate **PuTTY** on the desktop and open the Application.
6. Click to highlight and select the preconfigured **Cisco** connection.
7. Click **Open** to open the telnet session. A terminal window should open.
8. In the PuTTY terminal window, enter the **Telnet password** from the **student access sheet**.
9. Enter **`enable`** mode by typing ***`enable`***, and then enter the **enable password** from the **student access sheet.**

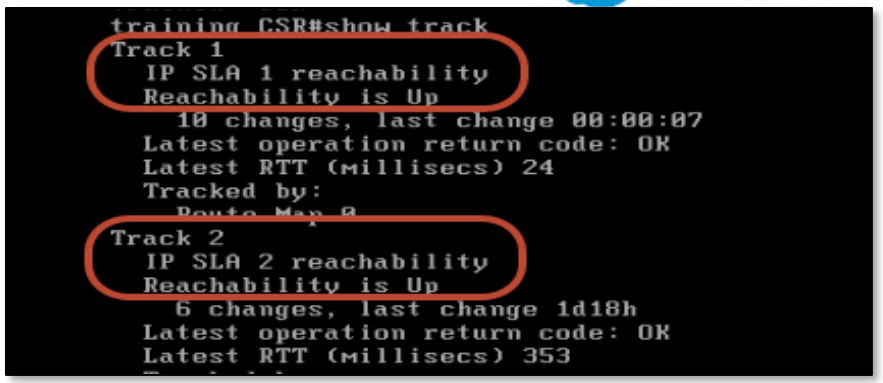




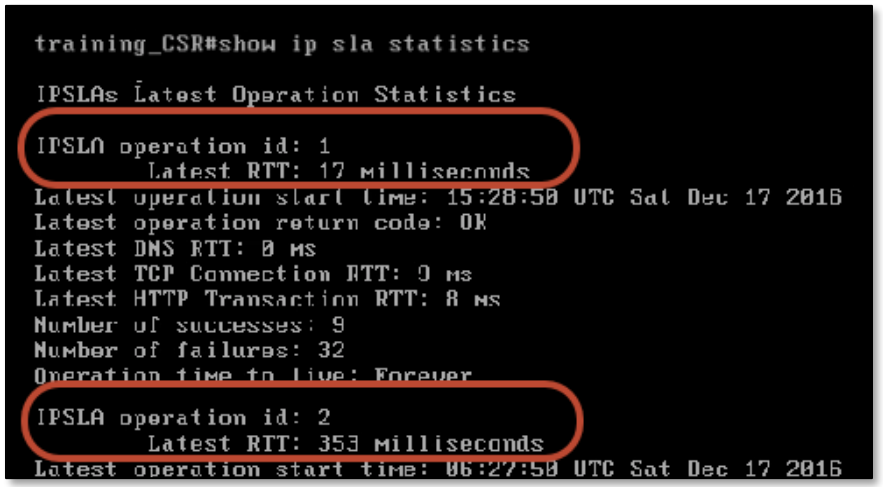
10. **Right-click** in the PuTTY terminal window to **paste** the **IPSLA** config.
Note: If you see any error messages, double check your IPSLA file for errors and try the process again. You will need to delete the previous IPSLA track configurations by going to **`conf t`** mode and using the commands **`no ip sla 1`** and **`no ip sla 2`**.



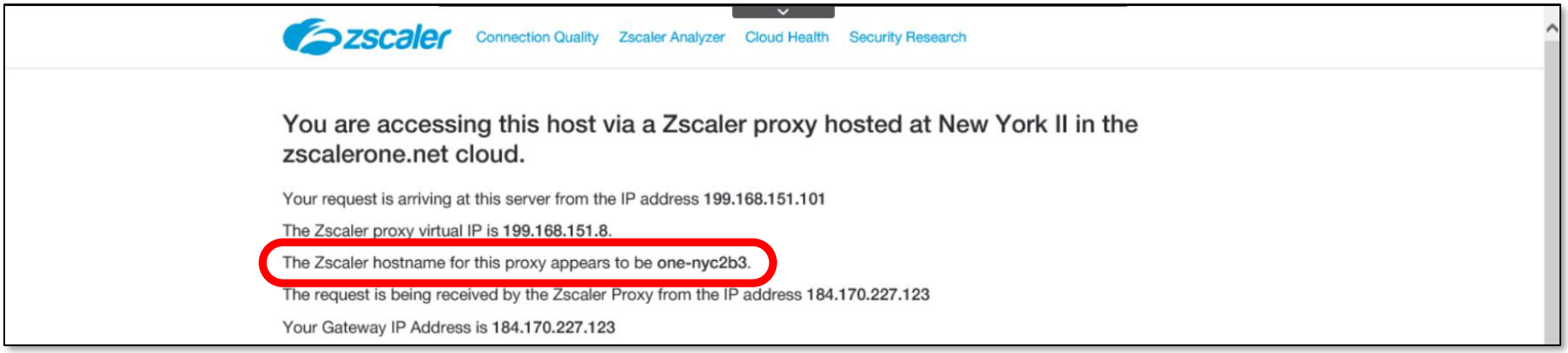
11. Exit **`Config terminal`** mode if needed by typing **`exit`**.
12. To save the running configuration to the boot configuration, enter the command **`write mem`**.
13. Check the IP SLA status by typing **`show track`**.
    - **`Track 1 reachability`** should show **`Up`**;
    - **`Track 2 reachability`** should also show **`Up`**.



14. Check IP SLA statistics by typing **`show ip sla statistics`**. Each Track should show the RTT for the GET operation. If it were to exceed the configured RTT it would trigger a failure.



15. On the **Windows Client PC** visit **http://ip.zscaler.com** and note the name of the Zscaler node the client is connected to.



16. We will now add an ACL to block web traffic in tunnel 30. This will block the GET operation for IPSLA (it will also block everything else) to simulate a network outage and trigger a failover. Enter the following commands into the PuTTY terminal session:

```
conf t
ip access-list extended BLOCKIPSLA
    deny tcp any eq www any established
    exit
exit
```

17. Add an access-group statement within Tunnel 30 that ties Tunnel 30 to the new ACL **BLOCKIPSLA**.

```
interface tunnel 30
    ip access-group BLOCKIPSLA in
    exit
exit
```

18. After a couple of minutes IPSLA will fail **Track 1**, as the website we are monitoring can no longer be reached. This will be observed via log message on the console.

19. Verify that IPSLA has triggered a failover with the following commands:

```
show track
show ip sla statistics
```

20. In a browser on the **Windows Client PC** visit **http://ip.zscaler.com** and note the name of the Zscaler node the client is connected to – it should have changed to the secondary node.

21. Initiate a failover back to tunnel 30 by removing the access-group configuration from Tunnel 30 which will allow communication with the web site IPSLA is monitoring. This will bring **Track 1** up, take **Track 2** down, and cause traffic to flow through Tunnel 30.

```
conf t
interface tunnel 30
    no ip access-group BLOCKIPSLA in
    exit
exit
```

22. After a couple of minutes IP SLA will fail **Track 2** as **Track 1** transitions back **Up**. This will be observed on the console. Verify that IPSLA has triggered a failover with the following commands:

```
Show track
Show ip sla statistics
```

23. Save your **Cisco** configuration by typing **write mem**.
24. In a browser on the **Windows Client PC** visit **http://ip.zscaler.com** and note the name of the Zscaler node the client is connected to – it should have changed back to the primary node.
25. Close the file named **IPSLA_config** and save changes.

Lab 7: Zscaler Best Practice: SSL Inspection

More and more web traffic is moving to SSL. If your organization is not inspecting SSL traffic, you are blind to massive amounts of data and potential threats. Zscaler Best Practice is to enable SSL Inspection.

Note: You have already installed the **Zscaler Root CA Certificate** onto the **Windows Client PC** in Lab 2, when you installed the Zscaler App. This certificate can also be installed automatically on client PCs using an AD GPO. Also note that for Windows devices it must be installed in the system certificate store under **Trusted Root Certification Authorities** and also in the Firefox certificate store, Zscaler App will do this for you automatically by default.

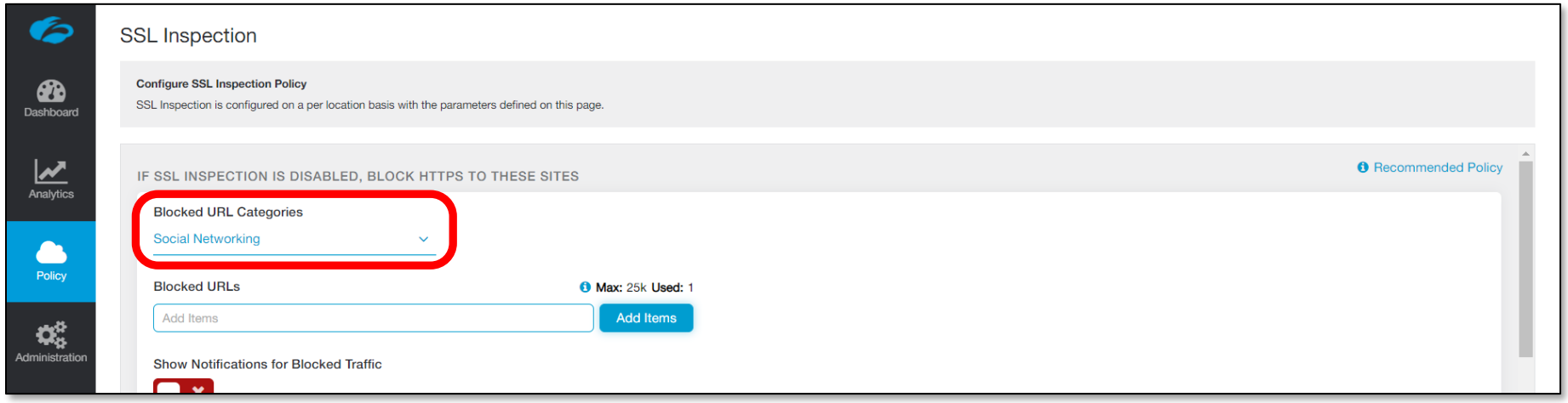
Blocking SSL traffic if SSL Inspection is disabled

It may be necessary to modify the SSL Inspection policy, even though you do not plan to enable SSL Inspection! In the SSL Inspection policy, you have the option of adding URLs or URL categories to be blocked even though SSL Inspection is not enabled. This is basically an SSL Inspection blacklist. In this section, you will configure the SSL Inspection policy, before you enable SSL Inspection. The policy will simply block access attempts to the **Social Media** URL category over SSL.

1. On your **Windows Client PC** open a browser and visit **http://www.facebook.com**. You will see that this site uses SSL and the traffic is allowed.
2. Begin by setting policy to block traffic by URL category that is attempting to use SSL:
    a. In the **Zscaler Admin Portal**, go to the **Policy > Web > ACCESS CONTROL > SSL Inspection** page;
    b. In the **IF SSL INSPECTION IS DISABLED, BLOCK HTTPS TO THESE SITES** section, select the **Blocked URL Categories** drop-down, scroll down to the **Society and Lifestyle** category then select **Social Networking**;

        Tip: You can also type social networking in the search bar.

    c. Click **Done**, then **Save** (at the bottom of the page), then **Activate** your changes.



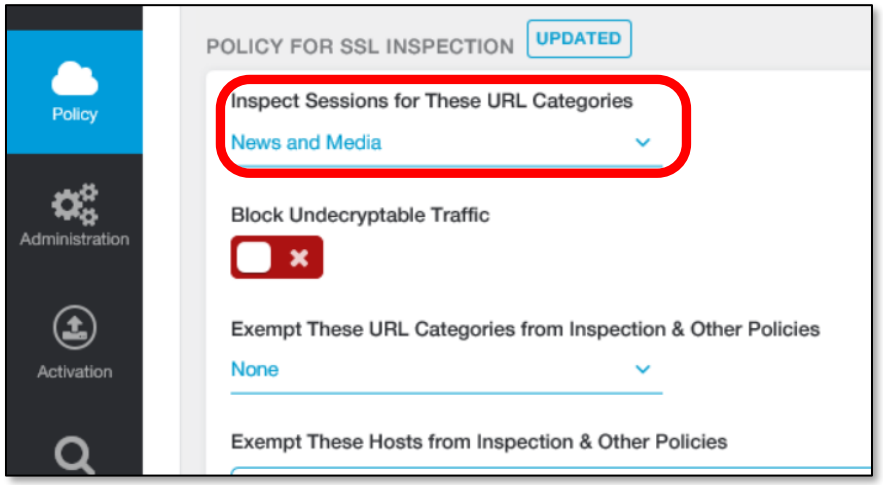
3. On your **Windows Client PC** in the browser visit **https://www.facebook.com** again. You will see that the connection could not be established. We are now blocking **Social Networking** sites that are using SSL, as we currently do not have the ability to inspect the traffic. This is coming in later steps.

Enabling SSL Inspection for specific destinations

In this section, you will enable SSL Inspection for your **Location** and for **Mobile** users, but for specific destinations only.

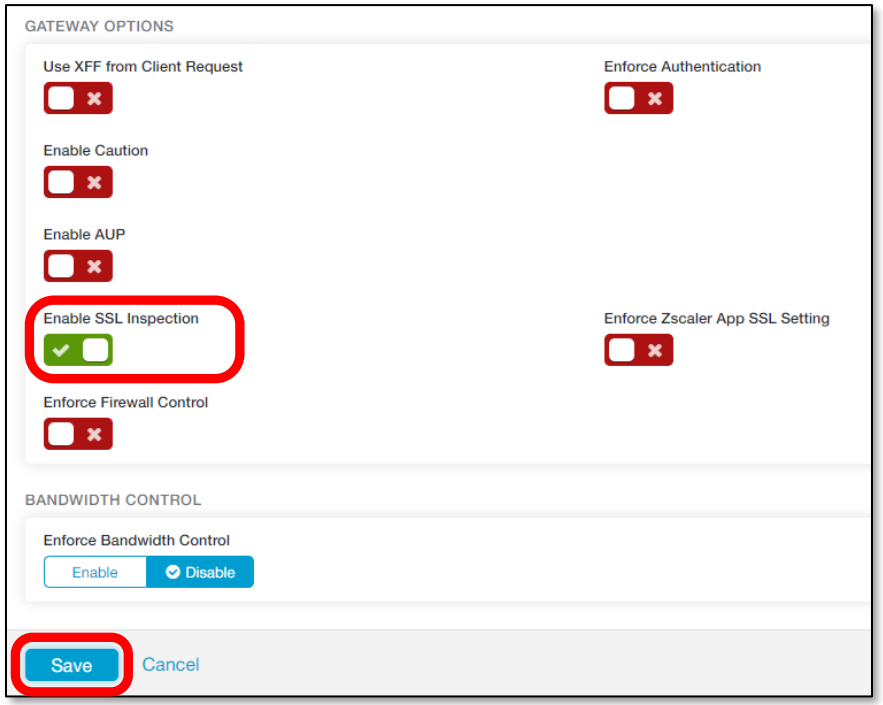
4. On your **Windows Client PC** open a browser and visit **https://www.cnn.com**.
5. Click the **lock icon** in the URL field, then click **View Certificates**. You will that you have received the certificate from the destination Web server.

   Note: To view the site's certificate in Chrome, go to the **Settings > More Tools > Developer Tools > Security** page.
6. Now, configure the **SSL Inspection Policy** to SSL Inspect traffic for a specific **URL Category**:
   a. In the **Zscaler Admin Portal** go to the **Policy > Web > ACCESS CONTROL > SSL Inspection** page;
   b. In the **POLICY FOR SSL INSPECTION** section, click in the **Inspect Sessions for these URL Categories** field, then click **Clear Selection**.
   c. Then click in the **Search** field and type **news**.
   d. Select the **News and Media** category, then click **Done**.
   e. Scroll down to the **POLICY FOR Z APP** section and enable the **Windows** option;
   f. Click **Save** at the bottom of the page, then **Activate** your changes.

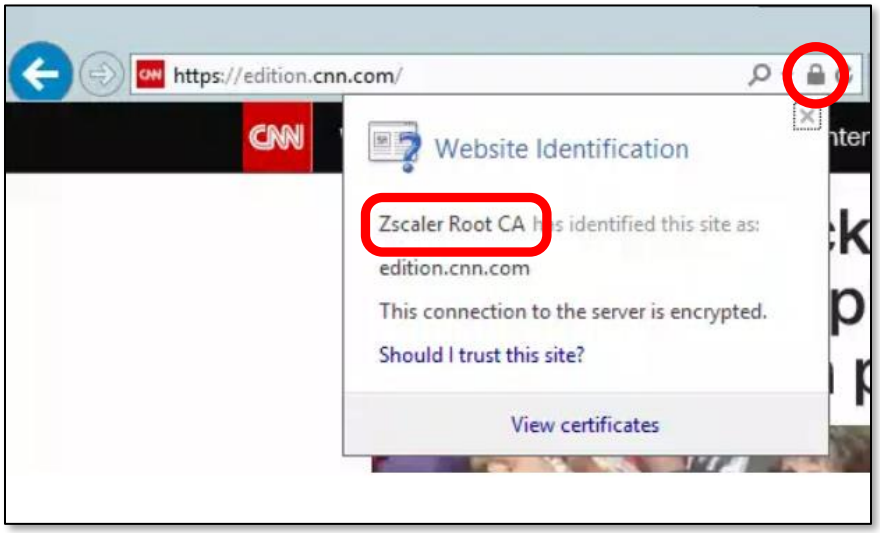


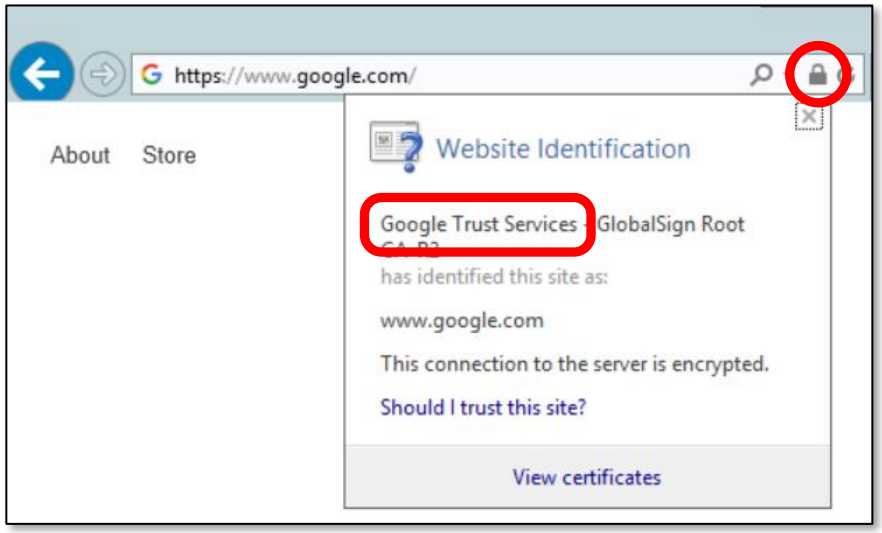
7. Now enable SSL Inspection for your Location:
   a. Go to the **Administration > Resources > TRAFFIC FORWARDING > Location Management** page;
   b. **Edit** the location you created previously.

      Note: This will be either be **Site_1_IPSec** or **Site_1_GRE** depending on which Tunneling lab you did last.
   c. Scroll down to the **GATEWAY OPTIONS** section and click **Enable SSL Inspection**, then click **Save** and **Activate** your changes.



8. Verify Inspection status:
    a. On your **Windows Client PC**, close the browser, then re-open it and load **https://www.cnn.com**.
    b. Click the **lock icon** in the URL field then click **View Certificates**. You will see that you have received a server certificate signed by Zscaler.
    c. Load a page that does not belong to the **News and Media** URL Category, e.g. **https://www.google.com**.
    d. Click the **lock icon** in the URL field then click **View Certificates**. You will see that you have received the server certificate from the destination server (it is NOT signed by Zscaler).



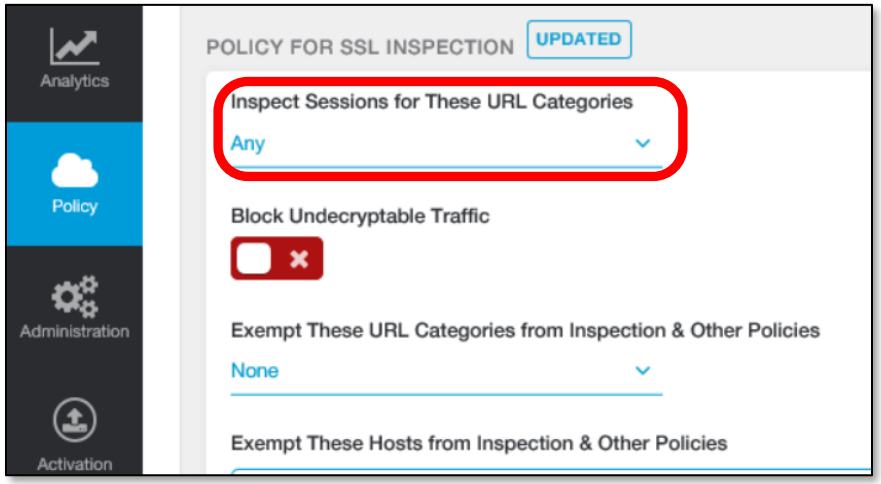


Enabling SSL Inspection for ALL destinations

In this section, you will enable SSL Inspection for your Location and for Mobile users, for ALL destinations.

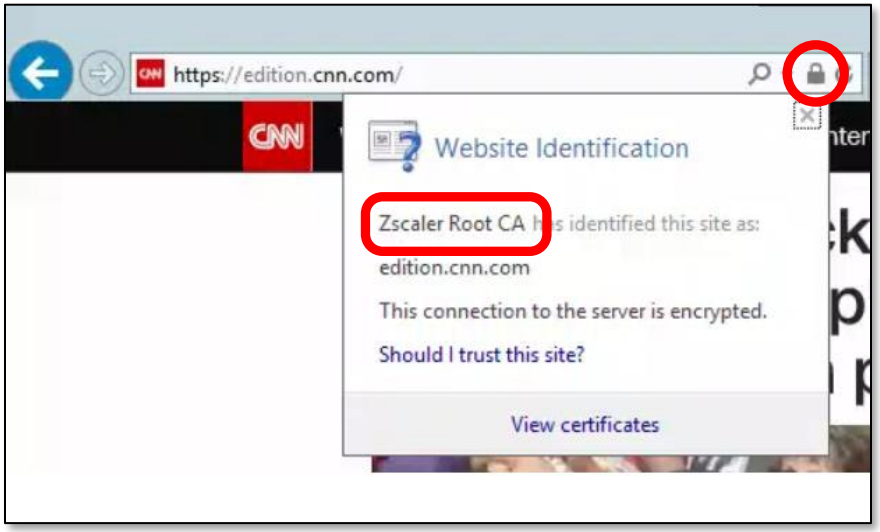
9. Configure the **SSL Inspection Policy** to SSL Inspect traffic for all destinations:
    a. In the **Zscaler Admin Portal** go to the **Policy > Web > ACCESS CONTROL > SSL Inspection** page;
    b. In the **POLICY FOR SSL INSPECTION** section, click in the **Inspect Sessions for These URL Categories** field and remove the **News and Media** category and click **Done**.

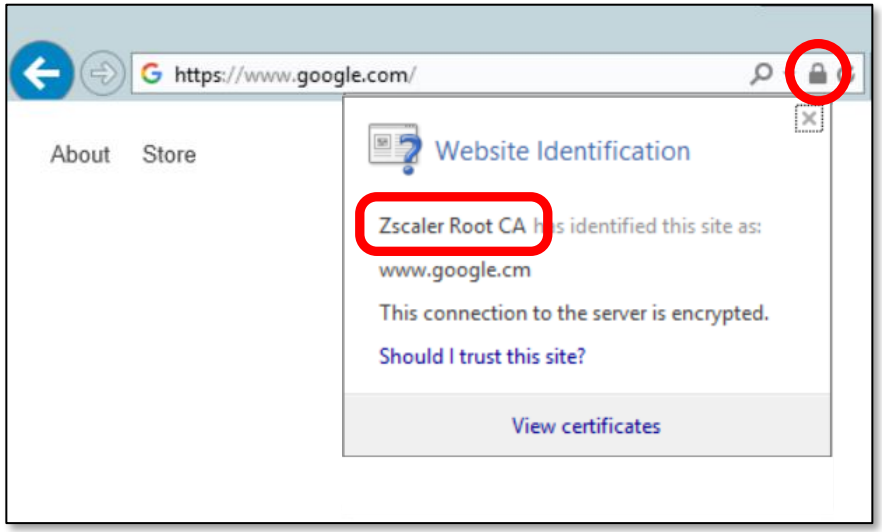
    Note: This field should now show **Any**.
    c. Click **Save** at the bottom of the page, then **Activate** your changes.



10. Verify Inspection status:
    a. On your **Windows Client PC**, close the browser, then re-open it and load any page requiring **HTTPS**.
    b. Click the **lock icon** in the URL field then click **View Certificates**. You will see that you have received a server certificate signed by Zscaler.

    Note: You should now also be able to reach **https://www.facebook.com** now that SSL Inspection has been enabled for all destinations.

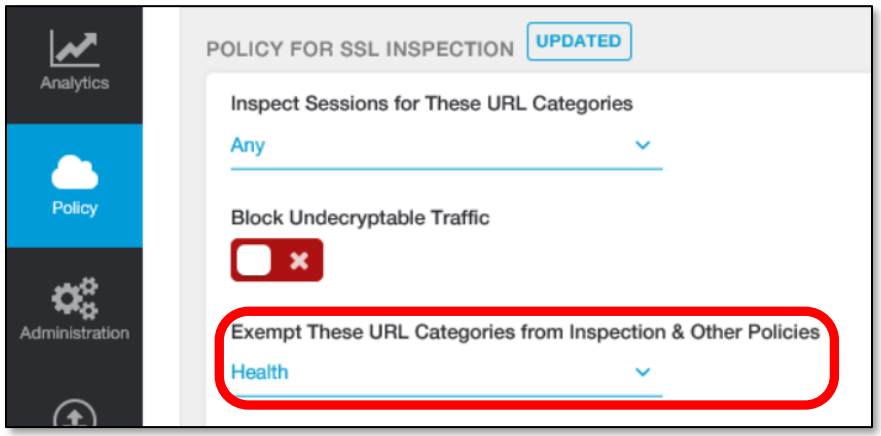




Enabling an SSL Exemption

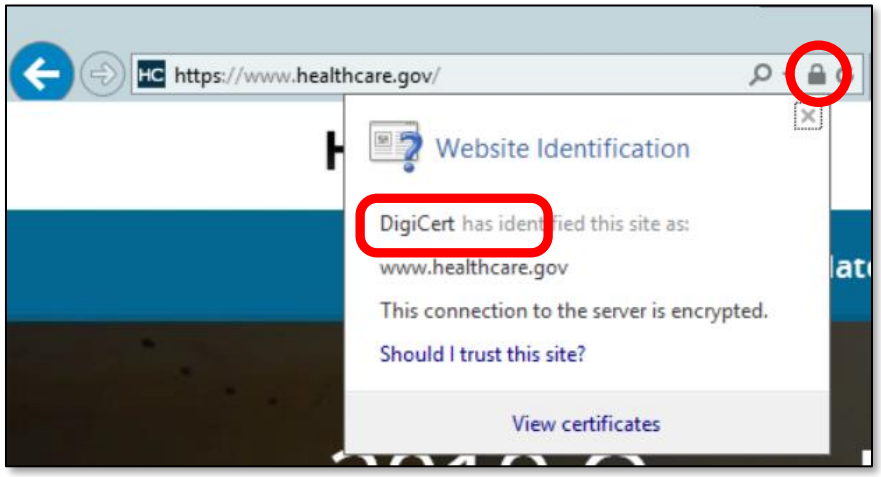
To ensure your user's privacy when visiting certain types of websites such as Healthcare and Financial sites you may wish, or even be required by local regulations, to block SSL Inspection for those websites.

11. In a browser on your **Windows Client PC** go to the page **https://healthcare.gov**. Check the certificate and you will see that it is issued by Zscaler, as Zscaler is now inspecting all SSL traffic.
12. Enable SSL Bypass for the **Health** URL Category:
    a. Go to the **Policy > Web > ACCESS CONTROL > SSL Inspection** page;
    b. In the **POLICY FOR SSL INSPECTION** section select the **Exempt These URL Categories from Inspection & Other Policies** drop-down and search for and select **Health**;
    c. Click **Done**;
    d. Click **Save** at the bottom of the page, then **Activate** your changes.



13. Refresh the page on **https://healthcare.gov** and view the certificate information again. You will see that the certificate is not issued by Zscaler as Zscaler did not intercept this traffic.

    Note: It is important to either refresh the page, or close the browser and re-open it, in order to re-initialize the connection and load the server certificate.



Lab 8: User Authentication: SAML with Okta

As discussed in the Authentication section of ZCCP-IA, there are two components to User Authentication – User Provisioning and User Authentication. Users must be provisioned in the Zscaler database before authentication can occur. There are several methods of provisioning users into the Zscaler DB: Manual creation in the Admin Portal; Import of a .csv; AD / LDAP sync; SAML Auto-Provisioning or with the SCIM protocol.

During this lab, you will configure Zscaler to authenticate users via SAML. In this example, we will use Okta as our Identity Provider (IdP), with Auto-Provisioning to allow the automatic addition of a new user to the Zscaler DB. For the purpose of this lab AD has been pre-configured.

There are three components to configure to enable SAML with Okta: The Okta AD integration agent on the AD server; Zscaler authentication; And the Okta service.

Okta Active Directory Integration Agent

The Okta Active Directory Integration Agent provides a communication path between Okta and Active Directory. Once installed, the agent securely establishes a connection with your Okta instance for synchronization – no network or inbound firewall configuration is required.

1. Log into your **Windows 2012 Server** and open a web browser. Log into the **Okta Admin Portal** using the information from the student access email that you received.

   Note: You must do this from the Windows 2012 server, as that is where you must sync your AD users from.

2. Mouse over the **Directory** tab then, from the drop-down, select **Directory Integrations**.
3. Under **Directory Integrations** click the **Add Directory** button and select **Add Active Directory**.
4. Run the setup wizard by clicking the **Set Up Active Directory** button near the bottom of the page.
5. Download the Okta **Active Directory Agent** by clicking the **Download Agent**. Save the file to the Windows server.
6. Note the values in **Section B** of the Okta web page. You will need the **Okta administrator account** information for use in a later step.

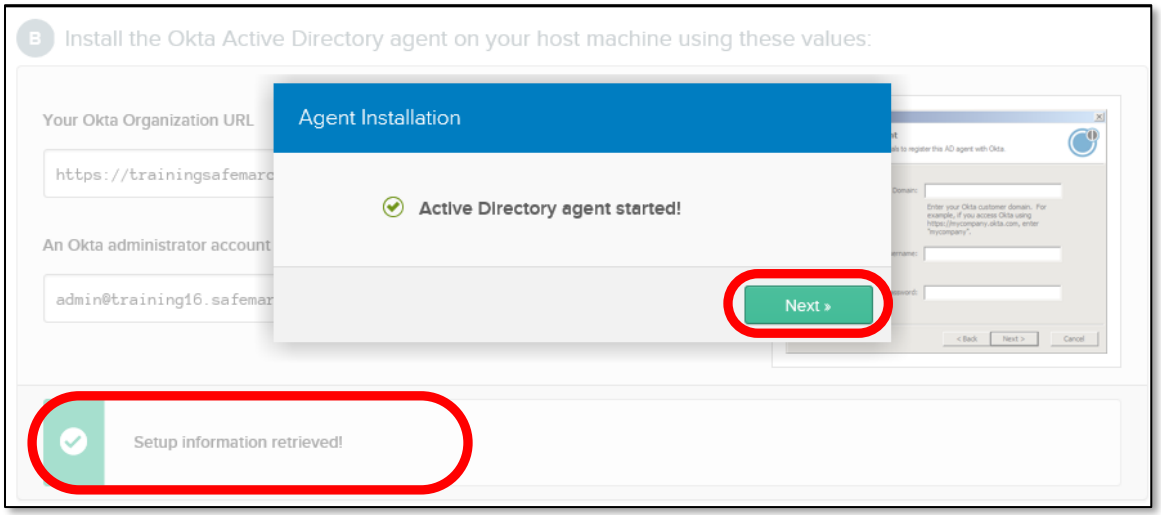
   Note: Okta best practice is to create a User in the Okta directory for the Okta AD Agent that will not be managed in AD. For this lab, you will use the **Okta Administrator account (admin@training[1-N].safemarch.com**), as this account has already been created for you.

7. Run the Okta **Active Directory Agent** installer to install it on the AD server and establish a persistent outbound TCP connection to Okta:
   a. Locate the installer (**\Downloads** folder) and double-click it to run it. Click **Next >** at the welcome screen.
   b. At the **Installation options** step, accept the default install folder and click **Install**.
   c. Verify the correct **Domain** is identified and auto-populated (**training[1-N].safemarch.com**) then click **Next >**.
   d. At the **Okta AD Agent Windows Service Account** step, use the default **Create or use OktaService account** and click **Next >**.
   e. Provide a password (use **Admin-123!**) then click **Next >**.
   f. Accept the defaults for the **Okta AD Agent Proxy Configuration** and click **Next >**.
   g. At the **Register Okta AD Agent** step, select **Production** and type **trainingsafemarch[1-N]** in the **Enter Subdomain** field (remember to substitute your student number), and click **Next >**.

      Note: Typically, this would be pre-selected by your IT administrator when creating the Okta account. For the purpose of this lab, this has already been done.

h. At the **Sign into Okta with agent service account** step, log in using the **Okta Administrator Account** (**admin@training[1-N].safemarch.com**) and the password from the student access email that you received.
i. Click the **Allow Access** button to allow the Agent to communicate with the Okta service API.
j. Click **Finish** to exit the installer.

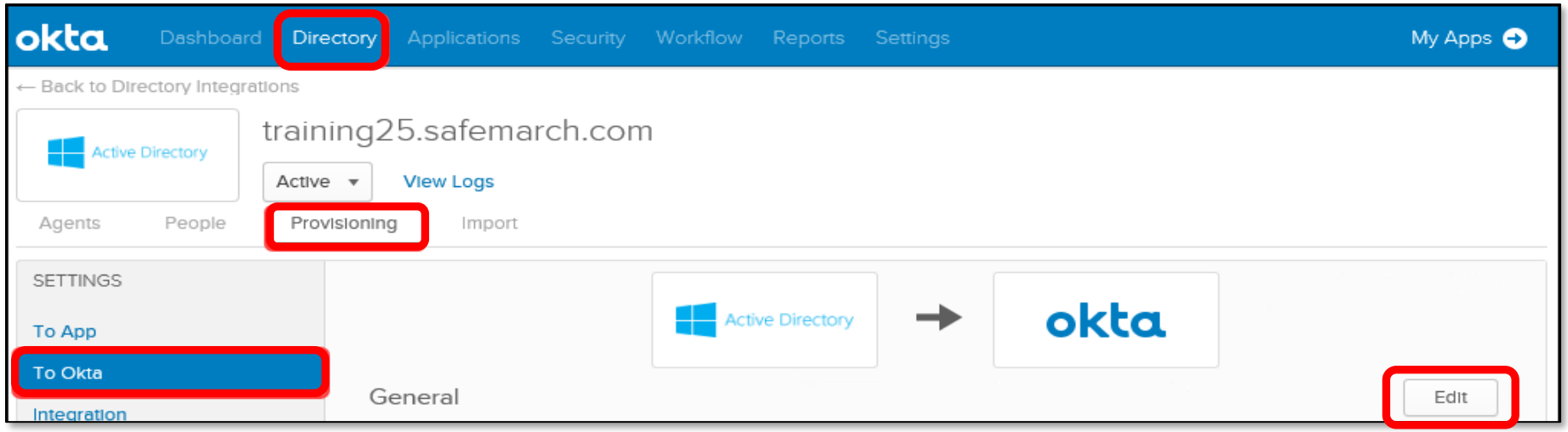
8. Back on the **Okta Admin Portal**, confirm that the dialog box near the bottom of the screen in the background (greyed out) states **Setup information retrieved!** and that the **Agent Installation** dialog box in the foreground states **Active Directory agent started!** Click **Next >**.



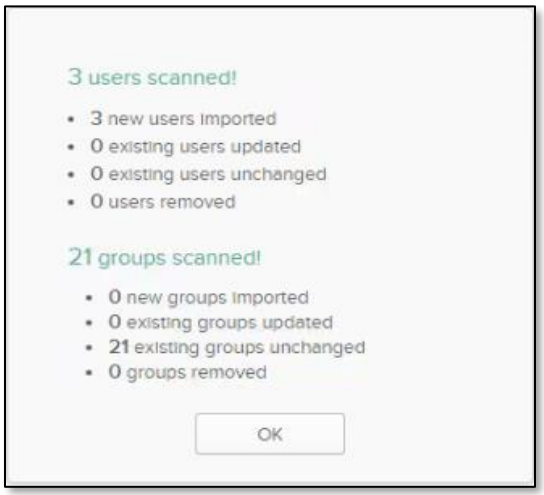
9. The setup wizard should now take you to **Step 2 – Basic Settings**. Be sure your **Organization Unit (OU)** has been automatically selected. Change the **Okta username format** at the bottom of the page to **Email address** then click **Next >**.
10. You should see a dialog box stating, **Active Directory agent configured!** Click **Next >**.
11. There is no need to select additional attributes, so click **Next >** to the right of the **Refresh Attribute List** button.

12. Click **Done** to complete the AD integration portion of the Okta config.

13. While still on the **Active Directory** > **Provisioning** tab, under Settings, click **To Okta**.



14. In the **General section** click the **Edit** button to the right of the page.
15. Select the **Okta username format drop-down** and select **Email Address**.
16. Scroll down to **Activation emails option** and check **Don't send new user activation emails for this domain**.
17. Click **Save**.
18. Under the User **Creation & Matching** section click **Edit.**
19. In the **Confirm matched users** section enable **Auto-confirm exact matches**. In the **Confirm new users** section enable **Auto-confirm new users** and **Auto-activate new users**. Click **Save** .



Okta User account import and provisioning

Now that you have a new user account created, go back to your Okta Admin Portal to complete the Okta configuration.

20. To avoid waiting for Okta and AD to automatically synchronize we will manually import users:
    a. Click on the **Import** tab at the top of the screen;
    b. Click the **Import Now** button;
    c. Select **Full Import**, then click **Import**;
    d. Review the summary pop-up information and click **OK**.

    Note: On import, new users will be automatically confirmed and activated, so that their accounts can immediately be used.

Adding Applications to SSO

Once applications, or Services, are added and configured, any user authenticated against Okta will be automatically logged into the Application. To enable SSO, Zscaler is treated as an application by Okta.

21. Click the **Applications** tab near the top of the screen, then click **Add Application**.
22. Near the top of the page select **Add Zscaler 2.0**.
23. You are now taken to the **General Settings** section, configure these settings as follows:
    a. Leave the Application Label as **Zscaler 2.0**;
    b. In the **Your Zscaler Domain** window, set the Zscaler domain based on your assigned cloud name.
    Note: During this lab, your assigned cloud name is the name in the URL to access the Zscaler Admin UI. for example:
    - https://admin.**zscalerone**.net -> **zscalerone**.net
    - https://admin.**zscalertwo**.net -> **zscalertwo**.net

    c. Click **Next**.

24. You are now taken to the **Sign-On Options** section, configure these settings as follows:
    a. Select **SAML 2.0**;
    b. Click the **View Setup Instructions** button;
    c. On the Okta Instructions page, scroll down to **Step 6**. Then click the link under **Public SSL Certificate** to download the **okta.pem** certificate for installation on the Zscaler Admin Portal later. **Save** the certificate to the AD server;

    Note: Keep this browser tab open in the background for reference later in the lab. Make a mental note of **Step 6** on this page for later use.

    d. Go back to your main Okta browser tab and, under **CREDENTIALS DETAILS**, select the **Application username format drop-down** and select **Email**.
    e. Click **Done** at the bottom of the page.

Complete the Configuration in the Zscaler Admin Portal

In this section, you will configure authentication in the Zscaler Admin Portal to use SAML and Okta as the IdP.

25. Go to your **Zscaler Admin Portal** browser tab and go to the **Administration > Authentication > Authentication Configuration > Authentication Settings** page.
26. On the **Authentication Profile** tab, set the **Directory Type** to **Hosted DB**.
27. For **Authentication Type** select **SAML** then click **Save**.

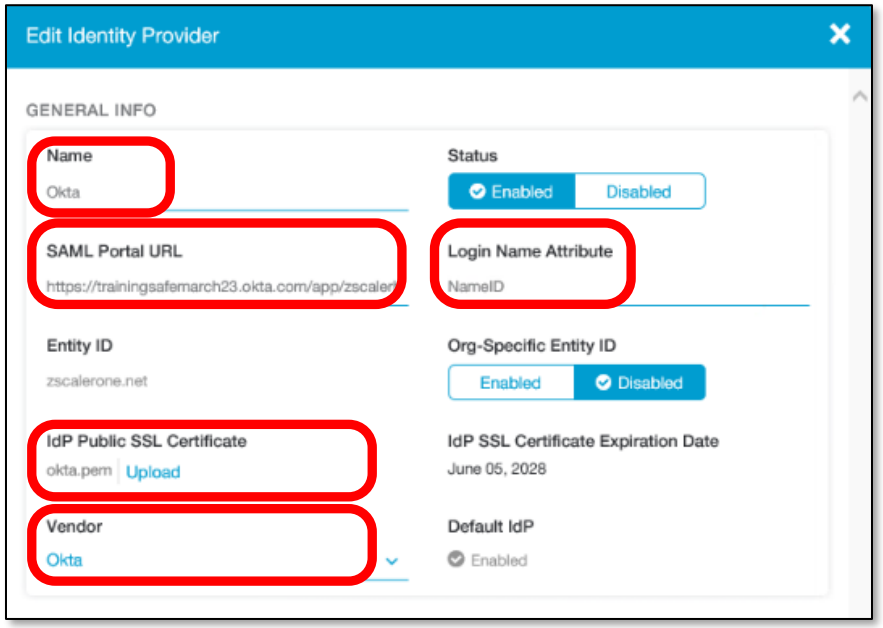
28. Click **Open Identity Providers** or click on the **Identity Providers** tab.
    a. Click the edit icon to the right of the **Default** IdP profile
    b. Change the Name to **Okta**.
    c. Set the **Status** to **Enabled**.
    d. Paste in the **SAML Portal URL** from Okta.

    Note: This is found on the Okta Setup SSO instructions in the browser tab you kept open in previously. Copy and paste the **SAML Portal URL** found on the Okta page (Step 6).

    e. In the **Login Name Attribute** field, type **NameID** (this came from the Okta instructions page Step 6).

    Note: This is case-sensitive.

    f. To upload the **Public SSL Certificate** you obtained from Okta previously (**okta.pem**), click **Upload**. Browse to the file location on the **Windows 2012 Server** (**\Downloads** folder), and then click **Upload**.
    g. From the **Vendor** dropdown list, select **Okta**.
    h. Under the **AUTO-PROVISIONING OPTIONS** section, select **Enable SAML Auto-Provisioning**.



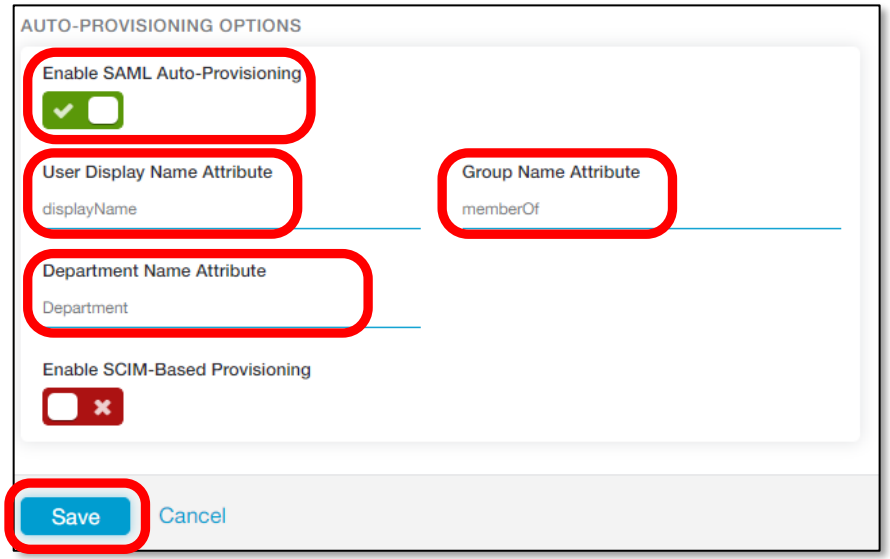
29. Once Auto-Provisioning is enabled, additional options will become visible. Configure the following:
    a. In the **User Display Name** Attribute field, enter **displayName**;

    b. In the **Group Name** Attribute field, enter **memberOf**;

    c. In the **Department Name** Attribute field, enter **Department**.

    Note: These are all case sensitive.

30. Click **Save**.
31. **Activate** your changes.



Assign the Zscaler Application to Users in Okta

Having added and configured the Zscaler Application in Okta, it is necessary to assign it to the users who require it. The assignment can be done either for individual users, or and more usefully for a complete group of users. In this Lab you will assign the Application to a Group.

32. AD users that will authenticate to Zscaler via Okta need to be assigned to the Zscaler App within Okta. The most common way to do this is using **AD Groups**:
    a. In the Okta Admin Portal click on the **Assignments** tab;
    b. Click the **Assign** button, and select the **Assign to Groups** option;
    c. You then select your AD Groups that contain users who will be using Zscaler. For this lab, we will assign the groups called **Marketing.** Enter **Marketing** in the search box;
    d. Click the **Assign** button next to the Windows Group **Marketing**;

       Note: If there is more than one group, use the group associated with your domain.

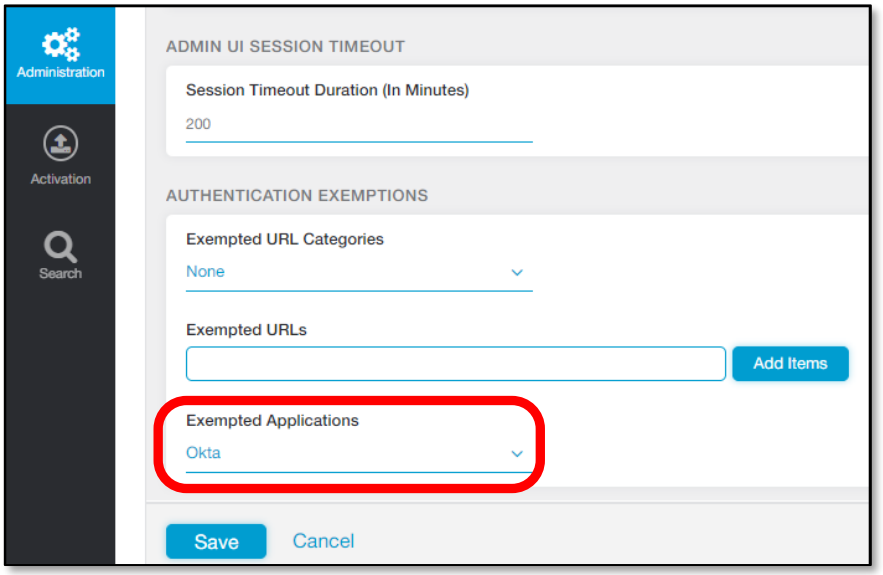
    e. Then click **Done**.

Add Authentication Exception for the Okta Application in the Zscaler Portal

The last item to configure is a bypass for the Okta authentication traffic. Remember from the eLearning that the client receives a web-redirect from Zscaler to Okta for authentication. However, since the client has not yet authenticated no web traffic for the user will pass so the redirect fails. A Bypass can be set in the browser PAC file; however, since this lab is tunneling traffic you will set the bypass in the Zscaler Admin Portal.

The bypass for the authentication traffic can be accomplished by enabling **Authentication Exemptions** which bypass the authentication traffic for the specified IdPs. This can be configured in one of three ways: Exempting **URL Categories** (Internet Services); By manually adding **Exempted URLs** (for the Okta service (**.okta.com** and **.oktacdn.com**); Or by selecting **Exempted Applications**.

The **Exempted Applications** option is a **One Click** configuration and automatically bypasses the required URLs for known Authentication services. For this lab you will configure **Exempted Applications**, in the ADFS lab (Lab 9) you will use **Exempted URLs**.



33. In the **Zscaler Admin Portal**, go to the **Administration > Settings > Cloud Configuration > Advanced Settings** page.
    In the **Authentication Exemptions** section under **Exempted Applications**, select **Okta** then click **Done**.

34. Click **Save**, then **Activate** your changes.

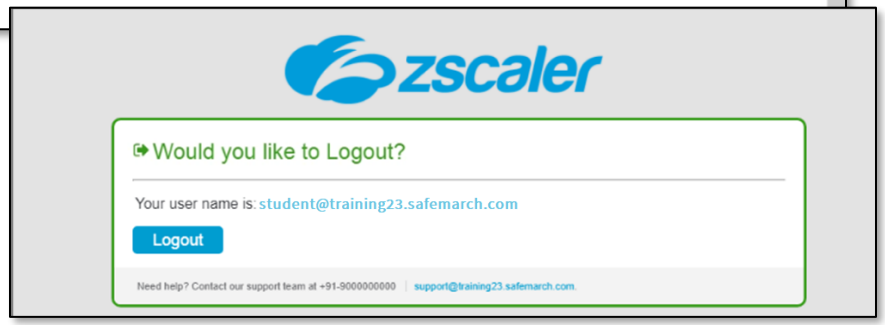
Testing the SAML Configuration

Configuration of the SAML solution is complete and you will now test your work. Up to this point, we have not required authentication coming from known locations (the GRE and IPSec tunnels). We need to enable the Enforce Authentication option on the Location which will trigger the authentication process anytime an unauthenticated user attempts to go out to the Internet.

35. In the Zscaler Admin Portal go to the **Administration > Resources > Traffic Forwarding > Location Management** page.
36. Edit the location you created in Lab 5 (**Site_1_GRE**), and under the **Gateway Options** section enable **Enforce Authentication**.
37. Optional, but a Zscaler Best Practice: click **Enable IP Surrogate**.

    Note: This enables User-to-Device mappings when the internal IP address of the device can be distinguished from the public-facing IP, which is the case in this lab as you previously disabled NAT on the Cisco. This is used to enforce User-level policies on devices that are not cookie compatible. Without it the cookie incompatible device would be limited to a Location-level policy only.
38. Click **Save**, then **Activate** your changes.
39. In the lab environment go to your **Windows Client PC**. Open a browser and visit any website, you should be redirected to the Okta SSO portal. Log in using **student@training[1-N].safemarch.com** with the password **Admin-123!** Once authentication completes you should automatically be redirected to your original URL request.

40. Now that your **Windows Client PC** has authenticated against the service go to **http://ip.zscaler. com**. The status window now shows the user name indicating that authentication was successful.



Lab 9: User Authentication: SAML with AD FS

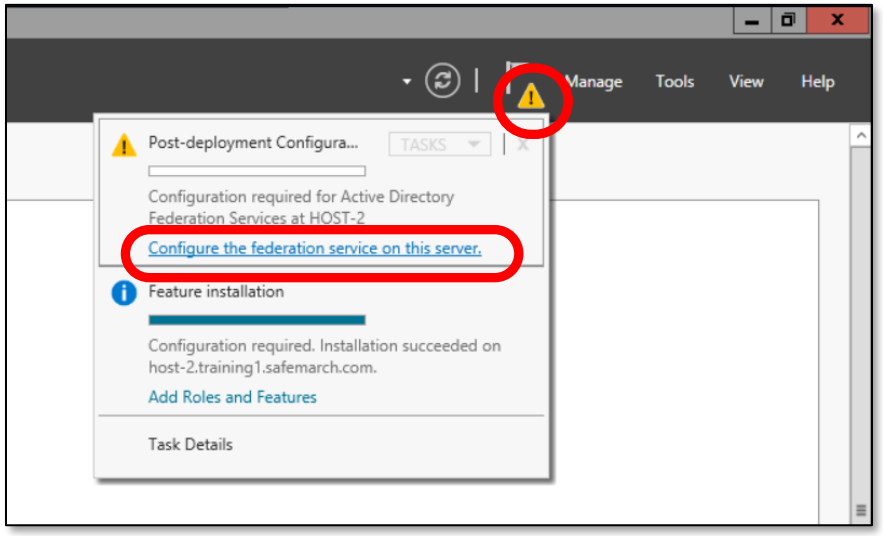
In this lab, you will authenticate users using SAML against the local Active Directory Domain Controller with Federation Services installed. AD Directory Services have been pre-configured for you, as have Certificate Services. The Root CA certificate for the CA has been pre-installed on the Windows Client PC. This lab demonstrates enabling Active Directory Federation Services on top of your existing AD configuration, configuring Zscaler for an AD FS IdP, and authenticating users.

Add and Configure AD Federation Services

AD Directory Services and Certificate Services are already installed and configured on the Windows Server 2012 VM. In this section, you will install and configure AD Federation Services.

1. To add AD Federation Services, on the **Windows 2012 Server**:
    a. From the Server Manager, select **Manage > Add Roles and Features**, and click **Next >**;
    b. At the **Installation Type** step, accept the default **Role-based or feature-based installation** and click **Next >**.
    c. At the **Server Selection** step, select the Windows server you would like to configure (there is only the one) then click **Next >**.
    d. At the **Server Roles** step, select **Active Directory Federation Services** then click **Next >**.
    e. At the **Features** step, accept the default features and click **Next >**.
    f. At the **AD FS** step, click **Next >**.
    g. At the **Confirmation** step, select **Restart the destination server automatically if required** then click **Yes**, then **Install**.
    h. When the configuration is successful click **Close**.

2. To configure AD FS:
    a. Click the **notifications flag** in the upper right corner. Then click **Configure the federation service on this server**;



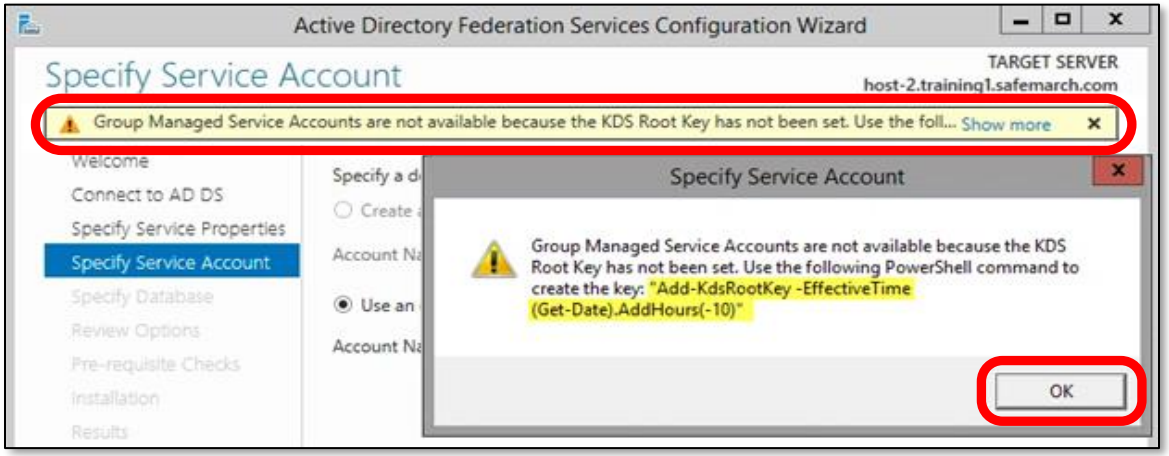
    b. At the **Welcome** step, ensure the default **Create the first federation server in a federation server farm** option is selected and click **Next >**;

    c. At the **Connect to AD DS** step, accept the defaults for the domain administrator and click **Next >**;

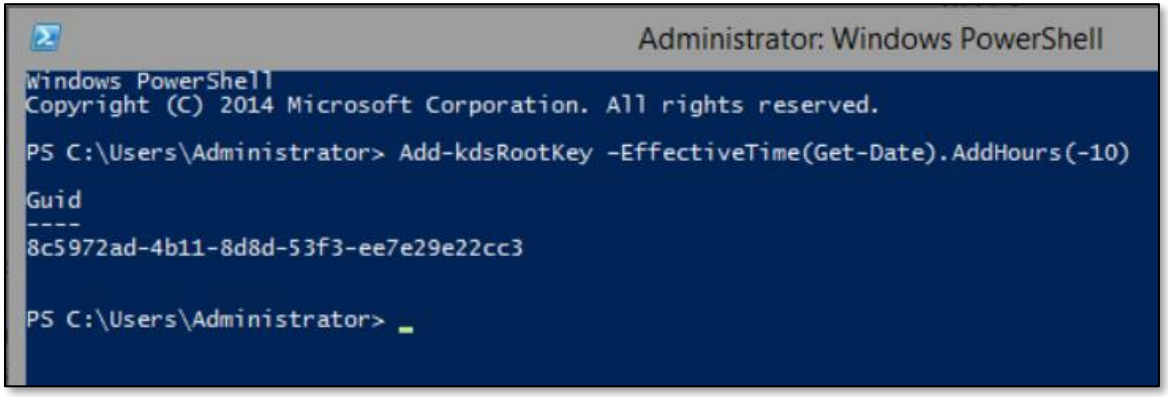
    d. At the Specify **Service Properties** step, click in the **SSL Certificate** field, and select the certificate from the drop-down list. Set the **Federation Service Display Name** to **training[1-N]_ADFS**;

    e. Then click **Next >**;

f. At the **Specify Service Account** step, click **Show more** on the alert, and note the CLI syntax you will need to run in Windows PowerShell;



g. Open **Windows PowerShell** using the Status Bar icon and type **`Add-kdsRootKey –EffectiveTime(Get-Date).AddHours(-10)`**, and once the command has executed close PowerShell;



h. Click **OK** to close the **Specify Service Account** notice. In the next step, you want to select **Create a Group Managed Service Account**, however it is currently greyed-out as it was unavailable until you ran the PowerShell command. Press **Previous**, then **Next**, and now select **Create a Group Managed Service Account**, type **ADFS** in the **Account Name** field, and click **Next >**;

i. At the **Specify Database** step, accept the default **Create a database on this server using Windows Internal Database** option and click **Next >**;

j. At the **Review Options** step, review your selections and click **Next >**;

k. At the **Pre-requisite Checks** step, if all prerequisite checks passed, click **Configure**. Once configuration completes, click **Close**.

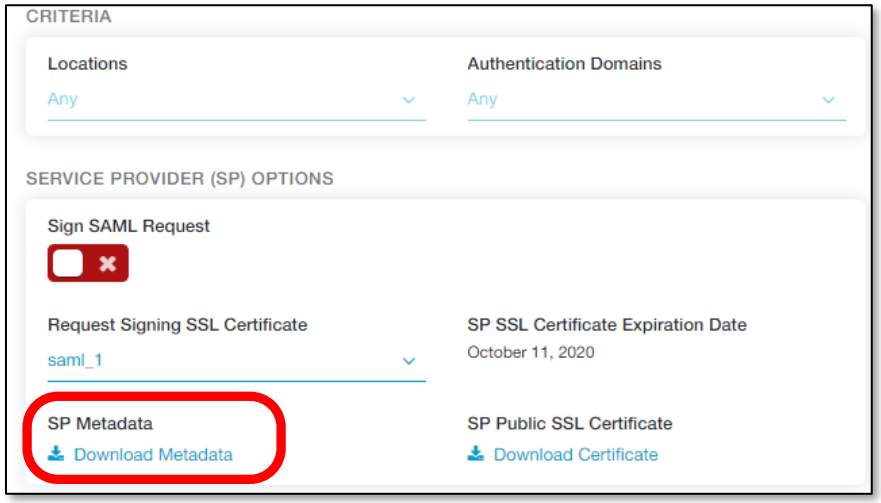
Note: You can ignore the warning messages.

Export Zscaler Metadata and Add a Relying Party Trust to AD FS

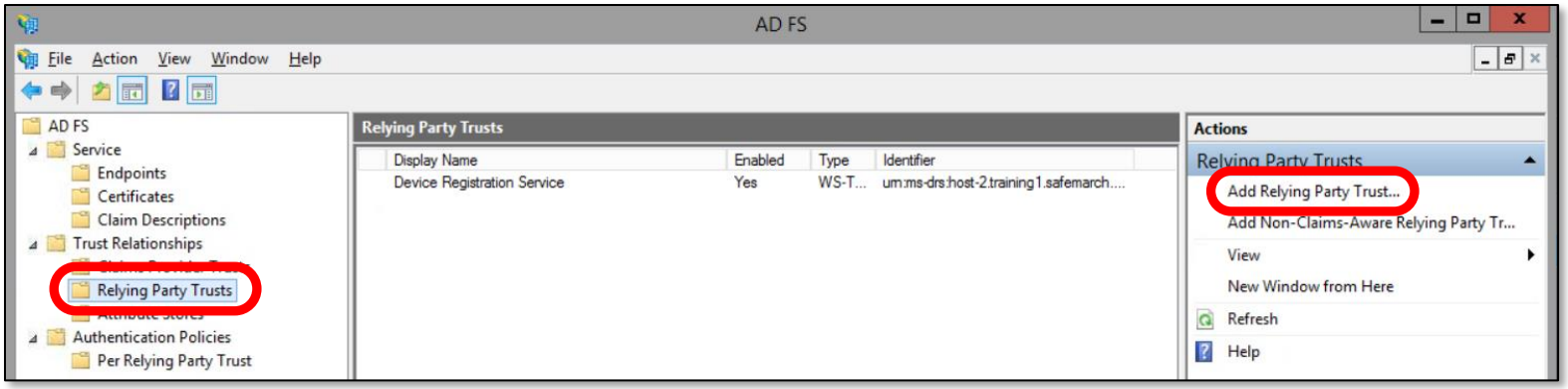
In this section, you will export the SAML Relying Party Metadata from the Zscaler SAML configuration and import it to AD FS. This import includes the Zscaler certificate.

3. On the Windows 2012 Server, open the Zscaler Admin Portal. On the **Administration > Authentication > Authentication Configuration > Authentication Settings** page, click the **Identity Providers** tab.
4. Click  next to the Okta IdP you configured in the previous lab.
5. In the IdP configuration, in the **Service Provider (SP) Options** section, click the **Download** link under **SP Metadata**, and save the file.

   Note: If you are unable to download the file in IE, open the Chrome browser and try again (if necessary download and install Chrome).



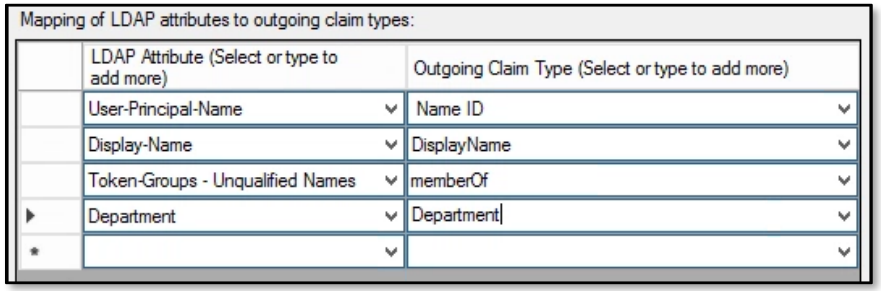
6. On the Windows 2012 Server in the Server Manager, go to **Tools > AD FS Management**.
7. Expand the AD FS tree in the left navigation panel, then expand **Trust Relationships** and click on **Relying Party Trusts**.
8. In the Actions panel to the right, under **Relying Party Trusts**, click on **Add Relying Party Trust…**, this will start the **Trust Wizard**.
   a. At the **Welcome** step, click **Start**;
   b. At the **Select Data Source** step, choose the **Import data about the relying party from file** option, and select the metadata file saved from Zscaler earlier. Click **Open** and then click **Next >**;



c. At the **Specify Display Name** step, enter **Zscaler_SAML** as the **Display Name** and click **Next >**;
d. At the **Configure Multi-Factor Authentication Now** step, accept the defaults and click **Next >**;
e. At the **Choose Issuance Authorization Rules** step, accept the defaults and click **Next >**.
f. At the **Ready to Add Trust** step, review your settings and click **Next >**;
g. At the **Finish** step, accept the default option to **Open the Edit Claims Rules dialog for this relying party trust when the wizard closes**, and click **Close**.

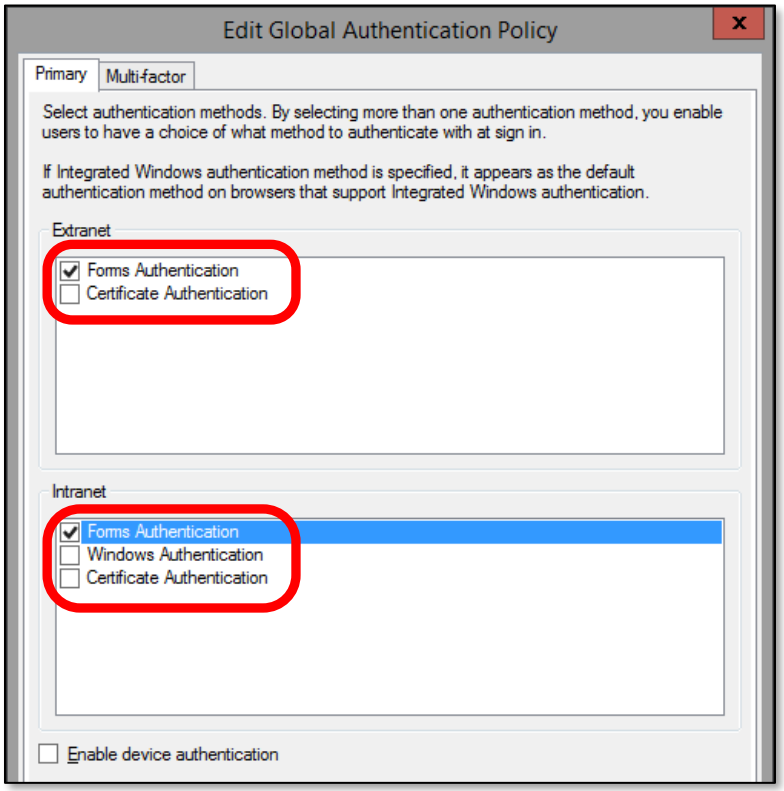
9. Add **Claims** for the Relying Party Trust, as follows:
   a. In the **Edit Claim Rules for Zscaler_SAML** dialog, on the **Issuance Transform Rules** tab click **Add Rule**;
   b. At the **Choose Rule Type** step, accept the defaults (**Send LDAP Attributes as Claims**) and click **Next>**;
   c. At the **Configure Claim Rule** step, under **Claim Rule Name** type **Zscaler_SAML**. Then under **Attribute Store**, select **Active Directory**;
   d. Set the **LDAP attributes mapping** as shown in the following image;
   e. Click **Finish**, then click **Apply**, then **OK**.

   Tip: **Name ID** is in the drop-down, but the others must be typed in. Also note the space in the **Name ID** Claim.

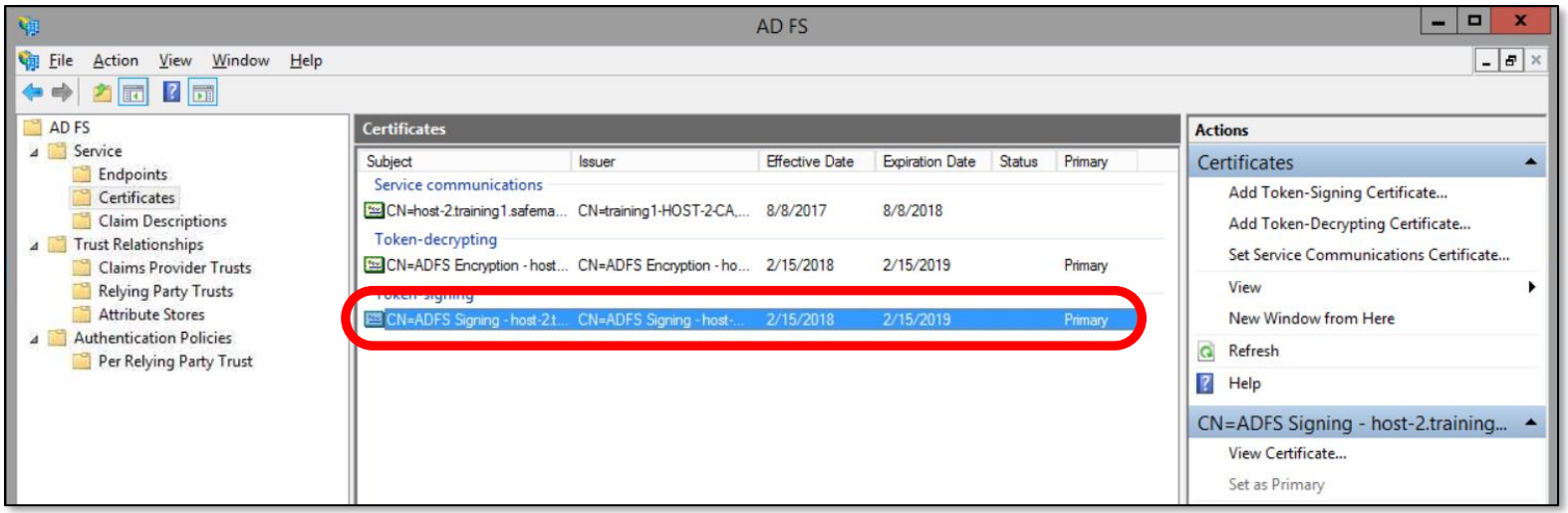


10. In the AD FS tree, below **Trust Relationships**, click on **Authentication Policies**, and in the right-hand navigation panel, under **Actions**, click **Edit Global Primary Authentication….**

11. Ensure that **Forms Authentication** is enabled for both **Extranet** and **Intranet** and disable **Windows Authentication** for **Intranet**, then click **Apply** and **OK**.



12. Export the **Public SSL Certificate** from AD FS and import it into Zscaler to replace the one used in the Okta lab:
    a. In the **Windows 2012 Server** AD FS Manager click on **Service > Certificates**;
    b. Right-click on the certificate under **Token-signing** then **View Certificate**;
    c. Click on the **Details** tab. Then click **Copy to File** to launch the **Certificate Export Wizard**, and click **Next**;
    d. Select **Base-64 encoded X.509 (.CER)** then click **Next**;
    e. Browse to the **Downloads** directory, name the file **adfs**, then click **Save**. Confirm the file path and name then click **Next**;
    f. Click **Finish**, then **OK** to close the Wizard, then **OK** to close the certificate properties;
    g. Go to the **\Downloads** directory. You will need to change the file extension name; however, by default Windows hides extensions for known file types. Change the Windows folder properties under **Control Panel > Appearance > Folder Options** and on the **View** tab uncheck **Hide extensions for known file types**;
    h. You should now see **adfs.cer**, rename the file to **adfs.pem**.



Configuring Zscaler SAML

Complete this section only after you have completed the SAML with Okta Lab. Some of the settings from the Okta lab are re-used in this lab.

13. On the **Windows 2012 Server** open the Zscaler Admin Portal and go to the **Administration > Authentication > Authentication Configuration > Authentication Settings** page.
14. If you completed the SAML with Okta lab, do nothing on this page and click the **Identity Providers** tab. Then, click  next to the **Okta** IdP.
15. Change the Name to **AD FS**.

16. Modify the **SAML Portal URL**, this was set in the previous lab to point to Okta, and you will now modify it to point to AD FS. Change the **SAML Portal URL** to **https://host-2.training[1-N] .safemarch.com:443/adfs/ls/**, then click **Save**.
17. Upload the file **adfs.pem** into the Zscaler SAML configuration:
    a. Under **IdP Public SSL Certificate**, click **Upload** to replace the Okta certificate with the new AD FS certificate;
    b. Browse to and select the file **adfs.pem** in the **\Downloads** directory then click **Upload**;
    c. Click the **Vendor** dropdown list, and select **AD FS**.
    d. Click **Save**, then **Activate** your changes.

Add URL Bypass for AD FS URL in the Zscaler Portal

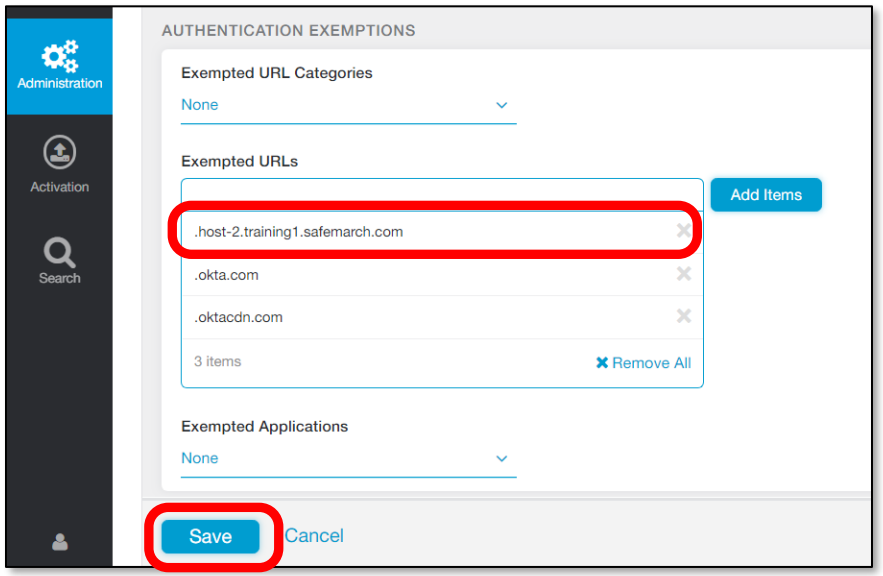
At this point the solution is almost complete. The last item to configure is a URL bypass for the AD FS URL. Remember from the eLearning that the client receives a web-redirect from Zscaler to AD FS for authentication. However, since the client has not yet authenticated no web traffic for the user will pass so the redirect fails. A URL Bypass can be set in the browser PAC file; however, since this lab is tunneling traffic you will set the bypass in the Admin Portal.

18. Go to the **Administration > Settings > Cloud Configuration > Advanced Settings** page.

19. In the **Authentication Exemptions** section under **Exempted URLs** type **.host-2.training[1-N] .safemarch.com** and click **Add Items**.

    Note: The preceding '**.**' Is critical, without it the exemption will not work.

20. Click **Save**, then **Activate** your changes.

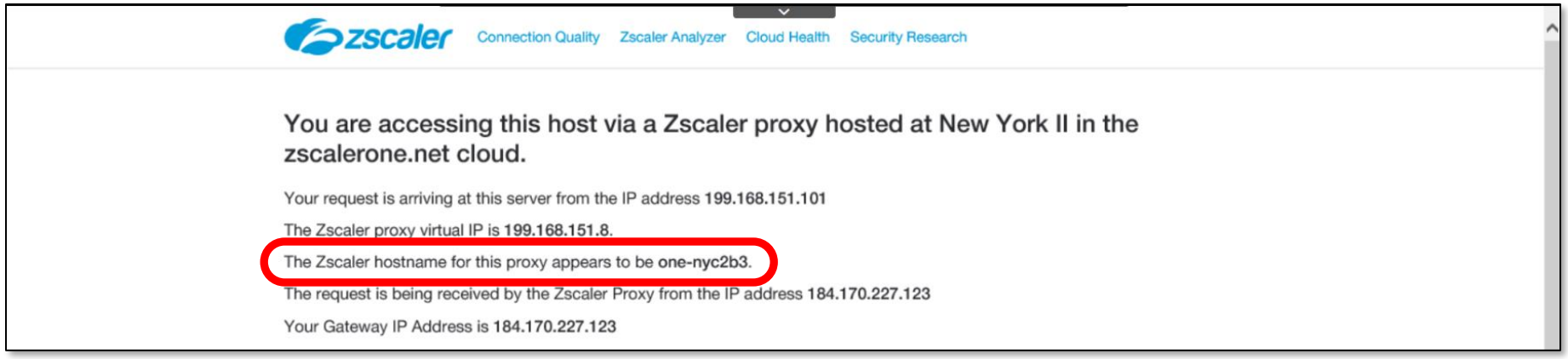


Testing the SAML Configuration

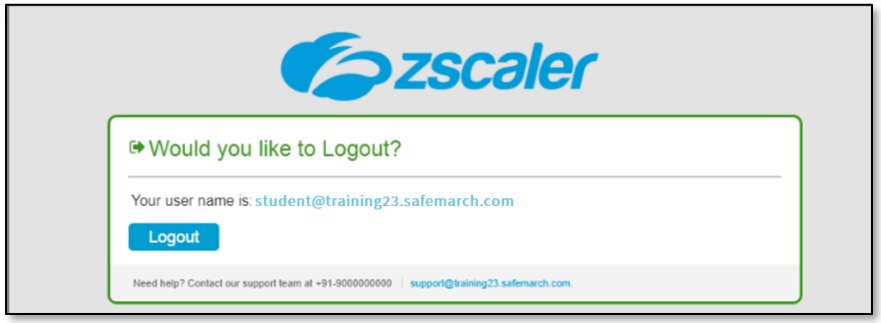
Configuration of the SAML solution with AD FS is complete and you will now test your work.

21. On the **Windows Client PC** open a browser and visit any website, and you should then be redirected to AD FS and receive a web page login prompt. Log in using the Student account that has been pre-populated in AD for you. User: **student@training[1-N].safemarch.com** and the password is **Admin-123!** Once authentication completes you should automatically be redirected to your original URL request.

    Note: if you use the Firefox browser you will need to export the Zscaler Root CA certificate from the system Certificate Store, and import it to the Firefox Store, to allow that browser to trust the connection to Zscaler for SSL inspection.



22. Now that your **Windows Client PC** has authenticated against the service, go to **http://ip.zscaler. com**. The status window now shows the username indicating that authentication was successful.



Note: This configuration is good for PCs and laptops on an internal network. To enable SAML using AD FS for devices on the Internet would require additional components and configuration: An AD FS Proxy installed in the Firewall and accessible on a public IP address from the Internet; and a split DNS configuration that returns the internal IP when a device is on the LAN, and the public IP for the AD FS Proxy when on the Internet.