Zscaler For Users - Essentials (EDU-200)

Hands-on Lab Guide

Zscaler For Users - Essentials (EDU-200) Hands-On Lab Guide
June 2024, Rev. 3.0

Table of Contents

About the Zscaler for Users - Essentials (EDU-200) Hands-on Lab

Welcome to the Zscaler for Users - Essentials (EDU-200) Hands-on Lab. During this lab, you will practice the skills you learned during the eLearning using the Zscaler remote lab. You will complete several labs designed to increase proficiency in configuring connectivity to the Zero Trust Exchange, configuring policy to allow / deny access through the Zero Trust Exchange, and using the administration interfaces to understand traffic patterns.

Lab Description and Scenario

For these lab exercises, consider the scenario where your organization (Safemarch) has deployed the Zscaler Zero Trust Exchange to protect against Internet security threats, control Internet access, and provide secure access to private resources. Your organization is also interested in the end user experience, which can be reported on with the Zero Trust Exchange.

You will deploy the Zscaler Client Connector application to end user devices to control Internet access, provide access to private applications, and to probe, benchmark, and measure the digital experiences for every single user within the organization.

To support the rollout, you are tasked to:

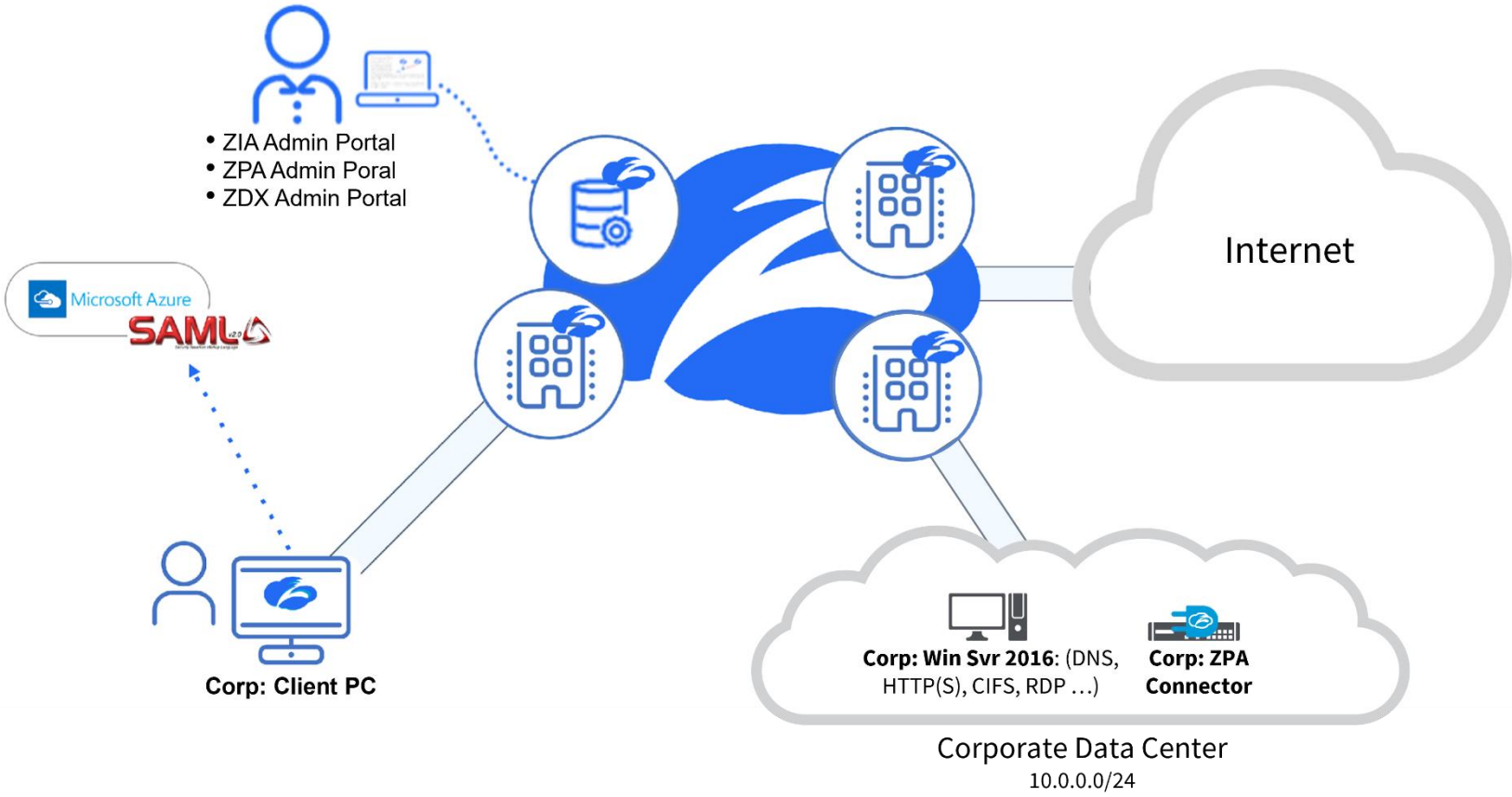
- Connect users to the Zero Trust Exchange by deploying Zscaler Client Connector to Windows client devices.
- Configure SSL inspection.
- Deploy Zscaler Digital Experience (ZDX) reporting and create an initial set of ZDX applications and probes.
- Configure user access to both Internet and private applications.
- Verify Cyberthreat Protection services.
- Verify Data Protection services.

Lab Setup

You will have access to Zscaler Zero Trust Exchange (ZIA/ZPA/ZDX), an account for the Microsoft Azure service and a Skytap ‘Pod’.

For your lab exercises, you will be configuring the ZIA, ZPA and ZDX services and explore the end user experience. You will use a Windows 10 Client PC in Skytap to connect to the Zero Trust Exchange.

Lab Topology



***Note**: For this Hands-on lab, Microsoft Azure is being used for user authentication. The required IDP configurations have been pre-configured for you.*

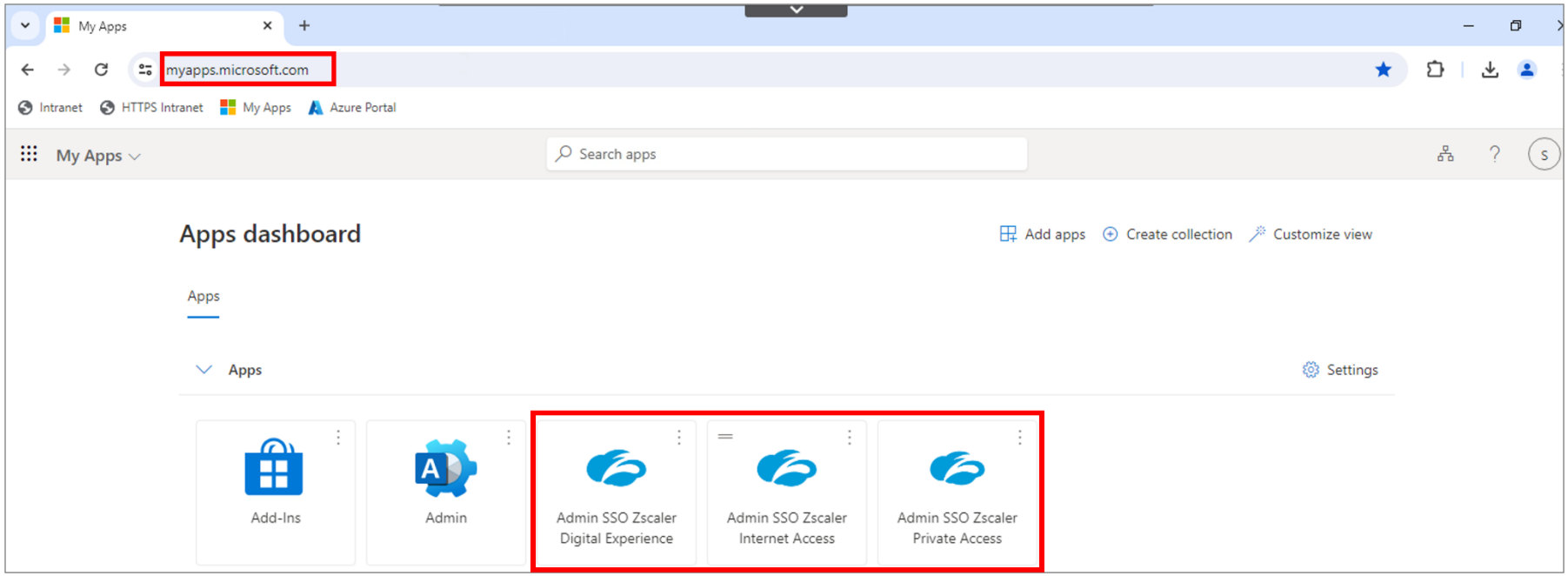
- Windows Client PC
  - Name - **Corp: Client PC**
  - The Client PC is joined to Active Directory patraining.safemarch.com.
  - You will additionally join the Client PC to the Azure AD tenant.
  - Username | Password: Student | Admin-123!

- Windows Server
  - Name - **Corp: Win Svr**
  - Provides local directory services through Active Directory.
  - Hosts the Active Directory domain patraining.safemarch.com, to which the Corp: Client PC is joined.
  - Runs HTTP/HTTPS Intranet applications and file services.
  - Functions as the DNS server for hosts in the data center.
  - Username | Password: Administrator | Admin-123!
- App Connectors
  - Names - **Corp: ZPA Connector**
  - This is a CentOS VMs, pre-deployed in the network to simulate the results of having previously instantiated the OVA/OVF file to deploy the VM with the App Connector RPM already installed.
  - Username | Password: admin | Zscaler

Lab Access Information

For this course, each student is assigned a unique student ID with a dedicated virtual environment (hosted in Skytap) and corresponding Student FQDN with a set of admin and test users accounts for Zscaler and Azure. User credentials and portal addresses are all contained in the lab access instructions that are provided to you for your assigned training pod. These include:

- Your **Student ID** which is a unique identifier for your pod (e.g. zs9901)
- Your **Student FQDN** which is a unique domain for your pod (e.g. zs9901.safemarch.com)
- Your admin logon credentials for access to the Azure and Zscaler Portals
  - The login name will be in the format **student@<Student FQDN>** where [Student FQDN] is the domain assigned to your pod. For example, student@zs9901.safemarch.com.
  - The password is unique for your session and is set as the same password on all the configured admin and user accounts for the pod.
- You may access the Zscaler Admin Portals by clicking the links in **https://myapps.microsoft.com**. Pre-configured tiles on this page enable single sign-on and convenient access to each of the Zscaler admin portals.



***Note**: You may still access the Zscaler portals directly if needed using the same login name and password student@<Student FQDN> for ZIA/ZPA and zdx-student@<Student FQDN> for ZDX.*

Lab 1: Connecting to the Virtual Lab

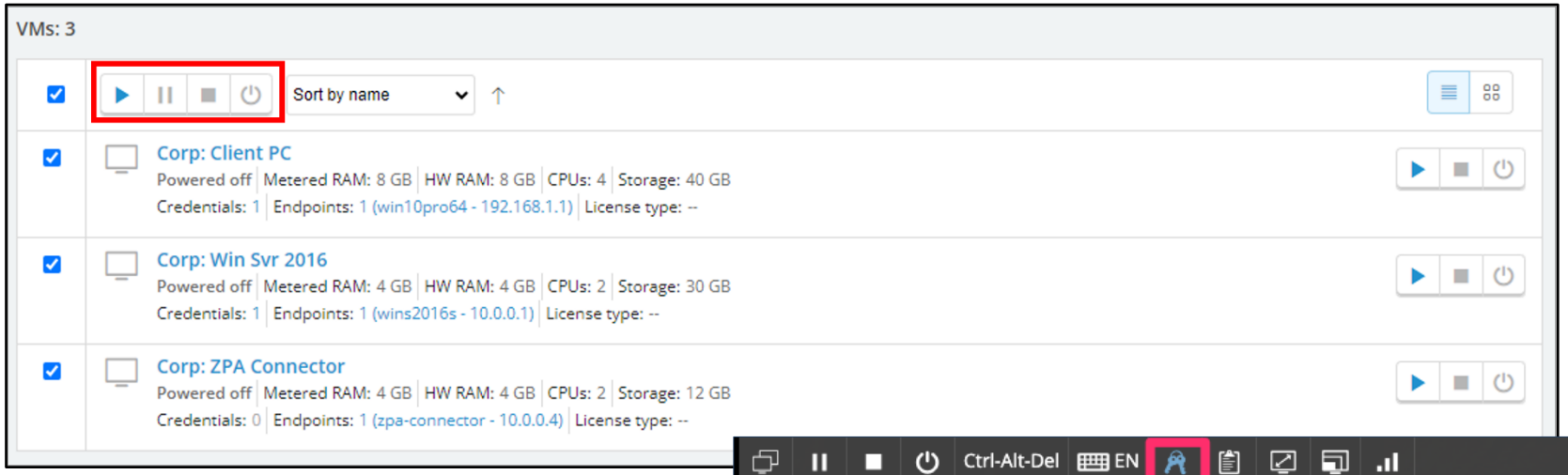
In this lab, you will connect to Skytap, start all virtual machines and spend some time to:

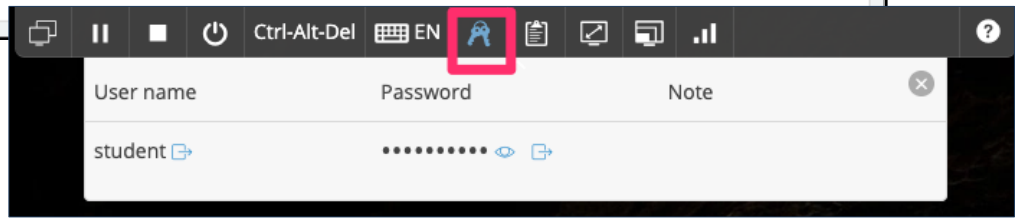
- Familiarize yourself with the logon options and clipboard copy/paste functions, and
- Ensure the keyboard is mapped appropriately for your locale.

Task 1.1: Test Your Lab Access and Start Your Environment

1. Start and connect to your Skytap pod:
    a. Click the **Skytap Portal URL** provided in your access instructions.
    b. Ensure the checkbox is checked to **select all VMs**,
    c. Click the **Play** button. All of the VMs will launch.

***Note**: VMs in the environment are set to start in stages, so the whole process will take a few minutes.*





2. Once the VMs have launched, you will be able to click them to open a browser window which provides direct access to the VM.
3. When connected to a VM, the **Keys** icon displays the username/password. Clicking the icon allows you to insert the credentials into the foreground application.

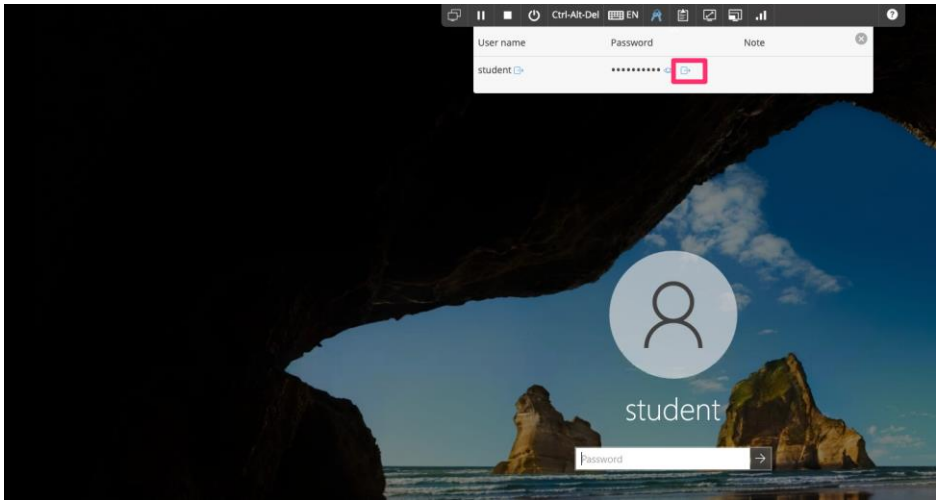
Task 1.2: Join the Corp: Client PC to the Student FQDN on Azure Active Directory

All the student lab environments are initially identical. To configure them for testing with the Zscaler and Azure tenants for the assigned Student FQDN, the Corp: Client PC must be joined to the Azure AD domain as part of the initial lab setup. This is done in two steps on the Corp: Client PC:

- Logon as the local **Student** user.
- Join the PC to the Student FQDN on Azure AD

> ***NOTE:*** *Throughout this lab guide* ***<Student FQDN>*** *is used to represent the domain assigned to your pod.*
>
> *For example, for Student ID* ***zs9901*** *with Student FQDN* ***zs9901.safemarch.com*** *, student@<Student FQDN> becomes student@****zs9901.safemarch.com***

1. Login to the Corp: Client PC as the local Student User:
    a. Launch the **Corp: Client PC** from the Skytap portal
    b. Click the **Ctrl-Alt-Del** icon in the Skytap Toolbar
    c. Click the **Credential** (keys icon) in the Skytap Toolbar
    d. Click the **Insert Credentials** icon next to the password field for the **student** username.

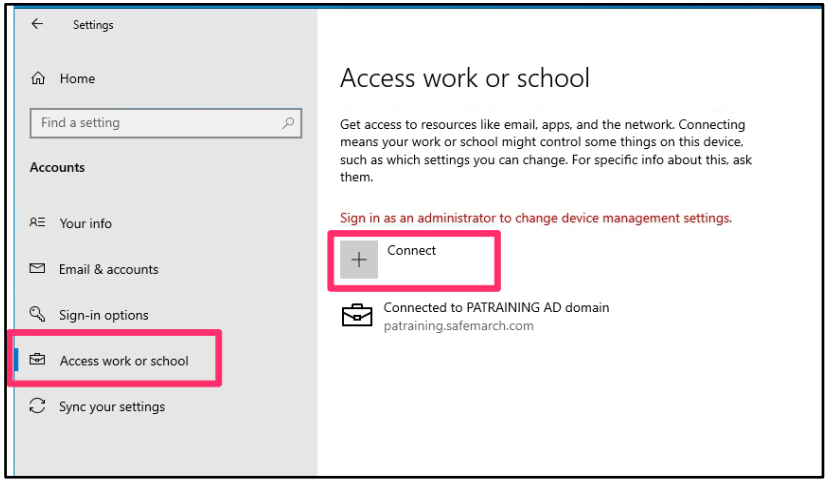


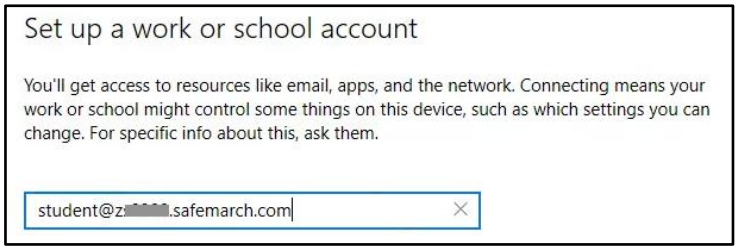
2. Join the PC to your Student FQDN on Azure AD:

Note: As part of the initial setup your lab pod has been pre-configured for authentication to your Student FQDN on a dedicated Azure Active Directory tenant with a set of test users as well as your Zscaler admin accounts.

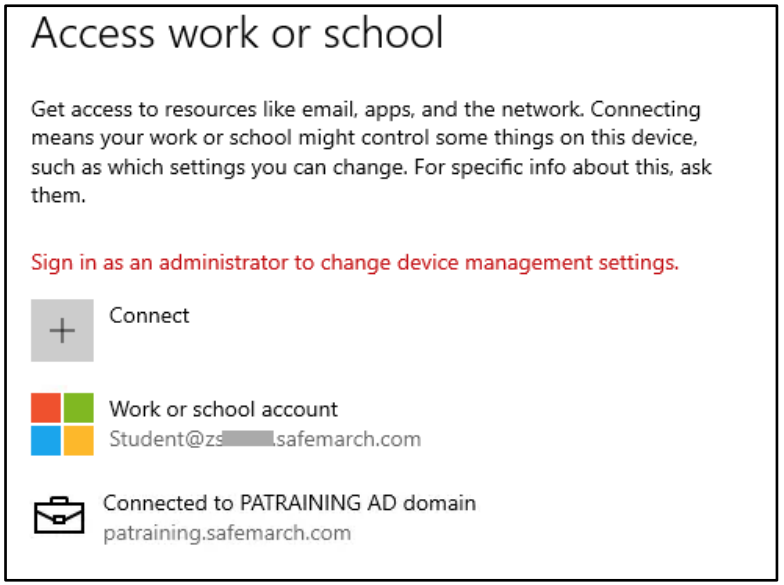
a. Click the **Windows** button in the bottom left
b. Click the Cog icon to open **Windows Settings**
c. Click **Accounts** to open the Account Settings screen
d. Select **Access work or school** on the left-hand side, and then
e. Click the **+ Connect** button
f. Authenticate to Azure AD using your **student@<Student FQDN>** username and password in the dialog box presented
g. Click **Done**.

Note: Password for your tenant is provided in your lab access instructions.





3. Verify that the PC is connected to **Azure AD Work or school account** as **student@<Student FQDN>**.



Task 1.3: Test Zscaler Admin Portal SSO Access

In this task, you will test that Admin Portal access and Single Sign-On (SSO) is configured and working. You can access the Zscaler and Azure Admin portals from the machine/browser of your choice. These are cloud services accessible from any machine with an Internet connection. To test Zscaler Admin portal SSO access, follow these steps.

1. Open the Microsoft Apps dashboard for the Student account assigned to you (see your Lab Access Instructions):
    a. In a browser window, open **https://myapps.microsoft.com**
    b. Authenticate with your student admin account:
        - Username: **student@<Student FQDN>**
        - Password: as provided in the Lab Access Instructions
2. Verify access to each of the Zscaler Admin Portals by clicking on the tiles for:
    a. Admin SSO Zscaler Internet Access
    b. Admin SSO Zscaler Private Access
    c. Admin SSO Zscaler Digital Experience

> **Note**: If needed, each of the Zscaler portals may be accessed directly using the same **student@<Student FQDN>** credentials for ZIA/ZPA, and as **zdx-student@<Student FQDN>** for ZDX.

Lab 2: Forwarding Traffic with Zscaler Client Connector

In this lab, you will practice the installation, management, and use of the Zscaler Client Connector to forward traffic to the Zero Trust Exchange (ZTE).

The Zscaler Client Connector will be installed on your users' computers to apply corporate policy for Internet Security and provide connectivity to private applications. The Client Connector tunnels user traffic to the Zero Trust Exchange and ensures that the security and access policies in the Zscaler Internet Access Admin Portal are enforced wherever the users may be accessing the Internet. The Client Connector also intercepts traffic for private applications and applies access control from the Zscaler Private Access Admin Portal to ensure users can access private applications.

The Zscaler Client Connector identifies the closest Service Edge for Internet and Private Access, including private Service Edge, and connects via Zscaler tunnels to the Service Edges.

The distribution method for deploying the Zscaler Client Connector will vary by your organization's capabilities. During this lab, you will install a single instance of the Zscaler Client Connector, manually, on the Corp: Client PC and will employ some of the available cli-based installation options.

The Zscaler Client Connector can be deployed with the default configuration; however, the user would be prompted for cloud configuration information. In this lab, we will customize the installation options to ensure an optimal end-user experience, and to ensure all traffic is correctly forwarded to the Zero Trust Exchange. We will create a *Forwarding Profile* to ensure all traffic is tunneled to the ZTE, and an *Application Profile* to control which ZTE service points are used. We will install the Zscaler Client Connector with installer options to provide transparent enrollment for the end user - minimizing the users' need to interact with the client during deployment.

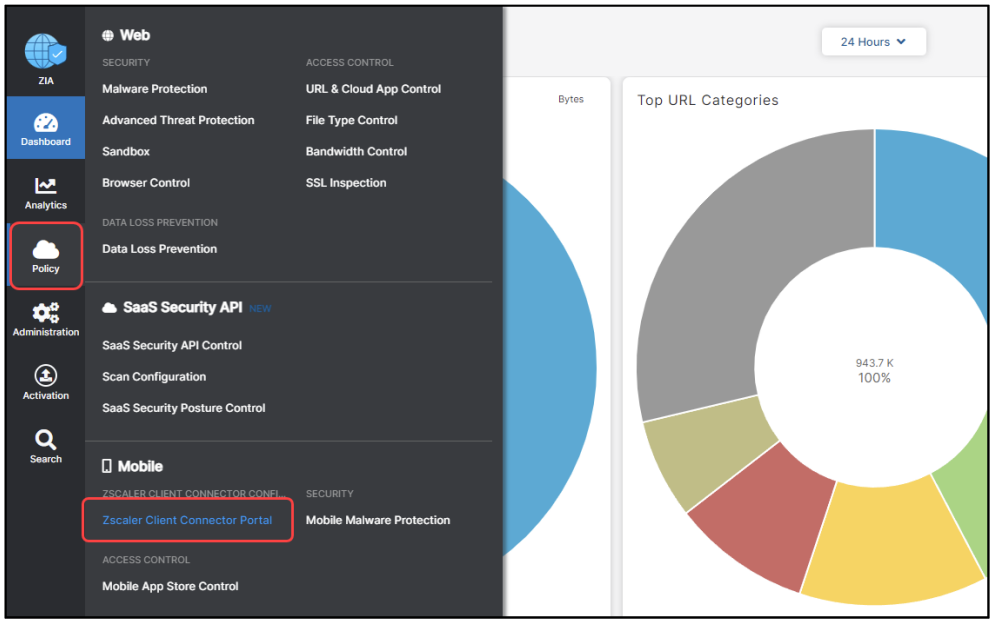
We will use the Corp: Client PC for administering the Zscaler platform, as this enables us to download the Zscaler Client Connector directly to the machine. You could use any machine, and copy/paste the URL's for download as necessary, however this is the simplest option.

Task 2.1: Configure Forwarding Options

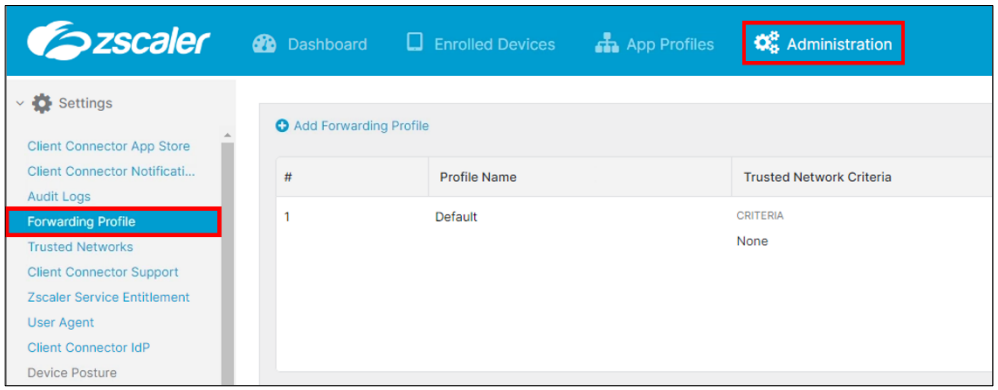
In this task, you will create a Forwarding Profile and configure how Zscaler Client Connector will behave to intercept traffic in different networking conditions. Zscaler Client Connector detects being on a corporate network by looking at DNS resolution options (what a host resolves to, what DNS search suffixes are provided by DHCP, and what DNS servers are provided by DHCP). It detects VPN's by identifying default routes and VPN adaptors. In this scenario, you will deploy Zscaler Client Connector to intercept traffic on all network types for Zscaler Internet Access and Zscaler Private Access. Therefore, we will configure a Forwarding Profile to intercept in all scenarios, regardless of the network type detected.

1. On the **Corp: Client PC**, log into the **Zscaler Internet Access Admin Portal**. Navigate to Zscaler Client Connector Portal via **Policy** > **Zscaler Client Connector Configuration** > **Zscaler Client Connector Portal**.

   Note: *You can also reach the Client Connector Portal from ZPA and ZDX Admin Portals.*



2. Navigate to the **Administration > Forwarding Profile** page.



3. To create and configure a Forwarding Profile, click **Add Forwarding Profile** and configure the policy:
    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 FOR ZIA** section under **On Trusted Network**, select **Tunnel**.
    d. For the **Tunnel Version Selection**, use **Z-Tunnel 2.0**.

Note: *Tunnel 2.0 is necessary to intercept all traffic to tunnel to ZIA for Firewall functionality.*

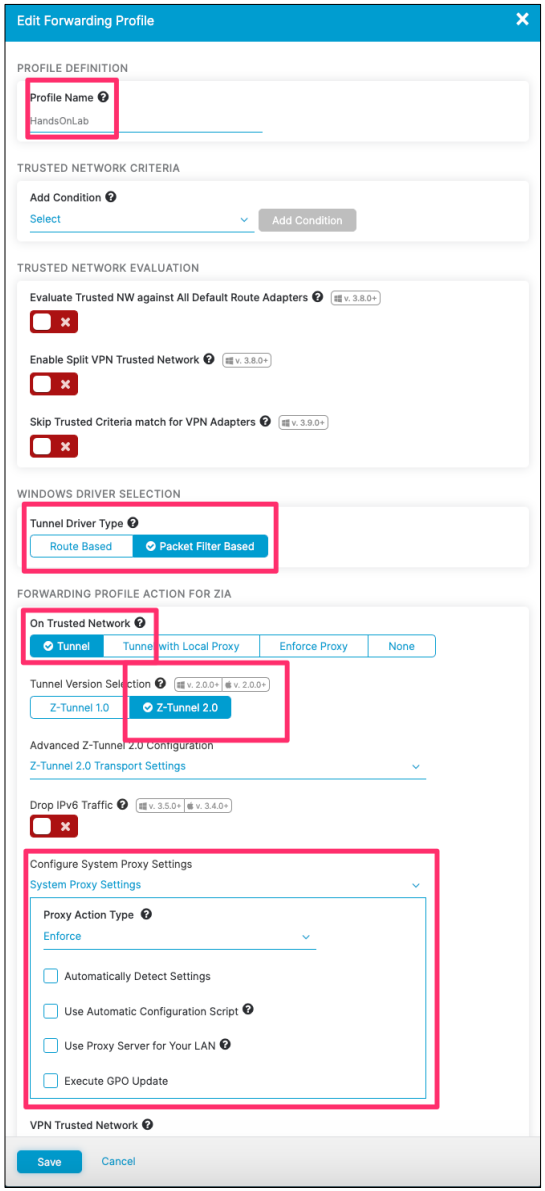
---

    e. Under **Configure System Proxy Settings**, select **Enforce** and ensure all the options are unchecked.

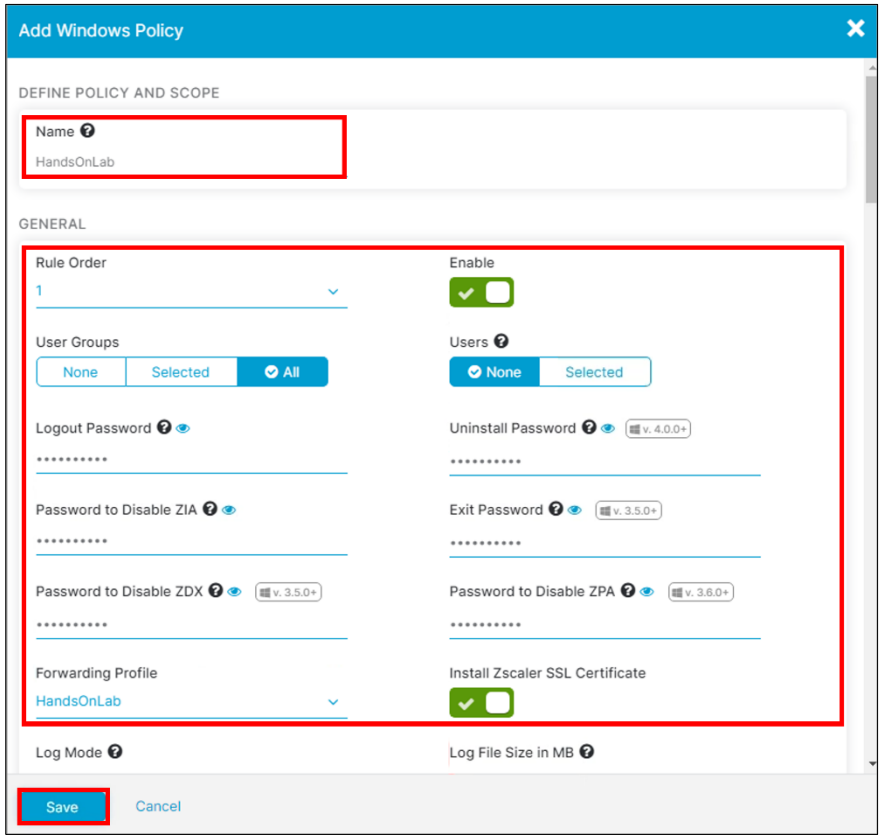
Note: *Enforcing no Proxy Settings ensures that nothing interferes with Zscaler Client Connector Tunnel Mode Interception. In production deployments it may be necessary to implement changes to the browser authentication settings and identify other changes necessary for how web browsers function to applications.*

---

    f. Under **VPN Trusted Network**, click the box next to the **Same as "On Trusted Network"** option.
    g. Under **Off Trusted Network**, click the box next to the **Same as "On Trusted Network"** option.
    h. In the **FORWARDING PROFILE ACTION FOR ZPA** section, select **Tunnel** for **On Trusted Network** and select the **Same as "On Trusted Network"** for **VPN Trusted Network** and **Off Trusted Network**.
    i. Click **Save**.



4. Navigate to the **App Profiles > Platforms > Windows page**.
5. 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. **Enable**.
    d. Groups: **ALL**.
    Optionally configure Logout Password, Disable Password, Exit Password, and Uninstall passwords: **Admin-123!** Otherwise leave them blank.
    e. Install Zscaler SSL Certificate: **Enable**.



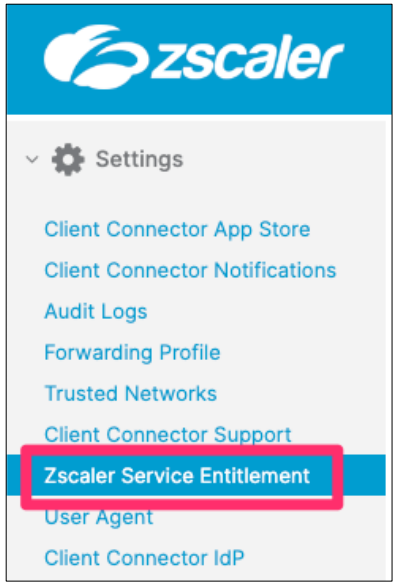
***Note**: This will install the Zscaler Root CA Certificate on the Client PC. If you have configured Zscaler for SSL Inspection (which we will do later) it is best practice to enable this option for your Zscaler Client Connector users.*

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

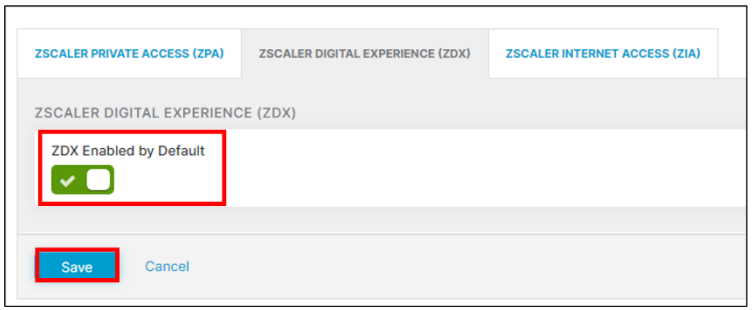
Task 2.2: Configure Service Entitlement

In this task, you will enable the Zscaler service for all users. It is possible to control which groups of users are entitled to Zscaler Private Access, Zscaler Digital Experience, and Zscaler Internet Access. By default, only Zscaler Internet Access is Enabled for all users.

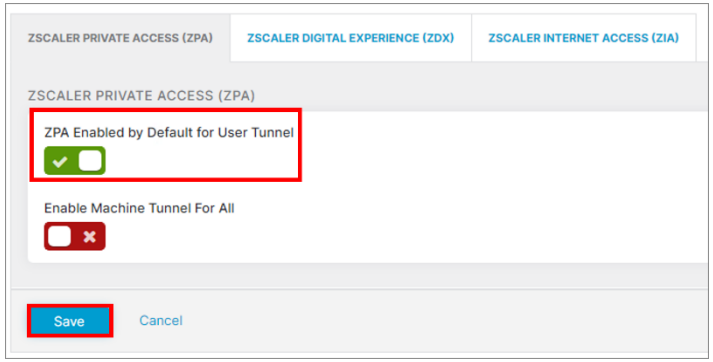
In the **Zscaler Client Connector Administration Portal**, perform the following steps:



1. Navigate to **Administration >Zscaler Service Entitlement**.
2. Select **Zscaler Digital Experience (ZDX)** tab and ensure **ZDX Enabled by Default** is selected.
3. If needed, enable the service and click **Save**.



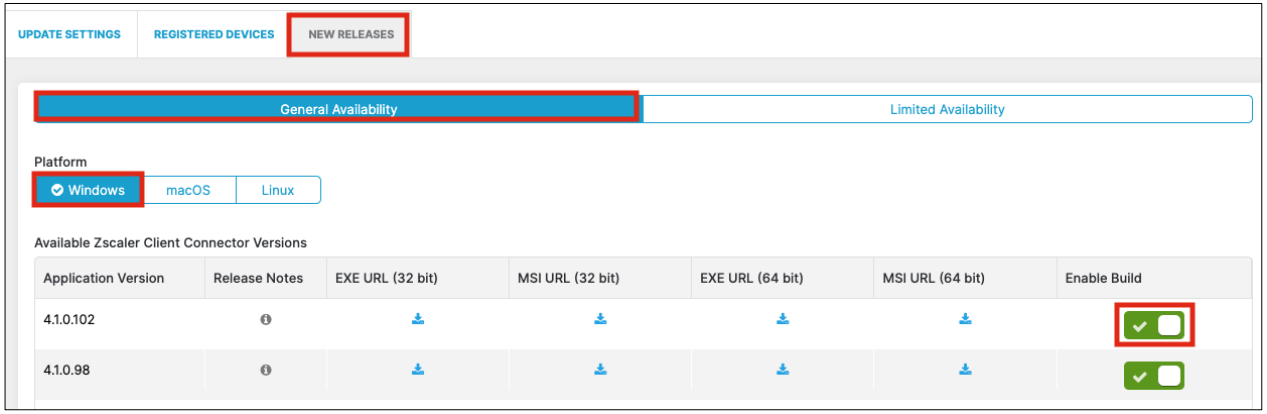
4. Select **Zscaler Private Access (ZPA)** tab and ensure **ZPA Enabled by Default** is selected.
5. If needed, enable the service and click **Save**.



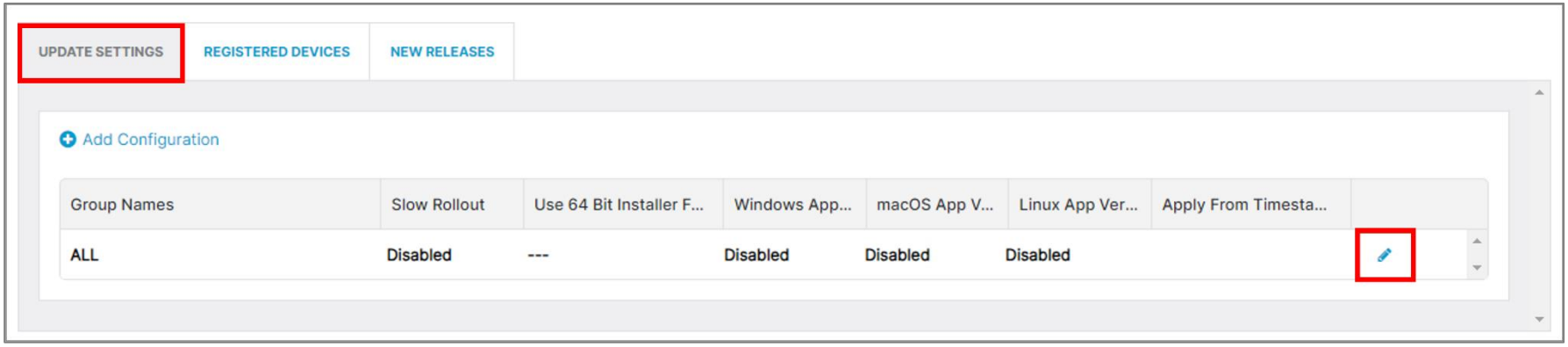
Task 2.3: Download the Zscaler Client Connector

In this task, you will download the Zscaler Client Connector installer to the Corp: Client PC. Multiple layers of controls are available to allow you, as the Administrator, to decide if you want to allow the most current version of the Zscaler Client Connector to roll out to your users, automatically, or restrict which version reaches your users, thus enabling you to test before rolling out the latest releases.

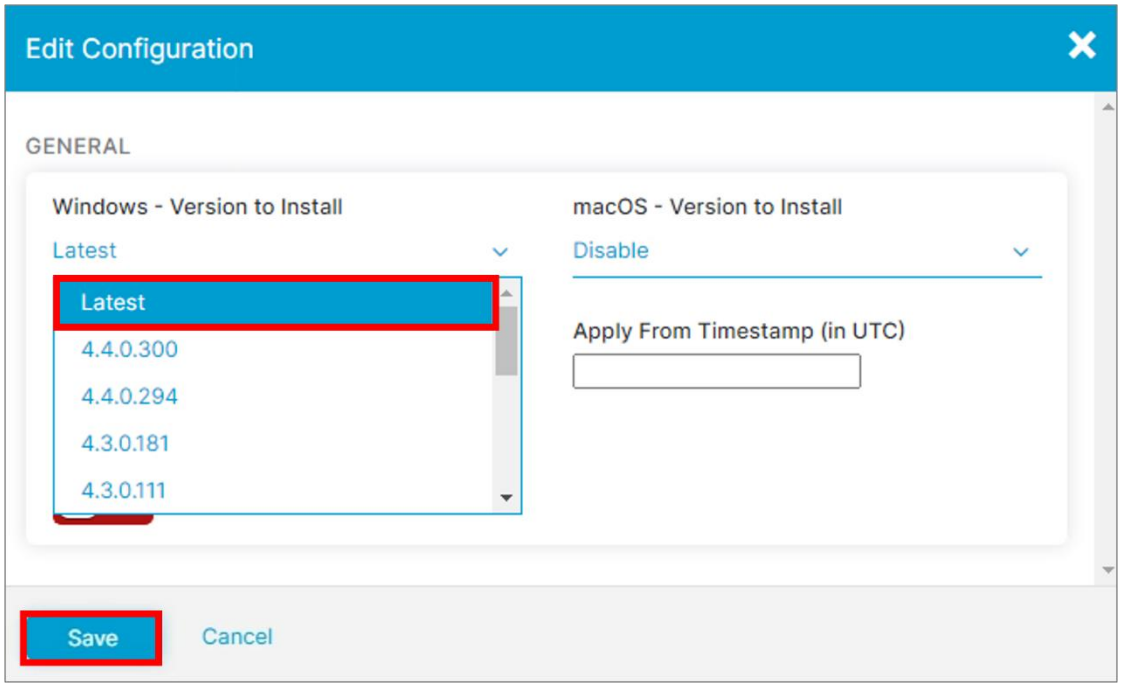
1. Within the Zscaler Client Connector Portal, navigate to the **Administration > Client Connector App Store** page.
2. Click on the **NEW RELEASES** tab and ensure that you have the **General Availability** tab selected. All the available Client Connector versions are listed for the selected platform. *Limited Availability* releases are those that have not seen wide testing and should be used with discretion. They are not enabled by default.
3. Enable the latest build under **General Availability**, then click **Save**.



4. Choose which versions to roll out to the users (You can control this by groups of users in production)
   a. Click on the **UPDATE SETTINGS** tab.
   b. Click to edit the Default Configuration.



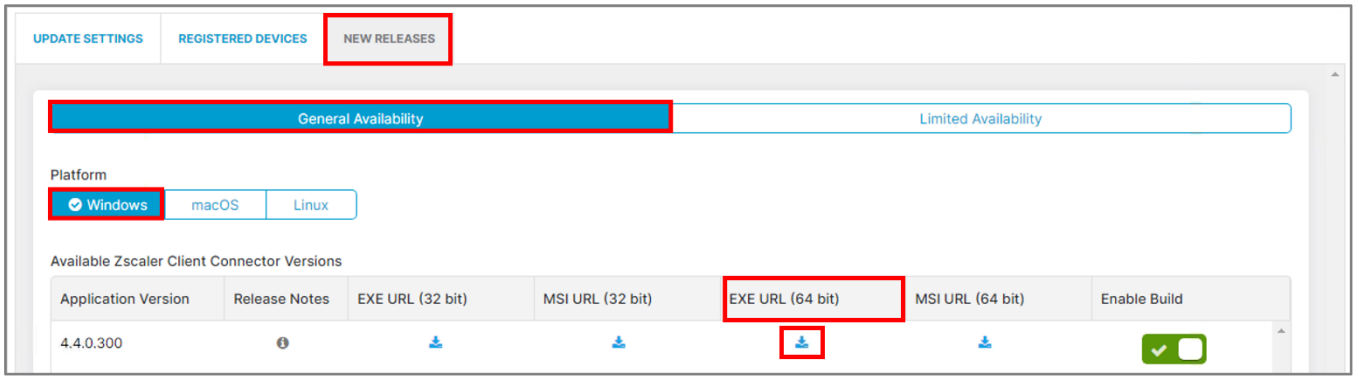
c. From the Windows – Version to Install dropdown list, select **Latest** and click **Save**. With this option selected, whatever the most current release that was enabled in the NEW RELEASES page.
d. Click **Proceed**.



Optionally, you can manually select which of the builds you enabled for Windows, Mac or Linux devices will be rolled out. This provides the option to control version rollouts more specifically. For example, you can prevent a brand-new release from being deployed automatically.

For further version control and internal IT testing you can create a custom configuration, select the most current release, and choose to push it to a select group of users for internal testing before pushing it out to the wider user community.

5. Under the **NEW RELEASES** tab, click on the **Download** link for the latest version of the App listed under the **EXE URL (64 bit)** column and save this to the Downloads folder on the Client PC.

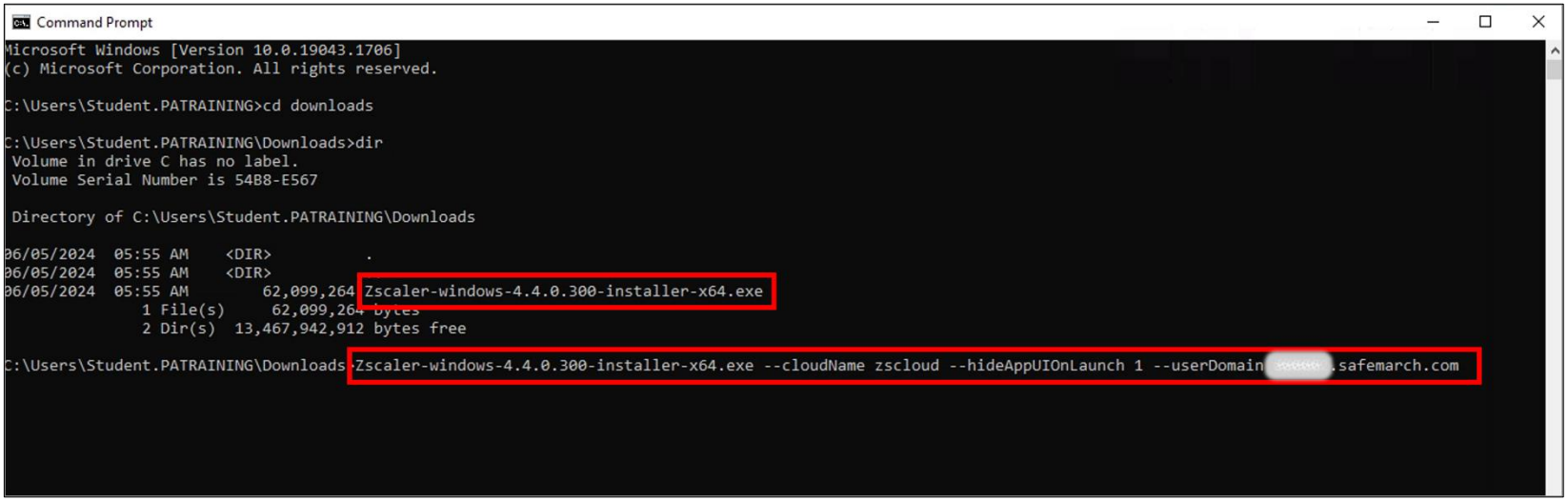


Task 2.4: Install the Zscaler Client Connector from the CLI with Install Options

Now that some basic policies are in place, you will install the Zscaler Client Connector.

In this task, you will manually install the Zscaler Client Connector, from the CLI, with Installation Options. Installation Options allow you to customize the Connector Installation for your organization. A complete list of the Installation Options can be found in the online help portal documentation. During this exercise you will use the following switches: **--cloudName, --hideAppUIOnLaunch**, and **–userDomain**.

1. On the **Corp Client PC**, open a **Windows Command Prompt**.
2. Change to the **Downloads directory** where you downloaded the Zscaler Client Connector. Type **cd downloads**.
3. On the CLI type the following command to run the installer with command line switches:
    a. **Zscaler-windows**-<file version>**-installer-x64 --cloudName zscloud --hideAppUIOnLaunch 1 --userDomain** <Student FQDN>



Options Description:
--cloudName: locks this Client installation to the specified Zscaler Internet Access Cloud. Helpful if an organization spans multiple Zscaler Clouds as the user is not prompted to select the appropriate cloud.

--hideAppUIOnLaunch: Prevents the Zscaler Client Connector login page from appearing on PC reboot. Still appears in the Windows Tray and the User must manually launch it. Switches: 0 (disabled) or 1 (Enabled).

--userDomain: Allows users to skip the initial app enrollment prompt in Zscaler Client Connector and redirects the user straight to the organizations' SAML SSO page (Azure in this lab).

Note**: The commands are case -sensitive! Remember to substitute your Student FQDN for <Student FQDN> . The command requires an admin user login to complete. When prompted to enter administrator login, the username is **administrator**, and the password is **Admin-123!

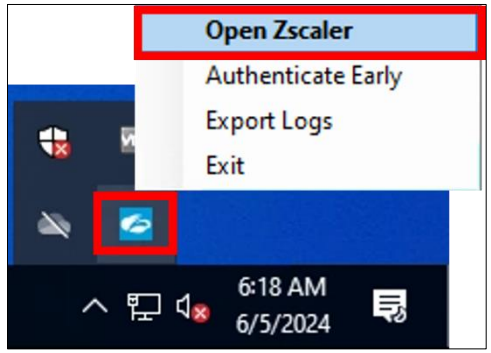
4. Follow the installation prompts on the client and click **Finish**.

***Note**: In a production deployment, you would use an MDM (SCCM/InTune/Airwatch) to install silently.*

Task 2.5: Login to the Zscaler Client Connector and Verify Protection

In this task, you will log into the Zscaler Client Connector, and confirm that the Corp: Client PC is now being protected by the App.

1. On the **Corp: Client PC**, the Zscaler Client Connector is now installed. However, as you used the **--hideAppUIOnLaunch** option, the Client Connector login screen does not automatically appear but remains closed in the Windows Tray. Launch the Zscaler Client Connector from either the Windows Tray icon or from the Windows Start bar under Zscaler.



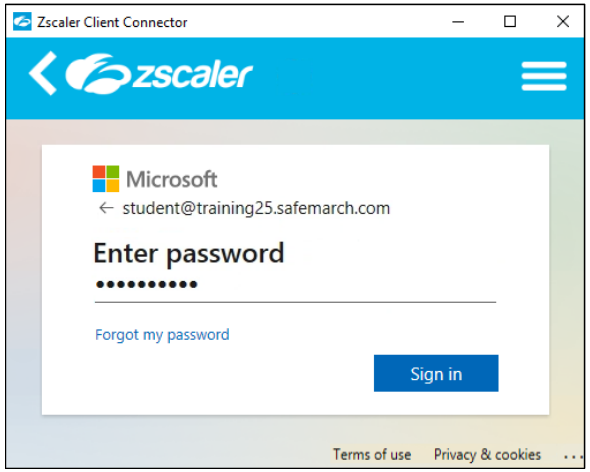
---

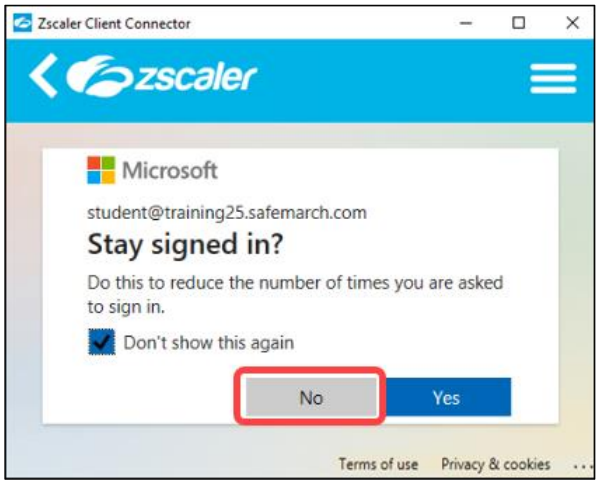
*As you installed the client using the **--userDomain** option, the client will automatically bypass the service enrollment screen and is taken directly to the IdP configured for this account (Azure in this example).*

*If you successfully joined the **Corp Client PC** to Azure AD (in the Azure AD Join Windows PC section), then the machine should have transparently authenticated to Azure AD and Zscaler Client Connector is enrolled. Otherwise, you will be prompted to authenticate by the Azure AD SAML IDP.*

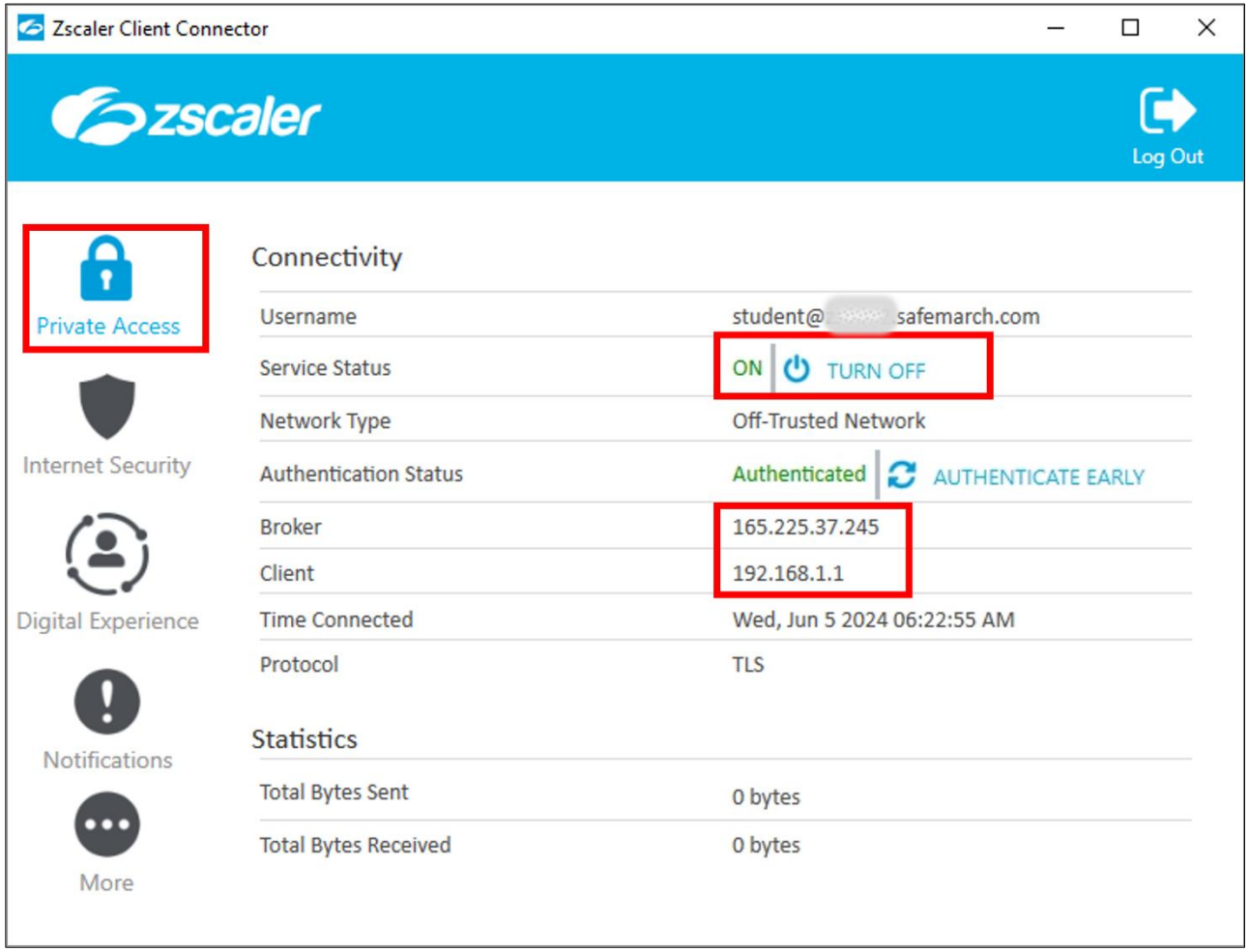
---

2. If prompted to sign in, enter the **student** account **Username** from the student access instructions that you received (**student@<Student FQDN>**) and click **Next**. Enter the student **password**, then click **Sign In**. Say **No** when asked to Stay signed in.

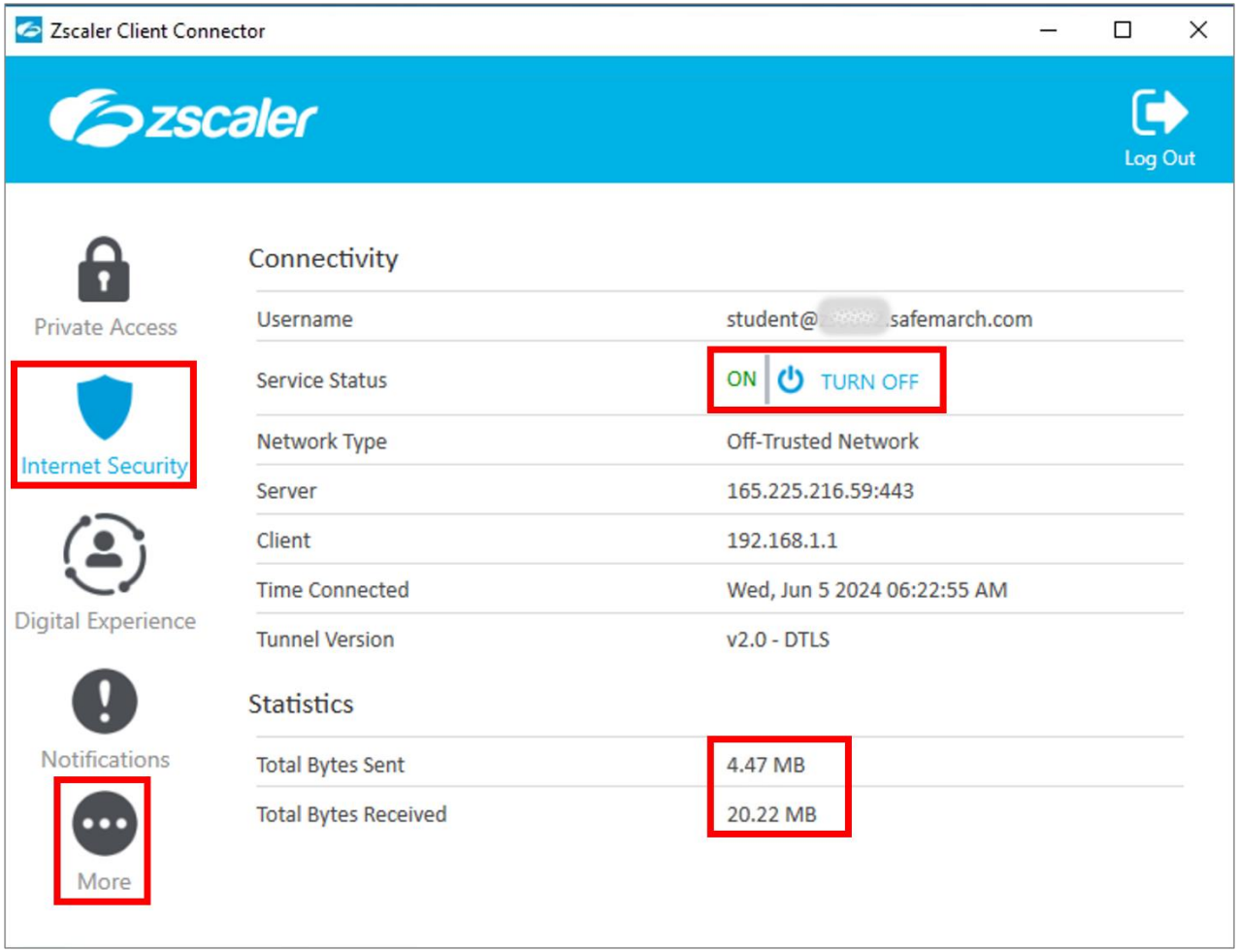




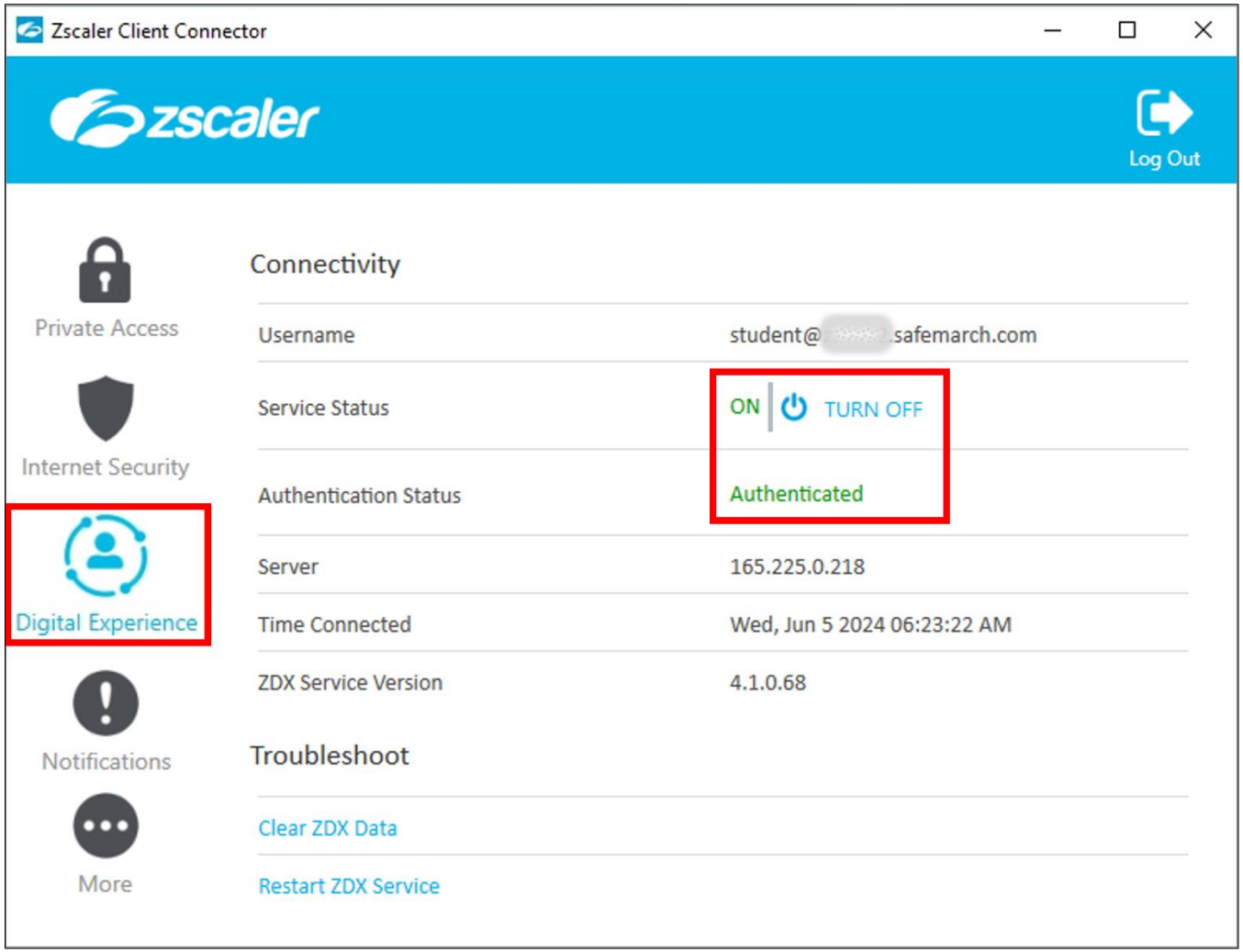
3. In the **Windows Task Bar**, at bottom right, click to **Show hidden icons**, click on the **Zscaler Client Connector icon**, then click **Open Zscaler**.
4. On the **Private Access** page, confirm that:
    a. **Service Status** indicates **ON**.
    b. Username is correct, and identifies you as the STUDENT and the correct tenant ID.
    c. **Client** and **Broker IP** addresses are populated.



5. On the **Internet Security** page, confirm that:
    a. Service Status indicates **ON**.
    b. **Username** is correct.
    c. **Total Bytes Sent** and **Total Bytes Received** increment when you load web pages.
    d. Click **More** to view the App Policy that is applied (HandsOnLab).



6. On the **Digital Experience** page, confirm that.
    a. **Service Status** indicates **ON**.
    b. **Authentication Status** indicates **Authenticated**.
    c. **Username** is correct.



7. In a browser window, navigate to **https://ip.zscaler.com**, and review the information displayed.

> ***Note:*** *You may see a different data center than the one shown below, depending on the region your class is in.*

Lab 3: Configuring SSL Inspection Policies

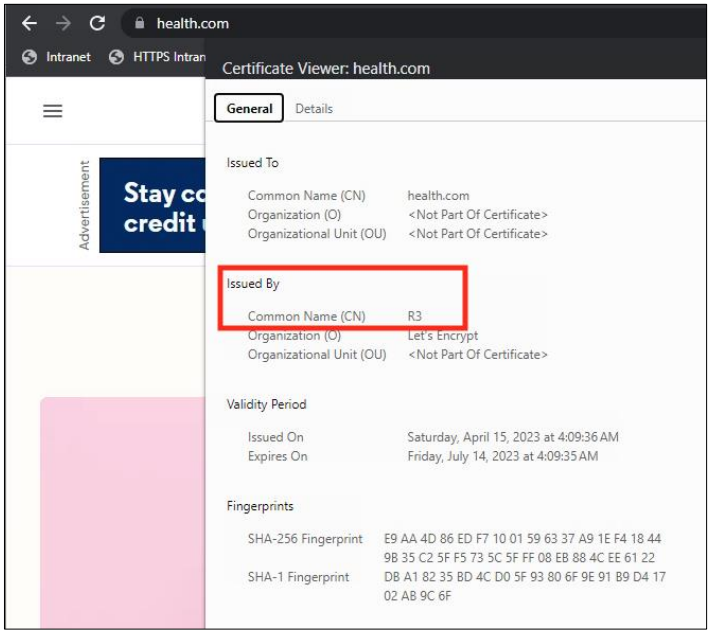
In this lab, you will enable SSL inspection for all destinations and also enable a SSL exemption. Increasing amounts of Internet traffic is now encrypted. If your organization is not inspecting SSL traffic, you are blind to the contents and potential threats. Zscaler Best Practice is to enable SSL Inspection.

Note: You have already installed the Zscaler Root CA Certificate onto the Windows 10 Client PCs in the previous lab, when you installed the Zscaler Client Connector. For Windows devices it must be installed in the system certificate store under Trusted Root Certification Authorities and in the Firefox certificate store. The Zscaler Client Connector did this based on the setting in the App Profile.

Task 3.1: Enable SSL Inspection for All Destinations

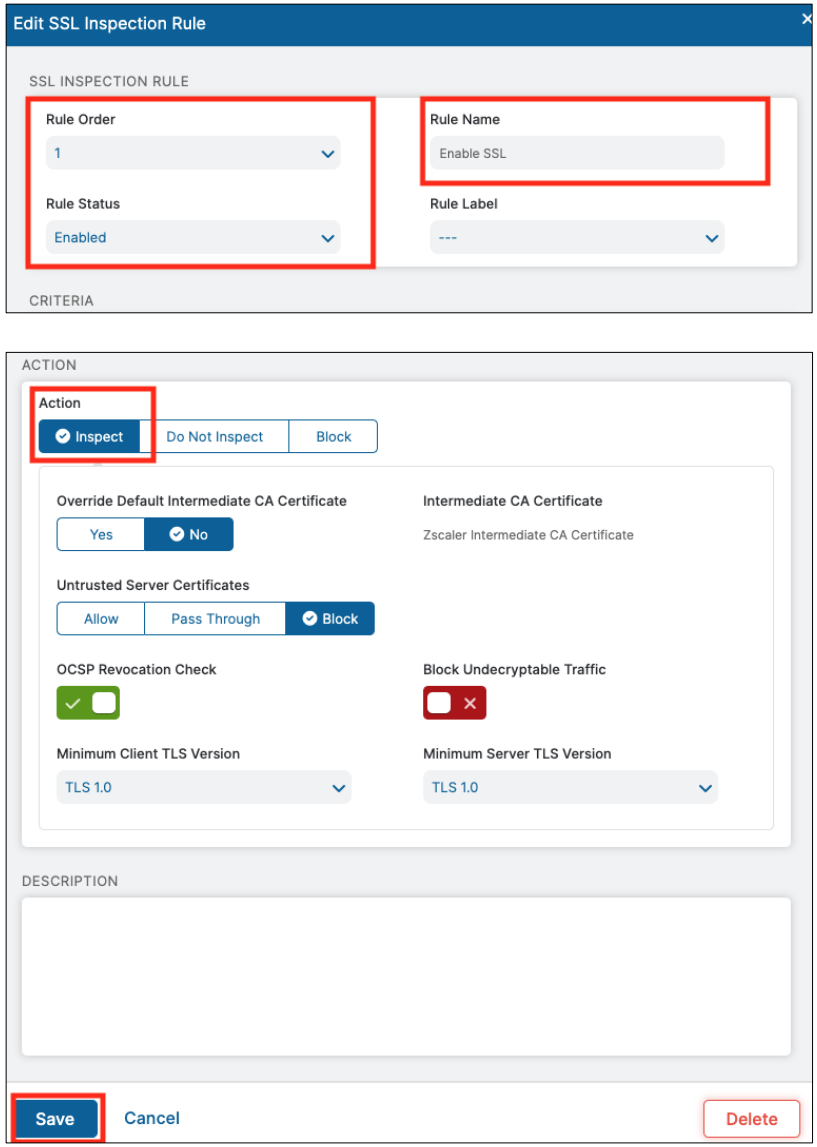
In this task, you will enable SSL Inspection for All traffic.

1. Verify that SSL traffic is **not** currently being inspected by viewing the certificates.
    a. On the **Corp: Client PC** open a Chrome browser window in **Incognito Mode** and visit **https://health.com**.
    b. Click the **lock icon** in the URL field, then click **Connection is secure** > **Certificate is valid**. You will see that you have received the certificate from the destination Web server.

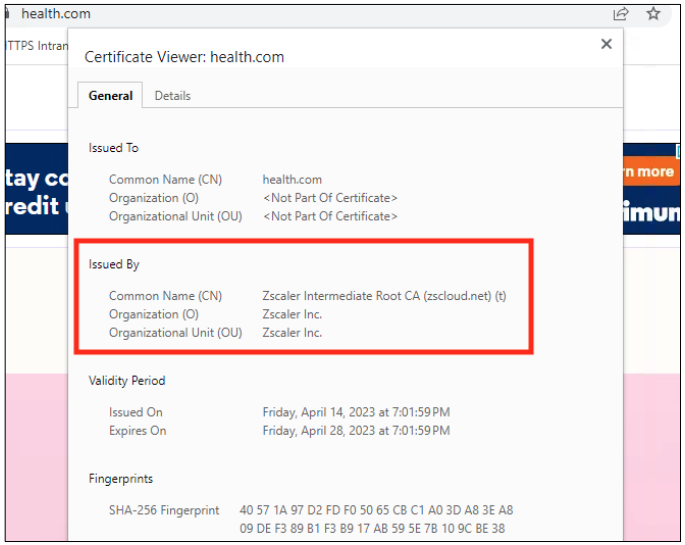


2. Now, configure the SSL Inspection Policy to SSL Inspect all of your organization's traffic. In the Zscaler Admin Portal go to the **Policy > Web > ACCESS CONTROL > SSL Inspection** page.
    a. While on the SSL Inspection Policy tab, click **+Add SSL Inspection Rule**.
    b. Set the Rule Order to **1**.
    c. Rule Name: **Enable SSL**
    d. Scroll down to the ACTION section and under **Action**, select **Inspect**.

3. Click **Save** at the bottom of the page, then **Activate** your changes.



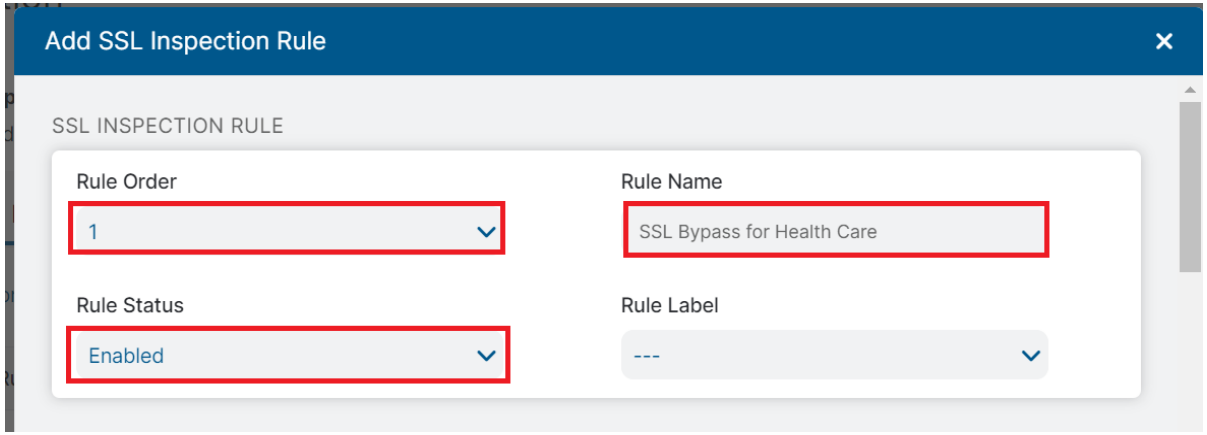
4. Verify Inspection status:
    a. On your **Inside Windows Client PC**, close the browser, then re-open it in Incognito Mode, and load **https://health.com** again.
    b. Click the **lock icon** in the URL field, then click **Connection is secure > Certificate is valid**. You will see that you have received a server certificate **signed by Zscaler**.

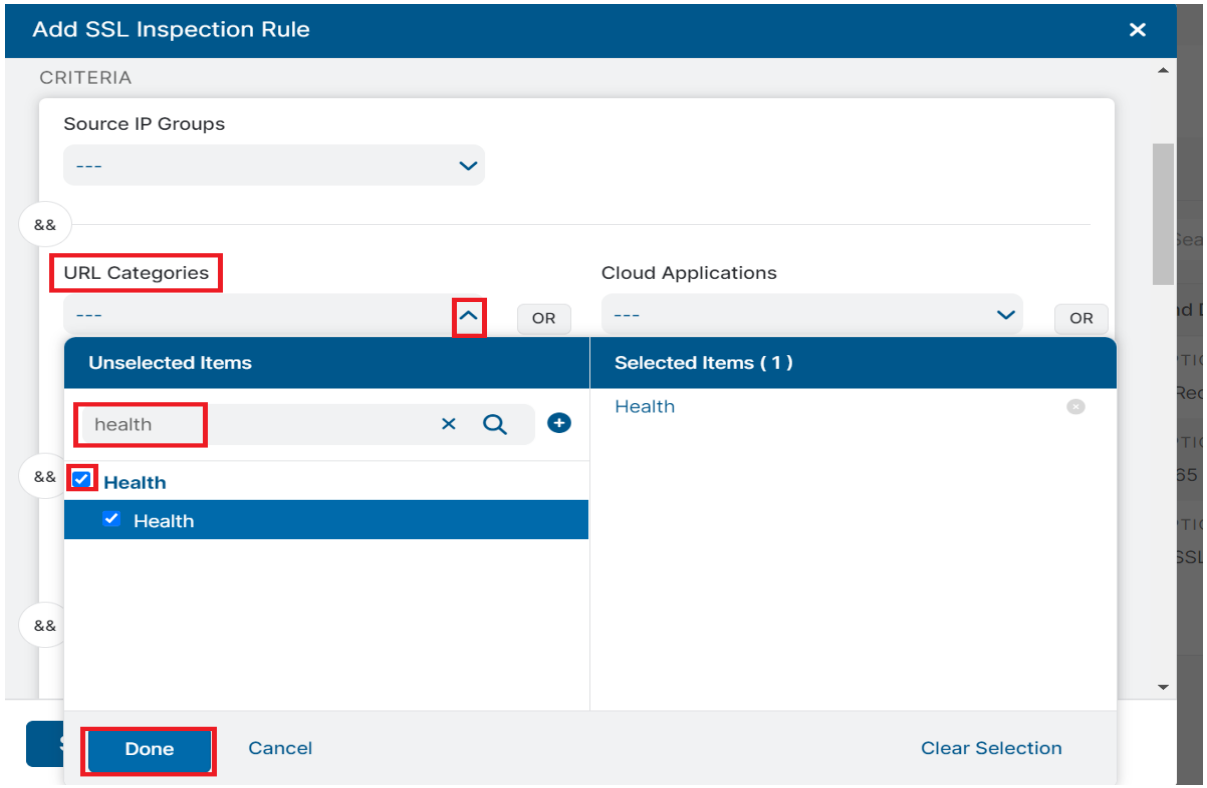


Task 3.2: Enable an SSL Exemption

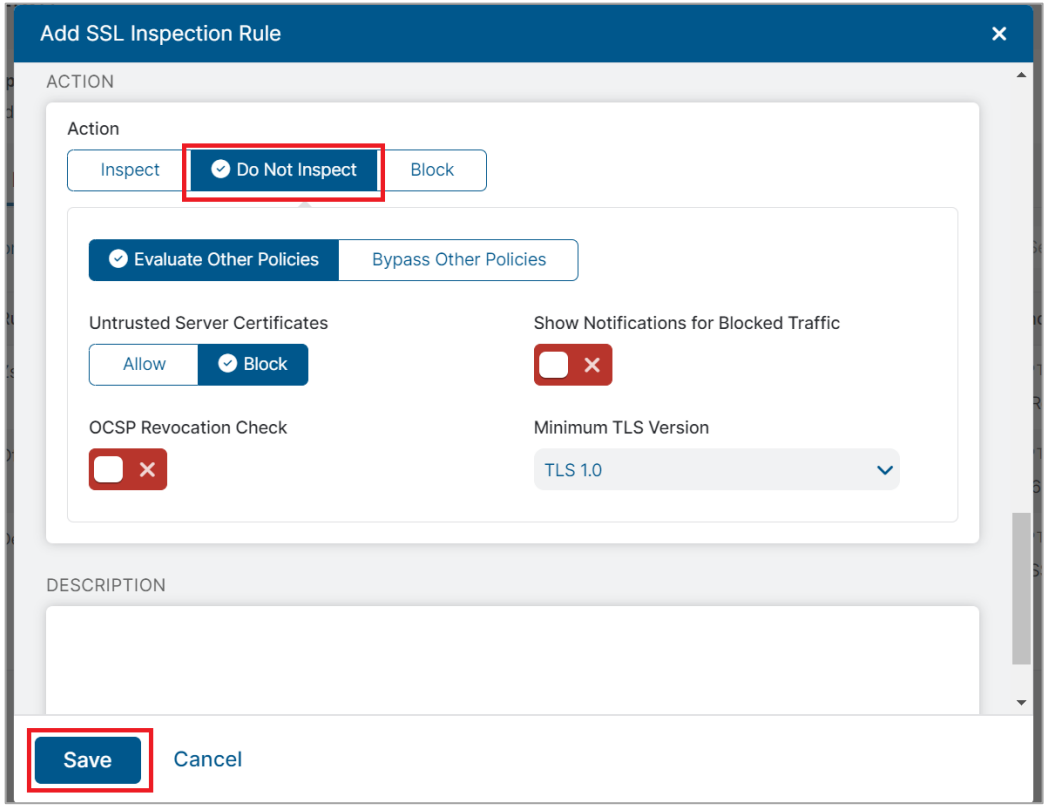
In this task, you will configure a SSL policy that ensures your user's privacy when visiting certain types of websites such as Healthcare and Financial sites you may wish, or even be required by local regulations, to block SSL Inspection for those websites.

1. In a browser on the **Corp 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.
2. Enable SSL Bypass for the Health URL Category:
    a. In the **Zscaler Admin Portal** go to **the Policy > Web > ACCESS CONTROL > SSL Inspection** page.
    b. Click **+Add SSL Inspection** Rule.
    c. Set the Rule Order to **1**.
    d. Change the Rule Name to **SSL Bypass for Health Care**.
    e. In the **Criteria section** select **the URL Categories** drop-down and search for and select the **Health** category. Click **Done**.





f. Scroll down to the ACTION section and under Action, select **Do Not Inspect**.
g. Click **Save** at the bottom of the page.
h. **Activate** your changes.



3. 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, to re-initialize the connection and load the server certificate.*

Lab 4: Configuring Cloud Applications Monitoring

Consider the scenario where your organization has identified an initial set of business-critical cloud applications that need to be configured in ZDX.

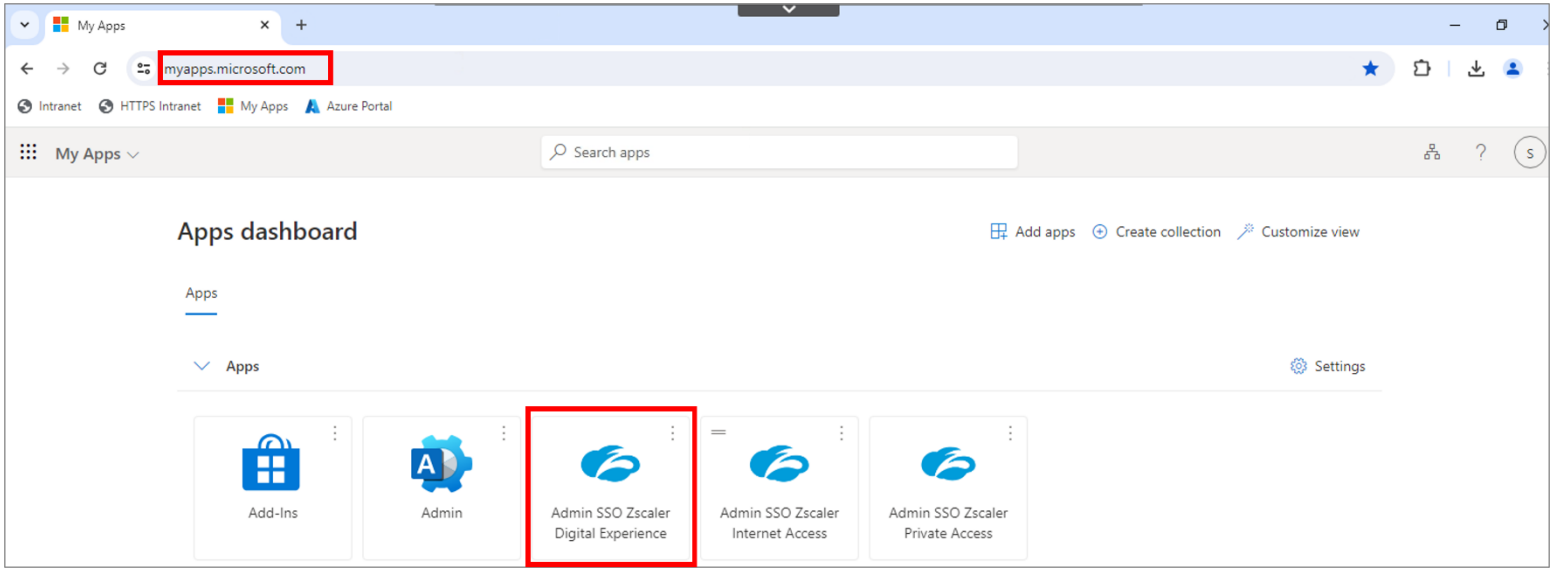
In this lab, you will:

- Enable a predefined cloud application for monitoring, and
- Create a custom application and probes for monitoring.

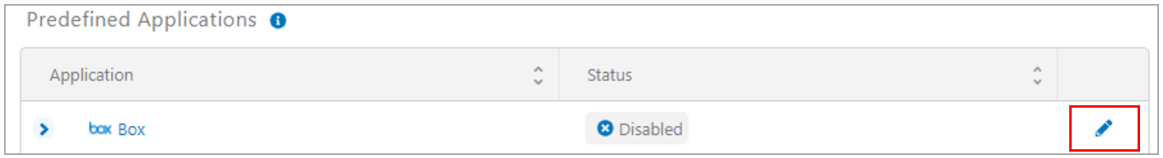
Task 4.1: Enable Predefined Applications

In this task, you will enable a predefined application template for common cloud applications. To enable a predefined application, follow these steps:

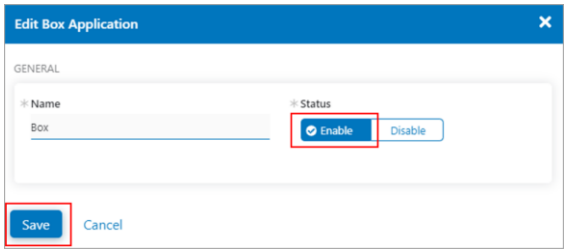
1. In a new browser tab, open the Zscaler Digital Experience Admin Portal by going to **https://myapps.microsoft.com** . You should automatically logon if you're using the Client PC, otherwise use your **student@<Student FQDN>** credential if using your own PC.
2. Click the **Admin SSO Zscaler Digital Experience** tile.



3. From the main menu on the left, select **Configuration**. We will configure the **Box** application. It will either be **pre-configured** and require Enabling, or, it will be **Un-Configured**, and need **Onboarding**.
4. To **Enable** a pre-configured Application:
   a. Click to edit **Box**.

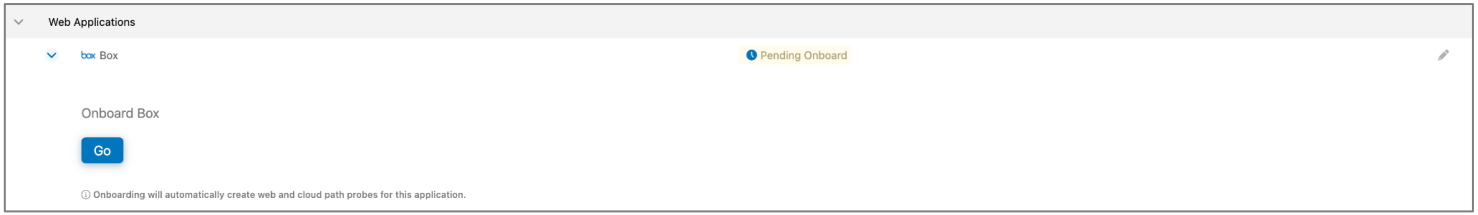


   b. Click **Enable**, then click **Save**.

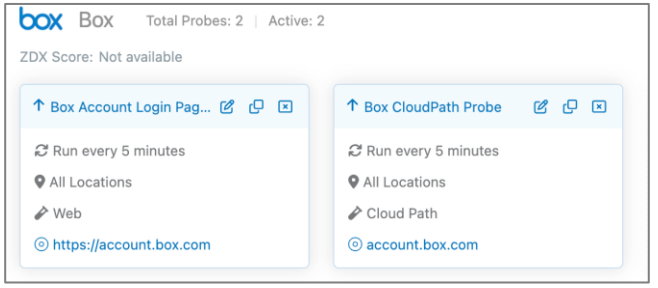


***Note**: The Box application has already been "onboarded", which is a one-time, one-button-click process. In your corporate environments, this step needs to be initially completed.*

5. To **Onboard** un-configured Application, expand the **Box** application, and click **GO**:



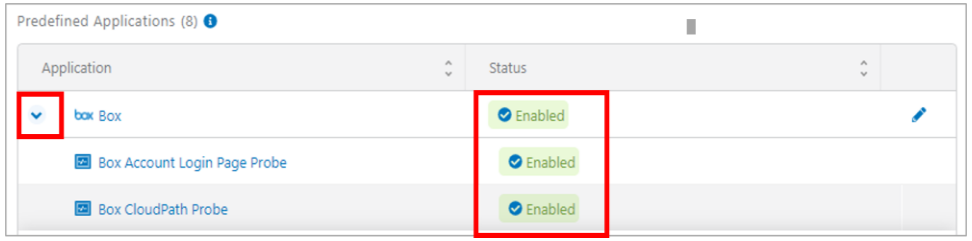
   a. The application will onboard automatically, and you will see the probes created.
   b. Click the **Applications** tab. You should now see the application and its associated probes are now **Enabled**.



Task 4.2: Configure a Custom Application

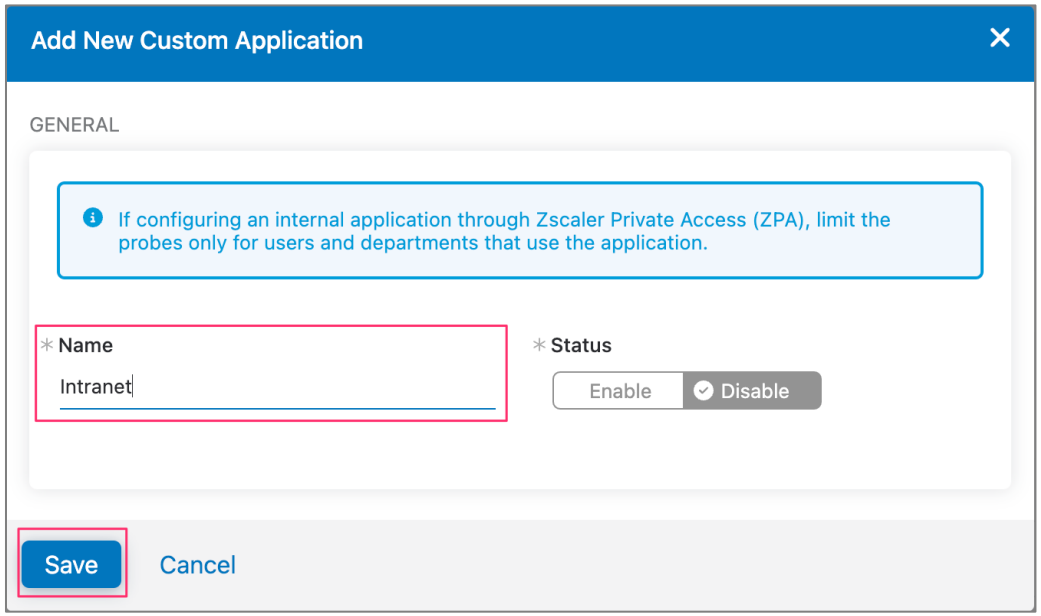
In this task, you will configure a custom application.

1. To configure and enable a custom application, follow these steps:
   a. From the main menu on the left, select **Configuration > Applications**.



   b. Select **Add New Custom Application**.

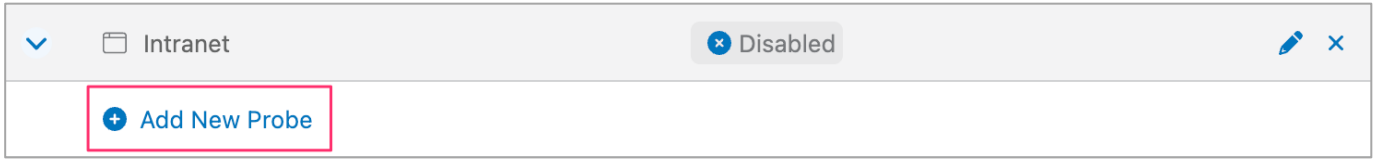
2. Enter a name, **Intranet**, and click **Save**.



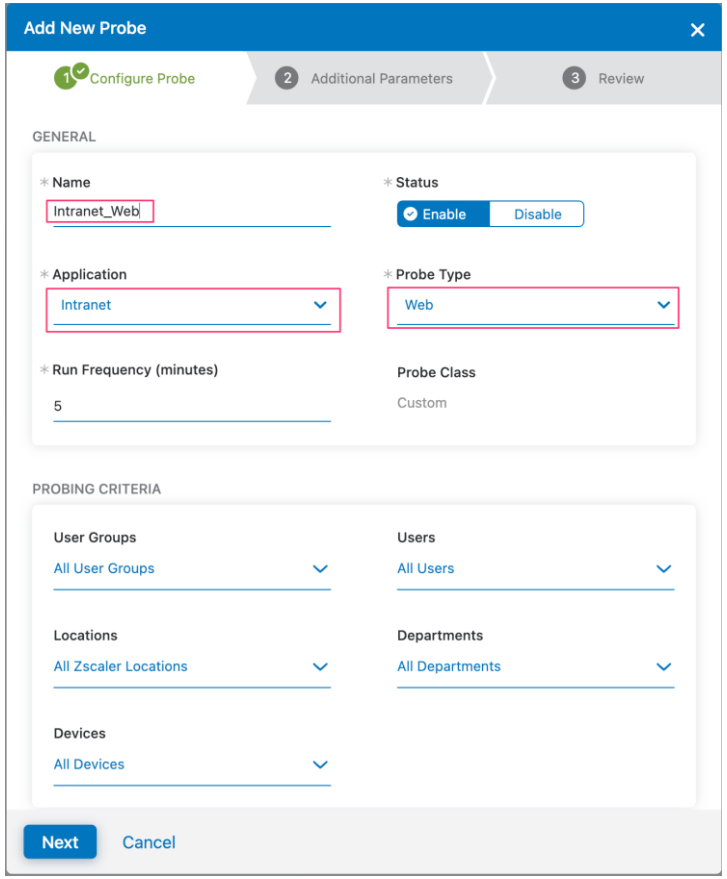
Task 4.3: Create a Custom Probe

In this task, you will configure a probe for the custom application you created in the previous task.

1. To configure a probe, follow these steps:
   a. Under the application you just created, click **Add New Probe**.



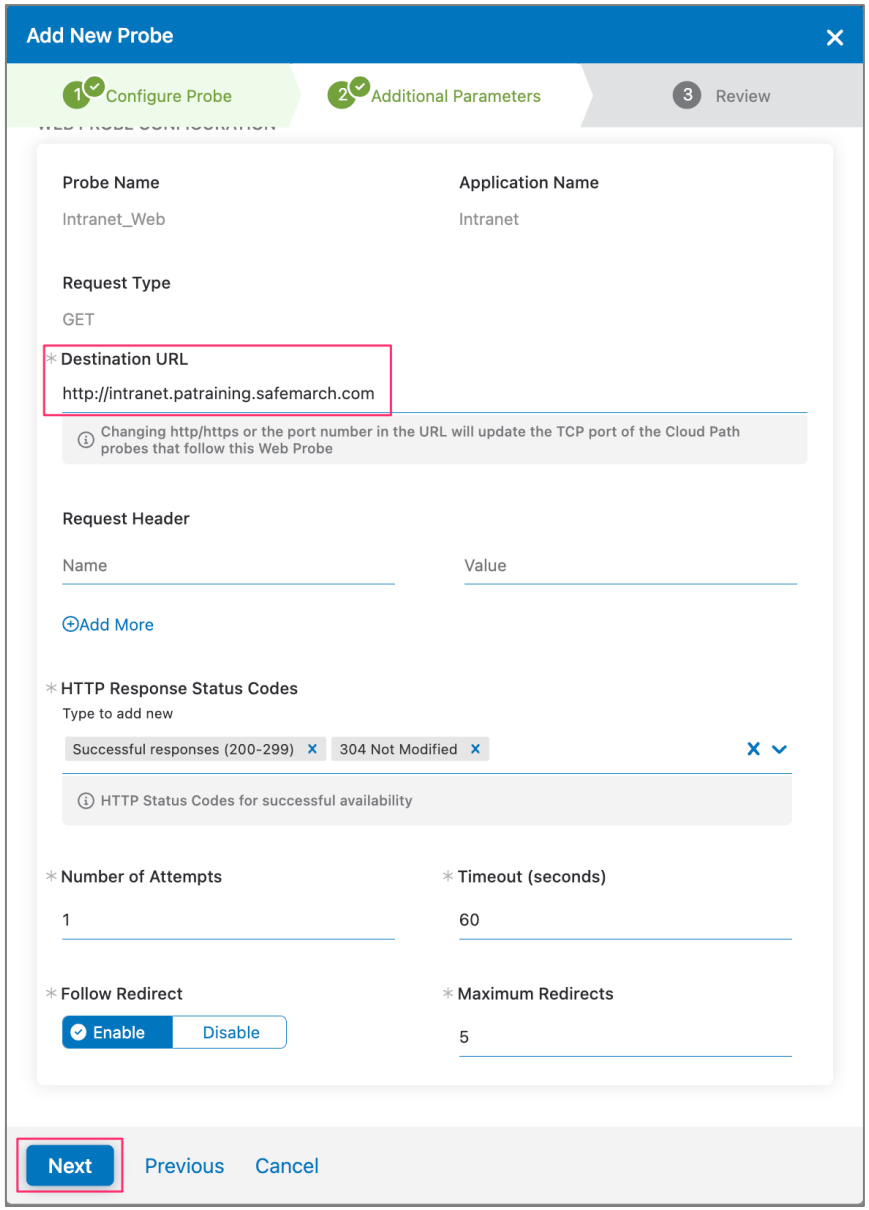
   b. At the **Configure Probe** step of the wizard:
      i. Enter a name, e.g. **Intranet_Web**.
      ii. The **Application** should already be populated with **Intranet**.
      iii. The **Probe Type** should already be populated with **Web**.



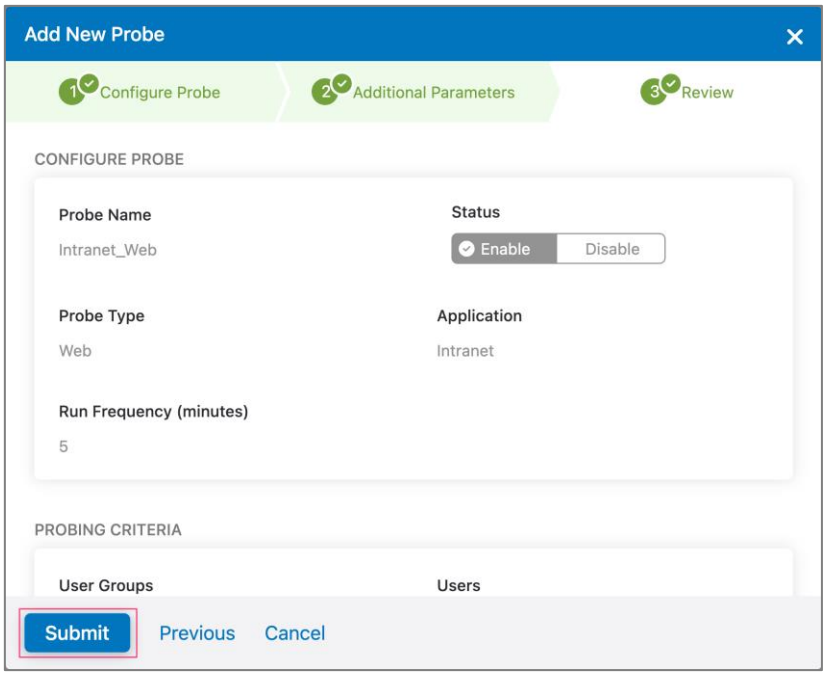
   c. Click **Next**.

d. At the **Additional Parameters** step of the wizard, in the Destination URL field, enter: **http://intranet.patraining.safemarch.com**

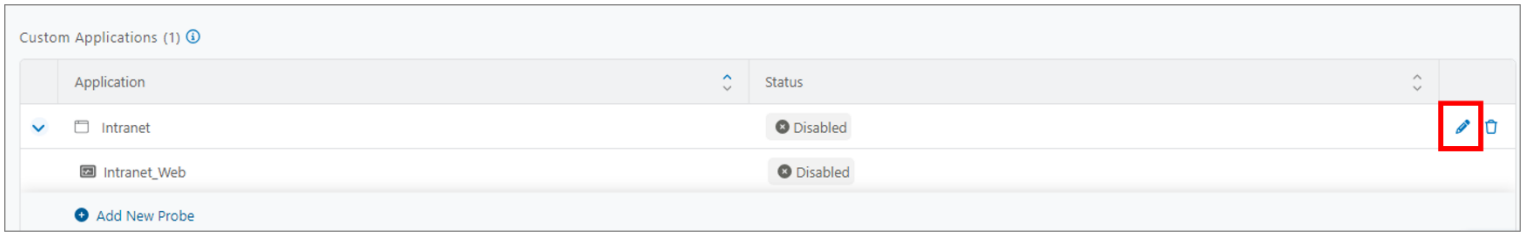
e. Click **Next**.



f. Review the configuration settings, then click **Submit**.

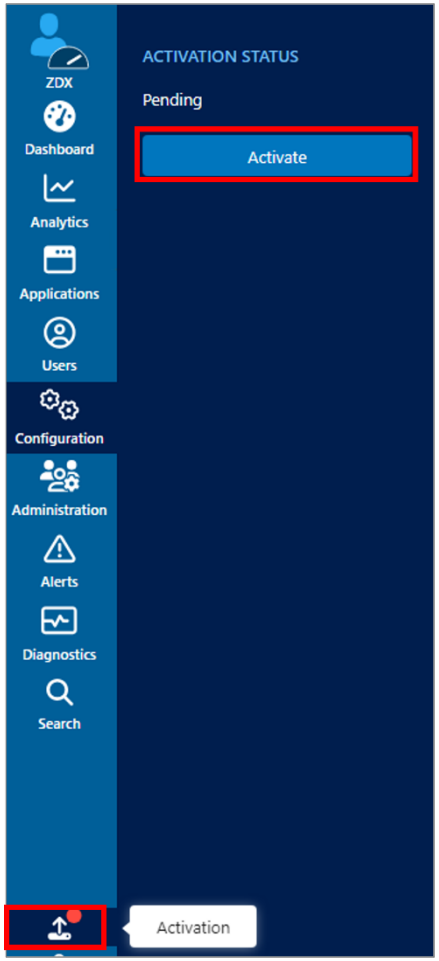


g. Go to **Configuration > Applications** and click to edit the Intranet application.

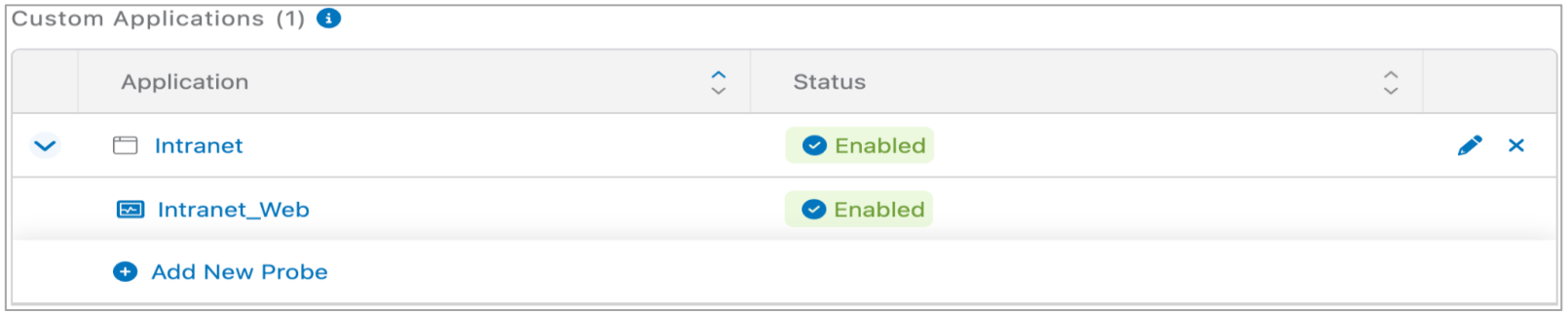


h. Click **Enable** and then click **Save**.

i. From the main menu, select **Activation** and then click **Activate**.

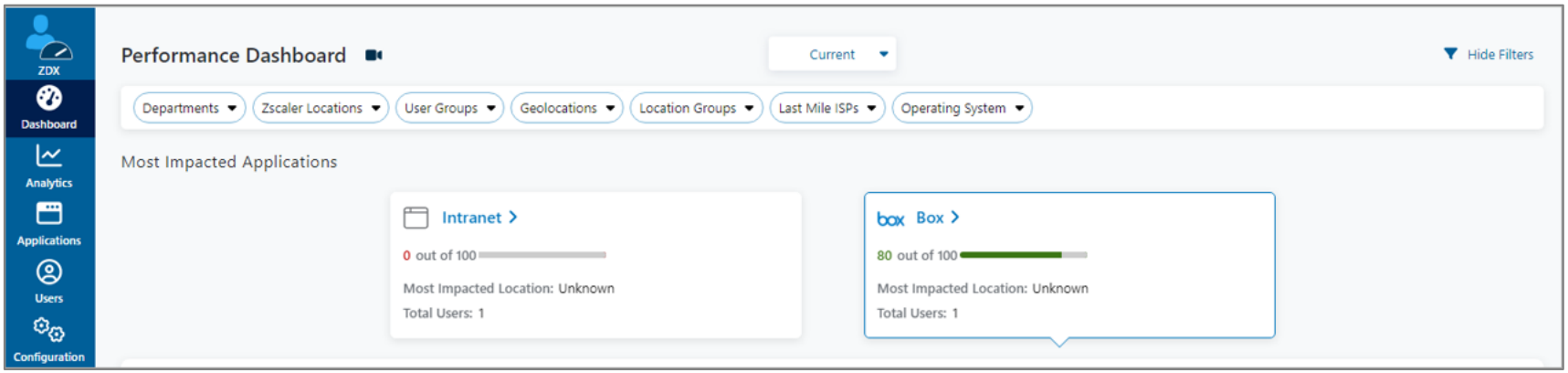


2. Verify that the custom application is now enabled.
   a. At the top of the screen, click **Applications**.
   b. Verify that the new custom application is listed as **Enabled**.



***Note**: Depending on your organization's ZDX plan, it may take 15-30 minutes for a newly configured application to start reporting metrics. We suggest you move on to the next lab and then return to the step listed below.*
Also, the Intranet application you created earlier will show a ZDX score of 0, until you have configured all required ZPA infrastructure components, including App Connector and Access Policies.

3. Click **Dashboard > Performance Dashboard** on the main menu and verify that Box and the custom Intranet application are now included in the reports.



Lab 5: Configuring Access Control Policies

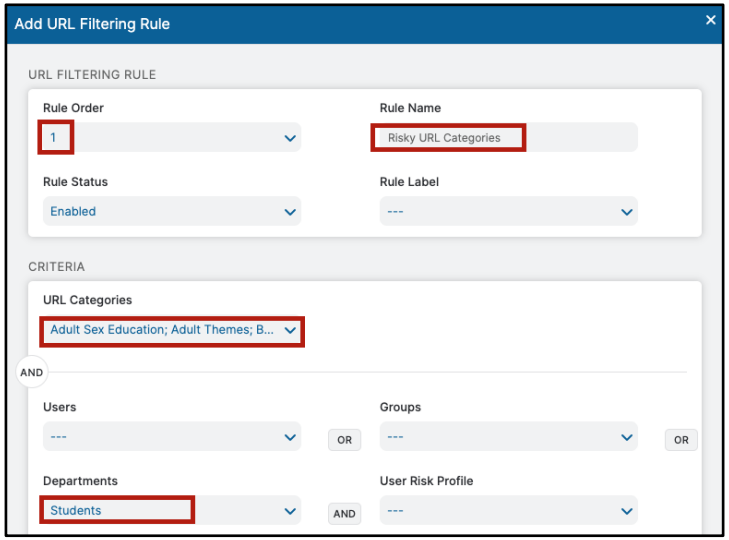
In this lab, consider the scenario where your organization has deployed the Zscaler service and access control policies need to be configured to protect users from exposure to risky locations, applications, or file downloads:

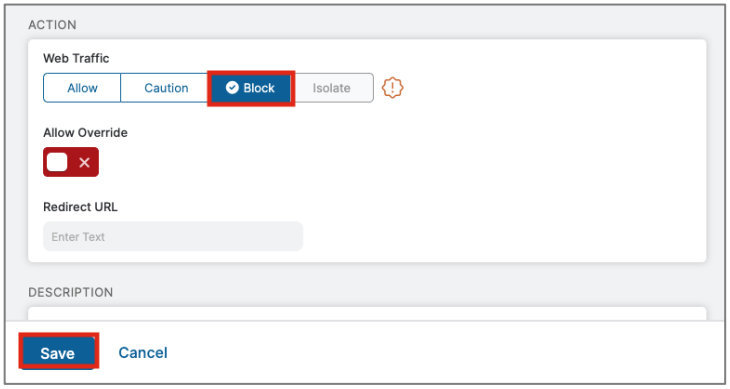
- Block access for a URL that is risky for a specific group of users;
- Restrict access to applications that are not needed for business use to limit potential threats;
- Block the download of Windows executable files from URLs that are not known to be trustworthy; and
- Exempt a URL from being scanned.

Task 5.1: Configure URL Filtering Rule

In this task, you will add a URL filtering rule to block users who access URLs in the Shopping and Auctions and Adult Material categories.

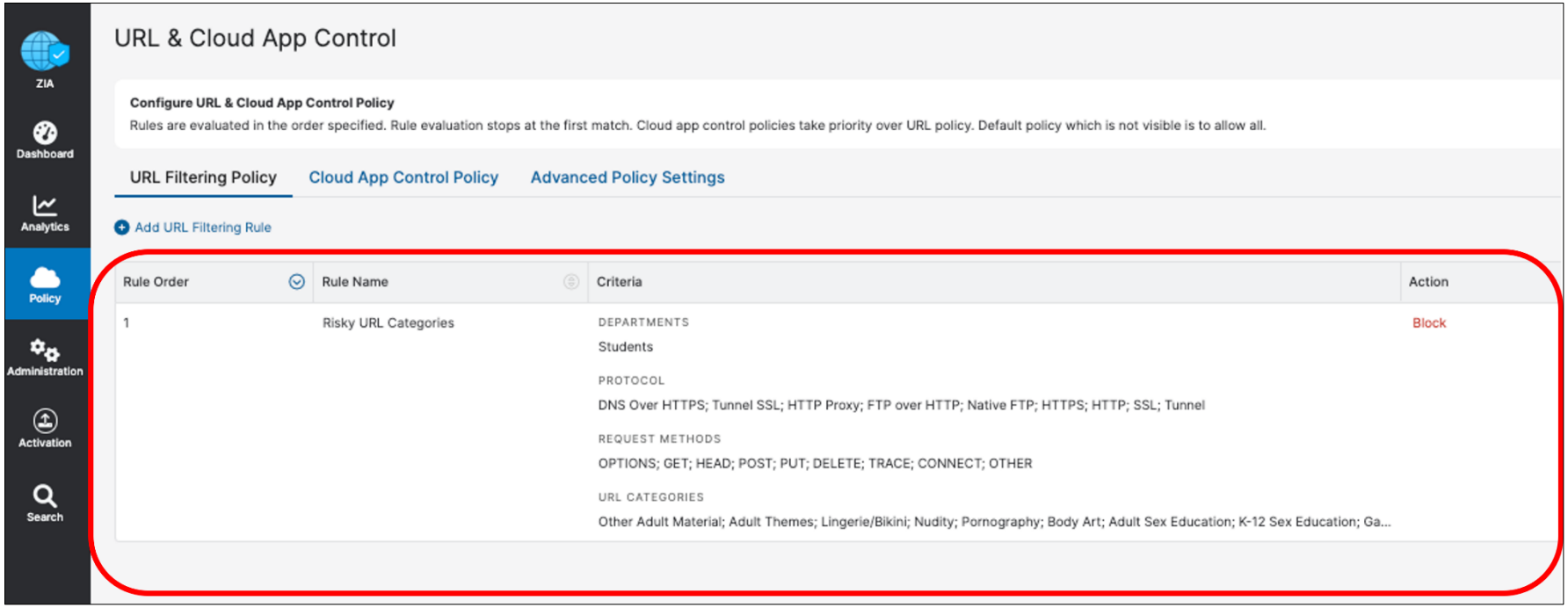
1. In the ZIA Admin Portal, go to **Policy > ACCESS CONTROL > URL & Cloud App Control > URL Filtering Policy**.
2. Click **+Add URL Filtering Rule** and set:
    a. Rule Order: **1**.
    b. Rule Name: **Risky URL Categories**.
    c. URL Categories: Select the URL Category Groups:
        i. **Adult Materials**
        ii. **Gambling**
        iii. **Shopping and Auctions**
        Click **Done** after all categories are selected.
    d. Department: **Students**.
    e. Action – Web Traffic: **Block**.
    f. Click **Save.**
    g. **Activate** the change to have it applied immediately to all users.



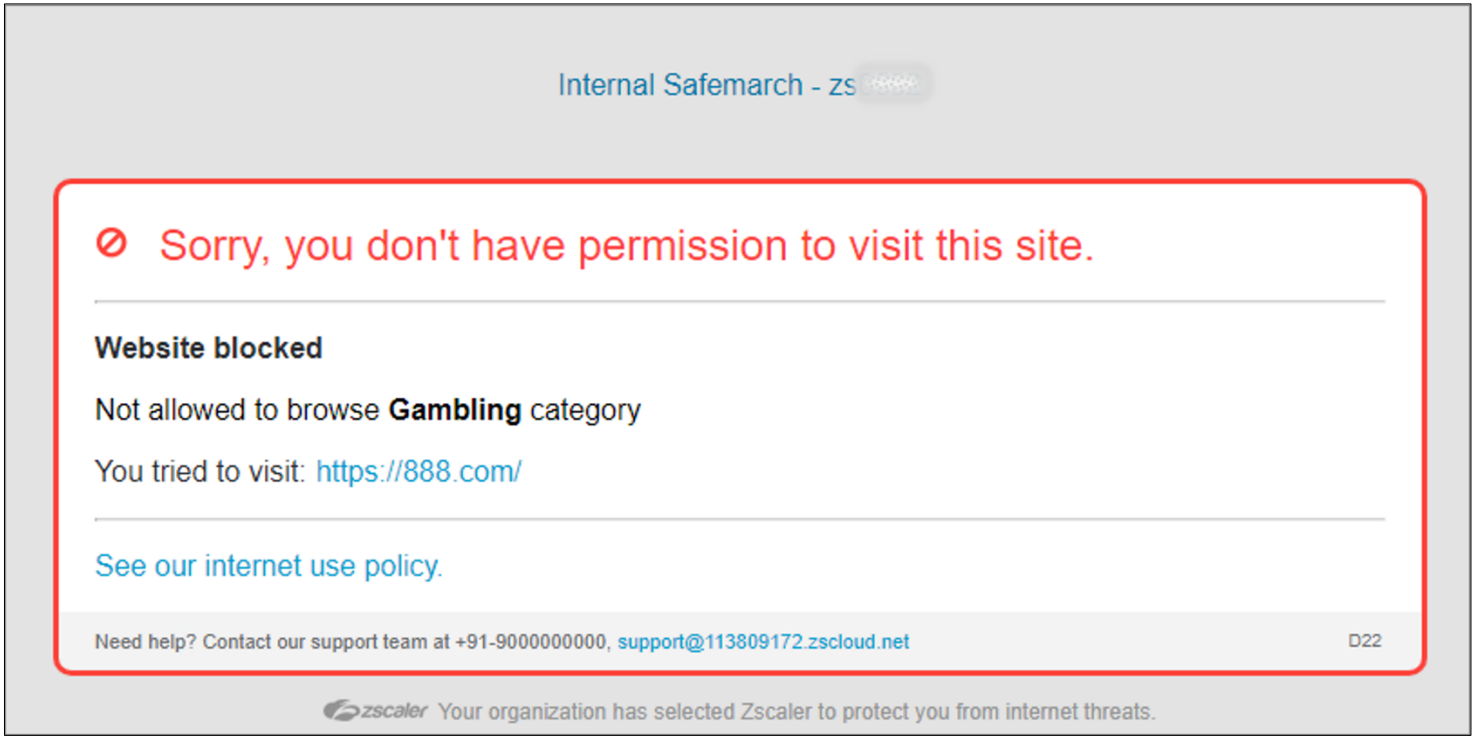


3. Verify that the Risky URL Categories rule appears at #1 in the rule order.

***Note**: Rules are evaluated top down starting at #1 and the first rule that matches is applied. Recommended best practice is to place the rules with the most specific matching criteria above rules with less specific matching criteria.*

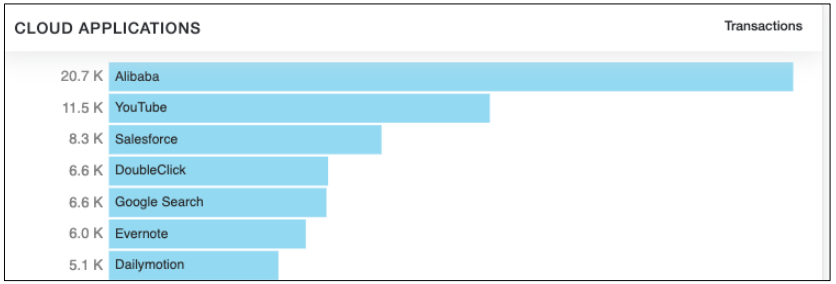


4. On the Windows Client PC, verify that you no longer have access to online shopping or gambling sites.
   a. Browse to **ebay.com** or **888.com**



Task 5.2: Configure Cloud App Control

In this task, you will investigate an issue with an unsanctioned application. The CIO at Safemarch has expressed concern about this week's CIO report showing that the top used cloud application for the week is Alibaba.



Note: *This is an example, you will not see the same data on your ZIA tenant in the training lab. On an operational system this would be viewable via Analytics -> Interactive Reports -> Cloud Applications).*

You are tasked by the CIO to look into this, and your investigation shows that URLs accessed with Alibaba classify mainly into Online Shopping and Business Use (both currently Allowed), and Adv. Security Risk (which would be blocked by the Advanced Threat Protection policy for Suspicious Destinations Protection).

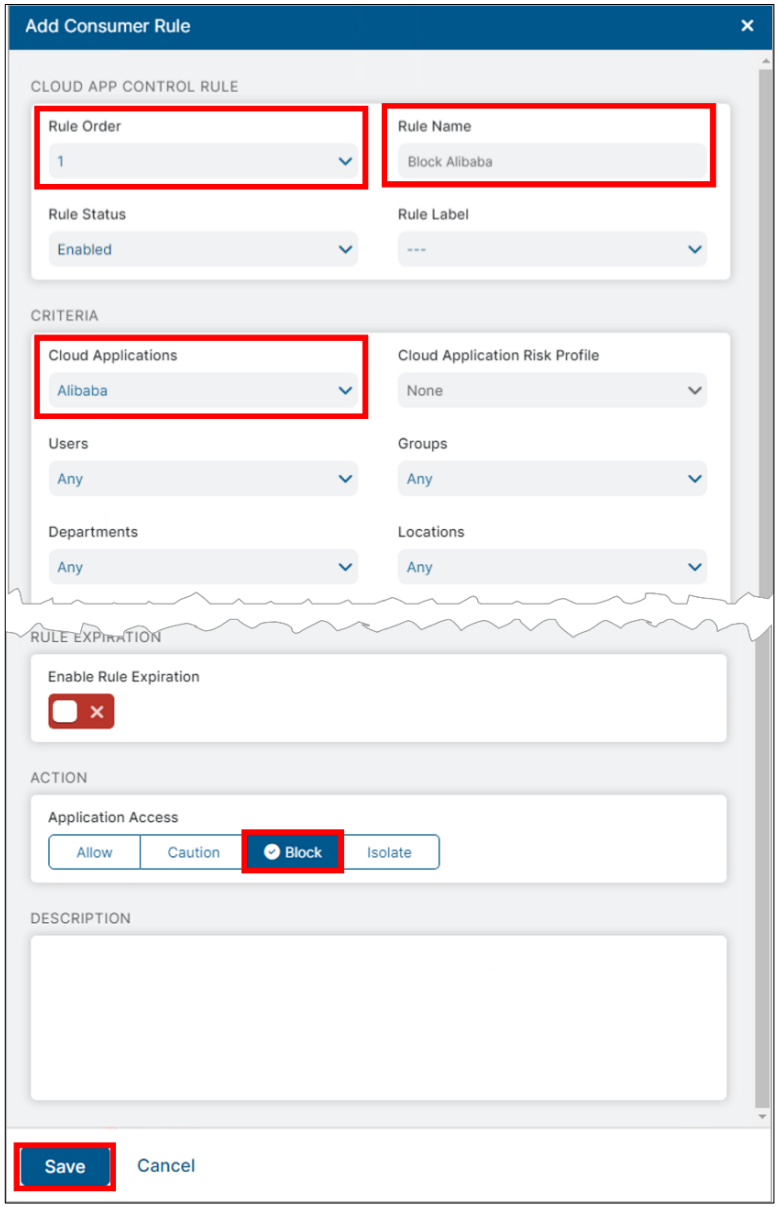
Insights Logs

Aug 18, 2019 09:06:50 PM - Aug 19, 2019 10:34:37 PM
1000 Log Records Found

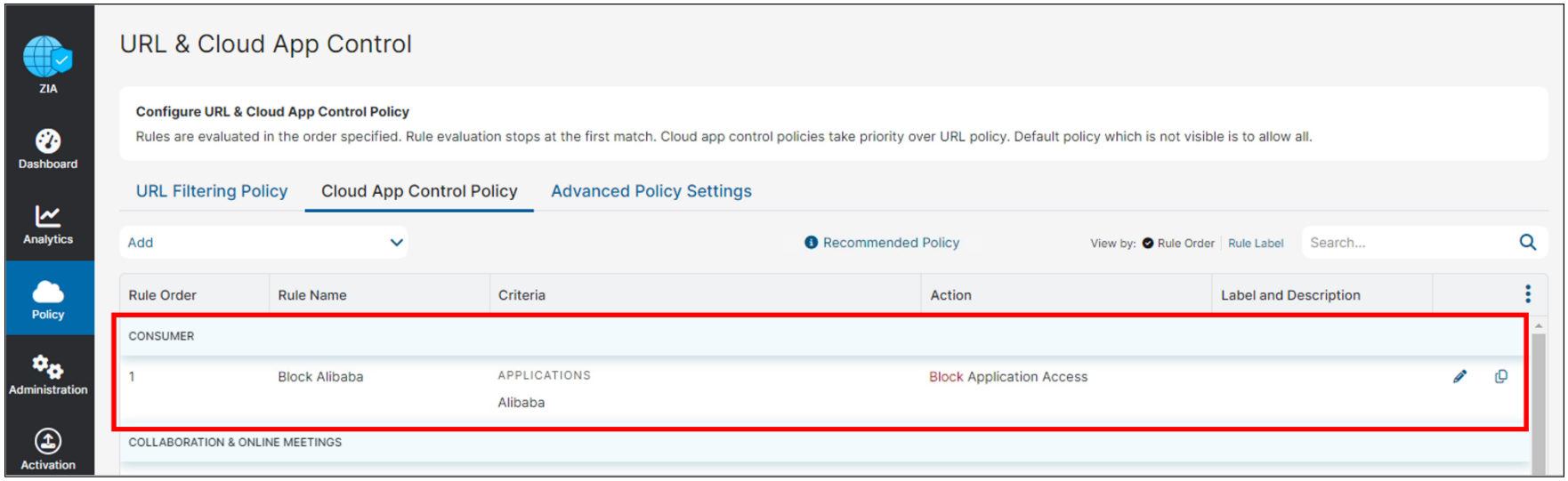
Policy Action	URL	URL Category	URL Class	Cloud Application
Allowed	aliexpress.com/	Online Shopping	Productivity Loss	Alibaba
Allowed	ae01.alicdn.com/kf/htb1rtuzkifpk1rj...	Other Business and Economy	Business Use	Alibaba
Allowed	img.alicdn.com/imgextra/i1/225515...	Other Business and Economy	Business Use	Alibaba
Allowed	img.alicdn.com/imgextra/i2/757937...	Other Business and Economy	Business Use	Alibaba
Allowed	img.alicdn.com/imgextra/i3/871886...	Other Business and Economy	Business Use	Alibaba
Allowed	img.alicdn.com/imgextra/i1/871886...	Other Business and Economy	Business Use	Alibaba
Country block outbound request: n...	ykimg.alicdn.com/develop/image/2...	Suspicious Destination	Adv. Security Risk	Alibaba
Country block outbound request: n...	ykimg.alicdn.com/develop/image/2...	Suspicious Destination	Adv. Security Risk	Alibaba

Based on your findings and recommendation the CIO has requested that a policy be applied to block access to Alibaba since it is not required for the conduct of the business of Safemarch and is sometimes trying to access suspicious destinations.

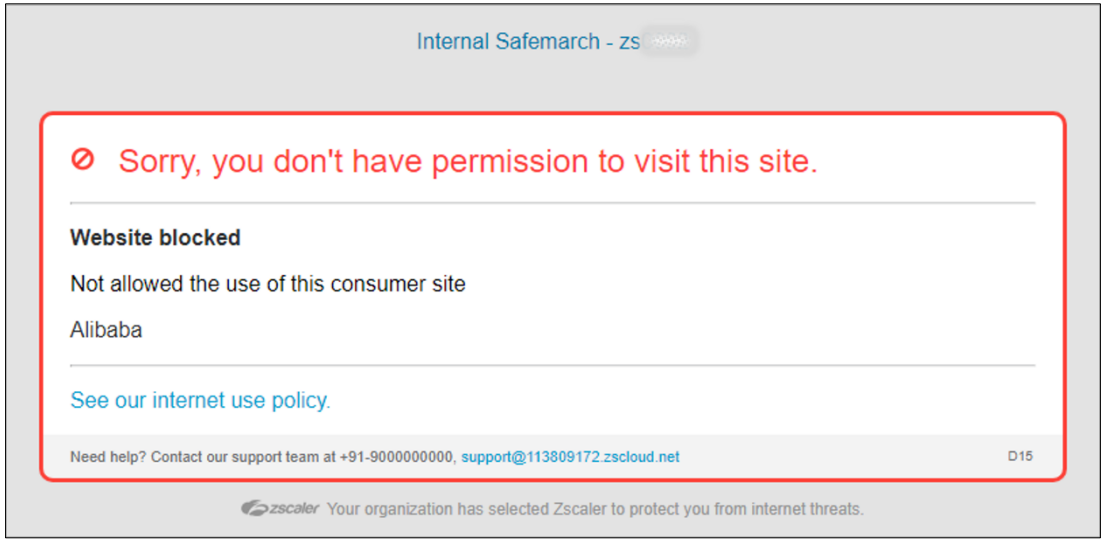
1. Add a Cloud App Control policy to block the Alibaba cloud app:
    a. Go to **Policy > URL & Cloud App Control**.
    b. Click the **Cloud App Control Policy** tab.
    c. Click the **Add** dropdown list.
    d. Select **Consumer**.
    e. Configure the following:
        i. Rule Order: **1**
        ii. Rule Name: **Block Alibaba**
        iii. Criteria - Cloud Applications: **Alibaba**
        iv. Action – Application Access: **Block**
    f. Click **Save**.
    g. **Activate** the change to have it applied immediately to all users.



2. Verify that the new rule has been added in the Consumer rules list to block application access to Alibaba.



3. Verify on the **Client PC** that access to alibaba.com is blocked.



Lab 6: Provisioning ZPA Infrastructure

In this lab, you will deploy an *App Connector* in the data center, which will establish the connection to the Zero Trust Exchange. The Zscaler Client Connector will connect to the ZTE, which will broker the connections for applications.

Users will connect to applications using the Zscaler Client Connector, previously installed on the Corp: Client PC. Applications are hosted on the Windows server in the Data center, so an App Connector is required to run on Corp: ZPA Connector VM.

Task 6.1: Provision an App Connector

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

1. Go to the VM labelled **Corp: Win Svr 2016** and login to Windows as the user **PATRAINING\Administrator** with password **Admin-123!**
2. Open Chrome, go to **https://myapps.microsoft.com** and log using the credentials assigned to you in the student access information that you received (**student@<Student FQDN>**). Sign in to **Admin SSO Zscaler Private Access**.

Note: *For this lab, you must access the ZPA Admin Portal in a browser on the* ***Windows 2016 server****, as you will need to upload a provisioning key to the App Connector VM using WinSCP.*

---

3. Go to the App Connectors page:
   Configuration & Control > Private Infrastructure > App Connectors.
4. Click the **Add App Connector** icon near the **top right** to add a new App Connector and step through the wizard as follows:
   a. Select **Create a new provisioning key** and click **Next**.

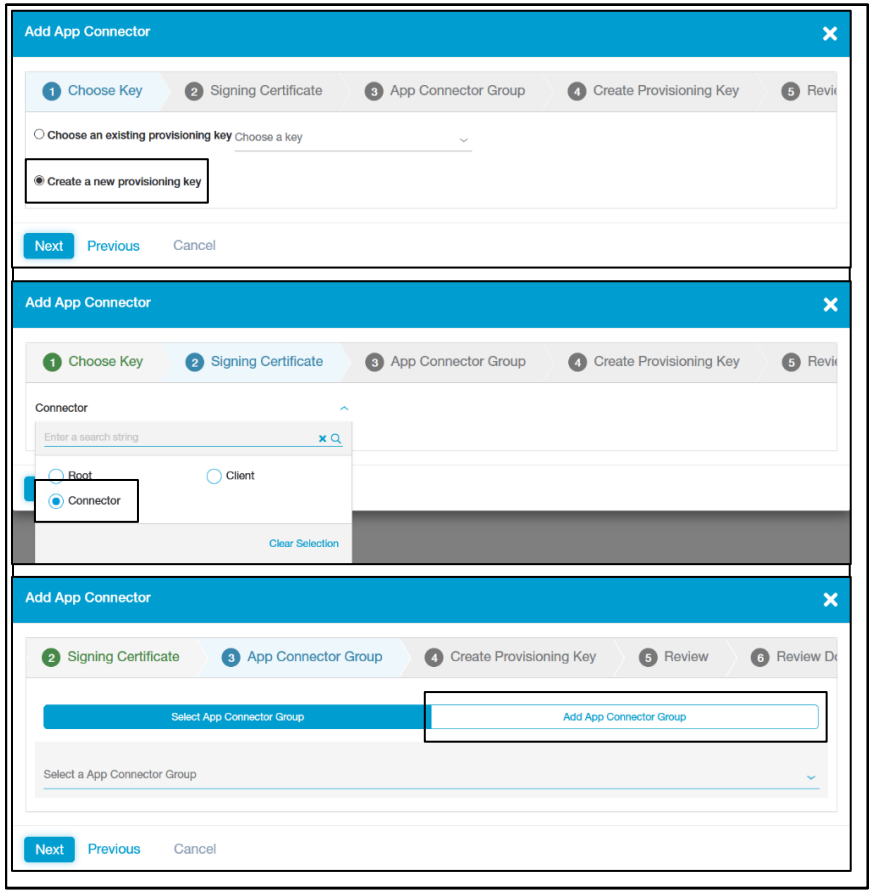
   b. Click **Select a certificate** and select the certificate named **Connector**, then click **Next**.

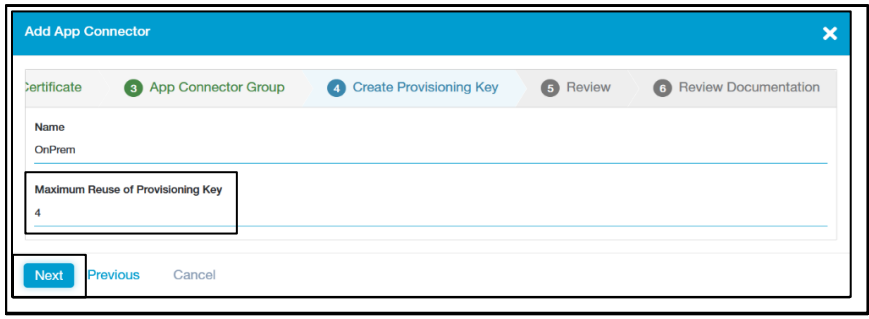
   c. Click **Add App Connector Group**.

   d. Name the group **OnPrem** and confirm that it is **Enabled**, add a description if you wish, leave the **IPv4 and IPv6 DNS Resolution** option unchanged, set the **App Connector Software Update Schedule** to occur on **Sundays** at **00:30**, and specify the location as **NYC, NY, USA**, then click **Next**.

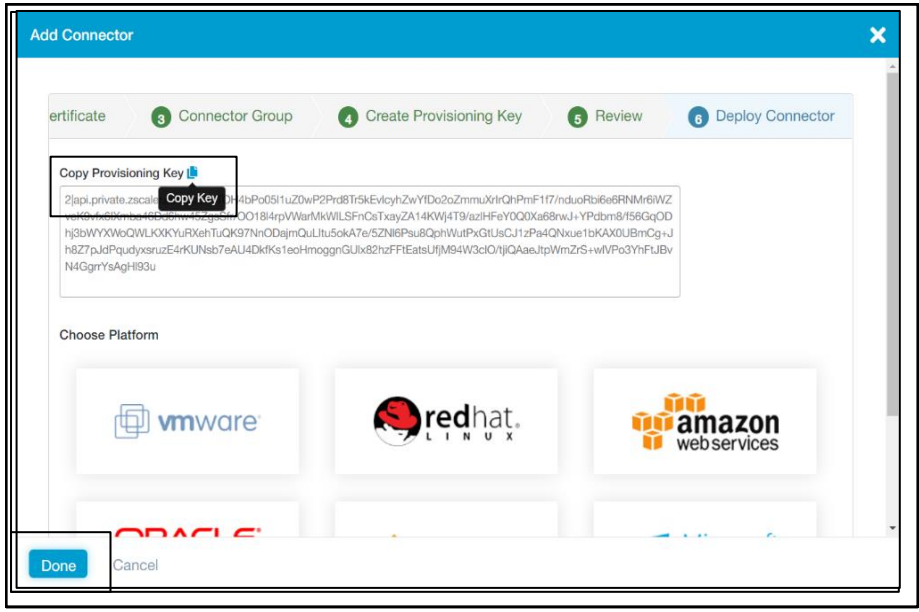
   e. Give the **Provisioning Key** the name **OnPrem** and specify a **Maximum Reuse of Provisioning Key** of **4**, then click **Next.**

   f. Review the App Connector settings and click **Save.**





5. Copy the provisioning key and save it to a file for transfer to the connector.
   a. By the **Copy Provisioning Key** text, click the **Copy icon** and confirm that the browser may access the data (it should show the caption **Copied!**).



*Alternatively, you can right-click and select **all data** in the **Copy Provisioning Key** field, then right-click again and select **Copy**.*

   b. Click the Windows **Start** menu, type **Notepad** and open that application, right-click and select **Paste** to paste the **Provisioning Key** text into the file.

   c. Save the file to the desktop with the name "**provision_key**" (save as with quotes around the filename will prevent Notepad adding a .txt extension and close Notepad.

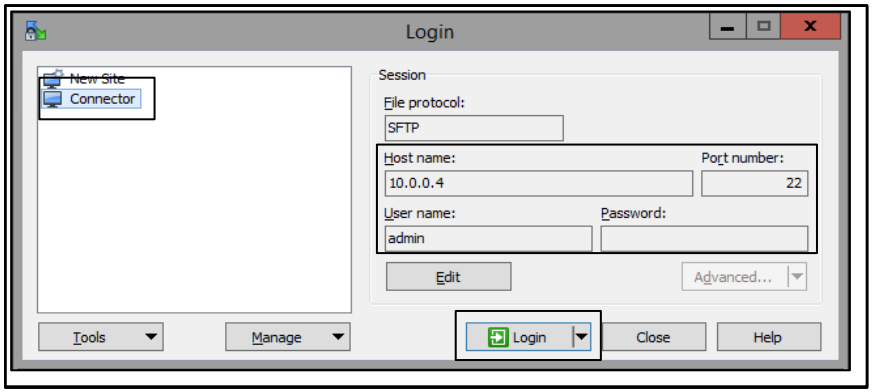
   d. Back in the ZPA Admin Portal, scroll down if necessary and click **Done**.

6. Click the **App Connector Groups** tab and confirm that the group has been created. Click on the name of the group to review details.
7. Click the **App Connector Provisioning Keys** tab to confirm that a key has been created to support a maximum of 4 App Connectors.

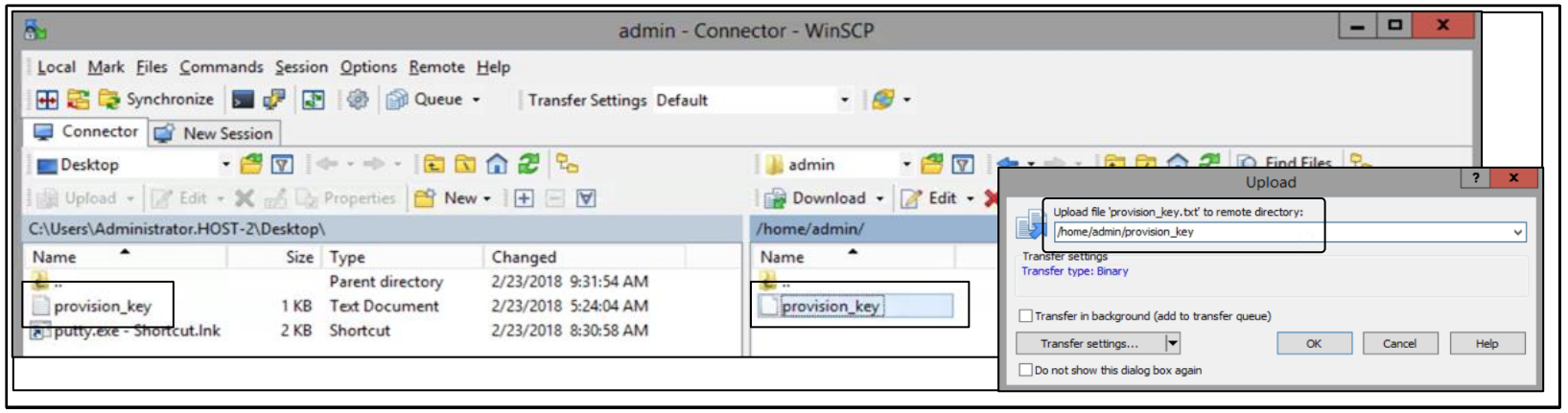
Task 6.2: Activate the App Connector

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

1. On the VM labelled **Corp: ZPA Connector**, login with the default username / password (**admin / zscaler**).
2. Start the **SSH Daemon** on the App Connector by entering the command: **sudo systemctl start sshd** (enter the password **zscaler** when prompted).
3. Verify that the **SSHD Daemon** has started using the command **sudo systemctl status sshd**, confirm that status is **active (running)**.
4. On the VM labelled **Corp: Win Svr 2016**, copy the provisioning key file to the Connector:
    a. Start **WinSCP** using the icon on the desktop or in the taskbar:
    b. Load the saved session named **Connector** (IP address **10.0.0.4**, Port **22**) and click **Login**.
    c. Login to the App Connector using the default user password (**zscaler**), accept the certificate if necessary.
    d. In the left-hand panel of WinSCP (the local Windows server), navigate to the **Desktop** folder and select the file **provision_key**.
    e. Right-click on the file and select **Upload**.
    f. Specify the path on the App Connector as /**home/admin /provision_key** and click **OK**.



Caution! *The name of the file is critical to the correct loading of the provisioning key; it is* ***case-sensitive*** *and must be named exactly* ***provision_key****.*



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

6. On the VM labelled **Corp: ZPA Connector**, stop the **SSH Daemon** on the App Connector by entering the command: **sudo systemctl stop sshd** (enter the password **zscaler** if prompted). Check that the **SSHD Daemon** has stopped using the command **sudo systemctl status sshd**.

Note: *For security reasons it is recommended to* ***not*** *leave the SSH Daemon running.*

---

7. Activate the App Connector with the new provisioning key file:
    a. First identify the current directory with the command **pwd** (you should be in **/home/admin**).
    b. List the contents of the directory with the command **ls** and confirm that the file **provision_key** is there.
    c. Stop the **App Connector** service with the command **sudo systemctl stop zpa-connector** (enter the password **zscaler** if prompted).
    d. Copy the file to the correct Zscaler directory using the command **sudo cp provision_key /opt/zscaler/var/**

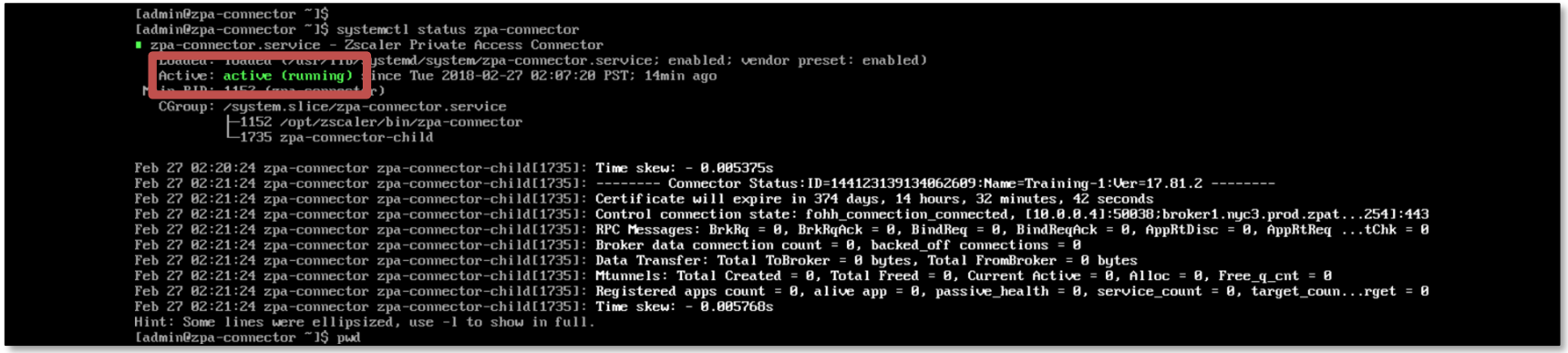
Caution! *The name of the file is critical to the correct loading of the provisioning key; it is case sensitive and is* ***provision_key*** *NOT provision_key.txt!*

---

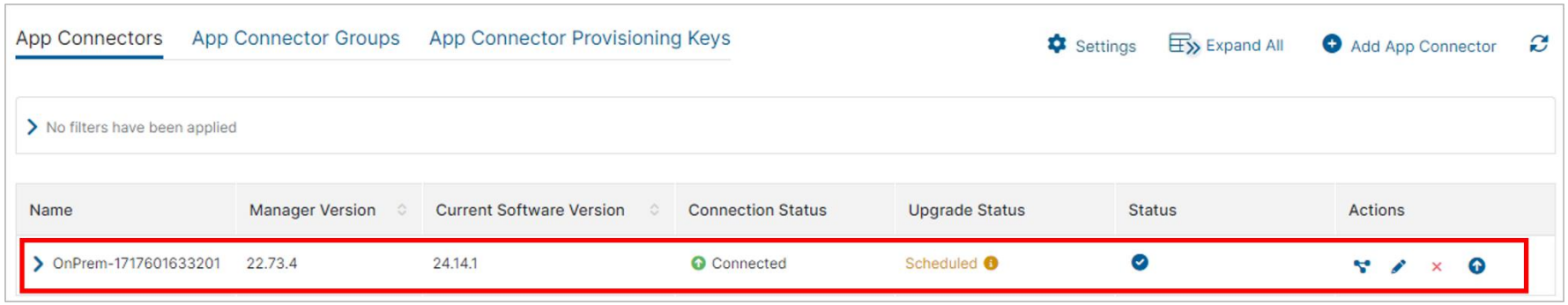
    e. Check that the file is there using the command **sudo ls /opt/zscaler/var/**
    f. Now restart the App Connector service with the command **sudo systemctl start zpa-connector**
    g. Enable the App Connector to auto start on boot with the command **sudo systemctl enable zpa-connector**

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

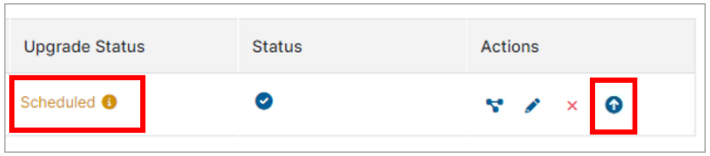
Note: *You should now see a set of key and certificate .pem files.*



9. On the VM labelled **Corp: Win Svr 2016**, in the ZPA Admin Portal, navigate to the **Configuration & Control > Private Infrastructure > App Connectors** page and confirm that the App Connector is listed.

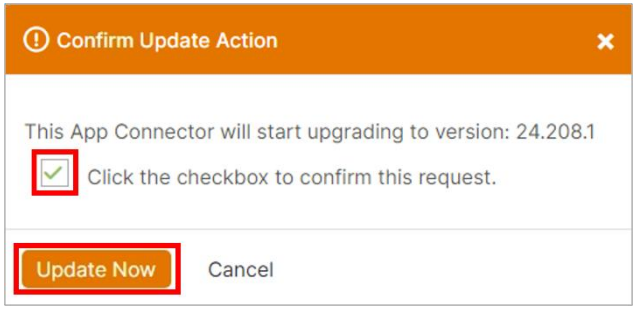


10. Check the **Update Status** field for the App Connector. If it is blank, or indicates **Failure**, navigate away from the page and come back to it in a couple of minutes; the status should change to either **Success** or **Scheduled**:



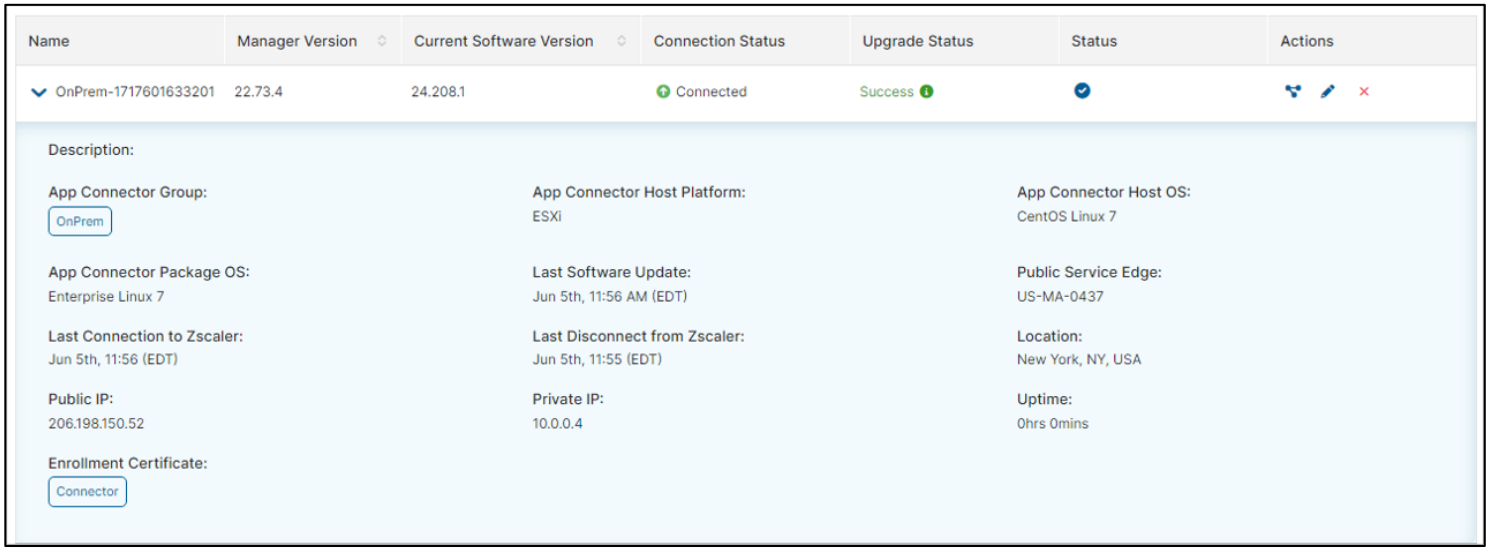
    a. If it indicates **Success**, this means that the App Connector is at the latest version of software and no update is necessary.
    b. If it indicates **Scheduled**, this means that a software update is required and will take place automatically at the next scheduled update interval for the **Connector Group**.

11. To manually start the update immediately:
    a. Click the **Update Now** control for the App Connector, in the pop-up window click in the check box to confirm the request, then click **Update Now**.
    b. Return to the **Connector** page in a few minutes to verify that the update is complete.



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

12. Click the name of the App Connector to expand details for it and review the information available.



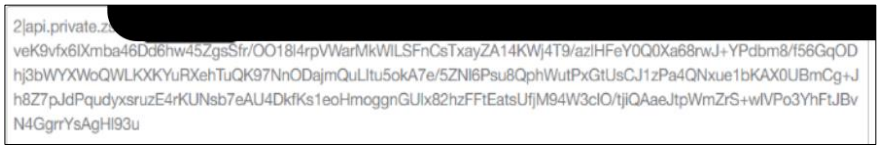
13. On the VM labelled **Corp: ZPA Connector**, it is recommended that you change the admin user password on the App Connector to a more secure value:
    a. Enter the command **passwd**.
    b. Enter the current password: **zscaler**.
    c. Enter the new password: **Zscaler-123!**
    d. Re-enter the new password.
    e. Enter the command **exit**.
    f. Log back into the App Connector VM using the new password.
    g. Once you have confirmed that you can log in successfully with the new password, log back out using the command **exit**.

Task 6.3: Troubleshoot App Connector Enrollment

The App Connector should enroll seamlessly with the provisioning key you've created. Problems occur if the provisioning key is not copied across correctly, named correctly, or has the incorrect file permissions.

In this task, you will explore CLI commands, that you can use if, after restarting the ZPA-CONNECTOR service, you do not see files being created in /opt/zscaler/var , perform the following steps:

1. Ensure the App Connector can resolve and connect to the Internet:
    a. **dig any.broker.prod.zpath.net** should resolve to public DNS entries.
    b. **curl https://admin.private.zscaler.com** should connect and return contents.



2. Check the contents of **/home/admin/provision_key** . It should be of a format beginning with a single digit and a pipe | followed by a Zscaler cloud name followed by a pipe | and approximately 1000 alphanumeric characters.

3. Check the contents of **/opt/zscaler/var** - it is easiest to clear this folder out and restart the enrollment process if you are in any doubt
    a. **sudo rm -rf /opt/zscaler/var/***

> ***Note**: Make sure you enter this command correctly to avoid deleting incorrect files.*

4. Copy the provision key back into the directory. This needs to be done using SUDO to put the correct file permissions on
    a. **sudo cp /home/admin/provision_key /opt/zscaler/var/provision_key .** We're explicitly setting the source and destination file name here to ensure it is named correctly.

5. Restart the ZPA service. This will trigger the provisioning key to be re-read, and the connector enrolled
    a. **sudo systemctl restart zpa-connector**

6. If this fails to enroll, you may have invalidated the provisioning key during creation. Recreate the provisioning key and App Connector group and start again.

Lab 7: Add a Corporate Application

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

Task 7.1: Add an Intranet Application

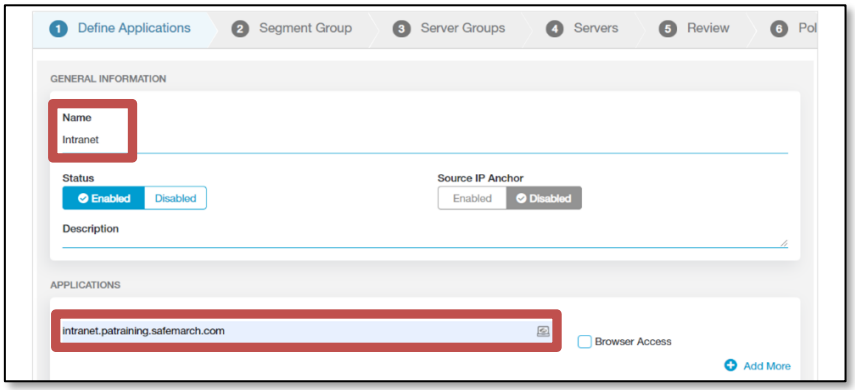
In this task, you will manually add an Application Segment for access to the corporate Intranet server on TCP ports 80 and 443.

1. In the **ZPA Admin Portal**, and go to the **Application Segments** page.
   Resource Management > Application Management > Application Segments

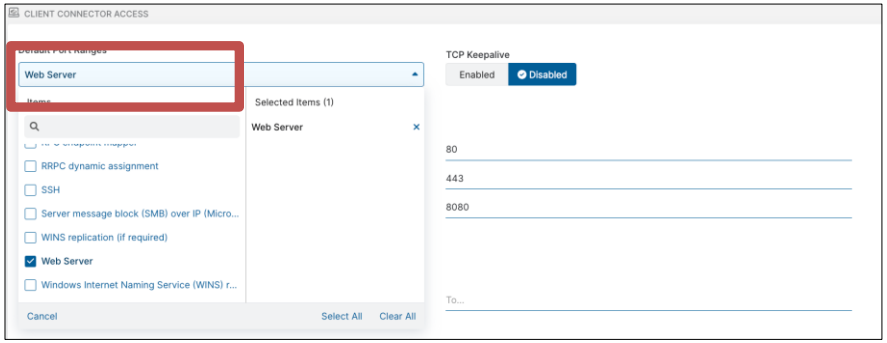
> ***Note:*** *Remember, you can also access the Admin Portal directly, in a browser on your own PC.*

2. If necessary, click the ⋮ icon at top right to expand the management menu, then click the ⊕ **Add Application Segment** link to add a new Application Segment and add an HTTP/S application for access to the corporate Intranet.
3. At the **Define Applications** step of the wizard, configure the following:
   a. In the **GENERAL INFORMATION** section, set the **Name** for the application to **Intranet**, set the **Status** to **Enabled**, leave the **Source IP Anchor** setting at **Disabled** and add a suitable description.
   b. In the **APPLICATIONS** section, click in the **Enter a domain or IP address** field and specify **intranet.patraining.safemarch.com**.

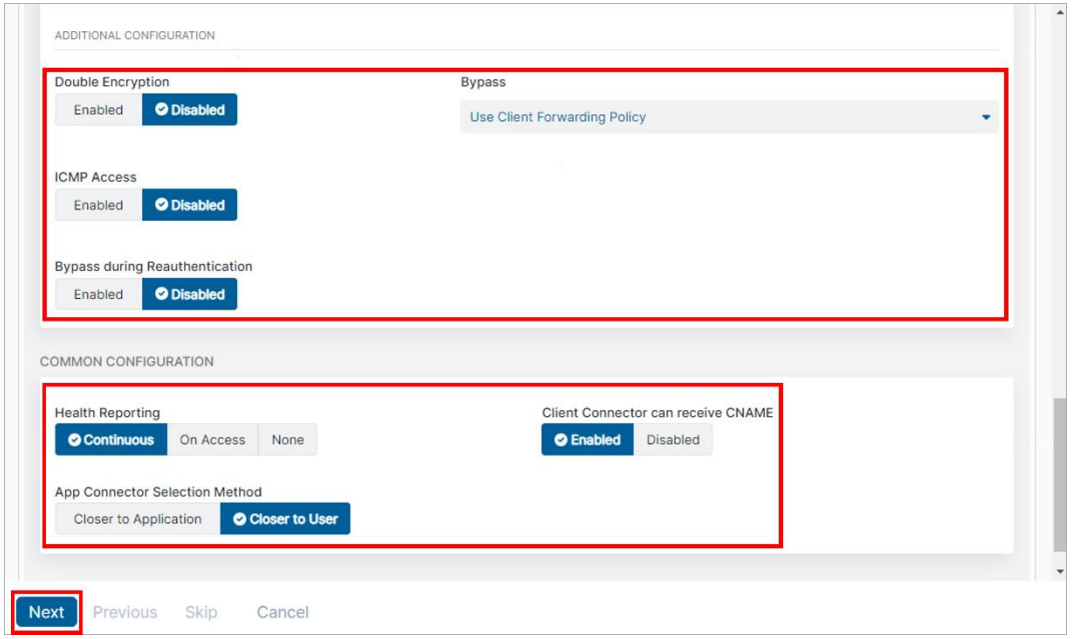
> ***Caution!*** *There is NO pod number in the domain!*



c. In the **CLIENT CONNECTOR ACCESS** section, click in the **Default Port Ranges** field, scroll down, and select **Web Server**. Click outside the dropdown box to close it. This should add TCP ports 80, 443, and 8080.
d. Ensure TCP Keepalive is set to **Disabled**.
e. Do not add a **UDP Port Range**.



f. In the **ADDITIONAL CONFIGURATION** section, leave **the Double Encryption** option at **Disabled**, the **Bypass** option at **Use Client Forwarding Policy** and the **ICMP Access** option at **Disabled**.



Note: *The ICMP Access option should only be enabled for applications that require ICMP connectivity between the client and the server. This feature is not intended to enable ICMP as a general troubleshooting tool for all applications using tools such as ping.*

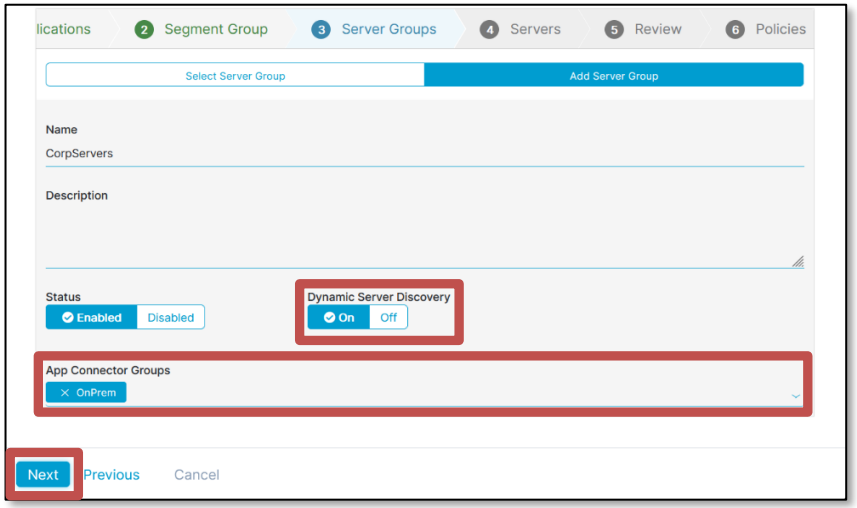
g. In the **COMMON CONFIGURATION** section, set **Health Reporting** to **Continuous**, **Zscaler Client Connector can receive CNAME** to **Enabled**, and **App Connector Selection Method** to **Closer to User**. Then click **Next**.

Note: *These are the default settings and should only be changed if needed to address an application access issue.*

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

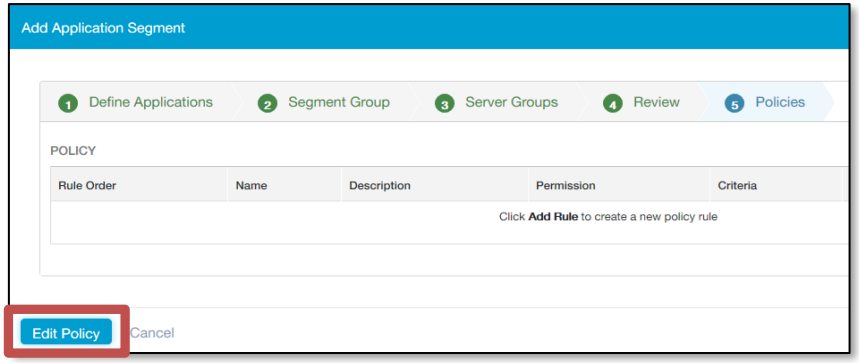
5. At the **Server Groups** step of the wizard, click **Add Server Group**, name the group **CorpServers**, optionally add a description, verify that the **Status** is set to **Enabled**, and set **Dynamic Server Discovery** to **On**.

6. Click in the **App Connector Groups** field and select the group **OnPrem** that you created earlier, then click **Next**.



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

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



Task 7.2: Add an Access Policy for the Intranet Application

Having clicked “Edit Policy” you will be taken to the Access Policy page. Alternatively, you can select Policy > Access Policy from the left-hand menu.

In this task, you will add an Access Policy to Allow access to the corporate Intranet server.

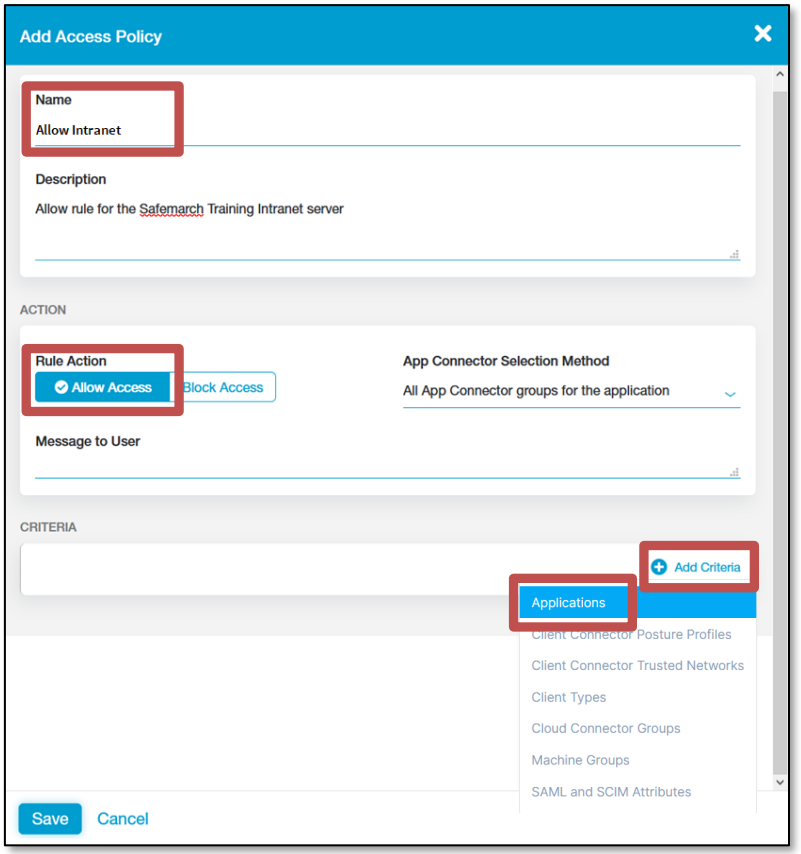
1. Add a policy rule to allow access to this application as follows:
   a. On the **Access Policy** page, click **Add Rule**.

   b. Name the rule **Allow Intranet** and optionally add a description.

   c. Set the **Action** to **Allow Access**.

   d. Leave the **App Connector Selection Method** at the **All App Connector groups for the application** setting, and the **Message to User** field blank.

   e. Click **Add Criteria** then from the list of available criteria, click **Applications**.

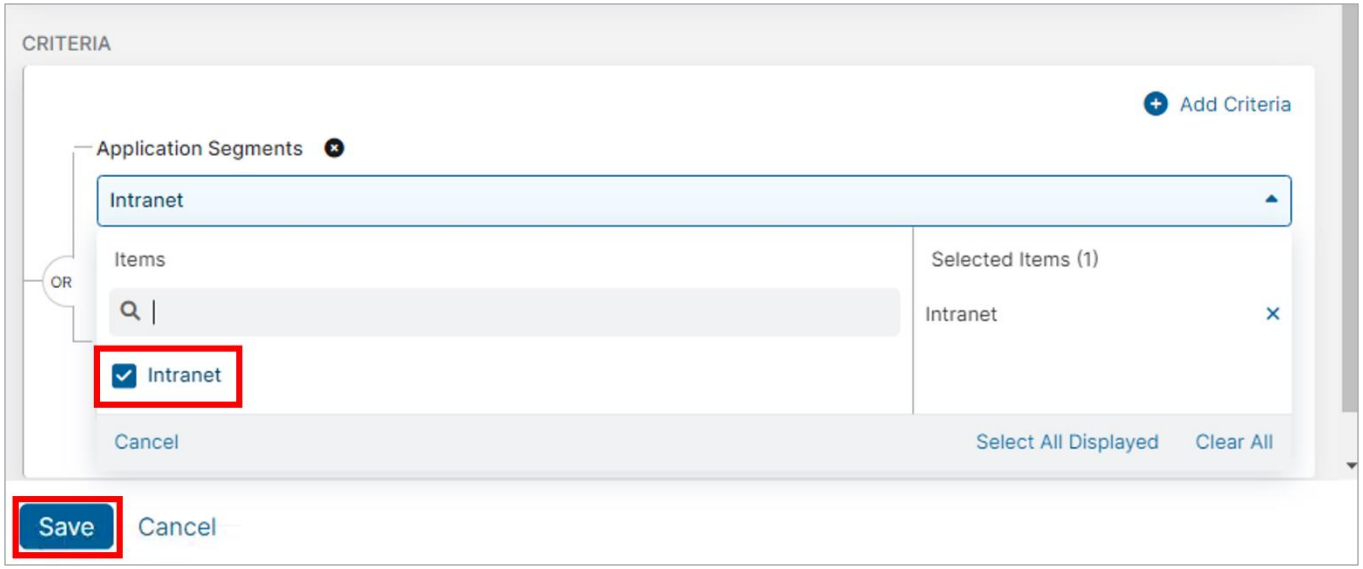


> ***Note**: The contents of the Criteria list may change over time.*

f. In the **Application Segments** field, select the **Intranet** Application Segment that you just created.

g. Do not add any **additional criteria**.

h. Click **Save**.

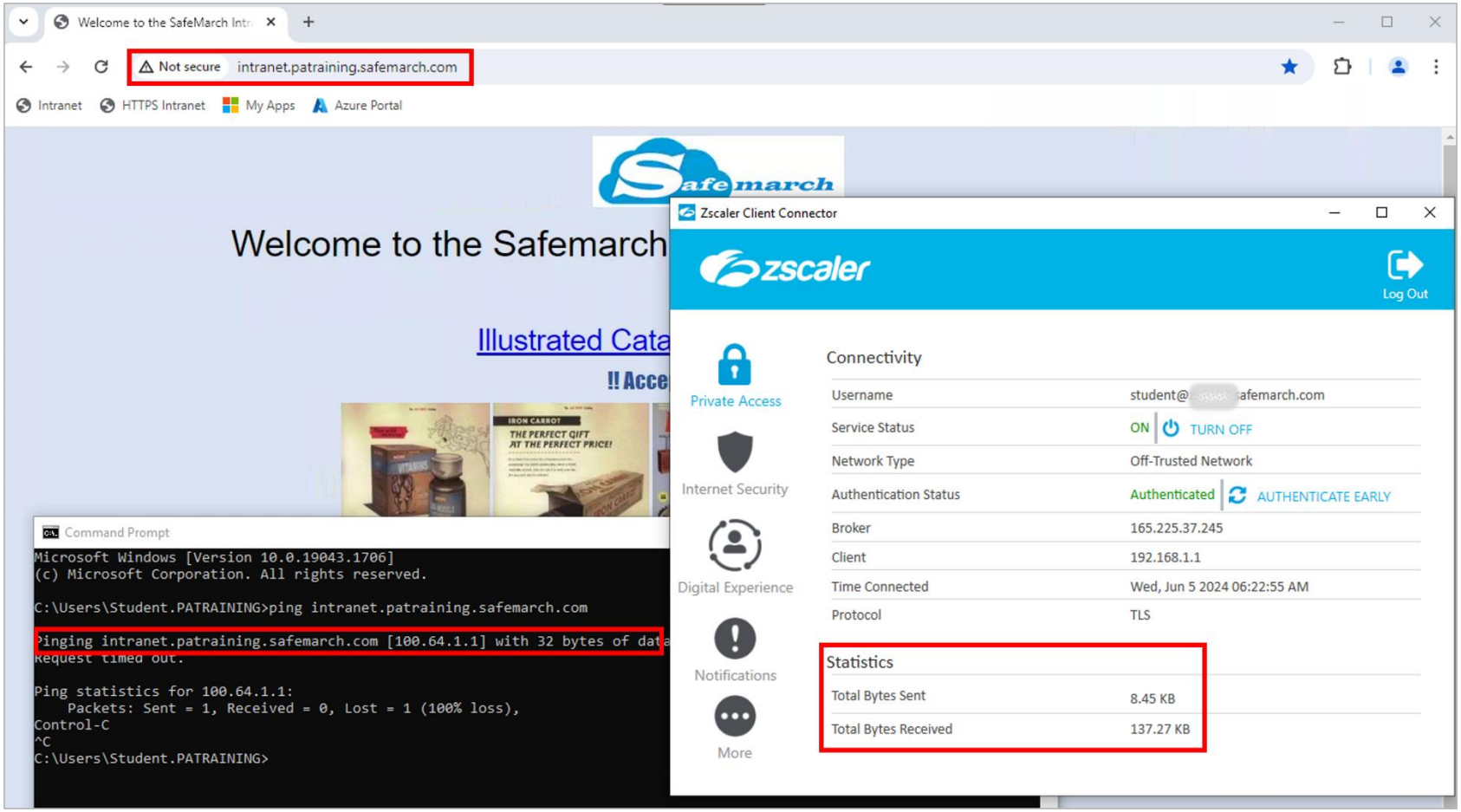


3. On the **Corp: Client PC**, open a web browser in a window and open the **Zscaler Client Connector** adjacent to it, so you can see the traffic counters as you load web pages.

4. Try to access the Intranet page at **http://intranet.patraining.safemarch.com** (a bookmark is provided) and confirm that the Intranet page loads. Also try to access the Intranet page using **HTTPS** (a bookmark is provided) and confirm that the Intranet page loads.

5. From the Windows **Start menu**, open a **Command prompt** and **ping** the host name at **intranet.patraining.safemarch.com**. Verify that it resolves to a **100.64.1.x** IP address (indicating that it is reachable using ZPA), but that it does not respond to pings.

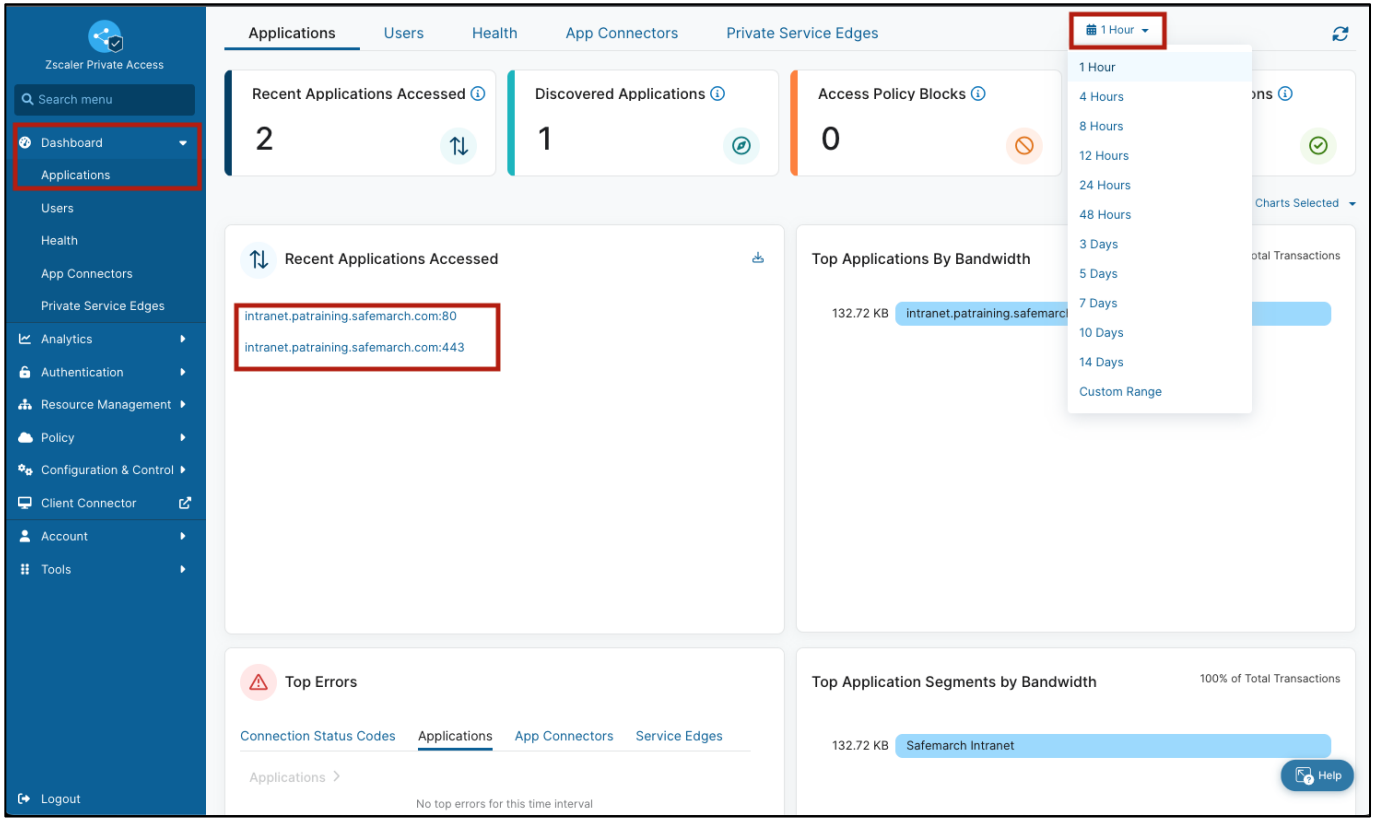
6. Refresh the Intranet page and view the **Total Bytes Sent / Received** counters in the Zscaler Client Connector and confirm they are incrementing.



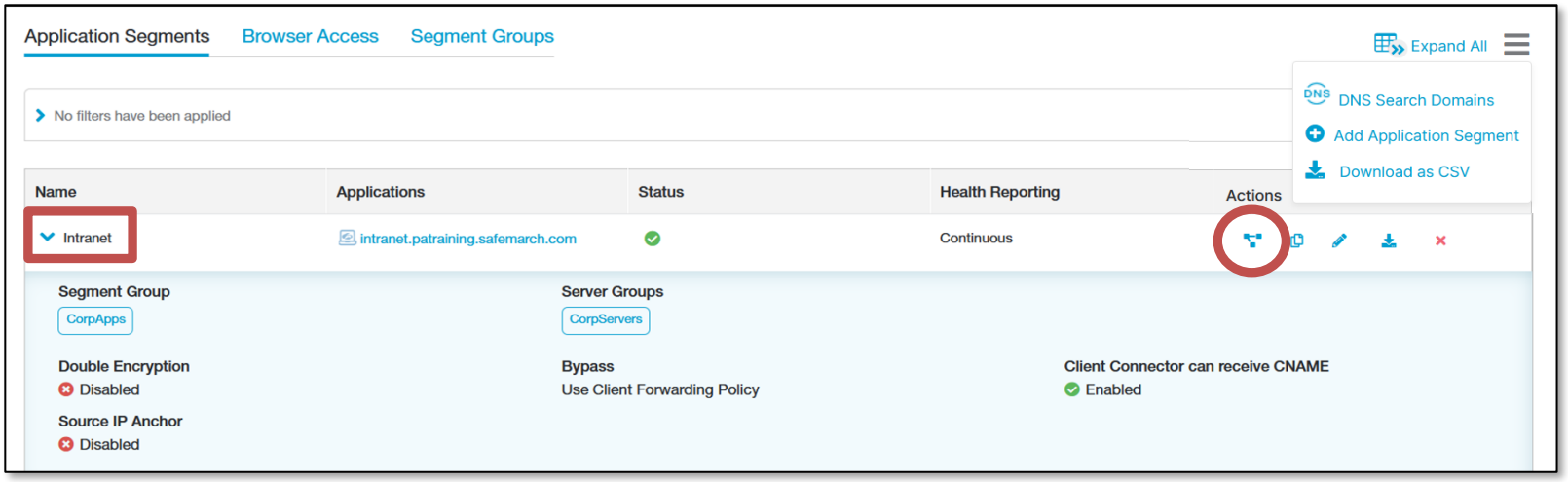
Task 7.3: Review Troubleshooting Information for the Intranet Application

In this task, you will review some of the summary and troubleshooting information available in the ZPA Admin Portal.

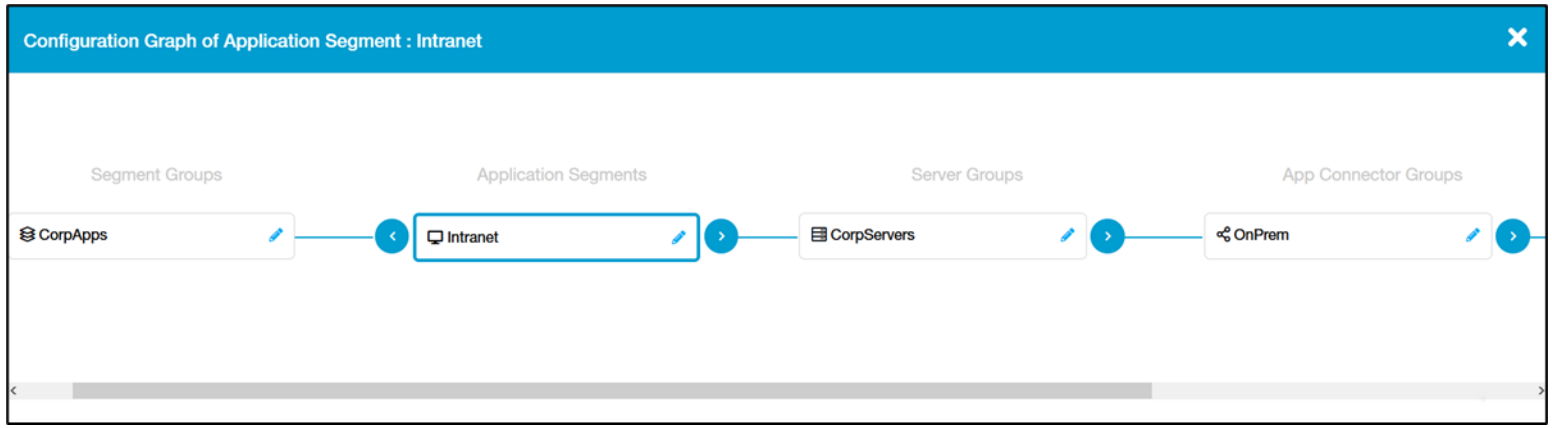
1. In the **ZPA Admin Portal**, click **Dashboard > Applications** and view the overview information available on **Applications Dashboard**.
2. Set the time range to **1 Hour** and verify that the **Intranet** application appears in the **Recent Applications Accessed** widget.



3. Navigate to the **Resource Management > Application Management > Application Segments** page and click on the **Name** of the Intranet Application Segment to view details for it, including the associated **Segment Group** and **Server Group** and the outline of the settings configured.

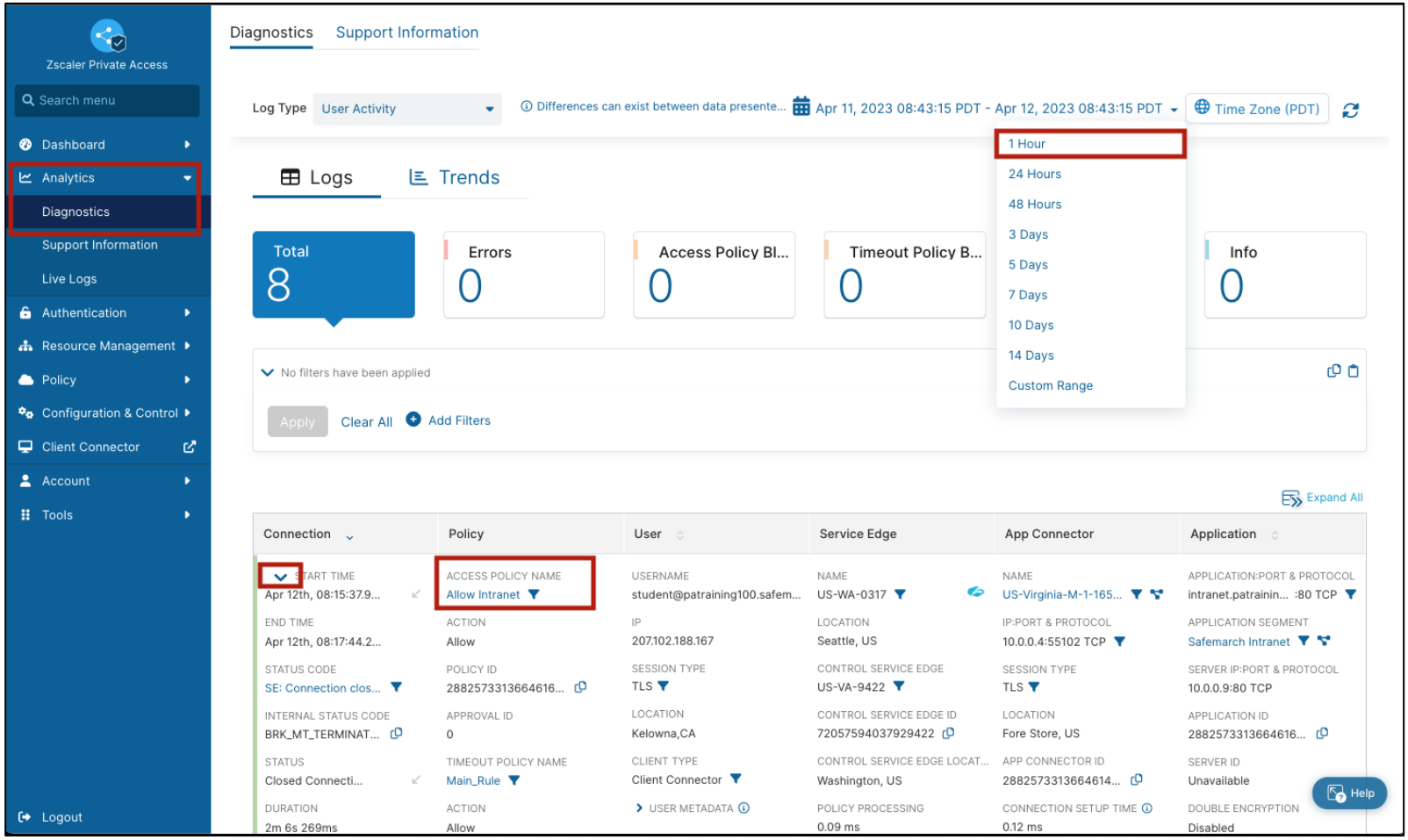


4. In the **Actions** column, click on the **Configuration Graph** tool to view the relationships between this **Application Segment** and the: **Segment Groups; Server Groups; App Connector Groups**; and individual **App Connectors**.



Note: *This view is also accessible from any of the other components listed and provides a quick and easy way to review the relationships when troubleshooting connectivity issues.*

5. Click the **Analytics > Diagnostics** option in the left-hand navigation menu.
6. Set the time range to **1 Hour** and verify that the **Allow Intranet** policy match appears in the list.
7. Click to expand one of the entries and review the data available for each successful end user connection attempt.



Lab 8: Discover Corporate Applications

The ZPA service is already active, and the end user has access to one defined application (intranet.patraining.safemarch.com), but what about the other domain applications that they may need access to? A useful way to find the applications that end users actually need is to configure ZPA for Application Discovery. With Application discovery, we configure a wildcard (*.domain.com) - when a user attempts to access an application which matches the wildcard, the request will be intercepted and ZPA will "Discover" the application through the App Connector. If the application is discovered, then policy will be applied to control access. This process of Discovery is similar to "Just in Time" provisioning of applications - the application is discovered, and a policy definition can later be created for it to granularly control access.

Task 8.1: Configure Application Discovery

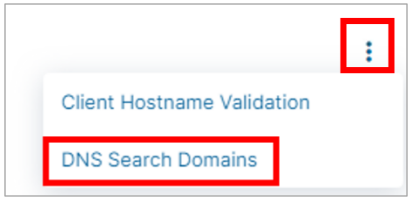
In this task, you will add an **Application Segment** in the ZPA Admin Portal, configured to allow application discovery. You will also add a **DNS Search Domain** to allow application discovery using short names (rather than having to use FQDNs).

1. In the ZPA Admin Portal, go to the Application Segments page.
   Resource Management > Application Management > Application Segments.

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

---

2. If necessary, click the ⋮ icon at top right to expand the management menu, then click the **DNS Search Domains** option to add a **Search Domain**:
   a. Add the domain **patraining.safemarch.com**.

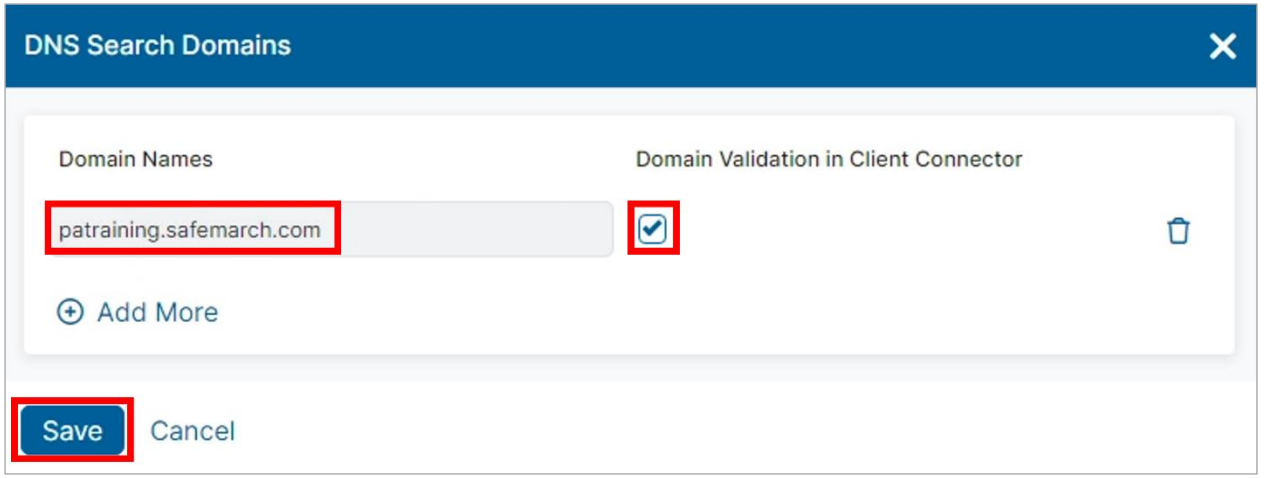


Caution! *There is **NO** pod number in the domain! This is the Active Directory DNS Domain inside the data center.*

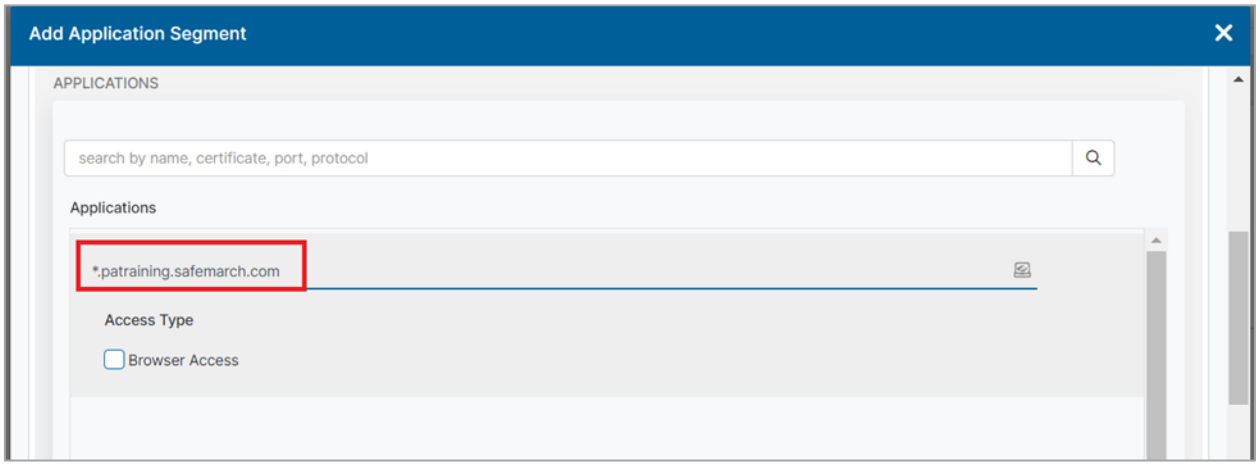
---

   b. Enable the **Domain Validation in Client Connector** and click **Save**.

Note: *This will allow the discovery of applications on this domain requested using a short name only. The* ***Domain Validation*** *option should be selected. This ensures that all search suffixes are applied to a short name, and sent through ZPA, before attempting to resolve against the local DNS server. This is a recommended best practice.*



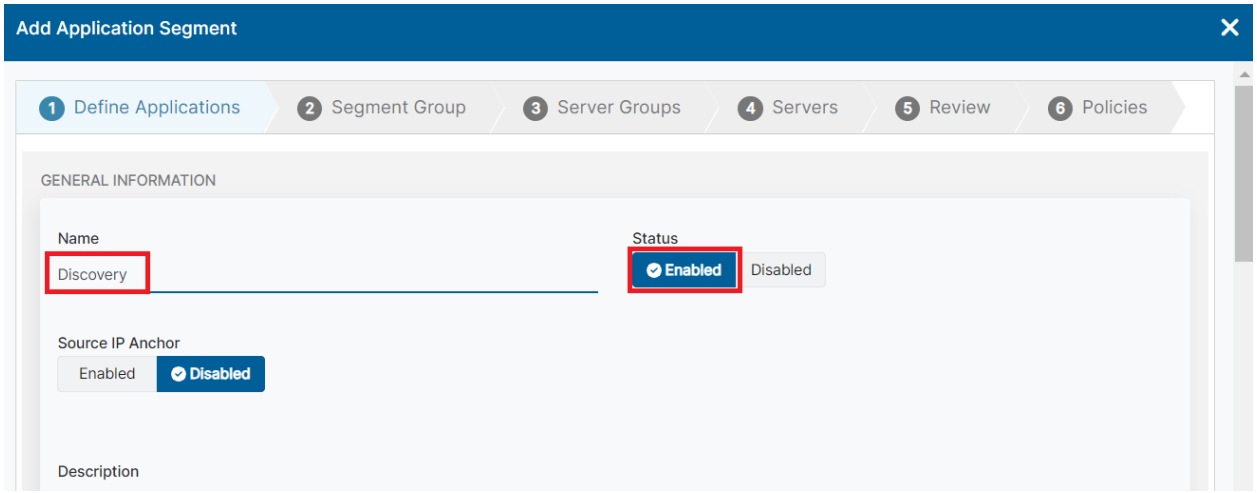
3. From the **Management** menu ⋮ at top right click, the **Add Application Segment** icon to add a **new Application Segment.**

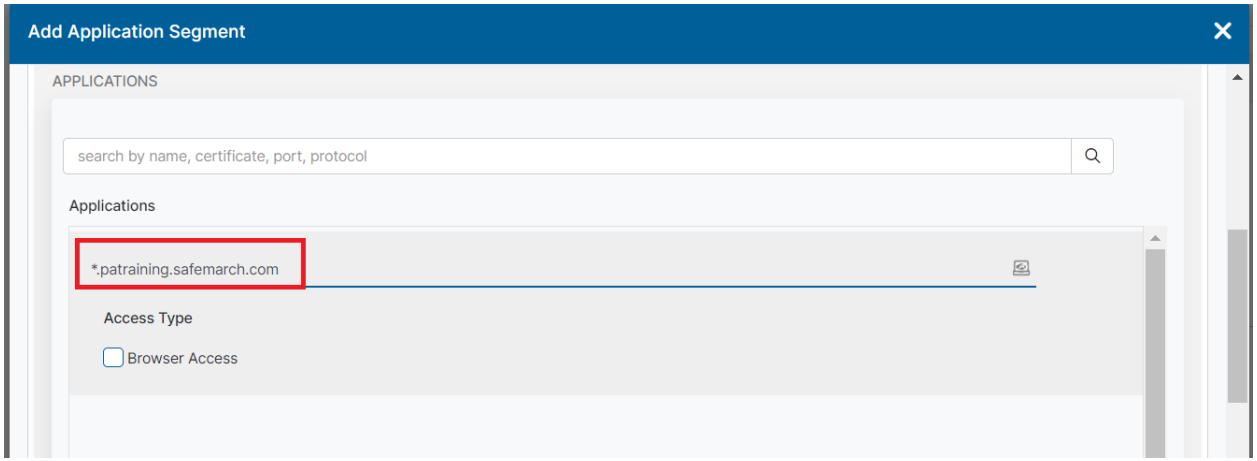


4. At the **Define Applications** step of the wizard, configure the following:
   a. In the **GENERAL INFORMATION** section, set the **Name** for the application to **Discovery**, set the **Status** to **Enabled**, leave the **Source IP Anchor** option **Disabled** and add a suitable Description.

b. In the **APPLICATIONS** section, click in the **Enter a domain or IP address** field and specify ***.patraining.safemarch.com**.

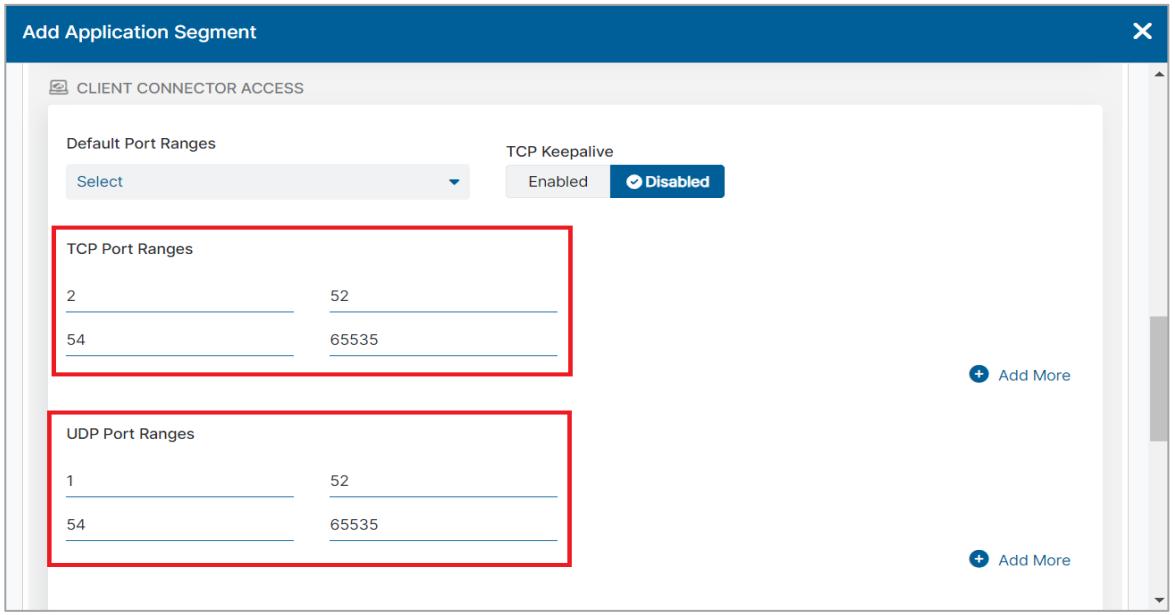
Caution! *there is NO pod number in the domain!*



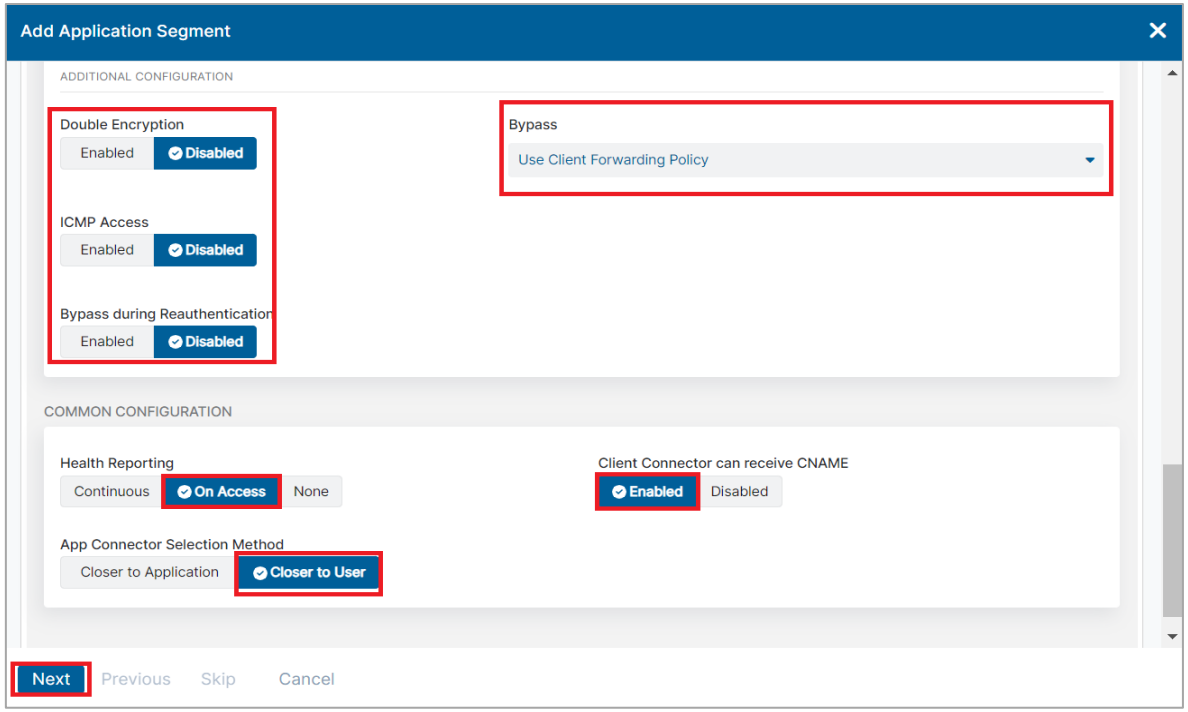


c. Scroll down, and in the CLIENT CONNECTOR ACCESS section, manually specify a **TCP Port Range** from **2 to 52**,
d. Click **Add More** and add the range **54 to 65535**.
e. Add a **UDP Port Range** of **1** to **52**,
f. Click **Add More** and add the range **54** to **65535**.

Note: *Zscaler recommends that you exclude TCP and UDP port 53 so as not to interfere with the operation of DNS. If UDP port 53 is included, it can result in unexpected DNS responses causing access issues.*

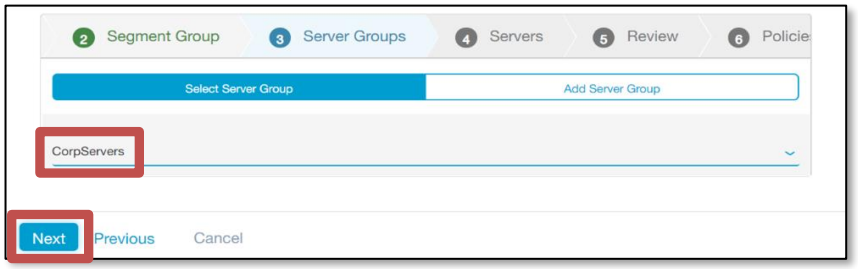


g. Leave the **Double Encryption** and **ICMP Access** options at **Disabled**, and the **Bypass** option at **Use Client Forwarding Policy**.
h. Scroll down and in the **COMMON CONFIGURATION** section, set:
    i. **Health Reporting** to **On Access**,
    ii. **Client Connector can receive CNAME** to **Enabled**, and
    iii. **App Connector Selection Method** to **Closer to User**.
i. Then click **Next**.



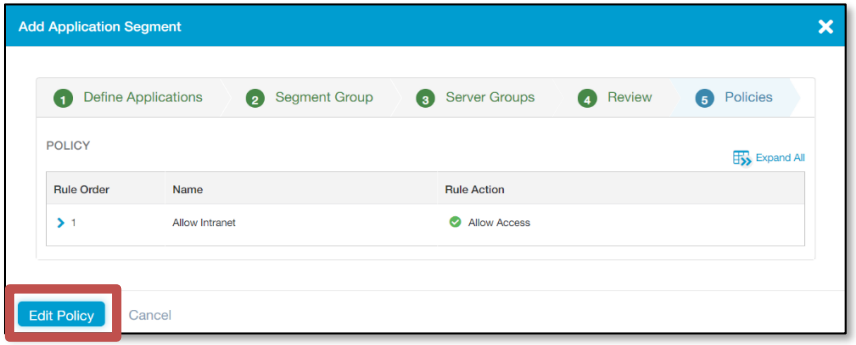
5. At the **Segment Group** step of the wizard, click **Add Segment Group**, name the group **Discovered**, optionally add a description, verify that the **Status** is set to **Enabled**, and click **Next**.

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



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

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



9. Add a policy rule to allow access to this application as follows:
   a. On the **Access Policy** page, click **Add Rule**.

   b. Name the rule **Allow Discovered** and optionally add a description.

   c. Set the **Action** to **Allow Access**.

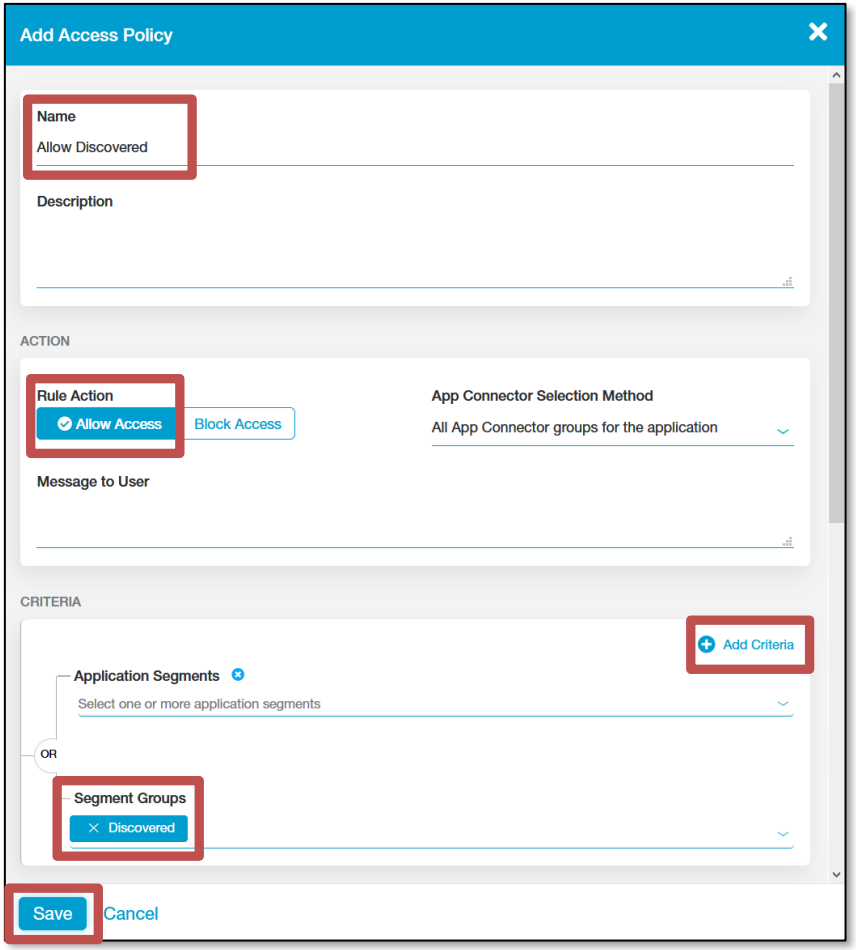
   d. Leave the **App Connector Selection Method** at the **All App Connector groups for the application** setting, do not add a **Message to User**.

   e. Click **Add Criteria** then from the list of available criteria, click **Applications**.

   f. In the **Segment Groups** field, select the **Discovered** Segment Group that you just created.

__Note__: Do not add any additional criteria.

   g. Click **Save**.

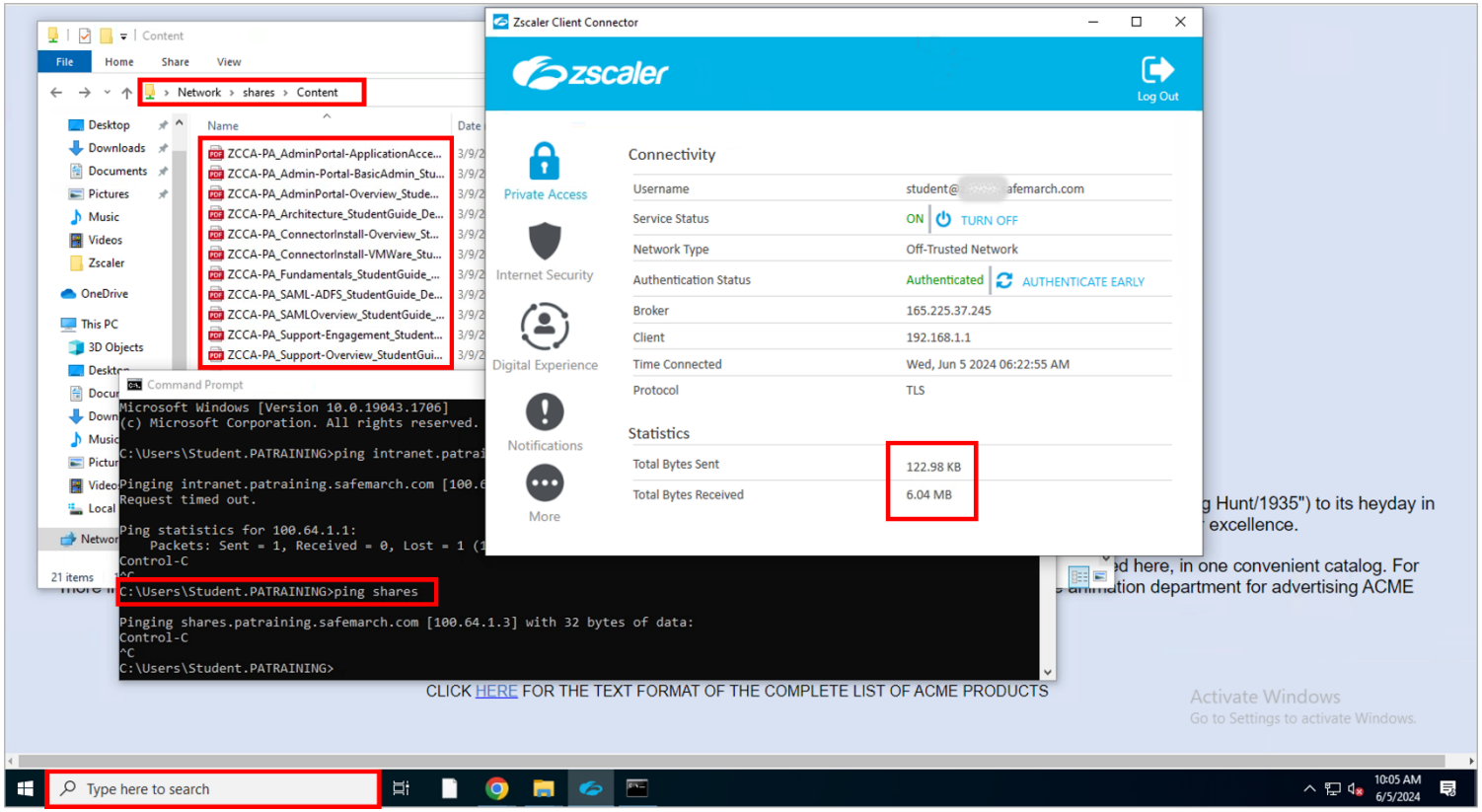


__Note__: This rule will be added at the bottom of the list of Access Policy rules. However, as this is a very general rule, that is a good position for it. Also, it would be possible to restrict this rule to apply only to your internal users using SAML Attributes, but for this lab we will leave it applicable to everyone.

Task 8.2: Discover Applications

In this task, you will attempt to access the various corporate applications available by their short names.

1. On the **Corp: Client PC**, click the **Search Windows** icon in the Status Bar (next to the Windows Start icon) and in the Search field, type **\\shares**. Confirm that the available shares are shown that you can access the share named Content and open one of the PDFs. Also, confirm that the Zscaler Client Connector traffic counters increment as you do so.

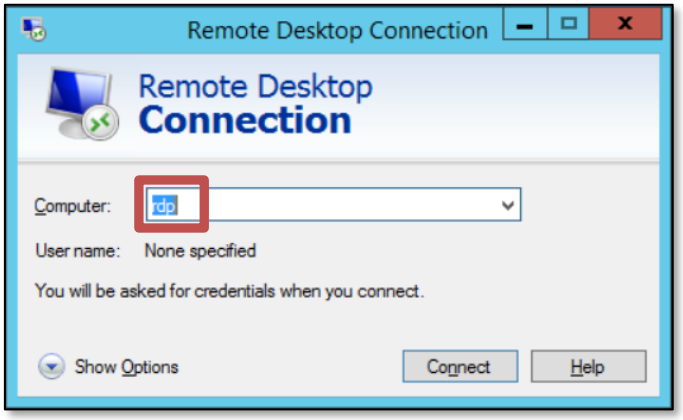


2. From the Windows **Start** menu, open a Command prompt and ping the host-name **shares**. Verify that it resolves to a **100.64.1.x** IP address (indicating that it is reachable using ZPA), and that it does not respond to pings.

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

---

3. Click the Search Windows icon in the Status Bar again and in the Search field, type **rdp** and try to connect to the server using just the application short name **rdp**. Try to login with the username **student** with password **Admin-123!** and accept the certificate.

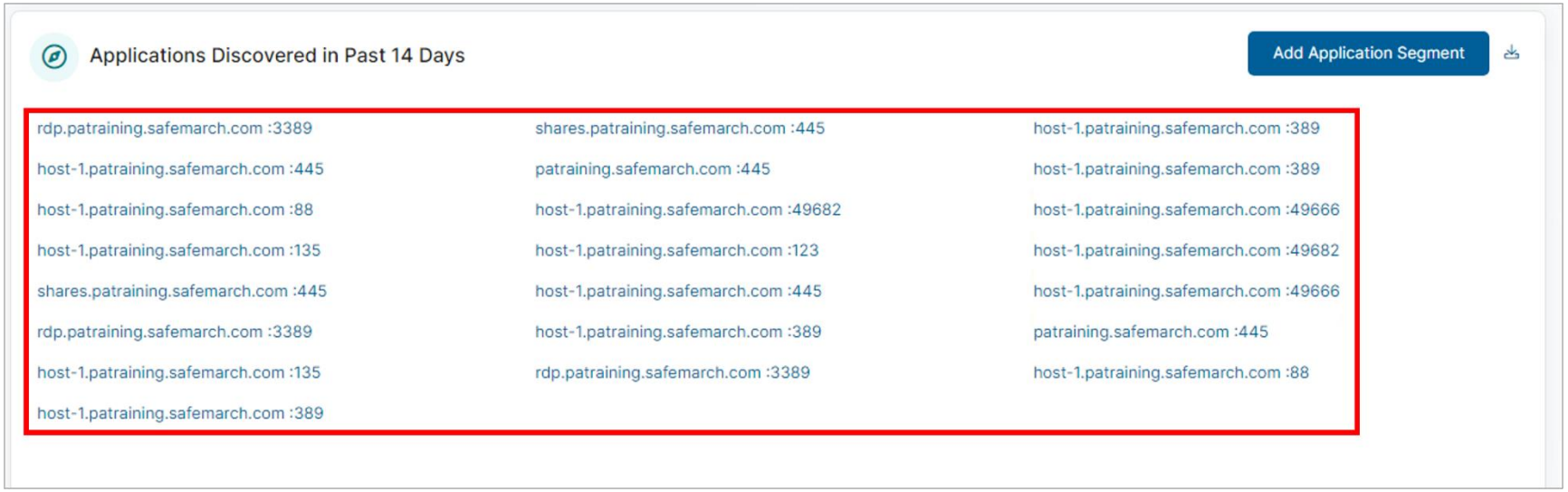


> ***Note:*** *There is no need to actually login to the server, you just need to show that an RDP connection is possible.*

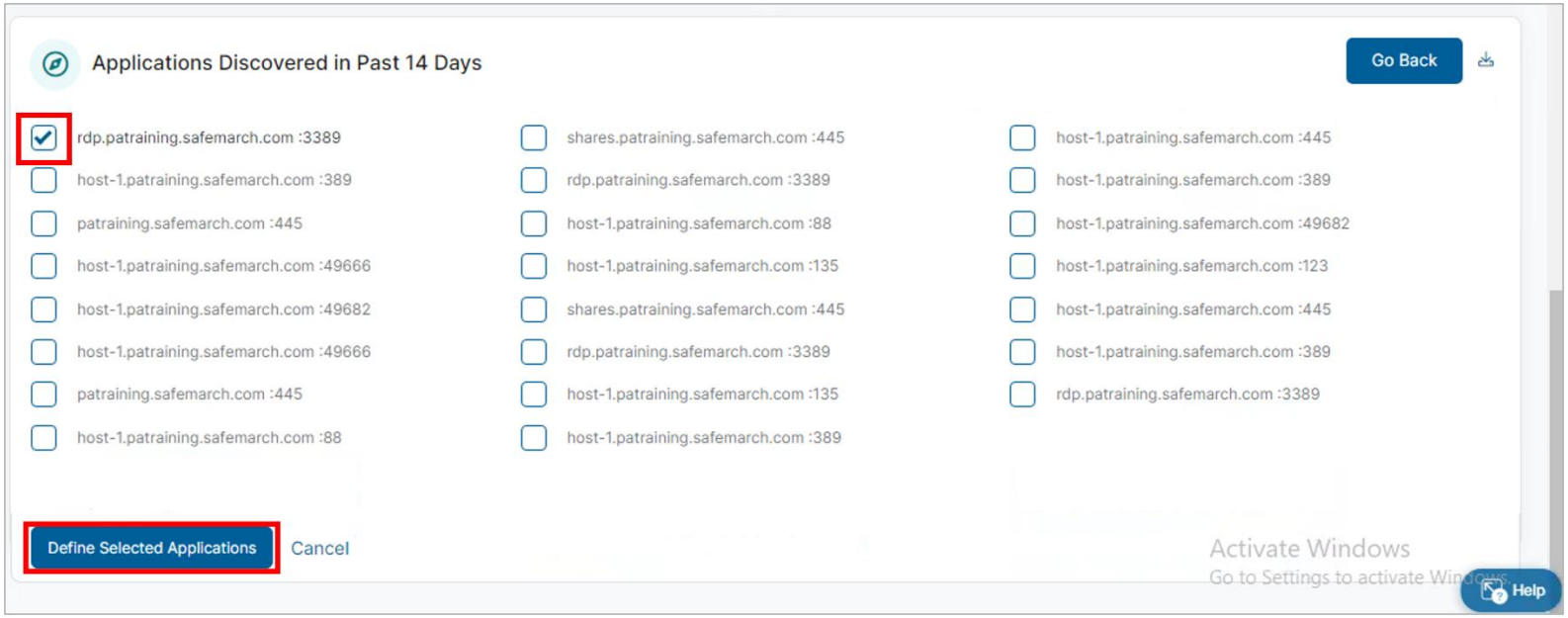
4. Close the RDP connection to the server.

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

5. Go back to the ZPA Admin Portal and navigate to the **Dashboard > Applications** page. Scroll down to view the **APPLICATIONS DISCOVERED IN PAST 14 DAYS** widget, check that the applications that you have accessed are all listed.



***Note**: From this widget, you can click **Add Application Segment**, select any of the auto-discovered applications and then click **Define Selected Applications**. This will then allow you to create an application segment and access policy, like you did in Lab 7.*

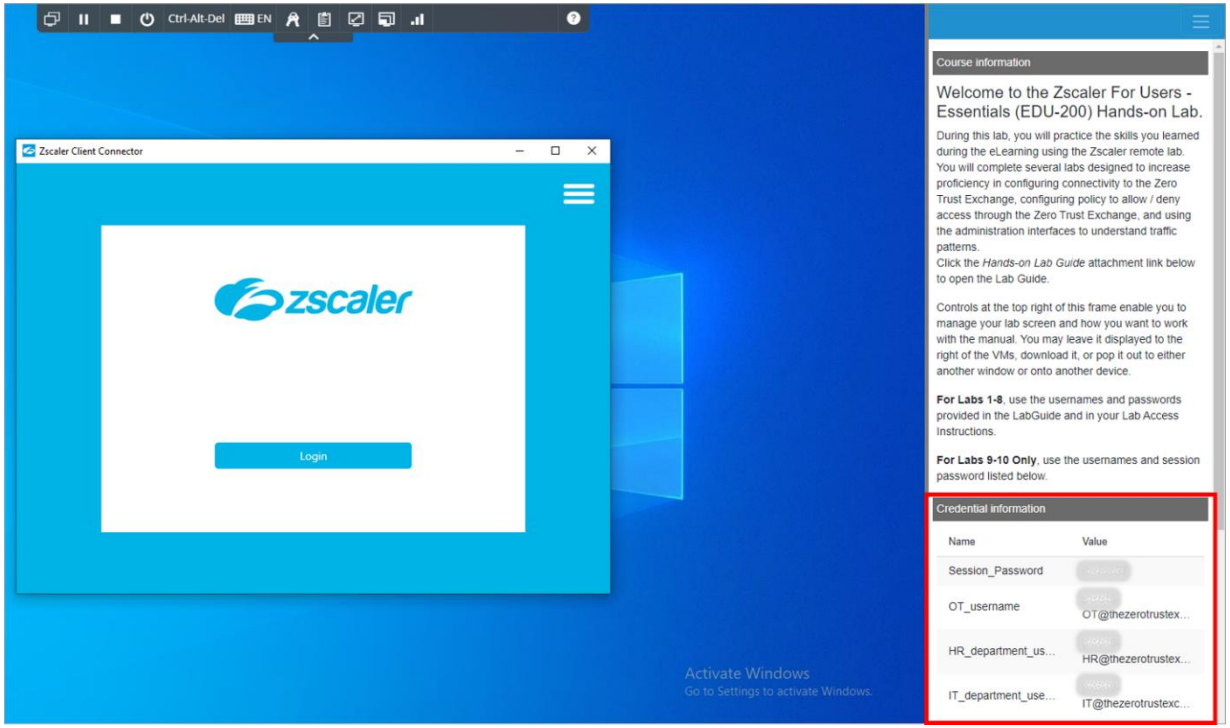


6. Navigate to the **Analytics > Diagnostics** page and review the list of **User Activity**. Look for entries that match your **Allow Intranet** and **Allow Discovered** Access Policy rules. Expand an entry and review the data available.

Lab Access Information for Labs 9 - 10

For the remaining labs, you will access *Zscaler's Software Demo Center (SDC)* tenant on **zscalerthree.net**, as a Read-Only Administrator.

This role affects what you will see in the Admin Portal. Use the usernames and session password listed in your Skytap pod's Credential Information section.



In Lab 2, you installed Zscaler Client Connector with switches that preconfigured the cloudName and userDomain options. In the following labs, we need to log into Client Connector as users on a different cloud (zscalerthree.net). To reconfigure Zscaler Client Connector, follow these steps:

1. On the **Corp Client PC**, log out and exit Zscaler Client Connector.
2. Open a Windows Command Prompt and type **cd downloads**.
3. On the CLI type the following command to run the installer again, with different command line switches:

   a. **Zscaler-windows**-<file version>-**installer-x64 --cloudName zscalerthree --hideAppUIOnLaunch 1**

Note: *This will update the Client Connector configuration to the new cloud name.*

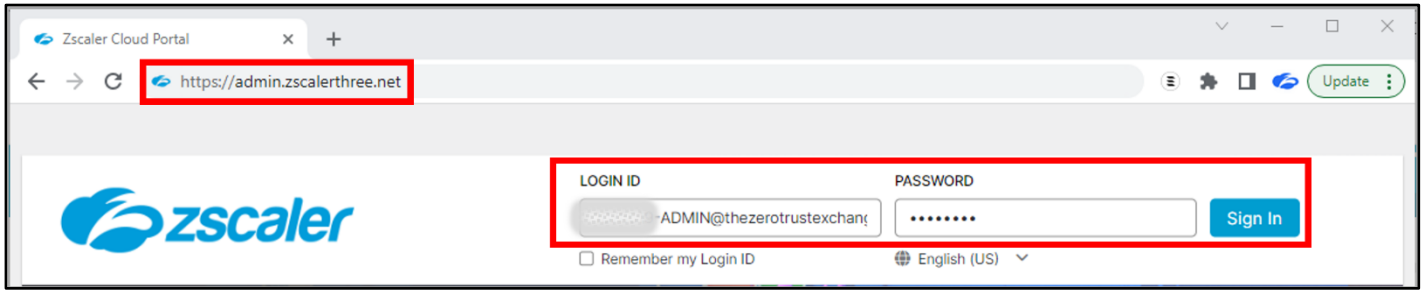
Lab 9: Protecting Against Cyberthreats

During this lab, you will explore some of the Zscaler Internet Access (ZIA) security features that help streamline your security operations and take full advantage of the multiple layers of security provided by Zscaler's Zero Trust Exchange. Much of combating cyberthreats is never letting them have a chance in the first place! Zscaler URL Filtering and Cloud App Controls are tools that can be used to provide controls around which sites and applications users can reach on the Internet.

Task 9.1: View Threat Protection Configurations & Risk Reports

In this task, you will review the current Threat Protections and explore reports that provide visibility into cyberthreats.

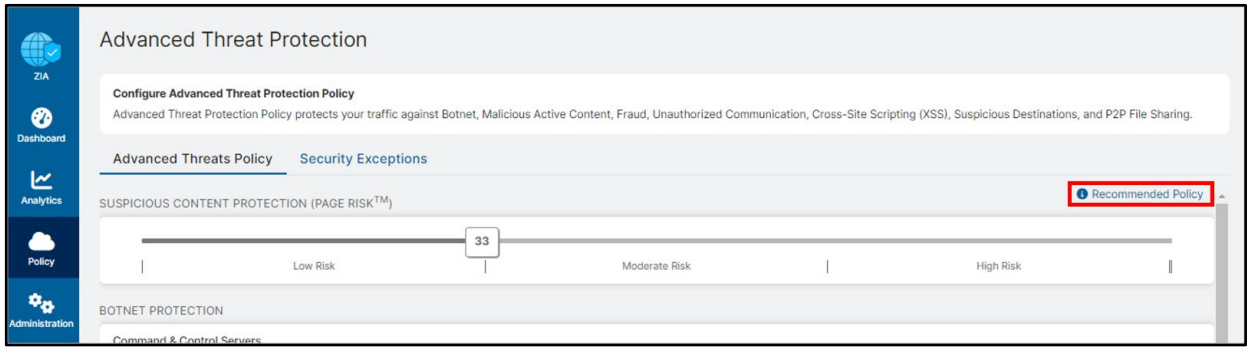
1. On your laptop (or the Client PC VM), open a web browser and go to **https://admin.zscalerthree.net**.



2. Log in to the ZIA Admin Portal with your assigned **Admin_User_ID** and **Session_Password**.
3. Go to **Policy > Malware Protection**.
4. Scroll through the settings and compare them to the **Recommended Policy** settings, taking notice of which Malware Protections have been enabled. These protection areas guard users against spyware, botnets, malicious active content, and more.

5. Go to **Policy > Advanced Threat Protection**.

6. Scroll through the settings and compare them to the **Recommended Policy** settings, taking notice of which Advanced Threat Protections have been enabled. These protection areas guard users against Command and Control Traffic, Malicious Sites, Fraud Protection, Phishing, Cryptomining, Tunneling, Cross-Site Scripting (XSS), etc.



7. Note the current **Page Risk Score Index** (SUSPICIOUS CONTENT PROTECTION (PAGE RISK™)).
8. Go to **Analytics > Configuration Risk Report**.

---

*The Zscaler service calculates the **Risk Index** of a page in real-time by identifying malicious content within the page (injected scripts, vulnerable ActiveX, zero-pixel iFrames, and many more) and creating a risk score, or Page Risk Index.*

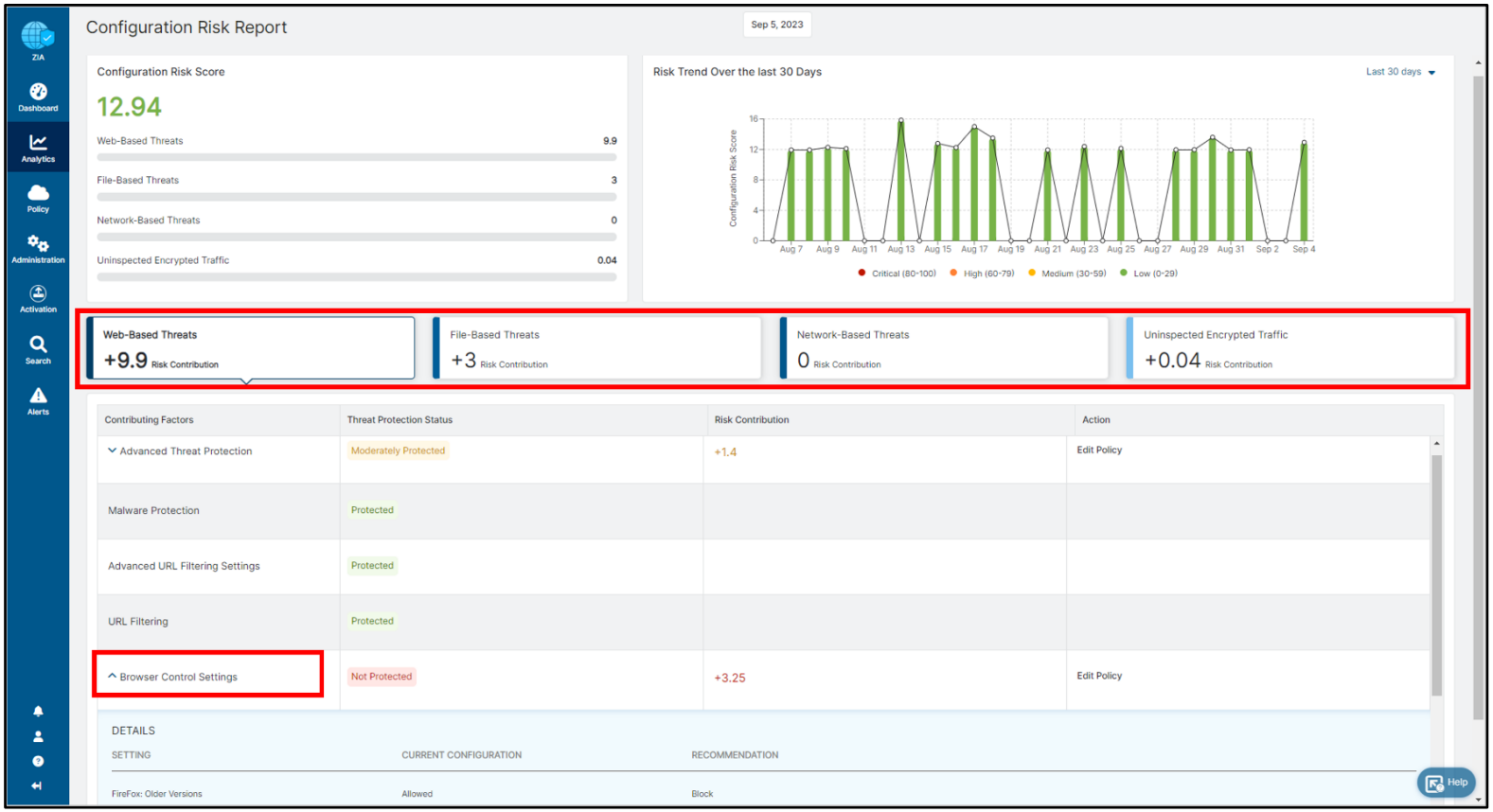
Simultaneously, a Domain Risk Index is created using data such as hosting country, domain age, past results, and links to high-risk top-level domains. The Page Risk and Domain Risk are combined to produce a single score for the Risk Index; this score is then evaluated against the Suspicious Content Protection (Page Risk™) value that you set in this policy. The Low Risk area indicates that you are willing to block anything that is even slightly suspicious; there is no tolerance for risk. The High Risk area indicates a high tolerance for risk and will allow users to access even very risky sites.

The Configuration Risk Report evaluates the current policy configuration, traffic pattern and feature capabilities against Zscaler's best practices and recommends configuration changes to better protect against emerging threats.

---

6. Click on each category, **Web-Based Threats**, **File-Based Threats**, **Network-Based Threats**, **Uninspected Encrypted Traffic**, to understand the current protection status and its contribution to the overall risk.

7. Navigate to the category with the highest Risk Contribution and drill into the details by clicking on the category name. Review the potential threats and recommended configuration changes.



8. Go to **Analytics > Company Risk Score Report**.

Company Risk Score Report *allows organizations to monitor and analyze the various factors that contribute to an organization's risk score, which can include recent malware outbreaks, risky user behavior, and other suspicious factors. Administrators can study how their users' and company's risk score has changed over time and compare their score against their industry peers and Zscaler cloud averages.*

Company Risk Score Report provides the following benefits and enables you to:

- *Configure stronger policies by monitoring your organizational, location, and user-level risk exposure.*
- *Study users' and company's risk scores change over time to determine the effectiveness of various policy configurations.*
- *Compare the risk scores against your industry peers and Zscaler cloud averages to understand your position against potential attacks.*

---

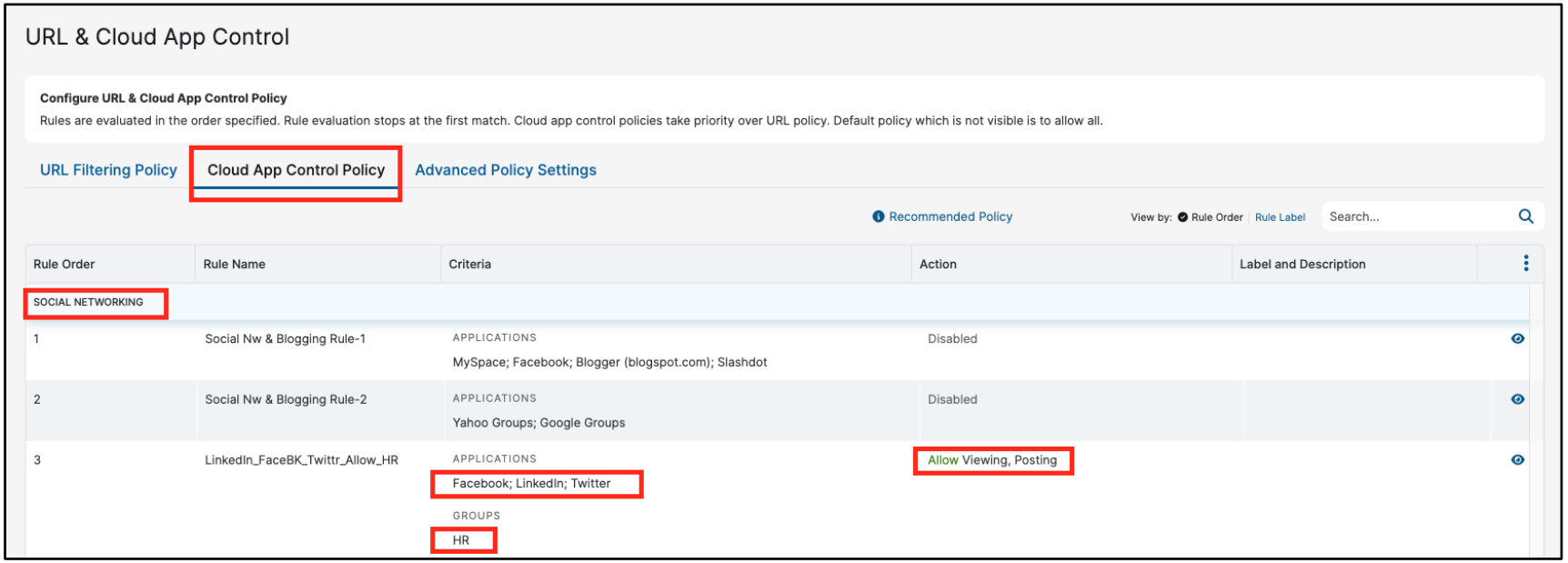
9. Review the sections **Events Contributing to the Risk Score** and **Top Advanced Threats Trend** to understand the user's risky behavior & activities trend that contributed to the current risk score.

10. Subsequently, you can click on any of the **Top Risky Users** to pivot to the User Risk Report to understand the selected user's behavior that contributed to the risk score and trends.

Task 9.2: View Content Filtering Controls

In this task, you will familiarize yourself with the current URL Filtering and Cloud App controls.

1. Go to **Policy > URL & Cloud App Control**.
2. Under the **URL Filtering Policy** tab, review the currently defined policies, for example blocking URLs in the Social Networking category and sending Miscellaneous traffic to Browser Isolation.
3. Under the **Cloud App Control Policy** tab, review pre-configured policies, including:
    a. Social Networking policies that only allow users in the HR department to view and post to social media sites.



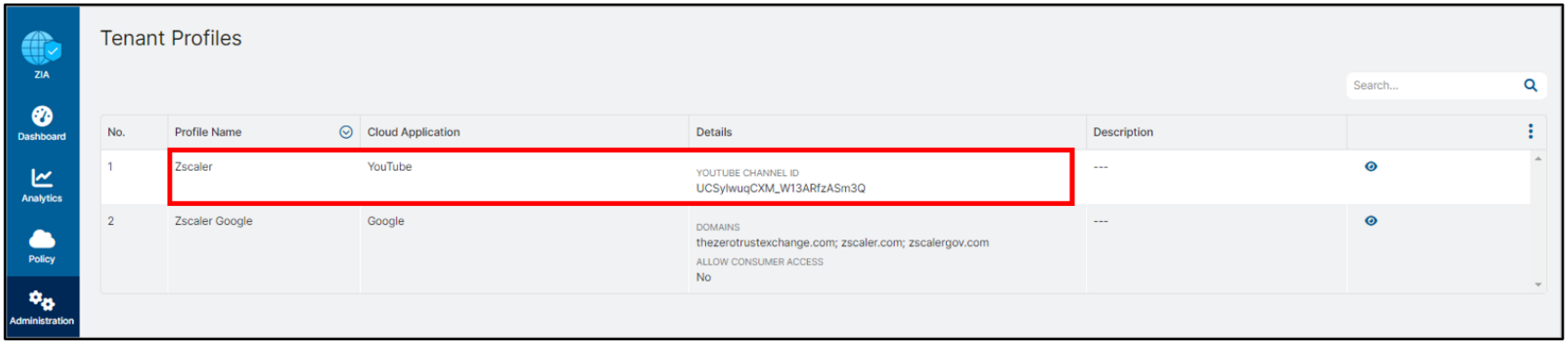
4. Scroll further down the list to see the rules configured in other categories. For example:
    a. **Streaming Media** policies that will allow users in the Marketing department to view Zscaler's YouTube channel, but block access to any other YouTube videos
    b. **Webmail** policies for sending Unsanctioned Mail apps to Browser Isolation.

5. Click the **Advanced Policy Settings** tab and review the recommended settings for Advanced URL Filtering options, such as SafeSearch, Suspicious New Domains Lookup and AI/ML based Content Categorization.

6. Go to **Administration > Tenant Profiles**.

7. Review the settings of Zscaler's YouTube channel, which was used in the Streaming Media policy you viewed previously.

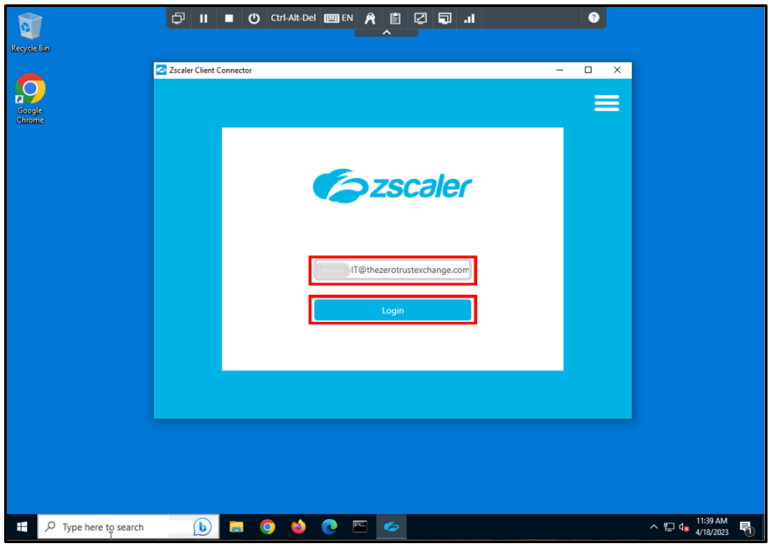
*Zscaler's **Tenancy Restriction** feature allows you to restrict access either to personal accounts, business accounts, or both for certain cloud applications.*



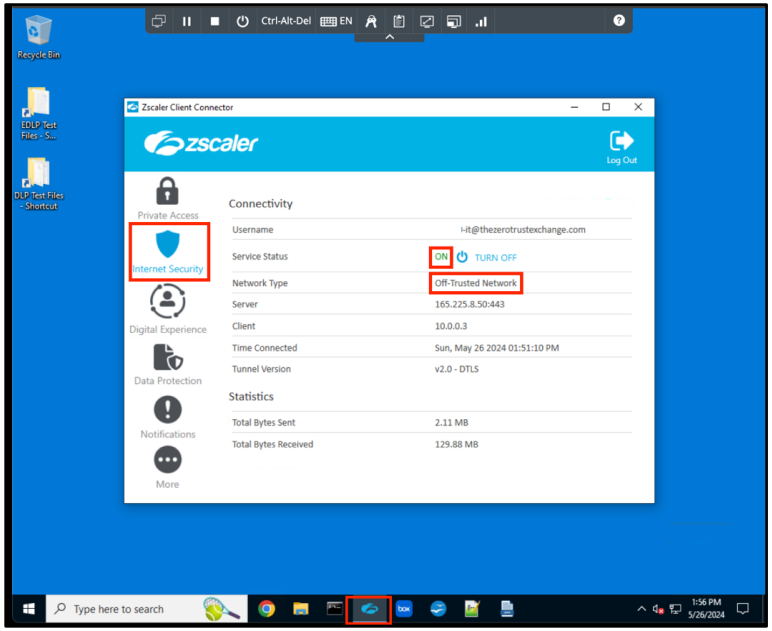
Task 9.3: Test End User Experience with Content Filtering

In this task, you will test the end user experience when accessing websites and cloud apps.

1. On the **Corp: Client PC,** log into the Zscaler Client Connector as the **Marketing** user:
   a. Enter the **MKT_department_username.**
   b. Click **Login.**
2. At the IdP authentication prompt:
   a. Enter the **MKT_department_username** again if it is not pre-filled, and click **Next**.
   b. Enter the **Session_Password** and click **Sign in**.
3. At the *Stay signed in?* prompt, click **No**.



4. Zscaler Client Connector will minimize to the Windows **taskbar** and go through some initialization steps.
5. Check that Zscaler Client Connector is running, and that:
   a. Internet Security Service Status shows **ON.**
   b. Network Type is shown as **Off-Trusted Network**.



6. Browse to the Zscaler YouTube channel to test tenant restrictions **https://www.youtube.com/channel/UCSylwuqCXM_W13ARfzASm3Q** (a bookmark is provided).
7. Go to **https://linkedin.com** to see if you can get to it.

Note: *Based on the policies you reviewed earlier, a user in the Marketing department should be able to view Zscaler YouTube videos and be Isolated when visiting social networking sites, like Twitter.*

---

4. [Optional]: Log out of Zscaler Client Connector and log back in with the **HR_department_username**. Verify that as a user in the HR department you are able to view Facebook, LinkedIn, or Twitter directly without being sent to Isolation.

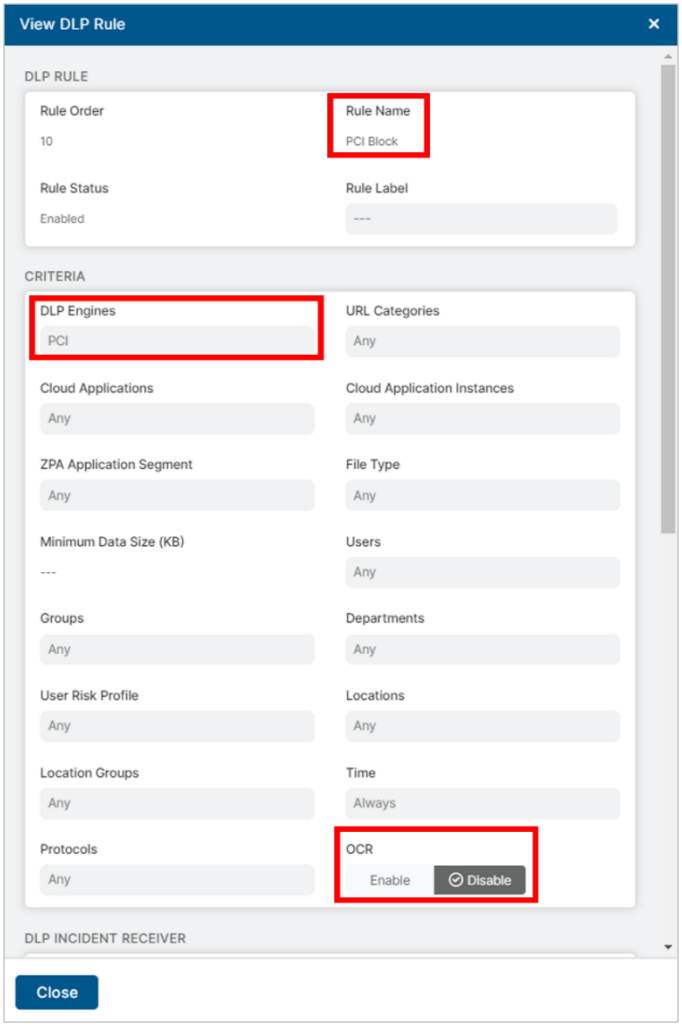
Lab 10: Protecting Against Data Loss

Corporate data can be leaked in different ways, i.e., through web mail, cloud storage, social media, and a variety of other applications. In this lab, consider a financial services company that needs to protect sensitive financial data, such as credit card numbers and bank account details. In this scenario, a Data Loss Prevention (DLP) policy can be configured to detect and block any attempts to transmit this data outside of the organization's network, such as via email or cloud storage services.

Task 10.1: Review DLP Configurations & Reports

In this task, you, as a DLP *Administrator*, will review an inline DLP rule for classifying financial data such as Credit Card numbers and ABA bank routing numbers. You will then view DLP-related widgets and graphs.

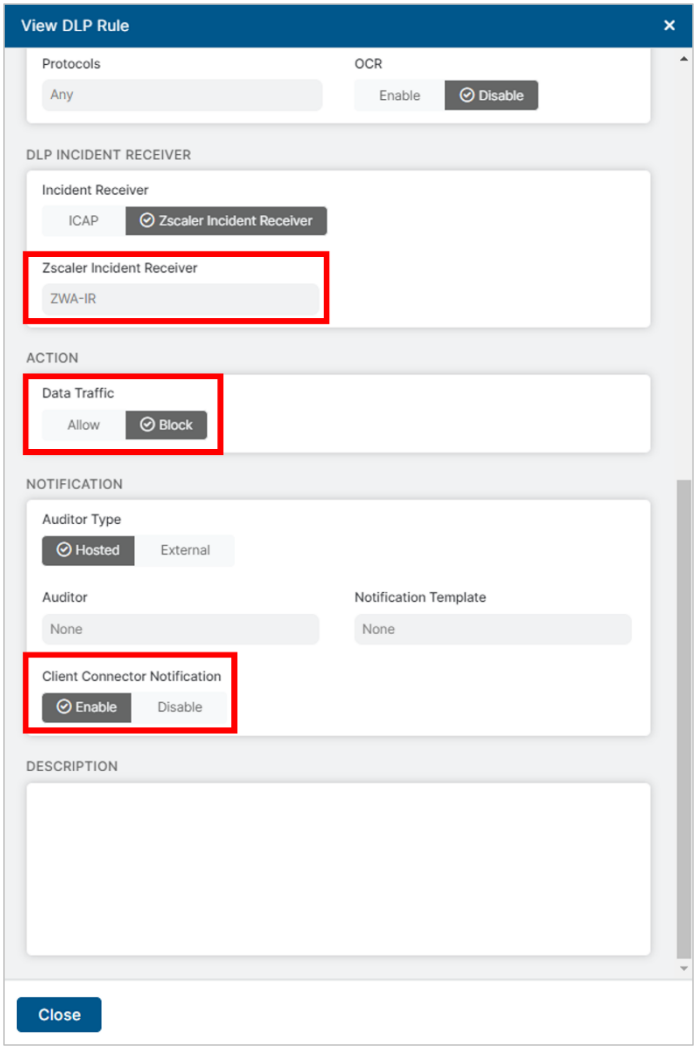
1. Navigate to **Policy > Data Loss Prevention**.
2. Search for policy name **PCI Block** and click to view its settings.
3. Familiarize yourself with the various options under Criteria such as DLP Engines, URL Categories and Cloud Applications, Private Applications, File Type, File Size and Users, Groups and Departments.



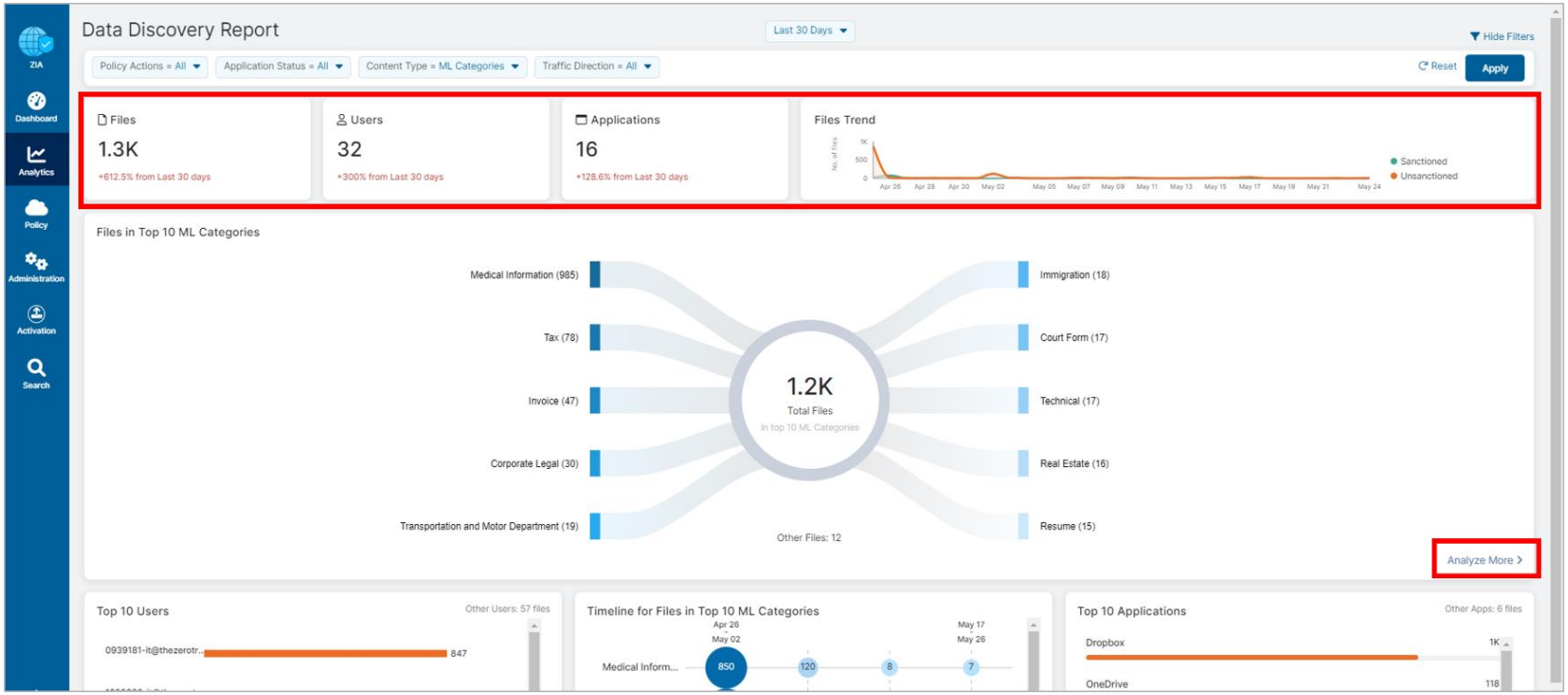
> ***Note:*** *An administrator can enable the* ***OCR*** *option to scan images as well as documents containing images.*

4. Scroll down to the bottom of the rule and review how the DLP admin receives incident notifications and evidence when this rule is violated as well as the policy action.

> ***Note:*** *Zscaler DLP can send evidence and trigger data to DLP administrators by various means such as an Email, on-prem Incident Receiver, or cloud-hosted Incident Receiver.*

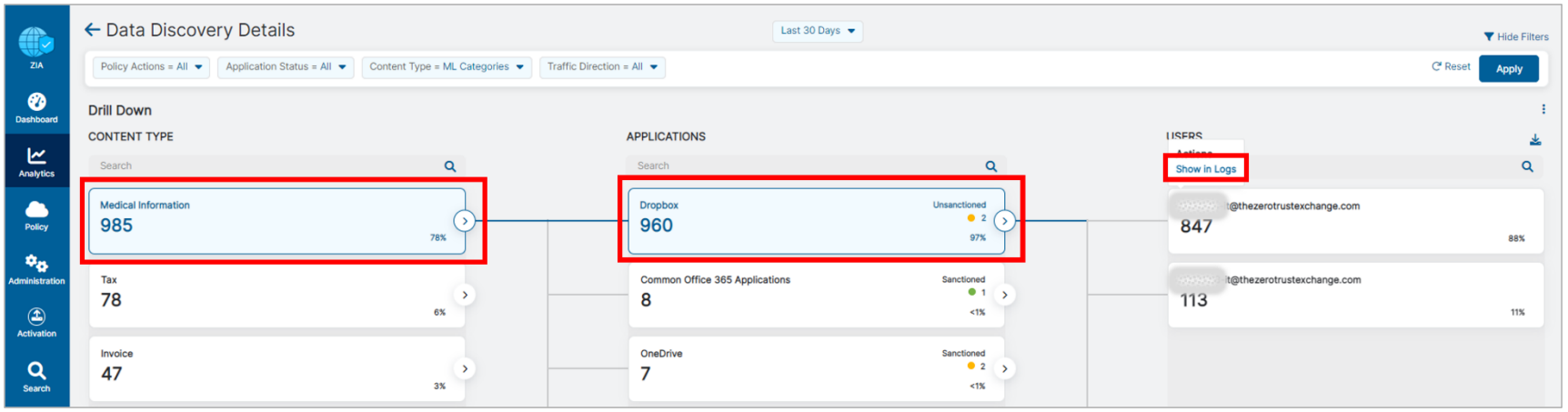


5. To review AI/ML-powered Auto Classification & Data Discovery reports, go to **Analytics > Data Discovery Report**.
6. Review the various widgets and graphs, for example the Top 10 **Users** sending sensitive content to various SaaS Applications.
7. Click **Analyze More** to get more insights into the data.

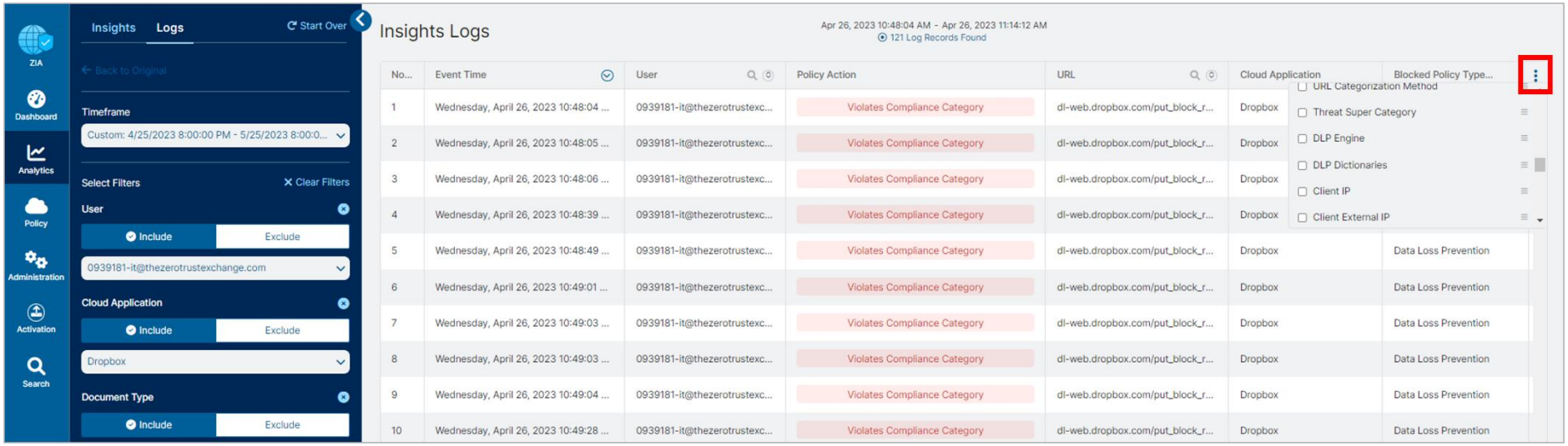


> ***Note:*** *To view more meaningful dashboard data, you may want to select a longer Timeframe from the dropdown, e.g.* ***Last 30 Days****.*

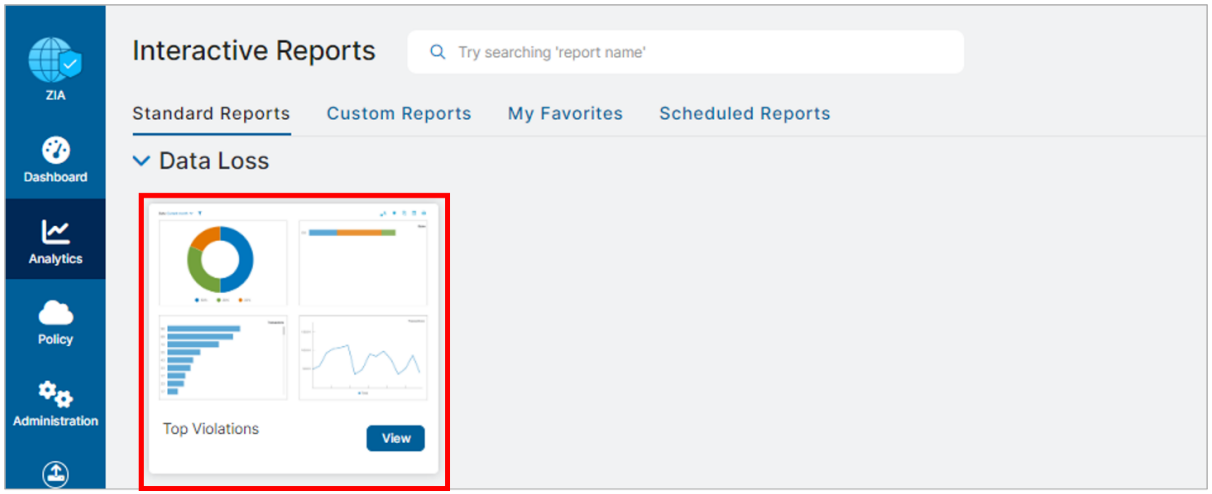
8. In the Analyze More view, you can see all the categories such as Medical Information, Invoice etc. Click on any of the categories, such as **Tax**, **Real Estate**, or **Medical Information** and it will show which Applications are used to upload sensitive content.



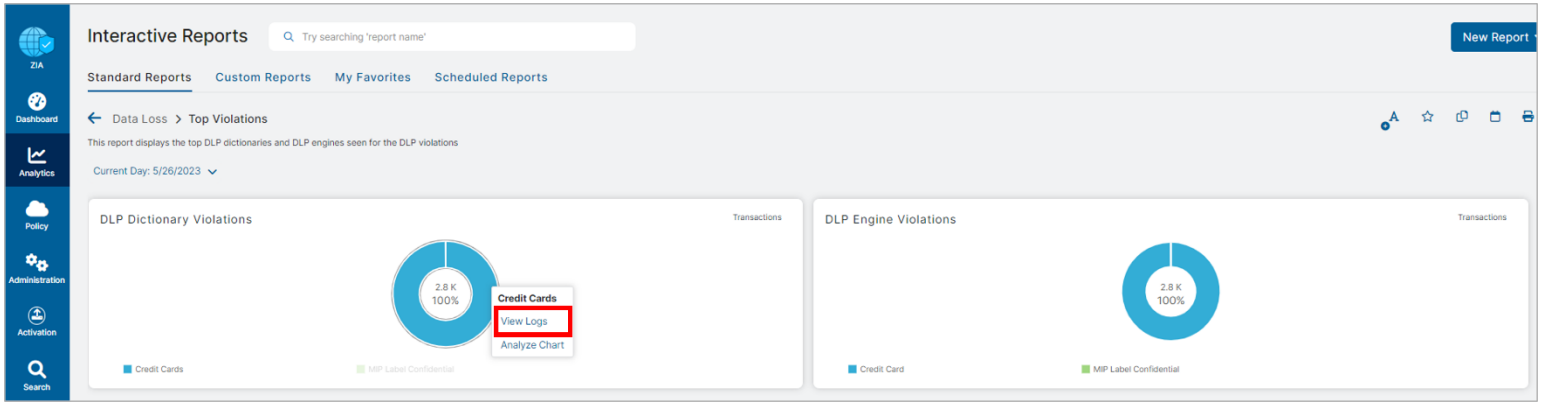
9. Clicking any **Application** will provide detailed user information.
10. Right-click on a user and select **Show in Logs**.
11. Scroll through the logs.
12. To customize the logs table, click the ⋮ icon and select/deselect table columns.



13. To review Incidents that were the result of DLP policy violations, go to **Analytics > Interactive Reports**.
14. Scroll down and click the **Data Loss** widget.



15. Here you can see the Top Violations for DLP Dictionaries and Engines. You can select the Timeframe from the dropdown menu, add notes and Analyze Charts and View Logs.

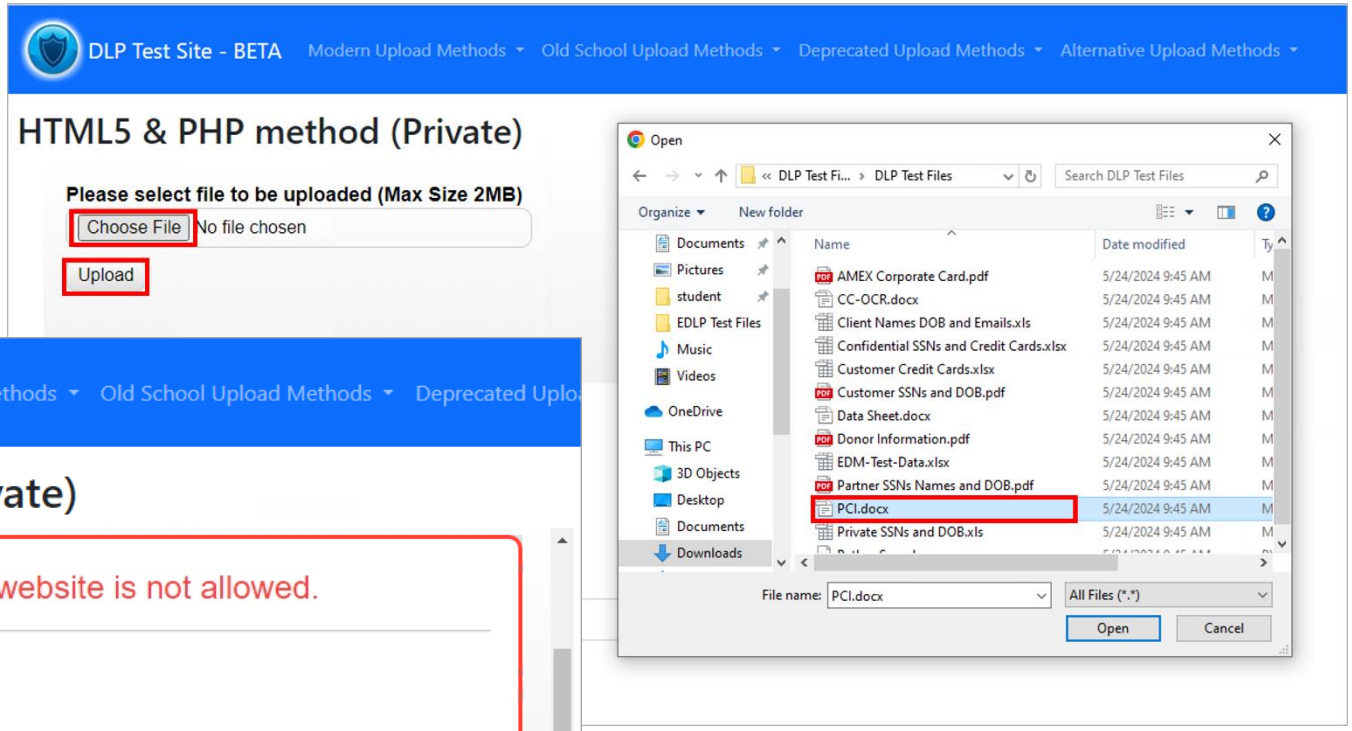


16. Click **View Logs** and review Web Insights logs, filtered based on DLP dictionaries or engines.

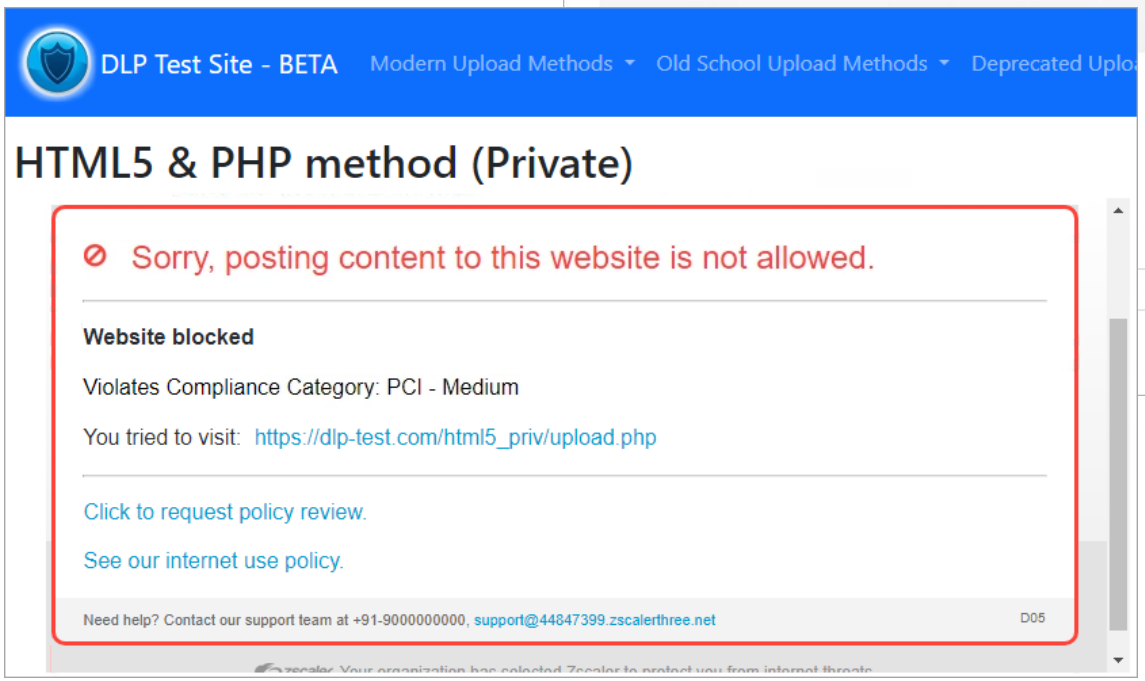
Task 10.2: Test End User Experience

In this task, you will test the end user experience content provided to you and upload it to cloud storage.

1. To test this rule, in a browser window on the **Corp: Client PC**, go to **https://dlp-test.com/html5_priv/** (a bookmark is provided).
2. Click **Choose File** and select **PCI.docx** from the **DLP Test Files** folder on the Desktop.
3. Click **Upload**.



4. Verify that a **Block** notification is displayed.



Thank you!