A screenshot of a phone

Description automatically generated

**Purpose:**

URL filters are a fundamental cybersecurity tool to prevent unauthorized internal users from gaining access to certain sites, as well as preventing outside users from accessing our internal network. The purpose of this lab is to teach us the skills required to set up an URL filter, which will help continue to familiarize us with the security capabilities of our firewall.

**Background:**

All of our configurations will be performed on Palo Alto’s GUI, or Graphical User Interface. GUIs are the visual components of applications, allowing users to control their programs using interactive elements such as buttons, and icons instead of commands in command-line interfaces.

A URL, otherwise known as Uniform Resource Locator, is a unique address that web servers use to locate pages on the internet. A URL typically has three major parts: protocol, domain, and path.

Web filters are a common tool on firewalls that are used to permit or restrict certain websites. The PA220’s web filter marks each website with a category, then checks which criteria it falls under and acts accordingly.

Certificates are digital credentials used to prove that specific websites and organizations are credible. For this lab, we are using Trusted Root Certificates, which are issued by Certificate Authorities. These certificates will be installed onto our local device, ensuring secure communication.

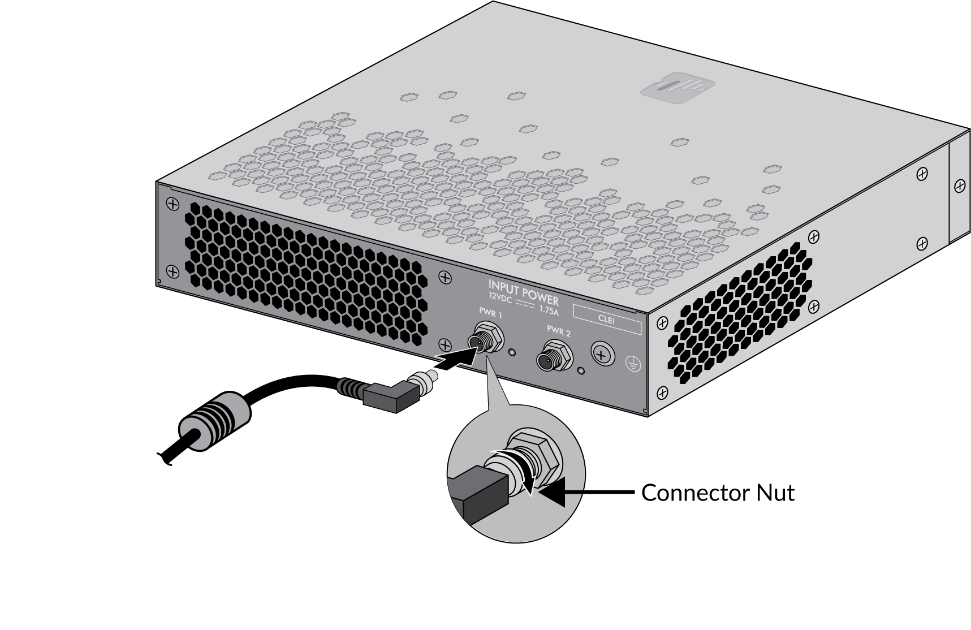
MMC, or Microsoft Management Console, can be found on Windows Operating Systems and provides administrative users with a console to manage and configure the hardware, software, or network of their device. We will be using the Certificates Snap-In to install our certificates onto our device.

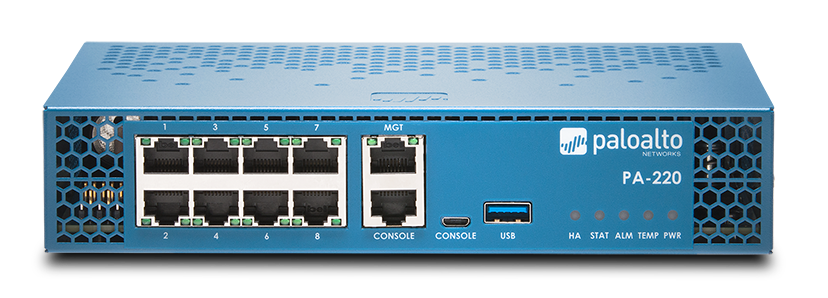
**Lab Summary:**

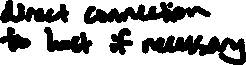
Prior to any URL Filtering configurations, we must first ensure that our firewall is updated to the latest release as older versions with security threats can render our configurations useless. We then created a URL filter by selecting categories to block, then attached it to our Outgoing Internet Policy. Next, we generated a certificate, paired it to a TLS Service Policy, and exported this certificate onto our local device. We then opened up MMC and installed our exported certificate into the Certificates Snap-In, which will have the device recognize all certificates from this source as trusted. Finally, we also implemented an override password for certain filtered sites.

**Lab Procedure:**

To turn on our firewall and get onto the Palo Alto GUI (assuming it has already been configured for SOHO use from the previous lab), follow these steps:

1. Plug the PA220 firewall into a power source using the provided power cable. 
2. Connect one ethernet cable into the firewall’s Port 1 and an internet source.
3. Connect the second ethernet cable into the firewall’s Port 2 and into the host.
4. Connect the third ethernet cable into the firewall’s Port 3 and back into its own Management Port.



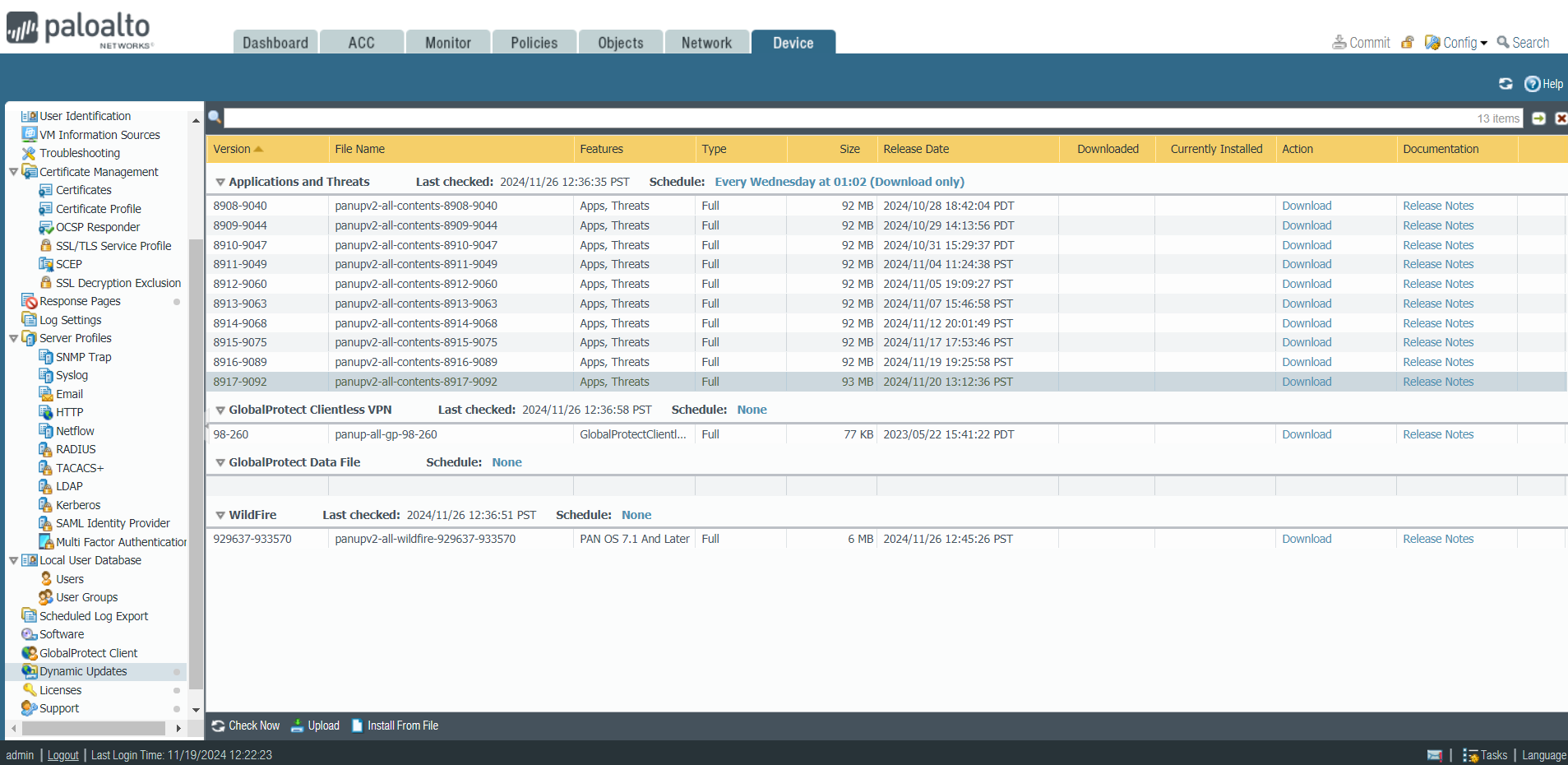


1. Launch an internet browser and enter the IP address of the firewall into the search bar as a URL (https://xxx.xxx.xxx.xxx).

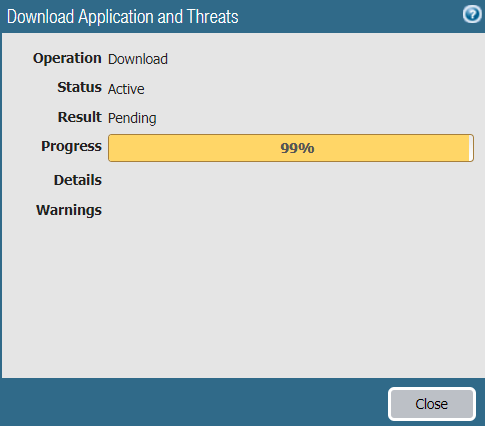
This lab will be split into 4 major portions: Updating PA220, Creating URL Filters, Installing Certificates, and Enabling Password Override.

Updating PA220

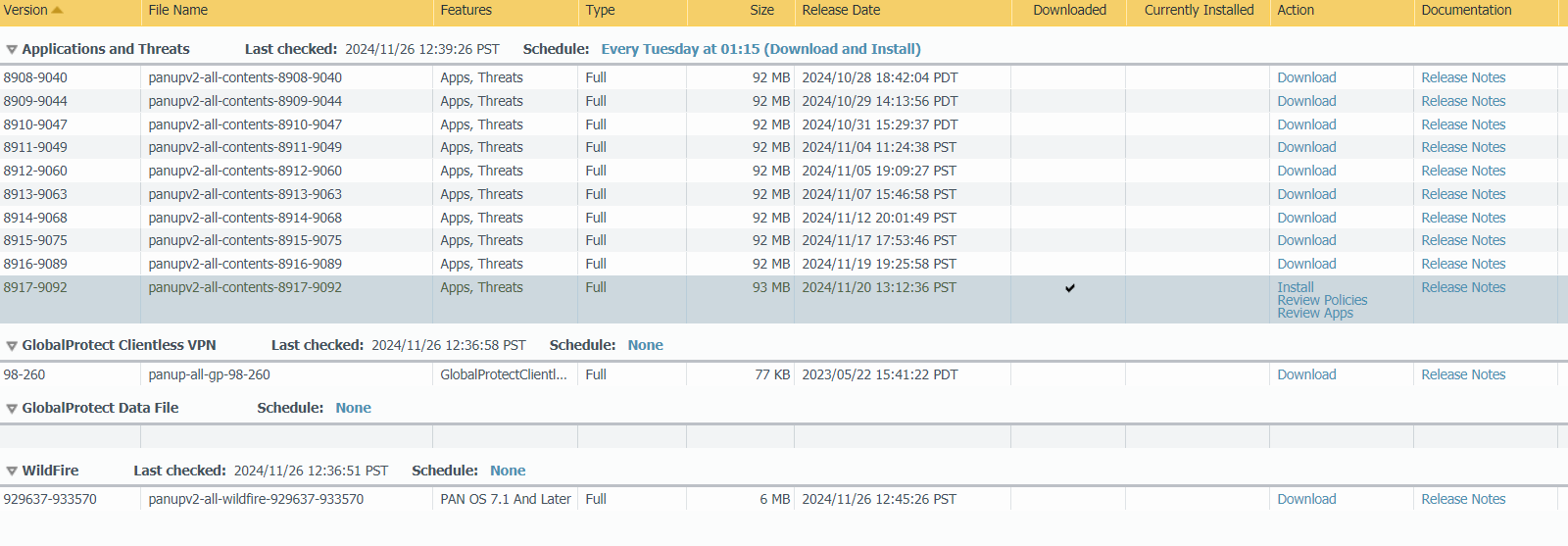
1. First, we need to download and install the latest Dynamic Content Update that Palo Alto has released, which is meant to equip the firewall with the most up-to-date threat prevention and intelligence. It is required for us to update our PA220’s version.

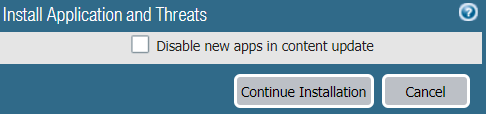


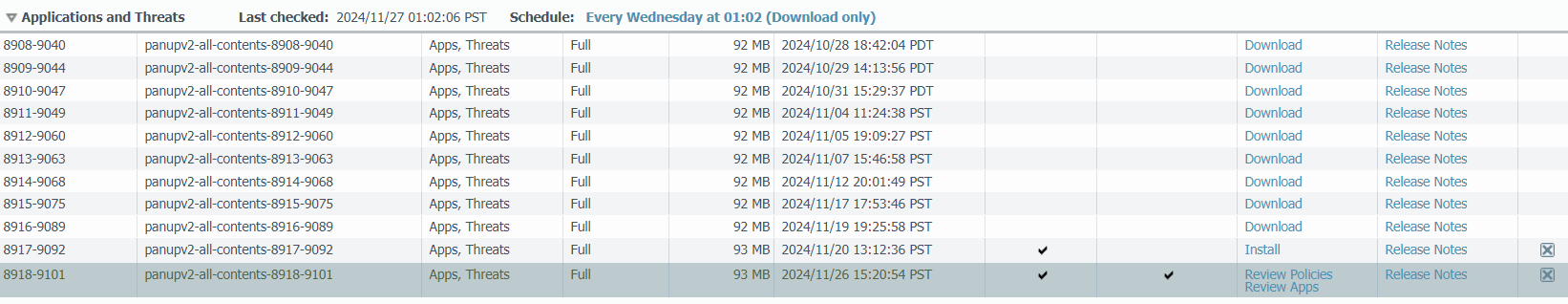
1. Select the most recently released version and click Download.



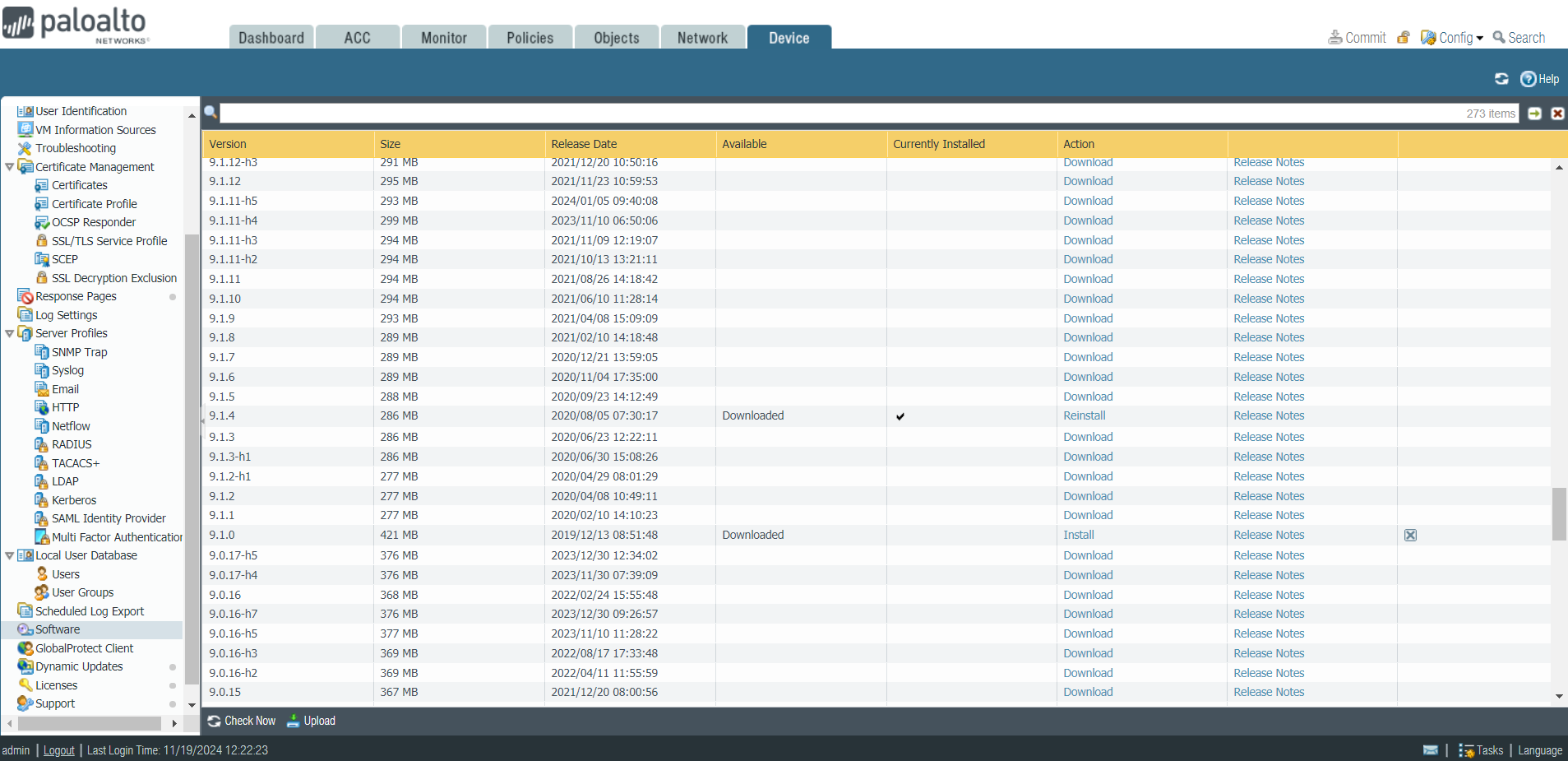
1. Once downloaded, click Install > Continue Installation.







1. Next, to check our PA220’s current version and the versions we have downloaded, go to Device > Software. For us, we are currently starting from version 9.1.4.



1. The sequence for updating the PA220 to its latest version is to download and install the latest version of the current series, then the first edition of the next series. In our case, we would want to find the latest edition of version 9.1, then move to the next version in the series, which is version 10.0.



1. Click Download. Once the download is completed, click Install.

A screenshot of a computer

Description automatically generated

A screenshot of a software update

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Once the version is installed, the firewall will request to reboot to implement changes. Click Yes.

A screenshot of a chat

Description automatically generated

1. Continue repeating this sequence of downloading, installing, and rebooting for every version. Our final sequence was 9.1.4 > 10.0.0 > 10.0.12-h6 > 10.1.0 > 10.1.14-h6 > 10.2.0 > 10.2.12-h2.
2. Once you reach the 10.1 series, it is possible that your software list is condensed like this. To see all versions and download the true latest version, uncheck Preferred Releases and Base Releases on the bottom bar.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

URL Filtering

1. To add a URL Filter to the PA220, go to Objects > URL Filtering.

A screenshot of a computer

Description automatically generated

1. Select the default filter and click the “Clone” button located on the bottom bar to create a new filter with the default settings.

A screenshot of a computer error

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Click into the newly duplicated filter and set a name.

A screenshot of a computer

Description automatically generated

1. Under Categories, switch all categories that would be inappropriate for the user to access to “block” under the column Site Access. There is also an option to allow certain categories to have a password override, which we will apply to Artificial Intelligence websites. Click Ok when finished customizing.

A screenshot of a computer

Description automatically generated

1. Next, go to Policies > Security and select our Internet Outgoing policy.

A screenshot of a computer

Description automatically generated

1. Select the Actions tab, then click on the dropdown for Profile Type and select “Profiles”.

A screenshot of a computer

Description automatically generated

1. Then, find the section labeled URL Filtering and select our URL Monitoring filter that we just set up. Click “Ok”, then commit the changes.

A screenshot of a computer

Description automatically generated

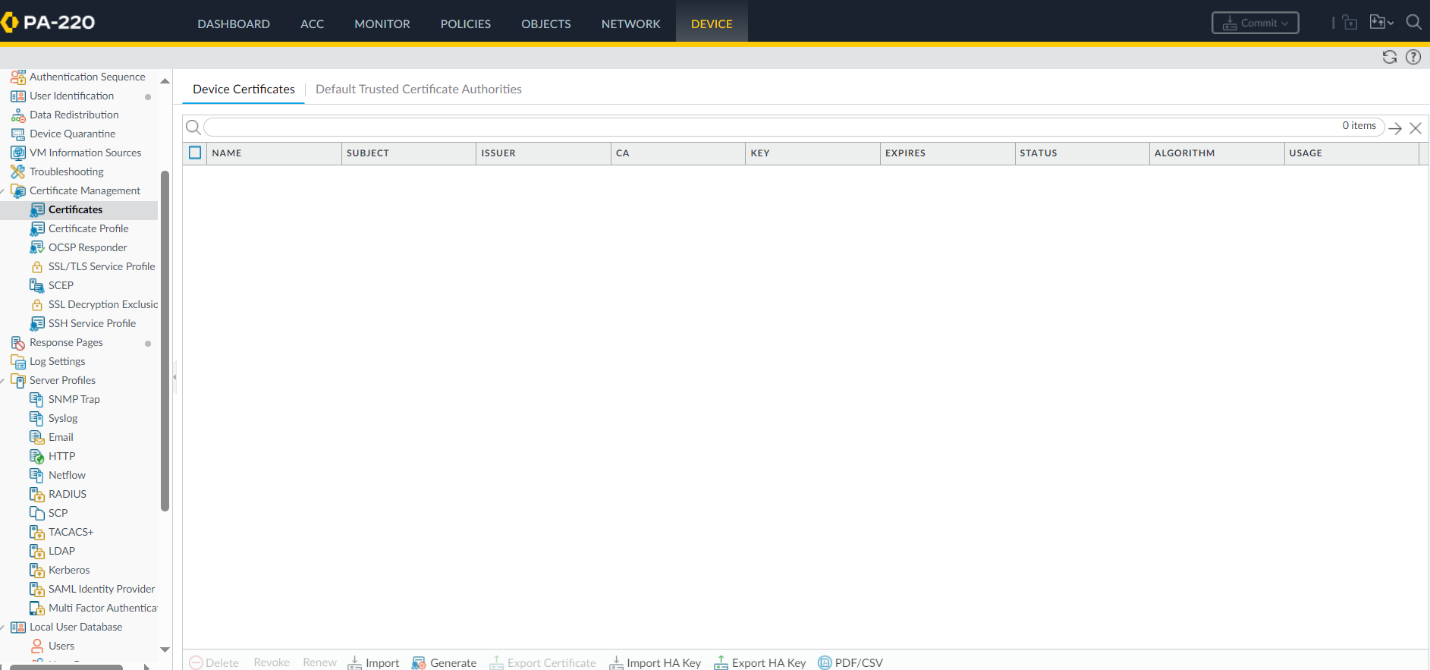
If you go to Monitor > URL Filtering, you should now see that website activity will be logged.

A screenshot of a computer

Description automatically generated

Installing Certificate

1. Go to Device > Certificate Management > Certificates. Click “Generate” on the bottom bar.



1. Set a name for the certificate. Click “Generate” again on the pop-up menu to save the certificate (default settings will work fine). Make sure Certificate Authority is checked.

A screenshot of a computer

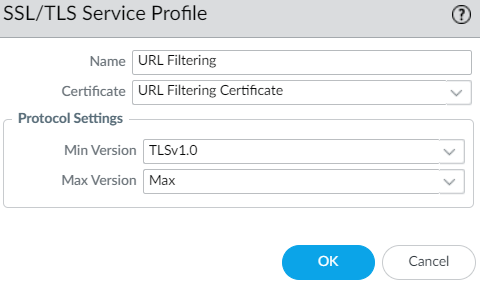
Description automatically generated

1. Staying under Device > Certificate Management, switch to the tab titled SSL/TLS Service Profile.

A screenshot of a computer

Description automatically generated

1. Click “Add” located on the bottom bar. Name the profile, then select our previously created certificate for Certificate dropdown. Click “Ok” and commit the changes.



1. Going back to the Certificates tab, click the “Export Certificate” button on the bottom bar.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Now we install to our local device. In the Windows search bar, type “mmc” to open up Microsoft Management Console.

A screenshot of a computer

Description automatically generated

1. Go to File > Add/Remove Snap-in.

A screenshot of a computer

Description automatically generated

1. Click Certificates > Add, then select the Console Root snap-in and click “Ok”.

A computer screen with a few screenshots

Description automatically generated

1. Click “My User Account”, then “Finish” for the Certificate Snap-In window that pops up.

A screenshot of a computer

Description automatically generated

1. Open the Certificates folder under the Trusted Root Certification Authorities folder dropdown. Select an existing certificate, then go to the Actions sidebar and click More Actions > All Tasks > Import.

A screenshot of a computer

Description automatically generated

1. File Explorer will open. Navigate to the certificate that we downloaded and import.

A screenshot of a computer

Description automatically generated

When the user attempts to access unauthorized pages, they will now see a screen like so:  
A screenshot of a computer

Description automatically generated

Enabling Password Override

1. Go to Device > Setup. Then, click the “Add” button on the panel titled URL Admin Override.

A screenshot of a computer

Description automatically generated

1. Create a password and retype to confirm. Set the SSL/TLS Service Profile to “URL Filtering” and the Mode to “Transparent”.

A screenshot of a login screen

Description automatically generated

1. Click Ok, and you should now see that you have an entry under URL Admin Override. Commit the changes.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

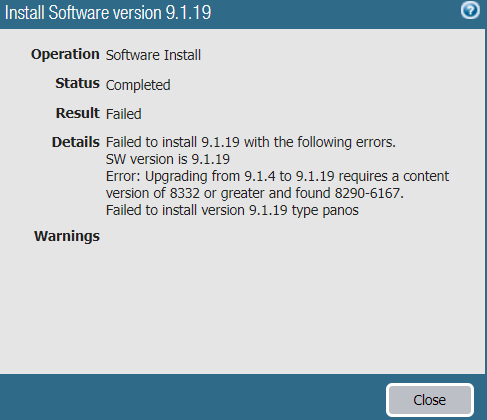
When a user attempts to access a page with a password override option, it’ll look like this:

A screenshot of a computer

Description automatically generated

**Problems:**

One major source of problem that we had was that we were unable to update our firewall to the latest version since we didn’t know about Dynamic Content Updates, which would give us this error message. After searching the error message online, we were able to find a guide that resolves this issue, which instructed us to navigate to the Dynamic Content Update tab and install the latest version of that.



Another issue that we occasionally encountered was due to the fact that we had to keep redownloading our certificate since our device would reset every time that we had to leave for our next period. This caused us inconsistencies as sometimes our certificate wouldn’t work for our block pages, making it impossible to password override our selected sites.

**Conclusion:**

In this lab, we learned how to set up URL filtering on our PA220 firewall. We also gained a deeper understanding of how URL filtering, digital certificates, and TLS services work together into guaranteeing network and device security. Overall, it was a valuable lab that taught us a common cybersecurity configuration skill.

**Sign Off:**

