FortiEDR

Lab Guide

for FortiEDR 5.0

FORTINET NSE Training Institute

Fortinet Training

https://training.fortinet.com

Fortinet Document Library

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://training.fortinet.com/local/staticpage/view.php?page=certifications

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Feedback

Email: askcourseware@fortinet.com

FORTINET

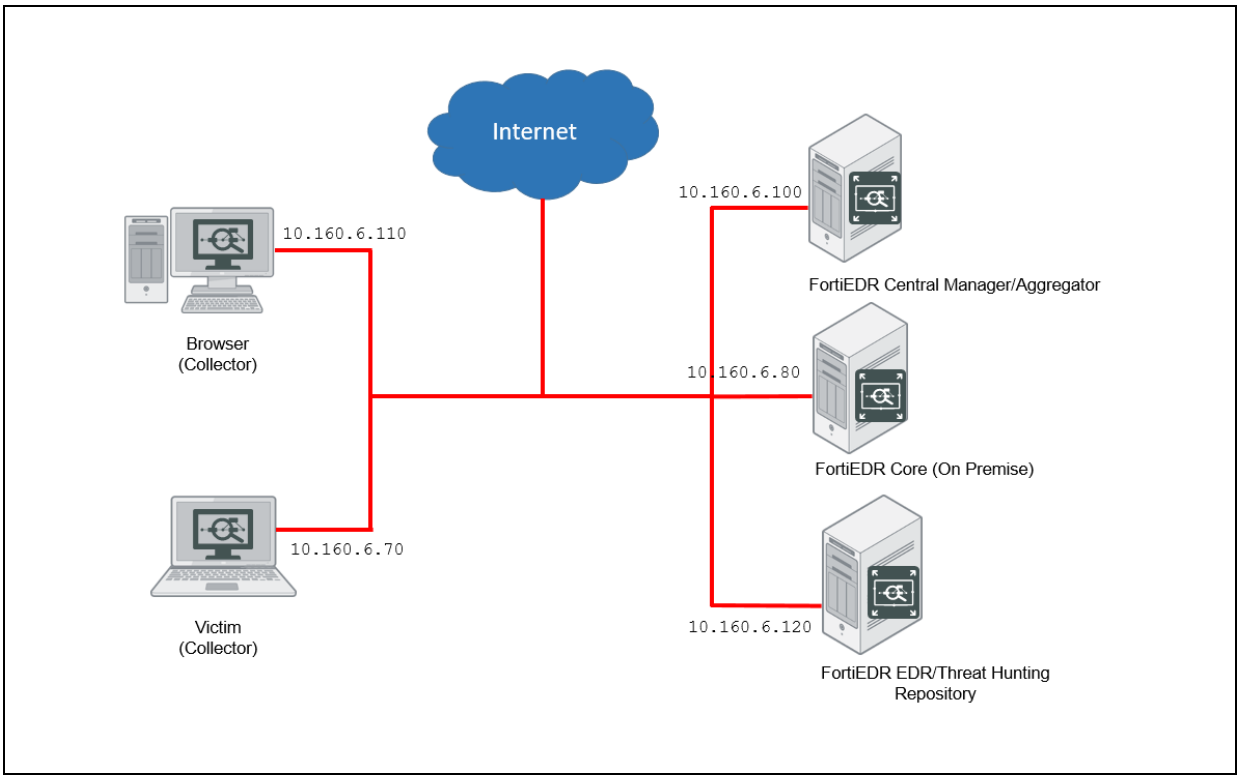
2/7/2022

TABLE OF CONTENTS

Network Topology 5
Lab 1: Installation and Architecture 6
Exercise 1: Installing and Configuring FortiEDR Server Components 8
Install and Configure the FortiEDR Core 8
Connect to the Management Server Console 12
Exercise 2: Installing the Collector 14
Reinstall the Collector Using the Automated Installer File 15
Lab 2: Administration 19
Exercise 1: Managing a FortiEDR Collector 20
Put the Collector Into Isolation Mode 21
Exercise 2: Creating a New Administrative User 25
Lab 3: Security Policies 28
Exercise 1: Managing Security Policies 29
Exercise 2: Understanding NGAV Operations 34
Exercise 3: Understanding the Difference Between NGAV and Post-Infection Protection 38
Lab 4: Playbooks 41
Exercise 1: Managing Playbooks 42
Lab 5: Communication Control 44
Exercise 1: Configuring Communication Control 45
Create a Rule to Block Applications Based on Reputation 45
Deny Communication Manually From an Application That Is on Your Organization's Block List 47
Allow Applications to Communicate Externally for Specific Groups 49
Exercise 2: Troubleshooting Webex Connections 54
Lab 6: Events and Alerting 57
Lab 7: Events, Alerts, and Forensics 58
Exercise 1: Aggregating Alert and Export Events 59
Exercise 2: Examining Event Work Flow 61
Create an exception 65
Lab 8: Fabric Integration and FortiXDR 67
Lab 9: RESTful API 68

Exercise 1: Configuring the RESTful API **69**
Investigate a Security Event 75
Remediate the Device 78
Exercise 2: Investigating and Creating an Exception for a Safe Process **82**
Investigate a User Issue With a Safe Process 82
Lab 10: Troubleshooting **85**
Exercise 1: Troubleshooting Newly Installed Collectors **86**
Exercise 2: Troubleshooting the Syslog Watcher Process **94**
Create an Exception to Use Syslog Watcher 98

Network Topology



Lab 1: Installation and Architecture

In this lab, you will examine the FortiEDR component installation and architecture.

Objectives

- Copy the installer file to the core server
- Install the core
- Configure the core
- Connect to the management console
- Install the collector
- Uninstall the collector and reinstall it using an automated installer

Time to Complete

Estimated: 45 minutes

Prerequisites

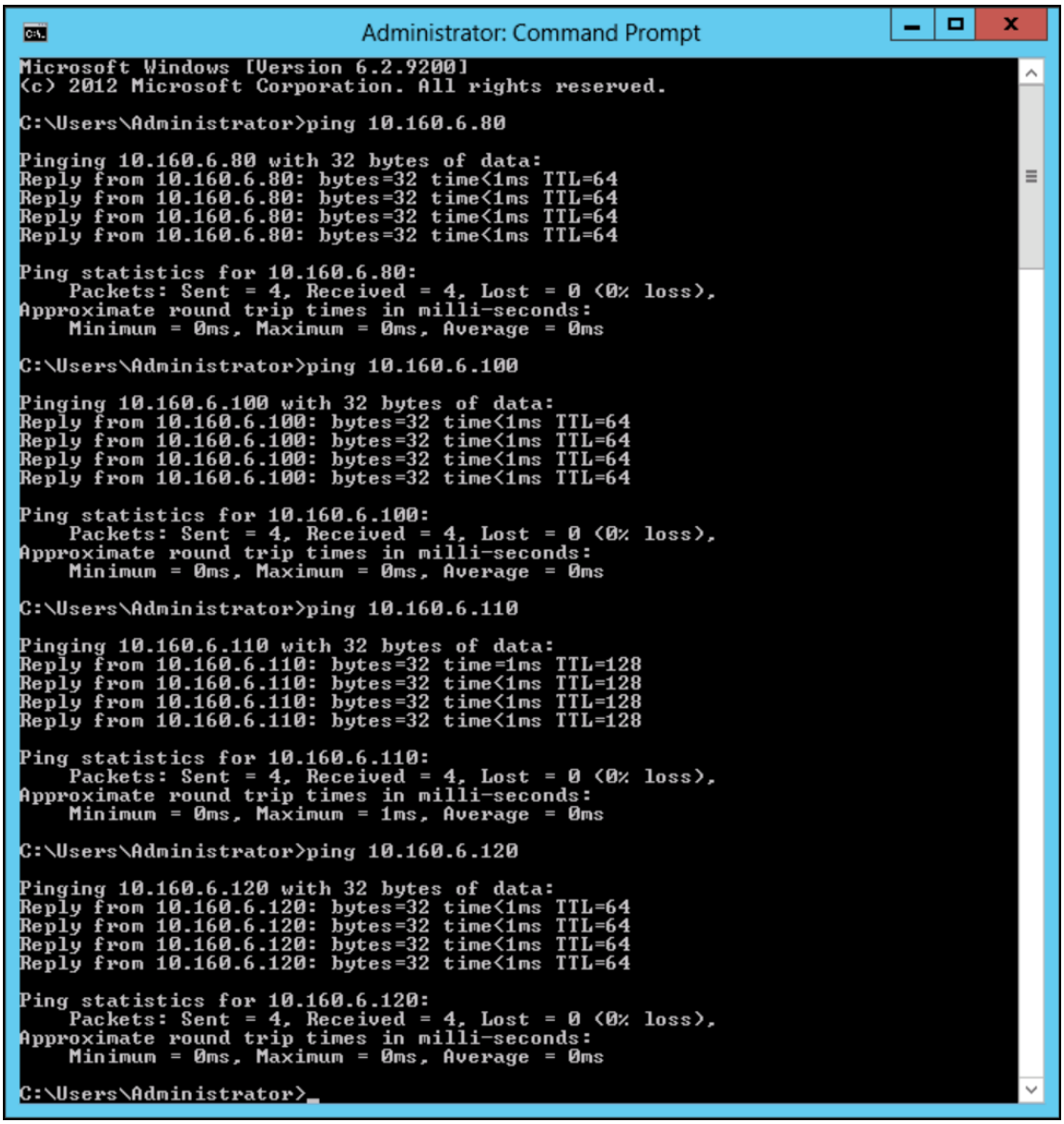
Before beginning this lab, you must verify the connectivity of all FortiEDR components.

To verify connectivity

1. On the left side of the window, click the **Browser** link.
2. On the Browser VM, open a command prompt (**Start** > **Command Prompt**) or PowerShell, and then ping the following IP addresses:

Name	IP address
Victim-Windows	10.160.6.70
FortiEDR Core	10.160.6.80
FortiEDR Central Manager Console	10.160.6.100
FortiEDR Threat Hunting Server	10.160.6.120

You should be able to ping all of the IP addresses from the Browser VM.



Exercise 1: Installing and Configuring FortiEDR Server Components

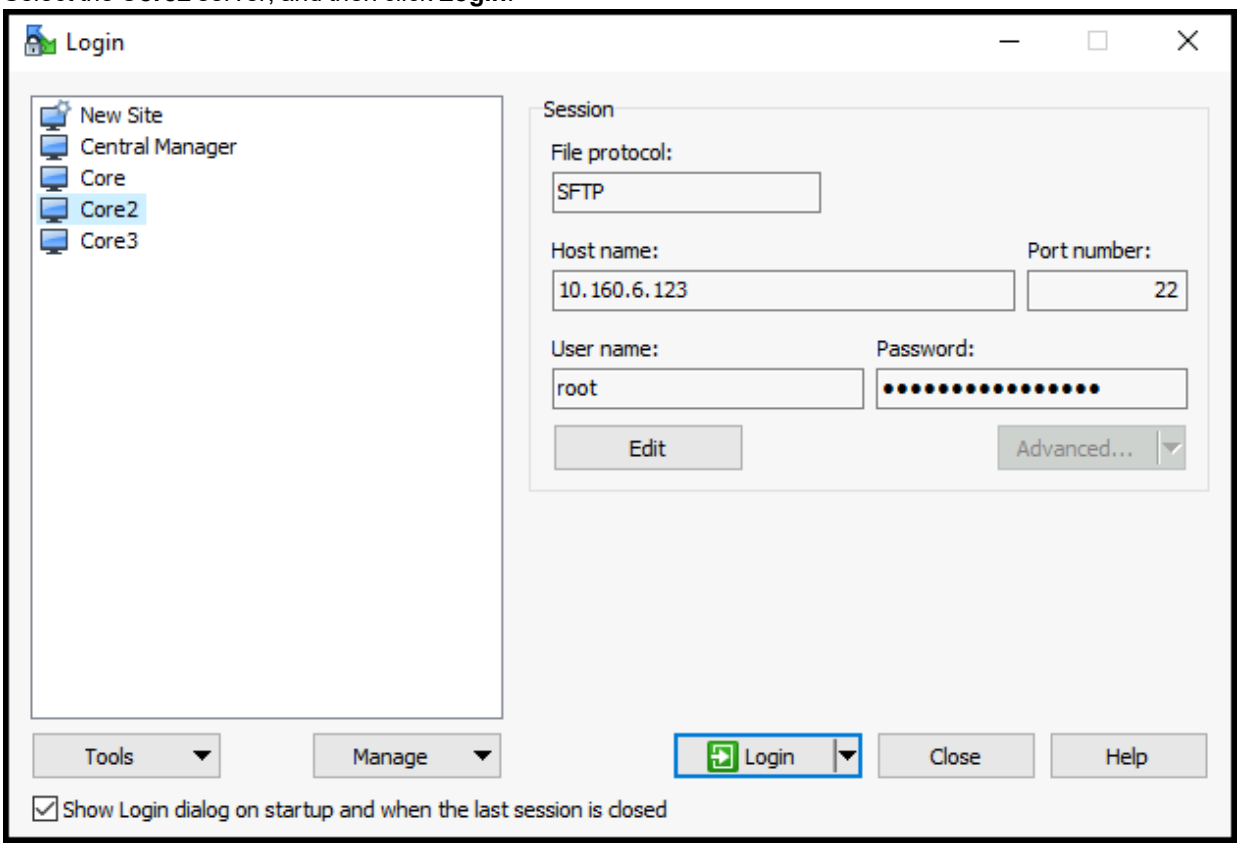
In this exercise, you will install and configure the FortiEDR core, and then access the FortiEDR GUI.

Install and Configure the FortiEDR Core

You will copy the installer file to the server, and then run a file to install the core.

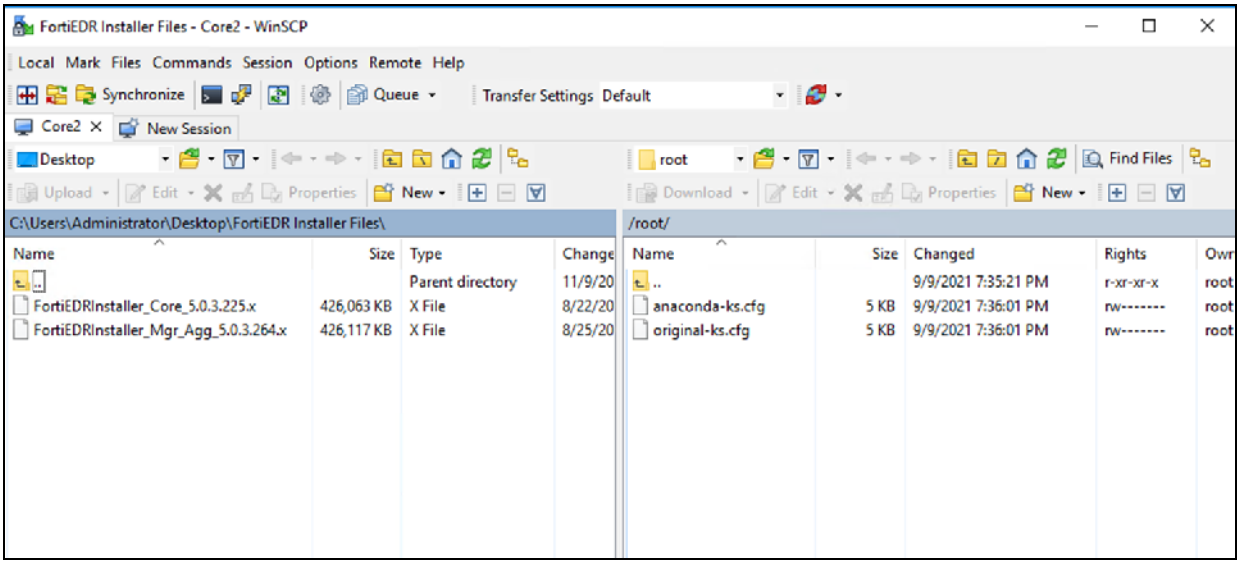
To copy the installer file

1. On the Browser VM, open WinSCP using the shortcut on the desktop.
2. Select the **Core2** server, and then click **Login**.

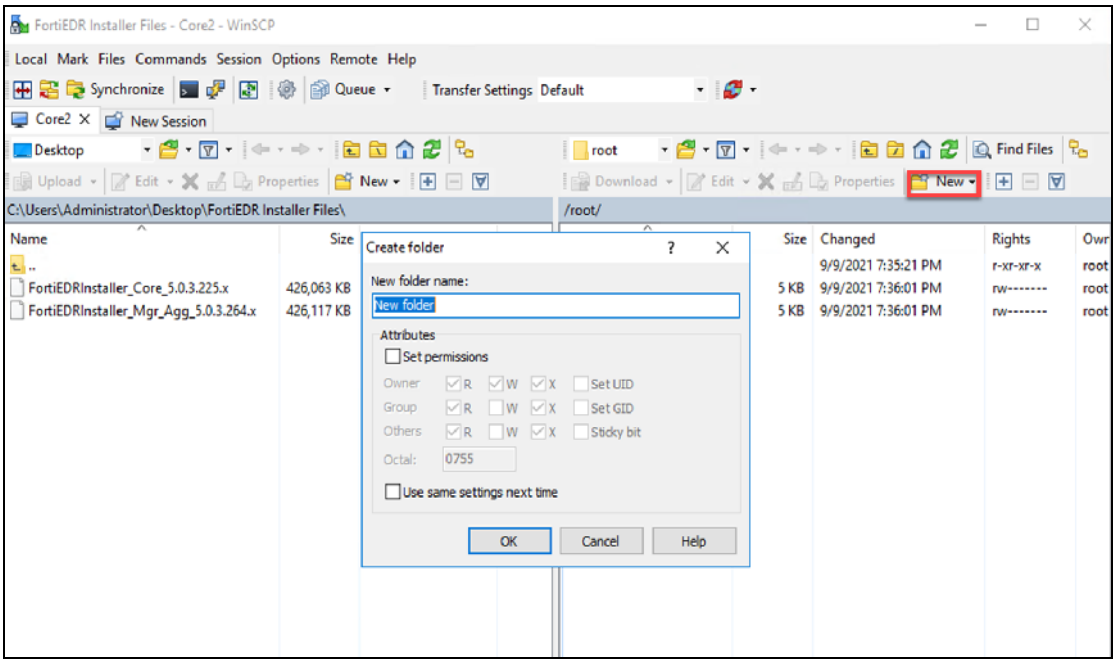


3. In the left panel of the WinSCP window, check the address bar to make sure that you are in the `FortiEDR Installer Files` directory. If not, navigate to that directory—it is located in **Desktop**.

Click the **..** folder at the top to go up one level.

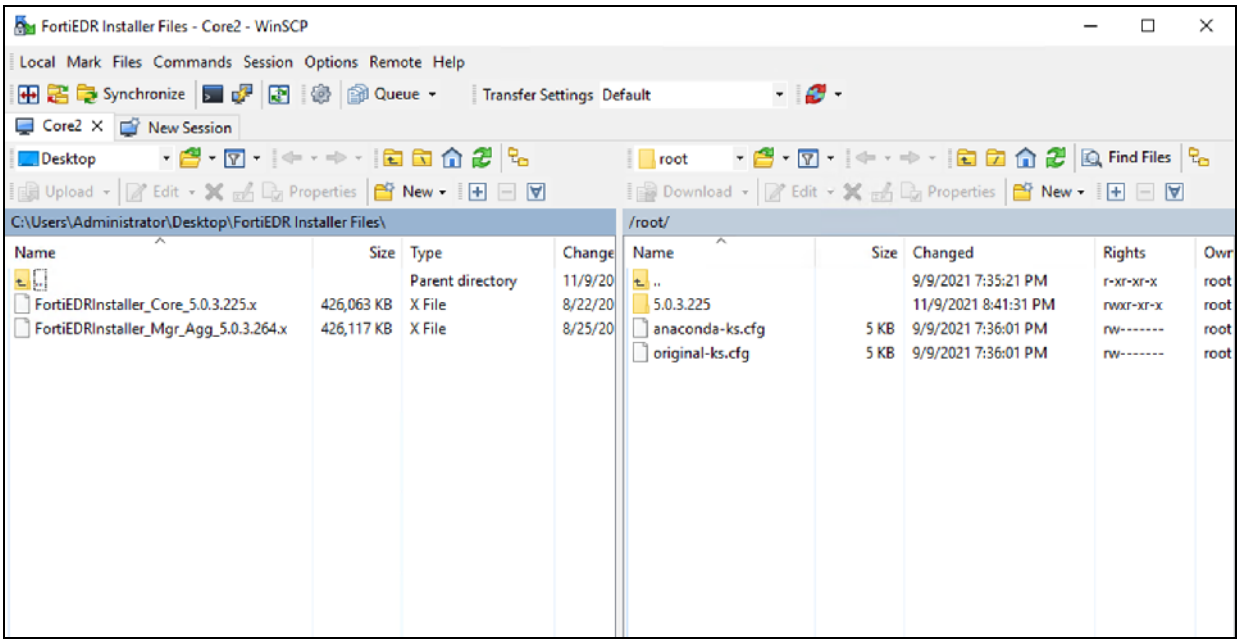


4. Make sure that the right panel is in the `/root` directory.
5. At the top of the right panel, click the **New** drop-down list, and then select **Directory**.
6. In the **Create folder** window, type a folder name that matches the version number of the most recent installer file `5.0.3.225`, and then click **OK**.



The new folder should appear in the right panel.

7. Double-click the folder to open it.



8. In the left panel, select the file that begins with `FortiEDRInstaller_Core_5.0.3.225.x`, and then drag it into the right panel to copy it into the new folder.
9. Click **OK** to copy the file.

To install the core

1. On the Browser VM desktop, double-click the **Core2** shortcut to log in using SSH.
2. Click inside the console window, type `cd 5.0.3.225`, and then press `Enter` to go to the installer directory.

Type `5.0`, and then press `Tab`. If there is only one folder that begins with 5.0, the rest of the folder name will be completed for you.

3. Type `ll`, and then press `Enter` to see the contents of the directory.
   You should see the file starting with `FortiEDRInstaller_Core_5.0.3.225`.
4. Type `chmod +x *.x`, and then press `Enter`.
5. Type `ll`, and then press `Enter`.
   The file should now appear in green, indicating that it is an executable file.
6. Type `./FortiEDRInstaller_Core_5.0.3.225.x`, and then press `Enter`.
   Wait until the installation is complete.

Note that the command is case sensitive.

7. Type `shutdown -r`, and then press `Enter` to restart the VM.
   Wait a couple of minutes for the reboot to finish.

To configure the core

1. On the Browser VM desktop, double-click the **Core2** shortcut to log in using SSH.
2. In the core console window, type `fortiedr config`, and then press `Enter`.
3. In the **Please select the device role** prompt, use the arrow keys to select **Next** to accept the selected role of **core**.
4. In the **Please enter your hostname** prompt, type `FortiEDR-core`, use the arrow keys to select **Next**, and then press `Enter` to continue.
5. In the **Please enter the organization name** prompt, leave the field empty, and then select **Next**.
6. In the **Please pick your registration password** prompt, type `DemoRegister` twice, and then select **Next**.
7. In the **Please enter the aggregator ip address or dns name** prompt, type `10.160.6.100`, and then select **Next**.
8. In the **Please enter the core external ip address** prompt, type `10.160.6.123`, and then select **Next**.
9. In the **Please pick your primary interface** prompt, select **ens160**, and then select **Next** to accept.
10. In the **Do you want to use dhcp** prompt, use the arrow keys and space bar to select `No`, and then select **Next**.
11. In the **Please set your ip address with prefix** prompt, accept the default IP address `10.160.6.123/24`, and then select **Next**.
12. In the **Please set your default gateway** prompt, accept the default gateway `10.160.6.254`, and then select **Next**.
13. In the **Please set your DNS server** prompt, select **Next** to accept the DNS server that is displayed.
14. In the **Do you want to set the environment in debug mode?** prompt, select **Next** to accept the default value of **No**.
15. In the **Please set the date** prompt, verify the date and change it if necessary (use the format **YYYY-MM-DD**), and then select **Next**.
16. When prompted, type the code for your continent (for example, `2` for Americas), country (for example, `49` for US), and time zone.
17. In the **Please set your Time** prompt, update the time if necessary, using a 24-hour format (for example, `14:15`), and then select **Next**.
18. In the **Do you want to enable web-proxy for the manager?** prompt, select **Next** to accept the default value of **No**.
19. Wait a minute while the installation processes, until you see the **Installation completed successfully** message.
20. Type `shutdown -r`, press `Enter`, and then wait a couple of minutes for the reboot to finish.
21. Close the console window, and then click **Core2** again to log in after the reboot.
22. Type `uptime`, and then press `Enter` to verify that the machine has rebooted.
    You should see that your current session has been running a very short time.
23. Type `fortiedr status`, and then press `Enter`.
    The `core` should be running.
24. If the `core` is not running, do the following:
    a. Type `fortiedr start`, and then press `Enter`.
    b. Type `fortiedr status` again to check the process status.

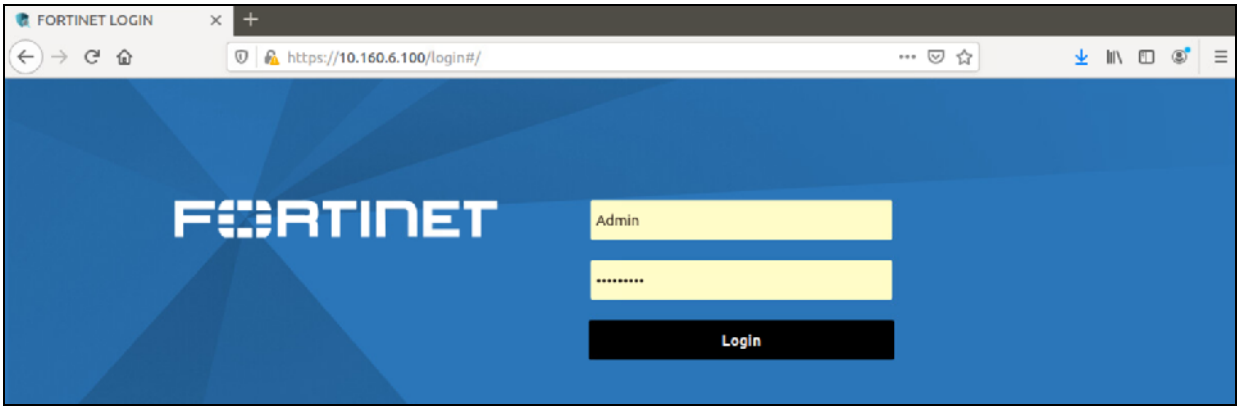
In this lab setup, the FortiEDR central manager and aggregator are preinstalled and configured. To configure these roles on the same machine, you must select *both*, and configure all settings required by the machine. Most of the settings are similar to other FortiEDR components that you configured in this exercise. The threat hunting repository is also preinstalled and configured, because the installation takes several minutes to complete. See the latest version of the *FortiEDR Installation and Administration Guide* for more details.

Connect to the Management Server Console

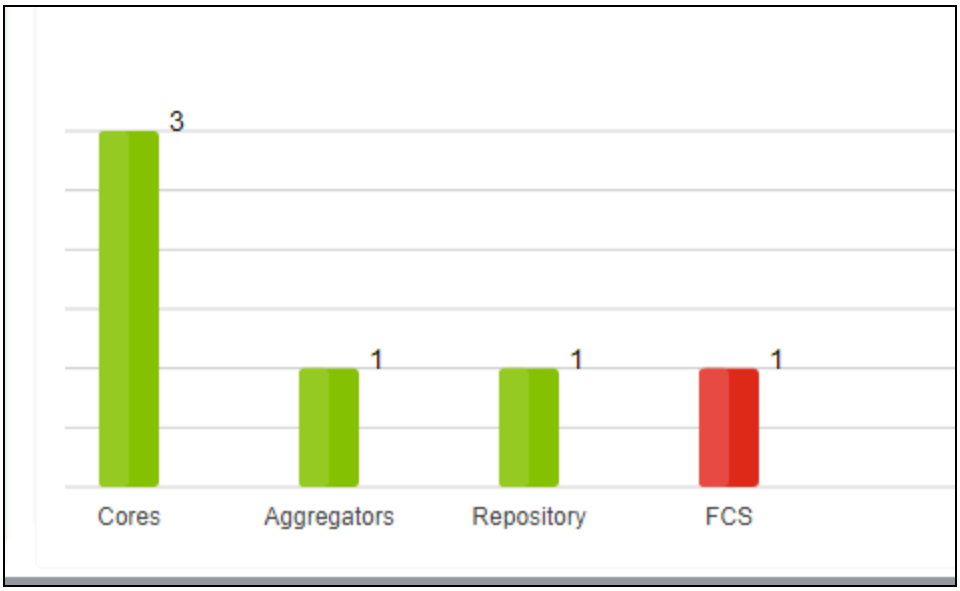
You will connect to the FortiEDR GUI.

To connect to the management server console

1. On the Browser VM, open a browser, and then connect to `https://10.160.6.100`.
2. If a warning appears stating that the site is not secure, click **Advanced**, and then proceed to the console.
3. At the login prompt, enter the username `Admin` and password `secureNOT` to log in to the FortiEDR GUI.



4. On the **DASHBOARD** tab, scroll to the bottom-right corner to find the **SYSTEM COMPONENTS** chart.
5. Verify that the **Cores**, **Aggregators**, and **Repository** are **Running**.



FCS is listed as **Disconnected** (red). This is because the lab environment is not configured with FCS. In a live environment, FCS should be listed as **Running** (green).

If the **Repository** appears as **Degraded**, reboot the core. On the Browser VM desktop, double-click the **Core** shortcut to log in using SSH. In the core console window, type `reboot`, and then press `Enter`. Wait a minute or two and then refresh the **DASHBOARD** tab on the FortiEDR GUI.

Exercise 2: Installing the Collector

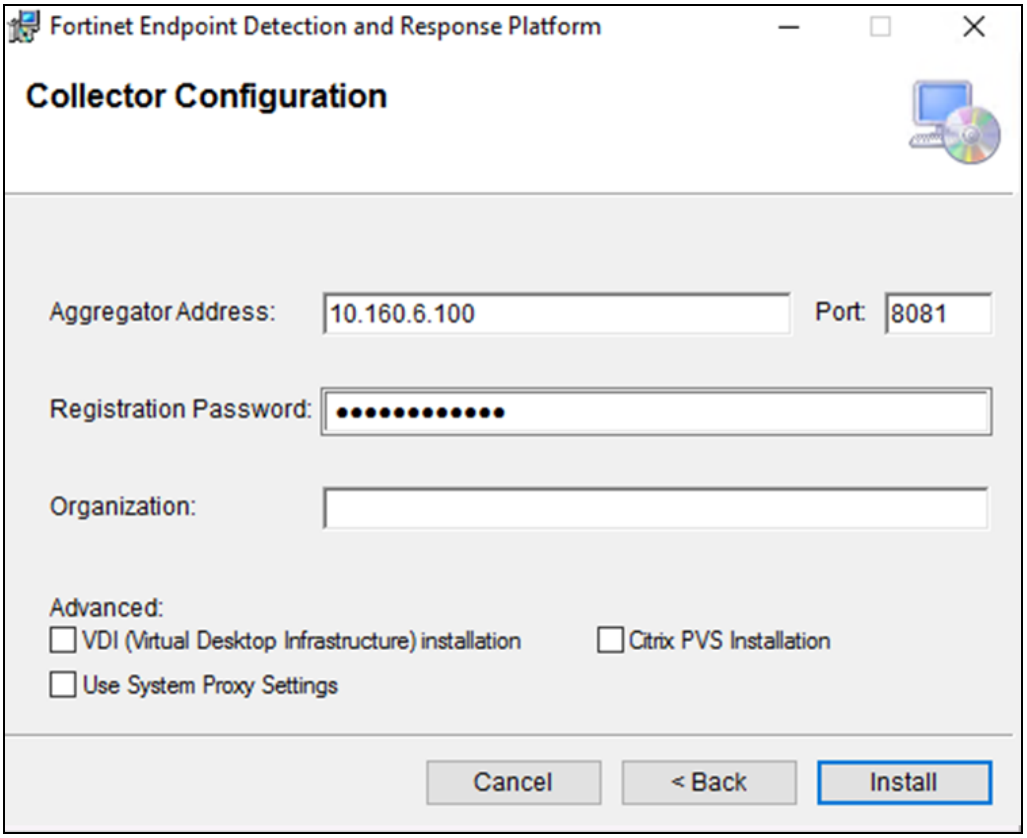
In this exercise, you will install the collector using standard and automated installer files.

To install the collector using the standard installer

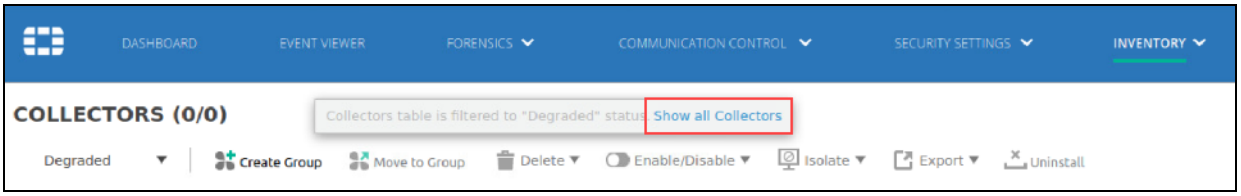
1. On the Victim VM desktop, open the **Resources** folder.
2. Double-click the `CollectorInstaller64_5.0.2.261.msi` file to launch the installer, and then click **Run** to start the installation.
3. Click **Next** until you reach the **Collector Configuration** screen.
4. Configure the following settings:

Field	Value
Aggregator Address	10.160.6.100
Port	8081
Registration Password	DemoRegister

Leave the **Organization** field empty.



5. Click **Install** to start the installation—accept any **User Account Control** warnings that appear.
6. When the **Installation Complete** screen appears, close the installer.
7. On the Browser VM, repeat steps 1 to 5 with the `CollectorInstaller64_5.0.2.261.msi` file.
8. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
9. Click the **INVENTORY** > **Collectors** tab.
10. Click the **Show all Collectors** link.



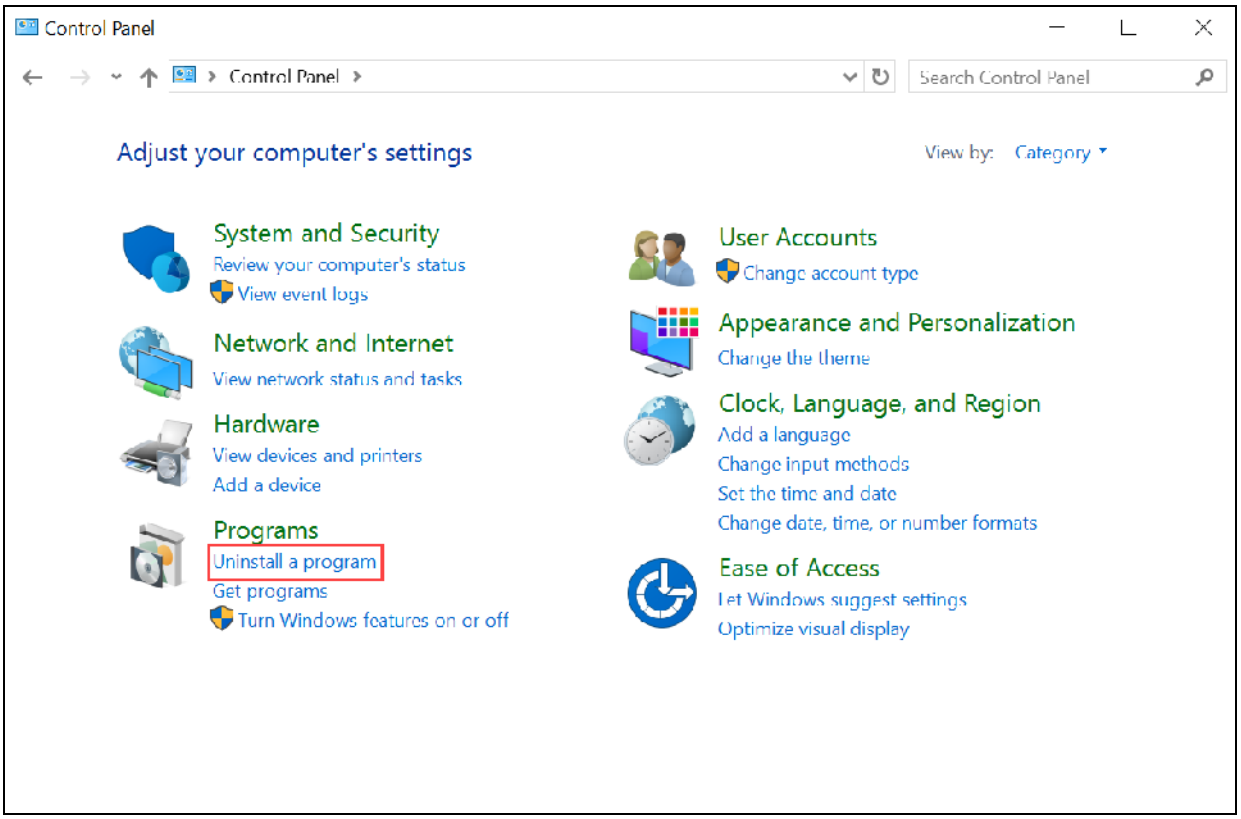
11. Click to expand the **Default Collector Group**.
    You should see the collectors that you installed.
12. If a collector appears as **Disconnected**, wait a few minutes, and then refresh the browser. If the collector still appears as **Disconnected**, you may need to reboot the Windows VMs.

Reinstall the Collector Using the Automated Installer File

You will reinstall the collector using the automated installer file. First, you must uninstall the previous collector agent.

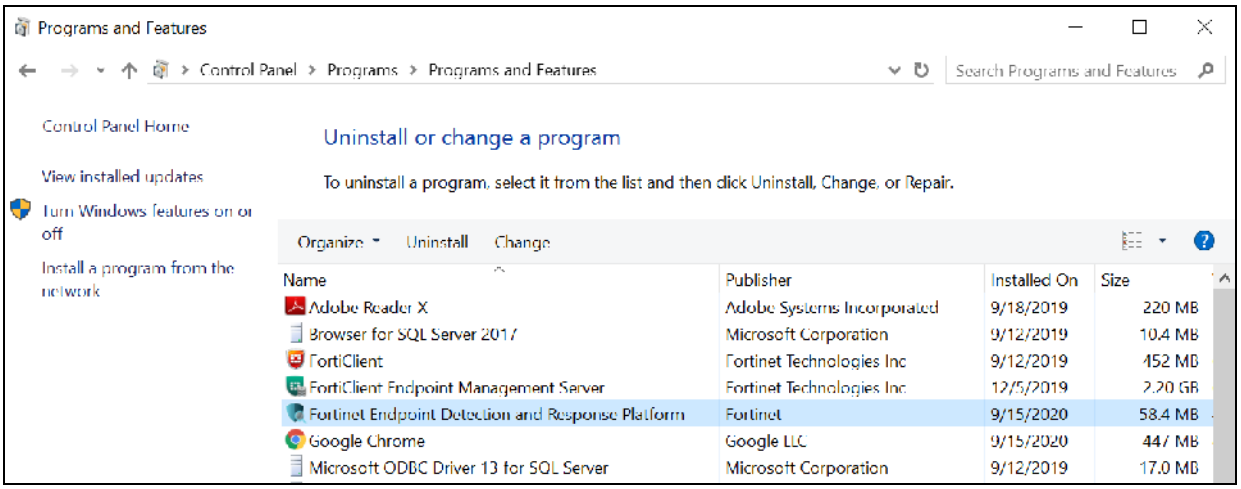
To uninstall the collector

1. On the Browser VM, open the Control Panel (**Start** > **Control Panel**), and then click **Uninstall a program**.

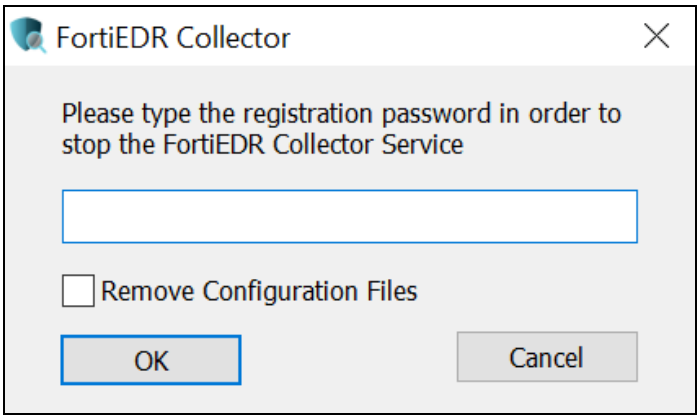


The Windows **Uninstall or change a program** window appears.

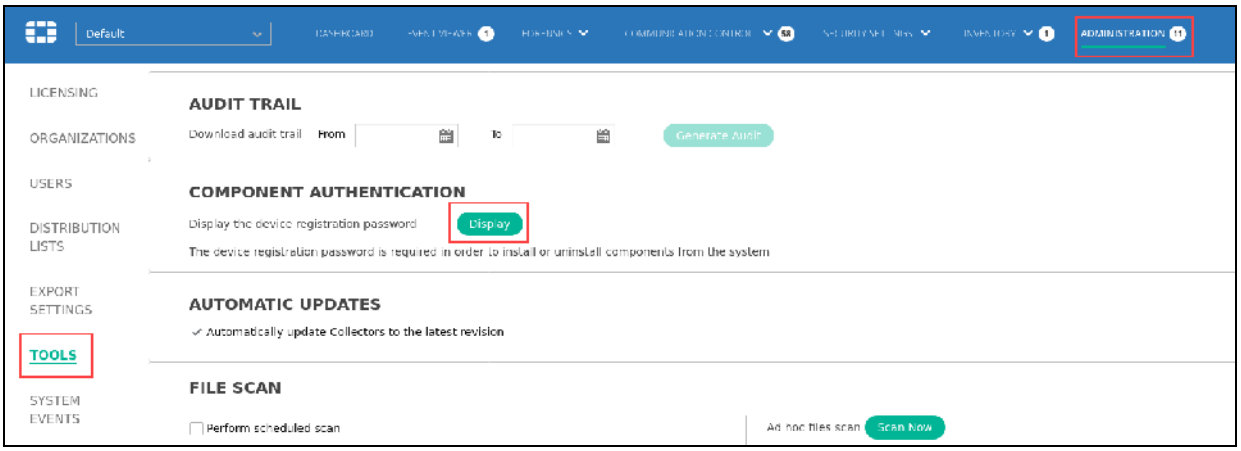
2. Locate and double-click **Fortinet Endpoint Detection and Response Platform**.



3. In the verification pop-up window, click **Yes**.
4. If a **Windows User Account Control** warning appears, click **Yes** to proceed.
5. When prompted, type the registration password to stop the FortiEDR Collector Service.
   You can find this password in the FortiEDR management console.

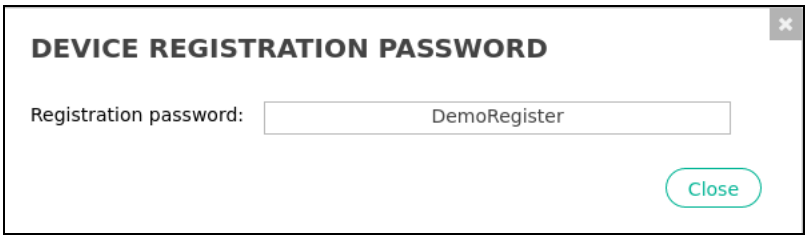


6. Return to the FortiEDR GUI, click the **ADMINISTRATION** tab, and then in the left panel, click **Tools**.
7. Under **COMPONENT AUTHENTICATION**, click **Display**.

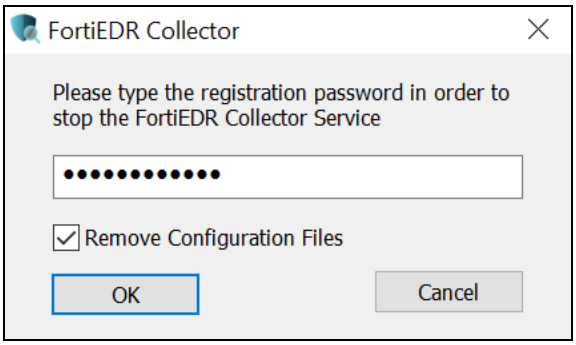


The **DEVICE REGISTRATION PASSWORD** window appears.

8. Copy the password.



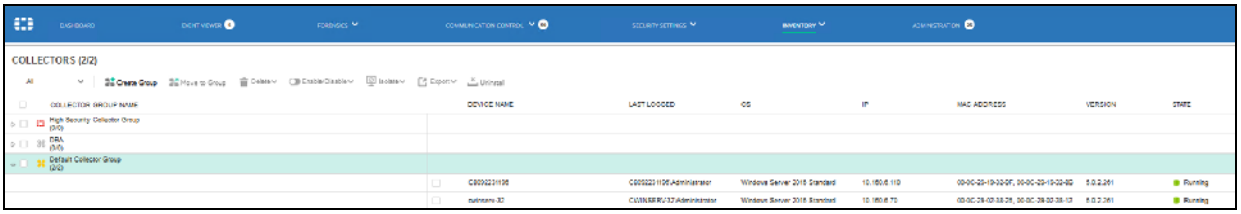
9. Return to the uninstall window, and then paste the password in the field.



10. Select the **Remove Configuration Files** checkbox, and then click **OK**.
11. When the uninstall process is complete, return to the FortiEDR GUI, and then click the **Inventory** tab.
    You should see that the collector is now listed as **Disconnected** in the **Status** column.

If the collector is still listed as **Running**, wait a minute or two, and then refresh the browser.

12. On the Browser VM desktop, open the **Resources** folder.
13. Double-click the `autoinstaller.bat` file to start the installation.
14. Return to the FortiEDR GUI, and then click the **INVENTORY** tab.
    You should see the collector restored to a **Running** state.



15. If the collector still appears as **Disconnected**, wait a few minutes, and then refresh the browser. If the collector still appears as **Disconnected**, you may need to reboot the Browser VM.

The `autoinstaller.bat` file runs a silent installation of the `CollectorInstaller64_5.0.2.261.msi` file, with the registration password and aggregator IP.

```
msiexec /i CollectorInstaller64_5.0.2.261.msi /qn
AGG=10.160.6.100:8081 PWD=DemoRegister
```

Lab 2: Administration

In this lab, you will examine the FortiEDR administrative settings.

Objectives

- Upload a content update
- Find the collector version that devices are running
- Put a collector into the high security group
- Put a collector into isolation mode
- Create a new console user

Time to Complete

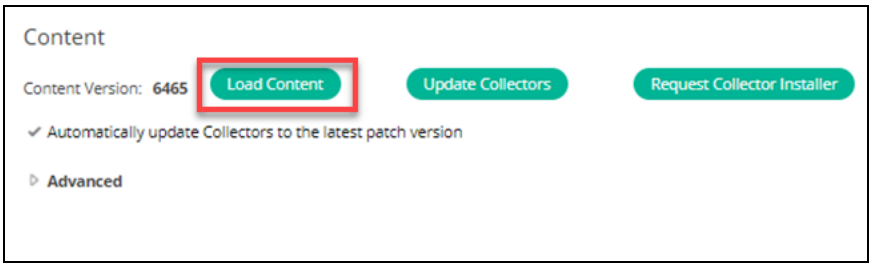
Estimated: 30 minutes

Exercise 1: Managing a FortiEDR Collector

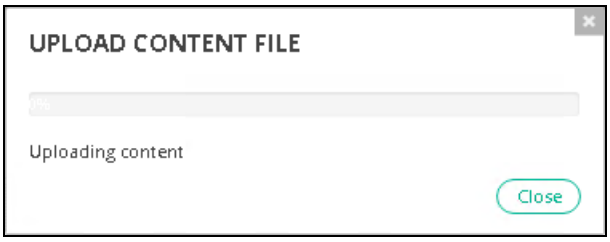
In this exercise, you will upload a content file using the management console and manage collectors.

To update the content using the management console

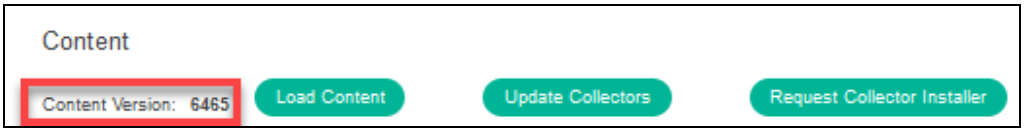
1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **ADMINISTRATION** tab, and then select **LICENSING** in the column on the left.
3. In the **Content** section, click **Load Content**.
   You may need to scroll down.



4. In the pop-up window, browse to `C:\Users\Administrator\Desktop\Resources`, select the `FortiEDRCollectorContent` file, and then click **Open**.
   A pop-up window that shows the content upload progress appears.



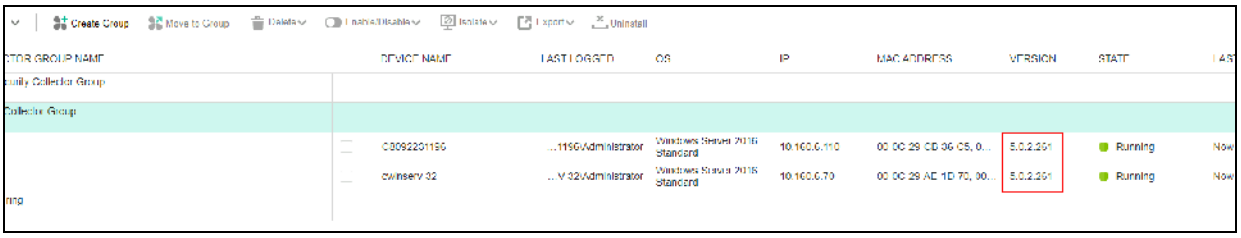
5. When the content has been updated successfully, click **Close**.
   You should notice that the **Content Version** field is updated.



   This lab is already using the updated content version and collectors—the content version will not change.

   You can update collectors automatically by enabling **Automatically update Collectors to the latest patch** or update collectors to specific versions and collector groups by clicking **Update collectors**.

6. On the FortiEDR GUI, click the **INVENTORY** > **Collectors** tab.
7. Click the **Show All Collectors** link to view the collector versions.

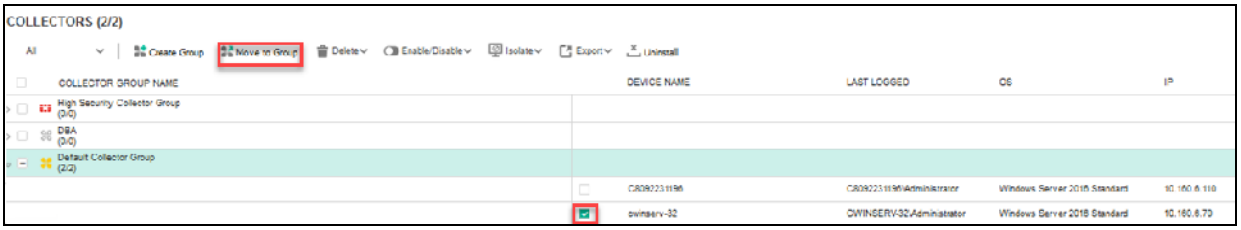


Put the Collector Into Isolation Mode

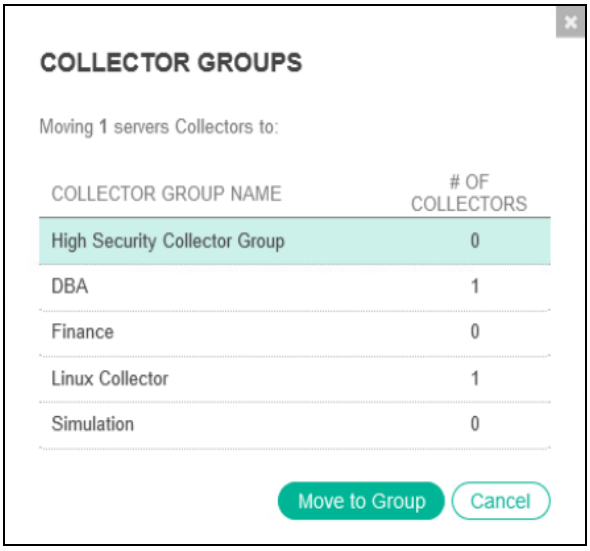
You investigated an event and concluded that it is malicious. Now, you will quarantine the affected device until it has been remediated on the **INVENTORY** tab.

To put the collector into isolation mode

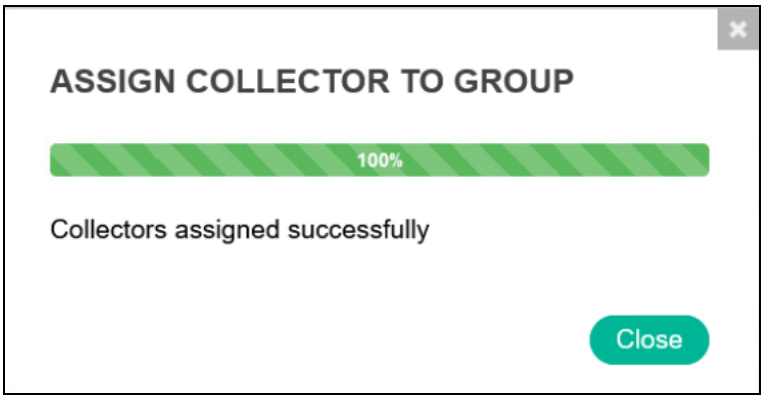
1. On the FortiEDR GUI, click the **INVENTORY** > **Collectors** tab.
2. Click the **Show all Collectors** link.
3. In the collector list, find the **cwinserv-32** collector.
4. Select the checkbox beside the collector, and then click **Move to Group**.



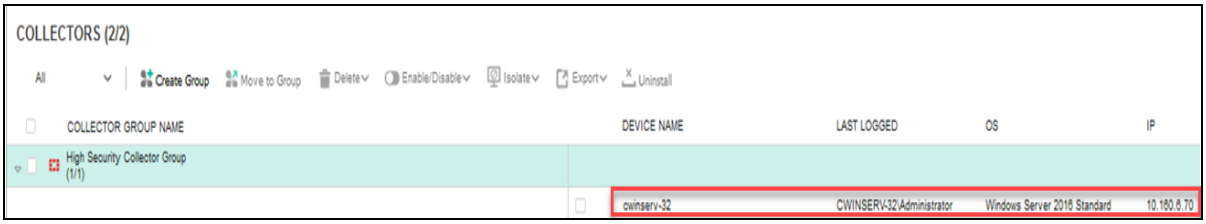
5. In the **COLLECTOR GROUPS** dialog box, select **High Security Collector Group** in the collector group list, and then click **Move to Group**.



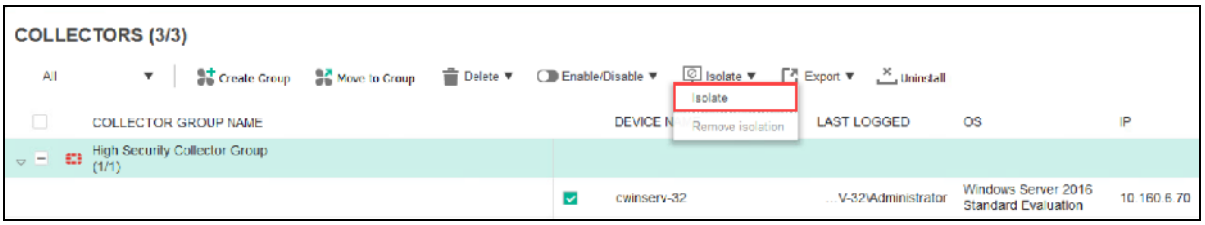
6. In the confirmation dialog box, click **Move**.
7. After the collector is assigned, click **Close**.



8. Click the **High Security Collector Group**, and then verify that the collector was moved.

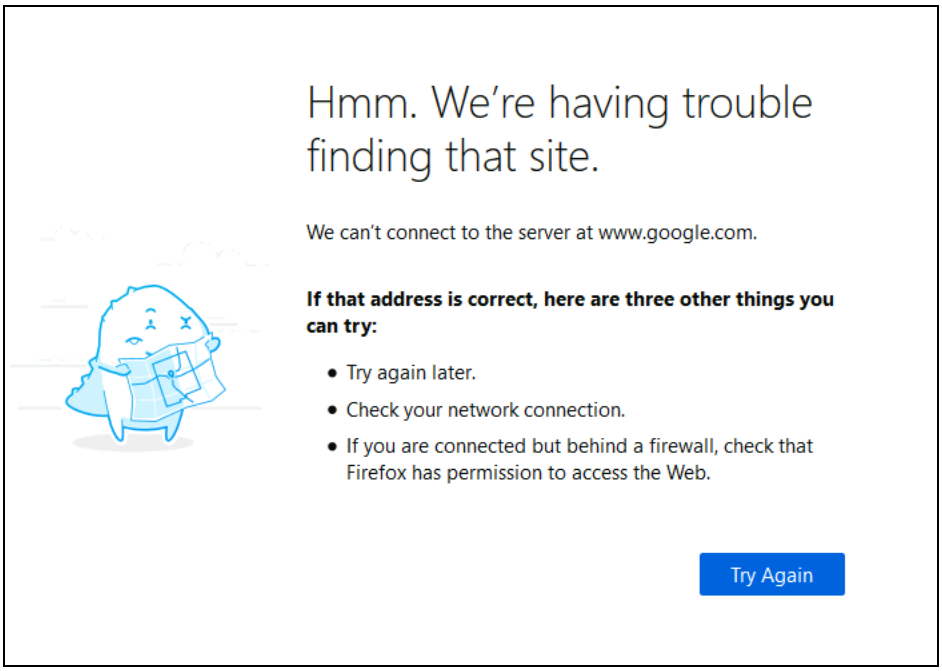


9. Select the checkbox for **cwinserv-32** again.
10. Click **Isolate**, and then select **Isolate** in the drop-down menu.



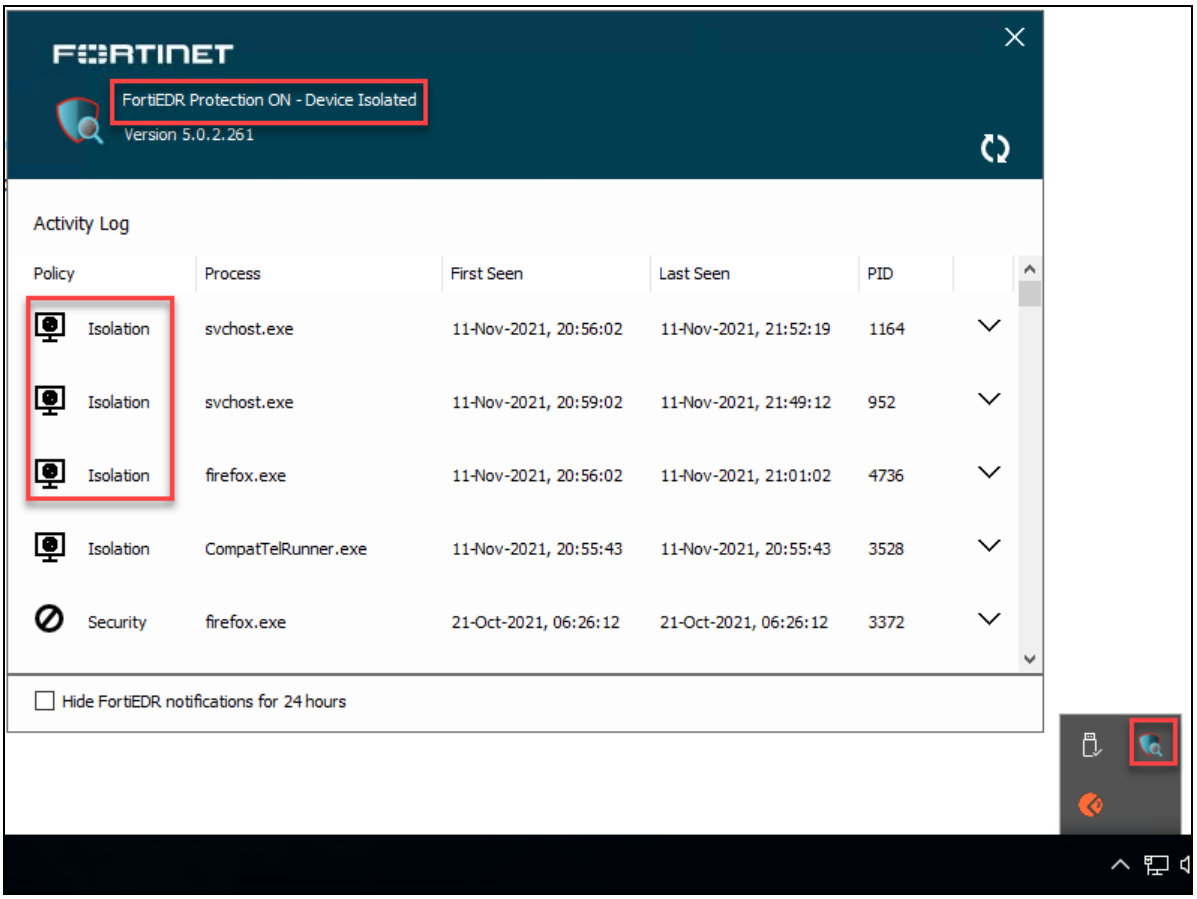
11. In the confirmation dialog box, click **Isolate**.
    You should see the **Isolation mode** icon appear beside the collector.

12. Click the Victim VM, open a browser, and then try to connect to the `www.google.com` website.
    You should see an **Unable to connect** error.



Wait a few minutes for the changes to reflect on the collector.

13. On the Victim VM Windows tray, double-click the FortiEDR collector icon to see the activity log. There are processes that are blocked by **Isolation**.



To remove the collector from isolation

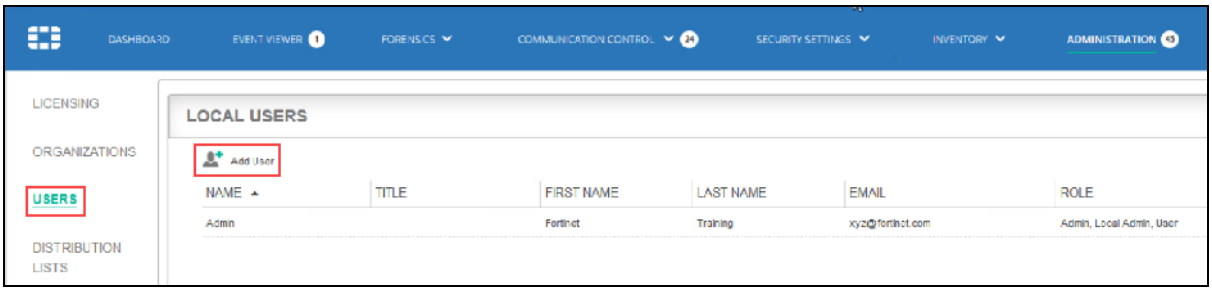
1. Return to the FortiEDR management console, and then click the **INVENTORY** > **Collectors** tab.
2. Click the **Show all Collectors** link.
3. Find the **cwinserv-32** collector in the collector list.
4. Select the **cwinserv-32** checkbox.
5. Click **Isolate**, and then select **Remove Isolation** in the drop-down menu.
6. In the confirmation dialog box, click **Remove**.
7. Select the checkbox beside the collector again, and then click **Move to Group**.
8. In the **COLLECTOR GROUPS** dialog box, select **Default Collector Group** in the collector group list, and then click **Move to Group**.
9. In the confirmation dialog box, click **Move**.
10. After the collector is assigned, click **Close**.

Exercise 2: Creating a New Administrative User

In this exercise, you will create a management console user for a new team member.

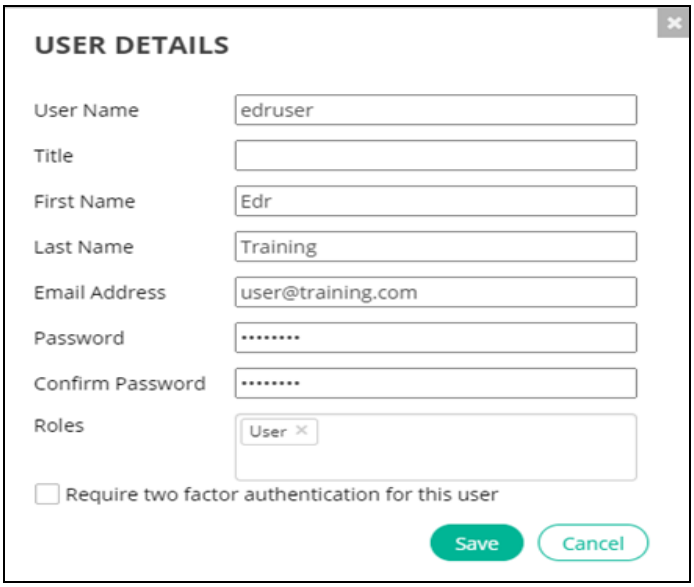
To create a new administrative user

1. On the Browser VM, log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click **ADMINISTRATION**.
3. In the left panel, select **USERS**.
4. Click **Add User**.



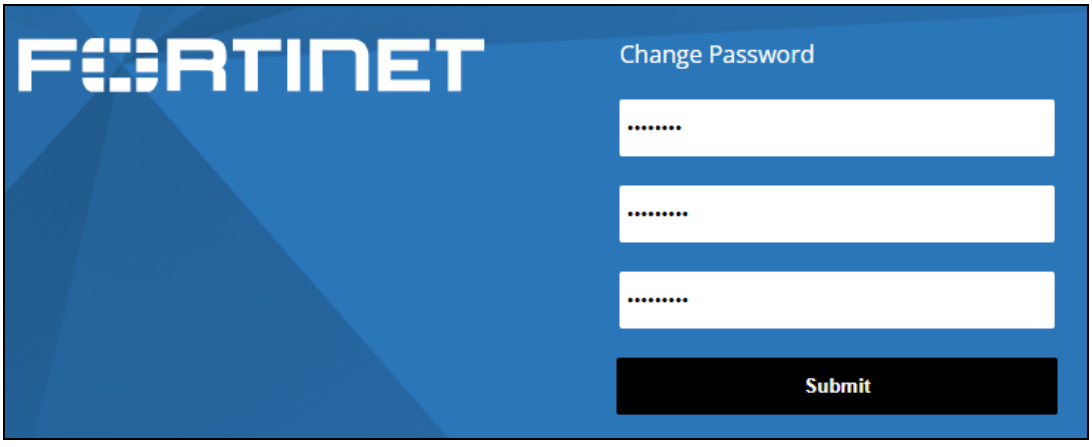
5. In the **USER DETAILS** panel, configure the following user information:

Field	Value
User Name	edruser
First Name	Edr
Last Name	Training
Email Address	user@training.com
Password	fortinet
Confirm Password	fortinet
Roles	User



6. Click **Save**.
   The user should appear in the **LOCAL USERS** list.

7. Click the **Admin** > **Logout** tab to log out of the FortiEDR GUI.
8. At the login prompt, enter the username `edruser` and password `fortinet`.
9. At the change password prompt, enter the old password `fortinet` and new password `fortinet!`.



10. Click **Submit**.
11. Log out of the FortiEDR GUI.

Note that the **ADMINISTRATION** tab is missing and you cannot access it because **edruser** was assigned a **User** role. This means this user can view and modify security events, policies, communication control, and inventory, but they can't retrieve the registration password, edit the end-user notification settings, create a new console user, or any of the other functions on the **ADMINISTRATION** tab.

Lab 3: Security Policies

In this lab, you will examine the FortiEDR security policies.

Objectives

- Clone a security policy
- Assign a collector group to a security policy
- Violate a rule in a security policy
- Change the action of a rule in a security policy
- Understand the NGAV order of operations
- Learn the difference between post-infection protection and NGAV
- Learn the difference between signature-based and next generation antivirus
- Configure a scheduled scan

Time to Complete

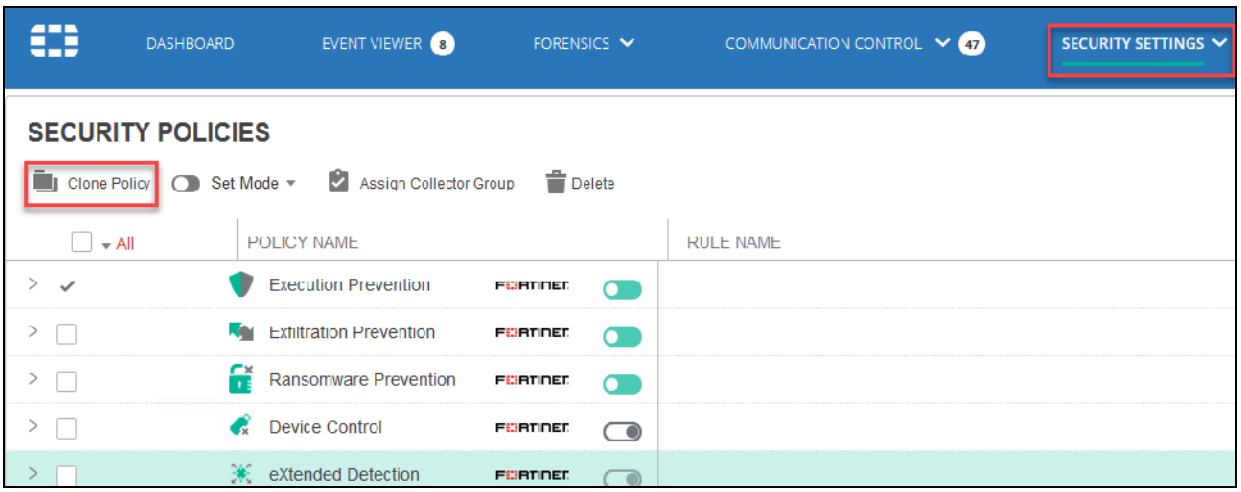
Estimated: 60 minutes

Exercise 1: Managing Security Policies

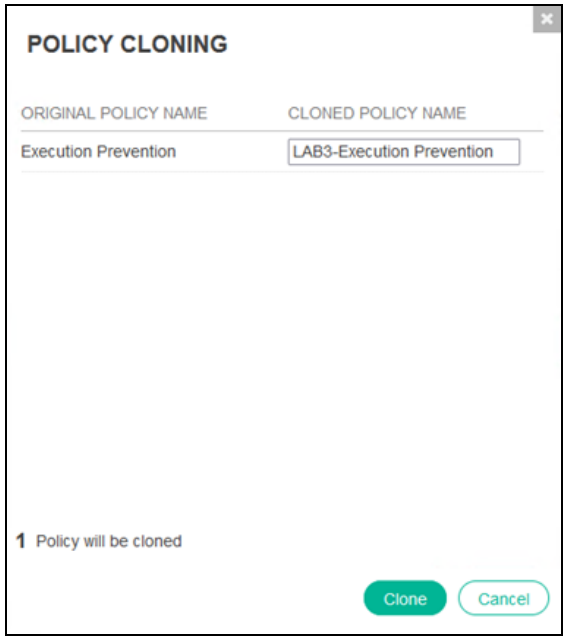
In this exercise, you will manage security policies by cloning a security policy, and then applying it to the **Default Collector** group. You will also change the default action of a rule, and then violate the rule.

To clone security policies

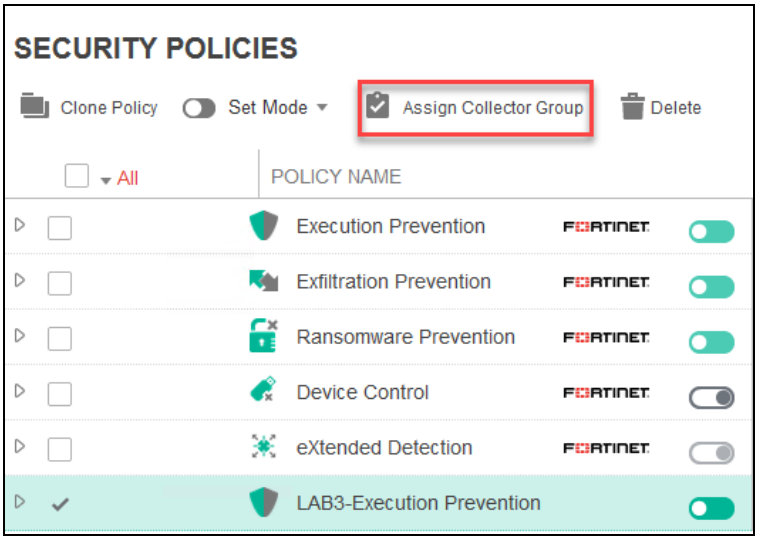
1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **SECURITY SETTINGS** > **Security Policies** tab.
3. Select the **Execution Prevention** policy checkbox.
4. Click **Clone Policy**.



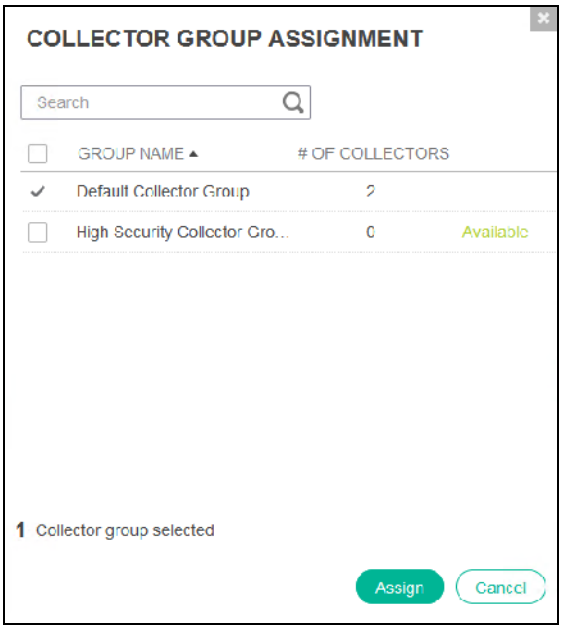
5. In the **POLICY CLONING** dialog box, type the name `LAB3-Execution Prevention`, and then click **Clone**.



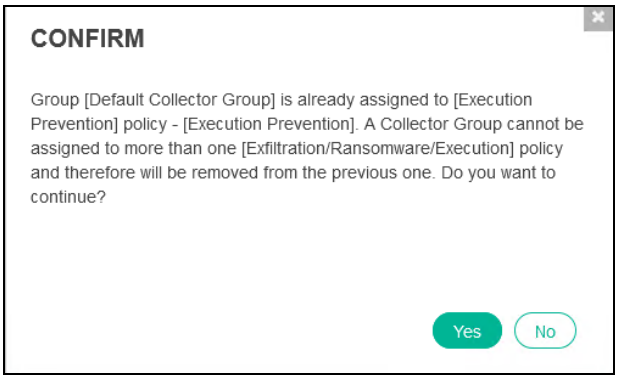
6. Select the **LAB3-Execution Prevention** policy checkbox.
7. Click **Assign Collector Group**.



8. In the **COLLECTOR GROUP ASSIGNMENT** dialog box, select the **Default Collector Group** checkbox, and then click **Assign**.

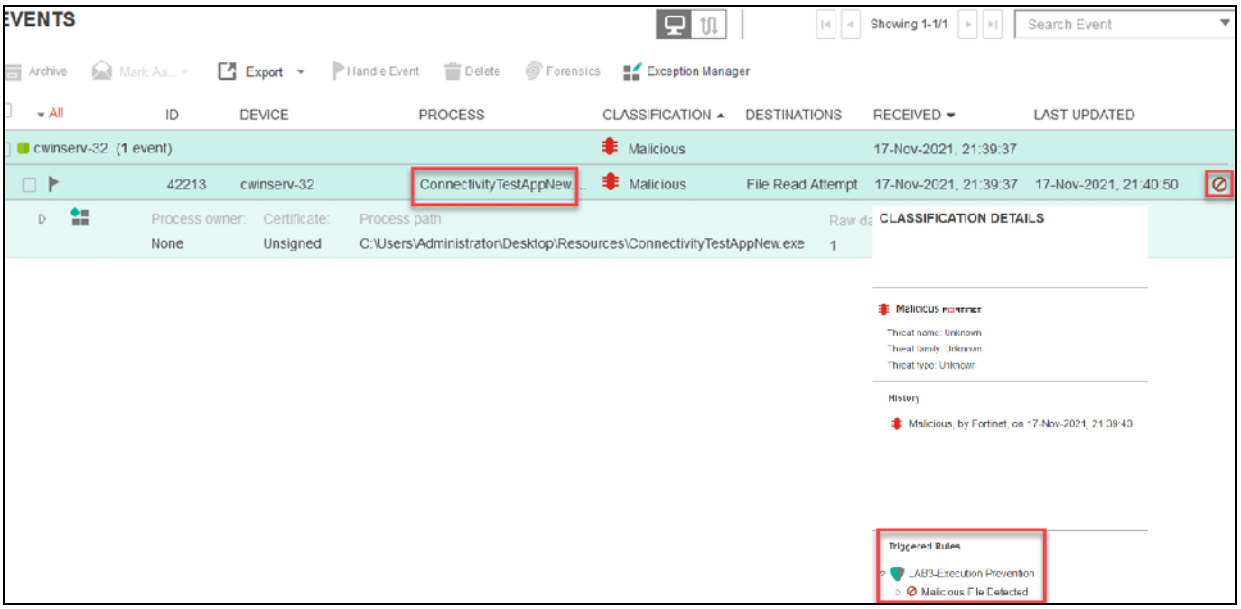


9. In the **CONFIRM** dialog box, click **Yes**.



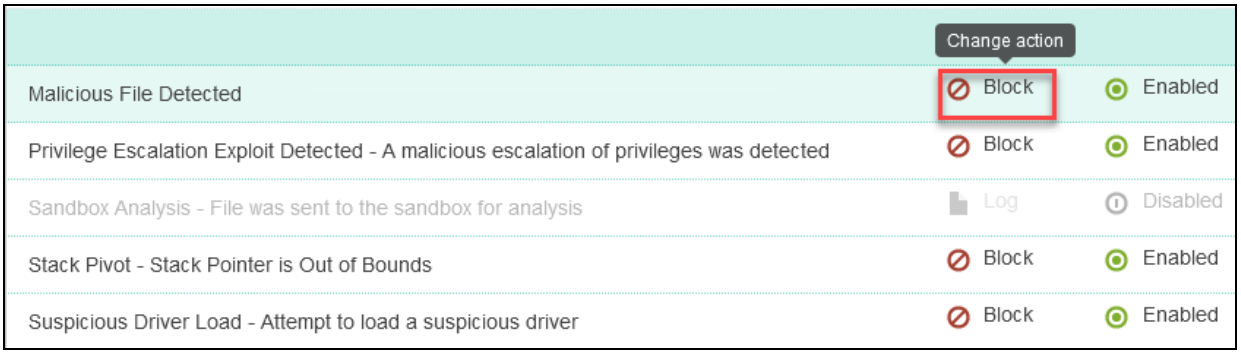
10. In the **ASSIGNMENT CONFIRMATION** dialog box, click **OK**, and then wait a minute to make sure your changes have taken effect.

11. On the Victim VM desktop, open the **Resources** folder.
12. Double-click the `ConnectivityTestAppNew.exe` file.
    A pop-up message stating that Windows cannot access the file should appear.
13. Click **OK** to close the window.
14. Return to the FortiEDR GUI, and then click the **EVENT VIEWER** tab.
    The top alert should be the **ConnectivityTestAppNew.exe** process for the **cwinserv-32** device, with a blocked icon ⊘. This process violated the **LAB3-Execution Prevention** policy using the **Malicious File Detected** rule.

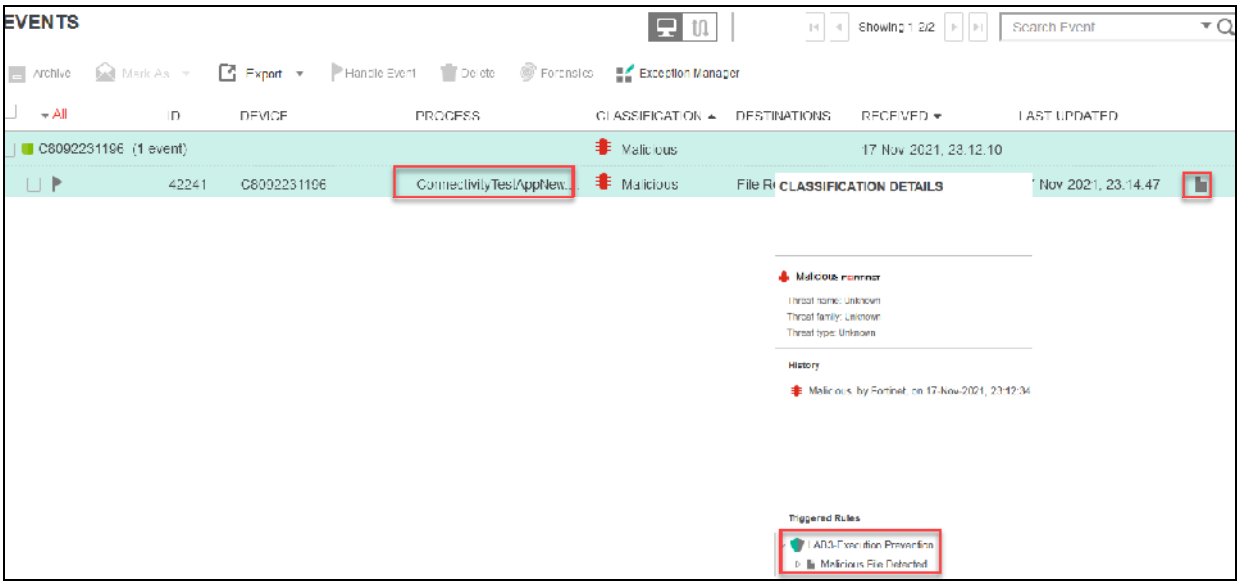


To change the default action of a rule

1. On the FortiEDR GUI, click the **SECURITY SETTINGS** > **Security Policies** tab.
2. Find the new **LAB3-Execution Prevention** policy in the list, and then click it to view the rules.
3. For the **Malicious File Detected** rule, click to change the **ACTION** from **Block** to **Log**, and then wait a minute to make sure your changes have taken effect.



4. On the Browser VM desktop, open the **Resources** folder.
5. Double-click the `ConnectivityTestAppNew.exe` file, and then click **Run**.
   This time the file should run successfully.
6. Return to the FortiEDR GUI, and then click the **EVENT VIEWER** tab.
   The top alert should be the **ConnectivityTestAppNew.exe** process for the **C80922311962** device, with a logged icon . This process violated the **LAB3-Execution Prevention** policy using the **Malicious File Detected** rule.



To move the collector group back to the Execution Prevention policy

1. Click the **SECURITY SETTINGS** > **Security Policies** tab.
2. Select the **Execution Prevention** policy checkbox.
3. Click **Assign Collector Group**.
4. In the **COLLECTOR GROUP ASSIGNMENT** dialog box, select **Default Collector Group**, and then click **Assign**.
5. In the **CONFIRM** dialog box, click **Yes**.
6. In the **ASSIGNMENT CONFIRMATION** dialog box, click **OK**.

Exercise 2: Understanding NGAV Operations

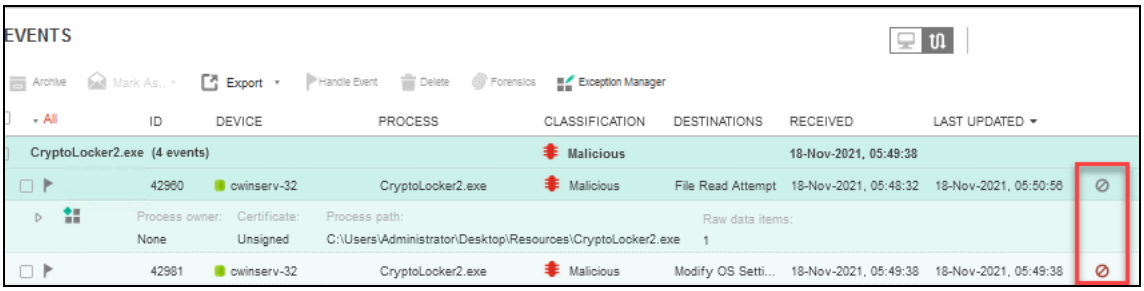
In this exercise, you will learn about the NGAV order of operations.

To understand the order of operations

1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **SECURITY SETTINGS** > **Security Policies** tab.
3. Toggle the mode slider beside **Execution Prevention**, and then click the toggle to set it to **Simulation** mode.
4. In the confirmation dialog, click **Set to Simulation**, and then wait a minute to make sure your changes have taken effect.
5. On the Victim VM desktop, open the **Resources** folder.
6. Double-click the `CryptoLocker2.exe` icon, and then click **Run** to run the process.
   A pop-up message indicating that FortiEDR has blocked the process should appear.

This is an actual malware file. Do not copy the file or attempt to run it on any other machine. The lab environment is protected by FortiEDR, but you should always use caution when handling malware.

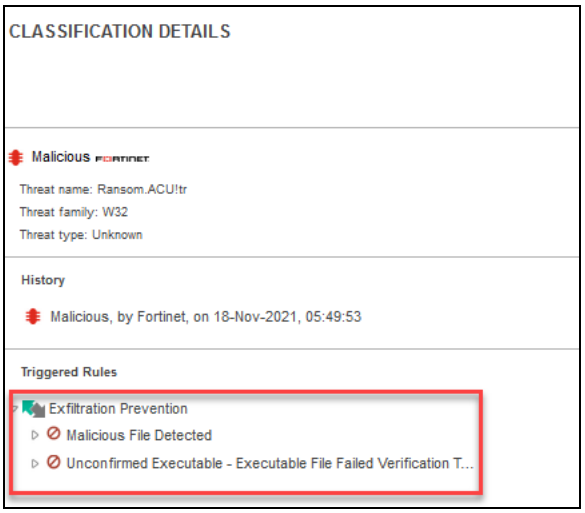
7. Return to the FortiEDR GUI, and then click the **EVENT VIEWER** tab.
8. Make sure the events are aggregated by process—if not, click **Process View** to change the view.
   The top alert should be **CryptoLocker2.exe**. Note that there are two events involving this process.



9. Click each event to view and compare the details.
   Note that one of the events is marked with a simulated block icon (⊘), and the other is marked with a blocked icon (⊘).
10. Click the simulated block event, and then look at the **Triggered Rules** section at the bottom of the **CLASSIFICATION DETAILS** pane on the right.

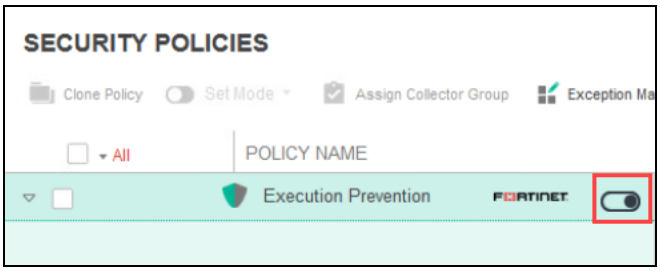
Note that the violated rule was in the **Execution Prevention** policy.

11. Select the blocked event, and then check the **CLASSIFICATION DETAILS** panel again.



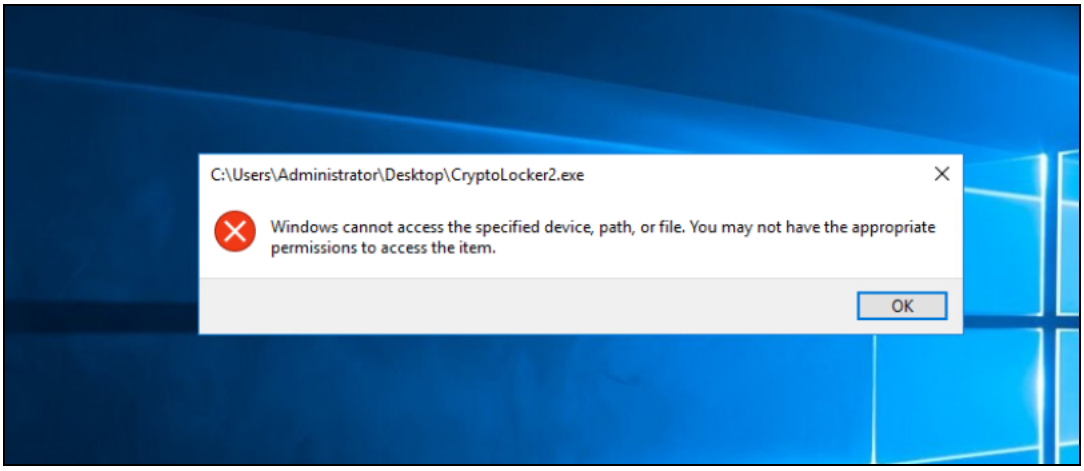
When **Execution Prevention** is set to **Simulation** mode, NGAV does not actively prevent infections, so malicious files may be allowed to launch. However, the post-infection protection policies, such as **Exfiltration Prevention** and **Ransomware Prevention**, which are in **Prevention** mode, still protect the device. The post-infection protection policies stopped the process before it was able to create or modify files. Even though the process was allowed to launch, FortiEDR blocked it before it was able to do harm.

12. Return to the FortiEDR GUI, and then click the **SECURITY SETTINGS** > **SECURITY POLICIES** tab.
13. Toggle the mode slider beside **Execution Prevention** to set it to **Prevention** mode.



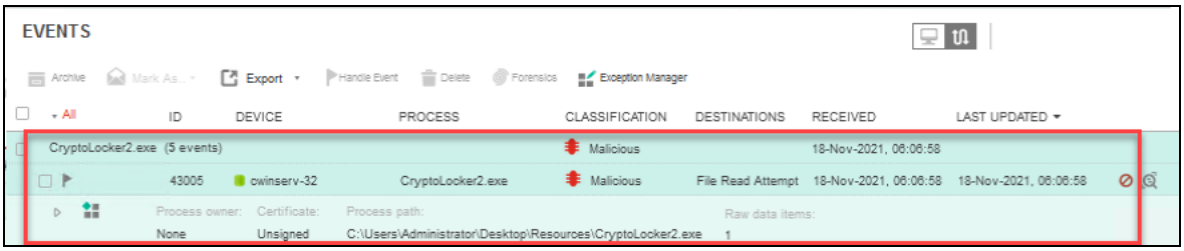
14. In the confirmation dialog, click **Set to Prevention**, and then wait a minute to make sure your changes have taken effect.
15. On the Victim VM, run `CryptoLocker2.exe` again.

    A warning that Windows cannot access the file should appear. This is because FortiEDR is blocking the file from launching.

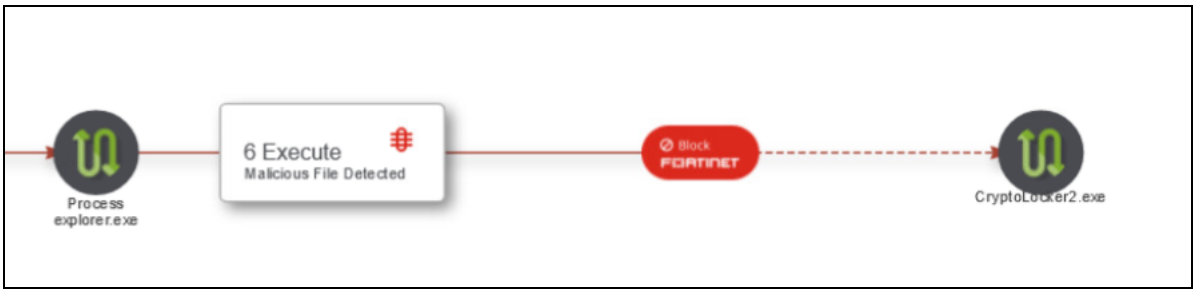


16. Click **OK** to close the window.
17. Return to the FortiEDR GUI, and then check the **EVENTS** list in the **EVENT VIEWER** tab.

    You may need to refresh the browser tab. A new event for `CryptoLocker2.exe` should appear.



18. Click the new event to highlight it, and then look at the **Advanced Data** pane.



The chain of events starts as before:

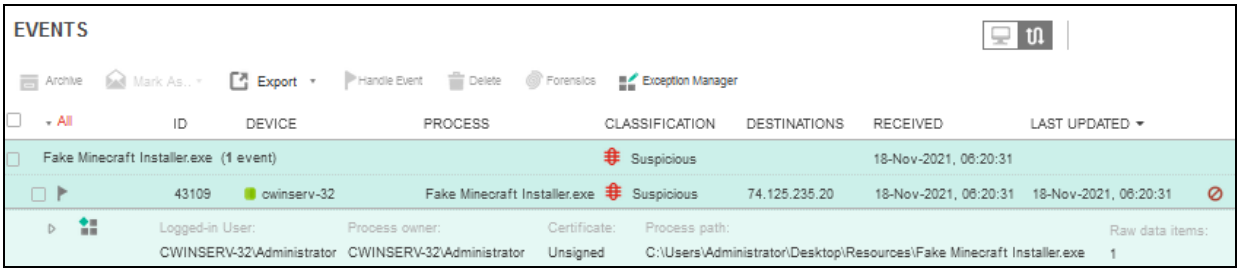
- The `explorer.exe` detected `CryptoLocker2.exe`.
- The file violated the **Malicious File Detected** rule. Because you put the **Execution Prevention** policy in **Prevention** mode, the last step is slightly different from the first time you ran the file.
- FortiEDR blocked the event from launching.

Exercise 3: Understanding the Difference Between NGAV and Post-Infection Protection

In this exercise, you will learn the difference between post-infection protection and NGAV. You will also learn the difference between signature-based and next generation antivirus. Finally, you will configure a scheduled scan.

To understand the differences

1. On the Victim VM desktop, open the **Resources** folder.
2. Double-click `Fake Minecraft Installer.exe` to launch it.
   A pop-up message from FortiEDR stating that the process has been blocked should appear.
3. Return to the FortiEDR management console, and then check the **Events** list in the **EVENT VIEWER** tab.
   You may need to refresh the browser tab.



4. Check the **Triggered Rules** section of the **CLASSIFICATION DETAILS** pane.

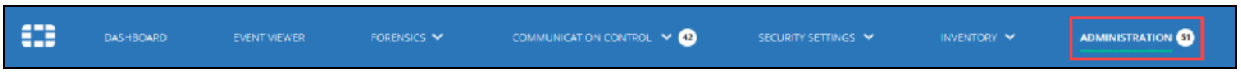
Note that the violated rule was in the **Exfiltration Prevention** policy.

Stop and think!

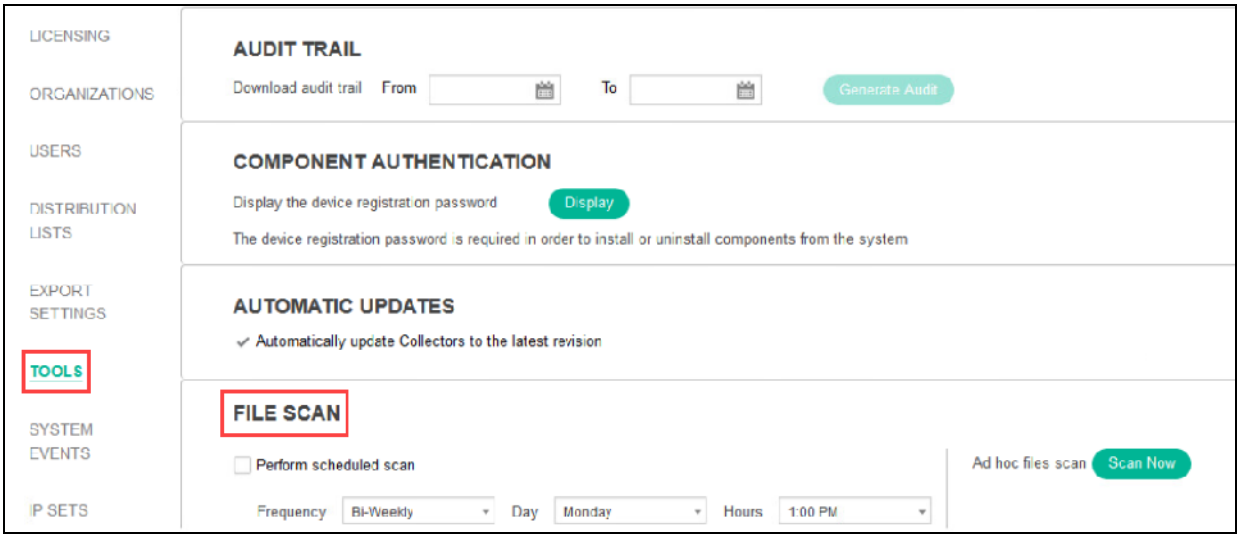
Why wasn't the process caught by the **Execution Prevention** policy like you saw earlier? Because, in some cases, with brand new or very sophisticated malware, NGAV cannot detect the attack. This is when the post-infection prevention policies really shine. An unrecognized malicious program may occasionally be allowed to launch, but FortiEDR will stop it before it is able to cause harm.

To configure a scheduled scan

1. On the FortiEDR GUI, click the **ADMINISTRATION** tab.

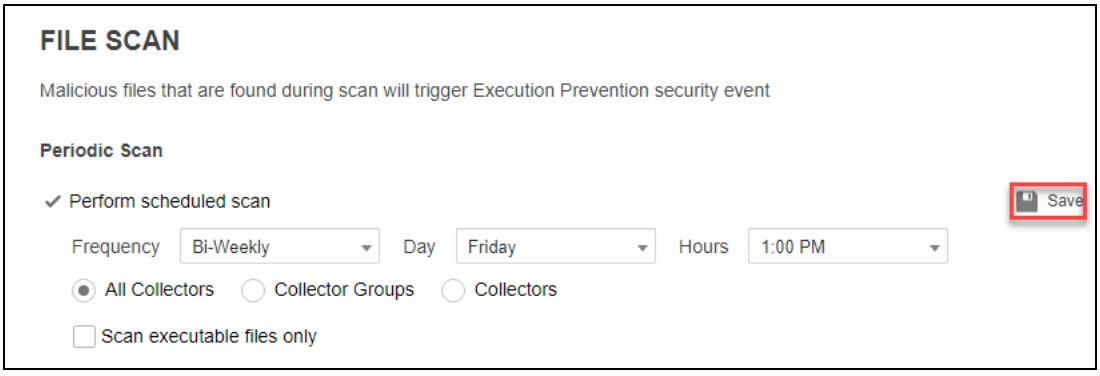


2. In the left panel, click **TOOLS**.



3. Under **FILE SCAN**, configure the following settings, and then click **Save**:

Field	Value
Perform scheduled scan	Select the checkbox to enable this setting.
Frequency	Bi-Weekly
Day	Friday
Hours	1:00 PM



Because FortiEDR evaluates files in real time when they are read or launched, it is not necessary to perform periodic scans. Scans are offered to fully comply with AV replacement standards.

Lab 4: Playbooks

In this lab, you will examine the FortiEDR playbooks.

Objectives

- Enable the default playbook
- Customize the playbook

Time to Complete

Estimated: 15 minutes

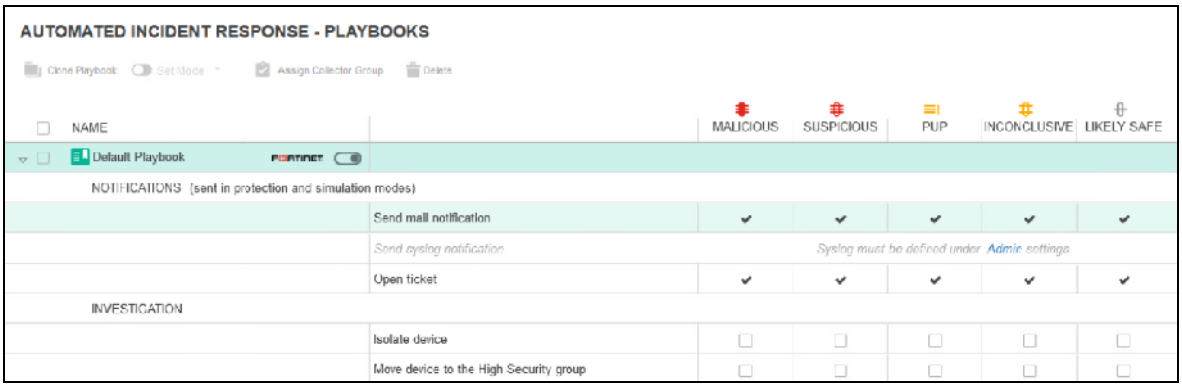
Exercise 1: Managing Playbooks

To take advantage of the FortiEDR automated incident response capabilities, you will enable the default playbook, and then customize its settings.

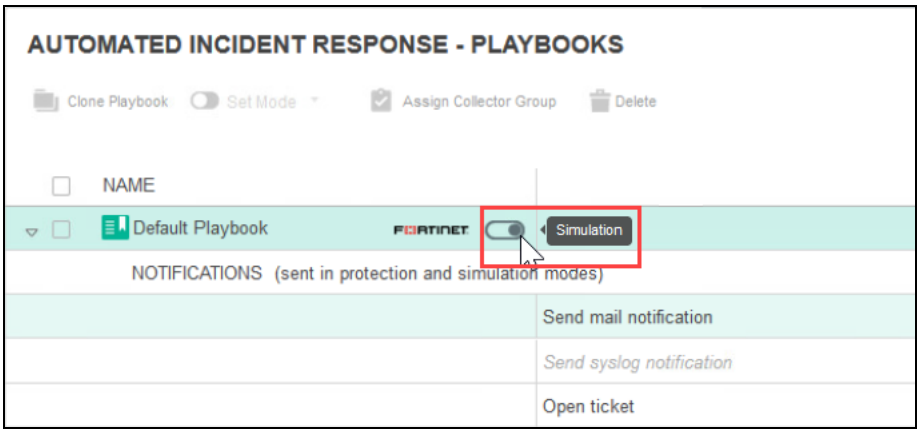
To manage playbooks

1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **SECURITY SETTINGS** > **Playbooks** tab.

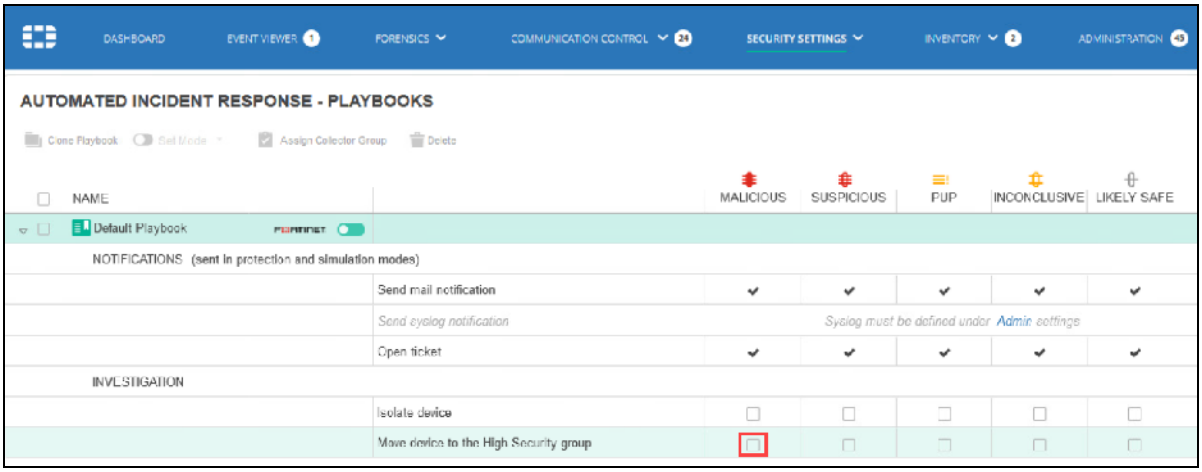
3. Click the **Default Playbook** to view the settings.



4. Review the different options that are available for playbooks.
5. Click the mode slider to put the **Default Playbook** into **Prevention** mode.



6. In the confirmation dialog, click **Set to Prevention**.
7. In the **MALICIOUS** column, select the **Move device to the High Security group** checkbox.



The playbooks automated incident response cannot be triggered because this lab environment is not configured with Fortinet Cloud Service (FCS). In a live environment, with the configuration above, when a malicious incident is triggered, the collector in question is moved to the **High Security group** for further investigation. Also, if the appropriate administrative settings are configured, an email is sent and a ticket is opened automatically for this incident.

Lab 5: Communication Control

In this lab, you will configure the communication control feature to manage applications on FortiEDR.

Objectives

- Create a rule that blocks applications with a reputation score of 1 or 2
- Find and block a safe, but unwanted, application
- Create a new policy, and then apply it to a group
- Allow applications for specific groups
- Troubleshoot employee problems using Webex

Time to Complete

Estimated: 45 minutes

Exercise 1: Configuring Communication Control

In this exercise, you will configure a rule and policy to block applications with a reputation score of 1 or 2, a safe but unwanted application, and a freeware application that handles sensitive data.

Create a Rule to Block Applications Based on Reputation

As a first step, you must tune your communication control policies, and set a rule that proactively blocks any application versions with a reputation score of 2 or lower.

To create a rule and enable it in the policy

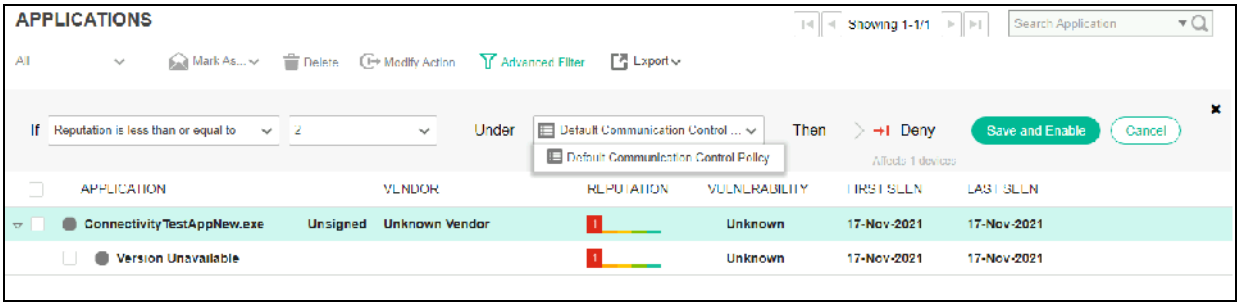
1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **COMMUNICATION CONTROL** > **Applications** tab, and then click **Advanced Filter**.

3. In the **Select Filter** drop-down list, select **Reputation is less than or equal to**.

4. In the **Select Criteria** drop-down list, select **2**.

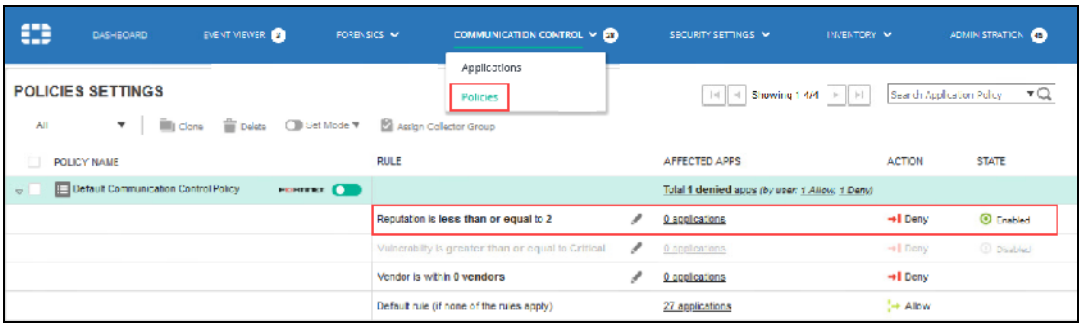
5. Click **Setup rule** to configure a rule that blocks any future application versions that fit your criteria.

6. In the **Select Policy** drop-down list, choose **Default Communication Control Policy**.



7. Click **Save and Enable** to apply a rule in the policy.

8. Click **OK** to save the rule.
9. On the **COMMUNICATION CONTROL** tab, click **Policies** to see your policy.



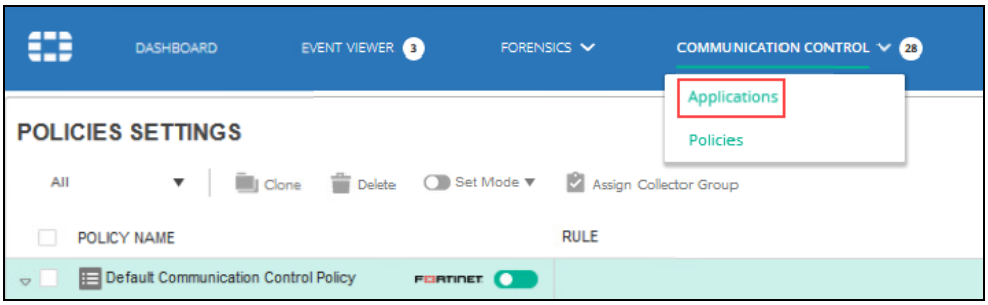
Your rule should be at the top of the **Default Communication Control Policy** rules list, and should appear as **Enabled**.

Deny Communication Manually From an Application That Is on Your Organization's Block List

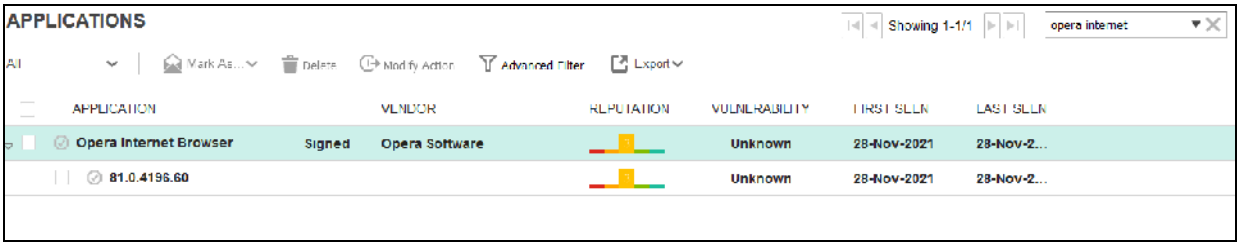
In some cases, you may want to block applications that are safe but not wanted. In this task, you will block external connections from the Opera browser.

To deny communication from an application manually

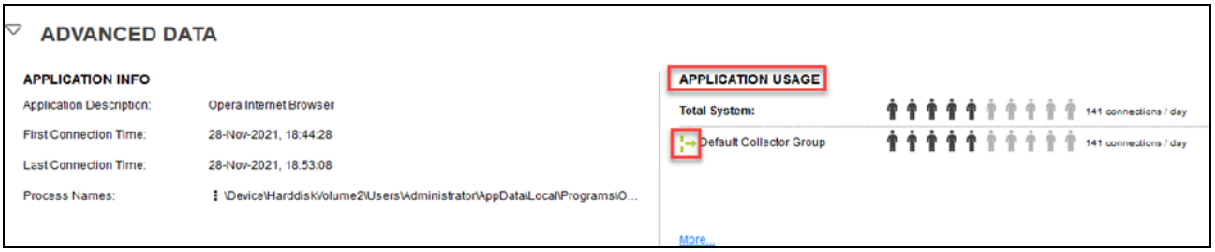
1. Click the **COMMUNICATION CONTROL** tab, and then click **Applications** to see the application list.



2. Use the search bar to find `Opera internet` in the application list.

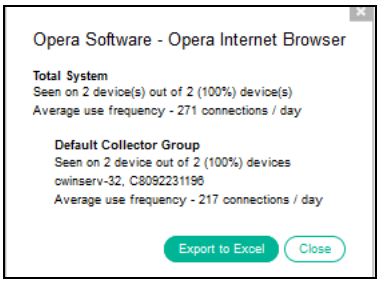


3. With **Opera Internet Browser** highlighted, click to expand the **ADVANCED DATA** pane at the bottom of the screen to investigate which users have been using **Opera Internet Browser** and the **Collector** group.



Notice that all of the devices using **Opera Internet Browser** are in the **Default Collector Group**. The green icon indicates that the connections were allowed.

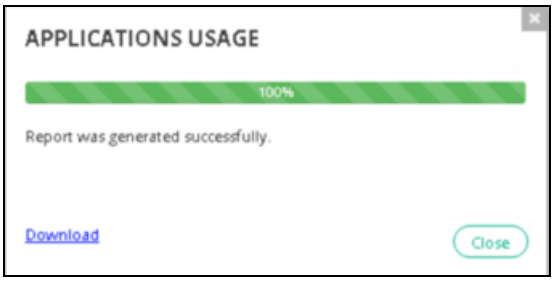
4. Click the **More** link to view the devices that connected to the network with **Opera Internet Browser**.



5. Click the **Export to Excel** button to generate an **Application Usage** report.

FortiEDR can block all attempted external connections from an application, but it does not prevent the applications from running offline. If an application is banned by the organization's guidelines, generate a report to see which users have installed the application, and then ask them to uninstall it.

6. When the report is generated, click the **Download** link to save the report.

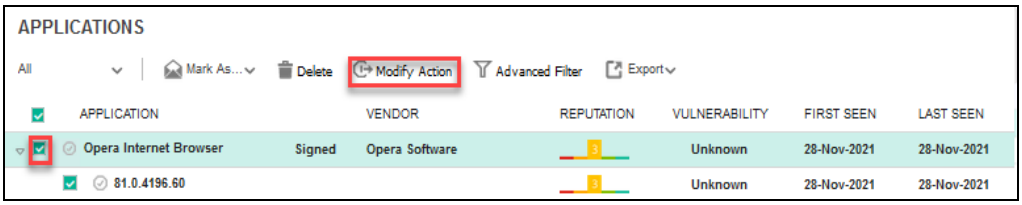


7. Click **Close** to exit both dialog boxes.
8. In the download menu of the browser window, click the file to view the report.

FORTINET	Fortinet Training	Report created by user Admin on 28-Nov-2021, 21:50
Application Usage		
Opera Software/Opera Internet Browser		
COLLECTOR NAME	COLLECTOR GROUP NAME	COLLECTOR IP
cwinserv-32	Default Collector Group	10.160.6.70
C8092231196	Default Collector Group	10.160.6.110

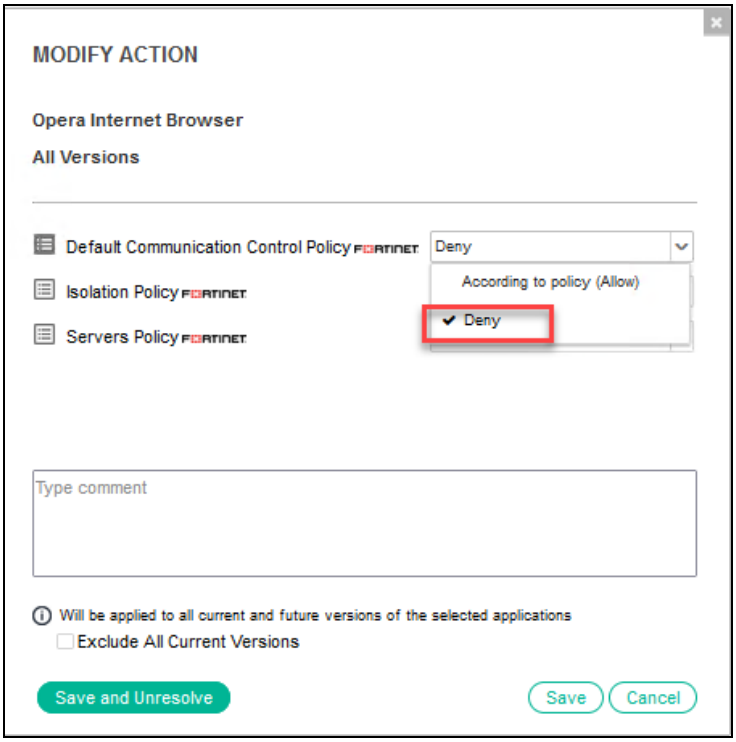
In this case, the application has been used by two collectors, **cwinserv-32** and **C8092231196**.

9. Return to the **COMMUNICATION CONTROL** tab of the management console.
10. Select the checkbox beside the **Opera Internet Browser** application, and then click **Modify Action**.



The **MODIFY ACTION** dialog box appears. There are only three policies, and only one is set to **Allow** by default—the **Default Communication Control Policy**.

11. In the action drop-down list beside the policy, select **Deny**.



12. Click **Save** to apply the changes.
13. Look at the **ADVANCED DATA** pane again.

You should now see a red icon indicating that communication is denied from the application.

14. On the Victim VM, double-click the **Opera Browser** icon.

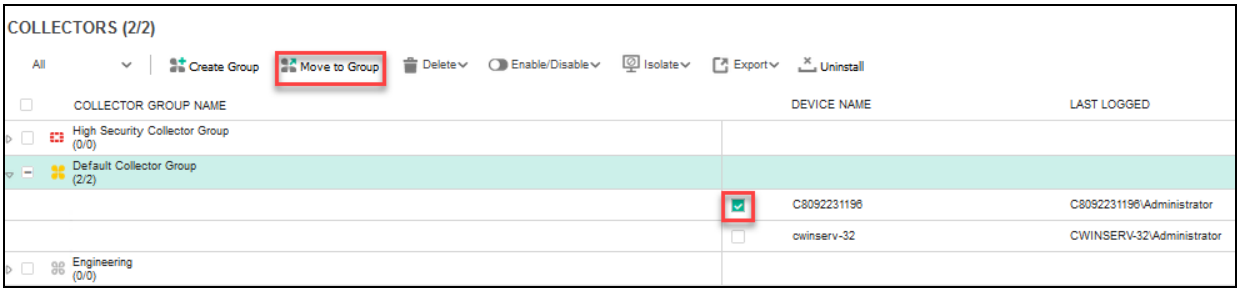
A pop-up message notifying you that FortiEDR has blocked the process should appear. Wait a minute to make sure your changes have taken effect.

Allow Applications to Communicate Externally for Specific Groups

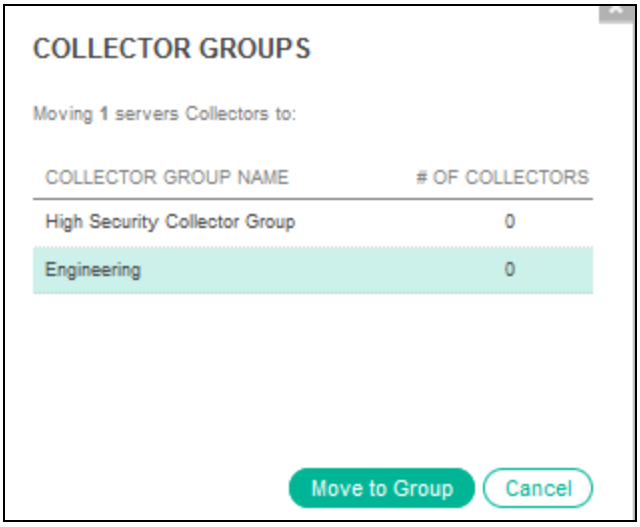
Your organization requires the Engineering group to have access to the Opera browser, so you must allow the application for this group, but block it for others.

1. Return to the FortiEDR GUI, and then click the **INVENTORY** > **Collectors** tab.
2. Expand **Default Collector Group**, and then select the checkbox beside the **C8092231196** device.

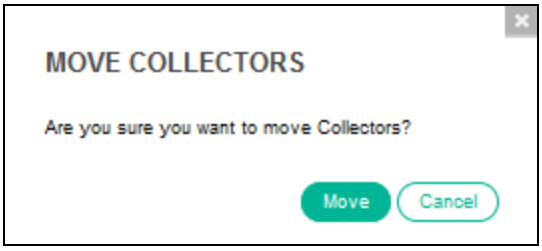
3. Click **Move to Group**.



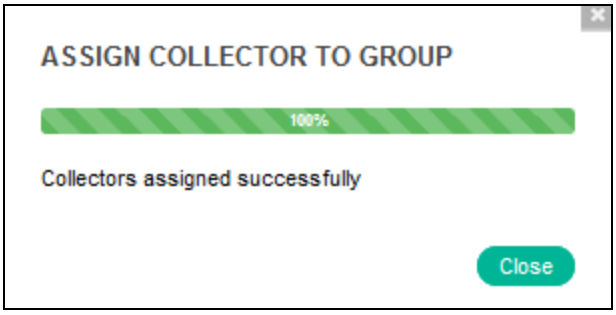
4. In the **COLLECTOR GROUPS** dialog box, select **Engineering**, and then click **Move to Group**.



5. In the **MOVE COLLECTORS** dialog box, click **Move**.



6. In the **ASSIGN COLLECTOR TO GROUP** dialog box, click **Close**, and then wait a minute to make sure your changes have taken effect.



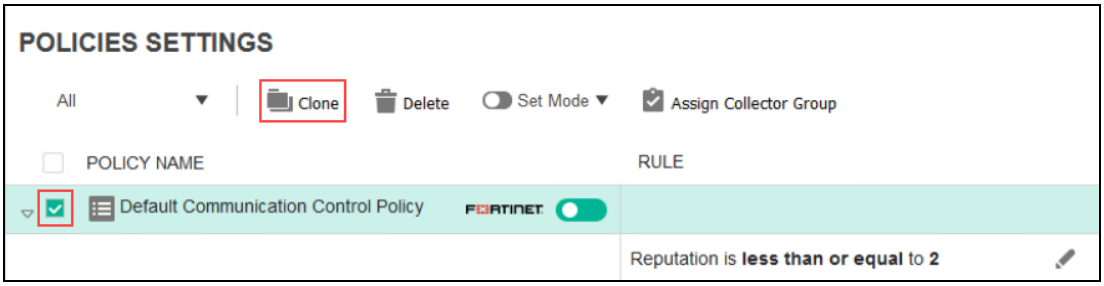
In a live environment, collectors are already assigned to different collector groups based on the organization's requirements. In this lab environment, we are moving collectors to simulate multiple collector groups using the same communication control policy.

To allow the Opera browser

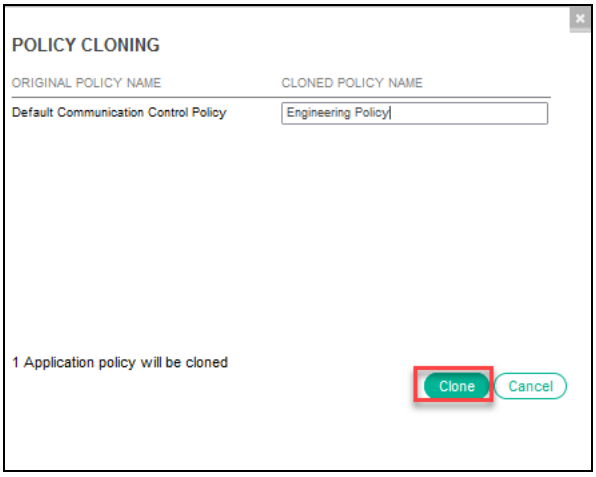
1. Continuing on the **COMMUNICATION CONTROL** tab, click **Applications** to see the application list.
2. View the **ADVANCED DATA** panel.

Notice that there are devices using **Opera Internet Browser** in the **Default Collector Group** and **Engineering** group.

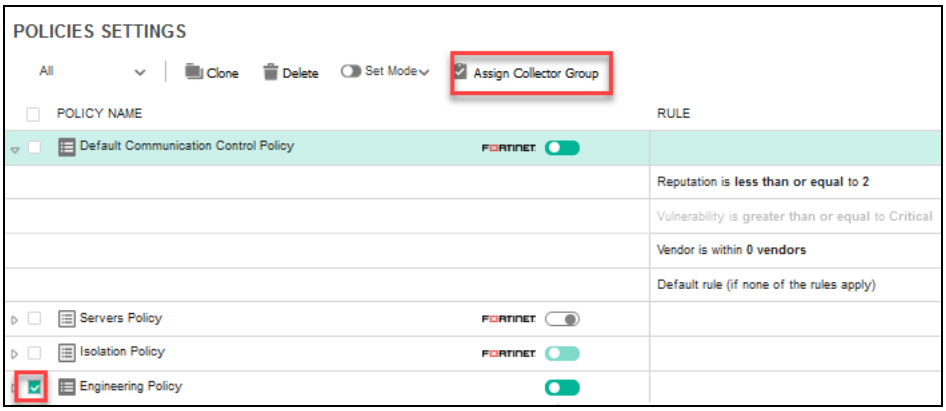
3. On the **COMMUNICATION CONTROL** tab, click **Policies**.
4. Select the **Default Communication Control Policy** checkbox, and then click **Clone**.



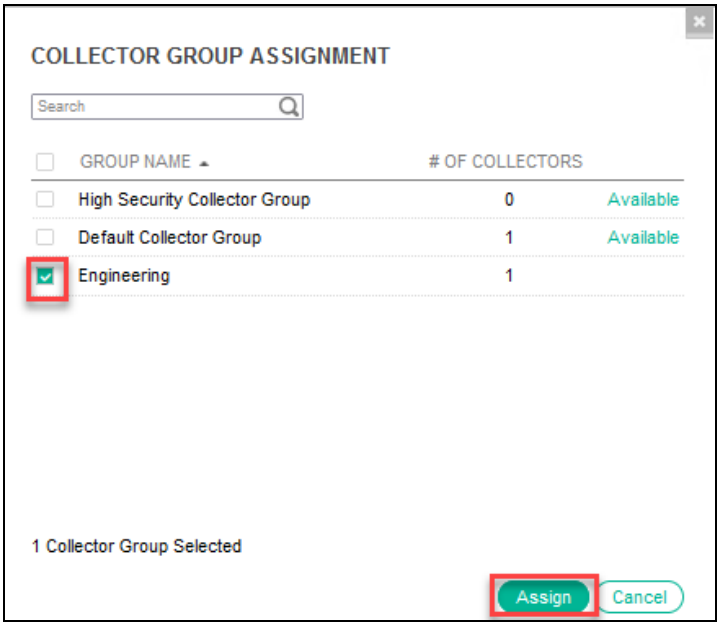
5. In the **POLICY CLONING** dialog box, type `Engineering Policy` for the new policy, and then click **Clone**.



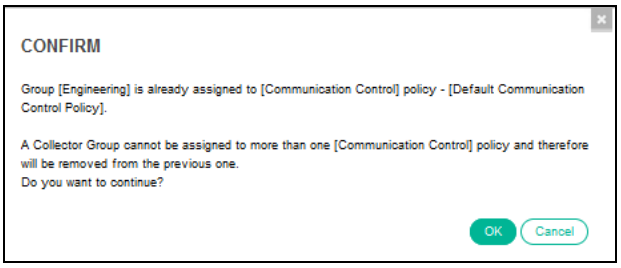
6. Select the **Engineering Policy** checkbox, and then click **Assign Collector Group**.



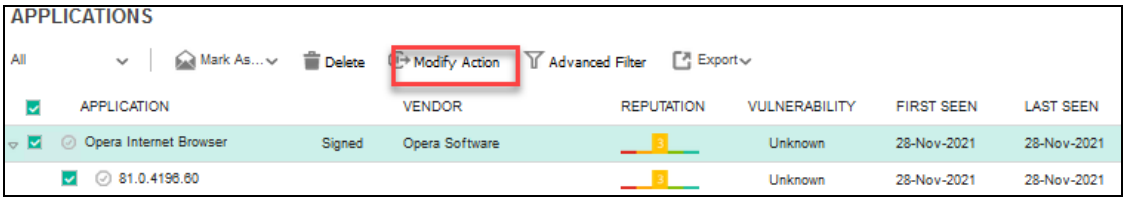
7. In the **Collector Group Assignment** dialog box, select the **Engineering** group checkbox, and then click **Assign**.



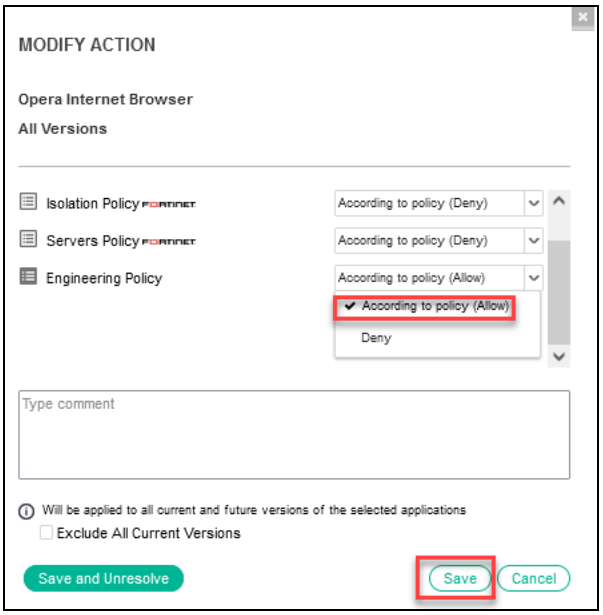
8. In the confirmation dialog box, click **OK** to confirm that you want to remove the **Engineering** group from the **Default Communication Control Policy**, and add it to the **Engineering Policy**.



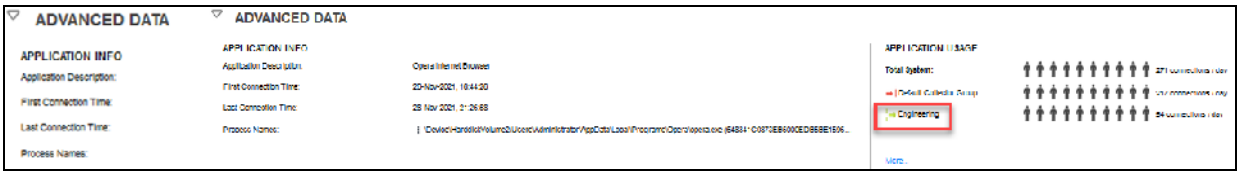
9. Click **OK** to close the **ASSIGNMENT CONFIRMATION** window.
10. Click the **Applications** sub-tab to return to the application list.
11. In the **APPLICATIONS** list, select the checkbox beside all **Opera Internet Browser** applications, and then click **Modify Action**.



12. In the **MODIFY ACTION** dialog box, in the drop-down list beside the communication control policy you just created, select **According to policy (Allow)**, and then click **Save**.



13. View the **ADVANCED DATA** pane.



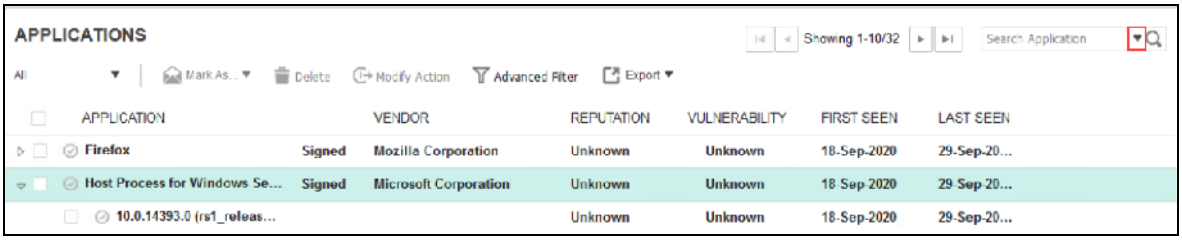
A green icon should appear beside the **Engineering** group, indicating that the connection is allowed.

Exercise 2: Troubleshooting Webex Connections

In this exercise, you will troubleshoot issues with Webex connections. Some users in the Engineering department are having trouble using Webex.

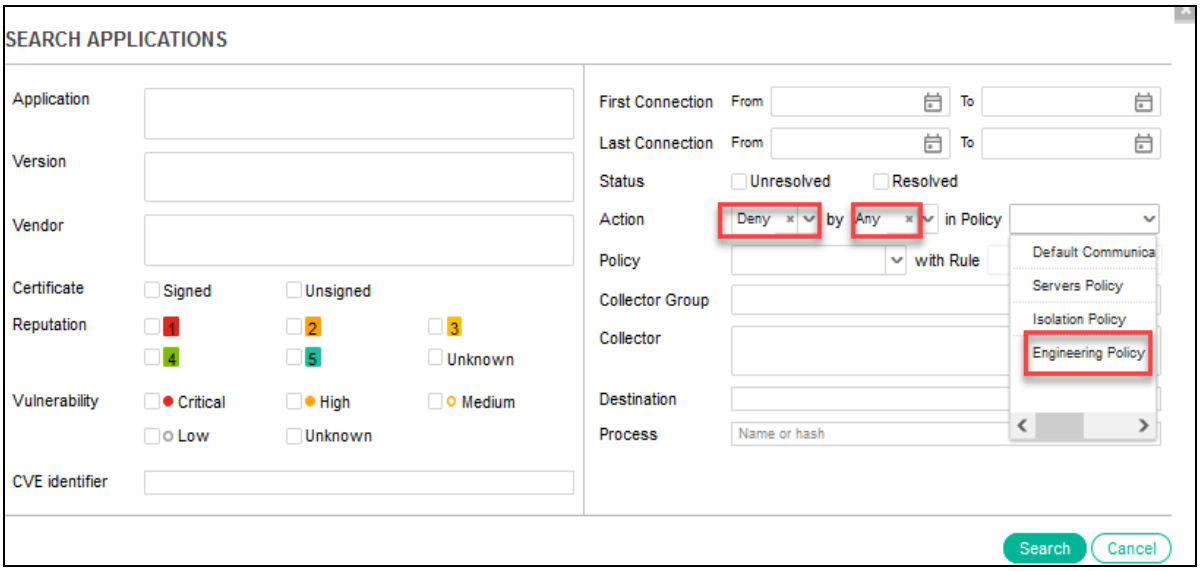
To troubleshoot Webex connections

1. On the **Application** tab, click the **X** in the search bar to clear the search results from the previous exercise.
2. Click the arrow in the search bar to open the **Advanced Search** window.

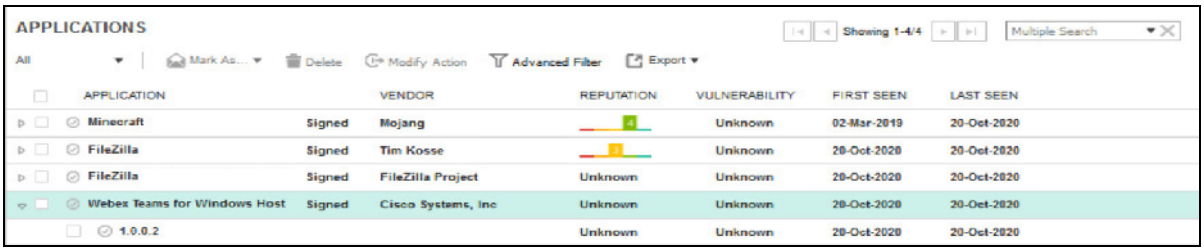


3. In the **SEARCH APPLICATIONS** window, configure the following settings to search applications:

Field	Value
Action	Deny
by	Any
in Policy	Engineering Policy

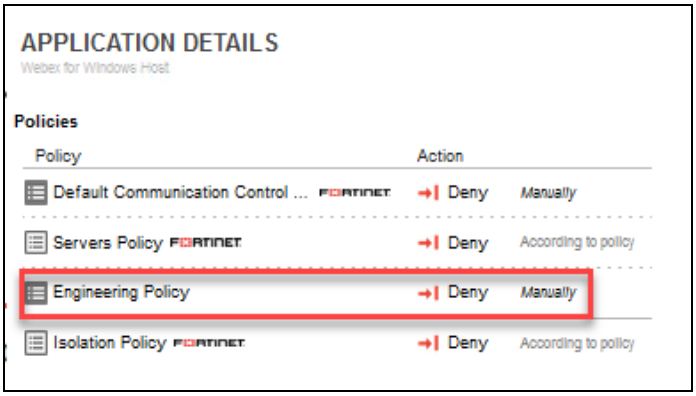


4. Click **Search**.
   A few applications should be listed, including **Webex Teams for Windows Host** or **Webex for Windows Host**, so this is likely the source of the Webex problems.
5. Click **Webex Teams for Windows Host** or **Webex for Windows Host** to view details.

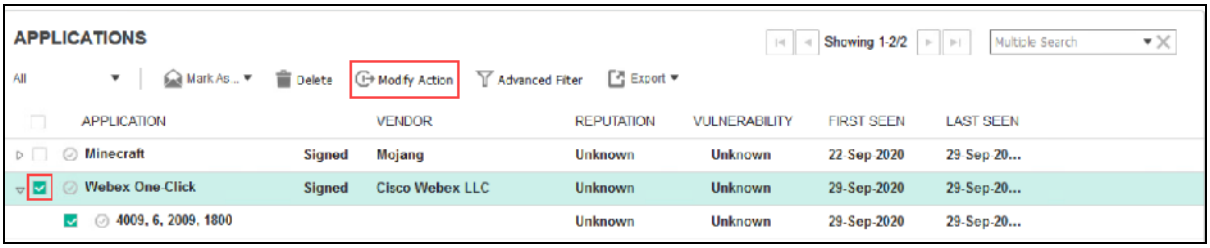


6. Look in the **APPLICATION DETAILS** pane to see the applied action for **Webex Teams for Windows Host** or **Webex for Windows Host** in each policy.

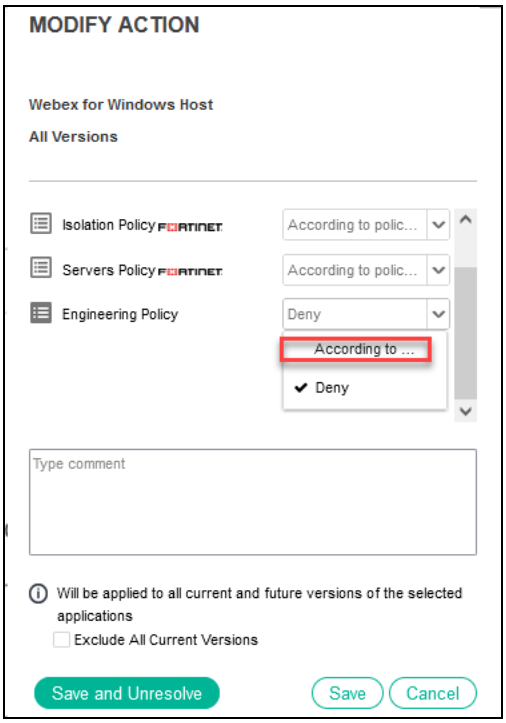
   Notice that it is set to **Deny** in both the **Engineering Policy** and **Default Communication Control** policy.



7. In the **APPLICATIONS** list, select the checkbox beside **Webex Teams for Windows Host** or **Webex for Windows Host**, and then click **Modify Action**.

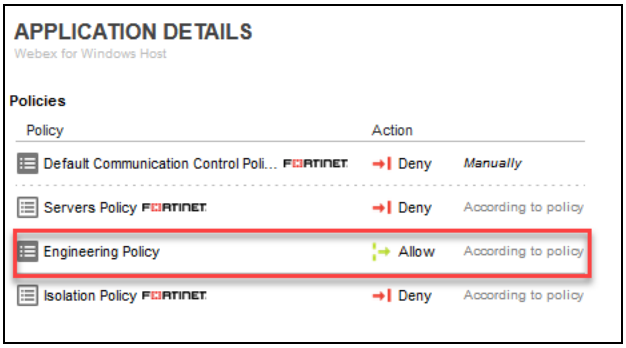


8. In the **MODIFY ACTION** dialog box, select **According to policy (Allow)** in the drop-down list beside **Engineering Policy**, and then click **Save**.



Since **Webex Teams for Windows Host** or **Webex for Windows Host** is no longer blocked, it disappears from the results list.

9. Click the **X** in the search field to clear the search results.
10. Find **Webex Teams for Windows Host** or **Webex for Windows Host** in the list, and then click to select it.
    In the **APPLICATION DETAILS** pane, you should see that for the **Engineering Policy**, the action for the application is now **Allow**.



To move the collector back to the Default Collector Group

1. Click the **INVENTORY** > **Collectors** tab.
2. Expand **Engineering** , and then select the **C8092231196** device checkbox.
3. Click **Move to Group**.
4. In the **COLLECTOR GROUPS** dialog box, select **Default Collector Group**, and then click **Move to Group**.
5. In the **MOVE COLLECTORS** dialog box, click **Move**.
6. In the **ASSIGN COLLECTOR TO GROUP** dialog box, click **Close**, and then wait a minute to make sure your changes have taken effect.

Lab 6: Events and Alerting

There is no lab associated with Lesson 6.

Lab 7: Events, Alerts, and Forensics

In this lab, you will manage FortiEDR collector events and alerts.

Objectives

- Filter and sort alerts
- Find an event
- Export events affecting a specific device
- View raw events
- View an event in the **Forensics** tab
- Set and review an exception
- Archive an event

Time to Complete

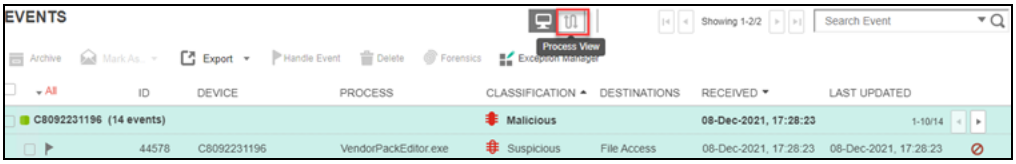
Estimated: 30 minutes

Exercise 1: Aggregating Alert and Export Events

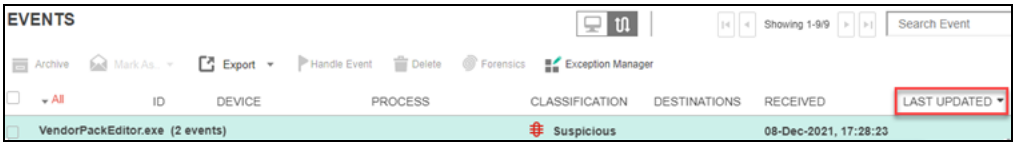
FortiEDR provides many ways to organize events. In this exercise, you will aggregate alert and export events that are affecting a specific device.

To aggregate and sort alerts

1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **EVENT VIEWER** tab.
3. Click the process view icon to aggregate the events by process.



4. Click the **LAST UPDATED** column heading to sort by the most recent occurrence of events.

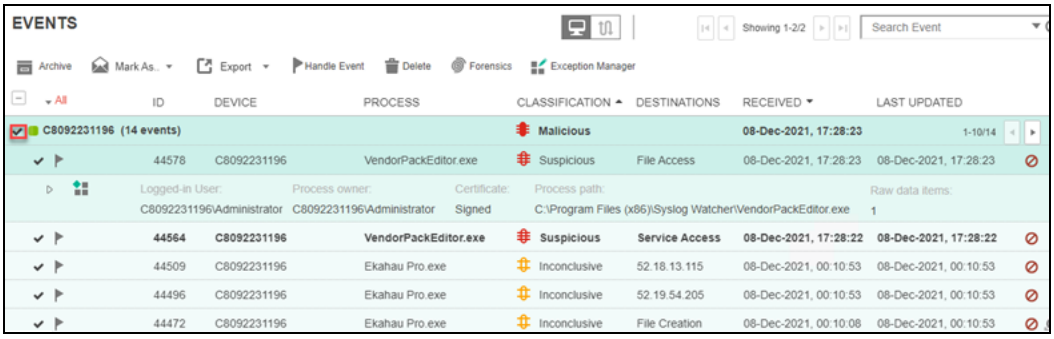


You should see a down arrow, LAST UPDATED ▼. If you see an up arrow, click the column heading again to view the most recent events first.

To export events

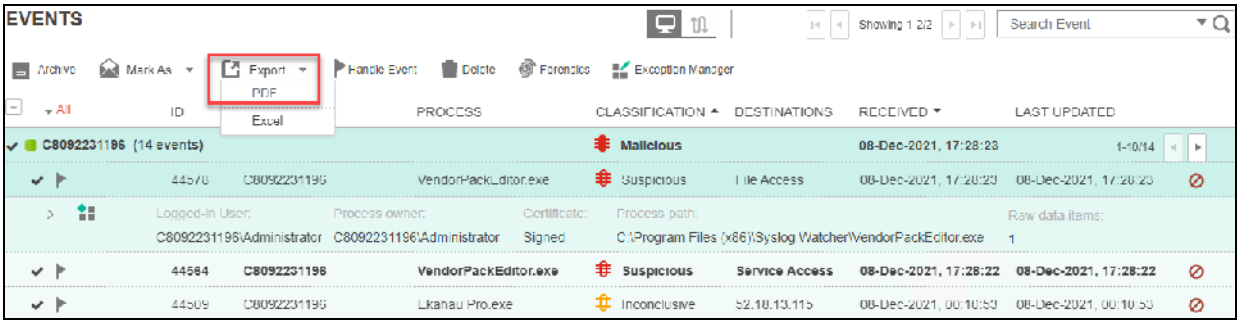
1. Continuing on the **EVENT VIEWER** tab, click the **Device View** button.

2. Select the checkbox for device **C8092231196** for an alert.

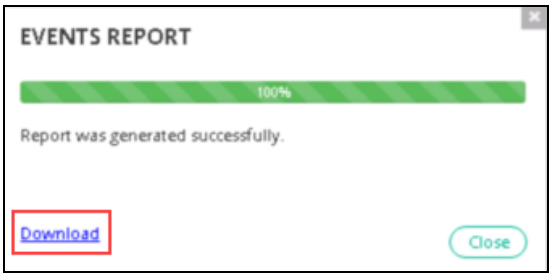


The events in the alert are also selected.

3. Click **Export**, and then select **PDF**.



4. After the file is generated, click the **Download** link to save the file.



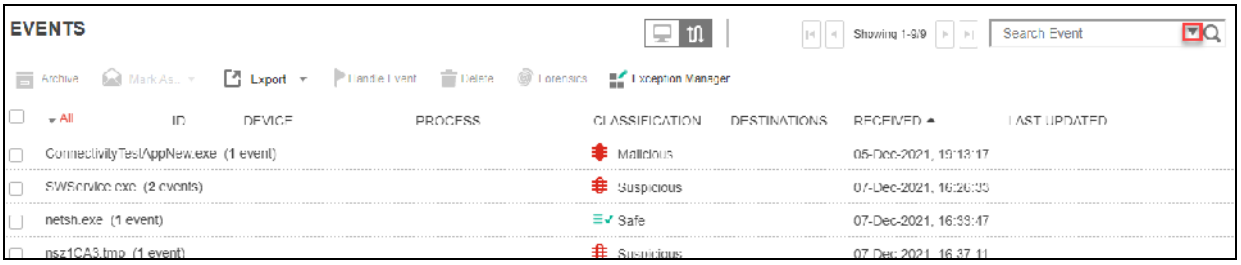
5. Click **Close** to close the download prompt window.
6. Click the file at the download option of the browser window to view it.

Exercise 2: Examining Event Work Flow

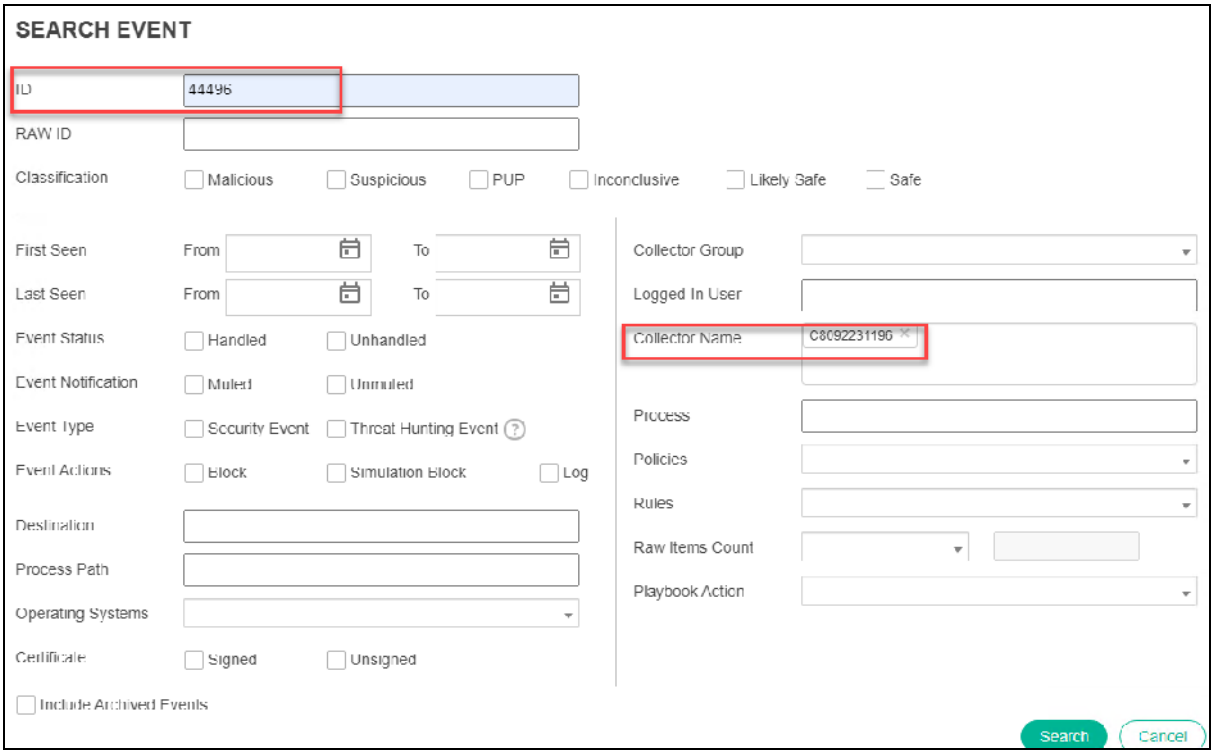
In this exercise, you will find a specific event, investigate it, and create an exception. The user's device name is **C8092231196** and the event ID is **44496**.

To find an event

1. Continuing on the management console, in the **EVENT VIEWER** tab, click the **Process View** button to switch back to the process view.
2. Click the arrow in the search bar to open the **Advanced Search** window.



3. In the **ID** field, type `44496`, in the **Collector Name** field, type `C8092231196`, and then click **Search**.

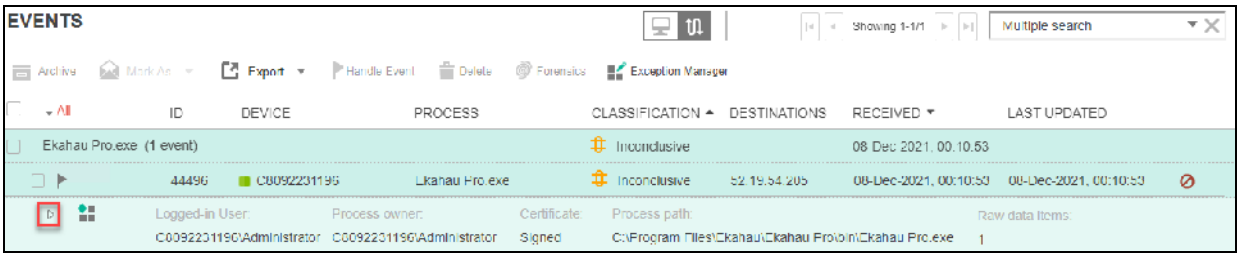


When you click inside the **Collector Name** field, you can see a list of all collectors registered to your network. Type the first few letters to narrow the list.

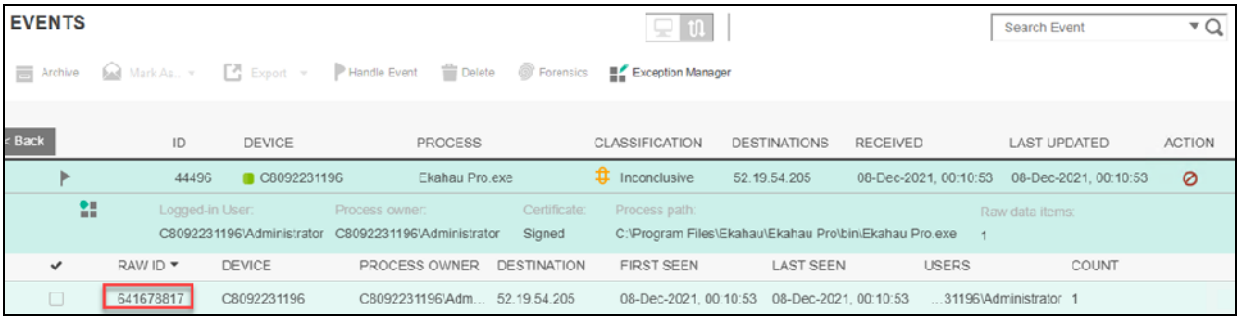
Event **44496** should now appear.

To investigate an event

1. Continuing on the **EVENT VIEWER** tab, click the arrow under the checkbox for event **44496** to view the raw event details.



2. Notice that the raw event has its own ID.

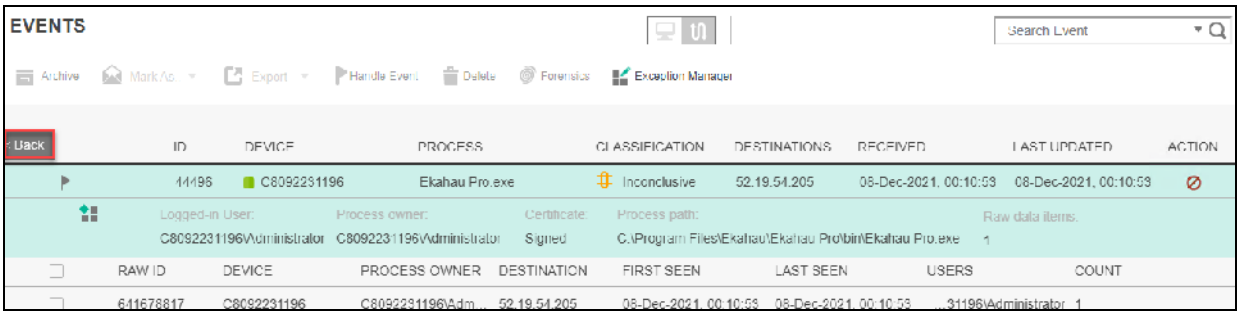


3. Click to expand the **Advanced Data** panel at the bottom of the raw events list. Note the following steps leading to the event:
   - `SYSTEM` created `smss.exe`.
   - `smss.exe` created `winlogon.exe`.
   - `winlogon.exe` created `userinit.exe`.
   - `userinit.exe` created `explorer.exe`.
   - `explorer.exe` created `Ekahau Pro.exe`.
   - `Ekahau Pro.exe` created a thread and attempted to connect to an external IP address using a dynamic code, but was blocked by FortiEDR because it violated the **Dynamic Code - Malicious Runtime Generated Code Detected** rule.

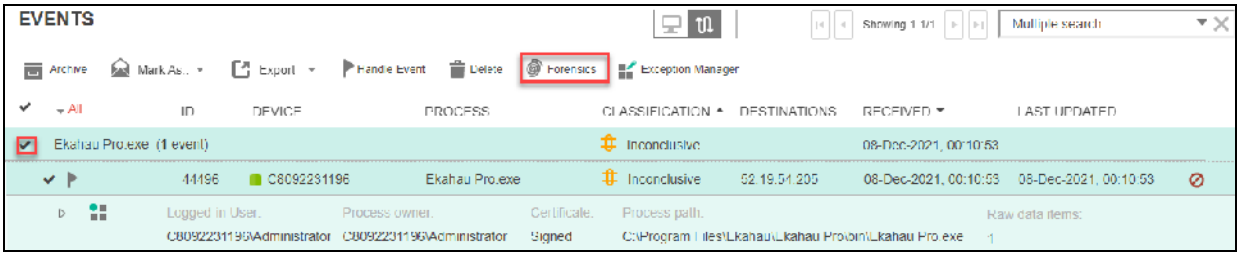
4. Click **Geo Location** to view information about the IP address that the process attempted to contact.

This event appears to have been communicating with an IP address that is registered to Amazon. Keep in mind that this information may be misleading because of IP spoofing. Now, you will investigate the event in the **Forensics** tab.

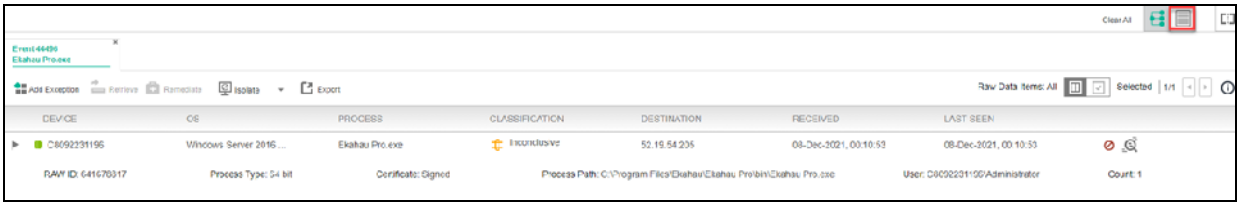
5. Click the **Back** button.



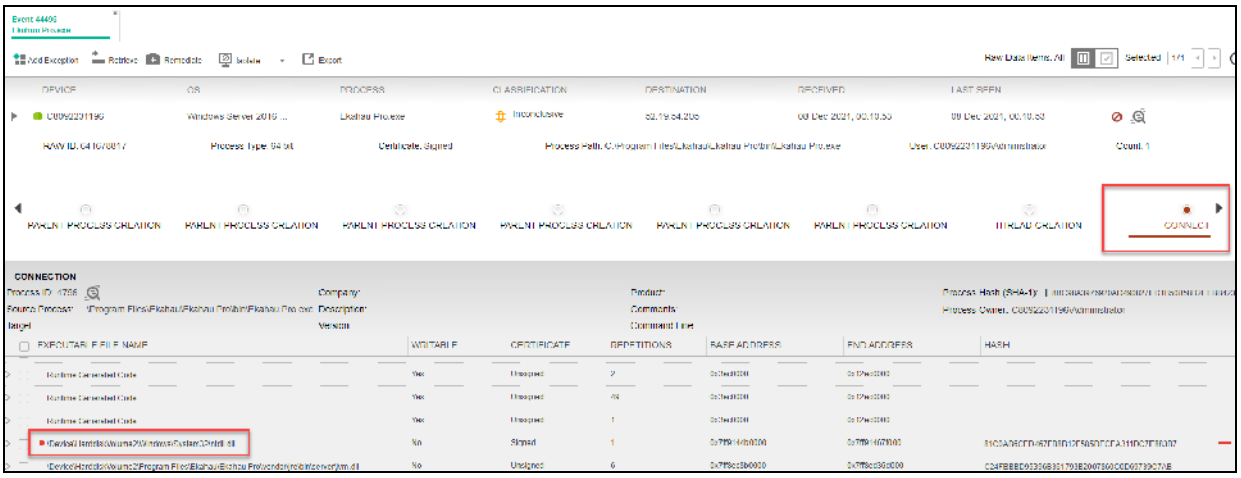
6. Select the checkbox for the process **Ekahau Pro.exe**, and then click **Forensics**.



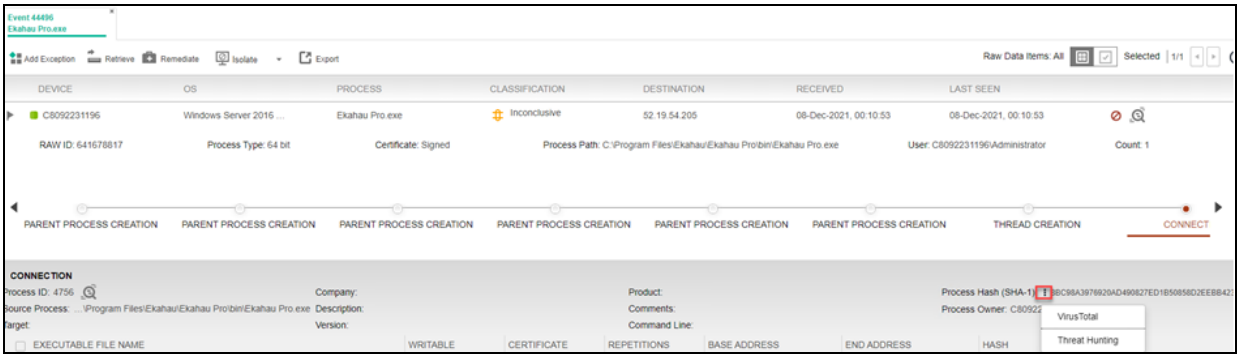
7. In the **Forensics** tab, click the **Stacks** button.



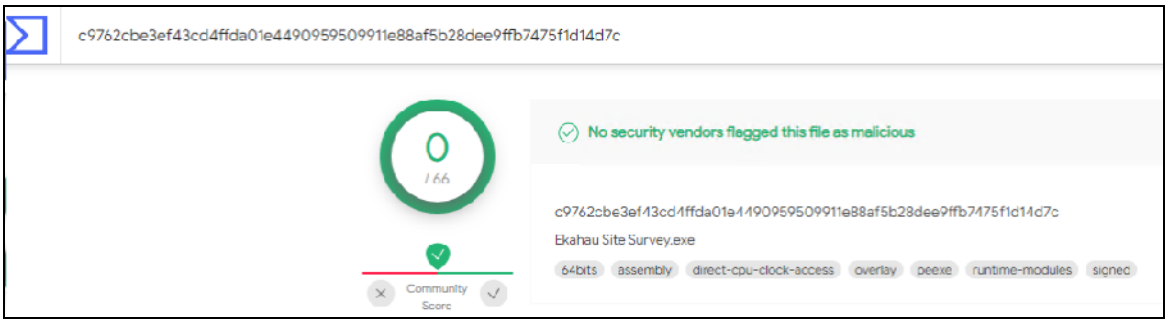
8. Check the process that violated a rule (marked with a red dot ●).



9. Click the three vertical dots (⋮) beside the hash, and then select **VirusTotal** to check the reputation of the hash.



There should not be a red flag.



VirusTotal is an external web resource that offers guidance and analysis with almost all anti-malware software in the market. It provides the number of traditional antivirus programs that have identified the file as malicious or undetected. 0/73 means that none of the antivirus programs have identified the file as malware. 67/73 means that 67 antivirus programs have identified the file as malware over 73 different antivirus software programs.

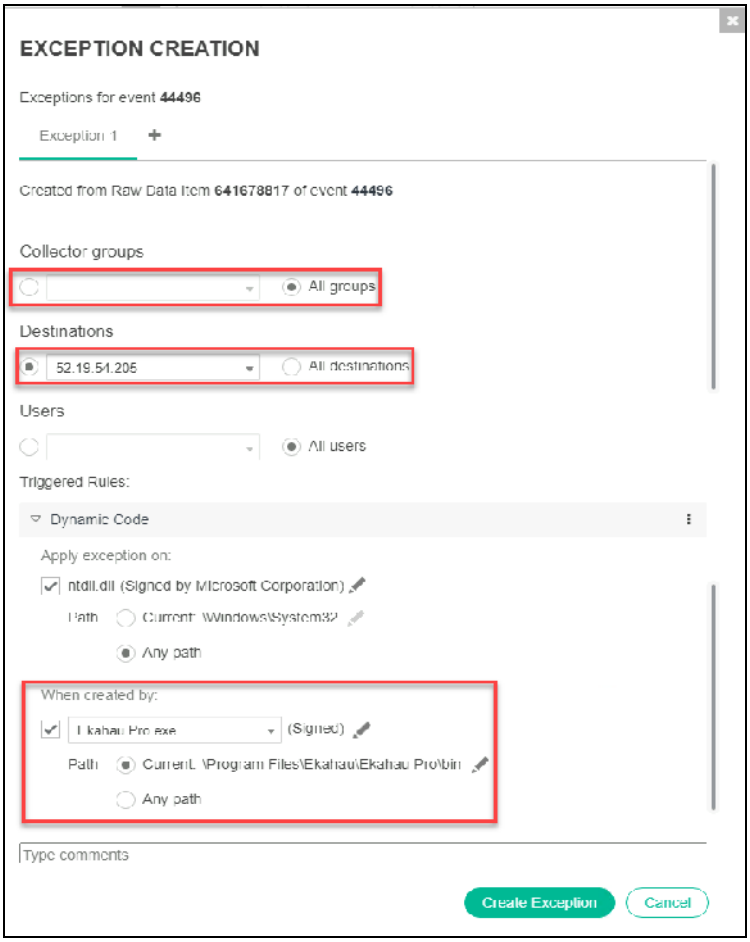
Create an exception

After thoroughly reviewing the `Ekahau Pro.exe` process, you have decided that you want to allow it to run. You will create an exception.

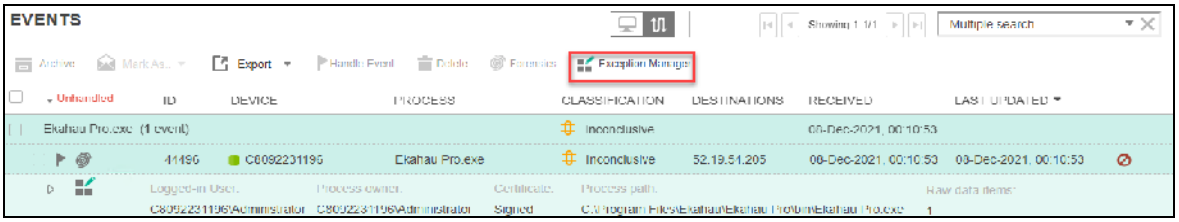
To create an exception

1. Return to the **EVENT VIEWER** tab, and then click the exception icon for the event.

2. In the **Collector groups** field, select **All groups**,.
3. In the **Destinations** field, select **52.19.54.205**.
4. In the **When created by** field, select **Ekahau Pro.exe** in the drop-down list.
5. In the **Path** field, select **Current: \Program Files\Ekahau\Ekahau Pro\bin**.



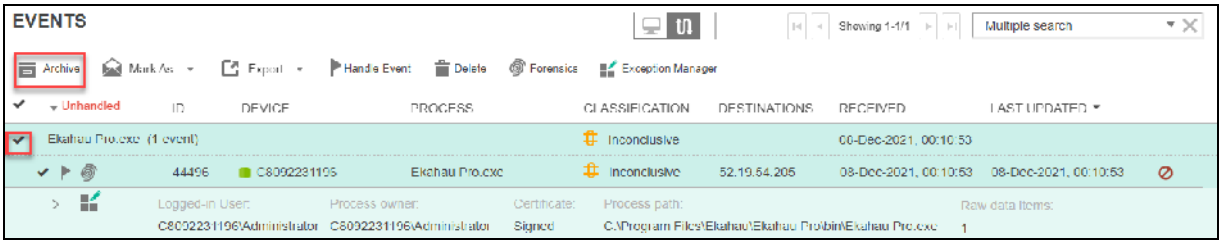
6. Click **Create Exception**.
7. In the **EXCEPTION SAVED SUCCESSFULLY** dialog box, click **Close**.
8. Above the events list, click **Exception Manager**.



The exception should be listed in the **EXCEPTION MANAGER**.

After you create an exception for an event, a best practice is to archive the event.

9. On the **EVENT VIEWER** tab, select the checkbox for the **Ekahau Pro.exe** event that you created exceptions for in the previous steps, and then click **Archive**.



The events disappear from your events list. If a variation of the event occurs that is not covered by the exceptions, a new event is created.

Lab 8: Fabric Integration and FortiXDR

There is no lab associated with Lesson 8.

Lab 9: RESTful API

In this lab, you will learn how to use the RESTful API with FortiEDR.

Objectives

- Create an API user
- Search for blocking events
- Retrieve a sample of a malicious file
- Remediate the infected device
- Move the collector into the high security collector group
- Archive events
- Find an event that is not malicious
- Create an exception

Time to Complete

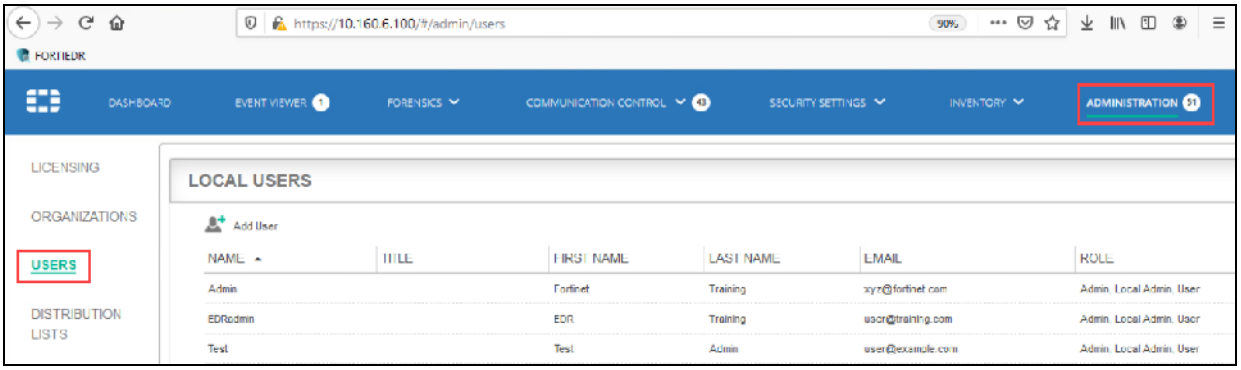
Estimated: 45 minutes

Exercise 1: Configuring the RESTful API

In this exercise, you will configure the RESTful API application to perform various tasks on the FortiEDR management server.

To create an API user on the FortiEDR management server

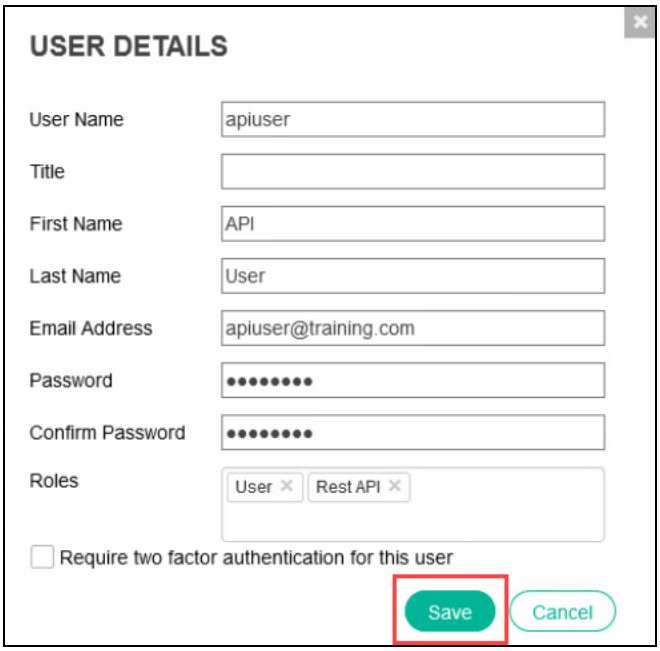
1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click the **ADMINISTRATION** tab, and then in the left pane, select **USERS**.



3. Click **Add User**, and then configure the following settings in the **USER DETAILS** pop-up window:

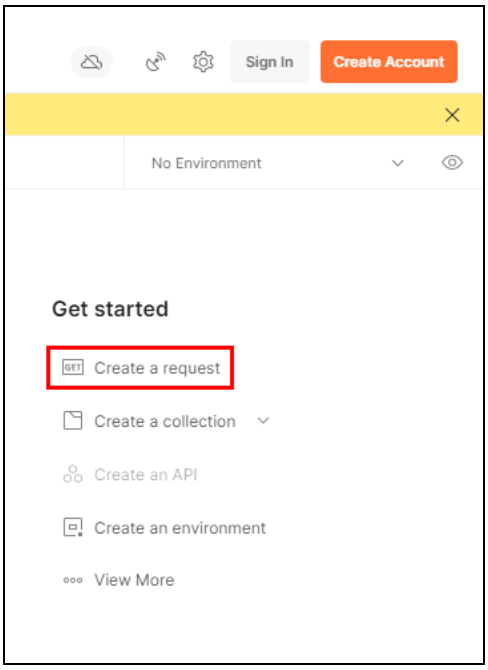
Field	Value
User Name	apiuser
First Name	API
Last Name	User
Email Address	apiuser@training.com
Password	training
Confirm Password	training
Roles	Select **User** and **Rest API**.

4. Click **Save** to create the API user.

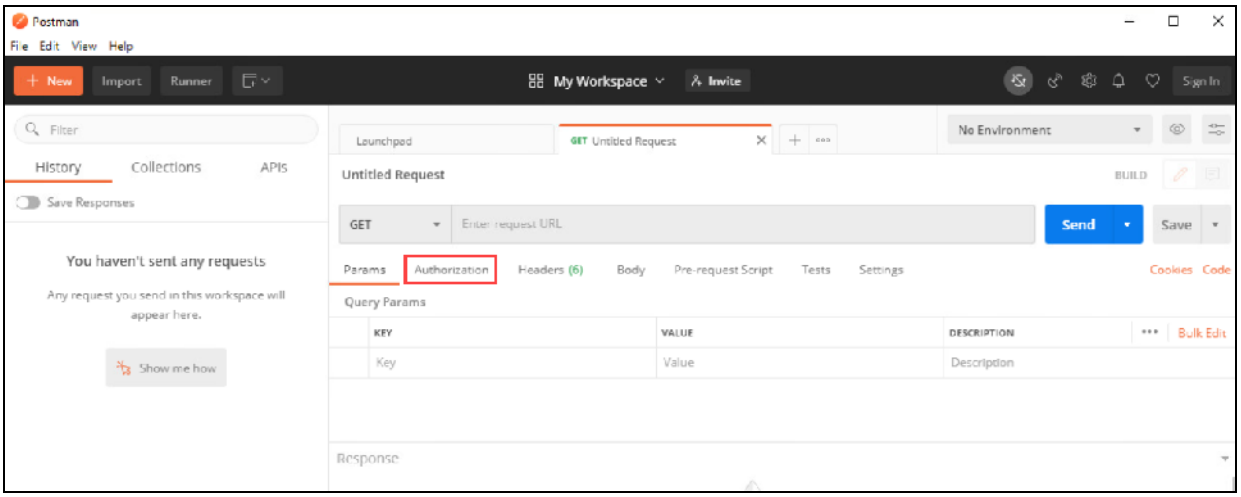


To adjust settings for the FortiEDR API

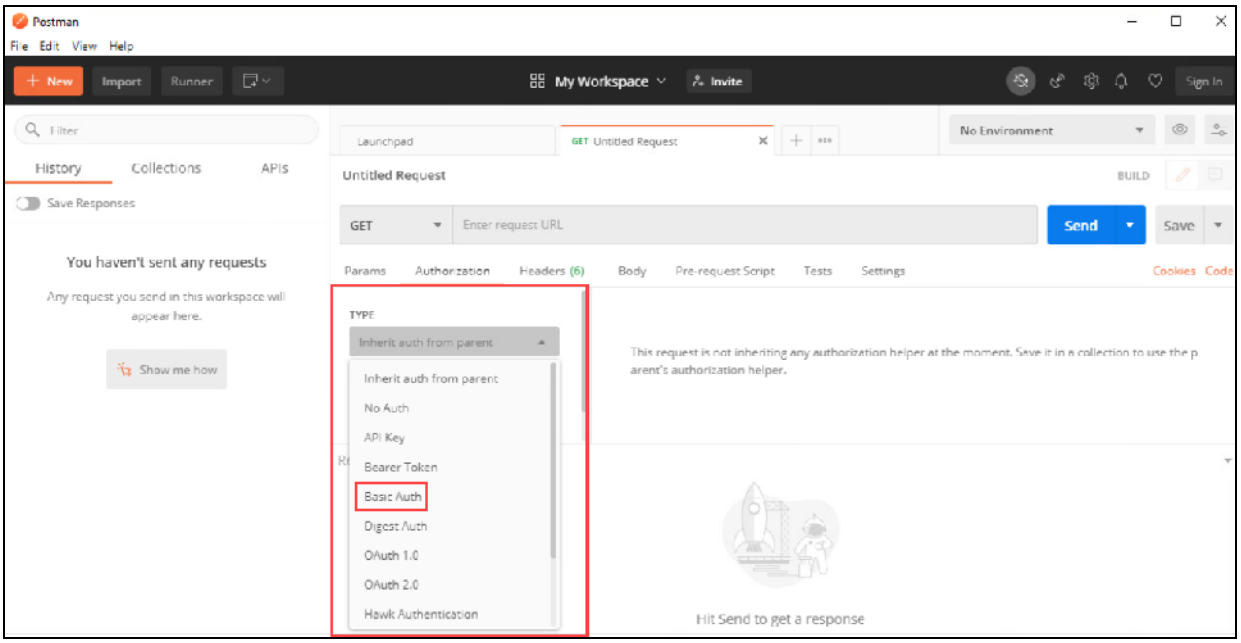
1. On the Browser VM desktop, double-click the **Postman** shortcut icon to launch the API application.
2. In the Postman application window, click **Create a request**.



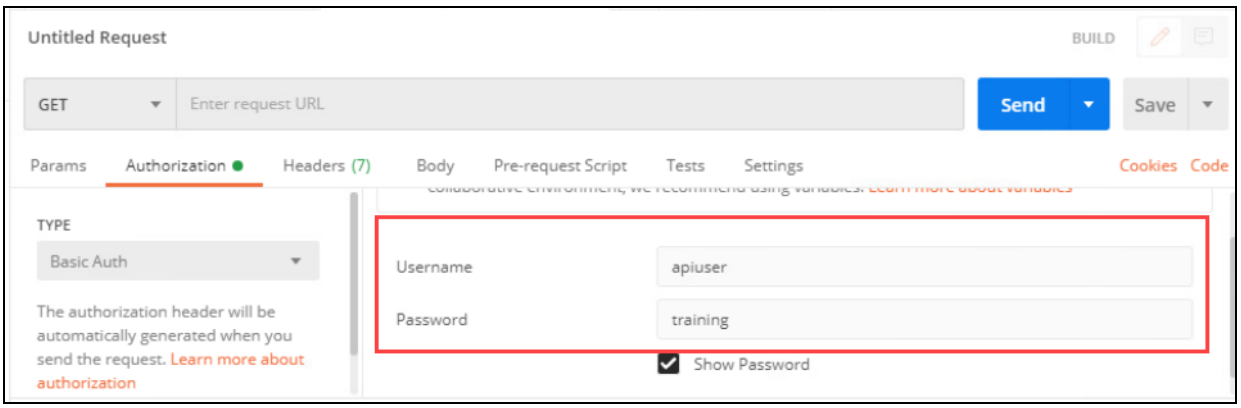
3. Click **Authorization**.



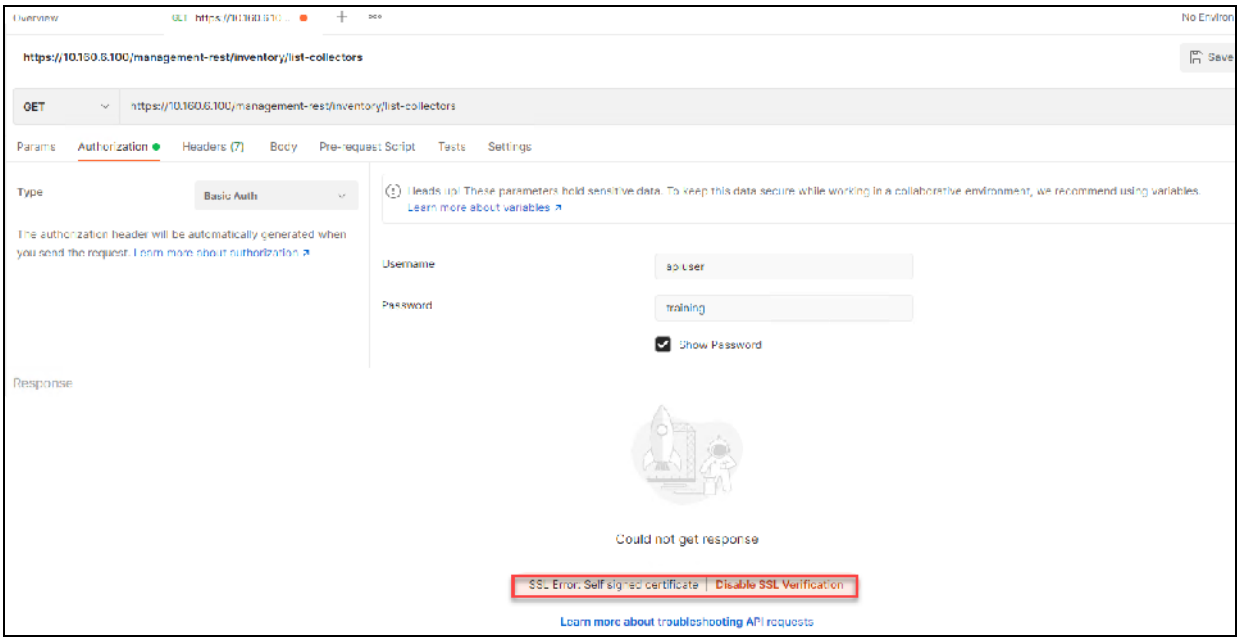
4. Click the **TYPE** drop-down menu, and then select **Basic Auth**.



5. In the **Username** field, type `apiuser`, and then in the **Password** field, type `training`.



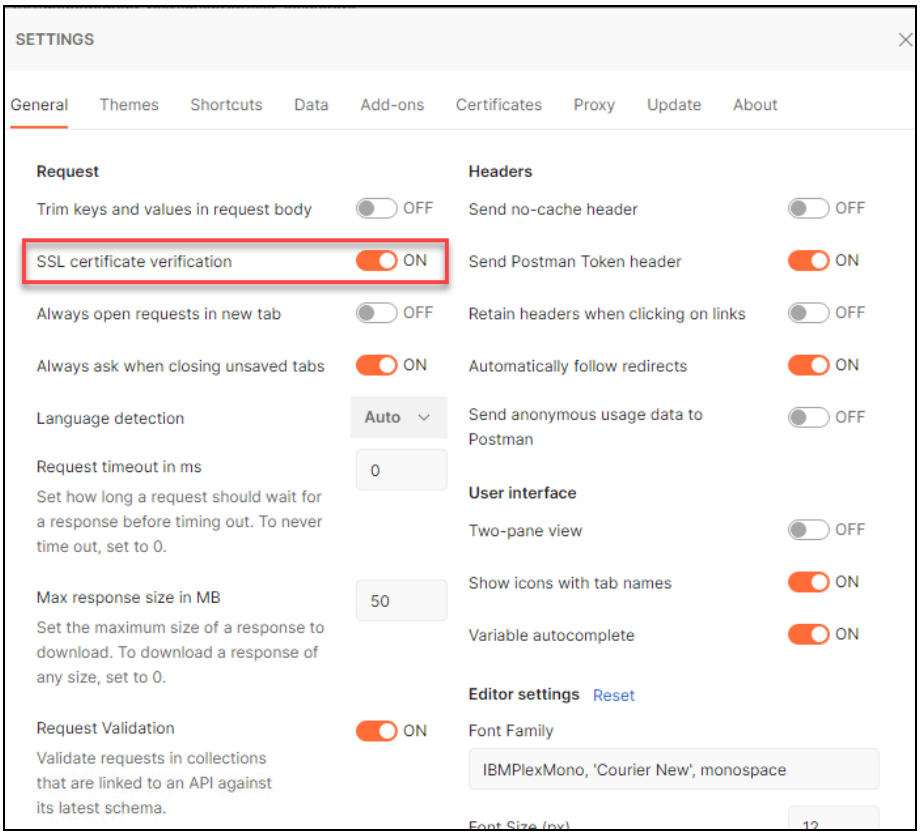
6. In the **GET** field in the top of the right panel, type `https://10.160.6.100/management-rest/inventory/list-collectors`, and then click **Send**.



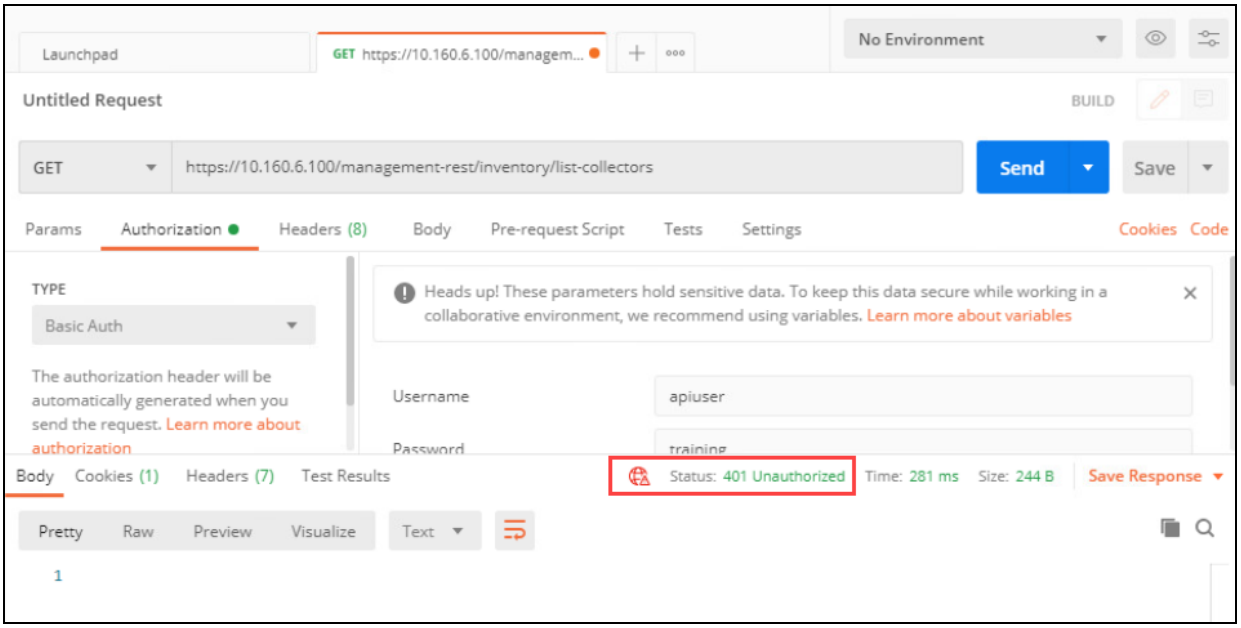
An error message will appear because Postman is blocking the management console's self-signed certificate.

A copy of the API calls used in this lab is in the `api.txt` file, which is located in the **Resources** folder on the Browser VM desktop.

7. To allow the self-signed certificate, click **File** > **Settings**, and then click the **SSL certificate verification** slider to set it to **OFF**.



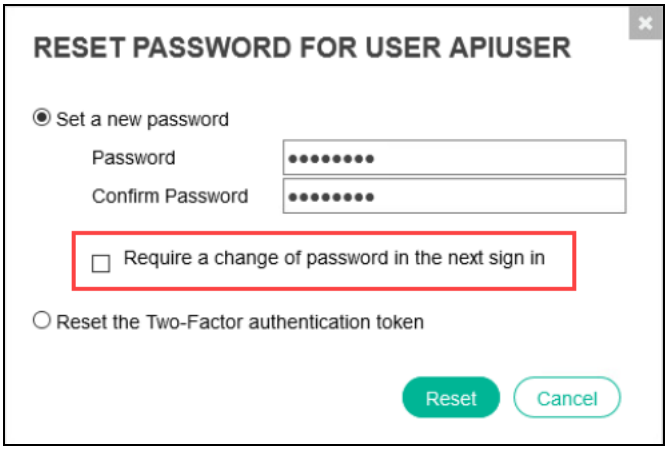
8. Close the **SETTINGS** window.
9. Click **Send** to try the test request again.
   The status of your request is **Unauthorized**.



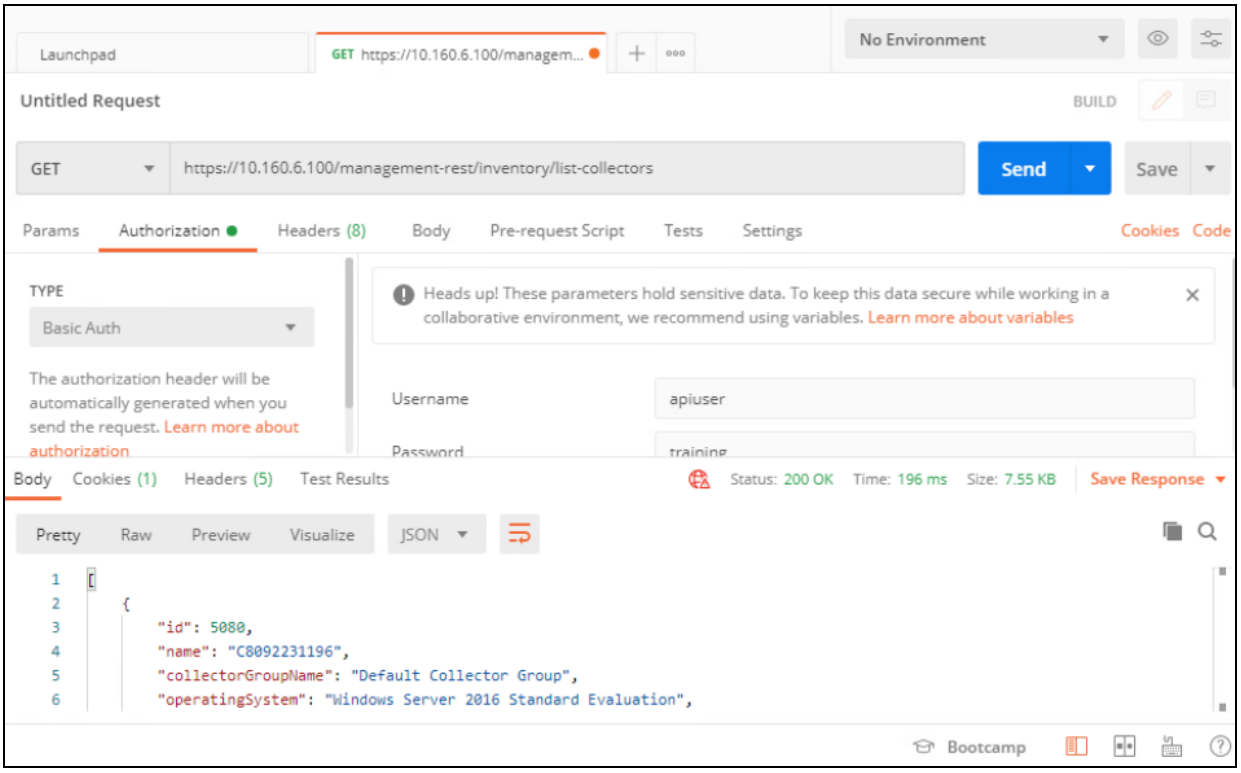
This status is because FortiEDR requires a password reset the first time a user logs in.

10. On the FortiEDR GUI, click the **ADMINISTRATION** tab, and then in the left panel, select **Users**.
11. In the user list, find **apiuser**, and then click **Reset Password**.

12. In the pop-up window, type the password `training`, and then re-enter the password to confirm.
13. Clear the **Require a change of password in the next sign in** checkbox, and then click **Reset**.



14. Return to the Postman application, and then click **Send** to send your request again.
There should be a list of collectors in the **Body** field at the bottom of the pane.

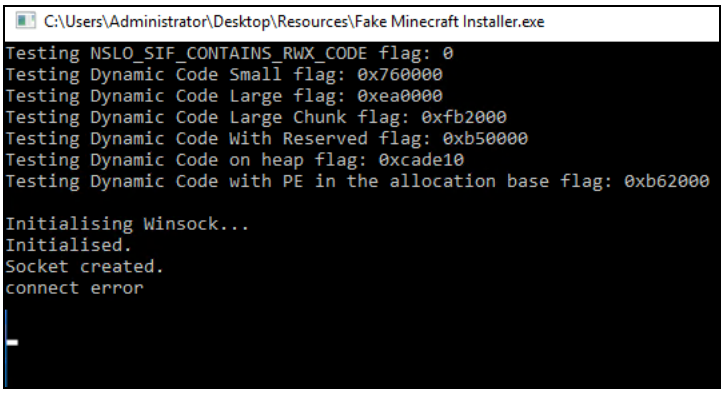


Investigate a Security Event

You will investigate a security event on the Browser VM.

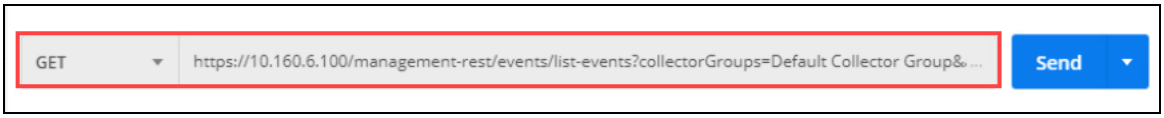
To investigate a security event

1. On the Victim VM desktop, open the **Resources** folder, and then double-click `Fake Minecraft Installer.exe` to run the file.
   You will see a connect error.

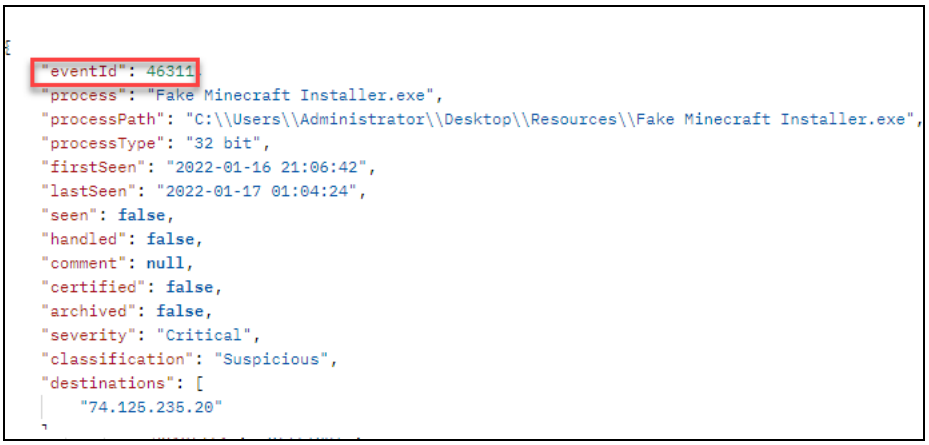


Although this file is not actually malicious, it is unusual behavior and will trigger an alert, which you can use to practice remediating malicious events while they are in memory.

2. Close the command prompt window.
3. In the Postman application, make sure the request type drop-down is set to **GET**, and then type `https://10.160.6.100/management-rest/events/list-events?collectorGroups=Default Collector Group&actions=Block&process=Fake Minecraft Installer.exe`



4. Click **Send**.
5. In the **Body** field at the bottom of the pane, review the returned data.
   You should see the event you just created, with the `Fake Minecraft Installer.exe` process at the top of the list.



6. Copy the **eventID** for this event to a separate text file.
   This is the main ID for the event.
7. Scroll down to the **collectors** section of the same event, find the **device** name, and then copy it to a text file.

8. To retrieve raw event details, in the Postman application, make sure the request type drop-down is set to **GET**, and then type `https://10.160.6.100/management-rest/events/list-raw-data-items?eventId=<eventID>&fullDataRequested=true`, where you replace `<eventID>` with an event ID you copied earlier.

9. Click **Send**.
   The results should look like the following example:

```
"EventId": 883801594,
"EventType": 1,
"Version": 10,
"FirstSeen": 1642385202000,
"LastSeen": 1642399464000,
"Protocol": 6,
"LocalIp": "0:0:0:0:0:0:0:0",
"LocalPort": 0,
"RemoteIp": "74.125.235.20",
"RemotePort": 80,
"Country": "USA",
"Asn": "15169 GOOGLE",
"Count": 4,
"MainProcessId": 672,
"OperatingSystem": "Windows Server 2016 Standard",
"OS": "Windows",
"GlobalAggregationCrc": 17413290151335015576,
"GlobalShaAggregationCrc": 1838554856802510904,
"Application": "\\Device\\HarddiskVolume2\\Users\\Administrator\\Desktop\\Resources\\Fake Minecraft Installer.exe",
"AppSha": "bmKiX/7z8WpwmcGxyi7rwPwPg9k=",
"AppScriptModule": "",
"AppVendor": "",
```

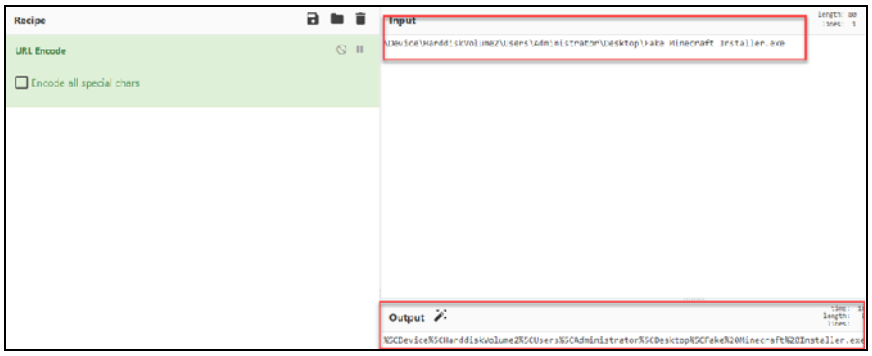

Note that this event ID is the *raw* event ID, which you need to retrieve the file sample.

10. To retrieve the executable, type the following parameters in the request:
`https://10.160.6.100/management-rest/forensics/get-event-file?rawEventId=<EventId>&processId=<MainProcessId>&filePaths=<Path>`

- For `<EventId>`, substitute the raw event ID you copied in the previous step.
- For `<MainProcessId>`, substitute the main process ID you copied in the previous step.
- For `<Path>`, substitute the application path in URL encoded format:
`%5CDevice%5CHarddiskVolume2%5CUsers%5CAdministrator%5CDesktop%5CResources%5CFake%20Minecraft%20Installer.exe%0A`

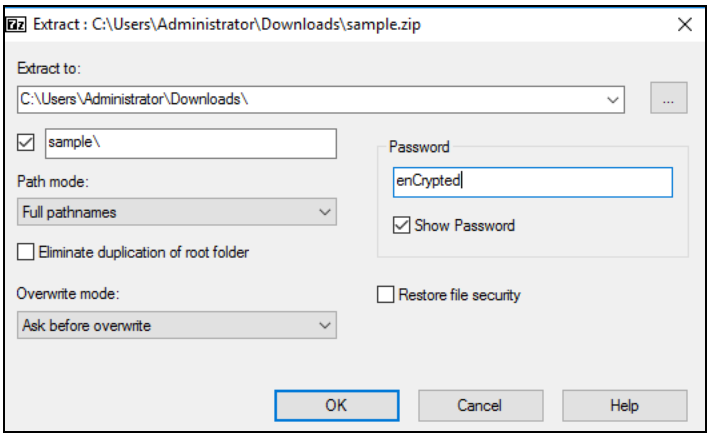
You must convert an application path to URL encoded. Otherwise, a **400 Bad Request** error code is returned if the given parameters do not match the expected format or values range.

In this exercise, the Cyberchef tool is used to convert a file path. You don't need to convert the path above because it is already converted.



11. Click the drop-down arrow beside the **Send** button, and then select **Send and Download**.

12. Wait for the file to generate, and then when prompted, name the file `sample.zip`, and save it to your **Downloads** folder, or any easily accessible location on the VM.
13. Browse to the folder where you saved the sample, right-click the sample file, and then select **7-Zip** > **Extract files**.
14. In the **Extract** window, type the password `enCrypted`, and then click **OK**.



15. Click **Close**.
    You should see the unzipped folder, which contains a file called `Fake Minecraft Installer.exe.ensilo`.
16. Remove `ensilo` from the filename, and accept any warnings about changing the file extension.
17. Double-click the file.
    The file should attempt to execute as it did previously.

When following these steps with an unknown file, be sure to execute the file only in a safe environment to avoid spreading malware.

18. Close the command prompt window.

Remediate the Device

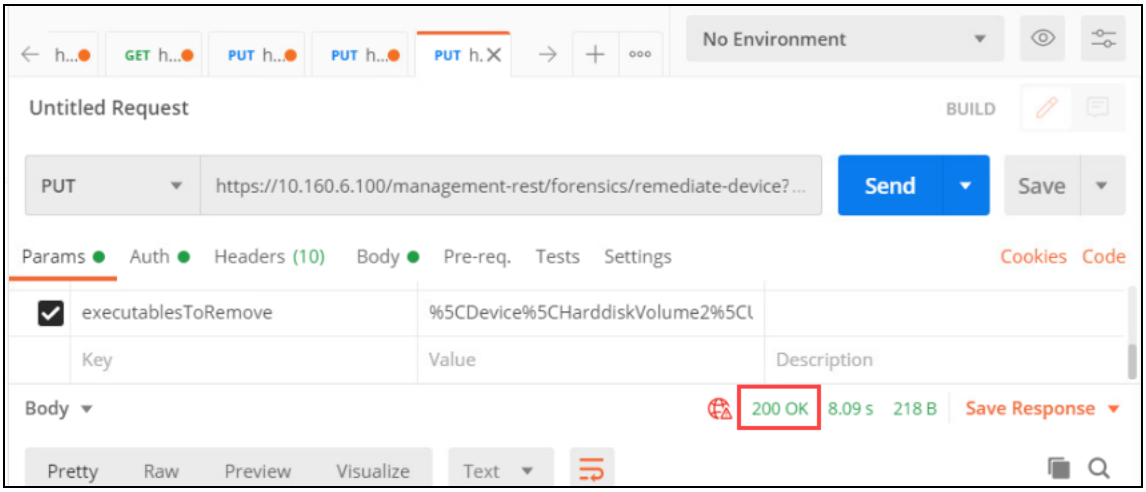
You will remove the malicious executable file, move the collector to the high security group, search other events for the same process, and archive events.

To remove the malicious executable

1. In the Postman application, in the request drop-down list, select **PUT**, and then type `https://10.160.6.100/management-rest/forensics/remediate-device?device=<DeviceName>&executablesToRemove=<ApplicationPath>`

- For `<DeviceName>`, substitute the name of the collector device you copied above.
- For `<Application Path>`, substitute the application path in URL encoded format: `%5CDevice%5CHarddiskVolume2%5CUsers%5CAdministrator%5CDesktop%5CResources%5CFake%20Minecraft%20Installer.exe%0A`

2. Click **Send**.
   When the request is complete, the status at the top of the body field should be **200 OK**.

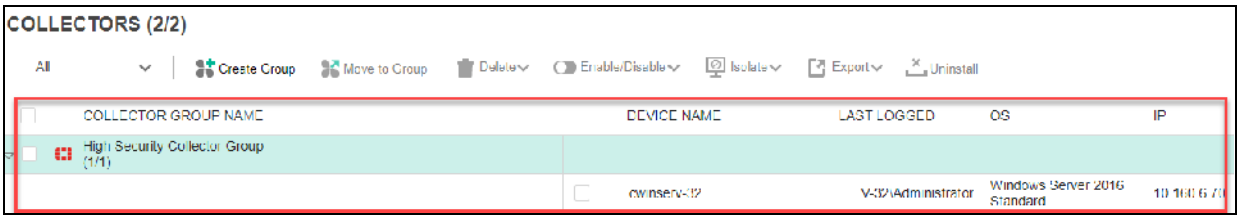


3. Look at the **Resources** folder on the Victim VM desktop.
   The `Fake Minecraft Installer.exe` file should no longer be there.

To move the collector to the high security collector group

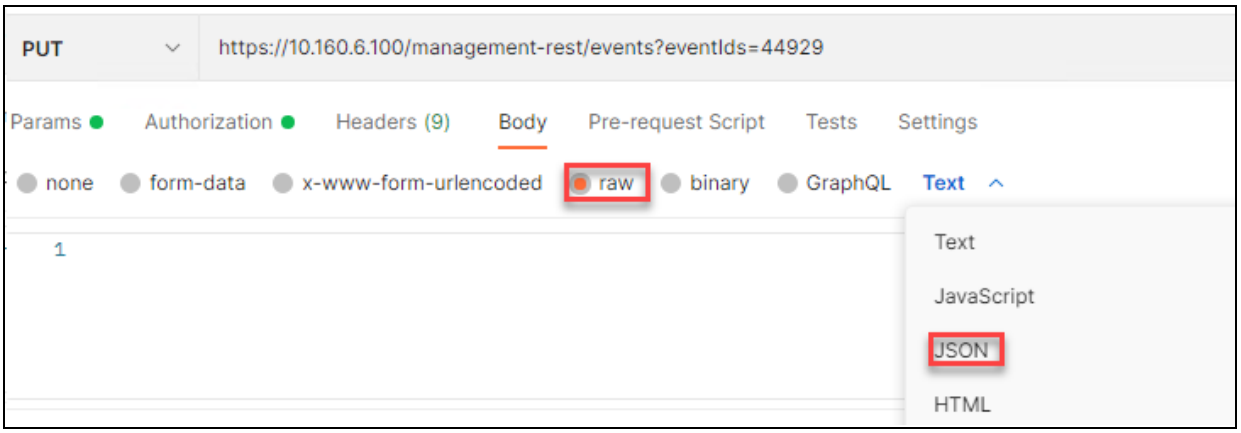
1. In the Postman application, in the request drop-down list, select **PUT**, and then type `https://10.160.6.100/management-rest/inventory/move-collectors?collectors=<DeviceName>&targetCollectorGroup=High Security Collector Group`.
   For `<DeviceName>`, substitute the name of the collector device you copied earlier (`cwinserv-32`).

2. Click **Send**.
   When the request is complete, the status at the top of the body field should be **200 OK**.
3. Return to the FortiEDR GUI, and then click the **INVENTORY** tab.
4. Click **Show all Collectors**, and then open the **High Security Collector Group** to verify that the collector is there.



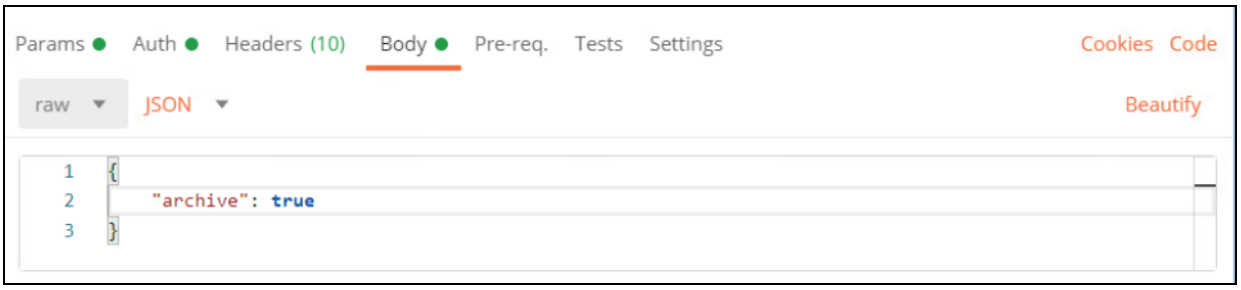
To archive events

1. In the **Request** type drop-down, select **PUT**.
2. Type the following parameters, replacing `<eventId>` with the event ID you copied in the event investigation steps: `https://10.160.6.100/management-rest/events?eventIds=<eventId>`. Do not press **Send** yet.
3. Under the **PUT** field, select the **Body** tab.
4. Select the **raw** radio button, and then in the input type drop-down list, select **JSON**.

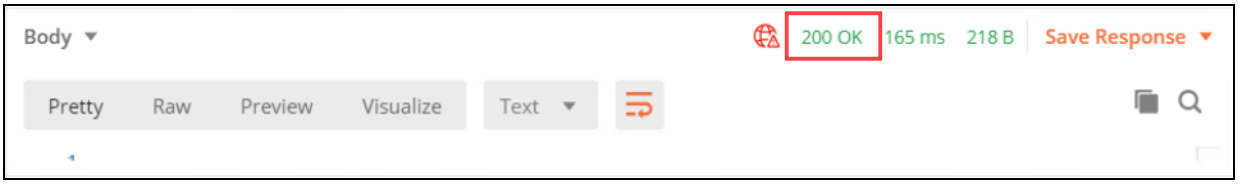


5. In the **Body** field, type the following:

```
{
"archive": true
}
```



6. Click the **Send** button.



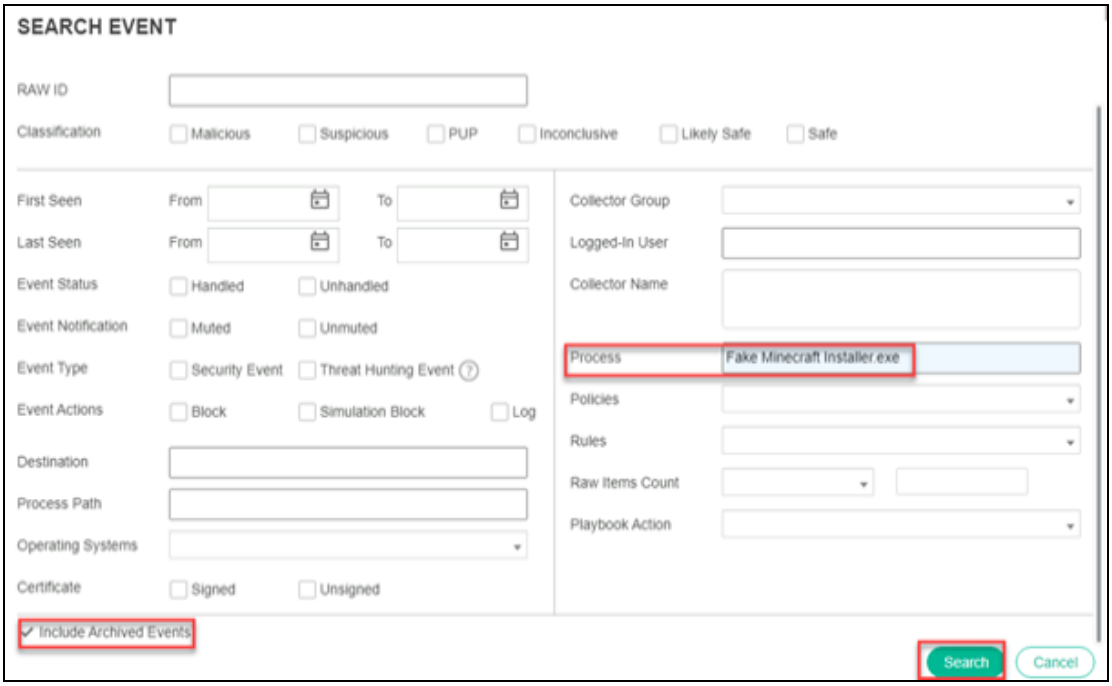
Under **Status**, you should see **200 OK**. You may need to scroll down to see the status.

To verify your changes in the GUI

1. On the FortiEDR GUI, log in with the username `Admin` and password `secureNOT`.
2. Click the **EVENT VIEWER** tab.
3. In the **Search** field, type the main event ID you copied earlier, and then press **Enter**.

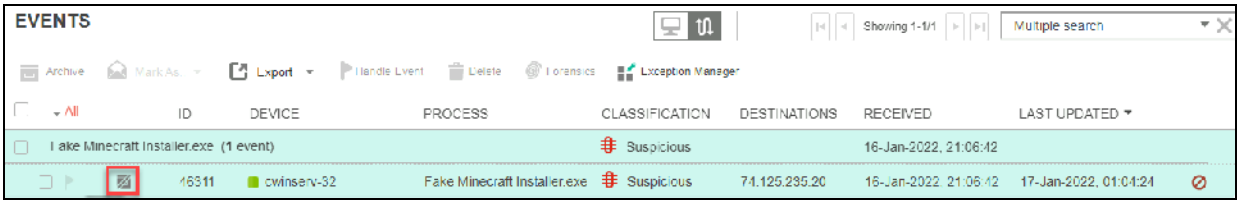
There should not be any results. This is because you marked the event as **Archived**.

4. In the **Search** field, click the arrow to open the **Advanced** search window.
5. In the **Process** field, type `Fake Minecraft Installer.exe`, and then select the **Include Archived Events** box at the bottom.



6. Click **Search**.

The events should now be marked as **Archived**.



Exercise 2: Investigating and Creating an Exception for a Safe Process

In this exercise, you will investigate a safe process, and then create an exception to allow a collector.

Investigate a User Issue With a Safe Process

You receive a support ticket from a specific user who is unable to run the upgrade installer for the Opera browser. First, you will look for blocking events affecting the user's device, **C8092231196**.

To view a user's collector event

1. On the Browser VM desktop, open the **Resources** folder.
2. Double-click the `OperaSetup.exe` file to launch the installer, and then click **Run** to start the installation.
   A pop-up message stating that a fatal error was encountered when the installer executable was loading should appear.
3. Click **OK** to close the window.
4. On the Postman application, make sure the **Request** type drop-down is set to **GET**.
5. Type the following parameters: `https://10.160.6.100/management-rest/events/list-events?actions=Block&device=C8092231196`
6. Click **Send**.

7. In the **Body** field at the bottom of the panel, review the returned data.
   You should see an event involving the process **OperaSetup.exe** at the top of the list. Opera is allowed in your organization, but you must make sure this executable is what it claims to be.
8. Copy the **eventId** for this event to a separate text file.

To investigate an event

1. Continuing on the Postman application, make sure the **Request** type drop-down is set to **GET**.
2. Type the following parameters, replacing `<EventId>` with the event ID you copied in the last step: `https://10.160.6.100/management-rest/events/list-raw-data-items?eventId=<eventID>&fullDataRequested=true`
3. Click **Send**.
4. Examine the resulting information and look for any signs that this file may not be what it claims to be.

```
{
  "EventId": 973235754,
  "EventType": 32,
  "Version": 10,
  "FirstSeen": 1639352107000,
  "LastSeen": 1639353951000,
  "Count": 3,
  "MainProcessId": 3720,
  "OperatingSystem": "Windows Server 2016 Standard",
  "OS": "Windows",
  "GlobalAggregationCrc": 12299834113709125481,
  "GlobalShaAggregationCrc": 6832178769482937281,
  "Application": "\\Device\\HarddiskVolume2\\Users\\Administrator\\Desktop\\Resources\\OperaSetup.exe",
  "AppSha": "2cZHXqD2sPQnve1tdwOG4zA107A=",
  "AppScriptModule": "",
  "AppVendor": "Opera Software",
```


In a real case, you should thoroughly investigate the event, including investigating file hashes and IP addresses, checking certificates, and retrieving a copy of the executable, if available, before you create an exception.

A seemingly legitimate program may be disguised malware or hijacked by malicious actors. In this case, assume that you have investigated and confirmed that the file is a legitimate copy of Opera, so you can proceed to creating an exception.

To create an exception

1. On the Postman application, make sure the drop-down is set to **POST**.
2. Type the following parameters, replacing `<EventId>` with the event ID you copied in an earlier step—do not use the raw event ID from the last step: `https://10.160.6.100/management-rest/events/create-exception?eventId=<EventID>&allCollectorGroups=true`.

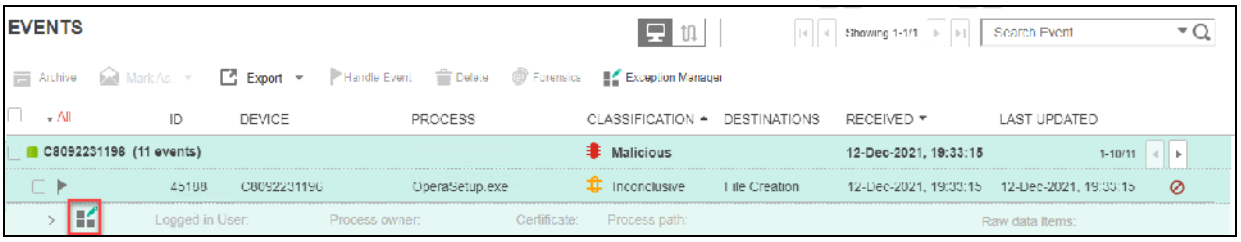
   This creates an exception that is applied to all collector groups.
3. Click **Send**.

   A confirmation message should appear.

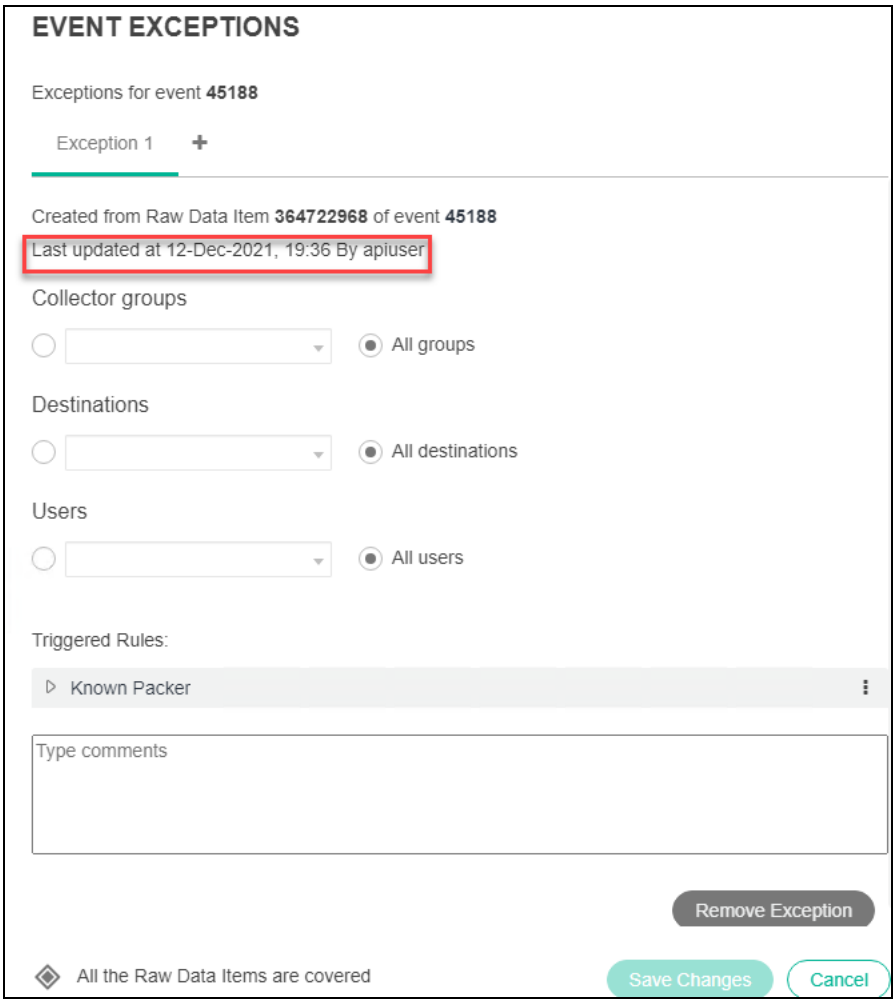
4. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
5. Click the **EVENT VIEWER** tab.
6. Search for the event ID you used to create the exception in a previous step.

If your previous search is still showing, click the **X** in the search bar to start a new search.

7. Verify that the event exception icon now indicates there is an existing exception.



8. Click the exception icon to view the exception details.



You will see that the exception was created by **apiuser**.

9. Close the Postman application.

Lab 10: Troubleshooting

In this lab, you will troubleshoot collector problems.

Objectives

- Determine why, on a brand new installation, two of the newly installed collectors are not working
- Determine why the DB administrator cannot run Syslog Watcher

Time to Complete

Estimated: 45 minutes

Prerequisites

Before beginning this lab, you must run the following scripts to break the communication from the collectors to the aggregator:

1. On the Victim VM desktop, open the **Resources** folder, and then double-click the `firewall.bat` script.
2. On the Browser VM desktop, open the **Resources** folder, and then double-click the `reconfigure.bat` script.
3. Wait a few minutes for the scripts to execute. Do not close any of the command prompt windows that are opened while executing the script.

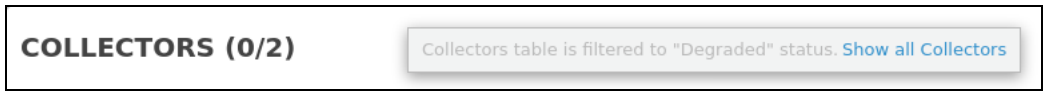
Exercise 1: Troubleshooting Newly Installed Collectors

You will troubleshoot a connectivity issue between newly installed collectors and the FortiEDR GUI.

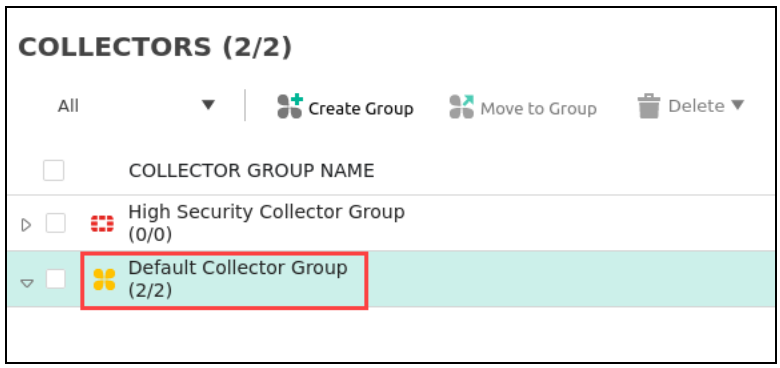
The steps outlined in this lab work only if you executed the scripts specified in the *Prerequisites* section of this lab.

To check the collector status

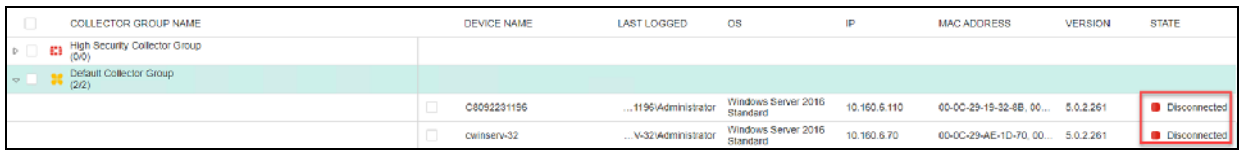
1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. On the **INVENTORY** tab, click to expand the **Collectors** bar.
   By default, the **COLLECTORS** view shows only *degraded* collectors.
3. Click **Show all Collectors** to see collectors that are not in a **Degraded** state:



4. If you do not see the **Show all Collectors** link, click the collectors bar to expand it.
   In this lab environment, there are two collectors, which are both in the **Default Collector Group**.



5. Click to expand the **Default Collector Group**.
   The state of both collectors should be **Disconnected**.

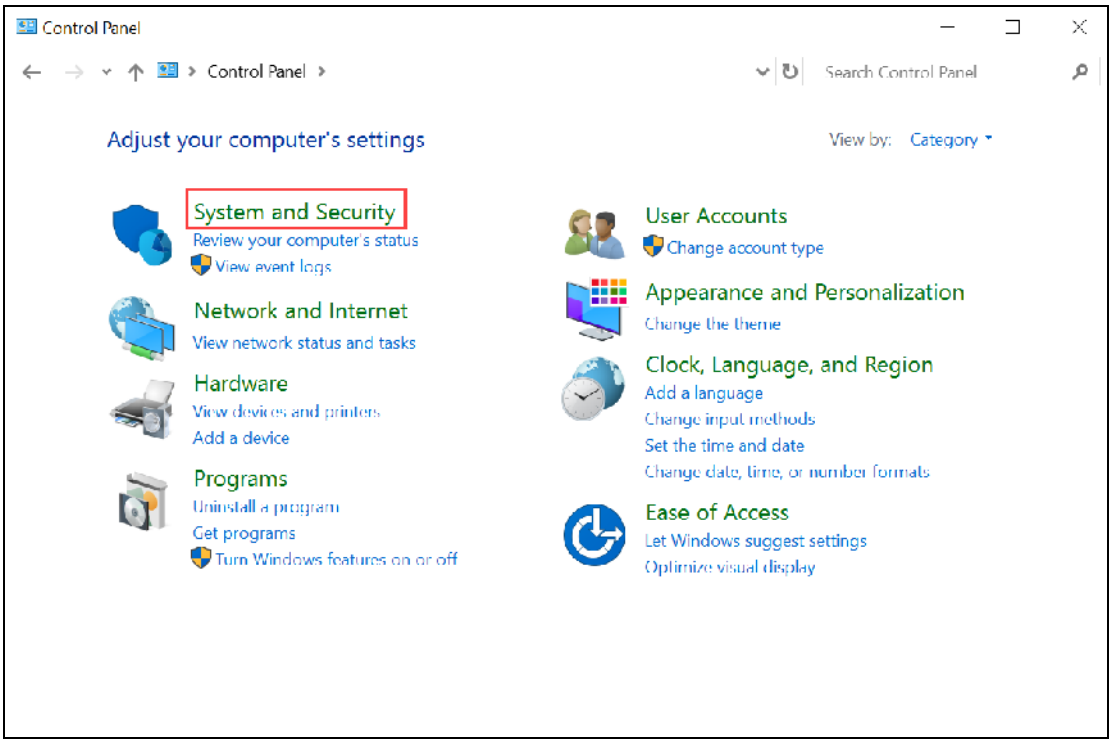


Remember, a **Disconnected** state is generally not a problem for a collector, because this is the state that is shown when a machine is offline or has been shut down. However, in this case, we know that both machines are running and should be connected to the network.

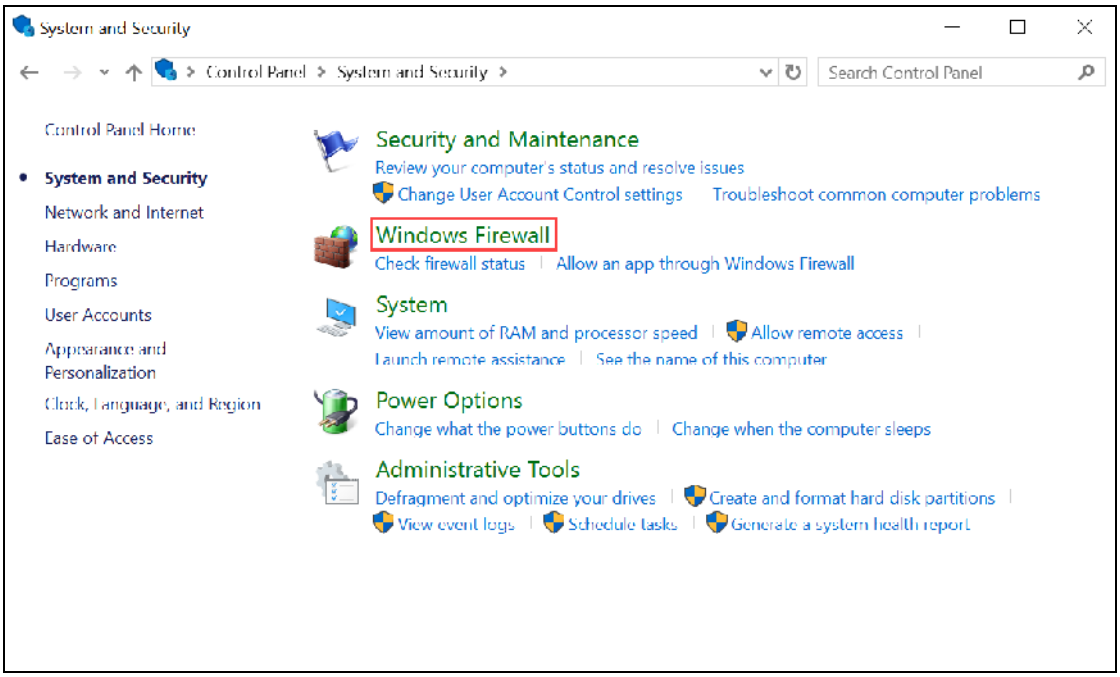
To troubleshoot the Victim VM

1. On the Victim VM, open the command prompt, and then ping the IP address `10.160.6.100`.
2. If you can ping the server, enter `telnet 10.160.6.100 8081` to test the connection to the central manager port.

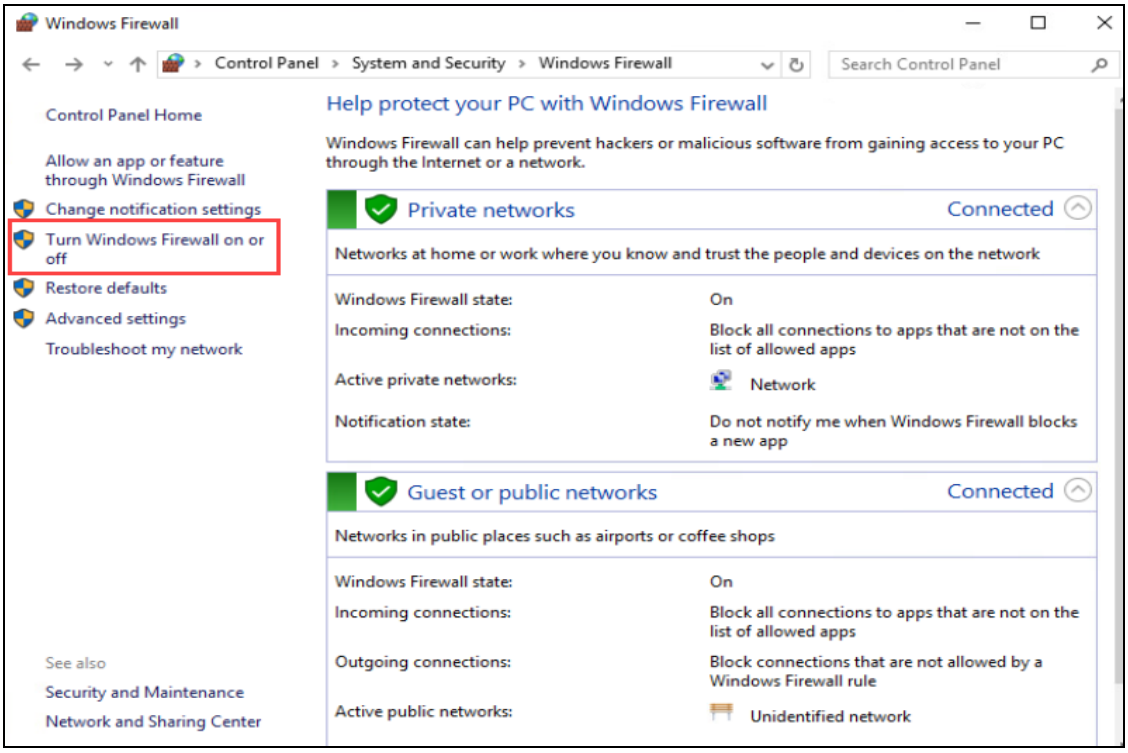
   The connection fails because Windows Firewall is active.
3. On the Victim VM, open the **Control Panel** (**Start** > **Control Panel**), and then click **System and Security**.



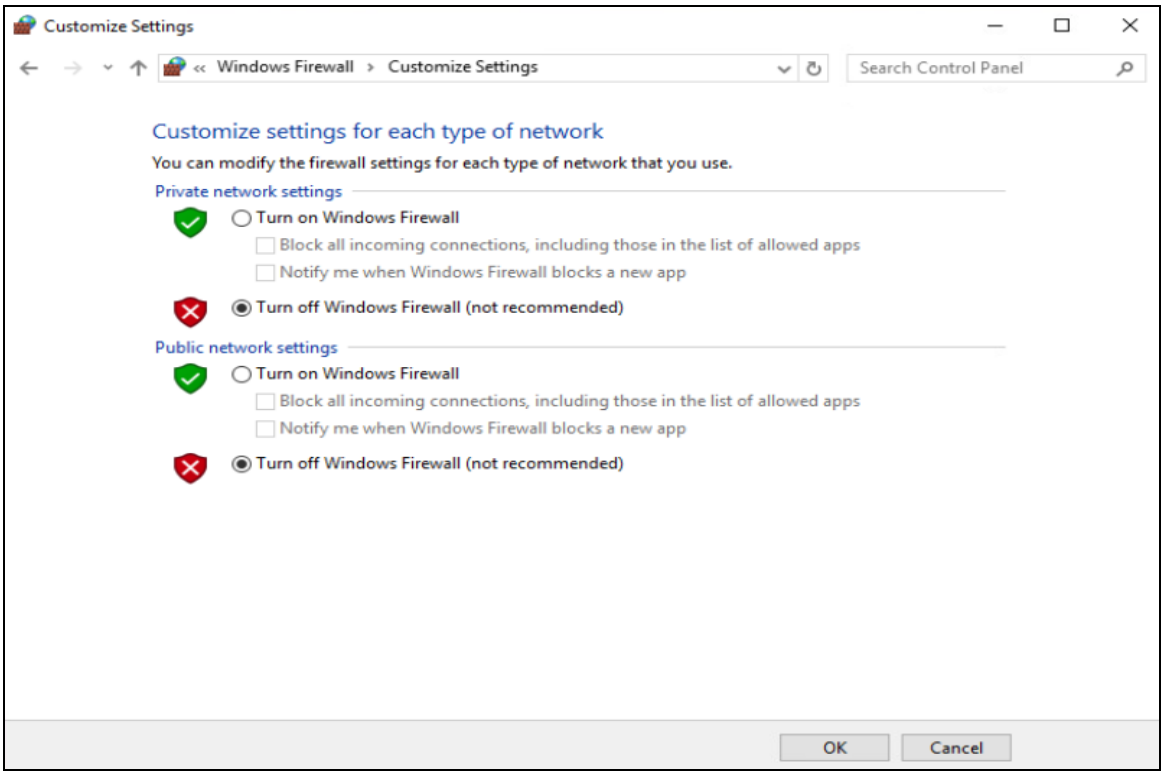
4. Click **Windows Firewall**.



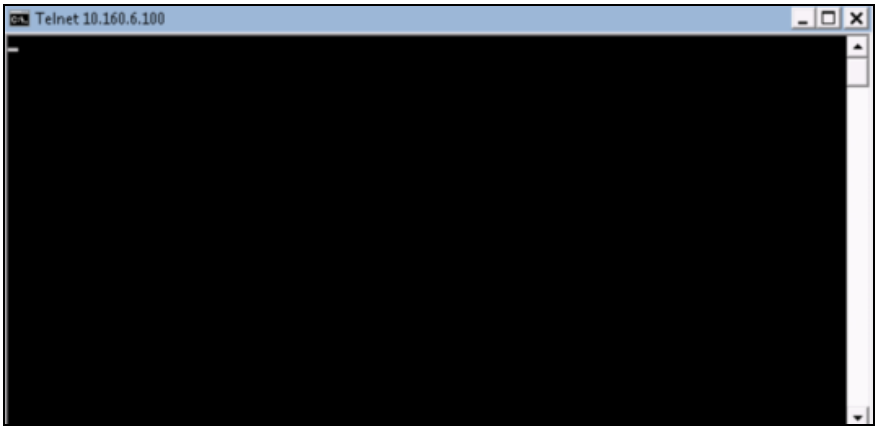
5. On the left, click **Turn Windows Firewall on or off**.



6. For each type of network, select **Turn off Windows Firewall**.

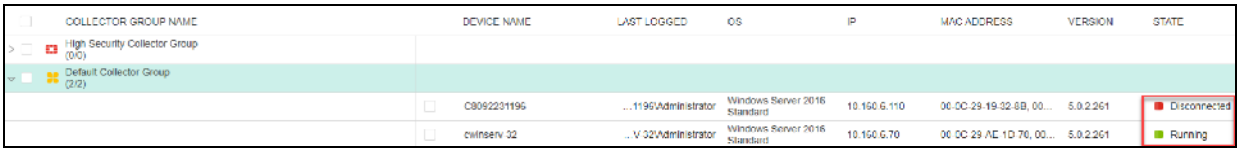


7. Click **OK** to save the settings.
8. Return to the command prompt, type `telnet 10.160.6.100 8081`, and then press `Enter` to test connectivity.



There should be an empty command prompt window labeled **Telnet 10.160.6.100**. This means the connection was successful.

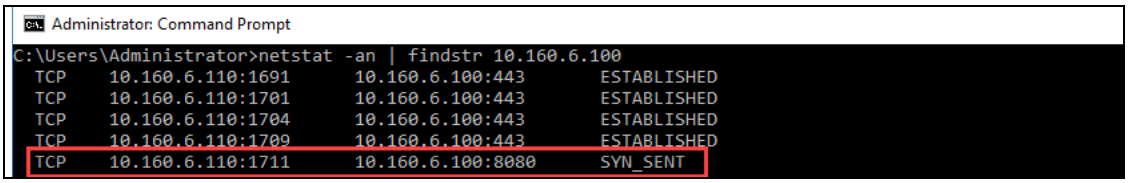
9. On the Browser VM, return to the FortiEDR GUI to check the collector status.



You should see that the **cwinserv-32** collector is now connected, but the other collector is still down.

To troubleshoot the Browser VM

1. On the Browser VM, open the command prompt, type `ping 10.160.6.100`, and then press `Enter` to run ping.
   Ping works.
2. In the command prompt window, type `telnet 10.160.6.100 8081`, and then press `Enter` to test the connection to the central manager port.
   You can connect to port 8081.
3. Close the window.
4. Open the command prompt again, type `netstat -an | findstr 8081`, and then press `Enter` to find instances of the collector attempting to communicate with the aggregator on the designated port.
   There are no results.
5. Enter `netstat -an | findstr 10.160.6.100` to get a full list of connections to the aggregator.

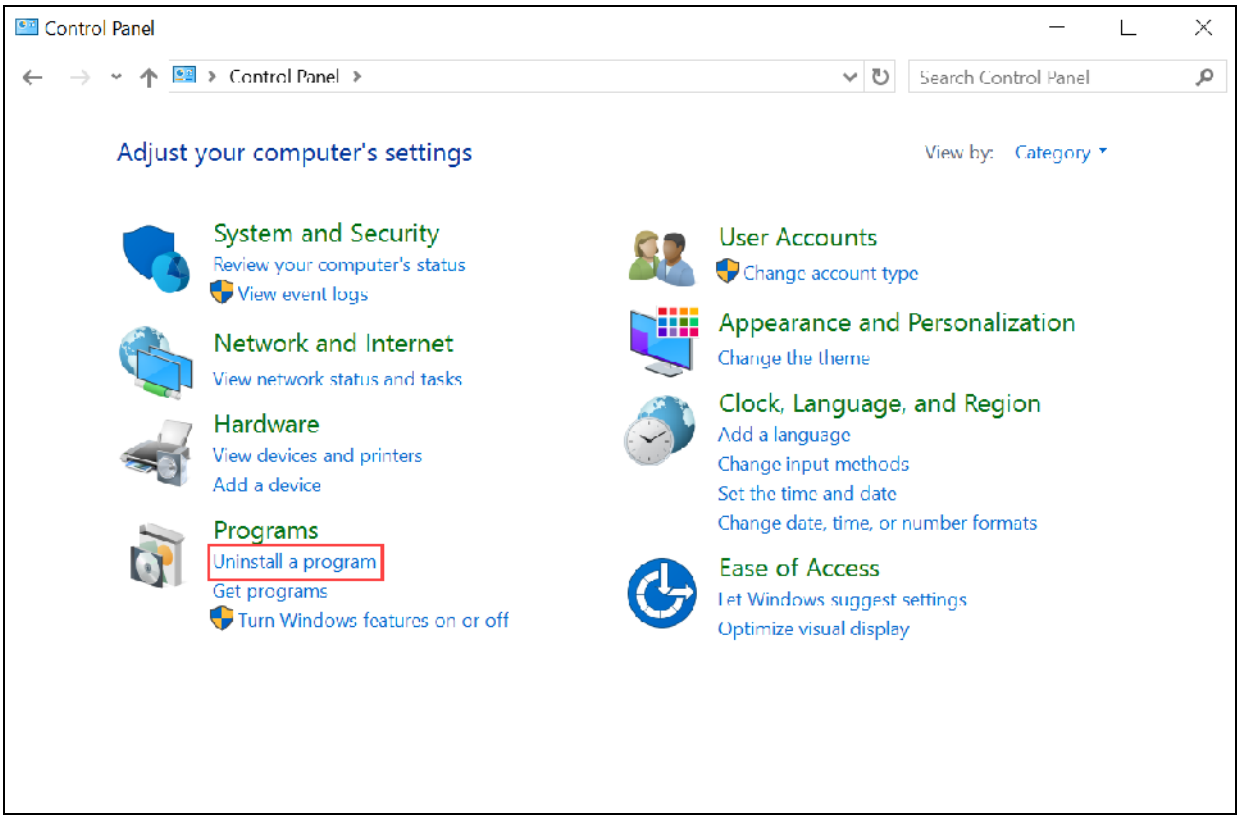


Stop and think!

Why is the collector attempting to communicate on port 8080 rather than port 8081? This is because the collector is configured to use port 8080 rather than the default, port 8081. To resolve this, you must reinstall the collector using the correct port setting.

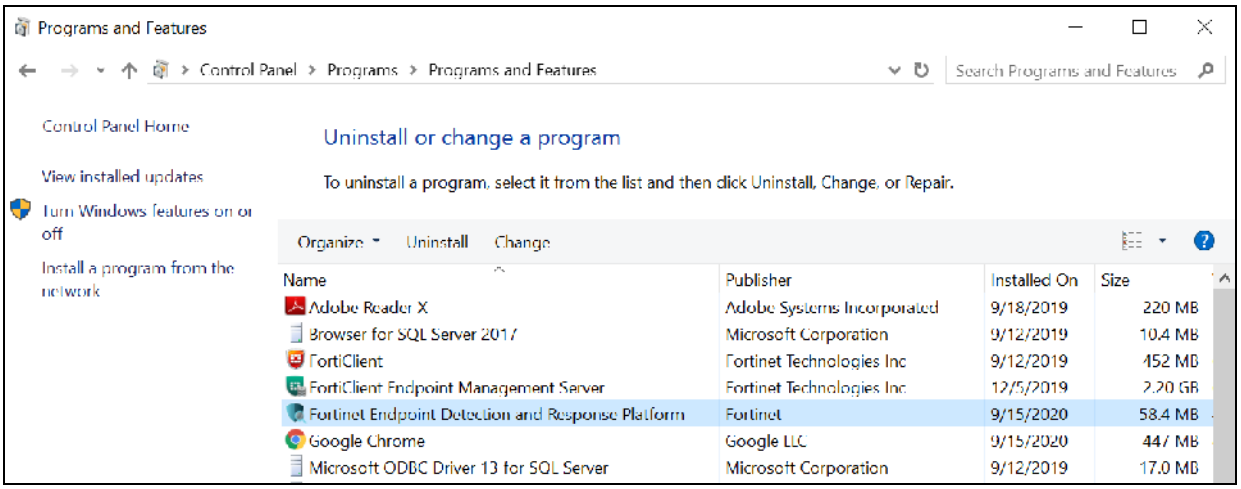
To uninstall the collector

1. On the Browser VM, open the **Control Panel** (**Start** > **Control Panel**), and then click **Uninstall a program**.

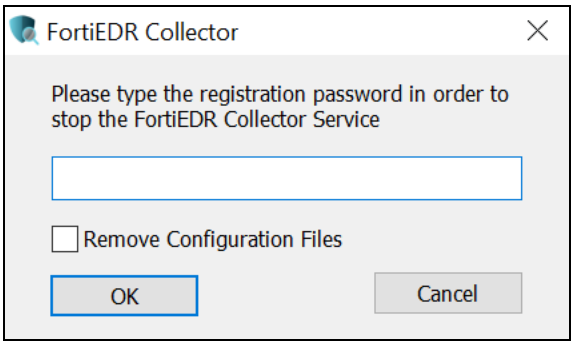


The Windows **Uninstall or change a program** window appears.

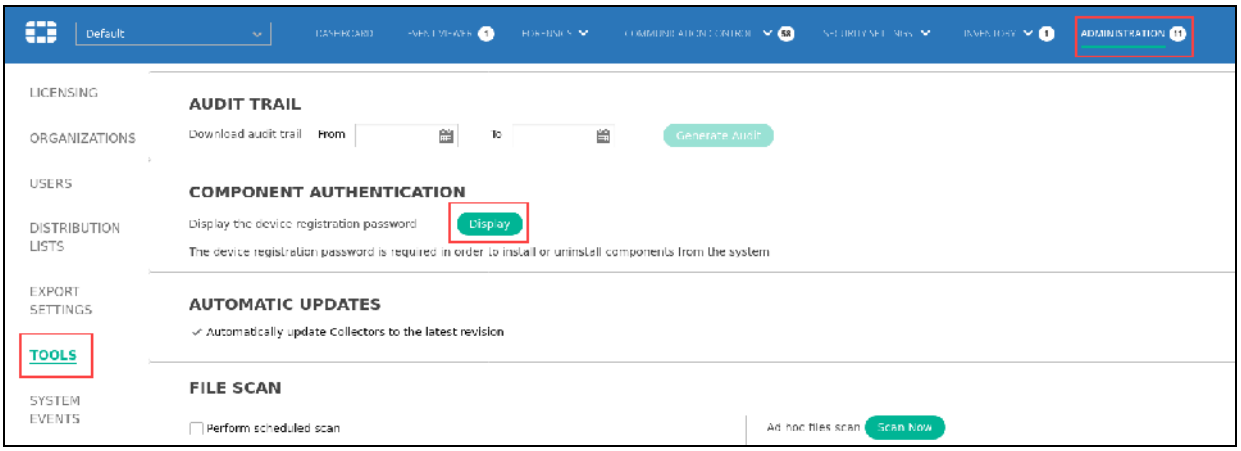
2. Locate and double-click the **Fortinet Endpoint Detection and Response Platform** program.



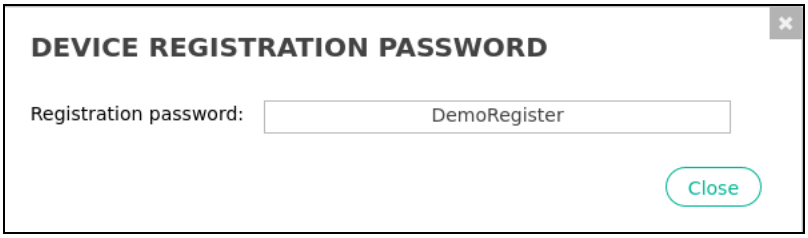
3. In the verification pop-up window, click **Yes**.
4. If a **Windows User Account Control** warning appears, click **Yes** to proceed.
5. When prompted, provide the registration password to stop the FortiEDR collector service.
   You can find this password on the FortiEDR GUI.



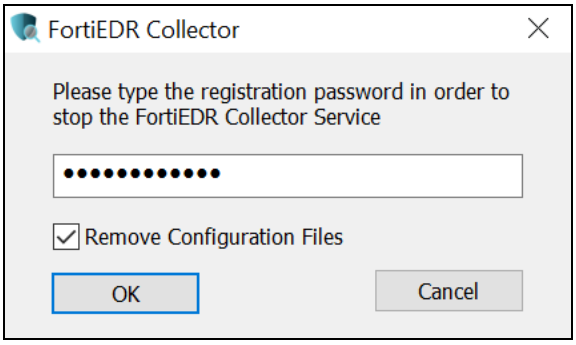
6. On the FortiEDR GUI, click **ADMINISTRATION**, and then in the left panel, select **TOOLS**.
7. Under **COMPONENT AUTHENTICATION**, click **Display**.



8. In the **DEVICE REGISTRATION PASSWORD** window, copy the password.



9. Return to the uninstall window, and then paste the password in the password field.



10. Select the **Remove Configuration Files** checkbox, and then click **OK**.
11. On the Browser VM desktop, open the **Resources** folder.

12. Double-click the `autoinstaller.bat` file to start the installation.
13. Return to the FortiEDR GUI, and then click **INVENTORY**.
    The collector should be restored to a **Running** state.

14. If the collector still appears as **Disconnected**, wait a few minutes, and then refresh the browser.

The `autoinstaller.bat` file runs a silent installation of the `CollectorInstaller64_5.0.2.261.msi` file, with the registration password and aggregator IP.

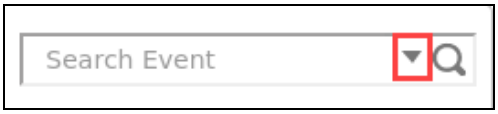
```
msiexec /i CollectorInstaller64_5.0.2.261.msi /qn
AGG=10.160.6.100:8081 PWD=DemoRegister
```

Exercise 2: Troubleshooting the Syslog Watcher Process

In this exercise, you will troubleshoot why a user cannot run Syslog Watcher.

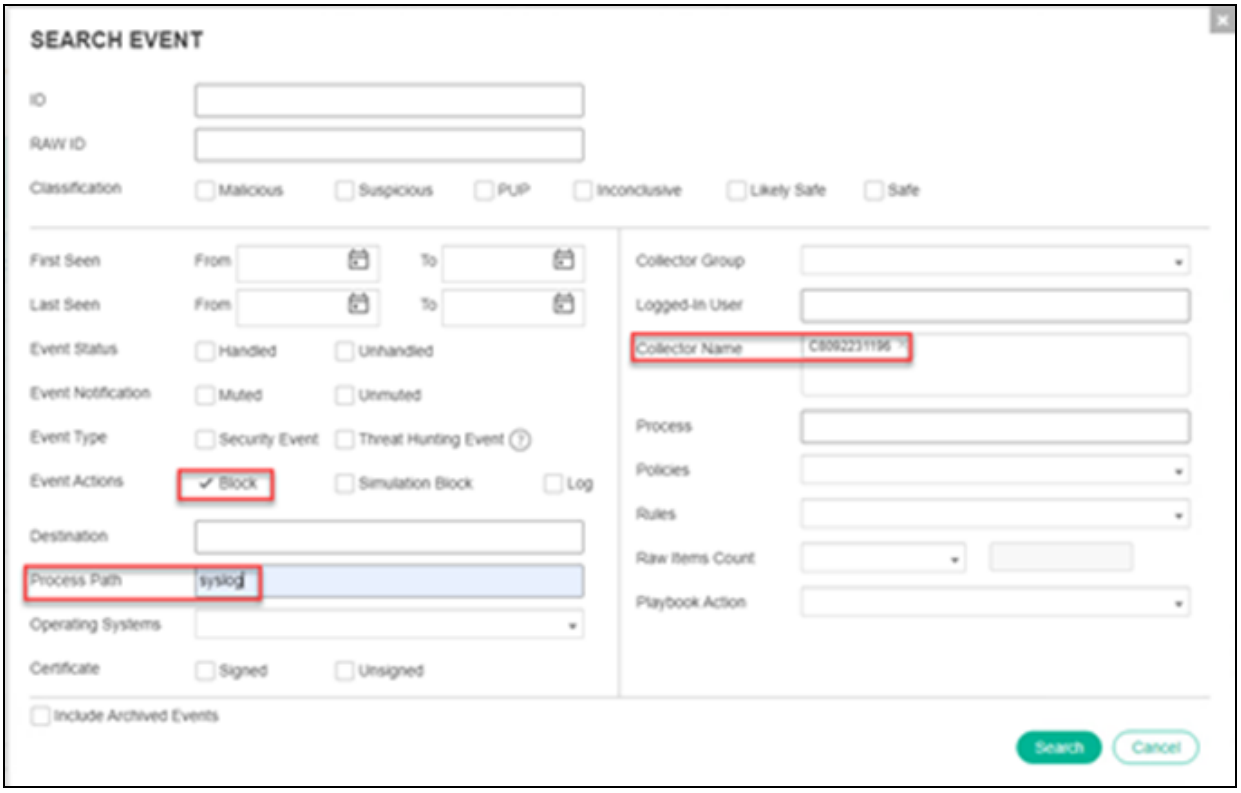
To view the block event on the FortiEDR GUI

1. On the Browser VM, open a browser, and then log in to the FortiEDR GUI with the username `Admin` and password `secureNOT`.
2. Click **EVENT VIEWER**, and then open the **Advanced Search** window.

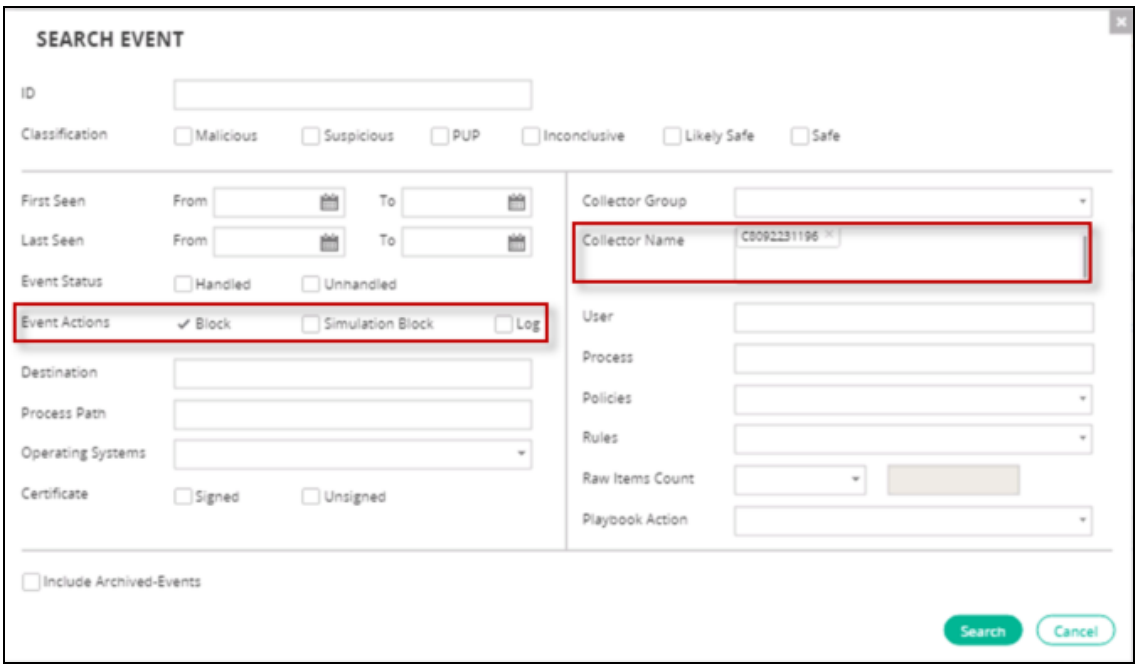


3. In the **SEARCH EVENT** window, use the following details to search for blocking events that involve the user's collector and the Syslog Watcher process:

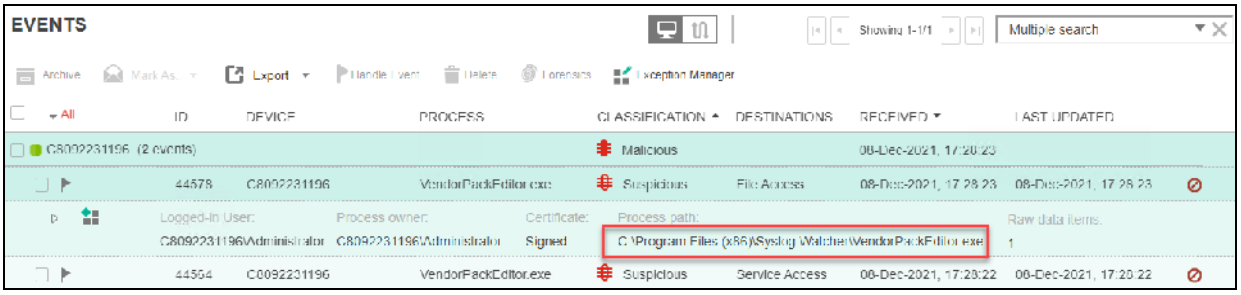
Field	Value
Event Actions	Block
Collector Name	C8092231196
Process Path	syslog



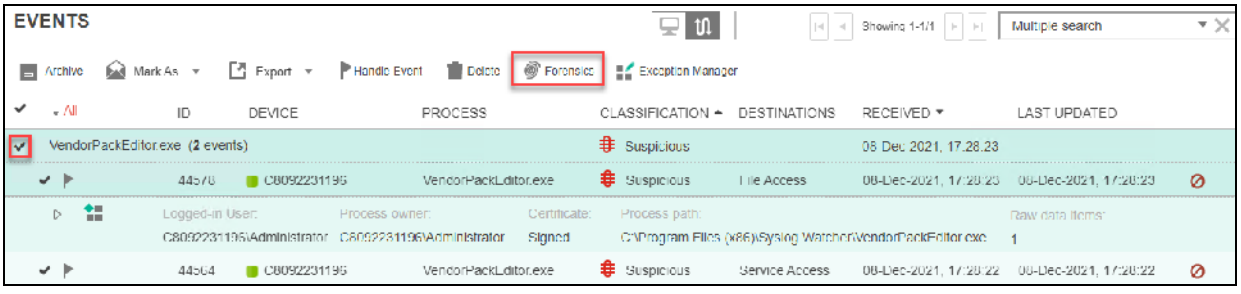
4. Click **Search**.
   If there are no results, clear the search by clicking the **X** in the search bar.
5. Repeat step 3, but leave the **Process Path** field empty, and then click **Search**.



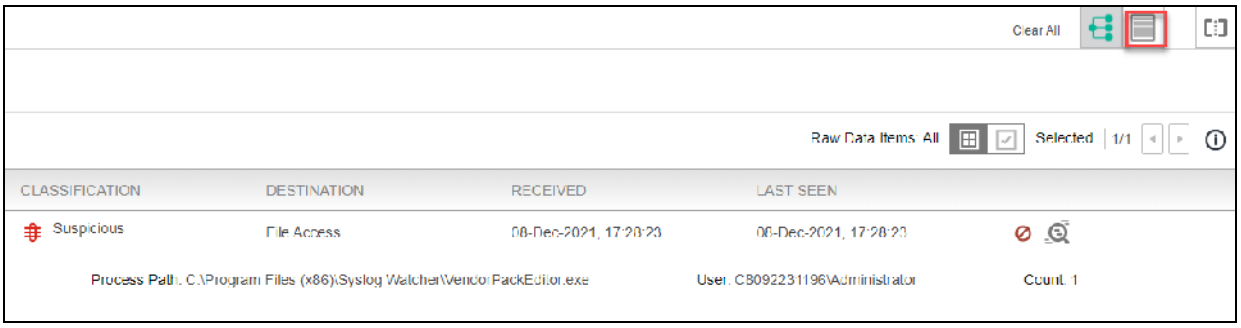
   A list of all blocking events that are associated with the specified collector should appear.
6. In the list, click **VendorPackEditor.exe**, and then look closely at the events.
   You can see that the process is running from the Syslog Watcher folder.



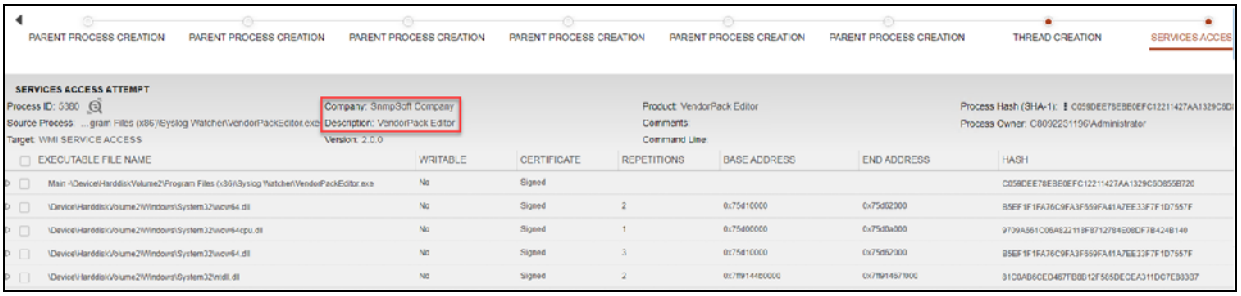
7. Select the alert checkbox to select all of the events, and then click **Forensics**.



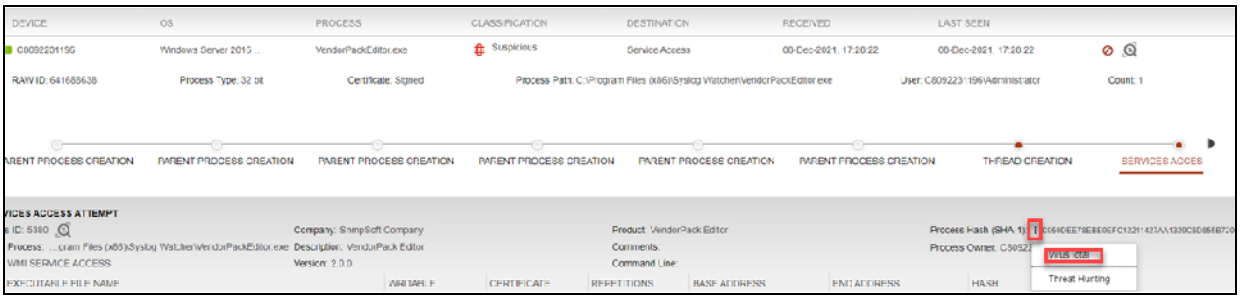
8. In the **Forensics** tab, click the **Stack View** button in the upper-right.



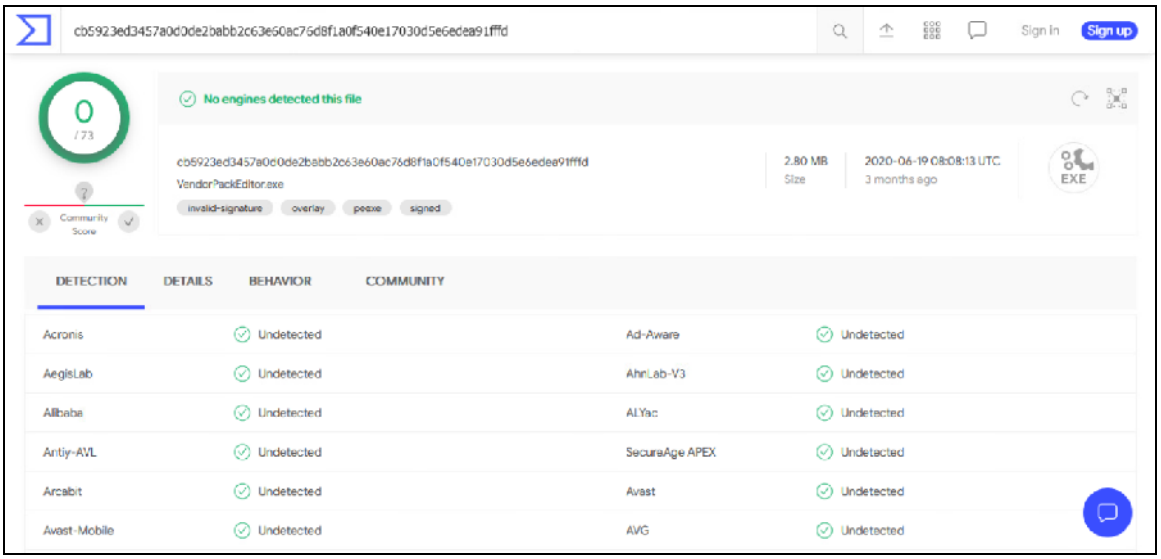
9. For each event, check the processes that violated a rule (marked with a red dot ●), and then check the company name, and if it is not familiar to you, search the internet to find out about its reputation.



10. In the **Stacks View** details pane, click the three vertical dots (⋮) beside each process hash that violated a rule, and then select **VirusTotal**.

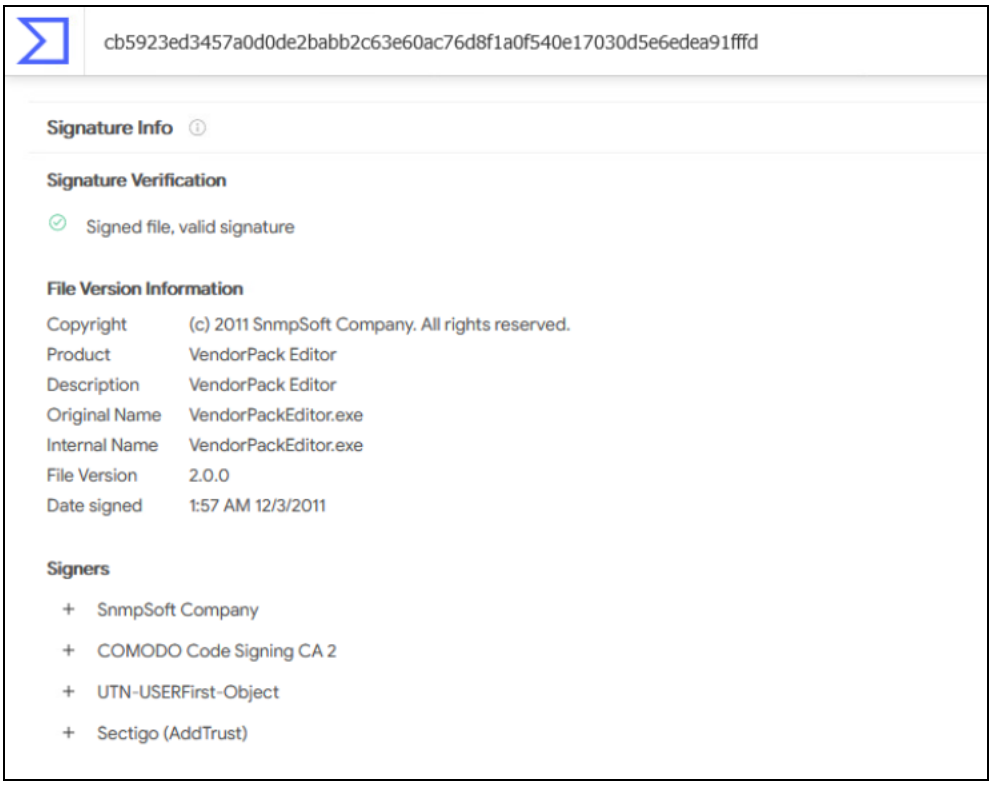


11. Click **VirusTotal** to check the detection rate.



There should not be any red flags.

12. Click the **Details** tab, and then scroll down to check the status of the signature.



There should be a signed and valid signature.

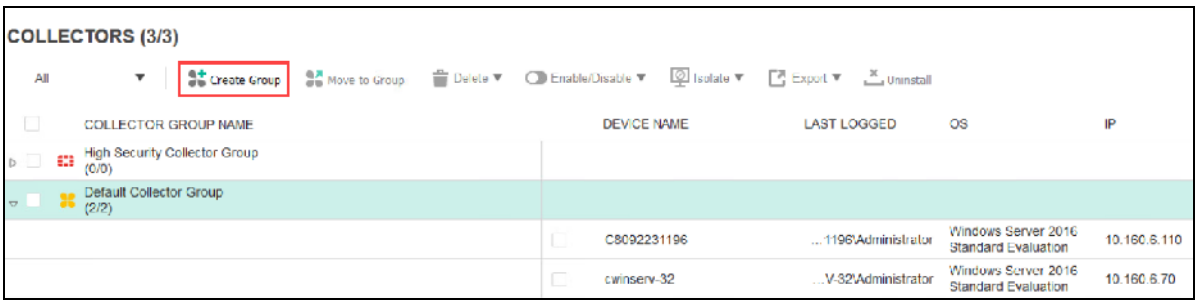
VirusTotal is an external web resource that offers guidance and analysis with almost all anti-malware software in the market. It provides the number of traditional antivirus programs that have identified the file as malicious or undetected. 0/73 means that none of the antivirus programs have identified the file as malware. 67/73 means that 67 antivirus programs have identified the file as malware over 73 different AV software programs.

Create an Exception to Use Syslog Watcher

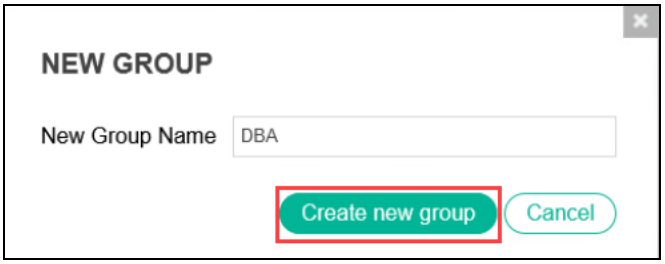
FortiEDR recommends applying exceptions to all groups, but in this case, you have decided that you want only DBA administrators to be able to run Syslog Watcher. To do this, you must create a new collector group, apply group policies to the new group, and create an exception.

To create a new collector group

1. On the FortiEDR GUI, click **INVENTORY**, and then click the **Show all Collectors** link.
2. Click **Create Group**.

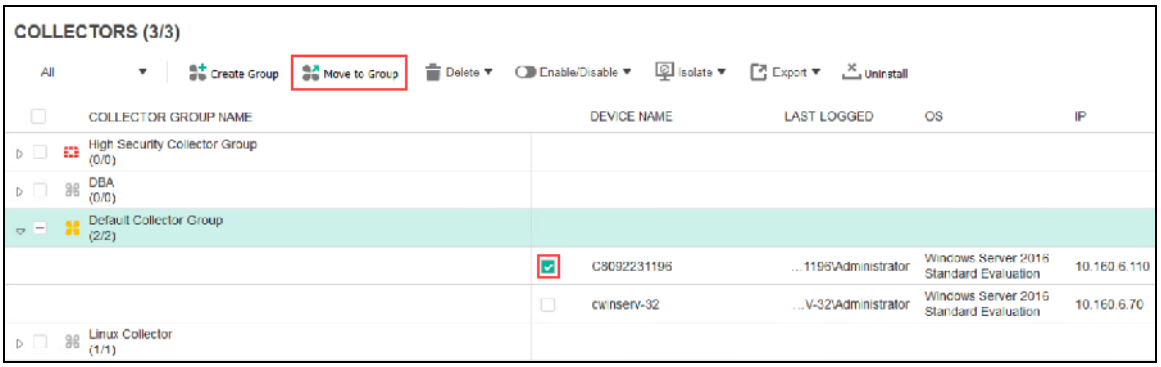


3. In the **New Group Name** field, type `DBA`, and then click **Create new group**.

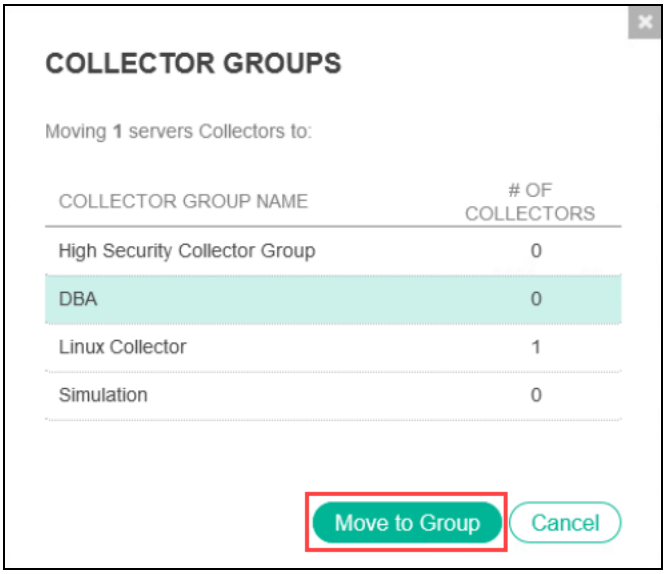


The new group should be in the collector group list.

4. Select the checkbox for collector **C8092231196** on **Default Collector Group**, and then click **Move to Group**.

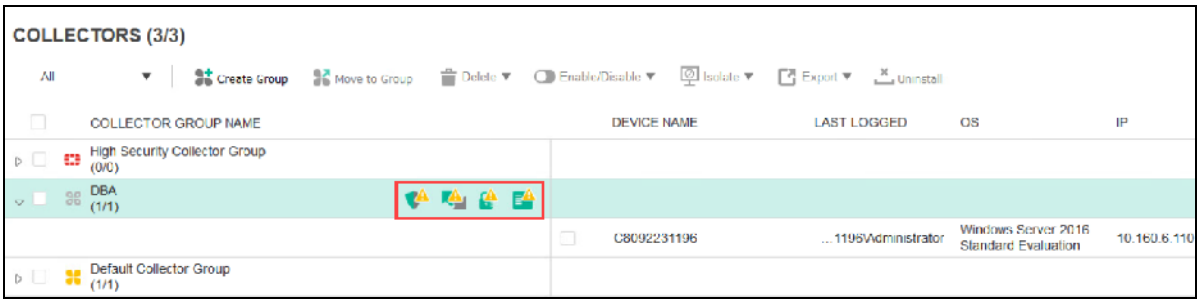


5. Select the new **DBA** group, and then click **Move to Group**.



6. In the confirmation dialog box, click **Move**.
7. After the collector is moved, click **Close**.

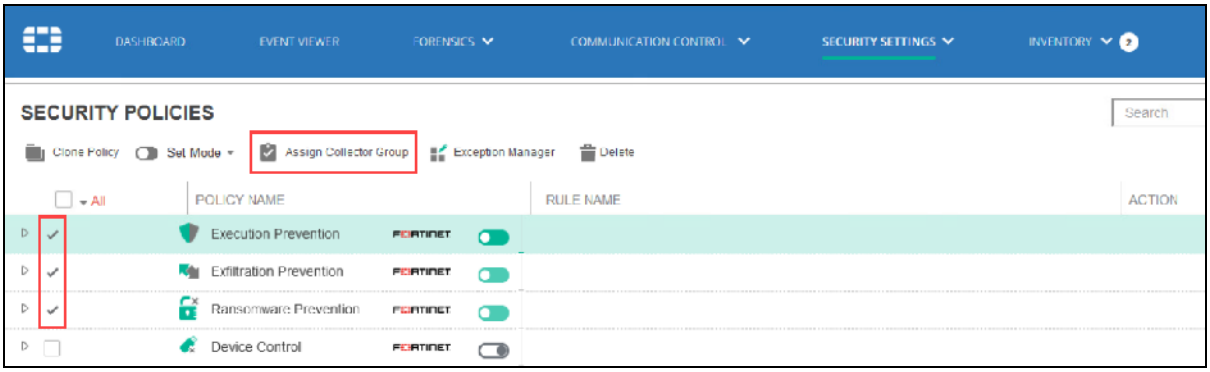
   You can see warning icons indicating that the new collector group has not been assigned to any policies, and is therefore not protected.



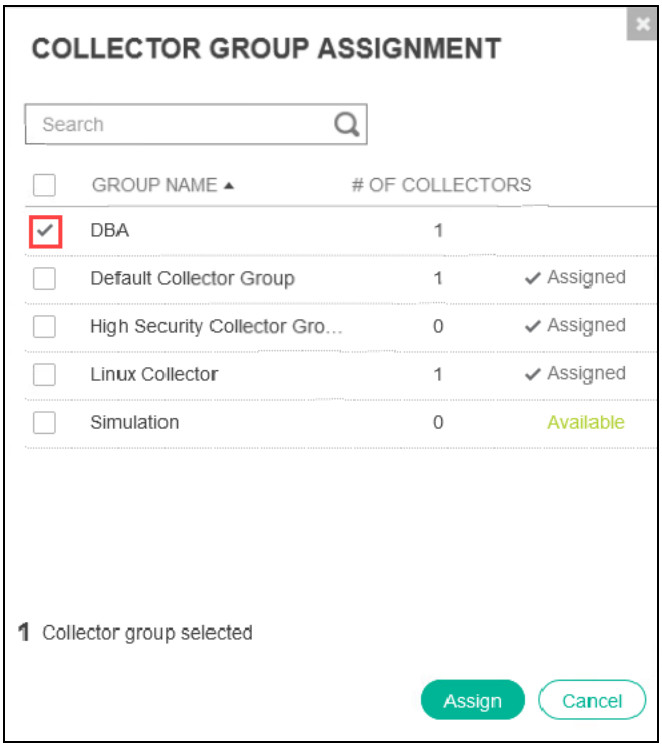
To configure DBA group policies to protect the collector

1. On the FortiEDR GUI, click **SECURITY SETTINGS**.
2. Select the three policies—**Execution Prevention**, **Exfiltration Prevention**, and **Ransomware Prevention**—and then click **Assign Collector Group**.

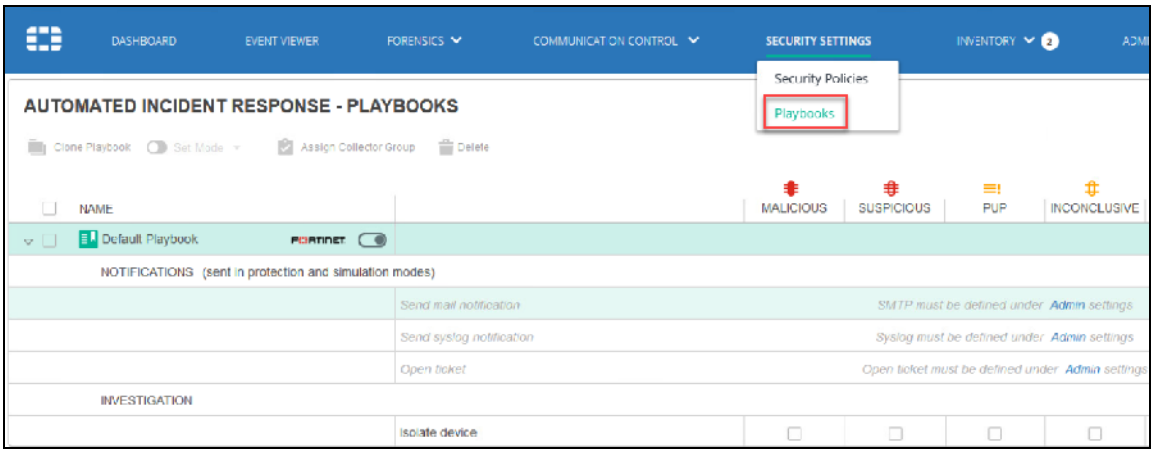
These policies are already in **Prevention Mode**.



3. In the **COLLECTOR GROUP ASSIGNMENT** dialog box, select the checkbox for the **DBA** collector group, and then click **Assign**.

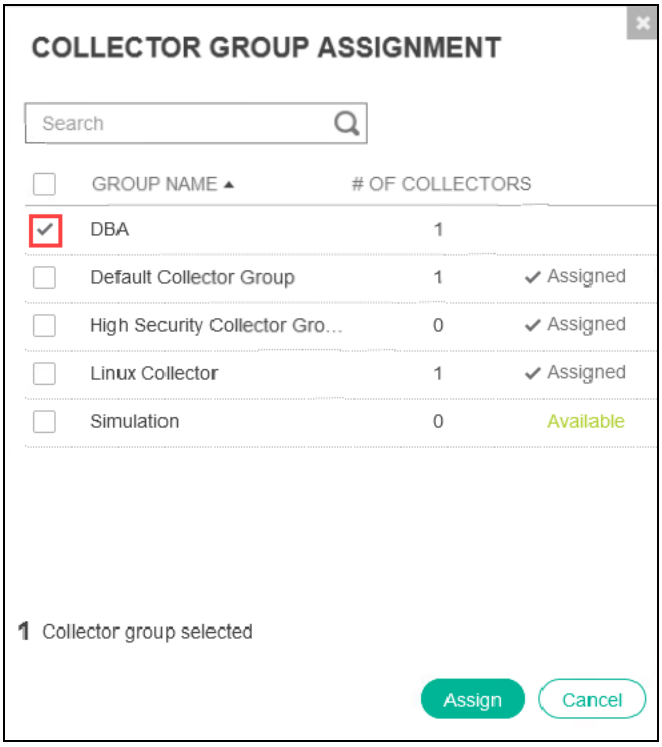


4. When a confirmation dialog box appears, click **OK**.
5. Click **SECURITY SETTINGS**, and then select **Playbooks**.



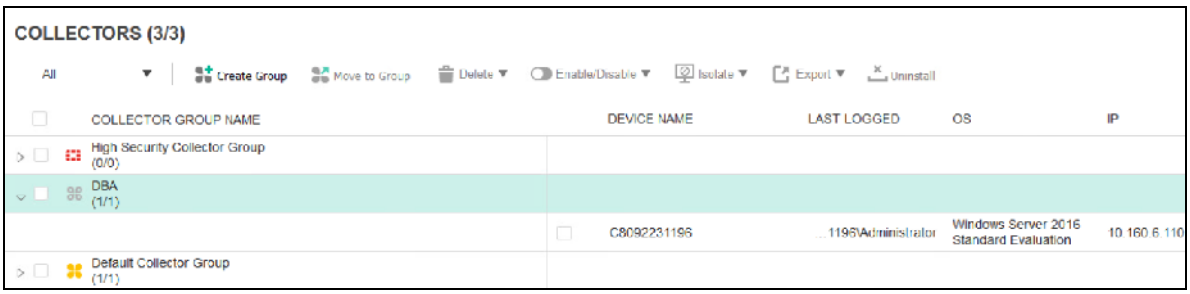
6. Select the **Default Playbook**, and then click **Assign Collector Group**.

7. In the **COLLECTOR GROUP ASSIGNMENT** dialog box, select the **DBA** group, and then click **Assign**.



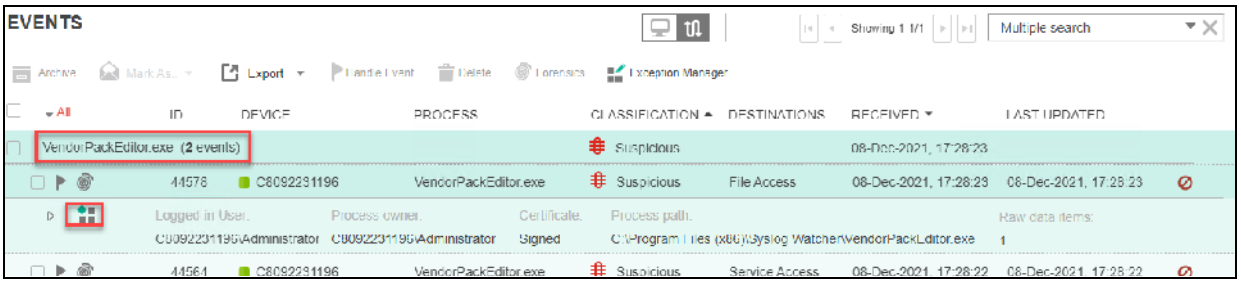
Because playbooks control notifications, it is important to assign each collector group to a playbook, even if the playbook is in simulation mode.

8. In the confirmation dialog box, click **OK**.
9. Click **INVENTORY** to verify that the warning icons no longer appear.

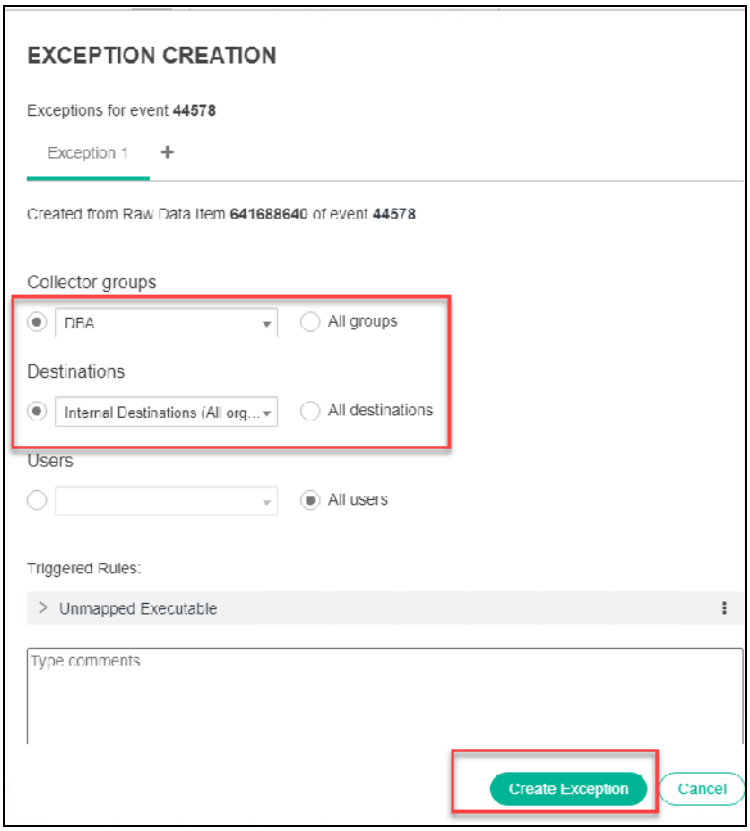


To create an exception

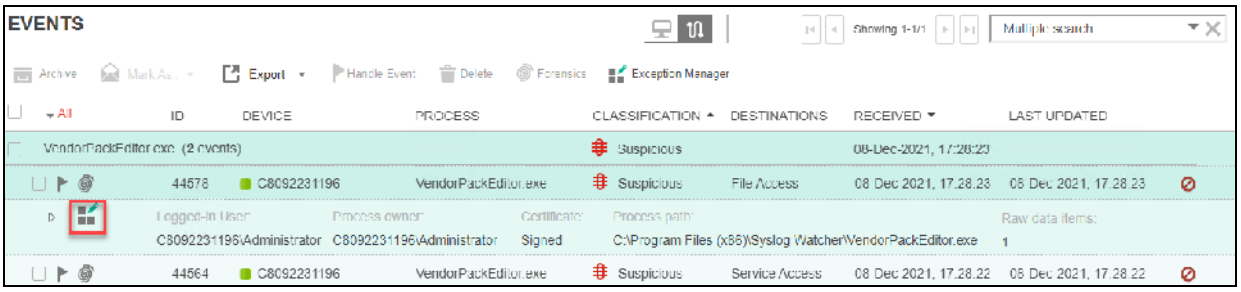
1. On the FortiEDR GUI, click **EVENT VIEWER**.
2. Click the exception icon for the first **VendorPackEditor.exe** event.



3. In the **Collector groups** field, select **DBA** in the drop-down list.
4. In the **Destinations** field, select **Internal Destinations** in the drop-down list.
5. Click **Create Exception** to save the settings.



6. In the **EXCEPTION SAVED SUCCESSFULLY** dialog box, click **Close**.
7. Click the **VendorPackEditor.exe** event to confirm it is covered by the exception.



8. Repeat these steps until all the events for **VendorPackEditor.exe** are covered by an exception.

FORTINET