

Lab: Protecting Endpoints with OpenEDR

Welcome to the Protecting Endpoints with Xcitium OpenEDR lab!

Introduction

Xcitium OpenEDR is a free, open-source endpoint protection and response (EDR) system that follows a client-server model. A centrally managed server hosts a security program, and an accompanying client program runs on each endpoint. The client sends information to the server, the server administrator uses a server EDR program to analyze this information, and defends endpoints from malware and additional threats.

In this lab, you will learn to manage and protect endpoints using Xcitium OpenEDR, manage endpoints and explore cloud manager.

Before you begin

This lab requires the download and installation of no-cost software. Before your begin this lab you need to be logged in as the administrator, or have administrative rights, to install the required software.

Objectives

After completing this lab, you will be able to:

- Set up the Xcitium Cloud Manager
- Add an endpoint device to the OpenEDR system
- Locate endpoint data in the Xcitium Cloud Manager

- Manage endpoint patches from the Xcitium Cloud Manager
- Scan an endpoint for malware and find the results in the Xcitium Cloud Manager

Let's begin!

Prerequisites

For this lab, you need to have

- A smartphone with an authenticator application installed. The common authenticator applications include:
 - Google Authenticator
 - Microsoft Authenticator
 - LastPass Authenticator
 - 2FAS
- One or more devices to use as endpoints. You can use internet-enabled computers, tablets, or smartphones with one of the following operating systems installed:
 - Windows
 - macOS
 - Linux
 - iOS
 - Android

You can set up endpoint protection on the same device you're using to explore the cloud manager.

Task 1: Set up open source version of Xcitium Cloud Manager

1. Open your browser and enter <https://openedr.com/>.
2. Select **Get Started for Free**.

onedr.com
to go forward, hold to see history

 [What is EDR?](#) [Join Community](#) [Get Certified on OpenEDR](#) [For MSP](#) [For MSSP](#)

OPENEDR

What is Open Source Endpoint Detection and Response (EDR)?

OpenEDR is an open source endpoint detection and response platform that provides analytic detection with Mitre ATT&CK visibility for event correlation and root cause analysis of adversarial cyber threat activity and behaviors in real time. This endpoint telemetry platform is a continuous monitoring solution available to all cybersecurity professionals, and every sized organization, to use for defending their organization or business against threat actors and cyber criminals.


[Get Started for Free](#)



1. Enter your information to create a free account.

Create Free Account

- ✓ OpenEDR – An Open Source Endpoint Detection and Response Platform, **Free** EDR!
- ✓ Enables Continuous and Comprehensive Endpoint Monitoring
- ✓ Defends Your Organization Against Threat Actors and Cyber Criminals
- ✓ Detects and Remediate Threats to Improve Your Security Posture
- ✓ Provides Visibility of Both Physical and Virtualized Environments
- ✓ Generates Actionable Alerts with Easy to Manage Reporting

 OPENEDR
provided by xcitem

The field is required

[CREATE FREE ACCOUNT](#)

By clicking **"CREATE FREE ACCOUNT"**, you agree to our [Terms and Conditions](#), [EULA](#) and [Privacy Notice](#)

[Already Have an Account? Sign In](#)



OPENEDR
Provided by XCITIUM

2FA Account Protection Enabled

If you lose access to your authentication device, you'll need one these backup codes to login to your account. Make a copy of these codes, and store it somewhere safe offline or secured digitally.

Each backup code may be used only once.

[Download backup codes as txt file](#)



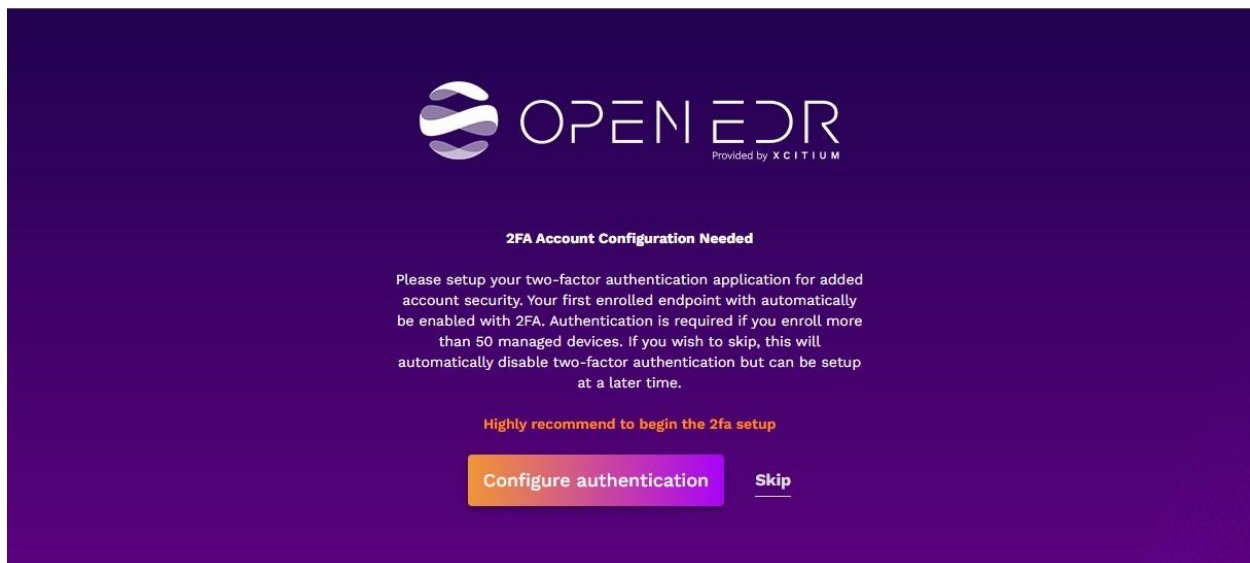
OPENEDR
Provided by XCITIUM

Set Secret Questions

Setting up secret questions will enhance your account security, and will be needed in case you forget your password, or when you need to reset Two Factor Authentication method.

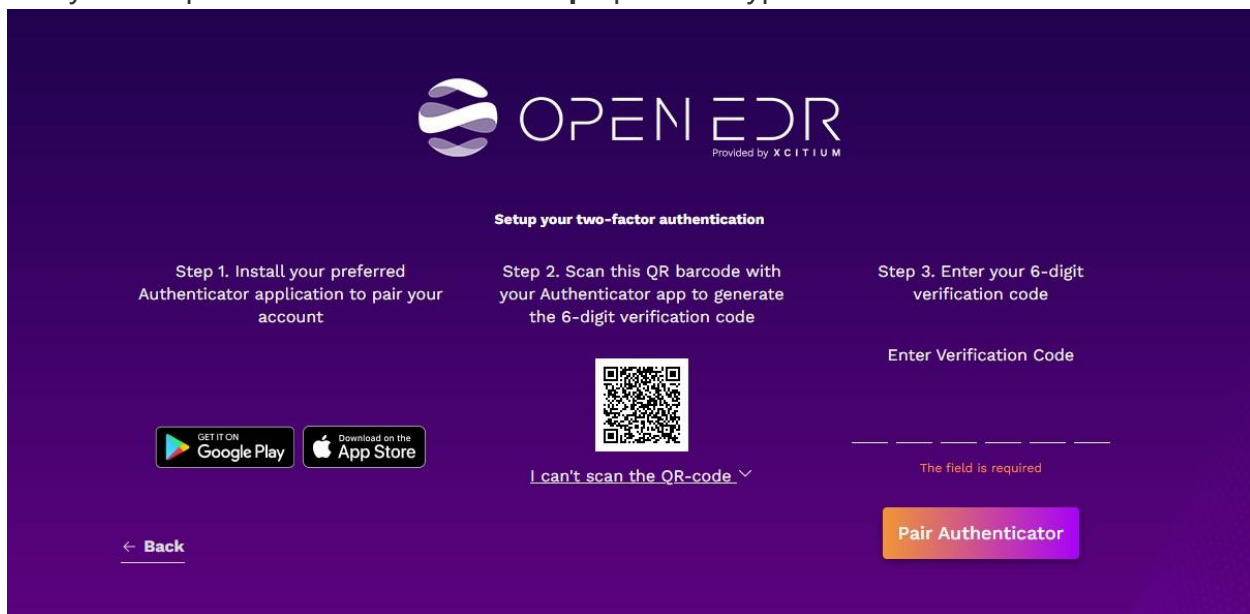
* Answer 1

1. After creating your account, Xcitium will prompt you to set up multifactor authentication (MFA) using the authenticator app on your mobile device. If you don't have an authenticator app, you can download one from Google Play or the Apple Store.

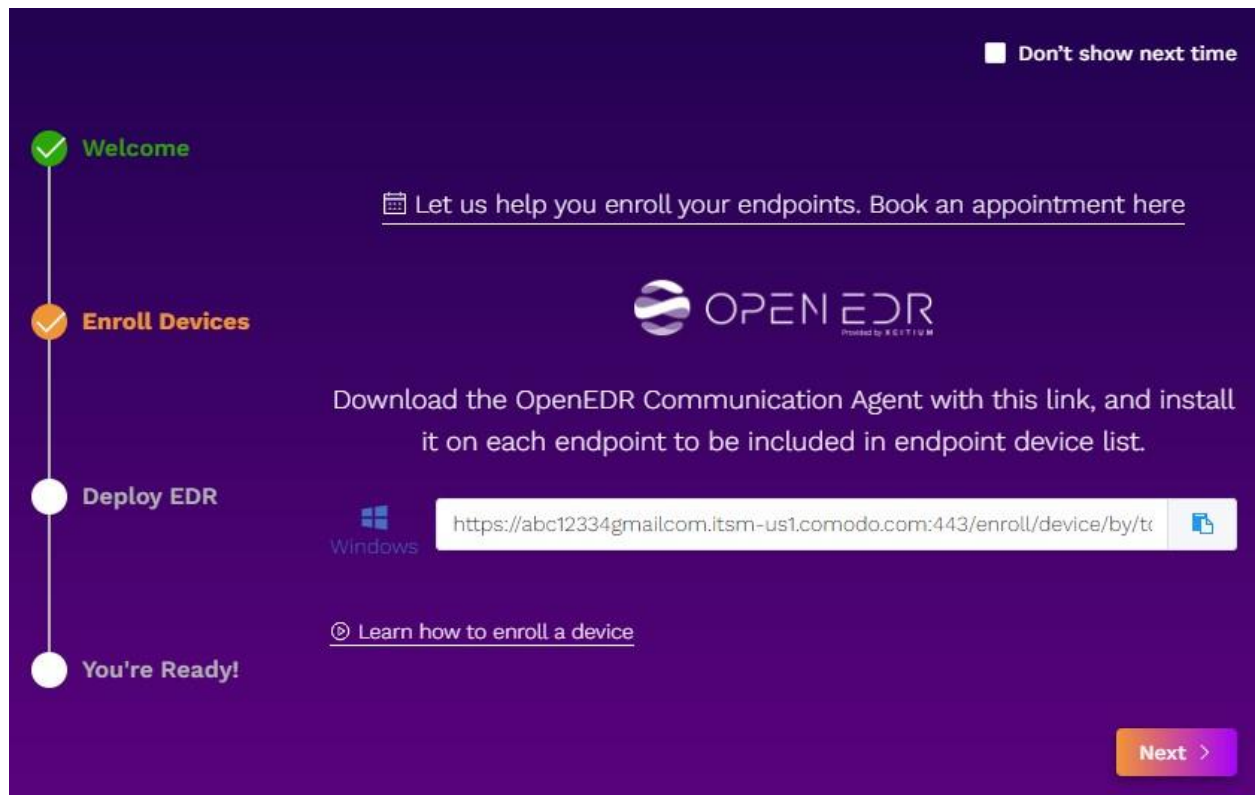


1. Use the authenticator app to scan the onscreen QR barcode to generate a six-digit verification code. Type or enter this code in the **Enter Verification Code** field on your browser window, and then select **Pair Authenticator**.

Note: You might see an optional, **Set Secret Questions** window. This lab does not require that you complete this task. Select the **Skip** option to bypass this task.



1. The **Welcome** screen opens. Select **Next**.



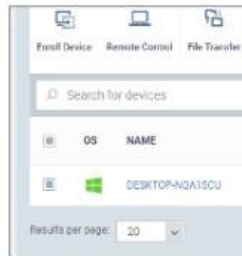
1. On the **Enroll Devices** screen, select **Finish**.



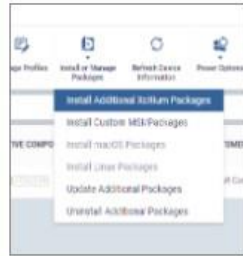
Now, let's install the OpenEDR Agent and connect to the OpenEDR Portal.



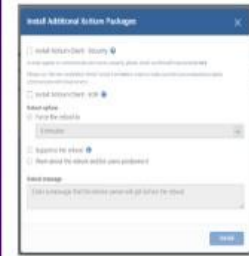
1. CheckAll or specific devices you wish to enroll



2. Click **Install or Manage Packages**
- Click **Install Additional Xcitium Packages**



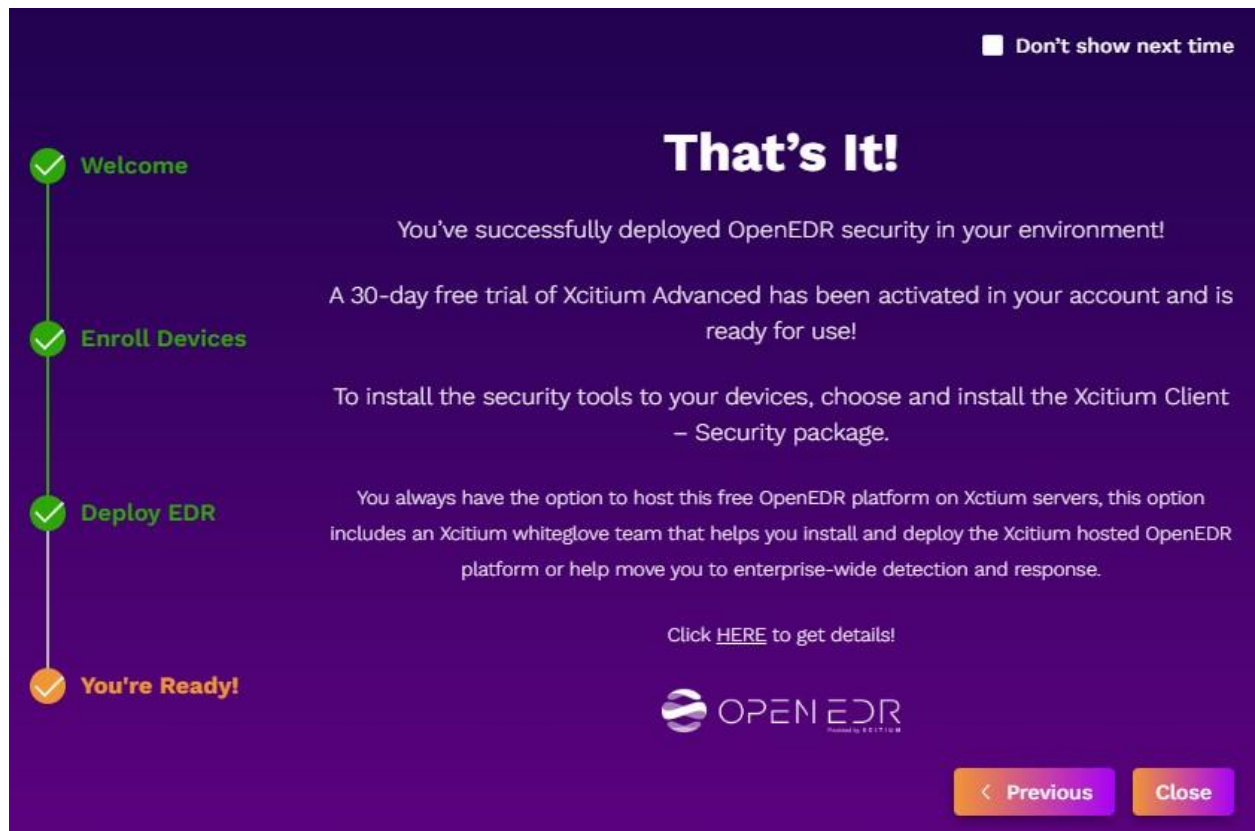
3.
 - Check **Install Xcitium Client-EDR**
 - Click **Install**



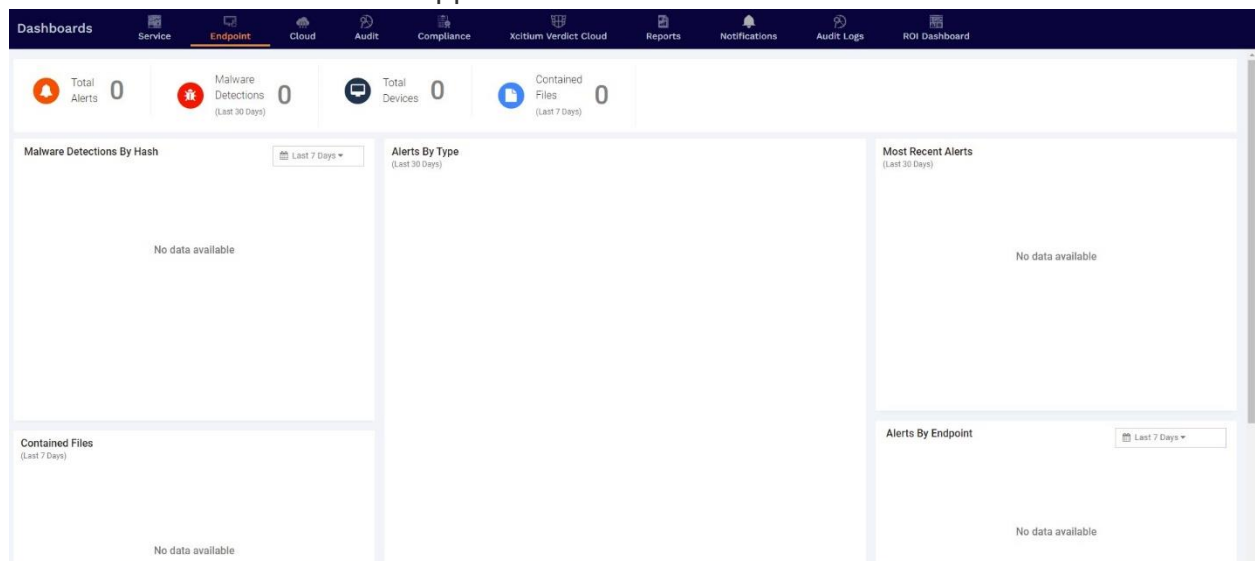
📺 Learn how to deploy EDR to your device

Finish

1. Next, select **Close** on the **That's It!** page.

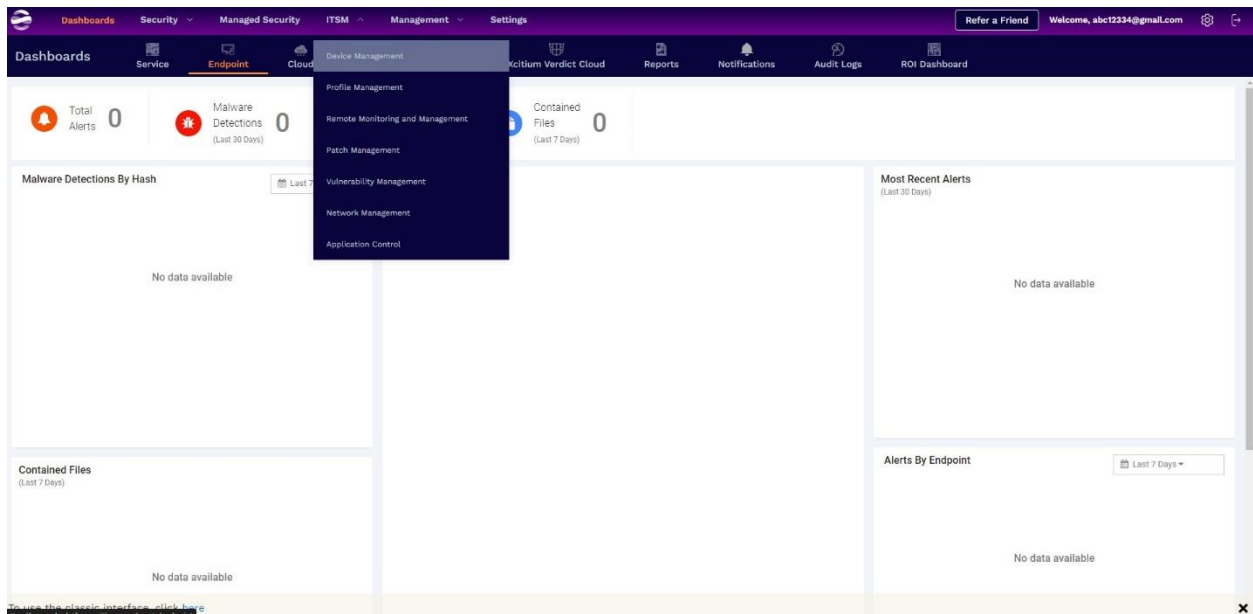


1. The **Dashboard** screen appears.

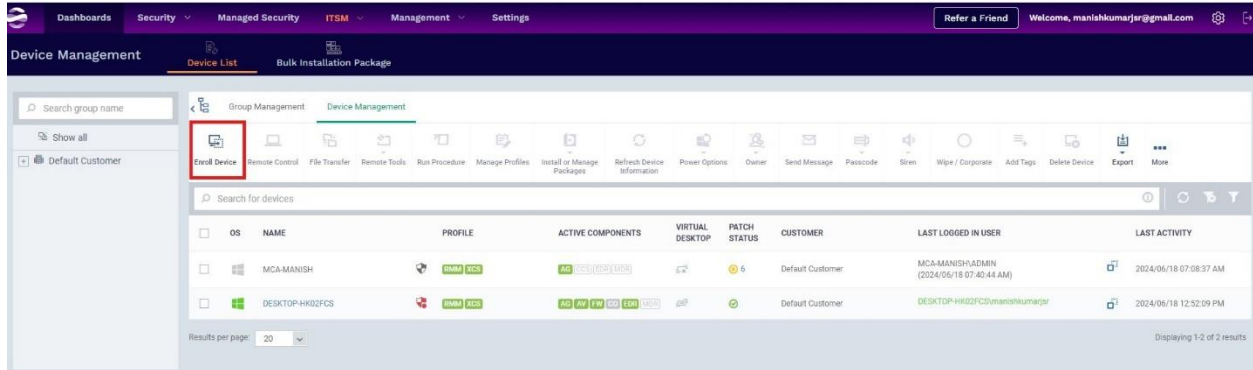


Task 2: Add an endpoint device to the OpenEDR system

Now you've set up the OpenEDR Cloud Manager. In this task, you'll add endpoints to the Cloud Manager.

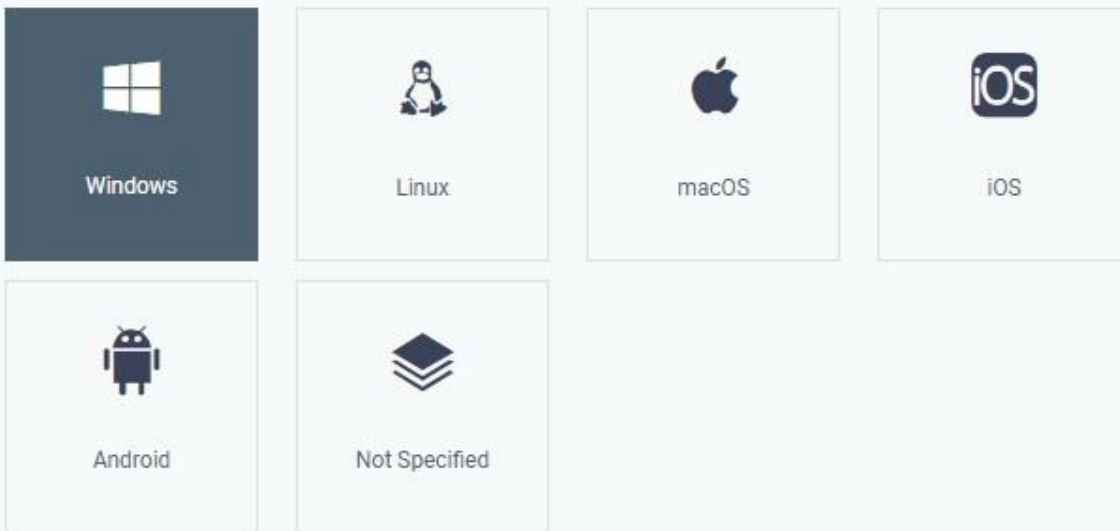


1. On the **ITSM** menu, select **Device Management** to open the **Enrollment Wizard** page. Next, select **Enroll Device**.



1. Select the operating system for your device.

Select Operating System of The Device



1. From the **Select Enrollment Type** list, select **Enroll and Protect**.

Select Enrollment Type

Notice, Enroll and Protect require device reboot and Enroll doesn't require.



Choose platform

Windows x64



1. Now, select your preferences from the **Set Reboot Options** list.

Set Reboot Options

Reboot options

☒ Force the reboot in

5 minutes

☐ Suppress the reboot ⓘ

☐ Warn about the reboot and let users postpone it

Reboot message

Your device will reboot in 5 minutes because it's required by your administrator

1. Keep the default values unchanged, scroll to the end of the page and select **Next**.

Device Name Options

Change the Device Name if you need to see it on a different name in the Device List. In case a device group is enrolled, devices will have the same Device Name. You always can restore an original device name in the way: Devices - Device List - [Device] - Device Name - Edit.

☒ Do Not Change

☐ Change

New Device Name...

Next

1. Enter the enrollment link into your browser's address bar or access the link on the device.

Enrollment Wizard

✓ Enrollment Options

2 Installation Instructions

Enrollment Link

To complete the user device enrollment, copy and send this link to user.


https://kutt.comodo.com/pVBMgz


Use a full link if needed:

https://manishkumarjsrgmailcom.itsm-us1.comodo.com/enroll/device/by/token/3e080e441f5fi

Send

What's next?

 Enroll Another Device

 Go to Bulk Installation Package

Back

Finish

1. Select **Finish**.
2. The Open EDR Cloud Manager is now active on your device. Next, install the client program, or agent, on the device.
3. Open the enrollment link to get the **Enrollment Wizard**.
4. Follow the installment instructions on the Enrollment Wizard page. Depending on your device, you will be prompted to download either an installer or an app.

Note: The agent name will vary depending on the device.

1. Now open the installer and restart your device to finish the agent setup process.

Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installer

Download Windows Installer

Installation Instruction



Step 1

Run installer of Communication Client after download complete. After that, your device will be enrolled and appears in Device List



Step 2

After Communication Client is installed, Security Client will be installed on your device automatically



Step 3

Your device will be **rebooted** after installation of Security Client is completed

For linux:

Welcome to Enrollment Wizard

In order to complete the connection of your device, follow the instruction below

Installer

Download Linux Installer

Installation Instruction

Step 1
Change installer mode to executable:
`$ chmod +x ($Installation files$)`

Step 2
Run installer with root privileges:
`$ sudo ./($Installation files$)`

Step 3
Security Client will be installed on your device

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
(windows@windows)-[~/Downloads]
$ chmod +x itsm_13LSSnf3_ccsl_installer.run
```

```
(windows@windows)-[~/Downloads]
$
```

```
(windows@windows)-[~/Downloads]
$ sudo ./itsm_13LSSnf3_ccsl_installer.run
[sudo] password for windows:
Creating directory /tmp/installer_1747160873/agent
Verifying archive integrity... All good.
Uncompressing Linux ITSM Agent/10.1.50439.25030 100%
systemd system
https://mdmsupport.comodo.com/enroll/resolve/token/13LSSnf3
INI = [General]
host=sohaibrafiqloundgmailcom.itsm-us1.comodo.com
port=443
token=603cf775606341c22adb5c579ff31195
suite=4
remove_third_party=0
PORT = 443
HOST = sohaibrafiqloundgmailcom.itsm-us1.comodo.com
MDM = 603cf775606341c22adb5c579ff31195
https://sohaibrafiqloundgmailcom.itsm-us1.comodo.com:443/enroll/linux/index/token/603cf775606341c22adb5c579ff31195
Created symlink '/etc/systemd/system/multi-user.target.wants/itsm.service' -> '/etc/systemd/system/itsm.service'.
before install ces ls
ITSM
Note, selecting 'ccs-linux' instead of '/tmp/installer_1747160873/linux-security.deb'
The following packages were automatically installed and are no longer required:
libbfg1 libglapi-mesa libglynd-core-dev openjdk-23-jre python3-ntlm-auth
```

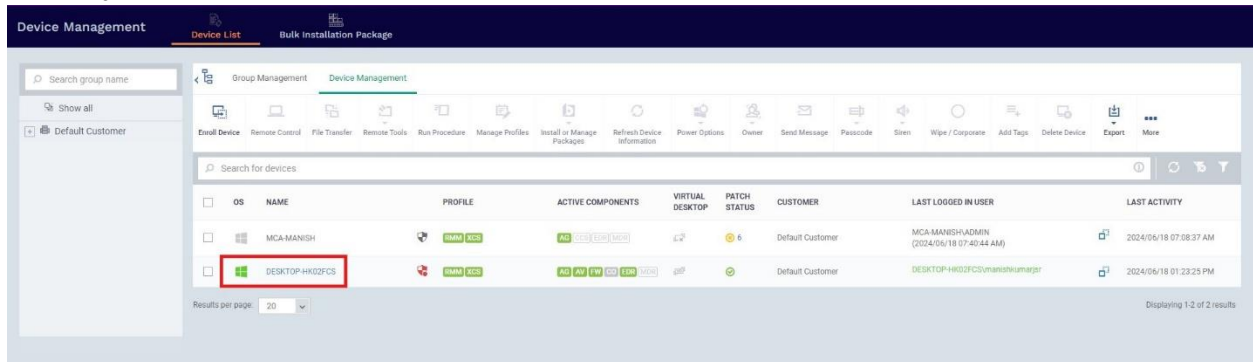
1. After completion of the agent installation, you will verify that the agent can communicate with the Cloud Manager.
2. Visit <https://openedr.com/> and log into the OpenEDR Cloud Manager. Select **Get Started**.

The screenshot shows the OpenEDR Cloud Manager interface. The top navigation bar includes 'Dashboards', 'Security', 'Managed Security', 'ITSM', 'Management', and 'Settings'. The 'Device Management' section is active, showing a 'Device List' tab. The main content area displays a table of devices with the following columns: OS, NAME, PROFILE, ACTIVE COMPONENTS, VIRTUAL DESKTOP, PATCH STATUS, CUSTOMER, LAST LOGGED IN USER, and LAST ACTIVITY. Two devices are listed:

OS	NAME	PROFILE	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LAST LOGGED IN USER	LAST ACTIVITY
Windows	MCA-MANISH	MANISH	MSI, MSN, MSN	Yes	6	Default Customer	MCA-MANISH-ADMIN (2024/05/18 07:40:44 AM)	2024/05/18 07:08:37 AM
Windows	DESKTOP-HK02FCS	MANISH	MSI, MSN, MSN	Yes	6	Default Customer	DESKTOP-HK02FCS\manishkumarj	2024/05/18 01:19:24 PM

Results per page: 20. Displaying 1-2 of 2 results.

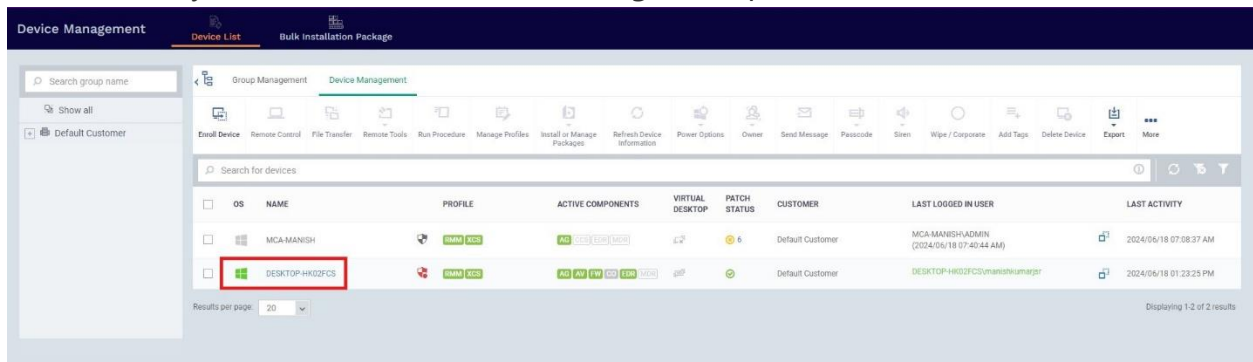
1. Select **ITSM** and then **Device Management** to view the connected devices. Check for your listed device.



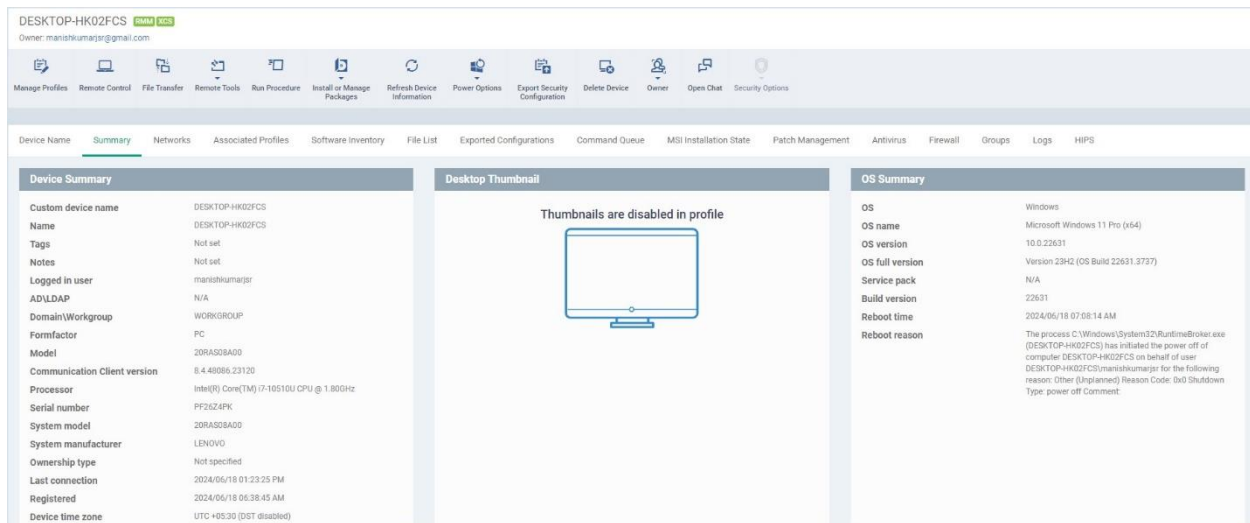
Task 3: Locate endpoint data in the Cloud Manager

Now that agent and the cloud manager are communicating well, let's look at the steps to analyze the data collected by the Cloud manager to manage endpoint protection.

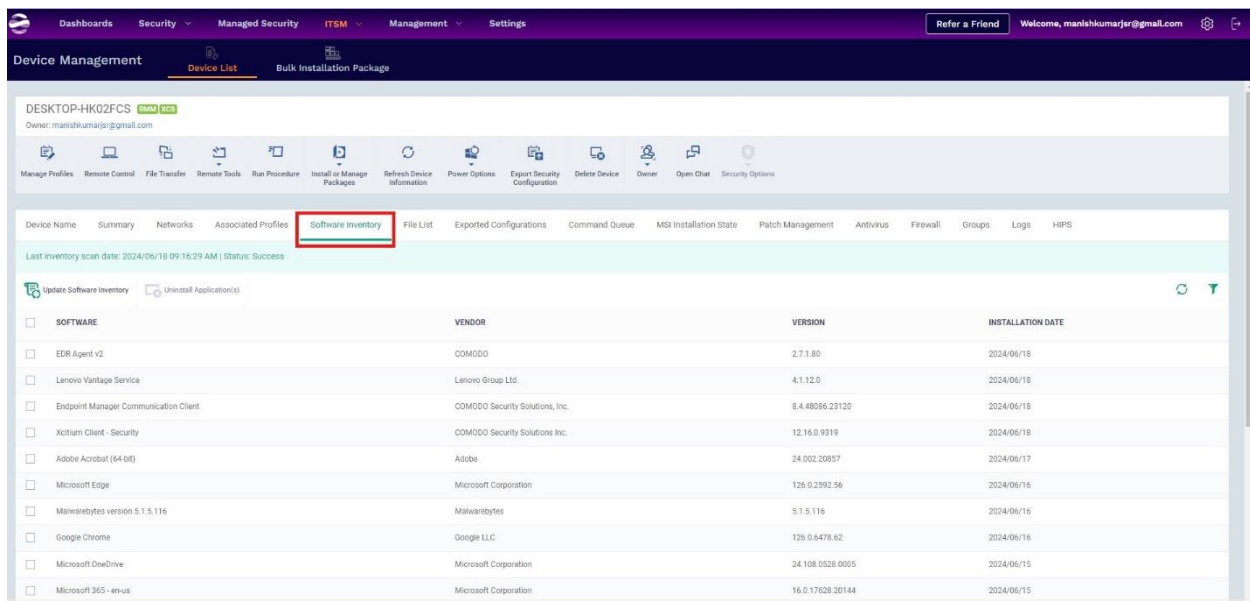
1. Select your device on the **Device Management** pane.



1. Review the detailed information on the **Summary** page for device's hardware, operating system, security software, and performance metrics, including CPU, RAM, and network usage.

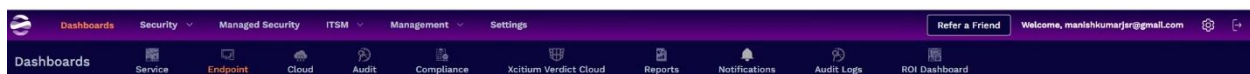


1. Navigate to the **Software Inventory** tab to access a detailed list of all applications installed on the device.

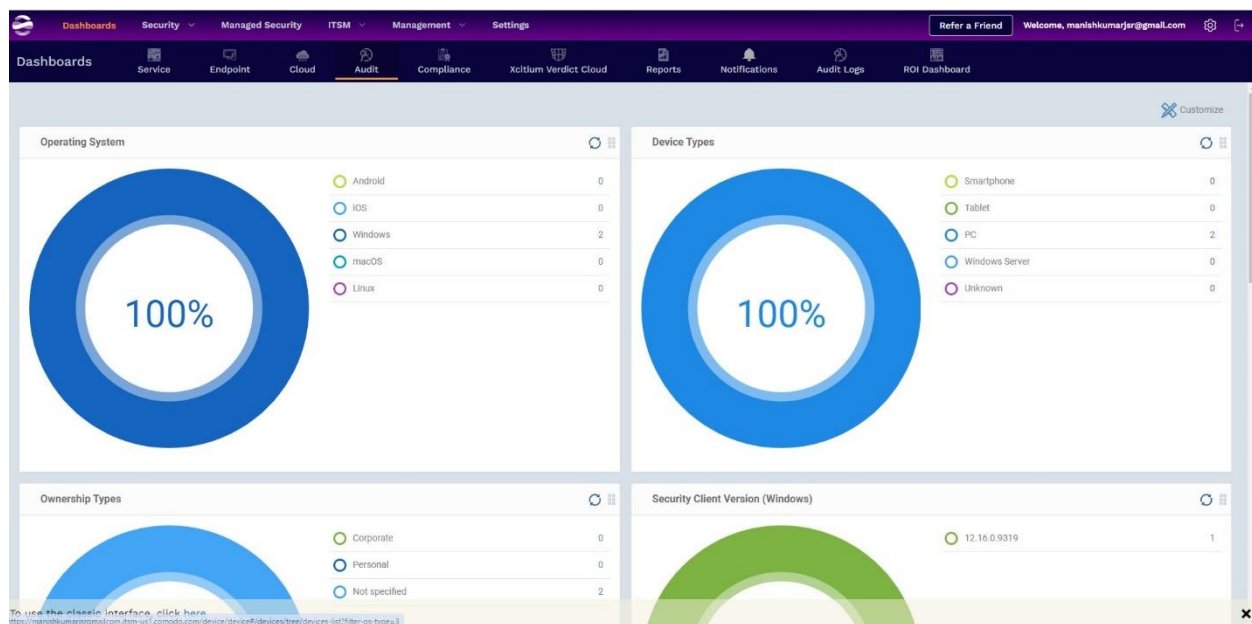


1. Navigate away from the **Device List** to explore additional information captured from endpoints. Explore the **Audit** pane.

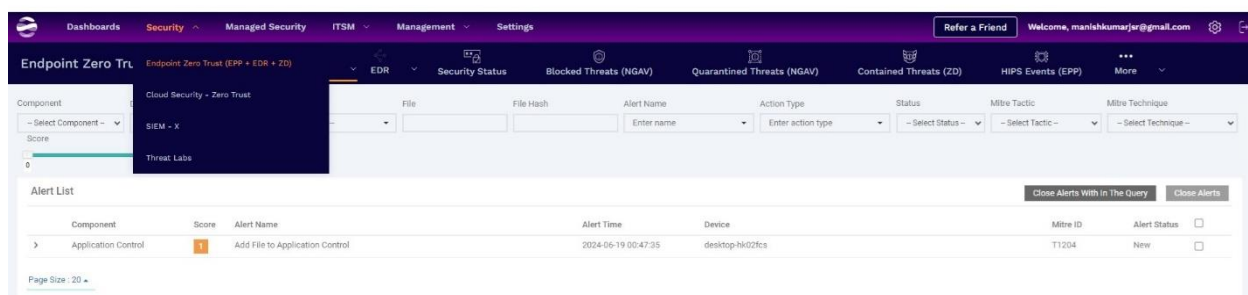
- Select the **Dashboard** tab.



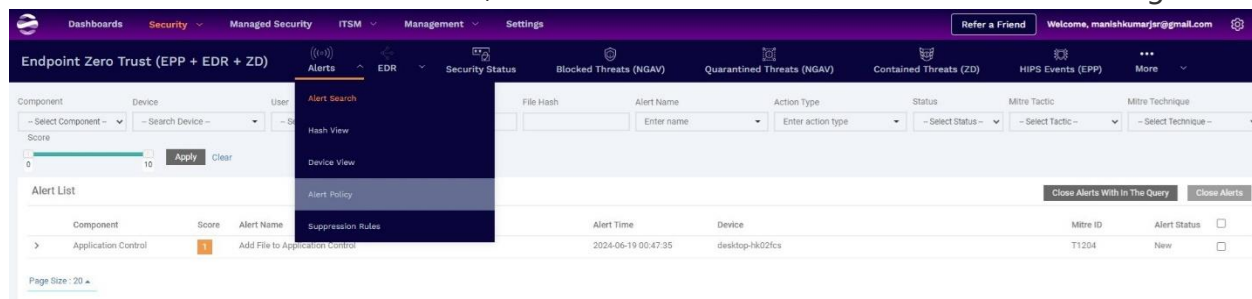
- Select the **Audit** tab to get an overview of the endpoints managed by OpenEDR.



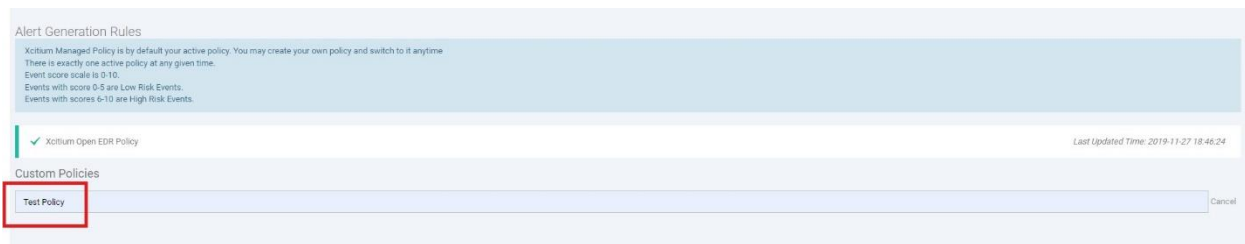
1. Select **Security** tab to view endpoint threat alerts. Next, select **Endpoint Zero Trust (EPP + EDR + ZD)** from the drop-down list.



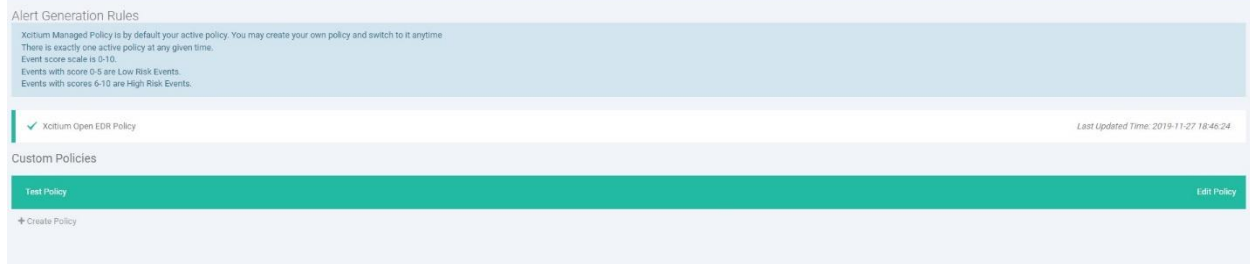
The **Endpoint Security** pane displays all EDR alerts based on severity levels. Events with a score from 0 to 5 are at the low risk, and those with a score from 6 to 10 are at the high risk.



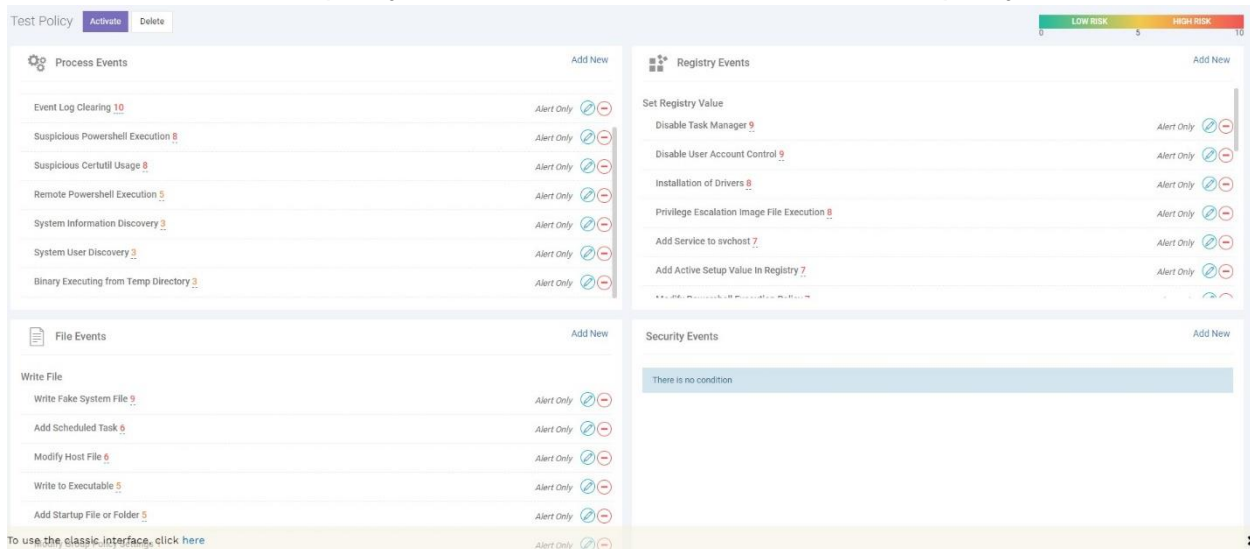
1. Next, establish new rules for monitoring potentially harmful executable downloads into the user's devices. For this, you should create a custom policy. Return to the **Alert Policy** page and select **Create Policy** to begin.



1. Type **Test Policy** in the **Custom Policies** field, and press **Enter** in your keyboard.



1. Click on custom policy named **Test Policy**, to view the various policy details.



Note: Your custom policy begins with the same rules as the Xcitium Predefined Policy. However, you have the option to add, edit, or delete rules based on custom policies.

1. For this lab, let's retain Xcitium's default rules. Select **Delete**.
2. Next, select **Yes, delete it** to confirm.



You are about to delete this policy permanently. Are you sure?

Yes, delete it!

Cancel

Task 4: Manage endpoint patches from the cloud manager

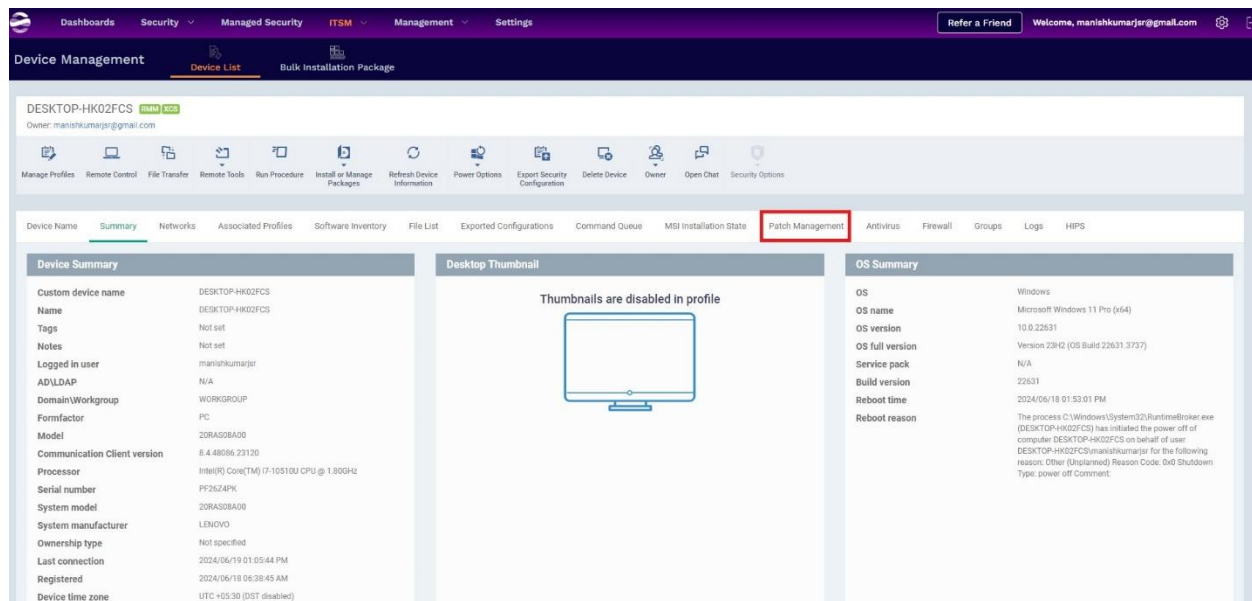
Patch management stands as a critical measure for organizations to prevent malicious attacks and ensure that each endpoint has their patches consistently updated. Let's explore how to manage patches on your endpoint devices.

1. Navigate to **ITSM** -> **Device Management** -> Select your **Device**.

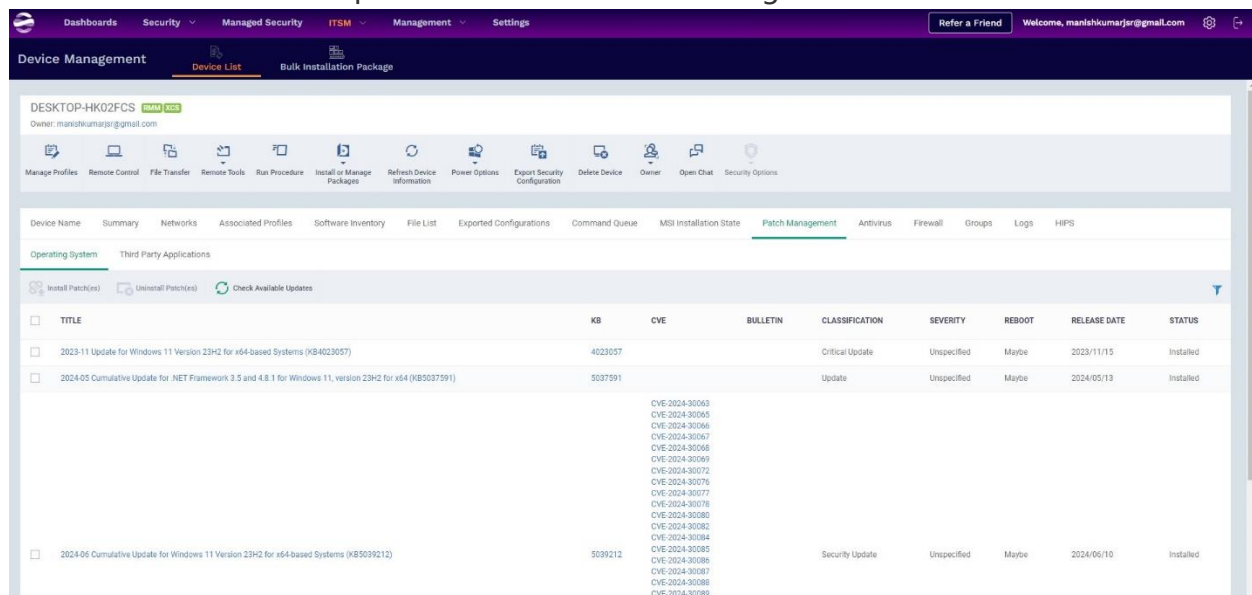
The screenshot shows the ITSM Device Management interface. The top navigation bar includes 'Dashboards', 'Security', 'Managed Security', 'ITSM', 'Management', and 'Settings'. The 'Device Management' section is active, showing a 'Device List' and a 'Bulk Installation Package' option. A search bar for devices is present. Below the search bar is a table of devices with columns: OS, NAME, PROFILE, ACTIVE COMPONENTS, VIRTUAL DESKTOP, PATCH STATUS, CUSTOMER, LAST LOGGED IN USER, and LAST ACTIVITY. The device 'DESKTOP-HK02PCS' is highlighted with a red box. The table shows two devices: 'MCA-MANISH' and 'DESKTOP-HK02PCS'. The 'DESKTOP-HK02PCS' device is associated with the 'Default Customer' and has a 'PATCH STATUS' of '4'.

OS	NAME	PROFILE	ACTIVE COMPONENTS	VIRTUAL DESKTOP	PATCH STATUS	CUSTOMER	LAST LOGGED IN USER	LAST ACTIVITY
	MCA-MANISH	MAN	20	100	4	Default Customer	MCA-MANISHADMIN (2024/06/19 06:02:57 AM)	2024/06/19 06:16:29 AM
	DESKTOP-HK02PCS	MAN	20	100	4	Default Customer	DESKTOP-HK02PCSmanishkumarj	2024/06/19 01:05:44 PM

1. Your selected device page will appear. Select the **Patch Management** tab.



The **Patch Management** page displays a comprehensive list of installed software that has available patches or more recent versions. The **Operating System** pane displays each security update available for the endpoint's operating system, along with detailed information such as its importance and whether installing it necessitates a device reboot.



1. Ensure that all available updates for the endpoint are visible. To instruct your device to recheck for new updates, Select **Check Available Updates**.

DESKTOP-HK02FCS new edit

Owner: manishkumarj@gmail.com

Manage Profiles Remote Control File Transfer Remote Tools Run Procedure Install or Manage Packages Refresh Device Information Power Options Export Security Configuration Delete Device Owner Open Chat Security Options

Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations Command Queue MSI Installation State Patch Management Antivirus Firewall Groups Logs HIPS

Operating System Third Party Applications

☐ Install Patch(es) ☐ Uninstall Patch(es) ☒ Check Available Updates

<input type="checkbox"/>	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
<input type="checkbox"/>	2023-11 Update for Windows 11 Version 23H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2023/11/15	Installed
<input type="checkbox"/>	2024-05 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 23H2 for x64 (KB5037591)	5037591			Update	Unspecified	Maybe	2024/05/13	Installed
			CVE-2024-30063 CVE-2024-30065 CVE-2024-30066 CVE-2024-30067 CVE-2024-30068 CVE-2024-30069 CVE-2024-30072 CVE-2024-30076 CVE-2024-30077 CVE-2024-30078 CVE-2024-30080 CVE-2024-30082 CVE-2024-30084						
<input type="checkbox"/>	2024-06 Cumulative Update for Windows 11 Version 23H2 for x64-based Systems (KB5039212)	5039212			Security Update	Unspecified	Maybe	2024/06/10	Installed
			CVE-2024-30085 CVE-2024-30086 CVE-2024-30087 CVE-2024-30088 CVE-2024-30089						

Note: Depending on the current update status of your device, you may not see any results initially. However, the additional entries will appear gradually as patches become available gradually.

1. To install patches directly from the cloud manager, select the checkbox next to the patch you wish to install, and then select **Install Patch(es)**.

DESKTOP-HK02FCS new edit

Owner: manishkumarj@gmail.com

Manage Profiles Remote Control File Transfer Remote Tools Run Procedure Install or Manage Packages Refresh Device Information Power Options Export Security Configuration Delete Device Owner Open Chat Security Options

Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations Command Queue MSI Installation State Patch Management Antivirus Firewall Groups Logs HIPS

Operating System Third Party Applications

☒ Install Patch(es) ☐ Uninstall Patch(es) ☐ Check Available Updates

<input type="checkbox"/>	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
<input type="checkbox"/>	2023-11 Update for Windows 11 Version 23H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2023/11/15	Installed
<input type="checkbox"/>	2024-05 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 23H2 for x64 (KB5037591)	5037591			Update	Unspecified	Maybe	2024/05/13	Installed
			CVE-2024-30063 CVE-2024-30065 CVE-2024-30066 CVE-2024-30067 CVE-2024-30068 CVE-2024-30069 CVE-2024-30072 CVE-2024-30076 CVE-2024-30077 CVE-2024-30078 CVE-2024-30080 CVE-2024-30082 CVE-2024-30084						
<input type="checkbox"/>	2024-06 Cumulative Update for Windows 11 Version 23H2 for x64-based Systems (KB5039212)	5039212			Security Update	Unspecified	Maybe	2024/06/10	Installed
			CVE-2024-30085 CVE-2024-30086 CVE-2024-30087 CVE-2024-30088 CVE-2024-30089						

1. Uninstall the patch that impacts other applications. To do so, select the checkbox next to the patch you want to remove, and then select **Uninstall Patch(es)**.

DESKTOP-HK02FCS Online MS

Owner: manishkumarj@gmail.com

Manage Profiles Remote Control File Transfer Remote Tools Run Procedure Install or Manage Packages Refresh Device Information Power Options Export Security Configuration Delete Device Owner Open Chat Security Options

Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations Command Queue MSI Installation State **Patch Management** Antivirus Firewall Groups Logs HIPS

Operating System Third Party Applications

Install Patch(es) **Uninstall Patch(es)** Check Available Updates

<input type="checkbox"/>	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
<input checked="" type="checkbox"/>	2023-11 Update for Windows 11 Version 23H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2023/11/15	Installed
<input type="checkbox"/>	2024-05 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 23H2 for x64 (KB5037591)	5037591			Update	Unspecified	Maybe	2024/05/13	Installed
			CVE-2024-30063 CVE-2024-30065 CVE-2024-30066 CVE-2024-30067 CVE-2024-30068 CVE-2024-30069 CVE-2024-30072 CVE-2024-30076 CVE-2024-30077 CVE-2024-30078 CVE-2024-30080 CVE-2024-30082 CVE-2024-30084 CVE-2024-30085 CVE-2024-30086 CVE-2024-30087 CVE-2024-30088 PUL-2024-00000						
<input type="checkbox"/>	2024-06 Cumulative Update for Windows 11 Version 23H2 for x64-based Systems (KB5039212)	5039212			Security Update	Unspecified	Maybe	2024/06/10	Installed

1. Navigate to the **Third Party Applications** tab next to the **Operating System** to review additional installed applications that have patches or available new versions.

DESKTOP-HK02FCS Online MS

Owner: manishkumarj@gmail.com

Manage Profiles Remote Control File Transfer Remote Tools Run Procedure Install or Manage Packages Refresh Device Information Power Options Export Security Configuration Delete Device Owner Open Chat Security Options

Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations Command Queue MSI Installation State **Patch Management** Antivirus Firewall Groups Logs HIPS

Operating System **Third Party Applications**

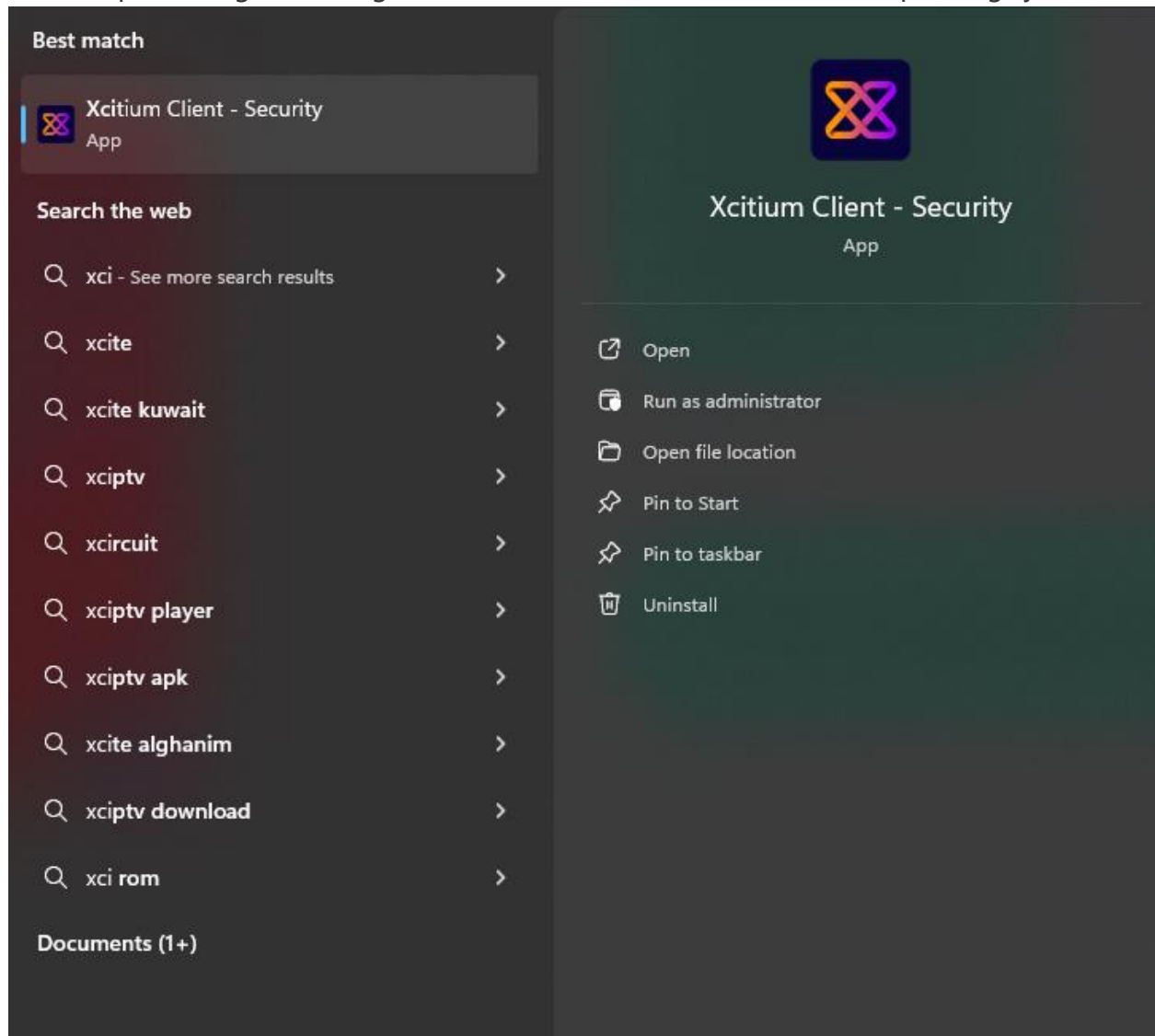
Install Patch(es) Refresh Available Updates

<input type="checkbox"/>	SOFTWARE NAME	VENDOR	SOFTWARE CATEGORY	INSTALLED VERSION	INSTALLATION DATE	LATEST VERSION AVAILABLE	SEVERITY	RELEASE DATE
<input type="checkbox"/>	Zoom	Zoom Video Communications, Inc.	Other	5.17.7 (21859)	2024/02/05	6.0.39959	Unspecified	2024/06/02
<input type="checkbox"/>	Wireshark 4.0.1 64-bit	The Wireshark developer community https://www.wireshark.org	Other	4.0.1	2022/12/06	4.0.5	Unspecified	2023/05/18
<input type="checkbox"/>	Webex	Cisco Systems, Inc.	Utilities	43.2.0.25211	2023/11/19	44.5.0.29672	Unspecified	2024/05/27
<input type="checkbox"/>	TeamViewer	TeamViewer	Developer Tools	15.15.5	2022/10/05	15.54.6	Unspecified	2024/06/13
<input type="checkbox"/>	OBS Studio	OBS Project	Utilities	30.0.2	2024/01/05	30.1.2	Unspecified	2024/04/29
<input type="checkbox"/>	Microsoft Visual Studio Code (User)	Microsoft Corporation	Utilities	1.89.1	2024/05/15	1.90.1	Unspecified	2024/06/18
<input type="checkbox"/>	Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332	Microsoft Corporation	Other	14.32.31332.0	2022/12/06	14.34.31931.0	Unspecified	2023/01/12
<input type="checkbox"/>	Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.34.28127	Microsoft Corporation	Other	14.34.28127.4	2022/10/05	14.34.31931.0	Unspecified	2023/01/12
<input type="checkbox"/>	Microsoft OneDrive	Microsoft Corporation	Online Storage	24.108.0528.0005	2024/06/14	24.111.0602.0003	Unspecified	2024/06/17
<input type="checkbox"/>	iTunes	Apple Inc.	Other	12.12.6.1	2022/10/24	12.13.2.3	Unspecified	2024/05/22

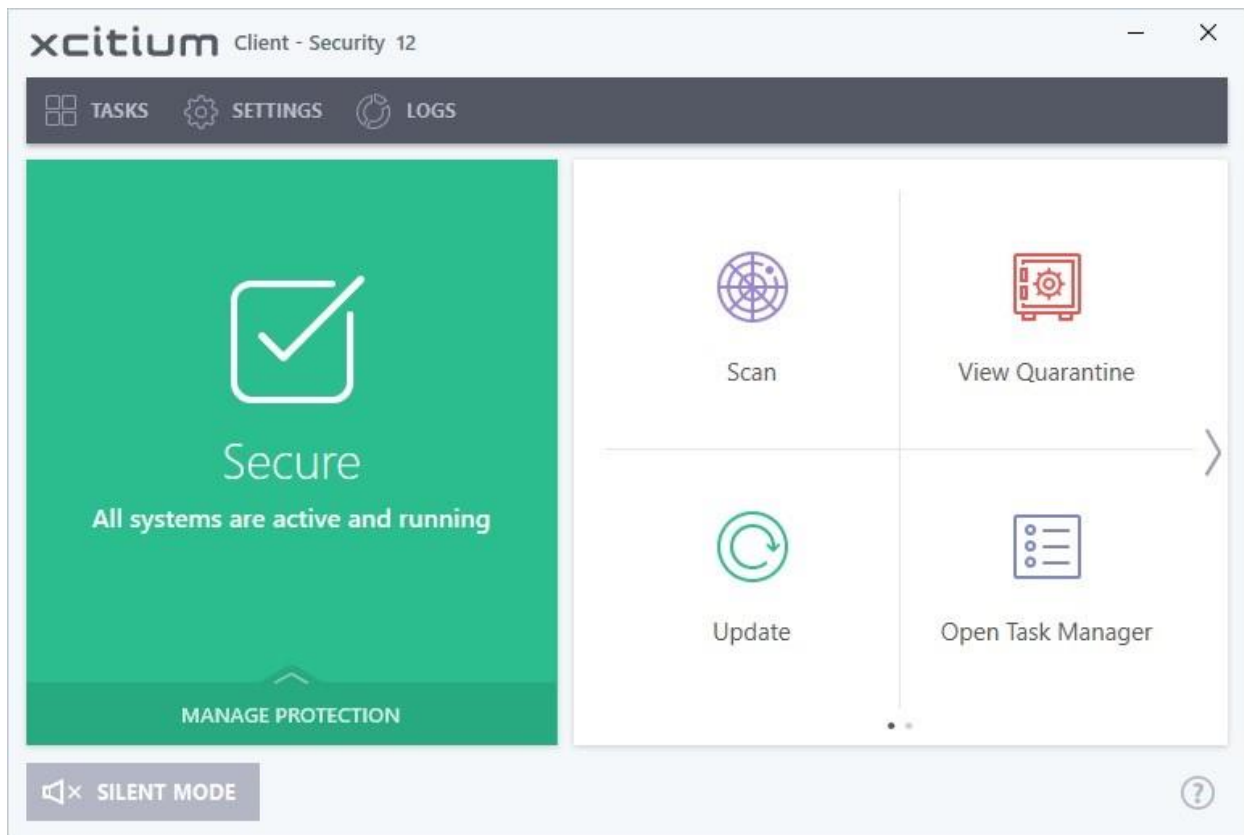
Task 5: Scan an endpoint for malware and find the results in the cloud manager

In this task, you'll use the agent to scan the endpoint for malware and then review the results reported to the cloud manager.

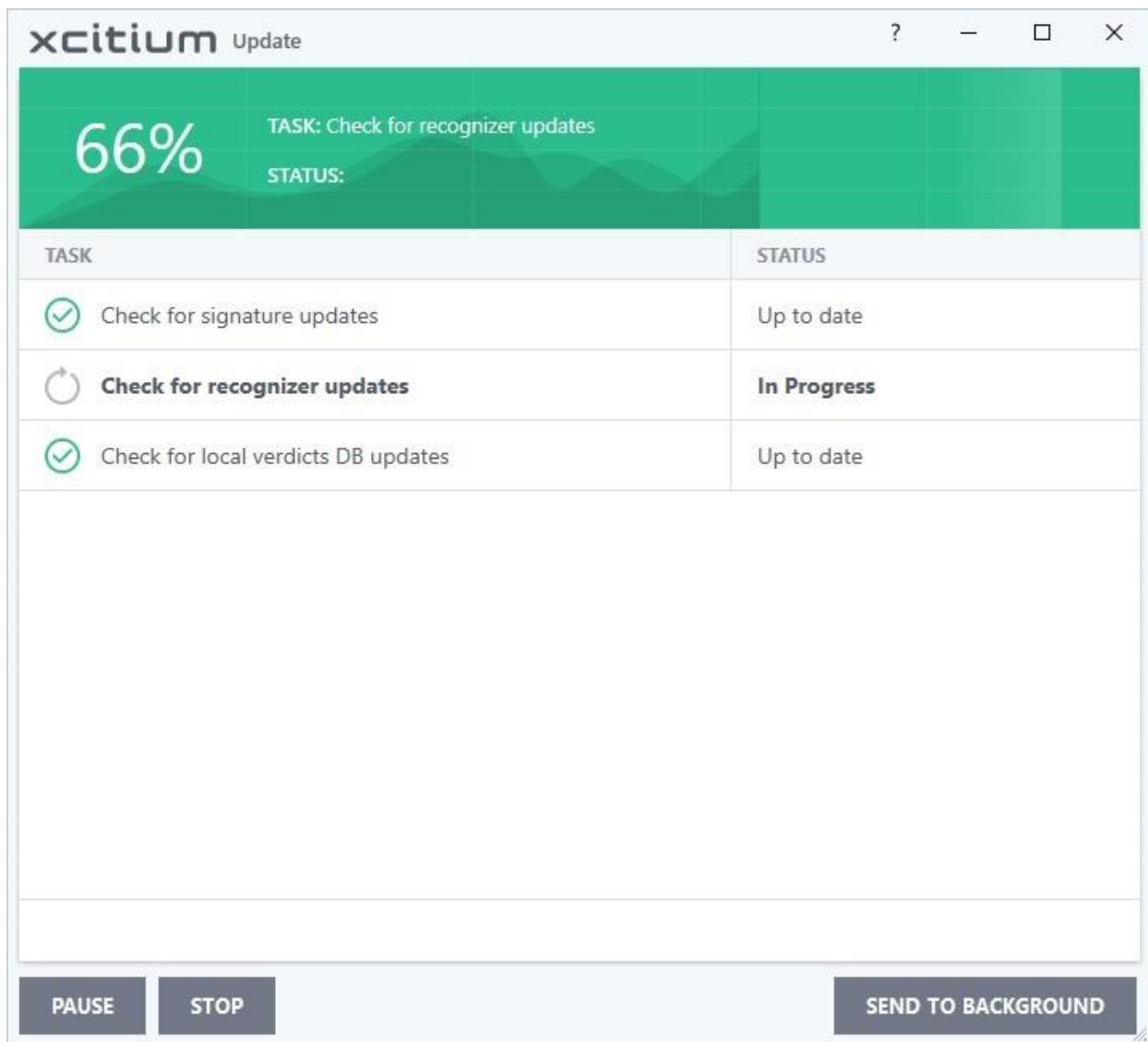
1. Open the agent. The agent's name varies based on the device's operating system.



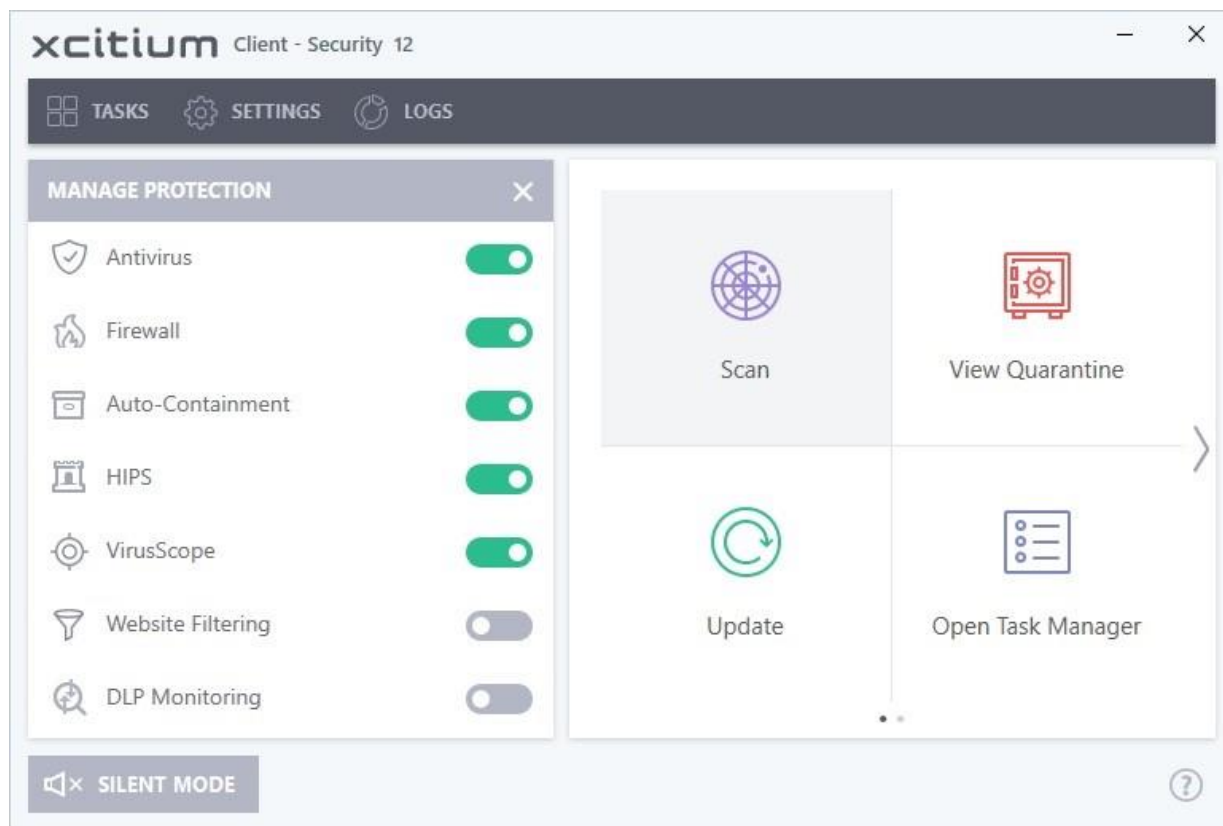
1. Select **Update** on the agent dashboard.



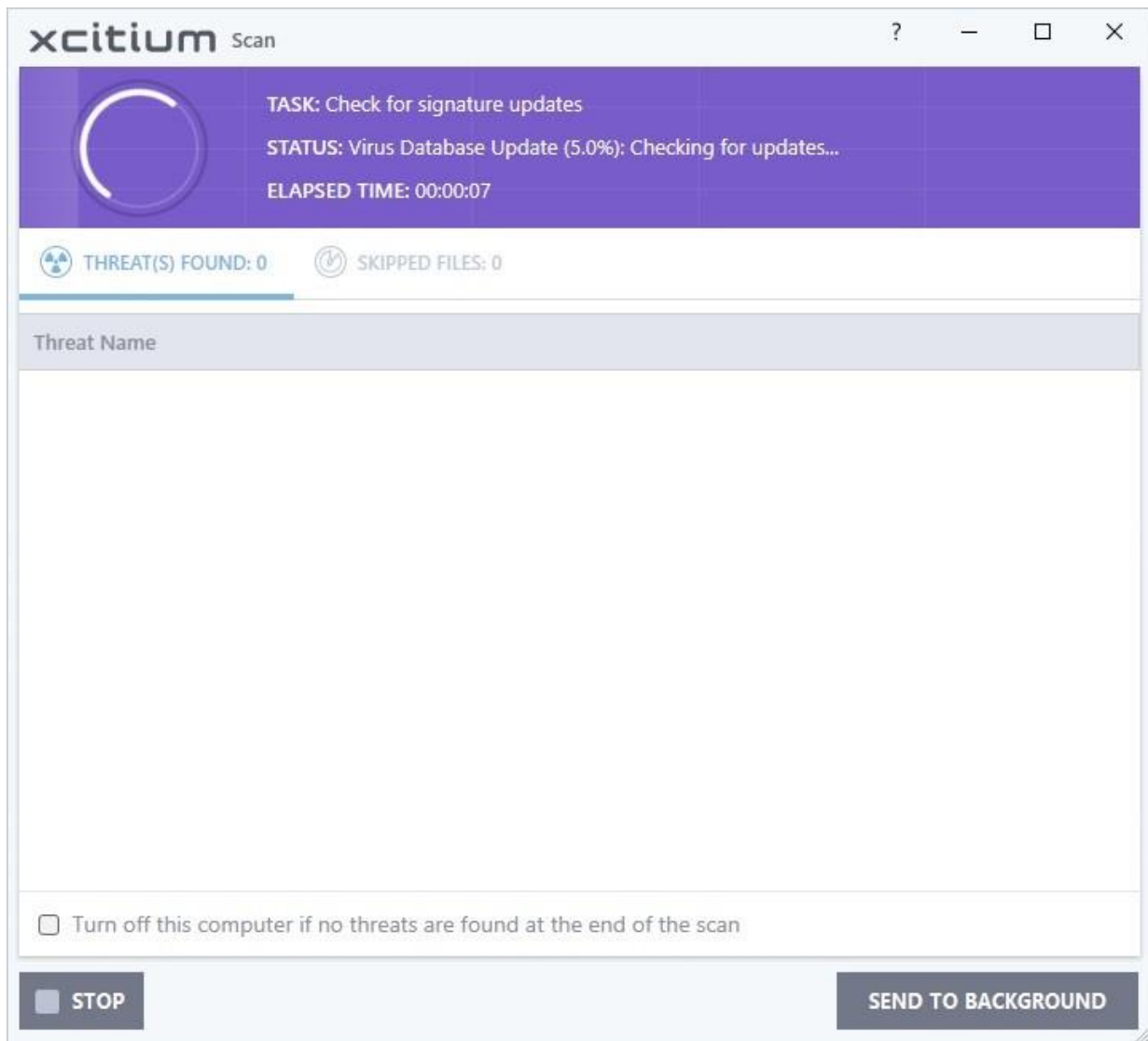
During the update process, the program reports the status of each update task to ensure that all the threat signatures are recent.



1. Once the update is complete, select **Scan** on the agent dashboard.

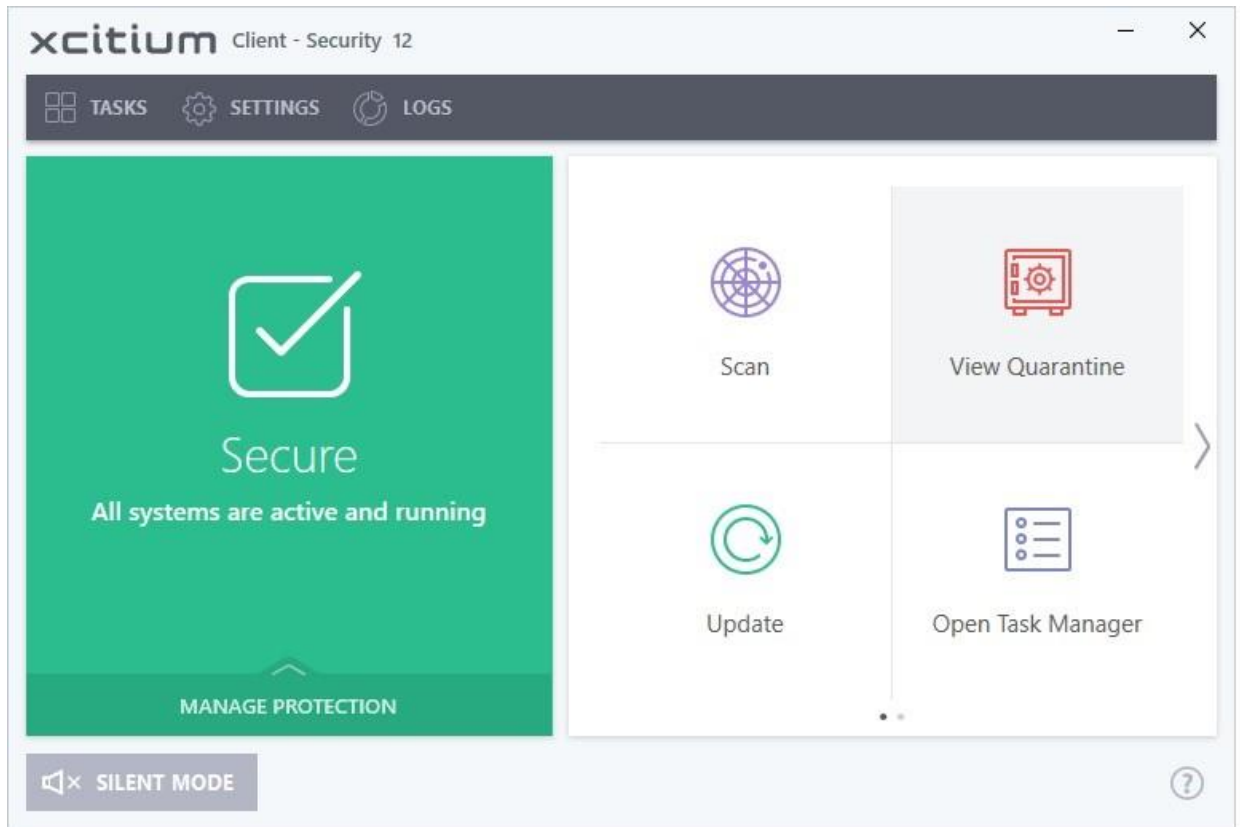


1. Next, select **Quick Scan** from the list of scans.

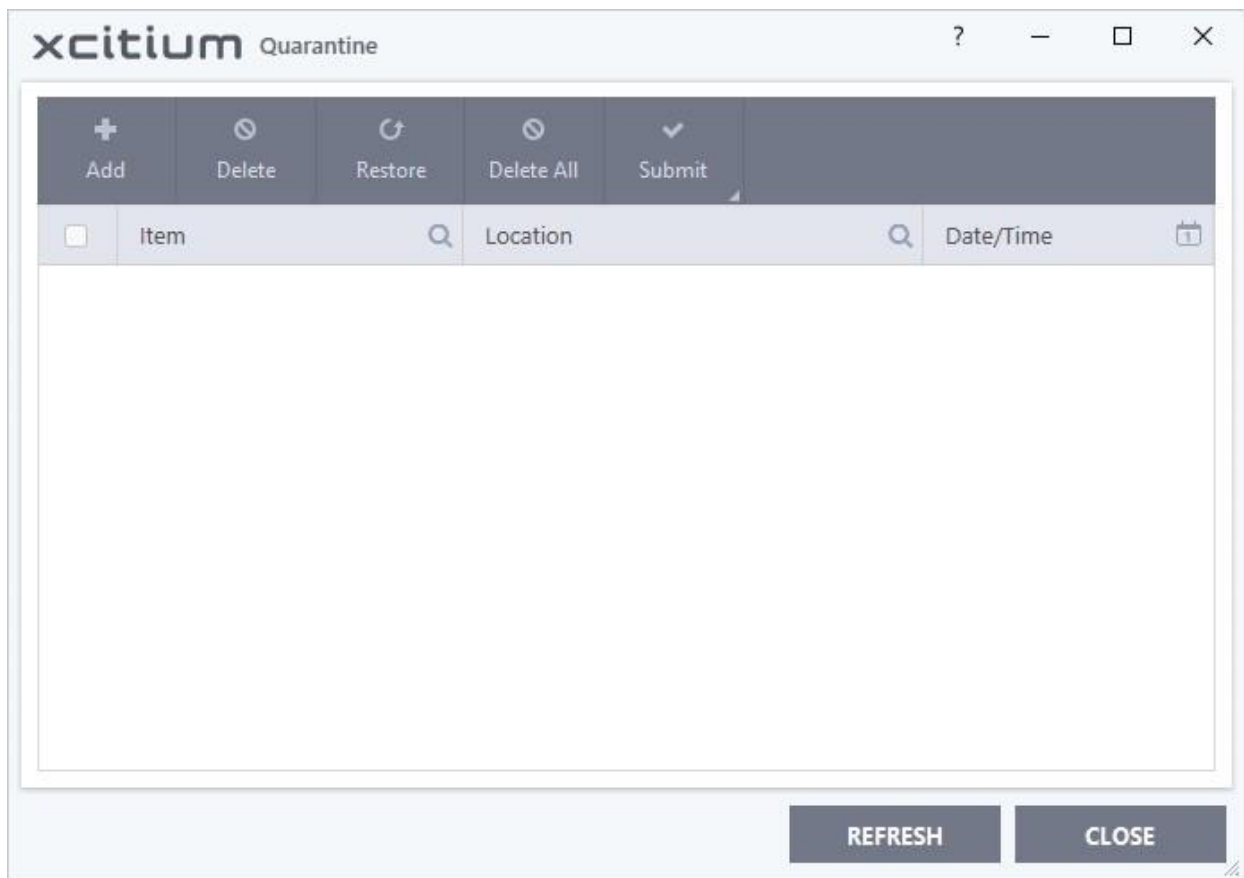


1. Post scanning the device, the system generates a report outlining each threat. To view each potential threat in quarantine, return to the agent dashboard, and then

select **View Quarantine**.



2. View the **Quarantine** dashboard to determine if any files remain in quarantine.



Practice exercises

Next, use these practice exercises to reinforce your learning.

Exercise 1: Create a new security policy in OpenEDR

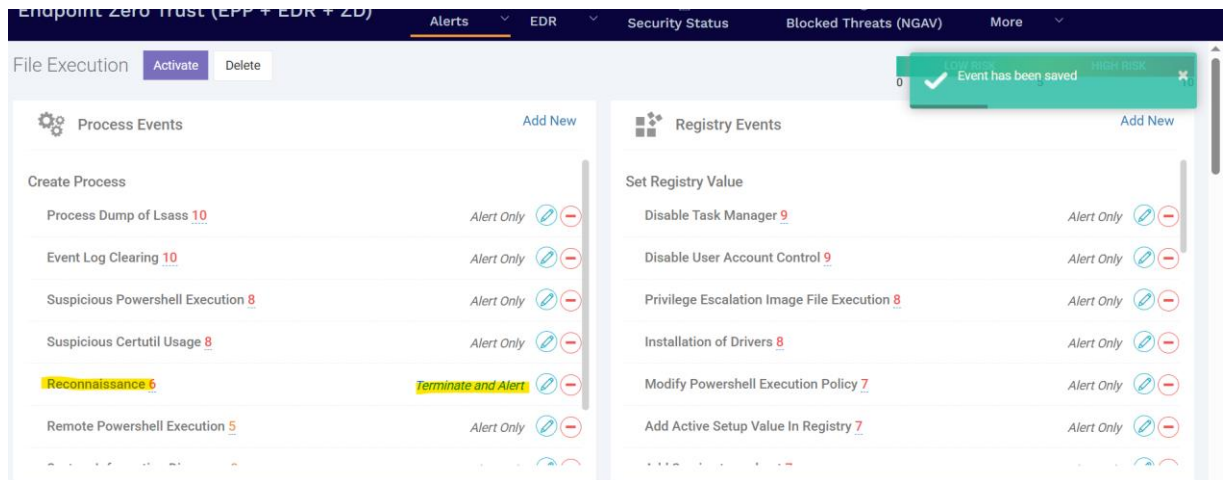
Objective: Create and apply a new security policy to protect against suspicious file execution.

Hint: The test file should be blocked or an alert should be generated according to the policy rules you set.

Solutions:

1. Open the OpenEDR console on your management server.

2. Navigate to the "Policies" section.
3. Click on "Create New Policy" and choose the type of policy you want to create (for example, "File Execution").
4. Set the policy conditions, such as blocking or alerting on executable files from unknown sources.
5. Save the policy and apply it to the desired endpoint group.
6. Test the policy by executing a test file that meets the policy conditions.



Exercise 2: Perform a system scan and remediation

Objective: Conduct a full system scan on an endpoint and take remediation actions based on the findings.

Hint: Ensure that the scan is comprehensive and covers all potential areas of concern including system files, installed applications, and user directories. After the scan, address detected threats, and run a follow-up scan to confirm that the system no longer contains the identified issues.

Solution:

Steps:

1. Open the OpenEDR console and navigate to the "Scans" section.
2. Initiate a full system scan on the selected endpoint.

3. Review the scan results for any detected threats or vulnerabilities.
4. Apply remediation actions such as quarantining malicious files, applying patches, or removing unauthorized applications.
5. Rescan the endpoint to ensure that all threats have been addressed and the system is clean.