



---

## *BS Cyber Security Department AU*

---

<b>Registration ID</b>	<b>233026,232079</b>
<b>Submitted By</b>	<b>Muhammad Sohaib Rafiq Muhammad Atif Waheed</b>
<b>Submitted To</b>	<b>Iram Fatima Hashmi</b>
<b>Date of Submission</b>	<b>06/09/2025</b>
<b>Project</b>	<b>Xicityum-OpenEDR</b>
<b>Subject</b>	<b>NS LAB</b>

# Project: Xcitium Endpoint Protection and Response System

## Introduction

**Xcitium OpenEDR** is a free, open-source Endpoint Detection and Response (EDR) solution that follows a client-server model. A centrally managed cloud server provides comprehensive threat monitoring and control, while each endpoint device runs a lightweight agent that reports data to the cloud manager. This setup enables you to detect, analyze, and respond to malware and security threats in real time.

In this project, you will configure and manage Xcitium OpenEDR to monitor endpoint devices, review security data, and apply critical patches—all from the centralized **Xcitium Cloud Manager**.

---

## Project Objectives

By completing this project, you will be able to:

- ☒ Set up and configure **Xcitium Cloud Manager**
  - ☒ Add and register endpoint devices in the **OpenEDR** system
  - ☒ View and analyze endpoint telemetry and threat data in **Cloud Manager**
  - ☒ Manage and deploy **endpoint patches**
  - ☒ Perform and review **malware scans** on endpoints
- 

## Prerequisites

To complete this project successfully, ensure you have the following:



### Authentication Requirements:

- A smartphone with an **Authenticator App** installed, such as:
  - Google Authenticator
  - Microsoft Authenticator
  - LastPass Authenticator
  - 2FAS

## Device Requirements:

- At least one internet-enabled device to act as the **endpoint**, such as:
  - Windows PC
  - macOS computer
  - Linux machine
  - Android phone/tablet
  - iOS phone/tablet

 **Note:** You can set up both the **Xcitium Cloud Manager** and endpoint agent on the same device if needed.

---

## Before You Begin

- Ensure you have **administrator privileges** on any device where you plan to install software.
  - Download the required software from the official [Xcitium OpenEDR website](#).
  - Familiarize yourself with the Xcitium dashboard layout and available tools.
- 

## Project Workflow

1. **Create a Xcitium Account** and log into the Cloud Manager
2. **Install Endpoint Agent** on the selected device
3. **Register and link the device** with your Xcitium account
4. **View endpoint data** in the Cloud Manager dashboard
5. **Initiate a malware scan** from the dashboard and review results
6. **Check for and deploy patches** to secure the endpoint
7. (Optional) Add more devices and scale your endpoint protection system

# Set up open source version of Xcitium Cloud Manager

---


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



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](#)



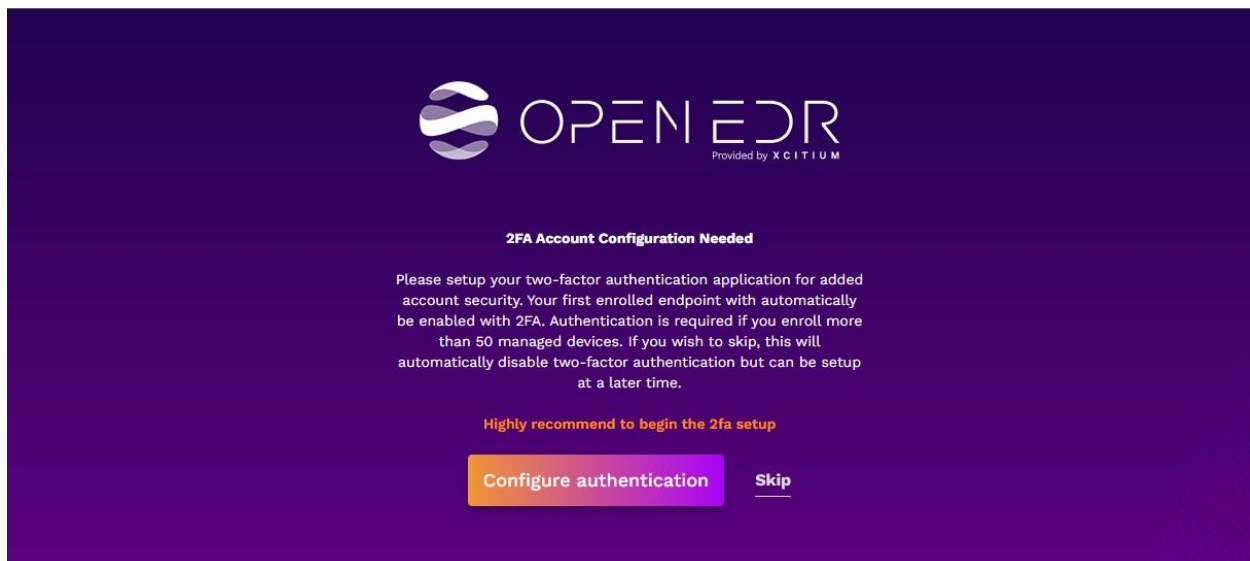
OPENEDR  
Provided by XCITIUM

### 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.

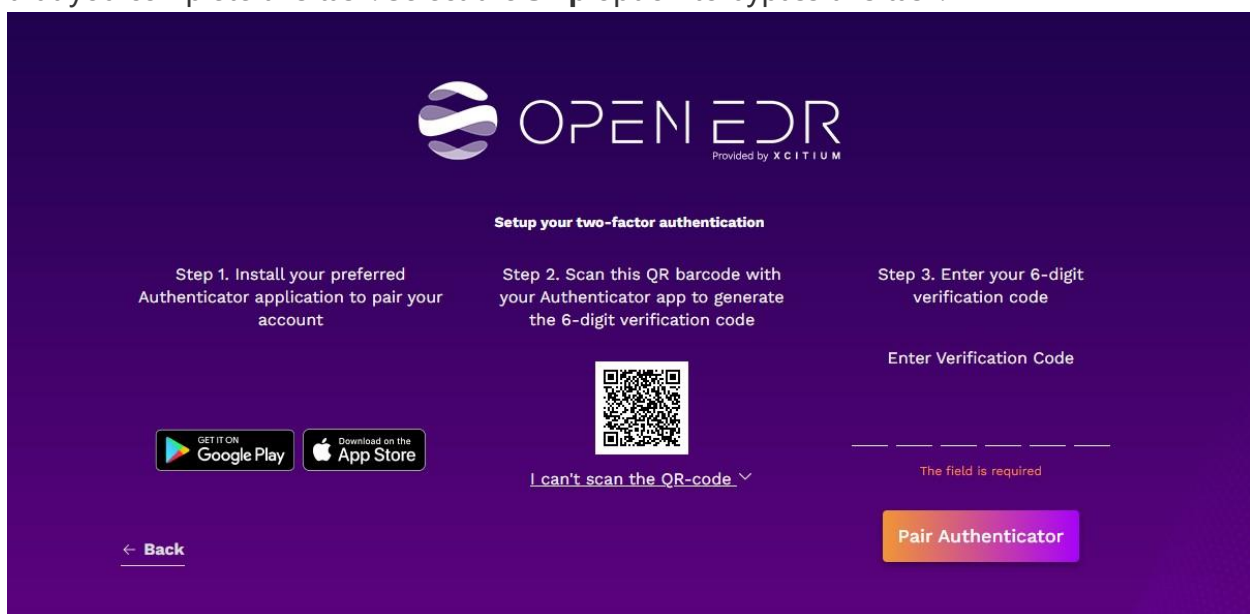
\* Answer 1

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.

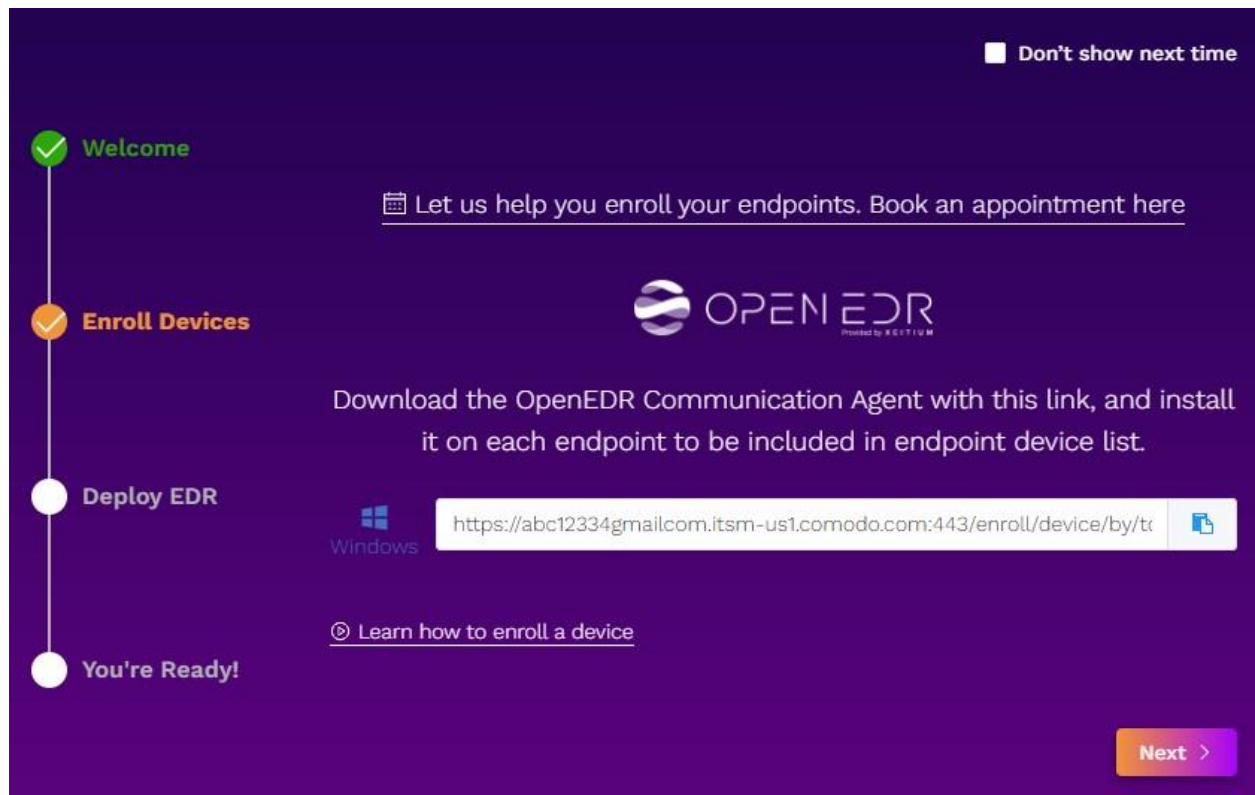


1. Use the authenticator app to scan the onscreen QR barcode to generate a six-digit verification code. Type or enter this code in the **Enter Verification Code** field on your browser window, and then select **Pair Authenticator**.

**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**.



☐ Don't show next time

Let us help you enroll your endpoints. [Book an appointment here](#)

 OPEN EDR  
Powered by Xcitiq™

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


✓ Welcome

✓ Enroll Devices

✓ Deploy EDR

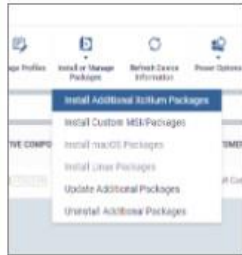
○ You're Ready!

1. CheckAll or specific devices you wish to enroll.




2. 

- Click **Install or Manage Packages**
- Click **Install Additional Xcitiq Packages**



3. 

- Check **Install Xcitiq Client-EDR**
- Click **Install**



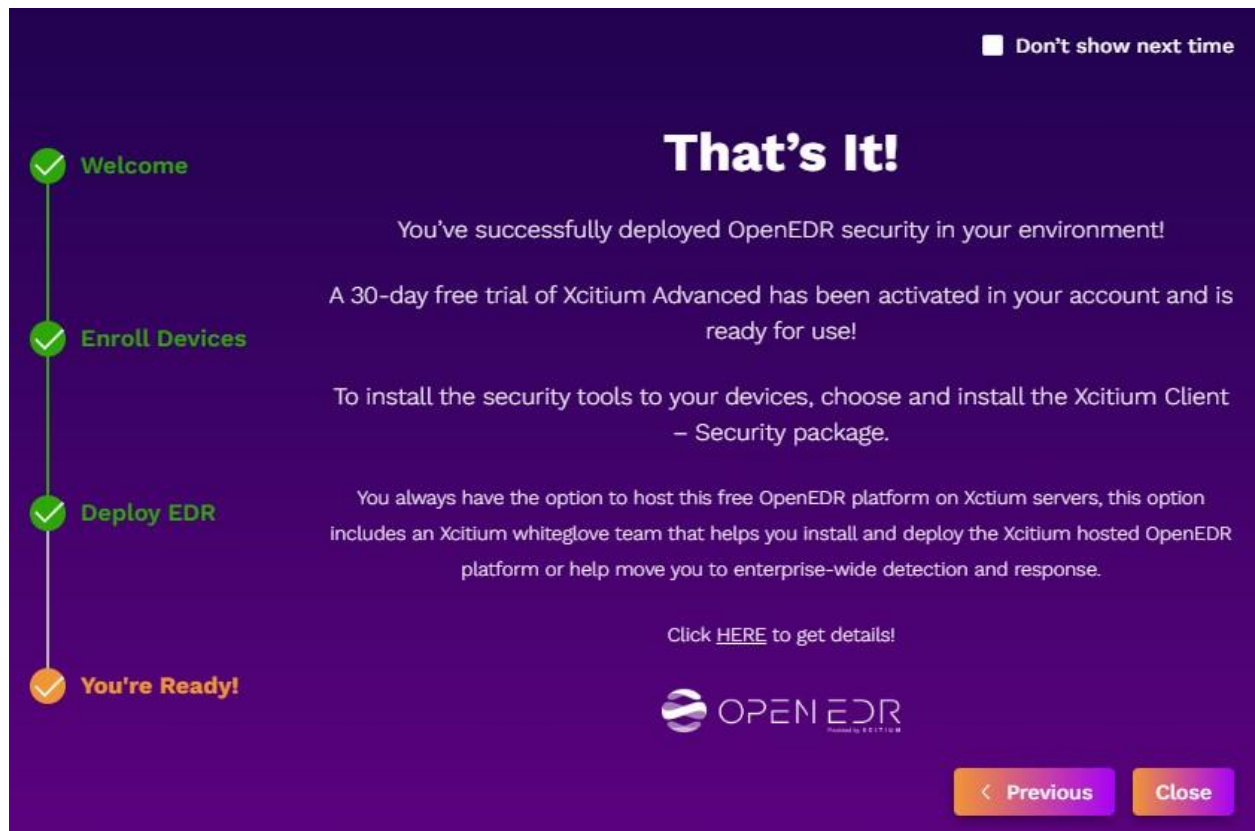
[Learn how to deploy EDR to your device](#)

< Previous

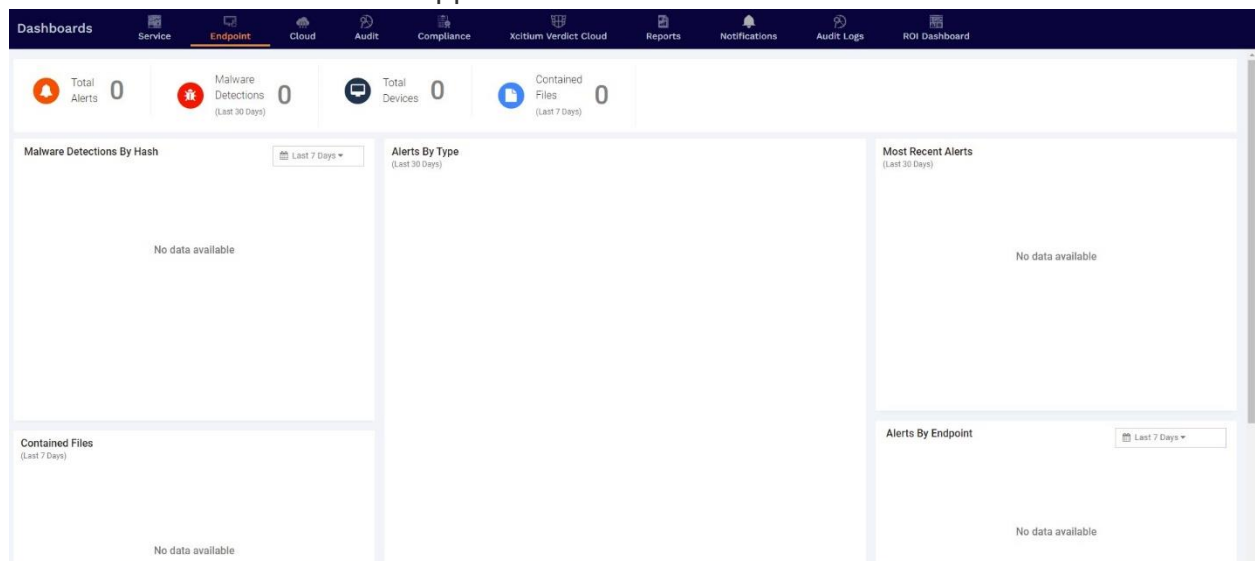
Finish

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



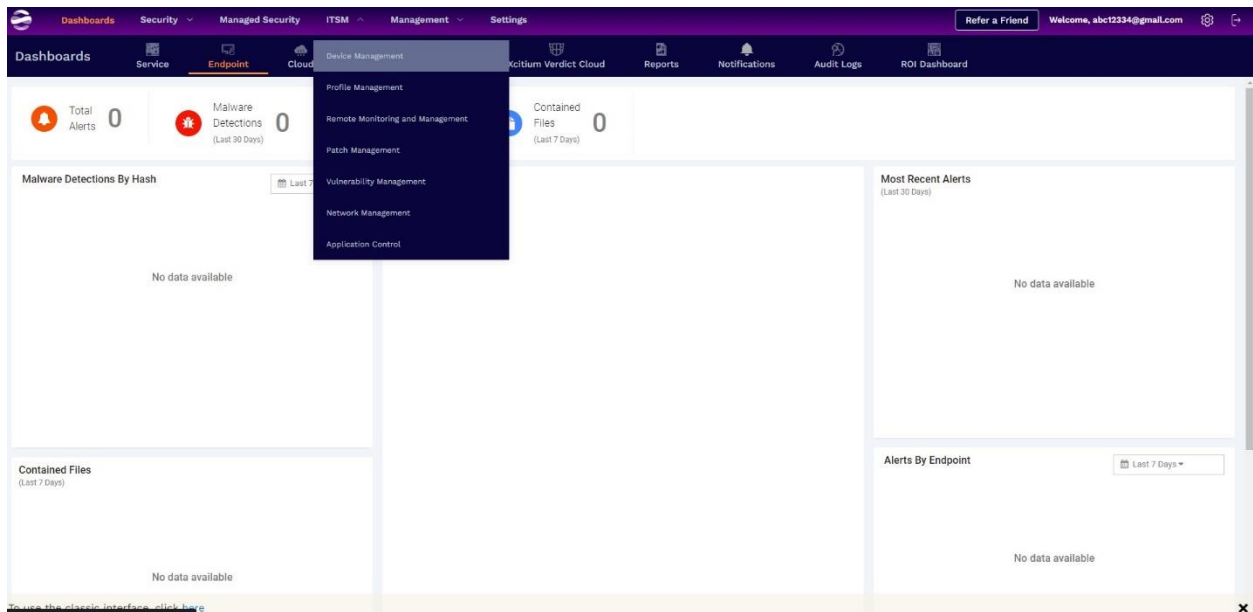


## 1. The **Dashboard** screen appears.

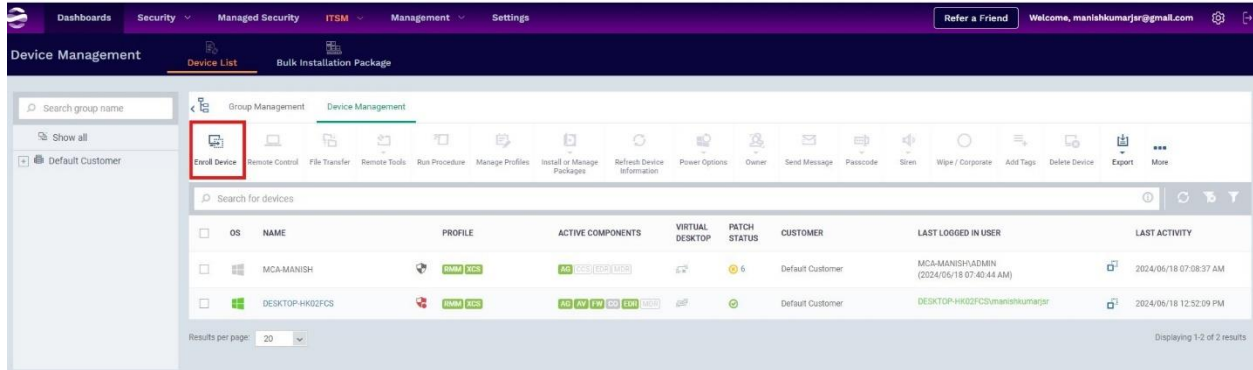


# Add an endpoint device to the OpenEDR system

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

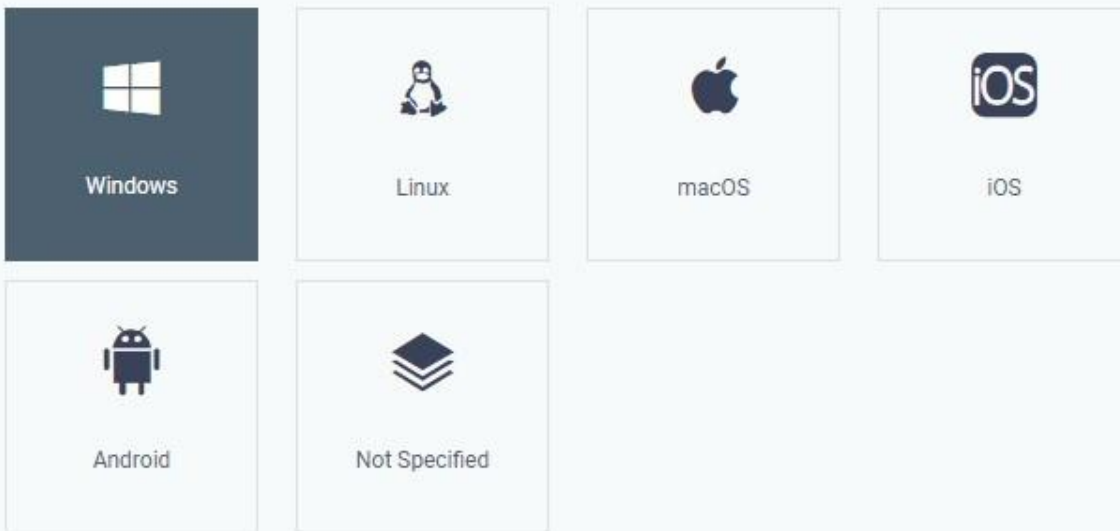


1. On the **ITSM** menu, select **Device Management** to open the **Enrollment Wizard** page. Next, select **Enroll Device**.



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

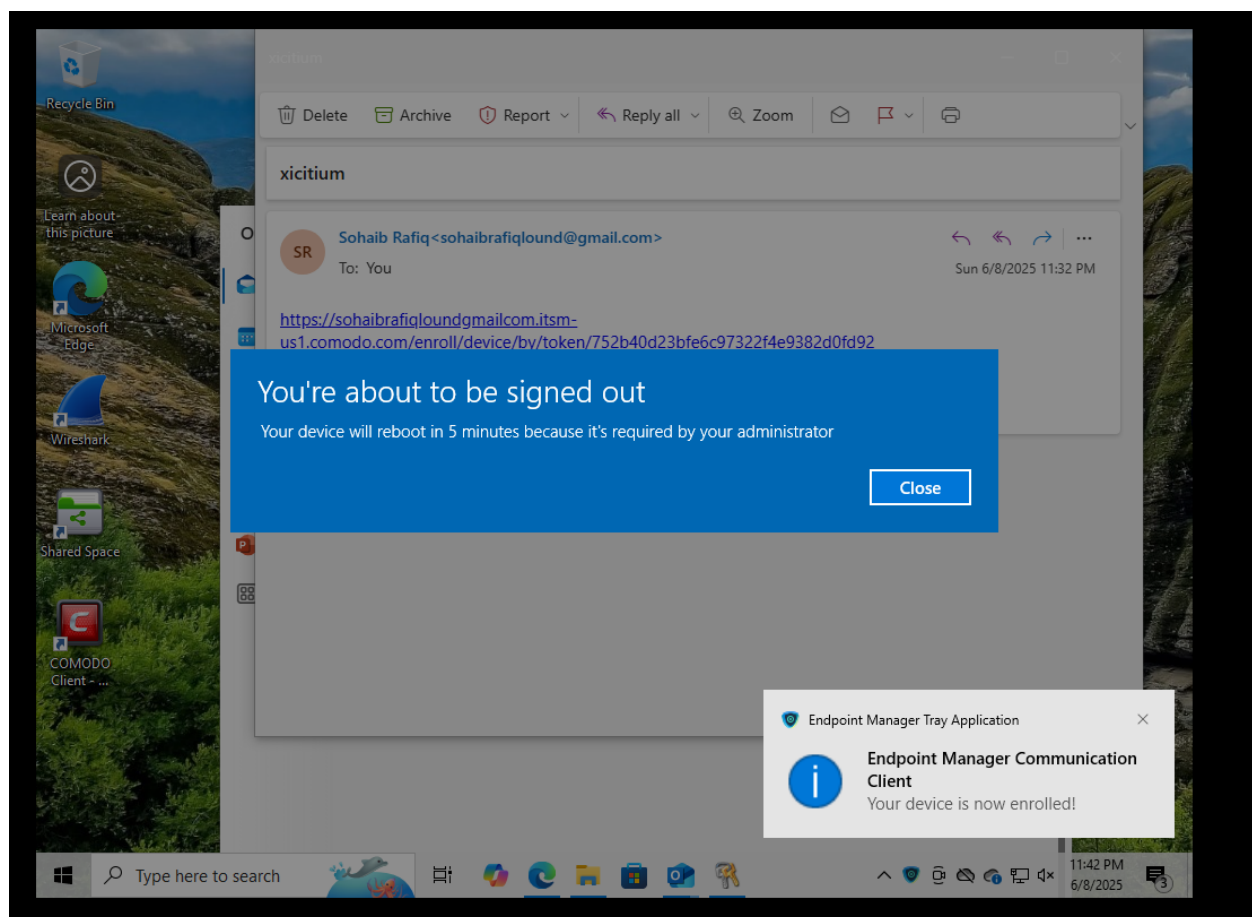
5 minutes

☐ 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

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.

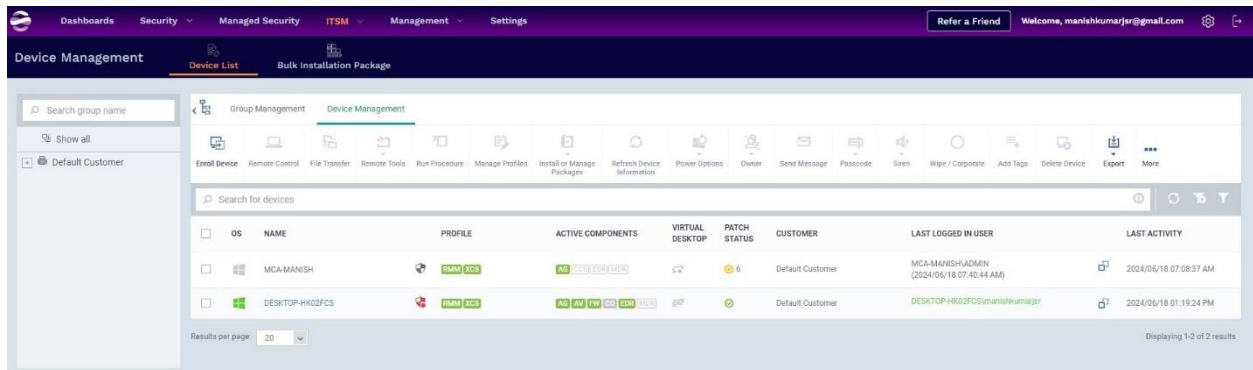
```
(windows@windows)-[~/Downloads]
$ chmod +x itsm_13LSSNf3_ccsl_installer.run
```

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

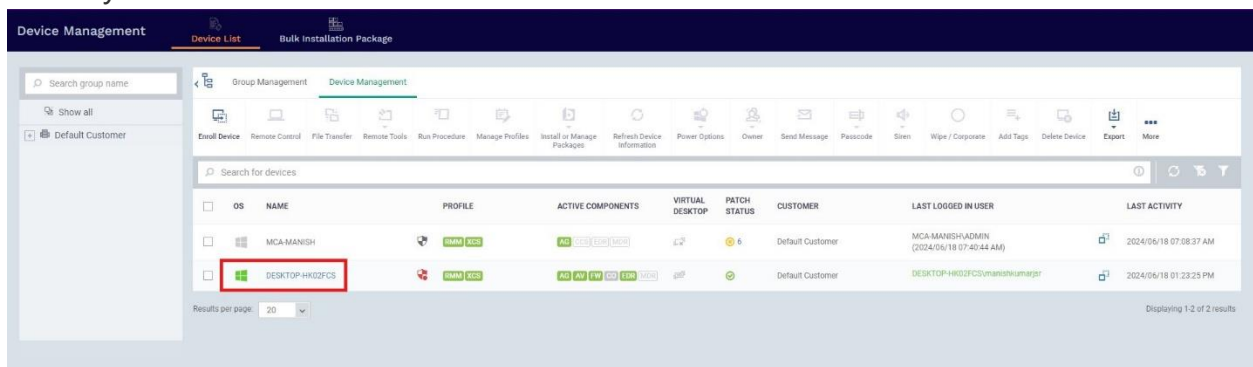
```
(windows@windows)-[~/Downloads]
$ sudo ./itsm_13LSSNf3_ccsl_installer.run
[sudo] password for windows:
Creating directory /tmp/installer_1747160873/agent
Verifying archive integrity... All good.
Uncompressing Linux ITSM Agent/10.1.50439.25030 100%
systemd system
https://mdmsupport.comodo.com/enroll/resolve/token/13LSSNf3
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:
libbfio1 libglapi-mesa libglvnd-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**.



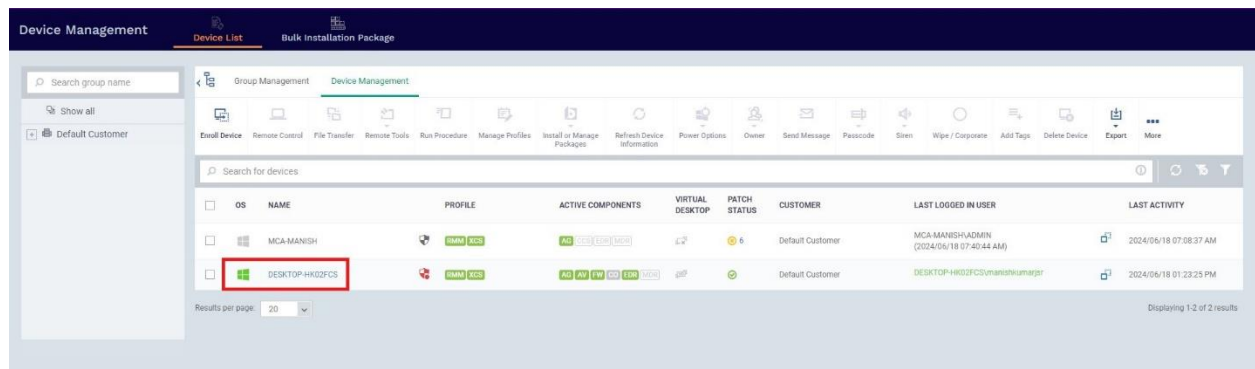
1. Select **ITSM** and then **Device Management** to view the connected devices. Check for your listed device.



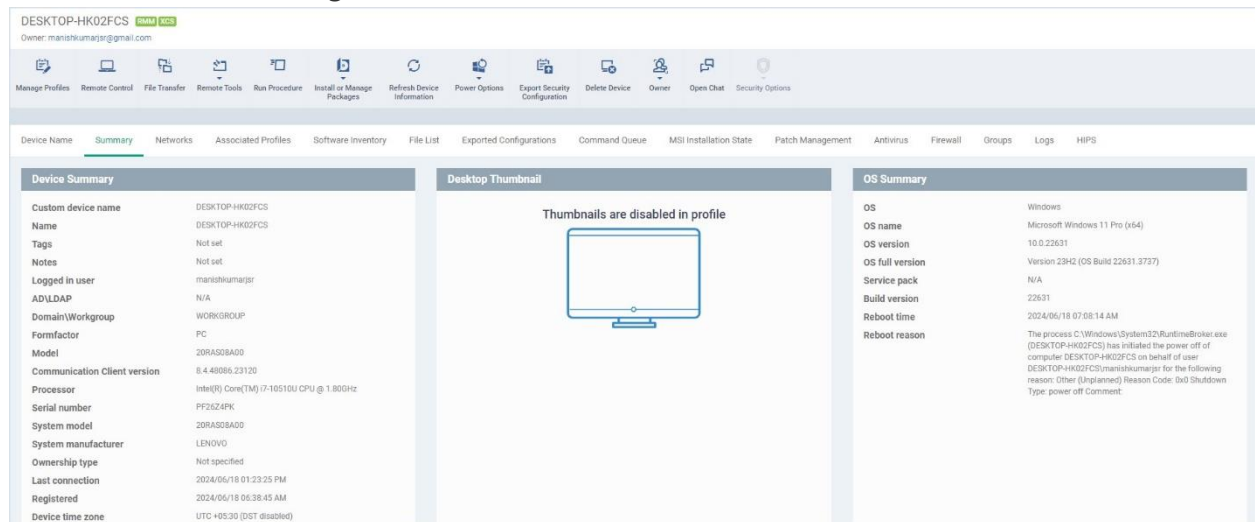
## Locate endpoint data in the Cloud Manager

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.

Device Management

DESKTOP-HK02FCS new

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

Last inventory scan date: 2024/06/18 09:16:29 AM | Status: Success

Update Software Inventory Uninstall Application(s)

SOFTWARE	VENDOR	VERSION	INSTALLATION DATE
EDR Agent v2	COMODO	2.7.1.80	2024/06/18
Lenovo Vantage Service	Lenovo Group Ltd.	4.1.12.0	2024/06/18
Endpoint Manager Communication Client	COMODO Security Solutions, Inc.	8.4.48086.23120	2024/06/18
Xcitium Client - Security	COMODO Security Solutions Inc.	12.16.0.9319	2024/06/18
Adobe Acrobat (64-bit)	Adobe	24.002.20857	2024/06/17
Microsoft Edge	Microsoft Corporation	126.0.2592.56	2024/06/16
Malwarebytes version 5.1.5.116	Malwarebytes	5.1.5.116	2024/06/16
Google Chrome	Google LLC	126.0.6479.62	2024/06/16
Microsoft OneDrive	Microsoft Corporation	24.108.0528.0005	2024/06/15
Microsoft 365 - en-us	Microsoft Corporation	16.0.17628.20144	2024/06/15

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

- Select the **Dashboard** tab.

Dashboards Security Managed Security ITSM Management Settings

Refer a Friend Welcome, manishkumarj@gmail.com

Dashboards Service Endpoint Cloud Audit Compliance Xcitium Verdict Cloud Reports Notifications Audit Logs ROI Dashboard

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

Dashboards Security Managed Security ITSM Management Settings

Refer a Friend Welcome, manishkumarj@gmail.com

Dashboards Service Endpoint Cloud **Audit** Compliance Xcitium Verdict Cloud Reports Notifications Audit Logs ROI Dashboard

Operating System

100%

- Android 0
- iOS 0
- Windows 2
- macOS 0
- Linux 0

Device Types

100%

- Smartphone 0
- Tablet 0
- PC 2
- Windows Server 0
- Unknown 0

Ownership Types

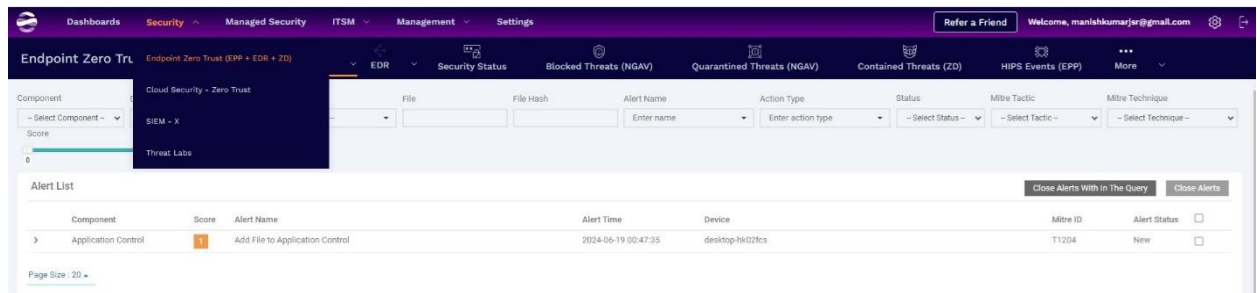
- Corporate 0
- Personal 0
- Not specified 2

Security Client Version (Windows)

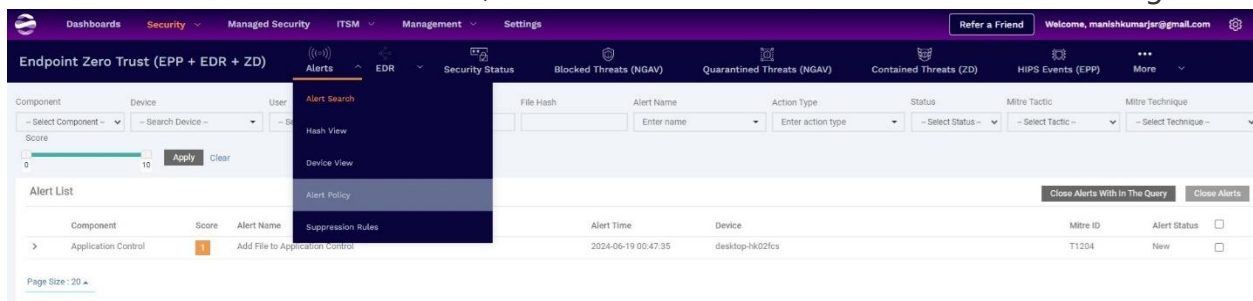
- 12.16.0.9319 1

To use the mobile interface, click here  
<https://manishkumarj@gmail.com/itm-us/1/comodo/device/device#devices/tree/devices-list?filter-os-types3>

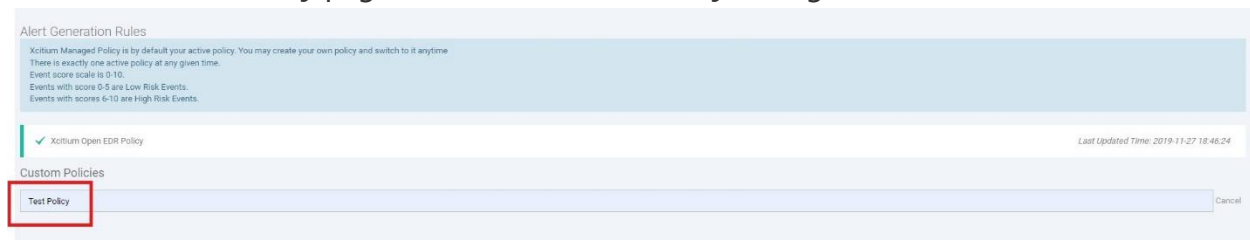
1. Select **Security** tab to view endpoint threat alerts. Next, select **Endpoint Zero Trust (EPP + EDR + ZD)** from the drop-down list.



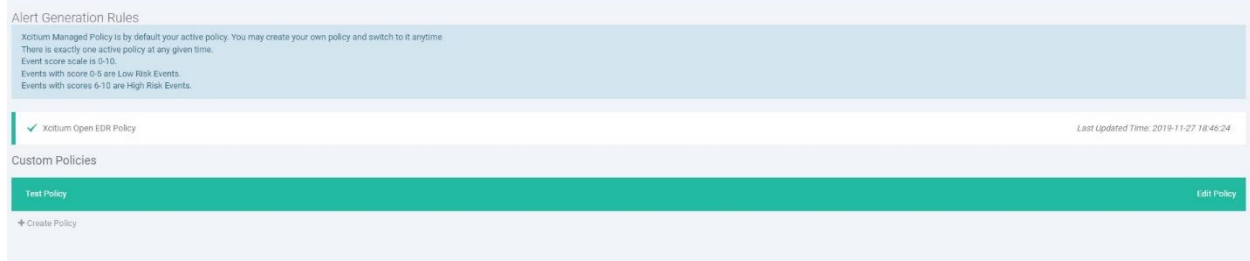
The **Endpoint Security** pane displays all EDR alerts based on severity levels. Events with a score from 0 to 5 are at the low risk, and those with a score from 6 to 10 are at the high risk.



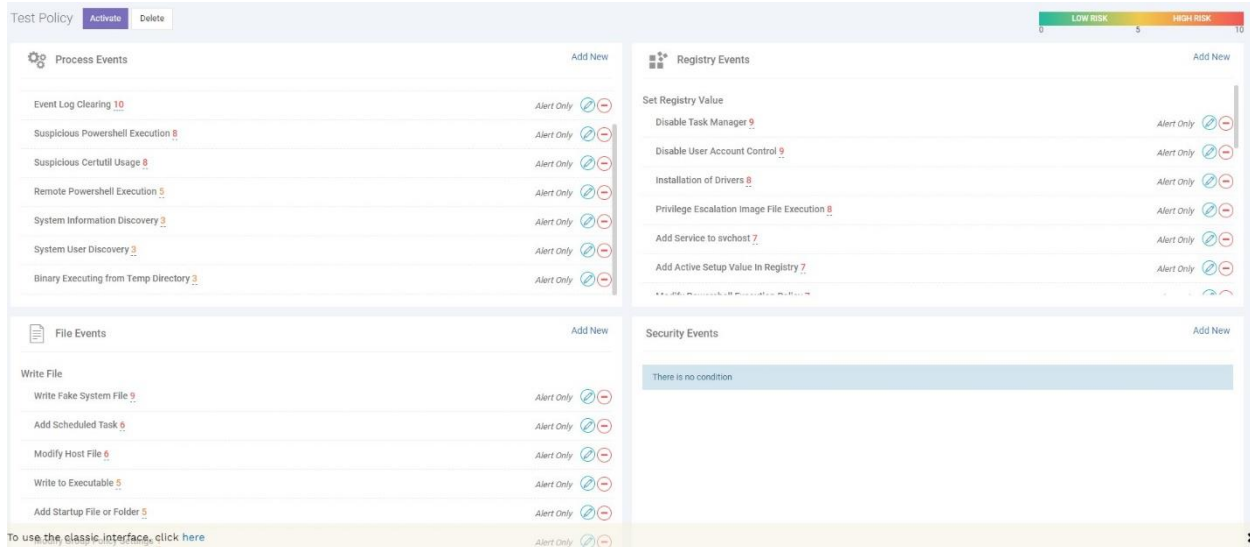
1. Next, establish new rules for monitoring potentially harmful executable downloads into the user's devices. For this, you should create a custom policy. Return to the **Alert Policy** page and select **Create Policy** to begin.



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?**

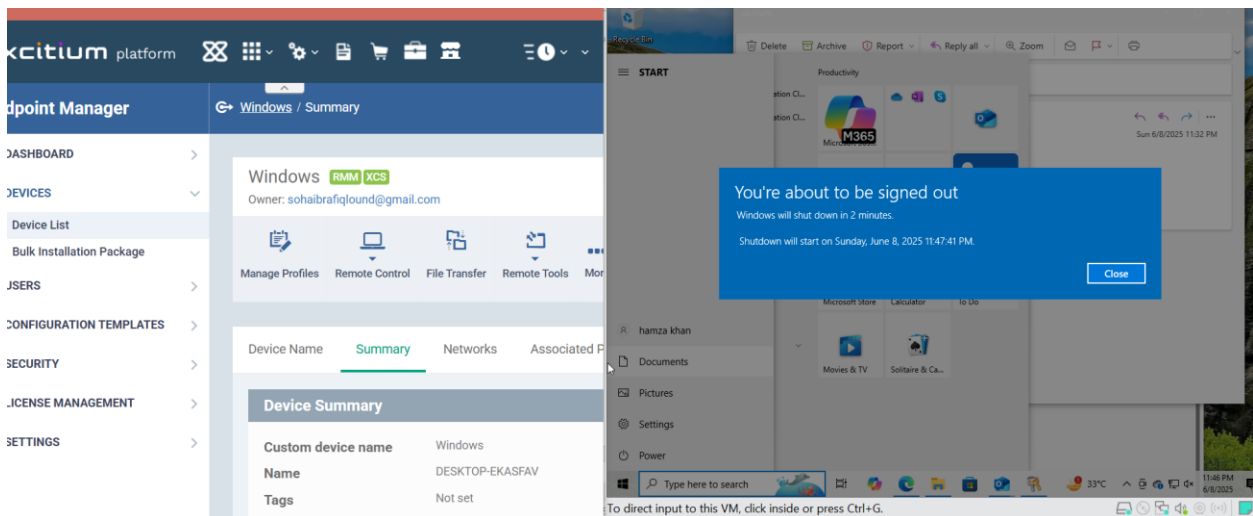
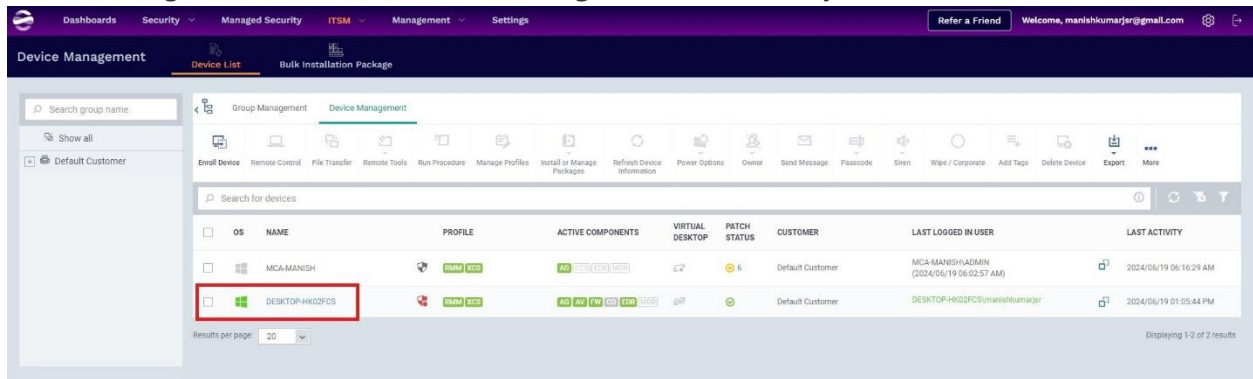
**Yes, delete it!**

**Cancel**

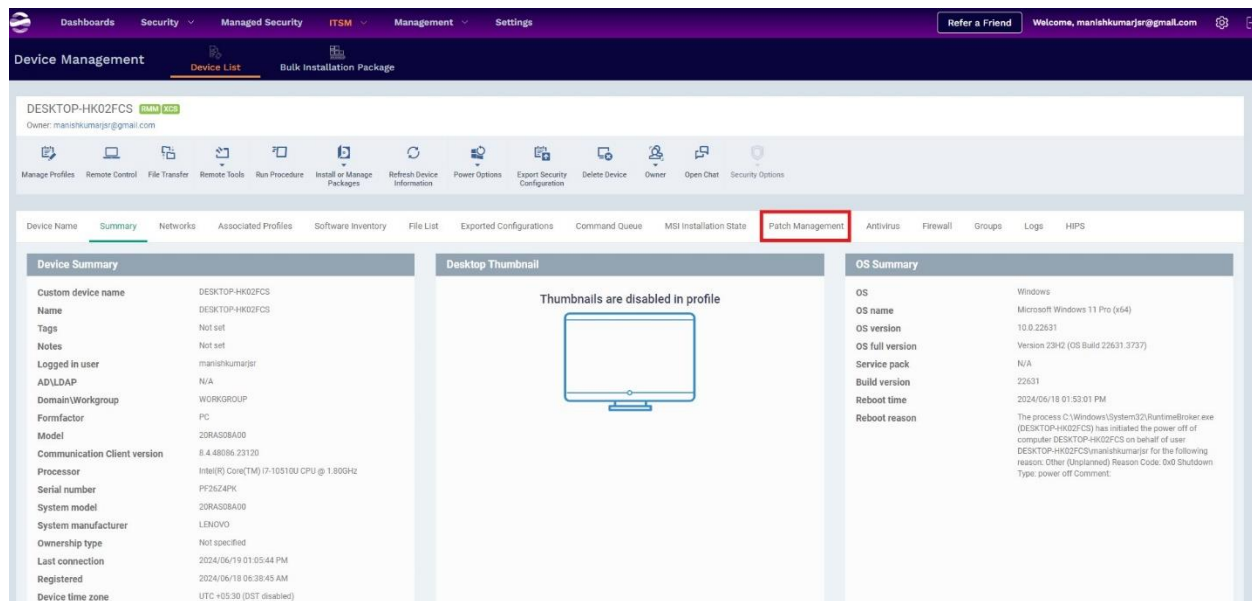
## Manage endpoint patches from the cloud manager

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.

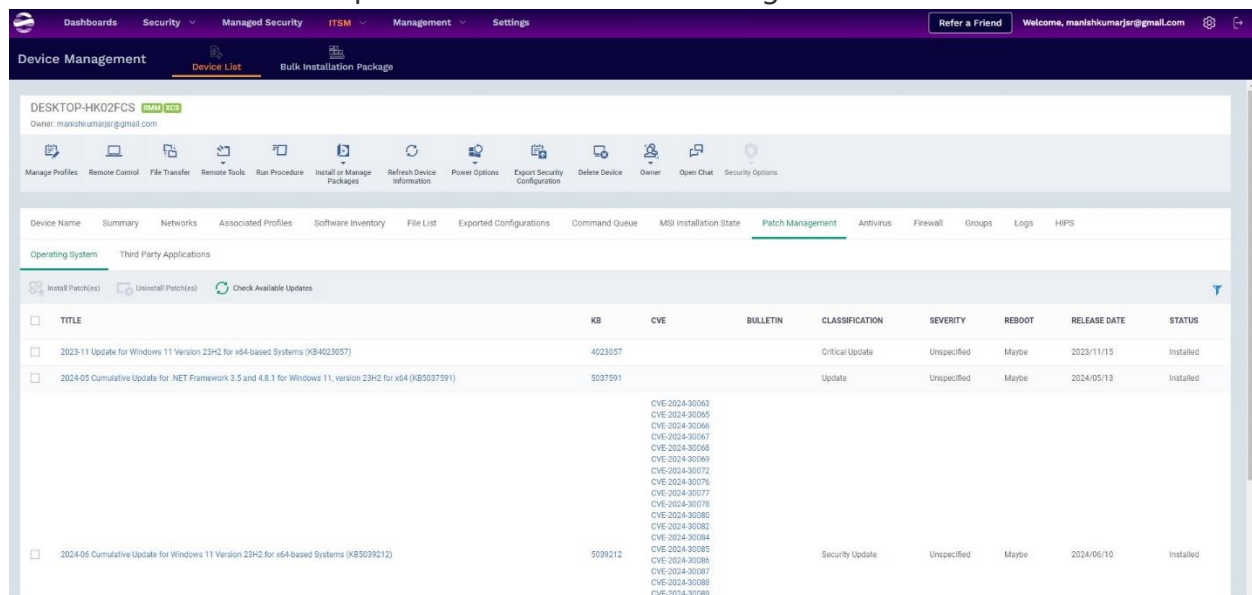
### 1. Navigate to **ITSM** -> **Device Management** -> Select your **Device**.



### 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.

- 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

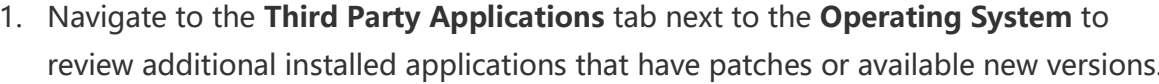
Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations Command Queue MSI Installation State **Patch Management** Antivirus Firewall Groups Logs HIPS

Operating System Third Party Applications

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

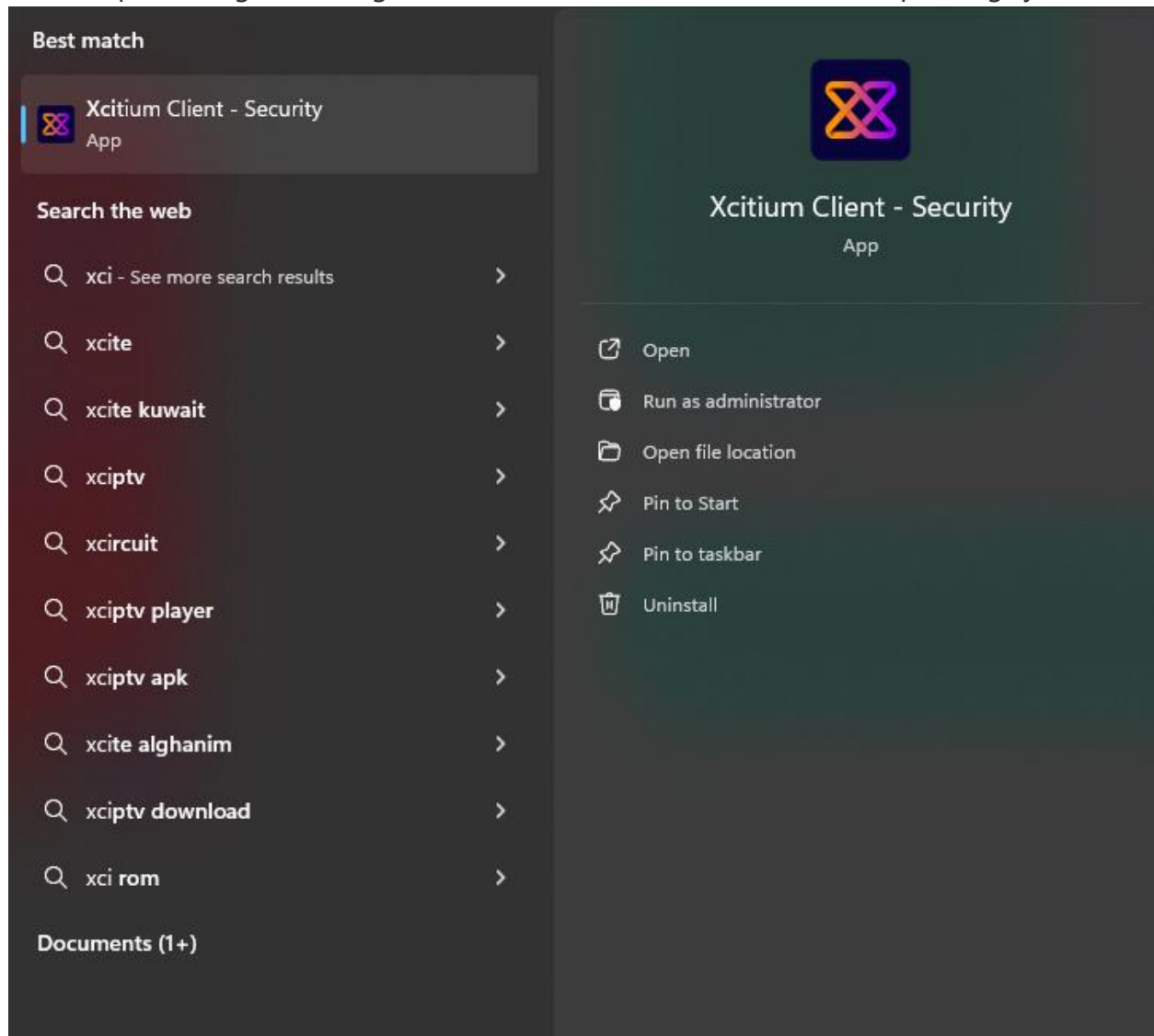
<input type="checkbox"/>	TITLE	KB	CVE	BULLETIN	CLASSIFICATION	SEVERITY	REBOOT	RELEASE DATE	STATUS
<input type="checkbox"/>	2023-11 Update for Windows 11 Version 23H2 for x64-based Systems (KB4023057)	4023057			Critical Update	Unspecified	Maybe	2023/11/15	Installed
<input type="checkbox"/>	2024-05 Cumulative 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						

- 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)**.

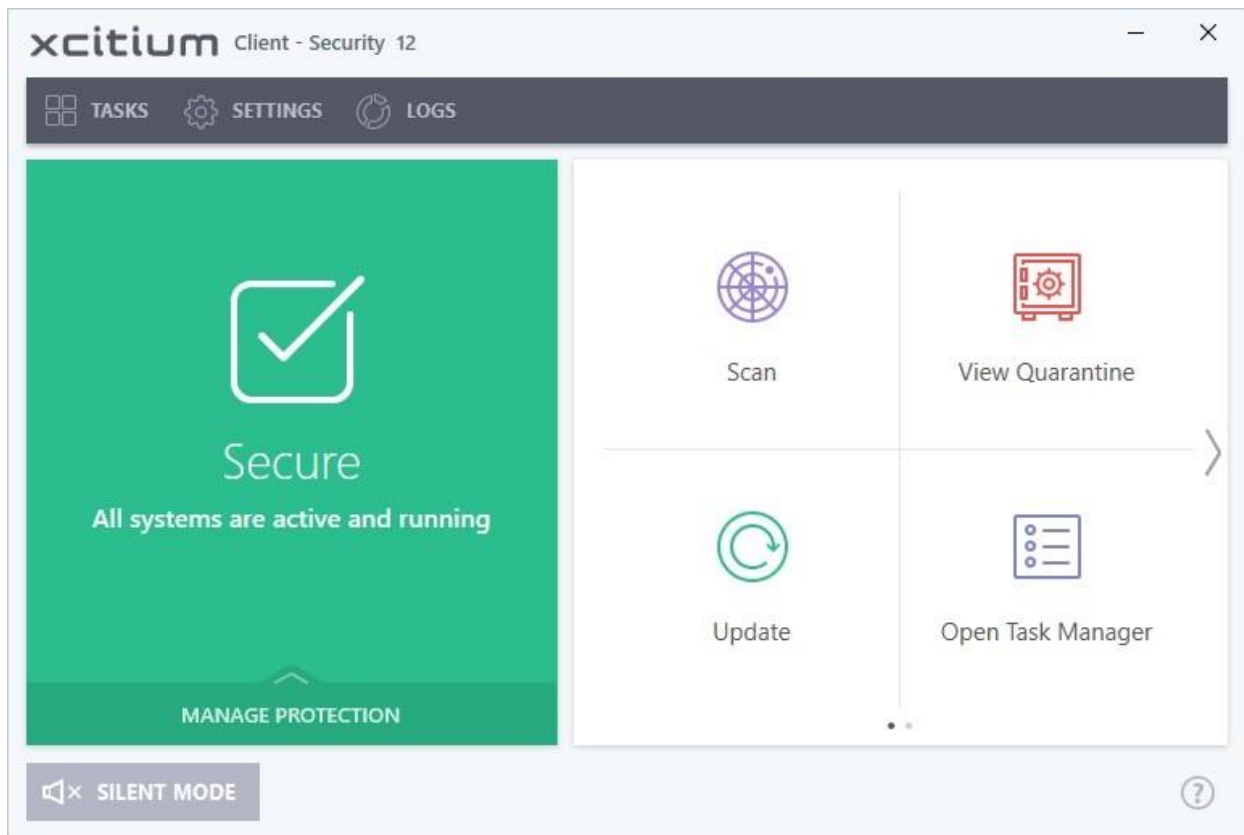


we use the agent to scan the endpoint for malware and then review the results reported to the cloud manager.

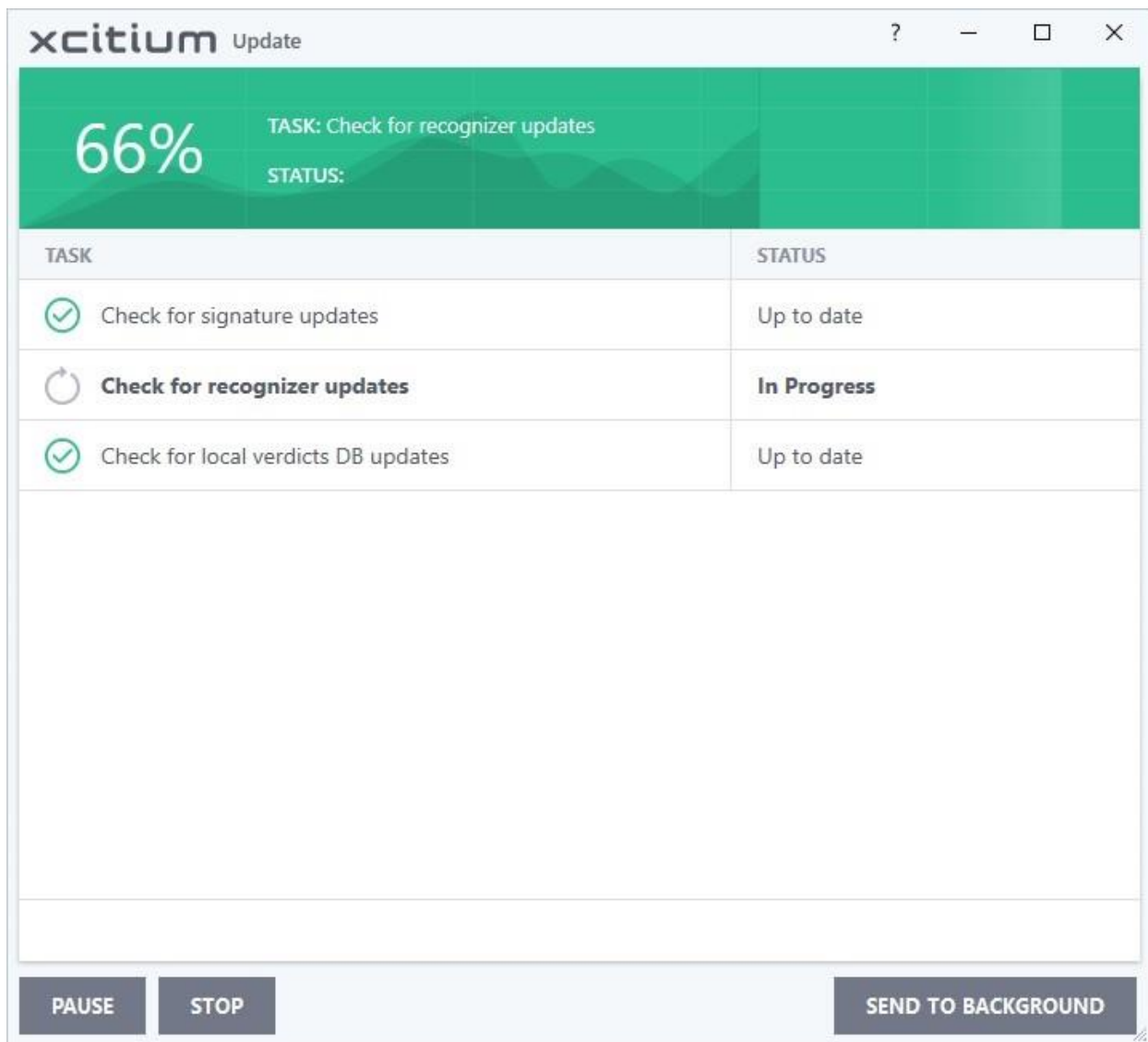
1. Open the agent. The agent's name varies based on the device's operating system.



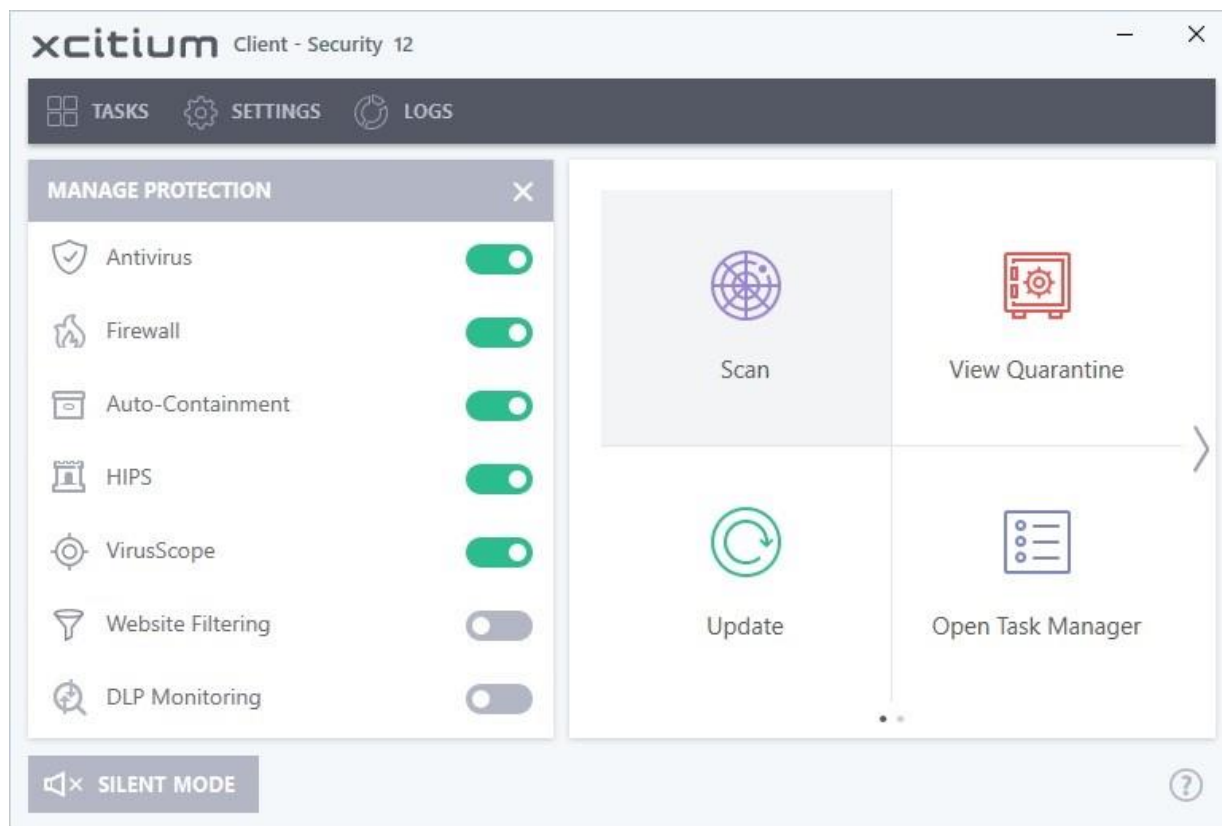
1. Select **Update** on the agent dashboard.



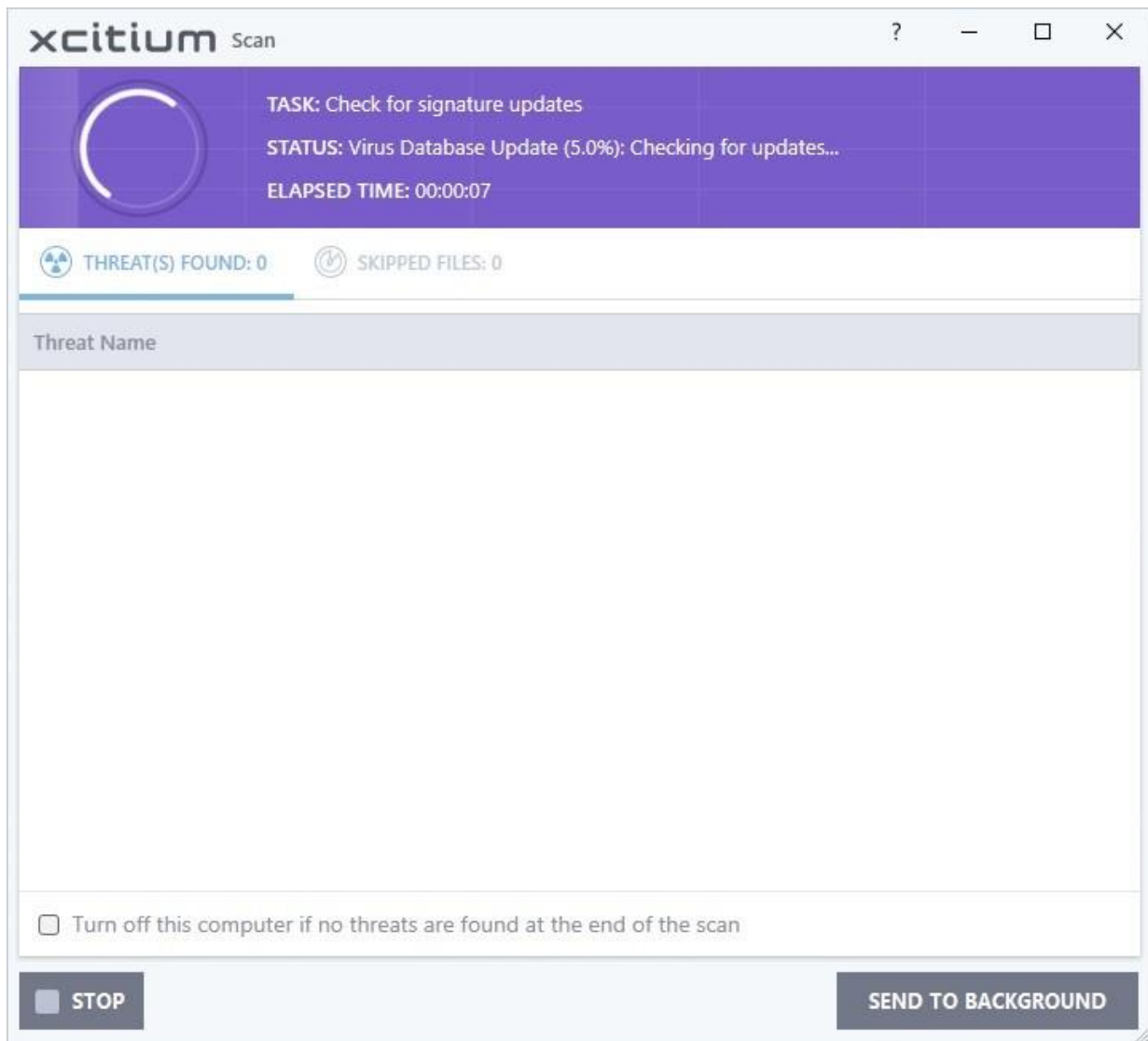
During the update process, the program reports the status of each update task to ensure that all the threat signatures are recent.



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



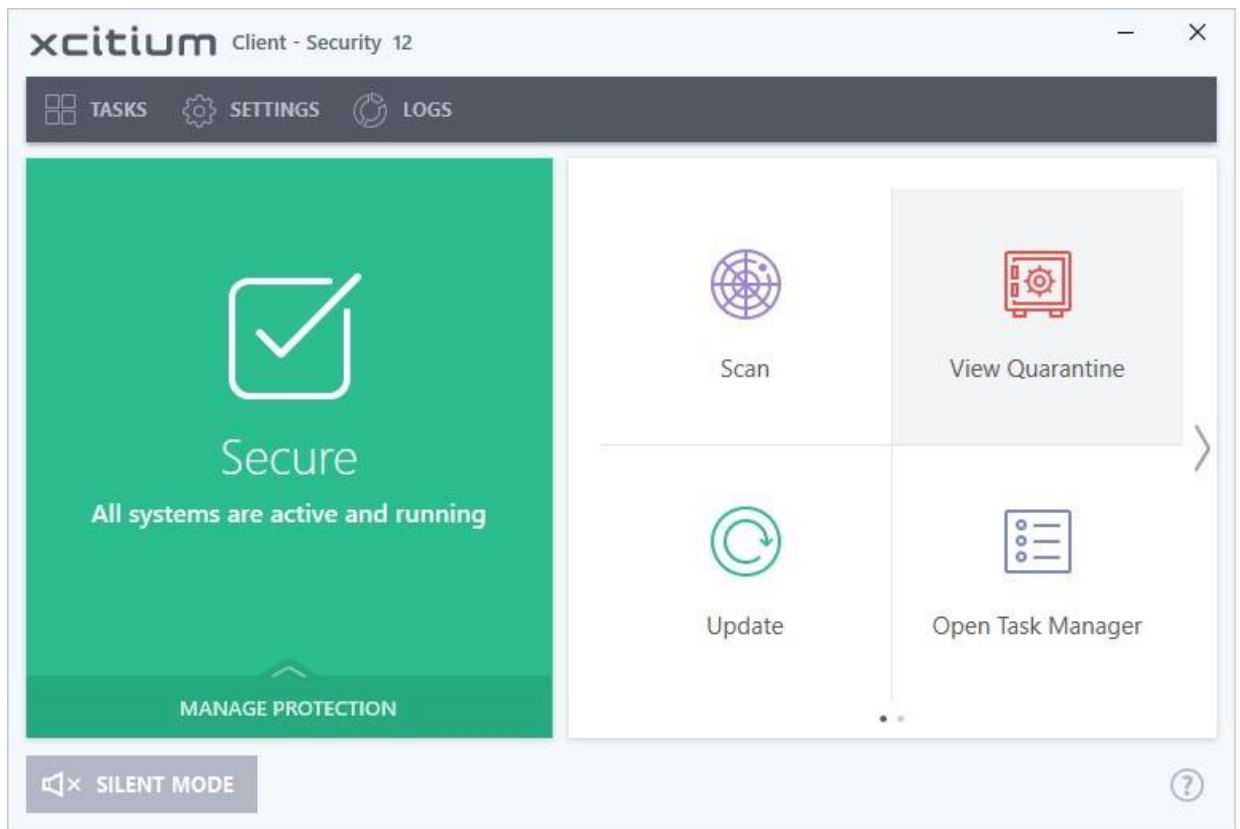
1. Next, select **Quick Scan** from the list of scans.



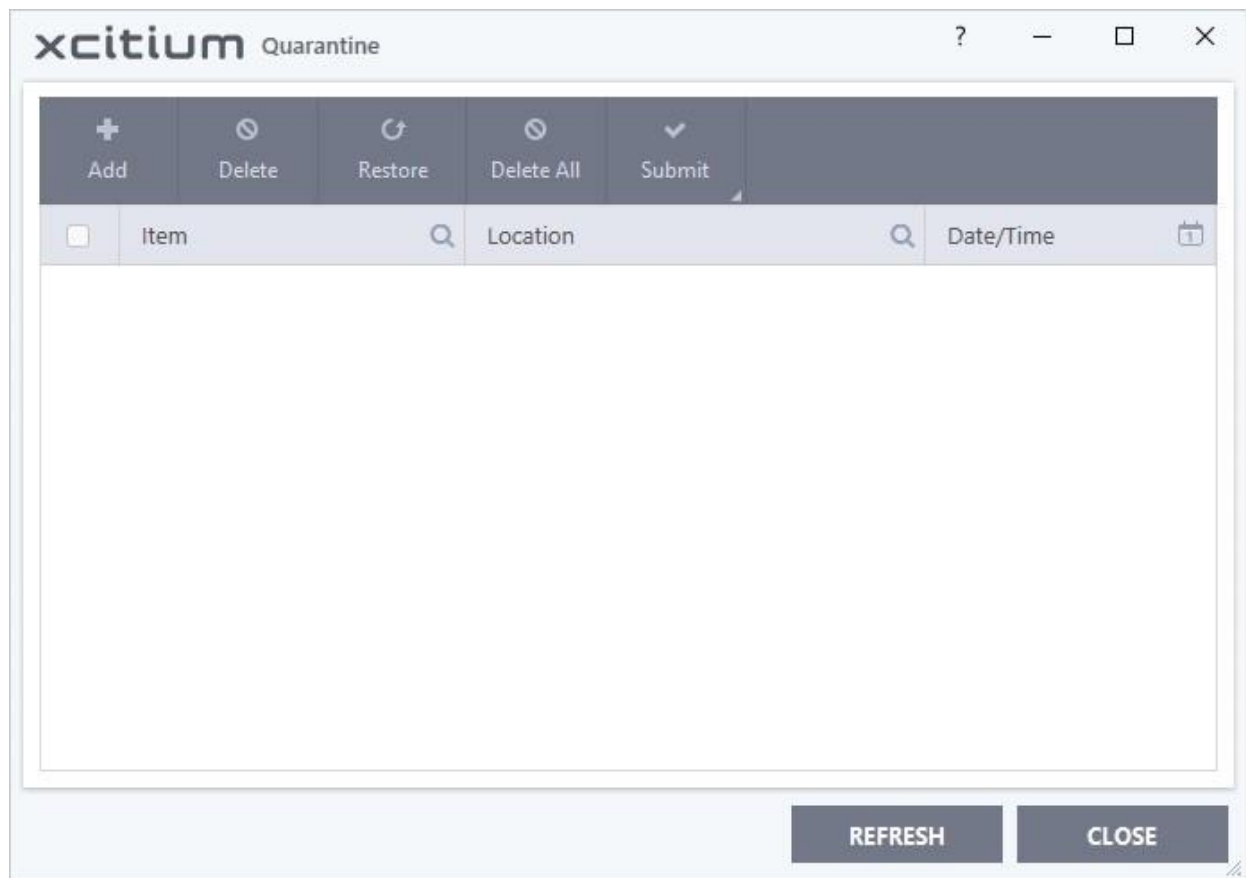
1. Post scanning the device, the system generates a report outlining each threat. To view each potential threat in quarantine, return to the agent dashboard, and then



select **View Quarantine**.



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



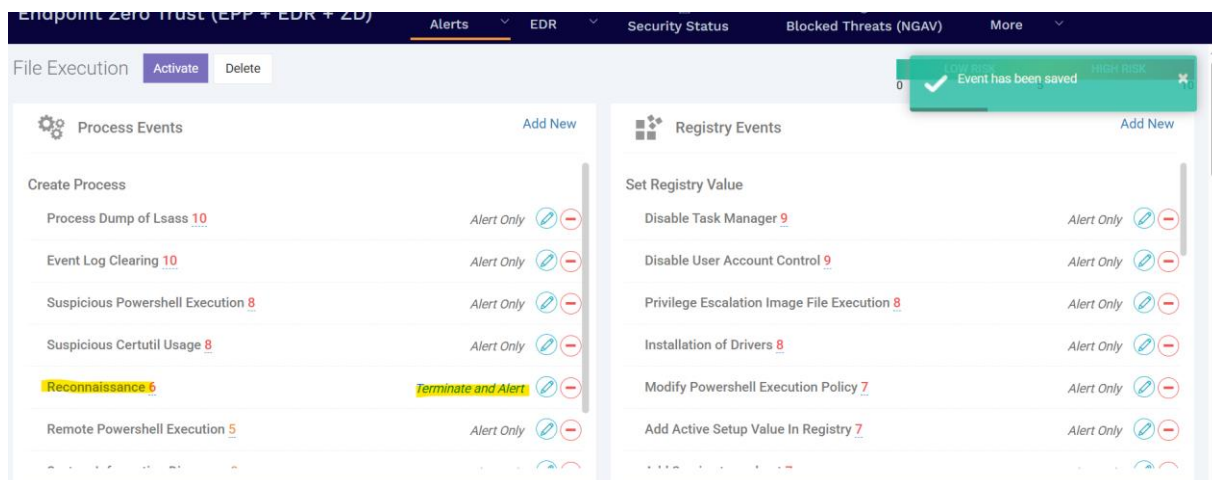
## Create a new security policy in OpenEDR

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

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.



## Remote Access & File Explorer Management using Xcitium

As part of the endpoint administration process, I utilized Xcitium's remote toolset to establish a secure connection to a target endpoint device. Through the **File Explorer** feature available in the remote tools section, I was able to navigate the system directories with **administrator privileges**. This allowed me to access and manage critical files and hidden system folders such as \$Recycle.Bin, ProgramData, System Volume Information, and Windows.

This capability is essential for remote incident response, enabling analysts to:

- Investigate system file integrity
- Check for unauthorized or suspicious files
- Collect forensic artifacts if needed
- Upload or download important logs or executables for further analysis

File Explorer

Processes

Services

Commands

Event Logs



C:\



NAME

SIZE

TYPE

MODIFIED

\$Recycle.Bin

Hidden folder

2025/05/29 02:48:13 PM

\$WinREAgent

Hidden folder

2025/06/08 12:12:42 PM

Documents and Settings

Hidden folder

2025/02/13 07:51:40 PM

OneDriveTemp

Hidden folder

2025/02/19 10:30:01 PM

PerfLogs

Folder

2019/12/07 03:14:52 AM

Program Files

Folder

2025/06/08 12:41:54 PM

Program Files (x86)

Folder

2025/06/08 12:42:23 PM

ProgramData

Hidden folder

2025/06/08 12:43:05 PM

Recovery

Hidden folder

2025/03/26 09:58:20 PM

System Volume Information

Hidden folder

2025/02/13 01:26:18 PM

Users

Folder

2025/06/08 12:28:36 PM

Windows

Folder

2025/05/29 02:40:16 PM

DumpStack.log.tmp

8 KB

Hidden file

2025/06/08 12:48:41 PM