Apex Central 2019

Best Practice Guide for Malware Protection

- Apex One™
- Apex One™ (Mac)

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Table of Contents

TrendMicro Apex Central Best Practice Guide for Malware Protection

Apex Central is a security management solution that gives an administrator the ability to control the enterprise products or appliances from a central location --regardless of the program or the appliance's physical location or platform. It allows the formulation of effective deployment and response plans

Policy Management

Policy management allows administrators to enforce product settings on managed products and endpoints from a single management console. They create a policy by selecting the targets and configuring a list of product settings.

Product: **Apex One Security Agent**

Apex One provides the following full-featured product benefits:

- **More efficient use of endpoint resources**

  Delivered via an architecture that uses endpoint resources more effectively and optimizes CPU and network utilization.

- **High-fidelity machine learning (pre-execution and runtime)**

  A blend of threat protection techniques that help eliminate security gaps across any user activity and any endpoint.

- **Behavioral analysis**

  Safeguards against scripts, injection, ransomware, memory and browser attacks.

- **Available as a service**

  Rapid deployment and simplified administration and maintenance with the same comprehensive enterprise threat protection as Trend Micro on-premises Apex One

Powered by the Trend Micro™ Smart Protection Network™, Trend Micro Apex One™ is a centrally managed anti-malware solution that protects endpoints (servers, desktops, and portable endpoints) from a wide variety of Internet threats. An integrated solution, Trend Micro Apex One consists of the Security Agent that resides at the endpoint and the Apex One server that manages all Security Agents.

Security Agents report to the server from which they were installed. They send event information such as threat detection, Security Agent startup, Security Agent shutdown, start of a scan, and completion of an update to the server in real time.

Configuring Scan Method

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Select the Product: **Apex One Security Agent**
4. Create or select the policy created.
5. On targets select Manage Targets and select target Apex One agents.
6. Under Apex One Agent Settings select Scan Methods

7. Select > Smart Scan

Configuring Manual Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Select the Product: **Apex One Security Agent**
4. Create or select the policy created.
5. On targets select Manage Targets and select target Apex One agents.
6. Under Apex One Agent Settings select Manual Scan Settings.
7. File to scan > All scannable files
8. Under Scan Settings checked the following:
   - Scan hidden folders.
   - Scan compressed files. > Maximum layers: 6
   - Scan OLE objects. > Maximum layers: 3
     - Detect exploit code in OLE files.
9. Virus/Malware Scan Settings Only > Scan boot area
10. CPU Usage > Medium: pause slightly between file scans
11. Scan Exclusion > Enable scan exclusion
    - Scan Exclusion list (Directories)
      - Exclude directories where Trend Micro products are installed.
    - Scan Exclusion list (Files)
    - Scan Exclusion list (File Extensions)
12. Configure the Action tab.
13. Virus/Malware > Use a specific action for each virus/malware type:
    - Joke: Quarantine
    - Trojans: Quarantine
    - Virus: Clean & Quarantine
    - Test Virus: Quarantine
    - Packer: Quarantine
    - Probable Malware: Quarantine
    - Other Malware: Clean & Quarantine
14. Checked Back up files before cleaning.
15. Damage Cleanup Services:
    - Cleanup type: Advanced cleanup
    - Enable > Run cleanup when probable virus/malware is detected
16. Spyware/Grayware > Clean: Apex One terminates processes or delete registries, files, cookies and shortcuts.
17. Click Deploy.

Configuring Real-time Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Select the Product: **Apex One Security Agent**
4. Create or select the policy created.
5. On targets select Manage Targets and select target Apex One agents.

6. Under Apex One Agent Settings select Real-time Scan Settings.
7. Enable virus/malware scan and enable spyware/grayware scan.
8. Configure the Target tab.
9. User Activity on Files > Scan files being: created/modified and retrieved
10. Files to Scan > All Scannable files
11. Under Scan Settings:
    - Scan floppy disks during shutdown (if you have still have floppy disk)
    - Scan the boot sector of the USB storage device after plugging in.
    - Scan all files in removable storage device after plugging in.
    - Quarantine malware variants detected in memory.
    - Scan compressed files. > Maximum layers: 3
    - Scan OLE objects. > Maximum layers: 3
        - Detect exploit code in OLE files.
12. Under Virus/Malware Scan Settings Only, enable Intellitrap.
13. Enable CVE exploit scanning for files downloaded through web and email channels.
14. Configure Scan Exclusion tab > Enable scan exclusion
    - Scan Exclusion list (Directories)
        - Exclude directories where Trend Micro products are installed.
    - Scan Exclusion list (Files)
    - Scan Exclusion list (Files Extensions)
15. Configure the Action tab.
16. Virus/Malware > Use a specific action for each virus/malware type:
    - CVE exploit: Quarantine
    - Joke: Quarantine
    - Trojans: Quarantine
    - Virus: Clean & Quarantine
    - Test Virus: Quarantine
    - Packer: Quarantine
    - Probable Malware: Quarantine
    - Other Malware: Clean & Quarantine

18. Back up files before cleaning.
19. Damage Cleanup Services:
    - Enable > Run cleanup when probable virus/malware is detected
20. Spyware/Grayware > Clean: Apex One terminates processes or delete registries, files, cookies and shortcuts.
21. Click Deploy.

Configuring Scheduled Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Select the Product: **Apex One Security Agent**
4. Create or select the policy name created.
5. On targets select Manage Targets and select target Apex One agents.
6. Enable virus/malware scan and enable spyware/grayware scan.
7. Configure the Target tab.
8. Configure Schedule Scan to run at least once a week.
9. Files to Scan > All Scannable Files

10. Under Scan Settings:
    - Scan compressed files. > Maximum layers: 3
    - Scan OLE objects. > Maximum layers: 6
        - o Detect exploit code in OLE files.
11. Virus/Malware Scan Settings Only > Scan boot area
12. CPU Usage > Medium: Pause between file scan if CPU consumption is higher than 50%, and do not pause if 50% or lower.
13. Scan Exclusion > Enable Scan Exclusion
    - Scan Exclusions lists (Directories)
        - Excludes directories where Trend Micro products are installed
    - Scan Exclusions Lists (Files)
    - Scan Exclusions Lists (File Extensions)

14. Configure the Action tab.
15. Virus/Malware > Use a specific action for each virus/malware type
    - Joke: Quarantine
    - Trojans: Quarantine
    - Virus: Clean & Quarantine
    - Test Virus: Quarantine
    - Packer: Quarantine
    - Probable Malware: Quarantine
    - Other Malware: Clean & Quarantine
    - Back up files before cleaning.
    - Damage Cleanup Services:
16. Clean type: Advance Cleanup
17. Enable > Run cleanup when probable virus/malware is detected.
18. Under Spyware/Grayware select Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts.
19. Click Deploy.

Configuring Scan Now Settings

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select Manage Targets and select target Apex One agents.
6. Enable virus/malware scan and enable spyware/grayware scan.
7. Configure the Target tab.
8. Files to Scan > All Scannable files
9. Scan Settings:
    - Scan compressed files. > Maximum layers: 3
    - Scan OLE objects. > Maximum layers: 6
10. Virus/Malware Scan Settings only > Scan boot area
11. CPU Usage > Medium: Pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower
12. Scan Exclusion > Enable Scan exclusion
    - Scan Exclusions lists (Directories)

    - Excludes directories where Trend Micro products are installed
  - Scan Exclusions Lists (Files)
  - Scan Exclusions Lists (File Extensions)

13. Configure the Action tab.
14. Virus/Malware > Use a specific action for each virus/malware type

  - Joke: Quarantine
  - Trojan: Quarantine
  - Virus: Clean & Quarantine
  - Test Virus: Quarantine
  - Packer: Quarantine
  - Probable Malware: Quarantine
  - Other Malware: Clean & Quarantine

15. Backup files before cleaning.
16. Damage Cleanup Services

  - Cleanup type: Advance Cleanup
  - Run cleanup when probable virus/malware is detected.

17. Enable Spyware/Grayware > Clean: Apex One terminates processes or delete registries, files, cookies and shortcuts.
18. Click Deploy.

Table Summary

	Real-time Scan	Manual Scan	Scheduled Scan	Scan Now
Files to scan	All Scannable	All Scannable	All Scannable	All Scannable
Scan hidden folders		✓		
Scan floppy disks during shutdown	✓			
Scan floppy disks during shutdown	✓			
Scan boot sector of USB storage device after plugging in	✓			
Scan all files in removable storage devices after plugging in	✓			
Quarantine malware variants detected in memory	✓			
Scan compressed files*	✓ 3 layers	✓ 6 layers	✓ 6 layers	✓ 6 layers
Scan OLE objects*	✓ 3 layers	✓ 3 layers	✓ 6 layers	✓ 6 layers
Detect exploit code in OLE files	✓	✓	✓	✓
Enable Intellitrap	✓			
Enable CVE exploit scanning for files downloaded through web and email channels	✓			
Scan boot area		✓	✓	✓
CPU usage		Medium	Medium	Medium
Cleanup type for Damage Cleanup Services		Advanced Cleanup	Advanced Cleanup	Advanced Cleanup
Run cleanup for probable virus	✓	✓	✓	✓
Clean action for detected Spyware	✓	✓	✓	✓

NOTE * Administrators can opt to disable/minimize other scanning setting should higher performance is required for those machines.

Enable Web Reputation

Web Reputation Service (WRS) allows Apex One to detect and block access to sites that harbor web-based threats. When an agent requests a URL, it first checks the "reputation score" of the URL by querying the Trend Micro reputation servers. Access to the URL is then allowed or denied depending on the score and the security level you configured.

To configure Web Reputation Service, please do the following:

1. On the Apex Central, log on to the Management Console.

2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or select the policy name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Select the **Web Reputation Settings**

Internal Agents:

- Enable Web Reputation on operating system matching your policy created
- Enable **Check HTTPS URLs**.
- Select **Medium** security level for the policy.
- Under Browser Exploit Prevention, enable **Block pages containing malicious script**.
- For Approved/Blocked URL list, You may add the URL's of the Web sites you want to approve or block. By default, TrendMicro and Microsoft websites are included in the Approved lists.
- Agent Log: Enable allow agents to send logs to Apex One Server. his option to analyze URL's blocked by Web Reputation Service.
- Click **Deploy**

External Agents:

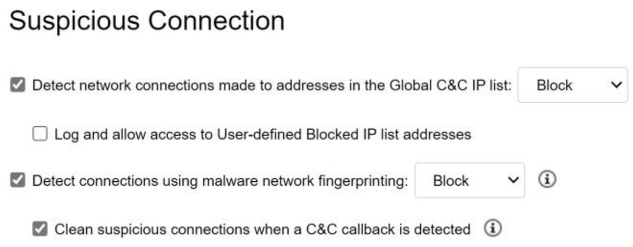
- Enable Web Reputation on operating system matching your policy created
- Enable **Check HTTPS URLs**.
- Select **Medium** security level for the policy.
- Untested URLs. You can use this option to Block pages that have not been tested by Trend Micro
- Under Browser Exploit Prevention, enable **Block pages containing malicious script**.
- For Approved/Blocked URL list, you may add the URL's of the Web sites you want to approve or block. By default, TrendMicro and Microsoft websites are included in the Approved lists.
- Agent Log: Enable allow agents to send logs to Apex One Server. his option to analyze URL's blocked by Web Reputation Service.
- Click **Deploy**.

Configure Global C&C Suspicious Connection Settings

Administrators can configure Apex One to log all connections between agents and confirmed C&C IP addresses. The Trend Micro Command & Control (C&C) Contact Alert Services provides enhanced detection and alert capabilities to mitigate the damage caused by Advanced Persistent Threats (APT) and targeted attacks.

The following are steps on how to configure it:

1. On the Apex Central, log on to the Management console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or select the policy name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Suspicious Connection Settings**.
7. Enable the following:
   - Detect network connections made to addresses in the Global C&C IP list: **Block**
   - Detect connections using malware network fingerprinting: **Block**



Suspicious Connection

☑ Detect network connections made to addresses in the Global C&C IP list: Block

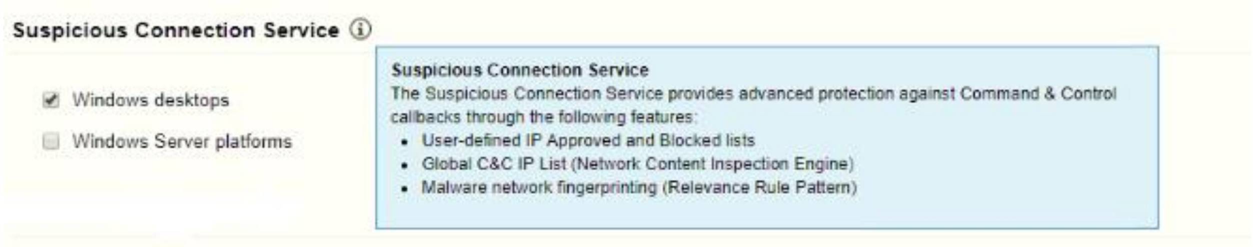
□ Log and allow access to User-defined Blocked IP list addresses

☑ Detect connections using malware network fingerprinting: Block

☑ Clean suspicious connections when a C&C callback is detected

   - Clean suspicious connections when C&C callback is detected

8. Go to **Additional Service Settings**.
9. Under Suspicious Connection Service, select **Windows desktops and Windows Server platforms**.



Suspicious Connection Service

☑ Windows desktops

□ Windows Server platforms

Suspicious Connection Service

The Suspicious Connection Service provides advanced protection against Command & Control callbacks through the following features:

- User-defined IP Approved and Blocked lists
- Global C&C IP List (Network Content Inspection Engine)
- Malware network fingerprinting (Relevance Rule Pattern)

10. Click **Deploy**.

Enable Behavior Monitoring / Ransomware Protection Feature

Apex One constantly monitors computers (or endpoints) for unusual modifications to the operating system or on installed software. Administrators can create exception lists that allow certain programs to start despite violating a monitored change, or completely block certain programs. In addition, programs with a valid digital signature or have been certified are always allowed to start.

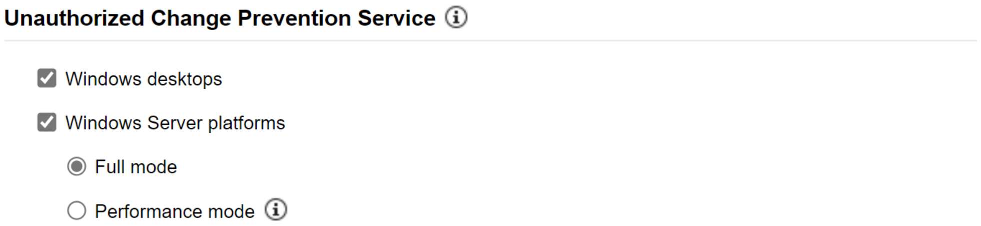
Behavior Monitor requires the following services:

- Unauthorized Change Prevention Service
- Advance Protection Service

Make sure to enable the required services for the appropriate Windows platform in **Additional Service Setting area.**

To enable, follow these steps;

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: Apex One Security Agent
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Additional Service Settings**.
7. Under Unauthorized Change Prevention Service:
    - Check **Enable Windows desktops**.
    - Check **Enable Windows Server Platforms**.
    - **Check Full Mode**



Unauthorized Change Prevention Service ⓘ

☑ Windows desktops

☑ Windows Server platforms

● Full mode

○ Performance mode ⓘ

8. Go to **Advance Protection Service**:

> **NOTE** 🗎 On Windows Server platform, the "Only enable services required by Security Agent Self-protection features" **ONLY** enables the Agent Self-protection. Other Features will be not available

- Check **Enable Windows desktops**.
- Check **Enable Windows Server Platforms**.

9. Click **Deploy**.

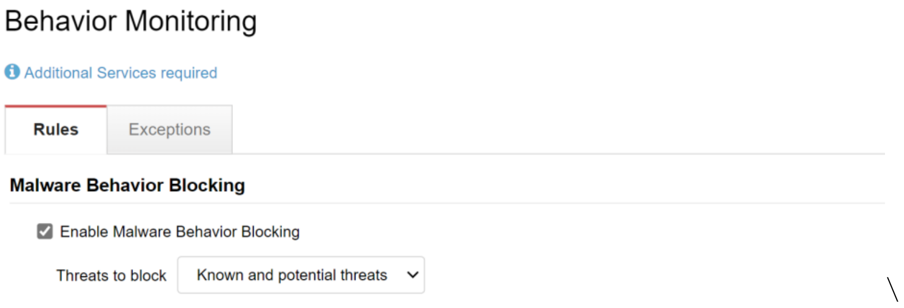
To configure Behavior Monitoring and Ransomware Protection features, please do the following:

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Behavior Monitoring Settings**.

Malware behavior blocking

Malware Behavior Blocking provides a necessary layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time. As programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats.

- Check **Enable Malware Behavior Blocking**.
- Under Threats to block, recommend to select **Known and potential threats**.



Behavior Monitoring

ⓘ Additional Services required

Malware Behavior Blocking

☑ Enable Malware Behavior Blocking

Threats to block: Known and potential threats

Ransomware Protection

Ransomware is a type of malware which restricts access to files and demands payment to restore the affected files. This type of threat can affect multiple files residing on your local and connected drives, it can also affect backups such as shadow copies. Ransomware Protection prevents the unauthorized modification or encryption of files on Apex One agents by "ransomware" threats.

- Check **Protect documents against unauthorized encryption or modification**.
- Check **Automatically backup and restore files changed by suspicious programs**.
- Check **Block processes commonly associated with ransomware**.

NOTE 🗎 To reduce the chance of Apex One detecting a safe process as malicious, ensure that the agent has internet access to perform additional verification processes using Trend Micro servers.

- Check **Enable program inspection to detect and block compromised executable files**.

NOTE 🗎 Program inspection provides increased security if you select "Known and potential threats" in the Threat to block drop-down

Anti-Exploit Protection

Anti-exploit protection works in conjunction with program inspection to monitor the behavior of programs and detect abnormal behavior that may indicate that an attacker has exploited program vulnerability. Once detected, Behavior Monitoring terminates the program processes.

- Check **Terminate programs that exhibit abnormal behavior associated with exploit attacks**.

NOTE 🗎 Anti –exploit Protection requires that you select Enable program inspection to detect and block compromised executable files

Newly Encountered Programs

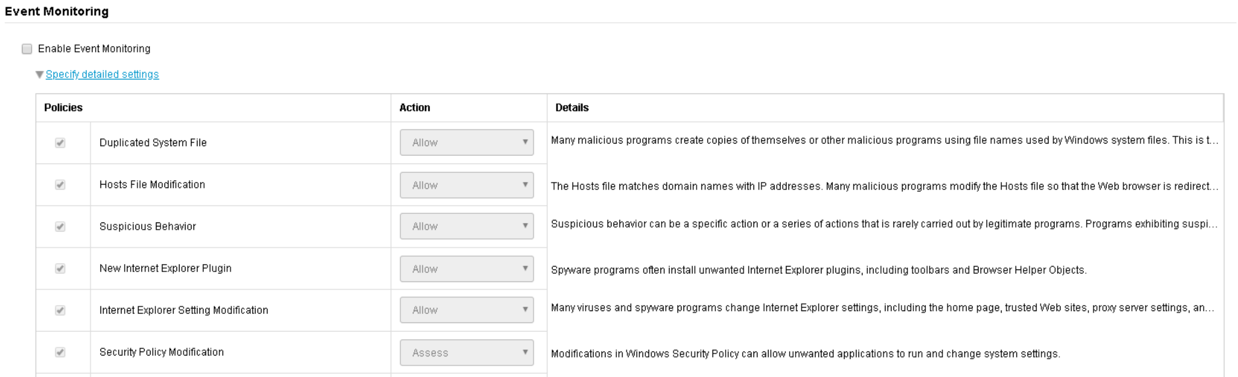
Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file determine by the Smart Protection Network.

- Check **Monitor newly encountered programs downloaded through HTTP or email applications**.
- Recommend to Select **Prompt user**.

NOTE 🗎 This notification requires that Administrators enable Real – time Scan and web Reputation

Event Monitoring

Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks. It monitors system areas for certain events, allowing administrators to regulate programs that trigger such events. Use Event Monitoring if you have specific system protection requirements that are above and beyond what is provided by Malware Behavior Blocking.



Event Monitoring

☐ Enable Event Monitoring

▼ Specify detailed settings

Policies		Action	Details
☑	Duplicated System File	Allow ▾	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is t...
☑	Hosts File Modification	Allow ▾	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the Web browser is redirect...
☑	Suspicious Behavior	Allow ▾	Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspi...
☑	New Internet Explorer Plugin	Allow ▾	Spyware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.
☑	Internet Explorer Setting Modification	Allow ▾	Many viruses and spyware programs change Internet Explorer settings, including the home page, trusted Web sites, proxy server settings, an...
☑	Security Policy Modification	Assess ▾	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.

7. Click **Deploy**.

Enable Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features.

Predictive Machine Learning also performs behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

Before enabling this feature, Predictive Machine Learning requires enabling the following;

- Advance Protection Service
- Unauthorized Change Prevention Service
- Real-Time Scan (For file detections)

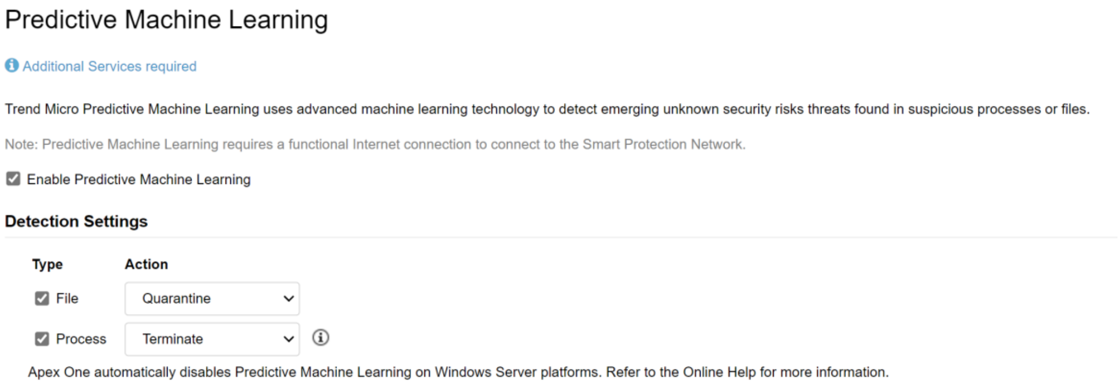
Make sure to enable the required service for appropriate Windows platforms in Additional Service Settings.

NOTE 🗎 Recommended settings for enhance process detection:

- **Enable Web Protection**.
- **Enable Malware Behavior Blocking** and **Enable program inspection to detect and block compromised executable samples**

To enable Predictive Machine Learning:

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Predictive Machine Learning Settings**.
7. Under Detection Settings, select the following:



Predictive Machine Learning

ℹ Additional Services required

Trend Micro Predictive Machine Learning uses advanced machine learning technology to detect emerging unknown security risks threats found in suspicious processes or files.

Note: Predictive Machine Learning requires a functional Internet connection to connect to the Smart Protection Network.

☑ Enable Predictive Machine Learning

Detection Settings

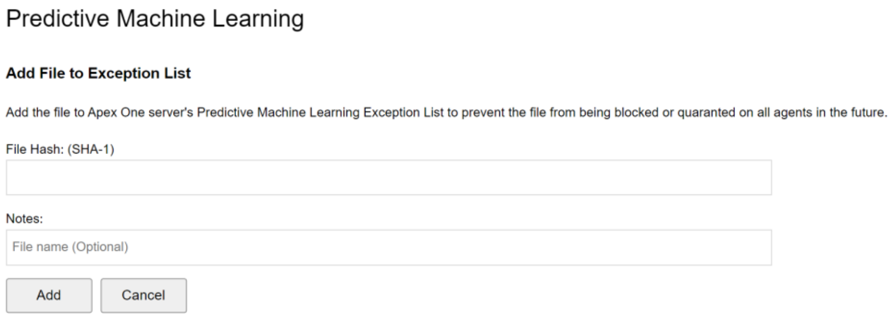
Type	Action
☑ File	Quarantine
☑ Process	Terminate

Apex One automatically disables Predictive Machine Learning on Windows Server platforms. Refer to the Online Help for more information.

- Select to automatically Quarantine files that exhibit malware-related features based on the Predictive Machine Learning analysis.
- Select to automatically Terminate processes that exhibit malware-related behaviors based on the Predictive Machine Learning analysis

NOTE 🗎 Predictive Machine Learning attempts to clean the files that executed the malicious processes If the clean action is unsuccessful, Apex One quarantines the affected files.

8. Under Exceptions, configure the global Predictive Machine Learning file exceptions to prevent all agents from detecting a file as malicious.
9. Click **Add** file hash.



Predictive Machine Learning

Add File to Exception List

Add the file to Apex One server's Predictive Machine Learning Exception List to prevent the file from being blocked or quaranted on all agents in the future.

File Hash: (SHA-1)

Notes:

File name (Optional)

   a. Specify the file SHA-1 hash value to exclude from scanning.
   b. Provide a note regarding the reason from the exception or to describe the file name(s) associate with the hash value. (Optional)
   c. Click **Add**.
10. Apex One will add the file hash to the exception lists.
11. Click **Deploy**.

Fileless Malware Protection settings

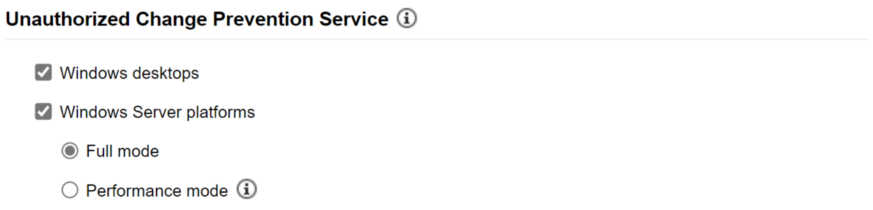
Apex One Agent policies provide increased real-time protection against the fileless attack methods through enhance memory scanning for suspicious process behaviors. Apex One Agents can terminate suspicious processes before any damages can be done.

With Apex One, enhancements are made to detect file-less malware executions. Malware with file-less characteristics only run on memory and uses evasive techniques so minimal trace of it is present on the disk of the affected machine. To fully leverage these protection techniques these features must be enabled:

Required Services

1. Go to **Policies** > **Policy Management**
2. Select the Product: **Apex One Security Agent**
3. Select the policy to which the settings will be applied
4. Go to Additional Service Settings
5. Enable the following:

   - **Unauthorized Change Prevention Service**



Unauthorized Change Prevention Service ⓘ

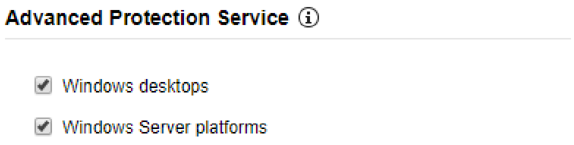
☑ Windows desktops

☑ Windows Server platforms

● Full mode

○ Performance mode ⓘ

- **Advanced Protection Service**



Advanced Protection Service ⓘ

☑ Windows desktops

☑ Windows Server platforms

> **NOTE** 🗎 Administrators can opt to enable the services and features to Windows Server Platforms should higher security is required for those machines.

Enable File-less Malware Solution Features:

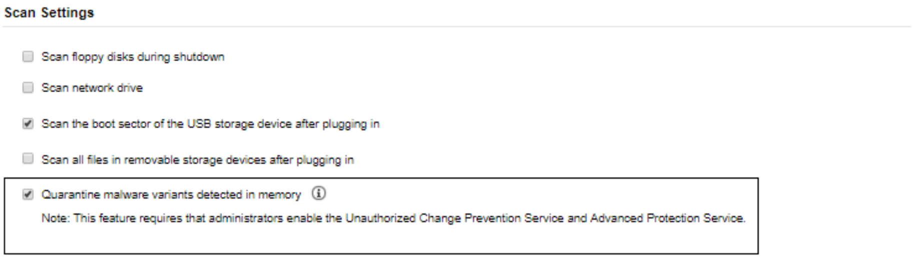
Behavior Monitoring Feature

1. Go to Policies > **Policy Management**
2. Select the Product: **Apex One Security Agent**
3. Select the policy to which the settings will be applied
4. Expand Behavior Monitoring Settings

   a. Check **Enable Behavior Monitoring Settings**
   b. Check **Anti-Exploit Protection**
   c. Check **Enable Program Inspection and Block Compromised Executable Files**

Real Time Scan Settings

1. Go to Policies > **Policy Management**
2. Select the Product: **Apex One Security Agent**
3. Select the policy to which the settings will be applied
4. Expand Real Time Scan Settings
5. Check **Enable Virus/Malware Scan**
6. Select Target
7. Check **Quarantine Malware Variants Detected in Memory**



Scan Settings

☐ Scan floppy disks during shutdown

☐ Scan network drive

☑ Scan the boot sector of the USB storage device after plugging in

☐ Scan all files in removable storage devices after plugging in

☑ Quarantine malware variants detected in memory

Note: This feature requires that administrators enable the Unauthorized Change Prevention Service and Advanced Protection Service.

Predictive Machine Learning

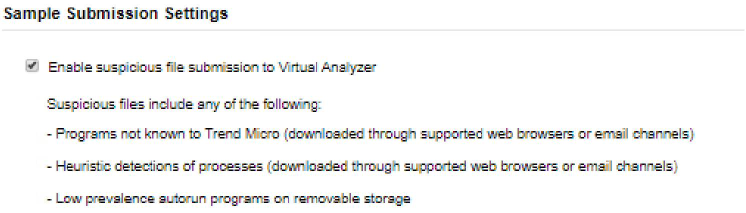
1. Go to Policies > Policy Management
2. Select the Product: **Apex One Security Agent**
3. Select the policy to which the settings will be applied
4. Expand Predictive Machine Learning Settings
5. Check **Enable Predictive Machine Learning**
6. Under Detection Settings
   a. Check **File** for File Scanning and Select **Quarantine** for Action
   b. Check **Process** for Process Scanning and Select **Terminate** for Action

Enable Sample Submission Feature

Configure Apex One agents to submit file objects that may contain previously unidentified threats to Virtual Analyzer for further analysis. Subscription to the Virtual Analyzer allows you to perform sample submission, synchronize suspicious object lists, and take action on user-defined suspicious objects.

To enable Sample Submission Feature:

1. On the Apex Central, log on to the Management console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Sample Submissions**.
7. Under Sample Submission Settings, enable **Suspicious file submissions to Virtual Analyzer**



Sample Submission Settings

☑ Enable suspicious file submission to Virtual Analyzer

Suspicious files include any of the following:

- Programs not known to Trend Micro (downloaded through supported web browsers or email channels)
- Heuristic detections of processes (downloaded through supported web browsers or email channels)
- Low prevalence autorun programs on removable storage

8. Click **Save** to deploy.

NOTE 🗎 Virtual Analyzer requires a valid license for each required product/service or contact your service provider to obtain an Activation Code.

Disabling Independent Mode for Machine in the network

Trend Micro recommends disabling Independent mode for the machines that are in the Local Area Network.

To disable, follow these steps;

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Privileges and Other Settings**.
7. On the Privileges tab under Independent mode, **uncheck** **Enable independent mode** option if enabled for LAN machines. Otherwise, leave it as is.
8. Click **Save** to deploy.

Configure Unload and Unlock protection

This section requires the user to input password when unloading or unlocking the Security Agent.

1. On the Apex Central, log on to the Management console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Privileges and Other Settings**.
7. On the Privileges tab under Unload and Unlock
8. Select Requires a password then input a complex password

Configure Uninstallation protection

This section requires the user to input password when unloading or unlocking the Security Agent.

1. On the Apex Central, log on to the Management console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Privileges and Other Settings**.
7. On the Privileges tab under Uninstallation
8. Select Requires a password then input a complex password

NOTE 🗎 It is recommended to have a different password on Unload and Uninstallation Protection

Configure Device Control

Device Control provides control feature that regulates access to external storage devices and network resources connected to computers. It helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

Device Control requires the following services:

- Unauthorized Change Prevention Service
- Data protection service

Make sure to enable the required services for the appropriate Windows platform in Additional Service Settings.

By default, Device Control Feature is enabled but ALL devices have Full Access. Block Autorun functions on USB devices are also enabled.

To configure Device Control, please do the following;

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Device Control Settings**.
7. Check Enable Device Control for both External and Internal Agents.
8. Click **All Users (default)**
9. Enable Block the Autorun function on USB storage devices.
10. Click **Ok**
11. Click **Save**.

Permissions for Storage devices

- Allow access to USB storage devices, CD/DVD, floppy disks, and network drives. You can grant full access to these devices or limit the level of access. Limiting the level of access brings up “Program lists” which allows programs on storage devices to have Modify, Read and execute, Read and List device content only.
- Configure the list of approved USB storage devices. Device Control allows you to block access to all USB storage devices, except those that have been added to the list of approved devices. You can grant full access to the approved devices or limit the level of access
- Configure the settings according to your preference.

Enabling Endpoint Sensor

Integration with Endpoint Sensor allows you to monitor, record, and perform both current and historical security investigations on your Apex One endpoints. Use the Apex Central console and perform preliminary investigations to locate at-risk endpoints before executing an in-depth Root Cause Analysis to identify the attack vectors.

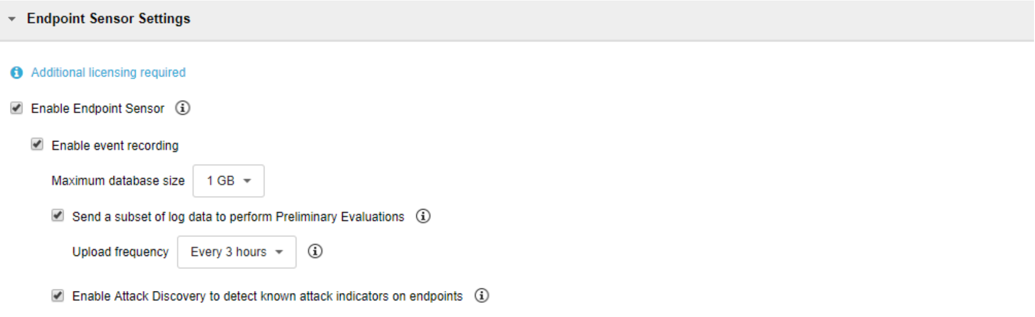
For more information you may refer to [Threat Investigation Overview.]

NOTE 🗎 Endpoint Sensor feature requires special licensing. Make sure that you have the correct license before deploying Endpoint Sensor policies to endpoints. Contact your support provider for more information.

To enable Endpoint Sensor Features, please follow these steps;

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Endpoint Sensor Settings**.
7. Check **Enable Endpoint Sensor**.

Apex Central On-Premise



▾ **Endpoint Sensor Settings**

ⓘ Additional licensing required

☑ Enable Endpoint Sensor ⓘ

☑ Enable event recording

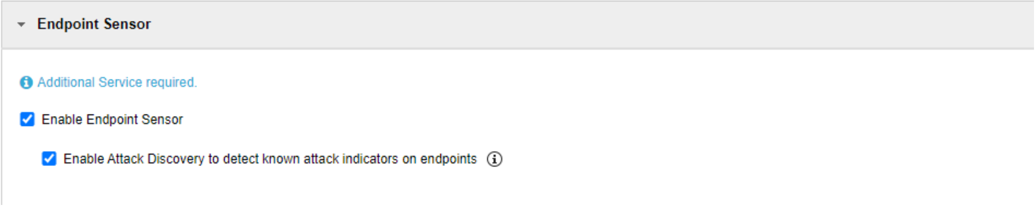
Maximum database size: 1 GB ▾

☑ Send a subset of log data to perform Preliminary Evaluations ⓘ

Upload frequency: Every 3 hours ▾ ⓘ

☑ Enable Attack Discovery to detect known attack indicators on endpoints ⓘ

Apex Central SaaS



▾ **Endpoint Sensor**

ⓘ Additional Service required.

☑ Enable Endpoint Sensor

☑ Enable Attack Discovery to detect known attack indicators on endpoints ⓘ

8. Click **Save** to deploy.

Enabling Application Control Integration

Integration with Application Control provides Apex One users with advanced application blocking and endpoint lockdown capabilities. You can run application inventories and create policy rules that only allow specific applications to execute on your endpoints. You can also create application control rules based on application category, vendor, or version.

Configure Application Control criteria that you can then assign to Security Agent policy rules. You can create "Allow" and "Block" criteria to limit the applications that users can execute or install on protected endpoints. You can also create assessment criteria to monitor the applications executing on endpoints and then refine the criteria based on the usage results.

NOTE 🗎 You must configure Application Control criteria before deploying an Application Control policy to Security Agents.

http://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/policies/policy-resources_001/application-control-.aspx

Each managed product provides different policy settings that you can configure and deploy to policy targets. You can find a complete list of supported managed products and the policy settings for each in the Apex Central as a Service Widget and Policy Management Guide.

You can view the guide using the following link:

http://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service.aspx

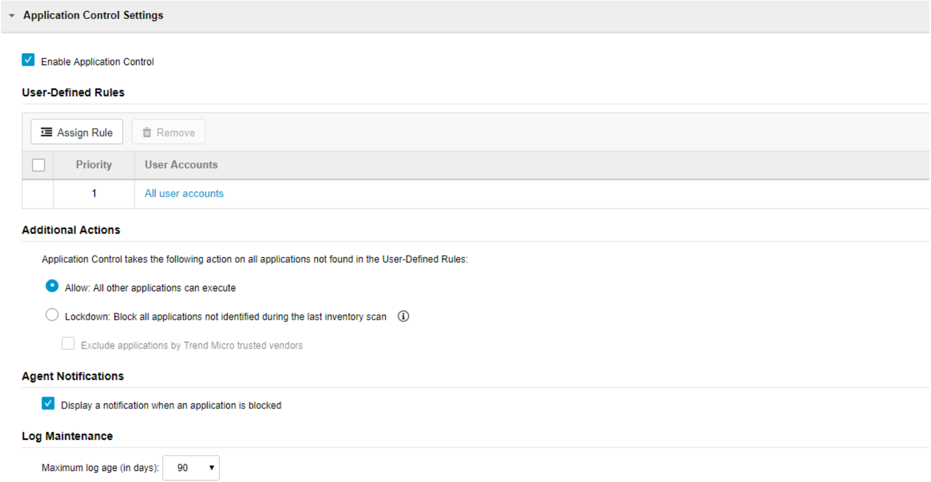
https://docs.trendmicro.com/en-us/enterprise/apex-central.aspx

You can also view the guide online using the following link:

https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-widget-and-policy-management-guide/officescan-agent-pol/application-control-_001/application-control/configuring-applicat.aspx

To enable Application Control, please follow these steps;

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Application Control Settings**.
7. Click **Enable Application Control**.



Application Control Settings

☑ Enable Application Control

User-Defined Rules

□	Priority	User Accounts
	1	All user accounts

Additional Actions

Application Control takes the following action on all applications not found in the User-Defined Rules:

● Allow: All other applications can execute

○ Lockdown: Block all applications not identified during the last inventory scan

□ Exclude applications by Trend Micro trusted vendors

Agent Notifications

☑ Display a notification when an application is blocked

Log Maintenance

Maximum log age (in days): 90

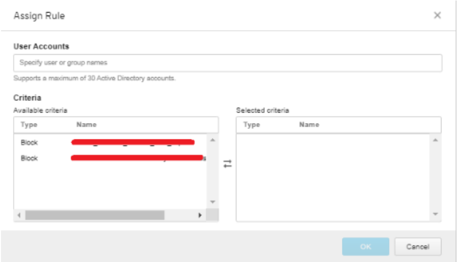
8. Click **Save** to deploy.

Rules and Criteria

A newly deploy application control enable Agent has no other rule to enforce until you create a criteria. That is why, creating criteria is a critical phase of application control deployment because it can cause programs to malfunction if an associated or a subsequent application was inadvertently added to the block criteria of the rule that the AC Agent is using.

Assigning a rule

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Application Control Settings**.
7. Assign Rule
8. Specify user or the group names
9. Select the criteria you want to assign. Click OK



Assign Rule

User Accounts

Specify user or group names

Supports a maximum of 30 Active Directory accounts.

Criteria

Available criteria

Type	Name
Block	[redacted]
Block	[redacted]

Selected criteria

Type	Name

Creating a Criteria

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Resources**.
3. Go to **Application Control Criteria**
4. Add a Criteria (Allow, Block, Import)

Malware Execution Prevention

Malwares or file infectors has to be executed or installed in order to do damage to endpoints. After being downloaded, it scans common folder variables such as %TEMP%, %USERPROFILE%, Startup folders and especially network shares and removable storage to propagate or execute its payloads. By denying execution of any unknown and unwanted applications to these folders, we can ensure that endpoint systems are only allowed to run regular programs and executables that are either approved by the company.

Here's an **example** rule-set we can use as a reference:

Criteria	Match Method	Target
Block	File Paths	- \Users\<user name>\AppData\Local\Temp - \Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup - \<file server>\users\Public\Downloads

Stopping "Drive by Exploit"

Also known as "Drive-by Download". This happens when visiting a website, viewing an email message or when clicking a fraudulent pop-up window that downloads and executes the infected file to the local machine. The following folders are common download and execute locations of this attack:

For Email and Website

%AppData%\Local\Microsoft\Windows\Temporary Internet Files\Content.OUTLOOK

%AppData%\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

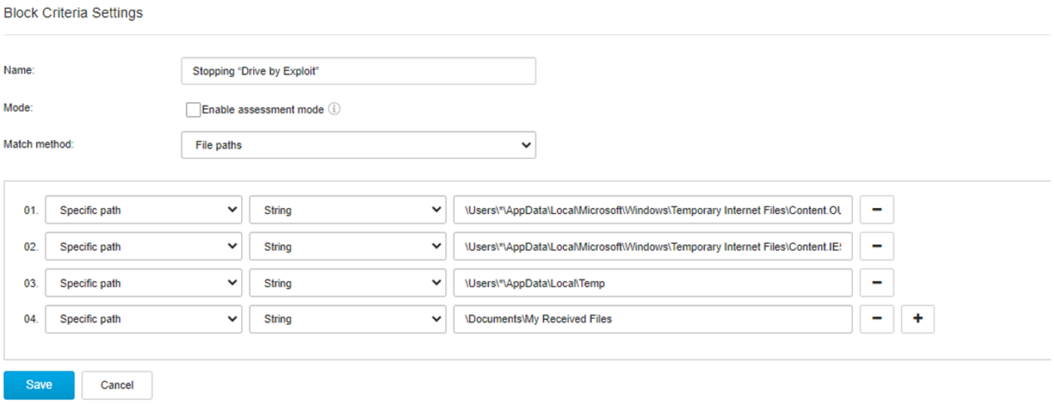
Pop-up Window

%AppData%\Local\Temp

Chat and Instant Messaging

%UserProfile%\Documents\My Received Files

Criteria	Match Method	Target
Block	File Paths	- \Users\<user name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.OUTLOOK - \Users\<user name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 - \Users\<user name>\AppData\Local\Temp - \Documents\My Received Files



Block Criteria Settings

Name:	Stopping "Drive by Exploit"
Mode:	□ Enable assessment mode
Match method:	File paths

01.	Specific path	String	\Users*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.OL
02.	Specific path	String	\Users*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE!
03.	Specific path	String	\Users*\AppData\Local\Temp
04.	Specific path	String	\Documents\My Received Files

NOTE 🗎 Use real "username" and "server name" or the wildcard "*" in <user name> and <file server> to specify actual targets

NOTE 🗎 The "Allow" rules is as important as the "Block" rule in the example rule-set above to make sure that legitimate applications and existing programs of the endpoint can still utilize the folder locations we specified in the blocking rule and avoid unexpected system behavior that could affect end-users' daily task.

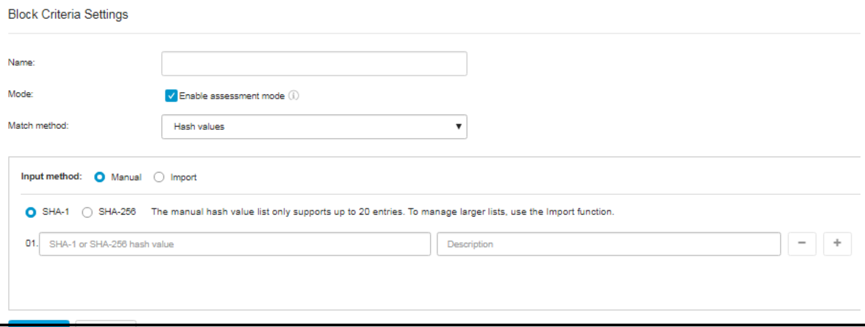
Using Lockdown feature of Application Control

The link below will show the best practice for lockdown mode

https://success.trendmicro.com/solution/1122134-using-the-application-control-lockdown-feature-in-apex-one-as-a-service

Blocked Hash Value

Administrators often tasked to block the IOCs. Application control can block SHA-1 and SHA-256.



Block Criteria Settings

Name:	
Mode:	☑ Enable assessment mode
Match method:	Hash values

Input method: ● Manual ○ Import

● SHA-1 ○ SHA-256 The manual hash value list only supports up to 20 entries. To manage larger lists, use the Import function.

01. SHA-1 or SHA-256 hash value | Description

NOTE 🗎 The manual hash values list can only support up to 20 entries. To manage larger lists, use the import function.

Enabling Vulnerability Protection Settings

Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with recommended Intrusion Prevention rules based on your network performance and security priorities.

To enable Vulnerability Protection service, follow these steps:

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One Security Agent**
4. Create or Select the Policy Name created.
5. On targets select **Manage Targets** and select target Apex One agents.
6. Go to **Vulnerability Protection Settings**.
7. Click **Enable Vulnerability Protection**.
8. Under **Intrusion Prevention Rules** tab go to Mode or Profile and choose between Recommended/Aggressive.

Select **View** > **Default (Enabled)**

NOTE 🗎

Performance Priority – Ensure protection against known Vulnerability Issues

Security Priority – Protect against known Vulnerability Issues and provide enhanced protection against suspicious network activities

It is recommended to choose the **Security Priority**

Frequently Asked Questions (FAQs) about Apex One Vulnerability Protection

https://success.trendmicro.com/solution/1122213-frequently-asked-questions-faqs-about-apex-one-vulnerability-protection

Apex One Managing Server Settings

This setting can only be configured in Apex One Server and cannot be seen in Apex Central

Enable Smart Feedback

Trend Micro Smart Protection Network provides a feedback mechanism to minimize the effort of threats harvesting, analysis and resolving. It not only helps increase the detection rate but also provides a quick real-world scenario. It also benefits customers to help ensure they get the latest protection in the shortest possible time.

To enable Smart Feedback, follow these steps:

1. On the **Apex One**, log on to the Management Console.
2. Go to **Administration**
3. Select **Smart Protection > Smart Feedback**
4. Check **Enable Trend Micro Smart Feedback and Smart Protection Network**.
5. Click **Save**.

Configure Global Agent Settings

Know advanced settings that will apply to all Apex One agents on your network.
To configure Global Agent Settings:

1. On the Apex Central page, go to **Administrations** > **Managed Servers > Server Registration.**
2. From the Server Type drop-down.
3. Select **Apex One**.
4. Click the Apex One server URL
5. The Apex One management console opens.
6. Go to **Agents** and select **Global Agent Settings**.
7. Go to Security Settings >

Scan Settings for Large Compressed Files.

Real-time Scan
Do not scan files if the compressed file size exceeds: **10 MB**
In a compressed file, scan only the first: **30 files**

NOTE 🗎 On certain scenarios, the default value prevents real-time scan from detecting compressed files. You may opt to change the value for performance concerns.

Spyware/Grayware Scan Settings Only

Enable "Scan for Cookies"
Enable "Count cookie into spyware log"

8. Go to **System** tab >

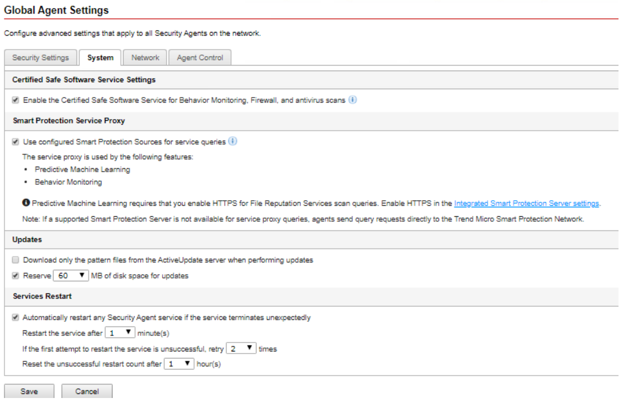
Certified Safe Software Service

Check Enable the Certified Safe Software Service for Behavior Monitoring, Firewall and antivirus scan

Check Use Configured Smart Protection Sources for service queries

NOTE 🗎 This option is not available in SaaS version

Check Automatically restart any Security Agent service if the service terminates unexpectedly.



Global Agent Settings

Configure advanced settings that apply to all Security Agents on the network.

Certified Safe Software Service Settings

☑ Enable the Certified Safe Software Service for Behavior Monitoring, Firewall, and antivirus scans

Smart Protection Service Proxy

☑ Use configured Smart Protection Sources for service queries

The service proxy is used by the following features:

- Predictive Machine Learning
- Behavior Monitoring

Predictive Machine Learning requires that you enable HTTPS for File Reputation Services scan queries. Enable HTTPS in the Integrated Smart Protection Server settings.

Note: If a supported Smart Protection Server is not available for service proxy queries, agents send query requests directly to the Trend Micro Smart Protection Network.

Updates

□ Download only the pattern files from the ActiveUpdate server when performing updates

☑ Reserve 60 ▼ MB of disk space for updates

Services Restart

☑ Automatically restart any Security Agent service if the service terminates unexpectedly

Restart the service after 1 ▼ minute(s)

If the first attempt to restart the service is unsuccessful, retry 2 ▼ times

Reset the unsuccessful restart count after 1 ▼ hour(s)

9. Go to **Network** tab >

Enhanced Encryption of Server-Agent Communication
"AES-256 encryption for communication between the Apex One server and Security agents: **Enabled**"

> **NOTE** 🗎 This option is not available in SaaS version. To know more about the On-Premise AES-256 encryption for communication

10. Click **Save**.

Outbreak Prevention Policy

When an outbreak occurs, enforce outbreak prevention measures to respond to and contain the outbreak

For **On-Premise** Configuration can be found here

For **SaaS** Configuration can be found here

Security Compliance for Unmanaged Endpoint

Security Compliance can query unmanaged endpoints in the network to which the Apex One server belongs.

For **On-Premise** Configuration can be found here

> **NOTE** 🗎 This Unmanaged Endpoint option is not available in SaaS version

Product: Apex One™ (Mac)

Trend Micro Apex One™ (Mac) provides the latest endpoint protection against security risks, blended threats, and platform independent web-based attacks. The Apex One (Mac) server is a plug-in program integrated with Trend Micro products such as Apex One and Worry-free Business Security and installed through the Plug-in Manager framework.

Agent Self-protection

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Agent Self-Protection**
   Select > Protect files used by the agent

Cache Settings for Scans

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Cache Setting for Scans**
   Select > Enable the on-demand scan cache

Configuring Device Control Settings

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select Device Control Settings
   External Agents> Enable Device Control
   Internal Agents> Enable Device Control
   Set the Device Type Permission depending on your preference here.

Configuring Endpoint Sensor Settings

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select Enable Endpoint Sensor
7. Enable eve
8. nt recording
9. Advanced Settings > Send a subset of log data to perform preliminary investigations
10. Upload Frequency:
11. Enable Additional hash types: SHA-256 & MD5

NOTE 🗎 Endpoint Sensor feature requires special licensing. Make sure that you have the correct license before deploying Endpoint Sensor policies to endpoints. Contact your support provider for more information.

Configuring Manual Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Manual Scan Settings**
7. **Target Tab >** File to Scan > **All scannable files**
8. Under Scan Settings >Enabled the following:
    a. Scan compressed files
    b. Scan Time Machine
9. **Action Tab** > Under Action
    a. Use the same action for all security risk types
    b. Select 1st Action: Clean | 2nd Action: Quarantine
10. CPU Usage:
    a. Set to "Low: pause longer between file scans"

Configuring Predictive Machine Learning Setting

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.

3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Predictive Machine Learning Settings**
    a. Enable Predictive Machine Learning

Configuring Real Time Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Real Time Scan Settings**
7. **Target Tab >** File to Scan > **Scan files being created/modified/executed**
8. Under Scan Settings >Enabled the following:
    a. Scan compressed files
9. **Action Tab** > Under Action
    b. Use the same action for all security risk types
    c. Select 1st Action: Clean | 2nd Action: Quarantine
10. Enable “Display a notification message on the endpoint when virus/malware is detected.”

Configuring Scan Method

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Scan Method**

    Select > Smart Scan

Configuring Schedule Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select **Schedule Scan Settings**
7. **Enable schedule Scan**
8. **Target Tab >** Schedule > **Weekly, (depending on preferred day and time)**

   a. **You may schedule the machines per group**

9. File to Scan: All scannable files
10. Under Scan Settings >Enabled the following:
    a. Scan compressed files
    b. Scan Time Machine
11. **CPU Usage:**
    a. Set to "Low: pause longer between file scans"
12. **Action Tab** > Under Action
    a. Use the same action for all security risk types
    b. Select 1st Action: Clean | 2nd Action: Quarantine

Scan Settings Table Summary

	Real-time Scan	Manual Scan	Scheduled Scan
Files to scan	created/modified/executed	All Scannable	All Scannable
Scan compressed files	✓	✓	✓
Scan Time Machine		✓	✓
CPU Usage		✓ Low	
Low: pause longer between file scans		✓	✓

Action Tab	Real-time Scan	Manual Scan	Scheduled Scan
Use the same action for all security risk types	✓	✓	✓
All Types			
1st Action : Clean	✓	✓	✓
2ndst Action : Quarantine	✓	✓	✓
Display a notification message on the endpoint when virus/malware is detected.	✓		

NOTE 🗎 * Administrators can opt to disable/minimize other scanning setting should higher performance is required for those machines.

Configuring Web Reputation Settings

1. On the Apex Central, log on to the Management Console.
2. Go to **Policies** > **Policy Management**.
3. Select the Product: **Apex One (Mac)**
4. Create or select the policy created.
5. On targets select **Manage Targets** and select target Apex One (Mac) agent/s.
6. Under Apex One (Mac) Settings select Web Reputation

External Agents> Enable Web Reputation Policy
Set to Medium
Agent Log: Enable "Allow agents to send logs to the Apex One (Mac) server"
Internal Agents> Enable Web Reputation Policy
Set to Medium
Agent Log: Enable "Allow agents to send logs to the Apex One (Mac) server"

Apex One (Mac) Managing Plugin Settings

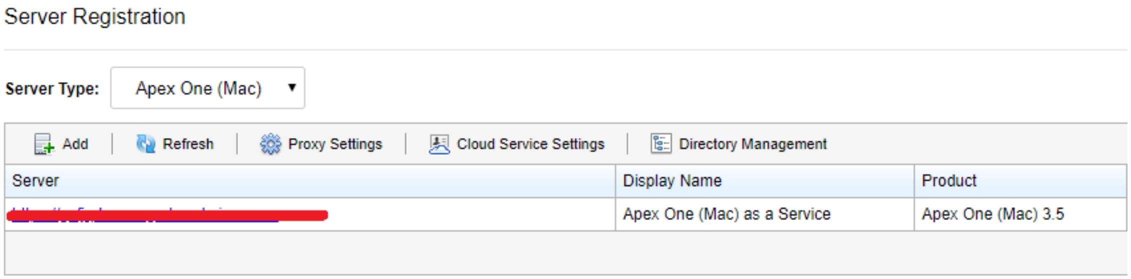
This setting can only be configured in Apex One (Mac) and cannot be set in Apex Central

Enable Smart Feedback

Trend Micro Smart Protection Network provides a feedback mechanism to minimize the effort of threats harvesting, analysis and resolving. It not only helps increase the detection rate but also provides a quick real-world scenario. It also benefits customers to help ensure they get the latest protection in the shortest possible time.

To enable Smart Feedback, follow these steps:

1. On the Apex Central, log on to the Management Console.
2. Go to **Administration** > **Managed Servers > Server Registration**.
3. Select the Server Type: **Apex One (Mac)> Click the server link**

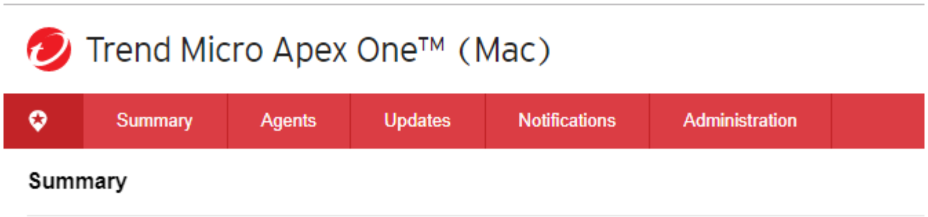


Server Registration

Server Type: Apex One (Mac)

Server	Display Name	Product
[redacted]	Apex One (Mac) as a Service	Apex One (Mac) 3.5

4. Apex One (Mac) Managing Console will open



Trend Micro Apex One™ (Mac)

Summary

5. Go to Administration> Smart Feedback
6. **Check** Enable Trend Micro Smart Feedback

Enable Certified Safe Software Service

The Certified Safe Software Service queries Trend Micro datacenters to verify the safety of a program detected by Malware Behavior Blocking, Event Monitoring, Firewall, or antivirus scans. Enable Certified Safe Software Service to reduce the likelihood of false positive detections.

To enable Certified Safe Software Service, follow these steps:

1. Open the Apex One (Mac) Managing Console
2. Go to Agents> Global Agent Settings> Certified Safe Software Service
3. **Check** Enable Certified Safe Software Service for antivirus scan

Connected Threat Defense

Apex Central brings together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage.

NOTE 🗎 Architecture Required/Optional Product List. See here.

Suspicious Object List

Suspicious objects are known or potentially malicious IP addresses, domains, URLs, and SHA-1 values found during sample analysis.

Apex Central consolidates Virtual Analyzer Suspicious Object lists and synchronizes all Suspicious Object lists among many managed products. The way each managed product implements the lists depends on how the product implements the feature. Refer to your managed product Administrator's Guide for more information about how the product uses and synchronizes the Suspicious Object lists.

Virtual Analyzer Suspicious Object

Managed products that integrate with a Virtual Analyzer submit suspicious files or URLs to Virtual Analyzer for analysis. If Virtual Analyzer determines that an object is a possible threat, Virtual Analyzer adds the object to the Suspicious Object list. Virtual Analyzer then sends the list to its registered Apex Central server for consolidation and synchronization purposes.

User-Defined Suspicious Object

Apex Central administrators can add objects they consider suspicious but are not currently in the list of Virtual Analyzer suspicious objects

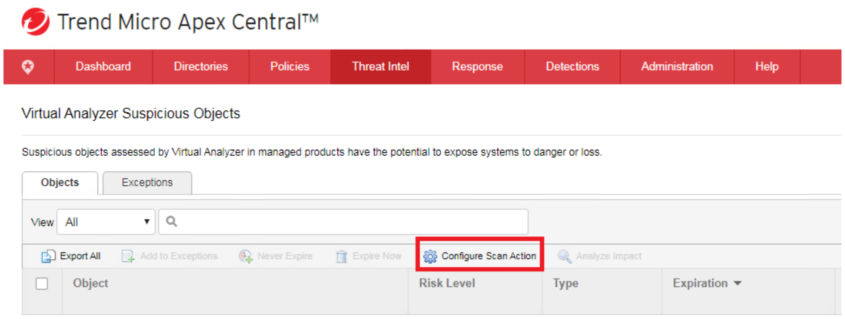
Suspicious Object Scan Action

Using the Apex Central console, administrators can configure scan actions that certain managed products take after detecting specific suspicious objects in the Virtual Analyzer Suspicious Objects list or the User-Defined Suspicious Objects list.

NOTE 🗎 Product Support list Scan Action can be found here.

Configuring Virtual Analyzer Suspicious Object Scan Action

1. On the Apex Central, log on to the Management Console.
2. Go to **Threat Intel> Virtual Analyzer Suspicious Objects**.
3. Select the **Configure Scan Action**



Virtual Analyzer Suspicious Objects

Suspicious objects assessed by Virtual Analyzer in managed products have the potential to expose systems to danger or loss.

4. Set the following Scan Action
   - File Objects: **Quarantine**
   - IP address Objects: **Block**
   - URL Objects: **Block**
   - Domain Objects: **Block**
   - Apply To: **All present and future objects**

> **NOTE** 🗎 You may opt to customize the scan action based on risk level.

Configuring User-Defined Suspicious Object Scan Action

Apex Central provides different ways to protect against suspicious objects not yet identified within your network. Use the User-Defined Suspicious Object list or import indicators from OpenIOC or STIX files to take proactive actions on suspicious threats identified by external sources.

Follow the instruction from the link below for adding SO:

http://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/connected-threat-def_001/preemptive-protectio.aspx

Recommended Scan action as follows:

- File: **Quarantine**
- File Sha-1: **Block**
- IP address: **Block**
- URL: **Block**
- Domain: **Block**

> **NOTE** 🗎 You can block IP, Domain, URL, File and File SHA-1 User-Defined Suspicious Object (UDSO). However, not all products sync and take action against all UDSO. For example, Apex One can only sync and take action against IP, Domain, URL, File but not File SHA-1. See Reference here.

Endpoint Detection & Response

You can now monitor, record, and perform current and historical threat investigations on your endpoints to determine the root cause analysis (RCA) across your entire environment

Use Threat Investigation to locate suspicious objects in the network. If the network is the target of an ongoing attack or an advanced persistent threat (APT), a threat investigation can assess the extent of damage caused by the targeted attack, provide information on the arrival and progression of the attack, and aid in planning an effective security incident response.

- Perform security and threat investigations
- Determine Root Cause Analysis (RCA) across your entire environment
- Easily sweep for malware, registry changes, and other indicators of compromise (IOCs)

You may check the Best Practice guideline using this feature here (page.76).

- Apex One/Office Scan Endpoint Isolation
- Investigate threat in your network
- Suspicious Object and Custom Intelligence with STIX and OpenIOC

NOTE 🗎 This feature requires Apex One Endpoint Sensor. Make sure that you have the correct license. Contact your support provider for more information.

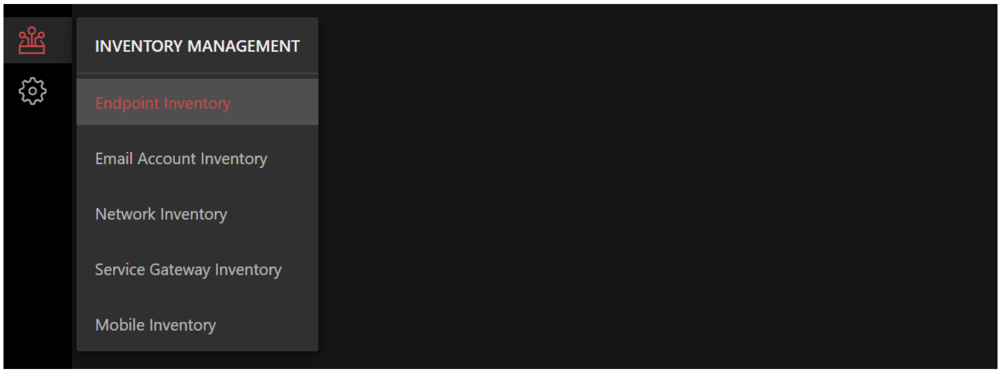
XDR Endpoint Sensor (xES)

XDR Endpoint Sensor is the succeeding version of Apex One Endpoint Sensor which is tightly integrated with Trend Micro Vision One. We encourage to upgrade their existing Apex One Endpoint Sensor to XDR Endpoint Sensor to take advantage of its advance features.

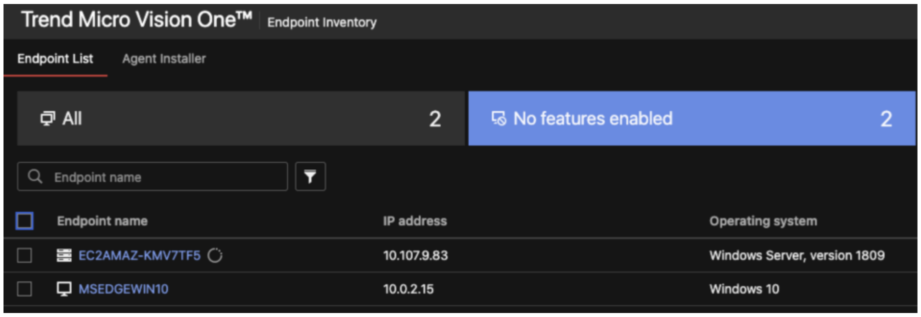
For the platforms that XDR Endpoint Sensor supports, refer to the following link [Trend Micro Vision One System Requirements]

To enable, follow these procedures.

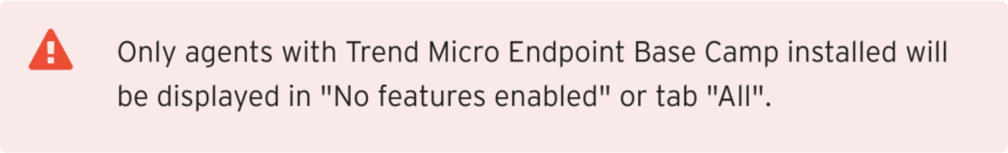
- Login to your **Customer Licensing Portal** Account or **Open Trend Micro Vision One Console**, https://portal.xx.xdr.trendmicro.com/
- Go to **Inventory Management App** and select **Endpoint Inventory**



- Select endpoints directory in tab **No Features Enabled** or tab **ALL**

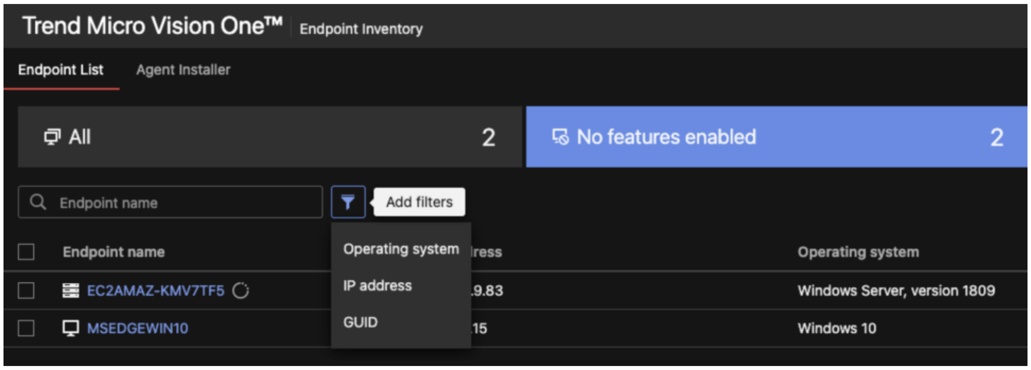


Endpoint name	IP address	Operating system
EC2AMAZ-KMV7TF5	10.107.9.83	Windows Server, version 1809
MSEDGEWIN10	10.0.2.15	Windows 10



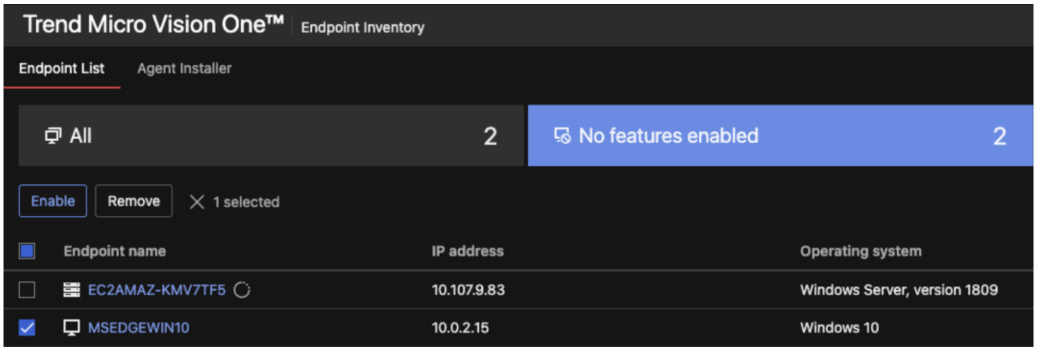
Only agents with Trend Micro Endpoint Base Camp installed will be displayed in "No features enabled" or tab "All".

- Search the endpoints by: (1) Endpoint name, (2) IP Address, (3) Operating System



	Endpoint name	ress	Operating system
□	EC2AMAZ-KMV7TF5	.9.83	Windows Server, version 1809
□	MSEDGEWIN10	15	Windows 10

- Click **Enable**



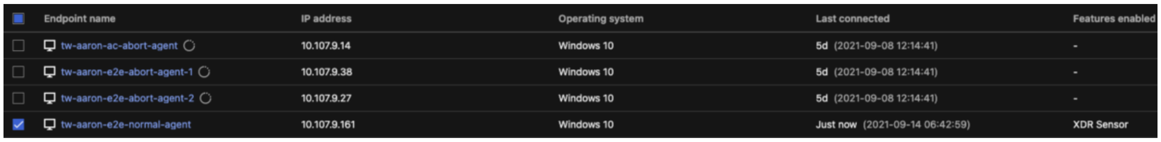
■	Endpoint name	IP address	Operating system
□	EC2AMAZ-KMV7TF5	10.107.9.83	Windows Server, version 1809
☑	MSEDGEWIN10	10.0.2.15	Windows 10

- Wait for the XDR Endpoint Sensor installation to finish
- UI Manual authentication after installation for Mac agents

  Since macOS 10.13, Apple made some restriction on Apps to forcibly ask user to manually allow permission for particular process.

  Check Authorizing the Apex One (Mac) XDR Endpoint Sensor for details about the popup authentication process after the installation of agent.

- After enabling XDR Endpoint Sensor, the agent's "Features enabled" column becomes "XDR Sensor".



■	Endpoint name	IP address	Operating system	Last connected	Features enabled
□	tw-aaron-ac-abort-agent	10.107.9.14	Windows 10	5d (2021-09-08 12:14:41)	-
□	tw-aaron-e2e-abort-agent-1	10.107.9.38	Windows 10	5d (2021-09-08 12:14:41)	-
□	tw-aaron-e2e-abort-agent-2	10.107.9.27	Windows 10	5d (2021-09-08 12:14:41)	-
☑	tw-aaron-e2e-normal-agent	10.107.9.161	Windows 10	Just now (2021-09-14 06:42:59)	XDR Sensor

For more information you may refer to the following link, Upgrading Apex One Endpoint Sensor to XDR Endpoint Sensor

Prevention Recommendation

Windows Platform

Disabling System Restore

On Windows operating systems, System Restore is a feature that restores your computer to a point where it is working fine. System Restore uses the last restore point made as its reference.

1. In Active Directory Users and Computers, navigate to Computer Configuration, Administrative Templates | System | System Restore.
2. Double-click **Turn off System Restore**, set it to Enabled. Click **OK**.
3. Close the policy and exit Active Directory Users and Computers.
4. The changes will take effect on the next policy refresh.

To disable System restore manually on a system, you may refer here:

Disabling Autorun

The AutoRun technology is a Windows® feature Microsoft introduced in Windows 95. It allows Windows Explorer to automatically launch programs from inserted storage drives and other media. Its command is rooted into the applications and can’t be edited by users.

The AUTORUN.INF text file, used for both the AutoRun and AutoPlay features, is placed in the root directory of a volume or storage drive to launch specific applications, such as installation of files. Cybercriminals abuse this technology by using worms that propagate through physical, removable, and network drives and by leaving a file named AUTORUN.INF. This file is used to automatically execute malware each time the infected drive is accessed.

The AutoPlay feature was updated in Windows 7 to address this issue by removing the ability to automatically launch programs from non-optical media such as USB drives.

To disable Autorun:

1. Click **Start** then **Run**.
2. Type “GPEDIT.MSC” then press Enter.
3. Go to **Local Computer Policy** | **Administrative Template** | **System**.
4. On the right pane, double-click **Turn off Autoplay**.
5. When you are in the properties dialog box, click **enabled**.
6. Choose **All drives** from the drop-down list.
7. Click **OK**.

References:

https://support.microsoft.com/en-us/help/967715/how-to-disable-the-autorun-functionality-in-windows

https://technet.microsoft.com/en-us/library/cc731387(WS.10).aspx

https://support.microsoft.com/en-ph/kb/967715

Microsoft Windows Operating systems update

Leverage Windows Server Update Services (WSUS) to distribute updates, keeping windows up-to-date. You may refer to the below article.

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

MacOS Platform

Keeping your Mac up to Date

How to : https://support.apple.com/en-mk/guide/mac-help/mchlpx1065/mac

Don't Disable System Integrity Protection

About System Integrity Protection: https://support.apple.com/en-us/HT204899

Others

Educate users not to click on the links they do not trust

Do not open suspicious links or files especially from instant messengers, emails from unidentified users and from pop-up windows.

You can utilize Trend Micro Phish Insight: https://phishinsight.trendmicro.com/en/