

Trend Micro Apex One™ as a Service

Trend Micro Apex Central™

Trend Micro Apex One™ (Mac)

Best Practice Guide for Malware Protection



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.

Copyright © 2019 Trend Micro Incorporated. All rights reserved.

No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Revision version	Author	Released Date
1.0.0	Mark Tongco	December 17, 2018
1.0.1	Vijay Alvarez	March 26, 2019
1.0.2	Vijay Alvarez	September 27, 2019

Table of Contents

TrendMicro Apex One™ as a Service / Apex One™ Best Practice Guide for Malware Protection	4
Global Policy Management	5
Configuring Scan Method	5
Configuring Manual Scan Settings	5
Configuring Real-time Scan Settings	6
Configuring Scheduled Scan Settings	7
Configuring Scan Now Settings	8
Table Summary	9
Enable Web Reputation	9
Internal Agents:	9
External Agents:	10
Configure Global C&C Suspicious Connection Settings	10
Enable Smart Feedback	11
Enable Behavior Monitoring / Ransomware Protection Feature	12
Malware behavior blocking	13
Ransomware Protection	13
Anti-Exploit Protection	14
Newly Encountered Programs	14
Event Monitoring	14
Enable Predictive Machine Learning	15
Fileless Malware Protection settings	16
Required Services	17
Enable File-less Malware Solution Features:	17
Enable Sample Submission Feature	18
Configure Global Agent Settings	18
Configure Apex One Agent self-protection	19
Configure Device Control	20
Permissions for Storage devices	20
Disabling Independent Mode for Machine in the network	21
Enabling Endpoint Sensor	21
Enabling Application Control Integration	22
Enabling Vulnerability Protection Settings	24
Frequently Asked Questions (FAQs) about Apex One Vulnerability Protection	24

TrendMicro Apex One™ (Mac) for Malware Protection	25
Agent Self-protection.....	25
Cache Settings for Scans	25
Configuring Device Control Settings	25
Configuring Endpoint Sensor Settings	26
Configuring Manual Scan Settings.....	26
Configuring Predictive Machine Learning Setting	26
Configuring Real Time Scan Settings.....	27
Configuring Scan Method.....	27
Configuring Schedule Scan Settings	27
Scan Settings Table Summary.....	28
Configuring Web Reputation Settings	28
Prevention Recommendation	29
Windows Platform	29
Disabling System Restore	29
Disabling Autorun	29
Run Microsoft Baseline Security Analyzer.....	30
MacOS Platform.....	30
Keeping your Mac up to Date	30
Don't Disable System Integrity Protection.....	30
Others.....	30
Educate users not to click on the links they do not trust.....	30

TrendMicro Apex One™ as a Service / Apex One™ Best Practice Guide for Malware Protection

Trend Micro Apex One™ as a Service / Apex One protects endpoints, on or off the corporate network, against malware, Trojans, worms, spyware, and ransomware, with protection that adapts against new unknown variants as they emerge.

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

Global Policy Management

System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console, to ensure consistent enforcement of your organization's virus/malware and content security policies.

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.

To perform policy management on a new managed product or endpoint, move the managed product from the New Entity folder to another folder in the Product Directory structure.

Please refer to this guide on [Policy Management and Deployment](#).

Configuring Scan Method

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Create or select the policy created.
4. On targets select Manage Targets and select target Apex One agents.
5. Under Apex One Agent Settings select Scan Methods
6. 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. Create or select the policy created.
4. On targets select Manage Targets and select target Apex One agents.
5. Under Apex One Agent Settings select Manual Scan Settings.
6. File to scan > All scannable files
7. Under Scan Settings:
 - Scan hidden folders.
 - Scan network drive.
 - Scan compressed files. > Maximum layers : 6
 - Scan OLE objects. > Maximum layers : 3
 - Detect exploit code in OLE files.
8. Virus/Malware Scan Settings Only > Scan boot area
9. CPU Usage > Medium: pause slightly between file scans
10. 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)
11. Configure the Action tab.
12. 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
13. Back up files before cleaning.
 14. Damage Cleanup Services:
 - Cleanup type: Advanced cleanup
 - Enable > Run cleanup when probable virus/malware is detected
 15. Spyware/Grayware > Clean: Apex One terminates processes or delete registries, files, cookies and shortcuts.
 16. 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. Create or select the policy created.
4. On targets select Manage Targets and select target Apex One agents.
5. Under Apex One Agent Settings select Real-time Scan Settings.
6. Enable virus/malware scan and enable spyware/grayware scan.
7. Configure the Target tab.
8. User Activity on Files > Scan files being: created/modified and retrieved
9. Files to Scan > All Scannable files
10. Under Scan Settings:
 - Scan floppy disks during shutdown (if you have still have floppy disk)
 - Scan network drive.
 - 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.
11. Under Virus/Malware Scan Settings Only, enable Intellitrapp.
12. Enable CVE exploit scanning for files downloaded through web and email channels.
13. 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)
14. Configure the Action tab.
15. 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
17. Back up files before cleaning.
 18. Damage Cleanup Services:
 - Enable > Run cleanup when probable virus/malware is detected
 19. Spyware/Grayware > Clean: Apex One terminates processes or delete registries, files, cookies and shortcuts.
 20. Click Deploy.

Configuring Scheduled Scan Settings

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Create or select the policy name created.
4. On targets select Manage Targets and select target Apex One agents.
5. Enable virus/malware scan and enable spyware/grayware scan.
6. Configure the Target tab.
7. Configure Schedule Scan to run at least once a week.
8. Files to Scan > All Scannable Files
9. Under Scan Settings:
 - Scan compressed files. > Maximum layers : 3
 - Scan OLE objects. > Maximum layers : 6
 - Detect exploit code in OLE files.
10. Virus/Malware Scan Settings Only > Scan boot area
11. CPU Usage > Medium: Pause between file scan 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
 - 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:
15. Clean type: Advance Cleanup
16. Enable > Run cleanup when probable virus/malware is detected.
17. Under Spyware/Grayware select Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts.
18. Click Deploy.

Configuring Scan Now Settings

1. On the Apex Central, log on to the Management Console.
2. Go to Policies > Policy Management.
3. Create or Select the Policy Name created.
4. On targets select Manage Targets and select target Apex One agents.
5. Enable virus/malware scan and enable spyware/grayware scan.
6. Configure the Target tab.
7. Files to Scan > All Scannable files
8. Scan Settings:
 - Scan compressed files.
 - Scan OLE objects.
9. Virus/Malware Scan Settings only > Scan boot area
10. CPU Usage > Medium: Pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower
11. 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)
12. Configure the Action tab.
13. 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
14. Backup files before cleaning.
15. Damage Cleanup Services
 - Cleanup type: Advance Cleanup
 - Run cleanup when probable virus/malware is detected.
16. Enable Spyware/Grayware > Clean: Apex One terminates processes or delete registries, files, cookies and shortcuts.
17. 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 network drive	✓	✓		
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 3 layers 3 layers	✓ 6 layers 6 layers	✓ 3 layers 3 layers	✓ 6 layers 6 layers
Scan OLE objects	✓ 3 layers 3 layers	✓ 3 layers 3 layers	✓ 3 layers 3 layers	✓ 3 layers 3 layers
Detect exploit code in OLE files	✓	✓	✓	✓
Enable Intellitrapp	✓			
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	✓	✓	✓	✓

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. Create or select the policy name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Select the **Web Reputation Settings**

Internal Agents:

- 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.
- Select whether to allow agents to send logs to Apex One Server. You can use this option to analyze URL's blocked by Web Reputation Service.
- Click **Deploy**

External Agents:

- 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.
- Select whether to allow agents to send logs to Apex One Server. You can use this 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. Create or select the policy name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Suspicious Connection Settings**.
6. Enable the following:
 - 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 C&C callback is detected

Suspicious Connection Settings

☒ 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

7. Go to **Additional Service Settings**.
8. 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)

9. Click **Deploy**.

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**.

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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Additional Service Settings**.
6. Under Unauthorized Change Prevention Service:
 - Check **Enable Windows desktops**.
 - Check **Enable Windows Server Platforms**.
 - **Uncheck** “Only enable services required by Security Agent Self-protection features”

Unauthorized Change Prevention Service ⓘ

☒ Windows desktops

☒ Windows Server platforms

☐ Only enable services required by Security Agent Self-protection features ⓘ

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

7. Go to **Advance Protection Service**:
 - Check **Enable Windows desktops**.
 - Check **Enable Windows Server Platforms**.
8. 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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. 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 **Know 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

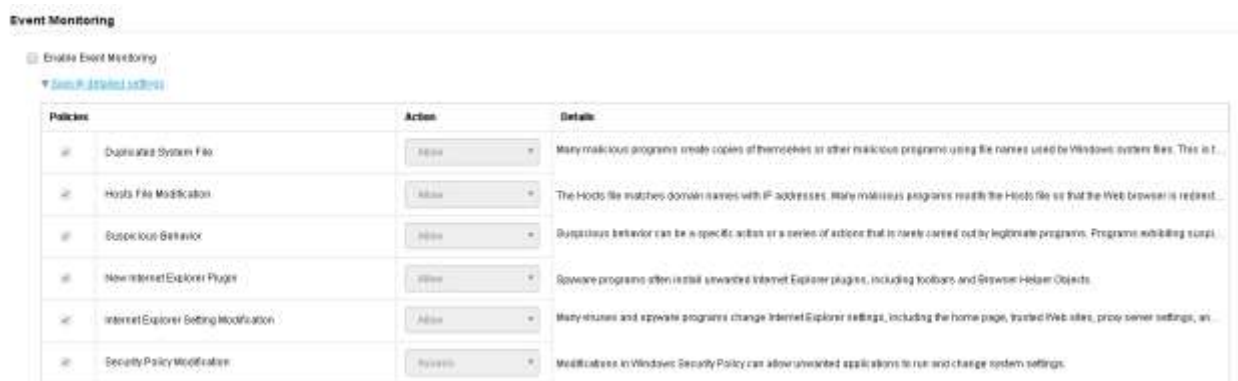
Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file determine by the Smart Protection Network.

- 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.



6. 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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Predictive Machine Learning Settings**.
6. Under Detection Settings, select the following:

Detection Settings

Type	Action
<input checked="" type="checkbox"/> File	Quarantine
<input checked="" type="checkbox"/> 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.

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

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 quarantined on all agents in the future.

File Hash (SHA-1)

Notes

Optional

Add **Cancel**

- Specify the file SHA-1 hash value to exclude from scanning.
 - Provide a note regarding the reason from the exception or to describe the file name(s) associate with the hash value. (Optional)
 - Click **Add**.
- Apex One will add the file hash to the exception lists.
 - 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 policy to which the settings will be applied
3. Go to Additional Service Settings
4. Enable the following:

- **Unauthorized Change Prevention Service**

Unauthorized Change Prevention Service ⓘ

- ☒ Windows desktops
- ☒ Windows Server platforms
- ☐ Only enable services required by Security Agent Self-protection features ⓘ

- **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 policy to which the settings will be applied
3. 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 policy to which the settings will be applied
3. Expand Real Time Scan Settings
4. Check **Enable Virus/Malware Scan**
5. Select Target
6. Check **Quarantine Malware Variants Detected in Memory**



Predictive Machine Learning

1. Go to Policies > Policy Management
2. Select the policy to which the settings will be applied
3. Expand Predictive Machine Learning Settings
4. Check **Enable Predictive Machine Learning**
5. 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

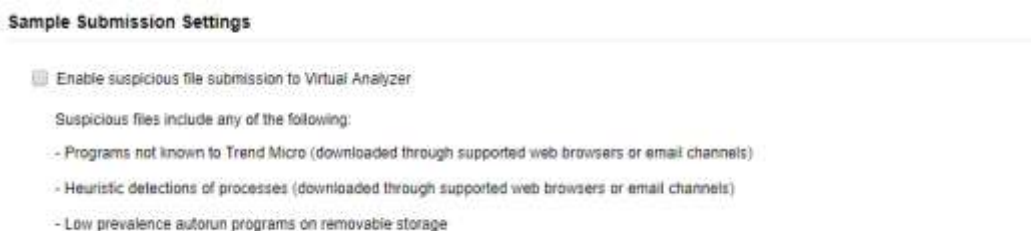
Enable Sample Submission Feature

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

To enable this feature, make sure you have a valid license for each required product/service or contact your service provider to obtain an Activation Code.

To enable Sample Submission Feature:

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



7. Click **Save** to deploy.

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 exceed: **10 MB**

In a compressed file, scan only the first: **10 files**

Manual Scan/Schedule Scan/Scan Now

Do not scan files if the compressed file size exceed: **30 MB**

In a compressed file, scan only the first: **100 files**

Spyware/Grayware Scan Settings Only

Enable “Scan for Cookies”

8. Go to **System** tab. Under Services Area, select **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.

Security Settings **System** Network Agent Control

Certified Safe Software Service Settings

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

Services Restart

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

Restart the service after minute(s)

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

Reset the unsuccessful restart count after hour(s)

Save Cancel

9. Click **Save**.

Configure Apex One Agent self-protection

To enable Sample Submission Feature, please do the following;

1. On the Apex Central, log on to the Management console.
2. Go to **Policies > Policy Management**.
3. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Privileges > Other Settings**.
6. Go to **Other Settings**.
7. Under Security Agent Self-protection, enable the following:

- Protect Security Agent services
- Protect files in the Security Agent installation folder
- Protect Security Agent registry keys
- Protect Security Agent processes



8. Click **Save** to deploy.

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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Device Control Settings**.
6. Check Enable Device Control for both External and Internal Agents.
7. Enable Block the Autorun function on USB storage devices.
8. 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.

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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Privileges > Other Settings**.
6. On the Privileges tab under Independent mode, **uncheck Enable independent mode** option if enabled for LAN machines. Otherwise, leave it as is.
7. Click **Save** to deploy.

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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Endpoint Sensor Settings**.
6. Check **Enable Endpoint Sensor**.

7. 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.

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 download a PDF version of the guide using the following link:

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

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

<http://docs.trendmicro.com/en-us/enterprise/apex-central-as-a-service-online-help-1907/policies/policy-management.aspx>

The following table outlines the tasks available on the Application Control Criteria screen

Task	Description
Add criteria	Click the Add Criteria drop-down button and select from the following options:

	Allow: Click to define "Allow" or "Lockdown" criteria
	For more information, see Defining Allowed Application Criteria.
	Block: Click to define "Block" or "Assessment" criteria
	For more information, see Defining Blocked Application Criteria.
	Copy: Select an existing criteria and click Copy to define new criteria based on the existing settings
	Import: Click to select a ZIP package exported from a compatible Application Control source
	<p>Note:</p> <p>If the imported package contains criteria names that match preexisting criteria, you have the option to Overwrite existing criteria or Skip the import of the criteria with duplicated names.</p>
Export criteria	Select the check box to the left of existing criteria and click Export to save the selected criteria to a ZIP package (<timestamp>_iACRuleExport.zip)
Delete criteria	Select the check box to the left of existing criteria and click Delete to remove the selected criteria from the list
	Warning:
	If you selected criteria used by existing Apex One Security Agent policies, you must confirm that you want to delete and remove the criteria from all affected Security Agent policies. You cannot undo this action.
Modify criteria	Click a Criteria Name to modify the criteria settings
	Note:
	Affected endpoints receive modified criteria settings the next time the Security Agents connect to the server.
View policy associations	Click the value in the Target Policies column to display a list of all Apex One Security Agent policies that implement the criteria.
	Tip:
	Click a policy name to open a new browser tab on which you can view or modify the policy settings.

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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Application Control Settings**.
6. Click **Enable Application Control**.

The screenshot shows the 'Application Control Settings' window. At the top, there's a toggle for 'Enable Application Control'. Below it is the 'User-Defined Rules' section, which includes a table with columns for 'Priority' and 'User Accounts'. A single rule is listed with priority '1' and 'All user accounts'. To the right of the table are 'Assign Rule' and 'Remove' buttons. The 'Additional Actions' section explains that Application Control takes action on applications not found in the User-Defined Rules, with three options: 'Allow' (selected), 'Lockdown' (block applications not identified during the last inventory scan), and 'Exclude' (excludes equipment by Trend Micro-trusted vendors). The 'Agent Notifications' section has a checkbox for 'Display a notification when an application is blocked'. The 'Log Maintenance' section has a dropdown for 'Maximum log age (in days)' set to '00'.

7. Click **Save** to deploy.

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. Create or Select the Policy Name created.
4. On targets select **Manage Targets** and select target Apex One agents.
5. Go to **Vulnerability Protection Settings**.
6. Click **Enable Vulnerability Protection**.
7. Under **Intrusion Prevention** tab go to mode Performance priority, then view.
8. Select **Define by mode** (Enabled).
9. Click **Save** to deploy.

Frequently Asked Questions (FAQs) about Apex One Vulnerability Protection

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

TrendMicro Apex One™ (Mac) for Malware Protection

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 event recording
8. Advanced Settings > Send a subset of log data to perform preliminary investigations
9. Upload Frequency:
10. Enable Additional hash types: SHA-256 & MD5

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 network drive
 - c. 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 network drive	✓	✓	
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			
1 st Action : Clean	✓	✓	✓
2 nd Action : Quarantine	✓	✓	✓
Display a notification message on the endpoint when virus/malware is detected.	✓		

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”

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

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

Run Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations.

1. Download the tool from [Microsoft](#).
2. Refer to this [Microsoft document](#) for more information on Microsoft Baseline Security Analyzer.

MacOS Platform

Keeping your Mac up to Date

How to : <https://support.apple.com/en-mk/guide/mac-help/mchlp1065/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/>