



Trend Micro Apex OneTM as a Service

March 2023

Administrator's Guide

For Enterprise and Medium Business

Trend Micro Incorporated reserves the right to make changes to this document and to the service described herein without notice. Before installing and using the service, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

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

Trend Micro, the Trend Micro t-ball logo, Apex One, OfficeScan, Apex Central, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2022. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM09510/220316

Release Date: April 2022

Protected by U.S. Patent No.: 5,951,698

This documentation introduces the main features of the service and/or provides installation instructions for a production environment. Read through the documentation before installing or using the service.

Detailed information about how to use specific features within the service may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<https://www.trendmicro.com/download/documentation/rating.asp>

Table of Contents

Preface

Preface	v
Apex One Documentation	vi
Audience	vi
Document Conventions	vii
Terminology	viii

Part I: Introducing Apex One as a Service

Chapter 1: Introducing Apex One as a Service

Trend Micro Apex One as a Service	1-2
Features and Benefits	1-2
Trend Micro Smart Protection Network	1-5
The Web Console	1-8

Part II: Security Agent Management

Chapter 2: Security Agent Installation

Security Agent System Requirements	2-2
Agent Packaging Tool	2-25
Security Agent Services	2-26
Security Agent Uninstallation	2-31

Chapter 3: Agent Tree Management

The Apex One Agent Tree	3-2
-------------------------------	-----

Agent Management Screen	3-2
Apex One Domains	3-6

Chapter 4: Security Agent Program Settings

Coexist and Full Feature Security Agent Comparison	4-2
Security Agent Icons	4-5
Global Agent Settings	4-18
Endpoint Location	4-20
Reference Servers	4-22

Part III: Endpoint Protection

Chapter 5: Anti-malware Scanning

Scan Now	5-2
Scan Actions	5-9
Scan Exclusion Support	5-16
Restoring Quarantined Files	5-17

Chapter 6: Apex One Firewall

Apex One Firewall Overview	6-2
Enabling or Disabling the Apex One Firewall on Endpoints ...	6-3
Firewall Policies	6-4
Firewall Profiles	6-11
Configuring Global Firewall Settings	6-16
Configuring Firewall Notifications for Security Agents	6-17
Testing the Apex One Firewall	6-17

Chapter 7: Using Outbreak Prevention

Outbreak Prevention Policies	7-2
Configuring Security Risk Outbreak Prevention	7-8
Disabling Outbreak Prevention	7-9

Part IV: Monitoring Apex One

Chapter 8: Dashboard

Tabs and Widgets	8-2
Summary Tab Widgets	8-6
Data Protection Widgets	8-12
Apex One Widgets	8-14
Management Widget	8-18

Chapter 9: Logs

Viewing Scan Operation Logs	9-2
Viewing Central Quarantine Restore Logs	9-3
Viewing System Event Logs	9-4

Chapter 10: Notifications

Security Agent Notifications	10-2
------------------------------------	------

Part V: Updates and Administration

Chapter 11: Updates

Configuring Scheduled Updates for Security Agents	11-2
Security Agent Update Sources	11-3

Chapter 12: Administrative Settings

Account Management	12-2
Smart Protection	12-3
Notification Settings	12-6
General Administrative Settings	12-6

Part VI: Getting Help

Chapter 13: Technical Support

Troubleshooting Resources	13-2
Contacting Trend Micro	13-3
Sending Suspicious Content to Trend Micro	13-4
Other Resources	13-5

Index

Index	IN-1
-------------	------

Preface

Preface

This document discusses getting started information, agent installation procedures, and Apex One server and agent management.

Topics include:

- *Apex One Documentation on page vi*
- *Audience on page vi*
- *Document Conventions on page vii*
- *Terminology on page viii*

Apex One Documentation

Apex One documentation includes the following:

TABLE 1. Apex One Documentation

DOCUMENTATION	DESCRIPTION
Administrator's Guide	A PDF document that discusses getting started information, Security Agent installation procedures, and Apex One server and agent management
Help	Web-based ASPX or local HTML files that provide "how to's", usage advice, and field-specific information. The Help is accessible from the Apex One server and agent consoles.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

Download the latest version of the PDF documents and readme at:

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

Audience

Apex One documentation is intended for the following users:





- **Apex One Administrators:** Responsible for Apex One management, including the Apex One server and Security Agent installation and management. These users are expected to have advanced networking and server management knowledge.

- End users: Users who have the Security Agent installed on their endpoints. The endpoint skill level of these individuals ranges from beginner to power user.

Document Conventions

The documentation uses the following conventions.

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the Apex One documentation:

TABLE 3. Apex One Terminology

TERMINOLOGY	DESCRIPTION
Security Agent	The Apex One agent program
Apex One	The Trend Micro endpoint security solution that provides the base architecture for the Apex One server
Agent endpoint	The endpoint where the Security Agent is installed
Agent user (or user)	The person managing the Security Agent on the agent endpoint
Server	The Apex One server program
Server computer	The endpoint where the Apex One server is installed
Administrator (or Apex One administrator)	The person managing the Apex One server
Console	The user interface for configuring and managing Apex One server and agent settings The console for the Apex One server program is called "web console", while the console for the Security Agent program is called "Security Agent console".
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
License service	Includes Antivirus, Damage Cleanup Services, and Web Reputation and Anti-spyware—all of which are activated during Apex One server installation
Apex One service	Services hosted through Microsoft Management Console (MMC). For example, <code>ofcservice.exe</code> , the Apex One Master Service.
Program	Includes the Security Agent

TERMINOLOGY	DESCRIPTION
Components	Responsible for scanning, detecting, and taking actions against security risks
Agent installation folder	<p>The folder on the endpoint that contains the Security Agent files. If you accept the default settings during installation, you will find the installation folder at any of the following locations:</p> <p>C:\Program Files\Trend Micro\Security Agent</p> <p>C:\Program Files (x86)\Trend Micro\Security Agent</p>
Dual-stack	<p>Entities that have both IPv4 and IPv6 addresses.</p> <p>For example:</p> <ul style="list-style-type: none">• Endpoints with both IPv4 and IPv6 addresses• Security Agents installed on dual-stack endpoints• Update Agents that distribute updates to agents• A dual-stack proxy server, such as DeleGate, can convert between IPv4 and IPv6 addresses
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

Part I

Introducing Apex One as a Service



Chapter 1

Introducing Apex One™ as a Service

This chapter provides an overview of the Apex One™ as a Service and introduces some key features.

Topics include:

- *Trend Micro™ Apex One™ as a Service on page 1-2*
- *Features and Benefits on page 1-2*
- *Trend Micro™ Smart Protection Network™ on page 1-5*
- *The Web Console on page 1-8*

Trend Micro™ Apex One™ as a Service

Trend Micro Apex One as a Service provides enhanced security against unknown, zero-day, and web-based threats on top of, and alongside, your current endpoint protection solution.

An integrated solution, Apex One consists of the Security Agent program that resides at the endpoint and a server program that manages all Security Agents. The Security Agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every Security Agent.

Apex One is powered by the Trend Micro Smart Protection Network™, a next generation cloud-client infrastructure that delivers security that is smarter than conventional approaches. Unique in-the-cloud technology and a lighter-weight Security Agent reduce reliance on conventional pattern downloads and eliminate the delays commonly associated with desktop updates. Businesses benefit from increased network bandwidth, reduced processing power, and associated cost savings. Users get immediate access to the latest protection wherever they connect—within the company network, from home, or on the go.

Features and Benefits

The following table outlines the key features and benefits provided by the Apex One.

FEATURE	BENEFIT
Ransomware Protection	Enhanced scan features can identify and block ransomware programs that target documents that run on endpoints by identifying common behaviors and blocking processes commonly associated with ransomware programs.

FEATURE	BENEFIT
Connected Threat Defense	<p>Configure Apex One to subscribe to the Suspicious Object lists from the Apex Central server. Using the Apex Central console, you can create customized actions for objects detected by the Suspicious Object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment.</p> <p>You can configure Security Agents to submit file objects that may contain previously unidentified threats to a Virtual Analyzer for further analysis. After assessing the objects, Virtual Analyzer adds any objects found to contain unknown threats to the Virtual Analyzer Suspicious Objects lists and distributes the lists to other Security Agents throughout the network.</p>
Predictive Machine Learning	<p>The Predictive Machine Learning engine can protect your network from new, previously unidentified, or unknown threats through advanced file feature analysis and heuristic process monitoring. Predictive Machine Learning can ascertain the probability that a threat exists in a file and the probable threat type, protecting you from zero-day attacks.</p>
Antivirus / Security Risk Protection	<p>Apex One protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. To contain outbreaks, Apex One enforces outbreak prevention policies and isolates infected computers until they are completely risk-free.</p> <p>Apex One uses smart scan to make the scanning process more efficient. This technology works by off-loading a large number of signatures previously stored on the local endpoint to Smart Protection Sources. Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoint systems is significantly reduced.</p>

FEATURE	BENEFIT
Damage Cleanup Services	<p>Damage Cleanup Services™ cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following:</p> <ul style="list-style-type: none">• Detects and removes live Trojans• Kills processes that Trojans create• Repairs system files that Trojans modify• Deletes files and applications that Trojans drop <p>Because Damage Cleanup Services runs automatically in the background, it is not necessary to configure it. Users are not even aware when it runs. However, Apex One may sometimes notify the user to restart their endpoint to complete the process of removing a Trojan.</p>
Web Reputation	<p>Web Reputation technology proactively protects agent endpoints within or outside the corporate network from malicious and potentially dangerous websites. Web Reputation breaks the infection chain and prevents the downloading of malicious code.</p> <p>Verify the credibility of websites and pages by integrating Apex One with the Trend Micro Smart Protection Network</p>
Apex One Firewall	<p>The Apex One Firewall protects endpoints and servers on the network using stateful inspections and high performance network virus scans.</p> <p>Create rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.</p>

FEATURE	BENEFIT
Data Loss Prevention	<p>Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention allows administrators to:</p> <ul style="list-style-type: none"> • Identify the digital assets to protect • Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email messages and external devices • Enforce compliance to established privacy standards
Device Control	<p>Device Control regulates access to external storage devices and network resources connected to endpoints. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.</p>
Behavior Monitoring	<p>Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software.</p>
Security solution agnostic	<p>agents running in “Coexist” mode are compatible on any supported Windows endpoint, running any endpoint security software.</p>
Software-as-a-Service solution	<p>Because the Apex One server is hosted and managed in the cloud, you do not have the overhead associated with managing local hardware.</p>

Trend Micro™ Smart Protection Network™

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight agents to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

For more information on the Smart Protection Network, visit:

<http://www.smartprotectionnetwork.com>

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation then continues to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Security Agents subject to web reputation policies use Web Reputation Services. Apex One administrators can subject all or several agents to web reputation policies.

Web Blocking List

The Web Blocking List is downloaded by smart protection sources. Security Agents that are subject to web reputation policies do not download the Web Blocking List.



Note

Administrators can subject all or several agents to web reputation policies.

Agents subject to web reputation policies verify a website's reputation against the Web Blocking List by sending web reputation queries to a smart protection source. The agent correlates the reputation data received from the smart protection source with the web reputation policy enforced on the

endpoint. Depending on the policy, the agent will either allow or block access to the site.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat.

By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in the protection of others. Because the gathered threat information is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Samples of information sent to Trend Micro:

- File checksums
- Websites accessed
- File information, including sizes and paths
- Names of executable files

You can terminate your participation to the program anytime from the web console.



Tip

You do not need to participate in Smart Feedback to protect your endpoints. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in Smart Feedback to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

<http://www.smartprotectionnetwork.com>

The Web Console

The web console is the central point for monitoring Apex One throughout the corporate network. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console uses standard Internet technologies, such as JavaScript, CGI, HTML, and HTTPS.

Use the web console to do the following:

- Manage agents installed on networked endpoints
- Group agents into logical domains for simultaneous configuration and management
- Set scan configurations on a single or multiple networked endpoints
- Configure notifications about security risks on the network and view logs sent by agents



Note

The web console does not support Windows 8, 8.1, 10, or Windows Server 2012 in Windows UI mode.

Getting Help

The **Help** menu provides access to the following support information:

- **Contents & Index:** Opens the Online Help
- **Support:** Displays the Trend Micro support web page, where you can submit questions and find answers to common questions about Trend Micro products

- **Threat Encyclopedia:** Displays the Threat Encyclopedia website which is the Trend Micro repository of malware-related information. Trend Micro threat experts regularly publish detections for malware, spam, malicious URLs, and vulnerabilities. The Threat Encyclopedia also explains high-profile web attacks and provides correlated information.
- **Contact Trend Micro:** Displays the Trend Micro **Contact Us** website with information about offices worldwide.
- **About:** Provides an overview of the product, instructions to check component version details, and a link to the Support Intelligence System.

For details, see [Support Intelligence System on page 1-9](#).

Support Intelligence System

Support Intelligence System is a page wherein you can easily send files to Trend Micro for analysis. This system determines the Apex One server GUID and sends that information with the file you send. Providing the Apex One server GUID ensures that Trend Micro can provide feedback regarding the files sent for assessment.

Part II

Security Agent Management



Chapter 2

Security Agent Installation

This chapter outlines the system requirements, installation methods, and uninstallation procedures for the Security Agent program.



Topics include:

- *Security Agent System Requirements on page 2-2*
- *Agent Packaging Tool on page 2-25*
- *Security Agent Services on page 2-26*
- *Security Agent Uninstallation on page 2-31*

Security Agent System Requirements


Windows Endpoint Platforms


Windows 7 (32-bit / 64-bit) Service Pack 1 Requirements

ITEM	REQUIREMENT
Editions <hr/>  Important Service Pack 1 is required.	<ul style="list-style-type: none"> • Home Basic • Home Premium • Ultimate • Professional • Enterprise • Professional for Embedded Systems • Ultimate for Embedded Systems • Thin PC
Processor	<ul style="list-style-type: none"> • Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.

ITEM	REQUIREMENT
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Simple File Sharing disabled • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin



Windows 8.1 (32-bit / 64-bit) Requirements

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • Standard • Pro • Enterprise
Processor	<ul style="list-style-type: none"> • Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/> <p> Note</p> <p>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> <hr/>

ITEM	REQUIREMENT
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin <hr/> <div>  Note Windows UI is not supported. </div>



Windows 10 (32-bit / 64-bit) Requirements

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • Home • Pro • Pro for Workstations • Education • Enterprise
Update support	<ul style="list-style-type: none"> • Windows 10 November 2021 Update (Windows 10 21H2) and earlier
Processor	<ul style="list-style-type: none"> • Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)

ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

Windows 11 (64-bit) Requirements

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Home Pro Education Enterprise
Processor	<ul style="list-style-type: none"> Minimum 2GHz (64-bit) Intel Pentium or equivalent AMD™ 64 processor Intel 64 processor

ITEM	REQUIREMENT
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/> <p> Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p>
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/> <p> Note Windows UI is not supported.</p>

Windows Server Platforms


Windows Server 2008 R2 (64-bit) Platforms

- [Windows Server 2008 R2 on page 2-7](#)
- [Windows Storage Server 2008 R2 on page 2-8](#)
- [Windows HPC Server 2008 R2 on page 2-9](#)

**Note**


For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.

TABLE 2-1. Windows Server 2008 R2

ITEM	REQUIREMENT
Editions (Service Pack 1)	<ul style="list-style-type: none"> • Standard • Enterprise • Datacenter • Web • Server Core
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div>


ITEM	REQUIREMENT
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin

TABLE 2-2. Windows Storage Server 2008 R2

ITEM	REQUIREMENT
Editions (Service Pack 1)	<ul style="list-style-type: none"> • Basic • Standard • Enterprise • Workgroup
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/> <p> Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p>

ITEM	REQUIREMENT
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin

TABLE 2-3. Windows HPC Server 2008 R2


ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • N/A
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div> <hr/>
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin

Windows MultiPoint Server 2010 (64-bit) Platform



Note

For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.


ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> N/A
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div> <hr/>
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin

Windows MultiPoint Server 2011 (64-bit) Platform



Note

For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Standard Premium
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/> <div>  Note <p>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> </div> <hr/>
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin

Windows Server 2012 (64-bit) Platforms

- [Windows Server 2012 on page 2-12](#)
- [Windows Server 2012 R2 on page 2-13](#)
- [Windows Storage Server 2012 on page 2-14](#)
- [Windows Storage Server 2012 R2 on page 2-15](#)
- [Windows MultiPoint Server 2012 on page 2-16](#)
- [Windows Server 2012 Failover Clusters on page 2-17](#)
- [Windows Server 2012 R2 Failover Clusters on page 2-18](#)



Note

For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.

TABLE 2-4. Windows Server 2012

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • Standard • Datacenter • Server Core
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)



ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

TABLE 2-5. Windows Server 2012 R2

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Standard Datacenter Server Core
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)



ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

TABLE 2-6. Windows Storage Server 2012

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Standard Workgroup
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)



ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

TABLE 2-7. Windows Storage Server 2012 R2

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Standard Workgroup
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)



ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

TABLE 2-8. Windows MultiPoint Server 2012

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Standard Premium
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)



ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

TABLE 2-9. Windows Server 2012 Failover Clusters

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> N/A
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)





ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

TABLE 2-10. Windows Server 2012 R2 Failover Clusters

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> N/A
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) Apex One with Endpoint Sensor: <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)

ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/>  Note Windows UI is not supported.

Windows Server 2016 (64-bit) Platforms

- [Windows Server 2016 on page 2-20](#)
- [Windows Server 2016 Failover Clusters on page 2-21](#)
- [Windows Storage Server 2016 on page 2-22](#)



Note

For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.

TABLE 2-11. Windows Server 2016



ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • Standard • Datacenter • Server Core
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/> <p> Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p>
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin <hr/> <p> Note Windows UI is not supported.</p>

TABLE 2-12. Windows Server 2016 Failover Clusters





ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> N/A
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div> <hr/>
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/> <div>  Note Windows UI is not supported. </div> <hr/>

TABLE 2-13. Windows Storage Server 2016

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • Standard • Workgroup
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> • 1.5GB minimum • 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div> <hr/>
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin <hr/> <div>  Note Windows UI is not supported. </div> <hr/>


Windows Server 2019 (64-bit) Platforms




Note

For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.

TABLE 2-14. Windows Server 2019

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> Standard Datacenter Server Core
Processor	<ul style="list-style-type: none"> Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) AMD™ 64 processor Intel 64 processor
RAM	<ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> 2GB minimum (exclusively for Apex One)
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div>

ITEM	REQUIREMENT
Others	<ul style="list-style-type: none"> • Monitor that supports 1024 x 768 resolution at 256 colors or higher • Allow printer/file sharing in the Windows firewall (if enabled) • Enable default local admin <hr/>  Note Windows UI is not supported.

Windows Server 2022 (64-bit) Platforms





Note

For processor and RAM requirements for a specific platform, refer to the Microsoft system requirements for that platform.

TABLE 2-15. Windows Server 2022

ITEM	REQUIREMENT
Editions (no Service Pack required)	<ul style="list-style-type: none"> • Standard • Datacenter • Server Core
Processor	<ul style="list-style-type: none"> • Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended) • AMD™ 64 processor • Intel 64 processor
RAM	<ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One) <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> • 2GB minimum (exclusively for Apex One)

ITEM	REQUIREMENT
Available Disk Space	<ul style="list-style-type: none"> 1.5GB minimum 2.0GB recommended <hr/> <div>  Note If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. </div> <hr/>
Others	<ul style="list-style-type: none"> Monitor that supports 1024 x 768 resolution at 256 colors or higher Allow printer/file sharing in the Windows firewall (if enabled) Enable default local admin <hr/> <div>  Note Windows UI is not supported. </div> <hr/>

Agent Packaging Tool

Use the **Agent Packaging Tool** to update the Security Agent installation package that the Apex One server sends to endpoints. When the server repackages the Security Agent installer, Apex One applies all root domain settings to the new package to ensure that new installations have the most updated settings.



Tip

Trend Micro recommends configuring general agent settings on the root domain and repackaging the Security Agent program before beginning to install agents across your network.

**Note**


Apex One automatically repackages the Security Agent program daily. Check the **Last package generation** time to determine whether to repackage the Security Agent again.

Procedure

1. Go to **Agents > Agent Packaging Tool**.
2. Click **Repackage Now**.
3. After repackaging completes, send the Security Agent installer to users using the Apex Central console.

Security Agent Services

The Security Agent runs the services listed in the following tables. You can view the status of these services from Microsoft Management Console.

SERVICE	FEATURES CONTROLLED
Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)	<ul style="list-style-type: none"> Behavior Monitoring Device Control Certified Safe Software Service <hr/> <div>  Note </div> <p>If this option is enabled, the Security Agent may prevent third-party products from installing successfully on endpoints. If you encounter this issue, you can temporarily disable the option and then re-enable it after the installation of the third-party product.</p>
Apex One NT Firewall (TmPfw.exe)	Apex One Firewall

SERVICE	FEATURES CONTROLLED
Apex One Data Protection Service (dsagent.exe)	<ul style="list-style-type: none"> Data Loss Prevention Device Control
Apex One NT Listener (tmlisten.exe)	Communication between the Security Agent and Apex One server
Apex One NT RealTime Scan (ntrtscan.exe)	<ul style="list-style-type: none"> Real-time Scan Scheduled Scan Manual Scan/Scan Now
Apex One Common Client Solution Framework (TmCCSF.exe)	Advanced Protection Service <ul style="list-style-type: none"> Browser Exploit Prevention Memory Scanning
Trend Micro Advanced Threat Assessment Service (Agent) (ATASAgent.exe)	Advanced Managed Detection and Response tasks and communication
Trend Micro Application Control Service (Agent) (TmIACAgentSvc.exe)	Application Control
<ul style="list-style-type: none"> Trend Micro Endpoint Sensor Engine Wrapper (TMESE.exe) Trend Micro Endpoint Sensor Service (Agent) (TMESC.exe) 	Endpoint Sensor
Trend Micro Vulnerability Protection Service (Agent) (iVPAgent.exe)	Vulnerability Protection
Apex One NT WSC Service (TmWSCSvc.exe)	Reports security status of Apex One Security Agents to Security Center

The following services provide robust protection but their monitoring mechanisms can strain system resources, especially on servers running system-intensive applications:

- Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)
- Apex One NT Firewall (TmPfw.exe)
- Apex One Data Protection Service (dsagent.exe)

For this reason, these services are disabled by default on Windows Server platforms. If you want to enable these services:

- Monitor the system's performance constantly and take the necessary action when you notice a drop in performance.
- For TMBMSRV.exe, you can enable the service if you exempt system-intensive applications from Behavior Monitoring policies. You can use a performance tuning tool to identify system intensive applications.

For desktop platforms, disable the services only if you notice a significant drop in performance.

Excluding Security Agent Services and Processes in Third-Party Applications

The following tables list the process names and full file locations of Security Agent processes that you may need to exclude from third-party applications.

TABLE 2-16. Default Processes

PROCESS	DESCRIPTION	LOCATION
TmListen.exe	Receives commands and notifications from the Apex One server and facilitates communication from the Security Agent to the server	<Agent installation folder> \tmlisten.exe
NTRtScan.exe	Performs Real-time, Scheduled, and Manual Scan on Security Agents	<Agent installation folder> \ntrtscan.exe


PROCESS	DESCRIPTION	LOCATION
TmPfw.exe	Provides packet level firewall and network virus scanning capabilities	<Agent installation folder> \TmPfw.exe
TMBMSRV.exe	<p>Regulates access to external storage devices and prevents unauthorized changes to registry keys and processes</p> <hr/> <p> Note If this option is enabled, the Security Agent may prevent third-party products from installing successfully on endpoints. If you encounter this issue, you can temporarily disable the option and then re-enable it after the installation of the third-party product.</p> <hr/>	<%Program Files (x86) folder%> \Trend Micro\BM \TMBMSRV.exe
TmCCSF.exe	Performs Browser Exploit Prevention and memory scanning	<Agent installation folder>\CCSF \TmCCSF.exe
TmWSCSvc.exe	Reports security status of Apex One Security Agents to Security Center	<Agent installation folder> \TmWSCSvc.exe

TABLE 2-17. Extended Feature Processes

PROCESS	DESCRIPTION	LOCATION
DSAgent.exe	Monitors the transmission of sensitive data and controls access to devices	<%Windows directory%> \system32\dsagent \DSAGENT.exe

PROCESS	DESCRIPTION	LOCATION
ATASAgent.exe	Advanced Managed Detection and Response tasks and communication	<%Program Files (x86) folder%> \Trend Micro \iService\iATAS \ATASAgent.exe
TMiACAgentSvc.exe	Trend Micro Application Control Service (Agent)	<%Program Files (x86) folder%> \Trend Micro \iService\iAC \ac_bin \TMiACAgentSvc.exe
ESEServiceShell.exe	Trend Micro Endpoint Sensor Engine Wrapper	<%Program Files (x86) folder%> \Trend Micro \iService\iES \ESE \ESEServiceShell.exe
ESClient.exe	Trend Micro Endpoint Sensor Service (Agent)	C:\Program Files (x86)\Trend Micro\iService\iES\ESE\ESClient.exe
iVPAgent.exe	Trend Micro Vulnerability Protection Service (Agent)	<%Program Files (x86) folder%> \Trend Micro \iService\iVP \iVPAgent.exe

TABLE 2-18. Additional Protected Processes

PROCESS	LOCATION
ShowMsg.exe	<%Windows directory%>\System32\ShowMsg.exe
TmSSClient.exe	<Agent installation folder>\TmSSClient.exe

PROCESS	LOCATION
LogServer.exe	<Agent installation folder>\Temp\LogServer\LogServer.exe
TmsalInstance64.exe	<Agent installation folder>\CCSF\module\BES\TmsalInstance64.exe
CNTAoSMgr.exe	<Agent installation folder>\CNTAoSMgr.exe
ESEFrameworkHost.exe	<%Program Files (x86) folder%>\Trend Micro\iService\iES\ESEFrameworkHost.exe


Security Agent Uninstallation

The following methods allow you to uninstall the Security Agent from endpoints.

Uninstalling the Security Agent from the Web Console

Uninstall the Security Agent program from the web console. Perform uninstallation only if you encounter problems with the program and then reinstall it immediately to keep the endpoint protected from security risks.

Procedure

1. Go to **Agents > Agent Management**.
2. In the agent tree, click the root domain icon  to include all agents or select specific domains or agents.
3. Click **Tasks > Agent Uninstallation**.
4. On the **Agent Uninstallation** screen, click **Initiate Uninstallation**.

The Security Agents receive the command after polling the server or during the next scheduled update.

The Security Agent Uninstallation Program

The Security Agent uninstallation privilege allows users to uninstall the Security Agent program on local endpoints.

Depending on your configuration, uninstallation may or may not require a password. If a password is required, ensure that you share the password only to users that will run the uninstallation program and then change the password immediately if it has been divulged to other users.

Running the Security Agent Uninstallation Program

Procedure

1. On the Windows **Start** menu, click **Programs > Trend Micro Apex One Security Agent > Uninstall Security Agent**.

You can also perform the following steps:

- a. Click **Control Panel > Uninstall a program**.
 - b. Locate **Trend Micro Apex One Security Agent** and click **Uninstall**.
 - c. Follow the on-screen instructions.
2. If prompted, type the uninstallation password. Apex One notifies the user of the uninstallation progress and completion.



Note

If you installed Data Protection on the agent, you must restart the endpoint to complete the uninstallation process.

Chapter 3

Agent Tree Management

This chapter describes the agent tree, the **Agent Management** screen, and Security Agent domain and grouping options.

Topics include:

- *The Apex One Agent Tree on page 3-2*
- *Agent Management Screen on page 3-2*
- *Apex One Domains on page 3-6*

The Apex One Agent Tree

The Apex One agent tree displays all the agents grouped into domains that the server currently manages. Agents are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

Agent Management Screen

To view this screen, go to **Agents > Agent Management**.

Manage general agent settings and view status information about specific agents (for example, **Logon User**, **IP Address**, and **Connection Status**) on the **Agent Management** screen.

The following table lists the tasks you can perform.

TABLE 3-1. Agent Management Tasks

MENU BUTTON	TASK
Status	View detailed agent information. For more information, see Viewing Security Agent Information on page 3-5 .
Tasks	Perform the following: <ul style="list-style-type: none">• Scan Now For more information, see Configuring Scan Now Settings on page 5-2.• Agent Uninstallation For more information, see Uninstalling the Security Agent from the Web Console on page 2-31.• Central Quarantine Restore For more information, see Restoring Quarantined Files on page 5-17.

MENU BUTTON	TASK
Scan Operation Logs	View the Scan Operation logs. For more information, see Viewing Scan Operation Logs on page 9-2 .
Manage Agent Tree	Manage the agent tree. For more information, see Apex One Domains on page 3-6 .
Export	Export a list of agents to a comma-separated value (.csv) file.

Searching the Agent Tree

Use the search and view features above the Agent Tree (**Agents > Agent Management**) to locate specific endpoints managed by Apex One.

Procedure

- Search for any agent to manage by specifying the agent name in the **Search for endpoints** text box.

A list of results appears in the agent tree. For more search options, click **Advanced Search**.



Note

You must use the Advanced Search feature to locate endpoints using IPv4 addresses.

- Perform an advanced search based on the following criteria:




SECTION	DESCRIPTION
Basic Criteria	<p>Includes basic information about endpoints such as IP address, operating system, domain, MAC address, scan method, and Web Reputation status</p> <ul style="list-style-type: none"> Searching by IPv4 segment requires a portion of an IP address starting with the first octet. The search returns all endpoints with IP addresses containing that entry. For example, typing 10.5 returns all computers in the IP address range 10.5.0.0 to 10.5.255.255. Searching by MAC address requires a MAC address range in hexadecimal notation, for example, 000A1B123C12.
Component Version	Select the check box next to the component name, narrow down the criteria by selecting Earlier than or Earlier than and including , and type a version number. The current version number displays by default.
Status	Includes agent settings






Click **Search** after specifying the search criteria. A list of endpoint names that meet the criteria appears in the agent tree.

Agent Tree Icons

The Apex One agent tree icons provide visual hints that indicate the type of endpoint and the status of Security Agents that Apex One manages.

TABLE 3-2. Apex One Agent Tree Icons


ICON	DESCRIPTION
	Domain
	Root
	Update agent

ICON	DESCRIPTION
	Conventional scan agent
	Smart scan available Security Agent
	Smart scan unavailable Security Agent
	Smart scan available update agent
	Smart scan unavailable update agent

Viewing Security Agent Information

The **View Status** screen displays important information about Security Agents, including privileges, endpoint software details and system events.

Procedure

1. Go to **Agents > Agent Management**.
 2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
 3. Click **Status**.
 4. View status information by expanding the agent endpoint's name. If you selected multiple agents, click **Expand All** to view status information for all the selected agents.
 5. (Optional) Use the **Reset** buttons to set the security risk count back to zero.
-

Apex One Domains

A domain in Apex One is a group of agents that share the same configuration and run the same tasks. By grouping agents into domains, you can configure, manage, and apply the same configuration to all domain members.

You can perform the following tasks when grouping agents in domains:

Adding a Domain

Procedure

1. Navigate to **Agents > Agent Management**.
2. Click **Manage Agent Tree > Add Domain**.
3. Type a name for the domain you want to add.
4. Click **Add**.

The new domain appears in the agent tree.

5. (Optional) Create subdomains.
 - a. Select the parent domain.
 - b. Click **Manage Agent Tree > Add Domain**.
 - c. Type the subdomain name.
-

Deleting a Domain or Agent

Procedure

1. Navigate to **Agents > Agent Management**.
2. In the agent tree, select:

- One or several domains
 - One, several, or all agents belonging to a domain
3. Click **Manage Agent Tree > Remove Domain/Agent**.
 4. To delete an empty domain, click **Remove Domain/Agent**. If the domain has agents and you click **Remove Domain/Agent**, the Apex One server will re-create the domain and group all agents under that domain the next time agents connect to the Apex One server. You can perform the following tasks before deleting the domain:
 - a. Move agents to other domains. To move agents to other domains, drag and drop agents to the destination domains.
 - b. Delete all agents.
 5. To delete a single agent, click **Remove Domain/Agent**.

**Note**

Deleting the agent from the agent tree does not remove the Security Agent from the agent endpoint. The Security Agent can still perform server-independent tasks, such as updating components. However, the server is unaware of the existence of the agent and will therefore not deploy configurations or send notifications to the agent.

Renaming a Domain

Procedure

1. Navigate to **Agents > Agent Management**.
2. Select a domain in the agent tree.
3. Click **Manage Agent Tree > Rename Domain**.
4. Type a new name for the domain.
5. Click **Rename**.

The new domain name appears in the agent tree.

Moving Security Agents to Another Domain or Server

Procedure

1. Navigate to **Agents > Agent Management**.
2. In the agent tree, select one, several, or all agents.
3. Click **Manage Agent Tree > Move Agent**.
4. To move agents to another domain:
 - Select **Move selected agent(s) to another domain**.
 - Select the domain.
 - (Optional) Apply the settings of the new domain to the agents.



Tip

You can also drag and drop agents to another domain in the agent tree.

5. To move agents to another server:
 - Select **Move selected agent(s) to another Apex One server**.
 - Type the server name or IPv4/IPv6 address and HTTP or SSL (443) port number.



Note

If you are moving Security Agents to Apex One as a Service, you can obtain the Apex One as a Service server information by accessing the Apex Central console. Go to **Directories > Product Servers** and, in the **Server Type** drop-down, select **Apex One**.

6. Click **Move**.
-

Chapter 4

Security Agent Program Settings

This chapter describes how the Security Agent communicates with the Apex One server, how to start and stop Security Agent services, and how to configure global Security Agent settings.

Topics include:

- *Coexist and Full Feature Security Agent Comparison on page 4-2*
- *Security Agent Icons on page 4-5*
- *Global Agent Settings on page 4-18*
- *Endpoint Location on page 4-20*
- *Reference Servers on page 4-22*

Coexist and Full Feature Security Agent Comparison

The following tables compare the features available for Security Agents configured in coexist mode and full feature set mode.



Important

When deploying settings to domains that contain both coexist mode and fully-featured Security Agents, Security Agents can only receive settings applicable to the configured mode. If you deploy Data Loss Prevention policies to a mixed domain, only the Security Agents in fully-featured mode can apply the policies. The coexist mode Security Agents ignore the Data Loss Prevention policy settings.

TABLE 4-1. Global Agent Settings

SETTING	FULL FEATURE MODE	COEXIST MODE
Security Settings		
Scan Settings	Configurable	-
Scheduled Scan Settings	Configurable	-
Firewall Settings	Configurable	-
Suspicious Connection Settings	Configurable	-
Behavior Monitoring Settings	Configurable	-
System		
Certified Safe Software Service Settings	Configurable	-
Services Restart	Configurable	-
Network		

SETTING	FULL FEATURE MODE	COEXIST MODE
Virus/Malware Log Bandwidth Settings	Configurable	Configurable
Server Polling Interval	Configurable	Configurable
Agent Control		
General Settings	Configurable	-
Alert Settings	Configurable	-
Agent Language Configuration	Configurable	Configurable

**Note**

Most Global Agent Settings have been moved to the Apex Central as a Service console. To manage Global Agent Settings for Apex One, go to Apex Central as a Service (**Policies > Policy Management**).

You can still manage Suspicious Connection Settings using the Apex One console to allow, block, or log all connections between Security Agents and user-defined C&C IP addresses.

For more information, go to [Global Agent Settings on page 4-18](#).

TABLE 4-2. Agent Features/Settings in Apex Central

SETTING	FULL FEATURE MODE	COEXIST MODE
Scan Settings	Configurable	-
Web Reputation Settings	Configurable	Configurable
Predictive Machine Learning Settings	Configurable	Configurable
Suspicious Connection Settings	Configurable	-
Behavior Monitoring Settings	Configurable	-




SETTING	FULL FEATURE MODE	COEXIST MODE
Device Control Settings	Configurable	-
DLP Settings	Configurable	-
Sample Submission	Configurable	-
Update Agent Settings	Configurable	-
Privileges and Other Settings	Configurable	Partially configurable Privilege Settings: <ul style="list-style-type: none"> • Independent Mode • Proxy Settings • Component Updates • Unload and Unlock • Uninstallation Other Settings: <ul style="list-style-type: none"> • Update Settings • Web Reputation Settings • C&C Contact Alert Settings • Predictive Machine Learning Settings • Security Agent Access Restriction • Restart Notification
Additional Service Settings	Configurable	Partially configurable: <ul style="list-style-type: none"> • Advanced Protection Service
Spyware/Grayware Approved List	Configurable	-
Trusted Program List	Configurable	-



SETTING	FULL FEATURE MODE	COEXIST MODE
Export Settings	Configurable	-
Import Settings	Configurable	-






Security Agent Icons



The Security Agent icon in the system tray provide visual hints that indicate the current status of the Security Agent and prompt users to perform certain actions. At any given time, the icon will show a combination of the following visual hints.

TABLE 4-3. Security Agent Status as Indicated in the Security Agent Icon

AGENT STATUS	DESCRIPTION	VISUAL HINT
Agent connection with the Apex One server	Online agents are connected to the Apex One server. The server can initiate tasks and deploy settings to these agents	<p>The icon contains a symbol resembling a heartbeat.</p>  <p>The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.</p>
	Offline agents are disconnected from the Apex One server. The server cannot manage these agents.	<p>The icon contains a symbol resembling the loss of a heartbeat.</p>  <p>The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.</p>
	Independent agents may or may not be able to communicate with the Apex One server.	<p>The icon contains the desktop and signal symbols.</p>  <p>The background color is a shade of blue or red, depending on the status of the Real-time Scan Service.</p>

AGENT STATUS	DESCRIPTION	VISUAL HINT
Availability of smart protection sources	Smart protection sources include Smart Protection Servers and Trend Micro Smart Protection Network.	The icon includes a check mark if a smart protection source is available. 
	Conventional scan agents connect to smart protection sources for web reputation queries.	The icon includes a progress bar if no smart protection source is available and the agent is attempting to establish connection with the sources. 
	Smart scan agents connect to smart protection sources for scan and web reputation queries.	For conventional scan agents, no check mark or progress bar appears if web reputation has been disabled on the agent.





AGENT STATUS	DESCRIPTION	VISUAL HINT
Real-time Scan Service status	<p>Apex One uses the Real-time Scan Service not only for Real-time Scan, but also for Manual Scan and Scheduled Scan.</p> <p>The service must be functional or the agent becomes vulnerable to security risks.</p>	<p>The entire icon is shaded blue if the Real-time Scan Service is functional. Two shades of blue are used to indicate the of the agent.</p> <ul style="list-style-type: none"> For conventional scan:  For smart scan: 
		<p>The entire icon is shaded red if the Real-time Scan Service has been disabled or is not functional.</p> <p>Two shades of red are used to indicate the scan method of the agent.</p> <ul style="list-style-type: none"> For conventional scan:  For smart scan: 
Real-time Scan status	<p>Real-time Scan provides proactive protection by scanning files for security risks as they are created, modified, or retrieved.</p>	<p>There are no visual hints if Real-time Scan is enabled.</p>
		<p>The entire icon is surrounded by a red circle and contains a red diagonal line if Real-time Scan is disabled.</p> 

AGENT STATUS	DESCRIPTION	VISUAL HINT
Pattern update status	Agents must update the pattern regularly to protect the agent from the latest threats.	There are no visual hints if the pattern is up-to-date or is slightly out-of-date.
		<p>The icon includes an exclamation mark if the pattern is severely outdated. This means that the pattern been not been updated for a while.</p> 
Apex One server trial license status	Online agents are connected to an Apex One server that is using an expired trial license.	<p>This icon indicates that the trial license on the Apex One server has expired.</p> 



Smart Scan Icons

Any of the following icons displays when Security Agents use smart scan.

TABLE 4-4. Smart Scan Icons

ICON	CONNECTION WITH APEX ONE SERVER	AVAILABILITY OF SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN
	Online	Available	Functional	Enabled
	Online	Available	Functional	Disabled
	Online	Available	Disabled or not functional	Disabled or not functional
	Online	Unavailable, reconnecting to sources	Functional	Enabled





ICON	CONNECTION WITH APEX ONE SERVER	AVAILABILITY OF SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN
	Online	Unavailable, reconnecting to sources	Functional	Disabled
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional
	Offline	Available	Functional	Enabled
	Offline	Available	Functional	Disabled
	Offline	Available	Disabled or not functional	Disabled or not functional
	Offline	Unavailable, reconnecting to sources	Functional	Enabled
	Offline	Unavailable, reconnecting to sources	Functional	Disabled
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional
	Independent	Available	Functional	Enabled
	Independent	Available	Functional	Disabled
	Independent	Available	Disabled or not functional	Disabled or not functional
	Independent	Unavailable, reconnecting to sources	Functional	Enabled











ICON	CONNECTION WITH APEX ONE SERVER	AVAILABILITY OF SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN
	Independent	Unavailable, reconnecting to sources	Functional	Disabled
	Independent	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional











Conventional Scan Icons



Any of the following icons displays when Security Agents use conventional scan.









TABLE 4-5. Conventional Scan Icons

ICON	CONNECTION WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Online	Available	Functional	Enabled	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Online	Available	Functional	Enabled	Severely outdated
	Online	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated






ICON	CONNECTI ON WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Online	Available	Functional	Disabled	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Online	Available	Functional	Disabled	Severely outdated
	Online	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Online	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Online	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Available	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated

ICON	CONNECTI ON WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Offline	Available	Functional	Enabled	Severely outdated
	Offline	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Offline	Available	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Available	Functional	Disabled	Severely outdated
	Offline	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Offline	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Offline	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated

ICON	CONNECTION WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Independent	Available	Functional	Enabled	Up-to-date or slightly outdated
	Independent	Unavailable, reconnecting to sources	Functional	Enabled	Up-to-date or slightly outdated
	Independent	Available	Functional	Enabled	Severely outdated
	Independent	Unavailable, reconnecting to sources	Functional	Enabled	Severely outdated
	Independent	Available	Functional	Disabled	Up-to-date or slightly outdated
	Independent	Unavailable, reconnecting to sources	Functional	Disabled	Up-to-date or slightly outdated
	Independent	Available	Functional	Disabled	Severely outdated
	Independent	Unavailable, reconnecting to sources	Functional	Disabled	Severely outdated
	Independent	Available	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Independent	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated

ICON	CONNECTI ON WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Independe nt	Available	Disabled or not functional	Disabled or not functional	Severely outdated
	Independe nt	Unavailable, reconnecting to sources	Disabled or not functional	Disabled or not functional	Severely outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Severely outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Severely outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Online	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Severely outdated







ICON	CONNECTI ON WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Severely outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Offline	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Severely outdated
	Indepe ndent	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Up-to-date or slightly outdated

ICON	CONNECTI ON WITH APEX ONE SERVER	WEB REPUTATION SERVICES PROVIDED BY SMART PROTECTION SOURCES	REAL-TIME SCAN SERVICE	REAL-TIME SCAN	VIRUS PATTERN
	Independe nt	Not applicable (Web reputation feature disabled on agent)	Functional	Enabled	Severely outdated
	Independe nt	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Up-to-date or slightly outdated
	Independe nt	Not applicable (Web reputation feature disabled on agent)	Functional	Disabled	Severely outdated
	Independe nt	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Up-to-date or slightly outdated
	Independe nt	Not applicable (Web reputation feature disabled on agent)	Disabled or not functional	Disabled or not functional	Severely outdated

Security Agent Icons (Coexist)

The Security Agent icon in the system tray provides visual hints that indicate the current status of the Security Agent program and prompts users to perform certain actions.

TABLE 4-6. Coexist Mode Agent Icons

ICON	DESCRIPTION
	<ul style="list-style-type: none"> The Security Agent is online. Predictive Machine Learning is enabled and functioning properly. The Security Agent is connected to the Trend Micro Smart Protection Network.
	<ul style="list-style-type: none"> The Security Agent is attempting to reconnect to the Trend Micro Smart Protection Network. The Security Agent is offline. Predictive Machine Learning is enabled.
	<ul style="list-style-type: none"> The Security Agent is online. Predictive Machine Learning is disabled.
	<ul style="list-style-type: none"> The Security Agent is offline. Predictive Machine Learning is disabled. The Security Agent cannot connect to the Trend Micro Smart Protection Network.
	<ul style="list-style-type: none"> The Security Agent is online. Predictive Machine Learning is not functional or a process is unavailable.
	<ul style="list-style-type: none"> The Security Agent is offline. Predictive Machine Learning is not functional or a process is unavailable. The Security Agent cannot connect to the Trend Micro Smart Protection Network.

Global Agent Settings

Most Global Agent Settings have been moved to the Apex Central as a Service console. To manage Global Agent Settings for Apex One, go to Apex Central as a Service (**Policies > Policy Management**).

You can still manage Suspicious Connection Settings using the Apex One console to allow, block, or log all connections between Security Agents and user-defined C&C IP addresses.

To configure Suspicious Connection Settings, complete the following steps:

Procedure

1. Go to **Agents > Global Agent Settings**.
2. Click the **Security Settings** tab.
3. Go to the **Suspicious Connection Settings** section.
4. Click **Edit User-defined IP List**.



Note

The User-defined IP Lists only support IPv4 addresses.

5. On the **Approved List** or **Blocked List** tab, add the IP addresses that you want to monitor.
 - a. Click **Add**.
 - b. On the new screen that appears, type the IP address, IP address range, or IPv4 address and subnet mask for Apex One to monitor.
 - c. Click **Save**.
 6. To remove IP addresses from the list, select the check box next to the address and click **Delete**.
 7. After configuring the lists, click **Close** to return to the **Global Agent Settings** screen.
 8. Click **Save** to deploy the updated list to agents.
-

Enabling Client Authentication Checksum Security

To enhance communication security between the Apex One server and Security Agents, you can enable Client Authentication Checksum (CAC) security in Apex One to authenticate Security Agents.



WARNING!

Before enabling Client Authentication Checksum (CAC) security, verify that all managed Security Agents reporting to the Apex One server are running supported versions (build version 12000 or later).

Procedure

1. Go to **Agents > Global Agent Settings**.
 2. Click the **Network** tab.
 3. Go to the **Server-Agent Communication** section.
 4. Click **Change** to enable or disable the setting.
A message appears.
 5. Click **Verify Versions** to confirm that you have updated all Security Agents to the supported versions (build version 12000 or later).
 6. Click **OK**.
-

Endpoint Location

Apex One provides a location awareness feature that determines whether the Security Agent is in the internal or external network. Location awareness is leveraged in the following Apex One features and services:

- Web Reputation
- Data Loss Prevention

- Device Control

The location of the Security Agent determines whether the Security Agent applies internal or external policy settings. Administrators typically enforce a stricter policy for external Security Agents.

Location Criteria

Specify whether location is based on the Security Agent endpoint's gateway IP address or the Security Agent's connection status with the Apex One server or any reference server.

- **Agent connection status:** If the Security Agent can connect to the Apex One server or any of the assigned reference servers on the Internet, the endpoint's location is internal. Additionally, if any endpoint outside the corporate network can establish connection with the Apex One server/reference server, its location is also internal. If none of these conditions apply, the endpoint's location is external.
- **Gateway IP and MAC address:** If the Security Agent endpoint's gateway IP address matches any of the gateway IP addresses you specified on the **Endpoint Location** screen, the endpoint's location is internal. Otherwise, the endpoint's location is external.

Configuring Location Settings

Procedure

1. Go to **Agents > Endpoint Location**.
2. Choose whether location is based on **Reference servers** or **Gateway IP and MAC address**.
 - **Reference servers:** Security Agents that can connect to a reference server are part of the internal network

For more information, see [Reference Servers on page 4-22](#).

- **Gateway IP address:** Security Agents that can connect to a gateway are part of the internal network
 - a. Type the gateway IPv4/IPv6 address in the text box provided.
 - b. (Optional) Type the MAC address.
 - c. Click **Add**.

**Note**

If you do not type a MAC address, Apex One includes all the MAC addresses belonging to the specified IP address.

3. Click **Save**.
-

Reference Servers

One of the ways the Security Agent determines which policy or profile to use is by checking its connection status with the Apex One server. If an internal Security Agent (or any agent within the corporate network) cannot connect to the server, the agent status becomes offline. The agent then applies a policy or profile intended for external agents. Reference servers address this issue.

Any Security Agent that loses connection with the Apex One server will try connecting to reference servers. If the agent successfully establishes connection with a reference server, it applies the policy or profile for internal agents.

Policies and profiles managed by reference servers include:

- Firewall profiles
- Web reputation policies
- Data Protection policies
- Device Control policies

Take note of the following:

- Assign computers with server capabilities, such as a web server, SQL server, or FTP server, as reference servers. You can specify a maximum of 320 reference servers.
- Security Agents connect to the first reference server on the reference server list. If connection cannot be established, the agent tries connecting to the next server on the list.
- Security Agents use reference servers when determining the antivirus (Behavior Monitoring, Device Control, firewall profiles, the web reputation policy) or Data Protection settings to use. Reference servers do not manage agents or deploy updates and agent settings. The Apex One server performs these tasks.
- The Security Agent cannot send logs to reference servers or use them as update sources

Managing the Reference Server List

Procedure

1. Go to **Agents > Firewall > Profiles** or **Agents > Endpoint Location**.
2. Depending on the displayed screen, do the following:
 - If you are on the **Firewall Profiles for Agents** screen, click **Edit Reference Server List**.
 - If you are on the **Endpoint Location** screen, click **reference server list**.
3. Select **Enable the Reference Server list**.
 - **Exclude agents using VPN or PPP dial-up connections:** Select to define endpoints that use a VPN or PPP (Point-to-Point Protocol) dial-up connection to the reference servers as **External Agents**
4. To add any endpoint to the list, click **Add**.

- a. Specify the endpoint's IPv4/IPv6 address, name, or fully qualified domain name (FQDN), such as:
 - `computer.networkname`
 - `12.10.10.10`
 - `mycomputer.domain.com`
- b. Type the port through which agents communicate with this endpoint. Specify any open contact port (such as ports 20, 23 or 80) on the reference server.

**Note**

To specify another port number for the same reference server, repeat steps 2a and 2b. The Security Agent uses the first port number on the list and, if connection is unsuccessful, uses the next port number.

- c. Click **Save**.
5. To edit the settings of any endpoint on the list, click the endpoint name. Modify the endpoint name or port, and then click **Save**.
 6. To remove any endpoint from the list, select the endpoint name and then click **Delete**.
 7. To enable the endpoints to act as reference servers, click **Assign to Agents**.
-

Part III

Endpoint Protection



Chapter 5

Anti-malware Scanning

This section describes how to configure anti-malware scanning on Security Agents.

Topics include:

- *[Scan Now on page 5-2](#)*
- *[Scan Actions on page 5-9](#)*
- *[Scan Exclusion Support on page 5-16](#)*
- *[Restoring Quarantined Files on page 5-17](#)*

Scan Now

Scan Now is initiated remotely by administrators through the web console and can be targeted to one or several Security Agent endpoints.

Configure and apply Scan Now settings to one or several Security Agents and domains, or to all Security Agents that the server manages.

Configuring Scan Now Settings

Procedure

1. Go to **Agents > Agent Management**.
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Tasks > Scan Now**.

The **Scan Now** screen appears.

4. To change the pre-configured **Scan Now** settings before initiating the scan, click **Settings**.
 - a. Select the following options:
 - **Enable virus/malware scan**
 - **Enable spyware/grayware scan**



Note

You must enable virus/malware scanning before you can enable spyware/grayware scanning.

- b. Configure the **Target** settings.

For more information, see [Scan Now: Target Tab on page 5-3](#).

- c. Configure the **Action** settings.

For more information, see [Scan Now: Action Tab on page 5-5](#).

- d. Configure the **Scan Exclusion** settings.

For more information, see [Scan Now: Scan Exclusion Tab on page 5-7](#).

- e. Click **< Back** to return to the **Scan Now** screen.

5. In the agent tree, select the Security Agents to scan and click **Initiate Scan Now**.

The server sends a notification to the selected Security Agents.

6. Click **Select Unnotified Endpoints** and then **Initiate Scan Now** to immediately resend the notification to the Security Agents that did not receive the notification.
7. Click **Stop Notification** to cancel the notification to Security Agents.

Security Agents that already started the scan continue the scan in progress.

Scan Now: Target Tab

Procedure

1. In the **Files to Scan** section, select from the following:
 - **All scannable files:** Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.



Note

This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.


- **File types scanned by IntelliScan:** Scans files based on true-file type.
- **Files with the following extensions (use commas to separate entries):** Manually specify the files to scan based on their extensions. Separate multiple entries with commas.


**Note**

When configuring a parent policy, specify how other users can configure child policies.

- **Inherit from parent:** Child policies must use the settings configured in the parent policy
- **Extend from parent:** Child policies can append additional settings to the settings inherited from the parent policy

2. In the **Scan Settings** section, configure the required settings.

SETTING	DESCRIPTION
Scan compressed files	<p>Scans the specified number of compression layers within an archived file</p> <hr/> <div> Note</div> <p>Scanning through more layers may detect malware intentionally buried within a compressed archive, however, the scan may affect system performance.</p>

SETTING	DESCRIPTION
Scan OLE objects	<p>Scans the specified number of Object Linking and Embedding (OLE) layers in a file</p> <p>Detect exploit code in OLE files: OLE Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code.</p> <hr/> <p> Note</p> <p>The specified number of layers is applicable to both the Scan OLE objects and Detect exploit code in OLE files options.</p> <hr/>
Scan boot area	Scans the boot sector of the hard disk on the endpoint for virus/malware

3. In the **CPU Usage** section, select from the following:

- **High:** No pausing between scans
- **Medium:** Pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower
- **Low:** Pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

Scan Now: Action Tab

Procedure

1. In the **Virus/Malware** section, configure the required settings.
 - a. Select the type of action that the Security Agent takes after detecting a security threat.
 - **Use ActiveAction:** Select to use a set of pre-configured scan actions for viruses/malware

For more information, see [ActiveAction on page 5-9](#).

- **Customize action for probable virus/malware:** Select and specify the action that the Security Agent takes on probable malware threats
- **Use the same action for all virus/malware types:** Specify the action that the Security Agent takes on all malware threats
- **Use a specific action for each virus/malware type:** Specify the action that the Security Agent takes on specific security threats

For more information, see [Custom Scan Actions on page 5-11](#).

- b. Select **Back up files before cleaning** to create an encrypted copy of the infected file on the endpoint in the <Agent installation folder>\Backup folder.

Creating a backup copy of the file allows you to restore the original version of the file if necessary.

- c. Specify the location of the quarantine directory.
 - **Quarantine to the Security Agent's managing server:** The Security Agent sends an encrypted copy of all quarantined files to the managing Apex One server
 - **Quarantine directory:** The Security Agent sends an encrypted copy of all quarantined files to the specified location

For more information, see [Quarantine Directory on page 5-12](#).

- d. In the **Damage Cleanup Services** section, configure the following:
 - **Cleanup type**
 - **Standard cleanup:** The Security Agent performs any of the following actions during standard cleanup:
 - Detects and removes live Trojans
 - Kills processes that Trojans create
 - Repairs system files that Trojans modify

- Deletes files and applications that Trojans drop
- **Advanced cleanup:** In addition to the standard cleanup actions, the Security Agent stops activities by rogue security software (also known as FakeAV) and certain rootkit variants.
- **Run cleanup when probable virus/malware is detected:** Performs the configured cleanup type on probable malware threats

**Note**

You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**.

2. In the **Spyware/Grayware** section, select the action the Security Agent takes after detecting spyware or grayware programs.
 - **Clean:** Terminates all related processes and deletes associated registry values, files, cookies and shortcuts

**Note**

After cleaning spyware/grayware, Security Agents back up spyware/grayware data, which you can restore if you consider the spyware/grayware safe to access.

- **Pass:** Logs the detection but allows the program to execute
-

Scan Now: Scan Exclusion Tab

Procedure

1. Select **Enable scan exclusion**.
2. In the **Scan Exclusion List (Directories)** section, configure the required settings.

- a. Select **Exclude directories where Trend Micro products are installed** to automatically exclude directories associated with other Trend Micro products.

For more information, see [Trend Micro Product Directory Exclusions on page 5-16](#).

- b. Type a directory path to exclude from scans and click the + button.

The Security Agent does not scan files located in the specified directory (and sub-directories).

**Note**

- You can specify a maximum of 256 directories to exclude from scanning.
- Directory exclusions support the use of wildcard characters.

For more information, see [Wildcard Exceptions on page 5-17](#).

3. In the **Scan Exclusion List (Files)** section, configure the required settings.

- a. Type a file name or the file name with full directory path to exclude from scans and click the + button.

**Note**

- You can specify a maximum of 256 files to exclude from scanning.
- File exclusions support the use of wildcard characters.

For more information, see [Wildcard Exceptions on page 5-17](#).

4. In the **Scan Exclusion List (File Extensions)** section, configure the required settings.

- a. Select or type a file extension to exclude from scans and click the **Add >** button.

**Note**

- You can specify a maximum of 256 file extensions to exclude from scanning.
- For Manual Scan, Scheduled Scan, and Scan Now, use a question mark (?) to replace a single character or an asterisk (*) to replace multiple characters as wildcard characters. For example, if you do not want to scan all files with extensions starting with D, such as DOC, DOT, or DAT, type **D*** or **D??**.

Scan Actions

You can configure Security Agents to use a set of predefined scan actions or custom actions based on the detected malware type.

**Important**

Some files are uncleanable.

For more information, see:

ActiveAction

Different types of virus/malware require different scan actions. Customizing scan actions requires knowledge about virus/malware and can be a tedious task. The Security Agent uses ActiveAction to counter these issues.

ActiveAction is a set of pre-configured scan actions for viruses/malware. If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus/malware, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.

- Virus writers constantly change the way virus/malware attack endpoints. ActiveAction settings are updated to protect against the latest threats and the latest methods of virus/malware attacks.

The following table illustrates how ActiveAction handles each type of virus/malware.

TABLE 5-1. Trend Micro Recommended Scan Actions Against Viruses and Malware


VIRUS/MALWARE TYPE	REAL-TIME SCAN		MANUAL SCAN/SCHEDULED SCAN	
	FIRST ACTION	SECOND ACTION	FIRST ACTION	SECOND ACTION
CVE exploit	Pass	N/A	N/A	N/A
Joke	Quarantine	N/A	Quarantine	N/A
Trojans	Quarantine	N/A	Quarantine	N/A
Virus	Clean	Quarantine	Clean	Quarantine
Test virus	Deny Access	N/A	Pass	N/A
Packer	Quarantine	N/A	Quarantine	N/A
Others	Clean	Quarantine	Clean	Quarantine
Probable malware	Deny Access or user-configured action	N/A	Pass or user-configured action	N/A



Note

- For probable virus/malware, the default action is “Deny Access” during Real-time Scan and “Pass” during Manual Scan and Scheduled Scan. If these are not your preferred actions, you can change them to “Quarantine”, “Delete”, or “Rename”.
- Some files are uncleanable.
- ActiveAction is not available for spyware/grayware scan.

Custom Scan Actions

ACTION	DESCRIPTION
Delete	Deletes the infected file.
Quarantine	<p>Renames and then moves the infected file to a temporary quarantine directory on the endpoint.</p> <p>The Security Agent then sends quarantined files to the designated quarantine directory, which is on the managing server by default.</p> <p>The Security Agent encrypts quarantined files sent to this directory.</p> <p>For more information, see Quarantine Directory on page 5-12.</p>
Clean	<p>Cleans the infected file before allowing full access to the file.</p> <p>If the file is uncleanable, the Security Agent performs a second action, which can be one of the following actions: “Quarantine”, “Delete”, “Rename”, and “Pass”.</p> <p>This action can be performed on all types of security threats except probable virus/malware.</p> <hr/> <div data-bbox="454 846 504 889"></div> <p>Note</p> <p>Some files are uncleanable. For more information, see Uncleanable Files on page 5-13.</p> <hr/>
Rename	<p>Changes the infected file's extension to v i r. Users cannot open the renamed file initially, but can do so if they associate the file with a certain application.</p> <p>The virus/malware may execute when opening the renamed infected file.</p>
Pass	Performs no action on detected threats but records the detection in the logs.
Deny Access	<p>When the Security Agent detects an attempt to open or execute an infected file, it immediately blocks the operation.</p> <p>Users can manually delete the infected file.</p>

Quarantine Directory

If the action for an infected file is "Quarantine", the Security Agent encrypts the file and moves it to a temporary quarantine folder located in <Agent installation folder>\SUSPECT and then sends the file to the designated quarantine directory.

**Note**

You can restore encrypted quarantined files in case you need to access them in the future.

Accept the default quarantine directory, which is located on the Apex One server computer. The directory is in URL format and contains the server's host name or IP address.

- If the server is managing both IPv4 and IPv6 agents, use the host name so that all Security Agents can send quarantined files to the server.
- If the server only has or is identified by its IPv4 address, only pure IPv4 and dual-stack Security Agents can send quarantined files to the server.
- If the server only has or is identified by its IPv6 address, only pure IPv6 and dual-stack Security Agents can send quarantined files to the server.

You can also specify an alternative quarantine directory by typing the location in URL, UNC path, or absolute file path format. Security Agents should be able to connect to this alternative directory. For example, the alternative directory should have an IPv6 address if it will receive quarantined files from dual-stack and pure IPv6 Security Agents. Trend Micro recommends designating a dual-stack alternative directory, identifying the directory by its host name, and using UNC path when typing the directory.

Refer to the following table for guidance on when to use URL, UNC path, or absolute file path:

TABLE 5-2. Quarantine Directory

QUARANTINE DIRECTORY	ACCEPTED FORMAT	EXAMPLE	NOTES
A directory on the managing server computer	URL	http://<osceserver>	This is the default directory. Configure settings for this directory, such as the size of the quarantine folder.
	UNC path	\\<osceserver>\ofcscan\Virus	
A directory on another Apex One server computer (if you have other Apex One servers on the network)	URL	http://<osceserver2>	Ensure that Security Agents can connect to this directory. If you specify an incorrect directory, the Security Agent keeps the quarantined files on the SUSPECT folder until a correct quarantine directory is specified. In the server's virus/malware logs, the scan result is "Unable to send the quarantined file to the designated quarantine folder". If you use UNC path, ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group.
	UNC path	\\<osceserver2>\ofcscan\Virus	
Another endpoint on the network	UNC path	\\<computer_name>\temp	
A different directory on the Security Agent	Absolute path	C:\temp	

Uncleanable Files

The Virus Scan Engine is unable to clean the following files:

TABLE 5-3. Uncleanable File Solutions

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
Files infected with Trojans	Trojans are programs that perform unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or formatting disks. Trojans do not infect files, thus cleaning is not necessary.

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
	Solution: The Damage Cleanup Engine and Damage Cleanup Template remove Trojans.
Files infected with worms	<p>A worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other endpoint systems. The propagation usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program.</p> <p>Solution: Trend Micro recommends deleting worms.</p>
Write-protected infected files	Solution: Remove the write-protection which allows for the cleaning of the file.
Password-protected files	<p>Password-protected files include password-protected compressed files or password-protected Microsoft Office files.</p> <p>Solution: Remove the password protection which allows for the cleaning of the file.</p>
Backup files	<p>Files with the RB0~RB9 extensions are backup copies of infected files. The cleaning process creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.</p> <p>Solution: If successfully cleaned, you do not need to keep the backup copy of the infected file. If the endpoint functions normally, you can delete the backup file.</p>
Infected files in the Recycle Bin	<p>The system may not allow the removal of infected files from the Recycle Bin because the system is running.</p> <ol style="list-style-type: none"> 1. Log on to the endpoint with Administrator privilege. 2. Close all running applications to prevent applications from locking the file, which would make Windows unable to delete it. 3. Open the command prompt. 4. Type the following to delete the files: <code>del /s %Recycle.Bin*</code> 5. Check if the files were removed.
Infected files in Windows Temp	The system may not allow the cleaning of infected files in the Windows Temp folder or the Internet Explorer temporary folder because the

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
Folder or Internet Explorer Temporary Folder	<p>endpoint uses them. The files to clean may be temporary files needed for Windows operation.</p> <ol style="list-style-type: none"> 1. Log on to the endpoint with Administrator privilege. 2. Close all running applications to prevent applications from locking the file, which would make Windows unable to delete it. 3. If the infected file is in the Windows Temp folder: <ol style="list-style-type: none"> a. Open the command prompt. b. Type the following to delete the files: <pre>del /s \Windows\Temp*</pre> c. Restart the endpoint in normal mode. 4. If the infected file is in the Internet Explorer temporary folder: <ol style="list-style-type: none"> a. Open a command prompt and go to the Internet Explorer Temp folder. <ul style="list-style-type: none"> • For Windows 7: %LocalAppData%\Microsoft\Windows\Temporary Internet Files • For Windows 8/8.1: %LocalAppData%\Microsoft\Windows\INetCache • For Windows 10: %LocalAppData%\Microsoft\Windows\INetCache\IE b. Type the following to delete the files: <pre>del /s .*</pre> <p>The last command deletes all files in the Internet Explorer temporary folder.</p> c. Restart the endpoint in normal mode.
Files compressed using an unsupported compression format	Solution: Uncompress the files.

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
Locked files or files that are currently executing	Solution: Unlock the files or wait until the files have been executed.
Corrupted files	Solution: Delete the files.

Scan Exclusion Support

When excluding directories and file names from anti-malware scanning, refer to the following support information:

Trend Micro Product Directory Exclusions

If you select **Exclude directories where Trend Micro products are installed** in the **Scan Exclusion List (Directories)** section, the Security Agent automatically excludes following product directories:

- <Server installation folder>
- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT

- ScanMail™ for Microsoft Exchange

Wildcard Exceptions

Scan exclusion lists for files and directories support the use of wildcard characters. Use the "?" character to replace one character and "*" to replace several characters.

Use wildcard characters cautiously. Using the wrong character might exclude incorrect files or directories. For example, adding C:* to the Scan Exclusion List (Files) would exclude the entire C:\ drive.

TABLE 5-4. Scan Exclusions Using Wildcard Characters

VALUE	EXCLUDED	NOT EXCLUDED
c:\director*\fil *.txt	c:\directory\fil\doc.txt c:\directories\fil\files \document.txt	c:\directory\file\ c:\directories\files\ c:\directory\file\doc.txt c:\directories\files \document.txt
c:\director? \file*.txt	c:\directory\file \doc.txt	c:\directories\file \document.txt
c:\director? \file\?.txt	c:\directory\file\1.txt	c:\directory\file\doc.txt c:\directories\file \document.txt
c:*.txt	All .txt files in the C:\ directory	All other file types in the C:\ directory
[]	Not supported	Not supported

Restoring Quarantined Files

You can restore files that Apex One quarantined if you believe that the detection was inaccurate. The Central Quarantine Restore feature allows you

to search for files in the quarantine directory and perform SHA1 verification checking to ensure that the files you want to restore have not been modified in any way.

Procedure

1. Go to **Agents > Agent Management**.
2. In the agent tree, select a domain or select any agent.
3. Click **Tasks > Central Quarantine Restore**.

The **Central Quarantine Restore Criteria** screen appears.

4. Type the name of the data you want to restore in the **Infected file/object** field.
5. Optionally specify the time period, security threat name, and file path of the data.
6. Click **Search**.

The **Central Quarantine Restore** screen appears displaying the results of the search.

7. Select **Add restored file to the domain-level exclusion list** to ensure that all Security Agents in the domain(s) where the files are restored add the file to the scan exclusion list.

This ensures that Apex One does not detect the file as a threat during future scans.



Important

Security Agents managed using Apex Central policies only apply the restored file exclusion until the next time that the Apex Central server updates the Security Agent policy and overwrites the exclusion list. To prevent the Security Agent from rescanning restored files, add the file exclusion to the Apex Central Security Agent policy.

8. Optionally type the SHA-1 value of the file for verification purposes.

9. Select the files to restore from the list and click **Restore**.

**Tip**

To view the individual Security Agents that restore the file, click the link in the **Endpoints** column.

10. Click **Close** in the confirmation dialog.

To verify that Apex One successfully restored the quarantined file, see [Viewing Central Quarantine Restore Logs on page 9-3](#).

Chapter 6

Apex One Firewall

This chapter describes the Apex One Firewall features and configurations.


Topics include:

- *Apex One Firewall Overview on page 6-2*
- *Enabling or Disabling the Apex One Firewall on Endpoints on page 6-3*
- *Firewall Policies on page 6-4*
- *Firewall Profiles on page 6-11*
- *Configuring Global Firewall Settings on page 6-16*
- *Configuring Firewall Notifications for Security Agents on page 6-17*
- *Testing the Apex One Firewall on page 6-17*

Apex One Firewall Overview

The Apex One Firewall protects Security Agents and servers on the network using stateful inspection and high performance network virus scanning. Through the central management console, you can create rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.

The following table describes the features provided by the Apex One Firewall.

FEATURE	DESCRIPTION
Traffic filtering	<p>The Apex One Firewall filters all incoming and outgoing traffic, providing the ability to block certain types of traffic based on the following criteria:</p> <ul style="list-style-type: none"> • Direction (inbound/outbound) • Protocol (TCP/UDP/ICMP) • Destination ports • Source and destination endpoints
Application filtering	<p>The Apex One Firewall filters incoming and outgoing traffic for applications specified in the Firewall Exception List, allowing these applications access to the network. The availability of network connections depends on the policies set by the administrator.</p>
Certified Safe Software List	<p>The local Certified Safe Software List contains a list of applications that can bypass firewall policy security levels. The Apex One Firewall automatically allows applications in the Certified Safe Software List to run and access the network.</p> <p>You can also allow Security Agents to query the dynamically-updated global Certified Safe Software List hosted on Trend Micro servers.</p> <hr/> <div>  Important Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. </div> <hr/>

FEATURE	DESCRIPTION
Network virus detection	The Apex One Firewall examines all network packets for network viruses.
Stateful inspection	The Apex One Firewall uses stateful inspection to monitor and remember all connections and connection states to the Security Agent. The Apex One Firewall can identify specific conditions in any connection, predict what actions should follow, and detect disruptions in normal connections. Therefore, effective use of the firewall not only involves creating profiles and policies, but also analyzing connections and filtering packets that pass through the firewall.

Enabling or Disabling the Apex One Firewall on Endpoints

You can directly enable or disable the Apex One Firewall on a selected endpoint.

Procedure

- Enable or disable the Apex One Firewall driver through Windows.
 - a. Open **Windows Network Connection Properties**.
 - b. Select or clear the **Trend Micro NDIS 6.0 Filter Driver** check box from the network card.
 - Enable or disable the Apex One Firewall driver using a command prompt.
 - a. Open a command prompt and type `services.msc`.
 - b. Start or stop **OfficeScan NT Firewall** from the Microsoft Management Console (MMC).
-

Firewall Policies

Apex One Firewall policies allow you to block or allow certain types of network traffic not specified in a policy exception. A policy also defines which Apex One Firewall features are enabled or disabled. Assign a policy to one or multiple Firewall profiles.

With Active Directory integration and role-based administration, each user role, depending on the permission, can create, configure, or delete policies for specific domains.

The following table outlines the tasks available on the **Firewall Policies** screen.

TASK	DESCRIPTION
Add new policies	Click Add to create a new policy. For more information, see Adding a Firewall Policy on page 6-5 .
Copy existing policy settings	Select an existing policy and click Copy to open the Copy Policy screen. Modify the policy settings as required.
Delete existing policies	Select an existing policy and click Delete to remove the policy from the list.
Edit the Exception Template	Click Edit Exception Template to view the current Exception Template list. For more information, see Editing the Apex One Firewall Exception Template List on page 6-7 .
Modify existing policies	Click the Policy Description of an existing policy to modify settings.

Default Firewall Policies

Apex One comes with a set of default policies, which you can modify or delete.

POLICY NAME	SECURITY LEVEL	AGENT SETTINGS	EXCEPTIONS	RECOMMENDED USE
All access policy	Low	Enable firewall	None	Use to allow agents unrestricted access to the network
Communication Ports for Trend Micro Apex Central	Low	Enable firewall	Allow all incoming and outgoing TCP/UDP traffic through ports 80 and 10319	Use when agents have an MCP agent installation
ScanMail for Microsoft Exchange console	Low	Enable firewall	Allow all incoming and outgoing TCP traffic through port 16372	Use when agents need to access the ScanMail console
InterScan Messaging Security Suite (IMSS) console	Low	Enable firewall	Allow all incoming and outgoing TCP traffic through port 80	Use when agents need to access the IMSS console

Adding a Firewall Policy

Procedure

1. Go to **Agents > Firewall > Policies**.
2. Select to add, copy, or modify a policy.
 - Click **Add** to create a new policy.
 - Select an existing policy and click **Copy** to open the **Copy Policy** screen. Modify the policy settings as required.
 - Click the **Policy Description** of an existing policy to modify settings.
3. In the **Firewall Policy** section, configure the following:
 - **Name:** Specify a unique name for the Apex One Firewall policy.

- **Security level:** Select from **High**, **Medium**, or **Low** to determine the type of traffic that the Apex One Firewall allows or blocks.

**Note**

The Apex One Firewall automatically allows or blocks connections through the ports specified in the **Exception Template** list.

For more information, see [Editing the Apex One Firewall Exception Template List on page 6-7](#).

4. In the **Firewall Features** section, configure the following:

- **Enable firewall:** Select to activate the Apex One Firewall for this policy.
- **Display a notification when a Firewall violation is detected:** Select to display a notification on the Security Agent when the Apex One Firewall blocks an outgoing packet.

**Important**

If you grant users the permission to configure Apex One Firewall settings using the Security Agent console, you cannot use the Apex One web console to override the settings that the user configures.

The information under **Settings** on the Security Agent console's **Firewall** tab always reflects the settings configured from the Security Agent console, not from the server web console.

5. In the **Certified Safe Software List** section, configure the following:

- **Enable the local Certified Safe Software List:** Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.
- **Enable the global Certified Safe Software List (Internet access required):** Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.

**Important**

Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.

6. In the **Exception** section, manage the Exception Template List that applies to this policy only.

The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.

For more information about adding exceptions, see [Adding a Firewall Policy Exception on page 6-9](#) (follow the instructions from step 3).


7. Click **Save**.

Editing the Apex One Firewall Exception Template List

You can use the **Edit Exception Template** screen to manage the network traffic to allow or block on Security Agents. The Apex One Firewall provides default exceptions that you can modify or delete.

For more information, see [Default Firewall Policy Exceptions on page 6-8](#).

The following table outlines the tasks available on the **Edit Exception Template** screen.

TASK	DESCRIPTION
Add new exceptions	<p>Click Add to create a new exception.</p> <p>For more information, see Adding a Firewall Policy Exception on page 6-9.</p> <hr/> <p> Important</p> <p>After adding a new exception, you must save the Exception Template list to apply the new exception. If you navigate away from the Edit Exception Template screen without saving changes, the Apex One Firewall does not save the new exception.</p> <hr/>
Delete existing exceptions	Select an existing exception and click Delete to remove the exception from the Exception Template list.
Modify existing exceptions	Click the Name of an existing template to modify the exception settings.
Reorder the priority of exceptions	Click the up or down arrows next to an exception to change the priority in which the Apex One Firewall takes action on network traffic.
Save changes to the exception list	<p>Click one of the following buttons to save changes to the Exception Template list:</p> <ul style="list-style-type: none"> • Save Template Changes: Saves the current exception template list settings but does not apply the settings to existing policies • Save and Apply to Existing Policies: Saves the current exception template list settings and immediately applies the settings to all existing policies

Default Firewall Policy Exceptions

EXCEPTION NAME	ACTION	PROTOCOL	PORT	DIRECTION
DNS	Allow	TCP/UDP	53	Incoming and outgoing
NetBIOS	Allow	TCP/UDP	137, 138, 139, 445	Incoming and outgoing

EXCEPTION NAME	ACTION	PROTOCOL	PORT	DIRECTION
HTTPS	Allow	TCP	443	Incoming and outgoing
HTTP	Allow	TCP	80	Incoming and outgoing
Telnet	Allow	TCP	23	Incoming and outgoing
SMTP	Allow	TCP	25	Incoming and outgoing
FTP	Allow	TCP	21	Incoming and outgoing
POP3	Allow	TCP	110	Incoming and outgoing
LDAP	Allow	TCP/UDP	389	Incoming and outgoing

**Note**

Default exceptions apply to all agents. If you want a default exception to apply only to certain agents, edit the exception and specify the IP addresses of the agents.

The LDAP exception is not available if you upgrade from a previous Apex One version. Manually add this exception if you do not see it on the exception list.

Adding a Firewall Policy Exception

When adding new exceptions, ensure that you do not block the ports used for communication between the Apex One server and Security Agents.

You can locate the listening ports used by the Apex One server and Security Agents as follows:

- Server listening port: Go to **Administration > Settings > Agent Connection**. The port number is under **Agent Connection Settings**.
- Security Agent listening port: Go to **Agents > Agent Management > Status**. The port number is under **Basic Information**.

Procedure

1. Go to **Agents > Firewall > Policies**.
2. Click **Edit Exception Template**.
3. Click **Add**.
4. Type a name for the policy exception.
5. Select the type of application. You can select all applications, or specify application path or registry keys.



Note

Verify the name and full paths entered. Application exception does not support wildcards.

6. Select the action Apex One performs on network traffic (block or allow traffic that meets the exception criteria) and the traffic direction (inbound or outbound network traffic on the Security Agent endpoint).
7. Select the type of network protocol: TCP, UDP, ICMP, or ICMPv6.
8. Specify ports on the Security Agent endpoint on which to perform the action.
9. Select Security Agent endpoint IP addresses to include in the exception.

For example, if you chose to deny all network traffic (inbound and outbound) and type the IP address for a single endpoint on the network, then any Security Agent that has this exception in its policy cannot send or receive data to or from that IP address.

- **All IP addresses:** Includes all IP addresses
- **Single IP address:** Type an IPv4 or IPv6 address, or a host name.
- **Range (for IPv4 or IPv6):** Type an IPv4 or IPv6 address range.
- **Range (for IPv6):** Type an IPv6 address prefix and length.
- **Subnet mask:** Type an IPv4 address and its subnet mask.

10. Click **Save**.

The **Edit Exception Template** screen appears with the new exception added.


11. Click one of the following buttons to apply the new exception to the list:



- **Save Template Changes:** Saves the current exception template list settings but does not apply the settings to existing policies
- **Save and Apply to Existing Policies:** Saves the current exception template list settings and immediately applies the settings to all existing policies

Firewall Profiles

Apex One Firewall profiles define which Security Agents apply a particular Apex One Firewall policy. Create user roles that can create, configure, or delete profiles for specific domains.

The following table outlines the tasks available on the **Firewall Profiles** screen.

TASK	DESCRIPTION
Overwrite Security Agent Firewall settings	<p>Select Overwrite agent security level/exception list to replace the Security Agent profile settings with the server settings.</p> <hr/> <p> Important Only users logged on using the built-in administrator account or users with full management permissions can enable the Overwrite agent security level/exception list option.</p> <hr/>
Add new profiles	<p>Click Add to create a new profile.</p> <p>For more information, see Adding a Firewall Profile on page 6-12.</p>

TASK	DESCRIPTION
Delete existing profiles	Select an existing profile and click Delete to remove the profile from the list.
Edit the Reference Server List	<p>Click Edit Reference Server List to define endpoint location settings. The Apex One Firewall uses the reference server list to determine whether an endpoint is in an internal or external network.</p> <hr/> <p> Important Only users logged on using the built-in administrator account or users with full management permissions can see and configure the reference server list.</p> <hr/> <p>For more information, see Reference Servers on page 4-22.</p>
Modify existing profiles	Click the Name of an existing profile to modify settings.
Reorder the priority of profiles	<p>Click the up or down arrows next to a profile to change the priority in which the Apex One Firewall takes action on Security Agents.</p> <hr/> <p> Important Security Agents endpoints that match multiple profile definitions only apply the profile settings of the highest priority profile.</p> <hr/>
Send profile settings to Security Agents	Click Apply Profiles to Agents to deploy all Apex One Firewall profile settings to Security Agents.

Adding a Firewall Profile


Procedure


1. Go to **Agents > Firewall > Profiles**.
2. Select to add or modify a profile.
 - Click **Add** to create a new profile.


- Click the **Name** of an existing profile to modify settings.
3. Select **Enable this profile** to allow Apex One to deploy the profile to Security Agents.
 4. In the **Profile Settings** section, configure the following:
 - **Name:** Type a unique name for the profile.
 - **Description:** (Optional) Type a description for the profile.
 - **Policy:** Select a preexisting Apex One Firewall policy to apply to the profile.

For more information, see [Firewall Policies on page 6-4](#).

- Select the criteria the Apex One Firewall uses to define the Security Agents to which the profile applies.

CRITERIA	DESCRIPTION
IP address	Select an option to specify the endpoint IP address, IP address range, or subnet.
Domain	<p>Click the button to open and select domains from the agent tree.</p> <hr/> <div>  Note Only users with full domain permissions can select domains. </div> <hr/>
Endpoint	<p>Select to apply the profile to Security Agents selected from the agent tree.</p> <p>Click Select Endpoints from Agent Tree to open the Firewall Profile Settings screen. Select the required Security Agents and click Select.</p>

CRITERIA	DESCRIPTION
Platform	<p>Select to apply the profile to specific operating system types.</p> <ul style="list-style-type: none">• Supported Windows Server platforms• Supported Windows desktop platforms <p>For a list of supported operating systems, see the <i>System Requirements</i> document.</p>
Logon name	<p>Select to apply the profile to specific users logged on to endpoints.</p> <p>Specify the logon name for particular users. The Apex One Firewall applies the profile on Security Agents on which the specified users logged on.</p>
NIC description	<p>Select to apply the profile to endpoints using specific Network Interface Cards (NIC).</p> <p>Type a full or partial NIC description.</p> <hr/> <p> Tip</p> <p>Trend Micro recommends typing the NIC card manufacturer because NIC descriptions typically start with the manufacturers name. For example, if you type "Intel", all Intel-manufactured NICs satisfy the criteria. If you type a particular NIC model, such as "Intel(R) Pro/100", only NIC descriptions that start with "Intel(R) Pro/100" satisfy the criteria.</p> <hr/>

CRITERIA	DESCRIPTION
Agent location	<p>Select to apply the profile based on the Security Agent connection status.</p> <ul style="list-style-type: none"> Internal - Security Agents can connect to a configured reference server <hr/> <div>  Note Click Edit reference server list to configure location settings. For more information, see Reference Servers on page 4-22. </div> <hr/> <ul style="list-style-type: none"> External - Security Agents cannot connect to a configured reference server

5. In the **User Privileges** section, configure the following:

- Allow user to change security level:** Select to allow users to define the Apex One Firewall security level using the Security Agent console
- Allow user to edit policy exceptions:** Select to allow users to define custom Apex One Firewall policy exceptions using the Security Agent console



Important

Only Security Agents with the **Display the Firewall settings on the Security Agent console** privilege display the firewall settings on the Security Agent console.

6. Click **Save**.

The profile displays in the Firewall Profiles list.

7. Click **Apply Profiles to Agents** to send the updated profiles to Security Agents.

Configuring Global Firewall Settings

Procedure

1. Go to **Agents > Global Agent Settings**.
2. Click the **Security Settings** tab.
 - a. Go to the **Firewall Settings** section.
 - b. Configure settings as required.
 - **Send firewall logs to the server every:** Sets the frequency that Security Agents with the **Allow Security Agents to send firewall logs to the Apex One server** privilege send Firewall logs to the server



Note

You can grant the **Allow Security Agents to send firewall logs to the Apex One server** privilege on the **Privileges** tab of the **Privileges and Other Settings** screen.

- **Update the Apex One firewall driver only after a system restart:** Prevents the Security Agent from attempting to update the Common Firewall Driver during normal operations
 - **Send firewall log count information to the Apex One server hourly to determine the possibility of a firewall outbreak:** Enables the Security Agent to send Firewall detection counts to the Apex One hourly
3. Click the **System** tab.
 - a. Go to the **Certified Safe Software Service Settings** section.
 - b. Configure settings as required.
 - **Enable the Certified Safe Software Service for Behavior Monitoring, Firewall, and antivirus scans:** Queries Trend Micro data centers to verify the safety of a program detected by

Malware Behavior Blocking, Event Monitoring, Firewall, or antivirus scans to reduce the likelihood of false positives

4. Click **Save**.
-

Configuring Firewall Notifications for Security Agents

You can configure the Security Agent to notify end users after the Apex One Firewall blocks outbound traffic that violated the firewall policy.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Firewall Violations**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Testing the Apex One Firewall

To ensure that the Apex One firewall works properly, perform a test on a single Security Agent or group of Security Agents.



WARNING!

Test Security Agent program settings in a controlled environment only. Do not perform tests on endpoints connected to the network or to the Internet. Doing so may expose Security Agent endpoints to viruses, hacker attacks, and other risks.

Procedure

1. Create and save a test policy. Configure the settings to block the types of traffic you want to test. For example, to prevent the Security Agent from accessing the Internet, do the following:
 - a. Set the security level to **Low** (allow all inbound/outbound traffic).
 - b. Select **Enable firewall and Notify users when a firewall violation occurs**.
 - c. Create an exception that blocks HTTP (or HTTPS) traffic.
 2. Create and save a test profile, selecting the agents to which you will test firewall features. Associate the test policy with the test profile.
 3. Click **Assign Profile to Agents**.
 4. Verify the deployment.
 - a. Click **Agents > Agent Management**.
 - b. Select the domain to which the agent belongs.
 - c. Select **Firewall view** from the agent tree view.
 - d. Check if there is a green check mark under the **Firewall** column of the agent tree.
 - e. Verify that the agent applied the correct firewall policy. The policy appears under the **Firewall Policy** column in the agent tree.
 5. Test the firewall on the agent endpoint by attempting to send or receive the type of traffic you configured in the policy.
 6. To test a policy configured to prevent the agent from accessing the Internet, open a web browser on the agent endpoint. If you configured Apex One to display a notification message for firewall violations, the message displays on the agent endpoint when an outbound traffic violation occurs.
-

Chapter 7

Using Outbreak Prevention

This section describes security risk outbreaks, which occur when detections of virus/malware, spyware/grayware, and shared folder sessions over a certain period of time exceed a certain threshold.

Topics include:

- *Outbreak Prevention Policies on page 7-2*
- *Configuring Security Risk Outbreak Prevention on page 7-8*
- *Disabling Outbreak Prevention on page 7-9*

Outbreak Prevention Policies

When outbreaks occur, enforce any of the following policies:

Limiting/Denying Access to Shared Folders

During outbreaks, limit or deny access to shared folders on the network to prevent security risks from spreading through the shared folders.

When this policy takes effect, users can still share folders but the policy will not apply to the newly shared folders. Therefore, inform users not to share folders during an outbreak or deploy the policy again to apply the policy to the newly shared folders.

Procedure

1. Go to **Agents > Outbreak Prevention**.
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Limit/Deny access to shared folders**.
5. Select from the following options:
 - **Allow read-only access:** Limits access to shared folders
 - **Deny access**



Note

The read access only setting does not apply to shared folders already configured to deny full access.

6. Click **Save**.

The **Outbreak Prevention Settings** screen displays again.

7. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.

Blocking Vulnerable Ports


During outbreaks, block vulnerable ports that viruses/malware might use to gain access to Security Agent endpoints.



WARNING!

Configure Outbreak Prevention settings carefully. Blocking ports that are in use makes network services that depend on them unavailable. For example, if you block the trusted port, Apex One cannot communicate with the agent for the duration of the outbreak.

Procedure

1. Go to **Agents > Outbreak Prevention**.
2. In the agent tree, click the root domain icon  to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Block Ports**.
5. Select whether to **Block trusted port**.
6. Select the ports to block under the **Blocked Ports** column.
 - a. If there are no ports in the table, click **Add**. In the screen that opens, select the ports to block and click **Save**.
 - **All ports (including ICMP)**: Blocks all ports except the trusted port. If you also want to block the trusted port, select the Block trusted port check box in the previous screen.

- **Specified ports**
 - **Commonly used ports:** Select at least one port number for Apex One to save the port blocking settings.
 - **Ports commonly used by Trojan programs:** Blocks ports commonly used by Trojan horse programs.
 - **Any port between 1 and 65535, or a port range:** Optionally specify the direction of the traffic to block and some comments, such as the reason for blocking the ports you specified.
 - **Ping protocol (Reject ICMP):** Click if you only want to block ICMP packets, such as ping requests.
 - b. To edit settings for the blocked port(s), click the port number.
 - c. In the screen that opens, modify the settings and click **Save**.
 - d. To remove a port from the list, select the check box next to the port number and click **Delete**.
7. Click **Save**.

The **Outbreak Prevention Settings** screen displays again.

8. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.


Denying Write Access to Files and Folders

Viruses/Malware can modify or delete files and folders on the host endpoints. During an outbreak, configure Apex One to prevent viruses/malware from modifying or deleting files and folders on Security Agent endpoints.

**WARNING!**

Apex One does not support denying write access to mapped network drives.

Procedure

1. Go to **Agents > Outbreak Prevention**.
 2. In the agent tree, click the root domain icon  to include all agents or select specific domains or agents.
 3. Click **Start Outbreak Prevention**.
 4. Click **Deny write access to files and folders**.
 5. Type the directory path. When you finish typing the directory path you want to protect, click **Add**.
-

**Note**

Type the absolute path, not the virtual path, for the directory.

6. Specify the files to protect in the protected directories. Select all files or files based on specific file extensions. For file extensions, to specify an extension that is not in the list, type it in the text box, and then click **Add**.
7. To protect specific files, under **Files to Protect**, type the full file name and click **Add**.
8. Click **Save**.

The **Outbreak Prevention Settings** screen displays again.

9. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.

Denying Access to Executable Compressed Files

During outbreaks, denying access to executable compressed files can prevent the possible security risks that these files may contain from spreading across the network. You can choose to allow access to trusted files created by the supported executable packer programs.

Procedure

1. Go to **Agents > Outbreak Prevention**.
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Deny access to executable compressed files**.
5. Select from the list of supported executable packer programs and click **Add** to allow access to executable packed files created by these packer programs.



Note

You can only approve the use of packed files created by the packer programs in the Executable Packers list. Outbreak Prevention denies access to all other executable packed file formats.

6. Click **Save**.

The **Outbreak Prevention Settings** screen displays again.

7. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.

Creating Mutual Exclusion Handling on Malware Processes/Files

You can configure Outbreak Prevention to protect against security threats that utilize mutex processes by overriding the resources that the threat requires to infect and spread throughout the system. Outbreak Prevention creates mutual exclusions on files and processes related to known malware, preventing the malware from accessing these resources.



Tip

Trend Micro recommends maintaining these exclusions until a solution to the malware threat can be implemented. Contact Support to obtain the correct mutex names to protect against during an outbreak.



Note

Mutual exclusion handling requires the Unauthorized Change Prevention Service and only supports 32-bit platforms.

Procedure

1. Go to **Agents > Outbreak Prevention**.
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click **Create mutual exclusion (mutex) handling on malware processes/files**.
5. Type the mutex name to protect against in the text field provided.
Add or remove mutex names from the list using the + and - buttons.



Note

Outbreak Prevention supports mutual exclusion handling on a maximum of six mutex threats.

6. Click **Save**.

The **Outbreak Prevention Settings** screen displays again.


7. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.

Configuring Security Risk Outbreak Prevention

When an outbreak occurs, enforce outbreak prevention measures to respond to and contain the outbreak. Configure prevention settings carefully because incorrect configuration may cause unforeseen network issues.

Procedure

1. Go to **Agents > Outbreak Prevention**.
2. In the agent tree, click the root domain icon () to include all agents or select specific domains or agents.
3. Click **Start Outbreak Prevention**.
4. Click any of the following outbreak prevention policies and then configure the settings for the policy:
 - [Limiting/Denying Access to Shared Folders on page 7-2](#)
 - [Blocking Vulnerable Ports on page 7-3](#)
 - [Denying Write Access to Files and Folders on page 7-4](#)
 - [Denying Access to Executable Compressed Files on page 7-6](#)
 - [Creating Mutual Exclusion Handling on Malware Processes/Files on page 7-7](#)
5. Select the policies you want to enforce.

6. Select the number of hours outbreak prevention will stay in effect. The default is 48 hours. You can manually restore network settings before the outbreak prevention period expires.

**WARNING!**

Do not allow outbreak prevention to remain in effect indefinitely. To block or deny access to certain files, folders, or ports indefinitely, modify endpoint and network settings directly instead of using Apex One.

7. Click **Start Outbreak Prevention**.

The outbreak prevention measures you selected display in a new window.

8. Back in the Outbreak Prevention agent tree, check the **Outbreak Prevention** column.

A check mark appears on endpoints applying outbreak prevention measures.

Apex One records the following events in the system event logs:

- Server events (initiating outbreak prevention and notifying agents to enable outbreak prevention)
- Security Agent event (enabling outbreak prevention)

Disabling Outbreak Prevention

When you are confident that an outbreak has been contained and that Apex One already cleaned or quarantined all infected files, restore network settings to normal by disabling Outbreak Prevention.

Procedure

1. Go to **Agents > Outbreak Prevention**.

2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Restore Settings**.
4. To inform users that the outbreak is over, select **Notify users after restoring the original settings**.
5. Accept or modify the default agent notification message.
6. Click **Restore Settings**.

**Note**

If you do not restore network settings manually, Apex One automatically restores these settings after the number of hours specified in **Automatically restore network settings to normal after __ hours** on the **Outbreak Prevention Settings** screen. The default setting is 48 hours.

Apex One records the following events in the system event logs:

- Server events (initiating outbreak prevention and notifying Security Agents to enable outbreak prevention)
 - Security Agent event (enabling outbreak prevention)
7. After disabling outbreak prevention, scan networked endpoints for security risks to ensure that the outbreak has been contained.
-

Part IV

Monitoring Apex One



Chapter 8

Dashboard

This chapter introduces the Apex One dashboard and available widgets. The dashboard provides a quick view of the security status for your network.

Topics include:

- *[Tabs and Widgets on page 8-2](#)*
- *[Summary Tab Widgets on page 8-6](#)*
- *[Data Protection Widgets on page 8-12](#)*
- *[Apex One Widgets on page 8-14](#)*
- *[Management Widget on page 8-18](#)*

Tabs and Widgets

Widgets are the core components of the dashboard. Widgets provide specific information about various security-related events. Some widgets allow you to perform certain tasks, such as updating outdated components.

The information that widgets display comes from:

- Apex One server and agents
- Plug-in solutions and their agents
- Trend Micro Smart Protection Network



Note

Enable Smart Feedback to display data from Smart Protection Network. For details about Smart Feedback, see [Smart Feedback on page 12-5](#).

Tabs provide a container for widgets. The **Dashboard** supports up to 30 tabs.

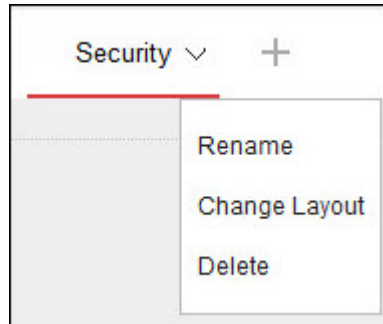
Working with Tabs

Manage tabs by adding, renaming, changing the layout, deleting, and automatically switching between tab views.

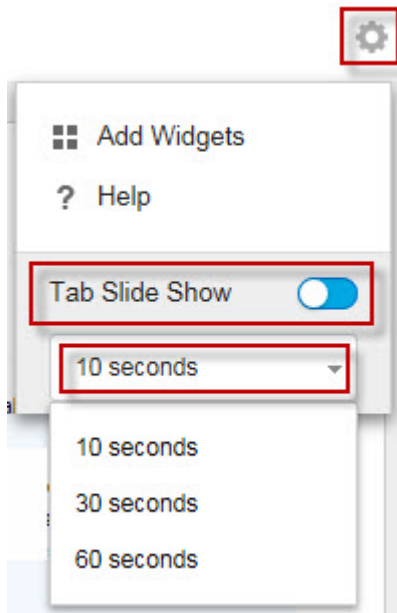
Procedure

1. Go to **Dashboard**.
2. To add a new tab:
 - a. Click the add icon.
 - b. Type a name for the new tab.
3. To rename a tab:

- a. Hover over the tab name and click the down arrow.



- b. Click **Rename** and type the new tab name.
4. To change the layout of the widgets for a tab:
 - a. Hover over the tab name and click the down arrow.
 - b. Click **Change Layout**.
 - c. Select the new layout from the screen that appears.
 - d. Click **Save**.
 5. To delete a tab:
 - a. Hover over the tab name and click the down arrow.
 - b. Click **Delete** and confirm.
 6. To play a tab slide show:
 - a. Click the **Settings** button to the right of the tab display.



- b. Enable the **Tab Slide Show** control.
 - c. Select the length of time each tab displays before switching to the next tab.
-

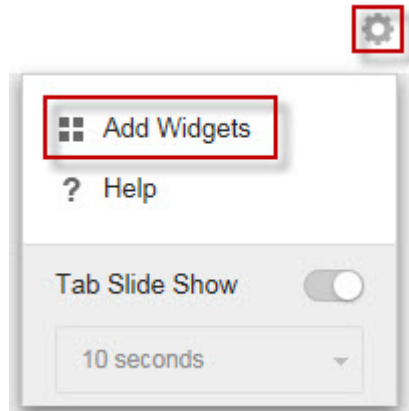
Working with Widgets


Manage widgets by adding, moving, resizing, renaming, and deleting items.

Procedure

1. Go to **Dashboard**.
2. Click a tab.
3. To add a widget:



- a. Click the **Settings** button to the right of the tab display.



- b. Click **Add Widgets**.
 - c. Select the widgets to add.
 - In the drop-down on top of the widgets, select a category to narrow down the selections.
 - Use the search text box on top of the screen to search for a specific widget.
 - d. Click **Add**.
4. To move a widget to a new location on the same tab, drag-and-drop a widget to a new location.
 5. Resize widgets on a multi-column tab by pointing the cursor to the right edge of the widget and then moving the cursor to the left or right.
 6. To rename a widget:
 - a. Click the settings icon (: > ).
 - b. Type the new title.

**Note**

For some widgets, such as the **Apex One and Plug-ins Mashup**, you can modify widget-related items.

- c. Click **Save**.
7. To delete a widget, click the delete icon ( > ).
-

Summary Tab Widgets

The **Summary** tab provides an overview of the security status of all the Security Agents on your network.

**Note**

You cannot add, delete, or modify the widgets that display on the **Summary** tab.

Available widgets:

Overall Threat Detections and Policy Violations Widget

This widget provides an overview of all the threat detections and policy violations across the network over the last 24 hours.

Hover over the threat or violation count to view a breakdown of the specific types of detections that occurred for each group. To view the logs for a specific feature, click the count to the right.

TABLE 8-1. Detection Categories

CATEGORY	DESCRIPTION
Known Threats	Displays all the features that detect security threats confirmed by Trend Micro <ul style="list-style-type: none">• Virus/Malware• Spyware/Grayware• Web Reputation
Unknown Threats	Displays all the features that detect potential threats using advanced heuristics, analysis, or feature modeling <ul style="list-style-type: none">• Predictive Machine Learning• Behavior Monitoring• Suspicious Connections• Suspicious File Objects
Policy Violations	Displays all the features that contain policy violations that are specific to your corporate security standards <ul style="list-style-type: none">• Firewall• Device Control• Data Loss Prevention

Endpoint Status Widget

This widget provides an overview of the connection and update status of Security Agents on your network.

Hover over a count to view a breakdown of the different statuses. To view the logs for a specific status, click the count to the right.

TABLE 8-2. Agent/Endpoint Groups

GROUP	DESCRIPTION
Managed Agents	Displays the last reported connection status of the Security Agents on your network <ul style="list-style-type: none">• Online• Offline
Outdated Agents	Displays a list of component categories and the count of Security Agents with an outdated component in each category

Ransomware Summary Widget

This widget provides an overview of all the attempted ransomware attacks for a specified time range.



The default view displays a summary of all the ransomware detections and further categorizes the attempts based on the infection channel.

- Click the ransomware detection count on the default view to open the **Security Risks - Ransomware** logs screen that lists the ransomware detection details.

Click any of the charts on the right side of the widget to display an enlarged view of the chart data.

- Hover over the node(s) for any particular day to view the total number of detections for the displayed detection category. Click a node to redirect to the **Security Risks - Ransomware** logs screen, which lists the ransomware detection details for that particular day.

TABLE 8-3. Ransomware Detection Channels

CHANNEL	DESCRIPTION	DETECTED BY
Web	Files downloaded using a web client (for example, browser or FTP client)	<ul style="list-style-type: none"> Web Reputation Real-time Scan Behavior Monitoring
Network traffic	Ransomware detected by the Suspicious Connections feature	<ul style="list-style-type: none"> Suspicious Connections
Cloud synchronization	Files synchronized to the local sync folder by the following supported cloud storage services: <ul style="list-style-type: none"> Microsoft™ OneDrive™ 	<ul style="list-style-type: none"> Real-time Scan Behavior Monitoring Predictive Machine Learning
Email	Email attachments opened using Microsoft Outlook <hr/>  Note Apex One classifies all attachments opened using other email client applications in the Local or network drive channel.	<ul style="list-style-type: none"> Real-time Scan Behavior Monitoring
AutoRun files	Programs located on removable storage drives and executed by an autorun file <hr/>  Note Apex One classifies all other files/programs not executed by the autorun program on removable storage devices in the Local or network drive channel.	<ul style="list-style-type: none"> Real-time Scan Behavior Monitoring

CHANNEL	DESCRIPTION	DETECTED BY
Local or network drive	Ransomware detected on local or network drives including: <ul style="list-style-type: none"> Email attachments opened using email clients other than Microsoft Outlook Files on removable storage devices not executed by the autorun program 	<ul style="list-style-type: none"> Real-time Scan Manual Scan Scheduled Scan Scan Now Behavior Monitoring

Security Threats - Ransomware Logs

The Security Threats - Ransomware logs provide an overview of all the ransomware threats detected on your network, regardless of the type of scan that detected the threat.

ITEM	DESCRIPTION
Date/Time	The time the detection occurred
Security Threat	The name of the security threat
Category	The type of scan that detected the threat
File Path / URL	The location where the threat detection occurred or the list used to detect the malicious website
Action	The action taken on the threat
Infection Channel	The channel the threat originated from
Endpoint	The endpoint on which the detection occurred

Top Ransomware Detections Widget

This widget provides an overview of the top ransomware detections for a specified time range.

Use the drop-down to select the type of ransomware data to display.

VIEW	DESCRIPTION
Endpoints	<p>Displays the endpoints with the greatest number of ransomware detections on your network</p> <p>Click the ransomware detection count to open the Security Risks - Ransomware logs screen that lists the ransomware detection details.</p>
Ransomware Types	<p>Displays the types of ransomware with the greatest number of detections on your network</p> <p>Click the Threat Name link to open the Trend Micro Threat Encyclopedia for further information regarding the specific threat type.</p>
Domains	<p>Displays the ransomware domains with the greatest number of detections on your network</p> <p>Click the Threat Name link to open the Trend Micro Threat Encyclopedia for further information regarding the specific domain.</p>

Security Risk Detections Over Time Widget

This widget provides an overview of the endpoints on your network with threat detections and the types of threats that affected your network for a specific time range.

Click the **Affected Endpoints** or **Threat Types** button to switch between the different views.

VIEW	DESCRIPTION
Affected Endpoints	<p>Displays the daily trend of endpoints with threat detections or policy violations for the specified time range</p> <p>Hover over the node(s) to view the total number of affected endpoints for that particular day.</p>

VIEW	DESCRIPTION
Threat Types	<p>Displays a graph that outlines the number of threats and policy violations logged for the specified time range</p> <ul style="list-style-type: none">• Click the threat type names at the bottom of the graph to show/hide detection information on the graph.• Hover over the node(s) for any particular day to view the total number of detections for the displayed threat types. Click a node to redirect to the logs screen for the threat type highlighted in the list.

Data Protection Widgets



Note

The Data Protection widgets are available after activating Apex One Data Protection.

Available widgets:

Data Loss Prevention Incidents Over Time Widget

This widget displays the overall number of Data Loss Prevention incidents for a specific time range.



Note

The detections include all Data Loss Prevention incidents regardless of the action taken (“Block” or “Pass”).

Top Data Loss Preventions Incidents Widget

This widget displays the top Users, Channels, Templates, or Endpoints that triggered Data Loss Prevention incidents for a specified time range.

**Note**

- This widget displays a maximum of 10 users, channels, templates, or endpoints.
- The detections include all Data Loss Prevention incidents regardless of the action taken (“Block” or “Pass”).

Select the type of Data Loss Prevention data that displays using the **View by** drop-down.

TABLE 8-4. Data Loss Prevention Views

VIEW	DESCRIPTION
User	<p>Users that transmitted the greatest number of digital assets</p> <ul style="list-style-type: none"> • Click the user names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the user name and number of Data Loss Prevention incidents for that user.
Channel	<p>Channels most often used to transmit digital assets</p> <ul style="list-style-type: none"> • Click the channel names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the channel name and number of Data Loss Prevention incidents for that channel.
Template	<p>Digital asset templates that triggered the most detections</p> <ul style="list-style-type: none"> • Click the template names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the template name and number of Data Loss Prevention incidents for that template.
Endpoints	<p>Endpoints that transmitted the greatest number of digital assets</p> <ul style="list-style-type: none"> • Click the endpoint names at the bottom of the graph to show/hide detection information on the graph. • Hover over the detection bars to view the endpoint name and number of Data Loss Prevention incidents for that endpoint.



Apex One Widgets

The Apex One widgets provide a quick reference for Security Agent security statuses and detections, plug-in program information, and outbreak incidents.

Available widgets:

C&C Callback Events Widget

This widget displays all C&C callback event information including the target of the attack and the source callback address.


You can choose to view C&C callback information from a specific C&C server list. To select the list source (Global Intelligence, Virtual Analyzer), click the edit icon ( > ) and select the list from the **C&C list source** drop-down.

Use the **View by** drop-down to select the type of C&C callback data that displays:

- **Compromised host:** Displays the most recent C&C information per targeted endpoint


TABLE 8-5. Compromised Host Information

COLUMN	DESCRIPTION
Compromised Host	The name of the endpoint targeted by the C&C attack
Callback Addresses	The number of callback addresses that the endpoint attempted to contact
Latest Callback Address	The last callback address that the endpoint attempted to contact

COLUMN	DESCRIPTION
Callback Attempts	<p>The number of times the targeted endpoint attempted to contact the callback address</p> <hr/> <div>  Note Click the hyperlink to open the C&C Callback Logs screen and view more detailed information. </div> <hr/>

- **Callback address:** Displays the most recent C&C information per C&C callback address

TABLE 8-6. C&C Address Information

COLUMN	DESCRIPTION
Callback Address	The address of C&C callbacks originating from the network
C&C Risk Level	The risk level of the callback address determined by either the Global Intelligence or Virtual Analyzer list
Compromised Hosts	The number of endpoints that the callback address targeted
Latest Compromised Host	The name of the endpoint that last attempted to contact the C&C callback address
Callbacks Attempts	<p>The number of attempted callbacks made to the address from the network</p> <hr/> <div>  Note Click the hyperlink to open the C&C Callback Logs screen and view more detailed information. </div> <hr/>

Security Risk Detections Widget

This widget displays the number of security risks detected and number of affected endpoints.

Click the endpoint count to open the **Agent Management** screen that lists the affected Security Agents in the agent tree.

Apex One and Plug-ins Mashup Widget

This widget combines data from Security Agents and installed plug-in programs and then presents the data in the agent tree. This widget helps you quickly assess the protection coverage on agents and reduces the overhead required to manage the individual plug-in programs.

This widget displays data from the following plug-in programs:

- Trend Micro Virtual Desktop Support



Important



You must activate a supported plug-in program before the mashup widget can display the corresponding data. Upgrade the plug-in programs if newer versions are available.

To select the columns that display in the agent tree, click the **More Options** button on the top right corner of the widget and click the **Widget Settings** button.


Click the data under any column to open the corresponding plug-in program console or the Apex One **Agent Management** screen. The screen that displays depends on the type of data that you clicked.

Antivirus Agent Connectivity Widget

This widget displays the connection status of Security Agents to the Apex One server in relation to the configured scan method (Smart Scan and Conventional Scan).

You can choose to display the data in a table or pie chart by clicking the display icons ( .

Use the drop-down list above the table/graph to change the type of data that displays. Click the count for any status to open the **Agent Management** screen that lists the related Security Agents in the agent tree.

VIEW	DESCRIPTION
All	Displays the connection status of all Security Agents for both scan methods
Conventional Scan	Displays the connection status of all Security Agents that use the Conventional Scan method
Smart Scan	<p>Displays the connection status of all Security Agents that use the Smart Scan method</p> <p>When viewing the agent connection status in a table:</p> <ul style="list-style-type: none"> Expand the “Online” agent information to view the connection status of agents with a Smart Protection Server. Click the URL to open the Smart Protection Server management console. <hr/> <p> Note Only online agents (reporting to the Apex One server) can report their connection status with Smart Protection Servers.</p>

Outbreaks Widget

The **Outbreaks** widget provides the status of any current security risk outbreaks and the last outbreak alert.

- Click the date/time link of the alert to view more details about the outbreak.
- Reset** the status of the outbreak alert information and immediately enforce outbreak prevention measures when Apex One detects an outbreak.

For details on enforcing outbreak prevention measures, see [Outbreak Prevention Policies on page 7-2](#).

- Click **View Top 10 Security Risk Statistics** to view the most prevalent security risks, the endpoints with the greatest number of security risks, and the top infection sources.

On the **Top 10 Security Risk Statistics** screen, you can:

- View detailed information about a security risk by clicking the security risk name.
- View the overall status of a particular endpoint by clicking the endpoint name.
- View security risk logs for the endpoint by clicking **View** corresponding to the endpoint name.
- Reset the statistics in each table by clicking **Reset Count**.

Agent Updates Widget

This widget displays components and programs that protect Security Agents from security risks.

Click the “Outdated” count to open the **Agent Management** screen that lists the Security Agents that require updates in the agent tree.



Management Widget

The management widget displays the connection status of Security Agents with the Apex One server.

Available widgets:

Agent-Server Connectivity Widget

This widget shows the connection status of all agents with the Apex One server.

You can switch between the table and pie chart by clicking the display icons ( ).

Click the count for any status to open the **Agent Management** screen that lists the related Security Agents in the agent tree.

Chapter 9

Logs

This chapter describes how to access system event and security detection logs using the web console.

Topics include:

- *[Viewing Scan Operation Logs on page 9-2](#)*
- *[Viewing Central Quarantine Restore Logs on page 9-3](#)*
- *[Viewing System Event Logs on page 9-4](#)*

Viewing Scan Operation Logs

When Manual Scan, Scheduled Scan, or Scan Now runs, the Security Agent creates a scan log that contains information about the scan. You can view the scan log by accessing the Apex One server or Security Agent consoles.

Procedure

1. Go to **Agents > Agent Management**.
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Scan Operation Logs**.

The **Scan Operation Log Criteria** screen appears.

4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

ITEM	DESCRIPTION
Start Time	The time the scan started
End Time	The time the scan stopped
Endpoint	The endpoint on which the scan occurred
Status	<p>The completion status of the scan</p> <ul style="list-style-type: none">• Completed: The scan completed normally.• Interrupted: The user stopped the scan before it completed.• Stopped unexpectedly: The scan was interrupted by the user, system, or an unexpected event. For example, the Apex One Real-time Scan service might have terminated unexpectedly or the user performed a forced restart of the endpoint.

ITEM	DESCRIPTION
Scan Type	The type of scan performed (Manual Scan, Scan Now, Scheduled Scan)
Scanned	Number of scanned objects
Virus/Malware	Number of virus/malware infected detections
Spyware/Grayware	Number of spyware/grayware detections
Smart Scan Agent Pattern	Smart Scan Agent Pattern version
Virus Pattern	Virus Pattern version
Spyware/Grayware Pattern	Spyware/Grayware Pattern version

6. To save logs to a comma-separated value (CSV) file, click **Export All to CSV**. Open the file or save it to a specific location.

Viewing Central Quarantine Restore Logs

After cleaning malware, Security Agents back up malware data. Notify an online agent to restore backed up data if you consider the data harmless. Information about which malware backup data was restored, the affected endpoint, and the restore result available in the logs.

Procedure

1. Go to **Logs > Agents > Central Quarantine Restore**.
2. Check the **Successful**, **Unsuccessful**, and **Pending** columns to see if Apex One successfully restored the quarantined data.
3. Click the count links in each column to view detailed information about each affected endpoint.

**Note**

For **Unsuccessful** restorations, you can attempt to restore the file again on the **Central Quarantine Restore Details** screen by clicking **Restore All**.

4. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.

Viewing System Event Logs

Apex One records events related to the server program, such as shutdown and startup. Use these logs to verify that the Apex One server and services work properly.

Procedure

1. Go to **Logs > System Events**.
2. Under **Event**, check for logs that need further action. Apex One logs the following events:

TABLE 9-1. System Event Logs

LOG TYPE	EVENTS
Apex One Master Service and Database Server	<ul style="list-style-type: none">• Master Service started• Master Service stopped successfully• Master Service stopped unsuccessfully
Role-based web console access	<ul style="list-style-type: none">• Logging on to the console• Logging off from the console• Session timeout (user automatically logged off)
Server authentication	<ul style="list-style-type: none">• The Security Agent received invalid commands from the server• Authentication certificate invalid or expired

3. To save logs to a comma-separated value (CSV) file, click **Export to CSV**. Open the file or save it to a specific location.
-

Chapter 10

Notifications

This chapter describes how to configure Apex One to notify end users after detecting a security risk.

Topics include:

- *[Security Agent Notifications on page 10-2](#)*

Security Agent Notifications

Apex One can display notification messages on Security Agent endpoints:

- Immediately after detecting a security risk. Enable the notification message and optionally modify its content.
- Immediately after detecting a web-based threat. Enable the notification message and optionally modify its content.

Configuring Virus/Malware Notifications for Security Agents

You can configure the Security Agent to notify end users of the result of attempting to clean or quarantine a virus/malware threat.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Virus/Malware**.
 3. Configure detection settings.
 - a. Choose to display one notification for all virus/malware related events, or separate notifications depending on the following severity levels:
 - **High:** The Security Agent was unable to handle critical malware
 - **Medium:** The Security Agent was unable to handle malware
 - **Low:** The Security Agent was able to resolve all threats
 - b. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring Spyware/Grayware Notifications for Security Agents

You can configure the Security Agent to notify end users of the result of attempting to clean or quarantine a spyware/grayware threat.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Spyware/Grayware**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring Firewall Notifications for Security Agents

You can configure the Security Agent to notify end users after the Apex One Firewall blocks outbound traffic that violated the firewall policy.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Firewall Violations**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring Web Reputation Notifications for Security Agents

You can configure the Security Agent to notify end users after detecting an attempt to access a malicious website.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Web Reputation Violations**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring Device Control Notifications for Security Agentss

You can configure the Security Agent to notify end users after blocking access to an unauthorized device.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Device Control Violations**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring Behavior Monitoring Notifications for Security Agents

You can configure the Security Agent to notify end users after blocking access to an application or process, or after detecting a newly-encountered program.

Procedure

1. Go to **Administration > Notifications > Agent**.
2. From the **Type** drop-down, select **Behavior Monitoring Policy Violations**.

3. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring C&C Callback Notifications for Security Agents

You can configure the Security Agent to notify end users whenever the endpoint attempts to contact a known C&C server.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **C&C Callbacks**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Configuring Predictive Machine Learning Notifications for Security Agents

You can configure the Security Agent to notify end users after detecting an unknown threat.

Procedure

1. Go to **Administration > Notifications > Agent**.
 2. From the **Type** drop-down, select **Predictive Machine Learning Violations**.
 3. Accept or modify the default messages.
 4. Click **Save**.
-

Part V

Updates and Administration



Chapter 11

Updates

This chapter discusses how to configure Security Agent updates and describes the components updated on the agents.

Topics include:

- *[Configuring Scheduled Updates for Security Agents on page 11-2](#)*
- *[Security Agent Update Sources on page 11-3](#)*

Configuring Scheduled Updates for Security Agents

Configure Apex One to automatically update all Security Agents on a set schedule. Keeping components updated ensures that you receive the best protection against the latest threats.

Procedure

1. Go to **Updates > Agents > Automatic Update**.
2. Configure the schedule for a **Schedule-based Update**.

- **Hour(s)**

The option to **Update agent configurations only once per day** is available when scheduling an hourly update frequency. The configuration file contains all Security Agent settings configured using the web console.



Tip

Trend Micro updates components often; however, Apex One configuration settings probably change less frequently. Updating the configuration files with the components requires more bandwidth and increases the time Apex One needs to complete the update. For this reason, Trend Micro recommends updating Security Agent configurations only once per day.

- **Daily or Weekly**

Specify the time of the update and the time period the Apex One server notifies agents to update components.

**Tip**

This setting prevents all online agents from simultaneously connecting to the server at the specified start time, significantly reducing the amount of traffic directed to the server. For example, if the start time is 12pm and the time period is 2 hours, Apex One randomly notifies all online agents to update components from 12pm until 2pm.

3. Click *Save*.

Security Agent Update Sources

Agents can obtain updates from the standard update source (Apex One server) or specific components from custom update sources such as the Trend Micro ActiveUpdate server. For details, see [Standard Update Source for Security Agents on page 11-4](#) and [Customized Update Sources for Security Agents on page 11-5](#).

IPv6 Support for Security Agent Updates

A pure IPv6 agent cannot update directly from pure IPv4 update sources, such as:

- A pure IPv4 Apex One server
- A pure IPv4 Update Agent
- Any pure IPv4 custom update source
- Trend Micro ActiveUpdate Server

Similarly, a pure IPv4 agent cannot update directly from pure IPv6 update sources, such as a pure IPv6 Apex One server or Update Agent.

A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the agents to connect to the update sources.

Standard Update Source for Security Agents

The Apex One server is the standard update source for agents.

If the Apex One server is unreachable, agents will not have a backup source and will therefore remain outdated. To update agents that cannot reach the Apex One server, Trend Micro recommends using Agent Packager. Use this tool to create a package with the latest components available on the server and then run the package on agents.



Note

The agent's IP address (IPv4 or IPv6) determines if connection to the Apex One server can be established. For details about IPv6 support for agent updates, see [IPv6 Support for Security Agent Updates on page 11-3](#).

Configuring the Standard Update Source for Security Agents

Procedure

1. Go to **Updates > Agents > Update Source**.
 2. Select **Standard update source (update from Apex One server)**.
 3. Click **Notify All Agents**.
-

Security Agent Update Process



Note

This topic discusses the update process for Security Agents. The update process for Update Agents is discussed in [Customized Update Sources for Update Agents on page 11-8](#).

After you have set up and saved the customized update source list, the update process proceeds as follows:

1. The Security Agent updates from the first source on the list.
2. If unable to update from the first source, the Security Agent updates from the second source, and so on.
3. If unable to update from all sources, the Security Agent checks the following settings on the **Update Source** screen:

TABLE 11-1. Additional Settings for Custom Update Sources

SETTING	DESCRIPTION
Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server	<p>If this setting is enabled, Update Agents update directly from the Apex One server and disregard the Customized Update Source List.</p> <p>If disabled, Update Agents apply the customized update source settings configured for normal agents.</p>
Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found:	
Components	<p>If this setting is enabled, the agent updates components from the Apex One server.</p> <p>If disabled, the agent then tries connecting directly to the Trend Micro ActiveUpdate server if any of the following is true:</p> <ul style="list-style-type: none"> • The ActiveUpdate server is not included in the Customized Update Source List.
Domain settings	If this setting is enabled, the agent updates domain-level settings from the Apex One server.
Security Agent programs and hot fixes	If this setting enabled, the agent updates programs and hot fixes from the Apex One server.

4. If unable to update from all possible sources, the agent quits the update process.

Customized Update Sources for Security Agents

Aside from the Apex One server, Security Agents can update from custom update sources. Custom update sources help reduce Security Agent update

traffic directed to the Apex One server and allow Security Agents that cannot connect to the Apex One server to get timely updates. Specify the custom update sources on the Customized Update Source List, which can accommodate up to 1024 update sources.

**Tip**

Trend Micro recommends assigning some Security Agents as Update Agents and then adding them to the list.

Configuring Customized Update Sources for Security Agents

**Important**

Apex One supports the use of HTTPS as the communication protocol between Update Agents and the Security Agents configured to receive updates from Update Agents. You must upgrade Update Agents and all Security Agents that report to the Update Agents to Apex One (or later) before changing the communication protocol to HTTPS.

Procedure

1. Go to **Updates > Agents > Update Source**.
2. Select **Customized Update Source**.
3. Select how Update Agents and Security Agents receive updates.
 - **Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server**
 - Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found:
 - **Components**
 - **Domain settings**
 - **Security Agent programs and hot fixes**

For more information, see [Security Agent Update Process on page 11-4](#).

4. If you specified at least one Update Agent as an update source, click **Update Agent Analytical Report** to generate a report that highlights the update status of endpoints.

For details about the report, see [Update Agent Analytical Report on page 11-10](#).

5. Add or edit **Customized Update Source List**.

- Click **Add** to specify a new update source.
- Click a value in the **IP Range** column to edit an existing update source.

**Note**

Edit an existing update source to change the communication protocol of an existing Apex One (or later) Update Agent to HTTPS.

The **Add/Edit IP Range and Update Source** screen appears.

6. Configure the IP addresses of endpoints that receive updates from the update source.
7. Specify the update source. You can select an Update Agent if one has been assigned or type the URL of a specific source.
 - **URL:** Specify the URL of the update source

**Note**

To change a preexisting Update Agent protocol from HTTP to HTTPS, modify the **URL** value.

- **Update Agent:** Select a preconfigured Update Agent from the drop-down and choose how Security Agents connect to the Update Agent
 - **Use the Update Agent IP address to connect**
 - **Use the Update Agent hostname to connect**

**Note**

Apex One automatically configures the **External Source** URL to use HTTPS protocol if the Update Agent has been updated to Apex One or later.

8. Click **Save**.
 9. Manage the **Customized Update Source List**.
 - a. Remove an update source from the list by selecting the check box and clicking **Delete**.
 - b. To move an update source, click the up or down arrow. You can only move one source at a time.
 10. Click **Notify All Agents**.
-

Customized Update Sources for Update Agents

Aside from the Apex One server, Update Agents can update from custom update sources. Custom update sources help reduce agent update traffic directed to the Apex One server. Specify the custom update sources on the Customized Update Source List, which can accommodate up to 1024 update sources. See [Customized Update Sources for Security Agents on page 11-5](#) for steps to configure the list.

**Note**

Ensure that the **Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server** option is disabled on the **Update Source for Agents** screen (**Updates > Agents > Update Source**) in order for Update Agents to connect to the customized update sources.

After you have set up and saved the list, the update process proceeds as follows:

1. The Update Agent updates from the first entry on the list.

2. If unable to update from the first entry, the agent updates from the second entry, and so on.
3. If unable to update from all entries, the agent checks the following options under the **Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found** heading:

- **Components:** If enabled, the agent updates from the Apex One server.

If the option is disabled, the agent then tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:

**Note**

You can only update components from the Active Update server. Domain settings, programs and hot fixes can only be downloaded from the server or Update Agents.

- In the assigned Security Agent policy in Apex Central, go to **Privileges and Other Settings > Other Settings > Update Settings**, the option **Security Agents download updates from the Trend Micro ActiveUpdate Server** is enabled.
 - The ActiveUpdate server is not included in the Customized Update Source List.
 - **Domain settings:** If enabled, the agent updates from the Apex One server.
 - **Security Agent programs and hot fixes:** If enabled, the agent updates from the Apex One server.
4. If unable to update from all possible sources, the Update Agent quits the update process.

The update process is different if the option **Standard update source (update from Apex One server)** is enabled and the Apex One server notifies the agent to update components. The process is as follows:

1. The agent updates directly from the Apex One server and disregards the update source list.
2. If unable to update from the server, the agent tries connecting directly to the Trend Micro ActiveUpdate server if any of the following are true:
 - In the assigned Security Agent policy in Apex Central, go to **Privileges and Other Settings > Other Settings > Update Settings**, the option **Security Agents download updates from the Trend Micro ActiveUpdate Server** is enabled.
 - The ActiveUpdate server is the first entry in the Customized Update Source List.

**Tip**

Place the ActiveUpdate server at the top of the list only if you experience problems updating from the Apex One server. When Security Agents update directly from the ActiveUpdate server, significant bandwidth is consumed between the network and the Internet.

3. If unable to update from all possible sources, the Update Agent quits the update process.

Update Agent Analytical Report

Generate the Update Agent Analytical Report to analyze the update infrastructure and determine which agents download partial updates from Update Agents and other update sources.

**Note**

This report includes all Security Agents configured to receive partial updates from Update Agents. If you have delegated the task of managing one or several domains to other administrators, they will also see all Security Agents configured to receive partial updates from Update Agents belonging to the domains that they are not managing.

Apex One exports the Update Agent Analytical Report to a comma-separated value (.csv) file.

This report contains the following information:

- Security Agent endpoint
- IP address
- Agent tree path
- Update source
- If agents download the following from Update Agents:
 - Components
 - Domain settings
 - Security Agent programs and hot fixes

**Important**

The Update Agent Analytical Report only lists Security Agents configured to receive partial updates from an Update Agent. Security Agents configured to perform complete updates from an Update Agent (including components, domain settings, and Security Agent programs and hot fixes) do not appear in the report.

For details on generating the report, see [Customized Update Sources for Security Agents on page 11-5](#).

Chapter 12

Administrative Settings

This chapter describes the available administrative settings for the Apex One server and Security Agents.

Topics include:

- *Account Management on page 12-2*
- *Smart Protection on page 12-3*
- *Notification Settings on page 12-6*
- *General Administrative Settings on page 12-6*

Account Management



Important

Creating a user account is only required in specific network environments. If you have a supported on-premises Apex Central or Control Manager server that you want to use to manage Apex One (Mac) as a Service and the Apex One as a Service console, you must create a user account to facilitate the communication between Apex One (Mac) as a Service and the Apex One as a Service console through Apex Central or Control Manager.

For more information on registering to an on-premises Apex Central or Control Manager server, see [Configuring Apex Central \(Control Manager\) Registration Settings on page 12-9](#).

For more information on registering Apex One (Mac) as a Service and the Apex One as a Service console using an on-premises Apex Central or Control Manager server, see <https://success.trendmicro.com/solution/1118614#step3>.

Procedure

1. Go to **Administration > Account Management > User Accounts**.

The **User Accounts** screen appears.

2. Click **Add**.
3. Ensure that you select the **Enable this account** check box.
4. Specify the **User name** for the account.
5. Specify the **Description** for the account.
6. Specify the **Password** and the confirmation password.

**Note**

Passwords must meet the following complexity requirements:

- Length of 8 to 32 characters
 - At least one of each: uppercase (A-Z), lowercase (a-z), numeric (0-9), and special character
 - Cannot contain the user name
 - Cannot contain non-printable ASCII characters
-

7. (Optional) Specify the **Email address** for the account.

8. Click **Next**.

The **Step 2 Agent Domain Control** screen appears.

**Important**

The settings on the screen do not affect the communication settings. You do not need to modify any settings.

9. Click **Next**.

The **Step 3 Define Agent Tree Menu** screen appears.

**Important**

The settings on the screen do not affect the communication settings. You do not need to modify any settings.

10. Click **Finish**.

The account appears in the table on the **User Accounts** screen.

Smart Protection

- [Smart Protection Sources for Internal Agents on page 12-4](#)

- [Smart Feedback on page 12-5](#)

Smart Protection Sources for Internal Agents

A Security Agent's location is internal if its gateway IP address matches any of the gateway IP addresses specified on the **Endpoint Location** screen, or if the agent can connect to any reference server. Configure the range of Security Agent IP addresses and assign a customized list of Smart Protection Servers to each.

For more information, see [Endpoint Location on page 4-20](#).

Procedure

1. Go to **Administration > Smart Protection > Smart Protection Sources**.
2. Click the **Internal Agents** tab.
3. Click **Add**.
4. In the **IP Range** section, specify an IPv4 address range.
5. In the **Custom Smart Protection Server List**, add the Smart Protection Servers.
 - a. Specify the Smart Protection Server's host name or IPv4 address.
 - b. Enable **File Reputation Services**.
 - c. Enable **SSL** if your organization uses HTTPS protocol.
 - d. Specify the Smart Protection Server's listening **Port** for the requests.
 - e. Enable **Web Reputation Services**. Agents send web reputation queries using the HTTP protocol. HTTPS is not supported.
 - f. Specify the Smart Protection Server's listening **Port** for the requests.
 - g. Click **Add to the List**.
 - h. Add more servers by repeating the previous steps.

- i. Select **Order** or **Random**.
 - **Order:** Agents pick servers in the order in which they appear on the list. If you select **Order**, use the arrows under the **Order** column to move servers up and down the list.
 - **Random:** Agents pick servers randomly.
 6. Click **Save**.

The **Smart Protection Sources** screen appears with the configured Security Agent IP range displaying in the table.
 7. Click **Save and Notify Agents**.
-

Smart Feedback

Smart Feedback shares protected threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats which also allows Trend Micro to scan Smart Feedback data for early attack indicators. You can disable Smart Feedback anytime through this console.

Participating in the Smart Feedback Program

Procedure

1. Go to **Administration > Smart Protection > Smart Feedback**.
2. Select **Enable Trend Micro Smart Feedback and agree to allow targeted attack indicator scanning and notification**.
3. To help Trend Micro understand your organization, select the **Industry** type.
4. To send information about potential security threats in the files on your Security Agents, select the **Enable feedback of suspicious program files** check box.

**Note**

Files sent to Smart Feedback contain no user data and are submitted only for threat analysis.

5. To configure the criteria for sending feedback, select the number of detections for the specific amount of time that triggers the feedback.
 6. Specify the maximum bandwidth Apex One can use when sending feedback to minimize network interruptions.
 7. Specify the recipient email addresses to receive notifications on discovered targeted attack indicators.
-

**Tip**

- You can add up to 20 entries separated by a comma.
 - To send test email messages to only the recipients you specify, click **Send Test Message**.
-

8. Click **Save**.
-

Notification Settings

Apex One allows you to configure agent notifications to inform end users about detections on specific endpoints.

For information regarding the different types of Security Agent notification settings, refer to the following chapter: [Notifications on page 10-1](#).

General Administrative Settings

- [Configuring Proxy Settings for Agent Connections on page 12-7](#)
- [Configuring Inactive Agent Removal Settings on page 12-7](#)

- [Configuring Apex Central \(Control Manager\) Registration Settings on page 12-9](#)
- [Configuring Web Console Settings on page 12-11](#)
- [Configuring Suspicious Object List Settings on page 12-12](#)
- [Migrating from an On-premises OfficeScan Server to Apex One as a Service on page 12-13](#)

Configuring Proxy Settings for Agent Connections

Agents use the proxy server settings configured in Windows Internet Options when connecting to the Apex One server and the Trend Micro Smart Protection Network.

Procedure

1. Go to **Administration > Settings > Proxy**.
 2. If the proxy server requires authentication, type the user name and password and then confirm the password.
 3. Click **Save**.
-

Configuring Inactive Agent Removal Settings

You can configure when Apex One changes the status of Security Agents to “inactive”. Apex One defines an agent as being “inactive” after the Security Agent does not report back to the server for any of the following reasons:

- The Security Agent program was removed from the endpoint manually
- A user disabled or unloaded the Security Agent program for an extended period

You can configure Apex One to automatically remove inactive Security Agents from the agent tree.

Procedure

1. Go to **Administration > Settings > Inactive Agents**.
 2. Select **Enable automatic removal of inactive agents**.
 3. Select how many days should pass before Apex One considers the Security Agent inactive.
 4. Click **Save**.
-

Enabling Client Authentication Checksum Security

To enhance communication security between the Apex One server and Security Agents, you can enable Client Authentication Checksum (CAC) security in Apex One to authenticate Security Agents.



WARNING!

Before enabling Client Authentication Checksum (CAC) security, verify that all managed Security Agents reporting to the Apex One server are running supported versions (build version 12000 or later).

Procedure

1. Go to **Agents > Global Agent Settings**.
 2. Click the **Network** tab.
 3. Go to the **Server-Agent Communication** section.
 4. Click **Change** to enable or disable the setting.
A message appears.
 5. Click **Verify Versions** to confirm that you have updated all Security Agents to the supported versions (build version 12000 or later).
 6. Click **OK**.
-

Configuring Apex Central (Control Manager) Registration Settings

By default, registration to Apex Central as a Service is automatically set up during the Apex One provisioning process. You can register to a different on-premises Apex Central or Control Manager server if required (for example, you want to subscribe to Suspicious Object Lists from an on-premises Apex Central or Control Manager server).



Important

- Apex One only supports re-registration to an on-premises Apex Central or Control Manager 7.0 (or later) server.
 - If you are registering to an on-premises Apex Central or Control Manager 7.0 (or later) server, you must first run the Apex One as a Service Remote Connection Tool on an endpoint in the DMZ to facilitate communication between the cloud-based Apex One console and the local Apex Central or Control Manager server.
-

Procedure

1. Go to **Administration > Settings > Apex Central**.
 2. Click **Register to a Different Apex Central Server**.
 3. Specify the **Server FQDN or IP address** of the new Apex Central (or Control Manager) server.
-



Important

- You must specify a different on-premises Apex Central or Control Manager server than the server that Apex One has currently registered.
 - If you have set up an endpoint to establish a remote connection to an on-premises Apex Central or Control Manager server, specify the **Server FQDN or IP address** of the reverse proxy endpoint.
-

4. Specify the **Port (HTTPS)** of the Apex Central or Control Manager server.

**Important**

If you have set up an endpoint to establish a remote connection to an on-premises Apex Central or Control Manager server, specify the **Port (HTTPS)** of the reverse proxy endpoint.

5. Beside **Apex Central certificate**, click **Browse...** and select the certificate file downloaded from the target Apex Central or Control Manager server.

To obtain the Apex Central or Control Manager certificate file, go to the on-premises Apex Central or Control Manager server and copy the certificate file to the Apex One server from the following location:

```
<Control Manager installation folder>\Certificate\CA  
\TMCMA_Cert.pem
```

**Important**

If your company uses a customized certificate on the Apex Central or Control Manager server, you must upload the Root CA certificate during the Apex Central or Control Manager registration.

For more information, see [Apex Central Certificate Authorization on page 12-11](#).

6. If the IIS web server of the on-premises Apex Central or Control Manager server requires authentication, type the user name and password.
7. Specify the **Entity display name** that identifies the Apex One server on the Apex Central or Control Manager console.

By default, entity display name includes the server computer's host name and this product's name (for example, Server01_OSCE).

8. Click **Connect**.
-

Apex Central Certificate Authorization

Before registering Apex One to the Apex Central server, you must first obtain the Apex Central certificate file from the Apex Central server from the following location:

```
<Apex Central installation folder>\Certificate\CA  
\TMCN_CA_Cert.pem
```

Apex One and Apex Central use the certificate and public key encryption to ensure that only authorized registration and policy management communication occurs between the servers. If either server detects unauthorized communication, the server rejects any registration or policy settings being received.



Important

If your company uses a customized certificate on the Apex Central server, you must upload the Root CA certificate during the Apex Central registration.

Configuring Web Console Settings

Configure the Apex One web console settings to determine how users access the web console and how often a screen refresh occurs.

Procedure

1. Go to **Administration > Settings > Web Console**.

2. Configure the Automatic Refresh Settings.

Select **Automatically refresh the web console** to enable the Apex One server to refresh screen data at the specified interval

- **Refresh interval:** Select the frequency (in seconds) in which the web console refreshes the screen data

3. Click **Save**.

Configuring Suspicious Object List Settings

During Apex One registration to an on-premises Apex Central, Apex Central deploys an API key to Apex One to start the subscription process. To enable this automatic subscription process, check with the Apex Central administrator to ensure that Apex Central is connected to a Virtual Analyzer or that the Suspicious Object Lists have been manually populated.

For details on registering to an on-premises Apex Central or Control Manager server, see [Configuring Apex Central \(Control Manager\) Registration Settings on page 12-9](#).



Important

If you are using Apex One as a Service with the Apex One Sandbox as a Service Add-on, you do not need to configure the **Suspicious Object List Subscription** settings.

Procedure

1. Go to **Administration > Settings > Suspicious Object List**.
2. Select which list to enable on Security Agents.
 - Suspicious URL List
 - Suspicious IP List (only available when subscribing to registered Apex Central or Control Manager server)
 - Suspicious File List (only available when subscribing to registered Apex Central or Control Manager server)
 - Suspicious Domain List (only available when subscribing to registered Apex Central or Control Manager server)

Administrators can manually synchronize the Suspicious Object lists at any time by clicking the **Sync Now** button.

3. Under **Update the Suspicious Object lists on Security Agents**, specify when agents update the Suspicious Object lists.

- **Based on the Security Agent component update schedule:** Security Agents update the Suspicious Object lists based on the current update schedule.
- **Automatically after updating the Suspicious Object lists on the server:** Security Agents automatically update the Suspicious Object lists after the Apex One server receives updated lists.

**Note**

Security Agents not configured to receive updates from Update Agents perform incremental updates of the subscribed Suspicious Object lists during synchronization.

4. Click **Save**.
-

Migrating from an On-premises OfficeScan Server to Apex One as a Service

Apex One supports migrating server and Security Agent settings from an on-premises OfficeScan server running version XG SP1 (or later). Ensure that you upgrade all Security Agents that you want to migrate to the Apex One server before attempting the migration process.

**Note**

If you have Security Agents running on virtual machines or using VPNs, ensure that your environments meets the prerequisite criteria.

[Migration Prerequisites for Virtual Desktops and VPN Clients on page 12-14](#)

The migration process requires that you perform the following tasks:

1. Use the Server Migration Tool to import the source OfficeScan or Apex One server settings to the Apex One console.

For more information, see *[Using the Apex One Settings Export Tool on page 12-15](#)*.

2. Migrate the source OfficeScan or Apex One server policy settings to the Apex Central as a Service console.

For more information, see [Migrating On-premises OfficeScan Policy Settings to the Apex Central Console on page 12-20](#).

3. Move Security Agents from the source server to Apex One



Important

Before moving Security Agents to the Apex One server, ensure that you change the proxy settings for the Security Agents on the on-premises server console to **Use Windows proxy settings** in order to allow the Security Agents to connect to the Apex One console.

For more information, see the *Configuring Internal Agent Proxy Settings* topic in the *OfficeScan Administrator's Guide*.

For more information, see [Moving Security Agents to Another Domain or Server on page 3-8](#).

Migration Prerequisites for Virtual Desktops and VPN Clients

Before migrating on-premises Security Agents running on virtual machines or using VPNs, ensure that the following settings are correct in the <Server installation directory>\PCCSRV\Private\ofcserver.ini file on the on-premises OfficeScan XG Service Pack 1 (or later) or Apex One server:

- For non-persistent Virtual Desktop Support environments:
 1. In the <Server installation directory>\PCCSRV\Private\ofcserver.ini file, locate the [INI_SERVER_SECTION].
 2. Ensure that the following value exists:


```
EnableCheckClientMacAddress=1
```
 3. Save the file.
 4. On the on-premises web console, go to **Agents > Global Agent Settings**.

5. Click **Save** to deploy the setting to all Security Agents.
- For VPN clients (for example, Cisco Anyconnect):
 1. In the <Server installation directory>\PCCSRV\Private\ofcserver.ini file, locate the [INI_SERVER_SECTION].
 2. Ensure that the following value exists:
`SP_DisableTmLwfRegistryKeyProtection=1`
 3. Save the file.
 4. On the on-premises web console, go to **Agents > Global Agent Settings**.
 5. Click **Save** to deploy the setting to all Security Agents.

Using the Apex One Settings Export Tool



Important

This version of Apex One only supports migrations from OfficeScan version XG SP1 and later. Ensure that you upgrade both the source OfficeScan server and all migrated Security Agents to version XG SP1 or later before attempting to migrate settings.

For a complete list of the settings that the Apex One Settings Export Tool migrates, see [The Apex One Settings Export Tool on page 12-17](#).

Procedure

1. Locate the Server Migration Tool package.
 - From the Apex One web console, go to **Administration > Settings > Server Migration** and click the **Download Apex One Settings Export Tool** link.
2. Copy the Apex One Settings Export Tool to the source OfficeScan server computer.

**Important**

You must use the Apex One Settings Export Tool on the source OfficeScan server version to ensure that all data is properly formatted for the new target server. Apex One is not compatible with older versions of the Server Migration Tool.

3. Open a command prompt with administrative privileges, change to the location of the tool, and execute `ApexOneSettingsExportTool.exe`.

The Apex One Settings Export Tool runs.

**Note**

The default names of the export packages are:




- `ApexOne_Agent_DLP_Policies.zip` (used to import DLP policy settings into Apex Central)
 - `ApexOne_Agent_Policies.zip` (used to import all other Security Agent policy settings into Apex Central)
 - `Server_Settings_Migration.zip` (used to import all Security Agent policy settings and OfficeScan server settings to another Apex One server)
-

4. Copy the export package(s) to a location that the destination Apex One or Apex Central server can access.
5. To import the settings to the destination Apex One server:
 - a. From the Apex One web console, go to **Administration > Settings > Server Migration** and click the **Import Settings...** button.
 - b. Locate the `Server_Settings_Migration.zip` package and click **Open**.
 - c. Verify that the server contains all the previous OfficeScan version settings.
6. To import the Security Agent policy settings to the destination Apex Central console:

- a. From the Apex Central web console, go to **Policies > Policy Management**.
 - b. In the **Product** drop-down, select **Apex One Security Agent**.
 - c. Click **Import Settings**.
 - d. Locate the `ApexOne_Agent_Policies.zip` package and click **Open**.
 7. To import the Security Agent DLP policy settings to the destination Apex Central console:
 - a. From the Apex Central web console, go to **Policies > Policy Management**.
 - b. In the **Product** drop-down, select **Apex One Data Loss Prevention**.
 - c. Click **Import Settings**.
 - d. Locate the `ApexOne_Agent_DLP_Policies.zip` package and click **Open**.
 8. Move the old Security Agents to the new Apex One server.
-

The Apex One Settings Export Tool

Apex One provides the Apex One Settings Export Tool, which allows administrators to copy Apex One settings from previous Apex One versions to the current version. The Apex One Settings Export Tool migrates the following settings:

FEATURE	MIGRATED SETTINGS
<p>Agent Management</p> <hr/>  Note The Apex One Settings Export Tool migrates the applicable Agent Management settings to the ApexOne_Agent_DLP_Policies.zip and ApexOne_Agent_Policies.zip packages for use during import to Apex Central.	<ul style="list-style-type: none"> Manual Scan Scheduled Scan Real-time Scan Scan Now Scan Method Web Reputation Behavior Monitoring Device Control Data Loss Prevention Privileges and Other Settings Additional Service Settings Spyware/Grayware Approved List Predictive Machine Learning Suspicious Connection Trusted Program List <hr/>  Note <ul style="list-style-type: none"> The Server Migration Tool does not migrate the backup directories for Manual Scan, Scheduled Scan, Real-time Scan, and Scan Now. Settings retain the configurations at both the root and domain level.
<p>Agent Grouping</p>	<p>All settings</p> <hr/>  Note The Active Directory domain structures display after synchronizing with Active Directory the first time.
<p>Global Agent Settings</p>	<p>All settings</p>
<p>Endpoint Location</p>	<ul style="list-style-type: none"> Location awareness settings Gateway IP address and MAC lists
<p>Data Loss Prevention</p>	<ul style="list-style-type: none"> Data Identifiers Templates
<p>Firewall</p>	<ul style="list-style-type: none"> Policies Profiles

FEATURE	MIGRATED SETTINGS
Log Maintenance	All settings
Agent Update Source	<ul style="list-style-type: none"> • Agent update source • Customized update source list
Smart Protection Sources	Customized smart protection source list
Notifications	<ul style="list-style-type: none"> • General notification settings • Administrator notification settings • Outbreak notification settings • Agent notification settings
Proxy	All settings
Inactive Agents	All settings
Quarantine Manager	All settings
Web Console	All settings
ofcscan.ini settings	<ul style="list-style-type: none"> • [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: All settings
ofcserver.ini settings	[INI_SERVER_DISK_THRESHOLD]: All settings

**Note**

- The tool does not back up the Security Agent listings of the Apex One server; only the domain structures.
- The tool only migrates features available on the older version of the Apex One server. For features that are not available on the older server, the tool applies the default settings.

Migrating On-premises OfficeScan Policy Settings to the Apex Central Console

OfficeScan XG SP1 (or later) provides a Policy Export Tool that you can use to migrate on-premises OfficeScan server policies to the Apex Central console to ensure that you maintain your current level of security without needing to reconfigure all of your current policy settings.



Note

The Policy Export Tool can only export domain-level policy settings. If you have configured individual Security Agents with customized settings, you must manually re-create the individual policies.

Procedure

1. Go to the source OfficeScan XG SP1 server computer.
2. Use a command line editor and point to the following directory:

```
<Server installation directory>\PCCSRV\Admin\Utility  
\PolicyExportTool
```

3. Execute the following command:

```
PolicyExportTool.exe -cmconsole
```

The Policy Export Tool saves the policy settings in the following location:

```
<Server installation directory>\PCCSRV\Admin\Utility  
\PolicyExportTool\PolicyClient_CMConsole.zip
```

4. Log on to the Apex Central console and go to **Policies > Policy Management**.
5. In the **Product** drop-down, select **Apex One Security Agent**.
6. Click **Import Settings**.

7. Select the <Server installation directory>\PCCSRV\Admin\Utility\PolicyExportTool\PolicyClient_CMConsole.zip file and import.

The migrated policy settings display in the Apex One Security Agent Policy Management list. Apex Central appends the original OfficeScan domain name to the end of each policy name.

Part VI

Getting Help



Chapter 13

Technical Support

Learn about the following topics:

- *[Troubleshooting Resources on page 13-2](#)*
- *[Contacting Trend Micro on page 13-3](#)*
- *[Sending Suspicious Content to Trend Micro on page 13-4](#)*
- *[Other Resources on page 13-5](#)*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to <https://success.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

To submit a support case online, visit the following URL:

<https://success.trendmicro.com/smb-new-request>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy.

The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<https://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:

<https://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

<https://servicecentral.trendmicro.com/en-us/ers/>

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

<https://success.trendmicro.com/solution/1112106>

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

<https://success.trendmicro.com/solution/1059565>

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

<https://global.sitesafety.trendmicro.com/>

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

<https://www.trendmicro.com/download/>

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<https://docs.trendmicro.com/en-us/survey.aspx>

Index

A

- ActiveAction, 5-9
- Additional Service Settings, 2-26
- agent grouping, 3-6–3-8
 - adding a domain, 3-6
 - deleting a domain or agent, 3-6
 - moving agents, 3-8
 - renaming a domain, 3-7
 - tasks, 3-6
- agents, 3-6, 3-8
 - deleting, 3-6
 - moving, 3-8
- agent tree, 3-2, 3-3
 - about, 3-2
 - advanced search, 3-3
 - general tasks, 3-3
 - specific tasks, 3-2
 - agent management, 3-2
- agent uninstallation, 2-31
- agent update
 - customized source, 11-5
 - standard source, 11-4
- Apex One
 - components, 8-18
 - documentation, vi
 - programs, 8-18
 - web console, 1-8
- C**
- C&C callbacks
 - widgets, 8-14
- Certified Safe Software List, 6-2
- components, 8-18

D

- Damage Cleanup Services, 1-4
- dashboards
 - Summary, 8-2
- Data Loss Prevention
 - widgets, 8-12
- Device Control, 1-5
- documentation, vi
- documentation feedback, 13-6
- domains, 3-6, 3-7
 - adding, 3-6
 - deleting, 3-6
 - renaming, 3-7

F

- firewall, 6-2
 - default policy exceptions, 6-8, 6-9
 - policies, 6-4
 - profiles, 6-11
 - testing, 6-17

G

- gateway IP address, 4-21

I

- inactive agents, 12-7

L

- location awareness, 4-20
- logs
 - central quarantine restore logs, 9-3
 - scan logs, 9-2
 - system event logs, 9-4

M

- MAC address, 4-21

N

notifications

- agent users, 10-2

O

outbreak prevention, 8-17

- disabling, 7-9

- policies, 7-2

outbreak prevention policy

- block ports, 7-3

- deny compressed file access, 7-6

- deny write access, 7-4

- executable compressed files, 7-6

- limit/deny access to shared

- folders, 7-2

- mutex handling, 7-7

- mutual exclusions, 7-7

P

pattern files

- Web Blocking List, 1-6

policies

- firewall, 6-4

port blocking, 7-3

programs, 8-18

Q

quarantine directory, 5-12

R

reference server, 4-22

S

scan exclusions, 5-17

Scan Now, 5-2

Security Agent, 2-3

- connection, 4-17

- connection with Apex One server, 4-5

- detailed agent information, 3-5

- icons, 4-17

- inactive agents, 12-7

- uninstallation, 2-31

- Windows 10, 2-4

- Windows 11, 2-5

- Windows 7, 2-2

- Windows 8.1, 2-3

- Windows HPC Server 2008 R2, 2-9

- Windows MultiPoint Server 2010, 2-10

- Windows MultiPoint Server 2011, 2-11

- Windows MultiPoint Server 2012, 2-16

- Windows Server 2008 R2, 2-7

- Windows Server 2012, 2-12

- Windows Server 2012 Failover Clusters, 2-17, 2-18

- Windows Server 2012 R2, 2-13

- Windows Server 2016, 2-20

- Windows Server 2016 Failover Clusters, 2-21

- Windows Server 2019, 2-23

- Windows Server 2022, 2-24

- Windows Storage Server 2008 R2, 2-8

- Windows Storage Server 2012, 2-14

- Windows Storage Server 2012 R2, 2-15

- Windows Storage Server 2016, 2-22

security risks

- protection from, 1-3

- smart protection, 1-5, 1-6

- pattern files, 1-6
 - Web Blocking List, 1-6
- Smart Protection Network, 1-5
- Smart Protection, 1-6
 - Web Reputation Services, 1-6
- Smart Protection Network, 1-5
- summary
 - dashboard, 8-2
- summary dashboard
 - components and programs, 8-18
- Summary dashboard, 8-2
 - tabs, 8-2
 - widgets, 8-2
- support
 - resolve issues faster, 13-4
- Support Intelligence System, 1-9

T

- tabs, 8-2
- terminology, viii
- Top 10 Security Risk Statistics for Networked Endpoints, 8-18
- Trojan horse program, 1-4

U

- uninstallation, 2-31
 - from the web console, 2-31
 - using the uninstallation program, 2-32
- Update Agent
 - analytical report, 11-10
- update source
 - agents, 11-3

W

- Web Blocking List, 1-6
- web console, 1-8

- about, 1-8
- Web Reputation, 1-4
- Web Reputation Services, 1-6
- widgets, 8-2, 8-12, 8-14–8-18
 - Agent-Server Connectivity, 8-18
 - Agent Updates, 8-18
 - Antivirus Agent Connectivity, 8-16
 - Apex One and Plug-ins Mashup, 8-16
 - C&C Callback Events, 8-14
 - Data Loss Prevention - Detections Over Time, 8-12
 - Data Loss Prevention - Top Detections, 8-12
 - Outbreaks, 8-17
 - Security Risk Detections, 8-15
- Windows 10, 2-4
- Windows 11, 2-5
- Windows 7, 2-2
- Windows 8.1, 2-3
- Windows HPC Server 2008 R2, 2-9
- Windows MultiPoint Server 2010, 2-10
- Windows MultiPoint Server 2011, 2-11
- Windows MultiPoint Server 2012, 2-16
- Windows Server 2008 R2, 2-7
- Windows Server 2012, 2-12
- Windows Server 2012 Failover Clusters, 2-17, 2-18
- Windows Server 2012 R2, 2-13
- Windows Server 2016, 2-20
- Windows Server 2016 Failover Clusters, 2-21
- Windows Server 2019, 2-23
- Windows Server 2022, 2-24
- Windows Storage Server 2008 R2, 2-8
- Windows Storage Server 2012, 2-14

Windows Storage Server 2012 R2, 2-15

Windows Storage Server 2016, 2-22



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM009709/230327