



Trend Micro Apex One™ Training for Certified Professionals

On-premises - Student Guide



Copyright © 2021 Trend Micro Incorporated. All rights reserved.

Trend Micro, the Trend Micro t-ball logo, InterScan, 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.

Portions of this manual have been reprinted with permission from other Trend Micro documents. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Information in this document is subject to change without notice.

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

Released: April 7, 2021
Trend Micro Apex One
Courseware v4.2 (on-premises edition)

Table of Contents

Lesson 1: Trend Micro Apex One Overview	1
Trend Micro Solutions.....	1
Network Defense	1
Hybrid Cloud Security	2
User Protection	2
Trend Micro Smart Protection Network	2
Visibility and Control	3
Trend Micro XGen™ Security	3
Smart	3
Optimized	3
Connected	4
Trend Micro Apex One	4
Trend Micro Apex One Deployment Methods	4
On-premises Deployment	4
Software as a Service Deployment	5
Key Features of Trend Micro Apex One	6
Malware Protection	6
Ransomware Protection	6
Predictive Machine Learning	6
Behavior Monitoring	6
Sandbox Analysis	7
Web Threat Protection	7
Firewall Protection	7
Data Loss Prevention	7
Device Control	7
Outbreak Control	7
Application Control	7
Virtual Patching	8
Endpoint Detection and Response	8
Endpoint Encryption	8
Cloud-based Intelligence	8
Automated Updates	8
Multi-Platform Support	8
Simplified Administration	9
Off-premises Management	9
Unified Agent	9
Trend Micro Apex One Components	10
Apex One Server	10
Apex One (Mac) Server	11
Database	11
Microsoft Internet Information Server	11
Apex One/Apex One (Mac) Web Management Console	11
Apex Central	11
Security Agents	12
Apex One Edge Relay Server	12
Trend Micro Smart Protection Network	12
Smart Protection Server	12
Trend Micro ActiveUpdate Server	12
Update Agents	12
Trend Micro Endpoint Encryption	13
Deep Discovery Analyzer	13

Mac Sandbox	13
Software as a Service Components	13
Optional Third-Party Components	14
Threat Detection	14
Detecting Threats at the Entry Point	14
Detecting Threats Pre-execution	15
Detecting Threats at Runtime	15
Detecting Threats at the Exit Point	15
Lesson 2: Trend Micro Apex One Server	17
Apex One Server Tasks	17
Apex One Server Services and Components	18
Web Server	19
Apex One (Mac) Plug-in	20
Data Loss Prevention Plug-in	20
Configuration Repositories.....	20
Apex One Database	21
Installing the Apex One Server.....	21
Hardware Requirements	22
Apex One Server Pre-Installation Checklist	22
Downloading Apex One Server for Windows	23
Running the Setup	23
Installation Logs	36
Confirming Successful Installation	36
Ports and Protocols to Allow	37
Upgrading OfficeScan to Apex One (on-premises).....	38
In-place Migration	38
New Server	42
Upgrading OfficeScan as a Service to Apex One as a Service.....	44
Upgrading OfficeScan Agents to Apex One Security Agents	44
Upgrading to the Integrated Agent	45
Upgrading to Apex One as a Service.....	45
Pre-Upgrade Backup Considerations.....	45
Server Service Setup Utility	46
Apex One (Mac)	48
Installing the Apex One (Mac) Plug-In	48
Apex One Plug-Ins.....	50
Apex One Data Protection	51
Trend Micro Endpoint Encryption Deployment Tool	51
Apex One (Mac)	51
Trend Micro Virtual Desktop Support	51
Trend Micro Apex One Toolbox	52
Apex One Utilities	52
Authentication Certificate Manager	52
Agent Packager	52
Cisco Trust Agent	52
Domains Schedule Update	53
Edge Relay Server Installer	53
Gateway Settings Importer	53
Image Setup	53
Agent Mover	54
Integrated Service Package	54
Integrated Smart Protection Server Tool	54
Device List Tool	54

Message Queue	54
Console Password Reset Tool	55
Plug-in Manager Installer	55
Apex One Settings Export Tool	55
Apex One Server Migration Tool	55
ServerProtect Normal Server Migration Tool	55
Server Tuner	56
Apex One VDI Pre-Scan Template Generation Tool	56
System Health Validator	56
Trend Micro Vulnerability Scanner	56
Cache Generator	56
Touch Tool	57
Decrypt Tool	57

Lesson 3: Trend Micro Apex One Web Management Console59

Logging into the Web Management Console	60
Web Management Console Communication	61
Login Process	62
Certificate warnings	62
Timeout Mechanism	63
Automatic Refresh	64
Active Directory Integration	64
Apex One Active Directory Integration Service	65
Authenticating Administrative Users From Active Directory	66
Administrative Accounts.....	66
Defining User Roles	67
Configuring User Accounts	69
Domain permissions	73
Recovering From Forgotten Passwords.....	73

Lesson 4: Managing Security Agents75

Security Agent Tasks	75
Security Agent Services and Components	76
Security Agent Tree	78
Security Agent System Requirements.....	79
Hardware Requirements	79
Security Agent Features by Platform.....	80
Installing Security Agents.....	81
Security Agent Deployment Prerequisites	81
Remote Installation	81
Unmanaged Endpoints	83
Installer Link	84
AutoPcc	84
Agent Packager	85
Microsoft System Center Configuration Manager or Active Directory Installation	86
Agent Disk Images	86
Apex Central	86
Migrating From Other Endpoint Security Software	88
tmuninst_as.ptn	88
tmuninst.ptn	89
Coexist Mode	89
Post Installation Tasks.....	90
Component Updates	90

Test Scan using EICAR Test Script	90
Installation Logs	90
Agent-To-Server Communication	91
Server-to-Agent Communication	92
Authenticating Server-Initiated Communications	94
Support for third-party certificates	95
Using a Single Key With Multiple Apex One Servers	95
Heartbeat	95
Server Polling	96
Agent Connection Status	96
Online	97
Offline	97
Independent	97
Off-premises	97
Endpoint Location.....	98
Reference Server List	98
Gateways	99
Moving Agents Between Apex One Servers.....	100
Agent Mover Tool	101
Uninstalling Security Agents.....	103
Uninstalling From the Web Management Console	103
Uninstalling from Windows Control Panel	103
Uninstalling Manually	104
Custom Uninstall Tool	104
Removing Inactive Agents.....	105
Security Agent Settings	105
Root Settings	106
Domain Settings	106
Agent Settings	107
Agent Grouping	107
Manual Grouping	107
Automatic Grouping	108
Viewing Agent Status.....	110
Viewing Agent Status on the Endpoint	111
Viewing Agent Status in the Web Management Console	112
Agent Self Protection	112
Configuring Unauthorized Change Prevention	113
Kernel Mode Termination Protection	115
Security Agent Service Restart	115
Agent Privileges	116
Lesson 5: Managing Off-premises Agents	119
Edge Relay Server and External Agent Communications.....	120
Installing the Apex One Edge Relay Server	121
Registering the Edge Relay Server.....	125
Viewing Off-premises Agents	126
Apex One Relay Server Digital Certificates.....	127
Renewing Edge Relay Server Certificate	127
Lesson 6: Keeping Trend Micro Apex One Up To Date	129
ActiveUpdate.....	129
ActiveUpdate Integrity	129
Pattern Updates	130

Incremental Updates	130
ActiveUpdate Logs	130
Updating the Apex One Server	131
Manual Server Updates	131
Scheduled Server Update	132
Server Update Source	132
Updating Security Agents	133
Automatic Updates	133
Manual Updates	134
Privilege-based Updates	135
Agent Update Source	135
Update Agents	136
Promoting an Agent to an Update Agent	137
Update Components	138
Downloading and Deploying Updates	139
Security Compliance	140
Services	141
Components	141
Scan Compliance	142
Settings	143
Update Summary	144
Rollback	145
Server Tuner Tool.....	146
Download Settings	147
Network Traffic Settings	147
Default Settings	148
Recommended Configurations for Improved Performance	148
Update Utilities	148
Domains Schedule Update Tool	148
Scheduled Update Configuration Tool	149
Lesson 7: Trend Micro Smart Protection	151
File Reputation Services	151
Web Reputation Services	151
Predictive Machine Learning Services	152
Census Service	152
Certified Safe Software Service	152
Smart Feedback	153
Service URLs	153
Smart Protection Sources	154
Trend Micro Smart Protection Network	154
Smart Protection Server	154
Configuring the Agent Smart Protection Source.....	156
Lesson 8: Protecting Endpoint Computers From Malware	159
Scanning for Malware	159
NT Real-time Scan Service	159
Scan Settings	160
Real-Time Scan Settings	161
Manual Scan Settings	169
Scheduled Scan Settings	173
Scan Now Settings	176
Trusted Program List	179

Scan Caching	179
Quarantining Detected Malware	181
Restoring Quarantined Files	183
Central Quarantine Restore	183
Smart Scan	184
File Reputation	185
Querying the File Reputation Database	187
CRC Caching	189
Spyware/Grayware Protection.....	190
VSAPI	190
SSAPI	191
Damage Cleanup Services	192
Damage Cleanup Services Components	194
Assessment Mode	194
Preventing Outbreaks.....	195
Outbreak Prevention Policy	195
Outbreak Notifications	196
Starting Outbreak Prevention	197
Terminating Outbreak Prevention	199
Lesson 9: Protecting Endpoint Computers Through Behavior Monitoring	201
Behavior Monitoring.....	201
Malware Behavior Blocking	202
Ransomware Protection	203
Anti-Exploit Protection	204
Fileless Malware Protection	204
Newly Encountered Program Protection	207
Event Monitoring	209
Behavior Monitoring Exception List	211
Lesson 10: Protecting Endpoint Computers From Unknown Threats	213
Common Vulnerabilities and Exposures Exploits.....	213
Supported File Types	214
Predictive Machine Learning.....	214
File Detections	215
Process Detections	216
Enabling Predictive Machine Learning	216
Exceptions	217
Connection Settings	217
Offline Predictive Machine Learning	219
Predictive Machine Learning Local File Model	220
Lesson 11: Blocking Web Threats	221
Web Reputation	221
Credibility Scores	222
Configuring Web Reputation Settings	223
Untested URLs	225
Sample Sites	226
Dealing With False Positives	226
Intercepting HTTPS Traffic	226
Bypassing Web Reputation Analysis	228
URL Analysis Order	229
Assessment Mode	230

Detecting Suspicious Connections	231
Detecting Connections Through the Global C&C List	231
Protecting Against Browser Exploits	232
Lesson 12: Protecting Endpoint Computers Through Traffic Filtering	233
Traffic Filtering.....	233
Firewall Filtering	233
Application Filtering	234
Certified Safe Software List	234
Stateful Inspection	234
Intrusion Detection System	234
Enabling the Apex One Firewall.....	235
Enabling the Apex One Firewall on Selected Endpoints	235
Firewall Policies and Profiles	236
Firewall Policies	236
Firewall Profiles	239
Viewing Firewall Rules	242
Lesson 13: Preventing Data Loss on Endpoint Computers	245
Apex One Data Loss Protection	245
Installing Data Protection	246
Digital Asset Control	248
Data Identifiers	248
Data Loss Prevention Templates	251
Data Loss Prevention Policies	252
Data Loss Prevention Logging.....	256
Forensic Folder and DLP Database	256
Device Control	257
USB Exception List	260
Lesson 14: Deploying Policies Through Trend Micro Apex Central	261
Apex Central.....	261
Apex Central Services.....	262
Apex Central Management Modes.....	263
On-premises Management Mode	263
Cloud Management Mode	263
Hybrid Mode	264
Managing Apex One Policies in Apex Central	265
Connecting Apex One and Apex Central	265
Creating an Apex Central User Account	267
Adding Apex One to the Apex Central Product Directory	269
Selecting the Destination Product	271
Identifying Policy Targets	272
Defining Policy Settings	274
Deploying the Policy	275
Policy Inheritance	276
Inherit From Parent	276
Are Customizable	277
Extend from parent	277
Data Discovery Policies	277
Data Discovery	277
Data Discovery Policy Management	277
Incident Investigation	281

Lesson 15: Detecting Emerging Malware Through Connected Threat Defense ...283

Detect	284
Respond	284
Protect	284
Visibility and control	284
Connected Threat Defense Requirements	284
How Connected Threat Defense Works.....	285
Suspicious Activities	286
Deep Discovery Analyzer	286
Connecting Deep Discovery Analyzer to Apex Central	287
Adding Deep Discover Analyzer to the Apex Central Product Directory	288
Suspicious Objects.....	290
Submitting Samples	290
Analyzing Samples	290
Distributing Suspicious Object Details	291
Mitigating Threats	291
Subscribing Apex One to the Suspicious Objects List	291
Tracking Suspicious Objects	293

Lesson 16: Blocking Unapproved Applications on Endpoint Computers297

Integrated Application Control	297
Application Control Blocking Methods.....	298
Lockdown Mode With Allow Criteria	298
Block Criteria	298
Lockdown Mode.....	298
Application Control Criteria	299
File Hash	300
File Paths	302
Digital Certificates	303
User-defined Rules	305
Best Practices for Enabling Application Control.....	306
Use Learn → Monitor → Refine	306
Use Lockdown	307
In-house Applications	307
Top Blocked Applications Widget	307
Trust Permissions	307
Application Control Criteria Pros and Cons	308

Lesson 17: Protecting Endpoint Computers From Vulnerabilities ..309

Integrated Vulnerability Protection	309
Vulnerability Protection Pattern.....	310
Vulnerability Protection Rules	311
Network Engine Settings.....	313

Lesson 18: Detecting and Investigating Security Incidents on Endpoint Computers..317

Integrated Endpoint Sensor	317
Enabling Endpoint Sensor	319
Endpoint Detection and Response.....	320
Apex One Incident Response Model.....	321
Preliminary Assessment.....	321
Preliminary Investigation	322
Custom Intelligence	324
Virtual Analyzer Suspicious Object	329

Root Cause Analysis.....	330
Incident Response.....	334
Terminating Suspicious Processes	334
Adding Processes to the Suspicious Objects List	335
Isolating Endpoints	335
Detailed Investigation	336
Attack Discovery.....	344
Viewing the Attack Discovery Engine Log	344
Managed Detection and Response Service	345
Trend Micro Managed XDR for Users	345
Service Components	347
Managed Service Flow	347
Configuring Apex Central for Managed XDR for Users	348
Lesson 19: Migrating to Apex One as a Service	351
Benefits of Apex One as a Service.....	351
Ease of Deployment	351
Reduced Costs	351
Up-to-date Features	352
Simplified Maintenance	352
Enhanced Security	352
Apex One as a Service Servers.....	352
Apex Central Server	352
Apex One Server	353
Logging into the Apex One as a Service	354
Migrating to Apex One as a Service	357
Integrating Apex Central with a Microsoft Active Directory	357
Migrating Apex One Global and Domain Settings	360
Migrating Apex Central Policies	363
Moving Agents Registered to the On-premises Apex One Server to Apex One as a Service	364
Creating Administrative Users in Apex Central as a Service	366
Create a New Administrative User Account	368
Appendix A: Troubleshooting Trend Micro Apex One	373
Debugging Security Agents.....	373
Debugging the Apex One Server.....	373
Changing the Security Agent Communication Port	374
On the Security Agent	374
Troubleshooting Agent/Server Communication Issues	375
Verify the Connection Status Manually	375
Verify the Connection Status Automatically	375
Verify the Results of the Connection Status	376
Troubleshooting Communication Issues Between Security Agent and Server	376
Verify Security Agent Registry settings	376
Confirm Correct Product Licensing	377
Verify Agent Privileges to Communicate With the Server	378
Verify Internet Information Services	378
Re-establish Communication Using autopcc.exe	379
Re-establish Communication Using IpXfer.exe	379
Verify Windows Firewall Blocking	380
Change the Agent Domain	380
Verify Server Hostname Resolution	380

Troubleshooting Virus Infection.....	381
Determining the Virus Infection Channel on the Server	381
Determining the Virus Infection Channel on the Agent	381
Determining Spyware/Grayware Infection Channel on the Server	382
Determining Spyware/Grayware Infection Channel on the Agent	382
Troubleshooting the Firewall Service	383
Troubleshooting the Unauthorized Change Prevention Service	383
Troubleshooting Edge Relay Server Certificates.....	384
Troubleshooting Sample Submission.....	384
Appendix B: What's New in Trend Micro Apex One	387
All-in-one Security Agent.....	387
Offline Predictive Machine Learning.....	387
Fileless Threat Detection Enhancements	387
Integrated Vulnerability Protection	387
Integrated Application Control	387
Investigative Capabilities	387
Mac Protection Features.....	388
Managed Detection and Response Service Support for SaaS	388
Indicator of Attack Behavioral Analysis Enhancements	388
Application Programming Interface Enhancements	388
Cloud Sandbox	388
Apex Central.....	388
Kernel Mode Termination Protection.....	388
Location Awareness Enhancement	389

Lesson 1: Trend Micro Apex One Overview

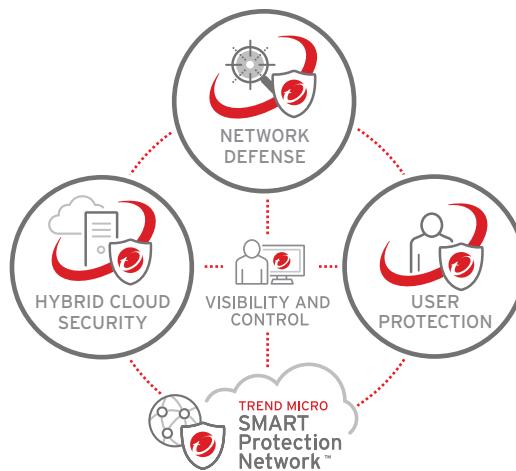
Lesson Objectives:

After completing this lesson, participants will be able to:

- Describe the key features of Apex One
- Identify the components in an on-premises Apex One installation and describe their purpose

Trend Micro Solutions

Trend Micro provides layered content security with interconnected solutions that share data so you can protect your users, network, data center, and cloud resources from data breaches and targeted attacks.



Network Defense

The enterprise is at the cross-hairs of an increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep the organization ahead of purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property. **Trend Micro Network Defense** detects and prevents breaches anywhere on the network to protect critical data and reputation. Rapidly detect, analyze, and respond to targeted attacks on your network. Stop targeted email attacks, and detect advanced malware and ransomware with custom sandbox analysis, before damage is done.

The Trend Micro Network Defense solution preserves the integrity of the network while ensuring that data, communications, intellectual property, and other intangible assets are not monetized by unwanted third parties. A combination of next-generation intrusion prevention and proven breach detection enables the enterprise to prevent targeted attacks, advanced threats, and ransomware from embedding or spreading within their network.

Hybrid Cloud Security

The Trend Micro Hybrid Cloud Security solution protects enterprise workloads in the data center and the cloud from critical new threats, like ransomware, that can cause significant business disruptions, while helping to accelerate regulatory compliance.

Hybrid Cloud Security delivers **comprehensive, automated security for physical, virtual and cloud servers**. The organization can secure critical data and applications across their cloud and virtualized environments with effective server protection that maximizes their operational and economic benefits.

Whether you are focused on securing physical, virtual, cloud, or hybrid environments, Trend Micro provides the advanced server security you need with the Trend Micro Deep Security platform. Available as software, in the Amazon Web Services and Azure marketplace, or as a service, Deep Security provides you with security optimized for VMware, Amazon Web Services, and Microsoft Azure.

User Protection

The threat landscape is constantly changing, and traditional security solutions on endpoint computers can't keep up. Turning to multiple point products on a single endpoint results in too many products that don't work together, increasing complexity, slowing users, and leaving gaps in an organization's security.

To further complicate matters, organizations are moving to the cloud and need flexible security deployment options that will adapt as their needs change.

Trend Micro User Protection is **an interconnected suite of security products and advanced threat defense techniques that protect users from ransomware and other threats, across endpoints, gateways and applications**, allowing the organization to secure all user activity on any application, any device, anywhere.

Trend Micro Smart Protection Network

The Trend Micro Smart Protection Network mines data around the clock and across the globe to ensure **up-to-the-second threat intelligence to immediately stamp out attacks** before they can harm valuable enterprise data assets.

Trend Micro rapidly and accurately collates this wealth of global threat intelligence to customize protection to the specific needs of your home or business and uses predictive analytics to protect against the threats that are most likely to impact you.

To maintain this immense scale of threat protection, Trend Micro has created one of the world's most extensive cloud-based protection infrastructures that collects more threat data from a broader, more robust global sensor network to ensure customers are protected from the volume and variety of threats today, including mobile and targeted attacks. New threats are identified quickly using finely tuned automated custom data mining tools and human intelligence to root out new threats within very large data streams.

Visibility and Control

Whether your endpoints are internal or external, you can manage a **comprehensive set of security capabilities from one single management console** providing a strong level of visibility and control. In addition, suspicious objects discovered by different applications can be consolidated into a single list and distributed within the entire environment.

Trend Micro XGen™ Security

Trend Micro's endpoint protection solution, powered by XGen, delivers a **blend of cross-generational threat defense techniques that are smart, optimized, and connected** to protect endpoint computers across the enterprise - all while preventing business disruptions and helping with regulatory compliance.



Smart

Protects against the full range of known and unknown threats using a cross-generational blend of threat defense techniques that applies the right technique at the right time, and is powered by global threat intelligence.

Optimized

Minimizes IT impact with solutions that are specifically designed for and integrated with leading customer platforms and applications on endpoints computers. The footprint on the client applications is minimized to ensure a more efficient use of resources.

Connected

Speeds time to response with automatic sharing of threat intelligence across security layers and centralized visibility and control XGen™ security uses proven techniques to quickly identify known good or bad data, freeing advanced techniques to more quickly and accurately identify unknown threats. This identification in rapid succession with right-time technology regardless of location and device across a connected system, maximizes both visibility and performance. This core set of techniques powers each of the Trend Micro solutions, in a way that is optimized for each layer of security: hybrid clouds, networks, and user environments.

Trend Micro Apex One

Apex One is the next evolution of the Trend Micro enterprise endpoint security solution and replaces OfficeScan as Trend Micro's flagship endpoint security product. Apex One can be installed as a new product in the enterprise or upgrade OfficeScan XG to Apex One.

Apex One protects endpoint computers from malware, network viruses, Web-based threats, spyware, and mixed threat attacks (both known and unknown). It uses a client/server architecture that consists of a Security Agent program that resides on the endpoint and a Server program that manages all Agents. The Agent guards the endpoint and reports on its security status to the Server. Apex One offers threat detection, response, and investigation within a single agent on both Windows and Mac computers.

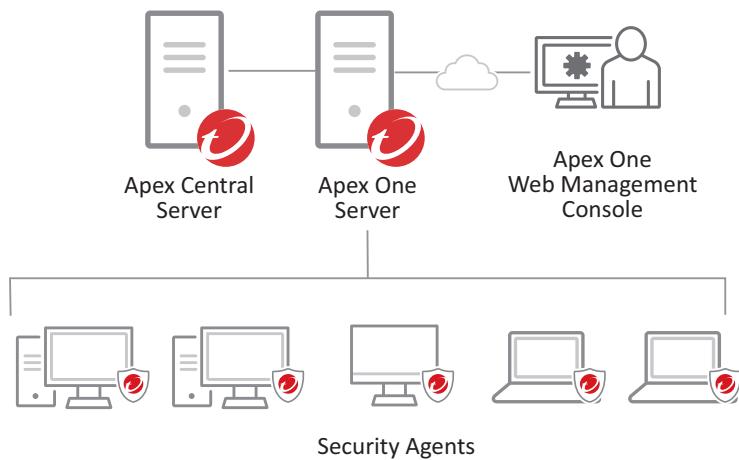
The Apex One Server provides real-time, bidirectional communication between the Server and Security Agents using Hypertext Transfer Protocol (HTTPS). The Apex One Web Management console makes it easy for administrators to set coordinated security policies and deploy updates to every endpoint Agent. In addition, different users access roles can be set up for specific administrative tasks such as policy configuration, log query, and report generation.

Trend Micro Apex One Deployment Methods

Apex One can be deployed in one of two models, depending on how the organization would like to manage the system.

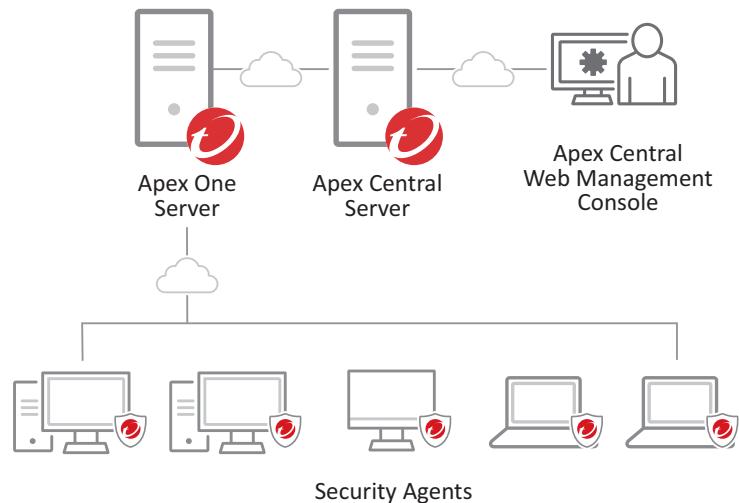
On-premises Deployment

In an on-premises deployment, the Apex One Server is installed as a standalone server within your environment. The database and other components also reside within your network. Apex Central can be installed as an optional component to simplify policy distribution and provide additional security capabilities. The Apex One Web Management Console is the main management interface into the system. Any software updates to the servers in an on-premises deployment must be manually applied by administrators.



Software as a Service Deployment

Apex One as a Service is a subscription-based cloud implementation of Apex One. Trend Micro hosts the database, Apex One Server and Apex Central Server components on Microsoft Azure virtual machines. The Apex Central Web Management console is the main management interface for the service offering. Any software updates to the servers are applied automatically by Trend Micro.



An on-premises deployment of Apex One can be migrated to Apex One as a Service.

Key Features of Trend Micro Apex One

Apex One provides a wide range of endpoint computer protection features. Some of these key features include the following:

Note: Some of these features may require additional licensing.

Malware Protection

Endpoint protection is the primary focus of Apex One. Apex One protects endpoint computers from security risks by scanning files for malware and then performing a specific action for each security risk detected. To easily monitor, investigate and back-up infected files, Security Agents can automatically forward infected or suspicious files to a quarantine folder.

Damage Cleanup Services clean computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process. Damage Cleanup Services runs automatically in the background without having to configure it. Users are not even aware when it runs unless Apex One needs to notify the user to restart their endpoint to complete the process of removing a Trojan.

Ransomware Protection

Enhanced scan features can identify and block ransomware programs that target documents on endpoint computers by identifying common behaviors and blocking processes commonly associated with ransomware programs.

Predictive Machine Learning

Predictive Machine Learning can protect your network from new, previously unidentified, or unknown threats through advanced file feature analysis and heuristic process monitoring. Apex One delivers this functionality through a cloud-based machine learning model and introduces a local model for computers without a network connection.

Behavior Monitoring

Behavior Monitoring constantly monitors and protects Agents from unusual and unauthorized modifications to the operating system or installed software.

Sandbox Analysis

Security Agents can submit suspicious file to Deep Discovery Analyzer, where the file is executed in a sandbox environment. Files determined to be dangerous are submitted to Apex Central for addition to the Suspicious Objects List. You can configure Apex One to subscribe to the Suspicious Object List and customized actions can be created for these objects. This provides custom defense against threats identified by endpoints protected by Trend Micro products in your environment.

Web Threat Protection

Web Reputation technology protects Agent computers within or outside the corporate network from malicious and potentially dangerous Web sites. This service breaks the infection chain and prevents downloading of malicious code. The credibility of Web sites and pages can be verified by integrating Apex One with the Smart Protection Server or the Trend Micro Smart Protection Network.

The Apex One Suspicious Connection Service monitors the behavior of connections that endpoint make to potential Command & Control servers and the Browser Exploit Protection blocks Web pages containing malicious scripts.

Firewall Protection

The Apex One firewall protects endpoint computers on the network using stateful inspection. Rules can be created to filter connections by application, IP address, port number and protocol, and then applied to different groups of users.

Data Loss Prevention

Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage.

Device Control

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

Outbreak Control

Apex One Outbreak Prevention Services shut down infection vectors and rapidly deploys attack specific security policies to prevent or contain outbreaks before pattern files are available.

Application Control

Application Control enhances defense against malware or targeted attacks by preventing unwanted and unknown application from executing on endpoints. Application Control is currently only supported on Windows endpoint computers.

Virtual Patching

Vulnerability Protection protects endpoints from being exploited by operating system vulnerability attacks. It automates the application of virtual patches to endpoint computer before official patches from the vendor become available.

Endpoint Detection and Response

Apex One provides actionable insights, expanded investigative capabilities, and centralized visibility across the network through an advanced Endpoint Detection and Response (EDR) toolset. Perform threat investigation through integrated EDR or by boosting your security teams with the Managed Detection and Response (MDR) service option. Endpoint Detection and Response capabilities are included in Apex One and Apex Central but are licensed separately.

Endpoint Encryption

Endpoint Encryption encrypts data on a wide range of devices including laptops and desktops, USB drives, and other removable media, providing full disk, file/folder, and removable media encryption to prevent unauthorized access and use of private information. Endpoint Encryption is a **standalone product that is licensed and installed separately from Apex One**, but its capabilities can be integrated into Apex One Security Agents through Apex Central policies.

Cloud-based Intelligence

Apex One benefits from a global cloud-based repository of threat data through the Trend Micro Smart Protection Network. Services, such as ActiveUpdate, File Reputation, Web Reputation, Predictive Machine Learning and more are delivered to Trend Micro products through the cloud-based Smart Protection Network.

Automated Updates

Apex One Agents benefit regular, automated updates to malware signatures and patterns.

Multi-Platform Support

Apex One provides endpoint protection features for both Windows and Mac operating systems. Support for Mac endpoints is enabled through a plug-in in Apex One. Not all Apex One functionality is currently available on Mac endpoint computers.

Simplified Administration

The Apex One Web Management console gives administrators access to all Agents and Servers on the network. From the Web Management console, administrators can coordinate automatic deployment of security policies, pattern files, and software updates on every Agent and server. Apex One also performs real-time monitoring, provides event notification and delivers comprehensive reporting. Administrators can perform remote administration, remote installation of Agents, set customized policies for individual desktops or groups, and lock Agent security settings.

Off-premises Management

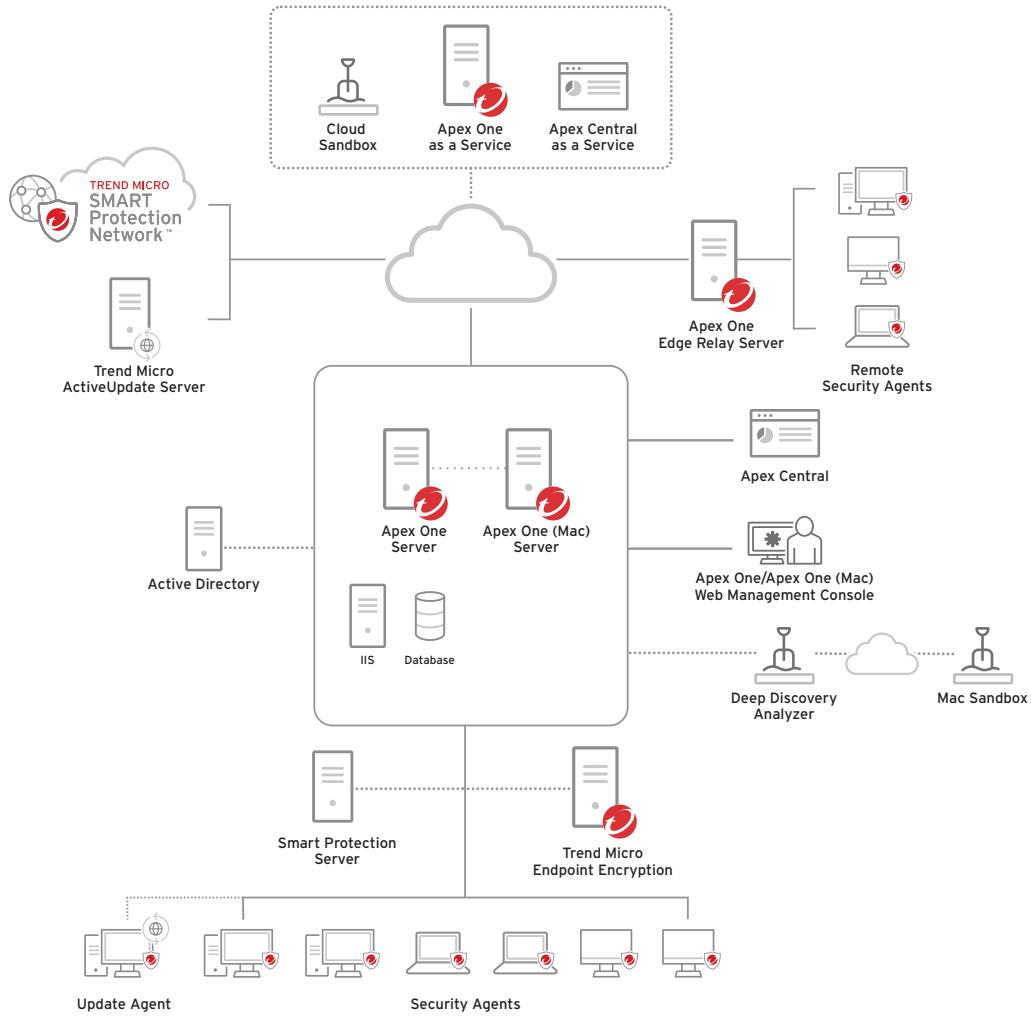
Apex One provides management to external Security Agents through the Edge Relay Server. This device provides log collection, sample submission and suspicious list deployment to Agents outside of the network.

Unified Agent

Apex One provides a wide breadth of capabilities through a single unified agent. This all-in-one lightweight agent provides deployment flexibility through both Software as a Service (SaaS) and on-premises options.

Trend Micro Apex One Components

Apex One consists of multiple components that work together to protect endpoint computers.



Apex One Server

The Apex One Server is the central repository for all Windows Agent configurations, security risk logs, and updates. The server performs two important functions:

- Installs, monitors, and manages Security Agents on Windows endpoints
- Downloads most of the components needed by Agents

Apex One (Mac) Server

The Apex One (Mac) Server is the central repository for all Mac Security Agent configurations, security risk logs, and updates. The server performs two important functions:

- Monitors and manages Security Agents on Mac endpoints
- Downloads components needed by Security Agents

Apex One (Mac) Server is activated through a plug-in within Apex One Server. The Server communicates with the Security Agents through the ActiveMQ protocol.

Database

The database stores all the information Apex One requires to operate. A Microsoft SQL Server database is required to complete the Apex One setup. Alternately, an SQL Server Express database can be installed as part of the setup process. The database can be hosted on the same server as Apex One, or can be hosted on a separate server.

Microsoft Internet Information Server

Microsoft Internet Information Server (IIS) makes it possible to access Apex One components from the Internet, including:

- Apex One Web Management console for management operations
- CGI applications or ISAPI for both Agent and Server functions
- Update components
- Integrated Smart Protection Server

Apex One/Apex One (Mac) Web Management Console

Apex One uses a Web-based administration interface to control policies and endpoint computers. Administrative users authenticate to the Apex One Web Management console using Apex One-created credentials, or credentials stored in Microsoft Active Directory. Separate Web Management consoles are available for Apex One and Apex One (Mac).

Apex Central

Apex Central (previously known as Control Manager) provides a single unified interface to manage, monitor, and report across multiple layers of security and deployment models. Customizable data displays allow administrators to rapidly assess status, identify threats, and respond to incidents. With Apex Central, administrators can manage Apex One, Apex One (Mac), as well as other Trend Micro products, from a single interface.

User-based visibility shows what is happening across all endpoints, enabling administrators to review policy status and make changes across all user devices. In the event of a threat outbreak, administrators have complete visibility of an environment to track how threats have spread.

Direct links to Trend Micro Threat Connect database provides access to actionable threat intelligence, which allows administrators to explore the complex relationships between malware instances, creators, and deployment methods.

Apex Central is responsible for compiling the Suspicious Objects for use in Connected Threat Defense. This list based on information provided by other components in the infrastructure.

Some features in Apex One, including Application Control, Vulnerability Protection and Endpoint Detection and Response require integration with Apex Central.

Security Agents

An Apex One Security Agent on each endpoint protects Windows and Mac computers from security risks. The Apex One Agent reports to the parent Apex One Server from which it was installed and sends security events and status information to the Server in real time. Security Agents can be installed on endpoints computer within and outside the corporate network.

Apex One Edge Relay Server

The Apex One Edge Relay Server provides off-premises protection for remote computing and traveling users. It provides visibility and protection for endpoints that leave the local intranet, without requiring a VPN to connect back to the Apex One Server.

Trend Micro Smart Protection Network

The Trend Micro Smart Protection Network is a cloud-client infrastructure that delivers protection from emerging threats by continuously evaluating and correlating threat and reputation intelligence for Websites, email sources, and files.

Smart Protection Server

The Smart Protection Server provides an internal, standalone version of the Smart Protection Servers for File and Web Reputation services. The Smart Protection Server can also be used to proxy service requests for Predictive Machine Learning scanning in air-gapped environments.

Trend Micro ActiveUpdate Server

Trend Micro ActiveUpdate Server serves as the default download source for pattern file and program updates. Other sources, including Apex Central or Update Agents can be used as the download location instead of the ActiveUpdate Server.

Update Agents

Update Agents are Security Agents that function as alternative update sites for other Agents within an Apex One network. Update Agents serve as local ActiveUpdate sites.

Trend Micro Endpoint Encryption

Trend Micro Endpoint Encryption encrypts data on a wide range of devices – both PCs and Macs, laptops and desktops, USB drives, and other removable media. This solution combines enterprise-wide full disk, file/folder, and removable media encryption to prevent unauthorized access and use of private information. Endpoint Encryption is an optional, standalone product, but can be incorporated into policies distributed through Apex Central.

Deep Discovery Analyzer

Deep Discovery Analyzer is a hardware device hosting multiple secure sandbox environments in which samples submitted by Trend Micro products are analyzed. Sandbox images allow for the observation of file and network behavior in a natural setting without any risk of compromising the network.

Deep Discovery Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Deep Discovery Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings which is then forwarded to Apex Central to build the Suspicious Objects List.

Mac Sandbox

Mac Sandbox is hosted service that analyzes possible threats for macOS.

Software as a Service Components

Apex One is available as a Software as a Service offering. Components available as a service are accessed from cloud servers hosted by Trend Micro.

Apex One as a Service

Apex One as a Service allows an organization to deploy and manage Apex One as cloud-based service and offers full feature parity with the on-premises option.

Apex Central as a Service

Apex Central as a Service provides Apex Central capabilities as a cloud-based service.

Cloud Sandbox

This cloud-based Virtual Analyzer allows you to perform sample submission, synchronize suspicious object lists, and take action on user-defined suspicious objects.

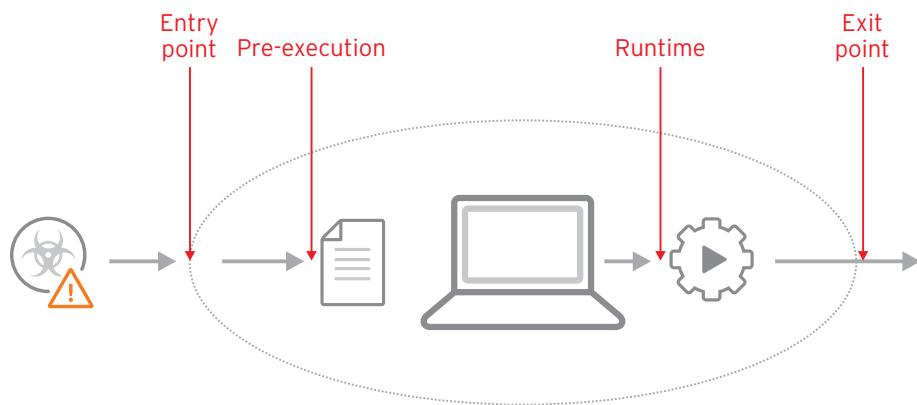
Optional Third-Party Components

Microsoft Active Directory

Apex One integrates with Microsoft™ Active Directory™ to manage Security Agents more efficiently. Web Management console permissions can be assigned using Active Directory accounts, endpoint computers without security Agents can be located and automated grouping of agents based on Active Directory domain can be performed. User-based application control rules can be created based on Active Directory groups.

Threat Detection

There are several points at which threats could enter the system through the endpoint computer. A variety of automated threat detection techniques can be enabled in Apex One to monitor for threats on the endpoint.



Detecting Threats at the Entry Point

Entry point detection uses methods to capture threats as they enter the endpoint. These methods include:

- **Web Reputation:** Web reputation blocks connections to malicious Web sites. This is done at the kernel level, allowing Apex One to not only block users from accessing a malicious site, but also blocking programs on the endpoint from accessing the site.
- **Operating System Vulnerability Protection:** Apex One blocks exploits of operating system vulnerabilities by applying a virtual patch. Trend Micro provides timely protection for operating system vulnerabilities with the industry's most timely vulnerability research.
- **Browser Exploits:** Malicious behavior can also be captured within the Web browser based on script inspection and site behavior.
- **Device Control:** Apex One can block unknown removable media devices, making it less likely for the endpoint to be infected with malware. This protection is now also available for the Mac in Apex One.

Detecting Threats Pre-execution

Detection methods used in the pre-execution phase capture and block threats as they are written to disk or to memory. These methods include:

- **Packer Detection:** Apex One identifies packed malware as it unpacks prior to execution, blocking threats attempting to hide themselves in memory.
- **Predictive Machine Learning:** File-based threats can be evaluated against a cloud-based model before they are run to predict if the file is malicious. Apex One can take advantage of an offline model in cases where the endpoint is not connected to the network. Mac computers can now benefit from this technique as well.
- **Application Control:** Application control prevents unrecognized software from executing.
- **Variant Protection:** Variant protection detects mutations of malicious samples by recognizing known fragments of malware code.
- **File-based Signatures:** The majority of threats still arrive at the endpoint as file-based attacks. File-based signatures provide an effective technique for detecting known malicious items.

Detecting Threats at Runtime

While many threats can be detected as they are written to disk, there are some threats that won't be detected until they execute. Detection methods used in this phase include:

- **Predictive Machine Learning:** Run-time machine learning techniques monitor anything that is executing and evaluates it against a separate run-time machine learning model.
- **Behavior Analysis:** Powerful behavior analysis techniques provide a clear indication if an attack is taking place based on file behavior. This provides an effective mechanism for detecting ransomware and file-less malware. New rules are continually being introduced to detect new suspicious behavior.
- **In-memory Runtime Analysis:** Some malware executes only in memory. In-memory runtime analysis can monitor for malicious script behavior or code injections in memory and stop them once they start running.

Detecting Threats at the Exit Point

Methods in this phase can detect and block attempts to forward data from the endpoint. Detection methods used in this phase include:

- **Web Reputation:** At this phase, Web reputation protection can block connections to malicious Web sites, such as Command & Control sites. Again, this protection is applied at the kernel level blocking connections from the Web browser, or from any other application running on the endpoint.
- **Host Intrusion Prevention:** Host intrusion prevention detects and blocks malware lateral movement behavior.
- **Data Exfiltration Detection:** Data Leak Prevention techniques can detect sensitive data leaving the endpoint and block its movement.
- **Device Control:** Unknown removable media devices can be blocked to prevent data leaving the endpoint

Lesson 2: Trend Micro Apex One Server

Lesson Objectives:

After completing this lesson, participants will be able to:

- Identify the responsibilities of the Apex One Server
- Describe the Apex One Server services and components
- Install the Apex One Server
- Upgrade OfficeScan XG and OfficeScan XG SP1 to Apex One

Apex One Server Tasks

The Apex One Server provides centralized management and control of the Apex One network. The Apex One server component performs the following tasks:

- Distributes protection setting to endpoint computers
- Initializes scanning, cleaning, and other tasks
- Receives action status results
- Maintains a central repository for all Agent configuration settings, virus and firewall logs, Outbreak Prevention Policies, and Agent software and updates
- Installs Security Agents
- Installs components such as the Smart Protection Server, Apex One (Mac) Server and other optional components included in the installation package
- Provides Server Authentication to ensure that all communication to and from the server is secure and trusted
- Collects suspicious file sample and forwards for analysis
- Retrieves Suspicious Objects list from Apex Central and forwards to Agents for logging/blocking purposes
- Stores metadata collected by Endpoint Sensor for Endpoint Detection and Response activities

Apex One Server Services and Components

The following services and components are installed as part of the Apex One Server.

Component	Description
Apex One Master Service (Ofcservice.exe)	<p>This component is the centralized management component of an Apex One network. It accepts and responds to commands and requests from Apex One Security Agents, the Web Management console, and Apex Central.</p> <p>This service will always be running on the Apex One Server and provides the following functionality for its clients:</p> <ul style="list-style-type: none"> • Stores Agent configuration settings • Consolidates Agent logs • Serves as the default source for update components (for example, patterns, engines, etc.) • Provides server authentication details to ensure that all communications that the Apex One Server sends to the Agents are trusted. <p>The Security Agent verifies the appended signature every time it receives a notification from the server. The Agents use a public key to verify that incoming communications are server-initiated and valid. The Agents will only respond if the verification is successful. If the signature verification fails, the Agent disregards the received settings.</p>
Apex One Apex Central Agent Service (OfficeScanCMAgent.exe)	Allows administrators to manage Apex One from the Apex Central console. This facilitates management of multiple Apex One Servers, Apex One (Mac) Servers as well as other Trend Micro products. Apex Central also compiles and enables access to the Suspicious Objects List.
Apex One Active Directory Integration Service (osceintegrationservice.exe)	This component interfaces with Microsoft Active Directory to provide: <ul style="list-style-type: none"> • Role-based administration • Compliance report generation • Identification of unprotected endpoints • Automatic grouping of Security Agents • User-based Application Control rules
Apex One Deep Discovery Service (OfcDdaSvr.exe)	This component handles the internal transmission of Suspicious Object samples and submits samples to Deep Discovery Analyzer.
Apex One Log Receiver Service (ofclogrecvsvc.exe)	This service receives log information from Apex One Servers and Security Agents.
Apex One Plug-in Manager (CNTAoSMgr.exe)	This service installs and manages Apex One plug-in programs.
Trend Micro Endpoint Sensor Service (TrendMicroEndpointSensorService.exe)	Manages communication and provides support for tasks required by Endpoint Sensor. This service is added when Endpoint Sensor policies are enabled.
Trend Micro Application Control Service (TMiACSVc.exe)	Manages the allowed, blocked, and lockdown policies of the Application Control feature. This service is added when Application Control policies are enabled.

Component	Description
Trend Micro Vulnerability Protection Service (iVPServer.exe)	Manages protected endpoints with Intrusion Prevention rules based on network performance and security priorities. This service is added when Vulnerability Protection policies are enabled.
Trend Micro Advanced Threat Assessment Service (AtasAgent.exe)	Identifies potentially compromised endpoints through on-demand assessment and monitoring. By integration with Trend Micro Threat Investigation Center, Advanced Threat Assessment Service allows administrators and information security experts to perform forensic tasks on endpoints for remote incident response.
Trend Micro Local Web Classification Server (LWCSService.exe)	Provides the local web classification scan function to Apex One Security Agents.
Trend Micro Smart Protection Server (iCRCService.exe)	Provides the Smart Scan functionality to Apex One Security Agents. <ul style="list-style-type: none"> • File Reputation: Provides Agents with a source for malware confirmation and removal information. Agents obtain this information by way of HTTP/HTTPS queries. • Integrated Web Reputation Service: Provides Agents with a source of information regarding known malicious websites.
Trend Micro Smart Protection Query Handler (SRService.exe)	Provides the smart relay function to Apex One Security Agents.
Trend Micro Cloud Endpoint Telemetry Service (CETASvc.exe)	Collects and send telemetry data about Trend Micro cloud endpoints.
Trend Micro Endpoint Basecamp (endpointbasecamp.exe)	Endpoint Basecamp provides the following features for Trend Micro endpoint security products such as the Apex One Security Agent: <ul style="list-style-type: none"> • Trend Micro endpoint security product deployment. • Pre-assessing the endpoint and listing the required actions for Trend Micro endpoint security product deployment. • Collecting endpoint basic information (without PII) for the security optimization and recommendation. • Enhanced support service and troubleshooting from Trend Micro backend.

SaaS: Access to the services and components is not available in the service implementation of Apex One.

Web Server

The Internet Information Server (IIS) Web Server makes it possible to access the following Apex One components from the Internet:

- Web Management console
- CGI applications or ISAPI for both Agent and Server functions
- Update components
- Integrated Smart Protection Server

Apex One (Mac) Plug-in

Apex One integrates support for Mac endpoints through the Apex One (Mac) Plug-in. A separate Web Management console is used to manage the Mac endpoints, or they can be managed through Apex Central.

Type	Detections	Affected Endpoints
Security Risks	0	0
Web Threats	0	0

Components	Current Version	Updated	Outdated	Update Rate

Data Loss Prevention Plug-in

Apex One provides data loss protection through a plug-in designed to minimize the risk of information loss and improve visibility of data usage patterns and risky business processes allowing private information to remain secure.

Configuration Repositories

Apex One Server configuration settings are stored in a variety of locations, including:

- Apex One Database:** The database tables used by Apex One are stored in a Microsoft SQL or SQL Express database.
- ous.ini:** Contains information about alternative update sources that an Apex One Server can use.
- ofcscan.ini:** This global Agent setting file contains settings that are common to all Security Agents that are registered with a specific Apex One Server. Agent-specific local settings however supersede the settings in this file.
- ofcserver.ini:** Contains the global Server setting information, including enabled services, license details, Web Management console configuration, and others.
- sscfg.ini:** Contains information about Smart Protection Servers.
- TrendAuthDef.xml:** Contains all users and log-in information. This file is located in:
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Private\AuthorStore
- TrendAuth.xml:** Contains role information for administrative access. Determines who can access the administrative console and what access they have. This file is located in:
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Private\AuthorStore

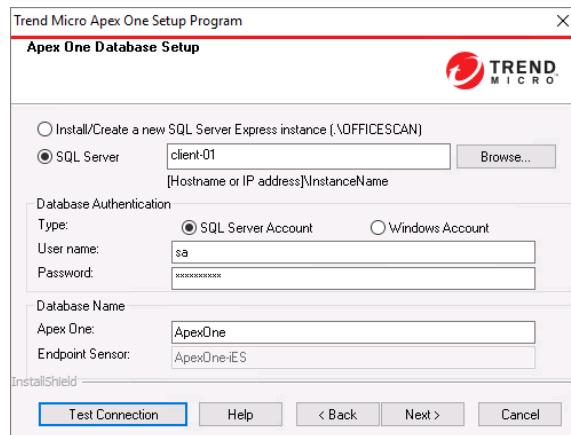
- Certificate backup zip files: Contains backed up certificates issued by the current Apex One Server. Backing up the Apex One Server certificates allows you to use these certificates if you need to reinstall the Apex One server. Run the `CertificateManager.exe` utility to backup the certificates and indicate the password and path for the backup file.

SaaS: Access to the configuration repositories is not available in the service implementation of Apex One.

Apex One Database

Apex One requires a Microsoft SQL Server database. A database instance must be created in SQL Server with a username and password assigned. These details must be provided during the setup of the Apex One Server. An additional database instance can be created to store Endpoint Sensor-related data, but only when using the full version of SQL Server 2016 with the **Full-Text and Semantic Extractions for Search** feature enabled.

If SQL Server is not available in the organization, SQL Server 2016 Express can be installed as part of the setup.



SaaS: Administrator access to the database is not available in the service implementation of Apex One.

Installing the Apex One Server

For a successful installation, review the system requirements for Apex One Server before proceeding with the steps in the installation.

SaaS: In the service implementation of Apex One, installation of the Apex One Server is the responsibility of Trend Micro.

The Apex One Server can be installed on computers running different versions of Microsoft Windows Server. Supported operating systems are listed in the following table:

Platform	OfficeScan XG	OfficeScan XG SP1	Apex One
Windows Server 2008	✓	x	x
Windows Server 2008 R2	✓	✓	x
Windows Server 2012	✓	✓	✓
Windows Server 2012 R2	✓	✓	✓
Windows Server 2016	✓	✓	✓
Windows Server 2019	x	x	✓

Hardware Requirements

- **Processor:** 1.4 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent, AMD 64 processor or Intel 64 processor
- **Memory:** 2GB minimum

Apex One Server Pre-Installation Checklist

Prior to installing Apex One, you should review the following conditions to ensure that all necessary permissions, ports and other settings are in place.

- Verify that the Windows Server that will be hosting the Apex One Server is running a supported version.
- An SQL Server database instance is available along with a corresponding administrator username and password. Alternately, SQL Server 2016 Express can be installed as part of the setup.
- You will require an Activation Code for the Apex One Server. In addition, some optional components, such as Endpoint Sensor, require separate licensing. Contact Trend Micro to get the appropriate codes for your installation.
- If a proxy is needed for Internet access in your environment, you will need to supply your proxy server address, port and log in credentials as part of the Apex One setup process.
- The Smart Protection Source should be considered as the option to install an integrated Smart Protection Server will be offered as part of the setup process.
- If the new installation of Apex One will be sharing digital certificates with an existing installation, the details of the certificates must be provided.

Downloading Apex One Server for Windows

You can download the latest version of the Apex One installation package from the **Trend Micro Download Center** at:

<http://downloadcenter.trendmicro.com/>

In the **Desktop** category, click **Trend Micro Apex One** to view the related downloads available.

On the **Product Download** tab, locate the installation package and download to the target computer.

The screenshot shows the Trend Micro Software Download Center interface. On the left, there's a sidebar with links like 'Download for Business', 'Scan Engines', 'All Pattern Files', and 'Consumer Downloads'. The main area is titled 'Apex One' with a sub-section 'Complementary access to Trend Micro™ Vision One'. Below this, there are two download options for 'Operating System: Windows':

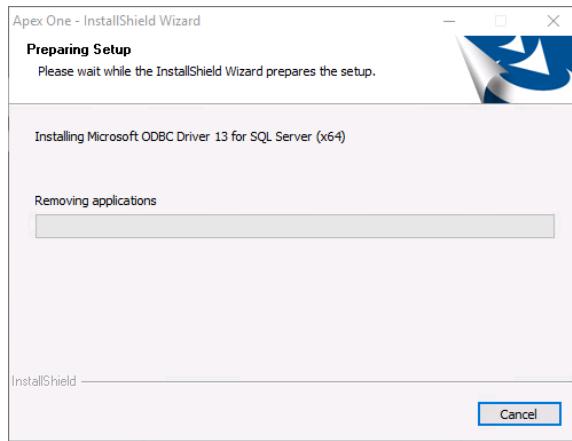
- Full Installation Package English (Release Date: 2019-09-05, File Name: apexone-2019-win-en-all-in-one-b2012.exe, Size: 2710 MB). The 'Download Package' button is circled in red.
- Full Installation Package English (Release Date: 2019-04-03, File Name: apexone-2019-win-en-gm-b1071.exe, Size: 2598 MB). The 'Download Package' button is also circled in red.

At the bottom of the page, there's a copyright notice: 'Copyright (c) 2021 Trend Micro Incorporated. All rights reserved.' followed by links to 'Careers', 'Privacy Policy', 'Legal Policies', and 'Sitemap'.

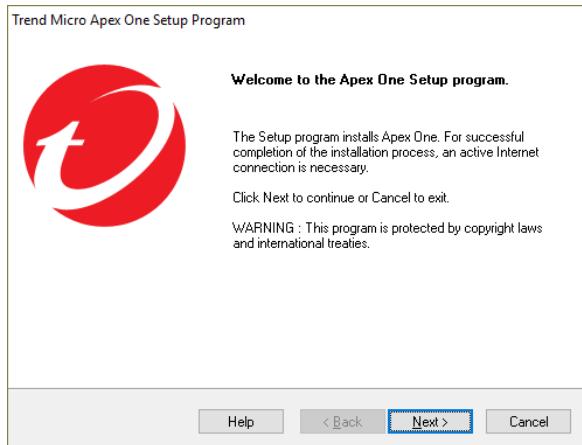
Running the Setup

Run the setup application by double-clicking the downloaded setup application and step through the **Setup Wizard** by clicking **Next** on each page after providing the required information.

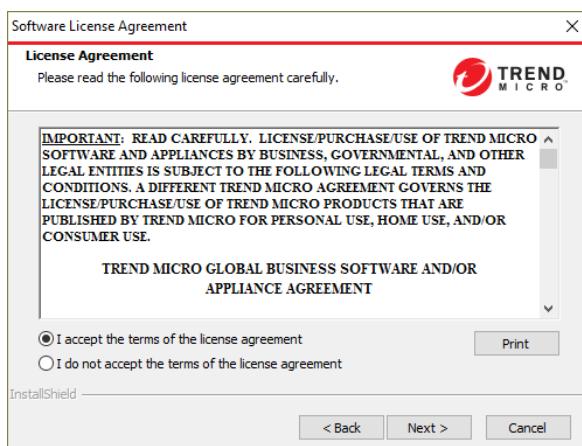
- 1 Before beginning the setup, the installer prepares and installs any missing Windows components.



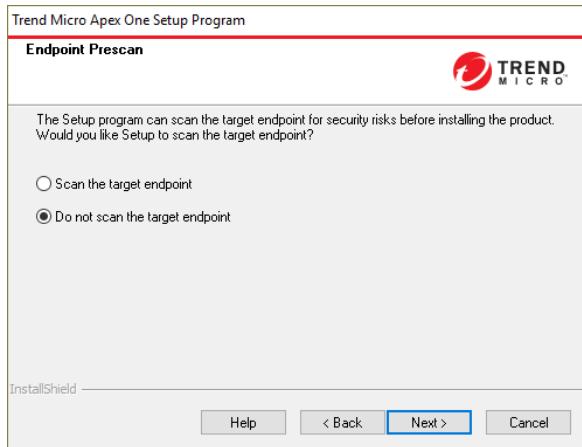
- 2 Click **Next** to acknowledge the **Welcome** window.



- 3 Click **I accept the terms of the license agreement** to proceed with the setup.

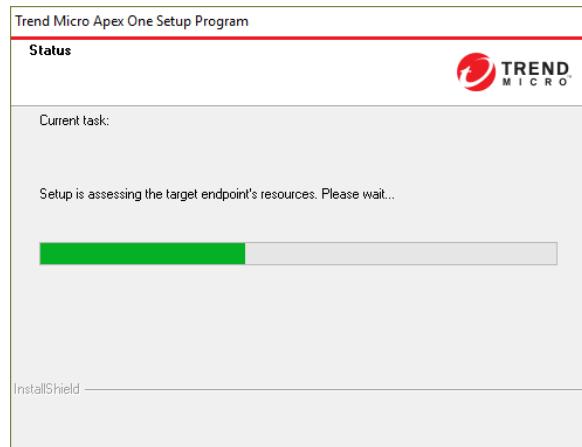


- 4 Select whether to scan the host computer before installing the Apex One Server. This option will scan selected folders on the host computer for security risks before beginning the setup. It may take a few minutes to complete the scan.

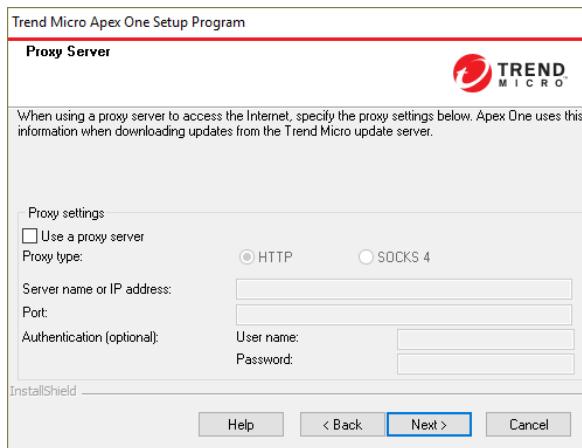


Note: An Endpoint Prescan only scans selected folders, it is not a thorough system scan. The \My Documents folder, for example, will not be scanned. This scan looks for files with specific file extensions, including .SYS, .COM, .EXE, .DOC, .DOT, .XLS, .VBS, .PIF, and .SCR. If the setup application detects a virus, you will be prompted for an action such as Clean, Rename, Delete and Pass. **The patterns used by this scan are those that existed when the setup package was created and could potentially be several months old.**

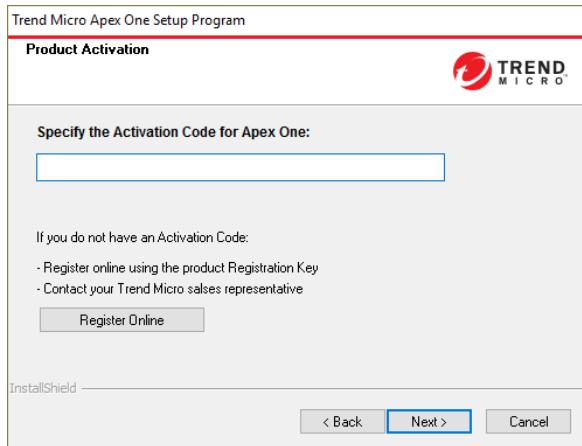
- 5 The Setup application will assess the resources on the Server to ensure it supports Apex One.



6 Identify the details of any proxy servers being used.

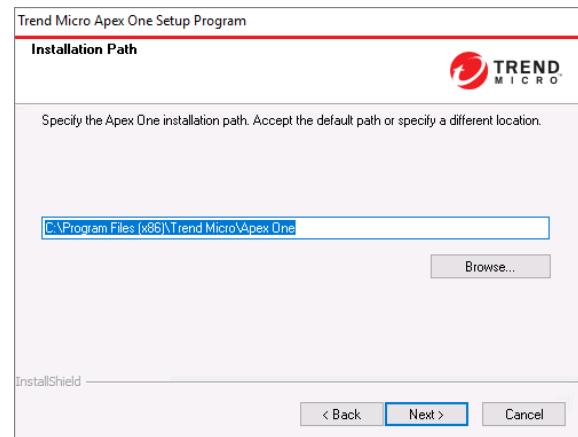


7 Enter the Activation Codes for Apex One.

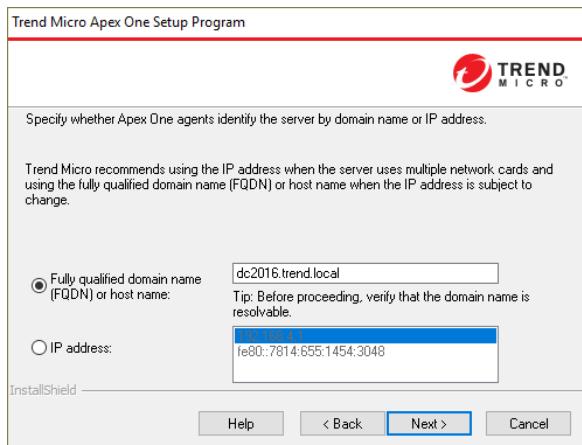


Note: Some services in Apex One may require additional licensing.

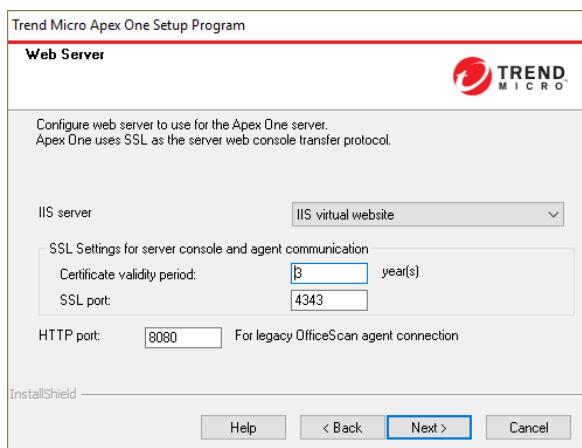
8 Select the installation path for the program files.



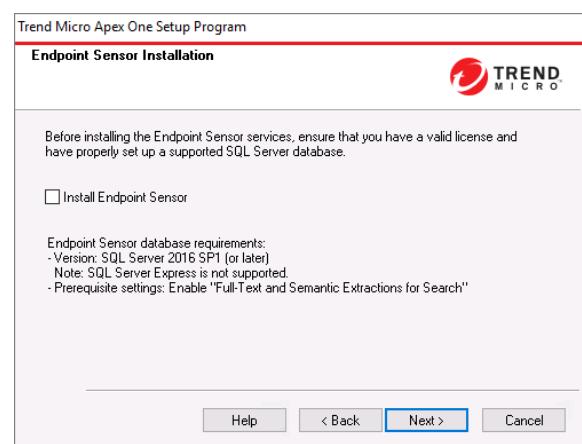
9 Confirm the fully qualified domain name or IP address details for the Apex One Server.



10 Identify the details of the IIS website to used.



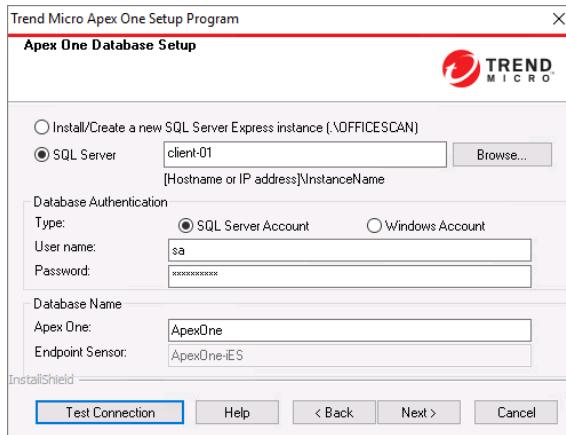
11 Click to enable Endpoint Sensor support on the Apex One Server, if required.



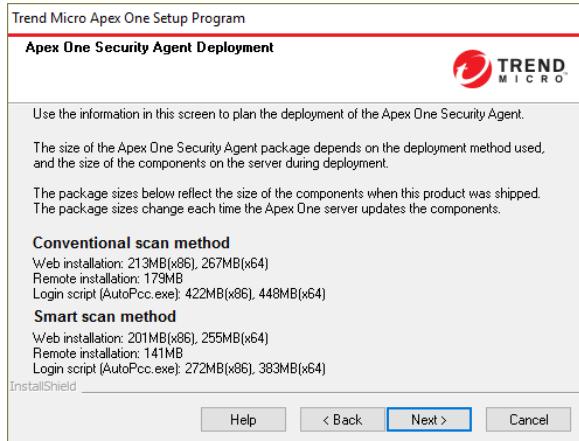
Lesson 2: Trend Micro Apex One Server

Note: The full version of Microsoft SQL Server 2016 or later must be used as the database if choosing to enable Endpoint Sensor support. SQL Server Express is not supported if Endpoint Sensor is to be enabled.

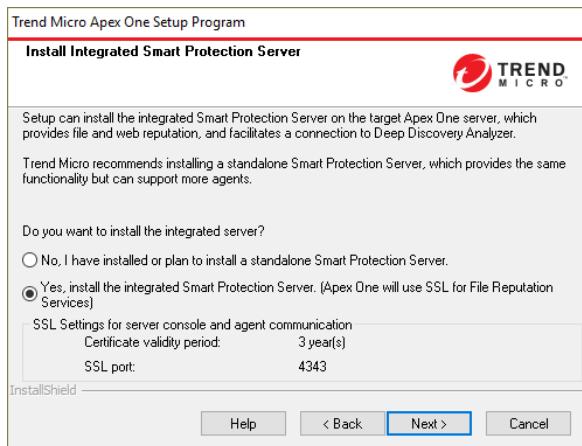
- 12 Identify the details of the SQL Server database, or select the option to install SQL Server Express 2016.



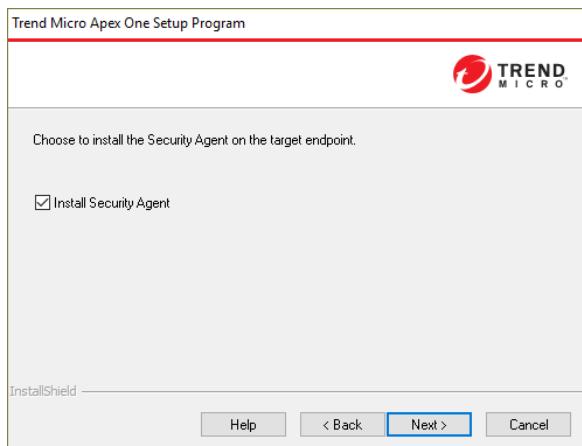
- 13 Informational details regarding Security Agent deployment is displayed.



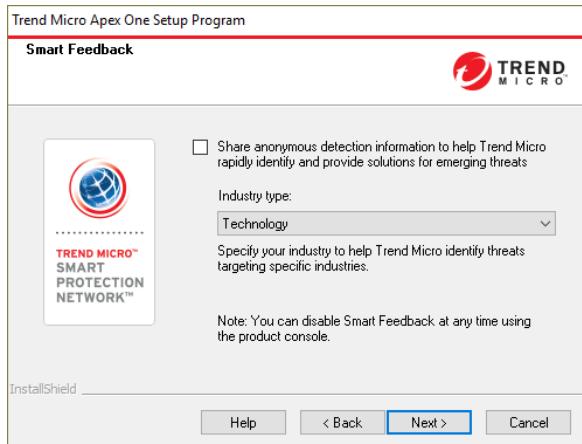
- 14 Click to install an integrated Smart Protection Server, if required.



- 15 Click to enable the installation of an Security Agent on the server, if required.



- 16 Select whether you want to enable **Trend Micro Smart Feedback**. When enabled, your installation contributes to the Trend Micro Smart Protection Network to improve analysis, identification, and prevention of new threats. You can enable or configure Smart Feedback later in the Apex One Web Management console. Optionally, enter the industry your organization belongs to by selecting it from the drop-down list.



Note: Trend Micro Smart Feedback provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. Each new threat identified through a single customer's routine reputation check automatically updates all of Trend Micro's threat databases, blocking any subsequent customer encounters of a given threat. For example, routine reputation checks are sent to the Smart Protection Network. By continuously processing the threat intelligence gathered through this global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides *better together* security. The privacy of a customer's personal or business information is always protected.

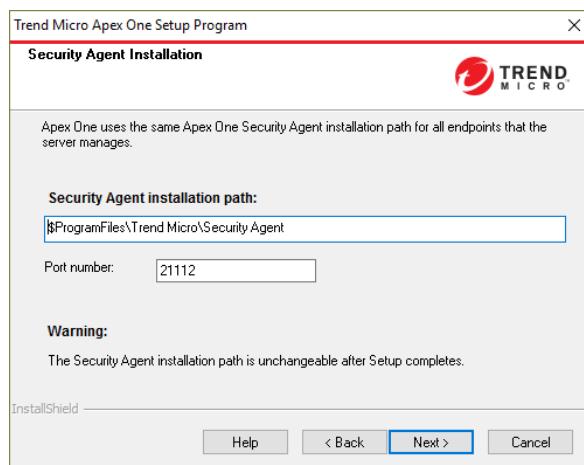
Trend Micro Smart Feedback is designed to collect and transfer relevant data from Trend Micro products to the Smart Protection Network so that further analysis can be conducted, and consequently, advanced solutions can evolve and be deployed to protect clients.

Samples of information sent to Trend Micro:

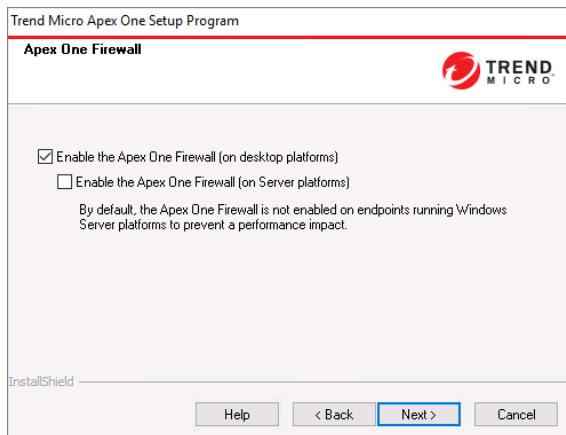
- File checksums
- Websites accessed
- File information, including sizes and paths
- Names of executable files

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

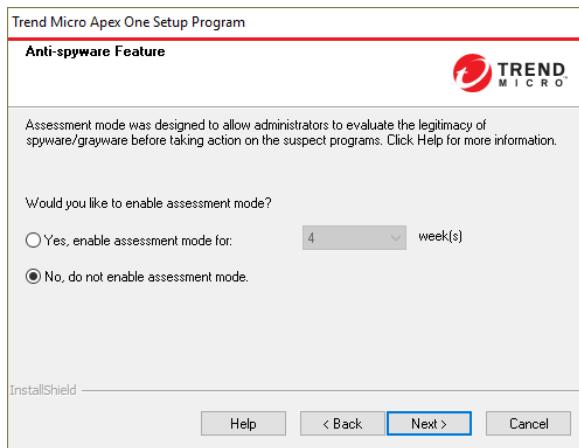
- 17 Identify the Agent installation path. The default port of 21112 is assigned for communication between the Apex One Server and the Agent. The port can be modified if required.



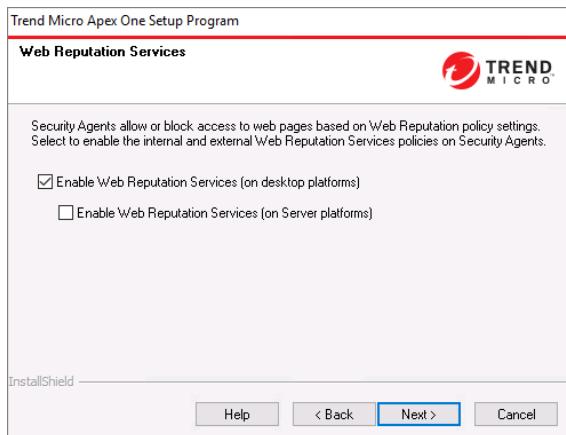
- 18 Click to enable the Apex One Firewall features on this server, if required.



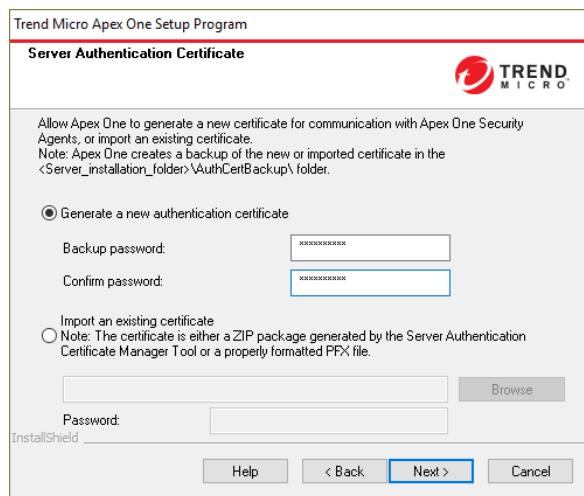
- 19 Click to enable assessment mode on this server, if required. When in assessment mode, all Agents managed by the server will log spyware/grayware detected during Manual Scan, Scheduled Scan, Real-time Scan, and Scan Now but will not clean spyware/grayware components. Cleaning terminates processes or deletes registries, files, cookies, and shortcuts.
- Trend Micro provides assessment mode to allow you to evaluate items that Trend Micro detects as spyware/grayware and then take appropriate action based on your evaluation.



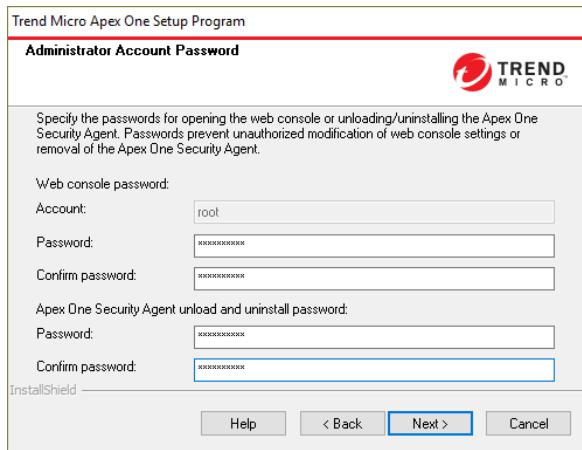
20 Click to enable the Apex One Web Reputation features on this server, if required.



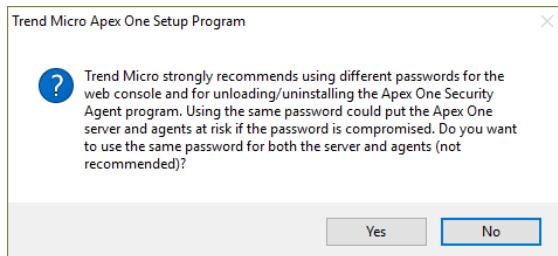
21 Enable the option to generate new authentication certificates, or use existing certificates from another Apex One Server.



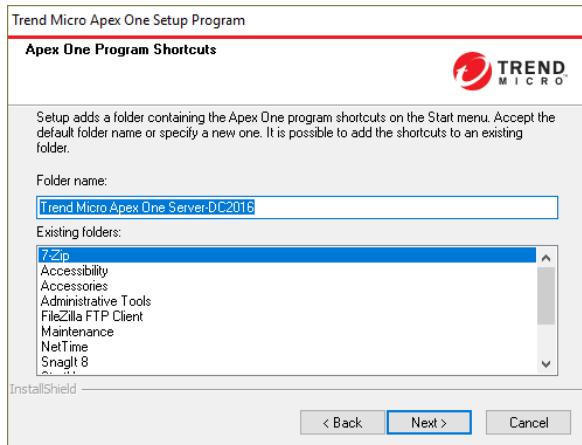
- 22** Type the login credentials for the **Root** Administrator. This administrator will be able to create identities for any other administrative users who require access to the Apex One Web Management console. As well, type the password that will be required to unload or uninstall the Security Agent from an endpoint computer.



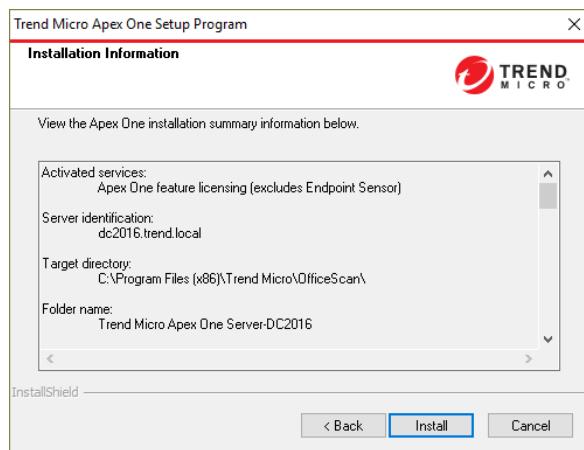
If the two password are identical, the setup program will display a warning. Click **Yes** to accept the use of the same passwords, or click **No** to retype new passwords.



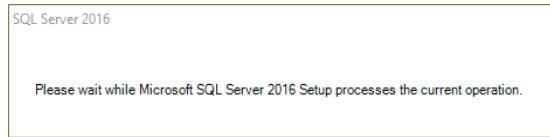
- 23** Confirm the folder group to display the Apex One program icons.



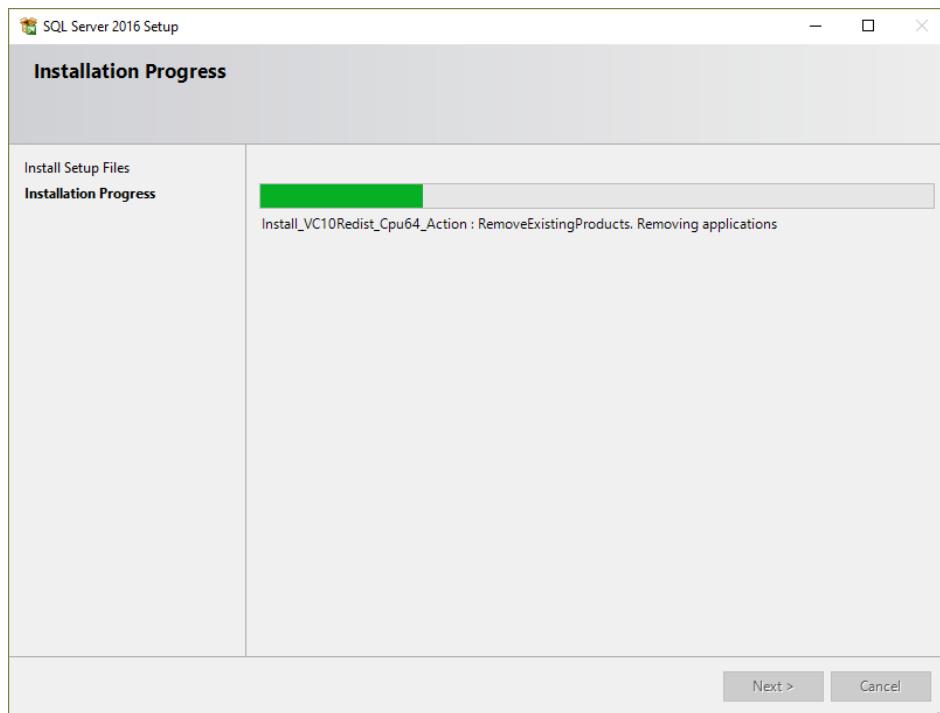
24 Finally, review the settings provided and click **Install**.



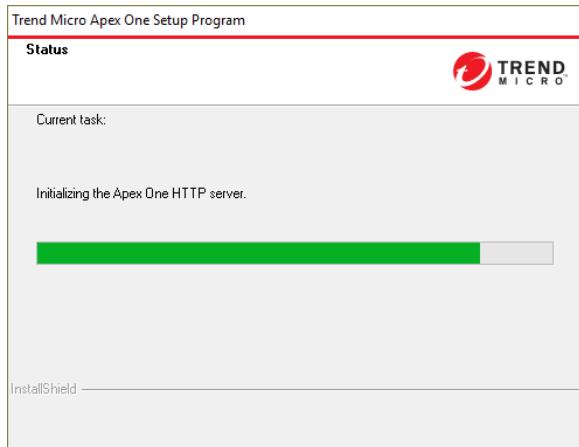
25 If the option to install an SQL Server Express 2016 instance, the setup for the database will launch.



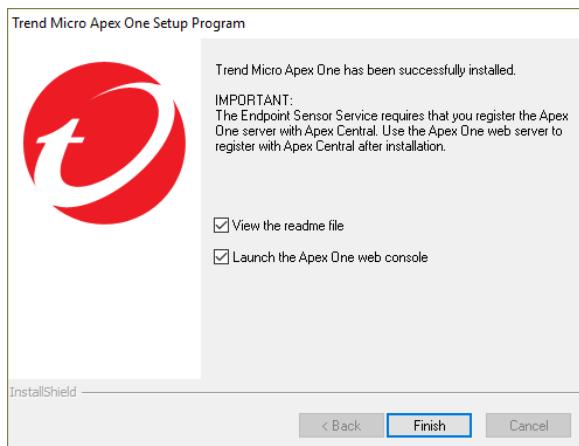
26 A progress bar will display the status of the database installation.



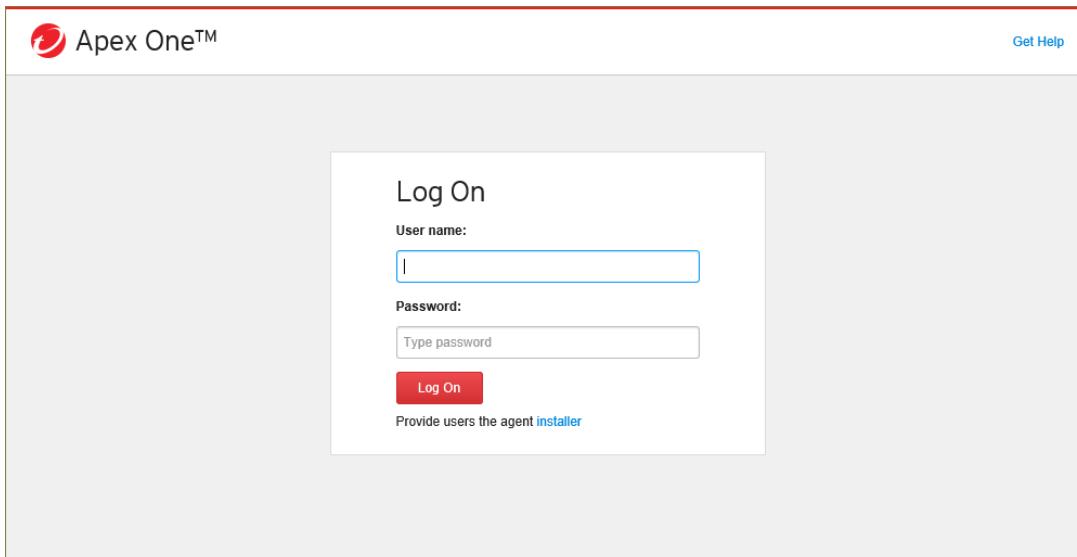
27 Once the SQL Server Express installation is complete, the **Setup Wizard** will continue with the Apex One setup operations.



28 Once complete, click **Finish** to close the wizard.

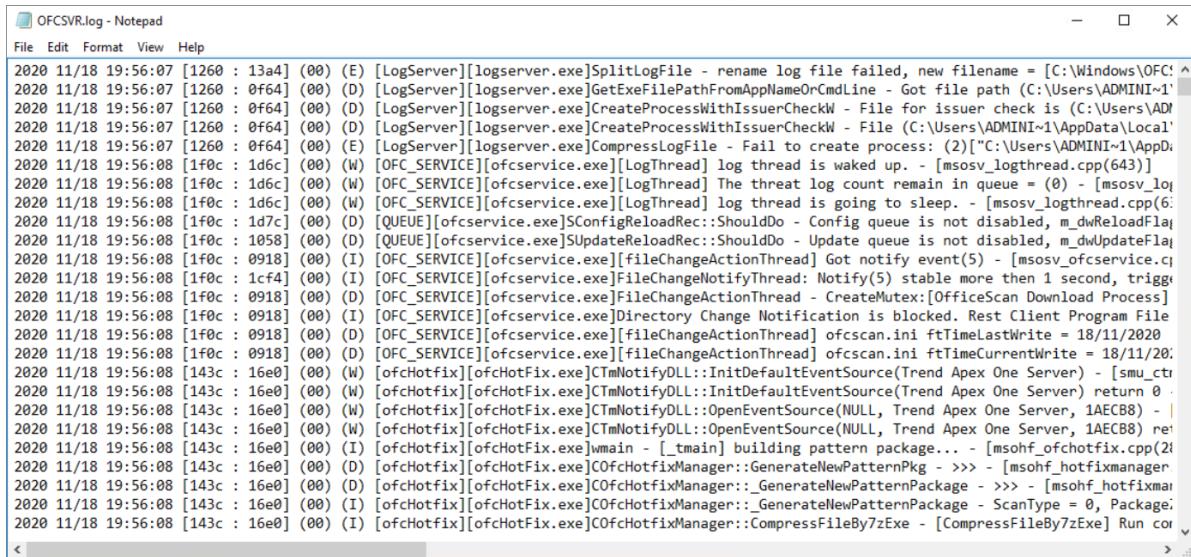


29 If the option to launch the console was enabled, the administrator is prompted to log in.



Installation Logs

The Apex One setup application records its actions in an installation log named `ofcmas.log`, which it creates in the `\Windows` folder.



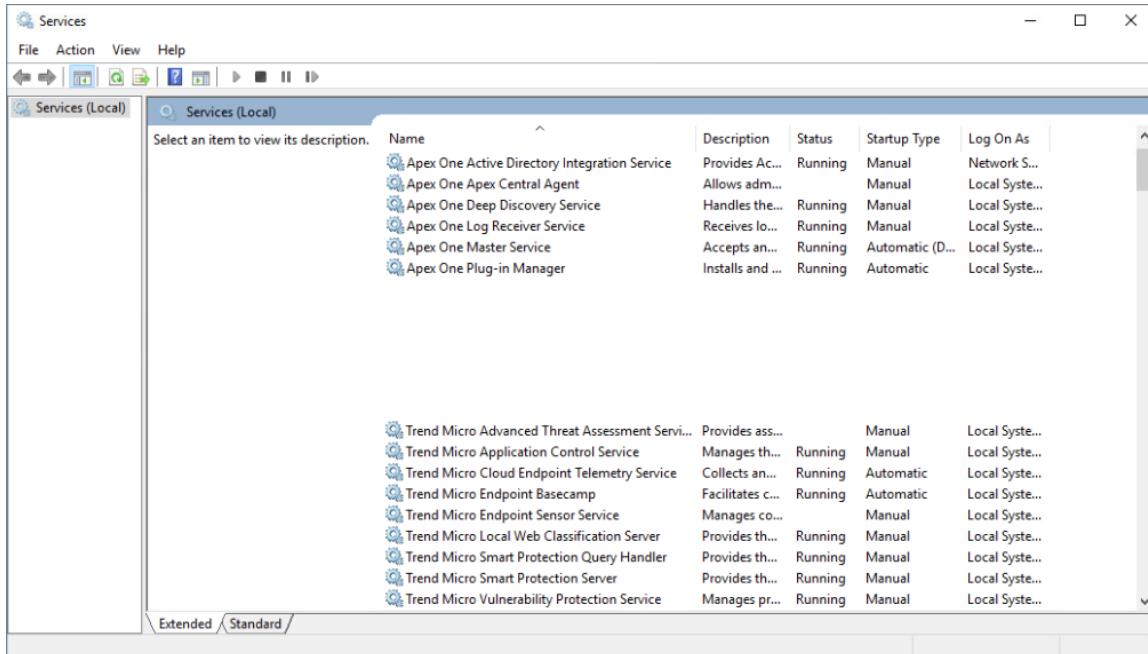
```

OFCSV.R.log - Notepad
File Edit Format View Help
2020 11/18 19:56:07 [1260 : 13a4] (00) (E) [LogServer][logserver.exe]SplitLogFile - rename log file failed, new filename = [C:\Windows\OFC\^
2020 11/18 19:56:07 [1260 : 0f64] (00) (D) [LogServer][logserver.exe]GetExeFilePathFromAppNameOrCmdLine - Got file path (C:/Users/ADMINI~1\
2020 11/18 19:56:07 [1260 : 0f64] (00) (D) [LogServer][logserver.exe]CreateProcessWithIssuerCheckW - File for issuer check is (C:/Users/ADMINI~1\
2020 11/18 19:56:07 [1260 : 0f64] (00) (D) [LogServer][logserver.exe]CreateProcessWithIssuerCheckW - File (C:/Users/ADMINI~1\AppData'\
2020 11/18 19:56:07 [1260 : 0f64] (00) (E) [LogServer][logserver.exe]CompressLogFile - Fail to create process: (2)[C:/Users/ADMINI~1/AppD\
2020 11/18 19:56:08 [1f0c : 1d6c] (00) (W) [OFC_SERVICE][ofcservice.exe][LogThread] log thread is waked up. - [msosv_logthread.cpp(643)]\
2020 11/18 19:56:08 [1f0c : 1d6c] (00) (W) [OFC_SERVICE][ofcservice.exe][LogThread] The threat log count remain in queue = (0) - [msosv_lo\
2020 11/18 19:56:08 [1f0c : 1d6c] (00) (W) [OFC_SERVICE][ofcservice.exe][LogThread] log thread is going to sleep. - [msosv_logthread.cpp(6\
2020 11/18 19:56:08 [1f0c : 1d7c] (00) (D) [QUEUE][ofcservice.exe]jConfigReloadRec::ShouldDo - Config queue is not disabled, m_dwReloadFlag\
2020 11/18 19:56:08 [1f0c : 1058] (00) (D) [QUEUE][ofcservice.exe]jUpdateReloadRec::ShouldDo - Update queue is not disabled, m_dwUpdateFlag\
2020 11/18 19:56:08 [1f0c : 0918] (00) (I) [OFC_SERVICE][ofcservice.exe][fileChangeActionThread] Got notify event(5) - [msosv_ofcservice.c\
2020 11/18 19:56:08 [1f0c : 1cf4] (00) (I) [OFC_SERVICE][ofcservice.exe]FileChangeNotifyThread: Notify(5) stable more than 1 second, trigge\
2020 11/18 19:56:08 [1f0c : 0918] (00) (D) [OFC_SERVICE][ofcservice.exe]FileChangeActionThread - CreateMutex:[OfficeScan Download Process]\
2020 11/18 19:56:08 [1f0c : 0918] (00) (I) [OFC_SERVICE][ofcservice.exe]Directory Change Notification is blocked. Rest Client Program File\
2020 11/18 19:56:08 [1f0c : 0918] (00) (D) [OFC_SERVICE][ofcservice.exe][fileChangeActionThread] ofcscan.ini ftTimeLastWrite = 18/11/2020\
2020 11/18 19:56:08 [1f0c : 0918] (00) (D) [OFC_SERVICE][ofcservice.exe][fileChangeActionThread] ofcscan.ini ftTimeCurrentWrite = 18/11/2020\
2020 11/18 19:56:08 [143c : 16e0] (00) (W) [ofcHotfix][ofcHotFix.exe]CTmNotifyDLL::InitDefaultEventSource(Trend Apex One Server) - [smu_ct\
2020 11/18 19:56:08 [143c : 16e0] (00) (W) [ofcHotfix][ofcHotFix.exe]CTmNotifyDLL::InitDefaultEventSource(Trend Apex One Server) return 0 \
2020 11/18 19:56:08 [143c : 16e0] (00) (W) [ofcHotfix][ofcHotFix.exe]CTmNotifyDLL::OpenEventSource(NULL, Trend Apex One Server, 1AECB8) - |\
2020 11/18 19:56:08 [143c : 16e0] (00) (W) [ofcHotfix][ofcHotFix.exe]CTmNotifyDLL::OpenEventSource(NULL, Trend Apex One Server, 1AECB8) re\
2020 11/18 19:56:08 [143c : 16e0] (00) (I) [ofcHotfix][ofcHotFix.exe]main - [_tmain] building pattern package... - [msohf_ofchotfix.cpp(21\
2020 11/18 19:56:08 [143c : 16e0] (00) (D) [ofcHotfix][ofcHotFix.exe]COfcHotfixManager::GenerateNewPatternPkg - >> - [msohf_hotfixmanager\
2020 11/18 19:56:08 [143c : 16e0] (00) (D) [ofcHotfix][ofcHotFix.exe]COfcHotfixManager::_GenerateNewPatternPackage - >> - [msohf_hotfixma\
2020 11/18 19:56:08 [143c : 16e0] (00) (I) [ofcHotfix][ofcHotFix.exe]COfcHotfixManager::_GenerateNewPatternPackage - ScanType = 0, Package\
2020 11/18 19:56:08 [143c : 16e0] (00) (I) [ofcHotfix][ofcHotFix.exe]COfcHotfixManager::CompressFileBy7zExe - [CompressFileBy7zExe] Run cor

```

Confirming Successful Installation

Open Windows Services and confirm that the Apex One services are running.



Ports and Protocols to Allow

Multiple ports must be allowed through an organization's firewall to enable Apex One to operate.

Name	Protocol	Port Number	Notes
Server Port	HTTP	8080	The web server listening port for the Apex One virtual directory. The HTTP or HTTPS ports are used by the Agents to download pattern file updates, and upload logs, quarantined files and status information. The HTTPS port is also used by Administrators to connect to the Apex One Web Management console.
	HTTPS	4343	These settings are stored in the Master_DomainPort parameter in the \PCCSRV\ofcscan.ini file.
Agent Port	TCP	21112	Configured during installation. Security Agent listening port where CGI commands such as update notifications and configuration changes are received from the Apex One server. Update Agent hosts also use the Agent Port to reply to download requests for scan engine and pattern file updates pulled by peer Security Agents. These settings are stored in the Client_LocalServer_Port parameter in the \PCCSRV\ofcscan.ini file.
Integrated Smart Protection Server (IIS)	HTTP	8080	Used to receive queries from Security Agents as part of cloud technology. When using the Apex One virtual site, the port is 8080 if the Apex One Web Management console uses HTTP. If HTTPS functionality is used, the port is 4343.
	HTTPS	4343	
Integrated Web Reputation Service (IIS)	HTTP	8080	Local Web Reputation Service uses this port to receive queries from Security Agents as part Web Reputation checks.
Apex Central	HTTP	80	Used for notification for updates from Apex Central as well as sending back status/virus events from Apex One Server to Apex Central.
	HTTPS	443	
NetBIOS for Remote Install	TCP/UDP	137, 139, 445	Used when installing Agents by Remote Install and when Agents send quarantined files to the Server using the UNC path.
LDAP for Active Directory	LDAP	389	Used when the Security Compliance function retrieves Active Directory information.
License Server	TCP/UDP	80, 60162, 60163	Used to access the Trend Micro License Server.
Edge Relay Server	HTTPS	443	Used for Security Agent to Edge Relay Server and Edge Relay Server to Apex One Server communication.
Unmanaged Endpoint	TCP	135	Used to check the endpoint connectivity. When connection is not established, Apex One immediately treats the endpoint as unreachable. The default port number is 135. Enabling this setting speeds up the query. When connection to endpoints cannot be established, the Apex One server no longer needs to perform all the other connection verification tasks before treating endpoints as unreachable.

SaaS: The only port and protocol requirement for the service implementation of Apex One is https, port 443.

Upgrading OfficeScan to Apex One (on-premises)

Apex One is the new name for OfficeScan; upgrading OfficeScan 11 SP1, XG and XG SP1 will update your installation to Apex One and convert OfficeScan Agents to new Apex One Security Agents.

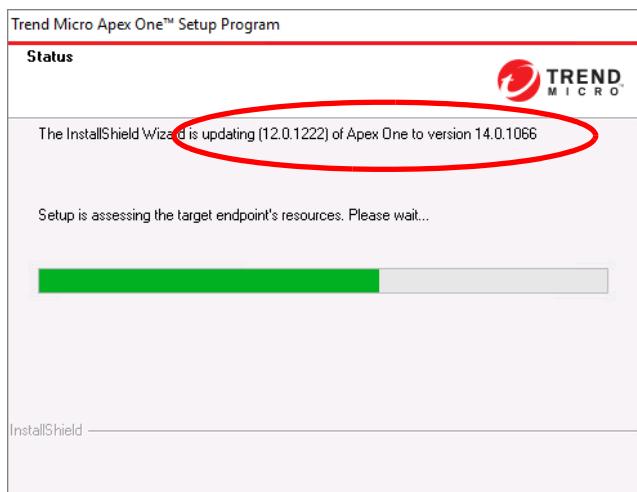
SaaS: In the service implementation of Apex One, upgrading the server is the responsibility of Trend Micro and is performed on a regular basis as needed.

OfficeScan 11 SP1, XG and XG SP1 can be upgraded directly to Apex One. If using a previous version of OfficeScan (11, 10.6 or 10.5), upgrade the installation to OfficeScan XG SP1, then upgrade to Apex One.

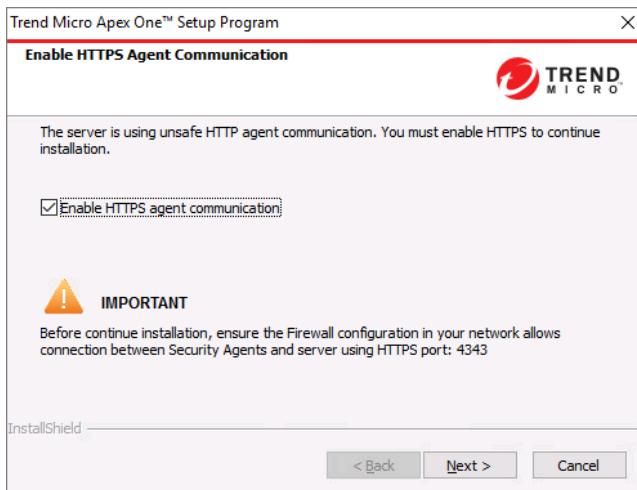
Note: A full back-up should be completed before running the upgrade, in case of any problems. Server Upgrade options can be classified into the following modes:

In-place Migration

This mode installs Apex One over an existing OfficeScan Server, and the installation program handles all the relevant changes.



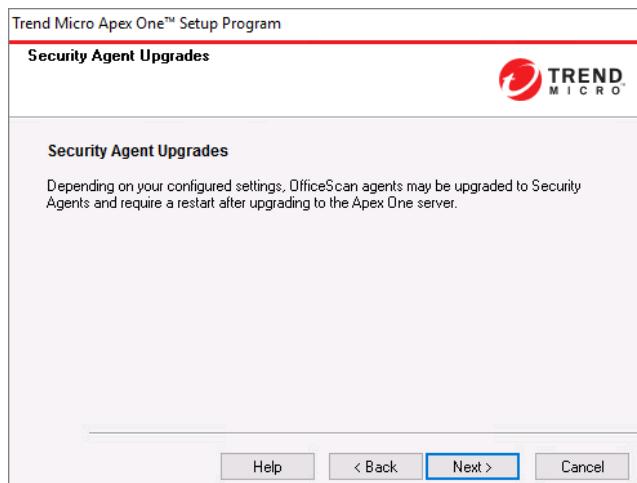
OfficeScan XG SP1 introduced the use of HTTPS for Server/Agent communication. If upgrading to Apex One from OfficeScan 11 SP1 or XG, the setup will prompt you to accept the use of HTTPS.



Note: Apex One moves the communication between Agents and the Server to HTTPS. By moving to HTTPS, the communication port on the server will also change from the HTTP port (default of 8080) to the HTTPS port (same as the Web Management console, default of 4343).

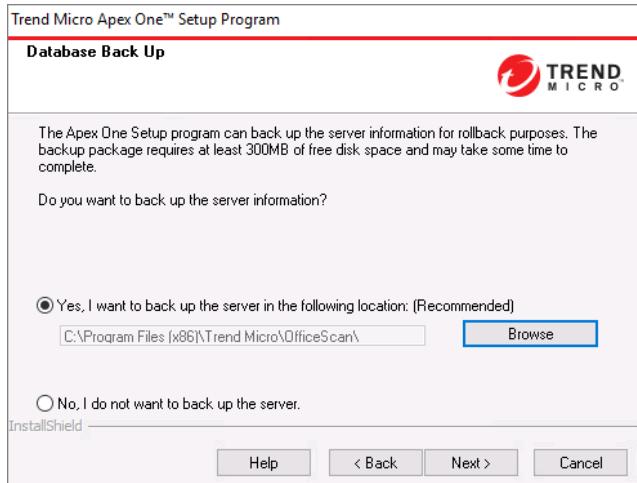
Some environments may encounter HTTPS communication issues due to various factors (for example, inconsistent SSL/TLS environments, firewalls blocking the HTTPS port, etc.). This can result in agents showing offline, failing to upgrade, and not uploading logs or quarantined files.

Depending on the permissions set in OfficeScan, Agents can be automatically upgraded to Apex One Security Agents as part of the upgrade process. This could introduce load issues in the environment if all Agents attempt an upgrade all at once. If this is a concern, disable the automatic upgrading of Agents in OfficeScan before launching the upgrade process.

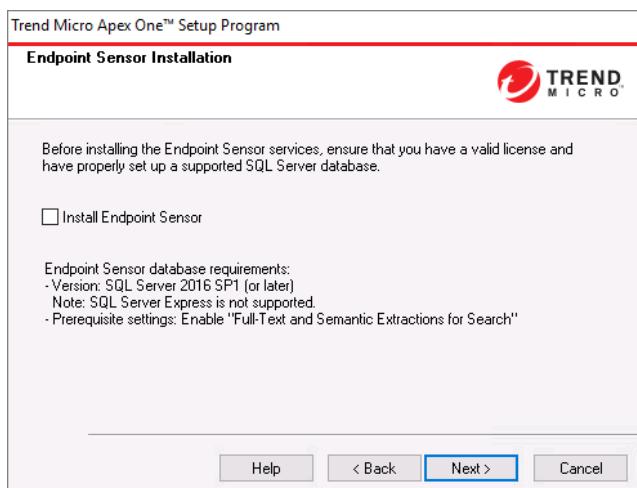


Lesson 2: Trend Micro Apex One Server

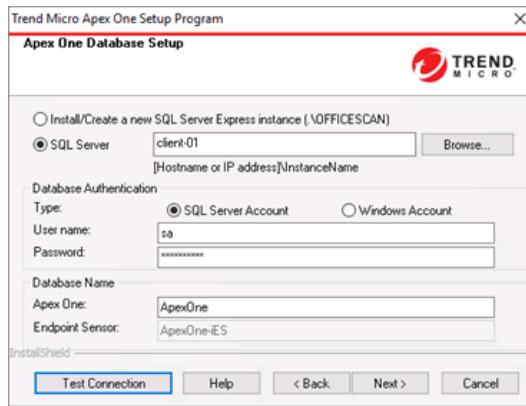
A backup of the server information is recommended before upgrading to Apex One. Click **Yes** to allow the setup application to perform a backup of the server data.



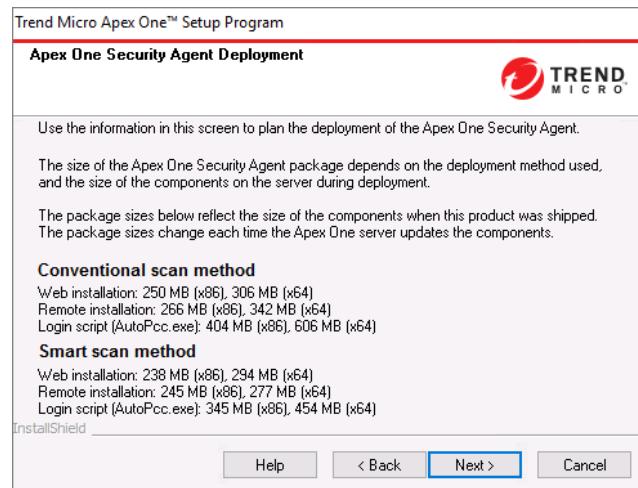
Apex One integrates Endpoint Sensor capabilities and this optional component can be installed during the upgrade, if required. Certain database conditions apply if this option is selected.



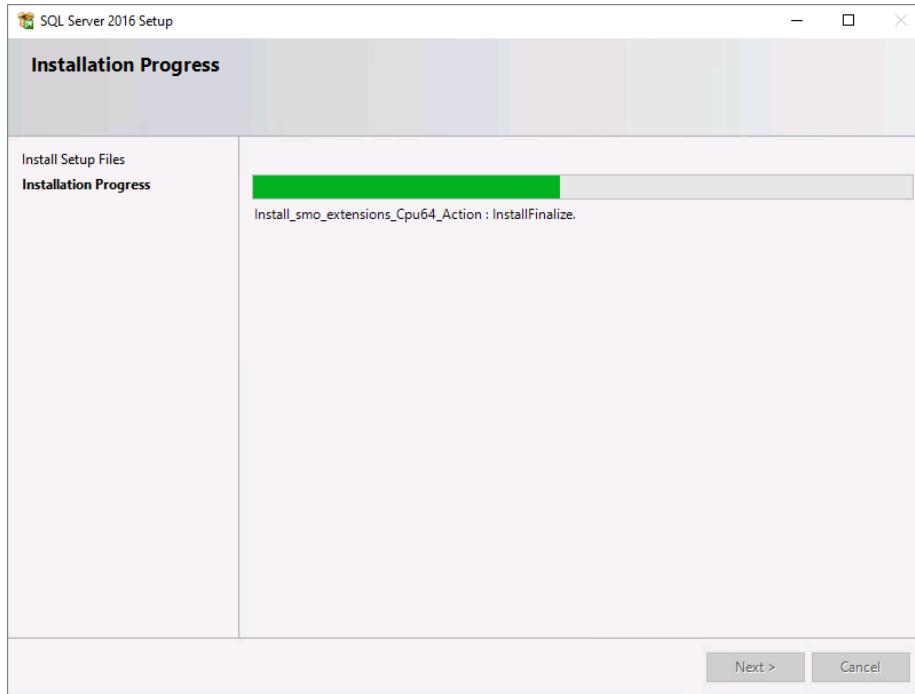
Apex One requires a Microsoft SQL Server database. If upgrading from an installation of OfficeScan 11 SP1, XG or XG SP1 using the built-in Codebase database, you will be prompted to provide details of an SQL Server instance. If an installation of SQL Server is not available, SQL Server Express can be installed as part of the setup.



To plan the deployment of Security Agents, sizing details of the Agent deployment packages are displayed.



If the option to use SQL Server Express was enabled, the database is installed and the Codebase tables are transitioned.



If Control Manager was used for policy management, it should be upgraded to Apex Central.

New Server

This mode installs Apex One on a separate, new server. Settings are exported from the existing OfficeScan installation, which are then imported into the new Apex One installation. OfficeScan Agents from the existing OfficeScan installation can then be moved to the new Apex One Server.

Best Practice: Since the new server installation provides more flexibility in determining when Agents are moved and also allows you to transition to different hardware or operating systems easily, this method is the recommended upgrade method.

Apex One Administrators can use the Server Migration Tool to copy settings from previous OfficeScan versions to the current version.

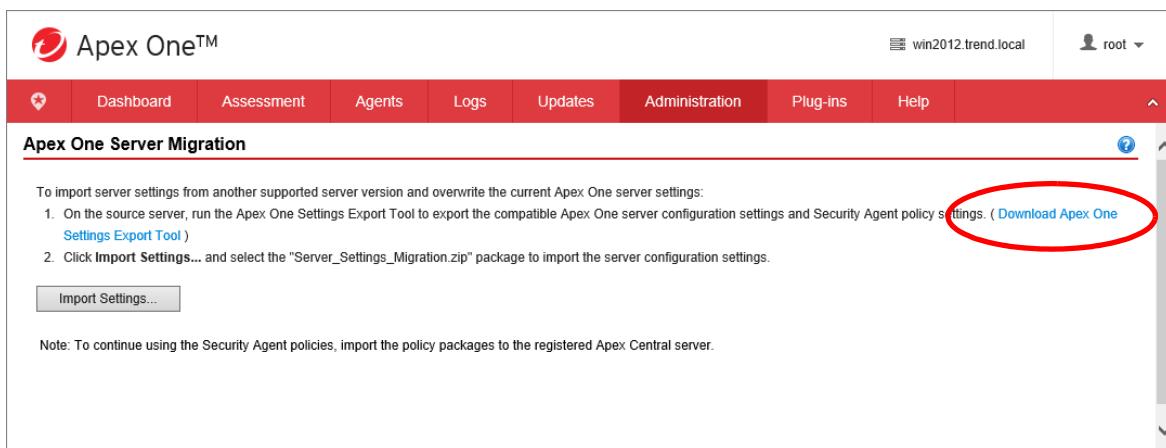
This tool exports the following settings from OfficeScan 10.0 and later, and imports the settings to the current version of Apex One:

- Domain structures
- Additional service settings *
- Manual Scan settings *
- Spyware/Grayware approved list *
- Scheduled Scan settings *

- Global Agent settings
- Real-time Scan settings *
- Endpoint location
- Scan Now settings *
- Firewall policies and profiles
- Web Reputation settings *
- Smart Protection sources
- Approved URL list *
- Server update schedule
- Behavior Monitoring settings *
- Agent update source and schedule
- Device Control settings *
- Notifications
- Data Loss Prevention settings *
- Proxy settings
- Privileges and other settings *
- OfficeScan_Agent_Port and Client_LocalServer_Port in the `ofcscan.ini` file

Note: Settings with an asterisk (*) retain the configurations at both the root and domain level. The tool does not back up the Security Agent listings of the Apex One Server only the domain structures. Security Agent only migrates features available on the older version of the Security Agent server. For features that are not available on the older server, Security Agent applies the default settings.

- 1 From the Apex One Web Management console on the new server, go to **Administration > Settings > Server Migration** and click **Download Apex One Settings Export Tool**. Save the `ApexOneSettingsExportTool.zip` file to the hard drive.



The screenshot shows the Apex One Web Management interface. The top navigation bar includes links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The current user is listed as 'root'. The main content area is titled 'Apex One Server Migration'. It contains instructions for importing server settings from another supported server version and overwriting the current Apex One server settings. Two steps are outlined: 1. On the source server, run the Apex One Settings Export Tool to export the compatible Apex One server configuration settings and Security Agent policy settings. (A red oval highlights the 'Download Apex One Settings Export Tool' link.) 2. Click Import Settings... and select the "Server_Settings_Migration.zip" package to import the server configuration settings. A note at the bottom states: 'Note: To continue using the Security Agent policies, import the policy packages to the registered Apex Central server.'

- 2 Copy the `ApexOneSettingsExportTool.zip` file to the source OfficeScan server computer and extract the files from the zip.

Alternately, navigate to the following folder on the Apex One Server computer:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\PolicyExportTool and copy this folder to the source OfficeScan server computer.

- 3 Double-click ApexOneSettingsExportTool.exe to start the **Apex One Settings Export Tool**.
- 4 Copy the resulting Server_Settings_Migration.zip package to a location that the destination Apex One Server can access.
- 5 To import the settings to the destination Apex One server, go to **Administration > Settings > Server Migration** and click **Import Settings**.

The screenshot shows the Trend Micro Apex One web interface. At the top, it says "Apex One™" and "win2012.trend.local". On the right, there's a user icon for "root". Below the header is a navigation bar with links: Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, Help. Under "Administration", the "Server Migration" link is highlighted. The main content area has a title "Apex One Server Migration". It contains instructions: "To import server settings from another supported server version and overwrite the current Apex One server settings:" followed by two steps. Step 1 points to "Download Apex One Settings Export Tool". Step 2 points to "Click Import Settings..." which is circled in red. Below these steps, a note says: "Note: To continue using the Security Agent policies, import the policy packages to the registered Apex Central server." There is also a "Help" link at the bottom right of the content area.

- 6 Locate the Server_Settings_Migration.zip package and click **Open**.
- 7 Verify that the server contains all the previous Apex One version settings.

The Server Migration Tool that is packaged with the current Apex One release must be used to export the settings from the previous OfficeScan version.

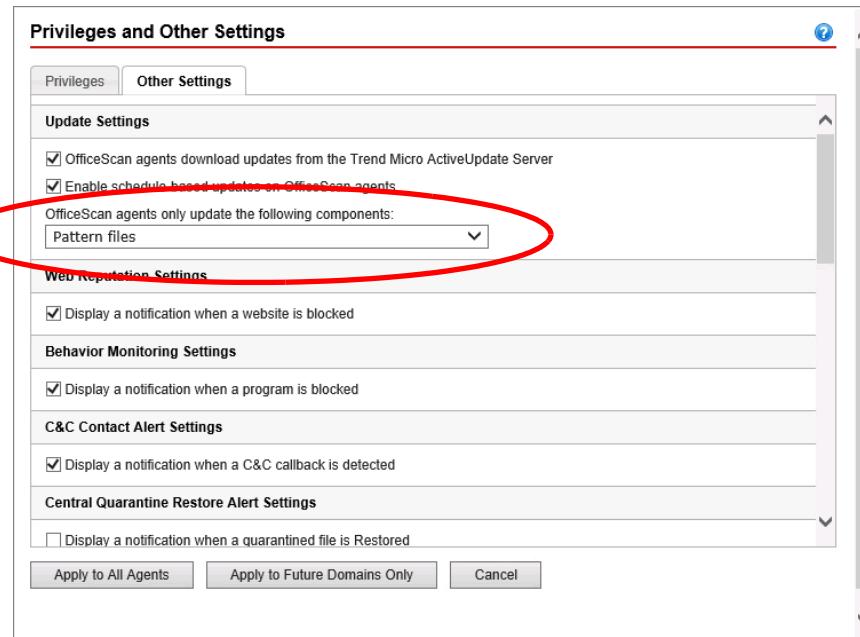
Upgrading OfficeScan as a Service to Apex One as a Service

Implementations of OfficeScan as a Service have already been upgraded to Apex One as a Service.

Upgrading OfficeScan Agents to Apex One Security Agents

OfficeScan Agents are automatically upgraded to Apex One Security Agents when the Server is upgraded. To delay the upgrade of Agents, turn off the Agent auto-update feature in OfficeScan XG before upgrading. This will be important in situations where bandwidth is limited.

In OfficeScan, access **Privileges and Other Settings** and set the **OfficeScan agents only update the following components** item to **Pattern files** only. Click **Apply to All Agents**.



When you decide to proceed with upgrading agents, In the new Apex One server, set this value to **All components (including hotfixes and the Agent program)**. When the OfficeScan Agent receives this new settings, it will upgrade to an Apex One Security Agent.

Upgrading to the Integrated Agent

In OfficeScan XG, Endpoint Sensor, Application Control, and Vulnerability Protection required a separate Agent on the endpoint. In Apex One, this functionality is now integrated in Apex One Server and Security Agent.

When Endpoint Sensor, Application Control, and Vulnerability Protection features are enabled through policy in Apex Central, and the policy is deployed to the Agents, the standalone Agent for that feature will be removed and a new Apex One services will be launched.

Upgrading to Apex One as a Service

The process for upgrading an on-premises installation of OfficeScan or Apex One are detailed in the Optional Lesson at the end of this document.

Pre-Upgrade Backup Considerations

It is important to back up the OfficeScan database and important configuration files before upgrading the Apex One Server. If upgrading a version of OfficeScan using the built-in Codebase database, it will be upgraded to Microsoft SQL Server as part of the process, using either a instance of SQL Server or a new

installation of SQL Server Express. Back up the OfficeScan Server database to a location outside the OfficeScan program directory.

- Back up the database from the OfficeScan Web Management console by going to **Administration > Database Backup**. If you have already transitioned to SQL with OfficeScan, use the SQL tools to backup the database
- Manually back up the following files and folders found in the C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV folder:
 - ofcscan.ini: Contains global client settings
 - ous.ini: Contains the update source table for antivirus component deployment
 - Private folder: Contains firewall and update source settings
 - ... \Web\tmOPP folder: Contains Outbreak Prevention settings
 - ... \Pccnt\Common\OfcPfw*.dat: Contains firewall settings
 - ... \Download\OfcPfw*.dat: Contains firewall deployment settings
 - ... \Log folder: Contains system events and the connection verification logs
 - ... \Virus folder: Contains quarantined files
 - ... \HTTPDB folder: Contains the OfficeScan database, if using Codebase
- Back up the existing key and certificate using the Authentication Certificate Manager Tool (CertificateManager.exe).
After the new installation completes, import the backed-up key and certificate to allow communication authentication between the Apex One Server and Security Agents to continue uninterrupted. If you create a new certificate during Server installation, Security Agents cannot authenticate Server communication because they would still be using the old certificate.

Server Service Setup Utility

The Server Service Setup Utility allows administrators to perform certain functions through a Command Line interface.

Open the Windows Command Prompt on the Apex One Server and navigate to the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\

Type the following command with the necessary parameters:

svrsvcsetup.exe [parameter]

A partial list of parameters is provided in this table.

Parameter	Description
/?	Displays parameter information for the command.
-install	<p>Installs and starts the Apex One Master Service, and creates virtual directories.</p> <p>This parameter will:</p> <ul style="list-style-type: none"> • Check dependencies and then stop related IIS services • Stop the IIS service • Delete the previous virtual key in the IIS metabase • Read virtual directory information (VIRDIR_INFO) from the uninstall configuration file (<code>ofuninst.ini</code>) • Write information to IIS metabase • Restart IIS and dependencies
-uninstall	<p>Uninstalls Apex One-related services but does not remove configuration files or the Apex One database.</p> <p>The Apex One Master Service, and Web server dependencies are removed.</p> <p>This parameter will:</p> <ul style="list-style-type: none"> • Check dependencies and then stop IIS-related services • Delete virtual directories ([VIRDIR_INFO]) information from uninstall log file (<code>ofuninst.ini</code>) • Restart IIS
-uninstall_upg	Back up settings and files for upgrade scenarios before removing Apex One.
-enablessl	<p>Enables SSL on the selected Web server. This command will:</p> <ul style="list-style-type: none"> • Create a new private key in <code>...\\PCCSRV\\Private\\certificate\\privkey.pem</code> • Blank the main login screen • Change the settings in the file to reflect these new keys • Generate <code>...\\PCCSRV\\Result.log</code> if the command is successful. The content of the log is: <p style="padding-left: 20px;">[RESULT]</p> <p style="padding-left: 20px;">Success=0</p>
-migratecmAgent	<p>Migrates the Apex One Server from the TMI-based Security Agent for Apex Central to the MCP-based Agent:</p> <ul style="list-style-type: none"> • <code>MigrateTMICfgToMCP</code> • <code>TryToUninstallITMIAgent</code>
-EnableIPv6	Enables IPv6 functionalities in the Apex One Server, and subsequently deploys IPv6 to Agents.

More information on `svrsvcsetup.exe` can be found in the following document in the Trend Micro Knowledge Base:

<http://esupport.trendmicro.com/solution/en-us/1036488.aspx>

SaaS: The Server Service Setup Utility is not available in the service implementation of Apex One.

Apex One (Mac)

Apex One (Mac) (previously known as Trend Micro Security for Mac) protects Mac endpoints against security risks, blended threats, and platform independent web-based attacks. As with Apex One for Windows, a Security Agent is installed on the Mac endpoint and reports its security status back to the Apex One (Mac) Server. The Server manages all the endpoints and administrators can easily configure security policies and deploy updates to every security agent through a separate Web Management console. Apex One (Mac) policies and endpoints can also be managed through Apex Central.

Apex One (Mac) maintains all the capabilities of Trend Micro Security for Mac but introduces some new features including:

- **Updated Web Management console:** The new Apex One (Mac) Server Web Management console makes it easier to manage and provides administrators with a modern interface experience.
- **Predictive Machine Learning support:** Apex One (Mac) adds a new engine to detect this emerging unknown security risks. It performs behavioral analysis on unknown, low-prevalence processes to determine if an emerging threat is attempting to infect the network.
- **Smart Scan enhancements:** Apex One (Mac) adds a new pattern called **Mac Heuristic Pattern**. This new pattern is used by Smart Scan to identify malware specifically targeting Mac platforms.
- **Device Control:** Apex One (Mac) has added Device control to allow administrators to limit usage on external devices.
- **Scan Mach-O File Type:** Apex One (Mac) introduces a new scan method called Scan Mach-O File Type. This method aims to improve the scan performance on Mac endpoints and is available for Full Scan and Manual Scans.
- **Trusted Program list:** Trusted Program List allows Security Agents to skip scanning of trusted processes to improve performance during scanning on endpoints. This list now includes common Mac applications.
- **Integrated Endpoint Sensor:** Metadata collected from Mac endpoints is collected by the integrated Endpoint Sensor and enables Preliminary Assessments on these endpoints.

Installing the Apex One (Mac) Plug-In

Apex One (Mac) is installed through the plug-in interface in Apex One. A separate Web Management console will become available to manage settings and configuration of the Mac Security Agents.

SaaS: No plug-in is required for Apex One (Mac) in the service implementation of Apex One.

- In the Apex One Web Management console, click the **Plug-ins** menu. In the **Apex One (Mac)** section, click **Download**.

The screenshot shows the 'Apex One (Mac)' section of the Trend Micro Apex One Web Management console. At the bottom, there is a download link for 'Available version: 3.5.2083 (42.78MB)'. The 'Download' button is highlighted with a red circle.

- Confirm the download of Apex One (Mac) and click **OK** to proceed. A progress bar displays the status of the download.

The screenshot shows the 'Apex One (Mac) Download' page. It displays a message: 'Downloading Apex One (Mac) version 3.5.2083, please wait. You may navigate to other Apex One pages while downloading.' Below this is a progress bar showing 'Progress: 0%'.

- After the download is complete, click **Install Now**, and accept the license agreement.

The screenshot shows the 'Apex One (Mac) Download' page again, but now it says 'Apex One (Mac) version 3.5.2083 download is complete.' Below this are two buttons: 'Install Now' and 'Install Later'. The 'Install Now' button is highlighted with a red circle.

- Once installed, click **Manage Program**.

The screenshot shows the 'Apex One (Mac)' section of the Trend Micro Apex One Web Management console. At the bottom, there is a 'Manage Program' button. This button is highlighted with a red circle.

5 Type the Apex One (Mac) Activation Code and click **Save**.

The screenshot shows the Trend Micro Apex One™ (Mac) activation page. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The URL in the address bar is dc2016.trend.local and the user is logged in as root. Below the navigation, it says "Trend Micro Apex One™ (Mac)". A note says "To obtain the Activation Code, please register online using the Registration Key that came with your product." There's a form for entering the Activation Code, which consists of six input fields separated by hyphens. The first field contains "Trend Micro Apex One™ (Mac)". A "Save" button is at the bottom.

Apex One (Mac) Web Management Console

To access the Apex One (Mac) console, open the Apex One Web Management console and click **Plug-ins**. In the **Apex One (Mac)** Section, click **Manage Program**.

The screenshot shows the Trend Micro Apex One™ (Mac) summary page. The navigation bar includes links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The main content area has tabs for "Trend Micro Apex One™ (Mac)" and "Summary". Under "Summary", there's a "Agents" section with a large grey circle icon. It shows "Connection Status" with 0 Online and 0 Offline agents. The "Detection Status" table shows 0 detections for Security Risks and 0 detections for Web Threats, both with 0 affected endpoints. Below this is an "Update Status" section with a table for various components like Virus Pattern, Spyware Active-monitoring Pattern, etc., all showing 0% update rate. A status message at the top right says "Status summary as of 3/19/2019 2:30:10 PM".

Apex One Plug-Ins

Apex One includes a framework called Plug-in Manager that integrates new solutions into the existing Apex One on-premises environment. Plug-in Manager delivers the following:

- **Native Product Features:** Some native Apex One features are licensed separately and activated through Plug-in Manager. In this release, two features fall under this category, namely, **Trend Micro Virtual Desktop Support** and **Apex One Data Protection**.

- **Plug-in programs:** Plug-in programs are not part of the Apex One program. The plug-in programs have separate licenses and management consoles. Access the management consoles from within the Apex One Web Management console. Examples of plug-in programs are **Trend Micro Apex One Toolbox**, **Apex One (Mac)** and some of the **Deployment Tools**.
- **Dashboard tabs and widgets:** The Apex One Dashboard screen requires Plug-in Manager to display the tabs and widgets used to monitor the Apex One Server and Agent protection status.

SaaS: No plug-ins are required in the service implementation of Apex One.

Plug-in Manager delivers the following plug-ins for Apex One:

Apex One Data Protection

Apex One Data Protection is designed to minimize the risk of information loss and improve visibility of data usage patterns and risky business processes so your private information remains secure. You gain broad coverage, high performance, and deployment flexibility needed to comply with regulatory mandates.

Trend Micro Endpoint Encryption Deployment Tool

Trend Micro Endpoint Encryption ensures end-to-end data protection by providing FIPS 140-2 full disk encryption for data at rest and file, folder, and removable media encryption for data in motion. The Trend Micro Endpoint Encryption Deployment Tool provides a framework to centrally manage, deploy, and execute Agent installation/uninstallation commands to endpoints managed by the Apex One server. The tool leverages the Apex One server client tree hierarchy to remotely execute deployment tasks.

Before attempting to install Trend Micro Endpoint Encryption, ensure that the environment meets all system requirements.

Apex One (Mac)

Apex One (Mac) (previously known as Trend Micro Security for Mac) protects Mac endpoints against security risks, blended threats, and platform independent web-based attacks.

Trend Micro Virtual Desktop Support

Optimize virtual desktop protection by using Trend Micro Virtual Desktop Support. This feature regulates tasks on Apex One clients residing in a single virtual server.

Trend Micro Apex One Toolbox

The Apex One Toolbox functions as a framework that manages, deploys, executes and consolidates logs for a variety of standalone Trend Micro tools. The Toolbox leverages the Agent tree hierarchy of the Apex One Server to remotely execute these tools on Security Agents managed by the Apex One Server.

Apex One Utilities

Apex One includes a collection of stand-alone utilities and tools to simplify certain server tasks. These utilities and tools can also be accessed from the following folder on the Apex One Server:

```
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\admin\Utility
```

SaaS: The utilities are not accessible from the Apex Server in the service implementation of Apex One. Instead, they can be accessed from the Trend Micro Support Web site.

Authentication Certificate Manager

The Authentication Certificate Manager tool is used to manage Trend Micro certificates and keys.

This utility (CertificateManager.exe) is located in the following folder on the Apex One Server:

```
... \PCCSRV\admin\Utility\CertificateManager
```

Agent Packager

The Agent Packager tool creates an installation package that you can send to users using conventional media such as CD-ROM. Users run the package on the Agent endpoint to install or upgrade the Security Agent and update components.

Agent Packager is especially useful when deploying the Security Agent or components to endpoints in low-bandwidth remote offices. Security Agents installed using Agent Packager report to the server where the package was created.

This utility (ClnPack.exe) is located in the following folder on the Apex One Server:

```
... \PCCSRV\admin\Utility\ClientPackager
```

Cisco Trust Agent

The Cisco Trust Agent (CTA) enables the Apex One client to report antivirus information to Cisco ACS.

The CTA packages are located in the following folder on the Apex One Server:

```
... \PCCSRV\admin\Utility\CTA
```

Domains Schedule Update

The update schedule configured in automatic client updates only applies to clients with scheduled update privileges. For other clients, you can set a separate update schedule. To do this, you will need to configure a schedule by client tree domains. All clients belonging to the domain will apply the schedule.

This utility (`dsu_convert.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\DomainScheduleUpdate
```

Edge Relay Server Installer

The Apex One Edge Relay Server provides administrators with visibility and increased protection of endpoints that users take outside of the company's intranet.

The installation program for the Edge Relay Server (`setup.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\EdgeServer
```

Gateway Settings Importer

Apex One checks the endpoint's location to determine the Web Reputation policy to use and the Smart Protection source to which to connect. One of the ways Apex One identifies the location is by checking the endpoint's gateway IP address and MAC address.

Configure the gateway settings on the Endpoint Location screen or use the Gateway Settings Importer tool to import a list of gateway settings to the Endpoint Location screen.

The Gateway Settings Importer tool (`GSIImporter.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\GatewaySettingsImporter
```

Image Setup

Disk imaging technology allows you to create an image of the Security Agent using disk imaging software and make clones of it on other computers on the network. Each Security Agent installation needs a Globally Unique Identifier (GUID) so that the server can identify Agents individually. Use the Apex One program called `ImgSetup.exe` to create a different GUID for each of the clones.

This utility (`ImgSetup.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\ImgSetup
```

Agent Mover

If you have more than one Apex One server on the network, use the Agent Mover tool to transfer Security Agents from one Apex One server to another. This is especially useful after adding a new Apex One server to the network and you want to transfer existing Security Agents to the new server.

This utility (`IpXfer.exe` or `IpXfer_x64.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\IpXfer
```

Integrated Service Package

This folder contains installers for the integrated Application Control, Vulnerability Protection, Advanced Threat Assessment and Endpoint Sensor components.

These installers are located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\iServicePackage
```

Integrated Smart Protection Server Tool

The Trend Micro Integrated Smart Protection Tool helps administrators install or uninstall an Integrated Smart Protection Server after the Apex One server installation is completed.

This Integrated Smart Protection Tool Installer program (`ISPSInstaller.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\ISPSInstaller
```

Device List Tool

Run the Device List Tool locally on each endpoint to query external devices connected to the endpoint. The tool scans an endpoint for external devices and then displays device information in a browser window. You can then use the information when configuring device settings for Data Loss Prevention and Device Control.

This utility (`ListDeviceInfo.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\ListDeviceInfo
```

Message Queue

This utility is used to interact with the Windows Message Queuing service.

This utility (`mqtool.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\MessageQueue
```

Console Password Reset Tool

This utility can reset the Apex One Web Management console password in situations where the password has been lost or the previous administrator has left the company without providing the password to the new staff.

This utility (`OSCEResetPW.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\OSCEResetPW
```

Plug-in Manager Installer

This utility installs the Apex One Plug-in Manager.

This utility (`PLMSetup.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\PLM
```

Apex One Settings Export Tool

This Apex One Settings Export Tool allows administrators to copy Apex One settings from previous Apex One versions to the current version.

This utility (`ApexOneSettingsExportTool.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\PolicyExportTool
```

Apex One Server Migration Tool

The Apex One Server Migration Tool is a tool that helps you to move the Apex One settings or configuration from one Apex One server to another.

This utility (`ServerMigrationTool.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\ServerMigrationTool
```

ServerProtect Normal Server Migration Tool

The ServerProtect Normal Server Migration Tool is a tool that helps migrate computers running Trend Micro ServerProtect Normal Server to the Security Agent.

This utility (`SPNSXfr.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\SPNSXfr
```

Server Tuner

Use Server Tuner to optimize the performance of the Apex One Server using parameters for server-related performance issues, including downloads and network traffic.

This utility (`SvrTune.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\SvrTune
```

Apex One VDI Pre-Scan Template Generation Tool

Use the Apex One VDI Pre-Scan Template Generation Tool to optimize on-demand scans or remove GUIDs from base or golden images. This tool scans the base or golden image and certifies the image. When scanning duplicates of this image, Apex One only checks parts that have changed. This ensures shorter scanning time.

This utility (`TCacheGen.exe` or `TCacheGen_x64.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\TCacheGen
```

System Health Validator

This utility is required to support Network Access Protection (NAP) in Apex One.

This utility (`OfficeScanNAPSAV_x64.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\SystemHealthValidator
```

Trend Micro Vulnerability Scanner

The Vulnerability Scanner checks the presence of security software on host machines and can install the Security Agent to unprotected host machines.

This utility (`TMVS.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\TMVS
```

Cache Generator

This utility is as part of the Gold Image creation process. Any machines provisioned from this gold image will be able to assign a new GUID by itself upon boot up. The standard user will not have to do anything related to Apex One on their machine.

This utility (`TCacheGen_x64.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\TCacheGen
```

Touch Tool

The Touch Tool synchronizes the time stamp of one file with the time stamp of another file or with the system time of the computer. If you unsuccessfully attempt to deploy a hot fix on the Apex One server, use the Touch Tool to change the time stamp of the hot fix. This causes Apex One to interpret the hot fix file as new, which makes the server attempt to automatically deploy the hot fix again.

This utility (`TMTouch.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\Touch
```

Decrypt Tool

To prevent quarantined infected from being opened, Apex One encrypts the file before quarantining it or when backing up a file before cleaning it. Apex One provides a tool that decrypts and then restores the file in case you need to retrieve information from it.

This utility (`VSEncode.exe`) is located in the following folder on the Apex One Server:

```
...\\PCCSRV\\admin\\Utility\\VSEncrypt
```

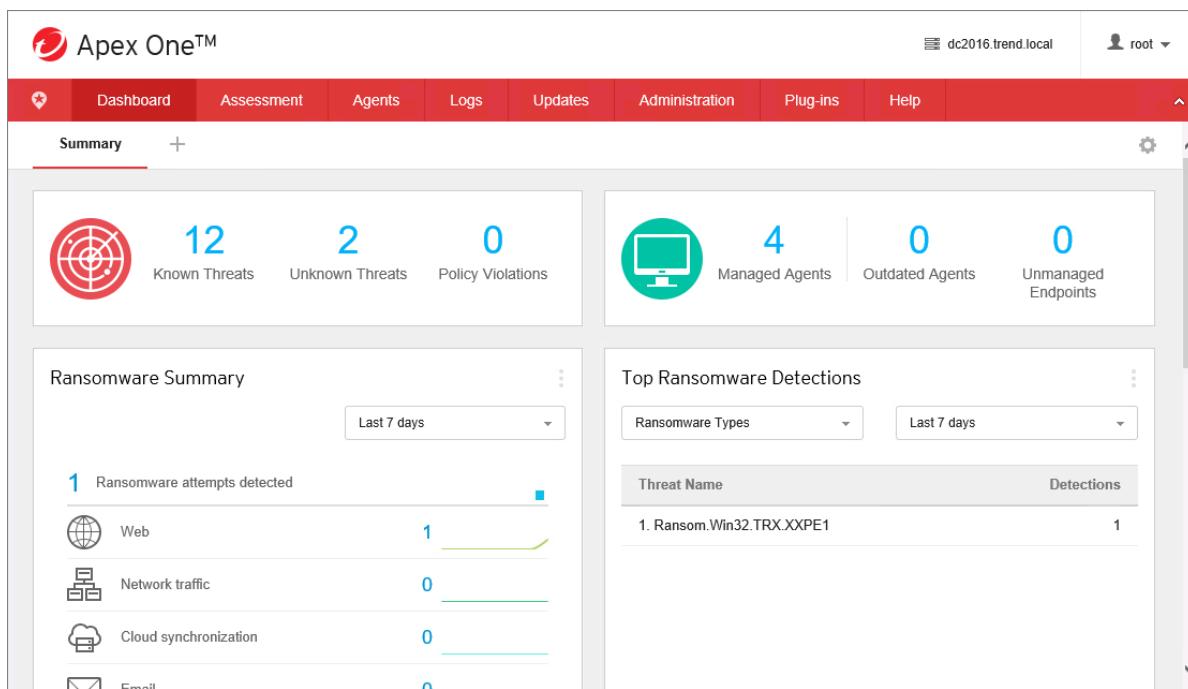

Lesson 3: Trend Micro Apex One Web Management Console

Lesson Objectives:

After completing this lesson, participants will be able to:

- Complete administrative tasks through the Apex One Web Management console
- Describe the steps in the Web Management console login process
- Create new roles and user accounts
- Import user accounts from Active Directory

The Apex One Web Management console allows administrative users with the appropriate permissions to manage policies, computers and system settings through a Web-based interface. Administrative users authenticate to the Apex One Web Management console through a supported browser, and click the appropriate menu and interface components to perform system operation.



SaaS: The service implementation of Apex One uses Apex Central for the majority of management tasks. Information in this section applies primarily to the on-premises implementation of Apex One.

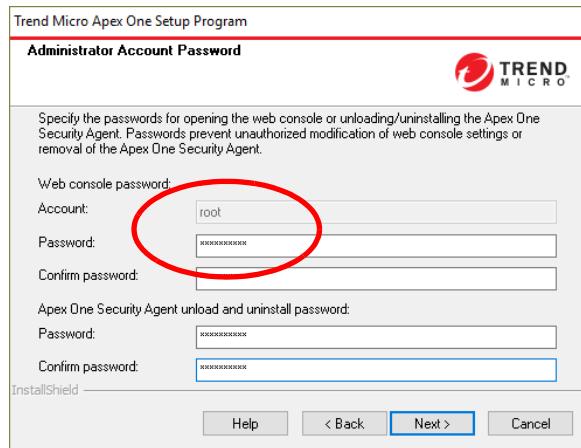
The Apex One Web Management console is the central point for monitoring Apex One throughout the corporate network. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The Web Management console uses standard Internet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

Some of the administrative tasks completed in the Web Management console include:

- Deploying and managing Security Agents installed on networked endpoints
- Grouping Agents into logical domains for simultaneous configuration and management
- Setting scan configurations and initiating manual scan on a single or multiple networked endpoints
- Configuring notifications about security risks on the network and viewing logs sent by Agents
- Configuring outbreak criteria and notifications
- Delegating Web Management console administration tasks to other Apex One administrators by configuring roles and user accounts
- Ensuring that Agents comply with security guidelines

Logging into the Web Management Console

The credentials used by the default root administrator are assigned during the Apex One Server setup process.



This default user account called **root** cannot be deleted using the Web Management console.

Upon first login, it is the responsibility of the root user to define user roles and set up user accounts to allow other administrative users to access the Web Management console without using the root account.

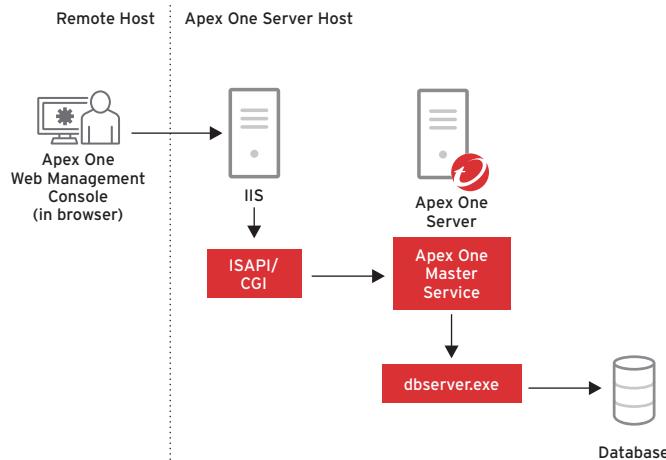
In a supported Web browser, type one of the following in the address bar based on the type of Apex One server installation.

- With SSL on a default site:
`https://<Apex One server FQDN or IP address>/officescan`
- With SSL on a virtual site:
`https://<Apex One server FQDN or IP address>:<port number>/officescan`

Alternately, the Web Management console can be accessed on the Apex One Server itself by clicking the **Apex One Web Management console** link in the **Trend Micro Apex One Server** program group in the Windows Apps list.

Web Management Console Communication

The Web Management console communicates with the Apex One Server over HTTPS at the server port using CGI programs. The Web Management console CGIs are unique to the communication made between the console and the Apex One Web server. A specific command handler responds to CGI requests sent from the Web Management console.



Note: The Web Management console does not support Windows 8, 8.1, or Windows Server 2012 in Windows UI mode.

The Web Management console invokes CGIs to display Agent information, respond to Agent requests and install Agents remotely. There are two types:

- **Administration CGIs:** These are used to display information on the Web Management console and to respond to Agent requests. These are stored in:

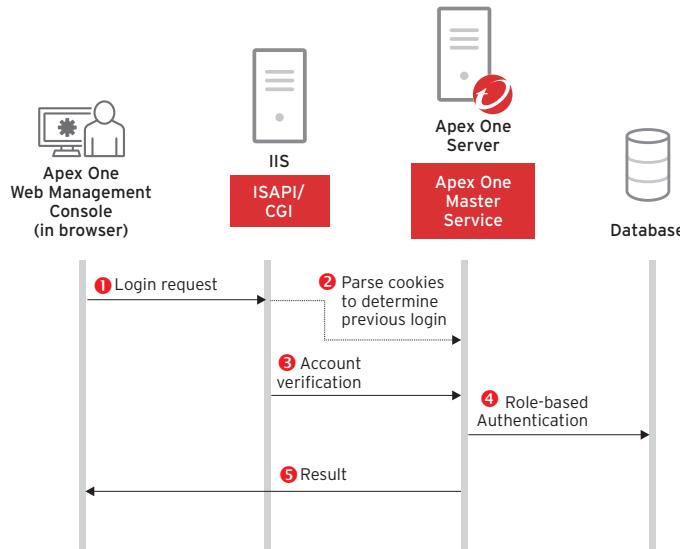
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Web_OSCE\Web_console\CGI

- **Remote Install CGIs:** These are used to deploy Security Agents as part of remote installation functionality. These are stored in:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Web_OSCE\Web_console\RemoteInstallCGI

Login Process

The steps involved in the Web Management console login include the following:



Certificate warnings

Since the digital certificate created during the Apex One Server setup process is self-signed, browsers may not recognize the digital signature applied to the certificate by the Apex One Server and a certificate warning will be displayed when administrators log into the Apex One Web Management console.

To access the console without any security warnings, the self-signed certificate of the Apex One Server can be imported in the certificate store on the administrative user's computer. Import the certificate into the **Trusted Root Certification Authorities > Registry** store.



Alternately, the self-signed certificate and corresponding private key can be replaced with a new pair of keys in which the public portion is submitted to a trusted commercial certification authority.

Timeout Mechanism

The Web Management console timeout mechanism revolves around a session file created in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\TEMP

Session files are named *.key_xxxxxx, where xxxxxx represents a series of random numbers. The Apex One Server creates this file each time a user logs on successfully.

Note: The inability to create this file will cause the Web Management console to always time-out even during the login phase.

Go to **Administration > Settings > Web Console** to configure the required timeout settings. Select **Automatically log off inactive users** to enable the Apex One server to log off users after a period of inactivity (in minutes).

The screenshot shows the Trend Micro Apex One Web Management Console interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The title 'Apex One™' is on the left, and the URL 'dc2016.trend.local' and user 'root' are on the right. Below the navigation is a red header bar with the text 'Web Console Settings'. Underneath, a sub-header says 'Configure web console settings that apply to the Apex One server.' There are two main sections: 'Automatic Refresh Settings' and 'Time-out Settings'. In the 'Time-out Settings' section, a checkbox labeled 'Automatically log off inactive users' is checked and circled in red. Below it, the 'Inactive interval' is set to '30 minutes'. At the bottom of this section are 'Save' and 'Cancel' buttons.

Automatic Refresh

The Web Management console can also be configured to automatically refresh the display of data. Click **Automatically refresh the web console** to enable the refresh screen data at the specified frequency (in seconds).

The screenshot shows the 'Web Console Settings' page of the Apex One interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The 'Administration' tab is active. On the left, there's a sidebar with 'Web Console Settings'. The main content area has two sections: 'Automatic Refresh Settings' and 'Time-out Settings'. In the 'Automatic Refresh Settings' section, there's a checked checkbox for 'Automatically refresh the web console' and a dropdown menu set to '30 seconds'. This entire section is circled in red. Below it is the 'Time-out Settings' section, which contains a checked checkbox for 'Automatically log off inactive users' and a dropdown menu set to '30 minutes'. At the bottom of the page are 'Save' and 'Cancel' buttons.

Active Directory Integration

Apex One can be integrated with an existing Microsoft Active Directory structure to manage Security Agents more efficiently, assign Web Management console permissions using Active Directory accounts, and determine which Agents do not have security software installed.

All users in the network domain can have secure access to the Apex One Web Management console. You can also configure limited access to specific users, even those in another domain. The authentication process and the encryption key provide validation of credentials for users.

Active Directory integration allows you to take full advantage of the following features:

- **Role-based administration:** Assign specific administrative responsibilities to users by granting them access to the Web Management console using their Active Directory accounts.
- **Custom Agent groups:** Use Active Directory or IP addresses to automatically group Agents and map them to domains in the Security Agent tree.
- **Unmanaged endpoints:** Locate any computers in the network that are not managed by the Apex One Server and install a Security Agent.
- **User-based rules:** Assign Application Control and Device Control rules based on Active Directory groups

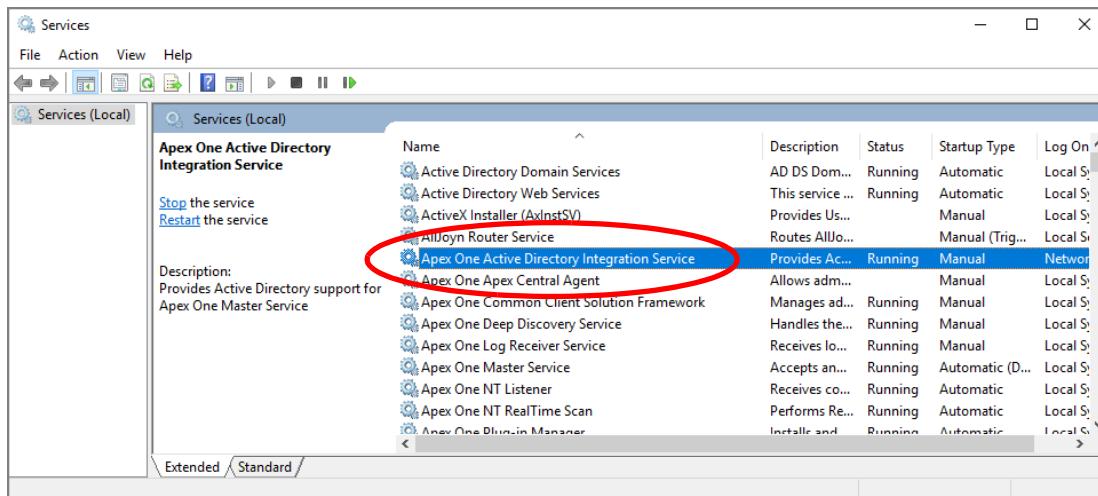
To integrate the Apex One Server with Active Directory, click **Administration > Active Directory > Active Directory Integration**. Provide the details of the Active Directory domain and click **Save and Synchronize**.

If required, click **Specify Domain Credentials** to provide a username and password for domain synchronization

The screenshot shows the 'Active Directory Domains' section of the configuration interface. It includes fields for entering domain names ('trend') and specifying domain credentials, along with encryption settings for domain credentials. Buttons for 'Save', 'Cancel', and 'Save and Synchronize' are at the bottom.

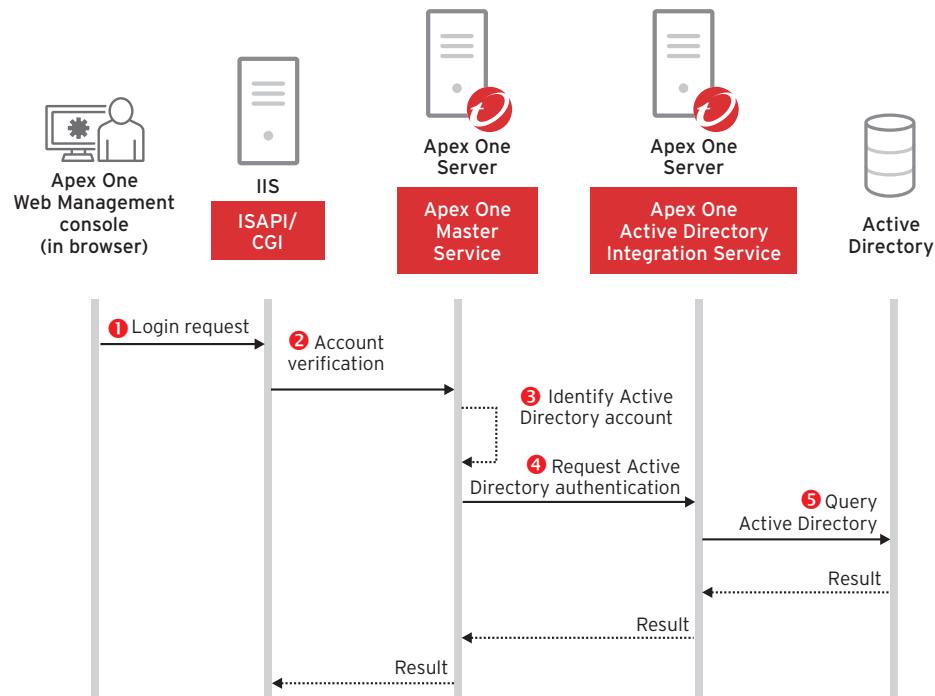
Apex One Active Directory Integration Service

The Apex One Server relies on the **Apex One Active Directory Integration Service** to interface with the Active Directory infrastructure. This service appears in the Windows service list.



Authenticating Administrative Users From Active Directory

The steps involved in authenticating administrative users with identities stored in Active Directory include the following:



Steps 1 and 2 are identical to how native Apex One accounts are processed. The difference arises when the Apex One Server detects that the account is an Active Directory account, as shown in Step 3.

When Apex One Server detects that an Active Directory account is being used, it passes authentication responsibility to the **Apex One Active Directory Integration Service**, which then interfaces with the Active Directory server to verify the password provided.

If the account passes authentication, the Role-Based Administration process begins.

Administrative Accounts

In addition to the root account, additional administrative accounts or Active Directory accounts can be added through the Apex One Web Management console.

Administrative accounts grant and control access to the Apex One Web Management console. If there are several Apex One administrators in your organization, you can use this feature to assign specific Web Management console privileges to the administrators and present them with only the tools and permissions necessary to perform specific tasks. You can also control access to the Agent tree by assigning them one or several domains to manage. In addition, you can grant non-administrators *view only* access to the Web Management console.

Each user (administrator or non-administrator) is assigned a specific role. A role defines the level of access to the Web Management console. Users log on to the Web Management console using custom user accounts or Active Directory accounts.

Role-based administration involves the following tasks:

- Defining user roles
- Configuring user accounts and assign a particular role to each user account.

The following activities related to administrative user access to the Web Management console are logged:

- Logging in to the Web Management console
- Modifying an administrative user password
- Logging off from the console
- Session timeout (user is automatically logged off)

Defining User Roles

Define and assign user roles to limit the access specific user accounts have to certain Web Management console screens. You can define user roles to completely hide Web Management console screens, limit access to Read Only, or grant full configuration rights.

Built-in Roles

There are two accounts and roles that are part of a default Apex One installation:

Administrator: Delegate this role to other Apex One administrators or users with sufficient knowledge of Apex One. Users with this role have **Configure** permissions to all menu items.

Guest User: Users with this role have **View** permissions to all menu items except:

- Plug-ins
- Administration > Account Management > User Roles
- Administration > Account Management > User Accounts

The screenshot shows the 'User Roles' section of the Apex One web interface. At the top, there are buttons for 'Add', 'Copy', 'Delete', 'Export', and 'Import'. Below this, a table lists user roles. The first row, 'Administrator (Built-in)', is highlighted with a red circle. A tooltip for this row states: 'This built-in role cannot be modified or removed. Users with this role have full access to all Apex One Web console menu items and functions.' The second row, 'Guest User (Built-in)', also has a tooltip: 'This built-in role cannot be modified or removed. Users with this role have no access to Plug-in Manager and Role-based Administration, and view only access to all other console items.' At the bottom of the table, there are more 'Add', 'Copy', 'Delete', 'Export', and 'Import' buttons.

Custom Roles

New custom user roles can be created if the available built-in roles do not satisfy the requirements.

To create a custom role, click **Add**, and complete the **Role Information** and **Role Permissions** sections.

The screenshot shows the 'Add Role' page in the Trend Micro Apex One web console. In the 'Role Information' section, the 'Name' field is set to 'Junior Administrator'. In the 'Role Permissions' section, the 'Menu Items for Servers/Agents' tab is selected and circled in red. The 'Available Menu Items' table shows the following permissions:

Available Menu Items	View	Configure
Agents	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Agent Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Agent Grouping	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Global Agent Settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Endpoint Location	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Connection Verification	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Outbreak Prevention	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Updates	<input type="checkbox"/>	<input type="checkbox"/>
Administration	<input type="checkbox"/>	<input type="checkbox"/>

- Click **Menu items for Servers/Agents** to specify permissions for menu settings for all servers and Agents, regardless of the selected domain.
- Click **Menu items for Managed Domains** to specific permissions for menu settings in domains configured in the Agent Tree Scope.

Importing Roles

If you have saved custom roles from a different Apex One server and want to use these roles in the current Apex One server, export the roles and import them into the current server. A *.dat file containing the custom roles will be used to transfer the role details. Consider the following when importing roles from another server:

- **User Roles** will be overwritten if you import a role with the same name.
- Importing roles can only be done between Servers that have the same version.
- A role imported from another Apex One Server retains the permissions for menu items for Servers/Agents and menu items for managed domains.
- A role imported from another Apex One server applies the default permissions for Agent Management menu items. On the other server, record the role's permissions for Agent Management menu items and then re-apply them to the role that was imported.

Configuring User Accounts

Configure a user account or use Active Directory accounts to assign permissions to view or configure the granular Agent settings, tasks, and data that are available in the Agent tree. You must assign a particular role to each user, which determines the Web Management console menu items that the user can view or configure. You can use Apex One user accounts to perform single sign-on to Apex One from the Apex Central console.

A **root** account is created as part of the Apex One Server setup process and is assigned the built-in Administrator role.

User Name	Description	Domain	Role	Enable
root	Administrator account created during installation		Administrator (Built-In)	<input checked="" type="checkbox"/>

Adding Apex One Accounts

To create an Apex One account, go to **Administration > Account Management > User Accounts** and click **Add**. Complete the details for the account, making sure to select an appropriate Role from the list.

The screenshot shows the 'User Accounts' creation interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration (which is highlighted in red), Plug-ins, Help, and a user dropdown for 'root'. Below the navigation is a sub-navigation bar for 'User Accounts' with tabs for Step 1 User Information, Step 2, and Step 3. A checked checkbox labeled 'Enable this account' is present. Under 'User Roles', a dropdown menu shows 'Junior Administrator'. The 'User Information' section contains fields for 'User name' (set to 'Kelly_Mills'), 'Description' (empty), 'Password' (filled with a series of asterisks), 'Confirm password' (also filled with asterisks), and 'Email address' (set to 'kelly.mills@acme.com'). A note at the bottom of this section says 'For example: johnsmith@yourcompany.com'. A red circle highlights the 'Custom account' radio button, which is selected over the 'Import from Active Directory' option.

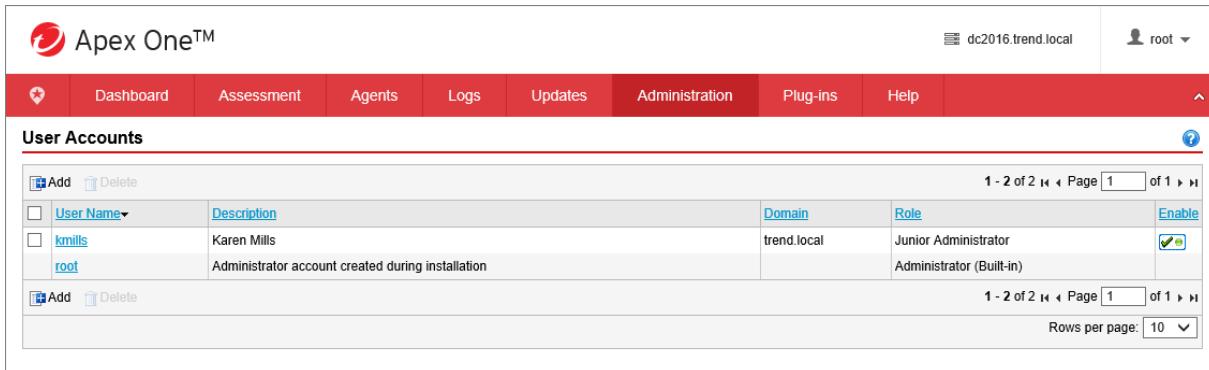
Importing Active Directory Accounts

Apex One administrators have the option to log on to the console using Active Directory credentials. Both Active Directory users and groups can be used. The account and assigned permissions exist in Apex One database, but login credentials remain in Active Directory account.

Apex One administrators can import Active Directory accounts which in turn creates an Apex One account that is designated as an Active Directory account. Use **Search** to locate the Active Directory user who will become an administrator, add to the **Selected Users and Groups** list and click **Next**.

Select the Agent Tree Scope to define the branches of the Agent Tree this administrator will have control over and click **Next**.

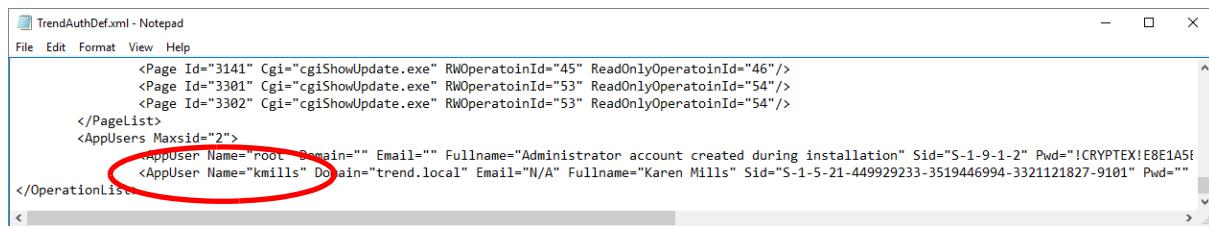
The new user account is displayed.



The screenshot shows the 'User Accounts' section of the Apex One console. There are two entries:

User Name	Description	Domain	Role	Enable
kmills	Karen Mills	trend.local	Junior Administrator	<input checked="" type="checkbox"/>
root	Administrator account created during installation	trend.local	Administrator (Built-in)	<input checked="" type="checkbox"/>

Accounts created by importing an Active Directory account also create a corresponding entry in TrendAuthDef.xml file located in C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Private\AuthStore.



The screenshot shows the 'TrendAuthDef.xml - Notepad' window. It contains XML code representing configuration settings. A red circle highlights the <AppUser> entry for the 'root' account:

```
<Page Id="3141" Cgi="cgiShowUpdate.exe" RWOperatoinId="45" ReadOnlyOperatoinId="46"/>
<Page Id="3301" Cgi="cgiShowUpdate.exe" RWOperatoinId="53" ReadOnlyOperatoinId="54"/>
<Page Id="3302" Cgi="cgiShowUpdate.exe" RWOperatoinId="53" ReadOnlyOperatoinId="54"/>
</PageList>
<AppUsers Maxsid="2">
    <AppUser Name="root" Domain="" Email="" Fullname="Administrator account created during installation" Sid="S-1-9-1-2" Pwd="!CRYPTEX!E8E1A5f..."/>
    <AppUser Name="kmills" Domain="trend.local" Email="N/A" Fullname="Karen Mills" Sid="S-1-5-21-449929233-3519446994-3321121827-9101" Pwd=""..."/>
</AppUsers>
</OperationList>
```

Note the following about imported accounts:

- Only the login name, full name of the user and Active Directory domain of which the account is a part are recorded.
- Password information for the Active Directory account is not stored. As a result, the password parameter is blank.
- The key account identifier is the **WinUser** parameter. If this is set to 1, then this is an Active Directory user. A 0 would indicate that it is a native Apex One account.
- The SID for this account corresponds to the Active Directory account's SID. Apex One accounts, on the other hand, use a locally generated number.

Note: Since the passwords for Active Directory administrators are not under the control of Apex One, any password changes for these administrators must be performed through the Active Directory tools.

Domain permissions

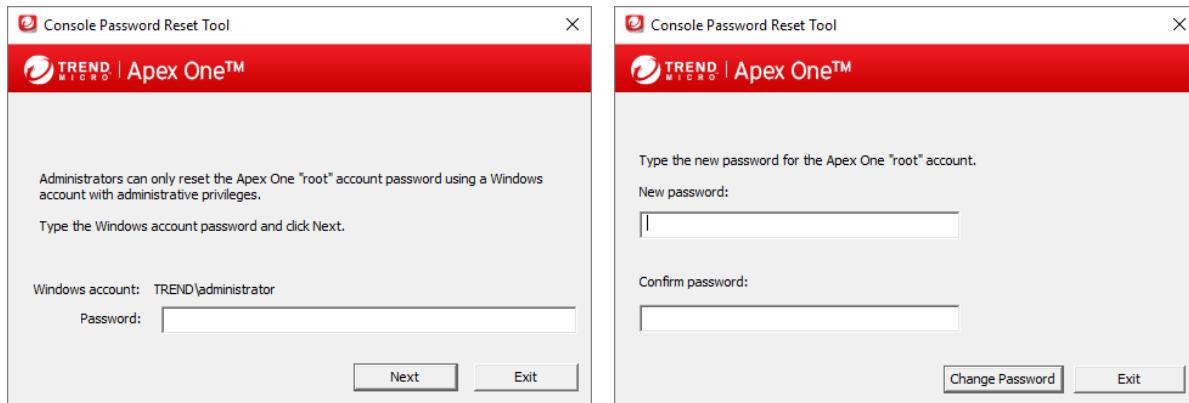
When defining permissions for domains, Apex One automatically applies the permissions for a parent domain to all the subdomains that it manages. A subdomain cannot have lesser permissions than its parent domain. For example, if the System Administrator has permission to view and configure all Agents that Apex One manages (the **Apex One Server** domain), the permissions for the subdomains must allow the System Administrator access to these configuration features. Removing a permission on a subdomain would mean that the System Administrator does not have full configuration permissions for all Agents.

Recovering From Forgotten Passwords

The Password Reset Tool (OSCEResetPW.exe) can recover the password of the root administrator. An administrative user must authenticate to the tool using their Windows Administrator password. Locate the tool at the following location:

```
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\  
OSCEResetPW
```

Run OSCEResetPW.exe and login with your Windows Domain Admin credentials to assign a new password to the root administrator account.



Lesson 4: Managing Security Agents

Lesson Objectives:

After completing this lesson, participants will be able to:

- Describe the responsibilities of the Security Agent
- Describe the Security Agent services and components
- Install and uninstall Security Agents on endpoint computers
- Migrate from other security products
- Define Reference Servers
- Configure Security Agent settings
- View the status of Security Agents
- Configure Security Agent self-protection
- Grant user privileges to modify Security Agent settings

Security Agent Tasks

Security Agents are the protection-tier component of an Apex One environment. The Agent is responsible for protecting hosts from malware, network threats, and Web threats. The Agent sends events (such as virus/malware detection) and status information (for example, completion of an update, Agent shutdown etc.) to the Apex One Server in real time.

Security Agents provide the following protection on endpoint computers:

- Conventional and SmartScan virus protection
- Grayware/Spyware protection
- Device control
- Firewall
- Outbreak prevention
- Smart Protection
- Behavior monitoring
- Data loss prevention
- Suspicious connection service
- Web threat protection
- Predictive Machine Learning protection
- Sample submission
- Memory scanning
- Browser Exploit protection
- Vulnerability protection
- Application Control protection

Security Agent Services and Components

The following services and components are installed as part of the Security Agent.

Component	Description
Apex One NT Listener Service (TmListen.exe)	<p>Receives commands and notifications from the Apex One Server and is responsible for the following functionality:</p> <ul style="list-style-type: none"> • Server-Agent communication • Updates • Component startup • Log delivery
Apex One NT Real-time Scan Service (Ntrtscan.exe)	<p>Performs manual, on-demand and real-time scanning functionality and is responsible for using the following scan engines:</p> <ul style="list-style-type: none"> • Virus Scanning API (VSAPI) • Spyware Scanning API (SSAPI) • Damage Cleanup Engine (DCE) • Advanced Threat Scanning Engine (ATSE) • iCRC modules <p>This service also assumes responsibility for starting the Unauthorized Change Prevention Service (TMBMSRV.exe).</p>
Apex One NT Firewall Service (TmPfw.exe)	Provides packet level firewall, network virus scanning, and intrusion detection capabilities. Through the Web Management console, administrators can create rules and apply them to filter connections (for example, by application, IP address, port number, or protocol).
Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)	<p>This service is responsible for protecting the Apex One registry settings from unauthorized changes and preventing processes and services from being stopped. This service is responsible for the following:</p> <ul style="list-style-type: none"> • Behavior Monitoring • Device Control • Certified Safe Software Service
Apex One Common Client Solution Framework (TmCCSF.exe)	<p>This service provides a pluggable platform for new Trend Micro Core Technologies. These technologies include:</p> <ul style="list-style-type: none"> • Browser Exploit Prevention, which checks the behavior of web pages in real time to detect malicious scripts and/or programs • Behavior-based, enhanced memory scanning • Advanced Threat Scan Engine DLL and Predictive Machine Learning
Trend Micro Endpoint Sensor Service (TMESC.exe)	This service provides integrated endpoint sensor capabilities.
Trend Micro Application Control Agent Service (TMiACAgentSvc.exe)	This service provides application and device control capabilities.

Component	Description
Trend Micro Vulnerability Protection Service (iVPAgent.exe)	This service provides integrated vulnerability protection capabilities. This service detects Intrusion Prevention rule violations and automates the application of virtual patches.
Trend Micro Advanced Threat Assessment Service (AtasAgent.exe)	Identifies potentially compromised endpoints through on-demand assessment and monitoring. By integration with Trend Micro Threat Investigation Center, Advanced Threat Assessment Service allows administrators and information security experts to perform forensic tasks on endpoints for remote incident response.

Apex One Security Agents use the following non-service applications to provide additional functionality.

Apex One NT Monitor (PccNTMon.exe)	<p>This process provides the user-interactive components of the Apex One Security Agent. It is responsible for the following functionalities:</p> <ul style="list-style-type: none"> Starting the security agent console (PccNt.exe) Displaying the security agent icon in the system tray Sending quarantined files to the Apex One Server Detecting Internet Explorer proxy settings
------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Configuration Repositories

Security Agent configuration settings are stored in the following locations:

- **Windows Registry:** The Registry serves as the main repository for Security Agent settings on Windows, including:
 - Scan settings
 - Agent-Server communication settings
 - Web threat functionality settings
 - Firewall settings
 - Location awareness settings
- **plist (Mac Agents):** Mac Security Agent settings are stored in the macOS plist file.
- **ous.ini:** Contains information about alternative update sources that an Security Agent can use
- **ofcscan.ini:** Contains global Agent settings. Security Agents download this file from the Server to obtain initial configuration settings
- **GetServer.ini:** Contains information regarding the Apex One Server when the Agent is roaming.
- **ssnotify.ini:** Contains information related to existing Smart Protection Servers. Every time a new Smart Protection Server becomes available for the Agent to choose from, it will be added to this file.

Security Agent Tree

The Security Agent tree displays all the Agents grouped into domains that the Server currently manages and allows you to simultaneously configure, manage, and apply the same configuration to all domain members.

The screenshot shows the Apex One™ Agent Management interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root' on the server 'dc2016.trend.local'. Below the navigation bar is a search bar and a link to 'Advanced search'. The main area is titled 'Agent Management' and contains a table of agents. The table has columns for Status, Tasks, Settings, Logs, Manage Agent Tree, and Export. The table lists five agents under the 'Trend' domain:

Domain/Endpoint	Logon User	IP Address	Listening...	Domain H...	Connecti...	GUID	Scan Met...	Restart Required	Data l
CLIENT-01	CLIENT-01\Administrator	192.168.4.2	21112	Trend\	Online	3945081d-396a-402e-b...	Smart Scan	No	Not in
CLIENT-02	CLIENT-02\Administrator	192.168.4.4	21112	Trend\	Online	62a5bd02-c2fb-4da7-93...	Smart Scan	No	Not in
CLIENT-03	CLIENT-03\Administrator	192.168.4.6	21112	Trend\	Online	e2b9522-ba58-45f9-ab...	Smart Scan	No	Not in
DC2016	TREND\Administrator	192.168.4.1	21112	Trend\	Online	8223ba62-85c5-4eed-a...	Smart Scan	No	Not in
WIN2012	WIN2012\Administrator	192.168.4.3	21112	Trend\	Online	e6edef5f1406-4783-be4...	Smart Scan	No	Not in

At the bottom of the table, it says 'Number of agents: 5', 'Agents using smart scan: 5', and 'Agents using conventional scan: 0'.

The Security Agent tree icons display the type of endpoint and the status of Security Agents that Apex One manages.

Above the Agent tree are menu items that allow administrators to perform specific tasks, such as configuring Agent settings or initiating Agent tasks. To perform any of the tasks, select the task target and then select a menu item. Alternately, menu items can be accessed by right-mouse clicking items in the tree, such as the tree root, domains, groups or individual computers.

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.

Security Agent System Requirements

The Security Agent can be installed on computers running Microsoft Windows or Mac platforms.

Platform	OfficeScan XG	OfficeScan XG SP1	Apex One
Windows XP	√	√	x
Windows 7 (SP1 required for Apex One)	√	√	√
Windows 8	√	√	x
Windows 8.1	√	√	√
Windows 10	√	√	√
Windows Server 2003	√	√	x
Windows Server 2008	√	√	x
Windows Server 2008 R2	√	√	√
Windows Server 2012	√	√	√
Windows Server 2012 R2	√	√	√
Windows Server 2016 R2	√	√	√
Windows Server 2019	x	x	√
OS X Mavericks 10.9 or later	√	√	√
OS X Yosemite 10.10 or later	√	√	√
OS X El Capitan 10.11	√	√	√
macOS Sierra 10.12	√	√	√
macOS High Sierra 10.13	√	√	√
macOS Mojave 10.14	x	x	√
macOS Catalina	x	x	√
macOS Big Sur	x	x	√

Hardware Requirements

- Processor: 300 MHz Intel Pentium or equivalent (Windows 7, 8.1, 10 family) and Intel Core processor for Mac
1.0 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent (Windows Embedded POSReady7)
1.4 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent (Windows 2008 R2, Windows 2016 family, Windows 2019 family)

- **Memory:** 512 MB minimum (2.0 GB recommended) with at least 100 MB exclusively for Apex One (Windows 2008 R2, 2012 family)
1.0 GB minimum (2.0 GB recommended) with at least 100 MB exclusively for Apex One (Windows 7 (x86), 8.1 (x86), Windows Embedded POSReady 7, 10 (x64) family)
2.0 GB minimum (4.0 GB recommended) with at least 100 MB exclusively for Apex One (Windows 7 (x64), 8.1 (x64), 10 (x64) family)
512 MB minimum for Apex One on Mac
- **Disk Space:** 1.5GB minimum (3GB recommended for all products) for Windows, 300 MB minimum for Mac

Security Agent Features by Platform

Security features available in Apex One Security Agent vary by platform as shown in this table:

Platform	Windows Client	Windows Server	Mac
Anti Malware	√	√	√
Behavior Monitoring	√	√	√
Predictive Machine Learning	√	√	√
Data Loss Prevention	√	√	x
Endpoint Sensor	√	√ ¹	√ ³
Application Control	√	√	x
Vulnerability Protection	√	√ ²	x
Web Reputation	√	√	√
Device Control	√	√	√
Firewall	√	√	x

¹ Endpoint Sensor on Windows Server platforms supported in Apex One as a Service only.

² Vulnerability Protection patterns available for Windows endpoint platforms only

³ Endpoint Sensor on Mac supported with limited capabilities

Installing Security Agents

In the on-premises implementation of Apex One, there are several installation methods available for Security Agent deployment. Factors which can affect the selection of the installation method used by your organization can include:

- The method used in the organization to deploy new endpoint computers (for example, are endpoint computers based on a golden image, or a scripted mechanism)
- The method used to distribute new software (for example, are new applications deployed automatically using SCCM, Active Directory policies, or installed by the end user)
- The network bandwidth available during the deployment
- Security policies in the organization
- The operating system used on the endpoint computer
- Administrator preference

SaaS: Installation methods for Security Agents are limited in the service implementation of Apex One.

Security Agent Deployment Prerequisites

Insure that the following prerequisites are met before attempting to install an Security Agent using one of the above methods:

- Communication with Apex One Server is available
- Administrative level privileges are required to install software
- No registry keys already on client from previous installation
- Client can access UNC path of Apex One installation folder (for Remote, Web, or AutoPCC installs)
- If an existing anti-virus application is present, it must be removable by Apex One
- File and Print Sharing must be excluded from the Windows Firewall for some methods
- Remote Registry Service enabled for some methods

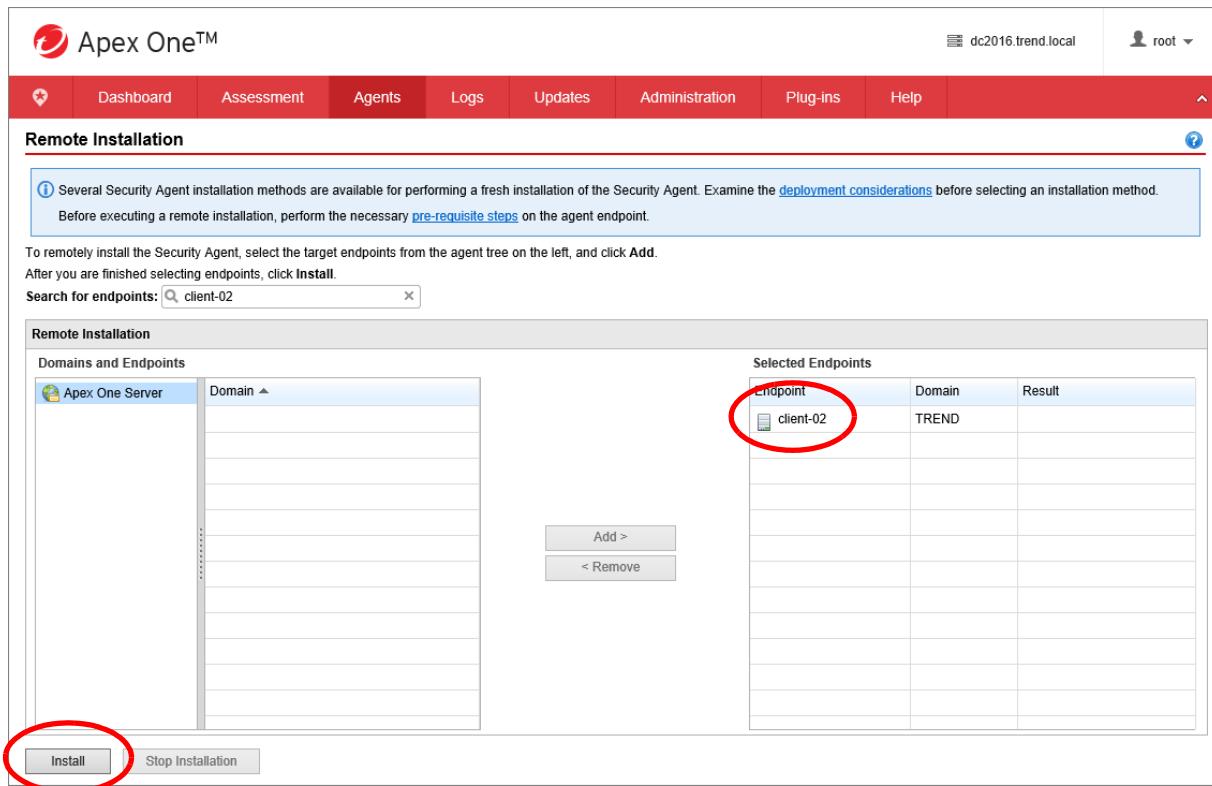
Remote Installation

This method installs a Security Agent remotely from the Apex One Server Web Management console page. This method can be used if the Apex One Server has been installed on one of the following platforms:

- Windows Server 2012 with IIS 8.0
- Windows Server 2012 R2 with IIS 8.5
- Windows Server 2016 with IIS 10
- Windows Server 2019 with IIS 10

Lesson 4: Managing Security Agents

The Agent can be installed from **Agents > Remote Installation** in the Apex One Web Management console.



The screenshot shows the Apex One Web Management interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The Agents link is highlighted. On the right, it shows the host name dc2016.trend.local and a user account root. Below the navigation bar, the title "Remote Installation" is displayed. A message box contains a note about available installation methods and prerequisites. The main area has two sections: "Domains and Endpoints" on the left and "Selected Endpoints" on the right. In the "Selected Endpoints" table, there is one entry: "client-02" under Endpoint, "TREND" under Domain, and an empty field under Result. Below these sections are buttons for "Add >" and "< Remove". At the bottom left, there are two buttons: "Install" (which is circled in red) and "Stop Installation".

Remote installation requires that **File and Printer Sharing** be excluded from the Windows Firewall and that the **Windows Remote Registry** service be running.

Note: Remote installation does not install the Security Agent on endpoints running an Apex One Server.

Unmanaged Endpoints

In an on-premises installation, Agent can be installed from **Assessment > Unmanaged Endpoints**. In this example, unmanaged endpoints in Active Directory will be displayed after using **Define Scope** and selecting a branch in the Directory tree.

Endpoint Name	Security Status	Apex One Server	Active Directory Tree
CLIENT-01	Unreachable		trend.local/Computers
CLIENT-02	No Security Agent installed		trend.local/Computers
CLIENT-03	No Security Agent installed		trend.local/Computers
WIN2012	No Security Agent installed		trend.local/Computers

To use **Unmanaged Endpoints**, ensure that the Apex One Server computer is part of the network and can query Active Directory domains or IP addresses. With this feature, administrators can check for computers with the following status:

- Security Agents within the network domains but managed by another Apex One Server
- Computers without Security Agents installed
- Unreachable computers that cannot connect to a specific checking port (the default port value is 135)
- Computers within the Active Directory domain but Apex One Server is unable to determine their security status

For the first two points listed above, Apex One Server attempts to connect to target Agents through port 135. It sends a request to the target machine, and the latter replies with a valid response.

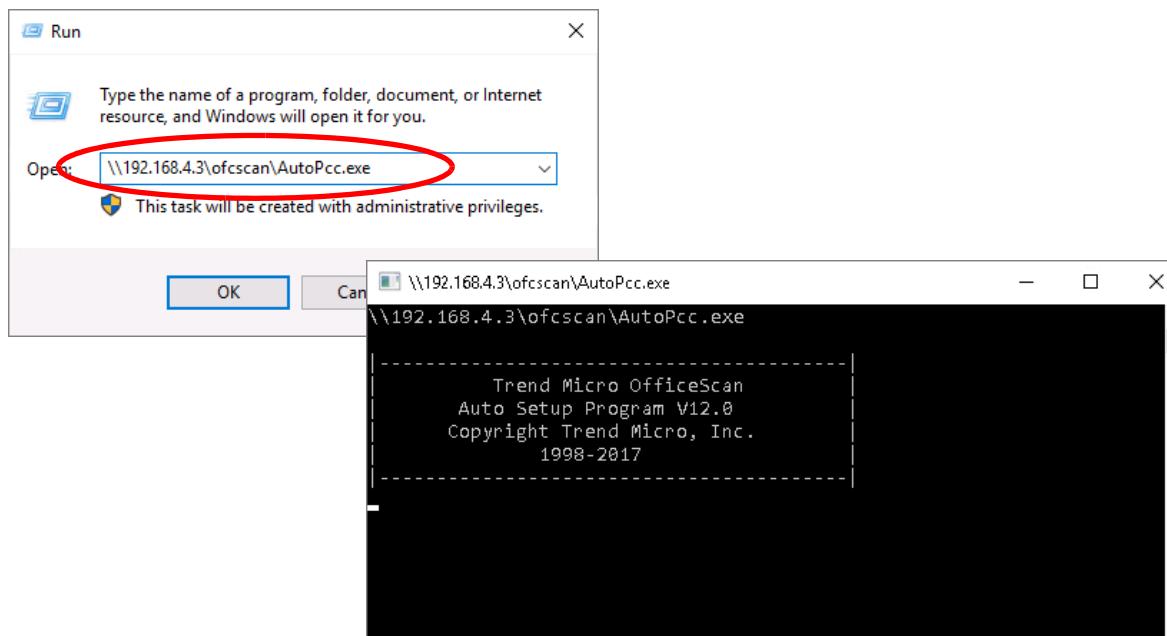
Installer Link

This method creates an email message that instructs users on the network to install the Security Agent by clicking the installer link provided in the email.

The screenshot shows the Apex One™ interface with a red navigation bar at the top. The main content area is titled "Email Link Installation". It contains a form with an "Email Properties" section. Under "Email subject", there is a text input field containing the URL "Please click the following URL to install Security Agent". Below the input field is a button labeled "Create Email", which is circled in red. At the bottom right of the form is a question mark icon.

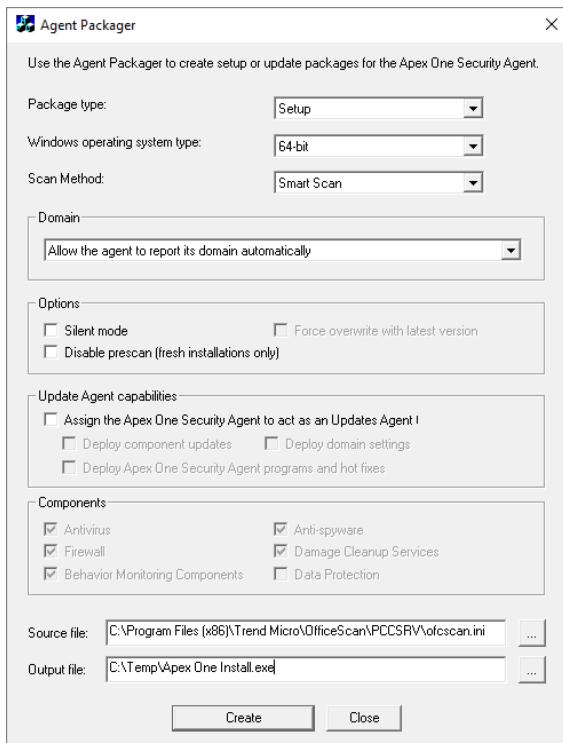
AutoPcc

This method uses a script to automate the installation of the Security Agent on unprotected computers. Endpoints must be part of the domain to be able to use AutoPcc using a Uniform Naming Convention (UNC) path.



Agent Packager

The Agent Packager utility (`clnpack.exe`) creates an installation package that you can send to users using conventional media such as CD-ROM or deployed using Microsoft SMS or Active Directory. Users run the packaged application on the Agent endpoint to install or upgrade the Security Agent and update components. Agent Packager is especially useful when deploying the Security Agent or components to Agents in low-bandwidth remote offices. Security Agents installed using Agent Packager report to the Server where the package was created.



An Agent package can also be downloaded from the Apex One Server login page, but the configuration options available are limited.

Microsoft System Center Configuration Manager or Active Directory Installation

An Security Agent MSI package created using the Agent Packager can be deployed using a Microsoft System Center Configuration Manager (SCCM) if you have Microsoft BackOffice installed on the Server. The SCCM Server needs to obtain the MSI file from the Apex One Server before it can deploy the package to target endpoints.

When Microsoft SCCM distributes the advertised program (that is, the Security Agent program) to target endpoints, a screen displays on each target endpoint. Instruct users to click **Yes** and follow the instructions provided by the wizard to install the Security Agent to their endpoints.

In addition, administrators can take advantage of Active Directory Group Policy features to deploy the MSI package simultaneously to multiple Agent endpoints.

Agent Disk Images

Disk imaging technology allows you to create an image of the Security Agent using disk imaging software and make clones of it on other computers on the network. Each Security Agent installation needs a Globally Unique Identifier (GUID) so that the Server can identify Agents individually. Use the Apex One program called `ImgSetup.exe` to create a different GUID for each of the clones.

Apex Central

The **Security Agent Download** page in the Apex Central Web Management console creates a Security Agent installation packages for Windows or Mac endpoint computers. You can use this page to download and install the Security Agent packages locally or to display a URL that you can send to users to install the Security Agent directly on a target endpoint.

SaaS: Downloading a Security Agent package from Apex Central is the only installation method available in the service implementation of Apex One. It is also the only method available to download a Security Agent for Mac package.

In the Apex Central Web Management console, click **Administration > Security Agent Download**.

The screenshot shows the 'Security Agent Download' section of the Trend Micro Apex Central interface. It includes fields for selecting the operating system (Windows 64-bit is selected), installation mode (Full feature set is selected), and package type (Standalone is selected). A note at the bottom states: 'To ensure that all Security Agents can properly communicate with the server, [configure prerequisite settings](#)'. Below the form are two buttons: 'Download Installer' (highlighted in blue) and 'Get Download Link'.

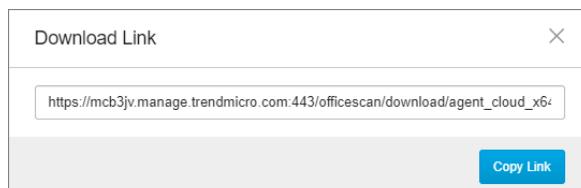
Select the operating system, installation mode, package type and click **Download Installer**. An installation package is downloaded:

- For Windows, a *.msi file is downloaded
- For Mac, a *.zip file is downloaded (this is the only method for creating a Mac Agent setup package)

The downloaded file is be distributed to end users using your preferred method.

A **Standalone** package can be copied to an endpoint computer and installed without an Internet connection as it contains all the required components. A **Web Installer** package, on the other hand, installs the Agent components from the Internet. It also checks for conflicting applications and verifies system requirements before downloading and installing the Security Agent.

Alternately, click **Download Link** to display a link to allow end users to download and install the installation package themselves through their Web browser. The link, which is unique for each operating system option, can be distributed to end users by email or other messaging method.



Note: Apex One must be available as a Managed Server in Apex Central for the Security Agent Download page to include the appropriate items.

Migrating From Other Endpoint Security Software

When you install the Security Agent on Windows, the installation program checks for any Trend Micro or third-party endpoint security software installed on the target endpoint. The installation program can automatically uninstall the software and replace it with the Security Agent.

For a list of endpoint security software that Apex One automatically uninstalls, open the `tmuninst.ptn` and `tmuninst_as.ptn` files in the `C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin` folder using a text editor such as Notepad.

If the software on the target endpoint is not included in the list, manually uninstall it first. Depending on the uninstallation process of the software, the endpoint may or may not need to restart after uninstallation.

SaaS: No administrator access to the `tmuninst.ptn` and `tmuninst_as.ptn` files is available in the service implementation of Apex One.

tmuninst_as.ptn

The `tmuninst_as.ptn` file contains uninstallation commands for Trend Micro security software that must be removed from the endpoint before installing the Security Agent. If an entry in the file exists for an application, the setup routine will be able to uninstall the application automatically.



The screenshot shows a Notepad window titled "tmuninst_as.ptn - Notepad". The window contains configuration scripts for Trend Micro Internet Security Pro. It includes sections for version 17, 16, and a general section for Trend Micro Internet Security Pro. Each section defines product keys, uninstall keys, platforms, unload programs, and support levels. The code uses square brackets to group sections and various parameters to specify the software's behavior during removal.

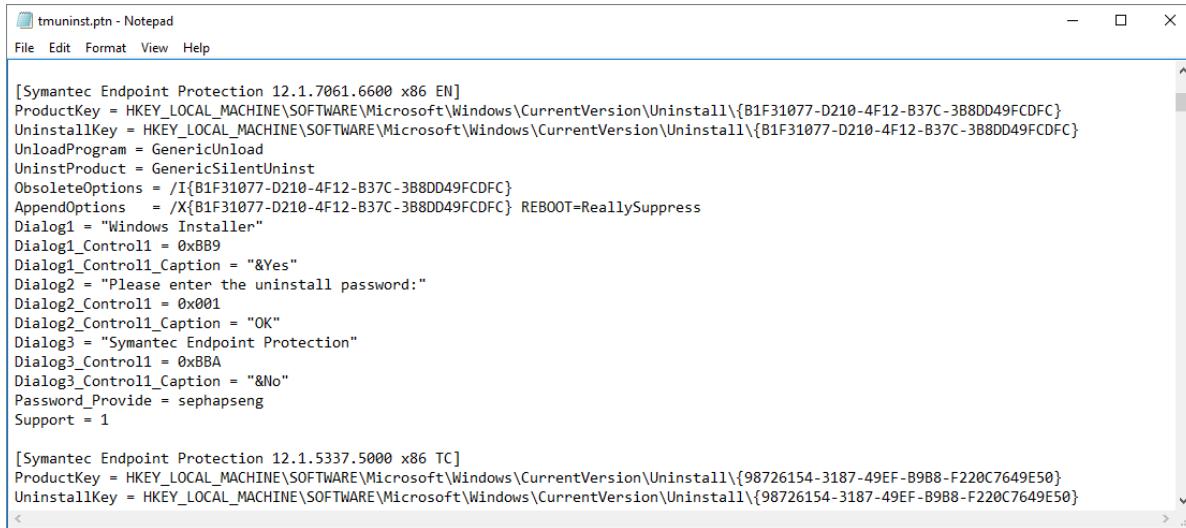
```
[Trend Micro Internet Security Pro 17]
ProductKey = HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillin
UninstallKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{40E12A55-C504-4223-AFAC-7672DBF1ACDE}
Platform = WinNT
UnloadProgram = GenericUnload
UninstProduct = UninstPCC2004
Support = 0
IsTrendProduct = 1

[Trend Micro Internet Security Pro 16]
ProductKey = HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillin
UninstallKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{A621B45A-D138-4A95-BE10-7CABA05EF94E}
Platform = WinNT
UnloadProgram = GenericUnload
UninstProduct = UninstPCC2004
Support = 0
IsTrendProduct = 1

[Trend Micro Internet Security Pro]
ProductKey = HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillin
UninstallKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{718D791F-F4E8-4aa7-98A6-15FDED17BDD0}
Platform = WinNT
UnloadProgram = GenericUnload
```

tmuninst.ptn

The `tmuninst.ptn` file contains uninstallation commands for third-party security software that must be removed from the endpoint before installing the Security Agent. If an entry in the file exists for an application, the setup routine will be able to uninstall the application automatically. If the application currently installed on the endpoint does not contain an entry in this file, the application must be manually removed through Control Panel before proceeding with the Agent setup.



```
[Symantec Endpoint Protection 12.1.7061.6600 x86 EN]
ProductKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B1F31077-D210-4F12-B37C-3B8DD49FCDFC}
UninstallKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{B1F31077-D210-4F12-B37C-3B8DD49FCDFC}
UnloadProgram = GenericUnload
UninstProduct = GenericSilentUninst
ObsoleteOptions = /I{B1F31077-D210-4F12-B37C-3B8DD49FCDFC}
AppendOptions = /X{B1F31077-D210-4F12-B37C-3B8DD49FCDFC} REBOOT=ReallySuppress
Dialog1 = "Windows Installer"
Dialog1_Control1 = 0xB89
Dialog1_Control1_Caption = "&Yes"
Dialog2 = "Please enter the uninstall password:"
Dialog2_Control1 = 0x001
Dialog2_Control1_Caption = "OK"
Dialog3 = "Symantec Endpoint Protection"
Dialog3_Control1 = 0xBB8
Dialog3_Control1_Caption = "&No"
Password_Provide = sephapseng
Support = 1

[Symantec Endpoint Protection 12.1.5337.5000 x86 TC]
ProductKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{98726154-3187-49EF-B9B8-F220C7649E50}
UninstallKey = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{98726154-3187-49EF-B9B8-F220C7649E50}
```

Coexist Mode

Though it is not a recommended implementation, the Apex One Security Agent can be installed on endpoints in **Coexist Mode**. This mode allows third-party anti-malware products to be used on the same endpoint as the Apex One Security Agent. In this implementation, Apex One provides some security features, like Application Control and Vulnerability Protection, while making use of the malware scanning capabilities of the other application.

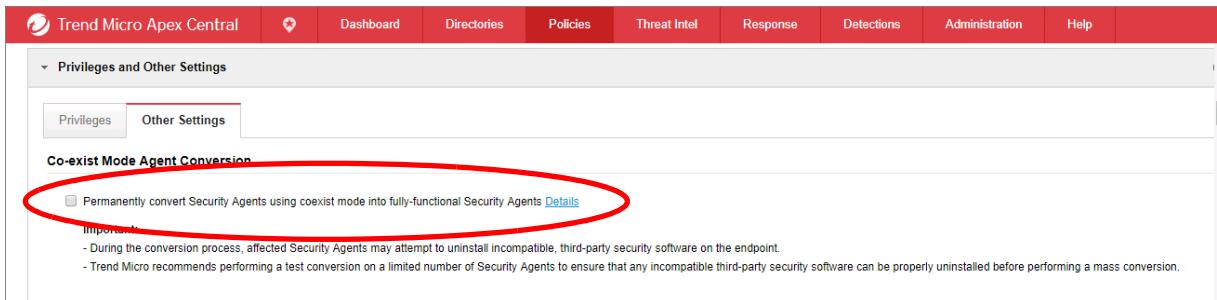
Anti-malware applications tested in co-exist mode include the following:

- Symantec Endpoint Protection 14
- Sophos Endpoint Security 10.6
- Kaspersky Security Center 10
- McAfee Endpoint Security 10.5
- Microsoft Defender / Microsoft Security Essentials

In coexist mode, Security Agents will not report their status to Windows Security Center. This is to keep other competitor applications running.

It is possible to upgrade Agents installed in **Coexist Mode** to full functionality through Apex Central. This process will also uninstall any non-Microsoft third-party security applications.

In Apex Central, create and deploy a policy to the Security Agent including the **Privileges and Other Settings** value of **Permanently Convert Security Agents using coexist mode into fully-functional Security Agents**.



The screenshot shows the Trend Micro Apex Central web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. Below the navigation bar, a sidebar on the left has a 'Privileges and Other Settings' section expanded. Under this section, the 'Other Settings' tab is active. In the main content area, there's a heading 'Co-exist Mode Agent Conversion' followed by a checkbox labeled 'Permanently convert Security Agents using coexist mode into fully-functional Security Agents'. A red oval surrounds this checkbox. Below the checkbox, there's a note with two bullet points: '- During the conversion process, affected Security Agents may attempt to uninstall incompatible, third-party security software on the endpoint.' and '- Trend Micro recommends performing a test conversion on a limited number of Security Agents to ensure that any incompatible third-party security software can be properly uninstalled before performing a mass conversion.'

Post Installation Tasks

Once the Security Agent is installed on the endpoint, the following tasks can be attempted to confirm its operation and update it to use the current malware patterns.

Component Updates

Update the Security Agent components to ensure that Agents have the most up-to-date protection against security risks. You can run manual Agent updates from the Web Management console or instruct users to run **Update Now** from their computers.

Test Scan using EICAR Test Script

The European Institute for Computer Antivirus Research (EICAR) developed the EICAR test script as a safe way to confirm proper installation and configuration of antivirus software. The EICAR web site is available at:

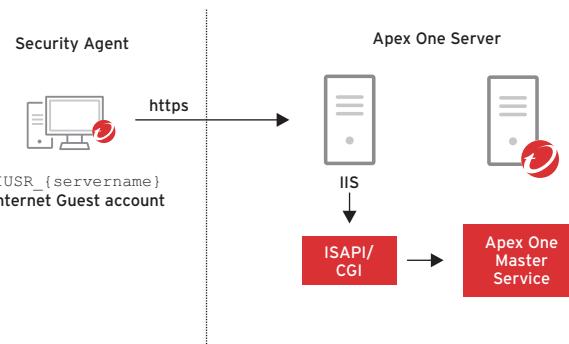
<http://www.eicar.org>

Installation Logs

The Security Agent installation log (ofcnt.log) exists in %windir% for all installation methods except MSI package installation and %temp% for the MSI package installation method.

Agent-To-Server Communication

Agents communicate with their Server by sending HTTPS messages to the Web Server on the Apex One Server and calling ISAPI/CGI commands. These commands invoke certain actions on the Server and the Server sends a corresponding answer to the Agent's request. These messages can be sent to the Server as a response to a Server notification. While doing this, they also pass information about the Agent, for example UID, computer name, program version, etc. These calls are processed by the Agent command handler, which checks if the Agent information is correct, complete and valid. If it is, the Server points the Agents to the location to download relevant files. Otherwise, the Server sends an error code to the Agents. You can configure Apex One to ensure that all communication between the Server and Agents are valid. Apex One provides public-key cryptography and enhanced encryption features to protect all communication between the Server and Agents.



Agent-to-Server (IIS) communication is performed using the `IUSR_{servername}` account (Internet Guest). This user account is essential for Apex One to function properly, so it must exist on the Server and have proper privileges (for example, privilege to run ISAPIs).

Web Server logs can be a useful source of troubleshooting information. In addition, to verify the Agent to Server communications, enter the following URL in Internet Explorer:

`https://<apexone_server>:port/officescan/cgi/cgionstart.exe`

If the number **-2** appears on the browser, then the Agent is able to communicate with the Server.

Note: Apex One moves the communication between Agents and the Server to HTTPS. By moving to HTTPS, the communication port on the Server will also change from the HTTP port (default of 8080) to the HTTPS port (same as the Web Management console, default of 4343).

Some environments may encounter HTTPS communication issues due to various factors (for example, inconsistent SSL/TLS environments, firewalls blocking the HTTPS port, etc.). This can result in agents showing offline, failing to upgrade, and not uploading logs or quarantined files.

Using HTTPS also creates the need for certificates and certificate validation. All Apex One Security Agents have their own self-signed certificate they use for communication and verification with the Apex One Server. This can be a problem in environments that deploy HTTPS Inspection gateways. With HTTPS Inspection, the Security Gateway can inspect the traffic that is encrypted by HTTPS.

The Security Gateway uses certificates and becomes an intermediary between the client computer and the secure website. This causes a problem as Apex One will not trust the Security Gateway's certificate. Thus, Apex One traffic must be excluded from HTTPS Inspection on Security Gateway products.

In some instances for compatibility or network inspection purposes, traffic can be reverted to HTTP.

Server-to-Agent Communication

When the Server initiates the action, it sends a TCP message to the Agent at the Agent port stored in the database. The default Agent communication port of 21112 is assigned, but can be modified during setup if necessary. The communication from Apex One Server to Agent (and vice-versa) is event driven. When specific events occur on the Agent or on the Server, an action may be triggered.

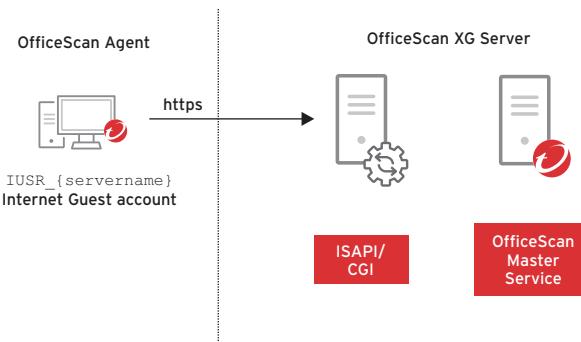
SaaS: Server-to-Agent communication is not available in the service implementation of Apex One; the service uses Agent-to-Server communication only.

Server-to-Agent communication is a four-step process. A simplified representation of how Apex One Servers and Agents communicate is illustrated here:

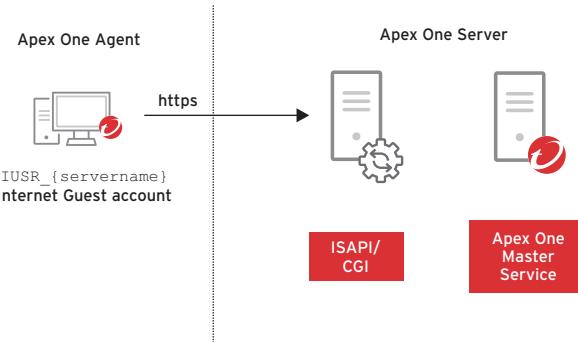
- 1 **Notification:** In this phase, the Apex One Server notifies the Security Agent to retrieve instructions from the Apex One Server.



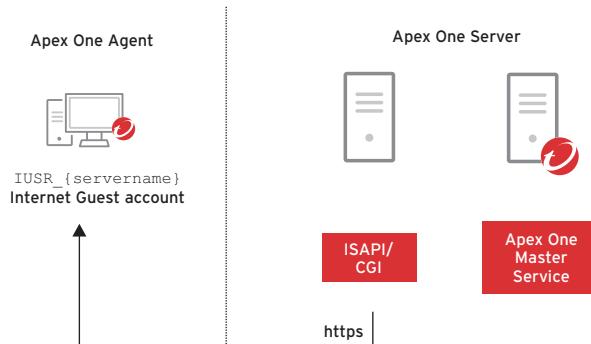
- 2 **Call ISAPI/CGI:** The Security Agent, specifically its TMListener component, responds to the notification in the previous phase by calling ISAPI/CGI applications on the Server. This phase actually involves calls to multiple ISAPI/CGI applications. The applications called depend on the type of command.



- 3 Server-side processing:** The ISAPI/CGI applications on the Server retrieve settings from the relevant Apex One information storage areas (for example, ofcscan.ini, Apex One database).



- 4 Response:** The Agent receives the required response from the ISAPI/CGI.



To optimize communication performance, the administrator can modify `ofcscan.ini`. The parameters related to Server performance are in the `[INI_SERVER_SECTION]`. Some of these parameters can also be easily reconfigured using the Server Tuner (`SvrTune.exe`) located following folder on the Server:

```
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility
```

Authenticating Server-Initiated Communications

Apex One uses two methods for authenticating Server-initiated communications:

- **Notification Authentication:** The Apex One Server signs the notification message before sending it out to the Agents. The Agent will accept or reject the notification depending on the results of the signature verification.
- **Data Authentication:** Data from the Apex One Server is authenticated and filtered by the Security Agent using a hash checking mechanism.

Notification Authentication

Apex One uses public-key cryptography to authenticate notifications from the Apex One Server to Security Agents. With public-key cryptography, the Server keeps a private key and deploys a public key certificate to all Agents. The Agents use the public key in the certificate to verify that incoming notifications are from the Apex One Server and they are valid. The Agents respond or carry out the instructions if the verification is successful.

Note: The Apex One Server does not authenticate communications from Security Agents.

During installation of the Apex One Server, the setup stores the public key certificate in the host computer's certificate store. Use the Authentication Certificate Manager tool to manage Trend Micro certificates and keys.

Before reinstalling the Apex One Server, ensure that you back up the existing certificate. After the new installation completes, import the backed up certificate to allow communication authentication between the Apex One Server and Security Agents to continue uninterrupted. If you create a new certificate during Server installation, Security Agents cannot authenticate Server communication because they are still using the old certificate (which no longer exists).

Data Authentication

Apex One uses the same keys and certificates for Data Authentication as it does for Notification Authentication. There are three types of data that the Agents may receive:

- **CGI/ISAPI:** When invoking a CGI or ISAPI, the Agent sends the serial number and issuer of the Certificate it has, plus a random salt value. The Server then appends the salt value to the result of the CGI/ISAPI and uses the private key associated with the Certificate to sign it. The Agent will then verify the signature with the Certificate and check the salt value before accepting the result.

If there is no issuer or serial number, the Server simply returns the content without providing any signature. If there is an issuer and a serial number but the Server does not have that Certificate, an HTTP 404 error is returned.

- **Program files:** When downloading a program file, the Agent creates an MD5 hash of the file and compares it to a hotfix table which has been downloaded at an earlier time and validated using the Static files authentication process.

- **Static files:** When downloading a static file, the Agent also downloads a signature file. The signature file has been created by the Apex One Server by taking a SHA-1 hash of the file, then signing this with each of the Server's private keys. Also included in the file is the Certificate serial number and issuer for the Certificates associated with each of those private keys. The Agent then verifies the appropriate signature with the Certificate it holds.

Support for third-party certificates

Apex One supports third-party signed authentication certificates given the following requirements:

- The import file must be in PFX format, which contains only one certificate
- The certificate must contain a signed key
- It must use either of the following algorithms:
 - Microsoft Enhanced Cryptographic Provider v1.0
 - Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
- The minimum key length of the certificate must be 1024 bits

SaaS: Support for third-party certificates is not available in the service implementation of Apex One.

Using a Single Key With Multiple Apex One Servers

When deciding on whether to use a single authentication key across all Apex One Servers, take note of the following:

- Implementing a single authentication key is a common practice for standard levels of security. This approach balances the security level of your organization with the overhead associated with maintaining multiple keys.
- Implementing multiple authentication keys across Apex One Servers provides a maximum level of security. This approach increases the maintenance required when certificates expire and need to be redistributed across the Servers and Agents.

Before reinstalling the Apex One Server, ensure that you back up the existing key and certificate. After the new installation completes, import the backed-up key and certificate to allow communication authentication between the Apex One Server and Security Agents to continue uninterrupted. If you create a new certificate during Server installation, Security Agents cannot authenticate Server communication because they would still be using the old certificate.

Heartbeat

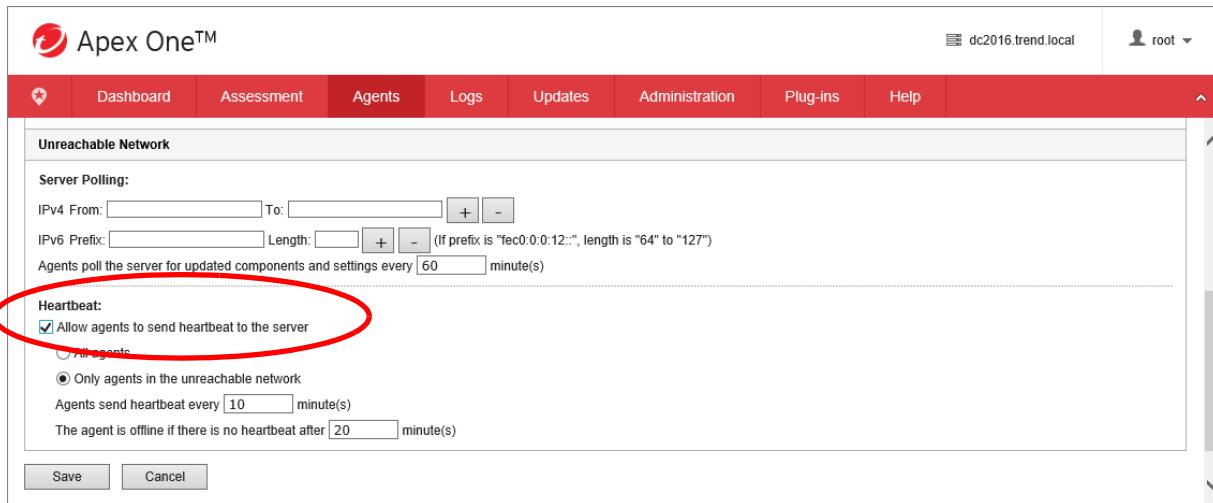
Heartbeats are real-time messages that Agents send to the Server over HTTP/TCP that indicates the connection from the Agent remains functional. It addresses the issue of Agents in unreachable networks always appearing as offline even when they can connect to the Server, for example, when behind a NAT firewall.

Lesson 4: Managing Security Agents

If the Server does not receive a heartbeat, it does not immediately treat the Agent as offline. These settings control the waiting time of the Server before changing an Agent's status to offline or unreachable/offline.

The Agent heartbeat status contains the last heartbeat sending status and new heartbeat sending status. By using these two values, the status handler can know if the Agent status is changed and only update the Agent status which has changed, instead of all unreachable Agents.

To configure the heartbeat period, click **Agents > Global Agent Settings > Network**. In the **Unreachable Networks** section, click **Allow Agents to send heartbeat to the server** and set the time period.



The screenshot shows the Apex One™ interface with the title bar "Apex One™" and user "root". The navigation menu includes Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The main content area is titled "Unreachable Network" under "Server Polling". It shows fields for IPv4 and IPv6 prefix ranges and a note about polling intervals. The "Heartbeat" section is highlighted with a red circle, containing a checked checkbox for "Allow agents to send heartbeat to the server" and a radio button for "Only agents in the unreachable network". Below these are fields for heartbeat frequency (10 minutes) and offline timeout (20 minutes). At the bottom are "Save" and "Cancel" buttons.

Server Polling

This feature is independent of the heartbeat feature and is related to updates polling regarding settings and components. The polling command from Agent to Server is another case of heartbeat sending.

SaaS: The heartbeat and server polling values are combined into one value in the service implementation of Apex One.

Agent Connection Status

The Security Agent connection status depends on the way in which the Apex One Server communicates with the Security Agent. The different connection statuses available for the Security Agent include:

Online

The Security Agent can connect to the Apex One Server for bi-directional communication of the following:

- Policy settings
- Updates
- Scan commands
- Suspicious Object list synchronization
- Sample submission
- Log submission

Offline

The Security Agent has no functional connection with the Apex One Server or an Edge Relay Server.

Independent

The Security Agent can connect to the on-premises Apex One Server but communication is limited. While in Independent mode:

- The Security Agent does not accept policy settings from the Server
- The Security Agent does not initiate scan commands from the Server
- The Security Agent does not send logs to the Server

You can configure Independent Agents with privileges to allow or block component updates if a functional connection to the Apex One Server is available.

End users can manually initiate scans and updates on Agents in Independent mode.

Off-premises

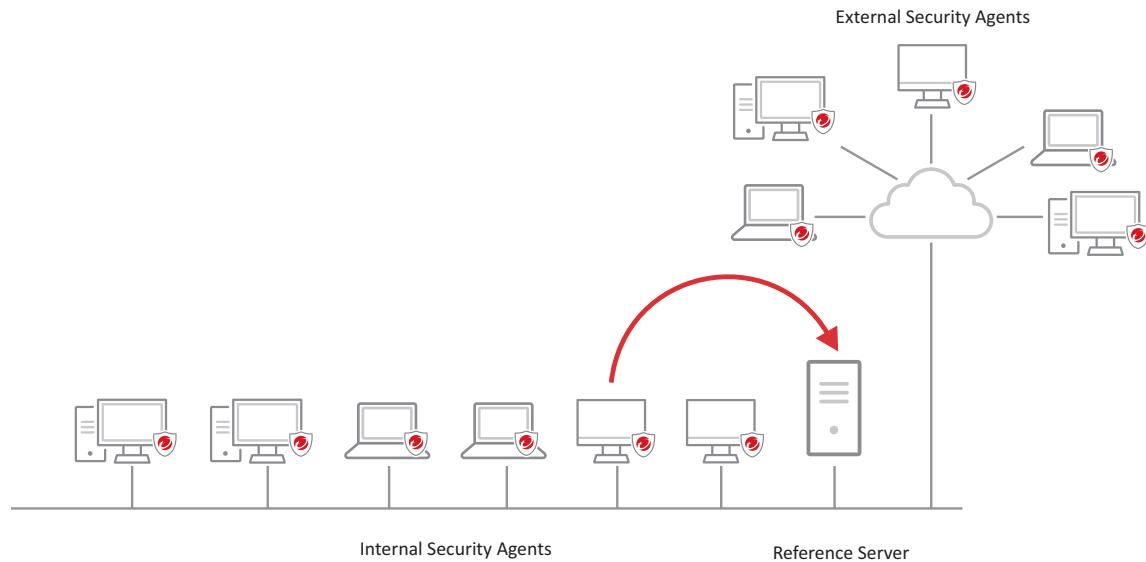
The Security Agent is outside of the corporate network and cannot connect to the on-premises Apex One Server directly. The Security Agent can, however, connect to an Edge Relay Server for the following:

- Suspicious Object list synchronization
- Sample submission
- Log submission

The Connection Status for an off-premises Agent displays as Offline in the Agent tree because the Apex One Server has no direct connection with the Security Agent.

Endpoint Location

One of the ways the Security Agent determines which policy or profile to use is by checking its connection status with a reference server. If a Security Agent can connect to the reference server, the internal policy is used. If a connection is not possible, the Agent then applies a policy or profile intended for external Agents.



Policies and profiles managed by reference servers include:

- Web reputation policies
- Data Protection policies
- Device Control policies
- Smart Protection sources

Reference Server List

Any Security Agent that loses connection with the Apex One Server will try connecting to reference servers using Telnet on a specified port. If the Agent successfully establishes connection with the reference server, it applies the policy or profile for internal Agents.

Security Agents connect to the first reference server on the list. If connection cannot be established, the Agent tries connecting to the next server on the list.

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.

Note: Reference servers do not manage Agents or deploy updates and Agent settings. The Apex One Server performs these tasks.

In the Apex One Web Management console, click **Agents > Endpoint Location** and click **Edit the Reference Servers** list. Click **Enable the reference server list** and click **Add** to add any Reference Servers by identifying the IP address, endpoint name or FQDN along with the port number.

Gateways

Alternately, Gateway IP addresses or MAC addresses can be used for endpoint location. Type the IP address of the Gateway and optionally, the MAC address and click **Add**. Multiple Gateway addresses can be added. The **Gateway Setting Importer** (GSImporter.exe) tool can be used to import a list of gateway IP addresses from a text file.

Excluding VPN Connections NEW

An enhancement for location awareness in Apex One will check the network adapter used to connect to the reference host and identify if the endpoint is internal or external.

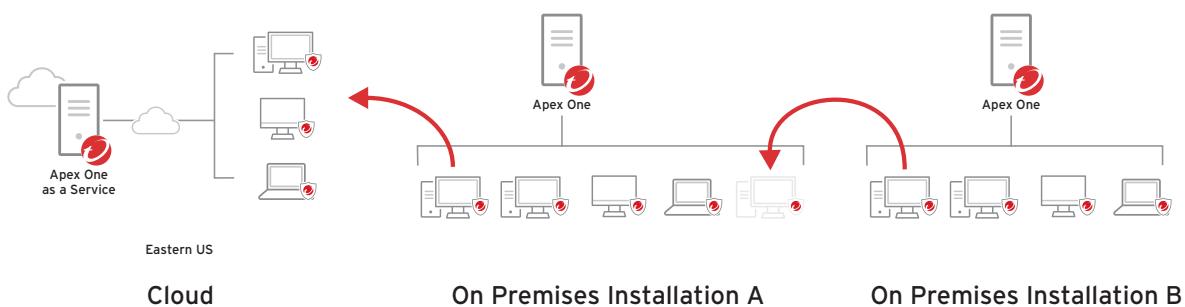
Previously, when an external Security Agent connects to the Apex One Server using VPN connection, it was referred as an internal agent and the related internal policy settings were

applied. VPN clients (Cisco, F5, Fortigate...) create a virtual network adapter as a network device to communicate with target network.

In Apex One, a new setting called **Exclude agents using VPN or PPP dial-up connections** is available. When enabled, Security Agents connected to the server using a VPN connection, they will be identified as an external Agent and apply corresponding configurations.

Moving Agents Between Apex One Servers

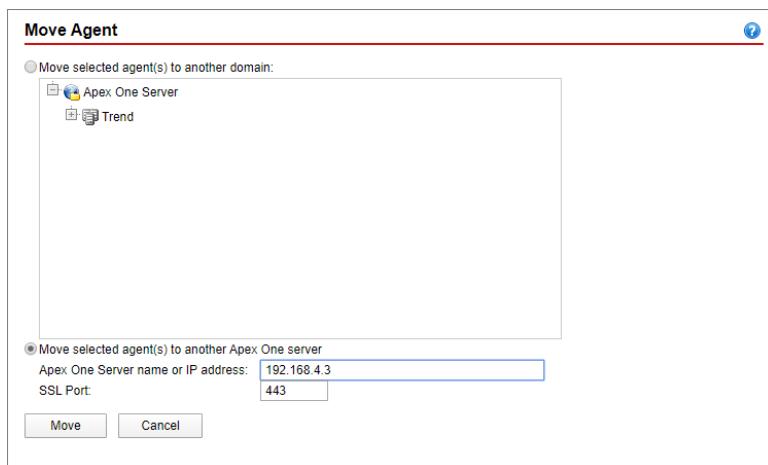
If you have more than one Apex One Server on the network, you can transfer existing Security Agents from one Apex One Server to another. Alternately, if you are transitioning from on-premises deployment of Apex One to the service, you can move Agents from the on-premises server to the Apex One as a Service server.



In the Apex One Web Management console, click **Agents > Agent Management**. Select the Security Agent to move and click **Manage Agent Tree > Move Agent**.

The screenshot shows the Trend Micro Apex One Web Management console. The top navigation bar includes links for Dashboard, Agents, Logs, Updates, Administration, and Help. The user is logged in as 'apex_one_training'. The main page title is 'Agent Management'. Below the title, a message says 'Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree.' There is a search bar labeled 'Search for endpoints:' and a link to 'Advanced search'. The central area features a table titled 'Agent tree view: View all'. The table has columns for Status, Domain/Endpoint, IP Address, Listening..., Domain H..., Connecti..., GUID, and Scan Met... . The table lists three agents under the 'Trend' domain: CLIENT-01, CLIENT-02, and CLIENT-03. The 'Move Agent' option is circled in red in the table. At the bottom of the table, there are statistics: 'Number of agents: 3', 'Agents using smart scan: 3', and 'Agents using conventional scan: 0'. The top right corner of the screen shows the server GUID: 491b6b96-9bd6-432b-84c5-abc5b0bb9d86.

Identify the details of the destination Apex One Server and click **Move**.



Agent Mover Tool

The Agent Mover tool (`IpXfer.exe`) can also be used to transfer Security Agents from one Apex One Server to another. The commands available with this tool can be used within scripts to move Agents, or if Agents don't move properly through the Web Management console. This tool is for moving Agent only and is not used for uninstalling or removing Agents from Apex One.

Note: Both Apex One Servers must be using the same language version. Also, if you are using Agent Mover to move an Security Agent running an **earlier** version of Apex One to a Server that is running the current version, the Security Agent will be upgraded automatically.

- 1 On the source Apex One Server, locate the following folder and copy the file `IpXfer.exe` to the Security Agent endpoint:
`C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\IpXfer`
If the Security Agent endpoint runs on 64-bit platform, copy `IpXfer_x64.exe` instead.
- 2 On the Security Agent endpoint, open a command prompt window and run `IpXfer.exe` with the following syntax:

```
IpXfer -s <server_name> -p <server_HTTP_listening_port>|-sp <server_HTTPS_listening_port> -c <agent_listening_port> -d <domain_or_domain_hierarchy> -e <Certificate_location_and_file_name> - pwd <agent_unload_and_unlock_privilege_password>
```

Parameter	Description
<executable file name>	<code>IpXfer.exe</code> or <code>IpXfer_x64.exe</code>
-s <server name>	The name of the destination Apex One Server.
-p <HTTP_server_listening_port>	The HTTP listening port (or trusted port) of the destination Apex One Server. To view the listening port on the Apex One Web Management console, click Administration > Settings > Agent Connection .
-sp <HTTPS_server_listening_port>	The HTTPS listening port (or trusted port) of the destination Apex One Server.

Parameter	Description
-c <Agent_listening_port>	The port number used by the Security Agent endpoint to communicate with the Server.
-d <domain_or_domain_hierarchy>	The Agent tree domain or group to which the Agent will be grouped.
-e <Certificate_location_and_file_name>	Imports a new authentication certificate for the Security Agent during the move process. If this parameter is not used, the Security Agent automatically retrieves the current authentication certificate from its new managing Server. NOTE: The default certificate location on the Apex One Server is: ... \PCCSRV\Pccnt\Common\OfcNTCer.dat. When using a certificate from a source other than Apex One, ensure that the certificate is in Distinguished Encoding Rules (DER) format.
-pwd <Agent_unload_and_unlock_privilege_password>	The unload and unlock privilege password configured in Privileges and Other Settings. If the unload and unlock password is required and you do not provide the password, Agent Mover prompts you before attempting to move Agents.

Examples:

```
ipXfer_64.exe -s Server01 -p 8080 -sp 4343 -c 21112 -d Workgroup -pwd unlock
```

3 To confirm whether the Security Agent is now reporting to the new Server:

- Go to the Security Agent endpoint.
- Right-click the Security Agent program icon in the system tray.
- Click **Component Versions**.
- Verify the Apex One Server that the Security Agent reports to by examining the **Server name/port** field.

Note: If the Security Agent does not appear in the Agent tree of the new Apex One Server managing it, try restarting the Master Service (`ofservice.exe`) on the destination Apex One Server.

Uninstalling Security Agents

Security Agents can be uninstalled from an endpoint computer using one of the following methods.

Uninstalling From the Web Management Console

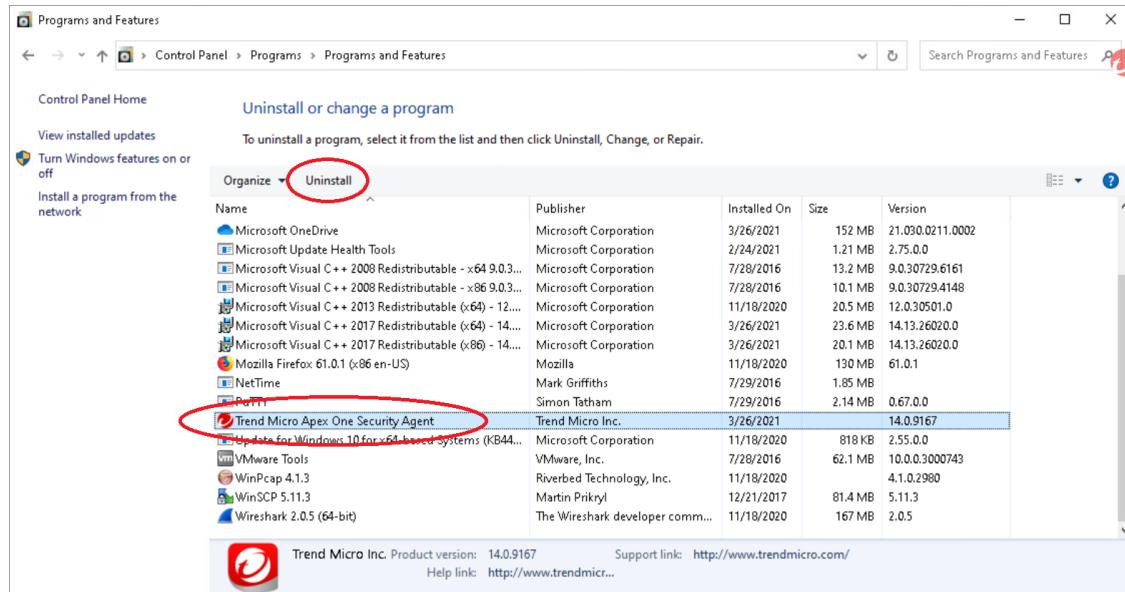
On the Agent Management menu, locate the endpoints for which the Agent will be uninstalled and click **Tasks > Agent Uninstallation**.

The screenshot shows the Apex One™ Web Management Console. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. On the right, it shows the server name 'dc2016.trend.local' and the user 'root'. Below the navigation bar is a section titled 'Agent Management' with a sub-instruction: 'Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree.' There's a search bar labeled 'Search for endpoints:' with an 'Advanced search' link. The main area is a table titled 'Agent tree view' with a 'View all' dropdown. The table has columns for Endpoint, Logon User, IP Address, Listening..., Domain H..., Connecti..., GUID, Scan Met..., and Resta...'. The table lists several endpoints, including 'Apex One Scan Now' (selected), 'Central Quarantine Restore', and 'Spyware/Grayware Restore'. The 'Apex One Scan Now' row has a 'Tasks' dropdown menu open, with 'Agent Uninstallation' highlighted and circled in red. At the bottom of the table, it says 'Number of agents: 5', 'Agents using smart scan: 5', and 'Agents using conventional scan: 0'.

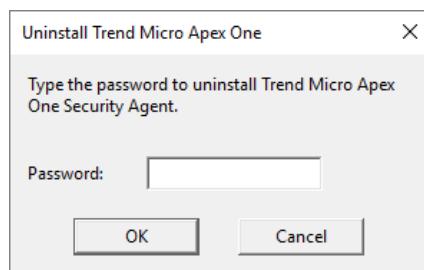
Uninstalling from Windows Control Panel

Users must be granted the privilege to uninstall the Security Agent program. Depending on your installation, users may be required to enter a password to perform the uninstall. If a password is required, ensure that you share the password only to users that will run the uninstallation program. Change the password immediately if it has been compromised.

In Windows Control Panel, select **Add or Remove Programs**. Locate **Trend Micro Security Agent** and click **Uninstall**.



If required by policy, authorization must be provided to complete the removal. The password for uninstalling the Agent was provided as part of the Apex One Server setup process.



Uninstalling Manually

If any problems are encountered using the above methods to uninstall the Security Agent, you can manually uninstall the Security Agent from a computer using the process described in the following article:

<https://success.trendmicro.com/solution/1039283-uninstalling-clients-or-Agents-in-officescan-osce>

Custom Uninstall Tool

If it is not possible to reinstall an Agent because there are still program entries in the Registry, Trend Micro Support can provide you with the Custom Uninstall Tool (CUT Tool). This time-limited tool (90 days) removes all trace of Apex One Security Agents from an endpoint.

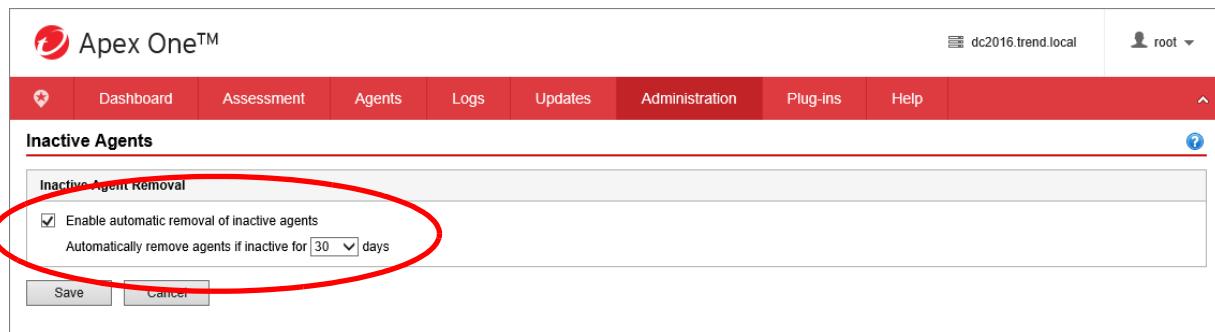
Removing Inactive Agents

When you use the Security Agent uninstallation program to remove the Security Agent program from endpoints, the program automatically notifies the Server. When the Server receives this notification, it removes the Security Agent icon in the Agent tree to show that the Agent does not exist anymore.

However, if you use other methods to remove the Security Agent, such as reformatting the endpoint hard drive or deleting the Security Agent files manually, Apex One will not be aware of the removal and it will display the Security Agent as offline. If a user unloads or disables the Security Agent for an extended period of time, the Server also displays the Security Agent as offline.

To have the Agent tree display active Agents only, configure Apex One to automatically remove inactive Agents from the Agent tree.

In the Apex One Web Management console, click **Administration > Settings > Inactive Agents**. Click **Enable automatic removal of inactive Agents** and select how many days should pass before Apex One considers the Security Agent inactive.

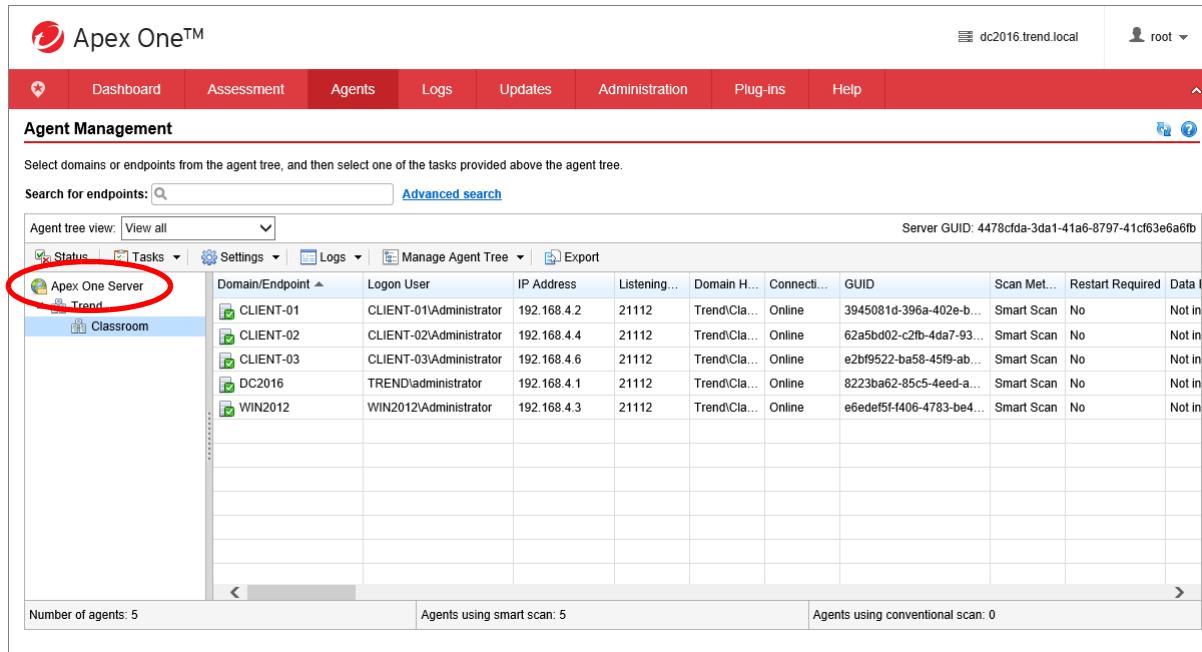


Security Agent Settings

Apex One administrators have the flexibility to apply security settings either to individual Agents or groups of Agents.

Root Settings

Settings at this control point define the global default. This is the only control point with the option to either overwrite all existing settings or define the settings for all future domains. Settings at this level are stored in the `ofcscan.ini`.



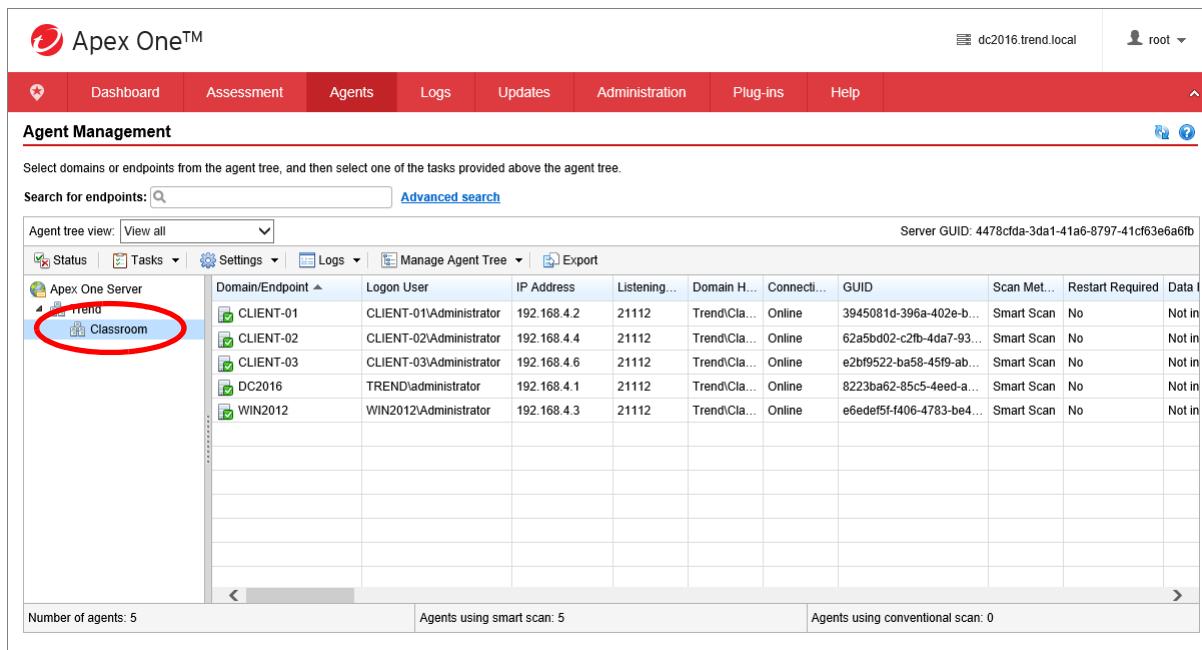
The screenshot shows the 'Agent Management' section of the Apex One™ web interface. The left sidebar displays a tree structure with 'Apex One Server' at the root, which has 'Trend' and 'Classroom' as children. The 'Trend' node is highlighted with a red circle. The main pane shows a table of agent details:

Domain/Endpoint	Logon User	IP Address	Listening...	Domain H...	Connecti...	GUID	Scan Met...	Restart Required	Data I...
CLIENT-01	CLIENT-01\Administrator	192.168.4.2	21112	Trend\Cla...	Online	3945081d-396a-402e-b...	Smart Scan	No	Not in...
CLIENT-02	CLIENT-02\Administrator	192.168.4.4	21112	Trend\Cla...	Online	62a5bd02-c2fb-4da7-93...	Smart Scan	No	Not in...
CLIENT-03	CLIENT-03\Administrator	192.168.4.6	21112	Trend\Cla...	Online	e2b9f522-ba58-45f9-ab...	Smart Scan	No	Not in...
DC2016	TREND\administrator	192.168.4.1	21112	Trend\Cla...	Online	8223ba62-85c5-4eed-a...	Smart Scan	No	Not in...
WIN2012	WIN2012\Administrator	192.168.4.3	21112	Trend\Cla...	Online	e6edef5f-f406-4783-be4...	Smart Scan	No	Not in...

At the bottom, there are summary counts: Number of agents: 5, Agents using smart scan: 5, and Agents using conventional scan: 0.

Domain Settings

These settings apply to all Agents in a particular domain. Agents automatically adopt domain settings when they join a domain. Settings at this level are stored in the Apex One Database.



This screenshot is identical to the one above, showing the 'Agent Management' interface. The 'Trend' node under 'Apex One Server' is highlighted with a red circle. The main pane displays the same table of agent details as the previous screenshot.

Agent Settings

Changes made at this control point apply to individual Agents. This allows administrators to customize settings for specific desktops. Settings at this level are stored in the Apex One Database.

The screenshot shows the 'Agent Management' section of the Apex One interface. At the top, there's a search bar for endpoints and a link to 'Advanced search'. Below that is a table with columns: Status, Tasks, Settings, Logs, Manage Agent Tree, and Export. The table lists several agents:

	Domain\Endpoint	Logon User	IP Address	Listening...	Domain H...	Connecti...	GUID	Scan Met...	Restart Required	Data I...
Apex One Server	CLIENT-01	CLIENT-01\Administrator	192.168.4.2	21112	Trend\Cla...	Online	3945081d-396a-402e-b...	Smart Scan	No	Not in...
Trend	CLIENT-02	CLIENT-02\Administrator	192.168.4.4	21112	Trend\Cla...	Online	62a5bd02-c2fb-4da7-93...	Smart Scan	No	Not in...
Classroom	CLIENT-03	CLIENT-03\Administrator	192.168.4.6	21112	Trend\Cla...	Online	e2bf9522-ba58-45f9-ab...	Smart Scan	No	Not in...
	DC2016	TREND\administrator	192.168.4.1	21112	Trend\Cla...	Online	8223ba62-85c5-4eed-a...	Smart Scan	No	Not in...
	WIN2012	WIN2012\Administrator	192.168.4.3	21112	Trend\Cla...	Online	e6edef5f-f406-4783-be4...	Smart Scan	No	Not in...

At the bottom, there are summary counts: Number of agents: 5, Agents using smart scan: 5, and Agents using conventional scan: 0.

Best Practice: Confusion can arise if settings are applied to many different endpoint computers at the Agent level. It is recommended that a new domain be created to assign settings to specific endpoints, instead of assigning them directly to the endpoints.

Agent Grouping

Agents in Apex One can be grouped to share the same configuration and run the same tasks. By grouping Agents into groups (referred to in Officescan as *domains*), you can configure, manage, and apply the same configuration to all domain members. There are two Agent grouping methods that can be used: manual and automatic.

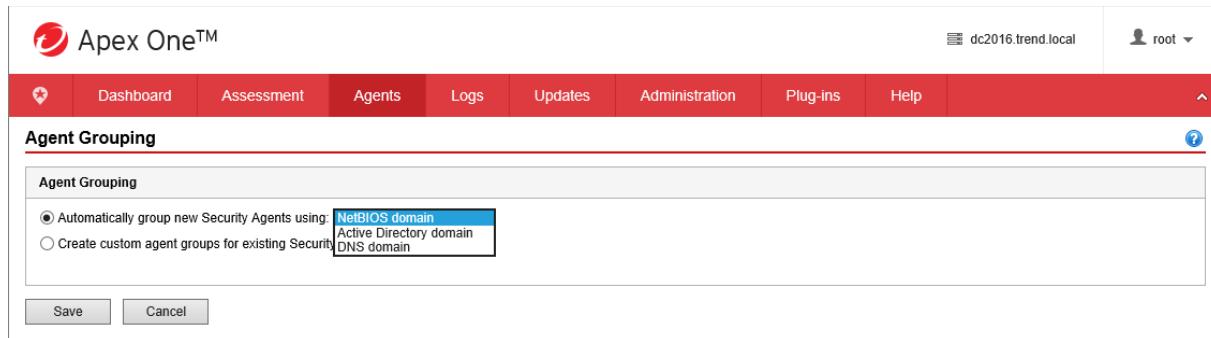
Manual Grouping

An Apex One Server uses this setting only during fresh Agent installations.

The installation program checks the network domain to which a target endpoint belongs. If the domain name already exists in the Agent tree, Apex One groups the Agent on the target endpoint under that domain and will apply the settings configured for the domain. If the domain name does not exist, Apex One adds the domain to the Agent tree, groups the Agent under that domain, and then applies the root settings to the domain and Agent.

Once the Agent appears in the Agent tree, it can be manually moved to another domain or to another Apex One Server. Manual Agent grouping includes the creation, management, and removal of domains in the Agent tree.

Manual Agent grouping defines the domain to which a newly installed Agent should belong, for example NetBIOS domain, Active Directory domain or DNS domain.



The screenshot shows the Apex One™ web interface with a red header bar containing links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The top right corner shows the server name 'dc2016.trend.local' and the user 'root'. Below the header is a navigation menu with 'Agent Grouping' selected. The main content area displays two options for automatic grouping: 'Automatically group new Security Agents using' (radio button selected) and 'Create custom agent groups for existing Security Agents' (checkbox). The 'NetBIOS domain' option is highlighted with a blue box. At the bottom are 'Save' and 'Cancel' buttons.

Automatic Grouping

Automatic (or Custom) grouping uses rules to sort Agents in the Agent tree. Once the rules are in place, Agents can be sorted manually or automatically into custom Agent groups when specific events occur or at scheduled intervals.

SaaS: Automatic grouping operations are not available in the service implementation of Apex One.

Automatic Agent grouping uses rules defined by IP addresses or Active Directory domains. If a rule defines an IP address or an IP address range, the Apex One Server will group Agents with a matching IP address to a specific domain in the Agent tree. Similarly, if a rule defines one or several Active

Directory domains, the Apex One Server will group Agents belonging to a particular Active Directory domain to a specific domain in the Agent tree.

The screenshot shows the Apex One™ web interface. The top navigation bar includes links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plugins, and Help. The user is logged in as 'root'. The main content area is titled 'Agent Grouping' and contains two sections: 'Automatic Agent Grouping' and 'IP Address Grouping'. In the 'Automatic Agent Grouping' section, there is a table with one row named 'Classroom'. The 'IP Address Grouping' section is currently active, showing a configuration dialog. The dialog has a checked checkbox for 'Enable grouping'. Under 'Define Grouping', the name is set to 'Classroom'. The 'IP address source' section contains three options: 'Single IPv4/IPv6' (unchecked), 'IPv4 range' (selected), and 'IPv6' (unchecked). For 'IPv4 range', 'From:' is set to '192.168.4.1' and 'To:' is set to '192.168.4.10'. Below these fields is a note: '(If prefix is "fec0:0:0:12::", length is "64" to "127")'. The 'Agent tree' section shows a tree structure with 'Apex One Server' expanded, showing 'Trend' as a child node. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

The Apex One Server groups Agents accordingly when the following events are triggered:

- The Agent registers to the Server for the first time
- The Agent connection status changes from offline to online
- The Agent IP address changes
- The Agent reloads

Grouping may also be done using the Sort Client command.

Note: If Agents match multiple rules during the grouping operation, the first matched rule will be applied. If no rules are matched during the grouping operation, the Agents are placed into a group called **Default**.

Lesson 4: Managing Security Agents

Scheduled domain sorting and creation is disabled by default. Administrators can use the **Scheduled Domain Creation** settings on Agent Grouping window to set the time and frequency for this task.

The screenshot shows the Apex One™ web interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root' on 'dc2016.trend.local'. The main content area is titled 'Agent Grouping'. It has two main sections: 'Agent Grouping' and 'Automatic Agent Grouping'. Under 'Automatic Agent Grouping', there's a table with one row named 'Classroom'. The 'Status' column shows a toggle switch set to 'On'. Below these sections is the 'Scheduled Domain Creation' section, which is circled in red. This section contains a checkbox for 'Enable scheduled domain creation' (which is checked), and three radio button options for frequency: 'Daily', 'Weekly, every [Monday dropdown]', and 'Monthly, on day [01 dropdown]'. There are also dropdowns for 'Start time' (set to 00:00) and a note '(hh:mm)'. At the bottom of this section are 'Save', 'Cancel', and 'Save and Create Domain Now' buttons, along with a timestamp 'Last updated: 2/13/2019 00:35:35'.

The sorting rule or automatic Agent grouping criteria are stored in:

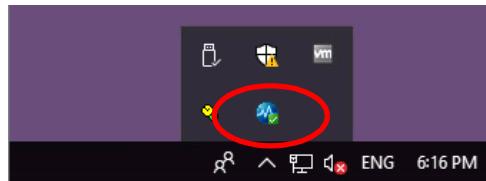
C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Private\SortingRuleStore\SortingRule.xml

Viewing Agent Status

Administrators can view the status of Agents from the Apex One Web Management console or directly on the endpoint computer.

Viewing Agent Status on the Endpoint

An icon in the Windows System Tray display the status of the Security Agents and their connection to the SmartScan Server.



Some examples of the different status icons are displayed in the table below:

Icon	Connection with Apex One Server	Availability of Smart Protection Source	Real Time Scan
	Online	Available	Enabled
	Online	Unavailable/ Reconnecting	Enabled
	Offline	Available	Enabled
	Offline	Unavailable/ Reconnecting	Enabled
	Online	Available	Service not running
	Online	Available	Manually disabled

Viewing Agent Status in the Web Management Console

Administrators can view the status of the Agent from the Agents list in the Web Management Console.

GUID:	62a5bd02-c2fb-4da7-9309-202e728995d2
Scan method:	Smart scan
Connection status:	Online
File Reputation Services status:	Available
File Reputation Services URL:	http://dc2016.trend.local:8080/tmcss/
Web Reputation Services status:	Available
Web Reputation Services URL:	http://dc2016.trend.local:8080/
Virus/Malware detected:	0
Spyware/Grayware detected:	0
Outbreak prevention policy:	Disabled
Restart required:	No
Data Protection status:	Not installed
Platform:	Windows 10 10.0.16299
Architecture:	x64
IP address:	192.168.4.4
MAC address:	00-50-56-02-2A-F7
Domain:	Trend\Classroom
Grouping:	Classroom
Port:	21112

Agent Self Protection

The protection that Apex One offers depends entirely on the ability of the Security Agent to implement authentic Apex One Server settings. The Agent, therefore, must be protected from all unauthorized attempts to change settings, which are all stored in the Windows Registry, and to disrupt its services. Unauthorized Change Prevention is responsible for evaluating system access events like file I/O and prevents unauthorized changes to registry keys and processes.

Security Agents maintain two layers of protection for its settings:

- **Change prevention:** This is a proactive defense measure. It is aimed at blocking unauthorized changes from happening in the first place.
- **Security Agent service restart:** Apex One restarts Agent services that stopped responding unexpectedly and were not stopped by a normal system process.

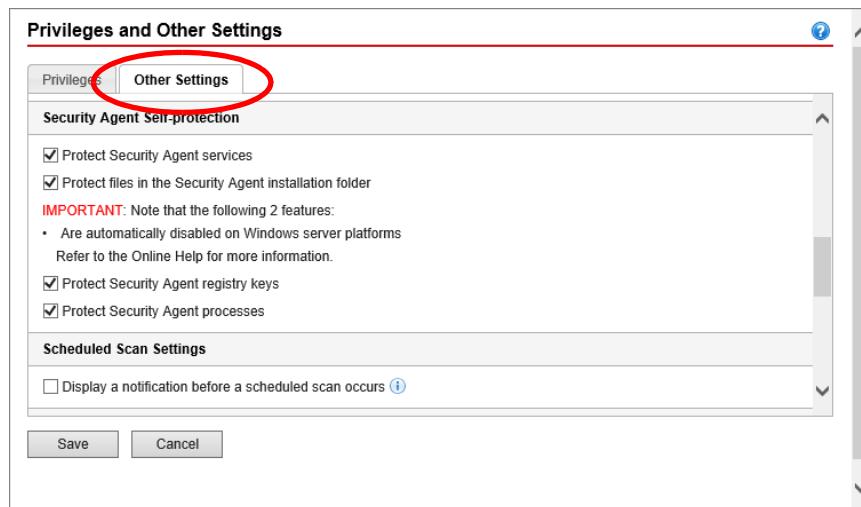
Configuring Unauthorized Change Prevention

Apex One protects Agent components and settings using the Unauthorized Change Prevention Service. This service is responsible for protecting Security Agents from changes other than those made through either the Apex One Server or Agent consoles.

The service appears in the Windows Service Control. The service itself is responsible for evaluating system access events (for example, file I/O, registry access, etc.) based on event-handling policies, and then taking action upon these events in accordance with the relevant policies (for example, prevent the change, block access, etc.)

When the options to protect registry keys and services are enabled in the Apex One Web management console, the NT Real-time Scan mechanism passes the relevant policy information to the Unauthorized Change Prevention Service, which then converts the information into policies that it implements.

To configure the **Security Agent Self-Protection**, click **Agent > Agent Management**. Select the appropriate domain, group or individual Agent from list and click **Settings > Privileges and Other Settings**. Click the **Other Settings** tab,



- **Protect Security Agent services:** Apex One blocks all attempts to terminate the following Security Agent services:
 - Apex One NT Listener (`TmListen.exe`)
 - Apex One NT RealTime Scan (`NTRtScan.exe`)
 - Apex One NT Firewall (`TmPfw.exe`)
 - Apex One Data Protection Service (`dsAgent.exe`)
 - Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)

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.

- Trend Micro Common Client Solution Framework (`TmCCSF.exe`)

- **Protect files in the Security Agent installation folder:** To prevent other programs and even the user from modifying or deleting Security Agent files, Apex One provides several enhanced protection capabilities. After enabling **Protect files in the Security Agent installation folder**, Apex One locks the following files in the root Agent installation folder:
 - All digitally-signed files with .exe, .dll, and .sys extensions
 - Some files without digital signatures, including:
 - bspatch.exe
 - bzip2.exe
 - NETWH32.dll
 - libcurl.dll
 - libeay32.dll
 - libMsgUtilExt.mt.dll
 - msvcm80.dll
 - MSVCP60.DLL
 - msycop80.dll
 - msocr80.dll
 - OfceSCV.dll
 - OFCESCPack.exe
 - patchbld.dll
 - patchw32.dll
 - patchw64.dll
 - PiReg.exe
 - ssleay32.dll
 - Tmeng.dll
 - TMNotify.dll
 - zlibwapi.dll

After enabling **Protect files in the Security Agent installation folder** and Real-time Scan for virus/malware threats, Apex One performs the following actions:

- **File integrity checking before launching .exe files in the installation folder:** During ActiveUpdate updates, Apex One verifies that the issuer of the file triggering the update is Trend Micro. If the issuer is not recognized as Trend Micro and ActiveUpdate cannot replace the incorrect file, Apex One logs the incident in the Windows event logs and blocks the update.
- **Prevents DLL hijacking:** Some malware writers copy dynamic link library files to the Security Agent installation folder or the Behavior Monitoring folder with the purpose of loading these files before the Agent loads. These files attempt to disrupt the protection offered by Apex One. To prevent the copying of hijacked files to the Security Agent folders, Apex One prevents the copying of files to the installation folder and Behavior Monitoring folder.

- **Protect Security Agent registry keys:** The Security Agent blocks all attempts to modify, delete, or add new entries under the following registry keys and subkeys:
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP
- **Protect Security Agent processes:** The Security Agent blocks all attempts to terminate the following processes:
 - TmListen.exe: Receives commands and notifications from the Apex One server and facilitates communication from the Security Agent to the server
 - NTRtScan.exe: Performs Real-time, Scheduled, and Manual Scan on Security Agents
 - TmProxy.exe: Scans network traffic before passing it to the target application
 - TmPfw.exe: Provides packet level firewall, network virus scanning, and intrusion detection capabilities
 - TMBMSRV.exe: Regulates access to external storage devices and prevents unauthorized changes to registry keys and processes

Kernel Mode Termination Protection

Change Prevention blocks user mode termination events but there are some applications that could potentially terminate processes through kernel mode. To address this issue, Apex One introduces a new Watchdog mechanism for kernel mode termination events. This mechanism will attempt to recover target processes after being terminated.

When the Security Agent is started, services will monitor processes on the endpoint. If the endpoint receives a terminate event, it will call Watchdog which checks if the process is still alive. If the process is not running, it will recover the service. Watchdog is dependent on Agent Self-Protection. Ensure that Security Agent Self-Protection is enabled to use this feature.

Security Agent Service Restart

Apex One restarts Agent services that stopped responding unexpectedly and were not stopped by a normal system process.

Lesson 4: Managing Security Agents

To configure the necessary settings to enable Security Agent services to restart, go to **Agents > Global Agent Settings** and on the **System** tab, go to the **Services Restart** section. Click **Automatically restart any Security Agent service if the service terminates unexpectedly**.

The screenshot shows the Apex One™ interface with the title bar "Apex One™" and user "root". The navigation bar includes Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The main content area has a header "Smart Protection Service Proxy" with a checkbox for "Use configured Smart Protection Sources for service queries". Below it is a note about Predictive Machine Learning and Behavior Monitoring. A note states: "Note: If a supported Smart Protection Server is not available for service proxy queries, agents send query requests directly to the Trend Micro Smart Protection Network." The "Updates" section contains a checkbox for "Download only the pattern files from the ActiveUpdate server when performing updates" and a dropdown for "Reserve [60] MB of disk space for updates". The "Services Restart" section is circled in red and contains a checkbox for "Automatically restart any Security Agent service if the service terminates unexpectedly". It includes fields for "Restart the service after [1] minute(s)", "If the first attempt to restart the service is unsuccessful, retry [2] times", and "Reset the unsuccessful restart count after [1] hour(s)". At the bottom are "Save" and "Cancel" buttons.

- **Restart the service after __ minutes:** Specify the amount of time (in number of minutes) that must elapse before Apex One restarts a service.
- **If the first attempt to restart the service is unsuccessful, retry __ times:** Specify the maximum retry attempts for restarting a service. Manually restart a service if it remains stopped after the maximum retry attempts.
- **Reset the unsuccessful restart count after__ hour(s):** If a service remains stopped after exhausting the maximum retry attempts, Apex One waits a certain number of hours to reset the failure count. If a service remains stopped after the number of hours elapses, Apex One restarts the service.

Agent Privileges

Modify privileges to grant users the ability to modify certain settings and perform high level tasks on the Security Agent. To grant privileges, click **Agents > Agent Management**. In the Agent tree, click the root domain icon to include all Agents or select specific domains or Agents. Click **Settings > Privileges and Other Settings**.

Privileges and Other Settings

Privileges Other Settings

Independent Mode

Enable Independent mode

Scans

Allow users to do the following:

Configure Manual Scan settings
 Configure Real-time Scan settings
 Configure Scheduled Scan settings

Scheduled Scans

Allow users to do the following:

Postpone Scheduled Scan
 Skip and stop Scheduled Scan

Firewall

Display the Firewall settings on the OfficeScan agent console

Allow users to enable/disable the firewall, Intrusion Detection System, and the firewall violation notification message
 Allow OfficeScan agents to send firewall logs to the OfficeScan server (i)

Behavior Monitoring

Display the Behavior Monitoring settings on the OfficeScan agent console

Trusted Program List

Display the Trusted Program List on the OfficeScan agent console

Mail Scan

Display the Mail Scan settings on the OfficeScan agent console (i)

Proxy Settings

Allow users to configure proxy settings (i)

Component Updates

Allow users to do the following:

Perform "Update Now"
 Enable/Disable schedule-based updates (i)

Unload and Unlock

Unloading the OfficeScan agent and unlocking advanced agent settings:

Does not require a password
 Requires a password:
Password:
Confirm password:

Uninstallation

Uninstalling the OfficeScan agent:

Does not require a password
 Requires a password:
Password:
Confirm password:

Lesson 5: Managing Off-premises Agents

Lesson Objectives:

After completing this lesson, participants will be able to:

- Define the responsibilities of the Apex One Edge Relay Server
- Install the Apex One Edge Relay Server
- Register the Apex One Edge Relay Server with the Apex One Server

Off-premises management of Security Agents is made possible through the Apex One Edge Relay Server. This allows administrative users to maintain visibility of roaming Agents (for example, traveling users) even when they are not using a VPN to connect into their corporate network.

SaaS: The Apex One Edge Relay Server is not required in the service implementation of Apex One. Information in this lesson applies exclusively to the on-premises implementation of Apex One.

The Edge Relay Server acts as a reverse proxy between off-premises Agents and the Apex One Server allowing these Agents to sync data with the Apex One Server. The architecture of the Edge Relay Server in Apex One has been updated to forward all Agent requests to the Apex One Server, including configuration and policy details. The location for the Edge Server can be anywhere (in the DMZ network, cloud, etc.), as long as:

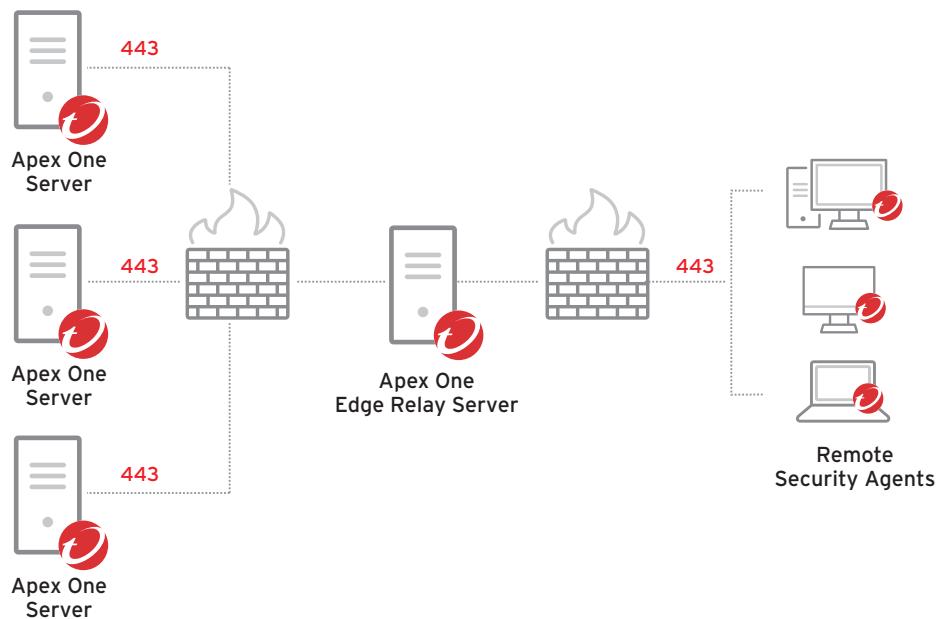
- It is publicly available to the Agent
- The Apex One Server can reach it

After configuring the Edge Relay Server, Security Agents receive settings and automatically report to the Edge Relay Server once a connection to the Apex One Server is unavailable.

Communication between the Edge Relay Server, Apex One Server, and Security Agents is secured using https encrypted communication.

One Apex One Edge Relay Server can support multiple Apex One Servers and its external Agents however, an Apex One Server can register to ONLY one Apex One Edge Relay Server.

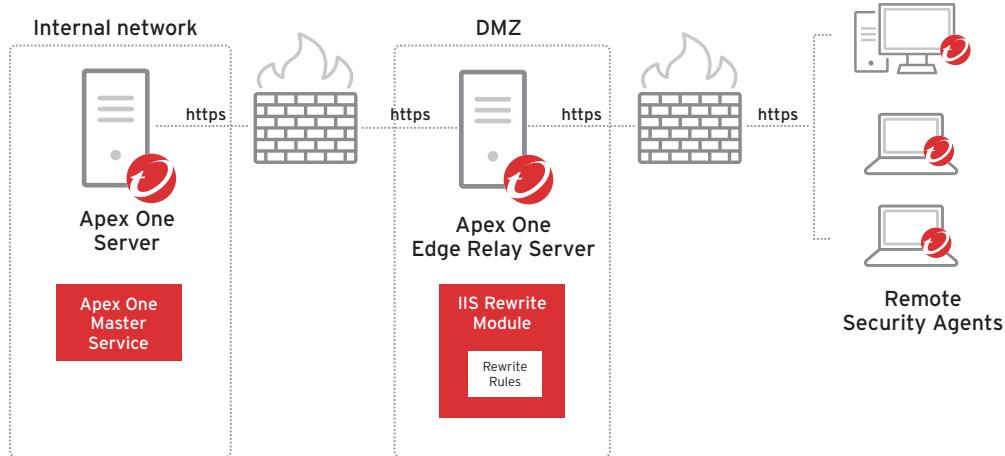
Note: Previous versions of the Edge Relay Server provided limited Security Agent protection features. The version of the Edge Relay Server provided with Apex One now enables full Security Agent capabilities to remote Agents, including configuration settings.



Edge Relay Server and External Agent Communications

Security Agents will feedback data to the Apex One Edge Relay Server, provided that the following conditions are met:

- Location is set to **out of office**
- The Agent has the Edge Relay Server information and certificate is in the Agent's registry key.



The IIS Rewrite Module, installed as a component of the IIS Web Server on the Edge Relay Server, serves as a reverse proxy to forward requests from Security Agents on the Internet to the Apex One Server on the internal network. The IIS Rewrite Module will replace the Server and port details received from the remote Agents with the Server and port details of the Apex One Server. The Edge Relay Server then forwards the request to the URL of the Apex One Server.

Installing the Apex One Edge Relay Server

Before installing the Edge Relay Server, ensure that the target server computer meets the minimum system requirements.

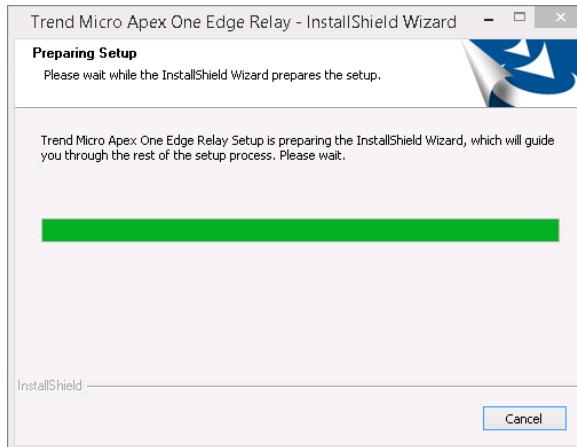
Resource	Requirements
Processor	2GHz Dual Core
Memory	512 MB minimum
Disk space	110 MB
Operating system	<ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 R2
Web Server	Microsoft Internet Information Server (IIS)
Network card	Network card configured to use different ports for intranet and Internet connections
Database	The version of the Edge Relay Server used with Apex One no longer requires a database

Note: The Edge Relay Server does not require two separate network interfaces as the same network interface can be used for internal and external communications as different ports are used internally and externally. However, if required for other purposes, having two network interfaces on the same machine as the Edge Relay Server is supported.

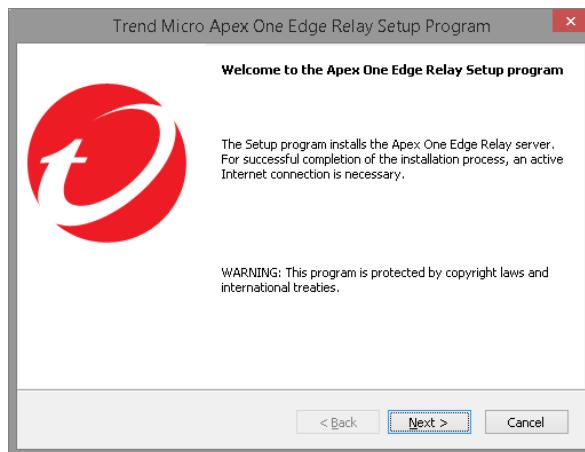
To install the Edge Relay Server, perform the following steps:

- 1 Locate the following folder on the Apex One Server computer, and copy the folder to the target Edge Relay Server computer:
`C:\Program Files (x86)\Trend Micro\Apex PCCSRV\Admin\Utility\EdgeServer\EdgeServer`
- 2 On the target Edge Relay Server, open the \EdgeServer folder and double-click `setup.exe` to start the setup process.

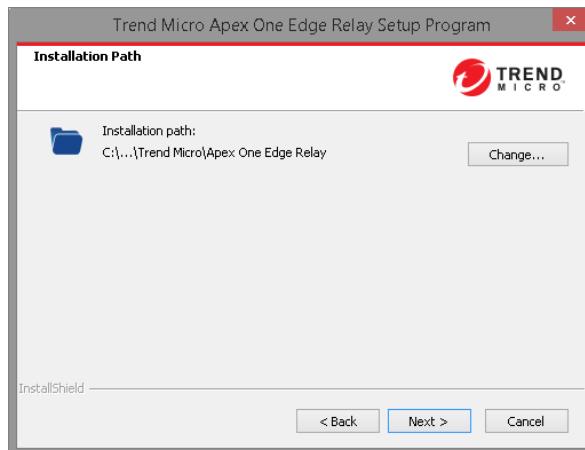
- 3 The setup package checks the server for required components. If any of the required Windows components do not exist on the server, click **Install** to allow the setup program to install the missing components during the Edge Relay Server installation process.



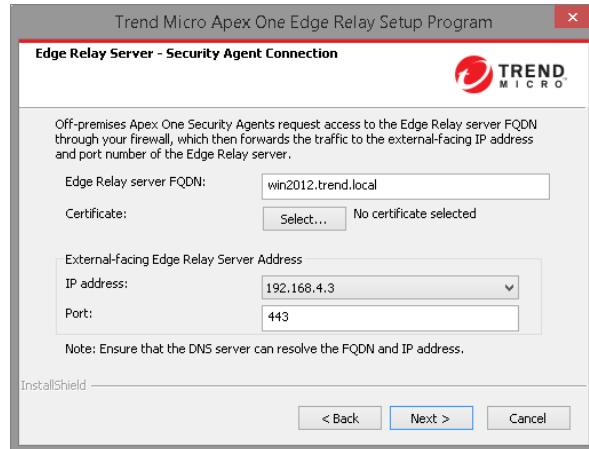
- 4 The Welcome screen is displayed. Click **Next**.



- 5 Accept the default installation directory or click **Change...** to select a different location and click **Next**.



- 6 Specify the following settings that off-premises Security Agents use to connect to the Edge Relay Server and click **Next**:



- Fully qualified domain name (FQDN)
- Certificate
- IP address

Note: The Edge Relay Server does not support IPv6 communication.

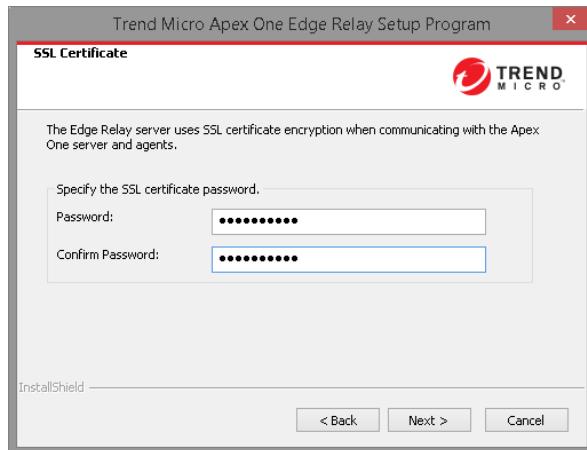
- Port

Note: You must configure your firewall and gateway to allow redirection of the Security Agent communication from the Internet to the Edge Relay Server and Communication through the port specified

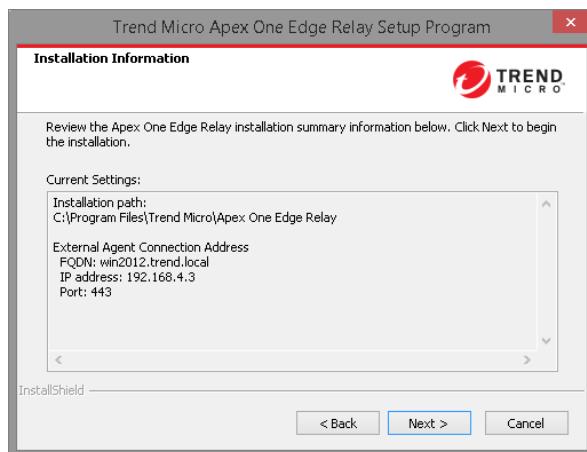
- 7 If no certificate is selected, an option to allow the setup to create a self-signed certificate is displayed. Click **Yes** to allow the setup to generate a certificate.



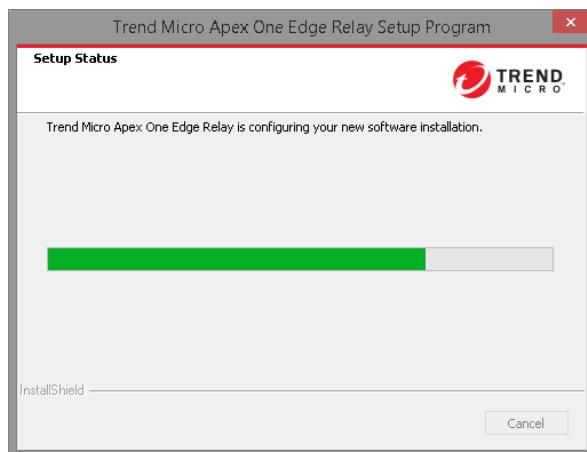
8 Specify and confirm the password used for the Edge Relay Server certificate and click **Next**.



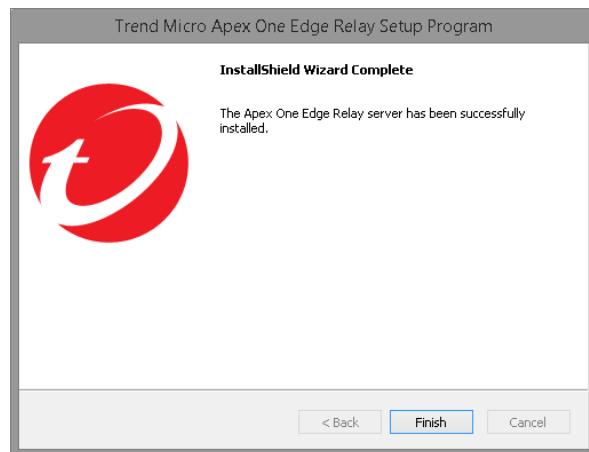
9 The Installation Information screen is displayed for review. Click **Next** to begin the setup.



10 The program files are installed.



- 11 Click **Finish** to complete the setup.



Registering the Edge Relay Server

After installing, you must use the **Edge Relay Server Registration Tool** to register the Edge Relay Server with each Apex One Server that off-premises Security Agents report to. Security Agents reporting to the Apex One Servers receive the registered connection settings and can automatically use the Edge Relay Server to contact the Apex One Server after leaving the corporate intranet.

On the Edge Relay Server computer, open a Command Prompt and navigate the following folder:

```
C:\Program Files\Trend Micro\Apex One Edge Relay\OfcEdgeSvc
```

Type the following command to register the Edge Relay Server:

```
ofcedgecfg.exe --cmd reg --server <server address> --port <port> --pwd  
<root password>
```

Where: <server address> is the Apex One Server IP address

<port> is the Apex One Server port number

<root password> is the Apex One Server **root** account password

For example: `ofcedgecfg.exe --cmd reg --server 192.168.4.1 --port 4343 --pwd trendmicro`

To view the status of the connection between the Apex One Server and the Edge Relay Server after registering, open the Apex One Web Management console and go to **Administration > Settings > Edge Relay**.

The Apex One Edge Relay server provides administrators visibility and increased protection of endpoints that users take outside of the company's intranet. By installing the Edge Relay server in the Demilitarized Zone (DMZ), you can continue to manage off-premises Security Agents that cannot establish a functional connection to the Apex One server.

To view other Edge Relay configuration commands, refer to the **Edge Relay Server Registration Tool** section in the Apex One Administrator Guide.

Viewing Off-premises Agents

To view Agents which recently connected to the Apex One Edge Relay Server, administrators can click **Off-premises Agent view** from the Agent Management page.

Logon User	IP Address	Listening...	Domain H...	Connecti...	GUID	Scan Met...
CLIENT-02\Administrator	192.168.4.4	21112	Trend\	Online	860b8147-97f0-43f9-93...	Smart Scan
CLIENT-03\Administrator	192.168.4.6	21112	Trend\	Online	424ce32f-c2e6-430c-9c...	Smart Scan
TREND\administrator	192.168.4.1	21112	Trend\	Online	68d0a7e5-c276-490b-8f...	Smart Scan
WIN2012\Administrator	192.168.4.3	21112	Trend\	Online	d4cb77c3-b687-40b2-a2...	Smart Scan

Number of agents: 4 Agents using smart scan: 4 Agents using conventional scan: 0

Additionally, administrators can view off-premises Agents using the following **Off-premises** widget. It displays the history of the Agent connection status. Administrators also have the option to switch the time range criteria to view by **Last 7 days** or **Last 24 hours**.

Apex One Relay Server Digital Certificates

Since the Apex One Edge Relay Server does not reside on the local network, certificates must be used to secure the data exchange channel. The certificates needed include the following:

Certificate Name	Certificate Path	Comments
OsceEdgeRoot	OSCE EDGE server - Trusted Root Certification Authority > Certificates	Edge Relay Server self-signed certificate
OsceOPA	OSCE Agent (off-premises) - OfcEdge > Certificates	Agent-server communication authenticated
Osceds OfcsslAgent	OSCE EDGE data server - Personal > Certificates	Encrypts data exchanged between Agents and Edge Relay Server as well as Edge Relay Server and Apex One Server
OsceDS Agent	OSCE EDGE server - Trusted People > Certificates	

The certificate deployment process includes the following steps:

- 1 The OsceEdgeRoot certificate is generated after the installation of the Apex One Edge Relay Server.
- 2 When the Apex One Server connects to Edge Relay Server, the OsceEdgeRoot certificate will be deployed to Apex One Server.
- 3 When the Security Agent connects to Apex One Server, it will deploy this new certificate. Once the Security Agent has this certificate, it can communicate and send information to the Apex One Edge Relay Server when required.

Note: The endpoint computer will only become aware of the Edge Relay Server after it has connected to the Apex One Server at least once after the Edge Relay Server has been installed.

Renewing Edge Relay Server Certificate

The **Edge Relay Server Registration Tool** can also be used to manually import/renew the certificate that is used to establish the Apex One Edge Relay Server connection. To renew the certificate, execute the following command:

```
OfcEdgeCfg.exe --renewcert --certpwd <password>
```

Off-premises Security Agents must connect to the Apex One server to obtain the new Edge Relay Server certificate. Any off-premises agents that do not receive the updated certificate can no longer communicate with the Edge Relay Server until connection with the Apex One server is established.

Lesson 6: Keeping Trend Micro Apex One Up To Date

Lesson Objectives:

After completing this lesson, participants will be able to:

- Update the Apex One Server
- Update Security Agents
- Promote Security Agents to become Update Agents

When updates are available, the Apex One Server and Smart Protection sources (Smart Protection Server or Smart Protection Network) download the updated components. There are no component download overlaps between the Apex One Server and Smart Protection sources because each one downloads a specific set of components.

You can configure both the Apex One Server and Smart Protection Server to update from a source other than the Trend Micro ActiveUpdate Server. To do this, you need to set up a custom update source.

The Apex One Server downloads most of the components that Agents need. The only component it does not download is the Smart Scan Pattern, which is downloaded by smart protection sources. If the Apex One Server manages a large number of Agents, updating may utilize a significant amount of Server computer resources, affecting the Server's stability and performance. To address this issue, Apex One has an Update Agent feature that allows certain Agents to share the task of distributing updates to other Agents.

ActiveUpdate

Apex One uses Trend Micro ActiveUpdate to obtain and distribute updates for specific program components. Two types of components can be updated:

- Engines
- Patterns
- Programs

The ActiveUpdate (AU) module is Apex One's interface to the ActiveUpdate system. As a Trend Micro common module, this module is developed independently of other products.

ActiveUpdate Integrity

With increasing reports of Advanced Protection Threat (APT) attacks from different organizations, ActiveUpdate was integrated into Apex One to prevent Man-in-the-Middle situations. In this scenario, hackers can perform ARP Spoofing and mislead the Agent to retrieve updates from the malicious source or attacker.

Integrity of the ActiveUpdate package is verified through digital signatures. The Apex One Server and Agents verify this signature on the update package before downloading the components. This ensures that the components being downloaded have been provided by Trend Micro and have not been tampered with.

To verify this feature, locate and open the `ofcscan.ini` file. In the **[Global Setting]** section, locate `EnforceAUSign=1`.

SaaS: There is no access to the `ofcscan.ini` file in the service implementation of Apex One.

Pattern Updates

Trend Micro releases two types of pattern updates:

- **Official Pattern Release:** Patterns are regularly made available to users as part of an Official Pattern Release (OPR). Upon release, these patterns are posted on the ActiveUpdate system once per day, where products can download using the default update source.
- **Controlled Pattern File Release:** These are pre-release version of a Trend Micro virus pattern file. It is a fully tested pattern file intended to provide additional antivirus protection in between official pattern file releases.

Incremental Updates

Incremental update technology limits the impact of updates on network bandwidth. This was originally only available for virus pattern updates, but has now been applied to other patterns. It does not, however, apply to engine updates.

For each new pattern on the Trend Micro update Server, there are several incremental patterns. Each incremental pattern contains the difference between the malware signatures in the latest version, and the version to which the increment corresponds.

Increments are provided for the 14 most recent Official Pattern Releases. If the pattern used in a product is older than any of the 14 incremental patterns, then the latest full pattern is downloaded.

ActiveUpdate Logs

ActiveUpdate-related activities are recorded in two logs:

- `TmuDump.txt`: the ActiveUpdate module records its activities in this log
- `Ofcdebug.log`: Apex One services record their activities in this log, making it ideal for studying calls from the product to the ActiveUpdate module

The ActiveUpdate module records all its actions in a log file called `TmuDump.txt`, making this file a very important source of troubleshooting information when analyzing update-related problems. This log can be written as a text file or as an HTML file, depending on settings in the ActiveUpdate configuration file.

The log files can be located in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Web\AU_Data\AU_Log

SaaS: There is no access to the TmuDump.txt or Ofcdebud.log file in the service implementation of Apex One.

Updating the Apex One Server

Apex One Server components can be updated manually or by configuring an update schedule.

SaaS: Server updates are performed by Trend Micro on a regular basis in the service implementation of Apex One.

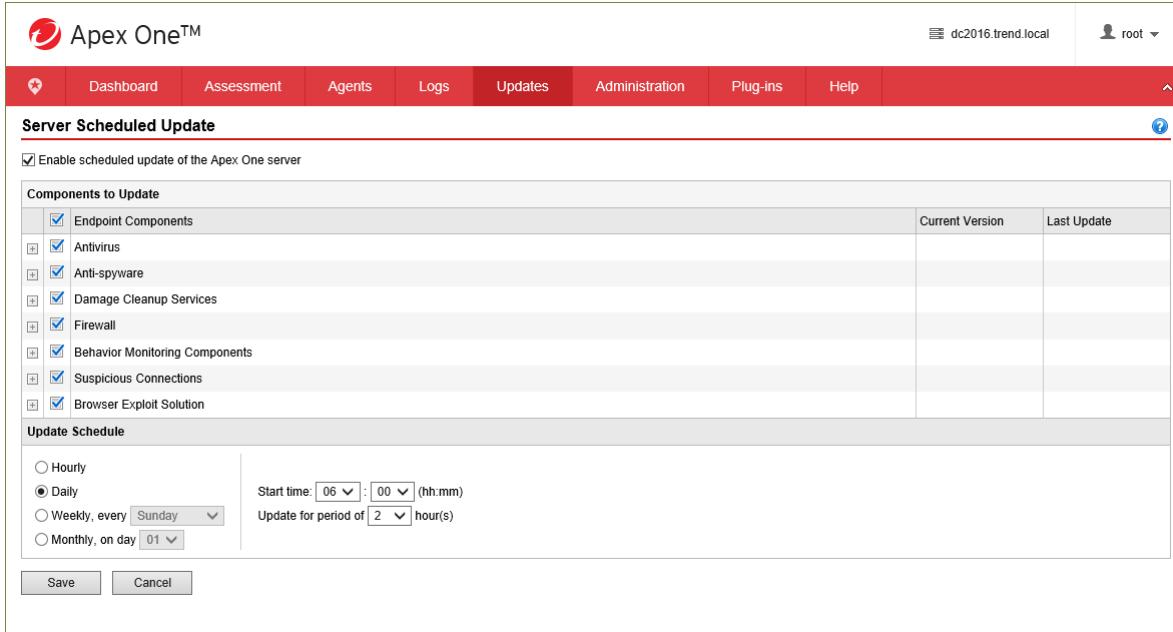
Manual Server Updates

When an update is critical, perform a manual update so the Apex One Server can obtain the updates immediately. In the Web Management console, click **Updates > Server > Manual Update**.

Components to Update				Current Version	Last Update
<input checked="" type="checkbox"/> Endpoint Components <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Antivirus <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Smart Scan Agent Pattern <input checked="" type="checkbox"/> Virus Pattern <input checked="" type="checkbox"/> IntelliTrap Pattern <input checked="" type="checkbox"/> IntelliTrap Exception Pattern <input checked="" type="checkbox"/> Virus Scan Engine (32-bit) <input checked="" type="checkbox"/> Virus Scan Engine (64-bit) <input checked="" type="checkbox"/> Memory Inspection Pattern <input checked="" type="checkbox"/> Early Launch Anti-Malware Pattern (32-bit) <input checked="" type="checkbox"/> Early Launch Anti-Malware Pattern (64-bit) <input checked="" type="checkbox"/> Contextual Intelligence Engine (32-bit) <input checked="" type="checkbox"/> Contextual Intelligence Engine (64-bit) <input checked="" type="checkbox"/> Contextual Intelligence Pattern <input checked="" type="checkbox"/> Contextual Intelligence Query Handler (32-bit) <input checked="" type="checkbox"/> Contextual Intelligence Query Handler (64-bit) <input checked="" type="checkbox"/> Advanced Threat Scan Engine (32-bit) <input checked="" type="checkbox"/> Advanced Threat Scan Engine (64-bit) <input checked="" type="checkbox"/> Advanced Threat Correlation Pattern <input checked="" type="checkbox"/> Anti-spyware <input checked="" type="checkbox"/> Damage Cleanup Services <input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> Behavior Monitoring Components <input checked="" type="checkbox"/> Suspicious Connections <input checked="" type="checkbox"/> Browser Exploit Solution 					
				14.807.00	13/02/2019 01:29:18
				14.809.00	13/02/2019 01:30:08
				0.247.00	24/01/2019 02:40:46
				1.583.00	13/02/2019 01:30:29
				11.000.1006	24/01/2019 02:27:45
				11.000.1006	24/01/2019 02:27:46
				1.489.00	13/02/2019 01:30:35
				21	24/01/2019 02:41:10
				21	24/01/2019 02:41:13
				1.7.1023	24/01/2019 02:27:46
				1.7.1023	24/01/2019 02:27:46
				1.026.00	24/01/2019 02:27:46
				1.1.1060	24/01/2019 02:27:47
				1.1.1060	24/01/2019 02:27:47
				11.000.1006	24/01/2019 02:27:47
				11.000.1006	24/01/2019 02:27:48
				1.112.00	24/01/2019 02:41:21

Scheduled Server Update

A scheduled update allows the Apex One Server to connect to the update source during the specified day and time to obtain the latest components. In the Web Management console, click **Updates > Server > Scheduled Update**.



The screenshot shows the 'Server Scheduled Update' configuration page in the Apex One Web Management console. At the top, there is a header bar with the 'Apex One™' logo, the IP address 'dc2016.trend.local', and a user icon for 'root'. Below the header is a navigation menu with links for Dashboard, Assessment, Agents, Logs, Updates (which is highlighted in red), Administration, Plug-ins, and Help.

The main content area is titled 'Server Scheduled Update'. It contains two main sections: 'Components to Update' and 'Update Schedule'.

Components to Update: This section lists various endpoint components that can be updated. Most components have checkboxes checked, indicating they are selected for update. The listed components include:

- Endpoint Components (checked)
- Antivirus (checked)
- Anti-spyware (checked)
- Damage Cleanup Services (checked)
- Firewall (checked)
- Behavior Monitoring Components (checked)
- Suspicious Connections (checked)
- Browser Exploit Solution (checked)

Update Schedule: This section allows setting the frequency and time of the scheduled update. The current settings are:

- Frequency: Daily (radio button selected)
- Start time: 06 : 00 (hh:mm)
- Update for period of 2 hour(s)

At the bottom of the page are 'Save' and 'Cancel' buttons.

Server Update Source

If the Apex One Server belongs to a network that is isolated completely from all outside sources, you can keep the server's components up-to-date by letting it update from an internal source that contains the latest components. This source can also be used in situations where an organization might want to control the release of new patterns, only allowing the patterns to be applied after internal testing.

The update source, such as Apex Central or a random host machine must have a reliable Internet connection so that it can download the latest components from the Trend Micro ActiveUpdate server. Without an Internet connection, the only way for the update source to have the latest components is to obtain the components yourself from Trend Micro and then copy them into the update source. Configure proxy settings if there is a proxy server between the Apex One Server and the update source and ensure that there is enough disk space for downloaded components. In the Web Management console, click **Updates > Server > Update Source**.

The screenshot shows the 'Server Update Source' configuration page. At the top, there are tabs for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The 'Updates' tab is selected. In the main area, there are three options for update sources:

- Trend Micro's ActiveUpdate Server (<https://osce14-p.activeupdate.trendmicro.com/activeupdate>)
- Other update source:
- Intranet location containing a copy of the current file
UNC path:
User name:
Password:

At the bottom of the form are 'Save' and 'Cancel' buttons.

Updating Security Agents

To allow the Server to deploy the updated components to Agents, enable Automatic Agent update. If automatic Agent update is disabled, the Server downloads the updates but does not deploy them to the Agents.

Automatic Updates

Agent updates can run automatically when certain events occur or when scheduled. In addition to components, Security Agents also receive updated configuration files during automatic update. In the Web Management console, click **Updates > Agents > Automatic Update**

The screenshot shows the 'Agent Automatic Updates' configuration page. At the top, there are tabs for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The 'Updates' tab is selected. The page has two main sections:

- Event-triggered Update**: Contains checkboxes for:
 - Initiate component update on agents immediately after the Apex One server downloads a new component
 - Include Independent and offline agent(s)
 - Let agents initiate component update after restarting and connecting to the Apex One server (Independent agents excluded)
 - Perform Scan Now after update (Independent agents excluded)
- Schedule-based Update**: Contains radio buttons for:
 - Minute(s)
 - Hour(s)
 - Daily
 - Weekly, every
 To the right of the radio buttons are fields for 'Start time' (16:00) and 'Update for a period of 4 hour(s)'.

At the bottom of the form are 'Save' and 'Cancel' buttons.

Event-Triggered Updates

The Server can notify online Agents to update components after it downloads the latest components, and offline Agents when they restart and then connect to the Server.

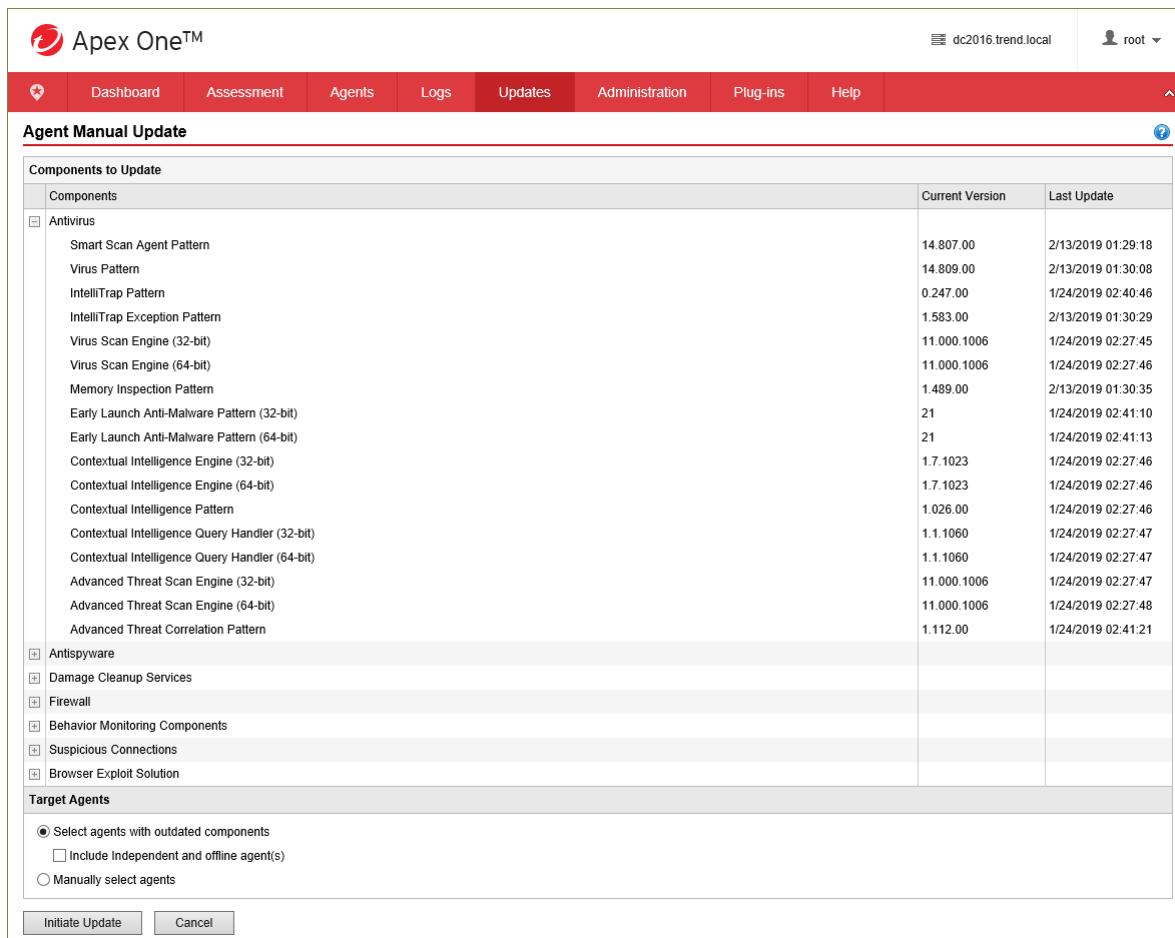
SaaS: Event-triggered updates are not available in the service implementation of Apex One.

Schedule-based Updates

Security Agents with appropriate privileges will run updates based on the schedule.

Manual Updates

When an update is critical, use Manual Update to immediately notify Agents to perform a component update. In addition to components, Security Agents also receive updated configuration files automatically during a Manual Update. In the Web Management console, click **Updates > Agents > Manual Update**.



The screenshot shows the Trend Micro Apex One™ Web Management console interface. At the top, there's a header with the logo, the server name 'dc2016.trend.local', and a user dropdown for 'root'. Below the header is a navigation bar with links: Dashboard, Assessment, Agents, Logs, Updates (which is highlighted in red), Administration, Plug-ins, and Help. A small upward arrow icon is next to the Help link. The main content area has a title 'Agent Manual Update' with a blue gear icon. Underneath is a table titled 'Components to Update' with two sections: 'Components' and 'Target Agents'. The 'Components' section lists various software components with their current version and last update date. The 'Target Agents' section contains three radio button options: 'Select agents with outdated components' (selected), 'Include Independent and offline agent(s)', and 'Manually select agents'. At the bottom are two buttons: 'Initiate Update' and 'Cancel'.

Components	Current Version	Last Update
Antivirus	14.807.00	2/13/2019 01:29:18
Smart Scan Agent Pattern	14.809.00	2/13/2019 01:30:08
Virus Pattern	0.247.00	1/24/2019 02:40:46
IntelliTrap Pattern	1.583.00	2/13/2019 01:30:29
IntelliTrap Exception Pattern	11.000.1006	1/24/2019 02:27:45
Virus Scan Engine (32-bit)	11.000.1006	1/24/2019 02:27:46
Virus Scan Engine (64-bit)	1.489.00	2/13/2019 01:30:35
Memory Inspection Pattern	21	1/24/2019 02:41:10
Early Launch Anti-Malware Pattern (32-bit)	21	1/24/2019 02:41:13
Early Launch Anti-Malware Pattern (64-bit)	1.7.1023	1/24/2019 02:27:46
Contextual Intelligence Engine (32-bit)	1.7.1023	1/24/2019 02:27:46
Contextual Intelligence Engine (64-bit)	1.026.00	1/24/2019 02:27:46
Contextual Intelligence Pattern	1.1.1060	1/24/2019 02:27:47
Contextual Intelligence Query Handler (32-bit)	1.1.1060	1/24/2019 02:27:47
Contextual Intelligence Query Handler (64-bit)	11.000.1006	1/24/2019 02:27:47
Advanced Threat Scan Engine (32-bit)	11.000.1006	1/24/2019 02:27:48
Advanced Threat Scan Engine (64-bit)	1.112.00	1/24/2019 02:41:21
Advanced Threat Correlation Pattern		
Antispyware		
Damage Cleanup Services		
Firewall		
Behavior Monitoring Components		
Suspicious Connections		
Browser Exploit Solution		

Target Agents

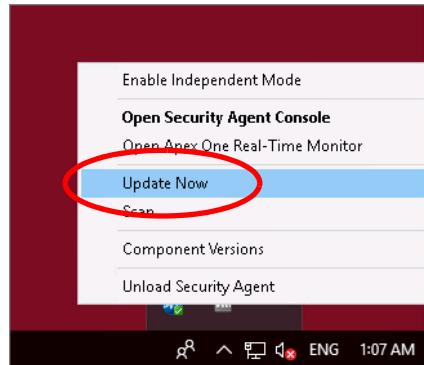
Select agents with outdated components
 Include Independent and offline agent(s)
 Manually select agents

Buttons: Initiate Update, Cancel

SaaS: Manual Agent updates are not available in the service implementation of Apex One.

Privilege-based Updates

Users with update privileges have greater control over when the Security Agent on their computers gets updated.



Agent Update Source

An alternate source for updates can be selected for specific Agents. In the Web Management console, click **Updates > Agents > Update Source**.

A screenshot of the Trend Micro Web Management console. The top navigation bar includes links for Dashboard, Assessment, Agents, Logs, Updates (which is selected and highlighted in red), Administration, Plug-ins, and Help. The user is logged in as 'root'. The main content area is titled 'Agent Update Source' and contains instructions for selecting alternative update sources. It shows two radio button options: 'Standard update source (update from Apex One server)' (selected) and 'Customized update source'. Below these are checkboxes for 'Update Agents update components, domain settings, and agent programs and hot fixes, only from the Apex One server' (checked) and 'Security Agents update the following items from the Apex One server if all customized sources are unavailable or not found' (unchecked). Under 'Components', 'Domain settings' is checked, while 'Security Agent programs and hot fixes' is unchecked. A 'Customized Update Source List' section shows a table with columns for Order, IP Range, and External Source. The table has three rows: one with 'Order' and 'IP Range' columns and an 'External Source' column; another with 'Add' and 'Delete' buttons; and a third with 'Order', 'IP Range', and 'External Source' columns. At the bottom of this section is a 'Notify All Agents' button.

Update Agents

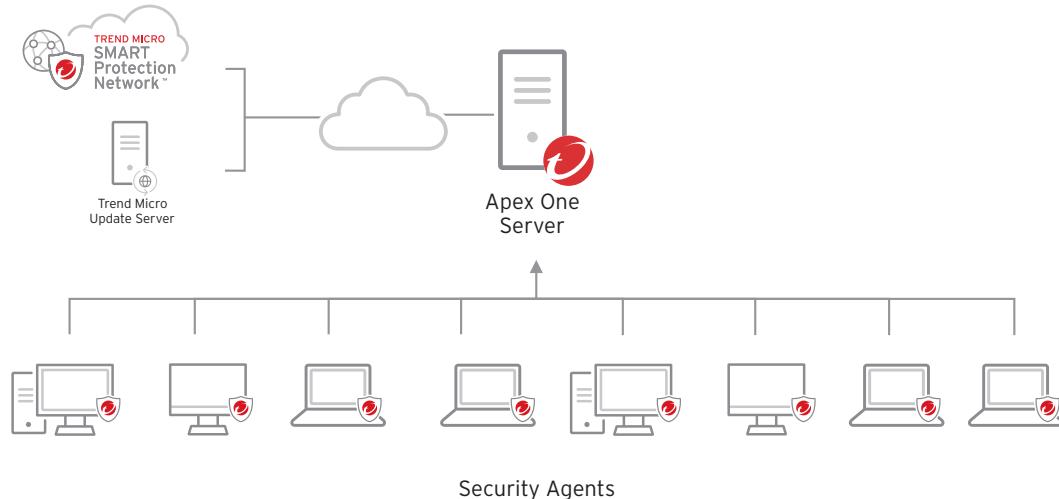
Update Agents are Security Agents that function as alternative update sites for other Agents within an Apex One network. They permit the deployment of settings to Agents whose connections to the Apex One Server would have been sufficient for regular Agent-Server messages but not for bandwidth-intensive updates, including:

- Component updates
- Domain settings
- Agent programs and hot fixes

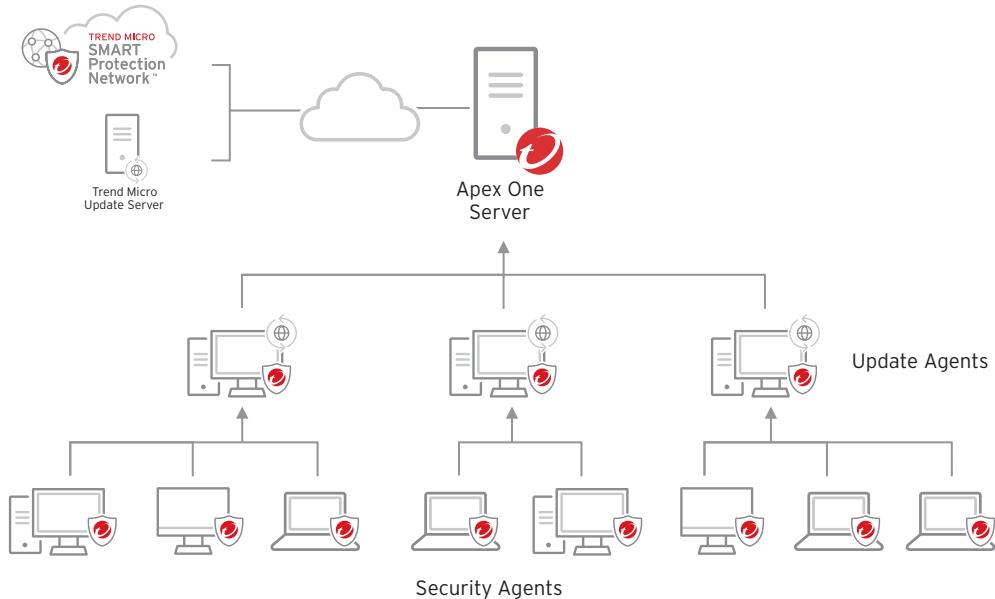
Update Agents serve as local ActiveUpdate sites. Like the Apex One Server, they offer both full and incremental patterns to their Agents by way of its own ActiveUpdate folder.

Best Practice: Any Security Agent can be promoted to an Update Agent, but typically, it is recommended that an Agent on an endpoint computer that remains on at all times be used.

Without Update Agents, all endpoint computers contact the Apex One Server for updates. In installations with many Security Agent, this can create network traffic issues.



With Update Agents in place, endpoint computers will contact their Update Agents for updates instead of contacting the Apex One Server. This reduces the amount of network traffic destined for the Apex One Server. Security Agent are assigned Update Agents based on their IP addresses.

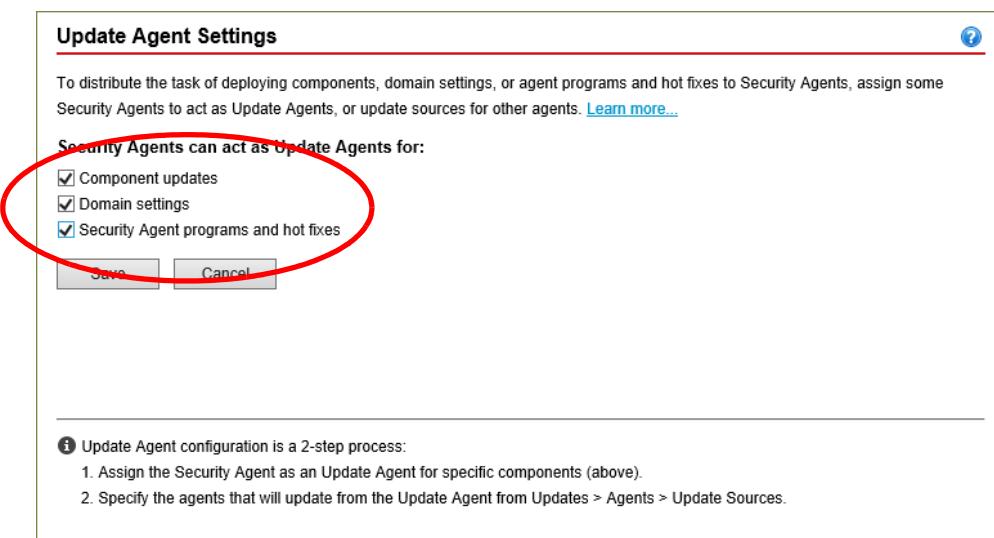


Best Practice: Since a single update agent can handle update requests from around 250 endpoints, it is recommended to create one update agent for every 250 endpoints. Do not promote the Security Agent on an Apex One Server to become the Update Agent.

Promoting an Agent to an Update Agent

Promoting an Agent to an Update Agent is a two-step process:

- 1 Click **Update Agent Settings** from the right-mouse button menu on any Security Agent in the Agents list. Select the options to be delivered by the Update Agent and click **Save**.



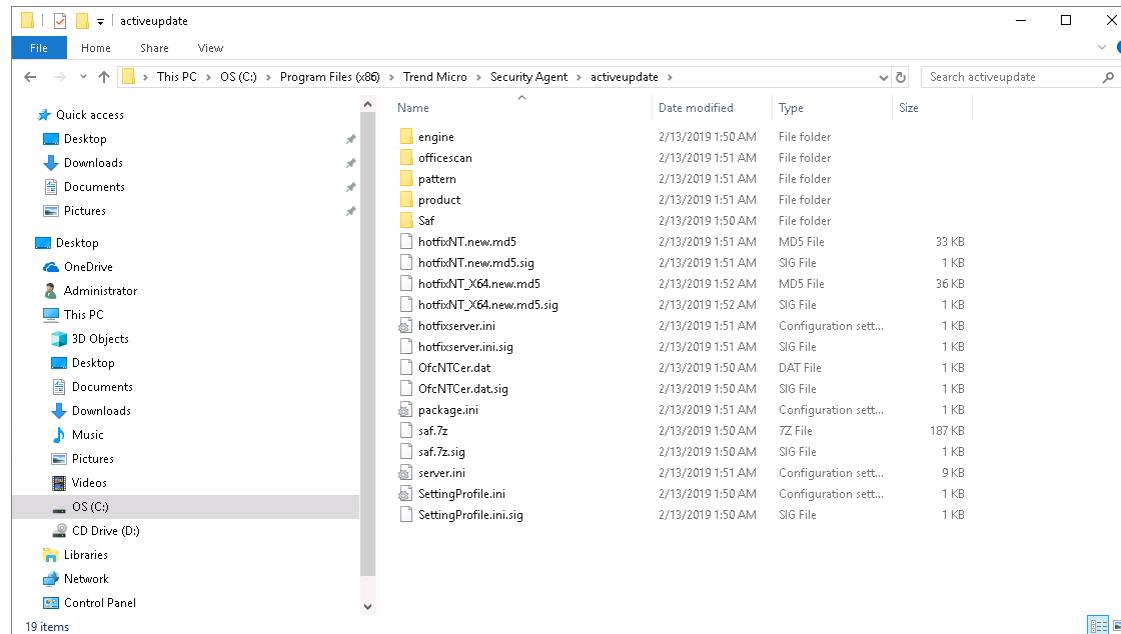
- 2 Modify the update source for a range of IP addresses. Click **Updates > Agents > Update Source**. Click **Customized Update Source** and **Add**. Identify an IP address range and select the **Update Source** as the newly created Update Agent.

The screenshot shows the 'Add IP Range and Update Source' configuration page. The 'Update source' section is highlighted with a red circle around the 'Update Agent' dropdown menu, which contains 'CLIENT-03'. Other options like 'Use the Update Agent IP address to connect' and 'Use the Update Agent hostname to connect' are also visible.

SaaS: Promoting an Agent to an Update Agent is done through Apex Central policies in the service implementation of Apex One.

Update Components

Components that Update Agents make available to other Security Agents are stored in the ActiveUpdate folder. This is essentially a copy of the download folder on the Apex One Server.



The components that the Update Agent itself uses, for its own purposes, are still stored in the main Security Agent folder.

The default Update Agent downloads the following components when the Agent is promoted to Update Agent status. The approximate size of a typical Update Agent and the elements it needs to download to become an Update Agent is outlined here.

Items stored	Location	Approximate size
Scan engine and pattern file updateable components	\engine \pattern	70 MB
Domain settings	\Safsa.7z	75 MB*
Programs and hot fixes	\Apex One newpnt.zip newpx64.zip	250 MB
Additional		200 MB

* Each domain with different settings increases about 9KB.

Promotion of an Agent to a default Update Agent transfers approximately 600MB of files to the Security Agent. It is, however, able to provide incremental updates to its Agents immediately.

Downloading and Deploying Updates

ActiveUpdate is used on Apex One networks for both obtaining updates from an update source, and then deploying them to Security Agents. The update process in an Apex One network can be broken down into the following steps.

1 Apex One determines if updates are required

The process begins when Apex One Server uses its ActiveUpdate module to download a server definition file (`server.ini`) from a pre-selected ActiveUpdate Server. The download could have been initiated either manually, or by a scheduled update event.

`Server.ini` contains a list of the versions of components currently available on the ActiveUpdate Server. ActiveUpdate compares the information in this file with the files on the Apex One Server to determine if an update is necessary.

Note: The Apex One Master Service is responsible for calling the ActiveUpdate module.

2 Updates are downloaded

If the ActiveUpdate module determines that an update is required, it downloads the necessary components from the ActiveUpdate Server. Afterwards, it updates its own `server.ini` file.

3 Update Agent notification and download

In response to an update request, the Apex One Server identifies Update Agents on its database. Once identified, the Server sends a message to these Update Agents.

After notifying the Update Agents, the server waits (by default 15 minutes) for the Update Agents to obtain their updates, and retries 5 times if no response has been received. This waiting period is defined in `ofcscan.ini` by the `Download_TimeOut_RA` parameter under the `[INI_SERVER_SECTION]` section.

You can also use the **SvrTune.exe**, located in the `...\\PCCSRV\\Admin\\Utility\\SvrTune` folder to change the settings.

4 Agent notification

After completing the download, Apex One can do one of the following:

- Immediately deploy updates to its Agents (default)
- Store updates for use in either a manual update deployment, or an Agent-initiated update

At deployment time, Apex One notifies its Agents about the availability of new components, thereby prompting Agents to use their respective ActiveUpdate modules to download the Apex One `server.ini` file.

5 Agents determine if updates are required

Upon receipt of the update notification, the Security Agents perform the same update verification done in Step 1. However in the Agent's case, the update source is either the Apex One Server itself, or an alternative update source.

6 Agents download updates

Agents download the increments or patterns as needed.

7 Agent notifies server it has the update

Agents notify their Apex One Server that they have been updated.

Security Compliance

Use Security Compliance in an on-premises environment to ensure that Agents have the latest services, components, settings and have run recent scans. Security Compliance determines component inconsistencies between the Apex One Server and Agents.

SaaS: Security Compliance is not available in the service implementation of Apex One.

Security Compliance generates a Compliance Report to help you assess the security status of Security Agents managed by the Apex One Server. Security Compliance generates the report on demand or according to a schedule. In the Web Management console, click **Assessment > Security Compliance > Manual Report or Scheduled Report**.

Services

Security Compliance checks whether the following Security Agent services are functional:

- Antivirus
- Anti-spyware
- Firewall
- Web Reputation
- Behavior Monitoring/Device Control (also referred to as Trend Micro Unauthorized Change Prevention Service)
- Data Protection
- Suspicious Connection

A non-compliant Agent is counted at least twice in the Compliance Report.

- In the Endpoints with Non-compliant Services category
- In the category for which the Security Agent is non-compliant. For example, if the Security Agent's Antivirus service is not functional, the Agent is counted in the Antivirus category. If more than one service is not functional, the Agent is counted in each category for which it is non-compliant.

Restart non-functional services from the Web Management console or from the Security Agent. If the services are functional after the restart, the Agent will no longer appear as non-compliant during the next assessment.

The screenshot shows the Trend Micro Apex One™ web interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. On the far right, it shows the user name 'dc2016 trend local' and 'root'. Below the navigation bar, a red box highlights the 'Services' tab under 'Manual Assessment'. The main content area has two main sections: 'Endpoints with Non-compliant Services' (which lists various services like Antivirus, Anti-spyware, Firewall, etc., with counts of 0 or 2) and 'Agent Tree Scope' (which shows a tree structure with 'Apex One Server' and 'Trend' selected). At the bottom, there's a table for 'Restart Security Agent' with two entries: 'CLIENT-02' and 'CLIENT-03', both marked as 'online' with 'Data Protection' listed under 'Services'.

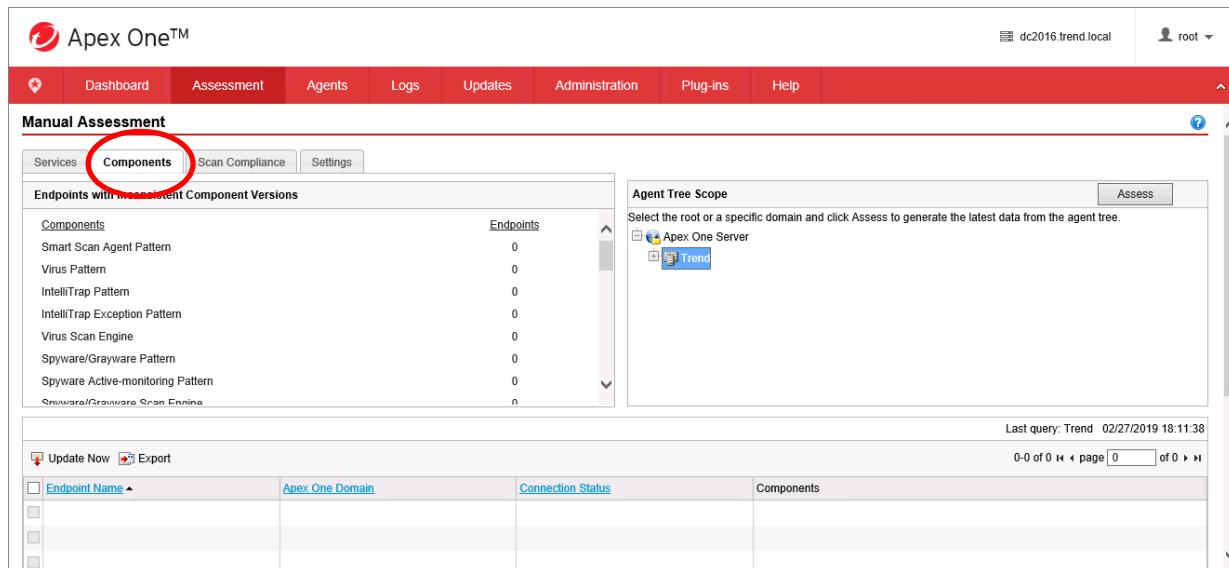
Components

Security Compliance determines component version inconsistencies between the Apex One server and Security Agents. Inconsistencies typically occur when Agents cannot connect to the Server to update components. If the Agent obtains updates from another source (such as the Trend Micro ActiveUpdate server), it is possible for the Agent component version to be newer than the version on the server.

A non-compliant Agent is counted at least twice in the Compliance Report.

- In the Endpoints with Inconsistent Component Versions category
- In the category for which the Agent is non-compliant. For example, if the Agent Smart Scan Agent Pattern version is not consistent with the version on the Server, the Agent is counted in the Smart Scan Agent Pattern category. If more than one component version is inconsistent, the Agent is counted in each category for which it is non-compliant.

To resolve component version inconsistencies, update outdated components on the Agents or server.



The screenshot shows the Trend Micro Apex One™ interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. On the far right, it shows the host name "dc2016.trend.local" and a user icon for "root". Below the navigation bar, the title "Manual Assessment" is displayed. Under "Manual Assessment", there are tabs for Services, Components (which is circled in red), Scan Compliance, and Settings. The main content area has a section titled "Endpoints with Inconsistent Component Versions" containing a table with columns for Components and Endpoints. The table lists various patterns and their counts. To the right of this table is the "Agent Tree Scope" panel, which allows selecting a root or specific domain and clicking "Assess" to generate data from the agent tree. It shows a tree structure with "Apex One Server" and "Trend" under it. At the bottom of the interface, there are buttons for "Update Now" and "Export", and a search bar with placeholder text "Last query: Trend 02/27/2019 18:11:38".

Scan Compliance

Security Compliance checks if **Scan Now** or **Scheduled Scans** are run regularly and if these scans are completed within a reasonable amount of time. Security Compliance can only report the Scheduled Scan status if Scheduled Scan is enabled on Agents.

Security Compliance uses the following scan compliance criteria:

- No Scan Now or Scheduled Scan performed for the last (x) days: The Security Agent is non-compliant if it did not run Scan Now or Scheduled Scan within the specified number of days.
- Scan Now or Scheduled Scan exceeded (x) hours: The Security Agent is non-compliant if the last Scan Now or Scheduled Scan lasted more than the specified number of hours.

A non-compliant Agent is counted at least twice in the Compliance Report.

- In the Endpoints with Outdated Scanning category
- In the category for which the Agent is non-compliant. For example, if the last Scheduled Scan lasted more than the specified number of hours, the Agent is counted in the Scan Now or Scheduled Scan exceeded <x> hours category. If the Agent satisfies more than one scan compliance criteria, it is counted in each category for which it is non-compliant.

Run **Scan Now** or **Scheduled Scan** on Agents that have not performed scan tasks or were unable to complete scanning.

Settings

Security Compliance determines whether Agents and their parent domains in the Agent tree have the same settings. The settings may not be consistent if you move any Agents to another domain that is applying a different set of settings, or if any Agent user with certain privileges manually configured settings on the Security Agent console.

A non-compliant Agent is counted at least twice in the Compliance Report.

- In the Endpoints with Inconsistent Configuration Settings category
- In the category for which the Agent is non-compliant. For example, if the scan method settings in the Agent and its parent domain are not consistent, the Agent is counted in the Scan Method category. If more than one set of settings is inconsistent, the Agent is counted in each category for which it is non-compliant.

Lesson 6: Keeping Trend Micro Apex One Up To Date

To resolve the setting inconsistencies, apply domain settings to the Agent.

The screenshot shows the Apex One™ web interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root'. Below the navigation is a section titled 'Manual Assessment' with tabs for Services, Components, Scan Compliance, and Settings. Under 'Settings', there's a table for 'Endpoints with Inconsistent Configuration Settings' showing various scan method configurations. To the right is an 'Agent Tree Scope' panel with a tree view of agents under 'Apex One Server' and 'Trend'. At the bottom, there's a table listing agents with their connection status and settings applied.

Update Summary

A summary report of updated online and offline Agents can be displayed. Click **Updates > Update Summary**.

The screenshot shows the 'Update Summary' section of the Apex One™ web interface. It includes a 'Notification Status' section with a circular progress bar, a 'Total number of agents: 5', and a 'Last notification: 2/13/2019 01:37:35' message. Below this are sections for 'Antivirus' and 'Pattern' updates. Each section has a table showing the number of agents in different update statuses (Updated, Outdated, Total) and a corresponding green progress bar indicating the percentage updated.

Rollback

Rolling back updates refers to restoring previous versions of updated or replaced components in an on-premises installation of Apex One.

SaaS: Update rollback is not available in the service implementation of Apex One.

The ActiveUpdate module performs the rollback procedure when:

- The update/patch application process cannot be completed because of an error. For example, there was a problem extracting a compressed update.
- The administrator issues a rollback command from the Web Management console. This means the update process itself was successfully completed, but the administrator wanted to use previous components for some reason.

Smart Scan Agent Pattern		
	Previous	Current
Version	14.777.00	14.807.00
Last Update	28/01/2019 07:31:40	13/02/2019 01:29:18
Roll Back Server and Agent Versions		Synchronize with Server

Virus Pattern		
	Previous	Current
Version	14.779.00	14.809.00
Last Update	29/01/2019 02:11:13	13/02/2019 01:30:09
Roll Back Server and Agent Versions		Synchronize with Server

Virus Scan Engine (32-bit)		
	Previous	Current
Version	N/A	11.000.1006
Last Update	N/A	26/01/2019 23:30:37
Roll Back Server and Agent Versions		Synchronize with Server

Virus Scan Engine (64-bit)		
	Previous	Current
Version	N/A	11.000.1006
Last Update	N/A	26/01/2019 23:30:37
Roll Back Server and Agent Versions		Synchronize with Server

Note: Agents that are updated through Update Agents cannot be rolled back using the Web Management console. The administrator must manually roll them back.

Rolling Back Patterns

When Agents receive a pattern rollback notification from the Server, they check the version of the pattern file on the Server. If the version on the Server is older than that on the Agent, a Force Update will be triggered and the Agents will roll back to the pattern file on the Server.

Note: Only full virus patterns can be rolled back from the Web Management console. Non-virus related patterns, and virus-related incremental patterns, are not covered by rollback functionality at this time.

The Apex One Server retains the last five virus patterns, which can all be used for rolling back. The Agent, on the other hand, only retains two older patterns.

Rolling Back Engines

When the scan engine files on the Server are updated, the following folder is created to store the last versions of the scan engine:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Download\Rollback

Records about the last scan engine versions are also stored in the rollback section of the ofcscan.ini, for example:

```
[INI_ROLLBACK_SECTION]  
RollBack_Previous_NT_Engine=6.810.1005
```

Note: Only the VSAPI scan engine can be rolled back from the Web Management console.

Both the Server and Agent retain the previous version of the scan engine for rollback purposes.

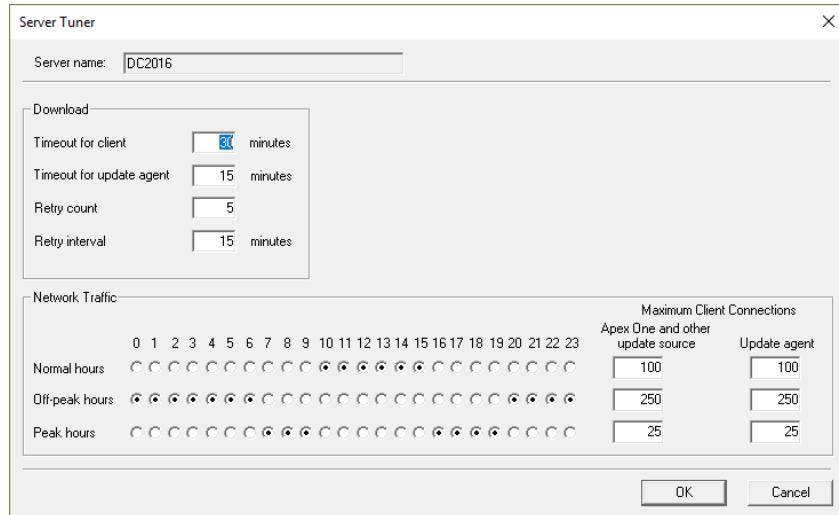
Server Tuner Tool

The Server Tuner Tool can be used to adjust the performance of Apex One updates.

SaaS: The Server Tuner tool is not available in the service implementation of Apex One.

The tool can be located in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\SrvTune



Download Settings

When the number of Security Agents (including Update Agents) requesting updates from the Apex One Server exceeds the Server's available resources, the Server moves the Agent update request into a queue and processes the requests when resources become available. After the Agent successfully updates components from the Apex One Server, it notifies the Server that the update is complete. Set the maximum number of minutes the Apex One Server waits to receive an update notification from the Agent. Also set the maximum number of times the server tries to notify the Agent to perform an update and to apply new configuration settings. The Server keeps trying only if it does not receive Agent notification.

- **Timeout for client:** specifies how long the Apex One Server will wait for the Agent to acknowledge the update as successful
- **Timeout for update Agent:** specifies how long the Apex One Server will wait for the Update Agent to acknowledge the update as successful
- **Retry count:** specifies how many times the Server will attempt to update an Agent
- **Retry interval:** specifies how long the Apex One Server will wait before checking the update queue

Network Traffic Settings

The **Network Traffic** section defines the hours of the day that constitute the normal, off-peak, and peak hours in your network. The Maximum Client Connections specify the number of Agents that the Server will notify about the updates at one time. There are two types of Agents:

- **Apex One and other update source:** Apex One Server or other update source (including ActiveUpdate Server, and internal update web pages)
- **Update Agent**

Note: After the Server notifies the Agents that updates are available, the Agents will attempt to update from their designated update sources. The number of Agents in the network and the network resources will determine the best timeout value for the setting.

Default Settings

The Apex One Server waits up to 30 minutes for each notified Agent in a group to complete the update sequence. If an Agent cannot finish the update within the 30 minutes time-frame, the Apex One Server will notify the next Agent in queue. By default, an Agent attempts to download updates from the Server up to five times at 15-minute intervals.

Recommended Configurations for Improved Performance

In large networks, small maximum connection settings, shorter timeouts, and fewer retries may update the Agents more quickly.

Under Network Traffic, specify the number of Agents the Server will notify at a time about the updates. Since the Update Agents receive their updates before the Agents are notified, you need to set the Timeout for Update Agent setting with sufficient time. The default setting of 10 minutes may require an increase if the network is very large.

Update Utilities

Apex One includes utilities that can be used to schedule updates.

SaaS: Update utilities are not available in the service implementation of Apex One.

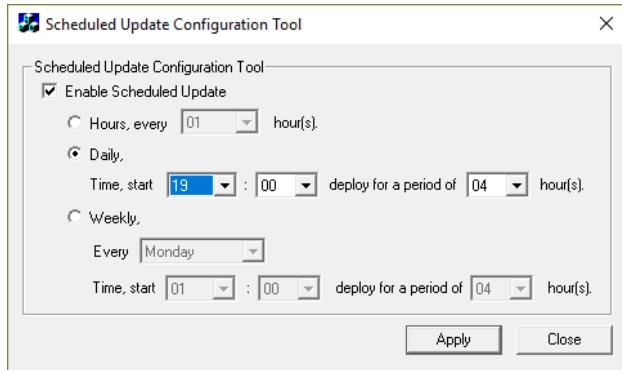
Domains Schedule Update Tool

This tool allows an organization to configure a schedule based on Agent Tree Domains. All Agents belonging to the domain will apply the schedule. The `dsu_convert.exe` tool can be found in the following folder:

`C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\DomainsScheduledUpdate`

Scheduled Update Configuration Tool

This tool (`SUCTool.exe`) is used to enable and configure scheduled updates on an Update Agent that was installed using Agent Packager. This tool is not available if the Update Agent was installed using other installation methods.



Lesson 7: Trend Micro Smart Protection

Lesson Objectives:

After completing this lesson, participants will be able to:

- Define the Smart Protection Services used by Apex One
- Configure Smart Protection Sources

Smart Protection includes services that provide anti-malware signatures, web reputation credibility scores, vulnerability patterns, in-the-cloud threat databases and more. Smart Protection Services used by Apex One include:

- File Reputation Services
- Web Reputation Services
- Predictive Machine Learning Services
- Census Service
- Certified Safe Software Service
- Smart Feedback

File Reputation Services

File Reputation Services check the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in the cloud, it is available instantly to all users. The cloud-Agent architecture eliminates the burden of pattern deployment while significantly reducing the overall Agent footprint.

Security Agents must be in Smart Scan mode to use File Reputation Services.

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.

Predictive Machine Learning Services

Apex One provides enhanced malware protection for unknown threats and zero-day attacks through Predictive Machine Learning. Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging security risks through digital DNA fingerprinting, API mapping, and other file features.

Predictive Machine Learning is effective in protecting against security breaches that result from targeted attacks using techniques such as phishing and spear phishing. In these cases, malware that is designed specifically to target your environment can bypass traditional malware scanning techniques.

During real-time scans, when Apex One detects an unknown or low-prevalence file, Apex One scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features. It then sends the report to the Predictive Machine Learning engine which is hosted on the Trend Micro Smart Protection Network. Through the use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains. If the file is identified as a threat, Apex One quarantines the file to prevent the threat from continuing to spread across your network.

Census Service

This service provides information about the prevalence of detected files. Prevalence is a statistical concept referring to the number of times a file was detected by Trend Micro sensors at a given time. If a file has not triggered any detections, the file becomes suspicious as over 80% of all malware is only seen once.

Census covers over 300 million distinct executable files. File prevalence and maturity is important because polymorphism is the primary weapon of malware. An unknown binary can mean a possible targeted attack.

Certified Safe Software Service

The Certified Safe Software Service provides a comprehensive list of applications considered to be safe by Trend Micro. The list includes most popular operating system files and binaries as well as applications for desktops, servers, and mobile devices. Trend Micro periodically provides updates to the list.

Certified Safe Software Service queries Trend Micro datacenters to check submitted sample files and objects against these databases. White listing known good files is used to:

- Reduce false positives
- Save computing time and resources
- Provide a mechanism for locking down systems from any undesired infiltration

Sources for the Certified Safe Software Service include:

- Internal sources, such as the File Reputation Service, Tech Support, All Trend Release Builds, etc.
- Partnerships with other tech companies, including Adobe, Apple, Google, Mozilla, Cisco, Acer, VMWare, Yahoo!, Citrix, Intel, Intuit, Bigfish Games, Electronics Arts, etc.

- Targeted, pro-active sourcing including software download sources, such as Cnet download.com, Majorgeeks, Softpedia, Sourceforge, crawlers, etc.
- Subscriptions, including National Software Reference Library, MSDN, and some regional magazines (especially from Europe) that include DVDs/applications
- Local sourcing teams for P regional file collection
- GRID (Good Reputation Index Database), the world's largest goodware catalog with over 700 million unique files and 130+ Grid Partners
- Customer Submission, for example, through Customer Support

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 through Smart Feedback include:

- 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 Management console. 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.

Service URLs

The URLs used by the Security Agent to communicate with these services include:

- **Predictive Machine Learning:** osce140-en-f.trx.trendmicro.com or osce140-en-b.trx.trendmicro.com
- **ActiveUpdate:** osce14-p.activeupdate.trendmicro.com/activeupdate
- **Census:** osce14-en-census.trendmicro.com
- **Certified Safe Software Service:** osce14-en.gfrbridge.trendmicro.com
- **Web Reputation:** osce14-0-en.url.trendmicro.com
- **Smart Scan:** osce14.icrc.trendmicro.com/tmcss
- **Smart Feedback:** osce140-en.fbs25.trendmicro.com

Smart Protection Sources

The Smart Protection source can be either:

- Trend Micro Smart Protection Network
- Smart Protection Server

Trend Micro Smart Protection Network

The Trend Micro Smart Protection Network is a cloud-client content security infrastructure designed to protect customers from security risks and Web threats. It powers both on-premises and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. 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.

Smart Protection Server

Smart Protection Servers are for users who have access to their local corporate network. Local servers localize Smart Protection Services, including File Reputation and Web Reputation, to the corporate network to optimize efficiency.

SaaS: The service implementation of Apex One cannot make use of local Smart Protection Servers.

There are two types of Smart Protection Servers:

- Integrated Smart Protection Server
- Standalone Smart Protection Server

Integrated Smart Protection Server

The Integrated Smart Protection Server is installed on the Apex One Server. It can be installed during Apex One Server installation or at later point by using the Integrated Smart Protection Server Installation Tool located in:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\ISPSInstaller\

This server is only recommended for networks with 1,000 Agents or less, and for test deployments.

The Integrated Smart Protection Server can be enabled through the Apex One Web Management console.

The screenshot shows the Apex One™ web interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root'. Below the navigation bar, the title 'Integrated Smart Protection Server' is displayed. Under this title, there are several configuration options:

- Enable File Reputation Services
 - Use HTTP for scan queries
 - Use HTTPS for scan queries
- Enable Web Reputation Services

Below these settings is a section titled 'Agent Connection' containing a table of service protocols and their corresponding URLs:

Services	Protocol	Server Address
File Reputation	HTTPS	https://dc2016.trend.local:4343/tmcss/
File Reputation	HTTP	http://dc2016.trend.local:8080/tmcss/
Web Reputation	HTTP	http://dc2016.trend.local:8080/

Finally, there is a 'Component Status' section with another table showing current versions and last update times for 'Smart Scan Pattern' and 'Web Blocking List' components:

Component	Current Version	Last Update	Action
Smart Scan Pattern	19088.014.00	02/13/2019 14:11:13	<button>Update Now</button>
Web Blocking List	10050257	02/13/2019 14:25:22	<button>Update Now</button>

Enabling or disabling the services related to Smart Protection Server changes the corresponding parameter in the `Ofcserver.ini` file. The Apex One Master Service is directly responsible for starting and stopping the Integrated Smart Protection Server service (`iCRCService.exe`) in response to Web Management console commands.

Standalone Smart Protection Server

The Standalone Smart Protection Server is recommended in the following situations:

- Larger networks of 1000 Agents or more
- Performance issues on Apex One server or not enough resources to contain an integrated SPS
- Remote office VPN with low bandwidth communication with the Apex One server
- For Load Balancing and High Availability

This server is available as a VMware image that runs CentOS and is compatible with the following virtual servers:

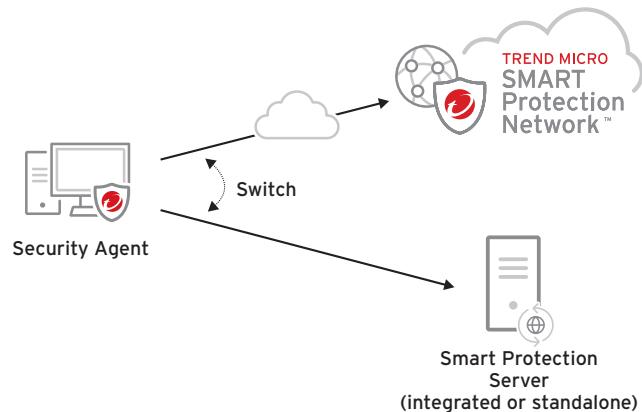
- VMware ESXi Server 6.5, 6.0 Update 2 and 5.5 Update 3b
- Microsoft Windows Server 2008 R2 with Hyper-V
- Microsoft Windows Server 2012 with Hyper-V
- Microsoft Windows Server 2012 R2 with Hyper-V
- Microsoft Windows Server 2016 with Hyper-V
- Citrix XenServer 7.2, 7.1, 6.5

The following table defines and highlights the differences between the Smart Protection Network and Local Smart Protection Servers:

	Smart Protection Network	Local Smart Protection Servers
Availability	External Agents: Agents that don't meet the location criteria specified on the Apex One Web Management console	Internal Agents: Agents that meet the location criteria specified on the Apex One Web Management console
Purpose	A globally scaled Internet-based infrastructure that provides Smart Protection Services to Agents that do not have immediate access to their corporate network	A local Smart Protection Service for the corporate network used to optimize efficiency
Connection Protocol	HTTPS	File Reputation: HTTP, HTTPS Web Reputation: HTTP only
Administration	Trend Micro	Apex One Server administrator
Pattern Update Source	Trend Micro ActiveUpdate	Trend Micro ActiveUpdate
Types	n/a	Integrated: Installed on the same computer where the Apex One Server is deployed Standalone: Installed on a VMware or Hyper-V server or Citrix XenServer

Configuring the Agent Smart Protection Source

Agents send queries to Smart Protection sources (the Trend Micro Smart Protection Network, or a local Smart Protection Server) when scanning for security risks and determining a Website's reputation.



Security Agents can switch between these Smart Protection sources based on their location relative to the corporate network. When the Agent detects that it is outside the corporate network, it will look for the Trend Micro Smart Protection Network, and when it is inside the network, it will look for pre-designated Smart Protection Servers.

To reduce the possibility of going off-line, Security Agents can be assigned multiple Smart Protection Servers. If the Agent is unable to query one Smart Protection Server, it can switch to an alternative Smart Protection Server if another is available, thereby avoiding a single-point-of-failure for cloud scanning functionality.

Note: If an Agent is internal and cannot connect to an internal Smart Protection Server, it will not automatically connect to the Global Smart Protection Server unless the URL of that server appears in the list.

Lesson 8: Protecting Endpoint Computers From Malware

Lesson Objectives:

After completing this lesson, participants will be able to:

- Configure malware and grayware scanning
- Quarantine malware
- Describe Smart Scan
- Configure and enable Outbreak Prevention

Apex One protects endpoint computers against malicious software, such as viruses, spyware, ransomware, Trojans and other malware. Different scanning techniques protect against known and unknown malware.

Scanning for Malware

Security Agents scan endpoint computers for malware through one of the following methods:

- **Real-time Scan:** This method scans files, folders and URLs as soon as they are accessed, triggered by I/O event hooking.
- **Manual Scan:** This method scans files and folders on demand, when initiated by the end user.
- **Scheduled Scan:** This method uses the same scanning methods and has the same detection capabilities as used for on-demand scanning. Scheduled scans are, however, triggered automatically based on a selected frequency (daily, weekly or monthly) and a specified time.
- **Scan Now:** This method scans files and folders on demand on one or more target computers when initiated by the Administrator.

NT Real-time Scan Service

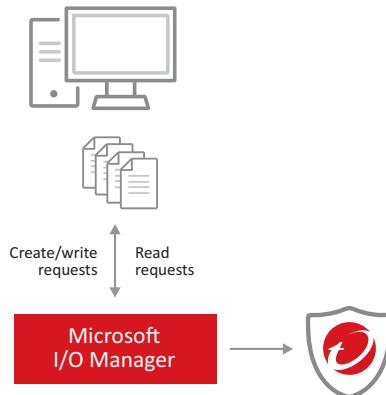
The NT Real-time Scan Service performs on-demand (Manual, Scheduled, Scan Now), and Real-time scanning functionality. This service (`NTRtScan.exe`) uses the following scan engines:

- Virus Scanning API (VSAPI)
- Spyware Scanning API (SSAPI)
- Damage Cleanup Engine (DCE)
- Advanced Threat Scan Engine (ATSE)

This service also assumes responsibility for starting the Unauthorized Change Prevention Service (`TMBMSRV.exe`).

When applications access or create files on the file system, they send information to the Microsoft I/O Manager. This is true for both legitimate applications and malware. To be able to differentiate between legitimate and malicious I/O events, and deal with them if they are of the latter variety, Trend Micro products need a way to monitor these events as they occur, evaluate them, and then take action when necessary.

Apex One registers with the Microsoft I/O Manager to identify file access and modification events on the file system. This registration also grants Apex One access to the file when scanning is required.



Scan Settings

These settings determine which files on the Security Agent host are scanned in each of the four scanning types. Scanning is a resource intensive process. Judicious use of scanning coverage options can strike a balance between security and minimizing the impact of scanning events on the network.

SaaS: Scan settings are configured through Apex Central policies in the service implementation of Apex One.

Each of the four scan types may have slightly different configuration options and include setting collections displayed through the following tabs:

- **Scan Target:** This tab defines how the Security Agent looks for files to scan.
- **Scan Action:** This tab defines the action to be taken when malware is detected.
- **Scan Exclusion:** This tab defines scan exclusions to increase the scanning performance and skip scanning files causing false alarms. When a particular scan type runs, Apex One checks the scan exclusion list to determine which files on the endpoint will be excluded from both virus/malware and spyware/grayware scanning. When you enable scan exclusion, Apex One will not scan a file under the following conditions:
 - The file is found under a specific directory (or any of its sub-directories).
 - The file name matches any of the names in the exclusion list.
 - The file extension matches any of the extensions in the exclusion list.

Real-Time Scan Settings

These settings are used when Real-time scanning is enabled on Security Agents.

Real-Time Scan Target Tab

Real-time Scan Settings

Enable virus/malware scan
 Enable spyware/grayware scan

Target	Action	Scan Exclusion
User Activity on Files		
Scan files being: <input type="text" value="created/modified and retrieved"/> <input type="button" value="▼"/>		
Files to Scan		
<input type="radio"/> All scannable files <input checked="" type="radio"/> File types scanned by IntelliScan (i) <input type="radio"/> Files with the following extensions (use commas to separate entries): <div style="border: 1px solid black; padding: 5px;"> .",,.ACCDDB,.ACE,.AMG,.ARJ,.BAT,.BIN,.BOO,.BOX,.BZ2,.CAB,.CDR,.CDT,.CHM,.CLX,.CLASS,.COM,.CPT,.CSC,.DLL,.DOC,.DOCX,.DOCX,.DOT,.DOTM,.DOTX,.DR V,.DVB,.DWG,.DWL,.EML,.EPOC,.EXE,.GMS,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JPEG,.JPG,.JS,.JSE,.JTD,.JTT,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSI,.MSO,.MST,.NWS,.OBD,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.PM,.POT,.POT </div>		
Scan Settings		
<input type="checkbox"/> Scan floppy disks during shutdown <input type="checkbox"/> Scan network drive <input type="checkbox"/> Scan the boot sector of the USB storage device after plugging in <input type="checkbox"/> Scan all files in removable storage devices after plugging in <input checked="" type="checkbox"/> Quarantine malware variants detected in memory (i) Note: This feature requires that administrators enable the Unauthorized Change Prevention Service and Advanced Protection Service. <input checked="" type="checkbox"/> Scan compressed files Maximum layers: <input type="text" value="2"/> (i) <input checked="" type="checkbox"/> Scan OLE objects Maximum layers: <input type="text" value="3"/> (i) <input checked="" type="checkbox"/> Detect exploit code in OLE files (i)		
Virus/Malware Scan Settings Only		
<input checked="" type="checkbox"/> Enable IntelliTrap (i) <input type="checkbox"/> Enable CVE exploit scanning for files downloaded through web and email channels		

User Activity on Files Section

- **Scan files being:** Files will be scanned when they are created/modified, retrieved or both

Files to Scan Section

- **Files with the following extensions:** Only scan files whose extensions are included in the file extension list. Add new extensions or remove any of the existing extensions.
 - **File types scanned by IntelliScan:** Some files can't be scanned, and cannot be malicious. The Agent won't scan files if it does not know how they can become infected. True file type detection is used by the Agent to identify the type of file it is dealing with, to decide if it is to be scanned, and how to scan it.

IntelliScan is a technique used by the Agent to make a scanning decision based on a list of file types which are considering dangerous, and skip the ones not considered dangerous.

- **All scannable files:** This option also uses true file type detection, but will also scan files even if it cannot determine the true file type.

As an example, the Agent detects a file called `dangerous.txt`. Since text files have no true file type, it will be scanned when **All files** is enabled, but not when **IntelliScan** is enabled as it considers `.txt` files to be safe. If the text file did contain a malicious script, it would be captured by the **All files** scan.

A file called `dangerous.com` is detected. No true file type detection is possible with `.com` files. This file will be scanned when **All files** is enabled, and also when Intelliscan is enabled as `.com` files are considered potentially dangerous.

The examples in this table can provide some examples on choosing between **File types scanned by IntelliScan or All files**.

Extension	Header in file	Considered dangerous	Scanned by IntelliScan	Scanned by All Files	Notes
<code>.exe</code>	yes	yes	yes	yes	Always scanned
<code>.jpeg</code>	yes	no	no	no	<code>.jpeg</code> files could contain malicious information, such as scripts, but to be malicious the application opening those infected files would also need to be compromised to use the malicious information in the file.
<code>.com</code>	no	yes	yes	yes	Always scanned
<code>.txt</code>	no	no	no	yes	A <code>.txt</code> file could contain malicious scripts, but it is not dangerous in <code>.txt</code> form, but could become dangerous if changed to <code>.com</code>

Scan Settings Section

Scan floppy disk during system shutdown: Real-time Scan scans any floppy disk for boot viruses before shutting down the endpoint. This prevents any virus/ malware from executing when a user reboots the endpoint from the disk.

Scan network drive: Scans network drives or folders mapped to the Security Agent endpoint during Manual Scan or Real-time Scan.

Scan the boot sector of the USB storage device after plugging in: Automatically scans only the boot sector of a USB storage device every time the user plugs it in (Real-time Scan).

Scan all files in removable storage devices after plugging in: Automatically scans all files on a USB storage device every time the user plugs it in (Real-time Scan).

Quarantine malware variants detected in memory: Behavior Monitoring scans the system memory for suspicious processes and Real-time Scan maps the process and scans it for malware threats. If a malware threat exists, Real-Time scan quarantines the process and/or file.

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

Scan compressed files: Allows Apex One to scan up to a specified number of compression layers and skip scanning any excess layers. Apex One also cleans or deletes infected files within compressed files. For example, if the maximum is two layers and a compressed file to be scanned has six layers, Apex One scans two layers and skips the remaining four. If a compressed file contains security threats, Apex One cleans or deletes the file.

Note: Apex One treats Microsoft Office 2007 files in Office Open XML format as compressed files. Office Open XML, the file format for Office 2007 applications, uses ZIP compression technologies. If you want files created using these applications to be scanned for viruses/malware, you need to enable scanning of compressed files.

Scan OLE objects: When a file contains multiple Object Linking and Embedding (OLE) layers, Apex One scans the specified number of layers and ignores the remaining layers.

Detect exploit code in OLE files: OLE Exploit Detection heuristically identifies malware by checking Microsoft Office files for exploit code. The specified number of layers is applicable to both Scan OLE objects and Detect exploit code options.

Enable IntelliTrap: Detects and removes virus/malware on compressed executable files. Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files after enabling IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.his option is available only for Real-time Scan.

Enable CVE exploit scanning for files downloaded through web and email channels: Blocks processes that attempt to exploit known vulnerabilities in commercially available products based on the Common Vulnerabilities and Exposures (CVE) system. This option is available only for Real-time Scan.

Real-Time Scan Action Tab

When the Security Agent detects malware, it can take the actions defined on this tab.

Real-time Scan Settings

Enable virus/malware scan
 Enable spyware/grayware scan

Action

Type	1st Action	2nd Action
All types	Clean	Quarantine

Use ActiveAction (i)
 Customize action for probable virus/malware: Quarantine

Use the same action for all virus/malware types
(If the first action is unsuccessful, Apex One performs the second action.)

Type	1st Action	2nd Action
CVE exploit	Pass	
Joke	Quarantine	
Trojans	Quarantine	
Virus	Clean	Quarantine
Test virus	Deny access	
Packer	Quarantine	
Probable malware	Quarantine	
Other malware	Clean	Quarantine

Display a notification on endpoints when virus/malware is detected
 Display a notification on endpoints when probable virus/malware is detected
 Back up files before cleaning
Quarantine directory:

Damage Cleanup Services
 Run cleanup when probable virus/malware is detected

Spyware/Grayware
 Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts
 Deny access
 Display a notification on endpoints when spyware/grayware is detected

Buttons

Save Cancel

Virus/Malware Section

Use ActiveAction: With this option, the administrator relies on Trend Micro action recommendations that are stored within the VSAPI pattern. Trend Micro Anti-virus engineers determine these actions based on their analysis of various malware types. Customizing the action allows the administrator to control the scan action according to the network's specific needs.

Use the same action for all virus/malware types: Select this option if you want the same action performed on all types of virus/malware, except probable virus/malware. If you choose **Clean** as the first action, select a second action that Apex One performs if cleaning is unsuccessful. If the first action is not **Clean**, no second action is configurable. If you choose Clean as the first action, Apex One performs the second action when it detects probable virus/malware.

Use a Specific Action for Each Virus/Malware Type: Manually select a scan action for each virus/malware type. For all virus/malware types except probable virus/malware, all scan actions are available. If you choose **Clean** as the first action, select a second action that Apex One performs if cleaning is unsuccessful. If the first action is not **Clean**, no second action is configurable.

- **Pass:** The Agent does nothing to the malware.
- **Rename:** Encrypt and rename the infected file. The Agent uses scan engine functions to change the file's extension to .VIR, (or to .VIO, .VI1 and so on). If a virus is found and the virus action is **Rename**, the action performed will be **Clean** or, if uncleanable, **Quarantine**. A compressed file with an infected file inside will be renamed.
- **Quarantine:** The Security Agent moves malware to a quarantine folder to an Agent, and then to a quarantine folder on the Apex One Server.
- **Clean:** Remove the virus code from the file. The Agent can only clean files within ZIP/LHA files up to one layer of compression.
- **Delete:** Delete the infected file. The Agent can delete files within ZIP/LHA file up to 6 layers of compression.
- **Deny Access:** Prevent access to infected file.

Note: Probable malware refers to suspicious files that have some of the characteristics of viruses/malware.

Display a Notification Message When Virus/Malware is Detected: When Apex One detects virus/malware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection. To modify the notification message, select Virus/Malware from the Type drop-down in **Administration > Notifications > Agent**.

Display a Notification Message When Probable Virus/ Malware is Detected: When Apex One detects probable virus/malware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection. To modify the notification message, select Virus/Malware from the Type drop-down in **Administration > Notifications > Agent**.

Back Up Files Before Cleaning: If Apex One is set to clean an infected file, it can first back up the file. This allows you to restore the file in case you need it in the future. Apex One encrypts the backup file to prevent it from being opened, and then stores the file in the identified folder.

Run cleanup when probable virus/malware is detected: You can only select this option if the action on probable virus/malware is not **Pass** or **Deny Access**. For example, if the Security Agent detects probable virus/malware during Real-time Scan and the action is quarantine, the Security Agent first quarantines the infected file and then runs cleanup if necessary. The cleanup type (standard or advanced) depends on your selection.

Spyware/Grayware Section

Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts. After cleaning spyware/grayware, Apex One agents back up spyware/ grayware data, which you can restore if you consider the spyware/ grayware safe to access.

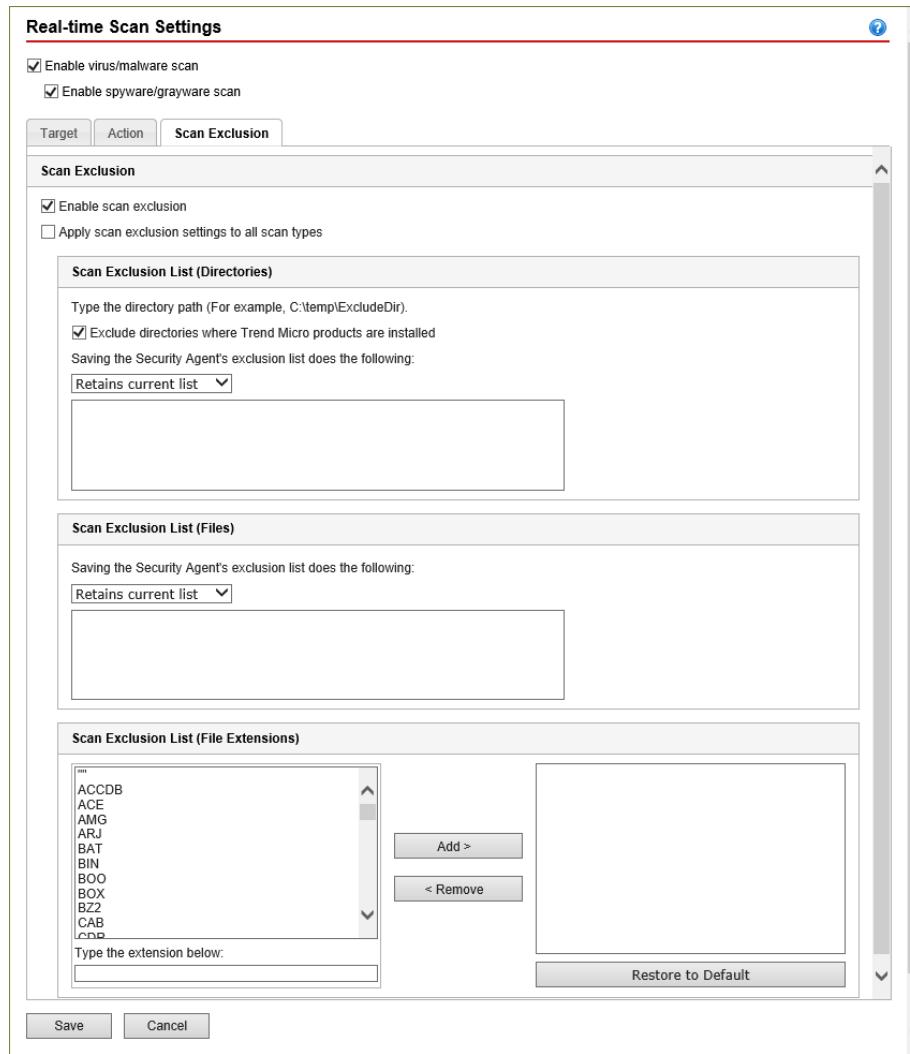
Deny access: Apex One denies access (copy, open) to the detected spyware/grayware components.

Display a notification on endpoints when spyware/grayware is detected: When Apex One detects spyware/grayware during Real-time Scan and Scheduled Scan, it can display a notification message to inform the user about the detection.

Real-Time Scan Exclusion Tab

Configure scan exclusions to increase the scanning performance and skip scanning files causing false alarms. When a particular scan type runs, Apex One checks the scan exclusion list to determine which files on the endpoint will be excluded from both virus/malware and spyware/grayware scanning.

Scan exclusions are stored in the Windows Registry on the endpoint computer.



Scan Exclusion Section

Enable scan exclusions: Enables the use of the Scan exclusions described on this tab.

Apply scan exclusion settings to all scan types: Enables the scan exclusions list to be used, regardless of the scan type.

Scan Exclusion List (Directories): Apex One will not scan all files found under a specific directory on the computer. You can specify a maximum of 256 directories. By excluding a directory from scans, Apex One automatically excludes all of the directory's sub-directories from scans.

- **Exclude directories where Trend Micro products are installed:** If you select this option, Apex One automatically excludes the directories of many Trend Micro products from scanning.

Scan Exclusion List (Files): Apex One will not scan a file if its file name matches any of the names included in this exclusion list. If you want to exclude a file found under a specific location on the endpoint, include the file path, such as C:\Temp\sample.jpg. You can specify a maximum of 256 files.

Scan Exclusion List (File Extensions): Apex One will not scan a file if its file extension matches any of the extensions included in this exclusion list. You can specify a maximum of 256 file extensions. A period (.) is not required before the extension.

- 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??.

Note: Real-time Scan does not support the use of wildcard characters when specifying extensions.

Manual Scan Settings

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the Apex One agent console. The time it takes to complete scanning depends on the number of files to scan and the Apex One agent endpoint's hardware resources.

Manual Scan Target Tab

The screenshot shows the 'Manual Scan Settings' dialog box. At the top, there are three tabs: 'Target' (selected), 'Action', and 'Scan Exclusion'. Below the tabs, the 'Files to Scan' section is expanded, showing three options: 'All scannable files' (radio button), 'File types scanned by IntelliScan' (radio button selected), and 'Files with the following extensions' (checkbox). A list box contains numerous file extensions separated by commas. The 'Scan Settings' section is also expanded, containing several checkboxes and dropdown menus for 'Scan hidden folders', 'Scan network drive', 'Scan compressed files' (with a dropdown for 'Maximum layers' set to 2), 'Scan OLE objects' (with a dropdown for 'Maximum layers' set to 3), and 'Detect exploit code in OLE files'. The 'Virus/Malware Scan Settings Only' section is partially visible. At the bottom, there are 'Save' and 'Cancel' buttons.

Scan Settings Section

Scan hidden folders: Allows Security Agents to detect and then scan hidden folders on the endpoint during Manual Scan

Scan boot area: Scans the boot sector of the hard disk for virus/malware during Manual Scan, Scheduled Scan and Scan Now.

CPU Usage Section

Apex One can pause after scanning one file and before scanning the next file. This setting is used during Manual Scan, Scheduled Scan, and Scan Now.

- **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

If you choose **Medium** or **Low**, when scanning is launched and CPU consumption is within the threshold (50% or 20%), Apex One will not pause between scans, resulting in faster scanning time. Apex One uses more CPU resource in the process but because CPU consumption is optimal, endpoint performance is not drastically affected. When CPU consumption begins to exceed the threshold, Apex One pauses to reduce CPU usage, and stops pausing when consumption is within the threshold again. If you choose High, Apex One does not check the actual CPU consumption and scans files without pausing.

Manual Scan Action Tab

Manual Scan Settings

Virus/Malware								
<input checked="" type="radio"/> Use ActiveAction (i) <input type="checkbox"/> Customize action for probable virus/malware: <select>Quarantine</select> <input type="radio"/> Use the same action for all virus/malware types <small>(If the first action is unsuccessful, Apex One performs the second action.)</small> <table border="1"> <thead> <tr> <th>Type</th> <th>1st Action</th> <th>2nd Action</th> </tr> </thead> <tbody> <tr> <td>All types</td> <td>Clean</td> <td>Quarantine</td> </tr> </tbody> </table> <input type="radio"/> Use a specific action for each virus/malware type			Type	1st Action	2nd Action	All types	Clean	Quarantine
Type	1st Action	2nd Action						
All types	Clean	Quarantine						
<input checked="" type="checkbox"/> Back up files before cleaning <input type="text"/> Quarantine directory: HTTP://dc2016.trend.local								
Damage Cleanup Services <table border="1"> <tr> <td>Cleanup type:</td> </tr> <tr> <td><input type="radio"/> Standard cleanup</td> </tr> <tr> <td><input checked="" type="radio"/> Advanced cleanup</td> </tr> <tr> <td><input type="checkbox"/> Run cleanup when probable virus/malware is detected</td> </tr> </table>			Cleanup type:	<input type="radio"/> Standard cleanup	<input checked="" type="radio"/> Advanced cleanup	<input type="checkbox"/> Run cleanup when probable virus/malware is detected		
Cleanup type:								
<input type="radio"/> Standard cleanup								
<input checked="" type="radio"/> Advanced cleanup								
<input type="checkbox"/> Run cleanup when probable virus/malware is detected								
Spyware/Grayware <table border="1"> <tr> <td><input checked="" type="radio"/> Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts</td> </tr> <tr> <td><input type="radio"/> Pass: Apex One logs the spyware/grayware detection for assessment</td> </tr> </table>			<input checked="" type="radio"/> Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts	<input type="radio"/> Pass: Apex One logs the spyware/grayware detection for assessment				
<input checked="" type="radio"/> Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts								
<input type="radio"/> Pass: Apex One logs the spyware/grayware detection for assessment								
<input type="button"/> Save <input type="button"/> Cancel								

Virus/Malware Section

Damage Cleanup Services: Damage Cleanup Services cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, and viral files). The Agent triggers Damage Cleanup Services before or after virus/malware scanning, depending on the scan 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. The Security Agent also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV and rootkit behavior.

Manual Scan Exclusion Tab

Manual Scan Settings

Target Action Scan Exclusion

Scan Exclusion

Enable scan exclusion
 Apply scan exclusion settings to all scan types

Scan Exclusion List (Directories)

Exclude directories where Trend Micro products are installed
Saving the Security Agent's exclusion list does the following:
Retains current list ▾

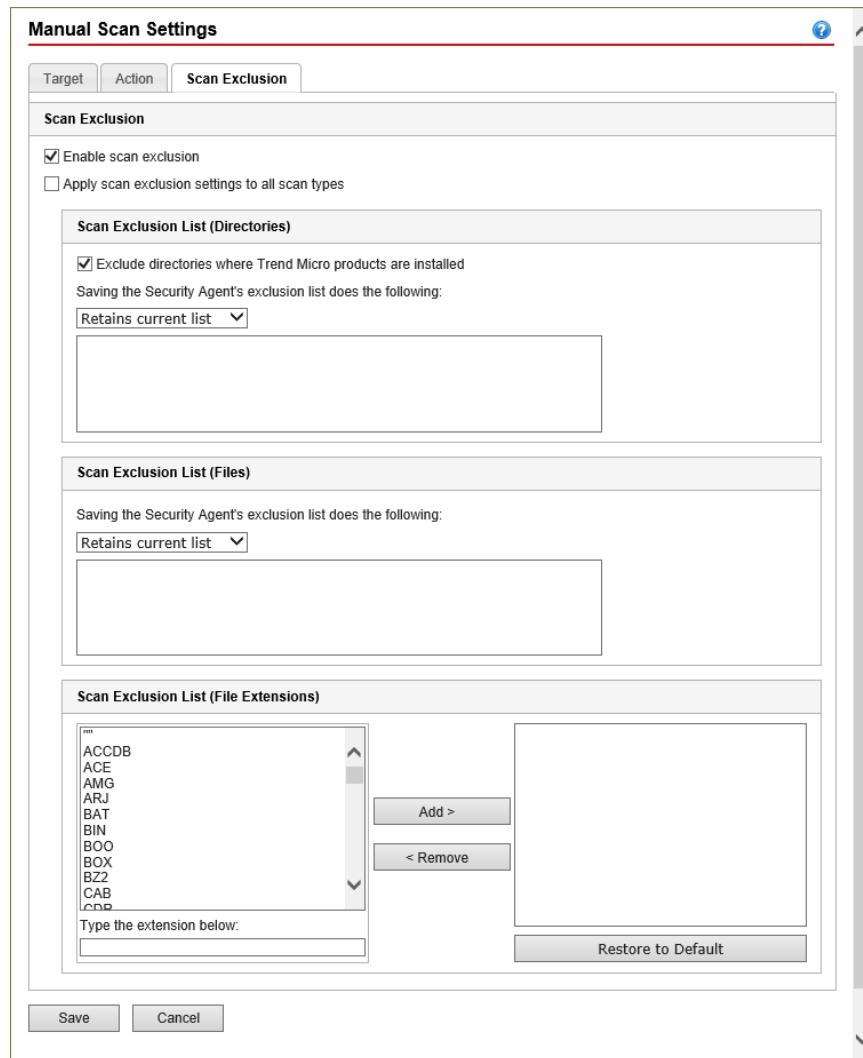
Scan Exclusion List (Files)

Saving the Security Agent's exclusion list does the following:
Retains current list ▾

Scan Exclusion List (File Extensions)

ACCDB
ACE
AMG
ARJ
BAT
BIN
BOO
BOX
BZ2
CAB
CAB
Type the extension below:
Save Cancel

Add >
< Remove
Restore to Default



Scheduled Scan Settings

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans on the agent and improve scan management efficiency.

Scheduled Scan Target Tab

The dialog box is titled "Scheduled Scan Settings". It has a "Target" tab selected. Under "Schedule", the "Weekly, every Monday" option is chosen with a start time of 12:00. The "Files to Scan" section includes options for "All scannable files" and "File types scanned by IntelliScan". A list of file extensions is provided: ".ACCDB,.ACE,.AMG,.ARJ,.BAT,.BIN,.BOO,.BOX,.BZ2,.CAB,.CDR,.CDT,.CHM,.CLA,.CLASS,.COM,.CPT,.CSC,.DLL,.DOC,.DOCM,.DOCX,.DOT,.DOTM,.DOTX,.DR^V,.DVB,.DWG,.DWT,.EML,.EPOC,.EXE,.GMS,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JPEG,.JPG,.JS,.JSE,.JTD,.JTT,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSI,.MSO,.MST,.NWS,.OBD,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.PM,.POT,.POT". The "Scan Settings" section contains checkboxes for "Scan compressed files" (checked, max layers 2), "Scan OLE objects" (checked, max layers 3), and "Detect exploit code in OLE files" (checked). The "Virus/Malware Scan Settings Only" section has a checked checkbox for "Scan boot area". The "CPU Usage" section allows pausing between file scans based on CPU consumption levels (High, Medium, Low). At the bottom are "Save" and "Cancel" buttons.

Schedule Section

Configure how often (daily, weekly, or monthly) and what time Scheduled Scan will run. For monthly Scheduled Scans, you can choose either a particular day of a month or a day of a week and the order of its occurrence.

Scheduled Scan Action Tab

Scheduled Scan Settings

Enable virus/malware scan
 Enable spyware/grayware scan

Action

Type	1st Action	2nd Action
All types	Clean	Quarantine

Use ActiveAction [?](#)
 Customize action for probable virus/malware: Quarantine

Use the same action for all virus/malware types
(If the first action is unsuccessful, Apex One performs the second action.)

Type	1st Action	2nd Action
Joke	Quarantine	
Trojans	Quarantine	
Virus	Clean	Quarantine
Test virus	Pass	
Packer	Quarantine	
Probable malware	Quarantine	
Other malware	Clean	Quarantine

Display a notification on endpoints when virus/malware is detected
 Display a notification on endpoints when probable virus/malware is detected
 Back up files before cleaning
Quarantine directory:

Damage Cleanup Services

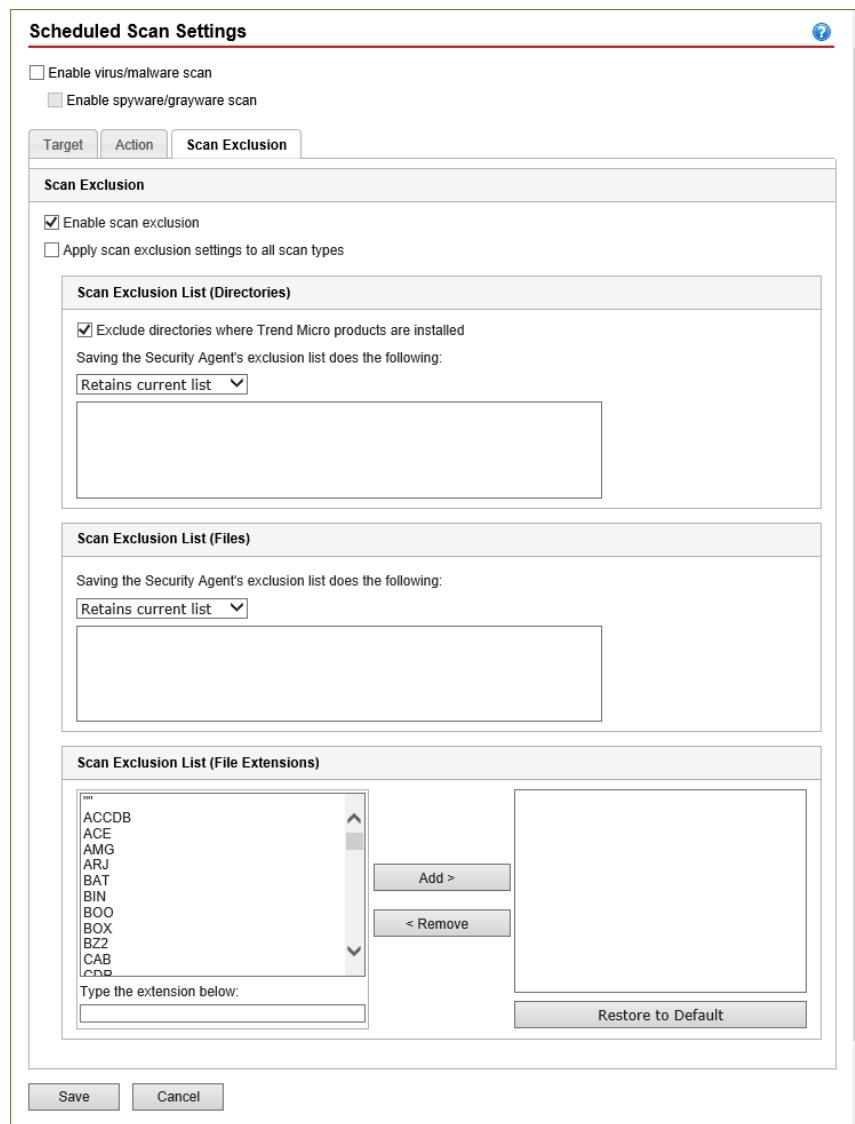
Cleanup type:
 Standard cleanup
 Advanced cleanup
 Run cleanup when probable virus/malware is detected

Spyware/Grayware

Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts
 Pass: Apex One logs the spyware/grayware detection for assessment

Buttons: Save, Cancel

Scheduled Scan Exclusion Tab



Scan Now Settings

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

Scan Now Target Tab

Scan Now Settings

Enable virus/malware scan
 Enable spyware/grayware scan

Target **Action** **Scan Exclusion**

Files to Scan

All scannable files
 File types scanned by IntelliScan [\(i\)](#)
 Files with the following extensions (use commas to separate entries):
".",ACCDB,ACE,AMG,ARJ,BAT,BIN,BOX,BZ2,CAB,CDR,CDT,CHM,CLA,CLASS,COM,CPT,CSC,DLL,DOC,DOCM,DOCX,DOT,DOTM,DOTX,DRV,DVB,DWG,DWT,EML,EPIC,EXE,GMS,GZ,HLP,HTA,HTM,HTML,HTT,IPI,JAR,JPEG.JPG,JS,JSE,DTD,TTT,LNK,LZH,MDB,MPD,MPP,MPT,MSG,IMSI,MSO,MST,NWS,OBD,OCX,OFT,OVL,PDF,PHP,PIF,PL,PM,POT,POT

Scan Settings

Scan compressed files
Maximum layers: [\(i\)](#)

Scan OLE objects
Maximum layers: [\(i\)](#)
 Detect exploit code in OLE files [\(i\)](#)

Virus/Malware Scan Settings Only

Scan boot area

CPU Usage

For agent endpoints that run CPU-intensive applications, Apex One can pause between file scans to free up CPU resources.

High: scan files one after another without pausing
 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

Save **Cancel**

Scan Now Action Tab

Scan Now Settings

Enable virus/malware scan
 Enable spyware/grayware scan

Action

Use ActiveAction [\(i\)](#)
 Customize action for probable virus/malware: **Quarantine** ▾
 Use the same action for all virus/malware types
 (If the first action is unsuccessful, Apex One performs the second action.)

Type	1st Action	2nd Action
All types	Clean	Quarantine

Use a specific action for each virus/malware type

Type	1st Action	2nd Action
Joke	Quarantine	Quarantine
Trojans	Quarantine	Quarantine
Virus	Clean	Quarantine
Test virus	Pass	Pass
Packer	Quarantine	Quarantine
Probable malware	Quarantine	Quarantine
Other malware	Clean	Quarantine

Back up files before cleaning
 Quarantine directory: **HTTP://dc2016.trend.local**

Damage Cleanup Services

Cleanup type:
 Standard cleanup
 Advanced cleanup
 Run cleanup when probable virus/malware is detected

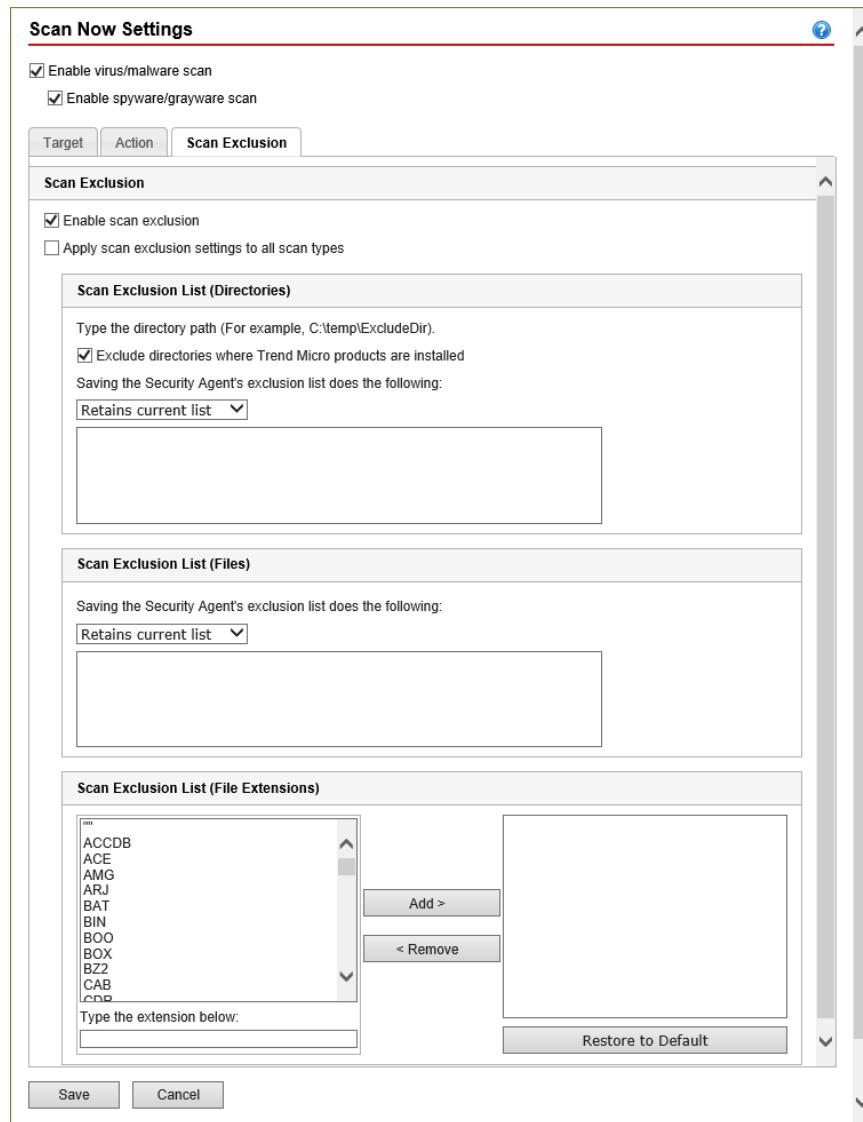
Spyware/Grayware

Clean: Apex One terminates processes or delete registries, files, cookies, and shortcuts
 Pass: Apex One logs the spyware/grayware detection for assessment

Buttons

Save **Cancel**

Scan Now Scan Exclusion Tab



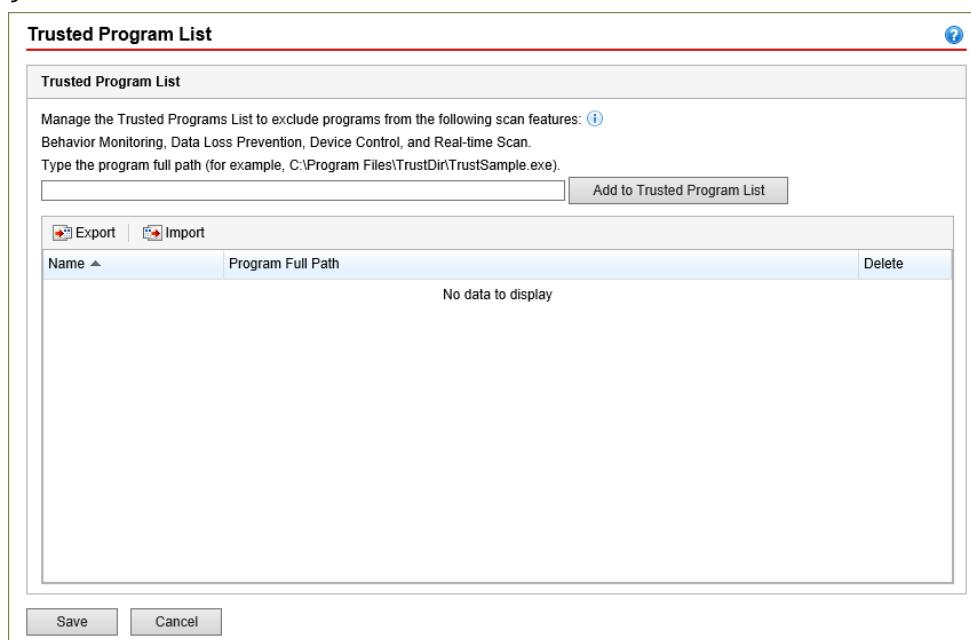
Trusted Program List

You can configure Security Agents to skip scanning of trusted processes during Real-time, Behavior Monitoring, Data Leak Prevention and Device Control scans (Scheduled, Manual and Scan Now scans do not make use of the Trusted Program List). Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints.

You can add program files to the Trusted Programs List if the following requirements are met:

- The program file is not located in the Windows system folder.
- The program file has a valid digital signature.

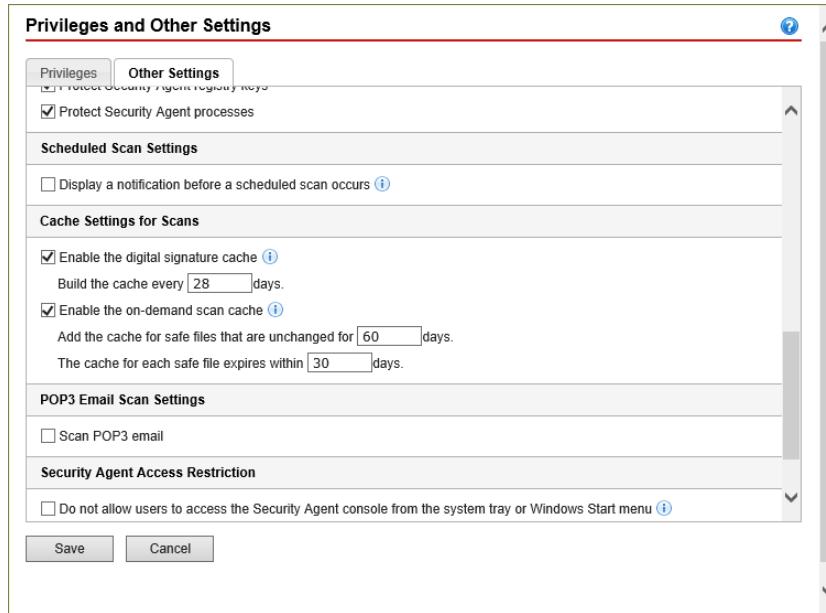
In the Apex One Web Management console, click **Agents > Agent Management** and right-mouse click specific domains or Agents. Click **Settings > Trusted Program List** and type the full program path of the program to exclude from the list.



Scan Caching

The Security Agent can build a digital signature and on-demand scan cache files to improve its scan performance. When an on-demand scan runs, the Security Agent first checks the digital signature cache file and then the on-demand scan cache file for files to exclude from the scan. Scanning time is reduced if a large number of files are excluded from the scan.

In the Apex One Web Management console, click **Agents > Agent Management** and right-mouse click the root domain, specific domains or Agents. Click **Settings > Privileges and Other Settings**.



Digital Signature Cache

Agents do not scan files whose signatures have been added to the digital signature cache file.

The Security Agent uses the same Digital Signature Pattern used for Behavior Monitoring to build the digital signature cache file. The Digital Signature Pattern contains a list of files that Trend Micro considers trustworthy and therefore can be excluded from scans.

Agents build the digital signature cache file according to a schedule, which is configurable from the Web Management console. Agents do this to:

- Add the signatures of new files that were introduced to the system since the last cache file was built.
- Remove the signatures of files that have been modified or deleted from the system.

During the cache building process, Agents check the following folders for trustworthy files and then adds the signatures of these files to the digital signature cache file:

- %PROGRAMFILES%
- %WINDIR%

Other folders are not checked for trustworthy files. The cache building process does not affect the endpoint's performance because Agents use minimal system resources during the process. Agents are also able to resume a cache building task that was interrupted for some reason (for example, when the host machine is powered off or when a wireless endpoint's AC adapter is unplugged).

On-demand Scan Cache

Security Agents do not scan files whose caches have been added to the on-demand scan cache file.

Each time scanning runs, the Security Agent checks the properties of threat-free files. If a threat-free file has not been modified for a certain period of time (the time period is configurable), the Security Agent adds the cache of the file to the on-demand scan cache file. When the next scan occurs, the file will not be scanned if its cache has not expired.

The cache for a threat-free file expires within a certain number of days (the time period is also configurable). When scanning occurs on, or after the cache expiration, the Security Agent removes the expired cache and scans the file for threats. If the file is threat-free and remains unmodified, the cache of the file is added back to the on demand scan cache file. If the file is threat-free but was recently modified, the cache is not added and the file will be scanned again on the next scan.

The cache for a threat-free file expires to prevent the exclusion of infected files from scans, as illustrated in the following examples:

- It is possible that a severely outdated pattern file may have treated an infected, unmodified file as threat-free. If the cache does not expire, the infected file remains in the system until it is modified and detected by Real-time Scan.
- If a cached file was modified and Real-time Scan is not functional during the file modification, the cache needs to expire so that the modified file can be scanned for threats.

The number of caches added to the on-demand scan cache file depends on the scan type and its scan target. For example, the number of caches may be less if the Security Agent only scanned 200 of the 1,000 files in the endpoint during Manual Scan.

If on-demand scans are run frequently, the on-demand scan cache file reduces the scanning time significantly. In a scan task where all caches are not expired, scanning that usually takes 12 minutes can be reduced to 1 minute. Reducing the number of days a file must remain unmodified and extending the cache expiration usually improve the performance. Since files must remain unmodified for a relatively short period of time, more caches can be added to the cache file. The caches also expire longer, which means that more files are skipped from scans.

If on-demand scans are seldom run, you can disable the on-demand scan cache since caches would have expired when the next scan runs.

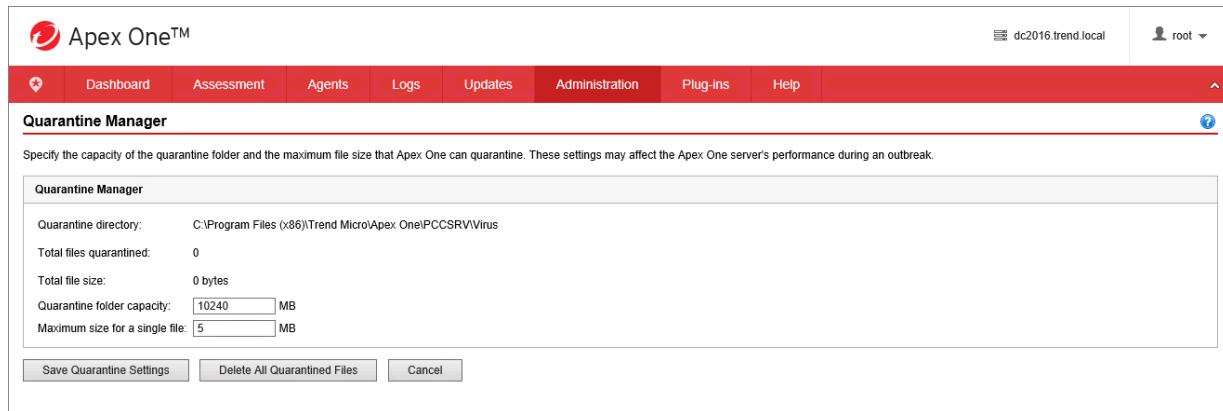
Quarantining Detected Malware

The Quarantine action instructs Security Agents to physically send detected malware to the Apex One Server, where it is stored in a centralized quarantine folder for future analysis.

When the Agent detects a malware instance that it is set to quarantine, it moves the file to its ... \Security Agent\SUSPECT folder. Afterwards, the Agent initiates the process of transferring the malware to a folder called ... \VIRUS on the Apex One Server, where it is rendered inert for safe storage.

Lesson 8: Protecting Endpoint Computers From Malware

Apex One administrators control how this folder is used by way of the **Quarantine Manager**. Click **Administration > Settings > Quarantine Manager**.



The screenshot shows the Apex One web interface with a red header bar containing links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root' on the right. The main content area has a white background with a red header titled 'Quarantine Manager'. Below it, a note says: 'Specify the capacity of the quarantine folder and the maximum file size that Apex One can quarantine. These settings may affect the Apex One server's performance during an outbreak.' A table displays current settings:

Quarantine directory:	C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Virus
Total files quarantined:	0
Total file size:	0 bytes
Quarantine folder capacity:	10240 MB
Maximum size for a single file:	5 MB

At the bottom are three buttons: 'Save Quarantine Settings', 'Delete All Quarantined Files', and 'Cancel'.

SaaS: The Quarantine Manager is not available in the service implementation of Apex One.

Two aspects of the quarantine folder are configurable:

- Capacity of the quarantine folder
- The maximum size of the individual malware that the server will accept from an Security Agent

Files stored in the Quarantine folder are renamed according to the following naming convention:

```
<Security Agent hostname>_<server upload timestamp in Epoch/Unix  
time>.<sequence>
```

The sequence number differentiates files that were uploaded to the server within the same second. To prevent infected files from being opened, Apex One encrypts the file before quarantining a file or when backing up a file before cleaning it.

Restoring Quarantined Files

Apex One provides mechanisms to decrypt and then restore the files in case you believe that a detection was inaccurate.

File	Description
Quarantined files on the Agent endpoint	These files are found in the ...\\SUSPECT\\Backup folder and are automatically purged after 7 days. These files are also uploaded to the designated Quarantine folder on the Apex One Server.
Quarantined files in the quarantine folder on the Server	By default, this folder is located on the Apex One Server computer in the ...\\PCCSRV\\Virus folder.
Backed up encrypted files	These are the backup of infected files that Apex One was able to clean. These files are found in the ...\\Backup folder on the Agent endpoint. To restore these files, users need to move them to the ...\\SUSPECT\\Backup folder on the Agent endpoint. Apex One only backs up and encrypts files before cleaning if you select Backup files before cleaning in Agents > Agent Management > Settings > Scan Settings > {Scan Type} > Action tab.

Note: Restoring an infected file may spread the virus/malware to other files and computers. Before restoring the file, isolate the infected endpoint and move important files on this endpoint to a backup location.

Central Quarantine Restore

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.

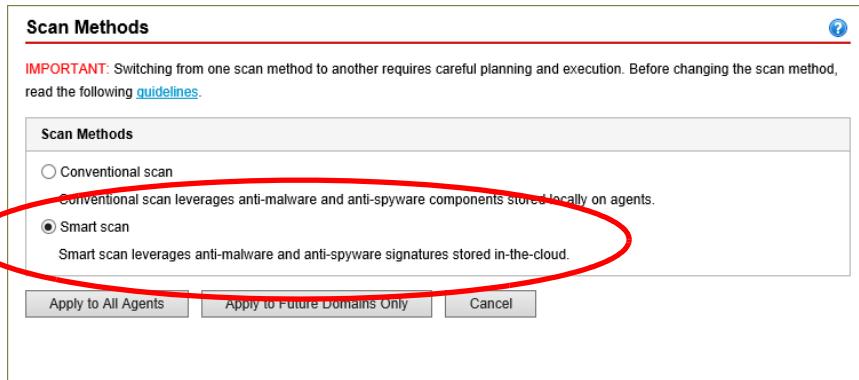
If the file is on the Security Agent, the VSEncode tool can be used to restore files from quarantine.

- 1 In Windows Explorer, navigate to the following folder on the Security Agent computer:
C:\\Program Files (x86)\\Trend Micro\\Security Agent\\
- 2 Double-click VSEncode.exe. A list of files found in the ...\\SUSPECT\\Backup folder is displayed.
- 3 Click to select a file and click **Restore**.
- 4 Specify the folder where to restore the file and click **OK**. The file is restored to the specified folder.

Note: The tool can only restore one file at a time.

Smart Scan

In addition to conventional pattern-based detection, Apex One offers Smart Scan, as a feature of the Trend Micro Smart Protection Network.



SaaS: Smart Scan settings are configured through Apex Central policies in the service implementation of Apex One.

Smart Scan shifts much of the malware and spyware scanning functionality to a Smart Protection Server. It keeps local pattern files small and reduces the size and number of updates required by Agents.

The move to in-the-cloud protection is driven by two considerations:

- Malware creation is outstripping traditional malware knowledge deployment. By the time a malware is recognized, it has already changed.
- As patterns grow in power, they grow in size. An inescapable consequence of a rise in the number of malware is accelerated growth of anti-malware patterns. As things currently stand, network administrators now have to be careful about when they schedule their updates, to avoid network disruption.

To address these conditions, Trend Micro re-thought how it deployed malware knowledge to its protection products. Instead of pre-deploying anti-malware knowledge to the end points, with the resulting deployment delay and bandwidth issues, this knowledge is now deployed on-demand from a centralized database that is updated more frequently than traditional methods through a mechanism called **File Reputation**.

Smart Scan provides the following features and benefits:

- Reduces the overall time it takes to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only needs to be delivered to the cloud and not to many endpoints
- Reduces the cost and overhead associated with corporate-wide pattern deployments
- Lowers kernel memory consumption on endpoints. Consumption increases minimally over time
- Provides fast, real-time security status lookup capabilities in the cloud and therefore increases overall protection

By default this option is set to on. Agents that are implementing the Smart Protection Network solution use the following components:

- **Smart Scan Agent Pattern**

The pattern file contains complete threat information for all malware that is currently *in the wild*.

- **Smart Query Filter**

This compressed index file references complete threat information that is stored in the Smart Scan Pattern on the Smart Protection Server.

- **Smart Scan Pattern**

This pattern file stores information for virus confirmation and actions to proceed in case of cleaning and is located on the Smart Protection Server.

File Reputation

File Reputation is an implementation of malware identification through the use of Cyclic Redundancy Check (CRC) values. Cyclic Redundancy Check information can be divided into two parts:

- **Part 1** - Used for initial malware **identification**
- **Part 2** - Used for malware **confirmation**

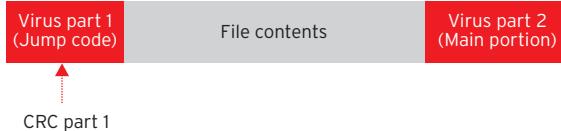
The following diagram represents a file that has been infected by a virus.



When a virus infects a file, it typically appends a part of itself to the front of the file. This serves two purposes:

- To keep other instances of the virus from re-infecting an already infected file, thereby ensuring efficient propagation.
- To ensure that the virus code in the file runs first, whenever the file is opened this front-appended portion often contains a jump command to the main portion of the virus, which is located elsewhere in the file.

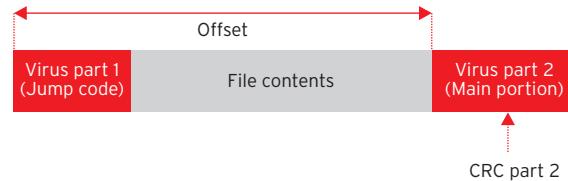
For this kind of virus, the CRC information in part 1 would be used to identify the first part of the virus added to the front of the file.



The scan engine uses this information to detect if a file has been infected with a specific virus.

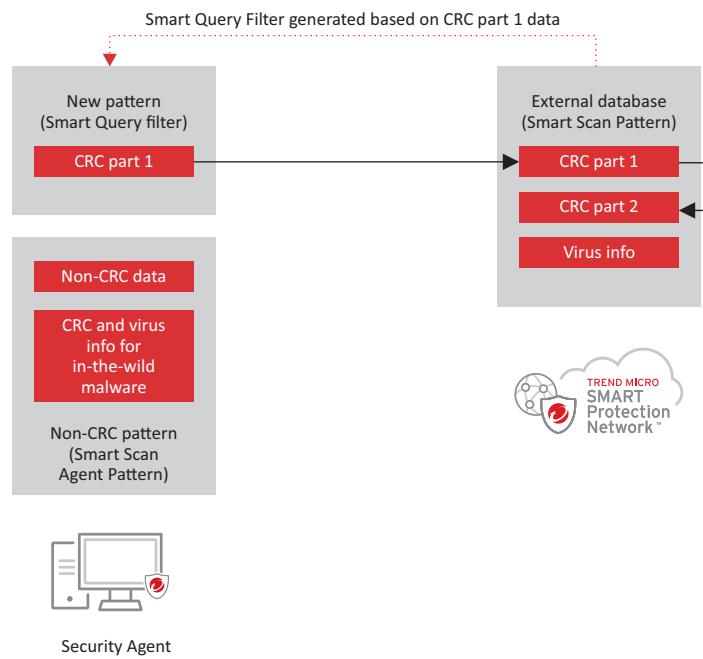
After detecting the first part of the virus using part 1 of the CRC information, the scan engine looks for the corresponding part 2 of the CRC for additional identification information about the remaining portion of the virus and to confirm that the file is indeed a virus.

To locate part 2 of the CRC information, the scan engine requires information about its expected location within the file. This information is stored in what pattern builders call the CRC table, and the location within the file is called its offset.



Once the virus has been identified, the scan engine requires information to clean/remove the virus. This information comes from the Smart Protection Server. Once the scan engine retrieves the cleaning/removal information that corresponds to the identified virus, it is then able to take action against the virus.

File Reputation addresses the needs enumerated in the previous section by de-constructing the existing pattern.



Note the following changes to the existing pattern:

- CRC and virus information is still stored locally for malware that are classified as *in-the-wild*. This means that the only malware information that is available locally corresponds to malware that is actively doing harm. This information resides in the Smart Scan Agent Pattern file.
- CRC and virus information for malware that are no longer considered *in-the-wild* is moved to an external database called the Smart Scan Pattern. This pattern contains all the CRC Parts 1 and 2 information of the traditional pattern. Non-CRC data is also stored in the Smart Scan Pattern.

- A compressed copy of CRC Part 1 information, for not-in-the-wild malware, is moved to a new pattern called the Smart Query Filter, which the Security Agent uses to determine when to query the external database for matching Part 2 information. This serves as a kind of index to the information in the external database.

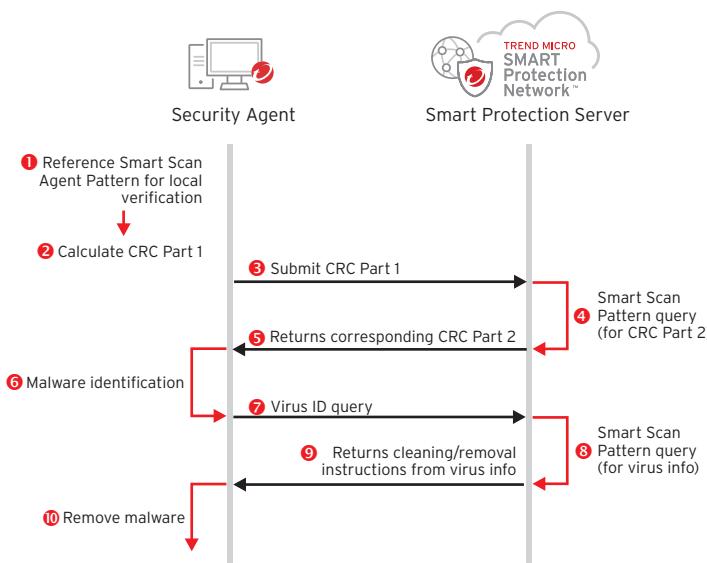
Note: Both the Smart Query Filter and Smart Scan Agent Pattern reside on the Security Agent.

Querying the File Reputation Database

Components on the Security Agent are responsible for looking for malware and taking action upon them when found. However, the knowledge required to identify malware does not completely reside within the product itself, part of this knowledge is located externally.

The CRC database contains CRC information that corresponds to known malware. This database resides on the Smart Protection Server. Security Agents can either refer to the global Trend Micro Smart Protection Network, or a local Smart Protection Server if it is available.

These elements work together as shown below.



1 Reference Smart Scan Agent Pattern

Each time the Security Agent scans a file, it first uses the local pattern file to check if the scanned content contains malware and obtain cleaning instructions. It does this by referencing information in the **Smart Scan Agent Pattern**. The Agent uses this to perform the In-the-wild verification and clean/remove these active viruses.

2 Calculate CRC Part 1

If the content looks suspicious but the malware cannot be detected and cleaned using the local pattern files, it calculates a Cyclic Redundancy Check (CRC) sum for the initial portion of the content (CRC Part 1).

3 Submit CRC Part 1

The Agent submits the CRC Part 1 sum to the local or in-the-cloud File Reputation Server on the Smart Protection network to query the malware database for all records matching the calculated CRC Part 1.

4 Smart Scan Pattern query for CRC Part 2

In this step, the Smart Protection Server uses the CRC Part 1 value to query for matching CRC Part 2 information, which enables the scan engine to confirm that the suspect file is indeed malware.

The CRC Part 2 information is stored in a database on the Smart Protection Server called the **Smart Scan Pattern**.

By design, the Agent only waits for a response from the Smart Protection Server for a specific period of time (a maximum of 500 milliseconds). For this brief period, the scan engine locks the file. If the scan engine is unable to query the Smart Protection Server, the server-side processing portion of this step does not occur, and the Agent attempts to query another Smart Protection Server if one is available, or proceeds using offline protection.

5 Reply with Corresponding CRC Part 2

If the CRC information sent in the query matches CRC Part 1 information in the Smart Scan Pattern, the Smart Protection Server returns all the corresponding CRC Part 2 records to the Agent.

6 Malware identification

When the Agent receives the CRC Part 2 information from the Smart Protection Server, it passes the information to the scan engine to perform matching operations. If no match is found, the file is safe and the scanning process ends.

7 Virus ID query

If a match is found, the Agent sends a second query to the Smart Protection Server for information about how to clean/remove the malware. Instead of sending CRC information like in the first query, the Agent sends the Virus ID of the CRC Part 2 record of the malware that was detected.

8 Smart Scan Pattern query

The Smart Protection Server then searches for the virus information that corresponds to this Virus ID submitted to retrieve cleaning instructions.

9 Cleaning instructions returned to Agents

Once the virus information is retrieved, the Smart Protection Server returns this to the Agent for use by the scan engine.

The Agent waits for a maximum of 500 milliseconds for the Smart Protection Server to reply. If the Agent does not receive a timely reply, the Agent will abandon the primary action, in favor of the secondary action. A failure in this operation would cause the Agent to quarantine the malware instead of cleaning it.

10 Remove Malware

Finally, the Security Agent receives the virus information from the Smart Protection Server, and the scan engine uses this information to clean/remove the virus.

Best Practice: Do not use Smart Scan if the computer doesn't have reliable network connectivity to the Trend Micro Smart Protection Network or your Smart Protection Server.

CRC Caching

The CRC cache contains the following information:

- Malware confirmation CRC information
- Malware removal information (VINFO)

SaaS: CRC caching is not available in the service implementation of Apex One.

Apex One uses both types of information during the local verification step of the File Reputation operation.

The ability of an offline Agent's scan engine to act upon suspected malware is entirely dependent on information in the cache. This information depends on types of cache.

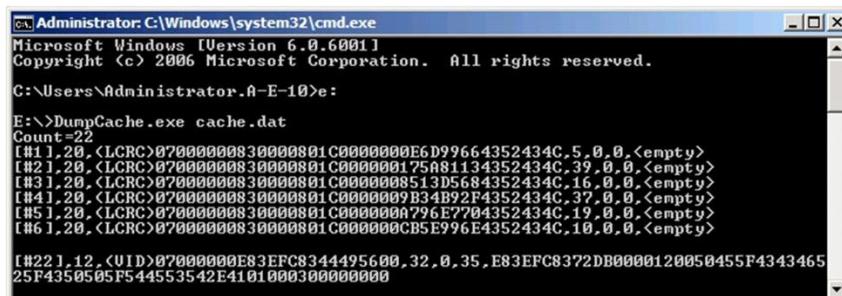
The following table describes what the Security Agent does in each of the following conditions:

CRC info	Virus info	Offline Behavior
X	X	File is entered in suspicious file list for re-scanning, and is allowed to pass. No action is taken upon the file.
✓	X	Since virus information is unavailable, the malware cannot be cleaned. If the first action is set to clean, then the Security Agent will perform the second action.
✓	✓	Security Agent cleans the virus based on information already in the cache.

Malware detected in offline conditions will be re-scanned once access to the Smart Protection Server is restored.

Cache.dat contains a snapshot of the contents of the memory-only CRC cache when the Security Agent shuts down. It serves as a repository of the CRC and VINFO information already retrieved in previous queries. When the Security Agent starts up, it reads this file to re-populate the cache.

The information in cache.dat is written in binary format, so it is unreadable. The only way to read the information that is stored in the CRC cache is by way of a command line tool called DumpCache.exe. A sample of the tool's output is shown below.



```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.A-E-10>:
E:\>DumpCache.exe cache.dat
Count=22
[#:1,20,<LCRC>07000000830000801C0000000E6D99664352434C,5,0,0,<empty>
[#:2,20,<LCRC>07000000830000801C000000175481134352434C,39,0,0,<empty>
[#:3,20,<LCRC>07000000830000801C0000008513D5684352434C,16,0,0,<empty>
[#:4,20,<LCRC>07000000830000801C0000009B34B92F4352434C,37,0,0,<empty>
[#:5,20,<LCRC>07000000830000801C000000A796E7704352434C,19,0,0,<empty>
[#:6,20,<LCRC>07000000830000801C000000CB5E996E4352434C,10,0,0,<empty>
[#:221,12,<VID>07000000E83EFC8344495600,32,0,35,E83EFC8372DB0000120050455F4343465
25F4350505F544553542E4101000300000000

```

The sample above shows Count=22, indicating there were 22 entries in the cache.

CRC Cache Updates

The CRC information that an Security Agent retrieves from the Smart Protection Server is stored in its memory-resident CRC cache. This allows the Agent to re-use information retrieved in previous queries, thereby reducing bandwidth consumption.

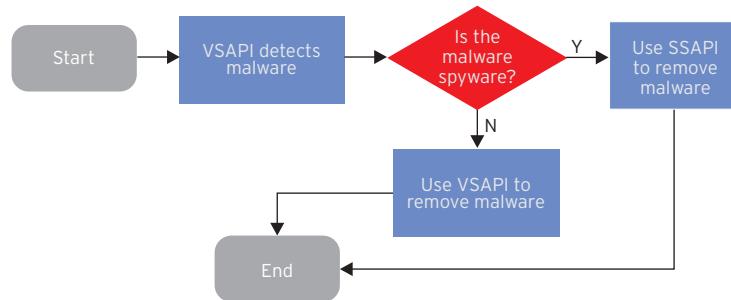
If the Smart Scan pattern on the Smart Protection Server is updated, there is a probability that the information in the cache is rendered either obsolete or incomplete. In which case, the information must either be updated by way of CRC cache updates, or purged entirely and recreated.

Spyware/Grayware Protection

Spyware and grayware comprises applications and components that collect information to be transmitted to a separate system or collected by another application. Spyware/grayware detections, although exhibiting potentially malicious behavior, may include applications used for legitimate purposes such as remote monitoring.

Apex One uses the Spyware Scanning API (SSAPI) to deal with spyware. This scan engine uses a variety of internal scanning functions to remove spyware-related files, as well as the changes these files make in various system areas (for example, Windows registry, shortcuts, etc.).

Ntrtscan.exe is the Security Agent component that is responsible for scanning functionality. For this purpose, it calls both VSAPI and SSAPI scan engines.



VSAPI

VSAPI is responsible for real-time spyware detection. Since spyware always involves a file component, these will still be detectable using conventional file scanning techniques.

Spyware removal, however, requires more than just removal of spyware-related files. Cookies, for example, not only reside in the user's cookie folder but also in a special registry for cookies. To effectively remove cookies, the latter must also be addressed. VSAPI lacks this ability to remove spyware-related alterations in different system areas. This is why SSAPI is part of the process.

SSAPI

Once VSAPI detects the creation of a spyware file-component on the system, it passes this information to `Ntrtscan.exe`, which then calls SSAPI to remove the spyware.

SSAPI can detect spyware based on either signatures or changes from a specific baseline. SSAPI signatures are stored in a definition file.

Enabling SSAPI Logs

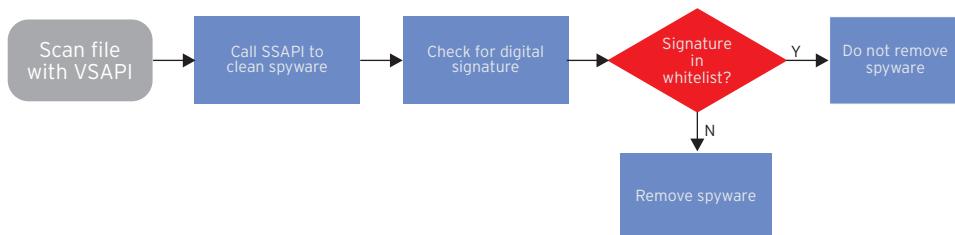
Scanner-specific communications all use SSAPI log entries to show the scanner's actions. To generate these logs, the following registry entry must be added:

```
HKLM\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc  
Dwords: EnableSSAPILog = 1
```

The debug log is created in the location specified for the Security Agent debug log.

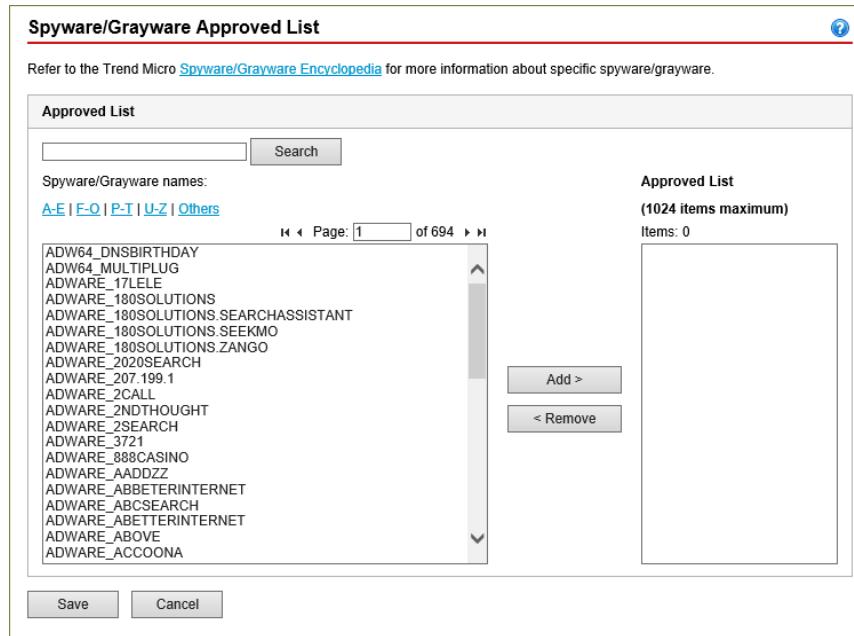
Digital Signatures

SSAPI checks the digital signatures of files that VSAPI recognizes as spyware. If the digital signature of the file identified as spyware exists in the allow list, the file is not removed. This applies to all types of scanning (e.g., real-time, manual, etc.).



Trend Micro maintains a list of known spyware/grayware that can be allowed by adding to your own allow list. Locate the application you would like to approve and add it to the Approved list.

To access the Spyware/Grayware Approved List, click **Agents > Agent Management**. Click **Settings > Spyware/Grayware Approved List**.



The screenshot shows the 'Spyware/Grayware Approved List' page. At the top, there's a note to refer to the Trend Micro [Spyware/Grayware Encyclopedia](#). Below this is a search bar and a 'Search' button. A sidebar on the left lists categories: A-E, F-Q, P-T, U-Z, and Others. The main area displays a large list of spyware/grayware names, with a scroll bar indicating many items. The list includes: ADW64_DNSBIRTHDAY, ADW64_MULTIPLUG, ADWARE_17LELE, ADWARE_180SOLUTIONS, ADWARE_180SOLUTIONS SEARCHASSISTANT, ADWARE_180SOLUTIONS SEEKMO, ADWARE_180SOLUTIONS ZANGO, ADWARE_2020SEARCH, ADWARE_207.199.1, ADWARE_2CALL, ADWARE_2NDTHOUGHT, ADWARE_2SEARCH, ADWARE_3721, ADWARE_888CASINO, ADWARE_AADDZZ, ADWARE_ABETTERINTERNET, ADWARE_ABCSEARCH, ADWARE_ABETTERINTERNET, ADWARE_ABOVE, and ADWARE_ACCONA. To the right, there's an 'Approved List' section showing '(1024 items maximum)' and 'Items: 0'. Buttons for 'Add >' and '< Remove' are present. At the bottom are 'Save' and 'Cancel' buttons.

SaaS: The Spyware/Grayware Approved List is configured through Apex Central policies in the service implementation of Apex One.

A file's digital signature can be seen in its properties, particularly in the digital signature tab.

Damage Cleanup Services

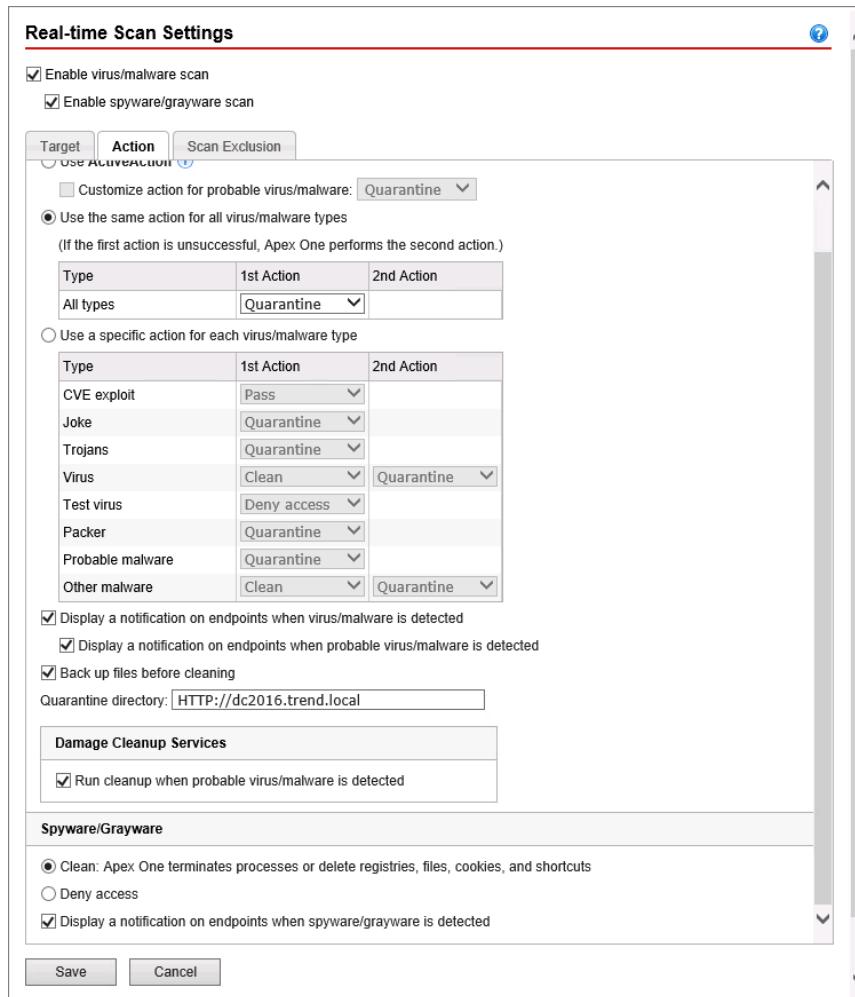
Damage Cleanup Services (DCS) remove files that cannot be cleaned by the Virus Scan Engine, such as files infected with Trojans. Damage Cleanup Services cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, Registry entries, viral files) through a fully-automated process.

Damage Cleanup Services performs the following functions:

- Detects and removes live Trojans
- Kills processes that Trojans create
- Repairs system files that Trojans modify
- Deletes files and applications that Trojans drop

Damage Cleanup Services run automatically in the background, and 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.

Configuration settings for Damage Cleanup Services can be found in **Real-Time Scan Settings > Action > Damage Cleanup Services**.



SaaS: Damage Cleanup Services are configured through Apex Central policies in the service implementation of Apex One.

Damage Cleanup Services does not run cleanup on probable virus/malware unless **Run cleanup when probable virus/malware is detected** is selected. Note that you can only select this option if the action on probable malware is not **Deny Access**.

For example, if the Security Agent detects probable malware during Real-time Scan and the action is quarantine, the Security Agent first quarantines the infected file and then runs cleanup if necessary.

Advanced Cleanup

In addition to the standard cleanup actions, Manual, Scheduled and Scan Now setting also includes an advanced cleanup option. With this enabled, the Security Agent stops activities by rogue security software (also known as FakeAV) and certain rootkit variants. The Security Agent also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV and rootkit behavior.

Damage Cleanup Services Components

Damage Cleanup Services consist of the following engine, template and driver components:

- **Damage Cleanup Engine:** The Damage Cleanup Engine scans for and removes Trojans and Trojan processes. This engine supports 32-bit and 64-bit platforms.
- **Damage Cleanup Template:** The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
- **Early Boot Cleanup Driver:** The Trend Micro Early Boot Cleanup driver loads before the operating system drivers which enables the detection and blocking of boot-type rootkits. After the Security Agent loads, Trend Micro Early Boot Clean Driver calls Damage Cleanup Services to clean the rootkit.

Assessment Mode

To help an administrator study the types of files that are flagged as spyware, Apex One provides an option to prevent Security Agents from deleting spyware, even if they are set to clean.

Unlike other forms of malware, there is little consensus on what constitutes spyware. Cookies are a good example of this. Like other security companies, Trend Micro can detect and remove cookies. However, many claim that cookies are not actually spyware.

Assessment Mode give administrators a chance to fine tune their own policies for files addressed as part of anti-spyware functionality. This assessment period allows the administrator to identify the files that they want excluded from spyware cleaning, and to add them to the Approved List. After the assessment period, the Security Agent implements spyware cleaning functionality.

When in assessment mode, Agents will log spyware/grayware detected during scan, but will not clean spyware/grayware components. Cleaning terminates processes or deletes registries, files, cookies, and shortcuts.

Preventing Outbreaks

To contain outbreaks, Apex One enforces outbreak prevention policies and isolates infected computers until they are completely risk-free. Attack-specific security policies are deployed to prevent or contain outbreaks before pattern files are available.

Outbreak Prevention Policy

Outbreak Prevention security policies can include the following:

- Limit/Deny access to shared folders
- Block Ports (only available/visible if Firewall is enabled)
- Deny write access to files and folders (excludes mapped drives)
- Deny access to executable compressed files
- Create mutual exclusion (mutex) handling on malware processes/files (only available if Unauthorized Change Prevention service is enabled)

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

Note: 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.

Outbreak Notifications

Administrators can be notified when conditions warrant configuring Outbreak Prevention. Click **Administration > Notifications > Outbreak**. Configure the outbreak criteria for different categories of threats.

The screenshot shows the Apex One™ software interface with the following details:

- Header:** Apex One™, dc2016.trend.local, root
- Navigation Bar:** Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, Help
- Section:** Outbreak Notifications
- Criteria Tab:** Criteria (selected), Email, SNMP Trap, NT Event Log
- Virus/Malware:**
 - Outbreak criteria:**
 - Unique sources: 1
Detections: 100
Time period: 24 hour(s)
- Spyware/Grayware:**
 - Outbreak criteria:**
 - Unique sources: 1
Detections: 100
Time period: 24 hour(s)
- Firewall Violations:**
 - Monitor firewall violations on Apex One Security Agents
 - Outbreak criteria:**
 - IDS logs: 100 record(s)
Firewall logs: 100 record(s)
Network virus logs: 100 record(s)
Time period: 3 hour(s)
- Shared Folder Sessions:**
 - Monitor shared folder sessions on your network
 - Shared folder sessions recorded: 0
 - Outbreak criteria:**
 - Shared folder sessions: 100
Time period: 3 minute(s)
- C&C Callbacks:**
 - Outbreak criteria:**
 - Same compromised host
 - C&C risk level: Any risk level Only high
 - Action: Any action
 - Detections: 10
 - Time period: 24 hour(s)
- Buttons:** Save, Cancel

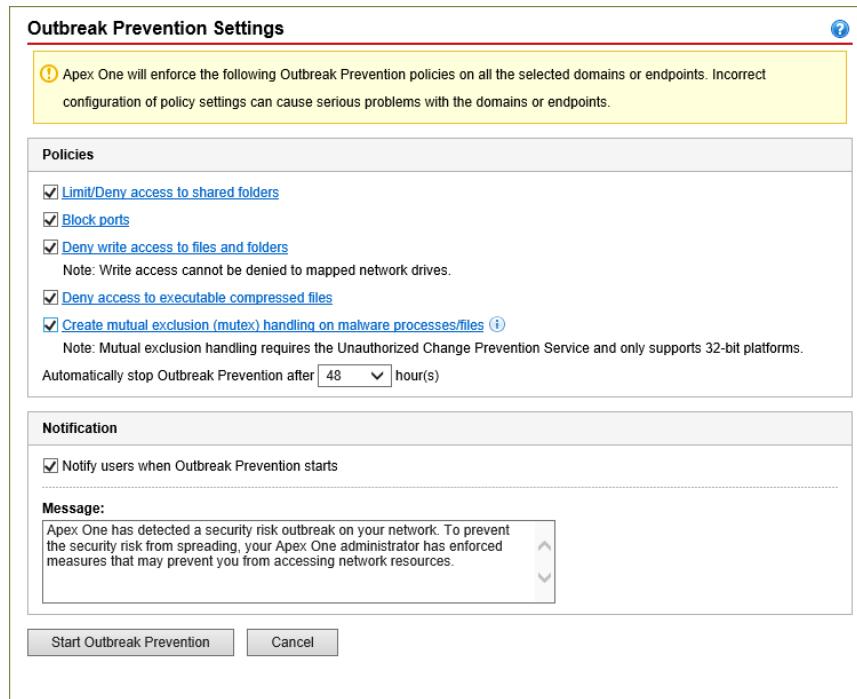
Starting Outbreak Prevention

When warranted, enable Outbreak Prevention to isolate infected endpoint computers. To access the configuration settings for Outbreak Prevention, go to **Agents > Outbreak Prevention**, select the appropriate domain or endpoints and click **Start Outbreak Prevention**.

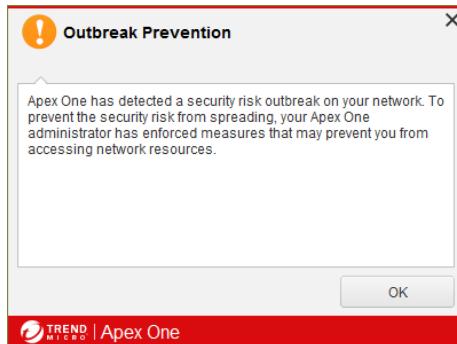
The screenshot shows the Apex One™ software interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root'. Below the navigation bar, the title 'Outbreak Prevention' is displayed. A sub-instruction says 'Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree.' There's a search bar labeled 'Search for endpoints:' with an advanced search link. On the left, an 'Agent tree view' shows a hierarchy: Apex One Server > Trend > Classroom. Under Classroom, several endpoints are listed: CLIENT-01, CLIENT-02, CLIENT-03, DC2016, and WIN2012. The DC2016 entry is selected, and its details are shown in a table. The 'Start Outbreak Prevention' button is highlighted with a red circle. The table includes columns for Domain/Endpoint, Logon User, IP Address, Listening..., Domain H..., Connecti..., and GUID. The DC2016 row has a different background color. At the bottom, there are summary statistics: Number of agents: 5, Agents using smart scan: 5, and Agents using conventional scan: 0.

Domain/Endpoint	Logon User	IP Address	Listening...	Domain H...	Connecti...	GUID
CLIENT-01	CLIENT-01\Administrator	192.168.4.2	21112	Trend\Cla...	Offline	3945081d-396a-402...
CLIENT-02	CLIENT-02\Administrator	192.168.4.4	21112	Trend\Cla...	Online	62a5bd02-c2fb-4da...
CLIENT-03	CLIENT-03\Administrator	192.168.4.6	21112	Trend\Cla...	Online	e2bf9522-ba58-45f...
DC2016	TREND\administrator	192.168.4.1	21112	Trend\Cla...	Online	8223ba62-85c5-4ee...
WIN2012		192.168.4.3	21112	Trend\Cla...	Online	e6edef5f-f406-4783...

Select the items to restrict when outbreak prevention is enabling by selecting them in the **Policies** section of the **Outbreak Prevention Settings**.



In addition, a notification message can be displayed to the users when Outbreak Prevention starts.



Terminating Outbreak Prevention

When you are confident that an outbreak has been contained and that Apex One has cleaned or quarantined all infected files, restore network settings to normal by disabling Outbreak Prevention. Right-mouse click the domain or endpoints using Outbreak Prevention and click **Restore Settings**.

The screenshot shows the Apex One™ interface with the title bar "Apex One™" and the server name "dc2016 trend.local". The user is logged in as "root". The main menu includes Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help.

The "Outbreak Prevention" tab is selected. A message at the top says: "Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree." Below this is a search bar labeled "Search for endpoints:" with an "Advanced search" link.

The "Agent tree view" shows a hierarchy: Apex One Server > Trend > Classroom. Under Classroom, there are five entries: CLIENT-01, CLIENT-02, CLIENT-03, DC2016, and WIN2012. The "DC2016" entry has a context menu open, with the "Restore Settings" option highlighted by a red circle.

The main table lists the agents with columns: Domain/Endpoint, Logon User, IP Address, Listening..., Domain H..., Connecti..., and GUID. The "DC2016" row is selected.

At the bottom, there are status indicators: "Number of agents: 5", "Agents using smart scan: 5", and "Agents using conventional scan: 0".

A message will be displayed on the endpoint computer advising the user that outbreak policies are no longer being enforced.



Lesson 9: Protecting Endpoint Computers Through Behavior Monitoring

Lesson Objectives:

After completing this lesson, participants will be able to:

- Protect an endpoint computer against ransomware
- Protect an endpoint computer against exploits
- Block unrecognized software
- Monitor for malware events

Behavior Monitoring

Behavior Monitoring (`TMBMSVR.exe`) constantly monitors endpoints for unusual modifications to the operating system or installed software.

Behavior Monitoring in Apex One protects endpoints through the following techniques:

- Malware behavior blocking
- Ransomware protection
- Anti-exploit protection
- Fileless malware protection
- Newly encountered program protection
- Event monitoring
- Certified Safe Software Service

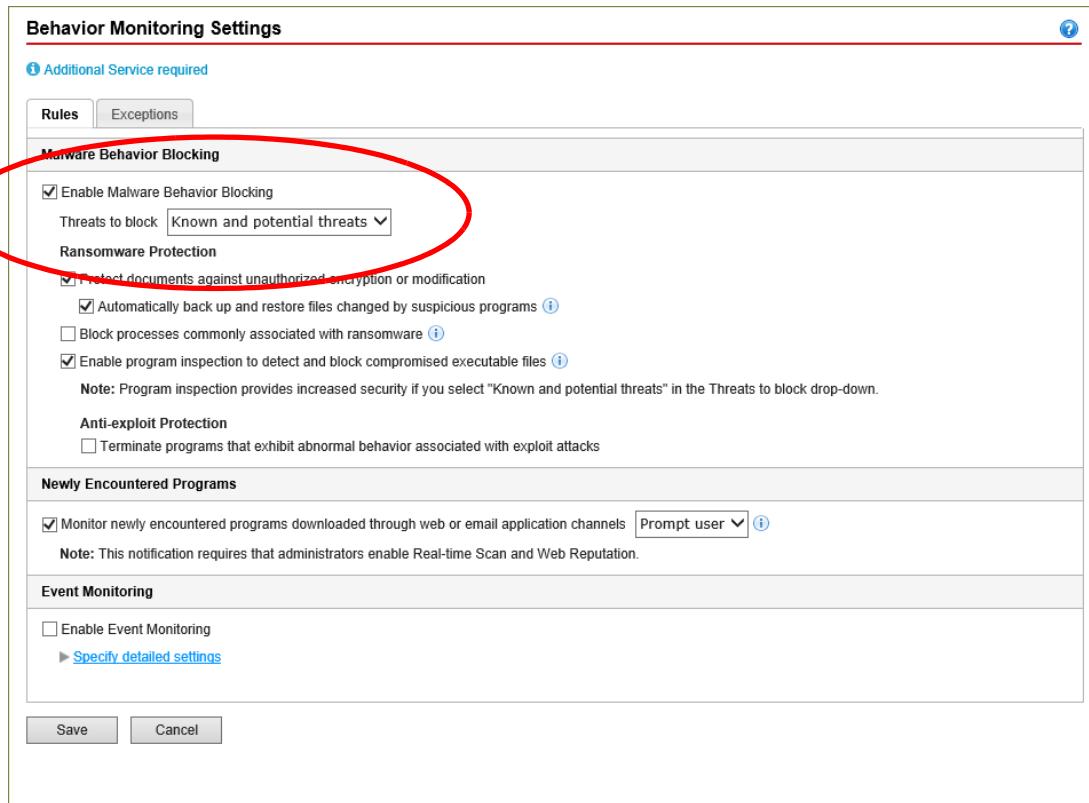
Malware Behavior Blocking

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

Behavior Monitoring can detect malicious scripts executed by legitimate Windows programs and the true payload path of script files executed by legitimate DLLs to protect endpoints against malware hidden in fileless attack vectors.

Malware Behavior Monitoring provides the following threat-level scanning for the following:

- **Known threats:** Blocks behaviors associated with known malware threats
- **Known and potential threats:** Blocks behavior associated with known threats and takes action on behavior that is potentially malicious



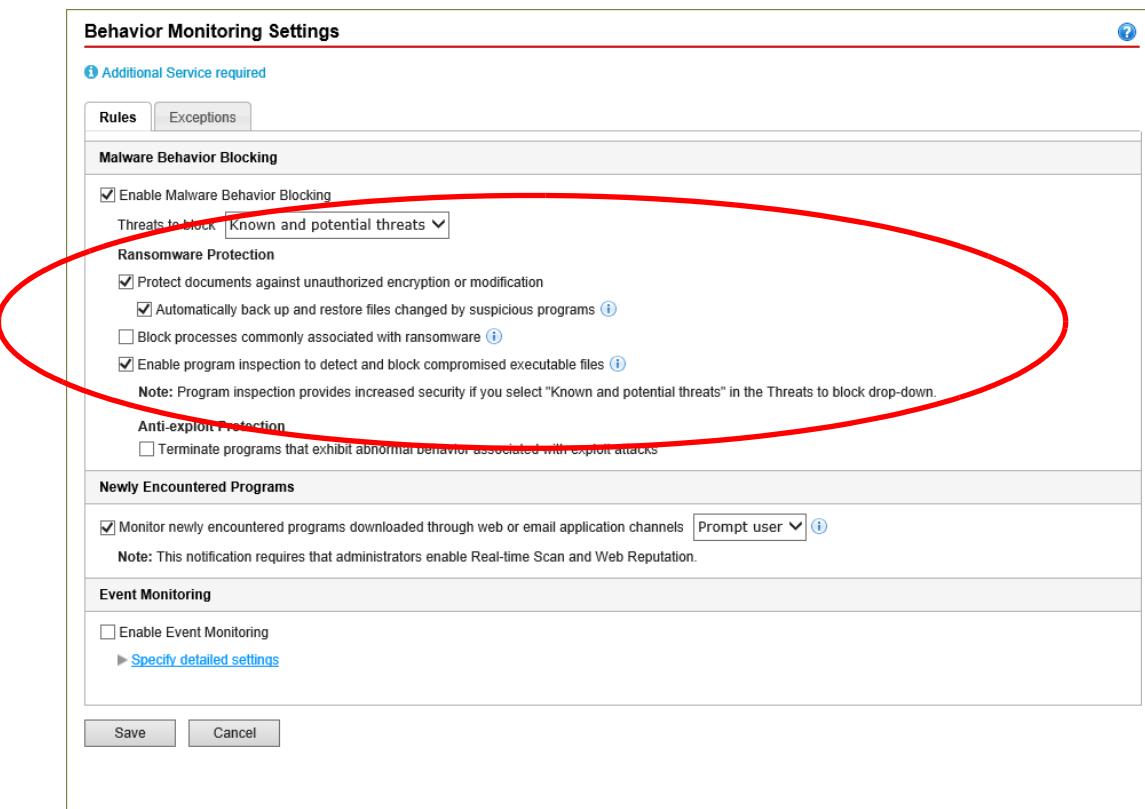
SaaS: Behavior Monitoring settings are configured through Apex Central policies in the service implementation of Apex One.

Ransomware Protection

Ransomware refers to a class of malware that holds a computer hostage until the user pays a particular amount or abides by specific demands. Ransomware restricts access to the system when executed and shows messages that force users into paying a ransom or performing a desired action. There are some ransomware variants that encrypt files found on the system's hard drive. Users are then forced to pay up in order to decrypt the important or critical files that were altered by the ransomware due to file encryption. Since these variants can hijack legitimate, normal file encryption methods to encrypt files, it is difficult to detect.

Behavior Monitoring can detect a specific sequence of events that may indicate a Ransomware attack. To enable ransomware protection, select the following options under **Behavior Monitoring Settings**.

In addition, set the option to automatically backup and restore files changed by suspicious applications. Apex One does not have the ability to decrypt files if encrypted by malware.

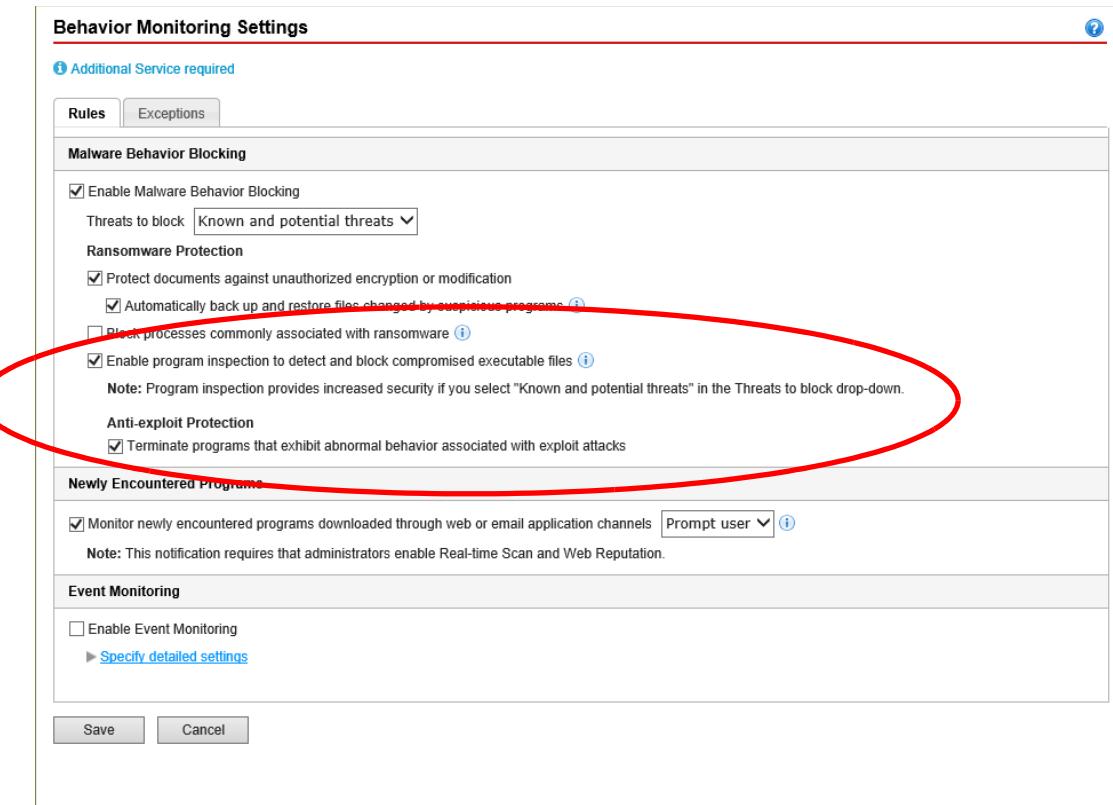


The AEGIS service can receive and reply to exploit events, and terminate processes if it meets violation rules.

Anti-Exploit Protection

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

Anti-exploit Protection requires that you select **Enable program inspection to detect and block compromised executable files**.



Fileless Malware Protection NEW

Fileless malware is a malicious program or code that runs directly from memory. While the infection is live, the attacker can steal sensitive information or download persistent malware. Apex One is able to detect and block these types of attacks even though they've already started running. These attacks use other vectors like Windows registry, memory, scheduled tasks and other. The violations for these kinds of attack are hard to define because the attack may occur on Windows process list and terminating a system process may cause too many false alarm issues that will greatly impact users.

In Apex One, fileless malware detection is used deal with such attacks. When Anti-exploit Protection is enabled on a Security Agent-protected endpoint, fileless protection is enabled as well. Apex One provides protection for fileless malware with two type of scans:

- Normal Object Scan
- Dynamic Memory Scan

Normal Object Scan

Normal Object Scan is incorporated into the Anti-exploit Protection configuration. When Anti-exploit Protection is enabled, Normal Object scan is enabled as well.

Normal Object Scan provides protection for four different type of type events that could potentially not require a file to be executed to distribute malware:

- **Windows Management Instrumentation:** Windows Management Instrumentation (WMI) is a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. WMI provides the ability to obtain management data from remote computers. Malware taking advantage of weaknesses in this technology does not reside on separate file or in the Registry but in special database in the Operating System.
- **Schedule Task:** The Task Scheduler in Windows enables administrators to automatically perform routine tasks on a chosen computer.
- **BitsJob:** Background Intelligent Transfer Service (BITS) is used to download files from or upload files to HTTP web servers or SMB file servers. BITS continues to transfer files after an application exits as long as the user who initiated the transfer remains logged on and a network connection is maintained. BITS will not force a network connection and resumes transfers after a network connection that had been lost is reestablished or after a user who had logged off logs back in. **Bitsadmin** is a windows built-in command-line tool that you can use to create download or upload jobs and monitor their progress. This tool is usually skipped by antivirus software due to it being signed by Microsoft.
- **RegRun:** Registry keys (Run and RunOnce) cause programs to run each time that a user logs on. This process can be compromised by adding parameters to the program startup.

Dynamic Memory Scan

Dynamic Memory Scan (MIP3) uses exploit events and suspicious memory events as the trigger to apply memory scanning on target processes. Other trigger points for memory scans can not capture fileless attacks and a result, this new memory scan is introduced in Apex One.

Dynamic Memory Scan is configured in the **Real-Time Scan Settings** by enabling **Quarantine malware variants detected in memory**. In addition, the **Unauthorized Change Prevention Service** and **Advanced Protection Service** must be enabled.

Real-time Scan Settings

Enable virus/malware scan
 Enable spyware/grayware scan

Target **Action** **Scan Exclusion**

User Activity on Files
Scan files being: **created/modified and retrieved**

Files to Scan

All scannable files
 File types scanned by IntelliScan (i)
 Files with the following extensions (use commas to separate entries):
".",ACCDB,ACE,AMG,ARJ,BAT,BIN,BOO,BOX,BZ2,CAB,CDR,CDT,CHM,,CL4,,CLASS,,COM,,CPT,,CSC,,DLL,,DOC,,DOCX,,DOT,,DOTM,,DOTX,,DR,V,,DVB,,DWG,,DWT,,EML,,EPOC,,EXE,,GMS,,GZ,,HLP,,HTA,,HTM,,HTML,,HTT,,I,NI,,JAR,,JPEG,,JPG,,JS,,JSE,,JTD,,JTT,,LNK,,LZH,,MDB,,MPD,,MPP,,MPT,,MSG,,MSI,,MSO,,MST,,NWS,,OBD,,OCX,,OFT,,OVL,,PDF,,PHP,,PIF,,PL,,PM,,POT,,POT"

Scan Settings

Scan floppy disks during shutdown
 Scan network drive
 Scan the boot sector of the USB storage device after plugging in
 Scan all files in removable storage devices after plugging in
 Quarantine malware variants detected in memory (i)
Note: This feature requires that administrators enable the Unauthorized Change Prevention Service and Advanced Protection Service.

Scan compressed files
Maximum layers: **2** (i)

Scan OLE objects
Maximum layers: **3** (i)

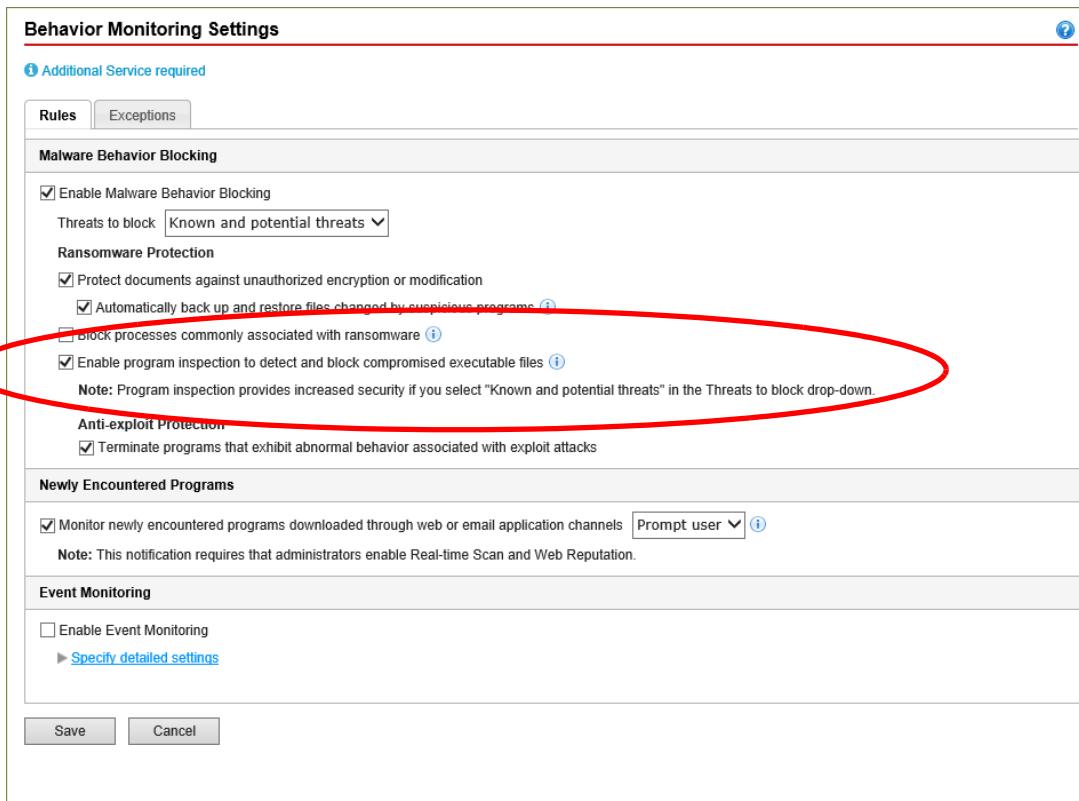
Detect exploit code in OLE files (i)

Virus/Malware Scan Settings Only

Enable IntelliTrap (i)
 Enable CVE exploit scanning for files downloaded through web and email channels

Save **Cancel**

The Behavior Monitoring Rule setting **Enable program inspection to detect and block compromised executable files** must also be enabled for this type of fileless scan.



Newly Encountered Program Protection

Behavior Monitoring works in conjunction with Web Reputation Services and Real-time Scan to verify the prevalence of files downloaded through web channels, email applications, or Microsoft Office macro scripts. After detecting a newly encountered file, administrators can choose to prompt users before executing the file. Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file as determined by the Smart Protection Network.

Census describes the rating of files based on their prevalence and maturity. Prevalence refers to how common a file is, while maturity refers to the period of time between the first time a file was recorded in the Census server and the time of the query.

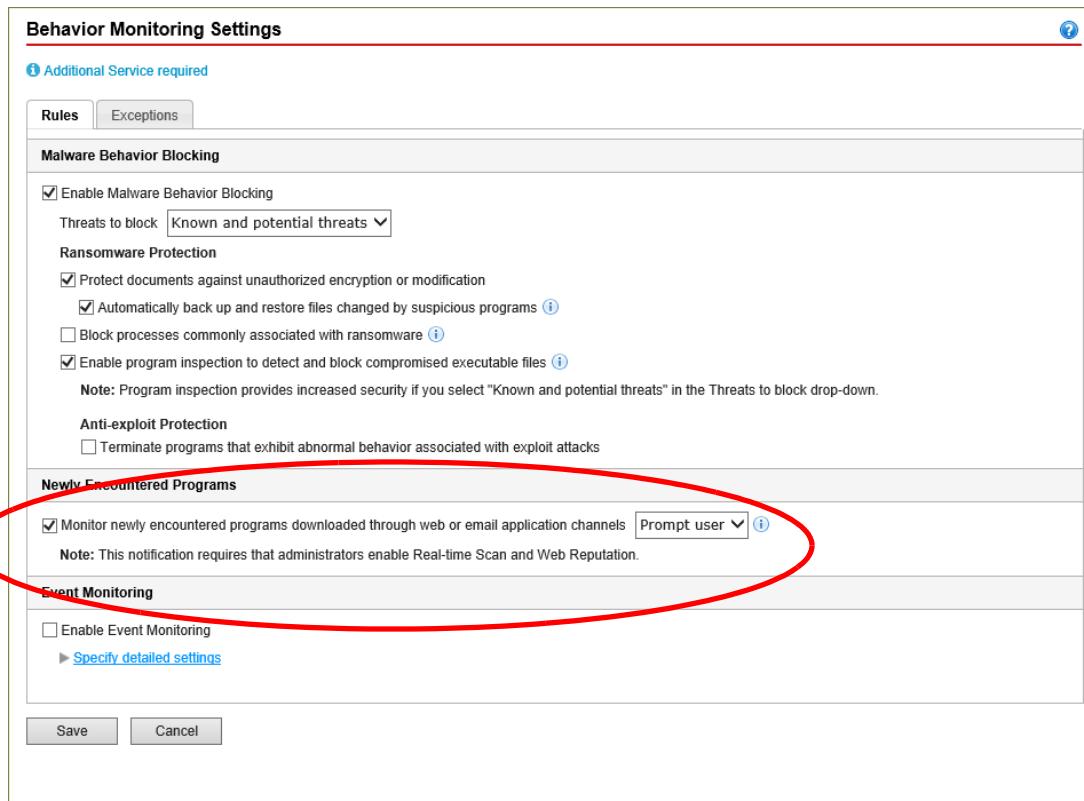
Apex One provides protection for Zero-Day Attacks through the Behavior Monitoring Engine, Web Reputation, and File Census to provide a score that VSAPI can use to take action on a possible malicious file.

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

Behavior Monitoring scans the following file types for each channel:

- **HTTP and HTTPS:** Scans .exe files
- **Email applications:** Scans .exe and compressed .exe files in unencrypted .zip and .rar files

In the **Behavior Monitoring Settings** windows, enable **Monitor newly encountered programs downloaded through HTTP or email applications**. After blocking an application, administrators can choose to prompt users before executing the file or merely log the event.

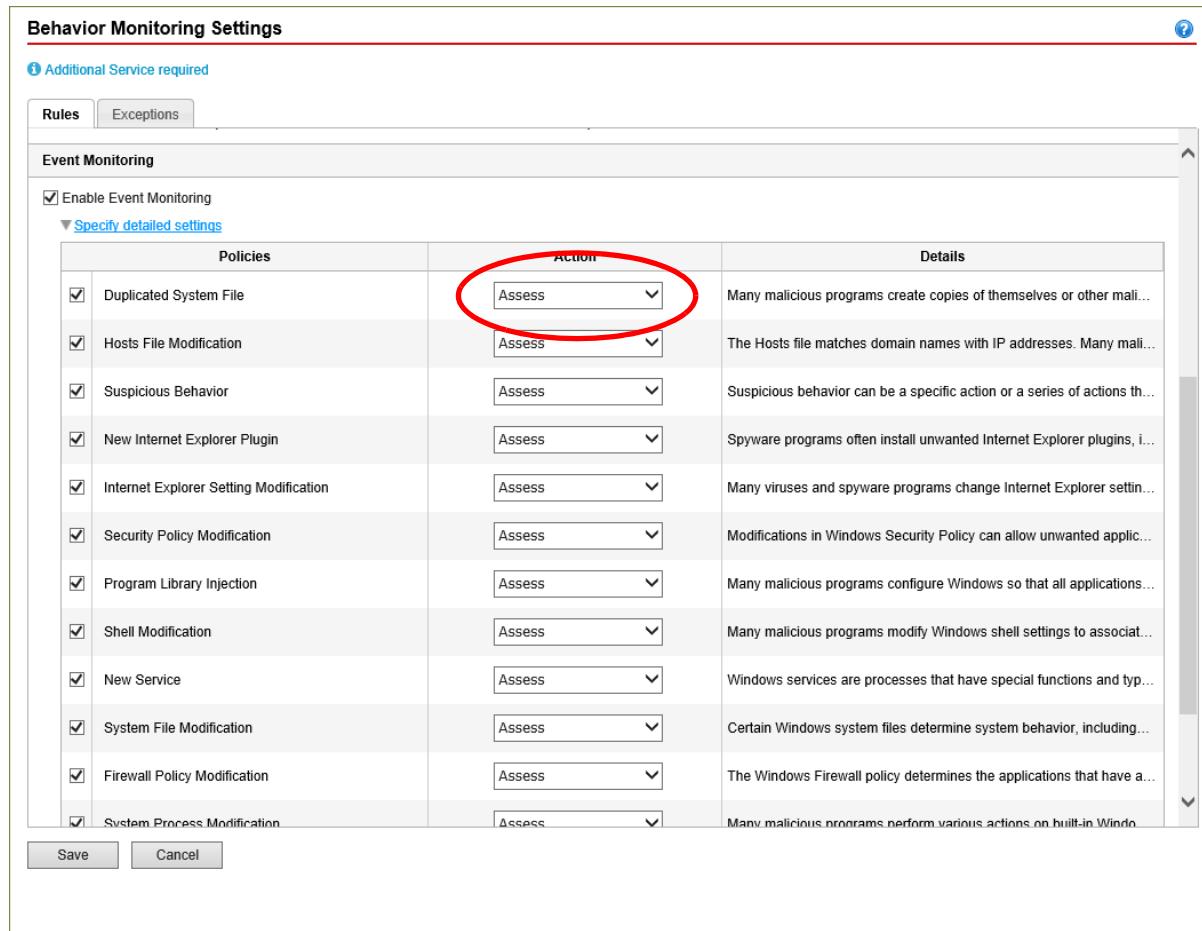


Note: If using Microsoft System Center Configuration Manager to distribute software, do not enable the **Prompt User** setting as the end user will not see the prompt and the software may not install properly.

Event Monitoring

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

In the **Behavior Monitoring Settings** windows, click **Enable Event Monitoring**. Expand **Specify detail settings** and select the appropriate items to monitor.



- Duplicated System File:** Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.
- Hosts File Modification:** The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the web browser is redirected to infected, non-existent, or fake websites.
- Suspicious Behavior:** Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspicious behavior should be used with caution.
- New Internet Explorer Plug-in:** Spyware/grayware programs often install unwanted Internet Explorer plug-ins, including toolbars and Browser Helper Objects.

- **Internet Explorer Setting Modification:** Many virus/malware change Internet Explorer settings, including the home page, trusted websites, proxy server settings, and menu extensions.
- **Security Policy Modification:** Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.
- **Program Library Injection:** Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.
- **Shell Modification:** Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.
- **New Service:** Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.
- **System File Modification:** Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.
- **Firewall Policy Modification:** The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.
- **System Process Modification:** Many malicious programs perform various actions on built-in Windows processes. These actions can include terminating or modifying running processes.
- **New Startup Program:** Malicious applications usually add or modify autostart entries in the Windows registry to automatically launch every time the computer starts.

Event Monitoring Actions

When Event Monitoring detects a monitored system event, it performs the action configured for the event.

- **Assess:** The Security Agent always allows programs associated with an event to run and logs the event for assessment. This is the default action for all monitored system events.
- **Allow:** The Security Agent always allows programs associated with an event to run.
- **Ask when necessary:** The Security Agent prompts users to allow or deny programs associated with an event from running and adds the programs to the exception list. If the user does not respond within a certain time period, the Security Agent automatically allows the program to run. The default time period is 30 seconds.
- **Deny:** The Security Agent always blocks programs associated with an event from running and logs the event. After blocking a program with notifications enabled, the Security Agent displays a notification on the endpoint.

Note: Since Event Monitoring creates a lot of logs, by default, Behavior Monitoring violations will be collected for a period of 1 hour, then uploaded to the server. In environments with many Agents, if all logs were sent separately like normal detections, the server would be flooded.

On the Agent this value will appear in the Windows Registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\AEGIS\SendBMLogPeriod

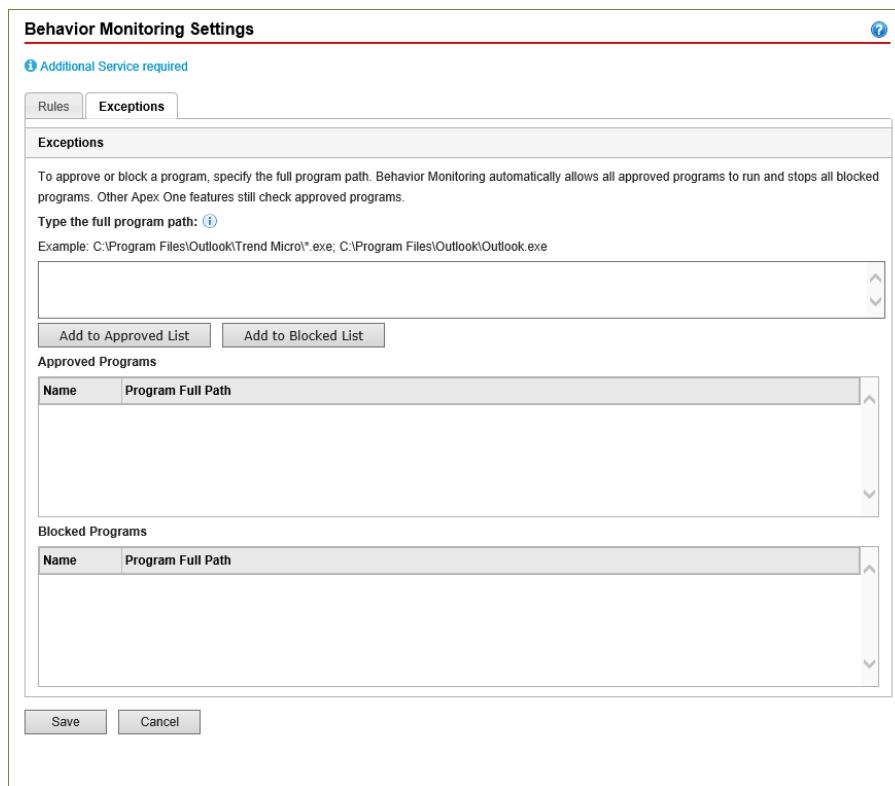
Behavior Monitoring Exception List

The Behavior Monitoring exception list contains programs that Security Agents do not monitor using Behavior Monitoring.

- **Approved Programs:** The Security Agent allows all programs in the **Approved Programs** list to bypass Behavior Monitoring scanning.

Note: Although Behavior Monitoring does not take action on programs added to the **Approved Programs list**, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run.

- **Blocked Programs:** The Security Agent blocks all programs in the Blocked Programs list.



The Behavior Monitoring Approved/Blocked List supports the use of wildcard characters when defining file path, file name, and file extension exception types. Use the following tables to properly format your exception lists to ensure that Apex One excludes the correct files and folders from scanning.

Supported wildcard characters:

- Asterisk (*): Represents any character or string of characters.
- Question mark (?): Represents a single character.

Lesson 10: Protecting Endpoint Computers From Unknown Threats

Lesson Objectives:

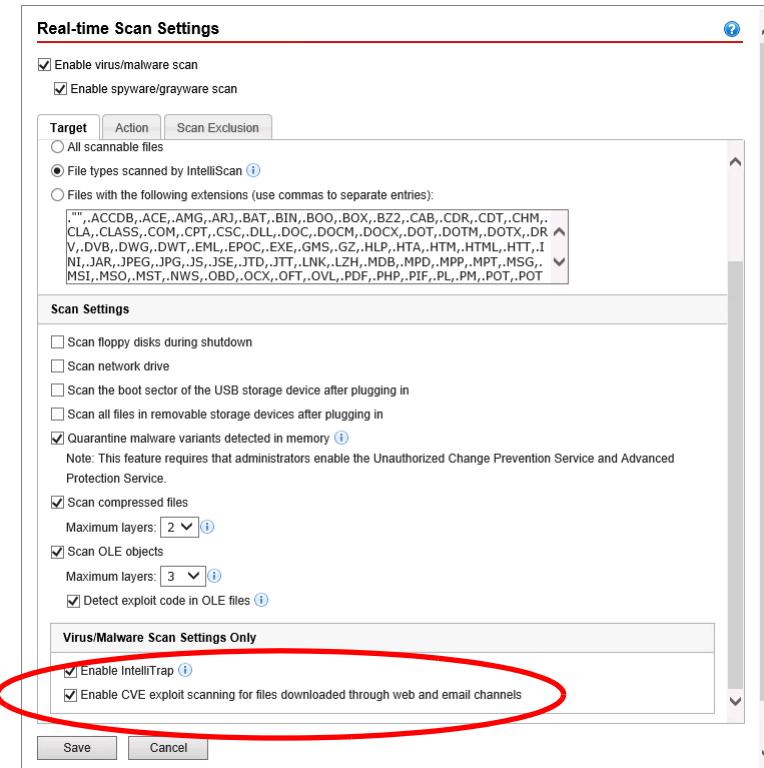
After completing this lesson, participants will be able to:

- Enable Predictive Machine Learning

The Advanced Threat Scan Engine (ATSE) enhances protection against zero day attacks. ATSE is an enhanced version of VSAPI that uses VSAPI output as a basis for heuristic detection (characteristic analysis).

Common Vulnerabilities and Exposures Exploits

If a file's characteristics match a Common Vulnerabilities and Exposures (CVE) Exploit rule, it will be detected by the ATSE scan engine through Real-time Scans.



SaaS: CVE settings are configured through Apex Central Real-Time Scan policies in the service implementation of Apex One.

Advanced Threat Scanning supports the following two application types.

- **Email:** Advanced Threat Scanning supports Outlook and Windows Live Mail. When a user opens an email with an attached sample, the attachment will be scanned by ATSE. The Agent will display a notification if the attachment contains a possible malware payload.
- **Web Browser:** When a user accesses a web site through their web browser using HTTP or HTTPS, files dropped onto the user's computer will be scanned by ATSE. If any malicious sample is dropped onto the user's machine, an alert will be displayed up notifying the user of a possible virus. Supported Web browsers include: Internet Explorer, Chrome, Firefox, Microsoft Edge, Opera, Safari and Sleipnir.

Supported File Types

The following file types are monitored by Advanced Threat Scanning:

Application	Extension
Microsoft Word	doc, docx, docm, dot, dotx, dotm
Microsoft Excel	xls, xlsx, xlsm, xlsb, xlt, xltx, xltm, xla, xlam
Microsoft PowerPoint	ppt, pptx, pptm, pot, potx, potm, pps, ppsx, ppsm, ppa, ppam
Microsoft Outlook	msg
Microsoft Office	xps, mht, mhtml
Other	pdf, rtf, swf, xlr, wps, wpd, odt

Predictive Machine Learning

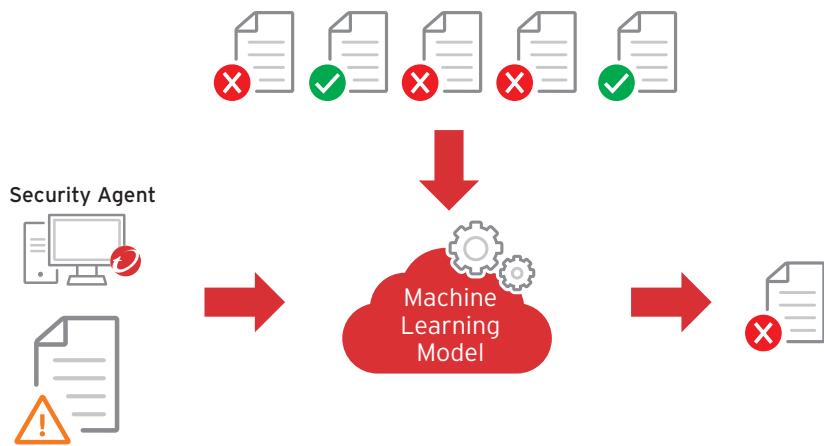
Apex One incorporates Predictive Machine Learning technology to provide better protection for threats such as ransomware or advanced persistent threats.

Predictive Machine Learning operates on the concept that a computer can learn information without human mediation. It uses algorithms to examine large volumes of information or training data to discover unique patterns. This system analyzes these patterns, groups them accordingly, and makes predictions. Through repetition, it learns by inference without a need to be deliberately programmed each and every time.

Predictive Machine Learning can evaluate unknown threats found in suspicious process of files originating from USB, web, or email channels. It does this by using good and bad sample files to extract the file features that will be used to train the Machine Learning Model. This model takes advantage of Trend Micro's Smart Protection Network and Threat Research, to educate the model with the file features that will enable the technology to have high detection rate.

Once Apex One detects an unknown file or process, it extracts the file/process features to the model and uses the technology to predict if the file is good or bad.

The Predictive Machine Learning design utilizes Portable Executable (PE) file features, such as Opcode, Import table or others like Entropy and Icon to train the Machine Learning Model.



Take the example of a known ransomware and an unknown variant. The two variations have different sizes and different SHA1 values. However, the unknown variant of ransomware can still be recognized through Predictive Machine Learning by using file features such as Opcode and Import table data information.

Predictive Machine Learning accuracy is largely based on the training from existing verified good and bad files in which the Trend Micro Smart Protection Network is a key component.

Machine Learning can extract many characteristics from the static file both before runtime and also during runtime. It can block malware before it is executed, however it can possibly be evaded by various kinds of obfuscation techniques commonly used by today's malware. With post-runtime, it analyzes the true intention (behavior) of malware and it is more difficult for malware to evade the detection. However in this case, some damage could have already occurred since the malware already executed.

While Apex One Predictive Machine Learning continues to advance its learning, there is only a small fraction of malware that is being missed with signatures and behavioral, and 99.7% of these were caught with machine learning as seen in test cases so far. By combining Machine Learning with other Apex One protection techniques you can create a layered approach which can lower false positives even more and help obtain a higher performance (For example, since only a smaller set of the files will need to get examined with deeper machine learning).

Once Machine Learning determines a file to be malicious, it gets sent off to our Smart Protection Network so that it is caught with higher performance file reputation technology for that customer on the next occurrence and also will be caught for other customers and across our other products that use the file reputation technology.

File Detections

After detecting an unknown or low-prevalence file, Apex One scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the PML engine, hosted on the Trend Micro Smart Protection Network. Through the use of malware modeling, PML compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains. Depending on the PML configuration settings, Apex One can attempt to quarantine the affected file to prevent the threat from continuing to spread across your network.

Process Detections

After detecting an unknown or low-prevalence process, Apex One monitors the process using the Contextual Intelligence Engine, and sends the behavioral report to the Predictive Machine Learning engine. Through the use of behavioral malware modeling, Predictive Machine Learning compares the process behavior to the model, assigns a probability score, and determines the probable malware type the process is executing. Depending on the Predictive Machine Learning configuration settings, Apex One can terminate the affected process and attempt to clean the file that executed the process.

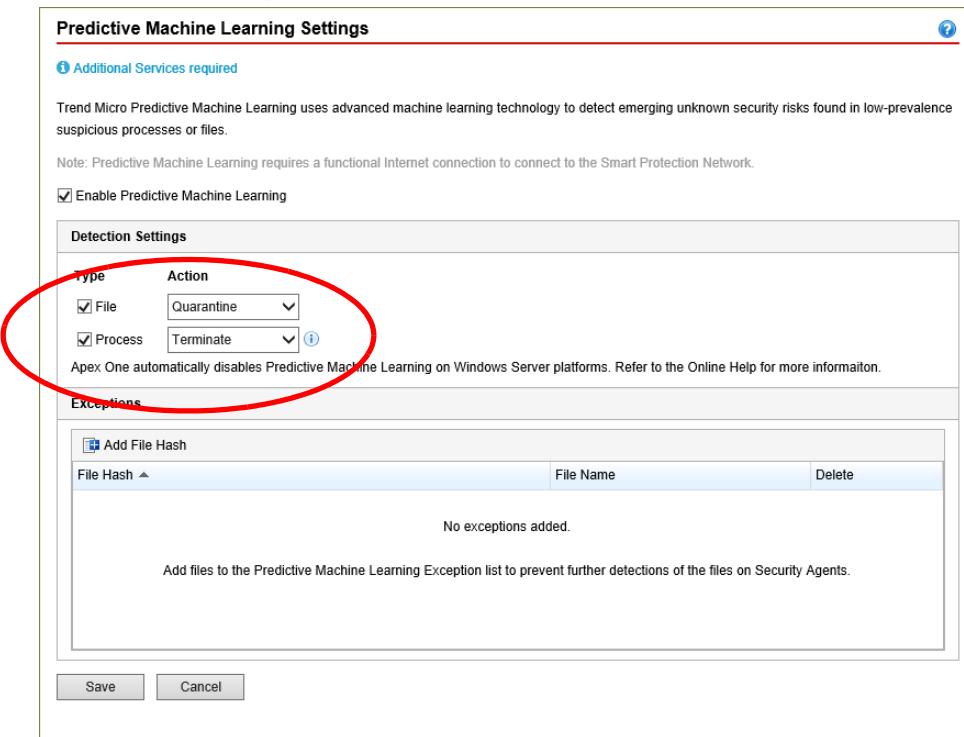
Enabling Predictive Machine Learning

Security Agents examine files from different channels:

- USB
- Web (no plug-in required, but only Internet Explorer, Chrome, Firefox, Edge)
- Email (Outlook only)

Combining Predictive Machine Learning with other protection techniques can lower false positives and obtain higher performance.

In the Apex One Web Management console, click **Agents > Agent Management** and right-mouse click specific domains or Agents. Click **Settings > Predictive Machine Learning Settings**. Click to **Enable Predictive Machine Learning** and select **File** and/or **Process** detection along with the **Action**.



SaaS: Predictive Machine Learning settings are configured through Apex Central policies in the service implementation of Apex One.

Predictive Machine Learning supports the following action on detection.

- **For File:** Log only, Quarantine (default)
- **For Process:** Log only, Terminate (default). After terminating the process, Apex One attempts to clean or quarantine the file and threat remnants from the endpoint.

Note: Predictive Machine Learning uses ATSE, and therefore supports the same browsers and mail applications. Both HTTP and HTTPS are supported and no plug-in is needed. When there is a file download, VSAPI callback is checked whether parent process is a browser or not. If it is a browser, then it will be identified as a browser download.

Exceptions

Configure the Predictive Machine Learning file exceptions to prevent agents from detecting a file as malicious.

In the **Exception** section of the **Predictive Machine Learning Settings**, click **Add File Hash**. Specify the SHA-1 hash value of the file to exclude from scanning.

The screenshot shows a dialog box titled "Add File to Exception List". It contains a descriptive message: "Add the file to Apex One server's Predictive Machine Learning Exception List to prevent the file from being blocked or quarantined on all agents in the future." Below this is a "File Hash: (SHA-1)" input field, a "Notes:" label, and a "File name (Optional)" input field. At the bottom are "Add" and "Cancel" buttons.

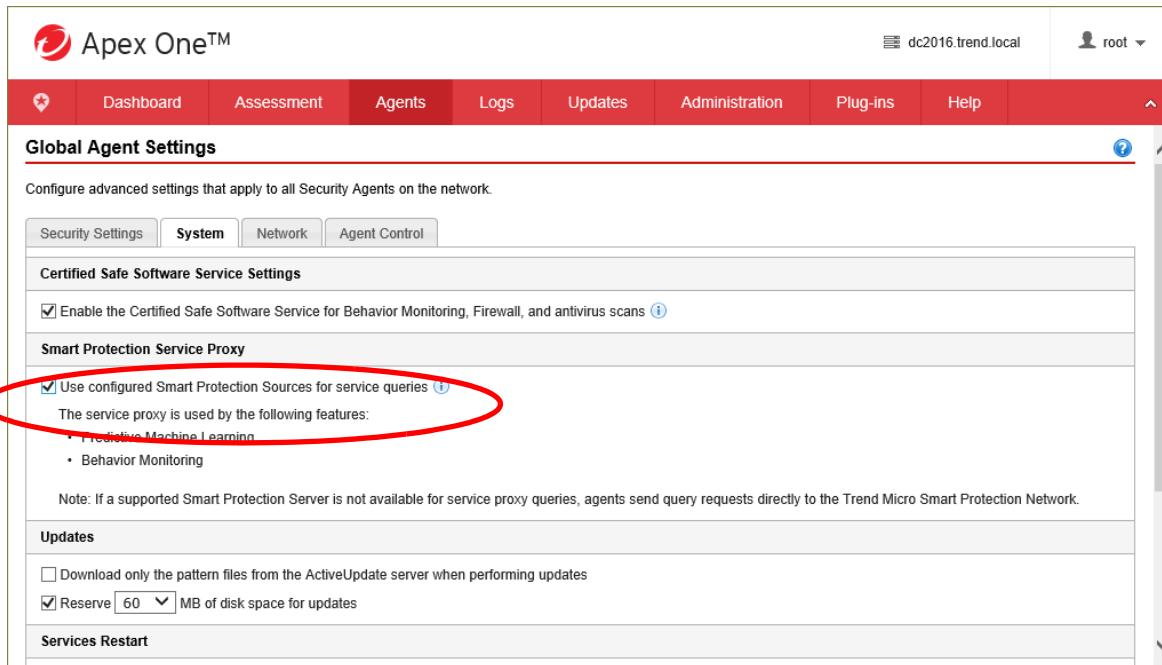
Connection Settings

Security Agents need to able to connect to the following URLs:

- <https://osce140-en-b.trx.trendicro.com>
- <https://osce140-en-f.trx.trendicro.com>

You can also configure your environment so that Machine Learning requests are performed through the Smart Protection Server if the endpoints don't have Internet access to submit file characteristics themselves.

To configure this scenario from the Apex One Server console, go to **Agents > Global Agent Settings > System**. In the **Smart Protection Service Proxy** section, click **Use configured Smart Protection Sources for service queries**.



The screenshot shows the Apex One™ Global Agent Settings interface. The top navigation bar includes links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, Help, and a user dropdown for 'root'. The main content area is titled 'Global Agent Settings' and contains tabs for Security Settings, System (which is selected), Network, and Agent Control. Under the 'System' tab, there are sections for 'Certified Safe Software Service Settings' and 'Smart Protection Service Proxy'. The 'Smart Protection Service Proxy' section contains a checked checkbox for 'Use configured Smart Protection Sources for service queries' (with a blue question mark icon) and a note stating: 'The service proxy is used by the following features: • Predictive Machine Learning • Behavior Monitoring'. A red circle highlights this checkbox. Below this, there is a note: 'Note: If a supported Smart Protection Server is not available for service proxy queries, agents send query requests directly to the Trend Micro Smart Protection Network.' The 'Updates' section includes options for downloading pattern files and reserving disk space (set to 60 MB). The 'Services Restart' section is also visible.

SaaS: Since Smart Protection Servers are not supported, the Smart Protection Service Proxy settings are not available in the service implementation of Apex One.

It is also necessary to enable File Reputation Service HTTPS query when using Smart Protection Service Relay. Predictive Machine Learning Query uses the current File Reputation Service server name and port to forward the request to the back end Machine Learning Service.

In the Apex One Web Management console, go to **Administration > Smart Protection > Integrated Server** and enable **Use HTTPS for scan queries**.

The screenshot shows the Apex One Web Management interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root'. Below the navigation bar, the title 'Integrated Smart Protection Server' is displayed. Under this title, there's a section for 'File Reputation Services' with three options: 'Enable File Reputation Services' (checked), 'Use HTTP for scan queries' (unchecked), and 'Use HTTPS for scan queries' (checked and circled in red). There's also a section for 'Agent Connection' listing services, protocols, and server addresses. Finally, there's a 'Component Status' section showing the current version and last update for 'Smart Scan Pattern' and 'Web Blocking List', each with an 'Update Now' button.

Offline Predictive Machine Learning NEW

Predictive Machine Learning requires a connection to the Smart Protection Network to submit file features to the learning model for analysis. If no connection to the Internet is available on the Agent endpoint, a local Smart Protection Server can be configured to proxy the Internet-based submission to the machine learning model.

In Apex One, a new local machine learning model is introduced to protect the Agent when there is no network connection. When an Agent query to the Internet-based machine learning model is unsuccessful in three attempts, it will switch to local scan mode. This local mode supports file-based pre-execution machine learning scans.

A query to the cloud-based Smart Protection model will be attempted again if any of the three conditions are met:

- A change to the IP address or Agent computer NIC is detected
- There is a change to the Predictive Machine Learning Settings, Smart Protection Service Proxy Settings or Smart Protection Server Port Settings
- Five minutes have elapsed since the last cloud query

If the cloud query is successful, the Security Agent will terminate local mode.

Predictive Machine Learning Local File Model

Predictive Machine Learning Local File Model is the new pattern file and whitelist used for local mode Predictive Machine Learning. This pattern is updated weekly for whitelisting while the local model is updated monthly. This pattern update is incremental. The size of the pattern file is around 2MB

Component Versions		
Component	Version	Last Update
IntelliTrap Pattern	0.247.00	2/20/2019
Memory Inspection Pattern	1.490.00	2/20/2019
Contextual Intelligence Query Handler (64-bit)	1.100.1060	
Advanced Threat Correlation Pattern	1.112.00	2/20/2019
Predictive Machine Learning Local File Model	1.103.00	
Advanced Threat Scan Engine (64-bit)	11.000.1006	
Spyware/Grayware Scan Engine (64-bit)	6.2.4015	
Spyware/Grayware Pattern	21.47	2/20/2019
Smart Feedback Engine (64-bit)	2.58.1004	

Lesson 11: Blocking Web Threats

Lesson Objectives:

After completing this lesson, participants will be able to:

- Configure Web Reputation to block potentially malicious Web sites
- Configure clients to bypass Web Reputation for selected Web sites
- Configure Suspicious Connection Service
- Configure Browser Exploit Prevention

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach.

One goal of these threats is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected endpoint may also become a vector to deliver phishing attacks or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions.

An additional goal of these threats is to hijack a user's CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam, conducting extortion in the form of distributed denial-of-service attacks, pay-per-click activities or cryptocurrency mining.

Apex One can protect endpoint computers against Web threats through the following capabilities:

- Blocking access to malicious URLs through Web Reputation
- Detecting suspicious connections
- Protecting against browser exploits

Web Reputation

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. Trend Micro continually analyzes websites and updates web reputation scores to prevent users from accessing potentially malicious content.

When a user attempts to access a website, the Security Agent queries a Smart Protection source to ascertain the risk level of the content. The configured Web Reputation policy for the Security Agent determines whether to allow access to the website.

The databases used include references to sites collected from a variety of sources, including URLs collected from malware analysis. Billions of URLs are processed per day by Trend Micro Web Reputation Services.

Sites in the database are classified and assigned credibility scores that reflect their potential for either becoming infecting computers or their involvement in a malware or spyware's lifecycle (for example, sources of instructions or components, etc). It contains over 11 million URLs classified as dangerous.

Trend Micro products with Web Reputation protection enabled use these credibility scores to regulate access to these sites. The Web site reputation score is correlated with the specific Web Reputation **Security Level** enforced on the computer. Depending on the Web Reputation Security Level being enforced, Apex One will then either block or allow access to the URL.

Different sources can be used for score requests.

- **Smart Protection Network**

External Agents query the Web Reputation Service hosted on the Trend Micro Smart Protection Network.

- **Smart Protection Server**

Internal Agents may query an onsite Smart Protection Server (either an integrated Smart Protection Server hosted on the Apex One Server, or a Standalone Smart Protection Server in the environment. This Server will refresh its credibility score data against the Smart Protection Network on a regular basis.

- **In-Memory Cache**

When a credibility score is retrieved from one of the sources, the score is cached locally. If a cached entry for the visited Web site exists, the URL Filtering Engine uses the existing cached rating.

Note: The URL Filtering Engine is not actually involved in the URL blocking function. It merely provides the information necessary for the blocking decision.

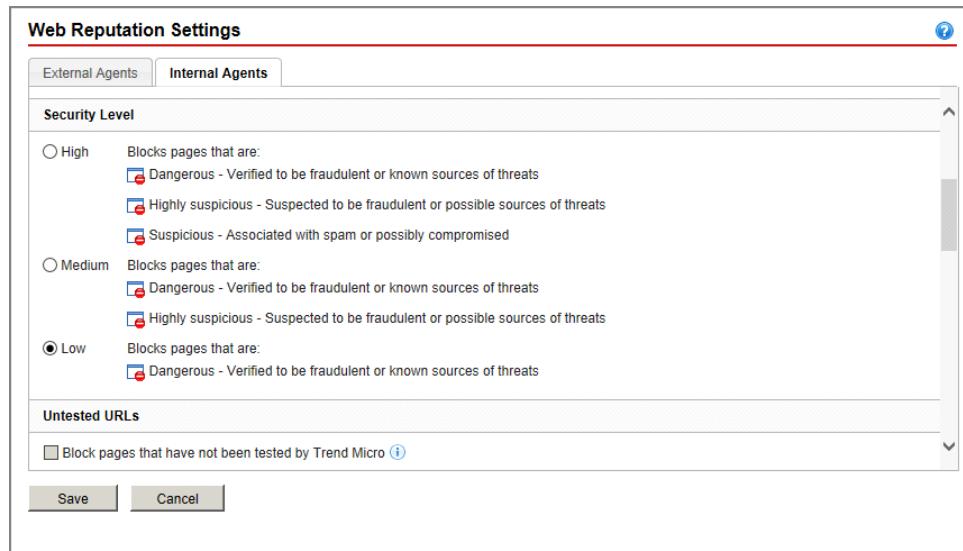
Credibility Scores

The Trend Micro Smart Protection Network, or the local Smart Protection Server, will return a credibility score as follows:

Score	Rating	Description
81-100	Safe	No known or potential threats.
66-80	Suspicious	Possibly a phishing page or a potential source of malware or spyware. Associated with spam or has a history of being compromised.
51-65	Highly Suspicious	
0-50	Dangerous	Verified to be a phishing page or a source of malware or spyware.
71	Untested	Has not been tested by Trend Micro. Untested pages are not blocked by default.

Configuring Web Reputation Settings

Apex One administrators determine the types of sites that are blocked by configuring the security levels in the Web Reputation settings. In the Apex One Web Management console, click **Agents > Agent Management** and right-mouse click specific domains or Agents. Click **Settings > Web Reputation Settings**



SaaS: Web Reputation settings are configured through Apex Central policies in the service implementation of Apex One.

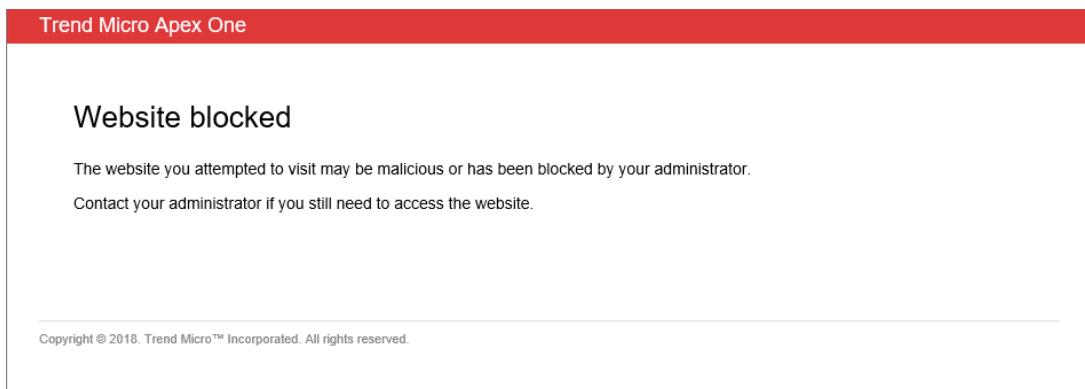
A site will be blocked if its score is less than or equal to the threshold value that a specific security setting prescribes.

Threshold values on the Apex One Server are stored in `ofcscan.ini`, in the `[URL_FILTER_INI_SECTION]` section.

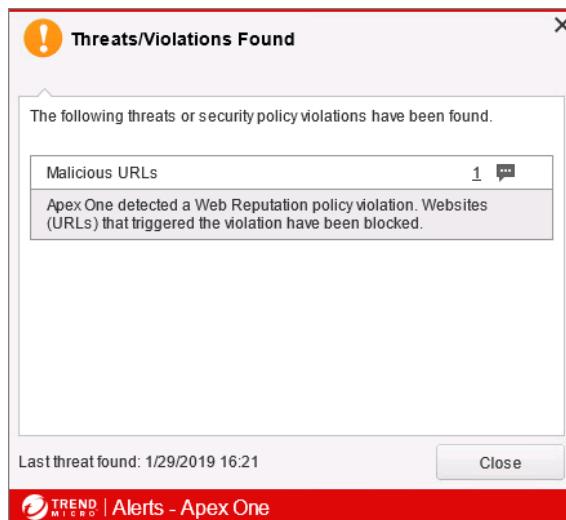
Web threat security can only perform two actions: **Block** or **Allow**. If the score obtained is lower than or equal to the threshold, then the website is blocked. Currently the lowest security setting uses a threshold score of 50.

Lesson 11: Blocking Web Threats

When a website is blocked, a notification window similar to this is displayed in the browser on the Security Agent host.



Additionally, a **Threat/Violation Found** notification is displayed by the Security Agent. Clicking the number next to **Malicious URLs** will display the log details of the violation.



Each time a URL is blocked a corresponding entry is also created in `OfcUrif.log`, which located in the following folder on the endpoint computer:

`C:\Program Files (x86)\Trend Micro\Security Agent\Misc`

A screenshot of a Notepad window titled 'OfcUrif.log - Notepad'. The window displays a single line of log entries: '20190129;>1621;>1;>http://wrs31.winshipway.com/<;>15;>Spyware;>1;>1;>C:\Program Files (x86)\Internet Explorer\iexplore.exe;>31;><;>20190129;>1621;>1;>http://wrs31.winshipway.com/favicon.ico;>15;>Spyware;>1;>1;>C:\Program Files\internet explorer\iexplore.exe;>31.' The Notepad window has standard Windows controls at the top and a scroll bar on the right.

Untested URLs

Administrators can also specify to block pages that have not been tested by Trend Micro. This setting will block URLs that have a credibility score of 71 (Untested).

The **Query Settings** and **Untested URLs** sections in the **Web Reputation Settings** describe the actions to perform on untested URLs.

Security Agents handle Untested URLs (score = 71) based on the relevant Web Reputation Settings.

- If **Send queries to Smart Protection Servers** is enabled, Agents will allow untested websites. Smart Protection Servers do not store web reputation data for these websites.
- If **Send queries to Smart Protection Servers** is disabled, Agents will look at the setting **Block pages that have not been tested by Trend Micro** and block or allow the websites accordingly.

The screenshot shows the 'Web Reputation Settings' page with the 'Internal Agents' tab selected. In the 'Query Settings' section, the 'Send queries to Smart Protection Servers' checkbox is checked and highlighted with a red oval. In the 'Untested URLs' section, the 'Block pages that have not been tested by Trend Micro' checkbox is also checked and highlighted with a red oval. Other settings like 'Check HTTPS URLs' and 'Scan common HTTP ports only' are also visible.

Sample Sites

Trend Micro maintains sample sites for purposes of testing and demonstrating blocking and score retrieval functionality. This is the Web Reputation Service equivalent to the EICAR test files and only works on Web Reputation Service requests to the Global Trend Micro Web Reputation Server. The following table lists these sites and their corresponding scores:

Credibility Score	URL
91	wrs91.winshipway.com
81	wrs81.winshipway.com
71	wrs71.winshipway.com
61	wrs61.winshipway.com
51	wrs51.winshipway.com
41	wrs41.winshipway.com
31	wrs31.winshipway.com
21	wrs21.winshipway.com

Dealing With False Positives

The following website allows administrators to verify the credibility score of sites and to request reassessments in the event that the prevailing score is inappropriate:

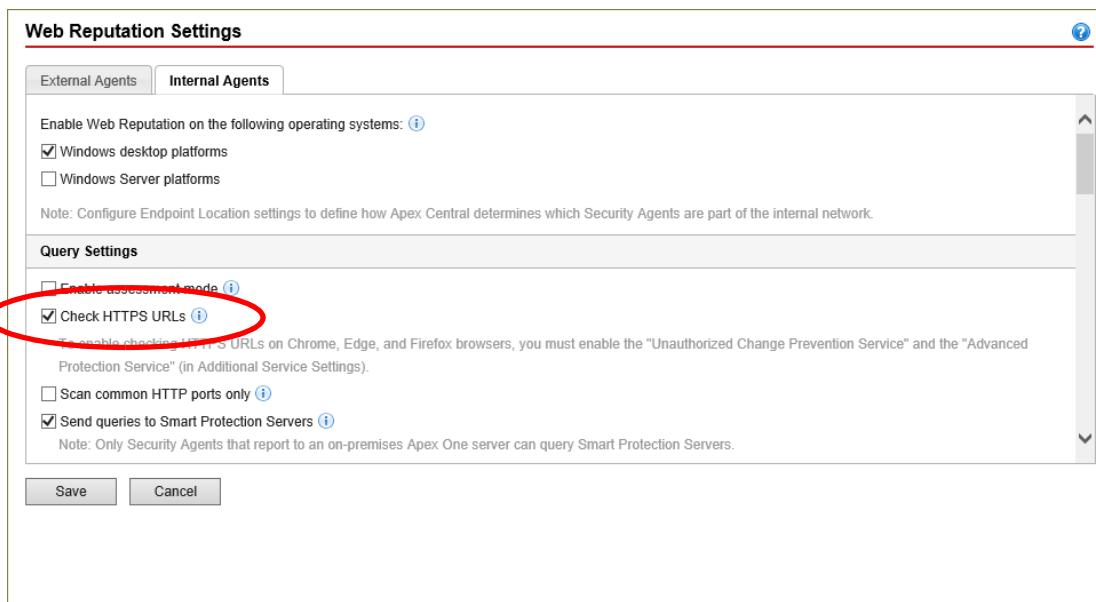
<http://sitesafety.trendmicro.com/>

Requests made through this site are not bound to a Service Level Agreement. Trend Micro customers that require site reassessment are advised to contact Technical Support directly.

Intercepting HTTPS Traffic

HTTPS communication uses certificates to identify web servers. It encrypts data to prevent theft and eavesdropping. Although more secure, accessing websites using HTTPS still has risks. Compromised sites, even those with valid certificates, can host malware and steal personal information. In addition, certificates are relatively easy to obtain, making it easy to set up malicious web servers that use HTTPS.

Enable Check HTTPS URLs to reduce exposure to compromised and malicious sites that use HTTPS.



For HTTPS monitoring in Firefox, Microsoft Edge, and Chrome, you must enable the **Unauthorized Change Prevention** and **Advance Protection** service as well as the **Behavior Monitoring > Enable program inspection to detect and block compromised executable files** feature on agents to scan HTTPS traffic.

For HTTPS monitoring in Internet Explorer, users must enable the **Trend Micro Osprey Plug-in** add-on in the browser pop-up window.



Bypassing Web Reputation Analysis

Apex One administrators can exclude specific Web sites from Web threat analysis. These sites are designated in the **Web Reputation Settings**.

The screenshot shows the 'Web Reputation Settings' page with the 'Internal Agents' tab selected. Under the 'Approved/Blocked URL List' section, there is a checked checkbox labeled 'Enable approved/blocked list'. Below it is a text input field containing 'http://'. A note says '* Wildcards are supported'. There are two buttons: 'Add to Approved List' and 'Add to Blocked List'. A dropdown menu 'View:' is set to 'Approved and Blocked'. At the bottom left are 'Export' and 'Import' buttons, and at the bottom right are 'Save' and 'Cancel' buttons.

URL	Action	Delete
http://www.trendmicro.com/*	Approved	trash
http://kb.trendmicro.com/*	Approved	trash
http://windowsupdate.microsoft.com/*	Approved	trash
http://wustat.windows.com/wutrack.bin?*	Approved	trash
http://download.windowsupdate.com/*	Approved	trash
http://office.microsoft.com/*	Approved	trash
http://c.microsoft.com/*	Approved	trash
http://download.microsoft.com/*	Approved	trash
http://servicecenter.antivirus.com/*	Approved	trash
http://uk.trendmicro-europe.com/*	Approved	trash
http://housecall.antivirus.com/*	Approved	trash
http://dc2016.trend.local:8080/*	Approved	trash
http://dc2016.trend.local/*	Approved	trash
https://dc2016.trend.local:4343/*	Approved	trash
https://dc2016.trend.local/*	Approved	trash

Type the URL and click either **Add to Approved List** or **Add to Blocked List**.

The approved list takes precedence over the blocked list. When a URL matches an entry in the approved list, Agents always allows access to the URL, even if it is in the blocked list.

Note: The internal and external policies can each only have 50 URLs on the approved list, for a total of 100 sites.

Approved lists can cover entire Web sites, or only specific pages.

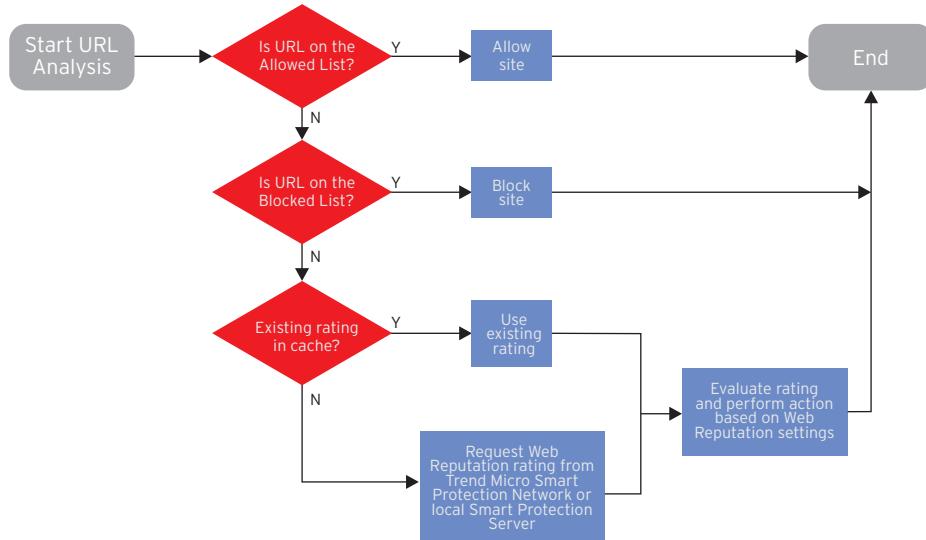
The default selection covers the entire site. Apex One achieves this by using wildcards and appending /* to the URL, as in this example:

```
http://uk.trendmicro-europe.com/*
```

To prevent tampering, URLs on the approved list are encrypted using the standard encryption method that Trend Micro uses for most of its products (for example, passwords). These approved list entries can be decrypted with existing support tools.

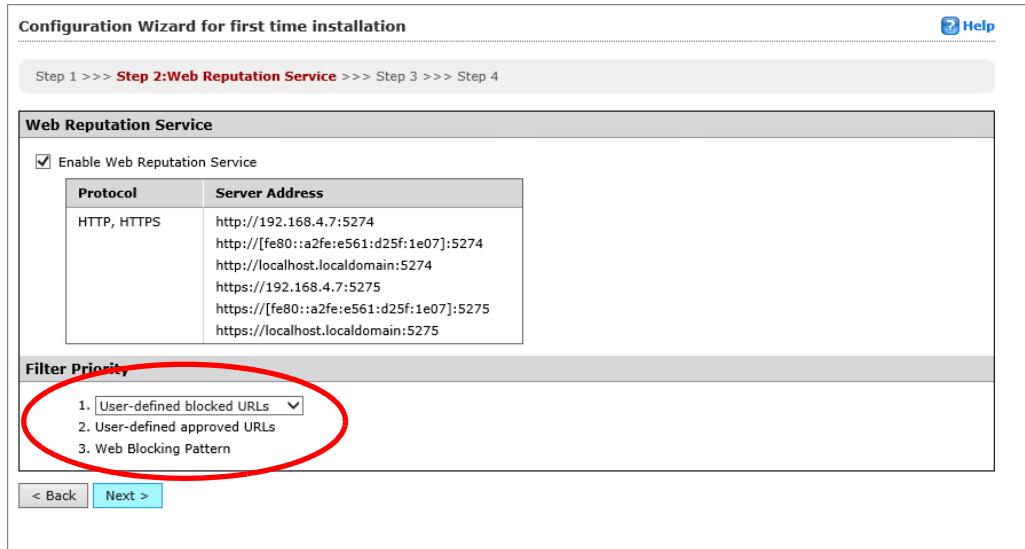
URL Analysis Order

The following flowchart illustrates the order of URL analysis decisions.



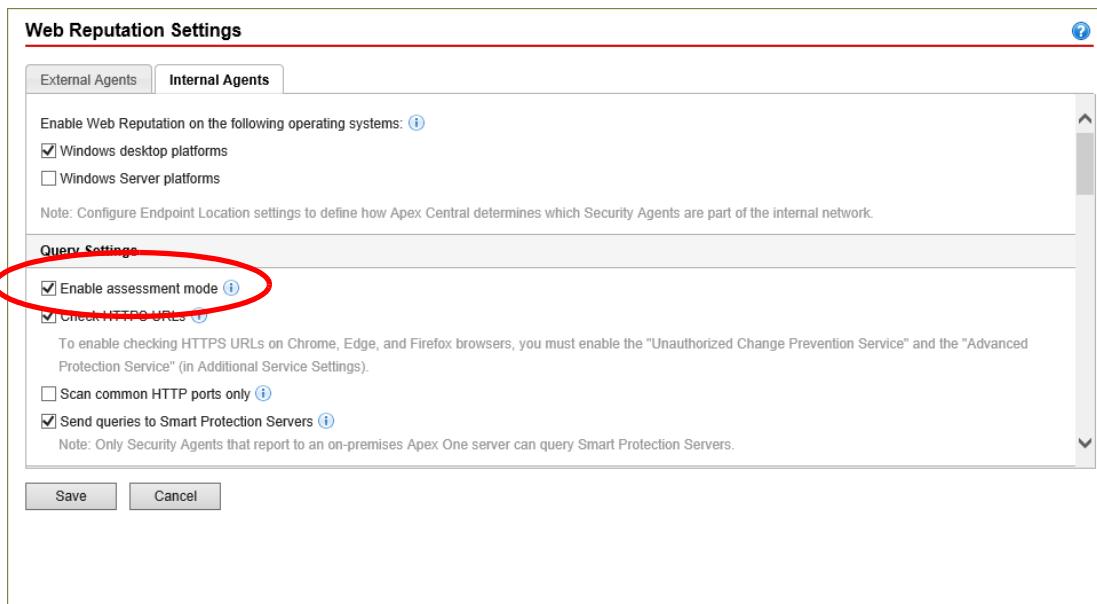
Note: If the Security Agent is not able to retrieve a score from any of the Smart Protection sources, it will default to a fail open and the web site will become accessible.

When a Standalone Smart Protection Server is being used, the order of analysis can be modified to verify the user-defined blocked list before the allowed List by making a **Filter Priority** selection during first time configuration.



Assessment Mode

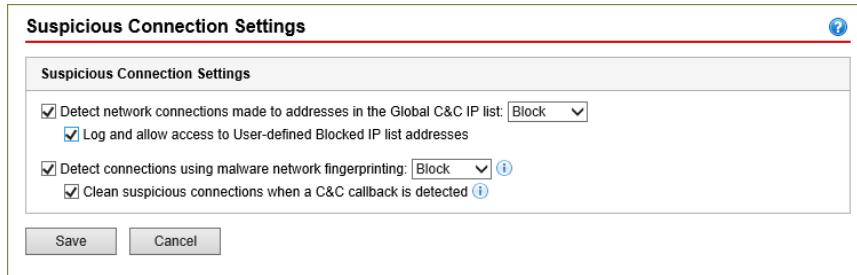
When in assessment mode, Security Agents allow access to all websites. For any accessed website that violates the configured Security Level setting, the Security Agent logs the event only. Assessment mode allows you to monitor website access and evaluate the safety of websites before actively blocking users access. Based on your evaluation of the access logs, you can add trusted websites to the Approved URL List before disabling assessment mode.



Detecting Suspicious Connections

The Suspicious Connection Service manages the User-defined and Global IP C&C lists, and monitors the behavior of connections that endpoints make to potential C&C servers.

In the Apex One Web Management console, click **Agents > Agent Management** and right-mouse click specific domains or Agents. Click **Settings > Suspicious Connection Settings**.



Detecting Connections Through the Global C&C List

The Global C&C IP list works in conjunction with the Network Content Inspection Engine (NCIE) to detect network connections with Trend Micro confirmed C&C servers. NCIE detects C&C server contact through any network channel. The Suspicious Connection Service logs all connection information to servers in the Global C&C IP list for evaluation.

Enable **Detect network connections made to addresses in the Global C&C IP list** to monitor connections made to Trend Micro confirmed C&C servers and select to **Log only** or **Block** connections.

The User-defined Approved and Blocked IP lists allow further control over whether endpoints can access specific IP addresses. Configure these lists when you want to allow access to an address blocked by the Global C&C IP list or block access to an address that may pose a security risk.

Detecting Connections Through Malware Network Fingerprinting

After detecting malware on endpoints through Relevance Rule Pattern matching on network packets, the Suspicious Connection Service can further investigate the connection behavior to determine if a C&C callback occurred. After detecting a C&C callback, the Suspicious Connection Service can attempt to block and clean the source of the connection using GeneriClean technology.

To allow Apex One agents to attempt to clean connections made to C&C servers, enable **Clean suspicious connections when a C&C callback is detected**. Apex One agents use GeneriClean to clean the malware threat and terminate the connection to the C&C server.

GeneriClean, also known as referential cleaning, is a new technology for cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, GeneriClean determines if the detected file has a corresponding process/service in memory and a registry entry, and then removes them altogether.

Protecting Against Browser Exploits

The Apex One Browser Exploit Solution consists of the following patterns:

- **Browser Exploit Prevention Pattern:** This pattern identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser.
- **Script Analyzer Pattern:** This pattern analyzes scripts in Web pages and identifies malicious scripts and Applets.

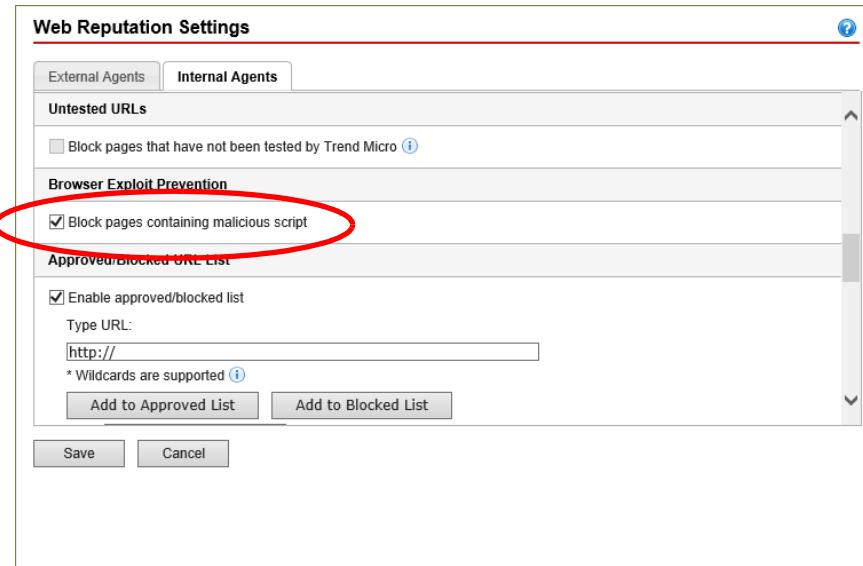
These files are stored on the Apex One Server in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Download\Pattern

When Agents are deployed, these pattern files zips are extracted and are deployed to the Agents in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\Security Agent\CCSF\module\BES

Click **Block pages containing malicious script** to identify Web browser exploits and malicious scripts, and prevent the use of these threats from compromising the web browser. Web Reputation utilizes both the Browser Exploit Prevention pattern and the Script Analyzer pattern to identify and block web pages before exposing the system.



These files are located on the Apex One Server in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Download\Pattern

Note: The Browser Exploit Prevention feature requires that you enable the **Advanced Protection Service** under **Agents > Agent Management**, then **Settings > Additional Service Settings**.

A browser add-on is **no longer needed** to use malicious script protection with Internet Explorer with the latest patch of Apex One.

Lesson 12: Protecting Endpoint Computers Through Traffic Filtering

Lesson Objectives:

After completing this lesson, participants will be able to:

- Enable traffic filtering on Security Agent endpoints
- Configure firewall policies
- Configure firewall profiles and assign to Agent computers

Traffic Filtering

The Security Agent provides the following options to filter network traffic:

- Filtering incoming and outgoing traffic based on certain criteria
- Filtering incoming and outgoing traffic generated by specific applications
- Filtering based on the Certified Safe Software List
- Filtering based on the connection state and specific conditions in a connection
- Filtering based on patterns in network packets that may signal an attack on the Agent computer through Intrusion Detection

Firewall Filtering

The Apex One Firewall filters all incoming and outgoing traffic, providing the ability to block certain types of traffic based on criteria, including:

- Direction (inbound/outbound)
- Protocol (TCP/UDP/ICMP/ICMPv6)
- Destination ports
- Source and destination endpoints

The Apex One firewall provides stateful packet-level inspection of TCP, UDP and ICMP traffic to help protect against network attacks, including ones that originate from within the network. The Apex One firewall can be enabled/disabled by domain, group or individual Agent. This configuration is applied through the firewall policies and profiles.

Apex One firewall functionality is provided by the Trend Micro Common Firewall Driver. The firewall driver is implemented as an NDIS intermediate driver and contains a mini-port interface. This detail will be useful for network administrators seeking to harden their Security Agent hosts.

Apex One uses Security Levels and Exceptions to define how traffic is filtered for the specified criteria.

Application Filtering

The Apex One Firewall filters incoming and outgoing traffic for applications specified in the Firewall Exception List, allowing these applications access to the network. Applications can be defined by identifying the full path or the corresponding Registry entries.

Certified Safe Software List

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.

You can also allow Security Agents to query the dynamically-updated global Certified Safe Software List hosted on Trend Micro servers.

Note: Querying the Global Certified Safe Software List requires that you enable both the **Unauthorized Change Prevention Service** and the **Certified Safe Software Service**.

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.

Intrusion Detection System

The Intrusion Detection System (IDS) helps identify patterns in network packets that may indicate an attack on the Security Agent. The Intrusion Detection System can help prevent the following well-known intrusions:

- **Too Big Fragment:** A Denial of Service attack where a hacker directs an oversized TCP/UDP packet at a target endpoint. This can cause a buffer overflow, which can freeze or restart the endpoint.
- **Ping of Death:** A Denial of Service attack where a hacker directs an oversized ICMP/ICMPv6 packet at a target endpoint. This can cause a buffer overflow, which can freeze or reboot the endpoint.
- **Conflicted ARP:** A type of attack where a hacker sends an Address Resolution Protocol (ARP) request with the same source and destination IP address to a targeted endpoint. The target endpoint continually sends an ARP response (its MAC address) to itself, causing the endpoint to freeze or crash.

- **SYN Flood:** A Denial of Service attack where a program sends multiple TCP synchronization (SYN) packets to the endpoint, causing the endpoint to continually send synchronization acknowledgment (SYN/ACK) responses. This can exhaust endpoint memory and eventually crash the endpoint.
- **Overlapping Fragment:** Similar to a Teardrop attack, this Denial of Service attack sends overlapping TCP fragments to the endpoint. This overwrites the header information in the first TCP fragment and may pass through a firewall. The firewall may then allow subsequent fragments with malicious code to pass through to the target endpoint.
- **Teardrop:** Similar to an overlapping fragment attack, this Denial of Service attack deals with IP fragments. A confusing offset value in the second or later IP fragment can cause the operating system on the receiving endpoint to crash when attempting to reassemble the fragments.
- **Tiny Fragment Attack:** A type of attack where a small TCP fragment size forces the first TCP packet header information into the next fragment. This can cause routers that filter traffic to ignore the subsequent fragments, which may contain malicious data.
- **Fragmented IGMP:** A Denial of Service attack that sends fragmented IGMP packets to a target endpoint, which cannot properly process the IGMP packets. This can freeze or slow down the endpoint.
- **LAND Attack:** A type of attack that sends IP synchronization (SYN) packets with the same source and destination address to the endpoint, causing the endpoint to send the synchronization acknowledgment (SYN/ ACK) response to itself. This can freeze or slow down the endpoint.

Enabling the Apex One Firewall

During the Apex One server installation, you are prompted to enable or disable the Apex One firewall. If you disabled the firewall during installation, you can enable it through the Apex One Web Management console to protect the Agent from intrusions. It can be enabled at any level in the Agent tree.

Enabling the Apex One Firewall on Selected Endpoints

To enable the firewall on selected endpoints, perform the following steps:

- 1 Go to **Agents > Agent Management**.
- 2 In the Agent tree, click the domain, group or specific Agents.
- 3 Click **Settings > Additional Service Settings** and enable the **Firewall service** on desktops or servers.

- 4 Click **Save** to apply settings to the domain, group or Agents. If you applied the service to the root domain, choose **Apply to All Agents** or **Apply to Future Domains Only**.

The screenshot shows the 'Additional Service Settings' dialog box. It contains three sections: 'Unauthorized Change Prevention Service', 'Firewall Service', and 'Suspicious Connection Service'. In the 'Firewall Service' section, there are two checkboxes: 'Windows desktops' (checked) and 'Windows Server platforms' (unchecked). A red oval highlights the 'Windows desktops' checkbox. Below the checkboxes is a note: 'Enabling or disabling the Firewall service temporarily disconnects endpoints from the network. Ensure that you change the settings only during non-critical hours to minimize connection disruptions.' At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Firewall Policies and Profiles

The Apex One firewall uses policies and profiles to organize and customize methods for protecting networked endpoints.

The following steps must be completed to make use of the Apex One firewall capabilities:

- 1 **Create a policy:** The policy allows you to select a security level that blocks or allows traffic on networked endpoints and enables firewall features.
- 2 **Add exceptions to the policy:** Exceptions allow Security Agents to deviate from a policy. With exceptions, you can specify Agents, and allow or block certain types of traffic, despite the security level setting in the policy. For example, block all traffic for a set of Agents in a policy, but create an exception that allows HTTP traffic so Agents can access a Web server.
- 3 **Create and assign profiles to Security Agents:** A firewall profile includes a set of Agent attributes and is associated with a policy. When any Agent matches the attributes specified in the profile, the associated policy is triggered.

Firewall Policies

Apex One Firewall policies allow you to block or allow certain types of network traffic. A policy also defines which firewall features are enabled or disabled. The policy is then assigned to one or multiple firewall profiles.

When configuring a firewall policy, the following settings are available:

- **Security Level:** This general setting blocks or allows all inbound and/or all outbound traffic on the Security Agent endpoint
- **Firewall Features:** These settings specify whether to enable or disable the Apex One firewall, the Intrusion Detection System (IDS), and the firewall violation notification message.
- **Certified Safe Software List:** These settings specify whether to allow certified safe applications to connect to the network.

- **Exceptions:** This list of configurable exceptions block or allow various types of network traffic.

You can grant end-users the privilege to modify the security level and policy exception list when creating Firewall Profiles.

To create or modify policies, complete the following steps:

- 1 Go to **Agents > Firewall > Policies**. Click an existing policy to modify, or click **Add Policy**.

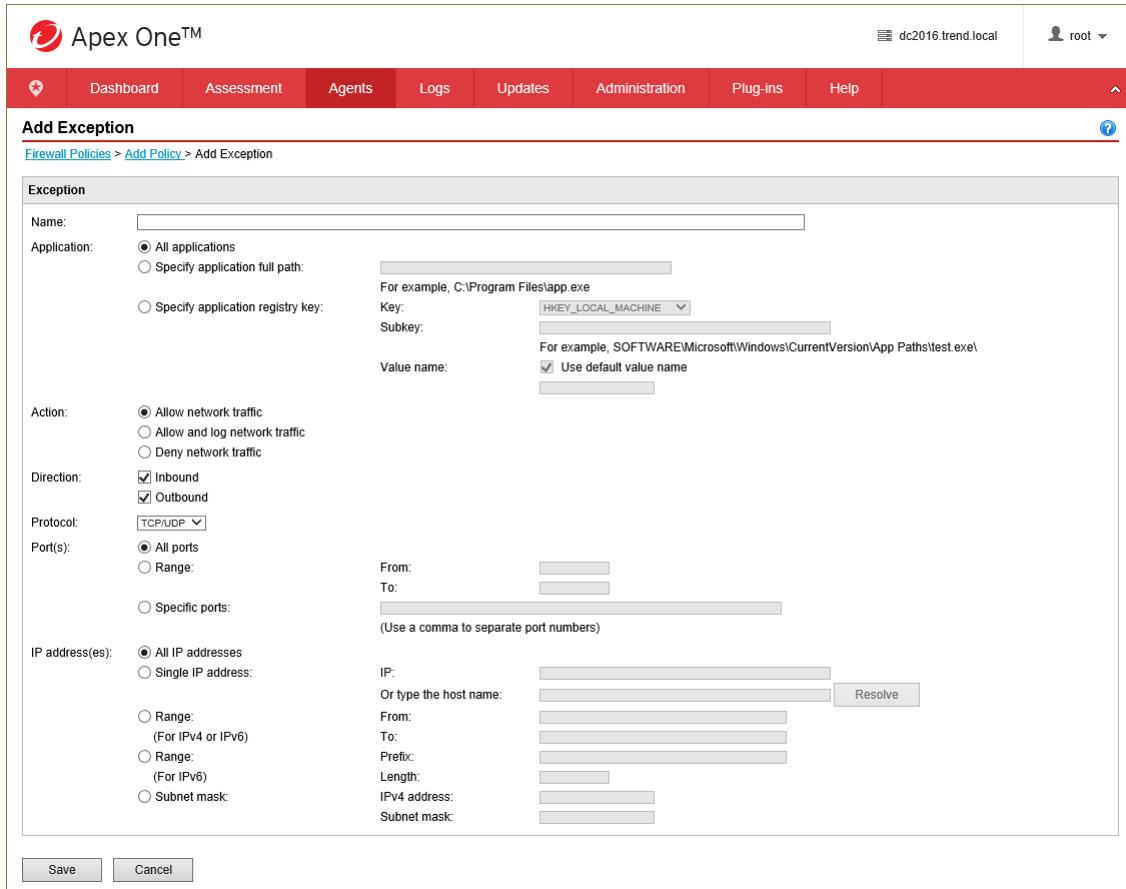
Order	Name	Action	Protocol	Port	Direction	IP Address	Application
1	DNS	Allow	TCP/UDP	Specified 53	Bi-directional	All	All applications
2	NetBIOS	Allow	TCP/UDP	Specified 137, ...	Bi-directional	All	All applications
3	HTTPS	Allow	TCP	Specified 443	Bi-directional	All	All applications
4	HTTP	Allow	TCP	Specified 80	Bi-directional	All	All applications
5	Telnet	Allow	TCP	Specified 23	Bi-directional	All	All applications
6	SMTP	Allow	TCP	Specified 25	Bi-directional	All	All applications
7	FTP	Allow	TCP	Specified 21	Bi-directional	All	All applications
8	POP3	Allow	TCP	Specified 110	Bi-directional	All	All applications
9	LDAP	Allow	TCP/UDP	Specified 389	Bi-directional	All	All applications

- 2 Type a **Name** for the policy.
- 3 Click to select a **Security level** from the list:
 - **High:** blocks all incoming and outgoing traffic except for that which meets the criteria defined in an exception
 - **Medium:** blocks inbound traffic, but allows outbound traffic except for that which meets the criteria defined in an exception
 - **Low:** Allows all inbound or outbound traffic except for that which meets the criteria defined in an exception
- 4 Click to enable the required **Firewall Features**. When **Intrusion Detection System** is enabled, all the intrusions listed previously are blocked.
- 5 Click to enable the **Local** or **Global Certified Safe Software List**. Applications in this list are exempt from filtering when the security level is set to **Medium** or **High**.
- 6 Click to select the firewall **Exceptions**, or click **Add** to create a new exception.
- 7 Click **Save**.

Exceptions

Exceptions override the security level assigned to the policy and block or allow various types of network traffic.

- 1 Click **Add Exception** on the **Firewall Policy** page:



The screenshot shows the 'Add Exception' dialog box within the Apex One™ software. The dialog box has a title bar 'Exception'. It contains several sections: 'Name' (empty input field), 'Application' (radio buttons for 'All applications' (selected), 'Specify application full path', and 'Specify application registry key'), 'Action' (radio buttons for 'Allow network traffic' (selected), 'Allow and log network traffic', and 'Deny network traffic'), 'Direction' (checkboxes for 'Inbound' (selected) and 'Outbound'), 'Protocol' (dropdown menu set to 'TCP/UDP'), 'Port(s)' (radio buttons for 'All ports' (selected), 'Range', and 'Specific ports'), 'IP address(es)' (radio buttons for 'All IP addresses' (selected) and 'Single IP address'), and 'IP' (fields for 'From', 'To', 'Prefix', 'Length', 'IPv4 address', and 'Subnet mask'). At the bottom are 'Save' and 'Cancel' buttons.

- 2 Type a **Name** for the policy exception.
- 3 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.

- 4 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).
- 5 Select the type of network **Protocol**:
 - TCP
 - UDP
 - ICMP
 - ICMPv6
- 6 Specify **Ports** on the Security Agent endpoint on which to perform the action.

- 7 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.
- 8 Click **Save**.
- 9 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.

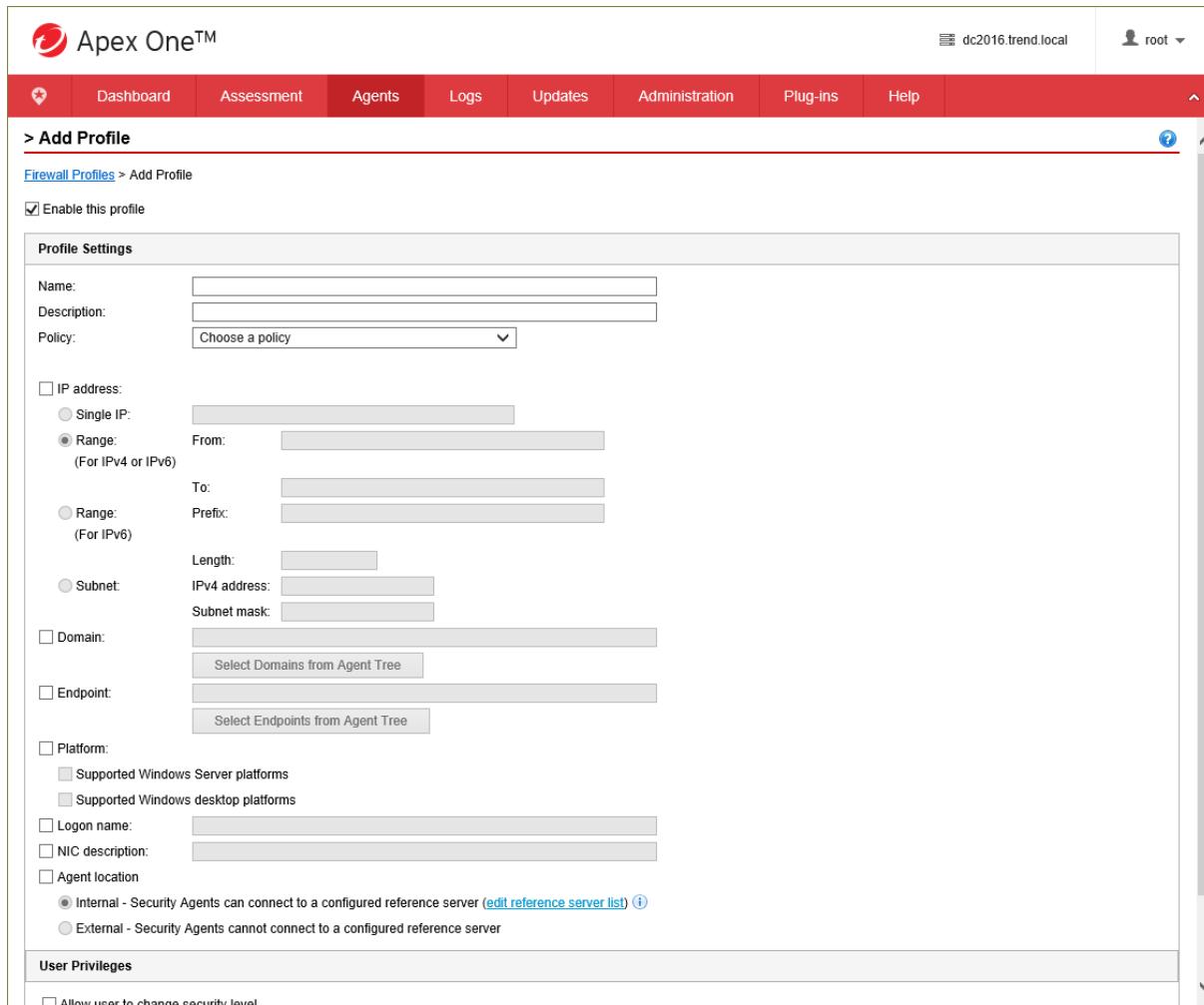
Firewall Profiles

Security Agent endpoints may require different levels of protection. Firewall profiles provide flexibility by allowing you to choose the attributes that a single Agent or group of Agents must have before applying a policy and identifies which Agents will receive the policy.

- 1 To view the available profiles, click **Agents > Firewall > Profiles**.

Order	Name	Associated Policy	Owner(s)	Enabled
1	All agents profile	All access policy	Administrator (Built-in)	<input checked="" type="checkbox"/>

- 2 Click a profile in the list to edit, or click **Add** to create a new profile.



The screenshot shows the Apex One™ software interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root' on 'dc2016.trend.local'. Below the navigation bar, a red header bar says '> Add Profile' and 'Firewall Profiles > Add Profile'. A checked checkbox labeled 'Enable this profile' is visible. The main area is titled 'Profile Settings' and contains several configuration sections:

- Name:** A text input field.
- Description:** A text input field.
- Policy:** A dropdown menu set to 'Choose a policy'.
- IP address:** A section with radio buttons for 'Single IP', 'Range (For IPv4 or IPv6)', and 'Subnet (For IPv6)'. It includes fields for 'From', 'To', 'Prefix', and 'Length'.
- Domain:** A section with a checkbox and a button labeled 'Select Domains from Agent Tree'.
- Endpoint:** A section with a checkbox and a button labeled 'Select Endpoints from Agent Tree'.
- Platform:** A section with checkboxes for 'Supported Windows Server platforms' and 'Supported Windows desktop platforms'.
- Logon name:** A text input field.
- NIC description:** A text input field.
- Agent location:** A section with radio buttons for 'Internal - Security Agents can connect to a configured reference server' (selected) and 'External - Security Agents cannot connect to a configured reference server'.
- User Privileges:** A section with a checkbox for 'Allow user to change security level'.

- 3 Click **Enable this profile** to allow Apex One to deploy the profile to Security Agents.
- 4 Type a **Name** to identify the profile and an optional description.
- 5 Select a **Policy** to be applied through this profile.
- 6 Specify the Agent endpoints to which Apex One applies the policy. Select endpoints based on the following criteria:
 - **IP address**
 - **Domain:** Click **Select Domains from the Agent Tree** and choose a domain

Note: Only users with full domain permissions can select domains.

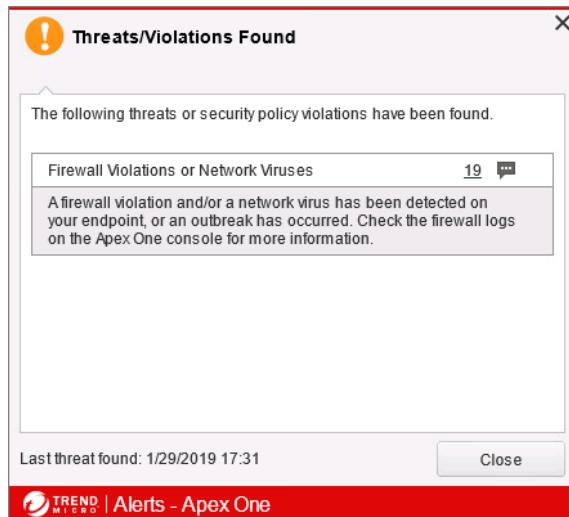
- **Endpoint:** Click **Select Endpoints from the Agent Tree** and choose a specific endpoint
- **Platform**
- **Logon name**
- **NIC description:** Type a full or partial description, without wildcards.

Note: Trend Micro recommends typing the NIC card manufacturer because NIC descriptions typically start with the manufacturer's name. For example, if you typed Intel, all Intel-manufactured NICs will satisfy the criteria. If you typed a particular NIC model, such as Intel (R) Pro/100, only NIC descriptions that start with Intel(R) Pro/100 will satisfy the criteria.

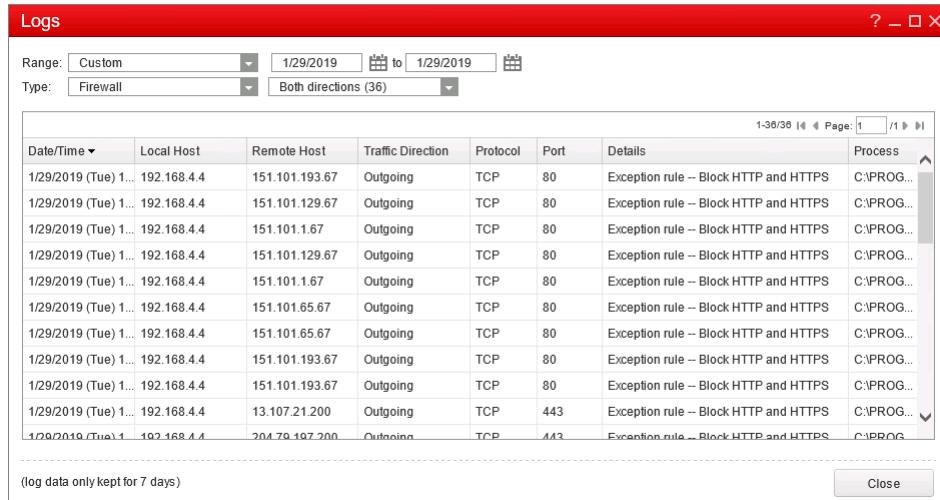
- 7 **Agent Location:** Select from the following:
 - **Internal** - Security Agents can connect to the Apex One Server or a configured reference server
 - **External** - Security Agents cannot connect to the Apex One Server or a configured reference server
- 8 Select whether to grant users the privilege to change the firewall security level or edit a configurable list of exceptions to allow specified types of traffic.
- 9 Click **Save**.
Click **Apply Profile to Agents**. The profile is deployed to the agent identified in the profile. A message is displayed advising you that the Security Agents are being notified of the new settings.

(i) Agents are now being notified. Please allow some time for the new settings to propagate to all agents. Unavailable agents will be notified when they are reconnected to the network.

- 10 When the policy is triggered, a notification is displayed on the Agent computer.



- 11 Click the number next to **Firewall Violations or Network Viruses** to view logging details regarding the firewall violation.



Date/Time	Local Host	Remote Host	Traffic Direction	Protocol	Port	Details	Process
1/29/2019 (Tue) 1...	192.168.4.4	151.101.193.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.129.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.1.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.129.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.1.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.65.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.65.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.193.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	151.101.193.67	Outgoing	TCP	80	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	192.168.4.4	13.107.21.200	Outgoing	TCP	443	Exception rule -- Block HTTP and HTTPS	C:\PROG...
1/29/2019 (Tue) 1...	102.168.4.4	204.70.107.200	Outgoing	TCP	443	Exception rule -- Block HTTP and HTTPS	C:\PROG...

Note: Firewall log uploads will upload every 4 hours by default. This can be changed in the Web Management console under **Agents > Global Agent Settings > Security Settings > Firewall Settings**.

On the Agent this will appear in the Windows Registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\PFW\ActiveLogReportFrequency

Viewing Firewall Rules

Administrators can view the rules currently in effect on an Security Agent by instructing the Agent to dump its firewall logs. By default, the dump of the firewall rules is stored in a text file called !PfwDump.txt created in the Security Agent folder.

To dump firewall logs, complete the following steps:

- 1 Open the Windows Command Prompt and navigate to the Security Agent folder, for example:

C:\Program Files (x86)\Trend Micro\Security Agent

- 2 Type the following command:

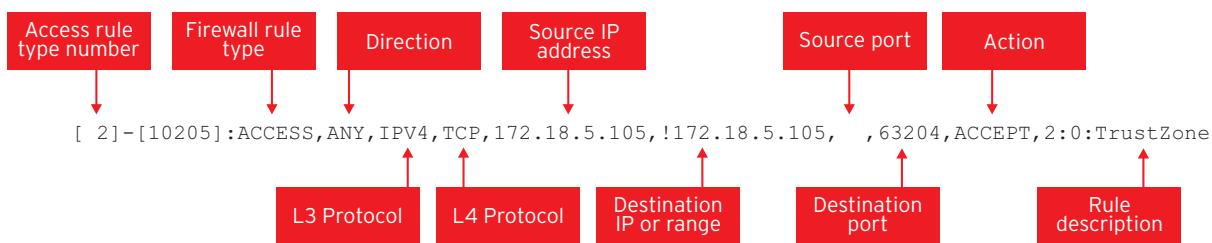
tmpfw dump

3 Locate the !PfwDump.txt file.

The following example shows the access rule-set portion of the dump.

```
===== CFW Rules =====
[65535]-[10]: ACCESS, ANY, IPV4, UDP, , , , 67:68, ACCEPT,
[65535]-[20]: ACCESS, ANY, IPV6, UDP, , , , 546:547, ACCEPT,
.
.
.
[2]-[10205]: ACCESS, ANY, IPV4, TCP, 172.16.5.105, ! 172.16.5.105, , 63204, ACCEPT, 2:0:TrustZone
.
.
.
[1]-[65000]: ACCESS, ANY, IPV4, ANY, , , , DROP, 8:0:Anchor
```

The following diagram shows the different parts of an rule dump file entry.



The following table explains each part of the rule shown:

Rule part	Description
Access rule type number	This identifies the type of access rule.
Firewall rule type	This identifies the type of rule. The ACCESS value in the sample above indicates that it is an access rule.
Direction	Specifies the direction of a packet relative to the Security Agent host. Valid values are: IN, OUT, and ANY.
L3 Protocol	This refers to the Network layer protocol used with the packet. Valid values are IPV4, IPV6, and Any. In the example above, the rule refers to IPv4 traffic.
L4 Protocol	This refers to the Transport layer protocol used with the packet. In the example above, the rule applies to TCP-based traffic.
Source IP address	This is the IP address of the origin of the packet. In the example above, the source is 172.18.5.105.
Destination IP address or range	This is the machine to which the packet is sent. Note the ! used in the example above. This character represents <i>not</i> , therefore, the rule in the sample applied to any packet that was not sent to the source itself.
Source port	This indicates the port through which the packet was sent. In the example above, a source port was not specified.
Destination port	This indicates the port at which an application at the destination is listening for the packet.
Action	This indicates the action that the firewall takes if a packet matches this rule.
Rule description	This is a description of the rule's purpose.

Lesson 13: Preventing Data Loss on Endpoint Computers

Lesson Objectives:

After completing this lesson, participants will be able to:

- Install the Data Protection Plug-in
- Configure Data Protection templates and policies
- Configure Device Control

Apex One uses Data Loss Prevention to protect Agents from the risk of data loss or leakage. Data Loss Prevention safeguards an organization's sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email and external devices
- Enforce compliance to established privacy standards

Data Loss Prevention in Apex One provides the following features:

- Digital Asset Control
- Device Control

Apex One Data Loss Protection

The Security Agent is responsible for the monitoring and detection of digital assets at the endpoint. The Data Loss Prevention Agent communicates with the Apex One Server and acquires the definition of digital assets, compliance templates, company policies, data discovery tasks and other system configurations. Using these definitions, the Agent can monitor and protect digital assets on the endpoint. If sensitive information is detected, it then performs the actions specified in the policies and notifies the server about the violation.

The Security Agent performs the following tasks:

- Scans transferred data and takes action on this data depending on company policies
- Reports security violations to the server

Installing Data Protection

Data Loss Prevention and Device Control are native Apex One features but are **licensed separately**. After you install the Apex One Server, these features are available but are not yet functional and cannot be deployed to Agents until the plug-in has been incorporated into the Apex One Server. You can then activate the Data Protection license to enable the features.

Apex One Data Protection installation and activation in an on-premises deployment are performed from the Plug-in Manager and gets deployed to Agents as soon as the Data Loss Prevention settings are enabled.

SaaS: No plug-in is required for Data Loss Prevention in the service implementation of Apex One.

- 1 In the Apex One Web Management console, click the **Plug-ins** menu. In the **Apex One Data Protection** section, click **Download**.

The screenshot shows the Apex One Web Management interface. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, **Plug-ins** (which is highlighted with a red circle), and Help. Below the navigation bar, there's a sidebar titled "Plug-in Manager". Under this, there's a section for "Apex One Data Protection" which includes a "Manage Program" button, an "Available version: 1.0.1035" link, and a prominent "Download" button (also circled in red). Further down, there's another section for "Trend Micro Endpoint Encryption Deployment Tool" with its own "Manage Program" button, "Available version: 6.0.2040" link, and "Download" button.

- 2 Confirm the download of Apex One Data Protection and click **OK** to proceed.

This screenshot shows the "Apex One Data Protection Download" page. At the top, there's a header with the Apex One logo, the server name "dc2016.trend.local", and a user account icon. Below the header, there's a message: "Downloading Apex One Data Protection version 1.0.1035, please wait. You may navigate to other Apex One pages while downloading." A progress bar indicates the download is at 1%. There's also a small link "[< Back](#)".

3 After the download is complete, click **Install Now**.

The screenshot shows the 'Apex One Data Protection Download' section. A red circle highlights the 'Install Now' button, which is located below the message 'Apex One Data Protection version 1.0.1035 download is complete.'.

4 When prompted, click **Agree** to accept the license agreement.

The screenshot shows the 'Apex One Data Protection License Agreement' section. A red circle highlights the 'Agree' button, which is located at the bottom left of the license text area.

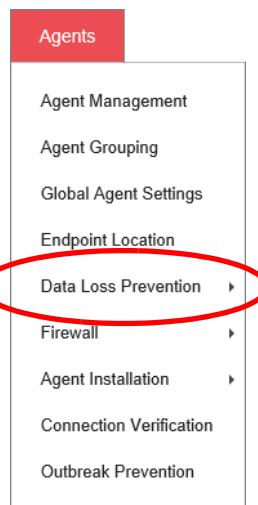
5 Once installed, click **Manage Program**.

The screenshot shows the 'Plug-in Manager' section. A red circle highlights the 'Manage Program' button, which is located in the 'Apex One Data Protection' panel. The button has a small icon of a gear and wrench.

6 Type the Data Protection Activation Code and click **Save**.

The screenshot shows the Apex One™ web interface with a red header bar containing links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The user is logged in as 'root'. The main content area has a title 'Product License New Activation Code' and a sub-instruction: 'To obtain the Activation Code, please [register online](#) using the Registration Key that came with your product.' A large input field labeled 'Apex One Data Protection New Activation Code' contains a string of hyphen-separated boxes. Below this field is a note: '(Tip: Copy the Activation Code and paste it on any of the text boxes above.)'. At the bottom of the form are two buttons: 'Save' and 'Cancel'.

7 A new menu item for Data Loss Prevention become available in the Web Management console.



Digital Asset Control

Digital assets are data and files that an organization must protect against unauthorized transmission. Examples of digital assets are:

- Confidential documents
- Customers private information

Data Identifiers

Administrators define digital assets through:

- Expressions
- File Attributes
- Keyword Lists

Expressions

Expressions define data that has a certain structure. For example, credit card numbers that typically have 16 digits and appear in the format nnnn-nnnn-nnnn-nnnn. Other expressions may be SWIFT or IBAN number, social security numbers (by country), email addresses, postal codes etc. Administrators can use predefined and customized expressions.

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted. Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

Name	Description	Expression	Type
China_UnionPay Card Number	Used to identify a UnionPay account holder's debit or credit card	[^\w-;,&]((62[0-9][4][\s-]*[0-9]{13}) (62[0-9][2][\s-]*[0-9]{4}[^\s-]*[0-9]{4}[^\s-]*[0-9]{4}[^\s-,&])	Predefined
Albania: IBAN (International Bank Account Number)	An international standard for identifying bank accounts with minimal risk of transcription errors	[^\w](A[L\d]{2})(\s(\d{4})s){2}([A-Za-z0-9]{4})s){3}[A-Za-z0-9]{4}\d{8}[A-Za-z0-9]{16}) [^w]	Predefined
All_Credit Card Number	Credit card numbers	[^\w-;,&](\d{14,16}) \d{4}[-]\d{4}[-]\d{4}[-]\d{4} \d{4}[-]\d{6}[-]\d{5}) ^\w;	Predefined
All_Email Address	Email addresses	[^\w.]([^\w.]{1,20}@[\w-9]{2,20}[\.][\w-9-]{2,5}[\w-]{0,10}) ^w.]	Predefined
All_Home Address	Home addresses in the United States and the United Kingdom	\D(\d+\s[a-z-]+\s)([a-z]+\s)(0,2)(\w+ n street st avenue ave road r place pl drive dr circle cr court ct boulevard blvd trail)\. ?[0-9a-z-#s\s]\.]{0,30}[\s,][a-z]{2}\s\d{5}\-\d{4})? ^d-	Predefined
All_IBAN (International Bank Account Number)	An international standard for identifying bank accounts with minimal risk of transcription errors	[^\w]((A-Z){2}\d{2})s? [A-Za-z0-9]{11,27} ([A-Za-z0-9]{4})s){3,6} [A-Za-z0-9]{0,3} ([A-Za-z0-9]{4})s){2}([A-Za-z0-9]{3,4})) ^\w]	Predefined
	Also known as BIN (bank identification		

SaaS: Data Loss Prevention settings, including DLP Data Identifiers, are configured through Apex Central policies in the service implementation of Apex One.

File Attributes

File attributes are file properties such as file type and file size. By themselves, file attributes are poor identifiers of sensitive files, but combining file attributes with other Data Loss Prevention identifiers can result in a more targeted detection of sensitive files.

Data Loss Prevention comes with a predefined file attributes list. This list cannot be modified or deleted. The list has its own built-in conditions that determine if the template should trigger a policy violation.

The screenshot shows a configuration interface for 'File Attributes'. At the top, there's a red header bar with the title 'Data Identifiers' and a help icon. Below it, a blue navigation bar says 'File Attributes > Add File Attributes'. The main area is divided into sections: 'Properties' (Name: [input], Description: [text area]), 'File Attributes' (File type: checkboxes for All, Documents and Encoding Methods, Graphics, Multimedia Files, Compressed Files, Database, Spreadsheets, Presentation and Diagram Files, Linked and Embedded Files, Encrypted Files, and File Extensions), and 'File size' (From [input] bytes To [input] bytes). At the bottom are 'Save' and 'Cancel' buttons.

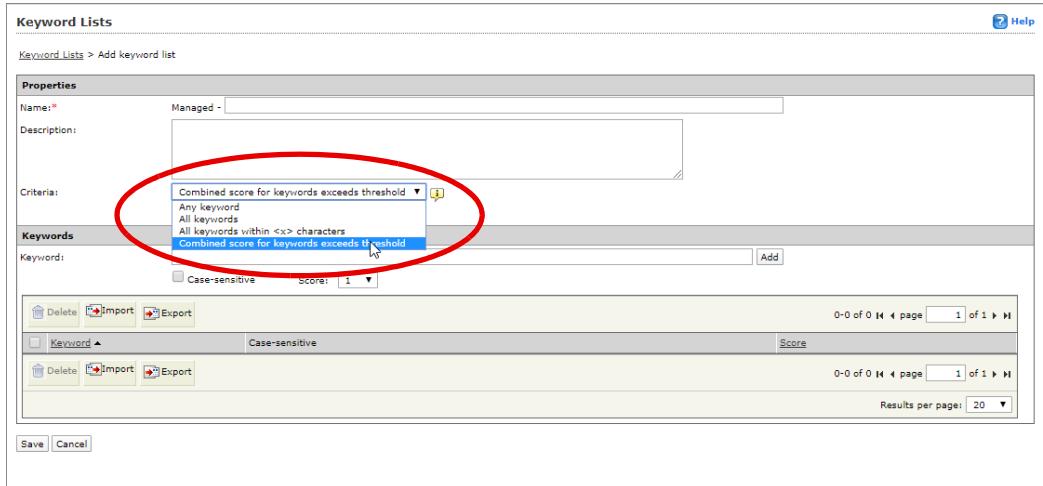
Keyword Lists

keyword lists include special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, *prognosis*, *blood type*, *vaccination*, and *physician* are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a Data Loss Prevention policy and then configure Data Loss Prevention to block files containing these keywords. Each keyword list contains a condition that requires a certain number of keywords be present in a document before the list triggers a violation.

The number of keywords condition contains the following values:

- **All keywords:** All of the keywords in the list must be present in the document.
- **Any keywords:** Any one of the keywords in the list must be present in the document.
- **All keywords within <x> characters:** This condition uses distance between keywords to determine if a violation is present. Distance refers to the amount of characters between the first character of one keyword and the first character of another keyword.

- **Combined score for keywords exceeds threshold:** This condition allows a score to be assigned to each individual keyword, the total scores for each instance of the keywords can not be above the assigned Threshold.



Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

Name	Description	Type
Adult	Words commonly associated with the adult entertainment industry, including pornographic websites	Predefined
Common Medical Terms	Terms used by hospitals and other health care providers	Predefined
Forms_(First_,(Middle)_Name	Common use of the (First), (Middle) and (Last Name) fields in documents such as forms	Predefined
Forms_Date_of_Birth	Common use of the (Birth Date), (Birthdate), or (Date of Birth) fields in documents such as forms	Predefined
Forms_Expiration Date	Common use of terms that indicate the expiration date of an item (such as a credit card) in documents such as forms	Predefined
Forms_First_Name,_Last_Name	Common use of the (First Name) and (Last Name) fields in documents such as forms	Predefined
Forms_Place_of_Birth	Common use of terms that indicate a person's birthplace in documents such as forms	Predefined
Forms_Street,_City,_State	Common use of the (State), (City) and (Street) fields in documents such as forms	Predefined
Japan_Surname_in_Hiragana_(Match_50)	Japanese surnames typed in Hiragana	Predefined
Japan_Surname_in_Kanji_1_(Match_10)	Japanese surnames typed in Kanji	Predefined
Japan_Surname_in_Kanji_2_(Match_50)	Japanese surnames typed in Kanji	Predefined
Japan_Surname_in_Kanji_3_(Match_100)	Japanese surnames typed in Kanji	Predefined
Japan_Surname_in_Katakana_(Match_50)	Japanese surnames typed in Katakana	Predefined
Japan_Surname_in_One-Byte_Katakana_(Match_50)	Japanese surnames typed in one-byte Katakana	Predefined

Data Loss Prevention Templates

A Data Loss Prevention policy contains one or more templates. A Data Loss Prevention template combines data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a Data Loss Prevention policy.

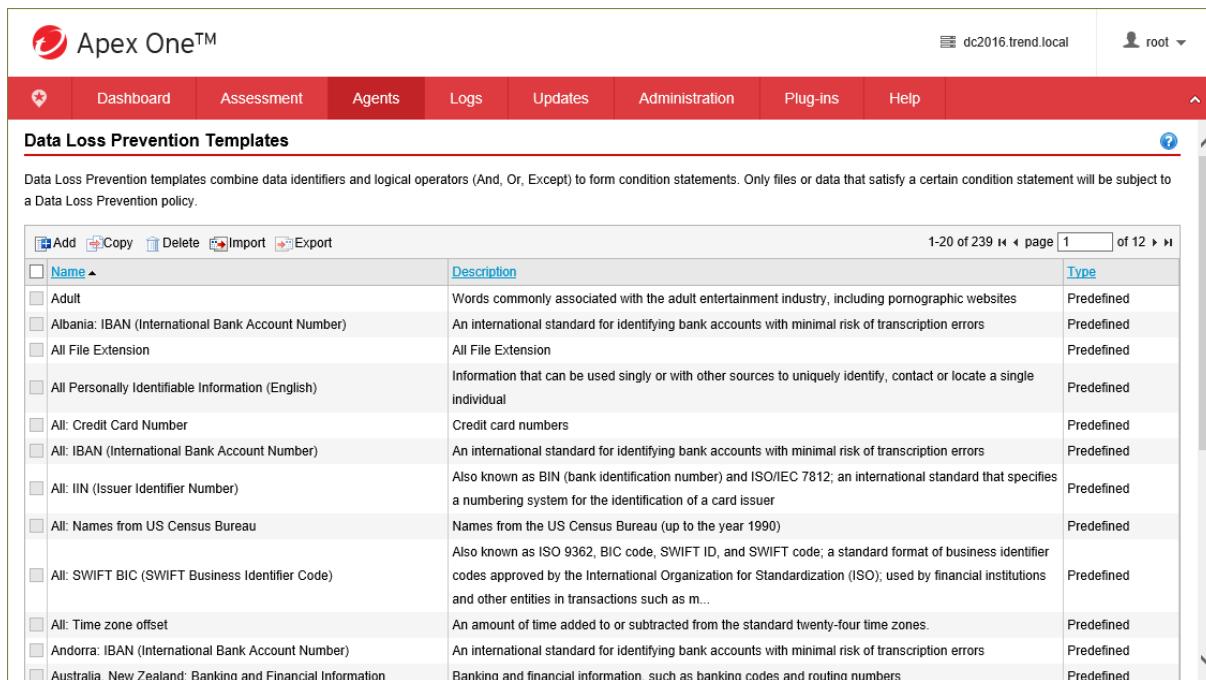
For example, a file must be a Microsoft Word file (**file attribute**) AND must contain certain legal terms (**keywords**) AND must contain ID numbers (**expressions**) for it to be subject to the **Employment Contracts** policy. This policy allows Human Resources personnel to transmit the file through printing so that the printed copy can be signed by an employee. Transmission through all other possible channels, such as email, is blocked. If a file or data matches the definition on more than one template, the higher priority template applies.

Data Loss Prevention comes with the following set of predefined templates that you can use to comply with various regulatory standards, for example:

- **GLBA:** Gramm-Leach-Billey Act
- **HIPAA:** Health Insurance Portability and Accountability Act
- **PCI-DSS:** Payment Card Industry Data Security Standard
- **SB-1386:** US Senate Bill 1386
- **US PII:** United States Personally Identifiable Information

Note: These templates cannot be modified or deleted.

You can also create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.



The screenshot shows the Apex One™ software interface with a red header bar containing the logo, the word "Apex One™", the IP address "dc2016.trend.local", and a user icon labeled "root". Below the header is a navigation menu with links: Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. A question mark icon is in the top right corner. The main content area has a title "Data Loss Prevention Templates". A sub-header states: "Data Loss Prevention templates combine data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a Data Loss Prevention policy." Below this is a table with the following columns: "Name", "Description", and "Type". The table lists 239 entries, with page 1 of 12 shown. Some entries include: "Adult", "Words commonly associated with the adult entertainment industry, including pornographic websites"; "Albania: IBAN (International Bank Account Number)", "An international standard for identifying bank accounts with minimal risk of transcription errors"; "All File Extension", "All File Extension"; "All Personally Identifiable Information (English)", "Information that can be used singly or with other sources to uniquely identify, contact or locate a single individual"; "All: Credit Card Number", "Credit card numbers"; "All: IBAN (International Bank Account Number)", "An international standard for identifying bank accounts with minimal risk of transcription errors"; "All: IIN (Issuer Identifier Number)", "Also known as BIN (bank identification number) and ISO/IEC 7812; an international standard that specifies a numbering system for the identification of a card issuer"; "All: Names from US Census Bureau", "Names from the US Census Bureau (up to the year 1990)"; "All: SWIFT BIC (SWIFT Business Identifier Code)", "Also known as ISO 9362, BIC code, SWIFT ID, and SWIFT code; a standard format of business identifier codes approved by the International Organization for Standardization (ISO); used by financial institutions and other entities in transactions such as m..."; "All: Time zone offset", "An amount of time added to or subtracted from the standard twenty-four time zones"; "Andorra: IBAN (International Bank Account Number)", "An international standard for identifying bank accounts with minimal risk of transcription errors"; and "Australia, New Zealand: Banking and Financial Information", "Banking and financial information, such as banking codes and routing numbers".

Data Loss Prevention Policies

Administrators can limit or prevent transmission of digital assets by creating policies. Apex One evaluates a file or data against the rules defined in the Data Loss Prevention policies. The policies determine files or data that requires protection from unauthorized transmission and the action that Apex One performs after detecting a transmission.

Administrators can configure policies for internal and external Security Agents. Typically, a stricter policy is configured for external Agents. The policies can be enforced for specific Agent groups or individual Agents.

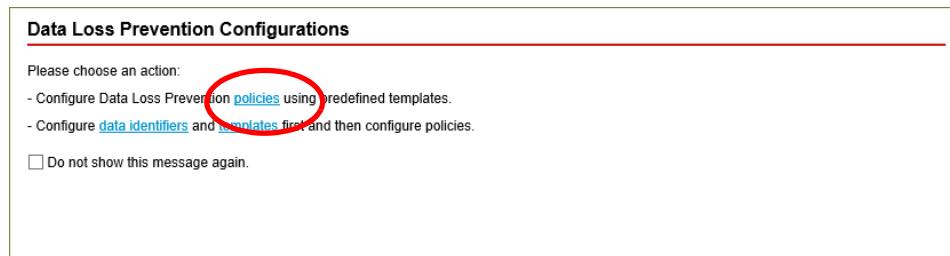
Policies are created by configuring and selecting the following:

- **Template:** Combines data expressions, keywords and file attributes (as described earlier).
- **Channel:** Channels are methods that transmit sensitive information. Data Loss Prevention supports popular transmission channels, such as email, FTP, HTTP/S, IM applications, SMB protocol, and webmail.
- **Action:** Data Loss Prevention performs one or several actions when it detects an attempt to transmit sensitive information through any of the channels. Different actions can be selected when there is a match, like blocking the file, or logging the event. Additional settings can be configured like displaying a notification message to the user or recording the data (makes a copy of the file for forensic/auditing purposes).

Note: Recording sensitive data may consume large amounts of hard disk space. It is highly recommended that you only choose this option for highly sensitive information.

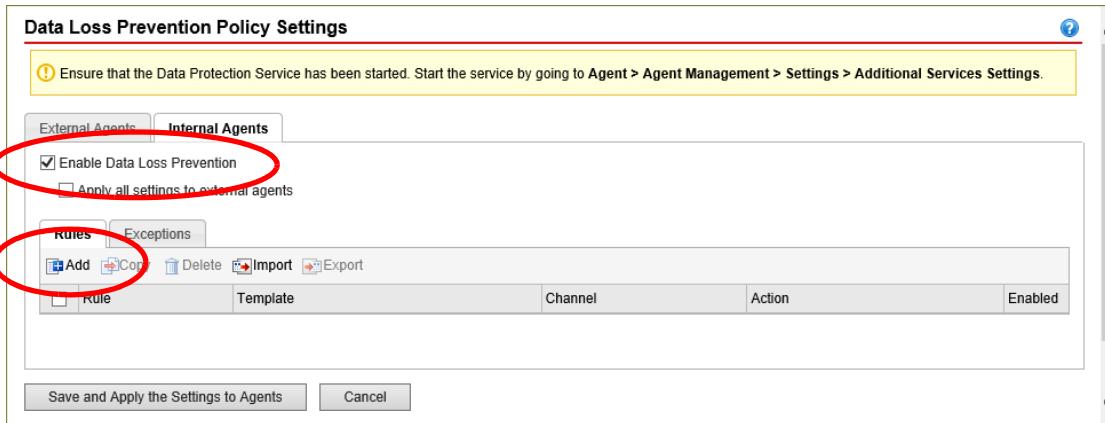
- **Exception:** Exceptions act as overrides to the configured Data Loss Prevention rules.

Data Loss Prevention Policies can be created by selecting the domain, group or Agents receiving the policy in the Agent Management list and clicking **Settings > DLP Settings** from the right-mouse button menu. Click the policies link to begin the policy configuration.



Configuration steps include:

- 1 Enabling Data Loss Prevention and adding new rule.



2 Selecting the template to apply to the policy.

Data Loss Prevention Policy Settings

Ensure that the Data Protection Service has been started. Start the service by going to Agent > Agent Management > Settings > Additional Services Settings.

External Agents Internal Agents

Enable this rule
Rule name: Sample Rule

① Template ② Channel ③ Action

Available templates

View: All templates Search

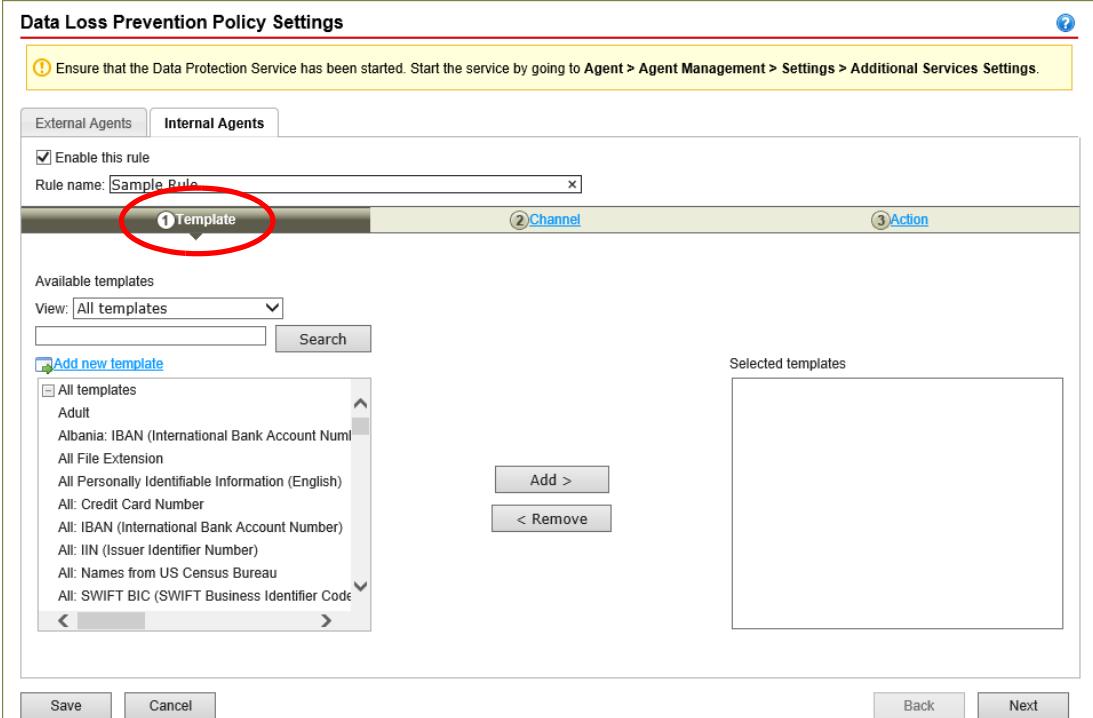
Add new template

- All templates
- Adult
- Albania: IBAN (International Bank Account Num)
- All File Extension
- All Personally Identifiable Information (English)
- All: Credit Card Number
- All: IBAN (International Bank Account Number)
- All: IIN (Issuer Identifier Number)
- All: Names from US Census Bureau
- All: SWIFT BIC (SWIFT Business Identifier Code)

Add > < Remove

Selected templates

Save Cancel Back Next



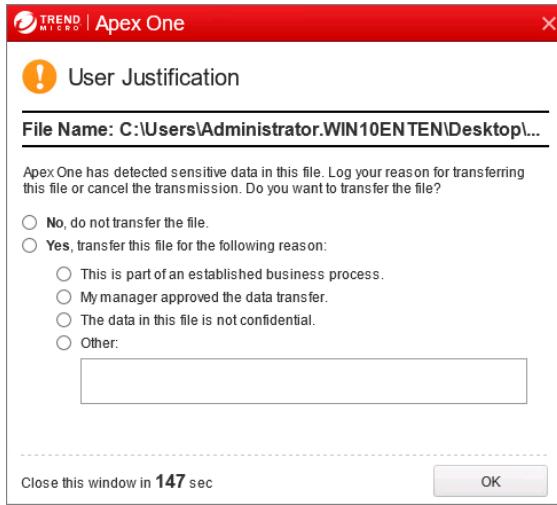
3 Selecting the channel that will be monitored by the policy.

The screenshot shows the 'Data Loss Prevention Policy Settings' window. At the top, there is a yellow tip box: 'Ensure that the Data Protection Service has been started. Start the service by going to Agent > Agent Management > Settings > Additional Services Settings.' Below this are tabs for 'External Agents' and 'Internal Agents', with 'Internal Agents' selected. A checkbox 'Enable this rule' is checked, and the 'Rule name' is set to 'Sample Rule'. The main area has three tabs at the bottom: 'Template' (selected), 'Channel' (circled in red), and 'Action'. Under 'Channel', there are two sections: 'Network Channels' and 'System and Application Channels', each with several checkboxes. In the 'Network Channels' section, all checkboxes are checked: Network Channels, Email clients, FTP, HTTP, HTTPS, IM applications, SMB protocol, and Webmail. In the 'System and Application Channels' section, most checkboxes are checked: Data recorders, PGP encryption, Peer-to-peer applications, Printer, Removable storage, Synchronization software, Windows clipboard, and Cloud storage service. At the bottom are 'Save' and 'Cancel' buttons, and a navigation bar with 'Back' and 'Next' buttons.

4 Selecting the action that will be triggered by the policy.

The screenshot shows the same 'Data Loss Prevention Policy Settings' window, but now the 'Action' tab is selected (circled in red). The main area contains a table with two columns: 'Action:' and 'Additional actions:'. Under 'Action:', there are two radio button options: 'Pass and log' and 'Block', with 'Block' selected. Under 'Additional actions:', there are three checkboxes: 'Notify the agent user', 'Record data', and 'User Justification', with 'User Justification' checked. At the bottom are 'Save' and 'Cancel' buttons, and a navigation bar with 'Back' and 'Next' buttons.

When **User Justification** is enabled, the end user will be able to transfer the file even though the action is set to **Block**, but they must select one of the listed reasons for the transfer before it completes the operation.



The list of justification reasons can be changed by editing the `ofcscan.ini` file on the Apex One Server and modifying the entries listed for `DlpUserJustificationItem`.

Data Loss Prevention Logging

When a violation is detected, the Real-Time Scan Service parses and writes to the violation log.

Data Loss Prevention Logs											
Data Loss Prevention Logs											
Date range All											
Export All to CSV											
1 - 1 of 1 Page 1 of 1 > >											
Date/Time	User Name	Endpoint	Domain	IP Address	Rule Name	Channel	Process	Source	Destination	Action	File/Data Size
14/03/2019 09:36:03	Administrator	CLIENT-02	TrendClassroom	192.168.4.4	Confidential current contracts	SMB	C:\Windows\explorer.exe	C:\Users\Administrator.WIN10ENTEN\Desktop\Data Leak Prevention Test Document.txt	\192.168.4.6\C\$\Data Leak Prevention Test Document.txt	Passed (user justified)	66
Export All to CSV											
1 - 1 of 1 Page 1 of 1 > >											
Results per page 10											
< Back						Close					

Forensic Folder and DLP Database

After a Data Loss Prevention incident occurs, Apex One logs the incident details in a specialized forensic database. Apex One also creates an encrypted file containing a copy of the sensitive data which triggered the incident and generates a hash value for verification purposes and to ensure the integrity of the sensitive data. Apex One creates the encrypted forensic files on the Agent machine and then uploads the files to a specified location on the server.

Since the encrypted forensic files contain highly sensitive data and administrators should exercise caution when granting access to these files.

Apex One integrates with Apex Central to provide Apex Central users with the DLP Incident Reviewer or DLP Compliance Officer roles the ability to access the data within the encrypted files.

Administrators can change the location and deletion schedule of the forensic folder, and the maximum size of files that Agents upload by modifying Apex One's *.ini files.

Note: Changing the location of the forensic folder after logging Data Loss Prevention incidents can cause a disconnect between the database data and the location of existing forensic files. Trend Micro recommends manually migrating any existing forensic files to the new forensic folder after modifying the forensic folder location.

Device Control

Device Control functionality as part of Data Loss Prevention provides a way to:

- Limit the access of an endpoint or a group of endpoints to specific devices
- Define an exception list (Approved Devices) for USB storage devices

Devices that are supported are shown below.

Device Type	Description
CD/DVD	Apex One monitors data recorded to physical and virtual CD/DVD devices (for example, Daemon Tools, PowerISO)
Ports	COM and LPT including all devices under Ports category in Device Manager
Floppy disk controllers	Virtual Machine Floppy Driver. Disk controllers (generally, for drives A/B)
Removable disk drives	Removable disks such as USB drives, Flash drives, storage cards, Hubs etc. NOTE: This option has an exception list discussed below.
IEEE 1394 Bus host controllers	IEEE 1394 interface on devices TIP: Also referred to as Firewire, it is a high-speed, serial input/output bus for computer peripherals and consumer electronics, capable of transfer speeds of up to 400 megabits per second
Imaging devices	Camera, scanners
Infrared devices	Devices that can send and receive infrared data such as infrared transceivers and adapters
Modems	Network interface
PCMCIA adapters	Peripheral interface for laptops TIP: PCMCIA stands for Personal Computer Memory Card International Association
Print Screen key	PrtSc or Print Screen key on keyboard
Wireless NICs	Wireless Network Cards of Trend Micro tested mobile devices
Bluetooth	Bluetooth adapters

Note: Apex One includes a native Device Control feature that regulates access to commonly used devices such as USB storage devices. Device Control included as part of the Data Protection module expands the range of monitored devices.

Lesson 13: Preventing Data Loss on Endpoint Computers

To configure Device Control Setting, select a domain, group or device under **Agent Management** and click **Settings > Device Control Settings**:

Device Control Settings

Additional Service required

External Agents **Internal Agents**

Enable Device Control
 Apply all settings to external agents
Tip: View a list of [supported device models](#) (requires Internet connection).

AutoRun on USB Storage Devices

Block the AutoRun function on USB storage devices

Mobile Devices	Permission
Mobile devices	Allow

Storage Devices	Permission
CD/DVD	Full access
Floppy disks	Full access
Network drives	Full access
USB storage devices	Full access

Non-Storage Devices	Permission
Bluetooth adapters	Allow
COM and LPT ports	Allow
IEEE 1394 interface	Allow
Imaging devices	Allow
Infrared devices	Allow
Modems	Allow
PCMCIA cards	Allow
Print screen key	Allow
Wireless NICs	Allow

Save **Cancel**

Permissions for **Mobile Devices** and **Non-Storage Devices** include:

Permissions	Files on the device	Incoming files
Allow	Permitted operations: Copy, Move, Open, Save, Delete, Execute	Permitted operations: Save, Move, Copy Files can be saved, moved, and copied to the device.
Block (available after installing Data Protection)	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

Permissions for **Storage Devices** include:

Permissions	Files on the device	Incoming files
Full access	Permitted operations: Copy, Move, Open, Save, Delete, Execute	Permitted operations: Save, Move, Copy Files can be saved, moved, and copied to the device.
Modify	Permitted operations: Copy, Move, Open, Save, Delete Prohibited operations: Execute	Permitted operations: Save, Move, Copy
Read and execute	Permitted operations: Copy, Open, Execute Prohibited operations: Save, Move, Delete	Prohibited operations: Save, Move, Copy
Read	Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute	Prohibited operations: Save, Move, Copy
List device content only	Prohibited operations: All operations The device and the files it contains are visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy
Block (available after installing Data Protection)	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

Note: File-based scanning complements, and may override, the device permissions. For example, if the permission allows a file to be opened but the Security Agent detects that the file is infected with malware, a specific scan action is performed on the file to eliminate the malware. If the scan action is **Clean**, the file opens after it is cleaned. However, if the scan action is **Delete**, the file is deleted.

USB Exception List

Removable disk drives support exemptions. To define USB disk drives, the Administrator must provide the following:

- **Vendor Disk:** drive's vendor name
- **Model:** Four bits product number
- **Serial Number:** Another device descriptor in HEX format

Getting these details is not always a straight-forward process. Some manufacturers even have their own way of displaying this information. To address this issue, Device Control provides an Auto-Detect Assistance tool (`listDeviceInfo.exe`).

This tool searches the local system for all connected USB disks and lists the vendor, model and serial number of each device as shown in the example below. The Administrator can then refer to this output to determine the information that needs to be provided in the exception list. A maximum of 200 USB disks can be exempted.

Removable Disk Drives:						
Computer	User	Port	Description	Vendor	Model	Serial ID
MICHAEL	TRENDUS	USB	Lexar USB Flash Drive USB Device	LEXAR	A81D	AAM39GDR0SQ2GIN4
MICHAEL	TRENDUS	USB	Kingston DataTraveler G3 USB Device	KINGSTON	6545	001CC0C83B2CEB81242100B1

Once the details of the USB drive are known, set the permissions for the USB device to **Block** and click **Approved Devices**. Complete the Approved devices list with the details retrieve from `listDeviceInfo.exe`.

* Vendor	Model	Serial ID
LEXAR	A81D	AAM39GDR0SQ2GIN4
KINGSTON	6545	001CC0C83B2CEB81242100B1

Approved USB storage devices will have the following permission:
Permission: Full access

< Back

Note: By default, Device Access Control violations will be collected for a period of 1 hour, then uploaded to the Apex One server. In environments with many Agents with strict controls, this could generate a large increase in the amount of logs sent to the server.

On the Agent this value will appear in the Registry under:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion\AEGIS\SendLogPeriod

Lesson 14: Deploying Policies Through Trend Micro Apex Central

Lesson Objectives:

After completing this lesson, participants will be able to:

- Register Apex Central in Apex One
- Configure Apex One policies in Apex Central for deployment to endpoints

Policies are used to enforce product settings on managed products. In Apex Central, policies for endpoints can be managed centrally from the Apex Central Web Management console. Administrators can set policies on endpoints identified using different criteria within Apex Central.

Policy Management is a powerful feature in Apex Central as it allows administrators to enforce settings on specific products and specific targets from a single console. Administrators can assign a policy to a large number of endpoints which sit across different servers and even across different domains.

Administrators can group endpoints from the Apex Central Web Management console instead of using the traditional Apex One server-domain structure product tree to manage endpoints. They can also easily check all deployment results from the Policy list, Policy Status widget and Data Leak Prevention violation widget and they can troubleshoot according to policy status of each endpoint returned by product.

Apex Central

Apex Central (previously known as Control Manager) provides a centralized console to manage, monitor, and report across multiple layers of security in all your Trend Micro product deployments.

Customizable data displays provide the visibility and situational awareness for administrators to rapidly assess status, identify threats, and respond to incidents. Administration can be streamlined to achieve more consistent policy enforcement with single-click deployment of data protection policies across endpoint, messaging, and gateway solutions.

User-based visibility shows what is happening across all endpoints owned by users, enabling administrators to review policy status and make changes across all user devices.

In the event of a threat outbreak, administrators have central access point for complete visibility of an environment to track how threats have spread.

With a better understanding of security events, it becomes easier to prevent them from reoccurring. Direct links to Trend Micro Threat Connect database provides access to actionable threat intelligence, which allows administrators to explore the complex relationships between malware instances, creators, and deployment methods. Apex Central is then able to apply policy on how these suspicious objects should be treated.

Lesson 14: Deploying Policies Through Trend Micro Apex Central

Apex One sends and can retrieve suspicious objects from Apex Central. Additionally, Apex One can leverage Scan Actions (for example Log or Block) from Apex Central.

The Dashboard in the Apex Central console provides the status summary for the entire Apex Central network.

The screenshot shows the Trend Micro Apex Central™ dashboard with the following sections:

- Critical Threats:** Last refreshed: 02/14/2019 14:56:46. Range: 1 Week. 0 critical threat types. Threat Type table:

Threat Type	Important Users	Other Users
Ransomware	0	0
Known Advanced Persistent Threat (APT)	0	0
Social engineering attack	0	0
Vulnerability attack	0	0
Lateral movement	0	0
Unknown threats	0	0
C&C callback	0	0
- Ransomware Prevention:** Last refreshed: 02/14/2019 14:56:46. Period: 1 week. Trend Micro can block ransomware threats at every stage of an attack. Learn More.
- Exposure Layer:** Last refreshed: 02/14/2019 14:57:02. 0 messages, 0 websites, 0 network traffic, 0 cloud sync.
- Infection Layer:** Last refreshed: 02/14/2019 14:57:02. 0 files, 0 behaviors.
- Users with Threats:** Last refreshed: 02/14/2019 14:57:02. Range: 1 Week. 0 important users, 0 other users.
- Endpoints with Threats:** Last refreshed: 02/14/2019 14:57:02. Range: 1 Week. 0 important endpoints, 0 other endpoints.

Apex Central Services

The following services are installed as part of Apex Central.

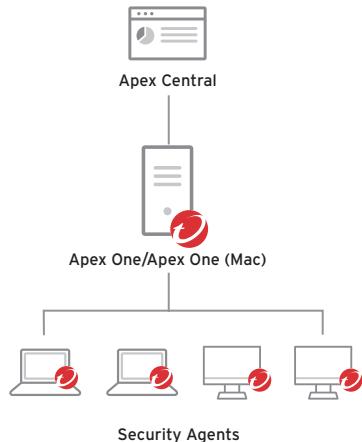
Component	Description
Trend Micro Apex Central Service (ProcessManager.exe)	This component launches and stops other Apex Central core processes.
Trend Micro Management Infrastructure (cm.exe)	Provides the Apex Central Web Management console and manages the Product Directory. Also manages the Message Routing Framework (the Communicator) which serves as the communications backbone for Apex Central. This component of the Trend Micro Infrastructure handles all communication between the Apex Central Server and managed products for all older Control Manager agents. They interact with older Control Manager agents to communicate with managed products.

Apex Central Management Modes

Apex Central can be deployed in a few different management modes, including a pure on-premises, cloud or hybrid deployment.

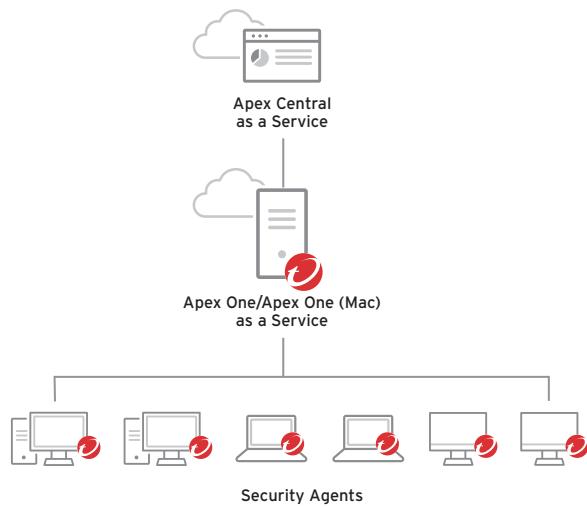
On-premises Management Mode

In on-premises management mode, an Apex Central Server is deployed to provide management and policy deployment capabilities to Apex One and Apex One (Mac) Servers. In this type of deployment, the Apex Central and Apex One Servers are installed on premises.



Cloud Management Mode

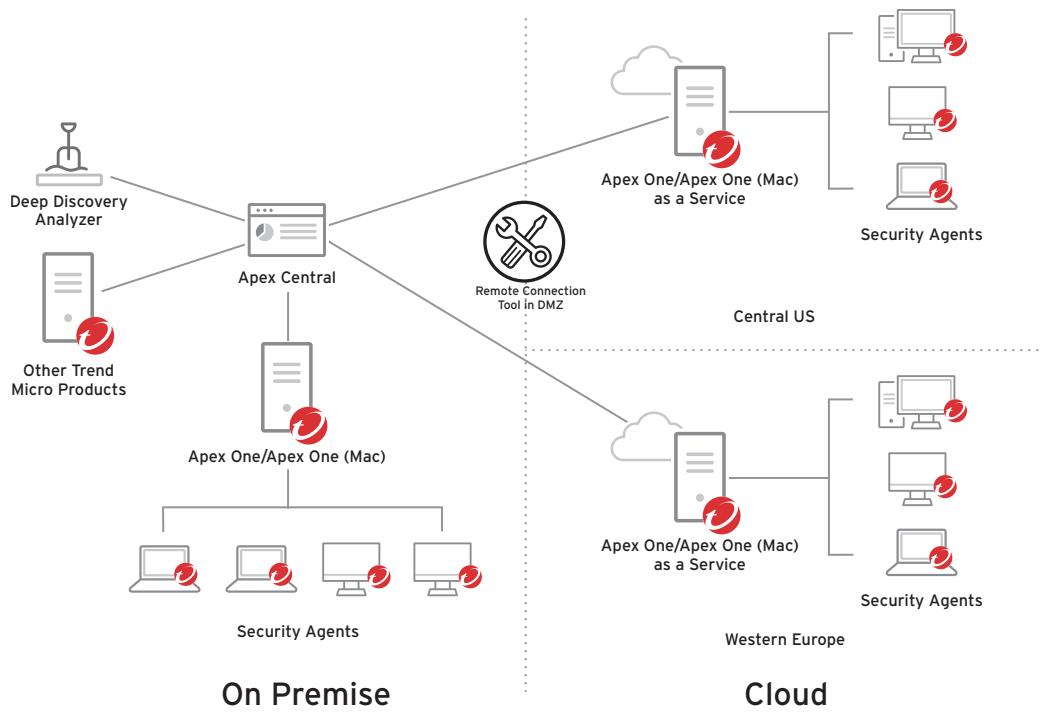
In cloud management mode, an instance of Apex Central as a Service is deployed to provide management and policy deployment capabilities to instances of Apex One and Apex One (Mac) as a Service.



Hybrid Mode

This management mode uses a combination of on-premises and cloud “as a service” servers. In the example displayed here, multiple instances of Apex One as a Service as well as an on-premises deployment of Apex One are registered to an on-premises Apex Central Server. This on-premises Apex Central can manage other Trend Micro products, like Deep Discovery Analyzer, Deep Security, Trend Micro Scan Mail for Microsoft Exchange and others.

This type of installation requires the Remote Connection Tool in the DMZ to allow the SaaS product consoles to register to the on-premises Apex Central Server. The Remote Connection Tool will run as a service named SmartRelay (Smart Relay Service).



The Remote Connection Tool can be downloaded, along with details on its use, from the Trend Micro Customer Success Web site at:

<https://success.trendmicro.com/solution/1118614-setting-up-apex-one-as-a-service-remote-connection-to-control-manager-tmcm>.

Managing Apex One Policies in Apex Central

To manage Apex One policies through Apex Central in an on-premises installation, an administrative user would complete the following steps:

- 1 Connect Apex Central and Apex One.
- 2 Create a user account for the Apex Central administrator in Apex One.
- 3 Add Apex One to the Apex Central Product Directory.
- 4 Select the Apex One Security Agent as the product on which you will configure policy settings.
- 5 Select the endpoints on which to assign and deploy the policy.
- 6 Create a policy template by identifying the policy settings required.
- 7 Deploy the policy.

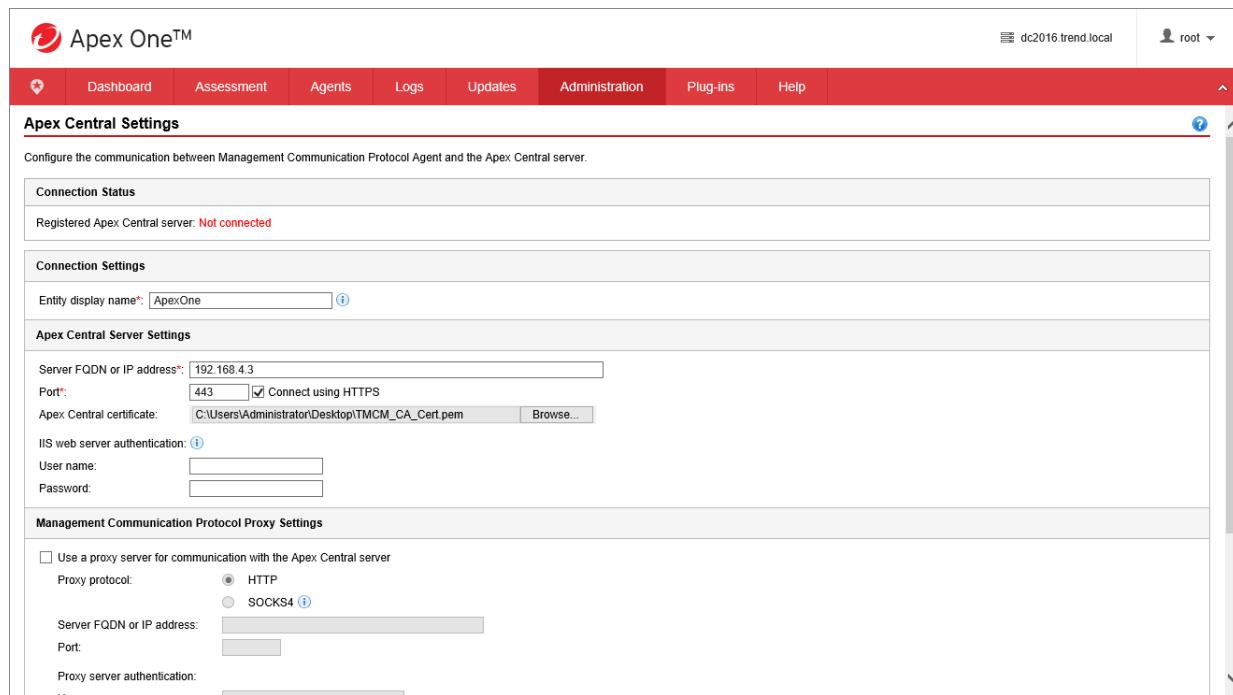
When a policy is created, administrators are able to specify the policy targets and the settings to be applied. However, as the policy can only cover endpoints where the Apex Central administrative user has access, it is important to plan who will create the policy. It is also possible for multiple administrators to have the same policy settings but different targets because they have only access to specific endpoints and entities.

Connecting Apex One and Apex Central

Communication between Apex One and Apex Central is configured through the Apex One Web Management console.

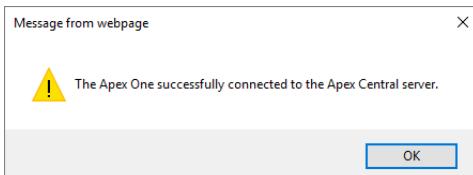
- 1 On the Apex Central server, locate the digital certificate created during the setup of the server. The certificate file is called `TMCM_CA_Cert.pem` and is located in the following folder on the Apex Central Server:
`C:\Program Files (x86)\Trend Micro\Control Manager\Certificate\CA\`
- 2 Log into the Apex One Web Management console and click **Administration > Settings > Apex Central**.
- 3 In the **Apex Central Settings** window, the **Connection Status** should be displayed as **Not connected**.

Complete the details of the Apex Central Server as follows:



- **Entity display name:** Type a name for the Apex One Server. This is the name used to display the Apex One Server in Apex Central.
- **Server FQDN or IP address:** Type the server fully qualified domain name or IP address.
- **Port:** Accept the default port of 443
- **Apex Central Certificate:** Click **Browse** and locate the `TMCM_CA_Cert.pem` certificate file from the Apex central Server

4 Click **Test connection**. A connection was successful message should be displayed. Click **OK**.



5 Click **Register**. The connection status is updated.



Creating an Apex Central User Account

The Apex Central administrator must have an account in Apex One with the appropriate administrative permissions. This account will enable single sign-on into Apex One from Apex Central.

- 1 Log into the Apex One Web Management console and click **Administration > Account Management > User Accounts**.
- 2 Click **Add** to create a new account. Complete the details for the account as follows:

User Accounts

Step 1 User Information >>> Step 2 >>> Step 3

Enable this account

User Roles

Select role:

User Information

Custom account

User name *: Use A to Z, a to z, 0 to 9, -, or _

Description *: Note: The following characters are not supported: <>&“

Password *:

Confirm password *:

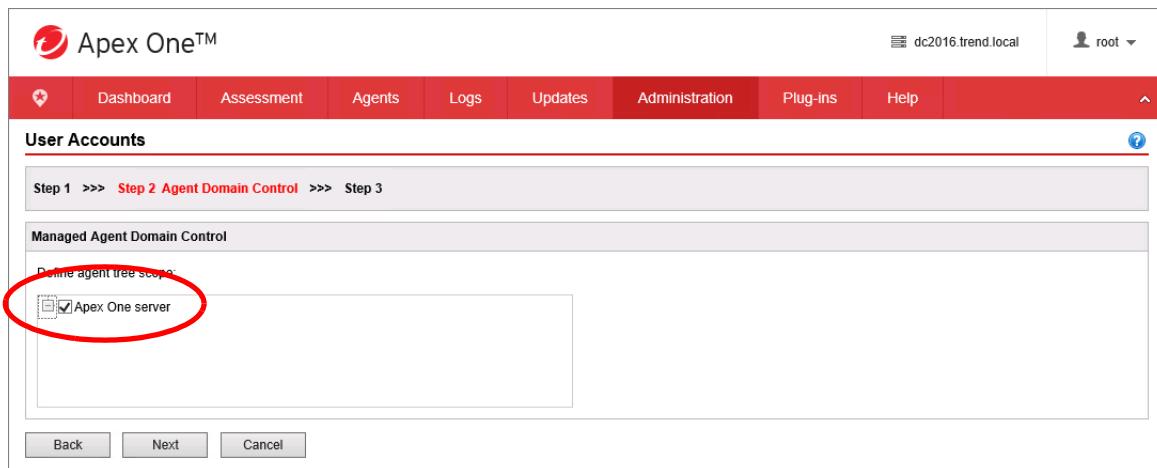
Email address:

For example: johnsmith@yourcompany.com

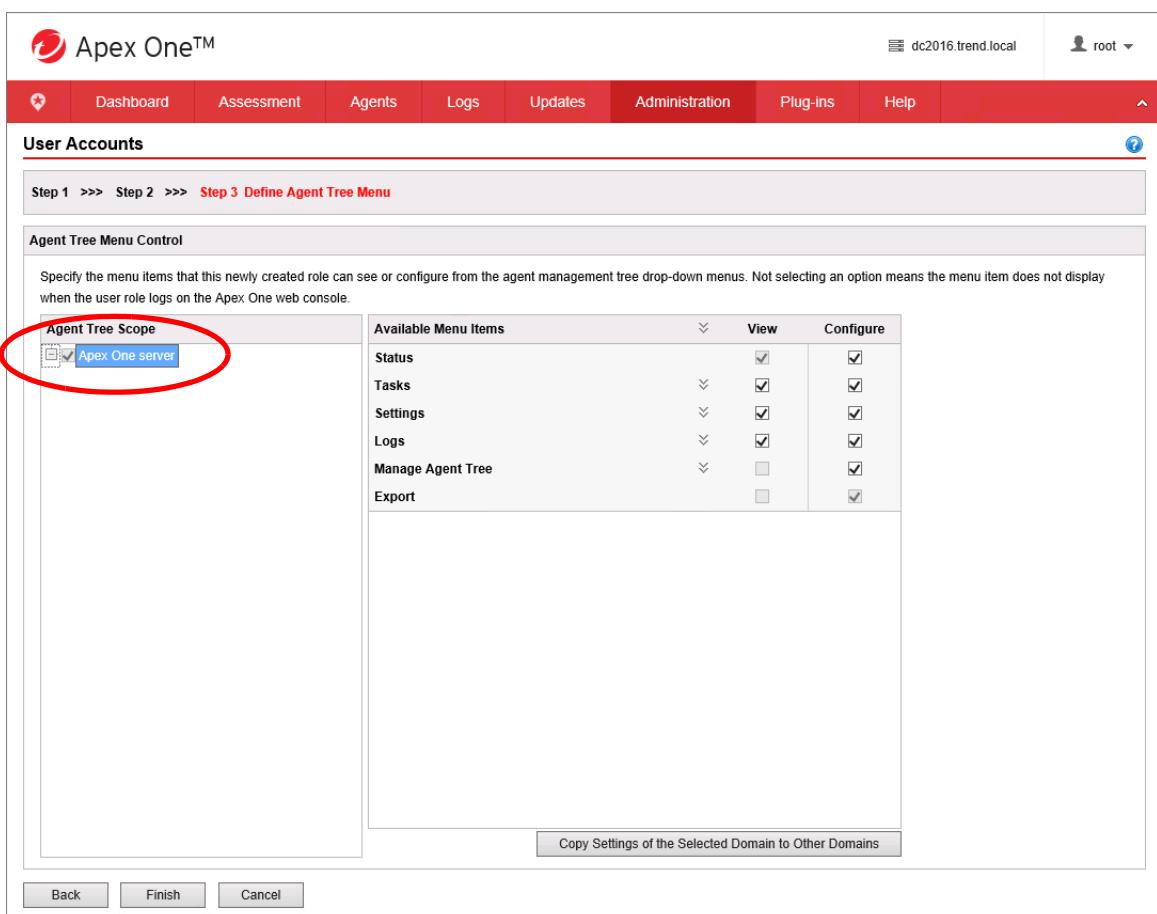
- **Select Role:** Select **Administrator (Built-in)** from the list
- **User name:** Type the name of the Apex Central administrator **as identified during the Apex Central setup**
- **Password:** Type the password for the Apex Central administrator **as identified during the Apex Central setup**

Click **Next**.

- 3 Select the Agent Tree Scope to define the branches of the Agent Tree this administrator will have control over. The top branch of **Apex One Server** is selected by default, click **Next**.



- 4 To enable the Apex One items that the Apex Central account will have permissions to control, click the **Apex One Server** at the top of the list and click **Finish**.



- 5 The new user account is displayed.

The screenshot shows the 'User Accounts' section of the Apex One interface. It displays two rows of user information:

Username	Description	Domain	Role	Enable
admin	Apex Central administrator account		Administrator (Built-in)	<input checked="" type="checkbox"/>
root	Administrator account created during installation		Administrator (Built-in)	<input checked="" type="checkbox"/>

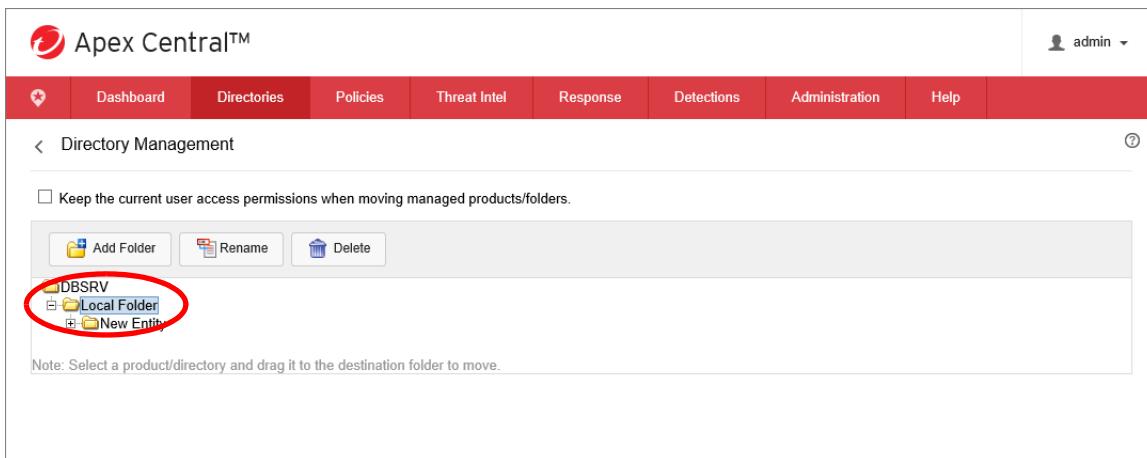
Adding Apex One to the Apex Central Product Directory

New products added to Apex Central are assigned to a folder in the Product Directory called **New Entity** by default. The product must be reassigned to another folder to enable management through Apex Central and assign the appropriate management permissions.

- In the Apex Central Web Management console, click **Directories > Products** and click **Directory Management**.

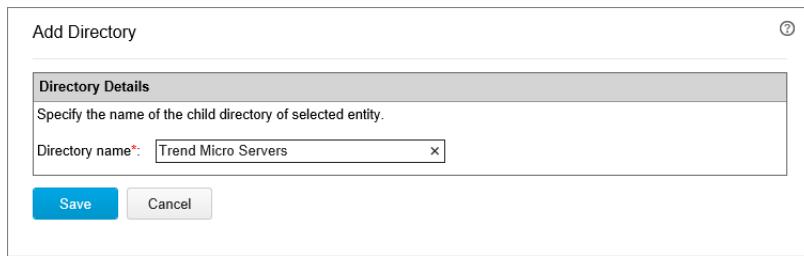
The screenshot shows the 'Product Directory' section of the Apex Central interface. The top navigation bar includes tabs for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The 'Directories' tab is selected. Below the navigation bar, there is a search bar labeled 'Find entity:' and several buttons: Advanced Search, Configure, Tasks, and Directory Management. The 'Directory Management' button is highlighted with a red circle. On the left, there is a sidebar with a tree view showing 'DBSRV' and its subfolders 'Local Folder' and 'Search Result'. The main panel shows a table with one row containing 'DBSRV\'. There are 'Status' and 'Folder' buttons at the bottom right of the main panel.

2 Click Local Folder, and click Add Folder.

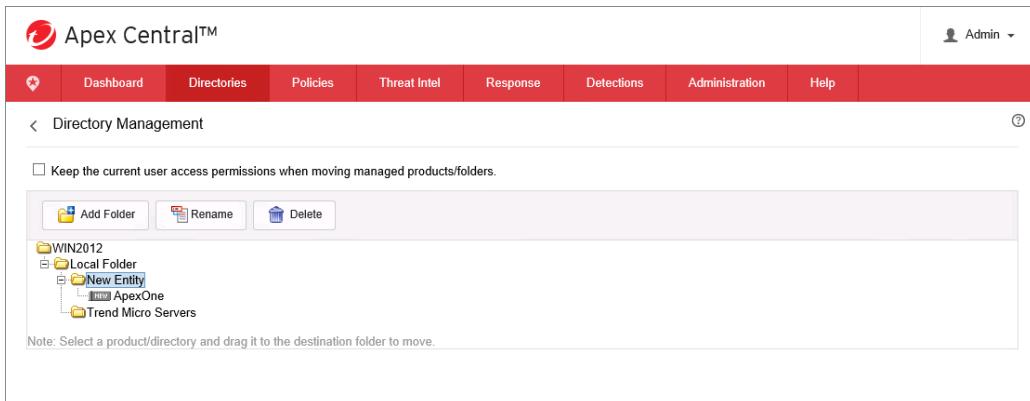


The screenshot shows the 'Directory Management' section of the Apex Central interface. At the top, there's a navigation bar with tabs like Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The user is logged in as 'admin'. Below the navigation bar, there's a sub-navigation for 'Directory Management' with a note about keeping current user access permissions. There are buttons for 'Add Folder', 'Rename', and 'Delete'. Under the main tree view, 'DBSRV' is expanded, showing 'Local Folder' and 'New Entity'. A red circle highlights 'Local Folder'. A note at the bottom says 'Note: Select a product/directory and drag it to the destination folder to move.'

3 Type a name for a new folder (or directory), for example, Trend Micro Servers and click Save. Click OK to confirm the creation of the directory.

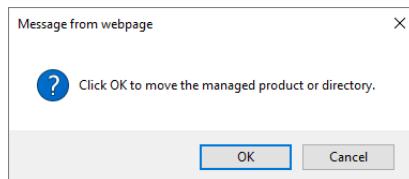


4 Expand the New Entity folder. Drag the Apex One Server device from New Entity folder to the newly created folder.



The screenshot shows the 'Directory Management' section again. The 'DBSRV' folder is expanded, showing 'Local Folder' and 'New Entity'. 'New Entity' is expanded, showing 'ApexOne'. A note at the bottom says 'Note: Select a product/directory and drag it to the destination folder to move.'

When prompted, click OK to acknowledge the move.



The Apex One Server should be displayed in the **Trend Micro Servers** folder.

The screenshot shows the Apex Central interface with the title 'Apex Central™'. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The user is logged in as 'Admin'. The main content area is titled 'Directory Management' and contains a note about keeping current user access permissions when moving managed products/folders. Below this are buttons for Add Folder, Rename, and Delete. A tree view shows a 'Local Folder' node with a 'Trend Micro Servers' folder, which contains an 'ApexOne' item. A red circle highlights the 'Trend Micro Servers' folder. A note at the bottom says 'Note: Select a product/directory and drag it to the destination folder to move.'

Selecting the Destination Product

Apex Central can deploy policy settings to a variety of Trend Micro products. The Apex One Security Agent can be selected as the destination product to receive policy attributes for protecting endpoint computers.

In the Apex Central Web Management console, click **Policies > Policy Management**. In the **Product** list, select **Apex One Security Agent**. To create a policy for this product, click **Create** or **Create one now**.

The screenshot shows the Apex Central interface with the title 'Apex Central™'. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The user is logged in as 'admin'. The main content area is titled 'Policy Management' and shows a 'Product' dropdown set to 'Apex One Security Agent'. Below the dropdown are buttons for Create, Copy Settings, Inherit Settings, Import Settings, Export Settings, Delete, Reorder, Change Owner, and Refresh. A table header includes columns for Priority, Policy, Parent Policy, Deviations, Owner, Last Editor, Last Edited, Targets, Deployed, Pending, Offline, and With Issues. A message at the bottom states 'You have not created a policy. [Create one now](#)'. A red circle highlights both the 'Apex One Security Agent' selection and the 'Create one now' link.

Identifying Policy Targets

Administrators can manually select the target endpoint or use a filter to automatically assign targets to their policies. The target selection can be dynamic filtering or static binding and can be selected by IP subnet, operating system, naming rules in the Apex Central product tree or Active Directory organizations units.

The screenshot shows the 'Create Policy' page in the Trend Micro Apex Central web interface. At the top, there's a navigation bar with links like Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. On the left, there's a sidebar titled 'Apex One Security Agent Settings' with several collapsed sections: Additional Service Settings, Application Control Settings, Behavior Monitoring Settings, Device Control Settings, Endpoint Sensor Settings, Manual Scan Settings, and Predictive Machine Learning Settings. In the main content area, there's a form for creating a policy. The 'Policy Name' field contains 'Demo_Policy'. Below it, the 'Targets:' section is highlighted with a red oval. It contains three radio button options: 'None (Draft only)', 'Filter by Criteria', and 'Specify Target(s)'. The 'None (Draft only)' option is selected. There are also 'Set Filter' and 'Select' buttons next to the radio buttons.

None (Draft only)

This option provides a way to save a policy definition **without** applying it to any targets. This allows an administrative user to fine tune settings and then switch over to either a **Specified** or **Filtered** policy that can be put into actual use. Drafts have the lowest priority and always stay in the bottom of the Policy List.

Filter by Criteria

Filter by Criteria is useful for deploying standard settings to a group of targets across the organization. The filter uses known characteristics for devices, including operating system, location, IP address or other metrics for the devices. If the specified criteria matches, Apex Central applies the corresponding policy. If the matching characteristics change over time, then a different policy gets deployed.

The screenshot shows the 'Filter by Criteria' dialog box. At the top, it says 'Define a filter to automatically assign current and future targets to the policy.' Below that, it says 'Match all of the selected criteria:' followed by four checkboxes: 'Match keywords in:', 'IP addresses:', 'Operating systems:', and 'Directories:'. Next to each checkbox is a dropdown menu and a text input field. For 'Match keywords in:', the dropdown is 'Host name' and the input field is empty. For 'IP addresses:', the dropdown is 'to' and the input field is empty. For 'Operating systems:', the dropdown is 'Add operating systems' and the input field is empty. For 'Directories:', the dropdown is 'Product Directory' and the input field is empty. At the bottom right of the dialog box are 'Save' and 'Cancel' buttons.

Specify Target(s)

This option is useful for deploying settings only to specific target devices. This method uses a static assignment, meaning once a policy is assigned to a selected targets, the assigned policy will never change or be re-evaluated. **This policy also has the highest priority and will always apply.** For a server in an environment where the security policy MUST be the same policy and never change, use **Specify Target(s)** to deploy a policy that is locked to the specified device(s).

Endpoint/Product	Assigned Policy	Policy Status	IP	Operating System
CLIENT-01		Without policy	192.168.4.2	Windows Server 2016
CLIENT-02		Without policy	192.168.4.4	Windows 10
CLIENT-03		Without policy	192.168.4.6	Windows 10
DC2016		Without policy	192.168.4.1	Windows Server 2016
WIN2012		Without policy	192.168.4.3	Windows Server 2012 R2

In the list of endpoints, click to select the appropriate endpoints and click **Add Selected Targets**. Click **OK**.

When defining policy targets, certain limitations must be kept in mind:

- Administrative users cannot apply a policy to a target which is listed under the **New Entity** folder in the Product Directory. Administrative users cannot browse or search for a target under this folder.

The target must be moved from the **New Entity** folder to another folder **before** creating the policy.

- Apex Central policy assignments are **not incremental; all settings deployed by the policy will overwrite any existing settings** that are currently configured on the endpoint.
- A specified policy takes precedence over a filtered policy. In the case where a server or endpoint matches multiple specified policies, the latest policy gets applied to the target. However, if a server or endpoint matches multiple filtered policies, it takes the first policy that it matched based on the order of priority. The priority order can be rearranged to meet the administrative requirement. Only one policy is applied to a server or endpoint.

For example, if Web Reputation must always be disabled for all developer workstations that are located on an isolated and secure subnet within an environment, administrative users can deploy a policy using **Specify Targets** (hard coded policy) that has Web Reputation turned OFF. Then, **Filter by Criteria** could be used to assign an additional policy with Web Reputation enabled to only Windows platform users.

Defining Policy Settings

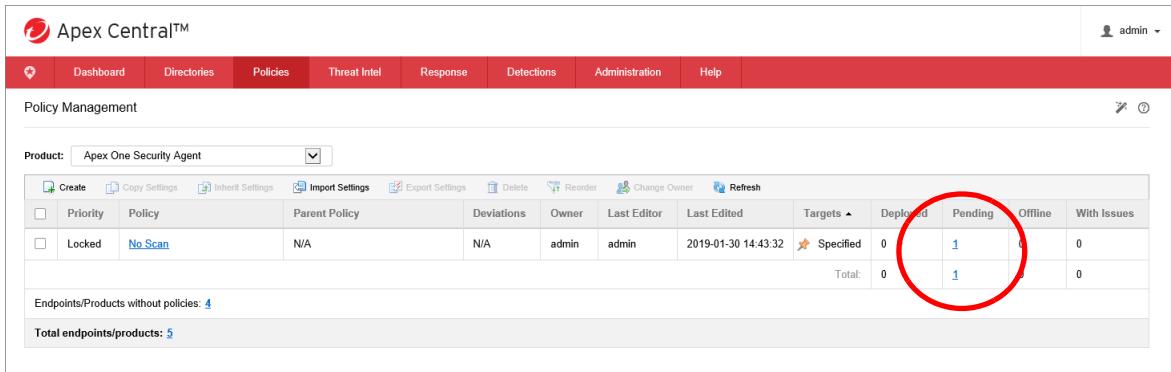
Once Apex Central deploys a policy to the target endpoints, the settings defined in the policy will **overwrite any settings configured for these targets by the Apex One Server**. Apex Central re-enforces the policy settings in the targets every 24 hours.

Although local administrators can make changes to the settings from the Apex One Web Management console, these changes are overwritten **every time Apex Central re-enforces the policy settings**. For certain product settings, Apex Central needs to obtain specific setting options from the managed products. If administrators select multiple targets for a policy, Apex Central can only obtain the setting options from the first selected target. To ensure a successful policy deployment, make sure the product settings are synchronized across the targets.

The screenshot shows the Trend Micro Apex Central web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies (which is currently selected), Threat Intel, Response, Detections, Administration, and Help. A user icon labeled 'admin' is also present. Below the navigation, a breadcrumb trail says '< Create Policy'. The main content area is titled 'Policy Name: Demo_Policy'. It includes sections for 'Targets' (with options for None (Draft only), Filter by Criteria, Set Filter, and Manage Targets, currently showing 3 target(s)), and 'Apex One Security Agent Settings' which includes 'Additional Service Settings', 'Application Control Settings', and 'Behavior Monitoring Settings'. Under 'Behavior Monitoring Settings', there's a note about 'Additional Services required'. Below this, there are tabs for 'Rules' (selected) and 'Exceptions'. The 'Malware Behavior Blocking' section contains a checked checkbox for 'Enable Malware Behavior Blocking' and a dropdown menu for 'Threats to block' set to 'Known and potential threats'. The 'Ransomware Protection' section has several checkboxes: 'Protect documents against unauthorized encryption or modification' (checked), 'Automatically back up and restore files changed by suspicious programs' (checked), 'Block processes commonly associated with ransomware' (unchecked), and 'Enable program inspection to detect and block compromised executable files' (checked). A note below states: 'Note: Program inspection provides increased security if you select "Known and potential threats" in the Threats to block drop-down.' The 'Anti-exploit Protection' section has one checkbox: 'Terminate programs that exhibit abnormal behavior associated with exploit attacks' (unchecked).

Deploying the Policy

Once the policy settings are configured and the target selected, click **Deploy**. The Apex One policy defined in the Apex Central Web Management console gets saved in the Apex One database and deployed to selected target products. The policy will display in the **Policy Management** list as **Pending** until it is applied on the endpoint. It takes several minutes for the policy to be applied to the endpoint.



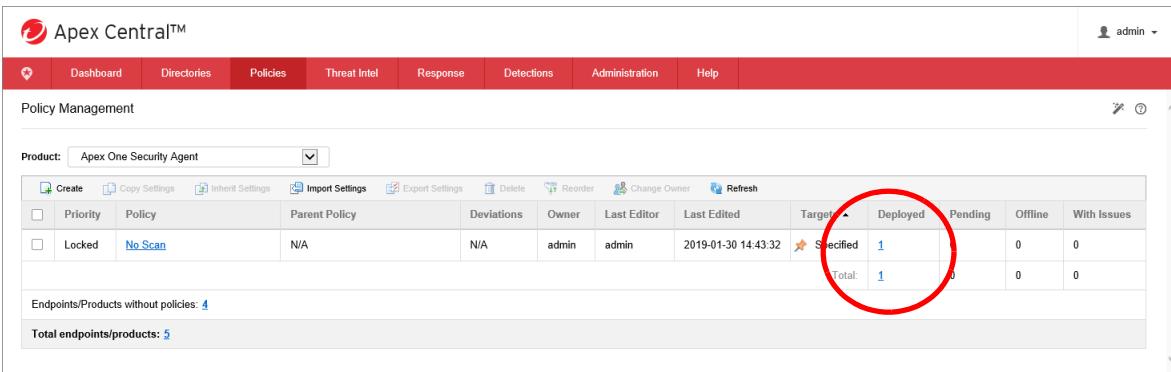
The screenshot shows the Trend Micro Apex Central web interface under the 'Policies' tab. A single policy entry is listed in the table:

Priority	Policy	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
<input type="checkbox"/>	No Scan	N/A	N/A	admin	admin	2019-01-30 14:43:32	Specified	0	1	0	0

Total: 0 Pending: 1

A red circle highlights the 'Pending' column value '1'.

Once applied, the endpoint will display with a status of **Deployed**.



The screenshot shows the Trend Micro Apex Central web interface under the 'Policies' tab. The same policy entry is now displayed with a 'Deployed' status:

Priority	Policy	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
<input type="checkbox"/>	No Scan	N/A	N/A	admin	admin	2019-01-30 14:43:32	Specified	1	0	0	0

Total: 1 Deployed: 1

A red circle highlights the 'Deployed' column value '1'.

Policy Inheritance

Policy inheritance is useful in deployments with several Apex One Servers and where an Apex Central administrative user manages global Apex One policies, and regional administrators defines local or regional policies requiring more specific settings.

Priority	Policy	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets ▾	Deployed	Pending	Offline	With Issues
<input checked="" type="checkbox"/>	Demo_Policy	N/A	N/A	admin	admin	2019-02-14 15:23:44	⚠ Specified	2	1	0	0
Total: 2 1 0 0											

Click to select a policy in the list and click **Inherit Settings**.

Configure the child policy settings in the policy to be inherited, customized, or extended by child policies.

Manual Scan Settings

Target Action Scan Exclusion

Files to Scan

- All scanable files
- File types scanned by IntelliScan
- Files with the following extensions (use commas to separate them):

Child policies: Inherit from parent Extend from parent

Scan Settings

- Scan hidden folders
- Scan network drive
- Scan compressed files

Maximum layers: 2

Inherit From Parent

With this method, an Apex Central administrative user creating a child policy cannot change the settings configured on the parent. For example, if the parent policy excludes PDF files from being scanned during a Manual Scan, the administrative user cannot modify this setting in a child policy.

Are Customizable

With this method, an Apex Central administrative user creating a child policy can modify the settings. For example, if a Scheduled Scan configured in the parent policy runs weekly and is customizable, an administrative user can modify the schedule in the child policy to run the scan daily.

Extend from parent

With this method, an Apex Central administrative user creating the child policy can add to the items in the parent policy. For example, if the parent policy excludes 20 file names from being scanned during a Manual Scan, the administrator can add 10 more file names that are deemed safe and trustworthy.

Data Discovery Policies

Apex Central integration with Data Loss Prevention allows administrators to manage and deploy Data Loss Prevention through Policy Management from the Apex Central Web Management console.

Data Discovery

In Apex Central and Apex One, Data Loss Prevention integration includes the ability to also protect data that is *at rest*. This allows Apex Central to scan file storage areas to identify where sensitive content is located. For example, it can be used to scan endpoints and identify documents containing credit card number information. Policies can dictate that if the endpoint is not authorized to store this type of data, the file must be encrypted.

Data Discovery tasks can be set up and scheduled to run on Security Agents. The schedule details is set as part of the policy setting. Additionally, sensitive files can be encrypted with a password or user/group key if Trend Micro File Encryption is installed. Also note that a Data Discovery task can resume if the scan service was stopped before the task completed and if the policy is unchanged, the Data Discovery task can perform an incremental scan.

Data Discovery Policy Management

Data Discovery policies search databases, endpoints and document management systems for the presence of sensitive information. Data Discovery widgets display data loss prevention compliance with an enterprise's policy. Using Data Discovery policies and widgets administrators can then perform remediation actions on their network.

Lesson 14: Deploying Policies Through Trend Micro Apex Central

- 1 In the Apex Central Web Management console, click **Policies > Policy Management**. Select **Apex One Data Loss Prevention** from the **Product** list.
Click **Create** or **Create one now** to create a new policy.

The screenshot shows the 'Policy Management' section of the Apex Central interface. The 'Product' dropdown is set to 'Apex One Data Loss Prevention'. A message at the bottom states 'You have not created a policy. [Create one now](#)'. Both the 'Product' dropdown and the 'Create one now' link are circled in red.

- 2 Click the **Internal Agents** or **External Agents** tabs as needed. Expand **Apex One DLP** and **Apex One Data Discovery** settings and enable them as needed.

The screenshot shows the 'Create Policy' page for a policy named 'Discovery_Policy'. Under 'Apex One Data Discovery', the 'Enable Data Discovery' checkbox is checked and highlighted with a red circle. A yellow warning message above the table says 'Trend Micro recommends deploying a Data Discovery policy to few endpoints, and then adjusting the policy, before deploying the policy to a large number of endpoints.' The 'Save' button is visible at the bottom.

- 3 Click **Add** in the **Apex One Data Discovery** section to create a new **Data Discovery** rule.
- 4 Click to enable the rule and specify a unique name for the rule. Complete the tabs in the **Data Discovery Policy Settings** window.

Target Folder

Data Discovery Policy Settings

Enable this rule
Rule name : Search_Documents

① Target Folder (highlighted with a red circle) **② Template** **③ Actions** **④ Schedule**

File Path: File location: C:\My Documents
Example: c:\test\

File Type Exceptions:

- Scan: Examples: *.doc|.txt
- Do not scan: Examples: *.doc|*.xls

Save Close

- File location:** Specify the folder to scan for files
- File Type Exceptions:** Specify any file type scanning exceptions

Note: Data Discovery supports the following wildcard characters:

*: Substitute all characters before or after the *
?: Substitute for a single character or a single double-byte character

You can separate multiple entries with pipes (|) using the following format:

For files: *.<file_extension> (for example: *.exe|*.doc)

For folders: Specify a file path (for example: *\Test*|C:\My-Docs\)

Template

Select any appropriate templates from the **Available Templates** list and then click **Add** to move them to the **Selected templates** list.

Data Discovery Policy Settings

Enable this rule
Rule name : Search_Documents

① Target Folder **② Template** (highlighted with a red circle) **③ Actions** **④ Schedule**

Available Templates

View: All templates Search

- All templates
 - Adult
 - Albania: IBAN (International Bank Account Number)
 - All File Extension
 - All Personally Identifiable Information (English)
 - All: Credit Card Number
 - All: IBAN (International Bank Account Number)
 - All: IIN (Issuer Identifier Number)
 - All: Names from US Census Bureau
 - All: SWIFT BIC (SWIFT Business Identifier Code)

Selected templates

All: Credit Card Number

Add > < Remove

Save Close

Actions

Specify one or more of the following: actions to perform when the policy is triggered

- **Monitor:** Detections are recorded for analysis
- **Encrypt:** Sensitive files are encrypted using one of the listed methods. **Integration with Trend Micro Endpoint Encryption is required to enable this capability.**

The screenshot shows the 'Data Discovery Policy Settings' window. At the top, there is a checkbox labeled 'Enable this rule' which is checked, and a text input field labeled 'Rule name : Search_Documents'. Below these are four tabs: ① Target Folder, ② Template, ③ Actions (which is highlighted with a red circle), and ④ Schedule. The 'Actions' tab displays a section titled 'Select Action' containing two options: 'Monitor' (checked) and 'Encrypt' (unchecked). Under 'Encrypt', there is a sub-section 'Encrypt with the following:' with three radio button options: 'User key' (selected), 'Group key', and 'Encryption password'. A link 'Create encryption password' is also present. At the bottom of the window are 'Save' and 'Close' buttons.

Schedule

Configure a schedule for the scan.

The screenshot shows the 'Data Discovery Policy Settings' window with the 'Schedule' tab selected (highlighted with a red circle). The 'Schedule Settings' section contains three radio button options: 'Every day' (unchecked), 'Every week on' (checked with 'Sunday' selected), and 'Every month on' (unchecked). Below this is a 'Start time' section with dropdown menus for hours (16) and minutes (35). At the bottom of the window are 'Save' and 'Close' buttons.

Click **Save** to preserve the selections in **Policy Settings**, then **Deploy** to push the policy to the identified endpoint computers.

- 5 The policy will display as **Pending** until it is deployed to the endpoints.

Priority	Policy	Owner	Last Editor	Targets ▾	Deployed	Pending	Offline	With Issues
Locked	Discovery_Policy	admin	admin	Specified	0	1	0	0

Total: 0 Pending: 1 Offline: 0 With Issues: 0

Once applied, the endpoint will display with a status of **Deployed**.

- 6 An alert on the endpoint will prompt the end user to restart the computer to complete the process.



Incident Investigation

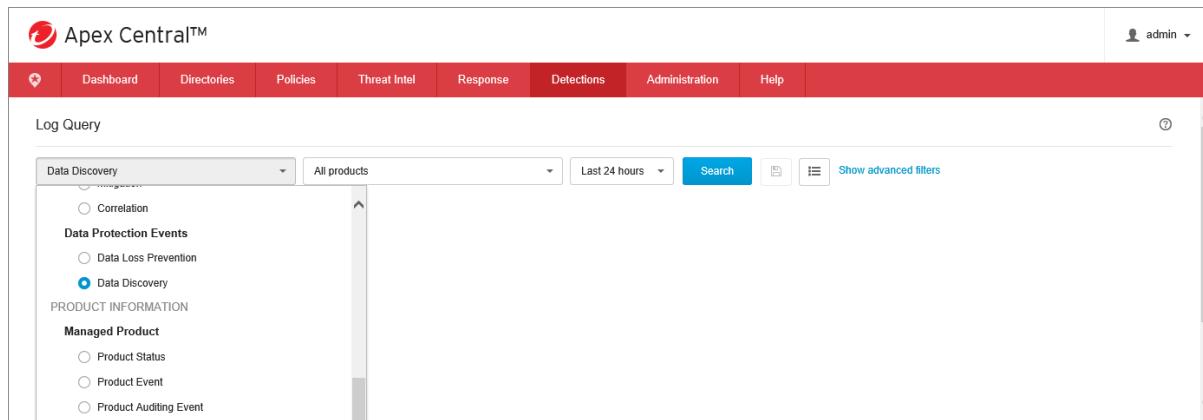
Data Leak Prevention incidents can be reviewed and updated by Data Leak Prevention compliance officers and incident reviewers.

To enable the incident review process, Apex Central administrators will need to complete some prerequisite tasks. These tasks are summarized below:

- Set up manager information in Active Directory
- Set up Active Directory integration to obtain user information
- Create user accounts specific for Data Leak Prevention incident investigation. Assign **DLP Compliance Officer** or **DLP Incident Reviewer** roles to users investigating Data Leak Prevention incidents (Remember that the DLP Compliance Officer and DLP Incident Reviewer roles are available to **Active Directory** users only.)
- Set up the **Scheduled incident summary** and **Incident details updated** notifications
- Export Data Leak Prevention logs for auditing purposes

Lesson 14: Deploying Policies Through Trend Micro Apex Central

After completing the above steps, DLP investigators will be able to view Data Leak Prevention and Data Discovery events from Apex Central by selecting **Detections > Logs > Log Query**.



The screenshot shows the Trend Micro Apex Central web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A user icon labeled "admin" is also in the top right corner. Below the navigation bar, the title "Log Query" is displayed. The main area is titled "Log Query" and contains several filter options: "Data Discovery" (selected), "All products", and "Last 24 hours". There are also "Search" and "Show advanced filters" buttons. On the left side, there are two sections: "Data Protection Events" (with Correlation, Data Loss Prevention, and Data Discovery options, where Data Discovery is selected) and "PRODUCT INFORMATION" (with Managed Product, Product Status, Product Event, and Product Auditing Event options). The interface has a clean, modern design with a white background and light gray borders for the different sections.

Lesson 15: Detecting Emerging Malware Through Connected Threat Defense

Lesson Objectives:

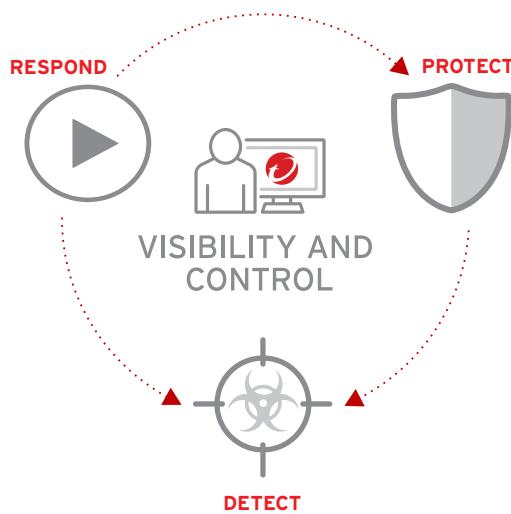
After completing this lesson, participants will be able to:

- Describe the components of the Connected Threat Defense system
- Integrate Deep Discovery Analyzer with Apex Central
- Track a suspicious object through the Connected Threat Defense cycle

In the modern data center, more and more security breaches are a result of targeted attacks using techniques such as phishing and spear-phishing. In these cases, malware writers can bypass traditional malware scanners by creating malware specifically targeted for your environment. Apex One adds enhanced malware protection for new and emerging threats through Connected Threat Defense.

Using heuristic detection, Apex One can identify document files that are deemed *suspicious* and submit them automatically to Deep Discovery Analyzer for analysis. If the analysis indicates that a particular file does contain malware, Deep Discovery will provide the information to Apex Central where an action for this particular malware can be specified. Apex One can use the Suspicious Object List from Apex Central to update its malware policies and remediate threats.

Connected Threat Defense allows multiple Trend Micro products to share threat information and analysis across multiple layers of protection critical to defending against advanced threats. Connected Threat Defense includes a complete set of security technology to detect, respond to and protect against for advanced threats.



Detect

Components of the Connected Threat Defense detect advanced malware, behavior and communications invisible to standard defenses. Connected Threat Defense analyzes the risk and nature of the attack and attacker within sandboxes to reveal malicious actions without relying on malware signatures.

Respond

Components of the Connected Threat Defense enable rapid response through shared threat intelligence and delivery of real-time security updates.

Protect

Components of the Connected Threat Defense assess potential vulnerabilities and proactively protect endpoints, servers and applications.

Visibility and control

Components of the Connected Threat Defense provide visibility across the system and analyze and assess the impact of threats.

Apex One's participation in Connected Threat Defense requires you to set up a connection between the Apex One Server, Deep Discovery Analyzer and Apex Central.

Connected Threat Defense Requirements

To participate in the Connected Threat Defense lifecycle, verify that your environment meets these requirements:

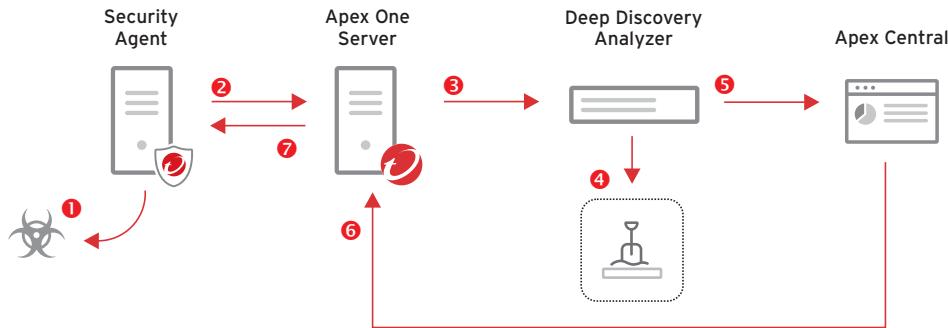
- Apex One Server is installed and configured with Security Agents protecting computers
- Deep Discovery Analyzer is installed and the sandbox virtual machines are provisioned

SaaS: The service implementation of Apex One uses a cloud-based sandbox for file analysis.

- Apex Central is installed
- Deep Discovery Analyzer and Apex One Server have been added to the Apex Central Managed Servers list and Product Directory

How Connected Threat Defense Works

When all the components are deployed and configured correctly Connected Threat Defense operates as described below.



- 1 Security Agents are configured with rules to enable detection of malware on the protected computers. Anti-Malware policies define how suspicious objects are to be handled.
- 2 Objects deemed to be suspicious are gathered and submitted to the Apex One Server. Suspicious objects can include:
 - Programs not known to Trend Micro downloaded through a web browser or email channels
 - Heuristic detections of processes downloaded through a web browser or email channels
 - Low prevalence autorun programs on removable storage
- 3 The Apex One Server submits the suspicious objects to Deep Discovery Analyzer for analysis. The objects are submitted to the Analyzer every 15 minutes by default.
- 4 Deep Discovery Analyzer executes and observes the suspicious file in a secure, isolated virtual sandbox environment.
- 5 Deep Discovery Analyzer pushes the analysis results to Apex Central, where an action can be specified for the file based on the analysis. The analysis report is pushed to Apex Central every 10 minutes by default. Once the action is specified, a list of emerging threats called a **Suspicious Object List** is created or updated. Other Trend Micro products, such as Deep Security, Deep Discovery Inspector or Deep Discovery Email Inspector, may also be connected to Apex Central and be able to update the list.
- 6 The Apex One Server receives the list of suspicious objects from Apex Central. This list is retrieved every 15 minutes by default.
- 7 The list is forwarded to Agents where protection against the suspicious object is applied.

Suspicious Activities

Deep Discovery Analyzer monitors the sandbox environment for activities deemed to be suspicious. The activities include the items listed below.

Anti-security, self-preservation	Autostart or other system reconfiguration	Deception, social engineering
<ul style="list-style-type: none"> Deleted AV registry entry Disabled AV service Locked registry Stopped or modified AV service Suspicious packer Used watchdog 	<ul style="list-style-type: none"> Added autorun in registry Added scheduled task Added startup file or folder Bypassed firewall Modified important registry items Modified Applnit_DLLs in registry Modified sensitive file Reset IP settings 	<ul style="list-style-type: none"> Created message box Deceiving extension name Double EXE header Double extension name with executable tail Dropped fake system file Fake icon File signature Porn-like file name
File drop, download, sharing, or replication	Hijack, redirection, or data theft	Suspicious network or messaging activity
<ul style="list-style-type: none"> Copied same file multiple times Copied self Deleted self Downloaded executable Dropped driver Dropped executable Dropped file into share Executed download Executed dropped file Opened share Renamed download Searched shares 	<ul style="list-style-type: none"> Accessed document files Installed BHO Modified configuration files Set up API hooks Stole IM password 	<ul style="list-style-type: none"> Created raw socket Established network connection Listened on port Opened IRC connection Performed DNS query Performed port scanning Requested suspicious URL Requested URL Sent email
Malformed, defective, or with known malware traits	Process, service, or memory object change	Rootkit, cloaking
<ul style="list-style-type: none"> Contains known malware string Crashed document reader Crashed process Failed to start 	<ul style="list-style-type: none"> Added service Created mutex Created named pipe Created process Injected memory with dropped files Memory resident Started self Started service Terminated process 	<ul style="list-style-type: none"> Attempted to hide file Hide file Hide registry Hide service

Deep Discovery Analyzer

Deep Discovery Analyzer provides custom sandbox analysis using virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Apex One can send these file types to Deep Discovery Analyzer:

- cell - Cell spreadsheet document
- chm - Compiled HTML file
- class - Java class file
- dll - Dynamic Link Library
- doc - Microsoft Word document
- docx - Microsoft Word 2007 and later document
- exe - Executable file
- gul - JungUm Global document
- hwp - Hancom Hangul Word Processor (HWP) document
- hwpx - Hancom Hangul Word Processor 2014 (HWPX) document
- jar - Java Applet Java application
- js - JavaScript file
- jse - JavaScript encoded script file
- jtd - JustSystems Ichitaro document

- **lnk** - Microsoft Windows Shell Binary Link shortcut
- **mov** - Apple QuickTime media
- **pdf** - Adobe Portable Document Format
- **ppt** - Microsoft PowerPoint presentation
- **pptx** - Microsoft PowerPoint 2007 and later presentation
- **ps1** - Microsoft Windows PowerShell script file
- **rtf** - Microsoft Rich Text Format document
- **swf** - Adobe Shockwave Flash file
- **vbe** - Visual Basic encoded script file
- **vbs** - Visual Basic script file
- **xls** - Microsoft Excel spreadsheet
- **xlsx** - Microsoft Excel 2007 and later spreadsheet
- **xml** - Microsoft Office 2003 and later XML file

Connecting Deep Discovery Analyzer to Apex Central

The Deep Discovery Analyzer must be added as a Managed Server in Apex Central.

- 1 In the Apex Central Web Management console, click **Administration > Managed Servers > Server Registration**.
- 2 Select **Deep Discovery Analyzer** from the **Server Type** list and click **Add a product**.

The screenshot shows the Control Manager interface with the following details:

- Header:** Control Manager, admin
- Navigation:** Dashboard, Directories, Policies, Logs, Notifications, Reports, Updates, Administration, Help
- Section:** Server Registration
- Server Type:** Deep Discovery Analyzer (highlighted by a red circle)
- Buttons:** Add, Refresh, Proxy Settings, Cloud Service Settings, Directory Management
- Table:** Shows a single row for 'Server' with columns: Display Name, Product, Connection Type, Last Report. An 'Add a product' button is located at the bottom of this table (highlighted by a red circle).
- Footer:** Records: 0 - 0 / 0 | Page 0

- 3 Type the details of the Deep Discovery Analyzer device and click **Save**.

Add Server

Server Information

Server: https://192.168.4.5
For example: http(s)://<server_name>:port_number

Display name: Analyzer

Product: Deep Discovery Analyzer

Authentication

User name: admin

Password: [REDACTED]

Connection

Use a proxy server for the connection

Save Cancel

- 4 Deep Discovery Analyzer is now listed as a **Managed Server**.

server	Display Name	Product	Connection Type	Last Report	Actions
https://192.168.4.5	Analyzer	Deep Discovery Analyzer 6.00	Manual	08/13/2018 16:50	

Adding Deep Discover Analyzer to the Apex Central Product Directories

In the Apex Central Web Management console, add the Deep Discover Analyzer to the Product Directories list.

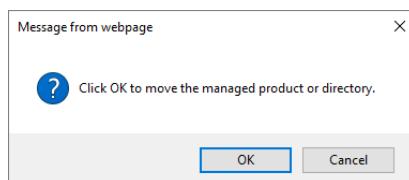
- 1 In the Apex Central Web Management console, click Directories > Products and click Directory Management.

The screenshot shows the Apex Central™ web interface. At the top, there's a red navigation bar with tabs: Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. On the far right of the bar is a user icon labeled "admin". Below the bar, the title "Product Directory" is displayed. Underneath is a search bar with a "Search" button. A horizontal menu bar contains "Advanced Search", "Configure", "Tasks", and "Directory Management". The "Directory Management" button is highlighted with a red oval. The main content area shows a tree view on the left under "DBSRV" with "Local Folder" and "Search Result" nodes, and a large empty panel on the right labeled "DBSRV". At the bottom right of the main area are "Status" and "Folder" buttons.

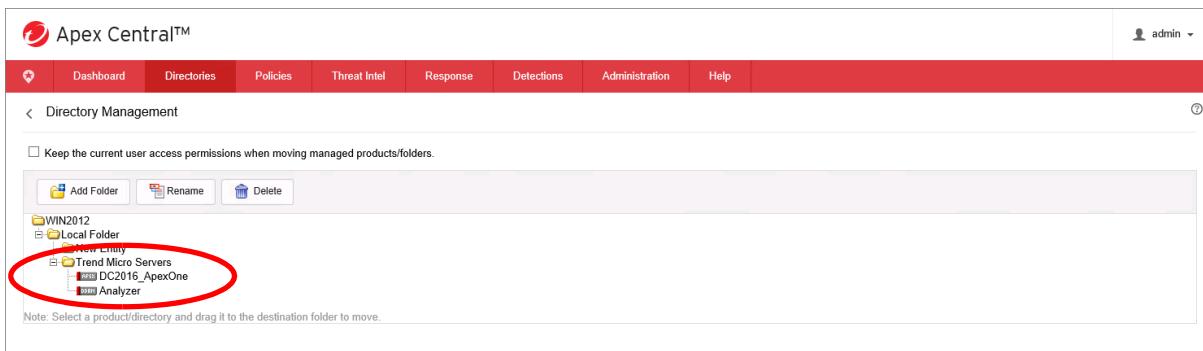
- 2 Expand the **New Entity** folder. Drag the **Analyzer** device from **New Entity** folder to the previously created **Trend Micro Servers** folder.

This screenshot shows the "Directory Management" page. The top navigation bar is identical to the previous screenshot. Below it, the title "Directory Management" is followed by a link "[Keep the current user access permissions when moving managed products/folders.](#)". The main content area features a tree view of product/directory structures. Under "WIN2012", there is a "Local Folder" node. Under "Local Folder", there is a "New Entity" node, which contains an "Analyzer" device node. There is also a "Trend Micro Servers" node. At the bottom of the content area, a note says "Note: Select a product/directory and drag it to the destination folder to move." A tooltip "Select a product/directory and drag it to the destination folder to move." is shown over the "Analyzer" node.

When prompted, click **OK** to acknowledge the move.



The Deep Discovery Analyzer should be displayed in the **Trend Micro Servers** folder.



The screenshot shows the Apex Central™ interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. On the far right, it shows a user icon and "admin". Below the navigation bar, the title "Directory Management" is displayed. There's a checkbox labeled "Keep the current user access permissions when moving managed products/folders.". Underneath, there are buttons for "Add Folder", "Rename", and "Delete". The main content area shows a tree view of folders: "WIN2012" has a "Local Folder" which contains "New Linux" and "Trend Micro Servers". "Trend Micro Servers" contains "DC2016_ApexOne" and "Analyzer". A red circle highlights the "Trend Micro Servers" folder. At the bottom of the interface, there's a note: "Note: Select a product/directory and drag it to the destination folder to move."

Suspicious Objects

When Deep Discovery Analyzer discovers suspicious objects through the sandbox analysis of a file, it can send information about the object (SHA-1, URL, IP, Domain) to Apex Central for local sharing. Apex Central can also send the **Suspicious Object List**, along with executable files, to the Trend Micro Smart Protection Network.

Trend Micro will validate the suspicious objects within a maximum of 6 hours. If suspicious objects are found to be malicious they will be added to Smart Protection Network and all products which integrate with the network can leverage this information.

Other Indicators of Compromise may also be manually configured and sent to Apex Central.

Trend Micro products, including Apex One and Deep Security, sync with Apex Central to obtain updated Suspicious Object Lists.

The process for handling suspicious object can be broken down into the following phases:

Submitting Samples

Apex One and other Trend Micro products use administrator-configured file submission rules to determine the samples to submit to Virtual Analyzer.

Analyzing Samples

Deep Discovery Analyzer tracks and analyzes the submitted samples. Analyzer flags suspicious objects based on their potential to expose systems to danger or loss. Supported objects include files (SHA-1 hash values), IP addresses, domains, and URLs.

Distributing Suspicious Object Details

Apex Central consolidates suspicious objects and scan actions against the objects and then distributes them to other products.

- **Exceptions to Virtual Analyzer Suspicious Objects:** Apex Central administrators can select objects from the list of suspicious objects that are considered safe and then add them to an exception list. Apex Central sends the exception list back to the products integrated with Virtual Analyzer. If a suspicious object from a managed product matches an object in the exception list, the product no longer sends it to Apex Central.
- **User-Defined Suspicious Objects:** Apex Central administrators can add objects they consider suspicious but are not currently in the list of Virtual Analyzer suspicious objects.
- **Suspicious Object Distribution:** Apex Central consolidates Virtual Analyzer and user-defined suspicious objects (excluding exceptions) and sends them to other managed products. These products synchronize and use all or some of these objects.

Configure scan actions (log, block, or quarantine) against suspicious objects that affect computers. Block and quarantine actions are considered *active* actions, while the log action is considered *passive*. If products take an active action, Apex Central declares the affected computers as mitigated. If the action is passive, computers are declared at risk.

Scan actions are configured separately for Virtual Analyzer and user-defined suspicious objects. Apex Central automatically deploys the actions to certain managed products.

Mitigating Threats

Security Agents perform active scan actions against suspicious objects.

When the scan action configured in Apex Central and deployed to Security Agents is **Block** or **Quarantine**, the affected computers are considered mitigated.

Apex Central also checks Web Reputation, URL filtering, network content inspection, and rule-based detection logs received from all managed products and then compares them with its list of suspicious objects. If there is a match from a specific computer and the managed product takes an active action such as **Block**, **Delete**, **Quarantine**, or **Override**, Apex Central treats the computer as mitigated.

Subscribing Apex One to the Suspicious Objects List

Apex One subscribes to the Suspicious Object List to retrieve the list on a regular basis.

- 1 In the Apex One Web Management console and click **Administration > Settings > Suspicious Object List**.

The screenshot shows the 'Suspicious Object List Settings' page in the Apex One Web Management console. At the top, there's a navigation bar with links for Dashboard, Assessment, Agents, Logs, Updates, Administration, Plug-ins, and Help. The current page is 'Suspicious Object List Settings'. The main content area is divided into sections: 'Suspicious Object List Subscription', 'Suspicious Object List', and 'Agent Settings'. In the 'Agent Settings' section, several checkboxes are checked under 'Enable Suspicious URL list', 'Enable Suspicious IP list', 'Enable Suspicious File list', and 'Enable Suspicious Domain list'. Below these settings, there's a note about updating the list on security agents, with two radio button options: 'Based on the Security Agent component update schedule' (unchecked) and 'Automatically after updating the Suspicious Object lists on the server' (checked). A note at the bottom states that Apex One uses Smart Protection Servers to deploy Suspicious URL lists to Security Agents. At the bottom of the page are 'Save' and 'Cancel' buttons.

In the **Agent Settings** section, verify that URL, IP and File and Domain are all enabled.

- 2 Click **Test Connection**. A success message should be displayed in the console window.

A green message box displays the text: 'Successfully connected to the Suspicious Object List source.'

- 3 Click **Save**.
- 4 In the Agent Management list, right mouse-click a domain or an Agent and click **Settings > Sample Submission**. Click to **Enable suspicious file submission to Virtual Analyzer** and click **Save**.

The 'Sample Submission' dialog box has a 'Sample Submission Settings' section containing a checkbox for 'Enable suspicious file submission to Virtual Analyzer'. A note below it specifies that suspicious files include programs known to Trend Micro, heuristic detections of processes, and low prevalence autorun programs on removable storage. At the bottom are 'Save' and 'Cancel' buttons.

- 5 A message is displayed confirming the configuration settings have been applied.

A message box displays the text: 'Configuration changes have been applied. OfficeScan agents are now being notified. Please allow some time for new configuration setting to propagate to all agents. Unavailable agents will be notified when they are reconnected to the network.' At the bottom is a 'Close' button.

Tracking Suspicious Objects

Submissions from the Security Agents are sent to the Apex One Server before being forwarded to the Deep Discovery Analyzer. The submitted items can be viewed on the Apex One Server before they are sent to the Deep Discovery Analyzer in the following folder:

C:\Program Files (x86)\Trend Micro\Apex One\TEMP\Sample Submission

In the Deep Discovery Analyzer Web Management console, click **Virtual Analyzer > Submissions**. On the **Processing** tab, any submitted files currently being processed by the Analyzer will be listed under today's date. There will be some delay before the file is submitted to the Deep Discovery Analyzer by the Apex One Server.

The screenshot shows the Trend Micro Deep Discovery Analyzer interface. At the top, there's a navigation bar with links for Dashboard, Virtual Analyzer, Alerts / Reports, Administration, and Help. Below that, a sub-navigation bar shows 'You are here: Virtual Analyzer > Submissions'. The main area is titled 'Submissions' and has tabs for 'Completed (0)', 'Processing (1)', 'Queued (0)', and 'Unsuccessful (0)'. A search bar at the top right allows searching by 'file name or URL'. Below the tabs is a table with columns: Event Logged, Elapsed Time, Source / Sender, Destination / Reci..., Protocol, File Name, URL, Submitter, Submitter Name, and SHA-1. The table contains one row of data: '2020-12-11 16:03:38', '0 00:02:16', 'client-03/192.168.4.6', '-', 'fd651677-6d71-4a3...', 'Office Scan', 'dc2016', '1F086CBE6DC135...', and 'SHA-1'. A 'Submit objects' button is located at the top right of the table area.

SaaS: There is no console for viewing or tracking suspicious objects in the service implementation of Apex One using the cloud-based sandbox for file analysis.

Once the submission has been processed, the entry will be displayed on the **Completed** tab. There will be some delay while the file is processed.

This screenshot shows the same Trend Micro Deep Discovery Analyzer interface as the previous one, but with the 'Completed' tab selected in the top navigation bar. The table below now shows one item: '2020-12-11 16:03:38', '2020-12-11 16:03:38', 'client-03/192.168.4.6', 'fd651677-6d71-4a3...', 'MS OLE doc...', 'Office Scan', 'dc2016', 'EXPL_CVE2...', and '1F086CBE6DC135A...'. The rest of the interface is identical to the previous screenshot.

Once the processing is complete, click **Virtual Analyzer > Suspicious Objects**. The object is now visible in the list.

Last Detected	Expiration	Risk Level	Type	Object	Latest Related Sample	Related Submissions
2020-12-11 16:08:59	2021-01-10 16:08:56	High	File	1F086CBE6DC1353A0A1C6D5C5836ACCD19FD4B0D	1F086CBE6DC1353A0A1C6D5C5836ACCD19FD4B0D	1

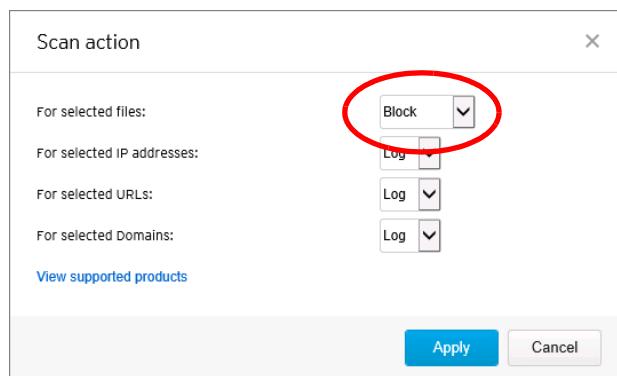
The details of the suspicious object are submitted to Apex Central for addition to the Suspicious Objects List. In the Apex Central Web Management console click **Administration > Threat Intel > Virtual Analyzer Suspicious Objects** to view the details in the list. You may need to wait several minutes for the results of the analysis to be passed to Apex Central.

Object	Risk Level	Type	Expiration Date	Affected Endpoints/Recipients	Scan Action	Handling Process
1F086CBE6DC1353A0A1C6D5C5836ACCD19FD4B0D	High	File	01/10/2021 16:08:56	Not yet assessed / 0	Log	View
1 - 1 / 1	< >	1 / 1	20 per page			

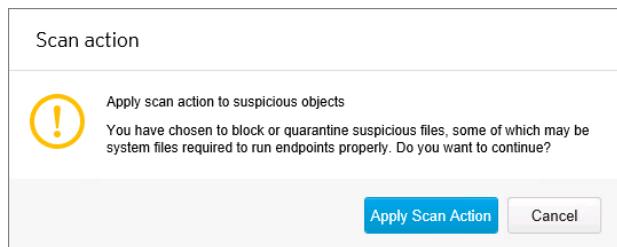
The action to be performed the next time the suspicious object is encountered can be configured. Click to select the object in the list and click **Configure Scan Action**.

Screenshot of the Trend Micro Apex Central™ interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The user is logged in as Admin. The main content area is titled "Virtual Analyzer Suspicious Objects" and displays a table of suspicious objects. The table has columns for Object, Risk Level, Expiration Date, Affected Endpoints/Recipients, Scan Action, and Handling Process. A message at the top of the table area states: "Impact analysis requires additional licensing. Ensure that you have a valid Endpoint Sensor license or contact your service provider to obtain an Activation Code." The "Configure Scan Action" button in the toolbar is circled in red. The selected object row, which includes a file named "1F086CBE6DC1353A0A1C6D5C5836ACCD19FD...", is also circled in red.

In the **Scan Action** window, select an action, for example, **Block** in the **For selected files** section and click **Apply**.



When prompted, confirm the application of the scan action. Click **Apply Scan Action**.



The Scan Action is changed to **Block**.

Object	Risk Level	Type	Expiration Date	Affected Endpoints/Recipients	Scan Action	Handling Process
1F086CBE6DC1353A0A1C6D5C5836ACCD19FD...	High	File	01/10/2021 16:08:56	Not yet assessed / 0	Block	View

Apex One will retrieve the Suspicious Object list from Apex Central on a regular basis. An administrator can also trigger the retrieval of the list manually. In the Apex One Web Management console, click **Administration > Settings > Suspicious Object List**.

Under **Suspicious Object List Subscription** section, click **Syn Now**.

Suspicious Object List Subscription
Apex One is subscribed to the Suspicious Object lists on the registered Apex Central server.
Server address: https://192.168.4.3:443/WebApp
Last sync: 12/11/2020 16:25:46 (Try every 10 minutes)
Sync Now Test Connection Unsubscribe

Suspicious Object List
Last modified: 12/11/2020 16:25:49

Agent Settings
<input checked="" type="checkbox"/> Enable Suspicious URL list ?
<input checked="" type="checkbox"/> Enable Suspicious IP list ?
<input checked="" type="checkbox"/> Enable Suspicious File list

The Security Agent will obtain the Suspicious Objects List from the Apex One Server on its next update.

When the Security Agent encounters the suspicious object in the future, a suspicious file violation will be displayed.

Lesson 16: Blocking Unapproved Applications on Endpoint Computers

Lesson Objectives:

After completing this lesson, participants will be able to:

- Define Application Control criteria to specify allow or block actions
- Create Application Control policies

Apex One's defense against malware and targeted attacks can be enhanced by preventing unwanted or unapproved applications from executing on Windows endpoint computers. Administrators configure policies and rules to define applications and then specify an operation of **Allow** or **Block** to be performed on the defined applications when encountered on the endpoint computer.

Integrated Application Control

Application Control functionality integrated into Apex One can monitor applications on an endpoint and prevent unknown application from running. A separate Agent and Server are no longer needed to provide Application Control capabilities.

If the separate Agent is in use for an existing OfficeScan XG installation, it will be automatically uninstalled when Application Control policies are deployed and a new Apex One service will be launched to integrate Application Control.

Policies using Apex One Application Control must be deployed through Apex Central.

Note: Application Control in Apex One is available for Windows endpoint computers only.

Application Control Blocking Methods

Application Control in Apex One can block applications using two different methods.

Lockdown Mode With Allow Criteria

Enabling Lockdown Mode on the endpoint triggers an inventory of all the applications currently installed on the endpoint and any application that is **not** part of that inventory will be blocked from executing on the endpoint. Any applications that should be allowed to execute, even though they are not part of the inventory, can be identified through an **Allow** criteria. These applications can be defined by their hash, by their path or by attributes of their digital certificate.

Block Criteria

Any applications not allowed to execute on the endpoint can be defined through a **Block** criteria. In this method, only the identified application are prevented from executing. No inventory of the endpoint is required. Blocked applications can be defined by their hash, by their path or by attributes of their digital certificate.

Lockdown Mode

When in Lockdown Mode, Security Agents block all applications not identified during an inventory scan. After endpoints receive this command, Application Control scans the endpoint and creates a complete application inventory. A hash value is calculated for every application on the computer, and the values are stored in the `invt.db` file on the endpoint computer. Application Control then locks down the endpoint and does not permit access to:

- Any application that does not specifically match an Allow criteria defined in the User-defined Rule table
- Any application that does not specifically match assessment criteria defined in the User-defined Rule table
- Any application not found in the inventory scan results for that particular endpoint

As an option, applications from Trend Micro trusted vendors can be excluded from lockdown. This option automatically allows all applications that Trend Micro threat experts have determined to come from trusted vendors.

The screenshot shows the Trend Micro Apex Central interface with a red header bar. In the top right corner, there is a user icon labeled 'Admin'. Below the header, a navigation bar has tabs for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The 'Policies' tab is selected. A sub-menu titled 'Create Policy' is open. The main area is titled 'Policy Name: Lockdown'. Under 'Targets', there are options for 'None (Draft only)', 'Filter by Criteria', and '1 target(s)'. A note says 'Manually assign targets to the policy. Specified policies take priority over filtered policies.' Below this, under 'Apex One Security Agent Settings', there is a section for 'Application Control Settings' with a checked checkbox for 'Enable Application Control'. Under 'User-Defined Rules', there is a table with one row: Priority (1), User Accounts (All user accounts), and Applied Criteria (empty). In the 'Additional Actions' section, a red oval highlights the 'Lockdown' option, which is selected (radio button is blue) and includes the sub-option 'Exclude applications by Trend Micro trusted vendors' (checkbox is checked). Other options like 'Allow' and 'Assessment mode' are also listed but not selected.

Application Control Criteria

Application Control provides the ability to define criteria that specifically allows or blocks certain applications to execute.

You can define **Allow** criteria to ensure that Application Control never blocks a certain application, or you can create a complete list of applications allowed to execute on endpoints when you deploy a Lockdown policy to the endpoints. While in Lockdown mode, users cannot execute, access, or install any application that you did not include in the Allow criteria.

You can define **Block** criteria to ensure that Application Control always blocks certain applications or you can create Assessment criteria to monitor the applications that users access. Application Control logs all applications that match the assessment criteria but takes no further action and allows the applications to execute normally.

Application Control Criteria defines applications through the following attributes:

- File Hash
- File Path
- Certificate

Note: The criteria of Gray Software List and Certified Safe Software List (also referred to as Application Reputation) are no longer used in Apex One, even though the menu items may display in the interface.

File Hash

Every file, including an application, has a unique hash value. For example, `notepad.exe` has the following hash values:

- **SHA-1 value:** 867B54F1BC5B71045A9A00BACA485A24176B202C
- **SHA-256 value:**
899346F9F283A4FD5AA03015A3F58CDE5B9C0B6A5C4D64C2CC74E9B22C1348D7

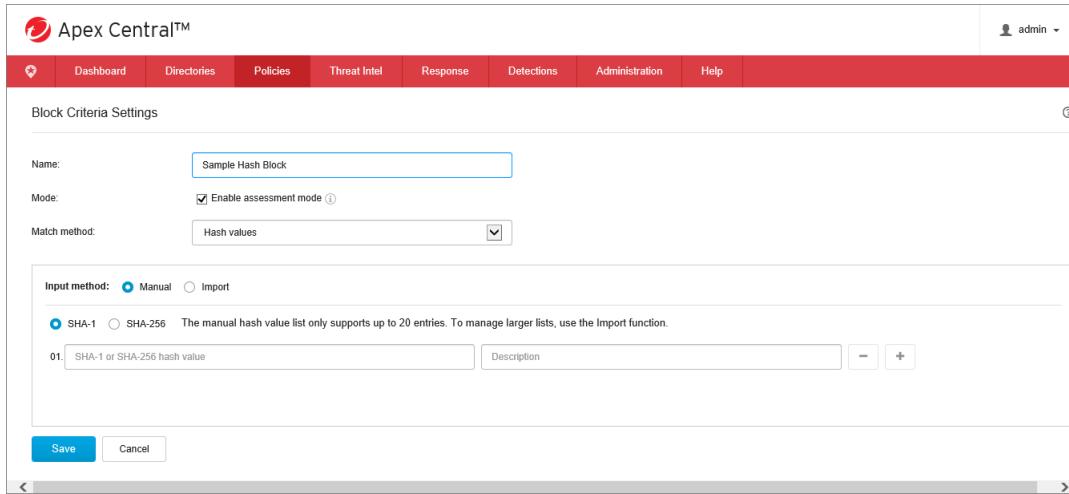
Application Control can use these hash values (either the SHA-1 or SHA-256 result) as the basis for identifying an application on which to perform the Allow or Block operation.

In creating a Hash rule, there are two input methods:

- Manual
- Import

Manual Input

Manual input allows administrators to enter the SHA-1 or SHA-256 values for identified applications. The list cannot contain a mixture of SHA-1 and SHA-256 formats, and administrators can manually specify up to 20 hash values with their description.



The screenshot shows the 'Block Criteria Settings' page in the Apex Central web interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A user icon labeled 'admin' is in the top right corner. The main form is titled 'Block Criteria Settings' and contains the following fields:

- Name: Sample Hash Block
- Mode: Enable assessment mode
- Match method: Hash values
- Input method: Manual (selected), Import
- SHA-1 (radio button selected)
- SHA-256 (radio button unselected)

A note below the radio buttons states: "The manual hash value list only supports up to 20 entries. To manage larger lists, use the Import function." Below this note is a table with one row, containing a hash value '01. SHA-1 or SHA-256 hash value' and a 'Description' field. There are also minus (-) and plus (+) buttons for managing the list. At the bottom of the form are 'Save' and 'Cancel' buttons.

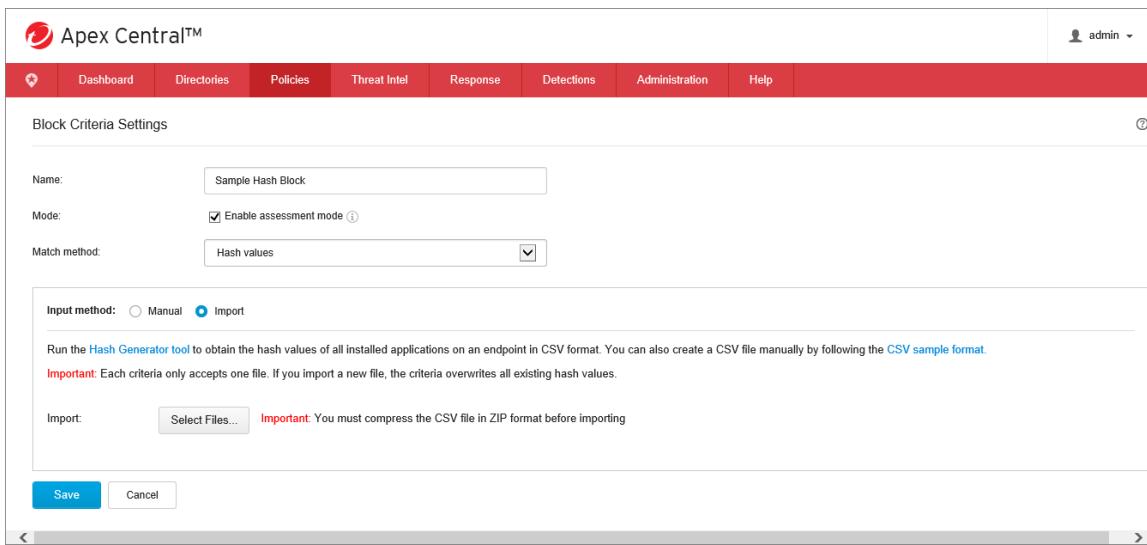
Import

This method uses the results from the **Hash Generation Tool** to identify the applications on the endpoint. The Hash Generator Tool scans and creates a SHA-256 hash value list of all portable executable (application) files found on an endpoint. You can then import the hash value list into

Application Control rules to specifically allow the execution of all identified applications. The hash value file can also be created manually, following the appropriate format. A sample CSV file can be downloaded directly from the Hash Values Criteria settings window.

Typically, the Hash Generator Tool is run on the golden image of the endpoint computer to build a common baseline for creating an allow criteria with the known good application inventory.

This method only supports SHA-256 hashes and the file import has a maximum size of 4MB. Each criteria only accepts one file; if a new file is imported, all existing hashes are overwritten.



The Hash Generation tool (`TMiAHashGen.exe`) can be downloaded directly from the **Hash Values Criteria** settings window, or directly from the following URL:

<https://success.trendmicro.com/solution/1120385>

```
C:\Users\Administrator\Downloads\TMiAHashGen\TMiAHashGen.exe
Input parameters:
Start dir:
Output path:C:\Users\Administrator\Downloads\TMiAHashGen\1548868837.csv
Mode:VSAPI_TRUE_FILE_TYPE(3)
Multi-Thread:1
Threads:3
Start scanning ...
```

Alternately, the hash file can be created manually in a CSV file with the appropriate formatting. A CSV sample file can also be downloaded from the **Hash Values Criteria** settings window.

File Paths

You can configure Application Control to specifically target certain directory locations based on absolute path, storage type, and Perl Compatible Regular Expressions (PCRE).

File paths can include any of the following

- **Specific path:** Only applies to applications in the exact path specified
- **Any built-in storage:** Only applies to applications in the path specified and stored on an internal storage device (internal hard disk drive)
- **Any local storage:** Only applies to applications in the path specified and stored on a non-removable local storage device (internal or external hard disk drive)
- **Any removable storage:** Only applies to applications in the path specified and stored on a removable storage device (USB drive, CD/DVD)
- **Network path:** Only applies to applications in the path specified and stored on a shared network resource
- **Program file folders:** Only applies to applications in the path specified and stored in the Program Files folders (default folders C:\Program Files and C:\Program Files (x86))
- **System volume:** Only applies to applications in the path specified and stored in the default Windows system drive

File paths can includes regular expressions and wildcards.

The screenshot shows the 'Block Criteria Settings' page in the Apex Central™ application. The 'Match method' dropdown is set to 'File paths'. A list of storage types is shown, with 'Specific path' selected. The 'String' field is empty, and the 'File path (wildcards supported)' field is also empty. Buttons for 'Save' and 'Cancel' are at the bottom.

Digital Certificates

Applications typically include a digital signature for file integrity purposes. The digital signature includes the digital certificate of the issuer and contains details such as the issuer name and validity details.

You can configure Application Control to specifically target applications based on the trust level of a certificate and contain specific certificate attributes. Select the type of certificate trust level and then specify the required certificate Issuer or Subject information. These Certificate properties can be retrieved from the Certificate Details.

The trust level combinations for Allow and Block criteria using Certificates differ.

Allow Criteria

- **Trusted (valid):** You have included the certificate in the trusted certificates list and the certificate must not have expired
- **Trusted (expired):** You have added the certificate in the trusted certificates list but the certificate has already expired
- **Untrusted:** The certificate is unknown or you did not add the certificate to the trusted certificates list

The screenshot shows the Trend Micro Apex Central™ web interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help, along with a user dropdown. The main content area is titled "Allow Criteria Settings". It features fields for "Name" (empty), "Trust permission" (set to "Application cannot execute external processes"), and "Match method" (set to "Certificates"). Below these, there's a section for "Specify certificate type:" with three radio button options: "Trusted (valid)" (unchecked), "Trusted (valid or expired)" (checked), and "Trusted (valid or expired) / Untrusted" (unchecked). A "Certificate properties:" section contains a dropdown menu set to "Issuer Country (C)". At the bottom are "Save" and "Cancel" buttons.

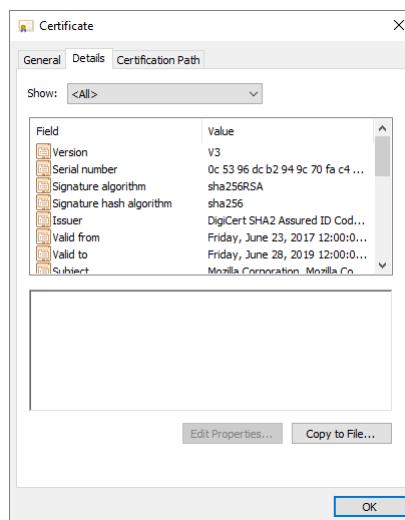
Block Criteria

- **Untrusted:** The certificate is unknown or you did not add the certificate to the trusted certificates list
- **Untrusted/Trusted (expired):** The certificate is unknown or you have added the certificate in the trusted certificates list but the certificate has already expired
- **Untrusted/Trusted (valid or expired):** The certificate is unknown or you must have added the certificate in the trusted certificates list but the certificate has already expired or is still valid

Lesson 16: Blocking Unapproved Applications on Endpoint Computers

The screenshot shows the Trend Micro Apex Central™ web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A user icon labeled "Admin" is also present. Below the navigation bar, the title "Block Criteria Settings" is displayed. The configuration form includes fields for "Name" (with a text input box), "Mode" (with an "Enable assessment mode" checkbox), and "Match method" (set to "Certificates"). Under "Specify certificate type:", the "Untrusted" option is selected. In the "Certificate properties:" section, there's a dropdown menu for "Issuer Country (C)" and logic operators ("AND" or "OR"). At the bottom of the form are "Save" and "Cancel" buttons.

The certificate properties required can be retrieved from the Windows **Certificate Details** window.



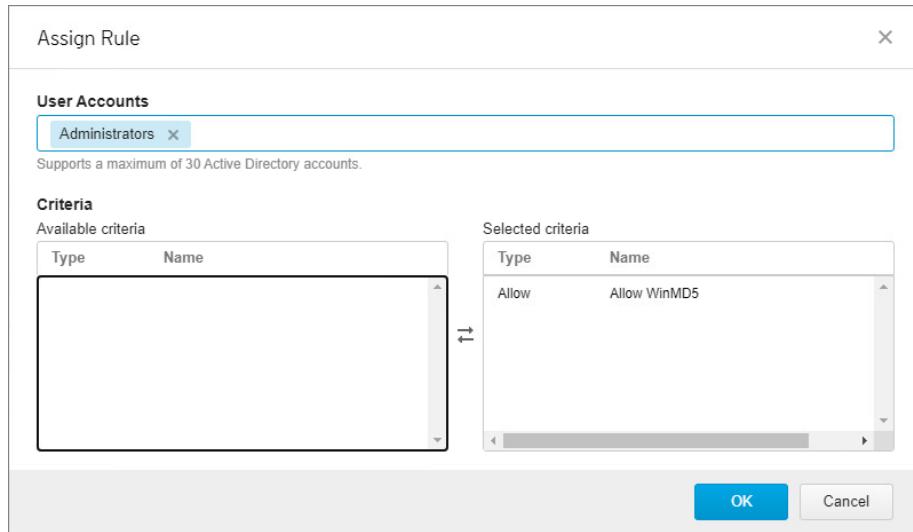
User-defined Rules

User-defined rules define which Application Control criteria will apply to specific users. Once the Allow or Block criteria have been defined, assign the criteria to the user account rule called **All user accounts**. This is the default rule that applies to any user not assigned to a any other rule.

The screenshot shows the Trend Micro Apex Central interface with a red header bar. The main menu includes Dashboard, Directories, Policies (which is selected), Threat Intel, Response, Detections, Administration, and Help. A user icon labeled 'Admin' is in the top right. Below the menu, a breadcrumb navigation shows '< Create Policy'. The policy name is set to 'Lockdown'. Under 'Targets', there are options for 'None (Draft only)', 'Filter by Criteria', and '1 target(s)'. A note says 'Manually assign targets to the policy. Specified policies take priority over filtered policies.' The 'Apex One Security Agent Settings' section has 'Additional Service Settings' expanded and 'Application Control Settings' collapsed, with 'Enable Application Control' checked. The 'User-Defined Rules' section contains a table with columns 'Priority', 'User/Group', and 'Applied Criteria'. A row for 'All user accounts' is selected and circled in red. In the 'Additional Actions' section, 'Lockdown' is selected as the action. The 'Agent Notifications' section is at the bottom.

If you have integrated Apex One with Active Directory, additional user account rules can be created to assign specific criteria to Active Directory users or groups. If you do not have Active Directory integration, you can only assign rules to the default **All user accounts** rule.

Click **Assign Rule** and type the name of the Active Directory users or groups. You can only assign 30 users or groups per rule. Create additional rules if you need to assign a greater number of users to a policy.



User Accounts: Specify the Active Directory user accounts or groups to which you want to assign the specific Application Control criteria,

Criteria: Move the necessary criteria from the Available list to the Selected list.

Best Practices for Enabling Application Control

The following are some recommended best practices when configuring Application Control in Apex One.

Use Learn → Monitor → Refine

- 1 Enable assessment mode in your policy when first using Application Control with Lockdown. Violations are logged, but the application will not yet blocked.
- 2 Monitor the Application Monitoring violations manually, using the Top Blocked Applications widget or by running a Log Query.
- 3 Refine the criteria and approve recognized software by creating **Allow** criteria to exempt from screening.

Use Lockdown

Lockdown is suitable for organizations which do not have frequent software changes or those who want to limit user access to certain application only. Recommended practices include:

- Create an **Allow** rule for Windows Update when enabling this setting
- Create a Golden Image of the endpoint after all applications have been installed or updated before enabling this setting.
- Deploy this setting gradually on a few endpoints before fully implementing the lockdown to a larger group.
- Enabling **Exclude applications by Trend Micro trusted vendors** is highly recommended in lockdown scenarios.

In-house Applications

In-house applications should be added to **Allow** rules using Hash Values as the Application Control criteria.

Top Blocked Applications Widget

To fine-tune Application Control policy enable the Top Blocked Applications Dashboard Widget. This widget will help Administrators to identify applications that are commonly blocked in their network.

Trust Permissions

Consider the following before changing the **Allow** trust permissions to **Applications can execute other processes** or **Inheritable execution rights (not recommended)**.

- Apply these permissions only to specific application that requires them to avoid granting extended rights to other applications that do not need it.
- Never use these permissions on web client applications like Internet Explorer, Chrome or Firefox to avoid exposing the endpoint to Drive-by Download exploits.
- These permissions are not recommended for File Path **Allow** rules as the specified folder location may be granting extended execute rights to unintended applications.

Application Control Criteria Pros and Cons

Criteria	Pro	Con	Best Practice
File Hash	- Direct criteria to allow or block the specific file	- Software might have different versions and/or different platforms - Regular maintenance required	Allow or block the specific application directly
File Path	- Direct criteria to allow or block the files under certain path	- Any files under that path will follow the criteria - If a software places files into multiple folders, it needs some configuration	Apply it with other big-scope allow/block criteria
Certificate	- Easily allow or block all the files of the companies by using digital signature	- All of the products by that company will apply the criteria. No middle ground. - Not all of the software has digital signature	Apply to the trustworthy or bad reputation companies

Lesson 17: Protecting Endpoint Computers From Vulnerabilities

Lesson Objectives:

After completing this lesson, participants will be able to:

- Create policies implementing Vulnerability Protection on Windows endpoint computers

Intrusion Prevention (IPS) functionality in Apex One protects Windows endpoint computers from being exploited through operating system vulnerability attacks. It automates the application of virtual patches to the endpoint computers which remain in place until an official patch to an operating system vulnerability to become available.

Note: Vulnerability Protection in Apex One is available for Windows endpoint computers only.

Integrated Vulnerability Protection

Intrusion Prevention (IPS) functionality is integrated into Apex One through Vulnerability Protection. A separate Vulnerability Protection Agent and Server are no longer needed to provide Vulnerability Protection capabilities.

If the separate Agent is in use for an existing OfficeScan XG installation, it will be automatically uninstalled when Vulnerability Protection policies are deployed and a new Apex One service will be launched to integrate Vulnerability Protection.

Policies using Apex One Vulnerability Protection must be deployed through Apex Central.

To streamline assignment of intrusion prevention rules, Vulnerability Protection in Apex One applies one of two profiles:

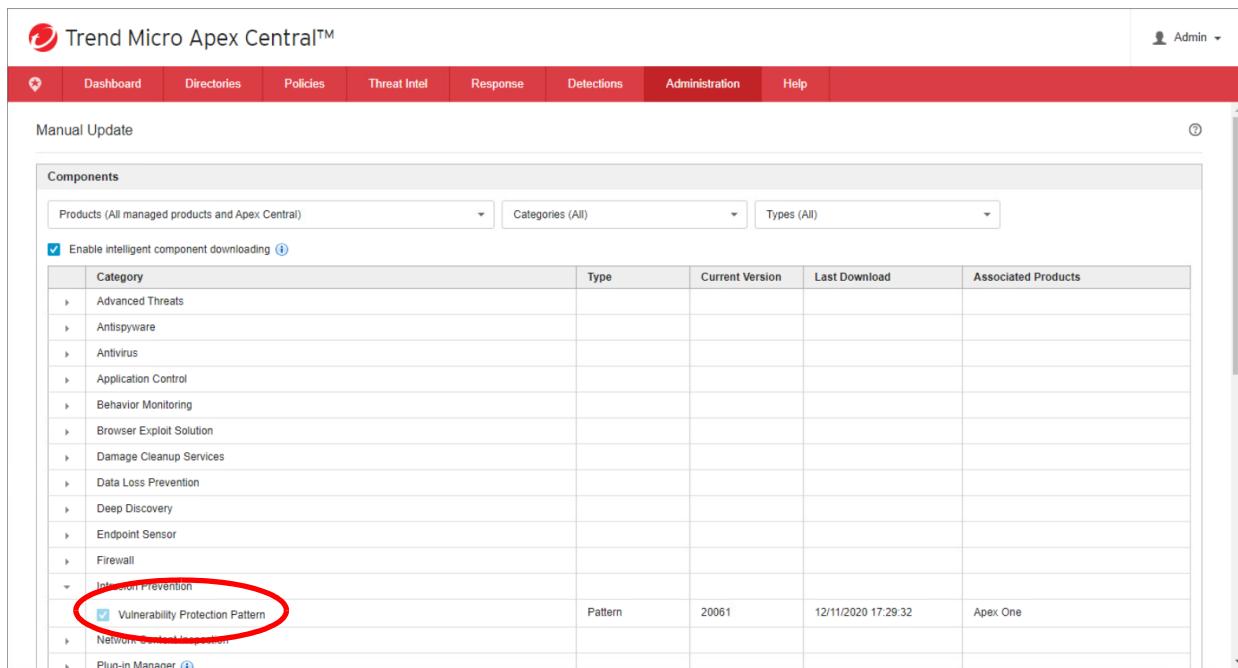
- **Recommended:** The **Recommended** profile applies a subset of intrusion prevention rules to conserve network resources. These are the rules recommended to be applied to reduce performance impact on the endpoint computer.
- **Aggressive:** The **Aggressive** profile uses the full set of intrusion prevention rules but requires additional network resources. Aggressive scanning may generate a large number of unnecessary logs and may affect endpoint performance.

Note: **Recommendation Scans** are no longer used with Vulnerability Protection. Instead, Intrusion Prevention Rules are derived from the priority mode assigned and are based on Trend Micro's analysis of operating system vulnerabilities.

Vulnerability Protection Pattern

The Vulnerability Protection Pattern used by Apex One contains the Intrusion Prevention Rules recommended by Trend Micro, based on in-depth analysis of operating system vulnerabilities. This pattern is released weekly or more often depending on the urgency of some vulnerabilities. Intrusion Prevention Rules deployed to the Security Agents through the pattern will examine the actual content and sequences of network packets. Based on the conditions set within the Rule, various actions are then carried out on these packets, including dropping the packets or resetting the connection.

When the Vulnerability Protection Pattern is downloaded to the Apex One Server, the pattern is saved and decoded. The decoded rules are displayed in the list of Intrusion Prevention Rules. Each rule includes information such as Name, Application Type, Severity and CVE. Search can be used to filter this list.



The screenshot shows the Trend Micro Apex Central interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help, along with a user icon labeled "Admin". Below the navigation is a search bar with dropdowns for Products, Categories, and Types, and a checkbox for "Enable intelligent component downloading". The main content area is titled "Components" and displays a table of available components. The table has columns for Category, Type, Current Version, Last Download, and Associated Products. A checkbox in the first column is checked for the "Vulnerability Protection Pattern" entry under the "Intrusion Prevention" category. This row is highlighted with a red oval. Other entries in the table include Advanced Threats, Antivirus, and Firewall.

Category	Type	Current Version	Last Download	Associated Products
Advanced Threats				
Antivirus				
Application Control				
Behavior Monitoring				
Browser Exploit Solution				
Damage Cleanup Services				
Data Loss Prevention				
Deep Discovery				
Endpoint Sensor				
Firewall				
Intrusion Prevention				
<input checked="" type="checkbox"/> Vulnerability Protection Pattern	Pattern	20061	12/11/2020 17:29:32	Apex One
Network Content Inspection				
Plug-in Manager				

Vulnerability Protection Rules

After enabling Vulnerability Protection for a domain, select the profile and the rules used by that profile are displayed.

The screenshot shows the Trend Micro Apex Central web interface. In the top navigation bar, the 'Vulnerability Protection' tab is selected. Under this tab, the 'Enable Vulnerability Protection' checkbox is checked. Below it, there are two radio button options: 'Recommended' (selected) and 'Aggressive'. A red circle highlights the 'Profile' dropdown menu. The main area displays a table of intrusion prevention rules with the following columns: Status, Identifier, Rule Name, Application Type, Severity, Mode, Type, and CVE. The table lists five rules, all of which are currently disabled (Default). The first rule is Microsoft Windows SMB2 Server Remote Code...

Status	Identifier	Rule Name	Application Type	Severity	Mode	Type	CVE
Default (Disabled)	1010653	Microsoft Windows SMB2 Server Remote Code ...	DCERPC Services	Critical	Detect O...	Vulner...	CVE-...
Default (Disabled)	1010652	Microsoft Windows SMB2 Server Information Dis...	DCERPC Services	Critical	Detect O...	Vulner...	CVE-...
Default (Disabled)	1010594	Google Chrome FreeType Font File Buffer Overfl...	DCERPC Services ...	Medium	Prevent	Exploit	CVE-...
Default (Disabled)	1010585	Identified Possible Ransomware File Extension ...	DCERPC Services ...	Critical	Detect O...	Smart	N/A
Default (Disabled)	1010556	Microsoft Windows Remote Desktop Protocol Inf...	Remote Desktop Pr...	Critical	Prevent	Exploit	CVE-...

Note: The list of rules used in a particular profile are not configurable, they are assigned to the mode by Trend Micro engineers.

Displayed columns include:

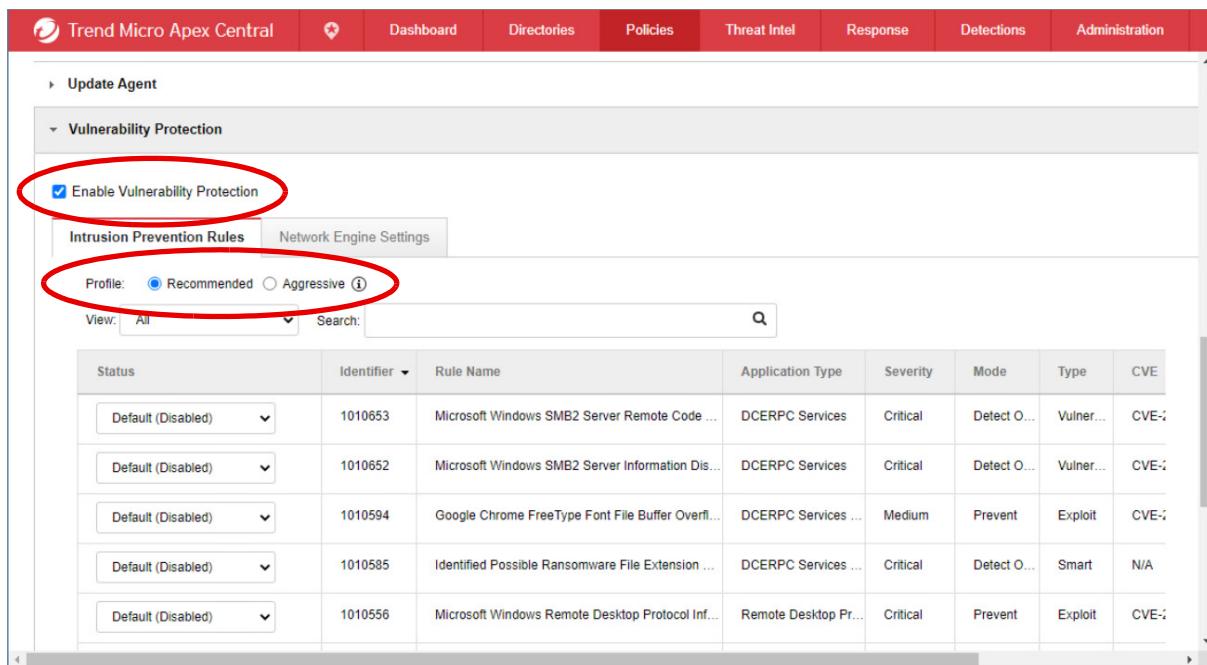
- **Identifier:** This column displays a unique numeric code assigned to the rule by Trend Micro.
- **Name:** This column displays short description of the rule, for naming purposes.
- **Application Type:** This column identifies the operating system component that requires the rule.
- **Severity:** This column displays one of four possible rule severity levels: Low, Medium, High, or Critical.
- **Mode:** Intrusion Prevention rules can operate in either **Prevent** or **Detect** modes. Detect mode rules generate log entries when triggered, but do not drop the packets or reset the connection. Prevent mode rules will enforce the action assigned to them.
- **Type:** This column identifies the type of rule, whether Exploit, Vulnerability or Smart. Exploit rules are used to protect against specific exploits in a one-to-one relationship. Vulnerability rules protect against multiple exploits and Smart rules protect against multiple vulnerabilities.
- **CVE:** This column list the globally unique Common Vulnerability and Exploit identifier.
- **Microsoft:** This column lists the Microsoft Common Vulnerabilities and Exposures (CVE) identifier.

- **CVSS Score:** This column displays the Common Vulnerability Scoring System score which can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. CVSS is a published standard used by organizations worldwide.
- **Last Updated:** This column displays the date when the rule was last updated.

Columns can be sorted by clicking the column header. The list of rules can also be searched by typing a string in the **Search** box at the top of the list.

Selecting a Profile

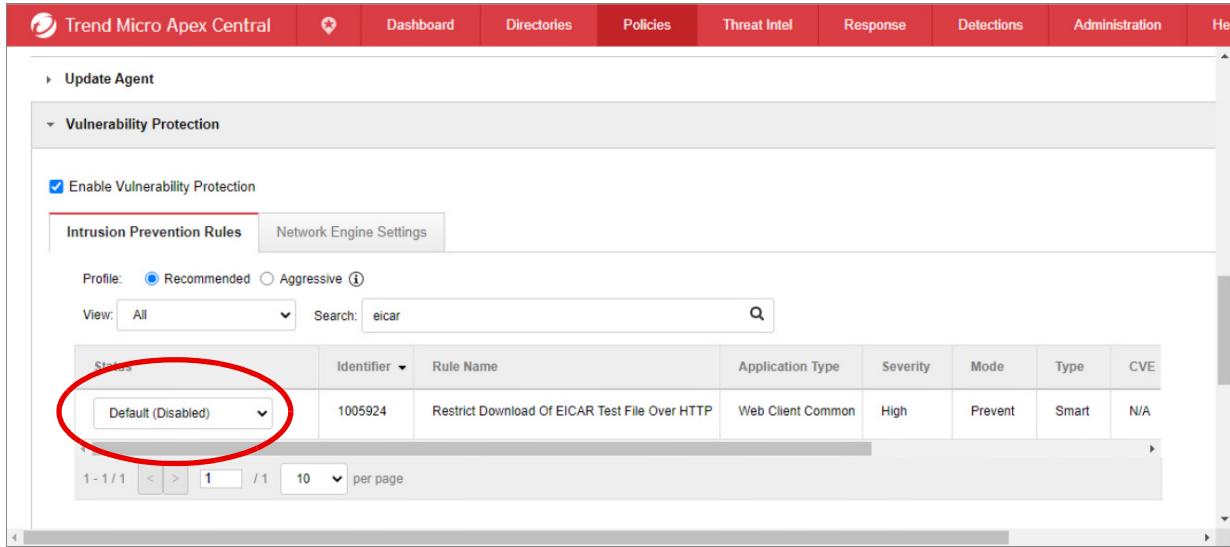
In a policy, click the **Vulnerability Protection** category and click the **Intrusion Prevention Rules** tab. Click to **Enable Vulnerability Protection**. Select either the **Recommended** or **Aggressive** profile.



The screenshot shows the Trend Micro Apex Central interface. In the navigation bar, the 'Policies' tab is selected. Under the 'Vulnerability Protection' section, the 'Intrusion Prevention Rules' tab is active. A red circle highlights the 'Enable Vulnerability Protection' checkbox, which is checked. Another red circle highlights the 'Profile' selection, where the 'Recommended' radio button is selected. Below these controls is a table listing intrusion prevention rules, with columns for Status, Identifier, Rule Name, Application Type, Severity, Mode, Type, and CVE. The first five rows of the table are shown, each detailing a different vulnerability rule.

Status	Identifier	Rule Name	Application Type	Severity	Mode	Type	CVE
Default (Disabled)	1010653	Microsoft Windows SMB2 Server Remote Code ...	DCERPC Services	Critical	Detect O...	Vulner...	CVE-2
Default (Disabled)	1010652	Microsoft Windows SMB2 Server Information Dis...	DCERPC Services	Critical	Detect O...	Vulner...	CVE-2
Default (Disabled)	1010594	Google Chrome FreeType Font File Buffer Overfl...	DCERPC Services ...	Medium	Prevent	Exploit	CVE-2
Default (Disabled)	1010585	Identified Possible Ransomware File Extension ...	DCERPC Services ...	Critical	Detect O...	Smart	N/A
Default (Disabled)	1010556	Microsoft Windows Remote Desktop Protocol Inf...	Remote Desktop Pr...	Critical	Prevent	Exploit	CVE-2

If a rule is required and is not part of the **Recommended** profile by default, the status can be changed from the drop-down list.



The screenshot shows the Trend Micro Apex Central interface. In the top navigation bar, the 'Vulnerability Protection' tab is selected. Under the 'Intrusion Prevention Rules' tab, there is a search bar with the term 'eicar'. A table lists a single rule:

Status	Identifier	Rule Name	Application Type	Severity	Mode	Type	CVE
Default (Disabled)	1005924	Restrict Download Of EICAR Test File Over HTTP	Web Client Common	High	Prevent	Smart	N/A

A red circle highlights the 'Status' dropdown menu for the first row. Below the table, there is a pagination control showing '1 - 1 / 1' and a dropdown for 'per page'.

Network Engine Settings

The **Network Engine Settings** tab allows the selection of the Network Engine detection mode. There are two possible modes:

- **Inline:** In Inline mode, live packet streams pass directly through the Vulnerability Protection network engine. All rules are applied to the network traffic before the packets proceed up the protocol stack.
- **Tap (Detect-only):** In Tap mode, live packet streams are replicated and diverted from the main stream. This mode is handy for evaluating the behavior of the rules as log entries will be generated without applying the rule action.

This tab also includes enables the configuration of timeouts and other options.

The screenshot shows the 'Vulnerability Protection Settings' page in the Apex Central web interface. The 'Network Engine Settings' tab is selected. It contains various configuration options for network connections:

- Network Engine detection mode: Inline Tap (Detect-only)
- ESTABLISHED Timeout: 3 Hours
- LAST_ACK Timeout: 30 Seconds
- Cold Start Timeout: 5 Minutes
- UDP Timeout: 10 Seconds
- Maximum TCP Connections: 1000
- Maximum UDP Connections: 1000
- Ignore Status Code: None
- Ignore Status Code: None
- Ignore Status Code: None
- Advanced Logging Policy: Default

At the bottom of the page are 'Deploy' and 'Cancel' buttons.

- **ESTABLISHED Timeout:** How long to stay in the ESTABLISHED state before closing the connection.
- **LAST_ACK Timeout:** How long to stay in the LAST-ACK state before closing the connection.
- **Cold Start Timeout:** Amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started.
- **UDP Timeout:** Maximum duration of a UDP connection.
- **Maximum TCP Connections:** Maximum simultaneous TCP Connections.
- **Maximum UDP Connections:** Maximum simultaneous UDP Connections.
- **Ignore Status Code:** This option lets you ignore certain types of Events. You can specify up to three Events to ignore.
- **Advanced Logging Policy:** Select from the following settings:
 - **Bypass:** No filtering of Events. Overrides the Ignore Status Code settings (above) and other advanced settings, but does not override logging settings defined on the Apex One server.
 - **Default:** Will switch to Tap Mode if the engine is in Tap Mode, and will switch to Normal if the engine is in Inline Mode.
 - **Normal:** All Events are logged except dropped retransmits.
 - **Backwards Compatibility Mode:** For support use only.
 - **Verbose Mode:** Same as **Normal** but including dropped retransmits.
 - **Stateful and Normalization Suppression:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy.
 - **Stateful, Normalization, and Frag Suppression:** Ignores everything that Stateful and Normalization Suppression ignores as well as events related to fragmentation.
 - **Stateful, Frag, and Verifier Suppression:** Ignores everything Stateful, Normalization, and Frag Suppression ignores as well as verifier-related events.

- **Tap Mode:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection.

Lesson 18: Detecting and Investigating Security Incidents on Endpoint Computers

Lesson Objectives:

After completing this lesson, participants will be able to:

- Create policies using Endpoint Sensor
- Define the phases in the Incident Response Model
- Perform a preliminary assessment using Endpoint Sensor recorded data
- Generate a root cause analysis
- Respond to security incidents
- Perform a detailed investigation

Apex One includes tools for detecting and investigating suspicious activities on endpoint computers. These capabilities allow threat investigators to explore detections and hunt for new threats using Endpoint Detection and Response (EDR). Endpoint Detection and Response uses advanced detection and response techniques integrated into the Security Agents on the endpoint computers to automate the identification and containment of advanced threats.

In addition to Endpoint Detection and Response, Trend Micro has introduced a Managed Detection and Response Service (MDR), where trained analysts in a Trend Micro Security Operation Centers (SOC) can assist organizations that don't have incident response staff to complete a detailed investigation of threats and provide the steps needed to deal with these threats.

Trend Micro Endpoint Sensor plays a vital role in preventing, monitoring and containing the extent of damage caused by targeted attacks on endpoints and servers.

Integrated Endpoint Sensor

Trend Micro Endpoint Sensor identifies affected endpoints through on-demand investigations and monitoring of threats, providing analysts with a comprehensive set of threat details that can help them respond effectively to attacks. Endpoint Sensor plays an import role in the solution against advanced persistent threats.

Separate Endpoint Sensor Agents and Servers are no longer needed to provide Endpoint Detection and Response capabilities in Apex One. If the separate Agent is in use for an existing OfficeScan XG installation, it will be automatically uninstalled when Apex One policies using Endpoint Sensor are deployed and a new Apex One service will be launched to integrate Endpoint Sensor.

Note: Endpoint Sensor is not supported on Windows Server platforms.

On the endpoint, the Apex One Security Agent records vectors commonly associated with targeted attacks, such as file executions, memory violations, registry changes, and more in the form of metadata. Endpoint Sensor utilizes the data during a preliminary investigation to identify affected endpoints. The Agent creates a database of all the files, activities, and important system resources, and continuously updates this database to record the arrival and execution of suspicious objects. This data is forwarded to Apex One Server on a regular basis.

The type of metadata collected depends on the operating system installed on the endpoint.

Metadata collected from Windows endpoints include:

- Host (name / IP address)
- User account
- File name
- File path
- Hash values (SHA-1, SHA-256 and MD5)
- Registry key
- Registry data
- Registry name
- Command line

Metadata collected from macOS endpoints include:

- Host (name / IP address)
- User account
- File name
- File path
- Hash values (SHA-1, SHA-256 and MD5)
- Command line

Policies using Endpoint Sensor must be deployed through Apex Central. Endpoint Sensor capabilities are built-in into the Apex One Server and Security Agent, however, an **additional license is required to activate them**.

Trend Micro Endpoint Sensor provides the following capabilities to assist in the investigation and mitigation of advanced threats:

- **Threat Investigation:** Endpoint Sensor provides a central location to investigate threats on multiple endpoints. Endpoint Sensor can investigate both the historical and current state of all managed endpoints. Each investigation can display a graphical breakdown of the threat activities, which allows administrators to re-construct the events related to the security incident from start to end.
If regular monitoring is part of the organization's security plan, Endpoint Sensor provides the option to schedule investigations at specified intervals.

- **Customized Endpoint Investigation:** Endpoint Sensor supports Indicators of Compromise (IOC) and YARA rules which allow the creation, sharing and re-use of existing threat information. IOC and YARA rules are fully customizable to address targeted attacks. Additionally, Endpoint Sensor also provides its own set of IOC rules, which are regularly updated to provide protection from the most recent threats.
- **Remote Endpoint Management:** Endpoint Sensor allows administrators to monitor, manage and run investigations on endpoints through the Apex Central Web-based management console. The Web Management console provides a means to configure the endpoint policies remotely, and view endpoint details, such as agent version, pattern version, and so forth, all from a central location.
- **Attack Discovery:** Endpoint Sensor can proactively monitor and discover suspicious files and behavior through user-defined IOC rules. Endpoint Sensor also leverages Trend Micro's threat intelligence through the use of regularly updated IOC rules to provide protection from the latest threats.
- **File Collection and Analysis:** Endpoint Sensor collects all files that match a monitoring rule. Once a suspicious file is found, it can be sent to a local file server, or sent to a Deep Discovery Analyzer device for further analysis. Deep Discovery Analyzer then provides Endpoint Sensor with a comprehensive set of threat details that can help administrators determine if a file is malicious or not.

Note: Endpoint Sensor requires the use of the full version of Microsoft SQL Server 2016 (not SQL Express) with the **Full-Text and Semantic Extractions for Search** feature enabled.

Enabling Endpoint Sensor

When enabled, Endpoint Sensor monitors the endpoint computer and forwards metadata to the Apex One server. **Policies using Endpoint Sensor must be deployed from Apex Central.**

The screenshot shows the Apex Central web interface with the following navigation bar:

- Dashboard
- Directories
- Policies
- Threat Intel
- Response
- Detections
- Administration
- Help

The main content area displays the "Endpoint Sensor Settings" section. It includes the following settings:

- Behavior Monitoring Settings:**
 - Enable Endpoint Sensor (circled in red)
 - Enable event recording
 - Maximum size of event database: 1 GB
- Advanced Settings:**
 - Send a subset of log data to perform Historical Investigation
 - Upload Frequency: Every 15 minutes
 - Additional batch types: 1MB, 2MB, 5MB
 - Enable Attack Discovery to detect known attack indicators on endpoint (circled in red)
- Other sections visible include "Manual Scan Settings" and "Predictive Machine Learning Settings".

In addition to enabling Endpoint Sensor, the option to enable Attack Discovery is available. Attack Discovery uses Trend Micro threat intelligence based on Indicators of Attack behavior. After detecting a known Indicator of Attack, Attack Discovery logs the detection.

Endpoint Detection and Response

Endpoint Detection and Response is a solution that allows administrators to continuously monitor endpoints and record activities that could be considered suspicious. This centrally stored data can then be searched for suspicious and malicious activities by a threat analyst.

The goals of the Endpoint Detection and Response system include:

- Detecting security incidents that may have been missed by other detection methods
- Containing the incident at the endpoint
- Providing guidance for further investigation of security events
- Providing remediation guidance

The key value of Endpoint Detection and Response solutions is detecting threats that have evaded other protection technologies.

Endpoint Detection and Response assists the analyst in their investigation by providing three primary functions:

- Recording and storing endpoint system-level behaviors. In Apex One, this function is provided by Endpoint Sensor which is now integrated into the Security Agent.
- Detecting or flagging suspicious system behaviors from recorded data using various data analytics techniques. In Apex One, this functionality is provided through Apex Central.
- Providing remediation suggestions to the analysts on how best to respond to the security incident.

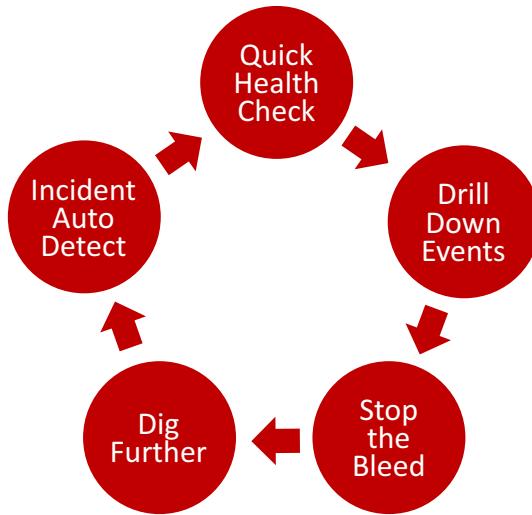
Based on the analysis of the collected data, the analyst can quickly answer some of the most common questions when systems are breached, such as:

- What is the extent of the breach?
- How did the breach happen?
- What did the hacker or malware do while it was active?
- How do we confidently restore the system so that all traces of the malware are removed?
- Was this a random attack, was it targeted, and what were the attackers goals?
- How do we prevent it from happening again?

Apex One Incident Response Model

The Apex One incident response model includes five distinct phases to deal with security incidents. These phases include:

- **Quick Health Check:** This phase provides a **Preliminary Assessment**.
- **Drill Down Events:** This phase provides a **Root Cause Analysis** for the security incident.
- **Stop the Bleed:** This phase provides **Incident Responses** to prevent further infection.
- **Dig Further:** To better understand the impact of the security incident, this phase performs a live **Detailed Investigation** of the endpoint. This phase does not rely on Endpoint Sensor recorded metadata.
- **Incident Auto-Detect:** This phase provides **Attack Discovery** based on rules generated from previously encountered incidents.



Preliminary Assessment

A preliminary assessment is a quick search of objects that is run against historical metadata recorded by Endpoint Sensor and stored on the Apex One Server. Since this task is not executed on the endpoints themselves, it provides visibility of the whole environment, even when some endpoints are offline.

Preliminary assessments aim to shorten the waiting time while performing an investigation. The average assessment scan takes between 5 to 10 seconds. The Apex One Security Agent can upload metadata to the Apex One Server every 3, 6, 12 or 24 hours. Once uploaded, the Apex Central will perform a quick scan against the Server database directly. The metadata retention period is based on the storage add-on license purchased. By default, metadata is stored for 30 days, but a license for 90, 180 or 365 days can be purchased.

Since preliminary assessment scans are performed against metadata, it **does not provide a real-time view** of the endpoint. This is by design, as it provides a fast response to a query.

Preliminary assessments can be performed from a few different locations in Apex Central.

Preliminary Investigation

In Apex Central, click **Response > Preliminary Investigation**.

The screenshot shows the Trend Micro Apex Central interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. On the far right, it shows 'Admin' with a dropdown arrow. Below the navigation bar, the title 'Preliminary Investigation' is displayed. Underneath, there are two tabs: 'Assessment' (which is selected) and 'Root Cause Analysis Results'. A section titled 'Criteria:' has two options: 'Custom criteria' (selected) and 'OpenIOC file'. Below this is a dropdown menu 'Match all of the following' with a 'Select Criteria' button. There's also a 'Add criteria' button. At the bottom of the screen are two buttons: 'Assess' and a 'Print' icon.

Preliminary investigations in Apex One will help administrators evaluate impact scope through custom criteria defined by the administrator or OpenIOC.

Note: The data available during Preliminary investigations is a subset of Security Agent data and only includes information about high risk file types. If an assessment returns no results, you may want to perform a detailed investigation.

Custom criteria

An assessment using custom criteria can determine the existence of a threat using simple criteria, such as user account, file name, registry values. An administrator can specify or load up to ten user-defined criteria.

This screenshot is similar to the one above, but the 'Custom criteria' option under 'Criteria:' is highlighted with a red oval. The rest of the interface is identical to the first screenshot.

OpenIOC File

An OpenIOC file is an XML file which contains one or more Indicators of Compromise (IOCs). Administrators can use OpenIOC rules to define investigation criteria. Preliminary investigations disregard all conditions and match any of the indicators specified in the OpenIOC file. A preliminary assessment can be performed when an analyst receives an indicator of compromise which is compared against the metadata stored on the Apex One Server to see if the environment is compromised.

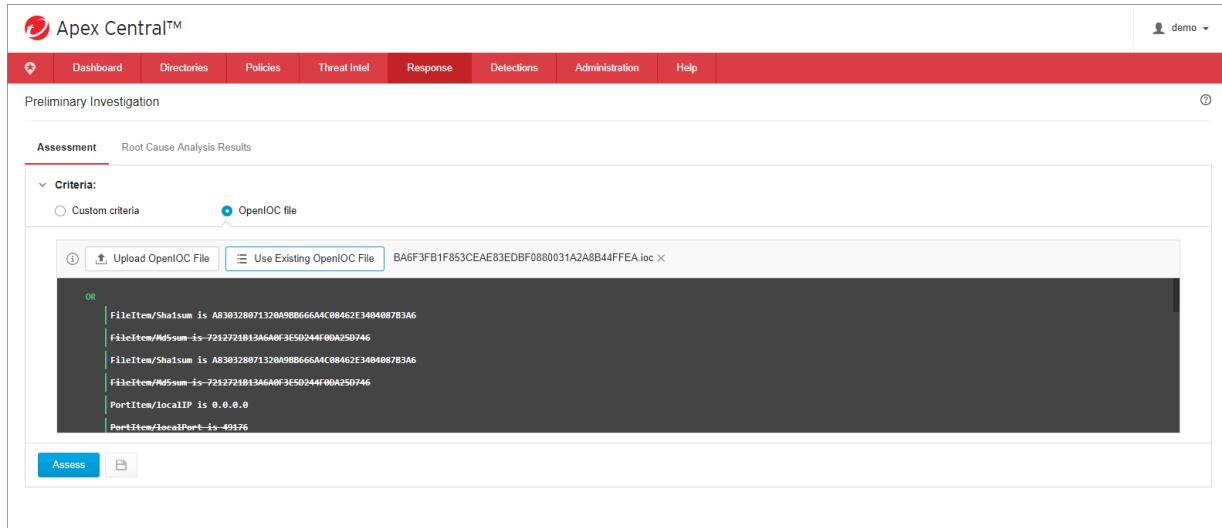
OpenIOC files can be provided by Trend Micro through Apex Central (click **Use Existing OpenIOC File**) or acquired from other sources and imported (**Upload OpenIOC File**).

OpenIOC Files					
<input type="text"/> File name, description, source and Added by					
File Name	Description	Added	Source	Added by	
<input checked="" type="radio"/> BA6F3FB1F853CEA...	OpenIOC For Sample...	11/19/2018 15:30:54	Manual	demo	
<input type="radio"/> iocbucket_5f16da435...	Operation Pitty Tiger ...	11/28/2018 16:12:30	Manual	demo	
<input type="radio"/> iocbucket_b43da0a62...	10004 - Mimikatz	01/17/2019 15:55:37	Manual	demo	
<input type="radio"/> openioc.ioc	Event #10	03/11/2019 22:50:14	Manual	demo	
<input type="radio"/> 2384c8ce-6eca-4d06-...	DARWIN (BLOGPOST)	03/11/2019 22:50:26	Manual	demo	

Records: 1-5 / 5 | 10 per page ▲ 1 / 1 < >

Apply **Cancel**

Select the OpenIOC file and click **Apply**.



Using OpenIOC files in preliminary investigations has the following limitations:

- Only one OpenIOC file can be loaded at a time.
- Any operator specified in the OpenIOC file is changed to OR.
- The only supported condition is IS. Entries using other conditions are ignored and marked with a strikethrough.
- The only supported indicators are the indicators that are applicable to the collected metadata. Entries using unsupported indicators are ignored and marked with a strikethrough.

Custom Intelligence

Preliminary assessment can also be used to sweep the environment for objects that have not yet been identified by Apex One as malicious. Suspicious objects defined in Custom Intelligence can be used as the basis of the sweep. These objects can come from variety of sources. Security Agents can be configured to automatically flag the defined objects when they enter the environment. Once the types of objects have been defined by importing or adding the appropriate files, click **Analyze Impact**.

In Apex Central, click Threat Intel > Custom Intelligence.

User-Defined Suspicious Objects

You can protect your network from objects not yet identified on your network by adding the suspicious objects to the User-Defined Suspicious Object list. Apex Central provides the option to add objects based on the file, file SHA-1, domain, IP address, or URL. You can also specify the scan action that supported Trend Micro products perform after detecting the suspicious objects.

Click Threat Intel > Custom Intelligence and click the User-Defined Suspicious Objects tab.

Click Add to create your own custom list of user-defined suspicious objects, or click Import to load a *.csv file containing the details.

Lesson 18: Detecting and Investigating Security Incidents on Endpoint Computers

Click to select the User-Defined Suspicious Object from the list and click **Analyze Impact**.

The screenshot shows the Apex Central™ interface with a red header bar containing links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A user profile icon 'demo' is in the top right. Below the header is a 'Custom Intelligence' section with a note to protect against objects not yet identified. The main area is titled 'User-Defined Suspicious Objects' with tabs for STIX and OpenIOC. It displays a table with columns: View, Object, Type, Affected Endpoints/Recipients, Scan Action, Source, Source Added By, Notes, and Last Modified. There are 6 items listed:

View	Object	Type	Affected Endpoints/Recipients	Scan Action	Source	Source Added By	Notes	Last Modified
All	E50D9E3BD91908E13A26B3E23EDEAF57...	File SHA-1	0 / 0	Block	Manual	demo		04/08/2019 08:13:48
	27925DA5BB9C7017681047182A5BC17ED...	File SHA-1	0 / 0	Block	Manual	demo		04/05/2019 06:22:55
	5330FEDAD48CE0E4C23B2ABE1075A1F98...	File SHA-1	0 / 0	Block	Manual	demo		04/05/2019 06:22:45
	141.108.2.157	IP address	0 / 0	Log	2384c8ce...	demo		04/01/2019 11:54:08
	video.csmcpr.com	Domain	0 / 0	Log	2384c8ce...	demo		04/01/2019 11:54:08
	icc.ignorelist.com	Domain	0 / 0	Log	2384c8ce...	demo		04/01/2019 11:54:08

Pagination controls at the bottom show 1 - 6 / 6, page 1 of 1, 20 per page.

It will take a few moments while the scan is performed.

- ✓ Preliminary Investigation started. Refresh the screen periodically to view updated results.
Security Agents on identified endpoints automatically perform a Root Cause Analysis.

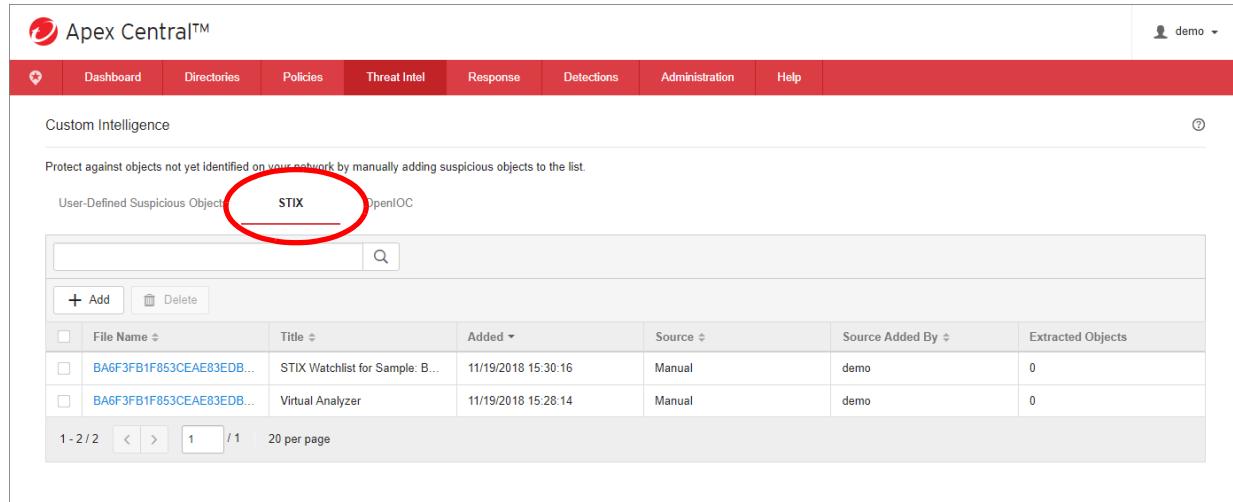
Important! Analysis times vary based on the number of endpoints and the Security Agent connection status.
To view individual results, expand the arrow in front of the Object and click View in the Root Cause Analysis column.

Structured Threat Information Expression

Structured Threat Information Expression (STIX) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner.

After obtaining a properly formatted Structured Threat Information Expression (STIX) file (*.xml) from a trusted external source (a security forum or other Deep Discovery Virtual Analyzer product), import the file to Apex Central to extract the suspicious file SHA-1, IP address, URL, and domain objects to the User-Defined Suspicious Object list. When uploading a file, you can also specify the scan action that supported Trend Micro products perform after detecting the suspicious objects.

Click Threat Intel > Custom Intelligence and click the STIX tab. Click Add to select the file to load.

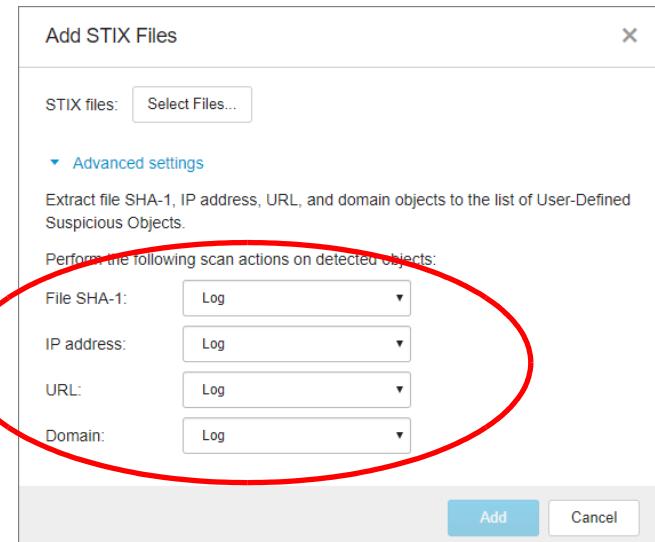


The screenshot shows the Apex Central web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel (which is the active tab), Response, Detections, Administration, and Help. Below the navigation bar, the page title is "Custom Intelligence". A sub-header says "Protect against objects not yet identified on your network by manually adding suspicious objects to the list." Under this, there's a section titled "User-Defined Suspicious Objects" with tabs for "STIX" (circled in red) and "OpenIOC". Below the tabs is a search bar and a table with columns: File Name, Title, Added, Source, Source Added By, and Extracted Objects. Two entries are listed:

File Name	Title	Added	Source	Source Added By	Extracted Objects
BA6F3FB1F853CEAE83EDB...	STIX Watchlist for Sample: B...	11/19/2018 15:30:16	Manual	demo	0
BA6F3FB1F853CEAE83EDB...	Virtual Analyzer	11/19/2018 15:28:14	Manual	demo	0

At the bottom of the table area, there are pagination controls (1 - 2 / 2), a search input, and a "20 per page" dropdown.

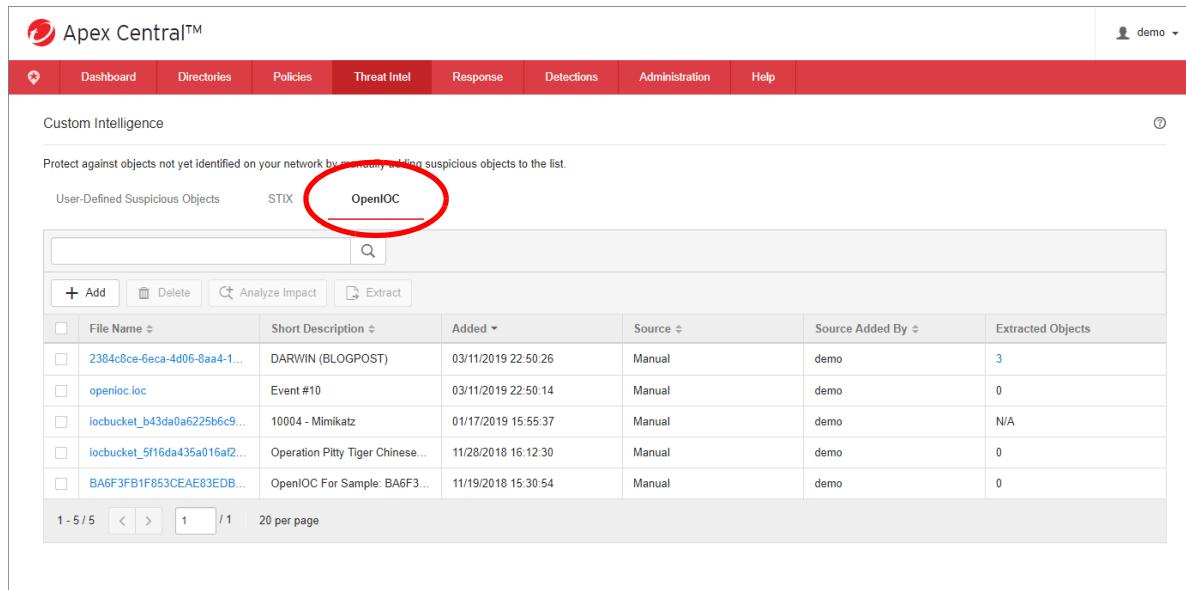
Locate the STIX file and select the action to be performed on detected objects.



The dialog box has a title "Add STIX Files" and a close button. It contains a "STIX files:" field with a "Select Files..." button. Below this is a "Advanced settings" section with a descriptive text: "Extract file SHA-1, IP address, URL, and domain objects to the list of User-Defined Suspicious Objects." Underneath is a heading "Perform the following scan actions on detected objects:" followed by four dropdown menus: "File SHA-1:" set to "Log", "IP address:" set to "Log", "URL:" set to "Log", and "Domain:" set to "Log". At the bottom right are "Add" and "Cancel" buttons.

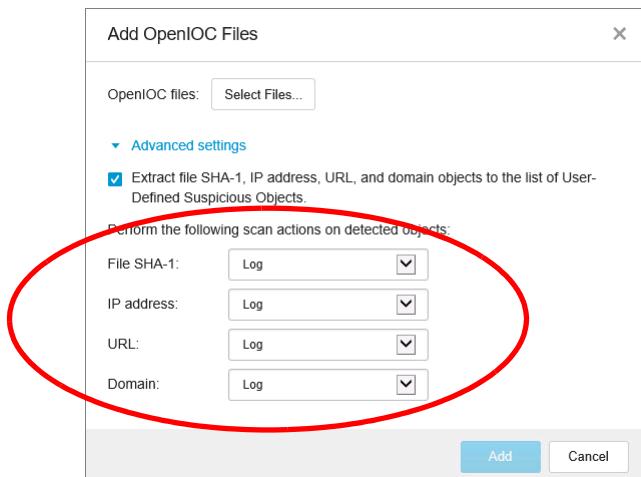
OpenIOC

You can protect your environment from objects not yet identified on your network by importing properly formatted OpenIOC files (*.ioc) and extracting suspicious file SHA-1, IP address, URL, and domain objects to the User-Defined Suspicious Object list. When uploading a file, you can specify the scan action that supported Trend Micro products perform after detecting the suspicious objects. After uploading an OpenIOC file, you can also select an uploaded file as the assessment criteria for a Preliminary or Detailed Investigation.



The screenshot shows the Apex Central™ interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A user profile icon with the name "demo" is in the top right. Below the navigation is a section titled "Custom Intelligence". It contains a sub-section for "User-Defined Suspicious Objects" and "STIX", with "OpenIOC" highlighted and circled in red. A table lists several entries with columns for File Name, Short Description, Added, Source, Source Added By, and Extracted Objects. At the bottom, there are pagination controls (1 - 5 / 5, 1 / 1, 20 per page).

Click **Add** to import an OpenIOC file, and select the scan action to perform on detected objects.



The dialog box has a title "Add OpenIOC Files" and a close button "X". It contains a "Select Files..." button under "OpenIOC files:". A "Advanced settings" section is expanded, showing a checked checkbox for "Extract file SHA-1, IP address, URL, and domain objects to the list of User-Defined Suspicious Objects". Below this, a section titled "Perform the following scan actions on detected objects:" is circled in red. It includes dropdown menus for "File SHA-1", "IP address", "URL", and "Domain", all set to "Log". At the bottom are "Add" and "Cancel" buttons.

Click to select the OpenIOC object from the list and click **Analyze Impact**.

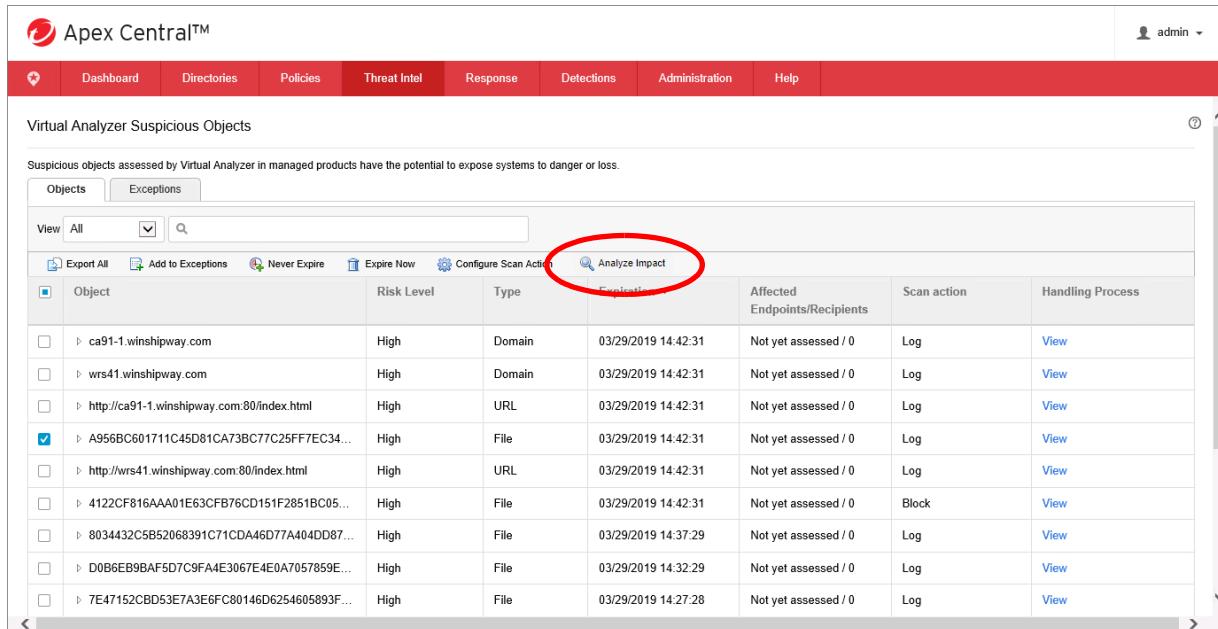
File Name	Short Description	Added	Source	Source Added By	Extracted Objects
<input checked="" type="checkbox"/> 2384c8ce-6eca-4d06-8aa4-1...	DAIWIN (BLOGPOST)	03/11/2019 22:50:26	Manual	demo	3
<input type="checkbox"/> openioc.ioc	Event #10	03/11/2019 22:50:14	Manual	demo	0
<input type="checkbox"/> iocbucket_b43da0a6225b6c9...	10004 - Mimikatz	01/17/2019 15:55:37	Manual	demo	N/A
<input type="checkbox"/> iocbucket_5f16da435a016af2...	Operation Pitty Tiger Chinese...	11/28/2018 16:12:30	Manual	demo	0
<input type="checkbox"/> BA6F3FB1F853CEAE83EDB...	OpenIOC For Sample: BA6F3...	11/19/2018 15:30:54	Manual	demo	0

Virtual Analyzer Suspicious Object

This assessment method leverages Suspicious Objects generated by Cloud Sandbox/Deep Discovery Analyzer, but is limited to file hash, domain, destination IP address.

The Virtual Analyzer Suspicious Objects window allows an administrator to perform an impact analysis on the network. The impact analysis uses Endpoint Sensor to contact Agents and performs a historical scan of its logs to determine if the suspicious objects have affected your environment for a period of time without detection.

In Apex Central, click **Threat Intel > Virtual Analyzer Suspicious Objects**. Click to select the desired object and click **Analyze Impact**.



The screenshot shows the Apex Central interface with the following details:

- Header:** Apex Central™, admin
- Navigation:** Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help
- Section:** Virtual Analyzer Suspicious Objects
- Message:** Suspicious objects assessed by Virtual Analyzer in managed products have the potential to expose systems to danger or loss.
- Toolbar:** Objects (selected), Exceptions, View All, Export All, Add to Exceptions, Never Expire, Expire Now, Configure Scan Action, Analyze Impact (circled in red).
- Table:** A grid of suspicious objects with columns: Object, Risk Level, Type, Last Seen*, Affected Endpoints/Recipients, Scan action, and Handling Process. One row is selected (checkbox checked) for the URL <http://A956BC601711C45D81CA73BC7C25FF7EC34...>.

Root Cause Analysis

Root Cause Analysis is the graphical representation of how the infection and/or suspicious activities occurred. This is very helpful in tracking down the root cause of the problem, identifying *patient zero* or the entry point.

If an assessment returns a match, administrators may generate a root cause analysis to:

- List all related objects to the specified criteria
- Identify if any of the related objects are noteworthy
- Review the sequence of events leading to the execution of the matched object.

Root Cause Analysis provides a forensic picture from the endpoint side of the attack to track down the root cause of infection and related suspicious/malicious activities. Root Cause Analysis tasks are created on Apex One Server as an investigation batch. Endpoints poll the Apex One Server every ten minutes for updates and to collect the batch of investigation tasks. Root Cause Analysis needs one to five minutes to complete and to upload the results.

Note: Root Cause Analysis is not supported for Mac Security Agents.

To manually generate the Root Cause Analysis, click **Response > Preliminary Investigation > Assessment**. Select the required endpoints and click **Generate Root Cause Analysis**.

The screenshot shows the Apex Central interface with the following details:

- Header:** Apex Central™, demo
- Navigation Bar:** Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help
- Section:** Preliminary Investigation
- Sub-Section:** Assessment (selected), Root Cause Analysis Results
- Criteria:**
 - Custom criteria (radio button selected)
 - OpenIOC file (radio button unselected)
 - Match all of the following dropdown: Host (Host name / IP address)
 - Input field: win10enten
 - Add criteria button
- Buttons:** Assess, Print
- Table:** Endpoints (1)

Endpoint	Action
WIN10ENTEN	Generate Root Cause Analysis (1)

Provide a name for the Root Cause Analysis report.

The dialog box contains the following fields:

- Name:** RCA on WIN10
- Criteria:** [Host: win10enten]
- Endpoints:** Endpoint (1)
WIN10ENTEN
- Period:** All (radio button selected)

Buttons at the bottom: Generate, Cancel

Lesson 18: Detecting and Investigating Security Incidents on Endpoint Computers

The Root Cause Analysis report will display as processing while the analysis takes place.

A screenshot of the Apex Central interface. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The user is logged in as 'demo'. Below the navigation is a section titled 'Preliminary Investigation' with tabs for 'Assessment' and 'Root Cause Analysis Results'. The 'Root Cause Analysis Results' tab is selected. A table displays two tasks: one labeled 'RCA on ...' (Status: Processing) and another labeled 'Win81ETEN' (Status: Completed). The table columns include Status, Task Name, Criteria, Matched Objects, Endpoint, IP Address, Started, Elapsed, and Creator. At the bottom of the table, it shows 'Records: 1-10 / 73 | 10 per page ▲ 1 / 8 < >'.

In Apex Central, click **Response > Preliminary Investigation > Root Cause Analysis Results** to view the results of all automated and manual Root Cause Analysis tasks.

A screenshot of the Apex Central interface, similar to the previous one but with a red circle highlighting the 'Root Cause Analysis Results' tab. The table below shows the same two tasks: 'RCA on WIN10' (Completed) and 'Win81ETEN' (Completed). The table structure and footer are identical to the first screenshot.

Click the **Task Name** to view the results of the analysis. The **Analysis Chains** tab displays the main Root Cause Analysis information in a graph view.

A screenshot of the 'RCA on WIN10' analysis chains tab. The tab has two sections: 'Analysis Chains' (selected) and 'Object Details'. The 'Analysis Chains' section contains four panels: 'Target Endpoint' (WIN10ENTEN), 'First Observed Object' (powershell.exe), 'Matched Objects (1)' (WIN10ENTEN), and 'Noteworthy Objects' (0). Below these panels is a graph visualization showing the relationships between various objects like powershell.exe, winlogon.exe, and explorer.exe over time. The graph includes nodes for objects and arrows for interactions, with specific timestamps like '2019/01/17 11:34:46' and '2019/01/17 11:36:03'.

Details on the graph include:

- **Target Endpoint:** Displays information of the root cause analysis result, and the ability to isolate the endpoint.
- **First Observed Object:** With built-in intelligence, Endpoint Sensor is able to find the potential entry point of the root cause chain.
- **Matched Objects:** Lists all the objects which matched with input criteria.
- **Noteworthy Objects:** Objects identified as suspicious or malicious will be displayed.

Icons and dots represents each component and their relationship. More information is available for each object by clicking on it (user, pid, hashes...). The root cause analysis area shows object types using the following icons:

Icon	Name	Description
	First Observed Object	Marks an object that most likely created the matched object
	Matched Criteria	Marks objects matching the investigation criteria
	Normal Object	Marks objects that have been verified to not pose a threat, such as common system files (icon in black)
	Unrated Object	Marks objects that are not system files but do not exhibit suspicious behavior (icon in grey)
	Suspicious Object	Marks objects that exhibit behaviors that are similar to known threats (icon in orange)
	Malicious Object	Marks objects that match a known threat (icon in red)
	Boot	Objects that launch during system startup
	Browser	Objects that are capable of displaying web pages, usually a web browser
	Email	Objects that can send and receive email messages, usually an email client or server
	File name	Objects that are files on the disk
	Network	Objects related to network connections or the Internet
	Process	Objects that are processes running during the time of execution
	Registry	Objects that are registry keys, entries or data
	Event	Indicates actions done by the object
.....	Association	Indicates relationships between two objects

If a process object is not normal, it can be terminated. If a process life was too short and the hash couldn't be calculated, termination won't be possible.

The **Objects Details** tab displays same information as **Analysis Chains**, but in tabular format.

Recorded Object	PID	Recorded	Activity	Object Reputation	Affected Endpoints
System	4	2019/01/07 10:31:54	-	Unrated	-
sms.exe	376	2019/01/08 10:38:16	-	Unrated	1 endpoints (33.33%)
smss.exe	28044	2019/01/08 10:38:16	Created by sms.exe	Unrated	1 endpoints (33.33%)
csrss.exe	28058	2019/01/08 10:38:16	Created by smss.exe	Unrated	1 endpoints (33.33%)
winlogon.exe	28116	2019/01/08 10:39:18	Created by smss.exe	Unrated	1 endpoints (33.33%)
userinit.exe	28904	2019/01/08 10:39:06	Created by winlogon.exe	Unrated	1 endpoints (33.33%)
windows storage.dll	-	2019/01/08 10:39:10	Loaded by explorer.exe	Unrated	-
crl.dll	-	2019/01/17 11:34:51	Loaded by powershell.exe	Unrated	-
System ni.dll	-	2019/01/17 11:35:02	Loaded by crl.dll	Unrated	-
System ni.dll	-	2019/01/17 11:35:04	Loaded by powershell.exe	Unrated	-
powershell.exe	111612	2019/01/17 11:36:57	Created by System ni.dll	Unrated	1 endpoints (33.33%)
powershell.exe	111612	2019/01/17 11:36:57	Injected by System	Unrated	1 endpoints (33.33%)
powershell.exe	111480	2019/01/17 11:38:17	Created by windows storage.dll	Unrated	1 endpoints (33.33%)
powershell.exe	111480	2019/01/17 11:38:17	Injected by csrss.exe	Unrated	1 endpoints (33.33%)
explorer.exe	28436	2019/01/19 00:49:21	Created by userinit.exe	Unrated	1 endpoints (33.33%)
explorer.exe	28436	2019/01/19 00:49:21	Injected by System	Unrated	1 endpoints (33.33%)

If an object is not normal, the file name/file hash/domain/IP/registry info can be used as Preliminary Investigation (Impact Assessment) and File hash/domain/IP can be added as Suspicious Objects.

Both Analysis Chains and Object Details can be exported to *.png or *.csv formats.

Incident Response

The incident response phase allows administrators to mitigate damage from infected endpoints, by terminating suspicious processes, banning suspicious applications through User Defined Suspicious Objects or isolating endpoints.

Terminating Suspicious Processes

When you click a process object in the Analysis Chain and its rating is not normal, you can terminate it remotely. After a certain time, the process will be terminated on the endpoint. Click the process object in the Analysis Chain graph and click **Terminate Object**.

SensorTest-WRS31.exe

Profile

Rating : Suspicious

Affected Endpoints: 1 endpoints (5%)

PID : 5468

User :

Terminate Object

Add to Suspicious Objects List

Add to Preliminary Investigation List

Adding Processes to the Suspicious Objects List

A process will not be able to execute/access again if it has been added to User Defined Suspicious Objects. The running process will be terminated as well. Click the process object in the Analysis Chain graph and click **Add to Suspicious Object List**



Apex One Application Control should be enabled for blocking SHA-1 at endpoint.

Isolating Endpoints

From the **Historical Investigation** results, one or more endpoint can be isolated from the network based on Windows Filtering Platform feature. All communication from/to this endpoint would be blocked except between the Apex One Server and Security Agent. Click **Response > Historical Investigation**. On the **Assessment** tab, select the endpoint in question and click **Isolate Endpoint**.

The screenshot shows the Apex Central interface under the 'Assessment' tab. It displays a 'Root Cause Analysis Results' section with criteria selection and a search bar. Below this is a table of endpoints. A red circle highlights the 'Isolate Endpoint (1)' button in the top right corner of the table header. The table shows one endpoint named 'WIN10ENTEN' with details like IP address, operating system, and managing server.

Endpoint	Status	IP Address	Operating System	User	Managing Server	First Logged	Details
WIN10ENTEN	Online	192.168.8.4	Windows 10	TREND\ariel	DBSRV_OSCE	2019/01/17 11:36:18	

When the crisis is resolved, restore endpoint connectivity. Click **Directories > Users/Endpoints**. In the **Endpoints** list, click All.

Endpoint	IP Address	Type	Operating System	Endpoint Server	User	Threats
CLIENT-02	192.168.4.4	Windows	Windows 10	ApexOne, Apex One	Administrator	0
CLIENT-03	192.168.4.6	Windows	Windows 10	ApexOne, Apex One	Administrator	0
DC2016	192.168.4.1	Windows	Windows 2016	ApexOne, Apex One	administrator	0
WIN2012	192.168.4.3	Windows	Windows 2012	ApexOne, Apex One	Administrator	0

Click the isolated endpoint and click Restore from the Task column.

Installed Product	Version	Build	Assigned Policy	Policy Status
Apex One Agent	14.0	1039		Without policy

Isolate Endpoint can be selected from the **Root Cause Analysis** result window, **Detailed Investigation** results and **Endpoint** view.

Detailed Investigation

Detailed (also referred to as Real-Time or Live) Investigation is the search process that deals with the current system state. It scans memory and the disk with specific indicators or examines running process. Detailed Investigation is currently not supported on Mac endpoints.

Detailed Investigation methods available include:

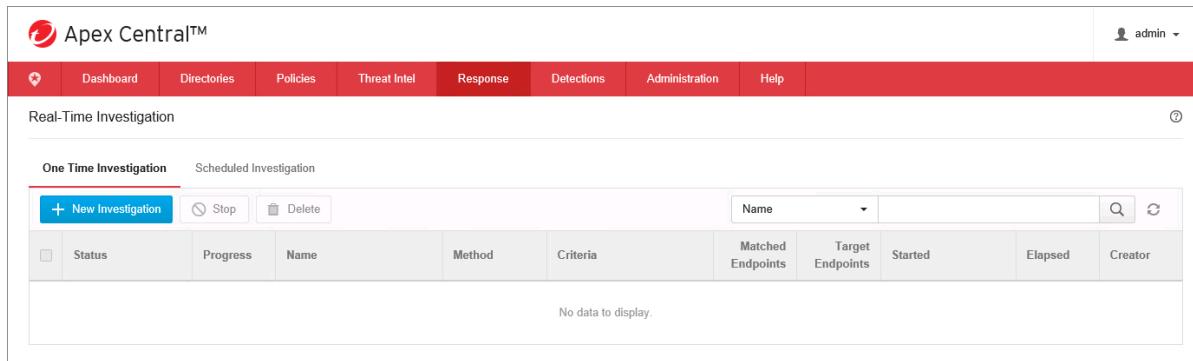
- Search memory using YARA files
- Search the hard disk using OpenIOC files
- Search the Windows Registry with custom criteria

Note: Preliminary Assessment is not run live, but runs on metadata submitted to the Apex One Server. This provides a fast search and works even if endpoint is offline. Detailed Investigation runs on the endpoint in real time.

Root cause analysis results are only available for YARA rules. Because detailed investigations run on the current system state, some files and registry entries may be locked or in use during this period. Root Cause Analysis results are not available for investigations using OpenIOC rules or registry search. To generate a root cause analysis using OpenIOC rules or registry data, use preliminary investigation.

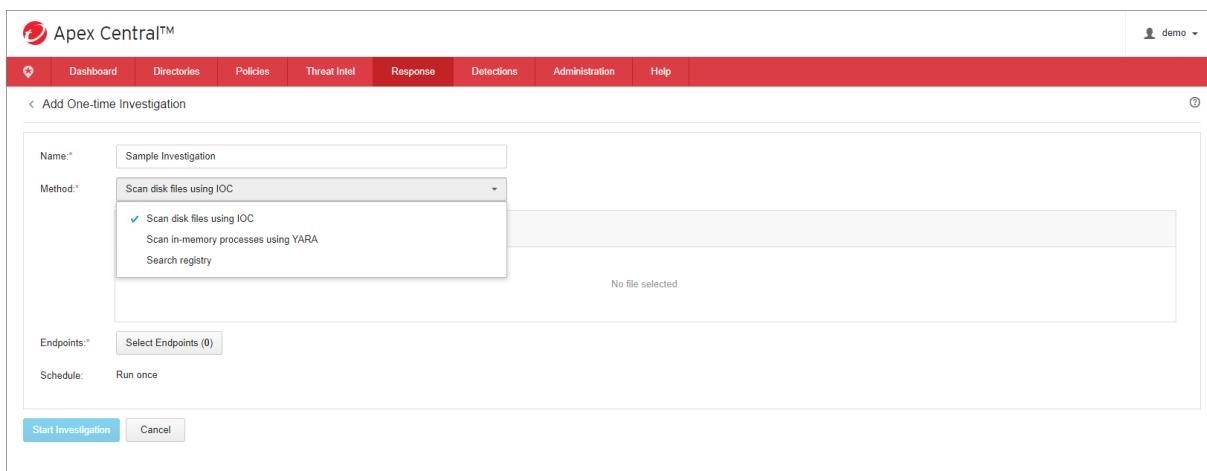
A Detailed Investigation can be run once or can be scheduled to run regularly using a set of similar settings. The average Detailed Investigation run time is about 40 min (Security Agent polling occurs every 10 minutes, the Detailed Investigation task and data upload takes about 20 to 30 minutes). The Polling interval can be reduced from Apex One Server by clicking **Agents > Global Agent Settings > Server Polling Interval**.

To begin a Detailed Investigation, click **Response > Detailed Investigation**.



The screenshot shows the Apex Central interface with the 'Response' tab selected. Under 'Real-Time Investigation', the 'One Time Investigation' tab is active. A table below shows no data with the following columns: Status, Progress, Name, Method, Criteria, Matched Endpoints, Target Endpoints, Started, Elapsed, and Creator. Buttons for '+ New Investigation', 'Stop', and 'Delete' are also present.

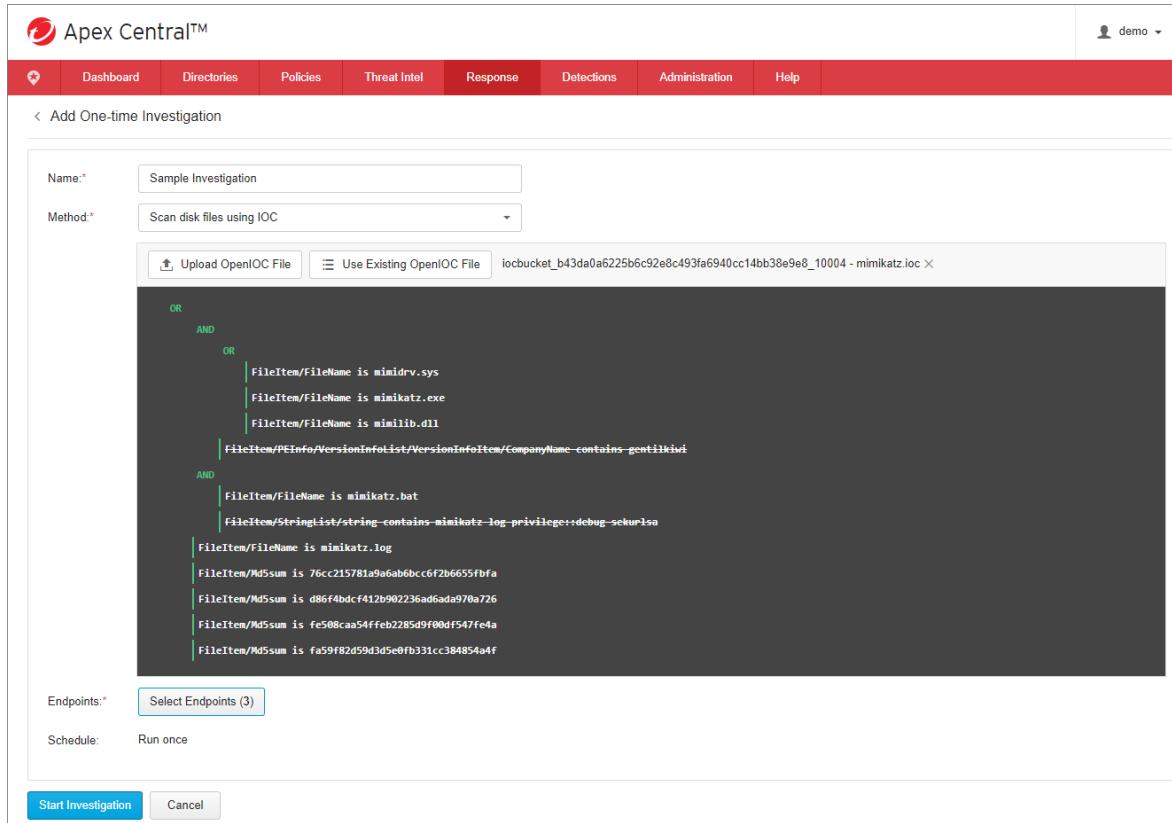
Click either the **One-Time Investigation** or **Scheduled Investigation** tabs and click **New Investigation**. Type a **Name**, select a Method and click **Select Endpoints** to identify the endpoint on which to run the investigation.



The screenshot shows the 'Add One-time Investigation' dialog. It includes fields for 'Name' (Sample Investigation), 'Method' (Scan disk files using IOC), 'Endpoints' (Select Endpoints (0)), and 'Schedule' (Run once). A dropdown menu for 'Method' lists 'Scan disk files using IOC', 'Scan in-memory processes using YARA', and 'Search registry'. Buttons for 'Start Investigation' and 'Cancel' are at the bottom.

Scan Disk Using OpenIOC

This option will scan files on the hard disk using OpenIOC 1.0 rules or repository rules to scan for all files currently on the disk. Click **Upload OpenIOC file** to import an OpenIOC file acquired from another source, or click **Use Existing OpenIOC file** to use a file provided by Trend Micro. Click **Select Endpoint** to identify the endpoints on which the investigation will be run.



The screenshot shows the 'Add One-time Investigation' page in the Apex Central interface. The 'Method' dropdown is set to 'Scan disk files using IOC'. The 'OpenIOC File' section displays a complex query:

```
OR
AND
OR
| FileItem/FileName is mimidrv.sys
| FileItem/FileName is mimikatz.exe
| FileItem/FileName is mimilib.dll
| FileItem/PEInfo/VersionInfoList/VersionInfoItem/CompanyName contains gentilkiwi
AND
| FileItem/FileName is mimikatz.bat
| FileItem/StringList/string contains mimikatz-log-privilege::debug_sekuRSA
| FileItem/FileName is mimikatz.log
| FileItem/Md5sum is 76cc215781a9a6ab6bccf6f2b6655fbfa
| FileItem/Md5sum is d86f4bdcf412b902236ad6ada970a726
| FileItem/Md5sum is fe508caa54ffeb2285d9f00df547fe4a
| FileItem/Md5sum is fa59f82d59d3d5e0fb331cc384854a4f
```

The 'Endpoints' field shows 'Select Endpoints (3)'. The 'Schedule' field is set to 'Run once'. At the bottom are 'Start Investigation' and 'Cancel' buttons.

Only one OpenIOC file can be used by the task and all conditions within OpenIOC file will be handled as OR (any of the criteria).

Click **Start Investigation**. A progress bar is displayed as the investigation proceeds.

The screenshot shows the Apex Central web interface. At the top, there's a navigation bar with links like Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. The user is logged in as 'demo'. Below the navigation is a section titled 'Detailed Investigation' with tabs for 'One Time Investigation' and 'Scheduled Investigation'. Under 'One Time Investigation', there's a button for '+ New Investigation'. The main area displays a table of investigations:

Status	Progress	Name	Method	Criteria	Matched Endpoints	Target Endpoints	Started	Elapsed	Creator
<input type="checkbox"/> Processing	<div style="width: 50%;">50%</div>	Sample Investigation	OpenIOC rule	iocbucket_b43da0a6225b6...	0	3	2019/04/08 15:40:30	(00:03:08)	demo
<input type="checkbox"/> Completed	100%	test	OpenIOC rule	BA6F3FB1F053CEAE83E...	0	3	2018/11/22 10:49:23	00:01:02	demo
<input type="checkbox"/> Completed	100%	test	YARA rule	test.yara.txt	0	3	2018/11/22 10:31:42	00:14:08	demo

At the bottom right of the table, there are pagination controls: 'Records: 1-10 / 10 per page ▲ 1 / 1 < >'.

The following indicators of compromise items and conditions are supported for Detailed Investigations.

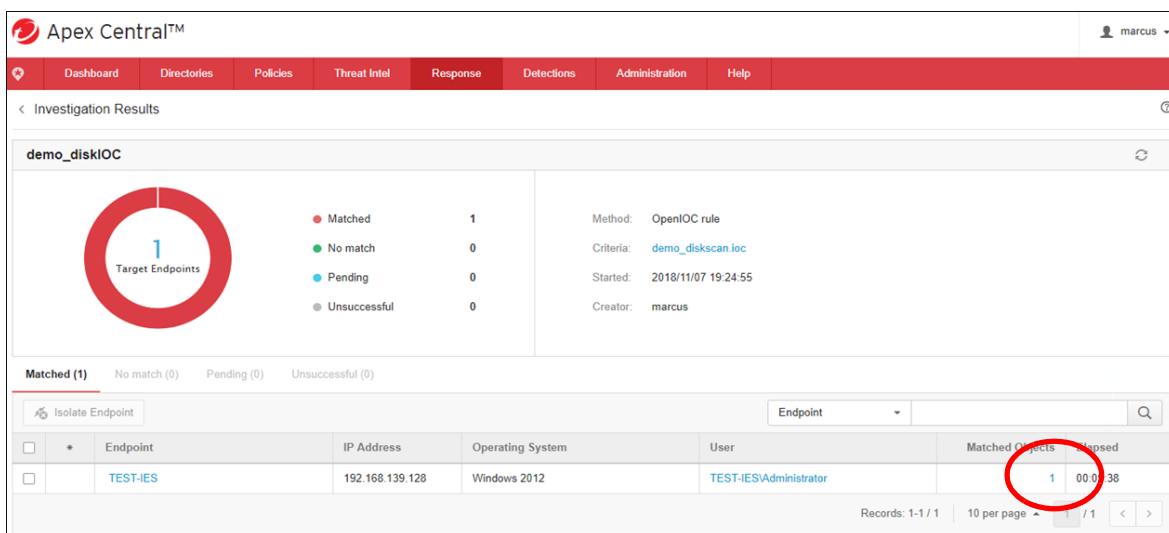
	Is	Contains	Starts-with	End-with	Greater-than	Less-than
fileitem/filepath	✓	✓	✓	✓		
fileitem/fullpath	✓					
fileitem/filename	✓	✓	✓	✓		
fileitem/md5sum	✓					
fileitem/sha1sum	✓					
fileitem/sha256sum	✓					
fileitem/sizeinbytes	✓				✓	✓
fileitem/created					✓	✓
fileitem/modified					✓	✓
fileitem/accessed					✓	✓

Certain limitations exist for **Scan disk files using IOC**, including:

- A hash is not generated for file larger than 64 MB
- Large files can't be checked by hash with OpenIOC
- Time format must be in the following UTC format yyyy-mm-ddThh:mm:ss to check on Fileitem/Created-modified-accessed.
- Apex One can only use a maximum of 100 indicator items, and max 50 for depth
- Search runs upon 10k files as limit
- Searches must be specific (directory as example)
- Search returns a maximum of 1000 items matched
- Search is not related to number of endpoints
- Unsupported items and conditions won't be used for the investigation task, and will be shown as strikethrough.

Lesson 18: Detecting and Investigating Security Incidents on Endpoint Computers

All endpoints that matched the OpenIOC file will appear on the **Matched** tab.



The screenshot shows the Apex Central interface with the following details:

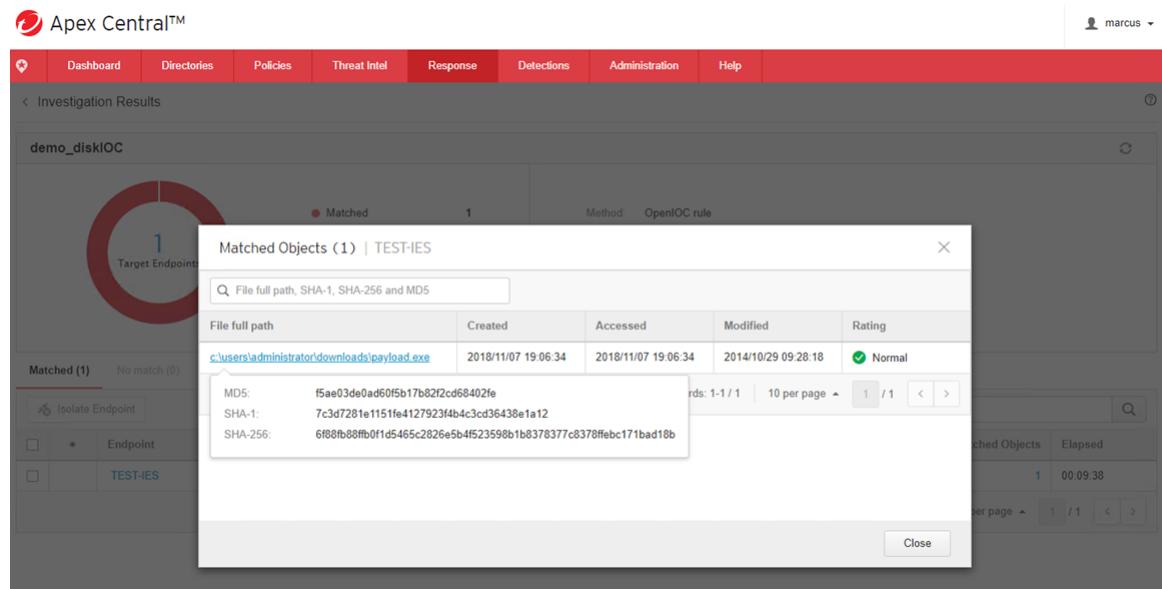
- Investigation Results:** demo_diskIOC
- Target Endpoints:** 1
- Statistics:**
 - Matched: 1
 - No match: 0
 - Pending: 0
 - Unsuccessful: 0
- Method:** OpenIOC rule
- Criteria:** demo_diskscan.loc
- Started:** 2018/11/07 19:24:55
- Creator:** marcus

A red circle highlights the 'Matched' status in the statistics section. Below the statistics, there is a table showing the matched endpoint details:

Endpoint	IP Address	Operating System	User	Matched Objects	Elapsed
TEST-IES	192.168.139.128	Windows 2012	TEST-IES\Administrator	1	00:09:38

Records: 1-1 / 1 | 10 per page | 1 / 1

Click the item for further details.



The screenshot shows the Apex Central interface with the following details:

- Investigation Results:** demo_diskIOC
- Target Endpoints:** 1
- Method:** OpenIOC rule

A red circle highlights the 'Matched Objects' link in the main navigation area. A modal window titled 'Matched Objects (1) | TEST-IES' is displayed, showing the following details:

File full path	Created	Accessed	Modified	Rating
c:\users\administrator\downloads\payload.exe	2018/11/07 19:06:34	2018/11/07 19:06:34	2014/10/29 09:28:18	Normal

MD5: f5ae03de0ad60f5b17b82f2cd68402fe
SHA-1: 7c3d7281e1151fe4127923f4b4c3cd36438e1a12
SHA-256: 6f88fb88ffbf0fd5465c2826e5b4f52359861b8378377c8378ffebc171bad18b

Records: 1-1 / 1 | 10 per page | 1 / 1

Scan In-Memory Processes Using YARA Rules

This option uses YARA rules to scan all processes currently running in memory. YARA rules allows a scan on running processes that contains strings that are identified. This can be used in situation where hash values can not be used as a criteria for investigation.

The screenshot shows the Apex Central web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. A user icon labeled 'demo' is also present. Below the navigation bar, the main content area has a title 'Add One-time Investigation'. Under this, there are fields for 'Name:' (set to 'Sample YARA') and 'Method:' (set to 'Scan in-memory processes using YARA'). A large text area displays a YARA rule file:

```

rule skeleton_key_patcher
{
    strings:
        $target_process = "lsass.exe" wide
        $dll1 = "crypt.dll"
        $dll2 = "samsvr.dll"

        $name = "HookDC.dll"

        $patched1 = "CDLocateCSystem"
        $patched2 = "SamIRetrievePrimaryCredentials"
        $patched3 = "SamIRetrieveMultiplePrimaryCredentials"

    condition:
        all of them
}

rule skeleton_key_injected_code
{
    strings:
}

```

Below the YARA code, there are sections for 'Endpoints:' (with a button to 'Select Endpoints (3)') and 'Schedule:' (set to 'Run once'). At the bottom of the form are two buttons: 'Start Investigation' (in blue) and 'Cancel'.

YARA rule files can be imported or selected from the repository. Only one YARA file can be used per task.

YARA rules are the only Detailed Investigation method that provides Root Cause Analysis data. Because Detailed Investigations run on the current system state, some files and registry entries may be locked or in use during this period.

All endpoints that match the YARA Rule file will appear on the **Matched** tab.

The screenshot shows the 'Investigation Results' page for a YARA rule named 'demo_yara'. The main summary indicates 1 Target Endpoint, 1 Matched, 0 No match, 0 Pending, and 0 Unsuccessful. The method is 'YARA rule' and the criteria is 'putty.yara'. The task was started on 2018/11/06 at 12:51:45 by user marcus. Below this, a table lists the matched endpoint details. The 'Root Cause Analysis' column for the single match contains a blue 'View' link, which is circled in red.

Matched (1)							
		No match (0)	Pending (0)	Unsuccessful (0)	Endpoint		
<input type="checkbox"/>	*	Endpoint	IP Address	Operating System	User	Matched Objects	Root Cause Analysis
		TEST-IES	192.168.139.128	Windows 2012	TEST-IES\Administrator	1	View

Click **View** in the Root Cause Analysis column to view the Analysis Chain graph.

The screenshot shows the 'Analysis Chains' section for the matched endpoint. It displays four main objects: 'Target Endpoint' (TEST-IES), 'First Observed Object' (cmd.exe), 'Matched Objects (1)' (putty.exe), and 'Noteworthy Objects' (0). Below this, a graph titled 'Root Cause Analysis' shows the flow from 'System' to 'cmd.exe' to 'putty.exe' to 'Explorer.EXE'.

```

graph LR
    System --> cmd[cmd.exe]
    cmd --> putty[putty.exe]
    putty --> explorer[Explorer.EXE]
  
```

Search Registry

This method uses manually defined settings to search the Windows Registry for the system current state. Define criteria with key (path), (key) name and value. Multiple items can be set and will be handled as an OR operation

The screenshot shows the 'Add Scheduled Investigation' page in the Apex Central interface. The 'Method' dropdown is set to 'Search registry' (circled in red). Below it is a table for defining search criteria, which is currently empty. At the bottom are 'Start Investigation' and 'Cancel' buttons.

Registry root key available for live scanning include:

- HKEY_CURRENT_USER
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS

Note: HKEY_CURRENT_CONFIG root key can't be scanned

All endpoints that match the Registry criteria will appear on the **Matched** tab.

The screenshot shows the 'check reg' tool interface. It displays a summary table with 1 Matched endpoint and 0 others. The 'Method' is listed as 'Registry search' (circled in red). Below is a table of matched endpoints, showing 1 result for FRLAB-ENDPOINTA. At the bottom are pagination controls.

Endpoint	IP Address	Operating System	User	Matched Objects	Elapsed
FRLAB-ENDPOINTA	192.168.200.15	Windows 10	FRLAB-ENDPOINTA\admin	1	00:02:28

Viewing Detailed Investigation Results

Investigation results are displayed in the **Detailed Investigation** windows. Previous results are retained for the time period allowed by the software license. Tasks can be stopped (under processing) or deleted.

Status	Progress	Name	Method	Criteria	Matched Endpoints	Target Endpoints	Started	Elapsed	Creator
<input checked="" type="checkbox"/> Processing	40%	ps_exec	OpenIOC rule	psexec.ioc	1	10	2019/01/25 10:52:25	(0:31:29)	osces_eas...
<input type="checkbox"/>	Completed	jesp_test	YARA rule	jesp.yar	1	1	2019/01/23 10:57:50	00:10:58	osces_eas...
<input type="checkbox"/>	Completed	No Psexec	YARA rule	antidebug_antimv.yar	1	1	2018/12/28 17:22:03	00:18:57	osces_eas...
<input type="checkbox"/>	Stopped	yara - powershell	YARA rule	check_suspicious_upload_...	0	2	2018/12/06 20:45:52	00:00:00	osces_eas...
<input type="checkbox"/>	Completed	loc_putty	OpenIOC rule	demo_diskscan - putty.ioc	0	2	2018/11/30 12:11:32	00:06:29	osces_eas...
<input type="checkbox"/>	Completed	check_autologon_frlab	Registry search	View	1	1	2018/11/29 15:34:03	00:01:19	osces_eas...
<input type="checkbox"/>	Completed	checkreg_autologon	Registry search	View	0	5	2018/11/29 15:10:02	1 day,00:00:18	osces_eas...
<input type="checkbox"/>	Completed	scan_registry_userinit	Registry search	View	0	5	2018/11/29 14:59:55	1 day,00:00:25	osces_eas...
<input type="checkbox"/>	Completed	Check SVCHOST run with Y...	YARA rule	test_svchost.yara	5	5	2018/11/27 11:37:48	23:52:48	osces_eas...

Attack Discovery

Attack Discovery uses an Indicator of Attack-based detection engine. This mechanism focuses on the detection of the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in an attack.

Attack Discovery behavior is based on the given Attack Discovery Engine (ADE) rules. The Attack Discovery Engine detection log could be a starting point of the investigation.

Viewing the Attack Discovery Engine Log

In Apex Central, click **Detections > Logs > Log Query**. Select **Attack Discovery Detections** from the list.

Generated	Received	Endpoint	Product	Managing Server E	Product Version	Endpoint IP	Risk Level	Pattern Version
No data to display								

Managed Detection and Response Service

Despite putting sophisticated threat detection techniques in place, there are still some advanced targeted attacks that can bypass traditional defenses.

Some of the approaches used to detect these advanced threats include:

- **Network Discovery:** Products like Deep Discovery Inspector are available to monitor the network on multiple protocols looking for Command & Control behavior and detecting lateral movement of threats. These tools also incorporate virtual sandboxing technology for definitive identification of advanced threats.
Network Discovery tools can sometimes be very complex to work with, and can generate a large number of alerts which could require investigation. Also, network tools can't identify threats at the point of entry.
- **Endpoint Detection and Response:** Detailed system activity can be recorded on the endpoint and threat investigators can query the endpoint searching for Indicators of Attack (IOA) or Indicators of Compromise (IOC). Advanced detection techniques implemented on the endpoint computer such as behavior analysis and predictive machine learning can identify emerging or unknown threats.

These approaches require well trained researchers with strong skills to deconstruct the attack and identify the correct indicators of attack. This investigation process can be very complex, time consuming and expensive. A large number of alerts detected on the network and endpoint can lead to alert fatigue and important details can be overlooked in the rush to investigate every activity that is occurring. The number of endpoints that need to be dealt with, including servers, endpoint computer and IoT devices further complicates the process. Once the threats have been identified, a mitigation plan must be devised and implemented to protect the environment from any further attack. And finally, a skill shortage in the industry can make it difficult for organizations to recruit researchers with the appropriate skill set.

All of this drives the need for a managed detection and response solution.

Trend Micro Managed XDR for Users

Trend Micro has introduced a new line of attack to deal with advanced threat detection and mitigation through its Managed XDR for Users service.

Advanced automation mechanisms available through Trend Micro's Security Operation Centers (SOC) can assist in correlating all alerts coming into our customers systems and prioritizing them.

Advanced Artificial Intelligence (AI) techniques can help reduce the number of manual investigations required to develop an appropriate mitigation scheme.

Once the prioritized list of alerts has been compiled, Trend Micro staff in the Security Operation Centers will be able to assist organizations that don't have incident response staff to complete a detailed investigation of threat and provide the steps needed to deal with the threat.



Trend Micro Managed XDR for Users includes three components:

- **Detection:** Since the Security Operation Center has the ability to correlate threats and events occurring on the network with threats occurring on the endpoint, they can get a better view into the advanced threats penetrating the organization and improve the detection of these threats. In addition, if Trend Micro obtains Indicator of Compromise information from a detected threat on another customer or from a third party, Trend Micro can sweep across all of the customer's device as well as all other Managed Detection and Response Service customers to insure that none of the indicators are in place.
- **Analysis:** Trend Micro Security Operation Center personnel will investigate and perform a deep dive to validate alerts, build a detailed threat analysis and create an impact report including a root cause analysis to identify how threats got into the network, where they first manifested themselves, how the threats may have changed over time, how it spread through the network and to how many users many be affected.
- **Response:** Security analysts in the Security Operation Center generate a report based on the root cause analysis, and provide a mitigation plan which includes recommendations on how to clean the affected devices, and in some cases, provide the damage cleanup tools that can assist in the process.

Service Components

The Trend Micro Managed XDR for Users is made up of three components.



- **Sensors:** Customers put the appropriate sensors in place to record system behavior and activities and forward metadata about these activities to the service. On the endpoint computer, Trend Micro Endpoint Sensor and Apex One will be used. Deep Discovery Inspector on the network will record similar metadata and send it to the service, and Deep Security will do the same for servers.
- **Threat Investigation Center:** The Threat Investigation Center at a centralized-managed Trend Micro Security Operation Center will take advantage of Trend Micro threat intelligence information, rules, machine learning, and artificial intelligence to correlate what is happening on an endpoint with what is happening on the network to identify prioritized alert situations.
- **Response:** Trend Micro analysts examine the alert details, perform a deep investigation and provide a response directly to Apex Central with the full plan to mitigate against the attack.

Managed Service Flow

As an example, a user downloads an infected file that was able to take over a remote PC through a Powershell script and compromise an IoT device.

Protection on the Endpoint identifies that this end user has been compromised. At the same time, Deep Discovery Inspector identifies Command & Control behavior. Taking these two events together, if the infected PC attempts to access that C&C server, a correlation can be established and a bigger picture around the advanced attack can be drawn.

Advanced detection techniques identify the relationship between the alerts and prioritize that this is something worth investigating. An Alert can be forwarded to the end user asking for approval to proceed with the investigation and the analysts performs an impact analysis.

The Trend Micro analysts identify the threat, identify the risk and impact, identify if anything else was downloaded and determine whether that target has been breached. The analyst proceeds with a root cause analysis that allows them to understand the story of the attack and develop a plan to mitigate it.

A report is compiled to provide all the information about attack, recommendations on how to mitigate the threat and in some cases, which tools can be provided to deal with its remediation.

The end customer is then responsible for the threat remediation which can include killing certain processes, re-imaging the endpoint, or implementing a pattern update.

The Threat Investigation Center will then build an Indicator of Compromise that will allow them to easily repeat the identification of the threat and continually monitor for same type of attack in the same customer's environment and on other Managed Detection and Response Service customers.

Customers are provided with a full report on each incident that detail response and remediation to the threat. Monthly and quarterly reports are also provided to the organization's management to re-inform the value provided through the service and provide specific actions and recommendations to improve their security posture.

Managed Detection and Response Service focuses on Detection, Analysis and Response; the customer or partner is responsible for Remediation.

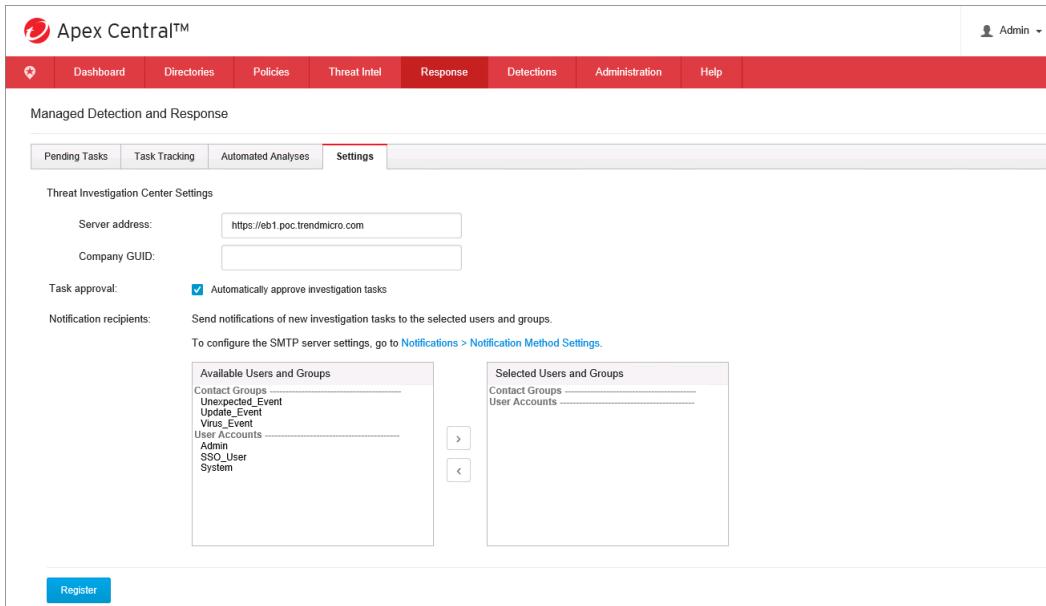


Configuring Apex Central for Managed XDR for Users

When a customer subscribes to the Managed Detection and Response service from Trend Micro, the details of the Threat Investigation Centre and the organization's unique ID must be provided.

- 1 Open the Apex Central Web Management console, and click **Response > Managed Detection and Response**.

2 Click the **Settings** tab and complete the details:



The screenshot shows the 'Managed Detection and Response' section of the Apex Central interface. The 'Settings' tab is selected in the navigation bar. Under 'Threat Investigation Center Settings', there are fields for 'Server address' (set to <https://eb1.poc.trendmicro.com>) and 'Company GUID'. A checkbox for 'Task approval' is checked, labeled 'Automatically approve investigation tasks'. A note says 'Send notifications of new investigation tasks to the selected users and groups.' Below this is a link to 'Notifications > Notification Method Settings'. On the left, a list of 'Available Users and Groups' includes Contact Groups, UserEvent_Event, Userfile_Event, Virus_Event, and User Accounts (Admin, SSO_User, System). On the right, a list of 'Selected Users and Groups' shows Contact Groups and User Accounts. Between them are two buttons: a right-pointing arrow and a left-pointing arrow.

- **Server address:** Type the HTTPS log server address of Threat Investigation Center, as provided by Trend Micro
- **Company GUID:** Type your unique company ID, as provided by Trend Micro
- **Task approval:** enable this setting to allow the Trend Micro Threat Investigation Center to initiate investigations without requiring approval from the customer
- **Notification recipients:** If automatic approval for investigations is not enabled, identify the users or groups to be queried for approval to allow the Trend Micro Threat Investigation Center to proceed with the investigation

Click **Register**.

Note: Apex Central sends detections to the Threat Investigation Center every 5 minutes.

Optional Lesson: Migrating to Apex One as a Service

Lesson Objectives:

After completing this lesson, participants will be able to:

- Migrate an on-premises installation Apex One to Apex One as a Service

Trend Micro Apex One as a Service provides an alternative to a standard on-premises software installation where the organization is responsible for building the servers, installing the applications, and configuring them. In Apex One as Service, the application servers reside on a remote cloud instance managed by Trend Micro and accessed by the customer through the Web or an API. Customers subscribe to the service and have the authorization to use it for a period of time.

Benefits of Apex One as a Service

Apex One as a Service provides benefits over an on-premises installation of Apex One, including the following:

Ease of Deployment

Apex One as a Service differs from a traditional on-premises software installation in that the application is already installed and configured. An organization provisions an instance of the service in the cloud, and in minutes, has Apex One ready for use. In addition, Apex One as a Service launches using best practices as determined by Trend Micro. This reduces the time spent on installing and configuring the application.

Reduced Costs

Apex One as a Service provide beneficial cost savings as it resides in a shared environment, where the hardware and software license costs are lower than a comparable on-premises installation. This allows small and medium businesses to use a software that otherwise would be prohibitive due to the high cost of licensing. Maintenance costs are reduced since Trend Micro owns the environment and costs are split among all customers that use the service. The subscription-based model used by Trend Micro Apex One as a Service protects the organization from the financial risk of expensive software.

Up-to-date Features

With Apex One as a Service, customers benefit from the most up-to-date feature set as Trend Micro applies regular upgrades which become immediately available to customers. The cost and effort associated with upgrades and new releases are lower than an on-premises installation where the organization may be required to pay for an upgrade and install it themselves. Customers are also protected from regular operating system upgrade requirements.

Simplified Maintenance

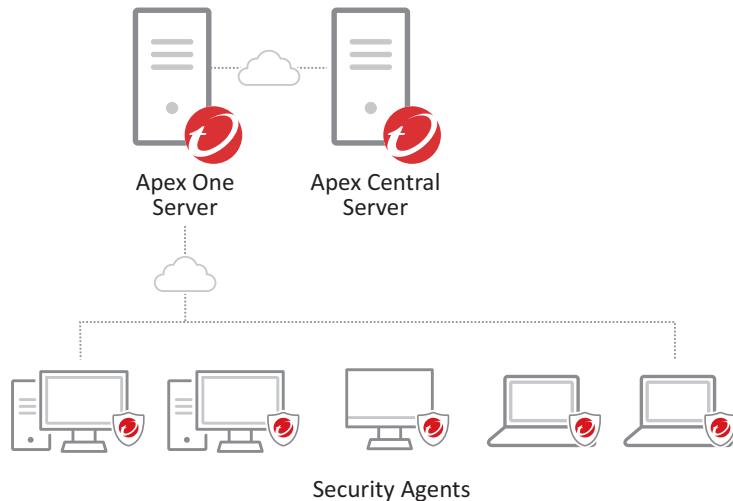
Trend Micro applies regular maintenance fixes and updates to the service. By eliminating problems like software maintenance and incompatibility, Trend Micro Apex One as a Service can provide streamlined focus and greater productivity.

Enhanced Security

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. Trend Micro insures that all the latest patterns and filters are used.

Apex One as a Service Servers

Apex One as a Service uses two server components to deliver its functionality.



Apex Central Server

The Apex Central Server is responsible for the following operations as part of the service:

- **Policy management:** System administrators use Apex Central to configure and deploy security settings to managed products and endpoints through policies. Using a single management console ensures consistent enforcement of your organization's virus/malware and content security policies.

- **Visibility across managed products:** Dashboard tabs and widgets provide extensive visibility of managed products and information about threat detections, component statuses, policy violations, and more.
- **User/Endpoint Directory:** View detailed information about all the users and endpoints within Apex Central registered products.
- **Logs:** Apex Central consolidates logs from all registered products without having to log on to each individual product console.
- **Event notifications:** Administrators are informed of network events at all times by configuring Apex Central to send email notifications.
- **Reports:** Reports from Apex Central provides actionable information you need to ensure network protection and security compliance.
- **Component updates:** Apex Central securely downloads and deploys antivirus patterns, rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date.
- **Connected Threat Defense:** Apex Central brings together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage.
- **Role-based administration:** Grant and control access to the Apex Central Web Management console by assigning specific privileges to administrators and providing only the tools and permissions necessary to perform specific tasks.
- **Command tracking:** Command tracking allows you to continuously monitor whether commands executed in Apex Central, such as anti-virus pattern updates and component deployment, have successfully completed.
- **License management:** Deploy new Activation Codes or reactivate existing Activation Codes on managed products.
- **Threat investigation:** Integration with Endpoint Sensor monitors, records, and performs both current and historical security investigations on your Apex One endpoints. Use the Apex Central console and perform preliminary investigations to locate at-risk endpoints before executing an in-depth Root Cause Analysis to identify the attack vectors.
- **Security Agent installation:** Download installation packages for Security Agents directly from the Apex Central console.

Apex One Server

The Apex One Server is responsible for the following operations as part of the service:

- **Security risk protection:** Apex One protects computers from security risks through a collection of techniques, including virus and spyware scanning, behavior monitoring, predictive machine learning, Connected Threat Defense, Web reputation, data loss prevention and more.
- **Firewall:** The Apex One Firewall protects endpoints and servers on the network using stateful inspections. Create rules in Apex One to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.
- **Global Agent settings:** Global agent settings apply to all agents that report to the Apex One as a Service server.

Logging into the Apex One as a Service

The credentials used by the default administrator, including account name and password, are assigned during the service account setup process.

In the address bar of a supported Web browser, type the URL provided by Trend Micro in your service activation confirmation email to directly access the Apex Central Web Management console. Alternately, type the following URL to access the **Sign in** page:

<https://manage.trendmicro.com>

The screenshot shows the login interface for Trend Micro's Apex Central as a Service. At the top left is the Trend Micro logo. To its right, the text "Apex Central™ as a Service" is displayed. Below this, there is a large banner featuring a globe and the text "Maximum Trend Micro™ XGen™ security from your proven security partner". On the right side of the page is a "Sign In" form. It includes fields for "Trend Micro Account" (with a placeholder "Enter account name") and "Password" (with a placeholder "Enter password"). Below these fields are links for "Forgot your password?" and "Forgot my account?". A "Remember me" checkbox is checked. A red "Sign In" button is located below the form. At the bottom of the page, there is a copyright notice: "Copyright © 2020 Trend Micro Incorporated. All rights reserved." followed by links to "Trend Micro", "Legal Policies & Privacy", "Contact Us", and "Help".

When prompted, type your **Trend Micro Account** name (the Logon ID you provided when you registered for the service account) and **Password** and click **Sign In**.

The Apex Central as a Service Web Management console is displayed.

Critical Threats

Last refresh: 03/17/2021 13:18:56
03/11/2021 ~ 03/17/2021

Range: Last 7 days

0 critical threat types

Threat Type	Important Users	Other Users
Ransomware	0	0
Known Advanced Persistent Threat (APT)	0	0
Social engineering attack	0	0
Vulnerability attack	0	0
Lateral movement	0	0
Unknown threats	0	0
C&C callback	0	0

Ransomware Prevention

Last refreshed: 03/17/2021 13:18:56
03/11/2021 - 03/17/2021

Period: Last 7 days

Trend Micro can block ransomware threats at every stage of an attack. [Learn More](#)

Exposure Layer

- Messages: 0
- Websites: 0
- Network Traffic: 0
- Cloud Sync: 0

Infection Layer

- Files: 0
- Behaviors: 0

Users with Threats

Last refresh: 03/17/2021 13:18:59
03/11/2021 ~ 03/17/2021

Range: Last 7 days

0 Important Users 0 Other Users

User Name	Department	Threats	Most Critical Threat
No data to display			

Endpoints with Threats

Last refresh: 03/17/2021 13:18:59
03/11/2021 ~ 03/17/2021

Range: Last 7 days

0 Important Endpoints 0 Other Endpoints

Host Name	IP Address	Threats	Most Critical Threat
No data to display			

Apex One as a Service is configured as an Apex Central as a Service managed server during the account setup process. If access to the Apex One Web Management console is required, for example, to configure firewall policies and profiles, access the server from the **Product Servers** list in the Apex Central Web Management console.

In the Apex Central Web Management console, click **Directories > Product Servers**. Both **Apex One as a Service** and **Apex One (Mac) as a Service** are displayed as links in the **Product Servers** list.

Product Servers

Server Type: All

Server	Display Name	Product	Connection Type	Last Report	Virtual Analyzer	Actions
https://ukdy8.manage.trendmicro.com	Apex One (Mac) as a Service	Apex One (Mac) 3.5	Manual	03/17/2021 13:17		Edit
https://ukdy8.manage.trendmicro.com:443/officescan/	Apex One as a Service	Apex One 14.0	Automatic	03/17/2021 10:28		Edit

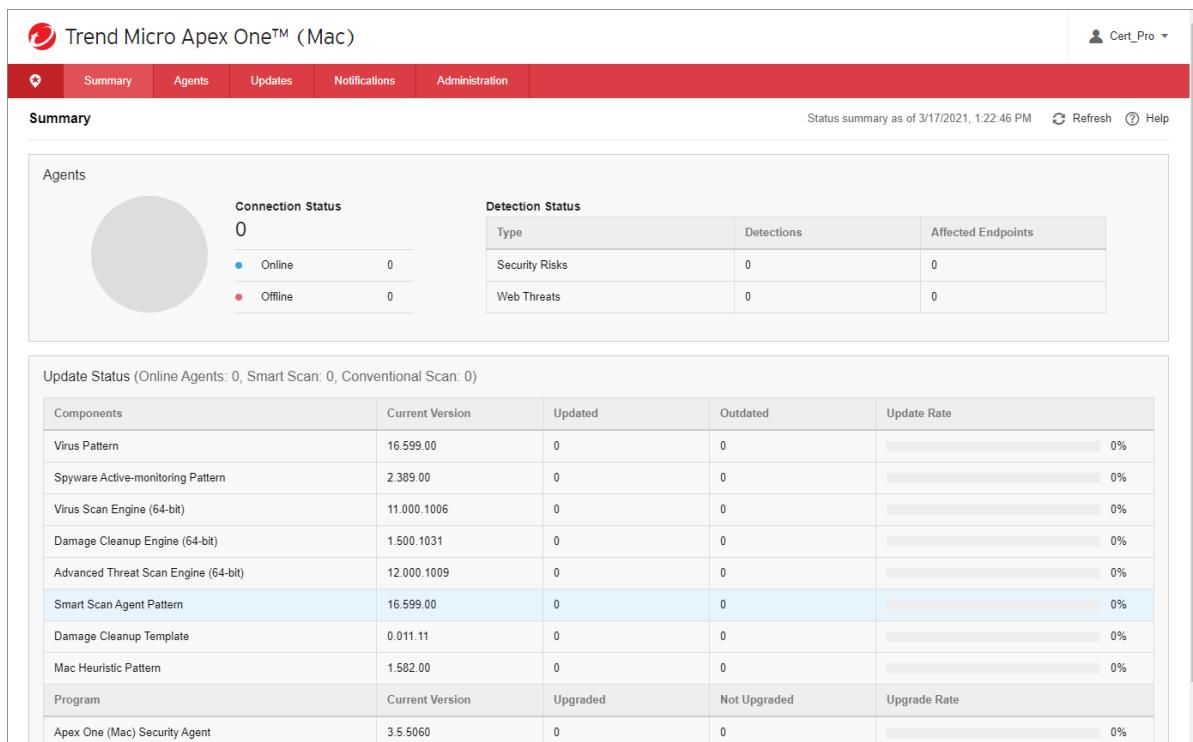
Records: 1 - 2 / 2 | « | < | 1 | > | » | 10 | per page

Optional Lesson: Migrating to Apex One as a Service

Click the link for **Apex One as a Service** to launch the Apex One Web Management console through Single Sign On.

The screenshot shows the Trend Micro Apex One™ web management interface. At the top, there's a navigation bar with links for Dashboard, Agents, Logs, Updates, Administration, and Help. The user is logged in as 'cert_pro'. The main area is divided into several sections: 'Known Threats' (0), 'Unknown Threats' (0), 'Policy Violations' (0); 'Managed Agents' (0), 'Outdated Agents' (0); 'Ransomware Summary' showing 0 attempts across various channels; 'Top Ransomware Detections' with no data displayed; and a 'Security Risk Detections Over Time' section.

Click the **Apex One as a Service (Mac)** link to launch the Apex One (Mac) Web Management console through Single Sign On.



The screenshot shows the Trend Micro Apex One (Mac) web management interface. The top navigation bar includes links for Summary, Agents, Updates, Notifications, and Administration. The user is logged in as 'Cert_Pro'. The 'Summary' tab is active, displaying 'Agents' status (0 agents, 0 online, 0 offline) and 'Detection Status' (0 detections for Security Risks and Web Threats). Below this are sections for 'Update Status' (listing components like Virus Pattern, Spyware Active-monitoring Pattern, etc., with their current versions and update rates) and 'Program' status (listing programs like Mac Heuristic Pattern, Program, and Apex One (Mac) Security Agent with their upgrade status).

Migrating to Apex One as a Service

The steps involved in migrating an on-premises installation of Apex One to Apex One as a Service include the following:

- Integrating the service instance with Active Directory
- Migrating Apex One global and domain settings
- Migrating Apex Central policies
- Moving Agents registered to the on-premises Apex One server to Apex One as a Service
- Creating administrative users in Apex Central as a Service

Integrating Apex Central with a Microsoft Active Directory

Integrating Apex Central with a Microsoft Active Directory server enables the following capabilities:

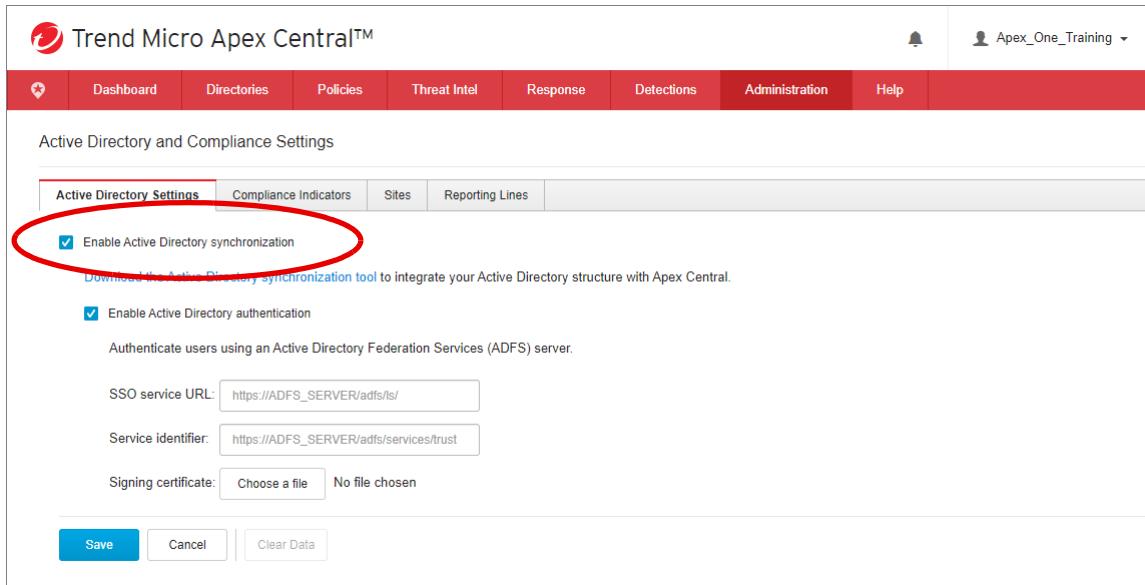
- Allows administrators to create user accounts for Web Management console access, based on Active Directory users or groups.
- Maps the User/Endpoint Directory according to your existing organizational structure and integrate endpoint information (such as threat detections and policy statuses) with Active Directory user information (such as login history and contact details).
- Use the site location and reporting line information in Active Directory to gain greater insight into your network protection status on the Operation Center tab.
- Create user-based application control and device control rules based on Active Directory users and groups.

Syncing With Active Directory

Apex Central supports synchronization with multiple Active Directory forests. Adding an Active Directory domain automatically synchronizes all domains from the same forest.

Optional Lesson: Migrating to Apex One as a Service

In Apex Central as a Service, click **Administration > Settings > Active Directory and Compliance Settings**. Click the **Active Directory Settings** tab and click **Enable Active Directory synchronization**. Click **Save**.



Trend Micro Apex Central™

Apex_One_Training

Dashboard Directories Policies Threat Intel Response Detections Administration Help

Active Directory and Compliance Settings

Active Directory Settings Compliance Indicators Sites Reporting Lines

Enable Active Directory synchronization

[Download the Active Directory synchronization tool](#) to integrate your Active Directory structure with Apex Central.

Enable Active Directory authentication

Authenticate users using an Active Directory Federation Services (ADFS) server.

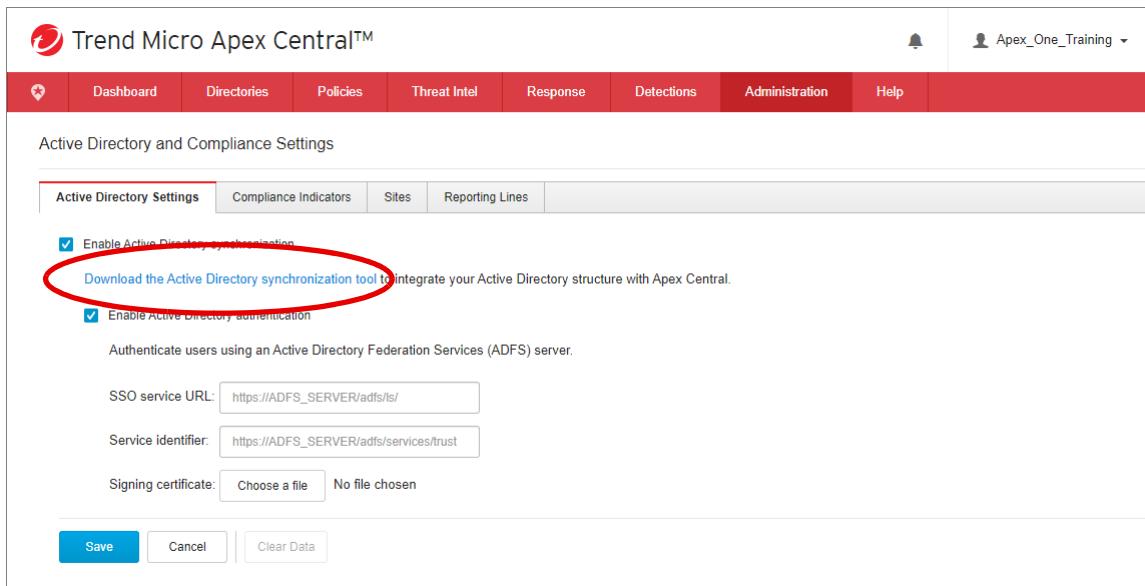
SSO service URL: https://ADFS_SERVER/adfs/ls/

Service identifier: https://ADFS_SERVER/adfs/services/trust

Signing certificate: Choose a file No file chosen

Save Cancel Clear Data

Synchronize endpoint and user information from Active Directory servers by using the Agent synchronization tool. Click **Download the Active Directory synchronization tool** link on the **Active Directory Settings** tab and save the `Apex_Central_ADSyncAgent_*.zip` file.



Trend Micro Apex Central™

Apex_One_Training

Dashboard Directories Policies Threat Intel Response Detections Administration Help

Active Directory and Compliance Settings

Active Directory Settings Compliance Indicators Sites Reporting Lines

Enable Active Directory synchronization

[Download the Active Directory synchronization tool](#) to integrate your Active Directory structure with Apex Central.

Enable Active Directory authentication

Authenticate users using an Active Directory Federation Services (ADFS) server.

SSO service URL: https://ADFS_SERVER/adfs/ls/

Service identifier: https://ADFS_SERVER/adfs/services/trust

Signing certificate: Choose a file No file chosen

Save Cancel Clear Data

Copy the zip file to a folder on the Active Directory server and extract the file.

From a Command Prompt on the Windows Server hosting Active Directory, navigate to the directory which contains the `ADSyncAgentTool.exe` file and execute the following command:

```
ADSyncAgentTool.exe -i
```

```
Administrator: Command Prompt - ADSyncAgentTool.exe -i
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd\temp

C:\temp>ADSyncAgentTool.exe -i
Current executor = TREND\administrator !
Configure Active Directory server settings.
Press any key to start configuration.
Follow the steps to configure Active Directory server settings.
Specify the server FQDN or IP address.
192.168.4.1
Specify the user name (domain\user name).
trend\administrator
Specify the password. Server: 192.168.4.1, User Name: trend\administrator
trendmicro
You configured 1 Active Directory servers.
Press any key to configure more settings.
Press "n" to exit.
n
```

Synchronize the server settings by executing the following command:

```
ADSyncAgentTool.exe -s
```

You may also use Windows Task Scheduler to synchronize configured servers using a scheduled task that has a time interval of at least 2 hours between each task repetition.

Once synchronized, return to **Administration > Settings > Active Directory and Compliance Settings** in the Apex Central Web Management console. On the **Active Directory Settings** tab, the synchronized server information appears.

Active Directory Settings	Compliance Indicators	Sites	Reporting Lines
<input checked="" type="checkbox"/> Enable Active Directory synchronization Download the Active Directory synchronization tool to integrate your Active Directory structure with Apex Central. Server: <input checked="" type="radio"/> 192.168.4.1 Last synchronized: 04/14/2020 11:48:49 <input type="checkbox"/> Enable Active Directory authentication Authenticate users using an Active Directory Federation Services (ADFS) server. SSO service URL: <input type="text" value="https://ADFS_SERVER/adfs/ls/"/> Service identifier: <input type="text" value="https://ADFS_SERVER/adfs/services/trust"/> Signing certificate: <input type="file" value="Choose a file"/> No file chosen <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Clear Data"/>			

Migrating Apex One Global and Domain Settings

To ensure that the global Agent settings in the service instance match what was in the on-premises installation, the Global Agent Settings should be imported into Apex One as a Service.

In addition, any protection settings applied to domains in the on-premises installation should be imported into Apex Central as a Service as policies (one policy for each collection of domain settings).

A settings export tool, downloaded from Apex One as a Service, creates a zip file with the data from the on-premises server. In Apex One as a Service, click **Administration > Settings > Server Migration**. Click **Download Apex One Settings Export Tool**.

The screenshot shows the Trend Micro Apex One web interface. At the top, there's a navigation bar with links for Dashboard, Agents, Logs, Updates, Administration, and Help. The user is logged in as 'migration_training'. Below the navigation bar, the title 'Apex One Server Migration' is displayed. The main content area contains instructions for migrating server settings, mentioning the 'ApexOneSettingsExportTool.zip' file. It includes two steps: running the export tool on the source server and importing it into the target server. A red circle highlights the blue link 'Download Apex One Settings Export Tool'.

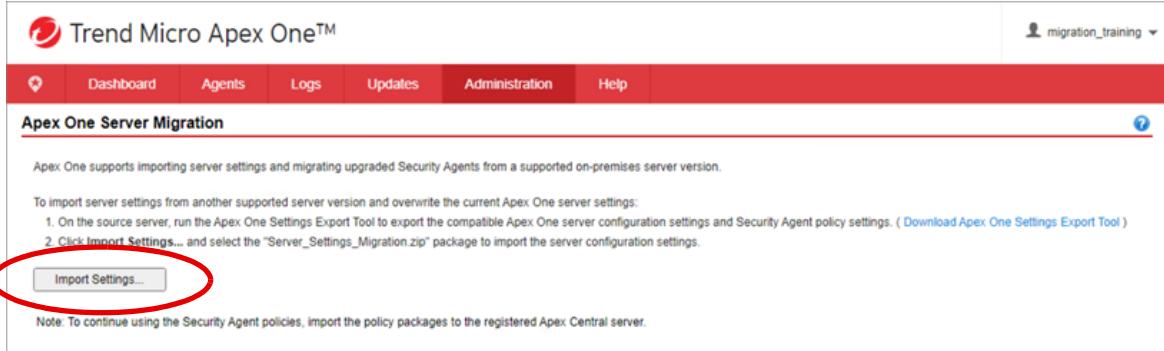
Copy the downloaded `ApexOneSettingsExportTool.zip` to a location on the on-premises Apex One server. Extract the files from the zip file and run `ApexOneSettingsExportTool.exe`.

Three files are created:

- `Server_Settings_Migration.zip`: This file contains Global Agent Settings along with the tree/domain structure used in the on-premises installation.
- `ApexOne_Agent_Policies.zip`: This file contains settings applied to domains in Apex One in a policy format used in Apex Central as a Service.
- `ApexOne_Agent_DLP_Policies.zip`: This file contains DLP settings applied to domains in Apex One in a policy format used in Apex Central as a Service.

Importing Global Agent Settings

In Apex One as a Service, click **Administration > Settings > Server Migration**. Click **Import Settings** and locate the **Server_Settings_Migration.zip** file. The Global Agent Settings from the Apex One server are copied to the Apex One as a Service instance.

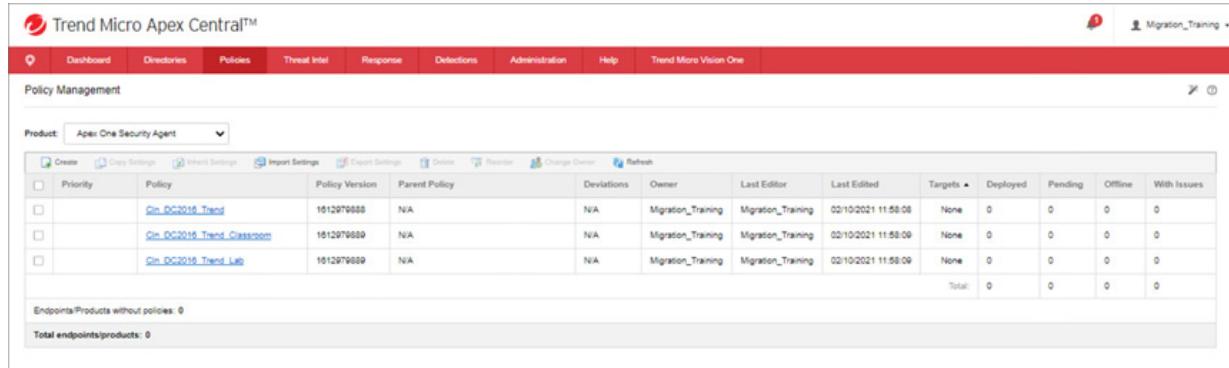


The screenshot shows the 'Apex One Server Migration' interface. At the top, there's a navigation bar with links for Dashboard, Agents, Logs, Updates, Administration, and Help. A user profile 'migration_training' is visible on the right. Below the navigation, a section titled 'Apex One Server Migration' contains instructions: 'Apex One supports importing server settings and migrating upgraded Security Agents from a supported on-premises server version.' It lists two steps: 1. On the source server, run the Apex One Settings Export Tool to export the compatible Apex One server configuration settings and Security Agent policy settings. (Download Apex One Settings Export Tool) 2. Click Import Settings... and select the "Server_Settings_Migration.zip" package to import the server configuration settings. A large red circle highlights the 'Import Settings...' button. A note at the bottom states: 'Note: To continue using the Security Agent policies, import the policy packages to the registered Apex Central server.'

Importing Security Agent Domain Settings

New Security Agent policies will be created that correspond to the settings applied to Agents in the Apex One domains. In Apex Central as a Service, click **Policies > Policy Management**. From the **Product** list, select **Apex One Security Agent**. Click **Import**, locate the **ApexOne_Agent_Policies.zip** file and click **Open**.

A policy for each of the originating domains will be created with the naming format of **CLN_ServerName_DomainName** that represents the settings assigned to the Agents in these domains.

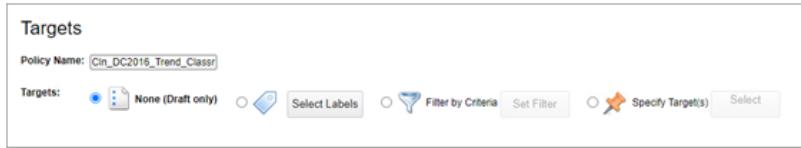


The screenshot shows the 'Policy Management' interface in Trend Micro Apex Central. The top navigation bar includes links for Dashboard, Directories, Policies, Threat Intel, Response, Defects, Administration, Help, and Trend Micro Vision One. A user profile 'Migration_Training' is shown on the right. The main area displays a table of policies under the product 'Apex One Security Agent'. The table columns are: Priority, Policy, Policy Version, Parent Policy, Deviations, Owner, Last Editor, Last Edited, Targets, Deployed, Pending, Offline, and With Issues. Three rows are listed, corresponding to the imported policies: 'Cn_DC2016_Trend' (Priority 1), 'Cn_DC2016_Classroom' (Priority 1), and 'Cn_DC2016_Lab' (Priority 1). At the bottom, status messages indicate 'Endpoints/Products without policies: 0' and 'Total endpoints/products: 9'.

In the example displayed here, the settings from three Apex One domains (Trend, Classroom and Lab) were imported.

Optional Lesson: Migrating to Apex One as a Service

Note: Imported policies will default to the endpoint **Targets of None**. This allows the administrator to review the imported policy and configure the appropriate targets for this policy.



Importing Data Loss Prevention Domain Settings

New Security Agent policies will also be created that correspond to the Data Loss Prevention settings applied to Agents in the Apex One domains. In Apex Central as a Service, click **Policies > Policy Management**. From the **Product** list, select **Data Loss Prevention**. Click **Import**, locate the `ApexOne_Agent_DLP_Policies.zip` file and click **Open**.

New policies will be created that correspond to the Data Loss Prevention settings applied to Agents in the OfficeScan/Apex One domains. A policy for each of the originating domains will be created with the name of `DLP_ServerName_DomainName` that represents the data loss prevention settings assigned to the Agents in these domains.

Priority	Policy	Owner	Last Editor	Targets	Deployed	Pending	Offline	With Issues
<input type="checkbox"/>	DLP_DC2016_Trend	Migration_Training	Migration_Training	None	0	0	0	0
<input type="checkbox"/>	DLP_DC2016_Trend_Classroom	Migration_Training	Migration_Training	None	0	0	0	0
<input type="checkbox"/>	DLP_DC2016_Trend_Lab	Migration_Training	Migration_Training	None	0	0	0	0

Total: 0 0 0 0

Endpoints/Products without policies: 0

Total endpoints/products: 0

Imported Data Loss Prevention policies will default to the endpoint **Targets of None**. This allows the administrator to review the imported policy and configure the appropriate targets for this policy.

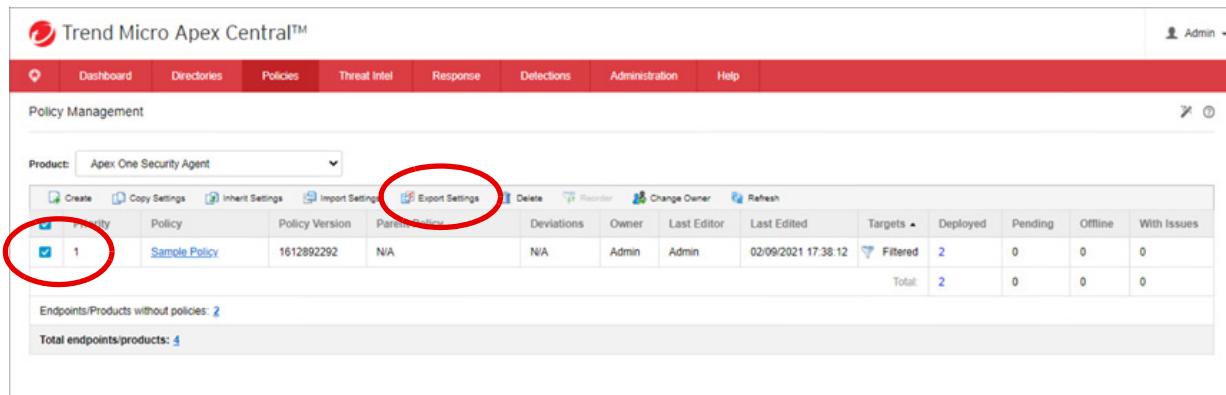


Migrating Apex Central Policies

Policies created and deployed in the on-premises installation of Apex Central must also be transferred to the instance of Apex Central as a Service.

Policies are exported from Apex Central as a *.cmpolicy file. The file is then imported into Apex Central as a Service.

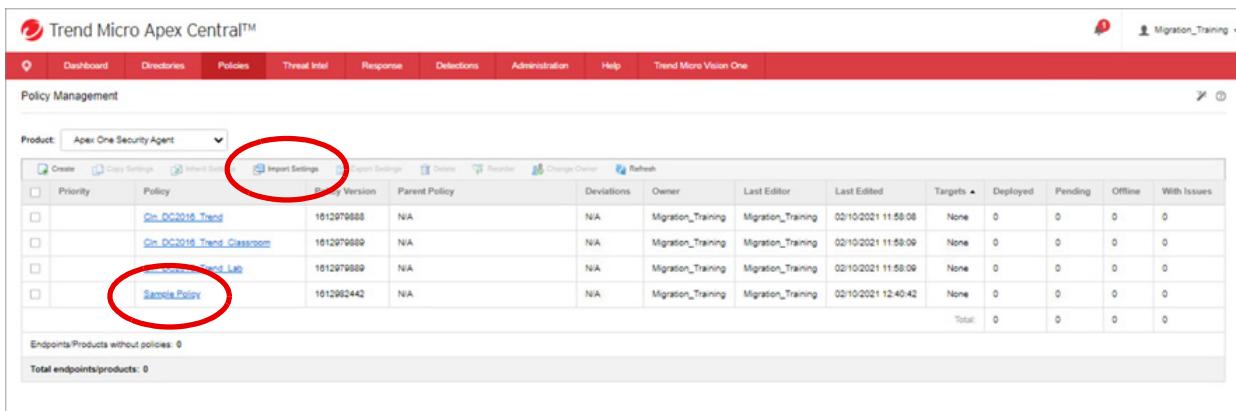
In the on-premises Apex Central server, click **Policies > Policy Management**. From the Product list, select **Apex One Security Agent**. Click to select the policies to export and click **Export Settings**. A *.cmpolicy file containing the policy details is created.



The screenshot shows the Trend Micro Apex Central Policy Management interface. The 'Product' dropdown is set to 'Apex One Security Agent'. A single policy, 'Sample Policy', is selected in the list. Two specific buttons are highlighted with red circles: 'Export Settings' (which has a tooltip 'Exports the selected policies as a .cmpolicy file') and the checkbox next to the policy name ('Sample Policy'). The table below lists various columns such as Priority, Policy, Policy Version, Parent Policy, Deviations, Owner, Last Editor, Last Edited, Targets, Deployed, Pending, Offline, and With Issues. The total count for endpoints/products is 2.

Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
<input checked="" type="checkbox"/>	1 Sample Policy	1612892292	N/A	N/A	Admin	Admin	02/09/2021 17:38:12	Filtered	2	0	0	0

In Apex Central as a Service, click **Policies > Policy Management**. From the Product list, select **Apex One Security Agent**. Click **Import Settings** and locate and open the *.cmpolicy file. Imported policies will default to the endpoint **Targets of None**. This allows the administrator to review the imported policy and configure the appropriate targets for this policy.



The screenshot shows the Trend Micro Apex Central Policy Management interface. The 'Product' dropdown is set to 'Apex One Security Agent'. A single policy, 'Sample Policy', is selected in the list. A red circle highlights the 'Import Settings' button. The table below lists various columns such as Priority, Policy, Policy Version, Parent Policy, Deviations, Owner, Last Editor, Last Edited, Targets, Deployed, Pending, Offline, and With Issues. The total count for endpoints/products is 0.

Priority	Policy	Policy Version	Parent Policy	Deviations	Owner	Last Editor	Last Edited	Targets	Deployed	Pending	Offline	With Issues
<input type="checkbox"/>	Cin DC2016_Trend	1612979888	N/A	N/A	Migration_Training	Migration_Training	02/10/2021 11:58:08	None	0	0	0	0
<input type="checkbox"/>	Cin DC2016_Trend_Classroom	1612979889	N/A	N/A	Migration_Training	Migration_Training	02/10/2021 11:58:09	None	0	0	0	0
<input type="checkbox"/>	Cin DC2016_Trend_Lab	1612979889	N/A	N/A	Migration_Training	Migration_Training	02/10/2021 11:58:09	None	0	0	0	0
<input checked="" type="checkbox"/>	Sample Policy	1612962442	N/A	N/A	Migration_Training	Migration_Training	02/10/2021 12:40:42	None	0	0	0	0

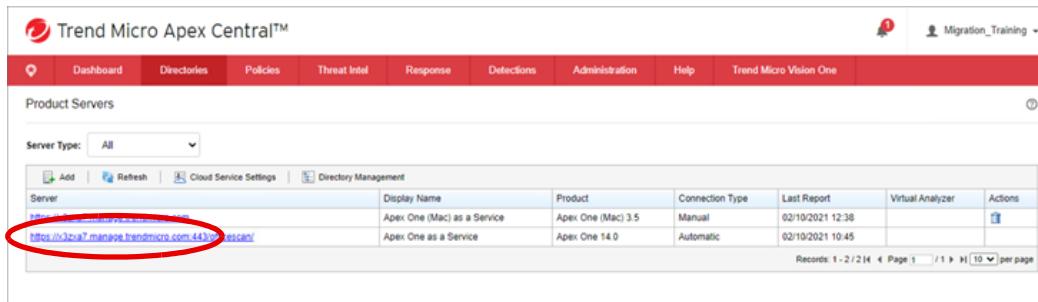
Repeat this process for any **Data Loss Prevention** or **Apex One (Mac)** policies created in the on-premises Apex Central.

Moving Agents Registered to the On-premises Apex OneServer to Apex One as a Service

Apex One Security Agents reporting to an on-premises Apex One server must be redirected to the Apex One as a Service instance. It is not required to uninstall the Agent and reinstall as the move user operation can change the reference to the Apex One server the Agent reports to. Two methods exist to move Agents from one installation to another:

- **Move Agent** operation in the Apex One Web Management console
- Agent Mover Tool

The Apex One as a Service instance name is required to move Agents from the on-premises Apex One server to your service instance. Log into the Apex Central as a Service Web Management console and click **Directories > Product Servers** and record the Apex One as a Service server instance name (for example, xxxxxxx.manage.trendmicro.com).



The screenshot shows the 'Product Servers' section of the Trend Micro Apex Central interface. There are two entries listed:

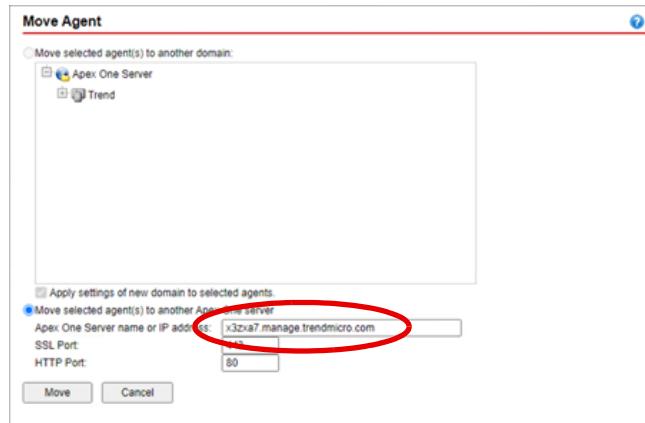
Server	Display Name	Product	Connection Type	Last Report	Virtual Analyzer	Actions
https://x3zx7.manage.trendmicro.com:443/escan/	Apex One (Mac) as a Service	Apex One (Mac) 3.5	Manual	02/10/2021 12:38		
https://x3zx7.manage.trendmicro.com:443/escan/	Apex One as a Service	Apex One 14.0	Automatic	02/10/2021 10:45		

A red circle highlights the URL 'https://x3zx7.manage.trendmicro.com:443/escan/' in the first row.

Move Agent

Log into the on-premises Apex One server and click **Agents > Agent Management**. Click a domain in the left-hand list and select all the Agents in the domain.

Click **Manage Agent Tree > Move Agent**. In the **Move Agent** window, click **Move selected agent(s) to another Apex One server** and type the Apex One as a Service instance name (for example, xxxxxxx.manage.trendmicro.com) with the SSL port of 443 and HTTP port of 80. Click **Move**.



The screenshot shows the 'Move Agent' dialog box. The 'Move selected agent(s) to another Apex One server' radio button is selected. The 'Apex One Server name or IP address:' field contains 'x3zx7.manage.trendmicro.com'. The 'SSL Port:' field is set to '443' and the 'HTTP Port:' field is set to '80'. At the bottom are 'Move' and 'Cancel' buttons.

Note: If you want to copy and paste the Apex One as a Service server instance name into the **Move Agent** window, it is important to highlight the text in the link and copy as opposed to right-clicking the link and selecting **Copy link address**. The latter will copy the URL behind the text which is an Apex Central as a Service redirection link, creating a URL that will cause the operation to fail

In the on-premises Apex One server you will notice the Agents going offline as they are transitioned to Apex One as a Service. After a while, you will notice the Agents disappearing from the Agent Management list in Apex One. The Agents will reappear in the Agent Management list in Apex One as a Service.

Note: There are several factors which could affect the time it takes to move the Agents to the service instance, but typically, it will take about five minutes for the Agents to appear in the Agent Management list in Apex One as a Service.

Return to the on-premise Apex One server and move the Agents in any additional domains.

Agent Mover Tool

The Agent Mover tool (`IpXfer_x64.exe`) can also be used to transfer Security Agents from one Apex One Server to another. The commands available with this tool can be used within scripts to move Agents, or if Agents don't move properly through the Web Management console.

Note: This tool is for moving Agent only and is not used for uninstalling or removing Agents from Apex One.

Both the originating and the destination Apex One Servers must be using the same language version. Also, if you are using the Agent Mover tool to move a Security Agent running an earlier version of Apex One to Apex One as a Service, the Security Agent will be upgraded automatically.

From your Apex One as a Service instance, download the Agent Mover tool called `IpXfer_x64.exe` and save it to a location on the Security Agent endpoint that is to be moved with the following URL:

`https://xxxxxx.manage.trendmicro.com/officescan/hotfix_admin/utility/`
`ipxfer/ipxfer_x64.exe`

(substitute `xxxxxx` with your instance identifier)

Note: If the Security Agent endpoint runs on 32-bit platform, download `IpXfer.exe` instead.

Optional Lesson: Migrating to Apex One as a Service

In addition, download the digital certificate data file from your Apex One as a Service instance with the following URL:

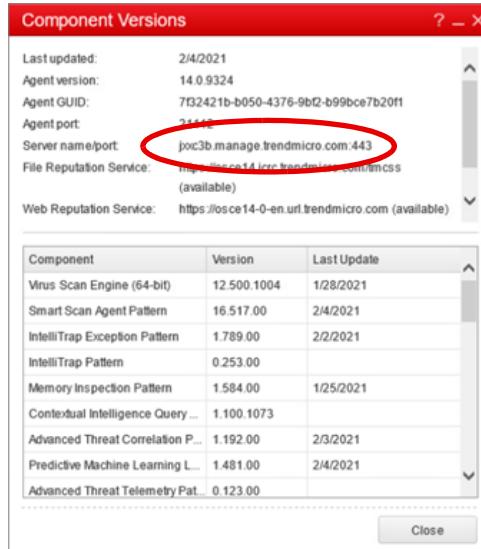
https://xxxxxx.manage.trendmicro.com:443/officescan/hotfix_pccnt/Common/OfcNTCer.dat

On the Security Agent endpoint that is to be moved, open Windows Command Prompt and navigate to the location where you saved the Agent Mover Tool. Run `IpXfer_x64.exe` with the following syntax:

```
ipxfer_x64.exe -s xxxxx.manage.trendmicro.com -p 80 -sp 443 -e  
ofcncer.dat -pwd <unload password>
```

(Use the unload password assigned to the installation of Apex One from which the Agent is moving)

To confirm that the moved Security Agent is now reporting to the Apex One as a Service instance, open the Security Agent console in the system tray and click **Component Versions**. The **Server name/ port** should list the instance name of your Apex One instance with the port of 443.



Creating Administrative Users in Apex Central as a Service

In addition to the predefined administrative roles, additional customized administrative roles can be added through the Apex Central as a Service Web Management console. This allows the organization to tailor the capabilities of administrators.

Creating a New Role

In the Apex Central as a Service Web Management console, click **Administration > Account Management > User Roles**. The list of pre-defined roles is displayed.

The screenshot shows the 'User Roles' section of the Trend Micro Apex Central interface. At the top, there are 'Add' and 'Delete' buttons. Below is a table with columns for 'Name' and 'Description'. The roles listed are:

Name	Description
Administrator	This role cannot monitor, review, or investigate DLP incidents triggered by any Active Directory user.
Administrator_and_DLP_Compliance_Officer	This role can monitor, review, and investigate DLP incidents triggered by all Active Directory users.
DLP_Compliance_Officer	This role can monitor, review, and investigate DLP incidents triggered by all Active Directory users.
DLP_Incident_Reviewer	This role can investigate DLP incidents triggered by Active Directory users that report to the DLP Incident Reviewer.
Operator	This role can view reports generated by other users, query logs, and update user account information.
Power_User	This role can generate and maintain reports, query and maintain logs, and update user account information.
Read-only_User	This role can view data on the management console and update user account information.
Threat_Investigator	This role can investigate security threat incidents on managed endpoints/servers.

Click **Add** and create a new role by identifying the menu items the holders of the new role will have access to, as well as the access rights.

The screenshot shows the 'Add Role' page. It includes fields for 'Name' (set to 'NewRole') and 'Description' (set to 'New role for demonstration purposes'). Under 'Menu Access Control', it lists accessible menus with checkboxes. The 'Policies' menu is selected, with its sub-items like 'Policy Management' and 'Policy Resources' also checked. At the bottom, under 'Specify access rights', there are three radio button options: 'Full control, except:' (selected), 'Create, copy and import policies', 'Monitor, review, and investigate DLP incidents triggered by all users', and 'Read only'. There are 'Save' and 'Cancel' buttons at the bottom.

Optional Lesson: Migrating to Apex One as a Service

Click **Save**. The new role is displayed in the **User Roles** list.

The screenshot shows the 'User Roles' section of the Trend Micro Apex Central web interface. At the top, there are 'Add' and 'Delete' buttons. Below is a table with columns for 'Name' and 'Description'. A new role, 'NewRole', is highlighted with a red oval. The table entries are:

Name	Description
Administrator	This role cannot monitor, review, or investigate DLP incidents triggered by any Active Directory user.
Administrator_and_DLP_Compliance_Officer	This role can monitor, review, and investigate DLP incidents triggered by all Active Directory users.
DLP_Compliance_Officer	This role can monitor, review, and investigate DLP Incidents triggered by all Active Directory users.
DLP_Incident_Reviewer	This role can investigate DLP incidents triggered by Active Directory users that report to the DLP Incident Reviewer.
NewRole	New role for demonstration purposes
Operator	This role can view reports generated by other users, query logs, and update user account information.
Power_User	This role can generate and maintain reports, query and maintain logs, and update user account information.
Read-only_User	This role can view data on the management console and update user account information.
Threat_Investigator	This role can investigate security threat incidents on managed endpoints/servers.

Create a New Administrative User Account

A new user account assigns the new roles to administrators. Still in the Apex Central as a Service Web Management console, click **Administration > Account Management > User Accounts**. Click **Add** and create a new custom account with the user's details.

The screenshot shows the 'User Accounts' creation form. It starts with a 'Step 1: User Information' step. The 'Enable this account' checkbox is checked. The 'User Information' section contains fields for a 'Custom account':

- User name*: gkirby
- Full name*: George Kirby
- Password*: (redacted)
- Confirm password*: (redacted)
- Email address: gkirby@company.com
- Telephone number: (redacted)
- Mobile phone number: (redacted)

Below this, there is an 'Active Directory user or group' section with fields for 'User/Group name*' and 'Base distinguished name*', both currently empty. There is also a 'Search' button and a 'Selected users/groups' list.

At the bottom are 'Next' and 'Cancel' buttons.

Click **Next** and from the **Select role** list, click the role required for the new user account.

The screenshot shows the 'User Accounts' section of the Trend Micro Apex Central interface. A message at the top says 'Step 1 >>> Step 2: Access control'. Below it, a checkbox 'Enable this account' is checked. A 'Managed Product Access Control' panel is open, showing a dropdown 'Select role' set to 'NewRole'. Under 'Select accessible products/folders:', there is a tree view with 'Apex Central as a Service' expanded, showing 'Local Folder' selected. Under 'Specify access rights:', checkboxes for 'Execute', 'Configure', and 'Edit Directory' are checked. At the bottom are 'Back', 'Save' (highlighted in blue), and 'Cancel' buttons.

Expand the product tree to select the products the administrator will have access to and click to enable the required access rights. Click **Save**.

The new user account is displayed in the list.

The screenshot shows the 'User Accounts' list. At the top, there are buttons for 'Add' and 'Delete', and a link 'Enable Two-Factor Authentication'. The table lists one user: 'gkirby' (Full Name: George Kirby, Type: Custom, User Role: NewRole, Locked: No, Enable: Yes). At the bottom are 'Add' and 'Delete' buttons.

<input type="checkbox"/>	User/Group Name	Full Name	Type	User Role	Locked	Enable
<input type="checkbox"/>	gkirby	George Kirby	Custom	NewRole	No	<input checked="" type="checkbox"/>

Optional Lesson: Migrating to Apex One as a Service

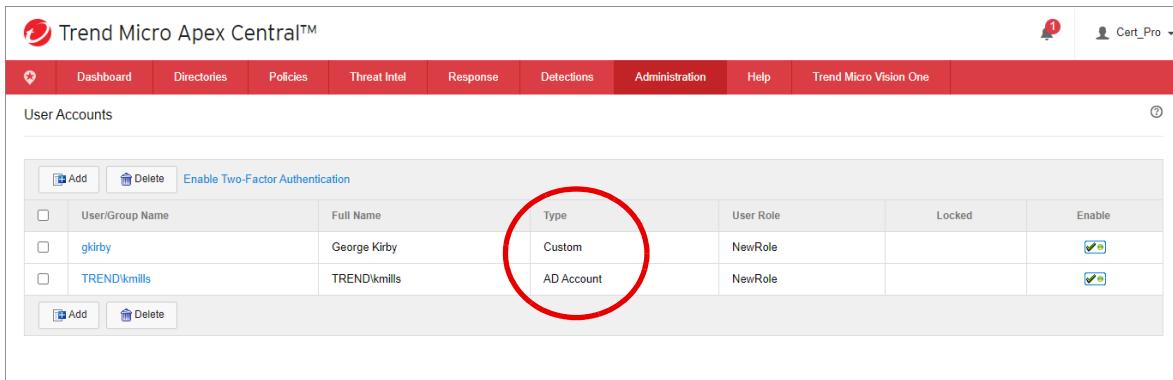
Alternately, if Apex Central as a Service has been integrated with Active Directory, accounts can be created based on an Active Directory entry. Search the branches in Active Directory to locate the required users or groups and click > to move them into the **Selected user/groups** list.

The screenshot shows the Trend Micro Apex Central interface. In the top navigation bar, there are links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, Help, and Trend Micro Vision One. A user icon with a notification count of 1 and the name 'Cert_Pro' is also present. The main content area is titled 'User Accounts'. A sub-dialog titled 'Step 1: User Information' is open. It contains fields for 'User name', 'Full name', 'Password', 'Confirm password', 'Email address', 'Telephone number', and 'Mobile phone number'. Below these, there's a radio button for 'Custom account' and another for 'Active Directory user or group', which is selected. Under 'Active Directory user or group', there are fields for 'User/Group name' and 'Base distinguished name'. A 'Search' button is available. To the right, a list titled 'Selected users/groups' shows 'TREND\kmills'. At the bottom of the dialog are 'Next' and 'Cancel' buttons.

Click **Next** and select a role and access rights.

The screenshot shows the 'Add New User' dialog. The top navigation bar and user icon are identical to the previous screenshot. The main content area is titled 'Add New User'. It includes a note: 'You can assign each user different access rights to a specified group of folders'. The 'Add New User' dialog itself has sections for 'Select role' (with 'NewRole' selected), 'Select accessible folders' (listing 'Apex Central as a Service' and 'Local Folder'), and 'Specify folder access rights' (with checkboxes for 'Execute', 'Configure', and 'Edit Directory' all checked). At the bottom are '<< Back', 'Save', and 'Cancel' buttons.

The **Type** column in the **User Accounts** list displays whether the account is a custom or Active Directory account.



<input type="checkbox"/> User/Group Name	Full Name	Type	User Role	Locked	Enable
<input type="checkbox"/> gkirby	George Kirby	Custom	NewRole		<input checked="" type="checkbox"/>
<input type="checkbox"/> TRENDikmills	TRENDikmills	AD Account	NewRole		<input checked="" type="checkbox"/>

Appendix A: Troubleshooting Trend Micro Apex One

This Appendix details some tips and methods for troubleshooting various Apex One components.

Debugging Security Agents

Enabling debug functions on the Security Agent allows an administrator to analyze many aspects of an Agent's operation. To enable debug logging on an Security Agent, perform the following steps:

- 1 Create and save a file called `ofcdebug.ini` in the Security Agent folder with the following entries:

```
[debug]  
  
DebugLevel=9 ← Level 1 (less detailed) to 9 (most detailed)  
  
DebugLog=<name and file path for the debug log>  
  
debugLevel_new=D  
  
debugSplitSize=104857600  
  
debugSplitPeriod=24  
  
debugRemoveAfterSplit=1
```

Note: The `debugLevel_new`, `debugSplitSize`, `debugSplitPeriod`, and `debugRemoveAfterSplit` entries instruct Apex One to split the debug files into smaller files.

- 2 Locate and double-click `Logserver.exe` in the Agent folder. This will start the debug logging.
- 3 After running for a period of time, open the log file to view details.
- 4 Close `Logserver.exe` and delete `ofcdebug.ini` to disable debugging.

Debugging the Apex One Server

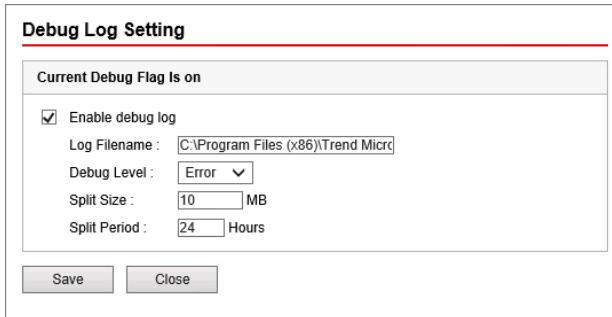
Enabling debug functions on the Apex One Server allows an administrator to analyze many aspects of the Apex One Server's operation. To enable debug logging on the Apex One Server, perform the following steps.

- 1 Log into the Apex One Web Management console with the appropriate administrative credentials.

- 2 Hover the cursor over the T in Trend Micro Apex One on the title banner of the console and click.



- 3 The Debug Log Setting window is displayed.



- 4 Specify the log settings required and click Save.

- 5 Locate the log file called `ofcdebug.log` in the following folder:

`C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Log`

- 6 Disable logging after the issue has been resolved.

Changing the Security Agent Communication Port

It might be necessary to change the Security Agent communication port as part of troubleshooting, or after upgrading or migrating the Apex One Server.

On the Security Agent

- 1 Copy the `IpXfer.exe` file from the following folder on the Apex One Server onto the Security Agent:

`C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\IpXfer\`

- 2 On the Security Agent, open a Windows Command Prompt. Navigate to the folder where the `ipxfer.exe` file was placed and execute the following command:

`ipxfer.exe -s <server_name> -sp 443 -c <agent_port> -pwd <password>`

Note: Use `ipxfer_x64.exe` on 64-bit systems.

Troubleshooting Agent/Server Communication Issues

Certain conditions may prevent the Agent tree from displaying the correct Agent connection status, for example, if the endpoint computer is physically disconnected from the network, the Agent will not be able to notify the Server that it is now offline and will display incorrectly as online. The Agent-Server connection can be manually verified or Apex One can perform a schedule verification.

Verify the Connection Status Manually

To verify the connection status manually, click **Agents > Connection Verification**. On the **Manual Verification** tab, click **Verify Now**.

The screenshot shows the 'Connection Verification' page in the Apex One interface. The 'Manual Verification' tab is active. Below it, a message states: 'To verify the server-agent connection status immediately, click Verify Now.' A large red circle highlights the 'Verify Now' button, which is located in a grey rectangular area below the message.

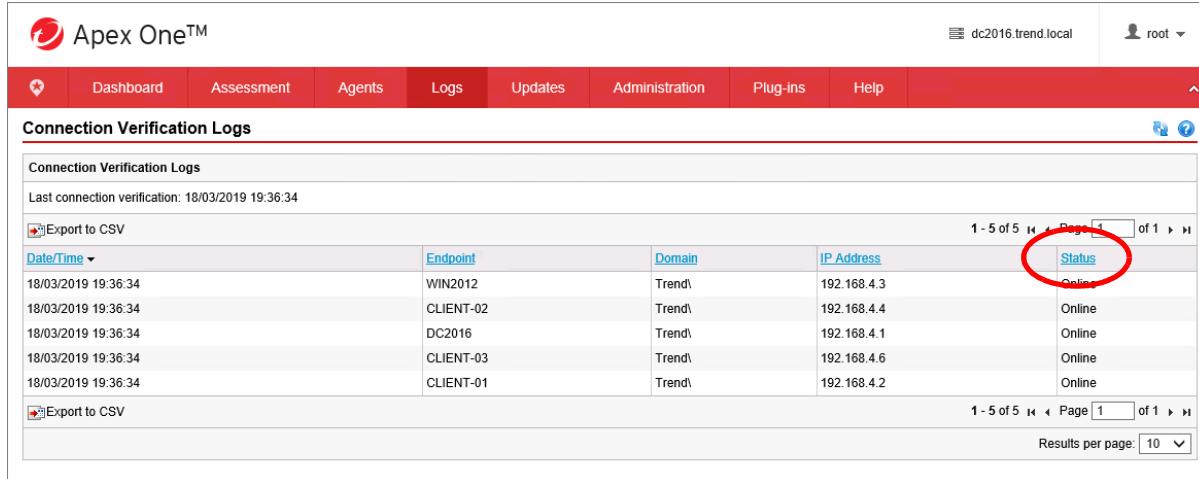
Verify the Connection Status Automatically

To verify the connection status automatically, click **Agents > Connection Verification**. On the **Scheduled Verification** tab configure the scheduled verification.

The screenshot shows the 'Connection Verification' page in the Apex One interface. The 'Scheduled Verification' tab is active. Under the 'Enable scheduled verification' section, the 'Daily' option is selected. To its right, a 'Start time' field is set to '10 : 30 (hh:mm)'. At the bottom of the form, there are 'Save' and 'Cancel' buttons, with the 'Save' button highlighted by a large red circle.

Verify the Results of the Connection Status

Apex One created a log entry each time the Agent/Server connection is checked. To check the logs, click **Logs > Agents > Connection Verification Logs**. Check the **Status** column for the results of the connection test.



The screenshot shows the Trend Micro Apex One interface with the title "Apex One™". The top navigation bar includes links for Dashboard, Assessment, Agents, Logs (which is selected), Updates, Administration, Plug-ins, and Help. The user is logged in as "root" on "dc2016.trend.local". The main content area is titled "Connection Verification Logs" and displays a table of log entries. The table has columns for Date/Time, Endpoint, Domain, IP Address, and Status. All entries show the status as "Online". The "Status" column is highlighted with a red circle. At the bottom of the table, there are buttons for "Export to CSV" and "Results per page: 10".

Date/Time	Endpoint	Domain	IP Address	Status
18/03/2019 19:36:34	WIN2012	TrendI	192.168.4.3	Online
18/03/2019 19:36:34	CLIENT-02	TrendI	192.168.4.4	Online
18/03/2019 19:36:34	DC2016	TrendI	192.168.4.1	Online
18/03/2019 19:36:34	CLIENT-03	TrendI	192.168.4.6	Online
18/03/2019 19:36:34	CLIENT-01	TrendI	192.168.4.2	Online

Troubleshooting Communication Issues Between Security Agent and Server

There are several potential causes for connection issues. Some of the remedies include:

- Verifying if the Server can ping the Agent, and vice versa.
- Checking if the Server can telnet to the Agent using the Agent communication port.
- Checking if the Agent can telnet to the Server using the Server communication port (default is 8080 for Apex One).
- Verifying if the Agent can resolve the Server's hostname.
- Open a browser then type the following address:

`http://<servername>:<port>/officescan`

Verify Security Agent Registry settings

In some cases the Agent Registry settings may be incorrect. Perform the following steps to confirm the settings:

- 1 On the Server machine, open the `ofcscan.ini` file in a text editor.

2 Note the values of the following parameters:

Master_DomainName

Master_DomainPort

Master_SSLPort

Client_LocalServer_Port

3 Open the Registry Editor on the Agent computer.

4 Open the following registry hive (for 64-bit machines):

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\TrendMicro\PC-cillinNTCorp\CurrentVersion

5 Check the values of the following registry keys and modify as necessary:

LocalServerPort ← must have the same value as Client_LocalServer_Port

Server ← must have the same value as Master_DomainName

ServerPort ← must have the same value as Master_DomainPort

ServerSSLPot ← must have the same value as Master_SSLPort

Confirm Correct Product Licensing

Invalid licensing of server and desktop components could create communication problems. From the Apex One Web Management console, go to **Administration > Settings > Product License** and verify that the licensing status displays as is **Activated**.

License Information	
Product:	Apex One: Anti-Malware feature licensing
Status:	Activated View online
Type:	Full
Seats:	50
Expiration Date:	3/16/2020 00:00:00
Activation Code:	AP-XX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
Last Updated:	3/17/2019 23:59:03
<input type="button" value="Refresh"/> <input type="button" value="Specify Activation Code"/>	

Verify Agent Privileges to Communicate With the Server

In some cases, the Agent may not have sufficient privileges to communicate with the Server. To verify, perform the following steps:

- 1 On the Apex One Server, open Windows Command Prompt.
- 2 Navigate to the C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV folder and run the following commands:

```
svrsvcsetup -setvirdir
```

```
svrsvcsetup -setprivilege
```

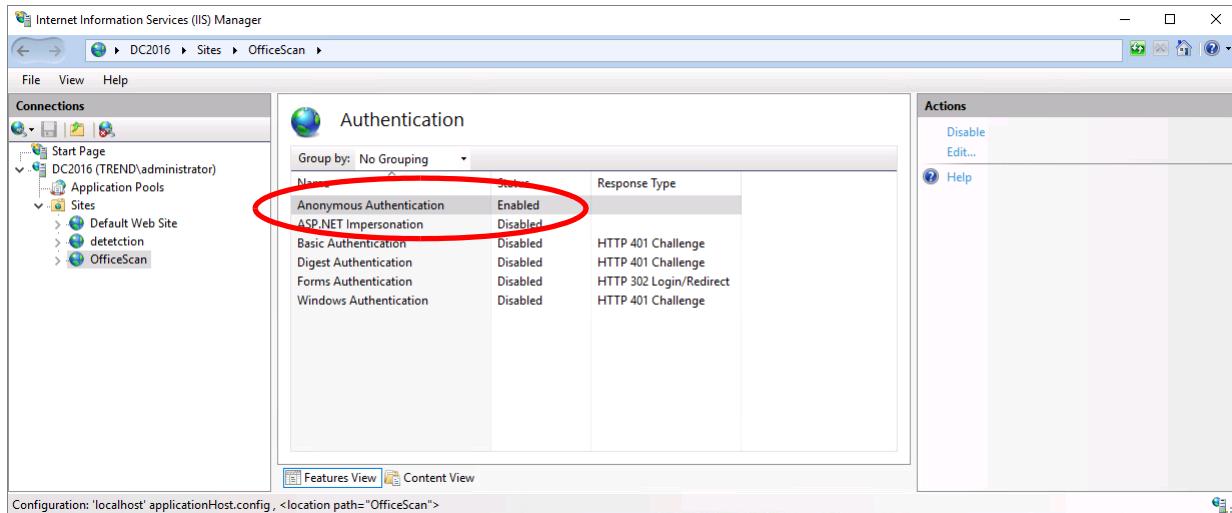
If you are using SSL, run the following command:

```
svrsvcsetup -enablessl
```

Verify Internet Information Services

In some cases the Internet Information Services (IIS) settings may be incorrect. To verify, perform the following steps.

- 1 Open the Internet Information Services Manager then expand <server name> > **Sites** > **OfficeScan**.
- 2 In the middle pane, double-click **Authentication**.
- 3 Ensure that **Anonymous access** is enabled.



- 4 Click **Edit** in the **Actions** frame and ensure that anonymous authentication is using the **IUSR** user.



Re-establish Communication Using **autopcc.exe**

Autopcc.exe can be used to re-establish connection between the Agent and Server. To force an update of the Security Agent and a reconnection, perform the following steps.

- 1 In Windows, click **Start > Run** and enter the following command:

```
\\"<Apex_One_Server_name_or_IP_address>\ofcscan\autopcc.exe -f -u
```

- 2 Open the Apex One Web Management console, and verify if the Security Agent now appears correctly

Re-establish Communication Using **IpXfer.exe**

Alternately, **IpXfer.exe** can be used to re-establish connection between the Security Agent and Apex One Server. To attempt a reconnection, perform the following steps:

- 1 On the Apex One Server, open the **C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\ofcscan.ini** file in a text editor
- 2 Note the values of the following parameters:
 - Master_DomainName**
 - Master_SSLPort**
 - Client_LocalServer_SSLPort**
- 3 Copy the **C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\Admin\Utility\IpXfer\IpXfer.exe** file to the Security Agent folder on the Agent endpoint computer.
- 4 On the Agent computer, open Windows Command Prompt window and navigate to the Security Agent folder and run the following command:

```
IpXfer.exe -s <value_of_Master_DomainName> -p
<value_of_Master_SSLPort> -c <value_of_Client_LocalServer_SSLPort>
```

- 5 Open the Web Management console then verify if the Security Agent now appears correctly.

Verify Windows Firewall Blocking

In some cases, the Windows Firewall may be blocking communication ports. To open the necessary ports, perform the following steps.

- 1 On the Apex One Server computer, open the C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\ofcscan.ini file in a text editor.
- 2 Note the values of the following parameters:

Master_SSLPort

Client_LocalServer_SSLPort

- 3 On the Agent machine, open **Control Panel > Windows Firewall**.
- 4 Click the **Exceptions** tab and click **Add Port**.
- 5 Enter the values of the Master_SSLPort and Client_LocalServer_SSLPort using TCP.
- 6 Restart the Apex One NT Listener service.
- 7 Clear Internet Explorer temporary Internet files, offline content, and cookies.
- 8 Open the Web Management console and verify if the Agent now appears correctly.

Change the Agent Domain

Changing the Agent domain may sometimes resolve communication issues. To change the Agent domain, perform the following steps.

- 1 Open the Apex One Web Management console and navigate to **Agents > Agent Management**.
- 2 Click **Manage Agent Tree > Add Domain**.
- 3 Type a name for the domain, and click **OK**.
- 4 Drag the Agent that has an offline or disconnected status to the new domain.
- 5 On that Security Agent endpoint, restart the Apex One NT Listener service.
- 6 Right-click the Apex One icon on the system tray then click **Update Now**.
- 7 Refresh the Web Management console then verify if the Agent now appears correctly.

Verify Server Hostname Resolution

If the Security Agent is unable to resolve the Apex One Server hostname to an IP address, communication issues may be encountered. To verify name resolution, perform the following steps.

- 1 On the Server machine, open the C:\Program Files (x86)\Trend Micro\Apex One\PCCSRV\ofcscan.ini file in a text editor.
- 2 Note the values of the following parameters:

Master_DomainName

Master_SSLPort

- 3 On the Agent computer, open a browser and type the following address:

`https://<value_of_Master_DomainName>:<value_of_Master_SSLPort>/officescan/cgi/cgionstart.exe`

- 4 If the page displays -2, the client can communicate with the server.

Troubleshooting Virus Infection

To better help administrators analyze the source of malware and spyware, they can verify the infection channel. This data exists in the real time scan logs for virus and spyware on both agents and servers, and can help administrators trace how users were infected by the malware or spyware.

Determining the Virus Infection Channel on the Server

The **Virus/Malware Logs** displayed in the Web Management console includes an **Infection Channel** column.



Virus/Malware Logs

Date range: 09/03/2019 10:02:38 - 16/03/2019 10:02:38

Export All to CSV

Date/Time	Endpoint	Security Threat	Infection Channel	Infected File/Object	Scan Type	Result	IP Address	MAC Address	Details
13/03/2019 14:52:30	CLIENT-02	Eicar test file	Web	eicar[1].com	Real-time Scan	Quarantined	192.168.4.4	00-50-56-02-2A-F7	View

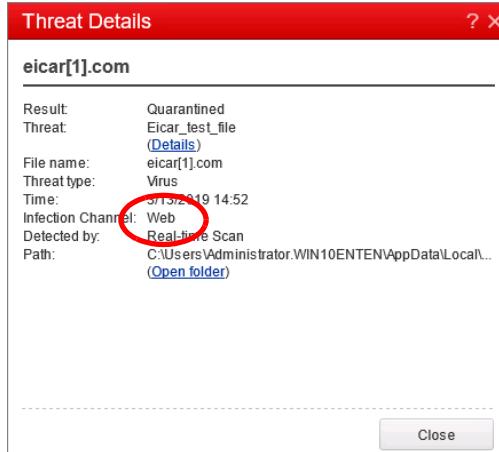
Export All to CSV

1 - 2 of 2 | Page [1] of 1 | Results per page: 10

< Back Close

Determining the Virus Infection Channel on the Agent

On the Security Agent, the **Infection Channel** details exist in the **Log Details**.



Threat Details

eicar[1].com

Result:	Quarantined
Threat:	Eicar_test_file (Details)
File name:	eicar[1].com
Threat type:	Virus
Time:	3/13/2019 14:52
Infection Channel:	Web
Detected by:	Real-time Scan
Path:	C:\Users\Administrator.WIN10ENTENAppData\Local\... (Open folder)

Close

Determining Spyware/Grayware Infection Channel on the Server

In the **Spyware/Grayware Log Details**, the **Infection Channel** is displayed in the **Spyware Components** section.

Spyware/Grayware Log Details

Spyware/Grayware Log Details	
Date/Time:	13/03/2019 14:53:42
Endpoint:	CLIENT-02
Domain:	Trend\Classroom
Platform:	Windows 10 10.0.16299
Spyware/Grayware name:	SPYCAR_TEST_FILE
Scan type:	Real-time Scan
Result:	Successful, no action required
IP address:	192.168.4.4
MAC address:	00-50-56-02-2A-F7

Spyware Components

Components	System Area	Spyware/Grayware Type	Risk	Result	Infection Channel
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-KillProgramsTab.exe	File System	General	Low	Cleaned	Web
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-KillPrivacyTab.exe	File System	General	Low	Cleaned	Web
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-KillGeneralTab.exe	File System	General	Low	Cleaned	Web
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-KillContentTab.exe	File System	General	Low	Cleaned	Web
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-KillConnectionsTab.exe	File System	General	Low	Cleaned	Web
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-KillAdvancedTab.exe	File System	General	Low	Cleaned	Web
C:\Users\Administrator.WIN10ENTEN\Desktop\Spycar_Files_Password_noivirus\Spycar_Files\IE-HomePageLock.exe	File System	General	Low	Cleaned	Web

< Back Close

Determining Spyware/Grayware Infection Channel on the Agent

On the Agent, the **Infection Channel** details exist in the **Log Details**.

Threat Details

SPYCAR_TEST_FILE

Result:	Successful
Threat name:	SPYCAR_TEST_FILE (Details)
Threat type:	Spyware
Time:	3/13/2019 14:53
Detected by:	Real-time Scan
Components:	3

Compon...	Affected ...	Type	Risk	Infection ...	Result
C:\Users...	File Syst...	General	Low	Web	Cleaned
C:\Users...	File Syst...	General	Low	Web	Cleaned
C:\Users...	File Syst...	General	Low	Web	Cleaned

Close

Troubleshooting the Firewall Service

Consider the following to help troubleshoot firewall-related issues:

- Verify that the protocol is supported. In Apex One, only TCP/UDP/ICMP protocols are supported.
- Dump rules using `tmpfw dump` command and verify rules in the `!Pfwdump.txt` file.

```

IPfwDump.txt - Notepad
File Edit Format View Help
Dump the current configuration
18/12/2018 16:16:09

===== DLL Load Status =====
CFW DLL Loaded ?: 1
CFW DLL File Path: "C:\Program Files (x86)\Trend Micro\OfficeScan Client\tmWfpApi.dll"

===== Versions =====
PFW Version: 5.83
PFW Build Number: 1059
CFW Driver Version: 5.83
CFW Driver Build Number: 1059
GSS Pattern Version: 10343

===== NIC Adapters Info =====
#V4-12: IP Address: 192.168.4.4
Subnet Mask: 255.255.240.0
Default Gateway: 192.168.0.1
Physical Address: 00:50:56:02:2A:F7
MTU: 1500
Description: "vmxnet3 Ethernet Adapter #2"
IfType : 0x6

===== CFW Macros =====

===== CFW Rules =====
[65535]-[ 10]: ACCESS, ANY, IPV4, UDP, , , 67:68, ACCEPT,
[65535]-[ 20]: ACCESS, ANY, IPV6, UDP, , , 546:547, ACCEPT,
[65535]-[ 30]: ACCESS, IN, IPV4, ICMP, , 3, 4, ACCEPT,
[65535]-[ 40]: ACCESS, ANY, IPV6, ICMPV6, , , 1, , ACCEPT,
[65535]-[ 50]: ACCESS, IN, IPV6, ICMPV6, , , 2, , ACCEPT,

```

Troubleshooting the Unauthorized Change Prevention Service

To enable debug logs for this service, perform the following steps.

- Add the following Registry key on the Security Agent host, and restart the service

Key	HKLM\Software\TrendMicro\AEGIS
Value	DebugLogFlags
Data	0x00000032
Type	REG_DWORD

Logs will be placed in:

```

... \BM\Log > TmCommengyyyymmdd_nn.log and TMPEMyyyyymmdd_nn.log
... \Security Agent\Log > TMBMCliyyyymmdd_nn.log

```

Troubleshooting Edge Relay Server Certificates

The Apex One Edge Relay Server uses digital certificates to secure communication between Agents, the Relay Server and Apex One Server. If communication issues arise, verify the following.

- Verify that Web Server certificate (OscePA) installed in the Trusted Root Certification Authorities store is signed by OsceEdgeRoot
- Verify the certificate used by the Data Service

Troubleshooting Sample Submission

To troubleshoot issues related to malware sample submission to a Deep Discovery Analyzer device, consider the following:

- Verify that the Apex One Server and Deep Discovery Analyzer have been registered in Apex Central and the devices are not listed in the New Entity folder

The screenshot shows the Trend Micro Apex Central web interface. At the top, there's a navigation bar with links for Dashboard, Directories, Policies, Threat Intel, Response, Detections, Administration, and Help. On the far right, it shows a user icon and 'admin'. Below the navigation is a breadcrumb trail: '< Directory Management'. There's a checkbox labeled 'Keep the current user access permissions when moving managed products/folders.' followed by three buttons: 'Add Folder', 'Rename', and 'Delete'. The main content area shows a tree view of folders. Under 'Local Folder', there are several entries: 'WIN2012', 'Local Folder' (which has a sub-item 'New Entity' circled in red), 'Trend Micro Servers' (which has sub-items 'DC2016_ApexOne' and 'Analyzer' also circled in red), and 'Analyzer'. At the bottom of the page, there's a note: 'Note: Select a product/directory and drag it to the destination folder to move.'

- Verify that the Apex One is subscribed to the Suspicious Object List

The screenshot shows the 'Suspicious Object List Settings' page in the Apex One web interface. At the top, it displays the server address as https://192.168.4.3:443/WebApp and the last sync time as 2/27/2019 13:53:22 (Try every 10 minutes). Below this, there are buttons for 'Sync Now', 'Test Connection', and 'Unsubscribe'. The 'Agent Settings' section contains four checked checkboxes: 'Enable Suspicious URL list', 'Enable Suspicious IP list', 'Enable Suspicious File list', and 'Enable Suspicious Domain list'. A note below states that Apex One uses Smart Protection Servers to deploy Suspicious URL lists to Security Agents. At the bottom are 'Save' and 'Cancel' buttons.

- Verify that the **Sample Submission Settings** are enabled for the Security Agent.

The screenshot shows the 'Sample Submission' settings page. Under 'Sample Submission Settings', there is a checked checkbox labeled 'Enable suspicious file submission to Virtual Analyzer'. A note below explains that suspicious files include programs not known to Trend Micro, heuristic detections of processes, and low prevalence autorun programs on removable storage. At the bottom are 'Save' and 'Cancel' buttons.

- Verify that the sample gets uploaded from the Agent to the Apex One Server by locating the sample in the following folder shortly after detection, but before processing by the Deep Discovery Analyzer:

C:\Program Files (x86)\Trend Micro\Apex One\TEMP\Sample Submission

Appendix B: What's New in Trend Micro Apex One

Trend Micro OfficeScan has evolved into Trend Micro Apex One. As an upgrade to OfficeScan, Apex introduces new functionality to endpoint protection. Some of the new features introduced in Apex One are described here.

All-in-one Security Agent

Apex One integrates capabilities like Application Control, Vulnerability Protection, Endpoint Sensor into a single Agent installed on the endpoint computer.

Offline Predictive Machine Learning

Apex One includes a new offline machine learning model for use in cases where the endpoint does not have network connectivity to query the cloud-based learning model hosted on the Trend Micro Smart Protection Network.

Fileless Threat Detection Enhancements

In-memory runtime analysis capabilities have been enhanced in Apex One to improve fileless threat detection.

Integrated Vulnerability Protection

Apex One's Vulnerability Protection provides timely blocking of operating system vulnerabilities. This Virtual Patching protection is simplified by configuring Vulnerability Protection in one of two modes: security or performance.

Integrated Application Control

Allows administrator to define which applications are allowed on the protected endpoint. Applications can be blocked on a category level, by a particular vendor, by specific application and even version of application.

Investigative Capabilities

Apex One integrates new Endpoint Detection and Response capabilities including server-side metadata sweeping, Indicator of Attack (IOA) behavior hunting, new query and automation Application Programming Interfaces (API).

Mac Protection Features

Apex One adds new protection features for Mac endpoints, including Endpoint Detection and Response, Predictive Machine Learning, and Device Control.

Managed Detection and Response Service Support for SaaS

The Trend Micro Managed Detection and Response (MDR) Service, which was previously only supported in on-premises deployments is now also supported in the Software as a Service deployment model.

Indicator of Attack Behavioral Analysis Enhancements

Apex One enhances the Indicator of Attack (IOA) Behavioral Analysis capabilities to detect known indicators of attack including ransomware, encryption behaviors and script launching.

Application Programming Interface Enhancements

Apex One enhances the Application Programming Interface (API) capabilities by introducing more reporting and control capabilities.

Cloud Sandbox

Apex One as a Service customers can now take advantage of an additional Cloud Sandbox (Deep Discover Analyzer as a Service) for Connected Threat Defense, which is available as an add-on service.

Apex Central

Trend Micro Control Manager has been rebranded to Apex Central. This application contains the same functionality as Control Manager and includes support for new Apex One features such as integrated Application Control, Vulnerability Protection and Endpoint Sensor.

Kernel Mode Termination Protection

Change protection blocks user mode termination event but there are some applications that could potentially terminate processes through kernel mode. To address this issue, Apex One introduces a new Watchdog mechanism for kernel mode termination events. This mechanism will attempt to recover target processes after being terminated.

Location Awareness Enhancement

An enhancement for location awareness in Apex One will check the network adapter used to connect to the reference host and identify if the endpoint is internal or external. Previously, when an external Security Agent connects to the Apex One Server using VPN connection, it was referred as an internal agent and the related internal policy settings were applied. VPN clients (Cisco, F5, Fortigate...) create a virtual network adapter as a network device to communicate with target network. In Apex One, a new setting called **Exclude agents using VPN or PPP dial-up connections** is available so Security Agents using the VPN connection will be identified as an external Agent.

