



# Trend Micro Apex Central™

## Patch 6

### Administrator's Guide

Centralized Security Management for Endpoints

---

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

<http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx>

Trend Micro, the Trend Micro t-ball logo, Trend Micro Apex Central, Trend Micro Apex One, Control Manager, and OfficeScan are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2023. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM09754/230720

Release Date: July 2023

Protected by U.S. Patent No.: 5,623,600; 5,889,943; 5,951,698; 6,119,165

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

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

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

Evaluate this documentation on the following site:

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

## **Privacy and Personal Data Collection Disclosure**

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Apex One™ as a Service collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

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

# Table of Contents

## **Preface**

|                            |   |
|----------------------------|---|
| Preface .....              | 1 |
| Documentation .....        | 2 |
| Audience .....             | 3 |
| Document Conventions ..... | 3 |
| Terminology .....          | 4 |

## **Part I: Introduction**

### **Chapter 1: Introducing Apex Central**

|                                 |     |
|---------------------------------|-----|
| About Apex Central .....        | 1-2 |
| What's New .....                | 1-2 |
| Key Features and Benefits ..... | 1-5 |
| Apex Central Architecture ..... | 1-7 |

## **Part II: Getting Started**

### **Chapter 2: The Web Console**

|   |     |
|---|-----|
| About the Web Console .....                     | 2-2 |
| Web Console Requirements .....                  | 2-2 |
| Assigning HTTPS Access to the Web Console ..... | 2-3 |
| Accessing the Web Console .....                 | 2-5 |
| Configuring Web Console Settings .....          | 2-7 |

### **Chapter 3: The Dashboard**

|                           |     |
|---------------------------|-----|
| About the Dashboard ..... | 3-2 |
|---------------------------|-----|

|   |      |
|---|------|
| Tabs and Widgets .....                            | 3-2  |
| Working with Tabs .....                           | 3-2  |
| Working with Widgets .....                        | 3-4  |
| Security Posture Tab .....                        | 3-6  |
| Compliance Indicators .....                       | 3-7  |
| Critical Threats .....                            | 3-9  |
| Resolved Events .....                             | 3-10 |
| Security Posture Chart .....                      | 3-10 |
| Security Posture Details Pane .....               | 3-12 |
| Summary Tab .....                                 | 3-17 |
| Critical Threats Widget .....                     | 3-17 |
| Users with Threats Widget .....                   | 3-20 |
| Endpoints with Threats Widget .....               | 3-21 |
| Apex Central Top Threats Widget .....             | 3-22 |
| Product Component Status Widget .....             | 3-23 |
| Product Connection Status Widget .....            | 3-25 |
| Ransomware Prevention Widget .....                | 3-26 |
| Data Loss Prevention Tab .....                    | 3-27 |
| DLP Incident Trends by User Widget .....          | 3-27 |
| DLP Incidents by Severity and Status Widget ..... | 3-28 |
| DLP Incidents by User Widget .....                | 3-30 |
| DLP Incidents by Channel Widget .....             | 3-31 |
| DLP Template Matches Widget .....                 | 3-32 |
| Top DLP Incident Sources Widget .....             | 3-33 |
| DLP Violated Policy Widget .....                  | 3-33 |
| Compliance Tab .....                              | 3-33 |
| Product Application Compliance Widget .....       | 3-34 |
| Product Component Status Widget .....             | 3-35 |
| Product Connection Status Widget .....            | 3-37 |
| Agent Connection Status Widget .....              | 3-38 |
| Threat Statistics Tab .....                       | 3-39 |
| Apex Central Top Threats Widget .....             | 3-39 |
| Apex Central Threat Statistics Widget .....       | 3-40 |
| Threat Detection Results Widget .....             | 3-42 |

|  |      |
|--|------|
| Policy Violation Detections Widget ..... | 3-44 |
| C&C Callback Events Widget .....         | 3-44 |

## **Chapter 4: Account Management**

|   |      |
|---|------|
| User Accounts .....                                   | 4-2  |
| Root Account .....                                    | 4-4  |
| Adding a User Account .....                           | 4-5  |
| Managed Product Access Control .....                  | 4-9  |
| Editing a User Account .....                          | 4-11 |
| Enabling or Disabling Two-Factor Authentication ..... | 4-12 |
| Viewing or Editing User Account Information .....     | 4-14 |
| User Roles .....                                      | 4-16 |
| Default User Roles .....                              | 4-17 |
| Adding a User Role .....                              | 4-20 |
| Editing a User Role .....                             | 4-22 |

## **Chapter 5: License Management**

|   |     |
|---|-----|
| Apex Central Activation and License Information .....       | 5-2 |
| Activating Apex Central .....                               | 5-2 |
| Viewing and Renewing Apex Central License Information ..... | 5-2 |
| Managed Product Activation and Registration .....           | 5-4 |
| License Management Details .....                            | 5-4 |
| Managed Product License Information .....                   | 5-5 |
| Activating Managed Products .....                           | 5-6 |
| Renewing Managed Product Licenses .....                     | 5-7 |

## **Chapter 6: Active Directory and Compliance Settings**

|  |     |
|--|-----|
| Active Directory Integration .....                           | 6-2 |
| Configuring Active Directory Connection Settings .....       | 6-2 |
| Troubleshooting Active Directory Synchronization .....       | 6-5 |
| Compliance Indicators .....                                  | 6-6 |
| Configuring the Antivirus Pattern Compliance Indicators .... | 6-8 |

|   |      |
|---|------|
| Configuring the Data Loss Prevention Compliance Indicator ..... | 6-10 |
| Endpoint and User Grouping .....                                | 6-11 |
| Sites .....   | 6-12 |
| Creating a Custom Site .....                                    | 6-12 |
| Merging Sites .....   | 6-13 |
| Reporting Lines .....   | 6-14 |
| Creating a Custom Reporting Line .....                          | 6-14 |
| Merging Reporting Lines .....                                   | 6-15 |

## **Chapter 7: User/Endpoint Directory**

|   |      |
|---|------|
| User/Endpoint Directory .....                                 | 7-2  |
| User Details .....  | 7-3  |
| Security Threats for Users .....                              | 7-6  |
| Policy Status .....   | 7-8  |
| Contact Information .....                                     | 7-9  |
| Synchronizing Contact Information with Active Directory ..... | 7-9  |
| Endpoint Details .....  | 7-10 |
| Endpoint Information .....                                    | 7-12 |
| Security Threats on Endpoints .....                           | 7-13 |
| Policy Status .....   | 7-16 |
| Notes for Endpoints .....                                     | 7-16 |
| General Information for Endpoints .....                       | 7-16 |
| Isolating Endpoints .....                                     | 7-17 |
| Active Directory Details .....                                | 7-19 |
| Affected Users .....  | 7-19 |
| General Information for Security Threats .....                | 7-21 |
| Analyzing Impact on Affected Users .....                      | 7-22 |
| Performing a Retro Scan on Affected Users .....               | 7-23 |
| Retro Scan in Deep Discovery Inspector .....                  | 7-23 |
| Using the Advanced Search .....                               | 7-24 |
| Advanced Search Categories .....                              | 7-26 |



|  |      |
|--|------|
| Custom Tags and Filters .....                  | 7-29 |
| Custom Tags .....                              | 7-31 |
| Creating a Custom Tag .....                    | 7-32 |
| Assigning Custom Tags to Users/Endpoints ..... | 7-33 |
| Filters .....                                  | 7-34 |
| Default Endpoint Filters .....                 | 7-35 |
| Creating a Custom Filter .....                 | 7-36 |
| User or Endpoint Importance .....              | 7-37 |

## **Chapter 8: Trend Vision One**

|  |     |
|--|-----|
| Integrating Apex Central with Trend Vision One ..... | 8-2 |
|--|-----|

# **Part III: Managed Product Integration**

## **Chapter 9: Managed Product Registration**

|   |      |
|---|------|
| Managed Product Registration Methods .....            | 9-2  |
| Server Registration .....                             | 9-2  |
| Managed Server Details .....                          | 9-4  |
| Adding a Managed Server .....                         | 9-5  |
| Editing a Managed Server .....                        | 9-7  |
| Deleting a Managed Server .....                       | 9-8  |
| Configuring Proxy Settings for Managed Products ..... | 9-9  |
| Configuring Cloud Service Settings .....              | 9-10 |
| Managed Product Communication .....                   | 9-11 |
| Modifying the Default Agent Communication Schedule .. | 9-12 |
| Configuring Agent Communication Schedules .....       | 9-13 |
| Configuring Managed Product Heartbeat Intervals ..... | 9-14 |

## **Chapter 10: Security Agent Installation**

|  |      |
|--|------|
| Downloading Security Agent Installation Packages ..... | 10-2 |
|--|------|

|   |       |
|---|-------|
| Apex One Security Agent System Requirements .....             | 10-4  |
| Windows Endpoint Platforms .....                              | 10-4  |
| Windows 7 (32-bit / 64-bit) Service Pack 1 Requirements ..... | 10-4  |
| Windows 8.1 (32-bit / 64-bit) Requirements .....              | 10-5  |
| Windows 10 (32-bit / 64-bit) Requirements .....               | 10-6  |
| Windows Server Platforms .....                                | 10-7  |
| Windows Server 2008 R2 (64-bit) Platforms .....               | 10-8  |
| Windows MultiPoint Server 2010 (64-bit) Platform .            | 10-11 |
| Windows MultiPoint Server 2011 (64-bit) Platform .            | 10-12 |
| Windows Server 2012 (64-bit) Platforms .....                  | 10-13 |
| Windows Server 2016 (64-bit) Platforms .....                  | 10-21 |
| Windows Server 2019 (64-bit) Platforms .....                  | 10-24 |
| Apex One (Mac) Security Agent Installation .....              | 10-26 |
| Apex One (Mac) Security Agent System Requirements .           | 10-26 |

## **Chapter 11: Product Directory**

|   |       |
|---|-------|
| Product Directory .....                                     | 11-2  |
| Connection Status Icons .....                               | 11-4  |
| Viewing Managed Product Status Summaries .....              | 11-5  |
| Performing an Advanced Search of the Product Directory .... | 11-6  |
| Executing Managed Product Tasks .....                       | 11-8  |
| Configuring Managed Product Settings .....                  | 11-9  |
| Querying Logs from the Product Directory .....              | 11-10 |
| Directory Management .....                                  | 11-11 |
| Managing the Product Directory .....                        | 11-13 |
| Recovering Managed Products .....                           | 11-15 |

## **Chapter 12: Component Updates**

|                         |      |
|-------------------------|------|
| Component Updates ..... | 12-2 |
| Component List .....    | 12-2 |
| Update Source .....     | 12-3 |

|  |       |
|--|-------|
| Deployment Plan .....  | 12-3  |
| Adding a Deployment Schedule .....   | 12-4  |
| Configuring Scheduled Update Settings .....  | 12-4  |
| Configuring Manual Update Settings .....   | 12-8  |
| Configuring Proxy Settings for Component/License Updates,<br>Cloud Services, and Syslog Forwarding ..... | 12-12 |

## **Chapter 13: Command Tracking and Product Communication**

|   |      |
|---|------|
| Command Tracking .....                            | 13-2 |
| Querying and Viewing Commands .....               | 13-3 |
| Command Details .....                             | 13-4 |
| Configuring Communication Time-out Settings ..... | 13-4 |

## **Part IV: Policies**

### **Chapter 14: Policy Management**

|  |       |
|--|-------|
| Policy Management .....                        | 14-2  |
| Creating a New Policy .....                    | 14-2  |
| Filtering by Criteria .....                    | 14-5  |
| Assigning Endpoints to Filtered Policies ..... | 14-7  |
| Specifying Policy Targets .....                | 14-8  |
| Working with Parent Policy Settings .....      | 14-10 |
| Copying Policy Settings .....                  | 14-12 |
| Inheriting Policy Settings .....               | 14-14 |
| Modifying a Policy .....                       | 14-15 |
| Importing and Exporting Policies .....         | 14-17 |
| Deleting a Policy .....                        | 14-18 |
| Changing the Policy Owner .....                | 14-19 |
| Understanding the Policy List .....            | 14-20 |
| Reordering the Policy List .....               | 14-23 |
| Policy Status .....                            | 14-24 |

## Chapter 15: Policy Resources

|  |       |
|--|-------|
| Application Control Criteria .....               | 15-2  |
| Defining Allowed Application Criteria .....      | 15-4  |
| Defining Blocked Application Criteria .....      | 15-6  |
| Application Match Methods .....                  | 15-8  |
| Application Reputation List .....                | 15-8  |
| File Paths .....                                 | 15-9  |
| File Path Example Usage .....                    | 15-11 |
| Certificates .....                               | 15-13 |
| Hash Values .....                                | 15-14 |
| Data Loss Prevention .....                       | 15-15 |
| Data Identifier Types .....                      | 15-16 |
| Expressions .....                                | 15-17 |
| Predefined Expressions .....                     | 15-17 |
| Viewing Settings for Predefined Expressions .... | 15-17 |
| Customized Expressions .....                     | 15-18 |
| Criteria for Customized Expressions .....        | 15-18 |
| Creating a Customized Expression .....           | 15-20 |
| Importing Customized Expressions .....           | 15-21 |
| File Attributes .....                            | 15-21 |
| Creating a File Attribute List .....             | 15-22 |
| Importing a File Attribute List .....            | 15-23 |
| Keywords .....                                   | 15-23 |
| Predefined Keyword Lists .....                   | 15-24 |
| How Keyword Lists Work .....                     | 15-24 |
| Number of Keywords Condition .....               | 15-24 |
| Distance Condition .....                         | 15-25 |
| Customized Keyword Lists .....                   | 15-25 |
| Customized Keyword List Criteria .....           | 15-26 |
| Creating a Keyword List .....                    | 15-27 |
| Importing a Keyword List .....                   | 15-29 |
| Data Loss Prevention Templates .....             | 15-29 |
| Predefined DLP Templates .....                   | 15-30 |
| Customized DLP Templates .....                   | 15-30 |
| Condition Statements and Logical Operators ...   | 15-30 |

|  |       |
|--|-------|
| Creating a Template .....                  | 15-31 |
| Importing Templates .....                  | 15-33 |
| Intrusion Prevention Rules .....           | 15-33 |
| Intrusion Prevention Rule Properties ..... | 15-35 |
| Device Control Allowed Devices .....       | 15-37 |

## Part V: Detections

### Chapter 16: Logs

|                                       |       |
|---------------------------------------|-------|
| Log Queries .....                     | 16-2  |
| Querying Logs .....                   | 16-2  |
| Log Names and Data Views .....        | 16-6  |
| Configuring Log Aggregation .....     | 16-14 |
| Configuring Syslog Forwarding .....   | 16-14 |
| Disabling Syslog Forwarding .....     | 16-18 |
| Supported Log Types and Formats ..... | 16-18 |
| Deleting Logs .....                   | 16-20 |

### Chapter 17: Notifications

|  |       |
|--|-------|
| Event Notifications .....                      | 17-2  |
| Notification Method Settings .....             | 17-3  |
| Configuring SMTP Server Settings .....         | 17-4  |
| Configuring SNMP Trap Settings .....           | 17-5  |
| Configuring Syslog Settings .....              | 17-5  |
| Configuring Trigger Application Settings ..... | 17-6  |
| Contact Groups .....                           | 17-6  |
| Adding Contact Groups .....                    | 17-7  |
| Editing Contact Groups .....                   | 17-8  |
| Advanced Threat Activity Events .....          | 17-9  |
| Attack Discovery Detections .....              | 17-9  |
| Behavior Monitoring Violations .....           | 17-11 |

|  |       |
|--|-------|
| C&C Callback Alert .....   | 17-12 |
| C&C Callback Outbreak Alert .....  | 17-13 |
| Correlated Incident Detections .....   | 17-14 |
| Email Messages with Advanced Threats .....                                     | 17-16 |
| High Risk Virtual Analyzer Detections .....                                    | 17-17 |
| High Risk Host Detections .....  | 17-19 |
| Known Targeted Attack Behavior .....   | 17-20 |
| Potential Document Exploit Detections .....                                    | 17-21 |
| Predictive Machine Learning Detections .....                                   | 17-23 |
| Rootkit or Hacking Tool Detections .....                                       | 17-24 |
| SHA-1 Deny List Detections .....   | 17-26 |
| Watchlisted Recipients at Risk .....   | 17-27 |
| Worm or File Infector Propagation Detections .....                             | 17-28 |
| Content Policy Violation Events .....  | 17-30 |
| Email Policy Violation .....   | 17-30 |
| Web Access Security Violation .....  | 17-31 |
| Data Loss Prevention Events .....  | 17-33 |
| Incident Details Updated .....   | 17-33 |
| Scheduled Incident Summary .....   | 17-34 |
| Significant Incident Increase .....  | 17-36 |
| Significant Incident Increase by Channel .....                                 | 17-37 |
| Significant Incident Increase by Sender .....                                  | 17-38 |
| Significant Incident Increase by User .....                                    | 17-39 |
| Significant Template Match Increase .....                                      | 17-40 |
| Known Threat Activity Events .....   | 17-42 |
| Network Virus Alert .....  | 17-42 |
| Special Spyware/Grayware Alert .....   | 17-43 |
| Special Virus Alert .....  | 17-45 |
| Spyware/Grayware Found - Action Successful .....                               | 17-46 |
| Spyware/Grayware Found - Further Action Required ...                           | 17-48 |
| Virus Found - First Action Successful .....                                    | 17-49 |
| Virus Found - First Action Unsuccessful and Second Action<br>Unavailable ..... | 17-51 |
| Virus Found - First and Second Actions Unsuccessful ..                         | 17-52 |
| Virus Found - Second Action Successful .....                                   | 17-53 |

|   |       |
|---|-------|
| Virus Outbreak Alert .....                            | 17-55 |
| Network Access Control Events .....                   | 17-56 |
| Network VirusWall Policy Violations .....             | 17-57 |
| Potential Vulnerability Attacks .....                 | 17-58 |
| Unusual Product Behavior Events .....                 | 17-60 |
| Managed Product Unreachable .....                     | 17-60 |
| Product Service Started .....                         | 17-61 |
| Product Service Stopped .....                         | 17-62 |
| Real-time Scan Disabled .....                         | 17-63 |
| Real-time Scan Enabled .....                          | 17-65 |
| Updates .....   | 17-66 |
| Antispam Rule Update Successful .....                 | 17-66 |
| Antispam Rule Update Unsuccessful .....               | 17-68 |
| Pattern File/Cleanup Template Update Successful ..... | 17-69 |
| Pattern File/Cleanup Template Update Unsuccessful ... | 17-70 |
| Scan Engine Update Successful .....                   | 17-72 |
| Scan Engine Update Unsuccessful .....                 | 17-73 |

## Chapter 18: Reports

|  |       |
|--|-------|
| Reports Overview .....                           | 18-2  |
| Custom Templates .....                           | 18-2  |
| Adding or Editing Custom Templates .....         | 18-3  |
| Configuring the Static Text Report Element ..... | 18-7  |
| Configuring the Bar Chart Report Element .....   | 18-8  |
| Configuring the Line Chart Report Element .....  | 18-11 |
| Configuring the Pie Chart Report Element .....   | 18-13 |
| Configuring the Dynamic Table Report Element ... | 18-16 |
| Configuring the Grid Table Report Element .....  | 18-19 |
| One-time Reports .....                           | 18-20 |
| Creating One-time Reports .....                  | 18-21 |
| Viewing One-Time Reports .....                   | 18-24 |
| Scheduled Reports .....                          | 18-25 |
| Adding Scheduled Reports .....                   | 18-26 |

|                                      |       |
|--------------------------------------|-------|
| Editing Scheduled Reports .....      | 18-31 |
| Viewing Scheduled Reports .....      | 18-35 |
| Configuring Report Maintenance ..... | 18-36 |
| Viewing My Reports .....             | 18-36 |

## **Chapter 19: Data Loss Prevention Incidents**

|   |      |
|---|------|
| Administrator Tasks .....   | 19-2 |
| Setting Up Manager Information in Active Directory Users<br>..... | 19-3 |
| Understanding DLP User Roles .....                                | 19-3 |
| Creating DLP Auditing Logs .....                                  | 19-5 |
| DLP Incident Review Process .....                                 | 19-6 |
| Understanding the Incident Information List .....                 | 19-6 |
| Reviewing Incident Details .....                                  | 19-8 |

## **Part VI: Threat Intelligence and Response**

### **Chapter 20: Connected Threat Defense**

|   |       |
|---|-------|
| About Connected Threat Defense .....                                      | 20-2  |
| Feature Requirements .....  | 20-2  |
| Suspicious Object List Management .....                                   | 20-5  |
| Suspicious Object Lists .....   | 20-6  |
| Adding Exceptions to the Virtual Analyzer Suspicious<br>Object List ..... | 20-7  |
| Suspicious Object Scan Actions .....                                      | 20-9  |
| Configuring Distribution Settings .....                                   | 20-13 |
| Suspicious Object Detection .....   | 20-15 |
| Viewing At Risk Endpoints and Recipients .....                            | 20-15 |
| Analyzing Impact from Virtual Analyzer Suspicious<br>Objects .....        | 20-16 |
| Historical Investigations in Endpoint Sensor ...                          | 20-17 |
| Viewing the Handling Process .....  | 20-18 |



|  |       |
|--|-------|
| Preemptive Protection Against Suspicious Objects .....                             | 20-20 |
| Adding Objects to the User-Defined Suspicious Object List .....                    | 20-21 |
| Importing User-Defined Suspicious Object Lists ....                                | 20-23 |
| Adding STIX Objects to the User-Defined Suspicious Object List .....               | 20-23 |
| Adding OpenIOC Objects to the User-Defined Suspicious Object List .....            | 20-26 |
| Analyzing Impact and Responding to IOCs from User-Defined Suspicious Objects ..... | 20-33 |
| Isolating Endpoints .....  | 20-34 |
| Connected Threat Defense Product Integration .....                                 | 20-37 |
| Apex Central .....   | 20-38 |
| Apex One .....   | 20-39 |
| Apex One Endpoint Sensor .....   | 20-40 |
| Apex One Sandbox as a Service .....  | 20-41 |
| Cloud App Security .....   | 20-42 |
| Deep Discovery Analyzer .....  | 20-42 |
| Deep Discovery Director .....  | 20-43 |
| Deep Discovery Email Inspector .....   | 20-43 |
| Deep Discovery Inspector .....   | 20-44 |
| Deep Discovery Web Inspector .....   | 20-45 |
| Deep Security Manager .....  | 20-45 |
| Email Security .....   | 20-46 |
| InterScan Messaging Security Virtual Appliance .....                               | 20-46 |
| InterScan Web Security Virtual Appliance .....                                     | 20-47 |
| ScanMail for Microsoft Exchange .....  | 20-47 |
| Smart Protection Server .....  | 20-48 |
| Endpoint Application Control .....   | 20-49 |
| Web Security .....   | 20-49 |

## **Chapter 21: Threat Investigation**

|                                     |      |
|-------------------------------------|------|
| Threat Investigation Overview ..... | 21-2 |
| Endpoint Sensor Metadata .....      | 21-2 |

|  |       |
|--|-------|
| Historical Investigations .....                              | 21-3  |
| Using User-defined Criteria for Historical Investigations    | 21-5  |
| Supported Formats for User-defined Criteria .....            | 21-10 |
| Using OpenIOC files for a Historical Investigation .....     | 21-13 |
| Supported IOC Indicators for Historical Investigations ..... | 21-17 |
| Starting a Root Cause Analysis from an Assessment .....      | 21-18 |
| Root Cause Analysis Results .....                            | 21-20 |
| Live Investigations .....                                    | 21-23 |
| Starting a One-time Investigation .....                      | 21-25 |
| One-Time Investigation .....                                 | 21-26 |
| Starting a Scheduled Investigation .....                     | 21-28 |
| Scheduled Investigation .....                                | 21-29 |
| Reviewing the Scheduled Investigation History .....          | 21-31 |
| Supported IOC Indicators for Live Investigations .....       | 21-32 |
| Investigation Results .....                                  | 21-33 |
| Analysis Chains .....  | 21-35 |
| Object Details: Profile Tab .....                            | 21-38 |
| Object Details: Related Objects Tab .....                    | 21-39 |
| Navigating the Analysis Chain .....                          | 21-40 |
| Root Cause Analysis Icons .....                              | 21-41 |
| Object Details .....   | 21-43 |

## Chapter 22: Managed Detection and Response

|   |       |
|---|-------|
| Managed Detection and Response Overview .....                           | 22-2  |
| Registering Apex Central to the Threat Investigation Center .....       | 22-3  |
| Unregistering from the Threat Investigation Center Server .....         | 22-5  |
| Suspending or Resuming the Managed Detection and Response Service ..... | 22-6  |
| Approving or Rejecting Investigation Tasks .....                        | 22-7  |
| Threat Investigation Center Task Commands .....                         | 22-10 |
| Endpoint Sensor Service Statuses .....                                  | 22-11 |
| Tracking Investigation Tasks .....                                      | 22-12 |
| Threat Investigation Center Task Statuses .....                         | 22-13 |

|   |       |
|---|-------|
| Threat Investigation Center Command Statuses ....                                 | 22-14 |
| Viewing Automated Analyses .....  | 22-15 |
| Tracking Managed Detection and Response Task Commands                             | 22-16 |
| Command Details .....   | 22-18 |
| Querying Supported Targets .....  | 22-18 |
| The Threat Investigation Center Agent for Managed Detection<br>and Response ..... | 22-20 |

## **Chapter 23: Suspicious Object Hub and Node Architecture**

|   |      |
|---|------|
| Suspicious Object Hub and Node Apex Central Servers .....                 | 23-2 |
| Configuring the Suspicious Object Hub and Nodes .....                     | 23-3 |
| Unregistering a Suspicious Object Node from the Hub Apex<br>Central ..... | 23-4 |
| Configuration Notes .....   | 23-5 |

## **Part VII: Automation Center**

### **Chapter 24: Apex Central Automation Center**

## **Part VIII: Tools and Support**

### **Chapter 25: Administering the Database**

|   |       |
|---|-------|
| Understanding the Apex Central Database .....                               | 25-2  |
| Understanding the db_ApexCentral Tables .....                               | 25-4  |
| Backing Up db_ApexCentral Using SQL Server Management<br>Studio .....       | 25-9  |
| Restoring Backup db_ApexCentral Using SQL Server<br>Management Studio ..... | 25-10 |
| Shrinking db_ApexCentral_Log.ldf Using SQL Commands .                       | 25-11 |

|   |       |
|---|-------|
| Shrinking db_ApexCentral_log.ldf Using SQL Server<br>Management Studio .....                    | 25-12 |
| Shrinking the db_ApexCentral_log.ldf File Size on Microsoft<br>SQL Server 2008 (or later) ..... | 25-12 |

## **Chapter 26: Apex Central Tools**

|   |      |
|---|------|
| About Apex Central Tools .....                              | 26-2 |
| Using the Agent Migration Tool (AgentMigrateTool.exe) ..... | 26-2 |
| Using the Database Configuration Tool (DBConfig.exe) .....  | 26-2 |

## **Chapter 27: Technical Support**

|   |      |
|---|------|
| Troubleshooting Resources .....                 | 27-2 |
| Using the Support Portal .....                  | 27-2 |
| Threat Encyclopedia .....                       | 27-2 |
| Contacting Trend Micro .....                    | 27-3 |
| Speeding Up the Support Call .....              | 27-3 |
| Sending Suspicious Content to Trend Micro ..... | 27-4 |
| Email Reputation Services .....                 | 27-4 |
| File Reputation Services .....                  | 27-4 |
| Web Reputation Services .....                   | 27-5 |
| Other Resources .....                           | 27-5 |
| Download Center .....                           | 27-5 |
| Documentation Feedback .....                    | 27-5 |

## **Appendices**

### **Appendix A: Apex Central System Checklists**

|  |     |
|--|-----|
| Server Address Checklist .....               | A-2 |
| Port Checklist .....                         | A-3 |
| Apex Central Conventions .....               | A-3 |
| Core Processes and Configuration Files ..... | A-4 |

|   |     |
|---|-----|
| Communication and Listening Ports ..... | A-6 |
|---|-----|

## **Appendix B: Data Views**

|   |      |
|---|------|
| Data View: Security Logs .....  | B-2  |
| Advanced Threat Information .....                                       | B-2  |
| Detailed C&C Callback Information .....                                 | B-2  |
| Detailed Predictive Machine Learning Information ..                     | B-3  |
| Detailed Suspicious File Information .....                              | B-5  |
| Virtual Analyzer Detection Information .....                            | B-6  |
| Detailed Virtual Analyzer Suspicious Object Impact<br>Information ..... | B-7  |
| Attack Discovery Detections .....                                       | B-10 |
| Attack Discovery Detection Information .....                            | B-10 |
| Detailed Attack Discovery Detection Information ...                     | B-11 |
| Content Violation Information .....                                     | B-13 |
| Content Violation Action/Result Summary .....                           | B-14 |
| Content Violation Detection Over Time Summary ...                       | B-14 |
| Content Violation Policy Summary .....                                  | B-15 |
| Content Violation Sender Summary .....                                  | B-16 |
| Detailed Content Violation Information .....                            | B-17 |
| Email Messages with Advanced Threats .....                              | B-18 |
| Data Discovery Information .....  | B-19 |
| Data Discovery Data Loss Prevention Detection<br>Information .....      | B-20 |
| Data Discovery Endpoint Information .....                               | B-20 |
| Data Loss Prevention Information .....                                  | B-21 |
| DLP Incident Information .....  | B-21 |
| DLP Template Match Information .....                                    | B-23 |
| Deep Discovery Information .....  | B-24 |
| Detailed Correlation Information .....                                  | B-24 |
| Detailed Mitigation Information .....                                   | B-25 |
| Detailed Suspicious Threat Information .....                            | B-26 |
| Overall Suspicious Threat Summary .....                                 | B-30 |
| Suspicious Source Summary .....   | B-32 |
| Suspicious Riskiest Endpoints Summary .....                             | B-32 |
| Suspicious Riskiest Recipient Summary .....                             | B-33 |
| Suspicious Sender Summary .....   | B-34 |

|  |      |
|--|------|
| Suspicious Threat Protocol Detection Summary .....     | B-35 |
| Suspicious Threat Detection Over Time Summary ..       | B-36 |
| Gray Detection Information .....                       | B-38 |
| Overall Threat Information .....                       | B-38 |
| Network Protection Boundary Information .....          | B-39 |
| Network Security Threat Analysis Information .....     | B-40 |
| Security Threat Endpoint Analysis Information .....    | B-41 |
| Security Threat Entry Analysis Information .....       | B-41 |
| Security Threat Source Analysis Information .....      | B-42 |
| Policy/Rule Violation Information .....                | B-43 |
| Device Access Control Information .....                | B-43 |
| Detailed Application Activity .....                    | B-44 |
| Detailed Application Control Violation Information     | B-46 |
| Detailed Behavior Monitoring Information .....         | B-48 |
| Detailed Endpoint Security Compliance Information .... | B-49 |
| Detailed Endpoint Security Violation Information ..    | B-50 |
| Detailed Firewall Violation Information .....          | B-51 |
| Detailed Intrusion Prevention Information .....        | B-52 |
| Integrity Monitoring Information .....                 | B-54 |
| Network Content Inspection Information .....           | B-54 |
| Spam Violation Information .....                       | B-55 |
| Detailed Spam Information .....                        | B-55 |
| Overall Spam Violation Summary .....                   | B-56 |
| Spam Connection Information .....                      | B-57 |
| Spam Detection Over Time Summary .....                 | B-58 |
| Spam Recipient Summary .....                           | B-58 |
| Spyware/Grayware Information .....                     | B-59 |
| Detailed Spyware/Grayware Information .....            | B-59 |
| Endpoint Spyware/Grayware .....                        | B-61 |
| Endpoint Spyware/Grayware Summary .....                | B-62 |
| Email Spyware/Grayware .....                           | B-63 |
| Network Spyware/Grayware .....                         | B-65 |
| Overall Spyware/Grayware Summary .....                 | B-66 |
| Spyware/Grayware Action/Result Summary .....           | B-67 |
| Spyware/Grayware Detection Over Time Summary .         | B-68 |
| Spyware/Grayware Source Summary .....                  | B-69 |

|   |       |
|---|-------|
| Web Spyware/Grayware .....                        | B-70  |
| Virus/Malware Information .....                   | B-71  |
| Detailed Virus/Malware Information .....          | B-72  |
| Endpoint Virus/Malware Information .....          | B-73  |
| Email Virus/Malware Information .....             | B-75  |
| Network Virus/Malware Information .....           | B-76  |
| Overall Virus/Malware Summary .....               | B-78  |
| Virus/Malware Action/Result Summary .....         | B-79  |
| Virus/Malware Detection Over Time Summary .....   | B-80  |
| Virus/Malware Endpoint Summary .....              | B-81  |
| Virus/Malware Source Summary .....                | B-81  |
| Web Virus/Malware Information .....               | B-82  |
| Web Violation/Reputation Information .....        | B-83  |
| Detailed Web Reputation Information .....         | B-84  |
| Detailed Web Violation Information .....          | B-86  |
| Overall Web Violation Summary .....               | B-88  |
| Web Violation Detection Over Time Summary .....   | B-89  |
| Web Violation Detection Summary .....             | B-90  |
| Web Violation Endpoint Summary .....              | B-91  |
| Web Violation Filter/Blocking Type Summary .....  | B-92  |
| Web Violation URL Summary .....                   | B-93  |
| Data View: Product Information .....              | B-93  |
| Apex Central Information .....                    | B-93  |
| Apex Central Event Information .....              | B-94  |
| Command Tracking Information .....                | B-94  |
| Detailed Command Tracking Information .....       | B-95  |
| Unmanaged Endpoint Information .....              | B-95  |
| User Access Information .....                     | B-96  |
| Component Information .....                       | B-96  |
| Endpoint Pattern/Engine Status Summary .....      | B-96  |
| Endpoint Pattern/Rule Update Status Summary ..... | B-97  |
| Engine Status .....                               | B-98  |
| Pattern/Rule Status .....                         | B-99  |
| Pattern File/Rule Status Summary .....            | B-101 |
| Product Component Deployment .....                | B-102 |
| Scan Engine Status Summary .....                  | B-103 |

|  |       |
|--|-------|
| License Information .....                  | B-104 |
| Detailed Product License Information ..... | B-104 |
| Product License Information Summary .....  | B-105 |
| Product License Status .....               | B-106 |
| Managed Product Information .....          | B-106 |
| Product Auditing Event Log .....           | B-106 |
| Product Distribution Summary .....         | B-107 |
| Product Event Information .....            | B-108 |
| Product Status Information .....           | B-109 |

### **Appendix C: Token Variables**

|   |      |
|---|------|
| Standard Token Variables .....                    | C-2  |
| Advanced Threat Activity Token Variables .....    | C-2  |
| Attack Discovery Token Variables .....            | C-5  |
| C&C Callback Token Variables .....                | C-6  |
| Content Policy Violation Token Variables .....    | C-8  |
| Data Loss Prevention Token Variables .....        | C-9  |
| Known Threat Activity Token Variables .....       | C-11 |
| Network Access Control Token Variables .....      | C-14 |
| Web Access Policy Violation Token Variables ..... | C-14 |

### **Appendix D: IPv6 Support**

|   |     |
|---|-----|
| Apex Central Server Requirements .....  | D-2 |
| IPv6 Support Limitations .....          | D-2 |
| Configuring IPv6 Addresses .....        | D-2 |
| Screens That Display IP Addresses ..... | D-3 |

### **Appendix E: MIB Files**

|  |     |
|--|-----|
| Using the Apex Central MIB File .....        | E-2 |
| Using the NVW Enforcer SNMPv2 MIB File ..... | E-2 |



## Appendix F: Syslog Content Mapping - CEF

|  |      |
|--|------|
| CEF Attack Discovery Detection Logs .....      | F-3  |
| CEF Behavior Monitoring Logs .....             | F-9  |
| CEF C&C Callback Logs .....                    | F-15 |
| CEF Content Security Logs .....                | F-20 |
| Filter Action Mapping Table .....              | F-25 |
| Filter Action Result Mapping Table .....       | F-26 |
| CEF Data Loss Prevention Logs .....            | F-28 |
| Action Result Mapping Table .....              | F-32 |
| Channel Mapping Table .....                    | F-34 |
| CEF Device Access Control Logs .....           | F-36 |
| Product ID Mapping Table .....                 | F-38 |
| CEF Endpoint Application Control Logs .....    | F-43 |
| CEF Engine Update Status Logs .....            | F-46 |
| CEF Intrusion Prevention Logs .....            | F-48 |
| CEF Managed Product Logon/Logoff Events .....  | F-51 |
| CEF Network Content Inspection Logs .....      | F-52 |
| CEF Pattern Update Status Logs .....           | F-56 |
| CEF Predictive Machine Learning Logs .....     | F-59 |
| Threat Type Mapping Table .....                | F-63 |
| CEF Product Auditing Events .....              | F-64 |
| CEF Sandbox Detection Logs .....               | F-65 |
| CEF Spyware/Grayware Logs .....                | F-69 |
| Action Mapping Table .....                     | F-73 |
| Spyware/Grayware Scan Type Mapping Table ..... | F-75 |
| Spyware/Grayware Risk Type Mapping Table ..... | F-76 |
| CEF Suspicious File Logs .....                 | F-77 |
| CEF Virus/Malware Logs .....                   | F-81 |
| Second Action Mapping Table .....              | F-85 |

|  |      |
|--|------|
| CEF Web Security Logs .....              | F-86 |
| Filter/Blocking Type Mapping Table ..... | F-91 |
| Protocol Mapping Table .....             | F-93 |

## **Index**

|             |      |
|-------------|------|
| Index ..... | IN-1 |
|-------------|------|





# Preface

## Preface


This document introduces Trend Micro Apex Central™ and discusses getting started information, managed product integration, and security monitoring details.

Topics in this section:

- *[Documentation on page 2](#)*
- *[Audience on page 3](#)*
- *[Document Conventions on page 3](#)*
- *[Terminology on page 4](#)*

## Documentation

Apex Central documentation includes the following:

| DOCUMENT                               | DESCRIPTION   |
|--|---|
| Readme file                            | Contains a list of known issues and may also contain late-breaking product information not found in the Online Help or printed documentation  |
| Installation and Upgrade Guide         | <p>A PDF document that discusses requirements and procedures for installing the Apex Central</p> <hr/> <p> <b>Note</b><br/>The Installation and Upgrade Guide may not be available for minor release versions, service packs, or patches.</p> <hr/>  |
| System Requirements                    | A PDF document that discusses requirements and procedures for installing Apex Central   |
| Administrator's Guide                  | A PDF document that provides detailed instructions of how to configure and manage Apex Central and managed products, and explanations on Apex Central concepts and features   |
| Online Help                            | HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is also accessible from the Apex Central console  |
| Widget and Policy Management Guide     | <p>Contains information that explains how to configure dashboard widgets and policy management settings in Apex Central</p> <p>To access this guide, go to <a href="https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-widget-and-policy-management-guide/preface-(wpg)_001.aspx">https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-widget-and-policy-management-guide/preface-(wpg)_001.aspx</a>.</p> |
| Automation Center                      | Online user guides and references that explain how to use the Apex Central Automation APIs: <a href="https://automation.trendmicro.com/apex-central/home">https://automation.trendmicro.com/apex-central/home</a>   |
| Data Protection Lists (Chapter 1 only) | A PDF document that lists predefined data identifiers and templates for Data Loss Prevention  |

| DOCUMENT       | DESCRIPTION  |
|----------------|--|
| Knowledge Base | An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: <a href="http://success.trendmicro.com">http://success.trendmicro.com</a> |

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

<http://docs.trendmicro.com/en-us/enterprise/apex-central.aspx>

## Audience

Apex Central documentation is intended for the following users:





- **Apex Central Administrators:** Responsible for Apex Central installation, configuration, and management. These users are expected to have advanced networking and server management knowledge.
- **Managed Product Administrators:** Users who manage Trend Micro products that integrate with Apex Central. These users are expected to have advanced networking and server management knowledge.

## Document Conventions

The documentation uses the following conventions.

**TABLE 1. Document Conventions**

| CONVENTION     | DESCRIPTION   |
|----------------|---|
| UPPER CASE     | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| <b>Bold</b>    | Menus and menu commands, command buttons, tabs, and options                     |
| <i>Italics</i> | References to other documents   |
| Monospace      | Sample command lines, program code, web URLs, file names, and program output    |


| CONVENTION   | DESCRIPTION   |
|--|---|
| <b>Navigation &gt; Path</b>  | The navigation path to reach a particular screen<br><br>For example, <b>File &gt; Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface |
|  <b>Note</b>      | Configuration notes   |
|  <b>Tip</b>       | Recommendations or suggestions  |
|  <b>Important</b> | Information regarding required or default configuration settings and product limitations  |
|  <b>WARNING!</b>  | Critical actions and configuration options  |

## Terminology

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

| TERMINOLOGY                                   | DESCRIPTION  |
|---|--|
| Administrator (or Apex Central administrator) | The person managing the Apex Central server                                    |
| Security Agent                                | The managed product program installed on an endpoint                           |
| Components                                    | Responsible for scanning, detecting, and taking actions against security risks |



| TERMINOLOGY  | DESCRIPTION   |
|--|---|
| Apex Central console, web console, or management console | <p>The web-based user interface for accessing, configuring, and managing a Apex Central</p> <hr/> <p> <b>Note</b><br/>Consoles for integrated managed products are indicated by the managed product name. For example, the Apex One web console.</p> <hr/> |
| Managed endpoint   | The endpoint where the managed product Security Agent is installed  |
| Managed product  | A Trend Micro product that integrates with Apex Central   |
| Managed server   | The endpoint where the managed product is installed   |
| Server   | The endpoint where the Apex Central server is installed   |
| Security risk  | The collective term for virus/malware, spyware/grayware, and web threats  |
| Dual-stack   | Entities that have both IPv4 and IPv6 addresses   |
| Pure IPv4  | An entity that only has an IPv4 address   |
| Pure IPv6  | An entity that only has an IPv6 address   |



# **Part I**

## **Introduction**





# Chapter 1

## Introducing Apex Central

This section introduces Trend Micro Apex Central™ and provides an overview of its features and capabilities.

Topics include:

- *About Apex Central on page 1-2*
- *What's New on page 1-2*
- *Key Features and Benefits on page 1-5*
- *Apex Central Architecture on page 1-7*


## About Apex Central

Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility.

## What's New

This version of Apex Central includes the following new features and enhancements.

| FEATURE                      | DESCRIPTION  |
|------------------------------|--|
| Trend Vision One integration | <p data-bbox="380 954 1069 1032">This release of Apex Central enables managed Apex One servers to send server configuration information to Trend Vision One to enhance product integration.</p> <hr data-bbox="380 1068 1092 1071"/> <p data-bbox="380 1084 1056 1179"> <b>Note</b><br/>This feature requires the installation of Apex One Service Pack 1 Patch 1 or above.</p> |

**TABLE 1-1. Previous Updates**

| FEATURE   | DESCRIPTION  |
|---|--|
| Trend Vision One integration                      | Integration with Trend Vision One allows Apex Central to forward detection events and managed Security Agent information to Trend Vision One for correlated detection and other advanced analytics.  |
| Enhancement Security Agent management             | This release of Apex Central supports multi-layer domain tree (up to five layers) for managed servers to enhance Security Agent management.  |
| New platform                                      | Apex Central supports installation on Windows Server 2022.   |
| Event Notifications                               | <p>The following Event Notification settings have been disabled to prevent too many unnecessary notifications from being sent to recipients (<b>Detections &gt; Notifications &gt; Event Notifications &gt; Advanced Threat Activity</b>):</p> <ul style="list-style-type: none"> <li>• C&amp;C callback alert</li> <li>• C&amp;C callback outbreak alert</li> <li>• Correlated incident detections</li> </ul> |
| Additional Advanced Threat Activity notifications | Apex Central supports Advanced Threat Activity event notifications for Behavior Monitoring violations and Predictive Machine Learning detections.  |
| Advanced Logging Policy optimization              | The Advanced Logging Policy for Apex One Vulnerability Protection ( <b>Policies &gt; Policy Management &gt; Apex One Security Agent &gt; Vulnerability Protection Settings &gt; Network Engine Settings</b> ) uses "Stateful, Frag, and Verifier Suppression" by default to exclude fragmentation and verifier related events.   |
| Concurrent session limitation                     | Apex Central allows administrators to prevent multiple web console sessions per user account.  |
| Critical event auditing                           | The Apex One server and Security Agents collect Windows event logs related to critical system events (move Security Agent, uninstall Security Agent, reset password) and sends the logs to Apex Central Product Auditing Event logs.   |

| FEATURE                         | DESCRIPTION   |
|---------------------------------|---|
| Dashboard enhancements          | <ul style="list-style-type: none"> <li>The name of the <b>Operation Center</b> tab has changed to <b>Security Posture</b>, the name of the <b>Threat Detection</b> tab has changed to <b>Threat Statistics</b>, and the widgets on the former <b>DLP Incident Investigation</b> tab have moved to the <b>Data Loss Prevention</b> tab.</li> <li>Toggle the <b>Table</b> view on the <b>Security Posture</b> dashboard tab to display the chart nodes, critical threats, and antivirus pattern compliance information in a table.</li> </ul>   |
| Enhanced API integration        | <p>Apex Central provides APIs for forwarding detection logs in CEF format, Product Auditing Events, Security Agent pattern update statuses, or Security Agent engine update statuses to SIEM servers.</p> <p>For more information, see <a href="https://automation.trendmicro.com/apex-central/home">https://automation.trendmicro.com/apex-central/home</a>.</p>   |
| Impact Analysis enhancement     | <p>The <b>Affected Users</b> screen automatically refreshes every 60 seconds when running an Impact Analysis.</p>   |
| New dashboard widgets           | <ul style="list-style-type: none"> <li>The <b>Quick Investigation</b> widget allows you to start Historical Investigations directly from the dashboard.</li> <li>Use the <b>Attack Discovery Detections</b> widget to view detection logs generated by the Endpoint Sensor Attack Discovery feature.<br/><br/>Attack Discovery logs include MITRE™ Tactics and Techniques information and Windows Antimalware Scan Interface (AMSI) data.</li> <li>The <b>Top Endpoints Affected by IPS Events</b>, <b>Top IPS Attack Sources</b>, and <b>Top IPS Events</b> widgets provide greater visibility for Intrusion Prevention events on your network.</li> </ul> |
| Password complexity enhancement | <ul style="list-style-type: none"> <li>Apex Central user accounts have stronger password complexity requirements.</li> <li>The Unload and Uninstall Security Agent features include enhanced password complexity requirements for better security.</li> </ul>   |
| Policy inheritance              | <p>Enhancements to Behavior Monitoring, Predictive Machine Learning, and the Trusted Program List policies allow for policy inheritance support.</p>  |
| SQL Server support              | <p>Apex Central supports Microsoft SQL Server 2019 Cumulative Update 4 (CU4) and SQL Server Express CU4.</p>  |



| FEATURE               | DESCRIPTION   |
|-----------------------|---|
| Syslog enhancements   | <ul style="list-style-type: none"> <li>Apex Central allows you to forward Intrusion Prevention and Product Auditing Event logs to a syslog server.</li> <li>Common Event Format (CEF) syslogs indicate the type of critical threat detected.</li> </ul> |
| Vulnerability patches | Apex Central has patched Cross Site Scripting (XSS) and SQL injection vulnerabilities.  |
| Web browser support   | Apex Central supports Microsoft Edge (Chromium).  |

## Key Features and Benefits

Apex Central provides the following features and benefits.

| FEATURE                      | BENEFITS   |
|------------------------------|--|
| Active Directory integration | Apex Central supports integration with multiple Active Directory forests and allows you to import Active Directory groups in addition to users. You can also enable Active Directory authentication to allow users or groups from federated business partners across an extranet to securely log on to the Apex Central console. |
| Dashboard                    | Use the <b>Dashboard</b> tabs and widgets for extensive visibility of managed product and Apex Central information about threat detections, component statuses, policy violations, and more.   |
| Security Posture             | Use the <b>Security Posture</b> tab to gain instant insights into the antivirus pattern and Data Loss Prevention compliance status, critical threat detections, as well as resolved and unresolved events on your network.   |
| User/Endpoint Directory      | View detailed information about all the users and endpoints within the Apex Central network and any security threat detections.  |
| Product Directory            | System administrators can immediately deploy configuration modifications to managed products or even run a manual scan from the Apex Central web console during a virus/malware outbreak.  |

| <b>FEATURE</b>                      | <b>BENEFITS</b>   |
|-------------------------------------|---|
| Global Policy Management            | System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console to ensure consistent enforcement of your organization's virus/malware and content security policies. |
| Logs                                | Use a single management console to view consolidated logs from all registered managed products without having to log on to each individual product console.   |
| Event Notifications                 | Keep administrators informed of network events at all times by configuring Apex Central to send notifications by email, Windows syslog, SNMP trap, or an in-house or industry-standard application used by your organization.                           |
| Reports                             | Create comprehensive reports from custom or static templates to obtain the actionable information you need to ensure network protection and security compliance.  |
| Component Updates                   | Securely download and deploy antivirus patterns, antispam 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.   |
| Secure communication infrastructure | Apex Central uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol and can even encrypt messages with authentication.  |
| Role-based Administration           | Grant and control access to the Apex Central web console by assigning specific web console 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 using the Apex Central web console, such as antivirus pattern updates and component deployment, have successfully completed.  |
| License management                  | Deploy new Activation Codes or reactivate existing Activation Codes on managed products.  |

| FEATURE                     | BENEFITS  |
|-----------------------------|---|
| Security Agent installation | Download Security Agent installation packages for Apex One or Apex One (Mac) directly from the Apex Central console.  |
| Two-Factor Authentication   | Two-Factor Authentication provides extra security on user accounts by requiring users to type the verification code generated by the Google Authenticator app in order to sign in to Apex Central.  |
| Browser support             | This version of Apex Central includes support for the following: <ul data-bbox="548 477 857 630" style="list-style-type: none"><li>• Microsoft™ Internet Explorer™</li><li>• Microsoft™ Edge™</li><li>• Microsoft™ Edge™ (Chromium)</li><li>• Google™ Chrome™</li></ul> |

## Apex Central Architecture

Trend Micro Apex Central™ provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy.

The following table describes the components that Apex Central uses.

| COMPONENT                                     | DESCRIPTION  |
|---|--|
| Apex Central server                           | <p>Acts as a repository for all data collected from the agents. The Apex Central server includes the following features:</p> <ul style="list-style-type: none"> <li>• An SQL database that stores managed product configurations and logs</li> </ul> <p>Apex Central uses the Microsoft SQL Server database (db_ApexCentral.mdf) to store data included in logs, managed product information, user account, network environment, and notification settings.</p> <ul style="list-style-type: none"> <li>• A web server that hosts the Apex Central web console</li> <li>• A mail client that delivers event notifications through email messages</li> </ul> <p>Apex Central can send notifications to individuals or groups of recipients about events that occur on the Apex Central network. Send event notifications by email, SNMP trap, syslog, or any in-house/industry standard application used by your organization to send notifications.</p> <ul style="list-style-type: none"> <li>• A report server that generates antivirus and content security product reports</li> </ul> <p>The Apex Central report is an online collection of figures about security threat and content security events that occur on the Apex Central network.</p> |
| Trend Micro Management Communication Protocol | <p>MCP handles the Apex Central server interaction with managed products that support the next generation agent.</p> <p>MCP agents install with managed products and use one/two way communication to communicate with Apex Central. MCP agents poll Apex Central for instructions and updates.</p>  |
| Web Service Integration communication         | <p>An agent-less integration model that allows Apex Central to communicate with managed products</p>   |

| <b>COMPONENT</b>             | <b>DESCRIPTION</b>   |
|------------------------------|--|
| Web-based management console | <p>Allows an administrator to manage Apex Central from virtually any computer with an Internet connection and web browser</p> <p>The Apex Central management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Apex Central server. It lets you administer the Apex Central network from any computer using a compatible web browser.</p> |
| Widget Framework             | Allows an administrator to create a customized dashboard to monitor the Apex Central network.  |



# **Part II**

## **Getting Started**







# Chapter 2

## The Web Console

This section discusses how to access and configure the Apex Central web-based management console.

Topics include:

- *[About the Web Console on page 2-2](#)*
- *[Assigning HTTPS Access to the Web Console on page 2-3](#)*
- *[Accessing the Web Console on page 2-5](#)*
- *[Configuring Web Console Settings on page 2-7](#)*

## About the Web Console

The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console lets you administer the Apex Central network from any machine using a compatible web browser.




### Note

View the web console at a screen resolution of 1366 x 768 pixels.

Apex Central supports the following web browsers:

- Microsoft Internet Explorer™ 11
- Microsoft Edge™
- Microsoft Edge™ (Chromium)
- Google Chrome™

## Web Console Requirements

| RESOURCE             | REQUIREMENT   |
|----------------------|---|
| Processor            | 300 MHz Intel™ Pentium™ processor or equivalent   |
| RAM                  | 128 MB minimum  |
| Available disk space | 30 MB minimum   |
| Browser              | <p>Microsoft Internet Explorer™ 11, Microsoft Edge™, Microsoft Edge™ (Chromium), or Google Chrome™</p> <hr/> <p> <b>Important</b><br/>When using Internet Explorer to access the Apex Central web console, turn off <b>Compatibility View</b>.</p> |

| RESOURCE | REQUIREMENT   |
|----------|---|
| Others   | Monitor that supports 1366 x 768 resolution at 256 colors or higher |

## Assigning HTTPS Access to the Web Console

During Apex Central installation, you can choose the level of security when accessing the management console. The least secure level only requires an HTTP connection. The most secure requires an HTTPS connection. If the least secure connection was selected during installation, you can change the access level after installation to the most secure connection.



### Important

- You must obtain a certificate and set up the Apex Central virtual directory before you can start sending encrypted or digitally signed information to and from the Apex Central server.
- The following procedure describes how to assign HTTPS access from a Windows Server 2012 R2 installation.

If you are running a different version of Windows Server, refer to the Microsoft documentation for your specific Windows Server installation.

### Procedure

1. Obtain a Web Site Certificate from any certification provider (for example, Thawte.com or VeriSign.co).
2. Log on to the Apex Central server.
3. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

The **Internet Information Services (IIS) Manager** screen appears.

4. From the **Connections** pane on the left, select the server name.
5. From the **Features View** pane in the center, double-click **Server Certificates**.

6. From the **Actions** pane on the right, click **Import...**

The **Import Certificate** screen appears.

7. Import the Web Site Certificate obtained in step 1:
  - a. Upload the certificate file.
  - b. Specify the password for the certificate.
  - c. Select the Certificate Store.
  - d. Click **OK**.

Windows Server imports the certificate file and closes the **Import Certificate** screen.

8. From the **Connections** pane on the right, expand the **Sites** folder and select the **<Web Site>** created during Apex Central installation.



**Note**

If you did not specify a custom **<Web Site>** name during Apex Central installation, the default **<Web Site>** name is **Default Web Site**.

---

9. Right-click the **<Web Site>** and select **Edit Bindings...**

The **Site Bindings** screen appears.

10. Configure site bindings:
  - a. Select the **https** type and click **Edit...**



**Tip**

If the **https** type does not appear in the **Site Bindings** list, click **Add...** to manually add the **https** type.

---

- b. Select the imported certificate file from the **SSL certificate** drop-down list.
  - c. Click **OK**.
  - d. Click **Close**.

---

**11.** Configure SSL settings:

- a. Expand the **<Web Site>** and select the **WebApp** virtual directory.
- b. From the **Features View** pane in the center, double-click **SSL Settings**.
- c. Select **Require SSL**.
- d. From the **Actions** pane on the right, click **Apply**.

The **Alerts** pane appears and indicates that the changes have been successfully saved.

**12.** Specify the HTTPS port number in the following locations:

- Registry key:

HKLM\Software\Wow6432Node\TrendMicro\TVCS\WebPort

- System configuration file:

In the **<Apex Central installation folder>** \systemconfiguration.xml file, locate m\_uiWebServer\_Https\_Port and set the value to the HTTPS port number.

**13.** Restart the following services:

- Trend Micro Apex Central
  - Trend Micro Management Infrastructure
  - W3WP
- 

## Accessing the Web Console

Log on to the Apex Central console from the Apex Central server or from any endpoint with Internet access and a supported web browser.

**Note**

- You cannot use the same user account to log onto the Apex Central management console from multiple browsers on the same endpoint.
  - You can use the same user account to log onto the Apex Central management console from different endpoints.
- 

**Procedure**

1. Access the Apex Central management console locally or remotely.
  - To access the console locally, on the Apex Central server, go to **Start > Programs > Trend Micro Apex Central > Trend Micro Apex Central**.
  - To access the console remotely, open a web browser and go the following address:

`http(s)://<host name>/WebApp/login.html`

Where <host name> is the fully qualified domain name (FQDN), IP address, or server name of the Apex Central server.

The **Log On** screen appears.

2. Provide logon credentials.
  - To log on using Apex Central account credentials, type the user name and password.
  - To log on with domain credentials, type the domain and user name in the following format, and then type the password.

`domain\user_name`

---

**Note**

Logging on with domain credentials requires an integrated Active Directory structure.

For more information, contact your Active Directory administrator.

---

---

### 3. Click **Log On**.

**Note**

If your administrator enabled Two-Factor Authentication, follow the on-screen prompts.

For more information on setting up Two-Factor Authentication, contact your administrator.

---

### 4. (Optional) When logging on with domain credentials, you can store the credentials for future use by clicking the **Log On with Domain Credentials** button.

**Note**

The **Log On with Domain Credentials** button only displays if the administrator added the Apex Central server to the Active Directory domain on the Active Directory server.

---

Apex Central prompts you to provide your domain credentials and confirm the automatic logon. The next time you access the console, click **Log On with Domain Credentials** to log on automatically.

### 5. To log off from the web console, go to the top right corner of the web console and click <account\_name> > **Log Off**.

---

## Configuring Web Console Settings

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

---

### Procedure

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

The **Web Console Settings** screen appears.

## 2. Configure the required settings.

| SECTION                       | SETTINGS  |
|-------------------------------|---|
| Web Console Auto Refresh      | Select <b>Enable Auto Refresh</b> to enable the Apex Central server to refresh screen data at the specified interval <ul style="list-style-type: none"><li>• <b>Refresh the web console every _ seconds:</b> Select the frequency (in seconds) in which the web console refreshes the screen data</li></ul>   |
| Web Console Timeout           | Select <b>Enable automatic log out from the web console</b> to enable the Apex Central server to log off users at the specified interval <ul style="list-style-type: none"><li>• <b>Automatically log out of the web console after _ minutes:</b> Select the period of inactivity (in minutes) in which the web console automatically logs off users</li></ul>  |
| Security Settings             | Select <b>Automatically lock user accounts after unsuccessful logon attempts</b> to enable the Apex Central server to lock user accounts after the specified number of unsuccessful logon attempts <ul style="list-style-type: none"><li>• <b>Consecutive unsuccessful attempts:</b> Specify the number of unsuccessful logon attempts</li><li>• <b>Account lock duration:</b> Specify the amount of time (in minutes) to lock the user account</li></ul> |
| Concurrent Session Limitation | Select <b>Enforce one session per account</b> to prevent multiple web console logon sessions for the same user account  |

## 3. Click **Save**.

---



# Chapter 3

## The Dashboard

This section discusses how to use the Apex Central dashboard tabs and widgets.

Topics include:

- *About the Dashboard on page 3-2*
- *Tabs and Widgets on page 3-2*
- *Security Posture Tab on page 3-6*
- *Summary Tab on page 3-17*
- *Data Loss Prevention Tab on page 3-27*
- *Compliance Tab on page 3-33*
- *Threat Statistics Tab on page 3-39*

## About the Dashboard

The **Dashboard** appears when you open the Apex Central web console or click **Dashboard** on the main menu. Each Apex Central user account has a completely independent dashboard. Any changes to the dashboard belonging to a specific user account will not affect the dashboards of the other user accounts.

The **Dashboard** contains the following:

- Tabs
- Widgets

## Tabs and Widgets

Widgets are the core components of the **Dashboard**. Widgets provide specific information about various security-related events.

The information that widgets display comes from:

- Apex Central database
- Registered managed products

For more information, see [Server Registration on page 9-2](#).

- Trend Micro Smart Protection Network

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

## Working with Tabs

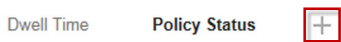
Manage tabs by adding, renaming, changing the layout, deleting, and automatically switching between tab views.

---

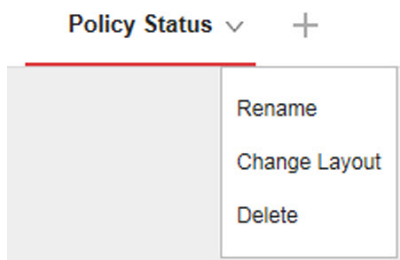
### Procedure

1. Go to the **Dashboard**.
2. To add a tab:

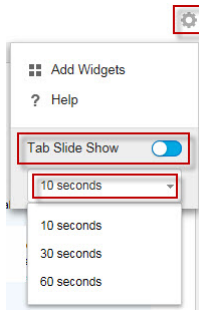
- a. Click the add icon (+).



- b. Type a name for the new tab.
3. To rename a tab:
    - a. Hover over the tab name and click the down arrow.



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



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

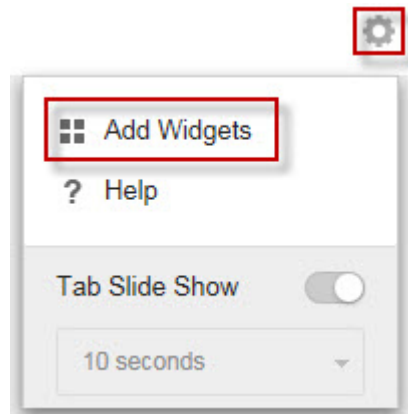
## Working with Widgets





Manage widgets by adding, moving, resizing, renaming, and deleting items. You can also modify the products that contribute data for the widget.



---

### Procedure

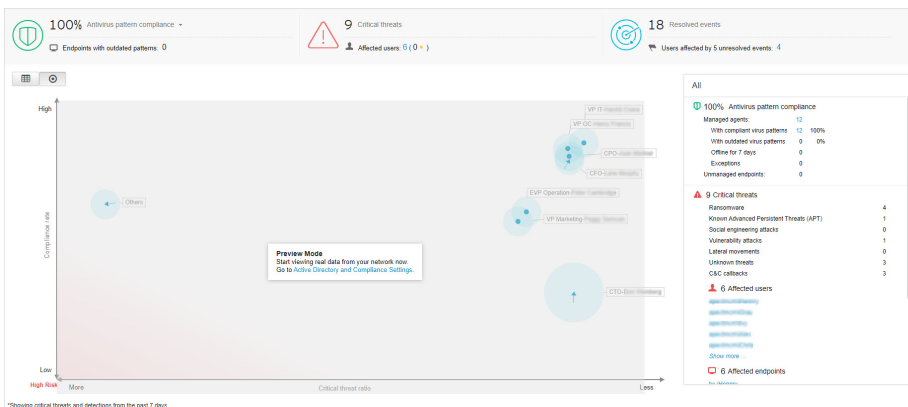
- 1.** Go to the **Dashboard**.
- 2.** Click a tab.
- 3.** To add a widget:
  - a.** Click the **Settings** button to the right of the tab display.



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

- b. Click the double arrow button ( >> ) in the **Scope** field.
  - c. (Optional) Click the funnel icon (  ) to filter and search for products.
  - d. Select the products that contribute data for the widget and click **OK**.
  - e. Click **Save**.
8. To delete a widget, click the delete icon (  ).

## Security Posture Tab



The **Security Posture** tab provides a holistic summary of your network protection status by consolidating data about the compliance levels, critical threat detections, and detections stopped on your network. You can use the **Security Posture** chart to quickly identify high risk users and groups from an integrated Active Directory structure.

**Note**

To change the sample chart data and display sites or reporting lines based on your company network, enable Active Directory integration or create custom sites based on IP addresses.

For more information, see [Active Directory and Compliance Settings on page 6-1](#).

---

By default, the **Security Posture** tab is toggled to **Chart** view (🎯). To display the chart nodes, critical threats, and antivirus pattern compliance information in a table, toggle the **Table** view (📊).

Click the settings icon (⋮ > ⚙️) to change the following information that displays on the tab.

- **Organization:** Specify the display name of the organization.
- **Active Directory grouping:** Specify whether the nodes on the chart represent **Sites** or **Reporting Lines** from your Active Directory.
- **Groups to display:** Select the top number of groups at the highest risk
- **Period:** Specify the time range for the data that displays on the chart.

## Compliance Indicators

This section of the **Security Posture** tab provides information about the antivirus pattern compliance level or the Data Loss Prevention compliance level of your network.

As your network compliance level changes, the color of the compliance indicator icon changes to reflect the thresholds configured on the **Active Directory and Compliance Settings** screen.


The default view displays information for the **Antivirus pattern compliance** indicator.

**Note**

Changing the compliance indicator also changes the compliance level information that displays in the **Security Posture** chart.

For more information, see [Security Posture Chart on page 3-10](#).

To change the compliance information that displays, click the name of the selected compliance indicator next to the down arrow icon ( ▼ ) and select one of the following indicators from the drop-down.

| INDICATOR                    | DESCRIPTION   |
|------------------------------|---|
| Antivirus pattern compliance | <p>Displays the following information:</p> <ul style="list-style-type: none"> <li>The percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions</li> </ul> <hr/> <p> <b>Note</b></p> <p>Apex Central supports Security Agents for the following managed products:</p> <ul style="list-style-type: none"> <li>Apex One</li> <li>Worry-Free Business Security Services</li> </ul> <hr/> <p>For more information about configuring compliance indicator settings, see <a href="#">Configuring the Antivirus Pattern Compliance Indicators on page 6-8</a>.</p> <ul style="list-style-type: none"> <li>The total number of endpoints with outdated antivirus patterns on your network</li> </ul> <p>Click the count for <b>Endpoints with outdated patterns</b> to view detailed information about the affected endpoints in the User/Endpoint Directory.</p> <p>For more information, see <a href="#">User/Endpoint Directory on page 7-2</a>.</p> |



| INDICATOR                       | DESCRIPTION   |
|---------------------------------|---|
| Data Loss Prevention compliance | <p>Displays the following information:</p> <ul style="list-style-type: none"> <li>The percentage of Data Loss Prevention enabled Security Agents with an acceptable number of threat detections</li> </ul> <p>For more information about configuring compliance indicator settings, see <a href="#">Configuring the Data Loss Prevention Compliance Indicator on page 6-10</a>.</p> <ul style="list-style-type: none"> <li>The total number of endpoints with Data Discovery threat detections</li> </ul> <p>Click the count for <b>Endpoints with unacceptable threat detections</b> to view detailed information about the affected endpoints in the User/Endpoint Directory.</p> <p>For more information, see <a href="#">User/Endpoint Directory on page 7-2</a>.</p> |

## Critical Threats

The **Critical Threats** section of the **Security Posture** tab displays the total number of unique critical threats (by threat type) detected on your network, the total number of affected users, and the number of affected important users (marked by the star).

For more information about defining important users or endpoints, see [User or Endpoint Importance on page 7-37](#).

Click the number of affected users to view additional details on the **User/Endpoint Directory** screen.

For more information, see [User/Endpoint Directory on page 7-2](#).

Critical threat detections include the following threat types.

| THREAT TYPE  | DESCRIPTION  |
|--------------|--|
| C&C callback | Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware |

| THREAT TYPE                            | DESCRIPTION   |
|--|---|
| Known Advanced Persistent Threat (APT) | Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents |
| Lateral movement                       | Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system                  |
| Ransomware                             | Malware that prevents or limits users from accessing their system unless a ransom is paid   |
| Social engineering attack              | Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file   |
| Unknown threats                        | Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer                 |
| Vulnerability attack                   | Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems   |

## Resolved Events

This section of the **Security Posture** tab displays the total number of resolved and unresolved events on your network.

Click the count for the **Users affected by \_\_ unresolved events** field to view detailed information about the users affected by unresolved events on your network.

For more information, see [User/Endpoint Directory on page 7-1](#).

## Security Posture Chart

The chart on the **Security Posture** tab displays the relationship between the critical threat ratio and compliance level of your network. The x-axis indicates the ratio of critical threats to total endpoints within a site or reporting line. The y-axis indicates the compliance levels of the sites or

reporting lines for the selected compliance indicator. You can use this data to quickly identify high risk users and groups from an integrated Active Directory structure.



**Note**

To change the sample chart data and display sites or reporting lines based on your company network, enable Active Directory integration or create custom sites based on IP addresses.

For more information, see [Active Directory and Compliance Settings on page 6-1](#).

---

Hover over a node to view compliance and critical threat information for particular sites or reporting lines. The tail on a node indicates the direction from which the security status has changed over the specified time period.



- Click the settings icon (  >  ) to change the **Active Directory grouping (Sites, Reporting Lines)** represented by the node.
- You can also customize sites and reporting lines by using the **Active Directory and Compliance Settings** screen.

For more information, see [Endpoint and User Grouping on page 6-11](#).

The default view displays the selected compliance indicator information for all nodes on your network for the last 7 days.

- Select a different compliance indicator to change the compliance information that displays.


For more information, see [Compliance Indicators on page 3-7](#).

- Click the settings icon (  >  ) to change the **Period** for the data that displays.
- Click a node to view detailed information about the selected node in the summary panel on the right.


For more information, see [Security Posture Details Pane on page 3-12](#).

## Security Posture Details Pane


All

 **100%** Antivirus pattern compliance

|                               |    |      |
|-------------------------------|----|------|
| Managed agents:               | 12 |      |
| With compliant virus patterns | 12 | 100% |
| With outdated virus patterns  | 0  | 0%   |
| Offline for 7 days            | 0  |      |
| Exceptions                    | 0  |      |
| Unmanaged endpoints:          | 0  |      |

 **9** Critical threats

|   |   |
|---|---|
| Ransomware                              | 4 |
| Known Advanced Persistent Threats (APT) | 1 |
| Social engineering attacks              | 0 |
| Vulnerability attacks                   | 1 |
| Lateral movements                       | 0 |
| Unknown threats                         | 3 |
| C&C callbacks                           | 3 |

 **6** Affected users

[\[blurred\]](#)

[\[blurred\]](#)


[\[blurred\]](#)

[\[blurred\]](#)

[\[blurred\]](#)

[\[blurred\]](#)

[Show more ...](#)

 **6** Affected endpoints

[\[blurred\]](#)

The details pane on the **Security Posture** tab displays more detailed information about the compliance levels, critical threat detections, and total resolved/unresolved events on your network.



The default view displays the selected compliance indicator information for all nodes on your network for the last 7 days.

- Select a different compliance indicator to change the compliance information that displays.

For more information, see [Compliance Indicators on page 3-7](#).

- Click a node on the chart to display only the information for the selected node.

For more information, see [Security Posture Chart on page 3-10](#).

- Click the settings icon (  >  ) to change the **Period** for the data that displays.

**TABLE 3-1. Compliance Information**

| INDICATOR                    | DESCRIPTION   |
|------------------------------|---|
| Antivirus pattern compliance | <p>Displays the percentage of Security Agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions</p> <p>You can also view the following details:</p> <ul style="list-style-type: none"> <li>• <b>Managed agents:</b> The number of endpoints that have Apex One or Worry-Free Business Security Services Security Agents installed <ul style="list-style-type: none"> <li>• <b>With compliant virus patterns:</b> The number of managed agents using acceptable Virus Pattern and Smart Scan Agent Pattern versions</li> <li>• <b>With outdated virus patterns:</b> The number of managed agents not using acceptable Virus Pattern and Smart Scan Agent Pattern versions</li> <li>• <b>Offline for 7 days:</b> The number of managed agents that have not communicated with the managed product server in 7 or more days</li> <li>• <b>Exceptions:</b> The number of users or endpoints excluded from the compliance calculations</li> </ul> </li> <li>• <b>Unmanaged endpoints:</b> The number of endpoints that do not have Apex One or Worry-Free Business Security Services Security Agents installed</li> </ul> <p>Expand the categories and click a count to view additional details about the affected endpoints.</p> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Antivirus Pattern Compliance Indicators on page 6-8</a></li> <li>• <a href="#">User/Endpoint Directory on page 7-1</a></li> </ul> |

| INDICATOR                       | DESCRIPTION  |
|---------------------------------|--|
| Data Loss Prevention compliance | <p>Displays the percentage of Data Loss Prevention enabled Apex One agents with an acceptable number of threat detections</p> <p>You can also view the following details:</p> <ul style="list-style-type: none"> <li>• <b>Managed agents:</b> The number of endpoints that have Apex One or Worry-Free Business Security Services Security Agents installed <ul style="list-style-type: none"> <li>• <b>With acceptable threat detections:</b> The number of managed agents with an acceptable number of threat detections</li> <li>• <b>With unacceptable threat detections:</b> The number of managed agents that exceeded the acceptable number of threat detections</li> <li>• <b>Offline for 7 days:</b> The number of managed agents that have not communicated with the managed product server in 7 or more days</li> <li>• <b>Exceptions:</b> The number of users or endpoints excluded from the compliance calculations</li> </ul> </li> <li>• <b>Unmanaged endpoints:</b> The number of endpoints that do not have Apex One or Worry-Free Business Security Services Security Agents installed</li> </ul> <p>Expand the categories and click a count to view additional details about the affected endpoints.</p> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring the Data Loss Prevention Compliance Indicator on page 6-10</a></li> <li>• <a href="#">User/Endpoint Directory on page 7-1</a></li> </ul> |

**TABLE 3-2. Critical Threats**

| SECTION            | DESCRIPTION  |
|--------------------|--|
| Critical threats   | <p>Displays the total number of unique critical threats (by threat type) detected on your network</p> <p>Lists all the critical threat types affecting your network</p> <p>For threat types with detections:</p> <ul style="list-style-type: none"> <li>• Expand the threat type to view a list of detections.</li> <li>• Click a detection to view additional details on the <b>Threat Information</b> screen.</li> </ul> <p>For more information, see <a href="#">Affected Users on page 7-19</a>.</p> |
| Affected users     | <p>Displays the total number of users affected by critical threats</p> <ul style="list-style-type: none"> <li>• Expand the section to view affected users.</li> <li>• Click an affected user to view additional details on the <b>User</b> information screen.</li> </ul> <p>For more information, see <a href="#">Security Threats for Users on page 7-6</a>.</p>   |
| Affected endpoints | <p>Displays the total number of endpoints affected by critical threats</p> <ul style="list-style-type: none"> <li>• Expand the section to view affected endpoints.</li> <li>• Click an affected endpoint to view additional details on the <b>Endpoint</b> information screen.</li> </ul> <p>For more information, see <a href="#">Security Threats on Endpoints on page 7-13</a>.</p>   |

**TABLE 3-3. Total Events**

| DATA              | DESCRIPTION  |
|-------------------|--|
| Total events      | Displays the total number of events detected                                 |
| Resolved events   | Displays the number of resolved events on your network                       |
| Unresolved events | Displays the number of unresolved events on your network that require action |



| DATA           | DESCRIPTION  |
|----------------|--|
| Affected users | <p>Displays the number of users affected by unresolved events on your network</p> <p>Click the count to view details about the affected users.</p> <p>For more information, see <a href="#">User/Endpoint Directory on page 7-1</a>.</p> |

## Summary Tab

The **Summary** tab contains a predefined set of widgets that provides an overview of the security status of your network.



### Note

You can add, delete, or modify the widgets that display on the **Summary** tab.

Available widgets:

- Critical Threats
- Users with Threats
- Endpoints with Threats
- Product Connection Status
- Product Component Status
- Ransomware Prevention

## Critical Threats Widget

This widget displays the total number of unique critical threat types detected on your network and the number of affected users and threat detections for each threat type.

Click the settings icon (  >  ) to change the default **View**.

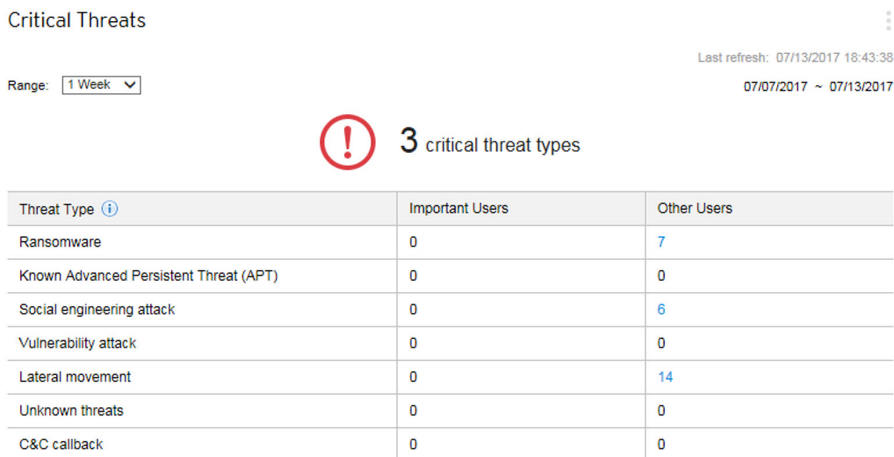
- On the **Summary** tab or a custom tab, the **Affected users** view is selected by default.

- On the **Threat Investigation** tab, the **Threat detections** view is selected by default.

**Note**

- The widget lists critical threat types in order of severity.
- Individual users may be affected by more than one critical threat type.

Use the **Range** drop-down to select the time period for the data that displays.



**FIGURE 3-1. Affected Users View**

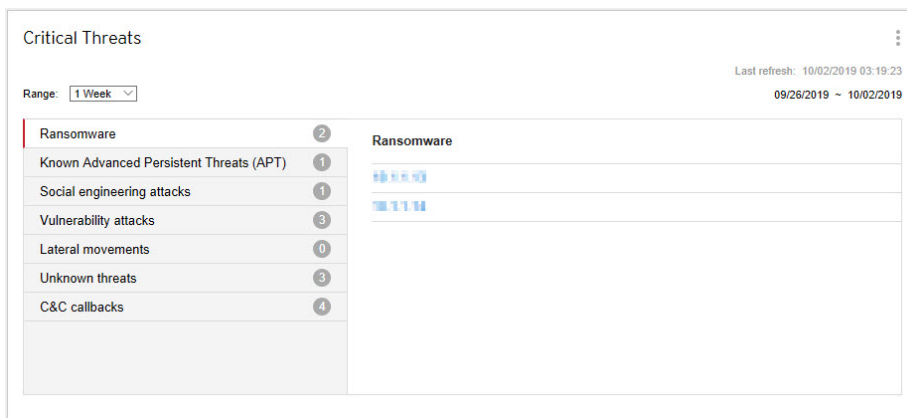
The **Affected users** view displays the number of **Important Users** and **Other Users** affected by each threat type.

- Click the count in the **Important Users** or **Other Users** column, and then click the affected user you want to view.

For more information, see [Security Threats for Users on page 7-6](#).

- You can define important users or endpoints on the **User/Endpoint Directory** screen.

For more information, see [User or Endpoint Importance on page 7-37](#).



**FIGURE 3-2. Threat Detections View**

The **Threat detections** view displays the number of detections for each critical threat type.

- Click a critical threat type to view the specific threat detections.
- Click the hyperlink for a specific threat detection to view details about the affected users and automatically start a Root Cause Analysis to determine whether the threat has affected other endpoints on your network.

For more information, see [Affected Users on page 7-19](#).

Critical threat detections include the following threat types.

| THREAT TYPE                             | DESCRIPTION   |
|---|---|
| Ransomware                              | Malware that prevents or limits users from accessing their system unless a ransom is paid   |
| Known Advanced Persistent Threats (APT) | Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents |

| THREAT TYPE                | DESCRIPTION   |
|----------------------------|---|
| Social engineering attacks | Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file   |
| Vulnerability attacks      | Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems   |
| Lateral movements          | Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system  |
| Unknown threats            | Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer |
| C&C callbacks              | Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware  |

## Users with Threats Widget

This widget displays information about users with security threat detections.

Use the **Range** drop-down to select the time period for the data that displays.

Click the **Important Users** or **Other Users** tabs to switch between the different views.

- For more information about defining important users or endpoints, see [User or Endpoint Importance on page 7-37](#).

The table lists affected users in order by critical threat type severity first, and then by the number of threat detections for the user.

- Click the number in the **Threats** column for the user you want to view.

For more information, see [Security Threats for Users on page 7-6](#).

The **Most Critical Threat** column displays the following threat types.

| THREAT TYPE                            | DESCRIPTION   |
|--|---|
| C&C callback                           | Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware  |
| Known Advanced Persistent Threat (APT) | Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents |
| Lateral movement                       | Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system                  |
| Ransomware                             | Malware that prevents or limits users from accessing their system unless a ransom is paid   |
| Social engineering attack              | Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file   |
| Unknown threats                        | Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer                 |
| Vulnerability attack                   | Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems   |

## Endpoints with Threats Widget

This widget displays information about endpoints with security threat detections.

Use the **Range** drop-down to select the time period for the data that displays.

Click the **Important Endpoints** or **Other Endpoints** tabs to switch between the different views.

- For more information about defining important users or endpoints, see [User or Endpoint Importance on page 7-37](#).

The table lists affected users in order by critical threat type severity first, and then by the number of threat detections for the user.

- Click the number in the **Threats** column for the user you want to view.



For more information, see [Security Threats on Endpoints on page 7-13](#).

The **Most Critical Threat** column displays the following threat types.

| THREAT TYPE                            | DESCRIPTION   |
|--|---|
| C&C callback                           | Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware  |
| Known Advanced Persistent Threat (APT) | Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents |
| Lateral movement                       | Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system                  |
| Ransomware                             | Malware that prevents or limits users from accessing their system unless a ransom is paid   |
| Social engineering attack              | Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file   |
| Unknown threats                        | Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer                 |
| Vulnerability attack                   | Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems   |

## Apex Central Top Threats Widget

This widget displays information about the malicious files and malicious URLs detected for a specified time range.



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

Use the drop-down list above the chart/table to select the type of threat data to display.

- **Malicious Files:** Ranks the malicious files detected on your network by the number of detections
- **Malicious URLs:** Ranks the malicious URLs detected on your network by the number of detections

Click a bar, threat name, or detection number to open the **Log Query** screen that displays information about the affected endpoints, threat details, and detection count.

The default view displays the top 10 threats from all the managed products for which the logged on user account has access rights.

- Click the settings icon (  >  ) to edit the widget title, product scope, or number of threats that displays.



## Product Component Status Widget

This widget displays the component versions and compliance status of managed products or endpoints on your network. Use this widget to track managed products or endpoints with outdated components.


The default view displays the latest versions of components managed by Apex Central and the compliance status of managed products. The **Pattern** and **Engine** sections list components in order of the highest rate of non-compliance first. You can click the **Rate** column to change the sort order.


Click any of the components in the **Pattern** or **Engine** columns to view a pie chart that displays the number of managed products or endpoints using each component version.

Click the counts in the **Outdated/All** columns to view information about the component versions on outdated managed products, all managed products, outdated endpoints, or all endpoints.

Click the settings icon (  >  ) to configure the following options:



**Note**

The settings icon (  ) does not display for widgets on the **Summary** tab.

- To modify the product scope of the widget, click the double arrow button (  ) in the **Scope** field and select the products that contribute data.
- To edit the components that display in the widget, select or clear components from the **Pattern** or **Engine** fields.
- To display compliance information for managed products, endpoints, or both, specify the **Source**.
- To specify whether to view data from all components reported by managed products or to view data from only components managed by Apex Central, select the **View**.

| DATA           | DESCRIPTION  |
|----------------|--|
| Pattern        | Displays the name of the pattern file, template, or antispy rule   |
| Engine         | Displays the name of the scan engine   |
| Latest Version | Displays the following information: <ul style="list-style-type: none"><li>• The latest version of the component downloaded by Apex Central</li><li>• The latest version of the component that is available for download (reported by managed products)</li></ul> |







| DATA         | DESCRIPTION   |
|--------------|---|
| Outdated/All | <p>Displays the following information:</p> <ul style="list-style-type: none"> <li>• <b>Outdated:</b> The number of managed products or endpoints with outdated components</li> </ul> <p>Click the first count in the <b>Outdated/All</b> column to view information about the component versions on the outdated managed products or endpoints.</p> <ul style="list-style-type: none"> <li>• <b>All:</b> The total number of managed products or endpoints that use the component</li> </ul> <p>Click the second count in the <b>Outdated/All</b> column to view information about the component versions on all managed products or endpoints.</p> <hr/> <p> <b>Note</b><br/>This column displays when <b>Both</b> is selected for the <b>Source</b>.</p> |
| Rate         | <p>Displays the percentage of managed products or endpoints with outdated components</p> <hr/> <p> <b>Note</b><br/>This column displays when <b>Both</b> is selected for the <b>Source</b>.</p>  |

## Product Connection Status Widget

This widget displays the connection status of all managed products that register to the Apex Central server.

The default view lists the connection status and managed server name of each managed product for which the logged on user account has access rights.

- To change the product scope, click the settings icon (  >  ) and select a new **Scope**.

- To view a summary of the total number of managed products for each connection status, click the settings icon (  >  ) and switch the **View** to **Summary**.

Click **View details** to view detailed information on the **Log Query** screen.

- For more information, see [Querying Logs on page 16-2](#).

| STATUS   | DESCRIPTION  |
|----------|--|
| Active   | Indicates that the product service is running and communication with the Apex Central server is established successfully                           |
| Inactive | Indicates that the product service is not running or is unable to establish communication with the Apex Central server                             |
| Abnormal | Indicates that the product service has not communicated with the Apex Central server within the user-defined agent communication time-out interval |

## Ransomware Prevention Widget

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

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

- Click the ransomware detection count to view additional details.

| CHANNEL         | DESCRIPTION  |
|-----------------|--|
| Messages        | Ransomware detected in email messages or email attachments   |
| Websites        | Ransomware detected by Web Reputation Services   |
| Network traffic | Ransomware detected by Apex One Suspicious Connections and Deep Discovery Inspector  |
| Cloud sync      | Ransomware detected by Cloud App Security on cloud storage and Office 365 servers (Exchange Online, SharePoint Online, and OneDrive), or detected by Apex One in local folders on Apex One agents that sync with cloud storage |

| CHANNEL   | DESCRIPTION   |
|-----------|---|
| Files     | Ransomware detected by File Reputation Services     |
| Behaviors | Ransomware detected by Apex One Behavior Monitoring |

## Data Loss Prevention Tab

The **Data Loss Prevention** tab contains widgets that display information about DLP incidents, template matches, and incident sources.

The predefined widgets include:

- DLP Incidents by Severity and Status
- DLP Incident Trends by User
- DLP Incidents by User
- DLP Incidents by Channel
- DLP Template Matches
- Top DLP Incident Sources
- DLP Violated Policy

### DLP Incident Trends by User Widget

This widget checks the number of DLP incident trends based on managed users. Data can be filtered by severity level, or filtered to show only the total number of incidents triggered by a specific user for a specified period of time. By default the widget displays data from all the managed products that a user's account privileges allow.

**Important**

This widget only displays data for Apex Central user accounts that have been assigned Data Loss Prevention (DLP) user roles.

For more information about reviewing DLP incidents and configuring DLP user roles, see [https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp\\_incidents](https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp_incidents).

Use the **Range** drop-down to select the time period for the data that displays.

Click the sections from the graph to open the **Incident Information** screen and review the summary of incidents.

Click the widget settings icon on the widget to access additional settings.

| SETTING          | DESCRIPTION  |
|------------------|--|
| Title            | Specify a new and meaningful title for the widget in the field.  |
| Range            | Specify the time range when the DLP incidents were triggered.  |
| Scope            | Specify the data scope displayed by the widget. <ul style="list-style-type: none"> <li>• Directly managed users</li> <li>• All managed users: Data is collected from both directly managed users and people under the directly managed users.</li> </ul> |
| Severity         | Specify the severity levels to filter the data.  |
| Users to display | Specify the number of managed users to display.  |

Click **Save** to apply changes and update the widget data.

## DLP Incidents by Severity and Status Widget

This widget checks the number of DLP incidents based on severity levels and incident status. Data can be filtered by severity level, as well as display the total number of new and high severity incidents. By default the widget displays data from all the managed products that a user's account privileges allow.

**Important**

This widget only displays data for Apex Central user accounts that have been assigned Data Loss Prevention (DLP) user roles.

For more information about reviewing DLP incidents and configuring DLP user roles, see [https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp\\_incidents](https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp_incidents).

Use the **Range** drop-down to select the time period for the data that displays.

Click the numbers in any column to open the **Incident Information** screen and review the summary of incidents.

To look up a specific incident, type an ID in the **Incident ID** field and click **Search**.

**Tip**

Each incident is assigned an ID number. ID numbers can be found by clicking a table link, in **Incident details updated** event notifications, or in **Data Loss Prevention** log query results.

Click the widget settings icon on the widget to access additional settings.

| SETTING  | DESCRIPTION   |
|----------|---|
| Title    | Specify a new and meaningful title for the widget in the field.   |
| Range    | Specify the time range when the DLP incidents were triggered.   |
| Scope    | Specify the data scope displayed by the widget. <ul style="list-style-type: none"> <li>• Directly managed users</li> <li>• All managed users: Data is collected from both directly managed users and people under the directly managed users</li> </ul> |
| Severity | Specify the severity levels to filter the data.   |

Click **Save** to apply changes and update the widget data.

## DLP Incidents by User Widget

This widget checks the number of DLP incidents based on severity levels and managed users. Data can be filtered by severity level, as well as display the total number of new and high severity incidents triggered by specific users. By default the widget displays data from all the managed products that a user's account privileges allow. The widget shows a maximum of 50 users.



### Important

This widget only displays data for Apex Central user accounts that have been assigned Data Loss Prevention (DLP) user roles.

For more information about reviewing DLP incidents and configuring DLP user roles, see [https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp\\_incidents](https://docs.trendmicro.com/en-us/enterprise/apex-central-online-help/dlp_incidents).

Use the **Range** drop-down to select the time period for the data that displays.

Click the numbers in any column to open the **Incident Information** screen and review the summary of incidents.

To look up a specific user, type a few characters in the **User** field and click **Search**. For example typing **ke** shows all user names with **ke**, such as “Ken” and “Brooke”. You can also type a domain and user name, such as `domain1\chris`.



### Note

User names must not contain the following characters: " [ ] ; | = + \* ? / \ < & > ,

Domain names must not contain the following characters: \ \* + = | ; " ? < & > ,

Click the widget settings icon on the widget to access additional settings.

| SETTING | DESCRIPTION   |
|---------|---|
| Title   | Specify a new and meaningful title for the widget in the field. |

| SETTING          | DESCRIPTION  |
|------------------|--|
| Range            | Specify the time range when the DLP incidents were triggered.  |
| Scope            | Specify the data scope displayed by the widget. <ul style="list-style-type: none"> <li>• Directly managed users</li> <li>• All managed users: Data is collected from both directly managed users and people under the directly managed users.</li> </ul> |
| Severity         | Specify the severity levels to filter the data.  |
| Users to display | Specify the number of managed users to display.  |

Click **Save** to apply changes and update the widget data.

## DLP Incidents by Channel Widget

This widget displays the total number of DLP incidents. Data can be filtered by the type of channels where the incident is triggered.

Use the **Range** drop-down to select the time period for the data that displays.

Use the **Channel** drop-down to filter out the type of channels where the incident is triggered.




This widget displays the number of DLP incidents and the ratio of channels compared to the total number of incidents. This widget displays this data by:

| DATA    | DESCRIPTION   |
|---------|---|
| P2P     | Displays all peer-to-peer DLP incidents by any managed product that the Data Scope specifies      |
| IM      | Displays all instant messaging DLP incidents by any managed product that the Data Scope specifies |
| Webmail | Displays all webmail DLP incidents by any managed product that the Data Scope specifies           |
| Email   | Displays all email DLP incidents by any managed product that the Data Scope specifies             |

| DATA    | DESCRIPTION   |
|---------|---|
| Web App | Displays all web application DLP incidents by any managed product that the Data Scope specifies |
| Others  | Displays the remaining DLP incidents by any managed product that the Data Scope specifies       |

Clicking links in the **Channel** column or sections from the graphs opens a screen that displays detailed information.

| DATA           | DESCRIPTION   |
|----------------|---|
| Channel        | Type of channels where the DLP incidents is triggered |
| Incidents      | Number of DLP incidents triggered                     |
| Percentage (%) | DLP incidents percentage of total number of incidents |

To change the information that the widget displays, click  > . On the dialog box that appears, specify the **Scope** by clicking  and selecting the parent servers that the widget uses as its source.

## DLP Template Matches Widget




This widget displays the type of DLP incidents on your network. Data can be filtered by template.

Use the **Range** drop-down to select the time period for the data that displays.

Clicking links in the **Template** column or sections from the graphs opens a screen that displays detailed information.

| DATA           | DESCRIPTION   |
|----------------|---|
| Template       | Template triggered by DLP incidents                   |
| Incidents      | Number of DLP incidents                               |
| Percentage (%) | DLP incidents percentage of total number of incidents |



To change the information that the widget displays, click  > . On the dialog box that appears, specify the **Scope** by clicking  and selecting the parent servers that the widget uses as its source.

## Top DLP Incident Sources Widget

This widget displays the total number of top DLP incident sources on your network. This data includes users, email addresses, host names, and IP addresses, which can be filtered by incident source.

Use the **Range** drop-down to select the time period for the data that displays.

Use the **Show** drop-down to select the data to be displayed.

## DLP Violated Policy Widget

This widget displays the DLP violated policy. Use this widget to check the total number of DLP incidents. By default data is sorted by the number of incidents. To sort data by policy name, click the **Policy** column title.

Use the **Range** drop-down to select the time period for the data that displays.

Clicking links in the **Incidents** column opens a screen that displays detailed information.

| DATA      | DESCRIPTION   |
|-----------|---|
| Policy    | Name of the policy where the DLP incidents is triggered |
| Incidents | Number of DLP incidents triggered                       |

## Compliance Tab

The **Compliance** tab contains widgets that display information relating to component or connection compliance for managed products or endpoints.



The predefined widgets are as follows:

- Product Application Compliance
- Product Component Status

- Product Connection Status
- Agent Connection Status

## Product Application Compliance Widget

This widget displays the product version, language, build, and update status for managed products. This provides administrators a quick way to discern which managed product's applications are up-to-date and which require updating.

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

Click the counts in the **Up-to-date** and **Out-of-date** columns to open a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

| DATA                | DESCRIPTION   |
|---------------------|---|
| Product             | The managed product registered to Apex Central  |
| Version             | Version of the managed product  |
| Language            | Language version of the managed product   |
| Build               | Build number of the managed product   |
| Up-to-date          | Number of products that are considered updated<br><br>Edit the widget to specify the minimum product version that should still be considered "up-to-date".<br><br>Click the count to view more details about the product. |
| Out-of-date         | Number of products that are "out-of-date"<br><br>Click the count to view more details about the product.  |
| Up-to-date Rate (%) | Percentage of products that are "up-to-date"  |

By default the widget displays data from all the managed products that a user's account privileges allow.

Specify a bar graph or a table to display the data. By default, data is displayed as a bar graph.

Click **Edit** to access the following options:

- Click **Scope > Browse** to specify the products that contribute data for the widget.

The data scope specifies the products which the widget uses to display data. This can have a drastic affect on the usefulness of the information that the widget displays.

- On the **Up-to-date range** drop-down, specify the number of product versions away from the latest build that should still be considered "up-to-date".

Click **Save** to apply changes and exit.


## Product Component Status Widget

This widget displays the component versions and compliance status of managed products or endpoints on your network. Use this widget to track managed products or endpoints with outdated components.


The default view displays the latest versions of components managed by Apex Central and the compliance status of managed products. The **Pattern** and **Engine** sections list components in order of the highest rate of non-compliance first. You can click the **Rate** column to change the sort order.


Click any of the components in the **Pattern** or **Engine** columns to view a pie chart that displays the number of managed products or endpoints using each component version.

Click the counts in the **Outdated/All** columns to view information about the component versions on outdated managed products, all managed products, outdated endpoints, or all endpoints.



Click the settings icon (  ) to configure the following options:

**Note**

The settings icon (  ) does not display for widgets on the **Summary** tab.

- To modify the product scope of the widget, click the double arrow button (  ) in the **Scope** field and select the products that contribute data.
- To edit the components that display in the widget, select or clear components from the **Pattern** or **Engine** fields.
- To display compliance information for managed products, endpoints, or both, specify the **Source**.
- To specify whether to view data from all components reported by managed products or to view data from only components managed by Apex Central, select the **View**.



| DATA           | DESCRIPTION   |
|----------------|---|
| Pattern        | Displays the name of the pattern file, template, or antispam rule   |
| Engine         | Displays the name of the scan engine  |
| Latest Version | Displays the following information: <ul style="list-style-type: none"> <li>• The latest version of the component downloaded by Apex Central</li> <li>• The latest version of the component that is available for download (reported by managed products)</li> </ul> |



| DATA         | DESCRIPTION   |
|--------------|---|
| Outdated/All | <p>Displays the following information:</p> <ul style="list-style-type: none"> <li>• <b>Outdated:</b> The number of managed products or endpoints with outdated components</li> </ul> <p>Click the first count in the <b>Outdated/All</b> column to view information about the component versions on the outdated managed products or endpoints.</p> <ul style="list-style-type: none"> <li>• <b>All:</b> The total number of managed products or endpoints that use the component</li> </ul> <p>Click the second count in the <b>Outdated/All</b> column to view information about the component versions on all managed products or endpoints.</p> <hr/> <p> <b>Note</b><br/>This column displays when <b>Both</b> is selected for the <b>Source</b>.</p> |
| Rate         | <p>Displays the percentage of managed products or endpoints with outdated components</p> <hr/> <p> <b>Note</b><br/>This column displays when <b>Both</b> is selected for the <b>Source</b>.</p>  |

## Product Connection Status Widget

This widget displays the connection status of all managed products that register to the Apex Central server.

The default view lists the connection status and managed server name of each managed product for which the logged on user account has access rights.

- To change the product scope, click the settings icon (  >  ) and select a new **Scope**.

- To view a summary of the total number of managed products for each connection status, click the settings icon (  >  ) and switch the **View** to **Summary**.

Click **View details** to view detailed information on the **Log Query** screen.

- For more information, see [Querying Logs on page 16-2](#).

| STATUS   | DESCRIPTION  |
|----------|--|
| Active   | Indicates that the product service is running and communication with the Apex Central server is established successfully                           |
| Inactive | Indicates that the product service is not running or is unable to establish communication with the Apex Central server                             |
| Abnormal | Indicates that the product service has not communicated with the Apex Central server within the user-defined agent communication time-out interval |

## Agent Connection Status Widget




This widget displays the connection status of agents with their parent servers. Agents for the following managed products are displayed:

- Endpoint Sensor
- Endpoint Encryption
- Mobile Security
- Mobile Security (for Mac)
- Apex One
- Vulnerability Protection
- Worry-Free Business Security Services

By default the widget displays data from all the managed products that a user's account privileges allow.

Click the values in the **Online**, **Offline**, or **Total** columns to view more information. Apex Central performs a log query to provide the information.

| DATA    | DESCRIPTION                                   |
|---------|---|
| Server  | Parent servers                                |
| Online  | Agents connected to their parent servers      |
| Offline | Agents disconnected from their parent servers |
| Total   | Total number of endpoints                     |

To change the information that the widget displays, click  > . On the dialog box that appears, specify the **Scope** by clicking  and selecting the parent servers that the widget uses as its source.

## Threat Statistics Tab



The **Threat Statistics** tab contains widgets that display aggregated detections of security threats.

The predefined widgets include:

- Apex Central Top Threats
- Apex Central Threat Statistics
- Threat Detection Results
- Policy Violation Detections
- C&C Callback Events

### Apex Central Top Threats Widget

This widget displays information about the malicious files and malicious URLs detected for a specified time range.

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


Use the drop-down list above the chart/table to select the type of threat data to display.

- **Malicious Files:** Ranks the malicious files detected on your network by the number of detections

- **Malicious URLs:** Ranks the malicious URLs detected on your network by the number of detections

Click a bar, threat name, or detection number to open the **Log Query** screen that displays information about the affected endpoints, threat details, and detection count.

The default view displays the top 10 threats from all the managed products for which the logged on user account has access rights.

- Click the settings icon (  ) to edit the widget title, product scope, or number of threats that displays.

## Apex Central Threat Statistics Widget

This widget displays the total number of security threat detections on your network. Data can be filtered by security threat type or by the location on your network where the threat is detected.

- Product Category

| DATA                | DESCRIPTION  |
|---------------------|--|
| File server         | Security threats on file servers detected by any managed product that the Data Scope specifies         |
| Network             | Security threats on your network detected by any managed product that the Data Scope specifies         |
| Unknown             | Unidentified security threats  |
| Mail                | Security threats on email servers detected by any managed product that the Data Scope specifies        |
| Desktop             | Security threats on desktops detected by any managed product that the Data Scope specifies             |
| Gateway             | Security threats at the gateway detected by any managed product that the Data Scope specifies          |
| Apex Central server | Security threats on Apex Central servers detected by any managed product that the Data Scope specifies |



- Violation Type

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Behavior Monitoring         | Behavior Monitoring violation detected by any managed product that the Data Scope specifies  |
| Content Violation           | Content security violations (spam, blocked keywords and expressions) detected by any managed product that the Data Scope specifies |
| Device Control              | Device Control violation detected by any managed product that the Data Scope specifies   |
| Firewall Violation          | Firewall violation by any managed product that the Data Scope specifies  |
| Network Content Inspection  | Network Content Inspection violation detected by any managed product that the Data Scope specifies                                 |
| Predictive Machine Learning | Predictive Machine Learning detection by any managed product that the Data Scope specifies   |
| Spyware/Grayware            | Spyware/grayware detected by any managed product that the Data Scope specifies   |
| Suspicious Files            | Suspicious file detection by any managed product that the Data Scope specifies   |
| Virus/Malware               | Viruses/malware detected by any managed product that the Data Scope specifies  |
| Web Security                | Web security violations (malicious URLs, blocked URLs) detected by any managed product that the Data Scope specifies               |

**Note**

The widget can display data for only one information type at a time.

Click the links in the **Detections** column to open a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

| DATA           | DESCRIPTION   |
|----------------|---|
| Type           | Type of security threat or managed product where the threat is detected |
| Detections     | Number of security threats detected                                     |
| Percentage (%) | Security threat percentage of total number of detected threats          |




Specify the date range for the data that the widget displays:

- Today
- Last 7 days
- Last 14 days
- Last 30 days

Specify how the widget displays the data:



- Pie chart
- Bar chart
- Tabular
- Line chart

By default the widget displays data from all the managed products that a user's account privileges allow.

To change the information that the widget displays, click  > . On the dialog box that appears, specify the **Scope** by clicking  and selecting the parent servers that the widget uses as its source.

## Threat Detection Results Widget


This widget displays the number of threat detections and the ratio of threats compared to the total number of detections. The widget can display data for only one information type at a time. Clicking links in the **Detections** column opens a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

| DATA           | DESCRIPTION  |
|----------------|--|
| Results        | <p>The action or result of the action performed by the managed product</p> <hr/>  <b>Note</b><br>This column does not display for the <b>Web Security</b> threat type |
| Policy/Rule    | <p>The type of policy/rule applied under the <b>Web Security</b> threat type.</p> <hr/>  <b>Note</b><br>This column does not display for other listed threat types.   |
| Detections     | The number of security threats detected  |
| Percentage (%) | The percentage of total detections that are security threats   |

This widget displays threat detections for the following threat types:

**TABLE 3-4. Threat Types**


| THREAT TYPE      | DESCRIPTION   |
|------------------|---|
| Virus/Malware    | Displays the action taken on all files by any managed product that the Data Scope specifies. For example: Cleaned, Access denied, and so on.                            |
| Spyware/Grayware | Displays the action taken on all files by any managed product that the Data Scope specifies. For example: Successful, Further action required, and so on.               |
| Content Security | Displays the action taken on all email messages by any managed product that the Data Scope specifies. For example: Deleted, Attachments stripped, and so on.            |
| Web Security     | Displays all web security violations blocked using the policies by any managed product that the Data Scope specifies. For example: File blocking, File name, and so on. |
| Network Virus    | Displays the action taken on all network viruses by any managed product that the Data Scope specifies   |

Click the settings icon (  ) to edit the widget title, product scope, or type of threats that displays.

## Policy Violation Detections Widget

This widget displays the policy violation detections for Network VirusWall Enforcer devices. Clicking links in the **Detections** column opens a screen that displays detailed information. Apex Central performs a log query to provide the detailed information.

| DATA       | DESCRIPTION  |
|------------|--|
| Type       | Lists <b>Service Violations</b> as a type of security threat           |
| Updated    | Last updated date  |
| Detections | Number of service violations Network VirusWall Enforcer devices detect |

Click the settings icon (  ) to edit the widget title or product scope.



### Note

This widget only displays policy violation detections for Network VirusWall Enforcer.



Click **Save** to apply changes and exit.


## C&C Callback Events Widget

This widget displays the number of C&C callback attempts based on compromised hosts or callback addresses. The widget can display data for only one information type at a time. Clicking the numbers in any table cells opens the **C&C Callback Events** screen, which contains the following callback summary data:

| DATA             | DESCRIPTION                    |
|------------------|--------------------------------|
| Compromised Host | Affected host or email address |

| DATA  | DESCRIPTION   |
|---|---|
| Callback Address  | URL, IP address, or email address to which a compromised host attempts a callback       |
| C&C Server Location   | Region and country where the C&C server locates   |
| Callback Attempts   | Number of contacts made between callback addresses and compromised hosts                |
| Latest Callback Address/<br>Compromised Host  | URL, IP address, or email address to which the last callback attempt was logged         |
| Callback Addresses/<br>Compromised Hosts<br>(with numbers<br>displayed in the<br>columns) | Number of compromised hosts or callback addresses associated with the callback attempts |
| Logged By   | Name of the managed product that logged the event                                       |

Click the settings icon (  >  ) to edit the following:

- **Title:** Modify the title of the **C&C Callback Events** widget.
- **Scope:** Click  and select the parent servers that the widget uses as the source.
- **C&C list source:** Select **Global Intelligence**, **Virtual Analyzer**, or **User-defined** as the C&C list sources.
- **Items to display:** Select the number of items to display on the widget.

Click **Save** to apply changes and exit.



# Chapter 4

## Account Management

This section discusses how to create and administer Apex Central user accounts and roles.

Topics include:



- *User Accounts on page 4-2*
- *User Roles on page 4-16*

## User Accounts



The **User Accounts** screen provides a list of all previously configured user accounts for the Apex Central console. You can use this screen to set up user account and a particular role to each user.



For more information about user roles, see [User Roles on page 4-16](#).

The following table outlines the tasks available on the **User Accounts** screen.

| TASK                             | DESCRIPTION   |
|----------------------------------|---|
| Add user accounts                | <p>Click <b>Add</b> to set up a new user account or import users or groups from an integrated Active Directory structure.</p> <p>For more information, see <a href="#">Adding a User Account on page 4-5</a>.</p> <hr/> <p> <b>Note</b><br/>Apex Central allows you to create user accounts for users and groups from an integrated Active Directory structure.</p> <p>For more information, see <a href="#">Active Directory Integration on page 6-2</a>.</p> |
| Delete user accounts             | <p>Select the check box next the <b>User/Group Name</b> of an existing account and click <b>Delete</b> to permanently remove an account.</p> <hr/> <p> <b>WARNING!</b><br/>Deleting an account permanently removes all previously configured account information from the Apex Central server.</p>  |
| Enable two-factor authentication | <p>Click the <b>Enable Two-Factor Authentication</b> link to require users to type the verification code generated by the Google Authenticator app in order to sign in to Apex Central.</p> <p>For more information, see <a href="#">Enabling or Disabling Two-Factor Authentication on page 4-12</a>.</p>  |



| TASK                              | DESCRIPTION  |
|-----------------------------------|--|
| Disable two-factor authentication | <p>Click the <b>Disable Two-Factor Authentication</b> link to only require the use of a valid user account and password to sign in to Apex Central.</p> <p>For more information, see <a href="#">Enabling or Disabling Two-Factor Authentication on page 4-12</a>.</p>   |
| Edit user accounts                | <p>Click the <b>User/Group Name</b> of a user account to edit the user information.</p> <p>For more information, see <a href="#">Editing a User Account on page 4-11</a>.</p>  |
| Unlock user accounts              | <p>Click the <b>Unlock</b> button in the <b>Locked</b> column to unlock an account that exceeded the specified number of consecutive unsuccessful logon attempts.</p> <p>For more information, see <a href="#">Configuring Web Console Settings on page 2-7</a>.</p>   |
| Enable user accounts              | <p>Click the  icon in the <b>Enable</b> column to enable a disabled account to sign in to the Apex Central console.</p> <hr/> <p> <b>Note</b><br/>You can also enable a disabled account by editing the account.</p> <p>For more information, see <a href="#">Editing a User Account on page 4-11</a>.</p> |

| TASK                  | DESCRIPTION   |
|-----------------------|---|
| Disable user accounts | <p>Click the  icon in the <b>Enable</b> column to temporarily prevent a user from signing in to the Apex Central console.</p> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"><li>• You can also disable a user account by editing the account.</li></ul> <p>For more information, see <a href="#">Editing a User Account on page 4-11</a>.</p> <ul style="list-style-type: none"><li>• Apex Central cannot disable accounts for Active Directory users or groups. To disable an Active Directory account, you must disable the account from the Active Directory server.</li></ul> <p>For more information, contact your Active Directory administrator.</p> |

## Root Account

Apex Central allows you to specify the name of the **<Root>** account upon installation. The **<Root>** account can view all the functions in the menu, use all available services, and install agents. You cannot delete the **<Root>** account.

The **<Root>** account also has the following additional privileges:

- The **<Root>** account can unlock a locked function by forcibly logging out the user who currently uses the function.
- The **<Root>** account can bypass Two-Factor Authentication.

**Note**

Apex Central accounts log on to Apex Central only and not the entire network. Apex Central user accounts are not the same as network domain accounts.

---

## Adding a User Account

Use the **User Accounts** screen to create new user accounts for Apex Central administrators or to import users or groups from an integrated Active Directory structure.

**Important**

- Only the **<Root>** account created during installation, or user accounts that have been assigned the **Administrator** or **Administrator and DLP Compliance Officer** user role, can create new user accounts on Apex Central.
- Importing users or groups from an Active Directory structure requires an integrated Active Directory structure.

For more information, see [Active Directory Integration on page 6-2](#).

- Integrating an Active Directory structure allows Active Directory users or groups to log on to Apex Central by using the **Log On with Domain Credentials** button without having to provide their user names and passwords.

For more information, see [Accessing the Web Console on page 2-5](#).

---

### Procedure

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

The **User Accounts** screen appears.

2. Click **Add**.

The **User Accounts > Step 1: User Information** screen appears.

3. Select **Enable this account** to enable the account upon creation.



**Note**


Apex Central cannot disable accounts for Active Directory users or groups. To disable an Active Directory account, you must disable the account from the Active Directory server.

For more information, contact your Active Directory administrator.

4. Select the account type.

- To create a new Apex Central user account:
  - a. Select **Custom account**.
  - b. Configure the following required account information:

| INFORMATION      | DESCRIPTION  |
|------------------|--|
| User name        | Type the account name that the user provides to log on to the Apex Central web console.  |
| Full name        | Type the full name of the user.  |
| Password         | Type the password that the user provides to log on to the Apex Central web console.<br><br><div data-bbox="612 984 673 1034" data-label="Image"> </div> <div data-bbox="681 980 739 1003" data-label="Section-Header"> <p><b>Note</b></p> </div> <div data-bbox="681 1015 1077 1075" data-label="Text"> <p>Users can change their passwords on the <b>My Account</b> screen.</p> </div> <div data-bbox="681 1099 1077 1190" data-label="Text"> <p>For more information, see <a href="#">Viewing or Editing User Account Information on page 4-14</a>.</p> </div> |
| Confirm password | Type the same password provided in the <b>Password</b> field.  |

| INFORMATION   | DESCRIPTION   |
|---------------|---|
| Email address | <p>Type the email address to which the user has notifications delivered.</p> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• This field is required for Apex Central to send reports and event notifications by email or when Two-Factor Authentication is enabled.</li> <li>• You must also configure SMTP server settings in order for Two-Factor Authentication to work properly and for Apex Central to send reports and notifications by email.</li> </ul> <p>For more information, see <a href="#">Configuring SMTP Server Settings on page 17-4</a>.</p> |

- To import users or groups from an integrated Active Directory structure:
  - a. Select **Active Directory user or group**.
  - b. Search for Active Directory users or groups using the following:
    - **User/Group name**

**Note**

- This field is required.
- You can use an asterisk wildcard (\*) to search using partial string matching.

For example, typing “tom\*” searches for all users or groups with names that start with “tom”.

- **Base distinguished name**

c. Click **Search**.

Active Directory accounts that match the specified criteria appear in the **Search result** list.

d. Select Active Directory users or groups from the **Search result** list and click >.

The selected Active Directory users or groups appear in the **Selected users/groups** list.



**Important**

- Apex Central requires you to manually synchronize Active Directory data before imported users or groups can log on to Apex Central using their Active Directory domain credentials.

For more information, see [Active Directory Integration on page 6-2](#):

- You do not need to manually synchronize Active Directory data from an Active Directory structure migrated from a previous version of Control Manager. Users and groups from the migrated Active Directory structure can log on to Apex Central as soon as the migration completes.

---

5. Click **Next**.

The **User Accounts > Step 2: Access Control** screen appears.

6. Select a user role from the **Select role** drop-down.

**Note**

- The access rights defined for a user role take precedence over the managed product/folder access rights that you configure for individual user accounts.
- The DLP Compliance Officer and DLP Incident Reviewer roles are only available to Active Directory users or groups.

For more information, see [User Roles on page 4-16](#).

---

7. In the **Select accessible products/folders** tree, select the products or folders that the user can access in the Product Directory structure.
- 

**Note**

You can restrict a user to a single managed product or allow access to the entire Product Directory. Assigning access to a folder allows users to access all of the sub-folders and managed products.

For more information, see [Managed Product Access Control on page 4-9](#).

---

8. Specify the managed product/folder access rights for the user account.
- 

**Note**

Access rights determine the actions that the user account can perform on managed products. Privileges granted to an account cannot exceed those of the grantor.

For more information, see [Managed Product Access Control on page 4-9](#).

---

9. Click **Finish**.

The new user account appears on the **User Accounts** screen.

---

## Managed Product Access Control

The access rights you specify for selected managed products/folders determine the controls available to the user on the **Product Directory**

screen. For example, if you only specify the **Execute** access right for the selected managed products/folders, then the user can only use the **Tasks** button on the **Product Directory** screen.

**Note**

The actions available on the **Product Directory** screen buttons dynamically change based on user role, managed product/folder access rights, and the managed product/folder you select in the Product Directory structure.

For more information, see [Product Directory on page 11-2](#).

You can specify one or more of the following access rights for the accessible managed products/folders.

| ACCESS RIGHT   | DESCRIPTION   |
|----------------|---|
| Execute        | Allows the user account to use the <b>Tasks</b> button on the <b>Product Directory</b> screen to execute tasks on managed products located in accessible folders<br><br>For more information, see <a href="#">Executing Managed Product Tasks on page 11-8</a> .  |
| Configure      | Allows the user account to use the <b>Configure</b> button on the <b>Product Directory</b> screen to configure managed product settings or log on to the managed product web console from Apex Central<br><br>For more information, see <a href="#">Configuring Managed Product Settings on page 11-9</a> . |
| Edit Directory | Allows the user account to use the <b>Directory Management</b> button to organize accessible managed products or folders in the Product Directory structure<br><br>For more information, see <a href="#">Directory Management on page 11-11</a> .   |



**Note**

When administrators specify which products a user can access, the administrator is also specifying what information a user can access from Apex Central. The following information is affected: component information, logs, product summary information, security information, and information available for reports and log queries.

Example:

Bob and Jane are Apex One administrators. Both have identical user role permissions (they have access to the same menu items in the web console). However, Jane oversees operations for all Apex One servers. Bob only oversees operations for Apex One servers protecting desktops for the Marketing department. The information that they can view in the web console will be very different. Bob logs on and only sees information that is applicable to the Apex One servers that his Apex Central user account allows (the Apex One servers for the Marketing department). When Jane logs on, she sees information for all Apex One servers, because her Apex Central user account grants her access to all Apex One servers registered to Apex Central.

---

## Editing a User Account

Use the **User Accounts** screen to edit the user information, user role, or managed product/folder access rights of any user account that you have permission to edit.

**Important**

- The **<Root>** account created during installation can edit any user account on the Apex Central network. Any user account assigned the **Administrator** or **Administrator and DLP Compliance Officer** user role can edit any other user account on the Apex Central network, except for the **<Root>** account.
  - Modifying the access rights of a user account terminates all Apex Central sessions for the modified account and all accounts created by the modified account.
  - You cannot change the user name of an existing account.
- 

**Procedure**

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

The **User Accounts** screen appears.

2. Click the **User/Group Name** of the account to modify.

The **User Accounts > Step 1: User Information** screen appears.

3. To enable or disable the account, select or deselect the **Enable this account** check box.
4. Modify the user information.
5. Click **Next**.

The **User Accounts > Step 2: Access control** screen appears.

6. Modify the user role, accessible products/folders, or access rights.
  7. Click **Finish** to apply changes.
- 

**Enabling or Disabling Two-Factor Authentication**

Two-Factor Authentication provides extra security on user accounts by requiring users to type the verification code generated by the Google Authenticator app in order to sign in to Apex Central.

**Important**

Two-Factor Authentication for Apex Central requires the following:

- Configuring an email address for each user account

For more information, see [Viewing or Editing User Account Information on page 4-14](#).

- Configuring SMTP server settings to send email notifications

For more information, see [Configuring SMTP Server Settings on page 17-4](#).

- Downloading and installing the Google Authenticator app on each user's mobile device
- 

**Note**

- The <Root> account can always bypass Two-Factor Authentication.
  - Although the verification code generated by the Google Authenticator app changes every 30 seconds, users can still use previously generated codes up to 5 minutes old to sign in to Apex Central.
- 

**Procedure**

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

The **User Accounts** screen appears.

2. To enable two-factor authentication:

- a. Click **Enable Two-Factor Authentication**.

A confirmation dialog box appears.

- b. Click **Enable**.

- A warning message appears at the top of the **User Accounts** screen, prompting you to configure email addresses for all user accounts.

Click the link to view users without configured email addresses.

- The email address field on the **Add User Account** screen becomes a required field.
  - Apex Central requires users to type the verification code generated by the Google Authenticator app, in addition to a valid user name and password, in order to sign in.
3. To disable two-factor authentication:
    - a. Click **Disable Two-Factor Authentication**.  
A confirmation dialog box appears.
    - b. Click **Disable**.  
Signing into the Apex Central web console will only require the use of a valid user account and password.

---

## Viewing or Editing User Account Information

Use the **My Account** screen to view or change account information for your own user account or for a user account that you created.

For information about editing the user role assigned to a particular user account, see [Editing a User Account on page 4-11](#).


---




### Procedure

1. Go to **Administration > Account Management > My Account**.

The **My Account** screen appears.

2. Configure the following account information:

| INFORMATION | DESCRIPTION   |
|-------------|---|
| Full name   | Type the full name of the user.<br><br><hr/>  <b>Note</b><br>This field is required. |

| INFORMATION         | DESCRIPTION  |
|---------------------|--|
| Password            | <p>Type the password that the user provides to log on to the Apex Central web console.</p> <hr/> <p> <b>Note</b><br/>This field is required.</p>  |
| Confirm password    | <p>Type the same password provided in the <b>Password</b> field.</p> <hr/> <p> <b>Note</b><br/>This field is required.</p>  |
| Email address       | <p>Type the email address to which the user has notifications delivered.</p> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>This field is required for Apex Central to send reports and event notifications by email and for Two-Factor Authentication.</li> </ul> <p>For more information about Two-Factor Authentication, see <a href="#">Enabling or Disabling Two-Factor Authentication on page 4-12</a>.</p> <ul style="list-style-type: none"> <li>In order for Apex Central to send reports and event notifications by email, you must also configure SMTP server settings.</li> </ul> <p>For more information, see <a href="#">Configuring SMTP Server Settings on page 17-4</a>.</p> |
| Telephone number    | <p>Type the landline phone number to associate with the user account.</p>  |
| Mobile phone number | <p>Type the cellular phone number to associate with the user account.</p>  |

3. Click **Save** to apply changes.
- 

## User Roles

The **User Roles** screen provides a list of all default user roles and all custom user roles that you can assign to user accounts. User roles define which areas of the Apex Central web console a user can access and control. You can use this screen to create and edit custom Apex Central user roles.

---



### Important

If a custom user role in a previous Apex Central version has permissions to Policy Management menu items, the role will have full control permissions after upgrading to the current release. You can change the permissions to “Maintain” or “Read-only”. When upgrading from a Apex Central version that does not include Policy Management, custom user roles have no permissions to manage or view Policy Management features until you choose to modify the role settings.

---





### Note

- Only the **<Root>** account created during installation, or user accounts that have been assigned the **Administrator** or **Administrator and DLP Compliance Officer** user role, can create new user accounts and assign user roles.
- The access rights defined for a user role take precedence over the managed product/folder access rights that you configure for individual user accounts.

For more information, see [Managed Product Access Control on page 4-9](#).

---

The following table outlines the tasks available on the **User Roles** screen.

| TASK              | DESCRIPTION   |
|-------------------|---|
| Add user roles    | <p>Click <b>Add</b> to create a new custom user role.</p> <p>For more information, see <a href="#">Adding a User Role on page 4-20</a>.</p>   |
| Delete user roles | <p>Select the check box next the <b>Name</b> of an custom user role and click <b>Delete</b> to permanently remove the role.</p> <hr/> <p> <b>Note</b><br/>You cannot delete any of the default user roles provided by Trend Micro Apex Central™.</p>   |
| Edit user roles   | <p>Click the <b>Name</b> of a user role to edit or view assigned access rights.</p> <p>For more information, see <a href="#">Editing a User Role on page 4-22</a>.</p> <hr/> <p> <b>Note</b><br/>You cannot edit any of the default user roles provided by Trend Micro Apex Central™.</p> <p>For more information about the default user roles, see <a href="#">Default User Roles on page 4-17</a>.</p> |

## Default User Roles

Apex Central provides default user roles that you can assign to user accounts. User roles define which areas of the Apex Central web console a user can access and control. Although you can add access rights to a default user role, you cannot remove any of the predefined access rights from a default user role.

**Note**

Only the <Root> account created during installation, or user accounts that have been assigned the **Administrator** or **Administrator and DLP Compliance Officer** user role, can create new user accounts and assign user roles.


For more information about adding or editing custom user roles, see the following topics:

- [Adding a User Role on page 4-20](#)
- [Editing a User Role on page 4-22](#)

The following table describes the default roles available on the **User Roles** screen.

| ROLE  | DESCRIPTION   |
|---|---|
| Administrator_and_DLP<br>Compliance_Officer | <ul style="list-style-type: none"> <li>• Can perform all actions on all menu items</li> <li>• Can monitor, review, and investigate DLP incidents triggered by any Active Directory user</li> </ul>  |
| Administrator                               | <ul style="list-style-type: none"> <li>• Can perform all actions on all menu items</li> <li>• Cannot monitor, review, or investigate DLP incidents triggered by any Active Directory user</li> </ul>  |
| DLP_Compliance_Officer                      | <ul style="list-style-type: none"> <li>• Can perform all actions on the <b>Dashboard</b></li> <li>• Can monitor, review, and investigate DLP incidents triggered by any Active Directory user</li> </ul> <hr/> <div data-bbox="431 1143 491 1193"></div> <div data-bbox="502 1141 556 1164"><b>Note</b></div> <div data-bbox="502 1175 1046 1235">This user role is only available to Active Directory users or groups.</div> |



| ROLE                  | DESCRIPTION  |
|-----------------------|--|
| DLP_Incident_Reviewer | <ul style="list-style-type: none"> <li>• Can perform all actions on the <b>Dashboard</b></li> <li>• Can only monitor, review, and investigate DLP incidents triggered by Active Directory users that report to the DLP Incident Reviewer</li> </ul> <hr/> <div style="display: flex; align-items: flex-start;">  <p><b>Note</b><br/>This user role is only available to Active Directory users or groups.</p> </div> <hr/> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Reporting Lines on page 6-14</a></li> <li>• <a href="#">Adding a User Account on page 4-5</a></li> </ul> |
| Operator              | <ul style="list-style-type: none"> <li>• Can perform all actions on all the <b>Dashboard</b> and <b>Directories</b> menu items</li> <li>• Can perform log queries, view reports generated and sent by other users, and update user account information</li> <li>• Can only view information on the <b>Policy Management</b> screen</li> <li>• Cannot monitor, review, or investigate DLP incidents triggered by any Active Directory user</li> </ul>   |
| Power_User            | <ul style="list-style-type: none"> <li>• Can perform all actions on all the <b>Dashboard</b> and <b>Directories</b> menu items</li> <li>• Can perform log queries, maintain logs, and generate and maintain reports</li> <li>• Can only view information on the <b>Policy Management</b> screen</li> <li>• Cannot monitor, review, or investigate DLP incidents triggered by any Active Directory user</li> </ul>  |

| ROLE                | DESCRIPTION   |
|---------------------|---|
| Read-only_User      | <ul style="list-style-type: none"> <li>• Can view information on all menu items and update user account information</li> <li>• Can perform all actions on the <b>Dashboard</b></li> <li>• Can perform log queries, generate reports, create custom report templates, search directories, and create and use custom tags/filters to manage the User/Endpoint Directory tree</li> <li>• Cannot view reports generated by other users</li> </ul> |
| SSO_User            | <ul style="list-style-type: none"> <li>• Can perform all actions on all menu items</li> <li>• Cannot monitor, review, or investigate DLP incidents triggered by any Active Directory user</li> </ul> <hr/> <div data-bbox="431 654 489 704"></div> <p><b>Note</b><br/>This user role is hidden by default.</p> <hr/>  |
| Threat_Investigator | <ul style="list-style-type: none"> <li>• Can investigate security threat incidents on managed endpoints/servers</li> </ul>  |

**Note**

The **Operator** and **Power User** roles in previous versions do not have permissions to perform actions on **Policy Management** menu items. After upgrading to this version, these two roles will have read-only permissions, which cannot be changed.

## Adding a User Role

You can use the **User Roles** screen to create custom user roles.

### Procedure

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

The **User Roles** screen appears.

---

2. Click **Add**.

The **Add Role** screen appears.

3. In the **Role Information** section:

- a. Type a unique user role name in the **Name** field.
- b. Provide a meaningful description for the user role in the **Description** field.



**Note**

The description appears in the User Roles list. Providing a meaningful description can help administrators quickly identify a user role if the user role name cannot fully convey the use for the user role.

---

4. In the **Menu Access Control** section, select the accessible menu items for the user role.

5. Specify access rights for the selected menu items.

- **Full control, except:** Select to allow users to perform all actions available on the accessible menu items
    - **Create, copy and import policies:** Select to prevent users from creating, copying, or importing policies on the **Policy Management** screen
- For more information, see [Policy Management on page 14-2](#).
- **Monitor, review, and investigate DLP incidents triggered by all users:** Select to prevent users from investigating DLP incidents triggered by all Active Directory users
  - **Read only:** Select to only allow users to view information on menu items selected in the **Menu Access Control** section

6. Click **Save**.

The new user role appears on the **User Roles** screen.

---

## Editing a User Role

Apex Central allows you to modify the access rights for a custom user role.

For information about editing the user role assigned to a particular user account, see [Editing a User Account on page 4-11](#).



### Note

Managed product information displayed on accessible menu items depends on the managed product/directory permissions that Apex Central administrators specify in an individual's user account.

Example:

Bob and Jane are Apex One administrators. Both have identical user role permissions (they have access to the same menu items in the web console). However, Jane oversees operations for all Apex One servers. Bob only oversees operations for Apex One servers protecting desktops for the Marketing department. The information that they can view in the web console will be very different. Bob logs on and only sees information that is applicable to the Apex One servers that his Apex Central user account allows (the Apex One servers for the Marketing department). When Jane logs on, she sees information for all Apex One servers, because her Apex Central user account grants her access to all Apex One servers registered to Apex Central.

---

## Procedure

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

The **User Roles** screen appears.

2. Click the **Name** of a user role to edit.

The **Edit Role** screen appears.

3. Edit the user role information.
  4. Click **Save** to apply changes.
-

# Chapter 5

## License Management

This section discusses how to activate or renew product licenses for Apex Central and managed products.

Topics include:

- *[Apex Central Activation and License Information on page 5-2](#)*
- *[Managed Product Activation and Registration on page 5-4](#)*

## Apex Central Activation and License Information

Activating Apex Central allows you to use all of the product features, including downloading updated program components.

### Activating Apex Central

The **License Management** screen allows you to activate Apex Central after obtaining an Activation Code from your Trend Micro sales representative or reseller.

If you purchased a license for Apex One Sandbox as a Service, you can also activate the license from the **License Management** screen.



#### **Important**

After activating Apex Central, log off and then log on to the Apex Central web console for changes to take effect.

---

### Procedure

1. Go to **Administration > License Management > Apex Central**.  
The **License Information** screen appears and displays the current license information.
  2. Click the **Specify a new Activation Code** link.
  3. Type your Activation Code.
  4. Click **Activate**.
  5. Log off and then log on to the Apex Central web console for the changes to take effect.
- 

## Viewing and Renewing Apex Central License Information

The **License Management** screen displays your current Apex Central license information and activation status. You can access the Trend Micro Customer Licensing Portal from this screen to update or renew your license.

If you purchased a license for Apex One Sandbox as a Service, the **License Management** screen also displays the license information and activation status.

---

### **Procedure**

- 1. Go to **Administration > License Management > Apex Central**.**

The **License Information** screen appears and displays the current license information.

- 2. To update the screen with the latest license information:**
    - a. Click **Update License Information**.**
    - b. Log off and then log on to the Apex Central web console for the changes to take effect.**
  - 3. To renew your license:**
    - a. Click the **Specify a new Activation Code** link.**
    - b. Type your Activation Code.**
    - c. Click **Activate**.**
    - d. Log off and then log on to the Apex Central web console for the changes to take effect.**
  - 4. To view information about the current license in the Trend Micro Customer Licensing Portal:**
    - a. Click **View online**.**
    - b. Sign in to the Customer Licensing Portal using your Trend Micro account and password.**
    - c. Click the **My Products/Services** menu tab.**
    - d. Expand the **Products/Services** categories to view license information for registered Trend Micro products.**
-

## Managed Product Activation and Registration

To use Apex Central, managed products (for example, Apex One, ScanMail for Microsoft Exchange) and other services, you need to obtain Activation Codes and activate the software or services. Included with the software is a Registration Key. Use that key to register your software online on the Trend Micro Customer Licensing Portal website and obtain an Activation Code.

When managed products register to Apex Central, the managed products add their Activation Codes to the managed product Activation Code list on the **License Management** screen. Administrators can add new Activation Codes to the list and redeploy renewed Activation Codes.

### License Management Details

The following table describes the managed product license information that displays on the **License Management** screen (**Administration > License Management > Managed Products**).



#### Tip

You can clear the **Hide expired Activation Codes** check box to view license details for all managed products.

| COLUMN NAME        | DESCRIPTION  |
|--------------------|--|
| Activation Code    | Displays the Activation Code for the managed product   |
| Note               | Displays additional information about the Activation Code  |
| Activated Products | Displays the number of managed products to which the Activation Code deploys   |
| License Status     | Displays the status of the Activation Code: <ul style="list-style-type: none"> <li>• Valid</li> <li>• Expired</li> </ul> |



| COLUMN NAME                     | DESCRIPTION   |
|---------------------------------|---|
| Type                            | <p>Displays the type of the Activation Code:</p> <ul style="list-style-type: none"> <li>• <b>Full:</b> Allows full use of the product for the maintenance period (typically 1 year)</li> <li>• <b>Trial:</b> Allows full use of the product for the evaluation period (typically 3 months)</li> </ul>     |
| Expiration Date                 | Displays the date the Activation Code expires   |
| Seat Count                      | Displays the number of seats the Activation Code allows   |
| View license information online | <p>Click the link to open your default web browser to the Trend Micro Customer Licensing Portal.</p> <p>This portal allows you to manage your Trend Micro business account, which includes Activation Codes for on-premise products and subscriptions to Trend Micro Software as a Service solutions.</p> |

## Managed Product License Information

Clicking an **Activation Code** on the **License Management** screen (**Administration > License Management > Managed Products**) displays the following license information about the managed product/service.

| FIELD           | DESCRIPTION   |
|-----------------|---|
| Activation Code | The code used to activate the license for the product/service   |
| Status          | The license status (for example, "Valid")   |
| Type            | The type of license for the product/service (for example, "Full" or "Trial")  |
| Expiration date | The expiration date of the product/service license  |
| Description     | <p>The user-defined description for the Activation Code</p> <ul style="list-style-type: none"> <li>• Type a description in the text box and click <b>Finish</b> to save changes.</li> </ul> |

## Activating Managed Products

Use the **License Management** screen to activate managed product licenses. Activating managed products allows you to use all the features for the product, including downloading updated program components. You can activate managed products after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

---

### Procedure

1. Go to **Administration > License Management > Managed Products**.

The **License Management** screen appears.

2. Click **Add and Deploy**.

The **Add and Deploy a New License > Step 1: Input Activation Code** screen appears.

3. Type the Activation Code for the product you want to activate in the **New activation code** field.

4. Click **Next**.

The **Add and Deploy a New License > Step 2: Select Targets** screen appears.

---



#### Note

If no products appear in the list, the selected Activation Code does not support any products currently registered to Apex Central. This could mean that the managed product does not support receiving Activation Codes from Apex Central servers.

---

5. Select the managed product(s) to which to deploy the Activation Code.
6. Click **Deploy**.

The **License Management** screen appears and lists the new Activation Code in the table.

**Note**

The Activation Code deployment status appears in a toast message at the top of the **License Management** screen.

Click the link in the message to view the deployment status details on the **Command Tracking** screen.

---

## Renewing Managed Product Licenses

Apex Central can deploy or redeploy Activation Codes to registered products from the **License Management** screen.

---

### Procedure

1. Go to **Administration > License Management > Managed Product**.

The **License Management** screen appears.

2. Select an Activation Code from the list.
3. Click **Re-Deploy**.

The **Re-Deploy License** screen appears.

4. Select the product(s) for Activation Code deployment.
- 

**Note**

- If no products appear in the list, the selected Activation Code does not support any products currently registered to Apex Central.
  - You must select at least one product in order to deploy the Activation Code.
- 

5. Click **Deploy**.

Apex Central deploys the Activation Code to the selected product(s).

---



## Chapter 6

# Active Directory and Compliance Settings

This section discusses how to configure Active Directory integration and compliance indicator settings in Apex Central.

Topics include:

- *Active Directory Integration on page 6-2*
- *Compliance Indicators on page 6-6*
- *Endpoint and User Grouping on page 6-11*

## Active Directory Integration

Integrate Apex Central with a Microsoft Active Directory server to:

- Allow administrators to create user accounts for web console access based on Active Directory users or groups.

For more information, see [Adding a User Account on page 4-5](#).

- Map 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).

For more information, see [User/Endpoint Directory on page 7-2](#).

- Use the site location and reporting line information in Active Directory to gain greater insight into your network protection status on the **Security Posture** dashboard tab.

For more information, see [Compliance Indicators on page 6-6](#).

## Configuring Active Directory Connection Settings

Specify the connection settings to allow Apex Central to synchronize endpoint and user information from Active Directory servers.



### Note

Apex Central supports synchronization with multiple Active Directory forests. Adding an Active Directory domain automatically synchronizes all domains from the same forest.

For more information about forest trusts, contact your Active Directory administrator.

---

### Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.

2. Click the **Active Directory Settings** tab.
3. Select **Enable Active Directory synchronization and authentication**.
4. Configure the connection settings to access an Active Directory server.

| FIELD          | DESCRIPTION   |
|----------------|---|
| Server address | Type the FQDN or IP address (IPv4 or IPv6) of the Active Directory server.  |
| User name      | Type the domain name and user name required to access the Active Directory server.<br>Example format, <code>domain\user_name</code> |
| Password       | Type the password required to access the Active Directory server.   |

- To add another Active Directory server, click the add icon (+).
  - To delete an Active Directory server, click the delete icon (-).
5. From the **Synchronization frequency (in hours)** drop-down list, select how often Apex Central synchronizes data with Active Directory servers.



#### Note

Active Directory synchronization times vary based on the size and complexity of the Active Directory database. You may need to wait for more than an hour before synchronization completes.

6. (Optional) Expand **Advanced settings** to configure the **Synchronization source** or **Connection mode**.
  - a. Select one of the following synchronization sources:
    - **Domain controllers:** Synchronizes all domains from multiple forests with trust relationships
    - **Global catalog:** Synchronizes all domains from a single forest

**Important**

Some information used by Apex Central, such as geographic location and user membership in global groups or domain local groups, cannot be synchronized from a global catalog with default settings. Choose to synchronize from a global catalog only if your network policy restricts Apex Central from connecting to all domain controllers.

---

**b.** Select one of the following connection modes:• **SSL****Important**

To use an SSL connection, import the Active Directory Certificate to the Apex Central server.

---

• **Non-SSL****7.** (Optional) Click **Test Connection** to test the server connection.**Note**

Testing the connection does not save the Active Directory server settings.

---

The Active Directory server connection status icon (✓ or ✗) appears in front of the server address.

**8.** Click **Save**.

Apex Central synchronizes endpoint and user information from the Active Directory server(s) according to the synchronization frequency.

**9.** (Optional) Configure which Active Directory domains and OUs Apex Central synchronizes by modifying the `ADSyncOUList.config` configuration file located at:

```
<Apex Central installation directory>\ADSyncOUList.config
```



10. (Optional) Click **Synchronize Now** to manually synchronize Active Directory data.

The Active Directory server connection status icon (✔ or ✘) appears in front of the server address.

11. To remove a synchronized Active Directory server:
- a. Clear the **Enable Active Directory synchronization** check box.
  - b. Click **Clear Data** to purge the Apex Central server of data from the removed Active Directory server.

Apex Central removes the synchronized Active Directory server.



**Note**

Clicking **Clear Data** triggers a scheduled task, which runs every 2 minutes, to purge all data of the removed Active Directory servers from the Apex Central database.

## Troubleshooting Active Directory Synchronization

Active Directory synchronization allows Apex Central to obtain user information (such as site and reporting line information) from Active Directory servers.

If an Active Directory related error appears on the **Dashboard** screen, refer to the following table for troubleshooting solutions.

| ISSUE                           | SOLUTION  |
|---------------------------------|---|
| Incorrect user name or password | <ul style="list-style-type: none"> <li>• Ensure that you specified the correct account information.</li> <li>• Verify that the user account has privileges to access the Active Directory server.</li> </ul> <p>For assistance, contact the Active Directory administrator.</p> |

| ISSUE  | SOLUTION  |
|--|---|
| Unable to connect to the Active Directory server | <ul style="list-style-type: none"> <li>• Ensure that you have configured the correct Active Server connection settings.<br/>For more information, see <a href="#">Configuring Active Directory Connection Settings on page 6-2</a>.</li> <li>• Check that the Active Directory server is available.</li> <li>• Check your network connection and firewall settings.</li> <li>• Ensure that both the Apex Central and Active Directory servers can establish communication with one another.<br/><br/>To test your Apex Central connection to Active Directory servers, click <b>Test Connection</b> on the <b>Active Directory and Compliance Settings</b> screen.</li> </ul> |
| Unable to access the Apex Central database       | <p>Ensure that the connection to the Apex Central database is present.<br/>For more information, see <a href="#">Understanding the Apex Central Database on page 25-2</a>.</p>  |

If the connection issue persists, contact Support.

For more information, see [Technical Support on page 27-1](#).

## Compliance Indicators

Apex Central includes the following compliance indicators and performs compliance calculations based on the indicator settings and the user and endpoint information synchronized from Active Directory servers. You can view the information for the compliance indicators on the **Security Posture** dashboard tab.

- **Antivirus Pattern Compliance:** The percentage of managed Apex One Security Agents using acceptable antivirus pattern (Virus Pattern and Smart Scan Agent Pattern) versions
- **Data Loss Prevention Compliance:** The percentage of managed Data Discovery-enabled Apex One and Cloud App Security agents with an acceptable number of sensitive data detection incidents

The following provides an overview of the procedures to get Apex Central to perform compliance calculations and display compliance information on the **Security Posture** dashboard tab.

---

### Procedure

1. Connect to an Active Directory server to synchronize the user and endpoint information.

For more information, see [Configuring Active Directory Connection Settings on page 6-2](#).

2. Configure the compliance indicator settings.

For more information, see the following topics:

- [Configuring the Antivirus Pattern Compliance Indicators on page 6-8](#)
- [Configuring the Data Loss Prevention Compliance Indicator on page 6-10](#)

3. (Optional) Customize endpoint and user grouping based on Active Directory sites and reporting lines.

For more information, see [Endpoint and User Grouping on page 6-11](#).

4. Go to the **Dashboard** to view the compliance information.



#### Note

To change the Active Directory grouping or view the Data Discovery compliance of your managed agents, configure the **Security Posture** tab settings.

For more information, see the following topics:

- [Security Posture Tab on page 3-6](#)
  - [Working with Widgets on page 3-4](#)
-

## Configuring the Antivirus Pattern Compliance Indicators

You can configure settings and exceptions for the Antivirus Pattern Compliance indicators to display the percentage of managed Security Agents using acceptable antivirus pattern (Virus Pattern and Smart Scan Agent Pattern) versions on the **Security Posture** tab.

**Note**

Apex Central supports Security Agents for the following managed products:

- Apex One
- Worry-Free Business Security Services

### Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.
2. Click the **Compliance Indicator** tab.
3. Click **Antivirus pattern compliance**.
4. The following table describes the available configuration options.

| COLUMN                      | DESCRIPTION   |
|-----------------------------|---|
| Acceptable pattern versions | Specify the pattern versions for endpoints to be considered compliant.                              |
| Alert indicator             | Adjust the slider control to set the thresholds (% of compliant agents) for different alert levels. |

5. In the **Exception List**, select custom tags or filters to exclude users or endpoints from compliance calculations.

**Note**

- The Exceptions list applies to all Apex Central users. You may only add or delete exceptions based on your permissions to modify the corresponding tags and filters.
  - For more information about creating tags or filters, see [Custom Tags and Filters on page 7-29](#).
- 

**a. Click **Add**.**

The **Add Exception** screen appears.

**b. From the **Type** drop-down list, select **User** or **Endpoint** to display the available custom filters and tags by type; otherwise, select **All** to view all entries.****Note**

To search for a custom filter or tag, type a name in the text field and press ENTER.

For more information on custom tags and filters, see [Custom Tags and Filters on page 7-29](#).

---

**c. Select one or more custom tags or filters and click **Add**.**

The selected items appear in the Exception List.

**d. Click **Close**.****e. Click **Save**.****f. Specify the scope of the added custom tags or filters from the **Apply exceptions added by** drop-down list.**

- **All user accounts:** Excludes all users and endpoints specified in custom filters and tags added by any user account
- **Only the logged on account:** Excludes only the users and endpoints specified in custom filters and tags added by the currently logged on user account

6. Click **Save**.

## Configuring the Data Loss Prevention Compliance Indicator

You can configure settings and exceptions for the Data Loss Prevention Compliance indicator to display the percentage of managed Data Discovery-enabled Security Agents with an acceptable number of sensitive data detection incidents on the **Security Posture** tab.

### Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.
2. Click the **Compliance Indicator** tab.
3. Click **Data Loss Prevention compliance**.
4. The following table describes the available configuration options.

| COLUMN                                 | DESCRIPTION   |
|--|---|
| Period                                 | Specify the time range for the displayed data.  |
| Acceptable number of threat detections | Type the acceptable number of sensitive data detection incidents.                                   |
| Alert indicator                        | Adjust the slider control to set the thresholds (% of compliant agents) for different alert levels. |

5. In the **Exception List**, select custom tags or filters to exclude users or endpoints from compliance calculations.



### Note

- The Exceptions list applies to all Apex Central users. You may only add or delete exceptions based on your permissions to modify the corresponding tags and filters.
- For more information about creating tags or filters, see [Custom Tags and Filters on page 7-29](#).

- a. Click **Add**.

The **Add Exception** screen appears.

- b. From the **Type** drop-down list, select **User** or **Endpoint** to display the available custom filters and tags by type; otherwise, select **All** to view all entries.

**Tip**

To search for a custom filter or tag, type a name in the text field and press ENTER.

For more information on custom tags and filters, see [Custom Tags and Filters on page 7-29](#).

---

- c. Select one or more custom tags or filters and click **Add**.

The selected items appear in the Exception List.

- d. Click **Close**.

- e. Click **Save**.

- f. Specify the scope of the added custom tags or filters from the **Apply exceptions added by** drop-down list.

- **All user accounts:** Excludes all users and endpoints specified in custom filters and tags added by any user account
- **Only the logged on account:** Excludes only the users and endpoints specified in custom filters and tags added by the currently logged on user account

6. Click **Save**.
- 

## Endpoint and User Grouping

Apex Central can group endpoints or users on the **Security Posture** tab based on the following information:

- Site locations


- Reporting line managers

By default, Apex Central synchronizes the user or endpoint site and reporting line information from Active Directory. You can configure custom site and reporting line groups to display compliance information.

## Sites

The following table describes the site information displayed on the **Sites** tab.

**TABLE 6-1. Sites**

| COLUMN       | DESCRIPTION   |
|--------------|---|
| Display Name | Type the name that displays on the <b>Security Posture</b> widget/tab.<br><br><div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note</b><br/>           By default, the <b>Others</b> group includes endpoints that do not belong to any site.         </div> |
| Site         | The site name synchronized from Active Directory  |

## Creating a Custom Site

You can create a custom site group to include endpoints or users in a specified IP address range.

### Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.
2. Click the **Sites** tab.
3. Click **Add Custom**.

The **Add Custom Site** screen appears.

4. Specify the **Display name** that identifies the group on the **Security Posture** widget/tab.



5. Select the **Node color** that identifies the group on the **Security Posture** widget/tab.
6. Specify the IPv4 or IPv6 address range of the endpoints included in the custom site
7. Click **Save**.

After creating a custom site:

- Click **Delete Custom** to delete a selected custom site.
- Click the custom site name to change the settings.

---

## Merging Sites

You can create a custom site by merging two or more sites. After merging preexisting sites, Apex Central removes the original sites from the list.



### Tip

Apex Central indicates a merged group using a solid dot icon (●).

---

## Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.
2. Click the **Sites** tab.
3. Select two or more sites.
4. Click **Merge**.

The **Merge Sites** screen appears.

5. Specify the **Display name** that identifies the group on the **Security Posture** widget/tab.
6. Select the **Node color** that identifies the group on the **Security Posture** widget/tab.


7. Click **Save**.

After merging sites, you can click **Split** to split a merged site.

## Reporting Lines

The following table describes the information displayed on the **Reporting Lines** tab.

**TABLE 6-2. Reporting Lines**

| DATA                 | DESCRIPTION   |
|----------------------|---|
| Reporting line level | The reporting line level indicates the level of management hierarchy for a user in Active Directory.<br><br>Select a level number from the <b>Reporting line level</b> drop-down list and click <b>Apply</b> to update the list.  |
| Display Name         | The name that displays on the <b>Security Posture</b> tab<br><br><div style="border: 1px solid black; padding: 5px;">  <b>Tip</b><br/>By default, the <b>Others</b> group includes all managers that are at reporting line levels higher than the selected level. </div> |
| Manager              | The reporting line manager<br><br>This information is synchronized from an Active Directory server.   |

## Creating a Custom Reporting Line

You can create a custom reporting line to group users that report directly or indirectly to the selected managers.

### Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.

2. Click the **Reporting Lines** tab.
3. (Optional) Change the **Reporting line level** setting and click **Apply** to update the list.

The reporting line level indicates the level of management hierarchy for a user in Active Directory.

4. Click **Add Custom**.  
The **Add Custom Reporting Line** screen appears.
5. Specify the **Display name** that identifies the group on the **Security Posture** widget/tab.
6. Select a user from the **Users** list and click the icon to add to the **Selected Users** list.

**Note**

To select more than one user, press CTRL and click the user names.

---

7. Click **Save**.

After creating a custom reporting line:

- Click **Delete Custom** to delete a selected custom reporting line.
  - Click the custom group name to change the settings.
- 

## Merging Reporting Lines

You can create a custom reporting line by merging two or more reporting lines. After merging preexisting reporting lines, Apex Central removes the original reporting lines from the list.

---

**Tip**

Apex Central indicates a merged group using a solid dot icon (●).

---

---

## Procedure

1. Go to **Administration > Settings > Active Directory and Compliance Settings**.
2. Click the **Reporting Lines** tab.
3. Select two or more reporting lines.
4. Click **Merge**.

The **Merge Reporting Line** screen appears.

5. Specify the **Display name** that identifies the group on the **Security Posture** widget/tab.
6. Click **Save**.

After merging reporting lines, you can click **Split** to split a merged reporting line.

---

# Chapter 7

## User/Endpoint Directory

This section discusses how to view information about all the users and endpoints within the Apex Central network.

Topics include:

- *User/Endpoint Directory on page 7-2*
- *User Details on page 7-3*
- *Endpoint Details on page 7-10*
- *Active Directory Details on page 7-19*
- *Affected Users on page 7-19*
- *Using the Advanced Search on page 7-24*
- *Custom Tags and Filters on page 7-29*

## User/Endpoint Directory

The **User/Endpoint Directory** screen displays information about all the users and endpoints within the Apex Central network for a specified time range.

- Use the drop-down controls below the **Endpoints** or **Users** tab to specify the time period for the data that displays or to switch between **Tabular view** and **Timeline view**.
- Click **Export** to export the data as a \*.csv file or \*.png image.



### Note

**Tabular view** only supports exporting data as a \*.csv file. **Timeline view** can export data as a \*.csv file or a \*.png image. The exported \*.png timeline image only displays information for a maximum of 30 users or endpoints.

---

The User/Endpoint tree organizes data into the following categories:

- **Users:** Contains information about any user that logs on an endpoint or that is part of the integrated Active Directory structure

For more information, see [User Details on page 7-3](#).

- **Endpoints:** Contains information about any endpoint that sends logs to Apex Central or that is part of the integrated Active Directory structure

For more information, see [Endpoint Details on page 7-10](#).

- **Active Directory:** Displays the organizational units of the integrated Active Directory server



### Note

Apex Central supports synchronization with multiple Active Directory forests. Adding an Active Directory domain automatically synchronizes all domains from the same forest.

For more information about forest trusts, contact your Active Directory administrator.

---

You can change the default data that displays in the **Users** and **Endpoints** nodes through use of advanced searches, tags, and filters.

For more information, see [Using the Advanced Search on page 7-24](#) and [Custom Tags and Filters on page 7-29](#).

## User Details

The **User/Endpoint Directory** screen displays User information for a specified time range.

- Use the drop-down controls below the **Endpoints** or **Users** tab to specify the time period for the data that displays or to switch between **Tabular view** and **Timeline view**.
- Click **Export** to export the data as a \*.csv file or \*.png image.






### Note

**Tabular view** only supports exporting data as a \*.csv file. **Timeline view** can export data as a \*.csv file or a \*.png image. The exported \*.png timeline image only displays information for a maximum of 30 users or endpoints.


The following table describes the User information that displays on the **User/Endpoint Directory** screen in **Tabular view**.

**TABLE 7-1. User Details in Tabular View**

| COLUMN  | DESCRIPTION   |
|---|---|
|  | <p>If the endpoint or user is assigned an importance tag, Apex Central displays a yellow star icon (  ) to indicate importance.</p> <p>For more information, see <a href="#">User or Endpoint Importance on page 7-37</a>.</p> |



| COLUMN  | DESCRIPTION   |
|---------|---|
| User    | <p>Apex Central identifies and associates users with endpoints based on the type of endpoint or through integration with Active Directory.</p> <ul style="list-style-type: none"> <li>• Server and desktop platforms: Apex Central associates the last logged on user with the endpoint</li> <li>• Mobile devices: <ul style="list-style-type: none"> <li>• If Active Directory synchronization is available, Apex Central resolves the registered email address for the mobile device with the associated Active Directory account</li> <li>• If Active Directory synchronization is not available, Apex Central displays the registered email address for the mobile device</li> </ul> </li> </ul> <p>Click a user name to view contact details.</p> <p>For more information, see <a href="#">Contact Information on page 7-9</a>.</p> <hr/> <p> <b>Note</b></p> <p>The <b>Users &gt; All</b> node lists all local users from various endpoints regardless of their duplicate status. Duplicate users having the same names can occur. Apex Central consolidates all endpoints from managed products that have multiple local users.</p> |
| Domain  | <ul style="list-style-type: none"> <li>• If Active Directory synchronization is available, this Apex Central displays the domain name that the user is a member of.</li> <li>• If Active Directory synchronization is not available, this Apex Central displays the endpoint/host name that the user was the last person to log on to.</li> </ul>   |
| Manager | <p>If Active Directory synchronization is available, Apex Central displays the manager of the user</p> <p>Click a name in the manager column to view the manager's contact details.</p> <p>For more information, see <a href="#">Contact Information on page 7-9</a>.</p>   |



| COLUMN    | DESCRIPTION   |
|-----------|---|
| Endpoints | <p>The number of endpoints currently associated with the user, based on the last log on information from the endpoints</p> <p>Click the count to view the related endpoint information in the table.</p> <p>For more information, see <a href="#">Endpoint Details on page 7-10</a>.</p>  |
| Policies  | <p>The number of policies currently associated with the user, based on the last log on information from the endpoints</p> <p>Click the <b>Policies</b> count to view the related policy information for the user.</p> <p>For more information, see <a href="#">Policy Status on page 7-8</a>.</p>   |
| Threats   | <p>The total number of security threats that occurred on endpoints associated with the user</p> <p>Click the <b>Threats</b> count to view the related threat information for the user.</p> <p>For more information, see <a href="#">Security Threats for Users on page 7-6</a>.</p> <p>For example, if Henry was the last user logged on to endpoint “us-mkt-dev1”, and that endpoint reported 10 virus/malware detections and 2 web violations, Henry’s <b>Threats</b> count displays as <b>12</b>.</p> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• If the network environment is not using Active Directory, the following detections/violations for gateway products do not display: email content violation, phishing email, and spam.</li> <li>• Security threats detected by endpoint products (for example, Apex One) are associated with the last logged-on user of the endpoint. Security threats detected by gateway products (for example, IWSVA) are associated with the user who triggered the detection.</li> </ul> |

The following table describes the User information that displays on the **User/Endpoint Directory** screen in **Timeline view**.

**TABLE 7-2. User Details in Timeline View**

| COLUMN     | DESCRIPTION   |
|------------|---|
| User       | Apex Central identifies and associates users with endpoints based on the type of endpoint or through integration with Active Directory.   |
| Threats    | <p>The total number of security threats that occurred on endpoints associated with the user</p> <p>Click the <b>Threats</b> count to view the related threat information for the user.</p> <p>For more information, see <a href="#">Security Threats for Users on page 7-6</a>.</p>   |
| <Timeline> | <p>The timeline indicates when the security threats occurred for each user.</p> <ul style="list-style-type: none"> <li>• Hover over a red warning dot (  ) to view the number of critical threats and the total number of all security threat detections for a user on a specific date.</li> <li>• Hover over a solid red dot (  ) to view the number of non-critical threat detections for a user on a specific date.</li> <li>• Click a red dot to view the related threat information for a specific date.</li> </ul> <p>For more information, see <a href="#">Security Threats for Users on page 7-6</a>.</p> |

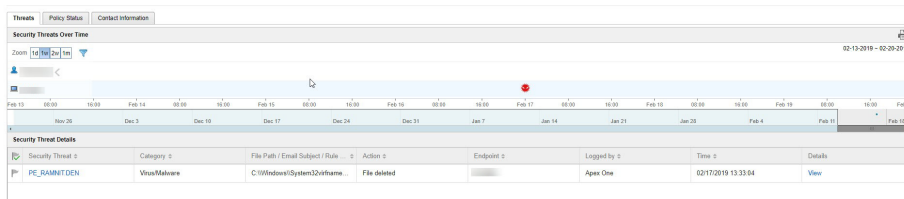
## Security Threats for Users



The **Threats** tab on the **User** information screen allows you to view all security threats detected on endpoints assigned to the selected user.

You can access this screen from the following widgets on the **Dashboard** > **Summary** tab on the Apex Central console.


- **Critical Threats:** Click a number in the **Important Users** or **Other Users** columns and then click the user you want to view.
- **Users with Threats:** Click the number in the **Threats** column for the user you want to view.

- **Endpoints with Threats:** Click the number in the **Threats** column for the endpoint you want to view. On the **Endpoint** information screen, click the **General Information** tab and click the user name.



- **Security Threats Over Time:** Provides a graphical representation of threat information based on the time of the detection and whether the detection occurred on an assigned endpoint or the user's account
  - Hover over a threat icon (for example, ) to view details about the detection.
  - Change the displayed time interval by changing the **Zoom** value.
  - Change the end date by scrolling through the dates displayed under the graph.
  - Apply filters by clicking the funnel icon () and selecting the following criteria and using the **OR** or **AND** operators to build advanced filters.
    - **Threat type:** Select a threat category from the second drop-down list
    - **Security threat:** Type a malware name or suspicious URL, IP address, or sender email address
    - **Threat status:** Select **Resolved by product**, **Action required**, or **Resolved manually**
- **Security Threat Details:** Provides more detailed information about the threats displayed on the **Security Threats Over Time** graph
  - Click a value in the **Security Threat** column to view the **Affected Users** screen.









For more information, see [Affected Users](#).

- Click **View** link in the **Details** column to view detailed information.
- Click a flag icon in the **Threat Status** column () to change the threat status for threats that require remediation.



### Note

Changing the threat status for a threat does not actually resolve the threat. The threat status is a case handling tool to help administrators track identified threats and indicate to other administrators that a threat has been resolved.

| THREAT STATUS   | DESCRIPTION  |
|---|--|
| Resolved by product (  ) | Indicates that the threat has been resolved by a managed product<br><hr/>  <b>Note</b><br>You cannot change this threat status.   |
| Action required (  )     | Indicates that remediation is required<br><br>Click the <b>Action required</b> icon (  ) to change the threat status to <b>Resolved manually</b> (  )                                 |
| Resolved manually (  ) | Indicates that remediation has been performed by an administrator<br><br>Click the <b>Resolved by product</b> icon (  ) to change the threat status to <b>Action required</b> (  ) |

## Policy Status

The **Policy Status** tab displays all the products installed on the target endpoint, any Apex Central policies assigned, and the current policy status for each installed product.

**Note**

Apex Central identifies and associates users with endpoints based on the type of endpoint or through integration with Active Directory.

---

Click the **Assigned Policy** name to view or edit a policy.

## Contact Information

The **Contact Information** screen displays user details, similar to the entries in Active Directory.

## Synchronizing Contact Information with Active Directory

Apex Central synchronizes data from the Active Directory Global Category (GC).

---

### Procedure

1. Open the Microsoft Management Console (mmc).
  2. Add a snap-in (Active Directory Schema).
  3. In left panel, go to **Attribute**.
  4. Enable **Replicate this attribute to Global Catalog** for each of the following:
    - **proxyAddresses**
    - **department**
    - **homephone**
    - **PhysicalDeliveryOfficeName**
    - **telephoneNumber**
    - **title**
  5. Wait until Active Directory replication occurs.
-

## Endpoint Details

The **User/Endpoint Directory** screen displays Endpoint information for a specified time range.



- Use the drop-down controls below the **Endpoints** or **Users** tab to specify the time period for the data that displays or to switch between **Tabular view** and **Timeline view**.
- Click **Export** to export the data as a \*.csv file or \*.png image.



### Note

**Tabular view** only supports exporting data as a \*.csv file. **Timeline view** can export data as a \*.csv file or a \*.png image. The exported \*.png timeline image only displays information for a maximum of 30 users or endpoints.



The following table describes the User information that displays on the **User/Endpoint Directory** screen in **Tabular view**.



| COLUMN  | DESCRIPTION   |
|---|---|
|  | If the endpoint or user is assigned an importance tag, Apex Central displays a yellow star icon (  ) to indicate importance.<br><br>For more information, see <a href="#">User or Endpoint Importance on page 7-37</a> . |
| Endpoint  | The host name or device name<br><br>Click an endpoint name to view the <b>Endpoint</b> screen that opens to the <b>Policy Status</b> tab.<br><br>For more information, see <a href="#">Policy Status on page 7-16</a> .   |
| IP Address  | The static or dynamic IP address of the endpoint  |
| Type  | Machine or device type: server, desktop, laptop, mobile device, and others  |
| Operating System  | The operating system running on the machine or device   |

| COLUMN          | DESCRIPTION   |
|-----------------|---|
| Endpoint Server | The server name and product installed on the server that manages the endpoint   |
| User            | The name or email address of the most recent user who logged on and/or used the endpoint<br><br>For more information, see <a href="#">Contact Information on page 7-9</a> .   |
| Threats         | The total number of security threats that occurred on the endpoint<br><br>Click the <b>Threats</b> count to view the related threat information for the endpoint.<br><br>For more information, see <a href="#">Security Threats on Endpoints on page 7-13</a> . |


The following table describes the Endpoint information that displays on the **User/Endpoint Directory** screen in **Timeline view**.

**TABLE 7-3. Endpoint Details in Timeline View**

| COLUMN   | DESCRIPTION  |
|----------|--|
| Endpoint | <p>The host name or device name</p> <p>Click an endpoint name to view the <b>Endpoint</b> screen that opens to the <b>Policy Status</b> tab.</p> <p>For more information, see <a href="#">Policy Status on page 7-16</a>.</p> <hr/> <p> <b>Note</b></p> <p>If the endpoint is assigned an important tag, Apex Central displays a yellow star icon (  ) in front of the endpoint name.</p> <p>For more information, see <a href="#">User or Endpoint Importance on page 7-37</a>.</p> |

| COLUMN     | DESCRIPTION  |
|------------|--|
| Threats    | <p>The total number of security threats that occurred on the endpoint</p> <p>Click the <b>Threats</b> count to view the related threat information for the endpoint.</p> <p>For more information, see <a href="#">Security Threats on Endpoints on page 7-13</a>.</p>  |
| <Timeline> | <p>The timeline indicates when the security threats occurred for each endpoint.</p> <ul style="list-style-type: none"> <li>• Hover over a red warning dot (  ) to view the number of critical threats and the total number of all security threat detections for an endpoint on a specific date.</li> <li>• Hover over a solid red dot (  ) to view the number of non-critical threat detections for an endpoint on a specific date.</li> </ul> <p>For more information, see <a href="#">Security Threats on Endpoints on page 7-13</a>.</p> |

## Endpoint Information

The **Endpoint** information screen provides more detailed information about the selected endpoint. The **Endpoint** information screen title displays the endpoint icon (  ) followed by the endpoint name.

Click one the following tabs to view related information.

- **Threats:** Displays all security threats detected on the selected endpoint  
For more information, see [Security Threats on Endpoints on page 7-13](#).
- **Policy Status:** Displays the list of policies associated with the selected endpoint  
For more information, see [Policy Status on page 7-16](#).
- **Notes:** Displays any manually added notes about the selected endpoint  
For more information, see [Notes for Endpoints on page 7-16](#).
- **General Information:** Displays basic information regarding the selected endpoint



For more information, see [General Information for Endpoints on page 7-16](#).

The **Endpoint** information screen also allows you to take specific actions on the selected endpoint by using the **Task** menu.

- **Assign tags:** Associates tags with the selected endpoint for search purposes

For more information, see [Custom Tags on page 7-31](#).

- **Isolate:** Limits the access the endpoint has to the network and Internet

For more information, see [Isolating Endpoints on page 20-34](#).

- **Restore:** Restores network access to the isolated endpoint

For more information, see [Isolating Endpoints on page 20-34](#).

## Security Threats on Endpoints

The **Threats** tab on the **Endpoint** information screen allows you to view all security threats detected on a specific endpoint.

You can access the **Threats** tab on the **Endpoint** information screen from the following locations:

- **Endpoints with Threats** widget: Click a count in the **Threats** column

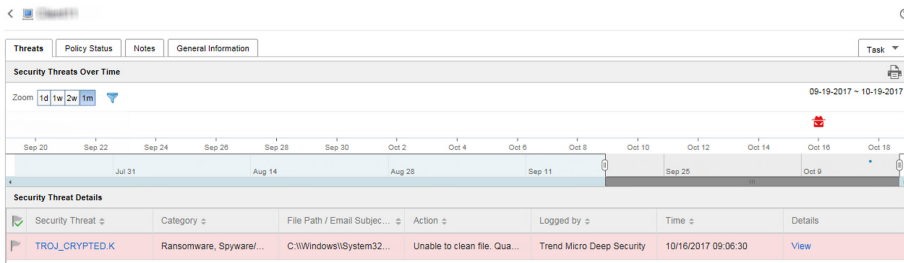
For more information, see [Endpoints with Threats Widget on page 3-21](#).

- **Endpoint Details** screen: Click a count in the **Threats** column

For more information, see [Endpoint Details on page 7-10](#).



- **Affected Users** tab on the **Security Threat** screen: Click an endpoint name in the **Host Name** column

For more information, see [Affected Users on page 7-19](#).




- **Task:** Allows you to **Assign tags**, or **Isolate** or **Restore** connections to the endpoint.

For more information, see [Isolating Endpoints on page 20-34](#).

- **Security Threats Over Time:** Provides a graphical representation of threat information based on the time of the detection and whether the detection occurred on an assigned endpoint or the user's account
  - Hover over a threat icon (for example, ) to view details about the detection.
  - Change the displayed time interval by changing the **Zoom** value.
  - Change the end date by scrolling through the dates displayed under the graph.
  - Apply filters by clicking the funnel icon () and selecting the following criteria and using the **OR** or **AND** operators to build advanced filters.
    - **Threat type:** Select a threat category from the second drop-down list
    - **Security threat:** Type a malware name or suspicious URL, IP address, or sender email address
    - **Threat status:** Select **Resolved by product**, **Action required**, or **Resolved manually**
- **Security Threat Details:** Provides more detailed information about the threats displayed on the **Security Threats Over Time** graph

- Click a value in the **Security Threat** column to view the **Affected Users** screen.









For more information, see [Affected Users](#).

- Click **View** link in the **Details** column to view detailed information.
- Click a flag icon in the **Threat Status** column () to change the threat status for threats that require remediation.



#### Note

Changing the threat status for a threat does not actually resolve the threat. The threat status is a case handling tool to help administrators track identified threats and indicate to other administrators that a threat has been resolved.

| THREAT STATUS   | DESCRIPTION  |
|---|--|
| Resolved by product (  ) | Indicates that the threat has been resolved by a managed product<br><br> <b>Note</b><br>You cannot change this threat status.   |
| Action required (  )    | Indicates that remediation is required<br>Click the <b>Action required</b> icon (  ) to change the threat status to <b>Resolved manually</b> (  )                              |
| Resolved manually (  ) | Indicates that remediation has been performed by an administrator<br>Click the <b>Resolved by product</b> icon (  ) to change the threat status to <b>Action required</b> (  ) |

## Policy Status

The **Policy Status** tab displays all the products installed on the target endpoint, any Apex Central policies assigned, and the current policy status for each installed product.

Click the **Assigned Policy** name to view or edit a policy.

## Notes for Endpoints

You can manually add notes to endpoints to help track issues and solutions on particular endpoints. For example, add additional notes on isolated endpoints while you are investigating and resolving threats or when you are about to restore the network connection after all threats have been resolved.

Apex Central automatically adds the following notes corresponding to specific actions:


- “Isolate”
- “Restore”
- “Assign Tag {tag name}”
- “Remove Tag {tag name}”

For more information, see [Assigning Custom Tags to Users/Endpoints on page 7-33](#) and [Isolating Endpoints on page 20-34](#).

## General Information for Endpoints

You can view the following information about the endpoint:

| INFORMATION      | DESCRIPTION                                  |
|------------------|--|
| IP Address       | The IP address of the endpoint               |
| Type             | The type of endpoint (for example, “Laptop”) |
| Operating System | The operating system on the endpoint         |

| INFORMATION | DESCRIPTION  |
|-------------|--|
| User        | <p>The user account associated with the endpoint</p> <hr/> <div data-bbox="529 329 585 378">  </div> <p><b>Note</b><br/>Apex Central identifies and associates users with endpoints based on the type of endpoint or through integration with Active Directory.</p> <hr/> |
| Domain      | The Active Directory domain associated with the endpoint   |

## Isolating Endpoints

Isolate at-risk endpoints to run an investigation and resolve security issues. Restore the connection promptly when all issues have been resolved.

---

### Procedure

1. Go to **Directories > Users/Endpoints**.
2. Select to view endpoints.
3. Click the name of an endpoint in the list.
4. On the **Endpoint** information screen that appears, click **Task > Isolate**.

Apex Central disables the **Isolate** option on endpoints for the following reasons:

- The agent on the endpoint runs an unsupported version.
  - The user account used to log on to Apex Central does not have the necessary permissions.
5. A message appears at the top of the **Endpoint** information screen that allows you to monitor the isolation status. After isolation completes, the message closes and a notification appears on the target endpoint to inform the user.


If a problem occurs during the isolation process, the message at the top of the **Endpoint - {name}** screen informs you of the problem.

6. To view all isolated endpoints on your Apex Central network, click the **Endpoints > Filters > Network Connection > Isolated** node in the User/Endpoint Directory tree.
7. (Optional) To configure allowed inbound and outbound traffic to all isolated endpoints:

For a list of default Trend Micro communication ports, see [Downloading Security Agent Installation Packages on page 10-2](#).

- a. Click the **Control** hyperlink in the note on the screen that appears.

Endpoint Isolation

 The endpoint that you wish to isolate will be disconnected from the network. Restore the connection after you finish your investigation.

For OfficeScan agents running versions 11 SP1 to XG SP1, you must enable the OfficeScan Firewall to perform endpoint isolation.

Note: You can **control** allowed traffic on endpoints while they are isolated.

Isolate Endpoint    Isolate Cancel

- b. Select **Control traffic on isolated endpoints**.
- c. Expand the **Inbound Traffic** or **Outbound Traffic** sections.
- d. Specify the allowed traffic by specifying the **Protocol, IP Address, and Destination Port**.  
Separate multiple destination ports using commas.
- e. Add multiple inbound and outbound entries by clicking the - control to the right of the **Destination Port** information.

**Note**

After modifying the allowed traffic settings, all previously isolated endpoints and any endpoints isolated later apply the inbound and outbound traffic settings.

---

8. After you have resolved the security threats on an isolated endpoint, restore network connectivity from the following locations:
    - **Endpoint** information screen: Click **Task > Restore**.
    - **Endpoints > Filters > Network Connection > Isolated**: Select the endpoint row in the table and click **Task > Restore Network Connection**.
  9. A message appears at the top of the screen that allows you to monitor the restoration status. After restoration completes, the message closes and a notification appears on the target endpoint to inform the user.

If a problem occurs during the restoration process, the message at the top of the screen informs you of the problem.
- 

## Active Directory Details

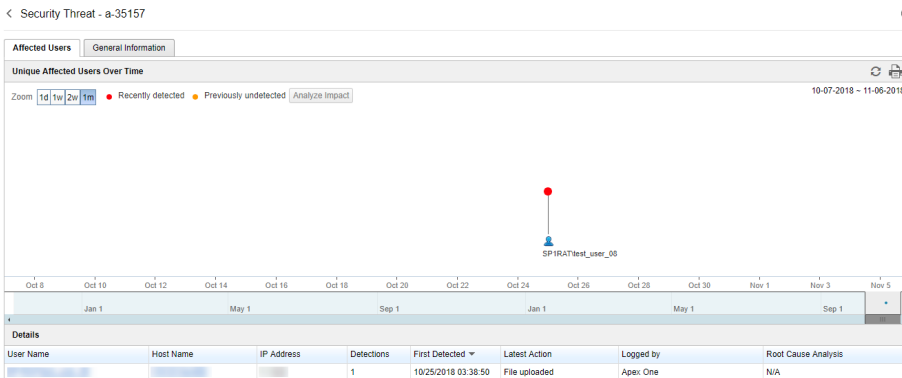
The Active Directory node displays the integrated Active Directory structure. When viewing an organizational unit in the Active Directory node, the list provides two tabs:

- **Users**: For more information, see [User Details on page 7-3](#).
- **Endpoints**: For more information, see [Endpoint Details on page 7-10](#).

## Affected Users

The **Affected Users** tab on the **Security Threat** screen allows you to view the users that a specific threat targeted across your network.

You can access the **Affected Users** tab from the **User** or **Endpoint** information screens by clicking a **Security Threat** name in the table.



- **Unique Affected Users Over Time:** Provides a graphical representation of which users the threat affected and the time of the detection
  - Click **Analyze Impact** to start a Root Cause Analysis to determine whether the threat has affected other endpoints on your network.



### Important

Performing an Impact Analysis from the **Threat Information** screen requires a valid Apex One Endpoint Sensor license and enabling the Enable Sensor feature for the appropriate **Apex One Security Agent** or **Apex One (Mac)** policies.

For more information, see [Analyzing Impact on Affected Users on page 7-22](#).

- Click **Start Retro Scan** to scan historical web access logs for callback attempts to C&C servers and other related activities on your network.



**Important**

Performing a Retro Scan from the **Threat Information** screen requires adding at least one Deep Discovery Inspector server on the **Server Registration** screen on Apex Central and enabling Retro Scan on the registered Deep Discovery Inspector server.

For more information, see [Performing a Retro Scan on Affected Users on page 7-23](#).

---

- Hover over a user icon to view all users affected by this specific threat and its detection history in your environment
  - **Recently detected:** The threat detection occurred during scanning
  - **Previously undetected:** The threat detection occurred during an impact analysis of log data
- Change the displayed time interval by changing the **Zoom** value.
- Change the end date by scrolling through the dates displayed under the graph.
- **Details:** Provides more detailed information about the threats displayed on the **Unique Affected Users Over Time** graph
  - Click a value in the **User Name** or **Host Name** column to view more details.

For more information, see [Security Threats for Users](#) or [Security Threats on Endpoints](#).

## General Information for Security Threats

The information shown varies by threat type and threat-related information received from managed products.

## Analyzing Impact on Affected Users

You can perform a historical impact analysis of security threats in your environment from the **Affected Users** tab on the **Security Threats** screen in Apex Central.

Apex One Endpoint Sensor analyzes the impact of suspicious files, IP addresses, and domains in your environment by contacting agents and performing a historical scan of the agent logs to determine if the suspicious objects have affected your environment for a period of time without detection.



### Important

Impact analysis requires a valid Apex One Endpoint Sensor license. Ensure that you have a valid Apex One Endpoint Sensor license and enable the Enable Sensor feature for the appropriate **Apex One Security Agent** or **Apex One (Mac)** policies.

For more information, see the *Apex Central Widget and Policy Management Guide*.

---

### Procedure

1. On the Apex Central console, go to **Dashboard**.
2. On the **Users with Threats** or **Endpoints with Threats** widgets, click a number.
3. On the screen that appears, click a **Security Threat** name in the **Security Threat Details** table.

The **Affected Users** screen appears.

4. Click **Analyze Impact**.

Endpoint Sensor scans historical network traffic and logs for any detections of the suspicious object.

For more information, see [Historical Investigations in Endpoint Sensor on page 20-17](#).

---

## Performing a Retro Scan on Affected Users

You can perform a Retro Scan to scan historical web access logs for callback attempts to C&C servers and other related activities on your network from the **Affected Users** tab on the **Security Threats** screen in Apex Central.

Deep Discovery Inspector analyzes the impact of suspicious URLs based on historical network traffic information collected by Trend Micro Retro Scan.



### Important

Performing a Retro Scan from the **Threat Information** screen requires adding at least one Deep Discovery Inspector server on the **Server Registration** screen on Apex Central and enabling Retro Scan on the registered Deep Discovery Inspector server.

For more information, see the *Deep Discovery Inspector Administrator's Guide*.

---

### Procedure

1. On the Apex Central console, go to **Dashboard**.
2. On the **Users with Threats** or **Endpoints with Threats** widgets, click a number.
3. On the screen that appears, click a **Security Threat** name in the **Security Threat Details** table.

The **Affected Users** screen appears.

4. Click **Start Retro Scan**

Deep Discovery Inspector scans historical web access logs for callback attempts to C&C servers and other related activities on your network.

For more information, see [Retro Scan in Deep Discovery Inspector on page 7-23](#).

---

## Retro Scan in Deep Discovery Inspector

Retro Scan is a cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in your network.

Web access logs may include undetected and unblocked connections to C&C servers that have only recently been discovered. Examination of such logs is an important part of forensic investigations to determine if your network is affected by attacks.

Retro Scan stores the following log information in the Smart Protection Network:

- IP addresses of endpoints monitored by Deep Discovery Inspector
- URLs accessed by endpoints
- GUID of Deep Discovery Inspector

Retro Scan then periodically scans the stored log entries to check for callback attempts to C&C servers in the following lists:

- Trend Micro Global Intelligence list: Trend Micro compiles the list from multiple sources and evaluates the risk level of each C&C callback address. The C&C list is updated and delivered to enabled products daily.
- User-defined list: Retro Scan can also scan logs against your own C&C server list. Addresses must be stored in a text file.

**Important**

The Retro Scan screen in Deep Discovery Inspector only displays information for scans that use the Trend Micro Global Intelligence list.

---

## Using the Advanced Search

Apex Central allows you to search for Users or Endpoints using partial string matching. You can also filter the Users or Endpoints that display in the list using Boolean operators.

---

### Procedure

1. Go to **Directories > Users/Endpoints**.

The **User/Endpoint Directory** screen appears.

2. Click the **Advanced** link above the table.
3. In the **Search** drop-down, select **Users** or **Endpoints**.

The search criteria in the second drop-down control dynamically changes based on your selection.

For more information, see [Advanced Search Categories on page 7-26](#).

4. Add multiple search criteria using the Boolean operators to the right of the filters.
5. Add multiple search criteria using the Boolean operators to the right of the filters.
  - **OR**: Allows you to search for multiple values for the specified criteria. All records that match either value display.
  - **AND**: Allows you to select a new search criteria. Only records that match the values specified for this criteria and all other selected criteria values display.

To filter all users with "ja" in their name in the Finance department that report to "Mary" or "Bill" in the Active Directory domain "HR", specify the following criteria:

|        |       |                              |         |   |        |
|--------|-------|------------------------------|---------|---|--------|
| Search | Users | User name                    | ja      | × | OR     |
|        | AND   | Department                   | Finance | × | OR     |
|        | AND   | Direct manager               | Mary    | × | OR     |
|        |       |                              | OR      | × | OR     |
|        | AND   | Location in Active Directory | HR      | × | OR AND |

6. Display results by clicking one of the following:
  - **Search**: Displays the search results in the list but does not save the search criteria.
  - **Save as New Custom Filter**: Displays the search results in the list and prompts you to save the search criteria to a custom filter. The custom filter displays under the **Users** or **Endpoints** node in the User/Endpoint Directory tree.

For more information, see [Filters on page 7-34](#).

7. (Optional) Use the drop-down controls below the **Endpoints** or **Users** tab to specify the time period for the data that displays or to switch between **Tabular view** and **Timeline view**.
8. (Optional) Click **Export** to export the data as a \*.csv file or \*.png image.

**Note**

- **Tabular view** only supports exporting data as a \*.csv file.
- **Timeline view** can export data as a \*.csv file or a \*.png image.

## Advanced Search Categories


During an Advanced Search, use the following search criteria options for **Users** and **Endpoints**.

**TABLE 7-4. User Categories**

| CATEGORY                     | DESCRIPTION  |
|------------------------------|--|
| User name                    | The account name of local users or people belonging to an Active Directory structure   |
| Direct manager               | The account name of the person who users are assigned to report to   |
| Location in Active Directory | The organization unit from which to begin your search  |
| Department                   | The name of the department in your company that groups users based on their function (for example, Accounting) or other criteria |
| Active Directory group       | A collection of Active Directory user and computer accounts, contacts and other groups that can be managed as a single unit      |
| Threat type                  | Select a security threat type from the third drop-down list  |
| Security threat              | Search for a specific security threat by typing a malware name, URL, IP address, or sender email address                         |

| CATEGORY              | DESCRIPTION  |
|-----------------------|--|
| Threat status         | The remediation status indicated by the flag icon in the first column on the <b>Security Threats</b> screen: Resolved by product, Action required, Resolved manually<br><br>For more information, see <a href="#">Security Threats for Users on page 7-6</a> . |
| Importance            | The assigned importance level<br><br>For more information, see <a href="#">User or Endpoint Importance on page 7-37</a> .  |
| Active Directory site | The site name synchronized from the Active Directory<br><br>For more information, see <a href="#">Endpoint and User Grouping on page 6-11</a> .  |
| Reporting line        | The display name for the reporting line synchronized from the Active Directory<br><br>For more information, see <a href="#">Endpoint and User Grouping on page 6-11</a> .  |

**TABLE 7-5. Endpoint Categories**

| CATEGORY                     | DESCRIPTION   |
|------------------------------|---|
| Endpoint name                | The host or device name of the endpoint   |
| IP address                   | The IPv4 address range<br><br><hr/>  <b>Note</b><br>Searching by IPv4 segment requires a specific range starting with the first octet. The search returns all endpoints with IP addresses containing the entry.<br><hr/> |
| Endpoint type                | The type of computer or device: server, desktop, laptop, mobile device, or other  |
| Operating system             | The type of operating system on the endpoint  |
| Location in Active Directory | The organization unit from which to begin your search   |
| Threat type                  | Select a security threat type from the third drop-down list   |

| CATEGORY                  | DESCRIPTION  |
|---------------------------|--|
| Security threat           | Search for a specific security threat by typing a malware name, URL, IP address, or sender email address   |
| Threat status             | <p>The remediation status indicated by the flag icon in the first column on the <b>Security Threats</b> screen: Resolved by product, Action required, Resolved manually</p> <p>For more information, see <a href="#">Security Threats on Endpoints on page 7-13</a>.</p> |
| Compliance                | <p>The antivirus pattern compliance or Data Loss Prevention compliance status</p> <p>For more information, see <a href="#">Compliance Indicators on page 6-6</a>.</p>  |
| Importance                | <p>The assigned importance level</p> <p>For more information, see <a href="#">User or Endpoint Importance on page 7-37</a>.</p>  |
| Active Directory site     | <p>The site name synchronized from the Active Directory</p> <p>For more information, see <a href="#">Endpoint and User Grouping on page 6-11</a>.</p>  |
| Reporting line            | <p>The display name for the reporting line synchronized from the Active Directory</p> <p>For more information, see <a href="#">Endpoint and User Grouping on page 6-11</a>.</p>  |
| Installation mode         | <p>The Security Agent installation mode</p> <p>For more information, see <a href="#">Downloading Security Agent Installation Packages on page 10-2</a>.</p>  |
| Services                  | <p>The Security Agent service</p> <p>For more information, see the <i>Apex Central Widget and Policy Management Guide</i>.</p>   |
| Apex One domain hierarchy | The location of the endpoint within the Apex One domain hierarchy  |



## Custom Tags and Filters

Use tags and filters based on your network and management requirements. Trend Micro suggests that you consider the following when using tags and filters:

- Group users based on your Active Directory organization
- Group endpoints based on their location
- Group users or endpoints with similar properties or characteristics

For example:

- Group users based on direct supervisor associations
- Group endpoints using the same operating system

**Note**

- Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
  - Apex Central automatically assigns importance to “Domain Admins” (users) and “Domain Controllers” (endpoints) after Active Directory synchronization.
    - The current version of Apex Central only supports one important “Domain Admin” and one important “Domain Controller” for each integrated Active Directory domain. Individual user accounts can no longer assign separate “important” tags for the same “Domain Admins” and “Domain Controllers”.
    - If you have preexisting “important” tags for “Domain Admins” and “Domain Controllers” created by separate user accounts on a previous version of Apex Central, the preexisting “Domain Admins” and “Domain Controllers” will be deleted and replaced with one important “Domain Admin” and one important “Domain Controller” for each integrated Active Directory domain.
-

**Tip**

- The **User Access** log query data view provides details about any user modifications related to any available custom tags or filters.

For more information, see the following topics:

- [Querying Logs on page 16-2](#)
- [User Access Information on page B-96](#)
- Generate custom reports for tagged users and endpoints by specifying the associated tags, filters, or importance labels as the report targets.

For more information, see the following topics:

- [Creating One-time Reports on page 18-21](#)
  - [Adding Scheduled Reports on page 18-26](#)
  - [Editing Scheduled Reports on page 18-31](#)
- 

## Custom Tags

Custom tags are labels that you can manually associate with one or more users/endpoints for grouping purposes.

- By default, Apex Central does not assign tags to any users or endpoints.
- You can apply multiple custom tags to multiple users/endpoints.
- Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.

## Creating a Custom Tag


---



### Note



- Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
- 

### Procedure

1. Go to **Directories > Users/Endpoints**.
2. Expand the **Custom Tags** node under **Users** or **Endpoints** in the tree.
3. Click **Add new custom tag**.
4. Type a descriptive name for the tag, and press ENTER or click  to save the new tag.

The tag appears in the list of **Users** or **Endpoints** tags.

After creating a custom tag:

- Click the  icon next to any custom tag to edit the tag name.
  - Click the  icon next to any custom tag to delete the tag.
-

---

## Assigning Custom Tags to Users/Endpoints

---

**Note**

- Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
- 

### Procedure

1. Go to **Directories > Users/Endpoints**.
2. Select the **Users** or **Endpoints** to view, or search for specific users/endpoints.
3. To associate a custom tag with a user/endpoint:
  - Click the user/endpoint row and click **Tasks > Assign/Remove Custom Tags**.
  - Right-click the user/endpoint row and click **Assign/Remove Custom Tags**.
4. In the **Assign/Remove Custom Tags** dialog, select or clear the necessary tag(s) from the list, and click **Save**.

You can verify the proper association of tags with the selected users or endpoints by selecting a tag from the **Customs Tags** list, and checking that the selected user or endpoint displays properly.

---

## Filters

Filters automatically group users or endpoints having the same criteria.

- You can group **Users** and **Endpoints** based on custom tags and filters or assign importance.

For more information, see [Creating a Custom Filter on page 7-36](#) and [User or Endpoint Importance on page 7-37](#).

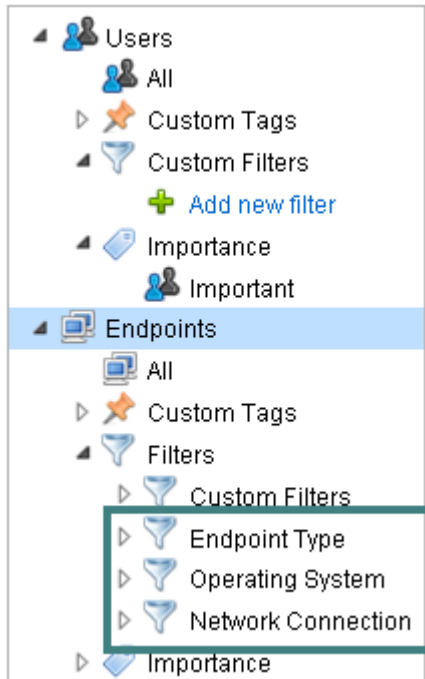
- In addition, the **Endpoints** tree can group endpoints based on default filters.

For more information, see [Default Endpoint Filters on page 7-35](#).

- Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.

## Default Endpoint Filters

By default, the **Endpoints** tree provides default filters based on the typical grouping of endpoints in an organization.



Expand one of the default filters and select the type of endpoint to display.

For details about the table columns and the data they contain, see [User Details on page 7-3](#).

The following are the default filters:

- **Endpoint Type:** Servers, desktops, laptops, mobile devices, and other types
- **Operating System:** Common operating systems installed on endpoints, including Windows, Mac OS, iOS, Android, and other operating systems

- **Network Connection:** Isolated endpoints

**Note**

After viewing the **Isolated** endpoints, you can click **Tasks > Restore Network Connection** to stop the isolation.

---

## Creating a Custom Filter

---

**Note**

- Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
- 

### Procedure

1. Go to **Directories > Users/Endpoints**.
2. Expand the **Custom Filters** node in the tree.
  - For **Users**, expand **Custom Filters**.
  - For **Endpoints**, expand **Filters**, and then expand **Custom Filters**.

3. Click **Add new filter**.

The **Search** area above the table changes to allow you to select the filter criteria.

4. Filter users or endpoints based on the available criteria.






The following example filters all users with "ja" in their name in the Finance department that report to "Mary" or "Bill" in the Active Directory domain "HR":

The screenshot shows a search filter configuration interface. It consists of several rows of criteria, each with a dropdown menu for the category, a text input for the value, and a small 'X' icon followed by a Boolean operator. The criteria are:
 

- Search: Users (dropdown), User name (input: ja), X OR
- AND: Department (dropdown), Finance (input), X OR
- AND: Direct manager (dropdown), Mary (input), X OR
- OR: Bill (input), X OR
- AND: Location in Active Directory (dropdown), HR (input), X OR AND

For more information, see [Advanced Search Categories on page 7-26](#).

After creating a custom filter:

- Click the  icon next to any custom filter to edit the filter name.
- Click the  icon next to any custom filter to update the Boolean expressions.
- Click the  icon next to any custom filter to delete the filter.

## User or Endpoint Importance

Assigning importance to groups of users and endpoints allows you to quickly monitor and respond to threats against these targets from the **Dashboard** screen. Apex Central provides several widgets that highlight threat events for “important” users and endpoints. You may want to apply stricter policies to important users or endpoints and constantly monitor their protection status.

You must first assign custom tags, or create custom filters, to identify the important users or endpoints. After identifying the important users or endpoints on your network, you can assign the “important” tag to provide greater visibility on the **Dashboard**.

For more information see [Custom Tags and Filters on page 7-29](#).

**Note**

- Manually assign importance to users/endpoints grouped using custom tags and filters.
  - Any Apex Central user account that has permission to create or modify custom tags, filters, or important labels in the **User/Endpoint Directory** can view or modify custom tags, filters, or important labels created by all other user accounts.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
  - Apex Central automatically assigns importance to “Domain Admins” (users) and “Domain Controllers” (endpoints) after Active Directory synchronization.
    - The current version of Apex Central only supports one important “Domain Admin” and one important “Domain Controller” for each integrated Active Directory domain. Individual user accounts can no longer assign separate “important” tags for the same “Domain Admins” and “Domain Controllers”.
    - If you have preexisting “important” tags for “Domain Admins” and “Domain Controllers” created by separate user accounts on a previous version of Apex Central, the preexisting “Domain Admins” and “Domain Controllers” will be deleted and replaced with one important “Domain Admin” and one important “Domain Controller” for each integrated Active Directory domain.
- 

**Procedure**

1. Go to **Directories > Users/Endpoints**.

2. Expand the **Importance** node under **Users** or **Endpoints** in the tree.
3. Click **Important** and click the edit icon (✎).
4. On the screen that displays:
  - Assign importance by selecting one or several custom tags or custom filters, and then click **Save**.
  - Remove importance by clearing one or several custom tags or custom filters, and then click **Save**.

The table in the main screen is updated with the list of endpoints or users that match the custom tags or custom filters.

For details about the table columns and the data they contain, see [User Details on page 7-3](#).

---



# Chapter 8

## Trend Vision One

**Note**

This feature is not available in all regions.

---

Trend Vision One extends detection and response beyond the endpoint to offer broader visibility and expert security analytics, leading to more detections and an earlier, faster response. With Trend Vision One, you can respond more effectively to threats, minimizing the severity and scope of a breach.

Integration with Trend Vision One allows Apex Central to forward detection events and managed Security Agent information to Trend Vision One for correlated detection and other advanced analytics.

## Integrating Apex Central with Trend Vision One

---



### Note

This feature is not available in all regions.

---

You can integrate Apex Central with Trend Vision One to forward detection logs and Security Agent information to Trend Vision One.

---



### Note

To get started with the integration, you need an active Trend Vision One account.

For more information on how to activate Trend Vision One with Essential Access using an existing product license, see [Activating Trend Vision One with Essential Access](#).

---

### Procedure

1. Generate an enrollment token in Trend Vision One. Do the following:
  - a. Go to **Trend Vision One > Access Trend Vision One**.
  - b. Log onto the Trend Vision One console.
  - c. Go to **Point Product Connection > Product Instance** or **Point Product Connection > Product Connector**.
  - d. Click **Add Existing Product** or **Connect**.
  - e. In the **Instance Type** or **Product name** field, select **Trend Micro Apex Central On-Premises**.
  - f. Click the link to generate an enrollment token.
  - g. Copy the enrollment token for use on the Apex Central web console.
  - h. Click **Save**.
2. On the Apex Central console, go to **Trend Vision One > Integration Settings**.

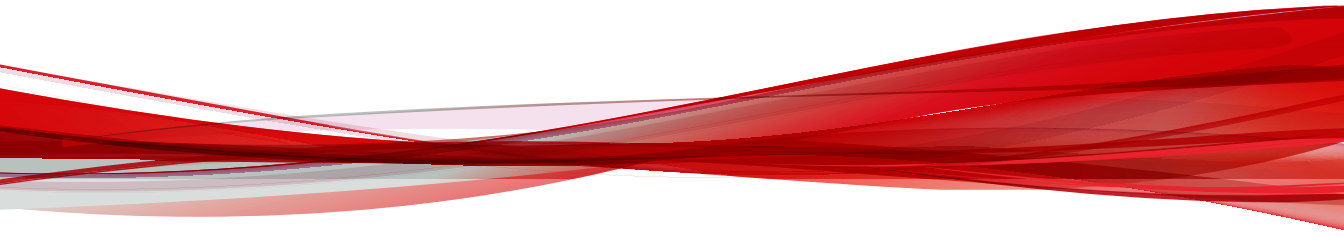
3. Paste the enrollment token you obtained from the Product Instance or Product Connector in Trend Vision One.
  4. Select **Forward detection logs and endpoint information to Trend Vision One.**
  5. Click **Register.**  
Wait until the registration process is complete.
-





# **Part III**

## **Managed Product Integration**





# Chapter 9

## Managed Product Registration

This section discusses how to register managed products and servers to the Apex Central server.

Topics include:

- *Managed Product Registration Methods on page 9-2*
- *Server Registration on page 9-2*
- *Managed Product Communication on page 9-11*

## Managed Product Registration Methods

Apex Central requires managed products to register to the Apex Central server by using one of the following methods:


- The **Server Registration** screen on the Apex Central management console
- The managed product's management console (through the Apex Central MCP agent)


## Server Registration

The **Server Registration** screen (**Administration** > **Managed Servers** > **Server Registration**) allows you to register, configure, or unregister managed products that register to Apex Central using the Apex Central management console.

For more information about products that register to Apex Central using the managed product web console, see [Connected Threat Defense Product Integration on page 20-37](#).

Use the **Server Registration** screen to perform the following tasks.

| TASK                | DESCRIPTION  |
|---------------------|--|
| Add managed servers | <p>Click <b>Add</b> to register managed products to the Apex Central server.</p> <p>For more information, see <a href="#">Adding a Managed Server on page 9-5</a>.</p> <hr/> <p> <b>Note</b><br/>If the <b>Add</b> icon is disabled, the managed product registers to Apex Central using the managed product console.</p> <hr/> |

| TASK  | DESCRIPTION  |
|---|--|
| Edit managed server settings                                | <p>Click the <b>Edit</b> icon in the <b>Actions</b> column to modify configuration settings for a managed server.</p> <p>For more information, see <a href="#">Editing a Managed Server on page 9-7</a>.</p>   |
| Delete managed servers                                      | <p>Click <b>Delete</b> icon in the <b>Actions</b> column to unregister a managed server from the Apex Central server.</p> <p>For more information, see <a href="#">Deleting a Managed Server on page 9-8</a>.</p>  |
| Configure proxy settings                                    | <p>Click <b>Proxy Settings</b> to configure proxy settings for managed products</p> <p>For more information, see <a href="#">Configuring Proxy Settings for Managed Products on page 9-9</a>.</p>  |
| Configure cloud service settings                            | <p>Click <b>Cloud Service Settings</b> to register, edit, or unregister cloud services</p> <p>For more information, see <a href="#">Configuring Cloud Service Settings on page 9-10</a>.</p>   |
| Organize managed servers in the Product Directory structure | <p>Click <b>Directory Management</b> to group or move managed products to new locations in the Product Directory structure</p> <p>For more information, see <a href="#">Managing the Product Directory on page 11-13</a>.</p>  |
| Single sign-on to managed product consoles                  | <p>Click the link in the <b>Server</b> column to single sign-on to the managed product console.</p> <hr/> <p> <b>Tip</b><br/>You can also single sign-on to managed product consoles from the <b>Product Directory</b> screen.</p> <p>For more information, see <a href="#">Product Directory on page 11-2</a>.</p> <hr/> |

**Note**

For more information about the details that display on the **Server Registration** screen, see [Managed Server Details on page 9-4](#).

## Managed Server Details

The following table describes the information that displays on the **Server Registration** screen.

| COLUMN NAME     | DESCRIPTION   |
|-----------------|---|
| Server          | <p>Displays the server name of the managed product</p> <hr/> <div data-bbox="400 630 460 680"></div> <div data-bbox="467 626 521 652"><b>Note</b></div> <p>Clicking the server name of a managed product that registers to Apex Central using an MCP agent redirects you to the managed product console.</p>  |
| Display Name    | Displays the server display name of the managed product   |
| Product         | Displays the name of the managed product  |
| Connection Type | <p>Displays how the managed product registers to Apex Central</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> The managed product registers to Apex Central through an MCP agent.<br/>For details, see <a href="#">Connected Threat Defense Product Integration on page 20-37</a>.</li> <li>• <b>Manual:</b> Administrators used the <b>Server Registration</b> screen to register the managed product.<br/>For details, see <a href="#">Adding a Managed Server on page 9-5</a>.</li> <li>• <b>Cloud Service:</b> The managed product registers through <b>Cloud Service Settings</b>.<br/>For details, see <a href="#">Configuring Cloud Service Settings on page 9-10</a>.</li> </ul> |
| Last Report     | Displays the most recent date and time when Apex Central received a response from the managed product   |

| COLUMN NAME      | DESCRIPTION   |
|------------------|---|
| Virtual Analyzer | Displays the registered Virtual Analyzer (if any) to which the managed product submits samples  |
| Actions          | <ul style="list-style-type: none"> <li>• <b>Edit:</b> Click this icon to update the server information<br/>For details, see <a href="#">Editing a Managed Server on page 9-7</a>.</li> <li>• <b>Delete:</b> Click this icon to unregister a managed server<br/>For details, see <a href="#">Deleting a Managed Server on page 9-8</a>.</li> </ul> |

## Adding a Managed Server

Use the **Server Registration** screen to register managed servers to the Apex Central server.



### Note

- If the **Add** button is disabled, then the product registers to Apex Central using the managed product management console.

For more information, see [Connected Threat Defense Product Integration on page 20-37](#).

- Before performing policy management on a newly added managed server, click **Directory Management** and move the managed product from the **New Entity** folder to another location.

For more information, see [Managing the Product Directory on page 11-13](#).

## Procedure

1. Go to **Administration > Managed Servers > Server Registration**.

The **Server Registration** screen appears.

2. Select a product from the **Server Type** drop-down list.

A list of registered managed servers appears.

3. Click the **Add** button or the **Add a product** link in the table.

The **Add Server** screen appears.

4. Specify the following server information:

- **Server:** Type the <managed product> server name, FQDN, or IPv4/IPv6 address and port number (if any).

**Important**

The server address should start with either **HTTP** or **HTTPS**.

---

- **Display name:** Specify the name of the <managed product> server that displays in Apex Central.
5. If logging on to the managed server requires authentication, specify the following credentials:
    - **User name:** Provide the name of a <managed product> account with administrator privileges.
    - **Password:** Type the password for the provided account.

**Important**

Apex Central requires an account with administrator privileges to deploy policy settings.

---

6. (Optional) To use a proxy server, select the **Use a proxy server for the connection** check box.

For more information, see [Configuring Proxy Settings for Managed Products on page 9-9](#).

7. To enable sample submission, select the Virtual Analyzer product/service from the **Virtual Analyzer** drop-down list.



**Important**

- For Deep Security and Trend Micro Endpoint Sensor, you must add the managed server first and then edit the server to select the Virtual Analyzer.
  - For all other managed products, you can select the Virtual Analyzer when you add the managed server for the first time.
  - For more information, see [Connected Threat Defense Product Integration on page 20-37](#).
- 

**8. Click Save.**

The newly added server appears in the list of registered managed servers.

---

## Editing a Managed Server

Use the **Server Registration** screen to edit information for managed servers registered to the Apex Central server.

---

### Procedure

**1. Go to Administration > Managed Servers > Server Registration.**

The **Server Registration** screen appears.

**2. Select a product from the Server Type drop-down list.**

A list of registered managed servers appears.

**3. Click the Edit icon in the Actions column for the managed server you want to edit.**

The **Edit Server** screen appears.

**4. Edit the server information.**

- **Authentication:** Provide the user name and password if the server requires authentication to log on.

- **Connection:** Select the **Use a proxy server for the connection** check box to use the configured proxy server.

For more information, see [Configuring Proxy Settings for Managed Products on page 9-9](#).

- **Sample Submission:** Select the Virtual Analyzer product/service from the **Virtual Analyzer** drop-down list.



### Important

- If the **Virtual Analyzer** drop-down list displays **Not supported**, then the Virtual Analyzer product/service must be configured from the managed product server console (for example, the Deep Discovery Inspector console) instead of Apex Central.
- Apex One servers managed by a Node Apex Central can select the Deep Discovery Analyzer registered to a Hub Apex Central as the Virtual Analyzer product/service.

---

For more information, see [Connected Threat Defense Product Integration on page 20-37](#).

5. Click **Save**.
- 

## Deleting a Managed Server

Use the **Server Registration** screen to unregister a managed server from Apex Central.

---

### Procedure

1. Go to **Administration > Managed Servers > Server Registration**.

The **Server Registration** screen appears.

2. Click **Directory Management**.
3. Expand the product tree and select the server you want to delete.

4. Click **Delete**.

A confirmation screen appears.

5. Click **OK**.

The selected server is deleted from the product tree.

**Note**

Deleting a managed server on the **Server Registration** screen does not uninstall the server program or related agents.

6. On the management console of the server, go to the product registration screen and unregister the server from Apex Central.

7. Click **OK**.

---

## Configuring Proxy Settings for Managed Products

Apex Central allows you to use a proxy server to connect to managed products on an internal network. After configuring proxy server settings for a managed product, enable the proxy server connection for specific managed servers.

For more information, see [Editing a Managed Server on page 9-7](#).

**Important**

You can only use one proxy server for all managed servers of the same managed product type.

---

### Procedure

1. Go to **Administration > Managed Servers > Server Registration**.

The **Server Registration** screen appears.

2. Select a product from the **Server Type** drop-down list.

A list of registered managed servers appears.

3. Click **Proxy Settings**.

The **Proxy Settings** screen appears.

4. Select one of the following protocols:

- **HTTP**
- **SOCKS 4**
- **SOCKS 5**

5. Specify the following fields:

- **Server:** Type the server name, FQDN, or IPv4 address of the proxy server
- **Port:** Type the port number that the proxy server uses for client connections

6. If the proxy server requires authentication, specify the following credentials:

- **User name**
- **Password**

7. Click **Save**.

8. To enable the proxy server connection:

- a. Click the **Edit** icon in the **Actions** column for the managed server you want to edit.

The **Edit Server** screen appears.

- b. Select the **Use a proxy server for the connection** check box in the **Connection** section.

- c. Click **Save**.
- 

## Configuring Cloud Service Settings

Use the **Server Registration** screen to register or unregister a managed cloud service from Apex Central.

---

## Procedure

1. Go to **Administration > Managed Servers > Server Registration**.

The **Server Registration** screen appears.

2. Click **Cloud Service Settings**.

The **Cloud Service Settings** screen appears.

3. To register a cloud service, provide the following credentials:

- **Account:** Type the user name you used to activate the cloud service subscription on the Trend Micro Customer Licensing Portal (<https://clp.trendmicro.com/>).
- **Password:** Type the password for the cloud service account.

4. To unregister a cloud service, click **Stop managing services with Apex Central** and agree to all succeeding prompts.

5. Click **OK**.
- 

## Managed Product Communication

Apex Central uses Management Communication Protocol (MCP) agents installed on managed servers to communicate with managed products that do not register to the Apex Central server through the Apex Central management console.

An MCP agent communicates with the Apex Central server by sending a heartbeat at a regular interval to indicate that the managed product is operating normally.

Administrators can configure the Agent Communication Schedule to determine when agents send heartbeats to the Apex Central server.

**Important**

Apex Central only allows you to configure the Agent Communication Schedule for managed products that register to the Apex Central server through the Apex Central management console.

## Modifying the Default Agent Communication Schedule

Apex Central uses the default agent communication schedule to communicate with all managed products that do not have a customized agent communication schedule.

Use the **Set Communicator Schedule** screen to modify the default schedule by clicking a time slot to change the communication status.

### Procedure

1. Go to **Administration > Managed Servers > Agent Communication Schedule**.

The **Agent Communication Schedule** screen appears.

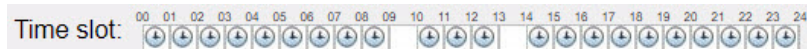
2. In the **Communicator** column, click **Default Schedule**.

The **Set Communicator Schedule** appears.

3. Click a time slot to change the agent communication status.

- Setting a time slot to **Idle** creates consecutive time periods during which the agent sends heartbeats to the Apex Central server.

For example, setting time slots 09 and 13 to **Idle** creates two periods of consecutive time slots.



- You can specify up to three consecutive time periods of **Scheduled** time slots during which the agent sends a heartbeat to the Apex Central server.

4. Click **Save**.

---

## Configuring Agent Communication Schedules

Customize the Agent Communication Schedule for a managed product by clicking a time slot on the **Set Communicator Schedule** screen to change the communication status.



### Important

You can only configure one Agent Communication Schedule per managed product.

---

### Procedure

1. Go to **Administration > Managed Servers > Agent Communication Schedule**.

The **Agent Communication Schedule** screen appears.

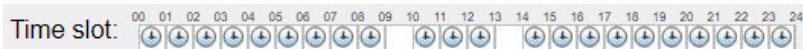
2. In the **Communicator** column, click the managed product to modify.

The **Set Communicator Schedule** screen appears.

3. Click a time slot to change the communication status.

- Setting a time slot to **Idle** creates consecutive time periods during which the agent sends heartbeats to the Apex Central server.

For example, setting time slots 09 and 13 to **Idle** creates two periods of consecutive time slots.



- You can specify up to three consecutive time periods of **Scheduled** time slots during which the agent sends a heartbeat to the Apex Central server.

4. Click **Save**.

## Configuring Managed Product Heartbeat Intervals

The **Managed Product Heartbeat Interval** settings determine how frequently the agent sends a heartbeat to the Apex Central server.

Use the **Communication Time-out Settings** screen to define the managed product heartbeat interval in minutes.

When configuring the managed product heartbeat interval, consider the following:

- The **Managed Product Heartbeat Interval** settings only apply to managed products that register to the Apex Central server using the Apex Central management console.
- Long heartbeat intervals consume less bandwidth but allow more network events to occur before Apex Central updates the communication status.
- Short intervals between heartbeats consume more bandwidth but present a more up-to-date picture of your network status.

---

### Procedure

1. Go to **Administration > Managed Servers > Communication Time-out Settings**.

The **Communication Time-out Settings** screen appears.

2. In the **Managed Product Heartbeat Interval** section, configure the following settings:

- **Report managed product status every:** Defines the agent communication heartbeat interval

Valid values are between 5 and 480 minutes.

- **If no communication, set status as abnormal after:** Defines the agent communication time-out interval

Valid values are between 15 and 1440 minutes.





**Important**

The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

---

3. Click **Save**.
-



# Chapter 10

## Security Agent Installation

This chapter describes Security Agent installation requirements and methods.

Topics include:

- *[Downloading Security Agent Installation Packages on page 10-2](#)*
- *[Apex One Security Agent System Requirements on page 10-4](#)*
- *[Apex One \(Mac\) Security Agent Installation on page 10-26](#)*

## Downloading Security Agent Installation Packages

Use the **Security Agent Download** screen to create and download Security Agent installation packages for Apex One or Apex One (Mac). You can download and install the Security Agent installation package or get a URL that you can send to users to download the Security Agent installation package directly onto a target endpoint.

**TABLE 10-1. Pre-installation Configuration**

| SECURITY AGENT | CONFIGURATION  |
|----------------|--|
| Apex One       | Before installing Apex One Security Agents: <ul style="list-style-type: none"> <li>• Change the default Apex One Security Agent unloading and uninstallation passwords</li> <li>• Ensure that endpoints can communicate through ports 80 and 443</li> <li>• Ensure that endpoints can access *.trendmicro.com</li> <li>• If required, configure Apex One Security Agent proxy server settings</li> </ul> |
| Apex One (Mac) | Before installing Apex One (Mac) Security Agents: <ul style="list-style-type: none"> <li>• Ensure that endpoints can communicate through port 61617 or 8443 (SaaS)</li> <li>• Ensure that endpoints can access *.trendmicro.com</li> <li>• If required, configure Apex One Security Agent proxy server settings</li> </ul>   |

For more information about system requirements for installing Security Agents on endpoints, see the following topics:

- [Apex One Security Agent System Requirements on page 10-4](#)
- [Apex One \(Mac\) Security Agent System Requirements on page 10-26](#)

---

### Procedure

1. Go to **Administration > Security Agent Download**.

2. Select the operating system.
  - **Windows 64-bit:** Select to create a 64-bit MSI installation package for Apex One Security Agents
  - **Windows 32-bit:** Select to create a 32-bit MSI installation package for Apex One Security Agents
  - **Mac:** Select to create a ZIP installation package for Apex One (Mac) Security Agents
3. For **Windows 64-bit** or **Windows 32-bit** Apex One Security Agents, select the **Installation mode**:
  - **Full feature set:** Installs the standard Apex One Security Agent with full feature capabilities
  - **Coexist:** The coexist mode Apex One Security Agent provides a limited subset of Apex One capabilities but is compatible with any supported Windows endpoint, running any endpoint security software.

**Tip**

Select **Coexist** mode to allow target endpoints to use third-party security software.

---

4. If you have more than one corresponding managed product server for the type of installation package selected, use the **Server** drop-down to select the server to which the Security Agent reports.

**Note**

If you only have one managed product server, only the managed product server name displays.

---

5. Click one of the following deployment options:
  - **Download:** Downloads a copy of the Security Agent installation package that you can install locally or later deploy to target endpoints

- **Get Download Link:** Displays a URL that you can send to users to install the Security Agent directly onto a target endpoint

**Note**

For Apex One servers, the Apex One Security Agent package applies the settings generated the last time the Security Agent Packaging Tool ran.


For more information, see the *Apex One Administrator's Guide*


## Apex One Security Agent System Requirements

This section outlines the Apex One Security Agent system requirements for fresh installations on supported Windows platforms.

### Windows Endpoint Platforms



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

| ITEM   | REQUIREMENT   |
|--|---|
| Editions<br><hr/>  <b>Important</b><br>Service Pack 1 is required. | <ul style="list-style-type: none"> <li>• Home Basic</li> <li>• Home Premium</li> <li>• Ultimate</li> <li>• Professional</li> <li>• Enterprise</li> <li>• Professional for Embedded Systems</li> <li>• Ultimate for Embedded Systems</li> <li>• Thin PC</li> </ul> |
| Processor  | <ul style="list-style-type: none"> <li>• Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul>   |

| ITEM                 | REQUIREMENT  |
|----------------------|--|
| RAM                  | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> Apex One with Endpoint Sensor: <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul>   |
| Available Disk Space | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/> <div style="display: flex; align-items: flex-start;">  <div> <p><b>Note</b></p> <p>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> </div> </div> <hr/> |
| Others               | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Simple File Sharing disabled</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul>   |

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



| ITEM                                | REQUIREMENT   |
|-------------------------------------|---|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Pro</li> <li>• Enterprise</li> </ul>   |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul> |

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

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

| ITEM                                | REQUIREMENT  |
|-------------------------------------|--|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Home</li> <li>• Pro</li> <li>• Pro for Workstations</li> <li>• Education</li> <li>• Enterprise</li> </ul> |



| ITEM                 | REQUIREMENT   |
|----------------------|---|
| Update support       | <ul style="list-style-type: none"> <li>Windows 10 November 2021 Update (Windows 10 21H2) and earlier</li> </ul>   |
| Processor            | <ul style="list-style-type: none"> <li>Minimum 1GHz (32-bit) / 2GHz (64-bit) Intel Pentium or equivalent (2GHz recommended)</li> <li>AMD™ 64 processor</li> <li>Intel 64 processor</li> </ul>   |
| RAM                  | <ul style="list-style-type: none"> <li>2GB minimum (exclusively for Apex One)</li> </ul> <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> <li>2GB minimum (exclusively for Apex One)</li> </ul>   |
| Available Disk Space | <ul style="list-style-type: none"> <li>1.5GB minimum</li> <li>2.0GB recommended</li> </ul> <hr/> <p> <b>Note</b><br/>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> <hr/> |
| Others               | <ul style="list-style-type: none"> <li>Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>Enable default local admin</li> </ul> <hr/> <p> <b>Note</b><br/>Windows UI is not supported.</p> <hr/>                        |

## Windows Server Platforms

## Windows Server 2008 R2 (64-bit) Platforms

- [Windows Server 2008 R2 on page 10-8](#)
- [Windows Storage Server 2008 R2 on page 10-9](#)
- [Windows HPC Server 2008 R2 on page 10-10](#)




### Note

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


**TABLE 10-2. Windows Server 2008 R2**

| ITEM                      | REQUIREMENT   |
|---------------------------|---|
| Editions (Service Pack 1) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Enterprise</li> <li>• Datacenter</li> <li>• Web</li> <li>• Server Core</li> </ul>  |
| Processor                 | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul>  |
| RAM                       | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> |

| ITEM                 | REQUIREMENT  |
|----------------------|--|
| Available Disk Space | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/> <div style="display: flex; align-items: flex-start;">  <div> <p><b>Note</b></p> <p>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> </div> </div> <hr/> |
| Others               | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul>   |


**TABLE 10-3. Windows Storage Server 2008 R2**

| ITEM                      | REQUIREMENT   |
|---------------------------|---|
| Editions (Service Pack 1) | <ul style="list-style-type: none"> <li>• Basic</li> <li>• Standard</li> <li>• Enterprise</li> <li>• Workgroup</li> </ul>  |
| Processor                 | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul>  |
| RAM                       | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> |

| ITEM                 | REQUIREMENT  |
|----------------------|--|
| Available Disk Space | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/> <div style="display: flex; align-items: flex-start;">  <div> <p><b>Note</b></p> <p>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> </div> </div> <hr/> |
| Others               | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul>   |

**TABLE 10-4. Windows HPC Server 2008 R2**

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

| ITEM                 | REQUIREMENT   |
|----------------------|---|
| Available Disk Space | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/>  <b>Note</b><br>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. |
| Others               | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul>  |


## Windows MultiPoint Server 2010 (64-bit) Platform



### Note

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

| ITEM                                | REQUIREMENT  |
|-------------------------------------|--|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• N/A</li> </ul>  |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul> |

| ITEM                 | REQUIREMENT   |
|----------------------|---|
| RAM                  | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> Apex One with Endpoint Sensor: <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul>  |
| Available Disk Space | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/>  <b>Note</b><br>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB. |
| Others               | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul>  |


## Windows MultiPoint Server 2011 (64-bit) Platform



### Note

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

| ITEM                                | REQUIREMENT   |
|-------------------------------------|---|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Premium</li> </ul> |

| ITEM                 | REQUIREMENT   |
|----------------------|---|
| Processor            | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul>  |
| RAM                  | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul>   |
| Available Disk Space | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/> <p> <b>Note</b><br/>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> |
| Others               | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul>  |

## Windows Server 2012 (64-bit) Platforms

- [Windows Server 2012 on page 10-14](#)
- [Windows Server 2012 R2 on page 10-15](#)
- [Windows Storage Server 2012 on page 10-16](#)
- [Windows Storage Server 2012 R2 on page 10-17](#)
- [Windows MultiPoint Server 2012 on page 10-18](#)
- [Windows Server 2012 Failover Clusters on page 10-19](#)

- [Windows Server 2012 R2 Failover Clusters on page 10-20](#)


**Note**

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


**TABLE 10-5. Windows Server 2012**


| ITEM                                | REQUIREMENT  |
|-------------------------------------|--|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Datacenter</li> <li>• Server Core</li> </ul>  |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul>   |
| RAM                                 | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> <p>Apex One with Endpoint Sensor:</p> <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul>  |
| Available Disk Space                | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <hr/> <div data-bbox="431 1068 491 1117" data-label="Image"> </div> <div data-bbox="502 1068 556 1091" data-label="Section-Header"><b>Note</b></div> <div data-bbox="502 1104 1094 1230" data-label="Text"> <p>If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.</p> </div> |




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


**TABLE 10-6. Windows Server 2012 R2**

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


| ITEM   | REQUIREMENT  |
|--------|--|
| Others | <ul style="list-style-type: none"> <li>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</li> <li>• Allow printer/file sharing in the Windows firewall (if enabled)</li> <li>• Enable default local admin</li> </ul> |
|        | <div style="border: 1px solid black; padding: 5px;">  <b>Note</b><br/>           Windows UI is not supported.         </div>                            |


**TABLE 10-7. Windows Storage Server 2012**

| ITEM                                | REQUIREMENT   |
|-------------------------------------|---|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Workgroup</li> </ul>   |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul>  |
| RAM                                 | <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul> Apex One with Endpoint Sensor: <ul style="list-style-type: none"> <li>• 2GB minimum (exclusively for Apex One)</li> </ul>  |
| Available Disk Space                | <ul style="list-style-type: none"> <li>• 1.5GB minimum</li> <li>• 2.0GB recommended</li> </ul> <div style="border: 1px solid black; padding: 5px;">  <b>Note</b><br/>           If you activate Application Control, Endpoint Sensor, Vulnerability Protection, and Data Protection on the Security Agent, Trend Micro recommends increasing the minimum disk space to 3.0GB.         </div> |


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


**TABLE 10-8. Windows Storage Server 2012 R2**

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


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


**TABLE 10-9. Windows MultiPoint Server 2012**

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


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


**TABLE 10-10. Windows Server 2012 Failover Clusters**

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

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

**TABLE 10-11. Windows Server 2012 R2 Failover Clusters**

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

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

## Windows Server 2016 (64-bit) Platforms

- [Windows Server 2016 on page 10-21](#)
- [Windows Server 2016 Failover Clusters on page 10-22](#)
- [Windows Storage Server 2016 on page 10-23](#)





### Note

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

**TABLE 10-12. Windows Server 2016**



| ITEM                                | REQUIREMENT  |
|-------------------------------------|--|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Datacenter</li> <li>• Server Core</li> </ul>  |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul> |

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

**TABLE 10-13. Windows Server 2016 Failover Clusters**



| ITEM                                | REQUIREMENT  |
|-------------------------------------|--|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• N/A</li> </ul>  |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul> |



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

**TABLE 10-14. Windows Storage Server 2016**

| ITEM                                | REQUIREMENT  |
|-------------------------------------|--|
| Editions (no Service Pack required) | <ul style="list-style-type: none"> <li>• Standard</li> <li>• Workgroup</li> </ul>  |
| Processor                           | <ul style="list-style-type: none"> <li>• Minimum 1.4GHz Intel Pentium or equivalent (2GHz recommended)</li> <li>• AMD™ 64 processor</li> <li>• Intel 64 processor</li> </ul> |

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



## Windows Server 2019 (64-bit) Platforms



### Note

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

**TABLE 10-15. Windows Server 2019**

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

## Apex One (Mac) Security Agent Installation

This section describes Apex One (Mac) Security Agent installation requirements and methods.

For more information, refer to the Apex One (Mac) documentation.

### Apex One (Mac) Security Agent System Requirements

The following are the requirements for installing the Security Agent on a Mac endpoint.

**TABLE 10-16. Security Agent installation requirements**

| RESOURCE                   | REQUIREMENT  |
|----------------------------|--|
| Operating system           | <ul style="list-style-type: none"> <li>• macOS™ Catalina 10.15</li> <li>• macOS™ Mojave 10.14</li> <li>• macOS™ High Sierra 10.13</li> <li>• macOS™ Sierra 10.12</li> <li>• OS X™ El Capitan 10.11</li> </ul>  |
| Hardware                   | <ul style="list-style-type: none"> <li>• <b>Processor:</b> Apple® M1, Apple® M2, or Intel® Core™ processor</li> <li>• <b>RAM:</b> 2GB minimum</li> <li>• <b>Available disk space:</b> 512MB minimum</li> </ul> |
| Server-agent communication | <ul style="list-style-type: none"> <li>• 8443 (SaaS)</li> <li>• 61617</li> </ul>   |
| Others                     | <ul style="list-style-type: none"> <li>• Access to *.trendmicro.com</li> <li>• If required, proxy server settings for Internet connection</li> </ul>   |

# Chapter 11

## Product Directory

This section discusses how to view information about all the managed products registered to the Apex Central server and the tasks available on the **Product Directory** screen.

Topics include:

- *Product Directory on page 11-2*
- *Viewing Managed Product Status Summaries on page 11-5*
- *Performing an Advanced Search of the Product Directory on page 11-6*
- *Executing Managed Product Tasks on page 11-8*
- *Configuring Managed Product Settings on page 11-9*
- *Querying Logs from the Product Directory on page 11-10*
- *Directory Management on page 11-11*

## Product Directory

The **Product Directory** screen displays information about all the managed product servers registered to the Apex Central server. You can use this screen to search for specific managed product entities, view managed server status summaries, execute managed product tasks, configure managed product settings, or query managed product logs.



### Tip

You can also use the **Log Query** screen to query managed product logs.

For more information, see [Querying Logs on page 16-2](#).

---

The Product Directory tree organizes managed products into the following default folders:

- **<Root>**: Displays the name of the Apex Central server and contains all the following subfolders
- **Local Folder**: Contains the **New Entity** folder and any custom folders you create
- **New Entity**: Contains all managed products newly registered to the Apex Central server
- **Search Result**: Contains all managed products that match the criteria for a basic or advanced search



### Note

Except for the **New Entity** folder, Apex Central lists all folders in ascending order, starting from special characters (!, #, \$, %, (, ), \*, +, -, comma, period, +, ?, @, [, ], ^, ~, {, |, }, and ~), numbers (0 to 9), or alphabetic characters (a/A to z/Z).


---

The **Product Directory** screen uses icons to represent managed products and the connection status of managed products.

For more information about the Product Directory connection status icons, see the [Connection Status Icons on page 11-4](#).





The following table outlines the tasks available on the **Product Directory** screen.

| TASK                                     | DESCRIPTION   |
|--|---|
| View status summaries                    | <p>Select a managed product entity in the Product Directory to view the status summary.</p> <p>For more information, see <a href="#">Viewing Managed Product Status Summaries on page 11-5</a>.</p>   |
| Find managed product entities            | <p>In the <b>Find entity</b> search box, search for managed product entities using partial string matching and click <b>Search</b>. Managed product entities that match the search criteria appear in the <b>Search Result</b> folder.</p> <p>For more information about performing an advanced search, see <a href="#">Executing Managed Product Tasks on page 11-8</a>.</p> |
| Configure managed product settings       | <p>Select a managed product entity in the Product Directory tree and select an option from the <b>Configure</b> drop-down.</p> <p>For more information, see <a href="#">Configuring Managed Product Settings on page 11-9</a>.</p>  |
| Execute managed product tasks            | <p>Select a managed product entity in the Product Directory tree and select an option from the <b>Tasks</b> drop-down.</p> <p>For more information, see <a href="#">Executing Managed Product Tasks on page 11-8</a>.</p>   |
| Query managed product logs               | <p>Select a managed product entity in the Product Directory and click <b>Logs</b>.</p> <p>For more information, see <a href="#">Querying Logs from the Product Directory on page 11-10</a>.</p>   |
| Organize the Product Directory structure | <p>Click <b>Directory Management</b> to create new folders or move or group managed product entities in the Product Directory tree.</p> <p>For more information, see <a href="#">Directory Management on page 11-11</a>.</p>  |



| TASK                                       | DESCRIPTION   |
|--|---|
| Single sign-on to managed product consoles | <p>Select the managed product server icon in the corresponding folder in the Product Directory tree and click <b>Configure &gt; &lt;Managed_Product&gt; Single Sign On.</b></p> <hr/> <p> <b>Tip</b><br/>You can also single sign-on to managed product consoles from the <b>Server Registration</b> screen.</p> <p>For more information, see <a href="#">Server Registration on page 9-2.</a></p> |

## Connection Status Icons

The Product Directory uses the following icons to indicate the status of communication between the Apex Central server and registered managed products.

| ICON  | MCP AGENT STATUS  | PRODUCT SERVICE STATUS |
|---|---|------------------------|
|  | Running   | Running                |
|  | Running   | Not running            |
|  | <p>Communication timed out</p> <hr/> <p> <b>Note</b><br/>The Apex Central server was unable to establish communication with the MCP agent on the managed product server within the heartbeat interval configured on the <b>Communication Time-out Settings</b> screen.</p> | Unknown                |



| ICON  | MCP AGENT STATUS  | PRODUCT SERVICE STATUS                         |
|---|---|--|
|  | <p data-bbox="478 256 592 277">Not running</p> <hr/> <p data-bbox="478 331 538 375"> <b>Note</b></p> <p data-bbox="552 367 821 688">The Apex Central server was unable to establish communication with the MCP agent on the managed product server after multiple unsuccessful attempts according to the criteria configured on the <b>Communication Time-out Settings</b> screen.</p> | <p data-bbox="845 256 959 277">Not running</p> |

## Viewing Managed Product Status Summaries

Apex Central allows you to use the **Product Directory** screen to view status summaries for managed products and folders.



### Tip

You can also view managed product status summaries by using the **Threat Detection Results** widgets on the **Dashboard**.

### Procedure

1. Go to **Directories > Products**.  
The **Product Directory** screen appears.
2. Select the following items in the Product Directory tree to display status summaries in the working area.

| ITEM                                 | DESCRIPTION  |
|--------------------------------------|--|
| Managed product                      | Select to view System Information and Product License Information  |
| Managed product folder               | Select to view Antivirus, Spyware/Grayware, Content Security, Web Security, Network Virus, Violation Status, and Component Status summaries                  |
| Managed product server               | Select a managed product server in the Product Directory tree and click <b>Folder &gt; Product View</b> to display all domains on the managed product server |
| Domain in the Product Directory tree | Select to display all clients that belong to this domain on the managed product server   |

**Note**

By default, Apex Central displays a seven days of information ending with the day of your query.

You can change the summary period by selecting **Today**, **Last 7 days**, **Last 14 days**, or **Last 30 days** from the **Period** drop-down list.

## Performing an Advanced Search of the Product Directory

Apex Central allows you to search the Product Directory for managed product entity names, domains, and endpoints using partial string matching. You can also perform advanced searches on folder objects to locate specific objects using Boolean operators.

**Note**

After performing a search, any matches appear in a new folder under the **Search Result** node of the Product Directory tree.

---

## Procedure

1. Go to **Directories > Products**.

The **Product Directory** screen appears.

2. Select a folder in the Product Directory tree to search.



### Important

The advanced search feature only searches within the selected folder and all subfolders. You cannot perform a search within the **Search Result** folder.

---

3. Click **Advanced Search**.

The **Advanced Search** screen appears.

4. In the **Match** drop-down, select from the following:

- **All of the criteria**
- **Any of the criteria**

5. Specify your filtering criteria.



### Note

- The available criteria, operators, and values change depending on the products registered to Apex Central and the previous filtering selections.
  - Apex Central supports up to 20 filtering criteria for searches.
- 

6. To add or remove search conditions, click the buttons to the right of the search criteria.

7. Click **Search**.

Managed products that match the search criteria appear in the **Search Result** folder in the Product Directory tree.

---

## Executing Managed Product Tasks

Use the **Tasks** drop-down menu to issue tasks to a specific managed product or a group of managed products.

The types of commands that display change depending on the managed products selected. Some common tasks include:

- Deploying components
- Sending scan commands
- Synchronizing agents



### Tip

Download the latest components from the Trend Micro ActiveUpdate server to the Apex Central server before deploying updates to a specific managed product or a group of managed products.

For more information, see [Configuring Manual Update Settings on page 12-8](#).

---

### Procedure

1. Go to **Directories > Products**.

The **Product Directory** screen appears.

2. Select a managed product or folder from the Product Directory tree.



### Note

If you select a folder, Apex Central attempts to send the selected command to all applicable managed products contained within the selected folder.

---

3. From the **Tasks** drop-down menu, select a task to perform.
4. To send the command to managed products, do the following:
  - For deployment commands: Click **Deploy now**.

- For scan commands:
    - a. Select a scan command.
    - b. Select the managed products.
    - c. Click **Send Request**.
  - 5. Click **Command Details** to monitor the task progress or click **OK** to proceed with other tasks.
- 

## Configuring Managed Product Settings

Apex Central allows you to configure a managed product by signing in to the managed product's web console or by replicating configuration settings to target machines through the Apex Central web console.

---



### Note

For additional information about configuring managed products, refer to the managed product's documentation.

---

### Procedure

1. Go to **Directories > Products**.  
The **Product Directory** screen appears.
2. Select a managed product from the Product Directory tree.
3. From the **Configure** drop-down, select one of the following:



### Note

Options on the **Configure** drop-down menu change depending on the managed product selected.

---

- **Configuration Replication:** Replicates configuration settings from the selected managed product to target machines

- **Replicate configuration to entire folder:** Replicates configuration settings to all other managed products in the same folder as the selected managed product
  - **<Managed Product> Single Sign On:** Logs you on to the managed product web console using your Apex Central credentials
  - **Configure <Managed Product>:** Logs you on to the managed product's web console
    - If prompted, type your user name and password to sign in to the managed product's web console.
    - If prompted, click **Yes** to proceed to the managed product's web console.
- 

## Querying Logs from the Product Directory

Apex Central allows you to perform a log query from the **Product Directory** screen by selecting a managed product or folder from the Product Directory tree as the source of information.

---



### Note

When querying logs from the Product Directory, Apex Central preselects the product scope based on the managed product server or folder you select on the **Product Directory** screen.

---

For more information about performing log queries from the **Log Query** screen, see [Querying Logs on page 16-2](#).

---

### Procedure

1. Go to **Directories > Products**.

The **Product Directory** screen appears.

2. Select a managed product or folder from the Product Directory tree.

**Note**

The selected managed product or folder determines the product scope of the log query.

---

3. Click the **Logs** button.

The **Log Query** screen appears.

4. Select a log type and click **OK**.
  5. Select a time period or specify a custom range of dates.
  6. To specify custom filtering criteria:
    - a. Click **Show advanced filters**.
    - b. Select **All of the criteria** or **Any of the criteria** as the criteria matching rule.
    - c. Select a filtering option from the **Select criteria...** drop-down.
    - d. Select an operator and specify the criteria.
- 

**Note**

Apex Central supports up to 20 custom filtering criteria for each log query.

---

7. Click **Search**.
- 

## Directory Management

The **Directory Management** screen allows you to customize the Product Directory structure to suit your administrative needs. To access the **Directory Management** screen, click the **Directory Management** button on the **Product Directories** screen (**Directories > Products**).

Group managed products according to geographical, administrative, or product-specific purposes. In combination with different access rights used to access managed products or folders in the directory, the following table

presents the recommended grouping types as well as their advantages and disadvantages.

**TABLE 11-1. Product Grouping Comparison**

| GROUPING TYPE                  | ADVANTAGES                                      | DISADVANTAGES                                 |
|--------------------------------|---|---|
| Geographical or Administrative | Clear structure                                 | No group configuration for identical products |
| Product type                   | Group configuration and status is available     | Access rights may not match                   |
| Combination of both            | Group configuration and access right management | Complex structure, may not be easy to manage  |

Plan this structure carefully, because the structure also affects the following:

**TABLE 11-2. Considerations for the Structure**

| CONSIDERATION       | EFFECT   |
|---------------------|--|
| User access         | When creating user accounts, Apex Central prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire directory. Granting access to a specific managed product only grants access to that specific product.                            |
| Deployment planning | Apex Central deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients. |

For more information, see [Managing the Product Directory on page 11-13](#).



**Important**

User accounts have specific access permissions assigned based on Product Directory folders.

- Changing the Product Directory structure may affect how Apex Central users can access the managed products.
- You can select the **Keep the current user access permissions when moving managed products/folders** check box to prevent changing the user access scope when changing the Product Directory structure.

For more information, see [User Accounts on page 4-2](#).

---

## Managing the Product Directory

Use the **Directory Management** screen to organize your Product Directory structure.

For more information, see [Directory Management on page 11-11](#).

---

**Important**

- Apex Central prevents multiple users from unknowingly making changes at the same time through use of a function-locking mechanism. Apex Central informs you if another user is already using the **Directory Management** screen. If you still want to make changes to the Product Directory and possibly affect the other user's changes, click **Break** to immediately access the screen.
- Changing the Product Directory structure may affect how Apex Central users can access the managed products. User accounts have specific access permissions assigned based on Product Directory folders.

For more information, see [User Accounts on page 4-2](#).

---

---

## Procedure

1. Go to **Directories > Products**.

The **Product Directory** screen appears.

2. Click the **Directory Management** button.

The **Directory Management** screen appears.

3. Enable the **Keep the current user access permissions when moving managed products/folders** check box if you want to maintain the current user access permissions for all managed products.



### Note

If you disable this option and move a managed product to a new location, the managed product inherits the permissions of the new folder location.

---

4. To organize the Product Directory, you can perform the following tasks:
  - **Add Folder:** Creates a new custom folder in the **Local Folder** node
  - **Rename:** Renames an existing custom folder
  - **Delete:** Deletes an existing custom folder



### Note

Apex Central cannot delete a custom folder that contains a registered managed product.

---

- **Move managed products or folders:** Drag and drop a managed product or folder to a new location



### Important

You cannot rename, delete, or add new products or folders to the “root”, **Cascading Folder**, or **New Entity** folders.

---

5. Click **Back** to apply changes and return to the **Product Directory** screen.
-

---

## Recovering Managed Products

---

**WARNING!**

The following actions may delete managed products from the Product Directory:

- Reinstalling the Apex Central server and selecting **Delete existing records and create a new database**
  - Replacing a corrupted Apex Central database with another database with the same name
- 

Use one of the following three methods to recover managed products that were accidentally deleted from the Product Directory.

---

**Procedure**

- Manually restart the Apex Central MCP agent service on the managed product server.
  - Wait for the MCP agent to automatically re-register to the Apex Central server after 8 hours.
  - Manually re-register the MCP agent to the Apex Central server from the managed product console.
-



# Chapter 12

## Component Updates

This section discusses how to configure component updates in Apex Central.

Topics include:

- *Component Updates on page 12-2*
- *Configuring Scheduled Update Settings on page 12-4*
- *Configuring Manual Update Settings on page 12-8*
- *Configuring Proxy Settings for Component/License Updates, Cloud Services, and Syslog Forwarding on page 12-12*

## Component Updates

The Apex Central server hosts component files that the managed products use to keep your network protected from the latest security threats.

Keep the components up-to-date by running manual or scheduled updates. Apex Central allows you to perform the following tasks:

- Download the latest component versions from an update source
- Deploy updated components to managed products

## Component List

You can view the list of available components on the Apex Central server on the **Scheduled Update** and **Manual Update** screens.

The following table describes the component information that displays on the **Scheduled Update** and **Manual Update** screens.

| FIELD               | DESCRIPTION  |
|---------------------|--|
| Category            | Displays the name of a component category<br>Click ▶ to display the list of components in a category.  |
| Type                | Displays the component type  |
| Current Version     | Displays the last version of the component successfully downloaded by Apex Central   |
| Last Download       | Displays the time Apex Central downloaded the <b>Current Version</b> of the component  |
| Associated Products | Displays the name of the managed product or the number of managed products using the component<br><br>If more than one managed products use the component, move the mouse cursor over the text to display the list of associated managed products. |

## Update Source

Configure the Apex Central server to download components from the Trend Micro ActiveUpdate server or other update sources. You can specify other update sources if the Apex Central server is unable to connect to the Trend Micro ActiveUpdate server directly or if you host an update server in your network.

By default, Apex Central uses a more secure HTTPS connection method to download components from the Trend Micro ActiveUpdate server.

To access other update sources, Apex Central supports Remote UNC authentication, which uses a user account from the update source server to share a folder for Apex Central to download updates.

## Deployment Plan

A deployment plan allows you to specify the scope and schedule in which the Apex Central server deploys updated components to managed products.

After the Apex Central server downloads a new component version from an update source, you can configure Apex Central to deploy updated components to managed products immediately, at a specified time, or after a delay period.

You can configure Apex Central to deploy updated components to selected managed products based on different deployment schedules.

When creating a deployment schedule, consider the following:

- You can only select one folder or managed product for each deployment schedule. However, you can specify more than one schedule for the deployment plan.
- Apex Central bases the deployment plan delays on the completion time of the download, and these delays are independent of each other.

For example, if you have three folders to update at 5-minute intervals, you can assign the first folder a delay of 5 minutes, and then set delays of 10 and 15 minutes for the two remaining folders, respectively.



**Note**

If you do not specify a deployment schedule in the deployment plan, Apex Central downloads the updates but does not deploy updated components to managed products.

---

## Adding a Deployment Schedule

You can configure a deployment schedule to deploy updated components to selected managed products based on the schedule you specify.

---

### Procedure

1. Access the **Scheduled Update** or **Manual Update** screen.
2. In the **Deployment Plan** section, select **Define different deployment plans for managed products**.
3. Click **+ Add**.

The **Add Schedule** screen appears.

4. Configure the deployment schedule.
5. From the **Managed Products/Folder** tree, select a managed product or product folder.
6. Click **OK** to save the settings.

After creating a deployment plan, you can perform the following tasks:

- Click a schedule to edit the deployment schedule settings.
  - Click **Delete** to remove a selected deployment schedule.
- 

## Configuring Scheduled Update Settings

Configure scheduled component update settings to allow the Apex Central server to download selected components from an update source based on the specified schedule.



You can also configure Apex Central to deploy updated components to managed products based on the deployment plan.

**Note**

Migrating to Apex Central directly from Control Manager 6.0 Service Pack 3 retains previously configured **Update Source**, **Download Schedule**, and **Deployment Plan** configurations for the **All Pattern files/Cleanup templates**, **except Deep Discovery Malware Pattern** component on the **Scheduled Update** screen.

---

**WARNING!**

Migrating to Apex Central directly from Control Manager 6.0 Service Pack 3 resets the **Components** configurations on the **Manual Update** and **Scheduled Update** screens to default settings.

---

**Procedure**

1. Go to **Administration > Updates > Scheduled Update**.
2. Use the drop-down lists to filter the component list. You can filter the component list based on the following:
  - **Products:** Select one or more managed products or all Trend Micro products from the drop-down and click **Apply**
  - **Categories:** Select one or more component categories from the drop-down and click **Apply**
  - **Types:** Select one or more component types from the drop-down and click **Apply**
3. In the **Components** section, select the component categories or expand the categories to select components to update.

For more information, see [Component List on page 12-2](#).



**Important**

If you select the **Enable intelligent component downloading** check box, Apex Central automatically selects all components based on the selected component categories. You cannot select individual components to update. To select individual components, clear the check box.

---



**Note**

To minimize Apex Central network traffic, disable the downloading of components that have no corresponding managed products or services.

---

4. (Optional) Select **Enable intelligent component downloading** to allow Apex Central to automatically detect and download new components based on the selected component categories from an update source.
- 



**Note**

If the intelligent component downloading feature is not enabled, Apex Central only downloads updates for existing components selected in the component list during a scheduled or manual update.

---

5. In the **Update Source** section, select one of the following options and configure the required settings:
  - **Trend Micro ActiveUpdate server:** Select this option to download component updates from the official Trend Micro ActiveUpdate server.
  - **Other update source:** Type the URL of the update source in the text field. You can specify up to five update sources by clicking the + icon.

If server authentication is required, click **Specify authentication credentials** and type the user name and password information.

For more information, see [Update Source on page 12-3](#).


**Note**

If the Apex Central server uses a proxy server to connect to an update source, configure the proxy settings on the **Proxy Settings** screen.

For more information, see [Configuring Proxy Settings for Component/License Updates, Cloud Services, and Syslog Forwarding on page 12-12](#).

6. In the **Download Schedule** section, select **Enable scheduled downloads** and specify the component download schedule.
7. In the **Deployment Plan** section, select a deployment option and configure the required settings.

| OPTION                                  | DESCRIPTION  |
|---|--|
| Deploy to all selected managed products | Select this option to deploy updated components to the selected managed products based on one of the following schedules: <ul style="list-style-type: none"> <li>• <b>Immediately:</b> Apex Central deploys the updated components to the managed products as soon as Apex Central finishes downloading new component versions.</li> <li>• <b>Start at:</b> Apex Central deploys updated components to managed products at the specified time.</li> <li>• <b>Delay:</b> Apex Central deploys updated components to managed products after waiting for the specified time.</li> </ul> |

| OPTION   | DESCRIPTION   |
|--|---|
| Define different deployment plans for managed products | <p>Select this option to configure deployment schedules for specified managed products.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Click <b>+</b> <b>Add</b> to add a new deployment schedule.</li> </ul> <p>For more information, see <a href="#">Adding a Deployment Schedule on page 12-4</a>.</p> <ul style="list-style-type: none"> <li>Click a schedule to edit the deployment schedule settings.</li> <li>Click <b>Delete</b> to remove a selected deployment schedule.</li> </ul> <hr/> <p> <b>Note</b></p> <p>If you do not specify a deployment schedule, Apex Central downloads the component updates but does not deploy updated components to managed products.</p> |
| Do not deploy  | <p>Select this option if you do not want Apex Central to automatically deploy updated components to managed products.</p> <p>You can manually deploy updated component to managed products on the <b>Products</b> screen.</p> <p>For more information, see <a href="#">Executing Managed Product Tasks on page 11-8</a>.</p>  |

8. Click **Save**.

## Configuring Manual Update Settings

You can start a Manual Update on the Apex Central server to download selected components from an update source.

You can also configure Apex Central to deploy updated components to managed products based on the deployment plan.

**WARNING!**

Migrating to Apex Central directly from Control Manager 6.0 Service Pack 3 resets the **Components** configurations on the **Manual Update** and **Scheduled Update** screens to default settings.

---

**Procedure**

1. Go to **Administration > Updates > Manual Update**.
2. Use the drop-down lists to filter the component list. You can filter the component list based on the following:
  - **Products:** Select one or more managed products or all Trend Micro products from the drop-down and click **Apply**
  - **Categories:** Select one or more component categories from the drop-down and click **Apply**
  - **Types:** Select one or more component types from the drop-down and click **Apply**
3. In the **Components** section, select the component categories or expand the categories to select components to update.

For more information, see [Component List on page 12-2](#).

**Important**

If you select the **Enable intelligent component downloading** check box, Apex Central automatically selects all components based on the selected component categories. You cannot select individual components to update. To select individual components, clear the check box.

---

**Note**

To minimize Apex Central network traffic, disable the downloading of components that have no corresponding managed products or services.

---

4. (Optional) Select **Enable intelligent component downloading** to allow Apex Central to automatically detect and download new components based on the selected component categories from an update source.



**Note**

If the intelligent component downloading feature is not enabled, Apex Central only downloads updates for existing components selected in the component list during a scheduled or manual update.

---

5. In the **Update Source** section, select one of the following options and configure the required settings:
  - **Trend Micro ActiveUpdate server:** Select this option to download component updates from the official Trend Micro ActiveUpdate server.
  - **Other update source:** Type the URL of the update source in the text field. You can specify up to five update sources by clicking the + icon.

If server authentication is required, click **Specify authentication credentials** and type the user name and password information.

For more information, see [Update Source on page 12-3](#).

---




**Note**

If the Apex Central server uses a proxy server to connect to an update source, configure the proxy settings on the **Proxy Settings** screen.

For more information, see [Configuring Proxy Settings for Component/License Updates, Cloud Services, and Syslog Forwarding on page 12-12](#).

---

6. In the **Deployment Plan** section, select a deployment option and configure the required settings.

| OPTION   | DESCRIPTION  |
|--|--|
| Deploy to all selected managed products                | <p>Select this option to deploy updated components to the selected managed products based on one of the following schedules:</p> <ul style="list-style-type: none"> <li>• <b>Immediately:</b> Apex Central deploys the updated components to the managed products as soon as Apex Central finishes downloading new component versions.</li> <li>• <b>Start at:</b> Apex Central deploys updated components to managed products at the specified time.</li> <li>• <b>Delay:</b> Apex Central deploys updated components to managed products after waiting for the specified time.</li> </ul>  |
| Define different deployment plans for managed products | <p>Select this option to configure deployment schedules for specified managed products.</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• Click <b>+ Add</b> to add a new deployment schedule.</li> </ul> <p>For more information, see <a href="#">Adding a Deployment Schedule on page 12-4</a>.</p> <ul style="list-style-type: none"> <li>• Click a schedule to edit the deployment schedule settings.</li> <li>• Click <b>Delete</b> to remove a selected deployment schedule.</li> </ul> <hr/> <p> <b>Note</b></p> <p>If you do not specify a deployment schedule, Apex Central downloads the component updates but does not deploy updated components to managed products.</p> |
| Do not deploy  | <p>Select this option if you do not want Apex Central to automatically deploy updated components to managed products.</p> <p>You can manually deploy updated component to managed products on the <b>Products</b> screen.</p> <p>For more information, see <a href="#">Executing Managed Product Tasks on page 11-8</a>.</p>   |

## 7. Click **Download Now**.

The download progress displays at the top of the **Manual Update** screen.

8. To cancel a download in progress:
    - Click the **Stop Current Update** button in the progress bar.
    - Click the **Download Now** button to cancel the download in progress and start a new download.
- 

## Configuring Proxy Settings for Component/License Updates, Cloud Services, and Syslog Forwarding

Apex Central allows you to use a proxy server for component/license updates, cloud services, and syslog forwarding.



### Note

You can also use the same proxy server for syslog forwarding if you select a SOCKS protocol for the server. Syslog forwarding does not support HTTP protocol proxy servers.

For more information, see [Configuring Syslog Forwarding on page 16-14](#).

---

### Procedure

1. Go to **Administration > Settings > Proxy Settings**.

The **Proxy Settings** screen appears.

2. Select **Use a proxy server for component/license updates, cloud services, syslog forwarding, and Suspicious Object Hub Apex Central server connections**.
3. Select the protocol:



### Note

Syslog forwarding does not support HTTP proxy servers. To use a proxy server for syslog forwarding, select a SOCKS protocol.

---



- **HTTP**
  - **SOCKS 4**
  - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP address** field.
  5. Type a port number in the **Port** field.
  6. Type a user name and password if your server requires authentication.
  7. Click **Save**.
-



# Chapter 13

## Command Tracking and Product Communication

This section discusses how to track commands issued from the Apex Central server.

Topics include:

- *Command Tracking on page 13-2*
- *Querying and Viewing Commands on page 13-3*
- *Configuring Communication Time-out Settings on page 13-4*

## Command Tracking

The **Command Tracking** screen provides a list of all previously issued commands sent from the Apex Central server. You can use this screen to monitor the status of the commands you issued to managed products from the Apex Central console. For example, after issuing a Start Scan Now task, which can take several minutes to complete, you can proceed with other tasks and then refer to the **Command Tracking** screen to query and view the status of the issued command.

For more information about querying and viewing commands, see [Querying and Viewing Commands on page 13-3](#).

The following table describes the command information that displays on the **Command Tracking** screen.

| COLUMN NAME  | DESCRIPTION  |
|--------------|--|
| Issued       | The date and time when the Apex Central server issued the command to the managed product   |
| Command      | The type of command issued by the Apex Central server  |
| User         | The name of the user who triggered the command   |
| Successful   | The number of managed products that completed the command<br>Click the count in the <b>Successful</b> column to view more detailed information about the command.<br>For more information, see <a href="#">Command Details on page 13-4</a> .      |
| Unsuccessful | The number of managed products unable to perform the command<br>Click the count in the <b>Unsuccessful</b> column to view more detailed information about the command.<br>For more information, see <a href="#">Command Details on page 13-4</a> . |

| COLUMN NAME | DESCRIPTION   |
|-------------|---|
| In Progress | <p>The number of managed products that are currently performing the command</p> <p>Click the count in the <b>In Progress</b> column to view more detailed information about the command.</p> <p>For more information, see <a href="#">Command Details on page 13-4</a>.</p> |
| All         | <p>The total number of managed products to which Apex Central issued the command</p> <p>Click the count in the <b>All</b> column to view more detailed information about the command.</p> <p>For more information, see <a href="#">Command Details on page 13-4</a>.</p>    |

## Querying and Viewing Commands

Use the **Command Tracking** screen to track and view previously issued commands.

### Procedure

1. Go to **Administration > Command Tracking**.

The **Command Tracking** screen appears.

2. To filter the command list, specify the following:
  - **Issued:** Specify when the managed product sent the command
  - **Command:** Select the command to monitor
  - **User:** Provide the account name used to send the command.



#### Tip

Leave this field blank to query commands issued by all users.

- **Status:** Select one or more command statuses and click **Apply**.
3. Click the count in the **Successful**, **Unsuccessful**, **In Progress**, or **All** column to view detailed command information.

The **Command Details** screen appears.

For more information, see [Command Details on page 13-4](#).

## Command Details

The **Command Details** screen displays the following information about an issued command.

| COLUMN NAME   | DESCRIPTION  |
|---------------|--|
| Last Reported | The date and time when the managed product last sent a response to the Apex Central server |
| Server/Entity | The host name of the managed product server  |
| Status        | The status of the issued command   |
| Description   | Additional details about the command status  |



### Note

The **Command Details** screen refreshes every 30 seconds.

## Configuring Communication Time-out Settings

The **Managed Product Heartbeat Interval** settings determine how frequently the agent sends a heartbeat to the Apex Central server.

- The **Managed Product Heartbeat Interval** settings only apply to managed products that register to the Apex Central server using the Apex Central management console.
- Long heartbeat intervals consume less bandwidth but allow more network events to occur before Apex Central updates the communication status.
- Short intervals between heartbeats consume more bandwidth but present a more up-to-date picture of your network status.

The **Command Time-out Settings** determines how long Apex Central attempts to send a command to a managed server.

---

## Procedure

1. Go to **Administration > Managed Servers > Communication Time-out Settings**.

The **Communication Time-out Settings** screen appears.

2. In the **Managed Product Heartbeat Interval** section, configure the following settings:

- **Report managed product status every:** Defines the agent communication heartbeat interval

Valid values are between 5 and 480 minutes.

- **If no communication, set status as abnormal after:** Defines the agent communication time-out interval

Valid values are between 15 and 1440 minutes.



### Important

The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

---

3. In the **Command Time-out Settings** section, select one of the following:
    - 24 hours
    - 48 hours
    - 72 hours
  4. Click **Save**.
-





# **Part IV**

## **Policies**





# Chapter 14

## Policy Management

This section contains information about how to perform policy management on managed products and endpoints.

---



### Important

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

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

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

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

<https://docs.trendmicro.com/en-us/enterprise/apex-central-widget-and-policy-management-guide/introduction.aspx>

---

Topics include:

- [Policy Management on page 14-2](#)
- [Policy Status on page 14-24](#)

## Policy Management

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

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

### Creating a New Policy

---



#### Important

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

You can download a PDF version of the guide, or view the guide online, using the following link:

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

---

#### Procedure

1. Go to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

The screen refreshes to display policies created for the selected managed product.

For more information about configuring policy settings for specific managed products, see the *Apex Central Widget and Policy Management Guide*.

3. Click **Create**.

The **Create Policy** screen appears.

4. Type a policy name.

5. Specify targets.

Apex Central provides several target selection methods that affect how a policy works.

The policy list arranges the policy targets in the following order:

- **Specify Targets:** Use this option to select specific endpoints or managed products.

For details, see [Specifying Policy Targets on page 14-8](#).

- **Filter by Criteria:** Use this option to allocate endpoints automatically based on the filtering criteria.

For details, see [Filtering by Criteria on page 14-5](#).

- **None (Draft only):** Use this option to save the policy as a draft without choosing any targets.

For more information about the policy list, see [Understanding the Policy List on page 14-20](#).

6. Click a managed product feature to expand it and configure its settings. Repeat this step to configure all features.

- Each feature has a link to a Help topic that discusses the feature and how to use it.
- 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.

- If you are creating a policy for **Apex One Security Agent** that you want to act as a parent to a future child policy, configure settings that can be inherited, customized, or extended on the child policy.
  - For a list of Security Agent settings that can be inherited, customized, or extended, see [Working with Parent Policy Settings on page 14-10](#).
  - For details on creating a child policy, see [Inheriting Policy Settings on page 14-14](#).

## 7. Click **Deploy** or **Save**.

If you clicked **Deploy**, Apex Central starts the deployment. The deployed policy appears in the list on the **Policy Management** screen. It usually takes a few minutes for Apex Central to deploy the policy to the targets.

Click **Refresh** on the **Policy Management** screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Apex Central and the targets. Also check if the targets are working properly.

Once Apex Central deploys a policy to the targets, the settings defined in the policy overwrite the existing settings in the targets. Apex Central enforces the policy settings in the targets every 24 hours. Although local administrators can make changes to the settings from the managed product console, the changes are overwritten every time Apex Central enforces the policy settings.

- Apex Central enforces the policy settings on the targets every 24 hours. Since policy enforcement only occurs every 24 hours, the product settings in the targets may not align with the policy settings if local administrators make changes through the managed product console between the enforcement period.
- Policy settings deployed to IMSVA servers take priority over the existing settings on the target servers instead of overwriting them. IMSVA servers save these policy settings on the top of the list.
- If an Apex One Security Agent assigned with a Apex Central policy has been moved to another Apex One domain, the agent settings

will temporarily change to the ones defined by that Apex One domain. Once Apex Central enforces the policy again, the agent settings will comply with the policy settings.

---

## Filtering by Criteria

Use this option to allocate endpoints automatically based on the filtering criteria.

This option:

- Is only available on the following managed products:
  - Apex One (Mac)
  - Apex One Data Loss Prevention
  - Apex One Security Agent
  - Mobile Security for Enterprise
  - Trend Micro Endpoint Application Control
- Uses a filter to automatically assign current and future targets to the policy
- Is useful for deploying standard settings to a group of targets

Administrators can change the priority of filtered policies in the policy list. When an administrator reorders the policy list, Apex Central re-assigns the targets to different filtered policies based on the target criteria and the user roles of each policy creator.

Apex Central can only assign endpoints without policies to a new filtered policy. To re-allocate an endpoint already assigned to a filtered policy, move another filtered policy with the matching criteria up the priority list.



See [Assigning Endpoints to Filtered Policies on page 14-7](#) for more information on how Apex Central assign targets to filtered policies.

## Procedure

1. On the **Create Policy** screen, go to the **Targets** section, select **Filter by Criteria**, and then click **Set Filter**.

The **Filter by Criteria** screen appears.

2. Select the following options and define the criteria.

| CRITERIA          | DESCRIPTION   |
|-------------------|---|
| Match keywords in | <p>Define keywords based on the host name or Apex Central display name.</p> <hr/> <p> <b>Note</b><br/>Apex Central performs partial matching for single keyword searches. You can search multiple, comma-separated keywords, however, Apex Central only provides full string matches for each keyword provided.</p>  |
| IP addresses      | <p>Define a range of IP addresses and click <b>Add</b>.</p> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• Policy management only supports IPv4 addresses.</li> <li>• When a new managed product or endpoint registers to Apex Central, it takes about an hour for the managed product or endpoint to become available for searching by IP address.</li> </ul> |
| Operating systems | <p>Select one or more operation systems from the drop-down list.</p>  |



| CRITERIA    | DESCRIPTION   |
|-------------|---|
| Directories | Select one of the following directories and define the criteria. <ul style="list-style-type: none"> <li>• <b>Product Directory:</b> Select folders from the Product Directory structure</li> <li>• <b>Active Directory:</b> Select organizational units from an integrated Active Directory structure</li> <li>• <b>Apex One domain hierarchy:</b> Type at least one Apex One domain hierarchy keyword</li> </ul> |

### 3. Click **Save**.

The **Create Policy** screen reloads.

## Assigning Endpoints to Filtered Policies

When a new endpoint registers to Apex Central, it goes through the filtered policies in the list in descending order. Apex Central assigns the new endpoint to a filtered policy when the following conditions are both satisfied:

- The new endpoint matches the target criteria in the policy
- The policy creator has the permission to manage the new endpoint

The same action applies to an endpoint already assigned to a policy, but the policy creator later deletes the policy.



### Note

For endpoints just registered to Apex Central and for those just released from deleted policies, there is a three-minute grace period during which no endpoint allocation occurs. These endpoints are temporarily without policies during this period.

If an endpoint does not meet the target criteria in any filtered policies, the endpoint does not associate with any policies. Apex Central allocates these endpoints again when the following actions occur:

- Create a new filtered policy

- Edit a filtered policy
- Reorder the filtered policies
- Daily endpoint allocation schedule

Apex Central uses a daily endpoint allocation schedule to ensure that endpoints are assigned to the correct policies. This action occurs once at 3:15 pm every day. When endpoint properties change, such as the operating system or IP address, these endpoints require the daily schedule to re-assign them to the correct policies.



#### Note

- If the endpoints are offline during the daily endpoint allocation schedule, the policy status for these endpoints will remain pending until they go online.
- If the Apex One domain of the endpoint is changed, Apex Central deploys the updated the policy after 10 minutes.

When the above actions occur, Apex Central allocate endpoints based on the following conditions:

**TABLE 14-1. Endpoint Allocation for Filtered Policies**

|                                    | New endpoints or endpoints from deleted policies | Endpoints without policies | Endpoints with policies |
|------------------------------------|--|----------------------------|-------------------------|
| Create a new policy                |  | ●                          |                         |
| Edit a policy                      | ●  | ●                          | ●                       |
| Reorder the filtered policies      | ●  | ●                          | ●                       |
| Daily endpoint allocation schedule | ●  | ●                          | ●                       |

## Specifying Policy Targets

Use this option to select specific endpoints or managed products.

This option:

- Uses the search or browse function to locate specific targets and manually assigns them to the policy
- Is useful when administrators plan to deploy specific settings only to a certain targets
- Remains static on the top of the policy list and takes priority over any filtered policies

---

### Procedure

1. On the **Create Policy** screen, go to the **Targets** section, select **Specify Target(s)**, and then click **Select**.

The **Specify Targets** screen appears.

2. Use **Search** or **Browse** to locate the targets.
  - **Search:** Use the following search criteria to find endpoints or managed products. The search results display the endpoints or managed products matching all of the selected criteria.
    - **Match keywords in:** Define keywords based on the host name or Apex Central display name.
    - **IP addresses:** Define a range of IP addresses and click **Add**.



#### Note

- Policy management only supports IPv4 addresses.
  - When a new managed product or endpoint registers to Apex Central, it takes about an hour for the managed product or endpoint to become available for search by IP address.
- 
- **Operating systems:** Select one or more operating systems from the drop-down.
  - **Browse:** Browse the Product Directory or Active Directory to locate endpoints or managed products to assign to the policy.



**Note**

To set up the Active Directory, see [Active Directory Integration on page 6-2](#).

---

3. Select the endpoints or managed products and then click **Add Selected Targets**.
4. Wait for the numbers in **View Action List** and **View Results** to change.
5. Click **OK**.

The **Create Policy** screen reloads.

---

## Working with Parent Policy Settings

Apex Central administrators who create a parent policy for an **Apex One Agent** can configure certain policy settings to be inherited, customized, or extended.

---



**Note**

These options are not available on other managed products.

---

- **Inherit from parent**

- A child policy administrator cannot change the setting at all. An Apex One administrator can manually change the setting from the Apex One server console. However, the setting will be overwritten when Apex Central deploys policies to the Apex One server.

For example, a Apex Central administrator can create a parent policy that enforces the exclusion of PDF files from a Manual Scan.

- Changes to the setting on the parent policy are always enforced on the child policy.
- If the permission on the parent policy changes from "Inherit from parent" to "Are customizable" or "Extend from parent", the child policy administrator can customize or extend the current setting. Changes to the setting on the parent policy are no longer enforced.

- **Are customizable**

- A child policy can deviate from the setting configured in the parent policy.

For example, if Scheduled Scan on the parent policy runs weekly but is customizable, the child policy administrator can change the schedule to daily.

- Changes to the setting on the parent policy are never enforced on the child policy.
- If the permission on the parent policy changes from "Are customizable" to "Inherit from parent", the current setting on the parent policy overwrites the setting on the child policy. Changes to the setting on the parent policy are always enforced.


- **Extend from parent**

- A child policy administrator can add to the items configured 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 safe and trustworthy files to the child policy.

- Items added or removed from the parent policy are also added or removed from the child policy. A removed item can be added back to the child.
- If the permission on the parent policy changes from "Extend from parent" to "Inherit from parent", items in the child policy that have no match in the parent are removed. Changes to the items on the parent policy are always enforced.

The following table lists the parent policy settings that can be inherited, customized, or extended.

| SETTING AND PATH   | AVAILABLE OPTIONS   |                  |   |
|--|---------------------|------------------|---|
|  | INHERIT FROM PARENT | ARE CUSTOMIZABLE | EXTEND FROM PARENT  |
| Scan schedule<br><b>Scheduled Scan Settings &gt; Target tab &gt; Schedule section</b>  | ●                   | ●                |   |
| File extensions to scan<br><b>Manual Scan / Real-time Scan / Scan Now / Scheduled Scan Settings &gt; Target tab &gt; Files to Scan section &gt; Files with the following extensions option</b> | ●                   |                  | ●   |
| Scan exclusion lists (directories, files, and file extensions to exclude from scans)<br><b>Manual Scan / Real-time Scan / Scan Now / Scheduled Scan Settings &gt; Scan Exclusion tab</b>       | ●                   |                  | <div style="border: 1px solid black; padding: 5px;">  <b>Note</b><br/>           When selecting <b>Extend from parent</b> from a scan exclusion list, the list expands to show a <b>Child Policy Restrictions</b> section where the parent policy creators can specify items that child policies cannot exclude from scans.         </div> |

## Copying Policy Settings

Administrators can copy the settings from an existing policy, create a new policy with the same settings, and deploy the settings to different endpoints or managed products.

**Note**

It is not possible to copy the settings of a child **Apex One Agent** policy. To determine whether the **Apex One Agent** policy is a child or a parent, check the **Parent Policy** column. A clickable value displays if the policy is a child, and N/A if otherwise.

---

**Procedure**

1. Go to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select the type of product settings from the Product list.

The screen refreshes to display policies created for the selected managed product.

3. Select a policy from the list.

4. Click **Copy Settings**.

The **Copy and Create Policy** screen appears.

5. In the **Policy Name** field, type a name for the policy.

6. Assign **Targets** to the policy.

7. (Optional) Change settings as necessary.

8. Click **Deploy**.

**Note**

- After clicking **Deploy**, please wait two minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
  - Apex Central enforces the policy settings on the targets every 24 hours.
-

## Inheriting Policy Settings

Create a new child policy by inheriting the settings of an existing parent policy. A child policy cannot be copied and its settings cannot be inherited.

This task requires a parent policy for the Apex One agent. A parent policy for the Apex One agent has the value **N/A** displayed under the **Parent Policy** column.

---

### Procedure

**1. Go to Policies > Policy Management.**

The **Policy Management** screen appears.

**2. Select Apex One Agent** from the Product list.

The screen refreshes to display policies created for the selected managed product.

**3. Select a parent policy** that does not have locally managed settings.

**4. Click Inherit Settings.**

The **Inherit and Create Policy** screen appears.

**5. In the Policy Name** field, type a name for the policy.

**6. Assign Targets** to the policy.

**7. (Optional) Review the settings** that can be customized or extended and then make changes as necessary. For a list of settings to review, see [Working with Parent Policy Settings on page 14-10](#).



**Note**

A setting cannot be customized or extended if the option selected on the parent policy is **Inherit from parent**.

---

For example:

- If the Scheduled Scan setting is customizable, you can change the schedule from weekly to daily.



- If the scan exclusion list for Real-time Scan can be extended, you can type additional file names that you deem safe and trustworthy. After the child policy is created, it will add those file names to the scan exclusion list.

## 8. Click **Deploy**.



### Note

- After clicking **Deploy**, please wait two minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
  - Apex Central enforces the policy settings on the targets every 24 hours.
- 

## Modifying a Policy

Administrators can modify policy targets and settings as necessary. The root account owner can modify every policy in the list, while other account owners can only modify the policies they created. After a policy is modified, Apex Central deploys the policy to the targets.



### Important

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

You can download a PDF version of the guide, or view the guide online, using the following link:

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

---

For a parent policy for the Apex One agent, if you modified the targets and settings for specific features, the modifications will apply to all child policies

and deployed to the respective targets. Some settings on a parent policy support **permissions**, which control the changes allowed on child policies. Modifications to these parent policy permissions are also applied to child policies and deployed to targets. For a list of settings that support permissions, see [Working with Parent Policy Settings on page 14-10](#).

For example:

- If you changed the scan schedule permission from "Inherit from parent" to "Are customizable", administrators can start to customize the existing schedule on their child policies.
- If you changed the Manual Scan file extensions permission from "Extend from parent" to "Inherit from parent", any file extensions that administrators added to child policies will be removed. In addition, administrators will no longer be able to add file extensions.

---

## Procedure

1. Navigate to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the **Policy** column.

The **Edit Policy** screen appears.

4. Modify the policy.



### Note

Modifying the filtering criteria in a filtered policy can affect target allocation. Apex Central may re-assign some targets to other filtered policies, or add additional targets to the current policy.

---

5. Click **Deploy**.

It usually takes a few minutes for Apex Central to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Apex Central and the targets. Also check if the targets are working properly.

Apex Central enforces the policy settings on the targets every 24 hours.

---

## Importing and Exporting Policies

Export policies for backup or to import to another Apex Central server of the same version.



### Note

- Apex Central exports policy settings but not policy targets.
- A parent policy stays as a parent after the export or import.
- A child policy becomes a parent after the export. Consequently, it is a parent after the import.
- Apex Central cannot import a policy if its name is the same as an existing child policy. If the existing policy is not a child, Apex Central overwrites it after the import.
- For more information, see the following topics:
  - [Creating a New Policy on page 14-2](#)
  - [Inheriting Policy Settings on page 14-14](#)

---

### Procedure

1. Go to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

The screen refreshes to display policies created for the selected managed product.

3. To export, select one or several policies, click **Export Settings**, and then save the resulting policy file.
  - If you exported a single policy, the resulting file has the extension \*.cmpolicy.
  - If you exported several policies, the resulting file is a compressed (\*.zip) file containing the individual .cmpolicy files.
4. To import, click **Import Settings** and then locate and load the policy file.
  - You can import an entire \*.zip file or import individual \*.cmpolicy files one by one.
  - If the policy already exists in the policy list, a confirmation prompt appears, asking if you want to overwrite the existing policy.

Click **OK** to proceed.

The screen refreshes and displays the imported policy at the top of the list.

For more information about reordering the policy list, see [Reordering the Policy List on page 14-23](#).

---

## Deleting a Policy

Administrators can remove a policy from the list. Apex Central then re-allocates the targets associated with the deleted policy if the targets match the filtering criteria of another policy. Those without a match become endpoints without policies, and they keep the settings defined by the deleted policy unless a managed product administrator modifies the settings.

Apex Central only allows policy creators to delete their own policies. However, the root account can delete every policy in the list.

It is not possible to delete an Apex One Agent parent policy with settings *inherited* by an existing child policy.

---

### Procedure

1. Go to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

The screen refreshes to display policies created for the selected managed product.

3. Select the policy to delete.

4. Click **Delete**.

A confirmation screen appears.

5. Click **OK**.
- 

## Changing the Policy Owner

The default owner of a policy is the user account that created the policy. You can use the **Policy Management** screen to change the owner of a policy to any Apex Central user account. You can also change the policy owner to an Active Directory group, which designates all Active Directory users within the group as owners of the policy.



### Important

If you change the owner of a policy to a user account that does not have access rights to the specified targets, the new owner can modify the policy settings but cannot view the policy data.

---

### Procedure

1. Go to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select one or more policies to change the owner.

3. Click **Change Owner**.

The **Change Policy Owner** screen appears.

4. Select a user account from the drop-down list.
5. Click **Save** to change the owner.

Apex Central sends an email notification to all user accounts assigned the “Administrator” role.

---

## Understanding the Policy List


The policy list displays the information and status of policies created by all users. When a new endpoint registers to Apex Central, it goes through the filtered policies in the list in descending order. Apex Central assigns the new endpoint to a filtered policy when the following conditions are both satisfied:


- The new endpoint matches the target criteria of the policy
- The policy creator has the permission to manage the new endpoint

The following table describes the policy list columns that display on the **Policy Management** screen. Click a column to sort the data.

**TABLE 14-2. Policy List**

| COLUMN   | DESCRIPTION   |
|----------|---|
| Priority | <p>Displays the priority of the policies</p> <ul style="list-style-type: none"><li>• Apex Central lists policies from the highest to the lowest priority.</li><li>• When administrators create a filtered policy, Apex Central saves the new policy as the lowest priority policy.</li><li>• A specified policy takes priority over any filtered policies and remains on the top of the list. Administrators cannot reorder specified policies.</li><li>• Apex Central places draft policies at the bottom of the list.</li></ul> |
| Policy   | <p>Displays the name of the policy</p>  |

| COLUMN         | DESCRIPTION   |
|----------------|---|
| Policy Version | <p>This column only appears if the selected product is <b>Apex One Security Agent</b>.</p> <p>Displays the latest policy version deployed</p> <hr/> <p> <b>Note</b><br/>Some targets might not have the latest policy version deployed. To view the current policy deployed on specific targets, click the number in the <b>Deployed</b> column.</p> |
| Parent Policy  | <p>This column only appears if the selected product is <b>Apex One Security Agent</b>.</p> <p>If a policy is a child policy (that is, it inherited its settings from a parent policy), this column shows the name of the parent policy. Otherwise, N/A displays.</p>  |
| Deviations     | <p>This column only appears if the selected product is <b>Apex One Security Agent</b>.</p> <p>If a policy is a child policy, this column shows the number of settings that have been changed on the policy and are therefore inconsistent with settings on the parent policy. If settings are consistent between the policy and its parent, 0 (zero) displays.</p> <p>If a policy is not a child policy, N/A displays.</p>            |

| COLUMN      | DESCRIPTION   |
|-------------|---|
| Owner       | <p>Displays the user who is currently assigned the policy</p> <hr/>  <b>Note</b><br>The default owner is the user who created the policy. <ul style="list-style-type: none"> <li>• If you change the owner of a policy to a user account that does not have access rights to the specified targets, the new owner can modify the policy settings but cannot view the policy data.</li> <li>• You can also assign multiple owners by assigning the policy to an Active Directory group.</li> </ul> <p>For more information, see <a href="#">Changing the Policy Owner on page 14-19</a>.</p>                                      |
| Last Editor | Displays the user who last edited the policy  |
| Last Edited | <p>This column only appears if the selected product is <b>Apex One Security Agent</b>.</p> <p>Displays when the policy was last edited</p>  |
| Targets     | <p>Displays how administrators select targets for the policy.</p> <ul style="list-style-type: none"> <li>• <b>Specified:</b> Uses the browse or search function to select specific targets for the policy. Specified policies remain static on the top of the policy list and take priority over filtered policies.</li> <li>• <b>Filtered:</b> Uses a filter to automatically assign current and future endpoints to the policy. Administrators can rearrange the priority of filtered policies. Hover over an item to conveniently view the filter criteria and make adjustments as necessary.</li> <li>• <b>None:</b> The policy creator saved the policy as a draft without selecting any targets.</li> </ul> |
| Deployed    | <p>Displays the number of targets that have applied the policy settings or have unactivated product services</p> <p>Click the number to view the policy status.</p>   |



| COLUMN      | DESCRIPTION   |
|-------------|---|
| Pending     | <p>Displays the number of targets that have not applied the policy settings</p> <p>Click the number to view the policy status.</p>  |
| Offline     | <p>Displays the number of targets that have offline agents</p> <p>Click the number to view the policy status.</p>   |
| With Issues | <p>Displays the number of targets that have not applied the policy settings due to unsupported policy deployment, no policy configuration, system errors, endpoint communication errors with the product server, unsupported endpoints, locally changed settings, disabled product services, or partial deployment</p> <p>Click the number to view the policy status.</p> |

**Note**

The numbers in **Deployed** and **Pending** columns only reflect the endpoints or managed products that an administrator has permission to manage.

## Reordering the Policy List

Administrators can use the **Reorder** button to change the order of the filtered policies. Rearranging the policy list can affect target allocation. Apex Central may re-assign some targets to different filtered policies.

**Note**

- Specified policies remain static and always take priority over filtered policies.
- This function is only available for managing Apex One settings.

### Procedure

1. Go to **Policies > Policy Management**.

The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

The screen refreshes to display policies created for the selected managed product.

3. Click **Reorder**.

The **Reorder Policies** screen appears.

4. Rearrange the order of the **Priority** column.

5. Click **Save**.

**Note**

After clicking **Save**, please wait two minutes for Apex Central to re-assign the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.

---

## Policy Status

Policy status allows administrators to check if Apex Central has successfully deployed a policy to its targets.

To check the policy deployment status, use one of the following methods:

- On the **Policy Management** screen, click a number in the policy list. The **Log Query** screen appears.
- On the dashboard, click a number in the **Policy Status** widget. The **Log Query** screen appears.
- Perform a log query

The following table provides the descriptions and suggestions about each policy status:

**TABLE 14-3. Policy Status**

| POLICY STATUS                        | DESCRIPTION  | SUGGESTIONS   |
|--------------------------------------|--|---|
| Pending                              | Apex Central is processing the policy.   | Wait a few minutes and then check the status again.   |
| Without policy                       | Apex Central has not assigned a policy to this endpoint or managed product.  | Assign a policy to the endpoint or managed product.   |
| Deployed                             | Apex Central has successfully deployed the policy.   | N/A   |
| Endpoint unable to connect to server | <ul style="list-style-type: none"> <li>• The endpoint did not receive the policy settings.</li> <li>• The server is currently busy.</li> </ul> | <ul style="list-style-type: none"> <li>• Check the connection status of the endpoint</li> <li>• Connect the endpoint to the company network</li> <li>• Wait for the updated policy status</li> </ul>  |
| Inapplicable product settings        | The managed product cannot process some of the policy settings.  | <ul style="list-style-type: none"> <li>• Verify the policy settings</li> <li>• Update to the latest policy template version</li> <li>• Check the settings on the managed product</li> <li>• Verify the IP address of the managed product on the <b>Managed Servers</b> screen</li> </ul> <p>If the IP address is incorrect, unregister and then register the managed product again to Apex Central.</p> <ul style="list-style-type: none"> <li>• Refer to the <i>Administrator's Guide</i> for the managed product</li> </ul> |
| Unsupported endpoint                 | The endpoint does not support some features specified in the policy settings.  | Upgrade the agent to a supported version.   |

| POLICY STATUS  | DESCRIPTION   | SUGGESTIONS  |
|--|---|--|
| Settings changed locally                             | Some settings on the endpoint or managed product do not comply with the settings specified in the policy because the managed product administrator has made some changes through the managed product console. | Verify the settings on the managed product console.  |
| Unactivated licenses                                 | The managed product has not activated the licenses for some of the services specified in the policy settings.   | Activate the licenses for the related services from the <b>License Management</b> screen on the Apex Central console |
| Disabled product services                            | The managed product has disabled some of the services specified in the policy settings.   | Enable the related services on the managed product.  |
| Partially deployed                                   | Apex Central has enforced a portion of the policy settings.   | Wait a few minutes and then check the status again.  |
| Managed by [Apex Central server name]                | Another Apex Central is currently managing the managed product.   | Remove the managed product from the Managed Server list and add the managed product to the list again.               |
| Invalid user name or password                        | The user name or password for authentication is incorrect.  | Verify the user name or password.  |
| Invalid product server or authentication information | The server name or the authentication information is incorrect.   | Verify the server name and the authentication information.   |

| POLICY STATUS                              | DESCRIPTION  | SUGGESTIONS  |
|--|--|--|
| Unable to automatically log on to product  | Apex Central cannot use the single sign-on function to access the managed product. | <ul style="list-style-type: none"> <li>• Check the single sign-on function in the Product Directory</li> <li>• Check the connection status of the MCP agent</li> <li>• Change the server connection type from <b>Automatic</b> to <b>Manual</b> in the <b>Managed Servers</b> list.</li> </ul> |
| Web server configuration error             | A web service error has occurred.  | Check the IIS configuration.   |
| Product communication error                | Unable to access the product console.  | <ul style="list-style-type: none"> <li>• Check if you can connect to the managed product's web console.</li> <li>• Check the settings of the managed product.</li> </ul>   |
| Unable to connect to product               | Apex Central cannot establish a connection with the managed product.               | <ul style="list-style-type: none"> <li>• Check the connection status of the managed product.</li> <li>• Check the network connection</li> </ul>  |
| Unsupported product version                | The managed product version is not supported.                                      | Upgrade the managed product to a supported version.  |
| Network configuration error                | A network connection error has occurred.   | Check the network connection.  |
| System error. Error ID: [error ID number]. | A system error has occurred.   | Contact your Trend Micro support representative.   |



# Chapter 15

## Policy Resources

This section contains information about policy resources for integrated products/services.

---



### Important

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

You can download a PDF version of the guide, or view the guide online, using the following link:

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

---

Topics include:

- *Application Control Criteria on page 15-2*
- *Data Loss Prevention on page 15-15*
- *Intrusion Prevention Rules on page 15-33*
- *Device Control Allowed Devices on page 15-37*

## Application Control Criteria

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



### Important

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

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



You can download a PDF version of the guide, or view the guide online, using the following link:



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

---

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



| TASK            | DESCRIPTION  |
|-----------------|--|
| Add criteria    | <p>Click the <b>Add Criteria</b> drop-down button and select from the following options:</p> <ul style="list-style-type: none"> <li>• <b>Allow:</b> Click to define “Allow” or “Lockdown” criteria<br/>For more information, see <a href="#">Defining Allowed Application Criteria on page 15-4</a>.</li> <li>• <b>Block:</b> Click to define “Block” or “Assessment” criteria<br/>For more information, see <a href="#">Defining Blocked Application Criteria on page 15-6</a>.</li> <li>• <b>Copy:</b> Select an existing criteria and click <b>Copy</b> to define new criteria based on the existing settings</li> <li>• <b>Import:</b> Click to select a ZIP package exported from a compatible Application Control source</li> </ul> <hr/> <p> <b>Note</b><br/>If the imported package contains criteria names that match preexisting criteria, you have the option to <b>Overwrite</b> existing criteria or <b>Skip</b> the import of the criteria with duplicated names.</p> |
| Export criteria | <p>Select the check box to the left of existing criteria and click <b>Export</b> to save the selected criteria to a ZIP package (<code>&lt;timestamp&gt;_iACRuleExport.zip</code>)</p>   |
| Delete criteria | <p>Select the check box to the left of existing criteria and click <b>Delete</b> to remove the selected criteria from the list</p> <hr/> <p> <b>WARNING!</b><br/>If you selected criteria used by existing Apex One Security Agent policies, you must confirm that you want to delete and remove the criteria from all affected Security Agent policies. You cannot undo this action.</p>   |

| TASK                     | DESCRIPTION   |
|--------------------------|---|
| Modify criteria          | <p>Click a <b>Criteria Name</b> to modify the criteria settings</p> <hr/> <p> <b>Note</b><br/>Affected endpoints receive modified criteria settings the next time the Security Agents connect to the server.</p>   |
| View policy associations | <p>Click the value in the <b>Target Policies</b> column to display a list of all Apex One Security Agent policies that implement the criteria.</p> <hr/> <p> <b>Tip</b><br/>Click a policy name to open a new browser tab on which you can view or modify the policy settings.</p> |

## Defining Allowed Application Criteria

Application Control provides the ability to define criteria that specifically allow 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 and then 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.

For more information about Lockdown policies, see *Application Control Policy Settings*.

### Procedure

1. Go to **Policies > Policy Resources > Application Control Criteria**.

The **Application Control Criteria** screen appears.

2. Click **Add Criteria** and select **Allow**.

The **Allow Criteria Settings** screen appears.

3. Type a unique **Name** for the criteria.
4. Select the level of **Trust permission** for the applications.

| PERMISSION  | DESCRIPTION   | EXAMPLE USE  |
|---|---|--|
| <b>Application cannot execute external processes</b>  | Applications cannot access any external processes or start any other applications   | Use when you want to allow standalone applications to run on endpoints but prevent access to other processes<br><br>For example, this setting allows Microsoft Word to run but prevents embedded OLE objects from executing.   |
| <b>Application can execute other processes</b>        | Applications can start external processes and applications that users are unable to access directly   | Use when you want to allow applications to run on endpoints and still allow access to required child processes or add-ons.<br><br>For example, this setting allows Internet Explorer to run and also allows Internet Explorer to execute any installed plug-ins.                         |
| <b>Inheritable execution rights (not recommended)</b> | Applications can install and start external processes and applications, and the child applications can also install and start external processes and applications | Use when you want to allow installation packages to execute on the endpoint<br><br><b>Inheritable execution rights (not recommended)</b> allows the installation package to perform all installation tasks and then also allows the installed application to run all required processes. |

5. Select the **Match method** used to identify applications and configure required settings.

| METHOD                             | DESCRIPTION  |
|------------------------------------|--|
| <b>Application Reputation List</b> | Allows you to apply the criteria to applications that Trend Micro has tested and assigned a security score for<br><br>For more information, see <a href="#">Application Reputation List on page 15-8</a> .   |
| <b>File paths</b>                  | Allows you to apply the criteria to any application installed in the specified location<br><br>For more information, see <a href="#">File Paths on page 15-9</a> .   |
| <b>Certificates</b>                | Allows you to apply the criteria to applications based on certificate validity and certificate attributes<br><br>For more information, see <a href="#">Certificates on page 15-13</a> .  |
| <b>Hash values</b>                 | Allows you to apply the criteria to applications based on SHA-1 or SHA-256 hash values<br><br>For more information, see <a href="#">Hash Values on page 15-14</a> .  |
| <b>Gray Software List</b>          | Allows you to include applications to the criteria that Trend Micro has tested and found to be potentially harmful<br><br>The Gray Software List is a subset of the Application Reputation List and contains applications that may be malicious if not used properly. Trend Micro recommends blocking or monitoring applications in the Gray Software List to ensure that your network remains secure. |

6. Click **Save**.

## Defining Blocked Application Criteria

Application Control provides the ability to define criteria that specifically block certain applications from executing. 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.

### Procedure

1. Go to **Policies > Policy Resources > Application Control Criteria**.

The **Application Control Criteria** screen appears.

2. Click **Add Criteria** and select **Block**.  
The **Block Criteria Settings** screen appears.
3. Type a unique **Name** for the criteria.
4. To create a monitoring rule, select **Enable assessment mode**.

**Note**

Application Control logs all applications that match the assessment criteria but takes no further action. Application Control allows the applications to execute normally.

---

5. Select the **Match method** used to identify applications and configure required settings.

| METHOD                             | DESCRIPTION  |
|------------------------------------|--|
| <b>Application Reputation List</b> | Allows you to apply the criteria to applications that Trend Micro has tested and assigned a security score for<br><br>For more information, see <a href="#">Application Reputation List on page 15-8</a> . |
| <b>File paths</b>                  | Allows you to apply the criteria to any application installed in the specified location<br><br>For more information, see <a href="#">File Paths on page 15-9</a> .   |
| <b>Certificates</b>                | Allows you to apply the criteria to applications based on certificate validity and certificate attributes<br><br>For more information, see <a href="#">Certificates on page 15-13</a> .                    |
| <b>Hash values</b>                 | Allows you to apply the criteria to applications based on SHA-1 or SHA-256 hash values<br><br>For more information, see <a href="#">Hash Values on page 15-14</a> .  |

| METHOD                    | DESCRIPTION  |
|---------------------------|--|
| <b>Gray Software List</b> | Allows you to include applications to the criteria that Trend Micro has tested and found to be potentially harmful<br><br>The Gray Software List is a subset of the Application Reputation List and contains applications that may be malicious if not used properly. Trend Micro recommends blocking or monitoring applications in the Gray Software List to ensure that your network remains secure. |

6. Click **Save**.

## Application Match Methods

Application Control provides multiple methods for identifying applications to include in the allow and block criteria.



**Note**

Application Control also provides the Gray Software List which you cannot modify.

The Gray Software List is a subset of the Application Reputation List and contains applications that may be malicious if not used properly. Trend Micro recommends blocking or monitoring applications in the Gray Software List to ensure that your network remains secure.

## Application Reputation List



The Application Reputation List is a comprehensive list of applications tested 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.



**Important**

Ensure that you have turned on regular updates to the Certified Safe Software Pattern to stay up-to-date with the latest application information.

You can search for applications by typing the name of **Vendors** or **Applications**. Select applications using the data provided.

| DATA         | DESCRIPTION   |
|--------------|---|
| Application  | <p>The name of the application</p> <hr/> <p> <b>Tip</b><br/>To view detailed information for each application version, expand the Application Reputation List.</p> <hr/> |
| AIR Score    | A comprehensive security score based on an application's popularity and reputation  |
| Global Usage | <p>The global prevalence of the application</p> <hr/> <p> <b>Tip</b><br/>Click the prevalence to view a regional breakdown of the application usage.</p> <hr/>           |

## 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).

Select whether to match by a specific path or a storage type, and specify the match string type (**String** or **Regular Expression (PCRE)**). Type the file paths that apply to the criteria.

**Note**

- Application Control supports the use of the asterisk (\*) wildcard when specifying a **String** type match. The asterisk character can represent one or more characters in a subdirectory of the specified string location.
- Application Control does not support the use of environment variables when specifying file paths for **String** or **Regular Expression (PCRE)** type matches.
- You cannot use wildcard characters to indicate the entire contents of the selected storage location.
- You can specify up to 100 file paths.

**TABLE 15-1. Supported Storage Locations**

| STORAGE LOCATION      | ENVIRONMENT VARIABLE | DESCRIPTION  |
|-----------------------|----------------------|--|
| Specific path         | Not applicable       | Only applies to applications in the exact path specified<br><br> <b>Note</b><br>Application Control does not check device type when using this location type. |
| Any built-in storage  | \$FixedDrives        | Only applies to applications in the path specified and stored on an internal storage device (internal hard disk drive)   |
| Any local storage     | \$LocalDrives        | 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 | \$Removable Drives   | Only applies to applications in the path specified and stored on a removable storage device (USB drive, CD/DVD)  |
| Network path          | \$RemoteDrives       | Only applies to applications in the path specified and stored on a shared network resource   |



| STORAGE LOCATION     | ENVIRONMENT VARIABLE | DESCRIPTION  |
|----------------------|----------------------|--|
| Program Files folder | \$ProgramFiles       | 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        | \$SystemDrive        | Only applies to applications in the path specified and stored in the default Windows system drive  |

### File Path Example Usage

| GOAL                                | ALLOW RULE | BLOCK RULE   | RESULTS  |
|-------------------------------------|------------|--|--|
| Monitor all users' Downloads folder | -          | <ol style="list-style-type: none"> <li><b>Enable assessment mode</b></li> <li><b>Any local storage</b></li> <li><b>String</b></li> <li>C:\Users\*\Downloads\*</li> </ol> | <p>Logs all attempts to access applications in all users' Downloads folder.</p> <p>Monitors:</p> <ul style="list-style-type: none"> <li>C:\Users\john_doe\Downloads\start.exe</li> <li>C:\Users\Administrator\Downloads\start.exe</li> </ul> |

| GOAL  | ALLOW RULE  | BLOCK RULE   | RESULTS   |
|---|---|--|---|
| Block all applications located in any folder under theMyApps subfolder of either Program Files directory  | -   | <ol style="list-style-type: none"> <li>1. <b>Program Files folders</b></li> <li>2. <b>String</b></li> <li>3. <b>\MyApps*</b></li> </ol>  | <p>Blocks:</p> <ul style="list-style-type: none"> <li>• C:\Program Files(x86)\MyApps\start.exe</li> <li>• C:\Program Files\MyApps\start.exe</li> <li>• C:\Program Files(x86)\MyApps\bin\start.exe</li> </ul> <p>Allows:</p> <ul style="list-style-type: none"> <li>• C:\Program Files(x86)\start.exe</li> </ul> |
| Allow all applications located in any folder under theMyApps subfolder of either Program Files directory but Block all other applications/folders | <ol style="list-style-type: none"> <li>1. <b>Program Files folders</b></li> <li>2. <b>String</b></li> <li>3. <b>\MyApps*</b></li> </ol> | <ol style="list-style-type: none"> <li>1. <b>Any local storage</b></li> <li>2. <b>String</b></li> <li>3. <b>C:\Program Files\*</b></li> </ol> <p>AND</p> <ol style="list-style-type: none"> <li>1. <b>Any local storage</b></li> <li>2. <b>String</b></li> <li>3. <b>C:\Program Files (x86)\*</b></li> </ol> | <p>Blocks:</p> <ul style="list-style-type: none"> <li>• C:\Program Files(x86)\start.exe</li> </ul> <p>Allows:</p> <ul style="list-style-type: none"> <li>• C:\Program Files(x86)\MyApps\start.exe</li> <li>• C:\Program Files\MyApps\start.exe</li> <li>• C:\Program Files(x86)\MyApps\bin\start.exe</li> </ul> |

| GOAL  | ALLOW RULE  | BLOCK RULE  | RESULTS   |
|---|---|---|---|
| Block only applications located in theMyApps subfolder of either Program Files directory but Allow all other applications/folders | <ol style="list-style-type: none"> <li>1. Allow the subfolders of the MyApps directory               <ol style="list-style-type: none"> <li>a. <b>Program Files folders</b></li> <li>b. <b>String</b></li> <li>c. <code>\MyApps\*</code><br/><code>\*</code></li> </ol> </li> </ol> | <ol style="list-style-type: none"> <li>1. <b>Program Files folders</b></li> <li>2. <b>String</b></li> <li>3. <code>\MyApps\*</code></li> </ol>                          | <p>Blocks:</p> <ul style="list-style-type: none"> <li>• C:\Program Files(x86)\MyApps\start.exe</li> <li>• C:\Program Files\MyApps\start.exe</li> </ul> <p>Allows:</p> <ul style="list-style-type: none"> <li>• C:\Program Files(x86)\start.exe</li> <li>• C:\Program Files(x86)\MyApps\bin\start.exe</li> </ul> |
| Block a specific application file name in any folder  | -   | <ol style="list-style-type: none"> <li>1. <b>Specific path</b></li> <li>2. <b>Regular expression (PCRE)</b></li> <li>3. <code>.*\\(?:i)test(?:-i)\\.*</code></li> </ol> | <p>Blocks:</p> <ul style="list-style-type: none"> <li>• C:\MyApps\test.exe</li> <li>• C:\Users\guet\AppData\Local\Temp\test.exe</li> <li>• C:\Program Files(x86)\MyApps\test.exe</li> </ul>   |

## Certificates

You can configure Application Control to specifically target applications based on the “trust” level of a certificate and that contain specific certificate attributes.

Select the type of certificate “trust” level and then specify the required certificate “Issuer” or “Subject” information.

**Note**

Application Control supports the use of the asterisk (\*) wildcard when specifying Certificate attributes, although you must use the wildcard in conjunction with other characters to limit the scope. For example, you cannot use only the wildcard character in any field.

The following table describes the different “trust” types.

| TYPE                     | DESCRIPTION   |
|--------------------------|---|
| <b>Trusted (valid)</b>   | You must have included the certificate in the trusted certificates list and the certificate must not have expired |
| <b>Trusted (expired)</b> | You must have added the certificate in the trusted certificates list but the certificate has already expired      |
| <b>Untrusted</b>         | The certificate is unknown or you did not add the certificate to the trusted certificates list                    |

**Note**



The “trust” level combinations for Allow and Block criteria differ.

## Hash Values

You can configure Application Control to match applications using SHA-1 or SHA-256 hash value formats. You can choose to manually specify hash values or import a list of generated values.

Select your **Input method** and follow the on-screen instructions.

| INPUT METHOD  | DESCRIPTION   |
|---------------|---|
| <b>Manual</b> | Allows you to manually specify up to 100 hash values (and descriptions) |

| INPUT METHOD  | DESCRIPTION  |
|---------------|--|
| <b>Import</b> | <p>Allows you to import a ZIP package containing a properly formatted hash value list in CSV format</p> <p>You can choose to use the <b>Hash Generator tool</b> or manually create the CSV file using the <b>CSV sample format</b>.</p> <hr/> <p> <b>WARNING!</b> You can only import one file into each set of criteria. If you attempt to import a new hash value list into the criteria, Application Control completely overwrites the existing values.</p> <hr/> <ul style="list-style-type: none"> <li>• <b>Hash Generator tool:</b> Download and execute the tool on a target endpoint that you have installed with all necessary applications. The tool automatically creates a valid ZIP package containing the hash values of all applications found on the endpoint.</li> <li>• <b>CSV sample format:</b> Download the sample file and follow the instructions to properly populate the hash value list. Once you have completed the list, compress the file in ZIP format before importing into the set of criteria.</li> </ul> <hr/> <p> <b>Important</b> The hash value list cannot contain a mixture of SHA-1 and SHA-256 formats. You must create separate hash value files and separate Application Control criteria for each type of hash value format.</p> <hr/> |

## Data Loss Prevention

Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data—referred to as digital assets—against accidental disclosure and intentional theft. DLP allows you to:

- Identify the digital assets to protect
- Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices

- Enforce compliance to established privacy standards

DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.



### Important

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

You can download a PDF version of the guide, or view the guide online, using the following link:

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

---

## Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- **Expressions:** Data that has a certain structure.

For details, see *Expressions on page 15-17*.

- **File attributes:** File properties such as file type and file size.

For details, see *File Attributes on page 15-21*.

- **Keyword lists:** A list of special words or phrases.

For details, see *Keywords on page 15-23*.



### Note

Administrators cannot delete a data identifier that a DLP template is using. Delete the template before deleting the data identifier.

---

## Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

Administrators can use predefined and customized expressions.

For details, see *Predefined Expressions on page 15-17* and *Customized Expressions on page 15-18*.

### Predefined 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.

For a complete list of predefined expressions, see the *Data Protection Lists* document at:

<http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>.

### Viewing Settings for Predefined Expressions

**Note**

Predefined expressions cannot be modified or deleted.

---

### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click the expression name.

#### 4. View settings in the screen that opens.

### Customized Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

<http://www.pcre.org/>

- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expressions on page 15-18*.

#### Criteria for Customized Expressions

**TABLE 15-2. Criteria Options for Customized Expressions**

| CRITERIA | RULE | EXAMPLE   |
|----------|------|---|
| None     | None | All - Names from US Census Bureau <ul style="list-style-type: none"> <li>• Expression: <code>[^\w]([A-Z][a-z]{1,12}(\s?,\s? [\s]\s([A-Z])\.\s)[A-Z][a-z]{1,12}){1,12}</code></li> </ul> |



| CRITERIA                   | RULE   | EXAMPLE   |
|----------------------------|--|---|
| Specific characters        | <p>An expression must include the characters you have specified.</p> <p>In addition, the number of characters in the expression must be within the minimum and maximum limits.</p>   | <p>US - ABA Routing Number</p> <ul style="list-style-type: none"> <li>• Expression: <code>[^d]{0123678}d{8}[^d]</code></li> <li>• Characters: 0123456789</li> <li>• Minimum characters: 9</li> <li>• Maximum characters: 9</li> </ul>   |
| Suffix                     | <p>Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters.</p> <p>In addition, the number of characters in the expression must be within the minimum and maximum limits.</p>                                       | <p>All - Home Address</p> <ul style="list-style-type: none"> <li>• Expression: <code>\D\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane ln street st avenue ave road rd place pl drive dr circle  cr  court ct boulevard blvd)\.?[0-9a-z#\s\.\]{0,30}[\s,][a-z]{2}\s\d{5}(-\d{4})?[^d-]</code></li> <li>• Suffix characters: 0123456789-</li> <li>• Number of characters: 5</li> <li>• Minimum characters in the expression: 25</li> <li>• Maximum characters in the expression: 80</li> </ul> |
| Single-character separator | <p>An expression must have two segments separated by a character. The character must be 1 byte in length.</p> <p>In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.</p> | <p>All - Email Address</p> <ul style="list-style-type: none"> <li>• Expression: <code>[^w.]{1,20}@[a-z0-9]{2,20}[\.\s][a-z]{2,5}[a-z\.\s]{0,10}[^w.]</code></li> <li>• Separator: @</li> <li>• Minimum characters to the left: 3</li> <li>• Maximum characters to the left: 15</li> <li>• Maximum characters to the right: 30</li> </ul>  |

## Creating a Customized Expression

---

### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Add**.

A new screen displays.

4. Type a name for the expression. The name must not exceed 100 bytes in length and cannot contain the following characters:

- > < \* ^ | & ? \ /

5. Type a description that does not exceed 256 bytes in length.
6. Type the displayed data.

For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.

7. Choose one of the following criteria and configure additional settings for the chosen criteria (see [Criteria for Customized Expressions on page 15-18](#)):
  - None
  - Specific characters
  - Suffix
  - Single-character separator

8. Test the expression against an actual data.

For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.

9. Click **Save** if you are satisfied with the result.

**Note**

Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

---

### Importing Customized Expressions

Use this option if you have a properly-formatted .dat file containing the expressions. You can generate the file by exporting the expressions from either the server you are currently accessing or from another server.

---

### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Import** and then locate the .dat file containing the expressions.
4. Click **Open**.

A message appears, informing you if the import was successful. If an expression to be imported already exists, it will be skipped.

---

### File Attributes

File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For example, a software development company may want to limit the sharing of the company's software installer to the R&D department, whose members are responsible for the development and testing of the software. In this case, the Apex Central administrator can create a policy that blocks the transmission of executable files that are 10 to 40 MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types, see the *Data Protection Lists* document at:

<http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>.

## Creating a File Attribute List

---

### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.

2. Click the **File Attribute** tab.

3. Click **Add**.

A new screen displays.

4. Type a name for the file attribute list. The name must not exceed 100 bytes in length and cannot contain the following characters:

- > \* ^ | & ? \ /

5. Type a description that does not exceed 256 bytes in length.

6. Select your preferred true file types.

7. If a file type you want to include is not listed, select **File extensions** and then type the file type's extension. Data Loss Prevention checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:

- Each extension must start with an asterisk (\*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, \*.pol matches 12345.pol and test.pol.
- You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (\*) to represent two or more characters. See the following examples:
  - \*.\*m matches the following files: ABC.dem, ABC.prm, ABC.sdc

- \*.m\*r matches the following files: ABC.mgdr, ABC.mtp2r, ABC.mdmr
  - \*.fm? matches the following files: ABC.fme, ABC.fml, ABC.fmp
  - Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: \*.do\* matches abc.doctor\_john.jpg and abc.donor12.pdf.
  - Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.
8. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.
  9. Click **Save**.
- 

### Importing a File Attribute List

Use this option if you have a properly-formatted .dat file containing the file attribute lists. You can generate the file by exporting the file attribute lists from either the server you are currently accessing or from another server.

---

#### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Import** and then locate the .dat file containing the file attribute lists.
4. Click **Open**.

A message appears, informing you if the import was successful. If a file attribute list to be imported already exists, it will be skipped.

---

### Keywords

Keywords are 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 DLP policy and then configure Data Loss Prevention to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see [Predefined Keyword Lists on page 15-24](#) and [Customized Keyword Lists on page 15-25](#).

## Predefined Keyword Lists

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.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at:

<http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>

## How Keyword Lists Work

### Number of Keywords Condition

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:** All of the keywords in the list must be present in the document.
- **Any:** Any one of the keywords in the list must be present in the document.
- **Specific number:** There must be at least the specified number of keywords in the document. If there are more keywords in the document than the number specified, Data Loss Prevention triggers a violation.

### Distance Condition

Some of the lists contain a “distance” condition 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. Consider the following entry:

**First Name:**\_John\_ **Last Name:**\_Smith\_

The **Forms - First Name, Last Name** list has a “distance” condition of fifty (50) and the commonly used form fields of “First Name” and “Last Name”. In the example above, Data Loss Prevention triggers a violation as the number of characters between the “F” in First Name and the “L” in Last Name is equal to eighteen (18).

For an example of an entry that does not trigger a violation, consider the following:

The **first name of our new employee from Switzerland is John. His last name is Smith.**

In this example, the number of characters between the “f” in “first name” and the “l” in “last name” is sixty-one (61). This exceeds the distance threshold and does not trigger a violation.

### Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meets your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before Data Loss Prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see [Customized Keyword List Criteria on page 15-26](#).

### Customized Keyword List Criteria

**TABLE 15-3. Criteria for a Keyword List**

| CRITERIA                           | RULE   |
|------------------------------------|--|
| Any keyword                        | A file must contain at least one keyword in the keyword list.  |
| All keywords                       | A file must contain all the keywords in the keyword list.  |
| All keywords within <x> characters | <p>A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within &lt;x&gt; characters of each other.</p> <p>For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20.</p> <p>If Data Loss Prevention detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less.</p> <p>The following data matches the criteria: DISK####WEB#####USB</p> <p>The following data does not match the criteria:<br/>DISK*****WEB****USB(23 characters between "D" and "W")</p> <p>When deciding on the number of characters, remember that a small number, such as 10, usually results in a faster scanning time but only covers a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.</p> |



| CRITERIA                                      | RULE  |
|---|---|
| Combined score for keywords exceeds threshold | <p>A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold.</p> <p>Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores.</p> <p>Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.</p> |

### Creating a Keyword List

#### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Add**.  
A new screen displays.
4. Type a name for the keyword list. The name must not exceed 100 bytes in length and cannot contain the following characters:
  - > < \* ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:
  - **Any keyword**
  - **All keywords**
  - **All keywords within <x> characters**

- **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:
  - a. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.
  - b. Click **Add**.
8. To add keywords by using the "import" option:



**Note**

Use this option if you have a properly-formatted .csv file containing the keywords. You can generate the file by exporting the keywords from either the server you are currently accessing or from another server.

---

- a. Click **Import** and then locate the .csv file containing the keywords.
- b. Click **Open**.

A message appears, informing you if the import was successful. If a keyword to be imported already exists in the list, it will be skipped.

9. To delete keywords, select the keywords and click **Delete**.
10. To export keywords:



**Note**

Use the "export" feature to back up the keywords or to import them to another server. All keywords in the keyword list will be exported. It is not possible to export individual keywords.

---

- a. Click **Export**.
- b. Save the resulting .csv file to your preferred location.

11. Click **Save**.
-

---

### Importing a Keyword List

Use this option if you have a properly-formatted .dat file containing the keyword lists. You can generate the file by exporting the keyword lists from either the server you are currently accessing or from another server.

---

#### Procedure

1. Go to **Policies > Policy Resources > DLP Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Import** and then locate the .dat file containing the keyword lists.
4. Click **Open**.

A message appears, informing you if the import was successful. If a keyword list to be imported already exists, it will be skipped.

---

## Data Loss Prevention Templates

A DLP template combines DLP 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 DLP 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.

You can create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see [Customized DLP Templates on page 15-30](#) and [Predefined DLP Templates on page 15-30](#).

---



#### Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

---

## Predefined DLP Templates

Data Loss Prevention comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA:** Gramm-Leach-Bliley 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

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at:

<http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx>

## Customized DLP Templates

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.

For more information and examples on how condition statements and logical operators work, see *Condition Statements and Logical Operators on page 15-30*.

### Condition Statements and Logical Operators

Data Loss Prevention evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

**TABLE 15-4. Sample Condition Statements**

| CONDITION STATEMENT  | INTERPRETATION AND EXAMPLE  |
|--|---|
| [Data Identifier 1] <b>And</b> [Data Identifier 2] <b>Except</b> [Data Identifier 3] | <p>A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3].</p> <p>For example:</p> <p>A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].</p> |
| [Data Identifier 1] <b>Or</b> [Data Identifier 2]                                    | <p>A file must satisfy [Data Identifier 1] or [Data Identifier 2].</p> <p>For example:</p> <p>A file must be [an Adobe PDF document] or [a Microsoft Word document].</p>  |
| <b>Except</b> [Data Identifier 1]  | <p>A file must not satisfy [Data Identifier 1].</p> <p>For example:</p> <p>A file must not be [a multimedia file].</p>  |

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

## Creating a Template

### Procedure

1. Go to **Policies > Policy Resources > DLP Templates**.

2. Click **Add**.

A new screen displays.

3. Type a name for the template. The name must not exceed 100 bytes in length and cannot contain the following characters:

• > \* ^ | & ? \ /

4. Type a description that does not exceed 256 bytes in length.
5. Select data identifiers and then click the "add" icon.

When selecting definitions:

- Select multiple entries by pressing and holding the CTRL key and then selecting the data identifiers.
  - Use the search feature if you have a specific definition in mind. You can type the full or partial name of the data identifier.
  - Each template can contain a maximum of 30 data identifiers.
6. To create a new expression, click **Expressions** and then click **Add new expression**. In the screen that appears, configure settings for the expression.
  7. To create a new file attribute list, click **File attributes** and then click **Add new file attribute**. In the screen that appears, configure settings for the file attribute list.
  8. To create a new keyword list, click **Keywords** and then click **Add new keyword**. In the screen that appears, configure settings for the keyword list.
  9. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before Data Loss Prevention subjects it to a policy.
  10. Choose a logical operator for each definition.

**Note**

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see [Condition Statements and Logical Operators on page 15-30](#).

---

11. To remove a data identifier from the list of selected identifiers, click the trash bin icon.

12. Below **Preview**, check the condition statement and make changes if this is not your intended statement.
  13. Click **Save**.
- 

### Importing Templates

Use this option if you have a properly-formatted .dat file containing the templates. You can generate the file by exporting the templates from either the server you are currently accessing or from another server.

---

#### Procedure

1. Go to **Policies > Policy Resources > DLP Templates**.
2. Click **Import** and then locate the .dat file containing the templates.
3. Click **Open**.

A message appears, informing you if the import was successful. If a template to be imported already exists, it will be skipped.

---

## Intrusion Prevention Rules

The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

- To filter the list of rules, use the **Search** box to specify full or partial strings that appear in any of the columns.
- To sort the list of Intrusion Prevention Rules by column data, click a column heading.
- To view detailed Intrusion Prevention Rule Properties, click the link in the **Rule Name** column of a rule.

- To exclude traffic from one or more source endpoints from Vulnerability Protection scanning, click **Configure Exceptions** and specify the source IP addresses.

**Note**

You can add up to 100 entries to the exception list.

---

**Note**

Apex Central automatically imports/updates Intrusion Prevention Rules from the Apex One server during manual or scheduled component updates.

---

**Important**

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

You can download a PDF version of the guide, or view the guide online, using the following link:


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

---

The following table outlines the rule information that displays on the **Intrusion Prevention Rules** screen.

| COLUMN           | DESCRIPTION  |
|------------------|--|
| Identifier       | The unique identifier tag for the Intrusion Prevention Rule          |
| Rule Name        | The name of the Intrusion Prevention Rule                            |
| Application Type | The Application Type this Intrusion Prevention Rule is grouped under |





| COLUMN       | DESCRIPTION  |
|--------------|--|
| Severity     | <p>The severity level that Trend Micro assigns to the rule</p> <hr/>  <b>Note</b><br>The severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Intrusion Prevention Rules.     |
| Mode         | The network engine detection mode used by the Intrusion Prevention module. Click a mode to configure the setting for the rule.   |
| Type         | <p>The type of vulnerability detected:</p> <ul style="list-style-type: none"> <li>• <b>Smart:</b> Known or unknown (for example, zero-day) vulnerability</li> <li>• <b>Exploit:</b> Known exploit (usually signature based) for a known vulnerability</li> <li>• <b>Vulnerability:</b> Known vulnerability for which one or more exploits may exist</li> </ul> |
| CVE          | <p>The Common Vulnerabilities and Exposures (CVE®) identifier that MITRE assigns to the vulnerability</p> <p>For more information, see <a href="http://cve.mitre.org/">http://cve.mitre.org/</a>.</p>  |
| Microsoft    | The Common Vulnerabilities and Exposures (CVE®) identifier that Microsoft assigns to the vulnerability   |
| CVSS Score   | <p>The Common Vulnerability Scoring System (CVSS) severity score of the vulnerability according the National Vulnerability Database</p> <p>For more information, see <a href="http://nvd.nist.gov/cvss.cfm">http://nvd.nist.gov/cvss.cfm</a>.</p>  |
| Last Updated | The date and time the rule was last modified   |

## Intrusion Prevention Rule Properties

The **Intrusion Prevention Rule Properties** screen displays detailed information about a specific Intrusion Prevention Rule and vulnerability. Click the **General** tab or the **Vulnerability** to view details about the rule.

The following tables describe the information provided on the **General** tab and **Vulnerability** tab.

**TABLE 15-5. General Information**

| DATA             | DESCRIPTION  |
|------------------|--|
| Identifier       | The unique identifier tag for the Intrusion Prevention Rule  |
| Name             | The name of the Intrusion Prevention Rule  |
| Description      | <p>The description of the Intrusion Prevention Rule</p> <hr/> <p> <b>Note</b><br/>Apex One Vulnerability Protection does not support the configuration options available on the standalone version of Trend Micro Vulnerability Protection.</p> <hr/>                                   |
| Application Type | The Application Type this Intrusion Prevention Rule is grouped under   |
| Priority         | The priority level of the Intrusion Prevention Rule. Higher priority rules are applied before lower priority rules.  |
| Severity         | <p>The severity level that Trend Micro assigns to the rule</p> <hr/> <p> <b>Note</b><br/>The severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Intrusion Prevention Rules.</p> <hr/> |
| Mode             | The network engine detection mode used by the Intrusion Prevention module. Click a mode to configure the setting for the rule.   |

| DATA         | DESCRIPTION   |
|--------------|---|
| Type         | The type of vulnerability detected: <ul style="list-style-type: none"> <li>• <b>Smart:</b> Known or unknown (for example, zero-day) vulnerability</li> <li>• <b>Exploit:</b> Known exploit (usually signature based) for a known vulnerability</li> <li>• <b>Vulnerability:</b> Known vulnerability for which one or more exploits may exist</li> </ul> |
| Issued       | The date the rule was released (not downloaded)   |
| Last Updated | The date and time the rule was last modified  |

**TABLE 15-6. Vulnerability Information**


| DATA                | DESCRIPTION   |
|---------------------|---|
| Severity            | The severity level of the vulnerability   |
| CVSS Score          | The Common Vulnerability Scoring System (CVSS) severity score of the vulnerability according the National Vulnerability Database<br>For more information, see <a href="http://nvd.nist.gov/cvss.cfm">http://nvd.nist.gov/cvss.cfm</a> . |
| Description         | The description of the vulnerability  |
| External References | Provides links to external references for more information about the vulnerability  |

## Device Control Allowed Devices

Import or export lists of **Device Control Allow Devices** that apply to all Apex One Security Agent policy targets.

**Note**

- Only Security Agents with Data Protection enabled override the “Block” or “Read” action on devices added to the Device Control Allowed Devices list.
- The Device Control Allowed Devices list does not apply to Security Agents without Data Protection and Security Agents with Device Control permission not set to “Block” or “Read”.

| ITEM                  | DESCRIPTION  |
|-----------------------|--|
| Import                | <p>Select a properly formatted CSV file containing a list of all the devices you want to allow on all Apex One Security Agent endpoints.</p> <hr/> <p> <b>Important</b> Importing a new list overwrites the previous list completely. To retain the existing list, export the list before importing a new CSV file.</p> <hr/> |
| Last imported         | The date/time the server imported the current list   |
| Total allowed devices | The total number of allowed devices in the currently applied list  |
| Export                | Exports the current allowed list in CSV format   |

# Part V

## Detections





# Chapter 16

## Logs

This chapter describes how to access Apex Central generated logs and logs from managed products registered to Apex Central.

Topics include:

- *Log Queries on page 16-2*
- *Querying Logs on page 16-2*
- *Configuring Log Aggregation on page 16-14*
- *Configuring Syslog Forwarding on page 16-14*
- *Deleting Logs on page 16-20*

## Log Queries

Apex Central allows you to query the Apex Central database for Apex Central generated logs and log data from registered managed products.

Apex Central also allows you to:

- Use advanced filters to narrow log query search results.
- Configure log aggregation settings to reduce network traffic when sending log data from managed products to the Apex Central server.
- Manually delete log entries by type or configure automatic log deletion.

## Querying Logs

Use the **Log Query** screen to query Apex Central generated logs and log data from registered managed products. You can also narrow the search results by using advanced custom filters, export the search results in XML or CSV format, or save and share the log query search criteria with other Apex Central administrators.

**Note**

Apex Central also allows you to perform a log query from the **Product Directory** screen.

For details, see [Querying Logs from the Product Directory on page 11-10](#).

---

### Procedure

1. Go to **Detections > Logs > Log Query**.

The **Log Query** screen appears.

2. Specify the log type.



**Note**

Log types correspond to specific data views used in Apex Central reports.

For more information about log types and data views, see [Log Names and Data Views on page 16-6](#).

---

- a. Select a log type from the first drop-down control.
  - b. Click **OK** to apply the selected log type.
3. To filter your search results to data from specific managed products:
- a. Click the second drop-down control.
  - b. Select targets for the query by using one of the following options:
    - **Directory:** Allows you to locate and select managed products from the Product Directory structure
    - **Type:** Allows you to choose a product type and select from a list of all registered managed products of the same type
    - **Tags and filters:** Allows you to select custom tags, filters, or important labels from the User/Endpoint Directory to query specific endpoints
- 

**Note**

- You can select up to 10 custom tags, filters, or important labels to perform a log query.
  - Custom filters that contain Compliance, Important, Threat Type, Security Threat, or Threat Status Criteria information cannot be used to perform a log query.
- 

- c. Click **OK** to apply the selected targets.
4. Select a time period from the **Time** drop-down control.
5. To filter search results using custom criteria:

- a. Click **Show advanced filters**.
  - b. Specify the **Match** rule for the custom filter:
    - **All of the criteria:** Data must match all the specified criteria
    - **Any of the criteria:** Data can match any of the specified criteria
  - c. In the **Select criteria...** drop-down list, select a data column to filter.
- 



**Note**

The data columns in the **Select criteria...** drop-down list dynamically change based on the log type you select in the first drop-down control.

For more information about the data columns, see [Log Names and Data Views on page 16-6](#) and refer to the corresponding data view details.

---

The filtering criteria that appear in the second and third drop-down lists dynamically change based on the data column you select.

- d. In the second drop-down list, select an operator.
  - e. In the third drop-down list, define the criteria.
- 



**Note**

Apex Central supports up to 20 custom filtering criteria for each log query.

---

**6. Click Search.**

The search results appear in the table on the **Log Query** screen.

**Note**


- The **Generated** column displays the local date and time on the endpoint for when the managed product first detected the threat.
  - The **Received** column displays the local date and time on the Apex Central server for when the Apex Central server received the data from the managed product server.
- 


7. (Optional) Click a link in a data column to drill down for more information.
8. (Optional) Customize the data columns in the search results.
  - Click **Customize Columns** to add or remove columns that display in the table.
  - Rearrange the order in which the columns display by dragging the column headings.
9. (Optional) Export the log query results.
  - a. Click **Export to CSV** or **Export to XML**.  
The **Log Query Exporting page** screen appears.
  - b. After the export completes, open or save the file.
10. (Optional) Save log query search criteria.


**Note**




- Saving a log query only saves the search criteria for the query. To save log query search results, export the results or create a report using a grid table.

For more information about creating reports, see [Reports on page 18-1](#).

- Saved queries are automatically visible to all users from the same Active Directory group.
- A gray user icon (  ) next to a saved query indicates a log query shared by a user from outside your Active Directory group. Hover over the icon to view the name of the user who shared the query.

- 
- a. Click the save button (  ).
  - b. Specify a name for the saved query.
  - c. Click **Save**.

After saving a log query, you can click the saved queries button (  ) to view a list of saved queries and perform the following actions.

- Click the name of a saved query to run the log query.
- Click the share icon (  ) next to a saved query name to share the log query with all Apex Central users.
- Click the stop sharing icon (  ) next to a saved query name to stop sharing the log query with all Apex Central users.
- Click the delete icon (  ) to remove the saved query.

---

## Log Names and Data Views

Apex Central log types correspond to specific data views for custom report templates. You can use the following data views to create custom report templates for your log query results.

For more information, see the following topics:

- [Custom Templates on page 18-2](#)
- [Data Views on page B-1](#)

**TABLE 16-1. Security Logs**

| LOG NAME              | DATA VIEW                                      | DESCRIPTION  |
|-----------------------|--|--|
| <b>System Events:</b> |  |  |
| Virus/Malware         | Detailed Virus/<br>Malware Information         | Provides specific information about the virus/<br>malware detections on your network, such as<br>the managed product that detected the<br>viruses/malware, the name of the virus/<br>malware, and the infected endpoint<br><br>For more information, see <a href="#">Detailed Virus/<br/>Malware Information on page B-72</a> .                        |
| Spyware/Grayware      | Detailed Spyware/<br>Grayware<br>Information   | Provides specific information about the<br>spyware/grayware detections on your<br>network, such as the managed product that<br>detected the spyware/grayware, the name of<br>the spyware/grayware, and the name of the<br>infected endpoint<br><br>For more information, see <a href="#">Detailed Spyware/<br/>Grayware Information on page B-59</a> . |
| Suspicious Files      | Detailed Suspicious<br>File Information        | Provides specific information about<br>suspicious files detected on your network<br><br>For more information, see <a href="#">Detailed Suspicious<br/>File Information on page B-5</a> .   |
| Behavior Monitoring   | Detailed Behavior<br>Monitoring<br>Information | Provides specific information about Behavior<br>Monitoring events on your network<br><br>For more information, see <a href="#">Detailed Behavior<br/>Monitoring Information on page B-48</a> .   |

| LOG NAME                     | DATA VIEW  | DESCRIPTION   |
|------------------------------|--|---|
| Integrity Monitoring         | Integrity Monitoring Information                   | <p>Use to monitor specific changes to an endpoint, such as installed software, running services, processes, files, directories, listening ports, registry keys, and registry values</p> <p>For more information, see <a href="#">Integrity Monitoring Information on page B-54</a>.</p> |
| Application Control          | Detailed Application Control Violation Information | <p>Provides specific information about application control violations on your network, such as the violated Security Agent policy and criteria</p> <p>For more information, see <a href="#">Detailed Application Control Violation Information on page B-46</a>.</p>                    |
| Device Control               | Device Access Control Information                  | <p>Provides specific information about Device Access Control events on your network</p> <p>For more information, see <a href="#">Device Access Control Information on page B-43</a>.</p>  |
| Endpoint Security Compliance | Detailed Endpoint Security Compliance Information  | <p>Provides specific information about endpoint security compliance on your network</p> <p>For more information, see <a href="#">Detailed Endpoint Security Compliance Information on page B-49</a>.</p>  |
| Endpoint Security Violations | Detailed Endpoint Security Violation Information   | <p>Provides specific information about endpoint security violations on your network</p> <p>For more information, see <a href="#">Detailed Endpoint Security Violation Information on page B-50</a>.</p>   |
| Predictive Machine Learning  | Detailed Predictive Machine Learning Information   | <p>Provides specific information about advanced unknown threats detected by Predictive Machine Learning</p> <p>For more information, see <a href="#">Detailed Predictive Machine Learning Information on page B-3</a>.</p>  |

| LOG NAME                            | DATA VIEW  | DESCRIPTION   |
|-------------------------------------|--|---|
| Virtual Analyzer                    | Detailed Virtual Analyzer Detection Information                | Provides specific information about advanced unknown threats detected by Virtual Analyzer<br><br>For more information, see <a href="#">Virtual Analyzer Detection Information on page B-6</a> .   |
| Virtual Analyzer Suspicious Objects | Detailed Virtual Analyzer Suspicious Object Impact Information | Provides detailed information about the impact of Virtual Analyzer suspicious objects<br><br>For more information, see <a href="#">Detailed Virtual Analyzer Suspicious Object Impact Information on page B-7</a> .   |
| Attack Discovery                    | Attack Discovery Detection Information                         | Provides general information about threats detected by Attack Discovery<br><br>For more information, see <a href="#">Attack Discovery Detection Information on page B-10</a> .  |
| Gray Detections                     | Gray Detection Information                                     | Provides detailed information about possible indicators of attack detected on your network<br><br>For more information, see <a href="#">Gray Detection Information on page B-38</a> .   |
| <b>Network Events:</b>              |  |   |
| Spam Connections                    | Spam Connection Information                                    | Provides specific information about the source of spam on your network, such as the managed product that detected the spam, the specific action taken by the managed product, and the total number of spam detected<br><br>For more information, see <a href="#">Spam Connection Information on page B-57</a> . |

| LOG NAME                             | DATA VIEW                               | DESCRIPTION   |
|--------------------------------------|---|---|
| Content Violations                   | Detailed Content Violation Information  | <p>Provides specific information about the email messages with content violations, such as the managed product that detected the content violation, the sender(s) and recipients(s) of the email message, the name of the content violation policy, and the total number of violations detected</p> <p>For more information, see <a href="#">Detailed Content Violation Information on page B-17</a>.</p> |
| Email Messages with Advanced Threats | Email Messages with Advanced Threats    | <p>Provides specific information about email messages with advanced threats, such as anomalous behavior, false or misleading data, suspicious and malicious behavior patterns, and strings that indicate system compromise but require further investigation to confirm</p> <p>For more information, see <a href="#">Email Messages with Advanced Threats on page B-18</a>.</p>                           |
| Web Reputation                       | Detailed Web Reputation Information     | <p>Provides compliance information about application activity detected by Web Reputation Services</p> <p>For more information, see <a href="#">Detailed Web Reputation Information on page B-84</a>.</p>  |
| Web Violations                       | Detailed Web Violation Information      | <p>Provides specific information about web violations on your network</p> <p>For more information, see <a href="#">Detailed Web Violation Information on page B-86</a>.</p>   |
| Firewall Violations                  | Detailed Firewall Violation Information | <p>Provides specific information about firewall violations on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations</p> <p>For more information, see <a href="#">Detailed Firewall Violation Information on page B-51</a>.</p>   |



| LOG NAME                   | DATA VIEW                                 | DESCRIPTION  |
|----------------------------|---|--|
| Network Content Inspection | Network Content Inspection Information    | <p>Provides specific information about network content violations on your network</p> <p>For more information, see <a href="#">Network Content Inspection Information on page B-54</a>.</p>  |
| Intrusion Prevention       | Detailed Intrusion Prevention Information | <p>Provides specific information to help you achieve timely protection against known and zero-day attacks, defend against web application vulnerabilities, and identify malicious software accessing the network</p> <p>For more information, see <a href="#">Detailed Intrusion Prevention Information on page B-52</a>.</p>  |
| C&C Callbacks              | Detailed C&C Callback Information         | <p>Provides specific information about C&amp;C callback events detected on your network</p> <p>For more information, see <a href="#">Detailed C&amp;C Callback Information on page B-2</a>.</p>  |
| Suspicious Threats         | Detailed Suspicious Threat Information    | <p>Provides specific information about suspicious threats on your network, such as the managed product that detected the suspicious threat, specific information about the source and destination, and the total number of suspicious threats on the network</p> <p>For more information, see <a href="#">Detailed Suspicious Threat Information on page B-26</a>.</p> |
| Application Activity       | Detailed Application Activity             | <p>Displays specific information about application activities that violate network security policies</p> <p>For more information, see <a href="#">Detailed Application Activity on page B-44</a>.</p>  |
| Mitigation                 | Detailed Mitigation Information           | <p>Provides specific information about tasks carried out by mitigation servers to resolve threats on your network</p> <p>For more information, see <a href="#">Detailed Mitigation Information on page B-25</a>.</p>   |

| LOG NAME                       | DATA VIEW   | DESCRIPTION  |
|--------------------------------|---|--|
| Correlation                    | Detailed Correlation Information                          | Provides specific information about detailed threat analyses and remediation recommendations<br><br>For more information, see <a href="#">Detailed Correlation Information on page B-24</a> .      |
| <b>Data Protection Events:</b> |   |  |
| Data Loss Prevention           | DLP Incident Information                                  | Provides specific information about incidents detected by Data Loss Prevention<br><br>For more information, see <a href="#">DLP Incident Information on page B-21</a> .                            |
| Data Discovery                 | Data Discovery Data Loss Prevention Detection Information | Displays specific information about incidents detected by Data Discovery<br><br>For more information, see <a href="#">Data Discovery Data Loss Prevention Detection Information on page B-20</a> . |

**TABLE 16-2. Product Information**

| LOG NAME                | DATA VIEW                  | DESCRIPTION   |
|-------------------------|----------------------------|---|
| <b>Managed Product:</b> |                            |   |
| Product Status          | Product Status Information | Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system<br><br>For more information, see <a href="#">Product Status Information on page B-109</a> . |
| Product Events          | Product Event Information  | Provides information about managed product events, such as managed products registering to Apex Central, component updates, and Activation Code deployments<br><br>For more information, see <a href="#">Product Event Information on page B-108</a> .  |

| LOG NAME                | DATA VIEW                      | DESCRIPTION   |
|-------------------------|--------------------------------|---|
| Product Auditing Events | Product Auditing Event Log     | <p>Provides information about managed product auditing events, such as managed product console access</p> <p>For more information, see <a href="#">Product Auditing Event Log on page B-106</a>.</p>  |
| <b>Apex Central:</b>    |                                |   |
| Command Tracking        | Command Tracking Information   | <p>Provides information about commands Apex Central issued to managed products, such as the date and time Apex Central issued commands for component updates or Activation Code deployments, and the status of the commands</p> <p>For more information, see <a href="#">Command Tracking Information on page B-94</a>.</p> |
| Apex Central Events     | Apex Central Event Information | <p>Provides information about Apex Central server events, such as managed products registering to Apex Central, component updates, and Activation Code deployments</p> <p>For more information, see <a href="#">Apex Central Event Information on page B-94</a>.</p>  |
| Unmanaged Endpoints     | Unmanaged Endpoints            | <p>Provides information about detected endpoints that do not have a Trend Micro Security Agent installed</p> <p>For more information, see <a href="#">Unmanaged Endpoint Information on page B-95</a>.</p>  |
| User Access             | User Access Information        | <p>Provides information about Apex Central user access and the activities users perform while logged on to Apex Central</p> <p>For more information, see <a href="#">User Access Information on page B-96</a>.</p>  |

| LOG NAME         | DATA VIEW                            | DESCRIPTION   |
|------------------|--------------------------------------|---|
| Product Licenses | Detailed Product License Information | Provides information about the Activation Codes and licensing status of managed products or services, such as the managed product version and license expiration date<br><br>For more information, see <a href="#">Detailed Product License Information on page B-104</a> . |

## Configuring Log Aggregation

Log aggregation allows you to conserve network bandwidth by sending only selected data from managed products to the Apex Central server.



### WARNING!

Apex Central cannot recover data that managed products do not send to the Apex Central server.

### Procedure

1. Go to **Detections > Logs > Log Aggregation Settings**.  
The **Edit Log Aggregation Rule** screen appears.
2. Select **Enable log aggregation**.
3. Expand log categories.
4. Clear check boxes to stop sending data from managed products to Apex Central.
5. Click **Save**.

## Configuring Syslog Forwarding

Use the **Syslog Settings** screen to configure Apex Central to forward supported logs to a syslog server.

For more information, see the following topics:

- [Disabling Syslog Forwarding on page 16-18](#)
- [Supported Log Types and Formats on page 16-18](#)

**Note**

- If you migrated to Apex Central from a previous Control Manager installation, Apex Central automatically imports your previous syslog forwarding settings configured using the LogForwarder tool (<Control Manager installation directory>\LogForwarder.exe).
- After migrating to Apex Central, you will no longer be able to execute the LogForwarder tool.

---

**Procedure**

1. Go to **Administration > Settings > Syslog Settings**.

The **Syslog Settings** screen appears.

2. Select the **Enable syslog forwarding** check box.
3. Configure the following settings for the server that receives the forwarded syslogs:
  - **Server address:** Syslog server IP address or FQDN
  - **Port:** Syslog server port number
  - **Protocol:** Select the transmission protocol

**Note**

If **SSL/TLS** is selected, Apex Central accepts valid self-signed certificates by default.

- If the server certificate contains a Subject Alternative Name, the Subject Alternative Name must contain the server FQDN or IP address.
  - For additional security, use a valid server certificate or upload the server certificate to Apex Central.
-

#### 4. (Optional) To upload a server certificate:



##### **Important**

- Apex Central only supports server certificates in X.509 format with .DER or .PEM encoding.

For more information, see <https://support.ssl.com/Knowledgebase/Article/View/19/0/der-vs-crt-vs-cer-vs-pem-certificates-and-how-to-convert-them>.

- Apex Central only supports uploading server certificates for SSL/TLS transmissions.
- 

- a. Select the **Use server certificate** check box.
- b. Click **Select** to select the server certificate from your computer.
- c. Click **Open**.

Apex Central uploads the selected server certificate.

#### 5. (Optional) To use a proxy server for syslog forwarding, select the **Use a SOCKS proxy server** check box.

---



##### **Important**

- Apex Central only supports syslog forwarding over a SOCKS protocol proxy server for SSL/TLS or TCP transmissions.
- Syslog forwarding does not support HTTP proxy servers. To use a proxy server for syslog forwarding, click **Configure proxy settings** and select a SOCKS protocol server on the **Proxy Settings** screen.

For more information, see *Configuring Proxy Settings for Component/License Updates, Cloud Services, and Syslog Forwarding on page 12-12*.

---

Apex Central uses the proxy server configured on the **Proxy Settings** screen (**Administration** > **Settings** > **Proxy Settings**) for syslog forwarding.

6. Select the log format:
  - **CEF:** Uses the standard Common Event Format (CEF) for log messages
  - **Apex Central format:** Sets the syslog **Facility** code to "Local0" and the **Severity** code to "Notice"

For more information, see [Supported Log Types and Formats on page 16-18](#).

7. Configure the frequency for when Apex Central forwards the logs.
8. Select the log type(s) to forward:
  - a. Select a log category from the **Log type** drop-down list:

**Note**

You can select log types from multiple log categories.

---

- **Security logs**
  - **Product information**
- b. Select the check box(es) for the log(s) you want to forward.

Apex Central displays the total number of selected log types next to the **Log type** drop-down list.
    - c. (Optional) Select another log category from **Log type** drop-down list to select additional logs types to forward.
  9. (Optional) Click **Test Connection** to test the server connection.

**Note**

Testing the connection does not save the syslog server settings.

---

The syslog server connection status appears at the top of the screen.

10. Click **Save**.

- Apex Central starts forwarding logs to the configured syslog server.
- To monitor the log forwarding status, go to **Administration** > **Command Tracking** and select **Forward Syslog** from the **Command** drop-down list.

For more information, see [Querying and Viewing Commands on page 13-3](#).

---

## Disabling Syslog Forwarding

Use the **Syslog Settings** screen to stop forwarding logs from Apex Central to a syslog server.

---

### Procedure

1. Go to **Administration** > **Settings** > **Syslog Settings**.

The **Syslog Settings** screen appears.

2. Clear the **Enable syslog forwarding** check box.
3. Click **Save**.

Apex Central stops forwarding logs to the configured syslog server.

---

## Supported Log Types and Formats

Apex Central can forward logs to a syslog server in the following log formats:

- **CEF**: Uses the standard Common Event Format (CEF) for log messages
- **Apex Central format**: Sets the syslog **Facility** code to "Local0" and the **Severity** code to "Notice"

The following tables outline the formats supported by each log type.



**TABLE 16-3. Security Logs**

| LOG TYPE                    | CEF | APEX CENTRAL FORMAT |
|-----------------------------|-----|---------------------|
| Application Control         | Yes | No                  |
| Attack Discovery            | Yes | No                  |
| Behavior Monitoring         | Yes | Yes                 |
| C&C Callbacks               | Yes | No                  |
| Content Violations          | Yes | No                  |
| Data Loss Prevention        | Yes | Yes                 |
| Device Control              | Yes | Yes                 |
| Intrusion Prevention        | Yes | No                  |
| Network Content Inspection  | Yes | No                  |
| Predictive Machine Learning | Yes | No                  |
| Spyware/Grayware            | Yes | No                  |
| Suspicious Files            | Yes | No                  |
| Virtual Analyzer            | Yes | No                  |
| Virus/Malware               | Yes | No                  |
| Web Violations              | Yes | No                  |

**TABLE 16-4. Product Information**

| LOG TYPE                            | CEF | APEX CENTRAL FORMAT |
|-------------------------------------|-----|---------------------|
| Engine Update Status                | Yes | Yes                 |
| Managed Product Logon/Logoff Events | Yes | Yes                 |
| Product Auditing Events             | Yes | No                  |
| Pattern Update Status               | Yes | Yes                 |

For information about mapping syslog content between CEF and Apex Central formats, see [Syslog Content Mapping - CEF on page F-1](#).

## Deleting Logs

Use the **Log Maintenance** screen to manually delete log entries by type or configure automatic log deletion.



### **WARNING!**

Manually deleting log data may affect report generation.

---



### **Tip**

Trend Micro recommends backing up Data Loss Prevention logs to your Security Information and Event Management (SIEM) server and keeping the logs for at least 2 years.

---

## **Procedure**

1. Go to **Detections > Logs > Log Maintenance**.

The **Log Maintenance** screen appears.

2. To delete logs manually:
  - a. Select the check box for the log type.
  - b. Click **Delete All** in the corresponding row for the type of log entries you want to delete.

A confirmation message appears.
  - c. Click **OK** to delete all logs for the selected type.
3. To configure automatic log deletion:
  - a. Select the check box for the log type.
  - b. In the **Maximum Log Entries** column, specify the maximum number of logs that Apex Central retains.

**Note**

By default, Apex Central retains a maximum of 1,000,000 log entries.

---

- c. In the **Purge Offset** column, specify the number of logs that Apex Central deletes when the number of logs reaches the number specified in the **Maximum Log Entries** column.
- 

**Note**

By default, the purge offset value is 1,000 log entries.

---

- d. In the **Maximum Log Age** column, specify the age of logs that Apex Central deletes automatically.
- 

**Note**

By default, the maximum log age is 90 days.

---

- e. Click **Save**.
-



# Chapter 17

## Notifications

This section discusses how to send notifications about events that occur on the Apex Central network.

Topics include:

- *Event Notifications on page 17-2*
- *Notification Method Settings on page 17-3*
- *Contact Groups on page 17-6*
- *Advanced Threat Activity Events on page 17-9*
- *Content Policy Violation Events on page 17-30*
- *Data Loss Prevention Events on page 17-33*
- *Known Threat Activity Events on page 17-42*
- *Network Access Control Events on page 17-56*
- *Unusual Product Behavior Events on page 17-60*
- *Updates on page 17-66*

## Event Notifications

Apex Central can notify individuals or groups of recipients about events detected by managed products. Supported notification methods include email messages, Windows system log notifications, SMNP traps, syslog messages, and trigger applications.

For more information, see [Notification Method Settings on page 17-3](#)

Use the **Event Notifications** screen to enable or disable notifications about events from the following categories.

| EVENT CATEGORY           | DESCRIPTION   |
|--------------------------|---|
| Advanced Threat Activity | Provides warnings about advanced and unknown threats<br><br>For more information, see <a href="#">Advanced Threat Activity Events on page 17-9</a> .                                  |
| Content Policy Violation | Provides warnings about email content and URL security policy violations<br><br>For more information, see <a href="#">Content Policy Violation Events on page 17-30</a> .             |
| Data Loss Prevention     | Provides information about Data Loss Prevention incidents and template matches<br><br>For more information, see <a href="#">Data Loss Prevention Events on page 17-33</a> .           |
| Known Threat Activity    | Provides warnings about viruses/spyware/grayware detected by antivirus managed products<br><br>For more information, see <a href="#">Known Threat Activity Events on page 17-42</a> . |
| Network Access Control   | Provides warnings from managed Network VirusWall products<br><br>For more information, see <a href="#">Network Access Control Events on page 17-56</a> .                              |

| EVENT CATEGORY           | DESCRIPTION  |
|--------------------------|--|
| Unusual Product Behavior | Provides information about product options or service activation and deactivation<br><br>For more information, see <a href="#">Unusual Product Behavior Events on page 17-60</a> . |
| Updates                  | Provides antivirus and content security component update results (successful or unsuccessful)<br><br>For more information, see <a href="#">Updates on page 17-66</a> .             |

## Notification Method Settings

Use the **Notification Method Settings** screen to configure settings for the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email               | Configure <b>SMTP Server Settings</b> to send email notifications about events detected by managed products.<br><br>For more information, see <a href="#">Configuring SMTP Server Settings on page 17-4</a> .                          |
| SNMP Trap           | Configure <b>SNMP Trap Settings</b> to send SNMP trap notifications about events detected by managed products.<br><br>For more information, see <a href="#">Configuring SNMP Trap Settings on page 17-5</a> .                          |
| Syslog              | Configure <b>Syslog Settings</b> to send syslog messages to selected recipients or supported third-party products.<br><br>For more information, see <a href="#">Configuring Syslog Settings on page 17-5</a> .                         |
| Trigger Application | Provide user credentials to trigger an in-house or industry-standard application used by your organization to send notifications.<br>For more information, see <a href="#">Configuring Trigger Application Settings on page 17-6</a> . |

## Configuring SMTP Server Settings

Apex Central allows you to send email messages to notify selected recipients about events detected by managed products.



### Important

You must configure **SMTP Server Settings** in order for Apex Central to send email messages.

---

### Procedure

1. Go to **Detections > Notifications > Notification Methods**.  
The **Notification Methods** screen appears.
  2. In the **SMTP Server Settings** section, specify the following:
    - a. **Server FQDN or IP address**: Type a valid FQDN, IPv4, or IPv6 address.
    - b. **Port**: Type the port number of the SMTP server.
    - c. **Sender email address**: Type the email address that sends the event notification.
    - d. **Attachment size limit (KB)**: Specify the maximum file attachment size in kilobytes.
  3. To use Extended SMTP (ESMTP):
    - a. Select **Enable ESMTP**.
    - b. Specify the user name and password.
    - c. Select the authentication method from the **Authentication** drop-down list.
  4. Click **Save**.
-



---

## Configuring SNMP Trap Settings

Apex Central allows you to send Simple Network Management Protocol (SNMP) traps to notify selected recipients about events detected by managed products.

---

### Procedure

1. Go to **Detections > Notifications > Notification Methods**.  
The **Notification Methods** screen appears.
  2. In the **SNMP Trap Settings** section, specify the following:
    - a. **Community name:** Type the SNMP community name.
    - b. **Server IP address:** Type the IPv4 or IPv6 address of the SNMP server.
  3. Click **Save**.
- 

## Configuring Syslog Settings

Apex Central allows you to send syslog messages to notify selected recipients about events detected by managed products.

You can also direct syslog messages to supported third-party products.

---

### Procedure

1. Go to **Detections > Notifications > Notification Methods**.  
The **Notification Methods** screen appears.
2. In the **Syslog Settings** section, specify the following:
  - a. **Server IP address:** Type the IPv4 or IPv6 address of the syslog server.
  - b. **Port:** The the port number of the syslog server.
  - c. **Facility:** Select the facility code.

**Note**

Add multiple syslog servers using the add icon (+).

---

3. Click **Save**.
- 

## Configuring Trigger Application Settings

Apex Central allows you to use in-house or industry-standard applications to notify selected recipients about events detected by managed products.

For example, if your organization uses a batch file that executes the **net send** command, you can use the **Notification Method Settings** screen to provide the credentials for a user account with the necessary privileges.

**Important**

Save the trigger application file in the following location on the Apex Central server:

```
<Apex Central installation directory>\Application\
```

---

### Procedure


1. Go to **Detections > Notifications > Notification Methods**.  
The **Notification Methods** screen appears.
  2. In the **Trigger Application Settings** section, select **Use a specified user to trigger the application**.
  3. Type the user name and password for an account with the privileges required by the trigger application.
  4. Click **Save**.
- 

## Contact Groups

The **Contact Groups** screen provides a list of all previously defined contact groups that are available when specifying report and event notification

recipients. Apex Central contact groups allow you to send notifications or reports to all the recipients in the same group without having to select user accounts individually.

The following table outlines the tasks available on the **Contact Groups** screen.

| TASK                           | DESCRIPTION  |
|--------------------------------|--|
| Add new contact groups         | Click <b>Add</b> to create a new contact group.<br>For more information, see <a href="#">Adding Contact Groups on page 17-7</a> .  |
| Remove existing contact groups | Select an existing contact group and click <b>Remove</b> .<br><br> <b>WARNING!</b> Deleting a contact group affects all reports or notifications using the group. |
| Edit existing contact groups   | Click the <b>Name</b> of an existing contact group to edit the recipients.<br>For more information, see <a href="#">Editing Contact Groups on page 17-8</a> .  |

## Adding Contact Groups

Use the **Add Group** screen to create new contact groups for reports and event notifications.

### Procedure

1. Go to **Detections > Notifications > Contact Groups**

The **Contact Groups** screen appears.

2. Click **Add**.

The **Add Group** screen appears.

3. Type a name for the contact group.
4. Specify recipients for the contact group.

- From the **Available User Accounts** list, select user accounts and click >.

The selected user accounts appear in the **Selected User Accounts** list.



**Note**

You can also add users and groups from an integrated Active Directory structure.

For more information, see [Active Directory Integration on page 6-2](#).

---

- In the **Additional recipients** field, type an email address and press **ENTER**.

The newly added email address appears below the **Additional recipients** field.



**Note**

You can only add one email address at a time.

---

5. Click **Save**.
- 

## Editing Contact Groups

Use the **Edit Group** screen to create new contact groups for reports and event notifications.



**Note**

You cannot edit the **Name** of an existing contact group.

---

### Procedure

1. Go to **Detections > Notifications > Contact Groups**

The **Contact Groups** screen appears.

2. Click the **Name** of the contact group you want to edit.

The **Edit Group** screen appears.

3. Specify recipients for the contact group.

- From the **Available User Accounts** list, select user accounts and click >.

The selected user accounts appear in the **Selected User Accounts** list.

**Note**

You can also add users and groups from an integrated Active Directory structure.

For more information, see [Active Directory Integration on page 6-2](#).

- In the **Additional recipients** field, type an email address and press **ENTER**.

The newly added email address appears below the **Additional recipients** field.

**Note**

You can only add one email address at a time.

4. Click **Save**.
- 

## Advanced Threat Activity Events

Use the **Event Notifications** screen to enable and configure notifications for advanced threat activity detected on your network.

## Attack Discovery Detections

Configure the following event notification to notify administrators when advanced threats have been detected by the Attack Discovery Engine.

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Attack Discovery Detections**.

The **Attack Discovery Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS       | DESCRIPTION  |
|----------------|--|
| Detection type | Select the risk level of the detections that trigger the event notification. |
| Period         | Specify the period of time.  |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION   |
|---------------|---|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Attack Discovery Token Variables on page C-5</a> . |

7. To test if recipients can receive the event notification, click **Test**.

8. Click **Save**.

---

## Behavior Monitoring Violations

Configure the following event notification to notify administrators when Behavior Monitoring violations have been detected.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Behavior Monitoring violations**.

The **Behavior Monitoring violations** screen appears.

4. Specify the following notification settings.

| SETTINGS  | DESCRIPTION  |
|---|--|
| Trigger an alert for each detection                           | Select to send an event notification for each detection.   |
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION   |
|---------------|---|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

---

## C&C Callback Alert

Configure the following event notification to notify administrators when communication between an endpoint and a known C&C callback address has been detected.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **C&C callback alert**.

The **C&C Callback Alert** screen appears.

4. Specify the following notification settings.

| SETTINGS        | DESCRIPTION                          |
|-----------------|--------------------------------------|
| C&C list source | Select one or more C&C list sources. |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.



- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD            | DESCRIPTION  |
|-------------------|--|
| Email message     | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">C&amp;C Callback Token Variables on page C-6</a> . |
| Windows event log | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">C&amp;C Callback Token Variables on page C-6</a> .                           |
| Syslog            | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## C&C Callback Outbreak Alert

Configure the following event notification to notify administrators when communications between multiple endpoints and known C&C callback addresses have been detected.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **C&C callback outbreak alert**.

The **C&C Callback Outbreak Alert** screen appears.

4. Specify the following notification settings.

| SETTINGS          | DESCRIPTION                              |
|-------------------|--|
| C&C list source   | Select one or more C&C list sources.     |
| Callback attempts | Specify the number of callback attempts. |
| Compromised hosts | Specify the number of compromised hosts. |
| Period            | Specify the period of time.              |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">C&amp;C Callback Token Variables on page C-6</a> . |

7. To test if recipients can receive the event notification, click **Test**.

8. Click **Save**.

## Correlated Incident Detections

Configure the following event notification to notify administrators when correlated incidents have been detected.

---

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Correlated incident detections**.

The **Correlated Incident Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS                  | DESCRIPTION   |
|---------------------------|---|
| Attach logs in CSV format | Select to send event notification recipients a *.csv file containing log data about the detections. |


5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Advanced Threat Activity Token Variables on page C-2</a>.</p> <hr/> <p> <b>Note</b></p> <p>The <code>%hostIP%</code> and <code>%group%</code> token variables are not applicable in email notifications because data is aggregated from multiple hosts.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Email Messages with Advanced Threats

Configure the following event notification to notify administrators when email messages with advanced threats have been detected.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Advanced Threat Activity**.  
A list of events appears.
3. In the **Event** column, click **Email messages with advanced threats**.  
The **Email Messages with Advanced Threats** screen appears.
4. Specify the following notification settings.

| SETTINGS       | DESCRIPTION  |
|----------------|--|
| Detections     | Type the number of threats detected by the managed product.                  |
| Period         | Specify the period of time.  |
| Detection type | Select the risk level of the detections that trigger the event notification. |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION   |
|---------------|---|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## High Risk Virtual Analyzer Detections

Configure the following event notification to notify administrators when Virtual Analyzer detects highly suspicious objects.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **High risk Virtual Analyzer detections**.

The **High Risk Virtual Analyzer Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS  | DESCRIPTION  |
|---|--|
| Trigger an alert for each detection                           | Select to send an event notification for each detection.   |
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format                                     | Select to send event notification recipients a *.csv file containing log data about the detections.  |

5. Select recipients for the notification.

a. From the **Available Users and Groups** list, select contact groups or user accounts.

b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.

8. Click **Save**.
- 

## High Risk Host Detections

Configure the following event notification to notify administrators when a high risk host has been detected on your network.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **High risk host detections**.

The **High Risk Host Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS  | DESCRIPTION  |
|---|--|
| Trigger an alert for each detection                           | Select to send an event notification for each detection.   |
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format                                     | Select to send event notification recipients a *.csv file containing log data about the detections.  |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a>.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Known Targeted Attack Behavior

Configure the following event notification to notify administrators when known targeted attack behavior has been detected on your network.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Known targeted attack behavior**.

The **Known Targeted Attack Behavior** screen appears.

4. Specify the following notification settings.

| SETTINGS                            | DESCRIPTION  |
|-------------------------------------|--|
| Trigger an alert for each detection | Select to send an event notification for each detection. |



| SETTINGS  | DESCRIPTION  |
|---|--|
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format                                     | Select to send event notification recipients a *.csv file containing log data about the detections.  |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Potential Document Exploit Detections

Configure the following event notification to notify administrators when documents that contain potential exploit code have been detected on your network.

---

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Potential document exploit detections**.

The **Potential Document Exploit Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS  | DESCRIPTION  |
|---|--|
| Trigger an alert for each detection                           | Select to send an event notification for each detection.   |
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format                                     | Select to send event notification recipients a *.csv file containing log data about the detections.  |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a>.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Predictive Machine Learning Detections

Configure the following event notification to notify administrators when emerging unknown security threats have been detected by Trend Micro Predictive Machine Learning.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Advanced Threat Activity**.  
A list of events appears.
3. In the **Event** column, click **Predictive Machine Learning detections**.  
The **Predictive Machine Learning detections** screen appears.
4. Specify the following notification settings.

| SETTINGS                            | DESCRIPTION  |
|-------------------------------------|--|
| Trigger an alert for each detection | Select to send an event notification for each detection. |

| SETTINGS  | DESCRIPTION  |
|---|--|
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION   |
|---------------|---|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Rootkit or Hacking Tool Detections

Configure the following event notification to notify administrators when a rootkit or hacking tool has been detected on your network.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Rootkit or hacking tool detections**.

The **Rootkit or Hacking Tool Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS  | DESCRIPTION  |
|---|--|
| Trigger an alert for each detection                           | Select to send an event notification for each detection.   |
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format                                     | Select to send event notification recipients a *.csv file containing log data about the detections.  |

5. Select recipients for the notification.

a. From the **Available Users and Groups** list, select contact groups or user accounts.

b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.

## 8. Click **Save**.

### SHA-1 Deny List Detections

Configure the following event notification to notify administrators when files with SHA-1 values that match objects in the Deny List have been detected on your network.

#### Procedure

##### 1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

##### 2. Click **Advanced Threat Activity**.

A list of events appears.

##### 3. In the **Event** column, click **SHA-1 Deny List detections**.

The **SHA-1 Deny List Detections** screen appears.

##### 4. Specify the following notification settings.

| SETTINGS  | DESCRIPTION  |
|---|--|
| Trigger an alert for each detection                           | Select to send an event notification for each detection.   |
| Specify the alert threshold that applies to a single endpoint | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format                                     | Select to send event notification recipients a *.csv file containing log data about the detections.  |

##### 5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a>.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Watchlisted Recipients at Risk

Configure the following event notification to notify administrators when Deep Discovery Email Inspector detects malicious or suspicious email messages or attachments sent to watchlisted recipients.

### Procedure

- Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
- Click **Advanced Threat Activity**.  
A list of events appears.
- In the **Event** column, click **Watchlisted recipients at risk**.  
The **Watchlisted Recipients at Risk** screen appears.
- Specify the following notification settings.

| CRITERIA                | DESCRIPTION   |
|-------------------------|---|
| Email address watchlist | Type the email addresses to be monitored. Use a semicolon (;) to separate multiple entries. |
| Type                    | Select the risk level of the detections that trigger the event notification.                |
| Detections              | Type the number of threats detected by the managed product.                                 |
| Period                  | Specify the time period for the detections.   |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

---

## Worm or File Infector Propagation Detections

Configure the following event notification to notify administrators when worm or file infector characteristics have been detected on your network.



---

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Advanced Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Worm or file infector propagation detections**.

The **Worm or File Infector Propagation Detections** screen appears.

4. Specify the following notification settings.

| SETTINGS                            | DESCRIPTION  |
|-------------------------------------|--|
| Trigger an alert for each detection | Select to send an event notification for each detection.   |
| Specify the alert threshold         | Select to send event notifications only for detections that match the specified criteria. <ul style="list-style-type: none"> <li>• Detections: Specify the number of detections</li> <li>• Period: Specify the time period in hours</li> </ul> |
| Attach logs in CSV format           | Select to send event notification recipients a *.csv file containing log data about the detections.  |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Advanced Threat Activity Token Variables on page C-2</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

---

## Content Policy Violation Events

Use the **Event Notifications** screen to enable and configure notifications for content policy violations detected on your network.

### Email Policy Violation

Configure the following event notification to notify administrators when an email has been detected violating content security policy.

---

#### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Content Violation Policy**.  
A list of events appears.
3. In the **Event** column, click **Email policy violation**.  
The **Email Policy Violation** screen appears.
4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Content Policy Violation Token Variables on page C-8</a>.</p> |
| Windows event log   | <p>To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Content Policy Violation Token Variables on page C-8</a>.</p>                           |
| SNMP trap           | <p>Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b>.</p>   |
| Trigger application | <p>Specify the full path of the application file and any parameters for the command.</p>   |
| Syslog              | <p>A standard for forwarding log messages in an IP network</p> <p>Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).</p>  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Web Access Security Violation

Configure the following event notification to notify administrators when access to a URL has been blocked for violating a security policy.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Content Violation Policy**.

A list of events appears.

3. In the **Event** column, click **Web access security violation**.

The **Web Access Security Violation** screen appears.

4. Select recipients for the notification.

a. From the **Available Users and Groups** list, select contact groups or user accounts.

b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Web Access Policy Violation Token Variables on page C-14</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Web Access Policy Violation Token Variables on page C-14</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .   |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |

| METHOD | DESCRIPTION  |
|--------|--|
| Syslog | A standard for forwarding log messages in an IP network<br><br>Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS). |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

---

## Data Loss Prevention Events

Use the **Event Notifications** screen to enable and configure notifications for Data Loss Prevention events detected on your network.

### Incident Details Updated

Configure the following event notification to notify administrators when incident details have been updated.

---

#### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Data Loss Prevention**.  
A list of events appears.
3. In the **Event** column, click **Incident details updated**.  
The **Incident Details Updated** screen appears.
4. Specify the criteria for the incident detail updates to be notified about:

| CRITERIA                 | DESCRIPTION   |
|--------------------------|---|
| Incident detail updates  | Select the type of incident detail updates. <ul style="list-style-type: none"> <li>• <b>Closed</b></li> <li>• <b>Any change</b></li> </ul>  |
| Filter by severity level | Select one or more of the following risk levels. <ul style="list-style-type: none"> <li>• <b>High</b></li> <li>• <b>Medium</b></li> <li>• <b>Low</b></li> <li>• <b>Informational</b></li> <li>• <b>Undefined</b></li> </ul> |

5. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a> . |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

---

## Scheduled Incident Summary

Configure the following event notification to send administrators a summary of the DLP incidents that occurred on your network.

---

### Procedure


1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Data Loss Prevention**.

A list of events appears.

- In the **Event** column, click **Scheduled incident summary**.

The **Scheduled Incident Summary** screen appears.

- Specify the following notification settings.

| CRITERIA                | DESCRIPTION   |
|-------------------------|---|
| Frequency               | Select to receive notifications on a daily or weekly basis.   |
| Attach incident details | <p>Select to attach incident logs to the notification.</p> <ul style="list-style-type: none"> <li>Select the content that DLP Compliance Officers receive: <ul style="list-style-type: none"> <li><b>Incidents from all managed users</b></li> <li><b>Incidents from direct reports only</b></li> </ul> </li> </ul> <hr/> <p> <b>Note</b><br/>DLP Incident Reviewers can only receive incidents from direct reports</p> <hr/> <ul style="list-style-type: none"> <li>Select the format of the log details</li> </ul> |

- Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a>.</p> |

- To test if recipients can receive the event notification, click **Test**.
- Click **Save**.

## Significant Incident Increase

Configure the following event to notify administrators when a significant increase in DLP incidents occurred over a predefined period.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Data Loss Prevention**.

A list of events appears.

3. In the **Event** column, click **Significant incident increase**.

The **Significant Incident Increase** screen appears.

4. Specify the following notification settings.

| SETTINGS | DESCRIPTION                             |
|----------|---|
| Hourly   | Specify the number of hourly incidents. |
| Daily    | Specify the number of daily incidents.  |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.



| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a>.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Significant Incident Increase by Channel

Configure the following event notification to notify administrators when a significant increase in DLP incidents by channel occurred over a predefined period.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Data Loss Prevention**.  
A list of events appears.
3. In the **Event** column, click **Significant incident increase by channel**.  
The **Significant Incident Increase By Channel** screen appears.
4. Specify the following notification settings.

| SETTINGS | DESCRIPTION                             |
|----------|---|
| Hourly   | Specify the number of hourly incidents. |
| Daily    | Specify the number of daily incidents.  |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a>.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Significant Incident Increase by Sender

Configure the following event notification to notify administrators when a significant increase in DLP incidents by sender occurred over a predefined period.

### Procedure

- Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
- Click **Data Loss Prevention**.  
A list of events appears.
- In the **Event** column, click **Significant incident increase by sender**.  
The **Significant Incident Increase by Sender** screen appears.
- Specify the following notification settings.

| SETTINGS | DESCRIPTION                             |
|----------|---|
| Hourly   | Specify the number of hourly incidents. |
| Daily    | Specify the number of daily incidents.  |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a>.</p> |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Significant Incident Increase by User

Configure the following event notification to notify administrators when a significant increase in DLP incidents by user occurred over a predefined period.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Data Loss Prevention**.

A list of events appears.

3. In the **Event** column, click **Significant incident increase by user**.

The **Significant Incident Increase by User** screen appears.

4. Specify the following notification settings.

| SETTINGS | DESCRIPTION                             |
|----------|---|
| Hourly   | Specify the number of hourly incidents. |
| Daily    | Specify the number of daily incidents.  |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a> . |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Significant Template Match Increase

Configure the following event notification to notify administrators when a significant increase in DLP template matches occurred over a predefined period.

---

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Data Loss Prevention**.

A list of events appears.

3. In the **Event** column, click **Significant template match increase**.

The **Significant Template Match Increase** screen appears.

4. Specify the following notification settings.

| SETTINGS | DESCRIPTION                             |
|----------|---|
| Hourly   | Specify the number of hourly incidents. |
| Daily    | Specify the number of daily incidents.  |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Data Loss Prevention Token Variables on page C-9</a> . |

7. To test if recipients can receive the event notification, click **Test**.

8. Click **Save**.
-

## Known Threat Activity Events

Use the **Event Notifications** screen to enable and configure notifications for known threat activity detected on your network.

### Network Virus Alert

Configure the following event notification to notify administrators when a network virus has been detected.

---

#### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Network virus alert**.

The **Network Virus Alert** screen appears.

4. Specify the following notification settings.

| SETTINGS                 | DESCRIPTION   |
|--------------------------|---|
| Detections               | Type the number of threats detected by the managed product. |
| Affected users/endpoints | Specify the number of affected users/endpoints.             |
| Period                   | Specify the period of time.                                 |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> , <a href="#">Known Threat Activity Token Variables on page C-11</a> and <a href="#">Network Access Control Token Variables on page C-14</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> , <a href="#">Known Threat Activity Token Variables on page C-11</a> and <a href="#">Network Access Control Token Variables on page C-14</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .   |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Special Spyware/Grayware Alert

Configure the following event notification to notify administrators when a spyware/grayware included in the list of monitored spyware/grayware threats has been detected.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Special spyware/grayware alert**.

The **Special Spyware/Grayware Alert** screen appears.

4. Type the names of the spyware/grayware to monitor.

5. Specify the following notification settings.

| SETTINGS | DESCRIPTION                 |
|----------|-----------------------------|
| Period   | Specify the period of time. |

6. Select recipients for the notification.

a. From the **Available Users and Groups** list, select contact groups or user accounts.

b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

7. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> .                           |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |



| METHOD | DESCRIPTION   |
|--------|---|
| Syslog | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS). |

8. To test if recipients can receive the event notification, click **Test**.
9. Click **Save**.

## Special Virus Alert

Configure the following event notification to notify administrators when a virus included in the list of monitored viruses has been detected.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Special virus alert**.

The **Special Virus Alert** screen appears.

4. Type the name of the viruses to monitor.

5. Specify the following notification settings.

| SETTINGS | DESCRIPTION                 |
|----------|-----------------------------|
| Period   | Specify the period of time. |

6. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

7. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> , <a href="#">Known Threat Activity Token Variables on page C-11</a> and <a href="#">Network Access Control Token Variables on page C-14</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> , <a href="#">Known Threat Activity Token Variables on page C-11</a> and <a href="#">Network Access Control Token Variables on page C-14</a> .                           |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

8. To test if recipients can receive the event notification, click **Test**.
9. Click **Save**.

---

## Spyware/Grayware Found - Action Successful

Configure the following event notification to notify administrators when the configured spyware/grayware scan actions are successful for the spyware/grayware detection.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Spyware/Grayware found - action successful**.

The **Spyware/Grayware Found - Action Successful** screen appears.

4. Select recipients for the notification.

a. From the **Available Users and Groups** list, select contact groups or user accounts.

b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .   |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
  7. Click **Save**.
- 

## Spyware/Grayware Found - Further Action Required

Configure the following event notification to notify administrators when spyware/grayware detections require further action.

Configure the following event notification to notify administrators when the configured spyware/grayware scan actions were unsuccessful/unavailable for the spyware/grayware detection.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Spyware/Grayware found - further action required**.

The **Spyware/Grayware Found - Further Action Required** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a>.</p> |
| Windows event log   | <p>To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a>.</p>                           |
| SNMP trap           | <p>Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b>.</p>   |
| Trigger application | <p>Specify the full path of the application file and any parameters for the command.</p>   |
| Syslog              | <p>Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).</p>   |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Virus Found - First Action Successful

Configure the following event notification to notify administrators when the first scan action for a virus detection is successful.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Virus Found - first action successful**.

The **Virus Found - First Action Successful** screen appears.

4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .   |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Virus Found - First Action Unsuccessful and Second Action Unavailable

Configure the following event notification to notify administrators when the first scan action for a virus detection is unsuccessful and the second action is unavailable.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Virus found - first action unsuccessful and second action unavailable**.

The **Virus Found - First Action Unsuccessful and Second Action Unavailable** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD        | DESCRIPTION  |
|---------------|--|
| Email message | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .                           |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Virus Found - First and Second Actions Unsuccessful

Configure the following event notification to notify administrators when the first and second scan actions for a virus detection are unsuccessful.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Virus found - first and second actions unsuccessful**.

The **Virus Found - First and Second Actions Unsuccessful** screen appears.



4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .   |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Virus Found - Second Action Successful

Configure the following event notification to notify administrators when the second scan action for a virus detection is successful.

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Virus found - second action successful**.

The **Virus Found - Second Action Successful** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD            | DESCRIPTION  |
|-------------------|--|
| Email message     | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a>.</p> |
| Windows event log | <p>To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a>.</p>                           |
| SNMP trap         | <p>Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b>.</p>   |

| METHOD              | DESCRIPTION   |
|---------------------|---|
| Trigger application | Specify the full path of the application file and any parameters for the command.   |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS). |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Virus Outbreak Alert

Configure the following event notification to notify administrators when a virus outbreak is detected.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Known Threat Activity**.

A list of events appears.

3. In the **Event** column, click **Virus outbreak alert**.

The **Virus Outbreak Alert** screen appears.

4. Specify the following notification settings.

| SETTINGS                 | DESCRIPTION   |
|--------------------------|---|
| Detections               | Type the number of threats detected by the managed product. |
| Affected users/endpoints | Specify the number of affected users/endpoints.             |
| Period                   | Specify the period of time.                                 |

5. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.
- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

6. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Known Threat Activity Token Variables on page C-11</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .   |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

7. To test if recipients can receive the event notification, click **Test**.
8. Click **Save**.

## Network Access Control Events

Use the **Event Notifications** screen to enable and configure notifications for Network VirusWall policy violations or potential vulnerability attacks detected on your network.

## Network VirusWall Policy Violations

Configure the following event notification to notify administrators when a Network VirusWall policy violation has been detected.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Network Access Control**.

A list of events appears.

3. In the **Event** column, click **Network VirusWall policy violations**.

The **Network VirusWall Policy Violations** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD            | DESCRIPTION   |
|-------------------|---|
| Email message     | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> . |
| Windows event log | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                           |

| METHOD              | DESCRIPTION  |
|---------------------|--|
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Potential Vulnerability Attacks

Configure the following event notification to notify administrators when Network VirusWall has detected potential vulnerability attacks.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Network Access Control**.

A list of events appears.

3. In the **Event** column, click **Potential vulnerability attacks**.

The **Potential Vulnerability Attacks** screen appears.

4. Specify the following notification settings.

| SETTINGS   | DESCRIPTION  |
|------------|--|
| Detections | Specify the amount of potential vulnerability attacks detected by Network VirusWall. |
| Period     | Specify the period of time.  |

| SETTINGS    | DESCRIPTION   |
|-------------|---|
| Reported by | Specify the number of Network VirusWall devices that reported the potential vulnerability attack. |

5. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
6. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION   |
|---------------------|---|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Network Access Control Token Variables on page C-14</a> . |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> and <a href="#">Network Access Control Token Variables on page C-14</a> .                           |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> .  |
| Trigger application | Specify the full path of the application file and any parameters for the command.   |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).   |

7. To test if recipients can receive the event notification, click **Test**.

8. Click **Save**.
- 

## Unusual Product Behavior Events

Use the **Event Notifications** screen to enable and configure notifications for unusual product behaviors detected on your network.

### Managed Product Unreachable

Configure the following event notification to notify administrators when a connection error occurs between Apex Central and a managed product server.

---

#### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Unusual Product Behavior**.  
A list of events appears.
3. In the **Event** column, click **Managed product unreachable**.  
The **Managed Product Unreachable** screen appears.
4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.  
The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
5. Enable one or more of the following notification methods.



| METHOD        | DESCRIPTION   |
|---------------|---|
| Email message | <p>To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.</p> <p>For more information, see <a href="#">Standard Token Variables on page C-2</a>.</p> |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

---

## Product Service Started

Configure the following event notification to notify administrators when a product service has started.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Unusual Product Behavior**.  
A list of events appears.
3. In the **Event** column, click **Product service started**.  
The **Product Service Started** screen appears.
4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.  
The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                    |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

---

## Product Service Stopped

Configure the following event notification to notify administrators when a product service has stopped.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Unusual Product Behavior**.  
A list of events appears.
3. In the **Event** column, click **Product service stopped**.  
The **Product Service Stopped** screen appears.

4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.
 

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                        |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Real-time Scan Disabled

Configure the following event notification to notify administrators when Real-time Scan is disabled.

## Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Unusual Product Behavior**.

A list of events appears.

3. In the **Event** column, click **Real-time Scan disabled**.

The **Real-time Scan Disabled** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                    |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |

---

| METHOD | DESCRIPTION   |
|--------|---|
| Syslog | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS). |

6. To test if recipients can receive the event notification, click **Test**.
  7. Click **Save**.
- 

## Real-time Scan Enabled

Configure the following event notification to notify administrators when Real-time Scan is enabled.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Unusual Product Behavior**.  
A list of events appears.
3. In the **Event** column, click **Real-time Scan enabled**.  
The **Real-time Scan Enabled** screen appears.
4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.  
The selected contact groups or user accounts appear in the **Selected Users and Groups** list.
5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                    |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Updates

Use the **Event Notifications** screen to enable and configure notifications for component update statuses.

### Antispam Rule Update Successful

Configure the following event notification to notify administrators when an antispam rule update is successful.

#### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Update**.

A list of events appears.

3. In the **Event** column, click **Antispam rule update successful**.

The **Antispam Rule Update Successful** screen appears.

4. Select recipients for the notification.

a. From the **Available Users and Groups** list, select contact groups or user accounts.

b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                        |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.

7. Click **Save**.

## Antispam Rule Update Unsuccessful

Configure the following event notification to notify administrators when an antispam rule update is unsuccessful.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Update**.

A list of events appears.

3. In the **Event** column, click **Antispam rule update unsuccessful**.

The **Antispam Rule Update Unsuccessful** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD            | DESCRIPTION   |
|-------------------|---|
| Email message     | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> . |
| Windows event log | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                           |



| METHOD              | DESCRIPTION  |
|---------------------|--|
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

---

## Pattern File/Cleanup Template Update Successful

Configure the following event notification to notify administrators when a pattern file or cleanup template update is successful.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Update**.  
A list of events appears.
3. In the **Event** column, click **Pattern file/Cleanup template update successful**.  
The **Pattern File/Cleanup Template Update Successful** screen appears.
4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                    |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Pattern File/Cleanup Template Update Unsuccessful

Configure the following event notification to notify administrators when a pattern file or cleanup template update is unsuccessful.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.  
The **Event Notifications** screen appears.
2. Click **Update**.

A list of events appears.

3. In the **Event** column, click **Pattern file/Cleanup template update unsuccessful**.

The **Pattern File/Cleanup Template Update Unsuccessful** screen appears.

4. Select recipients for the notification.
  - a. From the **Available Users and Groups** list, select contact groups or user accounts.
  - b. Click >.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                    |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br><br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.

7. Click **Save**.

---

## Scan Engine Update Successful

Configure the following event notification to notify administrators when a scan engine update is successful.

---

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Update**.

A list of events appears.

3. In the **Event** column, click **Scan engine update successful**.

The **Scan Engine Update Successful** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD            | DESCRIPTION   |
|-------------------|---|
| Email message     | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> . |
| Windows event log | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                           |

| METHOD              | DESCRIPTION  |
|---------------------|--|
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslog to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).   |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

## Scan Engine Update Unsuccessful

Configure the following event notification to notify administrators when a scan engine update is unsuccessful.

### Procedure

1. Go to **Detections > Notifications > Event Notifications**.

The **Event Notifications** screen appears.

2. Click **Update**.

A list of events appears.

3. In the **Event** column, click **Scan engine update unsuccessful**.

The **Scan Engine Update Unsuccessful** screen appears.

4. Select recipients for the notification.

- a. From the **Available Users and Groups** list, select contact groups or user accounts.

- b. Click **>**.

The selected contact groups or user accounts appear in the **Selected Users and Groups** list.

5. Enable one or more of the following notification methods.

| METHOD              | DESCRIPTION  |
|---------------------|--|
| Email message       | To customize the email notification template, use supported token variables or modify the text in the <b>Subject</b> and <b>Message</b> fields.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .                        |
| Windows event log   | To customize the notification template, use supported token variables or modify the text in the <b>Message</b> field.<br>For more information, see <a href="#">Standard Token Variables on page C-2</a> .  |
| SNMP trap           | Apex Central stores SNMP trap notifications in a Management Information Base (MIB). To view the SNMP trap notifications, go to <b>Notifications &gt; Notification Method Settings</b> and click <b>Download MIB file</b> under <b>SNMP Trap Settings</b> . |
| Trigger application | Specify the full path of the application file and any parameters for the command.  |
| Syslog              | Apex Central can direct syslogs to supported third-party products, including Cisco Security Monitoring, Analysis and Response (MARS).  |

6. To test if recipients can receive the event notification, click **Test**.
7. Click **Save**.

# Chapter 18

## Reports

This section discusses how to create reports using the data collected from all managed products registered to Apex Central.

Topics include:

- *Reports Overview on page 18-2*
- *Custom Templates on page 18-2*
- *One-time Reports on page 18-20*
- *Scheduled Reports on page 18-25*
- *Configuring Report Maintenance on page 18-36*
- *Viewing My Reports on page 18-36*

## Reports Overview

Apex Central allows you to generate, download, and send reports that consolidate data from all registered managed products without having to log on to multiple product consoles.

You can use Apex Central to:

- Generate one-time reports on demand.
- Add scheduled reports to automatically generate and send reports to specified recipients on a user-defined schedule.
- Create custom report templates from data views or use pre-defined custom templates and static templates.
- Generate custom reports for endpoints that have been assigned custom tags, filters, or important labels.

## Custom Templates

The **Custom Templates** screen provides a list of all available custom report templates. Apex Central provides pre-defined custom templates for you to use. You can copy a pre-defined template to edit or create a new template by selecting and configuring specific report elements.

**Note**

Custom templates use data views that correspond to specific Apex Central logs to define the scope of the report data.

For more information, see the following topics:

- [Log Names and Data Views on page 16-6](#)
  - [Data Views on page B-1](#)
- 

The following table outlines the available tasks on the **Custom Templates** screen.



| TASK                     | DESCRIPTION  |
|--------------------------|--|
| Add new custom templates | Click <b>Add</b> to create a new custom template.<br>For more information, see <a href="#">Adding or Editing Custom Templates on page 18-3</a> .   |
| Delete custom templates  | Select an existing template and click <b>Delete</b> .  |
| Edit custom templates    | Click the <b>Name</b> of an existing template to edit.<br>For more information, see <a href="#">Adding or Editing Custom Templates on page 18-3</a> .  |
| Copy custom templates    | Select an existing template and click <b>Copy</b> . Apex Central adds a new template to the list using the following naming:<br><code>Copy of &lt;original_template_name&gt;</code><br>For more information, see <a href="#">Adding or Editing Custom Templates on page 18-3</a> . |
| Import custom templates  | Click <b>Import</b> to import a properly formatted XML report template into Apex Central.  |
| Export custom templates  | Select an existing template and click <b>Export</b> . Apex Central exports the template in XML format.   |

## Adding or Editing Custom Templates

You can create custom templates to generate company-specific reports in multiple formats.

### Procedure

1. Go to **Detections > Reports > Custom Templates**.

The **Custom Templates** screen appears.

2. Add, edit, or copy a template.

- To add a new template, click **Add**.

The **Add Report Template** screen appears.

- To edit an existing template, click the **Name** of the template.

The **Edit Report Template** screen appears.

- To make a copy of an existing template to use as the basis for a new template:

- a. Select the check box to the left of the **Name** of the template you want to use.

- b. Click **Copy**.

Apex Central adds a new template to the list using the following naming:

Copy of <original\_template\_name>

- c. Click the newly added template **Name**.

The **Edit Report Template** screen appears.

3. Specify a unique **Name** for the template.
4. (Optional) Provide a **Description** for the new template.
5. Using the **Working Panel**, drag and drop report elements into the available “row” to design the section layout of your report.



**Important**

Each row only supports 3 report elements.

---




**Tip**

If the **Working Panel** does not appear, click the **Show working panel** button beside **Template Content**.

---

**TABLE 18-1. Report Elements**

| <b>TEMPLATE ELEMENT</b> | <b>DESCRIPTION</b>   |
|-------------------------|--|
| Static text             | <p>Provides a container for user-defined content</p> <hr/> <p> <b>Note</b><br/>Static text content can contain up to 4096 characters.</p> <hr/> <p>For more information, see <a href="#">Configuring the Static Text Report Element on page 18-7</a>.</p> |
| Bar chart               | <p>Inserts a customizable bar chart object</p> <p>For more information, see <a href="#">Configuring the Bar Chart Report Element on page 18-8</a>.</p>   |
| Line chart              | <p>Inserts a customizable line graph object</p> <p>For more information, see <a href="#">Configuring the Line Chart Report Element on page 18-11</a>.</p>  |
| Pie chart               | <p>Inserts a customizable pie chart object</p> <p>For more information, see <a href="#">Configuring the Pie Chart Report Element on page 18-13</a>.</p>  |
| Dynamic table           | <p>Inserts a customizable dynamic table / pivot table object</p> <p>The information in a dynamic table compares exactly two data fields either horizontally or vertically.</p> <p>For more information, see <a href="#">Configuring the Dynamic Table Report Element on page 18-16</a>.</p>  |
| Grid table              | <p>Inserts a customizable table object</p> <p>The information in a grid table will be the same as the information that displays in a log query.</p> <p>For more information, see <a href="#">Configuring the Grid Table Report Element on page 18-19</a>.</p>  |

6. Organize the layout of rows and pages in your report using the **Insert page break above**, **Insert row above**, **Insert row below**, and **Delete this row** buttons.



**Note**

Report elements added to the same row appear side-by-side in the order you added the elements to the template. This allows you to display multiple charts on the same line. If you want to display multiple charts on different lines within the same page, insert new rows but do not insert a page break.

---

## Add Report Template

The screenshot shows a 'Template Content' window with a 'Show working panel' button. Below the header, there are 'Name:' and 'Description:' labels with corresponding input fields. The main area contains two report elements: a 'Static Text' element and a 'Bar Chart' element. Each element has a preview window and control buttons (Edit, Del) at the top. Between and after the elements are buttons for 'Insert page break above', 'Insert row above', 'Delete this row', and 'Insert row below'.

**FIGURE 18-1.** Custom report template setup to display static text above a bar chart

7. Click **Save**.

## Configuring the Static Text Report Element

This task assumes that you have already added the **Static Text** report element to a custom report template row.

For more information, see [Adding or Editing Custom Templates on page 18-3](#).

---

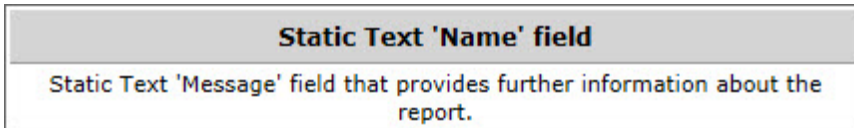
## Procedure

1. In the **Static Text** report element, click **Edit**.  
The **Edit Static Text** screen appears.
2. In the **Name** field, specify the title of the text box element.
3. In the **Message** field, specify any descriptive text to display in the message body.

**Note**

Static text content can contain up to 4096 characters.

---



**FIGURE 18-2.** Static text report output example

4. Click **Save** to return to the **Add/Edit Report Template** screen.
- 

## Configuring the Bar Chart Report Element

This task assumes that you have already added the **Bar Chart** report element to a custom report template row.

For more information, see [Adding or Editing Custom Templates on page 18-3](#).

---

## Procedure

1. In the **Bar Chart** report element, click **Edit**.  
The **Edit Bar Chart > Step 1: Data View** screen appears.
2. Select the type of report data you want to display from the **Data Views** directory.

For more information, see [Data Views on page B-1](#).

3. Click **Next** >.

The **Step 2: Set Query Criteria** screen appears.

4. To filter the data that displays, select **Custom criteria**.
5. Specify the **Match** rule for the custom filter.
  - **All of the criteria:** Data must match all the specified criteria.
  - **Any of the criteria:** Data can match any of the specified criteria.
6. Specify the filtering criteria, each of which consists of three parts:
  - **Data type:** Corresponds to a column returned by the data view
  - **Operator:** Used to match or exclude data type values
  - **Value:** Select criteria from the drop-down controls or specify values in the text boxes

**Note**

The options that display depend on the selected data view, and the selected data type and operator.

Apex Central supports a maximum of 20 filters.

---

7. Add or remove criteria using the plus (+) and minus (-) controls.
8. Click **Next** >.

The **Step 3: Specify Design** screen appears.
9. Specify the **Name** used as the title for the chart.
10. From the **Drag Available Fields** list, drag-and-drop the data that displays in the following locations:
  - **Data Field:** Specifies the total count for data appearing in the chart
  - **Category Field:** Specifies how the data is separated in the chart
  - **Series Field:** Defines the type of data to plot against the vertical and horizontal axes used as a comparison

**11.** In the **Data Properties** section, configure the following:

- **Aggregated by:** The method in which to display data
  - **Total number of instances:** Includes duplicate results in the data
  - **Number of unique instances:** Displays only one instance of duplicated result types

For example, if an endpoint detects 5 instances of “VirusA” and 3 instances of “VirusB” in the data, the detection count on the graph would display the following values:

- Total number of instances = 8 (virus detections, regardless of virus name)
- Number of unique instances = 2 (unique virus types, regardless of number of occurrences)

**12.** In the **Category Properties** section, configure the following:

- Specify the **Label** name that appears on the horizontal axis of the chart.
- Select the **Sorting** order and direction.
  - **Aggregation value:** Sorts based on the count value of the data
  - **Category name:** Sorts alphabetically based on the category name
- Select the **Filter summarized result** check box to filter the data that displays in the report.
  - Specify the maximum number of items to display.
  - Enable **Aggregate remaining items** to group all remaining data in the “Others” category.

**13.** In the **Series Properties** section, specify the **Label name** that appears to describe the data series.

**14.** Click **Save**.



The **Add/Edit Report Template** screen appears with the updated chart settings applied.

---

## Configuring the Line Chart Report Element

This task assumes that you have already added the **Line Chart** report element to a custom report template row.

For more information, see [Adding or Editing Custom Templates on page 18-3](#).

---

### Procedure

1. In the **Line Chart** report element, click **Edit**.

The **Edit Line Chart > Step 1: Data View** screen appears.

2. Select the type of report data you want to display from the **Data Views** directory.

For more information, see [Data Views on page B-1](#).

3. Click **Next >**.

The **Step 2: Set Query Criteria** screen appears.

4. To filter the data that displays, select **Custom criteria**.

5. Specify the **Match** rule for the custom filter.

- **All of the criteria:** Data must match all the specified criteria.
- **Any of the criteria:** Data can match any of the specified criteria.

6. Specify the filtering criteria, each of which consists of three parts:

- **Data type:** Corresponds to a column returned by the data view
- **Operator:** Used to match or exclude data type values
- **Value:** Select criteria from the drop-down controls or specify values in the text boxes

**Note**

The options that display depend on the selected data view, and the selected data type and operator.

Apex Central supports a maximum of 20 filters.

---

7. Add or remove criteria using the plus (+) and minus (-) controls.

8. Click **Next >**.

The **Step 3: Specify Design** screen appears.

9. Specify the **Name** used as the title for the chart.

10. From the **Drag Available Fields** list, drag-and-drop the data that displays in the following locations:

- **Data Field:** Defines the data value on the vertical axis of the chart
- **Category Field:** Defines the data value on the horizontal axis of the chart
- **Series Field:** Defines the type of data to plot against the vertical and horizontal axes used as a comparison

11. In the **Data Properties** section, configure the following:

- **Value label:** The label that appears on the vertical axis of the chart
- **Aggregated by:** The method in which to display data
  - **Total number of instances:** Includes duplicate results in the data
  - **Number of unique instances:** Displays only one instance of duplicated result types

For example, if an endpoint detects 5 instances of “VirusA” and 3 instances of “VirusB” in the data, the detection count on the graph would display the following values:

- Total number of instances = 8 (virus detections, regardless of virus name)

- Number of unique instances = 2 (unique virus types, regardless of number of occurrences)

**12.** In the **Category Properties** section, configure the following:

- Specify the **Label** name that appears on the horizontal axis of the chart.
- Select the **Sorting** order and direction.
  - **Aggregation value:** Sorts based on the count value of the data
  - **Category name:** Sorts alphabetically based on the category name
- Select the **Filter summarized result** check box to filter the data that displays in the report.
  - Specify the maximum number of items to display.
  - Enable **Aggregate remaining items** to group all remaining data in the “Others” category.

**13.** In the **Series Properties** section, specify the **Label name** that appears to describe the data series.

**14.** Click **Save**.

The **Add/Edit Report Template** screen appears with the updated chart settings applied.

---

## Configuring the Pie Chart Report Element

This task assumes that you have already added the **Pie Chart** report element to a custom report template row.

For more information, see [Adding or Editing Custom Templates on page 18-3](#).

---

### Procedure

**1.** In the **Pie Chart** report element, click **Edit**.

The **Edit Pie Chart > Step 1: Data View** screen appears.

2. Select the type of report data you want to display from the **Data Views** directory.

For more information, see [Data Views on page B-1](#).

3. Click **Next >**.

The **Step 2: Set Query Criteria** screen appears.

4. To filter the data that displays, select **Custom criteria**.

5. Specify the **Match** rule for the custom filter.

- **All of the criteria:** Data must match all the specified criteria.
- **Any of the criteria:** Data can match any of the specified criteria.

6. Specify the filtering criteria, each of which consists of three parts:

- **Data type:** Corresponds to a column returned by the data view
- **Operator:** Used to match or exclude data type values
- **Value:** Select criteria from the drop-down controls or specify values in the text boxes



**Note**

The options that display depend on the selected data view, and the selected data type and operator.

Apex Central supports a maximum of 20 filters.

---

7. Add or remove criteria using the plus (+) and minus (-) controls.

8. Click **Next >**.

The **Step 3: Specify Design** screen appears.

9. Specify the **Name** used as the title for the chart.

10. From the **Drag Available Fields** list, drag-and-drop the data that displays in the following locations:

- **Data Field:** Specifies the total count for data appearing in the chart

- **Category Field:** Specifies how the data is separated in the chart

**11.** In the **Data Properties** section, configure the following:

- **Aggregated by:** The method in which to display data
  - **Total number of instances:** Includes duplicate results in the data
  - **Number of unique instances:** Displays only one instance of duplicated result types

For example, if an endpoint detects 5 instances of “VirusA” and 3 instances of “VirusB” in the data, the detection count on the graph would display the following values:

- Total number of instances = 8 (virus detections, regardless of virus name)
- Number of unique instances = 2 (unique virus types, regardless of number of occurrences)

**12.** In the **Category Properties** section, configure the following:

- Specify the **Label** name that appears on the horizontal axis of the chart.
- Select the **Sorting** order and direction.
  - **Aggregation value:** Sorts based on the count value of the data
  - **Category name:** Sorts alphabetically based on the category name
- Select the **Filter summarized result** check box to filter the data that displays in the report.
  - Specify the maximum number of items to display.
  - Enable **Aggregate remaining items** to group all remaining data in the “Others” category.

**13.** Click **Save**.

The **Add/Edit Report Template** screen appears with the updated chart settings applied.

---

## Configuring the Dynamic Table Report Element

This task assumes that you have already added the **Dynamic Table** report element to a custom report template row.

For more information, see [Adding or Editing Custom Templates on page 18-3](#).

---

### Procedure

1. In the **Dynamic Table** report element, click **Edit**.

The **Edit Dynamic Table > Step 1: Data View** screen appears.

2. Select the type of report data you want to display from the **Data Views** directory.

For more information, see [Data Views on page B-1](#).

3. Click **Next >**.

The **Step 2: Set Query Criteria** screen appears.

4. To filter the data that displays, select **Custom criteria**.

5. Specify the **Match** rule for the custom filter.

- **All of the criteria:** Data must match all the specified criteria.
- **Any of the criteria:** Data can match any of the specified criteria.

6. Specify the filtering criteria, each of which consists of three parts:

- **Data type:** Corresponds to a column returned by the data view
- **Operator:** Used to match or exclude data type values
- **Value:** Select criteria from the drop-down controls or specify values in the text boxes

**Note**

The options that display depend on the selected data view, and the selected data type and operator.

Apex Central supports a maximum of 20 filters.

---

7. Add or remove criteria using the plus (+) and minus (-) controls.

8. Click **Next >**.

The **Step 3: Specify Design** screen appears.

9. Specify the **Name** used as the title for the chart.

10. From the **Drag Available Fields** list, drag-and-drop the data that displays in the following locations:

- **Row Field:** Defines how the data is separated horizontally in the table
  - **Column Field:** Defines how the data is separated vertically in the table
  - **Data Field:** Defines the data value that displays for the specified **Row Field** or **Column Field** in the table
- 

**Important**

The **Dynamic Table** report element requires exactly one **Data Field** and either one **Row Field** or one **Column Field**.

---

11. In the **Data Properties** section, configure the following:

- **Data field title:** The label for the data field
- **Aggregated by:** The method in which to display data
  - **Total number of instances:** Includes duplicate results in the data
  - **Number of unique instances:** Displays only one instance of duplicated result types

For example, if an endpoint detects 5 instances of “VirusA” and 3 instances of “VirusB” in the data, the detection count on the graph would display the following values:

- Total number of instances = 8 (virus detections, regardless of virus name)
- Number of unique instances = 2 (unique virus types, regardless of number of occurrences)

**12.** In the **Row Properties** section, configure the following:

- Specify the **Row header title**.
- Select the **Sorting** order and direction.
  - **Aggregation value:** Sorts based on the count value of the data
  - **Header title:** Sorts alphabetically based on the category name
- Select the **Filter summarized result** check box to filter the data that displays in the report.
  - Specify the maximum number of items to display.
  - Enable **Aggregate remaining items** to group all remaining data in the “Others” category.

**13.** In the **Column Properties** section, configure the following:

- Specify the **Column header title**.
- Select the **Sorting** order and direction.
  - **Aggregation value:** Sorts based on the count value of the data
  - **Header title:** Sorts alphabetically based on the category name
- Select the **Filter summarized result** check box to filter the data that displays in the report.
  - Specify the maximum number of items to display.
  - Enable **Aggregate remaining items** to group all remaining data in the “Others” category.



---

**14. Click Save.**

The **Add/Edit Report Template** screen appears with the updated chart settings applied.

---

## Configuring the Grid Table Report Element

This task assumes that you have already added the **Grid Table** report element to a custom report template row.

For more information, see [Adding or Editing Custom Templates on page 18-3](#).

---

### Procedure

1. In the **Grid Table** report element, click **Edit**.

The **Edit Grid Table > Step 1: Data View** screen appears.

2. Select the type of report data you want to display from the **Data Views** directory.

For more information, see [Data Views on page B-1](#).

3. Click **Next >**.

The **Step 2: Set Query Criteria** screen appears.

4. To filter the data that displays, select **Custom criteria**.
5. Specify the **Match** rule for the custom filter.
  - **All of the criteria:** Data must match all the specified criteria.
  - **Any of the criteria:** Data can match any of the specified criteria.
6. Specify the filtering criteria, each of which consists of three parts:
  - **Data type:** Corresponds to a column returned by the data view
  - **Operator:** Used to match or exclude data type values
  - **Value:** Select criteria from the drop-down controls or specify values in the text boxes



**Note**

The options that display depend on the selected data view, and the selected data type and operator.

Apex Central supports a maximum of 20 filters.

---

7. Add or remove criteria using the plus (+) and minus (-) controls.

8. Click **Next >**.

The **Step 3: Specify Design** screen appears.

9. Specify the **Name** used as the title for the chart.

10. Select the data fields to display in the report.

---



**Note**

By default, Apex Central selects all fields for the specified data view.

---

11. Select the **Sorting** order of the **Selected Fields**.

12. Select the **Display quantity** to define the maximum number of items included in the report.

13. Click **Save**.


The **Add/Edit Report Template** screen appears with the updated chart settings applied.

---

## One-time Reports

The **One-time Reports** screen provides a list of all previously generated one-time reports for your network. You can use this screen to create new one-time reports and view previously generated one-time reports.

The following table outlines the available tasks on the **One-time Reports** screen.

| TASK   | DESCRIPTION  |
|--|--|
| Add new one-time reports                     | Click <b>Add</b> to create a new one-time report.<br>For more information, see <a href="#">Creating One-time Reports on page 18-21</a> .   |
| Delete one-time reports                      | Select an existing one-time report and click <b>Delete</b> .   |
| Forward one-time reports to email recipients | Select an existing one-time report and click <b>Forward</b> to email the report as an attachment to specified recipients.  |
| View generated one-time reports              | Click the <b>View</b> link in the <b>View</b> column of the report you want to view.   |
| View one-time report profiles                | Click the <b>Name</b> of a previously generated one-time report to view the report profile.<br><br><hr/>  <b>Note</b><br>You cannot edit the profiles of previously generated one-time reports. |

## Creating One-time Reports

Use the **One-time Reports** screen to generate reports on demand. When creating reports, specify whether to use custom or static templates.

### Procedure

1. Go to **Detections > Reports > One-time Reports**.

The **One-time Reports** screen appears.

2. Click **Add**.

The **Add One-Time Report > Step 1: Contents** screen appears.

3. Type a name for the report in the **Name** field.
4. (Optional) Type a description for the report in the **Description** field.

5. In the **Report Content** section, select one of the following template types:

- **Custom Templates:** Select one or more custom report templates.

**Note**

Selecting multiple custom templates generates a single report that displays formatted data from all selected templates.

For more information about creating custom report templates, see [Adding or Editing Custom Templates on page 18-3](#).

---

- **Static Templates:** Select one or more of the static templates provided by Trend Micro.
    - a. Select a static template from the **Report category** drop-down.
    - b. Select the data to display in the report and specify any corresponding parameters.
6. Select the report generation format.
    - Custom template report formats:
      - Adobe PDF format (\*.pdf)
      - HTML format (\*.html)
      - XML format (\*.xml)
      - CSV format (\*.csv)
    - Static template report formats:
      - Adobe PDF format (\*.pdf)
      - Microsoft Word format (\*.docx)
      - Microsoft Excel format (\*.xlsx)
  7. Click **Next**.

The **Add One-Time Report > Step 2: Targets** screen appears.

8. Specify targets using one of the following views.
  - **Product Directory:** Select the managed products or folders containing the managed products that provide the report information.
  - **Tags and filters:** Select up to 10 custom tags, filters, or important labels containing the users or endpoints that provide the report information.

**Note**

- The **Tags and filters** view is only available for custom report templates.
  - Reports generated by a user account only include data from endpoints that the user account is authorized to view. If a user account selects a tag, filter, or importance label containing endpoints that the user account does not have permission to view, then the generated report excludes data from the unauthorized endpoints.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
- 
9. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
    - **All clients:** Generates reports from all Network VirusWall Enforcer devices
    - **IP range:** Generates reports from a specific IP address range
    - **Segment:** Generates reports from a specific network segment

**10. Click Next.**

The **Add One-Time Report > Step 3: Time Period** screen appears.

**11. Specify the time period for the report.**

**12. Click Next.**

The **Add One-Time Report > Step 4: Message Content and Recipients** screen appears.

**13. (Optional) Email the report as an attachment to selected recipients.**

- a.** In the **Subject** field, type a title for the email message that contains the report.
- b.** In the **Message** field, type a description about the report.
- c.** Select **Email the report as an attachment** to send the report to selected recipients.
- d.** Select contact groups or user accounts.
- e.** Click >>.

The selected contact groups or user accounts appear in the Recipient list.

**14. Click Finish.**

The **One-time Reports** screen appears and displays the newly added report generation task.

**15. To view a generated report:**

- a.** Click the **View** link in the **View** column for the generated report you want to view.
- b.** Open or save the generated report file.

---

## Viewing One-Time Reports

Use the **One-time Reports** screen to view previously generated one-time reports.

---

## Procedure

1. Go to **Detections > Reports > One-time Reports**.

The **One-time Reports** screen appears.




2. Click the **View** link in the **View** column for the generated report you want to view.
  3. Open or save the generated report file.
- 

## Scheduled Reports

The **Scheduled Reports** screen provides a list of all reports that automatically generate on a user-defined schedule. You can use this screen to view basic information about previously configured scheduled reports, add new scheduled reports, and enable/disable scheduled reports.

The following table outlines the available tasks on the **Scheduled Reports** screen.

| TASK                              | DESCRIPTION   |
|-----------------------------------|---|
| Add new scheduled report profiles | Click <b>Add</b> to create a new scheduled report profile.<br>For more information, see <a href="#">Adding Scheduled Reports on page 18-26</a> .  |
| Edit scheduled report profiles    | Click the <b>Name</b> of an existing scheduled report profile to edit.<br>For more information, see <a href="#">Editing Scheduled Reports on page 18-31</a> .   |
| Copy scheduled report profiles    | Select one or more existing scheduled report profiles and click <b>Copy</b> to replicate the selected profiles.<br><br>Click the <b>Name</b> of a copied scheduled report profile to edit.<br>For more information, see <a href="#">Editing Scheduled Reports on page 18-31</a> . |
| Delete scheduled report profiles  | Select existing scheduled report profiles and click <b>Delete</b> .   |

| TASK  | DESCRIPTION   |
|---|---|
| View previously generated scheduled reports | <p>Click the <b>View</b> link in the <b>History</b> column for the report you want to view.</p> <p>For more information, see <a href="#">Viewing Scheduled Reports on page 18-35</a>.</p>   |
| Enable or disable scheduled reports         | <ul style="list-style-type: none"> <li>• To disable a scheduled report, click the enabled () icon in the <b>Enable</b> column.</li> <li>• To enable a scheduled report, click the disabled () icon in the <b>Enable</b> column.</li> </ul> <hr/> <p> <b>Note</b><br/>Newly added scheduled report profiles are enabled by default.</p> |

## Adding Scheduled Reports

Use the **Scheduled Reports** screen to automatically generate reports on a user-defined schedule. When adding scheduled reports, specify whether to use custom or static templates.

### Procedure

1. Go to **Detections > Reports > Scheduled Reports**.

The **Scheduled Reports** screen appears.

2. Click **Add**.

The **Add Scheduled Report > Step 1: Contents** screen appears.

3. Type a name for the report in the **Name** field.
4. (Optional) Type a description for the report in the **Description** field.
5. In the **Report Content** section, select one of the following template types:

- **Custom Templates:** Select one or more custom report templates.



**Note**

Selecting multiple custom templates generates a single report that displays formatted data from all selected templates.

For more information about creating custom report templates, see [Adding or Editing Custom Templates on page 18-3](#).

---

- **Static Templates:** Select one or more of the static templates provided by Trend Micro.
  - a. Select a static template from the **Report category** drop-down.
  - b. Select the data to display in the report and specify any corresponding parameters.
- 6. Select the report generation format.
  - Custom template report formats:
    - Adobe PDF format (\*.pdf)
    - HTML format (\*.html)
    - XML format (\*.xml)
    - CSV format (\*.csv)
  - Static template report formats:
    - Adobe PDF format (\*.pdf)
    - Microsoft Word format (\*.docx)
    - Microsoft Excel format (\*.xlsx)
- 7. Click **Next**.

The **Add Scheduled Report > Step 2: Targets** screen appears.
- 8. Specify targets using one of the following views.
  - **Product Directory:** Select the managed products or folders containing the managed products that provide the report information.

- **Tags and filters:** Select up to 10 custom tags, filters, or important labels containing the users or endpoints that provide the report information.

**Note**

- The **Tags and filters** view is only available for custom report templates.
  - Reports generated by a user account only include data from endpoints that the user account is authorized to view. If a user account selects a tag, filter, or importance label containing endpoints that the user account does not have permission to view, then the generated report excludes data from the unauthorized endpoints.
  - Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.
- 
9. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
    - **All clients:** Generates reports from all Network VirusWall Enforcer devices
    - **IP range:** Generates reports from a specific IP address range
    - **Segment:** Generates reports from a specific network segment
  10. Click **Next**.

The **Add Scheduled Report > Step 3: Frequency** screen appears.
  11. Specify how often the reports generate:

- **Every 'n' days:** Reports generate every 1 to 6 days, depending on your selection.
- **Weekly:** Reports generate weekly on the specified day.
- **Bi-weekly:** Reports generate every two weeks on the specified day.
- **Monthly:** Reports generate monthly on the first, 5th, 10th, 15th, 20th, 25th, or the last day of the month.

12. Specify the data range:

- **Reports include data up to the Start the schedule time specified below:** This means that a report could have up to 23 hours more data contained in the report. While this has a small affect on weekly or monthly reports, this can make a "daily" report with almost two days worth of data depending on the Start schedule time.
- **Reports include data up to 23:59:59 of the previous day:** This means that data collection for the report stops just before midnight. Reports will be an exact time period (example: Daily reports will be 24 hours) but will not contain the absolute latest data.

13. Specify when the report schedule starts:

- **Immediately:** The report schedule starts immediately after enabling the report.
- **Start on:** The report schedule starts on the date and time specified in the accompanying fields.



**Tip**

Click the calendar icon next to the **mm/dd/yyyy** field to use a dynamic calendar to specify the date range.

---

14. Click **Next**.

The **Add Scheduled Report > Step 4: Message Content and Recipients** screen appears.

15. (Optional) Email the report as an attachment to selected recipients.

- a. In the **Subject** field, type a title for the email message that contains the report.
- b. In the **Message** field, type a description about the report.
- c. Select **Email the report as an attachment** to send the report to selected recipients.
- d. Select contact groups or user accounts.
- e. Click >>.

The selected contact groups or user accounts appear in the Recipient list.

**16. Click Finish.**

The **Scheduled Reports** screen appears and displays the newly added report generation task.



**Note**

By default, Apex Central enables newly added scheduled reports.

---

**17. To view a generated report:**

- a. Click the **View** link in the **History** column for the scheduled report you want to view.

The **Scheduled Report History** screen appears.

- b. Click the **View** link in the **View** column for the generated report you want to view.



**Tip**

If the scheduled report has not been generated, click the **Generate** button to create a quick report based on the scheduled report settings.

---

- c. Open or save the generated report file.
-

## Editing Scheduled Reports

Use the **Scheduled Reports** screen to automatically generate reports on a user-defined schedule. When adding scheduled reports, specify whether to use custom or static templates.

---

### Procedure

1. Go to **Detections > Reports > Scheduled Reports**.

The **Scheduled Reports** screen appears.

2. Click the **Name** of a scheduled report profile.

The **Edit Scheduled Report > Step 1: Contents** screen appears.

3. Type a name for the report in the **Name** field.
4. (Optional) Type a description for the report in the **Description** field.
5. In the **Report Content** section, select one of the following template types:

- **Custom Templates:** Select one or more custom report templates.



#### Note

Selecting multiple custom templates generates a single report that displays formatted data from all selected templates.

For more information about creating custom report templates, see [Adding or Editing Custom Templates on page 18-3](#).

---

- **Static Templates:** Select one or more of the static templates provided by Trend Micro.
    - a. Select a static template from the **Report category** drop-down.
    - b. Select the data to display in the report and specify any corresponding parameters.
6. Select the report generation format.

- Custom template report formats:
  - Adobe PDF format (\*.pdf)
  - HTML format (\*.html)
  - XML format (\*.xml)
  - CSV format (\*.csv)
- Static template report formats:
  - Adobe PDF format (\*.pdf)
  - Microsoft Word format (\*.docx)
  - Microsoft Excel format (\*.xlsx)

7. Click **Next**.

The **Edit Scheduled Report > Step 2: Targets** screen appears.

8. Specify targets using one of the following views.

- **Product Directory:** Select the managed products or folders containing the managed products that provide the report information.
- **Tags and filters:** Select up to 10 custom tags, filters, or important labels containing the users or endpoints that provide the report information.

**Note**

- The **Tags and filters** view is only available for custom report templates.
- Reports generated by a user account only include data from endpoints that the user account is authorized to view. If a user account selects a tag, filter, or importance label containing endpoints that the user account does not have permission to view, then the generated report excludes data from the unauthorized endpoints.
- Editing a tag, filter, or importance label on the **User/Endpoint Directory** screen also modifies the corresponding tag, filter, or importance label used by log queries and reports. For example, if the an endpoint is removed from a custom filter on the **User/Endpoint Directory** screen, then log queries and generated reports that use the filter will exclude data from the removed endpoint.

9. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
  - **All clients:** Generates reports from all Network VirusWall Enforcer devices
  - **IP range:** Generates reports from a specific IP address range
  - **Segment:** Generates reports from a specific network segment

10. Click **Next**.

The **Edit Scheduled Report > Step 3: Frequency** screen appears.

11. Specify how often the reports generate:
  - **Every 'n' days:** Reports generate every 1 to 6 days, depending on your selection.
  - **Weekly:** Reports generate weekly on the specified day.

- **Bi-weekly:** Reports generate every two weeks on the specified day.
- **Monthly:** Reports generate monthly on the first, 5th, 10th, 15th, 20th, 25th, or the last day of the month.

12. Specify the data range:

- **Reports include data up to the Start the schedule time specified below:** This means that a report could have up to 23 hours more data contained in the report. While this has a small affect on weekly or monthly reports, this can make a "daily" report with almost two days worth of data depending on the Start schedule time.
- **Reports include data up to 23:59:59 of the previous day:** This means that data collection for the report stops just before midnight. Reports will be an exact time period (example: Daily reports will be 24 hours) but will not contain the absolute latest data.

13. Specify when the report schedule starts:

- **Immediately:** The report schedule starts immediately after enabling the report.
- **Start on:** The report schedule starts on the date and time specified in the accompanying fields.



**Tip**

Click the calendar icon next to the **mm/dd/yyyy** field to use a dynamic calendar to specify the date range.

---

14. Click **Next**.

The **Edit Scheduled Report > Step 4: Message Content and Recipients** screen appears.

15. (Optional) Email the report as an attachment to selected recipients.

- a. In the **Subject** field, type a title for the email message that contains the report.
- b. In the **Message** field, type a description about the report.



- c. Select **Email the report as an attachment** to send the report to selected recipients.
- d. Select contact groups or user accounts.
- e. Click >>.

The selected contact groups or user accounts appear in the Recipient list.

**16. Click Finish.**

The **Scheduled Reports** screen appears and displays the newly added report generation task.

---

## Viewing Scheduled Reports

Use the **Scheduled Reports** screen to view previously generated scheduled reports.

---

### Procedure

**1. Go to **Detections > Reports > Scheduled Reports.****

The **Scheduled Reports** screen appears.

**2. Click the **View** link in the **History** column for the scheduled report you want to view.**

The **Scheduled Report History** screen appears.

**3. Click the **View** link in the **View** column for the generated report you want to view.**



**Tip**

If the scheduled report has not been generated, click the **Generate** button to create a quick report based on the scheduled report settings.

---

**4. Open or save the generated report file.**

---

## Configuring Report Maintenance

Configure **Report Maintenance** settings to delete reports when a maximum number of reports is reached.

---

### Procedure

1. Go to **Detections > Reports > Report Maintenance**.

The **Report Maintenance** screen appears.

2. Specify the maximum number of one-time and scheduled reports to keep.
  3. Click **Save**.
- 

## Viewing My Reports

The **My Reports** screen provides a list of all the reports generated by the current user. You can also view reports generated by other users belonging to the same groups as the current user.

---

### Procedure

1. Go to **Detections > Reports > My Reports**.

The **My Reports** screen appears.

2. Click the **View** link in the **View** column for the generated report you want to view.
  3. Open or save the generated report file.
-

# Chapter 19

## Data Loss Prevention Incidents

Apex Central provides the capability for DLP compliance officers and incident reviewers to review and update incident information.


Topics include:

- *Administrator Tasks on page 19-2*
- *DLP Incident Review Process on page 19-6*

## Administrator Tasks

To enable the incident review process, Apex Central administrators need to complete some prerequisite tasks. The following table lists the required tasks and references:

**TABLE 19-1. Administrator Tasks**

| TASK   | REFERENCES  |
|--|---|
| Set up manager information in Active Directory.  | <a href="#">Setting Up Manager Information in Active Directory Users on page 19-3</a>   |
| Set up Active Directory integration to obtain user information.  | <a href="#">Active Directory and Compliance Settings on page 6-1</a>  |
| <p>Create user accounts specific for DLP incident investigation.</p> <p>You can assign the following user roles to grant permission to review DLP incidents:</p> <ul style="list-style-type: none"> <li>• Administrator and DLP Compliance Officer</li> <li>• DLP Compliance Officer</li> <li>• DLP Incident Reviewer</li> </ul> <hr/> <p> <b>Note</b><br/>The DLP Compliance Officer and DLP Incident Reviewer roles are only available to Active Directory users.</p> | <ul style="list-style-type: none"> <li>• <a href="#">Understanding DLP User Roles on page 19-3</a></li> <li>• <a href="#">Default User Roles on page 4-17</a></li> <li>• <a href="#">Adding a User Account on page 4-5</a></li> </ul> |
| Set up the <b>Scheduled incident summary</b> and <b>Incident details updated</b> notifications.  | <ul style="list-style-type: none"> <li>• <a href="#">Scheduled Incident Summary on page 17-34</a></li> <li>• <a href="#">Incident Details Updated on page 17-33</a></li> </ul>  |
| Export DLP logs for auditing purposes.   | <a href="#">Querying Logs on page 16-2</a>  |

## Setting Up Manager Information in Active Directory Users

For managers to investigate DLP incidents, set up the manager information in each Active Directory user.

---

### Procedure

1. Open the Active Directory Users and Computers console. Click **Start > Administrative Tools > Active Directory Users and Computers**.

The **Active Directory Users and Computers** console appears.

2. Double-click a user.

The **<user> Properties** screen appears.

3. Click the **Organization** tab and then click **Change...**

The **Select User or Contact** screen appears.

4. Specify the manager information and click **OK**.

5. To verify the manager-user relationship, open the manager's **<user> Properties** screen, click the **Organization** tab, and check the user information under **Direct reports**.

---

## Understanding DLP User Roles

Apex Central provides the following Data Loss Prevention (DLP) user roles:

- Administrator and DLP Compliance Officer
- DLP Compliance Officer
- DLP Incident Reviewer







### Note

You can only assign the “DLP Compliance Officer” and “DLP Incident Reviewer” roles to Active Directory user accounts.

---

The following table describes the features and characteristics related to the DLP user roles:

| FEATURE        | ROLE                                     | DESCRIPTION   |
|----------------|--|---|
| DLP logs       | Administrator and DLP Compliance Officer | <ul style="list-style-type: none"> <li>View DLP log data for all Active Directory users</li> <li>Access specific widgets that display DLP incident information</li> </ul>   |
|                | DLP Compliance Officer                   | <ul style="list-style-type: none"> <li>Access limited to DLP logs related to directly managed users</li> </ul>  |
|                | DLP Incident Reviewer                    | <ul style="list-style-type: none"> <li>Access specific widgets that display DLP incident information</li> </ul>   |
| Incident scope | Administrator and DLP Compliance Officer | <ul style="list-style-type: none"> <li>View DLP incident data for all Active Directory users by clicking the settings icon (  &gt;  ) on any of the following <b>Data Loss Prevention</b> widgets and selecting <b>All managed users</b> for the <b>Scope</b>.</li> </ul>   |
|                | DLP Compliance Officer                   | <ul style="list-style-type: none"> <li>DLP Incidents by Severity and Status</li> <li>DLP Incident Trends by User</li> <li>DLP Incidents by User</li> </ul> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>By default, the scope for each <b>Data Loss Prevention</b> widget only allows this role to view incident data for <b>Directly managed users</b>.</li> <li>Changing the <b>Scope</b> for one <b>Data Loss Prevention</b> widget does not affect the scope of any other widget.</li> </ul> <hr/> <ul style="list-style-type: none"> <li>On all other screens: <ul style="list-style-type: none"> <li>User accounts assigned with the “Administrator and DLP Compliance Officer” role can view data from all Active Directory users reported by managed products according to the user account's product scope</li> <li>The “DLP Compliance Officer” role cannot view any data</li> </ul> </li> </ul> |

| FEATURE                                 | ROLE                                     | DESCRIPTION   |
|---|--|---|
|   | DLP Incident Reviewer                    | View DLP incident data for directly managed users   |
| Menu access                             | Administrator and DLP Compliance Officer | Access the <b>Data Loss Prevention</b> tab and the following widgets: <ul style="list-style-type: none"> <li>• DLP Incidents by Severity and Status</li> <li>• DLP Incident Trends by User</li> <li>• DLP Incidents by User</li> </ul> For more information, see <a href="#">Data Loss Prevention Tab on page 3-27</a> .  |
|   | DLP Compliance Officer                   |   |
|   | DLP Incident Reviewer                    |   |
| Scheduled incident summary notification | Administrator and DLP Compliance Officer | Receive the following: <ul style="list-style-type: none"> <li>• Daily or weekly email notification</li> <li>• Summary list of incident count by severity level</li> <li>• Link to the Apex Central web console</li> </ul>   |
|   | DLP Compliance Officer                   |   |
|   | DLP Incident Reviewer                    |   |
| Incident details updated notification   | Administrator and DLP Compliance Officer | Receive notification of changes to incident status or comments <hr/> <div style="display: flex; align-items: flex-start;">  <div> <p><b>Note</b></p> <p>The “DLP Incident Reviewer” role does not receive this notification.</p> </div> </div> <hr/> |
|   | DLP Compliance Officer                   |   |

## Creating DLP Auditing Logs

Administrators can use log queries to generate and export DLP auditing logs. Perform a log query as described in [Querying Logs on page 16-2](#) and configure the following:

- Log type: Select **User Access**

- Advanced filters: Add the following activities (**Activity**) to custom criteria:
  - Download DLP incident file
  - Update DLP incident

## DLP Incident Review Process

Once Apex Central administrators have completed the prerequisite tasks, the reviewers can start the incident review process. The following table lists the tasks and references:

**TABLE 19-2. DLP Incident Review Process**

| TASK   | DESCRIPTION  |
|--|--|
| Receive the scheduled incident summary notification message  | Apex Central summarizes and sends email notifications to the incident reviewers daily or weekly. |
| Review details about the incident using one of the following methods: <ul style="list-style-type: none"> <li>• Click the link provided in the message to log on to the Apex Central web console</li> <li>• Open the attachment (if available)</li> </ul> | <a href="#">Understanding the Incident Information List on page 19-6</a>                         |
| Update the incident status and provide comments  | <a href="#">Reviewing Incident Details on page 19-8</a>  |




## Understanding the Incident Information List

The **Incident Information** screen displays a list of incidents manageable for the reviewer. Incident reviewers can use this screen to do the following:

- View incident summary
- Take actions on incidents
- Export incident details





**TABLE 19-3. Incident Information List**



| ITEM     | DESCRIPTION   |
|----------|---|
| ID       | Unique incident ID  |
| Received | <p>Date and time when Apex Central received incident data</p> <hr/> <p> <b>Note</b><br/>After receiving DLP logs from managed products, Apex Central needs 30 minutes to process the logs before incident reviewers can view the data.</p> <hr/> |
| Severity | <p>Severity level of the incident</p> <hr/> <p> <b>Note</b><br/>Once Apex Central receives and processes a DLP incident, Apex Central does not update the severity level if changes occur in the managed product.</p> <hr/>                      |
| Policy   | <p>Name of the Apex Central policy that triggered the incident</p> <hr/> <p> <b>Note</b><br/>For incidents triggering DLP policies created in managed products, this appears as <b>N/A</b>.</p> <hr/>  |
| User     | Name of the user who triggered the incident   |
| Manager  | Name of the user's manager  |
| Status   | <p>Current status of the incident</p> <ul style="list-style-type: none"> <li>• New</li> <li>• Under Investigation</li> <li>• Escalated</li> <li>• Closed</li> </ul>   |
| Action   | Action available for managing the incident  |

## Reviewing Incident Details

By clicking the **Edit** icon in the **Action** column of the **Incident Information** screen, the **Incident Details** screen appears displaying detailed information about the incident. DLP incident reviewers can use this screen to update the incident status and provide comments on the incident.

**TABLE 19-4. Incident Details**

| ITEM     | DESCRIPTION  |
|----------|--|
| ID       | Unique incident ID   |
| Status   | Use this to update the review status of the incident.<br>Available options: <ul style="list-style-type: none"> <li>• <b>New</b></li> <li>• <b>Under Investigation</b></li> <li>• <b>Escalated</b></li> <li>• <b>Closed</b></li> </ul>  |
| Severity | Severity level of the incident<br><hr/>  <b>Note</b><br>Once Apex Central receives and processes a DLP incident, Apex Central does not update the severity level if changes occur in the managed product. |
| Policy   | Name of the Apex Central policy that triggered the incident<br><hr/>  <b>Note</b><br>For incidents triggering DLP policies created in managed products, this appears as <b>N/A</b> .                    |
| Rule     | Names of the rules from that triggered the incident  |

| ITEM               | DESCRIPTION   |
|--------------------|---|
| Received           | <p>Date and time when Apex Central received incident data</p> <hr/> <p> <b>Note</b><br/>After receiving DLP logs from managed products, Apex Central needs 30 minutes to process the logs before incident reviewers can view the data.</p> <hr/> |
| Generated          | Date and time the incident occurred in the managed product  |
| User               | Name of the user who triggered the incident   |
| Manager            | Name of the user's manager  |
| Endpoint           | Source host name  |
| IP address         | Source IP address   |
| Sender             | Source email address  |
| Subject            | Subject of the email message  |
| Recipient          | Destination email address   |
| Destination        | Intended destination of the file containing the digital asset or channel (if no source is available)  |
| Last modified date | Date and time of the last modification to the asset   |
| Last modified by   | Name of the user who last modified the asset  |
| Template           | Names of the templates that triggered the incident  |
| File               | <p>Name or link to the file that triggered the incident</p> <hr/> <p> <b>Note</b><br/>The file is quarantined in the managed product.</p> <hr/>  |
| SHA-1              | Hash information of the file  |
| Channel            | Channel through which the transmission occurred   |

| <b>ITEM</b>               | <b>DESCRIPTION</b>   |
|---------------------------|--|
| Action                    | Actions taken on the incident                                      |
| User justification reason | User-defined reasons for allowing users to transfer sensitive data |
| Matching content          | Digital assets that triggered the incident                         |
| Comments                  | User-defined notes about the incident                              |

# **Part VI**

## **Threat Intelligence and Response**





# Chapter 20

## Connected Threat Defense

This section discusses how to detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage.

Topics include:

- *About Connected Threat Defense on page 20-2*
- *Feature Requirements on page 20-2*
- *Suspicious Object List Management on page 20-5*
- *Preemptive Protection Against Suspicious Objects on page 20-20*
- *Connected Threat Defense Product Integration on page 20-37*


## About 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.


For more information, see [Connected Threat Defense Product Integration](#).

## Feature Requirements


The following table lists the features available with the Connected Threat Defense architecture and the required and optional products that integrate with each.

| FEATURE                    | REQUIRED PRODUCTS  | OPTIONAL PRODUCTS   |
|----------------------------|--|---|
| Security threat monitoring | <ul style="list-style-type: none"> <li>• Apex Central</li> <li>• Deep Discovery Inspector 5.0 (or later) or one of the following Virtual Analyzer products:               <ul style="list-style-type: none"> <li>• <a href="#">Apex One Sandbox as a Service</a></li> <li>• <a href="#">Deep Discovery Analyzer</a></li> </ul> </li> </ul> <hr/> <div style="display: flex; align-items: center;">  <div> <p><b>Important</b></p> <p>At least one optional product is required to evaluate log data.</p> </div> </div> <hr/> | <ul style="list-style-type: none"> <li>• Apex One 2019 or OfficeScan 11.0 SP1 (or later)</li> <li>• Apex One Endpoint Sensor</li> <li>• Cloud App Security 5.0 (or later)</li> <li>• Deep Security Manager 10.0 (or later)</li> <li>• InterScan Messaging Security Virtual Appliance 9.1 (or later)</li> <li>• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (or later)</li> <li>• ScanMail for Microsoft Exchange 12.5 (or later)</li> <li>• Trend Micro Endpoint Application Control 2.0 SP1 (or later)</li> </ul> |



| FEATURE   | REQUIRED PRODUCTS  | OPTIONAL PRODUCTS   |
|---|--|---|
| <p>Suspicious Object list synchronization</p> <p>For more information, see <a href="#">Suspicious Object Lists on page 20-6</a> and <a href="#">Connected Threat Defense Product Integration on page 20-37</a>.</p> | <ul style="list-style-type: none"> <li>• Apex Central</li> <li>• Deep Discovery Inspector 5.0 (or later) or one of the following Virtual Analyzer products:                             <ul style="list-style-type: none"> <li>• <a href="#">Apex One Sandbox as a Service</a></li> <li>• <a href="#">Deep Discovery Analyzer</a></li> </ul> </li> </ul> <hr/> <p> <b>Important</b><br/>At least one optional product is required for Suspicious Object list synchronization.</p> <hr/> | <ul style="list-style-type: none"> <li>• Apex One 2019 or OfficeScan 11.0 SP1 (or later)</li> <li>• Cloud App Security 5.0 (or later)</li> <li>• Deep Discovery Director</li> <li>• Deep Security Manager 10.0 (or later)</li> <li>• InterScan Messaging Security Virtual Appliance 9.1 (or later)</li> <li>• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (or later)</li> <li>• Smart Protection Server 3.3 Patch 2 (or later)</li> <li>• Trend Micro Endpoint Application Control 2.0 SP1 (or later)</li> </ul> |
| <p>Suspicious Object sample submission</p>  | <ul style="list-style-type: none"> <li>• Deep Discovery Inspector 5.0 (or later) or one of the following Virtual Analyzer products:                             <ul style="list-style-type: none"> <li>• <a href="#">Apex One Sandbox as a Service</a></li> <li>• <a href="#">Deep Discovery Analyzer</a></li> </ul> </li> </ul>   | <ul style="list-style-type: none"> <li>• Apex One 2019 or OfficeScan 11.0 SP1 (or later)</li> <li>• Apex One Endpoint Sensor</li> <li>• Deep Discovery Email Inspector 3.0 (or later)</li> <li>• Deep Security Manager 10.0 (or later)</li> <li>• InterScan Messaging Security Virtual Appliance 9.1 (or later)</li> <li>• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (or later)</li> <li>• ScanMail for Microsoft Exchange 12.5 (or later)</li> </ul>  |

| FEATURE   | REQUIRED PRODUCTS  | OPTIONAL PRODUCTS  |
|---|--|--|
| Suspicious Object management  | <ul style="list-style-type: none"> <li>• Apex Central</li> <li>• Deep Discovery Inspector 5.0 (or later) or one of the following Virtual Analyzer products:               <ul style="list-style-type: none"> <li>• <a href="#">Apex One Sandbox as a Service</a></li> <li>• <a href="#">Deep Discovery Analyzer</a></li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Apex One 2019 or OfficeScan 11.0 SP1 (or later)</li> <li>• Apex One Endpoint Sensor</li> <li>• Cloud App Security 5.0 (or later)</li> <li>• Deep Security Manager 10.0 (or later)</li> <li>• InterScan Messaging Security Virtual Appliance 9.1 (or later)</li> <li>• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (or later)</li> <li>• Trend Micro Endpoint Application Control 2.0 SP1 (or later)</li> </ul>                       |
| Suspicious Object scan actions<br><br>For more information, see <a href="#">Suspicious Object Scan Actions on page 20-9</a> . | <ul style="list-style-type: none"> <li>• Apex Central</li> </ul>   | <ul style="list-style-type: none"> <li>• Apex One 2019 or OfficeScan 11.0 SP1 (or later)</li> <li>• Cloud App Security 5.0 (or later)</li> <li>• Deep Security Manager 10.0 (or later)</li> <li>• InterScan Messaging Security Virtual Appliance 9.1 (or later)</li> <li>• InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (or later)</li> <li>• Smart Protection Server 3.3 Patch 2 (or later)</li> <li>• Trend Micro Endpoint Application Control 2.0 SP1 (or later)</li> </ul> |

| FEATURE  | REQUIRED PRODUCTS   | OPTIONAL PRODUCTS   |
|--|---|---|
| Impact analysis  | <ul style="list-style-type: none"> <li>• Apex Central</li> <li>• Apex One Endpoint Sensor</li> </ul> <hr/>  <b>Important</b><br>Performing an impact analysis on <b>Affected Users</b> screen also requires Deep Discovery Inspector 5.0 (or later).<br><br>For more information, see <a href="#">Analyzing Impact on Affected Users on page 7-22.</a> | <ul style="list-style-type: none"> <li>• Deep Discovery Inspector 5.0 (or later)</li> </ul> |
| Endpoint isolation<br><br>For more information, see <a href="#">Isolating Endpoints on page 20-34.</a> | <ul style="list-style-type: none"> <li>• Apex Central</li> <li>• Apex One 2019 or OfficeScan 11.0 SP1 (or later)</li> </ul>   | <ul style="list-style-type: none"> <li>• Apex One Endpoint Sensor</li> </ul>                |
| IOC management   | <ul style="list-style-type: none"> <li>• Apex Central</li> <li>• Apex One Endpoint Sensor</li> </ul>  | <ul style="list-style-type: none"> <li>• None</li> </ul>                                    |

## Suspicious Object List Management

Apex Central allows you to synchronize Suspicious Object lists among managed products and create User-Defined and Exception lists to further control the spread of suspicious objects. You can also configure specific actions that supported managed products take upon detecting suspicious objects in your environment.

Apex Central consolidates Virtual Analyzer and user-defined suspicious object lists (excluding exceptions) and synchronizes the lists with integrated managed products.

For more information about products that can synchronize Suspicious Objects lists with Apex Central, see *Suspicious Object list synchronization in Feature Requirements on page 20-2*.

## Suspicious Object Lists

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



### Note

Administrators can configure specific scan actions on suspicious objects using the Apex Central console. You can then configure certain managed products to perform actions based on the Suspicious Object list settings.

For more information, see *Suspicious Object Scan Actions on page 20-9*.

| LIST TYPE                           | DESCRIPTION  |
|-------------------------------------|--|
| Virtual Analyzer Suspicious Objects | <p>Managed products that integrate with a Virtual Analyzer submit suspicious files or URLs to Virtual Analyzer for analysis. If Virtual Analyzer determines that an object is a possible threat, Virtual Analyzer adds the object to the Suspicious Object list. Virtual Analyzer then sends the list to its registered Apex Central server for consolidation and synchronization purposes.</p> <p>On the Apex Central console, go to the <b>Threat Intel &gt; Virtual Analyzer Suspicious Objects &gt; Objects</b> tab to view the Virtual Analyzer Suspicious Objects list.</p> <p>For more information, see <i>Suspicious Object Detection on page 20-15</i>.</p> |

| LIST TYPE  | DESCRIPTION  |
|--|--|
| <p>Exceptions to Virtual Analyzer Suspicious Objects</p> | <p>From the list of Virtual Analyzer suspicious objects, Apex Central administrators can select objects that are considered safe and then add them to an exception list.</p> <p>On the Apex Central console, go to the <b>Threat Intel &gt; Virtual Analyzer Suspicious Objects &gt; Exceptions</b> tab to view the Virtual Analyzer Suspicious Object Exceptions list.</p> <p>Apex Central sends the exception list to the Virtual Analyzers (except for Apex One Sandbox as a Service) that subscribe to the list. When a Virtual Analyzer detects a suspicious object that is in the exception list, the Virtual Analyzer considers the object as “safe” and does not analyze the object again.</p> <p>For more information, see <a href="#">Adding Exceptions to the Virtual Analyzer Suspicious Object List on page 20-7</a>.</p> |
| <p>User-Defined Suspicious Objects</p>                   | <p>Apex Central administrators can add objects they consider suspicious but are not currently in the list of Virtual Analyzer suspicious objects by going to the <b>Threat Intel &gt; Custom Intelligence &gt; User-Defined Suspicious Objects</b>.</p> <p>For more information, see <a href="#">Preemptive Protection Against Suspicious Objects on page 20-20</a>.</p>   |

## Adding Exceptions to the Virtual Analyzer Suspicious Object List

Apex Central allows you to exclude objects from the Virtual Analyzer Suspicious Object list based on the file SHA-1, domain, IP address, or URL.



### Important

The User-Defined Suspicious Object list has a higher priority than the Virtual Analyzer Suspicious Object list.


## Procedure


1. Go to **Threat Intel > Virtual Analyzer Suspicious Objects**.

The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Exceptions** tab.
3. Click **Add**.
4. Specify the **Type** of object.
  - **File:** Specify the **File SHA-1** hash value for the file.
  - **IP address:** Specify the IP address.
  - **URL:** Specify the URL.
  - **Domain:** Specify the domain.

Apex Central allows you to use a wildcard character (\*) to exclude specific subdomains or subdirectories from the Virtual Analyzer Suspicious Object list.

| EXAMPLE               | DESCRIPTION   |
|-----------------------|---|
| https://*.domain.com/ | <p>Excludes all URLs within subdomains of the domain “domain.com” from the Virtual Analyzer Suspicious Object list</p> <hr/> <p> <b>Important</b><br/>If a URL contains a subdirectory, then the URL will not be excluded even if the URL contains a matching subdomain. For example, “https://abc.domain.com/abc” will not be excluded.</p> |
| *.abc.domain.com      | Excludes all subdomains of the subdomain “abc” from the Virtual Analyzer Suspicious Object list   |

| EXAMPLE                        | DESCRIPTION  |
|--------------------------------|--|
| https://<br>*.domain.com/abc/* | <p data-bbox="672 251 1169 365">Excludes all URLs within subdomains of the domain “domain.com” and all subdirectories of the subdirectory “abc” from the Virtual Analyzer Suspicious Object list</p> <hr data-bbox="672 397 1169 399"/> <p data-bbox="672 414 1169 576">  <b>Important</b><br/>           If a URL does not contain a subdirectory within subdirectory “abc”, then the URL will still be excluded. For example, “https://abc.domain.com/abc” will be excluded.         </p> |

5. (Optional) Specify a **Note** to assist in identifying the suspicious object.
6. Click **Add**.

The object appears in the Virtual Analyzer Exception list. Managed products that subscribe to the suspicious objects lists receive the new object information during the next synchronization.

## Suspicious Object Scan Actions



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

**TABLE 20-1. Scan Action Product Support**

| PRODUCT                               | VIRTUAL ANALYZER LIST   | USER-DEFINED LIST  |
|---------------------------------------|---|--|
| Apex One (any version)                | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>IP address:</b> Log, Block</li> <li>• <b>URL:</b> Log, Block</li> <li>• <b>Domain:</b> Log, Block</li> </ul> | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>File SHA-1:</b> Log, Block</li> <li>• <b>IP address:</b> Log, Block</li> <li>• <b>URL:</b> Log, Block</li> <li>• <b>Domain:</b> Log, Block</li> </ul> |
| OfficeScan XG SP1 (or later)          | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>IP address:</b> Log, Block</li> <li>• <b>URL:</b> Log, Block</li> <li>• <b>Domain:</b> Log, Block</li> </ul> | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>IP address:</b> Log, Block</li> <li>• <b>URL:</b> Log, Block</li> <li>• <b>Domain:</b> Log, Block</li> </ul>  |
| Deep Security Manager 10.0 (or later) | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>URL:</b> Log, Block</li> </ul>   | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>URL:</b> Log, Block</li> </ul>  |



| PRODUCT  | VIRTUAL ANALYZER LIST  | USER-DEFINED LIST  |
|--|--|--|
| <ul style="list-style-type: none"> <li>• Deep Discovery Inspector 5.0 (or later)</li> <li>• Deep Discovery Email Inspector 3.0 (or later)</li> </ul> | Synchronizes the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> No scan actions performed</li> <li>• <b>IP address:</b> No scan actions performed</li> <li>• <b>URL:</b> No scan actions performed</li> <li>• <b>Domain:</b> No scan actions performed</li> </ul>                  | Synchronizes the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> No scan actions performed</li> <li>• <b>IP address:</b> No scan actions performed</li> <li>• <b>URL:</b> No scan actions performed</li> <li>• <b>Domain:</b> No scan actions performed</li> </ul>                  |
| InterScan Messaging Security Virtual Appliance 9.1 (or later)  | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> </ul>  | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>File SHA-1:</b> Log, Block, Quarantine</li> </ul>   |
| InterScan Web Security Virtual Appliance 6.5 SP2 Patch 4 (or later)  | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>File SHA-1:</b> Log, Block, Quarantine</li> <li>• <b>IP address:</b> Log, Block</li> <li>• <b>URL:</b> Log, Block</li> <li>• <b>Domain:</b> Log, Block</li> </ul> | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>File SHA-1:</b> Log, Block, Quarantine</li> <li>• <b>IP address:</b> Log, Block</li> <li>• <b>URL:</b> Log, Block</li> <li>• <b>Domain:</b> Log, Block</li> </ul> |
| Trend Micro Endpoint Application Control 2.0 SP1 Patch 1 (or later)  | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> </ul>  | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>File SHA-1:</b> Log, Block, Quarantine</li> </ul>   |

| PRODUCT   | VIRTUAL ANALYZER LIST   | USER-DEFINED LIST   |
|---|---|---|
| Cloud App Security 5.0 (or later)   | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>URL:</b> Log, Block</li> </ul>   | Performs actions against the following suspicious object types: <ul style="list-style-type: none"> <li>• <b>File:</b> Log, Block, Quarantine</li> <li>• <b>URL:</b> Log, Block</li> </ul>   |
| <ul style="list-style-type: none"> <li>• Smart Protection Server 3.3 Patch 2 (or later)</li> <li>• OfficeScan 11.0 SP1 (or later) integrated Smart Protection Server</li> <li>• Trend Micro products that send Web Reputation queries to a supported Smart Protection Server</li> </ul> | Managed products perform actions against the following suspicious object types during Web Reputation queries: <ul style="list-style-type: none"> <li>• <b>URL:</b> Log, Block</li> </ul>  | Managed products perform actions against the following suspicious object types during Web Reputation queries: <ul style="list-style-type: none"> <li>• <b>URL:</b> Log, Block</li> </ul> <hr/> <div style="display: flex; align-items: center;">  <p><b>Important</b><br/>Smart Protection Server classifies all URLs in the User-Defined Suspicious Objects list as “High” risk.</p> </div> <hr/> |
|   | <div style="display: flex; align-items: flex-start;">  <p><b>Note</b><br/>Only certain managed products can directly perform the actions configured in Apex Central on suspicious URL objects. Other managed products take action on suspicious URL objects based on the product's configured Web Reputation settings.</p> <p>Logs that display on the managed products may not contain information related to suspicious object detections. Apex Central interprets logs sent from the managed product and displays the suspicious object detection on the Apex Central console.</p> </div> |   |

## Configuring Distribution Settings

Configure distribution settings to enable Apex Central to consolidate and send Virtual Analyzer and user-defined suspicious objects (excluding exceptions) to certain managed products. These products synchronize and use all or some of these objects.

Apex Central can also send suspicious IP addresses and domains to TippingPoint.



### Note

The **Distribution Settings** also allows you to configure Suspicious Object Hub and Node Apex Central server settings to synchronize suspicious object lists across multiple Apex Central servers.

For more information, see [Suspicious Object Hub and Node Architecture on page 23-1](#).

---

## Procedure

### 1. Go to **Threat Intel > Distribution Settings**.

The **Distribution Settings** screen appears.

### 2. To send suspicious objects to managed products:

- a. Click the **Managed Products** tab.
- b. Select the **Send suspicious objects to managed products** check box.
- c. Record the following information for use when configuring Apex Central as the Virtual Analyzer source in managed products:
  - **Service URL:** The service URL of Apex Central
  - **API key:** The code that identifies Apex Central to the managed product
- d. Click **Save**.

- e. Click **Sync Now**.
3. To send suspicious objects to TippingPoint:
    - a. Click the **TippingPoint** tab.
    - b. Select the **Send suspicious objects (IP addresses and domain names only) to TippingPoint** check box.



**Note**

Apex Central sends suspicious IP addresses and domain names analyzed by Virtual Analyzer. TippingPoint uses reputation filters to apply block, permit, or notify actions across an entire reputation group. For more information about reputation filters, refer to your TippingPoint documentation.

---

- c. Specify the following:
    - **Server name:** Type the server URL and port number for your TippingPoint deployment.
    - **User name:** Type the user name of an account with sufficient privileges to access the TippingPoint console.
    - **Password:** Type the password for the account.
  - d. (Optional) Click **Test Connection** to confirm the connection.
  - e. Select the severity level that triggers Apex Central to send domain names or IP address information to TippingPoint.
    - **High only:** IP addresses and domain names with high severity
    - **High and medium:** IP addresses and domain names with high and medium severity
    - **All:** Includes IP addresses and domain names with high, medium, and low severity
  - f. Click **Save**.
  - g. Click **Sync Now**.
-

## Suspicious Object Detection

You can view suspicious object detections in your environment in many ways using the Apex Central console. For information regarding the different ways of viewing suspicious object detections, refer to the following:

- [Viewing At Risk Endpoints and Recipients on page 20-15](#)
- [Analyzing Impact from Virtual Analyzer Suspicious Objects on page 20-16](#)



### Note

Apex Central only identifies users or endpoints exposed to suspicious objects in your environment. You cannot take any direct action on any suspicious objects using the Apex Central console.

---

## Viewing At Risk Endpoints and Recipients

Apex Central checks Web Reputation, URL filtering, network content inspection, and rule-based detection logs received from all managed products and then compares these logs with its list of suspicious objects.

---

### Procedure

1. Go to **Threat Intel > Virtual Analyzer Suspicious Objects**.

The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Objects** tab.
3. Expand the arrow to the left of the **Object** you want to view.
  - The **At Risk Endpoints** list displays all endpoints and users still affected by the suspicious object.
    - For **File** detections, the **Latest Action Result** column displays the last action result reported from managed products.
    - For all other detection types, the **Latest Action Result** column displays “N/A”.

- The **At Risk Recipients** list displays all recipients still affected by the suspicious object.
- 

## Analyzing Impact from Virtual Analyzer Suspicious Objects

The **Virtual Analyzer Suspicious Objects** screen allows you to perform an impact analysis on your network. The impact analysis uses Endpoint Sensor to contact agents and performs a historical scan of the agent logs to determine if the suspicious objects have affected your environment for a period of time without detection.

You can also perform an impact analysis for user-defined suspicious objects on the **Custom Intelligence** screen.

For more information, see [Analyzing Impact and Responding to IOCs from User-Defined Suspicious Objects on page 20-33](#).

---



### Important

Impact analysis requires a valid Apex One Endpoint Sensor license. Ensure that you have a valid Apex One Endpoint Sensor license and enable the Enable Sensor feature for the appropriate **Apex One Security Agent** or **Apex One (Mac)** policies.

For more information, see the *Apex Central Widget and Policy Management Guide*.

---

## Procedure

1. Go to **Threat Intel > Virtual Analyzer Suspicious Objects**.

The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Objects** tab.
  3. Select one or more objects from the list.
- 



### Note

Apex Central does not support analyzing impact for URL objects.

---

#### 4. Click **Analyze Impact**.

Endpoint Sensor contacts agents and evaluates the agent logs for any detections of the suspicious objects.

**Note**

Impact analysis times vary depending on your network environment.

---

#### 5. Expand the arrow to the left of the **Object** you want to view.

- The **At Risk Endpoints** list displays all endpoints and users still affected by the suspicious object.
    - For **File** detections, the **Latest Action Result** column displays the last action result reported from managed products.
    - For all other detection types, the **Latest Action Result** column displays “N/A”.
  - The **At Risk Recipients** list displays all recipients still affected by the suspicious object.
- 

### Historical Investigations in Endpoint Sensor

Historical Investigations assess historical events and analysis chains based on specified criteria. The results can be viewed as a root cause analysis map showing the execution flow of any suspicious activity. This facilitates the analysis of the enterprise-wide chain of events involved in a targeted attack.

Historical Investigations use the following object types for its investigation:

- DNS record
- IP address
- File name
- File path
- SHA-1 hash values
- MD5 hash values

- User account

Historical Investigations query a normalized database containing an endpoint's historical events. Compared to a traditional log file, this method uses less disk space and consumes fewer resources.

## Viewing the Handling Process

The **Handling Process** screen provides an overview of the life-cycle for a suspicious object in your environment and current effect of the suspicious object to your users or endpoints.



### Important

Viewing the handling process requires additional licensing for a product or service that includes Virtual Analyzer. Ensure that you have a valid license for at least one of the following:

- Apex One Sandbox as a Service
  - Deep Discovery Analyzer 6.5 (or later)
  - Deep Discovery Email Inspector 3.5 (or later)
  - Deep Discovery Inspector 5.0 (or later)
- 



## Procedure

1. Go to **Threat Intel > Virtual Analyzer Suspicious Objects**.
2. Click the **View** link in the **Handling Process** column of the table for a specific suspicious object.

The **Handling Process** screen appears.

3. Click any of the following tabs to view more information about the suspicious object.



| TAB                      | DESCRIPTION  |
|--------------------------|--|
| <b>Sample Submission</b> | <p>Displays information related to the first and latest analysis of the suspicious object</p> <p>Apex Central integrates with the following products, which use a Virtual Analyzer to analyze suspicious objects submitted by other managed products:</p> <ul style="list-style-type: none"> <li>• Deep Discovery Analyzer 6.5 (or later)</li> <li>• Deep Discovery Email Inspector 3.5 (or later)</li> <li>• Deep Discovery Inspector 5.0 (or later)</li> </ul> <hr/> <p> <b>Note</b><br/>Apex One Sandbox as a Service does not provide <b>Sample Submission</b> information.</p> |
| <b>Analysis</b>          | <p>Displays the Virtual Analyzer analysis of the submitted object</p> <p>Virtual Analyzer determines the risk level of 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.</p> <hr/> <p> <b>Note</b><br/>Apex One Sandbox as a Service does not provide <b>Product, Product host name, or Product IP address</b> information.</p>  |
| <b>Distribution</b>      | <p>Displays all products that synchronized the Suspicious Object list and the last synchronization time</p> <p>Apex Central consolidates Virtual Analyzer and user-defined suspicious object lists (excluding exceptions) and synchronizes the lists with integrated managed products.</p>   |

| TAB                                     | DESCRIPTION   |
|---|---|
| <b>Impact Analysis &amp; Mitigation</b> | <p>Displays all endpoints and users affected by the suspicious object</p> <ul style="list-style-type: none"> <li>• For <b>File</b> detections, the <b>Latest Action Result</b> column displays the last action result reported from managed products.</li> <li>• For all other detection types, the <b>Latest Action Result</b> column displays “N/A”.</li> </ul> <p>Click the <b>Root Cause Analysis</b> link to further investigate how the object affected the user or endpoint.</p> |

## Preemptive Protection Against Suspicious Objects

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

| FEATURE                              | DESCRIPTION  |
|--------------------------------------|--|
| User-Defined Suspicious Objects list | <p>The User-Defined Suspicious Objects list allows you to define suspicious file, file SHA-1, IP address, URL, and domain objects that your registered Virtual Analyzer has not yet detected on your network.</p> <p>Supported managed products that subscribe to the Suspicious Object lists can take action on the objects found in the list to prevent the spread of unknown threats.</p> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Adding Objects to the User-Defined Suspicious Object List on page 20-21</a></li> <li>• <a href="#">Suspicious Object Scan Actions on page 20-9</a></li> <li>• <a href="#">Analyzing Impact and Responding to IOCs from User-Defined Suspicious Objects on page 20-33</a></li> </ul> |

| FEATURE           | DESCRIPTION  |
|-------------------|--|
| STIX file list    | <p>The STIX file list allows you to import Structured Threat Import Expression (STIX) files and extract suspicious file SHA-1, IP address, URL, and domain objects to the User-Defined Suspicious Object list.</p> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Adding STIX Objects to the User-Defined Suspicious Object List on page 20-23</a></li> <li>• <a href="#">Analyzing Impact and Responding to IOCs from User-Defined Suspicious Objects on page 20-33</a></li> </ul> |
| OpenIOC file list | <p>The OpenIOC file list allows you to import OpenIOC files and extract suspicious file SHA-1, IP address, URL, and domain objects to the User-Defined Suspicious Object list.</p> <p>For more information, see the following topics:</p> <ul style="list-style-type: none"> <li>• <a href="#">Adding OpenIOC Objects to the User-Defined Suspicious Object List on page 20-26</a></li> <li>• <a href="#">Analyzing Impact and Responding to IOCs from User-Defined Suspicious Objects on page 20-33</a></li> </ul>                              |

## Adding Objects to the User-Defined Suspicious Object List

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 you the options 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.

For more information, see the following topics:

- [Importing User-Defined Suspicious Object Lists on page 20-23](#)
- [Adding OpenIOC Objects to the User-Defined Suspicious Object List on page 20-26](#)
- [Adding STIX Objects to the User-Defined Suspicious Object List on page 20-23](#)

---

## Procedure

1. Go to **Threat Intel > Custom Intelligence**.

The **Custom Intelligence** screen appears.

2. Click the **User-Defined Suspicious Objects** tab.

The User-Defined Suspicious Object list appears.

3. Click **Add**.

4. Specify the **Type** of object.

- **File:** Click **Browse** to upload a suspicious object file.
- **File:** Specify the **File SHA-1** hash value for the file.
- **IP address:** Specify the IP address.
- **URL:** Specify the URL.
- **Domain:** Specify the domain.

5. Specify the **Scan action** that supported products take after detecting the object.

- **Log**
- **Block**
- **Quarantine**



### Note

This scan action is only available for **File** or **File SHA-1** objects.

---

6. (Optional) Specify a **Note** to assist in identifying the suspicious object.
7. (Optional) Specify the expiration date.
8. Click **Add**.

The object appears in the User-Defined Suspicious Object list. Managed products that subscribe to the suspicious objects lists receive the new object information during the next synchronization.

---

## Importing User-Defined Suspicious Object Lists

Add multiple suspicious objects to the User-Defined Suspicious Objects list using a properly formatted CSV file.

---

### Procedure

1. Go to **Threat Intel > Custom Intelligence**.

The **Custom Intelligence** screen appears.

2. Click the **User-Defined Suspicious Objects** tab.

The User-Defined Suspicious Object list appears.

3. Click **Import**.

4. Select the CSV file containing the list of suspicious objects.
- 



#### Tip

Click the **Download sample CSV** link to obtain a properly formatted example CSV file with detailed instructions on creating a user-defined suspicious objects list.

---

5. Click **Import**.

Objects in the CSV file appear in the User-Defined Suspicious Objects list. Managed products that subscribe to the suspicious objects lists receive the new object information during the next synchronization.

---

## Adding STIX Objects to the User-Defined Suspicious Object List

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.

For more information about manually adding suspicious objects to the User-Defined Suspicious Object list, see [Adding Objects to the User-Defined Suspicious Object List on page 20-21](#).

**Important**

Apex Central only supports uploading properly formatted STIX files that have \*.xml file extensions and conform to the following STIX and Cybox releases:

- STIX 1.1
  - STIX 1.1.1
  - STIX 1.2
  - Cybox 2.1
- 

**Note**

Apex Central automatically extracts suspicious objects to the User-Defined Suspicious Object list when the STIX file is imported.

---

**Procedure**

1. Go to **Threat Intel > Custom Intelligence**.

The **Custom Intelligence** screen appears.

2. Click the **STIX** tab.

The STIX file list appears.

3. (Optional) To filter the files that display in the file list, use the search box to specify a full or partial string contained in the **File Name**, **Short Description**, or **Source Added By** columns.

---

4. Click **Add**.

The **Add STIX Files** screen appears.

5. Select STIX files (\*.xml) to upload.
- a. Click **Select Files....**
  - b. Select one or more files to upload.



**Note**

- The maximum file size for each file is 10 MB.
  - The total number of files uploaded at the same time cannot exceed 200 files.
- 

c. Click **Open**.

6. (Optional) Click **Advanced settings** to specify scan actions that supported products perform after detecting the object.



**Note**

You can also configure scan actions for suspicious objects on the User-Defined Suspicious Object list.

For more information, see [Suspicious Object Scan Actions on page 20-9](#).

---

7. Click **Add**.

Apex Central uploads the selected STIX files and extracts suspicious objects to the User-Defined Suspicious Object list.

- To download a copy of a specific file, click the link in the **File Name** column.
- To track the file extraction status, use the **Command Tracking** screen.

For more information, see [Command Tracking on page 13-2](#).

- To view the extracted suspicious objects on a filtered view of the User-Defined Suspicious Object list, click the count in the **Extracted Objects** column.
- To delete files, select the check box next to the **File Name** of at least one file and click **Delete**.

**Note**

- Deleting a file does not remove the extracted suspicious objects from the User-Defined Suspicious Object list.
  - You cannot delete a file until Apex Central has finished extracting suspicious objects from the file.
- 

## Adding OpenIOC Objects to the User-Defined Suspicious Object List

You can protect your network 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 Historical Investigation or a Live Investigation.

For details about manually adding suspicious objects directly to the User-Defined Suspicious Object list, see [Adding Objects to the User-Defined Suspicious Object List on page 20-21](#).

**Important**

Apex Central only supports OpenIOC 1.0.

---



**Note**

By default, Apex Central automatically extracts suspicious objects to the User-Defined Suspicious Object list when the OpenIOC file upload is complete.

Alternatively, you can choose to upload the OpenIOC file first, and then manually extract suspicious objects after the file upload is complete.

---

**Procedure**

1. Go to **Threat Intel > Custom Intelligence**.

The **Custom Intelligence** screen appears.

2. Click the **OpenIOC** tab.

The OpenIOC file list appears.

3. (Optional) To filter the files that display in the file list, use the search box to specify a full or partial string contained in the **File Name**, **Short Description**, or **Source Added By** columns.

4. Click **Add**.

The **Add OpenIOC Files** screen appears.

5. Select OpenIOC files (\*.ioc) to upload.

- a. Click **Select Files....**

- b. Select one or more files to upload.



**Note**

- The maximum file size for each file is 10 MB.
- The total number of files uploaded at the same time cannot exceed 200 files.
- The maximum number of objects for each suspicious object type in the User-Defined Suspicious Object list cannot exceed 10,000 objects for each type.

The extraction task for a suspicious object type will be unsuccessful if the maximum number of objects has been reached for the object type.

---

c. Click **Open**.

6. (Optional) Click **Advanced settings** to configure the following settings:

- To upload the file without automatically extracting the suspicious objects, clear the **Extract file SHA-1 hashes, IP addresses, URLs, or domains, and add the suspicious objects to the User-Defined Suspicious Objects list** check box.
- 



**Note**

If you disable automatic extraction when uploading files, you can still manually extract objects after the file upload is complete.

---

- Specify scan actions for supported products to perform after detecting the object.
- 



**Note**

You can also configure scan actions for suspicious objects on the User-Defined Suspicious Object list.

For more information, see [Suspicious Object Scan Actions on page 20-9](#).

---

---

## 7. Click **Add**.



### Tip

- To track the file upload status, perform a log query by using the **User Access** log type.

For more information, see [Querying Logs on page 16-2](#).

- To track the suspicious object extraction status, use the **Command Tracking** screen.

For more information, see [Command Tracking on page 13-2](#).

---

Apex Central uploads the selected OpenIOC files to the OpenIOC file list.

---



### Note

- If default settings are selected, Apex Central automatically extracts suspicious objects to the User-Defined Suspicious Object list.
  - The **Extracted Objects** column in the OpenIOC file list displays “N/A” for the following scenarios:
    - You uploaded the OpenIOC file without automatically extracting the suspicious objects.
    - Apex Central was unable to extract suspicious objects from the OpenIOC file.
- 

8. To manually extract suspicious objects from an uploaded OpenIOC file:
  - a. Select the check box next the **File Name** of the uploaded file.
  - b. Click **Extract**.

The **Extracted Objects** column displays the number of suspicious objects from the OpenIOC file to the User-Defined Suspicious Object list.

- To download a copy of a specific file, click the link in the **File Name** column.
- To track the file extraction status, use the **Command Tracking** screen.

For more information, see [Command Tracking on page 13-2](#).

- To view the extracted suspicious objects on a filtered view of the User-Defined Suspicious Object list, click the count in the **Extracted Objects** column.
- To delete files, select the check box next to the **File Name** of at least one file and click **Delete**.



**Note**

- Deleting a file does not remove the extracted suspicious objects from the User-Defined Suspicious Object list.
- You cannot delete a file until Apex Central has finished extracting suspicious objects from the file.

- 
9. To start a threat investigation using an uploaded OpenIOC file as the assessment criteria:




**Important**



- Threat investigations require a valid Endpoint Sensor license. Ensure that you have a valid Endpoint Sensor license or contact your service provider to obtain an Activation Code.
- After activating your Endpoint Sensor license, enable the Endpoint Sensor feature by creating an Apex One Agent policy or Apex One (Mac) policy on the **Policy Management** screen (**Policies > Policy Management**).

For more information, see the *Apex Central Widget and Policy Management Guide*.

---

- a. Select the check box next the **File Name** of the uploaded file.
- b. Perform one of the following types of threat investigation:

| INVESTIGATION            | DESCRIPTION   |
|--------------------------|---|
| Historical Investigation | <p>A Historical Investigation uses server metadata to identify endpoints that are possible candidates for further analysis.</p> <p>Hover over the <b>Analyze Impact</b> button and click <b>Historical Investigation</b>.</p> <hr/> <p> <b>Note</b><br/>You can also perform a Historical Investigation from the <b>Historical Investigation</b> screen (<b>Response &gt; Historical Investigation</b>).</p> <hr/> <p>For more information, see <a href="#">Using User-defined Criteria for Historical Investigations on page 21-5</a>.</p> <p>For specific information about the server metadata used for Historical Investigations, see <a href="#">Endpoint Sensor Metadata on page 21-2</a>.</p> |

| INVESTIGATION           | DESCRIPTION   |
|-------------------------|---|
| One-time Investigation  | <p>A One-time Investigation is a Live Investigation that is generated on demand and goes through all files currently on the disk and all processes currently running in memory.</p> <p>Hover over the <b>Analyze Impact</b> button and go to <b>Live Investigation &gt; One-time</b>.</p> <hr/> <p> <b>Note</b><br/>You can also perform a one-time investigation from the <b>One-time Investigation</b> tab on the <b>Live Investigation</b> screen (<b>Response &gt; Live Investigation</b>).</p> <hr/> <p>For more information, see <a href="#">One-Time Investigation on page 21-26</a>.</p> |
| Scheduled Investigation | <p>A Scheduled Investigation is a Live Investigation that runs automatically at specific intervals.</p> <p>Hover over the <b>Analyze Impact</b> button and go to <b>Live Investigation &gt; Scheduled</b>.</p> <hr/> <p> <b>Note</b><br/>You can also perform a scheduled investigation from the <b>Scheduled Investigation</b> tab on the <b>Live Investigation</b> screen (<b>Response &gt; Live Investigation</b>).</p> <hr/> <p>For more information, see <a href="#">Scheduled Investigation on page 21-29</a>.</p>   |

## Analyzing Impact and Responding to IOCs from User-Defined Suspicious Objects

After adding suspicious objects or properly formatted IOC (STIX or OpenIOC) files to Apex Central, you can perform an impact analysis by selecting specific file, file SHA-1, IP address, or domain objects to determine if the threat exists within your network and take mitigation steps to prevent the spread of the threat to other endpoints.

For more information, see the following topics:

- [Importing User-Defined Suspicious Object Lists on page 20-23](#)
- [Adding OpenIOC Objects to the User-Defined Suspicious Object List on page 20-26](#)
- [Adding STIX Objects to the User-Defined Suspicious Object List on page 20-23](#)



### Important

- Impact analysis requires a valid Apex One Endpoint Sensor license. Ensure that you have a valid Apex One Endpoint Sensor license and enable the Enable Sensor feature for the appropriate **Apex One Security Agent** or **Apex One (Mac)** policies.

For more information, see the *Apex Central Widget and Policy Management Guide*.

- Endpoint isolation requires that you install Apex One Security Agents on the target endpoints.

### Procedure

1. Go to **Threat Intel > Custom Intelligence**.

The **Custom Intelligence** screen appears.

2. Click the **User-Defined Suspicious Objects** tab.

The User-Defined Suspicious Object list appears.

3. Select one or more objects from the list.

**Note**

Apex Central does not support analyzing impact for URL objects.

---

4. Click **Analyze Impact**.

Endpoint Sensor contacts agents and evaluates the agent logs for any detections of the suspicious objects.

**Note**

Impact analysis times vary depending on your network environment.

---

5. Expand the arrow to the left of the **Object** you want to view.
    - The **At Risk Endpoints** list displays all endpoints and users still affected by the suspicious object.
      - For **File** detections, the **Latest Action Result** column displays the last action result reported from managed products.
      - For all other detection types, the **Latest Action Result** column displays “N/A”.
    - The **At Risk Recipients** list displays all recipients still affected by the suspicious object.
- 

## Isolating Endpoints

Isolate at-risk endpoints to run an investigation and resolve security issues. Restore the connection promptly when all issues have been resolved.

**Important**

- Endpoint isolation requires a valid Apex Central license.
  - For OfficeScan agents running versions 11 SP1 to XG SP1, you must enable the OfficeScan Firewall to perform endpoint isolation.
-



---

## Procedure

1. Go to **Directories > Users/Endpoints**.
2. Select to view endpoints.
3. Click the name of an endpoint in the list.
4. On the **Endpoint** information screen that appears, click **Task > Isolate**.

Apex Central disables the **Isolate** option on endpoints for the following reasons:

- The agent on the endpoint runs an unsupported version.
  - The user account used to log on to Apex Central does not have the necessary permissions.
5. A message appears at the top of the **Endpoint** information screen that allows you to monitor the isolation status. After isolation completes, the message closes and a notification appears on the target endpoint to inform the user.

If a problem occurs during the isolation process, the message at the top of the **Endpoint - {name}** screen informs you of the problem.

6. To view all isolated endpoints on your Apex Central network, click the **Endpoints > Filters > Network Connection > Isolated** node in the User/Endpoint Directory tree.
7. (Optional) To configure allowed inbound and outbound traffic to all isolated endpoints:
  - a. Select **Control traffic on isolated endpoints**.
  - b. Expand the **Inbound Traffic** or **Outbound Traffic** sections.
  - c. Specify the allowed traffic by specifying the **Protocol, IP Address, and Destination Port**.

Separate multiple destination ports using commas.
  - d. Add multiple inbound and outbound entries by clicking the - control to the right of the **Destination Port** information.



**Note**

After modifying the allowed traffic settings, all previously isolated endpoints and any endpoints isolated later apply the inbound and outbound traffic settings.

---

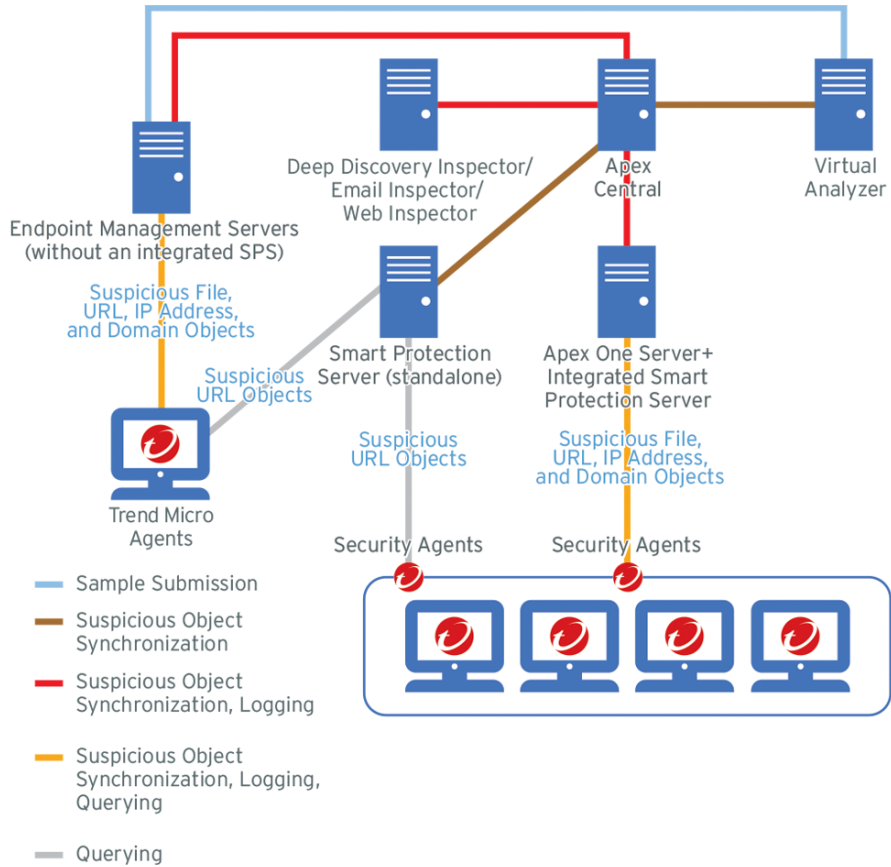
8. After you have resolved the security threats on an isolated endpoint, restore network connectivity from the following locations:
  - **Endpoint** information screen: Click **Task > Restore**.
  - **Endpoints > Filters > Network Connection > Isolated**: Select the endpoint row in the table and click **Task > Restore Network Connection**.
9. A message appears at the top of the screen that allows you to monitor the restoration status. After restoration completes, the message closes and a notification appears on the target endpoint to inform the user.

If a problem occurs during the restoration process, the message at the top of the screen informs you of the problem.

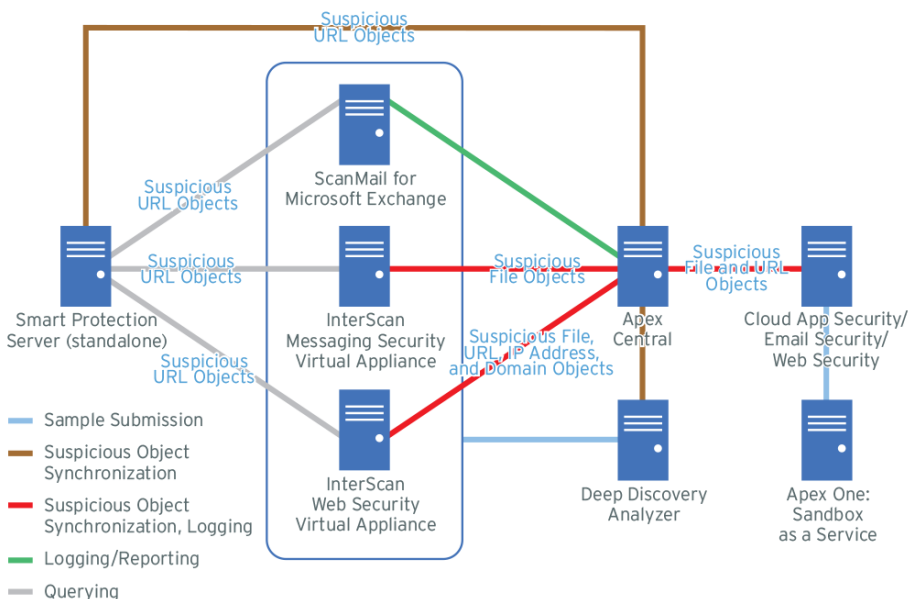
---

## Connected Threat Defense Product Integration

The Connected Threat Defense strategy integrates many Trend Micro products. The following diagrams illustrate how the major products interact.



**FIGURE 20-1. Endpoint Protection Example Topology**



**FIGURE 20-2. Messaging and Network Security Example Topology**

Apex Central further monitors other registered Trend Micro products through log analysis and comparison of detected files with the synchronized suspicious object lists.

For Apex Central registration and suspicious object list synchronization information for each major product, refer to the following:


### Apex Central

| REQUIREMENT     | DESCRIPTION  |
|-----------------|--|
| Product version | <ul style="list-style-type: none"> <li>• Apex Central (any version)</li> <li>• Control Manager 7.0 (or later)</li> </ul> |

| REQUIREMENT                                  | DESCRIPTION  |
|--|--|
| Apex Central registration                    | <p>For products that do not register to Apex Central through the Apex Central console, the following Apex Central registration information is required:</p> <ul style="list-style-type: none"> <li>• Server FQDN or IP address</li> <li>• Port: By default, Apex Central uses HTTP Port 80 or HTTPS Port 443</li> </ul> <p>For products that register using the Apex Central management console, go to <b>Administration &gt; Managed Servers &gt; Server Registration</b>, select the product from the <b>Server Type</b> list, and click <b>Add</b>.</p> |
| Suspicious Object list synchronization       | <p>For products that do not automatically synchronize the Suspicious Object lists with Apex Central, the following API information is required:</p> <ul style="list-style-type: none"> <li>• API key: To obtain the API key, open the Apex Central management console and go to <b>Threat Intel &gt; Distribution Settings</b>.</li> </ul>   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object management</li> <li>• Impact analysis</li> <li>• Endpoint isolation</li> <li>• IOC management</li> </ul>  |

## Apex One

| REQUIREMENT     | DESCRIPTION   |
|-----------------|---|
| Product version | <ul style="list-style-type: none"> <li>• Apex One 2019</li> <li>• OfficeScan 11.0 SP1 (or later)</li> </ul> |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Apex Central registration                    | <p>From the Apex One web console at <b>Administration &gt; Settings &gt; Apex Central</b></p> <p>Required Apex Central information:</p> <ul style="list-style-type: none"> <li>• Server FQDN or IP address</li> <li>• Port: By default, Apex Central uses HTTP Port 80 or HTTPS Port 443</li> </ul> <p>For more information, see the <i>Apex One Administrator's Guide</i>.</p>   |
| Suspicious Object list synchronization       | <p>From the Apex One web console at <b>Administration &gt; Settings &gt; Suspicious Object List</b></p> <p>Required Apex Central information:</p> <ul style="list-style-type: none"> <li>• None</li> </ul> <hr/> <p> <b>Note</b><br/>Apex One automatically obtains the required API key information from the Apex Central server during Apex Central registration</p> |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object management</li> <li>• Endpoint isolation</li> </ul>  |

## Apex One Endpoint Sensor

| REQUIREMENT     | DESCRIPTION   |
|-----------------|---|
| Activation Code | Additional licensing is required. Contact your service provider to obtain an Activation Code. |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Enable feature                               | <p>Enable Endpoint Sensor from the Apex Central management console. Go to <b>Policies &gt; Policy Management</b> and select <b>Apex One Security Agent</b> from the <b>Product</b> drop-down list to create or modify a policy. Expand <b>Endpoint Sensor Settings</b> and select the <b>Enable Endpoint Sensor</b> check box.</p> <p>For more information, see the <i>Apex Central Widget and Policy Management Guide</i>.</p> |
| Suspicious Object list synchronization       | Apex One Endpoint Sensor does not synchronize Suspicious Object lists with Apex Central   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> <li>• Impact analysis</li> <li>• Endpoint isolation</li> <li>• IOC management</li> </ul>  |

## Apex One Sandbox as a Service

| REQUIREMENT                            | DESCRIPTION   |
|--|---|
| Activation Code                        | Additional licensing is required. Contact your service provider to obtain an Activation Code.   |
| Apex Central registration              | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; License Management &gt; Apex Central</b> and click <b>Specify a new Activation Code</b> in the <b>Apex One Sandbox as a Service</b> section to provide and activate the Activation Code. |
| Suspicious Object list synchronization | <p>Automatic after registration to Apex Central</p> <p>The Suspicious Object lists synchronize with the Apex Central server every 10 minutes by default.</p>  |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> </ul> |

## Cloud App Security

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Product version                              | 5.0 (or later)  |
| Apex Central registration                    | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |
| Suspicious Objects list synchronization      | For more information, see the <i>Cloud App Security Online Help</i> .   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object management</li> <li>• Suspicious Object scan actions</li> </ul>          |

## Deep Discovery Analyzer

| REQUIREMENT               | DESCRIPTION   |
|---------------------------|---|
| Product version           | 6.5 (or later)  |
| Apex Central registration | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |



| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Suspicious Object list synchronization       | Automatic after registration to Apex Central<br>The Suspicious Object lists synchronize with the Apex Central server every 10 minutes by default.   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> </ul> |

## Deep Discovery Director

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Product version                              | 5.0 (or later)  |
| Apex Central registration                    | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |
| Suspicious Object list synchronization       | Automatic after registration to Apex Central<br>The Suspicious Object lists synchronize with the Apex Central server every 10 minutes by default.   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> </ul>     |

## Deep Discovery Email Inspector

| REQUIREMENT     | DESCRIPTION    |
|-----------------|----------------|
| Product version | 3.5 (or later) |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Apex Central registration                    | For more information, see the <i>Deep Discovery Email Inspector Administrator's Guide</i> .   |
| Suspicious Objects list synchronization      | For more information, see the <i>Deep Discovery Email Inspector Administrator's Guide</i> .   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> </ul> |

## Deep Discovery Inspector

| REQUIREMENT                            | DESCRIPTION   |
|--|---|
| Product version                        | 5.0 (or later)  |
| Apex Central registration              | <p>From the Deep Discovery Inspector management console at <b>Administration &gt; Integrated Products/Services &gt; Apex Central</b></p> <p>Required Apex Central information:</p> <ul style="list-style-type: none"> <li>• Server FQDN or IP address</li> <li>• Port: By default, Apex Central uses HTTP Port 80 or HTTPS Port 443</li> </ul> <p>For more information, see the <i>Deep Discovery Inspector Administrator's Guide</i>.</p>                            |
| Suspicious Object list synchronization | <p>From the Deep Discovery Inspector management console at <b>Administration &gt; Integrated Products/Services &gt; Apex Central</b></p> <p>Required Apex Central information:</p> <ul style="list-style-type: none"> <li>• API key: To obtain the API key, open the Apex Central management console and go to <b>Threat Intel &gt; Distribution Settings</b>.</li> </ul> <p>For more information, see the <i>Deep Discovery Inspector Administrator's Guide</i>.</p> |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> </ul> |

## Deep Discovery Web Inspector

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Product version                              | 2.5 (or later)  |
| Apex Central registration                    | For more information, see the <i>Deep Discovery Web Inspector Administrator's Guide</i> .   |
| Suspicious Objects list synchronization      | For more information, see the <i>Deep Discovery Web Inspector Administrator's Guide</i> .   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> </ul> |

## Deep Security Manager



### Important

Deep Security as a Service does not support Connected Threat Defense. Connected Threat Defense features are only supported by Deep Security Manager on-premises servers.

| REQUIREMENT               | DESCRIPTION   |
|---------------------------|---|
| Product version           | 10.0 (or later)   |
| Apex Central registration | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Suspicious Objects list synchronization      | Automatic after registration to Apex Central  |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> <li>• Suspicious Object scan actions</li> </ul> |

## Email Security

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Apex Central registration                    | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |
| Suspicious Objects list synchronization      | For more information, see the <i>Email Security Administrator Console Online Help</i> .   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object management</li> <li>• Suspicious Object scan actions</li> </ul>          |

## InterScan Messaging Security Virtual Appliance

| REQUIREMENT                            | DESCRIPTION   |
|--|---|
| Product version                        | 9.1 (or later)  |
| Apex Central registration              | For more information, see the <i>InterScan Messaging Security Virtual Appliance Administrator's Guide</i> . |
| Suspicious Object list synchronization | Automatic after registration to Apex Central  |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> <li>• Suspicious Object scan actions</li> </ul> |

## InterScan Web Security Virtual Appliance


| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Product version                              | 6.5 SP2 Patch 4 (or later)  |
| Apex Central registration                    | For more information, see the <i>InterScan Web Security Virtual Appliance Administrator's Guide</i> .   |
| Suspicious Objects list synchronization      | For more information, see the <i>InterScan Web Security Virtual Appliance Administrator's Guide</i> .   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object sample submission</li> <li>• Suspicious Object management</li> <li>• Suspicious Object scan actions</li> </ul> |

## ScanMail for Microsoft Exchange

| REQUIREMENT                             | DESCRIPTION  |
|---|--|
| Product version                         | 12.5 (or later)  |
| Apex Central registration               | For more information, see the <i>ScanMail for Microsoft Exchange Administrator's Guide</i> . |
| Suspicious Objects list synchronization | For more information, see the <i>ScanMail for Microsoft Exchange Administrator's Guide</i> . |

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object sample submission</li> </ul> |

## Smart Protection Server

| REQUIREMENT                            | DESCRIPTION  |
|--|--|
| Product version                        | 3.3 Patch 2 (or later)   |
| Apex Central registration              | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> .  |
| Suspicious Object list synchronization | <p>From the Smart Protection Server web console, go to <b>Smart Protection &gt; Suspicious Objects</b>.</p> <p>Required information about the Suspicious Object list source:</p> <ul style="list-style-type: none"> <li>• Service URL</li> <li>• Port</li> </ul> <p>If the list source is Apex Central, the default ports are HTTP Port 80 or HTTPS Port 443.</p> <ul style="list-style-type: none"> <li>• API key: Provided by the server administrator</li> </ul> <p>If the list source is Apex Central, open the Apex Central management console and go to <b>Administration &gt; Suspicious Objects &gt; Distribution Settings</b>.</p> <hr/> <p> <b>Note</b></p> <p>For Smart Protection Server 3.3 (or later), Apex Central automatically sends the required API key information to the Smart Protection Server during registration.</p> <hr/> <p>For more information, see the <i>Smart Protection Server Administrator's Guide</i>.</p> |

| REQUIREMENT                                  | DESCRIPTION  |
|--|--|
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object scan actions</li> </ul> |

## Endpoint Application Control

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Product version                              | 2.0 SP1 Patch 1 (or later)  |
| Apex Central registration                    | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |
| Suspicious Object list synchronization       | Automatic after registration to Apex Central  |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object management</li> </ul>  |

## Web Security

| REQUIREMENT                                  | DESCRIPTION   |
|--|---|
| Apex Central registration                    | Complete the registration from the Apex Central management console. Go to <b>Administration &gt; Managed Servers &gt; Server Registration</b> , select the product from the <b>Server Type</b> list, and click <b>Add</b> . |
| Suspicious Objects list synchronization      | For more information, see the <i>Web Security Online Help</i> .   |
| Integrated Connected Threat Defense features | <ul style="list-style-type: none"> <li>• Security threat monitoring</li> <li>• Suspicious Object list synchronization</li> <li>• Suspicious Object management</li> <li>• Suspicious Object scan actions</li> </ul>          |





# Chapter 21

## Threat Investigation

This section discusses how to perform investigations and analyze the results using Threat Investigation.

Topics include:

- *Threat Investigation Overview on page 21-2*
- *Historical Investigations on page 21-3*
- *Live Investigations on page 21-23*
- *Investigation Results on page 21-33*

## Threat Investigation Overview

Use **Threat Investigation** to locate suspicious objects in the network.

Threat Investigations can correlate information from Endpoint Sensor and Active Directory to display attack information about endpoints and user accounts throughout your network.

If the network is the target of an ongoing attack or an APT, a threat investigation can:

- Assess the extent of damage caused by the targeted attack
- Provide information on the arrival and progression of the attack
- Aid in planning an effective security incident response

The following types of threat investigation are available:

- Historical Investigations can quickly identify endpoints which are possible candidates for further analysis. A Historical Investigation uses server metadata to quickly return results.

For more information, see [Historical Investigations on page 21-3](#).

- Live Investigations perform the investigation on the current system state. Live Investigations can be configured to run at specific periods, and also support a wider set of criteria through the use of OpenIOC and YARA rules.

For more information, see [Live Investigations on page 21-23](#).

## Endpoint Sensor Metadata

Metadata refers to data collected from the endpoint and uploaded to the server. Endpoint Sensor utilizes the data during a Historical Investigation to identify affected endpoints.

For details, see [Historical Investigations on page 21-3](#).

The type of metadata collected depends on the operating system installed on the endpoint.

**TABLE 21-1. Metadata by Operating System**

| OPERATING SYSTEM | METADATA   |   |
|------------------|--|---|
| Windows          | <ul style="list-style-type: none"> <li>• Host (name / IP address)</li> <li>• User account</li> <li>• File name</li> <li>• File path</li> <li>• Hash values (SHA-1, SHA-256 and MD5)</li> </ul> | <ul style="list-style-type: none"> <li>• Registry key</li> <li>• Registry data</li> <li>• Registry name</li> <li>• Command line</li> <li>• URL</li> </ul> |
| macOS            | <ul style="list-style-type: none"> <li>• Host (name / IP address)</li> <li>• User account</li> <li>• File name</li> <li>• URL</li> </ul>   | <ul style="list-style-type: none"> <li>• File path</li> <li>• Hash values (SHA-1, SHA-256 and MD5)</li> <li>• Command line</li> </ul>                     |

**Note**

- URL collection only applies to process callback events and only supports HTTP protocol.
- Use the **Policy Management** screen to configure metadata settings.
- The data available during Historical 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 Live Investigation.

## Historical Investigations

Historical Investigations can quickly identify endpoints which are possible candidates for further analysis. A Historical Investigation uses server metadata to quickly return results.

To access this screen, go to **Response > Historical Investigation**.

The **Historical Investigation** screen has two tabs:

| TAB                         | DESCRIPTION   |
|-----------------------------|---|
| Assessment                  | <p>Use an assessment to perform the following:</p> <ul style="list-style-type: none"> <li>• Evaluate the prevalence of a threat, and how long the threat has been in the network. The assessment goes through all historical data.</li> <li>• Determine the existence of a threat using simple criteria. Assessments support only a limited set of criteria.</li> </ul> <p>An assessment supports the following criteria types:</p> <ul style="list-style-type: none"> <li>• <b>User-defined:</b> Specify or load up to 10 user-defined criteria, or load a C&amp;C callback event.</li> </ul> <p>For details, see <a href="#">Supported Formats for User-defined Criteria on page 21-10</a>.</p> <ul style="list-style-type: none"> <li>• <b>OpenIOC file:</b> Use OpenIOC rules to define investigation criteria. Historical Investigations disregard all conditions and match any of the indicators specified in the OpenIOC file.</li> </ul> <p>For more information, see <a href="#">Supported IOC Indicators for Historical Investigations on page 21-17</a>.</p> <p>The assessment goes through the server metadata and updates the result pane as soon it finds a match. It may take a few minutes to completely go through the server metadata.</p> <p>For more information, see <a href="#">Using User-defined Criteria for Historical Investigations on page 21-5</a>.</p> |
| Root Cause Analysis Results | <p>If an assessment returns a match, administrators may generate a Root Cause Analysis to:</p> <ul style="list-style-type: none"> <li>• List all related objects to the specified criteria</li> <li>• Identify if any of the related objects are noteworthy</li> <li>• Review the sequence of events leading to the execution of the matched object.</li> </ul> <p>Generating a Root Cause Analysis may take some time to complete. Use the <b>Root Cause Analysis</b> tab to monitor the progress of the task.</p> <p>For more information, see <a href="#">Analysis Chains on page 21-35</a>.</p>   |

---

## Using User-defined Criteria for Historical Investigations

---

**Note**

To perform an investigation on the current system state, use Live Investigation.

For more information, see [Starting a One-time Investigation on page 21-25](#).

---

### Procedure

1. Go to **Response > Historical Investigation**.
2. Click **User-defined**.
3. Select one of the following options:
  - **Match ALL criteria:** Find objects matching all of the criteria specified
  - **Match ANY criteria:** Find objects matching any of the criteria specified
4. Click **New criteria**, select a criteria type, and specify valid information.  
For details, see [Supported Formats for User-defined Criteria on page 21-10](#).

To manage the criteria:

- Click **Reset** to clear all specified criteria.
  - To save the criteria for future investigations, click  and specify a criteria name.
- 

**Note**

Historical Investigations support a maximum of 10 saved user-defined criteria.

---

5. (Optional) To load existing user-defined criteria, click **Select criteria**.
  - a. Click **Yes**.



**Note**

Applying existing criteria overwrites any criteria currently specified.

---

**b.** Go to the **Saved Criteria** tab.

**c.** Select criteria.

To manage the criteria:

- Sort the criteria using the **Last Used** column.
- Delete saved criteria using the **Delete** icon.

**d.** Click **Add Saved Criteria**.

**6.** (Optional) To load C&C callback events, click **Select Criteria**.

**a.** Click **Yes**.

---



**Note**

Applying existing criteria overwrites any criteria currently specified.

---

**b.** Go to the **C&C Callback Events** tab.

**c.** Select a criteria.

Click **Period** to filter the C&C callback events by the specified time.

**d.** Click **Load C&C Callback Events**.

---



**Note**

The **Log Query** screen provides additional details about C&C callback events in case you need to review them before selection. To go to the **Log Query** screen, navigate to **Detections > Logs > Log Query**, and then filter by **Network Events > C&C Callback**.

---

**7.** Click **Assess**.

8. On the results pane, review the results that appear.



**Note**

- Allow some time for the Historical Investigation to run. The investigation appends more rows to the results table as soon as matching objects are found in the metadata. It may take a few minutes for the investigation to complete.
- The data available during Historical 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 Live Investigation.

The following details are available:

| COLUMN NAME      | DESCRIPTION   |
|------------------|---|
| Endpoint         | Name of the endpoint containing the matching object<br>Click to view more details about the endpoint.   |
| Status           | Current connection status of the endpoint   |
| IP Address       | IP address of the endpoint containing the matching object<br>The IP address is assigned by the network  |
| Operating System | Operating system used by the endpoint   |
| User             | User name of the user logged in when the Security Agent first logged the matched object<br>Click the user name to view more details about the user. |
| Managing Server  | Server that manages the affected endpoint   |
| First Seen       | Date and time when the Security Agent first logged the matched object   |

| COLUMN NAME  | DESCRIPTION   |
|--------------|---|
| Details      | <p>Click the icon to open the <b>Match Details</b> screen.</p> <p>The <b>Match Details</b> screen displays the following details:</p> <ul style="list-style-type: none"> <li>• <b>Criteria:</b> Criteria used in the assessment</li> <li>• <b>First Seen:</b> Date and time when the Security Agent first logged the matched object</li> <li>• <b>CLI/Registry Occurrences:</b> Number of matches found in command line or registry entries</li> </ul> <p>Click the value to show more details.</p> <ul style="list-style-type: none"> <li>• <b>Rating:</b> Rating assigned by Trend Micro intelligence</li> </ul> <p>You can further examine objects with “Malicious” ratings in Threat Connect or VirusTotal.</p> <ul style="list-style-type: none"> <li>• <b>Affected Endpoints:</b> If the rating is malicious, the number of endpoints where a similar match was found</li> </ul> <p>The count only includes endpoints affected within the last 90 days.</p> |
| Asterisk (*) | Indicates an endpoint tagged as <i>Important</i>  |

9. Identify and select one or more endpoints that require further action.





**Note**

The Historical Investigation results may include macOS endpoints. Since there are no actions available for macOS endpoints, the check boxes for these endpoints are disabled.

| ACTION                       | DESCRIPTION  |
|------------------------------|--|
| Generate Root Cause Analysis | <p>Generates a Root Cause Analysis to review the sequence of events leading to the execution of the matched object.</p> <p>For details, see <a href="#">Starting a Root Cause Analysis from an Assessment on page 21-18</a>.</p> |




| ACTION                   | DESCRIPTION  |
|--------------------------|--|
| Start Live Investigation | <p>Runs a new investigation with the same criteria on the current system state.</p> <hr/> <p> <b>Important</b><br/>Only available for Security Agents installed on Windows platforms.</p> <hr/> <p>The <b>Live Investigation</b> screen appears and initiates a new one-time investigation using the existing criteria.</p> <p>For assessments using user-defined criteria, <b>Live Investigation</b> uses only the selected endpoints as criteria</p> <p>For details, see <a href="#">Starting a One-time Investigation on page 21-25</a>.</p>   |
| Isolate Endpoints        | <p>Disconnects the selected endpoints from the network.</p> <hr/> <p> <b>Important</b><br/>Only available for Security Agents installed on Windows platforms.</p> <hr/> <p>After resolving the security threats on an isolated endpoint, the following locations on the <b>Directories &gt; Users/Endpoints</b> screen provides options to restore the network connection of an isolated endpoint:</p> <ul style="list-style-type: none"> <li>• <b>Endpoints &gt; All:</b> Click the name of an endpoint in the table, and click <b>Task &gt; Restore</b> on the screen that appears.</li> <li>• <b>Endpoints &gt; Filters &gt; Network Connection &gt; Isolated:</b> Select the endpoint row in the table, and click <b>Task &gt; Restore Network Connection</b>.</li> </ul> |



## Supported Formats for User-defined Criteria





### Important

If your environment manages both Apex One on-premises and Apex One as a Service Security Agents, some features may be different compared to Apex One as a Service. Apex One as a Service Security Agents continue to send data to Trend Micro servers but investigation capabilities may differ from the Apex Central as a Service console.

| TYPE  | ITEM  |
|---|---|
| User name<br>(exact match only)                           | Specify the name of the Active Directory account or local user<br>Examples: <ul style="list-style-type: none"> <li>• jane_smith</li> </ul> <hr/>  <b>Note</b><br>Use the local user account name only (<user name>). Do not include the domain name. |
| File name<br>(exact match only)                           | Specify the full file name including extension<br>Example: <ul style="list-style-type: none"> <li>• filename.exe</li> </ul>   |
| File directory<br>(exact match only;<br>on-premises only) | Specify the full path excluding file name<br>Example: <ul style="list-style-type: none"> <li>• c:\windows\system32\wbem\</li> </ul>   |

| TYPE  | ITEM   |
|---|--|
| File hash value<br>(exact match only)                 | <p>Specify the hash value of a file.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• SHA-1: a2da9cda33ce378a21f54e9f03f6c0c9efba61fa</li> </ul> <hr/> <p> <b>Note</b><br/>Endpoint Sensor records SHA-1 values only by default. To use SHA-256 or MD5 hash values, update the agent policy to include additional hash types.</p>     |
| FQDN / IP address /<br>Hostname<br>(exact match only) | <p>Specify the remote endpoint FQDN, IP address, or hostname to identify network connections that the investigated endpoint made</p> <hr/> <p> <b>Note</b><br/>The IPv6 format is not supported.</p> <hr/> <p>Examples:</p> <ul style="list-style-type: none"> <li>• cncserver.com</li> <li>• malicioussite.com</li> <li>• 192.168.0.1</li> </ul> |

| TYPE  | ITEM   |
|---|--|
| Registry key<br>(partial matching supported)        | <p data-bbox="408 253 1005 277">Specify the full or partial registry key, value name, or value data</p> <hr/> <div data-bbox="413 329 471 378">  </div> <p data-bbox="485 329 534 349"><b>Note</b></p> <ul data-bbox="512 375 1076 813" style="list-style-type: none"> <li data-bbox="512 375 1076 431">• Trend Micro only records the activity of important registry locations to reduce the resource impact on the endpoint.<br/><br/>If your investigation is unsuccessful and you want to investigate further, perform a Live Investigation.</li> <li data-bbox="512 537 1076 594">• Do not specify SID values as registry criteria. Investigations do not support SID values as custom registry criteria.</li> <li data-bbox="512 618 1076 813">• Using registry data as investigation criteria has the following limitations: <ul data-bbox="559 699 978 813" style="list-style-type: none"> <li data-bbox="559 699 932 724">• A criteria can contain up to 10 entries.</li> <li data-bbox="559 740 978 764">• Each entry must have at least 2 characters.</li> <li data-bbox="559 789 864 813">• Entries cannot contain spaces.</li> </ul> </li> </ul> |
| Registry value name<br>(partial matching supported) |  |
| Registry value data<br>(partial matching supported) |  |
| CLI command<br>(partial matching supported)         | <p data-bbox="408 850 1072 907">Specify the full or partial command line string, and press ENTER to add an entry.</p> <hr/> <div data-bbox="413 959 471 1008">  </div> <p data-bbox="485 959 534 979"><b>Note</b></p> <p data-bbox="485 992 1072 1049">Using command line as investigation criteria has the following limitations:</p> <ul data-bbox="512 1073 932 1195" style="list-style-type: none"> <li data-bbox="512 1073 870 1097">• Criteria can contain up to 10 entries.</li> <li data-bbox="512 1122 932 1146">• Each entry must have at least 2 characters.</li> <li data-bbox="512 1170 821 1195">• Entries cannot contain spaces.</li> </ul>   |

---

## Using OpenIOC files for a Historical Investigation

---

**Note**

To perform an investigation on the current system state, use **Live Investigation**.

For more information, see [Starting a One-time Investigation on page 21-25](#).

---

### Procedure

1. Go to **Response > Historical Investigation**.
  2. Click the **OpenIOC file** tab.
- 

**Note**

Using OpenIOC files in Historical 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.

For details, see [Supported IOC Indicators for Historical Investigations on page 21-17](#).

---

3. To upload and investigate using a new OpenIOC file:
  - a. Click **Upload OpenIOC File**.
  - b. Select a valid OpenIOC file.
  - c. Click **Open**.

4. To investigate using an existing OpenIOC file:
  - a. Click **Use Existing OpenIOC File**.
  - b. Select a file.
  - c. Click **Apply**.
5. Click **Assess**.
6. On the results pane, review the results that appear.

**Note**

- Allow some time for the Historical Investigation to run. The investigation appends more rows to the results table as soon as matching objects are found in the metadata. It may take a few minutes for the investigation to complete.
- Hover over the **Endpoints** label to display a pop-up that displays the progress of the assessment.
- The data available during Historical 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 Live Investigation.

The following details are available:

| COLUMN NAME | DESCRIPTION  |
|-------------|--|
| Endpoint    | Name of the endpoint containing the matching object<br>Click to view more details about the endpoint.  |
| Status      | Current connection status of the endpoint  |
| IP Address  | IP address of the endpoint containing the matching object<br>The IP address is assigned by the network |

| COLUMN NAME      | DESCRIPTION   |
|------------------|---|
| Operating System | Operating system used by the endpoint   |
| User             | <p>User name of the user logged in when the Security Agent first logged the matched object</p> <p>Click the user name to view more details about the user.</p>  |
| Managing Server  | Server that manages the affected endpoint   |
| First Seen       | Date and time when the Security Agent first logged the matched object   |
| Details          | <p>Click the icon to open the <b>Match Details</b> screen.</p> <p>The <b>Match Details</b> screen displays the following details:</p> <ul style="list-style-type: none"> <li>• <b>Criteria:</b> Criteria used in the assessment</li> <li>• <b>First Seen:</b> Date and time when the Security Agent first logged the matched object</li> <li>• <b>CLI/Registry Occurrences:</b> Number of matches found in command line or registry entries</li> </ul> <p>Click the value to show more details.</p> <ul style="list-style-type: none"> <li>• <b>Rating:</b> Rating assigned by Trend Micro intelligence</li> </ul> <p>You can further examine objects with “Malicious” ratings in Threat Connect or VirusTotal.</p> <ul style="list-style-type: none"> <li>• <b>Affected Endpoints:</b> If the rating is malicious, the number of endpoints where a similar match was found</li> </ul> <p>The count only includes endpoints affected within the last 90 days.</p> |
| Asterisk (*)     | Indicates an endpoint tagged as <i>Important</i>  |


7. Identify and select one or more endpoints that require further action.

**Note**

The Historical Investigation results may include macOS endpoints. Since there are no actions available for macOS endpoints, the check boxes for these endpoints are disabled.

| ACTION                       | DESCRIPTION   |
|------------------------------|---|
| Generate Root Cause Analysis | Generates a Root Cause Analysis to review the sequence of events leading to the execution of the matched object.<br><br>For more information, see <a href="#">Starting a Root Cause Analysis from an Assessment on page 21-18</a> .   |
| Start Live Investigation     | Runs a new investigation with the same criteria on the current system state.<br><br>The <b>Live Investigation</b> screen appears and initiates a new one-time investigation using the existing criteria.<br><br>For assessments using an OpenIOC file, <b>Live Investigation</b> uses both the current OpenIOC file and selected endpoints as criteria<br><br>For more information, see <a href="#">Starting a One-time Investigation on page 21-25</a> . |



| ACTION            | DESCRIPTION   |
|-------------------|---|
| Isolate Endpoints | <p data-bbox="588 251 1099 277">Disconnects the selected endpoints from the network.</p> <hr data-bbox="588 313 1182 316"/> <div data-bbox="595 329 650 378">  </div> <p data-bbox="666 329 716 350"><b>Note</b></p> <p data-bbox="666 365 1180 488">After resolving the security threats on an isolated endpoint, the following locations on the <b>Directories &gt; Users/Endpoints</b> screen provides options to restore the network connection of an isolated endpoint:</p> <ul data-bbox="696 516 1180 721" style="list-style-type: none"> <li data-bbox="696 516 1180 607">• <b>Endpoints &gt; All:</b> Click the name of an endpoint in the table, and click <b>Task &gt; Restore</b> on the screen that appears.</li> <li data-bbox="696 634 1180 721">• <b>Endpoints &gt; Filters &gt; Network Connection &gt; Isolated:</b> Select the endpoint row in the table, and click <b>Task &gt; Restore Network Connection</b>.</li> </ul> |

## Supported IOC Indicators for Historical Investigations

An OpenIOC file is an XML file which contains one or more Indicators of Compromise (IOCs). Verify that the OpenIOC file uses indicator terms supported by the type of investigation selected.

The table below lists the IOC indicators supported in investigations.

**TABLE 21-2. Supported IOC Indicators for Historical Investigations**

| CATEGORY     | ITEM                   | REQUIRED CONDITION |
|--------------|------------------------|--------------------|
| DNSENTRYITEM | HOST                   | IS                 |
|              | RECORDDATA/HOST        | IS                 |
|              | RECORDDATA/IPV4ADDRESS | IS                 |
| FILEITEM     | FILENAME               | IS                 |
|              | SHA1SUM                | IS                 |

| CATEGORY     | ITEM  | REQUIRED CONDITION |
|--------------|---|--------------------|
|              | SHA2SUM                                     | IS                 |
|              | MD5SUM                                      | IS                 |
| PORTITEM     | LOCALIP                                     | IS                 |
|              | REMOTEIP                                    | IS                 |
| PROCESSITEM  | ARGUMENTS                                   | CONTAINS           |
|              | NAME  | IS                 |
|              | SECTIONLIST/<br>MEMORYSECTION/SHA1SUM       | IS                 |
|              | SECTIONLIST/<br>MEMORYSECTION/<br>SHA256SUM | IS                 |
|              | SECTIONLIST/<br>MEMORYSECTION/MD5SUM        | IS                 |
| REGISTRYITEM | KEYPATH                                     | CONTAINS           |
|              | VALUE                                       | CONTAINS           |
|              | VALUENAME                                   | CONTAINS           |
|              | USERNAME                                    | IS                 |

**Note**

After selection, Endpoint Sensor displays a preview of the OpenIOC file. Review the preview to verify if the OpenIOC file contains supported indicators and conditions. Unsupported combinations are formatted with a strike-through and are ignored during the investigation.

## Starting a Root Cause Analysis from an Assessment

The Root Cause Analysis is an investigation tool that displays the sequence of events leading to the execution of the matched object.

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.

Generating a Root Cause Analysis may take some time to complete.

---

### Procedure

1. Perform a Historical Investigation.

On the results pane, review the results that appear.

For more information, see [Using User-defined Criteria for Historical Investigations on page 21-5](#).

2. Identify and select one or more endpoints, and click **Generate Root Cause Analysis**.
3. Specify a name for the new **Root Cause Analysis** task.
4. Review the criteria displayed.
  - For assessments using user-defined criteria, generating a **Root Cause Analysis** combines multiple criteria using either the AND or OR operator.
  - For assessments using an OpenIOC file, generating a **Root Cause Analysis** uses the indicators in the current OpenIOC file as criteria.
5. Review the target endpoints.

**Note**

To remove endpoints from the list, click the delete icon.

---

6. Specify a period.

By default, the analysis is performed on all logged dates.

7. Click **Generate**.
8. Go to the **Root Cause Analysis Results** tab to monitor the progress of the analysis.

Generating a Root Cause Analysis may take some time to complete.

For more information, see [Root Cause Analysis Results on page 21-20](#).

9. After the task to complete, click the **Task** name.

**Note**

The task name is not displayed as a link if Endpoint Sensor is unable to generate a Root Cause Analysis, and may be due to the following reasons:

- The target endpoint has insufficient data.  
  
Verify that the data has not been purged. If the agent database reaches the maximum database size limit, Endpoint Sensor purges the oldest logs to make space for new event entries. To avoid this issue, specify a larger agent database size.
- The investigation was unable to find an object that matches all of the conditions specified in the OpenIOC file.

Assessments ignore all conditions in the OpenIOC file to return the initial results. However, a Root Cause Analysis task adds the conditions back as an additional criteria for the investigation. As a result, the Root Cause Analysis task may be unable to generate results that match both the OpenIOC criteria and its conditions.

- 
10. Review the results.
- 

## Root Cause Analysis Results

To monitor the progress of a Root Cause Analysis task, go to **Response > Historical Investigation**, and click the **Root Cause Analysis Results** tab.

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.

Generating a Root Cause Analysis may take some time to complete.

For more information, see [Starting a Root Cause Analysis from an Assessment on page 21-18](#).

The following table lists the investigations details available for review.

| <b>COLUMN NAME</b> | <b>DESCRIPTION</b>                       |
|--------------------|--|
| Status             | Progress of the Root Cause Analysis task |

| COLUMN NAME     | DESCRIPTION  |
|-----------------|--|
| Name            | <p>Name of the Root Cause Analysis task</p> <p>Click to open the <b>Analysis Chains</b> and <b>Object Details</b> screens.</p> <p>For more information, see <a href="#">Analysis Chains on page 21-35</a>.</p> <hr/> <p> <b>Note</b></p> <p>The task name is not displayed as a link if Endpoint Sensor is unable to generate a Root Cause Analysis, and may be due to the following reasons:</p> <ul style="list-style-type: none"> <li>The target endpoint has insufficient data.</li> </ul> <p>Verify that the data has not been purged. If the agent database reaches the maximum database size limit, Endpoint Sensor purges the oldest logs to make space for new event entries. To avoid this issue, specify a larger agent database size.</p> <ul style="list-style-type: none"> <li>The investigation was unable to find an object that matches all of the conditions specified in the OpenIOC file.</li> </ul> <p>Assessments ignore all conditions in the OpenIOC file to return the initial results. However, a Root Cause Analysis task adds the conditions back as an additional criteria for the investigation. As a result, the Root Cause Analysis task may be unable to generate results that match both the OpenIOC criteria and its conditions.</p> |
| Criteria        | Criteria specified for the Root Cause Analysis task  |
| Matched Objects | <p>Number of matching objects found in the endpoint</p> <p>Click the value to view more details.</p>   |
| Asterisk (*)    | Indicates an endpoint tagged as <i>Important</i>   |

| COLUMN NAME | DESCRIPTION  |
|-------------|--|
| Endpoint    | Name of the endpoint containing the matching object<br>Click the <b>Endpoint</b> name to view more details about the endpoint. |
| IP Address  | IP address of the endpoint containing the matching object<br>The IP address is assigned by the network                         |
| Started     | Date and time when the Root Cause Analysis task was started  |
| Elapsed     | Length of time elapsed since starting the task   |
| Creator     | User who created the task  |

To delete a Root Cause Analysis task, select an entry in the table and click **Delete**.

## Live Investigations

Live Investigations perform the investigation on the current system state. Live Investigations can be configured to run at specific periods, and also support a wider set of criteria through the use of OpenIOC and YARA rules.



### Important

Only available for Security Agents installed on Windows platforms.

---

Live Investigations support the following criteria:

- **OpenIOC rules:** Use OpenIOC rules to scan for all files currently on the disk.

**Note**

After selection, Endpoint Sensor displays a preview of the OpenIOC file. Review the preview to verify if the OpenIOC file contains supported indicators and conditions. Unsupported combinations are formatted with a strike-through and are ignored during the investigation.

For more information, see [Supported IOC Indicators for Live Investigations on page 21-32](#).

---

- **YARA rules:** Use YARA rules to scan all processes currently running in memory.
- 

**Note**

Root Cause Analysis results are only available for YARA rules.

Because Live 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 Historical Investigation.

For more information, see [Historical Investigations on page 21-3](#).

---

- **Search registry:** Specify registry keys, names and data to match on the target endpoints.
- 

**Note**

Investigations are performed only on registry values under the following root keys:

- HKEY\_CURRENT\_USER
  - HKEY\_CLASSES\_ROOT
  - HKEY\_LOCAL\_MACHINE
  - HKEY\_USERS
-



Administrators can specify the type of Live Investigation to run:

- A one-time investigation runs only once. The investigation runs immediately after creation.

For more information, see [Starting a One-time Investigation on page 21-25](#).

- A scheduled investigation can be configured to run automatically at specific intervals.

For more information, see [Starting a Scheduled Investigation on page 21-28](#).

Live Investigations take some time to complete.

## Starting a One-time Investigation

---

### Procedure

1. Go to **Response > Live Investigation**.
2. Click the **One Time Investigation** tab.
3. Click **New Investigation**.
4. Specify a **Name** for this investigation.
5. Select a **Method** based on what objects need to be matched:
  - **Scan disk files using OpenIOC:** objects on the disk that match the rules provided in an OpenIOC file



#### Note

After selection, Endpoint Sensor displays a preview of the OpenIOC file. Review the preview to verify if the OpenIOC file contains supported indicators and conditions. Unsupported combinations are formatted with a strike-through and are ignored during the investigation.

For more information, see [Supported IOC Indicators for Live Investigations on page 21-32](#).

---

- **Scan in-memory processes using YARA:** objects currently in memory that match the rules provided in a YARA file
  - **Search registry:** registry keys, names and data that match criteria defined by the user
6. Click **Select Endpoints** and specify which endpoints to include in the investigation.

**Note**

The **Target Endpoints** screen may not show all endpoints selected for the investigation.

- A user can only view endpoints where he has been granted sufficient access rights.
- Only available for Security Agents installed on Windows platforms.

7. Click **Start Investigation**.
8. To view the results and monitor the progress of one-time investigations:
- a. Go to **Response > Live Investigation**.
  - b. Click the **One Time Investigation** tab.

For details, see [One-Time Investigation on page 21-26](#).


## One-Time Investigation

A one-time investigation is an investigation that runs only once.

To view the results and monitor the progress of one-time investigations, go to **Response > Live Investigation**, and click the **One Time Investigation** tab.

The following details are available for review.

| COLUMN | DESCRIPTION                        |
|--------|------------------------------------|
| Status | Current state of the investigation |

| COLUMN            | DESCRIPTION  |
|-------------------|--|
| Progress          | Percentage of completion of the investigation  |
| Name              | User-defined name that identifies the investigation<br>Click to view the investigation results.  |
| Method            | Method used by the investigation   |
| Criteria          | <ul style="list-style-type: none"> <li>File name of the OpenIOC or YARA rule file</li> <li>User-defined registry value</li> </ul>  |
| Matched Endpoints | Number of endpoints that contain an object matching the specified criteria   |
| Target Endpoints  | <p>Total number of selected endpoints for investigation<br/>Click to view more details about the selected endpoints.</p> <hr/> <p> <b>Note</b><br/>The <b>Target Endpoints</b> screen may not show all endpoints selected for the investigation. A user can only view endpoints where he has been granted sufficient access rights.</p> <hr/> |
| Started           | Date and time when the investigation started   |
| Elapsed           | Time elapsed since the start of the investigation  |
| Creator           | User who created the investigation   |

Click **New Investigation** to start a new investigation.

Select at least one investigation to enable the following options:

- **Stop:** Cancels the investigation. Stopped investigations cannot be resumed.
- **Delete:** Stops the investigation, and then removes the investigation from the list. Removed investigations cannot be recovered.

## Starting a Scheduled Investigation

---

### Procedure

1. Go to **Response > Live Investigation**.
2. Click the **Scheduled Investigation** tab.
3. Click **New Investigation**.
4. Specify a **Name** for this investigation.
5. Select a **Method** based on what objects need to be matched:
  - **Scan disk files using OpenIOC:** objects on the disk that match the rules provided in an OpenIOC file



#### Note

After selection, Endpoint Sensor displays a preview of the OpenIOC file. Review the preview to verify if the OpenIOC file contains supported indicators and conditions. Unsupported combinations are formatted with a strike-through and are ignored during the investigation.

For more information, see [Supported IOC Indicators for Live Investigations on page 21-32](#).

---

- **Scan in-memory processes using YARA:** objects currently in memory that match the rules provided in a YARA file
  - **Search registry:** registry keys, names and data that match criteria defined by the user
6. Click **Select Endpoints** and specify which endpoints to include in the investigation.

**Note**

The **Target Endpoints** screen may not show all endpoints selected for the investigation.

- A user can only view endpoints where he has been granted sufficient access rights.
  - Only available for Security Agents installed on Windows platforms.
- 

7. Specify a schedule for this investigation.
    - **Period:** Specify a starting and ending date for the investigation. The investigation only runs within the dates provided. The default period is set to one month.
    - **Frequency:** Specify how often the investigation repeats during the duration of the schedule. The default frequency is set to **Daily at 08:00**.
  8. Click **Start Investigation**.
  9. To view the results and monitor the progress of scheduled investigations:
    - a. Go to **Response > Live Investigation**.
    - b. Click the **Scheduled Investigation** tab.

For details, see [Scheduled Investigation on page 21-29](#).
    - c. To view details for each schedule run, click the investigation name to open the **Scheduled Investigation History** screen.


For details, see [Reviewing the Scheduled Investigation History on page 21-31](#).
- 

## Scheduled Investigation

A scheduled investigation is an investigation that is set to run automatically at certain periods.

To view the results and monitor the progress of scheduled investigations, go to **Response > Live Investigation**, and click the **Scheduled Investigation** tab.

The following table lists the details available for review.

| COLUMN                 | DESCRIPTION   |
|------------------------|---|
| Enable                 | Current state of the investigation  |
| Name                   | User-defined name that identifies the investigation<br>Click to open the <b>Scheduled Task History</b> screen.  |
| Method                 | Method used by the investigation  |
| Criteria               | File name of the OpenIOC file<br>User-defined registry value  |
| Target Endpoints       | Total number of selected endpoints for investigation<br>Click to view more details about the selected endpoints.<br><br><div style="border: 1px solid black; padding: 5px;">  <b>Note</b><br/>           The <b>Target Endpoints</b> screen may not show all endpoints selected for the investigation. A user can only view endpoints where he has been granted sufficient access rights.         </div> |
| Frequency              | How often the investigation repeats during the duration of the schedule   |
| Latest Investigation   | Date and time when the latest investigation started   |
| Latest Time Elapsed    | Time elapsed since the start of the latest investigation  |
| Latest Match Endpoints | Number of endpoints that contain an object matching the specified criteria for the latest investigation   |
| Creator                | User who created the investigation  |

Click **New Investigation** to start a new investigation.

Click **Delete** to stop the investigation, and then removes the investigation from the list. Removed investigations cannot be recovered.



#### Note

Deleting an OpenIOC file will automatically disable any scheduled investigation that uses the deleted OpenIOC file.

## Reviewing the Scheduled Investigation History

Use the **Scheduled Investigation History** screen to view past schedules and monitor the progress of running schedules.

### Procedure

1. Access the **Scheduled Investigation History** screen:
  - a. Go to **Response > Live Investigation**.
  - b. On the **Scheduled Investigation** tab, click a value in the **Name** column.
2. Review the details listed in the schedule overview:
  - **Task name:** Name given to the schedule
  - **Period and frequency:** Shows when and how often the schedule runs the investigation.
  - **Method:** Criteria used for each run of the schedule. Click to show the full criteria.
  - **Target endpoints:** Click to view the list of endpoints included in the schedule.
3. Review the investigation details for each run of the schedule.

| COLUMN NAME | DESCRIPTION                                   |
|-------------|---|
| Status      | Current state of the investigation            |
| Progress    | Percentage of completion of the investigation |

| COLUMN NAME       | DESCRIPTION  |
|-------------------|--|
| Matched Endpoints | Number of endpoints that contain an object matching the specified criteria<br><br>Click to open the <b>Investigation Results</b> screen. |
| Started           | Date and time the investigation started  |
| Elapsed           | Time elapsed since the start of the investigation<br><br>For completed investigations, total time spent running the investigation        |

4. Select at least one investigation to enable the following options:
  - **Stop:** Cancels the investigation. Stopped investigations cannot be resumed.
  - **Delete:** Stops the investigation, and then removes the investigation from the list. Removed investigations cannot be recovered.

## Supported IOC Indicators for Live Investigations

An OpenIOC file is an XML file which contains one or more Indicators of Compromise (IOCs). Verify that the OpenIOC file uses indicator terms supported by the type of investigation selected.

The table below lists the IOC indicators supported in investigations.



### Important

When choosing an IOC file, you must ensure that the IOC indicators include the location of the file to match (either "FileItem/FullPath" or "FileItem/FilePath").

| CATEGORY | ITEM     | REQUIRED CONDITION | NOTES   |
|----------|----------|--------------------|---|
| FILEITEM | FULLPATH | IS                 | Refers to a complete directory path, file name, and extension |



| CATEGORY | ITEM        | REQUIRED CONDITION                   | NOTES  |
|----------|-------------|--------------------------------------|--|
|          | FILEPATH    | IS, CONTAINS, STARTS-WITH, ENDS-WITH | Partial matching supported                       |
|          | FILENAME    | IS, CONTAINS, STARTS-WITH, ENDS-WITH | Partial matching supported                       |
|          | MD5SUM      | IS                                   |  |
|          | SHA1SUM     | IS                                   |  |
|          | SHA256SUM   | IS                                   |  |
|          | SIZEINBYTES | IS                                   |  |
|          | CREATED     | GREATER-THAN, LESS-THAN              | Required format (in UTC):<br>yyyy-mm-ddThh:mm:ss |
|          | MODIFIED    | GREATER-THAN, LESS-THAN              | Required format (in UTC):<br>yyyy-mm-ddThh:mm:ss |
|          | ACCESSED    | GREATER-THAN, LESS-THAN              | Required format (in UTC):<br>yyyy-mm-ddThh:mm:ss |



### Note

After selection, Endpoint Sensor displays a preview of the OpenIOC file. Review the preview to verify if the OpenIOC file contains supported indicators and conditions. Unsupported combinations are formatted with a strike-through and are ignored during the investigation.

## Investigation Results





Use the **Investigation Results** screen to get a quick overview of the investigation results. This screen is accessible from the following locations:

- On the **One Time Investigation** tab, click the investigation **Name**.
- On the **Scheduled Investigation** tab, click the investigation **Name**, and then click a value in the **Matched Endpoints** column.

This screen displays the following information:

- A doughnut chart that shows the number of total endpoints already classified as **Matched**, **No Match**, **Queued** or **Cancelled**

A summary of the totals is given on the left of the chart. This summary updates in real time as the investigation progresses.

| ICON  | LABEL     | DESCRIPTION   |
|---|-----------|---|
|  | Matched   | Number of investigated endpoints containing a matching object   |
|  | No match  | Number of investigated endpoints that did not have a matching object  |
|  | Queued    | Number of endpoints still to be investigated.<br>An investigation is complete once there are no more queued endpoints to investigate. |
|  | Cancelled | Number of endpoints not investigated.<br>This may be due to user cancellation, system error, or endpoint timeout.                     |


- Parameters used when the investigation was created.

Click **Criteria** to review the search conditions used by the investigation.

- A table of results which provides more details about each endpoint included in the investigation.

This table groups the endpoints into tabs based on the investigation status. This table displays the following details:




| COLUMN NAME  | DESCRIPTION  |
|--------------|--|
| Asterisk (*) | Indicates an endpoint tagged as "Important"  |
| Endpoint     | Name of the endpoint containing the matching object<br>Click the <b>Endpoint</b> name to view more details about the endpoint. |
| IP Address   | IP address of the endpoint containing the matching object<br>The IP address is assigned by the network.                        |




| COLUMN NAME         | DESCRIPTION  |
|---------------------|--|
| Operating System    | Operating system used by the endpoint  |
| User                | <p>User name of the user logged in when the Endpoint Sensor agent first logged the matched object</p> <p>Click the user name to view more details about the user.</p>  |
| Match Details       | Click to view details of the match.  |
| Root Cause Analysis | <p>Click to view the <b>Root Cause Analysis</b> screen.</p> <hr/> <p> <b>Note</b></p> <p>Root Cause Analysis results are only available for YARA rules.</p> <p>Because Live 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 Historical Investigation.</p> <p>For details, see <a href="#">Starting a Root Cause Analysis from an Assessment on page 21-18</a>.</p> |
| Elapsed             | Time elapsed since the investigation started.  |

## Analysis Chains


The **Analysis Chains** tab displays the Root Cause Analysis and also highlights additional information which might be beneficial to the investigation.

Threat Investigations can correlate information from Endpoint Sensor and Active Directory to display attack information about endpoints and user accounts throughout your network.

| INFORMATION           | DESCRIPTION   |
|-----------------------|---|
| Target Endpoint       | <p>Displays details about the endpoint that was investigated</p> <p>Click the endpoint name and user name to view details.</p> <p>Click <b>Isolate Endpoint</b> to disconnect the endpoint from the network. During isolation, the agent can only communicate with the server.</p> <hr/> <p> <b>Note</b></p> <p>After resolving the security threats on an isolated endpoint, the following locations on the <b>Directories &gt; Users/Endpoints</b> screen provides options to restore the network connection of an isolated endpoint:</p> <ul style="list-style-type: none"> <li>• <b>Endpoints &gt; All:</b> Click the name of an endpoint in the table, and click <b>Task &gt; Restore</b> on the screen that appears.</li> <li>• <b>Endpoints &gt; Filters &gt; Network Connection &gt; Isolated:</b> Select the endpoint row in the table, and click <b>Task &gt; Restore Network Connection</b>.</li> </ul> |
| First Observed Object | <p>The first object in the analysis chain suspected to have been responsible for the creation of the investigated object.</p> <p>This is often the entry point of a targeted attack.</p> <p>Hover over an object and click  to locate the object in the Analysis Chain.</p>  |
| Matched Objects       | <p>Displays the object or a list of objects matching the investigation criteria</p> <p>Hover over an object and click  to locate the object in the Root Cause Analysis.</p>  |

| INFORMATION              | DESCRIPTION  |
|--------------------------|--|
| Noteworthy Objects       | <p>Highlights objects in the chain that are possibly malicious, based on existing Trend Micro intelligence</p> <p>The value counts the number of unique noteworthy objects in the chain.</p> <p>Click to view the list of noteworthy objects.</p> <p>Hover over an object and click  to locate the object in the Analysis Chain.</p>  |
| Root Cause Analysis area | <p>Displays a visual analysis of the objects involved in an event</p> <hr/> <p> <b>Note</b></p> <p>If the number of nodes in the analysis chain exceeds the presentation limit, only the main analysis chains are displayed. To avoid this issue, refine the investigation criteria.</p> <hr/> <p>Click any available node to view more information about the selected object.</p> <p>For more information on how to interpret Analysis Chains, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Object Details: Profile Tab on page 21-38</a></li> </ul> <hr/> <p> <b>Note</b></p> <p>The <b>Profile</b> tab is the default view if no other tabs are available for a selected object.</p> <hr/> <ul style="list-style-type: none"> <li>• <a href="#">Object Details: Related Objects Tab on page 21-39</a></li> <li>• <a href="#">Navigating the Analysis Chain on page 21-40</a></li> <li>• <a href="#">Root Cause Analysis Icons on page 21-41</a></li> </ul> |

**Note**

To export the data, click  and perform one of the following:

- Select **Analysis Chains** to export all root cause chains as .png files.
- Select **Object Details** to export all data as CSV files.

## Object Details: Profile Tab

The **Profile** tab shows the details applicable for the selected object type.



Some objects may show only a limited set of details, or may not have any details available at the time of execution.

**Note**

You can further examine objects with “Malicious” ratings in Threat Connect or VirusTotal.

The tab may also display additional options for **Matched Objects** and **Noteworthy Objects**.

| OPTION                  | DESCRIPTION   |
|-------------------------|---|
| <b>Terminate Object</b> | <p data-bbox="427 938 1032 992">Terminates all running instances of the object only on the target endpoint's current state</p> <hr/> <div data-bbox="434 1045 494 1096" data-label="Image"></div> <div data-bbox="501 1042 555 1065" data-label="Section-Header"><b>Note</b></div> <p data-bbox="505 1078 1080 1170">This action is available only for unrated, malicious, and suspicious “process” type objects. To verify if the command was successful, go to <b>Administration &gt; Command Tracking</b>.</p> |

| OPTION                                      | DESCRIPTION  |
|---|--|
| <b>Add to Suspicious Objects List</b>       | <p>Terminates all running instances of the object only on the target endpoint's current state, and then adds the object to the <b>User-Defined Suspicious Object</b> list</p> <hr/> <p> <b>Note</b><br/>If Application Control is enabled, processes that match the hash value of objects added to the <b>User-Defined Suspicious Object</b> list are not allowed to run on all endpoints. Endpoint Sensor also terminates “process” type objects before adding them to the list, and Application Control prevents them from starting again.</p>                      |
| <b>Add to Historical Investigation List</b> | <p>Adds the object as criteria for a new Historical Investigation</p> <p>To start the investigation, click the <b>Start a Historical Investigation</b> button above the Analysis Chain.</p> <hr/> <p> <b>Note</b><br/>If you decide that you no longer want to perform a Historical Investigation on an object in the Analysis Chain, click the object and then click the <b>Remove from Historical Investigation List</b> button.</p> <hr/> <p>For more information, see <a href="#">Using User-defined Criteria for Historical Investigations on page 21-5</a>.</p> |

## Object Details: Related Objects Tab

The **Related Objects** tab displays all the dependencies of the selected object.



### Note

The **Related Objects** tab only displays additional information for “Process” objects.

These are the objects required to run the matched object. This tab displays the following details:

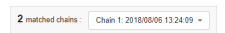
| PROPERTY           | DESCRIPTION   |
|--------------------|---|
| Action             | Action done by the object                                       |
| Logged             | Date and time of the recorded action                            |
| Rating             | Rating assigned to the object based on Trend Micro intelligence |
| Affected Endpoints | Affected endpoints, if any                                      |
| Destination path   | Target destination of the object                                |

The following options are available to manage the **Related Objects** tab:


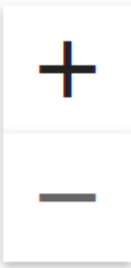

- The tab provides a drop-down that can filter objects based on the specified action. Click the drop down to view all available actions.
- Click **Show details** to view more details about the object.

## Navigating the Analysis Chain

To navigate the analysis chain, click and drag the area or use the available navigation icons.


| ICON  | DESCRIPTION   |
|---|---|
|  | <p>A Root Cause Analysis can contain one or more matched root cause chains.</p> <p>Click the drop-down to view other analysis chains for the selected endpoint.</p> |















| ICON   | DESCRIPTION  |
|--|--|
| <b>Start a Historical Investigation</b>  | <p>Click to start a Historical Investigation using the objects in the Historical Investigation list.</p> <p>If there are no objects in the Historical Investigation list, this feature is not available.</p> <p>To enable this feature, add at least one matched object or noteworthy object to the Historical Investigation list.</p> |
|   | <p>Click to enter full screen mode.</p> <p>Click again to exit full screen mode.</p>   |
|   | <p>Click to zoom in or zoom out.</p>   |
|  | <p>Hover to view an explanation of the symbols appearing in the analysis chain.</p> <p>For more information, see <a href="#">Root Cause Analysis Icons on page 21-41</a>.</p>  |

## Root Cause Analysis Icons

The analysis chain shows object types using the following icons:

| ICON  | NAME                  | DESCRIPTION   |
|---|-----------------------|---|
|  | First Observed Object | Marks an object that most likely created the matched object |

| ICON  | NAME              | DESCRIPTION  |
|---|-------------------|--|
|    | Matched Criteria  | Marks objects matching the investigation criteria  |
|    | Normal Object     | Marks objects that have been verified to not pose a threat<br>These are usually common system files. |
|    | Unrated Object    | Marks objects that have not yet been rated   |
|    | Suspicious Object | Marks objects that exhibit behaviors that are similar to known threats                               |
|    | Malicious Object  | Marks objects that match a known threat  |
|    | Boot              | Objects that launch during system startup  |
|    | Browser           | Objects that are capable of displaying web pages, usually a web browser                              |
|    | Email client      | Objects that can send and receive email messages, usually an email client or server                  |
|   | File              | 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  |

| ICON | NAME        | DESCRIPTION                                 |
|------|-------------|---|
| →    | Event       | Indicates actions done by the object        |
| ---  | Association | Indicates relationships between two objects |

## Object Details

The **Object Details** tab displays the same information as the **Root Cause Analysis** tab, but presents the information as a table. It also organizes the objects into the following tabs:


- **Objects:** Objects involved in the execution of the matched object, grouped by their parent processes. Click ► to expand the list.
- **Noteworthy events:** Objects in the chain that are possibly malicious, based on existing Trend Micro intelligence
- **File events:** Objects in the chain that are files
- **Registry events:** Objects in the chain that are registry keys, data and entries
- **IP address / DNS events:** Objects that are IP addresses or DNS events

The table provides the following details:

| COLUMN NAME     | DESCRIPTION  |
|-----------------|--|
| Recorded Object | Name of the recorded object<br>Click the object name to view more details. |
| PID             | Process ID of the recorded object  |
| Recorded        | Date and time when the object became involved in the chain                 |
| Activity        | Action done by the object<br>Click the object name to view more details.   |

| COLUMN NAME        | DESCRIPTION   |
|--------------------|---|
| Object Reputation  | Rating assigned to the object based on Trend Micro intelligence<br>You can further examine objects with “Malicious” ratings in Threat Connect or VirusTotal.  |
| Affected Endpoints | Number of endpoints where the object appears<br>Percentage of endpoints affected, based on the total number of endpoints on the network<br>Click the value to view more details about the endpoint. |

Use the following options to manage the table:

- On all tabs, select at least one object in the **Recorded Object** column, and click **Start a Historical Investigation** to start another investigation.
- On the **Objects** tab, click the filter icon (  ) to filter the table according to the specified criteria.
- On the **File events** tab, sort the table by clicking on the **Recorded** and **Object Reputation** columns.

# Chapter 22

## Managed Detection and Response

This chapter discusses how to configure Managed Detection and Response settings and administer investigation tasks using the Apex Central console.

Topics include:

- *Managed Detection and Response Overview on page 22-2*
- *Tracking Managed Detection and Response Task Commands on page 22-16*
- *Querying Supported Targets on page 22-18*
- *The Threat Investigation Center Agent for Managed Detection and Response on page 22-20*

## Managed Detection and Response Overview

The **Managed Detection and Response** screen allows you to deploy Managed Detection and Response settings and investigation tasks to specified targets from the Apex Central console.



### Tip

- To view the status of Managed Detection and Response task commands, use the **Command Tracking** screen.


For more information, see [Tracking Managed Detection and Response Task Commands on page 22-16](#).

- To perform an advanced search for targets that support the Managed Detection and Response Service, use the **User/Endpoint Directory** screen.

For more information, see [Querying Supported Targets on page 22-18](#).

Use the **Managed Detection and Response** screen to perform the following tasks.

| TASK   | DESCRIPTION  |
|--|--|
| Register to the Threat Investigation Center server     | <p>Click the <b>Settings</b> tab to register Apex Central to the Threat Investigation Center server.</p> <p>Apex Central integrates with Trend Micro Threat Investigation Center to enable Managed Detection and Response capabilities.</p> <p>For more information, see <a href="#">Registering Apex Central to the Threat Investigation Center on page 22-3</a>.</p> |
| Unregister from the Threat Investigation Center server | <p>Click the <b>Settings</b> tab to unregister Apex Central to the Threat Investigation Center server.</p> <p>For more information, see <a href="#">Unregistering from the Threat Investigation Center Server on page 22-5</a>.</p>  |

| TASK   | DESCRIPTION  |
|--|--|
| Suspend or resume the Managed Detection and Response Service | <p>Click the <b>Settings</b> tab to suspend or resume the Managed Detection and Response Service.</p> <hr/> <p> <b>Important</b></p> <p>Suspending the Managed Detection and Response Service stops the receipt of new investigation tasks and the sending of logs to the Threat Investigation Center server. Apex Central does not cancel any ongoing tasks and the results are still sent to the Threat Investigation Center server.</p> <hr/> <p>For more information, see <a href="#">Suspending or Resuming the Managed Detection and Response Service on page 22-6</a>.</p> |
| Approve or reject new investigation tasks                    | <p>Click the <b>Pending Tasks</b> tab to approve or reject new investigation tasks.</p> <p>For more information, see <a href="#">Approving or Rejecting Investigation Tasks on page 22-7</a>.</p>  |
| Track deployed investigation tasks                           | <p>Click the <b>Task Tracking</b> tab to track and view approved or rejected investigation tasks and commands.</p> <p>For more information, see <a href="#">Tracking Investigation Tasks on page 22-12</a>.</p>  |
| View automated analyses                                      | <p>Click the <b>Automated Analyses</b> tab to view information about the log data that Trend Micro collects to further protect your network.</p> <p>For more information, see <a href="#">Viewing Automated Analyses on page 22-15</a>.</p>  |

## Registering Apex Central to the Threat Investigation Center

Apex Central integrates with Trend Micro Threat Investigation Center to enable Managed Detection and Response capabilities.



### Important

- Managed Detection and Response capabilities require purchasing a service plan to obtain a valid server address and company GUID. Contact Trend Micro sales or your reseller to purchase a service plan.
- 

## Procedure

1. Go to **Response > Managed Detection and Response**.

The **Managed Detection and Response** screen appears.

2. Click the **Settings** tab.

3. Specify the following information:

- **Server address:** The Threat Investigation Center server address provided by Trend Micro sales or your reseller
- **Company GUID:** The Managed Detection and Response Service GUID provided by Trend Micro sales or your reseller

4. Configure automatic approval settings for new investigation tasks.
- 



### Note

- If automatic approval is enabled, Apex Central will send email notifications to inform recipients of new automatically approved investigation tasks.
  - If automatic approval is disabled, Apex Central will send email notifications for all new investigation tasks to request manual approval.
- 

- Select the **Automatically approve investigation tasks** check box to enable automatic approval of new investigation tasks.
- Clear the **Automatically approve investigation tasks** check box to disable automatic approval of new investigation tasks.



---

## 5. (Optional) Configure notification recipients.



### Note

- You can add new user accounts on the **User Accounts** screen (**Administration > Account Management > User Accounts**).
  - You can add new contact groups on the **Contact Groups** screen (**Detections > Notifications > Contact Groups**).
- 

- To add recipients, select contacts from the **Available Users and Groups** list and click >.

The selected contacts appear in the **Selected Users and Groups** list.

- To remove recipients, select contacts from the **Selected Users and Groups** list and click <.

The selected contacts appear in the **Available Users and Groups** list.

## 6. Click **Register**.

- The **Server address** field displays the address of the registered Threat Investigation Center server.
  - The **Sender ID** field replaces the **Company GUID** field and displays the GUID of the Apex Central server that receives investigation tasks from the registered Threat Investigation Center server.
- 

## Unregistering from the Threat Investigation Center Server

---



### Important

Unregistering automatically disables the Managed Detection and Response Service.

---

---

### Procedure

1. Go to **Response > Managed Detection and Response**.

The **Managed Detection and Response** screen appears.

2. Click the **Settings** tab.

3. Click **Unregister**.

A confirmation dialog appears.

4. Click **Unregister**.

The Managed Detection and Response Service automatically disables.

---

## Suspending or Resuming the Managed Detection and Response Service

---



### Important

Suspending the Managed Detection and Response Service stops the receipt of new investigation tasks and the sending of logs to the Threat Investigation Center server. Apex Central does not cancel any ongoing tasks and the results are still sent to the Threat Investigation Center server.

---

---

### Procedure

1. Go to **Response > Managed Detection and Response**.

The **Managed Detection and Response** screen appears.

2. Click the **Settings** tab.

3. To suspend the Managed Detection and Response Service:

- a. Click **Suspend Service**.

- b. On the confirmation dialog that appears:

- Click **Suspend Service** to suspend the Managed Detection and Response Service.

- Click **Cancel** to return to the **Settings** screen without suspending the Managed Detection and Response Service.
4. To resume the Managed Detection and Response Service, click **Resume Service**.

Apex Central resumes the receipt of new investigation tasks and the sending of logs to the Threat Investigation Center server.

---

## Approving or Rejecting Investigation Tasks

The **Pending Tasks** tab on the **Managed Detection and Response** screen displays investigation tasks submitted by the Threat Investigation Center that require manual administrator approval. You can view targets and commands for specific tasks, modify selected targets, and approve or reject selected tasks.

For more information about the Threat Investigation Center task commands that display on the **Managed Detection and Response** screen, see [Threat Investigation Center Task Commands on page 22-10](#).

---



### Tip

To view the status of Managed Detection and Response task commands, use the **Command Tracking** screen.

For more information, see [Tracking Managed Detection and Response Task Commands on page 22-16](#).

---



### Important

- Apex Central only retains investigation task information for 90 days after submission by the Threat Investigation Center.
- By default, new investigation tasks that are not approved or rejected within 72 hours of receipt by Apex Central will automatically time out.

For more information about investigation task command statuses, see [Threat Investigation Center Command Statuses on page 22-14](#).

---


## Procedure

1. Go to **Response > Managed Detection and Response**.

The **Managed Detection and Response** screen appears.


2. Click the **Pending Tasks** tab.

A table appears and displays a list of investigation tasks with the following information:

| COLUMN           | DESCRIPTION   |
|------------------|---|
| Task Description | The task name manually specified by the Threat Investigation Center administrator   |
| Command          | The task command to deploy to selected targets<br><br>For more information about the Threat Investigation Center task commands that display on the <b>Managed Detection and Response</b> screen, see <a href="#">Threat Investigation Center Task Commands on page 22-10</a> .  |
| Targets          | The number of targets for the task  |
| Expiration       | The local time on the Apex Central server for when the task will expire<br><br> <b>Important</b><br>By default, new investigation tasks that are not approved or rejected within 72 hours of receipt by Apex Central will automatically time out.<br><br>For more information about investigation task command statuses, see <a href="#">Threat Investigation Center Command Statuses on page 22-14</a> . |

3. To view targets for a pending task, click the right arrow icon (▶) next to the **Task Description** field.

A table appears and displays the following details:

| COLUMN                  | DESCRIPTION   |
|-------------------------|---|
| Endpoint                | The name of the target endpoint   |
| IP Address              | The IP address of the target endpoint   |
| User                    | The name of the user that last logged on to the target endpoint   |
| Endpoint Sensor Service | <p>The status of the Endpoint Sensor Service on the target endpoint</p> <p>For more information, see <a href="#">Endpoint Sensor Service Statuses on page 22-11</a>.</p> <hr/> <p> <b>Important</b></p> <p>In order for Apex Central to deploy investigation tasks to a specified target, the Endpoint Sensor Service must be enabled on the target.</p> <hr/> |

4. To approve pending investigation tasks:
- Select the check box next to the name of each task that you want to approve.

**Note**

Selecting a check box for a task selects all targets for that task.

- Click the right arrow icon (▶) next to a task name to modify selected targets for the task.

**Important**

In order for Apex Central to deploy investigation tasks to a specified target, the Endpoint Sensor Service must be enabled on the target.

- Select check box(es) next to the target(s) that you want to include.
- Clear check box(es) next to the target(s) that you want to exclude.

c. Repeat the previous steps for each pending task.

d. Click **Approve**.

Approved tasks display on the **Task Tracking** tab.

For more information, see [Tracking Investigation Tasks on page 22-12](#).

5. To reject pending investigation tasks:

a. Select the check box next to the name of each task that you want to reject.



**Note**

Selecting a check box for a task selects all targets for that task.

---

b. Click the right arrow icon (▶) next to a task name to modify selected targets for the task.

- Select check box(es) next to the target(s) that you want to include.
- Clear check box(es) next to the target(s) that you want to exclude.

c. Repeat the previous steps for each pending task.

d. Click **Reject**.

Rejected tasks display on the **Task Tracking** tab.

For more information, see [Tracking Investigation Tasks on page 22-12](#).

---


## Threat Investigation Center Task Commands

The following table describes the Threat Investigation Center task commands that display on the Apex Central **Managed Detection and Response** screen.

| COMMAND NAME                      | DESCRIPTION   |
|-----------------------------------|---|
| Collect File Samples              | Collects samples of suspicious files from target endpoints and sends the samples to the Threat Investigation Center           |
| Run Trend Micro Investigation Kit | Deploys and executes the Trend Micro Investigation Kit on target endpoints  |
| Run Advanced Threat Assessment    | Deploys and executes the Trend Micro Anti-Threat Toolkit on target endpoints  |
| Evaluate Impact                   | Starts an impact evaluation on target endpoints   |
| Run Root Cause Analysis           | Starts a root cause analysis on target endpoints by using criteria specified by the Threat Investigation Center administrator |

## Endpoint Sensor Service Statuses

The following table describes the agent statuses that display in the **Endpoint Sensor Service** column on the **Pending Tasks** tab.

| STATUS                                      | DESCRIPTION  |
|---|--|
| Enabled                                     | <p>The target endpoint has Endpoint Sensor enabled</p> <hr/> <p> <b>Important</b><br/>In order for Apex Central to deploy investigation tasks to a specified target, the Endpoint Sensor Service must be enabled on the target.</p> <hr/> |
| Disabled                                    | The target endpoint has Endpoint Sensor disabled   |
| Server license not supported                | The Apex One license does not support the Endpoint Sensor Service  |
| Requires a supported Security Agent version | The target endpoint does not have the Security Agent installed or the server version of the target endpoint is not supported   |

## Tracking Investigation Tasks

Use the **Task Tracking** tab on the **Managed Detection and Response** screen to track and view the statuses of approved or rejected investigation tasks and commands.



### Tip

To view the status of Managed Detection and Response task commands, use the **Command Tracking** screen.

For more information, see [Tracking Managed Detection and Response Task Commands on page 22-16](#).



### Important

Apex Central only retains investigation task information for 90 days after submission by the Threat Investigation Center.

## Procedure

1. Go to **Response > Managed Detection and Response**.

The **Managed Detection and Response** screen appears.

2. Click the **Task Tracking** tab.

A table appears and displays a list of investigation tasks with the following information:

| COLUMN           | DESCRIPTION   |
|------------------|---|
| Task Description | The task name manually specified by the Threat Investigation Center administrator   |
| Command          | The task command to deploy to selected targets<br>For more information, see <a href="#">Threat Investigation Center Task Commands on page 22-10</a> . |
| Targets          | The number of targets for the task  |



| COLUMN       | DESCRIPTION  |
|--------------|--|
| Task Status  | The deployment status of the investigation task<br>For more information, see <a href="#">Threat Investigation Center Task Statuses on page 22-13</a> . |
| Last Updated | The local time on the Apex Central server of the latest status update  |

- Click the right arrow icon (▶) next to a task description to view task command information.

A table appears and displays the following details:

| COLUMN                 | DESCRIPTION   |
|------------------------|---|
| Command Status         | The deployment status of the task command<br>For more information, see <a href="#">Threat Investigation Center Command Statuses on page 22-14</a> . |
| Endpoint               | The name of the target endpoint   |
| IP Address             | The IP address of the target endpoint   |
| User                   | The name of the user that last logged on to the target endpoint   |
| Approved / Rejected    | The local time on the Apex Central server for when the task was approved or rejected by the administrator   |
| Approved / Rejected By | The user account name of the administrator that approved or rejected the task   |
| Last Updated           | The local time on the Apex Central server of the latest status update   |

## Threat Investigation Center Task Statuses

The following table describes the statuses of the Threat Investigation Center tasks that display on the **Task Tracking** tab of the **Managed Detection and Response** screen.

For more information about the Threat Investigation Center task commands that display on the **Managed Detection and Response** screen, see [Threat Investigation Center Task Commands on page 22-10](#).

| STATUS      | DESCRIPTION   |
|-------------|---|
| In progress | Scenarios include: <ul style="list-style-type: none"> <li>• The task was approved but has not been deployed to the Apex One server</li> <li>• The task command was deployed to the Apex One server but has not been completed on the specified targets</li> </ul> |
| Completed   | The task was approved or rejected by the Apex Central administrator and completed on the specified targets successfully or unsuccessfully<br><br>For more information, see <a href="#">Threat Investigation Center Command Statuses on page 22-14</a> .           |

## Threat Investigation Center Command Statuses

The following table describes the command statuses that display on the **Task Tracking** screen.

| STATUS                    | DESCRIPTION  |
|---------------------------|--|
| Pending approval          | The task has not been approved or rejected by the Apex Central administrator                             |
| Rejected                  | The task has been rejected by the Apex Central administrator   |
| Sending command           | The task was approved and Apex Central is sending the task command to the specified targets              |
| In progress               | The task command was deployed to the Apex One server but has not been completed on the specified targets |
| Uploading                 | The managed product is uploading the task payload  |
| Successful                | The task command completed on the specified targets successfully   |
| Unable to process command | The task command completed on the specified targets unsuccessfully                                       |

| STATUS                                      | DESCRIPTION  |
|---|--|
| Command time-out                            | Scenarios include: <ul style="list-style-type: none"> <li>• The task was not approved by the Apex Central administrator within 72 hours of receipt</li> <li>• The managed product was unable to complete the task command within 9 days after approval</li> <li>• The task command timed out on the Apex One server</li> </ul> |
| No response from agent                      | The Apex One server is unable to establish communication with the target agent   |
| Endpoint Sensor disabled                    | The target endpoint has Endpoint Sensor disabled   |
| Requires a supported Security Agent version | The target endpoint does not have the Security Agent installed or the server version of the target endpoint is not supported   |
| Server license not supported                | The Apex One license does not support the Endpoint Sensor Service  |

## Viewing Automated Analyses

Trend Micro periodically performs automated analyses to collect log data to further protect your network. Use the **Automated Analyses** tab to view information about the logs that Trend Micro collects.



### Important

Apex Central only retains investigation task information for 90 days after submission by the Threat Investigation Center.

## Procedure

1. Go to **Response > Managed Detection and Response**.

The **Managed Detection and Response** screen appears.

2. Click the **Automated Analyses** tab.

A table appears and displays the following details:

| COLUMN     | DESCRIPTION   |
|------------|---|
| Start Time | The local time on the Trend Micro server for when the automated analysis task started   |
| End Time   | The local time on the Trend Micro server for when the automated analysis task completed |
| Status     | The status of the automated analysis task   |
| Command    | The type of automated analysis task   |
| Target     | The endpoint name or number of targets of the automated analysis task                   |

3. Click a count in the **Target** column to view targets.

The **Targets** screen appears and displays a list of affected endpoints.

## Tracking Managed Detection and Response Task Commands

Use the **Command Tracking** screen to query and view details of Managed Detection and Response task commands issued by the Apex Central server.

For information about tracking Threat Investigation Center task commands that display on the **Managed Detection and Response** screen, see [Tracking Investigation Tasks on page 22-12](#).



### Procedure

1. Go to **Administration > Command Tracking**.

The **Command Tracking** screen appears.

2. To filter the command list, specify the following:
  - **Issued:** Specify when Apex Central sent the task command
  - **Command:** Select the command type

Apex Central Managed Detection and Response task commands include the following:

| COMMAND NAME  | DESCRIPTION   |
|---|---|
| Deploy Threat Investigation Center settings to managed products | Command for deploying Threat Investigation Center settings to managed products  |
| Deploy Threat Investigation Center tasks to managed products    | Command for deploying Threat Investigation Center tasks to managed products   |
| Renew Threat Investigation Center certificate                   | <p>Command for renewing the Threat Investigation Center certificate on the Apex Central server</p> <hr/> <p> <b>Note</b><br/>The Threat Investigation Center server automatically deploys a task to renew the Threat Investigation Center certificate on the Apex Central server 30 days prior to the certificate expiration date.</p> |
| Pull Threat Investigation Center tasks                          | <p>Command for pulling tasks from the Threat Investigation Center server</p> <hr/> <p> <b>Note</b><br/>This command only displays on the <b>Command Tracking</b> screen if the task command is unsuccessful.</p>   |

- **User:** Provide the user account name used to send the command



**Tip**

Leave this field blank to query commands issued by all users.

- **Status:** Select one or more command statuses and click **Apply**.

- Click the count in the **Successful**, **Unsuccessful**, **In Progress**, or **All** column to view detailed command information.

The **Command Details** screen appears.

For more information, see [Command Details on page 13-4](#).

## Command Details

The **Command Details** screen displays the following information about an issued command.

| COLUMN NAME   | DESCRIPTION  |
|---------------|--|
| Last Reported | The date and time when the managed product last sent a response to the Apex Central server |
| Server/Entity | The host name of the managed product server  |
| Status        | The status of the issued command   |
| Description   | Additional details about the command status  |



### Note

The **Command Details** screen refreshes every 30 seconds.

## Querying Supported Targets

Use the **User/Endpoint Directory** screen to perform an advanced search for targets that support the Managed Detection and Response Service.

### Procedure

- Go to **Directories > Users/Endpoints**.

The **User/Endpoint Directory** screen appears.

- Click the **Advanced** link above the table.
- In the **Search** drop-down control, select **Endpoints**.

The search criteria in the second drop-down control dynamically changes based on your selection.

4. In the second drop-down control, select **Services**.  
A third drop-down control and a fourth drop-down control appear.
5. In the third drop-down control, select **Endpoint Sensor**.
6. In the fourth drop-down control, select the agent status:
  - **Enabled:** Searches for endpoints that have the Endpoint Sensor Service enabled
  - **Disabled:** Searches for endpoints that have the Endpoint Sensor Service disabled
7. Add multiple search criteria using the Boolean operators to the right of the filters.
  - **OR:** Allows you to search for multiple values for the specified criteria. All records that match either value display.
  - **AND:** Allows you to select a new search criteria. Only records that match the values specified for this criteria and all other selected criteria values display.
8. Display results by clicking one of the following:
  - **Search:** Displays the search results in the list but does not save the search criteria.
  - **Save as New Custom Filter:** Displays the search results in the list and prompts you to save the search criteria to a custom filter. The custom filter displays under the **Endpoints** node in the User/Endpoint Directory tree.
9. (Optional) Use the drop-down controls below the **Endpoints** tab to specify the time period for the data that displays or to switch between **Tabular view** and **Tabular view**.
10. (Optional) Click **Export** to export the data as a \*.csv file or \*.png image.

**Note**

- **Tabular view** only supports exporting data as a \*.csv file.
- **Timeline view** can export data as a \*.csv file or a \*.png image.

## The Threat Investigation Center Agent for Managed Detection and Response

The Threat Investigation Center Agent for Managed Detection and Response automatically sends the following information from the Apex Central server to the Threat Investigation Center server.

| DATA TYPE                    | DESCRIPTION   |
|------------------------------|---|
| Apex Central detection logs  | Includes logs related to system events, network events, and data protection events detected by managed products registered to the Apex Central server |
| Apex Central information     | Includes Apex Central server information  |
| Managed product information  | Includes information about Trend Micro products registered to the Apex Central server   |
| Managed endpoint information | Includes information about endpoints managed by Trend Micro products registered to the Apex Central server  |



# Chapter 23

## Suspicious Object Hub and Node Architecture

This section presents material administrators need to synchronize suspicious object lists across multiple Apex Central servers.

Topics include:

- *Suspicious Object Hub and Node Apex Central Servers on page 23-2*
- *Configuring the Suspicious Object Hub and Nodes on page 23-3*
- *Unregistering a Suspicious Object Node from the Hub Apex Central on page 23-4*
- *Configuration Notes on page 23-5*

## Suspicious Object Hub and Node Apex Central Servers

Trend Micro Apex Central™ Suspicious Object Hub and Node architecture allows you to synchronize suspicious object lists across multiple Apex Central servers. The suspicious object lists on the Hub Apex Central server consolidate the suspicious object lists from all Node Apex Central servers, and any other managed products registered to any of these servers, and then deploys the lists back to the Node Apex Central servers.

Administrators must first configure a Suspicious Object Hub Apex Central server and, depending on the environment, assign other Apex Central servers to act as Suspicious Object Node servers. Trend Micro Deep Discovery products can register to the Suspicious Object Hub or any Suspicious Object Node Apex Central server. This architecture requires that you configure all suspicious object actions through the Suspicious Object Hub Apex Central server console.

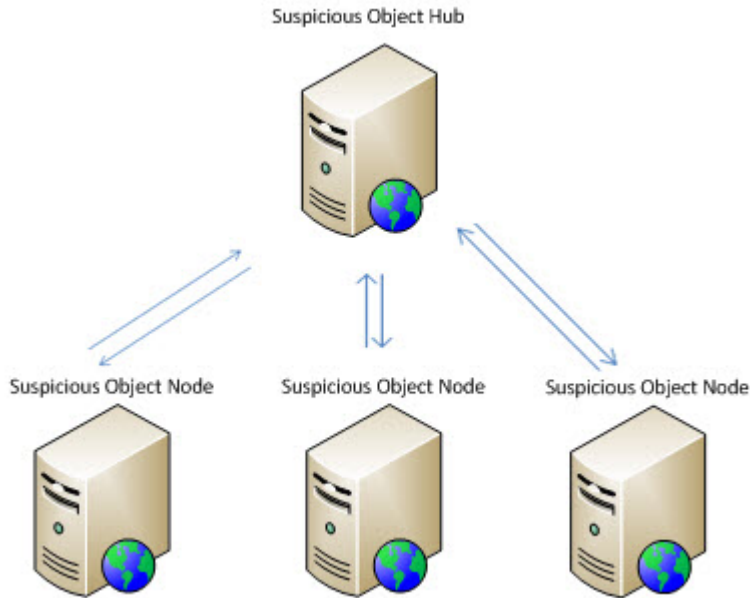


### **Important**

You must perform all operations on the suspicious object lists through the Suspicious Object Hub Apex Central to ensure that all Node Apex Central servers remain properly synchronized.

Scan actions performed on suspicious objects through a Suspicious Object Node Apex Central may not synchronize to all connected servers.

---



## Configuring the Suspicious Object Hub and Nodes

### Procedure

1. Log on to the Suspicious Object Hub Apex Central server console.
2. Go to **Threat Intel > Distribution Settings**.  
The **Distribution Settings** screen appears.
3. Click the **Managed Products** tab and copy (write down) the following settings:
  - **Service URL**
  - **API key**
4. Log on to the Suspicious Object Node Apex Central server console.

5. Go to **Threat Intel > Distribution Settings**.

The **Distribution Settings** screen appears.

6. On the **Hub Apex Central** tab, provide the following settings copied from the Suspicious Object Hub Apex Central:
  - **Service URL**
  - **API key**
7. (Optional) Select the **Use a proxy server** check box to connect to the Hub Apex Central through a proxy server.



**Note**

To configure or modify proxy server settings, click **Configure proxy settings**.

---

8. Click **Register**.

A confirmation dialog appears with a message indicating that the server is properly registered to the Hub Apex Central.

9. Repeat the process for each Suspicious Object Node Apex Central server.
  10. To configure the default synchronization interval:
    - a. Select a time period from the **Sync every** drop-down.
    - b. Click **Save**.
- 

## Unregistering a Suspicious Object Node from the Hub Apex Central

---



**Note**

After unregistering a Node Apex Central server, all previously synchronized objects remain in the Node Apex Central server suspicious object lists.

---

---

## Procedure

1. Log on to the Suspicious Object Node Apex Central server console.
  2. Go to **Threat Intel > Distribution Settings**.  
The **Distribution Settings** screen appears.
  3. In the **Hub Apex Central Settings** section, click **Unregister**.  
A confirmation dialog appears with a message indicating that the server is properly unregistered from the Hub Apex Central.
  4. If you are completely stopping the Suspicious Object Hub and Node deployment, repeat the process for each Suspicious Object Node Apex Central server.
- 

## Configuration Notes

After successfully setting up the Suspicious Object Hub and registering the Suspicious Object Node Apex Central servers, note the following configuration information.




### Note

After unregistering a Node Apex Central server, all previously synchronized objects remain in the Node Apex Central server suspicious object lists.

---

| CONFIGURATION                          | HUB APEX CENTRAL   | NODE APEX CENTRAL  |
|--|--|--|
| Synchronization interval               | N/A  | 5 minutes (default)  |
| Suspicious Object list synchronization | From the Hub Apex Central to Nodes: <ul style="list-style-type: none"> <li>• Virtual Analyzer list</li> <li>• User-Defined list</li> </ul> | From a Node Apex Central to the Hub: <ul style="list-style-type: none"> <li>• Virtual Analyzer list</li> </ul> |

| CONFIGURATION                                 | HUB APEX CENTRAL  | NODE APEX CENTRAL |
|---|---|-------------------|
|   | <div style="border: 1px solid black; padding: 5px;">  <b>Note</b> <ul style="list-style-type: none"> <li>• The Hub Apex Central server does not send data from the <b>Notes</b> column of the User-Defined list or the Exception list to the Node Apex Central servers.</li> <li>• When synchronizing lists, the User-Defined list has a higher priority than the Virtual Analyzer list.                             <ul style="list-style-type: none"> <li>• If an object is added to both the User-Defined list and the Virtual Analyzer list on the Hub Apex Central before the next synchronization, the Hub Apex Central server deploys both lists to the Node Apex Central servers.</li> <li>• If an object in the Node Apex Central Virtual Analyzer list also exists in the Hub Apex Central User-Defined list, the suspicious object risk level changes to “High” on the Node Apex Central Virtual Analyzer list during the next synchronization.</li> </ul> </li> </ul> </div> |                   |
| <p>Configuring Suspicious Object settings</p> | <p>Recommended</p> <p>Configuring Suspicious Objects through the Hub Apex Central ensures consistency across the registered Node Apex Central servers.</p>  | <p>N/A</p>        |

# **Part VII**

## **Automation Center**







# Chapter 24

## Apex Central Automation Center

Apex Central provides RESTful APIs that allow access to specific product functions. You can use the APIs to integrate third-party solutions with Apex Central, gather and share suspicious object information, and automate investigation and management tasks.

For more information, see <https://automation.trendmicro.com/apex-central/home>.



# **Part VIII**

## **Tools and Support**





# Chapter 25

## Administering the Database

This section presents material administrators will need to manage the Apex Central network.

Topics include:

- *Understanding the Apex Central Database on page 25-2*
- *Backing Up db\_ApexCentral Using SQL Server Management Studio on page 25-9*
- *Shrinking db\_ApexCentral\_Log.ldf Using SQL Commands on page 25-11*
- *Shrinking db\_ApexCentral\_log.ldf Using SQL Server Management Studio on page 25-12*

## Understanding the Apex Central Database

Apex Central uses the Microsoft SQL Server database (db\_ApexCentral.mdf) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings.

The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db\_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password.

To maximize the SQL server security, configure any SQL account used to manage db\_ApexCentral with the following minimum permissions:

- dbcreator for the server role
- db\_owner role for db\_ApexCentral

Logs from managed products contribute to database expansion. Managed products send various log types to Apex Central.

The following table lists the log count and database size for each log type.

**TABLE 25-1. Log Count and Database Size**

| LOG TYPE         | LOG COUNT | DATABASE SIZE (MB) |
|------------------|-----------|--------------------|
| Virus            | 100,000   | 150                |
|                  | 500,000   | 750                |
|                  | 1,000,000 | 1,500              |
| Spyware/Grayware | 100,000   | 150                |
|                  | 500,000   | 750                |
|                  | 1,000,000 | 1,500              |
| Web security     | 100,000   | 150                |
|                  | 500,000   | 750                |

| LOG TYPE             | LOG COUNT | DATABASE SIZE (MB) |
|----------------------|-----------|--------------------|
|                      | 1,000,000 | 1,500              |
| Behavior Monitoring  | 100,000   | 120                |
|                      | 500,000   | 600                |
|                      | 1,000,000 | 1,200              |
| Data Loss Prevention | 100,000   | 300                |
|                      | 500,000   | 1,500              |
|                      | 1,000,000 | 3,000              |
| File hash detection  | 100,000   | 180                |
|                      | 500,000   | 900                |
|                      | 1,000,000 | 1,800              |
| Attack Discovery     | 100,000   | 1,200              |
|                      | 500,000   | 6,000              |
|                      | 1,000,000 | 12,000             |
| Intrusion Prevention | 100,000   | 70                 |
|                      | 500,000   | 350                |
|                      | 1,000,000 | 700                |
| Application Control  | 100,000   | 200                |
|                      | 500,000   | 1,000              |
|                      | 1,000,000 | 2,000              |

The database space required for log storage can be calculated based on the log type and amount. For example:

- An Apex One managed product sends 20,000 virus logs and 10,000 web security logs to Apex Central daily.

- Apex Central keeps both log types for 90 days.

The database space required is 1.2 GB for virus logs and 1 GB for web security logs. However, there might be an additional space required for log summary or other features.

Because the Apex Central database runs on a scalable database — SQL Server, the theoretical limit is whatever the hardware can handle. Trend Micro has tested up to 2,000,000 entries. If the database server performance is overworked or pushed to its limit, the web console may experience connection time-outs.



#### Tip

Trend Micro recommends allocating a significant buffer space for database growth and monitoring the database to help obtain a precise database size measurement.

## Understanding the db\_ApexCentral Tables

To access all tables in the Apex Central database, use a Microsoft Access project (\*.adp/\*.ade) or Microsoft SQL Management Studio.



#### Note

Do not use any of the SQL tools to add, delete, or modify records without instructions from Trend Micro Technical Support.

The following tables make up the Apex Central database:

**TABLE 25-2. User/Endpoint Directory Tables**

| DIRECTORY MANAGEMENT TABLES | DESCRIPTION   |
|-----------------------------|---|
| tb_WebSecurityLog           | Stores Web access violation logs from products  |
| tb_SecurityLog              | Stores Content violation logs received from ScanMail and InterScan Messaging products |



| <b>DIRECTORY MANAGEMENT TABLES</b>  | <b>DESCRIPTION</b>   |
|---|--|
| tb_LogGeneral   | Stores Net packet scanning logs from network-based products such as Deep Discovery Inspector   |
| tb_LogDataLossPrevention  | Stores Data Loss Prevention related logs sent/received from products   |
| tb_AV*Log<br>* corresponds to Virus, Event, StatusEngineInfo, and StatusPatternInfo | Stores product logs<br>Virus table stores virus/malware incident logs detected by products. Other tables store the product status log as well as the pattern and engine version, update and deploy time, and unhandled virus counts. |
| tb_SpywareLog   | Stores malicious spyware information detected by product   |
| tb_PersonalFirewallLog  | Stores personal firewall detection log from OfficeScan   |
| tb_LogBehaviorMonitor   | Stores malicious system behavior incident detected by OfficeScan   |
| tb_Network_Content_Inspection_Engine_Log  | Stores blocked C&C server connection attempt logs from OfficeScan  |
| tb_FileHashDetectionLog   | Stores suspicious file detection logs from managed products  |
| tb_LogIntrusionPrevention   | Stores intrusion prevention logs from Deep Security and Vulnerability Protection   |
| tb_MachineLearning_Detection_Log  | Stores Predictive Machine Learning detection logs from OfficeScan  |
| tb_ApplicationControlEvent  | Stores endpoint application control violation logs from Endpoint Application Control   |
| tb_SandboxDetectionlog  | Stores Virtual Analyzer detection logs from managed products   |

**TABLE 25-3. Directory Management Tables**

| <b>DIRECTORY MANAGEMENT TABLES</b> | <b>DESCRIPTION</b>                     |
|------------------------------------|--|
| CDSM_Entity                        | Stores the managed product information |

| <b>DIRECTORY MANAGEMENT TABLES</b> | <b>DESCRIPTION</b>   |
|------------------------------------|--|
| CDSM_Agent                         | Stores Communicator information  |
| CDSM_Registry                      | Stores registry information  |
| CDSM_UserLog                       | Stores information as to who, which options, and what time a user accesses the web console; this is useful for auditing web console accesses |
| CDSM_SystemEventlog                | Stores system logs generated by internal processes   |

**TABLE 25-4. Server Command Controller Tables**

| <b>SERVER COMMAND CONTROLLER TABLES</b> | <b>DESCRIPTION</b>  |
|---|---|
| tb_TVCSCommandList                      | Stores managed product commands   |
| tb_TVCSCommandTaskQueue                 | Stores commands issued to managed products  |
| tb_CommandTracking                      | Stores command status   |
| tb_CommandItemTracking                  | Stores detailed command status  |
| tb_ProcessInfo                          | Stores information for MsgReceiver.exe, CmdProcessor.exe, LogReceiver.exe, LogRetriever.exe, etc. |
| tb_LoginUserSessionData                 | Stores user logon session control   |
| tb_ManualDownload                       | Stores manual download information  |
| tb_ScheduleDownload                     | Stores scheduled download information   |

**TABLE 25-5. Managed Product Tables**

| <b>MANAGED PRODUCT TABLES</b> | <b>DESCRIPTION</b>                     |
|-------------------------------|--|
| tb_EntityInfo                 | Stores the managed product information |

**TABLE 25-6. Log Tables**

| LOG TABLES   | DESCRIPTION  |
|--|--|
| tb_TempLog   | Stores the raw data of product logs  |
| tb_AV*Log  | Stores product log<br>* corresponds to Virus, Event, Status, PEInfo, WebSecurity.<br><br>These tables store the product status log as well as the pattern and engine version, update and deploy time, and the unhandled virus count. |
| tb_InvalidLog  | Stores unidentified log information  |
| <ul style="list-style-type: none"> <li>• tb_TotalWebSecurityCount</li> <li>• tb_TotalVirusCount</li> <li>• tb_TotalSecurityCount</li> <li>• tb_TopTenSource</li> <li>• tb_TopTenDestination</li> <li>• tb_TopTenVirus</li> </ul> | Stores virus summary information for Status Summary and reports  |
| tb_LogPurgePolicy  | Stores purge log settings  |
| tb_LogPurgeCounter   | Stores purge log counter   |
| <ul style="list-style-type: none"> <li>• tb_InstanceForVirusOutbreak</li> <li>• tb_InstanceForSpecialVirus</li> <li>• tb_InstanceForVirusOutbreak</li> </ul>   | Stores log instances used in alert notifications   |

**TABLE 25-7. Notification Tables**

| NOTIFICATION TABLES  | DESCRIPTION                    |
|--|--------------------------------|
| <ul style="list-style-type: none"> <li>• tb_Alert_NTF_JobList</li> <li>• tb_Event_NTF_JobList</li> </ul> | Stores notification queue list |

| <b>NOTIFICATION TABLES</b>  | <b>DESCRIPTION</b>                          |
|---|---|
| tb_EventNotificationFilter  | Stores Event Center configuration           |
| <ul style="list-style-type: none"> <li>• tb_SendEMailNotification</li> <li>• tb_SendSNMPTrapNotification</li> <li>• tb_SendWindowsNTEventLogNotification</li> <li>• tb_LaunchAProgramNotification</li> <li>• tb_SendSysLogNotification</li> </ul> | Stores notification method settings         |
| tb_VirusOutbreakPolicy  | Stores rules used during virus outbreak     |
| tb_SpecialVirusPolicy   | Stores the user specified virus name        |
| <ul style="list-style-type: none"> <li>• tb_VirusOutbreakAccumulate</li> <li>• tb_SpecialVirusAccumulate</li> </ul>   | Stores virus counter information            |
| <ul style="list-style-type: none"> <li>• tb_UGNtfRelation</li> <li>• tb_NtfUserGROUP</li> <li>• tb_GroupAndUserRelation</li> </ul>  | Stores user and group notification settings |

**TABLE 25-8. Report Tables**

| <b>REPORT TABLES</b>  | <b>DESCRIPTION</b>                         |
|---|--|
| <ul style="list-style-type: none"> <li>• tb_ReportScheduleTask</li> <li>• tb_ReportTaskQueue</li> </ul> | Stores and handles report generation tasks |
| tb_ReportItemTracking   | Stores report template file catalog        |

**TABLE 25-9. Pattern and Engine Deployment Tables**

| PATTERN AND ENGINE DEPLOYMENT TABLES   | DESCRIPTION  |
|--|--|
| <ul style="list-style-type: none"> <li>• tb_DeploymentPlans</li> <li>• tb_DeploymentPlansTF</li> </ul> | Stores deployment plan information                                     |
| tb_DeploymentPlanTasks   | Stores deployment task queue   |
| tb_DeployNowJobList  | Stores ongoing deployment plan status                                  |
| tb_DeployCommandTracking   | Stores deployment command tracking information                         |
| tb_DeploymentPlanTargets   | Stores the managed product information that applied the deploy command |

## Backing Up db\_ApexCentral Using SQL Server Management Studio

When using SQL Server, use the SQL Server Management Studio to back up the Apex Central database.



### Note

Trend Micro recommends regular backups of the Apex Central database. Always back up when you are about to modify the Apex Central database (for example, adding or installing a managed product).

### Procedure

1. From the Apex Central server, click **Start > All Programs > Microsoft SQL Server <version> > SQL Server Management Studio**.  
 <version> is the version of SQL Server Management Studio.
2. On the menu bar, click **View > Object Explorer**. In the **Object Explorer** panel, double-click <Host\Instance Name>, then double-click **Databases**.

<Host\Instance Name> is the SQL server host name and the SQL instance name.

3. Right-click **db\_ApexCentral** and then click **Tasks > Back up**.
  4. Under **Backup set**, provide the **name** and **description**.
  5. Under **Source > Backup Type**, select **Full**.
  6. Under **Destination**, click **Add** to specify the backup file destination.
  7. Click **OK** when the message “The backup operation has been completed successfully.” appears.
- 

## Restoring Backup db\_ApexCentral Using SQL Server Management Studio

Use the SQL Server Management Studio to restore the backup Apex Central database.

---

### Procedure

1. Stop Apex Central.
2. Click **Start > Programs > Administrative Tools > Services** to open the **Services** screen.
3. Right-click <**Apex Central service**>, and then click **Stop**.
4. Click **Programs > SQL Server Management Studio** to access the SQL Server Management Studio.
5. On the console, click **SQL server group > {SQL server} > Databases**.  
{SQL server} is the SQL Server host name.
6. Right-click **db\_ApexCentral > All tasks > Restore Database....**
7. On the **Restore database** screen, select the database to restore.
8. Click **OK** to start the restoration process.
9. Click **OK** when the message “Restore of database '{Apex Central database}' completed successfully.” appears.

10. Click **Start > Programs > Administrative Tools > Services** to open the **Services** screen.
  11. Right-click **<Apex Central service>**, and then click **Restart**.
  12. Start Apex Central.
- 

## Shrinking db\_ApexCentral\_Log.ldf Using SQL Commands

---

### Procedure

1. Backup the Apex Central database using the SQL Server Management Studio.
2. From the available databases, select the db\_ApexCentral database.
3. Execute the following SQL Script:

```
DBCC shrinkfile('db_ApexCentral_log', 10)
```

4. Verify the size of db\_ApexCentral\_Log.LDF is less than 10MB.

If db\_ApexCentral\_Log.LDF was not reduced in size, use the following SQL command to identify the Database Recovery Mode used:

```
SELECT name as DatabaseName, DATABASEPROPERTYEX(name, 'Recovery') as RecoveryMode FROM master.dbo.sysdatabases where name='db_ApexCentral'
```

If the Database Recovery Mode is FULL, execute following SQL script:

```
-- Truncate the log by changing the database recovery model to SIMPLE.  
ALTER DATABASE db_ApexCentral  
SET RECOVERY SIMPLE;  
GO  
-- Shrink the truncated log file to 10 MB.  
DBCC SHRINKFILE (db_ApexCentral_Log, 10);
```

```
GO
-- Reset the database recovery model.
ALTER DATABASE db_ApexCentral
SET RECOVERY FULL;
GO
```

For detailed information on shrinking SQL databases and SQL commands, refer to the *Microsoft SQL Server Administration* documents.

---

## Shrinking db\_ApexCentral\_log.ldf Using SQL Server Management Studio

The transaction log file for the Apex Central database is ...\\data\\db\_ApexCentral\_log.LDF. SQL Server generates the transaction log as part of its normal operation.

db\_ApexCentral\_log.LDF contains all managed product transactions using db\_ApexCentral.mdf.

By default, the transaction log file has no file size limit on the SQL Server configuration. This leads to filling up the available disk space.

## Shrinking the db\_ApexCentral\_log.ldf File Size on Microsoft SQL Server 2008 (or later)

---

### Procedure

1. Back up the Apex Central database using the SQL Server Management Studio.
2. Purge the transaction log.
3. On the SQL Server, click **Programs > SQL Server Management Studio** to open the SQL Server Management Studio.
4. Select the SQL server and specify the authentication credentials if prompted.



5. Right-click **db\_ApexCentral** and select **Properties**.  
The **Properties** dialog box appears.
  6. Click **Options**.  
The **Options** work area appears.
  7. Select **Simple** from the **Recovery model:** list.
  8. Click **OK**.
-



# Chapter 26

## Apex Central Tools

This section discusses how to use a number of Apex Central configuration tools.

Topics include:

- *About Apex Central Tools on page 26-2*
- *Using the Agent Migration Tool (AgentMigrateTool.exe) on page 26-2*
- *Using the Database Configuration Tool (DBConfig.exe) on page 26-2*

## About Apex Central Tools

Apex Central provides a number of tools to help you with specific configuration tasks. Apex Central houses most tools at the following location:

```
<Apex Central installation directory>\WebUI\download\tools\
```

## Using the Agent Migration Tool (AgentMigrateTool.exe)

The Agent Migration tool provided in Apex Central migrates agents administered by another Apex Central server.



### Note

The Agent Migration Tool supports Windows-based and Linux-based agent migration.

---

### Procedure

1. Log on to the destination server using the “Administrator” account.



### Important

Only the “Administrator” account has sufficient permission to run the Agent Migration Tool.

---

2. Run AgentMigrateTool.exe from the following location: <Apex Central installation directory>\
- 

## Using the Database Configuration Tool (DBConfig.exe)

The DBConfig.exe tool allows users to change the user account, password, and the database name for the Apex Central database.

The tool offers the following options:

- **DBName:** Database name
- **DBAccount:** Database account
- **DBPassword:** Database password
- **Mode:** Database authentication mode (SQL Server Authentication or Windows Authentication)

**Note**

The default database authentication mode is SQL Server Authentication mode. However, Windows Authentication mode is necessary when configuring for Windows authentication.

---

**Procedure**

1. Open a command prompt on the Apex Central server.
2. Use the following command to locate the directory which contains the DBConfig.exe file:

```
cd <Apex Central installation directory>\DBConfig
```

3. Type `dbconfig` and press `ENTER`.

The DBConfig tool interface appears.

4. Specify which settings you want to modify:
    - **Example 1:** `DBConfig -DBName="db_your_database>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
    - **Example 2:** `DBConfig -DBName="db_your_database>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`
    - **Example 3:** `DBConfig -DBName="db_your_database>" -DBPassword="sqlPwd"`
-



# Chapter 27

## Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 27-2*
- *Contacting Trend Micro on page 27-3*
- *Sending Suspicious Content to Trend Micro on page 27-4*
- *Other Resources on page 27-5*

## Troubleshooting Resources

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

### Using the Support Portal

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

---

#### Procedure

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



#### Tip

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

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

---

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

---

### Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.



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

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

## Contacting Trend Micro

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

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

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

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

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

## **Sending Suspicious Content to Trend Micro**

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

### **Email Reputation Services**

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

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

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

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

### **File Reputation Services**

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

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

Record the case number for tracking purposes.

## Web Reputation Services

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

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

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

## Other Resources

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

## Download Center

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

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

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

## Documentation Feedback

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

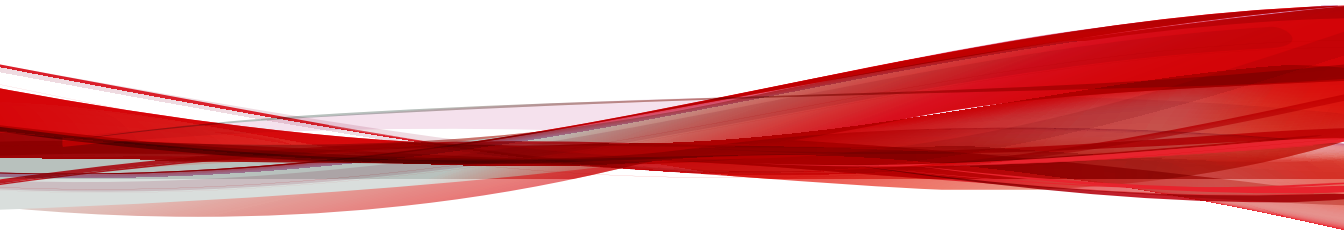
<https://docs.trendmicro.com/en-us/survey.aspx>



# Appendices

## Appendices

---





# Appendix A

## Apex Central System Checklists

Use the checklists in this section to record relevant system information as a reference.

Topics include:

- *Server Address Checklist on page A-2*
- *Port Checklist on page A-3*
- *Apex Central Conventions on page A-3*
- *Core Processes and Configuration Files on page A-4*
- *Communication and Listening Ports on page A-6*

## Server Address Checklist

You must provide the following server address information during the installation process, as well as during the configuration of the Apex Central server to work with your network. Record the information here for easy reference.

**TABLE A-1. Server Address Checklist**

| INFORMATION REQUIRED                        | EXAMPLE            | YOUR VALUE |
|---|--------------------|------------|
| Apex Central server information             |                    |            |
| IP address                                  | 10.1.104.255       |            |
| Fully qualified domain name (FQDN)          | server.company.com |            |
| NetBIOS (host) name                         | yourserver         |            |
| Web server information                      |                    |            |
| IP address                                  | 10.1.104.225       |            |
| Fully qualified domain name (FQDN)          | server.company.com |            |
| NetBIOS (host) name                         | yourserver         |            |
| SQL-based Apex Central database information |                    |            |
| IP address                                  | 10.1.104.225       |            |
| Fully qualified domain name (FQDN)          | server.company.com |            |
| NetBIOS (host) name                         | sqlserver          |            |
| Proxy server for component download         |                    |            |
| IP address                                  | 10.1.174.225       |            |
| Fully qualified domain name (FQDN)          | proxy.company.com  |            |
| NetBIOS (host) name                         | proxyserver        |            |



| INFORMATION REQUIRED  | EXAMPLE          | YOUR VALUE |
|---|------------------|------------|
| SMTP server information (Optional; for email message notifications) |                  |            |
| IP address  | 10.1.123.225     |            |
| Fully qualified domain name (FQDN)                                  | mail.company.com |            |
| NetBIOS (host) name   | mailserver       |            |
| SNMP Trap information (Optional; for SNMP Trap notifications)       |                  |            |
| Community name  | trendmicro       |            |
| IP address  | 10.1.194.225     |            |
| Syslog server information (Optional; for syslog notifications)      |                  |            |
| IP address  | 10.1.194.225     |            |
| Server port   | 514              |            |

## Port Checklist

Apex Central uses the following ports for the indicated purposes.

| PORT   | SAMPLE | YOUR VALUE |
|--|--------|------------|
| SMTP   | 25     |            |
| Proxy  | 8088   |            |
| Web Console and Update/<br>Deploy components | 80     |            |

## Apex Central Conventions

Refer to the following conventions applicable for the Apex Central installation or web console configuration.

- User names

- Max. length: 32 characters
- Allowed: A-Z, a-z, 0-9, -, \_, ., \$
- Folder names
  - Max. length: 32 characters
  - Not allowed: /, >, &, ", %, ^, =

**Note**

For the Apex Central server host name, the setup program supports servers with underscores ("\_") as part of the server name.

## Core Processes and Configuration Files

Apex Central saves system configuration settings and temporary files in XML format.

The following tables describe the configuration files and processes used by Apex Central.

**TABLE A-2. Apex Central Configuration Files**

| CONFIGURATION FILE           | DESCRIPTION  |
|------------------------------|--|
| AuthInfo.ini                 | Configuration file that contains information about private key file names, public key file names, certificate file names, and the encrypted passphrase of the private key as well as the host ID and port. |
| aucfg.ini                    | ActiveUpdate configuration file  |
| TVCS_Cert.pem                | Certificate used by SSL authentication   |
| TVCS_Pri.pem                 | Private Key used by SSL  |
| TVCS_Pub.pem                 | Public Key used by SSL   |
| ProcessManager.xml           | Used by ProcessManager.exe   |
| CmdProcessorEventHandler.xml | Used by CmdProcessor.exe   |

| <b>CONFIGURATION FILE</b> | <b>DESCRIPTION</b>  |
|---------------------------|---|
| DMRegisterinfo.xml        | Used by CasProcessor.exe                                    |
| DataSource.xml            | Stores the connection parameters for Apex Central processes |
| SystemConfiguration.xml   | Apex Central system configuration file                      |
| agent.ini                 | MCP agent file  |

**TABLE A-3. Apex Central Core Processes**

| <b>PROCESSES</b>   | <b>DESCRIPTION</b>   |
|--------------------|--|
| ProcessManager.exe | Launches and stops other Apex Central core processes   |
| CmdProcessor.exe   | Sends XML instructions, formed by other processes, to managed products, processes product registration, sends alerts, performs scheduled tasks, and applies Outbreak Prevention Policies                                 |
| LogReceiver.exe    | Receives managed product logs and messages. Starting with Control Manager 3.0 Service Pack 4, LogReceiver.exe only handles logs coming from Trend Micro Damage Control Services and Trend Micro Vulnerability Assessment |
| LogProcessor.exe   | Receives logs from managed products, and receives entity information from managed products   |
| LogRetriever.exe   | Retrieves and saves logs in the Apex Central database  |
| ReportServer.exe   | Generates Apex Central reports   |
| MsgReceiver.exe    | Receives messages from the Apex Central server and managed products  |
| CasProcessor.exe   | Allows a Apex Central server to manage other Apex Central servers  |
| inetinfo.exe       | Microsoft Internet Information Service process   |
| cm.exe             | Manages dmserver.exe and mrf.exe   |
| dmserver.exe       | Provides the Apex Central web console log on page and manages the Product Directory (Apex Central-side)  |

| PROCESSES               | DESCRIPTION  |
|-------------------------|--|
| sCloudProcessor.NET.exe | Requests the Apex Central web console or other processes to provide a job ID for the issuer to query statuses, query results, and cancel requests; used by the User/Endpoint Directory |

## Communication and Listening Ports

These are the default Apex Central communication and listening ports.

| SERVICE                 | SERVICE PORT |
|-------------------------|--------------|
| ProcessManager.exe      | 20501        |
| CmdProcessor.exe        | 20101        |
| cmdProcessor.NET.exe    | 21003        |
| LogReceiver.exe         | 20201        |
| LogProcessor.exe        | 21001        |
| LogRetriever.exe        | 20301        |
| ReportServer.exe        | 20601        |
| MsgReceiver.exe         | 20001        |
| CasProcessor.exe        | 20801        |
| sCloudProcessor.NET.exe | 21002        |

# Appendix B

## Data Views

This section describes data views that Apex Central supports for customizing report templates and log queries.

Topics include:

- *Data View: Security Logs on page B-2*
- *Data View: Product Information on page B-93*

## Data View: Security Logs

Displays information about security threats that managed products detect: viruses, spyware/grayware, phishing sites, and more.

## Advanced Threat Information

Displays summary and detailed data about advanced persistent threats and targeted attacks that managed products detect on your network.

## Detailed C&C Callback Information

Provides specific information about C&C callback events detected on your network

**TABLE B-1. Detailed C&C Callback Information Data View**

| DATA             | DESCRIPTION  |
|------------------|--|
| Received         | The date and time Apex Central received the data from the managed product  |
| Generated        | The date and time the managed product generated the data   |
| Compromised Host | The IP address, host name, or email address that attempted a callback  |
| Callback Address | The object from/to which a compromised host attempted a callback   |
| C&C List Source  | The C&C list source that identified the C&C server <ul style="list-style-type: none"><li>• C&amp;C IP List</li><li>• Global Intelligence List</li><li>• User-defined IP List</li><li>• Virtual Analyzer List</li></ul> |
| Network Groups   | The monitored network groups as defined by the administrators of managed products, such as Deep Discovery Inspector  |

| DATA                | DESCRIPTION   |
|---------------------|---|
| C&C Risk Level      | The risk level Trend Micro assigns to the event: <ul style="list-style-type: none"> <li>• <b>High:</b> Known malicious or involved in high-severity connections</li> <li>• <b>Medium:</b> IP address/domain/URL is unknown to reputation service</li> <li>• <b>Low:</b> Reputation service indicates previous compromise or spam involvement</li> </ul> |
| C&C Server Location | The region and country where the C&C server is located  |
| First Monitored     | The date and time the callback address was first detected by Trend Micro  |
| Last Activity       | The date and time the callback address was last contacted by a compromised host   |
| Malware Families    | The malware names associated with the callback address  |
| Product             | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Product Entity      | The display name of the managed product server in Apex Central  |

## Detailed Predictive Machine Learning Information

Provides specific information about advanced unknown threats detected by Predictive Machine Learning

**TABLE B-2. Detailed Predictive Machine Learning Information**

| DATA           | DESCRIPTION  |
|----------------|--|
| Detection Time | The date and time the managed product server or the Security Agent detected the threat |
| Received       | The date and time Apex Central received the data from the managed product              |

| <b>DATA</b>                 | <b>DESCRIPTION</b>  |
|-----------------------------|---|
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the endpoint</li> </ul> |
| Product/Endpoint IP         | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the endpoint</li> </ul>                           |
| Product                     | The name of the managed product or service  |
| Server                      | The display name of the managed product server in Apex Central  |
| Probable Threat Type        | The most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats   |
| Security Threat             | The name of the security threat   |
| Logon User                  | The logged on user name at the time of the event  |
| Type                        | The type of object that triggered the detection ("File" or "Process")   |
| File Path                   | The path of the file object or the path of the program that executed the process  |
| File Creation Time          | The date and time the file object was created   |
| Parent Process              | The process that triggered the detected process   |
| Process Command             | The command that executed the detected process  |
| Process Owner               | The user name that triggered the detected process   |
| Endpoint Infection Channel  | The channel that the threat originated from   |
| Infection Source            | The origin of the threat  |
| Threat Probability          | How closely the file/process matched the malware model  |
| Action Result               | The result of the action taken by the managed product   |
| Subject                     | The subject of the email message that triggered the detection   |



| DATA                 | DESCRIPTION  |
|----------------------|--|
| Delivery Time        | The date and time the email message was delivered to the mail server |
| Sender               | The sender of the email message that triggered the detection         |
| Recipients           | The recipient(s) of the email message that triggered the detection   |
| Cloud Service Vendor | The name of the cloud service vendor                                 |

## Detailed Suspicious File Information

Provides specific information about suspicious files detected on your network

**TABLE B-3. Detailed Suspicious File Information Data View**

| DATA                | DESCRIPTION  |
|---------------------|--|
| Received            | The date and time Apex Central received the data from the managed product                        |
| Detected            | The date and time the managed product detected the threat  |
| Endpoint            | The name of the endpoint   |
| Product             | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |
| Product Entity      | The display name of the managed product server in Apex Central                                   |
| Endpoint IP Address | The IP address of the endpoint   |
| Endpoint Host Name  | The host name of the endpoint  |
| File Type           | The type of file object  |
| File SHA-1          | The SHA-1 hash value of the file object  |
| File Path           | The path of the file object or the path of the program that executed the process                 |

| DATA            | DESCRIPTION   |
|-----------------|---|
| C&C List Source | The C&C list source that identified the C&C server <ul style="list-style-type: none"> <li>• C&amp;C IP List</li> <li>• Global Intelligence List</li> <li>• User-defined IP List</li> <li>• Virtual Analyzer List</li> </ul> |
| Action          | The action taken by the managed product   |
| Scan Type       | The type of scan that reported the event (for example, Real-time Scan, Scheduled Scan, Manual Scan)   |
| Created         | The date and time the file object was created   |
| Modified        | The date and time the file object was last modified   |

## Virtual Analyzer Detection Information

Provides specific information about advanced unknown threats detected by Virtual Analyzer

**TABLE B-4. Virtual Analyzer Detection Information**

| DATA          | DESCRIPTION   |
|---------------|---|
| Generated     | The date and time the managed product generated the data                  |
| Received      | The date and time Apex Central received the data from the managed product |
| Product       | The name of the managed product or service                                |
| Server Name   | The name of the server  |
| Host          | The name of the host  |
| Entry Channel | The infection channel   |
| Source        | The origin of the threat  |
| Destination   | The target location of the threat   |

| DATA                 | DESCRIPTION   |
|----------------------|---|
| Process Name         | The name of the process that triggered the detection                  |
| SHA1                 | The SHA-1 hash value of the file object that triggered the detection  |
| Type                 | The type of object that triggered the detection ("File" or "Process") |
| File Name            | The name of the file object that triggered the detection              |
| File Type            | The type of file object that triggered the detection                  |
| URL                  | The URL object that triggered the detection                           |
| Submission Rule      | The rule submitted by Virtual Analyzer                                |
| Submission Time      | The date and time Virtual Analyzer submitted the rule                 |
| Completed Time       | The date and time Virtual Analyzer completed the analysis             |
| Security Threat      | The name of the security threat                                       |
| Risk Level           | The risk level assigned by Virtual Analyzer                           |
| Threat Categories    | The type of security threat   |
| Most Critical Threat | The most critical threats by severity level                           |
| Cloud Service Vendor | The name of the cloud service vendor                                  |

## Detailed Virtual Analyzer Suspicious Object Impact Information

Provides detailed information about the impact of Virtual Analyzer suspicious objects

| DATA        | DESCRIPTION  |
|-------------|--|
| Type        | The type of suspicious object  |
| Object      | The name of the suspicious object  |
| Scan Action | The scan action taken by the managed product that detected the suspicious object (for example, Log, Block) |
| Risk Level  | The risk level of the security threat  |

| <b>DATA</b>                    | <b>DESCRIPTION</b>  |
|--------------------------------|---|
| Expiration                     | The date and time the suspicious object is set to expire  |
| First Submission Time          | The date and time the managed product first submitted the suspicious object to Virtual Analyzer         |
| First Submission Product Name  | The name of the managed product that first submitted the suspicious object to Virtual Analyzer          |
| First Submission Host Name     | The display name of the managed server that first submitted the suspicious object to Virtual Analyzer   |
| First Submission IP Address    | The IP address of the managed server that first submitted the suspicious object to Virtual Analyzer     |
| First Submission File Name     | The file name of the suspicious object that the managed product first submitted to Virtual Analyzer     |
| First Submission File Type     | The file type of the suspicious object that the managed product first submitted to Virtual Analyzer     |
| First Submission Source        | The source of the suspicious object that the managed product first submitted to Virtual Analyzer        |
| First Submission Destination   | The destination of the suspicious object that the managed product first submitted to Virtual Analyzer   |
| Latest Submission Time         | The date and time the managed product last submitted the suspicious object to Virtual Analyzer          |
| Latest Submission Product Name | The name of the managed product that last submitted the suspicious object to Virtual Analyzer           |
| Latest Submission Host Name    | The display name of the managed product that last submitted the suspicious object to Virtual Analyzer   |
| Latest Submission IP Address   | The IP address of the last managed server that last submitted the suspicious object to Virtual Analyzer |
| Latest Submission File Name    | The file name of the suspicious object that the managed product last submitted to Virtual Analyzer      |
| Latest Submission File Type    | The file type of the suspicious object that the managed product last submitted to Virtual Analyzer      |

| <b>DATA</b>                      | <b>DESCRIPTION</b>  |
|----------------------------------|---|
| Latest Submission File SHA-1     | The file SHA-1 of the suspicious object that the managed product last submitted to Virtual Analyzer     |
| Latest Submission Detection Name | The detection name of the suspicious object that the managed product last submitted to Virtual Analyzer |
| Latest Submission Source         | The source of the suspicious object that the managed product last submitted to Virtual Analyzer         |
| Latest Submission Destination    | The destination of the suspicious object that the managed product last submitted to Virtual Analyzer    |
| Endpoint Domain Name             | The domain name of the endpoint that triggered the detection  |
| Endpoint Host Name               | The display name of the endpoint that triggered the detection   |
| Endpoint User Domain Name        | The domain name of the user logged on to the endpoint at the time of the detection                      |
| Endpoint User Domain Account     | The domain account of the user logged on to the endpoint at the time of the detection                   |
| Endpoint User Name               | The logged on user name at the time of the event  |
| Endpoint IP Address              | The IP address of the endpoint  |
| Endpoint First Found Time        | The date and time the suspicious object was first detected on the endpoint                              |
| Endpoint First Product Detection | The name of the managed product that first detected the suspicious object on the endpoint               |
| Endpoint First Action Taken      | The first action taken on the endpoint by the managed product   |
| Endpoint Last Found Time         | The date and time the suspicious object was last detected on the endpoint                               |
| Endpoint Last Product Detection  | The name of the managed product that last detected the suspicious object on the endpoint                |
| Endpoint Last Action Taken       | The last action taken on the endpoint by the managed product  |

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Endpoint Last Action Result | The result of the last action taken on the endpoint by the managed product |

## Attack Discovery Detections

Displays information provided by Attack Discovery.

### Attack Discovery Detection Information

Provides general information about threats detected by Attack Discovery

**TABLE B-5. Attack Discovery Detection Information**

| DATA                   | DESCRIPTION  |
|------------------------|--|
| Generated              | The date and time the managed product generated the data   |
| Received               | The date and time Apex Central received the data from the managed product  |
| Endpoint               | The name of the endpoint   |
| Product                | The name of the managed product or service   |
| Managing Server Entity | The display name of the managed product server in Apex Central to which the endpoint reports   |
| Product Version        | The version of the managed product   |
| Tactics                | The MITRE ATT&CK™ tactic(s) detected<br>For more information, see <a href="https://attack.mitre.org/tactics/enterprise/">https://attack.mitre.org/tactics/enterprise/</a> .          |
| Techniques             | The MITRE ATT&CK™ technique(s) detected<br>For more information, see <a href="https://attack.mitre.org/techniques/enterprise/">https://attack.mitre.org/techniques/enterprise/</a> . |
| Endpoint IP            | The IP address of the endpoint   |
| Risk Level             | The risk level assigned by Attack Discovery  |
| Pattern Version        | The Attack Discovery pattern number for the detection type   |

| DATA                   | DESCRIPTION   |
|------------------------|---|
| Rule ID                | The serial number of the detection rule   |
| Rule Name              | The rules which specify behaviors to be detected by Attack Discovery  |
| Related Objects        | The number of detections<br>Click the count to view additional details.<br>For more information, see <a href="#">Detailed Attack Discovery Detection Information on page B-11</a> . |
| Generated (Local Time) | The time in the agent's local timezone when Attack Discovery detected the threat<br>The time is displayed with the UTC offset.  |
| Instance ID            | The detection ID assigned to the event<br>Entries having the same instance ID belong under the same event.  |

## Detailed Attack Discovery Detection Information

Provides general information about threats detected by Attack Discovery

**TABLE B-6. Detailed Attack Discovery Detection Information**

| DATA           | DESCRIPTION   |
|----------------|---|
| Object Value   | The name of the object targeted by the detected threat                  |
| Object Type    | The type of object targeted by the detected threat                      |
| First Logged   | The time when the threat detection was first logged by Attack Discovery |
| File Directory | The directory of the object targeted by the detected threat             |
| Process ID     | The PID of the process  |
| CLI Command    | The process command that triggered the threat detection                 |
| Signer         | The certificate signer  |
| User Domain    | The domain name of the detected user account                            |

| <b>DATA</b>                         | <b>DESCRIPTION</b>  |
|-------------------------------------|---|
| User Name                           | The account name associated with the object   |
| Impersonated User Name              | The user name that the threat impersonated  |
| Authentication ID                   | The local unique identifier assigned to the logon session                                     |
| Integrity Level                     | The level of protection or access assigned to the logon user                                  |
| File SHA-1                          | The SHA-1 hash value of the object file   |
| File SHA-256                        | The SHA-256 hash value of the object file   |
| File MD5                            | The MD5 hash value of the object file   |
| Census Rating                       | The rating determined by Trend Micro threat experts based on the recorded history of the file |
| File Security Owner                 | The current owner of the file according to the file properties                                |
| File Security Owner Domain          | The domain of the current owner of the file according to the file properties                  |
| File Security Previous Owner        | The previous owner of the file according to the file properties                               |
| File Security Previous Owner Domain | The domain of the previous owner of the file according to the file properties                 |
| Registry Key                        | The registry key that the threat accessed   |
| Registry Value Name                 | The registry value name that the threat accessed  |
| Registry Value Data                 | The registry value data that the threat accessed  |
| AMSI App Name                       | The application name or scripting language associated with the threat                         |
| AMSI App Full Path                  | The full path of the application associated with the threat                                   |
| AMSI App Version                    | The application version associated with the threat  |
| AMSI Script Source                  | The file name and extension of the script source  |
| AMSI Script Content                 | The content of the script   |



| <b>DATA</b>                 | <b>DESCRIPTION</b>   |
|-----------------------------|--|
| AMSI Script Source SHA-1    | The SHA-1 hash value of the script source  |
| AMSI Script Source SHA-256  | The SHA-256 hash value of the script source  |
| Source IP Address           | The source IP address of the detected threat                                       |
| Source IP Address Port      | The source IP address port number of the detected threat                           |
| Destination IP Address      | The IP address that the threat accessed  |
| Destination IP Address Port | The IP port number that the threat accessed  |
| Destination URL             | The URL that the threat accessed   |
| Destination Domain          | The domain name that the threat accessed   |
| WMI Event                   | The WMI event information associated with the threat                               |
| Windows Event Source        | The name of the software that logged the event according to the Windows Event Logs |
| Windows Event Log Content   | The Windows Event log content that triggered the detection                         |
| Auth Priv Name              | The Authorization Privilege Name that the threat modified                          |
| Auth Priv Attribute         | The Authorization Privilege Attribute that the threat modified                     |
| Auth Priv Disable All       | The status of the Authorization Privilege Disable All that the threat modified     |

## Content Violation Information

Displays summary and detailed data about prohibited content that managed products detect on your network.

## Content Violation Action/Result Summary

Provides a summary of actions managed products take against content violations. Example: the action managed products take against the content violation, the number of email messages affected by the action taken

**TABLE B-7. Content Violation Action/Result Summary Data View**

| DATA                             | DESCRIPTION  |
|----------------------------------|--|
| Action                           | Displays the type of action managed products take against email message in violation of content policies.<br><br>Example: forwarded, attachments stripped, deleted |
| Policy Violation Detection Count | Displays the number of violations with the specified action taken by managed products.   |

## Content Violation Detection Over Time Summary

Provides a summary of content violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints affected by the content violation, total number of unique content violations and total number of content violations on the network

**TABLE B-8. Content Violation Detection Over Time Summary Data View**

| DATA            | DESCRIPTION  |
|-----------------|--|
| Date/Time       | Displays the time that the summary of the data occurs.   |
| Unique Policies | Displays the number of unique policies in violation managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same policy on one computer.<br><br>Detections = 10 |

| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Unique Senders/<br>Users | Displays the number of unique email message addresses or users sending content that violates managed product policies.<br><br>Example: A managed product detects 10 violation instances of the same policy coming from 3 computers.<br><br>Unique Senders/Users = 3 |
| Unique Recipients        | Displays the number of unique email message recipients receiving content that violate managed product policies.<br><br>Example: A managed product detects 10 violation instances of the same policy on 2 computers.<br><br>Unique Recipients = 2                    |
| Detections               | Displays the total number of policy violations managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same policy on one computer.<br><br>Detections = 10   |

## Content Violation Policy Summary

Provides a summary of content violation detections due to specific policies. Example: name of the policy in violation, the type of filter that detects the content violation, the total number of content violations on the network

**TABLE B-9. Content Violation Policy Summary Data View**

| DATA        | DESCRIPTION  |
|-------------|--|
| Policy      | Displays the name of the policy that endpoints violate.  |
| Filter Type | Displays the type of filter that triggers the violation. Example: content filter, phishing filter, URL reputation filter |

| DATA                     | DESCRIPTION  |
|--------------------------|--|
| Unique Senders/<br>Users | <p>Displays the number of unique email message addresses or users sending content that violates managed product policies.</p> <p>Example: A managed product detects 10 violation instances of the same policy coming from 3 computers.</p> <p>Unique Senders/Users = 3</p> |
| Unique Recipients        | <p>Displays the number of unique email message recipients receiving content that violate managed product policies.</p> <p>Example: A managed product detects 10 violation instances of the same policy on 2 computers.</p> <p>Unique Recipients = 2</p>                    |
| Detections               | <p>Displays the total number of policy violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same policy on one computer.</p> <p>Detections = 10</p>   |

## Content Violation Sender Summary

Provides a summary of content violation detections due to specific senders. Example: name of the content sender, the number of unique content violations, the total number of content violations on the network

**TABLE B-10. Content Violation Sender Summary Data View**

| DATA        | DESCRIPTION  |
|-------------|--|
| Sender/User | <p>Displays the email message address or users sending content that violates managed product policies.</p>   |
| Detections  | <p>Displays the total number of policy violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same policy on one computer.</p> <p>Detections = 10</p> |

| DATA              | DESCRIPTION   |
|-------------------|---|
| Unique Recipients | <p>Displays the number of unique email message recipients receiving content that violate managed product policies.</p> <p>Example: A managed product detects 10 violation instances of the same policy on 2 computers.</p> <p>Unique Recipients = 2</p> |
| Unique Policies   | <p>Displays the number of unique policies in violation managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same policy on one computer.</p> <p>Detections = 10</p>   |

## Detailed Content Violation Information

Provides specific information about the email messages with content violations, such as the managed product that detected the content violation, the sender(s) and recipients(s) of the email message, the name of the content violation policy, and the total number of violations detected

**TABLE B-11. Detailed Content Violation Information Data View**

| DATA           | DESCRIPTION   |
|----------------|---|
| Received       | The date and time Apex Central received the data from the managed product                                   |
| Generated      | The date and time the managed product generated the data  |
| Product Entity | The display name of the managed product server in Apex Central  |
| Product        | <p>The name of the managed product or service</p> <p>Example: Apex One, ScanMail for Microsoft Exchange</p> |
| Recipient      | The email recipients receiving content that violate managed product policies                                |
| Sender/User    | The email address or user sending content that violates managed product policies                            |

| <b>DATA</b>          | <b>DESCRIPTION</b>  |
|----------------------|---|
| Subject              | The content of the subject line of the email that violates a policy   |
| Policy               | The name of the policy an email violates  |
| Policy Settings      | The settings for the policy that an email violates  |
| File Location        | The location of the file that violates a policy   |
| File                 | The name of the file that violates a policy   |
| URL                  | The URL in violation of the specified policy  |
| Risk Level           | The Trend Micro assessment of risk to your network<br>Example: high security, low security, medium security       |
| Filter Type          | The type of filter that detects the email in violation<br>Example: content filter, size filter, attachment filter |
| Sub-filter Type      | The type of sub-filter that detects the email in violation  |
| Filter Action        | The action the detecting filter takes against email in violation of a policy<br>Example: clean, quarantine, strip |
| Filter Action Result | The result of the action taken by the filter that detected the violation  |
| Action               | The action taken by the managed product<br>Example: deliver, strip, forward                                       |
| Detections           | The total number of detections  |

## Email Messages with Advanced Threats

Provides specific information about email messages with advanced threats, such as anomalous behavior, false or misleading data, suspicious and malicious behavior patterns, and strings that indicate system compromise but require further investigation to confirm

| <b>DATA</b>      | <b>DESCRIPTION</b>   |
|------------------|--|
| Received         | The date and time Apex Central received the data from the managed product                        |
| Product Entity   | The display name of the managed product server in Apex Central                                   |
| Product          | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |
| Recipients       | The recipient(s) of the email message that triggered the detection                               |
| Sender           | The sender of the email message that triggered the detection                                     |
| Subject          | The subject of the email message that triggered the detection                                    |
| Attachment Count | The number of email attachments  |
| Attachment       | The name of the email attachment   |
| Attachment Type  | The type of email attachment   |
| Action           | The action taken by the managed product<br>Example: deliver, strip, quarantine                   |
| Threat Type      | The type of security threat  |
| Threat Name      | The name of the security threat  |
| Risk Level       | The email message risk level after investigation   |
| Source IP        | The message transfer agent (MTA) IP address nearest to the email sender                          |
| Message ID       | The administrator-configured unique message ID   |
| Link Count       | The number of links in the email message   |
| Links            | The list of links in the email message   |

## Data Discovery Information

Displays information about Data Discovery detections.

## Data Discovery Data Loss Prevention Detection Information

Displays specific information about incidents detected by Data Discovery

**TABLE B-12. Data Discovery Data Loss Prevention Detection Information**

| DATA        | DESCRIPTION  |
|-------------|--|
| Received    | The date and time Apex Central received the data from the managed product                                |
| Generated   | The date and time the managed product generated the data   |
| Rule        | The name of the rule that triggered the detection  |
| Endpoint    | The name or IP address of the endpoint   |
| Domain      | The domain to which the managed product belongs  |
| User        | The logged on user name at the time of the event   |
| User Domain | The name of the domain to which the user belongs   |
| File Path   | The full path of the location containing the digital asset or channel (if no source is available)        |
| File        | The name of the file object that the threat accessed   |
| Template    | The exact rule name(s) and template(s) triggered by the incident   |
| Action      | The action taken by the managed product  |
| Details     | Additional information, such as the reason a user has provided for continuing to transfer sensitive data |

## Data Discovery Endpoint Information

**TABLE B-13. Data Discovery Endpoint Information**

| DATA      | DESCRIPTION  |
|-----------|--|
| Generated | Displays the time when the log data was generated in the managed product.                                |
| Endpoint  | Displays the IP address or host name of a computer where Data Loss Prevention detected the transmission. |



| DATA                | DESCRIPTION  |
|---------------------|--|
| Device Class        | Displays the name of the device category as shown in Windows Device Manager. |
| Device Display Name | Displays the display name of the device, as shown in Windows Device Manager. |
| Provider            | Displays the name of the company that provides the device.                   |

## Data Loss Prevention Information

Displays information about DLP incidents, template matches, and incident sources collected from the managed products.

### DLP Incident Information

Provides specific information about incidents detected by Data Loss Prevention

**TABLE B-14. DLP Incident Information**

| DATA                        | DESCRIPTION   |
|-----------------------------|---|
| Received                    | The date and time Apex Central received the data from the managed product |
| Generated                   | The date and time the managed product generated the data                  |
| Incident ID                 | The identifier of the incident  |
| Severity                    | The severity level of the event   |
| Status                      | The detection status of the incident                                      |
| Manager                     | The name of the manager of the department                                 |
| Department                  | The name of the department  |
| Policy                      | The policy that triggered the detection                                   |
| Product Entity/<br>Endpoint | The name of the endpoint  |

| <b>DATA</b>                       | <b>DESCRIPTION</b>   |
|-----------------------------------|--|
| Product                           | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Product/Endpoint IP               | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the endpoint</li> </ul>                  |
| Product/Endpoint MAC              | Depending on the related source: <ul style="list-style-type: none"> <li>• The MAC address of the managed product server</li> <li>• The MAC address of the Security Agent endpoint</li> </ul> |
| Managing Server                   | The display name of the managed product server in Apex Central to which the endpoint reports   |
| Endpoint                          | The IP address or host name of a computer with an agent (for example, Apex One agent) installed  |
| Incident Source (AD Display Name) | The Active Directory display name of the incident source   |
| Incident Source (AD Account)      | The Active Directory account name of the incident source   |
| Incident Source (Sender)          | The source email address   |
| Website                           | The URL of the website that triggered the incident   |
| Recipient                         | The destination email address  |
| Subject                           | The subject of the email message   |
| File Location                     | The location and the name of the file  |
| File                              | The name of the file from which the incident was triggered   |
| File/Data Size                    | The size of the file or data that triggered the incident   |
| Rule                              | The name of the rule triggered by the incident   |
| Template                          | The name of the template in which a template match was triggered   |

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Channel              | The entity through which a digital asset was transmitted |
| Destination          | The destination of the transmission                      |
| Action               | The action taken by the managed product                  |
| Incidents            | The number of incidents                                  |
| Cloud Service Vendor | The name of the cloud service vendor                     |

## DLP Template Match Information

**TABLE B-15. DLP Template Match Information**

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| ID                          | Displays the unique ID for the log.  |
| Received                    | Displays the time when the managed product received the incident information.  |
| Generated                   | Displays the time when the incident was triggered.   |
| Product Entity/<br>Endpoint | This data column displays one of the following: <ul style="list-style-type: none"> <li>The entity display name for a managed product. Apex Central identifies managed products using the managed product's entity display name.</li> <li>The IP address or host name of a computer with an agent (for example, Apex One agent) installed.</li> </ul> |
| Product                     | Displays the name of the managed product. Example: Apex One, ScanMail for Microsoft Exchange   |
| Product/Endpoint IP         | This data column displays one of the following: <ul style="list-style-type: none"> <li>The IP address of the server on which the managed product installs.</li> <li>The IP address of a computer with an agent (for example, Apex One agent) installed.</li> </ul>   |

| DATA                      | DESCRIPTION  |
|---------------------------|--|
| Product/Endpoint<br>MAC   | This data column displays one of the following: <ul style="list-style-type: none"> <li>• The MAC address of the server on which the managed product installs.</li> <li>• The MAC address of a computer with an agent (for example, Apex One agent) installed.</li> </ul> |
| Managing Server           | Displays the entity display name for a managed product to which an endpoint is registered. Apex Central identifies managed products using the managed product's entity display name.   |
| Endpoint                  | Displays the IP address or host name of a computer with an agent (for example, Apex One agent) installed.  |
| Incident Source<br>(User) | Displays the logged on user name.  |
| Recipient                 | Displays the destination email address.  |
| Subject                   | Displays the subject of the email message.   |
| File Location             | Displays the location and the name of the file.  |
| File                      | Displays the name of the file from which the incident was triggered.   |
| Rule                      | Displays the name of the rule triggered by the incident.   |
| Template                  | Displays the name of the template in which a template match was triggered.   |
| Channel                   | Displays the entity through which a digital asset was transmitted.   |

## Deep Discovery Information

Displays summary and detailed data about suspicious activity that managed products detect on your network.

## Detailed Correlation Information

Provides specific information about detailed threat analyses and remediation recommendations

**TABLE B-16. Detailed Correlation Information Data View**

| DATA                | DESCRIPTION   |
|---------------------|---|
| Generated           | The date and time the managed product generated the data                    |
| IP Address          | The IP address of the endpoint  |
| Network Group       | The monitored network group   |
| Protocol            | The broad protocol group from which the managed product detected the threat |
| Threat Type         | The type of security threat<br>Example: virus, spyware/grayware, fraud      |
| Severity            | The severity level of the event   |
| Detection           | The type of detection based on the correlation rules                        |
| Details             | Remarks or comments related to the detection                                |
| MAC Address         | The MAC address of the endpoint   |
| Host Name           | The name of the endpoint  |
| Correlation Rule ID | The rule ID of the correlation rule   |

## Detailed Mitigation Information

Provides specific information about tasks carried out by mitigation servers to resolve threats on your network

**TABLE B-17. Detailed Mitigation Information Data View**

| DATA              | DESCRIPTION   |
|-------------------|---|
| Received          | The date and time Apex Central received the data from the managed product |
| Generated         | The date and time the managed product generated the data                  |
| Mitigation Entity | The display name of the managed product server in Apex Central            |
| Product           | The name of the managed product or service                                |

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Endpoint IP          | The IP address of the endpoint   |
| Endpoint             | The name of the endpoint   |
| Data Source          | The Deep Discovery product or task that generated the threat event information   |
| Data Source Host     | The host name of the Deep Discovery product that generated the threat event information  |
| Threat Event         | The threat-related events logged by the mitigation server<br>For more information, see <a href="http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm">http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm</a> . |
| Mitigation Status    | The threat events by status groups<br>For more information, see <a href="http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm">http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm</a> .                        |
| Mitigation Details   | The mitigation details about the threat events<br>For more information, see <a href="http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/mitigation_status.htm">http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/mitigation_status.htm</a> .            |
| Detections           | The total number of detections   |
| Detailed Information | The details about the threats  |

## Detailed Suspicious Threat Information

Provides specific information about suspicious threats on your network, such as the managed product that detected the suspicious threat, specific information about the source and destination, and the total number of suspicious threats on the network

**TABLE B-18. Detailed Suspicious Threat Information Data View**

| DATA     | DESCRIPTION   |
|----------|---|
| Received | The date and time Apex Central received the data from the managed product |

| <b>DATA</b>                  | <b>DESCRIPTION</b>   |
|------------------------------|--|
| Generated                    | The date and time the managed product generated the data   |
| Product Entity               | The display name of the managed product server in Apex Central   |
| Product                      | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange       |
| Mitigation Host              | The host name of the mitigation server (for example, Network VirusWall Enforcer or Threat Mitigator)   |
| Traffic/Connection           | The direction of the transmission  |
| Protocol Group               | The broad protocol group from which the managed product detected the threat<br>Example: FTP, HTTP, P2P |
| Protocol                     | The protocol from which the managed product detected the suspicious threat<br>Example: ARP, BitTorrent |
| Destination IP Address       | The IP address that the threat accessed  |
| Destination Host             | The display name of the endpoint that the threat accessed  |
| Destination Port             | The IP port number that the threat accessed  |
| Destination MAC Address      | The MAC address that the threat accessed   |
| Destination OS               | The operating system on the endpoint that the threat accessed  |
| Destination User <x>         | The name used to log on to the target host<br><x> is the user name                                     |
| Logon (Destination User <x>) | The logon timestamp<br><x> represents the number of logon times and the specific timestamp             |
| Source IP Address            | The source IP address of the detected threat   |
| Source Host Name             | The name of the endpoint from which the security threat originated                                     |

| <b>DATA</b>             | <b>DESCRIPTION</b>   |
|-------------------------|--|
| Source Port             | The source IP address port number of the detected threat   |
| Source MAC Address      | The source MAC address of the detected threat  |
| Source OS               | The operating system on the endpoint from which the security threat originated                           |
| Source User <x>         | The name used to log on to the target source host<br><x> is the user names                               |
| Logon (Source User <x>) | The logon timestamp on the source<br><x> represents the number of logon times and the specific timestamp |
| Source Domain           | The domain of the endpoint from which the threat originated  |
| Security Threat Type    | The type of security threat<br>Example: virus, spyware/grayware, fraud                                   |
| Policy/Rule             | The policy or rule that triggered the detection  |
| Recipient               | The recipient(s) of the transmission that triggered the detection  |
| Sender                  | The sender of the transmission that triggered the detection  |
| Subject                 | The subject of the email message that triggered the detection  |
| Attachment File Name    | The file name and extension of the attachment  |
| Attachment File Type    | The file type of the attachment  |
| Attachment SHA-1        | The SHA-1 hash value of the attachment   |
| URL                     | The URL considered a suspicious threat   |
| User                    | The user name logged on to the destination when the managed product detected the threat                  |
| IM/IRC User             | The instant messaging or IRC user name logged on when Deep Discovery Inspector detects a violation.      |



| <b>DATA</b>             | <b>DESCRIPTION</b>   |
|-------------------------|--|
| Browser/FTP Client      | The web browser or FTP endpoint where the suspicious threat originates.  |
| File                    | The name of the file object or the program that executed the process   |
| File in Compressed File | The name of the affected file object in the compressed archive   |
| Archive SHA-1           | The SHA-1 hash value of the archived file object   |
| Archive File Type       | The type of archived file object   |
| Shared Folder           | Displays whether the suspicious threat originates from a shared folder   |
| SHA-1                   | The SHA-1 hash value of the file object  |
| Mitigation Action       | The action taken by the mitigation server<br>Example: File cleaned, File dropped, File deleted   |
| Mitigation Result       | The result of the action taken by the mitigation server  |
| Source IP Group         | The IP address group of the source where the suspicious threat originates  |
| Source Network Zone     | The network zone of the source where the suspicious threat originates  |
| Endpoint Group          | The IP address group of the endpoint the suspicious threat affects   |
| Endpoint Network Zone   | The network zone of the endpoint the suspicious threat affects   |
| Detections              | The total number of detections<br><br>Example: A managed product detects 10 violation instances of the same type on one computer.<br><br>Detections = 10 |

| DATA            | DESCRIPTION   |
|-----------------|---|
| C&C List Source | The C&C list source that identified the C&C server <ul style="list-style-type: none"> <li>• C&amp;C IP List</li> <li>• Global Intelligence List</li> <li>• User-defined IP List</li> <li>• Virtual Analyzer List</li> </ul> |
| C&C Risk Level  | The risk level of the C&C callback  |
| Remarks         | Additional information about the event  |
| C&C Server      | The name, URL, or IP address of the C&C server  |
| C&C Server Type | The type of C&C server  |
| Malware Type    | The type of malware   |

## Overall Suspicious Threat Summary

Provides specific information about suspicious threats on your network.

Example: the policy/rule in violation, summary information about the source and destination, the total number of suspicious threats on the network

**TABLE B-19. Overall Suspicious Threat Summary Data View**

| DATA             | DESCRIPTION  |
|------------------|--|
| Policy/Rule      | Displays the name of the policy/rule in violation.   |
| Protocol         | Displays the protocol over which the violation takes place.<br>Example: HTTP, FTP, SMTP  |
| Unique Endpoints | Displays the number of unique computers affected by the suspicious threat.<br><br>Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers.<br><br>Unique Endpoints = 2 |

| DATA                    | DESCRIPTION   |
|-------------------------|---|
| Unique Sources          | <p>Displays the number of unique sources where suspicious threats originate.</p> <p>Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers.</p> <p>Unique Sources = 3</p>  |
| Unique Recipients       | <p>Displays the number of unique email message recipients receiving content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers.</p> <p>Unique Recipients = 2</p>  |
| Unique Senders          | <p>Displays the number of unique email message senders sending content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers.</p> <p>Unique Senders = 3</p> |
| Detections              | <p>Displays the total number of policy/rule violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same type on one computer.</p> <p>Detections equals 10.</p>   |
| Mitigations             | <p>Displays the number of endpoints Network VirusWall Enforcer devices or Trend Micro™ Threat Mitigator™ take action against.</p>   |
| Cleaned Endpoints       | <p>Displays the total number of endpoints Trend Micro Threat Mitigator cleans.</p>  |
| Clean Endpoint Rate (%) | <p>Displays the percentage of endpoints Trend Micro Threat Mitigator cleans compared to the total Detections.</p>   |

## Suspicious Source Summary

Provides a summary of suspicious threat detections from a specific source. Example: name of the source, summary information about the destination and rules/violations, the total number of suspicious threats on the network

**TABLE B-20. Suspicious Source Summary Data View**

| DATA                  | DESCRIPTION  |
|-----------------------|--|
| Source IP             | Displays the IP addresses of sources where suspicious threats originate.   |
| Unique Policies/Rules | Displays the number of unique policies/rules the source computer violates.<br><br>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.<br><br>Unique Policies/Rules = 1 |
| Unique Endpoints      | Displays the number of unique computers affected by the suspicious threat.<br><br>Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers.<br><br>Unique Endpoints = 2       |
| Detections            | Displays the total number of policy/rule violations managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same type on one computer.<br><br>Detections = 10                 |

## Suspicious Riskiest Endpoints Summary

Provides a summary of the endpoints with the most suspicious threat detections. Example: name of the destination, summary information about the source and rules/violations, the total number of suspicious threats on the network

**TABLE B-21. Suspicious Threat Riskiest Endpoints Summary Data View**

| DATA                  | DESCRIPTION   |
|-----------------------|---|
| Endpoint IP           | Displays the IP addresses of computers affected by suspicious threats.  |
| Unique Policies/Rules | Displays the number of unique policies/rules the source computer violates.<br><br>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.<br><br>Unique Policies/Rules = 1      |
| Unique Sources        | Displays the number of unique sources where suspicious threats originate.<br><br>Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers.<br><br>Unique Sources = 3 |
| Detections            | Displays the total number of policy/rule violations managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same type on one computer.<br><br>Detections = 10                      |

## Suspicious Riskiest Recipient Summary

Provides a summary of the recipients with the most suspicious threat detections. Example: name of the recipient, summary information about the senders and rules/violations, the total number of suspicious threats on the network

**TABLE B-22. Suspicious Riskiest Recipient Summary Data View**

| DATA      | DESCRIPTION  |
|-----------|--|
| Recipient | Displays the email address of the recipient affected by the suspicious threat. |

| DATA                  | DESCRIPTION   |
|-----------------------|---|
| Unique Policies/Rules | <p>Displays the number of unique policies/rules the source computer violates.</p> <p>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.</p> <p>Unique Policies/Rules = 1</p>   |
| Unique Senders        | <p>Displays the number of unique email message senders sending content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers.</p> <p>Unique Senders = 3</p> |
| Detections            | <p>Displays the total number of policy/rule violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same type on one computer.</p> <p>Detections = 10</p>   |

## Suspicious Sender Summary

Provides a summary of suspicious threat detections from a specific sender. Example: name of the sender, summary information about the recipient and rules/violations, the total number of suspicious threats on the network

**TABLE B-23. Suspicious Sender Summary Data View**

| DATA                  | DESCRIPTION   |
|-----------------------|---|
| Sender                | Displays the email address for the source of policy/rule violations.  |
| Unique Policies/Rules | <p>Displays the number of unique policies/rules the source computer violates.</p> <p>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.</p> <p>Unique Policies/Rules = 1</p> |

| DATA              | DESCRIPTION   |
|-------------------|---|
| Unique Recipients | <p>Displays the number of unique email message recipients receiving content that violate managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers.</p> <p>Unique Recipients = 2</p> |
| Detections        | <p>Displays the total number of policy/rule violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same type on one computer.</p> <p>Detections = 10</p>   |

## Suspicious Threat Protocol Detection Summary

Provides a summary of suspicious threat detections over a specific protocol. Example: name of the protocol, summary information about the source and destination, the total number of suspicious threats on the network

**TABLE B-24. Suspicious Threat Protocol Detection Summary Data View**

| DATA                  | DESCRIPTION   |
|-----------------------|---|
| Protocol              | <p>Displays the name of the protocol over which the suspicious threat occurs. Example: HTTP, FTP, SMTP</p>  |
| Unique Policies/Rules | <p>Displays the number of unique policies/rules the source computer violates.</p> <p>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.</p> <p>Unique Policies/Rules = 1</p> |
| Unique Endpoints      | <p>Displays the number of unique computers affected by the suspicious threat.</p> <p>Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers.</p> <p>Unique Endpoints = 2</p>       |

| DATA              | DESCRIPTION   |
|-------------------|---|
| Unique Sources    | <p>Displays the number of unique sources where suspicious threats originate.</p> <p>Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers.</p> <p>Unique Sources = 3</p>  |
| Unique Recipients | <p>Displays the number of unique email message recipients receiving content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers.</p> <p>Unique Recipients = 2</p>  |
| Unique Senders    | <p>Displays the number of unique email message senders sending content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers.</p> <p>Unique Senders = 3</p> |
| Detections        | <p>Displays the total number of policy/rule violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same type on one computer.</p> <p>Detections = 10</p>   |

## Suspicious Threat Detection Over Time Summary

Provides a summary of suspicious threat detections over a period of time (daily, weekly, monthly). Example: time and date when summary data was collected, summary information about the source and destination, the total number of suspicious threats on the network

**TABLE B-25. Suspicious Threat Detection Over Time Summary Data View**

| DATA      | DESCRIPTION  |
|-----------|--|
| Date/Time | Displays the time that the summary of the data occurs. |



| DATA                  | DESCRIPTION   |
|-----------------------|---|
| Unique Policies/Rules | <p>Displays the number of unique policies/rules the source computer violates.</p> <p>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.</p> <p>Unique Policies/Rules = 1</p>   |
| Unique Endpoints      | <p>Displays the number of unique computers affected by the suspicious threat.</p> <p>Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers.</p> <p>Unique Endpoints = 2</p>   |
| Unique Sources        | <p>Displays the number of unique sources where suspicious threats originate.</p> <p>Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers.</p> <p>Unique Sources = 3</p>  |
| Unique Recipients     | <p>Displays the number of unique email message recipients receiving content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers.</p> <p>Unique Recipients = 2</p>  |
| Unique Senders        | <p>Displays the number of unique email message senders sending content that violates managed product suspicious threat policies.</p> <p>Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers.</p> <p>Unique Senders = 3</p> |
| Detections            | <p>Displays the total number of policy/rule violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same type on one computer.</p> <p>Detections = 10</p>   |

## Gray Detection Information

Provides detailed information about possible indicators of attack detected on your network

**TABLE B-26. Gray Detection Information Data View**

| DATA                   | DESCRIPTION  |
|------------------------|--|
| Received               | The date and time Apex Central received the data from the managed product  |
| Generated              | The date and time the managed product generated the data   |
| Endpoint               | The name of the endpoint   |
| Product                | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Managing Server Entity | The display name of the managed product server in Apex Central to which the endpoint reports   |
| Detection Type         | The type of gray detection   |
| Rule                   | The policy or rule that triggered the detection  |
| Details                | The JSON object containing additional information about the detection  |
| Tactics                | The MITRE ATT&CK™ tactic(s) detected<br>For more information, see <a href="https://attack.mitre.org/tactics/enterprise/">https://attack.mitre.org/tactics/enterprise/</a> .          |
| Techniques             | The MITRE ATT&CK™ technique(s) detected<br>For more information, see <a href="https://attack.mitre.org/techniques/enterprise/">https://attack.mitre.org/techniques/enterprise/</a> . |

## Overall Threat Information

Displays summary and statistical data about the overall threat landscape of your network.

## Network Protection Boundary Information

Displays information for a broad overview of security threats affecting your entire network. Examples: managed product network protection type (gateway, email), type of security threat, number of endpoints affected

**TABLE B-27. Network Protection Boundary Information Data View**

| DATA                     | DESCRIPTION  |
|--------------------------|--|
| Product Category         | Displays the category to which the managed product belongs.<br>Example: desktop products, mail server products, network products   |
| Product                  | Displays the name of the managed product.<br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Security Threat Category | Displays the broad category of the security threat managed products detect.<br>Example: Antivirus, Antispyware, Antiphishing   |
| Unique Endpoints         | Displays the number of unique computers affected by the security threat/violation.<br>Example: Apex One detects 10 virus instances of the same virus on 2 computers.<br>Unique Endpoints = 2                         |
| Unique Sources           | Displays the number of unique computers where security threats/violations originate.<br>Example: Apex One detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers.<br>Unique Sources = 3 |
| Detections               | Displays the total number of security threats/violations managed products detect.<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10                              |

## Network Security Threat Analysis Information

Displays information for overall security threats affecting your desktops.  
Examples: name of the security threat, total number of security threat detections, number of endpoints affected

**TABLE B-28. Network Security Threat Analysis Information Data View**

| DATA                     | DESCRIPTION  |
|--------------------------|--|
| Security Threat Category | Displays the broad category of the security threat managed products detect.<br><br>Example: Antivirus, Antispyware, Antiphishing   |
| Security Threat          | Displays the name of security threat managed products detect.  |
| Entry Type               | Displays the entry point for the security threat that managed products detect.<br><br>Example: virus found in file, HTTP, Windows Live Messenger (MSN)   |
| Unique Endpoints         | Displays the number of unique computers affected by the security threat/violation.<br><br>Example: Apex One detects 10 virus instances of the same virus on 2 computers.<br><br>Unique Endpoints = 2                         |
| Unique Sources           | Displays the number of unique computers where security threats/violations originate.<br><br>Example: Apex One detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers.<br><br>Unique Sources = 3 |
| Detections               | Displays the total number of security threats/violations managed products detect.<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br><br>Detections = 10                              |

## Security Threat Endpoint Analysis Information

Displays information with affected endpoints as the focus. Examples: name of the endpoint, the broad range of how the security threat enters your network, number of endpoints affected

**TABLE B-29. Security Threat Endpoint Analysis Information Data View**

| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Endpoint                 | Displays the name of the computer affected by the security threat/violation.  |
| Security Threat Category | Displays the broad category of the security threat managed products detect.<br>Example: Antivirus, Antispyware, Antiphishing  |
| Security Threat Name     | Displays the name of security threat managed products detect.   |
| Detections               | Displays the total number of security threats/violations managed products detect.<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10 |
| Detected                 | Displays the time and date of the last security threat/violation detection on the computer affected the security threat/violation.  |

## Security Threat Entry Analysis Information

Displays information with the entry point of security threats as the focus. Examples: managed product network protection type (gateway, email, desktop), name of the security threat, time of the last security threat detection

**TABLE B-30. Security Threat Entry Analysis Information Data View**

| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Entry Type               | <p>Displays the point of entry for security threats managed products detect.</p> <p>Example: Virus found in file, FTP, File transfer</p>  |
| Product                  | <p>Displays the name of the managed product which detects the security threat.</p> <p>Example: Apex One, ScanMail for Microsoft Exchange</p>  |
| Security Threat Category | <p>Displays the specific category for security threats managed products detect.</p> <p>Example: Antivirus, Antispyware, Content filtering</p>   |
| Unique Endpoints         | <p>Displays the number of unique computers affected by the security threat/violation.</p> <p>Example: Apex One detects 10 virus instances of the same virus on 2 computers.</p> <p>Unique Endpoints = 2</p>                         |
| Unique Sources           | <p>Displays the number of unique computers where security threats/violations originate.</p> <p>Example: Apex One detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers.</p> <p>Unique Sources = 3</p> |
| Detections               | <p>Displays the total number of security threats/violations managed products detect.</p> <p>Example: Apex One detects 10 virus instances of the same virus on one computer.</p> <p>Detections = 10</p>                              |

## Security Threat Source Analysis Information

Displays information with the security threat source as the focus. Examples: name of the security threat source, the broad range of how the security threat enters your network, number of endpoints affected

**TABLE B-31. Security Threat Source Analysis Information Data View**

| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Source Host              | Displays the name of the computer where the cause of the security threat/violation originates.  |
| Security Threat Category | Displays the broad category of the security threat managed products detect.<br>Example: Antivirus, Antispyware, Antiphishing  |
| Security Threat          | Displays the name of security threat managed products detect.   |
| Detections               | Displays the total number of security threats/violations managed products detect.<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10 |
| Detected                 | Displays the time and date of the last security threat/violation detection on the computer affected the security threat/violation.  |

## Policy/Rule Violation Information

Displays summary and detailed data about policy/rule violations that managed products detect on your network.

## Device Access Control Information

Provides specific information about events on your network that are related to Device Access Control.

**TABLE B-32. Device Access Control Information Data View**

| DATA      | DESCRIPTION  |
|-----------|--|
| Received  | Displays the time that Apex Central receives data from the managed product |
| Generated | Displays the time that the managed product generates data                  |

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Product Entity/<br>Endpoint | This data column displays one of the following: <ul style="list-style-type: none"> <li>The entity display name for a managed product. Apex Central identifies managed products using the managed product's entity display name</li> <li>The IP address or host name of a computer with an agent (for example, Apex One agent) installed</li> </ul> |
| Product                     | Displays the name of the managed product<br>Example: Apex One  |
| Target Process              | Displays the process the violation has targeted  |
| File Name                   | Displays the name of the file  |
| Device Type                 | Displays the type of device accessed   |
| Permission                  | Displays the permission type   |
| User                        | Displays the name of the user that was logged on to the endpoint when the managed product detected the event   |

## Detailed Application Activity

Displays specific information about application activities that violate network security policies

**TABLE B-33. Detailed Application Activity Data View**

| DATA           | DESCRIPTION  |
|----------------|--|
| Received       | The date and time Apex Central received the data from the managed product                        |
| Generated      | The date and time the managed product generated the data   |
| Product Entity | The display name of the managed product server in Apex Central                                   |
| Product        | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |



| <b>DATA</b>         | <b>DESCRIPTION</b>   |
|---------------------|--|
| VLAN ID             | The VLAN ID (VID) of the source from which the suspicious threat originates                                    |
| Detected By         | The filter, scan engine, or managed product which detects the suspicious threat                                |
| Traffic/Connection  | The direction of network traffic or the position on the network the suspicious threat originates               |
| Protocol Group      | The broad protocol group from which a managed product detects the suspicious threat<br>Example: FTP, HTTP, P2P |
| Protocol            | The protocol from which a managed product detects the suspicious threat<br>Example: ARP, Bearshare, BitTorrent |
| Description         | Detailed description of the incident by Trend Micro  |
| Endpoint Host       | The host name of the computer in compliance of the policy/rule   |
| Source IP           | The IP address of the source from which the suspicious threat originates                                       |
| Source MAC          | The MAC address of the source from which the suspicious threat originates                                      |
| Source Port         | The port number of the source from which the suspicious threat originates                                      |
| Source IP Group     | The IP address group of the source where the violation originates  |
| Source Network Zone | The network zone of the source where the violation originates  |
| Endpoint IP         | The IP address of the endpoint the suspicious threat affects   |
| Endpoint Port       | The port number of the endpoint the suspicious threat affects  |
| Endpoint MAC        | The MAC address of the endpoint the suspicious threat affects  |
| Endpoint Group      | The IP address group of the endpoint the suspicious threat affects   |

| DATA                                  | DESCRIPTION  |
|---------------------------------------|--|
| Endpoint Network Zone                 | The network zone of the endpoint the suspicious threat affects   |
| Detections                            | The total number of detections<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10   |
| Threat Type                           | The specific type of security threat managed products detect   |
| Detection Severity                    | The severity level of the incident   |
| IP Address (Interested)               | The IP address of the target endpoint (source or destination)<br>For an exchange occurring within the network, the Interested IP is the source IP address. If the traffic is an external traffic, the Interested IP is the destination IP address. |
| IP Address (Peer)                     | The IP address opposite of the Interested IP<br>For example, if the Interested IP is the source IP address, then the Peer IP is the destination IP address.  |
| Matching Classified Events            | The log count matching the same aggregated rule  |
| Aggregated Matching Classified Events | The aggregated log count matching the same rule  |
| Network Group                         | The name of the group  |
| Host Severity                         | The host severity  |
| Log ID                                | The log ID   |

## Detailed Application Control Violation Information

Provides specific information about application control violations on your network, such as the violated Security Agent policy and criteria

**TABLE B-34. Detailed Application Control Violation Information Data View**

| <b>DATA</b>         | <b>DESCRIPTION</b>   |
|---------------------|--|
| Generated           | The date and time the managed product generated the data                                     |
| Received            | The date and time Apex Central received the data from the managed product                    |
| User Name           | The logged on user name at the time of the event   |
| Endpoint            | The name of the endpoint   |
| Action              | The action taken by the managed product  |
| File                | The name of the file object or the program that executed the process                         |
| Process             | The process executed by the file object  |
| Policy              | The name of the policy applied by the Apex Central or managed product console                |
| Criteria            | The name of the rule for application usage   |
| Match Method        | The method used to identify applications in the allow and block criteria                     |
| Version             | The Certified Safe Software Pattern version  |
| Hash Type           | The type of hash algorithm used  |
| Hash Value          | The hash value of the file object  |
| Certificate Signer  | The issuer of the certificate  |
| Server              | The display name of the managed product server in Apex Central to which the endpoint reports |
| Connection Status   | The status of the connection between the endpoint and the managed product server             |
| Endpoint IP Address | The IP address of the endpoint   |
| Command             | The command issued   |
| Process Owner       | The user name of the account that issued the command   |

| DATA               | DESCRIPTION  |
|--------------------|--|
| Application        | The name of the application to which the file object belongs |
| Matched File Path  | The directory location of the file object                    |
| Detections         | The total number of detections                               |
| File Last Modified | The date and time the file object was last modified          |

## Detailed Behavior Monitoring Information

Provides specific information about events on your network that are related to Behavior Monitoring.

**TABLE B-35. Detailed Behavior Monitoring Information Data View**

| DATA                      | DESCRIPTION  |
|---------------------------|--|
| Time Received From Entity | Displays the time that Apex Central received the data from the managed product |
| Time Generated at Entity  | Displays the time that the managed product generates data                      |
| Host                      | Displays the IP address or host name of the computer accessed                  |
| Risk Level                | Displays the Trend Micro assessment of risk to your network                    |
| Log Type                  | Displays the type of log that triggers the violation                           |
| Policy                    | Displays the name of the policy triggered by the violation                     |
| Subject                   | Displays the specific file, including its directory                            |
| Event Type                | Displays the type of violation   |
| Target                    | Displays the path or directory specified by the Event Type                     |
| Action                    | Displays the action taken by the managed product                               |
| Operation                 | Displays read/write or execute operation                                       |
| Endpoint                  | Displays the host name of the computer under attack                            |

| DATA                       | DESCRIPTION  |
|----------------------------|--|
| Endpoint IP                | Displays the IP address of the computer under attack |
| Endpoint Infection Channel | Displays the channel the threat originated from      |
| Cloud Service Vendor       | Displays the name of the cloud service vendor        |

## Detailed Endpoint Security Compliance Information

Provides specific information about endpoint security compliance on your network

**TABLE B-36. Detailed Endpoint Security Compliance Information Data View**

| DATA           | DESCRIPTION  |
|----------------|--|
| Received       | The date and time Apex Central received the data from the managed product                        |
| Generated      | The date and time the managed product generated the data   |
| Product Entity | The display name of the managed product server in Apex Central                                   |
| Product        | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |
| Endpoint       | The host name of the computer in compliance of the policy/rule                                   |
| Endpoint IP    | The IP address of the computer in compliance of the policy/rule                                  |
| Endpoint MAC   | The MAC address of the computer in compliance of the policy/rule                                 |
| Policy/Rule    | The name of the policy/rule in compliance  |
| Service        | The name of the service/program in compliance of the policy/rule                                 |
| User           | The logged on user name at the time of the event   |
| Description    | The detailed description of the incident provided by Trend Micro                                 |

| DATA       | DESCRIPTION  |
|------------|--|
| Detections | The total number of detections<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br><br>Detections = 10 |

## Detailed Endpoint Security Violation Information

Provides specific information about endpoint security violations on your network

**TABLE B-37. Detailed Endpoint Security Violation Information Data View**

| DATA               | DESCRIPTION  |
|--------------------|--|
| Received           | The date and time Apex Central received the data from the managed product                            |
| Generated          | The date and time the managed product generated the data   |
| Product Entity     | The display name of the managed product server in Apex Central                                       |
| Product            | The name of the managed product or service<br><br>Example: Apex One, ScanMail for Microsoft Exchange |
| Endpoint           | The name of the endpoint   |
| Endpoint IP        | The IP address of the endpoint   |
| Endpoint MAC       | The MAC address of the endpoint  |
| Policy/Rule        | The name of the policy/rule that triggered the detection   |
| Service            | The name of the service/program that triggered the detection   |
| User               | The logged on user name at the time of the event   |
| Enforcement Action | The action enforced by the policy/rule   |
| Remediation Action | The action that helps stop payload caused by the violation   |
| Description        | The detailed description of the incident by Trend Micro  |

| DATA       | DESCRIPTION   |
|------------|---|
| Detections | The total number of detections<br><br>Example: Apex One detects 10 security violations of the same type on one computer.<br><br>Detections = 10 |

## Detailed Firewall Violation Information

Provides specific information about firewall violations on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations

**TABLE B-38. Detailed Firewall Violation Information Data View**

| DATA                        | DESCRIPTION   |
|-----------------------------|---|
| Received                    | The date and time Apex Central received the data from the managed product   |
| Generated                   | The date and time the managed product generated the data  |
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the endpoint</li> </ul> |
| Product                     | The name of the managed product or service<br><br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Event Type                  | The type of event that triggered the detection<br><br>Example: intrusion, policy violation  |
| Risk Level                  | The Trend Micro assessment of risk to your network<br><br>Example: High security, low security, medium security   |
| Traffic/Connection          | The direction of the transmission   |
| Protocol                    | The protocol the intrusion uses<br><br>Example: HTTP, SMTP, FTP   |

| DATA             | DESCRIPTION   |
|------------------|---|
| Source Port      | The source IP address port number of the detected threat  |
| Source IP        | The source IP address of the detected threat  |
| Destination Port | The port number accessed by the detected threat   |
| Destination IP   | The IP address of the endpoint accessed by the detected threat  |
| Target Process   | The process the violation targeted  |
| Description      | The detailed description of the incident by Trend Micro   |
| Action           | The action taken by the managed product<br>Example: file cleaned, file quarantined, file passed   |
| Detections       | The total number of detections<br>Example: A managed product detects 10 violation instances of the same type on one computer<br>Detections = 10 |

## Detailed Intrusion Prevention Information

Provides specific information to help you achieve timely protection against known and zero-day attacks, defend against web application vulnerabilities, and identify malicious software accessing the network

| DATA                        | DESCRIPTION   |
|-----------------------------|---|
| Generated                   | The date and time the managed product generated the data                  |
| Received                    | The date and time Apex Central received the data from the managed product |
| Server                      | The display name of the managed product server                            |
| Product Entity/<br>Endpoint | The name or IP address of the endpoint                                    |
| Affected IP Address         | The IP address of the endpoint affected by the threat                     |



| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Reason/Rule              | The Intrusion Prevention Rule triggered by the event  |
| Mode                     | The network engine detection mode used by the Intrusion Prevention module   |
| Action                   | The action taken by the managed product   |
| Application Type         | The <b>Application Type</b> associated with the Intrusion Prevention Rule triggered by the event  |
| Attack Source            | The source of the detected threat   |
| Source IP Address        | The source IP address of the detected threat  |
| Source MAC Address       | The source MAC address of the detected threat   |
| Source Port              | The source port of the detected threat  |
| Destination IP Address   | The IP address that the threat accessed   |
| Destination MAC Address  | The MAC address that the threat accessed  |
| Destination Port         | The port number that the threat accessed  |
| MAC Address (Interested) | Depending on the direction of network traffic: <ul style="list-style-type: none"> <li>• The <b>Source MAC Address</b> of inbound network traffic</li> <li>• The <b>Destination MAC Address</b> of outbound network traffic</li> </ul> |
| Protocol                 | The protocol that the threat used to enter the network  |
| Direction                | The direction of the transmission   |
| Priority                 | The importance of the detection according to the ranking system used by the standalone version of Vulnerability Protection  |
| Severity                 | The severity level of the event   |

## Integrity Monitoring Information

Use to monitor specific changes to an endpoint, such as installed software, running services, processes, files, directories, listening ports, registry keys, and registry values

| DATA      | DESCRIPTION   |
|-----------|---|
| Received  | The date and time Apex Central received the data from the managed product |
| Generated | The date and time the managed product generated the data                  |
| Server    | The host name of the managed product server                               |
| Change    | The change detected by the integrity rule                                 |
| User      | The logged on user name at the time of the event                          |
| Process   | The process from which the event originated                               |
| Type      | The type of registry key  |
| Key       | The registry key  |
| Rank      | The integrity rank  |
| Severity  | The severity level of the event   |

## Network Content Inspection Information

Provides specific information about network content violations on your network

**TABLE B-39. Network Content Inspection Information Data View**

| DATA      | DESCRIPTION   |
|-----------|---|
| Received  | The date and time Apex Central received the data from the managed product |
| Generated | The date and time the managed product generated the data                  |

| DATA                   | DESCRIPTION   |
|------------------------|---|
| Product/Endpoint IP    | Depending on the related source: <ul style="list-style-type: none"> <li>The display name of the managed product server in Apex Central</li> <li>The name or IP address of the endpoint</li> </ul> |
| Product                | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Traffic Direction      | The direction of the transmission   |
| Local IP Address       | The IP address of the Security Agent endpoint   |
| Local IP Address Port  | The IP address port number of the Security Agent endpoint   |
| Remote IP Address      | The IP address of the external endpoint   |
| Remote IP Address Port | The IP address port number of the external endpoint   |
| Remote Domain          | The domain name associated with the detection   |
| Process                | The process through which the contact was attempted (path \application_name)  |
| Action                 | The action taken by the managed product   |
| Pattern Type           | The type of pattern associated with the detection   |
| Threat Name            | The name of the security threat   |

## Spam Violation Information

Displays summary and detailed data about spam that managed products detect on your network.

## Detailed Spam Information

Provides specific information about the spam violations on your network, such as the managed product that detected the content violation, the name of the specific policy in violation, and the total number of spam violations on the network

**TABLE B-40. Detailed Spam Information Data View**

| DATA           | DESCRIPTION  |
|----------------|--|
| Received       | The date and time Apex Central received the data from the managed product  |
| Generated      | The date and time the managed product generated the data   |
| Product Entity | The display name of the managed product server in Apex Central   |
| Product        | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Recipient      | The recipient(s) of the email message that triggered the detection   |
| Sender         | The sender of the email message that triggered the detection   |
| Subject        | The subject of the email message that triggered the detection  |
| Policy         | The policy that triggered the detection  |
| Action         | The action taken by the managed product  |
| Detections     | The total number of detections<br><br>Example: The managed product detects 10 violation instances of the same spam on one endpoint.<br><br>Detections = 10 |

## Overall Spam Violation Summary

Provides a summary of spam violations on the network

| DATA              | DESCRIPTION   |
|-------------------|---|
| Recipient Domain  | Domain of recipients affected by spam   |
| Unique Recipients | Displays the number of unique recipients receiving spam from the specified domain.<br><br>Example: A managed product detects 10 violation instances of spam from the same domain on 3 computers.<br><br>Unique Recipients = 3 |

| DATA       | DESCRIPTION  |
|------------|--|
| Detections | <p>Displays the total number of spam violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same spam on one computer.</p> <p>Detections = 10</p> |

## Spam Connection Information

Provides specific information about the source of spam on your network, such as the managed product that detected the spam, the specific action taken by the managed product, and the total number of spam detected

**TABLE B-41. Spam Connection Information Data View**

| DATA           | DESCRIPTION  |
|----------------|--|
| Received       | The date and time Apex Central received the data from the managed product  |
| Generated      | The date and time the managed product generated the data   |
| Product Entity | The display name of the managed product server in Apex Central   |
| Product        | <p>The name of the managed product or service</p> <p>Example: Apex One, ScanMail for Microsoft Exchange</p>  |
| Source IP      | The source IP address of the detected threat   |
| Filter Type    | The type of filter that detected the event   |
| Action         | <p>The action taken by the managed product</p> <p>Example: drop connection, bypass connection</p>  |
| Detections     | <p>The total number of detections</p> <p>Example: Apex One detects 10 violation instances of the same spam on one computer.</p> <p>Detections = 10</p> |

## Spam Detection Over Time Summary

Provides a summary of spam detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints affected by spam, the total number of spam violations on the network

**TABLE B-42. Spam Detection Over Time Summary Data View**

| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Summary Time             | Displays the time that the summary of the data occurs.  |
| Unique Recipient Domains | Displays the total number of unique recipient domains affected by spam.<br><br>Example: A managed product detects 10 violation instances of the same spam from 2 domains on 1 recipient domain.<br><br>Unique Recipient Domains = 1 |
| Unique Recipients        | Displays the number of unique recipients receiving spam from the specified domain.<br><br>Example: A managed product detects 10 violation instances of spam from the same domain on 3 computers.<br><br>Unique Recipients = 3       |
| Detections               | Displays the total number of spam violations managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same spam on one computer.<br><br>Detections = 10                                     |

## Spam Recipient Summary

Provides a summary of spam violations on specific endpoints. Example: name of endpoint, total number of instances of viruses/malware on the endpoint

**TABLE B-43. Spam Recipient Summary Data View**

| DATA       | DESCRIPTION   |
|------------|---|
| Recipient  | Displays the name of the recipient who receives spam.   |
| Detections | Displays the total number of spam violations managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same spam on one computer.<br><br>Detections = 10 |

## Spyware/Grayware Information

Displays summary and detailed data about spyware/grayware that managed products detect on your network.

### Detailed Spyware/Grayware Information

Provides specific information about the spyware/grayware detections on your network, such as the managed product that detected the spyware/grayware, the name of the spyware/grayware, and the name of the infected endpoint

**TABLE B-44. Detailed Spyware/Grayware Information Data View**

| DATA                        | DESCRIPTION   |
|-----------------------------|---|
| Received                    | The date and time Apex Central received the data from the managed product   |
| Generated                   | The date and time the managed product generated the data  |
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the endpoint</li> </ul> |
| Product                     | The name of the managed product or service<br><br>Example: Apex One, ScanMail for Microsoft Exchange  |

| DATA                       | DESCRIPTION  |
|----------------------------|--|
| Product/Endpoint IP        | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the endpoint</li> </ul>                  |
| Product/Endpoint MAC       | Depending on the related source: <ul style="list-style-type: none"> <li>• The MAC address of the managed product server</li> <li>• The MAC address of the Security Agent endpoint</li> </ul> |
| Managing Server Entity     | The display name of the managed product server in Apex Central to which the endpoint reports   |
| Spyware/Grayware           | The name of the security threat  |
| Endpoint                   | The name or IP address of the endpoint   |
| Source Host                | The IP address or name of the endpoint from which the security threat originated   |
| User                       | The logged on user name at the time of the event   |
| Result                     | The result of the action taken by the managed product<br>Example: successful, further action required  |
| Action                     | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted   |
| Detections                 | The total number of detections<br><br>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.<br><br>Detections = 10                           |
| Entry Type                 | The entry point of the security threat   |
| Detailed Information       | A link that displays additional information about the specific detection   |
| Endpoint Infection Channel | The channel that the threat originated from  |



| DATA                      | DESCRIPTION  |
|---------------------------|--|
| Apex One Domain Hierarchy | The agent tree domain or subdomain to which the Security Agent belongs |
| Domain                    | The domain of the managed product server to which the endpoint reports |
| Operating System          | The operating system on the endpoint                                   |
| Cloud Service Vendor      | The name of the cloud service vendor                                   |

## Endpoint Spyware/Grayware

Provides specific information about endpoints with spyware/grayware detections, such as the managed product that detected the spyware/grayware, the type of scan that detected the spyware/grayware, and the file path on the endpoint to the detected spyware/grayware

**TABLE B-45. Endpoint Spyware/Grayware Data View**

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Received                    | The date and time Apex Central received the data from the managed product  |
| Generated                   | The date and time the managed product generated the data   |
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the Security Agent endpoint</li> </ul> |
| Product/Endpoint IP         | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the endpoint</li> </ul>  |
| Product                     | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Managing Server Entity      | The display name of the managed product server in Apex Central to which the endpoint reports   |

| <b>DATA</b>          | <b>DESCRIPTION</b>   |
|----------------------|--|
| Spyware/Grayware     | The name of the security threat  |
| Endpoint             | The IP address or name of the endpoint that the threat accessed  |
| Source Host          | The IP address or name of the endpoint from which the security threat originated                                     |
| User                 | The logged on user name at the time of the event   |
| Scan Type            | The type of scan that reported the event (for example, Real-time Scan, Scheduled Scan, Manual Scan)                  |
| Resource             | The specific resource affected by the security threat<br>Example: application.exe, H Key Local Machine\SOFTWARE\ACME |
| Resource Type        | The type of resource affected by the security threat<br>Example: registry, memory resource                           |
| Security Threat Type | The type of security threat<br>Example: adware, COOKIE, peer-to-peer application                                     |
| Risk Level           | The risk level of the security threat<br>Example: High security, Medium security, Low security                       |
| Result               | The result of the action taken by the managed product<br>Example: successful, further action required                |
| Action               | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted                     |
| Detections           | The total number of detections   |
| Cloud Service Vendor | The name of the cloud service vendor   |

## Endpoint Spyware/Grayware Summary

Provides a summary of spyware/grayware detections from specific endpoints. Example: name of endpoint, number of specific spyware/

grayware instances on the endpoint, total number of instances of spyware/grayware on the network

**TABLE B-46. Endpoint Spyware/Grayware Summary Data View**

| DATA              | DESCRIPTION   |
|-------------------|---|
| Endpoint          | Displays the host name or IP address of the computer affected by spyware/grayware.  |
| Unique Sources    | <p>Displays the number of unique sources where spyware/grayware originates.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources.</p> <p>Unique Sources = 2</p> |
| Unique Detections | <p>Displays the number of unique spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Unique Detections = 1</p>                    |
| Detections        | <p>Displays the total number of spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Detections = 10</p>                           |

## Email Spyware/Grayware

Provides specific information about email messages with spyware/grayware detections, such as the managed product that detected the spyware/grayware, the subject line content of the email message, and the sender of the email message containing spyware/grayware

**TABLE B-47. Email Spyware/Grayware Data View**

| <b>DATA</b>             | <b>DESCRIPTION</b>   |
|-------------------------|--|
| Received                | The date and time Apex Central received the data from the managed product  |
| Generated               | The date and time the managed product generated the data   |
| Product Entity          | The display name of the managed product server in Apex Central   |
| Product                 | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Spyware/Grayware        | The name of the security threat  |
| Recipient               | The recipient(s) of the email message that triggered the detection   |
| Sender                  | The sender of the email message that triggered the detection   |
| User                    | The logged on user name at the time of the event   |
| Subject                 | The subject of the email message that triggered the detection  |
| File                    | The name of the file object that the threat accessed   |
| File in Compressed File | The name of the affected file object in the compressed archive   |
| Result                  | The result of the action taken by the managed product<br>Example: successful, further action required  |
| Action                  | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted   |
| Detections              | The total number of detections<br>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.<br>Detections = 10 |
| Cloud Service Vendor    | The name of the cloud service vendor   |

## Network Spyware/Grayware

Provides specific information about the spyware/grayware instances found in network traffic, such as the managed product that detected the spyware/grayware, the protocol the spyware/grayware used to enter your network, and specific information about the source and destination of the spyware/grayware

**TABLE B-48. Network Spyware/Grayware Data View**

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Received                    | The date and time Apex Central received the data from the managed product  |
| Generated                   | The date and time the managed product generated the data   |
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>The display name of the managed product server in Apex Central</li> <li>The name or IP address of the Security Agent endpoint</li> </ul> |
| Product                     | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Spyware/Grayware            | The name of the security threat  |
| Traffic/Connection          | The direction of the transmission  |
| Protocol                    | The protocol that the threat used to enter the network<br>Example: HTTP, SMTP, FTP   |
| Endpoint IP                 | The IP address that the threat accessed  |
| Endpoint                    | The IP address or name of the endpoint that the threat accessed  |
| Endpoint Port               | The IP port number that the threat accessed  |
| Endpoint MAC                | The MAC address that the threat accessed   |
| Source IP                   | The source IP address of the detected threat   |
| Source Host                 | The IP address or name of the endpoint from which the security threat originated   |

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Source Port          | The source IP address port number of the detected threat   |
| Source MAC           | The source MAC address of the detected threat  |
| User                 | The logged on user name at the time of the event   |
| File                 | The name of the file object that the threat accessed   |
| Result               | The result of the action taken by the managed product<br>Example: successful, further action required  |
| Action               | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted   |
| Detections           | The total number of detections<br><br>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.<br><br>Detections = 10 |
| Cloud Service Vendor | The name of the cloud service vendor   |

## Overall Spyware/Grayware Summary

Provides overall specific summary for spyware/grayware detections.  
Example: name of spyware/grayware, number of endpoints affected by the spyware/grayware, total number of instances of the spyware/grayware on the network

**TABLE B-49. Overall Spyware/Grayware Summary Data View**

| DATA             | DESCRIPTION  |
|------------------|--|
| Spyware/Grayware | Displays the name of spyware/grayware managed products detect. |

| DATA             | DESCRIPTION  |
|------------------|--|
| Unique Endpoints | Displays the number of unique computers affected by the spyware/grayware.<br><br>Apex One detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers.<br><br>Unique Endpoints = 3                   |
| Unique Sources   | Displays the number of unique sources where spyware/grayware originates.<br><br>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources.<br><br>Unique Sources = 2 |
| Detections       | Displays the total number of spyware/grayware managed products detect.   |

### Spyware/Grayware Action/Result Summary

Provides a summary of the actions managed products take against spyware/grayware. Example: specific actions taken against spyware/grayware, the result of the action taken, total number of instances of spyware/grayware on the network

**TABLE B-50. Spyware/Grayware Action/Result Summary Data View**

| DATA   | DESCRIPTION  |
|--------|--|
| Result | Displays the results of the action managed products take against spyware/grayware.<br><br>Example: successful, further action required   |
| Action | Displays the type of action managed products take against spyware/grayware.<br><br>Example: File cleaned, File quarantined, File deleted |

| DATA             | DESCRIPTION   |
|------------------|---|
| Unique Endpoints | <p>Displays the number of unique computers affected by the spyware/grayware.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers.</p> <p>Unique Endpoints = 3</p>          |
| Unique Sources   | <p>Displays the number of unique sources where spyware/grayware originates.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources.</p> <p>Unique Sources = 2</p> |
| Detections       | <p>Displays the total number of spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Detections = 10</p>                           |

## Spyware/Grayware Detection Over Time Summary

Provides a summary of spyware/grayware detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints affected by the spyware/grayware, total number of instances of spyware/grayware on the network

**TABLE B-51. Spyware/Grayware Detection Over Time Summary Data View**

| DATA              | DESCRIPTION  |
|-------------------|--|
| Date/Time         | Displays the time that the summary of the data occurs.   |
| Unique Detections | <p>Displays the number of unique spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Unique Detections = 1</p> |



| DATA             | DESCRIPTION   |
|------------------|---|
| Unique Endpoints | <p>Displays the number of unique computers affected by the spyware/grayware.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers.</p> <p>Unique Endpoints = 3</p>          |
| Unique Sources   | <p>Displays the number of unique sources where spyware/grayware originates.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources.</p> <p>Unique Sources = 2</p> |
| Detections       | <p>Displays the total number of spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Detections = 10</p>                           |

## Spyware/Grayware Source Summary

Provides a summary of spyware/grayware detections from the source of the outbreak. Example: name of source computer, number of specific spyware/grayware instances from the source computer, total number of instances of spyware/grayware on the network

**TABLE B-52. Spyware/Grayware Source Summary Data View**

| DATA        | DESCRIPTION  |
|-------------|--|
| Source Host | Displays the name of the computer where spyware/grayware originates. |

| DATA              | DESCRIPTION  |
|-------------------|--|
| Unique Endpoints  | <p>Displays the number of unique computers affected by the spyware/grayware.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers.</p> <p>Unique Endpoints = 3</p> |
| Unique Detections | <p>Displays the number of unique spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Unique Detections = 1</p>           |
| Detections        | <p>Displays the total number of spyware/grayware managed products detect.</p> <p>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.</p> <p>Detections = 10</p>                  |

## Web Spyware/Grayware

Provides specific information about the spyware/grayware instances found in HTTP or FTP traffic, such as the managed product that detected the spyware/grayware, the direction of traffic where the spyware/grayware occurs, and the web browser or FTP client that downloaded the spyware/grayware

**TABLE B-53. Web Spyware/Grayware Data View**

| DATA      | DESCRIPTION   |
|-----------|---|
| Received  | The date and time Apex Central received the data from the managed product |
| Generated | The date and time the managed product generated the data                  |

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the Security Agent endpoint</li> </ul> |
| Product                     | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Spyware/Grayware            | The name of the security threat  |
| IP                          | The IP address of the endpoint   |
| Source URL                  | The URL of the web/FTP site from which the security threat originated  |
| Traffic/Connection          | The direction of the transmission  |
| Browser/FTP Client          | The web browser or FTP client that the threat accessed   |
| User                        | The logged on user name at the time of the event   |
| Result                      | The result of the action taken by the managed product<br>Example: successful, further action required  |
| Action                      | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted   |
| Detections                  | The total number of detections<br><br>Example: Apex One detects 10 spyware/grayware instances of the same spyware/grayware on one computer.<br><br>Detections = 10   |
| Cloud Service Vendor        | The name of the cloud service vendor   |

## Virus/Malware Information

Displays summary and detailed data about malware/viruses that managed products detect on your network.

## Detailed Virus/Malware Information

Provides specific information about the virus/malware detections on your network, such as the managed product that detected the viruses/malware, the name of the virus/malware, and the infected endpoint

**TABLE B-54. Detailed Virus/Malware Information Data View**

| DATA                          | DESCRIPTION   |
|-------------------------------|---|
| Received                      | The date and time Apex Central received the data from the managed product   |
| Generated                     | The date and time the managed product generated the data  |
| Product Entity/<br>Endpoint   | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the endpoint</li> </ul> |
| Product                       | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Product/Endpoint IP           | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the endpoint</li> </ul>                           |
| Product/Endpoint<br>MAC       | Depending on the related source: <ul style="list-style-type: none"> <li>• The MAC address of the managed product server</li> <li>• The MAC address of the Security Agent endpoint</li> </ul>          |
| Managing Server<br>Entity     | The display name of the managed product server in Apex Central to which the endpoint reports  |
| Domain                        | The domain of the managed product server to which the endpoint reports  |
| Virus/Malware                 | The name of the security threat   |
| Endpoint Infection<br>Channel | The channel that the threat originated from   |
| Endpoint                      | The name or IP address of the endpoint  |

| DATA                      | DESCRIPTION  |
|---------------------------|--|
| Source Host               | The IP address or name of the endpoint from which the security threat originated   |
| User                      | The logged on user name at the time of the event   |
| Result                    | The result of the action taken by the managed product  |
| Action                    | The action taken by the managed product  |
| Detections                | The total number of detections<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br><br>Detections = 10 |
| Entry Type                | The entry point of the security threat   |
| Detailed Information      | A link that displays additional information about the specific detection   |
| Apex One Domain Hierarchy | The agent tree domain or subdomain to which the Security Agent belongs   |
| Department                | The Active Directory department to which the endpoint belongs  |
| Operating System          | The operating system on the endpoint   |
| Pattern/Rule              | The pattern or rule that triggered the detection   |
| Pattern/Rule Version      | The version of the pattern or rule that triggered the detection  |
| Cloud Service Vendor      | The name of the cloud service vendor   |
| File                      | The name of the file object or the program that executed the process   |
| File Path                 | The path of the file object or the path of the program that executed the process   |

## Endpoint Virus/Malware Information

Provides specific information about endpoints with virus/malware detections, such as the managed product that detected the viruses/malware, the type of scan that detected the virus/malware, and the file path on the endpoint to the detected viruses/malware

**TABLE B-55. Endpoint Virus/Malware Information Data View**

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Received                    | The date and time Apex Central received the data from the managed product  |
| Generated                   | The date and time the managed product generated the data   |
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the Security Agent endpoint</li> </ul> |
| Product/Endpoint IP         | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the Security Agent endpoint</li> </ul>                           |
| Product                     | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Managing Server<br>Entity   | The display name of the managed product server in Apex Central to which the endpoint reports   |
| Virus/Malware               | The name of the security threat<br>Example: NIMDA, BLASTER, I_LOVE_YOU.EXE   |
| Endpoint                    | The name of the endpoint   |
| User                        | The logged on user name at the time of the event   |
| Scan Type                   | The type of scan that reported the event (for example, Real-time Scan, Scheduled Scan, Manual Scan)  |
| File                        | The name of the file object that the threat accessed   |
| File Path                   | The path of the file object that the threat accessed   |
| File in Compressed<br>File  | The name of the affected file object in the compressed archive   |
| Result                      | The result of the action taken by the managed product<br>Example: successful, further action required  |

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Action               | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted                                     |
| Detections           | The total number of detections<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10 |
| Cloud Service Vendor | The name of the cloud service vendor   |

## Email Virus/Malware Information

Provides specific information about email messages with virus/malware detections, such the managed product that detected the viruses/malware, the subject line content of the email message, and the sender of the email message containing viruses/malware

**TABLE B-56. Email Virus/Malware Information Data View**

| DATA           | DESCRIPTION  |
|----------------|--|
| Received       | The date and time Apex Central received the data from the managed product                        |
| Generated      | The date and time the managed product generated the data   |
| Product Entity | The display name of the managed product server in Apex Central                                   |
| Product        | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |
| Virus/Malware  | The name of the security threat<br>Example: NIMDA, BLASTER, I_LOVE_YOU.EXE                       |
| Recipient      | The recipient(s) of the email message that triggered the detection                               |
| Sender         | The sender of the email message that triggered the detection                                     |
| User           | The logged on user name at the time of the event   |

| DATA                    | DESCRIPTION  |
|-------------------------|--|
| Subject                 | The subject of the email message that triggered the detection  |
| File                    | The name of the file object that the threat accessed   |
| File in Compressed File | The name of the affected file object in the compressed archive   |
| Result                  | The result of the action taken by the managed product<br>Example: successful, further action required                                    |
| Action                  | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted   |
| Detections              | The total number of detections<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10 |
| Cloud Service Vendor    | The name of the cloud service vendor   |

## Network Virus/Malware Information

Provides specific information about the virus/malware instances found in network traffic, such as the managed product that detects the viruses/malware, the protocol the virus/malware uses to enter your network, specific information about the source and destination of the virus/malware

**TABLE B-57. Network Virus/Malware Information Data View**

| DATA      | DESCRIPTION   |
|-----------|---|
| Received  | The date and time Apex Central received the data from the managed product |
| Generated | The date and time the managed product generated the data                  |



| <b>DATA</b>                 | <b>DESCRIPTION</b>  |
|-----------------------------|---|
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the endpoint</li> </ul> |
| Product                     | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Virus/Malware               | The name of the security threat<br>Example: NIMDA, BLASTER, I_LOVE_YOU.EXE  |
| Endpoint                    | The IP address or name of the endpoint that the threat accessed   |
| Source Host                 | The IP address or name of the endpoint from which the security threat originated  |
| User                        | The logged on user name at the time of the event  |
| Traffic/Connection          | The direction of the transmission   |
| Protocol                    | The protocol that the threat used to enter the network<br>Example: HTTP, SMTP, FTP  |
| Endpoint Computer           | The IP address or name of the endpoint that the threat accessed   |
| Endpoint Port               | The IP port number that the threat accessed   |
| Endpoint MAC                | The MAC address that the threat accessed  |
| Source Computer             | The IP address or name of the endpoint from which the security threat originated  |
| Source Port                 | The source IP address port number of the detected threat  |
| Source MAC                  | The source MAC address of the detected threat   |
| File                        | The name of the file object that the threat accessed  |
| Result                      | The result of the action taken by the managed product<br>Example: successful, further action required   |

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Action               | The action taken by the managed product<br>Example: File cleaned, File quarantined, File deleted                                     |
| Detections           | The total number of detections<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10 |
| Cloud Service Vendor | The name of the cloud service vendor   |

## Overall Virus/Malware Summary

Provides overall specific summary for virus/malware detections. Example: name of virus/malware, number of endpoints affected by the virus, total number of instances of the virus on the network

**TABLE B-58. Overall Virus/Malware Summary Data View**

| DATA             | DESCRIPTION  |
|------------------|--|
| Virus/Malware    | Displays the name of viruses/malware managed products detect.<br>Example: NIMDA, BLASTER, I_LOVE_YOU.EXE   |
| Unique Endpoints | Displays the number of unique computers affected by the virus/malware.<br>Example: Apex One detects 10 virus instances of the same virus on 3 different computers.<br>Unique Endpoints = 3                     |
| Unique Sources   | Displays the number of unique infection sources where viruses/malware originate.<br>Example: Apex One detects 10 virus instances of the same virus originating from 2 infection sources.<br>Unique Sources = 2 |

| DATA       | DESCRIPTION  |
|------------|--|
| Detections | <p>Displays the total number of viruses/malware managed products detect.</p> <p>Example: Apex One detects 10 virus instances of the same virus on one computer.</p> <p>Detections = 10</p> |

## Virus/Malware Action/Result Summary

Provides a summary of the actions managed products take against viruses/malware. Example: specific actions taken against viruses/malware, the result of the action taken, total number of instances of viruses/malware on the network

**TABLE B-59. Virus/Malware Action/Result Summary Data View**

| DATA             | DESCRIPTION   |
|------------------|---|
| Result           | <p>Displays the results of the action managed products take against viruses/malware.</p> <p>Example: successful, further action required</p>  |
| Action           | <p>Displays the type of action managed products take against viruses/malware.</p> <p>Example: File cleaned, File quarantined, File deleted</p>  |
| Unique Endpoints | <p>Displays the number of unique computers affected by the virus/malware.</p> <p>Example: Apex One detects 10 virus instances of the same virus on 3 different computers.</p> <p>Unique Endpoints = 3</p>                     |
| Unique Sources   | <p>Displays the number of unique infection sources where viruses/malware originate.</p> <p>Example: Apex One detects 10 virus instances of the same virus originating from 2 infection sources.</p> <p>Unique Sources = 2</p> |

| DATA       | DESCRIPTION   |
|------------|---|
| Detections | <p>Displays the total number of viruses/malware managed products detect. Example: Apex One detects 10 virus instances of the same virus on one computer.</p> <p>Detections = 10</p> |

## Virus/Malware Detection Over Time Summary

Provides a summary of virus/malware detections over a period of time

| DATA              | DESCRIPTION   |
|-------------------|---|
| Date/Time         | <p>Displays the time that the summary of the data occurs.</p>   |
| Unique Detections | <p>Displays the number of unique virus/malware detections.</p> <p>Example: A managed product detects the same virus on 2 endpoints.</p> <p>Unique Detections = 1</p>              |
| Unique Endpoints  | <p>Displays the number of unique endpoints with virus/malware detections.</p> <p>Example: A managed product detects a virus on 4 endpoints.</p> <p>Unique Endpoints = 4</p>       |
| Unique Sources    | <p>Displays the number of unique sources of virus/malware.</p> <p>Example: A managed product detects 10 viruses from two different sources.</p> <p>Unique Sources = 2</p>         |
| Detections        | <p>Displays the total number of viruses/malware managed products detect.</p> <p>Example: A managed product detects 10 viruses/malware on one computer.</p> <p>Detections = 10</p> |

## Virus/Malware Endpoint Summary

Provides a summary of virus/malware detections from specific endpoints. Example: name of endpoint, number of specific virus/malware instances on the endpoint, total number of instances of viruses/malware on the network

**TABLE B-60. Virus/Malware Endpoint Summary Data View**

| DATA              | DESCRIPTION  |
|-------------------|--|
| Endpoint          | Displays the IP address or host name of the computer affected by viruses/malware.  |
| Unique Sources    | Displays the number of unique infection sources where viruses/malware originate.<br><br>Example: Apex One detects 10 virus instances of the same virus originating from 2 infection sources.<br><br>Unique Sources = 2 |
| Unique Detections | Displays the number of unique virus/malware managed products detect.<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br><br>Unique Detections = 1                               |
| Detections        | Displays the total number of viruses/malware managed products detect.<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br><br>Detections = 10                                    |

## Virus/Malware Source Summary

Provides a summary of virus/malware detections from the source of the outbreak. Example: name of source computer, number of specific virus/malware instances from the source computer, total number of instances of viruses/malware on the network

**TABLE B-61. Virus/Malware Source Summary Data View**

| DATA              | DESCRIPTION   |
|-------------------|---|
| Source Host       | Displays the IP address or host name of the computer where viruses/malware originate  |
| Unique Endpoints  | Displays the number of unique computers affected by the virus/malware<br><br>Example: Apex One detects 10 virus instances of the same virus on 3 different computers<br><br>Unique Detections = 3 |
| Unique Detections | Displays the number of unique virus/malware managed products detect<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer<br><br>Detections = 10                  |
| Detections        | Displays the total number of viruses/malware managed products detect<br><br>Example: Apex One detects 10 virus instances of the same virus on one computer<br><br>Detections = 10                 |
| Department        | Displays the name of the department that the endpoint belongs to  |

## Web Virus/Malware Information

Provides specific information about the virus/malware instances found in HTTP or FTP traffic, such as the managed product that detected the viruses/malware, the direction of traffic, and the web browser or FTP client that downloaded the virus/malware

**TABLE B-62. Web Virus/Malware Information Data View**

| DATA     | DESCRIPTION   |
|----------|---|
| Received | The date and time Apex Central received the data from the managed product |

| DATA                        | DESCRIPTION   |
|-----------------------------|---|
| Generated                   | The date and time the managed product generated the data  |
| Product Entity/<br>Endpoint | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the endpoint</li> </ul> |
| Product                     | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange  |
| Virus/Malware               | The name of the security threat<br>Example: NIMDA, BLASTER, I_LOVE_YOU.EXE  |
| Endpoint                    | The IP address or name of the endpoint that the threat accessed   |
| Source URL                  | The URL of the web/FTP site from which the security threat originated   |
| User                        | The logged on user name at the time of the event  |
| Traffic/Connection          | The direction of the transmission   |
| Browser/FTP Client          | The web browser or FTP client that the threat accessed  |
| Result                      | The result of the action taken by the managed product   |
| Action                      | The action taken by the managed product   |
| Detections                  | The total number of detections<br>Example: Apex One detects 10 virus instances of the same virus on one computer.<br>Detections = 10  |
| Cloud Service Vendor        | The name of the cloud service vendor  |

## Web Violation/Reputation Information

Displays summary and detailed data about Internet violations that managed products detect on your network.

## Detailed Web Reputation Information

Provides compliance information about application activity detected by Web Reputation Services

**TABLE B-63. Detailed Web Reputation Information Data View**

| DATA               | DESCRIPTION  |
|--------------------|--|
| Received           | The date and time Apex Central received the data from the managed product                                      |
| Generated          | The date and time the managed product generated the data   |
| Product Entity     | The display name of the managed product server in Apex Central   |
| Product            | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange               |
| VLAN ID            | The VLAN ID (VID) of the source from which the suspicious threat originates                                    |
| Detected By        | The filter, scan engine, or managed product that detected the threat   |
| Traffic/Connection | The direction of the transmission  |
| Protocol Group     | The broad protocol group from which a managed product detects the suspicious threat<br>Example: FTP, HTTP, P2P |
| Protocol           | The protocol from which a managed product detects the suspicious threat<br>Example: ARP, BitTorrent            |
| Description        | Detailed description of the incident by Trend Micro  |
| Endpoint           | The host name of the computer in compliance of the policy/rule   |
| Source IP          | The source IP address of the detected threat   |
| Source MAC         | The source MAC address of the detected threat  |
| Source Port        | The source IP address port number of the detected threat   |



| DATA                    | DESCRIPTION   |
|-------------------------|---|
| Source IP Group         | The IP address group of the source where the suspicious threat originates   |
| Source Network Zone     | The network zone of the source where the suspicious threat originates   |
| Endpoint IP             | The IP address of the endpoint the suspicious threat affects  |
| Endpoint Port           | The port number of the endpoint the suspicious threat affects   |
| Endpoint MAC            | The MAC address of the endpoint the suspicious threat affects   |
| Endpoint Group          | The IP address group of the endpoint the suspicious threat affects  |
| Endpoint Network Zone   | The network zone of the endpoint the suspicious threat affects  |
| Policy/Rule             | The policy or rule that triggered the detection   |
| URL                     | The URL object that triggered the detection   |
| Detections              | <p>The total number of detections</p> <p>Example: A managed product detects 10 violations of the same type on one computer.</p> <p>Detections = 10</p>  |
| C&C List Source         | The C&C list source that identified the C&C server  |
| C&C Risk Level          | The risk level of the C&C server  |
| Threat Type             | The type of security threat   |
| Detection Severity      | The severity level of the event   |
| IP Address (Interested) | <p>The IP address of the target endpoint (source or destination)</p> <p>For an exchange occurring within the network, the Interested IP is the source IP address. If the traffic is an external traffic, the Interested IP is the destination IP address.</p> |
| IP Address (Peer)       | <p>The IP address opposite of the Interested IP</p> <p>For example, if the Interested IP is the source IP address, then the Peer IP is the destination IP address.</p>  |

| DATA                                  | DESCRIPTION   |
|---------------------------------------|---|
| Matching Classified Events            | The log count matching the same aggregated rule                   |
| Aggregated Matching Classified Events | The aggregated log count matching the same rule                   |
| Network Group                         | The name of the group   |
| Host Severity                         | The host severity   |
| Log ID                                | The log ID  |
| Attack Phase                          | The phase with which the attack happened                          |
| Remarks                               | Additional information about the event                            |
| C&C Server                            | The name, URL, or IP address of the C&C server                    |
| C&C Server Type                       | The type of C&C server  |
| Sender                                | The sender of the transmission that triggered the detection       |
| Recipient                             | The recipient(s) of the transmission that triggered the detection |
| Subject                               | The subject of the email message containing the web URL           |

## Detailed Web Violation Information

Provides specific information about web violations on your network

**TABLE B-64. Detailed Web Violation Information Data View**

| DATA                   | DESCRIPTION  |
|------------------------|--|
| Received               | The date and time Apex Central received the data from the managed product                    |
| Generated              | The date and time the managed product generated the data                                     |
| Managing Server Entity | The display name of the managed product server in Apex Central to which the endpoint reports |
| Product Entity         | The display name of the managed product server in Apex Central                               |

| <b>DATA</b>           | <b>DESCRIPTION</b>  |
|-----------------------|---|
| Product               | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange                            |
| Traffic/Connection    | The direction of the transmission   |
| Protocol              | The protocol over which the violation takes place<br>Example: HTTP, FTP, SMTP   |
| URL                   | The URL object that triggered the detection   |
| User/IP               | The user or IP address of the endpoint that violates a policy   |
| User Group            | The user group for the user that violates a policy  |
| Endpoint              | The IP address of the endpoint that violates a policy   |
| Endpoint Host         | The IP address or host name of the endpoint that violates a policy  |
| Product Host          | The IP address or host name of the managed product which detects the violation  |
| Filter/Blocking Type  | The type of filter/blocking preventing access to the URL in violation<br>Example: URL blocking, URL filtering, web blocking |
| Blocking Rule         | The blocking rule preventing access to the URL in violation<br>Example: URL blocking  |
| Policy                | The policy that triggered the detection   |
| File                  | The name of the file that violates a policy   |
| Process               | The name of the process that violates a policy  |
| Web Reputation Rating | The relative safety, as a percentage, of a website according to Trend Micro   |
| Action                | The action taken by the managed product<br>Example: pass, block   |

| DATA       | DESCRIPTION   |
|------------|---|
| Detections | The total number of detections<br><br>Example: A managed product detects 10 violation instances of the same URL on one computer.<br><br>Detections = 10 |

## Overall Web Violation Summary

Provides a summary of web violations of specific policies. Example: name of the policy in violation, the type of filter/blocking to stop access to the URL, the total number of web violations on the network

**TABLE B-65. Overall Web Violation Summary Data View**

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Policy               | Displays the name of the policy the URL violates.  |
| Filter/Blocking Type | Displays the type of filter/blocking preventing access to the URL in violation.<br><br>Example: URL blocking, URL filtering, web blocking  |
| Unique Endpoints     | Displays the number of unique endpoints in violation of the specified policy.<br><br>Example: A managed product detects 10 violation instances of the same URL on 4 computers.<br><br>Unique Endpoints = 4 |
| Unique URLs          | Displays the number of unique URLs in violation of the specified policy.<br><br>Example: A managed product detects 10 violation instances of the same URL on one computer.<br><br>Unique URLs = 1          |

| DATA       | DESCRIPTION   |
|------------|---|
| Detections | Displays the total number of web violations managed products detect.<br><br>Example: A managed product detects 10 violation instances of the same URL on 1 computer.<br><br>Detections = 10 |

## Web Violation Detection Over Time Summary

Provides a summary of web violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints in violation, the total number of web violations on the network

**TABLE B-66. Web Violation Detection Over Time Summary Data View**

| DATA             | DESCRIPTION  |
|------------------|--|
| Date/Time        | Displays the time that the summary of the data occurs.   |
| Unique Policies  | Displays the number of the policies in violation.<br><br>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.<br><br>Unique Policies = 1                    |
| Unique Endpoints | Displays the number of unique endpoints in violation of the specified policy.<br><br>Example: A managed product detects 10 violation instances of the same URL on 4 computers.<br><br>Unique Endpoints = 4 |
| Unique URLs      | Displays the number of unique URLs in violation of the specified policy.<br><br>Example: A managed product detects 10 violation instances of the same URL on one computer.<br><br>Unique URLs = 1          |

| DATA       | DESCRIPTION  |
|------------|--|
| Detections | <p>Displays the total number of web violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same URL on one computer.</p> <p>Detections = 10</p> |

## Web Violation Detection Summary

Provides a summary of web violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints in violation, the total number of web violations on the network

**TABLE B-67. Web Violation Detection Summary Data View**

| DATA             | DESCRIPTION   |
|------------------|---|
| Unique Policies  | <p>Displays the number of the policies in violation.</p> <p>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.</p> <p>Unique Policies = 1</p>                    |
| Unique Endpoints | <p>Displays the number of unique endpoints in violation of the specified policy.</p> <p>Example: A managed product detects 10 violation instances of the same URL on 4 computers.</p> <p>Unique Endpoints = 4</p> |
| Unique URLs      | <p>Displays the number of unique URLs in violation of the specified policy.</p> <p>Example: A managed product detects 10 violation instances of the same URL on one computer.</p> <p>Unique URLs = 1</p>          |

| DATA               | DESCRIPTION   |
|--------------------|---|
| Unique Users/IPs   | <p>Displays the number of unique users or IP addresses of endpoints in violation of the specified policy.</p> <p>Example: A managed product detects 10 violation instances of the same URL from one user.</p> <p>Unique Users/IPs = 1</p> |
| Unique User Groups | <p>Displays the number of unique user groups for users in violation of the specified policy.</p> <p>Example: A managed product detects 10 violation instances of the same URL from one user group.</p> <p>Unique User Groups = 1</p>      |
| Detections         | <p>Displays the total number of web violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same URL on one computer.</p> <p>Detections = 10</p>                                      |

## Web Violation Endpoint Summary

Provides a summary of web violation detections from a specific endpoint.  
**Example:** IP address of the endpoint in violation, number of policies in violation, the total number of web violations on the network

**TABLE B-68. Web Violation Endpoint Summary Data View**

| DATA            | DESCRIPTION  |
|-----------------|--|
| Endpoint        | <p>Displays the IP address or host name of endpoints in violation of web policies.</p>   |
| Unique Policies | <p>Displays the number of the policies in violation.</p> <p>Example: A managed product detects 10 policy violation instances of the same policy on 2 computers.</p> <p>Unique Policies = 1</p> |

| DATA        | DESCRIPTION  |
|-------------|--|
| Unique URLs | <p>Displays the number of unique URLs in violation of the specified policy.</p> <p>Example: A managed product detects 10 violation instances of the same URL on one computer.</p> <p>Unique URLs = 1</p> |
| Detections  | <p>Displays the total number of web violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same URL on one computer.</p> <p>Detections = 10</p>     |

## Web Violation Filter/Blocking Type Summary

Provides a summary of the action managed products take against web violations. Example: the type of filter/blocking to stop access to the URL, the total number of web violations on the network

**TABLE B-69. Web Violation Filter/Blocking Type Summary Data View**

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Blocking Category    | <p>Displays the broad type of filter/blocking preventing access to the URL in violation.</p> <p>Example: URL blocking, URL filtering, Anti-spyware</p>   |
| Filter/Blocking Type | <p>Displays the specific type of filter/blocking preventing access to the URL in violation.</p> <p>Example: URL blocking, URL filtering, Virus/Malware</p>   |
| Detections           | <p>Displays the total number of web violations managed products detect.</p> <p>Example: A managed product detects 10 violation instances of the same URL on one computer.</p> <p>Detections = 10</p> |



## Web Violation URL Summary

Provides a summary of web violation detections from specific URLs.

Example: name of the URL causing the web violation, the type of filter/blocking to stop access to the URL, the total number of web violations on the network

**TABLE B-70. Web Violation URL Summary Data View**

| DATA                 | DESCRIPTION  |
|----------------------|--|
| URL                  | Displays the URL violating a web policy.   |
| Filter/Blocking Type | Displays the type of filter/blocking preventing access to the URL in violation.<br>Example: URL blocking, URL filtering, web blocking  |
| Unique Endpoints     | Displays the number of unique endpoints in violation of the specified policy.<br>Example: A managed product detects 10 violation instances of the same URL on 4 computers.<br>Unique Endpoints = 4 |
| Detections           | Displays the total number of web violations managed products detect.<br>Example: A managed product detects 10 violation instances of the same URL on one computer.<br>Detections = 10              |

## Data View: Product Information

Displays information about Apex Central, managed products, components, and licenses.

### Apex Central Information

Displays information about Apex Central user access, Command Tracking information, and Apex Central server events.

## Apex Central Event Information

Provides information about Apex Central server events, such as managed products registering to Apex Central, component updates, and Activation Code deployments

**TABLE B-71. Apex Central Event Information Data View**

| DATA        | DESCRIPTION   |
|-------------|---|
| Date/Time   | The that the event occurred   |
| Event Type  | The type of event that occurred (Example: notify TMI agent, server notify user, report service notify user) |
| Result      | The result of the event (Example: successful, unsuccessful)   |
| Description | The description of the activity (if available)  |

## Command Tracking Information

Provides information about commands Apex Central issued to managed products, such as the date and time Apex Central issued commands for component updates or Activation Code deployments, and the status of the commands

**TABLE B-72. Command Tracking Information Data View**

| DATA              | DESCRIPTION  |
|-------------------|--|
| Date/Time         | The time that the issuer of the command issues the command   |
| Command Type      | The type of command issued (Example: scheduled update, Activation Code deployment)                               |
| Command Parameter | The specific information relating to the command (Example: specific pattern file name, specific Activation Code) |
| User              | The user who issued the command  |
| Status Update     | The time of the latest status check of all commands for the selected Apex Central                                |
| Successful        | The number of successful commands  |

| DATA         | DESCRIPTION  |
|--------------|--|
| Unsuccessful | The number of unsuccessful commands                                    |
| In Progress  | The number of commands that are still in progress                      |
| All          | The total number of commands (Successful + Unsuccessful + In progress) |

## Detailed Command Tracking Information

Displays detailed information relating to commands. Examples: managed products registering to Apex Central, component updates, Activation Code deployments

**TABLE B-73. Detailed Command Tracking Information Data View**

| DATA                      | DESCRIPTION  |
|---------------------------|--|
| Date/Time                 | Displays the time that the command was issued.   |
| Command Type              | Displays the type of command issued. Example: scheduled update, Activation Code deployment                               |
| Command Parameter         | Displays the specific information relating to the command. Example: specific pattern file name, specific Activation Code |
| Product Entity            | Displays the managed product to which the command was issued.  |
| User                      | Displays the user who issued the command.  |
| Command Status            | Displays the status of the command: successful, unsuccessful, in progress  |
| Status Update             | Displays the time of the latest status check of all commands for the selected Apex Central.                              |
| Result Detail Description | Displays the description Apex Central provides for events.   |

## Unmanaged Endpoint Information

Provides information about detected endpoints that do not have a Trend Micro Security Agent installed

**TABLE B-74. Unmanaged Endpoint Information Data View**

| DATA     | DESCRIPTION              |
|----------|--------------------------|
| Endpoint | The name of the endpoint |

## User Access Information

Provides information about Apex Central user access and the activities users perform while logged on to Apex Central

**TABLE B-75. User Access Information Data View**

| DATA                   | DESCRIPTION   |
|------------------------|---|
| Date/Time              | Date and time the activity started  |
| User                   | Name of the user who initiated the activity   |
| Active Directory Group | Name of the Active Directory group  |
| User Role              | User role assigned to the user account in Apex Central  |
| Activity               | Activity the user performed on Apex Central (Example: log on, edit user account, add deployment plan) |
| Result                 | Result of the activity  |
| Description            | Description of the activity (if available)  |
| Description of Role    | Description of the user role assigned to the user account   |

## Component Information

Displays status, detailed, and summary information about out of date and up to date and component deployment of managed product components.

## Endpoint Pattern/Engine Status Summary

Displays summary information about pattern files/scan engine managed products use.

**TABLE B-76. Endpoint Pattern/Engine Status Summary**

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Product Host                | Displays the host name of the server on which the managed product installs.  |
| Domain                      | Displays the domain name of the host.  |
| Endpoints                   | Displays the host name of a computer with an agent (for example Apex One agent) installed.   |
| Patterns Out-of-Date        | Displays the number of managed products with out-of-date pattern files.  |
| Pattern Up-to-Date Rate (%) | Displays the percentage of managed products with up-to-date pattern files. This includes pattern files that return n/a as a value. |
| Engines Out-of-Date         | Displays the number of managed products with out-of-date scan engines.   |
| Engine Up-to-Date Rate (%)  | Displays the percentage of managed products with up-to-date scan engines. This includes scan engines that return n/a as a value.   |

## Endpoint Pattern/Rule Update Status Summary

This data view displays summary information about the update status of patterns or rules.

**TABLE B-77. Endpoint Pattern/Rule Update Status Summary Data View**

| DATA                 | DESCRIPTION  |
|----------------------|--|
| Pattern/Rule         | Displays the name of the pattern or rule   |
| Pattern/Rule Status  | Indicates whether the current version of the pattern or rule is up-to-date           |
| Pattern/Rule Version | Displays the version of the pattern or rule  |
| Pattern/Rule Updated | Indicates whether the pattern or rule has been updated successfully                  |
| Endpoint Count       | Displays the number of endpoints that use the current version of the pattern or rule |

| DATA            | DESCRIPTION   |
|-----------------|---|
| Total Endpoints | Displays the total number endpoints that use the pattern or rule                      |
| Rate (%)        | Displays the percentage of endpoints using the current version of the pattern or rule |

## Engine Status

Displays detailed information about scan engines managed products use. Examples: scan engine name, time of the latest scan engine deployment, and which managed products use the scan engine

**TABLE B-78. Engine Status Data View**

| DATA                        | DESCRIPTION  |
|-----------------------------|--|
| Product Entity/<br>Endpoint | This data column displays one of the following: <ul style="list-style-type: none"> <li>The entity display name for a managed product. Apex Central identifies managed products using the managed product's entity display name.</li> <li>The IP address or host name of a computer with an agent (for example, Apex One agent) installed.</li> </ul> |
| Product Host/<br>Endpoint   | This data column displays one of the following: <ul style="list-style-type: none"> <li>The host name of the server on which the managed product installs.</li> <li>The IP address of a computer with an agent (for example, Apex One agent) installed.</li> </ul>  |
| Product/Endpoint IP         | This data column displays one of the following: <ul style="list-style-type: none"> <li>The IP address of the server on which the managed product installs.</li> <li>The IP address of a computer with an agent (for example, Apex One agent) installed.</li> </ul>   |

| DATA              | DESCRIPTION   |
|-------------------|---|
| Connection Status | This data column displays one of the following: <ul style="list-style-type: none"> <li>• The managed product's connection status to Apex Central. Example: Normal, Abnormal, Offline</li> <li>• The endpoint agent's connection status to a managed product (Apex One). Example: Normal, Abnormal, Offline</li> </ul> |
| Product           | Displays the name of the managed product. Example: Apex One, ScanMail for Microsoft Exchange  |
| Product Version   | Displays the managed product's or managed product agent's version number. Example: Apex One 2019, Apex Central 2019   |
| Product Role      | Displays the role the managed product or a computer with an agent (for example, Apex One agent) has in the network environment. Example: server   |
| Engine            | Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine  |
| Engine Version    | Displays the version of the scan engine. Example: Anti-spam Engine (Windows): 3.000.1153, Virus Scan Engine IA 64 bit Scan Engine: 8.000.1008   |
| Engine Status     | Displays the scan engine currency status. Example: up-to-date, out-of-date  |
| Engine Updated    | Displays the time of the latest scan engine deployment to managed products or endpoints.  |

## Pattern/Rule Status

Displays detailed information about pattern files/rules managed products use. Examples: pattern file/rule name, time of the latest pattern file/rule deployment, and which managed products use the pattern file/rule

**TABLE B-79. Pattern/Rule Status Data View**

| DATA                                   | DESCRIPTION  |
|--|--|
| Product Entity/<br>Endpoint            | This data column displays one of the following: <ul style="list-style-type: none"> <li>• The entity display name for a managed product. Apex Central identifies managed products using the managed product's entity display name.</li> <li>• The IP address or host name of a computer with an agent (for example, Apex One agent) installed.</li> </ul> |
| Operating System                       | This data column displays the operating system of the server on which the managed product installs.  |
| Product Host/<br>Endpoint              | This data column displays one of the following: <ul style="list-style-type: none"> <li>• The host name of the server on which the managed product installs.</li> <li>• The IP address of a computer with an agent (for example, Apex One agent) installed.</li> </ul>  |
| Product/Endpoint IP                    | This data column displays one of the following: <ul style="list-style-type: none"> <li>• The IP address of the server on which the managed product installs.</li> <li>• The IP address of a computer with an agent (for example, Apex One agent) installed.</li> </ul>   |
| Update Agent                           | This data column displays Update Agents for the managed product.   |
| Domain                                 | This data column displays the domain of the server on which the managed product installs.  |
| Managing Server<br>Entity Display Name | This data column displays the managing server entity display name.   |
| Connection Status                      | This data column displays one of the following: <ul style="list-style-type: none"> <li>• The managed product's connection status to Apex Central. Example: Normal, Abnormal, Offline</li> <li>• The endpoint agent's connection status to a managed product (Apex One). Example: Normal, Abnormal, Offline</li> </ul>                                    |



| DATA                      | DESCRIPTION   |
|---------------------------|---|
| Product                   | Displays the name of the managed product. Example: Apex One, ScanMail for Microsoft Exchange  |
| Product Version           | Displays the managed product's or managed product agent's version number. Example: Apex One 2019, Apex Central 2019                             |
| Product Role              | Displays the role the managed product or a computer with an agent (for example, Apex One agent) has in the network environment. Example: server |
| Pattern/Rule              | Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern   |
| Pattern/Rule Version      | Displays the version of the pattern file or rule. Example: Virus Pattern File: 3.203.00, Anti-spam Pattern: 14256                               |
| Pattern/Rule Status       | Displays the pattern file/rule currency status. Example: up-to-date, out-of-date  |
| Pattern/Rule Updated      | Displays the time of the latest pattern file/rule deployment to managed products or endpoints.  |
| Apex One Domain Hierarchy | Displays the path on the Apex One domain hierarchy.   |

## Pattern File/Rule Status Summary

Displays summary information about pattern files/rules that managed products use. Examples: pattern file/rule name, pattern file/rule up-to-date rate, and the number of pattern files/rules out-of-date

**TABLE B-80. Pattern File/Rule Status Summary Data View**

| DATA              | DESCRIPTION   |
|-------------------|---|
| Pattern File/Rule | Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern                     |
| Version           | Displays the version of the pattern file or rule. Example: Virus Pattern File: 3.203.00, Anti-spam Pattern: 14256 |

| DATA                            | DESCRIPTION  |
|---------------------------------|--|
| Up-to-Date                      | Displays the number of managed products with up-to-date pattern files or rules.  |
| Out-of-Date                     | Displays the number of managed products with out-of-date pattern files or rules.   |
| Up-to-Date Rate (%)             | Displays the percentage of managed products with up-to-date pattern files/rules. This includes pattern files/rules that return n/a as a value. |
| 1 Version Old Rate (%)          | Displays the percentage of managed products with pattern files/rules that are 1 version old  |
| 2 Versions Old Rate (%)         | Displays the percentage of managed products with pattern files/rules that are 2 versions old   |
| 3 Versions Old Rate (%)         | Displays the percentage of managed products with pattern files/rules that are 3 versions old   |
| 4 Versions Old Rate (%)         | Displays the percentage of managed products with pattern files/rules that are 4 versions old   |
| 5 Versions Old Rate (%)         | Displays the percentage of managed products with pattern files/rules that are 5 versions old   |
| 6 or More Versions Old Rate (%) | Displays the percentage of managed products with pattern files/rules that are 6 or more versions old   |

## Product Component Deployment

Displays detailed information about components managed products use. Examples: pattern file/rule name, pattern file/rule version number, and scan engine deployment status

**TABLE B-81. Product Component Deployment Data View**

| DATA           | DESCRIPTION   |
|----------------|---|
| Product Entity | Displays the entity display name for a managed product. Apex Central identifies managed products using the managed product's entity display name. |

| DATA                           | DESCRIPTION   |
|--------------------------------|---|
| Product                        | Displays the name of the managed product. Example: Apex One, ScanMail for Microsoft Exchange                                |
| Product Version                | Displays the managed product's version number. Example: Apex One 2019, Apex Central 2019                                    |
| Connection Status              | Displays the connection status between the managed product and Apex Central server or managed products and their endpoints. |
| Pattern/Rule Status            | Displays the pattern file/rule currency status. Example: up-to-date, out-of-date  |
| Pattern/Rule Deployment Status | Displays the deployment status for the latest pattern file/rule update. Example: successful, unsuccessful, in progress      |
| Pattern/Rule Deployment        | Displays the time of the latest pattern file/rule deployment to managed products or endpoints.                              |
| Engine Status                  | Displays the scan engine currency status. Example: up-to-date, out-of-date  |
| Engine Deployment Status       | Displays the deployment status for the latest scan update. Example: successful, unsuccessful, in progress                   |
| Engine Deployment              | Displays the time of the latest scan engine deployment to managed products or endpoints.                                    |

## Scan Engine Status Summary

Displays summary information about scan engines managed products use. Examples: scan engine name, scan engine rate, and the number of scan engines out-of-date

**TABLE B-82. Engine Status Summary Data View**

| DATA   | DESCRIPTION  |
|--------|--|
| Engine | Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine |

| DATA                | DESCRIPTION   |
|---------------------|---|
| Version             | Displays the version of the scan engine. Example: Anti-spam Engine (Windows): 3.000.1153, Virus Scan Engine IA 64 bit Scan Engine: 8.000.1008 |
| Up-to-Date          | Displays the number of managed products with up-to-date scan engines.   |
| Out-of-Date         | Displays the number of managed products with out-of-date scan engines.  |
| Up-to-Date Rate (%) | Displays the percentage of managed products with up-to-date scan engines. This includes scan engines that return N/A as a value.              |

## License Information

Displays status, detailed, and summary information about Apex Central and managed product license information.

### Detailed Product License Information

Provides information about the Activation Codes and licensing status of managed products or services, such as the managed product version and license expiration date

**TABLE B-83. Detailed Product License Information Data View**

| DATA            | DESCRIPTION  |
|-----------------|--|
| Product Entity  | The display name of the managed product server in Apex Central                                   |
| Product         | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |
| Product Version | The version of the managed product or service  |
| Managed Service | The name of the managed service<br>Example: Web Reputation Service                               |
| License Status  | The status of the license for managed products<br>Example: Activated, Expired, In grace period   |

| DATA               | DESCRIPTION  |
|--------------------|--|
| Product Type       | The type of managed product the Activation Code provides<br>Example: Trial version, Full version |
| Activation Code    | The Activation Code for the managed product or service   |
| License Expiration | The date the license expires for the managed product or service                                  |
| Seats              | The number of seats the Activation Code allows   |
| Description        | The description for the Activation Code  |

## Product License Information Summary

Displays detailed information about the Activation Code and information on managed products that use the Activation Code. Examples: seat count that the Activation Code allows, evaluation or full product version, user-defined description about the Activation Code

**TABLE B-84. Product License Information Summary Data View**

| DATA                     | DESCRIPTION   |
|--------------------------|---|
| Activation Code          | Displays the Activation Code for managed products.  |
| User-defined Description | Displays the user-defined description for the Activation Code.  |
| Products/Services        | Displays the number of managed products or services that use the Activation Code.                       |
| License Status           | Displays the status of the license for managed products. Example: Activated, Expired, In grace period   |
| Product Type             | Displays the type of managed product the Activation Code provides. Example: Trial version, Full version |
| License Expiration       | Displays the date the license expires for the managed product.  |
| Seats                    | Displays the number of seats the Activation Code allows.  |

## Product License Status

Displays detailed information about the managed product and information about the Activation Code the managed product uses. Examples: managed product information, whether the Activation Code is active, the number of managed products the Activation Code activates

**TABLE B-85. Product License Status Data View**

| DATA               | DESCRIPTION   |
|--------------------|---|
| Product Entity     | Displays the entity display name for a managed product. Apex Central identifies managed products using the managed product's entity display name. |
| Product            | Displays the name of the managed product. Example: Apex One, ScanMail for Microsoft Exchange  |
| Product Version    | Displays the managed product's version number. Example: Apex One 2019, Apex Central 2019  |
| Service            | Displays the name of the managed product service. Example: Outbreak Protection Services   |
| License Status     | Displays the status of the license for managed products. Example: Activated, Expired, In grace period   |
| Activation Code    | Displays the Activation Code for managed products.  |
| Activation Codes   | Displays the number of Activation Codes a managed products uses.  |
| License Expiration | Displays the date the license expires for the managed product.  |

## Managed Product Information

Displays status, detailed, and summary information about managed products or managed product endpoints.

## Product Auditing Event Log

Provides information about managed product auditing events, such as managed product console access


**TABLE B-86. Product Auditing Event Log Data View**

| DATA              | DESCRIPTION  |
|-------------------|--|
| Received          | The date and time Apex Central received the data from the managed product  |
| Generated         | The date and time the managed product generated the data   |
| Host              | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server</li> <li>• The display name of the Security Agent endpoint</li> </ul> |
| User              | The logged on user name at the time of the event   |
| Event Category    | The type of event<br>Example: management console access  |
| Event Level       | The severity level of the event  |
| Event Description | A description of the event   |

## Product Distribution Summary

Displays summary information about managed products registered to Apex Central. Examples: managed product name, version number, and number of managed products

**TABLE B-87. Product Distribution Summary Data View**

| DATA                       | DESCRIPTION   |
|----------------------------|---|
| Registered to Apex Central | Displays the Apex Central server to which the managed product is registered.  |
| Product Category           | Displays the threat protection category for a managed product.<br>Example: Server-based products, Desktop (computers and mobile devices) products                 |
|                            | <hr/>  <b>Note</b><br>Desktop products includes mobile device solutions. <hr/> |

| DATA            | DESCRIPTION   |
|-----------------|---|
| Product         | Displays the name of the managed product. Example: Apex One, ScanMail for Microsoft Exchange  |
| Product Version | Displays the managed product's version number. Example: Apex One 2019, Apex Central 2019      |
| Product Role    | Displays the role the managed product has in the network environment. Example: server, client |
| Products        | Displays the total number of a specific managed product a network contains.                   |

## Product Event Information

Provides information about managed product events, such as managed products registering to Apex Central, component updates, and Activation Code deployments

**TABLE B-88. Product Event Information Data View**

| DATA            | DESCRIPTION  |
|-----------------|--|
| Received        | The date and time Apex Central received the data from the managed product                        |
| Generated       | The date and time the managed product generated the data   |
| Product Entity  | The display name of the managed product server in Apex Central                                   |
| Product         | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange |
| Product Version | The version of the managed product or service  |
| Event Severity  | The severity level of the event  |
| Event Type      | The type of event<br>Example: download virus found, file blocking, rollback                      |
| Command Status  | The status of the command<br>Example: successful, unsuccessful, in progress                      |



| DATA        | DESCRIPTION                |
|-------------|----------------------------|
| Description | A description of the event |

## Product Status Information

Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

**TABLE B-89. Product Status Information Data View**

| DATA                            | DESCRIPTION  |
|---------------------------------|--|
| Product Entity/<br>Endpoint     | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server in Apex Central</li> <li>• The name or IP address of the Security Agent endpoint</li> </ul> |
| Product Host/<br>Endpoint       | Depending on the related source: <ul style="list-style-type: none"> <li>• The display name of the managed product server</li> <li>• The display name of the Security Agent endpoint</li> </ul>                       |
| Product/Endpoint IP             | Depending on the related source: <ul style="list-style-type: none"> <li>• The IP address of the managed product server</li> <li>• The IP address of the Security Agent endpoint</li> </ul>                           |
| Product/Endpoint<br>MAC         | Depending on the related source: <ul style="list-style-type: none"> <li>• The MAC address of the managed product server</li> <li>• The MAC address of the Security Agent endpoint</li> </ul>                         |
| Managing Apex<br>Central Entity | The display name of the Apex Central server to which the managed product server reports  |
| Managing Server<br>Entity       | The display name of the managed product server in Apex Central to which the endpoint reports   |
| Domain                          | The domain to which the managed product belongs  |

| DATA                             | DESCRIPTION  |
|----------------------------------|--|
| Connection Status                | Depending on the related source: <ul style="list-style-type: none"> <li>• The status of the managed product server connection to Apex Central (Example: Normal, Abnormal, Offline)</li> <li>• The status of the Security Agent endpoint connection to the managed product server (Example: Normal, Abnormal, Offline)</li> </ul> |
| Data Protection Status           | The Data Loss Prevention status of the Security Agent<br>Example: Installed, Not installed   |
| Pattern Status                   | The status of the pattern files/rules used by the managed product or Security Agent<br>Example: up-to-date, out-of-date  |
| Engine Status                    | The status of the scan engines used by the managed product or Security Agent<br>Example: up-to-date, out-of-date   |
| Product                          | The name of the managed product or service<br>Example: Apex One, ScanMail for Microsoft Exchange   |
| Product Version                  | The version of the managed product or service  |
| Endpoint Sensor Version          | The version of Endpoint Sensor   |
| Application Control Version      | The version of Application Control   |
| Vulnerability Protection Version | The version of Vulnerability Protection  |
| Product Build                    | The build number of the managed product  |
| Product Role                     | The role the managed product server or Security Agent endpoint has in the network environment. (for example, server)   |
| Operating System                 | The operating system on the managed product server or Security Agent endpoint  |

| <b>DATA</b>                       | <b>DESCRIPTION</b>   |
|-----------------------------------|--|
| OS Version                        | The version of the operating system on the managed product server or Security Agent endpoint             |
| OS Service Pack                   | The service pack number of the operating system on the managed product server or Security Agent endpoint |
| Update Agent                      | If the Security Agent is an Update Agent   |
| Last Scheduled Scan               | The date and time of the last Scheduled Scan   |
| Last Manual Scan                  | The date and time of the last Manual Scan  |
| Last Scan Now                     | The date and time of the last Scan Now action  |
| Real-time Scan                    | If Real-time Scan is enabled   |
| Firewall                          | If the firewall is enabled   |
| Pattern/Rule<br>Deployment Status | The deployment status of the pattern/rule  |
| Pattern/Rule<br>Deployment        | The date and time of the pattern/rule deployment   |
| Engine Deployment<br>Status       | The scan engine deployment status  |
| Engine Deployment                 | The date and time of the scan engine deployment  |
| Logon User                        | The down-level logon name (NetBIOS_Domain\User_Name) of the last user logged on to the managed endpoint  |
| Last Startup                      | The date and time the Security Agent last started running  |
| Offline Time                      | The date and time the Security Agent last went offline   |
| User Name                         | The logged on user name at the time of the event   |



# Appendix C

## Token Variables

This section describes token variables that Apex Central supports for customizing event notification messages.

Topics include:

- *Standard Token Variables on page C-2*
- *Advanced Threat Activity Token Variables on page C-2*
- *Attack Discovery Token Variables on page C-5*
- *C&C Callback Token Variables on page C-6*
- *Content Policy Violation Token Variables on page C-8*
- *Data Loss Prevention Token Variables on page C-9*
- *Known Threat Activity Token Variables on page C-11*
- *Network Access Control Token Variables on page C-14*
- *Web Access Policy Violation Token Variables on page C-14*

## Standard Token Variables

The following table describes token variables for customizing all event notification messages.



### Note

Some event notifications support additional token variables. For the complete list of supported token variables for a specific event notification, refer to the notification method information for the specific event notification.

| VARIABLE     | DESCRIPTION  |
|--------------|--|
| %cmserver%   | The Apex Central server name   |
| %computer%   | The name of the endpoint   |
| %entity%     | The display name of the managed product server in Apex Central                                 |
| %event%      | The event detected   |
| %pname%      | The name of the managed product  |
| %pver%       | The version of the managed product   |
| %time%       | The time (hh:mm) when the event occurred   |
| %vloginuser% | The logged on user name at the time of the event   |
| %act%        | The action taken by the managed product. Example: file cleaned, file deleted, file quarantined |



## Advanced Threat Activity Token Variables



### Note


For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

The following table describes token variables for customizing Advanced Threat Activity event notification messages.


| VARIABLE     | DESCRIPTION   |
|--------------|---|
| %hostIP%     | <p>Depending on the traffic direction, %hostIP% is IP address determined by Deep Discovery Inspector:</p> <ul style="list-style-type: none"> <li>• Outbound traffic (internal traffic going to an external network): %hostIP% is the IP address of the endpoint in the network (source)</li> <li>• Traffic within the network: %hostIP% is the IP address of the endpoint in the network</li> <li>• External traffic to an endpoint in a network: %hostIP% is the IP address of the endpoint in the network</li> <li>• Traffic outside the network: %hostIP% is the IP address of the endpoint outside the network</li> </ul>   |
| %group%      | The name of the subnetwork  |
| %START_TIME% | <p>The start date and time of the detection period</p> <hr/> <p> <b>Note</b><br/>The specified time period for the notification criteria determines the start and end times.</p> <hr/>   |
| %END_TIME%   | <p>The end date and time of the detection period</p> <p>The start and end times define the time range interval. When logs are received during a certain interval, Apex Central calculates those logs. If the alert criteria is met, Apex Central counts the logs. %START_TIME% is the start time of the interval and %END_TIME% is the end time of the interval. The length of the interval is determined by the period threshold in the alert settings.</p> <hr/> <p> <b>Note</b><br/>The specified time period for the notification criteria determines the start and end times.</p> <hr/> |

| VARIABLE     | DESCRIPTION   |
|--------------|---|
| %detections% | <p>The number of detections</p> <p>For example:</p> <p>Event: High risk Virtual Analyzer detections</p> <p>IP address: %hostIP%</p> <p>Host name: %computer%</p> <p>Group: %group%</p> <p>Time range: %START_TIME% - %END_TIME%</p> <p>Detections: %detections%</p> |

The following table describes token variables for customizing event notification messages for Behavior Monitoring violations and Predictive Machine Learning detections.

| VARIABLE     | DESCRIPTION   |
|--------------|---|
| %hostIP%     | <p>Depending on the traffic direction, %hostIP% is IP address determined by Deep Discovery Inspector:</p> <ul style="list-style-type: none"> <li>• Outbound traffic (internal traffic going to an external network): %hostIP% is the IP address of the endpoint in the network (source)</li> <li>• Traffic within the network: %hostIP% is the IP address of the endpoint in the network</li> <li>• External traffic to an endpoint in a network: %hostIP% is the IP address of the endpoint in the network</li> <li>• Traffic outside the network: %hostIP% is the IP address of the endpoint outside the network</li> </ul> |
| %START_TIME% | <p>The start date and time of the detection period</p> <hr/> <p> <b>Note</b><br/>The specified time period for the notification criteria determines the start and end times.</p> <hr/>   |



| VARIABLE     | DESCRIPTION   |
|--------------|---|
| %END_TIME%   | <p>The end date and time of the detection period</p> <p>The start and end times define the time range interval. When logs are received during a certain interval, Apex Central calculates those logs. If the alert criteria is met, Apex Central counts the logs. %START_TIME% is the start time of the interval and %END_TIME% is the end time of the interval. The length of the interval is determined by the period threshold in the alert settings.</p> <hr/> <p> <b>Note</b><br/>The specified time period for the notification criteria determines the start and end times.</p> |
| %detections% | <p>The number of detections</p> <p>For example:</p> <p>Event: High risk Virtual Analyzer detections<br/>IP address: %hostIP%<br/>Host name: %computer%<br/>Group: %group%<br/>Time range: %START_TIME% - %END_TIME%<br/>Detections: %detections%</p>  |
| %domain%     | The root domain of the target in the Apex One domain hierarchy  |
| %hierarchy%  | The full path of the target in the Apex One domain hierarchy  |
| %BM_policy%  | The Behavior Monitoring policy ID   |
| %risklevel%  | The risk level of the event   |
| %target%     | The target of the event   |

## Attack Discovery Token Variables

The following table describes token variables for customizing Attack Discovery event notification messages.

| <b>VARIABLE</b>                 | <b>DESCRIPTION</b>  |
|---------------------------------|---|
| %cserver%                       | The Apex Central server name  |
| %computer%                      | The name of the endpoint  |
| %entity%                        | The display name of the managed product server in Apex Central                                      |
| %event%                         | The event detected  |
| %pname%                         | The name of the managed product   |
| %pver%                          | The version of the managed product  |
| %time%                          | The time (hh:mm) when the event occurred  |
| %vloginuser%                    | The logged on user name at the time of the event  |
| %act%                           | The action taken by the managed product. Example: file cleaned, file deleted, file quarantined      |
| %actresult%                     | The result of the action taken by the managed product. Example: successful, further action required |
| %highrisk_detection%            | The number of high-risk detections for the specified period   |
| %highrisk_detection_endpoint%   | The number of endpoints with high-risk detections for the specified period                          |
| %mediumrisk_detection%          | The number of medium-risk detections for the specified period                                       |
| %mediumrisk_detection_endpoint% | The number of endpoints with medium-risk detections for the specified period                        |
| %start_time%                    | The start date and time of the detection period   |
| %end_time%                      | The end date and time of the detection period   |

## C&C Callback Token Variables

The following table describes token variables for customizing C&C Callback event notification messages.

**Note**

For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

| VARIABLE            | DESCRIPTION   |
|---------------------|---|
| %CnC_LIST_SRC%      | Name of the list that contains the callback address                                   |
| %CNC_PD_NAME%       | Product ID of the managed product server that sent the log                            |
| %CNC_PD_VERSION%    | Version of the managed product server that sent the log                               |
| %CNC_PD_NODE%       | Endpoint name of the managed product server that sent the log                         |
| %CNC_PD_IP%         | IP address of the managed product server that sent the log                            |
| %CNC_EVTTIME%       | Time the log was generated  |
| %CNC_AGENTNAME%     | Name of the Security Agent endpoint that detected the callback                        |
| %CNC_AGENTIP%       | IP address of the Security Agent endpoint that detected the callback                  |
| %CNC_AGENTDOMAIN%   | Apex One domain of the Security Agent endpoint that detected the callback             |
| %CNC_POLICY_RULE%   | Name or rule ID of the policy that detected the callback                              |
| %CNC_ACTION%        | Action result from the security log, personal firewall, NCIE log, or web security log |
| %CNC_EMAIL_SENDER%  | Email sender associated with the callback   |
| %CNC_EMAIL_SUBJECT% | Email subject associated with the callback  |
| %CNC_RISKLEVEL%     | Risk level of the malware groups associated with the C&C server                       |
| %CNC_DETECT_SOURCE% | The C&C list that defined the detection rule  |
| %CNC_CHANNEL%       | The type ID that indicates the destination format                                     |

| <b>VARIABLE</b>           | <b>DESCRIPTION</b>  |
|---------------------------|---|
| %CNC_URL%                 | The remote URL that the endpoint attempted to contact                             |
| %CNC_URL_CATEGOR<br>Y%    | The URL category of the site that the endpoint attempted to contact               |
| %CNC_IP_PORT%             | The C&C server IP address and port  |
| %CNC_EMAIL_REPT%          | Email recipient associated with the callback                                      |
| %CNC_FIRST_SEEN%          | The first known detection of the C&C server                                       |
| %CNC_LAST_SEEN%           | The last known detection of the C&C server  |
| %CNC_LOCATION%            | The country code of the C&C server  |
| %CNC_MALEWARE_FA<br>MILY% | The malware family associated with the C&C detection                              |
| %CNC_ATTACK_GROU<br>P%    | The C&C group lists   |
| %CNC_PROCESS_NAM<br>E%    | The process name associated with the C&C detection                                |
| %CALLBACK_ADDR%           | URL, IP address, or email address to which a compromised host attempts a callback |
| %COMPR_HOST%              | Affected host or email address  |
| %CALLBACK_NUM%            | Number of contacts made between callback addresses and compromised hosts          |
| %COMPR_HOST_NUM%          | Number of compromised hosts involved in the outbreak                              |
| %CALLBACK_ADDR_N<br>UM%   | Number of callback addresses involved in the outbreak                             |

## Content Policy Violation Token Variables

The following table describes token variables for customizing Content Policy Violation event notification messages.

**Note**

For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

| VARIABLE     | DESCRIPTION   |
|--------------|---|
| %subject%    | Subject header of the email notification                      |
| %sender%     | Sender's email address  |
| %recipient%  | Recipient's email address                                     |
| %filtername% | Name of the content filter rule/policy that has been violated |
| %filteract%  | Action applied by the filter                                  |
| %msgact%     | Action applied to the message                                 |

## Data Loss Prevention Token Variables


The following table describes token variables for customizing Data Loss Prevention event notification messages.

**Note**

For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

| VARIABLE                  | DESCRIPTION   |
|---------------------------|---|
| %DLP_INCIDENT_TOTAL_NUM%  | The total number of incidents triggered by directly managed users                 |
| %DLP_INCIDENT_HIGH_NUM%   | The total number of high severity incidents triggered by directly managed users   |
| %DLP_INCIDENT_MEDIUM_NUM% | The total number of medium severity incidents triggered by directly managed users |

| <b>VARIABLE</b>                 | <b>DESCRIPTION</b>  |
|---------------------------------|---|
| %DLP_INCIDENT_LOW_NUM%          | The total number of low severity incidents triggered by directly managed users          |
| %DLP_INCIDENT_INFO_NUM%         | The total number of informational incidents triggered by directly managed users         |
| %DLP_INCIDENT_UNDEFINED_NUM%    | The total number of undefined severity incidents triggered by directly managed users    |
| %DLP_INCIDENT_ALLTOTAL_NUM%     | The total number of incidents triggered by all managed users                            |
| %DLP_INCIDENT_ALLHIGH_NUM%      | The total number of high severity incidents triggered by all managed users              |
| %DLP_INCIDENT_ALLMED_NUM%       | The total number of medium severity incidents triggered by all managed users            |
| %DLP_INCIDENT_ALLLOW_NUM%       | The total number of low severity incidents triggered by all managed users               |
| %DLP_INCIDENT_ALLINFO_NUM%      | The total number of informational incidents triggered by all managed users              |
| %DLP_INCIDENT_ALLUNDEFINED_NUM% | The total number of undefined severity incidents triggered by all managed users         |
| %DLP_START_TIME%                | The start date and time for the reporting period  |
| %DLP_END_TIME%                  | The end date and time for the reporting period  |
| %webLink%                       | The link to view details of the incident information listed in the notification message |
| %INCIDENTID%                    | Incident ID number  |
| %SEVERITY%                      | Incident severity level   |

| VARIABLE               | DESCRIPTION   |
|------------------------|---|
| %POLICY%               | Apex Central policy name<br><br> <b>Note</b><br>For incidents triggering DLP policies created on the managed product console, the Apex Central policy name appears as <b>N/A</b> . |
| %ACCOUNT%              | User name   |
| %OLD_STATUS%           | Incident status before modification   |
| %NEW_STATUS%           | Incident status after modification  |
| %LATEST_COMMENT%       | The latest comments about the incident  |
| %DLP_VIOLATION_NUMBER% | The number of violations matching DLP policies  |
| %DLP_THRESHOLD%        | The number of violations that must be triggered to indicate a significant increase on policy violations   |
| %DLP_TEMPLATE%         | Template matching the significant incident increase   |
| %DLP_USER_NAME%        | The user name associated with the endpoint that triggered the DLP policy violation  |
| %DLP_SENDER%           | The sender of the message that triggered the DLP policy violation   |
| %DLP_CHANNEL%          | The channel of the incident that triggered the DLP policy violation   |
| %STATUS_CHANGE_TIME%   | Incident details updated  |

## Known Threat Activity Token Variables

The following table describes token variables for customizing Known Threat Activity or Outbreak Prevention Service event notification messages.

**Note**

For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

| VARIABLE    | DESCRIPTION  |
|-------------|--|
| %device_ip% | IP address of an infected endpoint   |
| %egnver%    | <ul style="list-style-type: none"> <li>• Scan engine version</li> <li>• Used by the alert event category as well as the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Mode started" notifications. For the notification types of the alert event category, this variable refers to the scan engine version currently installed on the managed product server.</li> <li>• For the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Mode started" notifications, this variable refers to the Outbreak Prevention Policy required.</li> </ul>      |
| %hierarchy% | <ul style="list-style-type: none"> <li>• The location of the endpoint within the Apex One domain hierarchy</li> <li>• Used by the alert event category</li> </ul>  |
| %ptnver%    | <ul style="list-style-type: none"> <li>• Virus pattern version</li> <li>• Used by the alert event category and the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Services started" notifications. For the notification types of the alert event category, this variable refers to the virus pattern version currently installed on the managed product server.</li> <li>• For the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Services started" notifications, this variable refers to the Outbreak Prevention Policy required.</li> </ul> |



| VARIABLE      | DESCRIPTION   |
|---------------|---|
| %scanmethod%  | <p>The scan method for specific virus actions. This token is only available for the following alerts:</p> <ul style="list-style-type: none"> <li>• Virus found-first action unsuccessful and second action unavailable</li> <li>• Virus found-first and second actions unsuccessful</li> <li>• Virus found-first action successful</li> <li>• Virus found-second action successful</li> </ul> |
| %threat_info% | <ul style="list-style-type: none"> <li>• Virus/malware threat information provided by outbreak prevention policies</li> <li>• Used by "Active Outbreak Prevention Policy received" and "Outbreak Prevention Services started"</li> </ul>  |
| %vcnt%        | <ul style="list-style-type: none"> <li>• Virus count.</li> <li>• Used by virus outbreak alert.</li> </ul>   |
| %vdest%       | <ul style="list-style-type: none"> <li>• Virus/malware destination.</li> <li>• Examples:<br/> Email detection: %vdest% is the intended recipient<br/> Host-based/Endpoint detection: %vdest% is the endpoint IP address or host name</li> <li>• Used by the alert event category</li> </ul>   |
| %vfile%       | Infected file name. Used by the alert event category.   |
| %vfilepath%   | Infected file directory. Used by the alert event category.  |
| %vname%       | Virus or malware name. Used by the alert event category.  |
| %vsrcc%       | <ul style="list-style-type: none"> <li>• Virus/malware origin or infection source.</li> <li>• For example, the message sender takes the value of %vsrcc% if an antivirus managed product detected a virus/malware in an email message.</li> <li>• Used by the alert event category as well as the network virus alert notification type.</li> </ul>   |

## Network Access Control Token Variables

The following table describes token variables for customizing Network Access Control event notification messages.



### Note

For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

| VARIABLE      | DESCRIPTION  |
|---------------|--|
| %action%      | Network VirusWall Enforcer action (pass, drop, or quarantine) taken on the network virus |
| %description% | Error description used by the potential vulnerability attack detected events             |

## Web Access Policy Violation Token Variables

The following table describes token variables for customizing Web Access Policy Violation event notification messages.



### Note

For the list of standard token variables supported by all event notifications, see [Standard Token Variables on page C-2](#).

| VARIABLE    | DESCRIPTION                             |
|-------------|---|
| %url%       | URL in question                         |
| %vdestip%   | IP address of the target URL            |
| %blockrule% | Name of the rule that has been violated |
| %blocktype% | Action applied to the URL               |

# Appendix D

## IPv6 Support

This appendix contains information on the extent of IPv6 support in Apex Central.

Topics include:

- *Apex Central Server Requirements on page D-2*
- *IPv6 Support Limitations on page D-2*
- *Configuring IPv6 Addresses on page D-2*
- *Screens That Display IP Addresses on page D-3*

## Apex Central Server Requirements

IPv6 support is automatically enabled after installing and enabling the IPv6 stack on the Apex Central server.



### Note

Trend Micro assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

## IPv6 Support Limitations

The following table lists the limitations for IPv6 support:

| ITEM                    | LIMITATION  |
|-------------------------|---|
| Dual IP stacks          | Apex Central only supports dual IP stacks. IPv6 support may not work properly if the IPv4 stack is removed.   |
| IPv4 loopback interface | The IPv4 loopback interface is required. To verify that the TCP/IP software is working properly, ping 127.0.0.1.  |
| IPv6 address format     | Apex Central does not support the % character for IPv6 server addresses.  |
| Apex Central reports    | The following static reports do not support IPv6 addresses: <ul style="list-style-type: none"> <li>• Policy violation report</li> <li>• Service violation report</li> </ul>   |
| Apex Central features   | The following features do not support IPv6 addresses: <ul style="list-style-type: none"> <li>• IP address ranges for advanced log queries</li> <li>• IPv6 address normalization for suspicious object logs</li> </ul> |

## Configuring IPv6 Addresses

The web console allows you to configure an IPv6 address. The following are some configuration guidelines.

- Apex Central accepts standard IPv6 address presentations.

For example:

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334
```

```
2001:db7:85a3:0:0:8a2e:370:7334
```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- Apex Central also accepts link-local IPv6 addresses, such as:

```
fe80::210:5aff:feaa:20a2
```



**WARNING!**

Exercise caution when specifying a link-local IPv6 address because even though Apex Central can accept the address, it might not work as expected under certain circumstances. For example, Apex Central cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- 
- When the IPv6 address is part of a URL, enclose the address in square brackets ([]).

## Screens That Display IP Addresses

IP addresses are shown on the following screens:

- **Product Directory**
- **Log Query Results**
- **Server Registration**
- **Dashboard Widgets**



# Appendix E

## MIB Files

This section discusses the management information base (MIB) files that Apex Central supports.

Topics include:

- *Using the Apex Central MIB File on page E-2*
- *Using the NVW Enforcer SNMPv2 MIB File on page E-2*

## Using the Apex Central MIB File

Download the Apex Central MIB file from the following link and use an application that supports SNMP protocol to extract and import the file.

[https://CM\\_IP:CM\\_Port/TVCSDownload/tools/ApexCentral\\_mib.zip](https://CM_IP:CM_Port/TVCSDownload/tools/ApexCentral_mib.zip)

## Using the NVW Enforcer SNMPv2 MIB File

Download the NVW Enforcer SNMPv2 MIB file from the following link and use an application that supports SNMP protocol to extract and import the file.

- [https://CM\\_IP:CM\\_Port/TVCSDownload/tools/nvw2\\_mib2.zip](https://CM_IP:CM_Port/TVCSDownload/tools/nvw2_mib2.zip)



# Appendix F

## Syslog Content Mapping - CEF

The following tables map syslog content between Apex Central log output and CEF syslog types.

Topics include:

- *CEF Attack Discovery Detection Logs on page F-3*
- *CEF Behavior Monitoring Logs on page F-9*
- *CEF C&C Callback Logs on page F-15*
- *CEF Content Security Logs on page F-20*
- *CEF Data Loss Prevention Logs on page F-28*
- *CEF Device Access Control Logs on page F-36*
- *CEF Endpoint Application Control Logs on page F-43*
- *CEF Engine Update Status Logs on page F-46*
- *CEF Intrusion Prevention Logs on page F-48*
- *CEF Managed Product Logon/Logoff Events on page F-51*
- *CEF Network Content Inspection Logs on page F-52*
- *CEF Pattern Update Status Logs on page F-56*
- *CEF Predictive Machine Learning Logs on page F-59*

- *CEF Product Auditing Events on page F-64*
- *CEF Sandbox Detection Logs on page F-65*
- *CEF Spyware/Grayware Logs on page F-69*
- *CEF Suspicious File Logs on page F-77*
- *CEF Virus/Malware Logs on page F-81*
- *CEF Web Security Logs on page F-86*

## CEF Attack Discovery Detection Logs



### Note

If one Attack Discovery detection log relates to more than 4 objects, Apex Central only forwards the first 4 objects.

| CEF KEY            | DESCRIPTION                             | VALUE   |
|--------------------|---|---|
| Header (logVer)    | CEF format version                      | CEF:0   |
| Header (vendor)    | Appliance vendor                        | Trend Micro                                     |
| Header (pname)     | Appliance product                       | Apex Central                                    |
| Header (pver)      | Appliance version                       | 2019  |
| Header (eventid)   | Event ID                                | 700220  |
| Header (eventName) | Log name                                | Attack Discovery Detections                     |
| Header (severity)  | Severity                                | 3   |
| deviceExternalId   | ID                                      | Example: "38"                                   |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT +00:00"      |
| dhost              | Endpoint host name                      | Example: "ApexOneClient01"                      |
| dst                | Client IPv4 address                     | Example: "10.0.8.20"                            |
| C6a3               | Client IPv6 address                     | Example: "fd96:7521:9502:6:b5b0:b2b5:4173:3f5d" |
| duser              | User name                               | Example: "Admin004"                             |
| customerExternalID | Instance ID                             | Example: "8c1e2d8f-a03b-47ea-aef8-5aeab99ea697" |
| cn1Label           | Corresponding label for the "cn1" field | "SLF_RiskLevel"                                 |

| CEF KEY  | DESCRIPTION                             | VALUE  |
|----------|---|--|
| cn1      | Risk Level                              | Example: "0" <ul style="list-style-type: none"><li>• 0: Unknown</li><li>• 100: Low risk</li><li>• 500: Medium risk</li><li>• 1000: High risk</li></ul> |
| cn2Label | Corresponding label for the "cn2" field | "SLF_PatternNumber"  |
| cn2      | Pattern Number                          | Example: "30.1012.00"  |
| cs1Label | Corresponding label for the "cs1" field | "SLF_RuleID"   |
| cs1      | Rule ID                                 | Example: "powershell invoke expression"  |
| cat      | Category ID                             | Example: "point of entry"  |
| cs2Label | Corresponding label for the "cs2" field | "SLF_ADEObjectGroup_Info_1"  |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cs2      | Attack Discovery object information     | <p>Example:</p> <pre> process - powershell.exe - {   "META_FILE_MD5" :     "9393f60b1739074eb17c5f4ddd     efe239",   "META_FILE_NAME" :     "powershell.exe",   "META_FILE_SHA1" :     "887ce4a295c163791b60fc23d2     85e6d84f28ee4c",   "META_FILE_SHA2" :     "de96a6e50044335375dc1ac238     336066889d9ffc7d73628ef4fe     1b1b160ab32c",   "META_PATH" :     "c:\\windows\\system32\\wi     ndowspowershell\\v1.0\\",   "META_PROCESS_CMD" :     [ "powershell cmd " ],   "META_PROCESS_PID" : 7132,   "META_SIGNER" :     "microsoft windows",   "META_SIGNER_VALIDATION" :     true,   "META_USER_USER_NAME" :     "Administrator",   "META_USER_USER_SERVERNAME" :     "Host",   "OID" : 1 } </pre> |
| cs3Label | Corresponding label for the "cs3" field | "SLF_ADEObjectGroup_Info_2"   |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cs3      | Attack Discovery object information     | <p>Example:</p> <pre> process - powershell.exe - {   "META_FILE_MD5" :     "9393f60b1739074eb17c5f4ddd     efe239",   "META_FILE_NAME" :     "powershell.exe",   "META_FILE_SHA1" :     "887ce4a295c163791b60fc23d2     85e6d84f28ee4c",   "META_FILE_SHA2" :     "de96a6e50044335375dc1ac238     336066889d9ffc7d73628ef4fe     1b1b160ab32c",   "META_PATH" :     "c:\\windows\\system32\\wi     ndowspowershell\\v1.0\\",   "META_PROCESS_CMD" :     [ "powershell cmd " ],   "META_PROCESS_PID" : 7132,   "META_SIGNER" :     "microsoft windows",   "META_SIGNER_VALIDATION" :     true,   "META_USER_USER_NAME" :     "Administrator",   "META_USER_USER_SERVERNAME" :     "Host",   "OID" : 1 } </pre> |
| cs4Label | Corresponding label for the "cs4" field | "SLF_ADEObjectGroup_Info_3"   |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cs4      | Attack Discovery object information     | <p>Example:</p> <pre> process - powershell.exe - {   "META_FILE_MD5" :     "9393f60b1739074eb17c5f4ddd     efe239",   "META_FILE_NAME" :     "powershell.exe",   "META_FILE_SHA1" :     "887ce4a295c163791b60fc23d2     85e6d84f28ee4c",   "META_FILE_SHA2" :     "de96a6e50044335375dc1ac238     336066889d9ffc7d73628ef4fe     1b1b160ab32c",   "META_PATH" :     "c:\\windows\\system32\\wi     ndowspowershell\\v1.0\\",   "META_PROCESS_CMD" :     [ "powershell cmd " ],   "META_PROCESS_PID" : 7132,   "META_SIGNER" :     "microsoft windows",   "META_SIGNER_VALIDATION" :     true,   "META_USER_USER_NAME" :     "Administrator",   "META_USER_USER_SERVERNAME" :     "Host",   "OID" : 1 } </pre> |
| cs5Label | Corresponding label for the "cs5" field | "SLF_ADEObjectGroup_Info_4"   |

| CEF KEY             | DESCRIPTION                                | VALUE   |
|---------------------|--|---|
| cs5                 | Attack Discovery object information        | Example:<br><br><pre> process - powershell.exe - {   "META_FILE_MD5" :     "9393f60b1739074eb17c5f4ddd     efe239",   "META_FILE_NAME" :     "powershell.exe",   "META_FILE_SHA1" :     "887ce4a295c163791b60fc23d2     85e6d84f28ee4c",   "META_FILE_SHA2" :     "de96a6e50044335375dc1ac238     336066889d9ffc7d73628ef4fe     1b1b160ab32c",   "META_PATH" :     "c:\\windows\\system32\\wi     ndowspowershell\\v1.0\\",   "META_PROCESS_CMD" :     [ "powershell cmd " ],   "META_PROCESS_PID" : 7132,   "META_SIGNER" :     "microsoft windows",   "META_SIGNER_VALIDATION" :     true,   "META_USER_USER_NAME" :     "Administrator",   "META_USER_USER_SERVERNAME" :     "Host",   "OID" : 1 }           </pre> |
| deviceNtDomain      | Active Directory domain                    | Example: APEXTMCM   |
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1  |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName  |



| CEF KEY           | DESCRIPTION                             | VALUE  |
|-------------------|---|--|
| TMCMLogDetectedIP | IP address where the log event occurred | Example: 10.1.2.3                                  |
| ApexCentralHost   | Apex Central host name                  | Example: TW-CHRIS-W2019                            |
| devicePayloadId   | Unique message GUID                     | Example: 1C00290C0360-9CDE11EB-D4B8-F51F-C697      |
| TCMdevicePlatform | Endpoint operating system               | Example: Windows 7 6.1 (Build 7601) Service Pack 1 |

Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|700211|Attack Discovery
Detections|3|deviceExternalId=5 rt=Jan 17 2019 03:38:06 GMT+
00:00 dhost=VCAC-Winow-331 dst=10.201.86.150 customerExtern
alID=8c1e2d8f-a03b-47ea-aef8-5aeab99ea697 cn1Label=SLF_RiskL
evel cn1=0 cn2Label=SLF_PatternNumber cn2=30.1012.00 cs1Labe
l=SLF_RuleID cs1=powershell invoke expression cat=point of e
ntry cs2Label=SLF_ADEObjectGroup_Info_1 cs2=process - code9.
exe - {USER: administrator09} deviceNtDomain=APEXTMCM dntdom
=OSCEDomain1 TMCMLogDetectedHost=VCAC-Winow-331 TMCMLogDete
ctedIP=10.201.86.150 ApexCentralHost=TW-CHRIS-W2019devicePay
loadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TCMdevicePlatfo
rm=Windows 7 6.1 (Build 7601) Service Pack 1
```

## CEF Behavior Monitoring Logs

| CEF KEY         | DESCRIPTION        | VALUE        |
|-----------------|--------------------|--------------|
| Header (logVer) | CEF format version | CEF:0        |
| Header (vendor) | Product vendor     | Trend Micro  |
| Header (pname)  | Product name       | Apex Central |
| Header (pver)   | Product version    | 2019         |

| <b>CEF KEY</b>     | <b>DESCRIPTION</b>                      | <b>VALUE</b>                              |
|--------------------|---|---|
| Header (eventid)   | Behavior Monitoring policy ID           | BM:1000                                   |
| Header (eventName) | Log name                                | Behavior Monitoring                       |
| Header (severity)  | Severity                                | 3   |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00" |
| dvchost            | Host name                               | Example: "localhost"                      |
| cs2Label           | Corresponding label for the "cs2" field | "Policy"                                  |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cs2      | Policy type                             | <ul style="list-style-type: none"> <li>• Compromised executable file</li> <li>• New startup program</li> <li>• Host file modification</li> <li>• Program library injection</li> <li>• New Internet Explorer plugin</li> <li>• Internet Explorer setting modification</li> <li>• Shell modification</li> <li>• New service</li> <li>• Security policy modification</li> <li>• Firewall policy modification</li> <li>• System file modification</li> <li>• Duplicated system file</li> <li>• Layered service provider</li> <li>• System process modification</li> <li>• Suspicious behavior</li> <li>• Newly encountered programs</li> <li>• Unauthorized file encryption</li> <li>• Threat behavior analysis</li> <li>• User-defined policy</li> </ul> |
| sproc    | Target of the event                     | Example: "C:\\Windows\\SysWOW64\\rundll32.exe"  |
| cs3Label | Corresponding label for the "cs3" field | "Event_Type"  |

| CEF KEY  | DESCRIPTION  | VALUE  |
|----------|--|--|
| cs3      | Event type   | <ul style="list-style-type: none"><li>• Process</li><li>• Process image</li><li>• Registry</li><li>• File system</li><li>• Driver</li><li>• SDT</li><li>• System API</li><li>• User Mode</li><li>• Exploit</li><li>• All</li></ul>   |
| cs4Label | Corresponding label for the “cs4” field                  | “Operation”  |
| cs4      | The operation to be performed by the target of the event | <ul style="list-style-type: none"><li>• Create Process</li><li>• Open</li><li>• Terminate</li><li>• Delete</li><li>• Write</li><li>• Access</li><li>• Create File</li><li>• Close</li><li>• Execute</li><li>• Invoke</li><li>• Exploit</li><li>• Unhandled Operation</li></ul> |
| cs5Label | Corresponding label for the “cs5” field                  | “Risk_Level”   |

| CEF KEY       | DESCRIPTION       | VALUE  |
|---------------|-------------------|--|
| cs5           | Risk level        | Example: "1"<br><ul style="list-style-type: none"> <li>• 0: Low</li> <li>• 1: High</li> </ul>  |
| TMCMLogTarget | Target host       | Example: "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\COM+"   |
| act           | Translated action | <ul style="list-style-type: none"> <li>• Allow</li> <li>• Ask</li> <li>• Deny</li> <li>• Terminate</li> <li>• Read Only</li> <li>• Read/Write Only</li> <li>• Read/Execute Only</li> <li>• Feedback</li> <li>• Clean</li> <li>• Unknown</li> <li>• Assess</li> <li>• Terminated. Files were recovered.</li> <li>• Terminated. Some files were not recovered.</li> <li>• Terminated. Files were not recovered.</li> <li>• Terminated. Restart result: Files were recovered.</li> <li>• Terminated: Restart result: Some files were not recovered.</li> <li>• Terminated: Restart result: Files were not recovered.</li> </ul> |

| CEF KEY             | DESCRIPTION                                | VALUE  |
|---------------------|--|--|
| shost               | Source host (endpoint)                     | Example: "shost1"  |
| src                 | Source host IP address                     | Example: "10.0.147.105"  |
| deviceFacility      | Product                                    | Example: "Apex One"  |
| reason              | Critical threat type                       | Example: "E" <ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| deviceNtDomain      | Active Directory domain                    | Example: APEXTMCM  |
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1   |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName   |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3  |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019  |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMdevicePlatform  | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1   |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|BM:1000|Behavior Monitoring|3|rt=Sep 20 2019 01:02:03 GMT+00:00 dvchost=localhost cs
```

```
5Label=Risk_Level cs5=1 cs2Label=Policy cs2=Threat Behavior
Analysis sproc=subject cs3Label=Event_Type cs3=File system
TMCMLogTarget=HKCU\\Software\\Microsoft\\Windows\\CurrentVer
sion\\Run\\COM+ act=Ask cs4Label=Operation cs4=Create Proces
s shost=shost1 src=10.0.76.40 deviceFacility=Apex One reason
=G deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDetecte
dHost=shost1 TMCMLogDetectedIP=10.0.76.40 ApexCentralHost=TW
-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F
-C697 TMCMLogDevicePlatform=Windows 7 6.1 (Build 7601) Service
Pack 1
```

## CEF C&C Callback Logs

| CEF KEY            | DESCRIPTION                             | VALUE                        |
|--------------------|---|------------------------------|
| Header (logVer)    | CEF format version                      | CEF:0                        |
| Header (vendor)    | Appliance vendor                        | Trend Micro                  |
| Header (pname)     | Appliance product                       | Apex Central                 |
| Header (pver)      | Appliance version                       | 2019                         |
| Header (eventid)   | CnC:Action                              | CnC:Block                    |
| Header (eventName) | Name                                    | CnC Callback                 |
| Header (severity)  | Severity                                | 3                            |
| deviceExternalId   | ID                                      | Example: "12"                |
| cat                | Log type                                | Example: "1756"              |
| deviceFacility     | Product                                 | Example: "Apex One"          |
| cs2Label           | Corresponding label for the "cs2" field | Example: "El_ProductVersion" |
| cs2                | Product version                         | Example: "11.0"              |

| CEF KEY   | DESCRIPTION                              | VALUE  |
|-----------|--|--|
| rt        | Event trigger time in UTC                | Example: "Mar 22 2018 08:23:23 GMT+00:00"  |
| shost     | Endpoint host name                       | Example: "ApexOneClient01"   |
| src       | Endpoint IPv4 address                    | Example: "10.201.86.187"   |
| c6a2Label | Corresponding label for the "c6a2" field | Example: "SLF_ClientIP"  |
| c6a2      | Endpoint IPv6 address                    | Example:<br>"2620:101:4003:7a0:fd4b:52ed:53bd:ae3d"  |
| cs3Label  | Corresponding label for the "cs3" field  | Example: "SLF_DomainName"  |
| cs3       | Domain name                              | Example: "DOMAIN1"   |
| cs4Label  | Corresponding label for the "cs4" field  | Example: "SLF_PolicyName"  |
| cs4       | Policy name                              | Example: "C&C Server URL in Web Reputation Services database - HTTP (Request)"   |
| act       | Action                                   | Example: "Block" <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Pass</li> <li>• 2: Block</li> <li>• 3: Monitor</li> <li>• 4: Delete</li> <li>• 5: Quarantine</li> <li>• 6: Warn</li> <li>• 7: Warn and continue</li> <li>• 8: Override</li> </ul> |



| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cn1Label | Corresponding label for the “cn1” field | Example: “SLF_CCCA_RiskLevel”   |
| cn1      | C&C risk level                          | Example: “1” <ul style="list-style-type: none"> <li>• 0: SLF_CCCA_RISKLEVEL_UNKNOWN</li> <li>• 1: SLF_CCCA_RISKLEVEL_LOW</li> <li>• 2: SLF_CCCA_RISKLEVEL_MEDIUM</li> <li>• 3: SLF_CCCA_RISKLEVEL_HIGH</li> </ul> |
| cn2Label | Corresponding label for the “cn2” field | Example: “SLF_CCCA_DetectionSource”   |
| cn2      | C&C list source                         | Example: “1” <ul style="list-style-type: none"> <li>• 0: SLF_CCCA_GLOBAL_LIST</li> <li>• 1: SLF_CCCA_CUSTOM_LIST</li> <li>• 2: SLF_CCCA_CUSTOM_LIST_USER_DEFINED</li> </ul>                                       |
| cn3Label | Corresponding label for the “cn3” field | Example: “SLF_CCCA_DetectionFormat”   |
| cn3      | Callback address format                 | Example: “1” <ul style="list-style-type: none"> <li>• 0: IP</li> <li>• 1: IP</li> <li>• 2: HTTP</li> <li>• 3: SMTP</li> </ul>   |
| request  | URL                                     | Example: “http://CC13.jojo.com”   |

| CEF KEY                | DESCRIPTION  | VALUE  |
|------------------------|--|--|
| deviceCustomDate1Label | Corresponding label for the "deviceCustomDate1" field      | Example: "SLF_FirstSeen"   |
| deviceCustomDate1      | The UTC time when the callback attempt was first monitored | Example: "Oct 10 2017 16:58:03 GMT+00:00"                        |
| deviceCustomDate2Label | Corresponding label for the "deviceCustomDate2" field      | Example: "SLF_LastSeen"  |
| deviceCustomDate2      | The UTC time when the callback attempt was last monitored  | Example: "Oct 11 2017 10:58:03 GMT+00:00"                        |
| cs5Label               | Corresponding label for the "cs5" field                    | Example: "CnCDestination"  |
| cs5                    | Callback URL address                                       | Example: "http://CC13.jojo.com"                                  |
| dst                    | Callback IPv4 address                                      | Example: "10.201.86.195"   |
| c6a3Label              | Corresponding label for the "c6a3" field                   | Example: "CnCDestination"  |
| c6a3                   | Callback IPv6 address                                      | Example:<br>"fe80::38ca:cd15:443c:40bb%11"                       |
| deviceProcessName      | Process name   | Example: "C:\Program Files (x86)\Internet Explorer\iexplore.exe" |
| dvchost                | Host name  | Example: "localhost"   |
| deviceNtDomain         | Active Directory domain                                    | Example: APEXTMCM  |
| dntdom                 | Apex One domain hierarchy                                  | Example: OSCEDomain1   |
| TMCMLogDetectedHost    | Endpoint name where the log event occurred                 | Example: MachineHostName   |
| TMCMLogDetectedIP      | IP address where the log event occurred                    | Example: 10.1.2.3  |
| ApexCentralHost        | Apex Central host name                                     | Example: TW-CHRIS-W2019  |

| CEF KEY           | DESCRIPTION               | VALUE   |
|-------------------|---------------------------|---|
| devicePayloadId   | Unique message GUID       | Example:<br>1C00290C0360-9CDE11EB-D4B8-<br>F51F-C697  |
| deviceDirection   | Network traffic direction | Example: 0<br><br>The meaning of the value varies depending on the “cat” field value.<br><br>If the “cat” field value is 1756, 1707, or 1733: <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Inbound</li> <li>• 2: Outbound</li> </ul> If the “cat” field value is 1739, 1741, or 1723: <ul style="list-style-type: none"> <li>• 0: Outbound</li> <li>• 1: Inbound</li> <li>• 2: Unknown</li> </ul> If the “cat” field value is 1705, 1735, or 1775: <ul style="list-style-type: none"> <li>• -1: Unknown</li> <li>• 0: Outbound email</li> <li>• 1: Inbound email</li> <li>• 2: Internal email</li> </ul> |
| TMCdevicePlatform | Endpoint operating system | Example: Windows 7 6.1 (Build 7601) Service Pack 1  |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|CnC:Block|CnC Callback
|3|deviceExternalId=12 rt=Oct 11 2017 06:34:09 GMT+00:00 cat
=1756 deviceFacility=Apex One cs2Label=EI_ProductVersion cs2
```

```
=11.0 shost=ApexOneClient01 src=10.201.86.187 cs3Label=SLF_D
omainName cs3=DOMAIN act=Block cn1Label=SLF_CCCA_RiskLevel c
n1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1 cn3Label=SLF_CC
CA_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessNa
me=C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe
deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 dvchost=localhost
TMCMLogDetectedHost=ApexOneClient01 TMCMLogDetectedIP=10.201
.86.187 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C002
90C0360-9CDE11EB-D4B8-F51F-C697 deviceDirection=0 TMCMdevice
Platform=Windows 7 6.1 (Build 7601) Service Pack 1
```

## CEF Content Security Logs

| CEF KEY            | DESCRIPTION               | VALUE   |
|--------------------|---------------------------|---|
| Header (logVer)    | CEF format version        | CEF:0   |
| Header (vendor)    | Appliance vendor          | Trend Micro   |
| Header (pname)     | Appliance product         | Apex Central  |
| Header (pver)      | Appliance product version | 2019  |
| Header (eventid)   | MS: Filter action         | MS:Clean  |
| Header (eventName) | Policy name               | Policy  |
| Header (severity)  | Severity                  | 3   |
| cnt                | Number of detections      | Example: 10   |
| dhost              | List of all recipients    | Example:<br>employee_a1@Acompany.com;e<br>mployee_a2@Acompany.com |
| duser              | One of the recipients     | Example:<br>employee_a1@Acompany.com                              |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| act      | Filter action                           | Example: "Clean"<br><br>For more information, see <a href="#">Filter Action Mapping Table on page F-25</a> .  |
| cs1Label | Corresponding label for the "cs1" field | Example: "Policy_Settings"  |
| cs1      | Policy settings                         | Example: "Default_policy"   |
| cs2Label | Corresponding label for the "cs2" field | Example: "Product_Version"  |
| cs2      | Product version                         | Example: "11"   |
| cs3Label | Corresponding label for the "cs3" field | Example: "Filter_Type"  |
| cs3      | Filter type                             | Example: "URL reputation filter"<br><br><ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: ContentFilter</li> <li>• 2: AttachmentFilter</li> <li>• 3: StandardFilter</li> <li>• 4: SizeFilter</li> <li>• 5: DisclaimerMgr</li> <li>• 6: SpamFilter</li> <li>• 7: OPP</li> <li>• 8: ImportFilter</li> <li>• 9: PhishingFilter</li> <li>• 10: UrlReputationFilter</li> </ul> |
| cs4Label | Corresponding label for the "cs4" field | Example: "CLF_ReasonCode"   |
| cs4      | Reason Code                             | Example: "access"   |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cs5Label | Corresponding label for the “cs5” field | Example:<br>“CLF_ReasonCodeSource”  |
| cs5      | Reason code source                      | Example: “web”  |
| cs6Label | Corresponding label for the “cs6” field | Example: “Action_on_Message”  |
| cs6      | Action                                  | Example: “3” <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: N/A</li> <li>• 2: Deliver</li> <li>• 3: Delete</li> <li>• 4: Quarantine</li> <li>• 5: Postpone</li> <li>• 6: Forward</li> <li>• 7: Replace</li> <li>• 8: Archive</li> <li>• 100: Strip</li> <li>• 101: Pass</li> </ul> |
| cat      | Log type                                | Example: “1705”   |
| dvchost  | Endpoint host name                      | Example: “ApexOneClient01”  |
| rt       | Event trigger time in UTC               | Example: “Mar 22 2018 08:23:23 GMT+00:00”   |
| cn1Label | Corresponding label for the “cn1” field | Example: “Severity”   |

| CEF KEY          | DESCRIPTION                             | VALUE  |
|------------------|---|--|
| cn1              | Severity code                           | Example: "2" <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Information</li> <li>• 2: Warning</li> <li>• 3: Error</li> <li>• 4: Critical</li> </ul> |
| TMCMLogSeverity  | Description of severity                 | Second scan engine   |
| cn2Label         | Corresponding label for the "cn2" field | Filter_Action_Result   |
| cn2              | Filter action result                    | Example: 21<br>For more information, see <a href="#">Filter Action Result Mapping Table on page F-26</a> .   |
| deviceExternalId | ID                                      | Example: "5"   |
| fname            | File                                    | Example: "RERERW~42w.exe"  |
| msg              | Subject                                 | Example: "Open this email to win a free phone"   |
| shost            | List of all senders/users in violation  | Example: "bear" <bear@abc.mail.com>;"yumi" <yumi@abc.mail.com>   |
| suser            | One of the senders/users in violation   | Example: "bear" <bear@abc.mail.com>  |
| deviceFacility   | Product                                 | Example: "Deep Discovery Email Inspector"  |
| src              | Email sender IP address                 | Example: "10.206.155.122"  |
| filepath         | Suspicious file location                | Example: "https://ca91-1.testurl.com:443"  |

| CEF KEY           | DESCRIPTION               | VALUE  |
|-------------------|---------------------------|--|
| request           | Suspicious URL            | Example: "https://ca91-1.testurl.com:443"  |
| reason            | Critical threat type      | Example: "E" <ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| ApexCentralHost   | Apex Central host name    | Example: TW-CHRIS-W2019  |
| devicePayloadId   | Unique message GUID       | Example: 1C00290C0360-9CDE11EB-D4B8-F51F-C697  |
| TMCdevicePlatform | Endpoint operating system | Example: Windows 7 6.1 (Build 7601) Service Pack 1   |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|MS:Clean|This is a policy
name|3|deviceExternalId=90045 rt=Sep 17 2018 01:27:42 GMT+00
:00 dhost=user@test.com duser=user@test.com act=Clean cs1Label
=Policy_Settings cs1=This is policy content cs2Label=CLF_Produ
ctVersion cs2=3.2 cs3Label=Filter_Type cs3=URL reputation filt
er cs5Label=CLF_ReasonCodeSource cs5=20 cs6Label=Action_on_Mes
sage cs6=0 cat=1705 dvchost=ApexOneClient01 cn1Label=Severity
cn1=2 TMCMLogSeverity=Second scan engine fname=NE_AEP.1550
msg=plain_qp_no8_av1u_NE_AEP.1550 shost=user2@test.com suser=
user2@test.com cn2Label=Filter_Action_Result cn2=21 deviceFaci
lity=Deep Discovery Email Inspector src=10.206.155.122 reason=
```



```
B,G ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C036
0-9CDE11EB-D4B8-F51F-C697 TCMdevicePlatform=Windows 7 6.1 (B
uild 7601) Service Pack 1
```

## Filter Action Mapping Table

| VALUE | DESCRIPTION                |
|-------|----------------------------|
| 0     | Unknown                    |
| 1     | N/A                        |
| 2     | Clean                      |
| 3     | Delete                     |
| 4     | Move                       |
| 5     | Rename                     |
| 6     | Pass/Log                   |
| 7     | Strip                      |
| 8     | Drop                       |
| 9     | Quarantine                 |
| 10    | Insert/Replace             |
| 11    | Archive                    |
| 12    | Stamp                      |
| 13    | Block                      |
| 14    | Redirect mail for approval |
| 81    | Encrypt                    |
| 90    | Detect                     |
| 257   | Reset                      |

## Filter Action Result Mapping Table

| VALUE | DESCRIPTION                       |
|-------|-----------------------------------|
| 0     | Unknown                           |
| 1     | N/A                               |
| 21    | File cleaned                      |
| 22    | File deleted                      |
| 23    | File quarantined                  |
| 24    | File renamed                      |
| 25    | File passed                       |
| 26    | Unable to clean file. Passed      |
| 27    | Unable to clean file. Deleted     |
| 28    | Unable to clean file. Renamed     |
| 29    | Unable to clean file. Quarantined |
| 30    | File stripped                     |
| 31    | Unable to clean file. Stripped    |
| 32    | File replaced                     |
| 33    | File dropped                      |
| 34    | File archived                     |
| 35    | File blocked successfully         |
| 36    | File quarantined successfully     |
| 37    | File stamped successfully         |
| 38    | File uploaded                     |
| 39    | Unable to clean file. Quarantined |
| 40    | Unable to clean file. Passed      |

| <b>VALUE</b> | <b>DESCRIPTION</b>                      |
|--------------|---|
| 41           | Access denied                           |
| 42           | No action                               |
| 43           | Reboot system successfully              |
| 44           | Spyware/Grayware unsafe to clean        |
| 45           | Stop scan manually successfully         |
| 46           | Redirect Mail for Approval successfully |
| 81           | Encrypted                               |
| 121          | Unable to clean file                    |
| 122          | Unable to delete file                   |
| 123          | Unable to quarantine file               |
| 124          | Unable to rename file                   |
| 125          | Unable to pass file                     |
| 126          | Unable to clean or pass file            |
| 127          | Unable to clean or delete file          |
| 128          | Unable to clean or rename file          |
| 129          | Unable to clean or quarantine file      |
| 130          | Unable to strip file                    |
| 131          | Unable to clean or strip file           |
| 132          | Unable to replace file                  |
| 133          | Unable to drop file                     |
| 134          | Unable to archive file                  |
| 135          | Unable to block file                    |
| 136          | Unable to quarantine file               |

| VALUE | DESCRIPTION   |
|-------|---|
| 137   | Unable to stamp file  |
| 138   | Unable to upload file   |
| 139   | Unable to clean or quarantine file  |
| 140   | Unable to clean or pass file  |
| 141   | Unable to deny access   |
| 142   | Unable to perform action  |
| 143   | Action required - Restart the endpoint to finish cleaning the security threat   |
| 145   | Unable to stop scan manually  |
| 146   | Unable to Redirect Mail for Approval  |
| 201   | Action required - Perform a full system scan  |
| 202   | Action required - Use the "Rescue Disk" tool in the Apex One ToolBox to remove this threat. If the problem persists, contact Support    |
| 203   | Action required - Use the "Rootkit Buster" tool in the Apex One ToolBox to remove this threat. If the problem persists, contact Support |
| 204   | Action required - Use the "Clean Boot" tool in the Apex One ToolBox to remove this threat. If the problem persists, contact Support     |

## CEF Data Loss Prevention Logs

| CEF KEY          | DESCRIPTION        | VALUE        |
|------------------|--------------------|--------------|
| Header (logVer)  | CEF format version | CEF:0        |
| Header (vendor)  | Appliance vendor   | Trend Micro  |
| Header (pname)   | Appliance product  | Apex Central |
| Header (pver)    | Appliance version  | 2019         |
| Header (eventid) | Event ID           | 700106       |

| CEF KEY            | DESCRIPTION                             | VALUE  |
|--------------------|---|--|
| Header (eventName) | Log name                                | Data Loss Prevention                                   |
| Header (severity)  | Severity                                | 3  |
| cs1Label           | Corresponding label for the "cs1" field | "Policy GUID"  |
| cs1                | Policy GUID                             | Example:<br>"FAF492CF-164C-4672-9A79-F1AB9CB288A3"     |
| cn1Label           | Corresponding label for the "cn1" field | "Product"  |
| cn1                | Product type value                      | Example: "15"  |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00"              |
| src                | Source host IP address                  | Example: "10.0.57.160"                                 |
| smac               | Source host MAC address                 | Example: "74-27-00-0C-65-E7"                           |
| shost              | Source host name                        | Example: "shost1"                                      |
| cs4Label           | Corresponding label for the "cs4" field | "Incident_Source_(AD_Account)"                         |
| cs4                | The user name in violation              | Example: "Trend"                                       |
| suser              | Email sender                            | Example:<br>"sender@example.com"                       |
| request            | The URL accessed                        | Example: "https://<br>example.com/api/content"         |
| duser              | Comma (,) separated list of recipients  | Example:<br>"user1@example.com;user2@exa<br>mple.com;" |
| msg                | Subject                                 | Example: "Sample,20171017"                             |

| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| filepath | File path                               | Example: "D:\\Windows Live Mail\\Storage Folders\\Imported Fo e52\\Local Folders\\Sent Items\\Archive Aft de1\\Clients,Adv 22b\\" |
| fname    | Trigger file name                       | Example: "2B43363A-000000A4.eml"  |
| fsize    | File size in bytes                      | Example: "3"  |
| cs5Label | Corresponding label for the "cs5" field | "Rule"  |
| cs5      | Rule name                               | Example: "SAMPLE RULE SET"  |
| cs6Label | Corresponding label for the "cs6" field | "Template"  |
| cs6      | Template name                           | Example: "Apex One policy"  |
| cn3Label | Corresponding label for the "cn3" field | "Channel"   |
| cn3      | Channel type                            | Example: "3"<br><br>For more information, see <a href="#">Channel Mapping Table on page F-34</a> .                                |
| cn2Label | Corresponding label for the "cn2" field | "Action"  |
| cn2      | Action result                           | Example: "4"<br><br>For more information, see <a href="#">Action Result Mapping Table on page F-32</a> .                          |
| cs2Label | Corresponding label for the "cs2" field | "Policy"  |
| cs2      | Policy name                             | Example: "OfficeScan"   |

| CEF KEY             | DESCRIPTION   | VALUE   |
|---------------------|---|---|
| cs3Label            | Corresponding label for the “cs3” field               | “Product_Entity/Endpoint”   |
| cs3                 | Endpoint host name                                    | Example: “Sample_Host”  |
| dvchost             | Server host name                                      | Example: “localhost”  |
| deviceFacility      | Product name  | Example: “Apex One”   |
| deviceNtDomain      | Active Directory domain                               | Example: APEXTMCM   |
| dntdom              | Apex One domain hierarchy                             | Example: OSCEDomain1  |
| externalId          | Log ID of the event                                   | Example: “101”  |
| cfp1Label           | Corresponding label for the “cfp1Label” field         | “ForensicFileAvailable”   |
| cfp1                | Indicates whether the forensic file can be downloaded | <ul style="list-style-type: none"> <li>• 0: The file cannot be downloaded</li> <li>• 1: The file can be downloaded</li> </ul> |
| TMCMLogDetectedHost | Endpoint name where the log event occurred            | Example: MachineHostName  |
| TMCMLogDetectedIP   | IP address where the log event occurred               | Example: 10.1.2.3   |
| ApexCentralHost     | Apex Central host name                                | Example: TW-CHRIS-W2019   |
| devicePayloadId     | Unique message GUID                                   | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697  |
| TMCMdevicePlatform  | Endpoint operating system                             | Example: Windows 7 6.1 (Build 7601) Service Pack 1  |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|700106|Data Loss Prevention|3|cs3Label=Product_Entity/Endpoint cs3=Sample_Host dvc
```

```

host=Sampledvchost cs2Label=Policy cs2=N/A cn1Label=Product
cn1=15 rt=Oct 13 2017 02:54:04 GMT+00:00 src=10.0.9.34 smac=
34-E6-D7-84-BC-7F shost=shost1 cs4Label=Incident_Source_(AD_
Account) cs4=12467 filePath=D:\\2. DRIVER\\drivers WIN7\\Dri
vers\\DP_CardReader_14032.7z\\02Micro\\FORCED\\6x86\\ fname=
02MDFvst.INF cs5Label=Rule cs5=SAMPLE RULE SET cs6Label=Temp
late cs6=Apex One policy cn3Label=Channel cn3=0 cn2Label=Act
ion cn2=4 deviceFacility=Apex One deviceNtDomain=APEXTMCM dn
tdom=OSCEDomain1 externalId=101 cfp1Label=ForensicFileAvaila
ble cfp1=0 dvchost=localhost TCMLogDetectedHost=ApexOneClie
nt01 TCMLogDetectedIP=10.201.86.187 ApexCentralHost=TW-CHRI
S-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
TCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack
1

```

## Action Result Mapping Table

| VALUE | DESCRIPTION                     |
|-------|---------------------------------|
| -1    | Not available                   |
| 0     | Blocked                         |
| 1     | Deleted                         |
| 2     | Delivered                       |
| 3     | Logged                          |
| 4     | Passed                          |
| 5     | Quarantined                     |
| 6     | Replaced                        |
| 7     | Archived                        |
| 8     | Archived (message body only)    |
| 9     | Quarantined (message body only) |



| <b>VALUE</b> | <b>DESCRIPTION</b>                          |
|--------------|---|
| 10           | Passed (message body only)                  |
| 11           | Encrypted                                   |
| 12           | Alerted (endpoint)                          |
| 13           | Alerted (server)                            |
| 14           | Data recorded                               |
| 15           | User justified                              |
| 16           | Handed off                                  |
| 17           | Recipient altered                           |
| 18           | Blind carbon copied                         |
| 19           | Delivery postponed                          |
| 20           | Stamped                                     |
| 21           | Attachment deleted                          |
| 22           | Subject tagged                              |
| 23           | X-header tagged                             |
| 24           | Decrypted                                   |
| 25           | Re-encrypted                                |
| 26           | Tagged (mail)                               |
| 27           | Encrypted (user key)                        |
| 28           | Encrypted (group key)                       |
| 29           | Moved                                       |
| 30           | Passed (encrypted)                          |
| 31           | Passed (user justified)                     |
| 32           | Blocked (Endpoint Encryption not installed) |

| VALUE | DESCRIPTION                              |
|-------|--|
| 33    | Blocked (user justified)                 |
| 34    | Blocked (Endpoint Encryption logged off) |
| 35    | Blocked (Endpoint Encryption error)      |
| 36    | web upload                               |

## Channel Mapping Table

| VALUE | DESCRIPTION         |
|-------|---------------------|
| 65535 | Not available       |
| 0     | Removable storage   |
| 1     | SMB                 |
| 2     | Email               |
| 3     | IM                  |
| 4     | FTP                 |
| 5     | HTTP                |
| 6     | HTTPS               |
| 7     | PGP                 |
| 8     | Data recorders      |
| 9     | Printer             |
| 10    | Clipboard           |
| 11    | Sync                |
| 12    | P2P                 |
| 13    | Webmail             |
| 14    | Document management |

| <b>VALUE</b> | <b>DESCRIPTION</b>           |
|--------------|------------------------------|
| 15           | Cloud storage                |
| 121          | SMTP email                   |
| 122          | Exchange Client Mail         |
| 123          | Lotus Note Email             |
| 130          | Webmail (Yahoo! Mail)        |
| 131          | Webmail (Hotmail)            |
| 132          | Webmail (Gmail)              |
| 133          | Webmail (AOL Mail)           |
| 140          | IM (MSN)                     |
| 141          | IM (AIM)                     |
| 142          | IM (Yahoo Messenger)         |
| 143          | IM (Skype)                   |
| 191          | P2P (BitTorrent)             |
| 192          | P2P (EMule)                  |
| 193          | P2P (Winny)                  |
| 194          | P2P (HTCSYN)                 |
| 195          | P2P (iTunes)                 |
| 196          | Cloud storage (DropBox)      |
| 197          | Cloud storage (Box)          |
| 198          | Cloud storage (Google Drive) |
| 199          | Cloud storage (OneDrive)     |
| 200          | Cloud storage (SugarSync)    |
| 201          | Cloud storage (Hightail)     |

| VALUE | DESCRIPTION                      |
|-------|----------------------------------|
| 202   | IM (QQ)                          |
| 203   | Webmail (other)                  |
| 204   | Cloud storage (Evernote)         |
| 211   | Document management (SharePoint) |

## CEF Device Access Control Logs

| CEF KEY            | DESCRIPTION                             | VALUE                                     |
|--------------------|---|---|
| Header (logVer)    | CEF format version                      | CEF:0                                     |
| Header (vendor)    | Appliance vendor                        | Trend Micro                               |
| Header (pname)     | Appliance product                       | Apex Central                              |
| Header (pver)      | Appliance version                       | 2019                                      |
| Header (eventid)   | Event ID                                | 700107                                    |
| Header (eventName) | Log name                                | Device Access Control                     |
| Header (severity)  | Severity                                | 3   |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00" |
| cs1Label           | Corresponding label for the "cs1" field | "Product Entity/Endpoint"                 |
| cs1                | Server host name                        | Example: "Sample_Host"                    |
| shost              | Source host name                        | Example: "shost1"                         |
| duser              | User name                               | Example: "testserver\<br>\administrator"  |
| dvchost            | Target host name                        | Example: "localhost"                      |
| cn1Label           | Corresponding label for the "cn1" field | "Product"                                 |

| CEF KEY        | DESCRIPTION                             | VALUE  |
|----------------|---|--|
| cn1            | Product ID                              | Example: "Apex One"<br><br>For more information, see <a href="#">Product ID Mapping Table on page F-38</a> .   |
| sproc          | Target process                          | Example: "C:\\Windows\\explorer.exe"   |
| fname          | File name                               | Example: "F:\\Autorun.inf"   |
| cn2Label       | Corresponding label for the "cn2" field | "Device_Type"  |
| cn2            | Device type                             | Example: "0"<br><br><ul style="list-style-type: none"> <li>• 0: USB storage device</li> <li>• 1: Non-storage USB</li> <li>• 2: CD/DVD</li> <li>• 3: Floppy disks</li> <li>• 4: Network driver</li> </ul> |
| cn3Label       | Corresponding label for the "cn3" field | "Permission"   |
| cn3            | Permission                              | Example: "3"<br><br><ul style="list-style-type: none"> <li>• 0: Modify</li> <li>• 1: Read and execute</li> <li>• 2: Read</li> <li>• 3: List device content only</li> <li>• 4: Block</li> </ul>           |
| deviceFacility | Product                                 | Example: "Apex One"  |
| deviceNtDomain | Active Directory domain                 | Example: APEXTMCM  |
| dntdom         | Apex One domain hierarchy               | Example: OSCEDomain1   |

| CEF KEY             | DESCRIPTION                                | VALUE  |
|---------------------|--|--|
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName                           |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3                                  |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019                            |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMDevicePlatform  | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1 |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|700107|Device Access Control|3|rt=Aug 16 2017 04:49:15 GMT+00:00 cs1Label=Product_Entity/Endpoint cs1=Sample_Host shost=shost1 dvchost=localhost cn1Label=Product cn1=15 sproc=C:\\Windows\\explorer.exe filename=F:\\Autorun.inf cn2Label=Device_Type cn2=0 cn3Label=Permission cn3=3 deviceFacility=Apex One deviceNtDomain=APEXTMC M dntdom=OSCEDomain1 TMCMLogDetectedHost=shost1 TMCMLogDetectedIP=10.0.76.40 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMDevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

## Product ID Mapping Table

| VALUE | DESCRIPTION               |
|-------|---------------------------|
| 0     | Unknown product           |
| 1     | ScanMail for ccMail       |
| 2     | ScanMail for Lotus Domino |

| <b>VALUE</b> | <b>DESCRIPTION</b>               |
|--------------|----------------------------------|
| 3            | ScanMail for Microsoft Exchange  |
| 4            | ScanMail for Microsoft Mail      |
| 5            | ScanMail for OpenMail            |
| 6            | Reserved 1                       |
| 7            | Reserved 2                       |
| 8            | Reserved 3                       |
| 9            | Reserved 4                       |
| 10           | InterScan WebProtect             |
| 11           | Reserved 5                       |
| 12           | Reserved 6                       |
| 13           | Reserved 7                       |
| 14           | PC-cillin Corporate Edition      |
| 15           | Apex One                         |
| 16           | Apex One for Microsoft SBS       |
| 18           | ServerProtect for Windows        |
| 19           | ServerProtect for Windows (SOHO) |
| 20           | Apex Central                     |
| 21           | Generic                          |
| 22           | InterScan VirusWall for Unix     |
| 23           | InterScan VirusWall for Windows  |
| 24           | MOCA                             |
| 25           | GoldenGate                       |
| 26           | ActiveUpdate                     |

| VALUE | DESCRIPTION  |
|-------|--|
| 27    | IS_Y2K_SCANNER   |
| 28    | Y2K VIRUS TECH SUPPORT SRV                             |
| 30    | HouseCall  |
| 31    | PC-cillin ISP server                                   |
| 32    | PC-cillin ISP client                                   |
| 33    | eManager for ScanMail Exchange                         |
| 34    | InterScan Messaging Security Suite for Windows         |
| 35    | InterScan Messaging Security Suite for UNIX            |
| 36    | PortalProtect  |
| 37    | GateLock Corporate Edition                             |
| 38    | Firewall management (NetScreen)                        |
| 39    | InterScan Web Security Suite for Solaris               |
| 40    | InterScan Web Security Suite for Windows NT            |
| 41    | Nokia Message Protector                                |
| 42    | InterScan Web Security Suite for Linux                 |
| 43    | InterScan Web Security Suite for Appliance             |
| 44    | InterScan Messaging Security Appliance                 |
| 45    | InterScan for Small and Medium Business for Windows NT |
| 46    | InterScan Web Security Virtual Appliance               |
| 47    | InterScan Messaging Security Virtual Appliance         |
| 50    | InterScan Gateway Security Appliance                   |
| 51    | ServerProtect for Linux                                |
| 52    | ServerProtect for EMC                                  |



| <b>VALUE</b> | <b>DESCRIPTION</b>                             |
|--------------|--|
| 53           | ServerProtect for NetApp                       |
| 56           | Child Apex Central Server                      |
| 60           | Damage Cleanup Services                        |
| 65           | Golden Gate for NT                             |
| 66           | Network VirusWall 1200                         |
| 67           | Network VirusWall MIPS                         |
| 68           | Network VirusWall 2500                         |
| 69           | Network VirusWall 2500 v2                      |
| 70           | Vulnerability Assessment                       |
| 71           | Network Virus Wall Enforcer 1200               |
| 72           | Network VirusWall Enforcer                     |
| 73           | Network VirusWall Enforcer                     |
| 75           | Trend Micro Threat Mitigator                   |
| 85           | Anti-Spyware Enterprise Edition                |
| 87           | Trend Micro InterScan for Cisco CSC SSM-20     |
| 88           | Trend Micro InterScan for Cisco CSC SSM-10     |
| 90           | IM Security                                    |
| 95           | InterScan VirusWall                            |
| 96           | InterScan VirusWall for Linux                  |
| 100          | Control Manager Agent                          |
| 200          | eDoctor Server                                 |
| 300          | eDoctor Agent                                  |
| 132          | InterScan Messaging Security Suite for Solaris |

| <b>VALUE</b> | <b>DESCRIPTION</b>                       |
|--------------|--|
| 120          | Threat Discovery Appliance               |
| 131          | Database Protect for Linux               |
| 151          | Total Discovery Mitigation Server        |
| 154          | Deep Discovery Inspector                 |
| 155          | ScanMail for IBM Domino                  |
| 156          | Deep Discovery Email Inspector           |
| 1000         | InterScan eManager                       |
| 1001         | InterScan AppletTrap                     |
| 1002         | InterScan VirusWall Java                 |
| 1003         | IS_SEMAIL                                |
| 1004         | InterScan WebProtect for ICAP            |
| 10001        | NEC StarOffice                           |
| 20001        | Dr. Soloman Anti-virus                   |
| 20002        | Inoculan                                 |
| 20003        | Norton Anti-virus                        |
| 20004        | Sophos Sweep                             |
| 20005        | Intel LANProtect                         |
| 20006        | McAfee Virus Scan                        |
| 20007        | FProt                                    |
| 21000        | Other third-party product                |
| 31001        | Apex One (Mac)                           |
| 31002        | Trend Micro Endpoint Encryption          |
| 31003        | Trend Micro Endpoint Application Control |

| VALUE | DESCRIPTION                           |
|-------|---------------------------------------|
| 31004 | Trend Micro Deep Security             |
| 31006 | Vulnerability Protection              |
| 31005 | Trend Micro Mobile Security           |
| 31007 | Trend Micro Safe Mobile Workforce     |
| 31008 | Deep Discovery Analyzer               |
| 31009 | Trend Micro Endpoint Sensor           |
| 31012 | Deep Discovery Web Inspector          |
| 31101 | Trend Micro Email Security            |
| 31102 | Worry Free Business Security Services |
| 31103 | Trend Micro Web Security              |
| 31104 | Cloud App Security                    |
| 55555 | Demo product                          |

## CEF Endpoint Application Control Logs

| CEF KEY            | DESCRIPTION           | VALUE   |
|--------------------|-----------------------|---|
| Header (logVer)    | CEF format version    | CEF:0   |
| Header (vendor)    | Appliance vendor      | Trend Micro   |
| Header (pname)     | Appliance product     | Apex Central  |
| Header (pver)      | Appliance version     | 2019  |
| Header (eventid)   | Device event class ID | <ul style="list-style-type: none"> <li>• 0: Allow</li> <li>• 1: Block</li> <li>• 2: Lockdown</li> </ul> |
| Header (eventName) | Event name            | Endpoint Application Control Violation Information  |

| CEF KEY           | DESCRIPTION                      | VALUE   |
|-------------------|----------------------------------|---|
| Header (severity) | Severity                         | 3   |
| deviceExternalId  | ID                               | Example: "39"   |
| rt                | Event trigger time in UTC        | Example: "Mar 22 2018 08:23:23 GMT+00:00"   |
| dvchost           | Computer name                    | Example: "localhost"  |
| shost             | Client host name                 | Example: "shost1"   |
| cs1               | Product server pattern version   | Example: "1297"   |
| suser             | Client user name                 | Example: "TREND\User"   |
| cs2               | Client IPv4 address              | Example: "10.0.17.6"  |
| c6a3              | Client IPv6 address              | Example:<br>"fe80::38ca:cd15:443c:40bb%11"  |
| cn1               | Client status                    | <ul style="list-style-type: none"> <li>• 1: Rebuilding database</li> <li>• 2: Online</li> <li>• 3: Offline</li> </ul> |
| filehash          | Application file SHA-1 hash      | Example:<br>"D6712CAE5EC821F910E14945153AE7871AA536CA"  |
| fname             | Application file name            | Example: "notepad.exe"  |
| cs3               | Application process command line | Example: "notepad.exe"  |
| duser             | User name                        | Example: "Admin004"   |
| cs4               | Rule name                        | Example: "SAMPLE RULE SET"  |
| cs5               | Policy name                      | Example: "SAMPLE POLICY"  |

| CEF KEY            | DESCRIPTION               | VALUE  |
|--------------------|---------------------------|--|
| act                | Policy action             | <ul style="list-style-type: none"> <li>• 0: Allowed</li> <li>• 1: Blocked</li> <li>• 2: Reported as allowed</li> <li>• 3: Reported as blocked</li> </ul> |
| deviceFacility     | Product name              | Example: "Trend Micro Endpoint Application Control"  |
| deviceNtDomain     | Active Directory domain   | Example: APEXTMCM  |
| dntdom             | Apex One domain hierarchy | Example: OSCEDomain1   |
| ApexCentralHost    | Apex Central host name    | Example: TW-CHRIS-W2019  |
| devicePayloadId    | Unique message GUID       | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMdevicePlatform | Endpoint operating system | Example: Windows 7 6.1 (Build 7601) Service Pack 1   |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|EAC:1|Endpoint Application Control Violation Information|3|deviceExternalId=39 rt=Jun 27 2012 03:14:03 GMT+00:00 cs1Label=Version cs1=1.299.00 suser=TMCM\\QA cs2Label=ApplicationControlEvent_ClientIPAddress_V4 cs2=0.0.0.0 cn1Label=Connection_Status cn1=0 fileHash=c0869b72C5606D22D92A6AC986686BB87485A25b fname=P2P_TEST.exe cs3Label=Command cs3=C:\\P2P_TEST.exe duser=QA cs4Label=Rule cs4=Test cs5Label=Policy cs5=TestPolicy act=Blocked deviceFacility=Trend Micro Endpoint Application Control deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

## CEF Engine Update Status Logs

| CEF KEY            | DESCRIPTION                             | VALUE   |
|--------------------|---|---|
| Header (logVer)    | CEF format version                      | CEF:0   |
| Header (vendor)    | Product vendor                          | Trend Micro   |
| Header (pname)     | Product name                            | Apex Central  |
| Header (pver)      | Product version                         | 2019  |
| Header (eventid)   | Event ID                                | 800102  |
| Header (eventName) | Log name                                | Engine Update Status  |
| Header (severity)  | Severity                                | 3   |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00"   |
| shost              | Product Entity/Endpoint                 | Example: "shost1"   |
| cs2Label           | Corresponding label for the "cs2" field | "Product/Endpoint IP"   |
| cs2                | Product/Endpoint IP                     | Example: "10.0.17.6"  |
| cn1Label           | Corresponding label for the "cn1" field | "Connection Status"   |
| cn1                | Connection status                       | Example: "100" <ul style="list-style-type: none"> <li>• 0: Unable to connect</li> <li>• 1: Active</li> <li>• 2: Inactive</li> <li>• 100: Product active</li> <li>• 101: Product inactive but agent is active</li> <li>• 102: Roaming</li> </ul> |
| cn2Label           | Corresponding label for the "cn2" field | "Engine"  |

| CEF KEY         | DESCRIPTION                             | VALUE  |
|-----------------|---|--|
| cn2             | Engine                                  | Example: "4096"  |
| cn5Label        | Corresponding label for the "cn5" field | "Engine Version"   |
| cs5             | Engine version                          | Example: "9.950.1006"  |
| cn3Level        | Corresponding label for the "cn3" field | "Engine Status"  |
| cn3             | Engine status                           | Example: "1" <ul style="list-style-type: none"> <li>• 1: Up-to-date</li> <li>• 2: Out-of-date</li> </ul> |
| cs6Label        | Corresponding label for the "cs6" field | "AUComponent_Type"   |
| cs6             | ActiveUpdate component type             | Example: "1" <ul style="list-style-type: none"> <li>• 1: Engine</li> </ul>                               |
| deviceFacility  | Managed product name                    | Example: "Apex One"  |
| msg             | Engine type display name                | Example: "Virus Scan Engine DLL (Windows 2000/NT, 32-bit)"   |
| deviceNtDomain  | Active Directory domain                 | Example: APEXTMCM  |
| dntdom          | Apex One domain hierarchy               | Example: OSCEDomain1   |
| ApexCentralHost | Apex Central host name                  | Example: TW-CHRIS-W2019  |
| devicePayloadId | Unique message GUID                     | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|800102|Engine Update S
tatus|3|rt=Apr 20 2017 12:04:34 GMT+00:00 shost=shost1 cs2La
bel=Product/Endpoint_IP cs2=10.0.17.6 cn1Label=Connection_St
atus cn1=100 cn2Label=Engine cn2=4096 cs5Label=Engine_Versio
```

```
n cs5=9.950.1006 cn3Label=Engine_Status cn3=1 cs6Label=AUComponent_Type cs6=1 deviceFacility=Apex One deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

## CEF Intrusion Prevention Logs

| CEF KEY            | DESCRIPTION                              | VALUE                                      |
|--------------------|--|--|
| Header (logVer)    | CEF format version                       | CEF:0                                      |
| Header (vendor)    | Product vendor                           | Trend Micro                                |
| Header (pname)     | Product name                             | Apex Central                               |
| Header (pver)      | Product version                          | 2019                                       |
| Header (eventid)   | Event ID                                 |  |
| Header (eventName) | Log name                                 |  |
| Header (severity)  | Severity                                 | 3  |
| dvchost            | Display name of the managed endpoint     | Example: "localhost"                       |
| rt                 | Log generation time in UTC               | Example: "Nov 15 2017 08:43:57 GMT +00:00" |
| src                | Source IPv4 address                      | Example: "10.1.152.12"                     |
| c6a2Label          | Corresponding label for the "c6a2" field | SLF_SourceIPv6                             |
| c6a2               | Source IPv6 address                      | "2001:b011:1004:325b:8db7:6ca9:8fc5:321a"  |
| smac               | Source MAC address                       | Example: "18:31:BF:4F:30:DD"               |
| spt                | Source port                              | Example: "60886"                           |
| dst                | Destination IPv4 address                 | Example: "10.1.153.151"                    |
| c6a3Label          | Corresponding label for the "c6a3" field | SLF_DestinationIPv6                        |



| CEF KEY         | DESCRIPTION  | VALUE   |
|-----------------|--|---|
| c6a3            | Destination IPv6 address                                 | Example:<br>"2001:b011:1004:325b:8db7:6ca9:<br>8fc5:654a"   |
| dmac            | Destination host MAC address                             | Example: "D0:17:C2:95:ED:71"  |
| dpt             | Destination port   | Example: "139"  |
| cn2Label        | Corresponding label for the "cn2" field                  | SLF_IsDetectionOnly   |
| cn2             | Indicates whether the system is in "detection only" mode | Example: "0"<br><ul style="list-style-type: none"> <li>• 0 or NULL = No</li> <li>• 1 = Yes</li> </ul>   |
| act             | Action   | Example: "LOG"<br>SLF_ACTION maps: <ul style="list-style-type: none"> <li>• 0 = UNKNOWN</li> <li>• 3 = DELETE</li> <li>• 6 = LOG</li> <li>• 10 = INSERT/REPLACE</li> <li>• 13 = BLOCK</li> <li>• 257 = RESET</li> </ul> |
| deviceDirection | Incoming or outgoing direction                           | Example: "Apex One"   |
| cn3Label        | Corresponding label for the "cn3" field                  | SLF_Rank  |
| cn3             | Weighted priority of the incident                        | Example: "3"<br>Calculated from Severity x Asset Value  |
| cn4Label        | Corresponding label for the "cn4" field                  | SLF_SeverityCode  |

| CEF KEY  | DESCRIPTION                                       | VALUE  |
|----------|---|--|
| cn4      | The system defined incident severity value        | Example: "1"<br><ul style="list-style-type: none"> <li>• 1 = LOW</li> <li>• 2 = MEDIUM</li> <li>• 3 = HIGH</li> <li>• 4 = CRITICAL</li> </ul>  |
| proto    | The network protocol being exploited              | Example: "10009"<br><ul style="list-style-type: none"> <li>• 28 = ICMP</li> <li>• 46 = ICMPv6</li> <li>• 10003 = TCP</li> <li>• 10004 = UDP</li> <li>• 10005 = IGMP</li> <li>• 10006 = GGP</li> <li>• 10007 = PUP</li> <li>• 10008 = IDP</li> <li>• 10009 = ND</li> <li>• 10010 = RAW</li> </ul> |
| cs2Label | Corresponding label for the "cs2" field           | SLF_ConnectionType   |
| cs2      | The network application name                      | Example: "DCERPC Services"   |
| cn1Label | Corresponding label for the "cn1" field           | SLF_RuleID   |
| cn1      | The ID of the inspection rule                     | Example: "1005448"   |
| cs1Label | Corresponding label for the "cs1" field           | SLF_RuleContent  |
| cs1      | The string literal of the rule ID and description | Example: "1005448 - SMB Null Session Detected - 1"   |
| cnt      | Aggregated count                                  | Example: "1"   |

| CEF KEY        | DESCRIPTION               | VALUE                |
|----------------|---------------------------|----------------------|
| deviceNtDomain | Active Directory domain   | Example: APEXTMCM    |
| dntdom         | Apex One domain hierarchy | Example: OSCEDomain1 |

Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|Log|1009549 - Detected Terminal Services (RDP) Server Traffic - 1 (ATT&CK T1015,T1043,T1076,T1048,T1032,T1071)|3|rt=Apr 20 2020 03:33:20 GMT+00:00 dvchost=OSCEclient23 deviceFacility=Apex One act=Log,src=10.1.1.9 dst=80.1.1.9 smac=54-BF-64-84-7F-09 spt=89 dmac=54-BF-64-84-7F-19 dpt=449 cn2Label=SLF_IsDetectionOnly cn2=0 deviceDirection=Inbound cn3Label=SLF_Rank cn3=1 cn4Label=SLF_SeverityCode cn4=1 proto=10009 cs2Label=SLF_ConnectionType cs2=N/A cn1Label=SLF_RuleID cn1=1009549 cs1Label=SLF_RuleContent cs1=1009549 - Detected Terminal Services (RDP) Server Traffic - 1 (ATT&CK T1015,T1043,T1076,T1048,T1032,T1071) cnt=1 deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

## CEF Managed Product Logon/Logoff Events

| CEF KEY            | DESCRIPTION        | VALUE                               |
|--------------------|--------------------|-------------------------------------|
| Header (logVer)    | CEF format version | CEF:0                               |
| Header (vendor)    | Appliance vendor   | Trend Micro                         |
| Header (pname)     | Appliance product  | Apex Central                        |
| Header (pver)      | Appliance version  | 2019                                |
| Header (eventid)   | Event ID           | 700211                              |
| Header (eventName) | Log name           | Managed Product Logon/Logoff Events |
| Header (severity)  | Severity           | 3                                   |

| CEF KEY          | DESCRIPTION                             | VALUE                                      |
|------------------|---|--|
| deviceExternalId | ID                                      | Example: "38"                              |
| deviceFacility   | Product name                            | Example: "ScanMail for Microsoft Exchange" |
| cs1Label         | Corresponding label for the "cs1" field | Product_Version                            |
| cs1              | Product version                         | Example: "14"                              |
| cn1Label         | Corresponding label for the "cn1" field | Command_Status                             |
| cn1              | Command status                          | Example: "110"                             |
| msg              | Detailed event information              | Example: "Sample Message"                  |
| shost            | Product server name                     | Example: "SMEX01"                          |

#### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|700211|Managed Product Logon/Logoff Events|3|deviceExternalId=11 shost=SMEX01 deviceFacility=ScanMail for Microsoft Exchange cs1Label=Product_Version cs1=14 cn1Label=Command_Status cn1=110 msg=A user with the Administrator role(s) has logged on. Detail Information :UserName:TEST2013\\administrator,IP address:10.204.166.127, EventType:Log in/out,SourceType:SMEX UI. #015
```

## CEF Network Content Inspection Logs

| CEF KEY         | DESCRIPTION        | VALUE        |
|-----------------|--------------------|--------------|
| Header (logVer) | CEF format version | CEF:0        |
| Header (vendor) | Appliance vendor   | Trend Micro  |
| Header (pname)  | Appliance product  | Apex Central |

| CEF KEY            | DESCRIPTION                              | VALUE  |
|--------------------|--|--|
| Header (pver)      | Appliance version                        | 2019   |
| Header (eventid)   | NCIE:Action                              | NCIE:Pass  |
| Header (eventName) | Name                                     | Suspicious Connection                            |
| Header (severity)  | Severity                                 | 3  |
| deviceExternalId   | ID                                       | Example: "1"                                     |
| cat                | Log type                                 | Example: "1756"                                  |
| deviceFacility     | Product                                  | Example: "Apex One"                              |
| rt                 | Event trigger time in UTC                | Example: "Mar 22 2018 08:23:23 GMT+00:00"        |
| deviceProcessName  | Process                                  | Example: "C:\\Windows\\system32\\svchost-1.exe"  |
| src                | Local IPv4 address                       | Example: "10.201.86.152"                         |
| c6a2Label          | Corresponding label for the "c6a2" field | Example: "SLF_SourceIP"                          |
| c6a2               | Local IPv6 address                       | Example: "2620:101:4003:7a0:fd4b:52ed:53bd:ae3d" |
| spt                | Local IP address port                    | Example: "54594"                                 |
| dst                | Remote IPv4 address                      | Example: "10.69.81.64"                           |
| c6a3Label          | Corresponding label for the "c6a3" field | Example: "SLF_DestinationIP"                     |
| c6a3               | Remote IPv6 address                      | Example: "fe80::38ca:cd15:443c:40bb%11"          |
| dpt                | Remote IP address port                   | Example: "80"                                    |

| CEF KEY         | DESCRIPTION                             | VALUE   |
|-----------------|---|---|
| act             | Action                                  | Example: "Pass" <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Pass</li> <li>• 2: Block</li> <li>• 3: Monitor</li> <li>• 4: Delete</li> <li>• 5: Quarantine</li> <li>• 6: Warn</li> <li>• 7: Warn and continue</li> <li>• 8: Override</li> </ul> |
| deviceDirection | Traffic direction                       | Example: "Inbound" <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Inbound</li> <li>• 2: Outbound</li> </ul>   |
| cn1Label        | Corresponding label for the "cn1" field | Example: "SLF_PatternType"  |
| cn1             | Pattern type                            | Example: "2" <ul style="list-style-type: none"> <li>• 0: Global C&amp;C pattern</li> <li>• 1: Relevance rules</li> <li>• 2: User-defined block list</li> </ul>  |
| cs2Label        | Corresponding label for the "cs2" field | Example: "NCIE_ThreatName"  |
| cs2             | Threat name                             | Example:<br>"Malicious_identified_CnC_querying_on_UDP_detected"   |

| CEF KEY             | DESCRIPTION                                | VALUE   |
|---------------------|--|---|
| reason              | Critical threat type                       | Example: "E"<br><ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| dvchost             | Host name                                  | Example: "localhost"  |
| deviceNtDomain      | Active Directory domain                    | Example: APEXTMCM   |
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1  |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName  |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3   |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019   |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697  |
| TMCMdevicePlatform  | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1  |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|NCIE:Pass|Suspicious
Connection|3|deviceExternalId=1 rt=Oct 11 2017 06:34:06 GMT+0
0:00 cat=1756 deviceFacility=Apex One deviceProcessName=C:\\W
indows\\system32\\svchost-1.exe act=Pass src=10.201.86.152 ds
t=10.69.81.64 spt=54594 dpt=80 deviceDirection=None cn1Label=
```

```
SLF_PatternType cn1=2 cs2Label=NCIE_ThreatName cs2=Malicious_
identified_CnC_querying_on_UDP_detected reason=F deviceNtDoma
in=APEXTMCM dntdom=OSCEDomain1 dvchost=shost1 TCMLogDetected
Host=shost1 TCMLogDetectedIP=10.1.2.3ApexCentralHost=TW-CHRI
S-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697
TCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

## CEF Pattern Update Status Logs

| CEF KEY            | DESCRIPTION                             | VALUE                                     |
|--------------------|---|---|
| Header (logVer)    | CEF format version                      | CEF:0                                     |
| Header (vendor)    | Product vendor                          | Trend Micro                               |
| Header (pname)     | Product name                            | Apex Central                              |
| Header (pver)      | Product version                         | 2019                                      |
| Header (eventid)   | Event ID                                | 800101                                    |
| Header (eventName) | Log name                                | Pattern Update Status                     |
| Header (severity)  | Severity                                | 3   |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00" |
| shost              | Product Entity/Endpoint                 | Example: "shost1"                         |
| cs1Label           | Corresponding label for the "cs1" field | "Operating System"                        |
| cs1                | Operating system                        | Example: "Windows 7"                      |
| cs2Label           | Corresponding label for the "cs2" field | "Product/Endpoint IP"                     |
| cs2                | Product/Endpoint IP                     | Example: "10.0.7.20"                      |
| cs3Label           | Corresponding label for the "cs3" field | "Update Agent"                            |



| CEF KEY  | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cs3      | Update Agent                            | Example: "0"  |
| cs4Label | Corresponding label for the "cs4" field | "Domain"  |
| cs4      | Domain                                  | Example: "Default"  |
| cn1Label | Corresponding label for the "cn1" field | "Connection Status"   |
| cn1      | Connection status                       | Example: "100" <ul style="list-style-type: none"> <li>• 0: Unable to connect</li> <li>• 1: Active</li> <li>• 2: Inactive</li> <li>• 100: Product active</li> <li>• 101: Product inactive but agent is active</li> <li>• 102: Roaming</li> </ul> |
| cn2Label | Corresponding label for the "cn2" field | "Pattern/Rule"  |
| cn2      | Pattern/Rule                            | Example: "2048"   |
| cs5Label | Corresponding label for the "cs5" field | "Pattern/Rule Version"  |
| cs5      | Pattern/Rule version                    | Example: "1548"   |
| cn3Label | Corresponding label for the "cn3" field | "Pattern/Rule Status"   |

| CEF KEY         | DESCRIPTION                             | VALUE   |
|-----------------|---|---|
| cn3             | Pattern/Rule status                     | Example: "1" <ul style="list-style-type: none"> <li>• 1: Up-to-date</li> <li>• 2: 1 version old</li> <li>• 3: 2 versions old</li> <li>• 4: 3 versions old</li> <li>• 5: 4 versions old</li> <li>• 6: 5 versions old</li> <li>• 7: 6 or more versions old</li> </ul> |
| cs6Label        | Corresponding label for the "cs6" field | "AUComponent_Type"  |
| cs6             | ActiveUpdate component type             | Example: "2" <ul style="list-style-type: none"> <li>• 2: Pattern</li> </ul>   |
| deviceFacility  | Managed product name                    | Example: "Apex One"   |
| msg             | Pattern type display name               | Example: "Virus Pattern"  |
| deviceNtDomain  | Active Directory domain                 | Example: APEXTMCM   |
| dntdom          | Apex One domain hierarchy               | Example: OSCEDomain1  |
| ApexCentralHost | Apex Central host name                  | Example: TW-CHRIS-W2019   |
| devicePayloadId | Unique message GUID                     | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697  |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|800101|Pattern Update
Status|3|rt=Nov 02 2017 12:46:44 GMT+00:00 shost=shost1 cs1L
abel=Operating_System cs1=Windows 7 cs2Label=Product/Endpoi
nt_IP cs2=10.0.7.20 cs3Label=Update_Agent cs3=0 cs4Label=Dom
ain cs4=Default cn1Label=Connection_Status cn1=100 cn2Label=
Pattern/Rule cn2=2048 cs5Label=Pattern/Rule_Version cs5=1548
```

```
cn3Label=Pattern/Rule_Status cn3=1 cs6Label=AUComponent_Type
cs6=2 deviceFacility=Apex One deviceNtDomain=APEXTMCM dntd
om=OSCEDomain1
```

## CEF Predictive Machine Learning Logs

| CEF KEY            | DESCRIPTION                             | VALUE  |
|--------------------|---|--|
| Header (logVer)    | CEF format version                      | CEF:0  |
| Header (vendor)    | Product vendor                          | Trend Micro  |
| Header (pname)     | Product name                            | Apex Central   |
| Header (pver)      | Product version                         | 2019   |
| Header (eventid)   | PML:Action result                       | PML:File cleaned   |
| Header (eventName) | Detection name                          | virusa   |
| Header (severity)  | Severity                                | 3  |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00"  |
| dvchost            | Product server                          | Example: "Sample_Host"   |
| cn1Label           | Corresponding label for the "cn1" field | "ThreatType"   |
| cn1                | Probable threat type                    | Example: "35143"<br>For more information, see <a href="#">Threat Type Mapping Table on page F-63</a> . |
| cs2Label           | Corresponding label for the "cs2" field | "DetectionName"  |
| cs2                | Security threat                         | Example: "Troj.Win32.TRX.XXPE002FF017"   |
| shost              | Infected endpoint                       | Example: "10.0.0.1"  |

| CEF KEY           | DESCRIPTION                             | VALUE  |
|-------------------|---|--|
| suser             | Logon user                              | Example: "TREND\\User"   |
| cn2Label          | Corresponding label for the "cn2" field | "DetectionType"  |
| cn2               | Detection type                          | Example: "0"<br><ul style="list-style-type: none"> <li>• 0: File</li> <li>• 1: Process</li> </ul>  |
| filePath          | File path                               | Example: "D:\\"  |
| fname             | File name                               | Example: "ALCORMP.EXE"   |
| deviceCustomDate1 | File creation time                      | Example: "2017-04-26 05:53:27.000"   |
| sproc             | System process                          | Example: "notepad.exe"   |
| cn4Label          | Corresponding label for the "cn4" field | "ProcessCommandLine"   |
| cs4               | Process command                         | Example: "notepad.exe"   |
| duser             | Process owner                           | Example: "user1"   |
| app               | Infection channel                       | Example: "10"<br><ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Local drive</li> <li>• 2: Network drive</li> <li>• 3: AutoRun files</li> <li>• 10: Web</li> <li>• 11: Email</li> <li>• 999: Local or network drive</li> </ul> |
| cs3Label          | Corresponding label for the "cs3" field | "InfectionLocation"  |
| cs3               | Infection source                        | Example: "http://10.0.0.1/"  |

| CEF KEY          | DESCRIPTION                              | VALUE  |
|------------------|--|--|
| dst              | Product/Endpoint IPv4 Address            | Example: "10.0.17.6"   |
| c6a3Label        | Corresponding label for the "c6a3" field | "Product/Endpoint IP"  |
| c6a3             | Product/Endpoint IPv6 Address            | Example:<br>"fd66:5168:9882:6:b5b0:b2b5:4173:3f5d"   |
| cn3Label         | Corresponding label for the "cn3" field  | "Confidence"   |
| cn3              | Threat probability                       | Example: "82"  |
| act              | Action result                            | Example: "21"<br><br>For more information, see <a href="#">Action Mapping Table on page F-73</a> .   |
| filehash         | File SHA-1                               | Example:<br>"52c17c785b45ee961f68fb17744276076f383085"   |
| dhost            | Product entity/endpoint                  | Example: "dhost1"  |
| deviceExternalId | Log sequence number                      | Example: "100"   |
| deviceFacility   | Product                                  | Example: "Apex One"  |
| reason           | Critical threat type                     | Example: "E" <ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| deviceNtDomain   | Active Directory domain                  | Example: APEXTMCM  |

| CEF KEY             | DESCRIPTION                                | VALUE  |
|---------------------|--|--|
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1                               |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName                           |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3                                  |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019                            |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMDdevicePlatform | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1 |

#### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|PML:File cleaned|Detection01|3|deviceExternalId=1 rt=Dec 01 2018 16:01:00 GMT+00:00 deviceFacility=15 dvchost=OSCE01 cn1Label=ThreatType cn1=1 cs2Label=DetectionName cs2=Detection01 shost=10.0.0.1 suser=Sample_Domain\\Sample_User cn2Label=DetectionType cn2=0 filePath=C:\\test01\\aaa.exe fname=aaa.exe deviceCustomDate1Label=FileCreationDate deviceCustomDate1=Dec 02 2018 00:01:00 GMT+00:00 sproc=notepad.exe cs4Label=ProcessCommandLine cs4=notepad.exe -test duser=admin01 app=1 cs3Label=InfectionLocation cs3=https://10.1.1.1 dst=80.1.1.1 cn3Label=Confidence cn3=81 act=21 fileHash=177750B65A21A9043105FD0820B85B58CF148A01 dhost=OSCEClient11 reason=E deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDetectedHost=OSCEClient11 TMCMLogDetectedIP=80.1.1.1 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCMDdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

## Threat Type Mapping Table

| VALUE | DESCRIPTION       |
|-------|-------------------|
| 35140 | Adware            |
| 35141 | Backdoor          |
| 35142 | Browser modifier  |
| 35143 | DDoS              |
| 35144 | Dialer            |
| 35145 | Exploit           |
| 35146 | Hacking tool      |
| 35147 | Joke program      |
| 35148 | PUA               |
| 35149 | Ransomware        |
| 35150 | Rootkit           |
| 35151 | Spyware           |
| 35152 | Trojan            |
| 35153 | Trojan clicker    |
| 35154 | Trojan downloader |
| 35155 | Trojan dropper    |
| 35156 | Trojan proxy      |
| 35157 | Trojan spyware    |
| 35158 | File infector     |
| 35159 | Worm              |
| 35160 | Bot               |

## CEF Product Auditing Events

| CEF KEY            | DESCRIPTION                             | VALUE  |
|--------------------|---|--|
| Header (logVer)    | CEF format version                      | CEF:0  |
| Header (vendor)    | Product vendor                          | Trend Micro  |
| Header (pname)     | Product name                            | Apex Central   |
| Header (pver)      | Product version                         | 2019   |
| Header (eventid)   | Event ID                                | 1745   |
| Header (eventName) | Log name                                | Product Auditing Events  |
| Header (severity)  | Severity                                | 3  |
| cat                | Log type                                | 1745   |
| deviceFacility     | Managed product                         | Example: "Apex One"  |
| dvchost            | Display name of the managed endpoint    | Example: "localhost"   |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00"  |
| cn1Label           | Corresponding label for the "cn1" field | SLF_CategoryID   |
| cn1                | Category ID                             | Example: "536,870,912"   |
| cn2Label           | Corresponding label for the "cn2" field | SLF_SeverityLevel  |
| cn2                | Severity level                          | Example: "4" <ul style="list-style-type: none"> <li>• 1 = ERROR</li> <li>• 2 = WARNING</li> <li>• 4 = INFORMATION</li> <li>• 16 = FAILURE AUDIT</li> </ul> |



| CEF KEY         | DESCRIPTION   | VALUE  |
|-----------------|---|--|
| user            | The name of the user on whose behalf the event occurred | Example: "administrator"                         |
| deviceNtDomain  | Active Directory domain                                 | Example: APEXTMCM                                |
| dntdom          | Apex One domain hierarchy                               | Example: OSCEDomain1                             |
| ApexCentralHost | Apex Central host name                                  | Example: TW-CHRIS-W2019                          |
| devicePayloadId | Unique message GUID                                     | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697 |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|Delete|1009490 - Block Administrative Share - 1 (ATT&CK T1077,T1105)|3|rt=Apr 20 2020 03:33:15 GMT+00:00 dvchost=OSCEclient22 deviceFacility=Apex One act=Delete, src=10.1.1.8 dst=80.1.1.8 smac=54-BF-64-84-7F-08 spt=88 dmac=54-BF-64-84-7F-18 dpt=448 cn2Label=SLF_IsDetectionOnly cn2=1 deviceDirection=Outbound cn3Label=SLF_Rank cn3=100 cn4Label=SLF_SeverityCode cn4=4 proto=10008 cs2Label=SLF_ConnectionType cs2=Suspicious Client Application Activity cn1Label=SLF_RuleID cn1=1009490 cs1Label=SLF_RuleContent cs1=1009490 - Block Administrative Share - 1 (ATT&CK T1077,T1105) cnt=1 deviceNtDomain=APEXTMCM dntdom=OSCEDomain1
```

## CEF Sandbox Detection Logs



### Note

Sandbox Detection logs are called Virtual Analyzer Detections on the Apex Central console.

| CEF KEY                | DESCRIPTION               | VALUE   |
|------------------------|---------------------------|---|
| Header (logVer)        | CEF format version        | CEF:0   |
| Header (vendor)        | Appliance vendor          | Trend Micro   |
| Header (pname)         | Appliance product         | Apex Central  |
| Header (pver)          | Appliance version         | 2019  |
| Header (eventid)       | Device event class ID     | VAD   |
| Header (eventName)     | Event name                | Virtual Analyzer detection name   |
| Header (severity)      | Severity                  | 3   |
| deviceExternalId       | ID                        | Example: "2"  |
| rt                     | Event trigger time in UTC | Example: "Mar 22 2018 08:23:23 GMT+00:00"   |
| deviceFacility         | Product                   | Example: "Apex One"   |
| dvchost                | Server name               | Example: "OSCE01"   |
| dhost                  | Endpoint name             | Example: "Isolate-ClientA"  |
| dst                    | Endpoint IPv4 address     | Example: "10.0.17.6"  |
| c6a3                   | Endpoint IPv6 address     | Example:<br>"fe80::38ca:cd15:443c:40bb%11"  |
| app                    | Entry channel             | Example: "0"<br><br>For more information, see <a href="#">Protocol Mapping Table on page F-93</a> |
| sourceServiceName      | Source                    | Example:<br>"Test1@tmcm.extbeta.com"  |
| destinationServiceName | Destination               | Example:<br>"Test2@tmcm.extbeta.com;Test3@tmcm.extbeta.com"                                       |
| sproc                  | Process name              | Example: "VA"   |

| CEF KEY  | DESCRIPTION  | VALUE   |
|----------|--|---|
| fileHash | File SHA-1 hash  | Example:<br>“D6712CAE5EC821F910E1494515<br>3AE7871AA536CA”  |
| fname    | File name  | Example: “C:\\\\QA_Log.zip”   |
| request  | URL  | Example: “http://127.1.1.1”   |
| cs1      | The name of the security threat determined by Virtual Analyzer | Example:<br>“VAN_RANSOMWARE.umxxhellor<br>ansom_abc”  |
| cn1      | Displays the risk level assigned by Virtual Analyzer           | Example: “0” <ul style="list-style-type: none"> <li>• 0: No risk</li> <li>• 1: Low risk</li> <li>• 2: Medium risk</li> <li>• 3: High risk</li> <li>• 9999: Unknown</li> </ul> |
| cs2      | Displays the security threat type                              | Example: “Anti-security, self-preservation”   |

| CEF KEY             | DESCRIPTION                                | VALUE   |
|---------------------|--|---|
| cs3                 | Cloud storage vendor                       | Example: "Google Drive" <ul style="list-style-type: none"> <li>• Dropbox</li> <li>• Box</li> <li>• Google Drive</li> <li>• Microsoft OneDrive</li> <li>• SugarSync</li> <li>• Hightail</li> <li>• Evernote</li> <li>• Microsoft Exchange Online</li> <li>• Microsoft SharePoint Online</li> <li>• Unknown</li> <li>• N/A</li> </ul> |
| reason              | Critical threat type                       | Example: "E" <ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul>                          |
| deviceNtDomain      | Active Directory domain                    | Example: APEXTMCM   |
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1  |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName  |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.1.2.3   |

| CEF KEY           | DESCRIPTION               | VALUE  |
|-------------------|---------------------------|--|
| ApexCentralHost   | Apex Central host name    | Example: TW-CHRIS-W2019                            |
| devicePayloadId   | Unique message GUID       | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCdevicePlatform | Endpoint operating system | Example: Windows 7 6.1 (Build 7601) Service Pack 1 |

### Log sample:

```
CEF: 0|Trend Micro|Apex Central|2019|VAD|VAN_RANSOMWARE.um
xxhelloransom_abc|3|deviceExternalId=2 rt=Mar 22 2018 08:23:
23 GMT+00:00 deviceFacility=Apex One dvchost=OSCE01 dhost=
Isolate-ClientA dst=0.0.0.0 app=1 sourceServiceNameTest1@tre
nd.com.tw destinationServiceName=Test2@tmcm.extbeta.com;Test
3@tmcm.extbeta.com sproc=VA fileHash=3395856CE81F2B7382DEE72
602F798B642F14140 fname=C:\\\\QA_Log.zip request=http://127.
1.1.1 cs1Label=Security_Threat cs1=VAN_RANSOMWARE.umxxhellor
ansom_abc cn1Label=Risk_Level cn1=0 cs2Label=Threat_Categori
es cs2=Anti-security, self-preservation cs3Label=Cloud_Servi
ce_Vendor cs3=Google Drive reason=E deviceNtDomain=APEXTMCM
dntdom=OSCEDomain1 TCMLogDetectedHost=OSCEClient TCMLogDe
tectedIP=0.0.0.0 ApexCentralHost=TW-CHRIS-W2019 devicePaylo
adId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TMCdevicePlatfor
m=Windows 7 6.1 (Build 7601) Service Pack 1
```

## CEF Spyware/Grayware Logs

| CEF KEY         | DESCRIPTION        | VALUE        |
|-----------------|--------------------|--------------|
| Header (logVer) | CEF format version | CEF:0        |
| Header (vendor) | Appliance vendor   | Trend Micro  |
| Header (pname)  | Appliance product  | Apex Central |

| CEF KEY            | DESCRIPTION                             | VALUE  |
|--------------------|---|--|
| Header (pver)      | Appliance version                       | 2019   |
| Header (eventid)   | Device event class ID                   | Spyware Detected   |
| Header (eventName) | Event name                              | Spyware Detected   |
| Header (severity)  | Severity                                | 3  |
| cnt                | Number of detections                    | Example: "10"  |
| rt                 | Event trigger time in UTC               | Example: "Mar 22 2018 08:23:23 GMT+00:00"  |
| cn1Label           | Corresponding label for the "cn1" field | Example: "Pattern Type"  |
| cn1                | Pattern type                            | Example: "1073741840"  |
| cs1Label           | Corresponding label for the "cs1" field | Example: "VirusName"   |
| cs1                | Spyware/Grayware                        | Example: "ADW_OPEN CANDY"  |
| cs2Label           | Corresponding label for the "cs2" field | Example: "EngineVersion"   |
| cs2                | Engine version                          | Example: "6.2.3027"  |
| cs5Label           | Corresponding label for the "cs5" field | Example: "ActionResult"  |
| cs5                | Action                                  | Example: "Reboot system successfully"<br><br>For more information, see <a href="#">Action Mapping Table on page F-73</a> . |
| cs6Label           | Corresponding label for the "cs6" field | Example: "PatternVersion"  |
| cs6                | Pattern version                         | Example: "1297"  |
| cat                | Log type                                | Example: "1727"  |

| CEF KEY          | DESCRIPTION                              | VALUE  |
|------------------|--|--|
| dvchost          | Endpoint host name                       | Example: "ApexOneClient01"   |
| deviceExternalId | ID                                       | Example: "3"   |
| fname            | Resource                                 | Example: "F:\Malware\psas\<br>\rsrc2.bin"  |
| filePath         | Resource                                 | Example: "F:\Malware\psas\<br>\rsrc2.bin"  |
| dhost            | Endpoint host name                       | Example: "ApexOneClient01"   |
| dst              | Endpoint IPv4 address                    | Example: "50.8.1.1"  |
| c6a3Label        | Corresponding label for the "c6a3" field | Example: "SLP_DestinationIP"   |
| c6a3             | Endpoint IPv6 address                    | Example:<br>"fe80::38ca:cd15:443c:40bb%11"   |
| fileHash         | File SHA-1                               | Example:<br>"D6712CAE5EC821F910E1494515<br>3AE7871AA536CA"   |
| deviceFacility   | Product                                  | Example: "Apex One"  |
| duser            | User name                                | Example: "Admin004"  |
| cn2Label         | Corresponding label for the "cn2" field  | Example: "Scan_Type"   |
| cn2              | Scan type                                | Example: "Scan Now"<br><br>For more information, see<br><a href="#">Spyware/Grayware Scan Type Mapping Table on page F-75.</a> |
| cn3Label         | Corresponding label for the "cn3" field  | Example: "Security_Threat_Type"  |

| CEF KEY             | DESCRIPTION                                | VALUE  |
|---------------------|--|--|
| cn3                 | Security threat type                       | Example: "Adware"<br><br>For more information, see <a href="#">Spyware/Grayware Risk Type Mapping Table on page F-76</a> . |
| deviceNtDomain      | Active Directory domain                    | Example: APEXTMCM  |
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1   |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName   |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3  |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019  |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMdevicePlatform  | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1   |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|Spyware Detected|Spyware Detected|3|deviceExternalId=3 rt=Oct 06 2017 08:39:46 GMT +00:00 cnt=1 dhost=ApexOneClient01 cn1Label=PatternType cn1=1073741840 cs1Label=VirusName cs1=ADW_OPENCANDY cs2Label=EngineVersion cs2=6.2.3027 cs5Label=ActionResult cs5=Reboot system successfully cs6Label=PatternVersion cs6=1297 cat=1727 dvchost=ApexOneClient01 fname=F:\\Malware\\psas\\rsrc2.bin filePath=F:\\Malware\\psas\\rsrc2.bin dst=50.8.1.1 deviceFacility=Apex One deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDetectedHost=ApexOneClient01 TMCMLogDetectedIP=50.8.1.1 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-
```



9CDE11EB-D4B8-F51F-C697 TCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1

## Action Mapping Table

| VALUE | DESCRIPTION   |
|-------|---|
| 0     | Unknown   |
| 1     | N/A   |
| 21    | File cleaned  |
| 22    | File deleted  |
| 23    | File quarantined  |
| 24    | File renamed  |
| 25    | File passed   |
| 26    | Unable to clean file. Passed                                    |
| 27    | Unable to clean file. File deleted                              |
| 28    | Unable to clean file. File renamed                              |
| 29    | Unable to clean file. File quarantined                          |
| 31    | Unable to clean file. File deleted                              |
| 32    | File replaced   |
| 34    | File archived   |
| 35    | Blocked successfully  |
| 36    | Quarantined successfully  |
| 37    | Added additional information to email message body successfully |
| 38    | File uploaded   |
| 39    | Unable to clean file. File quarantined                          |

| VALUE | DESCRIPTION  |
|-------|--|
| 40    | Unable to clean file. Passed   |
| 41    | Access denied  |
| 42    | No action  |
| 43    | System rebooted  |
| 44    | Spyware/Grayware unsafe to clean   |
| 45    | Scan manually stopped successfully   |
| 46    | Email message redirected for approval successfully   |
| 81    | Encrypted  |
| 121   | Unable to clean file   |
| 122   | Unable to delete file  |
| 123   | Unable to quarantine file  |
| 124   | Unable to rename file  |
| 125   | Unable to pass file  |
| 126   | Unable to clean or pass file   |
| 127   | Unable to clean or delete file   |
| 128   | Unable to clean or rename file   |
| 129   | Unable to clean or quarantine file   |
| 130   | Unable to delete attachment  |
| 131   | Unable to clean or delete attachment   |
| 132   | One of the following: <ul style="list-style-type: none"><li>• Unable to replace file content</li><li>• Attachment name matched a content rule and the name changed</li></ul> |
| 134   | Unable to archive file   |

| VALUE | DESCRIPTION   |
|-------|---|
| 135   | Unable to block file  |
| 136   | Unable to quarantine file   |
| 137   | Unable to add additional information to email message body  |
| 138   | Unable to upload file   |
| 139   | Unable to clean or quarantine file  |
| 140   | Unable to clean or pass file  |
| 141   | Unable to deny access   |
| 142   | Unable to perform no action   |
| 143   | Action required - Restart the endpoint to finish cleaning the security threat   |
| 144   | Undefined   |
| 145   | Unable to stop scan manually  |
| 146   | Unable to redirect mail for approval  |
| 201   | Action required - Perform a full system scan  |
| 202   | Action required - Use the "Rescue Disk" tool in the OfficeScan  |
| 203   | Action required - Use the "Rootkit Buster" tool in the OfficeScan ToolBox to remove this threat. If the problem persists, contact Support |
| 204   | Action required - Use the "Clean Boot" tool in the OfficeScan ToolBox to remove this threat. If the problem persists, contact Support     |

### Spyware/Grayware Scan Type Mapping Table

| VALUE | DESCRIPTION |
|-------|-------------|
| 0     | Unknown     |
| 1     | N/A         |

| VALUE | DESCRIPTION             |
|-------|-------------------------|
| 11    | Real-time Scan          |
| 12    | Manual Scan             |
| 13    | Scheduled Scan          |
| 14    | Real-time Mail Scan     |
| 15    | Real-time Database Scan |
| 16    | Scan Now                |
| 17    | Card Scan               |
| 18    | Damage Cleanup Services |
| 19    | Storage Scan            |

### Spyware/Grayware Risk Type Mapping Table

| VALUE | DESCRIPTION  |
|-------|--------------|
| 0     | Unknown      |
| 1     | Trackware    |
| 2     | Adware       |
| 3     | Cookie       |
| 4     | Dialer       |
| 5     | Security low |
| 6     | General      |
| 7     | Key logger   |
| 8     | Trojan       |
| 9     | Suspect      |
| 10    | Hijack       |

| VALUE | DESCRIPTION                 |
|-------|-----------------------------|
| 11    | Parasite                    |
| 12    | Browser Helper Object (BHO) |
| 13    | LSP                         |
| 15    | URL shortcut                |
| 16    | Peer-to-Peer application    |
| 17    | Worm                        |
| 19    | Downloader                  |
| 20    | Virus                       |
| 21    | Eulaware                    |
| 22    | Variant                     |
| 23    | Security medium             |
| 24    | Security high               |
| 25    | Vulnerability Assessment    |

## CEF Suspicious File Logs

| CEF KEY            | DESCRIPTION        | VALUE            |
|--------------------|--------------------|------------------|
| Header (logVer)    | CEF format version | CEF:0            |
| Header (vendor)    | Appliance vendor   | Trend Micro      |
| Header (pname)     | Appliance product  | Apex Central     |
| Header (pver)      | Appliance version  | 2019             |
| Header (eventid)   | FH:Action          | FH:Log           |
| Header (eventName) | Name               | Suspicious Files |
| Header (severity)  | Severity           | 3                |

| CEF KEY          | DESCRIPTION                              | VALUE   |
|------------------|--|---|
| deviceExternalId | ID                                       | Example: "1"  |
| cat              | Log type                                 | Example: "1766"   |
| deviceFacility   | Product                                  | Example: "Apex One"   |
| cn1Label         | Corresponding label for the "cn1" field  | Example: "SLF_ProductVersion"   |
| cn1              | Product version                          | Example: "11"   |
| rt               | Event trigger time in UTC                | Example: "Mar 22 2018 08:23:23 GMT+00:00"   |
| dst              | Endpoint IPv4 address                    | Example: "10.201.86.151"  |
| c6a3Label        | Corresponding label for the "c6a3" field | Example: "Endpoint IPv6 Address"  |
| c6a3             | Endpoint IPv6 address                    | Example:<br>"2620:101:4003:7a0:fd4b:52ed:53bd:ae3d"   |
| dhost            | Endpoint host name                       | Example: "APEX-ONE-CLIENT-1"  |
| cs2Label         | Corresponding label for the "cs2" field  | Example: "SLF_TrueFileType"   |
| cs2              | File type                                | Example: "TEXT"   |
| fileHash         | File SHA-1                               | Example:<br>"D6712CAE5EC821F910E14945153AE7871AA536CA"  |
| cs3Label         | Corresponding label for the "cs3" field  | Example: "SLF_FileSource"   |
| cs3              | File path                                | Example: "C:\\Users\\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\017545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE" |

| CEF KEY        | DESCRIPTION                             | VALUE  |
|----------------|---|--|
| cn2Label       | Corresponding label for the “cn2” field | Example: “SLF_SourceType”  |
| cn2            | C&C list source                         | Example: “0” <ul style="list-style-type: none"> <li>• 0: Sandbox</li> <li>• 1: User-defined</li> </ul>   |
| act            | Action                                  | Example: “Log” <ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 2: Block</li> <li>• 3: Quarantine</li> </ul>   |
| cn3Label       | Corresponding label for the “cn3” field | Example: “SLF_ScanType”  |
| cn3            | Scan type                               | Example: “1” <ul style="list-style-type: none"> <li>• 1: Scheduled scan</li> <li>• 2: Manual scan</li> <li>• 3: Scan now</li> <li>• 4: Real-time scan</li> </ul>   |
| reason         | Critical threat type                    | Example: “E” <ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| deviceNtDomain | Active Directory domain                 | Example: APEXTMCM  |
| dntdom         | Apex One domain hierarchy               | Example: OSCEDomain1   |

| CEF KEY             | DESCRIPTION                                | VALUE  |
|---------------------|--|--|
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName                           |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3                                  |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019                            |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMDevicePlatform  | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1 |

### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|FH:Log|Suspicious File
s|3|deviceExternalId=1 rt=Nov 15 2016 02:47:21 GMT+00:00 cat
=1766 deviceFacility=Apex One cn1Label=SLF_ProductVersion cn
1=11 dst=10.201.86.151 dhost=APEX-ONE-CLIENT-1 cs2Label=SLF_
TrueFileType cs2=SLF_TrueFileType fileHash=D6712CAE5EC821F91
0E14945153AE7871AA536CA cs3Label=SLF_FileSource cs3=C:\\User
s\\Administrator\\Desktop\\BT-SHA1-SAMPLE\\BT-SHA1-SAMPLE\\@
17545113A434757C5F0F13095DBBF138BD76A40;0x36D572AE cn2Label=
SLF_SourceType cn2=0 act=Log cn3Label=SLF_ScanType cn3=1 rea
son=E deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TMCMLogDete
ctedHost=APEX-ONE-CLIENT-1 TMCMLogDetectedIP=10.201.86.151
ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-
9CDE11EB-D4B8-F51F-C697 TCMDevicePlatform=Windows 7 6.1 (Bu
ild 7601) Service Pack 1
```




## CEF Virus/Malware Logs

| CEF KEY            | DESCRIPTION                             | VALUE  |
|--------------------|---|--|
| Header (logVer)    | CEF format version                      | CEF:0  |
| Header (vendor)    | Appliance vendor                        | Trend Micro  |
| Header (pname)     | Appliance product                       | Apex Central   |
| Header (pver)      | Appliance version                       | 2019   |
| Header (eventid)   | AV:Action                               | AV:File renamed  |
| Header (eventName) | Virus/Malware name                      | JS_EXPLOIT.SMDN  |
| Header (severity)  | Severity                                | 3  |
| cnt                | Detections                              | Example: "10"  |
| dhost              | Endpoint                                | Example: "ApexOneClient01"   |
| duser              | User                                    | Example: "Admin004"  |
| act                | Action                                  | Example: "File renamed"<br>For more information, see <a href="#">Action Mapping Table on page F-73</a> . |
| rt                 | Log generation time in UTC              | Example: Oct 06 2017 08:39:46 GMT+00:00  |
| cn1Label           | Corresponding label for the "cn1" field | Example: "VLF_PatternNumber"   |
| cn1                | Pattern/Rule version                    | Example: "920500"  |
| cn2Label           | Corresponding label for the "cn2" field | Example: "VLF_SecondAction"  |
| cn2                | Second action                           | Example: "3"<br>For more information, see <a href="#">Second Action Mapping Table on page F-85</a> .     |

| CEF KEY  | DESCRIPTION                             | VALUE  |
|----------|---|--|
| cs1Label | Corresponding label for the “cs1” field | Example: “VLF_FunctionCode”  |
| cs1      | Scan type                               | Example: “Manual Scan” <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: N/A</li> <li>• 11: Real-time Scan</li> <li>• 12: Manual Scan</li> <li>• 13: Scheduled Scan</li> <li>• 16: Scan Now</li> <li>• 17: Card Scan</li> <li>• 18: Damage Cleanup Services</li> <li>• 19: Storage Scan</li> </ul> |
| cs2Label | Corresponding label for the “cs2” field | Example: “VLF_EngineVersion”   |
| cs2      | Engine version                          | Example: “9.500.1005”  |
| cs3Label | Corresponding label for the “cs3” field | Example: “CLF_ProductVersion”  |
| cs3      | Product version                         | Example: “11”  |
| cs4Label | Corresponding label for the “cs4” field | Example: “CLF_ReasonCode”  |
| cs4      | Reason code                             | Example: “virus log”   |
| cs5Label | Corresponding label for the “cs5” field | Example: “VLF_FirstActionResult”   |
| cs5      | First action result                     | Example: “Unable to clean file”<br>For more information, see <a href="#">Action Mapping Table on page F-73</a> .   |

| CEF KEY          | DESCRIPTION                             | VALUE  |
|------------------|---|--|
| cs6Label         | Corresponding label for the “cs6” field | Example: “Second Action Result”  |
| cs6              | Second action result                    | Example: “Unable to clean file. Passed”<br><br>For more information, see <a href="#">Action Mapping Table on page F-73</a> .   |
| cat              | Log type                                | Example: “1703”  |
| dvchost          | Product server name                     | Example: “ApexOneServer01”   |
| cn3Label         | Corresponding label for the “cn3” field | Example: “CLF_SeverityCode”  |
| cn3              | Severity code                           | Example: “2” <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Information</li> <li>• 2: Warning</li> <li>• 3: Error</li> <li>• 4: Critical</li> </ul> |
| deviceExternalId | ID                                      | Example: “3”   |
| fname            | File                                    | Example: “FakeMalwareRebootDel.exe”  |
| filePath         | File path                               | Example: “C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\Rar \$DR01.046\\”   |
| msg              | File in compressed file                 | Example: “BMAC Schedule of Events.xls”   |

| CEF KEY        | DESCRIPTION   | VALUE   |
|----------------|---|---|
| shost          | Source host, UNC, or email address<br><br> <b>Note</b><br>The system may not include this key in logs. | Example: "xxx@test.com"   |
| dst            | Endpoint IPv4 address   | Example: "50.8.1.1"   |
| c6a3Label      | Corresponding label for the "c6a3" field  | Example: "SLP_DestinationIP"  |
| c6a3           | Endpoint IPv6 address   | Example:<br>"fe80::38ca:cd15:443c:40bb%11"  |
| fileHash       | File SHA-1  | Example:<br>"D6712CAE5EC821F910E14945153AE7871AA536CA"  |
| deviceFacility | Product   | Example: "Apex One"   |
| reason         | Critical threat type  | Example: "E"<br><br><ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| deviceNtDomain | Active Directory domain   | Example: APEXTMCM   |
| dntdom         | Apex One domain hierarchy   | Example: OSCEDomain1  |

Log sample:

```

CEF:0|Trend Micro|Apex Central|2019|AV:File renamed|JS_EXP
LOIT.SMDN|3|deviceExternalId=104 rt=Feb 18 2016 14:34:00 G
MT+00:00 cnt=1 dhost=ApexOneClient01 duser=Admin004 act=Fi
le renamed cn1Label=VLF_PatternNumber cn1=920500 cn2Label=
VLF_SecondAction cn2=3 cs1Label=VLF_FunctionCode cs1=Manua
l Scan cs2Label=VLF_EngineVersion cs2=9.500.1005 cs3Label=
CLF_ProductVersion cs3=10.6 cs4Label=CLF_ReasonCode cs4=vi
rus log cs5Label=VLF_FirstActionResult cs5=File renamed cs
6Label=VLF_SecondActionResult cs6=N/A cat=1703 dvchost=Ape
xOneServer01 cn3Label=CLF_ServerityCode cn3=2 fname=0348C6
93056617D34FC5B5BAB4643885FEE5FEDF;0xD5D56AC2 filePath=C:\
\Users\Administrator\Desktop\trend_test_virus\Trojans\
\msg=BMAC Schedule of Events.xls shost=xxx@test.com dst=1
0.201.129.24 devic eFacility=Apex One reason=B deviceNtDom
ain=APEXTMCM dntdom=0 SCEDomain1 ApexCentralHost=TW-CHRIS-
W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697

```

## Second Action Mapping Table

| VALUE | DESCRIPTION |
|-------|-------------|
| 0     | Unknown     |
| 1     | N/A         |
| 2     | Clean       |
| 3     | Delete      |
| 4     | Move        |
| 5     | Rename      |
| 6     | Pass/Log    |
| 7     | Strip       |
| 8     | Drop        |

| VALUE | DESCRIPTION                |
|-------|----------------------------|
| 9     | Quarantine                 |
| 10    | Insert/Replace             |
| 11    | Archive                    |
| 12    | Stamp                      |
| 13    | Block                      |
| 14    | Redirect mail for approval |
| 81    | Encrypted                  |
| 90    | Detect                     |
| 257   | Reset                      |

## CEF Web Security Logs

| CEF KEY            | DESCRIPTION                               | VALUE   |
|--------------------|---|---|
| Header (logVer)    | CEF format version                        | CEF:0   |
| Header (vendor)    | Appliance vendor                          | Trend Micro   |
| Header (pname)     | Appliance product                         | Apex Central  |
| Header (pver)      | Appliance version                         | 2019  |
| Header (eventid)   | WB:Filter/Blocking Type                   | WB:1  |
| Header (eventName) | “Blocking Rule” or “Filter/Blocking Type” | 5   |
| Header (severity)  | Severity                                  | 3   |
| app                | Protocol                                  | Example: “3”<br><br>For more information, see <a href="#">Protocol Mapping Table on page F-93</a> . |

| CEF KEY   | DESCRIPTION                              | VALUE  |
|-----------|--|--|
| cnt       | Detections                               | Example: "10"  |
| dpt       | Server port                              | Example: "80"  |
| act       | Action                                   | Example: "0" <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Pass</li> <li>• 2: Block</li> <li>• 3: Monitor</li> <li>• 4: Delete</li> <li>• 5: Quarantine</li> <li>• 6: Warn</li> <li>• 7: Warn and continue</li> <li>• 8: Override</li> </ul> |
| rt        | Event trigger time in UTC                | Example: "Mar 22 2018 08:23:23 GMT+00:00"  |
| src       | Endpoint IPv4 address                    | Example: "10.1.128.34"   |
| c6a2Label | Corresponding label for the "c6a2" field | Example: "SLF_SourceIP"  |
| c6a2      | Endpoint IPv6 address                    | Example: "2620:101:4003:7a0:fd4b:52ed:53bd:ae3d"   |
| cs1Label  | Corresponding label for the "cs1" field  | Example: "SLF_PolicyName"  |
| cs1       | Policy                                   | Example: "External User Policy"  |
| cs4Label  | Corresponding label for the "cs4" field  | Example: "CLF_ReasonCode"  |
| cs4       | Reason Code                              | Example: "access"  |

| CEF KEY          | DESCRIPTION                             | VALUE  |
|------------------|---|--|
| cs5Label         | Corresponding label for the “cs5” field | Example:<br>“CLF_ReasonCodeSource”   |
| cs5              | Reason code source                      | Example: “web”   |
| deviceDirection  | Traffic/Connection                      | Example: “2” <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Inbound</li> <li>• 2: Outbound</li> </ul>  |
| cat              | Filter/Blocking Type                    | Example: “7”<br><br>For more information, see <a href="#">Filter/Blocking Type Mapping Table on page F-91</a> .  |
| dvchost          | Endpoint host name                      | Example: “ApexOneClient08”   |
| cn1Label         | Corresponding label for the “cn1” field | Example: “CLF_SeverityCode”  |
| cn1              | Severity code                           | Example: “0” <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Information</li> <li>• 2: Warning</li> <li>• 3: Error</li> <li>• 4: Critical</li> </ul> |
| deviceExternalId | ID                                      | Example: “38”  |
| fname            | File                                    | Example: “test.txt”  |
| request          | URL                                     | Example: “http://<br>www.violetsoft.net/counter/<br>insert.php?dbserver<br>\=db1&c_pcode\=25&c_pid<br>\=funpop1&c_kind\=4&c_mac<br>\=FE-ED-BE-EF-0C-E1”                |



| CEF KEY           | DESCRIPTION                             | VALUE  |
|-------------------|---|--|
| deviceFacility    | Product                                 | Example: "Apex One"  |
| duser             | User name                               | Example: "Admin004"  |
| shost             | Client host name                        | Example: "ABC-HOST-WKS12"  |
| cs2Label          | Corresponding label for the "cs2" field | Example: "Blocking_Rule"   |
| cs2               | Blocking rule                           | Example: "content filter"  |
| deviceProcessName | Process name                            | Example: "C:\\Windows\\system32\\svchost-1.exe"  |
| cn3Label          | Corresponding label for the "cn3" field | Example: "ReputationScore"   |
| cn3               | Reputation score                        | Example: "49"  |
| dst               | Server IP address                       | Example: "10.69.81.64"   |
| cn2Label          | Corresponding label for the "cn2" field | Example: "SLF_SeverityLevel"   |
| cn2               | Severity level                          | Example: "100" <ul style="list-style-type: none"> <li>• 100: High</li> <li>• 300: Medium high</li> <li>• 500: Medium</li> <li>• 700: Medium low</li> <li>• 900: Low</li> </ul> |

| CEF KEY             | DESCRIPTION                                | VALUE  |
|---------------------|--|--|
| reason              | Critical threat type                       | Example: "E" <ul style="list-style-type: none"> <li>• A: Known Advanced Persistent Threat (APT)</li> <li>• B: Social engineering attack</li> <li>• C: Vulnerability attack</li> <li>• D: Lateral movement</li> <li>• E: Unknown threats</li> <li>• F: C&amp;C callback</li> <li>• G: Ransomware</li> </ul> |
| deviceNtDomain      | Active Directory domain                    | Example: APEXTMCM  |
| dntdom              | Apex One domain hierarchy                  | Example: OSCEDomain1   |
| TMCMLogDetectedHost | Endpoint name where the log event occurred | Example: MachineHostName   |
| TMCMLogDetectedIP   | IP address where the log event occurred    | Example: 10.1.2.3  |
| ApexCentralHost     | Apex Central host name                     | Example: TW-CHRIS-W2019  |
| devicePayloadId     | Unique message GUID                        | Example:<br>1C00290C0360-9CDE11EB-D4B8-F51F-C697   |
| TMCMdevicePlatform  | Endpoint operating system                  | Example: Windows 7 6.1 (Build 7601) Service Pack 1   |

#### Log sample:

```
CEF:0|Trend Micro|Apex Central|2019|WB:7|7|3|deviceExternalId=38 rt=Nov 15 2017 08:43:57 GMT+00:00 app=17 cntLabel=AggregatedCount cnt=1 dpt=80 act=1 src=10.1.128.46 cs1Label=SLF_PolicyName cs1=External User Policy deviceDirection=2 cat=7 dvchost=ApexOneClient08 fname=test.txt request=http://www.violetsoft.net/counter/insert.php?dbserver\=db1&c_pcode\=25&c
```

```
_pid\=funpop1&c_kind\=4&c_mac\=FE-ED-BE-EF-0C-E1 deviceFacility=Apex One shost=ABC-HOST-WKS12 reason=G deviceNtDomain=APEXTMCM dntdom=OSCEDomain1 TCMLogDetectedHost=ABC-HOST-WKS12 TCMLogDetectedIP=10.1.128.46 ApexCentralHost=TW-CHRIS-W2019 devicePayloadId=1C00290C0360-9CDE11EB-D4B8-F51F-C697 TCMdevicePlatform=Windows 7 6.1 (Build 7601) Service Pack 1
```

## Filter/Blocking Type Mapping Table

| VALUE | DESCRIPTION                       |
|-------|-----------------------------------|
| 0     | Unknown                           |
| 1     | File name                         |
| 2     | Webmail site                      |
| 3     | Web server                        |
| 4     | URL pattern                       |
| 5     | Java/VB script                    |
| 6     | True file type                    |
| 7     | User-defined                      |
| 8     | Server-defined                    |
| 9     | Web policy                        |
| 11    | Phishing                          |
| 12    | Phishing/Spyware/Grayware         |
| 13    | Phishing/Virus/Malware accomplice |
| 14    | Phishing/Forged signature         |
| 15    | Phishing/Disease vector           |
| 16    | Phishing/Malicious applet         |
| 17    | Phishing reputation               |

| VALUE | DESCRIPTION                       |
|-------|-----------------------------------|
| 20    | IP translation policy             |
| 21    | Java scanning policy              |
| 22    | Malicious mobile code policy      |
| 31    | Pharming                          |
| 32    | URL blocking                      |
| 33    | URL filtering                     |
| 34    | Client IP blocking                |
| 35    | Destination port blocking         |
| 36    | Web reputation                    |
| 41    | Unsupported file type             |
| 42    | Exceeds total file count limit    |
| 43    | Exceeds file size limit           |
| 44    | Exceeds decompression layer limit |
| 45    | Exceeds decompression time frame  |
| 46    | Exceeds compression ratio limit   |
| 47    | Password protected file           |
| 48    | Restricted spyware/grayware type  |
| 60    | String pattern                    |
| 70    | HTTP inspection                   |
| -1    | Virus/Malware                     |
| -2    | Spyware/Grayware                  |
| -3    | Network virus                     |
| -4    | IntelliTrap                       |

| VALUE | DESCRIPTION                 |
|-------|-----------------------------|
| -5    | Suspicious virus/malware    |
| -6    | Suspicious spyware/grayware |
| -7    | Fraud                       |
| -8    | Suspicious behavior         |

## Protocol Mapping Table

| VALUE | DESCRIPTION                  |
|-------|------------------------------|
| 0     | Unknown                      |
| 1     | SMTP                         |
| 2     | POP3                         |
| 3     | IRC                          |
| 4     | DNS Response                 |
| 5     | HTTP                         |
| 6     | FTP                          |
| 7     | TFTP                         |
| 8     | SMB                          |
| 9     | Windows Live Messenger (MSN) |
| 10    | AIM                          |
| 11    | Yahoo! Messenger             |
| 12    | Gmail                        |
| 13    | Yahoo! Mail                  |
| 14    | Windows Live Hotmail         |
| 15    | RDP                          |

| VALUE | DESCRIPTION       |
|-------|-------------------|
| 16    | DHCP              |
| 17    | Telnet            |
| 18    | LDAP              |
| 19    | File transfer     |
| 20    | SSH               |
| 21    | Dameware          |
| 22    | VNC               |
| 23    | Cisco Telnet      |
| 24    | Kerberos          |
| 25    | DCE RPC           |
| 26    | SQL               |
| 27    | pcAnywhere        |
| 28    | ICMP              |
| 29    | SNMP              |
| 30    | Virus pattern TCP |
| 31    | Virus pattern UDP |
| 32    | HTTPS             |
| 33    | SMB2              |
| 34    | MMS               |
| 35    | IMAP4             |
| 36    | RADIUS            |
| 37    | Radmin            |
| 38    | FTP_Response      |

| VALUE | DESCRIPTION   |
|-------|---------------|
| 48    | RTSP/RTP-UDP  |
| 49    | RTSP/RTP-TCP  |
| 50    | RTSP/RDT-UDP  |
| 51    | RTSP/RDT-TCP  |
| 52    | WMSP          |
| 53    | SHOUTCast     |
| 54    | RTMP          |
| 68    | DNS Request   |
| 256   | BitTorrent    |
| 257   | Kazaa         |
| 258   | Limewire      |
| 259   | Bearshare     |
| 260   | Bluester      |
| 261   | Edonkey emule |
| 262   | Edonkey2000   |
| 263   | Filezilla     |
| 264   | Guncleus      |
| 265   | Gnutella      |
| 266   | Winnie        |
| 267   | Napster       |
| 268   | Morpheus      |
| 269   | Napster       |
| 270   | Shareaza      |

| VALUE | DESCRIPTION       |
|-------|-------------------|
| 271   | WinMX             |
| 272   | Mldonkey          |
| 273   | Direct Connect    |
| 274   | Soulseek          |
| 275   | OpenAP            |
| 276   | Kuro              |
| 277   | Imesh             |
| 278   | Skype             |
| 279   | Google Talk       |
| 317   | Cabos             |
| 318   | Zultrax           |
| 319   | Foxy              |
| 320   | eDonkey           |
| 321   | Ares              |
| 322   | Miranda           |
| 323   | Kceasy            |
| 324   | MoodAmp           |
| 325   | Deepnet Explorer  |
| 326   | FreeWire          |
| 327   | Gimme             |
| 328   | GnucDNA GWebCache |
| 329   | Jubster           |
| 330   | MyNapster         |



| VALUE | DESCRIPTION           |
|-------|-----------------------|
| 331   | Nova GWebCache        |
| 332   | Swapper GWebCache     |
| 333   | Xnap                  |
| 334   | Xolox                 |
| 335   | Ppstream              |
| 640   | AIM Express           |
| 641   | Chikka SMS Messenger  |
| 642   | eBuddy                |
| 643   | ICQ2Go                |
| 644   | ILoveIM Web Messenger |
| 645   | IMUnitive             |
| 646   | Mabber                |
| 647   | Meebo                 |
| 648   | Yahoo! Web Messenger  |
| 848   | SIP2                  |
| 1024  | GPass                 |
| 10001 | IP                    |
| 10002 | ARP                   |
| 10003 | TCP                   |
| 10004 | UDP                   |
| 10005 | IGMP                  |
| 60    | ORACLE                |
| 44    | MySQL                 |

| <b>VALUE</b> | <b>DESCRIPTION</b> |
|--------------|--------------------|
| 520          | MSSQL              |
| 337          | Postgres           |
| 41           | ICMPv6             |
| 10006        | GGP                |
| 10007        | PUP                |
| 10008        | IDP                |
| 10009        | ND                 |
| 10010        | RAW                |

# Index

## A

- access rights, 4-9
- account management
  - user roles
    - default user roles, 4-17
    - editing, 4-22
- accounts
  - my account, 4-14
- activating
  - Apex Central, 5-2
  - managed products, 5-4, 5-6
- Activation Code, 5-2
- Active Directory
  - connection settings, 6-2
  - integration, 6-2
  - manual synchronization, 6-2
  - reporting lines, 6-14
  - sites, 6-12
  - synchronization frequency, 6-2
  - troubleshoot connection issues, 6-5
- adding
  - Active Directory groups, 4-5
  - Active Directory users, 4-5
  - managed servers, 9-5
  - user accounts, 4-5
- administering
  - Managed Detection and Response, 22-2
- administration
  - adding managed servers, 9-5
  - cloud service settings, 9-10
  - deleting managed servers, 9-8
  - editing managed servers, 9-7
  - managed servers, 9-2
  - stop managing cloud services, 9-10
- advanced search
  - User/Endpoint Directory, 7-24, 22-18
- agent
  - Threat Investigation Center, 22-20
- Agent Migration tool, 26-2
- Antivirus Pattern, 6-6
- Antivirus Pattern Compliance
  - indicator settings, 6-8
- Apex Central, 1-2, 1-8
  - about, 1-2
  - activating, 5-2
  - database tables, 25-4
  - license information, 5-2
  - mail server, 1-8
  - managed products, 11-2
  - MCP, 1-8
  - Product Directory, 11-2
  - report server, 1-8
  - SQL database, 1-8
  - web-based management console, 1-9
  - web server, 1-8
  - web service integration, 1-8
  - widget framework, 1-9
- Apex Central server
  - web console, 2-2, 2-3
- Apex One
  - Security Agent, 10-2
- Apex One (Mac)
  - Security Agent, 10-2
- approved tasks, 22-12

approving tasks, 22-7

auditing logs, 19-5

Automated Analyses, 22-15

## B

bar charts, 18-8

browsing targets, 14-9

## C

case handling, 7-8, 7-15

CEF syslog mapping

Attack Discovery Detections, F-3

Behavior Monitoring, F-9

C&C Callback, F-15

Content Security, F-20

Data Loss Prevention, F-28

Device Access Control, F-36

Endpoint Application Control,  
F-43

Engine Update Status, F-46

Intrusion Prevention Logs, F-48

Managed Product Logon/Logoff  
Events, F-51

Network Content Inspection, F-52

Pattern Update Status, F-56

Predictive Machine Learning, F-59

Product Auditing Events, F-64

Sandbox Detection Logs, F-65

Spyware/Grayware, F-69

Suspicious File, F-77

Virtual Analyzer, F-65

Virus/Malware, F-81

Web Security, F-86

checklist

ports, A-3

server address, A-2

cloud service configuration, 9-10

Command Details, 13-4, 22-18

Command Tracking, 13-2

Command Details, 13-4, 22-18

Managed Detection and

Response, 22-16

querying, 13-3

viewing, 13-3

compliance indicator, 6-6

compliance tab, 3-33

component list, 12-2

component update notification, 12-3

component updates, 12-2, 12-8

deployment plan, 12-3

deployment schedule, 12-3

proxy settings, 12-12

scheduled, 12-4

update notification, 12-3

condition statements, 15-30

configure

log aggregation, 16-14

configuring

managed products, 11-9

configuring proxy settings

managed server list, 9-9

contact groups, 17-6

adding, 17-6, 17-7

editing, 17-8

removing, 17-6

Control Manager, 1-1

about, 1-1

notifications, 17-3

copying policy settings, 14-12

creating

auditing logs, 19-5

creating policies, 14-2, 14-17

- copying settings, 14-12
  - settings, 14-3
  - criteria
    - customized expressions, 15-18, 15-19
    - keywords, 15-26, 15-27
  - customized expressions, 15-18, 15-19, 15-21
    - criteria, 15-18, 15-19
    - importing, 15-21
  - customized keywords, 15-25
    - criteria, 15-26, 15-27
    - importing, 15-29
  - customized templates, 15-30
    - creating, 15-31
    - importing, 15-33
  - custom templates, 18-2
- D**
- dashboard
    - tabs, 3-2
      - adding, 3-2
      - deleting, 3-3
      - renaming, 3-2
      - slide show, 3-2
      - summary, 3-17
    - widgets, 3-2
      - adding, 3-4
      - modifying product scope, 3-5
      - moving, 3-4
  - database tables, 25-4
  - data identifiers, 15-16
    - expressions, 15-16
    - file attributes, 15-16
    - keywords, 15-16
  - Data Loss Prevention, 15-16
    - compliance indicator, 6-6
    - data identifiers, 15-16
    - DLP Compliance Officer, 19-3
    - DLP Incident Reviewer, 19-3
    - expressions, 15-17-15-19, 15-21
    - file attributes, 15-21-15-23
    - Incident Information list, 19-6
    - incident investigation, 19-1, 19-6
      - administrator tasks, 19-2
      - auditing logs, 19-5
      - DLP Compliance Officer, 19-3
      - DLP Incident Reviewer, 19-3
      - exporting incident details, 19-6
      - notifications, 19-5
    - keywords, 15-23-15-27, 15-29
    - templates, 15-29-15-31, 15-33
  - Data Loss Prevention (DLP), 15-15
  - Data Loss Prevention Compliance indicator settings, 6-10
  - data views
    - product information, B-93
    - security threat information, B-2
  - DBConfig tool, 26-2
  - default user roles, 4-17
  - deleting
    - logs, 16-20
    - user accounts, 4-2
  - deleting managed servers, 9-8
  - deleting policies, 14-18
  - deployed targets, 14-22
  - deployment plans, 12-3
  - Directory Management, 11-11, 11-13
  - disabling
    - syslog forwarding, 16-18
    - user accounts, 4-4

- DLP, 15-15
- DLP Incident Reviewer, 19-6
  - Incident Information list, 19-6
- documentation, 2
- documentation feedback, 27-5
- draft policies, 14-3

## E

- editing
  - user accounts, 4-11
  - user roles, 4-22
- editing managed servers, 9-7
- editing policies, 14-15
- email, 17-3
- enabling
  - syslog forwarding, 16-14
  - user accounts, 4-3
- endpoint details, 7-10
  - tabular view, 7-10
  - timeline view, 7-10
- Endpoint grouping, 6-11
- enrollment token, 8-1
- exporting
  - DLP incident details, 19-6
- expressions, 15-16, 15-17
  - customized, 15-18, 15-21
    - criteria, 15-18, 15-19
  - predefined, 15-17

## F

- file attributes, 15-16, 15-21–15-23
  - creating, 15-22
  - importing, 15-23
  - wildcards, 15-22
- filter by criteria, 14-3
- filtered policies

- reordering, 14-23

## I

- incident details updated notification, 19-5
- Incident Information list, 19-6
- investigating DLP incidents, 19-1, 19-6
  - administrator tasks, 19-2
  - auditing logs, 19-5
  - DLP Compliance Officer, 19-3
  - DLP Incident Reviewer, 19-3
  - exporting incident details, 19-6
  - Incident Information list, 19-6
  - notifications, 19-5
- investigation tasks
  - approving, 22-7
  - rejecting, 22-7
  - statuses, 22-13
  - tracking, 22-12

## K

- keywords, 15-16, 15-23
  - customized, 15-25–15-27, 15-29
  - predefined, 15-24, 15-25

## L

- license information, 5-2
  - renewing, 5-2
  - viewing, 5-2
- license management
  - details, 5-4
  - managed products, 5-4
- License Management, 5-2
- license updates
  - proxy settings, 12-12
- logging off, 2-7

- logging on, 2-6
  - locally, 2-6
  - remotely, 2-6
- logging on with domain credentials, 2-6
- logical operators, 15-30
- log maintenance, 16-20
- Log On with Domain Credentials button, 2-7
- log query, 16-2
- logs, 16-1, 16-2
  - configure log aggregation, 16-14
  - deleting, 16-20
  - querying, 16-2
- M**
- Managed Detection and Response
  - Automated Analyses, 22-15
  - Command Tracking, 22-16
  - Pending Tasks, 22-7
  - Task Tracking, 22-13
  - Threat Investigation Center tasks, 22-10
- Managed Detection and Response Service
  - resuming, 22-3, 22-6
  - suspending, 22-3, 22-6
- managed products, 11-2
  - activating, 5-4, 5-6
  - configuring, 11-9
  - deploying components, 11-8
  - issue tasks, 11-8
  - license management, 5-4
  - registering, 5-4, 5-7
  - viewing logs, 11-10
- managed server list
  - configuring proxy settings, 9-9
- managed servers, 9-2
  - editing servers, 9-7
  - registering, 9-5
  - unregistering, 9-8
- manual component updates, 12-8
- manual update
  - components, 12-2
- MCP, 1-8
- MIB file
  - Apex Central, E-2
  - NVW Enforcer SNMPv2, E-2
- my account, 4-14
- my reports, 18-36
- N**
- notifications, 17-3
  - configuring, 17-3
  - incident details updated, 19-5
  - scheduled incident summary, 19-5
- notifications and reports
  - contact groups
    - adding, 17-7
    - editing, 17-8
- O**
- offline targets, 14-23
- one-time reports, 18-20
  - viewing, 18-24
- P**
- PCRE, 15-18
- pending targets, 14-23
- Pending Tasks, 22-7
- Perle Compatible Regular Expressions, 15-18

pie charts, 18-13

policies

creating, 14-2, 14-17

deleting, 14-18

editing, 14-15

reordering, 14-23

policy list, 14-7, 14-20

policy management, 14-2

changing owners, 14-19

copying policy settings, 14-12

creating policies, 14-2, 14-17

deleting policies, 14-18

deployed targets, 14-22

DLP, 15-15

draft policies, 14-3

editing policies, 14-15

offline targets, 14-23

owner, 14-22

pending targets, 14-23

policy list, 14-7, 14-20

policy priority, 14-9, 14-20

reordering policies, 14-23

settings, 14-3

specified policies, 14-3

targets, 14-22

targets with issues, 14-23

understanding, 14-2

policy priority, 14-20

policy settings

copying, 14-12

policy targets, 14-22

policy types

draft, 14-3

policy priority, 14-20

reordering policies, 14-23

specified, 14-3

port

checklist, A-3

predefined expressions, 15-17

viewing, 15-17

predefined keywords

distance, 15-25

number of keywords, 15-24

predefined templates, 15-30

Product Connector, 8-1

Product Directory, 11-2

managed products, 11-2

managing, 11-11, 11-13

tasks, 11-2

product scope

widgets, 3-5

proxy settings

component updates, 12-12

license updates, 12-12

managed server list, 9-9

syslog forwarding, 12-12

## Q

querying

investigation task commands,

22-16

supported targets, 22-18

## R

registering

managed products, 5-4, 5-7

managed servers, 9-5

Threat Investigation Center, 22-2,

22-3

rejected tasks, 22-12

rejecting tasks, 22-7

reordering policies, 14-23



- reporting lines, 6-14
  - create custom, 6-14
  - merge, 6-15
  - view, 6-14
- report maintenance, 18-36
- reports
  - custom report templates
    - adding, 18-3
  - custom templates, 18-2, 18-3
    - bar charts, 18-8
    - pie charts, 18-13
  - deleting, 18-36
  - formats, 18-22, 18-27, 18-31
    - custom templates, 18-22, 18-27, 18-32
    - static templates, 18-22, 18-27, 18-32
  - my reports, 18-36
  - one-time reports, 18-20, 18-21
  - scheduled reports, 18-25, 18-26, 18-31
  - templates, 16-6, 18-3
  - viewing
    - scheduled reports, 18-35
  - viewing reports
    - one-time reports, 18-24
- report templates
  - custom, 18-3
- resuming
  - Managed Detection and Response, 22-3, 22-6
- reviewing DLP incidents, 19-6
  - Incident Information list, 19-6
- S**
  - scheduled incident summary notification, 19-5
  - scheduled reports, 18-25
    - viewing, 18-35
  - scheduled updates, 12-4
  - schedule update
    - components, 12-2
  - Security Agent, 10-5
    - Apex One, 10-2
    - Apex One (Mac), 10-2
    - downloading, 10-2
    - Windows 10, 10-6
    - Windows 7, 10-4
    - Windows 8.1, 10-5
    - Windows HPC Server 2008 R2, 10-10
    - Windows MultiPoint Server 2010, 10-11
    - Windows MultiPoint Server 2011, 10-12
    - Windows MultiPoint Server 2012, 10-18
    - Windows Server 2008 R2, 10-8
    - Windows Server 2012, 10-14
    - Windows Server 2012 Failover Clusters, 10-19, 10-20
    - Windows Server 2012 R2, 10-15
    - Windows Server 2016, 10-21
    - Windows Server 2016 Failover Clusters, 10-22
    - Windows Server 2019, 10-25
    - Windows Storage Server 2008 R2, 10-9
    - Windows Storage Server 2012, 10-16
    - Windows Storage Server 2012 R2, 10-17
    - Windows Storage Server 2016, 10-23

- security threat details
    - threat status, 7-8, 7-15
  - security threats
    - endpoints, 7-13
    - users, 7-6
  - selecting targets
    - filter by criteria, 14-3
  - server
    - address checklist, A-2
  - server address checklist, A-2
  - server registration, 9-2
    - adding, 9-5
    - cloud service settings, 9-10
    - deleting, 9-8
    - editing, 9-7
    - methods, 9-2
  - setting
    - access rights, 4-9
  - Single sign-on
    - Product Directory, 11-4
    - Server Registration, 9-3
  - sites, 6-12
    - create custom, 6-12
    - merge, 6-13
    - view, 6-12
  - Small Network Management Protocol
    - See SNMP, 17-3
  - SNMP, 17-3
  - specified policies, 14-3
    - priority, 14-9
  - specify targets
    - browsing, 14-9
  - SSO, 9-3, 11-4
  - summary tab, 3-17
  - support
    - resolve issues faster, 27-3
  - supported targets
    - querying, 22-18
  - suspending
    - Managed Detection and Response, 22-3, 22-6
  - syslog forwarding, 16-18
    - disabling, 16-18
    - enabling, 16-14
    - proxy settings, 12-12
  - Syslog Settings, 16-18
    - configuring, 16-14, 16-18
- ## T
- tabs, 3-2
    - compliance, 3-33
    - summary, 3-17
    - Threat Statistics, 3-39
    - widgets, 3-2
  - tabular view
    - endpoint details, 7-10
    - user details, 7-3
  - tags and filters, 7-29
  - targets, 14-22
    - browsing, 14-9
    - deployed, 14-22
    - filter by criteria, 14-3
    - offline, 14-23
    - pending, 14-23
    - with issues, 14-23
  - targets with issues, 14-23
  - tasks
    - approved, 22-12
    - rejected, 22-12
    - Threat Investigation Center, 22-10
  - Task Tracking, 22-12
  - templates, 15-29–15-31, 15-33

- condition statements, 15-30
  - customized, 15-30, 15-31, 15-33
  - custom reports, 18-3
  - logical operators, 15-30
  - predefined, 15-30
  - terminology, 4
  - Threat Investigation Center
    - agent, 22-20
    - command statuses, 22-14
    - registration, 22-2, 22-3
    - task commands, 22-10
    - task status, 22-13
  - Threat Investigation Center Agent for Managed Detection and Response, 22-20
  - Threat Statistics tab, 3-39
  - threat status, 7-8, 7-15
  - timeline view
    - endpoint details, 7-10
    - user details, 7-3
  - tool
    - NVW Enforcer SNMPv2 MIB file, E-2
  - tools
    - Agent Migration tool, 26-2
    - Apex Central MIB file, E-2
    - DBConfig tool, 26-2
  - Trend Vision One
    - enrollment token, 8-1
    - Product Connector, 8-1
  - Trigger Application, 17-3
  - Two-Factor Authentication, 2-6, 2-7, 4-12
- U**
- understand
    - user accounts, 4-2
  - unlocking
    - user accounts, 4-3
  - unregistering
    - managed servers, 9-8
  - updates, 12-2
    - component list, 12-2
    - components, 12-2
    - manual, 12-8
  - User/Endpoint Directory, 22-18
    - advanced search, 7-24, 22-18
    - advanced search categories, 7-26
    - endpoint details, 7-10
    - exporting data, 7-26, 22-19
    - tags and filters, 7-29
    - user details, 7-3
  - user accounts
    - access rights, 4-9
    - adding, 4-5
    - deleting, 4-2
    - disabling, 4-4
    - editing, 4-11
    - enabling, 4-3
    - understanding, 4-2
    - unlocking, 4-3
    - user roles, 4-16
  - user details, 7-3
    - tabular view, 7-3
    - timeline view, 7-3
  - User grouping, 6-11
  - user roles, 4-16
    - adding, 4-20
    - default user roles, 4-17
    - editing, 4-22
  - users
    - deleting accounts, 4-2
    - disabling accounts, 4-4

- editing accounts, 4-11
- enabling accounts, 4-3

## **V**

### viewing

- automated analyses, 22-15
- managed products logs, 11-10

## **W**

web console, 2-2, 2-3

- logging off, 2-7

widgets, 3-2

wildcards, 15-22

- file attributes, 15-22

Windows 10, 10-6

Windows 7, 10-4

Windows 8.1, 10-5

Windows HPC Server 2008 R2, 10-10

Windows MultiPoint Server 2010, 10-11

Windows MultiPoint Server 2011, 10-12

Windows MultiPoint Server 2012, 10-18

Windows Server 2008 R2, 10-8

Windows Server 2012, 10-14

Windows Server 2012 Failover

Clusters, 10-19, 10-20

Windows Server 2012 R2, 10-15

Windows Server 2016, 10-21

Windows Server 2016 Failover

Clusters, 10-22

Windows Server 2019, 10-25

Windows Storage Server 2008 R2, 10-9

Windows Storage Server 2012, 10-16

Windows Storage Server 2012 R2, 10-17

Windows Storage Server 2016, 10-23



**TREND MICRO INCORPORATED**

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

[www.trendmicro.com](http://www.trendmicro.com)

Item Code: APEM09754/230720