1.6 TREND MICRO
Endpoint Sensor
Update 3 Critical Patch
Administrator's Guide
Next Generation Endpoint Security Against Targeted Attacks and Advanced Threats
for Windows™
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:


Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, and Trend Micro Endpoint Sensor 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 © 2017. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM18105/171129

Release Date: November 2017

Protected by U.S. Patent No.: Patents pending.
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.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
Table of Contents

Preface

Preface .................................................................................................................. v
Documentation .................................................................................................. vi
Audience ............................................................................................................ vii
Document Conventions .................................................................................. vii
Terminology ..................................................................................................... viii

Chapter 1: Introduction

About Trend Micro Endpoint Sensor ............................................................... 1-2
What's New ..................................................................................................... 1-2
Features and Benefits ..................................................................................... 1-3
  Threat Investigation ........................................................................................ 1-3
  Customized Endpoint Investigation ............................................................. 1-3
  Remote Endpoint Management .................................................................... 1-3
  Attack Discovery ........................................................................................... 1-4
  File Collection and Analysis ........................................................................ 1-4
Integration with Deep Discovery Analyzer ................................................... 1-4
Integration with Control Manager ................................................................. 1-5
Compatibility .................................................................................................. 1-5

Chapter 2: Getting Started

Getting Started Tasks ........................................................................................ 2-2
The Management Console ............................................................................... 2-2
  Opening the Management Console ............................................................... 2-3
  Logging on the Management Console ......................................................... 2-3
Dashboard ..................................................................................................... 2-4
  Intelligent Monitoring Summary by Host .................................................... 2-5
  Calendar ....................................................................................................... 2-6
Chapter 3: Performing an Investigation

Investigation .......................................................... 3-2
Running an Investigation .............................................. 3-2
Investigating Historical Records ................................. 3-9
Investigating System Snapshots ................................. 3-13
Analyzing the Results .............................................. 3-18
Investigation Troubleshooting ................................. 3-32

Chapter 4: Monitoring Files

Monitoring .......................................................... 4-2
Monitoring Rules ...................................................... 4-3
Submission Settings .................................................. 4-5
Deep Discovery Analyzer Integration ......................... 4-7
Submitted for Analysis ............................................. 4-7
Rule Category ......................................................... 4-9
Monitoring Log ..................................................... 4-10
Purging Monitoring Tables ....................................... 4-13

Chapter 5: Managing Trend Micro Endpoint Sensor

Administration ........................................................ 5-2
Updates .............................................................. 5-2
Proxy ................................................................. 5-4
Management Console ........................................... 5-5
Accounts ............................................................ 5-6
About ................................................................. 5-8
License ............................................................... 5-9

Chapter 6: Technical Support

Troubleshooting Resources ......................................... 6-2
Using the Support Portal ........................................... 6-2
Threat Encyclopedia ............................................... 6-2
Contacting Trend Micro ................................................................. 6-3
  Speeding Up the Support Call ...................................................... 6-4
Sending Suspicious Content to Trend Micro ................................. 6-4
  Email Reputation Services ......................................................... 6-4
  File Reputation Services .......................................................... 6-5
  Web Reputation Services .......................................................... 6-5
Other Resources ........................................................................... 6-5
  Download Center ....................................................................... 6-5
  Documentation Feedback .......................................................... 6-6

Appendix

Appendix A: OfficeScan Integration
  About Trend Micro OfficeScan Integration ................................. A-2
  About Plug-in Manager .............................................................. A-2
  Installing OfficeScan ............................................................... A-3
  Agent Installation Considerations When Using OfficeScan .......... A-4
  Using the Trend Micro Endpoint Sensor Deployment Tool .......... A-4
  Trend Micro Endpoint Sensor Agent Deployment Tasks ............ A-11
  The OfficeScan Agent Tree ....................................................... A-14

Appendix B: Trend Micro Control Manager Integration
  About Trend Micro Control Manager .......................................... B-2
  Supported Control Manager Versions ....................................... B-2
  Control Manager Integration in this Release .............................. B-3
  Registering with Control Manager ............................................ B-4
  Adding the Endpoint Sensor Widgets ....................................... B-5
  Using the Endpoint Sensor Investigation Widget ....................... B-6
  Using Automatic Updates ........................................................ B-7
Trend Micro Endpoint Sensor Policy ................................................................. B-9

Appendix C: Supported IOC Indicator Terms

IOC Samples for Historical Records IOCs ......................................................... C-12
IOC Samples for System Process IOCs ............................................................... C-16
IOC Sample for Disk Scanning IOCs ................................................................. C-21
IOC Sample for Monitoring IOCs ................................................................. C-22

Index

Index ......................................................................................................................... IN-1
Welcome to the Trend Micro™ Endpoint Sensor™ Administrator's Guide. This document discusses getting started information, investigation steps, and product management details.

- Documentation on page vi
- Audience on page vii
- Document Conventions on page vii
- Terminology on page viii
Documentation

The documentation set for Endpoint Sensor includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Guide</td>
<td>The Installation Guide discusses requirements and procedures for installing the Endpoint Sensor server and agent.</td>
</tr>
<tr>
<td>Readme</td>
<td>The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.</td>
</tr>
<tr>
<td>Online Help</td>
<td>The Online Help contains explanations of Endpoint Sensor components and features, as well as procedures needed to configure Endpoint Sensor.</td>
</tr>
<tr>
<td>Support Portal</td>
<td>The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

View and download product documentation from the Trend Micro Online Help Center: http://docs.trendmicro.com/en-us/home

Evaluate this documentation at the following website: http://docs.trendmicro.com/en-us/survey.aspx
Audience

The Endpoint Sensor documentation is written for network administrators, systems engineers, and information security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, which includes the following topics:

- Network topologies
- Server management
- Database management
- Incident response procedures
- Content security protection

Document Conventions

The documentation uses the following conventions.

**TABLE 2. Document Conventions**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPER CASE</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td>Bold</td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td>Italics</td>
<td>References to other documents</td>
</tr>
<tr>
<td>Monospace</td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td>Navigation &gt; Path</td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, File &gt; Save means, click File and then click Save on the interface</td>
</tr>
</tbody>
</table>
**Terminology**

The following table provides the official terminology used throughout the Endpoint Sensor documentation:

**TABLE 3. Endpoint Sensor Terminology**

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The Endpoint Sensor server</td>
</tr>
<tr>
<td>Agent endpoint</td>
<td>The host where the Endpoint Sensor agent is installed</td>
</tr>
<tr>
<td>Administrator (or Endpoint Sensor administrator)</td>
<td>The person managing the Endpoint Sensor server</td>
</tr>
<tr>
<td>Management console</td>
<td>The user interface for configuring and managing Endpoint Sensor server settings</td>
</tr>
<tr>
<td>Activation Code</td>
<td>Codes that enable all Endpoint Sensor features for a specified period of time.</td>
</tr>
</tbody>
</table>
## Terminology

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
</table>
| Agent installation folder   | The folder on the host that contains the Endpoint Sensor agent files. If you accept the default settings during installation, you will find the agent installation folder at the following location:  
C:\Program Files\Trend Micro\ESE |
| Server installation folder  | The folder on the host that contains the Endpoint Sensor server files. If you accept the default settings during installation, you will find the server installation folder at the following location:  
C:\Program Files\Trend Micro\Trend Micro Endpoint Sensor |
Chapter 1

Introduction

This section provides an overview of Endpoint Sensor and the features available in this release.

Topics include:

• About Trend Micro Endpoint Sensor on page 1-2
• What's New on page 1-2
• Features and Benefits on page 1-3
• Compatibility on page 1-5
About Trend Micro Endpoint Sensor

Endpoint Sensor identifies affected endpoints through on-demand investigations and monitoring that are fully customizable to the user's needs. Integration with Deep Discovery Analyzer provides a comprehensive set of threat details that can help administrators and information security experts respond effectively to attacks. As part of the solution against advanced persistent threats, Endpoint Sensor plays a vital role in preventing, monitoring and containing the extent of damage caused by targeted attacks on endpoints and servers.

Endpoint Sensor consists of an agent program that resides at the endpoint, and a server program that manages all agents.

On the endpoint, the Endpoint Sensor agent performs recording of vectors commonly associated with targeted attacks — file executions, memory violations, registry changes, and more. The agent creates a database of all the files, activities, and important system resources, and continuously updates this database to record the arrival and execution of suspicious objects.

The Endpoint Sensor server, through the web-based management console, provides a central location to perform investigations and manage agents.

What's New

<table>
<thead>
<tr>
<th>TABLE 1-1. What's New in Version 1.6 Update 3 Critical Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE / ENHANCEMENT</strong></td>
</tr>
<tr>
<td>Security enhancements</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Agent improvements</td>
</tr>
</tbody>
</table>
TABLE 1-2. What's New in Version 1.6 Update 3

<table>
<thead>
<tr>
<th>FEATURE / ENHANCEMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Windows 10 Redstone 2</td>
<td>Endpoint Sensor adds support for Windows 10 Redstone 2 (32-bit and 64-bit).</td>
</tr>
<tr>
<td>Use of management console to upgrade agents</td>
<td>Endpoint Sensor 1.6 Update 3 server adds support to automatically update agents which were released after the 1.6 Update 3 (Build 3092) version. To upgrade agents with versions lower than 1.6 Update 3 (Build 3092), reinstall the agents manually.</td>
</tr>
<tr>
<td>Security enhancements</td>
<td>Endpoint Sensor adds security enhancements to address CVE-2017-5565.</td>
</tr>
</tbody>
</table>

Features and Benefits

The following sections describe the Endpoint Sensor features and benefits:

Threat Investigation

Endpoint Sensor provides a central location to investigate for the existence of threats on multiple endpoints. All investigation criteria are fully customizable by the user. Endpoint Sensor can investigate both historical and current states of all managed endpoints. Each investigation provides a graphical breakdown of the threat’s activities, which helps administrators re-construct the events of the security incident from start to end.

If regular monitoring is part of the organization’s security plan, Endpoint Sensor provides the option to perform investigations scheduled at specified intervals.

Customized Endpoint Investigation

Endpoint Sensor supports IOC and YARA rules which allow the creation, sharing and re-use of existing threat information. IOC and YARA rules are fully customizable to
address targeted attacks. Additionally, Endpoint Sensor also provides its own set of IOC rules, which are regularly updated to provide protection from the most recent threats.

Remote Endpoint Management

Endpoint Sensor allows administrators to monitor, manage and run investigations on endpoints through a web-based management console. The management console provides a means to configure the endpoints remotely, and view endpoint details — such as agent version, pattern version, etc. — all from a central location.

Attack Discovery

Endpoint Sensor can proactively monitor and discover suspicious files and behavior through user-defined IOC rules. Endpoint Sensor also leverages on Trend Micro’s threat intelligence through the use of regularly updated IOC rules to provide protection from the latest threats.

File Collection and Analysis

Endpoint Sensor collects all files that match a monitoring rule. Once a suspicious file is found, it can be sent to a local file server, or sent to a Deep Discovery Analyzer server for further analysis. Deep Discovery Analyzer then provides Endpoint Sensor with a comprehensive set of threat details that can help administrators determine if a file is malicious or not.

For details, see Integration with Deep Discovery Analyzer on page 1-4.

Integration with Deep Discovery Analyzer

Endpoint Sensor supports integration with Deep Discovery Analyzer™ 5.1 and later.

Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports out-of-the-box integration to augment or centralize the sandbox analysis of other Trend Micro products. The custom sandboxing environments created
within Deep Discovery Analyzer precisely match target desktop software configurations, resulting in more accurate detections and fewer false positives.

For details, refer to the documentation available at:


Integration with Control Manager

Endpoint Sensor 1.6 Update 3 Critical Patch supports integration with Trend Micro\textsuperscript{TM} Control Manager\textsuperscript{TM}. Control Manager manages Trend Micro products and services at the gateway, mail server, file server and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for products and services throughout the network. Use Control Manager to manage several Endpoint Sensor servers from a single location.

For details, see the Trend Micro Control Manager documentation.

Compatibility

Endpoint Sensor is designed to be compatible with Trend Micro solutions with the exception of the following:

\textbf{Table 1-3. Software Incompatibilities}

<table>
<thead>
<tr>
<th>ENDPOINT SENSOR SOFTWARE</th>
<th>INCOMPATIBLE SOFTWARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>• Trend Micro Safe Lock\textsuperscript{TM} agent</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro Safe Lock\textsuperscript{TM} Intelligent Manager</td>
</tr>
<tr>
<td><strong>Endpoint Sensor Software</strong></td>
<td><strong>Incompatible Software</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Agent</td>
<td>• Trend Micro™ Titanium™</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro™ Internet Security</td>
</tr>
<tr>
<td></td>
<td>• Deep Security 10.0 Update 2</td>
</tr>
</tbody>
</table>

**Note**

Installation of a Trend Micro Endpoint Sensor agent and a Deep Security 10.0 Update 2 agent on one endpoint is supported only on Windows 2008 R2, Windows 2012 and Windows 2012 R2.

**Important**

Setup does not check for these incompatibilities, and will continue with the installation. The incompatible program may prevent Endpoint Sensor from functioning properly.

To ensure that Endpoint Sensor is successfully installed, refer to the pre- and post-installation sections of the Installation Guide available at:

This section describes how to get started with Endpoint Sensor.

Topics include:

- *Getting Started Tasks on page 2-2*
- *The Management Console on page 2-2*
- *Dashboard on page 2-4*
- *Endpoint on page 2-7*
Getting Started Tasks

Getting Started Tasks provides a high-level overview of all procedures required to get Endpoint Sensor up and running as quickly as possible.

Procedure

1. Log on the management console.
   For details, see Logging on the Management Console on page 2-3.
2. Verify that all endpoints are detected.
   For details, see Endpoint on page 2-7.
3. Configure updates.
   For details, see Updates on page 5-2.
   For details, see Proxy on page 5-4.
5. Configure management console settings.
   For details, see Management Console on page 5-5.
   For details, see Monitoring on page 4-2.

The Management Console

The management console is the central point for monitoring and launching a Endpoint Sensor investigation. Use the Endpoint Sensor management console to perform the following tasks:

• Monitor and investigate endpoints
• Analyze the enterprise-wide chain of events involved in an attack
• Update the product license
• Manage the administrator account

Opening the Management Console

Open the management console from any endpoint on the network that has the following specifications:

**TABLE 2-1. Required Hardware and Software Components for the Management Console**

<table>
<thead>
<tr>
<th>REQUIREMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware requirements</td>
<td>Any computer with the following specifications:</td>
</tr>
<tr>
<td></td>
<td>• 300 MHz Intel™ Pentium™ processor or equivalent</td>
</tr>
<tr>
<td></td>
<td>• 128 MB of RAM</td>
</tr>
<tr>
<td></td>
<td>• At least 30 MB of available disk space</td>
</tr>
<tr>
<td></td>
<td>• Monitor that supports 1024 x 768 resolution at 256 colors or higher</td>
</tr>
<tr>
<td>Web browsers</td>
<td>Any of the following supported web browsers:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer 9 or later</td>
</tr>
<tr>
<td></td>
<td>• The latest version of Google Chrome</td>
</tr>
<tr>
<td></td>
<td>• The latest version of Mozilla Firefox</td>
</tr>
</tbody>
</table>

Accessing the management console requires an administrator account and a password. These are set during server installation.

Logging on the Management Console

**Procedure**

1. On the web browser, type the following in the address bar:
https://<FQDN or IP address of Trend Micro Endpoint Sensor>:8000/

The Log on screen appears.

2. Specify the following information.
   - **User name**: Type `admin`.
   - **Password**: Type the password you supplied during installation.

3. Click Log on.

The Endpoint Sensor **Dashboard** screen appears.

**Dashboard**

The Endpoint Sensor **Dashboard** screen is the default screen that appears when you access the management console. Use the **Dashboard** to view a quick summary of all monitoring and investigation activities through the following widgets:
Note

On first use, widgets have no data to display since widgets get data from investigation results. To display widget data, proceed to the **Investigation** screen to start an investigation.

For details, see *Investigation on page 3-2.*

----------

## Intelligent Monitoring Summary by Host

This widget displays a summary of the most recently affected endpoints, based on the enabled monitoring rules. To manage monitoring rules, go to **Monitoring > Monitoring Setting.**

The widget displays the following details:

**TABLE 2-2. Intelligent Monitoring Summary by Host**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The host name of the endpoint</td>
</tr>
<tr>
<td>Hit Counts</td>
<td>The number of matching rules triggered on the endpoint</td>
</tr>
<tr>
<td>Rule Category</td>
<td>Category of the most recent rules matched on the endpoint. These categories are based on the six stages of a targeted attack. For details, see <em>Rule Category on page 4-9.</em></td>
</tr>
<tr>
<td>Detection time</td>
<td>The date and time when the rule was last triggered in the endpoint</td>
</tr>
</tbody>
</table>

The default time period is **Last 24 hours.** Change the time period according to your preference.
Calendar

This widget displays a calendar showing all the investigation schedules.

By default, this widget presents an overview of all the investigations occurring for the current month. The current date is highlighted in yellow. To review schedules, perform any of the following:
Getting Started

- Click on a schedule to view a quick summary of the investigation results. To view the full results, click **View results**.
- Use the **Month, Week** and **Day** buttons to customize the display to your preferred view.
- Use the **< >** buttons to navigate through the calendar and view past or future schedules. To return to the current date, click **Today**.

**Note**
- Endpoint Sensor does not support automatic adjustments for Daylight Saving Time (DST). To minimize issues, review the schedule details and make necessary adjustments to ensure that the schedule runs at the intended time.
- Use the **Schedule** screen to manage schedules.

For details, see *Managing Schedules on page 3-8*.

---

**Endpoint**

Use the **Endpoint** screen to manage all endpoints detected by the Endpoint Sensor server.

**Note**
- The **Endpoint** screen can only show endpoints that have the Endpoint Sensor agent installed.

For details about agent requirements and installation, refer to the *Trend Micro Endpoint Sensor Installation Guide* available at:

The following table lists the endpoint details available for review:

**TABLE 2-3. Endpoint Details**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The computer name of the Windows endpoint running the Endpoint Sensor agent. This column also shows the status of the endpoint:</td>
</tr>
<tr>
<td></td>
<td>• A green status indicator indicates that the endpoint is online</td>
</tr>
<tr>
<td></td>
<td>• A gray status indicator indicates that the server has received no response from the endpoint for more than 15 minutes</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address of the agent endpoint.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The Windows variant running on the endpoint.</td>
</tr>
<tr>
<td>Event Recording</td>
<td>The status of the agent if it is actively recording events.</td>
</tr>
<tr>
<td>Registered</td>
<td>The date and time when Endpoint Sensor first communicated with the agent.</td>
</tr>
<tr>
<td>Latest Response</td>
<td>The date and time when the agent last communicated with the Endpoint Sensor server.</td>
</tr>
</tbody>
</table>
Select at least one endpoint to enable the following options:

- Click **Configure** to set the properties for the selected endpoints. The following options are available:
  - **Asset tag**: Specify an asset tag for the endpoint.
  - **Database size**: Select a maximum size for the agent database.
  - **Event recording**: Toggles event recording for the selected endpoints. This is useful if the selected endpoint is undergoing maintenance (for example, installing system updates) and it is required to temporarily stop the agent.

- Click **Remove** to remove the endpoint from the list of managed endpoints.

**Note**

- Once removed, Endpoint Sensor will not be able to manage the endpoint, and the endpoint will no longer be available for investigation purposes. If you need to re-register the endpoint, contact Trend Micro support.
- Removing an endpoint from this list does not uninstall the agent on the endpoint. For details on uninstalling an agent, see the Endpoint Sensor Installation Guide.

- Click **Upgrade (All)** to upgrade all registered endpoints.
Note

The Endpoint Sensor 1.6 Update 3 server can only automatically update agents released after the 1.6 Update 3 (Build 3092) version. To upgrade agents with versions lower than 1.6 Update 3 (Build 3092), reinstall the agents manually.

- If the Endpoint Sensor server is integrated with OfficeScan, use the Trend Micro Endpoint Sensor Deployment Tool to manually install agents to selected endpoints.
  
  For details, see Installing the Trend Micro Endpoint Sensor Agent on page A-13.

- Other installation methods may be available depending on your environment. For assistance on other installation methods, contact Trend Micro support.

Use Search to locate a specific endpoint by using any of the following criteria:

- **Host Name:** Specify the host name of the endpoint you want to locate.

- **IP Address:** Specify a range of IP addresses to locate.

- **Asset Tag:** Specify the asset tag of the endpoint you want to locate.

Use the following options to manage this list:

- Use **Filters** to filter the list by tags. Select one or more tags to display only the endpoints with that tag.

- Use the pagination control at the bottom of the list to display 10, 25, 50 or 100 endpoints at a time.
Chapter 3

Performing an Investigation

This section provides information on how to use Endpoint Sensor to perform an investigation.

Topics include:

• Running an Investigation on page 3-2
• Investigating Historical Records on page 3-9
• Investigating System Snapshots on page 3-13
• Analyzing the Results on page 3-18
• Investigation Troubleshooting on page 3-32
Investigation

Investigations locate occurrences of a suspicious object in specified endpoints. They are used to assess the extent of damage caused by targeted attacks on endpoints and servers. They also provide information on the arrival and progression of an attack. This information is useful in planning an effective security incident response.

Endpoint Sensor classifies investigations according to source:

- A **Historical records** investigation performs the investigation on historical events. Historical records are useful in analyzing the timeline of an attack.
- A **System snapshot** investigation performs the investigation on the target's current state.

To start an investigation using your preferred source, click **Investigation**, and select **New Investigation** under the correct classification.

Running an Investigation

On the **New Investigation** screen, perform the following steps.
Performing an Investigation

Procedure

1. Specify a unique Name for the investigation.

2. Specify a Period.

   Endpoint Sensor performs the investigation on events that occurred during the period specified. The following options are available:
   - All logged dates performs the investigation on all data, regardless of date.
   - Custom range limits the investigation to a specific time period.

3. Select a Target.

   Endpoint Sensor performs the investigation on all endpoints by default. However, to perform the investigation on specific endpoints only, click to show the Select Targets screen. This screen allows you to choose which endpoints to include in the investigation.

   For details, see Selecting Targets on page 3-4.

4. Specify Tags.

   Tags are user defined strings used to identify this investigation. Type multiple tags by separating each individual tag with a comma. These tags appear in the Results screen table and are useful in locating your investigation later.

5. Specify a Schedule to set how often the investigation repeats.

   The following options are available:
   - Run Once: The investigation runs only once.
   - Repeat: The investigation starts on the specified Start date and repeats on a daily, weekly or monthly basis, until the specified End date is reached.

   For details, see Adding a Schedule on page 3-6.

6. Select an investigation method and specify valid criteria.

   - For methods applicable for Historical Records, see Investigating Historical Records on page 3-9.
For methods applicable for System Snapshot, see *Investigating System Snapshots on page 3-13.*

Once the investigation starts, Endpoint Sensor updates the following screens:

- The investigation is added to the **Results** screen.
  
  For details, see *Investigation Results on page 3-20.*

- If the investigation recurrence has been set to **Repeat**, the given schedule name appears in the **Schedule** screen.
  
  For details, see *Managing Schedules on page 3-8.*

- Data from finished investigations is added to the **Dashboard** screen.
  
  For details, see *Dashboard on page 2-4.*

**Selecting Targets**

Use the **Select Targets** screen to select specific endpoints to use in an investigation.
This screen displays the following details:

**TABLE 3-1. Select Targets Screen**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Computer name of the endpoint running the Endpoint Sensor agent program</td>
</tr>
<tr>
<td>IP Address</td>
<td>IPv4 address of the agent endpoint</td>
</tr>
<tr>
<td>Operating System</td>
<td>The Windows variant running on the endpoint</td>
</tr>
<tr>
<td>Event Recording</td>
<td>The status of the agent, if it is actively recording events.</td>
</tr>
<tr>
<td>Asset Tag</td>
<td>A user-defined string that identifies the endpoint</td>
</tr>
</tbody>
</table>

To include specific endpoints in the investigation, select the check box of the endpoints and click **Confirm**. Otherwise, click **Cancel** to discard the selection.

Use **Search** to locate a specific endpoint. You can search for the following properties:

- **Host Name**: specify the host name of the endpoint you want to locate.
- **IP Address**: specify a range of IP addresses to locate.
- **Asset Tag**: specify the asset tag of the endpoint you want to locate.

Use the following options to manage this list:

- Use **Filters** to filter the list by tags. Select one or more tags to display only the endpoints with that tag.
- Use the pagination control at the bottom of the list to display 10, 25, 50 or 100 endpoints at a time.

---
**Note**

To set the **Asset Tag** of an endpoint and remove unnecessary endpoints, use the **Endpoints** screen.

For details, see *Endpoint on page 2-7.*
Adding a Schedule

Use the **Add Schedule** screen to set the investigation to repeat at specified intervals.

![Add Schedule Screen](image)

Specify the following required settings:

**TABLE 3-2. Add Schedule Screen**

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>ACTION REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Assign a name for this schedule.</td>
</tr>
<tr>
<td>Start date</td>
<td>Specify a starting date and time for the schedule. The schedule is enabled on this date.</td>
</tr>
</tbody>
</table>
### Options

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>ACTION REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>End date</td>
<td>Specify an ending date and time for the schedule. The schedule is disabled on this date.</td>
</tr>
</tbody>
</table>

**Note**
- Values for the Start and End dates must not refer to the same day.
- The schedule does not run during the End date specified.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Specify how often the investigation repeats during the duration of the schedule. The following options are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Daily</strong>: Set the schedule to run at a specified time everyday.</td>
</tr>
<tr>
<td></td>
<td><strong>Weekly</strong>: Specify a time and day of the week to run the schedule.</td>
</tr>
<tr>
<td></td>
<td><strong>Monthly</strong>: Specify a time and day of the month to run the schedule.</td>
</tr>
</tbody>
</table>

**Note**
If a schedule is specified to run on the 31st day of every month, Endpoint Sensor moves the investigation to the end of every month. For example, a schedule set to run from January to May on the 31st day of each month will run on the following dates: January 31, February 28, March 31, April 30, May 31.

---

**Important**

Endpoint Sensor does not support automatic adjustments for Daylight Saving Time (DST). To minimize issues, review the schedule details and make necessary adjustments to ensure that the schedule runs at the intended time.

Once the investigation starts, use the **Schedule** screen to manage the schedule.

For details, see *Managing Schedules on page 3-8*. 

---
Managing Schedules

Use the **Investigation Schedules** screen to manage all investigation schedules.

![Investigation Schedules](image)

The following table lists the schedule details available for review:

**TABLE 3-3. Schedule Details**

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Name</td>
<td>The name given to the schedule.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the schedule.</td>
</tr>
<tr>
<td>Frequency</td>
<td>The recurrence pattern set for the schedule.</td>
</tr>
<tr>
<td>Next Schedule</td>
<td>The time when the next investigation occurs.</td>
</tr>
<tr>
<td>Start</td>
<td>The start date of a schedule. After this date, the schedule runs the</td>
</tr>
<tr>
<td></td>
<td>investigation repeatedly until the <strong>End</strong> date is reached.</td>
</tr>
<tr>
<td>End</td>
<td>The end date of a schedule. The investigation no longer runs on and after</td>
</tr>
<tr>
<td></td>
<td>this date.</td>
</tr>
<tr>
<td>History</td>
<td>The number of times the investigation has repeated.</td>
</tr>
</tbody>
</table>

Select at least one schedule to activate the following options:
Performing an Investigation

- Click **Toggle Status > Disable** to temporarily disable the schedule.
- Click **Toggle Status > Enable** to enable a disabled schedule.
- Click **Remove** to remove the schedule.

Use the following options to manage this list:

- Use **Filters** to filter the list by tags. Select one or more tags to display only the endpoints with that tag.
- Use the pagination control at the bottom of the list to display 10, 25, 50 or 100 endpoints at a time.

**Note**

- To add a schedule, run a new investigation.
  For more details, see *Investigation on page 3-2*.
- Endpoint Sensor does not support automatic adjustments for Daylight Saving Time (DST). To minimize issues, review the schedule details and make necessary adjustments to ensure that the schedule runs at the intended time.
  For details, see *Dashboard on page 2-4*.

**Investigating Historical Records**

To investigate historical records, click **Investigation** and select **New Investigation** under the **Historical records** category.

Endpoint Sensor uses the following methods to investigate historical records.
Retro Scan

Use Retro Scan to search historical events and their activity chain based on specified criteria.

This criteria requires an object type and an item. The following table shows the required format for each object type:

**TABLE 3-4. Valid Item Formats for Retro Scan**

<table>
<thead>
<tr>
<th>TYPE</th>
<th>ITEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS record</td>
<td>Type a domain name accessed by an endpoint.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">cnccserver.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="#">malicioussite.com</a></td>
</tr>
<tr>
<td>IP address</td>
<td>Type an IP address accessed by an endpoint.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">192.168.0.1</a></td>
</tr>
<tr>
<td>File name</td>
<td>Type the full file name or the file extension.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">wmiprvse</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="#">suhost</a></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| File path | Type the folder name or full path. If the folder name or full path cannot be determined, use an asterisk (*) as the keyword suffix to perform a partial match. A suffix refers to the last segment of an expression.  
For example, to search for `c:\windows\system32\wbem\wmiprvse.exe`, use any of the following keywords:  
  - `windows`  
  - `win*`  
  - `system32`  
  - `system*`  
  - `wbem`  
  - `wmiprvse`  
  - `wmi*` |
| SHA-1 hash values | Type the SHA-1 hash value of a file.  
Example:  
`a2da9cda33ce378a21f54e9f03f6c0c9efba61fa` |
| MD5 hash values | Type the MD5 hash value of a file.  
Example:  
`395dc2c9ff1dce7d150ad047e78c93e1` |
| User account | Type the name of the Active Directory account or local user.  
Examples:  
  - Active Directory user `<domain>\<user name>`: `jp\jane_doe`  
  - Local user `<user name>`: `jane_doe` |
Note

- A Retro Scan investigation can include up to 128 search criteria.
- Free-form search supports partial matching of terms, provided that the term does not include spaces.
- Search conditions are NOT case-sensitive.

IOC Rule

Use the IOC rule method to search events and their activity chain based on the indicator terms parsed from an uploaded IOC file. An IOC file is an XML file which contains one or more Indicators of Compromise (IOCs) using indicator terms defined in the OpenIOC schema. Verify that the IOC file to be uploaded uses indicator terms supported by Endpoint Sensor.

For details, see Supported IOC Indicator Terms on page C-1.

Use the IOCTool available in the \<Trend Micro Endpoint Sensor server installation path>\CmdTool\IOCTool\ folder to troubleshoot invalid IOC files.

For details, see Troubleshooting Invalid IOC Files on page 3-34.
Performing an Investigation

Note

- The maximum file size for an IOC file is 1024KB.
- Endpoint Sensor can store a total of 10 IOC files. Once this limit is reached, older IOC files are removed when new ones are uploaded.
- Once uploaded, the IOC file is available for all future investigations. Ensure that an IOC file is selected before you start the investigation.

Investigating System Snapshots

To investigate system snapshots, click Investigation and select New Investigation under the System snapshot category.

Endpoint Sensor uses the following methods to investigate system snapshots.

Registry Search

Use Registry search to search for registry keys, names, or data that are potentially related to malware and other threats.

Registry search requires the following details:

**TABLE 3-5. Registry Search Requirements**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Searches for key instances that match the value provided</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Searches for name instances that match the value provided</td>
</tr>
</tbody>
</table>
| Data  | Searches for data instances that match the value provided, based on these criteria:  
- Contains  
- Does not contain  
- Exact match |

---

**Note**

A registry search investigation can include up to 128 search criteria.

Endpoint Sensor searches for threats in the `Computer\HKEY_CURRENT_USER` hive by enumerating the SIDs under `HKEY_USERS\[SID]`, and then searching for specific locations.

For example, if the following registry key is specified:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Themes
```

Endpoint Sensor searches the following matching objects:

```
HKEY_USERS\.default\software\microsoft\windows\currentversion\themes  
HKEY_USERS\(NT AUTHORITY/LOCAL SERVICE)s-1-5-19\software\microsoft\windows\currentversion\themes  
HKEY_USERS\(NT AUTHORITY/NETWORK SERVICE)s-1-5-20\software\microsoft\windows\currentversion\themes  
HKEY_USERS\s-1-5-21-329068152-1770027372-1177238915-1003\software\microsoft\windows\currentversion\themes  
HKEY_USERS\(VM_XP003/Administrator)s-1-5-21-329068152-1770027372-1177238915-500\software\microsoft\windows
```
System Audit

Use System Audit to scan all running processes, running services, loaded modules and autorun processes. Up to 50 endpoints can be selected for system audit. This method does not require any additional parameters.

**IOC Rule**

IOC rules can also be used to investigate system snapshots. To use IOC rules, follow the same guidelines mentioned in Historical Records.

For details, see *IOC Rule on page 3-12*.

**Disk IOC Rule**

Use the **Disk IOC rule** method to use an uploaded disk IOC file to search for files in a system snapshot. The uploaded disk IOC file has to include at least one `fileitem/filepath` or `fileitem/fullpath` indicator.
For details, see *Supported IOC Indicator Terms on page C-1.*

Use the **IOCTool** available in the `<Trend Micro Endpoint Sensor server installation path>\CmdTool\IOCTool\` folder to troubleshoot invalid IOC files.

For details, see *Troubleshooting Invalid IOC Files on page 3-34.*

---

**Note**

- The maximum file size for a disk IOC file is 1024KB.
- Endpoint Sensor can store a total of 10 disk IOC files. Once this limit is reached, older disk IOC files are removed when new ones are uploaded.
- Once uploaded, the disk IOC file is available for all future investigations. Ensure that a disk IOC file is selected before you start the investigation.

---

**YARA Rule**

Use the **YARA rule** method to enumerate all running processes and scan the memory based on a given set of YARA rules. The YARA rule method scans processes that consume less than 512 MB of memory.
Performing an Investigation

For details about YARA rules, see [http://plusvic.github.io/yara/](http://plusvic.github.io/yara/).

A YARA file contains rules that describe malware in textual or binary patterns. Endpoint Sensor uses YARA rules to monitor and investigate running processes on agents. With YARA, Endpoint Sensor is able to check the whole memory space of a process.

Verify that all YARA files to be uploaded use the following format:

```
rule ExampleRule
{
    strings:
        $my_test_string1 = "Behavior Inject DLL" wide
        $my_test_string2 = "Behavior Inject DLL"

    condition:
        $my_test_string1 or $my_test_string2
}
```

Use the YARA tool available in the `<Trend Micro Endpoint Sensor server installation path>\CmdTool\YARA` folder to troubleshoot invalid YARA rules.
For details, see *Troubleshooting Invalid YARA Rules on page 3-35.*

**Note**

- The maximum file size for a YARA file is 1024KB.
- Endpoint Sensor can store a total of 10 YARA files. Once this limit is reached, older YARA files are removed when new ones are uploaded.
- Once uploaded, the YARA file is available for all future investigations. Ensure that a YARA file is selected before you start the investigation.

### YARA Sample for Driver Files

The following YARA file sample searches for driver files based on a given set of strings:

```plaintext
rule APT_driver
{
  strings:
    $s1 = "Services\riodrv32" wide ascii
    $s2 = "riodrv32.sys" wide ascii
    $s3 = "svchost.exe" wide ascii
    $s4 = "wuauserv.dll" wide ascii
    $s5 = "arp.exe" wide ascii
    $pdb = "projects\auriga" wide ascii

  condition:
    all of ($s*) or $pdb
}
```

### Analyzing the Results

Perform the following steps to analyze the investigation results.

**Procedure**

1. Click **Investigation**, and select the correct result screen for your investigation source.
2. On the **Results** screen, monitor the progress of the investigation. Wait for the investigation to show a **processing** status. Click on the investigation name to view more information.

   For details, see *Investigation Results on page 3-20*.

3. On the **Information** screen, view the investigation activity. Endpoint Sensor investigates each endpoint. Once finished with the investigation for an endpoint, Endpoint Sensor updates the screen in real-time to add the result for that endpoint. It then proceeds to investigate the next endpoint.

   For details, see *Information on page 3-22*.

4. Review the results using the tools available in Endpoint Sensor:
   - **Result Details on page 3-24**
   - **Root Cause Chain on page 3-25**
   - **Recorded Objects on page 3-31**
Investigation Results

Use the **Investigation Results** screen to view an investigation's details and its progress. Once an investigation starts, the investigation appears here. Recently created investigations appear first.

The following table lists all the investigation details available for review:

**TABLE 3-6. Results Details**

<table>
<thead>
<tr>
<th><strong>COLUMN NAME</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the investigation, if the investigation is <strong>Pending</strong>, <strong>Processing</strong>, <strong>Completed</strong> or <strong>Cancel</strong>.</td>
</tr>
<tr>
<td>Progress</td>
<td>The investigation's percentage of completion.</td>
</tr>
<tr>
<td>Investigated Time</td>
<td>The date and time when the investigation was started.</td>
</tr>
</tbody>
</table>
Performing an Investigation

<table>
<thead>
<tr>
<th><strong>COLUMN NAME</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name given to the investigation.</td>
</tr>
<tr>
<td>Method</td>
<td>The method used by the investigation.</td>
</tr>
</tbody>
</table>
| Tags            | The user-defined string given when the investigation was created.  
For details, see *Investigation on page 3-2*. |
| Target Endpoints| The number of endpoints included in the investigation.  
For details, see *Selecting Targets on page 3-4*. |
| Matched         | The number of matching objects found on the endpoint. |
| Time Elapsed    | Time elapsed since the investigation started. |

Use the following options to manage the investigations:

- Click **Cancel** to stop the progress of the investigation. However, results for endpoints already investigated are still available for review. Cancelled investigations cannot be resumed.

---

**Note**

- After the investigation has been cancelled, the Trend Micro Endpoint Sensor server may show the status of some endpoints as still being processed for investigation. The server stops updating the screen once an investigation is cancelled. However, if an endpoint is in the middle of being investigated, Trend Micro Endpoint Sensor will finish the investigation for that endpoint, but will no longer proceed with the remaining endpoints.

- If a previous investigation is cancelled and a new investigation is started, the new investigation may some time to start. If the user cancels the investigation, investigations for all remaining pending endpoints are dropped, but Trend Micro Endpoint Sensor will still complete the investigation for the currently investigated endpoint before stopping completely. This investigation can take some time to complete. Note that the previous investigation has to completely stop before a new investigation can begin.
• Click **Remove** to remove the investigation from the list. The investigation and all endpoint data related to the investigation will be removed from the server. Removed investigations cannot be recovered.

• Use **Filters** to filter the list by tags. Select one or more tags to display only the endpoints with that tag.

• Use the pagination control at the bottom of the list to display 10, 25, 50 or 100 endpoints at a time.

To view more details, click the investigation's **Name**.

**Information**

On the **Result** screen, click the investigation name to get a quick overview of the investigation results. To cancel the investigation, click **Stop**.
This screen displays the following details:

- A doughnut chart showing the number of total endpoints already classified as being **Matched, Safe, Pending** or **Cancelled**

  The number of total endpoints is regularly updated while the investigation is running.

**TABLE 3-7. Investigation Status**

<table>
<thead>
<tr>
<th>ICON</th>
<th>LABEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Matched]</td>
<td>Matched</td>
<td>Number of investigated endpoints containing a match</td>
</tr>
<tr>
<td>![Safe]</td>
<td>Safe</td>
<td>Number of investigated endpoints where a match was not found</td>
</tr>
<tr>
<td>![Pending]</td>
<td>Pending</td>
<td>Number of endpoints still to be investigated. An investigation is complete once there are no more pending endpoints to investigate.</td>
</tr>
</tbody>
</table>
| ![Cancelled] | Cancelled | Number of endpoints which were not investigated. This may be caused by user cancellation, system error, or endpoint timeout  
For details, see *Troubleshooting Investigation Status on page 3-32.* |

A breakdown of the totals is given on the left of the chart.

- Parameters used when the investigation was created

  Click **Criteria** to review the search conditions used by the investigation.

  For details, see *Investigation on page 3-2.*

- A table of results of 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:
<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The host name of the endpoint. Click the endpoint's host name to go to that endpoint's <strong>Matched Endpoint</strong> screen. For details, see <em>Result Details on page 3-24</em>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address of the endpoint.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The version of Windows installed on the endpoint.</td>
</tr>
<tr>
<td>Asset Tag</td>
<td>The tags associated with the endpoint.</td>
</tr>
<tr>
<td>Object Count</td>
<td>The number of matched objects found on the endpoint.</td>
</tr>
<tr>
<td>Time Elapsed</td>
<td>Time elapsed since the investigation started.</td>
</tr>
</tbody>
</table>

Click **View Investigation Criteria** to review the search conditions used by the investigation.

For details, see *Investigation on page 3-2*.

### Result Details

Use the **Result Details** screen to analyze the investigation results.
Performing an Investigation

Note

To return to the previous Investigation Result screen, use the breadcrumb navigation at the top.

The Matched Endpoint screen is composed of the following areas:

- **Root Cause Chain** displays a visual representation of the matched object and all its related objects. It presents an analysis of events by showing the objects used by the matched object to execute.

  To narrow your investigation down to specific items on the root cause chain, click View More Details.

  For details, see Root Cause Chain on page 3-25.

- **Recorded Objects** displays details about the matched object and all its related objects. Details shown here come from the Objects List screen.

  For details, see Recorded Objects on page 3-31.

Root Cause Chain

The Root Cause Chain screen displays a visual analysis of the objects involved in an event.
The following example shows the root cause chain for a Retro Scan investigation. The investigation tries to locate all objects that use the file name `notepad`.

### Procedure

1. Review the root cause chain.

   The root cause chain may contain multiple results for one endpoint. The root cause chain uses icons to represent the objects by type.

   For details, see *Root Cause Chain Icons on page 3-29.*

   The following objects are shown in red:
Performing an Investigation

- The matched object. This is the object that meets the search criteria set by the investigation.

- All the dependencies of the matched object. These are the objects required to run the matched object.

All other objects in the chain (that did not contribute to the execution of the matched object) are shown in blue. Objects that branch out of the matched object are also shown in blue.

2. Review all the objects (both red and blue). If one of the objects appears suspicious, select the object and perform any of the following:

- Use the tooltip on the left to review the details of the selected object. These details come from the Object List screen. For details, see Recorded Objects on page 3-31.

- Use the following options on the right to manage the objects shown in the root cause chain:

**TABLE 3-8. Customization Options for the Root Cause Chain**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get more</td>
<td>Appends a new branch to the selected object</td>
</tr>
<tr>
<td>Expand</td>
<td>Expands the selected object to show objects affected further down the chain</td>
</tr>
<tr>
<td>Expand All</td>
<td>Expands all the branches in the root cause chain to show objects affected further down the chain</td>
</tr>
<tr>
<td>Collapse</td>
<td>Hides the expanded branch of the selected object. This option appears only if the object has an expanded branch</td>
</tr>
<tr>
<td>Collapse all</td>
<td>Hides all the expanded branches. This option appears only if at least one object has an expanded branch.</td>
</tr>
</tbody>
</table>

- Use the following options on the right to collect objects for later investigation by adding them to the Interested Objects list.
### Table 3-9. Options for Interested Objects

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add to interested objects list</td>
<td>Adds the object as a new item in the Interested Objects list</td>
</tr>
<tr>
<td>Remove from interested objects list</td>
<td>Removes the object from the Interested Objects list</td>
</tr>
<tr>
<td>Remove from root cause chain</td>
<td>Unmarks the object as suspicious and turns the icon blue</td>
</tr>
<tr>
<td>Add to root cause chain</td>
<td>Marks the object as suspicious and turns the icon red</td>
</tr>
</tbody>
</table>

To add or remove objects from the Interested Objects list, click Actions.

3. Once the suspicious files have been narrowed down, initiate a new investigation.
   - To initiate an investigation for a single object, click the object and select Investgate further. This initiates a new investigation using the selected object as a search condition.
   - To initiate an investigation for the Interested Objects list, select at least one object, and click Actions. From the options, select Investigate further to initiate an investigation that uses all the selected objects in the list.

4. The new investigation creates another root cause chain. Repeat the review until the analysis is complete.
Performing an Investigation

---

**Note**

Use the following options to navigate the root cause chain:

- Use the **Contents** list to view all objects shown in red. The objects are organized according to the root cause chain they belong to. Click an item in the **Contents** list to center that item on the root cause chain area.

- To increase the space available for the root cause chain area, click ➔ and ◀ to hide the **Interested Objects** and the **Contents** list respectively.

- Use the **Current Screen** to determine the location of the object in relation to the area of the root cause chain.
  - The gray box represents the full area of the root cause chain. This box expands as more branches are added to the initial root cause chain.
  - The box with the blue outline represents the current area being viewed. If the screen is resized, this box resizes to match the new screen size.

---

**Root Cause Chain Icons**

The **Root Cause Chain** screen shows object types using the following icons:

**TABLE 3-10. Icon Legend**

<table>
<thead>
<tr>
<th>ICON</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>💾</td>
<td>File</td>
<td>Files created by the processes related to the matched object.</td>
</tr>
<tr>
<td>🔄</td>
<td>Process</td>
<td>Processes that start other services or create files. Processes usually have an associated user account displayed under the process name.</td>
</tr>
<tr>
<td>🌐</td>
<td>IP address and port</td>
<td>IP addresses that the connected process, service, or file attempted to access.</td>
</tr>
<tr>
<td>🌐</td>
<td>Domain</td>
<td>Domains that the connected process, service, or file attempted to access.</td>
</tr>
<tr>
<td>👤</td>
<td>User account</td>
<td>The user account with the domain that started the connected process, service, or file.</td>
</tr>
<tr>
<td>ICON</td>
<td>TYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td>Services that create files, or start other processes and services. Services usually have an associated user account displayed under the service name.</td>
</tr>
<tr>
<td></td>
<td>Registry</td>
<td>Registry operations implemented by a process, service or module, especially for autorun processes.</td>
</tr>
<tr>
<td></td>
<td>Autorun Process</td>
<td>Registry entries that launch processes and services during system startup.</td>
</tr>
<tr>
<td></td>
<td>Module</td>
<td>Modules loaded by a process or service to perform a routine.</td>
</tr>
<tr>
<td></td>
<td>Mutex</td>
<td>Objects used in coordinating mutually exclusive access to a shared resource.</td>
</tr>
<tr>
<td></td>
<td>Semaphore</td>
<td>A software flag with a value that indicates the status of a common resource.</td>
</tr>
<tr>
<td></td>
<td>Inject API</td>
<td>APIs used by the matched object to inject itself or any of its dependencies into a process.</td>
</tr>
<tr>
<td></td>
<td>WinINet API</td>
<td>APIs that are used for network connection and information transfer.</td>
</tr>
<tr>
<td></td>
<td>Downloaded file</td>
<td>Files that are downloaded from a URL.</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td>Unknown modules and files.</td>
</tr>
<tr>
<td></td>
<td>Internet API</td>
<td>APIs that are used to connect to the Internet via application level. For example, HTTP/FTP.</td>
</tr>
</tbody>
</table>

**Note**

Click **Legend** to view the icon descriptions.
Recorded Objects

Use the **Recorded Objects** tab to view the extracted information of all the objects that appear in the **Root Cause Chain** screen.

### Recorded Objects

This screen displays the following details:

**TABLE 3-11. Recorded Objects Details**

<table>
<thead>
<tr>
<th><strong>COLUMN NAME</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Recorded Object</td>
<td>The name of the recorded object.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of matched object. For details, see <em>Table 3-4: Valid Item Formats for Retro Scan on page 3-10</em>.</td>
</tr>
<tr>
<td>Created</td>
<td>The time when the object was first discovered.</td>
</tr>
<tr>
<td>Activity</td>
<td>The current activity of the recorded object during the investigation.</td>
</tr>
<tr>
<td>Detail</td>
<td>Additional information extracted from the object. Endpoint Sensor shows only the details applicable for the object type. Also, some objects may contain only a limited set of details, or no details at all.</td>
</tr>
</tbody>
</table>

**Note**

Click **Export** to export the list to a .csv file
Investigation Troubleshooting

The following topics describe specific potential issues involving investigations.

Troubleshooting Investigation Status

The **Information** screen displays the status of each endpoint included in an investigation. Use the table below to troubleshoot errors reported on the **Information** screen.

For details, see *Information on page 3-22*.

**TABLE 3-12. Investigation Status**

<table>
<thead>
<tr>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command waiting to be deployed.</td>
<td>Endpoint has been queued for investigation. Endpoint Sensor updates the status once the investigation command is sent to the agent.</td>
</tr>
<tr>
<td>Command in progress.</td>
<td>Endpoint is being investigated. Wait for the investigation to finish.</td>
</tr>
</tbody>
</table>
| An endpoint error has occurred.| Endpoint is online, but the Endpoint Sensor agent encountered an error.  
If you encounter this message, perform any of the following:  
• Check that the Endpoint Sensor services **ESClient** and **ESE** are running on the endpoint.  
• Restart the endpoint, and then run the investigation again. |
<table>
<thead>
<tr>
<th>STATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Canceled due to timeout.      | No response was received from the endpoint and the timeout period has been reached. After the timeout period, the Endpoint Sensor server stops sending the command, and excludes the endpoint from the current investigation.  
To investigate the endpoint again, include the endpoint in a new investigation. Before performing the new investigation, perform any of the following:  
• Check that the endpoint is running and that the agent is properly installed.  
• By default, the timeout period is set to 86400 seconds (24 hours). This value is set by the **Expiration** parameter. Increase this value if the selected endpoint requires more than 24 hours to send a response.  
For details, see *Modifying the Expiration value on page 3-36*. |
| Canceled due to error         | An unknown error has occurred and Endpoint Sensor has canceled the investigation for the endpoint.  
Once Endpoint Sensor cancels the investigation for an endpoint, it excludes the endpoint from the current investigation. To investigate the endpoint again, include the endpoint in a new investigation. Before performing the new investigation, perform any of the following:  
• Check that the endpoint is running and that the agent is properly installed.  
• Restart the endpoint, and then run the investigation again. |
| Canceled due to user interaction | The user has manually canceled the investigation for the endpoint.  
Once Endpoint Sensor cancels the investigation for an endpoint, it excludes the endpoint from the current investigation. To investigate the endpoint again, include the endpoint in a new investigation. |
Troubleshooting Invalid IOC Files

Ensure that the default `OpenIOC.xsd` file is present on the Endpoint Sensor server.

---

**Note**

`OpenIOC.xsd` verifies the content of an IOC file

---

**Procedure**

1. On the Endpoint Sensor server computer, open a command prompt (`cmd.exe`) and navigate to the `<Trend Micro Endpoint Sensor server installation path>`\`\CmdTool\IOCTool\` folder.

2. Issue the following command:

```
$ ...
```

---

**Note**

The `OpenIOC.xsd` and `IOCTool.exe` files must be in the IOCTool folder.

---

```
C:\...
```

---

The following output appears:

```
Use schema: OpenIOC.xsd, ns:_http://OpenIOC.org/schemas/IOC_1.1
ERROR: The '_http://OpenIOC.org/schemas/IOC_1.1:ioc' element is not declared.
```

The `ERROR: ...` indicates that the IOC file in question does not adhere to the syntax and conditions required to validate and parse IOC files. To solve the issue, follow the IOC schemas and related instructions available in [http://OpenIOC.org/](http://OpenIOC.org/).
Troubleshooting Invalid YARA Rules

Procedure

1. On the Endpoint Sensor server, open a command prompt (cmd.exe) and navigate to the `<Trend Micro Endpoint Sensor server installation path>\CmdTool\YARA` folder.

2. Issue the following command:

   ```
   $...\CmdTool\YARA>yara –m <YARA_file>
   ```

   `<YARA_file>` corresponds to full file name of the YARA file in question.

   **Note**

   For additional command line options, refer to the YARA documentation online:


The following output appears:

   ```
   $:\...\CmdTool\YARA>yara -m c:\invalid.yara
   c:\invalid.yara(6): error: unterminated string
   c:\invalid.yara(6): error: syntax error, unexpected $end, expecting _REGEXP_
   ```

   The `error: ...` results indicate that the YARA file in question does not adhere to the syntax required to validate and parse YARA files. To solve the issue, follow the instructions available from [http://plusvic.github.io/yara/](http://plusvic.github.io/yara/).

Troubleshooting Server Database Size

The Endpoint Sensor server uses a database to store its records. By default, the database grows in size as it records more information. However, the database may be configured to limit itself to a fixed size. To change the server database size, perform the following procedure:
Before performing the following steps, Trend Micro recommends creating a back up of the Endpoint Sensor SQL database using your preferred SQL application.

Procedure

1. Use any application that can send a query statement to the SQL server.
2. Connect to the Endpoint Sensor SQL database, and send the following commands:
   • To turn the auto-purge feature on:
     ```sql
     UPDATE dbo.Setting set Value = CAST('1' as varbinary)
     WHERE Category='/TMSL/SQLServer/' AND [Key]='CheckDBSize'
     UPDATE dbo.Setting set Value = CAST('<value>' as varbinary)
     WHERE Category='/TMSL/SQLServer/' AND [Key]='DBSizeLimitMB'
     ```
   • To turn the auto-purge feature off:
     ```sql
     UPDATE dbo.Setting set Value = CAST('0' as varbinary)
     WHERE Category='/TMSL/SQLServer/' AND [Key]='CheckDBSize'
     ```

   Note
   Set `<value>` to the preferred maximum size of the database in MB.

3. The database resizes when the next investigation is triggered. Server performance may be affected while the database is resizing. Performance returns to normal once the database has been set to the specified size.

Note
To manage the database size of Endpoint Sensor agents, use the Endpoints screen. For details, *Endpoint on page 2-7.*

Modifying the Expiration value

The Endpoint Sensor server also uses the `config.xml` file to control how often it resends the investigation command to offline or unreachable agents. It may be necessary
to edit these values to ensure that endpoints are given sufficient time to respond. To change how often these commands are sent, perform the following procedure:

**Procedure**

1. Stop the Endpoint Sensor service using the command prompt:
   
   C:\>sc stop TrendMicroEndpointSensorService

2. Locate `<Trend Micro Endpoint Sensor server installation path>\config.xml`.

3. Back up the `config.xml` file, then open the file using a text editor.

4. Locate and edit the following value:

   ```xml
   <TaskTracking>
   <Expiration>86400</Expiration>
   </TaskTracking>
   ```

   `<Expiration>86400</Expiration>` sets how long Endpoint Sensor server waits before it stops resending the investigation command. The value is expressed in seconds. After this time, the server displays a Command processing timeout status for the agent. The default value is 86400 seconds, or after 24 hours.

   **Note**

   Ensure that the value for `<Expiration>` is greater than zero.

5. To apply the new values, restart the Endpoint Sensor service using the command prompt:

   C:\>sc start TrendMicroEndpointSensorService
Chapter 4

Monitoring Files

This section provides information on how to use Endpoint Sensor to monitor endpoints for suspicious files.

Topics include:

• Monitoring on page 4-2
• Submitted for Analysis on page 4-7
• Monitoring Log on page 4-10
• Purging Monitoring Tables on page 4-13
Monitoring

To protect against attacks, Endpoint Sensor can monitor each endpoint for specific files through the use of monitoring rules. Monitoring rules follow the same IOC format used in investigations. Administrators can define and upload monitoring rules customized to their needs. Endpoint Sensor also comes with a preloaded IOC rule provided by Trend Micro which automatically updates to ensure protection against the latest threats.

Once a monitored file is found, Endpoint Sensor can either collect the file in a specific location, or send the file to Deep Discovery Analyzer for further analysis.

For details, see Deep Discovery Analyzer Integration on page 4-7.

The Monitoring menu contains the following options to configure the monitoring behavior:

- **Monitoring Settings**: Use this screen to manage monitoring rules. Monitoring rules use the IOC format.

- **Submitted for Analysis**: Use this screen to view the analysis results of files sent to Deep Discovery Analyzer.

- **Monitoring Log**: Use this screen to view all collected files.

Monitoring is disabled by default. To start monitoring, go to Monitoring > Monitoring Settings and perform the following steps:

---

**Procedure**

1. Select Enable monitoring and submission to enable the monitoring and collection of files.

2. Upload a customized IOC file to add specific files to monitor. By default, Trend Micro Endpoint Sensor uses the provided IOC file from Trend Micro.

   For details, see Monitoring Rules on page 4-3.

3. Configure monitoring settings.

   For details, see Submission Settings on page 4-5.
4. Click **Save** to start monitoring.

5. Review the following screens to view monitoring results.
   
   • **Submitted for Analysis** shows the analysis results of the files sent to Deep Discovery Analyzer
     
     For details, see *Submitted for Analysis on page 4-7*.
   
   • **Monitoring Log** shows details of all files collected by Trend Micro Endpoint Sensor.
     
     For details, see *Monitoring Log on page 4-10*.

---

**Monitoring Rules**

Use the **Monitoring Rules** tab to view and manage monitoring rules. Monitoring rules come from the following sources:

- **Trend Micro**
  
  Displays monitoring rules provided by Trend Micro. The following table lists all the details available for review:

  **TABLE 4-1. Trend Micro monitoring rules**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Name of the rule</td>
</tr>
<tr>
<td>Version</td>
<td>Version information for the rule</td>
</tr>
<tr>
<td>Latest Update</td>
<td>Date and time when the rule was uploaded</td>
</tr>
<tr>
<td>Action</td>
<td>Commands available to interact with the rule</td>
</tr>
</tbody>
</table>

- **User defined**
  
  Shows all the custom monitoring rules uploaded by the user. The following table lists all the details available for review:
TABLE 4-2. User defined monitoring rules

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Specifies if the rule is disabled or enabled</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name of the uploaded rule</td>
</tr>
<tr>
<td>Description</td>
<td>A short user-defined description of the uploaded rule</td>
</tr>
<tr>
<td>Uploaded</td>
<td>Date and time when the rule was uploaded</td>
</tr>
</tbody>
</table>

Use the following options to manage the table:

- Click **Upload IOC Rule** to select and upload a new monitoring rule. Ensure that the monitoring rule uses the correct IOC format.
  
  For details, see *Supported IOC Indicator Terms on page C-1*.

- Select a rule, and click **Toggle Status** to toggle the status of the rule.

- Select a rule, and click **Remove** to remove the rule from list.
Submission Settings

Use the **Submission Settings** tab to configure if the collected files should be sent to a local file server, or sent to Deep Discovery Analyzer for further analysis. The following options are available:

**Server Location**

- **Send files to local file server**
  - **Path:** `\windows-uucp\nt\submission`
  - **User name:** `administrator`
  - **Password:** `********`
  - **Archive password:** `virus`

- **Send files to Deep Discovery Analyzer for analysis**
  - **Server address:** `10.1.173.182`
  - **Port:** `443`
  - **API key:** `808BE229-4302-49F2-A3C6-C9EAF5FS81`

To configure proxy settings, go to **Proxy Settings**.

[Image of the Endpoint Sensor interface]
### Table 4-3. Destination

<table>
<thead>
<tr>
<th>Option</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send files to local file server</td>
<td>Specify the following details:</td>
</tr>
<tr>
<td></td>
<td>• Path</td>
</tr>
<tr>
<td></td>
<td>• User name</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Archive password</td>
</tr>
<tr>
<td></td>
<td>Endpoint Sensor compresses the files in a password protected zip file before sending the file to the file server. Specify the default archive password here.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>Endpoint Sensor is unable to send files to a local server that requires a proxy server to access.</td>
</tr>
<tr>
<td>Send files to Deep Discovery Analyzer for analysis</td>
<td>Specify the following details:</td>
</tr>
<tr>
<td></td>
<td>• Server Address</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• API key</td>
</tr>
<tr>
<td></td>
<td>For details, see Deep Discovery Analyzer Integration on page 4-7.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>If a proxy is required for connecting to the Deep Discovery Analyzer server, configure the proxy settings first in the Proxy Setting screen.</td>
</tr>
<tr>
<td></td>
<td>For details, see Proxy on page 5-4.</td>
</tr>
</tbody>
</table>
Deep Discovery Analyzer Integration

For integration, obtain the following information from a Deep Discovery Analyzer server installed on the same network:

• API key. This is available on the Deep Discovery Analyzer management console, in Help > About.

• Deep Discovery Analyzer IP address. If unsure of the IP address, check the URL used to access the Deep Discovery Analyzer management console. The IP address is part of the URL.

• Deep Discovery Analyzer SSL port 443.

Note

• Endpoint Sensor supports integration with Deep Discovery Analyzer 5.1 and later.

• If the Deep Discovery Analyzer API key changes after integration, clear the old Deep Discovery Analyzer settings from Endpoint Sensor before specifying a new API key.

• Since the Endpoint Sensor agents send the samples directly to Deep Discovery Analyzer server, ensure that the Endpoint Sensor agents have network access to the Deep Discovery Analyzer server to be integrated.

For details, refer to the documentation available at:


Submitted for Analysis

Once Endpoint Sensor finds a file matching the attributes defined in the monitoring rule, it uploads the file to a local server, or sends the file to Deep Discovery Analyzer. Use the Submitted for Analysis screen to view all collected files submitted to Deep Discovery Analyzer. The following table lists all the details available for review:
### TABLE 4-4. Submitted for Analysis

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis Status</td>
<td>Status of the submitted file base on the analysis made by Deep Discovery Analyzer</td>
</tr>
<tr>
<td>File Name</td>
<td>File name of the submitted object</td>
</tr>
<tr>
<td>File Path</td>
<td>Local path of the submitted object in the endpoint</td>
</tr>
<tr>
<td>SHA-1 Hash Value</td>
<td>SHA-1 hash value of the submitted object</td>
</tr>
<tr>
<td>Rule Category</td>
<td>Classification based on the six stages of a targeted attack. For details, see Rule Category on page 4-9.</td>
</tr>
<tr>
<td>Source Host</td>
<td>Host name of the endpoint that submitted the object</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of the endpoint that submitted the object</td>
</tr>
<tr>
<td>Submitted Time</td>
<td>Date and time when object was submitted</td>
</tr>
</tbody>
</table>

Click ▶ to view more details about each file.
Rule Category

Endpoint Sensor classifies the analyzed files based on the object's behavior and origin.

**TABLE 4-5. Rule Categories**

<table>
<thead>
<tr>
<th>STAGE</th>
<th>BEHAVIOR DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence gathering</td>
<td>Performs extensive research using readily available public information, network scanning tools, social media, and other sources to identify promising points of entry, and uncover the structure of existing defenses</td>
</tr>
<tr>
<td>Point of entry</td>
<td>Uses tactics and techniques used to gain entry to a network, including but not limited to:</td>
</tr>
<tr>
<td></td>
<td>• Sending emails with a malicious file attachment, or a link to a malicious URL</td>
</tr>
<tr>
<td></td>
<td>• Compromising a legitimate web site to download malware</td>
</tr>
<tr>
<td></td>
<td>• Directly hacking the target system</td>
</tr>
<tr>
<td></td>
<td>• Penetrating a partner’s network and hitching a ride into yours via normal communication</td>
</tr>
<tr>
<td></td>
<td>• Using unsecured or third-party networks (hotel, coffee shop, airport, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Delivering attack code via a USB or other removable storage media</td>
</tr>
<tr>
<td>Command-and-control (C&amp;C)</td>
<td>Initiates communication with a C&amp;C server to deliver information, receive instructions, and download other malware. This allows attackers to actively respond to security efforts, or to new information about the network. C&amp;C traffic can occur to/from a trusted IP address or a malicious host, using various communication and encryption protocols.</td>
</tr>
<tr>
<td>Lateral movement</td>
<td>Identifies other assets within the network that it can use to move from system to system. These search for directories, email, and administration servers to map the internal structure of the network and obtain credentials to access these systems.</td>
</tr>
<tr>
<td>STAGE</td>
<td>BEHAVIOR DESCRIPTION</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Asset/data discovery</td>
<td>Locates the specific servers and services that contain the most valuable data by scanning selected ports, monitoring internal traffic, etc.</td>
</tr>
<tr>
<td>Data exfiltration</td>
<td>Copies data for extraction and monetization, through the use of encryption, compression, and other techniques to disguise the activity. Data is transmitted to external locations, where it will be put up for sale on the black market.</td>
</tr>
<tr>
<td>Attack accomplice</td>
<td>Runs functions that assist in the routines of other malware involved in the attack.</td>
</tr>
<tr>
<td>User defined</td>
<td>Files specified by the user through user-defined IOC files.</td>
</tr>
</tbody>
</table>

The classification is based mainly on the six stages of a targeted attack.

For details, refer to the documentation available at:


**Monitoring Log**

Use the **Monitoring Logs** screen to view all files collected by the monitoring process.
The following table lists all the details available for review:

**TABLE 4-6. Monitoring Log**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Time</td>
<td>Date and time when the object was detected.</td>
</tr>
<tr>
<td>Rule Category</td>
<td>Classification based on the six stages of a targeted attack. For details, see Rule Category on page 4-9.</td>
</tr>
<tr>
<td>Host</td>
<td>Endpoint where the object was found.</td>
</tr>
<tr>
<td>Objects</td>
<td>Number of objects found in the endpoint.</td>
</tr>
<tr>
<td>Upload Pending</td>
<td>Number of objects to be uploaded to Deep Discovery Analyzer.</td>
</tr>
<tr>
<td>COLUMN NAME</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>High Suspicious Objects</td>
<td>Number of objects classified as highly suspicious by Deep Discovery Analyzer.</td>
</tr>
</tbody>
</table>

Use Filters to filter this list by Detection, Host, Objects, Category and Risk Level.

To view more details about a collected object, click the value in the Objects, Upload Pending or High Suspicious Objects column to open the Object List screen. This screen contains the following details for review:

**TABLE 4-7. Object List**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Name</td>
<td>Name of the object collected.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Type of the object collected.</td>
</tr>
<tr>
<td>Analysis Result</td>
<td>Severity level based on the analysis by Deep Discovery Analyzer</td>
</tr>
<tr>
<td>File Path</td>
<td>Local path which specifies the location of the object in the endpoint</td>
</tr>
<tr>
<td>Upload Location</td>
<td>Uniform Naming Convention (UNC) path which specifies the location of the server where the object was sent.</td>
</tr>
<tr>
<td>Detection Time</td>
<td>Date and time when the object was detected.</td>
</tr>
<tr>
<td>Signer Name</td>
<td>Name of the signer, if the object was signed</td>
</tr>
</tbody>
</table>

Use the following options to manage the list:

- The list can be filtered by Upload Status and Analysis Result.
- Click Upload Location path to copy the UNC location to the clipboard.

**Note**

The UNC path is given using the Windows format. It may be necessary to modify the path to use the copied string in a different operating system.
Purging Monitoring Tables

It may be necessary to purge the Submitted for Analysis and Monitoring Log tables to improve server performance. To purge the Submitted for Analysis and Monitoring Log tables, perform the following procedure:

**Procedure**

1. Install SQL Server Management Studio.
2. Open SQL Server Management Studio, locate and connect to the Endpoint Sensor database SMARTSENSOR.
3. Open Programmability > Stored Procedures.
4. Locate and right-click the following items. For each item, click Execute Stored Procedure. On the screen that appears, update the values according to your preference.

<table>
<thead>
<tr>
<th>STORED PROCEDURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbo.SP_IRB_DeleteInspectedReportByDay</td>
<td>Stored procedure purges reports <em>n</em> days before today.</td>
</tr>
<tr>
<td>dbo.SP_IRB_DeleteInspectedReportByNumber</td>
<td>Stored procedure purges <em>n</em> oldest reports.</td>
</tr>
</tbody>
</table>
5. After updating each item, press **Enter**, or click **OK** to run the stored procedure.
Chapter 5

Managing Trend Micro Endpoint Sensor

This section describes how to perform administrative tasks to configure Endpoint Sensor.

Topics include:

• Updates on page 5-2
• Proxy on page 5-4
• Management Console on page 5-5
• Accounts on page 5-6
• About on page 5-8
• License on page 5-9
Administration

The **Administration** menu contains the following options to configure Endpoint Sensor:

**Updates**

Use the **Updates** screen to manage updates for Endpoint Sensor.
Select **Download monitoring rules from the following source** to enable the update options. Afterwards, configure a download source for monitoring rules:

- Trend Micro's Active Update Server
- Other update source

Click **Test server connection** to verify if the specified source is accessible.

If the update source requires a proxy, specify the details below:

**TABLE 5-1. Proxy Settings Requirements**

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>ACTION REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a proxy to connect to the source</td>
<td>Proxy settings are disabled by default. Select to use and configure a proxy for the connection.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select HTTP or SOCKS5 protocols</td>
</tr>
<tr>
<td>Server name or IP address</td>
<td>Specify the IP address or URL of the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the listening port of the proxy server.</td>
</tr>
<tr>
<td>Proxy server authentication</td>
<td>Select if the proxy server requires a user name and password for access.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the user name for authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password for authentication.</td>
</tr>
</tbody>
</table>
Proxy

Use the **Proxy** screen to configure communication over a proxy.

Specify the proxy settings for the following connections:

- Endpoint to Server
- Endpoint to Deep Discovery Analyzer
- Server to Active Update Server
- Server to Deep Discovery Analyzer

Select the check box in the preferred tab to enable the proxy options. Afterwards, change the following options according to your preference:
Table 5-2. Proxy Requirements

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>ACTION REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select HTTP or SOCKS5 protocols</td>
</tr>
<tr>
<td>Server name or IP address</td>
<td>Specify the IP address or URL of the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the listening port of the proxy server.</td>
</tr>
<tr>
<td>Proxy server authentication</td>
<td>Select if the proxy server requires a user name and password for access.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the user name for authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password for authentication.</td>
</tr>
</tbody>
</table>

**Note**

The Endpoint Sensor management console sets the proxy settings for new agents only. To change the proxy settings of existing agents, contact Trend Micro support.

Management Console

Use the Management Console screen to configure settings for Endpoint Sensor.

![Management Console Screen](image)

Timeout settings

- **Enable automatic log out from the management console settings**
  - Automatically log out of the management console after **30** minutes

Change the following options according to your preference:
TABLE 5-3. Management Console

<table>
<thead>
<tr>
<th>OPTIONS</th>
<th>ACTION REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic log out from the web console</td>
<td>Select to enable the timeout period. The timeout period is disabled by default.</td>
</tr>
<tr>
<td>Automatically log out of the web console after x minutes</td>
<td>Specify a timeout value in minutes. The console logs the user out after the specified period of inactivity.</td>
</tr>
</tbody>
</table>

Accounts

Use the Accounts screen to manage accounts used to access Endpoint Sensor.

The following options are available:

TABLE 5-4. Account Information

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Specify an account name and password for the new account. Once saved, account names cannot be edited.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the password for the selected account. Account names cannot be edited. Select at least one account to activate this option.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the selected account from the list. Select at least one account to activate this option.</td>
</tr>
</tbody>
</table>

Endpoint Sensor uses the following criteria to check the password strength:

- The password is 8 to 64 characters long
- The password contains:
  - at least one number
  - at least one lower-case character
  - at least one upper-case character
  - at least one symbol character
- The password does not contain any of these unsupported symbols: | > < " or space

**Tip**

Follow the guidelines below to select a secure password:

- Use a long password. Trend Micro recommends using a password of at least 10 characters, but longer passwords are preferred.
- Avoid names or words in dictionaries.
- Use a combination of mixed-case letters, numbers, and other characters.
- Avoid simple patterns such as “101010” or “abcde.”
About

Use the About screen to view details about the Endpoint Sensor server.

This Server Information section displays the following details:

- GUID
- Version
- Agent Version
- Attack Discovery
- Endpoint Sensor Exception Pattern
- Endpoint Sensor Trusted Pattern
- Third party licenses

Guidance: 20a2674c-689a-5b29-aa52-179dc5e29a2
Version: 1.6.0.3076
Agent Version: 1.6.0.3075
Attack Discovery: 10.1039.00
Endpoint Sensor Exception Pattern: 2.0.27
Endpoint Sensor Trusted Pattern: 1.113.0
Third party licenses: License attributions
Click License Attributions to view the licenses for third party components used by Endpoint Sensor.

License

Use the License screen to review the license status and update the activation codes for the following installations:

- Endpoint Agent
- Server Agent

This screen displays the following details for each installation:
## Table 5-5. License Details

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>Displays the Activation Code of the product. Click <strong>Update</strong> to type a new Activation Code.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the Activation Code. Status may be any of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Grace period</td>
</tr>
<tr>
<td></td>
<td>• Activated</td>
</tr>
<tr>
<td></td>
<td>• Not activated</td>
</tr>
<tr>
<td></td>
<td>• Near expiry date</td>
</tr>
<tr>
<td></td>
<td>• Expired</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of Activation Code. Type may be any of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Full</td>
</tr>
<tr>
<td></td>
<td>• Invalid</td>
</tr>
<tr>
<td>Expiration date</td>
<td>Displays the date when the Activation Code will expire.</td>
</tr>
</tbody>
</table>

**Note**

Contact your Trend Micro representative if any of the following conditions are true:

- The **Status** of the Activation Code is displayed as **Near expiry date**, **Grace Period** or **Expired**.
- The **Type** of the Activation Code is displayed as **Invalid**.
- The **Expiration date** of the Activation Code has already passed.
Chapter 6

Technical Support

Learn about the following topics:

• Troubleshooting Resources on page 6-2
• Contacting Trend Micro on page 6-3
• Sending Suspicious Content to Trend Micro on page 6-4
• Other Resources on page 6-5
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

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:


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 [http://about-threats.trendmicro.com/us/threatencyclopedia#malware](http://about-threats.trendmicro.com/us/threatencyclopedia#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:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Incorporated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225 E. John Carpenter Freeway, Suite 1500</td>
</tr>
<tr>
<td></td>
<td>Irving, Texas 75062 U.S.A.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone</th>
<th>Phone: +1 (817) 569-8900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Toll-free: (888) 762-8736</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Website</th>
<th><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Email address</th>
<th><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></th>
</tr>
</thead>
</table>

- Worldwide support offices:
  

- Trend Micro product documentation:
  
  [http://docs.trendmicro.com](http://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://ers.trendmicro.com/

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

File Reputation Services

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


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):

http://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:

http://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:

http://www.trendmicro.com/download/documentation/rating.asp
OfficeScan Integration

The following content explains how to use the Trend Micro Endpoint Sensor Deployment Tool OfficeScan plug-in to deploy Endpoint Sensor across an enterprise with endpoints managed by OfficeScan.

Topics include:

• About Trend Micro OfficeScan Integration on page A-2
• About Plug-in Manager on page A-2
• Installing OfficeScan on page A-3
• Agent Installation Considerations When Using OfficeScan on page A-4
• Using the Trend Micro Endpoint Sensor Deployment Tool on page A-4
• Trend Micro Endpoint Sensor Agent Deployment Tasks on page A-11
• The OfficeScan Agent Tree on page A-14
About Trend Micro OfficeScan Integration

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.

The agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent.

Note
For information about OfficeScan, see the supporting documentation at:


Use the OfficeScan Trend Micro Endpoint Sensor Deployment Tool plug-in to deploy Endpoint Sensor agents to OfficeScan managed endpoints. You can select endpoints based on specific criteria and see the status of the deployment.

After the Trend Micro Endpoint Sensor Deployment Tool plug-in deploys the Endpoint Sensor agent software, the Endpoint Sensor agent synchronizes to the Endpoint Sensor server specified in the plug-in. OfficeScan does not manage Endpoint Sensor agents or perform investigations. The OfficeScan agent and the Endpoint Sensor agent are independent on the same endpoint.

About Plug-in Manager

OfficeScan includes a framework called Plug-in Manager that integrates new solutions into the existing OfficeScan environment. To help ease the management of these solutions, Plug-in Manager provides at-a-glance data for the solutions in the form of widgets.

Note
None of the plug-in solutions currently support IPv6. The server can download these solutions but is not able to deploy the solutions to pure IPv6 Trend Micro Endpoint Sensor agents or pure IPv6 hosts.
Plug-in Manager delivers the following:

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

- **Plug-in programs**
  
  Plug-in programs are not part of the OfficeScan program. The plug-in programs have separate licenses and management consoles. Access the management consoles from within the OfficeScan web console. Examples of plug-in programs are **Trend Micro OfficeScan ToolBox** and **Trend Micro Security (for Mac)**.

- **Dashboard tabs and widgets**
  
  The OfficeScan **Summary** screen requires Plug-in Manager to display the tabs and widgets used to monitor the OfficeScan server and agent protection status.

This document provides a general overview of plug-in program installation and management and discusses plug-in program data available in widgets. Refer to specific plug-in program documentation for details on configuring and managing the program.

### Installing OfficeScan

For information about installing and configuring OfficeScan, see the documentation available at:


For information on how to prepare the OfficeScan Trend Micro Endpoint Sensor Deployment Tool before deploying agents, see the *Endpoint Sensor Installation and Migration Guide*. 
Agent Installation Considerations When Using OfficeScan

When using OfficeScan to install the Endpoint Sensor agent, check that your environment meets the following criteria:

• The server must have one of the following versions of OfficeScan installed:
  • OfficeScan version 10.6
  • OfficeScan version 10.6 Service Pack 1
  • OfficeScan version 10.6 Service Pack 2
  • OfficeScan version 10.6 Service Pack 3
  • OfficeScan version 11
  • OfficeScan version 11 Service Pack 1
  • OfficeScan XG

• The server must have Microsoft Internet Explorer 9 or later installed.

• The OfficeScan installation must have Plug-in Manager installed.

• The OfficeScan installation must not be installed in an Apache HTTP Server environment. Endpoint Sensor does not support Apache HTTP Server environments.

Using the Trend Micro Endpoint Sensor Deployment Tool

This section outlines how to configure OfficeScan in order to install or uninstall the Trend Micro Endpoint Sensor Deployment Tool.

Topics include:

• Trend Micro Endpoint Sensor Deployment Tool Installation on page A-5
Trend Micro Endpoint Sensor Deployment Tool Installation

Plug-in programs display on the Plug-in Manager console. Use the console to download, install, and manage the programs. Plug-in Manager downloads the installation package for the plug-in program from the Trend Micro ActiveUpdate server or from a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts the installation, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program installation or management from the Trend Micro Control Manager single sign-on function.

Installing Trend Micro Endpoint Sensor Deployment Tool

Procedure

1. Open the OfficeScan web console and click Plug-in Manager in the main menu.

2. On the Plug-in Manager screen, go to the Endpoint Sensor plug-in section and click Download.

   The size of the plug-in program package displays beside the Download button. Plug-in Manager stores the downloaded package to <OSCE server installation folder>\PCCSRV\Download\Product.

   Monitor the progress or navigate away from the screen during the download.

3. Click Agree to install the plug-in program.
Monitor the progress or navigate away from the screen during the download.

After the installation, the current plug-in program version displays on the **Plug-in Manager** screen.

---

**Note**
- If OfficeScan encounters problems downloading or installing the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs > Server Update**.
- Trend Micro recommends using Internet Explorer 9 to access Trend Micro Endpoint Sensor Deployment Tool.

---

**Plug-in Program Management**

Configure settings and perform program-related tasks from the plug-in program’s management console, which is accessible from each OfficeScan web console. Tasks include activating the program and deploying the plug-in program agent to endpoints. Consult the documentation of the specific plug-in program for details on configuring and managing the program.

---

**Managing Trend Micro Endpoint Sensor Deployment Tool**

**Procedure**

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

---

**Trend Micro Endpoint Sensor Deployment Tool Uninstallation**

Uninstall a plug-in program in the following ways:
• Uninstall the OfficeScan server, which uninstalls Plug-in Manager and all installed plug-in programs. For instructions on uninstalling the OfficeScan server, see the *OfficeScan Installation and Upgrade Guide*.

• Uninstall the plug-in program from the Plug-in Manager console.

---

**WARNING!**

Uninstalling the Trend Micro Endpoint Sensor Deployment Tool automatically uninstalls all agents listed in the agent tree. To ensure that all agents uninstall properly, use the agent tree to uninstall all agents first before uninstalling the Trend Micro Endpoint Sensor Deployment Tool.

For details, see *Uninstalling the Trend Micro Endpoint Sensor Agent on page A-17*.  

---

**Uninstalling Trend Micro Endpoint Sensor Deployment Tool from the Plug-in Manager Console**

**Procedure**

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.

2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Uninstall**.

3. Refresh the **Plug-in Manager** screen after the uninstallation.

   The plug-in program is available for reinstallation.

---

**Deployment Tool Error Codes**

The following error codes may appear while using the Trend Micro Endpoint Sensor Deployment Tool. Use the following list for potential solutions to issues you may encounter.
TABLE A-1. Deployment Tool Error Codes

<table>
<thead>
<tr>
<th>ERROR CODE</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>-113</td>
<td>Endpoint Sensor is unable to obtain required Windows environment information. Endpoint Sensor cannot determine whether the environment uses x86 or x64 architecture. Contact your system administrator.</td>
</tr>
</tbody>
</table>
| -114       | Verification of the installation package or Endpoint Sensor program was unsuccessful.  
• If you were installing Endpoint Sensor, download the installation package again and retry installation.  
• If you were uninstalling Endpoint Sensor, check if the program files have been successfully removed from the endpoint. If files have not been removed, contact technical support. |
| -116       | The Endpoint Sensor certificate or the certificate manager tool is either missing or corrupt. Download the installation package again and retry installation. |
| -151       | Endpoint Sensor is unable to perform installation. This problem could be caused by a variety of reasons. Check the following and try again:  
• The user account may have insufficient permissions to install the program.  
• A previous Endpoint Sensor agent may not have been completely removed.  
• Another process or service may be interrupting installation.  
• The system may be busy or locked.  
If installation is still unsuccessful, download the installation package again and retry installation. If this problem persists, contact technical support. |
<p>| -152       | A Endpoint Sensor agent is already installed on the endpoint. If you were attempting to update the Endpoint Sensor agent version, uninstall the previous agent, and try again. |</p>
<table>
<thead>
<tr>
<th>ERROR CODE</th>
<th>DETAILS</th>
</tr>
</thead>
</table>
| -153       | Endpoint Sensor is unable to install requisite files. This problem could be caused by a variety of reasons. Check the following and try again:  
  • The user account may have insufficient permissions to install the program.  
  • Another process or service may be interrupting installation.  
  • The system may be busy or locked.  
  If installation is still unsuccessful, download the installation package again and retry installation. If this problem persists, contact technical support. |
<p>| -154       | The Endpoint Sensor service, ESClient, is unable to start. Either the service has timed out, or the system may be busy. Wait for a few minutes, and try again. If this problem persists, check the system logs through Event Viewer to find the cause or contact your system administrator. |
| -157       | Endpoint Sensor is unable to write to the Windows registry. Check that the user account has sufficient permissions to edit the registry and try again. |
| -158       | Endpoint Sensor is unable to read the Windows registry. Check that the user account has sufficient permissions regarding registry and try again. |
| -167       | The configuration file is missing or corrupted, or your user account does not have sufficient privileges to read the configuration file. Check that the user account has sufficient permissions and try again. If this problem persists, contact technical support. |</p>
<table>
<thead>
<tr>
<th>ERROR CODE</th>
<th>DETAILS</th>
</tr>
</thead>
</table>
| -170       | Endpoint Sensor is unable to perform uninstallation. This problem could be caused by a variety of reasons. Check the following and try again:  
- The user account may have insufficient permissions to install the program.  
- Another process or service may be interrupting uninstallation.  
- The system may be busy or locked.  
If this problem persists, contact technical support. |
| -180       | Endpoint Sensor is unable to extract files from the installation package. This problem could be caused by a variety of reasons. Check the following and try again:  
- The installation package may be corrupt. Download the installation package again and retry installation.  
- The endpoint or partition may have insufficient disk space to extract the required files.  
- The system may be busy or locked.  
If this problem persists, contact technical support. |
| -199       | Endpoint Sensor is unable to move files from the temporary folder. This problem could be caused by a variety of reasons. Verify the following and try again:  
- The user account may have insufficient permissions to move files.  
- The endpoint or partition may have insufficient disk space to move the files.  
- The system may be busy or locked.  
If this problem persists, contact technical support. |
Trend Micro Endpoint Sensor Agent Deployment Tasks

The following procedure explains how to install Endpoint Sensor agents.

Procedure

1. Install and open the Trend Micro Endpoint Sensor Deployment Tool plug-in.
   For details, see Using the Trend Micro Endpoint Sensor Deployment Tool on page A-4.

2. Configure the Endpoint Sensor server and download the agent installation package.
   For details, see Downloading the Installation Package on page A-11.

3. Install the Endpoint Sensor agent program to selected endpoints.
   For information on using Agent Tree to select domains and agents, see Agent Tree Specific Tasks on page A-14.
   For information about agent installation, see Installing the Trend Micro Endpoint Sensor Agent on page A-13.

   Once installation is complete, each OfficeScan agent acts independently of each Endpoint Sensor agent.

4. On the Summary screen, verify that all agents have been installed.
   For information about the Summary screen, see Monitoring Trend Micro Endpoint Sensor Agents on page A-14.

5. Use the Endpoint Sensor management console to manage agents and perform investigations.

Downloading the Installation Package

Before you can deploy the Endpoint Sensor agents, you must specify the location where the Endpoint Sensor server downloads the agent installation package.
Note
At any time, if you want to change the current server URL or reset the proxy settings, click Reset Trend Micro Endpoint Sensor Server URL and proxy server.

Procedure

1. Go to Administration > Server Setup.

2. Specify the URL of the Endpoint Sensor server.

   This is the same URL of the Endpoint Sensor server management console. Endpoint Sensor agents report to this server.

3. If you intend to download the agent installation package over a proxy, specify your proxy settings.

   Endpoint Sensor can also use the same proxy server set in OfficeScan. To specify proxy settings for Endpoint Sensor, use the Trend Micro Endpoint Sensor Deployment Tool Set Server screen.

   **TABLE A-2. Proxy Setting Requirements**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy settings toggle</td>
<td>Check the box to enable communication over a proxy.</td>
</tr>
<tr>
<td>Proxy protocol</td>
<td>Endpoint Sensor supports proxy over HTTP or SOCKS5 protocols.</td>
</tr>
<tr>
<td>Server name or IP address</td>
<td>Specify the IP address or URL of the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port of the proxy server.</td>
</tr>
<tr>
<td>User ID</td>
<td>If the proxy server requires authentication, specify the user name for authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>If the proxy server requires authentication, specify the password for authentication.</td>
</tr>
</tbody>
</table>

4. Click Set and Download.
Endpoint Sensor tests the connection to the server, sets the server for Endpoint Sensor agent management, and then attempts to download the latest agent installation package from that server.

---

**Note**

After configuration, the screen changes to show which server has been set up. To download the latest agent installation package, click **Get latest package**.

---

### Installing the Trend Micro Endpoint Sensor Agent

---

**Note**

You can install the Endpoint Sensor agent program to domains or individual agents but not to the root domain.

---

**Procedure**

1. Open the plug-in console and go to the **Agent Management** screen.
2. In the agent tree, select specific domains or agents.
3. Click **Deploy Agent**.
   
   The **Deploy Agent** confirmation screen appears.

---

**Important**

Verify that the operating system of the endpoints where agents will be deployed is supported by Trend Micro Endpoint Sensor Deployment Tool, as the tool will skip installation on endpoints with unsupported operating systems. Trend Micro Endpoint Sensor will generate a list of the endpoints that the Endpoint Sensor agent was not installed on after installation. For details on supported operating systems, refer to the System Requirements section of the Installation Guide.

---

4. Click **Install**.

   Endpoint Sensor begins deploying the agent to the selected endpoints.
If Endpoint Sensor agent installation was skipped on any endpoints, Endpoint Sensor generates a list of those endpoints.

5. Click Close to return to the Agent Management screen.

Monitoring Trend Micro Endpoint Sensor Agents

The Summary screen shows the installation status of the Endpoint Sensor agents.

The Agent Installation Status widget displays the number of endpoints with the Endpoint Sensor agent installed.

Note
Click the Agents hyperlink to view the agents in the Agent Management tree.

The OfficeScan Agent Tree

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

Figure A-1. OfficeScan agent tree

The OfficeScan Agent Tree

The OfficeScan agent tree displays all the agents grouped into domains that the server currently manages. This allows administrators to configure, manage, and apply the same configuration to all domain members.

Agent Tree Specific Tasks

The agent tree displays when you access certain screens on the web console. Above the agent tree are menu items specific to the screen you have accessed. These menu items
allow you to perform specific tasks, such as configuring agent settings or initiating agent tasks. To perform any of the tasks, first select the task target and then select a menu item.

The agent tree provides access to the following functions:

- **Search for computers**: Locate specific endpoints by typing search criteria in the text box.
- **Advanced Search**: Click the hyperlink to display the Advanced Search screen. Locate specific endpoints by using specific search criteria. For details, see *Performing an Advanced Search on page A-15*.
- **Synchronize with OfficeScan**: Synchronize the plug-in program’s agent tree with the OfficeScan server’s agent tree. For details, see *Synchronizing the Agent Tree on page A-16*.
- **Deploy Agent**: Install and deploy Endpoint Sensor agents to selected endpoints or upgrade existing Endpoint Sensor agents to the latest version. For details, see *Installing the Trend Micro Endpoint Sensor Agent on page A-13*.
- **Uninstall**: Uninstall Endpoint Sensor agents from the selected endpoints. For details, see *Uninstalling the Trend Micro Endpoint Sensor Agent on page A-17*.

Administrators can also manually search the agent tree to locate endpoints or domains. Specific computer information displays in the table on the right.

**Performing an Advanced Search**

**Procedure**

1. Open the plug-in program console. On the Agent Management screen, click the Advanced Search link.

   The Advanced Search screen appears.

2. Search for agents by specifying the available criteria.
TABLE A-3. Search Criteria

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 range</td>
<td>Searching by IPv4 address range requires a portion of an IP address starting with the first octet. The search returns all endpoints with IP</td>
</tr>
<tr>
<td></td>
<td>addresses containing that entry. For example, typing 10.5 returns all endpoints in the IP address range 10.5.0.0 to 10.5.255.255.</td>
</tr>
<tr>
<td>Host name</td>
<td>Search by host name.</td>
</tr>
<tr>
<td>Platform</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Endpoint Sensor supports both 32-bit and 64-bit platforms.</td>
</tr>
<tr>
<td></td>
<td>For example, type <strong>Windows Server</strong> to return a list of all Windows Server platform endpoints available.</td>
</tr>
<tr>
<td></td>
<td>Search by operating system.</td>
</tr>
<tr>
<td>Connection status</td>
<td>Search by agent connection status.</td>
</tr>
<tr>
<td>Installation status</td>
<td>Search by agent installation status.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Search by agent domain name.</td>
</tr>
<tr>
<td>Build version</td>
<td>Search by agent version.</td>
</tr>
</tbody>
</table>

3. Click Search.

Synchronizing the Agent Tree

Before the plug-in program can deploy settings to agents, administrators need to synchronize the agent tree with the OfficeScan server.

Procedure

1. Open the plug-in console.
2. On the Agent Management screen, click Synchronize with OfficeScan.
A confirmation message screen appears.

3. Allow a few moments for the synchronization to complete.

After the synchronization completes, the message The client tree has been successfully synchronized with the OfficeScan server appears.

4. Click Close to return to the Agent Management screen.

---

Uninstalling the Trend Micro Endpoint Sensor Agent

**Procedure**

1. Open the plug-in console and go to the Agent Management screen.
2. In the agent tree, select specific domains or agents.
3. Click Uninstall.
4. Click OK to confirm the uninstallation.
5. Click Close in the confirmation dialog.

---

**Tip**

Allow some time for the uninstallation process to complete. Click the Refresh button periodically to view the updated status.
Trend Micro Control Manager Integration

The following content explains how to integrate Endpoint Sensor with Trend Micro Control Manager.

Topics include:

- About Trend Micro Control Manager on page B-2
- Supported Control Manager Versions on page B-2
- Control Manager Integration in this Release on page B-3
- Registering with Control Manager on page B-4
- Adding the Endpoint Sensor Widgets on page B-5
- Using the Endpoint Sensor Investigation Widget on page B-6
- Using Automatic Updates on page B-7
- Trend Micro Endpoint Sensor Policy on page B-9
About Trend Micro Control Manager

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network.

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates, and the configuration and administration of products as groups or as individuals for added flexibility.

Supported Control Manager Versions

Endpoint Sensor supports the following Control Manager versions.

**TABLE B-1. Supported Control Manager versions**

<table>
<thead>
<tr>
<th>ENDPOINT SENSOR VERSION</th>
<th>CONTROL MANAGER VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6 Update 3</td>
<td>• 6.0 SP3 Patch 3</td>
</tr>
<tr>
<td></td>
<td>• 7.0</td>
</tr>
</tbody>
</table>

**Important**

Additional hot fixes need to be installed to enhance integration between Control Manager and Endpoint Sensor. Contact Trend Micro support for details.

Apply the latest patches and critical hot fixes for these Control Manager versions to enable Control Manager to manage Endpoint Sensor. To obtain the latest patches and hot fixes, visit the Trend Micro Update Center at:

[http://www.trendmicro.com/download](http://www.trendmicro.com/download)
After installing Endpoint Sensor, register it to Control Manager and then configure settings for Endpoint Sensor on the Control Manager management console. See the Control Manager documentation for information on managing Endpoint Sensor servers.

Note

- Control Manager 6.0 supports Internet Explorer versions 8 to 11. However, to use Control Manager for configuring settings, managing policies, and viewing investigation results of the registered Endpoint Sensor servers, Internet Explorer 10 and above is recommended.

- Control Manager 7.0 supports Internet Explorer 11, Edge and Google Chrome.

- For known issues related to the integration between Endpoint Sensor and Control Manager, refer to the Control Manager readme.

Control Manager Integration in this Release

This release includes the following features and capabilities when managing Endpoint Sensor servers from Control Manager:

- Use uploaded IOC files in Control Manager to initiate investigations directly to Endpoint Sensor from the Control Manager console.

- Register multiple Endpoint Sensor servers. Control Manager can start simultaneous investigations on multiple Endpoint Sensor servers.

- Pull data from Endpoint Sensor investigation results. The data is then displayed in a Control Manager widget.

- Create and deploy policies to Endpoint Sensor servers registered with Control Manager.

For details, see the Creating and Deploying Policies on page B-10.

- Manage monitoring rules in Control Manager.

For details, see Managing Monitoring Rules on page B-10.

- Configure and deploy Submission settings to Endpoint Sensor servers registered with Control Manager.
For details, see *Managing Submission Settings on page B-12*.

**Registering with Control Manager**

**Procedure**

1. Open the Control Manager management console.

   To open the Control Manager console on any endpoint on the network, open a web browser and type the following:

   https://<Control Manager server name>/Webapp/index.html

   Where `<Control Manager server name>` is the IP address or host name of the Control Manager server.

2. Depending on the version of Control Manager, perform the following:
   - For Control Manager 6.0 SP3 Patch 3:
     Go to **Administration > Managed Servers**.
   - For Control Manager 7.0:
     Go to **Administration > Managed Servers > Server Registration**.

3. On the screen that appears, select **Trend Micro Endpoint Sensor** as the **Server Type**, and then click **Add**.

4. In the **Add Server** screen, provide the following details:
   - Server
   - Display name
   - User name
   - Password

5. Click **Save** to add the server to the list. Repeat these steps to add another server.
Adding the Endpoint Sensor Widgets

Procedure

1. Depending on the version of Control Manager, perform the following:
   - For Control Manager 6.0 SP3 Patch 3:
     Go to Dashboard, and click Server Visibility.
   - For Control Manager 7.0:
     Go to Administration > Managed Servers > Server Registration.

2. On the screen that appears, select Trend Micro Endpoint Sensor as the Server Type, and then click Add.

3. Specify the details of the Endpoint Sensor server to be added, and click Save.

4. Click Close to return to the Dashboard screen.

5. Click Add widgets. On the screen that appears, select the Endpoint Sensor category on the left menu.

The following widgets are available:

**TABLE B-2. Endpoint Sensor Widgets**

<table>
<thead>
<tr>
<th>Widget Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Monitoring Summary by Host</td>
<td>Displays the endpoints which triggered a monitoring rule. Manually refresh the widget to view the most recent data. To configure the widget settings, click ▼.</td>
</tr>
</tbody>
</table>
Endpoint Sensor 1.6 Update 3 Critical Patch Administrator's Guide

<table>
<thead>
<tr>
<th>Widget Name</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Sensor Investigation</td>
<td>Run an investigation and view a quick summary of the latest Trend Micro Endpoint Sensor investigation started from Control Manager. By default, the widget automatically refreshes every 2 minutes. To configure the widget settings, click ▼. For details, see Using the Endpoint Sensor Investigation Widget on page B-6.</td>
<td>After registering a new Endpoint Sensor server, refresh the <strong>Endpoint Sensor Investigation</strong> and <strong>Intelligent Monitoring Summary by Host</strong> widgets to update the contents of the widgets with data from the new server.</td>
</tr>
</tbody>
</table>

6. Select one or both widgets, and click Add widget.

7. The widget now appears in the Dashboard. These widgets display a summary of the most recent investigations and monitoring results of all the registered servers.

---

**Using the Endpoint Sensor Investigation Widget**

**Procedure**

1. Open the Control Manager management console.

2. Go to the tab where the Endpoint Sensor Investigation widget has been added.

3. In the Endpoint Sensor Investigation widget, click **Start a New Investigation**, and then click **Historical Records** or **System Snapshot**, depending on the type of investigation you plan to run.

4. In the screen that appears, specify the required information.

   For details, see Running an Investigation on page 3-2.
The Endpoint Sensor Investigation widget also supports importing C&C callback events as investigation criteria.

a. On the Endpoint Sensor Investigation widget, click **Start a New Investigation > Historical Records**.

b. Select **Retro Scan** as the investigation method.

c. Click **Import from C&C Callback Events**.

d. On the screen that appears, select the C&C callback events that need to be investigated, and click **OK**. The events will be added as investigation criteria.

5. **Click Investigate.**

The screen refreshes and displays the progress of the investigation.

---

**Note**

To stop an ongoing investigation, click **Cancel**.

6. Once the investigation is finished, the widget shows the number of endpoints classified as **Matched**, **Safe**, **Pending** or **Cancelled** during the investigation. Click the result of each classification to view more details.

---

**Using Automatic Updates**

To use Control Manager as a local update server for Endpoint Sensor, perform the following steps:

---

**Procedure**

1. Set up Control Manager to perform a scheduled download of the following patterns:
   - Endpoint Sensor Exception Pattern
   - Endpoint Sensor Trusted Pattern
• Attack Discovery Pattern

---

**Note**

The procedure for configuring Control Manager for automatic updates varies by version. For details, refer to the documentation of the Control Manager version being configured.

---

2. Configure Endpoint Sensor to use Control Manager as its update source.
   a. Open the Endpoint Sensor server management console.
   b. Click **Administration > Updates**.
   c. Enable **Download monitoring rules from the following source**.
   d. Select **Other update source**, and type the following in the textbox below:
      
      http://<Control Manager server Name>/TVCSDownload/Activeupdate
      
   e. Click **Save**.

3. Verify that the update process completes successfully in both Control Manager and Endpoint Sensor.
   • During the next Control Manager update, Control Manager should include the Endpoint Sensor patterns.

---

**Note**

To download the patterns immediately, select **Updates > Manual Download** in Control Manager.

---

• Endpoint Sensor then downloads these patterns from Control Manager during the next Endpoint Sensor scheduled update.
Trend Micro Endpoint Sensor Policy

Control Manager includes a Policy Management feature which allows administrators to remotely update monitoring rules and deploy submission settings on registered servers.

**Note**

Multiple Endpoint Sensor policies can be created, but each server can issue only one policy at a time.

For details, see the Control Manager documentation at:


Preparing the Server for Policy Deployment

By default, recently added Endpoint Sensor servers are placed in the New Entity folder. The servers have to be moved to another folder to be visible for policy deployment.

**Procedure**

1. Open the Control Manager management console.
2. Go to Directories > Products, and click Directory Management.
3. In the directory tree, expand the New Entity folder and locate the server you wish to manage.
4. Perform any of the following:
   - Drag and drop the server to another folder
   - Click Add Folder to create a new folder, and then drag and drop the server to the new folder.
Creating and Deploying Policies

Procedure

1. Open the Control Manager management console.
2. Go to Policies > Policy Management.
4. Click Create.
5. Click Specify Target(s) and select which Endpoint Sensor servers you wish to deploy to.
6. On the Monitoring Settings section, configure monitoring rules and submission settings for the new policy.
7. Click Deploy to immediately start the policy deployment.

Afterwards, Control Manager enforces any subsequent updates to the policy on the target Endpoint Sensor servers every 24 hours.

For details, see the Control Manager documentation at:


Managing Monitoring Rules

Take note of the following considerations:

• Managing monitoring rules:

The Monitoring Rules tab displays user-defined rules only. While monitoring rules are shared across policies, the status of a monitoring rule (Enabled/Disabled/remove) is independent for each policy. Administrators can customize policies by selecting which monitoring rules are enabled, disabled, or remove for each policy. New monitoring rules are disabled by default.

Control Manager is limited to remotely controlling monitoring rules in Endpoint Sensor servers where the rules are part of a Endpoint Sensor policy.
If a new Endpoint Sensor server is registered, Control Manager automatically includes the new Endpoint Sensor server in its rule deployment schedule. Once the next deployment schedule is due, Control Manager uploads all active monitoring rules to the newly registered server.

- **Uploading monitoring rules:**

  To upload a monitoring rule, Click **Policies > Policies Management**, and select **Trend Micro Endpoint Sensor** as the **Product**. Click **Create** to create a new policy, or click an existing policy to open the **Create / Edit Policy** screen. Expand **Monitoring Settings**, click **Upload IOC Rule > Choose File**, and navigate to the location of the monitoring rule. Click **Open** to automatically upload the monitoring rule. After the upload is complete, click **Save** or **Deploy**.

**Note**

- It is recommended to specify the target Endpoint Sensor servers before uploading the rule.

- The **Upload IOC Rule** feature is enabled only when there is at least one Endpoint Sensor server registered to Control Manager.

  For details, see *Registering with Control Manager on page B-4*.

Uploading the same monitoring rule in both Control Manager and in a Endpoint Sensor server registered with Control Manager may cause conflicts. Regularly keep track of the uploaded monitoring rules through the **Monitoring Settings** screen to avoid duplication.

If a duplicate monitoring rule is encountered, the following message appears:
"Unable to upload file. The file already exists in the Endpoint Sensor server. Use the Endpoint Sensor management console to remove the file first, and try again."

- **Changing the status of a monitoring rule:**

  To change the status of a monitoring rule, click **Toggle Status**, and select **Enable** or **Disable**. Afterwards, update the remote rule of the Endpoint Sensor servers specified as targets in this policy.

  The status of a monitoring rule is independent for each policy.
• Removing monitoring rules:

To remove a rule, select the rule and click **Remove**. The status of the removed rule changes to **remove**. Click **Save** or **Deploy** to complete the process.

---

**WARNING!**

- Removal of a monitoring rule also removes the monitoring rule from all other Endpoint Sensor policies.
- If the same rule is re-uploaded in a new policy, the old policy will remove the rule again during its scheduled run.

If problems persist, contact Trend Micro support for assistance.

---

**Managing Submission Settings**

Use the **Submission Settings** tab to specify if the collected files are sent to a local file server, or sent to Deep Discovery Analyzer for further analysis.

For details, see *Submission Settings on page 4-5*.

Control Manager is unable to configure a proxy connection between Endpoint Sensor endpoints and Deep Discovery Analyzer. To configure a proxy connection between Endpoint Sensor endpoints and Deep Discovery Analyzer, use the **Proxy** screen of the Endpoint Sensor server computer.

For details, see *Proxy on page 5-4.*
IOC files consist of one or more indicator terms. These indicator terms specify the variables to use in the investigation. Endpoint Sensor performs the following steps to parse uploaded IOC files:

- Extracts all indicator terms from IOC files
- Converts the supported indicator terms into SQL commands
- Applies these SQL commands as investigation parameters
- Skips all unsupported indicator terms in the IOC file

Endpoint Sensor classifies IOC files as follows:

- Historical records IOCs
  IOC files used for investigating historical events. These IOC files are uploaded in Historical search > IOC files.
  For details, see IOC Samples for Historical Records IOCs on page C-12.

- System process IOCs
  IOC files used for investigating running system processes based on the current system state. These IOC files are uploaded in System snapshot > IOC files.
  For details, see IOC Samples for System Process IOCs on page C-16.
• Disk scanning IOCs

IOC files used for investigating specific files on the system. The uploaded disk IOC file has to include at least one fileitem/filepath or fileitem/fullpath indicator. These IOC files are uploaded in System snapshot > Disk IOC files.

For details, see IOC Sample for Disk Scanning IOCs on page C-21.

• Monitoring IOCs

IOC files used for monitoring specific files on the system. These IOC files are uploaded in Monitoring Setting > User defined.

For details, see Monitoring Rules on page 4-3.

Each classification supports a specific set of indicator terms. Use the table below to determine which indicator term to use.

**TABLE C-1. Supported IOC Indicator Items in Endpoint Sensor 1.6 Update 3 Critical Patch**

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>HISTORICAL RECORDS</th>
<th>SYSTEM PROCESS</th>
<th>DISK SCANNING</th>
<th>MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DnsEntryItem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  **Use DnsEntryItem indicators in Historical Records IOCs to search for network-related queries in database logs.**

  **Use DnsEntryItem indicators in Monitoring IOCs to monitor network-related behavior on the system.**

| dnsentryitem/host             | ✔                   |                | ✔             |            |
| DNS host                      |                     |                |               |            |
| dnsentryitem/recorddata/host  | ✔                   |                |               |            |
| Host name                     |                     |                |               |            |
| dnsentryitem/recorddata/ipv4address | ✔           |                |               | ✔          |
| IPv4 address of the DNS host  |                     |                |               | ✔          |
Supported IOC Indicator Terms

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>HISTORICAL RECORDS</th>
<th>SYSTEM PROCESS</th>
<th>DISK SCANNING</th>
<th>MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileItem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use **FileItem** indicators in **Historical Records** IOCs to search for loaded modules in database logs.

Use **FileItem** indicators in **System Process** IOCs to search for loaded modules in a system snapshot. Do not use **FileItem** indicators for running processes and Windows services.

Use **FileItem** indicators in **Disk Scanning** IOCs to search for loaded modules in a system snapshot. Endpoint Sensor requires at least one **fileitem/filepath** or **fileitem/fullpath** indicator for **Disk Scanning** IOCs.

Use **FileItem** indicators in **Monitoring** IOCs to monitor file access (drop/open) behavior on the system.

| fileitem/accessed           |                    |                |               | ✔          |
| Timestamp when a file was last accessed |                    |                |               |            |
| **Example:** 2000-04-12T09:14:38Z |                    |                |               | ✔          |

| fileitem/created            | ✔                  | ✔              | ✔              |            |
| Timestamp when a file was created |                    |                |               |            |
| **Example:** 2000-04-12T09:14:38Z |                    |                |               | ✔          |

| fileitem/fileextension      | ✔                  |                | ✔              | ✔          |
| File extension name         |                    |                |               |            |
| **Example:** exe            |                    |                |               | ✔          |

| fileitem/filename           | ✔                  | ✔              | ✔              |            |
| Suspicious file name        |                    |                |               |            |

---

**Supported IOC Indicator Terms**

**FileItem** indicators are used to search for loaded modules in database logs, system snapshots, disk scanning, and monitoring. They are categorized as follows:

- **Historical Records**
  - Timestamp and file extension
- **System Process**
  - Timestamp and file extension
- **Disk Scanning**
  - Timestamp and file extension
- **Monitoring**
  - Timestamp and file extension
<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>HISTORICAL RECORDS</th>
<th>SYSTEM PROCESS</th>
<th>DISK SCANNING</th>
<th>MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>fileitem/filepath</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Target landing folder without a file name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For Disk Scanning IOCs, add an asterisk (*) after the path to recursively search subfolders.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> C:\Windows\System32*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Scanning IOCs require at least one filepath or fullpath indicator.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/fullpath</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Full target landing folder including the file name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> C:\Windows \System32\WinSync.dll</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Scanning IOCs require at least one filepath or fullpath indicator.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/md5sum</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Suspicious file MD5 hash value, in hexadecimal format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/modified</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Timestamp when a file was last modified</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> 2000-04-12T09:14:38Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/peinfo/digitalsignature/certificateissuer</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keywords in the file digital certificate issuer section</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INDICATOR</td>
<td>HISTORICAL RECORDS</td>
<td>SYSTEM PROCESS</td>
<td>DISK SCANNING</td>
<td>MONITORING</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>fileitem/peinfo/digitalsignature/certificatesubject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keywords in the file digital certificate subject section</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/shalsum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious file SHA-1 hash value, in hexadecimal format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/sizeInbytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size of file or range of file sizes in bytes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> 101000 TO 120000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/username</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name of the account that created the file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/devicepath</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device path of the file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fileitem/drive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drive of the file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• PortItem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use PortItem indicators in <strong>Historical Records</strong> IOCs for network-related queries and to search for running processes in database logs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use PortItem indicators in <strong>Monitoring</strong> IOCs to to monitor network-related behavior on the system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portitem/creationtime</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp when the connection was established</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> 2000-04-12T09:14:38Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>INDICATOR</strong></td>
<td><strong>HISTORICAL RECORDS</strong></td>
<td><strong>SYSTEM PROCESS</strong></td>
<td><strong>DISK SCANNING</strong></td>
<td><strong>MONITORING</strong></td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------</td>
<td>--------------------</td>
<td>-------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>portitem/localip</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binding local IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portitem/localport</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binding local port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portitem/process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process name binding on a specific port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portitem/remoteip</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected remote IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portitem/remoteport</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected remote port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• ProcessItem

**Use** ProcessItem indicators in **Historical Records** IOCs for network-related queries in database logs.

**Use** ProcessItem indicators in **System Process** IOCs to search for running processes in a system snapshot. Do not use FileItem indicators for running processes and Windows services.

**Use** ProcessItem indicators in **Monitoring** IOCs to monitor the process activity on the system.

<table>
<thead>
<tr>
<th>processitem/handlelist/handle/name</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Handle name or path to handle</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/handlelist/handle/type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows handle type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection created by a specific process name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INDICATOR</td>
<td>HISTORICAL RECORDS</td>
<td>SYSTEM PROCESS</td>
<td>DISK SCANNING</td>
<td>MONITORING</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>processitem/path</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File path to the executable file of the process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/pid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows process ID number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/portlist/portitem/creationtime</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timestamp when a process was created</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example: 2000-04-12T09:14:38Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/portlist/portitem/localip</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected local IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/portlist/portitem/remoteip</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected remote IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/sectionlist/memorysection/digitalsignature/certificateissuer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keywords in the process certificate issuer section</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/sectionlist/memorysection/digitalsignature/certificatesubject</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keywords in the process certificate subject section</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>INDICATOR</strong></td>
<td><strong>HISTORICAL RECORDS</strong></td>
<td><strong>SYSTEM PROCESS</strong></td>
<td><strong>DISK SCANNING</strong></td>
<td><strong>MONITORING</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>-------------------</td>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>processitem/sectionlist/memorysection/shalsum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-1 hash value associated with the process or file, in hexadecimal format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/sectionlist/memorysection/md5sum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious process MD5 hash value, in hexadecimal format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>processitem/username</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account of the process owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **RegistryItem**

  **Use RegistryItem indicators in Historical Records and System Process IOCs for Windows registry-related queries in a system snapshot.**

  **Use RegistryItem indicators in Monitoring IOCs to monitor registry changes related to autorun processes on the system.**

| **registryitem/keypath** | | | |
| Full registry path | | | |
| **Example:** | | | |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Notepad\DefaultFonts | | | |
| **registryitem/path** | | | |
| Keywords within the registry path | | | |
| **registryitem/value** | | | |
| Keywords within the registry data | | | |
### Supported IOC Indicator Terms

<table>
<thead>
<tr>
<th>INDICATOR</th>
<th>HISTORICAL RECORDS</th>
<th>SYSTEM PROCESS</th>
<th>DISK SCANNING</th>
<th>MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>registryitem/valuename</strong></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Name of the registry entry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ServiceItem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use <strong>ServiceItem</strong> indicators in <strong>System Process</strong> IOCs to search for active Windows services in a system snapshot. Do not use <strong>FileItem</strong> indicators for running processes and Windows services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem/description</strong></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keywords within the service description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem/descriptivename</strong></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full descriptive Windows service name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem/name</strong></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short name of the Windows service as stored in the registry</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem/servicedllcertificateissuer</strong></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Keywords in the service DLL certificate issuer section</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem/servicedllcertificatesubject</strong></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Keywords in the service DLL certificate subject section</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem/servicedllmd5sum</strong></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious service MD5 hash value, in hexadecimal format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceitem.startedas</strong></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>User account that started the service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INDICATOR</td>
<td>HISTORICAL RECORDS</td>
<td>SYSTEM PROCESS</td>
<td>DISK SCANNING</td>
<td>MONITORING</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>serviceitem/status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Service status:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• active</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• inactive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>serviceitem/type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Windows service type</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UserItem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use <strong>UserItem indicators</strong> in <strong>Historical Records</strong> IOCs to search for user accounts in database logs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>useritem/fullname</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Domain and user account name</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example: <a href="mailto:user@domain.com">user@domain.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>useritem/grouplist/groupname</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Group name</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>useritem/lastlogin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Most recent/last known access</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example: 2000-04-12T09:14:38Z</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>useritem/username</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User account name</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Note**

- Ensure that IOC files follow the correct syntax. Follow the IOC schemas and related instructions available in [http://OpenIOC.org/](http://OpenIOC.org/).

- Use the **IOCTool** available in the `<Trend Micro Endpoint Sensor installation path>\CmdTool\IOCTool\` folder to troubleshoot invalid IOC files.

  For details, see *Troubleshooting Invalid IOC Files on page 3-34.*
IOCs for Historical Records IOCs

The following IOC sample searches for EXE, DLL, or RAR files in the Recycle Bin.

```xml
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="88e454e9-f94d-4771-baf8-14fc625ea4e4"
last-modified="2014-08-06T06:52:49"
xmns="http://schemas.mandiant.com/2010/ioc">
    <short_description>*New Unsaved Indicator*</short_description>
    <authored_date>2014-08-05T06:35:39</authored_date>
    <links />
    <definition>
        <Indicator operator="AND">
            <IndicatorItem condition="contains">
                <Context document="FileItem"
                    search="FileItem/FileExtension"/>
                <Content type="string">.exe</Content>
            </IndicatorItem>
        </Indicator>
        <IndicatorItem condition="contains">
            <Context document="FileItem"
                search="FileItem/FileExtension"/>
            <Content type="string">.dll</Content>
        </IndicatorItem>
        <IndicatorItem condition="contains">
            <Context document="FileItem"
                search="FileItem/FileExtension"/>
            <Content type="string">.rar</Content>
        </IndicatorItem>
    </definition>
</ioc>
```
The following IOC sample searches for registry entries using the full registry key path Software/Microsoft/Windows/CurrentVersion/run.

<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    id="1ec0039d-b114-40e3-a227-7d936cb07c13"
    last-modified="2015-10-27T10:29:56"
    xmlns="http://schemas.mandiant.com/2010/ioc">
    <short_description>
    *New Unsaved Indicator*
    </short_description>
    <authored_date>2015-10-27T10:29:03</authored_date>
    <links />
    <definition>
        <Indicator operator="OR"
            id="c3962aa6-00e1-494a-b448-1b57f60114af">
            <IndicatorItem id="86a9ff7f-1876-4def-a2f6-05d546cfa7d7" condition="is">
                <Context document="RegistryItem"
                    search="RegistryItem/KeyPath" type="mir" />
                <Content type="string">
                    Software/Microsoft/Windows/CurrentVersion/run
                </Content>
            </IndicatorItem>
        </Indicator>
    </definition>
</ioc>

Conditions for Historical Records IOCs

The following table summarizes the conditions applicable for indicators used by Historical Records IOCs.
<table>
<thead>
<tr>
<th>ITEMS</th>
<th>INDICATOR</th>
<th>CONTAINS</th>
<th>IS</th>
<th>GREATERTHAN</th>
<th>LESSTHAN</th>
<th>STARTSWITH</th>
<th>ENDSWITH</th>
<th>IS_NOT</th>
<th>CONTAINS_NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>fileitem</td>
<td>fileextension</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>fullpath</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>filepath</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>filename</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>username</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>sha1sum</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>md5sum</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>created</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>modified</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>accessed</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>portitem</td>
<td>createiointime</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>process</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>remoteip</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>remoteport</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>localip</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>localport</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ITEMS</td>
<td>INDICATOR</td>
<td>CONTAINS</td>
<td>IS</td>
<td>GREATER_THAN</td>
<td>LESS_THAN</td>
<td>STARTSWITH</td>
<td>ENDSWITH</td>
<td>IS_NOT</td>
<td>CONTAINS_NOT</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------</td>
<td>----</td>
<td>--------------</td>
<td>-----------</td>
<td>-------------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>processitem</td>
<td>name</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>username</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>sectionlist / memorysection / digitalsig / cert</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>sectionlist / memorysection / sha1sum</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>starttime</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>dnsentryitem</td>
<td>host</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>recorddata / host</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>recorddata / ipv4address</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>item</td>
<td>fullname</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>username</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>grouplist / groupname</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>registryitem</td>
<td>fullpath</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
IOC Samples for System Process IOCs

The following IOC sample searches for a qtshark.exe running process using the file path C:\program files\wireshark\qtshark.exe.

```xml
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="88e454e9-f94d-4771-baf8-14fc625ea4e4"
last-modified="2014-08-06T06:52:49"
xmns="http://schemas.mandiant.com/2010/ioc">
  <short_description>*New Unsaved Indicator*
  </short_description>
  <authored_date>2014-08-05T06:35:39</authored_date>
  <links />
  <definition>
    <Indicator operator="AND"
      id="5be0c2e0-53e0-49e9-842d-75d92d3261b3">
      <IndicatorItem
        id="da7e0a00-d6b1-4139-b71f-e4d3e8e47513"
        condition="is">
        <Context document="ProcessItem"
          search="ProcessItem/path" type="mir" />
        <Content type="string">
          C:\program files\wireshark\qtshark.exe
        </Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```

The following IOC file sample searches for a Windows service including the string “support for synchronizing objects” in the description.

```xml
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="88e454e9-f94d-4771-baf8-14fc625ea4e4"
last-modified="2014-08-06T06:52:49"
xmns="http://schemas.mandiant.com/2010/ioc">
  <short_description>*New Unsaved Indicator*
  </short_description>
  <authored_date>2014-08-05T06:35:39</authored_date>
  <links />
  <definition>
    <Indicator operator="AND"
      id="5be0c2e0-53e0-49e9-842d-75d92d3261b3">
      <IndicatorItem
        id="da7e0a00-d6b1-4139-b71f-e4d3e8e47513"
        condition="is">
        <Context document="ProcessItem"
          search="ProcessItem/path" type="mir" />
        <Content type="string">
          C:\program files\wireshark\qtshark.exe
        </Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```
The following IOC file sample searches for a loaded module that contains \program files\wireshark\ in the file path.

```xml
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    id="88e454e9-f94d-4771-baf8-14fc625ea4e4"
    last-modified="2014-08-06T06:52:49"
    xmlns="http://schemas.mandiant.com/2010/ioc">
    <short_description>*New Unsaved Indicator*
    <short_description>
    <authored_date>2014-08-05T06:35:39</authored_date>
    <links />
    <definition>
    <Indicator operator="AND"
        id="5be0c2e0-53e0-49e9-842d-75d92d3261b3">
        <IndicatorItem
            id="da7e0a00-d6b1-4139-b71f-e4d3e8e47513"
            condition="contains">
            <Context document="FileItem"
                search="FileItem/FullPath" type="mir" />
            <Content type="string">
                \program files\wireshark\</Content>
        </IndicatorItem>
    </Indicator>
    </definition>
</ioc>
```
## Conditions for System Process IOCs

The following table summarizes the conditions applicable for indicators used by System Process IOCs.

<table>
<thead>
<tr>
<th>ITEMS</th>
<th>INDICATOR</th>
<th>CONTAINS</th>
<th>IS</th>
<th>GREATERTHAN</th>
<th>LESSTHAN</th>
<th>STARTSWITH</th>
<th>ENDSWITH</th>
<th>IS_NOT</th>
<th>CONTAINS_NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>fileitem</td>
<td>filepath</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>fullpath</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>md5sum</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sizeinbytes</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>created</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>modified</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>accessed</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>peinfo / digitalsignature / certificateissuer</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>peinfo / digitalsignature / certificatesubject</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Supported IOC Indicator Terms

<table>
<thead>
<tr>
<th>ITEMS</th>
<th>INDICATOR</th>
<th>CONTAINS</th>
<th>IS</th>
<th>GREATERTHAN</th>
<th>LESSTHAN</th>
<th>STARTSWITH</th>
<th>ENDSWITH</th>
<th>IS_NOT</th>
<th>CONTAINS_NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>processitem</td>
<td>pid</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>path</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>sectionlist / memorysection / digitalsignature / certificateissuer</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>sectionlist / memorysection / digitalsignature / certificatesubject</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>sectionlist / memorysection / md5sum</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>handlelist / handle / type</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>handlelist / handle / name</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>starttime</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITEMS</td>
<td>INDICATOR</td>
<td>CONTAINS</td>
<td>IS</td>
<td>GREATERTHAN</td>
<td>LESSTHAN</td>
<td>STARTSWITH</td>
<td>ENDSWITH</td>
<td>IS_NOT</td>
<td>CONTAINS_NOT</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------</td>
<td>---------</td>
<td>----</td>
<td>-------------</td>
<td>----------</td>
<td>------------</td>
<td>----------</td>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td>serviceitem</td>
<td>type</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>descriptivename</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>description</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>startedas</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>servicedllcertificat eissuer</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>servicedllcertificat esubject</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>servicedllmd5sum</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>registryitem</td>
<td>keypath</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>path</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>valuename</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>✔️  ✔️</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
IOC Sample for Disk Scanning IOCs

The following IOC sample searches for a file that contains vmtoolsd.exe in the file name and C:\Program Files\VMware\VMware Tools in the file path.

```xml
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    id="72b85cfa-ea89-4633-983b-c2aa01a2b312"
    last-modified="2014-03-12T12:03:59"
    xmlns="http://schemas.mandiant.com/2010/ioc">
    <short_description>QA</short_description>
    <authored_by>Smart Sensor Team</authored_by>
    <authored_date>2014-03-12T11:48:50</authored_date>
    <definition>
        <Indicator operator="OR"
            id="5be0c2e0-53e0-49e9-842d-75d92d3261b3">
            <Indicator operator="AND"
                id="5be0c2e0-53e0-49e9-842d-75d92d3261b3">
                <IndicatorItem
                    id="10ee8b41-3586-41ad-b8ce-90e088706ef4"
                    condition="contains">
                    <Context document="FileItem"
                        search="FileItem/FilePath" type="mir" />
                    <Content type="string">
                        C:\Program Files\VMware\VMware Tools
                    </Content>
                </IndicatorItem>
                <IndicatorItem
                    id="10ee8b41-3586-41ad-b8ce-90e088706ef4"
                    condition="contains">
                    <Context document="FileItem"
                        search="FileItem/FileName" type="mir" />
                    <Content type="string">vmtoolsd.exe</Content>
                </IndicatorItem>
            </Indicator>
        </Indicator>
    </definition>
</ioc>
```
**Conditions for Disk Scanning IOCs**

The following table summarizes the conditions applicable for indicators used by Disk Scanning IOCs.

<table>
<thead>
<tr>
<th>ITEMS</th>
<th>INDICATOR</th>
<th>CONTAINS</th>
<th>IS</th>
<th>GREATERTHAN</th>
<th>LESS_THAN</th>
<th>STARTSWITH</th>
<th>ENDSWITH</th>
<th>IS_NOT</th>
<th>CONTAINS_NOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>fileitem</td>
<td>fileextension</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>filepath</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>fullpath</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>filename</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>md5sum</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sha1sum</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sizeinbytes</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>created</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>modified</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>accessed</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IOC Sample for Monitoring IOCs**

The following IOC sample searches for a `malware.exe` file that connects to an IP address.
Supported IOC Indicator Terms

`<?xml version="1.0" encoding="us-ascii"?>
<ioc>
  <rule_name>CompanyPolicy_1</rule_name>
  <rule_type>KnownThreat</rule_type>
  <rule_description>malware.exe connect ip</rule_description>
  <last_modified_time>2016-02-22T14:32:02</last_modified_time>
  <rule_category></rule_category>
  <author_name>TM_Tester</author_name>
  <source>TMES</source>
  <internalnote>malware.exe connect ip</internalnote>
  <definition>
    <Indicator operator="AND" type="knownthreat">
      <Indicator operator="AND">
        <IndicatorItem condition="is">
          <Context document="FileItem"
            search="FileItem/FileName"/>
          <Content type="string">malware.exe</Content>
        </IndicatorItem>
      </Indicator>
      <IndicatorItem condition="is">
        <Context document="FileItem"
          search="FileItem/Fileextension "/>
        <Content type="string">exe</Content>
      </IndicatorItem>
    </Indicator>
    <Indicator operator="AND">
      <IndicatorItem condition="is">
        <Context document="DnsEntryItem"
          search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">54.209.221.129</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>

Requirements for Monitoring IOCs

Ensure that monitoring IOCs strictly meet the following requirements:

- Contain the following header info:
• Include type="knownthreat" as an attribute of the first Indicator term.

```xml
<Indicator operator="AND" type="knownthreat">
```

• Use only the Indicator terms that are supported by monitoring IOCs.

For details, see Supported IOC Indicator Terms on page C-1.

• Use "AND" operators and "IS" conditions only. Any other condition (such as "contains", "starts-with", etc.) will be ignored.

• Indicator items should explicitly specify the details of the objects to be monitored. Endpoint Sensor will take action only if all given indicator items are exactly matched.

If another IOC rule type is intended to be converted as a monitoring IOC, verify that all the above requirements are met. Add any missing information to ensure compatibility.

As a general rule, Endpoint Sensor matches all indicator items before performing the action specified in the Submission Settings screen. However, if any of the following indicator items are present in the monitoring IOC, finding a match will trigger the action immediately:

• ProcessItem/Portlist/PortItem/Remoteip
• FileItem/Fullpath
• FileItem/Md5sum
• FileItem/Sha1sum
• Portitem/Remoteip
• Dnsentryitem/Host
• Dnsentryitem/Recorddata/Ipv4address

For details, see *Submission Settings on page 4-5*. 
# Index

## A
- about
  - OfficeScan, A-2
- add schedules, 3-6
- Administration, 5-2
- agent
  - install, A-13
  - monitoring, A-14
  - uninstall, A-17
- agent tree, A-14
  - about, A-14
  - specific tasks, A-14
  - synchronize, A-16
- appendix, 1

## C
- Control Manager
  - integration with Trend Micro Endpoint Sensor, B-3

## D
- dashboard, 2-4
- data source
  - historical records, 3-2
  - system snapshot, 3-2
- disk IOC rule, 3-15
- documentation feedback, 6-6

## E
- endpoints, 2-7
  - result details, 3-24

## F
- features and capabilities, 1-3
- frequently asked questions, 1-5

## I
- icons, 3-29
- information, 3-22
- installation
  - agent, A-13
  - plug-in program, A-5
  - status, A-14
- investigation, 3-2
- IOC
  - disk IOC rule, 3-15
  - rule, 3-12
  - sample for disk scanning IOC, C-21
  - sample for Indicators of Compromise, C-12
  - sample for monitoring IOC, C-22
  - sample for registry IOC, C-13
  - samples for system process IOCs, C-16
  - supported IOC Indicator terms, C-1
- IOC rule, 3-12

## M
- management console, 2-2
  - Administration, 5-2
  - admin password, 5-7
  - dashboard, 2-4
  - endpoints, 2-7
  - investigation, 3-2
  - investigation results, 3-20
  - logging on, 2-3
  - schedule, 3-8
  - settings, 5-1
- matched endpoint
  - object list, 3-31
- matched object
icons, 3-29

method
disk IOC rule, 3-15
IOC rule, 3-12
registry search, 3-13
Retro Scan, 3-10
YARA rule, 3-16

O
object list, 3-31
OfficeScan
  synchronize, A-16

P
password, 5-7
period, 3-3
  any, 3-3
  specific, 3-3
Plug-in Manager, A-2
plug-in program
  installation, A-5
  uninstall, A-7

R
recurrence
  repeat, 3-3
  run once, 3-3
registry search, 3-13
result details, 3-24
results, 3-20
  information, 3-22
  result details, 3-24
  root cause chain, 3-25
Retro Scan, 3-10
root cause chain, 3-25
  contents, 3-29
  current screen, 3-29
  customization options, 3-27
  detailed, 3-25
  icons, 3-29
  options for interested objects, 3-27

S
schedule, 3-3, 3-8
  add, 3-6
select targets, 3-4
server, 1-2
  database size, 3-36
settings, 5-1
support
  resolve issues faster, 6-4

T
tags, 3-3
target, 3-3
  select, 3-4
Trend Micro Endpoint Sensor
  about, 1-2
  server, 1-2

U
uninstallation
  agent, A-17
  plug-in program, A-7

Y
YARA rule, 3-16
  sample for driver files, 3-18