TREND MICRO™

1.6 TREND MICRO™ Endpoint Sensor Repack

Administrator's Guide

Next Generation Endpoint Security Against Targeted Attacks and Advanced Threats

for Windows™

Endpoint Security

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

http://docs.trendmicro.com/en-us/enterprise/trend-micro-endpoint-sensor.aspx

Document Part No.: APEM17438/160706

Release Date: August 2016

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://docs.trendmicro.com/en-us/survey.aspx

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Getting Started

Chapter 3: Performing an Investigation

Chapter 4: Monitoring Files

Chapter 5: Managing Trend Micro Endpoint Sensor

Chapter 6: Technical Support

Appendix

Appendix A: OfficeScan Integration

Appendix B: Trend Micro Control Manager Integration

Appendix C: Supported IOC Indicator Terms

Index

Preface

Preface

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

Documentation

The documentation set for Trend Micro Endpoint Sensor includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Trend Micro Endpoint Sensor, and explanations of Trend Micro Endpoint Sensor concepts and features.
Installation Guide	The Installation Guide discusses requirements and procedures for installing the Trend Micro Endpoint Sensor server and agent.
Readme	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.
Online Help	The Online Help contains explanations of Trend Micro Endpoint Sensor components and features, as well as procedures needed to configure Trend Micro Endpoint Sensor.
Support Portal	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: http://esupport.trendmicro.com

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 Trend Micro 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

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

Convention	Description
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Terminology

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

Table 3. Trend Micro Endpoint Sensor Terminology

Terminology	Description
Server	The Trend Micro Endpoint Sensor server
Agent endpoint	The host where the Trend Micro Endpoint Sensor agent is installed
Administrator (or Trend Micro Endpoint Sensor administrator)	The person managing the Trend Micro Endpoint Sensor server
Management console	The user interface for configuring and managing Trend Micro Endpoint Sensor server settings
Activation Code	Codes that enable all Trend Micro Endpoint Sensor features for a specified period of time.

TERMINOLOGY	DESCRIPTION
Agent installation folder	The folder on the host that contains the Trend Micro 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 Trend Micro 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 Trend Micro Endpoint Sensor and the features available in this release.

Topics include:

About Trend Micro Endpoint Sensor

Trend Micro 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, Trend Micro Endpoint Sensor plays a vital role in preventing, monitoring and containing the extent of damage caused by targeted attacks on endpoints and servers.

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

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

What's New

TABLE 1-1. What's New in Version 1.6

FEATURE / ENHANCEMENT	DESCRIPTION
File and behavior monitoring	Trend Micro Endpoint Sensor monitors the entry and routines of suspicious objects, including objects in the Windows registry and memory. Monitoring rules come from the following sources: • User uploaded IOC rules Users can define and upload their own IOC rules to specify files and events to monitor. • Trend Micro Attack Discovery rules To protect the system from recent threats, Trend Micro Endpoint Sensor uses IOC rules from Trend Micro to monitor endpoints for suspicious objects.
File collection	Trend Micro Endpoint Sensor sends all files that match a monitoring rule to a local file server, or to Deep Discovery Analyzer for further analysis.
Active Update	Trend Micro Endpoint Sensor uses the Trend Micro Active Update channel to provide regular updates to the Attack Discovery Rule and the exception list.
Integration with Deep Discovery Analyzer	Trend Micro Endpoint Sensor integrates with Deep Discovery Analyzer to analyze files and provide a comprehensive set of threat details. For details, see *Integration with Deep Discovery Analyzer on page 1-5*.
Improved user interface	The Trend Micro Endpoint Sensor user interface has been redesigned to provide a more intuitive and streamlined experience.

Feature / Enhancement	Description
Multiple user accounts	Trend Micro Endpoint Sensor now supports the creation of multiple accounts for better product management and configuration.
Enhanced security	Trend Micro Endpoint Sensor enforces the use of HTTPS for server communication.

Features and Benefits

The following sections describe the Trend Micro Endpoint Sensor features and benefits:

Threat Investigation

Trend Micro 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. Trend Micro 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, Trend Micro Endpoint Sensor provides the option to perform investigations scheduled at specified intervals.

Customized Endpoint Investigation

Trend Micro 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, Trend Micro 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

Trend Micro 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

Trend Micro Endpoint Sensor can proactively monitor and discover suspicious files and behavior through user-defined IOC rules. Trend Micro 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

Trend Micro 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 Trend Micro 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 1-5*.

Integration with Deep Discovery Analyzer

Trend Micro 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:

http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx

Integration with Control Manager

Trend Micro Endpoint Sensor 1.6 supports integration with Trend Micro™ Control Manager™. 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 Trend Micro Endpoint Sensor servers from a single location.

For details, see the Trend Micro Control Manager documentation.

Compatibility

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

TABLE 1-2. Software Incompatibilities

TREND MICRO ENDPOINT SENSOR SOFTWARE	INCOMPATIBLE SOFTWARE
Server	• Trend Micro Safe Lock™ agent • Trend Micro Safe Lock™ Intelligent Manager
Agent	• Trend Micro™ Titanium™ • Trend Micro™ Internet Security

Important

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

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

http://docs.trendmicro.com/en-us/enterprise/trend-micro-endpoint-sensor/

Chapter 2

Getting Started

This section describes how to get started with Trend Micro Endpoint Sensor.

Topics include:

Getting Started Tasks

Getting Started Tasks provides a high-level overview of all procedures required to get Trend Micro 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*.

4. Configure proxy settings.

   For details, see *Proxy on page 5-4*.

5. Configure management console settings.

   For details, see *Management Console on page 5-5*.

6. Configure monitoring settings.

   For details, see *Monitoring on page 4-2*.

The Management Console

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

- Monitor and investigate endpoints regardless of their location—on premises, remote, or cloud-based

- 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

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

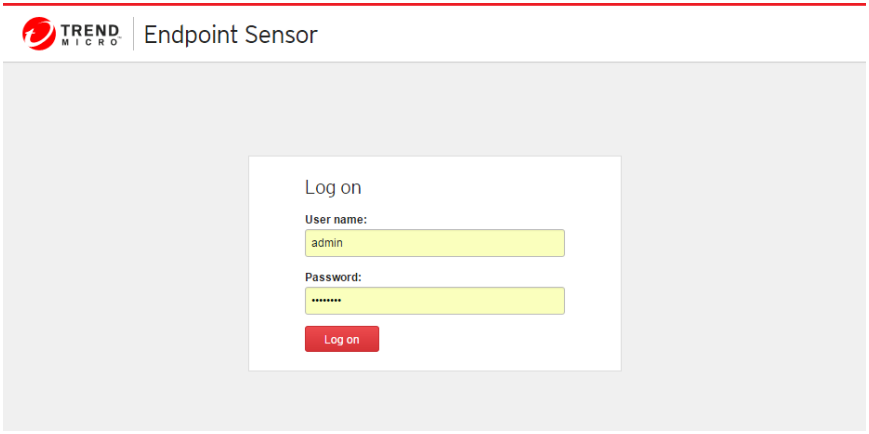
Accessing the management console requires an administrator account and a password. These are set during server installation.

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/
```



2. Specify the following information.

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

     During the Trend Micro Endpoint Sensor server installation, Setup creates the default admin account and prompts you to set the password for this account.

3. Click **Log on**.

The Trend Micro Endpoint Sensor **Dashboard** screen appears.

Dashboard

The Trend Micro 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 hosts, based on the enabled monitoring rules. To manage monitoring rules, go to **Monitoring** > **Monitoring Setting**.

The widget displays the following details:

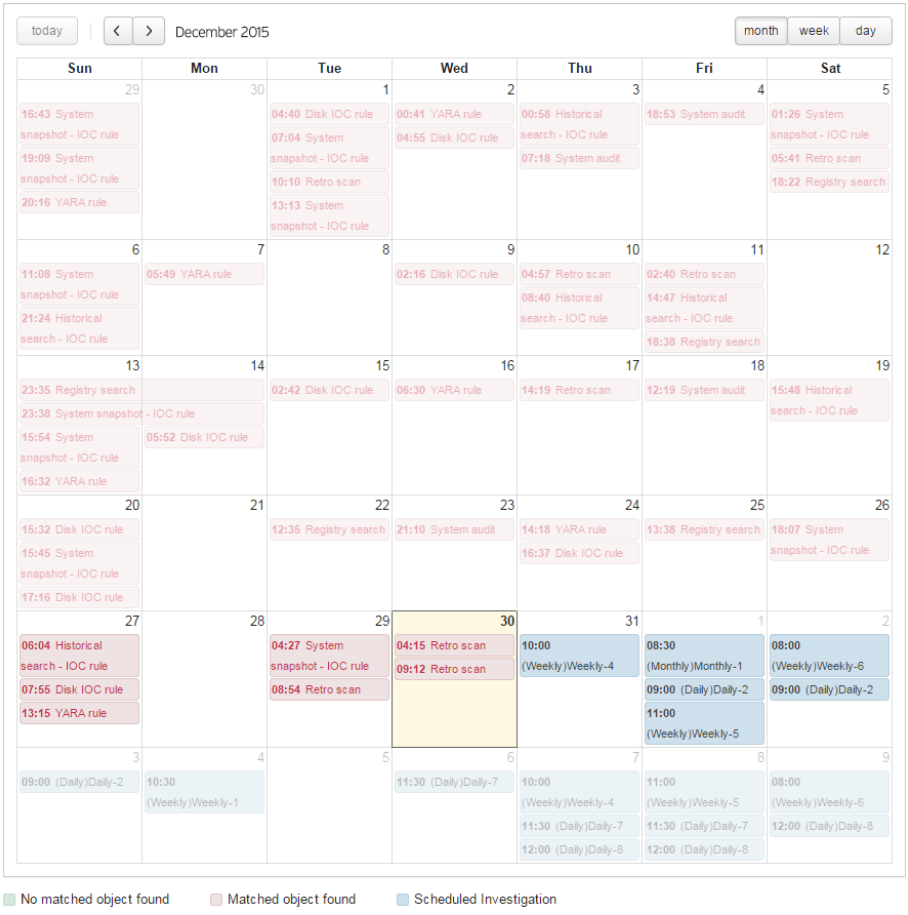
TABLE 2-2. Intelligent Monitoring Summary by Host

COLUMN NAME	DESCRIPTION
Host Name	The host name of the endpoint
Hit Counts	The number of matching rules triggered on the endpoint
Rule Category	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 *Rule Category on page 4-8*.
Detection time	The date and time when the rule was last triggered in the endpoint

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:

- 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

- Only one investigation can run at a time. If the specified schedule conflicts with an existing investigation, Trend Micro Endpoint Sensor displays the next possible date and time. To avoid conflicts, use the **Calendar** widget on the **Dashboard** to plan investigation schedules ahead of time.
- Use the **Schedule** screen to manage schedules.

  For details, see *Managing Schedules on page 3-9*.

Endpoint

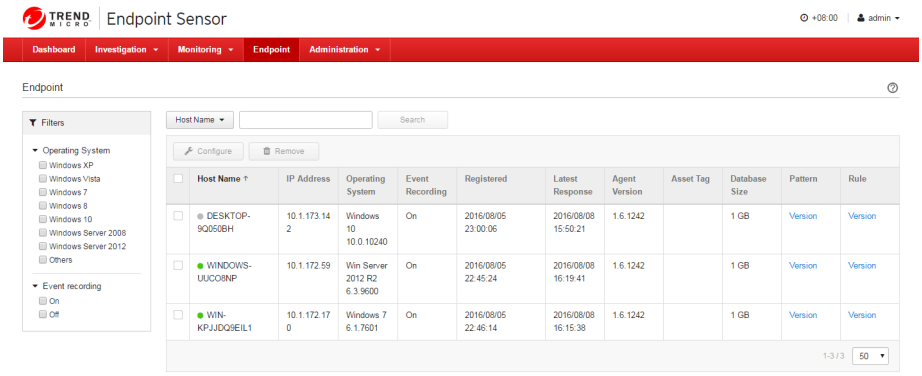
Use the **Endpoint** screen to manage all endpoints detected by the Trend Micro Endpoint Sensor server.

Note

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

  For details about agent requirements and deployment, refer to the Installation Guide available at:

  http://docs.trendmicro.com/en-us/enterprise/trend-micro-endpoint-sensor.aspx



The following table lists the endpoint details available for review:

TABLE 2-3. Endpoint Details

COLUMN NAME	DESCRIPTION
Host Name	The computer name of the Windows endpoint running the Trend Micro Endpoint Sensor agent. This column also shows the status of the endpoint: • A green status indicator indicates that the endpoint is online • A gray status indicator indicates that the server has received no response from the endpoint for more than 15 minutes
IP Address	The IPv4 address of the agent endpoint.
Operating System	The Windows variant running on the endpoint.
Event Recording	The status of the agent if it is actively recording events.
Registered	The date and time when Trend Micro Endpoint Sensor first communicated with the agent.
Latest Response	The date and time when the agent last communicated with the Trend Micro Endpoint Sensor server.
Agent Version	The version of the Trend Micro Endpoint Sensor agent installed on the endpoint.

Column Name	Description
Asset Tag	A user-defined string that identifies the endpoint. Click **Actions** to add an **Asset Tag** to an endpoint.
Database Size	The maximum size allowed for the agent database. Once the agent database reaches this size, Trend Micro Endpoint Sensor purges old records to accommodate new ones.
Pattern	The version of the pattern deployed to the endpoint.
Rule	The monitoring rules enabled for the endpoint.

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, Trend Micro 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 Trend Micro Endpoint Sensor Installation Guide.

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 Trend Micro Endpoint Sensor to perform an investigation.

Topics include:

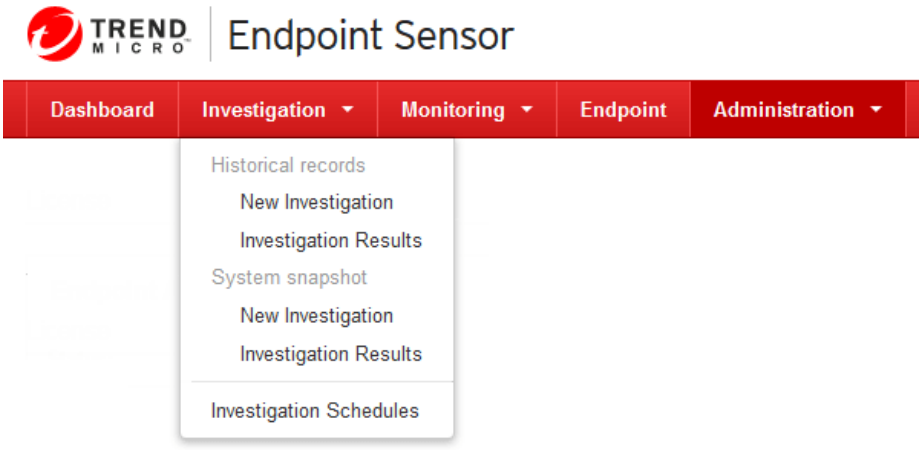
Investigation

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.

Trend Micro 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.

Procedure

1. Specify a unique **Name** for the investigation.

2. Specify a **Period**.

   Trend Micro 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**.

   Trend Micro 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 3-5*.

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 3-7*.

6. Select an investigation method and specify valid criteria.

   - For methods applicable for Historical Records, see *Investigating Historical Records on page 3-10*.

- For methods applicable for System Snapshot, see *Investigating System Snapshots on page 3-14*.

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

- The investigation is added to the **Results** screen.

  For details, see *Investigation Results on page 3-21*.

- If the investigation recurrence has been set to **Repeat**, the given schedule name appears in the **Schedule** screen.

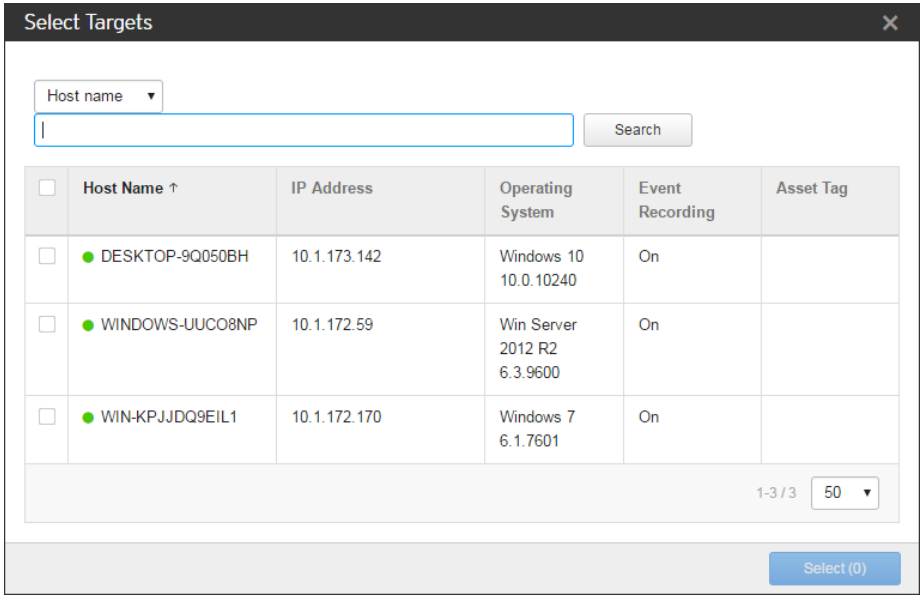
  For details, see *Managing Schedules on page 3-9*.

- 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

COLUMN NAME	DESCRIPTION
Host Name	Computer name of the endpoint running the Trend Micro Endpoint Sensor agent program
IP Address	IPv4 address of the agent endpoint
Operating System	The Windows variant running on the endpoint

Column Name	Description
Event Recording	The status of the agent, if it is actively recording events.
Asset Tag	A user-defined string that identifies the endpoint

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.

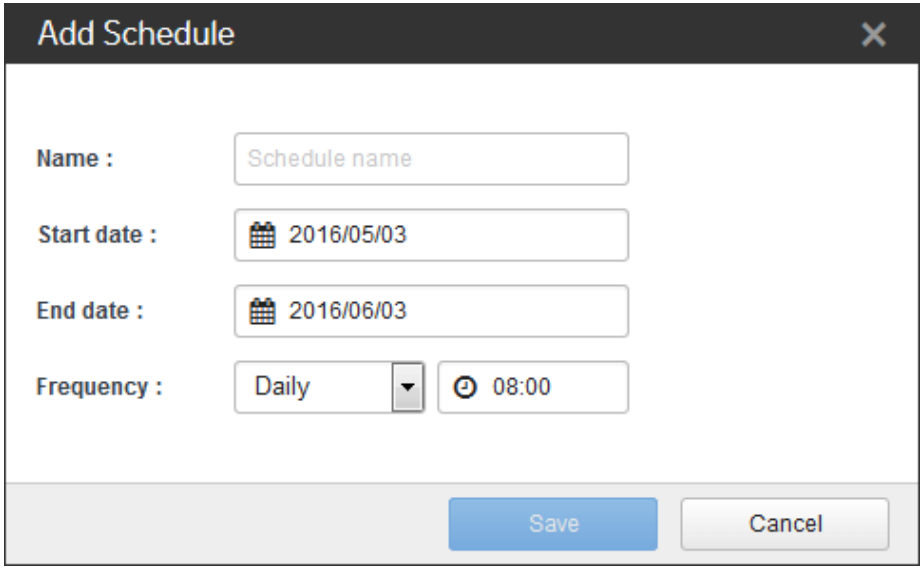
Note

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.



Specify the following required settings:

TABLE 3-2. ADD SCHEDULE SCREEN

OPTIONS	ACTION REQUIRED
Name	Assign a name for this schedule.
Start date	Specify a starting date and time for the schedule. The schedule is enabled on this date.
End date	Specify an ending date and time for the schedule. The schedule is disabled after this date.

Options	Action Required
Frequency	Specify how often the investigation repeats during the duration of the schedule. The following options are available: • **Daily**: Set the schedule to run at a specified time everyday. • **Weekly**: Specify a time and day of the week to run the schedule. • **Monthly**: Specify a time and day of the month to run the schedule.

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

For details, see *Managing Schedules on page 3-9*.

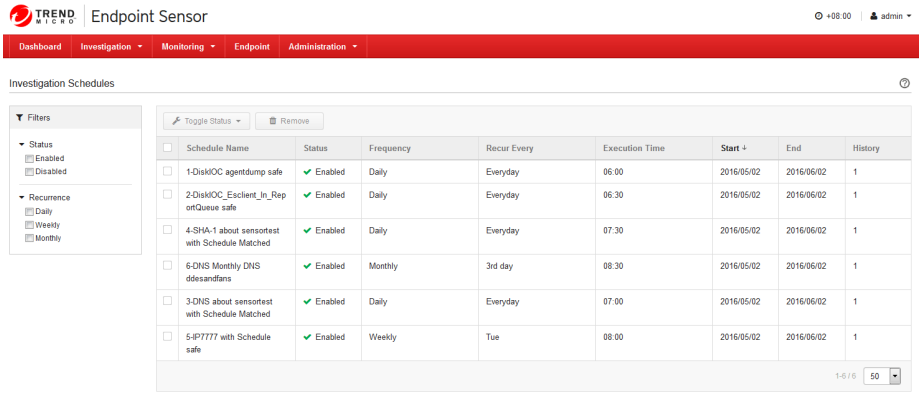
Note

Only one investigation can run at a time. If the specified schedule conflicts with an existing investigation, Trend Micro Endpoint Sensor displays the next possible date and time. To avoid conflicts, use the **Calendar** widget on the **Dashboard** to plan investigation schedules ahead of time.

For details, see *Dashboard on page 2-4*.

Managing Schedules

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



The following table lists the schedule details available for review:

TABLE 3-3. Schedule Details

COLUMN NAME	DESCRIPTION
Schedule Name	The name given to the schedule.
Status	The current status of the schedule.
Frequency	The recurrence pattern set for the schedule.
Recur Every	The frequency of the investigation.
Execution Time	The time when the next investigation occurs.
Start	The start date of a schedule. After this date, the schedule runs the investigation repeatedly until the **End** date is reached.
End	The end date of a schedule. The investigation no longer runs after this date.
History	The number of times the investigation has repeated.

Select at least one schedule to activate the following options:

- 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*.

- Only one investigation can run at a time. If the specified schedule conflicts with an existing investigation, Trend Micro Endpoint Sensor displays the next possible date and time. To avoid conflicts, use the **Calendar** widget on the **Dashboard** to plan investigation schedules ahead of time.

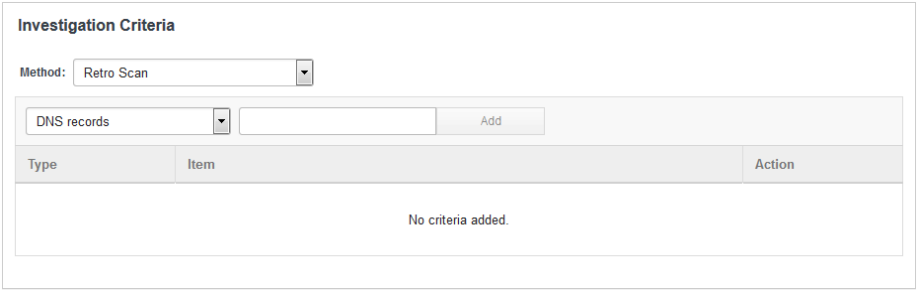
  For details, see *Dashboard on page 2-4*.

Investigating Historical Records

Trend Micro 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

TYPE	ITEM
DNS record	Type a domain name accessed by an endpoint. Examples: • `cncserver.com` • `maliciousssite.com`
IP address	Type an IP address accessed by an endpoint. Examples: • `192.168.0.1`
File name	Type the full file name or the file extension. Examples: • `wmiprvse` • `suhost`

TYPE	ITEM
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`

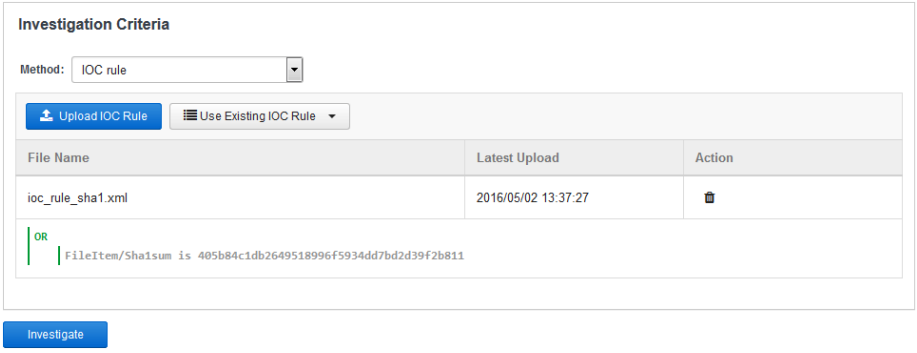
Note

- 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 uses Indicators of Compromise (IOCs) and communicates these digital artifacts in a machine readable format. Verify that the IOC file to be uploaded uses indicator terms supported by Trend Micro 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 3-35*.

Note

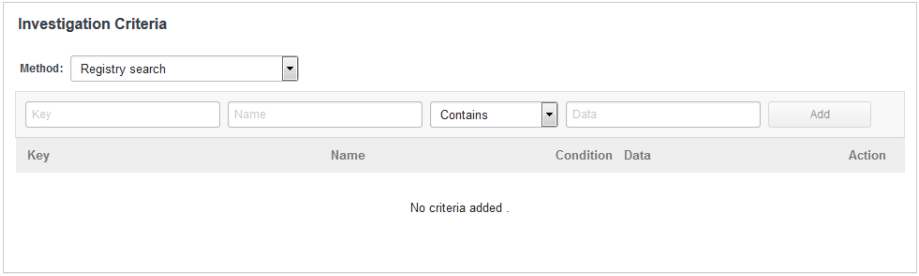
- The maximum file size for an IOC file is 1024KB.
- Trend Micro Endpoint Sensor can store a total of 10 IOC files. Once this limit is reached, older IOC files are removed when new ones are uploaded.
- Once uploaded, the IOC file is available for all future investigations. Ensure that an IOC file is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

Investigating System Snapshots

Trend Micro 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

FIELD	DESCRIPTION
Key	Searches for key instances that match the value provided

FIELD	DESCRIPTION
Name	Searches for name instances that match the value provided
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.

Trend Micro 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
```

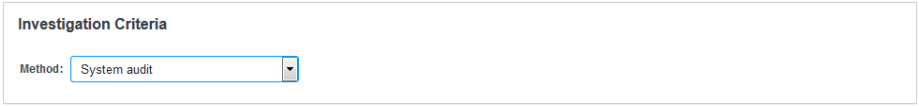
Trend Micro Endpoint Sensor searches the following matching objects:

```
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
```

```
\currentversion\themes

HKEY_USERS\(NT AUTHORITY/SYSTEM)s-1-5-18\software\microsoft
\windows\currentversion\themes
```

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

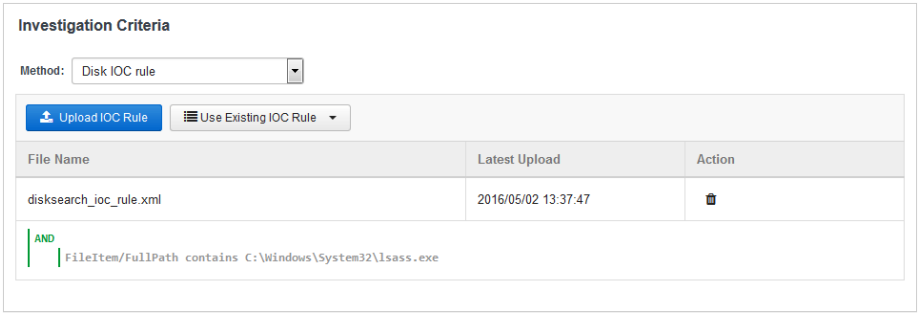
IOC rules can also be used to investigate system snapshots. To use IOC rules, follow the same guidelines mentioned in Historical Records.

For details, see *IOC Rule on page 3-13*.

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 3-35*.

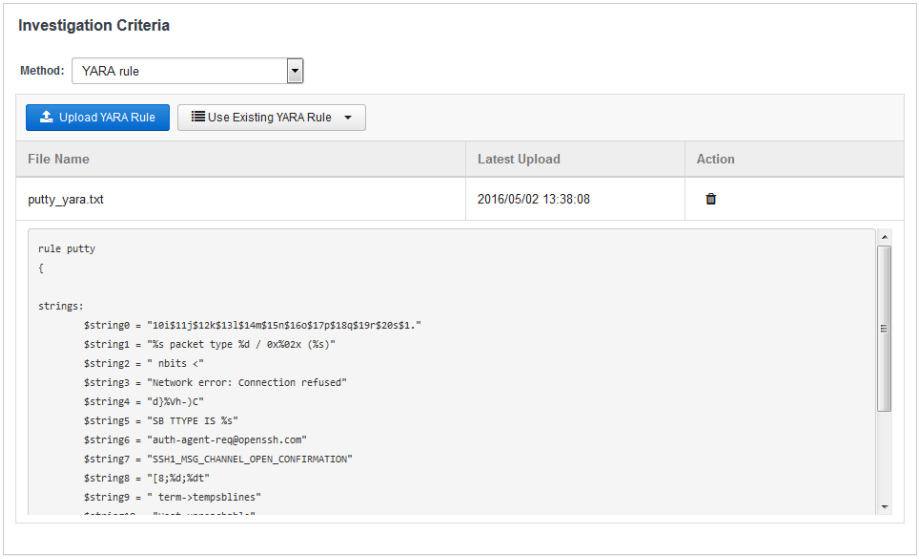
Note

- The maximum file size for a disk IOC file is 1024KB.
- Trend Micro 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.

For details about YARA rules, see http://plusvic.github.io/yara/.



A YARA file contains rules that describe malware in textual or binary patterns. Trend Micro Endpoint Sensor uses YARA rules to monitor and investigate running processes on agents. With YARA, Trend Micro 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 3-36*.

Note

- The maximum file size for a YARA file is 1024KB.
- Trend Micro 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:

```
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 3-21*.

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

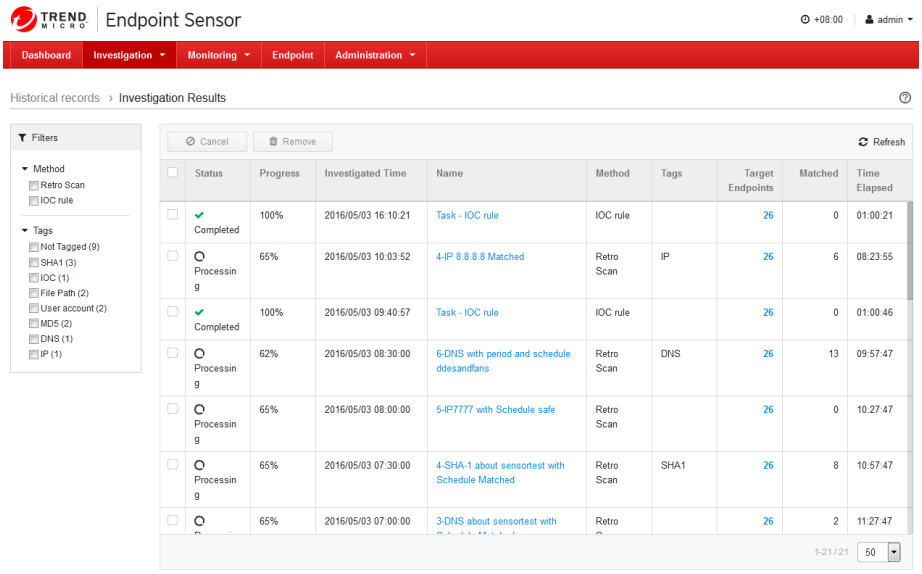
   For details, see *Information on page 3-23*.

4. Review the results using the tools available in Trend Micro Endpoint Sensor:

   - *Result Details on page 3-25*
   - *Root Cause Chain on page 3-26*
   - *Recorded Objects on page 3-32*

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

COLUMN NAME	DESCRIPTION
Status	The status of the investigation, if the investigation is **Pending**, **Processing**, **Completed** or **Cancel**.
Progress	The investigation's percentage of completion.
Investigated Time	The date and time when the investigation was started.

Column Name	Description
Name	The name given to the investigation.
Method	The method used by the investigation.
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 3-5*.
Matched	The number of matching objects found on the endpoint.
Time Elapsed	Time elapsed since the investigation started.

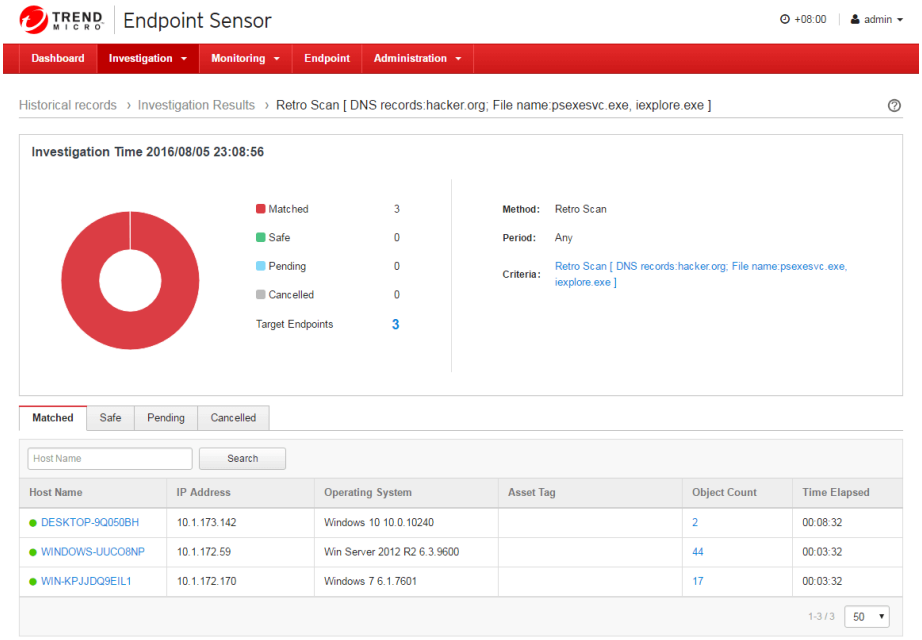
Use the following options to manage the investigations:

- Click **Stop** to stop the progress of the investigation. However, results for endpoints already investigated are still available for review. Stopped investigations cannot be resumed.
- 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 is divided into the following areas:

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

TABLE 3-7. Investigation Status

ICON	LABEL	DESCRIPTION
	Matched	Number of investigated endpoints containing a match
	Safe	Number of investigated endpoints where a match was not found
	Pending	Number of endpoints still to be investigated. An investigation is complete once there are no more pending endpoints to investigate.
	Cancelled	Number of endpoints which were not investigated. This may be caused by an user cancellation, system error, an endpoint timeout For details, see *Troubleshooting Investigation Status on page 3-33*.

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

- The **Details** area summarizes the 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*.

- **Target Endpoints**: Displays the results of 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 3-8. Target Endpoints Details

COLUMN NAME	DESCRIPTION
Host Name	The host name of the endpoint. Click the endpoint's host name to go to that endpoint's **Matched Endpoint** screen. For details, see *Result Details on page 3-25*.
IP Address	The IPv4 address of the endpoint.
Operating System	The version of Windows installed on the endpoint.

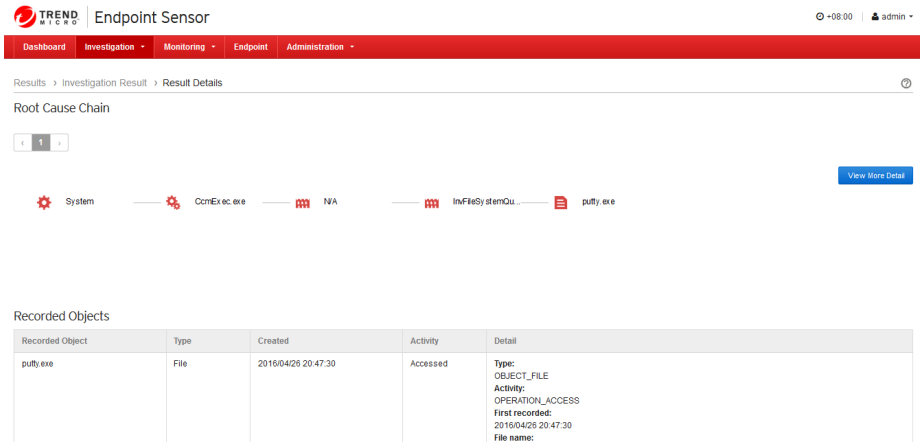
Column Name	Description
Asset Tag	The tags associated with the endpoint.
Object Count	The number of matched objects found on the endpoint.
Time Elapsed	Time elapsed since the investigation started.

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.



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 3-26*.

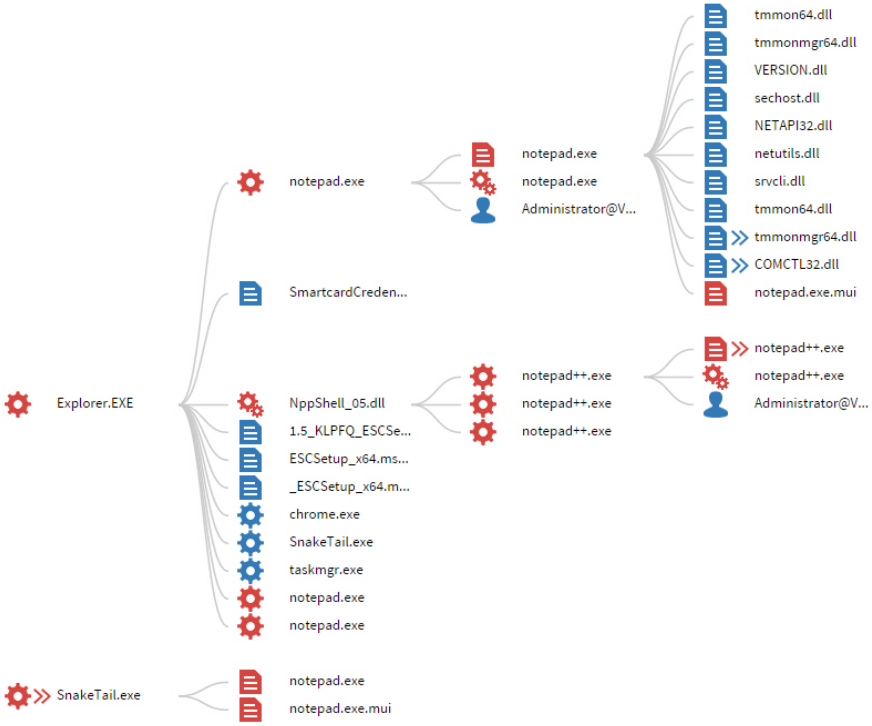
- **Recorded Objects** displays details about the matched object and all its related objects. Details shown here come from the **Objects List** screen.

  For details, see *Recorded Objects on page 3-32*.

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 3-30*.

   The following objects are shown in red:

- 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 3-32*.
   - Use the following options on the right to manage the objects shown in the root cause chain:

     TABLE 3-9. Customization Options for the Root Cause Chain

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

   - Use the following options on the right to collect objects for later investigation by adding them to the **Interested Objects** list.

TABLE 3-10. Options for Interested Objects

OPTION	DESCRIPTION
Add to interested objects list	Adds the object as a new item in the **Interested Objects** list
Remove from interested objects list	Removes the object from the **Interested Objects** list
Remove from root cause chain	Unmarks the object as suspicious and turns the icon blue
Add to root cause chain	Marks the object as suspicious and turns the icon red

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 **Investigate 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.

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 3-11. Icon Legend

ICON	TYPE	DESCRIPTION
	File	Files created by the processes related to the matched object.
	Process	Processes that start other services or create files. Processes usually have an associated user account displayed under the process name.
	IP address and port	IP addresses that the connected process, service, or file attempted to access.
	Domain	Domains that the connected process, service, or file attempted to access.
	User account	The user account with the domain that started the connected process, service, or file.

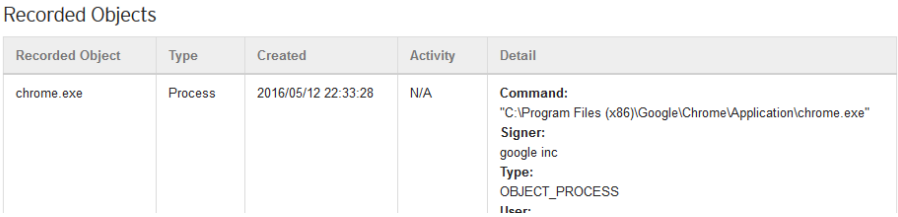
Icon	Type	Description
	Service	Services that create files, or start other processes and services. Services usually have an associated user account displayed under the service name.
	Registry	Registry operations implemented by a process, service or module, especially for autorun processes.
	Autorun Process	Registry entries that launch processes and services during system startup.
	Module	Modules loaded by a process or service to perform a routine.
	Mutex	Objects used in coordinating mutually exclusive access to a shared resource.
	Semaphore	A software flag with a value that indicates the status of a common resource.
	Inject API	APIs used by the matched object to inject itself or any of its dependencies into a process.
	WinINet API	APIs that are used for network connection and information transfer.
	Downloaded file	Files that are downloaded from a URL.
	Unknown	Unknown modules and files.
	Internet API	APIs that are used to connect to the Internet via application level. For example, HTTP/FTP.

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.



This screen displays the following details:

TABLE 3-12. Recorded Objects Details

COLUMN NAME	DESCRIPTION
Recorded Object	The name of the recorded object.
Type	The type of matched object. For details, see *Object Types on page 3-11*.
Created	The time when the object was first discovered.
Activity	The current activity of the recorded object during the investigation.
Detail	Additional information extracted from the object. Trend Micro 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.

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 3-23*.

TABLE 3-13. Investigation Status

STATUS	DESCRIPTION
Command waiting to be deployed.	Endpoint has been queued for investigation. Trend Micro Endpoint Sensor updates the status once the investigation command is sent to the agent.
Command in progress.	Endpoint is being investigated. Wait for the investigation to finish.
An endpoint error has occurred.	Endpoint is online, but the Trend Micro Endpoint Sensor agent encountered an error. If you encounter this message, perform any of the following: • Check that all required Trend Micro Endpoint Sensor services are running on the endpoint. • Restart the endpoint, and then run the investigation again.

STATUS	DESCRIPTION
Canceled due to timeout.	No response was received from the endpoint and the timeout period has been reached. After the timeout period, the Trend Micro 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 3-37*.
Canceled due to error	An unknown error has occurred and Trend Micro Endpoint Sensor has canceled the investigation for the endpoint. Once Trend Micro 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 Trend Micro 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 Trend Micro Endpoint Sensor server.

Note

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

Procedure

1. On the Trend Micro Endpoint Sensor server, 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.

   ```
   $ ...\CmdTool\IOCTool>IOCTool.exe <ioc_file>
   ```

   `<ioc_file>` corresponds to full file name of the `IOC` file in question

   The following output appears:

   ```
   C:\...\CmdTool\IOCTool>IOCTool.exe c:\temp\abc.ioc
   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/.

Troubleshooting Invalid YARA Rules

Procedure

1. On the Trend Micro 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:

http://yara.readthedocs.org/en/latest/commandline.html

The following output appears:

```
$:\...\CmdTool\YARA>yara -m c:\invalid.yara
c:\invalid.yara(6): error: untermindated 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/.

Troubleshooting Server Database Size

The Trend Micro 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:

Procedure

1. Use any application that can send a query statement to the SQL server.
2. Connect to the Trend Micro Endpoint Sensor SQL database, and send the following commands:

   • To turn the auto-purge feature on:

   ```
   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:

   ```
   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 Trend Micro Endpoint Sensor agents, use the **Endpoints** screen.

For details, *Endpoint on page 2-7*.

Modifying the Expiration value

The Trend Micro 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 Trend Micro 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:

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

   `<Expiration>86400</Expiration>` sets how long Trend Micro 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 Trend Micro Endpoint Sensor service using the command prompt:

   ```
   C:\>sc start TrendMicroEndpointSensorService
   ```

Chapter 4

Monitoring Files

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

Topics include:

Monitoring

To protect against attacks, Trend Micro 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. Trend Micro 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, Trend Micro Endpoint Sensor can either collect the file in a specific location, or send the file to Deep Discovery Analyzer for further analysis.

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

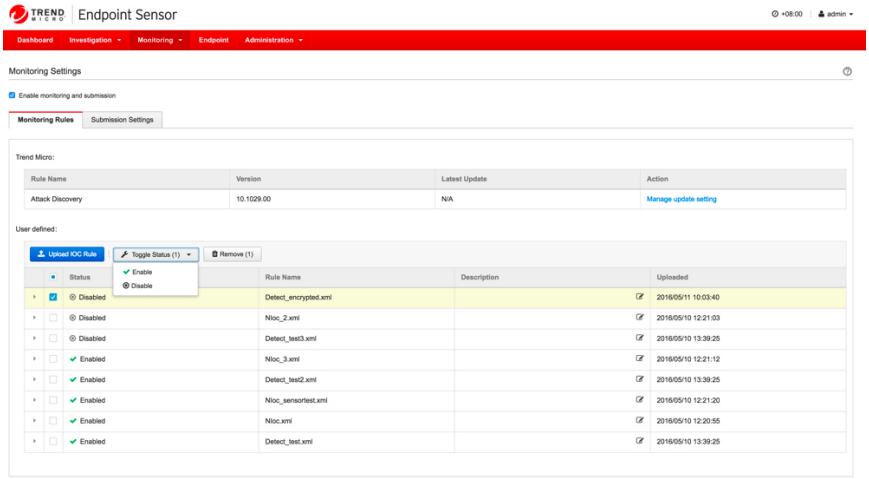
COLUMN NAME	DESCRIPTION
Rule Name	Name of the rule
Version	Version information for the rule
Latest Update	Date and time when the rule was uploaded
Action	Commands available to interact with the rule

- **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

COLUMN NAME	DESCRIPTION
Status	Specifies if the rule is disabled or enabled
Rule Name	Name of the uploaded rule
Description	A short user-defined description of the uploaded rule
Uploaded	Date and time when the rule was uploaded



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:

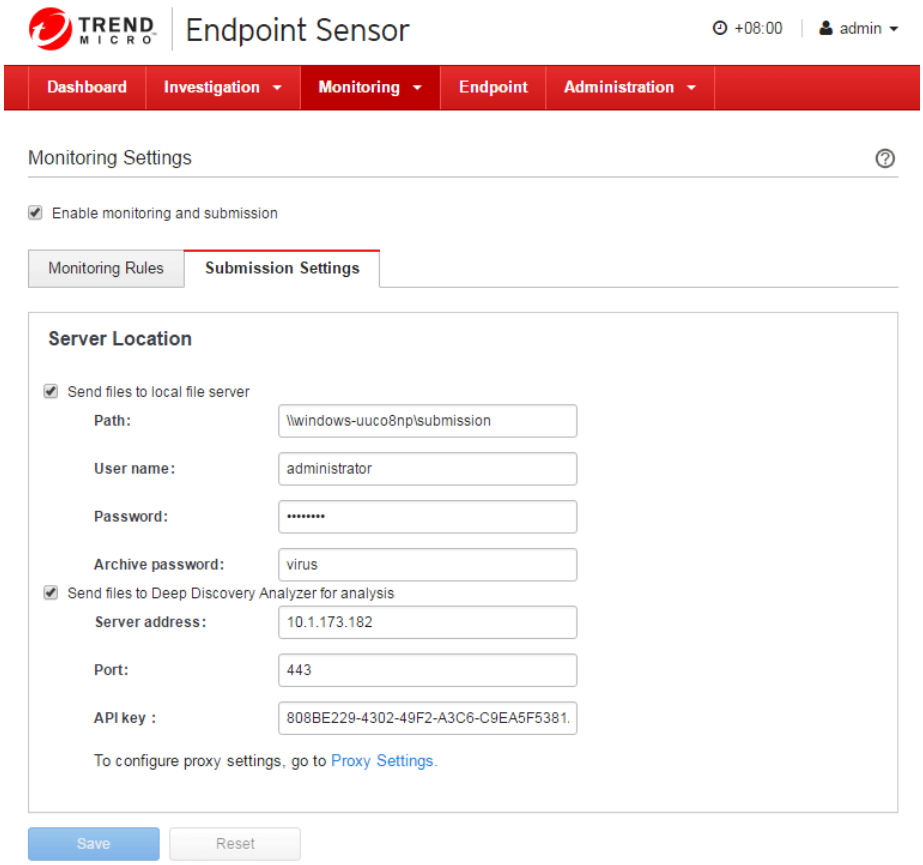


TABLE 4-3. Destination

OPTION	ACTION REQUIRED
Send files to local file server	Specify the following details: • Path • User name • Password • Archive password Trend Micro 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.
Send files to Deep Discovery Analyzer for analysis	Specify the following details: • Server Address • Port • API key For details, see *Deep Discovery Analyzer Integration on page 4-6*.
To configure proxy settings, go to Proxy Settings.	If a proxy is required for the connection, click to open the **Proxy Setting** screen. For details, see *Proxy on page 5-4*.

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

- Trend Micro 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 Trend Micro Endpoint Sensor before specifying a new API key.

For details, refer to the documentation available at:

http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx

Submitted for Analysis

Once Trend Micro 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:

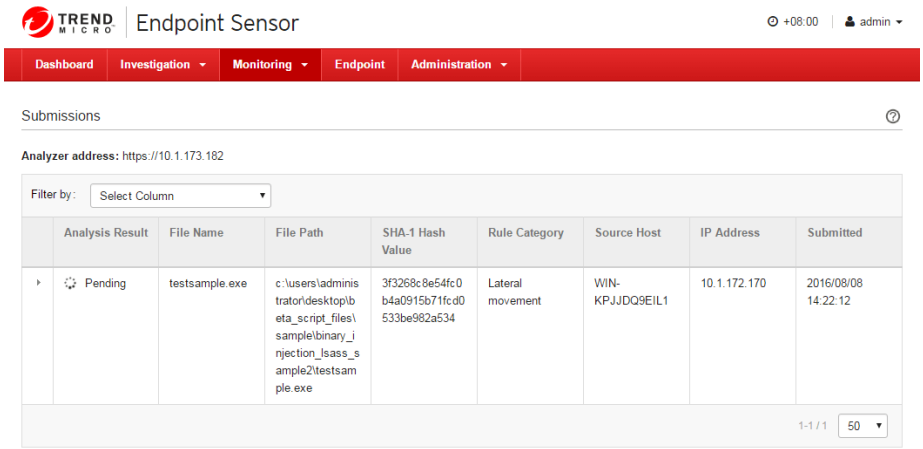


TABLE 4-4. Submitted for Analysis

COLUMN NAME	DESCRIPTION
Analysis Status	Status of the submitted file base on the analysis made by Deep Discovery Analyzer
File Name	File name of the submitted object
File Path	Local path of the submitted object in the endpoint
SHA-1 Hash Value	SHA-1 hash value of the submitted object
Rule Category	Classification based on the six stages of a targeted attack. For details, see *Rule Category on page 4-8*.
Source Host	Host name of the endpoint that submitted the object
IP	IP address of the endpoint that submitted the object
Submitted Time	Date and time when object was submitted

Click ▶ to view more details about each file.

Rule Category

Trend Micro Endpoint Sensor classifies the analyzed files based on the six stages of a targeted attack:

TABLE 4-5. Six stages of a targeted attack

STAGE	BEHAVIOR DESCRIPTION
Intelligence gathering	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

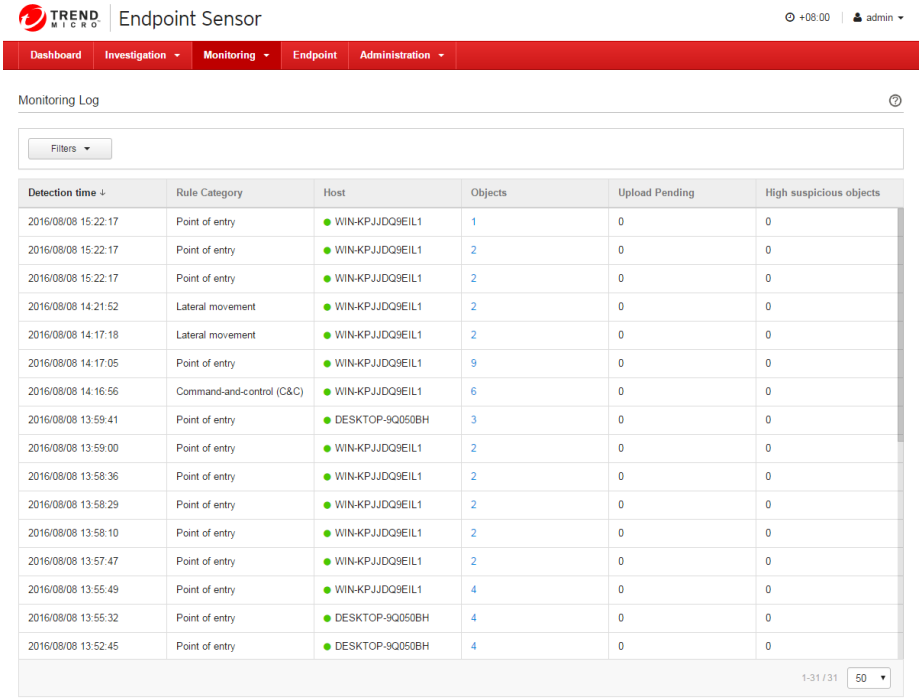
Stage	Behavior Description
Point of entry	Uses tactics and techniques used to gain entry to a network, including but not limited to: • Sending emails with a malicious file attachment, or a link to a malicious URL • Compromising a legitimate web site to download malware • Directly hacking the target system • Penetrating a partner's network and hitching a ride into yours via normal communication • Using unsecured or third-party networks (hotel, coffee shop, airport, etc.) • Delivering attack code via a USB or other removable storage media
Command-and-control (C&C)	Initiates communication with a C&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&C traffic can occur to/from a trusted IP address or a malicious host, using various communication and encryption protocols.
Lateral movement	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.
Asset/data discovery	Locates the specific servers and services that contain the most valuable data by scanning selected ports, monitoring internal traffic, etc.
Data exfiltration	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.
Attack accomplice	Runs functions that assist in the routines of other malware involved in the attack.
User defined	Files specified by the user through user-defined IOC files.

For details, refer to the documentation available at:

http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/#what-happens-during-an-attack.

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

COLUMN NAME	DESCRIPTION
Detection Time	Date and time when the object was detected.
Rule Category	Classification based on the six stages of a targeted attack. For details, see *Rule Category on page 4-8*.
Host	Endpoint where the object was found.
Objects	Number of objects found in the endpoint.
Upload Pending	Number of objects uploaded to Deep Discovery Analyzer.
High Suspicious Objects	Number of objects classified as highly suspicious by Deep Discovery Analyzer.

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

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

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** and connect to the Trend Micro Endpoint Sensor database.
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.

Stored Procedure	Description
`dbo.SP_IRB_DeleteInspectedReportByDay`	Stored procedure purges reports *n* days before today.
`dbo.SP_IRB_DeleteInspectedReportByNumber`	Stored procedure purges *n* oldest reports.

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 Trend Micro Endpoint Sensor.

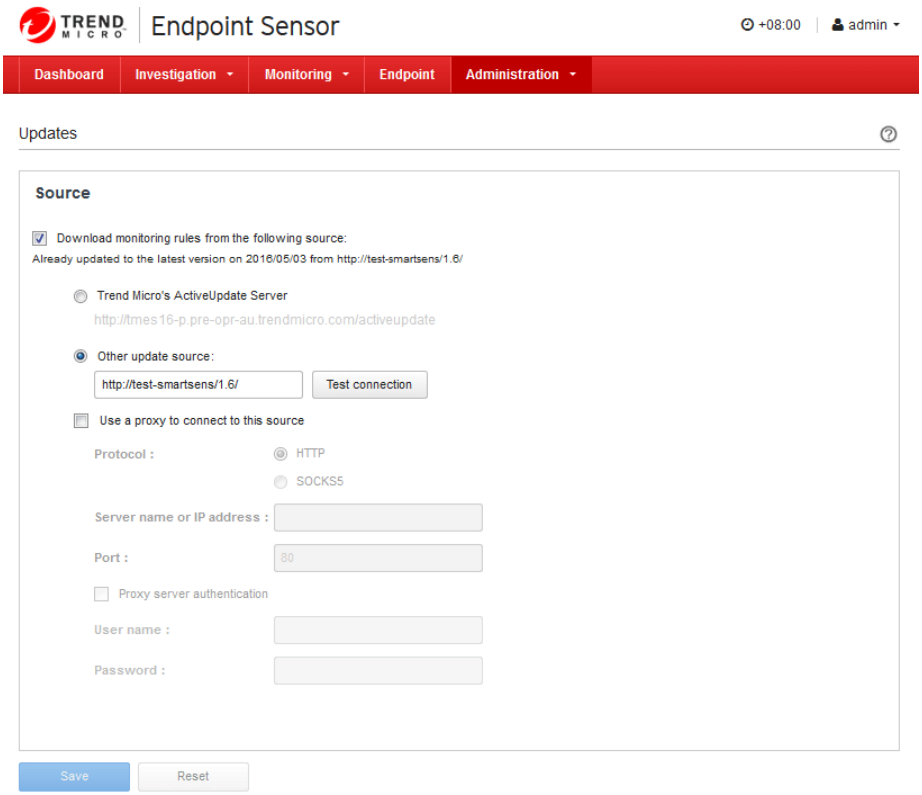
Topics include:

Administration

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

Updates

Use the **Updates** screen to manage updates for Trend Micro 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.

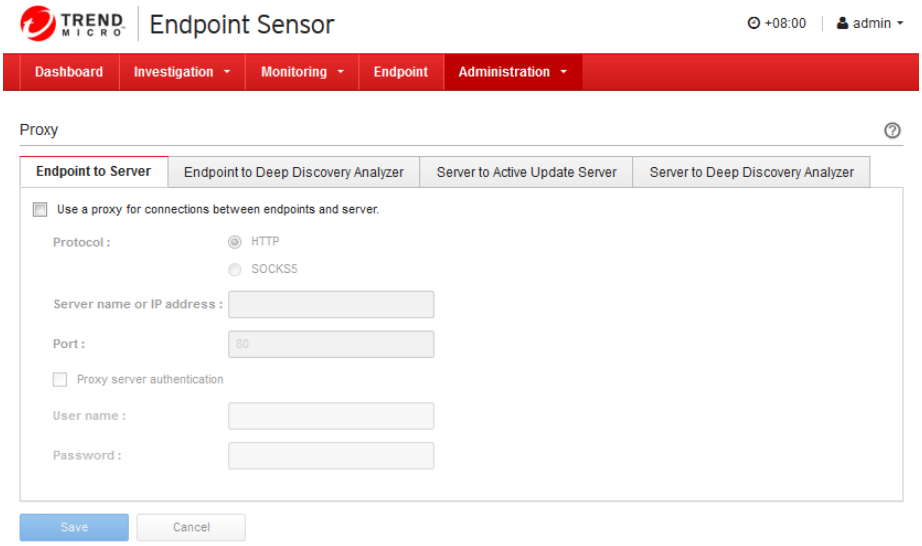
If the update source requires a proxy, specify the details below:

TABLE 5-1. Proxy Settings Requirements

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

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

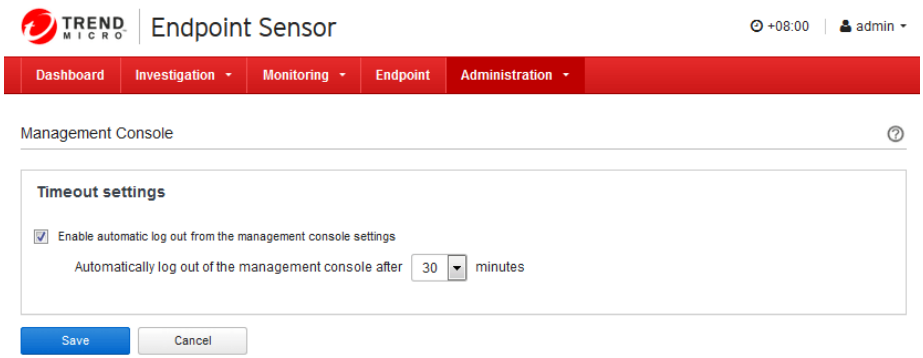
OPTIONS	ACTION REQUIRED
Protocol	Select HTTP or SOCKS5 protocols
Server name or IP address	Specify the IP address or URL of the proxy server.
Port	Specify the listening port of the proxy server.
Proxy server authentication	Select if the proxy server requires a user name and password for access.
User name	Specify the user name for authentication.
Password	Specify the password for authentication.

Note

The Trend Micro 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 Trend Micro Endpoint Sensor.



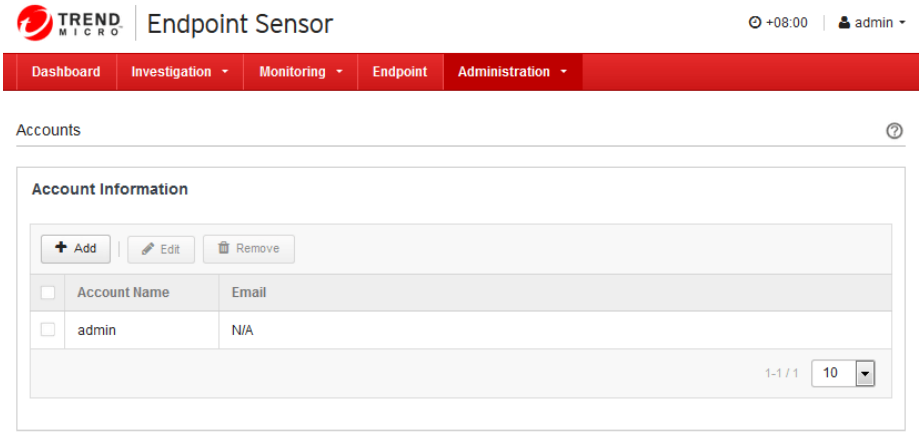
Change the following options according to your preference:

TABLE 5-3. Management Console

OPTIONS	ACTION REQUIRED
Enable automatic log out from the web console	Select to enable the timeout period. The timeout period is disabled by default.
Automatically log out of the web console after x minutes	Specify a timeout value in minutes. The console logs the user out after the specified period of inactivity.

Accounts

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



The following options are available:

TABLE 5-4. Account Information

OPTION	DESCRIPTION
Add	Specify an account name and password for the new account. Once saved, account names cannot be edited.
Edit	Edits the password for the selected account. Account names cannot be edited. Select at least one account to activate this option.
Remove	Removes the selected account from the list. Select at least one account to activate this option.

Trend Micro 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 Trend Micro Endpoint Sensor server.

This **Server Information** section displays the following details:

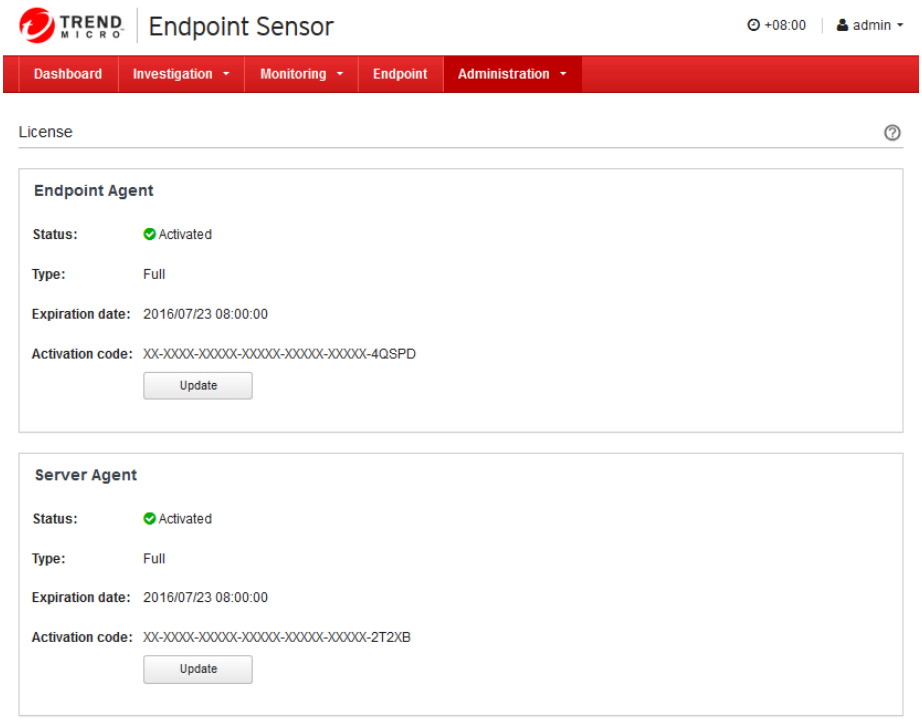
- GUID
- Version
- Attack Discovery
- Endpoint Sensor Exception Pattern
- Endpoint Sensor Trusted Pattern
- Third party licenses

Click **License Attributions** to view the licenses for third party components used by Trend Micro Endpoint Sensor.

License

Use the **License** screen to 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

DETAIL	DESCRIPTION
Activation Code	Displays the Activation Code of the product. Click **Update** to type a new Activation Code.

DETAIL	DESCRIPTION
Status	Displays the status of the Activation Code. Status may be any of the following values: • Grace period • Activated • Not activated • Near expiry date • Expired
Type	Displays the type of Activation Code. Type may be any of the following values: • Full • Invalid
Expiration date	Displays the date when the Activation Code will expire.

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

This chapter describes how to find solutions online, use the Support Portal, and contact Trend Micro.

Topics include:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

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

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined 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 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, fax, or email:

Address	Trend Micro, Inc., 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  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 hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint agent version
- 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:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

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

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

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.

TrendLabs

TrendLabs™ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Appendices

Appendix

Appendix A

OfficeScan Integration

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

Topics include:

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:

http://docs.trendmicro.com/en-us/enterprise/officescan.aspx

Use the OfficeScan Trend Micro Endpoint Sensor Deployment Tool plug-in to deploy Trend Micro 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 Trend Micro Endpoint Sensor agent software, the Trend Micro Endpoint Sensor agent synchronizes to the Trend Micro Endpoint Sensor server specified in the plug-in. OfficeScan does not manage Trend Micro Endpoint Sensor agents or perform investigations. The OfficeScan agent and the Trend Micro 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 Trend Micro Endpoint Sensor agents or hosts that only have an IPv6 address assigned.

Plug-in Manager delivers two types of solutions:

- **Native Product Features**

  Some native OfficeScan features are licensed separately and activated through Plug-in Manager. **Trend Micro Virtual Desktop Support** and **OfficeScan Data Protection** are examples of two features that fall under this category.

- **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 **Intrusion Defense Firewall**, **Trend Micro Security (for Mac)**, and **Trend Micro Mobile Security**.

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:

http://docs.trendmicro.com/en-us/enterprise/officescan.aspx

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

Agent Installation Considerations When Using OfficeScan

When using OfficeScan to install the Trend Micro 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
- 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. Trend Micro 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*
- *Plug-in Program Management on page A-7*

Trend Micro Endpoint Sensor Deployment Tool Installation

The Trend Micro Endpoint Sensor Deployment Tool is installed as a plug-in program in OfficeScan.

OfficeScan plug-in programs appear 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 single sign-on function of Trend Micro Control Manager.

Preparing the Trend Micro Endpoint Sensor Deployment Tool Installation Package

Important

Contact Support to receive the Trend Micro Endpoint Sensor deployment tool before proceeding. This plug-in program is not available on the ActiveUpdate server.

Procedure

1. Save the Trend Micro Endpoint Sensor deployment tool installation package to any folder on the same machine as the OfficeScan server.
2. Create a deployment folder and extract the contents of the installation package to this folder.

3. Share the deployment folder. Take note of the folder's Uniform Naming Convention (UNC) path.

4. Open the OfficeScan web console and go to **Updates** > **Server** > **Update Source**.

5. On the screen that appears, select **Intranet location containing a copy of the current file**, and type the UNC path of the deployment folder. Specify the user name and password for the folder, if necessary.

6. Click **Save**.

7. Modify the following registry key on the OfficeScan server:

   - For 32-bit systems:

     Path: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS`

     Key: `OSCE_Addon_Service_CompList_Version`

     Value: `1.0.0000`

   - For 64-bit systems:

     Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\OfficeScan\service\AoS`

     Key: `OSCE_Addon_Service_CompList_Version`

     Value: `1.0.0000`

8. Restart the OfficeScan Plug-in Manager service.

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

10. Verify that the Trend Micro Endpoint Sensor plug-in appears in the list of available plug-in programs.

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 plug-in program 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 installation.

After the installation, the current plug-in program version appears 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-19*.

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

ERROR CODE	DETAILS
-113	Trend Micro Endpoint Sensor is unable to obtain required Windows environment information. Trend Micro Endpoint Sensor cannot determine whether the environment uses x86 or x64 architecture. Contact your system administrator.
-114	Verification of the installation package or Trend Micro Endpoint Sensor program was unsuccessful. • If you were installing Trend Micro Endpoint Sensor, download the installation package again and retry installation. • If you were uninstalling Trend Micro 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 Trend Micro Endpoint Sensor certificate or the certificate manager tool is either missing or corrupt. Download the installation package again and retry installation.

Error Code	Details
-151	Trend Micro 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 Trend Micro 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.
-152	A Trend Micro Endpoint Sensor agent is already installed on the endpoint. If you were attempting to update the Trend Micro Endpoint Sensor agent version, uninstall the previous agent, and try again.
-153	Trend Micro 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.
-154	The Trend Micro 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.

Error Code	Details
-157	Trend Micro 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	Trend Micro 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.
-170	Trend Micro 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	Trend Micro 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.

Error Code	Details
-199	Trend Micro 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 Trend Micro 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 Trend Micro Endpoint Sensor server and download the agent installation package.

   For details, see *Downloading the Installation Package on page A-13*.

3. Install the Trend Micro 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-16*.

   For information about agent installation, see *Installing the Trend Micro Endpoint Sensor Agent on page A-14*.

Once installation is complete, each OfficeScan agent acts independently of each Trend Micro 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-15*.

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

Downloading the Installation Package

Before you can deploy the Trend Micro Endpoint Sensor agents, you must specify the location where the Trend Micro 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 Trend Micro Endpoint Sensor server.

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

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

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

TABLE A-2. Proxy Setting Requirements

FIELD	ACTION REQUIRED
Proxy settings toggle	Check the box to enable communication over a proxy.
Proxy protocol	Trend Micro Endpoint Sensor supports proxy over HTTP or SOCKS5 protocols.
Server name or IP address	Specify the IP address or URL of the proxy server.
Port	Specify the port of the proxy server.
User ID	If the proxy server requires authentication, specify the user name for authentication.
Password	If the proxy server requires authentication, specify the password for authentication.

4. Click **Set and Download**.

   Trend Micro Endpoint Sensor tests the connection to the server, sets the server for Trend Micro 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 Trend Micro 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 Trend Micro 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**.

   Trend Micro Endpoint Sensor begins deploying the agent to the selected endpoints.

   If Trend Micro Endpoint Sensor agent installation was skipped on any endpoints, Trend Micro 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 Trend Micro Endpoint Sensor agents.

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

Note

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

Managing the Agent Tree

This section outlines how to install, manage, and uninstall Trend Micro Endpoint Sensor agents.

Topics include:

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 appears 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 providing more search criteria.

  For details, see *Performing an Advanced Search on page A-17*.
- **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-18*.

- **Deploy Agent**: Install and deploy Trend Micro Endpoint Sensor agents to selected endpoints or upgrade existing Trend Micro Endpoint Sensor agents to the latest version.

  For details, see *Installing the Trend Micro Endpoint Sensor Agent on page A-14*.

- **Uninstall**: Uninstall Trend Micro Endpoint Sensor agents from the selected endpoints.

  For details, see *Uninstalling the Trend Micro Endpoint Sensor Agent on page A-19*.

Administrators can also manually search the agent tree to locate endpoints or domains.

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

CRITERIA	DESCRIPTION
IPv4 range	Searching by IPv4 address range requires a portion of an IP address starting with the first octet. The search returns all endpoints with IP addresses containing that entry. For example, type 10.5 to return all endpoints in the IP address range `10.5.0.0` to `10.5.255.255`.
Host name	Search by host name.

CRITERIA	DESCRIPTION
Platform	**Note** Trend Micro Endpoint Sensor supports both 32-bit and 64-bit platforms. For example, type `Windows Server` to return a list of all Windows Server platform endpoints available. Search by operating system.
Connection status	Search by agent connection status.
Installation status	Search by agent installation status.
Domain name	Search by agent domain name.
Build version	Search by agent version.

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.
6. Monitor the uninstallation of the Trend Micro Endpoint Sensor agent in the **Installation Status** column of the **Agent Management** screen.

Tip

Allow some time for the uninstallation process to complete. Click the **Refresh** button periodically to view the updated status.

Appendix B

Trend Micro Control Manager Integration

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

Topics include:

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

Trend Micro Endpoint Sensor supports the following Control Manager versions.

TABLE B-1. Supported Control Manager versions

TREND MICRO ENDPOINT SENSOR VERSION	CONTROL MANAGER VERSION
1.0	6.0 SP1, 6.0 SP2
1.5	6.0 SP3
1.6	6.0 SP3 Patch 1

Important

Additional hot fixes need to be installed to enable integration between Control Manager 6.0 SP3 Patch 1 and Trend Micro Endpoint Sensor 1.6. 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 Trend Micro Endpoint Sensor. To obtain the latest patches and hot fixes, visit the Trend Micro Update Center at:

http://www.trendmicro.com/download

After installing Trend Micro Endpoint Sensor, register it to Control Manager and then configure settings for Trend Micro Endpoint Sensor on the Control Manager management console. See the Control Manager documentation for information on managing Trend Micro Endpoint Sensor servers.

Note

Control Manager requires Internet Explorer 8 and above. However, to use Control Manager for configuring settings, managing policies, and viewing investigation results of the registered Trend Micro Endpoint Sensor servers, Internet Explorer 10 and above is recommended.

Control Manager Integration in this Release

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

- Use uploaded IOC files in Control Manager to initiate investigations directly to Trend Micro Endpoint Sensor from the Control Manager console.
- Register multiple Trend Micro Endpoint Sensor servers. Control Manager can start simultaneous investigations on multiple Trend Micro Endpoint Sensor servers.
- Pull data from Trend Micro Endpoint Sensor investigation results. The data is then displayed in a Control Manager widget.
- Create and deploy policies to Trend Micro 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 Trend Micro 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. Go to **Administration** > **Managed Servers**.
3. Click **Server Type**, and select **Trend Micro Endpoint Sensor**.
4. Click **Add**. 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. Go to **Dashboard**, and click **Server Visibility**. On the screen that appears, click **Add**.
2. Specify the details of the Trend Micro Endpoint Sensor server to be added, and click **Save**.

3. Click **Close** to return to the **Dashboard** screen.

4. Click **Add widgets**. On the screen that appears, select the Trend Micro Endpoint Sensor category on the left menu.

   The following widgets are available:

TABLE B-2. Endpoint Sensor Widgets

WIDGET NAME	DESCRIPTION
Intelligent Monitoring Summary by Host	Displays the endpoints which triggered a monitoring rule. Manually refresh the widget to view the most recent data. To configure the widget settings, click ▼.
Endpoint Sensor Investigation	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-7*.

5. Select one or both widgets, and click **Add widget**.

6. 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.

Note

After using **Server Visibility** to register a new Trend Micro Endpoint Sensor server, refresh the **Endpoint Sensor Investigation** and **Intelligent Monitoring Summary by Host** widgets to update the contents of the widgets with data from the new server.

Using Control Manager to Check Status

To check the status of registered Trend Micro Endpoint Sensor servers and agents, perform the following steps:

Procedure

1. Open the Control Manager management console.
2. On the **Dashboard** screen, use the following widgets to check the Trend Micro Endpoint Sensor status:
   - **Product Connection Status** widget displays the server status. By default, this widget appears on the **Summary** and **Compliance** tabs.
   - **Agent Connection Status** widget displays the agent status. By default, this widget appears on the **Compliance** tab.

   These widgets display the status of servers added via **Administration** > **Managed Servers**.
3. To add these widgets to a custom tab, perform the following steps:
   a. Go to an existing tab, or create a new tab. Click **Add Widgets**.
   b. On the **Add widgets** screen, select the **Compliance** category.
   c. Select **Agent Connection Status** or **Product Connection Status**, and click **Add**.
   d. The widgets should now appear on the current tab.

   For details, see the Control Manager documentation.
4. To check the status of servers used by the Trend Micro Endpoint Sensor widgets, use the **Server Visibility** screen.
   a. Go to **Dashboard**, and click **Server Visibility**.
   b. A screen listing all servers registered via **Server Visibility** appears. A check mark on the server icon indicates that the server is online.

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 Trend Micro Endpoint Sensor, perform the following steps:

Procedure

1. Set up automatic updates in Control Manager.
   a. Open the Control Manager management console.
   b. Click **Updates** > **Scheduled Download**
   c. Locate the following patterns:
      - Endpoint Sensor Exception Pattern
      - Endpoint Sensor Trusted Pattern
      - Attack Discovery Pattern
   d. For each pattern, click the pattern name, and select **Enable scheduled downloads**. Leave everything else at the default values.

      
      Note
      For Trend Micro Endpoint Sensor integration, only the **Deploy to All Managed Products Now** deployment plan is supported.

   e. Click **Save**.
2. Configure Trend Micro Endpoint Sensor to use Control Manager as its update source.
   a. Open the Trend Micro 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 Manger server Name>/TVCSDownload/
Activeupdate
```

e. Click **Save**.

Afterwards, Control Manager will include the Trend Micro Endpoint Sensor patterns during the next 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 Trend Micro Endpoint Sensor policies can be created, but each server can issue only one policy at a time.

For details, see the Control Manager documentation.

Preparing the Server for Policy Deployment

By default, recently added Trend Micro 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, click 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 in the **Product Directory** tree
   - 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**.
3. On the **Product** drop down, select **Trend Micro Endpoint Sensor**.
4. Click **Create**.
5. Click **Specify Target(s)** and select which Trend Micro 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 start the policy deployment.

   Control Manager enforces the policy settings on the target Trend Micro Endpoint Sensor servers every 24 hours.

   For details, see the Control Manager documentation.

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 Trend Micro Endpoint Sensor servers where the rules are part of a Trend Micro Endpoint Sensor policy.

If a new Trend Micro Endpoint Sensor server is registered via **Administration** > **Managed Servers**, Control Manager automatically includes the new Trend Micro 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, go to **Administration** > **Managed Servers**. Click **Upload IOC Rule** > **Choose File**, and navigate to the location of the monitoring rule. Click **Open** to automatically upload the monitoring rule. After upload is complete, click **Save** or **Deploy**.

  Note

  - It is recommended to specify the target Trend Micro Endpoint Sensor servers before uploading the rule.
  - The **Upload IOC Rule** feature is enabled only when there is at least one Trend Micro 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 Trend Micro Endpoint Sensor server registered with Control Manager results in a duplicate file issue. It is recommended to upload monitoring rules solely through Control Manager if using a Trend Micro Endpoint Sensor server registered with Control Manager. Additionally, 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 Trend Micro Endpoint Sensor server. Use the Trend Micro Endpoint Sensor management console to remove the file first, and try again." It is recommended to remove the duplicate rule from both the Trend Micro Endpoint Sensor server and the Control Manager server before trying 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 Trend Micro 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 Trend Micro Endpoint Sensor endpoints and Deep Discovery Analyzer. To configure a proxy connection between Trend Micro Endpoint Sensor endpoints and Deep Discovery Analyzer, use the **Proxy** screen of the Trend Micro Endpoint Sensor server.

For details, see *Proxy on page 5-4*.

Appendix C

Supported IOC Indicator Terms

IOC files consist of one or more indicator terms. These indicator terms specify the variables to use in the investigation. Trend Micro 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

Trend Micro 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-14*.

- 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-16*.

- 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 Trend Micro Endpoint Sensor 1.6

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
• `DnsEntryItem` Use `DnsEntryItem` indicators in **Historical Record**s IOCs to search for network-related queries in database logs. Use `DnsEntryItem` indicators in **Monitoring** IOCs to 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	✓			✓

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
• `FileItem` 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. Trend Micro 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	✓		✓	✓

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
`fileitem/filepath` Target landing folder without a file name For Disk Scanning IOCs, add an asterisk (*) after the path to recursively search subfolders. Example: `C:\Windows\System32\*` Disk Scanning IOCs require at least one `filepath` or `fullpath` indicator.	✓	✓	✓	✓
`fileitem/fullpath` Full target landing folder including the file name Example: `C:\Windows\System32\WinSync.dll` Disk Scanning IOCs require at least one `filepath` or `fullpath` indicator.	✓	✓	✓	✓
`fileitem/md5sum` Suspicious file MD5 hash value, in hexadecimal format	✓	✓	✓	✓
`fileitem/modified` Timestamp when a file was last modified Example: `2000-04-12T09:14:38Z`	✓	✓	✓	
`fileitem/peinfo/digitalsignature/certificateissuer` Keywords in the file digital certificate issuer section		✓		

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
`fileitem/peinfo/digitalsignature/certificatesubject` Keywords in the file digital certificate subject section		✓		✓
`fileitem/sha1sum` Suspicious file SHA-1 hash value, in hexadecimal format	✓		✓	✓
`fileitem/sizeInbytes` Size of file or range of file sizes in bytes Example: `101000 TO 120000`		✓	✓	
`fileitem/username` Name of the account that created the file	✓			
`fileitem/devicepath` Device path of the file				✓
`fileitem/drive` Drive of the file				✓
• `Network` Use `Network` indicators in **Historical Records** IOCs to search for DNS records in database logs.				
`network/dns` DNS record obtained from a network appliance	✓			

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
• `PortItem` Use `PortItem` indicators in **Historical Records** IOCs for network-related queries and to search for running processes in database logs. Use `PortItem` indicators in **Monitoring** IOCs to to monitor network-related behavior on the system.				
`portitem/creationtime` Timestamp when the connection was established Example: `2000-04-12T09:14:38Z`	✓			
`portitem/localip` Binding local IP address	✓			
`portitem/localport` Binding local port	✓			
`portitem/process` Process name binding on a specific port	✓			
`portitem/remoteip` Connected remote IP address	✓			✓
`portitem/remoteport` Connected remote port	✓			

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
• `ProcessItem` Use `ProcessItem` indicators in **Historical Record**s 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 to monitor the process activity on the system.				
`processitem/handlelist/handle/name` Handle name or path to handle		✓		
`processitem/handlelist/handle/type` Windows handle type		✓		
`processitem/name` Connection created by a specific process name	✓			✓
`processitem/path` File path to the executable file of the process		✓		✓
`processitem/pid` Windows process ID number		✓		
`processitem/portlist/portitem/creationtime` Timestamp when a process was created Example: `2000-04-12T09:14:38Z`	✓			
`processitem/portlist/portitem/localip` Connected local IP address	✓			

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
`processitem/portlist/portitem/remoteip` Connected remote IP address	✓			✓
`processitem/sectionlist/memorysection/digitalsignature/certificateissuer` Keywords in the process certificate issuer section	✓	✓		
`processitem/sectionlist/memorysection/digitalsignature/certificatesubject` Keywords in the process certificate subject section		✓		
`processitem/sectionlist/memorysection/sha1sum` SHA-1 hash value associated with the process or file, in hexadecimal format	✓			
`processitem/sectionlist/memorysection/md5sum` Suspicious process MD5 hash value, in hexadecimal format		✓		
`processitem/username` Account of the process owner	✓			

- `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.

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING

`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		✓		
`registryitem/valuename` Name of the registry entry		✓		
• `ServiceItem` Use `ServiceItem` indicators in **System Process** IOCs to search for active Windows services in a system snapshot. Do not use `FileItem` indicators for running processes and Windows services.				
`serviceitem/description` Keywords within the service description		✓		
`serviceitem/descriptivename` Full descriptive Windows service name		✓		
`serviceitem/name` Short name of the Windows service as stored in the registry		✓		
`serviceitem/servicedllcertificateissuer` Keywords in the service DLL certificate issuer section		✓		

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
`serviceitem/servicedllcertificatesubject` Keywords in the service DLL certificate subject section		✓		
`serviceitem/servicedllmd5sum` Suspicious service MD5 hash value, in hexadecimal format		✓		
`serviceitem/startedas` User account that started the service		✓		
`serviceitem/status` Service status: • `active` • `inactive`		✓		
`serviceitem/type` Windows service type		✓		
• `UserItem` Use `UserItem` indicators in **Historical Records** IOCs to search for user accounts in database logs.				
`useritem/disabled` Disabled user	✓			
`useritem/fullname` Domain and user account name Example: `user@domain.com`	✓			
`useritem/grouplist/groupname` Group name	✓			

INDICATOR	HISTORICAL RECORDS	SYSTEM PROCESS	DISK SCANNING	MONITORING
`useritem/lastlogin` Most recent/last known access Example: `2000-04-12T09:14:38Z`	✓			
`useritem/username` User account name	✓			

Note

- Ensure that IOC files follow the correct syntax. Follow the IOC schemas and related instructions available in 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 3-35*.

IOC Samples for Historical Records IOCs

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

```
<?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 /><ioc>
  <definition>
    <Indicator operator="AND">
      <Indicator operator="OR">
        <IndicatorItem condition="contains">
          <Context document="FileItem"
                   search="FileItem/FileExtension"/>
          <Content type="string">.exe</Content>
        </IndicatorItem>
        <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>
        <Indicator operator="OR">
          <IndicatorItem condition="contains">
            <Context document="FileItem"
                     search="FileItem/FullPath"/>
            <Content type="string">Recycler</Content>
          </IndicatorItem>
          <IndicatorItem condition="contains">
            <Context document="FileItem"
                     search="FileItem/FullPath"/>
```

```
            <Content type="string">Recycle.bin</Content>
          </IndicatorItem>
        </Indicator>
      </Indicator>
    </Indicator>
  </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>
```

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 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="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 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="ServiceItem"
            search="ServiceItem/description" type="mir" />
            <Content type="string">
            support for synchronizing objects
            </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 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>
```

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 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>
   <links />
   <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>
```

IOC Sample for Monitoring IOCs

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

```
<?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>
        <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>
    </Indicator>
  </definition>
</ioc>
```

Requirements for Monitoring IOCs

Ensure that monitoring IOCs strictly meet the following requirements:

- Contain the following header info:

```
<ioc>
  <rule_name></rule_name>
  <rule_type></rule_type>
  <rule_description></rule_description>
  <last_modified_time></last_modified_time>
  <rule_category></rule_category>
  <author_name></author_name>
  <source></source>
  <internalnote></internalnote>
  <definition></definition>
</ioc>
```

- Include `type="knownthreat"` as an attribute of the first Indicator term.

```
  <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. Trend Micro 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, Trend Micro 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

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM17438/160706