TREND MICRO™

7.0 TREND MICRO™ Control Manager

Connected Threat Defense Primer

Centralized Security Management for the Enterprise

Document Part No.: CMEM78079/171019

Release Date: November 2017

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Connected Threat Defense

Chapter 2: Suspicious Object List Exporter and Importer User Guide

Chapter 3: Suspicious Object Hub and Node Control Manager Architecture

Index

Preface

Preface

Welcome to the Trend Micro™ Control Manager™ *Connected Threat Defense Primer*. This document explains how to use Control Manager and integrated Trend Micro products to detect, analyze, and respond to targeted attacks and advanced threats.

Topics in this section:

Documentation

Control Manager documentation includes the following:

DOCUMENT	DESCRIPTION
Readme file	Contains a list of known issues and may also contain late-breaking product information not found in the Online Help or printed documentation
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the Control Manager **Note** The Installation and Upgrade Guide may not be available for minor release versions, service packs, or patches.
System Requirements	A PDF document that discusses requirements and procedures for installing Control Manager
Administrator's Guide	A PDF document that provides detailed instructions of how to configure and manage Control Manager and managed products, and explanations on Control Manager concepts and features
Online Help	HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is also accessible from the Control Manager console
Connected Threat Defense Primer	A PDF document that explains how use Control Manager to bring together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage
Widget and Policy Management Guide	A PDF document that explains how to configure dashboard widgets and policy management settings in Control Manager
Data Protection Lists (Chapter 1 only)	A PDF document that lists predefined data identifiers and templates for Data Loss Prevention

DOCUMENT	DESCRIPTION
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

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

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

Audience

Control Manager documentation is intended for the following users:

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

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents

CONVENTION	DESCRIPTION
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the Control Manager documentation:

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

TERMINOLOGY	DESCRIPTION
Control Manager console, web console, or management console	The web-based user interface for accessing, configuring, and managing a Control Manager **Note** Consoles for integrated managed products are indicated by the managed product name. For example, the OfficeScan web console.
Managed endpoint	The endpoint where the managed product agent is installed
Managed product	A Trend Micro product that integrates with Control Manager
Managed server	The endpoint where the managed product is installed
Server	The endpoint where the Control Manager server is installed
Security risk	The collective term for virus/malware, spyware/grayware, and web threats
Product service	Control Manager services hosted through Microsoft Management Console (MMC).
Dual-stack	Entities that have both IPv4 and IPv6 addresses.
Pure IPv4	An entity that only has an IPv4 address
Pure IPv6	An entity that only has an IPv6 address

Chapter 1

Connected Threat Defense

This section discusses how to detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage.

Topics include:

About Connected Threat Defense

Control Manager brings together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage.

For more information, see *Connected Threat Defense Product Integration*.

Feature Requirements

The following table lists the features available with the Connected Threat Defense architecture and the required and optional products that integrate with each.

FEATURE	REQUIRED PRODUCTS	OPTIONAL PRODUCTS
Security threat monitoring	• Control Manager 7.0 (or later) • Deep Discovery Inspector 3.8 (or later) or Deep Discovery Analyzer 5.1 (or later) **Note** At least one optional product is required to evaluate log data.	• OfficeScan 11.0 SP1 (or later) • Deep Security 10.0 (or later) • Endpoint Sensor 1.5 (or later) • InterScan Messaging Security Virtual Appliance 9.1 (or later) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (or later) • ScanMail for Microsoft Exchange 12.5 (or later) • Trend Micro Endpoint Application Control 2.0 SP1 (or later) • Cloud App Security 5.0 (or later)

FEATURE	REQUIRED PRODUCTS	OPTIONAL PRODUCTS
Suspicious Object list synchronization For more information, see *Suspicious Object Lists on page 1-5* and *Connected Threat Defense Product Integration on page 1-26*.	• Control Manager 7.0 (or later) • Deep Discovery Inspector 3.8 (or later) or Deep Discovery Analyzer 5.1 (or later) **Note** At least one optional product is required for synchronization.	• Smart Protection Server 3.0 Patch 1 (or later) • OfficeScan 11.0 SP1 (or later) • Deep Security 10.0 (or later) • InterScan Messaging Security Virtual Appliance 9.1 (or later) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (or later) • Trend Micro Endpoint Application Control 2.0 SP1 (or later) • Cloud App Security 5.0 (or later)
Suspicious Object sample submission	• Deep Discovery Inspector 3.8 (or later) or Deep Discovery Analyzer 5.1 (or later)	• Deep Security 10.0 (or later) • OfficeScan 11.0 SP1 (or later) • Endpoint Sensor 1.5 (or later) • InterScan Messaging Security Virtual Appliance 9.1 (or later) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (or later) • ScanMail for Microsoft Exchange 12.5 (or later) • Deep Discovery Email Inspector 3.0 (or later)

FEATURE	REQUIRED PRODUCTS	OPTIONAL PRODUCTS
Suspicious Object management	• Control Manager 7.0 (or later) • Deep Discovery Inspector 3.8 (or later) or Deep Discovery Analyzer 5.1 (or later)	• OfficeScan 11.0 SP1 (or later) • Deep Security 10.0 (or later) • Endpoint Sensor 1.5 (or later) • InterScan Messaging Security Virtual Appliance 9.1 (or later) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (or later) • Trend Micro Endpoint Application Control 2.0 SP1 (or later) • Cloud App Security 5.0 (or later)
Suspicious Object scan actions For more information, see *Suspicious Object Scan Actions on page 1-8*.	• Control Manager 7.0 (or later)	• Smart Protection Server 3.0 Patch 1 (or later) • OfficeScan 11.0 SP1 (or later) • Deep Security 10.0 (or later) • InterScan Messaging Security Virtual Appliance 9.1 (or later) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (or later) • Trend Micro Endpoint Application Control 2.0 SP1 (or later) • Cloud App Security 5.0 (or later)

FEATURE	REQUIRED PRODUCTS	OPTIONAL PRODUCTS
Impact assessment	• Control Manager 7.0 (or later) • Endpoint Sensor 1.5 (or later)	• None
Endpoint isolation For more information, see *Isolating Endpoints on page 1-23*.	• Control Manager 7.0 (or later) • OfficeScan 11.0 SP1 (or later)	• Endpoint Sensor 1.5 (or later)
IOC management	• Control Manager 7.0 (or later) • Endpoint Sensor 1.5 (or later)	• None

Suspicious Object List Management

Control Manager allows you to synchronize Suspicious Object lists among managed products and create User-Defined and Exception lists to further control the spread of suspicious objects. You can also configure specific actions that supported managed products take upon detecting suspicious objects in your environment.

Control Manager consolidates Virtual Analyzer and user-defined suspicious object lists (excluding exceptions) and synchronizes the lists with integrated managed products.

For more information about products that can synchronize Suspicious Objects lists with Control Manager, see *Suspicious Object list synchronization* in *Feature Requirements on page 1-2*.

Suspicious Object Lists

Control Manager consolidates Virtual Analyzer Suspicious Objects lists and synchronizes all Suspicious Object lists among many managed products. The way each managed product implements the lists depends on how the product implements the

feature. Refer to your managed product Administrator's Guide for more information about how the product uses and synchronizes the Suspicious Object lists.

Note

Administrators can configure specific scan actions on Suspicious Objects using the Control Manager console. You can then configure certain managed products to perform actions based on the Suspicious Objects list settings.

For more information, see *Suspicious Object Scan Actions on page 1-8*.

LIST TYPE	DESCRIPTION
Virtual Analyzer Suspicious Objects	Managed products that integrate with a Virtual Analyzer submit suspicious files or URLs to Virtual Analyzer for analysis. If Virtual Analyzer determines that an object is a possible threat, Virtual Analyzer adds the object to the Suspicious Object list. Virtual Analyzer then sends the list to its registered Control Manager server for consolidation and synchronization purposes. On the Control Manager console, go to the **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects** > **Objects** tab to view the Virtual Analyzer Suspicious Objects list.
Exceptions to Virtual Analyzer Suspicious Objects	From the list of Virtual Analyzer suspicious objects, Control Manager administrators can select objects that are considered safe and then add them to an exception list. On the Control Manager console, go to the **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects** > **Exceptions** tab to view the Virtual Analyzer Suspicious Object Exceptions. Control Manager sends the exception list to the Virtual Analyzers that subscribe to the list. When a Virtual Analyzer detects a suspicious object that is in the exception list, the Virtual Analyzer considers the object as “safe” and does not analyze the object again. For more information, see *Adding Exceptions to the Virtual Analyzer Suspicious Object List on page 1-7*.

List Type	Description
User-Defined Suspicious Objects	Control Manager administrators can add objects they consider suspicious but are not currently in the list of Virtual Analyzer suspicious objects by going to **Administration** > **Suspicious Objects** > **User-Defined Objects**. For more information, see *Preemptive Protection Against Suspicious Objects on page 1-19*.

Adding Exceptions to the Virtual Analyzer Suspicious Object List

Control Manager allows you to exclude objects from the Virtual Analyzer Suspicious Object list based on the file SHA-1, domain, IP address, or URL.

Important

The User-Defined Suspicious Object list has a higher priority than the Virtual Analyzer Suspicious Object list.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**.

   The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Exceptions** tab.

3. Click **Add**.

4. Specify the **Type** of object.

   - **File SHA-1**: Specify the SHA-1 hash value for the file.
   - **IP address**: Specify the IP address.
   - **URL**: Specify the URL.
   - **Domain**: Specify the domain.

Control Manager allows you to use a wildcard character (*) to exclude specific subdomains or subdirectories from the Virtual Analyzer Suspicious Object list.

EXAMPLE	DESCRIPTION
https://*.domain.com/	Excludes all subdomains of the domain "domain.com" from the Virtual Analyzer Suspicious Object list
*.abc.domain.com	Excludes all subdomains of the subdomain "abc" from the Virtual Analyzer Suspicious Object list
https:// *.domain.com/abc/*	Excludes all subdomains of the domain "domain.com" and subdirectories of the subdirectory "abc" from the Virtual Analyzer Suspicious Object list

5. (Optional) Specify a **Note** to assist in identifying the suspicious object.
6. Click **Add**.

   The object appears in the Virtual Analyzer Exception list. Managed products that subscribe to the suspicious objects lists receive the new object information during the next synchronization.

Suspicious Object Scan Actions

Using the Control Manager console, administrators can configure scan actions that certain managed products take after detecting specific suspicious objects in the **Virtual Analyzer Suspicious Objects** list or the **User-Defined Suspicious Objects** list.

TABLE 1-1. Scan Action Product Support

PRODUCT	VIRTUAL ANALYZER LIST	USER-DEFINED LIST
OfficeScan XG SP1 (or later)	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **IP address**: Log, Block • **URL**: Log, Block • **Domain**: Log, Block	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **IP address**: Log, Block • **URL**: Log, Block • **Domain**: Log, Block
Deep Security 10.0 (or later)	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **URL**: Log, Block	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **URL**: Log, Block
• Deep Discovery Inspector 5.0 (or later) • Deep Discovery Email Inspector 3.0 (or later)	Synchronizes the following suspicious object types: • **File**: No scan actions performed • **IP address**: No scan actions performed • **URL**: No scan actions performed • **Domain**: No scan actions performed	Synchronizes the following suspicious object types: • **File**: No scan actions performed • **IP address**: No scan actions performed • **URL**: No scan actions performed • **Domain**: No scan actions performed

PRODUCT	VIRTUAL ANALYZER LIST	USER-DEFINED LIST
InterScan Messaging Security Virtual Appliance 9.1 (or later)	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **File SHA-1**: Log, Block, Quarantine
InterScan Web Security Virtual Appliance 6.5 Patch 2 (or later)	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **File SHA-1**: Log, Block, Quarantine • **IP address**: Log, Block • **URL**: Log, Block • **Domain**: Log, Block	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **File SHA-1**: Log, Block, Quarantine • **IP address**: Log, Block • **URL**: Log, Block • **Domain**: Log, Block
Trend Micro Endpoint Application Control 2.0 SP1 Patch 1 (or later)	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **File SHA-1**: Log, Block, Quarantine
Cloud App Security 5.0 (or later)	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **URL**: Log, Block	Performs actions against the following suspicious object types: • **File**: Log, Block, Quarantine • **URL**: Log, Block

<table>
<tr><th>PRODUCT</th><th>VIRTUAL ANALYZER LIST</th><th>USER-DEFINED LIST</th></tr>
<tr><td rowspan="2">Smart Protection Server 3.0 Patch 1 (or later)
OfficeScan 11.0 SP1 (or later) integrated Smart Protection Server
Trend Micro products that send Web Reputation queries to a supported Smart Protection Server</td><td>Managed products perform actions against the following suspicious object types during Web Reputation queries:
URL: Log, Block</td><td>Managed products perform actions against the following suspicious object types during Web Reputation queries:
URL: Log, Block
Important
Smart Protection Server classifies all URLs in the User-Defined Suspicious Objects list as “High” risk.</td></tr>
<tr><td colspan="2">Note
Only certain managed products can directly perform the actions configured in Control Manager on suspicious URL objects. Other managed products take action on suspicious URL objects based on the product's configured Web Reputation settings.

Logs that display on the managed products may not contain information related to suspicious object detections. Control Manager interprets logs sent from the managed product and displays the suspicious object detection on the Control Manager console.</td></tr>
</table>

Configuring Distribution Settings

Configure distribution settings to enable Control Manager to consolidate and send Virtual Analyzer and user-defined suspicious objects (excluding exceptions) to certain managed products. These products synchronize and use all or some of these objects.

Control Manager can also send suspicious IP addresses and domains to TippingPoint.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **Distribution Settings**.

   The **Distribution Settings** screen appears.

2. To send suspicious objects to managed products:

   a. Click the **Managed Products** tab.

   b. Select the **Send suspicious objects to managed products** check box.

   c. Record the following information for use when configuring Control Manager as the Virtual Analyzer source in managed products:

      - **Service URL**: The service URL of Control Manager
      - **API key**: The code that identifies Control Manager to the managed product

   d. Click **Save**.

   e. Click **Sync Now**.

3. To send suspicious objects to TippingPoint:

   a. Select the **Send suspicious objects (IP addresses and domain names only) to TippingPoint** check box.

   Note

   Control Manager sends suspicious IP addresses and domain names analyzed by Deep Discovery Inspector and Deep Discovery Analyzer. TippingPoint uses reputation filters to apply block, permit, or notify actions across an entire reputation group. For more information about reputation filters, refer to your TippingPoint documentation.

   b. Specify the following:

      - **Server name**: Type the server URL and port number for your TippingPoint deployment.
      - **User name**: Type the user name of an account with sufficient privileges to access the TippingPoint console.

- **Password**: Type the password for the account.

c. (Optional) Click **Test Connection** to confirm the connection.

d. Select the severity level that triggers Control Manager to send domain names or IP address information to TippingPoint.

- **High only**: IP addresses and domain names with high severity
- **High and medium**: IP addresses and domain names with high and medium severity
- **All**: Includes IP addresses and domain names with high, medium, and low severity

4. Click **Save**.

5. Click **Sync Now**.

Suspicious Object Detection

You can view suspicious object detections in your environment in many ways using the Control Manager console. For information regarding the different ways of viewing suspicious object detections, refer to the following:

- *Viewing At Risk Endpoints and Recipients on page 1-13*
- *Assessing Impact Using Endpoint Sensor on page 1-15*

Note

Control Manager only identifies users or endpoints exposed to suspicious objects in your environment. You cannot take any direct action on any suspicious objects using the Control Manager console.

Viewing At Risk Endpoints and Recipients

Control Manager checks Web Reputation, URL filtering, network content inspection, and rule-based detection logs received from all managed products and then compares these logs with its list of suspicious objects.

Required Products	Optional Products
• Control Manager 7.0 (or later) • At least one optional product	• Trend Micro products managed by Control Manager • Endpoint Sensor 1.5 (or later) **Important** • Endpoint Sensor 1.5 only provides information related to the **File** and **IP address** suspicious object types. • Endpoint Sensor 1.6 (or later) provides information related to the **File**, **IP address**, and **Domain** suspicious object types.

Procedure

1. On the Control Manager console, go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**.
2. Expand the arrow to the left of the **Object** you want to view.
   - The **At Risk Endpoints** list displays all endpoints and users still affected by the suspicious object.
     - For **File** detections, the **Latest Action Result** column displays the last action result reported from managed products.
     - For all other detection types, the **Latest Action Result** column displays "N/A".
   - The **At Risk Recipients** list displays all recipients still affected by the suspicious object.

Assessing Impact Using Endpoint Sensor

Endpoint Sensor contacts agents and performs a historical scan of the agent logs to determine if the suspicious objects have affected your environment for a period of time without detection.

Required Products	Optional Products
• Control Manager 7.0 (or later) • Endpoint Sensor 1.5 (or later) **Important** • Endpoint Sensor 1.5 only provides information related to the **File** and **IP address** suspicious object types. • Endpoint Sensor 1.6 (or later) provides information related to the **File**, **IP address**, and **Domain** suspicious object types.	• None

Procedure

1. On the Control Manager console, go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**.
2. Select the check box next to the **Object** you want to assess.
3. Click **Assess Impact**.

   Endpoint Sensor contacts agents and evaluates the agent logs for any detections of the suspicious objects.

Retro Scan in Endpoint Sensor

Retro Scan investigates historical events and their activity chain based on a specified search condition. The results can be viewed as a mind map showing the execution flow

of any suspicious activity. This facilitates the analysis of the enterprise-wide chain of events involved in a targeted attack.

Retro Scan uses the following object types for its investigation:

- DNS record
- IP address
- File name
- File path
- SHA-1 hash values
- MD5 hash values
- User account

Retro Scan queries a normalized database containing an endpoint's historical events. Compared to a traditional log file, this method uses less disk space and consumes less resources.

Viewing the Handling Process

The **Handling Process** screen provides an overview of the life-cycle for a suspicious object in your environment and current effect of the suspicious object to your users or endpoints.

Required Products	Optional Products
• Control Manager 7.0 (or later) • Deep Discovery Inspector 3.8 (or later) or Deep Discovery Analyzer 5.1 (or later) • At least one optional product is required to view **Impact Assessment** and **Mitigation** data	• Trend Micro products managed by Control Manager • Endpoint Sensor 1.5 (or later) **Important** • Endpoint Sensor 1.5 only provides information related to the **File** and **IP address** suspicious object types. • Endpoint Sensor 1.6 (or later) provides information related to the **File**, **IP address**, and **Domain** suspicious object types.

Procedure

1. On the Control Manager console, go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**.
2. Click the **View** link in the **Handling Process** column of the table for a specific suspicious object.

   The **Handling Process** screen appears.
3. Click any of the following tabs to view more information about the suspicious object.

Tab	Description
Sample Submission	Displays information related to the first and latest analysis of the suspicious object Control Manager integrates with the following products, which use a Virtual Analyzer to analyze suspicious objects submitted by other managed products: • Deep Discovery Analyzer 5.1 (or later) • Deep Discovery Endpoint Inspector 3.0 (or later) • Deep Discovery Inspector 3.8 (or later)
Analysis	Displays the Virtual Analyzer analysis of the submitted object Virtual Analyzer determines the risk level of suspicious objects based on their potential to expose systems to danger or loss. Supported objects include files (SHA-1 hash values), IP addresses, domains, and URLs.
Distribution	Displays all products that synchronized the Suspicious Object list and the last synchronization time Control Manager consolidates Virtual Analyzer and user-defined suspicious object lists (excluding exceptions) and synchronizes the lists with integrated managed products.
Impact Assessment & Mitigation	Displays all endpoints and users affected by the suspicious object • For **File** detections, the **Latest Action Result** column displays the last action result reported from managed products. • For all other detection types, the **Latest Action Result** column displays “N/A”. Click the **Suspicious Activities** link to further investigate how the object affected the user or endpoint.

Preemptive Protection Against Suspicious Objects

Control Manager provides different ways to protect against suspicious objects not yet identified within your network. Use the User-Defined Suspicious Objects list or import Indicators of Compromise (IOCs) to take proactive actions on suspicious threats identified by external sources.

FEATURE	DESCRIPTION
User-Defined Suspicious Objects list	The User-Defined Suspicious Objects list allows you to define suspicious file, IP address, URL, and domain objects that your registered Virtual Analyzer has not yet detected on your network. Supported managed products that subscribe to the Suspicious Object lists can take action on the objects found in the list to prevent the spread of unknown threats. *Adding Objects to the User-Defined Suspicious Object List on page 1-20* *Suspicious Object Scan Actions on page 1-8*
Indicators of Compromise	Import IOC files to perform an in-depth historical analysis on endpoints on your network to determine if a threat has already affected your environment. Performing an impact assessment on IOCs requires detailed log information regarding the behavior of the endpoint over time. Only endpoints with Endpoint Sensor 1.5 (or later) installed collect the necessary log information required to perform this type of detailed analysis. Through integration with OfficeScan 11.0 SP1 (or later) agents, you can isolate affected endpoints to prevent the further spread of the threats identified on endpoints. *Assessing Impact and Responding to IOCs on page 1-21*

Adding Objects to the User-Defined Suspicious Object List

You can protect your network from objects not yet identified on your network by adding the suspicious objects to the User-Defined Suspicious Objects list. Control Manager provides you the options to add objects based on the file, file SHA-1, domain, IP address, or URL. You can also specify the scan action that supported Trend Micro products take after detecting the suspicious objects (excluding domain objects).

Procedure

1. Go to **Administration** > **Suspicious Objects** > **User-Defined Objects**.

   The **User-Defined Suspicious Objects** screen appears.

2. Click **Add**.

3. Specify the **Type** of object.

   - **File**: Click **Browse** to upload a suspicious object file.
   - **File SHA-1**: Specify the SHA-1 hash value for the file.
   - **IP address**: Specify the IP address.
   - **URL**: Specify the URL.
   - **Domain**: Specify the domain.

4. Specify the **Scan action** that supported products take after detecting the object.

   - **Log**
   - **Block**
   - **Quarantine**

   Note

   This option is only available for **File** or **File SHA-1** objects.

5. (Optional) Specify a **Note** to assist in identifying the suspicious object.

6. Click **Add**.

   The object appears in the User-Defined Suspicious Objects list. Managed products that subscribe to the suspicious objects lists receive the new object information during the next synchronization.

Importing User-Defined Suspicious Object Lists

Add multiple suspicious objects to the User-Defined Suspicious Objects list using a properly formatted CSV file.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **User-Defined Objects**.

   The **User-Defined Suspicious Objects** screen appears.

2. Click **Import**.

3. Select the CSV file containing the list of suspicious objects.

   Tip

   Click the **Download sample CSV** link to obtain a properly formatted example CSV file with detailed instructions on creating a user-defined suspicious objects list.

4. Click **Import**.

   Objects in the CSV file appear in the User-Defined Suspicious Objects list. Managed products that subscribe to the suspicious objects lists receive the new object information during the next synchronization.

Assessing Impact and Responding to IOCs

After obtaining properly formatted IOC files from a trusted external source (a security forum or other Deep Discovery Virtual Analyzer product), import the file to Control Manager to determine if the threat exists within your network and take mitigation steps to prevent the spread of the threat to other endpoints.

Important

- Impact assessment of external IOC data requires that Endpoint Sensor 1.5 (or later) is registered to Control Manager and installed on the target endpoints.
- Endpoint isolation requires that you install OfficeScan 11.0 SP1 (or later) agents with the OfficeScan firewall enabled on the target endpoints.

Procedure

1. Go to **Administration** > **Indicators of Compromise**.

   The **Indicators of Compromise (IOCs)** screen appears.

2. Click **Add**.

3. Select the IOC file you want to use as the source of your investigation.

4. Click **Upload**.

   A screen appears listing the supported indicators contained within the file.

5. To start an investigation, select the IOC file from the list and click **Assess Impact**.

   The **Investigate Now** screen appears.

6. From the **Target endpoints** drop-down, select **All**, or **Specific** and type the endpoint names or IP addresses to investigate.

   Use a new line to add multiple endpoint names or IP addresses.

7. Click **Investigate Now**.

   Note

   Performing an investigation may take some time to complete. Monitor the investigation progress in the **Progress** column.

8. After the assessment completes, click the number in the **At Risk** column to view more details or take action on affected endpoints.

Note

The **Pending/With Issues** column displays the number of endpoints on which the assessment has not yet completed. For example, the assessment cannot start on an endpoint until the endpoint reconnects to the network.

The **Indicators of Compromise > At Risk Endpoints** screen appears.

9. To prevent the spread of suspicious objects across your network, click **Isolate** in the **Action** column to stop network traffic on the affected endpoints.

Important

Endpoint isolation requires that you install OfficeScan 11.0 SP1 (or later) agents with the OfficeScan firewall enabled on the target endpoints.

10. Click the **Modify Allowed Traffic** button to optionally configure allowed inbound and outbound traffic to all isolated endpoints.

    a. Select **Control traffic on isolated endpoints**.

    b. Expand the **Inbound Traffic** or **Outbound Traffic** sections.

    c. Specify the allowed traffic by specifying the **Protocol**, **IP Address**, and **Destination Port**.

       Separate multiple destination ports using commas.

    d. Add multiple inbound and outbound entries by clicking the **-** control to the right of the **Destination Port** information.

Note

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

Isolating Endpoints

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

Required Products	Optional Products
• Control Manager 7.0 (or later) • OfficeScan 11.0 SP1 (or later) **Important** Endpoint isolation requires that you install OfficeScan agents with the OfficeScan firewall enabled on the target endpoints.	• Endpoint Sensor 1.5 (or later)

Procedure

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

   Control Manager disables the **Isolate** option on endpoints for the following reasons:

   - The agent on the endpoint runs an unsupported version.
   - The user account used to log on to Control Manager does not have the necessary permissions.

5. A message appears at the top of the **Endpoint - {name}** screen that allows you to monitor the isolation status. After isolation completes, the message closes and a notification appears on the target endpoint to inform the user.

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

6. To view all isolated endpoints on your Control Manager network, click the **Endpoints** > **Filters** > **Network Connection** > **Isolated** node in the User/Endpoint Directory tree.

7. Click the **Modify Allowed Traffic** button to optionally configure allowed inbound and outbound traffic to all isolated endpoints.

   a. Select **Control traffic on isolated endpoints**.

   b. Expand the **Inbound Traffic** or **Outbound Traffic** sections.

   c. Specify the allowed traffic by specifying the **Protocol**, **IP Address**, and **Destination Port**.

      Separate multiple destination ports using commas.

   d. Add multiple inbound and outbound entries by clicking the **-** control to the right of the **Destination Port** information.

Note

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

8. After you have resolved the security threats on an isolated endpoint, restore network connectivity from the following locations:

   - **Endpoint - {name}**: Click **Task** > **Restore**.
   - **Endpoints** > **Filters** > **Network Connection** > **Isolated**: Select the endpoint row in the table and click **Restore Network Connection**.

9. A message appears at the top of the screen that allows you to monitor the restoration status. After restoration completes, the message closes and a notification appears on the target endpoint to inform the user.

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

Connected Threat Defense Product Integration

The Connected Threat Defense strategy integrates many Trend Micro products. The following diagrams illustrate how the major products interact.

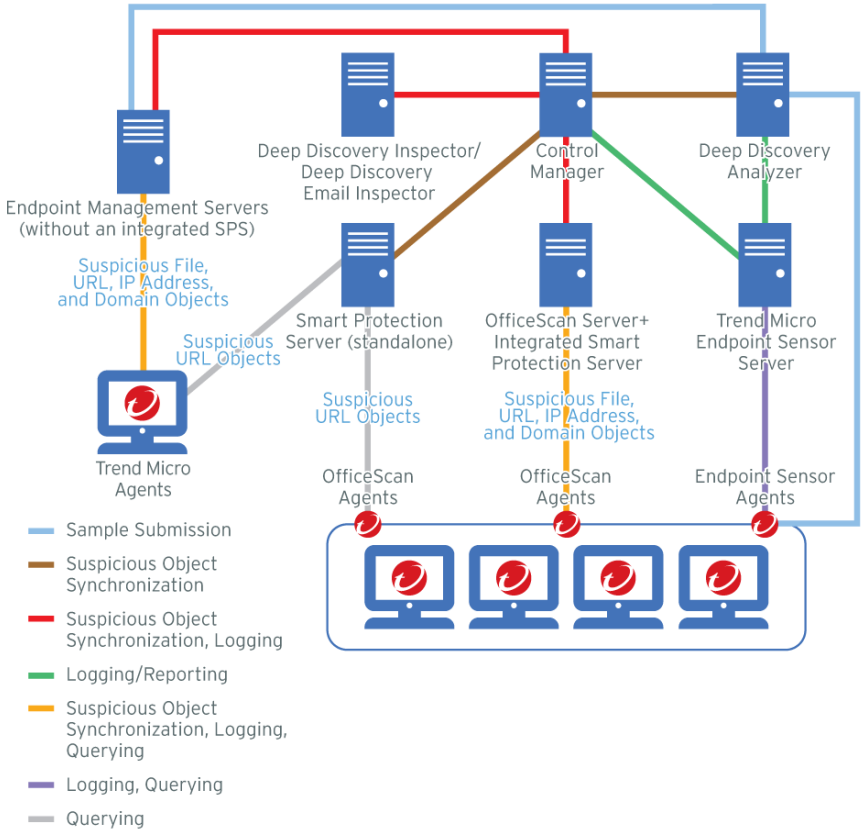


FIGURE 1-1. Endpoint Protection

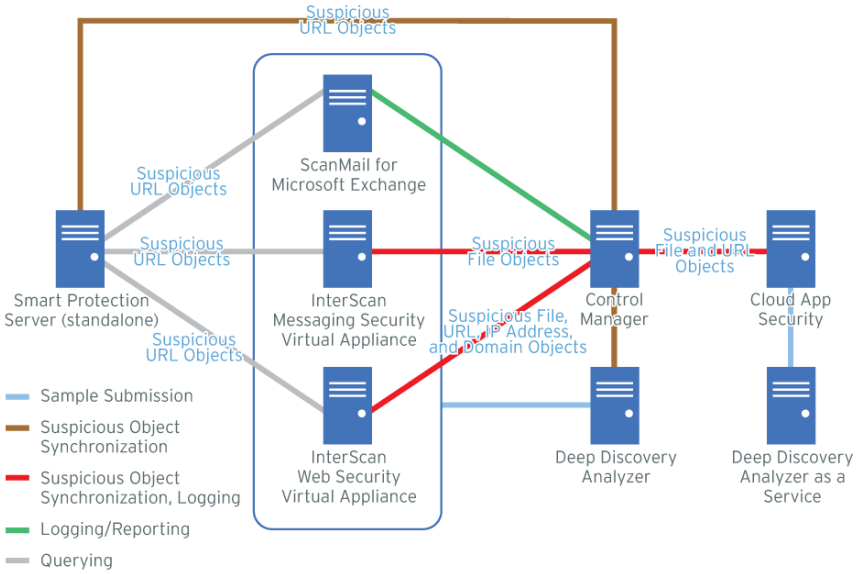


FIGURE 1-2. Messaging and Network Security

Control Manager further monitors other registered Trend Micro products through log analysis and comparison of detected files with the synchronized Suspicious Objects lists.

For Control Manager registration and Suspicious Objects list synchronization information for each major product, refer to the following:

- *Control Manager on page 1-28*
- *Deep Discovery Analyzer on page 1-29*
- *Trend Micro Endpoint Sensor on page 1-30*
- *Deep Discovery Inspector on page 1-30*
- *Deep Security on page 1-31*
- *OfficeScan on page 1-32*

Control Manager

REQUIREMENT	DESCRIPTION
Product version	7.0 (or later)
Control Manager registration information	For products that do not register to Control Manager through the Control Manager console, the following Control Manager registration information is required: • Server FQDN or IP address • Port: By default, Control Manager uses HTTP Port 80 or HTTPS Port 443 For products that register using the Control Manager management console, go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.
Suspicious Objects list synchronization	For products that do not automatically synchronize the Suspicious Objects lists with Control Manager, the following API information is required: • API key: To obtain the API key, open the Control Manager management console and go to **Administration** > **Suspicious Objects** > **Distribution Settings**.

Requirement	Description
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object management • Impact assessment • Endpoint isolation • IOC management

Deep Discovery Analyzer

Requirement	Description
Product version	5.1 (or later)
Control Manager registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.
Suspicious Objects list synchronization	Automatic after registration to Control Manager The Suspicious Objects lists synchronize with the Control Manager server every 10 minutes by default.
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object sample submission • Suspicious Object management

Trend Micro Endpoint Sensor

Note

- Previously named Deep Discovery Endpoint Sensor (version 1.5 and older).
- Endpoint Sensor does not support Suspicious Object list synchronization.

REQUIREMENT	DESCRIPTION
Product version	1.5 (or later)
Control Manager registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object sample submission • Suspicious Object management • Impact assessment • Endpoint isolation • IOC management

Deep Discovery Inspector

REQUIREMENT	DESCRIPTION
Product version	3.8 (or later)

Requirement	Description
Control Manager registration	From the Deep Discovery Inspector management console at **Administration** > **Integrated Products/Services** > **Control Manager** Required Control Manager information: • Server FQDN or IP address • Port: By default, Control Manager uses HTTP Port 80 or HTTPS Port 443 For more information, see the *Deep Discovery Inspector Administrator's Guide*.
Suspicious Objects list synchronization	From the Deep Discovery Inspector management console at **Administration** > **Integrated Products/Services** > **Control Manager** Required Control Manager information: • API key: To obtain the API key, open the Control Manager management console and go to **Administration** > **Suspicious Objects** > **Distribution Settings**. For more information, see the *Deep Discovery Inspector Administrator's Guide*.
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object sample submission • Suspicious Object management

Deep Security

Requirement	Description
Product version	10.0 (or later)

Requirement	Description
Control Manager registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.
Suspicious Objects list synchronization	Automatic after registration to Control Manager
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object sample submission • Suspicious Object management • Suspicious Object scan actions

OfficeScan

Requirement	Description
Product version	11.0 SP1 (or later)
Control Manager registration	From the OfficeScan web console at **Administration** > **Settings** > **Control Manager** Required Control Manager information: • Server FQDN or IP address • Port: By default, Control Manager uses HTTP Port 80 or HTTPS Port 443 For more information, see the *OfficeScan Administrator's Guide*.

REQUIREMENT	DESCRIPTION
Suspicious Objects list synchronization	From the OfficeScan web console at **Administration** > **Settings** > **Suspicious Object List** Required Control Manager information: • None **Note** OfficeScan automatically obtains the required API key information from the Control Manager server during Control Manager registration
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object management • Endpoint isolation

Smart Protection Server

REQUIREMENT	DESCRIPTION
Product version	3.0 Patch 1 (or later)
Control Manager registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.

REQUIREMENT	DESCRIPTION
Suspicious Object list synchronization	From the Smart Protection Server web console: • For Smart Protection Server 3.0 Patch 1, go to **Smart Protection** > **C&C Contact Alert** • For Smart Protection Server 3.0 Patch 2 (or later), go to **Smart Protection** > **Suspicious Objects** Required information about the Suspicious Object list source: • Service URL • Port If the list source is Control Manager, the default ports are HTTP Port 80 or HTTPS Port 443. • API key: Provided by the server administrator If the list source is Control Manager, open the Control Manager management console and go to **Administration** > **Suspicious Objects** > **Distribution Settings**. **Note** For Smart Protection Server 3.3 (or later), Control Manager automatically sends the required API key information to the Smart Protection Server during registration. For more information, see the *Smart Protection Server Administrator's Guide*.
Integrated Connected Threat Defense features	• Suspicious Object list synchronization • Suspicious Object scan actions

InterScan Messaging Security Virtual Appliance

REQUIREMENT	DESCRIPTION
Product version	9.1 (or later)

REQUIREMENT	DESCRIPTION
Control Manager registration	For more information, see the *InterScan Messaging Security Virtual Appliance Administrator's Guide*.
Suspicious Objects list synchronization	Automatic after registration to Control Manager
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object sample submission • Suspicious Object management • Suspicious Object scan actions

InterScan Web Security Virtual Applicance

REQUIREMENT	DESCRIPTION
Product version	6.5 SP2 Patch 2 (or later)
Control Manager registration	For more information, see the *InterScan Web Security Virtual Appliance Administrator's Guide*.
Suspicious Objects list synchronization	For more information, see the *InterScan Web Security Virtual Appliance Administrator's Guide*.
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object sample submission • Suspicious Object management • Suspicious Object scan actions

ScanMail for Microsoft Exchange

Requirement	Description
Product version	12.5 (or later)
Control Manager registration	For more information, see the *ScanMail for Microsoft Exchange Administrator's Guide*.
Suspicious Objects list synchronization	For more information, see the *ScanMail for Microsoft Exchange Administrator's Guide*.
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object sample submission

Trend Micro Endpoint Application Control

Requirement	Description
Product version	2.0 SP1 Patch 1 (or later)
Control Manager registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.
Suspicious Objects list synchronization	Automatic after registration to Control Manager
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object management

Deep Discovery Email Inspector

Requirement	Description
Product version	3.0 (or later)
Control Manager registration	For more information, see the *Deep Discovery Email Inspector Administrator's Guide*.
Suspicious Objects list synchronization	For more information, see the *Deep Discovery Email Inspector Administrator's Guide*.
Integrated Connected Threat Defense features	• Suspicious Object list synchronization • Suspicious Object sample submission

Cloud App Security

Requirement	Description
Product version	5.0 (or later)
Control Manager registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** > **Server Registration**, select the product from the **Server Type** list, and click **Add**.
Suspicious Objects list synchronization	For more information, see the *Cloud App Security Administrator's Guide*.
Integrated Connected Threat Defense features	• Security threat monitoring • Suspicious Object list synchronization • Suspicious Object management • Suspicious Object scan actions

Chapter 2

Suspicious Object List Exporter and Importer User Guide

This section discusses how to use the Control Manager Suspicious Object List Exporter (`SuspiciousObjectExporter.exe`) and Importer (`ImportSOFromCSV.exe`) tools.

Topics include:

Suspicious Object List Exporter and Importer User Guide

The Trend Micro Control Manager™ Suspicious Object List Exporter and Importer tools allow you to export and import Control Manager Suspicious Object lists without having to sign in to the Control Manager management console.

- Suspicious Object List Exporter: Exports Suspicious Object lists from the Control Manager server in multiple file formats.
- Suspicious Object List Importer: Imports properly formatted comma-separated value (CSV) suspicious object data into Control Manager.

Use the Exporter and Importer tools to synchronize suspicious object data across multiple Control Manager servers and supported third-party applications to enhance your protection against unknown and emerging threats.

Using the Suspicious Object List Exporter (SuspiciousObjectExporter.exe)

Use the Suspicious Object List Exporter tool (`SuspiciousObjectExporter.exe`) to export Control Manager Suspicious Object lists in multiple file formats. By default, the Suspicious Object List Exporter tool exports suspicious object data in XML format.

For details on how to change the output file format, see *Modifying the Configuration File on page 2-7*.

Important

The Suspicious Object List Exporter tool requires Control Manager 7.0 (or later).

To download the latest installation package, see http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4202&lang_loc=1.

Procedure

1. Open a command prompt on the Control Manager server.
2. Use the following command to locate the directory which contains the `SuspiciousObjectExporter.exe` file:

   `cd <Control Manager installation directory>\SOTools`

3. Execute `SuspiciousObjectExporter.exe` using the following command:

   `SuspiciousObjectExporter.exe [/s <Start ID> /e <End ID>] [/f <y | n>] [/d]`

Note

Running **`SuspiciousObjectExporter.exe`** without any parameters displays usage details and prompts you to provide <Start ID> and <End ID> values.

PARAMETER	DESCRIPTION	EXAMPLE
/s <Start ID>	Indicates the ID of the first object to export **Note** • Requires that you specify the /e <End ID> value • Specifying a value of 0 indicates the start of the list	• `SuspiciousObjectExporter.exe /s 0 /e 0` Exports all suspicious objects and locks the command line interface during the export process • `SuspiciousObjectExporter.exe /s 3 /e 8` Exports suspicious objects starting from ID 3 to ID 8 and locks the command line interface during the export process • `SuspiciousObjectExporter.exe /s 0 /e 4` Exports suspicious objects starting from the beginning of the list to ID 4 and locks the command line interface during the export process

PARAMETER	DESCRIPTION	EXAMPLE
/e <End ID>	Indicates the ID of the last object to export **Note** • Requires that you specify the /s <Start ID> value • Specifying a value of 0 indicates the end of the list	• `SuspiciousObjectExporter.exe /s 0 /e 0` Exports all suspicious objects and locks the command line interface during the export process • `SuspiciousObjectExporter.exe /s 3 /e 8` Exports suspicious objects starting from ID 3 to ID 8 and locks the command line interface during the export process • `SuspiciousObjectExporter.exe /s 4 /e 0` Exports suspicious objects starting from ID 4 to the end of the list and locks the command line interface during the export process

PARAMETER	DESCRIPTION	EXAMPLE
/f <y | n>	Specifies whether to lock the command line interface during the export process **Note** Optional parameter; if not specified, the default is "yes" **Important** You must specify the following parameter in the **Add arguments (optional)** field when scheduling automatic exports using the `SuspiciousObjectExporter.exe` tool, a PowerShell script, or a batch script in Windows Task Scheduler: **`/f n`**	• **`SuspiciousObjectExporter.exe /f y`** Exports all suspicious objects and locks the command line interface during the export process • **`SuspiciousObjectExporter.exe /s 0 /e 0 /f y`** Exports all suspicious objects and locks the command line interface during the export process • **`SuspiciousObjectExporter.exe /f n`** Exports all suspicious objects and unlocks the command line interface during the export process
/d	Use to enable debug mode **Note** Optional parameter normally used by Support to identify errors	**`SuspiciousObjectExporter.exe /d`** Exports all suspicious objects with additional debugging logs

4. To view the exported Suspicious Object list, go to the `<current directory>\SOTools\` directory and open the `SuspiciousObjectList.xml` file.

Note

If you followed this procedure, the `<current directory>` is the `<Control Manager installation directory>`.

5. To view all export logs, go to the `<current directory>\SOTools\` directory and open the `ExportRecord.txt` file.

Note

If you followed this procedure, the `<current directory>` is the `<Control Manager installation directory>`.

Modifying the Configuration File

To change the default configuration settings of the Suspicious Object List Importer, go to the `<Control Manager installation directory>\SOTools` directory and modify the `SuspiciousObjectExporter.exe.config` file.

Tip

Trend Micro recommends creating a backup file of the configuration file before making any modifications.

KEY	DESCRIPTION	EXAMPLE
outputRootFolderPath Location: `<appSettings>`	Indicates the working directory for the `SuspiciousObjectExporter.exe` tool	• `<add key="outputRootFolderPath" value="."/>` The tool uses the directory in which the `SuspiciousObjectExporter.exe` program resides to process the lists • `<add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager"/>` The tool uses the specified directory (`C:\Program Files (x86)\Trend Micro\Control Manager`) to process the lists
outputFolderName Location: `<appSettings>`	Indicates the output directory for the exported Suspicious Object list file	• `<add key="outputFolderName" value="SOTools"/>` Exports the file to the `<outputRootFolderPath>\SOTools` directory • `<add key="outputFolderName" value="SOList"/>` Exports the file to the `<outputRootFolderPath>\SOList` directory

KEY	DESCRIPTION	EXAMPLE
styleSheetFile Location: `<appSettings>`	Indicates the style sheet that the tool applies to the exported list	• `<add key="styleSheetFile" value=""/>` Exports all lists in XML format to a `*.txt` or `*.xml` file as specified by the `outputFile` key • `<add key="styleSheetFile" value="ExportCSV.xslt"/>` Used to export the Virtual Analyzer Suspicious Object list, User-Defined Suspicious Object list, or Exception list with a limited subset of columns in CSV format **Important** After selecting the `ExportCSV.xslt` style sheet, you can no longer configure which columns the tool exports. The tool only exports the columns specified in the style sheet. • `<add key="styleSheetFile" value="ExportSTIX.xslt"/>` Used to export all Suspicious Object lists in STIX format • `<add key="styleSheetFile" value="ExportCPL.xslt"/>` Used to export all Suspicious Object lists in CPL format **Important** If you specify a style sheet, you must set the `defaultSampleTemplates` key to the same value.

KEY	DESCRIPTION	EXAMPLE
outputFile Location: `<appSettings>`	Indicates the file name and extension of the exported Suspicious Object list file Specify a new file extension to change the output file format	• `<add key="outputFile" value="SuspiciousObjectList.xml"/>` Exports the Suspicious Object list as an `*.xml` file named `SuspiciousObjectList.xml` • `<add key="outputFile" value="SuspiciousObjectList.txt"/>` Exports the Suspicious Object list as a `*.txt` file named `SuspiciousObjectList.txt`
defaultSampleTemplates Location: `<appSettings>`	Indicates the source file for the style sheet that the tool applies to the exported list	• `<add key="defaultSampleTemplates" value="ExportCSV.xslt"/>` Locates the specified style sheet file **Important** The specified value must match the value specified for the `styleSheetFile` or `defaultSampleTemplates` key. **Note** The default value is `"ExportCPL.xslt|ExportSTIX.xslt|ExportCSV.xslt"`.

KEY	DESCRIPTION	EXAMPLE
<suspiciousObjectColumns> Location: `<soDataColumnSettings>`	Indicates the data columns on the selected list Set `isEnable="true"` to export the specified data column	• `<add id="1" name="SeqID" isEnable="true"></add>` Exports the "SeqID" data column from the selected list • `<add id="1" name="MD5Key" isEnable="false"></add>` Explicitly excludes the "MD5Key" data column from the selected list **Important** If you specified the `ExportCSV.xslt` style sheet, the tool only exports the columns specified in the style sheet.
<suspiciousObjectTypeList> Location: `<soTypeSettings>`	Indicates the types of objects to export from the selected list Set `isEnable="true"` to export the specified object type	• `<add value="0" description="IP" isEnable="true"></add>` Exports all IP address type objects from the selected list • `<add value="1" description="Domain" isEnable="false"></add>` Explicitly excludes all "Domain" objects from the exported list

KEY	DESCRIPTION	EXAMPLE
<suspiciousObjectSourceType> Location: `<soTypeSettings>`	Indicates the suspicious object source type Set `isEnable="true"` to export the specified object type	• `<add value="0" description="SourceType" isEnable="true"/>` Selects the Virtual Analyzer Suspicious Object list • `<add value="1" description="SourceType" isEnable="true"/>` Selects the User-Defined Suspicious Object list • `<add value="2" description="SourceType" isEnable="true"/>` Selects the Virtual Analyzer Exception list **Important** • If you specified the `ExportCSV.xslt` style sheet and select the Virtual Analyzer Suspicious Object list or the User-Defined Suspicious Object list, the tool exports the following columns: **Object**, **Type**, **Scan Prefilter**, **Notes** and **Scan Action**. • If you specified the `ExportCSV.xslt` style sheet and select the Virtual Analyzer Exception list, the tool exports the following columns: **Object**, **Type**, **Scan Prefilter**, and **Notes**.

Using Control Manager to Export the Virtual Analyzer Exception List

Important

Control Manager only supports exporting the Virtual Analyzer Suspicious Object Exception list in CSV format.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**.

   The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Exceptions** tab.

3. Click **Export All**.

   A progress screen appears.

4. When the export finishes, click **Download**.

   A confirmation box appears.

5. Click **Save**.

   The **Save As** screen appears.

6. (Optional) Specify a new location or file name.

7. Click **Save**.

Using Control Manager to Export the User-Defined List

Important

Control Manager only supports exporting the User-Defined Suspicious Object list in CSV format.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **User-Defined Objects**

   The **User-Defined Suspicious Objects** screen appears.

2. Click **Export All**.

A progress screen appears.

3. When the export finishes, click **Download**.

   A confirmation box appears.

4. Click **Save**.

   The **Save As** screen appears.

5. (Optional) Specify a new location or file name.

6. Click **Save**.

Using the Suspicious Object List Importer (ImportSOFromCSV.exe)

Use the Suspicious Object List Importer tool (`ImportSOFromCSV.exe`) to import properly formatted `*.csv` files of suspicious object data into Control Manager.

Important

The Suspicious Object List Importer tool requires Control Manager 7.0 (or later).

To download the latest Control Manager installation package, see http://downloadcenter.trendmicro.com/index.php?regs=NABU&clk=latest&clkval=4202&lang_loc=1.

Procedure

1. Open a command prompt on the Control Manager server.

2. Use the following command to locate the directory which contains the `ImportSOFromCSV.exe` file:

   ```
   cd <Control Manager installation directory>
   ```

3. Execute `ImportSOFromCSV.exe` using the following command:

`ImportSOFromCSV.exe "<full path>" {UserDefinedSO | ExceptionSO}`

Where:

- **`<full path>`**: Indicates the directory and file name of the properly formatted CSV file
- **`{UserDefinedSO}`**: Indicates the file that contains User-Defined Suspicious Object list data
- **`{ExceptionSO}`**: Indicates the file that contains Virtual Analyzer Exception list data

For example:

- **`SuspiciousObjectImporter.exe "c:\Program Files (x86)\Trend Micro\Control Manager \importExceptionSample.csv" ExceptionSO`**

  Imports the `importExceptionSample.csv` file from the `c:\Program Files (x86)\Trend Micro\Control Manager` directory to the Virtual Analyzer Exception list in Control Manager

Using Control Manager to Import the Virtual Analyzer Exception List

Important

Control Manager only supports importing properly formatted `*.csv` files of Virtual Analyzer Exception list data.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**

   The **Virtual Analyzer Suspicious Objects** screen appears.

2. Click the **Exceptions** tab.
3. Click **Import**.

   The **Import Exception** screen appears.
4. Click **Browse...** and select the `*.csv` file containing the Exception list data.

   Tip

   Click the **Download sample CSV** link to obtain an example of a properly formatted `*.csv` file with detailed instructions.
5. Click **Open**.
6. Click **Import**.

   The **Import Exception** screen closes and the imported exceptions appear in the Virtual Analyzer Suspicious Object Exception list.

Using Control Manager to Import the User-Defined List

Important

Control Manager only supports importing properly formatted `*.csv` files of user-defined suspicious object data.

Procedure

1. Go to **Administration** > **Suspicious Objects** > **User-Defined Objects**

   The **User-Defined Suspicious Objects** screen appears.
2. Click **Import**.

   The **Import User-Defined List** screen appears.

3. Click **Browse...** and select the `*.csv` file containing the user-defined suspicious object data.

Tip

Click the **Download sample CSV** link to obtain an example of a properly formatted `*.csv` file with detailed instructions.

4. Click **Open**.

5. Click **Import**.

   The **Import User-Defined List** screen closes and the imported objects appear in the User-Defined Suspicious Object list.

Chapter 3

Suspicious Object Hub and Node Control Manager Architecture

This section presents material administrators need to synchronize suspicious object lists across multiple Control Manager servers.

Topics include:

Suspicious Object Hub and Node Control Manager Architecture

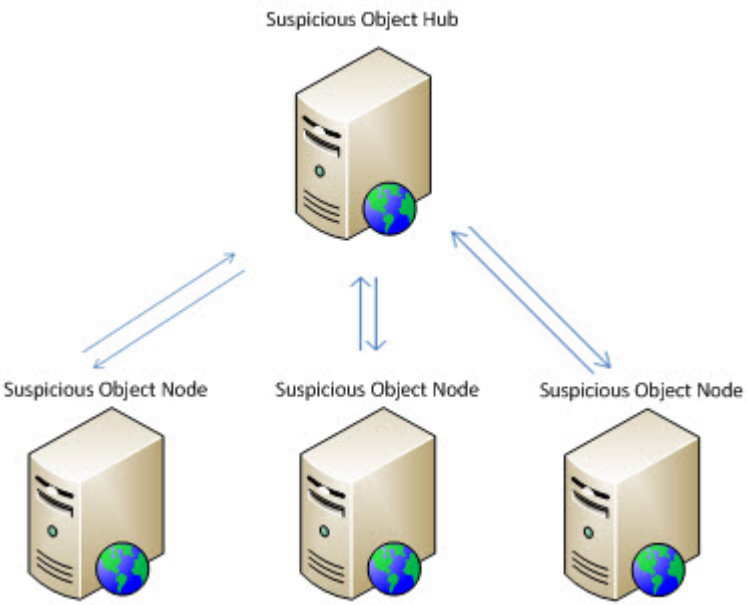
Trend Micro Control Manager™ Suspicious Object Hub and Node architecture allows you to synchronize suspicious object lists across multiple Control Manager servers. The suspicious object lists on the Hub Control Manager server consolidate the suspicious object lists from all Node Control Manager servers, and any other managed products registered to any of these servers, and then deploys the lists back to the Node Control Manager servers.

Administrators must first configure a Suspicious Object Hub Control Manager server and, depending on the environment, assign other Control Manager servers to act as Suspicious Object Node servers. Trend Micro Deep Discovery products can register to the Suspicious Object Hub or any Suspicious Object Node Control Manager server. This architecture requires that you configure all suspicious object actions through the Suspicious Object Hub Control Manager server console.

Important

You must perform all operations on the suspicious object lists through the Suspicious Object Hub Control Manager to ensure that all Node Control Manager servers remain properly synchronized.

Scan actions performed on suspicious objects though a Suspicious Object Node Control Manager may not synchronize to all connected servers.



Configuring the Suspicious Object Hub and Nodes

Procedure

1. Log on to the Suspicious Object Hub Control Manager server console.
2. Go to **Administration** > **Suspicious Objects** > **Distribution Settings**.

   The **Distribution Settings** screen appears.
3. Click the **Managed Products** tab and copy (write down) the following settings:
   - **Service URL**

- **API key**

4. Log on to the Suspicious Object Node Control Manager server console.
5. Go to **Administration** > **Suspicious Objects** > **Distribution Settings**.

   The **Distribution Settings** screen appears.
6. On the **Hub Control Manager** tab, provide the following settings copied from the Suspicious Object Hub Control Manager:

   - **Service URL**
   - **API key**
7. Click **Register**.

   A confirmation dialog appears with a message indicating that the server is properly registered to the Hub Control Manager.
8. Repeat the process for each Suspicious Object Node Control Manager server.
9. To configure the default synchronization interval:

   a. Select a time period from the **Sync every** drop-down.

   b. Click **Save**.

Unregistering a Suspicious Object Node from the Hub Control Manager

Note

After unregistering a Node Control Manager server, all previously synchronized objects remain in the Node Control Manager server suspicious object lists.

Procedure

1. Log on to the Suspicious Object Node Control Manager server console.

2. Go to **Administration** > **Suspicious Objects** > **Distribution Settings**.
3. In the **Hub Control Manager Settings** section, click **Unregister**.

   A confirmation dialog appears with a message indicating that the server is properly unregistered from the Hub Control Manager.
4. If you are completely stopping the Suspicious Object Hub and Node deployment, repeat the process for each Suspicious Object Node Control Manager server.

Configuration Notes

After successfully setting up the Suspicious Object Hub and registering the Suspicious Object Node Control Manager servers, note the following configuration information.

Note

After unregistering a Node Control Manager server, all previously synchronized objects remain in the Node Control Manager server suspicious object lists.

CONFIGURATION	HUB CONTROL MANAGER	NODE CONTROL MANAGER
Synchronization interval	N/A	5 minutes (default)

<table>
<tr><th>CONFIGURATION</th><th>HUB CONTROL MANAGER</th><th>NODE CONTROL MANAGER</th></tr>
<tr><td rowspan="2">Suspicious Object list synchronization</td><td>From the Hub Control Manager to Nodes:
Virtual Analyzer list
User-Defined list</td><td>From a Node Control Manager to the Hub:
Virtual Analyzer list</td></tr>
<tr><td colspan="2">Note
The Hub Control Manager server does not send data from the Notes column of the User-Defined list or the Exception list to the Node Control Manager servers.
When synchronizing lists, the User-Defined list has a higher priority than the Virtual Analyzer list.
If an object is added to both the User-Defined list and the Virtual Analyzer list on the Hub Control Manager before the next synchronization, the Hub Control Manager server deploys both lists to the Node Control Manager servers.
If an object in the Node Control Manager Virtual Analyzer list also exists in the Hub Control Manager User-Defined list, the suspicious object risk level changes to “High” on the Node Control Manager Virtual Analyzer list during the next synchronization.
Automatic synchronization of the Exception list from a migrated Control Manager 6.0 installation requires enabling Suspicious Object Hub and Node Control Manager architecture on the Control Manager 6.0 server prior to migration.
The Control Manager 7.0 installation preserves the Suspicious Object Hub and Node architecture from the migrated Control Manager 6.0 installation.
To enable Suspicious Object Hub and Node Control Manager architecture on the Control Manager 6.0 server before migration, locate the <code>m_iTmcmSoDist_ForceSyncWhitelist</code> tag in the <code>SystemConfiguration.xml</code> file and change the value to “1”.</td></tr>
</table>

CONFIGURATION	HUB CONTROL MANAGER	NODE CONTROL MANAGER
Configuring Suspicious Object settings	Recommended Configuring Suspicious Objects through the Hub Control Manager ensures consistency across the registered Node Control Manager servers.	Not recommended **Important** To ensure that all the suspicious object lists on the Node Control Manager servers remain synchronized, do not perform any actions (for example, **Add** or **Expire** objects) on suspicious object lists through the Node Control Manager server consoles.

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: CMEM78079/171019