6.0

TREND MICRO™

Control Manager

Service Pack 3

Connected Threat Defense Primer

Centralized Security Management for the Enterprise

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

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

Document Part No.: CMEM66976/150527

Release Date: July 2015

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

The user documentation for Trend Micro Control Manager introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's website.

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.

Please evaluate this documentation on the following site:

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

About Connected Threat Defense

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.

Learn more:

Connected Threat Defense product integration

Suspicious Objects and IOC Files

Targeted attacks and advanced threats are designed to breach your network by evading existing security defenses.

Control Manager facilitates the investigation of targeted attacks and advanced threats using:

- **Suspicious objects**: Files, IP addresses, domains, or URLs that have the potential to expose systems to danger or loss
- **IOC files**: Describe Indicators of Compromise (IOC) identified on a host or network. IOC files help administrators and investigators analyze and interpret threat data in a consistent manner.

Learn more:

- *Suspicious object management and handling process*
- *IOC management*

Endpoint Isolation

You can isolate at-risk endpoints to run an investigation and resolve security issues.

Learn more:

Endpoint isolation

Enhanced Security Threat Monitoring

Use the following widgets on the **Summary** tab to monitor security across the network and respond to the most critical threats:

- Critical Threats
- Users with Threats
- Endpoints with Threats

These widgets provide links to a Security Threats screen. This screen plots threats (by **user** or **endpoint**) over a period of time.

From the Security Threats screen, you can focus your attention on a particular threat to see if it has recently **affected** other users and endpoints. Initiate **impact assessment** to see if the same threat has affected more users and endpoints over an extended period of time.

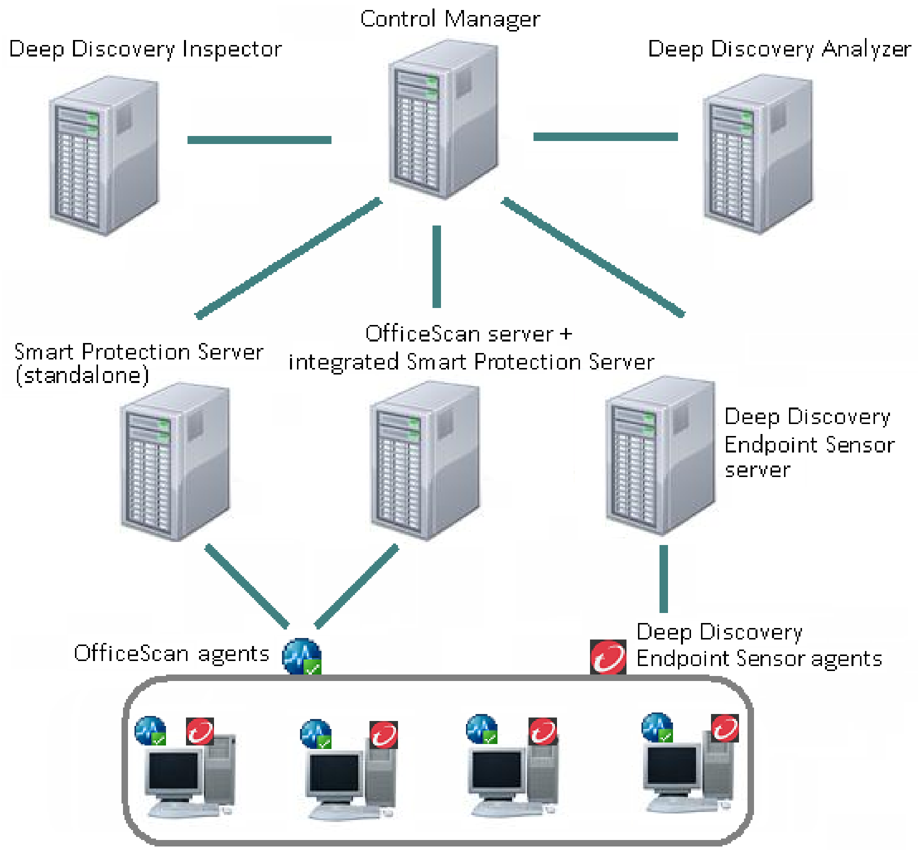
These holistic views allow you to see an enterprise-wide chain of events that may lead to an attack, including at-risk endpoints used to prepare for or carry out the attack.

Learn more:

- *Security Threats screen (User)*
- *Security Threats screen (Endpoint)*
- *Affected Users screen*
- *Impact assessment*

Connected Threat Defense Product Integration

ℹ **Main Products** Connected Threat Defense requires the following Trend Micro products: • Control Manager • Deep Discovery Inspector • OfficeScan • Smart Protection Server (standalone) or integrated with OfficeScan	ℹ **Other Supported Products** The following Trend Micro products can also be integrated to Control Manager for Connected Threat Defense: • Deep Discovery Endpoint Sensor • Deep Discovery Analyzer


Control Manager
Deep Discovery Inspector
Deep Discovery Analyzer
Smart Protection Server (standalone)
OfficeScan server + integrated Smart Protection Server
Deep Discovery Endpoint Sensor server
OfficeScan agents
Deep Discovery Endpoint Sensor agents

The role of each product in the Connected Threat Defense strategy is discussed in detail in *Suspicious Object Management and Handling Process on page 10* and *IOC Management on page 18*.

Install these products and register them to Control Manager. The following tables list the references and resources to help you install and register the products.

Important

Register Deep Discovery Inspector and/or Deep Discovery Analyzer **before** registering OfficeScan. If OfficeScan is registered first, it will not be able to obtain suspicious objects from the Deep Discovery products.

Control Manager	
Minimum version	6.0 SP3
Installation	References: • Installation Guide for version 6.0 to install the product • Readme for the service pack to install the service pack http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

Control Manager Information	Some managed products require the following Control Manager information: - **Host name** (preferably FQDN) or **IP address**: Required by Deep Discovery Inspector and OfficeScan for registration. Registration is performed on these products' console. **Note** Registration for the other Connected Threat Defense products is performed on the Control Manager console. - **API key**: Required by Deep Discovery Inspector, OfficeScan, and Smart Protection Server for suspicious object synchronization Manually deploy the API key to Deep Discovery Inspector 3.8 or later, OfficeScan 11 SP1, and Smart Protection Server 3.0 Patch 1. To obtain the API key, open the Control Manager management console and go to **Administration** > **Suspicious Objects** > **Distribution Settings**. For later versions of OfficeScan and Smart Protection Server, the API key automatically deploys after Control Manager registration, as long as there is one Deep Discovery product already registered to Control Manager.

Deep Discovery Inspector	
Minimum version	3.8
Installation and deployment	References: - Quick Start Card - Installation and Deployment Guide http://docs.trendmicro.com/en-us/enterprise/deep-discovery-inspector.aspx

Registration and suspicious object synchronization	Complete the registration and enable suspicious object synchronization from the Deep Discovery Inspector management console. You can conveniently launch the Deep Discovery Inspector management console from the Managed Servers screen in Control Manager. Registration and synchronization instructions: http://docs.trendmicro.com/all/ent/ddi/v3.8/en-us/ddi_3.8_olh/admin_int-prods-srvcs_tmcm_register.html

Deep Discovery Analyzer	
Minimum version	5.1
Installation and deployment	References: • Quick Start Card • Installation and Upgrade Guide http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx
Registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** and select Deep Discovery Analyzer from the list of products.

OfficeScan	
Minimum version	11 SP1

Installation	References: • Installation and Upgrade Guide for version 11 to install the server program • Readme for the service pack to install the service pack to the server • Online Help or Administrator's Guide for version 11 or later to install agents and use the integrated Smart Protection Server http://docs.trendmicro.com/en-us/enterprise/officescan.aspx
Registration and suspicious object synchronization	Before registering OfficeScan, be sure that you have registered at least one Deep Discovery product to Control Manager. Complete the registration and enable suspicious object synchronization from the OfficeScan server web console. You can conveniently launch the OfficeScan server web console from the Managed Servers screen in Control Manager. • Registration instructions: http://docs.trendmicro.com/en-us/enterprise/officescan-110-sp1-server/managing-the-product/osce-company_name-co/osce-registering-pro.aspx • Synchronization instructions (OfficeScan 11 SP1 only): http://docs.trendmicro.com/en-us/enterprise/officescan-110-sp1-server/managing-the-product/suspicious-objects-c/configuring-suspicio.aspx **Note** Later OfficeScan versions or non-English releases of OfficeScan 11 SP1 have been enhanced to automatically synchronize suspicious objects with Control Manager after registration.

Smart Protection Server (Standalone)	
Minimum version	3.0 Patch 1

Installation	References: - Installation and Upgrade Guide for version 3.0 to install the product - Readme for the patch to install the patch http://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx
Suspicious object synchronization	Synchronization instructions (Smart Protection Server 3.0 Patch 1 only): http://docs.trendmicro.com/all/ent/sps/v3.0p1/en-us/sps_3.0p1_olh/using_smart_prot_ccca_configure.html **Note** Only Smart Protection Server versions later than 3.0 Patch 1 support registration with Control Manager. After the registration is complete, Smart Protection Server automatically synchronizes suspicious objects with Control Manager.

Deep Discovery Endpoint Sensor	
Minimum version	1.5 (Preview Release)
Installation	Reference: Installation Guide (for server and agent installation instructions) http://docs.trendmicro.com/en-us/enterprise/deep-discovery-endpoint-sensor.aspx
Registration	Complete the registration from the Control Manager management console. Go to **Administration** > **Managed Servers** and select Deep Discovery Endpoint Sensor from the list of products.

Suspicious Object Management and Handling Process

The suspicious object handling process can be broken down into the following phases:

1

Sample Submission

Virtual Analyzer built into the following managed products processes submitted samples:

- **Deep Discovery Inspector 3.8**: Uses administrator-configured file submission rules to determine the samples to submit to its Virtual Analyzer
- **Deep Discovery Analyzer 5.1**: Receives samples uploaded by product administrators or sent by other Trend Micro products

2

Analysis

Virtual Analyzer in managed products tracks and analyzes submitted samples. Virtual Analyzer flags **suspicious objects** based on their potential to expose systems to danger or loss. Supported objects include files (SHA-1 hash values), IP addresses, domains, and URLs.

3

Distribution

Control Manager consolidates suspicious objects and scan actions against the objects and then distributes them to other products.

3.1. Virtual Analyzer Suspicious Objects

Managed products with Virtual Analyzer send a list of suspicious objects to Control Manager.

Control Manager displays suspicious objects in **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**, in the **Objects** tab.

3.2. Exceptions to Virtual Analyzer Suspicious Objects

From the list of Virtual Analyzer suspicious objects (**Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**), Control Manager administrators can select objects that are considered safe and then add them to an exception list.

The exception list displays in the **Exceptions** tab next to the **Objects** tab.

Control Manager sends the exception list back to the managed products with Virtual Analyzer. If a suspicious object from a managed product matches an object in the exception list, the product no longer sends it to Control Manager.

3.3. 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**.

3.4. Suspicious Object Distribution

Control Manager consolidates Virtual Analyzer and user-defined suspicious objects (excluding exceptions) and sends them to certain managed products. These products synchronize and use all or some of these objects.

The following are the supported managed products and the required minimum versions:

- **Deep Discovery Inspector 3.8**: Expands its list of **suspicious objects** to include user-defined objects and those detected by other Deep Discovery products
- **OfficeScan 11 SP1**: Searches for suspicious **files**, **IP addresses**, and **URLs** during routine scans
- **Smart Protection Server 3.0 Patch 1 (standalone) or integrated with OfficeScan 11 SP1**: Relays **suspicious URL** information to Trend Micro products (such as OfficeScan agents, ScanMail, and Deep Security) that send Web Reputation queries

3.5. Scan Actions

Configure scan actions (log, block, or quarantine) against suspicious objects that affect endpoints.

Block and quarantine are considered "active" actions, while "log" is considered "passive". If products take an active action, Control Manager declares the affected endpoints as **mitigated**. If the action is passive, endpoints are declared **at risk**.

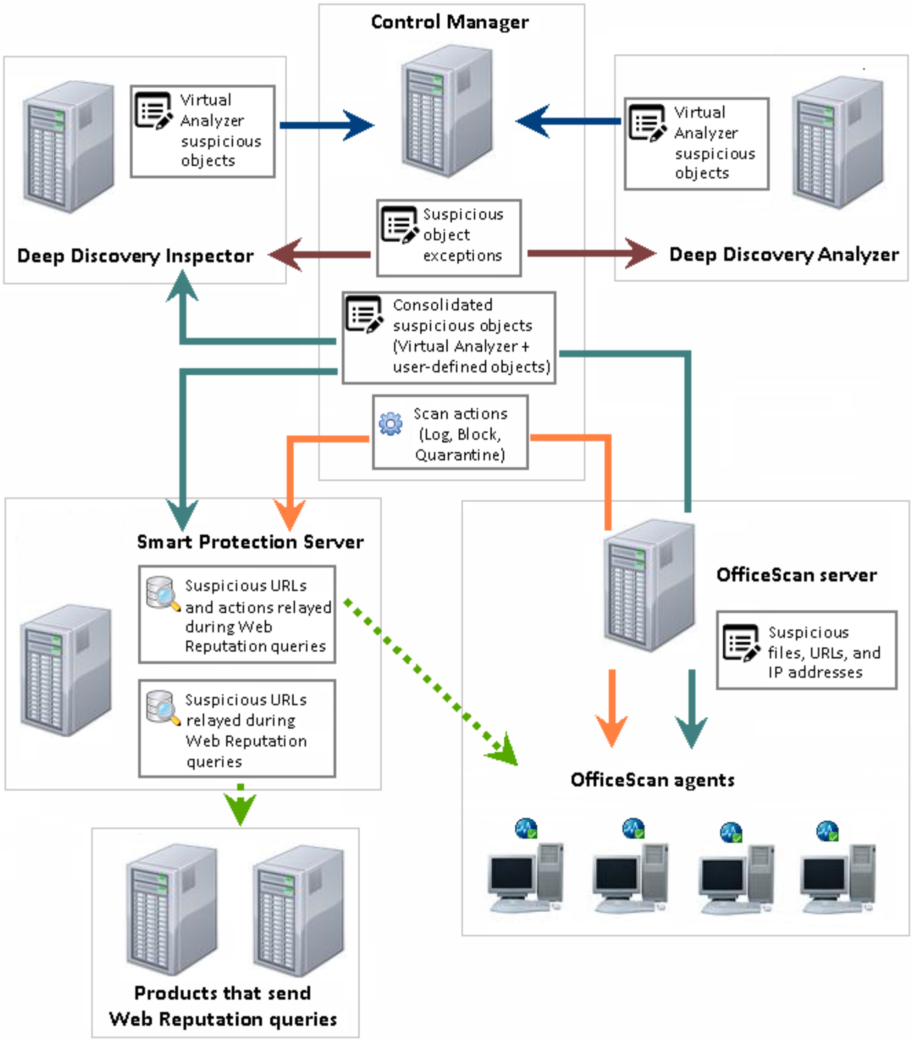
Scan actions are configured separately for Virtual Analyzer and user-defined suspicious objects.

- **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**
- **Administration** > **Suspicious Objects** > **User-Defined Objects**

Control Manager automatically deploys the actions to certain managed products.

The following are the supported managed products and the required minimum versions:

- **OfficeScan 11 SP1**: Performs actions against Virtual Analyzer suspicious **files**, **IP addresses**, and **URLs** (actions against user-defined objects are not supported)
- **Smart Protection Server 3.0 Patch 1 (standalone) or integrated with OfficeScan 11 SP1**: Relays actions against suspicious URLs to OfficeScan agents that send Web Reputation queries.

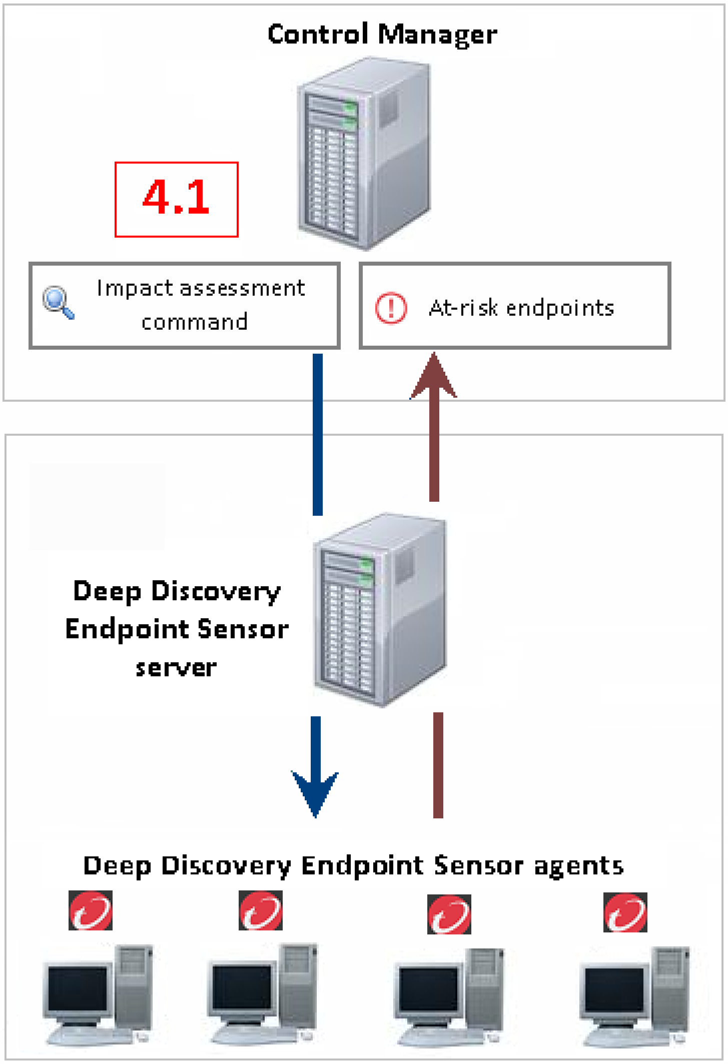

Control Manager
Virtual Analyzer suspicious objects
Virtual Analyzer suspicious objects
Suspicious object exceptions
Deep Discovery Inspector
Deep Discovery Analyzer
Consolidated suspicious objects (Virtual Analyzer + user-defined objects)
Scan actions (Log, Block, Quarantine)
Smart Protection Server
Suspicious URLs and actions relayed during Web Reputation queries
Suspicious URLs relayed during Web Reputation queries
OfficeScan server
Suspicious files, URLs, and IP addresses
OfficeScan agents
Products that send Web Reputation queries

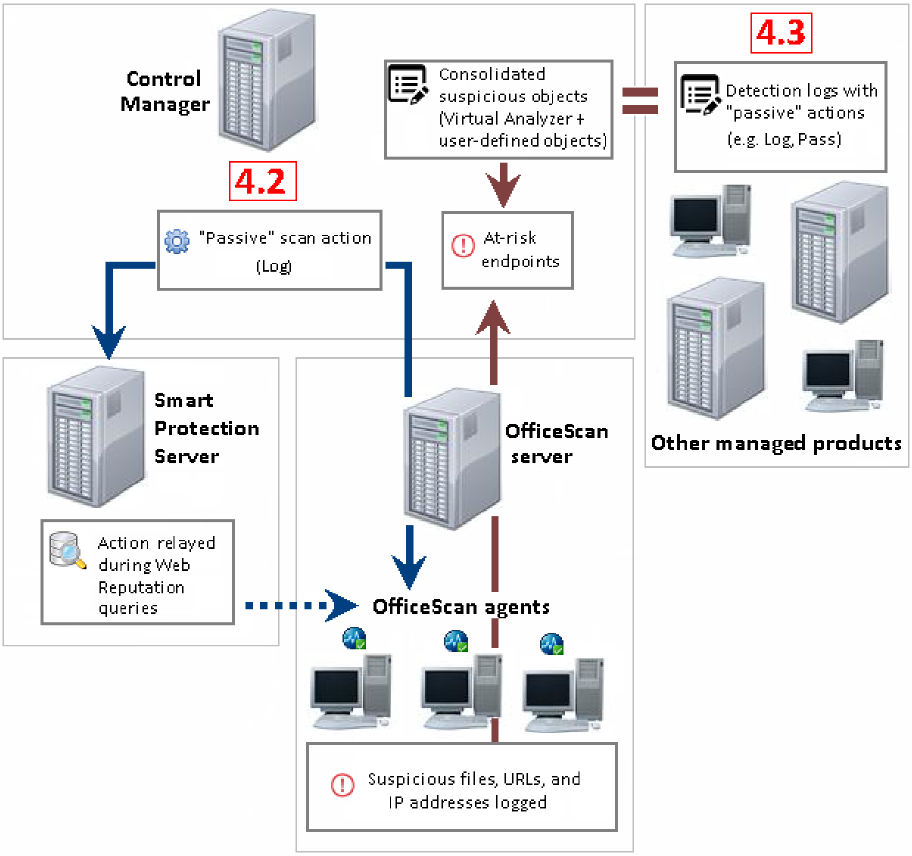
Impact Assessment

Impact assessment checks endpoints for suspicious activities associated with suspicious objects. Endpoints with confirmed suspicious activities are considered **at risk**.

Control Manager also considers endpoints to be at risk if products take "passive" actions against suspicious objects.

4.1. Impact Assessment From the list of Virtual Analyzer suspicious objects in **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**, run impact assessment to determine at-risk endpoints. Impact assessment requires **Deep Discovery Endpoint Sensor**. The minimum required version is **1.5**. This product only performs assessment and does not take action on at-risk endpoints.	**4.3. Detection Matching** Control Manager also checks Web Reputation, URL filtering, network content inspection, and rule-based detection logs received from all managed products and then compares them with its list of suspicious objects. If there is a match from a specific endpoint and the managed product takes a "passive" action (such as Log, Pass, or Warn and Continue), the endpoint is also considered at risk.
4.2. "Passive" Scan Action When the scan action configured in Control Manager and deployed to OfficeScan agents is "passive" (log), the affected endpoints are considered at risk.	**At-risk Endpoints** To view the number of at-risk endpoints, go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects** and see the **At Risk Endpoints** column. To view detailed information for at-risk endpoints, go to the **Object** column and click the arrow icon (if available) before the suspicious object name. The screen expands to show a table with details about the suspicious object and at-risk endpoints.


Control Manager
4.1
Impact assessment command
At-risk endpoints
Deep Discovery Endpoint Sensor server
Deep Discovery Endpoint Sensor agents


Control Manager
4.2
"Passive" scan action (Log)
Consolidated suspicious objects (Virtual Analyzer + user-defined objects)
At-risk endpoints
4.3
Detection logs with "passive" actions (e.g. Log, Pass)
Other managed products
Smart Protection Server
Action relayed during Web Reputation queries
OfficeScan server
OfficeScan agents
Suspicious files, URLs, and IP addresses logged

5

Mitigation

The OfficeScan agent and other managed products perform "active" scan actions against suspicious objects.

5.1. Control Manager Scan Actions

When you deploy an "active" scan action (Block or Quarantine) from Control Manager to OfficeScan agents, the threats to the affected endpoints are considered mitigated.

5.2. Managed Product Scan Actions

Managed products can perform product-specific scan actions (such as Block, Delete, Quarantine, or Block with override) on detected threats. If Control Manager matches a suspicious object in the logs (Web Reputation, URL filtering, network content inspection, and rule-based detection) of any managed product, a threat assessment is performed. Control Manager considers all threats to endpoints as mitigated if the managed product took an "active" action on the suspicious object.

Note

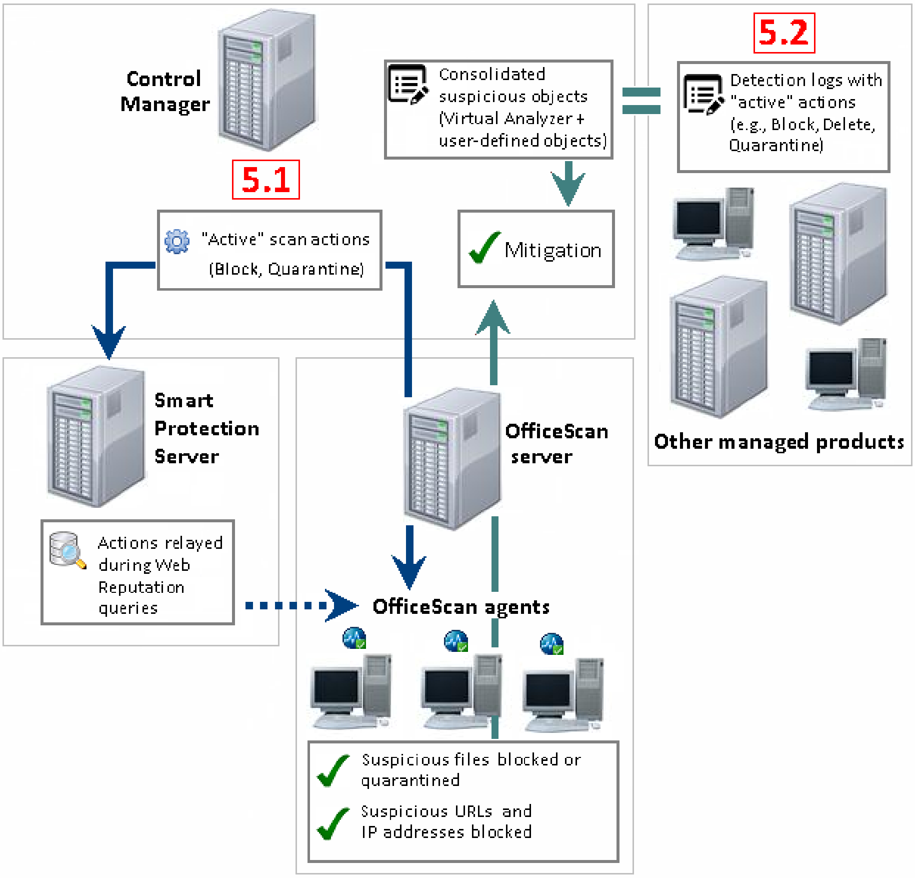
Refer to your managed products' Administrator's Guides for more information about the types of actions that specific products can take on detected threats.

Endpoint Isolation

An alternative action is isolating at-risk endpoints. Perform this action if you need to perform a detailed investigation.

Only endpoints with **OfficeScan agents** can be isolated. The minimum required version is **11 SP1**. The agents' firewall must be enabled.

For more information, see *Endpoint Isolation and Connection Restoration on page 33*.


Control Manager
5.1
Consolidated suspicious objects (Virtual Analyzer + user-defined objects)
=
5.2
Detection logs with "active" actions (e.g., Block, Delete, Quarantine)
"Active" scan actions (Block, Quarantine)
Mitigation
Other managed products
Smart Protection Server
Actions relayed during Web Reputation queries
OfficeScan server
OfficeScan agents
Suspicious files blocked or quarantined
Suspicious URLs and IP addresses blocked

IOC Management

Managing IOCs (Indicators of Compromise) involves the following tasks:

1

IOC File Generation

Obtain IOC files from your peers and other security experts. Open the Control Manager management console and go to **Administration** > **Indicators of Compromise** to add the IOC files.

If, for some reason, a suspicious object from Deep Discovery Analyzer 5.1 or Deep Discovery Inspector 3.8 does not display in the Virtual Analyzer Suspicious Objects screen (**Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**), download the corresponding suspicious object investigation package from the managed product's console. This investigation package (available as a single compressed file), contains IOC-compliant files and other investigation resources.

As Control Manager only requires IOC files for impact assessment, extract the .ioc files from the compressed file and then add them to Control Manager. It is not possible to add the compressed file.

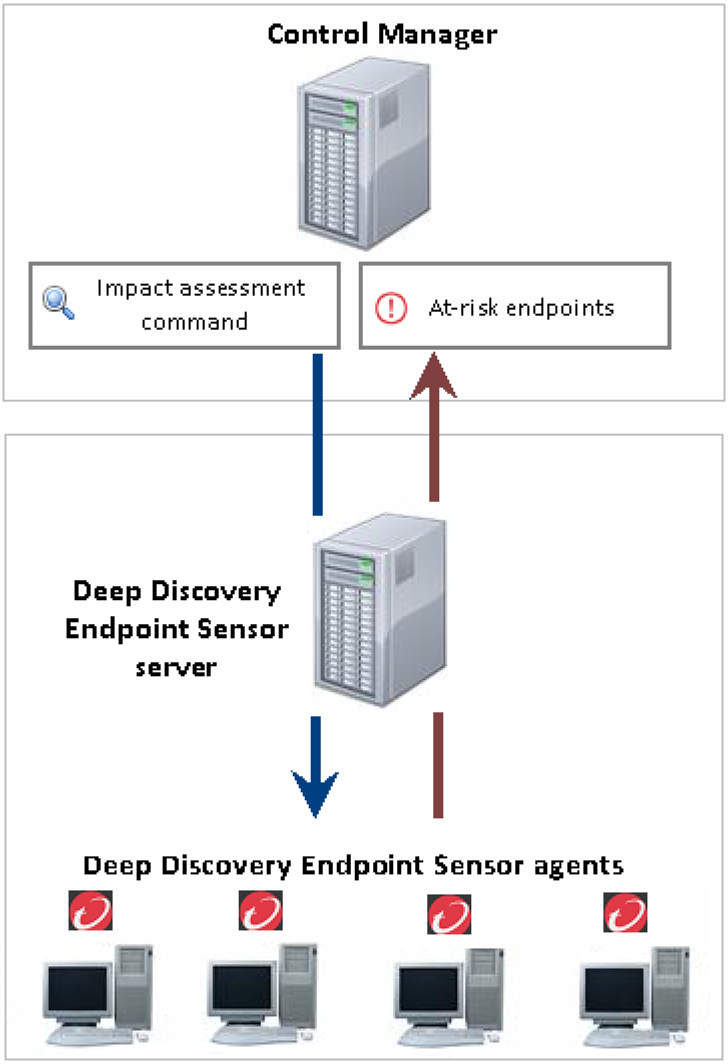
Important

After extracting and adding the .ioc files, delete the compressed file from the computer as it contains potentially malicious files.

2

Impact Assessment

Initiate impact assessment to check for suspicious activities based on the indicators listed in the IOC files. Endpoints with suspicious activities are considered **at risk**.


Control Manager
Impact assessment command
At-risk endpoints
Deep Discovery Endpoint Sensor server
Deep Discovery Endpoint Sensor agents

Go to **Administration** > **Indicators of Compromise** and run an impact assessment on one or several IOC files to determine at-risk endpoints.

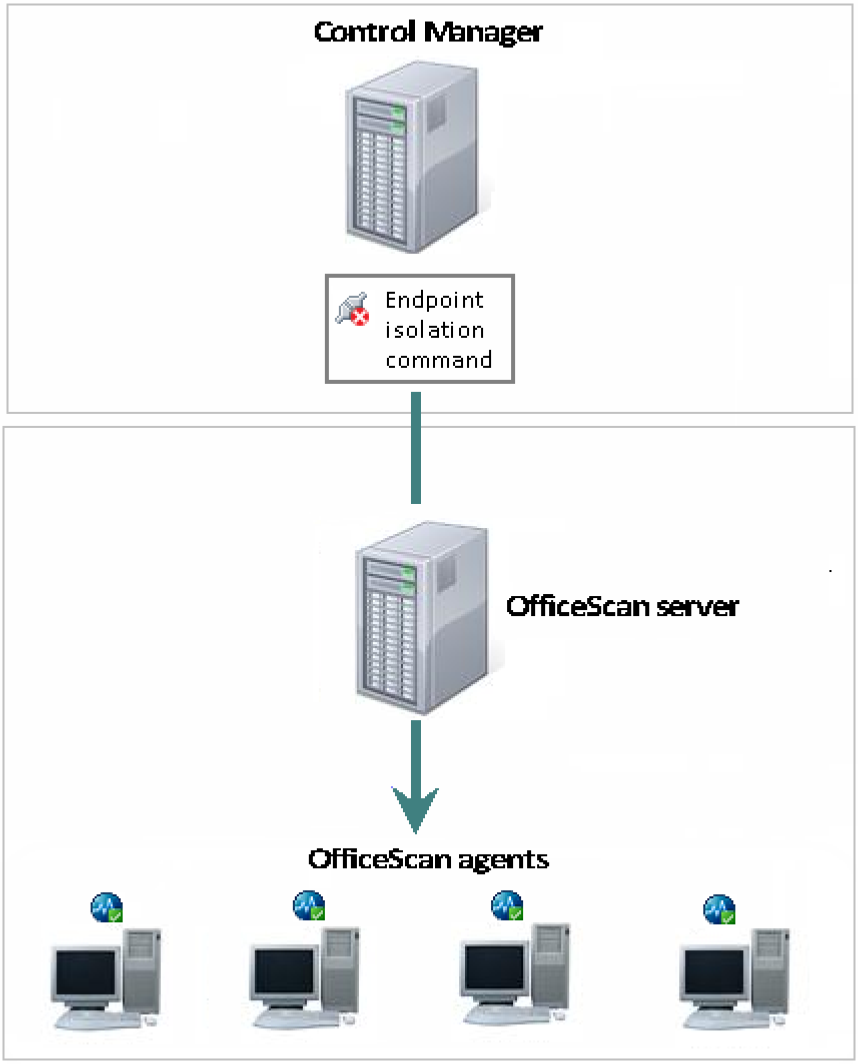
Impact assessment requires **Deep Discovery Endpoint Sensor** . The minimum required version is **1.5**.

This product only performs assessment and does not take action on at-risk endpoints.

3

Endpoint Isolation

Isolate an affected endpoint to perform a detailed investigation. To perform this task, navigate to **Administration** > **Indicators of Compromise**, go to the **At Risk** column and click a number representing the number of at-risk endpoints.



Only endpoints with **OfficeScan agents** can be isolated. The minimum required version is **11 SP1**. The agents' firewall must be enabled.

For more information, see *Endpoint Isolation and Connection Restoration on page 33*.

Enhanced Security Threat Monitoring

Use the following widgets on the **Summary** tab to monitor security across the network and respond to the most critical threats:

- Critical Threats
- Users with Threats
- Endpoints with Threats

These widgets provide links to a Security Threats screen. This screen plots threats (by **user** or **endpoint**) over a period of time.

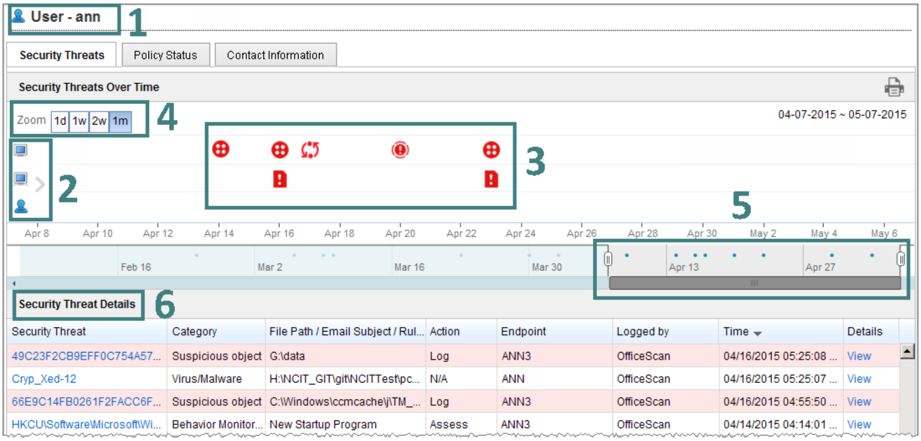
From the Security Threats screen, you can focus your attention on a particular threat to see if it has recently **affected** other users and endpoints. Initiate **impact assessment** to see if the same threat has affected more users and endpoints over an extended period of time.

These holistic views allow you to see an enterprise-wide chain of events that may lead to an attack, including at-risk endpoints used to prepare for or carry out the attack.

Security Threats (User)

View security threats detected on all endpoints owned by a user.

There are several ways to access this screen. The recommended way is to go to the **Users with Threats** widget on the dashboard and click a value representing the number of threats detected on all the endpoints owned by a user.



Security Threat	Category	File Path / Email Subject / Rul...	Action	Endpoint	Logged by	Time	Details
49C23F2CB9EFF0C754A57...	Suspicious object	G:\data	Log	ANN3	OfficeScan	04/16/2015 05:25:08 ...	View
Cryp_Xed-12	Virus/Malware	H:\NCIT_GIT\git\NCITTest\pc...	N/A	ANN	OfficeScan	04/16/2015 05:25:07 ...	View
66E9C14FB0261F2FACC6F...	Suspicious object	C:\Windows\ccmcache\j\TM_...	Log	ANN3	OfficeScan	04/16/2015 04:55:50 ...	View
HKCU\Software\Microsoft\Wi...	Behavior Monitor...	New Startup Program	Assess	ANN3	OfficeScan	04/14/2015 04:14:01 ...	View

The major user interface elements in the screen are as follows:

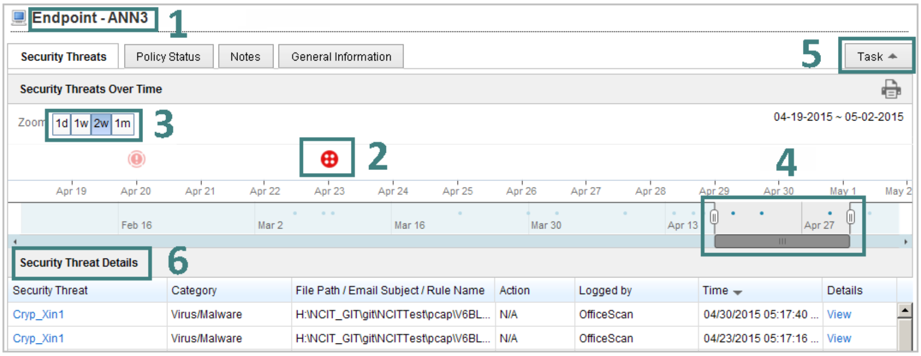
Number	Description
1	User with endpoints that have security threats
2	Endpoints that the user owns (represented by a monitor icon) and the user (represented by a person icon) By default, the host name of an endpoint and the domain name of the user display next to the icons. Click the gray arrow to show or hide the host and domain names.

<table>
<tr><th>Number</th><th colspan="3">Description</th></tr>
<tr><td rowspan="6">3</td><td colspan="3">Security threats detected on the endpoints, represented by icons
Mouseover an icon to view threat details.</td></tr>
<tr><td>Application violation</td><td>Behavior Monitoring violation</td><td>C&C callback</td></tr>
<tr><td>DLP incident</td><td>Content violation</td><td>Firewall violation</td></tr>
<tr><td>Intrusion Prevention event</td><td>Network content violation</td><td>Phishing email</td></tr>
<tr><td>Spam</td><td>Spyware/Grayware</td><td>Suspicious object</td></tr>
<tr><td>Virus/Malware</td><td>Web violation</td><td>Multiple events</td></tr>
<tr><td>4 and 5</td><td colspan="3">Filter used for controlling the number of detected security threats within a certain time range</td></tr>
<tr><td>6</td><td colspan="3">Table with details about the security threats
Critical threats are shaded light red for easy recognition.
To display details, do one of the following:
• Click a value in the **Security Threat** column to view *users affected by the threat*.
• Click a value in the **Details** column to view a log entry.</td></tr>
</table>

Security Threats (Endpoint)

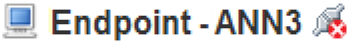
View security threats detected on a particular endpoint.

There are several ways to access this screen. The recommended way is to go to the **Endpoints with Threats** widget on the dashboard and click a value representing the number of threats detected on an endpoint.



Security Threat	Category	File Path / Email Subject / Rule Name	Action	Logged by	Time	Details
Cryp_Xin1	Virus/Malware	H:\NCIT_GIT\git\NCITTest\pcap\V6BL...	N/A	OfficeScan	04/30/2015 05:17:40 ...	View
Cryp_Xin1	Virus/Malware	H:\NCIT_GIT\git\NCITTest\pcap\V6BL...	N/A	OfficeScan	04/23/2015 05:17:16 ...	View

The major user interface elements in the screen are as follows:

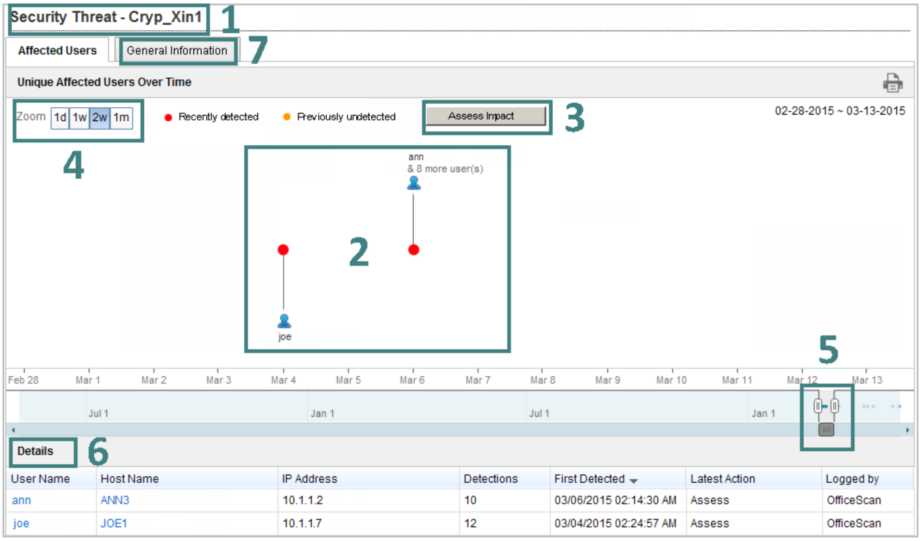
Number	Description
1	Endpoint with security threats An icon displays after the endpoint name (as shown below) if Control Manager has *isolated* the endpoint or is in the process of restoring its network connection.  Endpoint - ANN3

<table>
<tr><th>NUMBER</th><th colspan="3">DESCRIPTION</th></tr>
<tr><td rowspan="6">2</td><td colspan="3">Security threats detected on the endpoints, represented by icons
Mouseover an icon to view threat details.</td></tr>
<tr><td>Application violation</td><td>Behavior Monitoring violation</td><td>C&C callback</td></tr>
<tr><td>DLP incident</td><td>Content violation</td><td>Firewall violation</td></tr>
<tr><td>Intrusion Prevention event</td><td>Network content violation</td><td>Phishing email</td></tr>
<tr><td>Spam</td><td>Spyware/Grayware</td><td>Suspicious object</td></tr>
<tr><td>Virus/Malware</td><td>Web violation</td><td>Multiple events</td></tr>
<tr><td>3 and 4</td><td colspan="3">Filter used for controlling the number of detected security threats within a certain time range</td></tr>
<tr><td>5</td><td colspan="3">The following tasks that can be performed on the endpoint:
• Assign tags
• <i>Isolate endpoint</i></td></tr>
</table>

Number	Description
6	Table with details about the security threats Critical threats are shaded light red for easy recognition. To display details, do one of the following: • Click a value in the **Security Threat** column to view *users affected by the threat*. • Click a value in the **Details** column to view a log entry.

Affected Users

Clicking a threat name in the *Security Threats (User)* or *Security Threats (Endpoint)* screen opens the Affected Users screen displaying a list of unique users affected by the threat.



User Name	Host Name	IP Address	Detections	First Detected	Latest Action	Logged by
ann	ANN3	10.1.1.2	10	03/06/2015 02:14:30 AM	Assess	OfficeScan
joe	JOE1	10.1.1.7	12	03/04/2015 02:24:57 AM	Assess	OfficeScan

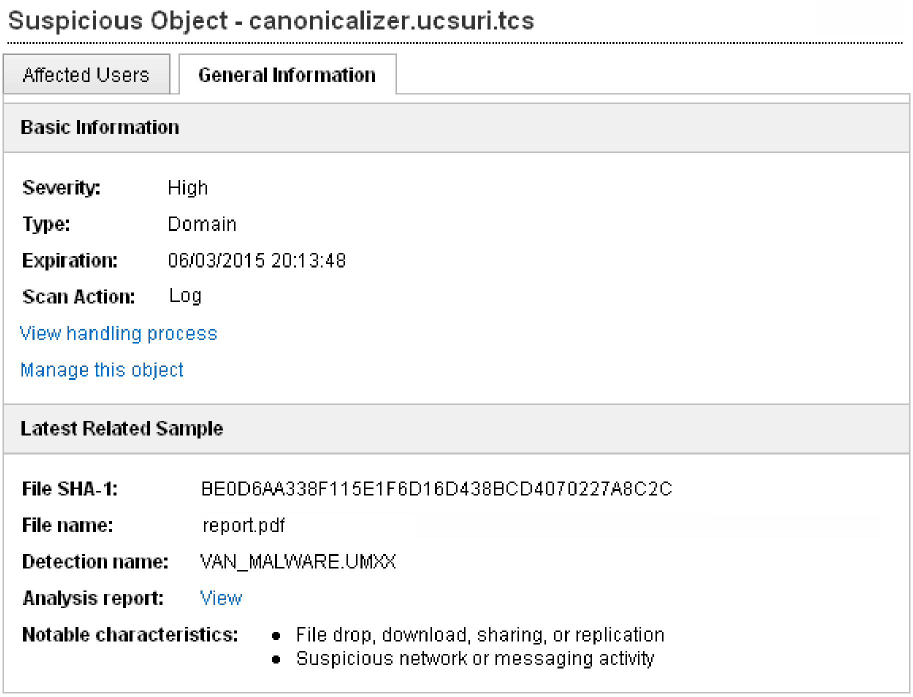
The major user interface elements in the screen are as follows:

Number	Description
1	Security threat affecting one or several users
2	Affected users and the nature of detection (**Recently detected** or **Previously undetected**), represented by icons The nature of a detection is represented by a specific color. Refer to the legend before the **Assess Impact** button to see what each color represents. If a user has detections similar to others users, a number displays below the user name. Mouseover the user name to view all affected users.
3	Button for initiating impact assessment on security threats Impact assessment on security threats requires **Deep Discovery Endpoint Sensor** and **Deep Discovery Inspector**. Both these products use *Retro Scan* to perform the assessment. If only one of these products is registered to Control Manager, a partial impact assessment will be performed. After the assessment, the graph will be updated with a list of previously undetected threats. These are stealthy and sophisticated threats that have previously evaded detection.
4 and 5	Time filter used for controlling the number of affected users shown
6	Table with details about affected users Click a value in the **User Name** or **Host Name** column to view *security threats on the user's endpoint*.
7	Tab with *general information* about the security threat

General Information for Security Threats

View information about a particular security threat.

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



Suspicious Object - canonicalizer.ucsuri.tcs

Basic Information

Severity: High

Type: Domain

Expiration: 06/03/2015 20:13:48

Scan Action: Log

Latest Related Sample

File SHA-1: BE0D6AA338F115E1F6D16D438BCD4070227A8C2C

File name: report.pdf

Detection name: VAN_MALWARE.UMXX

Analysis report: View

Notable characteristics:

- File drop, download, sharing, or replication
- Suspicious network or messaging activity

Impact Assessment

There are several ways to initiate impact assessment.

Impact Assessment on Suspicious Objects

Initiate impact assessment to check for suspicious activities associated with suspicious objects. Endpoints with suspicious activities are considered **at risk**.

Impact assessment on suspicious objects requires a Trend Micro product called **Deep Discovery Endpoint Sensor**.

To initiate the assessment, go to **Administration** > **Suspicious Objects** > **Virtual Analyzer Objects**.

Impact Assessment on IOC files

Initiate impact assessment to check for suspicious activities based on the indicators listed in the IOC files. Endpoints with suspicious activities are considered **at risk**.

Impact assessment on IOC files requires a Trend Micro product called **Deep Discovery Endpoint Sensor**.

To initiate the assessment, go to **Administration** > **Indicators of Compromise**.

Impact Assessment on Security Threats

Initiate impact assessment on security threats to check which endpoints they affect. This is especially useful for checking stealthy and sophisticated threats that have previously evaded detection.

Impact assessment on security threats requires both **Deep Discovery Endpoint Sensor** and **Deep Discovery Inspector**. These products use **Retro Scan** to perform the assessment.

If only one of these products is registered to Control Manager, a partial impact assessment will be performed.

To initiate the assessment:

1. Go to the *Security Threats (User)* or *Security Threats (Endpoint)* screen.
2. Click a threat name. This opens the *Affected Users* screen, with the **Assess Impact** option.

Learn more:

Retro Scan

Retro Scan

Retro Scan in Deep Discovery Inspector

Retro Scan is a cloud-based service that scans historical web access logs for callback attempts to C&C servers and other related activities in your network. Web access logs may include undetected and unblocked connections to C&C servers that have only recently been discovered. Examination of such logs is an important part of forensic investigations to determine if your network is affected by attacks.

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

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

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

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

Important

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

Retro Scan in Deep Discovery 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 folder

- 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.

Endpoint Isolation and Connection Restoration

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

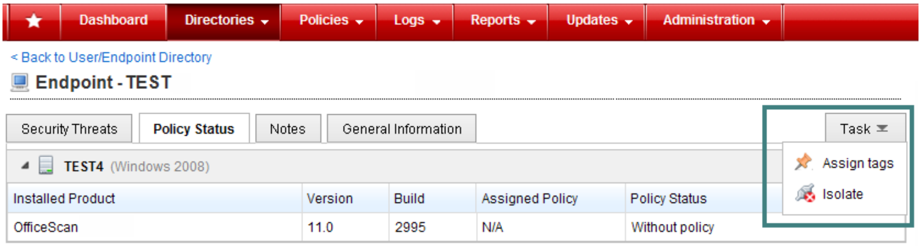
Endpoint isolation and connection restoration require the **OfficeScan agent**. The minimum required version is **11 SP1**. In addition, the OfficeScan agent's **firewall** must be enabled.

1

Initiating Endpoint Isolation

The **Isolate** option is available from the following screens:

1.1. Endpoint screen



TEST4 (Windows 2008)

Installed Product	Version	Build	Assigned Policy	Policy Status
OfficeScan	11.0	2995	N/A	Without policy

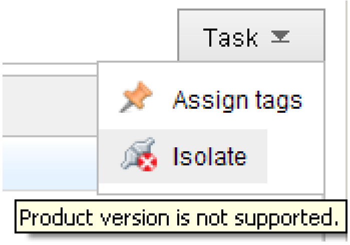
Note

All the tabs in the Endpoint screen provide the **Isolate** option.

There are several ways to access this screen. The recommended way is to go to **Directories** > **Users/Endpoints**, use the search feature in the screen to find the endpoint to isolate, and then click the endpoint name when the search results display.

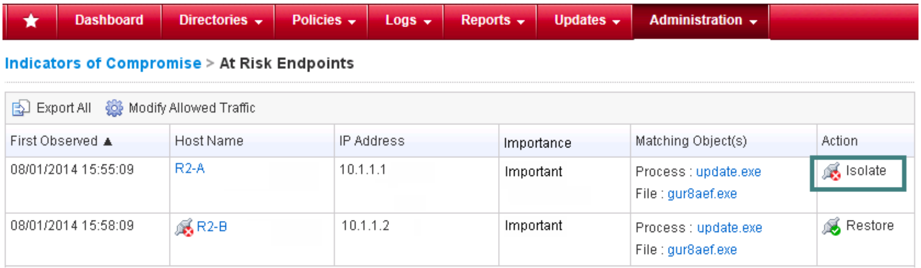
If isolation cannot be performed, a message displays below the **Isolate** option to indicate any of the following issues:

- 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.



Product version is not supported.

1.2. At Risk Endpoints screen



Indicators of Compromise > At Risk Endpoints

First Observed ▲	Host Name	IP Address	Importance	Matching Object(s)	Action
08/01/2014 15:55:09	R2-A	10.1.1.1	Important	Process : update.exe File : gur8aef.exe	Isolate
08/01/2014 15:58:09	R2-B	10.1.1.2	Important	Process : update.exe File : gur8aef.exe	Restore

Note

To access this screen, go to **Administration** > **Indicators of Compromise**, go to the **At Risk** column and click a number representing the number of at-risk endpoints.

2

Monitoring the Isolation Status

While an endpoint is being isolated, a message displays on top of the Endpoint or At Risk Endpoints screen, informing you that endpoint isolation is in progress.

The message disappears when the isolation is complete. On the endpoint, a notification appears to inform the user of the isolation.

If there is an issue, the message changes. Issues include:

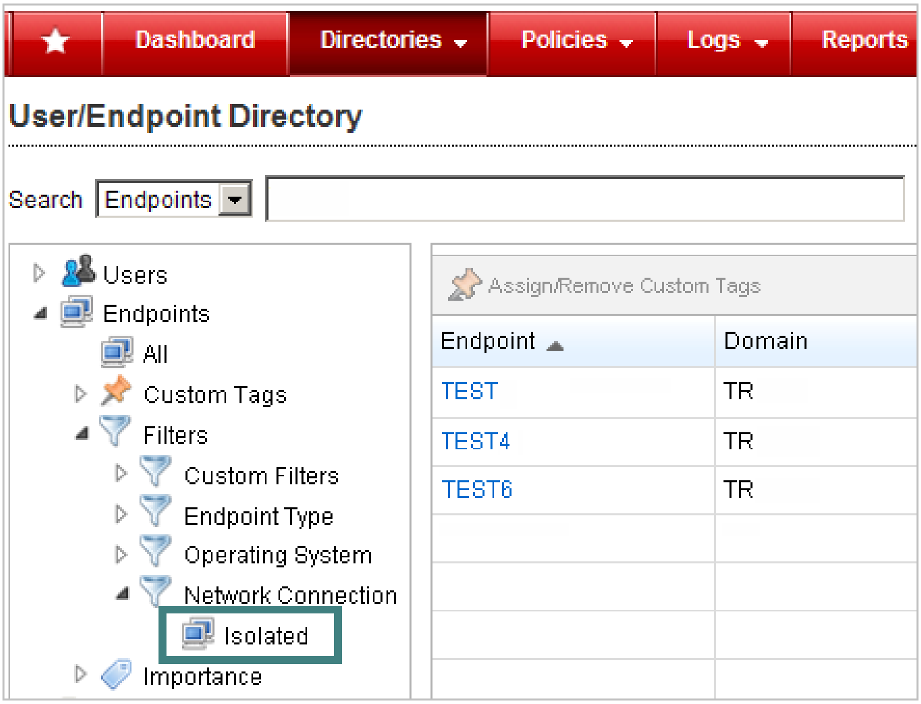
- The OfficeScan agent firewall was disabled by the OfficeScan server administrator or by the user, who has privileges to configure firewall settings. It is also possible that the firewall has become non-functional.
- There is no connection between the OfficeScan agent on the endpoint and its parent server.
- Both the OfficeScan server and agent are installed on the endpoint. Isolating the endpoint will cause disruptions to OfficeScan server functions.
- An unexpected error occurred.

Refresh the screen to get the latest status.

3

Monitoring Isolated Endpoints

A list of isolated endpoints is available in the Endpoint tree, when you select the default filter, **Isolated**.



User/Endpoint Directory

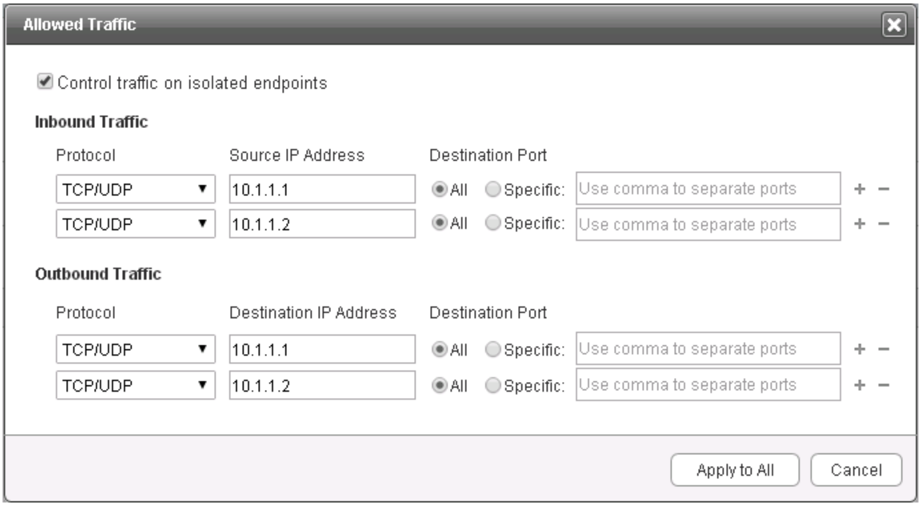
Search: Endpoints

Endpoint	Domain
TEST	TR
TEST4	TR
TEST6	TR

4

Configuring Allowed Traffic

By default, endpoint isolation blocks all inbound and outbound traffic, except traffic between the OfficeScan agent and its parent server.



☑ Control traffic on isolated endpoints

Inbound Traffic

Protocol	Source IP Address	Destination Port	
TCP/UDP	10.1.1.1	● All ○ Specific:	Use comma to separate ports
TCP/UDP	10.1.1.2	● All ○ Specific:	Use comma to separate ports

Outbound Traffic

Protocol	Destination IP Address	Destination Port	
TCP/UDP	10.1.1.1	● All ○ Specific:	Use comma to separate ports
TCP/UDP	10.1.1.2	● All ○ Specific:	Use comma to separate ports

You can configure inbound and outbound traffic that you want to allow on isolated endpoints. These settings apply to **all** isolated endpoints and cannot be configured for individual endpoints.

If other Trend Micro agents are installed on endpoints, be sure to configure allowed traffic so that the agents can continue to communicate with their parent servers.

Agent	Inbound Traffic	Outbound Traffic	Other Requirements
Vulnerability Protection	**Protocol**: TCP **Source IP address**: IP address of the parent server **Destination port**: 4118	**Protocol**: TCP **Destination IP address**: IP address of the parent server **Destination port**: 4120	If the Vulnerability Protection server installs using DNS settings, add the protocol, IP address, and destination ports of the DNS server.

Agent	Inbound Traffic	Outbound Traffic	Other Requirements
Endpoint Encryption	**Protocol**: TCP **Source IP address**: IP address of the parent server **Destination port**: 80, 8080	**Protocol**: TCP **Destination IP address**: IP address of the parent server **Destination port**: 80, 8080	If the Endpoint Encryption server installs using DNS settings, add the protocol, IP address, and destination ports of the DNS server.
Deep Discovery Endpoint Sensor	**Protocol**: TCP **Source IP address**: IP address of the parent server **Destination port**: 8081	**Protocol**: TCP **Destination IP address**: IP address of the parent server **Destination port**: 8002, 8003	DNS settings (inbound): **Protocol**: UDP **Source IP address**: IP address of the DNS server **Destination port**: 53 DNS settings (outbound): **Protocol**: UDP **Destination IP address**: IP address of the DNS server **Destination port**: 53
Endpoint Application Control	**Protocol**: TCP **Source IP address**: IP address of the parent server **Destination port**: 80, 443, 8080, 4343	**Protocol**: TCP **Destination IP address**: IP address of the parent server **Destination port**: 8085, 8443	If the Endpoint Application Control server installs using DNS settings, add the protocol, IP address, and destination ports of the DNS server.

Click **Apply to All** to deploy the settings to OfficeScan servers with agents that have isolated or are in the process of isolating endpoints.

5

Restoring Endpoint Connection

After you are finished with your investigation and have confirmed that the endpoint is threat-free, restore the endpoint's network connection. A **Restore** option is available on the Endpoint screen or At Risk Endpoints screen.

After clicking **Restore**, a message displays on top of the screen, informing you that connection restoration is in progress. The message disappears when the restoration is complete.

If there is an issue, the message changes. Issues include:

- The OfficeScan agent firewall was disabled by the OfficeScan server administrator or by the user, who has privileges to configure firewall settings. It is also possible that the firewall has become non-functional. As a result, network connection was automatically restored but the endpoint remains in the **Isolated** filter in the Control Manager Endpoint tree.

  Enable the firewall on the agent or verify that it is working properly and then initiate endpoint isolation from Control Manager (to keep the endpoint isolated) or connection restoration (to remove the endpoint from the **Isolated** filter in the Endpoint tree).

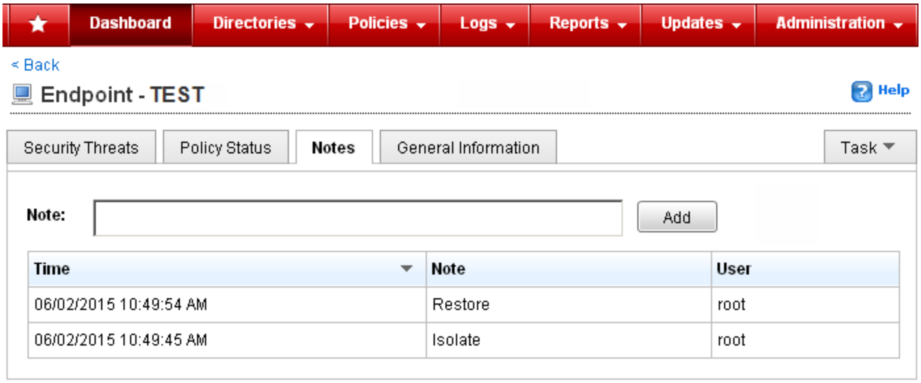
- There is no connection between the OfficeScan agent on the endpoint and its parent server.

- An unexpected error occurred.

Refresh the screen to get the latest status.

Endpoint Isolation and Connection Restoration History

Control Manager keeps a record of all isolation and connection restoration tasks performed on an endpoint. To view these records, go to the Endpoint screen and click the **Notes** tab.



Time	Note	User
06/02/2015 10:49:54 AM	Restore	root
06/02/2015 10:49:45 AM	Isolate	root

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: CMEM66976/150527