TREND MICRO

6.0 TREND MICRO™ Control Manager

Service Pack 3

Administrator's Guide

Centralized Security Management for the Enterprise

Document Part No.: CMEM66957/150518

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

Table of Contents

Preface

Part I: Getting Started

Chapter 1: Introducing Trend Micro Control Manager

Chapter 2: Getting Started with Control Manager

Chapter 3: Configuring User Access

Chapter 4: User/Endpoint Directory Basics

Chapter 5: Product Directory Basics

Chapter 6: Working with Managed Servers

Chapter 7: Downloading and Deploying Components

Part II: Monitoring the Control Manager Network

Chapter 8: Working with the Dashboard and Widgets

Chapter 9: Using Command Tracking

Chapter 10: Using Notifications

Chapter 11: Working with Logs

Chapter 12: Working with Reports

Part III: Administering Control Manager

Chapter 13: MCP and Control Manager Agents

Chapter 14: Administering Managed Products

Chapter 15: Activating Control Manager and Managed Products

Chapter 16: Managing Child Servers

Chapter 17: Policy Management

Chapter 18: Investigating Data Loss Prevention Incidents

Chapter 19: Responding to Targeted Attacks and Advanced Threats

Chapter 20: Administering the Database

Part IV: Services and Tools

Chapter 21: Using Trend Micro Services

Chapter 22: Using Control Manager Tools

Part V: Removing Control Manager and Contacting Support

Chapter 23: Removing Trend Micro Control Manager

Chapter 24: Getting Support

Appendices

Appendix A: Control Manager System Checklists

Appendix B: Data Views

Appendix C: IPv6 Support in Control Manager

Appendix D: Checking Policy Status

Index

Preface

This Administrator's Guide introduces Trend Micro™ Control Manager™ 6.0 Service Pack 3 and walks you through configuring Control Manager to function according to your needs.

This preface contains the following topics:

What's New in This Version

This section lists the new features and enhancements available in each release.

Control Manager 6.0 SP3 Features and Enhancements

A wizard showing an overview of new features and enhancements is available when you open the Control Manager management console after installing this service pack.

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*
- View Connected Threat Defense topics as a PDF file

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 that 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*

USER AND ENDPOINT IMPORTANCE

Assign importance to groups of users and endpoints. For example, assign external-facing servers as important so you can apply a strict policy to these servers and constantly monitor their protection status.

The **Critical Threats**, **Users with Threats**, and **Endpoints with Threats** widgets on the **Summary** tab highlight important users and endpoints so you can prioritize them.

Learn more:

How to assign importance

SUMMARY TAB ENHANCEMENT

The enhanced **Summary** tab contains a predefined set of widgets that provide timely security information.

The tab and all its predefined widgets are now "read-only" (regular tab and widget operations are not allowed).

If you upgraded and you do not see the Summary tab you were using in the previous version, you can bring it back.

Learn more:

- *Summary Tab*
- *How to bring back the old Summary tab*

POLICY INHERITANCE

This feature is useful in organizations with several OfficeScan servers and administrators, where a Control Manager administrator manages global OfficeScan policies, while other administrators define local or regional policies.

In this situation, the Control Manager administrator creates a "parent" policy with global settings that cannot be overridden and recommended settings that can be customized or extended. Other administrators use "child" policies created from the parent. These policies inherit global settings and allow customizations of recommended settings.

Learn more:

- *OfficeScan settings that support policy inheritance*
- *How to create a parent OfficeScan policy*
- *How to create a child policy*
- *How policy inheritance affects centrally and locally managed features available in previous versions*

POLICY PERMISSIONS

Control policy permissions when adding a user role. Users with the role can have full control, maintenance, or read-only permissions to Policy Management and/or Policy Resources features and functions.

Learn more:

How to add a user role and configure policy permissions

Connected Threat Defense Product Integration

Main Products

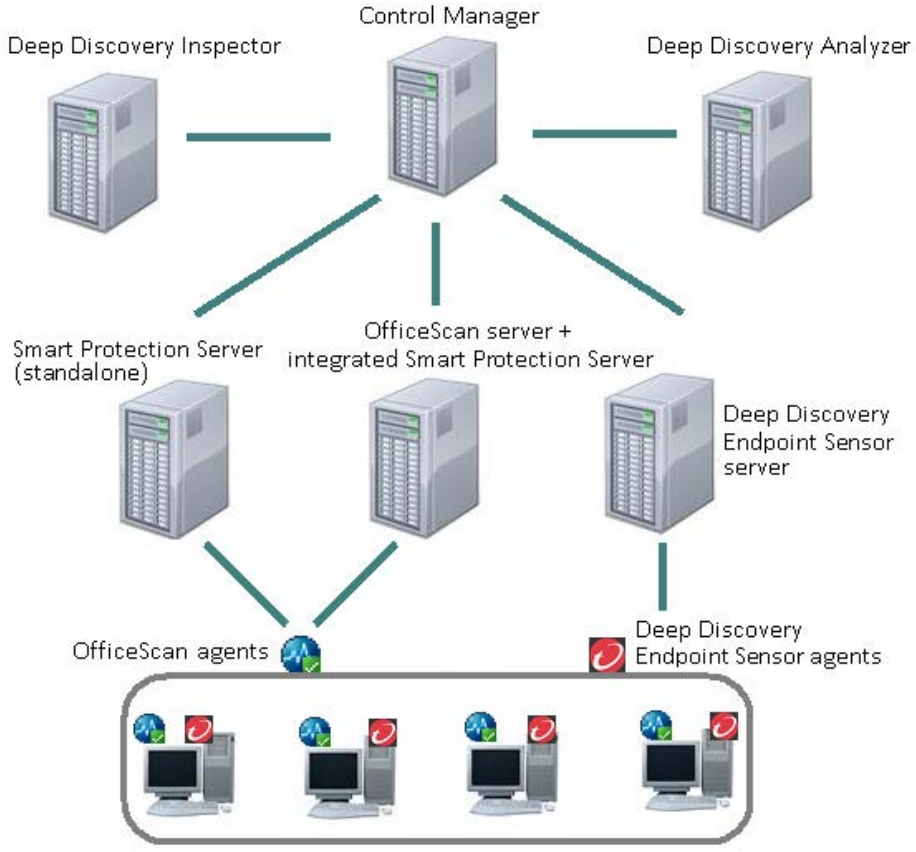
Connected Threat Defense requires the following Trend Micro products:

- Control Manager
- Deep Discovery Inspector
- OfficeScan
- Smart Protection Server (standalone) or integrated with OfficeScan

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



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

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:

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

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.

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.	**3.3. 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**.
3.2. 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.	**3.4. 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**.

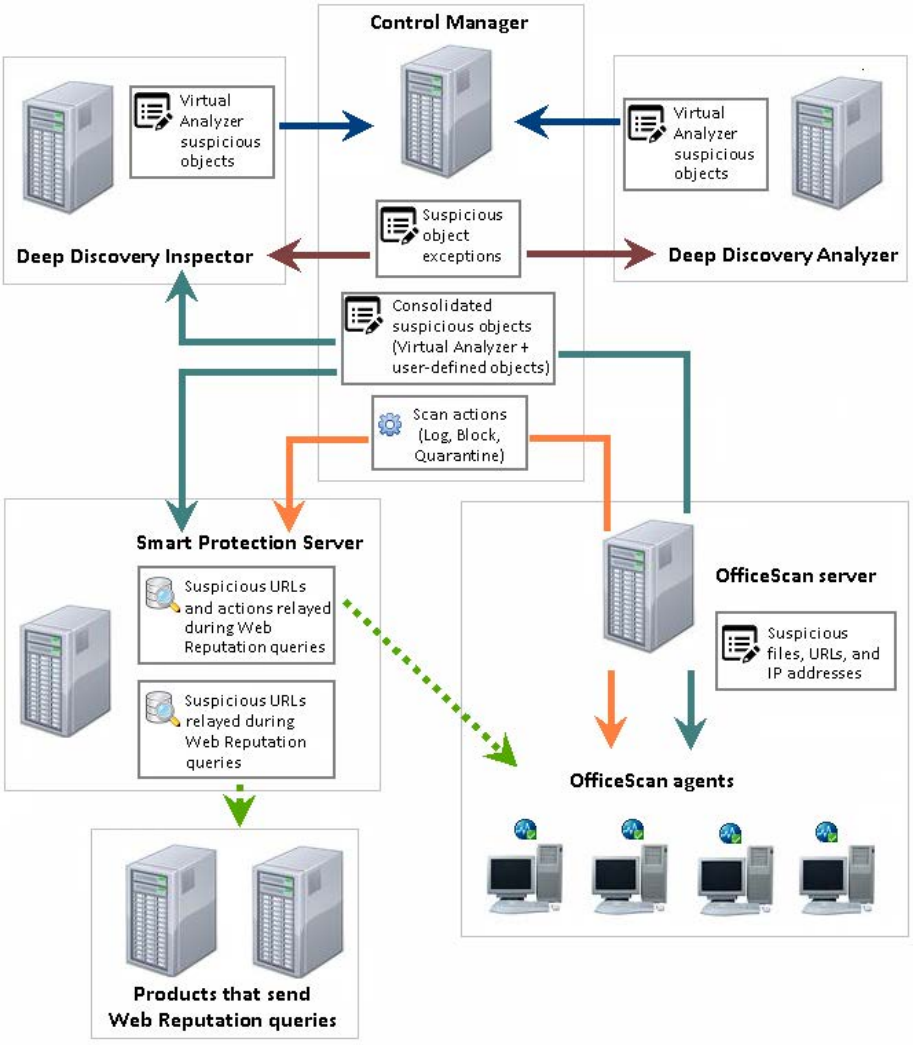
Scan actions are configured separately for Virtual Analyzer and user-defined suspicious objects.

- **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.

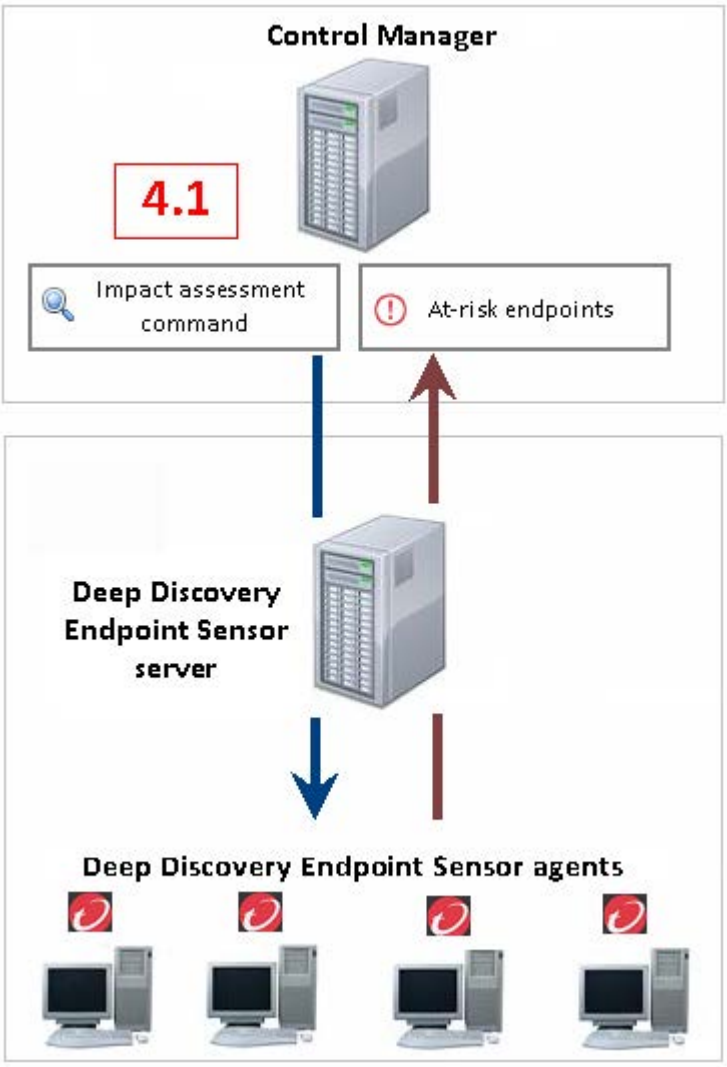

Control Manager
Virtual Analyzer suspicious objects
Virtual Analyzer suspicious objects
Deep Discovery Inspector
Suspicious object exceptions
Deep Discovery Analyzer
Consolidated suspicious objects (Virtual Analyzer + user-defined objects)
Scan actions (Log, Block, Quarantine)
Smart Protection Server
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

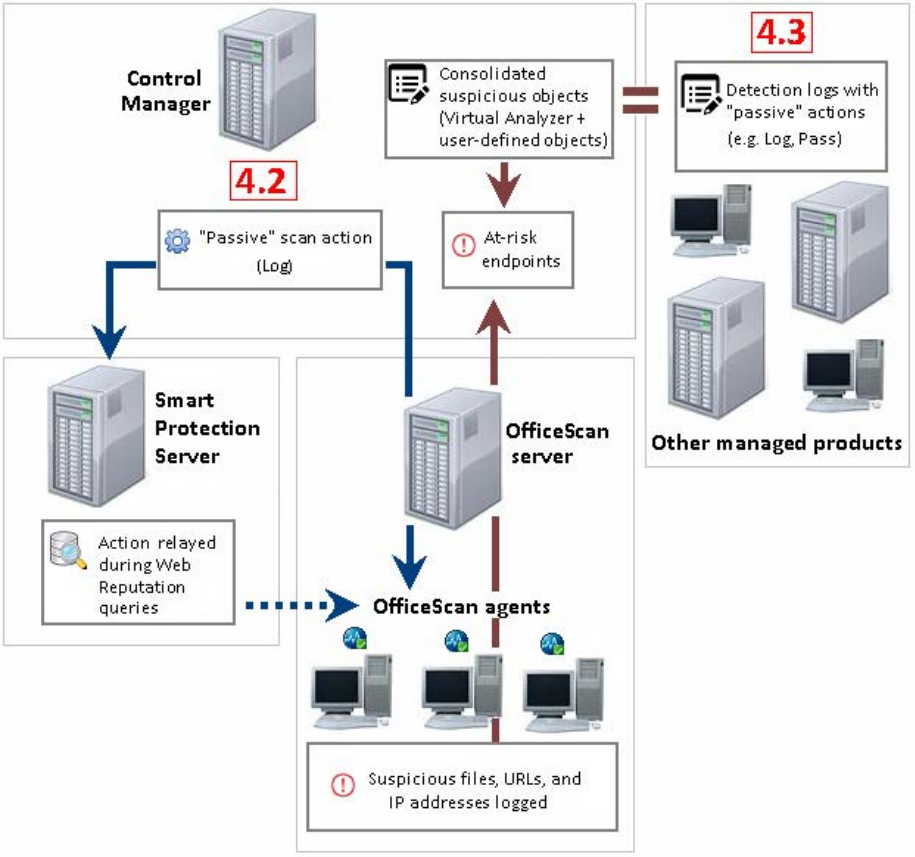
Impact Assessment

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.

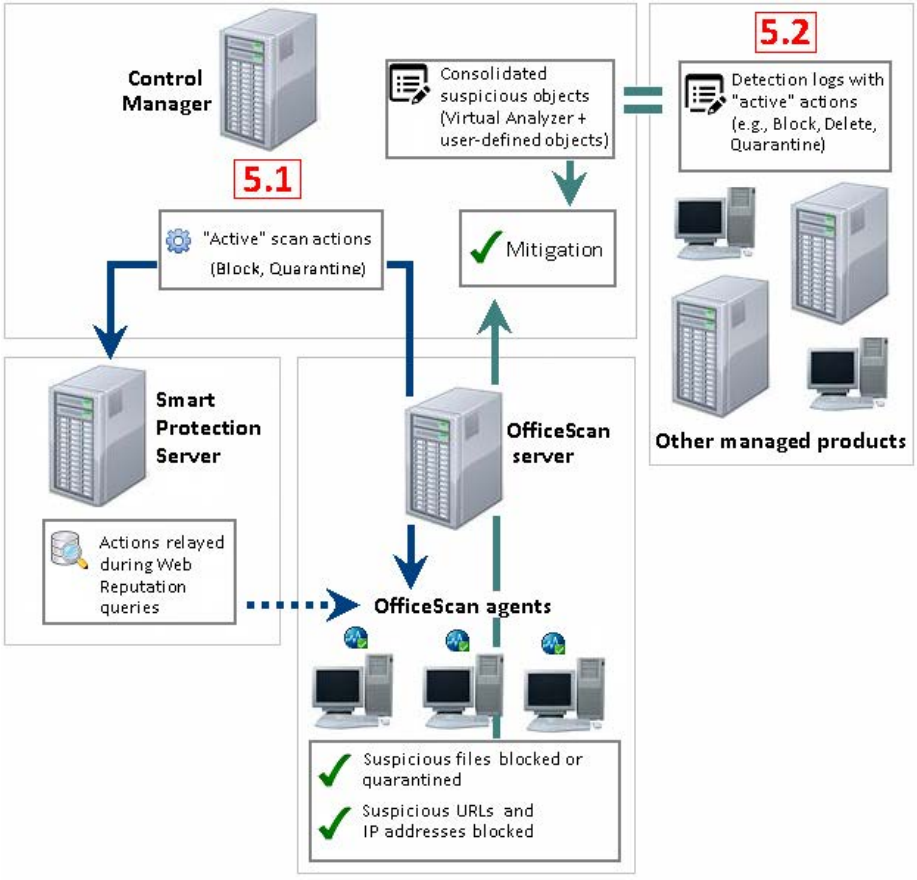

Control Manager
4.1
Impact assessment command
At-risk endpoints
Deep Discovery Endpoint Sensor server
Deep Discovery Endpoint Sensor agents



Mitigation

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

5.1. "Active" Scan Actions When the scan action configured in Control Manager and deployed to OfficeScan agents is "active" (block or quarantine), the affected endpoints are considered mitigated.	 **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 xxxix*.
5.2. 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 an "active" action (such as Block, Delete, Quarantine, or Override), Control Manager treats the endpoint as mitigated.	



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.

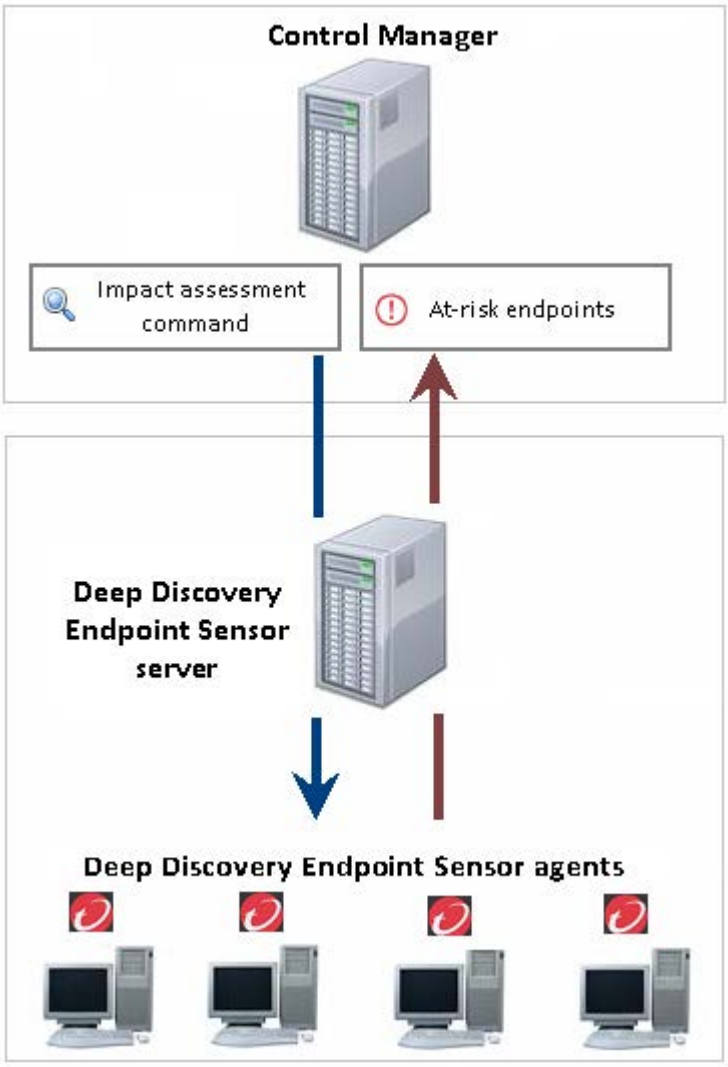
As Control Manager only requires IOC files for impact assessment, extract the .ioc files from the compressed file and then add them to Control Manager. It is not possible to add the compressed file.

Important

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

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**.



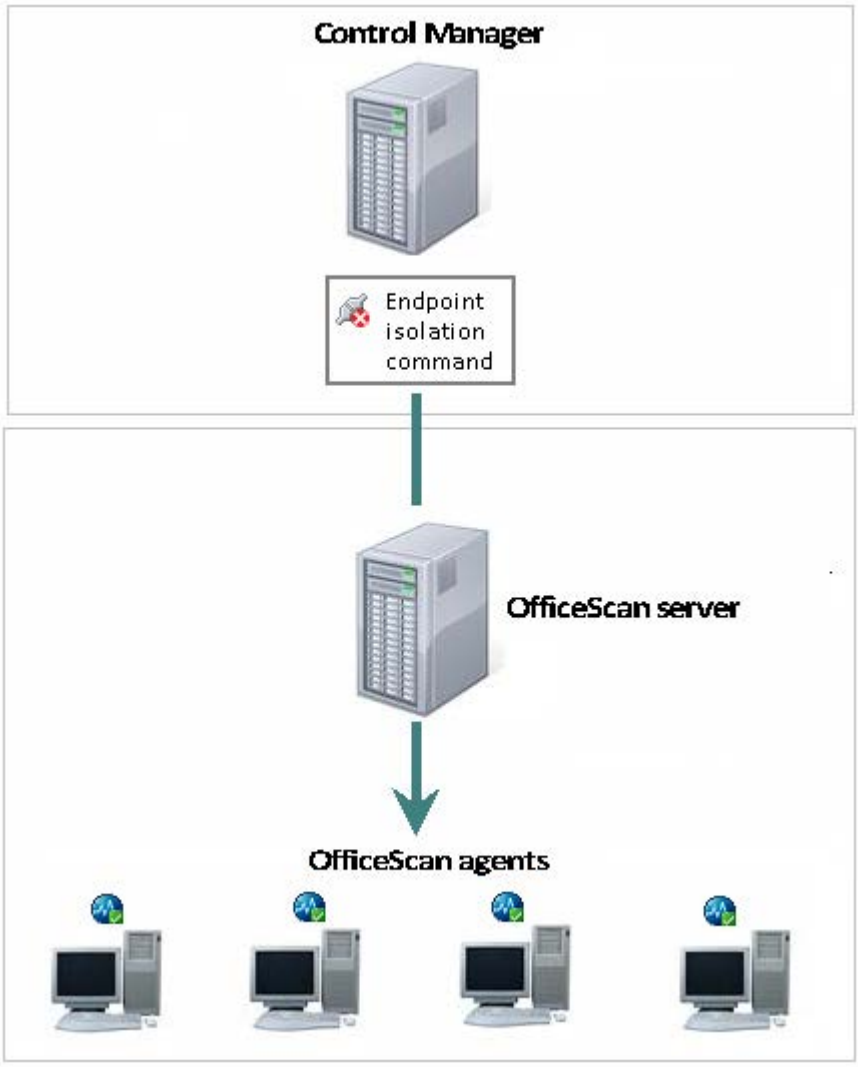
Go to **Administration** > **Indicators of Compromise** and run an impact assessment on one or several IOC files to determine at-risk endpoints.

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.

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 xxxix*.

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

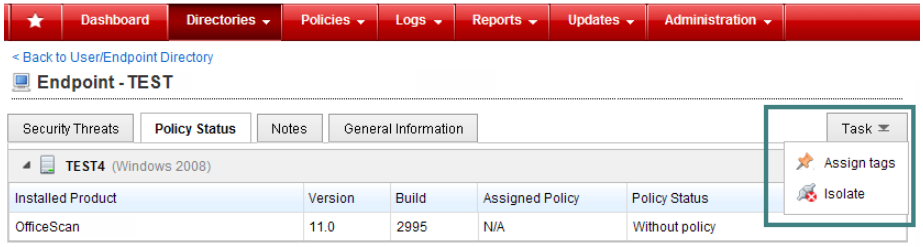
Isolate at-risk endpoints to run an investigation and resolve security issues. Restore the connection promptly when all issues have been resolved.

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.

Initiating Endpoint Isolation

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

1.1. Endpoint screen



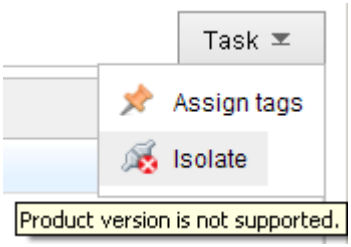
Note

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

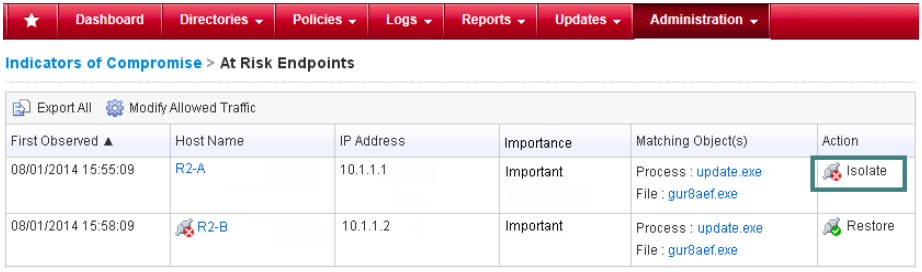
There are several ways to access this screen. The recommended way is to go to **Directories** > **Users/Endpoints**, use the search feature in the screen to find the endpoint to isolate, and then click the endpoint name when the search results display.

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.



1.2. At Risk Endpoints screen



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.

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.

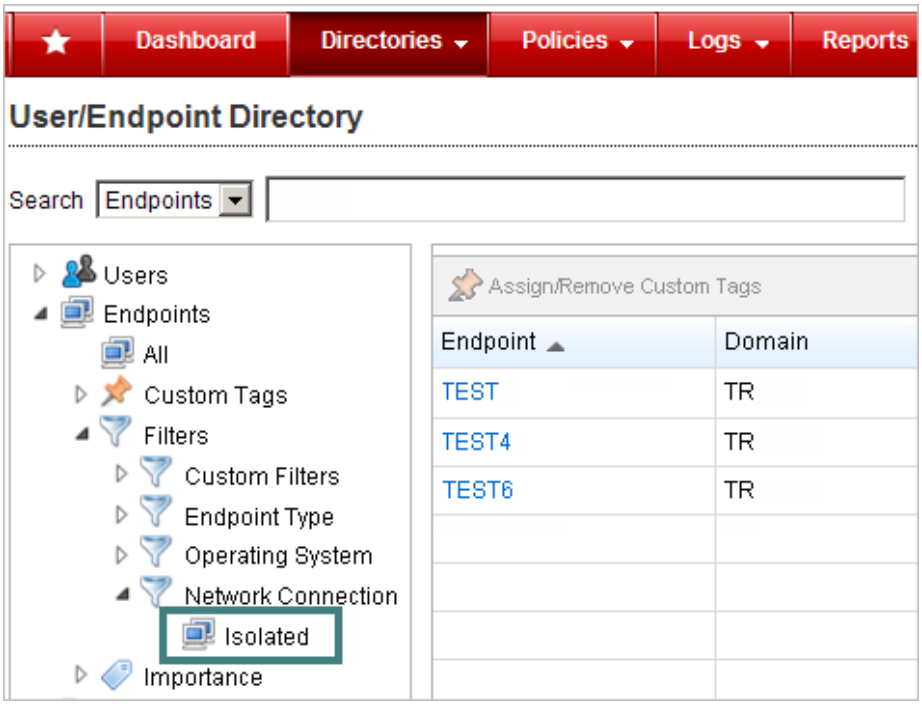
If there is an issue, the message changes. Issues include:

- 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.

Monitoring Isolated Endpoints

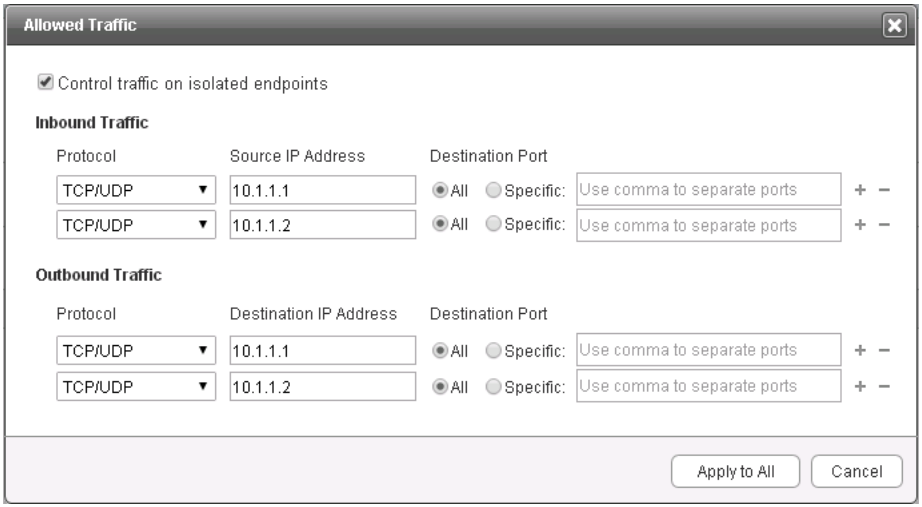
A list of isolated endpoints is available in the Endpoint tree, when you select the default filter, **Isolated**.



4

Configuring Allowed Traffic

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



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.

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).

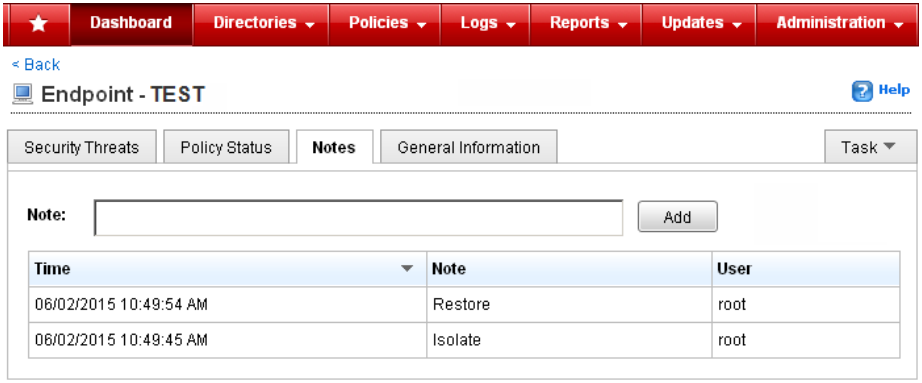
- There is no connection between the OfficeScan agent on the endpoint and its parent server.

- 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.



Control Manager 6.0 SP2 Features and Enhancements

Control Manager Service Pack 2 (SP2) provides the following new features and enhancements:

Feature	Description
Deep Discovery Inspector integration	With Deep Discovery Inspector integration, the following features are now available: • The **Administrator** > **Suspicious Objects** option provides information about Deep Discovery Inspector detections based on threat engines, Virtual Analyzer, and user-defined lists • Two new Deep Discovery Inspector widgets: System Status and Affected Hosts A detections screen offers detailed actionable information that highlights the hosts requiring priority attention. For deeper investigation, administrators can drill down from overall traffic detected into detailed logs. • New **Event Center** alert for Advanced Persistent Threats • The new Host Severity Report custom template provides information about threat detections by host Threats are mapped to threat life cycle rules to determine overall host vulnerability levels, and then displayed in summary and detailed subreports. Administrators can take action on affected hosts supported by clear evidence from Deep Discovery Inspector.
Support for HP TippingPoint Security Management System (SMS)	Share the suspicious objects list to customize your HP TippingPoint SMS filters. Deep Discovery Inspector provides the suspicious objects list.

Control Manager 6.0 SP1 Features and Enhancements

Control Manager Service Pack 1 (SP1) provides the following new features and enhancements:

FEATURE	DESCRIPTION
User/Endpoint Directory on page 4-2	The User/Endpoint Directory is a graphical representation of the organization of your Control Manager network. This directory allows you to organize your network into groups of users or endpoints with custom or predefined criteria. The following functionalities are now possible: • User view with Security Threat, Policy Status, and Contact Information • Endpoint view with Policy Status • Basic or advanced user/endpoint search • Custom filters to automatically group users/endpoints • Custom tags to manually group users/endpoints based on specific criteria • Active Directory integration and display of available structure **Important** Control Manager supports synchronization of Active Directory domains coming from the same forest.
Hosts with C&C Callback Attempts widget on page 8-15	This widget provides information about hosts that attempt to establish connection with known C&C servers.
Manage cloud-based services on page 6-2	In addition to products offering endpoint or server protection,you can now include supported Trend Micro SaaS solutions in the Control Manager managed servers list. The following functionalities are now possible: • Access and configure any of the managed SaaS solutions through Control Manager using single sign-on • You can, at any time, stop managing any registered SaaS solutions

Control Manager 6.0 Patch 3 Features and Enhancements

New features and enhancements related to the Command-and-Control Contact Alert (CCCA) service are available in version 6.0 Service Pack 3 Patch 3.

Feature	Description
Widgets	• C&C Callback Events • Unique Compromised Hosts Over Time
Notifications	• C&C callback alert • C&C callback outbreak alert
Logs	C&C Callback Information data view available under Security Threat Information
Components	Patterns available for updates: • C&C Information Pattern • Advanced Malware Pattern

Control Manager 6.0 Patch 2 Features and Enhancements

The following new features and enhancements are available in version 6.0 Service Pack 3 Patch 2.

Feature	Description
User roles	DLP user roles available for DLP incident investigation: • DLP Compliance Officer • DLP Incident Reviewer
Notifications	DLP notifications available for DLP incident investigation: • Scheduled incident summary • Incident details updated

Feature	Description
DLP template severity levels	Visible DLP template severity levels: • High • Medium • Low • Informational • Undefined
DLP incident investigation	• DLP dashboard widgets available for monitoring and reviewing DLP incidents based on severity levels and managed users • View a summary list of DLP incidents triggered by managed users • Review and update incident detailed information
DLP auditing logs	Export DLP auditing logs

Control Manager 6.0 Features and Enhancements

The following new features and enhancements are available in version 6.0 Service Pack 3.

Feature	Description
Policy management	• Deploy product settings to managed products using policies • Flexible policy types • Role-based administration • Easy policy template updates from the web console
Policy status dashboard widget	• Up-to-date deployment status of product settings • Monitor the numbers of deployed and pending targets • Check the detailed status of the pending targets

Feature	Description
Policy template updates	When new or updated templates become available, administrators can easily perform the update from the web console.
Data Loss Prevention (DLP) integration	DLP is a feature of the Data Protection module that monitors the transmission of digital assets. The DLP feature can minimize the risk of information loss and improve visibility of data usage patterns and risky business processes. Control Manager has integrated the following DLP features: • Manageable DLP templates and data identifiers • Deploy DLP settings to managed products using policy management, DLP templates, and data identifiers • Collect DLP logs for reports and event notifications • 22 pre-defined DLP report templates • Five DLP event notifications • Four dashboard widgets • Product support: OfficeScan, IMSVA, and ScanMail for Microsoft Exchange
Favorites	Administrators can add menu shortcuts to the **Favorites** menu for quick access.

Control Manager Documentation

This documentation assumes a basic knowledge of security systems. There are references to previous versions of Control Manager to help system administrators and personnel who are familiar with earlier versions of the product. If you have not used earlier versions of Control Manager, the references may help reinforce your understanding of the Control Manager concepts.

TABLE 1. Control Manager Documentation

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Control Manager web console. The online help contains explanations of Control Manager components and features, as well as procedures needed to configure Control Manager.
Trend Micro Online Help Center (http://docs.trendmicro.com)	The Trend Micro Online Help Center provides the latest product documentation.
Readme file	The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Installation Guide	PDF documentation is accessible from the Trend Micro Enterprise DVD or downloadable from the Trend Micro website. The Installation Guide contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running".
Administrator's Guide	PDF documentation that is accessible from the Trend Micro Solutions DVD for Control Manager or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions of how to configure and manage Control Manager and managed products, and explanations on Control Manager concepts and features.
Tutorial	PDF documentation that is accessible from the Trend Micro Solutions DVD for Control Manager or downloadable from the Trend Micro website. The Tutorial contains hands-on instructions of how to deploy, install, configure, and manage Control Manager and managed products registered to Control Manager.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Part I

Getting Started

Chapter 1

Introducing Trend Micro™ Control Manager™

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

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

This chapter contains the following topics:

- *Trend Micro™ Smart Protection Network™ on page 1-11*

Control Manager Standard and Advanced

Control Manager is available in two versions: Standard and Advanced. Control Manager Advanced includes features that Control Manager Standard does not. For example, Control Manager Advanced supports a cascading management structure. This means the Control Manager network can be managed by a parent Control Manager Advanced server with several child Control Manager Advanced servers reporting to the parent Control Manager Advanced server. The parent server acts as a hub for the entire network.

Note

Control Manager Advanced supports the following as child Control Manager servers:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

For a complete list of all features Standard and Advanced Control Manager servers support see *Control Manager Product Version Comparison on page A-9*

Introducing Control Manager Features

Trend Micro designed Control Manager to manage antivirus and content security products and services deployed across an organization's local and wide area networks.

TABLE 1-1. Control Manager Features

FEATURE	DESCRIPTION
Policy management	System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console.

FEATURE	DESCRIPTION
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console. These features help ensure consistent enforcement of your organization's virus/malware and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus/malware outbreak.
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure web console access and component download.
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager web console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager web console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control managed products in real time. Control Manager immediately sends configuration modifications made on the web console to the managed products. System administrators can run manual scans from the web console. This command system is indispensable during a virus/malware outbreak.

FEATURE	DESCRIPTION
Centralized update control	Update virus patterns, antispam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date.
Centralized reporting	Get an overview of the antivirus and content security product performance using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

Understanding Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) agent is the next generation agent for Trend Micro managed products. MCP replaces Trend Micro Management Infrastructure (TMI) as the way Control Manager communicates with managed products. MCP has several features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and two-way communication support
- Single sign-on (SSO) support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

- XML parsing requires more system resources compared to other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your server or device).

- The agent footprint required to transfer information is much larger in XML compared with other data formats.
- Data processing performance is slower due to the larger data footprint.
- Packet transmissions take longer and the transmission rate is less than other data formats.

MCP's data format is designed to resolve these issues. MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length, and value. This BLOB format has the following advantages.

TABLE 1-2. BLOB Format Advantages

ADVANTAGE	DESCRIPTION
Smaller data transfer size compared to XML	Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.
Faster parsing speed	With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
Improved design flexibility	Design flexibility has also been considered since each item is composed of name ID, type, length, and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with or without compression. With this type of data transfer strategy, network bandwidth can be preserved and improved scalability is also created.

NAT and Firewall Traversal Support

With limited addressable IP addresses on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will

translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with Control Manager 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks when the agent sits behinds a NAT device (or the Control Manager server sits behind a NAT device) since the connection can only route to the NAT device, not the product behind the NAT device (or the Control Manager server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

The MCP deals with this issue by introducing a one-way communication model. With one-way communication, only the agent initiates the network connection to the server. The server cannot initiate connection to the agent. This one-way communication works well for log data transfers. However, the server dispatching of commands occurs under a passive mode. That is, the command deployment relies on the agent to poll the server for available commands.

HTTPS Support

The MCP integration protocol applies the industry standard communication protocol (HTTP/HTTPS). HTTP/HTTPS has several advantages over TMI:

- A large majority of people in IT are familiar with HTTP/HTTPS, which makes it easier to identify communication issues and find solutions those issues
- For most enterprise environments, there is no need to open extra ports in the firewall to allow packets to pass
- Existing security mechanisms built for HTTP/HTTPS, such as SSL/TLS and HTTP digest authentication, can be used

Using MCP, Control Manager has three security levels:

- **Normal security**: Control Manager uses HTTP for communication
- **Medium security**: Control Manager uses HTTPS for communication if HTTPS is supported and HTTP if HTTPS is not supported
- **High security**: Control Manager uses HTTPS for communication

One-Way Communication

NAT traversal has become an increasingly more significant issue in the current, real-world network environment. In order to address this issue, MCP uses one-way communication. One-way communication has the MCP client initiating the connection to and polling of commands from the server. Each request is a CGI-like command query or log transmission. In order to reduce the network impact, the connection is kept alive and open as much as possible. A subsequent request uses an existing open connection. Even if the connection is dropped, all connections involving SSL to the same host benefit from session ID cache that drastically reduces reconnection time.

Two-Way Communication

Two-way communication is an alternative to one-way communication. It is still based on one-way communication, but has an extra channel to receive server notifications. This extra channel is also based on HTTP protocol. Two-way communication can improve real-time dispatching and processing of commands from the server by the MCP agent. The MCP agent side needs a web server or CGI compatible program that can process CGI-like requests to receive notifications from the Control Manager server.

Single Sign-on (SSO) Support

Through MCP, Control Manager supports single sign-on (SSO) functionality for Trend Micro products. This feature allows users to sign in to Control Manager and access the resources of other Trend Micro products without having to sign in to those products as well.

Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy. The following table provides a list of components Control Manager uses.

TABLE 1-3. Control Manager Components

COMPONENT	DESCRIPTION
Control Manager server	Acts as a repository for all data collected from the agents. It can be a Standard or Advanced Edition server. A Control Manager server includes the following features: • An SQL database that stores managed product configurations and logs Control Manager uses the Microsoft SQL Server database (`db_ControlManager.mdf`) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings. • A web server that hosts the Control Manager web console • A mail server that delivers event notifications through email messages Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure Event Center to send notifications through email messages, Windows event log, MSN Messenger, SNMP, Syslog, pager, or any in-house/industry standard application used by your organization to send notification. • A report server, present only in the Advanced Edition, that generates antivirus and content security product reports A Control Manager report is an online collection of figures about security threat and content security events that occur on the Control Manager network.

COMPONENT	DESCRIPTION
Trend Micro Management Communication Protocol	MCP handles the Control Manager server interaction with managed products that support the next generation agent. MCP is the new backbone for the Control Manager system. MCP agents install with managed products and use one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.
Trend Micro Management Infrastructure	Handles the Control Manager server interaction with older managed products. The Communicator, or the Message Routing Framework, is the communication backbone of the older Control Manager system. It is a component of the Trend Micro Management Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. They interact with Control Manager 2.x agents to communicate with older managed products.
Control Manager 2.x Agents	Receives commands from the Control Manager server and sends status information and logs to the Control Manager server The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Therefore, install agents on the same computer as managed products.
Web-based management console	Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™ The Control Manager management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible web browser.

COMPONENT	DESCRIPTION
Widget Framework	Allows an administrator to create a customized dashboard to monitor the Control Manager network.

Trend Micro™ Smart Protection Network™

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight agents to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

For more information on the Smart Protection Network, visit:

www.smartprotectionnetwork.com

Email Reputation

Trend Micro's email reputation technology validates IP addresses by checking them against a reputation database of known spam sources and by using a dynamic service that can assess email sender reputation in real time. Reputation ratings are refined through continuous analysis of the IP addresses' "behavior," scope of activity and prior history. Email reputation blocks malicious email messages in the cloud based on the sender's IP address, preventing threats from reaching the network or the user's PC.

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-agent

architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall agent footprint.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation then continues to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat.

By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in the protection of others. Because the gathered threat information is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Samples of information sent to Trend Micro:

- File checksums

- Websites accessed
- File information, including sizes and paths
- Names of executable files

You can terminate your participation to the program anytime from the web console.

Tip

You do not need to participate in Smart Feedback to protect your computers. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in Smart Feedback to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Chapter 2

Getting Started with Control Manager

The Control Manager web-based management console allows you to administer managed products and other Control Manager servers.

This chapter contains the following topics:

Using the Management Console

The Control Manager management console is a web-based console published on the Internet or Intranet through Microsoft™ Internet Information Services (IIS) and hosted by the Control Manager server. The web console lets you administer the Control Manager network from any machine using a compatible web browser.

Note

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

The web console consists of the following: main menu, drop-down menus, working area, and Help menu.

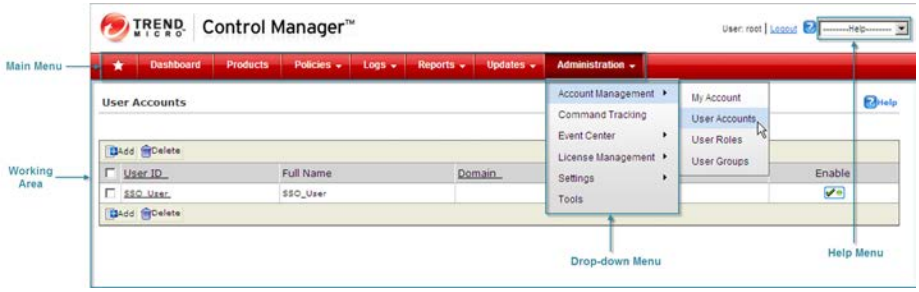


FIGURE 2-1. Control Manager management console

Main Menu

The web console main menu includes links to the following Control Manager functions.

TABLE 2-1. Contents of the Control Manager Main Menu

MAIN MENU ITEM	DESCRIPTION
Favorites (*)	Allows users to add menu shortcuts for quick access

Main Menu Item	Description
Dashboard	Allows the addition of widgets that provide at-a-glance summaries of your network. The widgets also include shortcuts to detailed information screens and ad hoc queries.
Directories	Includes the following options: • Users/Endpoints: allows you to view user/endpoint information, and conduct security investigations • Products: allows you to administer managed products, communicators, and child servers
Policies	Includes options to perform policy management and update policy templates.
Logs	Includes options to view logs for all products register to the Control Manager server.
Reports	Includes options to manage Control Manager managed products and child server reports.
Updates	Provides options for configuring manual and scheduled updates and component deployment plans.
Administration	Includes the **Account Management**, **Command Tracking**, **Event Center**, **License Management**, **Settings**, **Outbreak Prevention Services**, and **Tools** options.

Drop-Down Menu

The drop-down menus for each main menu item appear after moving the cursor over the specified item. Only the Dashboard menu items do not contain a drop-down menu.

Working Area

Use the working area to manage the Control Manager network. Here users can administer managed products or child server settings, invoke tasks, or view system status, logs, and reports.

Help Menu

The **Help** menu provides the following supports:

- Advanced feature descriptions and detailed configuration information
- Product information and procedures provided by the Trend Micro Support team
- Latest malware advisories as well as the list of the current top 10 security threats
- Control Manager version, build number, and copyright information

Understanding the Function-Locking Mechanism

The web console has a function-locking mechanism that prevents two users from accessing the **Directory Management** screen at the same time.

This means that when user A is arranging managed products using Directory Management, user B, who is also logged on to the web console, cannot access the **Directory Management** screen.

If you attempt to access a locked option, the locked option information screen appears. Control Manager only allows one user to use the function at a time.

To verify that the function is still in use, periodically click **Reload**.

To release the lock, click **Break** to release the lock.

Note

The unlock function is available for users with the privileges to manage product folders.

Accessing the Management Console

You have two ways to access the web console:

- Locally on the Control Manager server

- Remotely using any compatible browser

Accessing the Web Console Locally from the Control Manager Server

Procedure

1. Click **Start** > **Programs** > **Trend Micro Control Manager** > **Trend Micro Control Manager**.
2. Provide the user name and password in the fields provided.
3. Click **Log On**.

Accessing the Console Remotely

Procedure

1. Type the following in your browser's address field to open the **Log On** screen:

   ```
   http(s)://{host name}/WebApp/login.aspx
   ```

   Where host name is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name.
2. Provide the user name and password in the fields provided.
3. Click **Log on**.

Upon opening the web console, the dashboard displays the status summary for the whole Control Manager network. This summary is identical to the status summary generated from the Product Directory. User rights determine the Control Manager functions a user can access.

Note

Control Manager does not allow using the same Control Manager web console in more than one browser on the same computer if you use the same user name and password. Multiple instances on different computers using the same user name and password are supported.

Changing Access to the Management Console

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

You must obtain a certificate and set up the Control Manager virtual directory before you can start sending encrypted or digitally signed information to and from a Control Manager server.

Assigning HTTPS Access to the Control Manager Web Console

Procedure

1. Obtain a Web site Certificate from any certification providers (for example, `Thawte.com` or `VeriSign.com`).
2. Click **Start** > **Programs** > **Administrative Tools** > **Internet Services Manager** to open the IIS Microsoft Management Console (MMC).
3. Click the **+** sign adjacent to the IIS server to expand the virtual site list.
4. Select **Default Web Site** and then right-click **Properties**.
5. On the **Default Web Site Properties** screen, select the **Directory Security** tab and then click **Server Certificate** to create a server certificate request using the new Certificate Wizard.

a. Click **Next**.

b. On the **Server Certificate Method** screen, select **Import a certificate from a Key Manager backup file** and then click **Next**.

c. Type the key **full path** and **file name** (for example, `cm_cert.key`) and then click **Next**.

d. Specify the key **password** and then click **Next**.

e. On the **Imported Certificate Summary** screen, click **Next** to implement the server certificate or click **Back** to modify settings.

6. Click **OK** to apply the Default Web Site server certificate and go back to the Default Web Site list.

7. Select the **Control Manager** virtual directory from the Default Web Site list and then right-click **Properties**.

8. Click the **Directory Security** tab and then click **Edit** under **Secure communications**.

   The **Secure Communications** window appears.

9. Select **Require secure channel (SSL)** and **Require 128-bit encryption**.

10. Click **OK** to close the **Secure Communications** window.

11. Click **OK** to apply changes and go back to the Default Web Site list.

    The next time you access the web console using HTTP, the following message appears:

    "You must view this page over a secure channel"

Configuring Web Console Settings

From the **Web Console Settings** screen, configure the console auto refresh and time-out settings. Enabling the auto refresh function allows the web console to update the screen periodically. When the console times out, Control Manager requires user authentication (logging on) to access the web console.

Procedure

1. Navigate to **Administration** > **Settings** > **Web Console Settings**.

   The **Web Console Settings** screen appears.

2. On the working area under **Web Console Auto Refresh**, select **Enable Auto Refresh**.

3. Specify the auto refresh frequency from **10** to **300** seconds (Dashboard only).

4. On the working area under **Web Console Timeout Setting**, select **Enable automatic log out from the web console**.

5. Specify the console time-out setting from **10** to **30** minutes (Dashboard and Product Directories).

6. On the working area under **Web Console Security**, select **Enable web console security**.

7. Specify the number of consecutive unsuccessful logon attempts before a user account is locked.

8. Specify the duration of an account lockout.

9. Click **Save**.

Configuring Command Time-out Settings

From the **Communication Time-out Settings** screen, configure the command time-out settings. When a command times out, Control Manager stops trying to execute the command (for example a deploy component command to OfficeScan servers).

Procedure

1. Navigate to **Administration** > **Settings** > **Communication Time-out Settings**.

   The **Communication Time-out Settings** screen appears.

2. On the working area under **Command Time-out Settings**, specify the command time-out setting:
   - **24** hours
   - **48** hours
   - **72** hours
3. Click **Save**.

Logging Off from the Management Console

To log off from the management console, perform one of the following:

Procedure

- Click **Log Off** on the top right corner of the web console.
- Press the CTRL and W keys simultaneously.

Chapter 3

Configuring User Access

Administrators can control which web console screens a user can view and the user's access to managed products that are registered to the Control Manager server.

Understanding User Access

Control Manager access control consists of the following four sections.

TABLE 3-1. Control Manager User Access Options

SECTION	DESCRIPTION
My Account	The **My Account** screen contains all the account information that Control Manager has for a specific user. The information on the **My Account** screen varies from user to user.
User Accounts	The **User Accounts** screen displays all Control Manager users. The screen also provides the options for users to create and maintain Control Manager user accounts. Use these functions to define clear areas of responsibility for users by restricting access rights to certain managed products and limiting what actions users can perform on the managed products. The functions are: • Execute • Configure • Edit Directory
User Roles	The **User Roles** screen displays all Control Manager user roles. The screen also provides the options for users to create and maintain Control Manager user roles. User roles define which areas of the Control Manager web console a user can access.
User Groups	The **User Groups** screen contains Control Manager groups and provides options for creating groups. Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. Control Manager groups do not allow administrators to create a group that shares the same access rights.

Note

Assign users with different access rights and privileges to permit the delegation of certain management tasks without compromising security.

Root Account Information

Control Manager creates the **Root** account upon installation. The Root and Administrator accounts can view all the functions in the menu, use all available services, and, on older managed products, can install agents.

The Root account also has the following additional privileges:

- Only the Root account can see all user accounts on the server; other accounts can only see their child accounts.
- The Root account can unlock a locked function by forcibly logging out the user who currently uses the function.

Note

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

Understanding User Roles

Control Manager uses the following as the default user roles. Administrators cannot modify access permissions for the default user roles. A description for each role is available on the management console.

- Administrator and DLP Compliance Officer
- Administrator
- DLP Compliance Officer
- DLP Incident Reviewer
- Operator

- Power User
- SSO Users

Control Manager also supports custom user roles. Custom user roles allow Control Manager administrators to specify which Control Manager web console menu items other users can access.

Note

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

If a custom user role in a previous Control Manager version has permissions to Policy Management menu items, the role will have full control permissions after upgrading to the current release. You can change the permissions to "maintain" or "read-only". A custom user role without these permissions will continue to not have permissions after upgrading.

TABLE 3-2. User Role Access

MENU ITEM		ADMINISTRATOR*	DLP COMPLIANCE OFFICER	DLP INCIDENT REVIEWER	OPERATOR	POWER USER
Dashboard		●	●	●	●	●
Directories	Users/Endpoints	●	No permission	No permission	●	●
	Products	●	No permission	No permission	●	●

Menu Item			Administrator*	DLP Compliance Officer	DLP Incident Reviewer	Operator	Power User
Policies	Policy Management			No permission	No permission	Read only	Read only
	Policy Resources	Policy Template Settings		No permission	No permission	No permission	No permission
		DLP Data Identifiers		No permission	No permission	No permission	No permission
		DLP Templates		No permission	No permission	No permission	No permission
Logs	New Ad Hoc Query			No permission	No permission		
	Saved Ad Hoc Queries			No permission	No permission		
	Log Aggregation			No permission	No permission	No permission	No permission
	Log Maintenance			No permission	No permission	No permission	

Menu Item		Administrator*	DLP Compliance Officer	DLP Incident Reviewer	Operator	Power User
Reports	My Reports	●	No permission	No permission	●	●
	One-time Reports	●	No permission	No permission	No permission	●
	Scheduled Reports	●	No permission	No permission	No permission	●
	Custom Templates	●	No permission	No permission	No permission	●
	Report Maintenance	●	No permission	No permission	No permission	●

Menu Item		Administrator*	DLP Compliance Officer	DLP Incident Reviewer	Operator	Power User
Updates	Manual Download	●	No permission	No permission	No permission	●
	Scheduled Download	●	No permission	No permission	No permission	●
	Component List	●	No permission	No permission	No permission	●
	Deployment Plan	●	No permission	No permission	No permission	●
	Scheduled Download Exceptions	●	No permission	No permission	No permission	●
	Update / Deployment Settings	●	No permission	No permission	No permission	●

Menu Item			Administrator*	DLP Compliance Officer	DLP Incident Reviewer	Operator	Power User
Administration	Account Management	My Account	●	No permission	No permission	●	●
		User Accounts	●	No permission	No permission	No permission	No permission
		User Roles	●	No permission	No permission	No permission	No permission
		User Groups	●	No permission	No permission	No permission	No permission
	Managed Servers		●	No permission	No permission	No permission	No permission
	Command Tracking		●	No permission	No permission	No permission	●
	Event Center	Event Notifications	●	No permission	No permission	No permission	No permission
		General Event Settings	●	No permission	No permission	No permission	No permission
	License Management	Control Manager	●	No permission	No permission	No permission	No permission
		Managed Product	●	No permission	No permission	No permission	No permission

Menu Item			Administrator*	DLP Compliance Officer	DLP Incident Reviewer	Operator	Power User
Administration	Settings	Agent Communication Schedule	●	No permission	No permission	No permission	No permission
		Communication Time-out Settings	●	No permission	No permission	No permission	No permission
		Proxy Settings	●	No permission	No permission	No permission	No permission
		Web Console Settings	●	No permission	No permission	No permission	No permission
		Smart Protection Network Settings	●	No permission	No permission	No permission	No permission
		Product Agent Settings	●	No permission	No permission	●	●
		Active Directory and Widget Settings	●	No permission	No permission	No permission	No permission
		Parent Control Manager Settings	●	No permission	No permission	No permission	No permission

Menu Item	Administrator*	DLP Compliance Officer	DLP Incident Reviewer	Operator	Power User
Suspicious Objects (including sub-menus)	●	No permission	No permission	No permission	No permission
Indicators of Compromise	●	No permission	No permission	No permission	No permission
Tools	●	No permission	No permission	No permission	No permission

Note

The Administrator role and the following roles have the same access permissions:

Administrator and DLP Compliance Officer

SSO Users

Trend Micro suggests configuring user roles and user account settings in the following order:

1. Specify which products/directories the user can access (step 4 of *Editing a User Account on page 3-25*).
2. Specify which menu items the user can access. If the default user roles are not sufficient, see *Adding a User Role on page 3-11* or *Editing a User Role on page 3-14*.
3. Specify the user role for the user's account (step 4 of the *Editing a User Account on page 3-25*).

About Adding User Roles

Each default user role has assigned permissions on select menu items in the Control Manager web console. Administrators can add additional permissions for menu items but cannot remove predefined permissions from the default user roles.

If the default user roles are not flexible enough for an administrator's needs, administrators can now create their own user roles. User-specified user roles allow administrators to customize the permissions of any Control Manager web console elements.

Note

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

Example:

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

Adding a User Role

Procedure

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

The **User Roles** screen appears.

2. On the working area, click **Add**.

   The **Add Role** screen appears.

3. On the working area under Role Information, type a unique user role name in the **Name** field.

4. Provide a meaningful description for the user role in the **Description** field.

Note

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

5. On the working area under **Menu Access Control**, select the accessible menu items for the user role. The following menu items are accessible to every user role: **Dashboard**, **Favorites**, and **Help**.

6. If you selected **Policies** or any of its submenu items, select a permission under **Policy Management**.

   The following table lists the operations in the Policy Management screen (**Policies** > **Policy Management**) that each permission allows.

Operation	Permission		
	Full Control	Maintain	Read Only
Create a policy	Allowed	Not allowed	Not allowed
Copy a policy's settings	Allowed	Not allowed	Not allowed
Inherit a policy's settings	Allowed	Allowed	Not allowed
Import policies	Allowed	Not allowed	Not allowed
Export policies	Allowed	Allowed	Allowed
Delete a policy	Allowed	Allowed	Not allowed
Reorder policies in the list	Allowed	Allowed	Not allowed
Refresh the policy list	Allowed	Allowed	Allowed

7. Under **Data Loss Prevention**, select the option to monitor, review, and investigate DLP incidents triggered by all users.

8. Click **Save**.

The **User Roles** screen appears and the new user role appears in the User Roles list.

About Editing User Roles

Control Manager allows users to modify customized user roles. Users can only modify the names and descriptions of the default user roles but not their accessible menu items.

Edit user roles when a user role becomes outdated or requires minor maintenance.

Note

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

Example:

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

Editing a User Role

Procedure

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

The **User Roles** screen appears.

2. Click a user role from the **Name** column.

   The **Edit Role** screen appears.

3. Edit the required user role information.

4. Click **Save**.

   The **User Roles** screen appears and the user role appears in the User Roles list.

Understanding User Accounts

Administrators can use the functions on the **User Accounts** screen to assign users clearly defined areas of responsibility by restricting their access rights to certain managed products and limiting the actions that they can perform.

Note

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

Example:

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

Setting Access Rights

User access rights determine the controls available to the user in the Product Directory. For example, when you only assign a user the Execute right, then only the options associated with this right appear on the Product Directory.

You can give each user account the following access rights to a product.

TABLE 3-3. Control Manager User Account Options

PERMISSION	DESCRIPTION
Execute	This right permits the user to run commands on managed products in assigned folders. For example: • Start Scan Now • Deploy pattern files/cleanup templates • Enable Real-time Scan • Deploy program files • Deploy engines • Deploy license profiles
Configure	This right gives the user access to the configuration consoles of the managed products in the assigned folders. Users with this right can see **Configure <managed product>** and similar product-specific controls (for example, OfficeScan password configuration features) on their menus.
Edit Directory	This right permits the user to modify the organization of the managed products/directories the user can access.

Note

The options that actually appear also depend on the product's profile. For example, if a product does not have a scanning function, such as eManager, then the Scan Now control does not appear in the Product Tree Tasks menu.

The **User Accounts** screen displays the following.

TABLE 3-4. User Accounts Screen Contents

ACCOUNT INFORMATION	DESCRIPTION
User ID	The user name of the account user.
Full Name	The full name of the account user.

ACCOUNT INFORMATION	DESCRIPTION
Domain	The Active Directory domain (if any) to which the user belongs.
User Role	The user role assigned to the user (example: Administrator).
Locked	The user account has been locked because the user exceeded the allowed number of unsuccessful logon attempts, a setting that is configured in *Configuring Web Console Settings on page 2-7*.
Enable	The current status of the account.

Note

Upon installation, Control Manager automatically creates a root account.

About Adding/Importing User Accounts

Control Manager user accounts allow administrators to specify which products or directories other users can access.

Note

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

Example:

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

Add user accounts to do the following:

- Allow administrators to specify which products or directories other users can access
- Allow other users to log on to the Control Manager web console
- Allow administrators to specify the user on the recipient list for notifications
- Allow the administrator to add the user to user groups.

Note

Trend Micro suggests configuring user role and user account settings in the following order:

1. Specify which products/directories the user can access (step 4 of *Editing a User Account on page 3-25*).
2. Specify which menu items the user can access. If the default user roles are not sufficient, see *Adding a User Role on page 3-11* or *Editing a User Role on page 3-14*.
3. Specify the user role for the user account (step 4 of *Editing a User Account on page 3-25*).

When adding a user account, you need to provide information to identify the user, assign a user role, and set folder access rights.

Note

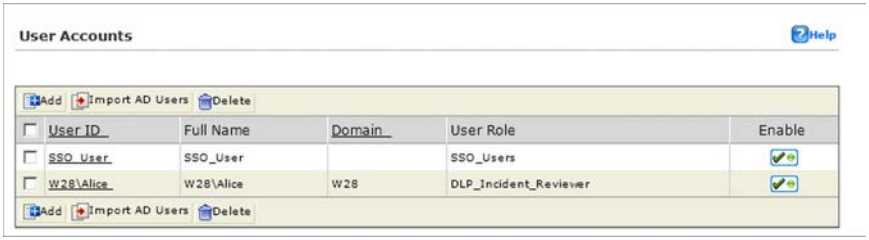
Active Directory users cannot have their accounts disabled from Control Manager. To disable an Active Directory user, you must disable the account from the Active Directory server.

Adding/Importing a User Account

Procedure

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

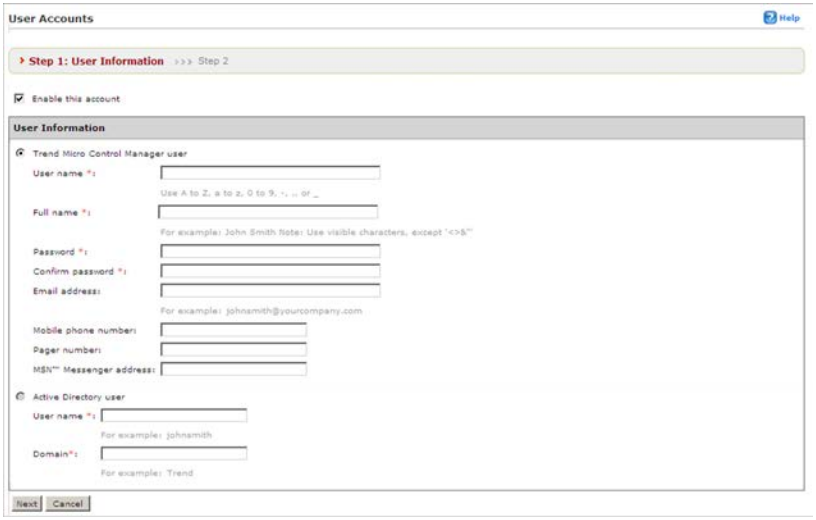
The **User Accounts** screen appears.



2. Click one of the following buttons to create the account:

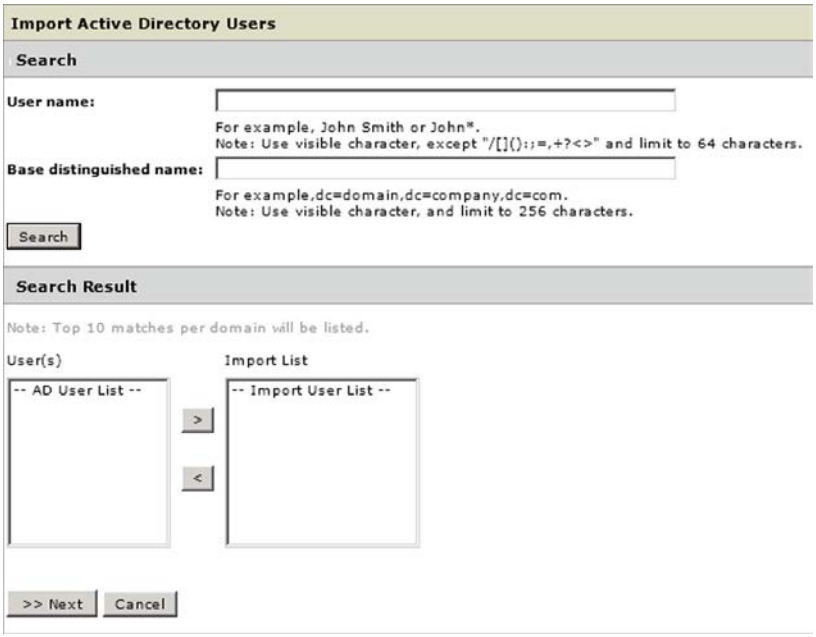
   - **Add**

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



   - **Import AD Users**

The **Import Active Directory Users** screen appears. Search for and add users to the Import List. Continue to step 5.



3. Select **Enable this account** to enable the Control Manager user.
4. Select the type of user to add:
   - To add a Trend Micro Control Manager user:

   a. Select **Trend Micro Control Manager user**.

   b. Provide the following required information to create an account:
      - **User name**: The name the user will use to log on to the Control Manager web console.

        For example, OfficeScan_Admin.
      - **Full name**: The full name of the user.

For example, John Smith.

- **Password** and **Confirm password**: Type and confirm your password in the fields provided. All users can change their log on password on the **My Account** screen.

c. The following additional information is optional. All users can also change these settings on the **My Account** screen.

- **Email address**: The email address to which the user has notifications delivered.
- **Mobile phone number**: The cell phone to which the user has notifications delivered.
- **Pager number**: The pager to which the user has notifications delivered. (Precede the pager number with a 9 and a comma "," [each comma causes a 2 second pause])
- **MSN Messenger address**: The instant messenger address to which the user has notifications delivered.

- To add an Active Directory user:

Note

Active Directory users cannot have their accounts disabled from Control Manager. To disable an Active Directory user, you must disable the account from the Active Directory server.

a. Select **Active Directory user**.

b. Provide the following required information to create an account:

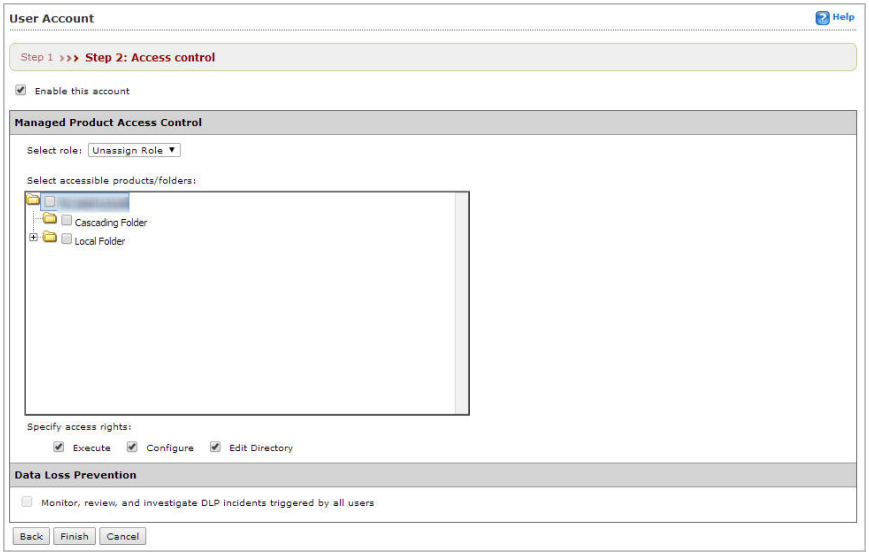
- **User name**: The user's Active Directory identification
- **Domain**: The domain to which the user belongs

Note

User names and domain names can be up to 32 characters in length.

5. Click **Next**.

The **Step 2: Access Control** screen appears.



6. Select a default or custom user role from the **Select role** list. Control Manager provides the following user roles by default:

   - **Administrator**
   - **DLP Compliance Officer**
   - **DLP Incident Reviewer**
   - **Operator**
   - **Power User**

Note

The DLP Compliance Officer and DLP Incident Reviewer roles are available to Active Directory users only.

7. Select the products or directories the user has access to from **Select accessible products/folders**.

Note

Carefully organize the Product Directory for ease of use. Assigning access to a folder allows users to access all of its sub-folders and managed products. You can restrict a user to a single managed product.

8. Select the rights to assign to the user. These rights determine the actions that the user can perform on managed products.

Note

Privileges granted to an account cannot exceed those of the grantor. That means you cannot assign a user access rights that are greater than your own. In addition, if you reduce an account's rights, you also reduce all of its child accounts.

9. Select **Monitor, review, and investigate DLP incidents triggered by all users** to grant the DLP_Compliance_Officer role to users with Administrator privileges.

10. Click **Finish**.

About Editing User Accounts

You can change the information of any user account including the account information, user role, or folder access rights. If you reduce an account's rights, you also reduce the rights of all its child accounts.

When editing accounts, remember:

- Root users can edit all the accounts that exist on the system. Users with **Administrator** accounts, however, can only edit accounts that they created themselves.
- An account's rights are a subset of those of its grantor and adjust accordingly if the grantor's rights are reduced.
- Modification of an account's privileges terminates all sessions using that account. If this modification involves a reduction of rights, child accounts whose privileges are also affected will also log out.

- You cannot change an existing account's user name.

Editing a User Account

Procedure

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

   The **User Accounts** screen appears.

2. Click the account to modify.

   The **Edit User Account** screen appears.

3. Modify the account information, and then click **Next**.

4. Modify the user role, accessible folders, and access rights.

5. Click **Finish**.

Disabling a User Account

Disable a user account to temporarily prevent a user from accessing the Control Manager network. This preserves the user account information and still allows the user account to be re-enabled anytime in the future.

Procedure

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

   The **User Accounts** screen appears.

2. Complete one of the following:

   - Click the status icon (a green check) under the **Enable** column of the User Accounts table. The status icon changes to a red icon.

   - Clear the **Enable this account** check box:

     a. Access the user's account screen.

b. On the working area of the **Add User** or **Edit User** screen, clear the **Enable this account** check box.

c. Click **Next**.

d. Click **Finish**.

Deleting a User Account

You can permanently remove a user account from accessing the Control Manager network. After you delete a user account, Control Manager removes the account from any groups the account belonged to, and the user no longer receives notifications for those events for which the user account was part of a recipient list.

Procedure

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

   The **User Accounts** screen appears.

2. Select the check box for the account to delete.

3. Click **Delete**.

Understanding My Account

The **My Account** screen contains all the account information Control Manager has for a specific user. The information on this screen varies with the user.

The **My Account** screen displays the following:

Account Information	Description	Examples
User name	The user name of the account user. This is a required field.	Administrator

ACCOUNT INFORMATION	DESCRIPTION	EXAMPLES
Full name	The full name of the account user. This is a required field.	John Smith
Password	Password used to log on to Control Manager. This is a required field.	MyPassword!
Confirm password	Confirm the password required to log on to Control Manager. This is a required field.	MyPassword!
Email address	The email address for the account user.	`johnsmith@mycompany.com`
Mobile phone number	The cellular phone number for the account user.	555-5551234
Pager number	The pager number for the account user.	555-5552345
MSN™ Messenger email address	The MSN email address for the user	`johnsmith@mycompany.com`

Understanding User Groups

User groups simplify the management of Control Manager users by providing a convenient way to send notifications to a single group rather than to individual users. The **User Groups** screen contains Control Manager groups. Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually.

Example: Multiple OfficeScan administrators would want to be informed of an outbreak, even if an outbreak was not a server that was managed by that particular administrator.

The **User Groups** screen displays the following.

TABLE 3-5. User Group Table

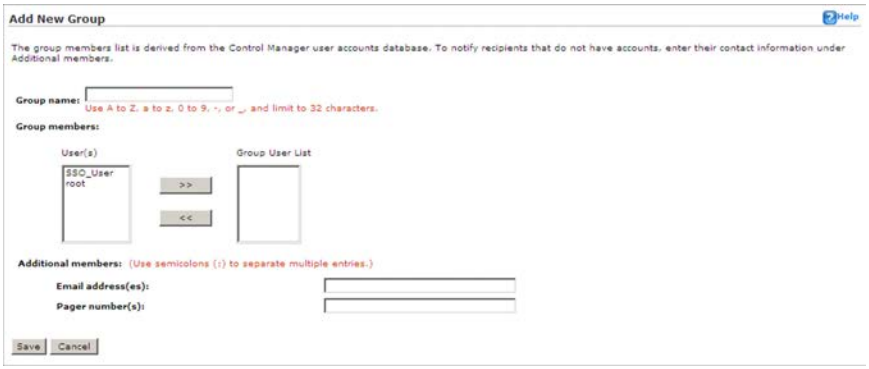
GROUP INFORMATION	DESCRIPTION
Groups	The name of the group.
Edit	Click the accompanying link in this row to edit the users who belong to the group.
Delete	Click the accompanying link in this row to delete a group from Control Manager.

Adding a User Group

You can add users to groups according to similar properties including user types, location, or the type of notifications they should receive. If a user does not have a Control Manager user account, you can still add the user to a group by typing their email address. However, they will only receive notifications if the group has been added to the recipient list for specific events.

Procedure

1. Navigate to **Administration** > **Account Management** > **User Groups**.
2. On the working area, click **Add New Group**.



3. Type a descriptive name for the group in **Group name**.

4. Under **Group Members**, add or remove users to the group list.

   - To add a user:

   a. Select a user from the User(s) list. Use the CTRL key to select multiple users.

   b. Click **>>** to add the selected user(s) to the Group User List. Control Manager sends notifications to users based on the contact information specified during their account setup.

   - To remove a user:

   a. Select a user from the Group User List. Use the CTRL key to select multiple users.

   b. Click **<<** to remove the user.

5. To add individuals who do not have Control Manager accounts to the Group User List, provide the following under **Additional members**:

   - Email address(es)
   - Pager number(s) (precede the pager number with the number your company uses to dial out and a comma "," [each comma causes a 2 second pause]) Separate multiple entries with semicolons.

6. Click **Save**.

7. Click **OK**.

Editing a User Group

Users can be added or removed to a group at anytime, including those users that do not have a Control Manager user account.

Procedure

1. Navigate to **Administration** > **Account Management** > **User Groups**.
2. On the working area, click **Edit** beside the group to modify.
3. Change the entries as required.

4. Click **Save**.
5. Click **OK**.

Deleting a User Group

Permanently remove a user group from the Control Manager network after you no longer require the group. After you delete a user group, members will no longer receive notifications for those events for which the user group was added to the recipient list.

Procedure

1. Navigate to **Administration** > **Account Management** > **User Groups**.
2. Click **Delete** beside the group to delete.
3. Click **OK** to delete the user group.
4. Click **OK**.

Chapter 4

User/Endpoint Directory Basics

The User/Endpoint Directory displays all users and associated endpoints.

Understanding the User/Endpoint Directory

The User/Endpoint Directory is a graphical representation of the organization of your Control Manager network. Control Manager 6.0 Service Pack 3 allows you to organize your network into groups of users or endpoints.

The default User/Endpoint Directory follows this structure:

Note

All users are placed in the **Users** tree under the following circumstances:

- If a local user logs on to a registered endpoint
- If they are part of Active Directory and the administrator enables Active Directory integration

Users cannot be removed from the complete users list even if a user creates their own grouping.

Consequently, all endpoints are lumped in the **Endpoints** tree, with Endpoint Type, Operating System, and Network Connection as default filters. These default trees and grouping can neither be deleted nor renamed.

- **Users**: Offers a list of all users in your managed network
- **Endpoints**: Offers a list of all endpoints and devices in your managed network (from endpoint-based managed products)
- **Active Directory**: Offers a one-to-one mapping of your Active Directory structure

  Control Manager supports synchronization of Active Directory domains coming from the same forest.

You can organize the User/Endpoint Directory through any of these methods:

- Filter-based grouping: Use filters to group users or endpoints based on specific characteristics
- Tag-based grouping: Use tags to assign users or endpoints manually
- Active Directory mapping: Synchronize automatically with your Active Directory server

User/Endpoint Directory on Parent Control Manager Servers

Administrators of parent Control Manager can monitor entities of child servers through the **User/Endpoint Directory**. By default, child servers will sync the following information with its parent server hourly:

Note

The timing is based on the time interval setting in the `SystemConfiguration.xml`.

The default is every 30 minutes, as set by the `m_uiCasMcpChildTriggerDataSyncFreqInMin` parameter.

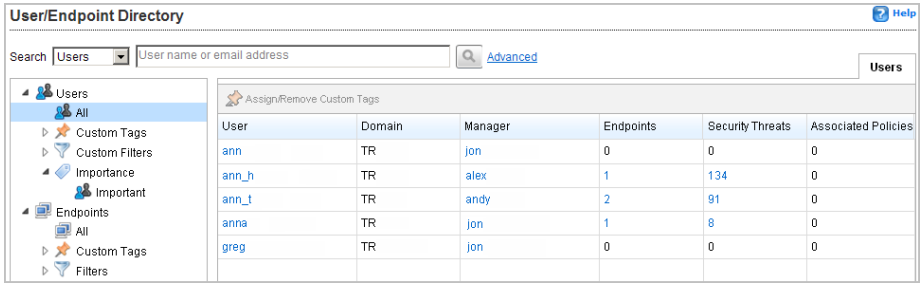
- Managed entity and physical machine relationship
- Corresponding policy of each endpoint entity
- Non-Active Directory users in the incident log

Accessing the User Tree

Procedure

1. Access the Control Manager management console.
2. Navigate to **Directories** > **Users/Endpoints**.
3. Go to **Users** > **All**.

A screen similar to the following appears:



Column Name	Description
User	The name or email address of the user depending on the endpoint: • Computer/server: The most recent user who logged on and/or used the computer/server is identified as the current owner. • Mobile device: The email address associated with the mobile device is used to find the corresponding user in Active Directory. If the corresponding AD user cannot be found or if AD synchronization is not available, the email address is used as the current owner. **Note** The **Users** > **All** node list all local users from various endpoints regardless of their duplicate status. Duplicate users having the same names can occur. Control Manager consolidates all endpoints from managed products having multiple local users.
Domain	If Active Directory integration is enabled, this corresponds to the name of the domain. Without Active Directory, the value in this column reflects the endpoint name/host name.
Manager	The user's direct reporting manager, as saved in Active Directory
Endpoints	The number of endpoints, which the user is currently logged on to or was the last one to log on.

Column Name	Description
Security Threats	The total number of threats logged in 90 days Control Manager counts and consolidates detections having these types of threats: • Virus/Malware • Spyware/Grayware • Email content violation • Spam • Phishing email • Web violation • DLP incident • C&C callback • Behavior Monitoring violation • Firewall violation • Application violation • Suspicious file • Intrusion prevention event • Network content violation For example, while Henry is the last user using endpoint `us-mkt-dev1`, there are 10 virus/malware detections and two web violations. Because Henry was the last one to use the endpoint, Henry's security threats count is 12. **Note** If the network environment is not using Active Directory the following detections/violations for gateway products do not display: email content violation, phishing email, spam. Security threats detected by endpoint products (example: OfficeScan) are tied to the last logon user of the endpoint. Security threats detected by gateway products (example: IWSVA) are tied to the user who triggered the detection.

Column Name	Description
Associated Policies	The number of policies assigned to endpoints, which the user is currently logged on to or was the last one to log on.

What to do next

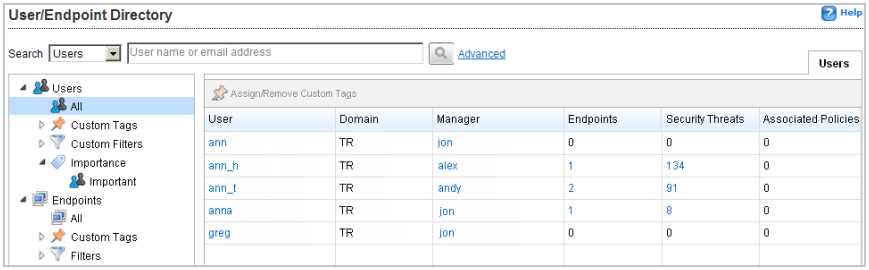
- You can perform *basic* or *advanced* search of users.
- To automatically group users by creating a *custom filter*, refer to *Creating a Custom Filter on page 4-39*.
- To manually group users by creating a *custom tag*, refer to *Creating a Custom Tag on page 4-34*

Displaying User Details

Procedure

1. *Access the User/Endpoint Directory*.
2. Do one of the following:
   - *Search for a user*.
   - Navigate to the **Users** > **All** node.
   - If you have group users according to custom tags/filters, go to the custom tag/filter of your choice.

   Here is an example displaying the **Users** > **All** node:



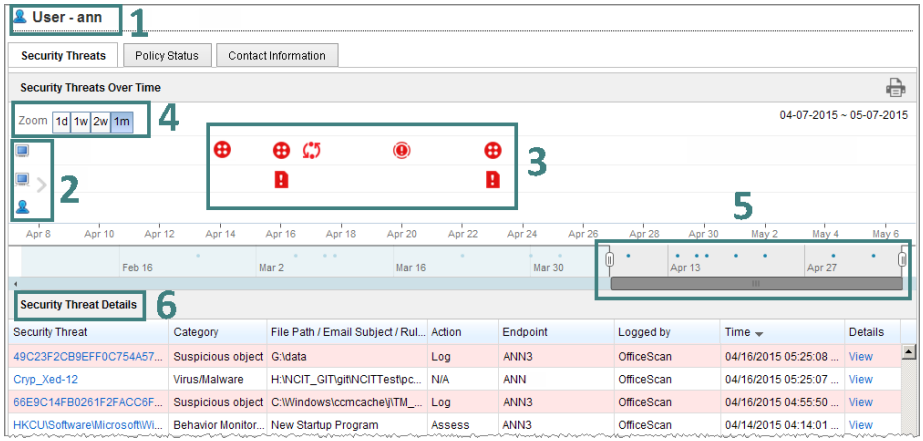
3. To display details, do one of the following:

   - Click a value in the **User** or **Manager** column to view *contact information*.
   - Click a value in the **Endpoints** column to view *endpoint details*.
   - Click a value in the **Security Threats** column to open a screen with a graph showing the distribution of *security threats* over a certain period of time.
   - Click a value in the **Associated Policy** column to view *policies* assigned to the user.

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.



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

<table>
<tr><th>Number</th><th colspan="3">Description</th></tr>
<tr><td>1</td><td colspan="3">User with endpoints that have security threats</td></tr>
<tr><td>2</td><td colspan="3">Endpoints that the user owns (represented by a monitor icon) and the user (represented by a person icon)

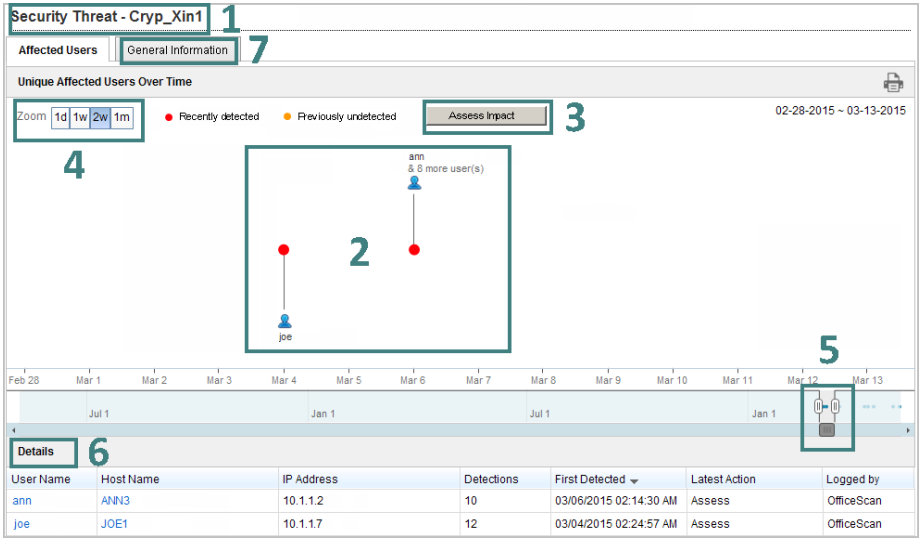
By default, the host name of an endpoint and the domain name of the user display next to the icons. Click the gray arrow to show or hide the host and domain names.</td></tr>
<tr><td rowspan="6">3</td><td colspan="3">Security threats detected on the endpoints, represented by icons

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>
</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.



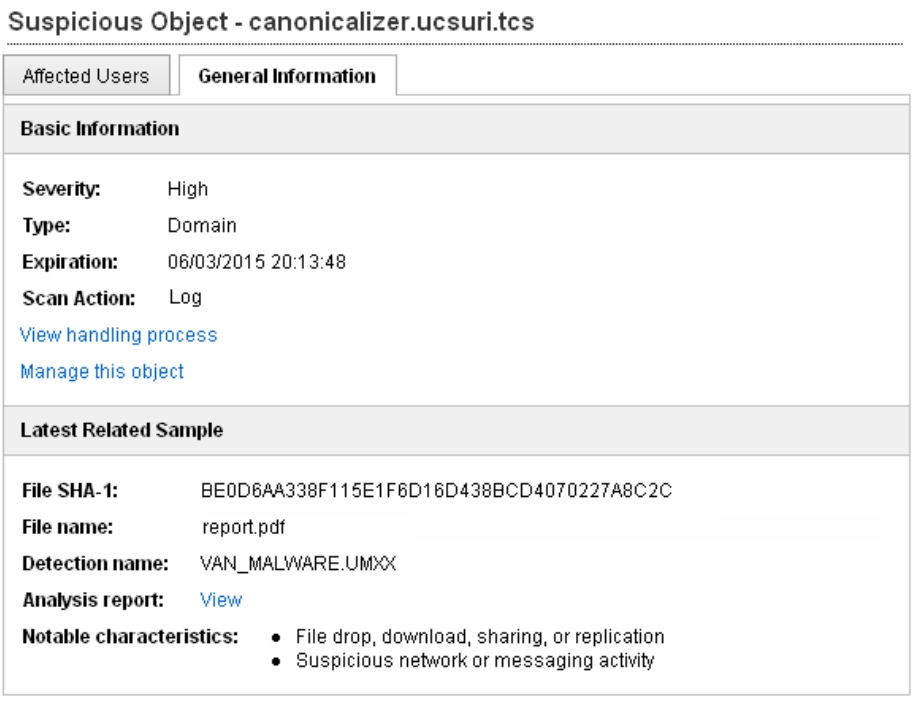
The major user interface elements in the screen are as follows:

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

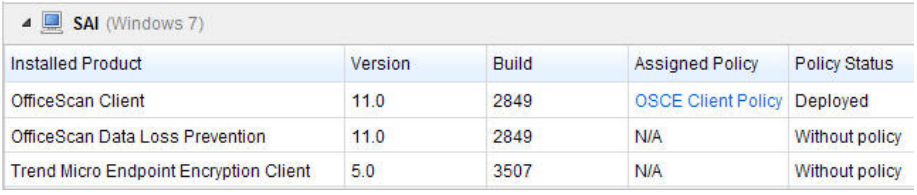
View information about a particular security threat.

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



Policy Status

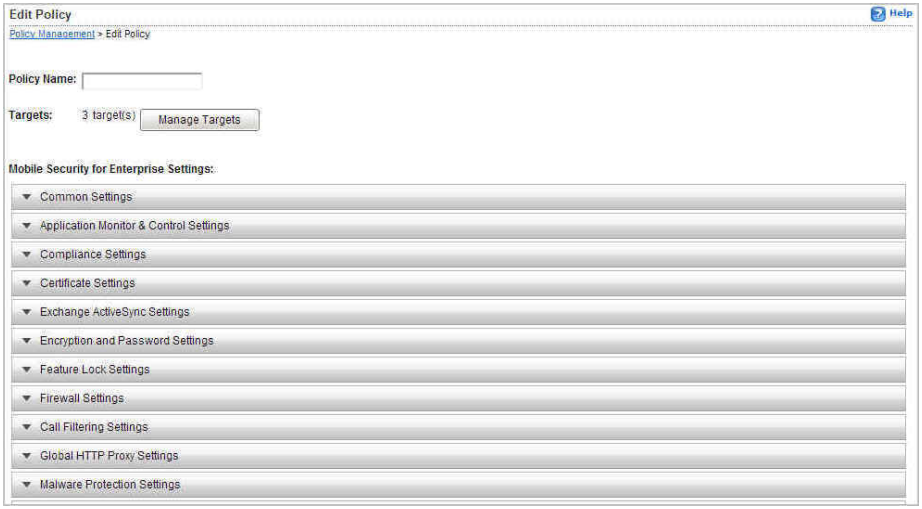
The **Policy Status** tab displays the list of policies associated with an endpoint, including the policy status, managed product where such policy originates, and the managed product's version and build.



Tip

Click the name of the assigned policy to open the specific policy page of the managed product and view/edit related settings.

For example, clicking the policy name OSCE Client Policy opens an **Edit Policy** screen similar to the following:

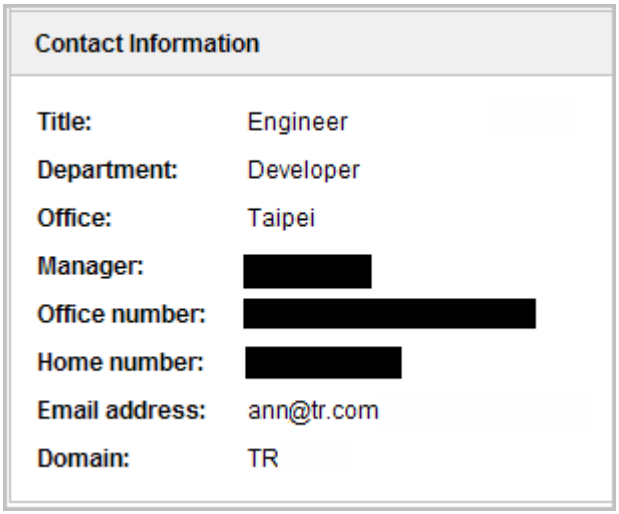


Note

In this example, if User Henry is not the policy creator, buttons that could trigger any changes to the policy (for example, **Set Filter**, **Manage Targets**, **Deploy**) are disabled on the **Edit Policy** screen. Only users with specific privileges can edit and save any changes to a policy.

Contact Information

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



Synchronizing Contact Information with Active Directory

Control Manager synchronizes data from the Active Directory Global Category (GC).

Procedure

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

- title

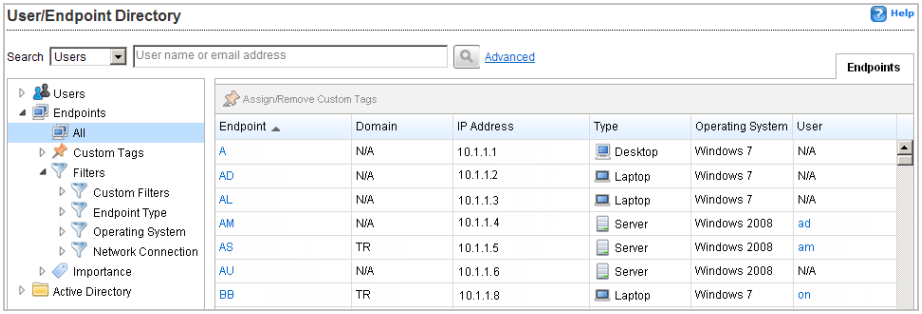
5. Wait until Active Directory replication occurs.

Accessing the Endpoint Tree

Procedure

1. Access the Control Manager management console.
2. Navigate to **Directories** > **Users/Endpoints**.
3. Go to **Endpoints** > **All**.

A screen similar to the following appears:



Column Name	Description
Endpoint	The host name or device name
Domain	If Active Directory integration is enabled, this corresponds to the name of the domain. Without Active Directory, the value in this column is N/A.
IP Address	The static or dynamic IP address of the endpoint

Column Name	Description
Type	Machine or device type: server, desktop, laptop, mobile device, and others
Operating System	The operating system running on the machine or device: supported Windows desktop/server systems, Mac OS, iOS, Android, Symbian, and Windows Mobile
User	The name or email address of the most recent user who logged on and/or use the endpoint

What to do next

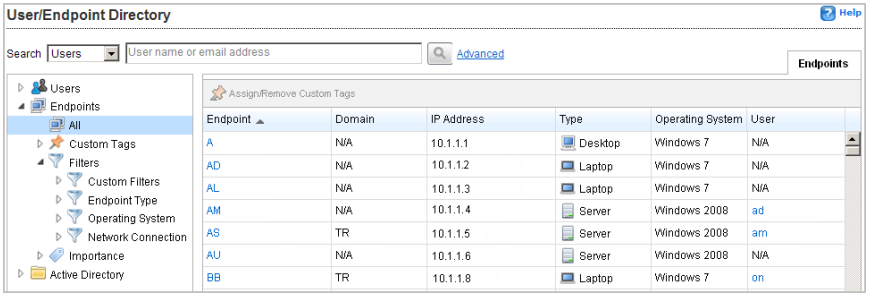
- Sort the results by clicking any of the column headers. The icon  placed next to the header indicates that the Endpoint table is sorted according to this column.
- You can perform *basic* or *advanced* search of endpoints.
- To automatically group endpoints by creating a *custom filter*, refer to *Creating a Custom Filter on page 4-39*.
- To manually group endpoints by creating a *custom tag*, refer to *Creating a Custom Tag on page 4-34*

Displaying Endpoint Details

Procedure

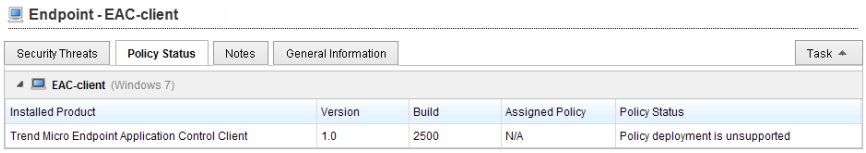
1. *Access the Endpoint tree*.
2. Do one of the following:
   - *Search for an endpoint*.
   - Navigate to the **Endpoint** > **All** tree.

A screen similar to the following appears:



3. To display endpoint details, click a value in the **Endpoint** column.

4. In the Endpoint Screen that opens (with the **Policy Status** tab shown by default):



   a. View *policies*.

   b. Click the *Security Threats*, *Notes*, or *General Information* tab to view other endpoint details.

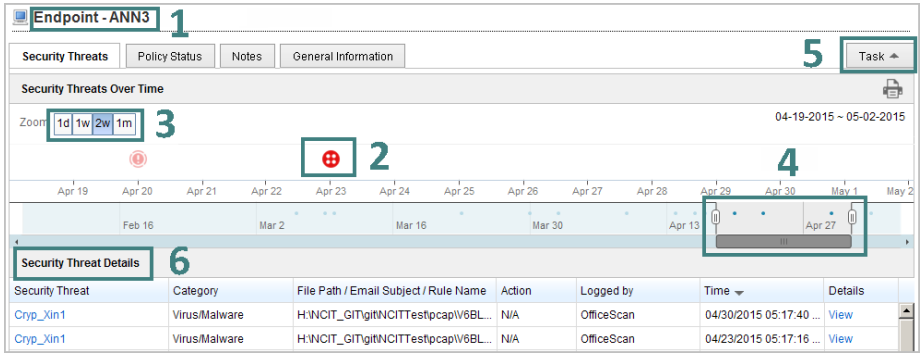
   c. At the top right corner of the screen, click **Task** and then select **Assign tags** or **Isolate**. For details about assigning tags, see *Working with Custom Tags on page 4-34*. For details about isolating endpoints, see *Endpoint Isolation and Connection Restoration on page xxxix*.

5. Click a value in the **User** column to view the user's *contact information*.

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.



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

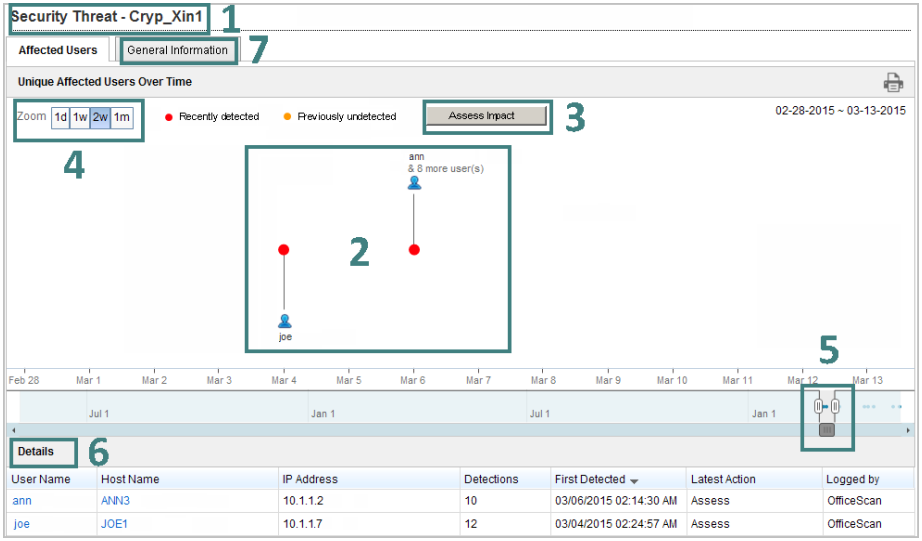
Number	Description
1	Endpoint with security threats An icon displays after the endpoint name (as shown below) if Control Manager has *isolated* the endpoint or is in the process of restoring its network connection. 

<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 colspan="4"></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
• Isolate endpoint</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.



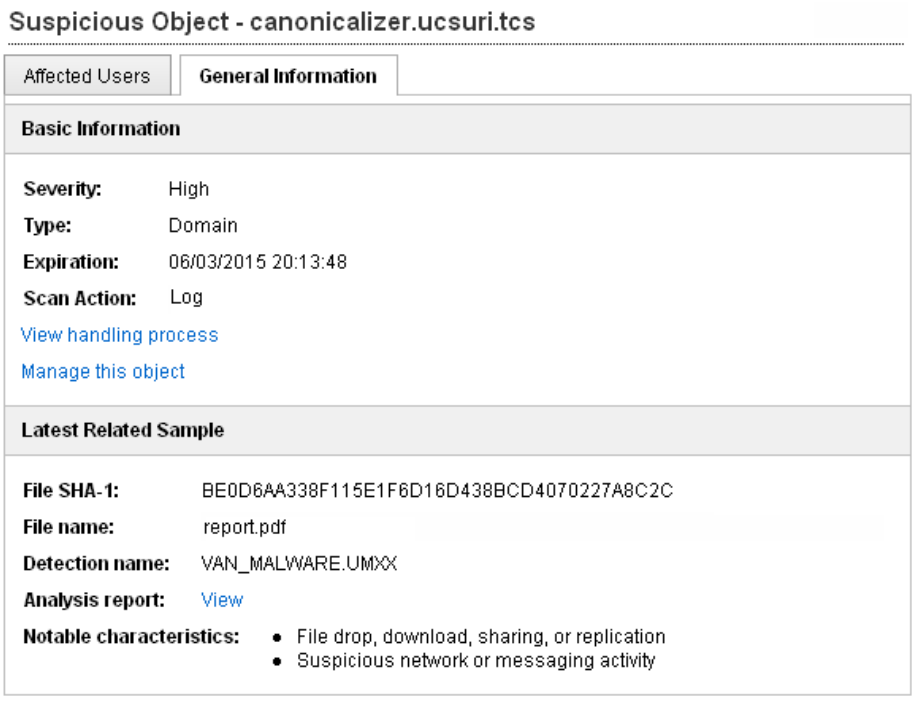
The major user interface elements in the screen are as follows:

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

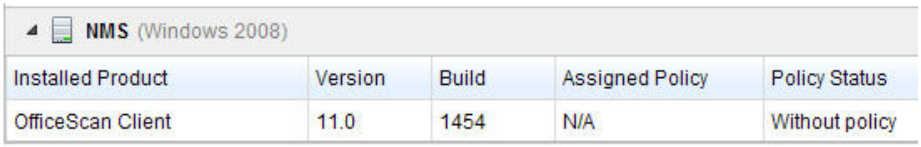
View information about a particular security threat.

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



Policy Status

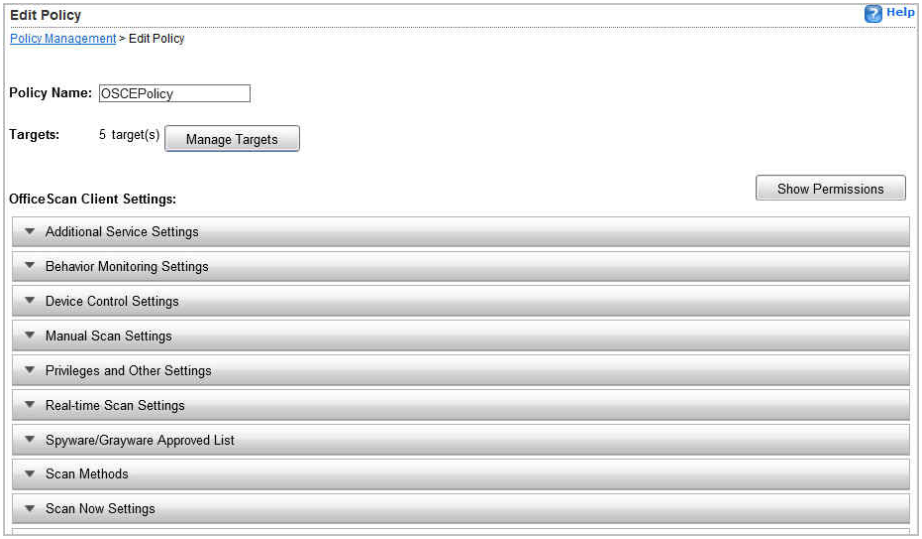
The **Policy Status** screen displays the list of policies associated with an endpoint, including the policy status, managed product where such policy originates, and the managed product's version and build.



Tip

Click the name of the assigned policy to open the specific policy page of the managed product and view/edit related settings.

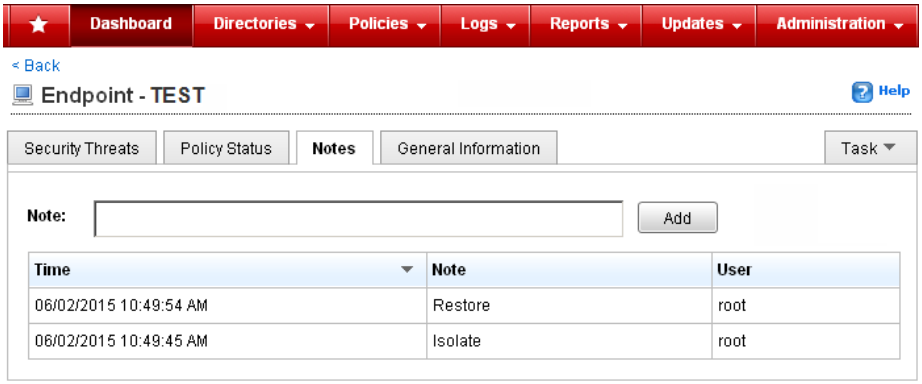
For example, clicking the policy name OSCEPolicy opens an **Edit Policy** screen similar to the following:



Notes for Endpoints

The following notes are automatically added to this screen:

- **Isolate**: *Endpoint isolated*
- **Restore**: Network connection restored
- **Assign Tag {tag name}**: *Custom tag* assigned to the endpoint
- **Remove Tag {tag name}**: Custom tag unassigned from the endpoint

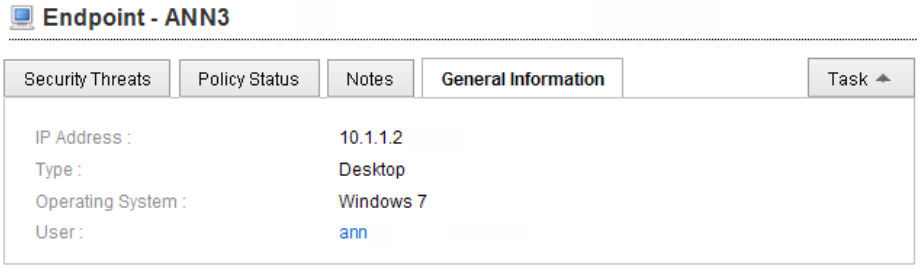


Manually add notes, especially as you perform actions on particular endpoints. For example, add additional notes on isolated endpoints while you are investigating and resolving threats or when you are about to restore the network connection after all threats have been resolved.

Each note is added to the table on the screen. The table also shows the date and time the note was added and the user who added the note.

General Information for Endpoints

View information about the endpoint, such as its IP address, type, operating system, and the user associated with it.



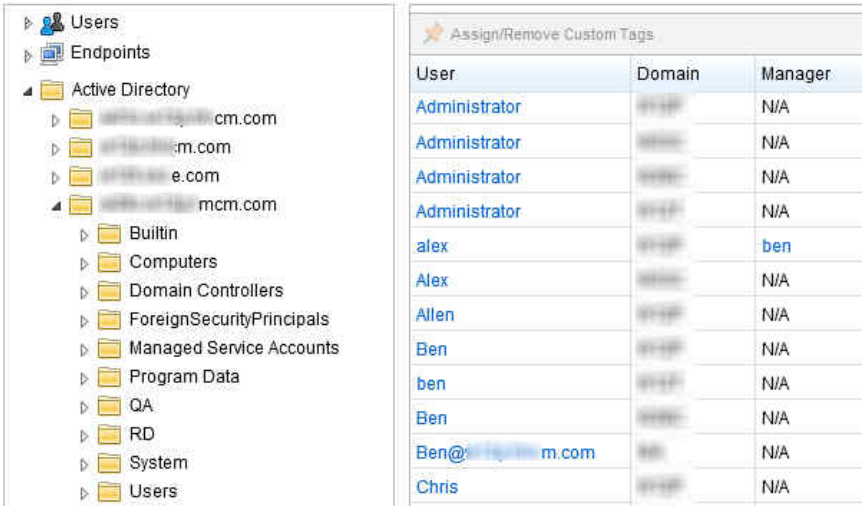
Understanding the Active Directory Synchronization

If your organization runs Active Directory and its organization meets your management needs, integrate with your Active Directory to populate and map the User/Endpoint Directory according to your existing organizational structure. Once synchronized, Control Manager updates the User/Endpoint Directory with any new users/groups from your Active Directory.

Take note of the following considerations when *enabling this feature on page 8-10*:

- Control Manager supports synchronization of Active Directory domains coming from the same forest.

  The following example shows the **Active Directory** tree with multiple domains from the same forest:



- If there are duplicate users created from endpoints as local users and Active Directory members, Control Manager removes duplicates by listing all Active Directory users.

Note

Control Manager consolidates all users—with duplicate and unique names. Having duplicate users listed in the **Users/Endpoint Directory** is possible because endpoints such as computers, servers, or laptops can have multiple local accounts with the same name.

To configure the Active Directory connection, refer to *Configuring Active Directory and Endpoint Protection Verification Widget Settings on page 8-10*.

Accessing the Active Directory Tree

Before you begin

Enable Active Directory synchronization on page 4-24 to view the Active Directory tree.

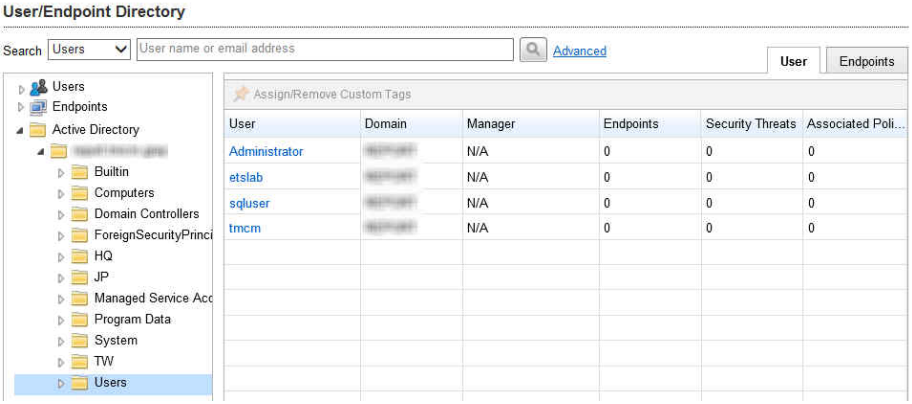
The Active Directory tree has the following characteristics:

- It varies depending on your network and organizational setup
- Provides two tabs, **Users** and **Endpoints**, to enable quick access to user or endpoint information and security details

Procedure

1. Access the Control Manager management console.
2. Navigate to **Directories** > **Users/Endpoints**.
3. Go to **Active Directory**, and expand the folders to display available items.

A screen similar to the following appears:



Refer to the following table for details:

Column Name	Description
User	The name or email address of the user Click the name to open the **User Details** > **Contact Information** screen. Refer to *Displaying User Details on page 4-6* for details. **Note** With Active Directory integration disabled, the **Users** > **All** tree list all local users from various endpoints regardless of their duplicate status. Users having the same user names can occur as computers/servers/laptops can have multiple local users.
Domain	If Active Directory integration is enabled, this corresponds to the name of the domain. Without Active Directory, the value in this column reflects the endpoint name/host name.
Manager	The user's direct reporting manager, as saved in Active Directory
Endpoints	The number of endpoints, which a user is currently logged on.

Column Name	Description
Security Threats	The number of security threats detected over 90 days Click the value to display the **User Details** > **Security Threats** screen. Refer to *Displaying User Details on page 4-6*for details. Control Manager counts and consolidates detections having these types of threats: • Virus/Malware • Spyware/Grayware • Content violation • Spam • Phishing email • Web violation • DLP incident • C&C callback • Behavior Monitoring violation • Firewall violation For example, while `Henry` is using endpoint `us-mkt-dev1`, there are 10 virus/malware detections and two web violations. Therefore, Henry's security threats count is 12.
Associated Policies	The number of *Control Manager policies on page 17-2* assigned to the user Click the value to display the **User Details** > **Policy Status** screen. Refer to *Displaying User Details on page 4-6* for details.

Troubleshooting Issues Related to Active Directory Integration

Active Directory integration allows you to manage Active Directory information through the *User/Endpoint Directory on page 4-1* of the Control Manager console.

In an event when an error appears on the **Dashboard**, refer to the following list to help try and troubleshoot the issue:

Procedure

- Network connectivity, including the network firewall settings

  Ensure that both the Control Manager and Active Directory servers can establish communication with one another.

- User name and password to access the Active Directory server

  Ensure that the *account information on page 8-10* used is correct and has enough privileges to access the Active Directory server.

- Control Manager database status and connectivity

  Check whether the connection to the *Control Manager database on page 20-2* is present.

What to do next

If the issue persists, please contact *Support on page 24-2*.

Searching for Users or Endpoints

Control Manager uses partial matching to conduct the following functionalities:

- *Basic search on page 4-30*: quickly search for users or endpoints using a single keyword
- *Advanced search on page 4-31*: include Boolean operators and multiple keywords based on the available user/endpoint categories

Tip

Refer to *Advanced Search Categories on page 4-29* for the list of categories available when performing a search.

Advanced Search Categories

Users

Use any of the following categories applicable to advanced searches:

TABLE 4-1. User Categories

CATEGORY	DESCRIPTION
User name	The account name of local users or people belonging to an Active Directory structure
Direct manager	The account name of the person who users are assigned to report to
Location in Active Directory	The organization unit from which to begin your search
Department	The name of the department in your company that groups users based on their functionalities (for example, Accounting)
Active Directory Group	A collection of Active Directory user and computer accounts, contacts and other groups that can be managed as a single unit

Endpoints

Use any of the following categories when searching for endpoints:

TABLE 4-2. Endpoint Categories

CATEGORY	DESCRIPTION
Endpoint name	The host or device name of the endpoint
IP address	The IPv4 address range **Note** Searching by IPv4 segment requires a specific range starting with the first octet. The search returns all endpoints with IP addresses containing that entry.

CATEGORY	DESCRIPTION
Endpoint type	The type of computer or device: server, desktop, laptop, mobile device, or other
Operating system	The type of operating system: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 2000, Windows 2003, Windows 2008, Windows 2012, Mac OS, iOS, Android, Symbian, Windows Mobile, or others
Location in Active Directory	The organization unit from which to begin your search

Using the Basic Search

Use this feature to quickly search for users or endpoints one keyword at a time. Control Manager uses partial matching when returning and displaying results.

Procedure

1. *Access the User/Endpoint Directory on page 4-3*.
2. On the top-most part of the screen, above the tree and working pane, click the **Search** drop-down list to search for users or endpoints.

FIGURE 4-1. Basic user search

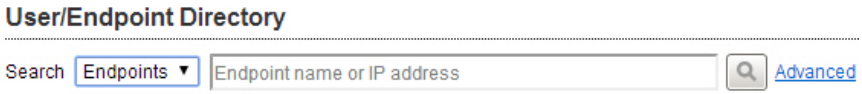


FIGURE 4-2. Basic endpoint search

Note

Control Manager can only search for IPv4 addresses.

3. Type the keywords in the field provided.

   For example, use the *user name* or *email address* criterion to search for users having the same mail server (like `@yourdomain.com`)

Tip

To search for endpoints based on an IPv4 range, use *Advanced on page 4-31* search.

4. Press **Enter** or the Search icon 
   .

The entries that match the characters you typed are displayed. Control Manager filters users or endpoints from the **Users**, **Endpoints**, or **Active Directory** tree that partially match the keywords entered.

Related information

↪ *Using the Advanced Search*

Using the Advanced Search

This feature provides the following functionalities:

- Search using operators that allow you to find an item from your tree quickly and accurately
- Set up filters so that you can organize your tree automatically

Procedure

1. Search for users or endpoints. Refer to *Using the Basic Search on page 4-30* for steps.

Refer to *Advanced Search Categories on page 4-29* for the list of categories available when performing a search.

2. Click

   Advanced

   .

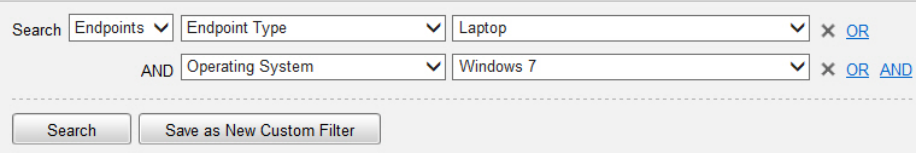
3. Use any or all of the following Boolean operators:

   - AND: all conditions must exactly match to display the results
   - OR: any of the matching conditions will prompt Control Manager to display the results

4. Click **Search** to display results.

   Alternatively, click **Save as New Custom Filter** to use the specified criteria to build the new custom filter. Doing so will prompt Control Manager to automatically group users or endpoints that match your specified criteria into this new custom filter.

For example, to search for laptops running Microsoft Windows 7, follow these settings:



Understanding Custom Tags and Filters

With tags or filters, you can:

- View a list of users and actionable information such as associated security threats, policy status, and contact information per user
- View a list of endpoints and policy status per endpoint
- View a timeline chart for incident investigation

Tip

The **User Access Information** in an ad hoc query (see *Understanding Ad Hoc Queries on page 11-12*) provides details about any user modifications related to any available custom tags or filters.

General Recommendations

Tagging or filtering users or endpoints depend on your network and management needs, along with your business plans. As general recommendations:

- The **User Access Information** in an ad hoc query (see *Understanding Ad Hoc Queries on page 11-12*) provides details about any user modifications related to any available custom tags or filters
- Group users based on your Active Directory organization
- Group endpoints based on their location (that is, their IP ranges)
- Group users or endpoints with similar properties or characteristics

  For example: who manages a group of users, who accesses a group of servers, endpoints with the same operating system type or host names
- Group users or endpoints based on any other criteria that support your needs

  For example, it is a common practice to divide networks according to the roles of those using the network—Marketing, Finance, Human Resources, Product Development, etc.

Tip

Plan your User/Endpoint Directory structure and consider your network environment to simplify maintenance—especially for an enterprise with a large network.

Manually tag users or endpoints showing a specific behavior. For example, as the network administrator for Company ABC, Joni sees similar malware behavior resulting from laptops XYZ and 123. She can then tag laptops XYZ and 123 for easy identification.

Consequently, create filters to group users or endpoints based on specific known characteristics. For example, filter users based on who their manager is. You can then associate a filter to those users having the same manager.

Working with Custom Tags

Custom tags are labels that you can manually associate with one or more users/endpoints. Create custom labels to group certain users or endpoints. Control Manager offers the following features related to tags:

- By default, all users and endpoints have no tags association
- Manually apply one or more tags to one or more users/endpoints
- All users with access to the User/Endpoint Directory can create/edit/delete/view tags

  Note

  A user can only delete or modify the tags he/she created.

- Only the user account that installed Control Manager can delete/modify/view all users' tags

  For example, the Root account.

Creating a Custom Tag

Procedure

1. *Access the User/Endpoint Directory on page 4-3*, and then navigate to the **Users** or **Endpoints** tree.
2. Do one of the following:
   - From the User/Endpoint Directory pane:

a. Navigate to the **Custom Tags** node, and then click

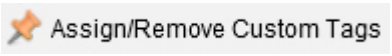
.

b. Type a descriptive name, and press Enter or click

to save the new tag.

- From the list of the **All** users/endpoints displayed on the working pane:

a. Click anywhere on the user or endpoint row, and then click



.

Alternatively, right-click anywhere on the row, and then select **Assign/Remove Custom Tags** from the popup menu.

b. On the **Assign/Remove Custom Tags** dialog, type a descriptive **name**, and then click **Save**.

Note

If you click the link on the **User** or **Endpoint** column, a screen displaying details about that item appears.

The tag is added to the list of tags under the corresponding **User** or **Endpoint** tree.

What to do next

Click the

icon on any custom tag to edit the tag name.

Deleting a Custom Tag

Procedure

1. *Access the User/Endpoint Directory on page 4-3*, and then navigate to the **Users** or **Endpoints** tree.
2. On the tree pane, hover your mouse over the tag that you want to delete, and then click
   
   .

The tag is deleted from the list of **Custom Tags** under the corresponding **User** or **Endpoint** tree.

Applying a Custom Tag to Selected Users/Endpoints

Procedure

1. *Access the User/Endpoint Directory on page 4-3*, and then navigate to the **Users** or **Endpoints** tree.
2. Select the user or endpoint, and then right-click or click **Assign/Remove Custom Tags** to select a tag (or more than one tags) from the dialog. Alternatively, you can create a new tag and assign the new tag to selected users/endpoints.

   
   Note

   Use `Ctrl + Click` to select multiple users/endpoints.
3. In the **Assign/Remove Custom Tags** dialog, select the desired tag(s) from the list, and then click **Save**.

Verify that certain users or endpoints are associated with a tag. Select a tag from the **Customs Tags** list, and then ensure that the user or endpoint you have just associated is listed.

Disassociating a Custom Tag from Selected Users/ Endpoints

Procedure

1. *Access the User/Endpoint Directory on page 4-3*, and then navigate to the **Users** or **Endpoints** tree.
2. Click **Assign/Remove Custom Tags** or right-click the user or endpoint, and then select **Assign/Remove Custom Tags**.
3. In the **Assign/Remove Custom Tags** dialog, deselect the desired tag(s) from the list, and then click **Save**.

Verify that certain users or endpoints are no longer associated with a tag. Select a tag from the **Customs Tags** list, and then ensure that the user or endpoint you have just disassociated is not listed.

Working with Filters

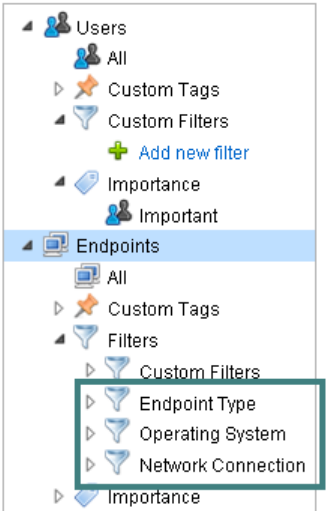
Filters automatically group users or endpoints having the same criteria.

The **Users** and **Endpoints** tree can group users based on *custom filters* and *importance*, as configured by administrators.

In addition, the **Endpoints** tree can group endpoints based on *default filters*.

Default Endpoint Filters

By default, the **Endpoints** tree provides default filters based on the typical grouping of endpoints in an organization.



Clicking a filter criteria updates the table in the main screen with the list of endpoints or users that match the criteria. For details about the table columns and the data they contain, see *Accessing the User Tree on page 4-3*.

The following are the default filters:

- **Endpoint Type**: Servers, desktops, laptops, mobile devices, and other types
- **Operating System**: Popular operating systems that can be installed on endpoint types, including Windows, Mac OS, iOS, Android, and other operating systems.
- **Network Connection**: Endpoints that have been manually isolated by Control Manager administrators so that threats in these endpoints can be resolved. For information on isolating endpoints, see *At-risk Endpoints Tasks on page 19-16*.

Note

If you click the **Isolated** filter, you have the additional task of undoing the isolation on endpoints that are now threat-free. To do so, select the endpoints and click **Restore Network Connection**.

Creating a Custom Filter

Procedure

1. *Access the User/Endpoint Directory on page 4-3*, and then navigate to the **Users** or **Endpoints** tree.

2. Navigate to the **Custom Filters** folder, and then click

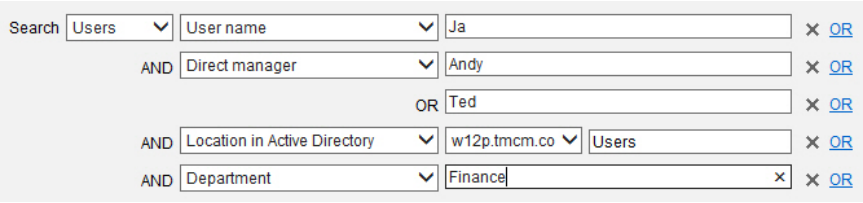
   Add new filter

   .

3. Filter users or endpoints based on the available characteristics.

   Refer to *Advanced Search Categories on page 4-29* for the list of categories available when performing a search.

   The following example filters all "`Ja`" users in the Active Directory `w12p.tmcm.co`:



What to do next

Click the

icon on any custom filter to edit the filter name. To update the Boolean expressions per custom filter, click

and update the condition(s).

Deleting a Custom Filter

Procedure

1. *Access the User/Endpoint Directory on page 4-3*, and then navigate to the **Users** or **Endpoints** tree.
2. On the tree pane, hover your mouse over the custom filter that you want to delete, and then click
   
   .

The custom filter is deleted from the list of **Custom Filters** under the corresponding **User** or **Endpoint** tree.

Working with User or Endpoint Importance

Assign importance to groups of users and endpoints. For example, assign external-facing servers as important so you can apply a strict policy to these servers and constantly monitor their protection status.

To assign importance, first create *custom tags* or *filters*. You can then assign importance to endpoints or users with the custom tags or returned by the custom filter.

- By default, all users and endpoints are not assigned importance.
- Manually assign importance to one or more custom tags and custom filters.
- All users with access to the User/Endpoint Directory can assign or unassign importance.

Procedure

1. *Access the User/Endpoint Directory*, and then navigate to the **Users** or **Endpoints** tree.

2. Navigate to the **Importance** node, mouseover **Important**, and then click  .

3. In the popup window that displays:

   - Assign importance by selecting one or several custom tags and custom filters and then clicking **OK**.
   - Unassign importance by clearing one or several custom tags and custom filters and then clicking **OK**.

   The table in the main screen is updated with the list of endpoints or users that match the custom tags or custom filters. For details about the table columns and the data they contain, see *Accessing the User Tree on page 4-3*.

Chapter 5

Product Directory Basics

The Product Directory displays all managed products registered to a Control Manager server.

This chapter contains the following topics:

Understanding the Product Directory

A managed product is a representation of an antivirus, content security, or web protection product in the Product Directory. Managed products display as icons (for example, [] or []) in the Control Manager web console **Product Directory** section. These icons represent Trend Micro antivirus, content security, and web protection products. Control Manager supports dynamic icons, which change with the status of the managed product. See your managed product's documentation for more information on the icons and associated statuses for your managed product.

Indirectly administer the managed products either individually or by groups through the Product Directory. The following table lists the menu items and buttons on the **Product Directory** screen.

TABLE 5-1. Product Directory Options

OPTIONS	DESCRIPTION
Menu Items	
Advanced Search	Click this menu item to specify search criteria to perform a search for one or more managed products.
Configure	After selecting a managed product/directory, move the cursor over this menu item and select a task, to log on to a web-based console using SSO or to configure a managed product.
Tasks	After selecting a managed product/directory, move the cursor over this menu item and select a task, to perform a specific function (such as deploying the latest components) to a specific managed product or child server or groups of managed products or child servers. Initiate a task from a directory and Control Manager sends requests to all managed products belonging to that directory.
Directory Management	Click this button to open the **Directory Management** screen. From the screen, move entities/directories (by dragging and dropping them) or create new directories.
Buttons	

OPTIONS	DESCRIPTION
Search	Click this button, after typing a managed product's name, to perform a search for the specified managed product.
Status	Click this button, after selecting a managed product/directory, to obtain status summaries about the managed product or managed products found in the directory.
Folder	Click this button, after selecting a directory, to obtain status summaries about the managed products and the managed product endpoints found in the directory.

Note

Managed products belonging to child Control Manager servers cannot have tasks issued to them by the parent Control Manager server.

Grouping Managed Products Using Directory Management

Use the **Directory Management** screen to customize the Product Directory organization to suit your administration model's needs. For example, you can group products by location or product type (messaging security, web security, file storage protection).

Group managed products according to geographical, administrative, or product specific reasons. In combination with different access rights used to access managed products or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages:

TABLE 5-2. Advantages and Disadvantages when Grouping Managed Products

GROUPING TYPE	ADVANTAGE	DISADVANTAGE
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match

Grouping Type	Advantage	Disadvantage
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

Product Directory Structure Recommendations

Trend Micro recommends the following when planning your Product Directory structure for managed products and child servers:

Table 5-3. Considerations when Grouping Managed Products or Child Servers

Structure	Description
Company network and security policies	If different access and sharing rights apply to the company network, group managed products and child servers according to company network and security policies.
Organization and function	Group managed products and child servers according to the company's organizational and functional division. For example, have two Control Manager servers that manage the production and testing groups.
Geographical location	Use geographical location as a grouping criterion if the location of the managed products and child servers affects the communication between the Control Manager server and its managed products or child servers.
Administrative responsibility	Group managed products and child servers according to system or security personnel assigned to them. This allows group configuration.

The Product Directory provides a user-specified grouping of managed products which allows you to perform the following for administering managed products:

- Configuring managed products
- Request products to perform a Scan Now (if this command is supported)
- View product information, as well as details about its operating environment (for example, product version, pattern file and scan engine versions, operating system information, and so on)

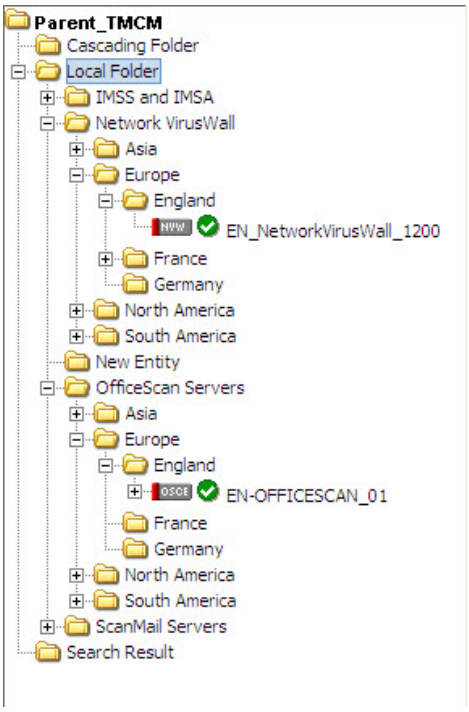
- View product-level logs
- Deploy virus pattern, scan engine, anti-spam rule, and program updates

Plan this structure carefully, because the structure also affects the following:

TABLE 5-4. Considerations for the Structure

CONSIDER	EFFECT
User access	When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire directory. Granting access to a specific managed product only grants access to that specific product.
Deployment planning	Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments	OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

A sample Product Directory appears below:



Managed products identify the registered antivirus or content security product, as well as provide the connection status.

Note

If the location is unspecified during registration, on-premise managed products appear in the **New Entity** folder.

SaaS solutions use **New Entity** during registration, and appear in Directory Management.

TABLE 5-5. Managed Product Icons

ICON	DESCRIPTION
	OfficeScan Corporate Edition
	ServerProtect Information Server
	ServerProtect Domain
	ServerProtect for Windows (Normal Server)
	ServerProtect for NetWare (Normal Server)
	InterScan Messaging Security Suite

Icon	Description
	InterScan Web Security Suite
	InterScan VirusWall for Windows
	ScanMail for Microsoft Exchange
	ScanMail for Lotus Notes/Domino
	Network VirusWall
	Managed Product connection status icon

Arrange the Product Directory using the Directory Manager. Use descriptive folder names to group your managed products according to their protection type or the Control Manager network administration model.

Default Folders for the Product Directory

After a fresh Control Manager installation, the Product Directory initially consists of the following directories:

Table 5-6. Product Directory Default Folders

Structure	Description
Root	All managed products and child Control Manager servers fall under the Root directory.
Cascading Folder	In a cascading environment, all child servers for the parent server appear in the Cascading Folder.
Local Folder > New Entity	Newly registered managed products handled by Control Manager agents usually appear in the New Entity folder.
Search Result	When performing a basic or advanced search, all managed products that fit the search criteria display in the Search Result folder.

Accessing the Product Directory

Use the Product Directory to administer managed products registered to the Control Manager server.

Note

Viewing and accessing the folders in the Product Directory depends on the Account Type and user account access rights.

Procedure

- Click **Directories** > **Products** from the main menu.

  The **Product Directory** screen appears.

Understanding Cascading Management

Control Manager Advanced provides a cascading management structure, which allows control of multiple Control Manager servers, known as child servers, from a single parent server.

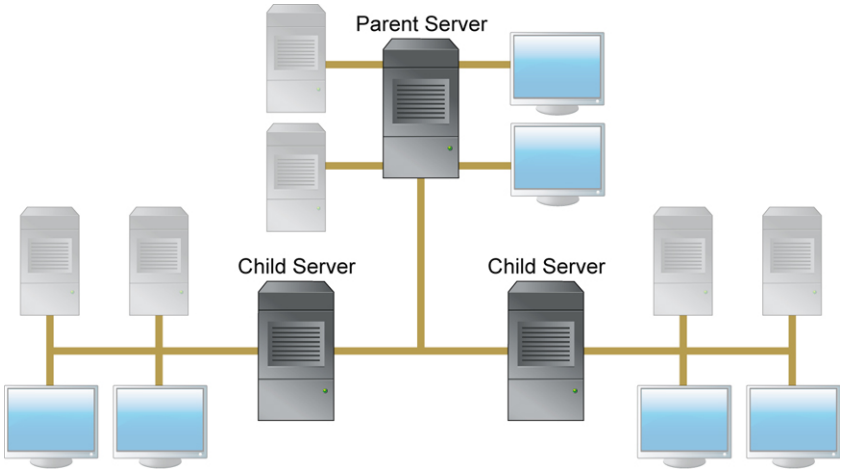


FIGURE 5-1. The cascading management structure uses two-tier parent-child architecture

A parent server is a Control Manager server that manages Standard or Advanced Edition Control Manager servers, referred to as child servers. A child server is a Control Manager server managed by a parent server.

Note

Control Manager 6.0 Service Pack 3 Advanced supports the following as child Control Manager servers:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

TABLE 5-7. Parent and Child Server Feature Comparison

FEATURE	AVAILABLE IN PARENT	AVAILABLE IN CHILD
Support two-tier cascading structure	●	●
Manage Advanced servers	●	
Administer managed products	●	●
Handle multiple child servers	●	
Issue global tasks	●	
Create global reports	●	

Note

A parent server cannot register itself to another parent server. In addition, both parent and child servers cannot perform dual roles (become a parent and child server at the same time).

The Product Directory structure, using the Control Manager web console, allows system administrators to manage, monitor, and perform the following actions on all child servers belonging to a parent server:

- Using Control Manager widgets, monitor the Antivirus, Content Security, and Web Security summaries
- Query logs
- Initiate tasks
- View reports
- Access the child server web console

The Product Directory structure can effectively manage your organization's antivirus and content security products (nationwide or worldwide).

Chapter 6

Working with Managed Servers

The **Managed Servers** screen shows the servers administrators can manage using policy management.

This chapter contains the following topics:

Understanding Managed Servers

Use the **Managed Servers** screen to add and edit managed products.

Note

When the **Add** button is disabled, this implies that the managed product is registered using the MCP agent.

For managed products, Control Manager uses the Single Sign-on (SSO) function to access these products by default.

Note

Control Manager is able to support solutions with or without management consoles. Those products or services having their own consoles use SSO.

Administrators can edit the authentication information for the following reasons:

- The SSO function does not function properly
- Administrators want to access the managed product using another account

TABLE 6-1. Managed Server List

MENU ITEM	DESCRIPTION
Server	Displays the server name of the managed product.
Display Name	Displays the server display name of the managed product.
Product	Displays the name of the managed product.

MENU ITEM	DESCRIPTION
Connection Type	Displays how the managed product registers to Control Manager. • **Automatic**: The managed product registers to Control Manager through an MCP agent. • **Manual**: Administrators manually added the managed product to the **Managed Servers** screen. • **Cloud Service**: Corresponds to the SaaS solutions that can be managed by Control Manager.  **Note** As of the Control Manager 6.0 Service Pack 1 release, Managed Servers can support Hosted Email Security, InterScan Web Security as a Service, and Worry-Free Business Security Services. A managed product's connection type is Cloud Service if it is registered through **Cloud Service Settings**. See details in *Configuring the Cloud Service Settings on page 6-6*.
Last Report	Shows the date and time when Control Manager received a response from the managed product.
Actions	• **Edit**: Click this icon to update the server information. • **Delete**: Click this icon to delete a manually added server.

Adding a Server

Procedure

1. Navigate to Administration > Managed Servers.

   The Managed Servers screen appears.

2. Select a server type.

3. Click Add.

The **Add Server** screen appears.

4. Type the server name in the **Server** field.
5. Specify a **display name** in the field provided.
6. Provide the **user name** and **password** for the managed product.

   An account with administrator privileges is required for Control Manager to deploy policy settings.
7. Select **Use a proxy server for the connection**.

   See *Configuring Proxy Settings for Managed Products on page 6-5* for details about setting up the proxy server connection.
8. Click **Save**.

Note

To perform policy management on a new managed product, move the managed product from the **New Entity** folder to another folder in the **Directory Management**.

Editing a Server

Procedure

1. Navigate to **Administration** > **Managed Servers**.

   The **Managed Servers** screen appears.
2. Select a server type.
3. Click the **Edit** icon in the **Actions** column.
4. Edit the server information.
5. Click **Save**.

Deleting a Server

Procedure

1. Navigate to **Administration** > **Managed Servers**.

   The **Managed Servers** screen appears.

2. Select a server type.

3. Click the **Delete** icon in the **Actions** column.

4. Agree to the prompt to continue.

The deleted server is removed from the list. The server program and related agents remain intact. However, they no longer report any information to Control Manager.

Configuring Proxy Settings for Managed Products

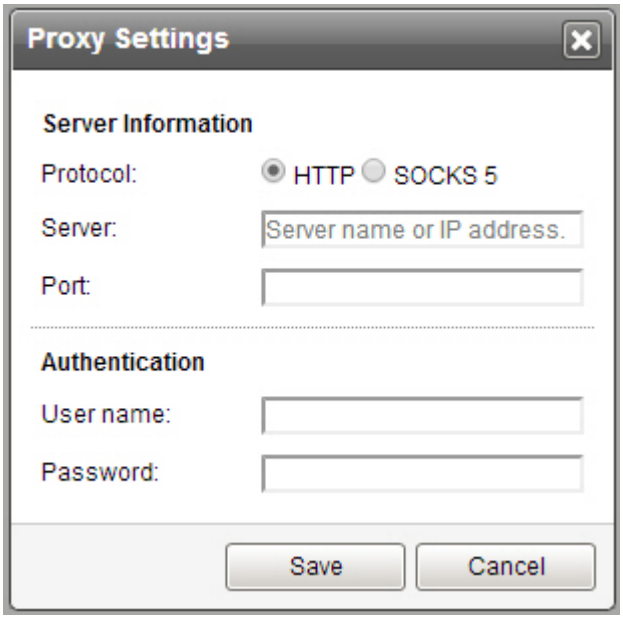
Use a proxy server to connect to the managed products.

Procedure

1. Navigate to **Administration** > **Managed Servers**.

   The **Managed Servers** screen appears.

2. Click **Proxy Settings**.



3. Select the protocol:
   - HTTP
   - SOCKS 5
4. Type the server name in the **Server** field.
5. Type the port number in the **Port** field.
6. Type the user name and password to access the server if it requires authentication.
7. Click **Save**.

Configuring the Cloud Service Settings

Use the **Managed Servers** screen to register or unregister any of your SaaS solutions as one of the managed cloud services in Control Manager.

Procedure

1. Navigate to **Administration** > **Managed Servers**.

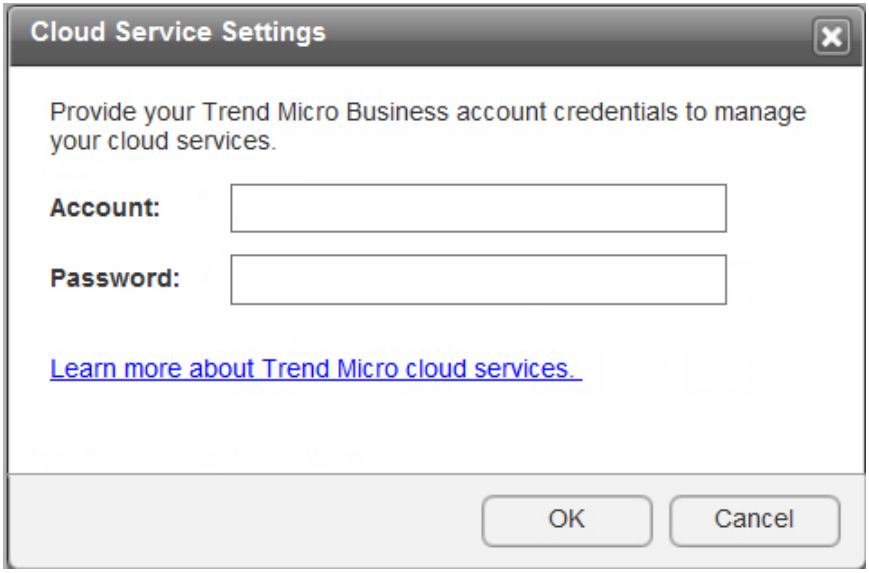
   The **Managed Servers** screen appears.

2. Click

   .

   The following **Cloud Service Settings** dialog appears:



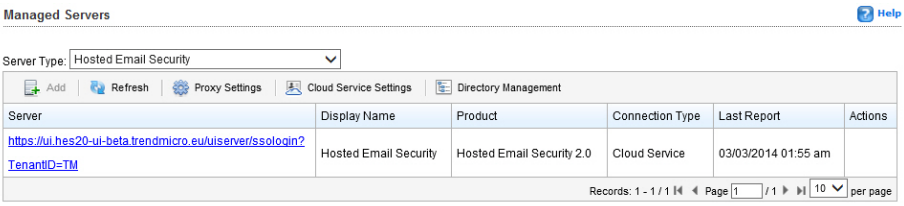
3. Supply the following details:

   - **Account**: user name set via the Trend Micro Customer Licensing Portal during activation of your service subscription
   - **Password**: password for this account

4. Click **OK** to save.

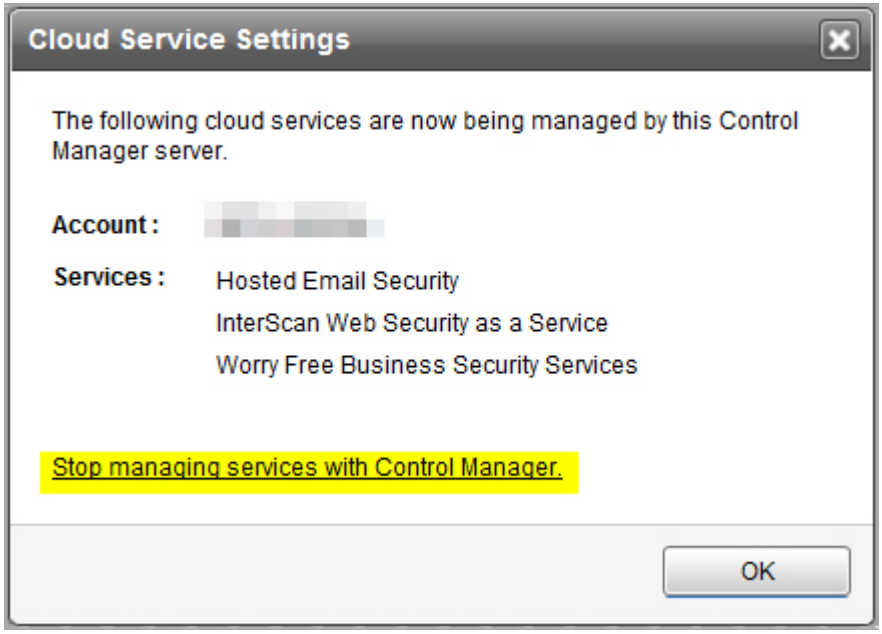
After configuring the cloud service settings, the Managed Servers list displays information related to the managed cloud service solution that Control Manager obtains from using the account you provided.

For example, if you have set Control Manager to administer your Hosted Email Security subscription, a screen similar to the following appears:



What to do next

In case your account's subscription to a particular cloud service ends, use a dialog similar to the following to configure Control Manager to stop managing such service (refer to *Stop Managing Cloud Services on page 6-9* for detailed steps.):



Stop Managing Cloud Services

Stopping a cloud service management is manually triggered when any of the following events is true:

- Your account's subscription to a particular cloud service ends
- You would like to administer a cloud service from another Control Manager server.

  For example, InterScan Web Security as a Service is initially managed by `CM-server-cupertino`. Because of new organization changes and processes, `CM-`

`server-tokyo` is delegated to administer all SaaS solutions. In this case, after completing the steps below, ensure that you configure the cloud service settings on `CM-server-tokyo`.

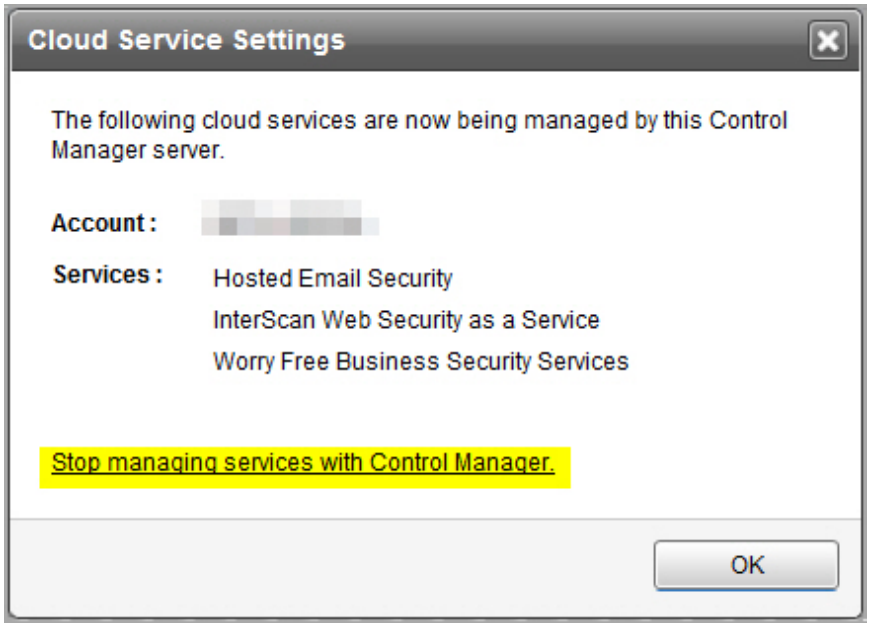
Procedure

1. Navigate to **Administration** > **Managed Servers**.

   The **Managed Servers** screen appears.

2. Click **Cloud Service Settings**.

   A dialog similar to the following appears:



3. Click **Stop managing services with Control Manager**, and agree to all succeeding prompts to stop managing SaaS solutions through Control Manager.

The **Managed Servers** list should no longer display the stopped cloud service.

Chapter 7

Downloading and Deploying Components

The Product Directory displays all managed products registered to a Control Manager server.

This chapter contains the following topics:

Downloading and Deploying New Components

Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats.

By default, Control Manager enables download only on components belonging to managed products registered to the Control Manager server. Control Manager enables virus pattern download even if no managed products are registered to the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update).

TABLE 7-1. Available Components

COMPONENT	DESCRIPTION
Pattern files/ Cleanup templates	Pattern files/Cleanup templates contain hundreds of malware signatures (for example, viruses or Trojans) and determine the managed product's ability to detect and clean malicious file infections
Antispam rules	Antispam rules are the Trend Micro-provided files used for antispam and content filtering
Engines	Engines refer to virus/malware scan engines, Damage Cleanup engine, VirusWall engines, the Spyware/Grayware engine and so on. These components perform the actual scanning and cleaning functions.

COMPONENT	DESCRIPTION
OfficeScan Plug-in Programs	OfficeScan Plug-in Programs (for example, Trend Micro Security for Mac). **Note** The OfficeScan web console displays all available Plug-in Programs. You can specify to download any of them from Control Manager. However, Control Manager may not have the downloaded the Plug-in Program. Which means that OfficeScan cannot download the specified Plug-in Program from Control Manager. Before specifying a Plug-in Program for download, from Control Manager to OfficeScan, verify that Control Manager has already downloaded the Plug-in Program.
Product programs and widget pool	Product-specific components (for example, Service Pack releases) and the Control Manager widget pool

Note

Only registered users are eligible for components update.

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

The **Component List** screen presents a full list of all components that Control Manager has available for managed products. The list also matches components with managed

products that use the component. Click **Updates** > **Component List** to open the **Component List** screen.

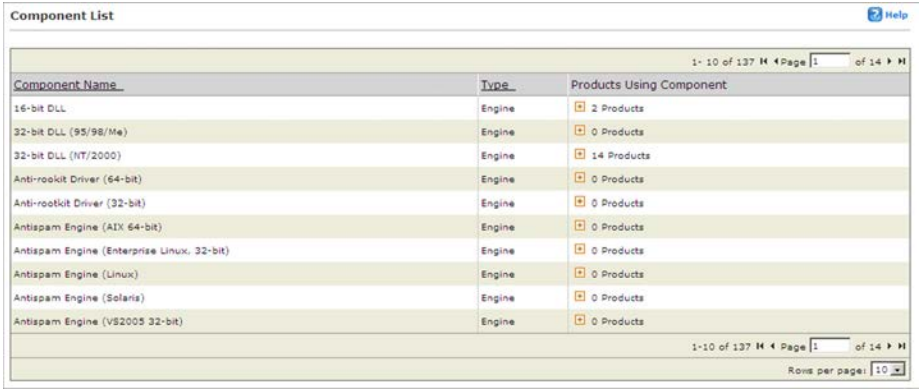


FIGURE 7-1. The Component List screen

The Control Manager server only retains the latest component version. You can trace a component's version history by viewing `root>:\Program Files\Trend Micro \Control Manager\AU_log\TmuDump.txt` entries. `TmuDump.txt` generates when ActiveUpdate debugging is enabled.

Tip

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed products or services. Configure the manual or scheduled download settings for newly-registered products or newly-activated services.

Manually Downloading Components

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Trend Micro recommends the following method to configure manual downloads. Manually downloading components requires multiple steps:

Tip

Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

Step 1: Configure a Deployment Plan for Your Components

Procedure

1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.

2. Click **Add**.

   The **Add New Plan** screen appears.

3. Type a deployment plan name in the **Name** field.
4. Click **Add** to provide deployment plan details.

The **Add New Schedule** screen appears.

5. On the **Add New Schedule** screen, choose a deployment time schedule by selecting one the following options:

   - **Start at**: Performs the deployment at a specific time.

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

   The **Add New Plan** screen appears.

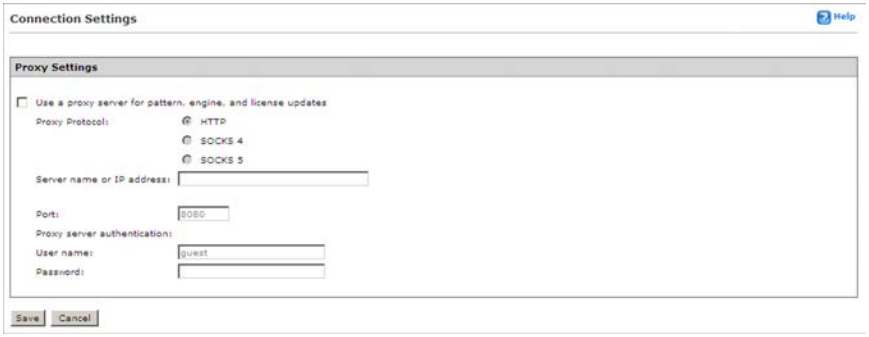
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

The **Connection Settings** screen appears.



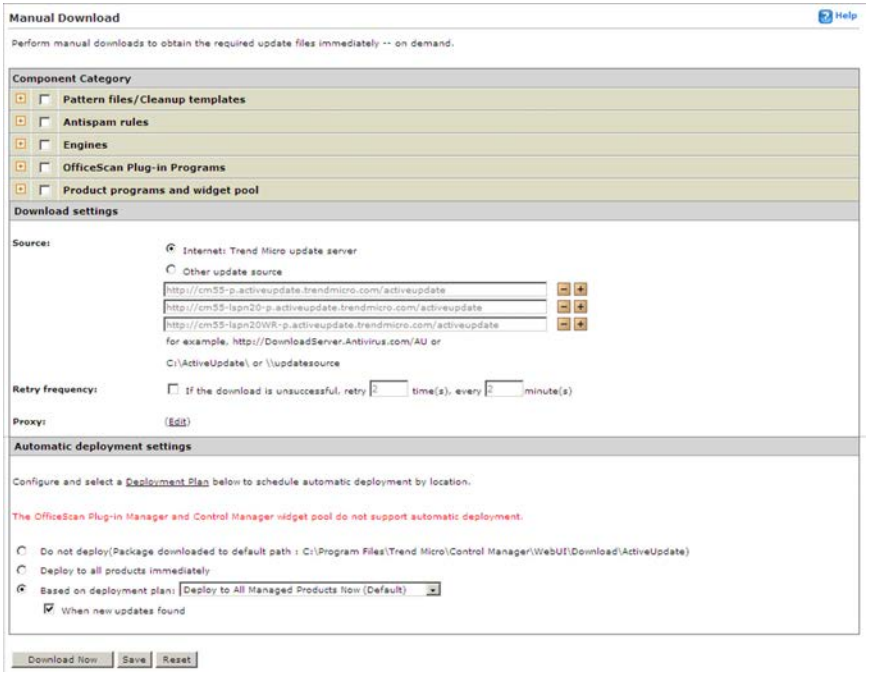
2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP address** field.
5. Type a port number in the **Port** field.
6. Type a log on name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the Components to Update

Procedure

1. Navigate to **Updates** > **Manual Download**.

The **Manual Download** screen appears.



2. From the **Component Category** area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **Pattern files/Cleanup templates**
      - **Antispam rules**
      - **Engines**
      - **OfficeScan Plug-in Programs**

- Product programs and widget pool

Step 4: Configure the Download Settings

Procedure

1. Select the update source:
   - **Internet: Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source**: Type the URL of the update source in the accompanying field.

     After selecting **Other update source**, you can specify multiple update sources. Click the + icon to add an update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

   Tip

   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.
3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.

Step 5: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the **Automatic deployment settings** area. The options are:

- **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
  - Deploying to the managed products individually
  - Testing the updated components before deployment
- **Deploy to all products immediately**: Components download to Control Manager, and then deploy to managed products
- **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
- **When new updates found**: Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Tip

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

Step 6: Complete the Manual Download

Procedure

1. Click **Download Now** and then click **OK** to confirm.

   The download response screen appears. The progress bar displays the download status.

2. Click **Command Details** to view details from the **Command Details** screen.

3. Click **OK** to return to the **Manual Download** screen.

Understanding Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature is particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

Note

Daily scheduled exceptions apply to the selected days, while hourly scheduled exceptions apply to every day of the week.

Example:

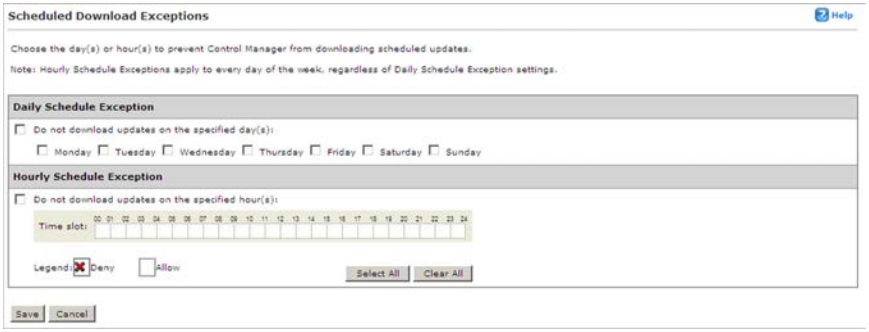
The administrator decides that they do not want Control Manager to download components on weekends or after working hours throughout the week. The administrator enables **Daily Schedule Exception** and selects **Saturday** and **Sunday**. The administrator then enables **Hourly Schedule Exception** and specifies the hours of **00:00 to 9:00** and **18:00 to 24:00**.

Configuring Scheduled Download Exceptions

Procedure

1. Navigate to **Updates** > **Scheduled Download Exceptions**.

The **Scheduled Download Exceptions** screen appears.



2. Do one or more of the following:

   - To schedule a daily exception, under **Daily Schedule Exception**, select the day(s) to prevent downloads, and then select **Do not download updates on the specified day(s)**. Every week, Control Manager blocks all downloads during the selected day(s).
   - To schedule an hourly exception, under **Hourly Schedule Exception**, select the hour(s) to prevent downloads, and then select **Do not download updates on the specified hour(s)**. Every day, Control Manager blocks all downloads during the selected hours.

3. Click **Save**.

Configuring Scheduled Downloads

Configure scheduled downloading of components to keep your components up to date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling a download for a component group downloads all components in the group.

Use the **Scheduled Download** screen to obtain the following information for components currently in your Control Manager system:

- **Frequency**: Shows how often the component updates
- **Enabled**: Indicates if the schedule for the component is enabled or disabled
- **Update Source**: Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for Your Components

Procedure

1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.

2. Click **Add**.

   The **Add New Plan** screen appears.

3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. Choose a deployment time schedule by selecting one the following options:

   - **Start at**: Performs the deployment at a specific time.

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

   The **Add New Plan** screen appears.

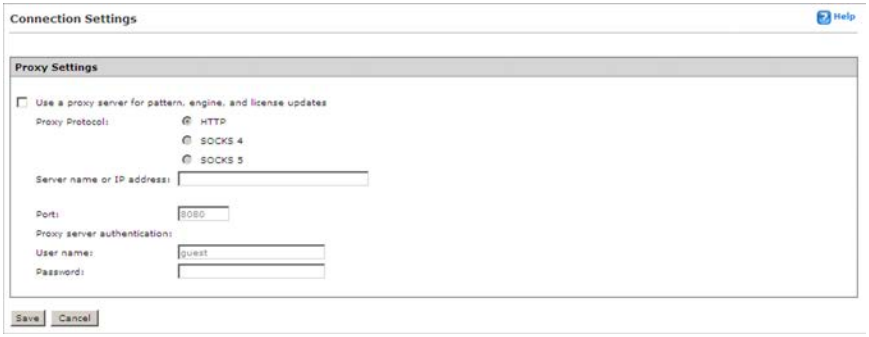
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



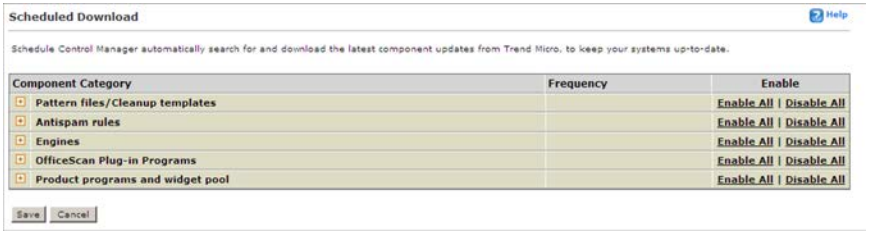
2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP** address field.
5. Type a port number for the proxy server in the **Port** field.
6. Type a logon name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the Components to Update

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.



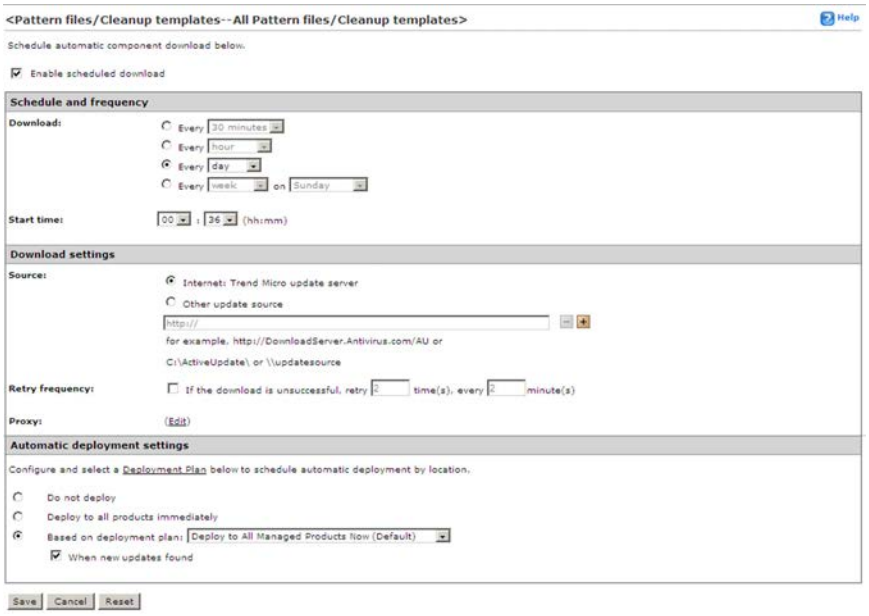
2. From the **Component Category** area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        The **Component Name>** screen appears. Where Component Name> represents the name of the selected component.



Step 4: Configure the Download Schedule

Procedure

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.

2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download by minutes, hours, days, or weeks.

3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the Download Settings

Procedure

1. Select the update source:

   - **Internet**: **Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source**: Type the URL of the update source in the accompanying field.

     After selecting **Other update source**, you can specify multiple update sources. Click the **+** icon to add an update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

   Note

   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.

Step 6: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the **Automatic deployment settings** area. The options are:

   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually

- Testing the updated components before deployment

- **Deploy immediately**: Components download to Control Manager, then deploy to managed products
- **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
- **When new updates found**: Components download to Control Manager, and deploy to managed products when new components are available from the update source

Note

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the **Deployment Plan** screen.
3. Click **Save**.

Step 7: Enable the Schedule and Save Settings

Procedure

1. Click the status button in the **Enable** column.
2. Click **Save**.

Configuring Scheduled Download Schedule and Frequency

Specify how often Control Manager obtains component updates at the Schedule and Frequency group.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the **Component Category** area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        The **Component Name>** screen appears. Where Component Name> represents the name of the selected component.

3. Under Schedule and frequency:

   a. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minutes, hours, days, or weeks.

   b. Use the **Start time** drop-down menus to specify the date and time the schedule starts to take effect.

4. Click **Save**.

Configuring Scheduled Download Settings

The **Download Settings** group defines the components Control Manager automatically downloads and the download method.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the **Component Category** area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        The **Component Name>** screen appears. Where Component Name> represents the name of the selected component.

3. Under **Download settings**, select one of the following update sources:

   - **Internet: Trend Micro update server**: (default setting) Control Manager downloads the latest components from the Trend Micro ActiveUpdate server
   - **Other update source**: specify the URL of the latest component source, for example, your company's Intranet server

     After selecting **Other update source**, you can specify multiple update sources. Click the ± icon to add an additional update source. You can configure up to five update sources.

4. Select **Retry frequency** to instruct Control Manager to retry downloading latest components. Specify the number of attempts and the frequency of each set of attempts in the appropriate fields.

Note

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

5. If you are using a proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings from the **Connection Settings** screen.

6. Click **Save**.

Configuring Scheduled Download Automatic Deployment Settings

Use the Automatic deployment settings group to set how Control Manager deploys updates.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the **Component Category** area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

The **Component Name>** screen appears. Where Component Name> represents the name of the selected component.

3. Select a deployment plan after components download to Control Manager, from the **Deployment Plan** screen.

4. Click **Save**.

Note

The settings in **Automatic deployment settings** only apply to components used by managed products.

Understanding Deployment Plans

A deployment plan allows you to set the order in which Control Manager updates your groups of managed products. With Control Manager, you can implement multiple deployment plans to different managed products at different schedules. For example, during an outbreak involving an email-borne virus, you can prioritize the update of your email message scanning software components such as the latest virus pattern file for Trend Micro ScanMail for Microsoft Exchange.

The Control Manager installation creates two deployment plans:

- Deploy to All Managed Products Now (Default): default plan used during component updates
- Deploy to All Immediately (Outbreak-Prevention): default plan for the Outbreak Prevention Services Prevention Stage

By default, these plans deploy updates to all products in the Product Directory immediately.

Select or create plans from the Manual and Scheduled download screens. Customize these plans, or create new ones, as required by your network. For example, create deployment plans according to the nature of the outbreak:

- Email-borne virus

- File-sharing virus

Deploying updates to the Product Directory is separate from the download process.

Control Manager downloads the components and follows the deployment plan according to manual or scheduled download settings.

When creating or implementing a deployment plan, consider the following points:

- Assign deployment schedules to folders, not to specific products.

  Planning the contents of the Product Directory folders, therefore, becomes very important.

- You can only include one folder for each deployment plan schedule.

  However, you can specify more than one schedule per deployment plan.

- Control Manager bases the deployment plan delays on the completion time of the download, and these delays are independent of each other.

  For example, if you have three folders to update at 5 minute intervals, you can assign the first folder a delay of 5 minutes, and then set delays of 10 and 15 minutes for the two remaining folders.

Creating Deployment Plans

Create a new plan if none of the existing plans suits your needs.

Procedure

1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.

2. Click **Add**.

   The **Add New Plan** screen appears.

3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. Choose a deployment time schedule by selecting one the following options:

   - **Start at**: Performs the deployment at a specific time.

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
7. Click **Save**.

   The **Add New Plan** screen appears.
8. Click **Save** to apply the new deployment plan.

Modifying a Deployment Plan

Use the **Edit Plan** screen to add, modify, or remove schedules from a deployment plan.

Procedure

1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.
2. Click the name of the plan to modify.

   The **Edit Plan** screen appears.
3. Click the name of the schedule to modify.

   The **Edit Schedule** screen appears.
4. Modify the deployment time or Product Directory folder.

   Note

   You cannot remove a schedule if there are no other schedules available.
5. Click **Save**.

   The **Edit New Plan** screen appears.
6. After completing all the necessary modifications, click **Save**.

   The **Deployment Plan** screen appears.

Duplicating a Deployment Plan

Create new deployment plans based on an existing plan.

Procedure

1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.

2. Select the accompanying check box for the plan to copy.

3. Click **Copy**.

   The **Add New Plan** screen appears.

4. Type a unique name for the plan. **New Plan** is the default name of copied plans.

5. Modify the deployment plan as required.

   Note

   You cannot remove a schedule if there are no other schedules available.

6. Click **Save**.

Removing a Deployment Plan

You can delete obsolete or outdated plans.

Procedure

1. Navigate to **Updates** > **Deployment Plan**. The Deployment Plan screen appears.

2. Select the accompanying check box for the plan to delete.

3. Click **Delete**.

   The selected plans delete from the Deployment Plan list.

Configuring the Proxy Settings for Component Updates

Configure the proxy server connection for component downloads and license updates.

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.

2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP address** field.
5. Type a port number in the **Port** field.
6. Type a log on name and password if your server requires authentication.

7. Click **Save**.

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server (the default download source) or other update source provides a more secure method for retrieving components.

Downloading components from a shared folder in a network requires setting the local Windows and Remote UNC authentications.

The local Windows authentication refers to the Active Directory user account in the Control Manager server. The account should have:

- Administrator privilege
- **Log on as a batch job policy** set

The **remote UNC authentication** feature uses a user account from the component source server that has permission to share a folder to which Control Manager will download updates.

Enabling HTTPS Download

Procedure

1. Navigate to **Updates** > **Update/Deployment Settings**.

The **Update/Deployment Settings** screen appears.

2. Select **Enable HTTPS for the default update download source**.
3. Click **Save**.
4. Navigate to the **Manual Download** or **Scheduled Download** screen.
5. On the working area under **Download settings**, select **Internet: Trend Micro update server** or specify your organization's component source server in the **Other update source** field.
6. Click **Save**.

Enabling UNC Download

Procedure

1. Navigate to **Updates** > **Update/Deployment Settings**.

   The **Update/Deployment Settings** screen appears.
2. Type the **Local Windows Authentication** and **Remote UNC Authentication** user names and passwords.
3. Click **Save**.
4. Navigate to the **Manual Download** or **Scheduled Download** screen.

5. On the working area under **Download settings**, select **Other update source** and then specify the shared network folder.

6. Click **Save**.

Setting "Log on as batch job" Policy

The local Windows authentication refers to the Active Directory user account in the Control Manager server. The account should have:

- Administrator privilege
- **Log on as a batch job** policy set

Procedure

1. Click **Start** > **Settings** > **Control Panel**.
2. Click **Administrative Tools**.
3. Open **Local Security Policy**.

   The **Local Security Settings** screen appears.
4. Click **Local Polices** > **User Rights Assignment**.
5. Double-click **Log on as a batch job**.

   The **Log on as a batch job Properties** dialog box appears.
6. Add the user if they do not appear on the list.

Part II

Monitoring the Control Manager Network

Chapter 8

Working with the Dashboard and Widgets

The **Dashboard** replaces the Summary screen from previous versions of Control Manager.

This chapter contains the following topics:

Using the Dashboard

The Control Manager dashboard provides at-a-glance information for the Control Manager network. The dashboard is comprised of two components:

- **Tabs:** Allow administrators to create a screen that contains one or more widgets

  Click **Play Tab Slide Show** to automatically switch between tab views.

  Click **Pause Tab Slide Show** to pause at a tab view.

- **Widgets:** Provide specific information about various security-related events

Note

Enabling Smart Feedback is required for some widgets to function. See *Configuring Smart Protection Network Settings on page 8-19* for more information on enabling Smart Feedback.

User Accounts and the Dashboard

Each user account displays it's own dashboard. When a user logs on to Control Manager for the first time, the default tabs and the widgets contained within the tabs appear on the dashboard.

Each user account can customize the dashboard, tabs, and widgets for the account's specific needs. Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Understanding Tabs

The Control Manager dashboard uses tabs to provide flexibility for administrators. Tabs provide a container for widgets allowing administrators to create their own customized dashboard. The dashboard supports up to 30 tabs per user account.

You can move widgets on tabs by dragging and dropping widgets in various locations on the tab. The layout for a tab determines where you can move the widget.

Note

Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Default Tabs

The dashboard provides the following tabs:

- **Summary**
- **DLP Incident Investigation**
- **Data Loss Prevention**
- **Compliance**
- **Threat Detection**
- **Smart Protection Network**

Note

Deleting the default tabs permanently removes the tabs from viewing for the user account that removed the tabs. There is no way to recover a deleted tab. Deleting a default tab has no impact on the dashboard for other user accounts.

Summary Tab

The **Summary** tab replaces the Control Manager **Home** screen. All information that was available on the Control Manager **Home** screen is available through the widgets on the **Summary** tab.

Starting in version 6.0 Service Pack 3, this tab contains a predefined set of widgets. In addition, the tab and all the predefined widgets are "read-only". This means that regular tab and widget operations are not allowed in this tab.

The predefined widgets are as follows:

- Critical Threats
- Users with Threats
- Endpoints with Threats
- Control Manager Top Threats
- Product Connection Status
- Product Component Status

For details about widget categories and getting Help information for each widget, see *Widget Categories and Help Information on page 8-15*.

Working with a Legacy Summary Tab

Starting in version 6.0 Service Pack 3, the **Summary** tab contains a predefined set of widgets. In addition, the tab and all the predefined widgets are "read-only". This means that regular tab and widget operations are not allowed in this tab.

If you renamed the Summary tab in your previous Control Manager version (for example, from Summary to My Summary), the tab will be migrated as-is after you upgrade to version 6.0 Service Pack 3.

If you did not rename the Summary tab and then upgraded to version 6.0 Service Pack 3, one of two things can happen.

- You do not see the old Summary tab (the tab you were using in the previous version). This happens if you did **not** change the tab's settings, such as its layout or auto-fit setting, in the previous version. You can bring back this tab by following the steps below.
- There are two Summary tabs - the new read-only tab and the old tab. This happens if you changed the old tab's settings. To avoid confusion, rename the old tab.

Follow these steps to bring back the old Summary tab.

Procedure

1. Open Microsoft Management Console and stop the Control Manager service.
2. Open a command prompt and change to one of the following directories, depending on the installation folder for Control Manager:
   - `C:\Program Files\Trend Micro\Control Manager\WebUI \WebApp\widget\repository\widgetPool`
   - `C:\Program Files (x86)\Trend Micro\Control Manager\WebUI \WebApp\widget\repository\widgetPool`
3. Type the following command:

   `php interface_request.php enableDisabledTabs.php`
4. Start the Trend Micro Control Manager service.
5. Open the Control Manager management console.

   The old tab appears as **Summary (Old)**.

DLP Incident Investigation Tab

The **DLP Incident Investigation** tab contains widgets that display information about DLP incidents based on incident status, severity levels, and managed users.

The predefined widgets are as follows:

- DLP Incidents by Severity and Status
- DLP Incident Trends by User
- DLP Incidents by User

For details about widget categories and getting Help information for each widget, see *Widget Categories and Help Information on page 8-15*.

Data Loss Prevention Tab

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

The predefined widgets are as follows:

- DLP Incidents by Channel
- DLP Template Matches
- Top DLP Incident Sources
- DLP Violated Policy

For details about widget categories and getting Help information for each widget, see *Widget Categories and Help Information on page 8-15*.

Compliance Tab

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

The predefined widgets are as follows:

- Product Application Compliance
- Product Component Status
- Product Connection Status
- Agent Connection Status

For details about widget categories and getting Help information for each widget, see *Widget Categories and Help Information on page 8-15*.

Threat Detection Tab

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

The predefined widgets are as follows:

- Control Manager Top Threats
- Control Manager Threat Statistics
- Threat Detection Results
- Policy Violation Detections
- C&C Callback Events

Note

On parent Control Manager servers, the **Control Manager Top Threats** and **File Reputation Top Threat Detections** widgets require scheduled log uploads from child Control Manager servers, to display accurate data.

To enable scheduled log uploads from child Control Manager servers, configure on the parent Control Manager server:**Directories** > **Products** > **Select a child server from the Product Directory** > **Configure** > **Schedule Child Control Manager server log uploads**

For details about widget categories and getting Help information for each widget, see *Widget Categories and Help Information on page 8-15*.

Smart Protection Network Tab

The **Smart Protection Network** tab contains widgets that contain information exclusively from the Trend Micro Smart Protection Network (which includes Email Reputation, File Reputation, and Web Reputation) and information that is combined with information from the Control Manager network.

The predefined widgets are as follows:

- File Reputation Top Threat Detections
- Smart Protection Network Connections
- Smart Protection Network Threat Statistics
- File Reputation Threat Map

For details about widget categories and getting Help information for each widget, see *Widget Categories and Help Information on page 8-15*.

Adding Tabs

Add tabs to the dashboard to provide a customized information matrix for your Control Manager network needs.

Procedure

1. Navigate to the **Dashboard** screen.
2. Click the **+** button.

   The **New Tab** screen appears.
3. Type a meaningful title for the tab in the **Title** field.
4. Select a layout for the tab.

   Note

   The number of widgets that you can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, you must remove a widget from the tab or create a new tab for the widget.
5. Click **Save**.

   The empty tab appears on the dashboard.
6. Click **Add Widgets** to populate the tab with widgets.

Configuring Tab Settings

You can change the default name of a tab using the **Tab Settings** screen.

Procedure

1. Navigate to the **Dashboard** screen.

2. Click **Tab Settings**.

   The **Tab Settings** screen appears.

3. Type a meaningful title for the tab in the **Title** field.

4. Select a tab layout.

5. Configure slide show and auto-fit settings.

6. Click **Save**.

Understanding Widgets

Widgets are the core components for the dashboard. Tabs provide the layout and widgets provide the actual data for the dashboard.

Note

Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Download the Control Manager widget pool (under **Product programs and widget pool** on the **Manual Download** and **Scheduled Download** screens) periodically to check for new or updated widgets.

The data a widget displays comes from one of the following places:

- Control Manager database
- Trend Micro Smart Protection Network
- Managed products added to the Dashboard **Server Visibility** list

Note

Smart Feedback must be enabled to display data for widgets that include data from Smart Protection Network.

The data a widget displays is controlled in two ways:

TABLE 8-1. Widget Data

ITEM	DETAILS
User account	A user's account grants or restricts access to any managed product registered to Control Manager.
Scope	The data scope on many widgets can be individually configured. This means a user can further specify the data source location for the widget. Example: An OfficeScan administrator, who manages multiple OfficeScan servers, could create one tab and add widgets that display data for only one OfficeScan server.

Each widget provides targeted security-related information. Widgets can display this information in one of the following ways:

- Bar chart
- Pie chart
- Line chart
- Table

Widget Requirements

Some widgets require configuring very specific settings before the widgets can be used. For example, the **Endpoint Protection Verification** widget requires connection to your Active Directory server, OfficeScan servers, and Deep Security servers.

Configuring Active Directory and Endpoint Protection Verification Widget Settings

The Endpoint Protection Verification widget requires connection to your Active Directory server, OfficeScan servers, and Deep Security servers to work properly.

WARNING!

The OfficeScan server agent trees and Active Directory trees must be synchronized for the **Endpoint Protection Verification Widget** to work properly.

Procedure

1. Navigate to **Administration** > **Settings** > **Active Directory and Widget Settings**.

   The **Active Directory and Endpoint Protection Verification Widget Settings** screen appears.

2. Select **Enable specified connections**.

3. Configure the **Active Directory Server Connection Settings**:

   - **Server FQDN or IP address**: The FQDN or IP address for your Active Directory server
   - **Domain\user name**: The domain name and user name required to log on to your Active Directory server
   - **Password**: The password required to log on to your Active Directory server

   Important

   Depending on various factors such as the size of your organization, the initial Active Directory synchronization might take more than an hour.

4. Configure the **OfficeScan Connection Settings**:

   - **Product ID**: A short identifier for the OfficeScan server used by the widget
   - **Server name or IP address**: The host name or IP address for your OfficeScan server
   - **Port**: The port number used for communication with your OfficeScan server

     Default is 4343.

   - **User name**: The domain name and user name required to log on to your OfficeScan server

- **Password**: The password required to log on to your OfficeScan server

5. Configure the **Deep Security Manager Connection Settings**:
   - **Product ID**: A short identifier for the Deep Security server used by the widget
   - **Server name or IP address**: The host name or IP address for your Deep Security server
   - **Port**: The port number used for communication with your Deep Security server

     Default is 4119.
   - **User name**: The domain name and user name required to log on to your Deep Security server
   - **Password**: The password required to log on to your Deep Security server
6. To add more than one OfficeScan or Deep Security server click the **+** icon. You can add up to five OfficeScan servers and up to five Deep Security servers.
7. Configure **Synchronization Settings**:
   - Specify how often all of the servers configured on this screen will synchronize with the **Endpoint Protection Verification** widget.
   - Select the **Synchronize after clicking "Save"** check box to force all of the servers configured on this screen to synchronize with the **Endpoint Protection Verification** widget, after clicking save.
8. Click **Save**.

Endpoint Encryption Connection Settings

Widgets that get information from the Endpoint Encryption server must first connect to the server.

Procedure

1. Navigate to the **Dashboard** screen.

2. Click **Server Visibility**.
3. Click **Add**.
4. Configure the connection settings:
   - **Server Name**: The FQDN or IP address and the port number for your server
   - **Server Type**: Select **Endpoint Encryption** from the list
   - **Account**: The user name required to log on to the server
   - **Password**: The password required to log on to the server
   - **Enterprise**: The enterprise for the associated endpoints.
5. Click **Save**.
6. Click ( ) next to **Proxy Settings** and configure the settings, if you network uses a proxy server.
7. Click **Apply**.
8. To add more than one product server click **Add**.

Using Widgets

Use widgets by performing the following tasks:

TABLE 8-2. Widget Tasks

TASK	STEPS
Move a widget	Use drag-and-drop to move widgets to different locations within the tab.
Resize a widget	Resize widgets on a multi-column tab by pointing the cursor to the right edge of the widget and then moving the cursor to the left or right.

TASK	STEPS
Refresh widget data	Click the refresh icon ().
Closing a widget	Click  , and then select **X Close Widget**.
Understand widget	Click the help icon on a widget to view the following types of information: • Overview: Description for the widget and how the widget can be used • Widget Data: Detailed information about the data that displays in the widget's table • Configure: Description of settings that are readily visible on the widget • Edit: Description of settings that require clicking the edit icon to modify

Detailed Widget Information

Displaying widget data in a table provides an added benefit to users. The data in some columns can be clicked to view detailed information.

Example: From the **Control Manager Top Threats** widget on the **Threat Statistics** tab, clicking any link from the **Detections** column opens to a table with the following information:

TABLE 8-3. Widget Drill-down Example

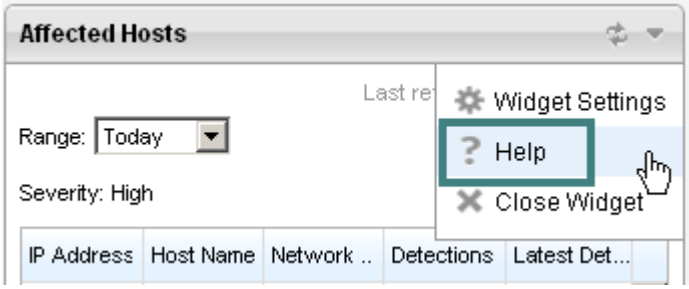
DATA	DESCRIPTION
Endpoint	Host name for the endpoint with a virus
Product Entity	Name of the product that detected the virus

DATA	DESCRIPTION
Virus	Name of the virus
Start time	Time of first detection of the virus
End time	Time of the last detection of the virus
Detections	Number of virus detections

Widget Categories and Help Information

A list of widgets grouped by categories is available when you click **Add Widgets** from the dashboard. The image below shows a partial list of widget categories.

After adding a widget, refer to the widget Help to view detailed information about it.



Note

On parent Control Manager servers, the **Control Manager Top Threats** and **File Reputation Top Threat Detections** widgets require scheduled log uploads from child Control Manager servers, to display accurate data.

To enable scheduled log uploads from child Control Manager servers: **Products** > **Select a child server from the Product Directory** > **Configure** > **Schedule Child Control Manager server log uploads**

Configuring Widgets

Configuring a widget means modifying settings for the widget that are readily visible on the widget. The following table lists some examples of the widget settings administrators can modify.

TABLE 8-4. Configuring Widgets

SETTING	DESCRIPTION
Range	Modify the time range for data that displays: • Today • 1 week • 2 weeks • 1 month
Data aggregation	Modify the aggregation for the data: • Malicious URLs • Malicious files or • Product category • Threat type
Display	Modify how the data displays: • Bar chart • Line chart • Pie chart • Table

Editing Widgets

Editing a widget means modifying settings for the widget that are not readily visible on the widget. Examples include:

TABLE 8-5. Editing Widgets

SETTING	DESCRIPTION
Title	Modify the name that displays for the widget.

SETTING	DESCRIPTION
Scope	Specifies the data source location for the widget. By default the widget displays data from all managed products that their user access allows. **WARNING!** The data source has a significant impact on what the widget displays. Use care when modifying this setting. For example, someone specifies that the widget displays data for only a portion of your network.
Others	Some widgets provide settings to modify the amount of data a widget displays (range of entries) or the type of data that displays (security threat type or component type with the product type).

Procedure

1. Navigate to the **Dashboard** screen.
2. Click a tab that has a widget with an edit icon.
3. Click the down arrow at the upper right section of the widget and then click **Widget Settings**. A new screen appears.
4. Modify settings, including the title, scope (if available), and other widget-specific settings.
5. Click **Save**.

   The widget reloads applying the new settings.

Adding Widgets

The number of widgets that you can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, you must remove a widget from the tab or create a new tab for the widget.

Procedure

1. Navigate to any tab on the dashboard.
2. Click **Add Widgets**.

   A new screen appears.
3. Select the widgets you wish to add. Use the categories at the left section of the screen to filter the widgets. If you have a specific widget in mind, use the search text box on top of the screen to search for the widget.
4. Click **Add**.

Configuring Smart Protection Network Settings

Enable Trend Micro Smart Feedback to share threat information with the Trend Micro Smart Protection Network. This provides better protection for your network because Trend Micro is able to quickly identify and address new threats.

Enabling Smart Protection Network Settings is also required for some widgets to function. This is because the widgets receive their data directly from Trend Micro Smart Protection Network.

Note

Email Reputation, File Reputation, and Web Reputation are all part of the Smart Protection Network.

Procedure

1. Navigate to **Administration** > **Settings** > **Smart Protection Network Settings**.

   The **Smart Protection Network Settings** screen appears.
2. Select **Enable Trend Micro Smart Feedback and Smart Protection Network widgets**.

3. Specify how often Control Manager will send completely anonymous threat information to the Smart Protection Network from the **Time interval** drop-down list.

4. Specify the industry that your company is in from the **Your industry** drop-down list.

5. Click **Save**.

Chapter 9

Using Command Tracking

Use Command Tracking to view records of all commands issued to managed products and child servers.

This chapter contains the following topics:

Understanding Command Tracking

The Control Manager server maintains a record of all commands issued to managed products and child servers. Commands refer to instructions given to managed products or child server to perform specific tasks (for example, performing a component update). Command Tracking enables you to monitor the progress of all commands.

For example, after issuing a Start Scan Now task, which can take several minutes to complete, you can proceed with other tasks and then refer to Command Tracking later for results.

The **Command Tracking** screen presents the following details in table format:

TABLE 9-1. Command Tracking Details

INFORMATION	DESCRIPTION
Date/Time Issued	The date and time when the Control Manager server issued the command to the managed product or child server
Command	The type of command issued
Successful	The number of managed products or child servers that completed the command
Unsuccessful	The number of managed products or child servers unable to perform the command
In Progress	The number of managed products or child servers that are currently performing the command
All	The total number of managed products and child servers to which Control Manager issued the command

Note

Clicking the available links in the **Successful**, **Unsuccessful**, **In Progress**, or **All** column opens the **Command Details** screen.

Understanding Command Details

The **Command Details** screen provides in-depth information about the result of a command. Control Manager records and groups command details according to the following:

- Managed products or services involved
- Details for individual products or services

The **Command Details** screen refreshes every 30 seconds.

Managed Products or Services Involved

TABLE 9-2. General Command Details

INFORMATION	DESCRIPTION
Started	Indicates the date and time when the Control Manager server issued the command to the managed product or child server, and additional command information. For example, when you invoke a Manual Download, the **Issued** field will contain the Parameter information about the component Control Manager could or could not download. A Manual Download Command Detail can have a Parameter called "engine". This parameter determines that Control Manager downloaded the scan engine component. For other commands that do not apply additional details, the Parameter is **N/A**.
Last Reported	Indicates the date and time when the Control Manager server received a response from a managed product or child server.
User	Indicates the user account that issued the task to the managed product or child server.
Successful	Indicates the number of managed products or child servers that completed the command.
Unsuccessful	Indicates the number of managed products or child servers that could not perform the command.

INFORMATION	DESCRIPTION
In Progress	Indicates the number of managed products or child servers that are currently performing the command.

Details for Individual Products or Services

TABLE 9-3. Command Details for Individual Products or Services

INFORMATION	DESCRIPTION
Last Reported	Indicates the date and time when the managed product sends a response to the Control Manager server
Server/Entity	Indicates the host name of the child or managed product server
Status	Indicates the status of the issued command • Successful • In Progress • Unsuccessful • Skip • Submit • Time Out • Not supported • Tracking • Cancelled • Successful • Accepted • Not Available
Description	Explains the Status

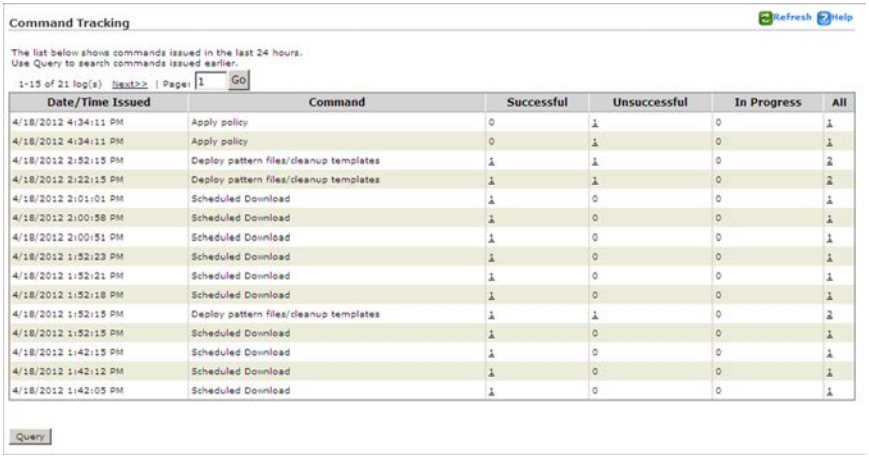
Querying and Viewing Commands

Use the **Command Tracking Query** screen to track and view previously issued commands.

Procedure

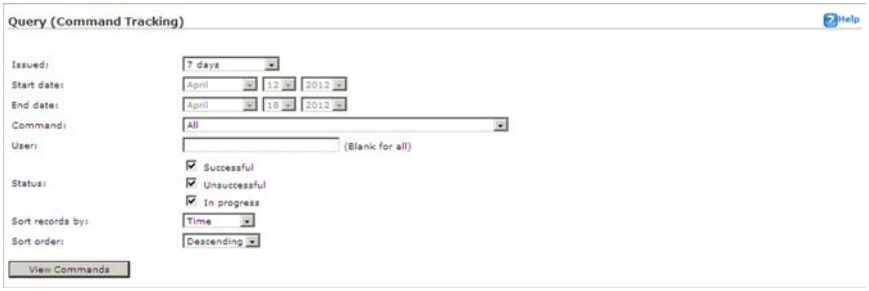
1. Navigate to **Administration** > **Command Tracking**.

The **Command Tracking** screen appears.



2. On the working area, click **Query**.

   The **Query (Command Tracking)** screen appears.



3. On the **Query (Command Tracking)** screen, specify values for the following parameters:

   - **Issued**: Specify the time range for the query

     Choose among the predetermined ranges, or specify your own range.

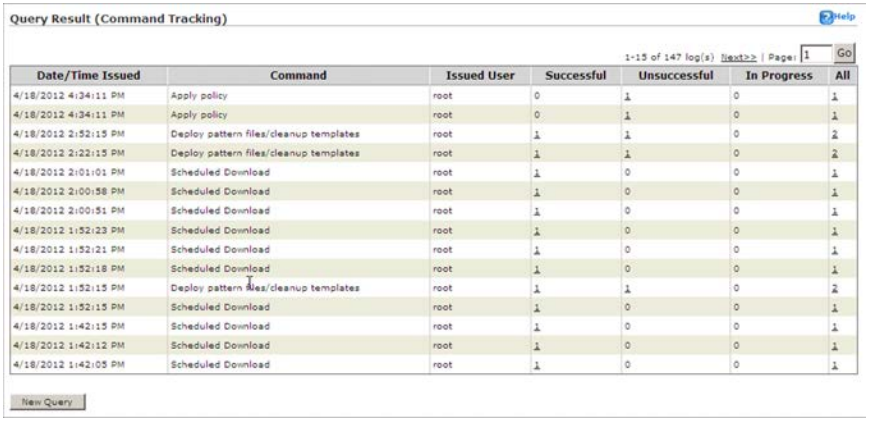
   - **Start date**/**End date**: Set the custom range based on months, days, or years

- **Command**: Select the command to monitor
- **User**: Provide the user account name to query. Leave this field blank to query commands issued by all users
- **Status**: Select the command status
- **Sort records by**: Specify how the **Query Result** screen will display results

  Arrange the query results according to **Time**, **Command**, or **User**.
- **Sort order**: Specify whether the **Query Result** screen will display results in ascending or descending order

4. Click **View Commands**.

   The **Query Result (Command Tracking)** screen shows the number of products affected by the command, as well as the results.



5. Click the available link in the **Successful**, **Unsuccessful**, **In Progress**, or **All** column to view the specified Command Details.

Chapter 10

Using Notifications

Use Event Center to configure Control Manager to send notifications about events that occur in the Control Manager network.

This chapter contains the following topics:

Understanding Event Center

Events refer to actions detected by a managed product and relayed to the Control Manager server. The Event Center enables you to set notifications for different events.

The Event Center categorizes events according to the following types:

TABLE 10-1. Event Center Events

EVENT TYPES	DESCRIPTION
Alert	Provides warning about viruses/spyware/grayware detected by antivirus managed products. For more information, see *Alert Events on page 10-3*.
Advanced Threat Activity	Provides warning about advanced persistent threats. For more information, see *Advanced Threat Activity on page 10-4*.
Outbreak Prevention Services	Provides information about policy application and update information about Outbreak Prevention Services (OPS). Outbreak Prevention Services notification types group the following service events: • Active Outbreak Prevention Policy received • Outbreak Prevention Mode started • Outbreak Prevention Mode stopped • Outbreak Prevention Policy update unsuccessful • Outbreak Prevention Policy update successful
Statistics	Provides "Violation Statistics" event notification for Network VirusWall products.
Update	Provides antivirus and content security component update results (successful or unsuccessful). For more information, see *Update Alert Events on page 10-5*.

Event Types	Description
Unusual	Provides information about product options or service activation and deactivation. For more information, see *Unusual Alert Events on page 10-6*.
Security Violation	Provides warning about email message content violations and client Web violations. For more information, see *Security Violation Events on page 10-6*.
Data Loss Prevention	Provides information about Data Loss Prevention incidents and template matches. For more information, see *Data Loss Prevention Events on page 10-6*.

Alert Events

Table 10-2. Alert Events

Alert	Description
Virus outbreak alert	Applicable to antivirus managed products
Special virus alert	Applicable to antivirus managed products
Special spyware/grayware alert	Applicable to anti-spyware/grayware managed products
Virus found	The following options are available: • First action unsuccessful and second action unavailable - applicable to antivirus managed products • First and second actions unsuccessful - applicable to antivirus managed products • First action successful - applicable to antivirus managed products • Second action successful - applicable to antivirus managed products

Alert	Description
Network virus alert	Applicable to packet-scanning products (for example, Network VirusWall Enforcer 1500)
Potential vulnerability attack detected	Applicable to packet-scanning products (for example, Network VirusWall 1500)
Spyware/Grayware found	The following options are available: • Action successful - applicable to anti-spyware/grayware managed products • Further action required - applicable to anti-spyware/grayware managed products

Advanced Threat Activity

Table 10-3. Advanced Threat Activity

Event	Description
C&C callback alert	Applicable to antivirus and threat discovery managed products
C&C callback outbreak alert	Applicable to antivirus and threat discovery managed products
High risk Virtual Analyzer detections	Suspicious objects with high severity detections, as reported by Virtual Analyzer
High risk host detections	Hosts with high severity detections
SHA-1 Deny List detections	Detections that match SHA-1 values in the Deny List
Known targeted attack behavior	Detections that match known targeted attack behavior
Potential document exploit detections	Detections that match embedded exploit code
Rootkit or hacking tool detections	Detections that match known rootkit characteristics

Event	Description
Worm or file infector propagation detections	Detections that match known worm or file infector characteristics
Correlated incidents	Detections that match the Deep Discovery Inspector correlation rule
Email Messages with Advanced Threats	Email messages with malicious and suspicious behavior, as detected by Deep Discovery Email Inspector Suspicious behavior includes anomalous behavior, false or misleading data, suspicious and malicious behavioral patterns, and strings that indicate system compromise but require further investigation to confirm.
Advanced threats sent to recipients in watchlist	Watchlist configured by Deep Discovery Email Inspector administrators that triggers an alert when suspicious or malicious email message are detected

Update Alert Events

Table 10-4. Update Alert Events

Event	Description
Scan engine update unsuccessful	Applicable to antivirus managed products
Scan engine update successful	Applicable to antivirus managed products
Pattern files/Cleanup templates update unsuccessful	Applicable to antivirus managed products
Pattern files/Cleanup templates update successful	Applicable to antivirus managed products
Anti-spam rule update unsuccessful	Applicable to content security managed products
Anti-spam rule update successful	Applicable to content security managed products

Unusual Alert Events

TABLE 10-5. Unusual Alert Events

ALERT	DESCRIPTION
Real-time scan enabled	Applicable to antivirus managed products
Real-time scan disabled	Applicable to antivirus managed products
Product service started	Applicable to antivirus and content security managed products
Product service stopped	Applicable to antivirus and content security managed products
Managed product unreachable	A managed product is disconnected from Control Manager

Security Violation Events

TABLE 10-6. Security Violation Events

EVENT	DESCRIPTION
Content security violation	Applicable to content security managed products. For example, InterScan Messaging Security Suite.
Web security violation	Applicable to Web security managed products. For example, InterScan Web Security Suite.

Data Loss Prevention Events

TABLE 10-7. Data Loss Prevention Events

EVENT	DESCRIPTION
Significant incident increase	Applicable to antivirus managed products
Significant template match increase	Applicable to antivirus managed products

Event	Description
Significant incident increase by user	Applicable to antivirus managed products
Significant incident increase by sender	Applicable to antivirus managed products
Significant incident increase by channel	Applicable to antivirus managed products
Scheduled incident summary	Applicable to antivirus managed products
Incident details updated	Applicable to antivirus managed products

Customizing Notification Messages

Use variables to customize event notifications. Insert these variables when you configure notifications to provide details to notification recipients.

Control Manager supports the following variables:

Table 10-8. Common Notification Message Variables

Variable	Description
Common variables used by all event notifications	
`%cmserver%`	Control Manager server host name
`%computer%`	Network name of the computer where an event was detected
`%entity%`	Product Directory path of the managed product where an event occurred
`%event%`	Event that triggered the notification
`%pname%`	Managed product name
`%pver%`	Managed product version
`%time%`	Time (hh:mm) when an event occurred

VARIABLE	DESCRIPTION
%vloginuser%	The logon user information for customized events in spyware logs
%act%	The action taken by the managed product. Example: file cleaned, file deleted, file quarantined
%actresult%	The result of the action taken by the managed product. Example: successful, further action required

TABLE 10-9. Virus Notification Message Variables

VARIABLE	DESCRIPTION
Virus variables: Used by alert or Outbreak Prevention Service event notifications	
%device_ip%	IP address of an infected endpoint.
%egnver%	• Scan engine version. • Used by the alert event category as well as the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Mode started" notifications. For the notification types of the alert event category, this variable refers to the scan engine version currently installed on the managed product server. • For the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Mode started" notifications, this variable refers to the Outbreak Prevention Policy required.
%ptnver%	• Virus pattern version. • Used by the alert event category and the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Services started" notifications. For the notification types of the alert event category, this variable refers to the virus pattern version currently installed on the managed product server. • For the "Active Outbreak Prevention Policy received" and "Outbreak Prevention Services started" notifications, this variable refers to the Outbreak Prevention Policy required.

VARIABLE	DESCRIPTION
%scanmethod%	The scan method for specific virus actions. This token is only available for the following alerts: • Virus found-first action unsuccessful and second action unavailable • Virus found-first and second actions unsuccessful • Virus found-first action successful • Virus found-second action successful
%threat_info%	• Virus/malware threat information provided by outbreak prevention policies. • Used by "Active Outbreak Prevention Policy received" and "Outbreak Prevention Services started."
%vcnt%	• Virus count. • Used by virus outbreak alert.
%vdest%	• Virus/malware destination. • Examples: Email detection: %vdest% is the intended recipient Host-based/Endpoint detection: %vdest% is the endpoint IP address or host name • Used by alert event category.
%vfile%	Infected file name. Used by alert event category.
%vfilepath%	Infected file directory. Used by alert event category.
%vname%	Virus or malware name. Used by alert event category.
%vsrc%	• Virus/malware origin or infection source. • For example, the message sender takes the value of %vsrc% if an antivirus managed product detected a virus/malware in an email message. • Used by the alert event category as well as the network virus alert notification type.

TABLE 10-10. Special Notification Message Variables

VARIABLE	DESCRIPTION
Special variables: Used by Network VirusWall Enforcer task completed-related events	
%action%	Network VirusWall Enforcer action (pass, drop, or quarantine) on network virus.
%description%	Error description used by the potential vulnerability attack detected events.

TABLE 10-11. DLP Notification Message Variables

VARIABLE	DESCRIPTION
DLP variables: Used by scheduled incident summary and incident details updated events	
%DLP_INCIDENT_TOTAL_NUM%	The total number of incidents triggered by directly managed users
%DLP_INCIDENT_HIGH_NUM%	The total number of high severity incidents triggered by directly managed users
%DLP_INCIDENT_MED_NUM%	The total number of medium severity incidents triggered by directly managed users
%DLP_INCIDENT_LOW_NUM%	The total number of low severity incidents triggered by directly managed users
%DLP_INCIDENT_INFO_NUM%	The total number of informational incidents triggered by directly managed users
%DLP_INCIDENT_UNDEFINED_NUM%	The total number of undefined severity incidents triggered by directly managed users
%DLP_INCIDENT_ALLTOTAL_NUM%	The total number of incidents triggered by all managed users
%DLP_INCIDENT_ALLHIGH_NUM%	The total number of high severity incidents triggered by all managed users
%DLP_INCIDENT_ALLMED_NUM%	The total number of medium severity incidents triggered by all managed users

VARIABLE	DESCRIPTION
%DLP_INCIDENT_ALLOW_NUM%	The total number of low severity incidents triggered by all managed users
%DLP_INCIDENT_ALLINFO_NUM%	The total number of informational incidents triggered by all managed users
%DLP_INCIDENT_ALLUNDEFINED_NUM%	The total number of undefined severity incidents triggered by all managed users
%DLP_START_TIME%	The start date and time for the reporting period
%DLP_END_TIME%	The end date and time for the reporting period
%weblink%	The link to view details of the incident information listed in the notification message
%INCIDENTID%	Incident ID number
%SEVERITY%	Incident severity level
%POLICY%	Control Manager policy name **Note** For incidents triggering DLP policies created in managed products, this appears as **N/A**.
%ACCOUNT%	User name
%OLD_STATUS%	Incident status before modification
%NEW_STATUS%	Incident status after modification
%LATEST_COMMENT%	The latest comments about the incident
%DLP_VIOLATION_NUM%	The number of violations matching DLP policies
%DLP_THRESHOLD%	The number of violations that must be triggered to indicate a significant increase on policy violations
%DLP_TEMPLATE%	Template matching the significant incident increase

VARIABLE	DESCRIPTION
%DLP_USER_NAME%	Significant incident increase by user
%DLP_SENDER%	Significant incident increase by sender
%DLP_CHANNEL%	Significant incident increase by channel
%STATUS_CHANGE_TIME%	Incident details updated

TABLE 10-12. Content Security Violation Notification Message Variables

VARIABLE	DESCRIPTION
%subject%	Subject header of the email notification
%sender%	Sender's email address
%recipient%	Recipient's email address
%filtername%	Name of the content filter rule/policy that has been violated
%filteract%%	Action applied by the filter
%msgact%	Action applied to the message

TABLE 10-13. Web Security Violation Notification Message Variables

VARIABLE	DESCRIPTION
%url%	URL in question
%vdestip%	IP address of the target URL
%blockrule%	Name of the rule that has been violated
%blocktype%	Action applied to the URL

TABLE 10-14. C&C Callback Notification Message Variables

VARIABLE	DESCRIPTION
%CALLBACK_ADDR%	URL, IP address, or email address to which a compromised host attempts a callback

VARIABLE	DESCRIPTION
%COMPR_HOST%	Affected host or email address
%CnC_LIST_SRC%	Name of the list that contains the callback address
%CALLBACK_NUM%	Number of contacts made between callback addresses and compromised hosts
%COMPR_HOST_NUM%	Number of compromised hosts involved in the outbreak
%CALLBACK_ADDR_NUM%	Number of callback addresses involved in the outbreak

TABLE 10-15. Advanced Threat Activity Variables

VARIABLE	DESCRIPTION
%hostIP%	Depending on the traffic direction, %hostIP% is IP address determined by Deep Discovery Inspector: • Outbound traffic (internal traffic going to an external network): %hostIP% is the IP address of the endpoint in the network (source) • Traffic within the network: %hostIP% is the IP address of the endpoint in the network • External traffic to an endpoint in a network: %hostIP% is the IP address of the endpoint in the network • Traffic outside the network: %hostIP% is the IP address of the endpoint outside the network
%group%	Name of the subnetwork
%START_TIME%	Start time
%END_TIME%	End time The start and end times define the time range interval. When logs are received during a certain interval, Control Manager calculates those logs. If the alert criteria is met, Control Manager counts the logs. %START_TIME% is the start time of the interval and %END_TIME% is the end time of the interval. The length of the interval is determined by the period threshold in the alert settings.

VARIABLE	DESCRIPTION
%detections%	Number of detections For example: Event: High risk Virtual Analyzer detections IP address: %hostIP% Host name: %computer% Group: %group% Time range: %START_TIME% - %END_TIME% Detections: %detections%

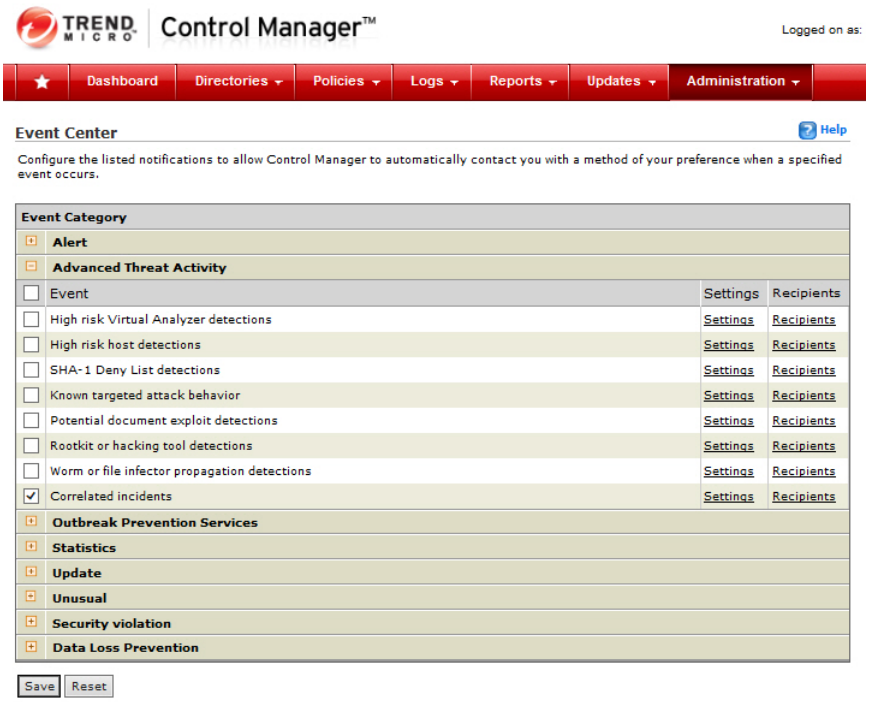
Enabling or Disabling Notifications

Enable or disable notifications from the **Event Center** screen.

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

The **Event Center** screen appears.



2. Expand the Event Category containing the event notification to enable or disable.
3. Do one of the following:
   - Select or clear specific event check boxes.
   - Select or clear the **Event** check box to select all notifications for an entire section.
4. Click **Save**.

Understanding Notification Methods

Control Manager can notify individuals or groups of recipients about events that occur in the Control Manager network. Configure Event Center to send notifications through the following methods:

TABLE 10-16. Notification Delivery Methods

DELIVERY METHOD	DESCRIPTION
Email	Messages sent to a mailbox belonging to the organization's email message system or to an SMTP account (for example, Yahoo!™ or Hotmail™).
Windows event log	The Windows Event Viewer application log contains events logged by Control Manager.
SNMP trap	An SNMP (Simple Network Management Protocol) trap is a method of sending notifications to network administrators who use web consoles that support this protocol. Control Manager stores notification in Management Information Bases (MIBs). Use the **MIBs browser** to view SNMP trap notification.
Pager	An electronic device that accepts messages from a special radio signal.
Trigger Application	Any in-house or industry-standard application used by your organization to send notification. For example, your organization is using a batch file that calls the "net send" command. Use the **Parameters** field to define commands applied by the trigger application.
MSN Messenger	An online service provided by Microsoft that establishes real-time communication between two users. Control Manager sends notifications to an online MSN Messenger account. An off-line MSN Messenger account cannot receive Control Manager notifications.

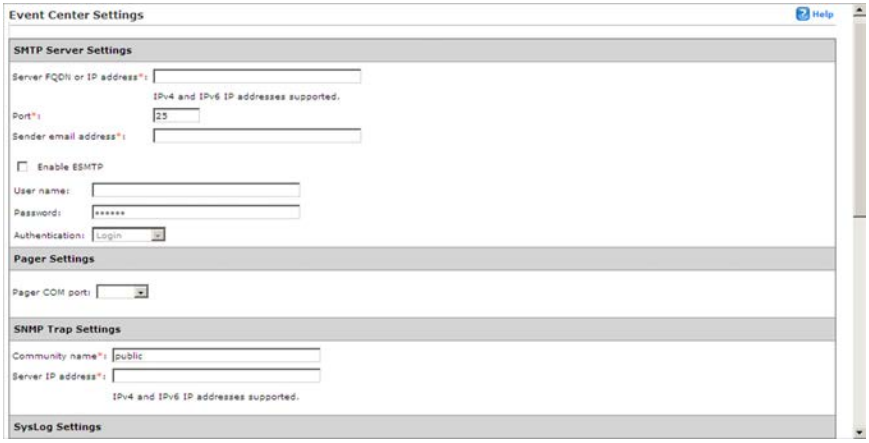
DELIVERY METHOD	DESCRIPTION
Syslog	A standard for forwarding log messages in an IP network. Control Manager can direct syslogs to other supported products. For example, Cisco Security Monitoring, Analysis and Response System (MARS)

Configuring Notification Method Settings

Procedure

- Navigate to **Administration** > **Event Center** > **General Event Settings**.

  The **Event Center Settings** screen appears.



  See the following sections for details about configuring different notification methods.

Setting Email Notifications

Procedure

1. Under **SMTP Server Settings**, type the fully qualified domain name (FQDN) (for example, proxy.company.com) or IP address of the SMTP server in the field provided.
2. Specify the port number in the **Port** field.
3. Type the Control Manager sender email address in the field provided. Control Manager uses this address as the sender address (a requirement for some SMTP servers).
4. To use ESMTP, select **Enable ESMPT**.
5. Type the user name and password in the fields provided for ESMPT authentication.
6. Select the authentication method from the **Authentication** list.
7. Click **Save**.

Setting Pager Notifications

Procedure

1. Under **COM Port**, select the appropriate **Pager COM port** from the list.
2. Click **Save**.

Setting SNMP Notifications

Procedure

1. Under **SNMP Trap Settings**, specify the **Community name**.
2. Specify the SNMP trap **Server IP address**.

3. Click **Save**.

Setting Syslog Notifications

Procedure

1. Under **Syslog Settings**, type the **Server IP address** and **Server Port** of the syslog server.
2. Select the **Facility** for syslogs from the list.
3. Click **Save**.

Triggering a Specified Application

Procedure

1. Under **Trigger Application Settings**, select **Use a specified user to trigger the application**.
2. Type the user name and password of the user who triggers the specified application.
3. Click **Save**.

Setting MSN Messenger Notifications

Procedure

1. Under **MSN Messenger Settings**, specify the **MSN Messenger email address**. This is the user name in MSN Messenger.
2. Type the email address password.
3. If you use a proxy server to connect to the Internet, select **Connect using a proxy server** to connect to the MSN server.

a. Specify the proxy server **Host name** and **Port**.

b. Select the proxy server protocol—**SOCKS 4** or **SOCKS 5**.

c. Type the **logon name** and **password** used for proxy authentication.

4. Click **Save**.

Configuring Notification Recipients and Testing Notification Delivery

Use the **Edit Recipients** screen to configure the notification recipients for each event.

Procedure

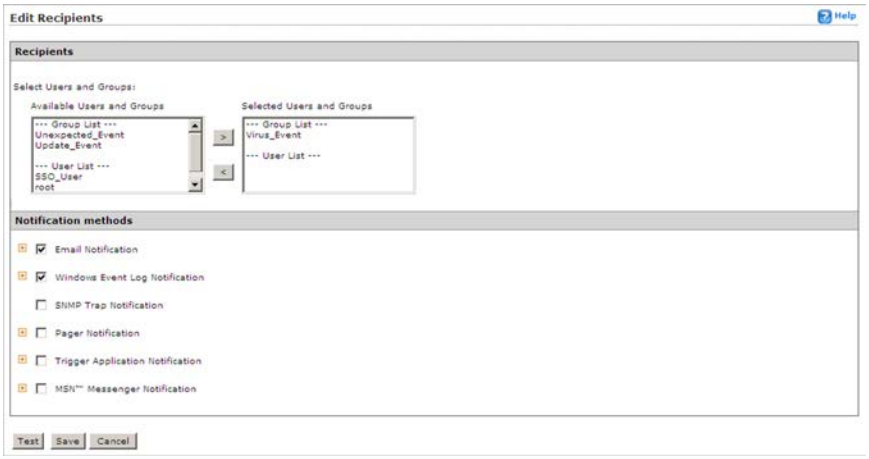
1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the Event Category containing the event notification to configure.

3. Click the **Recipients** link of the event to configure.

   The **Edit Recipients** screen appears.



4. Under **Recipients**, add or remove users in the Selected Users and Groups list for notification recipients:

   - To add recipients to the list:

   a. Click the user or group from the Available Users and Groups list. To select multiple recipients, use the CTRL key.

   b. Click **>** to add the entry to the **Selected Users and Groups** list.

   - To remove a recipient from the list:

   a. Click the user or group from the Selected Users and Groups list. To select multiple recipients, use the CTRL key.

   b. Click **>** to remove the entry from the Selected Users and Groups list.

5. Select a notification method: Configure the notification method settings through the **Event Center Settings** screen.

   Refer to *Configuring Notification Method Settings on page 10-17*.

6. Expand the notification method and provide a **notification message** in the corresponding message fields.

7. Click **Save**.

Note

You can also click **Test** to determine if your system can deliver the notifications. Control Manager will save the settings after the test. However, the test function is not available in the following event types:

- Alerts: C&C callback alert, C&C callback outbreak alert
- Data Loss Prevention: Scheduled incident summary, Incident details updated

Configuring Alert Settings

Alert settings specify when a notification is sent to an administrator or other recipients.

The following table lists the notifications that support modification of notification triggers.

TABLE 10-17. Alert Settings

ALERT	DESCRIPTION
Virus outbreak	Provides a system-wide perspective on virus/malware outbreaks
Special virus	Provides an early warning of a potential virus/malware outbreak
Special spyware/grayware	Provides an early warning of a potential spyware/grayware outbreak
Network virus	Provides a system-wide perspective of a potential network virus outbreak
Potential vulnerability attack detected	Provides a system-wide perspective of a potential attack caused by system vulnerabilities
C&C callback and callback outbreak	Provide system-wide perspectives of potential C&C callback alerts and outbreaks
Advanced Threat Activity	Provide system-wide perspectives of potential advanced persistent threat alerts

Configuring Virus Outbreak Alert Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Alert** Event Category, and click the **Settings** link for **Virus outbreak alert**.

The **Virus Outbreak Alert Settings** screen appears.

3. Under **Alert Settings**, provide the following:
   - **Detections**: The number of viruses that triggers an outbreak alert
   - **Computer or Users**: The number of computers/users infected
   - **Period**: The period of consideration for virus count parameter
4. Click **Save**.

Configuring Special Virus Alert Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Alert** Event Category, and click the **Settings** link for **Special virus alert**.

   The **Special Virus Alert Settings** screen appears.

3. Type the name of the viruses to monitor.

   You can specify up to 10 viruses.

4. Under **Alert Settings**, specify the **Period** (in hours).

5. Click **Save**.

Configuring Special Spyware/Grayware Alert Settings

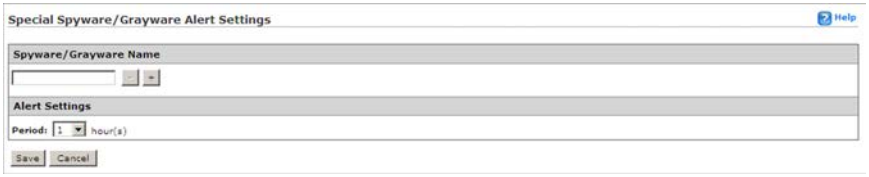
Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Alert** Event Category, and click the **Settings** link for **Special spyware/ grayware alert**.

   The **Special Spyware/Grayware Alert Settings** screen appears.



3. Type the names of the spyware/grayware to monitor.

   You can list up to 10 items of spyware/grayware.

4. Under **Alert Settings**, specify the **Period** (in hours).

5. Click **Save**.

Configuring Network Virus Alert Settings

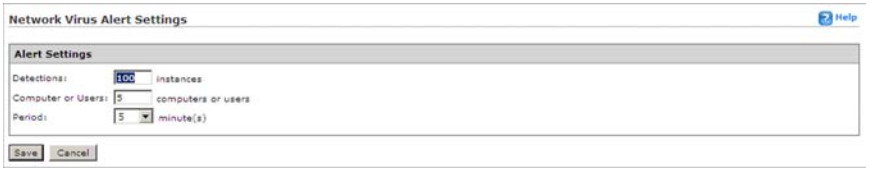
Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Alert** Event Category, and click the **Settings** link for **Network virus alert**.

   The **Network Virus Alert Settings** screen appears.



3. Under Alert Settings, provide the following:

   - **Detections**: The number of viruses that trigger an outbreak alert
   - **Computer or Users**: The number of computers or users infected
   - **Period**: The period of consideration for the virus count parameter

4. Click **Save**.

Configuring Potential Vulnerability Attack Detected Settings

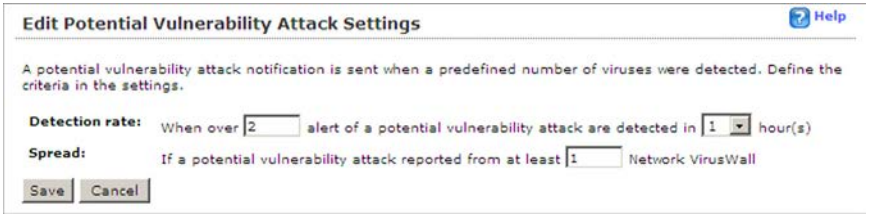
Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Alert** Event Category, and click the **Settings** link for **Potential vulnerability attack detected**.

   The **Edit Potential Vulnerability Attack Settings** screen appears.



3. Provide values for the following:

   - **Detection rate**: The number of alerts triggered over time
   - **Spread**: The number of Network VirusWall Enforcer devices which report the attack

4. Click **Save**.

Configuring C&C Callback Alert Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Advanced Threat Activity Alert Event** category, and click the **Settings** link for **C&C callback alert**.

   The **C&C Callback Alert Settings** screen appears.

3. Select the type of C&C list source to include in the notification message.

4. Click **Save**.

Configuring C&C Callback Outbreak Alert Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Advanced Threat Activity Alert Event** category, and click the **Settings** link for **C&C callback outbreak alert**.

   The **C&C Callback Outbreak Alert Settings** screen appears.

3. Select the type of C&C list source to include in the notification message.

4. Provide the following:

   - **Callback attempts**: The number of callback attempts that trigger an outbreak alert
   - **Compromised hosts**: The number of affected hosts or email addresses
   - **Period**: The period of consideration for callback count parameter

   The **Event Center** settings screen of C&C callback outbreak alert, **Callback attempts**, **Compromised hosts**, and **Period** are conditions that trigger an outbreak alert. For example, if **Period** is set to 1 hour and both **Callback attempts** and **Compromised hosts** have 10 counts, Control Manager issues an alert if there are 10 callback attempts related to 10 compromised hosts in an hour.

5. Click **Save**.

Configuring Advanced Threat Activity Alert Settings

Procedure

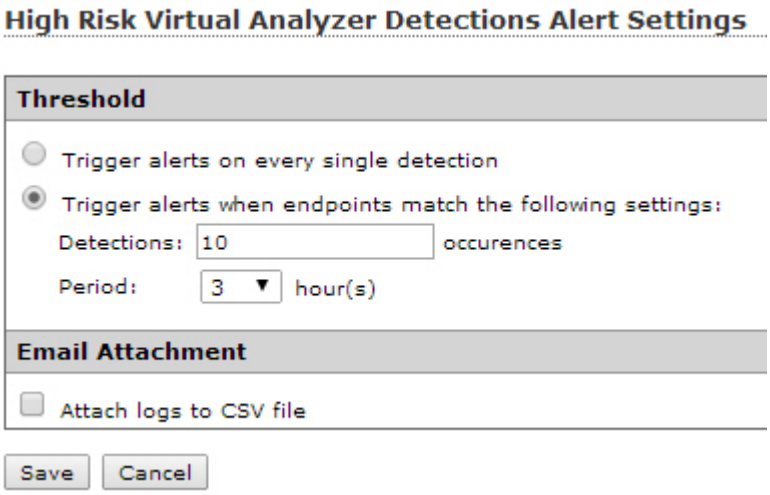
1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Advanced Threat Activity** Event Category, and click the **Settings** link for any of the related events.

   For details, see *Advanced Threat Activity on page 10-4*.

   The **<Advanced Threats Event Type> Settings** screen appears.



3. Under **Threshold**, select any of the following:

   - **Trigger alerts on every single detection**: Send notification when an advanced threat event is detected
   - **Trigger alerts when endpoints match the following settings**: Send only when the number of **detections** and **period** of consideration are met

4. Under **Email Attachment**, select **Attach logs to CSV file** to include a `*.CSV` file attachment with detection details in the notification.

5. Click **Save**.

Configuring Data Loss Prevention Settings

Use the Data Loss Prevention setting screens to specify the time and type of information to send to administrators or other recipients.

Configuring Significant Incident Increase Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Data Loss Prevention** Event Category, and click the **Settings** link for one of the significant incident increase notifications.

   The settings screen for the selected DLP notification appears.

3. Specify the numbers of instances required to trigger the notification in the following fields:

   - **Hourly**
   - **Daily**

4. Click **Save**.

Configuring Scheduled Incident Summary Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Data Loss Prevention** Event Category, and click the **Settings** link for Scheduled incident summary.

   The **Scheduled Incident Summary Settings** screen appears.

3. Under **Frequency**, specify how often to send a notification:
   - **Daily**
   - **Weekly**

   Note
   Control Manager starts to generate notifications at 03:00 on the specified date and updates the status in the **Last notification sent** field.

4. To include an attachment with incident details in the notification, select **Attach incident details** in the following format:
   - CSV (*.csv)
   - Microsoft Excel (*.xls): charts are included

   Note
   Remind incident reviewers to handle the matched content in the attachment with caution, as copying or forwarding the content can trigger additional DLP incidents. Alternatively, administrators can set up exceptions in the DLP rules for actions taken on the matched content.

5. Click **Save**.

Configuring Incident Details Updated Settings

Procedure

1. Navigate to **Administration** > **Event Center** > **Event Notifications**.

   The **Event Center** screen appears.

2. Expand the **Data Loss Prevention** Event Category, and click the **Settings** link for Incident details updated.

   The **Incident Details Updated Settings** screen appears.

3. Specify the updated information to receive:

- **Closed**: Select this to receive notifications when an incident has been closed.
- **Any change**: Select this to receive notifications for any updates, including status change and comment edits.

4. To receive notifications about specific severity levels, specify the filter options:
   - **High**
   - **Medium**
   - **Low**
   - **Informational**
   - **Undefined**
5. Click **Save**.

Chapter 11

Working with Logs

Query logs from all managed products registered to Control Manager from the **Ad Hoc Query** screen.

This chapter contains the following topics:

Using Logs

Although Control Manager receives data from various log types, Control Manager allows users to query the log data directly from the Control Manager database. Users can then specify filtering criteria to gather only the data they need.

Control Manager also introduces log aggregation. Log aggregation can improve query performance and reduce the network bandwidth managed products require when sending logs to Control Manager. However, this comes at a cost of lost data through aggregation. Control Manager cannot query data that does not exist in the Control Manager database.

Understanding Control Manager Generated Logs

Control Manager logs consist of two categories: License and Control Manager Information.

TABLE 11-1. Control Manager Logs

CATEGORY LOG	DESCRIPTION
License Information	These logs record license information for Control Manager and managed products registered to the Control Manager server. • Product License Status • Product License Information Summary • Detailed Product License Information
Control Manager Information	These logs record user actions and product events. • User Access Information • Control Manager Event Information • Command Tracking Information • Detailed Command Tracking Information

Understanding Managed Product Logs

Managed product logs contain information about the performance of your managed products. You can obtain information for specific products or groups of products administered by the parent or child server. With Control Manager's data query on logs and data filtering capabilities, administrators can focus on the information they need.

Note

More logs mean abundant information about the Control Manager network. However, these logs occupy disk space. You must balance the need for information with your available system resources.

Managed products generate different kinds of logs depending on their function.

TABLE 11-2. Managed Product Logs

LOG CATEGORY	DESCRIPTION
Product Information	Product information logs provide information on subjects ranging from user access and events on managed products to component deployment and update status. • Managed Product Information • Component Information

Log Category	Description
Security Threat Information	Security threat logs provide information on known and potential security threats detected on your network. • Virus/Malware Information • Spyware/Grayware Information • Content Violation Information • Spam Violation Information • Policy/Rule Violation Information • Web Violation/Reputation Information • Deep Discovery Information • Advanced Threat Inforrmation Information • Overall Threat Information
Data Protection Information	Data Protection logs provide information on DLP incidents, template matches, and incident sources. • Data Loss Prevention Information • Data Discovery Information

Understanding Log Aggregation

Control Manager log aggregation provides a way for administrators to decrease the impact that managed products have on network bandwidth. By configuring log aggregation administrators can choose which log information managed products send to Control Manager.

Note

Log aggregation comes at a cost. Information that managed products do not send to Control Manager is lost. Control Manager cannot create reports or queries for information the server does not have. This can raise issues if information that seems unimportant, and managed products drop, later becomes of critical importance with no way to recover the dropped data.

Configuring Log Aggregation Settings

Procedure

1. Navigate to **Logs** > **Log Aggregation Settings**.

   The **Edit Log Aggregation Rule** screen appears.

2. Select **Enable log aggregation**.
3. Expand the required log categories.
4. Clear the check boxes for data that managed products will not send to Control Manager.

5. Click **Save**.

Querying Log Data

Ad Hoc Queries provide administrators with a quick method to pull information directly from the Control Manager database. The database contains all information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Ad Hoc Queries provide a very powerful tool for administrators.

While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML format for further analysis or save the query for future use. Control Manager also supports sharing saved queries with other users so others can benefit from useful queries.

Completing an Ad Hoc query consists of the following process:

- Step 1: Select the managed product or current Control Manager server for the query
- Step 2: Select the data view to query
- Step 3: Specify filtering criteria and the specific information that displays
- Step 4: Save and complete the query
- Step 5: Export the data to a CSV or XML file

Note

Control Manager supports sharing saved Ad Hoc Queries with other users. Saved and shared queries appear on the **Saved Ad Hoc Queries** screen.

Understanding Data Views

A data view is a table consisting of clusters of related data cells. Data views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Control Manager allows direct queries to the Control Manager database. Data views are available to Custom report templates and to Ad Hoc Query requests.

Data views are tables filled with information. Each heading in a data view acts as a column in a table. For example, the Virus/Malware Action/Result Summary data view has the following headings:

- Action Result
- Action Taken
- Unique Endpoints
- Unique Sources
- Detections

As a table, a data view takes the following form with potential subheadings under each heading:

TABLE 11-3. Sample Data View

ACTION RESULT	ACTION TAKEN	UNIQUE ENDPOINTS	UNIQUE SOURCES	DETECTIONS

This information is important to remember when specifying how data displays in a report template.

Control Manager separates data views into three major categories: Product Information, Security Threat Information, and Data Protection Information. See the appendix for more information about data views. The major categories separate further into several subcategories, with the subcategories separated into summary information and detailed information.

Related information

↳ *Product Information*
↳ *Security Threat Information*
↳ *Data Protection Information*

Product Information

Product Information data views provide information about Control Manager, managed products, components, and product licenses.

TABLE 11-4. Product Information Data Views

CATEGORY	DESCRIPTION
Control Manager Information	Displays information about Control Manager user access, Command Tracking information, and Control Manager server events.
Managed Product Information	Displays status, detailed, and summary information about managed products or managed product endpoints.
Component Information	Displays status, detailed, and summary information about out of date and up to date and component deployment of managed product components.
License Information	Displays status, detailed, and summary information about Control Manager and managed product license information.

Security Threat Information

Displays information about security threats that managed products detect: viruses, spyware/grayware, phishing sites, and more.

TABLE 11-5. Security Threat Information Data Views

CATEGORY	DESCRIPTION
Virus/Malware Information	Displays summary and detailed data about malware/viruses that managed products detect on your network.
Spyware/Grayware Information	Displays summary and detailed data about spyware/grayware that managed products detect on your network.
Content Violation Information	Displays summary and detailed data about prohibited content that managed products detect on your network.
Spam Violation Information	Displays summary and detailed data about spam that managed products detect on your network.

CATEGORY	DESCRIPTION
Policy/Rule Violation Information	Displays summary and detailed data about policy/rule violations that managed products detect on your network.
Web Violation/ Reputation Information	Displays summary and detailed data about Internet violations that managed products detect on your network.
Deep Discovery Information	Displays summary and detailed data about suspicious activities that managed Deep Discovery products, such as Deep Discovery Inspector and Deep Discovery Email Inspector, detect on your network.
Advanced Threat Information	Displays summary and detailed data about advanced persistent threats and targeted attacks that managed products detect on your network.
Overall Threat Information	Displays summary and statistical data about the overall threat landscape of your network.

Note

See *Data View: Security Threat Information on page B-20* for more information about the available data views Control Manager supports.

Data Protection Information

The Data Loss Prevention Information category displays detailed information about the DLP incidents, incident sources, and template matches that manage products collect on your network.

TABLE 11-6. Data Protection Information Data Views

CATEGORY	DESCRIPTION
Data Loss Prevention Information	Displays summary and detailed data about incidents that DLP found on your network or detections that match available DLP templates.

CATEGORY	DESCRIPTION
Data Discovery Information	Displays summary and detailed data about DLP detections or Data Discovery endpoints, including detailed information about sensitive files and OfficeScan endpoints.

Data View Terminology

Control Manager uses the following terms in data views, returned queries, and generated reports.

Note

For a complete list of data view terminology, see *Data Views on page B-1*.

TABLE 11-7. Data View Terminology

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of a computer.
IP	Displays the IP address of a computer.
Port	Displays the port number of an computer.
MAC	Displays the MAC address of an computer.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product Host	Displays the host name of the server on which the managed product installs.
Product IP	Displays the IP address of the server on which the managed product installs.
Product MAC	Displays the MAC address of the server on which the managed product installs.

DATA	DESCRIPTION
Product Version	Displays the managed product's version number. Example: OfficeScan 10.0, Control Manager 5.0
Source Host	Displays the IP address or host name of the computer where security threats originate.
Source IP	Displays the IP address of the computer where security threats originate.
Source Port	Displays the port number of the computer where security threats originate.
Source MAC	Displays the MAC address of the computer where security threats originate.
Unique Endpoints	Displays the number of unique computers affected by security threats. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. Unique Endpoints = 3
Unique Sources	Displays the number of unique infection sources where security threats originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. Unique Sources = 2
Unique Senders/ Users	Displays the number of unique email message addresses or users sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. Unique Senders/Users = 3
Unique Recipients	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. Unique Recipients = 2

DATA	DESCRIPTION
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Unique Detections = 1
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Understanding Ad Hoc Queries

An Ad Hoc Query is a direct request to the Control Manager database for information. The query uses data views to narrow the request and improve performance. After specifying the data view, users can further narrow their search by specifying filtering criteria for the request.

Note

For more information on data views see *Understanding Data Views on page 11-6*.

For example, Chris, an OfficeScan administrator, wants to check the status of pattern files for the OfficeScan servers for which she is responsible. Chris first selects **Managed Products**. She then selects the data view **Pattern/Rule Status** found under **Product Information** > **Component Information**. Proceeding to the next step in the process, she specifies the filtering criteria as follows: Product Type: OfficeScan, Pattern Status: Out-of-date. Clicking **Change column display**, Chris also selects the fields the query displays after the query completes. Chris selects the following to display: Pattern Version, Host Name, IP Address. She does not select Product Name or Pattern Status, because she already knows the results that Control Manager returns meet that criteria.

Note

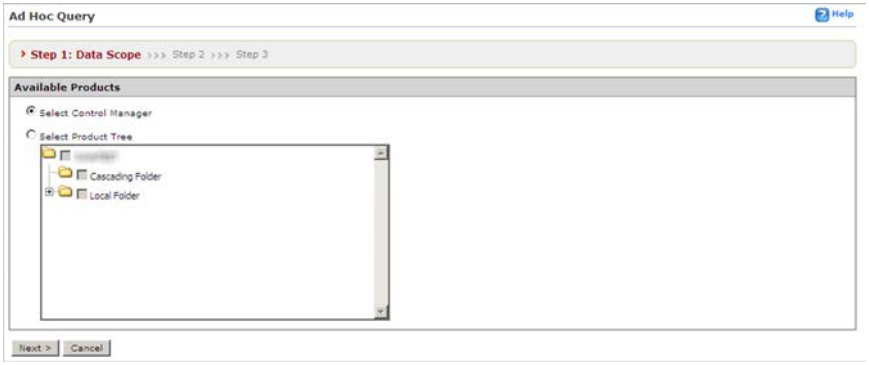
Saving an Ad Hoc Query saves only the criteria specified for the query. The data an Ad Hoc Query returns does not save. To save the data, export the query results or create a report using a grid table.

Performing an Ad Hoc Query

Procedure

1. Navigate to **Logs** > **New Ad Hoc Query**.

   The **Ad Hoc Query** screen appears.



2. Follow the steps below to perform an Ad Hoc Query.

Step 1: Specify the Origin of the Information

Procedure

1. From the **Ad Hoc Query** screen, select the origin for the information query:

   - **Select Control Manager**: Specifies that information originates from the Control Manager server to which the user is currently logged on.

Specifying this option disables the Product Tree, because the information only comes from the Control Manager server to which the user is logged on.

- **Select Product Tree**: Specifies that information originates from the managed products the Control Manager server manages. This can include managed products from child Control Manager servers.

  After specifying this option, the user must then select the managed products or directory from which the information originates.

Note

Selecting the managed product or directory on this screen affects the available data views on the following screen. For example, by selecting OfficeScan in the product directory, only data views associated with OfficeScan display in the Available Data Views list.

2. Click **Next**.

Step 2: Specify a Data View for the Query

Procedure

1. Select a data view from the **Available Data Views** list.

   For more information on data views, see *Understanding Data Views on page 11-6*.

2. Click **Next**.

Step 3: Specify the Display Sequence

Procedure

1. Click **Change Column Display**.

The **Select Display Sequence** screen appears.

2. From the **Available Fields** list, select the data view columns to display when the query returns information.

   Selected columns highlight.

Note

Select the columns one at a time or use the SHIFT or CTRL keys to select multiple columns.

Selecting and adding one column at a time is one method that allows users to specify the sequence in which the information displays.

---

3. Click (>) to include the fields in the **Selected Fields** list.

   Selected columns appear in the Selected Fields list.

4. Continue selecting and adding columns until you have all the columns you require.

5. Use the **Move Up** and **Move Down** buttons, after selecting a column in the Selected Fields list, to specify the display sequence of the information. The column at the top of the list appears as the left-most column in the returned query.

6. Click **Back**.

Step 4: Specify the Filtering Criteria

Procedure

1. Specify the **Required Criteria**:

   - Specify a Summary Time for the data, and for spyware/grayware data views, whether you want COOKIES to appear in your results.

2. Specify the **Custom Criteria**:

   a. Select **Custom criteria**.

   The custom criteria options appear.

   b. Specify the criteria filtering rules for the data categories from the **Match** field:

   - **All of the criteria**: This selection acts as a logical "AND" function. Data appearing in the report must meet all the filtering criteria.
   - **Any of the criteria**: This selection acts as a logical "OR" function. Data appearing in the report must meet any of the filtering criteria.

   c. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

   Note

   If you do not specify any filtering criteria, the Ad Hoc Query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

   i. From the left-most drop-down list, select the column to filter.

   ii. From the middle drop-down list, select the matching condition for the filter.

   iii. In the right-most field, provide the filter criteria. A list box or text box appears here depending on the column selected to filter.

   iv. Click the **+** icon to add another filter criterion for the data view.

Step 5: Save and Complete the Query

Procedure

1. Click **Save this query to the saved Ad Hoc Queries list** under **Save Query Settings** to save the Ad Hoc Query.
2. Specify an Ad Hoc Query name in the **Query Name** field.

   Note

   Control Manager supports sharing saved Ad Hoc Queries with other users. Saved Queries appear on the **Saved Ad Hoc Queries** screen.

3. Click **Query**.

Step 6: Export the Query Results to CSV or XML

Procedure

1. A **File Download** dialog box appears after clicking one of the following:
   - **Export to CSV**: Exports the query results to CSV format.
   - **Export to XML**: Exports the query results to XML format.
2. Complete one of the following:
   - Click **Open** to view the query results immediately in CSV or XML format.
   - Click **Save**. A **Save As** dialog box appears. Specify the location to save the file.
3. To save the settings for the query:
   a. Click **Save query settings**.

      A confirmation dialog box appears.

   b. Type a name for the saved query in the **Query Name** field.

c. Click **OK**.

Working with Saved and Shared Ad Hoc Queries

Control Manager supports saving an Ad Hoc Query a user creates. Saved Ad Hoc Queries appear on the **Saved Ad Hoc Queries** screen. The **Saved Ad Hoc Queries** screen contains two tabs: **My Queries** and **Available Queries**.

The **My Queries** section of the **Saved Ad Hoc Queries** screen displays all Ad Hoc Queries the logged on user created. From the **My Queries** tab, the user can add, edit, view, delete, export, and share/unshare queries. Sharing saved queries makes the queries available to other users.

Note

Control Manager access control, provided by the user account and user role, restricts the information to which a user has access. This means that even though all users can view shared queries, access control limits the effectiveness of the query.

Example:

OfficeScan administrator Chris creates and shares an Ad Hoc Query that targets OfficeScan server information. ScanMail for Exchange administrator Sam has access to the shared query, but if she tries to generate an Ad Hoc Query using Chris' query, the query returns blank. This occurs because Sam does not have access to OfficeScan server information. This example assumes Chris only has access to OfficeScan servers and Sam only has access to ScanMail for Exchange servers.

Editing Saved Ad Hoc Queries

Control Manager supports modifying saved Ad Hoc Queries from the **My Queries** tab of the **Saved Ad Hoc Queries** screen.

Procedure

1. Navigate to **Logs** > **Saved Ad Hoc Queries**.

   The **Saved Ad Hoc Queries** screen appears.

2. Click the name of the saved Ad Hoc Query to edit.

   The **Select Product Tree** screen appears.

Step 1: Specify the Origin of the Information

Procedure

1. From the **Ad Hoc Query** screen, specify the network protection category (managed product or directory) from which the report generates.

   - **Select Control Manager**: Specifies that information originates from the Control Manager server to which the user is currently logged on.

     Specifying this option disables the Product Tree, because the information only comes from the Control Manager server to which the user is logged on.

   - **Select Product Tree**: Specifies that information originates from the managed products the Control Manager server manages.

     After specifying this option, the user must then select the protection category from which the information originates. The user does this by selecting managed products/directories from the Product Directory.

   Note

   Selecting the managed product/directory on this screen affects the available data views. For example, by selecting OfficeScan in the product directory only data views associated with desktop protection display in the Data Views list.

2. Click **Next**.

Step 2: Specify a Data View for the Query

Procedure

1. Select a data view from the **Available Data Views** list.

For more information on data views, see *Understanding Data Views on page 11-6*.

2. Click **Next**.

Step 3: Specify the Display Sequence

Specify the display and sequence for the information the query returns:

Procedure

1. Click **Change column display**.

   The **Select Display Sequence** screen appears.

2. From the **Available Fields** list, select the data view columns that display when the query returns information.

   Selected columns highlight.

   Tip

   Select the columns one at a time or use the **Shift** or **Ctrl** keys to select multiple columns.

   Selecting and adding one column at a time is one method that allows users to specify the sequence which the information displays.

   ---

3. Click (>) to include the fields in the **Selected Fields** list.

   Selected columns appear in the Selected Fields list.

4. Continue selecting and adding columns until you have all the columns you require.

5. Use the **Move Up** and **Move Down** buttons, after selecting a column in the Selected Fields list, to specify the display sequence of the information. The column at the top of the list appears as the left-most column in the returned query.

6. Click **Back**.

Step 4: Specify the Filtering Criteria

When querying for summary data (any data view with the word Summary in the title), you must specify items under **Required Criteria**.

Procedure

1. Specify the **Required Criteria**:
   - Specify a Summary Time for the data or whether you want COOKIES to appear in your reports.
2. Specify the **Custom Criteria**:
   a. Select **Custom criteria**.

      The custom criteria options appear.

   b. Specify the criteria filtering rules for the data categories from the **Match** field:
      - **All of the criteria**: This selection acts as a logical "AND" function. Data appearing in the report must meet all the filtering criteria.
      - **Any of the criteria**: This selection acts as a logical "OR" function. Data appearing in the report must meet any of the filtering criteria.

   c. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

      Note

      If you do not specify any filtering criteria, the Ad Hoc Query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

      i. From the left-most drop-down list, select the column to filter.

      ii. From the middle drop-down list, select the matching condition for the filter.

      iii. In the right-most field, provide the filter criteria. A list box or text box appears here depending on the column selected to filter.

iv. Click the + icon to add another filter criterion for the data view.

Step 5: Save and Complete the Query

Procedure

1. Click **Save this query to the saved Ad Hoc Queries list** under **Save Query Settings** to save the Ad Hoc Query.
2. Specify an Ad Hoc Query name in the **Query Name** field.

> **Note**
>
> Control Manager supports sharing saved Ad Hoc Queries with other users. Saved queries appear on the **Saved Ad Hoc Queries** screen.

3. Click **Query**.

Step 6: Export the Query Results to CSV or XML

Procedure

1. A **File Download** dialog box appears after clicking one of the following:
   - **Export to CSV**: Exports the query results to CSV format.
   - **Export to XML**: Exports the query results to XML format.
2. Complete one of the following:
   - Click **Open** to view the query results immediately in CSV or XML format.
   - Click **Save**. A **Save As** dialog box appears. Specify the location to save the file.

Sharing Saved Ad Hoc Queries

Control Manager supports sharing saved Ad Hoc Queries from the **My Queries** tab of the **Saved Ad Hoc Queries** screen.

Procedure

1. Navigate to **Logs** > **Saved Ad Hoc Queries**.

   The **Saved Ad Hoc Queries** screen appears.

2. Click the check box for the associated Ad Hoc Query to share.

3. Click **Share**.

   An icon appears in the **Shared** column for the saved Ad Hoc Query.

Working With Shared Ad Hoc Queries

After creating an Ad Hoc Query, a user can share the query with other users. All shared queries from all users appear on the Available Queries tab of the **Saved Ad Hoc Queries** screen. Users can view and export shared queries.

Procedure

1. Navigate to **Logs** > **Saved Ad Hoc Queries**.

   The **Saved Ad Hoc Queries** screen appears.

2. Click the **Available Queries** tab.

3. Use the queries to view information or to export shared queries.

Deleting Logs

Use the **Log Maintenance** screen to immediately delete logs or to configure automatic log deletion.

Note

Trend Micro recommends backing up Data Loss Prevention logs to Security Information and Event Management (SIEM) and keeping them for at least 2 years.

Procedure

1. Navigate to **Logs** > **Log Maintenance**.

   The **Log Maintenance** screen appears.

2. Select the corresponding check box for the logs you want to delete.

3. Click **Delete All** in the corresponding row for logs you want to remove.

Configuring Automatic Log Deletion Settings

The **Log Maintenance** screen provides two methods for deleting logs automatically:

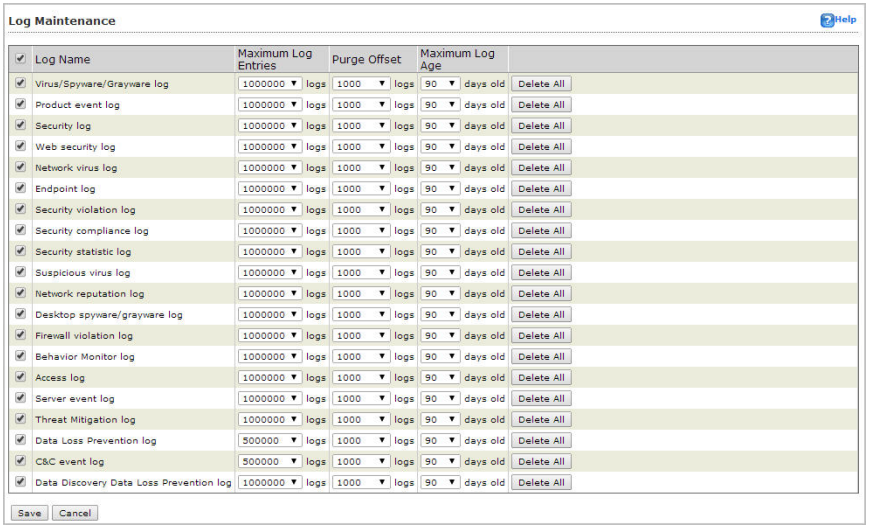
- By number of logs (minimum: 30,000, maximum: 1,000,000, default: 1,000,000)
- By the age of logs (minimum: 1 day, maximum: 360 days, default: 90 days)

Purge offset specifies the number of logs Control Manager deletes when the number of logs for a log type reaches the maximum. The default purge setting is 1000 for all log types.

Procedure

1. Navigate to **Logs** > **Log Maintenance**.

The **Log Maintenance** screen appears.



2. Select the corresponding check box for the logs for which you want to configure settings.

3. Specify the maximum number of logs that Control Manager retains in the **Maximum Log Entries** column.

4. In **Purge Offset**, specify the number of logs Control Manager removes when the number of logs reaches the number specified in the **Maximum Log Entries** column.

5. In **Maximum Log Age**, specify the age of logs that Control Manager deletes automatically.

6. Click **Save**.

Chapter 12

Working with Reports

Generate reports using the log data collected from all managed products registered to Control Manager.

This chapter contains the following topics:

Understanding Reports

Control Manager reports consist of two parts: report templates and report profiles. Where a report template determines the look and feel of the report, the report profile specifies the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 introduced radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control Manager 6.0 Service Pack 3 continues to support report templates from previous Control Manager versions, including custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager categorizes report templates according to the following types:

- Custom templates: User-defined customized report templates that use direct database queries (database views) and report template elements (charts and tables). Users have greater flexibility specifying the data that appears in their reports compared to report templates from previous Control Manager versions. For more information on Custom templates, see *Understanding Custom Templates on page 12-3*.

  Note

  Default customized report templates do not support generating PDFs in landscape format. Use the portrait format for default templates or make a new tempate using the landscape format.

- Static templates: Includes pre-defined templates. For more information on Static templates, see *Understanding Static Templates on page 12-10*.

Understanding Custom Templates

Custom templates use database views as the information foundation for reports. For more information on data views, see *Understanding Data Views on page 11-6*. The look and feel of generated reports falls to the report elements. Report elements consist of the following.

TABLE 12-1. Custom Template Elements

TEMPLATE ELEMENT	DESCRIPTION
Page break	Inserts a page break for a report. Each report page supports up to three report template elements.
Static text	Provides a user-defined description or explanation for the report. Static text content can contain up to 4096 characters.
Bar chart	Inserts a bar chart into a report template.
Line chart	Inserts a line graph into a report template.
Pie chart	Inserts a pie chart into a report template.
Dynamic table	Inserts a dynamic table/pivot table into a report template.
Grid table	Inserts a table into a report template. The information in a grid table will be the same as the information that displays in an Ad Hoc Query.

Each Custom template can contain up to 100 report template elements. Each page in the report template can contain up to three report template elements. Use page breaks to create report template pages.

To better understand Custom templates, Trend Micro provides the following pre-defined report templates.

Note

Access the **Report Templates** screen to view the Trend Micro pre-defined templates.

TABLE 12-2. Pre-defined Custom Templates

TEMPLATE	DESCRIPTION
DDEI Daily Report	Deep Discovery Email Inspector provides scheduled reports (daily, weekly, or monthly) to assist in mitigating threats and optimizing system settings. Scheduled reports can be generated from the provided templates. Deep Discovery Email Inspector offers flexibility in specifying the content for each report.
DDEI Monthly Report	
DDEI Weekly Report	
TM-Content Violation Detection Summary	Provides the following information: • Content Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Sender/Users in Violation Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Content Violation Policy Summary (Grid table) • Top 25 Senders/Users in Violation (Bar chart) • Content Violation Senders/Users in Violation Summary (Grid table) • Action Result Summary (Pie chart)

TEMPLATE	DESCRIPTION
TM-Deep Discovery Inspector Host Severity Summary	Provides the following information: • Summary (number of affected hosts and detections reported by Deep Discovery Inspector threat engines, and Virtual Analyzer, in relation to the attack phases) • Detections by Attack Phase (Grid table) • Trends by Type (Line chart) • Detection Trends (Line chart) • Affected Hosts (Grid table) • Threat Activity Details for Affected Hosts (CSV file) • C&C Communication (Grid table) • Geographic Distribution of C&C Servers (Pie chart and map) • Virtual Analyzer Detections (Grid table) • Scan Engine Detections (Grid table) • Lateral Movement (Grid table)

TEMPLATE	DESCRIPTION
TM-Deep Discovery Inspector Suspicious Threat Detection Summary	Provides the following information: • Suspicious Threat Detection Grouped by Day (Line chart) • Rule in Violation Count Grouped by Day (Line chart) • Sender Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Source IP Address Count Grouped by Day (Line chart) • Destination IP Address Count Grouped by Day (Line chart) • Top 25 Senders (Bar chart) • Top 25 Recipients (Bar chart) • Suspicious Threat Sender Summary (Grid table) • Suspicious Threat Riskiest Recipient Summary (Grid table) • Top 25 Source IP Addresses (Bar chart) • Top 25 Destination IP Addresses (Bar chart) • Suspicious Threat Source Summary (Grid table) • Suspicious Threat Riskiest Destination Summary (Grid table) • Top 25 Protocol Names (Bar chart) • Suspicious Threat Protocol Detection Summary (Grid table) • Overall Suspicious Threat Summary (Grid table)

TEMPLATE	DESCRIPTION
TM-Managed Product Connection/ Component Status	Provides the following information: • Server/Appliance Connection Status (Pie chart) • Client Connection Status (Pie chart) • Server/Appliance Pattern File/Rule Update Status (Pie chart) • Client Pattern File/Rule Update Status (Pie chart) • Server/Appliance Scan Engine Update Status (Pie chart) • Client Scan Engine Update Status (Pie chart) • Pattern File/Rule Summary for Servers/Appliances (Grid table) • Pattern File/Rule Summary for Clients (Grid table) • Scan Engine Summary for Servers/Appliances (Grid table) • Scan Engine Summary for Clients (Grid table)
TM-Overall Threat Summary	Provides the following information: • Complete Network Security Risk Analysis Summary (Grid table) • Network Protection Boundary Summary (Grid table) • Security Risk Entry Point Analysis Information (Grid table) • Security Risk Destination Analysis Information (Grid table) • Security Risk Source Analysis Information (Grid table)

TEMPLATE	DESCRIPTION
TM-Spam Detection Summary	Provides the following information: • Spam Detection Grouped by Day (Line chart) • Recipient Domain Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Top 25 Recipient Domains (Bar chart) • Overall Spam Violation Summary (Grid table) • Top 25 Spam Recipients (Bar chart) • Spam Recipient Summary (Grid table)
TM-Spyware/ Grayware Detection Summary	Provides the following information: • Spyware/Grayware Detection Grouped by Day (Line chart) • Unique Spyware/Grayware Count Grouped by Day (Line chart) • Spyware/Grayware Source Count Grouped by Day (Line chart) • Spyware/Grayware Destination Count Grouped by Day (Line chart) • Top 25 Spyware/Grayware (Bar chart) • Overall Spyware/Grayware Summary (Grid table) • Top 25 Spyware/Grayware Sources (Bar chart) • Spyware/Grayware Source Summary (Grid table) • Top 25 Spyware/Grayware Destinations (Bar chart) • Spyware/Grayware Destination Summary (Grid table) • Action Result Summary (Pie Chart) • Spyware/Grayware Action/Result Summary (Grid table)

TEMPLATE	DESCRIPTION
TM-Virus/Malware Detection Summary	Provides the following information: • Virus/Malware Detection Grouped by Day (Line chart) • Unique Virus/Malware Count Grouped by Day (Line chart) • Infection Destination Count Grouped by Day (Line chart) • Top 25 Virus/Malware (Bar chart) • Overall Virus/Malware Summary (Grid table) • Top 25 Infection Sources (Bar chart) • Virus/Malware Infection Source Summary (Grid table) • Top 25 Infection Destinations (Bar chart) • Virus/Malware Infection Destination Summary (Grid table) • Action Result Summary (Pie chart) • Virus/Malware Action/Result Summary (Grid table)
TM-Web Violation Detection Summary	Provides the following information: • Web Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Client in Violation Count Grouped by Day (Line chart) • URL in Violation Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Overall Web Violation Summary (Grid table) • Top 25 Clients in Violation (Bar chart) • Web Violation Client IP Address Summary (Grid table) • Top 25 URLs in Violation (Bar chart) • Web Violation URL Summary (Grid table) • Filter/Blocking Type Summary (Pie chart)

Understanding Static Templates

Control Manager provides 91 pre-generated report templates divided into seven categories: Executive Summary, Gateway, Mail Server, Server, Desktop, Network Products, Data Loss Prevention and Data Discovery.

Note

In Control Manager 3.5, spyware/grayware were no longer considered viruses. This change affects the virus count in all original virus-related reports.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

Use the Report Category list on the Control Manager screen to peruse the six categories of reports listed below:

TABLE 12-3. Executive Summary Reports and Report Types

EXECUTIVE SUMMARY REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/Grayware (10, 25, 50, 100) • Detected Spyware/Grayware list for all entities
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100) • Virus infection list for all entities
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month) • Damage cleanups, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month)

Executive Summary Reports	Report Types
Vulnerability Reports	• Machine risk level assessment • Vulnerability assessment • Most commonly cleaned infections (10, 25, 50, 100) • Worst damage potential vulnerabilities (10, 25, 50, 100) • Vulnerabilities ranked by risk level

Table 12-4. Gateway Product Reports and Report Types

Gateway Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary • OPS deployment rate for IMSS

TABLE 12-5. Mail Server Product Reports and Report Types

MAIL SERVER PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Top senders of infected email (10, 25, 50, 100) • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

TABLE 12-6. Server Based Product Reports and Report Types

SERVER BASED PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

TABLE 12-7. Desktop Product Reports and Report Types

DESKTOP PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	The data in this report type contains both computer and mobile device detections. • Spyware/Grayware detected • Most commonly detected Spyware/Grayware (10,25,50,100)
Virus Detection Reports	The data in this report type contains both computer and mobile device detections. • Viruses detected • Most commonly detected viruses (10,25,50,100)
OfficeScan Agent Information Reports	• Detailed summary • Basic summary
OfficeScan Product Registration Report	Registration status
Comparative Reports	The data in this report type contains both computer and mobile device detections. • Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
OfficeScan Server Deployment Reports	• Detailed summary • Basic summary • Detailed failure rates summary
OfficeScan Damage Cleanup Services Reports	• Detailed summary • Most commonly cleaned infections (10, 25, 50, 100)

TABLE 12-8. Network Product Reports and Report Types

NETWORK PRODUCT REPORTS	REPORT TYPES
Network VirusWall Reports	• Policy violation report, grouped by (Day, Week, Month) • Most commonly detected violative clients (10, 25, 50, 100) • Service violation report, grouped by (Day, Week, Month)
Trend Micro Deep Discovery Inspector Reports	• Incident summary report, grouped by (Day, Week, Month) • High risk clients (10, 25, 50, 100) • Summary of known and unknown risks report

TABLE 12-9. Data Loss Prevention Reports and Report Types

DATA LOSS PREVENTION REPORTS	REPORT TYPES
Top DLP Incident Sources	• Incidents by sender (10, 20, 30, 40, 50) • Incidents by host name (10, 20, 30, 40, 50) • Incidents by recipient (10, 20, 30, 40, 50) • Incidents by source IP address (10, 20, 30, 40, 50) • Incidents by URL (10, 20, 30, 40, 50) • Incidents by User (10, 20, 30, 40, 50) • Top template matches (10, 20, 30, 40, 50) • Incident distribution by channel • Incident trend, grouped by (Day, Week, Month) • Incidents by channel, grouped by (Day, Week, Month)

Data Loss Prevention Reports	Report Types
Significant Incident Increase	• Significant incident increase (%) by channel (10, 20, 30, 40, 50) • Significant incident increase by channel (10, 20, 30, 40, 50) • Significant incident increase (%) by sender (10, 20, 30, 40, 50) • Significant incident increase by sender (10, 20, 30, 40, 50) • Significant incident increase (%) by hostname (10, 20, 30, 40, 50) • Significant incident increase by hostname (10, 20, 30, 40, 50) • Significant incident increase (%) by user (10, 20, 30, 40, 50) • Significant incident increase by user (10, 20, 30, 40, 50) • Significant incident increase (%) by source IP address (10, 20, 30, 40, 50) • Significant incident increase by source IP address (10, 20, 30, 40, 50) • Significant incident increase (%) by template (10, 20, 30, 40, 50) • Significant incident increase by template (10, 20, 30, 40, 50)

Table 12-10. Data Discovery Reports and Report Types

Data Discovery Reports	Report Types
Top Data Discovery Detection Sources	• Top endpoints with sensitive files (3, 5, 10) • Top Data Discovery template matches (3, 5, 10) • Top sensitive file policy detections (3, 5, 10) • Top sensitive files (3, 5, 10)

Adding Custom Templates

Custom templates allow greater flexibility for report generation than previous versions of Control Manager templates. Custom templates directly access the Control Manager database, providing users the opportunity to create reports based on any information the Control Manager database contains.

Adding a Custom template requires the following steps:

Procedure

1. *Step 1: Access the Add Report Template Screen and Name the Template on page 12-16*
2. *Step 2: Specify the Template Component to Add to the Report Template on page 12-18*
3. *Step 3: Specify the Data View for the Template on page 12-18*
4. *Step 4: Specify the Query Criteria for the Template on page 12-20*
5. *Step 5: Specify the Data to Appear in the Report and the Order in Which the Data Appears on page 12-21*
6. *Step 6: Complete Report Template Creation on page 12-31*

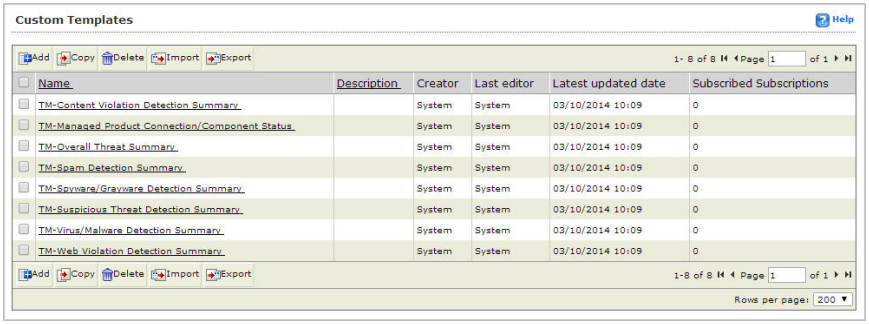
Step 1: Access the Add Report Template Screen and Name the Template

---

Procedure

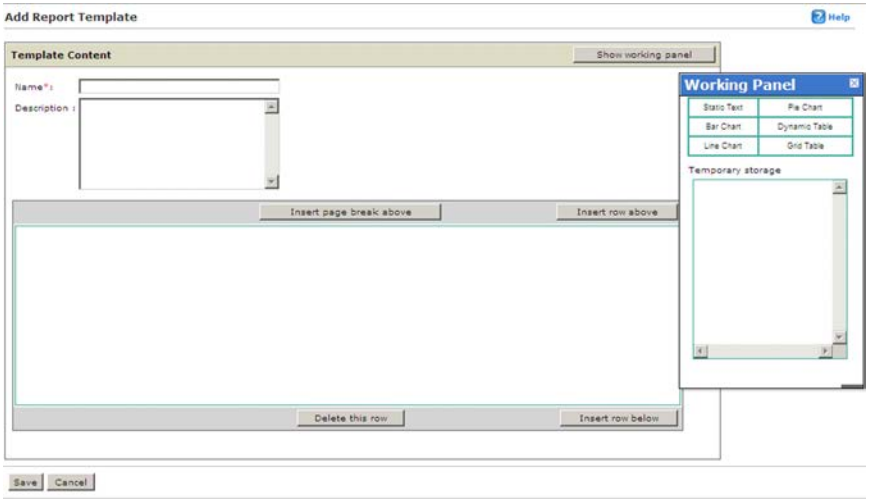
1. Navigate to **Reports** > **Custom Templates**.

The **Custom Templates** screen appears.



2. Click **Add**.

   The **Add Report Template** screen appears.



3. Type a name for the report template in the **Name** field.
4. Type a description for the report template in the **Description** field.

Step 2: Specify the Template Component to Add to the Report Template

Procedure

1. Drag a report template element from the Working Panel to the report template:
   - **Static Text**: Text a user inserts into the template. This could be a summary of the information that the report presents.
   - **Pie Chart**: Report data displays in a pie chart
   - **Bar Chart**: Report data displays in a bar chart
   - **Dynamic Table**: Report data displays in a table similar to a pivot table
   - **Line Chart**: Report data displays in a line chart
   - **Grid Table**: Report data displays in a table like an Ad Hoc Query table
2. Add multiple components to make the report comprehensive.

   You can add up to three components per page and 100 report components to a report template.
3. Add page breaks and rows to the report template to separate data or report template elements.

Step 3: Specify the Data View for the Template

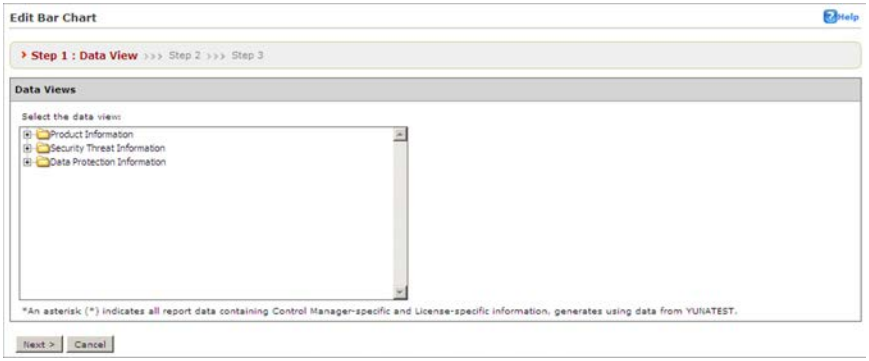
Procedure

1. Click **Edit** on a report template element.

   The **Edit <Report Template Element> Step 1: Data View** screen appears.

Note

For every component except Static text, the **Edit <Report Template Element> Step 1: Data View** screen appears. The **Edit** link in Static Text opens the **Edit Static Text** screen.



2. Select the data to query from the **Data Views** area.

   For more information on Data Views, see *Understanding Data Views on page 11-6*.

3. Click **Next**.

The **Step 2: Set Query Criteria** screen appears.

Step 4: Specify the Query Criteria for the Template

Note

If you do not specify any filtering criteria, the report returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the report returns.

Procedure

1. Select **Custom criteria**.
2. Specify the criteria filtering rules for the data categories:
   - **All of the criteria**: This selection acts as a logical "AND" function. Data appearing in the report must meet all the filtering criteria.
   - **Any of the criteria**: This selection acts as a logical "OR" function. Data appearing in the report must meet any of the filtering criteria.
3. Specify the data, the operator, and the specific criteria to filter. Control Manager supports specifying up to 20 criteria for filtering data.

Step 5: Specify the Data to Appear in the Report and the Order in Which the Data Appears

Depending on the selection for the report element, specify the data to display in reports:

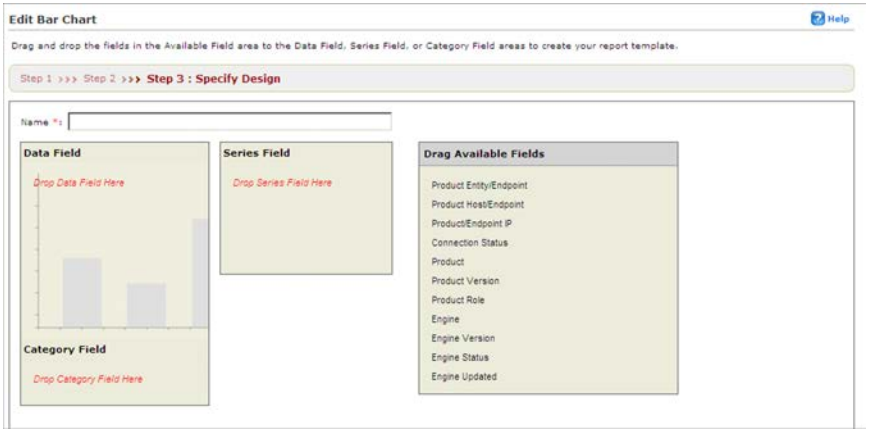
- Bar chart
- Pie chart
- Dynamic table
- Grid table
- Line chart

Configuring Bar Chart Settings

Procedure

1. Click **Next**.

   The **Step 3: Specify Design** screen appears.



2. Type a name for the bar chart in the **Name** field.

3. Drag items from the **Drag Available Fields** list to the following areas:

   - **Data Field**: Specifies the data that appears along the vertical axis of the bar chart
   - **Series Field**: Specifies additional data that can appear along the horizontal axis
   - **Category Field**: Specifies the data that appears along the horizontal axis of the bar chart

4. Specify the Data Properties for the Data Field:

   a. Type a meaningful label in the **Value label** field.

   b. Specify how the data displays for **Data Field** from the Aggregated by list:

      - **Total number of instances**: Specifies that the total count for the number of incidents is used for the results
      - **Number of unique instances**: Specifies that only the count for distinct items is used for the results
      - **Sum of value**: Specifies that the sum of all the values in the "Count" of a Data View column is used for the results

      Example: OfficeScan detects 10 virus instances of the same virus on one computer. The **Count number of row** displays 10, while Count distinct row displays 1.

5. Specify the Category Properties for the **Category Field**:

   a. Type a meaningful name in the **Label name** field.

   b. Specify how to sort the data in the chart from the Sorting lists:

      - **Aggregation value**: Sorts the data according to the data values.
      - **Category name**: Sorts the data according to the alphabetic order of the category names.
      - **Ascending**: Sorts the data in ascending order.
      - **Descending**: Sorts the data in descending order.

c. Specify how many items display in the **Category Field** by selecting **Filter summarized result** and specifying a value in the **Display top** text box.

The default value is 10.

d. Select **Aggregate remaining items** to put all remaining items into the group "Other" on the graph.

6. Specify the Series Properties for the **Series Field**:

a. Type a meaningful label in the **Label name** field.

7. Click **Save**.

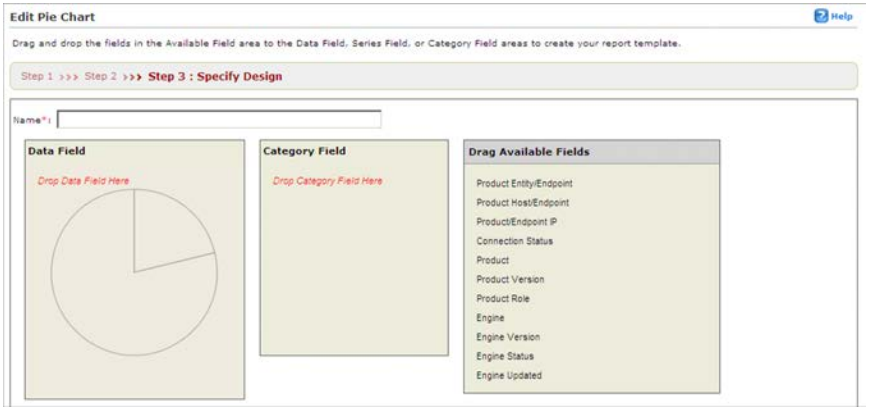
The **Add Report Template** screen appears.

Configuring Pie Chart Settings

Procedure

1. Click **Next**.

The **Step 3: Specify Design** screen appears.



2. Type a name for the pie chart in the **Name** field.

3. Drag items from the **Drag Available Fields** list to the following areas:

   - **Data Field**: Specifies the total count for data appearing in the chart
   - **Category Field**: Specifies how the data is separated in the chart

   Example: To provide a graph that displays virus distribution across your network Data Fields would represent the total number of viruses in your network. Category Fields would represent how the total number of viruses would be broken down as a percentage.

4. Specify the Data Properties for the **Data Field**.

   a. Specify how the data displays for the **Data Field** from the Aggregated by list:

      - **Total number of instances**: Specifies that the total count for the number of incidents is used for the results
      - **Number of unique instances**: Specifies that only the count for distinct items is used for the results
      - **Sum of value**: Specifies that the sum of all the values in the "Count" of a Data View column is used for the results

      Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Count number of row would display 10, while Count distinct row displays 1.

5. Specify the Category Properties for the **Category Field**:

   a. Type a meaningful label in the **Label name** field.

   b. Specify how to sort the data in the chart from the Sorting list:

      - **Aggregation value**: Sorts the data according to the data values.
      - **Category name**: Sorts the data according to the alphabetic order of the category names.
      - **Ascending**: Sorts the data in ascending order.
      - **Descending**: Sorts the data in descending order.

   c. Specify how many items display in the **Category Field** by selecting **Filter summarized result** and specifying a value in the **Display top** text box.

The default value is 10.

d. Select **Aggregate remaining items** to put all remaining items into the group "Other" on the graph.

6. Click **Save**.

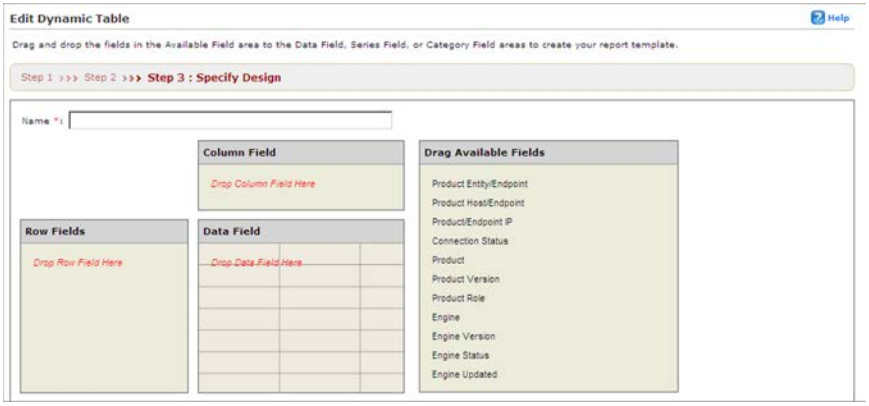
   The **Add Report Template** screen appears.

Configuring Dynamic Table Settings

Procedure

1. Click **Next**.

   The **Step 3: Specify Design** screen appears.



2. Type a name for the table in the **Name** field.
3. Drag items from the **Drag Available Fields** list to the following areas:
   - **Data Field**: Specifies the total count for data appearing in the table
   - **Row Fields**: Specifies how the data is separated horizontally in the table
   - **Column Field**: Specifies how the data is separated vertically in the table

Example: Olivia selects the Data View "Detailed Virus/Malware Information". She does not specify any filtering criteria. She wants a table that displays infected clients, the viruses infecting the clients, and the action taken against the viruses by the managed product. Olivia drags the following fields to the Data, Row, and Column Fields:

- **Data Field**: Detections
- **Row Fields**: Virus/Malware and Action
- **Column Field**: Host

4. Specify the Data Properties for the **Data Field**:

   a. Type a name for the **Data field title**.

   b. Specify how the data displays for the **Data Field** from the Aggregated by list:

      - **Total number of instances**: Specifies that the total count for the number of incidents is used for the results
      - **Number of unique instances**: Specifies that only the count for distinct items is used for the results
      - **Sum of value**: Specifies that the sum of all the values in the "Count" of a Data View column is used for the results

      Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Count number of row would display 10, while Count distinct row displays 1.

5. Specify the Row Properties for the Row Fields.

   a. Type a name for the **Row header title**.

   b. Specify how to sort the data in the table from the Sorting list:

      - **Aggregation value**: Sorts the data according to the data values.
      - **Header title**: Sorts the data according to the alphabetic order of the header names.
      - **Ascending**: Sorts the data in ascending order.
      - **Descending**: Sorts the data in descending order.

c. Specify how many items display in the **Row Fields** by selecting **Filter summarized result** and specifying a value in the **Display top** text box.

The default value is 10.

d. Select **Aggregate remaining items** to put all remaining items into the group "Other" on the graph.

6. Specify the Column Properties for the **Column Field**.

a. Type a name for the **Column header title**.

b. Specify how to sort the data in the table from the Sorting list:

- **Aggregation value**: Sorts the data according to the data values.
- **Header title**: Sorts the data according to the alphabetic order of the header names.
- **Ascending**: Sorts the data in ascending order.
- **Descending**: Sorts the data in descending order.

c. Specify how many columns display by selecting **Filter column** and specifying a value in the **Display top** text box.

The default value is 10.

d. Select **Aggregate remaining items** to put all remaining items into the group "Other" on the graph.

7. Click **Save**.

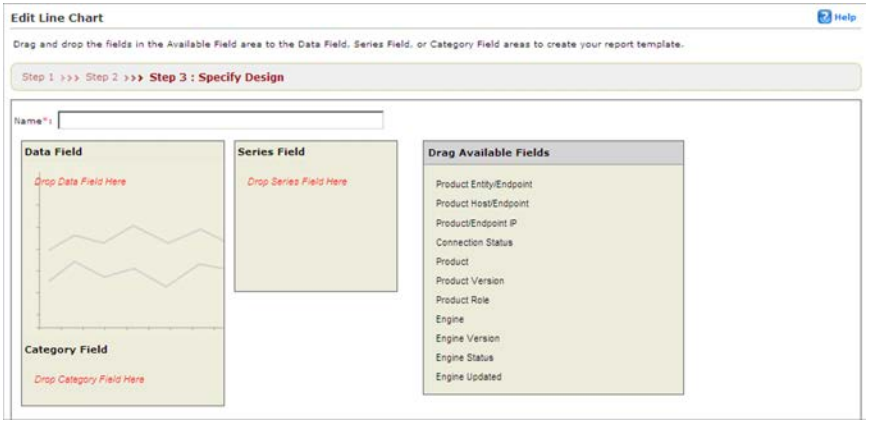
The **Add Report Template** screen appears.

Configuring Line Chart Settings

Procedure

1. Click **Next**.

The **Step 3: Specify Design** screen appears.



2. Type a name for the line chart in the **Name** field.
3. Drag items from the **Drag Available Fields** list to the following areas:
   - **Data Field**: Specifies the total count for data appearing in the table
   - **Series Field**: Specifies how the data is separated in the chart along the vertical axis
   - **Category Field**: Specifies how the data is separated in the chart along the horizontal axis

   Example: Olivia selects the Data View "Detailed Virus/Malware Information". She does not specify any filtering criteria. She wants a chart that displays virus infections over time. Olivia drags the following fields to the Data, Series, and Category Fields:
   - **Data Field**: Detections
   - **Category Field**: Generated
   - **Series Field**: Virus/Malware
4. Specify the Data Properties for the **Data Field**.
   a. Type a meaningful label in the **Value label** field.

b. Specify how the data displays for **Data Field** from the Aggregated by list:

- **Total number of instances**: Specifies that the total count for the number of incidents is used for the results
- **Number of unique instances**: Specifies that only the count for distinct items is used for the results
- **Sum of value**: Specifies that the sum of all the values in the "Count" of a Data View column is used for the results

Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Count number of row would display 10, while Count distinct row displays 1.

5. Specify the Category Properties for the **Category Field**.

a. Type a meaningful label in the **Label name** field.

b. Specify how to sort the data in the chart from the Sorting list:

- **Aggregation value**: Sorts the data according to the data values.
- **Category name**: Sorts the data according to the alphabetic order of the category names.
- **Ascending**: Sorts the data in ascending order.
- **Descending**: Sorts the data in descending order.

c. Specify how many items display in the **Category Field** by selecting **Filter summarized result** and specifying a value in the **Display top** text box.

The default value is 10.

d. Select **Aggregate remaining items** to put all remaining items into the group "Other" on the graph.

6. Specify the Series Properties for the **Series Field**:

a. Type a meaningful label in the **Label name** field.

7. Click **Save**.

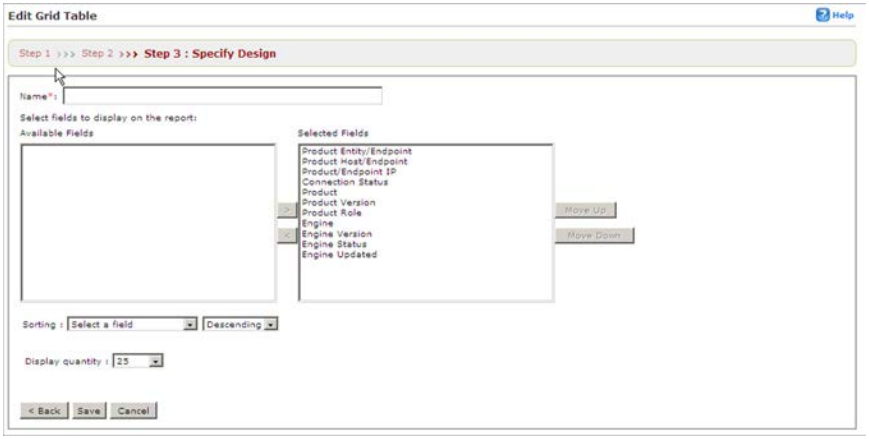
The **Add Report Template** screen appears.

Configuring Grid Table Settings

Procedure

1. Click **Next**.

   The **Step 3: Specify Design** screen appears.



2. Type a name for the table in the **Name** field.
3. Specify which columns appear in the table and in which order the columns appear.
4. Specify how the columns sort.
5. Specify the number of items that appear in the table.
6. Click **Save**.

   The **Add Report Template** screen appears.

Step 6: Complete Report Template Creation

Procedure

1. Add or remove Report Template Elements as you require.
2. Click **Save**.

Understanding One-time Reports

One-time reports generate on demand. Creating one-time reports provides an effective way for administrator's to create management type reports for their network's during outbreaks.

The One-time Report table contains the following:

TABLE 12-11. One-time Reports List

ITEM	DESCRIPTION
Name	Displays the name of the report.
Description	Displays the user-defined description for the report.
Period	Displays the time and date range for the report.
Created time	Displays when the report was created.
Generated time	Displays when the report generated.
Format	Displays the format that the report generates (Example: PDF, HTML, XML, CSV).
Size	Displays the size of reports.
View	Click the associated View link to view the report.

Adding One-time Reports

Control Manager supports generating one-time reports from Static and Custom report templates. Users need to create Custom report templates, while Trend Micro provided

the Static report templates. The process for creating a one-time report is similar for all report types and involves the following:

Procedure

1. *Step 1: Access the Add One-time Report Screen and Select the Report Type on page 12-32*
2. *Step 2: Specify the Product/Products From Which the Report Data Generates on page 12-35*
3. *Step 3: Specify the Date That the Product/Products Produced the Data on page 12-35*
4. *Step 4: Specify the Recipient of the Report: on page 12-37*

Step 1: Access the Add One-time Report Screen and Select the Report Type

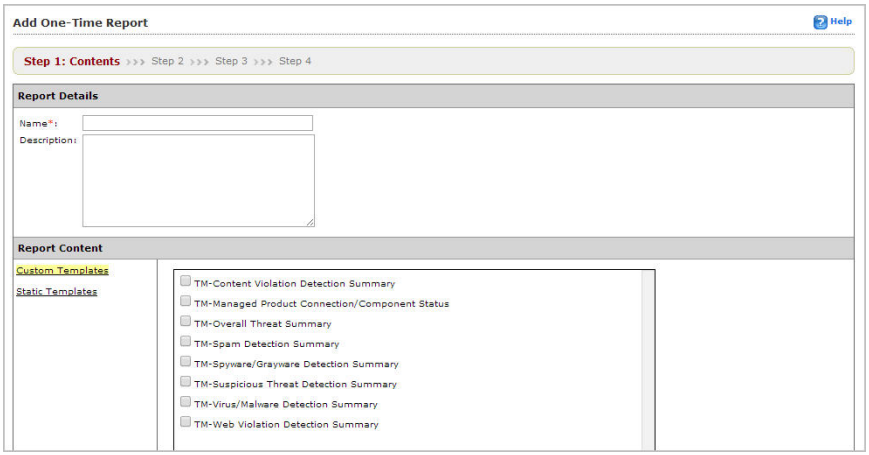
Procedure

1. Navigate to **Reports** > **One-time Reports**.

   The **One-time Reports** screen appears.

2. Click **Add**.

The **Add One-time Report > Step 1: Contents** screen appears.



3. Type a name for the report in the **Name** field, under Report Details.
4. Type a description for the report in the **Description** field, under Report Details.
5. Select the Control Manager template to generate the report:
   - **Custom templates**: Select the Custom report template to generate the report. If the existing reports do not fulfill your requirements, create one from the **Report Templates** screen. See *Adding Custom Templates on page 12-16* for more information.
   - **Static templates**:
     a. Click **Static Templates** under **Report Content**. The Static templates appear in the work area to the right, under **Report Content**.
     b. Select the report category on which to base the report.
     c. Select the static template data on which to base the template.
6. Select the report generation format:
   - **Custom template** report formats:
     - **Adobe PDF Format (*.pdf)**

- HTML Format (*.html)
- XML Format (*.xml)
- CSV Format (*.csv)

- **Static template** report formats:
  - Rich Text Format (*.rtf)
  - Adobe PDF Format (*.pdf)
  - ActiveX
  - Crystal Report Format (*.rpt)

7. Click **Next**.

   The **Add One-Time Report > Step 2: Targets** screen appears.

Step 2: Specify the Product/Products From Which the Report Data Generates

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.
2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment
3. Click **Next**.

   The **Add One-Time Report > Step 3: Time Period** screen appears.

Step 3: Specify the Date That the Product/Products Produced the Data

Procedure

1. Specify the data generation date:

- From the drop down list select one of the following:
  - **All dates**

    Note

    Only custom templates provide the **All dates** generation date.

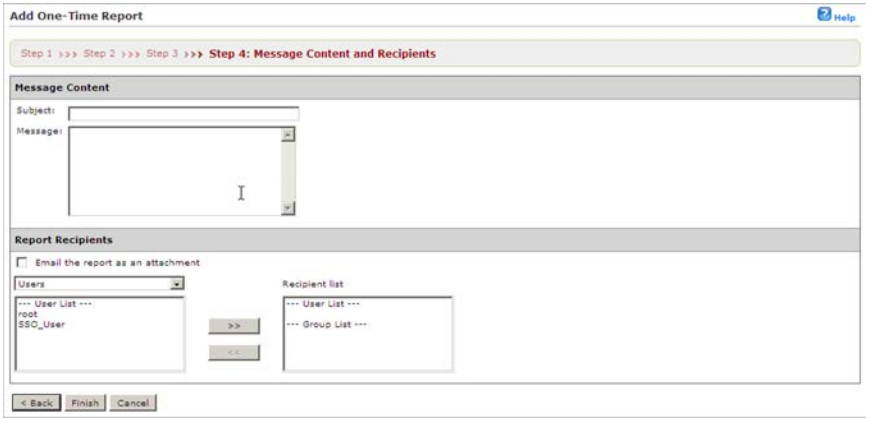
  - **Last 24 hours**
  - **Today**
  - **Last 7 days**
  - **Last 14 days**
  - **Last 30 days**
- Specify a date range:
  - Type a date in the **From** field.
  - Specify a time in the accompanying **hh** and **mm** fields.
  - Type a date in the **To** field.
  - Specify a time in the accompanying **hh** and **mm** fields.

  Note

  Click the calendar icon next to the **From** and **To** fields to use a dynamic calendar to specify the date range.

2. Click **Next**.

The **Add Onetime Report > Step 4: Message Content and Recipients screen** appears.



Step 4: Specify the Recipient of the Report:

Procedure

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.
5. Select the users/groups to receive the report and click the **>>** button.
6. Click **Finish** after selecting all users/groups to receive the report.

Understanding Scheduled Reports

Scheduled reports generate based on a user-specified schedule. Creating scheduled reports provide an effective way for administrator's to create management type reports for their network's during normal operation.

The Scheduled Reports table contains the following:

TABLE 12-12. Scheduled Reports List

ITEM	DESCRIPTION
Name	Displays the name of the report
Description	Displays the user-defined description for the report
Frequency	Displays how often the report generates
Created time	Displays when the report was created
Last generated time	Displays when the latest report generated
Next schedule	Displays when to generate the next report
History	Click the associated View link to view the report
Enable	Displays the status of the report (enabled or disabled)

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Custom and Static templates. Users need to create Custom Templates; Trend Micro , while Trend Micro provides Static templates. The process for creating a scheduled report is similar for all report types:

Procedure

1. *Step 1: Access the Add Scheduled Report Screen and Select the Report Type on page 12-39*
2. *Step 2: Specify the Product/Products from Which the Report Data Generates on page 12-41*

3. *Step 3: Specify the Date that the Product/Products Produced the Data on page 12-42*

4. *Step 4: Specify the Recipient of the Report on page 12-44*

Step 1: Access the Add Scheduled Report Screen and Select the Report Type

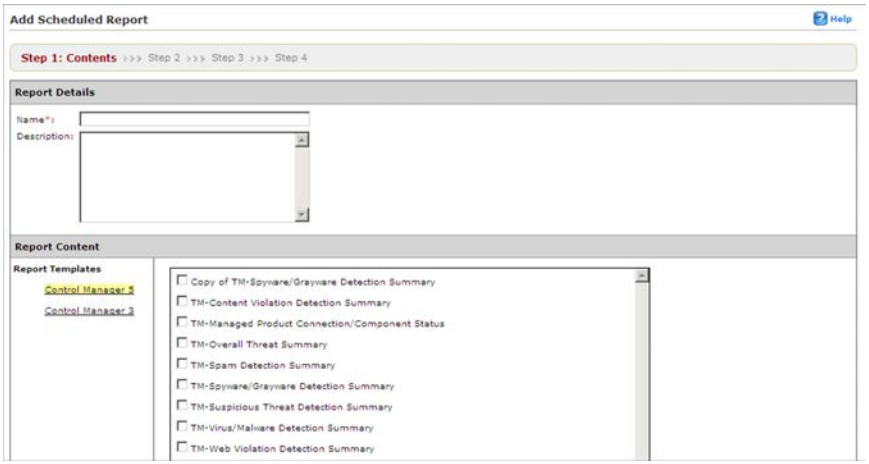
Procedure

1. Navigate to **Reports** > **Scheduled Reports**.

   The **Scheduled Reports** screen appears.

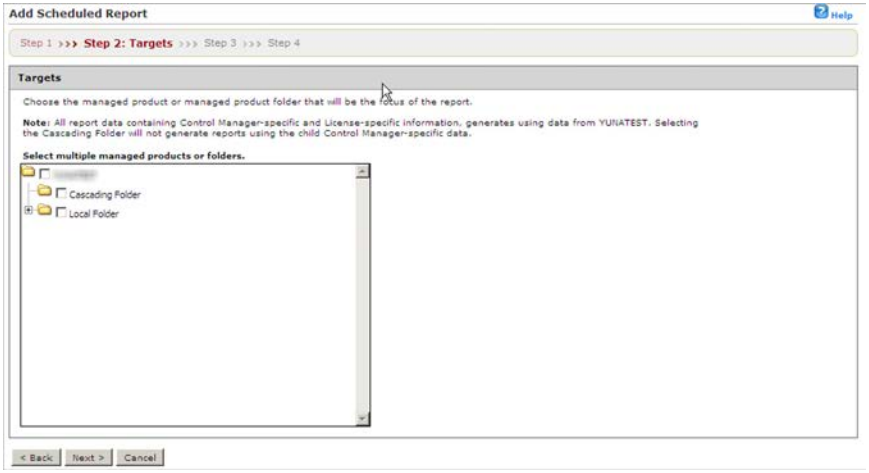
2. Click **Add**.

   The **Add Scheduled Report > Step 1: Contents** screen appears.



3. Type a name for the report in the **Name** field.
4. Type a meaningful description for the report in the **Description** field.
5. Select the Control Manager template to generate the report:
   - Custom report template:
     a. Select the Custom Template to generate the report. If the existing reports do not fulfill your requirements, create one from the **Report Templates** screen. See *Adding Custom Templates on page 12-16* for more information.
   - Static report template:
     a. Click **Static Template** under **Report Content**. The Static templates appear in the work area to the right, under **Report Content**.
     b. Select the report category on which to base the report.
     c. Select the Static template data on which to base the template.
6. Select the report generation format:
   - Custom template report formats:
     - Adobe PDF Format (*.pdf)
     - HTML Format (*.html)
     - XML Format (*.xml)
     - CSV Format (*.csv)
   - Static template report formats:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)
7. Click **Next**.

The **Add Scheduled Report > Step 2: Targets** screen appears.



Step 2: Specify the Product/Products from Which the Report Data Generates

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.
2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment
3. Click **Next**.

The **Add One-Time Report > Step 3: Frequency** screen appears.

Step 3: Specify the Date that the Product/Products Produced the Data

Procedure

1. Specify how often reports generate:
   - **Every 'n' days**: Reports generate on a per day or every 'n' days, depending on your selection (1~6).
   - **Weekly**: Reports generate weekly on the specified day.
   - **Bi-weekly**: Reports generate every two weeks on the specified day.
   - **Monthly**: Reports generate monthly on the first, 5th, 10th, 15th, 20th, 25th, or the last day of the month.
2. Specify the data range:
   - **Reports include data up to the Start the schedule time specified below**: This means that a report could have up to 23 hours more data contained in the report. While this has a small affect on weekly or monthly reports, this can

make a "daily" report with almost two days worth of data depending on the Start schedule time.

- **Reports include data up to 23:59:59 of the previous day**: This means that data collection for the report stops just before midnight. Reports will be an exact time period (example: Daily reports will be 24 hours) but will not contain the absolute latest data.

3. Specify when the report schedule starts:

   - **Immediately**: The report schedule starts immediately after enabling the report.
   - **Start on**: The report schedule starts on the date and time specified in the accompanying fields.

   a. Type a date in the **mm/dd/yyyy** field.

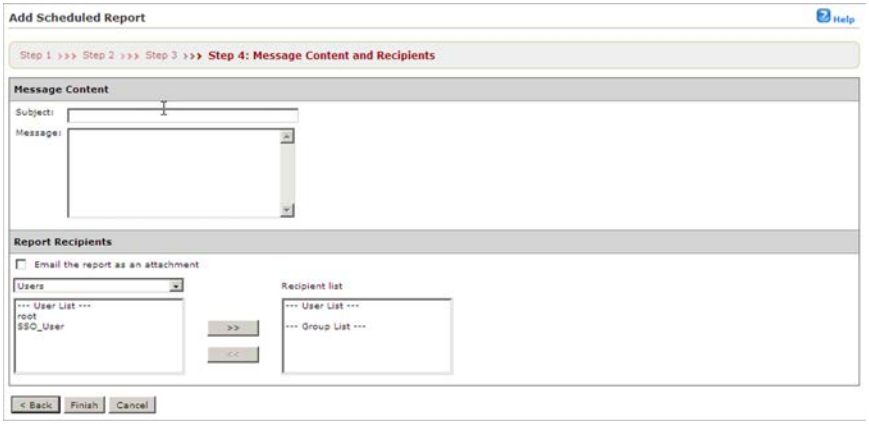
   b. Specify a time in the accompanying **hh** and **mm** fields.

Note

Click the calendar icon next to the **mm/dd/yyyy** field to use a dynamic calendar to specify the date range.

4. Click **Next**.

The **Add Scheduled Report > Step 4: Message Content and Recipients** screen appears.



Step 4: Specify the Recipient of the Report

Procedure

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.
5. Select the users/groups to receive the report and click the **>>** button.
6. Click **Finish** after selecting all users/groups to receive the report.

Enabling/Disabling Scheduled Reports

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it through the **Scheduled Reports** screen.

Procedure

1. Navigate to **Reports** > **Scheduled Reports**.

   The **Scheduled Reports** screen appears.

2. Click the enabled ()/disabled () icon in the **Enable** column of the Scheduled Reports table.

   A disabled/enabled icon appears in the column.

Viewing Generated Reports

Aside from sending reports as email message attachments, view generated reports from one of these areas:

- One-time Reports
- Scheduled Reports

Viewing One-Time Reports

Procedure

1. Navigate to **Reports** > **One-time Reports**.

   The **One-time Reports** screen appears.

2. Click the link for the report you want to view from the **View** column.

Viewing Scheduled Reports

Procedure

1. Navigate to **Reports** > **Scheduled Reports**.

   The **Scheduled Reports** screen appears.

2. Click the link for the report you want to view from the **History** column.

   The **Scheduled Report History** screen for that report appears.

3. Select the report to view from the **Scheduled Report History** screen.

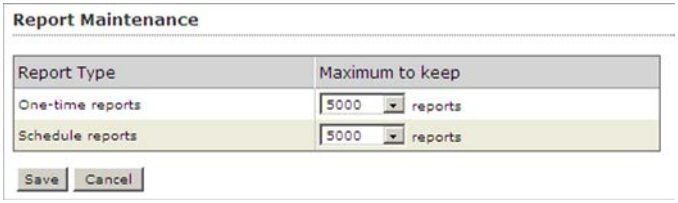
Configuring Report Maintenance

Configure **Report Maintenance** settings to delete reports.

Procedure

1. Navigate to **Reports** > **Report Maintenance**.

   The **Report Maintenance** screen appears.



2. Specify the maximum number of one-time and scheduled reports to keep.

3. Click **Save**.

Understanding My Reports

The **My Reports** screen contains all the reports a particular user (and the groups the user belongs to) creates. For each user that logs on to Control Manager the screen displays only the reports that the particular user (or group that the user belongs to) generated.

The **My Reports** screen displays the following:

TABLE 12-13. My Reports List

ITEM	DESCRIPTION
Name	The name of the generated report.
Period	The time and date when the report was generated.
Submitted Time	The time when the report was initiated.
Generated Time	The time when the report completed generation.
Format	The format used to generate the report (for example, PDF or xml).
Size	The size of the generated report.
View	Click the associated link in the row to view the report.

Part III

Administering Control Manager

Chapter 13

MCP and Control Manager Agents

This chapter presents material administrators can use to understand the agents Control Manager uses to manage the network.

This chapter contains the following topics:

Understanding Agents

Control Manager uses MCP and Control Manager 2.x agents to manage products on the Control Manager network:

- Control Manager Agent (version 2.51 or higher) - Older versions of Trend Micro products require this agent, built according to the Control Manager 2.5/3.0 architecture.
- Trend Micro Management Communication Protocol (MCP) Agent - The next generation agent from Trend Micro, that supports enhanced security, SSO, one-way and two-way communication, and cluster nodes.

The following table enumerates the features supported by Control Manager 2.x and MCP agents.

TABLE 13-1. Agent Comparison

FEATURE	MCP AGENTS	CONTROL MANAGER 2.X AGENTS
Outbreak Prevention Services (OPS)	●	●
Single Sign-on (SSO)	●	
One-way/two-way communication	●	
NAT support	●	
Cluster node support	●	
Agent polls Control Manager for updates and commands	●	
Re-registration with the Control Manager server if the agent database is corrupted or deleted	N/A (This issue does not occur with MCP agents)	Automatic after 8 hours
Communication security	HTTPS/HTTP	Encryption with optional authentication
Communicators		●

Feature	MCP Agents	Control Manager 2.x Agents
Work and idle state support	●	●
Agent/Communicator heartbeat	●	●
Notification: Virus pattern expired	●	●
Notification: Agent unable to update components	●	●
Notification: Agent unable to deploy components	●	●
Notification: Product service stopped	●	●

Each managed product has its own agent responsible for the following:

Table 13-2. MCP / 2.x Agent Comparison

MCP Agents	2.x Agents
Polling commands for the managed product from the Control Manager server	Receiving commands from the Control Manager server, through the Communicator
Collecting managed product status and logs, and sending them to the Control Manager server, through HTTPS or HTTP	Collecting managed product status and logs, and sending them to the Control Manager server, through the Communicator

Understanding Communicators

The Communicator, or the Message Routing Framework, serves as the communications backbone for the older managed products and Control Manager. This component of the Trend Micro Management Infrastructure (TMI) handles all communication between the Control Manager server and managed products for older products. Communicators interact with Control Manager to communicate with older managed products.

By installing the Control Manager 2.5 agent on a managed product server, you can use this application to manage the product with Control Manager. Agents interact with the

managed product and Communicator. An agent serves as the bridge between managed product and communicator. Hence, you must install agents on the same computer as managed products.

The Control Manager installation checks if the Communicator is already available on the managed product server. If so, it does not install another instance of the Communicator. Multiple agents in a product server share a single Communicator. The Communicator takes care of:

- Securing messages by encryption and anti-replay functions provided by the OpenSSL open source library, and Trend Micro-developed end-to-end authentication
- Receiving and relaying commands from the Control Manager server to the managed product
- Receiving and relaying status information from managed products to the Control Manager server

The above descriptions highlight the following points:

- TMI can exist by itself; managed products, on the other hand, cannot operate in the absence of communicator
- Though there can be as many agents on a server as there are managed products, only one Communicator is required for each server
- Multiple managed products can share communicator functions

Understanding Connection Status Icons

The Control Manager managed products, managed servers, Communicators, and child server use the following connection status icons:

TABLE 13-3. Status Icons for Managed Products/Servers

CONNECTION STATUS DESCRIPTION	MANAGED PRODUCT
Product service is running	

Connection Status Description	Managed Product	
Product service is not running		
TMI service is not running		Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting
The socket or network connection between the Communicator and managed product is broken		
Unable to resolve the DNS name between the Communicator and Control Manager server		Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting

Table 13-4. Status Icons for Communicators

Connection Status Description	Communicators	
TMI service is running		
TMI service is not running		Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting
Idle mode following the Agent/ Communicator Scheduler		
The socket or network connection between the Communicator and managed product is broken		
Unable to resolve the DNS name between the Communicator and Control Manager server		

TABLE 13-5. Status Icons for Child Servers

CONNECTION STATUS DESCRIPTION	CHILD	
TMI service is not running	Status is unchanged	Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting
The child server service (Casprocessor.exe) is running		
`Casprocessor.exe` or the child server's Communicator is not running. Either the child server is shutdown or the Communicator service is disabled		
The child server is disabled from the parent server web console		

Understanding Control Manager Security Levels

Control Manager has three security levels used for the communication between the server and managed products and child servers for both older agents and MCP agents. For MCP agents, Security Level applies to the virtual folders of IIS, comprising of three different levels: high, medium, and normal.

- High: Specifies Control Manager communicates only using HTTPS
- Medium: Specifies Control Manager uses HTTPS to communicate when available, but uses HTTP when HTTPS is not available
- Normal: Specifies Control Manager uses HTTP to communicate

The security behavior corresponds to each security level listed below:

Features	Security Level		
	High	Medium	Normal
Supports only HTTPS UI access	●	●	
Supports HTTPS and HTTP UI access			●
Supports redirect to HTTPS or HTTP product UI	●	●	●
Only integrates with HTTPS supported products (MCP)	●		
Integrates with both HTTP and HTTPS supported products		●	●
Allow products to download updates from Control Manager through either HTTP or HTTPS	●	●	●

Depending on the security level of older agents, Control Manager provides the following encryption and authentication:

- SSL packet-level encryption: Control Manager applies Secure Socket Layer (SSL) packet-level encryption to all security levels. SSL packet-level encryption is a protocol developed by Netscape for secure transactions across the web. SSL uses a form of public key encryption, where the information can be encoded by the browser using a publicly available public key, but can only be decoded by a party who knows the corresponding private key.

  The Control Manager agents can encrypt their communication using the public key. In return, the Control Manager server uses a private key to decrypt the agent message.

- Trend Micro authentication: Control Manager applies Trend Micro authentication 5 (High) security level.

  When using High level, Control Manager first applies the SSL packet-level encryption and then further strengthens the encryption through Trend Micro authentication.

Note

You can modify the Control Manager security level through `TMI.cfg`. However, doing so requires the modification of all `TMI.cfg` present in the Control Manager network. This includes the `TMI.cfg` of the Control Manager server and all managed products and child servers. Otherwise, the server and agent communication will not work.

TABLE 13-6. Security Level Behavior for Older Agents

SECURITY LEVEL (FOUND IN TMI.CFG)	SECURITY LEVEL SELECTION (DURING INSTALLATION)	END-TO-END AUTHENTICATION	MESSAGE-LEVEL ENCRYPTION
1	Low	N/A	40-bit (RC4)
2	Medium	N/A	128-bit (RC4)
5	High	Trend Micro authentication	128-bit (RC4 + 3DES)

Using the Agent Communication Schedule

The Agent Communication Schedule determines the periods when the agent sends information to the Control Manager server, allowing you to manage the flow of information.

The Control Manager agent installation assigns a default communication schedule. You can modify the schedule to suit your Control Manager network needs. The Agent Communication Scheduler follows a daily setting, that is, it applies the schedule to an agent on a daily basis. There is no weekly or monthly work hour configuration available.

When you set a schedule, that schedule applies to all managed products registered to Control Manager.

Note

When an agent is idle during an Outbreak Prevention Mode, corresponding managed products still perform Outbreak Prevention Service commands without reporting the result to Control Manager. As a result, Control Manager does not know the status or result. Command Tracking lists the result of Outbreak Prevention Policy-related commands under the Fail category.

The Agent Communication idle and working schedules apply only to the managed product agents. You cannot set the idle schedule for Control Manager 3.5 child servers.

Note

The Agent Communication Schedule lists the child server agents.

Understanding the Agent/Communicator Heartbeat

"Heartbeat" refers to the MCP or Control Manager 2.x agent message that notifies the Control Manager server with "I am alive" information. The agent provides this mechanism to determine whether the managed products remain active.

Note

Use the **Agent Communication Schedule** screen to define the heartbeat working and idle hours.

The agent polls the Control Manager server at regular intervals to ensure that the Control Manager console displays the latest information and to verify the connection between the managed product and the server remains functional.

There are three heartbeat statuses:

- **Active**: the Control Manager agent on the managed product is active and the product service status is running or unknown

- **Inactive**: the managed product is disconnected or disabled, roaming mode is enabled, or the Control Manager agent is active and the product service status is not running
- **Abnormal**: network connection error

Refer to *Understanding Connection Status Icons on page 13-4* for details.

Note

In addition to providing periodic heartbeat to the Control Manager server, the agent also sends real-time managed product status information to the server.

MCP Heartbeat

To monitor the status of managed products, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the managed product and to check for commands to the managed product from Control Manager. The Control Manager web console then presents the product status. This means that the managed product's status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each managed product in a sequential manner in the background. Control Manager changes the status of managed products to offline when a fixed period of time elapses without a heartbeat from the managed product.

Active heartbeats are not the only means Control Manager determines the status of managed products. The following also provide Control Manager with the managed product's status:

- Control Manager receives logs from the managed product. Once Control Manager receives any type of log from the managed product successfully, this implies that the managed product is working fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the managed product to retrieve the pending command. If server connects to the managed product successfully, it also indicates that the product is working fine and this event counts as a heartbeat.
- In one-way communication mode, the MCP agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The MCP heartbeats implement in the following ways:

- **UDP**: If the product can reach the server using UDP, this is the lightest weight, fastest solution available. However, this does not work in NAT or firewall environments. In addition, the transmitting client cannot verify that the server does indeed receive the request.
- **HTTP/HTTPS**: To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the managed product applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains managed product activity information to display on the console.

Using the Schedule Bar

Use the schedule bar on the **Agent Communication Schedule** screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

The slots with clock icons denote working status or the hours that the Agent/ Communicator sends information to the Control Manager server. White slots indicate idle time. Define working or idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

FIGURE 13-1. Schedule bar

The active periods specified by the bar are from 0:00 to 7:00, 8:00 to 4:00 PM, and from 6:00 P.M. to midnight.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest managed product status information and the need to manage system resources. The default setting is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

TABLE 13-7. Heartbeat Recommendations

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status in the Control Manager web console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

Configuring Agent Communication Schedules

You can define up to three sets of schedules that specify when the managed product interacts with the Control Manager server.

A child Control Manager server should always have constant communication with the parent Control Manager server; the **Agent Communication Schedule** screen does not allow changes in a child server's agent communication schedule with the child server's managed products.

Setting an Agent Communication Schedule for a Managed Product

Procedure

1. Navigate to **Administration** > **Settings** > **Agent Communication Schedule**.

   The **Agent Communication Schedule** screen appears.

2. Select the managed product schedule to modify.

   The **Set Communicator Schedule** screen appears.

3. Define the schedule. Specify a new time or use the default setting:

   - To specify a new setting, change the appropriate time slots in the schedule bar and then click **Save**
   - To use the default setting, return to the **Agent Communication Schedule** screen. Select the schedule to apply and click **Reset to Default Schedule**

Modifying the Default Agent Communication Schedule

Use the default schedule to automatically set the agent communication schedule.

Procedure

1. Navigate to **Administration** > **Settings** > **Agent Communication Schedule**.

   The **Agent Communication Schedule** screen appears.

2. On the working area, click **Default Schedule**.

3. On the **Daily Schedule**, change the appropriate time slots.

4. Click **Save**.

Configuring the Agent Communicator or Managed Server Heartbeat

Use the **Communication Time-out** screen to define the frequency and maximum delay times (in minutes) for the Control Manager server and *product agent on page 13-2*/ *managed server on page 6-2* communication.

Note

The agent/communicator heartbeat setting only applies to Communicators for managed products directly controlled by the Control Manager server. Child Control Manager server agent/communicators use pre-defined values:

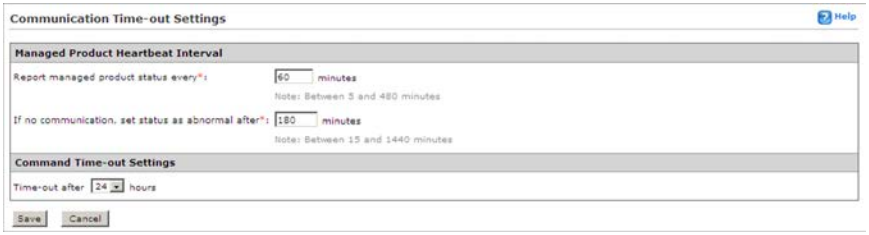
Frequency: 3 minutes

Maximum delay: 5 minutes

Procedure

1. Navigate to **Administration** > **Settings** > **Communication Time-out Settings**.

   The **Communication Time-out** screen appears.



2. On the working area, leave the default values or specify new settings for the following:

   - **Report managed product status every**: Defines how often the managed product or server responds to Control Manager server messages. Valid values are between 5 to 480 minutes

- **If no communication, set status as abnormal after**: Specifies how long Control Manager waits for a response from the managed product or server before changing its web console status to (inactive). Valid values are between 15 and 1440 minutes.

Note

The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

3. Click **Save**.

Stopping and Restarting Control Manager Services

Use the **Windows Services** screen to restart any of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager

Note

These are the services that run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services).

Procedure

1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.
2. Right-click **<Control Manager service>**, and then click **Stop**.

3. Right-click **<Control Manager service>**, and then click **Start**.

Modifying the Control Manager External Communication Port

The Communicator is responsible for agent and server communication.

By default, the Communicator uses port 10198 for communication between Control Manager processes (internal communication) and port 10319 for communication between the Control Manager agent and server (external communication).

Changing the External Communication Port on the Control Manager Server

Procedure

1. Open `<root>\Program Files\Trend Micro\COMMON\ccgi\commoncgi\config\CCGI_Config.xml` using a text editor (for example, Notepad).

   WARNING!

   Use care when modifying Control Manager `*.xml` or `*.cfg` files. To ensure that you can roll back to the original settings, back up `CCGI_Config.xml`.

2. Specify a new value for the `OuterPort` parameter.

   This value represents the external communication port. For example, set `OuterPort="2222"` to use port 2222.

3. Save and close `CCGI_Config.xml`.

4. Open `<root>\Program Files\Trend Micro\COMMON\TMI\TMI.cfg` using a text editor.

WARNING!

Making incorrect changes to the configuration file can cause serious system problem. Back up `TMI.cfg` to restore your original settings.

5. Replace the `OuterPort` parameter value to match the value of `CCGI_Config.xml`.
6. Save and close `TMI.cfg`.
7. Stop and restart all Control Manager services.

Modifying the Security Level for TMI Agents

Control Manager implements the security level you specified during the Control Manager installation. `TMI.cfg` allows you to change the security level without reinstalling the product.

Procedure

1. Open `<root>:\Program files\Trend Micro\COMMON\TMI\TMI.cfg` using any text editor (for example, Notepad).

WARNING!

Making incorrect changes to the configuration file can cause serious system problem.

2. Back up `TMI.cfg` to restore your original settings.
3. Change the value of `MaxSecurity` parameter. Use `1`, `2`, or `5`, which corresponds to the security level you want.
4. Save and close `TMI.cfg`.
5. Open the **Windows Services** screen to stop and then restart the Control Manager services.
6. Repeat steps 1 to 3 to modify `TMI.cfg` for all agents present in your Control Manager network.

WARNING!

Set all `TMI.cfg` in your Control Manager network (server and agents) to the same security level value (MaxSecurity). Otherwise, the server and agent communication will not work.

Modifying the Communicator Heartbeat Protocol

By default, the connectionless User Datagram Protocol (UDP) is used to send Communicator Heartbeat from managed product to the Control Manager server.

Procedure

1. Open `<root>:\program files\Trend Micro\COMMON\TMI\TMI.cfg` using any text editor (for example, Notepad).

WARNING!

Making incorrect changes to the configuration file can cause serious system problem. Back up `TMI.cfg` to restore your original settings.

2. Change the value of `AllowUDP` parameter to `0`.
3. Save and close `TMI.cfg`.
4. Open the **Windows Services** screen to stop and then restart the Control Manager services.
5. Repeat steps 1 to 3 to modify `TMI.cfg` for all agents present in your Control Manager network.

WARNING!

Set all `TMI.cfg` in your Control Manager network (server and agents) to the same security level value (AllowUDP). Otherwise, the server and agent communication will not work.

Verifying the Communication Method Between MCP and Control Manager

Control Manager auto-detects the connection method MCP agents use when communicating with Control Manager. For two-way communication, Control Manager uses CGI notifications to communicate with MCP agents.

Verifying Control Manager Uses Two-way Communication

This procedure uses the default installation settings for Control Manager.

Procedure

1. Open the SQL server management application and locate the Control Manager database table.
2. Locate **CDSM_Entity**.
3. Locate and verify the following from CDSM_Entity:

   Locate the **Token** column. Information in the column appears in the following format: `URLTOKEN:2; http;<IP address>;80; cgiCmdNotify;;!CRYPT!10…`

   - `URLTOKEN:1` signifies that the agent uses one-way communication to communicate with Control Manager.
   - `URLTOKEN:2` signifies that the agent uses two-way communication to communicate with Control Manager.

Verifying Control Manager Uses Two-way Communication from the Web Console

Procedure

1. Click **Products**.

The **Product Directory** screen appears.

2. Click the product or directory in the Product Directory.
3. Click **Folder**.

   The information in the work area changes.

4. Select **Connection Information View** from the **Folder** drop-down list.

   The **Mode** column displays which communication mode, the MCP agent on the managed product uses.

Understanding Control Manager Agent Remote Installation

Control Manager can supports Control Manager 2.5x and MCP agents. However, only Control Manager 2.5x agents require a separate installation. Use the **Product Agent Settings** screen to obtain the remote installation programs for Control Manager 2.x agents.

Note

Remote installation is the preferred installation method for deploying Control Manager 2.x agents on large numbers of older managed product servers. This capability allows you to install Control Manager 2.x agents without being physically at the target server.

There are two agent remote installation programs for installing Control Manager 2.x agents:

AGENT	DESCRIPTION
`CMAgentSetup.exe`	The basis of this agent installation program is a program similar to the one used in Trend Virus Control System 1.x. All agents required for the corresponding products are contained in this file. Use `CMAgentSetup.exe` to install the Control Manager agent for InterScan Messaging Security Suite 5.1 (InterScan Messaging Security Suite 5.15 and above uses RemoteInstall.exe).
`RemoteInstall.exe`	This is an agent installation tool introduced in Control Manager 2.5. It serves two purposes: • To install agents to supported product servers • To upload agent packages to Control Manager servers This tool differs from the original `CMAgentSetup.exe` program because it does not actually contain any agents. Instead, it uses agent packages stored on Control Manager servers. The tool merely identifies the target servers, and then the setup programs in the agent packages themselves perform the installation. After a fresh Control Manager installation, Control Manager servers do not contain agent packages. The antivirus or content security product uploads and stores their agents to the server, before you can install these agents.

Chapter 14

Administering Managed Products

This chapter presents material administrators need when managing the Control Manager network.

This chapter contains the following topics:

Manually Deploying Components Using the Product Directory

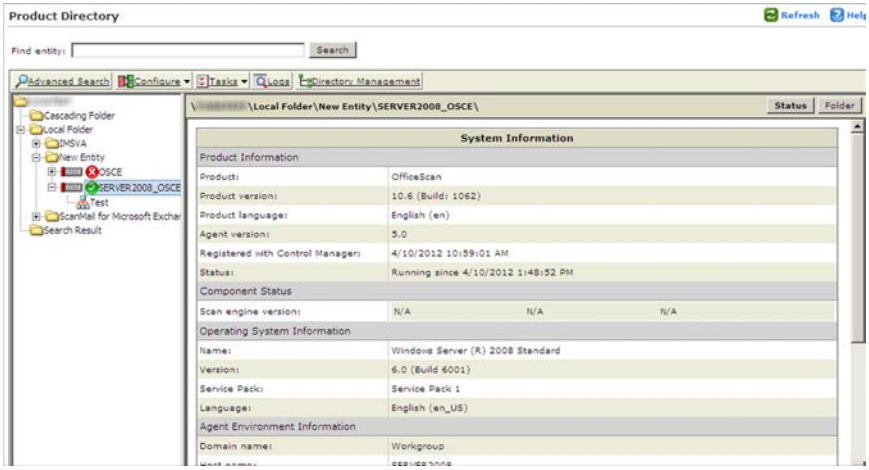
Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your managed products on demand. Use this method of updating components during virus outbreaks.

Download new components before deploying updates to a specific managed product or groups of managed products.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.



2. Select a managed product or directory from the Product Directory.

   The managed product or directory highlights.

3. Move the cursor over **Tasks** from the Product Directory menu.

4. Select **Deploy <component>** from the drop-down menu.

5. Click **Deploy Now** to start the manual deployment of new components.
6. Monitor the progress through the **Command Tracking** screen.
7. Click the **Command Details** link on the **Command Tracking** screen to view details for the Deploy Now task.

Viewing Status Summaries for Managed Products

The **Product Status** screen displays the Antivirus, Content Security, and Web Security summaries for all managed products present in the Product Directory tree.

There are two ways to view the managed products status summary:

- Through the dashboard using the **Threat Detection Results** widget (found on the **Threat Detection** tab)
- Through the Product Directory

Accessing Through the Dashboard

Upon opening the Control Manager web console, the **Summary** tab on the **Dashboard** displays the summary of the entire Control Manager network. This summary is identical to the summary provided by the **Product Status** tab in the Product Directory Root folder.

Accessing Through the Product Directory

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.
2. From the Product Directory tree, select the desired folder or managed product.

- If you click a managed product, the **Product Status** tab displays the managed product's summary.
- If you click the Root folder, New entity, or other user-defined folder, the **Product Status** tab displays Antivirus, Content Security, and Web Security summaries.

Note

By default, the **Status Summary** displays a week's worth of information ending with the day of your query. You can change the scope to **Today**, **Last Week**, **Last Two Weeks**, or **Last Month** in the **Display** summary for list.

Configuring Managed Products

Depending on the product and agent version you can configure the managed product from the managed product's web console or through a Control Manager-generated console.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select the desired managed product from the **Product Directory** tree.

   The product status appears in the right-hand area of the screen.

3. Move the cursor over **Configure** in the **Product Directory** menu.

4. Select one of the following:

   - **Configuration Replication**: The **Configuration Settings** screen appears.

Note

All selected managed products must run the exact product version and build. For example, to replicate OfficeScan settings, servers **osce-tokyo1** and **osce-munich2** must have OfficeScan 11.0 running.

a. Select the folder to which the selected managed product's settings replicate from the **Product Directory** tree.

b. Click **Replicate**.

The selected managed product's settings replicate to the target managed products.

- **<Managed Product Name> Single Sign On**: The managed product's web console or Control Manager-generated console appears.

a. Configure the managed product from the web console.

Note

For additional information about configuring managed products, refer to the managed product's documentation.

Issuing Tasks to Managed Products

Use the **Tasks** menu item to invoke available actions to a specific managed product. Depending on the managed product, all or some of the following tasks are available:

- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Enable or disable Real-time Scan
- Start Scan Now

Deploy the latest spam rule, pattern, or scan engine to managed products with outdated components. To successfully do so, the Control Manager server must have the latest

components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select the managed product or directory to issue a task.

3. Move the cursor over **Tasks**.

4. Click a task from the list. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Querying and Viewing Managed Product Logs

Use the **Logs** tab to query and view logs for a group or a specific managed product.

Procedure

1. Click **Directories** > **Products** from the main menu.

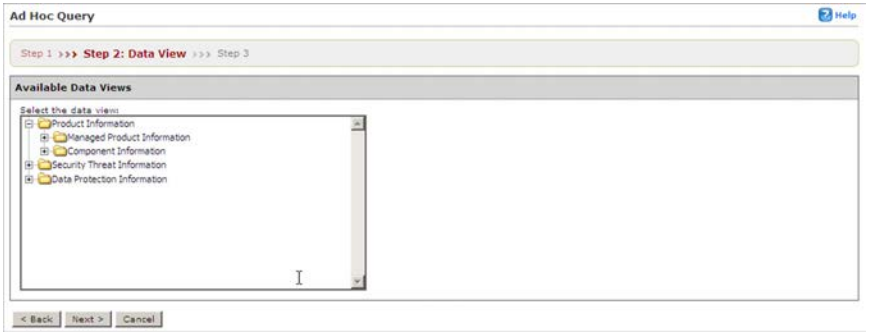
   The **Product Directory** screen appears.

2. Select the desired managed product or folder from the **Product Directory**.

3. Move the cursor over **Logs** in the **Product Directory** menu.

4. Click **Logs** from the drop-down menu.

The **Ad Hoc Query > Step 2: Select Data View** screen appears.

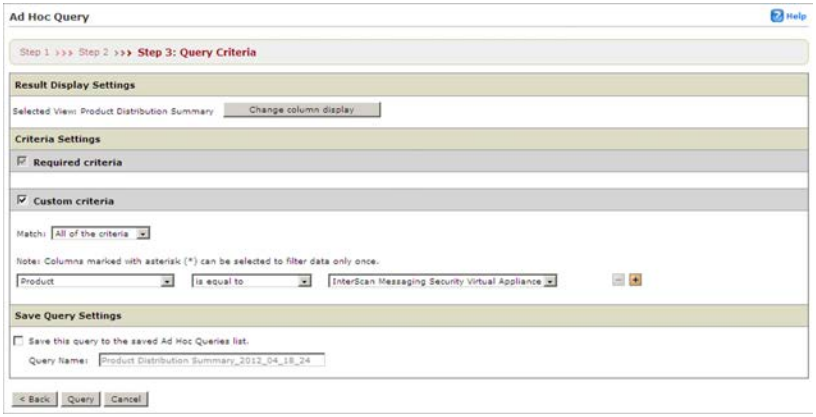


5. Specify the data view for the log:

   a. Select the data to query from the **Available Data Views** area.

   b. Click **Next**.

      The **Ad Hoc Query > Step 3: Query Criteria** screen appears.



6. Specify the data to appear in the log and the order in which the data appears. Items appearing at the top of the Selected Fields list appear as the left most column of the table. Removing a field from Selected Fields list removes the corresponding column from the Ad Hoc Query returned table.

a. Click **Change column display**.

The **Select Display Sequence** screen appears.

b. Select a query column from the Available Fields list.

Select multiple items using the SHIFT or CTRL keys.

c. Click **>** to add items to the Selected Fields list.

d. Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

e. Click **Back** when the sequence fits your requirements.

7. Specify the filtering criteria for the data:

Note

When querying for summary data, users must specify the items under **Required criteria**.

- **Required criteria**:
  - Specify a **Summary Time** for the data or whether you want COOKIES to appear in your reports.
- **Custom criteria**:
  a. Specify the criteria filtering rules for the data categories:

- **All of the criteria**: This selection acts as a logical "AND" function. Data appearing in the report must meet all the filtering criteria.
- **Any of the criteria**: This selection acts as a logical "OR" function. Data appearing in the report must meet any of the filtering criteria.

b. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

Tip

If you do not specify any filtering criteria, the Ad Hoc Query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

8. Save the query:
   a. Click **Save this query to the saved Ad Hoc Queries list**.
   b. Type a name for the saved query in the **Query Name** field.
9. Click **Query**.

   The **Results** screen appears.
10. Save the report as a CSV file:
    a. Click **Export to CSV**.
    b. Click **Download**.
    c. Specify the location to save the file.
    d. Click **Save**.
11. Save the report as an XML file:
    a. Click **Export to XML**.
    b. Click **Download**.
    c. Specify the location to save the file.
    d. Click **Save**.

Tip

To query more results on a single screen, select a different value in **Rows per page**.

12. Save the settings for the query:

    a. Click **Save query settings**.

    b. Type a name for the saved query in the **Query Name** field.

    c. Click **OK**.

    The saved query appears on the **Saved Ad Hoc Queries** screen.

About Recovering Managed Products Removed From the Product Directory

The following scenarios can cause Control Manager to delete managed products from the Product Directory:

- Reinstalling the Control Manager server and selecting **Delete existing records and create a new database**

  This option creates a new database using the name of the existing one.

- Replacing the corrupted Control Manager database with another database of the same name

- Accidentally deleting the managed product from **Directory Management**

If the records for a Control Manager server's managed products are lost, TMI agents on the products still "know" where they are registered. The Control Manager agent automatically re-registers itself after 8 hours or when the service restarts.

MCP agents do not re-register automatically. Administrators must manually re-register managed products using MCP agents.

Recovering Managed Products Removed From the Product Directory

Procedure

- Restart the Trend Micro Control Manager service on the managed product server.

  For more information, see *Stopping and Restarting Control Manager Services on page 13-16*.

- Wait for the Agent to re-register itself: By default, the older Control Manager agents verify their connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.

  Refer to *Changing Control Manager 2.x Agent Connection Re-Verification Frequency on page 14-11* to modify the agent verification time.

- Manually re-register to Control Manager: MCP agents do not re-register automatically and need to be manually re-registered to the Control Manager server.

Changing Control Manager 2.x Agent Connection Re-Verification Frequency

By default, Control Manager 2.x agents verify their connection with the Control Manager server every eight hours. Edit a configuration file on the agent computer to modify the frequency.

Note

MCP agents cannot reconnect to Control Manager if the connection is lost. A user must manually re-register the managed products.

Procedure

1. From the managed product's server, navigate to the Control Manager agent home directory (for example, `C:\Program Files\Trend\IMSS\Agent`).
2. Back up `Entity.cfg`.

3. Open `Entity.cfg` using a text editor (for example, Notepad).
4. Search for the parameter `ENTITY_retry_hour` and specify an integer value to modify the default verification time. The `ENTITY_retry_hour` value is in terms of number of hours. Acceptable values are from 1 to 24 hours.
5. Save and close `Entity.cfg` to apply the new verification time.

Searching for Managed Products, Product Directory Folders, or Computers

Use the **Search** button to quickly locate a specific managed product in the Product Directory.

Searching for a Folder or Managed Product

Procedure

1. Access the Product Directory.
2. Type the display name of the managed product in the **Find entity** field.
3. Click **Search**.

Performing an Advanced Search

Procedure

1. Access the Product Directory.
2. Click **Advanced Search**.

   The **Advanced Search** screen appears.

3. Specify your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.
4. Click **Search** to start searching.

   Search results appear in the **Search Result** folder of the Product Directory.

Refreshing the Product Directory

Procedure

- On the **Product Directory** screen, click the **Refresh** icon on the upper right corner of the screen.

Understanding the Directory Management Screen

After registering to Control Manager, the managed product appears in the Product Directory under the default folder.

Use the **Directory Management** screen to customize the Product Directory organization to suit your administration needs. For example, you can group products by location or product type (messaging security, web security, file storage protection).

The directory allows you to create, modify, or delete folders, and move managed products between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the managed products belonging to each folder. Consider the following factors when planning and implementing your folder and managed product structure:

- Product Directory
- User Accounts
- Deployment Plans

- Ad Hoc Query
- Control Manager reports

Group managed products according to geographical, administrative, or product-specific reasons. In combination with different access rights used to access managed products or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages.

TABLE 14-1. Product Grouping Comparison

GROUPING TYPE	ADVANTAGES	DISADVANTAGES
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

Using the Directory Management Screen Options

Use these options to manipulate and organize managed products in your Control Manager network.

The **Directory Management** screen provides several options:

- Add directories to the Product Directory
- Rename directories in the Product Directory
- Move managed products or directories in the Product Directory
- Remove managed products or directories from the Product Directory

Note

The keep permissions check box allows a folder to keep its source permission when moved.

Using the Directory Management Screen

Procedure

- Select a managed product or directory and click **Rename** to rename a managed product or directory
- Click **+** or the folder to display the managed products belonging to a folder
- Drag managed products or directories to move the managed products or directories in the Product Directory
- Click **Add Folder** to add a directory to the Product Directory

Accessing the Directory Management Screen

Use the **Directory Management** screen to group managed products together.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the **Product Directory** menu.

The **Directory Management** screen appears.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the **Product Directory** menu.

   The **Directory Management** screen appears.

3. Select **Local Folder**.

4. Click **Add Folder**.

   The **Add Directory** screen appears.

5. Type a name for the new directory in the **Directory name** field.

6. Click **Save**.

> **Note**
>
> Except for the **New Entity** folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabetic characters (a/A to z/Z).

Renaming Folders or Managed Products

Rename directories and managed products on the **Directory Management** screen.

> **Note**
>
> Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the **Product Directory** menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to rename.

4. Click **Rename**.

   The **Rename Directory** screen appears.

5. Type a name for the managed product or directory in the **Directory name** field.

6. Click **Save**.

7. Click **OK**.

The managed product or directory displays in the Product Directory with the new name.

Moving Folders or Managed Products

When moving folders pay special attention to the **Keep the current user access permissions when moving managed products/folders** check box. If you select this check box and move a managed product or folder, the managed product or folder keeps the permissions from its source folder. If you clear the keep permissions check box, and then move a managed product or folder, the managed product or folder assumes the access permissions from its new parent folder.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the **Product Directory** menu.

   The **Directory Management** screen appears.

3. On the working area, select the folder or managed product to move.

4. Drag the folder or managed product to the target new location.

5. Click **Save**.

Deleting User-Defined Folders

Take caution when deleting user-defined folders on the **Directory Management** screen. You may accidentally delete a managed product which causes it to unregister from the Control Manager server.

Note

You cannot delete the **New Entity** folder.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the **Product Directory** menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to delete.

4. Click **Delete**.

   A confirmation dialog box appears.

5. Click **OK**.

6. Click **Save**.

Chapter 15

Activating Control Manager and Managed Products

This chapter presents material administrators will need to activate or renew product licenses for Control Manager or managed products.

This chapter contains the following topics:

Activating and Registering Managed Products

To use the functionality of Control Manager 6.0 Service Pack 3, managed products (OfficeScan, ScanMail for Microsoft Exchange), and other services (Outbreak Prevention Services), you need to obtain Activation Codes and activate the software or services. Included with the software is a Registration Key. Use that key to register your software online to the Trend Micro Online Registration website and obtain an Activation Code.

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

All Activation Codes share the following characteristics:

- Created in real-time during registration
- Created based on Registration Key information
- Has an expiration date
- Product version independent

Note

In previous versions of Control Manager, a serial number was included with the product, and users needed to register online to use all the features of the software.

Understanding License Management

From the **License Management** screen, view, manage, and deploy the licenses of all managed products.

Note

Vary the number of Activation Codes the **License Management** screen displays using the **Rows per page** feature. The **License Management** screen can display 10 (default setting), 15, 30, or 50 Activation Codes at a time.

Screen Component	Description
Activation Code	Displays the Activation Code for the managed product.
Note	Displays additional information about the Activation Code.
Products	Displays the number of managed products to which the Activation Code deploys.
Status	Displays the status of the Activation Code: • Activated • Expired
Type	Displays the type of the Activation Code: • **Full**: Allows full use of the product for the maintenance period (typically 1 year) • **Trial**: Allows full use of the product for the evaluation period (typically 3 months)
Expiration Date	Displays the date the Activation Code expires.
Seat Count View license information online	Displays the number of seats the Activation Code allows. Opens your default Internet browser to launch the Trend Micro Customer License Portal. This portal allows you to manage your Trend Micro business account, which includes: • Activation Codes for on-premise products • *Subscriptions to Trend Micro Software as a Service solutions on page 6-6*

Activating Managed Products

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

Procedure

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

   The **License Management** screen appears.

2. Click **Add and Deploy**.

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

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

4. Click **Next**.

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

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

5. Select the managed product to which to deploy the Activation Code.

6. Click **Finish**.

   The **License Management** screen appears, with the new Activation Code listed in the table.

Renewing Managed Product Licenses

Control Manager can deploy or redeploy Activation Codes to registered products from the Product Directory or from the **License Management** screen.

Renewing Managed Product Licenses from the License Management Screen

Procedure

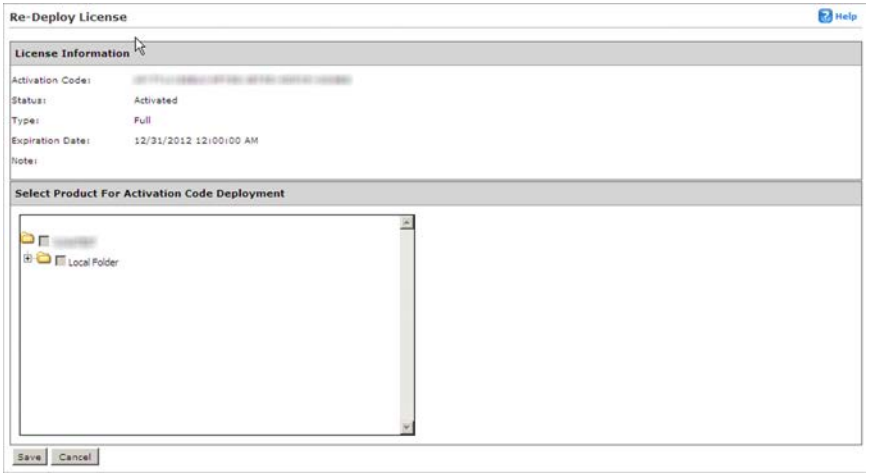
1. Navigate to **Administration** > **License Management** > **Managed Products**.

   The **License Management** screen appears.

2. Select an Activation Code from the list.

3. Click **Re-Deploy**.

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



4. Click **Save**.

Note

If no products appear in the list, the selected Activation Code does not support any products currently registered to Control Manager.

Renewing Managed Product Licenses from the Product Directory

Procedure

1. Access the **Product Directory**.
2. Select a managed product from the Product Directory tree.
3. Click **Tasks** from the **Product Directory** menu.
4. From the list of tasks, select **Deploy license profiles**.

5. On the **License Profiles** screen, click the **Deploy Now** link to make Control Manager load updated license information from the Trend Micro license server. Control Manager then deploys the license profiles automatically.

6. Click the **Command Details** link to open the **Command Details** screen, where you can review when Control Manager deployed the license profiles, the time of the last report, the user who authorized the deployment, and a breakdown of deployments in progress and successfully or unsuccessfully completed. You can also see a list of deployments by server.

About Activating Control Manager

Activating Control Manager allows you to use all of the product features, including downloading updated program components. You can activate Control Manager after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

Note

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

Understanding License Information

The **License Information** screen displays product information for Control Manager and Control Manager managed services.

Each section contains the following information:

TABLE 15-1. The License Information Screen

SCREEN COMPONENT	DESCRIPTION
Product	Displays the number of managed products to which the Activation Code deploys.

Screen Component	Description
Version	Displays the type of the Activation Code: • **Full**: Allows full use of the product for the maintenance period (typically 1 year) • **Trial**: Allows full use of the product for the evaluation period (typically 3 months)
Status	Displays the status of the Activation Code: • **Activated** • **Expired**
Activation Code	Displays the Activation Code for the managed product.
Expiration Date	Displays the date the Activation Code expires.

Activating Control Manager

Procedure

1. Navigate to Administration > License Management > Control Manager.

The **License Information** screen appears.

2. Click the **Specify a new Activation Code** link.

3. In the **New** box, type your Activation Code. If you do not have an Activation Code, click the **Register online** link and follow the instructions on the Online Registration website to obtain one.

4. Click **Activate**, and then click **OK**.

Renewing Maintenance for Control Manager or Managed Service

Renew maintenance for Control Manager or its integrated related products and services (Outbreak Prevention Services) using one of the following methods.

Make sure you already have obtained an updated Registration Key to acquire a new Activation Code to renew your product or service maintenance.

Renewing Maintenance Using Check Status Online

Procedure

1. Navigate to **Administration** > **License Management** > **Control Manager**.

   The **License Information** screen appears.

2. On the working area under the product or service to renew, click **Check Status**.

3. Click **OK**.

4. Log off and then log on to the web console for changes to take effect.

Renewing Maintenance by Manually Entering an Updated Activation Code

Procedure

1. Navigate to **Administration** > **License Management** > **Control Manager**.

   The **License Information** screen appears.

2. On the working area under the product or service to renew, click the **Specify a new Activation Code** link (to obtain an Activation Code, click the Register online link, and follow the instructions on the Online Registration website).

3. In the **New** box, type your Activation Code.
4. Click **Activate**.
5. Click **OK**.
6. Log off and then log on to the web console for changes to take effect.

Chapter 16

Managing Child Servers

This chapter presents material administrators will need when managing the Control Manager network. For information on the cascading management structure, see *Understanding Cascading Management on page 5-9* for details.

This chapter contains the following topics:

Understanding Parent-Child Communication

The Product Directory enumerates the parent server and all child servers in a Control Manager network.

The following table describes the connection status in a Control Manager cascading tree:

TABLE 16-1. Parent and Child Server Relationship

ACTION	PARENT  CHILD 	PARENT  CHILD 	PARENT  CHILD 	PARENT  CHILD 	STAND-ALONE SERVER
Direct unregistration from parent Control Manager server	√				
Registration to parent Control Manager server					√
Uninstall Control Manager (save the database)	√	√	√	√	√
Uninstall Control Manager (delete the database)	√	√	√	√	√

Based on the table:

- Direct unregistration of a disabled child server is not allowed
- Direct or forced unregistration of an active child server retains the child server record in the parent server database and removes the child server record in the child server database
- If you uninstall the Control Manager application on a disabled child server, save the Control Manager database, reinstall Control Manager, and then re-register it to the same parent server, the child server status will remain the same—disabled

- If you uninstall the Control Manager application on a disabled child server, delete the Control Manager database, reinstall Control Manager, and then re-register it to the same parent server, the child server status will become active

In addition, the table highlights the following parent and child server relationship when the cascading relationship is set to enable:

- The parent server:
  - Polls each child servers to update the Status Summary screen in real time
  - Updates a child server connection status every 60 minutes
- The child server:
  - Sends logs to the parent server
  - Sends new or updated report profiles

Disabling a child server does not permanently cut the connection between the two Control Manager servers. The parent and child server connection is still present. The parent server issues a single command to the child server — Enable Cascading Control Manager. Once the child server receives and accepts this command, the parent server resumes managing the child server.

Registering or Unregistering Child Servers

The action to register or unregister child servers does not generate the same result as to enable or disable child servers. Unregistering a child server permanently cuts the parent and child server connection. Disabling a child server temporarily suspends the connection and maintains the heartbeat connection between the parent and child servers.

For example, if you registered child server XYZ to parent server A. Then unregistered XYZ from parent server A and registered it to parent server B. Parent server B manages XYZ. A's Product Directory tree removes XYZ from the list.

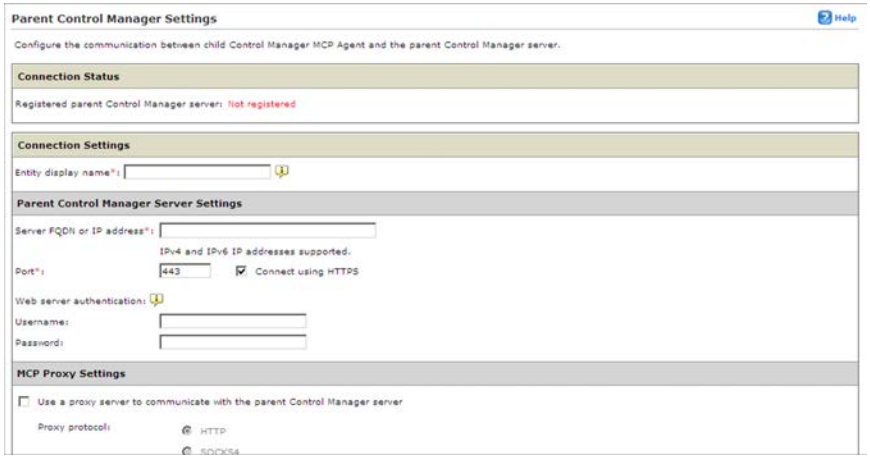
Use the **Parent Control Manager Settings** screen to register or unregister from a Control Manager parent server.

Registering a Child Server

Procedure

1. Navigate to **Administration** > **Settings** > **Parent Control Manager Settings**.

   The **Parent Control Manager Settings** screen appears.



2. Configure Connection Settings:

   - Type the name the child server displays in the parent Control Manager in the **Entity display name** field.

3. Configure Parent Control Manager Server Settings:

   a. Type the FQDN or IP address for the parent Control Manager server in the **Server FQDN or IP address** field.

   b. Type the port number the parent Control Manager uses to communicate with MCP agents in the **Port** field.

   Note

   For increased security, select **Connect using HTTPS**.

c. If the IIS Web server of Control Manager requires authentication, type the user name and password.

4. Configure MCP Proxy Settings:

   a. If you will use a proxy server to connect to the Control Manager server, select **Use a proxy server to communicate with the Control Manager server**.

   b. Select the protocol the proxy uses:

      - HTTP
      - SOCKS 4
      - SOCKS 5

   c. Type the proxy server's FQDN or IP address in the **Server name or IP address** field.

   d. Type the proxy server port number in the **Port** field.

   e. If the proxy server requires user authentication, type the user name and password.

5. Configure Two-way Communication Port Forwarding:

   a. If you will use port forwarding with MCP agents, select **Enable two-way communication port forwarding**.

   b. Type the forwarding IP address in the **IP address** field.

   c. Type the port number in the **Port** field.

6. To verify the child server can connect to the parent Control Manager server, click **Test Connection**.

7. Click **Register** to connect to the parent Control Manager server.

Note

If you change any of the settings on this screen after registration, click **Update Settings** to notify the Control Manager server of the changes. If you no longer want the Control Manager server to manage the server, click **Unregister** anytime.

Checking the Status in the Control Manager Web Console

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Check the **Cascading Folder** for newly registered Control Manager child servers.

Unregistering a Child Server

The action to register or unregister child servers does not generate the same result as to enable or disable child servers. Unregistering a child server permanently cuts the parent and child server connection. Disabling a child server temporarily suspends the connection and maintains the heartbeat connection between the parent and child servers.

When you want to balance the server load between servers a and b, these are the common scenarios:

- Parent server A is managing more child servers than parent server B
- Parent server A becomes overloaded and you want to reduce the load and transfer some child servers to parent server B

Use the **Parent Control Manager Settings** screen to unregister a child server from a parent server.

Procedure

1. Navigate to **Administration** > **Settings** > **Parent Control Manager Settings**.

The **Parent Control Manager Settings** screen appears.

2. Click **Unregister** at the bottom of the screen.

Accessing the Cascading Folder

Use the Product Directory to view and access functions for child servers.

Note

You can access the Cascading Folder only through the parent server web console.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Expand the **Cascading Folder** in the Product Directory.

Viewing Child Server Status Summaries

The **Product Directory** screen displays the Antivirus, Spyware/Grayware, Content Security, Web Security, and Network Virus summaries for all managed products. By default, a week's worth of summaries displays. You can change the scope to Today, Last Week, Last Two Weeks, or Last Month available in the **Display summary for** list.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select a child server.

   All child servers send status summaries to the parent server.

Note

The timing is based on the time interval setting in the `SystemConfiguration.xml`.

The default is every 30 minutes, as set by the `m_uiCasMcpChildTriggerDataSyncFreqInMin` parameter.

The default time interval is 3 minutes and the start time is 12:00 am. Configure these values to suit your management needs. All child servers send status summaries to the parent server. The timing is based on the time interval setting in `SystemConfiguration.xml` file.

Note

A child server uploads status summaries to the parent server when either 2,500 records is reached or 3 minutes elapses. During the time when the child server has not yet uploaded new logs to the parent server, the Outdated, Current, and Total managed product information in the Component Status table of the child server Product Status screen may not be current.

Configuring Log Upload Settings

Use the child server Configuration tab to set the schedule as to when the child server sends logs to the parent server.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select a child server from the Product Directory.

   The item highlights.

3. Move the cursor over **Configure** from the **Product Directory** menu.

   A drop-down menu appears.

4. Click **Schedule child Control Manager server log uploads**.

5. Under **Log Upload**, select **Upload child Control Manager server logs to the parent server**.

6. Set the upload schedule.

   - **Upload logs as soon as they are available**

     Select this option to instruct the child server to immediately send logs to the parent server.

     Note

     Selecting **Upload logs immediately** will prompt the child server to constantly send logs to the parent server, affecting network traffic.

   - **Schedule log upload to upload logs at a specific schedule**

   a. Set the **Frequency**: Daily or Weekly.

   b. Set the **Start time** by selecting the hour and minutes from the list. By default, the Start time is 20:00.

7. Select **Set the maximum upload time: hours** and set the maximum upload time, which determines the length of time that the child server will upload logs to the parent server.

   The default maximum upload time is 8 hours.

8. Click **Save**.

Note

Trend Micro recommends that you schedule the log upload with **Frequency = Daily** and **Start Time = after office hours or during off-peak hours** to prevent heavy network traffic during business hours. However, when the child server has not yet uploaded new logs to the parent server, the Component Status table of the child server's **Product Status** screen may not show current Outdated, Current, and Total managed product information.

Enabling or Disabling Child Server Connection

Use the **Configuration** menu item to enable or disable child server connection to the parent server.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select a child server from the Product Directory.

   The item highlights.

3. Move the cursor over **Configure** from the **Product Directory** menu.

   A drop-down menu appears.

4. Click the **Enable or Disable a child server connection** link.

5. On the working area, do one of the following:

   - Select **Enable a connection to this child Control Manager server** to enable a disabled child server
   - Select **Disable the connection to this child Control Manager server** to disable an enabled child server

   WARNING!

   Use care when disabling a child server connection. Managed products information registered to a disabled child server does not automatically upload to the parent server after you re-enable the child server connection. Restart the Trend Micro Control Manager service after enabling a child server to upload new managed product information to the parent server.

6. Click **Apply**.

Issuing Tasks to Child Servers

Use the Tasks menu item to perform any of the following actions to specific or all child servers.

- Deploy Anti-spam rules
- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select a child server from the Product Directory.

3. Perform one of the following:

   - Issue a task to the child server

     a. Move the cursor over **Tasks** from the **Product Directory** menu.

        A drop-down menu appears.

     b. Click any of the available tasks.

     c. Click **Deploy now**.

        A confirmation screen appears once Control Manager has completed the task.

     d. Click the **Command Details** link at the response screen to view command information, or click **OK**.

   - Access the child server's web console

     a. Move the cursor over **Configure** from the **Product Directory** menu.

        A drop-down menu appears.

b. Click **Child Control Manager Single Sign On**.

The child server's web console appears in a new window.

c. Log on to the child server and complete the required tasks.

Viewing Child Server Reports

Use the **Tasks** > **Reports** menu item to view a child server's existing report profiles for Static templates.

To view reports generated using Custom templates, using single sign-on, log on to the child Control Manager web console.

Procedure

1. Navigate to the **Product Directory** screen.
2. Select a child server from the Product Directory.

   The item highlights.
3. Move the cursor over **Tasks** from the **Product Directory** menu.

   A drop-down menu appears.
4. Select **Reports** from the drop-down menu.

   The **Reports** screen appears in the working area.

   Note

   When multiple reports are available on the **Reports** screen, sort reports according to Report Profile or Last Created date.
5. Under Available Reports, click the **View** link of the report profile that you want to open.
6. On the Available Reports for {profile name}, sort reports according to **Submission Time** or **Stage Completion Time**.

7. Under the **Status** column, click **View Child Control Manager Report**.

   A new browser window opens that displays the reports content.

Refreshing the Product Directory

Procedure

- On the **Product Directory** screen, click the **Refresh** icon on the upper right corner of the screen.

Renaming a Child Server

Use the rename option to change a child server's entity display name.

Procedure

1. Click **Directories** > **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the **Product Directory** menu.

   The **Directory Management** screen appears.

3. Select the child server to rename.

4. Click **Rename**.

   The **Rename Directory** screen appears.

5. Type a name for the child server in the **Directory name** field.

6. Click **Save**.

   A confirmation screen appears.

7. Click **OK**.

The child server displays in the Product Directory with the new name.

Removing Child Servers Accidentally Removed from the Cascading Manager

If you accidentally remove a child server from the Product Directory, you need to unregister and then re-register the child server to the parent server.

Chapter 17

Policy Management

This chapter contains information about how to perform policy management on managed products and endpoints.

Understanding Policy Management

Policy management allows administrators to enforce product settings on managed products and endpoints from a single management console. Administrators create a policy by selecting the targets and configuring a list of product settings.

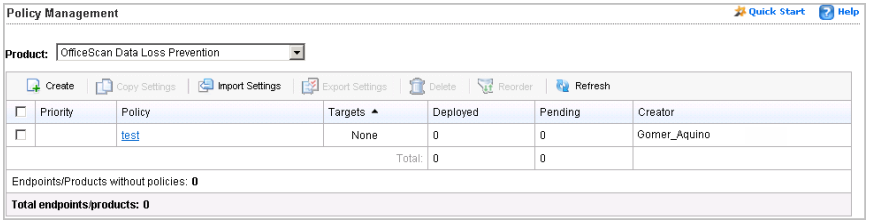
To perform policy management on a new managed product or endpoint, move the managed product from the New Entity folder to another folder in the Product Directory.

Creating a New Policy

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.



2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. Click **Create**.

The **Create Policy** screen appears.

4. Type a policy name.

5. Specify targets.

   Control Manager provides several target selection methods, which affect how a policy works.

   Note

   To include a managed product or endpoint as a target, make sure the product version of the managed product or endpoint supports policy management in Control Manager. The **Policy Template Settings** screen (**Policies** > **Policy Resources** > **Policy Template Settings**) contains information about supported product versions.

   The *policy list* arranges the policy targets in the following order:

   - **Specify Targets**: Use this option to select specific endpoints or managed products. For details, see *Specifying Policy Targets on page 17-8*.
   - **Filter by Criteria**: Use this option to allocate endpoints automatically based on the filtering criteria. For details, see *Filtering by Criteria on page 17-5*.
   - **None (Draft only)**: Use this option to save the policy as a draft without choosing any targets.

6. Click a managed product feature to expand it and configure its settings. Repeat this step to configure all features.

- Each feature has a link to a Help topic that discusses the feature and how to use it.
- For certain product settings, Control Manager needs to obtain specific setting options from the managed products. If administrators select multiple targets for a policy, Control Manager can only obtain the setting options from the first selected target. To ensure a successful policy deployment, make sure the product settings are synchronized across the targets.
- If you are creating a policy for **OfficeScan Agent** that you want to act as a parent to a future child policy, configure settings that can be inherited, customized, or extended on the child policy.
  - For a list of OfficeScan agent settings that can be inherited, customized, or extended, see *Working with Parent Policy Settings on page 17-10*.
  - For details on creating a child policy, see *Inheriting Policy Settings on page 17-14*.
- If you upgraded Control Manager 6.0 to 6.0 Service Pack 2 with **locally managed settings** to version 6.0 Service Pack 3, see the guidelines in *Working with Legacy Policy Settings and Permissions on page 17-12*.

7. Click **Deploy** or **Save**.

   If you clicked **Deploy**, Control Manager starts the deployment. The deployed policy appears in the list on the **Policy Management** screen. It usually takes a few minutes for Control Manager to deploy the policy to the targets.

   Click **Refresh** on the **Policy Management** screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Control Manager and the targets. Also check if the targets are working properly.

   Once Control Manager deploys a policy to the targets, the settings defined in the policy overwrite the existing settings in the targets. Control Manager enforces the policy settings in the targets every 24 hours. Although local administrators can make changes to the settings from the managed product console, the changes are overwritten every time Control Manager enforces the policy settings.

- Control Manager enforces the policy settings on the targets every 24 hours. Since policy enforcement only occurs every 24 hours, the product settings in the targets may not align with the policy settings if local administrators make changes through the managed product console between the enforcement period.
- Policy settings deployed to IMSVA servers take priority over the existing settings on the target servers instead of overwriting them. IMSVA servers save these policy settings on the top of the list.
- If an OfficeScan agent assigned with a Control Manager policy has been moved to another OfficeScan domain, the agent settings will temporarily change to the ones defined by that OfficeScan domain. Once Control Manager enforces the policy again, the agent settings will comply with the policy settings.

Filtering by Criteria

Use this option to allocate endpoints automatically based on the filtering criteria.

This option:

- Is only available on the following managed products:
  - OfficeScan
  - Mobile Security for Enterprise
  - Trend Micro Security (for Mac)
- Uses a filter to automatically assign current and future targets to the policy
- Is useful for deploying standard settings to a group of targets

Administrators can change the priority of filtered policies in the *policy list*. When an administrator reorders the policy list, Control Manager re-assigns the targets to different filtered policies based on the target criteria and the user roles of each policy creator.

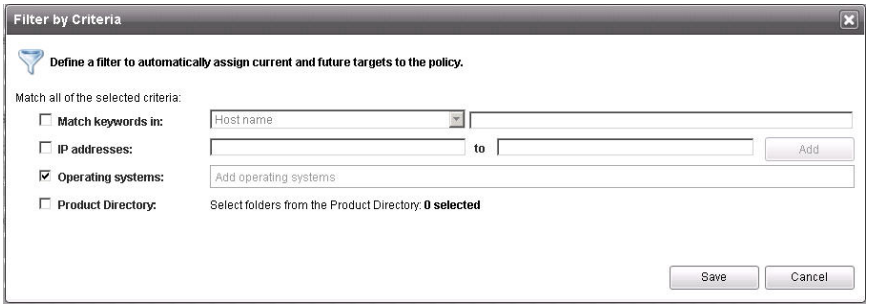
Control Manager can only assign endpoints without policies to a new filtered policy. To re-allocate an endpoint already assigned to a filtered policy, move another filtered policy with the matching criteria up the priority list.

See *Assigning Endpoints to Filtered Policies on page 17-7* for more information on how Control Manager assign targets to filtered policies.

Procedure

1. On the *Create Policy screen*, go to the **Targets** section, select **Filter by Criteria**, and then click **Set Filter**.

   The **Filter by Criteria** screen appears.



2. Select the following options and define the criteria. Control Manager assigns an endpoint to the policy if the target matches all of the selected criteria.

   - **Match keywords in**: Define keywords based on the host name or Control Manager display name.
   - **IP addresses**

     Note

     - Policy management only supports IPv4 addresses.
     - When a new managed product or endpoint registers to Control Manager, it takes about an hour for the managed product or endpoint to become available for search by IP address.

   - **Operating systems**
   - **Product Directory**: Select a folder from the Product Directory.

3. Click **Save**.

   The *Create Policy screen* reloads.

Assigning Endpoints to Filtered Policies

When a new endpoint registers to Control Manager, it goes through the filtered policies in the list in descending order. Control Manager assigns the new endpoint to a filtered policy when the following conditions are both satisfied:

- The new endpoint matches the target criteria in the policy
- The policy creator has the permission to manage the new endpoint

The same action applies to an endpoint already assigned to a policy, but the policy creator later deletes the policy.

Note

For endpoints just registered to Control Manager and for those just released from deleted policies, there is a three-minute grace period during which no endpoint allocation occurs. These endpoints are temporarily without policies during this period.

If an endpoint does not meet the target criteria in any filtered policies, the endpoint does not associate with any policies. Control Manager allocates these endpoints again when the following actions occur:

- Create a new filtered policy
- Edit a filtered policy
- Reorder the filtered policies
- Daily endpoint allocation schedule

  Control Manager uses a daily endpoint allocation schedule to ensure that endpoints are assigned to the correct policies. This action occurs once at 3:15 pm every day. When endpoint properties change, such as the operating system or IP address, these endpoints require the daily schedule to re-assign them to the correct policies.

Note

If the endpoints are offline during the daily endpoint allocation schedule, the policy status for these endpoints will remain pending until they go online.

When the above actions occur, Control Manager allocate endpoints based on the following conditions:

TABLE 17-1. Endpoint Allocation for Filtered Policies

	New endpoints or endpoints from deleted policies	Endpoints without policies	Endpoints with policies
Create a new policy		●	
Edit a policy	●	●	●
Reorder the filtered policies	●	●	●
Daily endpoint allocation schedule	●	●	●

Specifying Policy Targets

Use this option to select specific endpoints or managed products.

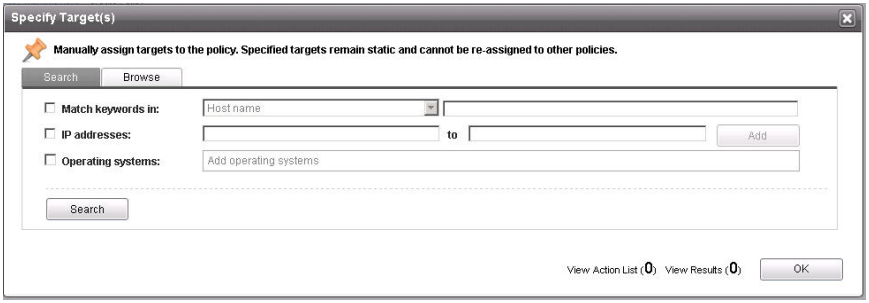
This option:

- Uses the search or browse function to locate specific targets and manually assigns them to the policy
- Is useful when administrators plan to deploy specific settings only to a certain targets
- Remains static on the top of the policy list and takes priority over any filtered policies

Procedure

1. On the *Create Policy screen*, go to the **Targets** section, select **Specify Target(s)**, and then click **Select**.

The **Specify Targets** screen appears.



2. Use **Search** or **Browse** to locate the targets.

   - **Search**: Use the following search criteria to find endpoints or managed products. The search results display the endpoints or managed products matching all of the selected criteria.

     - **Match keywords in**: Define keywords based on the host name or Control Manager display name.

     - **IP addresses**

       Note

       - Policy management only supports IPv4 addresses.
       - When a new managed product or endpoint registers to Control Manager, it takes about an hour for the managed product or endpoint to become available for search by IP address.

     - **Operating systems**

   - **Browse**: Browse the Product Directory or Active Directory to locate the endpoints or managed products and assign them to the policy.

     Note

     To set up the Active Directory, see *Configuring Active Directory and Endpoint Protection Verification Widget Settings on page 8-10* for details.

3. Select the endpoints or managed products and then click **Add Selected Targets**.
4. Wait for the numbers in **View Action List** and **View Results** to change.
5. Click **OK**.

   The *Create Policy screen* reloads.

Working with Parent Policy Settings

A Control Manager administrator creating a parent policy for **OfficeScan Agent** can configure certain settings on the policy to be inherited, customized, or extended.

Note

These options are not available on other managed products.

- **Inherit from parent**
  - A child policy administrator cannot change the setting at all. An OfficeScan administrator can manually change the setting from the OfficeScan server console. However, the setting will be overwritten when Control Manager deploys policies to the OfficeScan server.

    For example, a Control Manager administrator can create a parent policy that enforces the exclusion of PDF files from a Manual Scan.
  - Changes to the setting on the parent policy are always enforced on the child policy.
  - If the permission on the parent policy changes from "Inherit from parent" to "Are customizable" or "Extend from parent", the child policy administrator can customize or extend the current setting. Changes to the setting on the parent policy are no longer enforced.
- **Are customizable**
  - A child policy can deviate from the setting configured in the parent policy.

    For example, if Scheduled Scan on the parent policy runs weekly but is customizable, the child policy administrator can change the schedule to daily.

- Changes to the setting on the parent policy are never enforced on the child policy.
- If the permission on the parent policy changes from "Are customizable" to "Inherit from parent", the current setting on the parent policy overwrites the setting on the child policy. Changes to the setting on the parent policy are always enforced.

- Extend from parent
  - A child policy administrator can add to the items configured in the parent policy.

    For example, if the parent policy excludes 20 file names from being scanned during a Manual Scan, the administrator can add 10 more safe and trustworthy files to the child policy.
  - Items added or removed from the parent policy are also added or removed from the child policy. A removed item can be added back to the child.
  - If the permission on the parent policy changes from "Extend from parent" to "Inherit from parent", items in the child policy that have no match in the parent are removed. Changes to the items on the parent policy are always enforced.

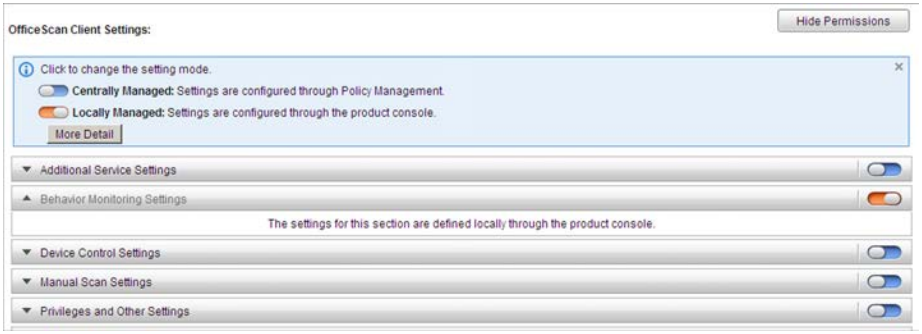
The following table lists the parent policy settings that can be inherited, customized, or extended.

Setting and Path	Available Options		
	Inherit From Parent	Are Customizable	Extend From Parent
Scan schedule **Scheduled Scan Settings** > **Target** tab > **Schedule** section	●	●	

Setting and Path	Available Options		
	Inherit From Parent	Are Customizable	Extend From Parent
File extensions to scan **Manual Scan / Real-time Scan / Scan Now / Scheduled Scan Settings** > **Target** tab > **Files to Scan** section > **Files with the following extensions** option	●		●
Scan exclusion lists (directories, files, and file extensions to exclude from scans) **Manual Scan / Real-time Scan / Scan Now / Scheduled Scan Settings** > **Scan Exclusion** tab	●		● When selecting **Extend from parent** from a scan exclusion list, the list expands to show a **Child Policy Restrictions** section where the parent policy creators can specify items that child policies cannot exclude from scans.

Working with Legacy Policy Settings and Permissions

In Control Manager 6.0 to 6.0 Service Pack 2, Control Manager administrators have the following options when configuring permissions for managed product settings:



- **Centrally Managed** (Blue): The assigned targets will comply with the settings defined in the policy.
- **Locally Managed** (Orange): Control Manager does not deploy the settings of the selected feature to the targets. Managed product administrators can define the settings through the product console.When administrators deploy a policy with all feature settings switched to locally managed, the policy status of the targets will remain in the pending state.

Starting in version 6.0 Service Pack 3, all features are considered centrally managed (switching permissions is no longer possible), except for features set to be locally managed in versions 6.0 to 6.0 Service Pack 2. For these locally managed features, administrators can keep them as they are. They can also change the permission to "centrally managed" (by sliding the orange-colored button to the left), which is permanent and therefore cannot be reversed later.

Copying Policy Settings

Administrators can copy the settings from an existing policy, create a new policy with the same settings, and deploy the settings to different endpoints or managed products.

Note

It is not possible to copy the settings of a child policy for **OfficeScan agent**. To determine whether a policy for OfficeScan agent is a child or a parent, check the **Parent Policy** column. A clickable value displays if the policy is a child, and N/A if otherwise.

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the Product list.

   The screen refreshes to display policies created for the selected managed product.

3. Select a policy from the list.

4. Click **Copy Settings**.

The **Copy and Create Policy** screen appears.

5. In the **Policy Name** field, type a name for the policy.
6. Assign **Targets** to the policy.
7. (Optional) Change settings as necessary.
8. Click **Deploy**.

Note

- After clicking **Deploy**, please wait two minutes for Control Manager to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
- Control Manager enforces the policy settings on the targets every 24 hours.

Inheriting Policy Settings

Create a new child policy by inheriting the settings of an existing parent policy. A child policy cannot be copied and its settings cannot be inherited.

This task requires a parent policy for **OfficeScan Agent** without *locally managed settings*. A parent policy for OfficeScan agent has the value **N/A** displayed under the **Parent Policy** column.

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.
2. Select **OfficeScan Agent** from the Product list.

   The screen refreshes to display policies created for the selected managed product.
3. Select a parent policy that does not have locally managed settings.
4. Click **Inherit Settings**.

The **Inherit and Create Policy** screen appears.

5. In the **Policy Name** field, type a name for the policy.

6. Assign **Targets** to the policy.

7. (Optional) Review the settings that can be customized or extended and then make changes as necessary. For a list of settings to review, see *Working with Parent Policy Settings on page 17-10*.

   Note

   A setting cannot be customized or extended if the option selected on the parent policy is **Inherit from parent**.

   For example:

   - If the Scheduled Scan setting is customizable, you can change the schedule from weekly to daily.
   - If the scan exclusion list for Real-time Scan can be extended, you can type additional file names that you deem safe and trustworthy. After the child policy is created, it will add those file names to the scan exclusion list.

8. Click **Deploy**.

   Note

   - After clicking **Deploy**, please wait two minutes for Control Manager to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.
   - Control Manager enforces the policy settings on the targets every 24 hours.

Modifying a Policy

Administrators can modify policy targets and settings as necessary. The root account owner can modify every policy in the list, while other account owners can only modify the policies they created. After a policy is modified, Control Manager deploys the policy to the targets.

For a parent policy for OfficeScan agent, if you modified the targets and settings for specific features, the modifications will apply to all child policies and deployed to the respective targets. Some settings on a parent policy support **permissions**, which control the changes allowed on child policies. Modifications to these parent policy permissions are also applied to child policies and deployed to targets. For a list of settings that support permissions, see *Working with Parent Policy Settings on page 17-10*.

For example:

- If you changed the scan schedule permission from "Inherit from parent" to "Are customizable", administrators can start to customize the existing schedule on their child policies.
- If you changed the Manual Scan file extensions permission from "Extend from parent" to "Inherit from parent", any file extensions that administrators added to child policies will be removed. In addition, administrators will no longer be able to add file extensions.

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. Click a policy name in the **Policy** column.

   The **Edit Policy** screen appears.

4. Modify the policy.

   Note

   Modifying the filtering criteria in a filtered policy can affect target allocation. Control Manager may re-assign some targets to other filtered policies, or add additional targets to the current policy.

   ---

5. Click **Deploy**.

It usually takes a few minutes for Control Manager to deploy the policy to the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list. If the status of the deployment remains pending after an extended period of time, there might be issues with the targets. Check if there is a connection between Control Manager and the targets. Also check if the targets are working properly.

Control Manager enforces the policy settings on the targets every 24 hours.

Importing and Exporting Policies

Export policies to back them up or to import them to another Control Manager server of the same version.

Notes:

- Control Manager exports policy settings but not policy targets.
- A *parent policy* stays as a parent after the export or import.
- A *child policy* becomes a parent after the export. Consequently, it is a parent after the import.
- Control Manager cannot import a policy if its name is the same as an existing child policy. If the existing policy is not a child, Control Manager overwrites it after the import.

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. To export, select one or several policies, click **Export Settings**, and then save the resulting policy file.

   If you exported a single policy, the resulting file has the extension `.cmpolicy`.

If you exported several policies, the resulting file is a compressed (`.zip`) file containing the individual `.cmpolicy` files. If you plan to import these files later to the same or another server, be sure to extract the individual files. It is not possible to import the compressed file.

4. To import, click **Import Settings** and then locate and load the `.cmpolicy` file.

   Import one file at a time. If the policy already exists in the policy list, a prompt message appears, asking if the Control Manager

   Control Manager will overwrite the existing policy. Click **Ok** to proceed.

   The screen refreshes to include the imported policy. The policy appears on top of the list. *Reorder* the policy list as necessary.

Deleting a Policy

Administrators can remove a policy from the list. Control Manager then re-allocates the targets associated with the deleted policy if the targets match the filtering criteria of another policy. Those without a match become endpoints without policies, and they keep the settings defined by the deleted policy unless a managed product administrator modifies the settings.

Control Manager only allows policy creators to delete their own policies. However, the root account can delete every policy in the list.

It is not possible to delete an OfficeScan Agent parent policy with settings *inherited* by an existing child policy.

Procedure

1. Navigate to **Policies** > **Policy Management**.

   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. Select the policy to delete.

4. Click **Delete**.

   A confirmation screen appears.

5. Click **OK**.

Understanding the Policy List

The policy list displays the information and status of policies created by all users. When a new endpoint registers to Control Manager, it goes through the filtered policies in the list in descending order. Control Manager assigns the new endpoint to a filtered policy when the following conditions are both satisfied:

- The new endpoint matches the target criteria of the policy
- The policy creator has the permission to manage the new endpoint

The following table describes the columns in the Policy Management screen, where the policy list displays. Click a column to sort its data.

TABLE 17-2. Policy List

MENU ITEM	DESCRIPTION
Priority	Displays the priority of the policies. • Control Manager lists policies from the highest to the lowest priority. • When administrators create a filtered policy, Control Manager saves the new policy as the lowest priority policy. • A specified policy takes priority over any filtered policies and remains on the top of the list. Administrators cannot reorder specified policies. • Control Manager places draft policies at the bottom of the list.
Policy	Displays the name of the policy

MENU ITEM	DESCRIPTION
Parent Policy	This column only appears if the selected product is **OfficeScan Agent**. If a policy is a child policy (that is, it inherited its settings from a parent policy), this column shows the name of the parent policy. Otherwise, N/A displays.
Deviations	This column only appears if the selected product is **OfficeScan Agent**. If a policy is a child policy, this column shows the number of settings that have been changed on the policy and are therefore inconsistent with settings on the parent policy. If settings are consistent between the policy and its parent, 0 (zero) displays. If a policy is not a child policy, N/A displays.
Targets	Displays how administrators select targets for the policy. • **Specified**: Uses the browse or search function to select specific targets for the policy. Specified policies remain static on the top of the policy list and take priority over filtered policies. • **Filtered**: Uses a filter to automatically assign current and future endpoints to the policy. Administrators can rearrange the priority of filtered policies. Mouseover an item to conveniently view the filter criteria and make adjustments as necessary. • **None**: The policy creator saved the policy as a draft without selecting any targets.
Deployed	Displays the number of targets that have applied the policy settings.
Pending	Displays the number of targets that have not applied the policy settings. Click the pending number to check the policy status.
Creator	Displays the user who created the policy.
Endpoints/Products without policies	Displays the number of managed products or endpoints to which Control Manager has not assigned a policy.

MENU ITEM	DESCRIPTION
Total endpoints/ products	Displays the number of managed products or endpoints available for policy management.

Note

The numbers in Deployed, Pending, Endpoints/Products without policies, and Total endpoints/products only reflect the endpoints or managed products an administrator has the permissions to manage.

Reordering the Policy List

Administrators can use the **Reorder** button to change the order of the filtered policies. Rearranging the policy list can affect target allocation. Control Manager may re-assign some targets to different filtered policies.

Note

- Specified policies remain static and always take priority over filtered policies.
- This function is only available for managing OfficeScan settings.

Procedure

1. Navigate to **Policies** > **Policy Management**.

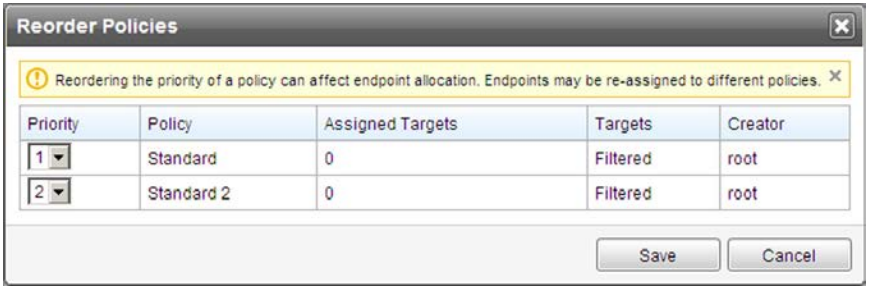
   The **Policy Management** screen appears.

2. Select the type of product settings from the **Product** list.

   The screen refreshes to display policies created for the selected managed product.

3. Click **Reorder**.

The **Reorder Policies** screen appears.



4. Rearrange the order of the **Priority** column.

5. Click **Save**.

Note

After clicking **Save**, please wait two minutes for Control Manager to re-assign the targets. Click **Refresh** on the **Policy Management** screen to update the status information in the policy list.

Updating the Policy Templates

The **Policy Template Settings** screen lists the following components available for administrators to enable or upgrade:

- Policy Management Framework: The overall policy structure
- Product Support: The setting templates for managed products and endpoints

Note

To check the product versions that support policy management, move the mouse cursor over the information icon in the **Template Version** column.

Procedure

1. Download the latest **Control Manager widget pool and policy templates (for Control Manager 6.0 and later)** component.

   A blue notification appears on the top of the **Dashboard** and **Policy Management** screens.

2. Click **Update Now** in the notification box on either of the screens.

3. Click **OK** when the update completes.

   The screen refreshes and the logon screen appears.

4. Log on to the web console.

5. Navigate to **Policies** > **Policy Resources** > **Policy Template Settings**.

   The **Policy Template Settings** screen appears.

6. Click **Update <version number>** in the Policy framework row.

7. To add a new policy template, click **Enable** in the **Action** column.

   Administrators can then select the new setting templates from the **Product** list on the **Policy Management** screen.

8. To update an existing template, click **Update <version number>** in the **Action** column.

   Note

   To see more information about the update, click **Details** in the **Action** column.

   Once the update completes, administrators can check the updated features by editing existing policies. Under the **Settings** section, a red message appears next to the new feature title.

Understanding Data Loss Prevention

Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data-referred to as digital assets-against accidental disclosure and intentional theft. DLP allows you to:

- Identify the digital assets to protect
- Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices
- Enforce compliance to established privacy standards

DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. You can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure. For details, see *Expressions on page 17-25*.
- **File attributes**: File properties such as file type and file size. For details, see *File Attributes on page 17-29*.
- **Keywords**: A list of special words or phrases. For details, see *Keywords on page 17-31*.

Note

It is not possible to delete a data identifier that is being used in a DLP template. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

You can use predefined and customized expressions. For details, see *Predefined Expressions on page 17-25* and *Customized Expressions on page 17-26*.

Predefined Expressions

A Trend Micro product comes with a set of predefined expressions. These expressions cannot be modified or deleted.

A Trend Micro product verifies these expressions using pattern matching and mathematical equations. After a Trend Micro product matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Viewing Settings for Predefined Expressions

Note

Predefined expressions cannot be modified or deleted.

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click the expression name.
4. View settings in the screen that opens.

Customized Expressions

Create customized expressions if none of the predefined expressions meet your requirements.

Expressions are a powerful string-matching tool. Ensure that you are comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, if you are creating an expression that includes a date, you can refer to the expressions prefixed with "Date".
- Note that a Trend Micro product follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

There are several criteria that you can choose from when creating expressions. An expression must satisfy your chosen criteria before a Trend Micro product subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expression on page 17-26*.

Criteria for Customized Expression

TABLE 17-3. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

Criteria	Rule	Example
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number Expression: [^\d]([0123678]\d{8})[^\d] Characters: 0123456789 Minimum characters: 9 Maximum characters: 9
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] Suffix characters: 0123456789- Number of characters: 5 Minimum characters in the expression: 25 Maximum characters in the expression: 80
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] Separator: @ Minimum characters to the left: 3 Maximum characters to the left: 15 Maximum characters to the right: 30

Creating a Customized Expression

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the expression. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Type the expression and specify whether it is case-sensitive.
7. Type the displayed data.

   For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.
8. Choose one of the following criteria and configure additional settings for the chosen criteria (see *Criteria for Customized Expression on page 17-26*):

   - None
   - Specific characters
   - Suffix
   - Single-character separator
9. Test the expression against an actual data.

   For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.
10. Click **Save** if you are satisfied with the result.

Note

Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

Importing Customized Expressions

Use this option if you have a properly-formatted `.dat` file containing the expressions. You can generate the file by exporting the expressions from either the Trend Micro product server you are currently accessing or from another Trend Micro product server.

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Import** and then locate the `.dat` file containing the expressions.
4. Click **Open**.

   A message appears, informing you if the import was successful. If an expression to be imported already exists, it will be skipped.

File Attributes

File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For example, a software development company may want to limit the sharing of the company's software installer to the R&D department, whose members are responsible for the development and testing of the software. In this case, the Trend Micro product administrator can create a policy that blocks the transmission of executable files that are 10 to 40MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Creating a File Attribute List

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the file attribute list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Select your preferred true file types.
7. If a file type you want to include is not listed, select **File extensions** and then type the file type's extension. A Trend Micro product checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:

   - Each extension must start with an asterisk (*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, `*.pol` matches `12345.pol` and `test.pol`.
   - You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (*) to represent two or more characters. See the following examples:

     - `*.*m` matches the following files: `ABC.dem`, `ABC.prm`, `ABC.sdcm`
     - `*.m*r` matches the following files: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`
     - `*.fm?` matches the following files: `ABC.fme`, `ABC.fml`, `ABC.fmp`

- Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: `*.do*` matches `abc.doctor_john.jpg` and `abc.donor12.pdf`.
- Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.

8. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.
9. Click **Save**.

Importing a File Attribute List

Use this option if you have a properly-formatted `.dat` file containing the file attribute lists. You can generate the file by exporting the file attribute lists from either the Trend Micro product server you are currently accessing or from another Trend Micro product server.

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.
2. Click the **File Attribute** tab.
3. Click **Import** and then locate the `.dat` file containing the file attribute lists.
4. Click **Open**.

   A message appears, informing you if the import was successful. If a file attribute list to be imported already exists, it will be skipped.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a

DLP policy and then configure a Trend Micro product to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 17-32* and *Customized Keyword Lists on page 17-33*.

Predefined Keyword Lists

A Trend Micro product comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation

For details about the predefined keyword lists in a Trend Micro product, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

How Keyword Lists Work

Number of Keywords Condition

Each keyword list contains a condition that requires a certain number of keywords be present in a document before the list will trigger a violation.

The number of keywords condition contains the following values:

- **All**: All of the keywords in the list must be present in the document.
- **Any**: Any one of the keywords in the list must be present in the document.
- **Specific number**: There must be at least the specified number of keywords in the document. If there are more keywords in the document than the number specified, a violation will trigger.

Distance Condition

Some of the lists contain a "distance" condition to determine if a violation is present. "Distance" refers to the amount of characters between the first character of one keyword and the first character of another keyword. Consider the following entry:

First Name:_John_ Last Name:_Smith_

The **Forms - First Name, Last Name** list has a "distance" condition of fifty (50) and the commonly used form fields of "First Name" and "Last Name". In the example above, a violation will trigger as the number of characters between the "F" in First Name and the "L" in Last Name is equal to eighteen (18).

For an example of an entry that would not trigger a violation, consider the following:

The first name of our new employee from Switzerland is John. His last name is Smith.

In this example, the number of characters between the "f" in "first name" and the "l" in "last name" is sixty-one (61). This exceeds the distance threshold and does not trigger a violation.

Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meet your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before a Trend Micro product subjects it to a DLP policy. Choose one of the following criteria for each keyword list:

- Any keyword
- All keywords
- All keywords within <x> characters
- Combined score for keywords exceeds threshold

For details regarding the criteria rules, see *Customized Keyword List Criteria on page 17-33*.

Customized Keyword List Criteria

TABLE 17-4. Criteria for a Keyword List

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.

CRITERIA	RULE
All keywords	A file must contain all the keywords in the keyword list.
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If a Trend Micro product detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK******************WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, will usually result in faster scanning time but will only cover a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Creating a Keyword List

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Add**.

   A new screen displays.
4. Type a name for the keyword list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
5. Type a description that does not exceed 256 bytes in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:

   - **Any keyword**
   - **All keywords**
   - **All keywords within <x> characters**
   - **Combined score for keywords exceeds threshold**
7. To manually add keywords to the list:

   a. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.

   b. Click **Add**.
8. To add keywords by using the "import" option:

Note

Use this option if you have a properly-formatted .csv file containing the keywords. You can generate the file by exporting the keywords from either the Trend Micro product server you are currently accessing or from another Trend Micro product server.

a. Click **Import** and then locate the `.csv` file containing the keywords.

b. Click **Open**.

A message appears, informing you if the import was successful. If a keyword to be imported already exists in the list, it will be skipped.

9. To delete keywords, select the keywords and click **Delete**.

10. To export keywords:

Note

Use the "export" feature to back up the keywords or to import them to another Trend Micro product server. All keywords in the keyword list will be exported. It is not possible to export individual keywords.

a. Click **Export**.

b. Save the resulting `.csv` file to your preferred location.

11. Click **Save**.

Importing a Keyword List

Use this option if you have a properly-formatted `.dat` file containing the keyword lists. You can generate the file by exporting the keyword lists from either the Trend Micro product server you are currently accessing or from another Trend Micro product server.

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Data Identifiers**.

2. Click the **Keyword** tab.

3. Click **Import** and then locate the `.dat` file containing the keyword lists.

4. Click **Open**.

   A message appears, informing you if the import was successful. If a keyword list to be imported already exists, it will be skipped.

Data Loss Prevention Templates

A DLP template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources personnel to transmit the file through printing so that the printed copy can be signed by an employee. Transmission through all other possible channels, such as email, is blocked.

You can create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see *Customized DLP Templates on page 17-38* and *Predefined DLP Templates on page 17-37*.

Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

A Trend Micro product comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA**: Gramm-Leach-Billey Act
- **HIPAA**: Health Insurance Portability and Accountability Act

- **PCI-DSS**: Payment Card Industry Data Security Standard
- **SB-1386**: US Senate Bill 1386
- **US PII**: United States Personally Identifiable Information

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized DLP Templates

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see *Condition Statements and Logical Operators on page 17-38*.

Condition Statements and Logical Operators

A Trend Micro product evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

TABLE 17-5. Sample Condition Statements

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier1] **And** [Data Identifier 2] **Except** [Data Identifier 3]	A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier 1] **Or** [Data Identifier 2]	A file must satisfy [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].
Except [Data Identifier 1]	A file must not satisfy [Data Identifier 1]. For example: A file must not be [a multimedia file].

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

Creating a Template

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Templates**.
2. Click **Add**.

   A new screen displays.
3. Type a name for the template. The name must not exceed 100 bytes in length and cannot contain the following characters:

   - > < * ^ | & ? \ /
4. Type a description that does not exceed 256 bytes in length.
5. Select data identifiers and then click the "add" icon.

   When selecting definitions:

   - Select multiple entries by pressing and holding the **CTRL** key and then selecting the data identifiers.

- Use the search feature if you have a specific definition in mind. You can type the full or partial name of the data identifier.
- Each template can contain a maximum of 30 data identifiers.

6. To create a new expression, click **Expressions** and then click **Add new expression**. In the screen that appears, configure settings for the expression.
7. To create a new file attribute list, click **File attributes** and then click **Add new file attribute**. In the screen that appears, configure settings for the file attribute list.
8. To create a new keyword list, click **Keywords** and then click **Add new keyword**. In the screen that appears, configure settings for the keyword list.
9. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before a Trend Micro product subjects it to a DLP policy.
10. Choose a logical operator for each definition.

Note

Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see *Condition Statements and Logical Operators on page 17-38*.

11. To remove a data identifier from the list of selected identifiers, click the trash bin icon.
12. Below **Preview**, check the condition statement and make changes if this is not your intended statement.
13. Click **Save**.

Importing Templates

Use this option if you have a properly-formatted `.dat` file containing the templates. You can generate the file by exporting the templates from either the Trend Micro product server you are currently accessing or from another Trend Micro product server.

Procedure

1. Navigate to **Policies** > **Policy Resources** > **DLP Templates**.
2. Click **Import** and then locate the `.dat` file containing the templates.
3. Click **Open**.

   A message appears, informing you if the import was successful. If a template to be imported already exists, it will be skipped.

Chapter 18

Investigating Data Loss Prevention Incidents

Control Manager provides the capability for DLP compliance officers and incident reviewers to review and update incident information.

This chapter contains the following topics:

Administrator Tasks

To enable the incident review process, Control Manager administrators need to complete some prerequisite tasks. The following table lists the required tasks and references:

TABLE 18-1. Administrator Tasks

TASK	REFERENCES
Set up manager information in Active Directory.	*Setting Up Manager Information in Active Directory Users on page 18-3*
Set up Active Directory integration to obtain user information.	*Configuring Active Directory and Endpoint Protection Verification Widget Settings on page 8-10*
Create user accounts specific for DLP incident investigation. Assign DLP Compliance Officer or DLP Incident Reviewer roles to users investigating DLP incidents. **Note** The DLP Compliance Officer and DLP Incident Reviewer roles are available to Active Directory users only.	• *Understanding DLP User Roles on page 18-5* • *Understanding User Roles on page 3-3* • *About Adding/Importing User Accounts on page 3-18*
Set up the **Scheduled incident summary** and **Incident details updated** notifications.	• *Configuring Scheduled Incident Summary Settings on page 10-29* • *Configuring Incident Details Updated Settings on page 10-30*
Export DLP logs for auditing purposes.	• *Creating DLP Auditing Logs on page 18-7* • *Querying Log Data on page 11-6*

Setting Up Manager Information in Active Directory Users

For managers to investigate DLP incidents, set up the manager information in each Active Directory user.

Procedure

1. Open the Active Directory Users and Computers console. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.

   The **Active Directory Users and Computers** console appears.

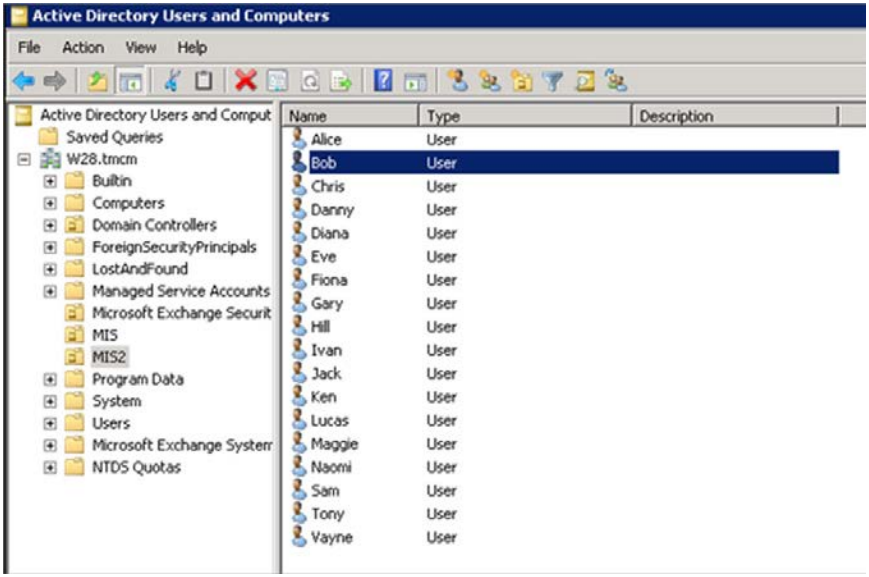


FIGURE 18-1. Active Directory Users and Computers console

2. Double-click a user.

The **<user> Properties** screen appears.

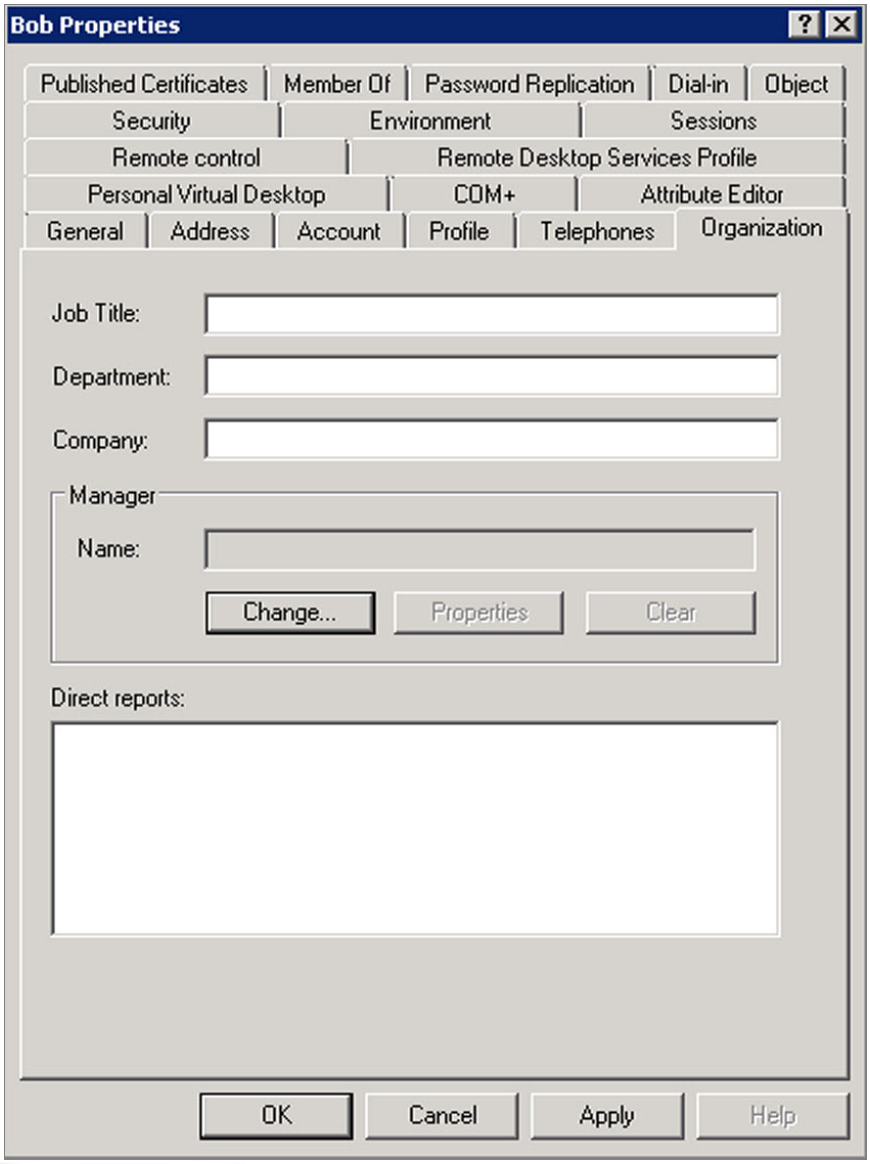


FIGURE 18-2. <user> Properties screen

3. Click the **Organization** tab and then click **Change...**.

   The **Select User or Contact** screen appears.

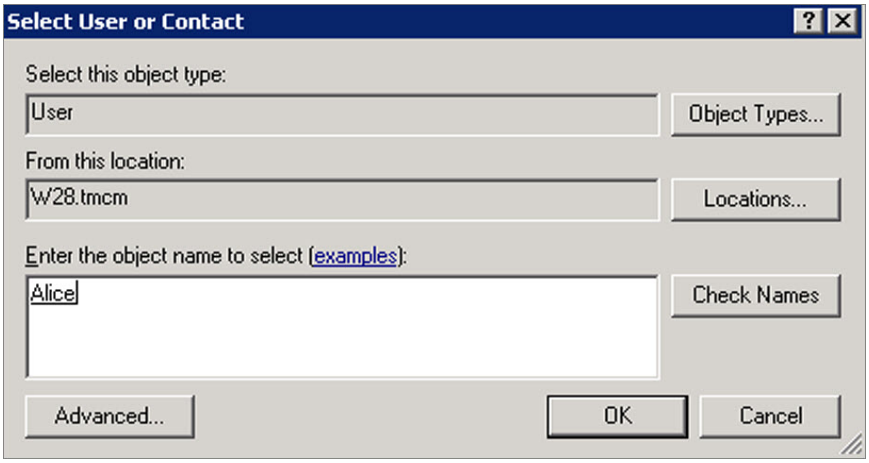


FIGURE 18-3. Select User or Contact screen

4. Specify the manager information and click **OK**.

5. To verify the manager-user relationship, open the manager's **<user> Properties** screen, click the **Organization** tab, and check the user information under **Direct reports**.

Understanding DLP User Roles

The DLP Compliance Officer and DLP Incident Reviewer are the only two roles with the permission to review DLP incidents.

Note

The DLP Compliance Officer and DLP Incident Reviewer roles are available to Active Directory users only.

The following table describes the features and characteristics related to these user roles:

TABLE 18-2. DLP Compliance Officer and DLP Incident Reviewer Features

ITEM	DESCRIPTION

DLP logs	Access to DLP logs is strictly limited to the following user roles:
	• DLP Compliance Officer:
	  • Complete access
	  • Specific widgets display DLP incident information
	• DLP Incident Reviewer:
	  • Access limited to DLP logs related to directly managed users
	  • Specific widgets display DLP incident information

Incident scope	• DLP Compliance Officer: Views incident data of the entire Active Directory users • DLP Incident Reviewer: Views incident data of directly managed users
Menu access	**Dashboard** and the widgets listed in the **DLP Incident Investigation** tab: • DLP Incidents by Severity and Status • DLP Incident Trends by User • DLP Incidents by User See *DLP Incident Investigation Tab on page 8-5* for more information.
Scheduled incident summary notification	• Daily or weekly email notification • Summary list of incident count by severity level • Link to the Control Manager web console • Both the DLP Compliance Officer and DLP Incident Reviewer receive this notification
Incident details updated notification	• Notification of modification to incident status or comments • Only the DLP Compliance Officer receives this notification

Creating DLP Auditing Logs

Administrators can use Ad Hoc Query to generate and export DLP auditing logs. Perform a log query as described in *Querying Log Data on page 11-6* and configure the following:

- Data scope: **Select Control Manager**
- Data view: Select **User Access Information**
- Query criteria: Add the following activities to Custom criteria:
  - Delete DLP logs
  - Delete access logs
  - Download DLP incident file
  - Enable access log maintenance
  - Enable DLP log maintenance
  - Disable access log maintenance
  - Disable DLP log maintenance
  - Update DLP incident
  - Change DLP log maintenance setting
  - Update access log maintenance settings

DLP Incident Review Process

Once Control Manager administrators have completed the prerequisite tasks, the reviewers can start the incident review process. The following table lists the tasks and references:

TABLE 18-3. DLP Incident Review Process

TASK	DESCRIPTION
Receive the scheduled incident summary notification message	Control Manager summarizes and sends email notifications to the incident reviewers daily or weekly.
Review details about the incident using one of the following methods: • Click the link provided in the message to log on to the Control Manager web console • Open the attachment (if available)	*Understanding the Incident Information List on page 18-8*
Update the incident status and provide comments	*Reviewing Incident Details on page 18-10*

Understanding the Incident Information List

The **Incident Information** screen displays a list of incidents manageable for the reviewer. Incident reviewers can use this screen to do the following:

- View incident summary
- Take actions on incidents
- Export incident details

TABLE 18-4. Incident Information List

ITEM	DESCRIPTION
ID	Unique incident ID

ITEM	DESCRIPTION
Received	Date and time when Control Manager received incident data **Note** After receiving DLP logs from managed products, Control Manager needs 30 minutes to process the logs before incident reviewers can view the data.
Severity	Severity level of the incident **Note** Once Control Manager receives and processes a DLP incident, Control Manager does not update the severity level if changes occur in the managed product.
Policy	Name of the Control Manager policy that triggered the incident **Note** For incidents triggering DLP policies created in managed products, this appears as **N/A**.
User	Name of the user who triggered the incident
Manager	Name of the user's manager
Status	Current status of the incident • New • Under Investigation • Escalated • Closed
Action	Action available for managing the incident

Reviewing Incident Details

By clicking the **Edit** icon in the **Action** column of the **Incident Information** screen, the **Incident Details** screen appears displaying detailed information about the incident. DLP incident reviewers can use this screen to update the incident status and provide comments on the incident.

TABLE 18-5. Incident Details

ITEM	DESCRIPTION
ID	Unique incident ID
Status	Use this to update the review status of the incident. Available options: • **New** • **Under Investigation** • **Escalated** • **Closed**
Severity	Severity level of the incident **Note** Once Control Manager receives and processes a DLP incident, Control Manager does not update the severity level if changes occur in the managed product.
Policy	Name of the Control Manager policy that triggered the incident **Note** For incidents triggering DLP policies created in managed products, this appears as **N/A**.
Rule	Names of the rules from that triggered the incident

ITEM	DESCRIPTION
Received	Date and time when Control Manager received incident data **Note** After receiving DLP logs from managed products, Control Manager needs 30 minutes to process the logs before incident reviewers can view the data.
Generated	Date and time the incident occurred in the managed product
User	Name of the user who triggered the incident
Manager	Name of the user's manager
Sender	Source email address
Recipient	Destination email address
Endpoint	Source host name
IP	Source IP address
Template	Names of the templates that triggered the incident
Matching content	Digital assets that triggered the incident
File	Name or link to the file that triggered the incident **Note** The file is quarantined in the managed product.
SHA-1	Hash information of the file
Subject	Subject of the email message
Channel	Channel through which the transmission occurred
Action	Actions taken on the incident
User Justification Reason	The reasons provided by the agent users when administrators allow users to transfer sensitive data

ITEM	DESCRIPTION
Comments	User-defined notes about the incident

Chapter 19

Responding to Targeted Attacks and Advanced Threats

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

Control Manager combines threat-related data collected from Deep Discovery solutions and mitigation capabilities from endpoint security products (such as OfficeScan) to enable you to rapidly detect, analyze, and respond to these targeted attacks and advanced threats before they unleash lasting damage.

Virtual Analyzer Suspicious Objects

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.

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

For a list of supported managed products, see *Suspicious Object Management and Handling Process on page xxii*.

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

Note

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**.

The following columns show information about objects added to the suspicious objects list:

TABLE 19-1. Suspicious Objects Columns

COLUMN NAME	INFORMATION
Object	The suspicious object If an arrow icon is available before the suspicious object, click the icon to expand the table with details about the suspicious object.

Column Name	Information
Risk Level	If the suspicious object is: • **IP address or domain**: The risk rating that typically shows is High or Medium (see risk rating descriptions below). This means that high- and medium-risk IP addresses/domains are treated as suspicious objects. **Note** An IP address or domain with the Low risk rating is also displayed if it is associated with other potentially malicious activities, such as downloading executable files. • **URL**: The risk rating that shows is High or Medium. • **SHA-1 hash value**: The risk rating that shows is always High. Risk level descriptions: • **High**: Known malicious or involved in high-severity connections • **Medium**: IP address/domain/URL is unknown to reputation service • **Low**: Reputation service indicates previous compromise or spam involvement
Type	Suspicious object type: IP address, domain, URL, or SHA-1 hash value
Expiration	Date and time Virtual Analyzer will remove the object from the **Objects** tab

Column Name	Information
At Risk Endpoints	Endpoints with suspicious activities related to suspicious objects Sort the column to see which suspicious object affect the most number of endpoints. To view details for all endpoints, go to the **Handling Process** column and click **View**. In the new screen that opens, click **Impact Assessment**. If the status is **Not yet assessed**, select the object and then click **Assess Impact** to see the number of affected endpoints. Impact assessment on suspicious objects requires a Trend Micro product called **Deep Discovery Endpoint Sensor**. 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.
Scan Action	Action configured by Control Manager administrators against the suspicious object Control Manager automatically deploys the actions to certain managed products. For a list of supported managed products, see *Suspicious Object Management and Handling Process on page xxii*.
Handling Process	A link to a screen that breaks down the suspicious object handling process into phases. For details, see *Handling Process on page 19-6*.

Suspicious Objects Tasks

The following table lists all options available:

TABLE 19-2. Suspicious Objects Tasks

TASK	STEPS
Export All	Click **Export All** to save all the objects to a CSV file.
Add to Exception	Select one or several objects that you consider harmless and then click **Add to Exception** . The objects move to the **Exceptions** tab.
Never Expire	Select one or several objects that you always want flagged as suspicious and then click **Never Expire** .
Expire Now	Select one or several objects that you want removed from the **Objects** tab and then click **Expire Now** . When the same object is detected in the future, it will be added back to the **Objects** tab.
Configure Scan Action	Select one or several objects that you want managed products to take an action against (or do not make any selection to select all objects) and then click **Configure Scan Action**. In the new window that opens, select the action. There are separate actions for files and IP addresses/URLs. Control Manager automatically deploys the actions to certain managed products. For a list of supported managed products, see *Suspicious Object Management and Handling Process on page xxii*.
Assess Impact	Select one or several **files** or **IP addresses** and then click **Assess Impact** to see how many endpoints are affected by these objects. A message displays on top of the screen, informing you that *impact assessment* has started. Impact assessment on suspicious objects requires a Trend Micro product called **Deep Discovery Endpoint Sensor**. After the assessment is complete, check the **At Risk Endpoints** column to see the number of affected endpoints.

TASK	STEPS
Data Filters	If there are too many entries in the table, limit the entries by performing these tasks: • Select an object type in the **View** dropdown box. • Type some characters in the text box next to **View** and then press **Enter**. Control Manager searches only the **Object** column for matches.
Records and Pagination Controls	The panel on the bottom right section of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.

Handling Process

The Handling Process screen breaks down the suspicious object handling process into phases.

Note

A detailed explanation of the handling process is discussed in *Suspicious Object Management and Handling Process on page xxii*.

TABLE 19-3. Suspicious Object Handling Process

PHASE	FOCUS
Sample Submission	First and last submission of a sample that triggered the detection of the suspicious object
Analysis	The analyzing product, a link to an analysis report, and a list of notable characteristics exhibited by the suspicious object
Distribution	A list of Trend Micro products to which Control Manager sends suspicious objects

PHASE	FOCUS
Impact Assessment	List of at-risk endpoints (endpoints affected by suspicious objects) and suspicious activities on these endpoints Managed products took a "passive" action (such as Log or Pass) against these suspicious objects. If products took an "active" action, the endpoints will be listed under the **Mitigation** tab. Click a link under **Suspicious Activities** to investigate further or open a new screen showing the sequence of activities in a graph.
Mitigation	"Active" actions (such as Block, Quarantine, or Delete) taken against suspicious objects during mitigation tasks

Exceptions

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.

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.

The following columns show information about objects in the exception list.

TABLE 19-4. Exceptions Columns

COLUMN NAME	INFORMATION
Object	The IP address, domain, URL, or SHA-1 hash value
Type	IP address, domain, URL, or SHA-1 hash value
Notes	Notes for the object
Added	Date and time Control Manager added the object to the **Exceptions** tab

Exceptions Tasks

The following table lists all the options available:

TABLE 19-5. Exceptions Tasks

TASK	STEPS
Add	Click **Add** to add an object. In the new window that opens, configure the following: • **Type**: Select an object type and then type the object (IP address, domain, URL or SHA-1 hash value) in the next field. • **Note**: Type some notes for the object
Import	Click **Import** to add objects from a properly-formatted CSV file. In the new window that opens: • If you are importing exceptions for the first time, click **Download sample CSV**, save and populate the CSV file with objects (see the instructions in the CSV file), click **Browse**, and then locate the CSV file. • If you have imported exceptions previously, save another copy of the CSV file, populate it with new objects, click **Browse**, and then locate the CSV file.
Export All	Click **Export All** to save all the objects to a CSV file.
Delete	Select one or several objects to remove and then click **Delete**.
Data Filters	If there are too many entries in the table, limit the entries by performing these tasks: • Select an object type in the **View** dropdown box. • Type some characters in the text box next to **View** and then press **Enter**. Control Manager searches only the **Object** column for matches.
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.

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**.

User-defined suspicious objects have a higher priority than Virtual Analyzer suspicious objects.

The following columns show information about objects added to the suspicious objects list:

TABLE 19-6. User-Defined Suspicious Objects Columns

COLUMN NAME	INFORMATION
Object	The suspicious object
Type	Suspicious object type: IP address, domain, URL, or file SHA-1
Scan Action	Action configured by Control Manager administrators against the suspicious object Control Manager automatically deploys the actions to certain managed products. For a list of supported managed products, see *Suspicious Object Management and Handling Process on page xxii*.
Notes	Additional information about the suspicious object
Last Modified	Date and time information about the suspicious object was modified

User-Defined Suspicious Objects Tasks

The following table lists all options available:

TABLE 19-7. User-defined Suspicious Objects Tasks

TASK	STEPS
Add	Click **Add** to add a suspicious object. In the new window that opens, configure the following: • **Type**: Select an object type and then type the object (IP address, domain, URL or SHA-1) in the next field. • **Scan action**: Select an action a managed product will take against the object. This field is not available if the type selected is **Domains**. Control Manager automatically deploys the actions to certain managed products. For a list of supported managed products, see *Suspicious Object Management and Handling Process on page xxii*. • **Note**: Type some notes for the object.
Import	Click **Import** to add objects from a properly-formatted CSV file. In the new window that opens: • If you are importing objects for the first time, click **Download sample CSV**, save and populate the CSV file with objects (see the instructions in the CSV file), click **Browse**, and then locate the CSV file. • If you have imported objects previously, save another copy of the CSV file, populate it with new objects, click **Browse**, and then locate the CSV file.
Edit	Select an object to modify and then click **Edit**. In the new window that opens, modify the action and notes as necessary.
Export All	Click **Export All** to save all the objects to a CSV file.
Delete	Select one or several objects to remove and then click **Delete**.
Data Filters	If there are too many entries in the table, limit the entries by performing these tasks: • Select an object type in the **View** dropdown box. • Type some characters in the text box next to **View** and then press **Enter**. searches only the **Object** column for matches.

TASK	STEPS
Records and Pagination Controls	The panel on the bottom right section of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view.

Distribution Settings

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.

For a list of supported managed products, see *Suspicious Object Management and Handling Process on page xxii*.

Control Manager can also send suspicious IP addresses and domains to a third-party product called HP TippingPoint.

Procedure

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

   The **Distribution Settings** screen appears.

2. In the **Trend Micro Managed Product Settings** section:

   a. Mark the check box to send suspicious objects to managed products.

   b. 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

3. In the **HP TippingPoint Settings** section:

   a. Mark the check box to send suspicious objects to HP TippingPoint.

Control Manager sends suspicious IP addresses and domain names analyzed by Deep Discovery Inspector and Deep Discovery Analyzer. HP 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 HP TippingPoint documentation.

b. Provide the following information:

- **Server name**: Service URL of your HP TippingPoint deployment
- **User name** and **password**: Account with sufficient privileges to access the HP TippingPoint console

c. Click **Test Connection** to confirm the connection.

d. Select the **severity** that triggers Control Manager to send IP address/domain name information to HP 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

e. Specify the column names that HP TippingPoint will display, along with the tag it will use to categorize the list.

Control Manager sends the corresponding values for the following tags:

Important

Add tag categories to the HP TippingPoint Reputation Database before submitting the reputation list. Otherwise, missing or misspelled tags in HP TippingPoint will cause a mismatch and prevent Control Manager from sending the suspicious objects list.

- **Severity**: Tag name of the severity column

  Possible values: High, Medium, Low

- **Product Name**: Deep Discovery

- **Publisher Name**: Column header of the software publisher

  Possible value: Trend Micro Control Manager

4. Click **Save**.

Indicators of Compromise (IOCs)

Files in OpenIOC format describe Indicators of Compromise (IOC) identified on a host or network. IOCs help administrators and investigators analyze and interpret threat data in a consistent manner.

A Trend Micro product called Deep Discovery Endpoint Sensor can run impact assessment on an IOC file.

The following columns show information about IOCs:

TABLE 19-8. Indicators of Compromise (IOCs) Columns

COLUMN NAME	INFORMATION
File Name	IOC file name. Clicking the file name opens a new window with a list of supported indicators. Unsupported indicators are grayed out and appear as strikethrough text.
Description	Additional information about the IOC file

Column Name	Information
Latest Investigation	If you run *impact assessment* on the IOC file, the following columns show information about the status of the assessment: • **Started**: Date and time the assessment was started • **Progress**: Percentage of assessment completion • **Settings**: Link to a new window with the IOC settings you specified before running impact assessment • **At Risk**: Number of at-risk endpoints determined after the assessment. Clicking the number opens a new screen with additional tasks for endpoints that require mitigation. For details, see *At-risk Endpoints on page 19-15*. • **Safe**: Number of safe endpoints determined after the assessment • **Pending/With Issues**: Number of endpoints that are currently being assessed (pending) or with issues. Clicking the number opens a new screen with detailed status information. For details, see *Pending Agents and Agents with Issues on page 19-19*.

Indicators of Compromise (IOCs) Tasks

The following table lists all options available:

Table 19-9. Indicators of Compromise (IOCs) Tasks

Task	Steps
Add	Click **Add** to add an IOC file. In the new window that opens, locate the file and then click **Upload**. You can add IOC files generated from Deep Discovery products. For details, see *IOC Management on page xxxi*.
Remove	Select one or several files to delete and then click **Remove**.

Task	Steps
Assess Impact	*Impact assessment* on IOC files requires a Trend Micro product called Deep Discovery Endpoint Sensor. Select one or several files to assess and then click **Assess Impact**. In the new window that opens, select the target endpoints with Deep Discovery Endpoint Sensor installed. You can select all endpoints or specify several endpoints (one endpoint per line) identified by their host names or IP addresses. Click **Investigate Now** to start the assessment. Back in the main screen, check the assessment status in the **Latest Investigation** columns.
Refresh	Click **Refresh** to update the screen with the latest information.

At-risk Endpoints

After running impact assessment, perform mitigation tasks on at-risk endpoints.

Column Name	Information
First Observed	Date and time when an artifact's presence is detected on target endpoints
Host Name	Name of the agent endpoint that harbors the matching suspicious object Clicking a value in the **Host Name** column opens a screen that shows a graph of the execution flow of any suspicious activities involving or originating from that endpoint. This lets you analyze the enterprise-wide chain of events involved in a targeted attack. For details, see *Detailed Mindmap on page 19-16*.
User Name	Name of the user logged on to the endpoint
IP Address	IPv4 or IPv6 address of the endpoint

Column Name	Information
Importance	Importance assigned by a Control Manager administrator to the endpoint. For details, see *Working with User or Endpoint Importance on page 4-40*. Take immediate action on important endpoints.
Matching Object(s)	Identifier(s) or component(s) of an attack that indicate what attacks are and how they are established
Action	Options to isolate or restore the connection of an endpoint. For details, see *Endpoint Isolation and Connection Restoration on page xxxix*.

At-risk Endpoints Tasks

The following table lists all options available:

Task	Steps
Export all	Click **Export All** to save the current information to a CSV file. In the new window that opens, monitor the export progress and then click **Download** when the export is complete.
Modify allowed traffic	Click **Modify Allowed Traffic** to make changes to the traffic allowed on all isolated endpoints. In the new window that opens, update the inbound and outbound traffic allowed.
Isolate	On the last column in the table, click **Isolate** to disconnect an endpoint from the network and perform a detailed investigation. For details, see *Endpoint Isolation and Connection Restoration on page xxxix*.
Restore	After an isolated endpoint has been properly investigated and found to be threat-free, click **Restore**. For details, see *Endpoint Isolation and Connection Restoration on page xxxix*.

Detailed Mindmap

Use the **Detailed Mindmap** screen to customize the mindmap.

The Mindmap provides a graphical representation of events and associated objects originating from an investigated suspicious object. This screen has the following parts:

- Mindmap area: The mindmap area shows all the objects matched in the investigations. Objects colored red are suspicious objects or are linked to suspicious objects. Objects are represented by the following icons:

TABLE 19-10. Mind Map View Legend

ICON	TYPE	DESCRIPTION
	File	Files created by the connected process.
	Process	Processes that start other services or processes or create files. Processes usually have an associated user account displayed under the process name and connected to the process.
	IP address and port	IP addresses that the connected process, service, or file attempted to connect to.
	Domain	Domains that the connected process, service, or file attempted to connect to.
	User account	The user account with domain that started the connected process, service, or file.
	Service	Services that start other processes or services or create files. Services usually have an associated user account displayed under the service name and connected to the service.
	Registry	Registry operations implemented by a process, service or module, especially for autorun process.
	Autorun Process	Autorun processes that are started by a registry autorun key.
	Module	Modules loaded by a process or service.
	Signature	System signatures, such as Event, Semaphore, Mutant, etc.
	Inject API	APIs that are used to inject into a process.

ICON	TYPE	DESCRIPTION
	Winnet API	APIs that are used to connect to a network and transfer information.
	URL download file	Files that are downloaded from a URL.
	Unknown	Unknown modules and files.
	Internet API	APIs that are used to connect to the internet via application level, e.g. HTTP/FTP, etc.

Click and drag the mindmap area to navigate around the mindmap. To show a submenu for customizing the mindmap, click an object in the mindmap area.

Use the tooltip on the left to review the details of the selected object. The tooltip pulls these details from the **Object List** screen.

Use the submenu on the right to review and edit the mindmap:

TABLE 19-11. Customization Options for Mindmap

SUBMENU ITEM	DESCRIPTION
Expand	Expands the selected branch to show objects affected further down the chain
Expand All	Expands all the branches in the mindmap to show objects affected further down the chain
Collapse	Hides the expanded branch of the selected object. This option appears only if the object has an expanded branch
Collapse all	Hides all the expanded branches. This option appears only if at least one object has an expanded branch.
Remove from root cause chain	Unmarks the object as suspicious and turns the icon blue
Add to root cause chain	Marks the object as suspicious and turns the icon red

- **Contents** pane: The **Contents** pane lists all the objects appearing in the mindmap. The objects are organized according to the **Root Cause Chain** they belong to. Click an item in the **Contents** pane to center that item on the mindmap area. To increase the space available for the mindmap area, click « to hide the **Contents** pane.
- **Current Screen**: Use the **Current Screen** to determine the location of the object in relation to the area of the mindmap.
  - The gray box represents the full area of the mindmap. This box expands as more branches are added to the initial **Root Cause Chain**.
  - The box with the blue outline represents the current area being viewed. If the screen is resized, this box resizes to match the new screen size.

Pending Agents and Agents with Issues

The **Pending Agents** screen provides the following details:

- **Host Name**: Name of the endpoint running the Deep Discovery Endpoint Sensor agent
- **IP address**: IPv4 or IPv6 address of the endpoint
- **Reason**: These are the possible reasons why an investigation is pending or has issues:
  - Pending
    - Command in progress
    - Command waiting to be deployed
  - With issues
    - Command processing timeout
    - An agent error has occurred
    - Agent is unreachable

Note

Ensure that network connectivity is present and that the agent program is running on the host. Consider restarting the endpoint if the issue persists.

- **Last Reported**: Date and time when the agent last communicated with the Deep Discovery Endpoint Sensor server

For details on troubleshooting offline or unreachable agents, see the Deep Discovery Endpoint Sensor documentation.

Chapter 20

Administering the Database

This chapter presents material administrators will need to manage the Control Manager network.

This chapter contains the following topics:

Understanding the Control Manager Database

Control Manager uses the Microsoft SQL Server database (`db_ControlManager.mdf`) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings.

The Control Manager server establishes the database connection using a System DSN ODBC connection. The Control Manager installation generates this connection as well as the ID and password used to access `db_ControlManager.mdf`. The default ID is sa. Control Manager encrypts the password.

To maximize the SQL server security, configure any SQL account used to manage db_ControlManager with the following minimum permissions:

- dbcreator for the server role
- db_owner for the db_ControlManager role

Logs from managed products contribute to database expansion. Managed products send various log types to Control Manager. Trend Micro measures the database size of the following common log types:

- Virus logs
- Spyware logs
- Web Security logs
- Content Security logs

Refer to the following table to obtain the database size:

TABLE 20-1. Log Count and Database Size

LOG TYPE	LOG COUNT	DATABASE SIZE (MB)
Virus	100,000	156
	500,000	667
	1,000,000	1,191

LOG TYPE	LOG COUNT	DATABASE SIZE (MB)
Spyware	100,000	156
	500,000	770
	1,000,000	1,570
Content security	100,000	121
	500,000	543
	1,000,000	1,263
Web security	100,000	99
	500,000	562
	1,000,000	1,106

The database space required for log storage can be calculated based on the log type and amount. For example:

- An OfficeScan managed product sends 20,000 virus logs and 10,000 web security logs to Control Manager daily.

- Control Manager keeps both log types for 90 days.

The database space required is 1.2 GB for virus logs and 1 GB for web security logs. However, there might be an additional space required for log summary or other features.

Because the Control Manager database runs on a scalable database — SQL Server, the theoretical limit is whatever the hardware can handle. Trend Micro has tested up to 2,000,000 entries. If the database server performance is overworked or pushed to its limit, the web console may experience connection time-outs.

Tip

Trend Micro recommends allocating a significant buffer space for database growth and monitoring the database to help obtain a precise database size measurement.

Understanding the db_ControlManager Tables

To access all tables in the Control Manager database, use a Microsoft Access project (`*.adp` /`*.ade`) or Microsoft SQL Management Studio.

Note

Do not use any of the SQL tools to add, delete, or modify records without instructions from Trend Micro Technical Support.

The following tables make up the Control Manager database:

TABLE 20-2. User/Endpoint Directory Tables

DIRECTORY MANAGEMENT TABLES	DESCRIPTION
tb_WebSecurityLog	Stores Web access violation logs from products
tb_SecurityLog	Stores Content violation logs received from ScanMail and InterScan Messaging products
tb_LogGeneral	Stores Net packet scanning logs from network-based products such as Deep Discovery Inspector
tb_LogDataLossPrevention	Stores DLP related logs sent received from products
tb_AV*Log * corresponds to Virus, Event, StatusEngineInfo, and StatusPatternInfo	Stores product logs Virus table stores virus/malware incident logs detected by products. Other tables store the product status log as well as the pattern and engine version, update and deploy time, and unhandled virus counts.
tb_SpywareLog	Stores malicious spyware information detected by product
tb_PersonalFirewallLog	Stores personal firewall detection log from OfficeScan
tb_LogBehaviorMonitor	Stores malicious system behavior incident detected by OfficeScan
tb_Network_Content_Inspection_Engine_Log	Stores blocked C&C server connection attempt logs from OfficeScan

TABLE 20-3. DIRECTORY MANAGEMENT TABLES

DIRECTORY MANAGEMENT TABLES	DESCRIPTION
CDSM_Entity	Stores the managed product information
CDSM_Agent	Stores Communicator information
CDSM_Registry	Stores registry information
CDSM_UserLog	Stores information as to who, which options, and what time a user accesses the web console; this is useful for auditing web console accesses
CDSM_SystemEventlog	Stores system logs generated by internal processes

TABLE 20-4. SERVER COMMAND CONTROLLER TABLES

SERVER COMMAND CONTROLLER TABLES	DESCRIPTION
tb_TVCSCommandList	Stores managed product commands
tb_TVCSCommandTaskQueue	Stores commands issued to managed products
tb_CommandTracking	Stores command status
tb_CommandItemTracking	Stores detailed command status
tb_ProcessInfo	Stores `MsgReceiver.exe`, `CmdProcessor.exe`, `LogReceiver.exe`, `LogRetriever.exe`, and `UIProcessor.exe` information
tb_LoginUserSessionData	Stores user logon session control
tb_ManualDownload	Stores manual download information
tb_ScheduleDownload	Stores scheduled download information

TABLE 20-5. MANAGED PRODUCT TABLES

MANAGED PRODUCT TABLES	DESCRIPTION
tb_EntityInfo	Stores the managed product information

Managed Product Tables	Description
tb_VirtualEntity	Stores TVCS1.x agent registration information

Table 20-6. Log Tables

Log Tables	Description
tb_TempLog	Stores the raw data of product logs
tb_AV*Log	Stores product log * corresponds to Virus, Event, Status, PEInfo, WebSecurity. These tables store the product status log as well as the pattern and engine version, update and deploy time, and the unhandled virus count.
tb_InValidLog	Stores unidentified log information
• tb_TotalWebSecurityCount • tb_TotalVirusCount • tb_TotalSecurityCount • tb_TopTenSource • tb_TopTenDestination • tb_TopTenVirus	Stores virus summary information for Status Summary and reports
tb_LogPurgePolicy	Stores purge log settings
tb_LogPurgeCounter	Stores purge log counter
• tb_InstanceForVirusOutbreak • tb_InstanceForSpecialVirus • tb_InstanceForVirusOutbreak	Stores log instances used in alert notifications

TABLE 20-7. Notification Tables

NOTIFICATION TABLES	DESCRIPTION
• tb_Alert_NTF_JobList • tb_Event_NTF_JobList	Stores notification queue list
tb_EventNotificationFilter	Stores Event Center configuration
• tb_SendEMailNotification • tb_SendPagerNotification • tb_SendSNMPTrapNotification • tb_SendWindowsNTEventLogNotification	Stores notification method settings
tb_VirusOutBreakPolicy	Stores rules used during virus outbreak
tb_SpecialVirusPolicy	Stores the user specified virus name
• tb_VirusOutbreakAccumulate • tb_SpecialVirusAccumulate	Stores virus counter information
• tb_UGNtfRelation • tb_NtfUserGROUP • tb_GroupAndUserRelation	Stores user and group notification settings

TABLE 20-8. Report Tables

REPORT TABLES	DESCRIPTION
• tb_ReportScheduleTask • tb_ReportTaskQueue	Stores and handles report generation tasks

Report Tables	Description
tb_ReportItemTracking	Stores report template file catalog

Table 20-9. Pattern and Engine Deployment Tables

Pattern and Engine Deployment Tables	Description
• tb_DeploymentPlans • tb_DeploymentPlansTF	Stores deployment plan information
tb_DeploymentPlanTasks	Stores deployment task queue
tb_DeployNowJobList	Stores ongoing deployment plan status
tb_DeployCommandTracking	Stores deployment command tracking information
tb_DeploymentPlanTargets	Stores the managed product information that applied the deploy command

Backing Up db_ControlManager Using osql

If the Control Manager database is corrupted or non-functional, use a backup copy to restore your settings. When using MSDE, use the MSDE command line interface — osql, to generate a database backup.

Procedure

1. From the Control Manager server, click **Start** > **Run**.
2. Type cmd and then click **OK**.
3. On the Command prompt, execute the following commands:

   ```
   osql -U {ID} -P {password} -n -Q "BACKUP DATABASE {Control
   Manager database} TO DISK = '{path and backup name}'"
   ```

   Where:

{ID}: user name of the administrator account used to access the Control Manager database. This is defined during Control Manager setup.

{password}: password used to access the Control Manager database. This is defined during Control Manager setup.

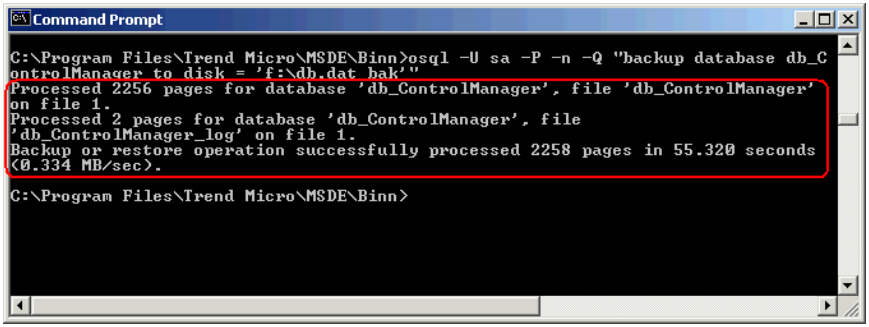
{Control Manager database}: name of the Control Manager database

{path and backup name}: target location and the backup file name

For example:

```
osql -U sa -P -n -Q "BACKUP DATABASE db_ControlManager TO
DISK = 'f:\db.dat_bak'"
```

A successful database backup produces a result similar to the following:



If the backup file `db.dat_bak` already exists, the command `osql` inserts new records into the existing file to back up new information.

Note

Trend Micro recommends backing up the Control Manager database regularly. Always back up when you are about to modify the Control Manager database (for example, installing a managed product).

Restoring Backup db_ControlManager Using osql

Use the MSDE command line interface that comes with your version of MSDE, `<root>:\Program Files\Trend Micro\MSDE\osql`, to restore backup database.

Procedure

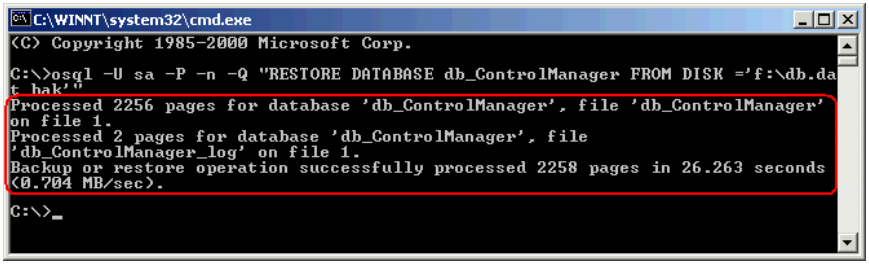
1. Stop Control Manager.
2. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.
3. Right-click **<Control Manager service>**, and then click **Stop**.
4. Click **Start** > **Run**.
5. Type cmd and then click **OK**.
6. On the Command prompt, execute the following commands:

   ```
   osql -U {ID} -P {password} -n -Q "RESTORE DATABASE {Control
   Manager database} FROM DISK = '{path and backup name}'"
   ```

   For example:

   ```
   osql -U sa -P -n -Q "RESTORE DATABASE db_ControlManager
   FROM DISK = 'f:\db.dat_bak'"
   ```

   A successful database restoration produces a result similar to the following:



7. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.

8. Right-click **<Control Manager service>**, and then click **Restart**.
9. Start Control Manager.

   For more information on how to use osql, refer to the MSDN library.

Backing Up db_ControlManager Using SQL Server Management Studio

When using SQL Server, use the SQL Server Management Studio to back up the Control Manager database.

Note

Trend Micro recommends regular backups of the Control Manager database. Always back up when you are about to modify the Control Manager database (for example, adding or installing a managed product).

Procedure

1. From the Control Manager server, click **Start** > **All Programs** > **Microsoft SQL Server <version>** > **SQL Server Management Studio**.

   `<version>` is the version of SQL Server Management Studio.

2. On the menu bar, click **View** > **Object Explorer**. In the **Object Explorer** panel, double-click <Host\Instance Name>, then double-click **Databases**.

   <Host\Instance Name> is the SQL server host name and the SQL instance name.

3. Right-click **db_ControlManager** and then click **Tasks** > **Back up**.
4. Under **Backup set**, provide the **name** and **description**.
5. Under **Source** > **Backup Type**, select **Full**.
6. Under **Destination**, click **Add** to specify the backup file destination.

7. Click **OK** when the message "The backup operation has been completed successfully." appears.

Restoring Backup db_ControlManager Using SQL Server Management Studio

Use the SQL Server Management Studio to restore the backup Control Manager database.

Procedure

1. Stop Control Manager.
2. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.
3. Right-click **<Control Manager service>**, and then click **Stop**.
4. Click **Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio** to access the SQL Server Management Studio.
5. On the console, click **Microsoft SQL Server 2005** > **SQL server group** > **{SQL server}** > **Databases**.

   {SQL server} is the SQL Server host name.
6. Right-click **db_ControlManager** > **All tasks** > **Restore Database…**.
7. On the **Restore database** screen, select the database to restore.
8. Click **OK** to start the restoration process.
9. Click **OK** when the message "Restore of database '{Control Manager database"}' completed successfully." appears.
10. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.
11. Right-click **<Control Manager service>**, and then click **Restart**.

12. Start Control Manager.

Shrinking db_ControlManager_Log.LDF Using SQL Commands

Procedure

1. Backup the Control Manager database using the SQL Server Management Studio.
2. From the available databases, select the `db_ControlManager` database.
3. Execute the following SQL Script:

```
DBCC shrinkfile('db_ControlManager_log', 10)
```

4. Verify the size of `db_ControlManager_Log.LDF` is less than 10MB.

   If `db_ControlManager_Log.LDF` was not reduced in size, use the following SQL command to identify the Database Recovery Mode used:

```
SELECT name as DatabaseName, DATABASEPROPERTYEX(name, 'Recovery') as
```

   If the Database Recovery Mode is `FULL`, execute following SQL script:

```
-- Truncate the log by changing the database recovery model to SIMPLE
ALTER DATABASE db_ControlManager
SET RECOVERY SIMPLE;
GO
-- Shrink the truncated log file to 10 MB.
DBCC SHRINKFILE (db_ControlManager_Log, 10);
GO
-- Reset the database recovery model.
ALTER DATABASE db_ControlManager
SET RECOVERY FULL;
GO
```

For detailed information on shrinking SQL databases and SQL commands, refer to the *Microsoft SQL Server Administration* documents.

Shrinking db_ControlManager_log.ldf Using SQL Server Management Studio

The transaction log file for the Control Manager database is ...\data \db_ControlManager_log.LDF. SQL Server generates the transaction log as part of its normal operation.

db_ControlManager_log.LDF contains all managed product transactions using db_ControlManager.mdf.

By default, the transaction log file has no file size limit on the SQL Server configuration. This leads to filling up the available disk space.

Shrinking the db_ControlManager_log.ldf File Size on Microsoft SQL Server 2008/2005 SP 3/2012

Procedure

1. Back up the Control Manager database using the SQL Server Management Studio.
2. Purge the transaction log.
3. On the SQL Server, click **Programs** > **Microsoft SQL Server 2008/2005** > **SQL Server Management Studio** to open the SQL Server Management Studio.
4. Select the SQL server and specify the Windows authentication if prompted.
5. Right-click **db_ControlManager** and select **Properties**.

   The **Properties** dialog box appears.
6. Click **Options**.

   The **Options** work area appears.

7. Select **Simple** from the **Recovery model:** list.
8. Click **OK**.
9. Check the `db_ControlManager_log.ldf` file size. It should be 10MB.

Shrinking the db_ControlManager_log.ldf File Size on Microsoft SQL Server 2005

Procedure

1. Back up the Control Manager database using the SQL Server Management Studio.
2. Purge the transaction log.
3. On the SQL Server, click **Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio** to open the SQL Server Management Studio.
4. Select the SQL server and specify the Windows authentication if prompted.
5. On the list, select the **db_ControlManager** database.
6. Copy and paste the following SQL script:

```
DBCC shrinkDatabase(db_ControlManager)

BACKUP LOG db_ControlManager WITH TRUNCATE_ONLY DBCC
SHRINKFILE(db_ControlManager_Log, 10)
```

> **Note**
>
> On the `SHRINKFILE(db_ControlManager_Log, 10)` function, the parameter 10 will be the resulting file size of `db_ControlManager_Log.ldf` in megabytes (MB).

7. Click **Execute** to run the SQL script.
8. Check the `db_ControlManager_log.ldf` file size. It should be 10MB.

Part IV

Services and Tools

Chapter 21

Using Trend Micro Services

This chapter provides details about the various services available for Control Manager.

This chapter contains the following topics:

Understanding Trend Micro Services

Trend Micro recognized that a new approach to antivirus management was needed to significantly reduce the threat and costs of virus attacks. After considerable research and testing, Trend Micro has redefined virus protection (moving beyond reactive, point products to a proactive, centralized protection system that enables a rapid, methodical response to any attack on any system) from Internet gateways to PCs, file servers, and email servers.

The Trend Micro integrated approach to virus protection begins when an administrator sends a virus sample to TrendLabs where a targeted prevention policy (a pre-pattern file recommendation) is created to contain the outbreak and prevent spreading. When Control Manager retrieves this information, system administrators can use Outbreak Prevention Services to quickly understand the scope of the attack and take effective interim steps against it without jeopardizing business productivity by having to shut down a port. They can also quickly disseminate Outbreak Prevention Policy recommendations to other system administrators within the enterprise who may be hit with the same problem.

This proactive response—the ability to incorporate antivirus knowledge throughout the network and have real-time visibility into all virus-related events as they happen—can only be accomplished with central management. The rapid identification services and delivery systems shorten the time to containment, thereby limiting the spread of the virus. This process minimizes the effect of the virus on the productivity of the enterprise, as well as dramatically reducing the costs of cleanup.

Understanding Enterprise Protection Strategy

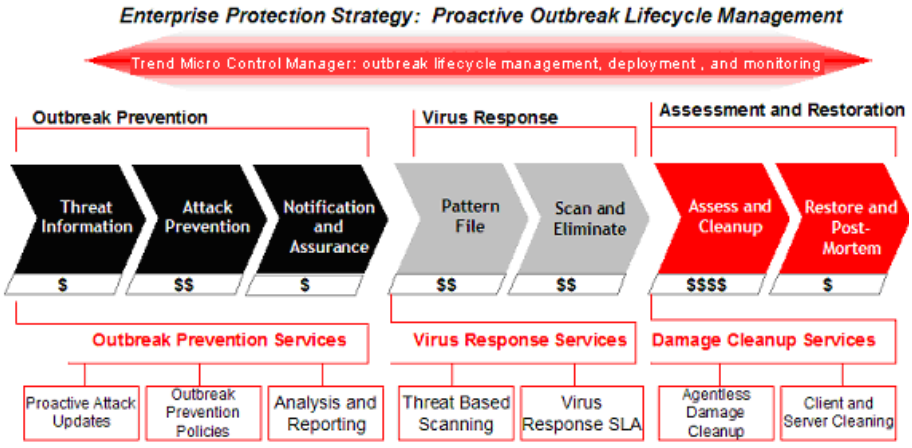


FIGURE 21-1. Enterprise Protection Strategy

Enterprise Protection Strategy (EPS) arms businesses with industry-specific services and support to wage war against mixed-threat attacks with confidence.

- Proactive services combat viruses by containing infiltration and cleaning potential attackers hiding in systems
- Industry's only Virus Response Service Level Agreement guarantees virus detection
- EPS architecture exports Trend Micro's 'think-tank' of antivirus knowledge and support to vulnerable points on the network

EPS establishes a 'command center' to help identify and defend all vulnerabilities within the enterprise.

- Enterprise-wide policy coordination and reporting
- Heterogeneous platform support

EPS provides a battle plan during an attack while minimizing casualties and damage.

- Virus Outbreak Lifecycle approach– industry unique and based on real customer experience
- Enterprise-wide coordination identifies network vulnerabilities and helps enable customers to proactively attack outbreaks
- Focus on the critical stages before and after pattern file deployment manages explosive costs and system damage

Highlighting the Value of EPS

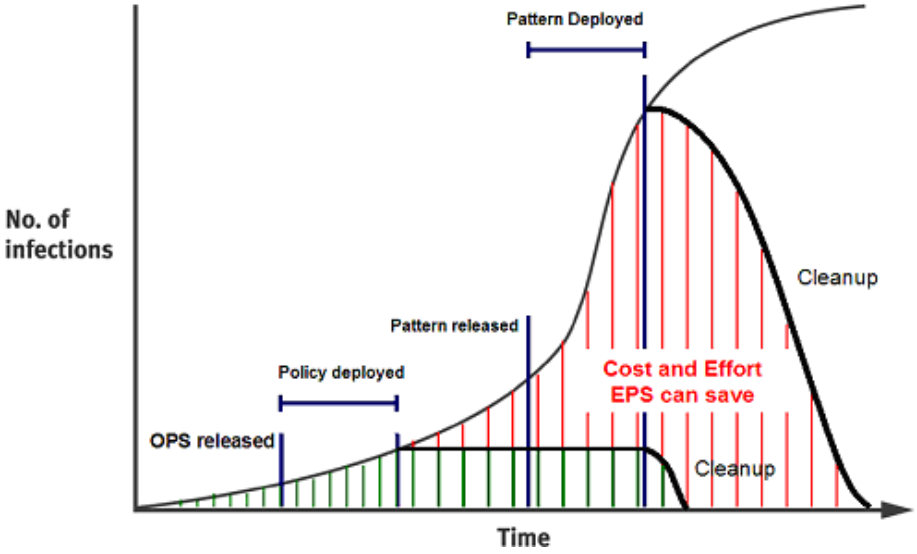


FIGURE 21-2. Cost vs. Effort

The graph demonstrates that putting protection in place as quickly as possible and ridding the network of post-attack vulnerabilities can minimize the devastating effects of outbreaks over time.

By using EPS and Outbreak Prevention Services, enterprises can minimize their risk and dramatically lower costs. By deploying policies early in the life cycle and before pattern file generation, an organization can dramatically reduce the cost and effort (area under the curve), in addition to increasing the overall level of protection.

Trend Micro's expertise, architecture, and services provide a strong return on investment, improve overall protection, and increase the productivity of enterprise networks.

Understanding Outbreak Prevention Services

FIGURE 21-3. Outbreak Prevention Services

The Outbreak Prevention phase refers to the critical period when managed products have identified a virus outbreak, but before a pattern file has become available. During this crucial time, system administrators must endure a chaotic, time-consuming process of communication—often to global and decentralized groups within their organizations.

Outbreak Prevention Services deliver notification of new threats and continuous and comprehensive updates on system status as an attack progresses. The timely delivery of detailed virus data coupled with pre-defined, threat-specific action and scanning policies delivered immediately after a new threat identification allows enterprises to quickly contain viruses and prevent them from spreading.

Additionally, by centrally deploying and managing policy recommendations, Outbreak Prevention Services helps eliminate the potential for miscommunication, applies policies, and deploys critical attack information as it is happening.

By providing automatic or manual download and deployment of policies through Trend Micro Control Manager, Outbreak Prevention Services import knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro's global security research and support network.

This subscription-based service requires minimal up-front investment and provides enterprise-wide coordination and outbreak management through Trend Micro products which reside across critical points on the network including the Internet gateway, mail server, file server, caching server, client, remote and broadband user.

Benefits of Outbreak Prevention Services

Besides quickening the enterprise's response time, Outbreak Prevention Services can deliver significant operational protection and cost benefits.

TABLE 21-1. Benefits of OPS

BENEFIT	REASONS
Proactive Protection Against Mixed Threat Attacks	• Contains outbreaks without stopping business productivity (that is, shut down ports) • Reduces the chaos associated with defining the threat and behavior • Automatic policy creates a 24x7, no-touch defense system
Expertise and Knowledge	• Recommendations from the experts– policy formulation • Knowledge base of policies for prior viruses
Consistency, Reduced Coordination, Cost Reduction	• Consistent application of policy • Removes logistical challenges of notifying critical parties
Policy and Attack Correlation	• Assurance and reporting = Enterprise-wide visibility and coordination

Activating Outbreak Prevention Services

Before you begin

Important

If you have subscribed to Trend Micro Smart Protection Complete, Outbreak Prevention Services is not supported in Customer Licensing Portal. Please refer to the Smart Protection Complete documentation for information about alternative solutions.

After activating Outbreak Prevention Services, administrators still need to start Outbreak Prevention Mode to protect the network during a virus outbreak.

Procedure

1. Navigate to **Administration** > **License Management** > **Control Manager**.

   The **License Information** screen appears.

2. On the working area under **Outbreak Prevention Services License Information**, click the **Activate the product** link.

3. Do the following:

   - If you do not have an Activation Code, click the **Register online** link and follow the instructions on the Online Registration web site to obtain an Activation Code
   - If you have an Activation Code, in the **New** box, type your Activation Code

4. Click **Activate**.

Viewing Outbreak Prevention Services Status

View the **Outbreak Prevention Services** screen to instantly know the state of the following service status items:

TABLE 21-2. OPS Status

ITEM	DESCRIPTION	STATE
Scheduled policy download	Provides information about whether Control Manager automatically downloads Outbreak Prevention Policies according to a specified schedule.	On/Off
Automatic Outbreak Prevention Mode for red alert	Provides information about whether Control Manager will automatically trigger Outbreak Prevention Mode for red alert viruses.	On/Off
Automatic Outbreak Prevention Mode for yellow alert	Provides information about whether Control Manager will automatically trigger Outbreak Prevention Mode for yellow alert viruses.	On/Off

In addition, this screen also provides an easy way to view the Control Manager components and the version that are currently in use.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Policies**.

Note

This page automatically refreshes to make sure the top threat and status information is current.

Preventing Virus Outbreaks and Understanding Outbreak Prevention Mode

Even before receiving the appropriate pattern file from Trend Micro, an enterprise can deflect, isolate and stem attacks with the help of attack-specific information and Outbreak Prevention Policies from Trend Micro Outbreak Prevention Services. With Outbreak Prevention Services, you can centrally deploy policy recommendations to minimize coordination efforts and help ensure a consistent application of policies throughout the network. Policy recommendations delivered through Outbreak Prevention Services help system administrators respond quickly against new viruses to contain outbreaks, minimize system damage and prevent undue downtime.

Using deployment plans you can restrict the application of Outbreak settings to specific segments of the network if you have divided your network segment into different deployment plans. This approach can prove very useful for large networks composed of several sites. Administrators can apply the settings to only those areas actually affected by the outbreak.

Outbreak Prevention Mode includes the following elements:

- Downloads Outbreak Prevention Policies — a collection of recommended software settings for handling the virus outbreak
- Displays the product settings that will be set, thereby allowing you to modify the settings according to the demands of your network

  Outbreak Prevention Services provide recommendations for managed products that must be set.

- Blocks/deflects malicious code from entering or spreading throughout the network
- Customizes Control Manager's notification functions for the outbreak
- Real-time reporting on policy deployment and status
- Ability to approve and deploy policy manually or automatically
- Allows you to set a special, abbreviated, update-download schedule that is only active for the duration of the policy

  This enables you to automatically update new virus patterns as soon as they become available.
- Detailed information on threats as soon as they are characterized

Understanding Outbreak Prevention Policies

Apply Outbreak Prevention Policies, collections of product settings, to your managed products using Outbreak Prevention Services. Trend Micro creates these settings in response to virus outbreaks, and provides them to Trend Micro users as part of the Outbreak Prevention Services.

These policies serve as the key to protecting a network during a virus outbreak. They protect critical points on the network, including the Internet gateway, mail server, file server, caching server, client, remote and broadband user. For example, viruses that only propagate through email will only have policies with settings for messaging systems.

The following diagram illustrates how Trend Micro can deploy policies at all layers to protect critical points during a virus outbreak.

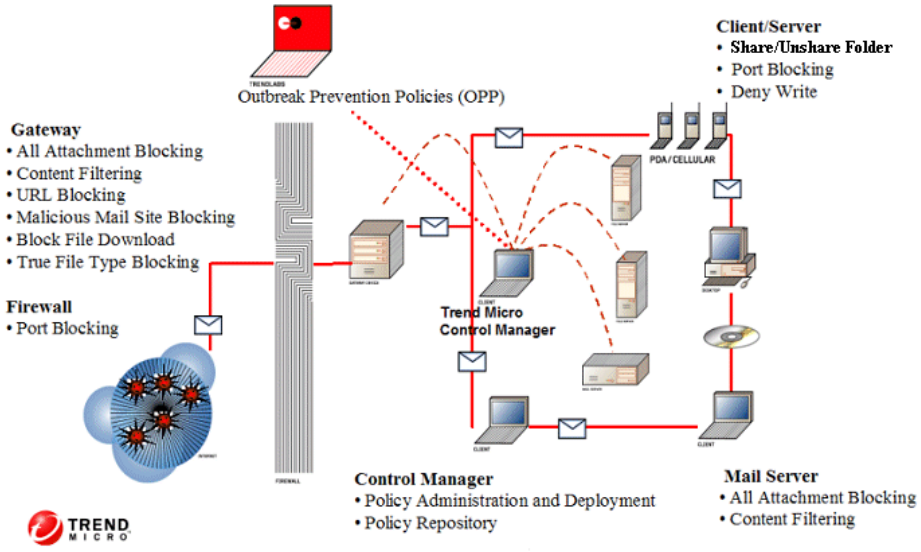


FIGURE 21-4. Deploying OPP

Accessing the Outbreak Prevention Services Settings Screen

- Navigate to **Administration** > **Outbreak Prevention Services** > **Settings**. The **Outbreak Prevention Services Settings** screen appears.

  This page automatically refreshes to make sure the top threat and status information is current.

Updating Outbreak Prevention Policies

It is important to use the latest Outbreak Prevention Policies to protect your network during virus outbreaks. Update Outbreak Prevention Policies both manually or set a scheduled update.

Note

After installing Control Manager for the first time, Trend Micro strongly recommends you perform an Update Now to update your policies immediately. For subsequent updates, use the Scheduled Update function.

Updating Outbreak Prevention Policies Manually

To avoid additional maintenance tasks, schedule Control Manager to automatically check for and download the latest Outbreak Prevention Policies.

Note

The **Outbreak Prevention Services** screen automatically refreshes to make sure the top threat and status information is current.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Policies**.
2. On the working area under **Service Status**, click **Update Now** to download the latest Outbreak Prevention Policies.
3. Click **OK** after downloading the Outbreak Prevention Policies.

Configuring Automatic Updates for Outbreak Prevention Policies

Procedure

1. Navigate to the **Administration** > **Outbreak Prevention Services** > **Settings**.
2. Under Scheduled policy download settings, select **Enable scheduled policy update**.
3. From the Download frequency list, choose the number of minutes for Control Manager to check for updated Outbreak Prevention Policies.
4. Under Download source, select the source that contains the latest Outbreak Prevention Policies. Trend Micro ActiveUpdate server is the default option. If you choose another Internet source, type the location in **Other update source**.

5. Click **Save**.
6. Click **OK**.

Starting Outbreak Prevention Mode

During a virus outbreak, start Outbreak Prevention Mode to deploy attack-specific Outbreak Prevention Policies and minimize the chance of your network becoming infected. Start Outbreak Prevention Mode to counter a single, specific threat.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Policies**.

   The **Outbreak Prevention Services** screen appears.

   This screen automatically refreshes to make sure the top threat and status information is current.

2. On the working area under **Service Status**, click **Update Now** to download the latest Outbreak Prevention Policies (this is optional if you have already enabled Scheduled Update and are using the latest Outbreak Prevention Policies).
3. Click **OK** after downloading the Outbreak Prevention Policies.
4. Under **Top Threats Around the World**, click the name of the virus that currently presents a threat to your network. By default, Control Manager lists the newest threat first, and the remaining threats in alphabetic order. Each Outbreak Prevention Policy is designed to counter a specific threat.
5. Click **Start Outbreak Prevention Mode**.
6. Under **Outbreak Prevention Policy**, in the Policy in effect for list, choose the number of days that Control Manager continues in Outbreak Prevention Mode.
7. From the Deployment plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products.
8. Under **Outbreak Prevention Policy Details**, select **Do not block permitted port numbers specified in the Outbreak Prevention settings** to ensure ports defined as exceptions are not blocked.

9. Configure managed product settings or click **Recommended Settings**.

10. Click **Activate**.

11. Click **OK**.

    Outbreak Prevention Mode has started and the () icon appears in the management console header.

Editing an Outbreak Prevention Policy

After you have started Outbreak Prevention Mode, modify Outbreak Prevention Policies to suit your network needs. For example, you could:

- Change the duration of the length of Outbreak Prevention Mode
- Choose a different deployment plan
- Permit specified port numbers
- Configure registered managed product settings

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Policies**.

   The **Outbreak Prevention Services** screen appears.

   This page automatically refreshes to make sure the top threat and status information is current.

2. On the working area, click **Edit Policy**.

3. Under Outbreak Prevention Policy, in the Policy in effect for list, choose the number of days that Control Manager continues in Outbreak Prevention Mode.

4. From the Deployment Plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products (to view/edit or add deployment plans, move the cursor over **Updates**, and then click **Deployment Plan**).

5. Under Outbreak Prevention Policy Details, select **Do not block permitted port numbers specified in the Outbreak Prevention settings** to ensure ports defined as exceptions are not blocked.

6. Configure managed product settings or click **Recommended Settings**.

> **Tip**
>
> When you click **Recommended Settings**, the TrendLabs recommended settings are applied and any user-defined settings are removed. If necessary, based on the latest information, these recommendations are updated with each Outbreak Prevention Policy release. Trend Micro recommends you apply the recommended settings.

7. Click **Activate**.

Setting Automatic Outbreak Prevention Mode

Outbreaks can occur anytime. Automatic Outbreak Prevention can automatically deploy Outbreak Prevention Policies for red or yellow alert viruses to managed products and send notifications.

TABLE 21-3. Virus Alert Criteria

VIRUS ALERT	DESCRIPTION
Criteria for Red Alert Viruses	Several infection reports from each business unit reporting rapidly spreading malware, where gateways and email message servers may need to be patched. The industry's first 45-minute Red Alert solution process is started: An official pattern release (OPR) is deployed with notification of its availability, any other relevant notifications are sent out, and fix tools and information regarding vulnerabilities are posted on the download pages.

VIRUS ALERT	DESCRIPTION
Criteria for Yellow Alert Viruses	Infection reports are received from several business units as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download. In case of an email-spreading malware, content filtering rules, called Outbreak Prevention Policies (OPP), are sent out to automatically block related attachments on servers equipped with the product functionality.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Settings**.

   The **Outbreak Prevention Services Settings** screen appears.

   This page automatically refreshes to make sure the top threat and status information is current.

2. Click the **Automatic Outbreak Prevention Mode** tab.

3. Do the following:

   - To set Automatic Outbreak Prevention Mode for red alert viruses, under Red Alert Viruses, select **Enable automatic outbreak prevention**.

   - To set Automatic Outbreak Prevention Mode for yellow alert viruses, under Yellow Alert Viruses, select **Enable automatic outbreak prevention**.

4. From the Prevention duration list, choose the number of days that Outbreak Prevention Mode is active.

5. From the Deployment plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products.

6. Do the following:

   - Under Excluded products, select managed products that will not receive Outbreak Prevention Policies.

WARNING!

These products will not benefit from Outbreak Prevention Services and will have a greater chance of becoming infected during outbreaks.

- Under **Permitted ports**, specify ports that Control Manager will keep open during an outbreak.
- Select **Stop OPP automatically after the prevention duration expires** to automatically stop OPP.

7. Click **Save**.

Configuring Outbreak Prevention Mode Download Settings

Configure how often Control Manager checks for updated Outbreak Prevention Policies during Outbreak Prevention Mode. In addition, you can also choose which deployment plan to use to deploy the updated Outbreak Prevention Policies.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Settings**.

   The **Outbreak Prevention Settings** screen appears.

   This page automatically refreshes to make sure the top threat and status information is current.

2. Under Outbreak Prevention Mode download settings do the following:
   - In the Download frequency list, choose how often Control Manager checks for updated Outbreak Prevention Policies.
   - In the Components to deploy list, choose a deployment plan to use to deploy downloaded components. For more information about deployment plans, see *Understanding Deployment Plans on page 7-23*.
   - To deploy the virus pattern file only, select **Exclude Scan Engine Deployment**.

3. Click **Save**.

Stopping Outbreak Prevention Mode

Manually stop Outbreak Prevention Mode before the policy duration has been exceeded.

When Control Manager is in Outbreak Prevention Mode, the () icon appears in the web console.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **Policies**.

   The **Outbreak Prevention Services** screen appears.

   This page automatically refreshes to make sure the top threat and status information is current.

2. Click **Stop Outbreak Prevention Mode**.

3. Click **OK**.

Viewing Outbreak Prevention Mode History

This Outbreak Prevention Services feature allows you to view applied Outbreak Prevention Policies. The **History** screen shows the following information:

TABLE 21-4. History Screen Information

HEADING	DESCRIPTION
#	Indicates the order in which the tasks were performed; a lower the number indicates a newer task
Virus	The virus or malware that caused the outbreak
Started by	The user name of the Control Manager user that applied the policy

HEADING	DESCRIPTION
Outbreak Prevention Mode Duration	Indicates how long Outbreak Prevention Mode was active. The starting time appears on the left, the completion (or abort) time is on the right.
Status	Indicates the results of the task. To view the result or status of a task, click View beside the task.
Report	The number of detected viruses by OPP during the OPS. If no viruses are detected, no data appears under Report.

Procedure

1. Navigate to **Administration** > **Outbreak Prevention Services** > **History**.

   The **History** screen appears.

2. To view the status of a specific Outbreak Prevention Policy, click **View** in the same row.

   The status screen displays the number of viruses detected by your antivirus products.

Using Outbreak Prevention Mode

This tutorial guides you through starting Outbreak Prevention Mode, and is divided into the following topics:

Step 1: Identifying the Source of the Outbreak

Trend Micro provides registered customers with services that help identify the threats that threaten their systems. The following warn you of potential or emerging virus or malware outbreaks:

TABLE 21-5. Identifying the Source of the Outbreak

ALERT METHODS	DESCRIPTION
Scheduled Outbreak Prevention Policy downloads	Control Manager can inform you if it downloads Outbreak Prevention Policies that correspond to an ongoing virus outbreak. To receive notification about this event, enable Active Outbreak Prevention Policy received at the Event Center. Upon receiving the notification, start Outbreak Prevention Mode immediately.
Your Technical Account Manager (TAM)	Depending on the support arrangement you have with Trend Micro, your Technical Account Manager will inform you of any outbreak alerts. Upon receipt of the warning, update your outbreak prevention policies.
Trend Micro virus bulletins	You can subscribe to this service at the Trend Micro website.
Special Virus alert	This Control Manager feature, configured at the Event Center, warns you when a Trend Micro product detects an outbreak-causing virus on your network. This allows you to immediately take precautionary measures, such as warning your company's employees about certain kinds of email messages.

Step 2: Evaluating Existing Policies

Upon receiving a virus outbreak warning, assess your system to determine if it is equipped to deal with the threat. On the **Outbreak Prevention Services** screen, examine the Outbreak Prevention Policies currently on your Control Manager server to see if existing policies cover the virus causing the outbreak.

Tip

Simplify this evaluation process by enabling Control Manager features that inform you about the availability of outbreak prevention policies that correspond to ongoing virus outbreaks.

For Outbreak Prevention Services alerts, see *Understanding Event Center on page 10-2*

For creating scheduled policy downloads, see *Updating Outbreak Prevention Policies on page 21-10*

What best describes the capabilities of your Control Manager server?

- The virus is covered by the Outbreak Prevention Policies currently on Control Manager
- The virus is not covered by the Outbreak Prevention Policies currently on Control Manager

Virus Covered by Existing Policies

Control Manager can handle the outbreak. Start Outbreak Prevention Mode and apply the Outbreak Prevention Policy that corresponds to the virus outbreak.

Virus Not Covered by Existing Policies

If existing Outbreak Prevention Policies do not cover the virus outbreak, you must obtain a new policy from Trend Micro.

Trend Micro recommends manually updating outdated Outbreak Prevention Policies.

Step 3: Starting Outbreak Prevention Mode

Start Outbreak Prevention Mode to apply the policy that corresponds to the virus outbreak. After Control Manager has entered Outbreak Prevention Mode, you can evaluate product-setting recommendations from Trend Micro and modify them to suit your network. Policies implement product settings that block known virus-entry points.

When TrendLabs deploys an Outbreak Prevention Policy, it is very likely that they are still testing the appropriate virus pattern. The Outbreak Prevention Policy settings,

therefore allow you to protect your network during the critical period before TrendLabs releases a new pattern.

Before you start Outbreak Prevention Mode, set outbreak recipients and the notification method in the Event Center.

Considerations for Starting Outbreak Prevention

To start outbreak prevention, answer the following questions:

- How long do you want this policy to be active?

  Specify how long the policy will remain active at the Policy in effect for list. The duration starts from the time you start Outbreak Prevention Mode. By default, Outbreak Prevention Policies remain active for two days.

  Note

  If you edit the policy, Control Manager resets and starts the duration on the day you applied the changes.

- How to deploy the policy?

  Select an appropriate Deployment Plan for this stage. The plan determines which segments of the Product Directory will receive the settings contained in the policy.

  Note

  If none of the existing Deployment Plans suits your needs, create a new plan. See *Understanding Deployment Plans on page 7-23*.

- Which entry points do you want this policy to block?

  The products involved in this stage are:

  - InterScan Messaging Security Suite for Windows
  - InterScan Messaging Security Suite for UNIX/IMSA/Solaris
  - InterScan Web Security Suite for Windows/Solaris/Linux/Appliance
  - InterScan Gateway Security Appliance

- InterScan VirusWall for Windows/Linux
- Network VirusWall
- PortalProtect
- ScanMail for Microsoft Exchange
- ScanMail for Lotus Notes/ScanMail for Domino
- IM Security for Microsoft Live Communications Server
- ServerProtect for Windows
- ServerProtect for Linux
- OfficeScan Corporate Edition
- Firewall Management-NetScreen

If settings for a particular product are included in the policy, then Control Manager automatically selects the product's check box.

Note

If any of the above products do not belong to your Control Manager network, Control Manager ignores the settings for those products.

Evaluating or Modifying Any of the Product Settings

Procedure

1. Click the product's link or the + icon to view its settings.
2. To view the settings for all the products, click **Expand All**. Trend Micro recommendations appear in non-editable fields on the right side of the screen.
3. Modify the settings to suit your needs.

Step 4: Follow-Up Procedures

After completing the Outbreak Prevention tutorial, monitor the progress of the policy using the Outbreak Prevention Mode history.

Tip

Manually stop Outbreak Prevention Mode after the policy duration expires. Otherwise, the Outbreak Prevention Mode Scheduled Update feature cannot automatically apply new Outbreak Prevention Policies.

Chapter 22

Using Control Manager Tools

Control Manager provides a number of tools to help you with specific configuration tasks. Control Manager houses most tools at the following location:

```
<root>:\Control Manager\WebUI\download\tools\
```

Control Manager 6.0 Service Pack 3 supports the following tools:

- *Using Agent Migration Tool (AgentMigrateTool.exe) on page 22-7*: To migrate Control Manager agents to a Control Manager 6.0 Service Pack 3 server
- *Using the Control Manager MIB File on page 22-7*: Use the Control Manager MIB file with an application (for example, HP OpenView) that supports SNMP protocol
- *Using the NVW Enforcer SNMPv2 MIB File on page 22-8*: Use the NVW Enforcer MIB file with an application (for example, HP OpenView) that supports SNMP protocol
- *Using the DBConfig Tool on page 22-8*: Use the DBConfig to change the user account, password, and the database name for the Control Manager database

Using Syslog Forwarder

Control Manager Syslog Forwarder periodically sends the following logs to Syslog servers:

- Behavior Monitoring
- Data Loss Prevention
- Device Access Control
- Engine update status
- Pattern update status

Procedure

1. Go to the Control Manager root folder.

   `C:\Program Files\Trend Micro\Control Manager` or

   `C:\Program Files (x86)\Trend Micro\Control Manager`

2. Launch `DataExportTool.exe`.
3. Configure log receiver settings.
   - **Severity**: Severity type (default: Notice)
   - **IP address**: Syslog server address
   - **Port**: Syslog server port (default: 514)
   - **Facility**: Syslog facility (default: Local0)
4. Configure log forwarding settings.
   - **Frequency**: How often Syslog Forwarder will query Control Manager for logs (default: 12 hours)
   - **Logs to forward**: Log types (default: no selection)
   - **Format**: CEF or Control Manager format

FORMAT	DETAILS
CEF (for ArcSight Server)	• Column names follow the CEF standard. • The corresponding Control Manager format keys are defined in the file `DataExportTool.exe.config` found in the Control Manager root folder. • Column values are the original values queried from the Control Manager database. Sample data: `03-02-2015 16:54:15 Local7.Critical 10.1.1.1 March 02 12:54:46 WIN-VM1.trend.com CEF:0|Trend Micro| Control Manager|6.0|700107| Device Access Control Logs|2| rt=Mar 02 2015 12:53:51 GMT+00:00 cs1Label=Product_Entity/Endpoint cs1=OSCE1 shost=tw-a dvchost=ComputerDAC cn1Label=Product cn1=1 sproc=fake SLF_ProcessName fname=DAC_fileName cn2Label=Device_Type cn2=1 cn3Label=Permission cn3=1`
Control Manager format	• Column values are mapped to the original values queried from the Control Manager database. • Mapping rules are defined by Control Manager. • Spaces in column names are replaced by underscores (_). Sample data: `March 01 07:41:55 TMCM:700107 Generated="2015-03-01T19:41:41.347" Product_Entity/Endpoint="OSCE1" Endpoint="tw-a" Managing_Server="fake SLF_ComputerName" Product="ScanMail for ccMail" Target_Process="fake SLF_ProcessName" File_Name="fake SLF_FileName" Device_Type="Non-storage USB" Permission="Read and execute"`

5. Click **Start**.
6. Check the **Last log forwarded** data to see the progress.

When the syslog forwarding task is complete, the **Start** button is available again.

If the task is not complete and you want to pause:

a. a. Click **Pause** or close the tool.

b. b. To resume, click **Resume**. If the tool was closed, open the tool, select log types, and click **Resume**.

Debug Logging for Syslog Forwarder

Enable debug logging to collect logs that may be useful when troubleshooting Syslog Forwarder issues.

Procedure

1. Go to the Control Manager root folder.

   `C:\Program Files\Trend Micro\Control Manager` or

   `C:\Program Files (x86)\Trend Micro\Control Manager`

2. Open `DataExportTool.exe.config` using a text editor.

3. Search for the `log4net debug` string and then set the value to `"true"`.

   For example: `set log4net debug="true"`

4. Search for the `priority value` string and then set the value to `"debug"`.

   For example: `priority value="debug"`

5. Save and close the file.

   Debug logs are available at:

   `<Control Manager root folder>\DebugLog \TMCM_DataExportTool.log`

Retrieving Logs with a Particular Engine Update Status

By default, Control Manager Syslog Forwarder retrieves logs with the following engine update status:

- Up-to-date
- Out-of-date

You can configure Syslog Forwarder to only retrieve a particular status.

Procedure

1. Go to the Control Manager root folder.

   `C:\Program Files\Trend Micro\Control Manager` or

   `C:\Program Files (x86)\Trend Micro\Control Manager`

2. Open `DataSource_Localhost.ini` using a text editor.

3. Go to the `[engine_updated_status]` section, search for the `ComponentStatus` string and then set the value to `1` or `2`.

   1 = Up-to-date

   2 = Out-of-date

   For example:

   ```
   [engine_updated_status]

   event_id=800102

   enable=0

   ComponentStatus=1
   ```

4. Save and close the file.

Retrieving Logs with a Particular Pattern Update Status

By default, Control Manager Syslog Forwarder retrieves logs with the following pattern update status:

- Up-to-date
- 1, 2, 3, 4, 5, and 6 versions old

You can configure Syslog Forwarder to only retrieve a particular status.

Procedure

1. Go to the Control Manager root folder.

   `C:\Program Files\Trend Micro\Control Manager` or

   `C:\Program Files (x86)\Trend Micro\Control Manager`

2. Open `DataSource_Localhost.ini` using a text editor.

3. Go to the `[pattern_updated_status]` section, search for the `ComponentStatus` string and then set one or several values.

   1 = Up-to-date

   2 = 1 version old

   3 = 2 versions old

   4 = 3 versions old

   5 = 4 versions old

   6 = 5 versions old

   7 = 6 versions old

   For example:

   ```
   [pattern_updated_status]

   event_id=800101
   ```

```
enable=0

ComponentStatus=1,2,3,4
```

4. Save and close the file.

Using Agent Migration Tool (AgentMigrateTool.exe)

The Agent Migration tool provided in Control Manager 6.0 Service Pack 3 Standard or Advanced Edition migrates agents administered by a Control Manager 5.5 or 5.0 server .

Note

The Agent Migration Tool supports Windows-based and Linux-based agent migration.

In addition, use an account with sufficient permission to access the source server.

Procedure

1. Log on to the destination server.
2. Run `AgentMigrateTool.exe` from the following location: `<root>\Program Files\Trend Micro\Control Manager\`

Using the Control Manager MIB File

Download and use the Control Manager MIB file with an application (for example, HP™ OpenView) that supports SNMP protocol.

Procedure

1. Navigate to the **Administration** > **Tools**.

   The **Tools** screen appears.

2. On the working area, click **Control Manager MIB file**.
3. On the **File Download** screen, select **Save**, specify a location on the server, and then click **OK**.
4. On the server, extract the Control Manager MIB file `cm2.mib`, Management Information Base (MIB) file.
5. Import `cm2.mib` using an application (for example, HP OpenView) that supports SNMP protocol.

Using the NVW Enforcer SNMPv2 MIB File

Download and use the NVW Enforcer SNMPv2 MIB file with an application (for example, HP OpenView) that supports SNMP protocol.

Procedure

1. Navigate to **Administration** > **Tools**.

   The **Tools** screen appears.
2. Click **NVW Enforcer SNMPv2 MIB file**.
3. On the **File Download** screen, select **Save**, specify a location on the server, and then click **OK**.
4. On the server, extract the NVW Enforcer SNMPv2 MIB file `nvw2.mib2`, Management Information Base (MIB) file.
5. Import `nvw2.mib2` using an application (for example, HP OpenView) that supports SNMP protocol.

Using the DBConfig Tool

The DBConfig tool allows users to change the user account, password, and the database name for the Control Manager database.

The tool offers the following options:

- **DBName:** Database name
- **DBAccount:** Database account
- **DBPassword:** Database password
- **Mode:** Database's authentication mode (SQL or Windows authentication)

Note

The default mode is SQL authentication mode, however Windows authentication mode is necessary when configuring for Windows authentication.

Procedure

1. From the Control Manager server, click **Start** > **Run**.
2. Type `cmd`, and then click **OK**.

   The command prompt screen appears.
3. Change the directory to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\DBConfig`).
4. Type `dbconfig`.

   The DBConfig tool interface appears.
5. Specify which settings you want to modify:
   - Example 1: `DBConfig -DBName="db_your_database>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - Example 2: `DBConfig -DBName="db_your_database>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`
   - Example 3: `DBConfig -DBName="db_your_database>" -DBPassword="sqlPwd"`

Part V

Removing Control Manager and Contacting Support

Chapter 23

Removing Trend Micro Control Manager

This chapter contains information about how to remove Control Manager components from your network, including the Control Manager server, Control Manager agents, and other related files.

This chapter contains the following sections:

Removing a Control Manager Server

You have two ways to remove Control Manager automatically (the following instructions apply to a Windows 2003 environment; details may vary slightly, depending on your Microsoft Windows platform):

Procedure

- From the **Start** menu, click **Start** > **Programs** > **Trend Micro Control Manager** > **Uninstalling Trend Micro Control Manager**.
- Using Add/Remove Programs:

  a. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

  b. Select **Trend Micro Control Manager**, and then click **Remove**.

  This action automatically removes other related services, such as the Trend Micro Management Infrastructure and Common CGI services, as well as the Control Manager database.

  c. Click **Yes** to keep the database, or **No** to remove the database.

  Note

  Keeping the database allows you to reinstall Control Manager on the server and retain all system information, such as agent registration, and user account data.

If you reinstalled the Control Manager server, and deleted the original database, but did not remove the agents that originally reported to the previous installation, then the agents will re-register with the server when:

- Managed product servers restart the agent services
- Control Manager agents verify their connection after an 8-hour period

---

Manually Removing Control Manager

This section describes how to remove Control Manager manually. Use the procedures below only if the Windows Add/Remove function or the Control Manager uninstall program is unsuccessful.

Note

Windows-specific instructions may vary between operating system versions. The following procedures are written for Windows Server 2003.

Removing Control Manager actually involves removing distinct components. These components may be removed in any order; they may even be removed together. However, for purposes of clarity, the uninstallation for each module is discussed individually, in separate sections. The components are:

- Control Manager application
- Trend Micro Management Infrastructure
- Common CGI Modules
- Control Manager Database (optional)
- PHP
- FastCGI

Other Trend Micro products also use the Trend Micro Management Infrastructure and Common CGI modules, so if you have other Trend Micro products installed on the same computer, Trend Micro recommends not removing these two components.

Note

After removing all components, you must restart your server. You only have to do this once — after completing the removal.

Removing the Control Manager Application

Manual removal of the Control Manager application involves the following steps:

Stopping Control Manager Services

Use the **Windows Services** screen to stop all of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager
- Trend Micro NTP

Note

These services run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services).

Stopping Control Manager Services from the Windows Services Screen

Procedure

1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.
2. Right-click **<Control Manager service>**, and then click **Stop**.

Stopping IIS and Control Manager Services from the Command Prompt

Procedure

- Run the following commands at the command prompt:

```
net stop w3svc
```

```
net stop tmcm
```

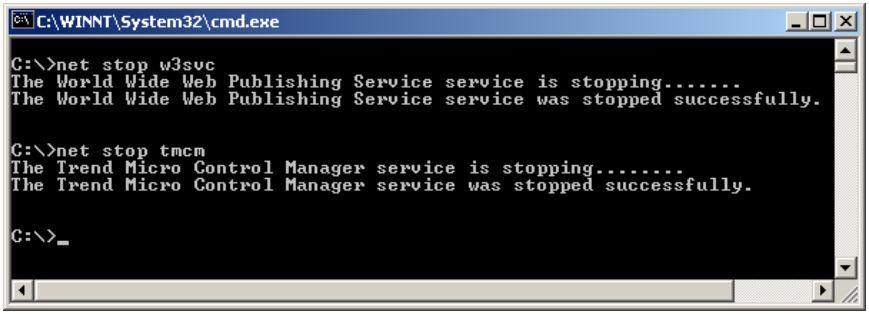


FIGURE 23-1. View of the command line with the necessary services stopped

Removing Control Manager IIS Settings

Remove the Internet Information Services settings after stopping the Control Manager services.

Procedure

1. From the Control Manager server, click **Start** > **Run**.

   The **Run** dialog box appears.

2. Type the following in the **Open** field:

   ```
   %SystemRoot%\System32\Inetsrv\iis.msc
   ```

3. On the left-hand menu, double-click the server name to expand the console tree.

4. Double-click **Default Web Site**.
5. Delete the following virtual directories:
   - `ControlManager`
   - `TVCSDownload`
   - `crystalreportviewers12`
   - `TVCS`
   - `Jakarta`
   - `WebApp`
6. On IIS 6 only:
   a. Right-click the IIS website you set during the installation.
   b. Click **Properties**.
7. Select the **ISAPI Filters** tab.
8. Delete the following ISAPI filters:
   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy
9. On IIS 6 only, delete the following web service extensions:
   - Trend Micro Common CGI Redirect Filter (If removing CCGI)
   - Trend Micro Control Manager CGI Extensions

Removing Crystal Reports, PHP, FastCGI, TMI, and CCGI

Removal of PHP, FastCGI, TMI and CCGI is optional. Use Add/Remove Programs to uninstall Crystal Reports, PHP, and FastCGI.

Removing Crystal Reports

Procedure

1. On the Control Manager server, click **Start** > **Settings** > **Control Panel** > **Add/ Remove Programs**.
2. Scroll down to Crystal Reports Runtime Files, and then click **Remove** to remove the Crystal Reports related files automatically.

Removing PHP and FastCGI

Procedure

1. On the Control Manager server, click **Start** > **Settings** > **Control Panel** > **Add/ Remove Programs**.
2. Scroll down to PHP, and then click **Remove** to remove PHP related files automatically.
3. Scroll down to FastCGI, and then click **Remove** to remove FastCGI related files automatically.

Removing TMI and CCGI

Procedure

1. Run the Microsoft service tool `Sc.exe`.
2. Type the following commands:

```
sc delete "TrendCGI"

sc delete "TrendMicro Infrastructure"
```

Deleting Control Manager Files/Directories and Registry Keys

Procedure

1. Delete the following directories:
   - `.Trend Micro\Control Manager`
   - `.Trend Micro\COMMON\ccgi`
   - `.Trend Micro\COMMON\TMI`
   - `.PHP`
   - `C:\Documents and Settings\All Users\Start Menu\Programs\PHP 5`
   - `C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro Control Manager`
2. Delete the following Control Manager registry keys:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DamageCleanupService`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPPTrustPort`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\VulnerabilityAssessmentServices`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI`

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP`

Removing the Database Components

This section describes how to remove the following database components from the Control Manager server:

- Removing Control Manager ODBC Settings
- Removing the Control Manager SQL Server 2008 Express Database

Removing Control Manager ODBC Settings

Procedure

1. On the Control Manager server, click **Start** > **Run**.

   The **Run** dialog box appears.

2. Type the following in the **Open** field:

   `odbcad32.exe`

3. On the **ODBC Data Source Administrator** screen, click the **System DSN** tab.
4. Under **Name**, select **ControlManager_Database**.
5. Click **Remove**, and then click **Yes** to confirm.

Removing the Control Manager SQL Server 2008 R2 Express Database

Procedure

1. On the Control Manager server, click **Start** > **Control Panel** > **Add/Remove Programs**.
2. Scroll down to **SQL Server 2008 R2** and then click **Remove** to remove the related files automatically.

Tip

Trend Micro recommends visiting the Microsoft website for instructions on removing SQL Server 2008 R2 Express if you have any issues with the uninstallation:

http://support.microsoft.com/kb/955499

Removing Control Manager and NTP Services

Procedure

1. Run the Microsoft service tool `Sc.exe`.
2. Type the following commands:

```
sc delete "TMCM"

sc delete "TrendMicro_NTP"
```

Removing a Windows-Based Control Manager 2.x Agent

To remove one or more agents, you must run the uninstallation component of the Control Manager Agent setup program.

Uninstall agents remotely, either by running the program from the Control Manager server, or another server, or locally, by running the setup program on the agent computer.

Procedure

1. Navigate to **Administration** > **Settings** > **Product Agent Settings**.

   The **Product Agent Settings** screen appears.

2. Click the **RemoteInstall.exe** link to download the application.

3. Using Microsoft Explorer, go to the location where you saved the agent setup program.

4. Double-click the `RemoteInstall.exe` file.

The **Trend Micro Control Manager Agent Setup** screen appears.

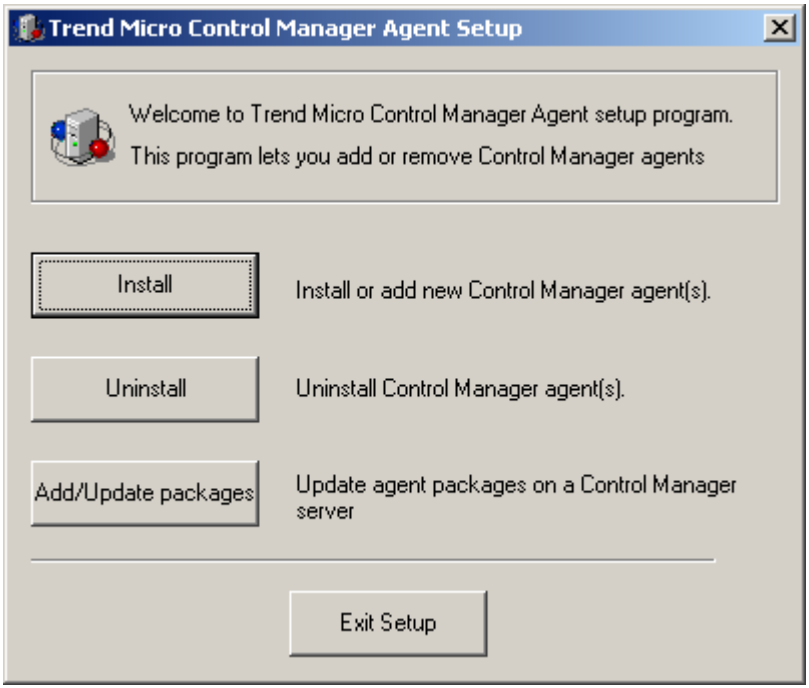


FIGURE 23-2. Trend Micro Control Manager Agent setup program

5. Click **Uninstall**.

   The **Welcome** screen appears.

6. Click **Next**.

The **Control Manager source server logon** screen appears.

FIGURE 23-3. Control Manager source server logon

7. Specify and provide Administrator-level logon credentials for the Control Manager server. Type the following information:

   - Host name
   - User name
   - Password

8. Click **Next**. Select the product whose agent you want to remove.

9. Click **Next**. Select the servers from which to remove the agents. You have two ways to select those servers:

   - To select from the list:

   a. In the left list box, double-click the domain containing the antivirus servers, and the domain expands to show all the servers inside.

b. Select the target server(s) from the left list box, and then click **Add**. The chosen server appears on the right list box. Click **Add All** to add agents to all servers in the selected chosen domain. Alternatively, you can double-click on a server to add it to the left list.

- To specify a server name directly:

a. Type the server's FQDN or IP address in the **Server name** field.

b. Click **Add**.

The server appears on the right list box.

c. To remove servers from the list, select a server from the right list box, and then click **Remove**. To remove all servers, click **Remove All**.

10. Click **Back** to return to the previous screen, **Exit** to abort the operation, or **Next** to continue.

11. Provide Administrator-level logon credentials for the selected servers. Type the required user name and password in the appropriate field.

12. Click **OK**. The **Analyze Chosen Server** screen provides the following details about the target servers: server name, domain, and the type of agent detected.

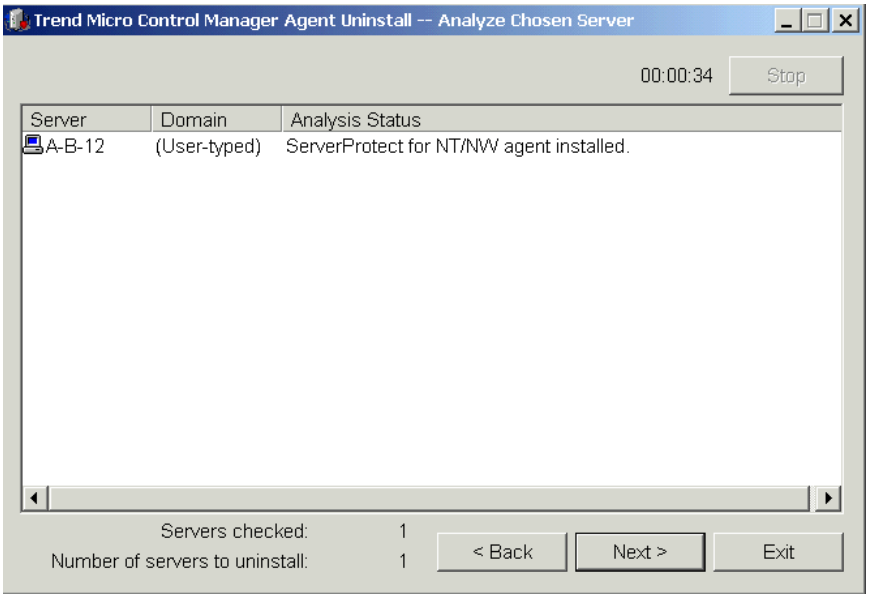


FIGURE 23-4. Analyze chosen Control Manager server

13. Click **Next** to continue.

    The table on this screen shows the following information about the target servers: server name, operating system version, IP address, Domain name, and the version of the agent you will remove. Click **Back** to return to the previous screen, **Exit** to abort the operation, or **Uninstall** to remove the agent.

    The uninstallation begins.

14. Click **OK**, and then on the **Removing Agents** screen, click **Exit**.

Chapter 24

Getting Support

Trend Micro has committed to providing service and support that exceeds our users' expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter contains the following topics:

Before Contacting Technical Support

Before contacting Technical Support, here are two things you can quickly do to try and find a solution to your problem:

- Check your documentation: the manual and online help provide comprehensive information about Control Manager. Search both documents to see if they contain your solution.
- Visit our Technical Support website: our Technical Support website contains the latest information about all Trend Micro products. The support website has answers to previous user inquiries.

  To search the Knowledge Base, visit

  http://esupport.trendmicro.com/en-us/default.aspx

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at *http://esupport.trendmicro.com*
- Get the latest Trend Micro product documentation at *http://docs.trendmicro.com*

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

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

Resolve Issues Faster

To resolve the issue faster, when you contact our staff, provide as much of the following information as you can:

- Product serial number
- Control Manager Build version
- Operating system version, Internet connection type, and database version (for example, SQL 2005 or SQL 2008)
- Exact text of the error message, if any
- Steps to reproduce the problem

TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

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

Other Useful Resources

Trend Micro offers a host of services through its website, http://www.trendmicro.com.

Internet-based tools and services include:

- Trend Micro™ Smart Protection Network™: monitor security threat incidents around the world
- HouseCall™: Trend Micro online virus scanner

Appendices

Appendices

Appendix A

Control Manager System Checklists

Use the checklists in this appendix to record relevant system information as a reference.

This appendix contains the following sections:

Server Address Checklist

You must provide the following server address information during the installation process, as well as during the configuration of the Control Manager server to work with your network. Record the information here for easy reference.

TABLE A-1. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server information		
IP address	10.1.104.255	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Web server information		
IP address	10.1.104.225	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
SQL-based Control Manager database information		
IP address	10.1.104.225	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	sqlserver	
Proxy server for component download		
IP address	10.1.174.225	
Fully qualified domain name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	

Information Required	Sample	Your Value
SMTP server information (Optional; for email message notifications)		
IP address	10.1.123.225	
Fully qualified domain name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP Trap information (Optional; for SNMP Trap notifications)		
Community name	trendmicro	
IP address	10.1.194.225	

Ports Checklist

Control Manager uses the following ports for the indicated purposes.

Port	Sample	Your Value
SMTP	25	
Proxy	8088	
Pager COM	COM1	
Proxy for Trend VCS Agent (Optional)	223	
Web Console and Update/ Deploy components	80	
Firewall, "forwarding" port (Optional; used during the Control Manager Agent installation)	224	

PORT	SAMPLE	YOUR VALUE
Trend Micro Management Infrastructure (TMI) internal process communication (for remote products)	10198	
TMI external process communication	10319	
Entity emulator	10329	

Note

Control Manager requires the exclusive use of ports 10319 and 10198.

Control Manager 2.x Agent Installation Checklist

The following information is used during agent installation.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server administrator account user name	root	
Encryption key location	`C:\MyDocuments \E2EPulic.dat`	

Note

You can use any user name instead of the root account. However, Trend Micro recommends using the root account, because deleting the user name specified while installing the agent makes managing the agent very difficult.

PRODUCT NAME	ADMINISTRATOR-LEVEL ACCOUNT	IP ADDRESS	HOSTNAME
Sample	Admin	10.225.225.225	PH-antivirus

Control Manager Conventions

Refer to the following conventions applicable for the Control Manager installation or web console configuration.

- User names
  - Max. length: 32 characters
  - Allowed: A-Z, a-z, 0-9, -, _
- Folder names
  - Max. length: 40 characters
  - Not allowed: / > & "

Note

For the Control Manager server host name, the setup program supports servers with underscores ("_") as part of the server name.

Core Process and Configuration Files

Control Manager saves system configuration settings and temporary files in XML format.

The following tables describe the configuration files and processes used by Control Manager.

TABLE A-2. Control Manager Configuration Files

CONFIGURATION FILE	DESCRIPTION
AuthInfo.ini	Configuration file that contains information about private key file names, public key file names, certificate file names, and the encrypted passphrase of the private key as well as the host ID and port.
aucfg.ini	ActiveUpdate configuration file
TVCS_Cert.pem	Certificate used by SSL authentication
TVCS_Pri.pem	Private Key used by SSL
TVCS_Pub.pem	Public Key used by SSL
ProcessManager.xml	Used by ProcessManager.exe
CmdProcessorEventHandler.xml	Used by CmdProcessor.exe
UIProcessorEventHandler.xml	Used by UIProcessor.exe
DMRegisterinfo.xml	Used by CasProcessor.exe
DataSource.xml	Stores the connection parameters for Control Manager processes
SystemConfiguration.xml	Control Manager system configuration file
CascadingLogConfiguration.xml	Log upload configuration file used for child servers
agent.ini	MCP agent file
TMI.cfg	Trend Micro Management Infrastructure configuration file

TABLE A-3. Control Manager Processes

PROCESSES	DESCRIPTION
ProcessManager.exe	Launches and stops other Control Manager core processes.

PROCESSES	DESCRIPTION
CmdProcessor.exe	Sends XML instructions, formed by other processes, to managed products, processes product registration, sends alerts, performs scheduled tasks, and applies Outbreak Prevention Policies.
UIProcessor.exe	Processes and transforms user input made in the Control Manager web console into actual commands.
LogReceiver.exe	Receives managed product logs and messages. Starting with Control Manager 3.0 Service Pack 4, LogReceiver.exe only handles logs coming from Trend Micro Damage Control Services and Trend Micro Vulnerability Assessment.
LogProcessor.exe	Receives logs from managed products, and receives entity information from managed products and child Control Manager servers.
LogRetriever.exe	Retrieves and saves logs in the Control Manager database.
ReportServer.exe	Generates Control Manager reports.
MsgReceiver.exe	Receives messages from the Control Manager server, managed products, and child servers.
CasProcessor.exe	Allows a Control Manager server (a parent server) to manage other Control Manager servers (child servers).
DCSProcessor.exe	Performs Damage Cleanup Services functions.
Ntpd.exe	Network Time Protocol service.
inetinfo.exe	Microsoft Internet Information Service process.
jk_nt_service.exe java.exe	Java server side extensions used to build web-based user interface by defining the interface instead of using a lot of standalone CGI programs.
cm.exe	Manages dmserver.exe and mrf.exe.
mrf.exe	The Communicator process.

PROCESSES	DESCRIPTION
dmserver.exe	Provides the Control Manager web console log on page and manages the Product Directory (Control Manager-side).
sCloudProcessor.NET.exe	Manages tasks related to Policy Management.

Communication and Listening Ports

These are the default Control Manager communication and listening ports.

TYPE	COMMUNICATION PORT
Internal communication	10198
External communication	10319

SERVICE	SERVICE PORT
ProcessManager.exe	20501
CmdProcessor.exe	20101
UIProcessor.exe	20701
LogReceiver.exe	20201
LogProcessor.exe	21001
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
CasProcessor.exe	20801

Service	Service Port
DcsProcessor.exe	20903

Control Manager Product Version Comparison

The following table provides a comparison of features between Control Manager versions.

Table A-4. Product Version Comparison

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
2.x and MCP agent interfaces with the managed products	●	●	●	●	●	●
Ad Hoc Query	●	●	●	●	●	●
Automatic component (for example, patterns/rules) update	●	●	●	●	●	●
Cascading management structure	●		●		●	
Central database for all virus log and system events	●	●	●	●	●	●
Centralized, web-based, virus management solution for the enterprise	●	●	●	●	●	●
Child server monitoring	●		●		●	
Child server task issuance	●		●		●	
Command Tracking	●	●	●	●	●	●
Communicator Heartbeat	●	●	●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Communicator Scheduler	●	●	●	●	●	●
Component download granularity	●	●	●	●	●	●
Configuration by group	●	●	●	●	●	●
Configure multiple download sources	●	●	●	●	●	●
Consistent managed product and Control Manager UI	●	●	●	●	●	●
Control Manager MIB files (previously called HP OpenView MIB)	●	●	●	●	●	●
Customized user types	●	●	●	●	●	●
Deployment Plans	●	●	●	●	●	●
Directory Manager	●	●	●	●	●	●
Enhanced Security Communication	●	●	●	●	●	●
Event Center	●	●	●	●	●	●
Improved Navigation	●	●	●	●	●	●
Improved User Interface	●	●	●	●	●	●
InterScan Web Security Service integration	●	●	●	●	●	●
Logging Enhancements	●	●	●	●	●	●
Log processing speed enhancements			●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Manage antivirus and content security products	●	●	●	●	●	●
Manage services	●	●	●	●	●	●
Managed product license manager	●		●		●	
Managed product reporting	●		●		●	
Web console rendering enhancement			●	●	●	●
Microsoft SQL Express or Microsoft SQL 2005	●	●	●	●	●	●
Microsoft SQL Express or Microsoft SQL 2008			●	●	●	●
Microsoft SQL 2012					●	●
MSDE or Microsoft SQL 7/2000	●	●				
MSN Messenger notification	●	●	●	●	●	●
Notification and Outbreak Alert	●	●	●	●	●	●
OfficeScan Integration Enhancements			●	●	●	●
Outbreak Commander / Outbreak Prevention Services (OPS) • Automatic Download and Deployment of OPP • Manual Download and Deployment of OPP	●	●	●	●		
Passive Support for 3rd Party Product	●		●			

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Policy management					●	●
Remote and Local Agent Installation	●	●	●	●	●	●
Remote management	●	●	●	●	●	●
Reporting	●		●		●	
Secure communication between Server and Agents	●	●	●	●	●	●
Single sign-on (SSO) for managed products that support SSO	●	●	●	●	●	●
Smart Protection Network integration			●	●	●	●
SNMP trap notification	●		●		●	
SSL support for ActiveUpdate	●	●	●	●	●	●
SSL support for web console	●	●	●	●	●	●
Support Control Manager 2.x agents	●	●	●	●	●	●
Support HTTPS communication between server, agents, and managed products	●	●	●	●	●	●
Support MCP agents	●	●	●	●	●	●
Syslog notification	●		●		●	
Threat Intelligence-Oriented Dashboard			●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Trend Micro InterScan for Cisco Content Security and Control Security Services Module (ISC CSC SSM) integration	●	●	●	●	●	●
Trend Micro Network VirusWall Enforcer 1500i/3500i integration	●	●	●	●	●	●
Trend Micro Network VirusWall Enforcer 3600i integration					●	●
Trend Micro Product Registration server integration	●	●	●	●	●	●
TrendLabs Message Board	●	●	●	●		
User account management	●	●	●	●	●	●
Vulnerability Assessment	●	●	●	●		
Windows Authentication	●	●	●	●	●	●
Work-hour control	●	●	●	●	●	●

Appendix B

Data Views

Database views are available to Control Manager report templates and to Ad Hoc Query requests.

This appendix contains the following sections:

Data View: Product Information

Displays information about Control Manager, Managed Products, components, and licenses.

License Information

Displays status, detailed, and summary information about Control Manager and managed product license information.

Product License Status

Displays detailed information about the managed product and information about the Activation Code the managed product uses. Examples: managed product information, whether the Activation Code is active, the number of managed products the Activation Code activates

TABLE B-1. Product License Status Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Service	Displays the name of the managed product service. Example: Outbreak Protection Services
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Activation Code	Displays the Activation Code for managed products.

DATA	DESCRIPTION
Activation Codes	Displays the number of Activation Codes a managed products uses.
License Expiration	Displays the date the license expires for the managed product.

Product License Information Summary

Displays detailed information about the Activation Code and information on managed products that use the Activation Code. Examples: seat count that the Activation Code allows, evaluation or full product version, user-defined description about the Activation Code

TABLE B-2. Product License Information Summary Data View

DATA	DESCRIPTION
Activation Code	Displays the Activation Code for managed products.
User-defined Description	Displays the user-defined description for the Activation Code.
Products/Services	Displays the number of managed products or services that use the Activation Code.
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Product Type	Displays the type of managed product the Activation Code provides. Example: Trial version, Full version
License Expiration	Displays the date the license expires for the managed product.
Seats	Displays the number of seats the Activation Code allows.

Detailed Product License Information

Displays information about the Activation Code and information on managed products that use the Activation Code. Examples: managed product information, evaluation or full product version, license expiration date

TABLE B-3. Detailed Product License Information Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Managed Service	Displays the name of the managed service. Example: Web Reputation Service
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Product Type	Displays the type of managed product the Activation Code provides. Example: Trial version, Full version
Activation Code	Displays the Activation Code for managed products.
License Expiration	Displays the date the license expires for the managed product.
Seats	Displays the number of seats the Activation Code allows.
Description	Displays the description for the Activation Code.

Managed Product Information

Displays status, detailed, and summary information about managed products or managed product endpoints.

Product Distribution Summary

Displays summary information about managed products registered to Control Manager. Examples: managed product name, version number, and number of managed products

TABLE B-4. Product Distribution Summary Data View

DATA	DESCRIPTION
Registered to Control Manager	Displays the Control Manager server to which the managed product is registered.
Product Category	Displays the threat protection category for a managed product. Example: Server-based products, Desktop (computers and mobile devices) products **Note** Desktop products includes mobile device solutions.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Product Role	Displays the role the managed product has in the network environment. Example: server, client
Products	Displays the total number of a specific managed product a network contains.

Product Status Information

Displays detailed information about managed products registered to Control Manager. Examples: managed product version and build number, operating system

TABLE B-5. Product Status Information Data View

DATA	DESCRIPTION
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.

Data	Description
Product Host/ Endpoint	This data column displays one of the following: • The host name of the server on which the managed product installs. • The host name of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with an agent (for example OfficeScan agent) installed.
Managing Control Manager Entity	Displays the entity display name of the Control Manager server to which the managed product is registered.
Managing Server Entity	Displays the entity display name for a managed product to which an endpoint is registered. Control Manager identifies managed products using the managed product's entity display name.
Domain	Displays the domain to which the managed product belongs.
Connection Status	This data column displays one of the following: • The managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline • The endpoint agent's connection status to a managed product (OfficeScan). Example: Normal, Abnormal, Offline
Pattern Status	Displays the status of the pattern files/rules the managed product or a computer with an agent (for example OfficeScan agent) uses. Example: up-to-date, out-of-date

DATA	DESCRIPTION
Engine Status	Displays the status of the scan engines the managed product or a computer with an agent (for example OfficeScan agent) uses. Example: up-to-date, out-of-date
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's or managed product agent's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Product Build	Displays the build number of the managed product. This information appears on the About screen for products. Example: Version: 5.0 (Build 1219)
Product Role	Displays the role the managed product or a computer with an agent (for example OfficeScan agent) has in the network environment. Example: server
Operating System	Displays the operating system of the computer where the managed product/agent installs.
OS Version	Displays the version number of the operating system of the computer where the managed product/agent installs.
OS Service Pack	Displays the service pack number of the operating system of the computer where the managed product/agent installs.
Update Agent	If the agent is an Update Agent
Last Scheduled Scan	Date and time of last Scheduled Scan
Last Manual Scan	Date and time of last Manual Scan
Last Scan Now	Date and time of last Scan Now
Real-time Scan	If Real-time Scan is enabled
Firewall	If the firewall is enabled

Product Event Information

Displays information relating to managed product events. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE B-6. Product Event Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data about the managed product event.
Generated	Displays the time that the managed product generates data about the event.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Event Severity	Displays the severity of an event. Example: Information, Critical, Warning
Event Type	Displays the type of event that occurred. Example: download virus found, file blocking, rollback
Command Status	Displays the status of the command. Example: successful, unsuccessful, in progress
Description	Displays the description a managed product provides for the event.

Product Auditing Event Log

Displays auditing information related to managed products. For example, auditing management console accesses.

TABLE B-7. Product Auditing Event Log Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data about the managed product event.
Generated	Displays the time that the managed product generates data about the event.
Host	Displays one of the following: • The host name of the server on which the managed product installs. • The host name of a computer with an engine (for example OfficeScan agent) installed.
User	Displays account information.
Event Category	Displays the category of event that occurred. Example: management console access
Event Level	Displays the severity of an event.
Event Description	Displays the description a managed product provides for the event.

Component Information

Displays status, detailed, and summary information about out of date and up to date and component deployment of managed product components.

Engine Status

Displays detailed information about scan engines managed products use. Examples: scan engine name, time of the latest scan engine deployment, and which managed products use the scan engine

TABLE B-8. Engine Status Data View

DATA	DESCRIPTION
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Product Host/ Endpoint	This data column displays one of the following: • The host name of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Connection Status	This data column displays one of the following: • The managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline • The endpoint agent's connection status to a managed product (OfficeScan). Example: Normal, Abnormal, Offline
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's or managed product agent's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Product Role	Displays the role the managed product or a computer with an agent (for example OfficeScan agent) has in the network environment. Example: server

DATA	DESCRIPTION
Engine	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine
Engine Version	Displays the version of the scan engine. Example: Anti-spam Engine (Windows): 3.000.1153, Virus Scan Engine IA 64 bit Scan Engine: 8.000.1008
Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Engine Updated	Displays the time of the latest scan engine deployment to managed products or endpoints.

Pattern/Rule Status

Displays detailed information about pattern files/rules managed products use. Examples: pattern file/rule name, time of the latest pattern file/rule deployment, and which managed products use the pattern file/rule

TABLE B-9. Pattern/Rule Status Data View

DATA	DESCRIPTION
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Operating System	This data column displays the operating system of the server on which the managed product installs.
Product Host/ Endpoint	This data column displays one of the following: • The host name of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.

DATA	DESCRIPTION
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Update Agent	This data column displays Update Agents for the managed product.
Domain	This data column displays the domain of the server on which the managed product installs.
Managing Server Entity Display Name	This data column displays the managing server entity display name.
Connection Status	This data column displays one of the following: • The managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline • The endpoint agent's connection status to a managed product (OfficeScan). Example: Normal, Abnormal, Offline
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's or managed product agent's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Product Role	Displays the role the managed product or a computer with an agent (for example OfficeScan agent) has in the network environment. Example: server
Pattern/Rule	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Pattern/Rule Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: 3.203.00, Anti-spam Pattern: 14256
Pattern/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date

DATA	DESCRIPTION
Pattern/Rule Updated	Displays the time of the latest pattern file/rule deployment to managed products or endpoints.
OfficeScan Domain Hierarchy	Displays the path on the OfficeScan domain hierarchy.

Product Component Deployment

Displays detailed information about components managed products use. Examples: pattern file/rule name, pattern file/rule version number, and scan engine deployment status

TABLE B-10. Product Component Deployment Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Version	Displays the managed product's version number. Example: OfficeScan- 10.0, Control Manager- 5.0
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their endpoints.
Pattern/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date
Pattern/Rule Deployment Status	Displays the deployment status for the latest pattern file/rule update. Example: successful, unsuccessful, in progress
Pattern/Rule Deployment	Displays the time of the latest pattern file/rule deployment to managed products or endpoints.
Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date

DATA	DESCRIPTION
Engine Deployment Status	Displays the deployment status for the latest scan update. Example: successful, unsuccessful, in progress
Engine Deployment	Displays the time of the latest scan engine deployment to managed products or endpoints.

Scan Engine Status Summary

Displays summary information about scan engines managed products use. Examples: scan engine name, scan engine rate, and the number of scan engines out-of-date

TABLE B-11. Engine Status Summary Data View

DATA	DESCRIPTION
Engine	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine
Version	Displays the version of the scan engine. Example: Anti-spam Engine (Windows): 3.000.1153, Virus Scan Engine IA 64 bit Scan Engine: 8.000.1008
Up-to-Date	Displays the number of managed products with up-to-date scan engines.
Out-of-Date	Displays the number of managed products with out-of-date scan engines.
Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date scan engines. This includes scan engines that return N/A as a value.

Pattern/Rule Status Summary

Displays summary information about pattern files/rules managed products use. Examples: pattern file/rule name, pattern file/rule up-to-date rate, and the number of pattern files/rules out-of-date

TABLE B-12. Pattern File/Rule Status Summary Data View

DATA	DESCRIPTION
Pattern/Rule	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: 3.203.00, Anti-spam Pattern: 14256
Up-to-Date	Displays the number of managed products with up-to-date pattern files or rules.
Out-of-Date	Displays the number of managed products with out-of-date pattern files or rules.
Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date pattern files/rules. This includes pattern files/rules that return n/a as a value.

Endpoint Pattern/Engine Status Summary

Displays summary information about pattern files/scan engine managed products use.

TABLE B-13. Endpoint Pattern/Engine Status Summary

DATA	DESCRIPTION
Product Host	Displays the host name of the server on which the managed product installs.
Domain	Displays the domain name of the host.
Endpoints	Displays the host name of a computer with an agent (for example OfficeScan agent) installed.
Patterns Out-of-Date	Displays the number of managed products with out-of-date pattern files.
Pattern Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date pattern files. This includes pattern files that return n/a as a value.
Engines Out-of-Date	Displays the number of managed products with out-of-date scan engines.

DATA	DESCRIPTION
Engine Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date scan engines. This includes scan engines that return n/a as a value.

Control Manager Information

Displays information about Control Manager user access, Command Tracking information, and Control Manager server events.

User Access Information

Displays Control Manager user access and the activities users perform while logged on to Control Manager.

TABLE B-14. User Access Information Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the activity starts.
User	Displays the name of the user who initiates the activity.
Account Type	Displays the account type a Control Manager administrator assigns to a user. For example: Root, Power User, or Operator.
Account Type Description	Displays the description of the Account Type. This description comes from Control Manager for default account types and from user-defined descriptions for custom account types.
Activity	Displays the activity the user performs on Control Manager. Example: log on, edit user account, add deployment plan
Result	Displays the result of the activity.
Description	Displays the a description of the activity, if a description exists.

Control Manager Event Information

Displays information relating to Control Manager Server events. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE B-15. Control Manager Event Information Data View

DATA	DESCRIPTION
Date/Time	Displays the that the event occurred.
Event Type	Displays the type of event that occurred. Example: notify TMI agent, server notify user, report service notify user
Result	Displays the result of the event. Example: successful, unsuccessful
Description	Displays the description of the activity, if a description exists.

Command Tracking Information

Displays information relating to commands Control Manager delivers to managed products. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE B-16. Command Tracking Information Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the issuer of the command issues the command.
Command Type	Displays the type of command issued. Example: scheduled update, Activation Code deployment
Command Parameter	Displays the specific information relating to the command. Example: specific pattern file name, specific Activation Code
User	Displays the user who issued the command.
Status Update	Displays the time of the latest status check of all commands for the selected Control Manager.

Data	Description
Successful	Displays the number of successful commands.
Unsuccessful	Displays the number of unsuccessful commands.
In Progress	Displays the number of commands that are still in progress.
All	Displays the total number of commands (Successful + Unsuccessful + In progress).

Detailed Command Tracking Information

Displays detailed information relating to commands. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

Table B-17. Detailed Command Tracking Information Data View

Data	Description
Date/Time	Displays the time that the command was issued.
Command Type	Displays the type of command issued. Example: scheduled update, Activation Code deployment
Command Parameter	Displays the specific information relating to the command. Example: specific pattern file name, specific Activation Code
Product Entity	Displays the managed product to which the command was issued.
User	Displays the user who issued the command.
Command Status	Displays the status of the command: successful, unsuccessful, in progress
Status Update	Displays the time of the latest status check of all commands for the selected Control Manager.
Result Detail Description	Displays the description Control Manager provides for events.

Data View: Security Threat Information

Displays information about security threats that managed products detect: viruses, spyware/grayware, phishing sites, and more.

Virus/Malware Information

Displays summary and detailed data about malware/viruses that managed products detect on your network.

Overall Virus/Malware Summary

Provides overall specific summary for virus/malware detections. Example: name of virus/malware, number of endpoints affected by the virus, total number of instances of the virus on the network

TABLE B-18. Overall Virus/Malware Summary Data View

DATA	DESCRIPTION
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Unique Endpoints	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. Unique Endpoints = 3
Unique Sources	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. Unique Sources = 2

Data	Description
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Virus/Malware Source Summary

Provides a summary of virus/malware detections from the source of the outbreak. Example: name of source computer, number of specific virus/malware instances from the source computer, total number of instances of viruses/malware on the network

Table B-19. Virus/Malware Source Summary Data View

Data	Description
Source Host	Displays the IP address or host name of the computer where viruses/malware originate.
Unique Endpoints	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. Unique Detections = 3
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Virus/Malware Endpoint Summary

Provides a summary of virus/malware detections from specific endpoints. Example: name of endpoint, number of specific virus/malware instances on the endpoint, total number of instances of viruses/malware on the network

TABLE B-20. Virus/Malware Endpoint Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of the computer affected by viruses/malware.
Unique Sources	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. Unique Sources = 2
Unique Detections	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Unique Detections = 1

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Virus/Malware Action/Result Summary

Provides a summary of the actions managed products take against viruses/malware. Example: specific actions taken against viruses/malware, the result of the action taken, total number of instances of viruses/malware on the network

TABLE B-21. Virus/Malware Action/Result Summary Data View

DATA	DESCRIPTION
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Unique Endpoints	Displays the number of unique computers affected by the virus/malware. Example: OfficeScan detects 10 virus instances of the same virus on 3 different computers. Unique Endpoints = 3
Unique Sources	Displays the number of unique infection sources where viruses/malware originate. Example: OfficeScan detects 10 virus instances of the same virus originating from 2 infection sources. Unique Sources = 2

DATA	DESCRIPTION
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Virus/Malware Detection Over Time Summary

Provides a summary of virus/malware detections over a period of time

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.
Unique Detections	Displays the number of unique virus/malware detections. Example: A managed product detects the same virus on 2 endpoints. Unique Detections = 1
Unique Endpoints	Displays the number of unique endpoints with virus/malware detections. Example: A managed product detects a virus on 4 endpoints. Unique Endpoints = 4
Unique Sources	Displays the number of unique sources of virus/malware. Example: A managed product detects 10 viruses from two different sources. Unique Sources = 2
Detections	Displays the total number of viruses/malware managed products detect. Example: A managed product detects 10 viruses/malware on one computer. Detections = 10

Detailed Virus/Malware Information

Provides specific information about the virus/malware instances on your network. Example: the managed product which detects the viruses/malware, the name of the virus/malware, the name of the endpoint with viruses/malware

TABLE B-22. Detailed Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with an agent (for example OfficeScan agent) installed.
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.

DATA	DESCRIPTION
Domain	Displays the domain of the managed product server to which an endpoint is registered.
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: `NIMDA, BLASTER, I_LOVE_YOU.EXE`
Endpoint	Displays the IP address or host name of the computer affected by viruses/malware.
Source Host	Displays the IP address or host name of the computer where viruses/malware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections =10
Entry Type	Displays the entry point for the virus/malware that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)

Data	Description
Detailed Information	Used only for Ad Hoc Queries. Displays detailed information about the selection. In Ad Hoc Queries this column displays the selection as underlined. Clicking the underlined selection displays more information about the selection. Example: Host Details, Network Details, HTTP/FTP Details
OfficeScan Domain Hierarchy	Displays the path to the OfficeScan domain hierarchy.

Endpoint Virus/Malware Information

Provides specific information about the virus/malware instances found on endpoints. Example: the managed product that detects the viruses/malware, the type of scan that detects the virus/malware, the file path on the endpoint to detected viruses/malware

Table B-23. Endpoint Virus/Malware Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.

DATA	DESCRIPTION
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: `NIMDA, BLASTER, I_LOVE_YOU.EXE`
Endpoint	Displays the name of the computer affected by viruses/malware.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Scan Type	Displays the type of scan the managed product uses to detect the virus/malware. Example: Real-time, scheduled, manual
File	Displays the name of the file managed products detect affected by viruses/malware.
File Path	Displays the file path on the endpoint computer where managed products detect the virus/malware.
File in Compressed File	Displays the name of the infected file/virus/malware in a compressed file.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Web Virus/Malware Information

Provides specific information about the virus/malware instances found in HTTP or FTP traffic. Example: the managed product that detects the viruses/malware, the direction of traffic where the virus/malware occurs, the Internet browser or FTP endpoint that downloads the virus/malware.

TABLE B-24. Web Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: `NIMDA, BLASTER, I_LOVE_YOU.EXE`
Endpoint	Displays the IP address or host name of the computer on which managed products detect viruses/malware.
Source URL	Displays the URL of the web/FTP site which the virus/malware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Traffic/Connection	Displays the direction of virus/malware entry.
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the viruses/ malware originates.

DATA	DESCRIPTION
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Email Virus/Malware Information

Provides specific information about the virus/malware instances found in email messages. Example: the managed product that detects the viruses/malware, the subject line content of the email message, the sender of the email message that contains viruses/malware

TABLE B-25. Email Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: `NIMDA, BLASTER, I_LOVE_YOU.EXE`

DATA	DESCRIPTION
Recipient	Displays the recipient of the email message containing viruses/malware.
Sender	Displays the sender of email message containing viruses/malware.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Subject	Displays the content of the subject line of the email message containing viruses/malware.
File	Displays the name of the file managed products detect affected by viruses/malware.
File in Compressed File	Displays the name of the infected file/virus/malware in a compressed file.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Network Virus/Malware Information

Provides specific information about the virus/malware instances found in network traffic. Example: the managed product that detects the viruses/malware, the protocol the virus/malware uses to enter your network, specific information about the source and destination of the virus/malware

TABLE B-26. Network Virus/Malware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: `NIMDA, BLASTER, I_LOVE_YOU.EXE`
Endpoint	Displays the IP address/ host name of the computer affected by viruses/malware.
Source Host	Displays the IP address or host name of the computer where viruses/malware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects viruses/malware.
Traffic/Connection	Displays the direction of virus/malware entry.
Protocol	Displays the protocol that the virus/malware uses to enter the network. Example: HTTP, SMTP, FTP
Endpoint Computer	Displays the computer name of the computer affected by viruses/ malware.
Endpoint Port	Displays the port number of the computer affected by viruses/ malware.

DATA	DESCRIPTION
Endpoint MAC	Displays the MAC address of the computer affected by viruses/ malware.
Source Computer	Displays the computer name of the computer where viruses/ malware originates.
Source Port	Displays the port number of the computer where viruses/malware originates.
Source MAC	Displays the MAC address of the computer where viruses/ malware originates.
File	Displays the name of the file managed products detect affected by viruses/malware.
Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Spyware/Grayware Information

Displays summary and detailed data about spyware/grayware that managed products detect on your network.

Overall Spyware/Grayware Summary

Provides overall specific summary for spyware/grayware detections. Example: name of spyware/grayware, number of endpoints affected by the spyware/grayware, total number of instances of the spyware/grayware on the network

TABLE B-27. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Sources	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. Unique Sources = 2
Detections	Displays the total number of spyware/grayware managed products detect.

Spyware/Grayware Source Summary

Provides a summary of spyware/grayware detections from the source of the outbreak. Example: name of source computer, number of specific spyware/grayware instances from the source computer, total number of instances of spyware/grayware on the network

TABLE B-28. Spyware/Grayware Source Summary Data View

DATA	DESCRIPTION
Source Host	Displays the name of the computer where spyware/grayware originates.

DATA	DESCRIPTION
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Detections	Displays the number of unique spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Unique Detections = 1
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Endpoint Spyware/Grayware Summary

Provides a summary of spyware/grayware detections from specific endpoints. Example: name of endpoint, number of specific spyware/grayware instances on the endpoint, total number of instances of spyware/grayware on the network

TABLE B-29. Endpoint Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the host name or IP address of the computer affected by spyware/grayware.

DATA	DESCRIPTION
Unique Sources	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. Unique Sources = 2
Unique Detections	Displays the number of unique spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Unique Detections = 1
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Spyware/Grayware Detection Over Time Summary

Provides a summary of spyware/grayware detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints affected by the spyware/grayware, total number of instances of spyware/grayware on the network

TABLE B-30. Spyware/Grayware Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.

DATA	DESCRIPTION
Unique Detections	Displays the number of unique spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Unique Detections = 1
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Sources	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. Unique Sources = 2
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Spyware/Grayware Action/Result Summary

Provides a summary of the actions managed products take against spyware/grayware. Example: specific actions taken against spyware/grayware, the result of the action taken, total number of instances of spyware/grayware on the network

TABLE B-31. Spyware/Grayware Action/Result Summary Data View

DATA	DESCRIPTION
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Unique Endpoints	Displays the number of unique computers affected by the spyware/grayware. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on 3 different computers. Unique Endpoints = 3
Unique Sources	Displays the number of unique sources where spyware/grayware originates. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware originating from 2 infection sources. Unique Sources = 2
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Detailed Spyware/Grayware Information

Provides specific information about the spyware/grayware instances on your network. Example: the managed product that detects the spyware/grayware, the name of the spyware/grayware, the name of the endpoint with spyware/grayware

TABLE B-32. Detailed Spyware/Grayware Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/ grayware.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/ grayware.
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.

DATA	DESCRIPTION
Endpoint	Displays the IPaddress or host name of the computer affected by spyware/grayware.
Source Host	Displays the IPaddress or host name of the computer where spyware/grayware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10
Entry Type	Displays the entry point for the spyware/grayware that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)
Detailed Information	Used only for Ad Hoc Queries. Displays detailed information about the selection. In Ad Hoc Queries this column displays the selection as underlined. Clicking the underlined selection displays more information about the selection. Example: Host Details, Network Details, HTTP/FTP Details

Endpoint Spyware/Grayware

Provides specific information about the spyware/grayware instances found on endpoints. Example: the managed product that detects the spyware/grayware, the type of scan that detects the spyware/grayware, the file path on the endpoint to detected spyware/grayware

TABLE B-33. Endpoint Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/grayware.
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/ grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managing Server Entity	Displays the entity display name of the managed product server to which an endpoint is registered.
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.

DATA	DESCRIPTION
Endpoint	Displays the IPaddress or host name of the computer affected by spyware/grayware.
Source Host	Displays the IPaddress or host name of the computer where the spyware/grayware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
Scan Type	Displays the type of scan the managed product uses to detect the spyware/grayware. Example: Real-time, scheduled, manual
Resource	Displays the specific resource affected. Example: `application.exe`, `H Key Local Machine\SOFTWARE\ACME`
Resource Type	Displays the type of resource affected by spyware/grayware. Example: registry, memory resource
Security Threat Type	Displays the specific type of spyware/grayware managed products detect. Example: adware, COOKIE, peer-to-peer application
Risk Level	Displays the Trend Micro-defined level of risk the spyware/grayware poses to your network. Example: High security, Medium security, Low security
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of spyware/grayware managed products detect.

Web Spyware/Grayware

Provides specific information about the spyware/grayware instances found in HTTP or FTP traffic. Example: the managed product that detects the spyware/grayware, the direction of traffic where the spyware/grayware occurs, the Internet browser or FTP endpoint that downloads the spyware/grayware

TABLE B-34. Web Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
IP	Displays the IP address of the computer on which managed products detect spyware/grayware.
Source URL	Displays the URL of the web/FTP site which the spyware/ grayware originates.
Traffic/Connection	Displays the direction of spyware/grayware entry.
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the spyware/grayware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.

DATA	DESCRIPTION
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Email Spyware/Grayware

Provides specific information about the spyware/grayware instances found in email messages. Example: the managed product that detects the spyware/grayware, the subject line content of the email message, the sender of the email message that contains spyware/grayware

TABLE B-35. Email Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

DATA	DESCRIPTION
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Recipient	Displays the recipient of the email message containing spyware/grayware.
Sender	Displays the sender of email message containing spyware/grayware.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
Subject	Displays the content of the subject line of the email message containing spyware/grayware.
File	Displays the name of the file managed products detect affected by spyware/grayware.
File in Compressed File	Displays the file name of the spyware/grayware occurring in a compressed file.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Network Spyware/Grayware

Provides specific information about the spyware/grayware instances found in network traffic. Example: the managed product that detects the spyware/grayware, the protocol

the spyware/grayware uses to enter your network, specific information about the source and destination of the spyware/grayware

TABLE B-36. Network Spyware/Grayware Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is affected by spyware/grayware.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.
Traffic/Connection	Displays the direction of spyware/grayware entry.
Protocol	Displays the protocol that the spyware/grayware uses to enter the network. Example: HTTP, SMTP, FTP
Endpoint IP	Displays the IP address of the computer affected by spyware/ grayware.
Endpoint	Displays the IP address or host name of the computer affected by spyware/grayware.
Endpoint Port	Displays the port number of the computer affected by spyware/ grayware.
Endpoint MAC	Displays the MAC address of the computer affected by spyware/ grayware.

DATA	DESCRIPTION
Source IP	Displays the IP address of the computer where spyware/grayware originates.
Source Host	Displays the host name of the computer where spyware/grayware originates.
Source Port	Displays the port number of the computer where spyware/grayware originates.
Source MAC	Displays the MAC address of the computer where spyware/grayware originates.
User	Displays the user name logged on to the endpoint computer when a managed product detects spyware/grayware.
File	Displays the name of the file managed products detect affected by spyware/grayware.
Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Detections	Displays the total number of spyware/grayware managed products detect. Example: OfficeScan detects 10 spyware/grayware instances of the same spyware/grayware on one computer. Detections = 10

Content Violation Information

Displays summary and detailed data about prohibited content that managed products detect on your network.

Content Violation Policy Summary

Provides a summary of content violation detections due to specific policies. Example: name of the policy in violation, the type of filter that detects the content violation, the total number of content violations on the network

TABLE B-37. Content Violation Policy Summary Data View

DATA	DESCRIPTION
Policy	Displays the name of the policy that endpoints violate.
Filter Type	Displays the type of filter that triggers the violation. Example: content filter, phishing filter, URL reputation filter
Unique Senders/ Users	Displays the number of unique email message addresses or users sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. Unique Senders/Users = 3
Unique Recipients	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. Unique Recipients = 2
Detections	Displays the total number of policy violations managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. Detections = 10

Content Violation Sender Summary

Provides a summary of content violation detections due to specific senders. Example: name of the content sender, the number of unique content violations, the total number of content violations on the network

TABLE B-38. Content Violation Sender Summary Data View

DATA	DESCRIPTION
Sender/User	Displays the email message address or users sending content that violates managed product policies.
Detections	Displays the total number of policy violations managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. Detections = 10
Unique Recipients	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. Unique Recipients = 2
Unique Policies	Displays the number of unique policies in violation managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. Detections = 10

Content Violation Detection Over Time Summary

Provides a summary of content violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints affected by the content violation, total number of unique content violations and total number of content violations on the network

TABLE B-39. Content Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.

DATA	DESCRIPTION
Unique Policies	Displays the number of unique policies in violation managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. Detections = 10
Unique Senders/ Users	Displays the number of unique email message addresses or users sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. Unique Senders/Users = 3
Unique Recipients	Displays the number of unique email message recipients receiving content that violate managed product policies. Example: A managed product detects 10 violation instances of the same policy on 2 computers. Unique Recipients = 2
Detections	Displays the total number of policy violations managed products detect. Example: A managed product detects 10 violation instances of the same policy on one computer. Detections = 10

Content Violation Action/Result Summary

Provides a summary of actions managed products take against content violations. Example: the action managed products take against the content violation, the number of email messages affected by the action taken

TABLE B-40. Content Violation Action/Result Summary Data View

DATA	DESCRIPTION
Action	Displays the type of action managed products take against email message in violation of content policies. Example: forwarded, attachments stripped, deleted
Policy Violation Detection Count	Displays the number of violations with the specified action taken by managed products.

Detailed Content Violation Information

Provides specific information about the content violations on your network. Example: the managed product that detects the content violation, the name of the specific policy in violation, the total number of content violations on the network

TABLE B-41. Detailed Content Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Recipient	Displays the email recipients receiving content that violate managed product policies.
Sender/User	Displays the email address or user sending content that violates managed product policies.
Subject	Displays the content of the subject line of the email that violates a policy.
Policy	Displays the name of the policy an email violates.

DATA	DESCRIPTION
Policy Settings	Displays the settings for the policy that an email violates.
File Location	Displays the location of the file that violates a policy.
File	Displays the name of the file that violates a policy.
URL	Displays the URL in violation of the specified policy.
Risk Level	Displays the Trend Micro assessment of risk to your network. Example: high security, low security, medium security
Filter Type	Displays the type of filter that detects the email in violation. Example: content filter, size filter, attachment filter
Sub-filter Type	Displays the type of sub-filter that detects the email in violation.
Filter Action	Displays the action the detecting filter takes against email in violation of a policy. Example: clean, quarantine, strip
Filter Action Result	Displays the action result of the filter that detects the email in violation.
Action	Displays the type of action managed products take against email in violation of content policies. Example: deliver, strip, forward
Detections	Displays the total number of policy violations managed products detect.

Email Messages with Advanced Threats

Displays all email messages with malicious and suspicious behavior. Suspicious behavior includes anomalous behavior, false or misleading data, suspicious and malicious behavioral patterns, and strings that indicate system compromise but require further investigation to confirm.

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Recipients	Displays the email recipients receiving content that violate managed product policies.
Sender	Displays the email address sending content that violates managed product policies.
Subject	Displays the content of the subject line of the email that violates a policy.
Attachment Count	Number of attachments
Attachment	Attachment name
Atttachment Type	Attachment type
Action	Displays the type of action managed products take against email in violation of content policies. Example: deliver, strip, quarantine
Threat Type	Threat type
Threat Name	Threat name
Risk Level	Email message risk levels after investigation
Source IP	MTA IP address nearest to the email sender
Message ID	Administrator-configured unique message ID
Link Count	Number of links in the message
Links	List of links

Spam Violation Information

Displays summary and detailed data about spam that managed products detect on your network.

Overall Spam Violation Summary

Provides a summary of spam violations on the network

Data	Description
Recipient Domain	Domain of recipients affected by spam
Unique Recipients	Displays the number of unique recipients receiving spam from the specified domain. Example: A managed product detects 10 violation instances of spam from the same domain on 3 computers. Unique Recipients = 3
Detections	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. Detections = 10

Spam Recipient Summary

Provides a summary of spam violations on specific endpoints. Example: name of endpoint, total number of instances of viruses/malware on the endpoint

Table B-42. Spam Recipient Summary Data View

Data	Description
Recipient	Displays the name of the recipient who receives spam.

Data	Description
Detections	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. Detections = 10

Spam Detection Over Time Summary

Provides a summary of spam detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints affected by spam, the total number of spam violations on the network

Table B-43. Spam Detection Over Time Summary Data View

Data	Description
Summary Time	Displays the time that the summary of the data occurs.
Unique Recipient Domains	Displays the total number of unique recipient domains affected by spam. Example: A managed product detects 10 violation instances of the same spam from 2 domains on 1 recipient domain. Unique Recipient Domains = 1
Unique Recipients	Displays the number of unique recipients receiving spam from the specified domain. Example: A managed product detects 10 violation instances of spam from the same domain on 3 computers. Unique Recipients = 3
Detections	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. Detections = 10

Detailed Spam Information

Provides specific information about the spam violations on your network. Example: the managed product that detects the content violation, the name of the specific policy in violation, the total number of spam violations on the network

TABLE B-44. Detailed Spam Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Recipient	Displays the recipients of email containing spam.
Sender	Displays the sender of email containing spam.
Subject	Displays the content of the subject line of the email containing spam.
Policy	Displays the name of the policy the email violates.
Action	Displays the type of action managed products take against spam found in email. Example: deliver, forward, strip
Detections	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. Detections = 10

Spam Connection Information

Provides specific information about the source of spam on your network. Example: the managed product that detects the spam violation, the specific action managed products take against spam violations, the total number of spam violations on the network

TABLE B-45. Spam Connection Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Source IP	Displays the IP address of the mail server where spam originates.
Filter Type	Displays the type of filter that detects the email in violation. Example: Real-time Blackhole List (RBL+), Quick IP List (QIL)
Action	Displays the type of action managed products take against spam to prevent spam from entering the email server. Example: drop connection, bypass connection
Detections	Displays the total number of spam violations managed products detect. Example: A managed product detects 10 violation instances of the same spam on one computer. Detections = 10

Policy/Rule Violation Information

Displays summary and detailed data about policy/rule violations that managed products detect on your network.

Detailed Firewall Violation Information

Provides specific information about the firewall violations on your network. Example: the managed product that detects the firewall violation, specific information about the source and destination, the total number of firewall violations on the network

TABLE B-46. Detailed Firewall Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is under attack.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Event Type	Displays the type of event that triggers the violation. Example: intrusion, policy violation
Risk Level	Displays the Trend Micro assessment of risk to your network. Example: high security, low security, medium security
Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol the intrusion uses. Example: HTTP, SMTP, FTP

Data	Description
Source IP	Displays the IP address of the computer attempting an intrusion on your network.
Endpoint Port	Displays the port number of the computer under attack.
Endpoint IP	Displays the IP address of the computer under attack.
Target Application	Displays the application the intrusion has targeted.
Description	Detailed description of the incident by Trend Micro.
Action	Displays the type of action managed products take against policy violations. Example: file cleaned, file quarantined, file passed
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Network Content Inspection Information

Provides specific information about the network content violations on your network.

Table B-47. Network Content Inspection Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

DATA	DESCRIPTION
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is under attack.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Traffic/Connection	Displays the direction of violation entry.
Endpoint IP	Displays the IP address of the computer under attack.
Endpoint Port	Displays the port number of the computer under attack.
Destination IP	Displays the IP address of the computer that is a possible target on your network.
Endpoint Port	Displays the port number of the computer under attack.
Target Process	Displays the process the violation has targeted.
Action	Displays the type of action managed products take against policy violations.
Pattern Type	Displays the type of pattern matching the violation.

Detailed Endpoint Security Violation Information

Provides specific information about endpoint security violations on your network.

TABLE B-48. Detailed Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

Data	Description
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Endpoint	Displays the host name of the computer in compliance of the policy/rule.
Endpoint IP	Displays the IP address of the computer in compliance of the policy/rule.
Endpoint MAC	Displays the MAC address of the computer in compliance of the policy/rule.
Policy/Rule	Displays the name of the policy/rule in compliance.
Service	Displays the name of the service/program in compliance of the policy/rule.
User	Displays the user name logged on to the endpoint when a managed product detects a policy/rule compliance.
Enforcement Action	Displays the action enforced by the policy/rule.
Remediation Action	Displays the action that helps stop payload caused by the violation.
Description	Detailed description of the incident by Trend Micro.
Detections	Displays the total number of policy/rule compliances managed products detect. Example: A managed product detects 10 compliance instances of the same type on one computer. Detections = 10

Detailed Endpoint Security Compliance Information

Provides specific information about the endpoint security compliance instances on your network. Example: the managed product that detects the security compliance, the name of the specific policy in compliance, the total number of security compliances on the network

TABLE B-49. Detailed Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Endpoint	Displays the host name of the computer in compliance of the policy/rule.
Endpoint IP	Displays the IP address of the computer in compliance of the policy/rule.
Endpoint MAC	Displays the MAC address of the computer in compliance of the policy/rule.
Policy/Rule	Displays the name of the policy/rule in compliance.
Service	Displays the name of the service/program in compliance of the policy/rule.
User	Displays the user name logged on to the endpoint when a managed product detects a policy/rule compliance.
Description	Detailed description of the incident by Trend Micro.

Data	Description
Detections	Displays the total number of policy/rule compliances managed products detect. Example: A managed product detects 10 compliance instances of the same type on one computer. Detections = 10

Detailed Application Activity

Displays overall information about application activity on your network. Example: the managed product which detects the security compliance, the name of the specific policy in compliance, the total number of security compliances on the network

Table B-50. Detailed Application Activity Data View

Data	Description
Received	The time at which Control Manager receives data from the managed product.
Generated	The time at which the managed product generates data.
Product Entity	The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	The name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
VLAN ID	Displays the VLAN ID (VID) of the source from which the suspicious threat originates.
Detected By	Displays the filter, scan engine, or managed product which detects the suspicious threat.
Traffic/Connection	Displays the direction of network traffic or the position on the network the suspicious threat originates.

DATA	DESCRIPTION
Protocol Group	Displays the broad protocol group from which a managed product detects the suspicious threat. Example: FTP, HTTP, P2P
Protocol	Displays the protocol from which a managed product detects the suspicious threat. Example: ARP, Bearshare, BitTorrent
Description	Detailed description of the incident by Trend Micro.
Endpoint Host	Displays the host name of the computer in compliance of the policy/rule.
Source IP	Displays the IP address of the source from which the suspicious threat originates.
Source MAC	Displays the MAC address of the source from which the suspicious threat originates.
Source Port	Displays the port number of the source from which the suspicious threat originates.
Source IP Group	Displays the IP address group of the source where the violation originates.
Source Network Zone	Displays the network zone of the source where the violation originates.
Endpoint IP	Displays the IP address of the endpoint the suspicious threat affects.
Endpoint Port	Displays the port number of the endpoint the suspicious threat affects.
Endpoint MAC	Displays the MAC address of the endpoint the suspicious threat affects.
Endpoint Group	Displays the IP address group of the endpoint the suspicious threat affects.
Endpoint Network Zone	Displays the network zone of the endpoint the suspicious threat affects.

DATA	DESCRIPTION
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10
Threat Type	Displays the specific type of security threat managed products detect.
Detection Severity	Displays the severity level of the incident.
IP Address (Interested)	Displays the IP address of the target endpoint (source or destination). For an exchange occurring within the network, the Interested IP is the source IP address. If the traffic is an external traffic, the Interested IP is the destination IP address.
IP Address (Peer)	Displays the IP address opposite of the Interested IP. For example, if the Interested IP is the source IP address, then the Peer IP is the destination IP address.
Matching Classified Events	Displays the log count matching the same aggregated rule.
Aggregated Matching Classified Events	Displays the aggregated log count matching the same rule.
Network Group	Displays the name of the group.
Host Severity	Displays the host severity.
Log ID	Displays the log ID.

Detailed Behavior Monitoring Information

Provides specific information about events on your network that are related to Behavior Monitoring.

TABLE B-51. Detailed Behavior Monitoring Information Data View

DATA	DESCRIPTION
Time Received From Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Host	Displays the IP address or host name of the computer accessed.
Risk Level	Displays the Trend Micro assessment of risk to your network.
Log Type	Displays the type of log that triggers the violation.
Policy	Displays the name of the policy triggered by the violation.
Subject	Displays the specific file, including its directory.
Event Type	Displays the type of violation.
Target	Displays the path or directory specified by the Event Type.
Action	Displays the action taken by the managed product.
Operation	Displays read/write or execute operation.
Endpoint	Displays the host name of the computer under attack.
Endpoint IP	Displays the IP address of the computer under attack.

Device Access Control Information

Provides specific information about events on your network that are related to Device Access Control.

TABLE B-52. Device Access Control Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

Data	Description
	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed, that is under attack.
Product	Displays the name of the managed product. Example: OfficeScan
Target Process	Displays the process the violation has targeted.
File Name	Displays the name of the file.
Device Type	Displays the type of device accessed.
Permission	Displays the permission type.

Detailed Endpoint Application Control Violation Information

Provides specific information about application violations on your network. For example: the violated policy and rule name, the specific information about the endpoint and application

Table B-53. Detailed Endpoint Application Control Violation Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
User Name	Displays the name of the user account.
Endpoint	Displays the host name of the affected computer.
Action	Displays the action type: Allow, Block, Lockdown.
Application	Displays the name of the application that triggers the rule.

DATA	DESCRIPTION
Version	Displays the version information.
Policy	Displays the name of the Trend Micro™ Endpoint Application Control™ policy.
Rule	Displays the name of the rule for application usage.
Server	Displays the host name of the Endpoint Application Control server.
Connection Status	Displays the status of the specific Endpoint Application Control server connected to.
Endpoint IP Address	Displays the IP address of the computer in compliance of the policy/rule.
SHA-1	Displays the file signature.
Command	Displays the type of command issued.
Process Owner	Displays the user name of the account that issued the command.

Detailed Intrusion Prevention Information

Use the information to achieve timely protection against known and zero-day attacks, defend against web application vulnerabilities, and identify malicious software accessing the network.

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Server	Displays the host name of the managed product server.
Source IP	IP address of the intrusion source
Source MAC	MAC address of the intrusion source

DATA	DESCRIPTION
Source Port	Port number of the intrusion source
Destination IP	IP address of the intrusion destination
Destination MAC	MAC address of the intrusion destination
Destination Port	Port number of the intrusion destination
MAC (Interested)	Displays the MAC address of the target endpoint (source or destination). For an intrusion occurring within the network, the Interested MAC is the source MAC address. If the traffic is an external traffic, the Interested IP is the destination MAC address.
Mode	Inline or tap
Action	Displays the type of action managed products take against intrusions. Example: prevent, detect
Direction	Communication direction
Rank	Intrusion rank
Severity	Intrusion severity
Protocol	Protocol used during intrusion
Application	Vulnerable applications
Reason	Reason for denied packets

Integrity Monitoring Information

Use the information to monitor specific areas on a computer for changes, such as installed software, running services, processes, files, directories, listening ports, registry keys, and registry values.

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.

DATA	DESCRIPTION
Generated	Displays the time that the managed product generates data.
Server	Displays the host name of the managed product server.
Change	Computer changes
User	User logged on to the computer
Process	Processes changed
Type	Type of registry key
Key	Registry key
Rank	Integrity rank
Severity	Severity of changes

Web Violation/Reputation Information

Displays summary and detailed data about Internet violations that managed products detect on your network.

Overall Web Violation Summary

Provides a summary of web violations of specific policies. Example: name of the policy in violation, the type of filter/blocking to stop access to the URL, the total number of web violations on the network

TABLE B-54. Overall Web Violation Summary Data View

DATA	DESCRIPTION
Policy	Displays the name of the policy the URL violates.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, web blocking

DATA	DESCRIPTION
Unique Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4
Unique URLs	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. Unique URLs = 1
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on 1 computer. Detections = 10

Web Violation Endpoint Summary

Provides a summary of web violation detections from a specific endpoint. Example: IP address of the endpoint in violation, number of policies in violation, the total number of web violations on the network

TABLE B-55. Web Violation Endpoint Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of endpoints in violation of web policies.
Unique Policies	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies = 1

DATA	DESCRIPTION
Unique URLs	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. Unique URLs = 1
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. Detections = 10

Web Violation URL Summary

Provides a summary of web violation detections from specific URLs. Example: name of the URL causing the web violation, the type of filter/blocking to stop access to the URL, the total number of web violations on the network

TABLE B-56. Web Violation URL Summary Data View

DATA	DESCRIPTION
URL	Displays the URL violating a web policy.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, web blocking
Unique Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4

DATA	DESCRIPTION
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. Detections = 10

Web Violation Filter/Blocking Type Summary

Provides a summary of the action managed products take against web violations. Example: the type of filter/blocking to stop access to the URL, the total number of web violations on the network

TABLE B-57. Web Violation Filter/Blocking Type Summary Data View

DATA	DESCRIPTION
Blocking Category	Displays the broad type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Anti-spyware
Filter/Blocking Type	Displays the specific type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Virus/Malware
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. Detections = 10

Web Violation Detection Over Time Summary

Provides a summary of web violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints in violation, the total number of web violations on the network

TABLE B-58. Web Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.
Unique Policies	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies = 1
Unique Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4
Unique URLs	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. Unique URLs = 1
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. Detections = 10

Web Violation Detection Summary

Provides a summary of web violation detections over a period of time (daily, weekly, monthly). Example: time and date of when summary data was collected, number of endpoints in violation, the total number of web violations on the network

TABLE B-59. Web Violation Detection Summary Data View

DATA	DESCRIPTION
Unique Policies	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies = 1
Unique Endpoints	Displays the number of unique endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. Unique Endpoints = 4
Unique URLs	Displays the number of unique URLs in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on one computer. Unique URLs = 1
Unique Users/IPs	Displays the number of unique users or IP addresses of endpoints in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL from one user. Unique Users/IPs = 1
Unique User Groups	Displays the number of unique user groups for users in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL from one user group. Unique User Groups = 1

DATA	DESCRIPTION
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. Detections = 10

Detailed Web Violation Information

Provides specific information about the web violations on your network. Example: the managed product that detects the web violation, the name of the specific policy in violation, the total number of web violations on the network

TABLE B-60. Detailed Web Violation Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP
URL	Displays the name of the URL that violates a web policy.
User/IP	Displays the user or IP address of the endpoint that violates a policy.
User Group	Displays the user group for the user that violates a policy.

DATA	DESCRIPTION
Endpoint Host	Displays the IP address or host name of the endpoint that violates a policy.
Product Host	Displays the IP address or host name of the managed product which detects the violation.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, web blocking
Blocking Rule	Displays the blocking rule preventing access to the URL in violation. Example: URL blocking
Policy	Displays the name of the policy the URL violates.
File	Displays the name of the file that violates the policy.
Web Reputation Rating	Displays the relative safety, as a percentage, of a website according to Trend Micro.
Action	Displays the type of action managed products take against policy violations. Example: pass, block
Detections	Displays the total number of web violations managed products detect. Example: A managed product detects 10 violation instances of the same URL on one computer. Detections = 10

Detailed Web Reputation Information

Displays overall information about application activity on your network. Example: the managed product that detects the security compliance, the name of the specific policy in compliance, the total number of security compliance on the network

TABLE B-61. Detailed Web Reputation Information Data View

DATA	DESCRIPTION
Received	The time at which Control Manager receives data from the managed product.
Generated	The time at which the managed product generates data.
Product Entity	The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	The name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
VLAN ID	Displays the VLAN ID (VID) of the source from which the suspicious threat originates.
Detected By	Displays the filter, scan engine, or managed product which detects the suspicious threat.
Traffic/Connection	Displays the direction of network traffic or the position on the network the suspicious threat originates.
Protocol Group	Displays the broad protocol group from which a managed product detects the suspicious threat. Example: FTP, HTTP, P2P
Protocol	Displays the protocol from which a managed product detects the suspicious threat. Example: ARP, Bearshare, BitTorrent
Description	Detailed description of the incident by Trend Micro.
Endpoint	Displays the host name of the computer in compliance of the policy/rule.
Source IP	Displays the IP address of the source from which the suspicious threat originates.
Source MAC	Displays the MAC address of the source from which the suspicious threat originates.

DATA	DESCRIPTION
Source Port	Displays the port number of the source from which the suspicious threat originates.
Source IP Group	Displays the IP address group of the source where the suspicious threat originates.
Source Network Zone	Displays the network zone of the source where the suspicious threat originates.
Endpoint IP	Displays the IP address of the endpoint the suspicious threat affects.
Endpoint Port	Displays the port number of the endpoint the suspicious threat affects.
Endpoint MAC	Displays the MAC address of the endpoint the suspicious threat affects.
Endpoint Group	Displays the IP address group of the endpoint the suspicious threat affects.
Endpoint Network Zone	Displays the network zone of the endpoint the suspicious threat affects.
Policy/Rule	Displays the policy/rule the suspicious threat violates.
URL	Displays the URL considered a suspicious threat.
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10
C&C List Source	Displays the C&C list source that identified the C&C server.
C&C Risk Level	Displays the risk level of the C&C server.
Threat Type	Displays the specific type of security threat managed products detect.
Detection Severity	Displays the severity level of the incident.

DATA	DESCRIPTION
IP Address (Interested)	Displays the IP address of the target endpoint (source or destination). For an exchange occurring within the network, the Interested IP is the source IP address. If the traffic is an external traffic, the Interested IP is the destination IP address.
IP Address (Peer)	Displays the IP address opposite of the Interested IP. For example, if the Interested IP is the source IP address, then the Peer IP is the destination IP address.
Matching Classified Events	Displays the log count matching the same aggregated rule.
Aggregated Matching Classified Events	Displays the aggregated log count matching the same rule.
Network Group	Displays the name of the group.
Host Severity	Displays the host severity.
Log ID	Displays the log ID.
Attack Phase	Displays the phase with which the attack happened.
Remarks	Displays descriptions related to the attack.
C&C Server	Displays the name, URL, or IP address of the C&C server.
C&C Server Type	Displays the server type.
Sender	Displays the sender address where the transmission originated.
Recipient	Displays the destination address(es) of the transmission.
Subject	Displays the subject line of the email message containing the web URL.

Deep Discovery Information

Displays summary and detailed data about suspicious activity that managed products detect on your network.

Overall Suspicious Threat Summary

Provides specific information about suspicious threats on your network. Example: the policy/rule in violation, summary information about the source and destination, the total number of suspicious threats on the network

TABLE B-62. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Policy/Rule	Displays the name of the policy/rule in violation.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP
Unique Endpoints	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. Unique Sources = 3
Unique Recipients	Displays the number of unique email message recipients receiving content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. Unique Recipients = 2

DATA	DESCRIPTION
Unique Senders	Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. Unique Senders = 3
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections equals 10.
Mitigations	Displays the number of endpoints Network VirusWall Enforcer devices or Trend Micro™ Threat Mitigator™ take action against.
Cleaned Endpoints	Displays the total number of endpoints Trend Micro Threat Mitigator cleans.
Clean Endpoint Rate (%)	Displays the percentage of endpoints Trend Micro Threat Mitigator cleans compared to the total Detections.

Suspicious Source Summary

Provides a summary of suspicious threat detections from a specific source. Example: name of the source, summary information about the destination and rules/violations, the total number of suspicious threats on the network

TABLE B-63. Suspicious Source Summary Data View

DATA	DESCRIPTION
Source IP	Displays the IP addresses of sources where suspicious threats originate.

DATA	DESCRIPTION
Unique Policies/ Rules	Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies/Rules = 1
Unique Endpoints	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. Unique Endpoints = 2
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Suspicious Riskiest Endpoints Summary

Provides a summary of the endpoints with the most suspicious threat detections. Example: name of the destination, summary information about the source and rules/ violations, the total number of suspicious threats on the network

TABLE B-64. Suspicious Threat Riskiest Endpoints Summary Data View

DATA	DESCRIPTION
Endpoint IP	Displays the IP addresses of computers affected by suspicious threats.

DATA	DESCRIPTION
Unique Policies/ Rules	Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies/Rules = 1
Unique Sources	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. Unique Sources = 3
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Suspicious Riskiest Recipient Summary

Provides a summary of the recipients with the most suspicious threat detections. Example: name of the recipient, summary information about the senders and rules/ violations, the total number of suspicious threats on the network

TABLE B-65. Suspicious Riskiest Recipient Summary Data View

DATA	DESCRIPTION
Recipient	Displays the email address of the recipient affected by the suspicious threat.

DATA	DESCRIPTION
Unique Policies/ Rules	Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies/Rules = 1
Unique Senders	Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. Unique Senders = 3
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Suspicious Sender Summary

Provides a summary of suspicious threat detections from a specific sender. Example: name of the sender, summary information about the recipient and rules/violations, the total number of suspicious threats on the network

TABLE B-66. Suspicious Sender Summary Data View

DATA	DESCRIPTION
Sender	Displays the email address for the source of policy/rule violations.
Unique Policies/ Rules	Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies/Rules = 1

DATA	DESCRIPTION
Unique Recipients	Displays the number of unique email message recipients receiving content that violate managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. Unique Recipients = 2
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Suspicious Threat Protocol Detection Summary

Provides a summary of suspicious threat detections over a specific protocol. Example: name of the protocol, summary information about the source and destination, the total number of suspicious threats on the network

TABLE B-67. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Protocol	Displays the name of the protocol over which the suspicious threat occurs. Example: HTTP, FTP, SMTP
Unique Policies/ Rules	Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies/Rules = 1

DATA	DESCRIPTION
Unique Endpoints	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. Unique Sources = 3
Unique Recipients	Displays the number of unique email message recipients receiving content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. Unique Recipients = 2
Unique Senders	Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. Unique Senders = 3
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Suspicious Threat Detection Over Time Summary

Provides a summary of suspicious threat detections over a period of time (daily, weekly, monthly). Example: time and date when summary data was collected, summary

information about the source and destination, the total number of suspicious threats on the network

TABLE B-68. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.
Unique Policies/ Rules	Displays the number of unique policies/rules the source computer violates. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. Unique Policies/Rules = 1
Unique Endpoints	Displays the number of unique computers affected by the suspicious threat. Example: A managed product detects 10 suspicious threat instances of the same type on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique sources where suspicious threats originate. Example: A managed product detects 10 suspicious threat instances of the same type originating from 3 computers. Unique Sources = 3
Unique Recipients	Displays the number of unique email message recipients receiving content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy on 2 computers. Unique Recipients = 2

Data	Description
Unique Senders	Displays the number of unique email message senders sending content that violates managed product suspicious threat policies. Example: A managed product detects 10 suspicious threat violation instances of the same policy coming from 3 computers. Unique Senders = 3
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Detailed Suspicious Threat Information

Provides specific information about suspicious threats on your network. Example: the managed product that detects the suspicious threat, specific information about the source and destination, the total number of suspicious threats on the network

Table B-69. Detailed Suspicious Threat Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Mitigation Host	Displays the host name of the mitigation server (Network VirusWall Enforcer or Threat Mitigator)

DATA	DESCRIPTION
Traffic/Connection	Displays the direction of network traffic or the position on the network the suspicious threat originates.
Protocol Group	Displays the broad protocol group from which a managed product detects the suspicious threat. Example: FTP, HTTP, P2P
Protocol	Displays the protocol from which a managed product detects the suspicious threat. Example: ARP, Bearshare, BitTorrent
Destination IP Address	Displays the IP address of the endpoint the suspicious threat affects.
Destination Host	Displays the host name of the endpoint the suspicious threat affects.
Destination Port	Displays the port number of the endpoint the suspicious threat affects.
Destination MAC Address	Displays the MAC address of the endpoint the suspicious threat affects.
Destination OS	Displays the operating system running on the target host.
Destination User <x>	Displays the name used to log on to the target host. <x> is the user name
Logon (Destination User <x>)	Displays the logon timestamp. <x> represents the number of logon times and the specific timestamp.
Source IP Address	Displays the IP address of the source where the suspicious threat originates.
Source Host Name	Displays the host name of the source where the suspicious threat originates.
Source Port	Displays the port number of the source where the suspicious threat originates.
Source MAC Address	Displays the MAC address of the source where the suspicious threat originates.

Data	Description
Source OS	Displays the operating system running on the target source host.
Source User <x>	Displays the name used to log on to the target source host. <x> is the user names
Logon (Source User <x>)	Displays the logon timestamp on the source. <x> represents the number of logon times and the specific timestamp.
Source Domain	Displays the domain of the source where the suspicious threat originates.
Security Threat Type	Displays the specific type of security threat managed products detect. Example: virus, spyware/grayware, fraud
Policy/Rule	Displays the policy/rule the suspicious threat violates.
Recipient	Displays the recipient of the suspicious threat.
Sender	Displays the sender of the suspicious threat.
Subject	Displays the content of the subject line of the email containing spyware/grayware.
Attachment File Name	Displays the file and extension name of the attachment.
Attachment File Type	Displays the file type of the attachment.
Attachment SHA-1	Displays the SHA-1 hash of the attachment.
URL	Displays the URL considered a suspicious threat.
User	Displays the user name logged on to the destination when a managed product detects a suspicious threat.
IM/IRC User	Displays the instant messaging or IRC user name logged on when Deep Discovery Inspector detects a violation.

DATA	DESCRIPTION
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the suspicious threat originates.
File	Displays the name of the suspicious file.
File in Compressed File	Displays whether the suspicious threat originates from a compressed file.
Archive SHA-1	Displays the SHA-1 hash of the archived file.
Archive File Type	Displays the type of the archived file.
Shared Folder	Displays whether the suspicious threat originates from a shared folder.
SHA-1	Displays the SHA-1 hash.
Mitigation Action	Displays the action the mitigation server takes against suspicious threats. Example: File cleaned, File dropped, File deleted
Mitigation Result	Displays the result of the action the mitigation server takes against suspicious threats.
Source IP Group	Displays the IP address group of the source where the suspicious threat originates.
Source Network Zone	Displays the network zone of the source where the suspicious threat originates.
Endpoint Group	Displays the IP address group of the endpoint the suspicious threat affects.
Endpoint Network Zone	Displays the network zone of the endpoint the suspicious threat affects.
Detections	Displays the total number of policy/rule violations managed products detect. Example: A managed product detects 10 violation instances of the same type on one computer. Detections = 10

Data	Description
C&C List Source	Name of the list that contains the callback address • Global Intelligence (Trend Micro Global Intelligence network, including Smart Protection Network) • Virtual Analyzer in managed products • User-defined C&C list configured in managed products
C&C Risk Level	Severity level of the callback
Remarks	Displays descriptions related to the attack.
C&C Server	Displays the name, URL, or IP address of the C&C server.
C&C Server Type	Displays the server type.
Malware Type	Displays the malware type.

Detailed Mitigation Information

Provides specific information about tasks carried out by mitigation servers to resolve threats on your network.

Table B-70. Detailed Mitigation Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.
Mitigation Entity	Displays the entity display name of the mitigation server (Network VirusWall Enforcer or Threat Mitigator)
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Endpoint IP	Displays the IP address of the endpoint the threat affects.
Endpoint	Displays the host name of the endpoint the threat affects.

DATA	DESCRIPTION
Data Source	Displays the Deep Discovery product or task that generated threat event information.
Data Source Host	Displays the host name of the Deep Discovery product that generated threat event information.
Threat Event	Displays threat-related events logged by the mitigation server. See the following reference: http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm
Mitigation Status	Displays threat events by status groups. See the following reference: http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/help/info/threat_event_logs.htm
Mitigation Details	Displays details about threat events. See the following reference: http://docs.trendmicro.com/all/ent/tms/v2.6/en-us/tmtm_2.6_olh/start.htm#help/info/mitigation_status.htm
Detections	Displays the total number of threats managed products detect.
Detailed Information	Displays details about threats.

Detailed Correlation Information

Provides specific information about detailed threat analyses and remediation recommendations.

TABLE B-71. Detailed Correlation Information Data View

DATA	DESCRIPTION
Generated	Displays the time that the managed product generates data.
IP Address	Displays the IP address of the endpoint the suspicious threat affects.
Network Group	Displays the monitored network group.

Data	Description
Protocol	Displays the broad protocol group from which a managed product detects the suspicious threat.
Threat Type	Displays the specific type of security threat managed products detect. Example: virus, spyware/grayware, fraud
Severity	Displays the host severity.
Detection	Displays the type of detection, based on correlation rules
Details	Displays remarks or comments related to the detection.
MAC Address	Displays the MAC address of the endpoint the suspicious threat affects.
Host Name	Displays the host name of the endpoint the suspicious threat affects.
Correlation Rule ID	Displays the rule ID.

Advanced Threat Information

Displays summary and detailed data about advanced persistent threats and targeted attacks that managed products detect on your network.

Detailed C&C Callback Information

Provides specific information about detected C&C callback events from the network.

Table B-72. Detailed C&C Callback Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Generated	Displays the time that the managed product generates data.

DATA	DESCRIPTION
Compromised Host	IP address, host name, or email address that attempted a callback
Callback Address	The object from/to which a compromised host attempted a callback
C&C List Source	The source of the list containing C&C addresses • Global Intelligence (Trend Micro Global Intelligence network, including Smart Protection Network) • Analyzers (Virtual Analyzer and Network Content Inspection Engine) in managed products • User-defined C&C list configured in Control Manager and in the managed product, such as Deep Discovery Inspector
Network Groups	Monitored network groups as defined by the administrators of managed products, such as Deep Discovery Inspector
C&C Risk Level	• **High**: Known malicious or involved in high-severity connections • **Medium**: IP address/domain/URL is unknown to reputation service • **Low**: Reputation service indicates previous compromise or spam involvement
C&C Server Location	Region and country where the C&C server is located
First Monitored	Date and time the callback address was first detected by Trend Micro
Last Activity	Date and time the callback address was last contacted by a compromised host
Malware Families	Malware names associated with the callback address
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

Data	Description
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

Detailed Suspicious File Information

Provides specific information about suspicious files detected in the network.

Table B-73. Detailed Suspicious File Information Data View

Data	Description
Received	Displays the time that Control Manager receives data from the managed product.
Detected	Displays the time that the managed product detected the suspicious object
Endpoint	The endpoint where the suspicious object was found.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product Entity	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Endpoint IP Address	IP address of the endpoint
Endpoint Host Name	Host name of the endpoint
File Type	File type of suspicious object
File SHA-1	SHA-1 hash value of the suspicious object
File Path	File path and name of suspicious object

DATA	DESCRIPTION
C&C List Source	The source of the list containing C&C addresses • Global Intelligence (Trend Micro Global Intelligence network, including Smart Protection Network) • Analyzers in managed products (Virtual Analyzer or Network Content Inspection Engine relevance rules) • User-defined C&C list configured in Control Manager and in the managed product, such as Deep Discovery Inspector
Action	Action to address the suspicious object
Scan Type	Scan type that detected the suspicious object
Created	Displays the time the suspicious object was created in the endpoint
Modified	Displays the time the suspicious object was modified in the endpoint

Overall Threat Information

Displays summary and statistical data about the overall threat landscape of your network.

Network Security Threat Analysis Information

Displays information for overall security threats affecting your desktops. Examples: name of the security threat, total number of security threat detections, number of endpoints affected

TABLE B-74. Network Security Threat Analysis Information Data View

DATA	DESCRIPTION
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing

DATA	DESCRIPTION
Security Threat	Displays the name of security threat managed products detect.
Entry Type	Displays the entry point for the security threat that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)
Unique Endpoints	Displays the number of unique computers affected by the security threat/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique computers where security threats/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. Unique Sources = 3
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Network Protection Boundary Information

Displays information for a broad overview of security threats affecting your entire network. Examples: managed product network protection type (gateway, email), type of security threat, number of endpoints affected

TABLE B-75. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Product Category	Displays the category to which the managed product belongs. Example: desktop products, mail server products, network products
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Unique Endpoints	Displays the number of unique computers affected by the security threat/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique computers where security threats/ violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. Unique Sources = 3
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Security Threat Entry Analysis Information

Displays information with the entry point of security threats as the focus. Examples: managed product network protection type (gateway, email, desktop), name of the security threat, time of the last security threat detection

TABLE B-76. Security Threat Entry Analysis Information Data View

DATA	DESCRIPTION
Entry Type	Displays the point of entry for security threats managed products detect. Example: Virus found in file, FTP, File transfer
Product	Displays the name of the managed product which detects the security threat. Example: OfficeScan, ScanMail for Microsoft Exchange
Security Threat Category	Displays the specific category for security threats managed products detect. Example: Antivirus, Antispyware, Content filtering
Unique Endpoints	Displays the number of unique computers affected by the security threat/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. Unique Endpoints = 2
Unique Sources	Displays the number of unique computers where security threats/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. Unique Sources = 3
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10

Security Threat Source Analysis Information

Displays information with the security threat source as the focus. Examples: name of the security threat source, the broad range of how the security threat enters your network, number of endpoints affected

TABLE B-77. Security Threat Source Analysis Information Data View

DATA	DESCRIPTION
Source Host	Displays the name of the computer where the cause of the security threat/violation originates.
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Security Threat	Displays the name of security threat managed products detect.
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10
Detected	Displays the time and date of the last security threat/violation detection on the computer affected the security threat/violation.

Security Threat Endpoint Analysis Information

Displays information with affected endpoints as the focus. Examples: name of the endpoint, the broad range of how the security threat enters your network, number of endpoints affected

TABLE B-78. Security Threat Endpoint Analysis Information Data View

DATA	DESCRIPTION
Endpoint	Displays the name of the computer affected by the security threat/ violation.

DATA	DESCRIPTION
Security Threat Category	Displays the broad category of the security threat managed products detect. Example: Antivirus, Antispyware, Antiphishing
Security Threat Name	Displays the name of security threat managed products detect.
Detections	Displays the total number of security threats/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. Detections = 10
Detected	Displays the time and date of the last security threat/violation detection on the computer affected the security threat/violation.

Data View: Data Protection Information

Displays information about Data Loss Prevention (DLP), including DLP incidents and DLP template matches.

Data Loss Prevention Information

Displays information about DLP incidents, template matches, and incident sources collected from the managed products.

DLP Incident Information

TABLE B-79. DLP Incident Information

DATA	DESCRIPTION
Received	Displays the time when Control Manage r received the log.

DATA	DESCRIPTION
Generated	Displays the time when the log data was generated in the managed product.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with an agent (for example OfficeScan agent) installed.
Managing Server	Displays the entity display name for a managed product to which an endpoint is registered. Control Manager identifies managed products using the managed product's entity display name.
Endpoint	Displays the IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Incident Source (User)	Displays the logged on user name.
Incident Source (Sender)	Displays the source email address.
Recipient	Displays the destination email address.

Data	Description
Subject	Displays the subject of the email message.
File Location	Displays the location and the name of the file.
File	Displays the name of the file from which the incident was triggered.
Rule	Displays the name of the rule triggered by the incident.
Template	Displays the name of the template in which a template match was triggered.
Channel	Displays the entity through which a digital asset was transmitted.
Destination	Displays the destination.
Action	Displays the action taken on the incident.
Incidents	Displays the number of incidents.

DLP Template Match Information

Table B-80. DLP Template Match Information

Data	Description
ID	Displays the unique ID for the log.
Received	Displays the time when the managed product received the incident information.
Generated	Displays the time when the incident was triggered.
Product Entity/ Endpoint	This data column displays one of the following: • The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name. • The IP address or host name of a computer with an agent (for example OfficeScan agent) installed.

DATA	DESCRIPTION
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Product/Endpoint IP	This data column displays one of the following: • The IP address of the server on which the managed product installs. • The IP address of a computer with an agent (for example OfficeScan agent) installed.
Product/Endpoint MAC	This data column displays one of the following: • The MAC address of the server on which the managed product installs. • The MAC address of a computer with an agent (for example OfficeScan agent) installed.
Managing Server	Displays the entity display name for a managed product to which an endpoint is registered. Control Manager identifies managed products using the managed product's entity display name.
Endpoint	Displays the IP address or host name of a computer with an agent (for example OfficeScan agent) installed.
Incident Source (User)	Displays the logged on user name.
Recipient	Displays the destination email address.
Subject	Displays the subject of the email message.
File Location	Displays the location and the name of the file.
File	Displays the name of the file from which the incident was triggered.
Rule	Displays the name of the rule triggered by the incident.
Template	Displays the name of the template in which a template match was triggered.
Channel	Displays the entity through which a digital asset was transmitted.

Data Discovery Information

Displays information about data discovery information.

Data Discovery Data Loss Prevention Detection Information

TABLE B-81. Data Discovery Data Loss Prevention Detection Information

DATA	DESCRIPTION
Received	Displays the time when Control Manager received the log.
Generated	Displays the time when the log data was generated in the managed product.
Rule	Displays the name of the rule triggered by the incident.
Endpoint	Displays the IP address or host name of a computer where Data Loss Prevention detected the transmission.
Domain	Displays the domain to which the managed product belongs.
User	Displays the name of the user who initiates the activity.
User Domain	Displays the name of the domain where the user belongs.
File Path	Displays the full path of the location containing the digital asset, or channel (if no source is available).
File	Displays the full file name.
Template	Displays the exact rule name(s) and template(s) triggered by the incident.
Action	Displays the action taken on the transmission.
Details	Displays additional information such as the reason a user has provided for continuing to transfer sensitive data.

Data Discovery Endpoint Information

TABLE B-82. Data Discovery Endpoint Information

DATA	DESCRIPTION
Generated	Displays the time when the log data was generated in the managed product.
Endpoint	Displays the IP address or host name of a computer where Data Loss Prevention detected the transmission.
Device Class	Displays the name of the device category as shown in Windows Device Manager.
Device Display Name	Displays the display name of the device, as shown in Windows Device Manager.
Provider	Displays the name of the company that provides the device.

Appendix C

IPv6 Support in Control Manager

This appendix is required reading for users who plan to deploy Control Manager in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in Control Manager.

Trend Micro assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.

IPv6 support for Control Manager started in this version 6.0 Service Pack 3. Earlier Control Manager versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading the Control Manager server that satisfies the IPv6 requirements.

Control Manager Server Requirements

The IPv6 requirements for the Control Manager server are as follows:

- The server must be installed on Windows Server 2008 (or newer). It cannot be installed on Windows Server 2003 because this operating system only supports IPv6 addressing partially.
- Install the IPv4 and IPv6 stacks, and enable the IPv6 stack.

IPv6 Server Limitations

The following table lists the limitations for IPv6 support:

TABLE C-1. IPv6 Support Limitations

ITEM	LIMITATION
Dual IP stacks	Control Manager only supports dual IP stacks. IPv6 support may not work properly if the IPv4 stack is removed.
IPv4 loopback interface	The IPv4 loopback interface is required. To verify that the TCP/IP software is working properly, ping `127.0.0.1`.
Windows Server 2008	Windows Server 2008 (or newer) is required for IPv6 support.
MCP agent	IPv6 support only works for MCP agents. It does not work for Control Manager 2.x agents.
IPv6 address format	The **%** character is not supported for IPv6 addresses.
Control Manager report	IPv6 addresses may not display correctly in pre-defined reports.

Configuring IPv6 Addresses

The web console allows you to configure an IPv6 address. The following are some configuration guidelines.

- Control Manager accepts standard IPv6 address presentations.

  For example:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Control Manager also accepts link-local IPv6 addresses, such as:

  fe80::210:5aff:feaa:20a2

  WARNING!

  Exercise caution when specifying a link-local IPv6 address because even though Control Manager can accept the address, it might not work as expected under certain circumstances. For example, Control Manager cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- When the IPv6 address is part of a URL, enclose the address in square brackets ([]).

Screens That Display IP Addresses

IP addresses are shown on the following screens:

- **Product Directory**
- **Ad Hoc Query Results**
- **Managed Servers**

Appendix D

Checking Policy Status

Policy status allows administrators to check if Control Manager has successfully deployed a policy to its targets.

To check the policy deployment status, use one of the following methods:

- On the **Policy Management** screen, click a number in the policy list. The **Ad Hoc Query Results** screen appears.
- On the dashboard, click a number in the **Policy Status** widget. The **Ad Hoc Query Results** screen appears.
- Perform an Ad Hoc Query

Policy Status

The following table provides the descriptions and suggestions about each policy status:

TABLE D-1. Policy Status

POLICY STATUS	DESCRIPTION	SUGGESTIONS
Pending	Control Manager is processing the policy.	Wait a few minutes and then check the status again.
Without policy	Control Manager has not assigned a policy to this endpoint or managed product.	Assign a policy to the endpoint or managed product.
Deployed	Control Manager has successfully deployed the policy.	N/A
Endpoint unable to connect to server	• The endpoint did not receive the policy settings. • The server is currently busy.	• Check the connection status of the endpoint • Connect the endpoint to the company network • Wait for the updated policy status

Policy Status	Description	Suggestions
Inapplicable product settings	The managed product cannot process some of the policy settings.	• Verify the policy settings • Update to the latest policy template version • Check the settings on the managed product • Verify the IP address of the managed product on the **Managed Servers** screen If the IP address is incorrect, unregister and then register the managed product again to Control Manager. • Refer to the *Administrator's Guide* for the managed product
Unsupported endpoint	The endpoint does not support some features specified in the policy settings.	Upgrade the agent to a supported version.
Settings changed locally	Some settings on the endpoint or managed product do not comply with the settings specified in the policy because the managed product administrator has made some changes through the managed product console.	Verify the settings on the managed product console.
Unactivated product services	The managed product has not activated some of the services specified in the policy settings.	Activate the related services on the managed product.
Disabled product services	The managed product has disabled some of the services specified in the policy settings.	Enable the related services on the managed product.
Partially deployed	Control Manager has enforced a portion of the policy settings.	Wait a few minutes and then check the status again.

Policy Status	Description	Suggestions
Managed by [Control Manager server name]	Another Control Manager is currently managing the managed product.	Remove the managed product from the Managed Server list and add the managed product to the list again.
Invalid user name or password	The user name or password for authentication is incorrect.	Verify the user name or password.
Invalid product server or authentication information	The server name or the authentication information is incorrect.	Verify the server name and the authentication information.
Unable to automatically log on to product	Control Manager cannot use the single sign-on function to access the managed product.	• Check the single sign-on function in the Product Directory • Check the connection status of the MCP agent • Change the server connection type from **Automatic** to **Manual** in the **Managed Servers** list.
Web server configuration error	A web service error has occurred.	Check the IIS configuration.
Product communication error	Unable to access the product console.	• Check if you can connect to the managed product's web console. • Check the settings of the managed product.
Unable to connect to product	Control Manager cannot establish a connection with the managed product.	• Check the connection status of the managed product. • Check the network connection

Policy Status	Description	Suggestions
Unsupported product version	The managed product version is not supported.	Upgrade the managed product to a supported version.
Network configuration error	A network connection error has occurred.	Check the network connection.
System error. Error ID: [error ID number].	A system error has occurred.	Contact your Trend Micro support representative.

Index

D

E

F

N

O

P

S

T

W

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: CMEM66957/150518