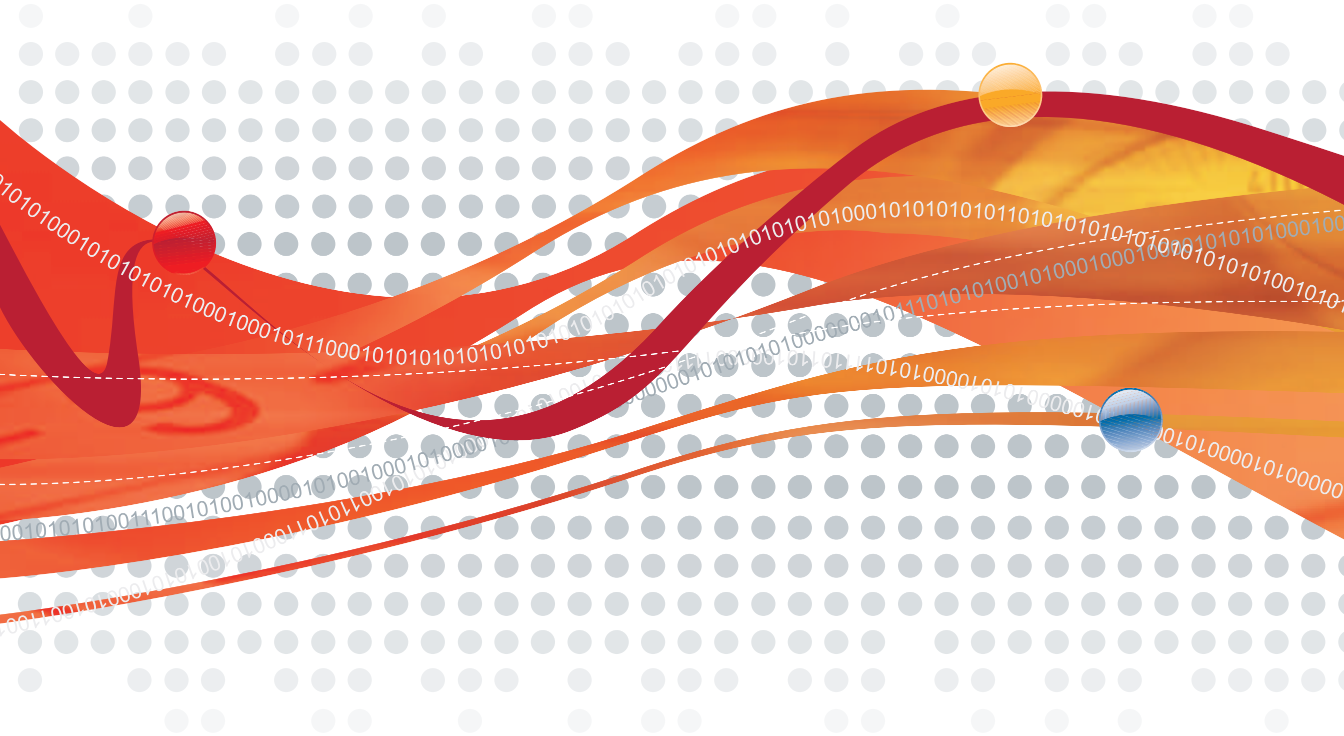
TREND MICRO™

Trend Micro Control Manager™ 5

Administrator's Guide



Control Manager

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

http://downloadcenter.trendmicro.com/

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. CMEM54525/100720

Release Date: August 2010

The *Administrator's Guide for Trend Micro*™ *Control Manager*™ is intended to introduce the main features of the software and provide details on how best to use and configure Control Manager. You should read through it prior to installing or using the software.

For technical support, please refer to *Contacting Technical Support on page 19-2* for technical support information and contact details. Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base at the Trend Micro website.

Contents

Preface

Section 1: Getting Started

Chapter 1: Introducing Trend Micro™ Control Manager™

Chapter 2: Getting Started with Control Manager

Chapter 3: Configuring User Access

Chapter 4: Product Directory Basics

Chapter 5: Downloading and Deploying Components

Section 2: Monitoring the Control Manager Network

Chapter 6: Working with the Dashboard and Widgets

Chapter 7: Using Command Tracking

Chapter 8: Using Notifications

Chapter 9: Working with Logs

Chapter 10: Working with Reports

Section 3: Administering Control Manager

Chapter 11: MCP and Control Manager Agents

Chapter 12: Managing Managed Products

Chapter 13: Activating Managed Products

Chapter 14: Managing Child Servers

Chapter 15: Administering the Database

Section 4: Services and Tools

Chapter 16: Using Trend Micro Services

Chapter 17: Using Control Manager Tools

Section 5: Removing Control Manager and Contacting Support

Chapter 18: Removing Trend Micro Control Manager

Chapter 19: Getting Support

Section 6: Appendixes

Appendix A: System Checklists

Appendix B: Data Views

Index

Preface

Preface

This *Administrator's Guide* introduces Trend Micro™ Control Manager™ 5.5, 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 on page xvi
- Control Manager Documentation on page xviii
- Document Conventions on page xix

What’s New in This Version

Trend Micro Control Manager 5.5 represents a significant advance in monitoring and management software for antivirus and content security products. Architectural improvements in this new version make Control Manager more flexible and scalable than ever before.

Control Manager 5.5 Features and Enhancements

The following new features and enhancements are available in version 5.5.

Threat Intelligence-Oriented Dashboard

The Summary screen has been replaced with an Adobe™ Flash™-based, customizable dashboard that supports Trend Micro widgets. Trend Micro widgets provide administrators with at-a-glance information. For detailed information the administrator can click the content in the widget. Retrieving the detailed widget content leverages the Control Manager Ad Hoc Query feature.

The widget framework integration for Control Manager supports the following widget types.

TABLE PREFACE-1. Control Manager Widget Types

WIDGET TYPE	DESCRIPTION
Summary	• Threat Detection Results (Virus/Spyware/Web Security/Content Security/Network Virus) • Policy Violation Detections • Product Component Status
Smart Protection Network	• Smart Protection Network Connections • Smart Protection Network Threat Statistics • Web Reputation Top Threat Sources • Web Reputation Top Threatened Users • Email Reputation Threat Map • File Reputation Threat Map • File Reputation Top Threat Detections

TABLE PREFACE-1. Control Manager Widget Types (Continued)

WIDGET TYPE	DESCRIPTION
Enterprise Security Metrics	• Control Manager Top Threats • Control Manager Threat Statistics • Product Application Compliance • Product Connection Status • OfficeScan Endpoint Connection Status

OfficeScan Integration Enhancements

Control Manager enhances integration with OfficeScan by providing consummate data synchronization between OfficeScan and Control Manager. Control Manager also supports OfficeScan 10.5 integration with the inclusion of Plug-in Manager Plug-in Programs component updates.

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 specifing a Plug-in Program for download, from Control Manager to OfficeScan, verify that Control Manager has already downloaded the Plug-in Program.

Improved Scalability

Control Manager 5.5 has significantly improved log processing speeds, compared to Control Manager 5.0. With the improved log processing speeds, Control Manager can support significantly more managed products (and endpoints registered to managed products).

Other Enhancements

Control Manager also provides the following enhancements:

- Web console now renders faster
- Web console has been rebranded

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 PREFACE-2. 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.
Knowledge Base	The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com/enterprise/default.aspx
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".

TABLE PREFACE-2. Control Manager Documentation (Continued)

DOCUMENT	DESCRIPTION
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 deploy, install, 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

To help you locate and interpret information easily, the Control Manager documentation uses the following conventions.

TABLE PREFACE-3. Control Manager Documentation Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
`Monospace`	Examples, sample command lines, program code, and program output
Note:	Provides configuration notes or recommendations

TABLE PREFACE-3. Control Manager Documentation Conventions

CONVENTION	DESCRIPTION
Tip:	Provides best practice information and Trend Micro recommendations
WARNING!	Provides warnings about processes that may harm your network

Section 1

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. 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 prescheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

This chapter contains the following topics:

- Control Manager Standard and Advanced on page 1-2
- How to Use Control Manager on page 1-3
- Understanding Trend Micro Management Communication Protocol on page 1-5
- Control Manager Architecture on page 1-8

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 5.5 Advanced supports the following as child Control Manager servers:

- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition

Control Manager 5.0/5.5 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-10.

How to Use Control Manager

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
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.

TABLE 1-1. Control Manager Features

FEATURE	DESCRIPTION
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.
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:

- **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 and Two-Way Communication Support

MCP supports one way and two-way 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 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. Refer to *Table 1-2* on page 1-9 for a list of components Control Manager uses.

TABLE 1-2. 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 **r**eport 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.

TABLE 1-2. Control Manager Components (Continued)

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.

TABLE 1-2. Control Manager Components (Continued)

COMPONENT	DESCRIPTION
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.
Widget Framework	Allows administrator to create a customized dashboard to monitor 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 web threats. It powers both on-premise and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight clients 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.

Email Reputation

Trend Micro 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. Malicious emails are blocked in the cloud based on the sender's IP address, preventing threats such as zombies or botnets from reaching the network or the user's PC.

File Reputation

Trend Micro file reputation technology checks the reputation of each file against an extensive in-the-cloud database before permitting user access. 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-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

Web Reputation

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. 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 the company's 24/7 threat research centers and technologies. Each new threat identified through a 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 protection of others. Because the threat information gathered 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.

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 Control Manager server. The web console lets you administer the Control Manager network from any machine using a compatible Web browser.

Tip: View the web console at a screen resolution of 1024 x 768 pixels.

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

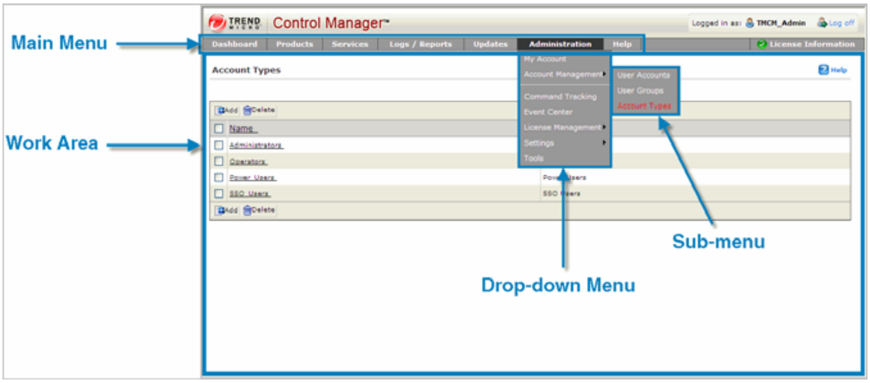


FIGURE 2-1. Control Manager Management Console

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
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.
Products	Includes options to administer Managed Products, Communicators, and Child servers.
Services	Provides access to Outbreak Prevention Services.
Logs/Reports	Includes options to manage Control Manager managed products and child server reports and to view logs for all products registered to the Control Manager server.
Updates	Provides options for configuring manual and scheduled updates and component deployment plans
Administration	Includes the Command Tracking, Event Center, Account Management settings, License Management settings, Connection Settings, and Tools options
Help	Provides the following: • 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

Drop-Down Menu

The drop-down menus for each main menu item appear after moving the cursor over the specified item. Only the following menu items have drop down menus: Logs/Reports, Updates, Administration, and Help.

Work Area

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

Understanding The Function-Locking Mechanism

The web console has a function-locking mechanism that prevents two users from accessing the same screen and option at the same time. The table below shows the web console options that Control Manager locks when in use

TABLE 2-2. Function-Locking Mechanism

OPTION IN USE	LOCKED OPTION(S)
Account Management	• Account Management • Directory Management
Directory Management	• Account Management • Directory Management
Agent Communication Schedule	Agent Communication Schedule
Heartbeat Settings	Heartbeat Settings

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

If you attempt to access a locked option, the locked option information screen appears. It displays the following information:

- User ID
- Date and time that the user logged on to the Control Manager server
- IP address of the computer used to access Control Manager web console

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

Note: A user with an **Administrator** account can unlock a locked function by forcibly logging out the user who is using it. To do this, click **Unlock** in the locked option information screen.

Whenever the logged out user attempts to use the previously locked function, a **Log on session expired** window appears. Clicking **OK** opens the web console Log On screen.

Accessing the Management Console

You have two ways to access the web console:

- Locally on the Control Manager server

  To access the web console locally from the Control Manager server:

  a. Click **Start** > **Programs** > **Trend Micro Control Manager** > **Trend Micro Control Manager**.

  b. Provide the user name and password in the fields provided.

  c. Click **Log on**.

- Remotely using any compatible browser

  To access the console remotely:

  a. 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.

  b. Provide the user name and password in the fields provided.

  c. Click **Log on**.

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

Note: Control Manager does not allow the same Control Manager web console in more than one browser on the same computer if you use the same User ID and password. Multiple instances on different computers using the same User ID 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.

To assign HTTPS access to the Control Manager web console:

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.

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

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

9. 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 Time-Out Settings

From the Time-out Settings screen, configure the console and command time-out settings. When the console times out, Control Manager requires user authentication (logging on) to access the web console. When a command times out, Control Manager stops trying to execute the command (for example a deploy component command to OfficeScan servers).

To configure timeout settings:

Path: Administration > Settings > Time-out Settings

1. Navigate to the Time-out Settings screen.
2. Specify the command time-out setting:
   - 24 hours
   - 48 hours
   - 72 hours

3. Specify the console time-out setting:
    - Never time out
    - Time-out after the specified time:
        - 10 minutes
        - 15 minutes
        - 30 minutes
        - 50 minutes
4. Click **Save**.

Logging Off from the Management Console

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

- 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.

This chapter contains the following topics:

- Understanding User Access on page 3-2
- Understanding Account Types on page 3-3
- Understanding User Accounts on page 3-11
- Understanding User Groups on page 3-21

Understanding User Access

Control Manager access control consists of the following four sections.

TABLE 3-1. Control Manager User Account 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 functions allowing you 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 Groups	The Group Accounts 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.
User Types	The Account Types screen displays all Control Manager user roles. The screen also provides functions allowing you to create and maintain Control Manager user roles. User roles define which areas of the Control Manager Web console a user can access.

Tip: 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 Account Types

In previous versions of Control Manager, four user account types existed. Control Manager 5.5 uses these account types as **default** account types:

- Operator
- Power User
- Administrator/Root

Control Manager 5.0 introduced custom account types. Custom account types allow Control Manager administrators to specify which Control Manager Web console menu items other users can access. Administrators cannot modify access permissions for default account types.

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

1. Specify which products/directories the user can access. (Step 8 of Editing a User Account on page 3-19.)

2. Specify which menu items the user can access. (If the default account types are not sufficient, see Adding Account Types on page 3-7 or Editing Account Types on page 3-9)

3. Specify the account type for the user's account. (Step 7 of the Editing a User Account on page 3-19.)

The following table shows all the features that each default account can access.

TABLE 3-2. User Account Access

MENU ITEM	OPERATOR	POWER USER	ADMINISTRATOR
Dashboard	●	●	●
Products	●	●	●
Services			●

Table 3-2. User Account Access (Continued)

Menu Item			Operator	Power User	Administrator
Logs/Reports	New Ad Hoc Query		●	●	●
	Saved Ad Hoc Queries		●	●	●
	My Reports		●	●	●
	One-time Reports			●	●
	Scheduled Reports			●	●
	Settings	Log Aggregation			●
		Log Maintenance		●	●
		Report Maintenance		●	●
Updates	Manual Download			●	●
	Scheduled Download			●	●
	Component List			●	●
	Deployment Plan			●	●
	Component Rollback			●	●
	Settings	Schedule Download Exceptions		●	●
		Update / Deployment		●	●

TABLE 3-2. User Account Access (Continued)

Menu Item			Operator	Power User	Administrator
Administration	My Account		●	●	●
	Account Management	User Accounts			●
		User Groups			●
		Account Types			●
	Command Tracking			●	●
	Event Center				●
	License Management	Managed Product			●
		Control Manager			●
	Settings	Agent Communication Schedule			●
		Control Manager Parent Setting			●
		Event Center Settings			●
		Heartbeat Settings			●
		Proxy Settings			●
		Time-out Settings			●
		Smart Protection Network Settings			●
		Add/Remove Product Agents	●	●	●
	Tools				●

Adding Account Types

Control Manager provides three default account types for administrators: Operator, Power User, and Administrator. Each account type has assigned permissions on select menu items on the Control Manager web console. You can add permissions for menu items, but you cannot remove permissions for the default account types.

If the default account types are not flexible enough for an administrator's needs, administrators can now create their own account types. User-specified account types allow for any Control Manager web console elements.

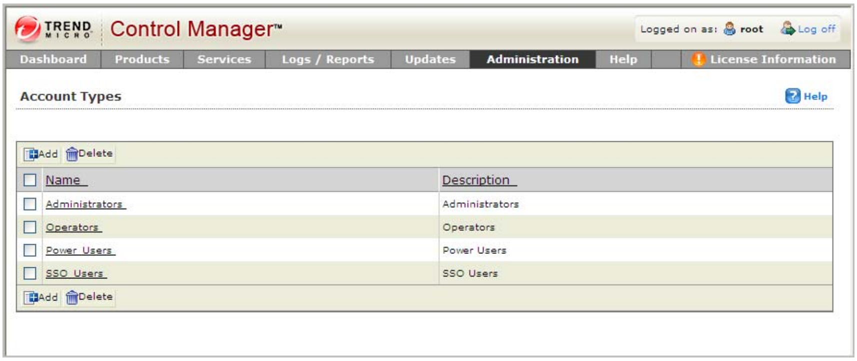
Tip: Managed product information displayed on accessible menu items depends on the managed product/directory permissions that Control Manager administrators specify in an individual's user account.

Example: Bob and Jane are OfficeScan administrators. Both have identical account type 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 on 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.

To add an account type:

Path: Administration > Account Management > Account Types | Add

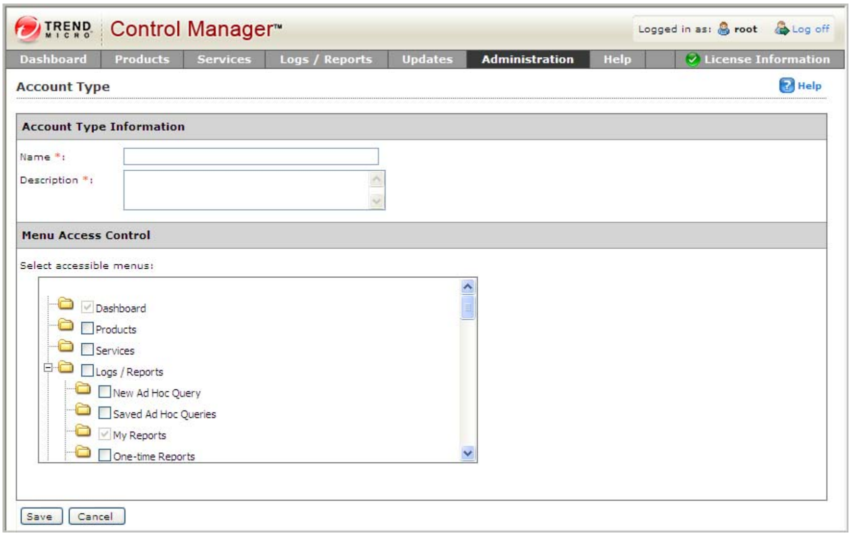
1. Navigate to the Account Types screen.



Account Types

□ Name	Description
□ Administrators	Administrators
□ Operators	Operators
□ Power Users	Power Users
□ SSO Users	SSO Users

2. In the working area, click **Add**. The Add Account Type screen appears.



Account Type

Account Type Information

Name *:

Description *:

Menu Access Control

Select accessible menus:

- ☑ Dashboard
- □ Products
- □ Services
- □ Logs / Reports
  - □ New Ad Hoc Query
  - □ Saved Ad Hoc Queries
  - ☑ My Reports
  - □ One-time Reports

3. Type a unique account type name in the **Name** field.

4. Provide a meaningful description for the account type in the **Description** field.

Tip: The description appears in the Account Type list. Providing a meaningful description can help administrators quickly identify an account type if the account type name cannot fully convey the use for the account type.

5. Select the accessible menu items for the account type. The following menu items are accessible to every account type: **Dashboard**, **My Reports**, and **My Account**.
6. Click **Save**. The Account Type screen appears and the new account type appears in the Account Type list.

Editing Account Types

Control Manager provides three default account types for administrators: Operator, Power User, and Administrator. Users can only modify user-specified account types. Users cannot modify the default account types.

Edit account types when an account type becomes outdated or requires minor maintenance.

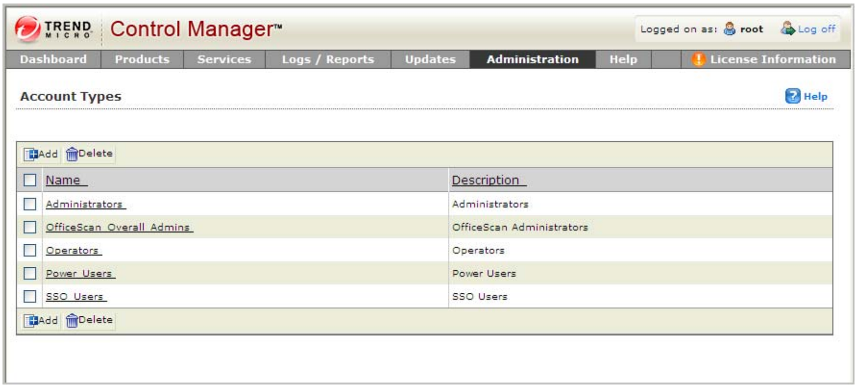
Tip: Managed product information displayed on accessible menu items depends on the managed product/directory permissions that Control Manager administrators specify in an individual's user account.

Example: Bob and Jane are OfficeScan administrators. Both have identical account type 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 on 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.

To edit an account type:

Path: Administration > Account Management > Account Types | *Account*

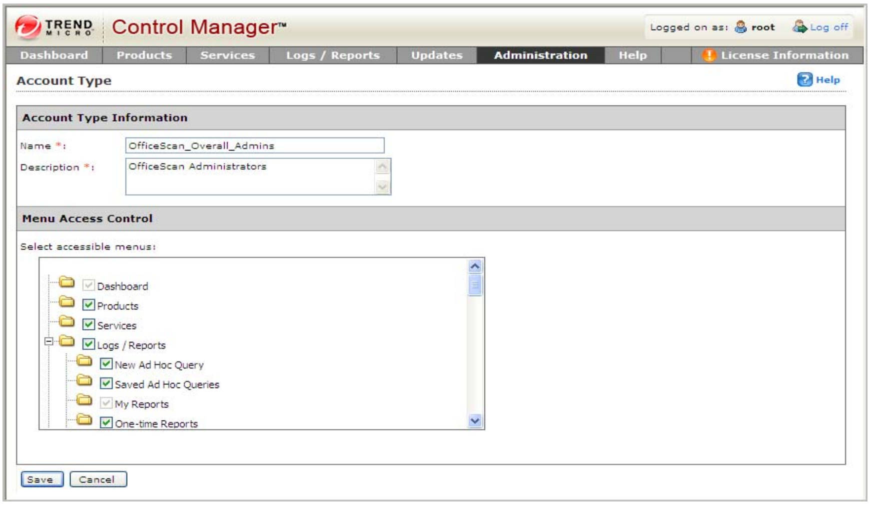
1. Navigate to the Account Types screen appears.



Account Types

□ Name	Description
□ Administrators	Administrators
□ OfficeScan Overall Admins	OfficeScan Administrators
□ Operators	Operators
□ Power Users	Power Users
□ SSO Users	SSO Users

2. Click the account type to edit from the Name column. The Account Type screen appears.



Account Type

Account Type Information

Name *: OfficeScan_Overall_Admins

Description *: OfficeScan Administrators

Menu Access Control

Select accessible menus:

- ☑ Dashboard
- ☑ Products
- ☑ Services
- ☑ Logs / Reports
  - ☑ New Ad Hoc Query
  - ☑ Saved Ad Hoc Queries
  - ☑ My Reports
  - ☑ One-time Reports

3. Edit the required account type information.
4. Click **Save**. The Account Type screen appears and the account type appears in the Account Type list.

Understanding User Accounts

Path: Administration > Account Management > 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.

Tip: 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 account type 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 on 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.

TABLE 3-4. User Accounts Screen Contents (Continued)

ACCOUNT INFORMATION	DESCRIPTION
Full name	The full name of the account user.
Domain	The Active Directory domain (if any) to which the user belongs.
Account Type	The account type assigned to the user (example: Administrator).
Enable	The current status of the account.

Note: Upon installation, Control Manager automatically creates a root account.

Adding a User Account

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

Tip: 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 account type 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 on 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.

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

1. Specify which products/directories the user can access. (Step 8 of Editing a User Account on page 3-19.)

2. Specify which menu items the user can access. (If the default account types are not sufficient, see Adding Account Types on page 3-7 or Editing Account Types on page 3-9)

3. Specify the account type for the user's account. (Step 7 of the Editing a User Account on page 3-19.)

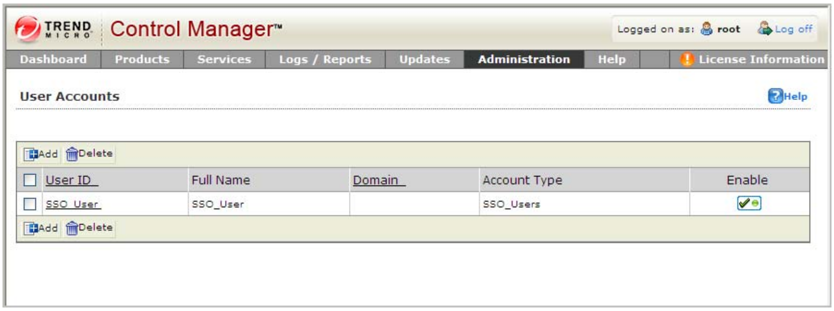
When adding a user account, you need to provide information to identify the user, assign an account type, and set folder access rights.

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.

To add a user account:

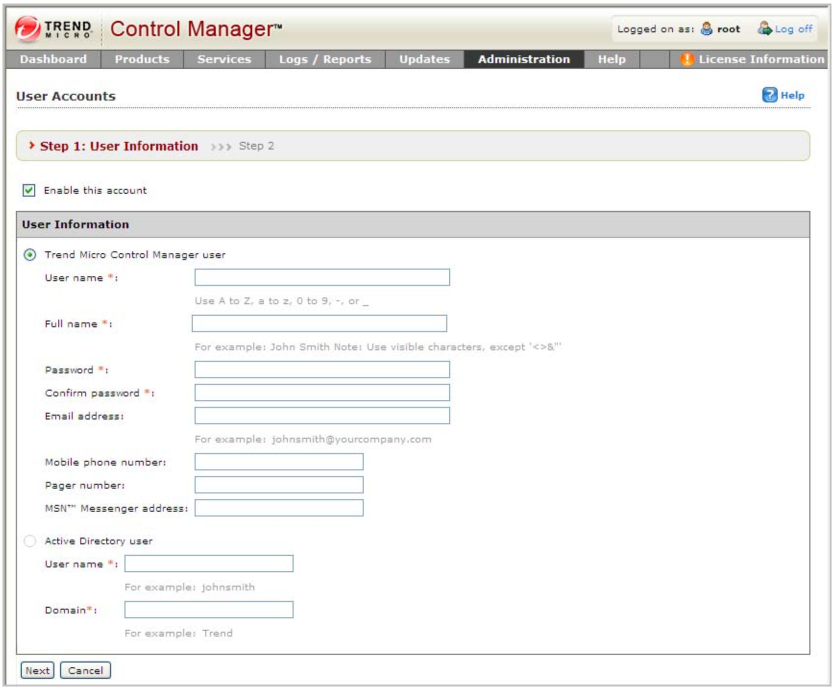
Path: Administration > Account Management > User Accounts | Add

1. Navigate to the User Accounts screen.



□	User ID	Full Name	Domain	Account Type	Enable
□	SSO_User	SSO_User		SSO_Users	✓

2. Click **Add**. The Step 1: User Information screen appears.



User Accounts

› Step 1: User Information ››› Step 2

☑ Enable this account

User Information

● Trend Micro Control Manager user

User name *:

Use A to Z, a to z, 0 to 9, -, or _

Full name *:

For example: John Smith Note: Use visible characters, except '<>&"'

Password *:

Confirm password *:

Email address:

For example: johnsmith@yourcompany.com

Mobile phone number:

Pager number:

MSN™ Messenger address:

○ Active Directory user

User name *:

For example: johnsmith

Domain*:

For example: Trend

3. Select **Enable this account** to enable Control Manager users.

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:** You must confirm the password in the field 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.

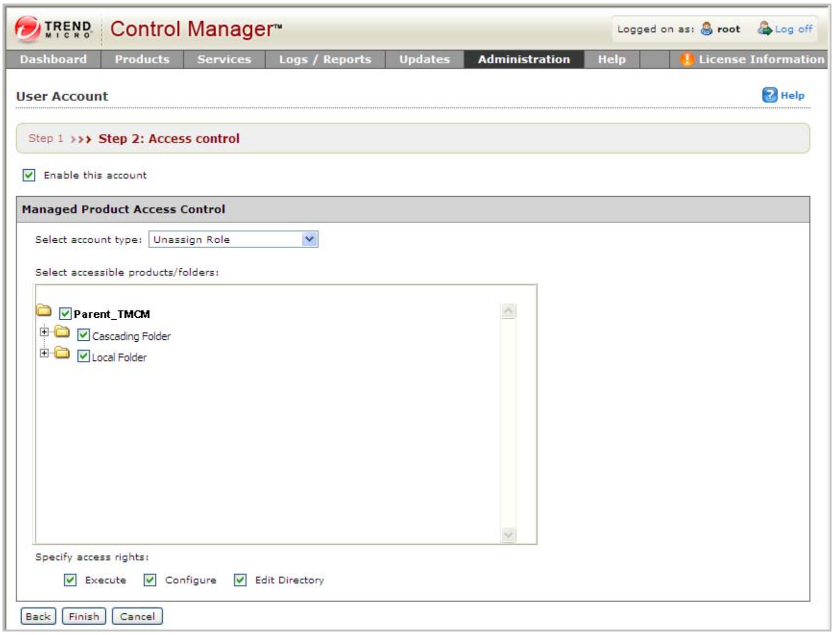
a. Select **Active Directory user**.

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.



User Account

Step 1 >>> Step 2: Access control

☑ Enable this account

Managed Product Access Control

Select account type: Unassign Role

Select accessible products/folders:

- ☑ Parent_TMCM
  - ☑ Cascading Folder
  - ☑ Local Folder

Specify access rights:

☑ Execute ☑ Configure ☑ Edit Directory

6. Select an account type from the account type list.

   The default options are **Operator**, **Power User**, and **Administrator**, however users can create their own account types.

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

Tip: Carefully organize the Product Directory for ease of use.

Assigning access to a folder allows users access to all 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. Click **Finish**.

Editing a User Account

You can change the information of any user account including the account information, account type, 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.

To edit a user account:

Path: Administration > Account Management > User Accounts | Edit

1. Navigate to the User Accounts screen.
2. Click the account to modify. The Edit User Account screen appears.
3. Modify the account information, and then click **Next>>**.
4. Modify the 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.

To disable a user account:

Path: Administration > Account Management > User Accounts | *Account*

1. Navigate to the User Accounts screen.
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.

   Or

   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.

To delete a user account:

Path: Administration > Account Management > User Accounts | *Account*

1. Navigate to the User Accounts screen.
2. Select the check box for the account to delete.
3. Click **Delete**.

Understanding User Groups

Path: Administration > Account Management > 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 3-1. 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.

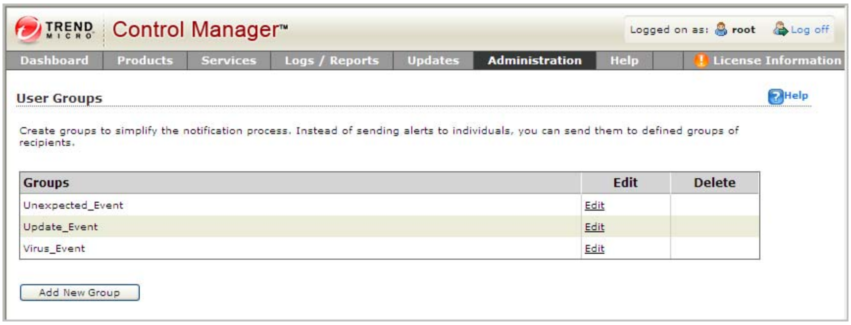
Adding a User Group

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.

To add a user group:

Path: Administration > Account Management > User Groups | Add New Group

1. Navigate to the User Groups screen.

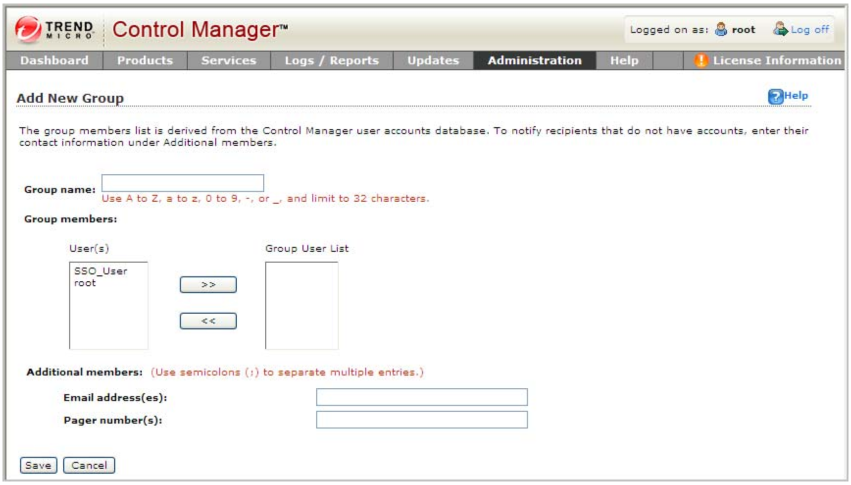


User Groups

Create groups to simplify the notification process. Instead of sending alerts to individuals, you can send them to defined groups of recipients.

Groups	Edit	Delete
Unexpected_Event	Edit	
Update_Event	Edit	
Virus_Event	Edit	

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



Add New Group

The group members list is derived from the Control Manager user accounts database. To notify recipients that do not have accounts, enter their contact information under Additional members.

Group name:

Use A to Z, a to z, 0 to 9, -, or _, and limit to 32 characters.

Group members:

User(s): SSO_User, root

Group User List

Additional members: (Use semicolons (;) to separate multiple entries.)

Email address(es):

Pager number(s):

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 **Add 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.

To edit a user group:

Path: Administration > Account Management > User Groups | Edit

1. Navigate to the User Groups screen.
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.

To delete a user group:

Path: Administration > Account Management > User Groups

1. Navigate to the User Groups screen.
2. Click **Delete** beside the group to delete.
3. Click **OK** to delete the user group.
4. Click **OK**.

Chapter 4

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 on page 4-2
- Grouping Managed Products in the Product Directory on page 4-3
- Understanding Cascading Management on page 4-10
- Registering or Unregistering Child Servers on page 4-12

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, SMEX or FW) 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 4-1. Product Directory Options

Menu Items	Description
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.

TABLE 4-1. Product Directory Options (Continued)

MENU ITEMS	DESCRIPTION
Logs	Click this menu item, after selecting a managed product/directory, to query and view product logs. If you select a managed product, you can only query logs for that specific product. Otherwise, you can query all the products available in the 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	**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 in the Product Directory

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).

Group managed products according to geographical, administrative, or product-specific reasons. The following table presents the recommended grouping types as well as their advantages and disadvantages.

TABLE 4-2. 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
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 4-3. 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 divisions. For example, have two Control Manager servers that manage the production and testing groups.

TABLE 4-3. Considerations when grouping managed products or child servers

STRUCTURE	DESCRIPTION
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 structure supports group configuration.

The Product Directory provides a user-specified grouping of managed products. This grouping enables you to administer managed products using the following tasks:

- Configuring managed products
- Request products to perform Scan Now (if the managed product supports this command)
- View product information and details about the managed product's 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, antispam rule, and program updates

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

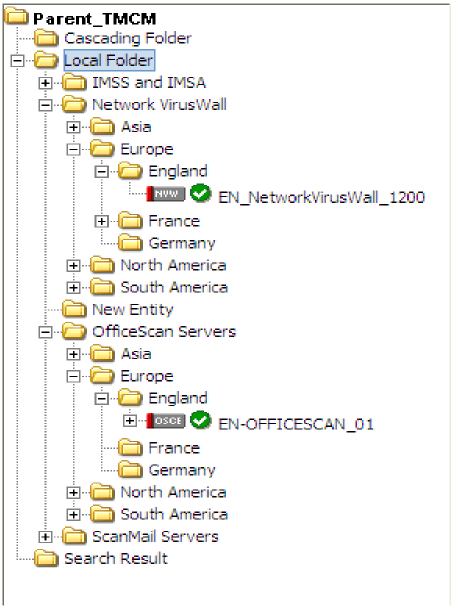
TABLE 4-4. Considerations for the structure

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.

TABLE 4-4. Considerations for the structure (Continued)

CONSIDER	EFFECT
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 to individual products. A well-structured directory therefore simplifies the designation of recipients.
Outbreak Prevention Policy (OPP) deployment	OPP deployment depend on deployment plans for efficient distribution of Outbreak Prevention Policy.

A sample Product Directory appears below:



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

Note: All newly registered managed products usually appear in the **New Entity** folder regardless of the agent type.

TABLE 4-5. Managed Product Icons

ICON	DESCRIPTION
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	ServerProtect Information Server
	ServerProtect Domain

TABLE 4-5. **Managed Product Icons (Continued)**

ICON	DESCRIPTION
NT	ServerProtect for Windows (Normal Server)
NW	ServerProtect for NetWare (Normal Server)
IMSS	InterScan Messaging Security Suite
IWSS	InterScan Web Security Suite
ISNT	InterScan VirusWall for Windows
ISUX	InterScan VirusWall for UNIX
SMEX	ScanMail for Microsoft Exchange
SMLN	ScanMail for Lotus Notes
NVW	Network VirusWall
FW	NetScreen Global PRO Firewall
✓	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 4-6. 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	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.

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.

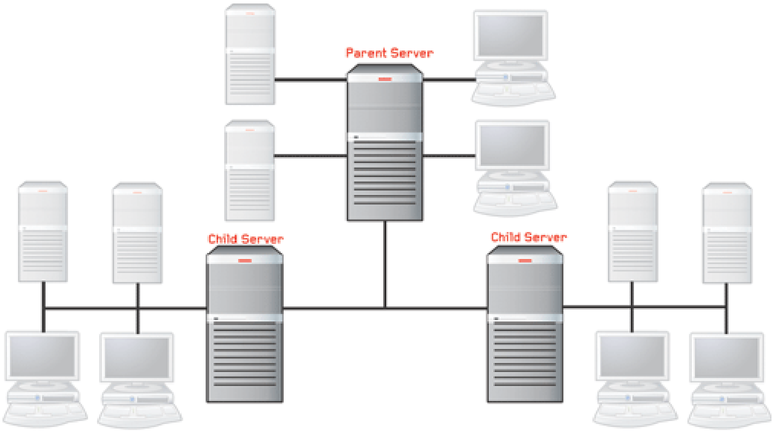


FIGURE 4-1. The cascading management structure uses two-tier parent-child architecture

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 5.5 Advanced supports the following as child Control Manager servers:

- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition

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

Aside from its own managed products, a parent server indirectly manages a large number of managed products handled directly by child servers.

The following table lists the differences between parent and child servers.

TABLE 4-7. 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).

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 Control Manager Parent Settings screen to register or unregister from a Control Manager parent server.

Chapter 5

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 5-1. 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.

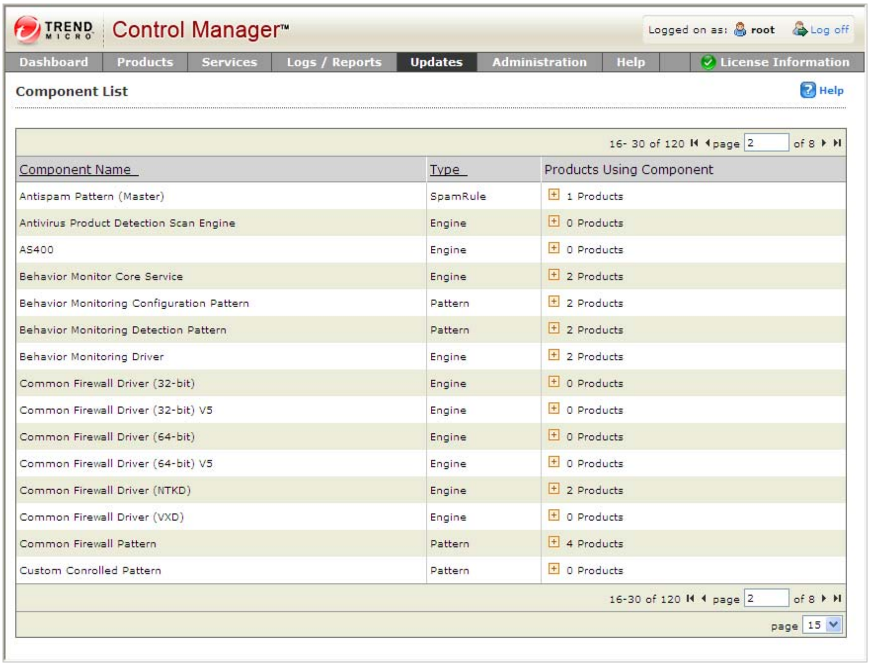
TABLE 5-1. Available Components (Continued)

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.



Component List

16- 30 of 120 page 2 of 8

Component Name	Type	Products Using Component
Antispam Pattern (Master)	SpamRule	1 Products
Antivirus Product Detection Scan Engine	Engine	0 Products
AS400	Engine	0 Products
Behavior Monitor Core Service	Engine	2 Products
Behavior Monitoring Configuration Pattern	Pattern	2 Products
Behavior Monitoring Detection Pattern	Pattern	2 Products
Behavior Monitoring Driver	Engine	2 Products
Common Firewall Driver (32-bit)	Engine	0 Products
Common Firewall Driver (32-bit) V5	Engine	0 Products
Common Firewall Driver (64-bit)	Engine	0 Products
Common Firewall Driver (64-bit) V5	Engine	0 Products
Common Firewall Driver (NTKD)	Engine	2 Products
Common Firewall Driver (VXD)	Engine	0 Products
Common Firewall Pattern	Pattern	4 Products
Custom Conrolled Pattern	Pattern	0 Products

16-30 of 120 page 2 of 8

page 15

FIGURE 5-1. 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. When you register managed products or activate services at a later time, be sure to configure the manual or scheduled download of applicable components.

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

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

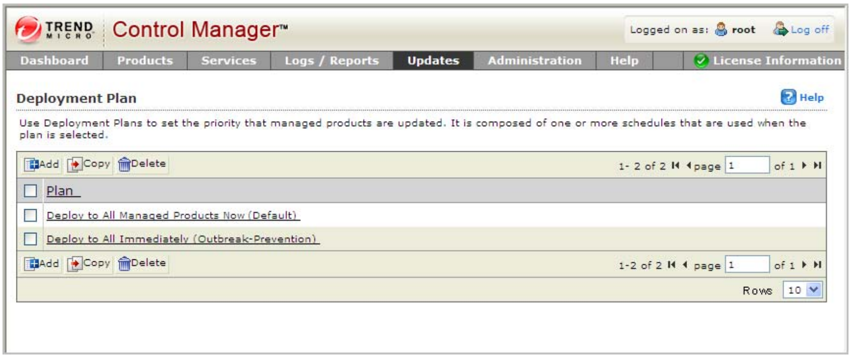
Step 6: Complete the manual download

To manually download components:

Step 1: Configure a Deployment Plan for your components

Path: Updates > Deployment Plan

1. Navigate to the Deployment Plan screen.

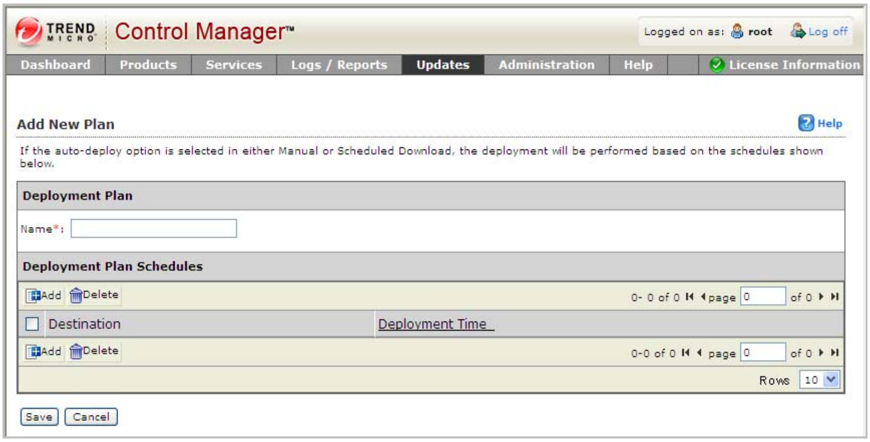


Deployment Plan

Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

	Plan
□	Deploy to All Managed Products Now (Default)
□	Deploy to All Immediately (Outbreak-Prevention)

2. Click **Add**. The **Add New Plan** screen appears.



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Deployment Plan

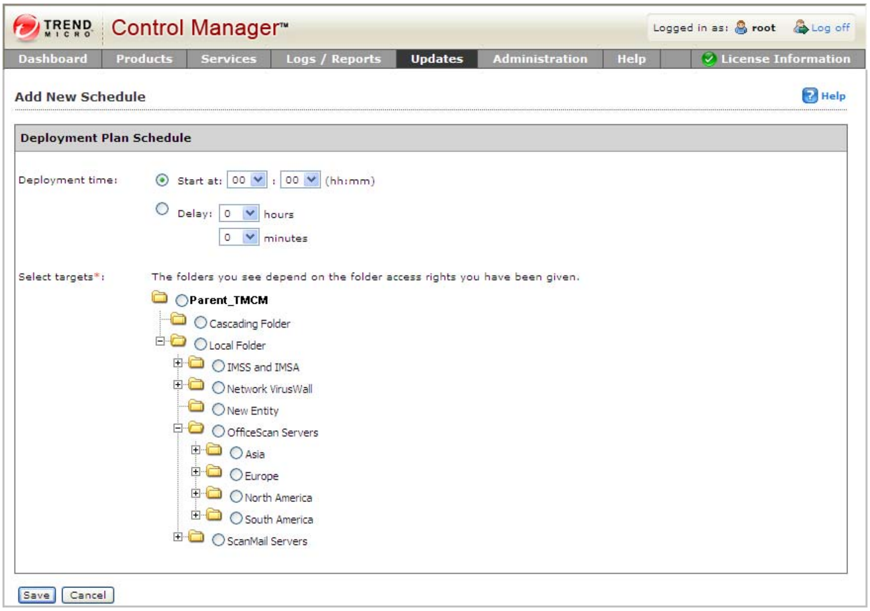
Name*:

Deployment Plan Schedules

	Destination	Deployment Time

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

4. Click **Add** to provide deployment plan details. The Add New Schedule screen appears.



Add New Schedule

Deployment Plan Schedule

Deployment time: ● Start at: 00 : 00 (hh:mm)

○ Delay: 0 hours

0 minutes

Select targets*: The folders you see depend on the folder access rights you have been given.

○ Parent_TMCM
- ○ Cascading Folder
- ○ Local Folder
  - ○ IMSS and IMSA
  - ○ Network VirusWall
  - ○ New Entity
  - ○ OfficeScan Servers
    - ○ Asia
    - ○ Europe
    - ○ North America
    - ○ South America
  - ○ ScanMail Servers

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.

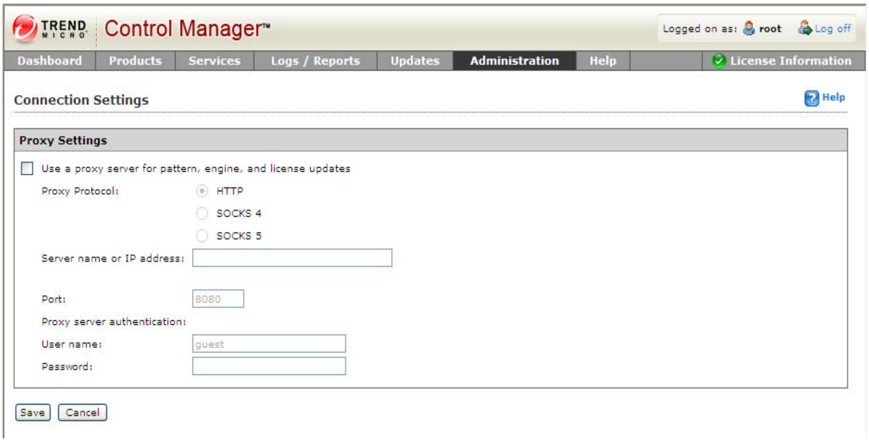
     Use the menus to designate the time in hours and minutes.
   - **Delay:** after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     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

Path: Administration > Settings > Proxy Settings

1. Navigate to the Connection Settings screen.



Connection Settings

Proxy Settings

□ Use a proxy server for pattern, engine, and license updates

Proxy Protocol: ● HTTP ○ SOCKS 4 ○ SOCKS 5

Server name or IP address:

Port: 8080

Proxy server authentication:

User name: guest

Password:

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.

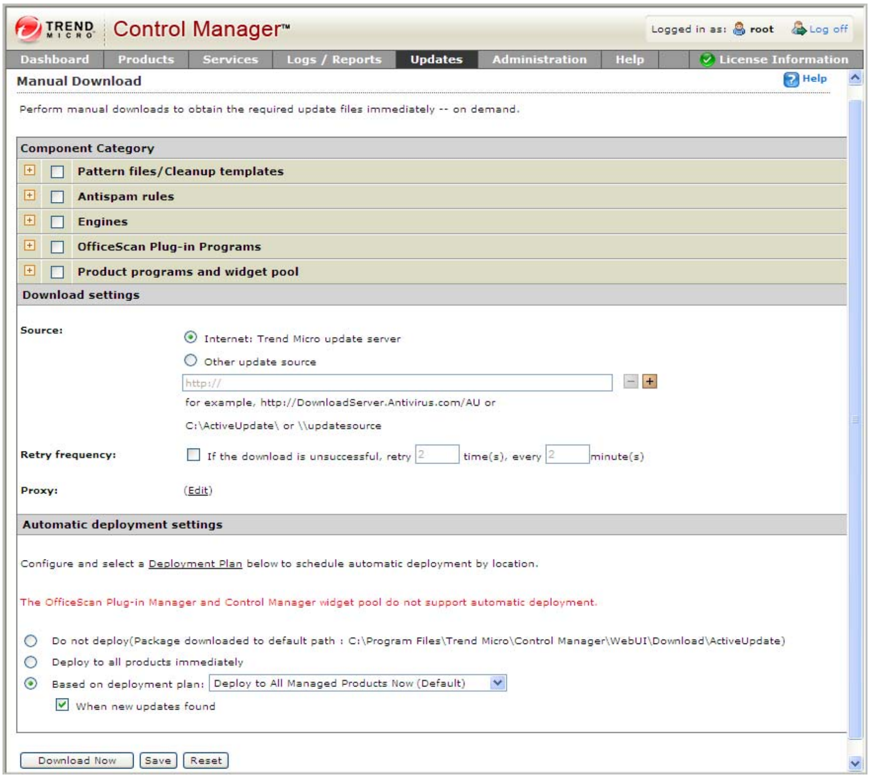
6. Type a log on name and password if your server requires authentication.

7. Click **Save**.

Step 3: Select the components to update

Path: Updates > Manual Download

1. Navigate to the Manual Download screen.



Manual Download

Perform manual downloads to obtain the required update files immediately -- on demand.

Component Category

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

Download settings

Source: ● Internet: Trend Micro update server
○ Other update source
http://
for example, http://DownloadServer.Antivirus.com/AU or
C:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

The OfficeScan Plug-in Manager and Control Manager widget pool do not support automatic deployment.

○ Do not deploy(Package downloaded to default path : C:\Program Files\Trend Micro\Control Manager\WebUI\Download\ActiveUpdate)
○ Deploy to all products immediately
● Based on deployment plan: Deploy to All Managed Products Now (Default)
☑ When new updates found

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

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

1. Select when to deploy downloaded components from the Schedule 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, 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.

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

Step 6: Complete the manual download

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.

Configuring 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.

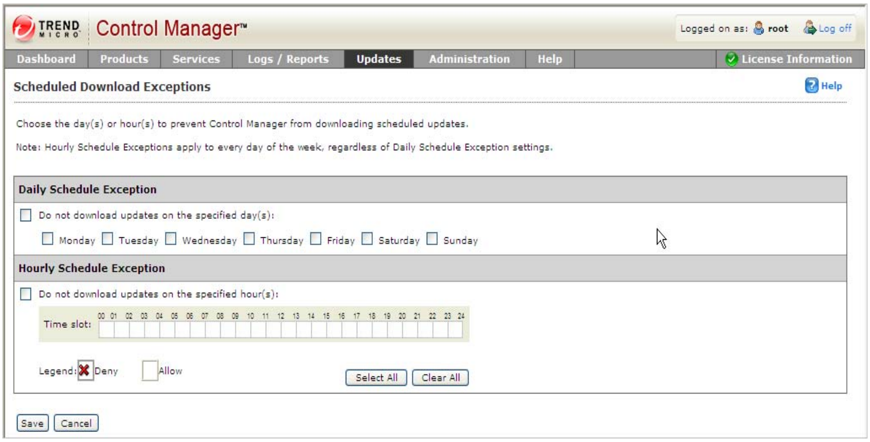
Note: Daily scheduled exceptions apply to the selected days, while hourly scheduled exceptions apply to every day of the week.

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**.

To configure scheduled download exceptions:

Path: Updates > Settings > Scheduled Download Exceptions

1. Navigate to the Scheduled Download Exceptions screen.



Scheduled Download Exceptions

Choose the day(s) or hour(s) to prevent Control Manager from downloading scheduled updates.

Note: Hourly Schedule Exceptions apply to every day of the week, regardless of Daily Schedule Exception settings.

Daily Schedule Exception

□ Do not download updates on the specified day(s):

□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Hourly Schedule Exception

□ Do not download updates on the specified hour(s):

Time slot: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Legend: ☒ Deny □ Allow

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

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

Step 6: Configure the automatic deployment settings

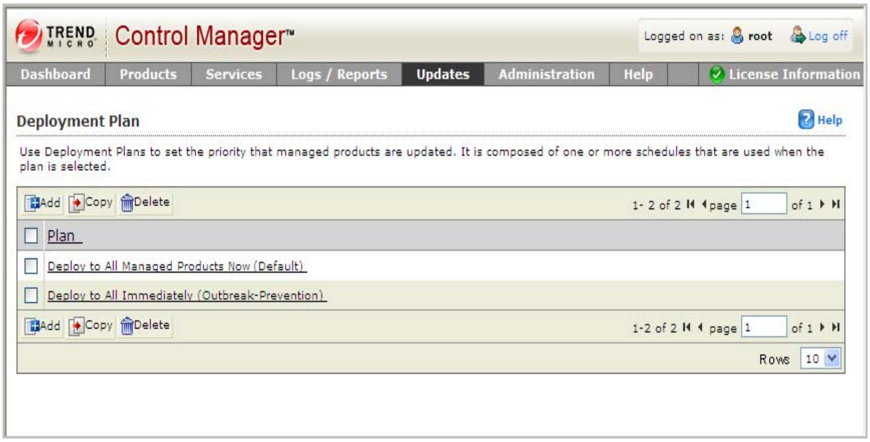
Step 7: Enable the schedule and save settings

To configure scheduled downloads:

Step 1: Configure a Deployment Plan for your components

Path: Administration > Deployment Plan

1. Navigate to the Deployment Plan screen.



Deployment Plan

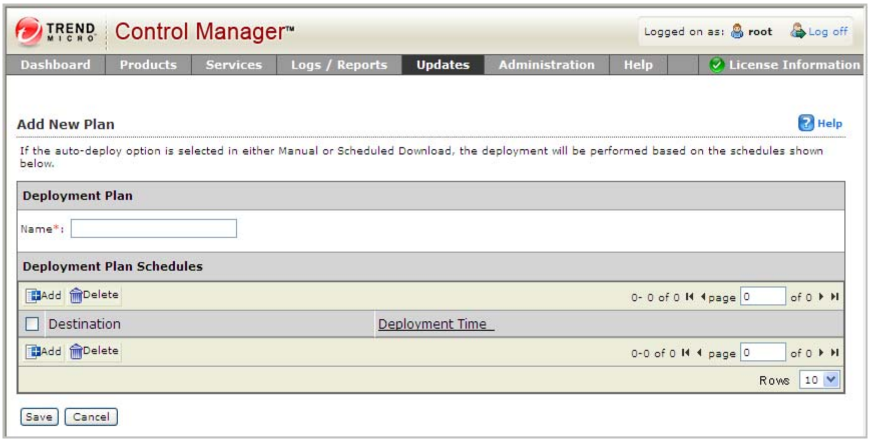
Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

1- 2 of 2 page 1 of 1

	Plan
□	Deploy to All Managed Products Now (Default)
□	Deploy to All Immediately (Outbreak-Prevention)

1-2 of 2 page 1 of 1

2. Click **Add**. The **Add New Plan** screen appears.



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Deployment Plan

Name*:

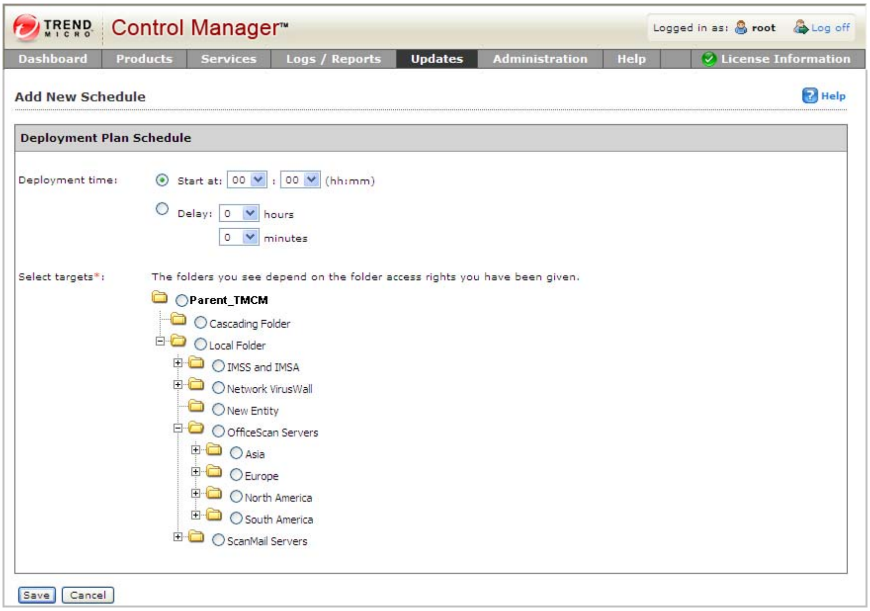
Deployment Plan Schedules

0- 0 of 0 page 0 of 0

	Destination	Deployment Time

0-0 of 0 page 0 of 0

3. On the Add New Plan screen, type a deployment plan name in the **Name** field.
4. Click **Add** to provide deployment plan details. The Add New Schedule screen appears.



Add New Schedule

Help

Deployment Plan Schedule

Deployment time: ● Start at: 00 : 00 (hh:mm)

○ Delay: 0 hours

0 minutes

Select targets*: The folders you see depend on the folder access rights you have been given.

- ○ Parent_TMCM
  - ○ Cascading Folder
  - ○ Local Folder
    - ○ IMSS and IMSA
    - ○ Network VirusWall
    - ○ New Entity
    - ○ OfficeScan Servers
      - ○ Asia
      - ○ Europe
      - ○ North America
      - ○ South America
    - ○ ScanMail Servers

Save Cancel

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.

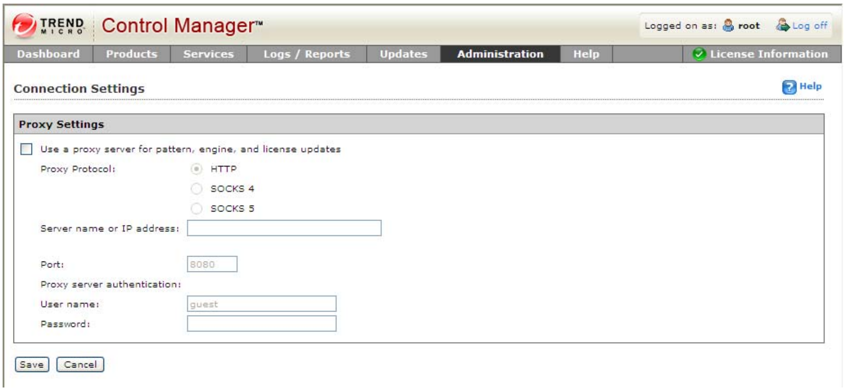
     Use the menus to designate the time in hours and minutes.
   - **Delay:** after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     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

Path: Administration > Settings > Proxy Settings

1. Navigate to the Connection Settings screen.



Connection Settings

Proxy Settings

□ Use a proxy server for pattern, engine, and license updates

Proxy Protocol: ● HTTP ○ SOCKS 4 ○ SOCKS 5

Server name or IP address:

Port: 8080

Proxy server authentication:

User name: guest

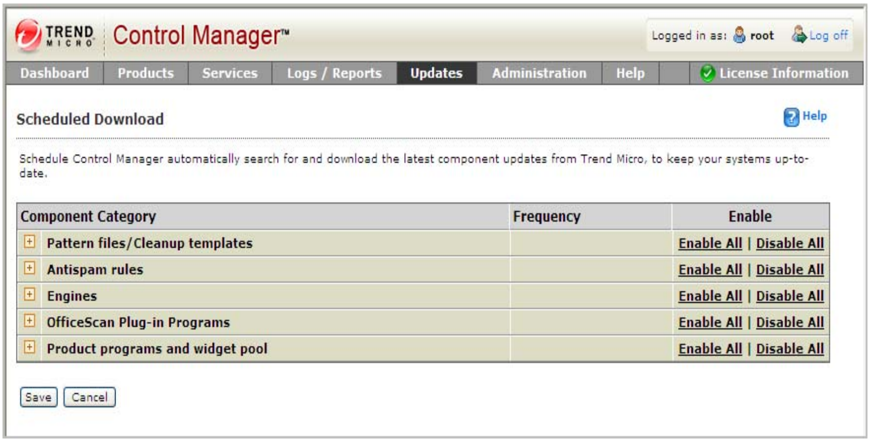
Password:

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

Path: Updates > Scheduled Download

1. Navigate to the Scheduled Download screen.



Scheduled Download

Schedule Control Manager automatically search for and download the latest component updates from Trend Micro, to keep your systems up-to-date.

Component Category	Frequency	Enable
⊞ Pattern files/Cleanup templates		Enable All | Disable All
⊞ Antispam rules		Enable All | Disable All
⊞ Engines		Enable All | Disable All
⊞ OfficeScan Plug-in Programs		Enable All | Disable All
⊞ Product programs and widget pool		Enable All | Disable All

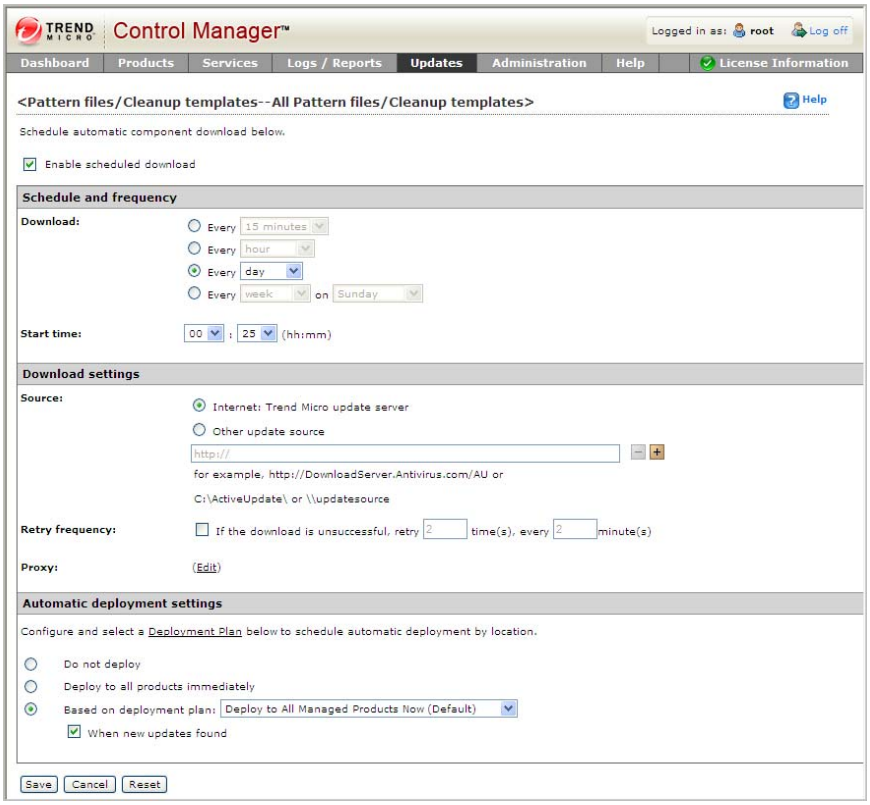
2. From the Component Category area select the components to download.

   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.



<Pattern files/Cleanup templates--All Pattern files/Cleanup templates>

Schedule automatic component download below.

☑ Enable scheduled download

Schedule and frequency

Download:
- ○ Every 15 minutes
- ○ Every hour
- ● Every day
- ○ Every week on Sunday

Start time: 00 : 25 (hh:mm)

Download settings

Source:
- ● Internet: Trend Micro update server
- ○ Other update source

http://

for example, http://DownloadServer.Antivirus.com/AU or

C:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

- ○ Do not deploy
- ○ Deploy to all products immediately
- ● Based on deployment plan: Deploy to All Managed Products Now (Default)
  - ☑ When new updates found

Save | Cancel | Reset

Step 4: Configure the download schedule

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

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 6: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule 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

Tip: 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** list.
3. Click **Save**.

Step 7: Enable the schedule and save settings

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.

To configure scheduled download schedule and frequency:

Path: Updates > Scheduled Download

1. Navigate to the Scheduled Download screen.
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> is the name of the component you selected.
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.

To configure scheduled download settings:

Path: Updates > Scheduled Download

1. Navigate to the Scheduled Download screen.
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.

Under Download settings:

3. Under Source, select one of the following update sources:

   - **Internet: Trend Micro update server:** (default setting) Control Manager downloads 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 Auto-deploy Setting group to set how Control Manager deploys updates.

To configure scheduled download auto-deploy settings:

Path: Updates > Scheduled Download

1. Navigate to the Scheduled Download screen.
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.

Under Automatic deployment settings

3. Select when to deploy downloaded components from the Schedule 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 when new components are available from the update source, but deploy to managed products based on the schedule you select

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

4. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
5. 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 pages. 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.

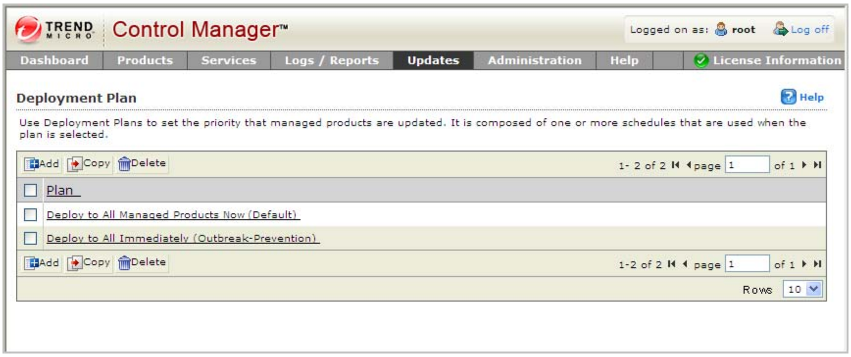
Create Deployment Plans

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

To create a new deployment plan:

Path: Updates > Deployment Plan

1. Navigate to the Deployment Plan screen.

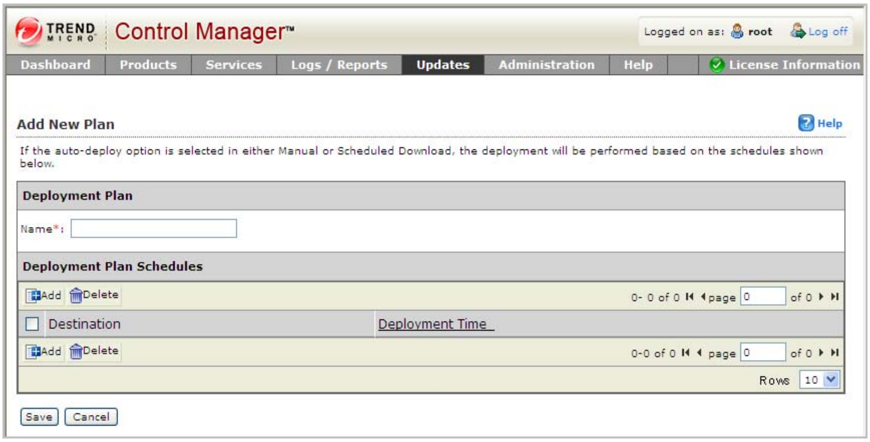


Deployment Plan

Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

□	Plan
□	Deploy to All Managed Products Now (Default)
□	Deploy to All Immediately (Outbreak-Prevention)

2. Click **Add**. The **Add New Plan** screen appears.



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Deployment Plan

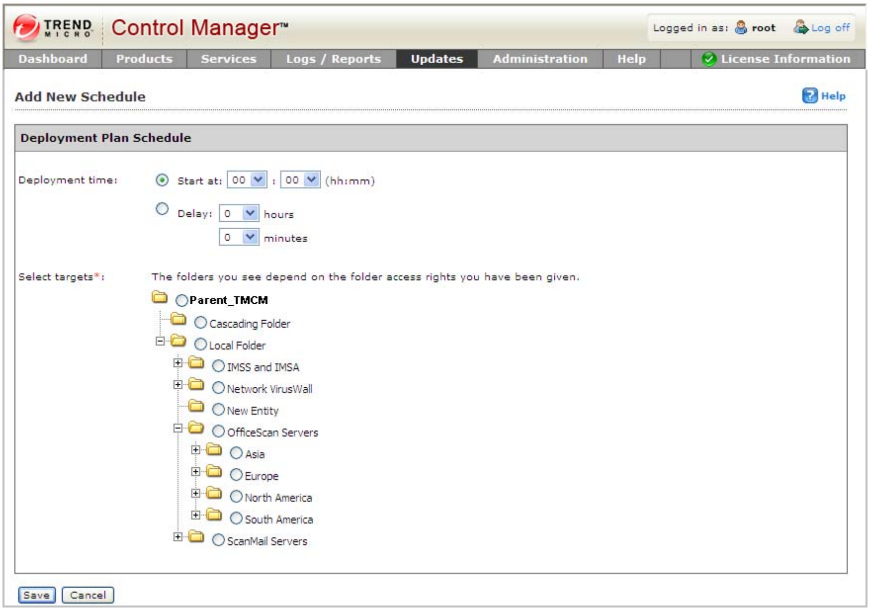
Name*:

Deployment Plan Schedules

□	Destination	Deployment Time

3. On the Add New Plan screen, type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details. The Add New Schedule screen appears.



Add New Schedule

Deployment Plan Schedule

Deployment time: ● Start at: 00 : 00 (hh:mm)

○ Delay: 0 hours

0 minutes

Select targets*: The folders you see depend on the folder access rights you have been given.

- ○ Parent_TMCM
  - ○ Cascading Folder
  - ○ Local Folder
    - ○ IMSS and IMSA
    - ○ Network VirusWall
    - ○ New Entity
    - ○ OfficeScan Servers
      - ○ Asia
      - ○ Europe
      - ○ North America
      - ○ South America
    - ○ ScanMail Servers

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.

Modify a Deployment Plan

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

To edit a deployment plan:

Path: Updates > Deployment Plan | <plan to edit> | <schedule to edit>

1. Click the name of the plan to modify. The Edit Plan screen appears.
2. Click the name of the schedule to modify. The Edit Schedule appears.
3. Modify the deployment time or Product Directory folder.

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

4. After completing all the necessary modifications, click **Save**. The Deployment Plan screen appears.

Duplicate a Deployment Plan

Create new deployment plans based on an existing plan.

To duplicate a deployment plan:

Path: Updates > Deployment Plan

1. Navigate to the Deployment Plan screen.
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.

To remove a deployment plan:

Path: Updates > Deployment Plan

1. Navigate to the Deployment Plan screen.
2. Select the accompanying check box for the plan to delete.
3. Click **Delete**. The selected plans delete from the Deployment Plan list.

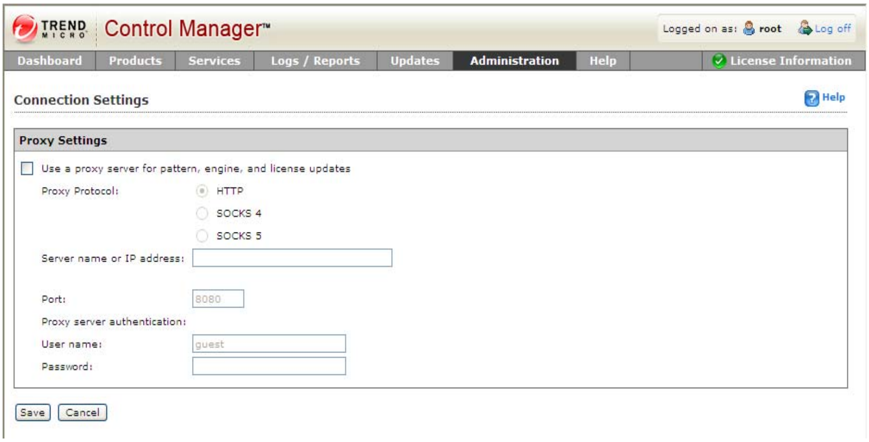
Configuring Proxy Settings

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

To configure proxy server settings:

Path: Administration > Settings > Proxy Settings

1. Navigate to the Connection Settings Screen.



Connection Settings

Proxy Settings

☐ Use a proxy server for pattern, engine, and license updates

Proxy Protocol: ● HTTP ○ SOCKS 4 ○ SOCKS 5

Server name or IP address:

Port: 8080

Proxy server authentication:

User name: guest

Password:

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 (http://cm55-p.activeupdate.trendmicro.com) 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:

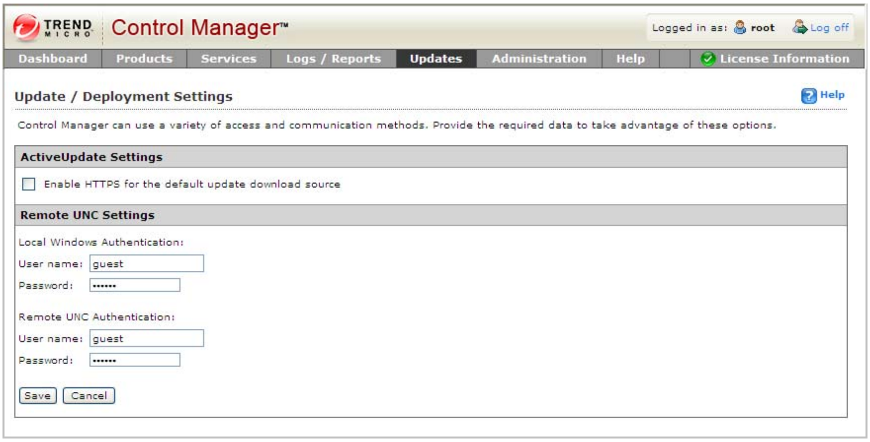
- Administrator privilege
- *Log on as a batch job* policy set

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

To enable HTTPS download:

Path: Updates > Settings > Update/Deployment Settings

1. Navigate to the Update/Deployment Settings screen.



Update / Deployment Settings

Control Manager can use a variety of access and communication methods. Provide the required data to take advantage of these options.

ActiveUpdate Settings

□ Enable HTTPS for the default update download source

Remote UNC Settings

Local Windows Authentication:

User name: guest

Password: ••••••

Remote UNC Authentication:

User name: guest

Password: ••••••

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

To enable UNC download:

Path: Updates > Settings > Update/Deployment Settings

1. Navigate to the Update/Deployment Settings screen.
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 > Source**, select **Other update source** and then specify the shared network folder.
6. Click **Save**.

Enabling HTTPS Download

Using HTTPS to download components from the Trend Micro ActiveUpdate server (http://cm55-p.activeupdate.trendmicro.com) or other Internet source is a two-step process.

To enable HTTPS download:

Path: Updates > Settings > Update/Deployment Settings

1. Navigate to the Update/Deployment Settings screen.
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 > Source**, 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

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

To enable UNC download:

Path: Updates > Settings > Update/Deployment Settings

1. Navigate to the Update/Deployment Settings screen.
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 > Source**, 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

To verify the user is on the "Log on as batch job" list:

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.

Section 2

Monitoring the Control Manager Network

Chapter 6

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
- **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 6-16 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 four default tabs:

- Summary
- Threat Statistics
- Compliance
- 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.

TABLE 6-1. Summary Tab Widgets

WIDGET	DESCRIPTION
Threat Detection Results	Displays the number of threat detections and the ratio of threats compared to the total number of detections. This widget displays this data by: • Virus/Malware • Spyware/Grayware • Content Security • Web Security • Network Virus
Policy Violation Detections	Displays the policy violation detections for Network VirusWall Enforcer devices.

TABLE 6-1. Summary Tab Widgets

WIDGET	DESCRIPTION
Product Component Status	Displays the component's (pattern, template, engine, rule) version and status (up-to-date or out-of-date) for managed products or endpoints. This widget provides administrators with a quick way to discern which managed products or endpoints are up to date.

Threat Statistics Tab

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

Note: On parent Control Manager servers, the **Control Manager Top Threats** and **File Reputation Top Threat Detections** widgets require scheduled log updates 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**

TABLE 6-2. Threat Statistics Tab Widgets

WIDGET	DESCRIPTION
Control Manager Top Threats	This widget displays the top 10/25/50 detected: • Malicious files • Malicious URLs
Control Manager Threat Statistics	Displays the number of threat detections and the ratio of threats compared to the total number of detections. This widget displays this data by: • Product category • Threat type

TABLE 6-2. Threat Statistics Tab Widgets

WIDGET	DESCRIPTION
Smart Protection Network Threat Statistics	Displays the number of threat detections globally, within an industry, and locally on your network. This widget displays this data by: • Product category • Threat type
File Reputation Top Threat Detections	Displays the top 10 threat detections made by File Reputation. The data is a comparison between global detections on the threat and detections made on your network.

Compliance Tab

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

TABLE 6-3. Compliance Tab Widgets

WIDGET	DESCRIPTION
Product Application Compliance	Displays the product version, build, and update status for managed products. This widget provides administrators with a quick way to discern which managed product's applications are up to date and which require updating.
Product Component Status	Displays the component's (pattern, template, engine, rule) version and status (up-to-date or out-of-date) for managed products or endpoints. This widget provides administrators with a quick way to discern which products or endpoints are up to date.
Product Connection Status	Displays the managed product's connection status to Control Manager (online, offline, disabled, abnormal).

TABLE 6-3. Compliance Tab Widgets

WIDGET	DESCRIPTION
OfficeScan Endpoint Connection Status	Displays the OfficeScan client's connection status to its OfficeScan server (online, offline, roaming).

Smart Protection Network Tab

The Smart Protection Network tab contains all 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.

TABLE 6-4. Smart Protection Network Tab Widgets

WIDGET	DESCRIPTION
File Reputation Top Threat Detections	Displays the top 10 threat detections made by File Reputation. The data is a comparison between global detections on the threat and detections made on your network.
Web Reputation Top Threat Sources	Displays the total number of security threat detections made by Web Reputation. The information is displayed in a world map by geographic location.
Smart Protection Network Connections	Displays the number of endpoints on your network that connect to the Trend Micro Smart Protection Network for updates or security threat verifications.
Smart Protection Network Threat Statistics	Displays the number of threat detections globally, within an industry, and locally on your network. This widget displays this data by: • Product category • Threat type

TABLE 6-4. Smart Protection Network Tab Widgets

WIDGET	DESCRIPTION
File Reputation Threat Map	Displays the total number of security threat detections made by File Reputation. The information is displayed on a world map by geographic location.
Email Reputation Threat Map	Displays the total number of spam detections made by Email Reputation. The information is displayed on a world map by geographic location.
Web Reputation Top Threatened Users	Displays the number of users affected by malicious URLs detected by Web Reputation. The information is displayed on a world map by geographic location.

Adding Tabs

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

To add a tab to the dashboard:

Path: Dashboard

1. Navigate to the Dashboard screen.
2. Click **New Tab**. 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 Widget** to populate the tab with widgets.

Configuring Tab Settings

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

To change the title for a tab:

Path: Dashboard | Tab Settings

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. 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 two places:

- Control Manager database
- Trend Micro Smart Protection Network

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 6-5. 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.

Using Widgets

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

- Bar graph
- Pie chart
- Line graph
- Table

Click the help icon on a widget to view the following types of information:

TABLE 6-6. Widget Help

WIDGET TOPIC	DESCRIPTION
Overview	Provides a description for the widget and how the widget can be used

TABLE 6-6. Widget Help (Continued)

WIDGET TOPIC	DESCRIPTION
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 6-7. Widget drill-down example

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

The following table lists widgets available on the dashboard.

Note: On parent Control Manager servers, the **Control Manager Top Threats** and **File Reputation Top Threat Detections** widgets require scheduled log updates 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**

TABLE 6-8. Control Manager Widget List

WIDGET	PURPOSE
Threat Detection Results	Use this widget to track which endpoints or managed products need further action from administrators. **Example:** You want to know which endpoints or managed products have viruses that could not be cleaned, deleted, or quarantined.
Policy Violation Detections	Use this widget to track Network VirusWall Enforcer service violations.
Product Component Status	Use this widget to track managed products or endpoints with out of date components. **Example:** You want to know which endpoints with OfficeScan clients do not have the latest version of the Virus Pattern File.
Control Manager Top Threats	Use this widget to track the top malicious files detected or malicious URLs your endpoints access across your network. **Example:** You want to know the top malicious URLs detected by a specific segment of your network.

TABLE 6-8. Control Manager Widget List

WIDGET	PURPOSE
Control Manager Threat Statistics	Use this widget to check the total number of security threat detections on your network. Data can be filtered by security threat type or by the location on your network where the threat is detected. **Example 1:** You want to know the total number of virus detections across your network. **Example 2:** You want to know the total number of security threat detections from file servers on your network.
Smart Protection Network Threat Statistics	Use this widget as a reference for security threat detections on your network, globally, and globally within an industry.
Product Application Compliance	Use this widget to track which managed product's applications are not up to date. **Example:** You want to know which OfficeScan 10 servers are not within three build releases of the latest version of OfficeScan 10.
Product Connection Status	Use this widget to track which managed products are offline, disabled, or that have an abnormal connection to Control Manager.
OfficeScan Endpoint Connection Status	Use this widget to track OfficeScan clients that are offline or roaming.
File Reputation Top Threat Detections	Use this widget as a reference between the top threats globally and the threats on your network.
Web Reputation Top Threat Sources	Use this widget as a reference for global trends in malicious URLs.
Smart Protection Network Connections	Use this widget to track the number of endpoints that connect to the Smart Protection Network.

TABLE 6-8. Control Manager Widget List

WIDGET	PURPOSE
File Reputation Threat Map	Use this widget as a reference for global trends in malicious files.
Email Reputation Threat Map	Use this widget as a reference for global trends in spam.
Web Reputation Top Threatened Users	Use this widget as a reference for global trends in malicious URLs.

Configuring Widgets

"Configuring" a widget means modifying settings for the widget that are readily visible on the widget. Examples include:

TABLE 6-1. Configure Widgets

SETTING	DESCRIPTION
Range	Modify the time range for data that displays: • 24 hours • 1 week • 2 weeks • 1 month
Data aggregation	Modify the aggregation for the data: • Malicious URLs • Malicious files or • Product category • Threat type

TABLE 6-1. Configure Widgets

SETTING	DESCRIPTION
Display	Modify how the data displays • Bar graph • Line graph • Pie chart • Table

Editing Widgets

"Editing" a widget means modifying settings for the widget that are not readily visible on the widget. Click the edit icon to access these settings. Examples include:

TABLE 6-9. Editing Widgets

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

To edit a widget:

Path: Dashboard | <Any tab> | <Any widget with an Edit icon>

1. Navigate to a tab that has a widget with an edit icon.
2. Click the **Edit** icon on the widget. The Edit screen appears.
3. Specify a meaningful title for the widget in the **Title** field.
4. Click the browse button next to **Scope**. A version of the Product Directory appears.
5. Specify the data source for the widget from the Product Directory.
6. Click **OK**.
7. Specify values for any other settings available on the widget.

Note: For more information about "other" settings, check the Help for that specific widget.

8. 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.

To add a widget:

Path: Dashboard | <Any tab>

1. Navigate to any tab on the dashboard.
2. Click **Add Widget**. The Add Widget window appears.
3. Click one of the following to filter the widgets that display:

TABLE 6-10. Widget Categories

CATEGORY	DESCRIPTION
Latest Widgets	Displays only the latest widgets available

TABLE 6-10. Widget Categories

CATEGORY	DESCRIPTION
All Widgets	Displays all widgets available
Smart Protection Server	Displays only Smart Protection Server widgets
Control Manager	Displays only Control Manager widgets
Threat Statistic	Displays only widgets that contain threat statistic information (example: top threats in your network, total number of threats in your network)
Smart Protection Network	Displays only Smart Protection Network widgets
Compliance	Displays only widgets that contain compliance information (example: component compliance, product application compliance)

4. Select one or more widgets to add to a tab.
5. Click **Add and Reload**.

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.

To enable Smart Protection Network Settings Feedback:

Path: Administration > Settings > Smart Protection Network Settings

1. Navigate to the Smart Protection Network Settings screen.
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 7

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

Path: Administration > 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 7-1. 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

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

Understanding Command Details

Path: Administration > Command Tracking | *Tracking Results*

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

TABLE 7-1. 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
Success	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

Table 7-1. General Command Details (Continued)

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 7-2. Command Details for Individual Products or Services

<table>
<tr><th>Information</th><th>Description</th></tr>
<tr><td>Last Reported</td><td>Indicates the date and time when the managed product sends a response to the Control Manager server</td></tr>
<tr><td>Server/Entity</td><td>Indicates the host name of the child or managed product server</td></tr>
<tr><td>Status</td><td>Indicates the status of the issued command
For example, the <b>Status</b> is <b>Skip</b> when you invoke a <b>Deploy patterns/rules</b> task to a child server, and the child server already contains the latest pattern file. These are the Status values.
<table>
<tr><td>Successful</td><td>In Progress</td><td>Unsuccessful</td></tr>
<tr><td>Skip</td><td>Submit</td><td>Time Out</td></tr>
<tr><td>Not supported</td><td>Tracking</td><td>Cancelled</td></tr>
<tr><td>Successful</td><td>Accepted</td><td>Not Available</td></tr>
<tr><td colspan="2"></td><td>Unsuccessful</td></tr>
</table>
</td></tr>
<tr><td>Description</td><td>Explains the Status</td></tr>
</table>

The Command Details screen refreshes every thirty (30) seconds.

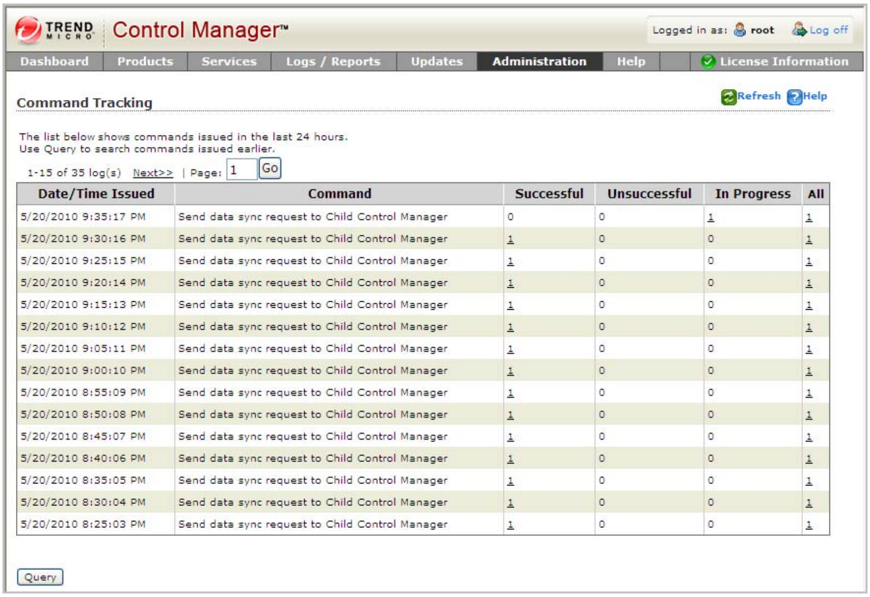
Querying and Viewing Commands

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

To query and view commands issued in the past 24 hours:

Path: Administration > Command Tracking | Query

1. Navigate to the Command Tracking screen.



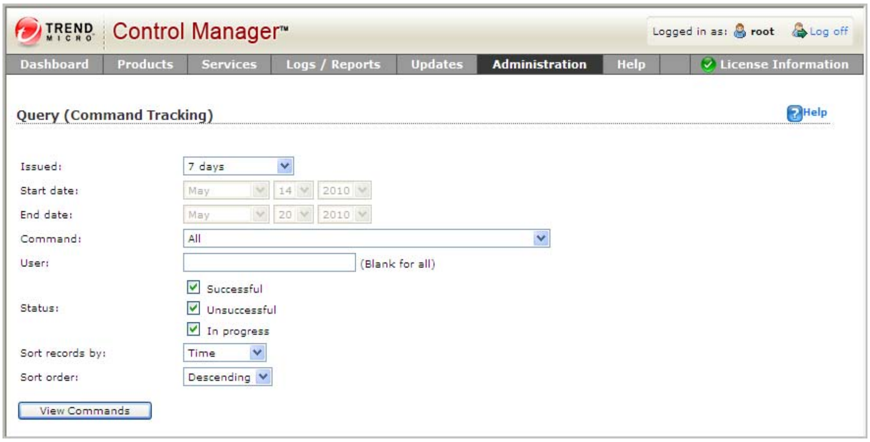
Command Tracking

The list below shows commands issued in the last 24 hours.
Use Query to search commands issued earlier.

1-15 of 35 log(s) Next>> | Page: 1 Go

Date/Time Issued	Command	Successful	Unsuccessful	In Progress	All
5/20/2010 9:35:17 PM	Send data sync request to Child Control Manager	0	0	1	1
5/20/2010 9:30:16 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 9:25:15 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 9:20:14 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 9:15:13 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 9:10:12 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 9:05:11 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 9:00:10 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:55:09 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:50:08 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:45:07 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:40:06 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:35:05 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:30:04 PM	Send data sync request to Child Control Manager	1	0	0	1
5/20/2010 8:25:03 PM	Send data sync request to Child Control Manager	1	0	0	1

2. On the working area, click **Query**. The Query (Command Tracking) screen appears.



Query (Command Tracking)

Issued: 7 days

Start date: May 14 2010

End date: May 20 2010

Command: All

User: (Blank for all)

Status: ☑ Successful ☑ Unsuccessful ☑ In progress

Sort records by: Time

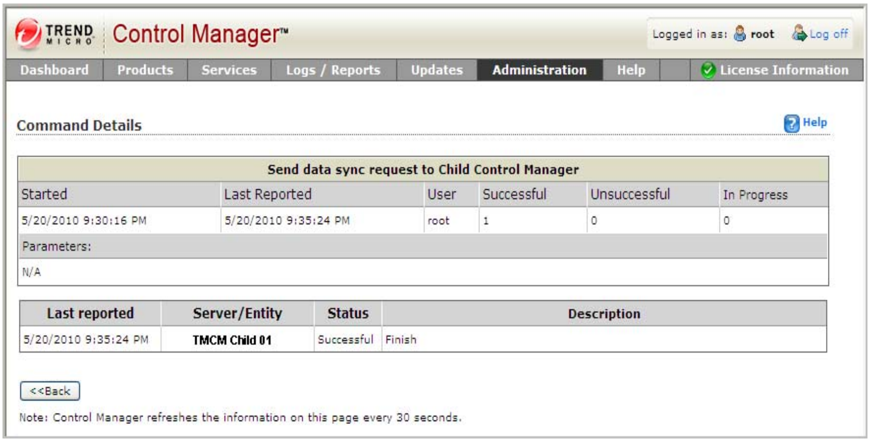
Sort order: Descending

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. Set custom ranges according to months, days, and 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 screen shows the number of products affected by the command, as well as the results.

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



Command Details

Send data sync request to Child Control Manager

Started	Last Reported	User	Successful	Unsuccessful	In Progress
5/20/2010 9:30:16 PM	5/20/2010 9:35:24 PM	root	1	0	0

Parameters:

N/A

Last reported	Server/Entity	Status	Description
5/20/2010 9:35:24 PM	TMCM Child 01	Successful	Finish

Note: Control Manager refreshes the information on this page every 30 seconds.

Chapter 8

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:

Using 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 8-1. Event Center Events

EVENT TYPES	DESCRIPTION
Alert	Provides warning about viruses/spyware/grayware detected by antivirus managed products. For more information, see *Table 8-2* on page 8-3.
Outbreak Prevention Services	Provides information about policy application and update information about Outbreak Prevention Services (OPS). OPS 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
Vulnerability Assessment	Provides "Vulnerability Assessment task completed" event notification.
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 *Table 8-3* on page 8-4.
Unusual	Provides information about product options or service activation and deactivation. For more information, see *Table 8-4* on page 8-4.

TABLE 8-1. Event Center Events (Continued)

EVENT TYPES	DESCRIPTION
Security Violation	Provides warning about email message content violations and client Web violations. For more information, see *Table 8-2* on page 8-3.

Alert Events

TABLE 8-2. Alert Events

ALERT	DESCRIPTION
Virus outbreak alert	Applicable to antivirus managed products
Special virus alert	Applicable to antivirus managed products
Virus found	• 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
Special spyware/grayware alert	Applicable to anti-spyware/grayware managed products
Spyware/Grayware found	• Spyware/Grayware found - first or second actions successful - applicable to anti-spyware/grayware managed products • Spyware/Grayware found - first and second actions unsuccessful/unavailable - applicable to anti-spyware/grayware managed products
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)

Update Alert Events

TABLE 8-3. Update Alert Events

ALERT	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 8-4. 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

Security Violation Events

TABLE 8-5. Security Violation Events

ALERT	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.

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 8-6. 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
`%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 8-7. Virus Notification Message Variables

VARIABLE	DESCRIPTION
Virus variables: Used by alert or Outbreak Prevention Service event notifications	

TABLE 8-7. Virus Notification Message Variables (Continued)

VARIABLE	DESCRIPTION
`%engver%`	• Scan engine version • Used by the alert event category as well as 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 scan engine 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.
`%ptnver%`	• Virus pattern version • Used by the alert event category as well as 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.
`%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

TABLE 8-7. Virus Notification Message Variables (Continued)

VARIABLE	DESCRIPTION
`%vdest%`	• Virus/malware destination. • For example, the intended recipient takes the value of %vdest% if an antivirus managed product detected a virus/malware in an email message. • 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 8-8. 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.

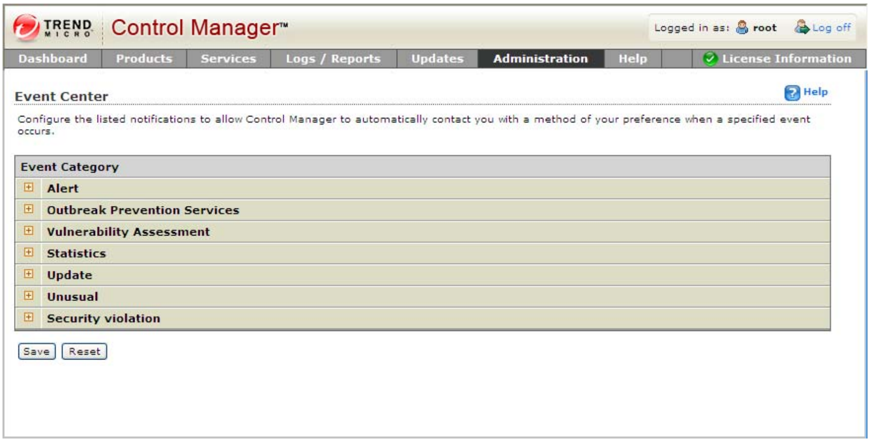
Enabling or Disabling Notifications

Enable or disable notifications from the Event Center screen.

To enable or disable notifications:

Path: Administration > Deployment Plan

1. Navigate to the Event Center screen.



Event Center

Configure the listed notifications to allow Control Manager to automatically contact you with a method of your preference when a specified event occurs.

Event Category
⊞ Alert
⊞ Outbreak Prevention Services
⊞ Vulnerability Assessment
⊞ Statistics
⊞ Update
⊞ Unusual
⊞ Security violation

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**.

Configuring 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 8-9. 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 **Parameter** 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.

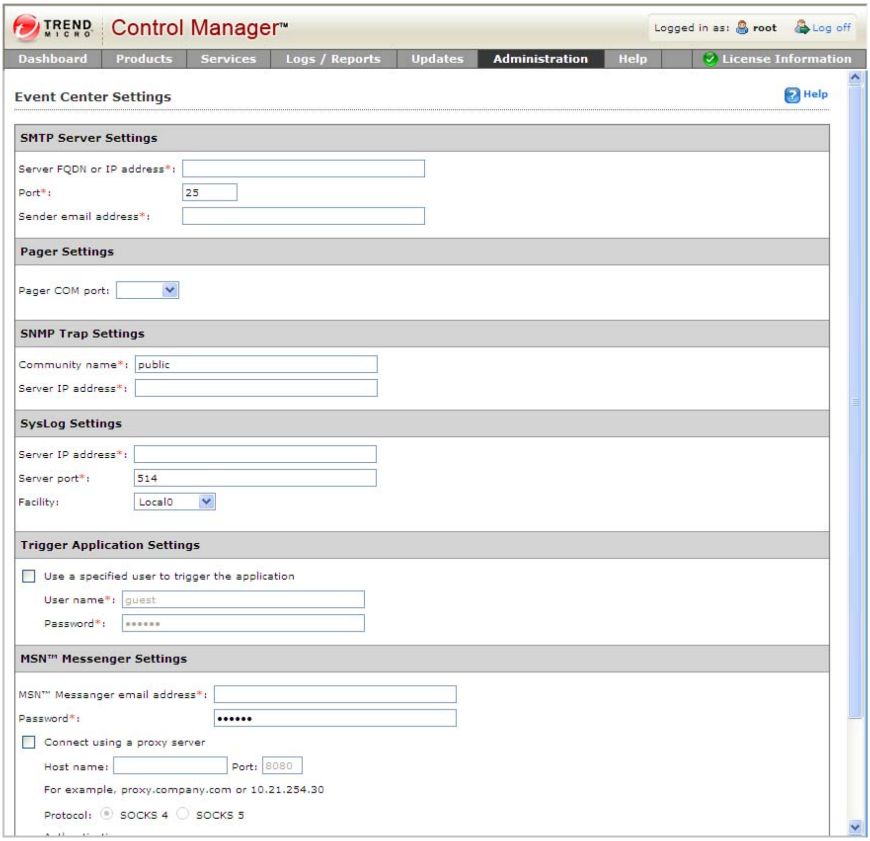
TABLE 8-9. Notification Delivery Methods

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)

To configure notification method settings:

Path: Administration > Settings > Event Center Settings

1. Navigate to the Event Center Settings screen.



Event Center Settings

SMTP Server Settings

Server FQDN or IP address*:

Port*: 25

Sender email address*:

Pager Settings

Pager COM port:

SNMP Trap Settings

Community name*: public

Server IP address*:

SysLog Settings

Server IP address*:

Server port*: 514

Facility: Local0

Trigger Application Settings

□ Use a specified user to trigger the application

User name*: guest

Password*: ••••••

MSN™ Messenger Settings

MSN™ Messanger email address*:

Password*: ••••••

□ Connect using a proxy server

Host name: Port: 8080

For example, proxy.company.com or 10.21.254.30

Protocol: ● SOCKS 4 ○ SOCKS 5

2. Configure the notification method:

   To set email notifications:

   a. On the working area under **SMTP Server Settings**, type the **host name** and **port number** of the SMTP server in the fields provided. Use the fully qualified domain name (FQDN) (example, `proxy.company.com`), or the IP address of the SMTP server.

b. Type the Control Manager **Sender's email address**. Control Manager will use this address as the sender's address (a requirement for some SMTP servers).

To set pager notifications:

- On the working area under **Pager COM Port**, select the appropriate **COM port** from the list.

To set SNMP notifications:

a. On the working area under **SNMP Trap Settings**, specify the **Community name**.

b. Specify the SNMP trap server **IP address.**

To set syslog notifications:

a. On the working area under **Syslog Settings**, type the **host name** and **port number** of the syslog server in the fields provided. Use the fully qualified domain name (FQDN) (example, `proxy.company.com`), or the IP address of the syslog server.

b. Specify the facility for syslogs.

To trigger a specified application:

a. On the working area under **Trigger Application Settings**, select **Use a specified user to trigger the application**.

b. Type the **user name** and **password** of the user who triggers the specified application.

To set MSN Messenger notifications:

a. On the working area under **MSN Messenger Settings**, specify the **MSN Messenger email address**. This is the user name in MSN Messenger.

b. Type the email address **password**.

c. If you use a proxy server to connect to the Internet, select **Use a proxy server to connect to MSN server**.

  i. Specify the proxy server **host name** and **port**.

  ii. Select the proxy server protocol—**SOCKS 4** or **SOCKS 5**.

  iii. Type the **log on name** and **password** used for proxy authentication.

3. Click **Save**.

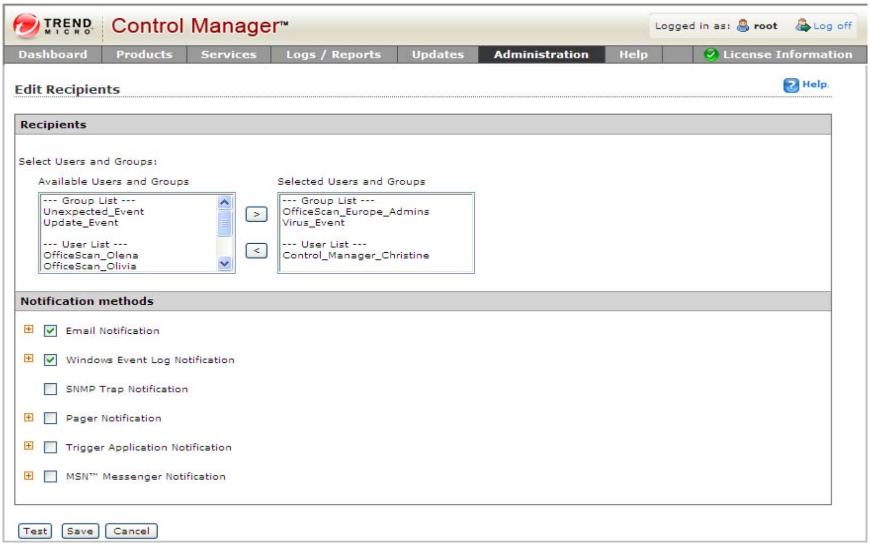
Configuring Notification Recipients and Testing Notification Delivery

Use the Edit Recipients screen to configure the notification recipients for each event.

To configure the notification recipients and test notification delivery:

Path: Administration > Event Center | *Event* | Recipients

1. Navigate to the Event Center screen.
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.



Edit Recipients

Recipients

Select Users and Groups:

Available Users and Groups

```
--- Group List ---
Unexpected_Event
Update_Event

--- User List ---
OfficeScan_Olena
OfficeScan_Olivia
```

Selected Users and Groups

```
--- Group List ---
OfficeScan_Europe_Admins
Virus_Event

--- User List ---
Control_Manager_Christine
```

Notification methods

- ☑ Email Notification
- ☑ Windows Event Log Notification
- □ SNMP Trap Notification
- □ Pager Notification
- □ Trigger Application Notification
- □ MSN™ Messenger Notification

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 **Recipients** list.

To remove a recipient from the list:

a. Click the user or group from the Recipient list. To select multiple recipients, use the CTRL key.

b. Click < to remove the entry from the Recipients list.

5. Select a **notification method**:

   Configure the notification method settings through the Event Center Settings screen. Refer to Configuring Notification Methods on page 8-10.

6. Expand the notification method and provide a **notification message** in the corresponding message fields.
7. Click **Test** to determine if your system can deliver the notifications.
8. Click **Save**.

Configuring Alert Settings

Alert settings specify when a notification is sent to an administrator or other recipients.

Table 8-1 lists the notifications that support modification of notification triggers.

TABLE 8-1. Alert Settings

ALERT	DESCRIPTION
Virus Outbreak	Provide a system-wide perspective on virus/malware outbreaks.

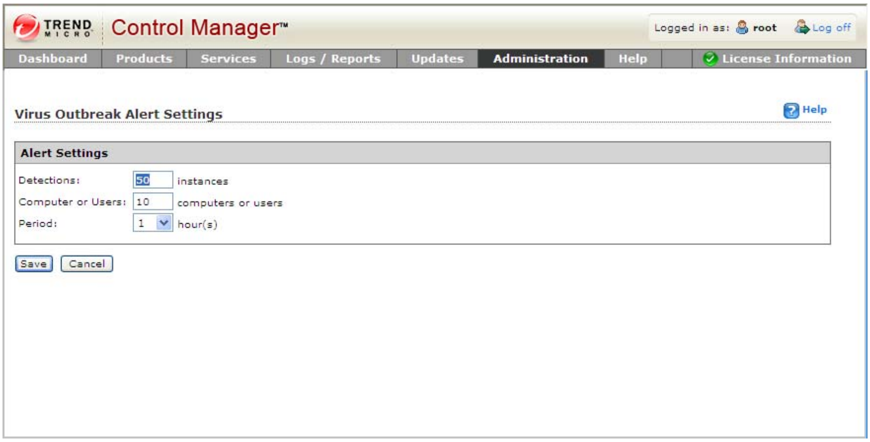
TABLE 8-1. Alert Settings

ALERT	DESCRIPTION
Special Virus	Configure Control Manager to send notifications whenever it detects a virus/malware on your network. Special virus alert notifications provide an early warning of a potential virus/malware outbreak.
Special Spyware/Grayware	Configure Control Manager to send notifications whenever it detects spyware/grayware on your network. Special spyware/grayware alert notifications provide an early warning of potential spyware/grayware.
Network Virus	Network virus alerts provide a system-wide perspective of a potential network virus outbreak.
Potential Vulnerability Attack	Potential vulnerability attack alerts provide a system-wide perspective of a potential attack caused by system vulnerabilities.

To configure virus outbreak alert settings:

Path: Administration > Event Center | *Alert* | *Virus outbreak alert* | Settings

1. Navigate to the Event Center screen.
2. Expand the **Alert** Event Category, and click the **Settings** link for **Virus outbreak alert**. The Virus Outbreak Alert Settings screen appears.



Virus Outbreak Alert Settings

Alert Settings

Detections: 50 instances

Computer or Users: 10 computers or users

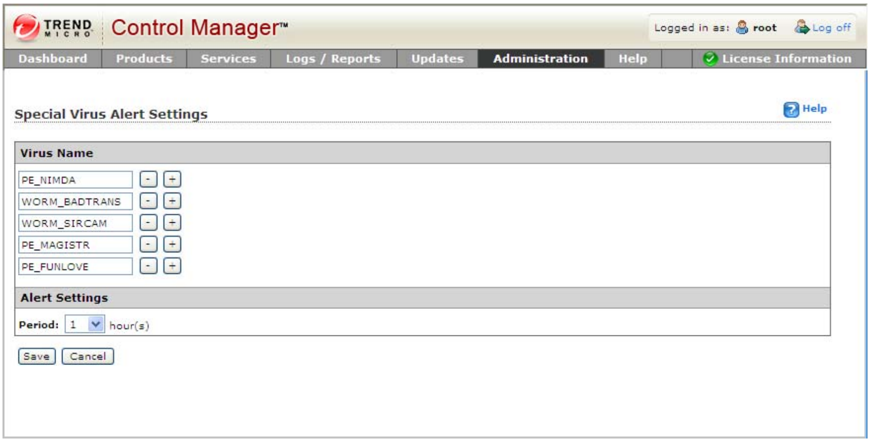
Period: 1 hour(s)

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**.

To configure special virus alert settings:

Path: Administration > Event Center | *Alert* | *Special virus alert* | Settings

1. Navigate to the Event Center screen.
2. Expand the **Alert** Event Category, and click the **Settings** link for **Special virus alert**.



Special Virus Alert Settings

Virus Name

PE_NIMDA
WORM_BADTRANS
WORM_SIRCAM
PE_MAGISTR
PE_FUNLOVE

Alert Settings

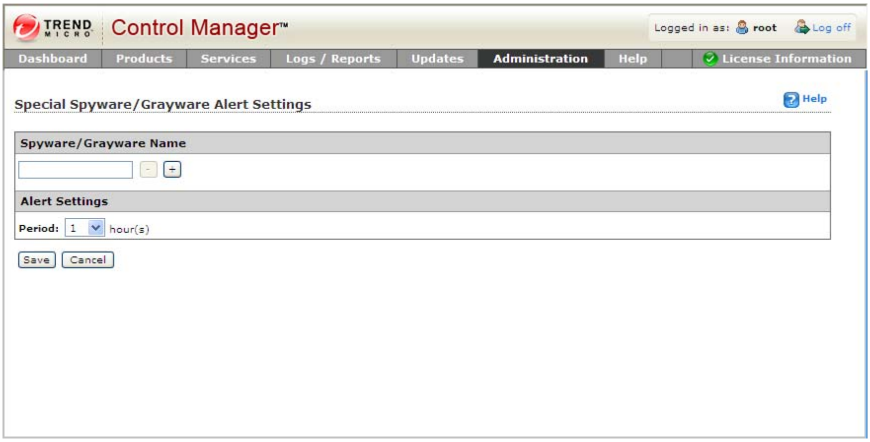
Period: 1 hour(s)

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**.

To configure special spyware/grayware alert settings:

Path: Administration > Event Center | *Alert* | *Special spyware/grayware alert* | Settings

1. Navigate to the Event Center screen.
2. Expand the **Alert** Event Category, and click the **Settings** link for **Special spyware/grayware alert**.



Special Spyware/Grayware Alert Settings

Spyware/Grayware Name

Alert Settings

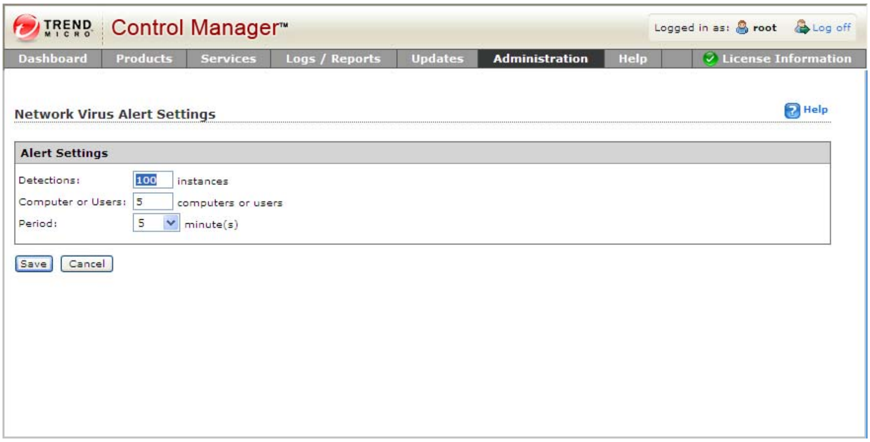
Period: 1 hour(s)

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**.

To configure network virus alert settings:

Path: Administration > Event Center | *Alert* | *Network virus alert* | Settings

1. Navigate to the Event Center screen.
2. Expand the **Alert** Event Category, and click the **Settings** link for **Network virus alert**.



Network Virus Alert Settings

Alert Settings

Detections: 100 instances

Computer or Users: 5 computers or users

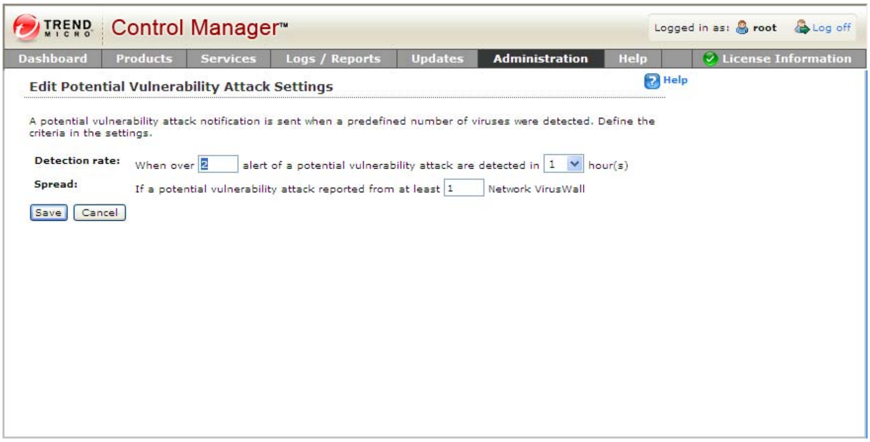
Period: 5 minute(s)

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**.

To configure potential vulnerability attack detected settings:

Path: Administration > Event Center | *Alert* | *Potential vulnerability attack detected* | Settings

1. Navigate to the Event Center screen.
2. Expand the **Alert** Event Category, and click the **Settings** link for **Potential vulnerability attack detected**.



Edit Potential Vulnerability Attack Settings

A potential vulnerability attack notification is sent when a predefined number of viruses were detected. Define the criteria in the settings.

Detection rate: When over 2 alert of a potential vulnerability attack are detected in 1 hour(s)

Spread: If a potential vulnerability attack reported from at least 1 Network VirusWall

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**.

Chapter 9

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

The Control Manager logs are separated into: License and Control Manager Information.

TABLE 9-1. 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.

Managed products generate different kinds of logs depending on their function.

TABLE 9-2. 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
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 • Suspicious Threat Information • Overall Threat Information

Tip: 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.

Understanding Log Aggregation

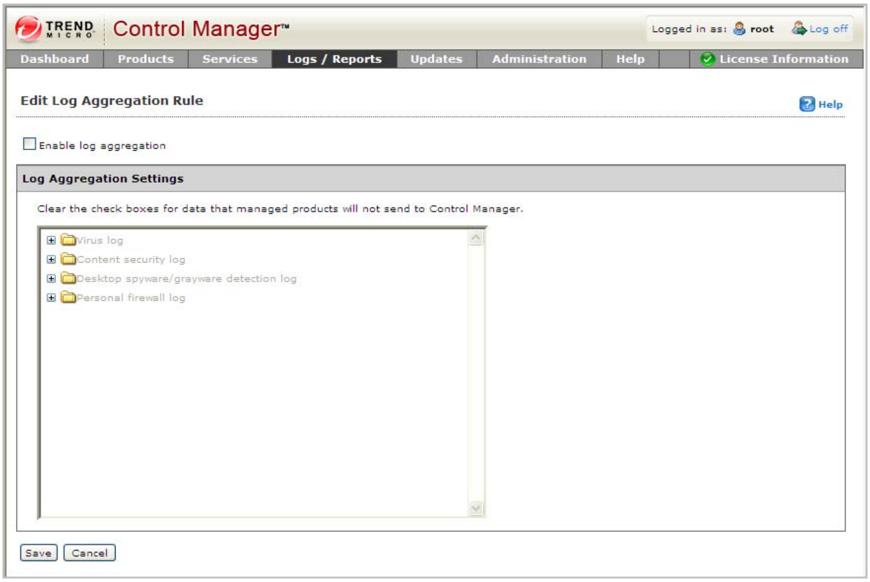
Control Manager log aggregation provides a way for administrators to decrease the impact that managed products have on network bandwidth. By configuring log aggregation administrators can choose which log information managed products send to Control Manager.

WARNING! **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.**

To configure log aggregation settings:

Path: Logs/Reports > Settings > Log Aggregation Settings

1. Navigate to the Edit Log Aggregation Rule screen.



Edit Log Aggregation Rule

□ Enable log aggregation

Log Aggregation Settings

Clear the check boxes for data that managed products will not send to Control Manager.

⊞ Virus log
⊞ Content security log
⊞ Desktop spyware/grayware detection log
⊞ Personal firewall log

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 **Logs/Reports > 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 5.5 allows direct queries to the Control Manager database. Data views are available to Control Manager 5 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 9-1. 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 two major categories: Product Information and Security Threat Information. See *Understanding Data Views* on page B-2 for more information about data views. The major categories separate further into several subcategories, with the subcategories separated into summary information and detailed information.

Product Information

Product Information data views provide information about Control Manager, managed products, components, and product licenses.

TABLE 9-2. 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 9-3. Security Threat Information Data Views

CATEGORY	DESCRIPTION
Overall Threat Information	Displays summary and statistical data about the overall threat landscape of your network.

TABLE 9-3. 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.
Web Violation Information	Displays summary and detailed data about Internet violations that managed products detect on your network.
Policy/Rule Violation Information	Displays summary and detailed data about policy/rule violations that managed products detect on your network.
Suspicious Threat Information	Displays summary and detailed data about suspicious activity that managed products detect on your network.

Note: For more information about the available data views Control Manager supports, see *Understanding Data Views* on page B-2.

Data View Terminology

Control Manager uses the following terms in data views, returned queries, and generated reports.

TABLE 9-3. 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.
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.

TABLE 9-3. Data View Terminology

DATA	DESCRIPTION
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

TABLE 9-3. Data View Terminology

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

Performing an Ad Hoc Query

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 9-5.

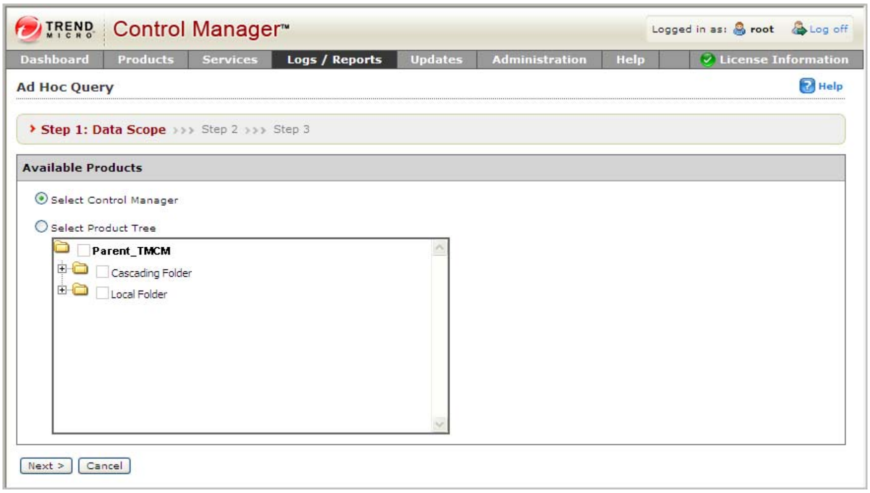
For example, Chris, an OfficeScan administrator, wants to check the status of pattern files for the OfficeScan servers for which she is responsible. Chris first selects **Managed Products**. She then selects the data view **Managed Product Pattern File Status** found under **Product Information > Component 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.

To perform an Ad Hoc query:

Path: Logs/Reports > New Ad Hoc Query

1. Navigate to the Ad Hoc Query screen.

Step 1: Specify the Origin of the Information:



● Select Control Manager

○ Select Product Tree

- □ Parent_TMCM
  - □ Cascading Folder
  - □ Local Folder

1. From the New 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.

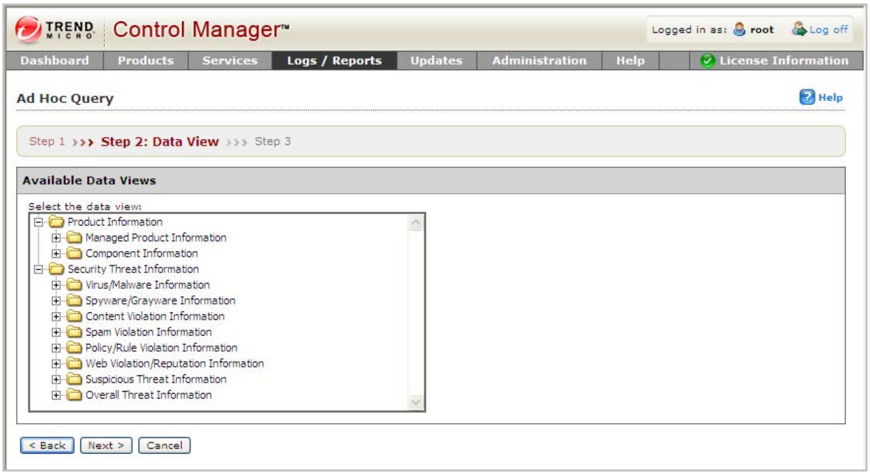
     After specifying this option, the user must then select the managed products or directory from which the information originates.

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**. The Step 2: Data View screen appears.

Step 2: Specify a Data View for the Query:



Ad Hoc Query

Step 1 >>> Step 2: Data View >>> Step 3

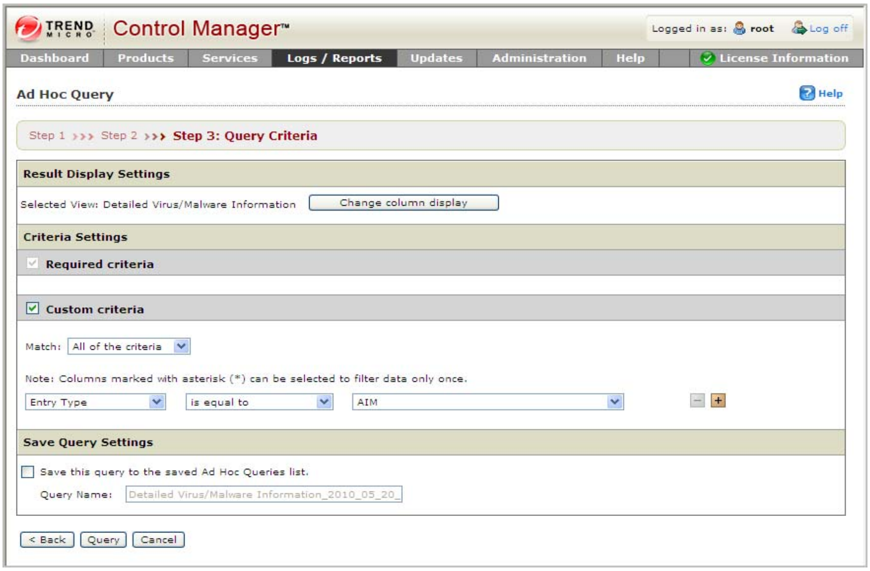
Available Data Views

Select the data view:

- Product Information
  - Managed Product Information
  - Component Information
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
  - Content Violation Information
  - Spam Violation Information
  - Policy/Rule Violation Information
  - Web Violation/Reputation Information
  - Suspicious Threat Information
  - Overall Threat Information

1. Select a data view from the **Available Data Views** list. For more information on data views, see *Understanding Data Views* on page 9-5.
2. Click **Next**. The Step 3: Query Criteria screen appears.

Step 3: Specify the Display Sequence:



Ad Hoc Query

Step 1 >>> Step 2 >>> Step 3: Query Criteria

Result Display Settings

Selected View: Detailed Virus/Malware Information [Change column display]

Criteria Settings

☑ Required criteria

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Entry Type | is equal to | AIM

Save Query Settings

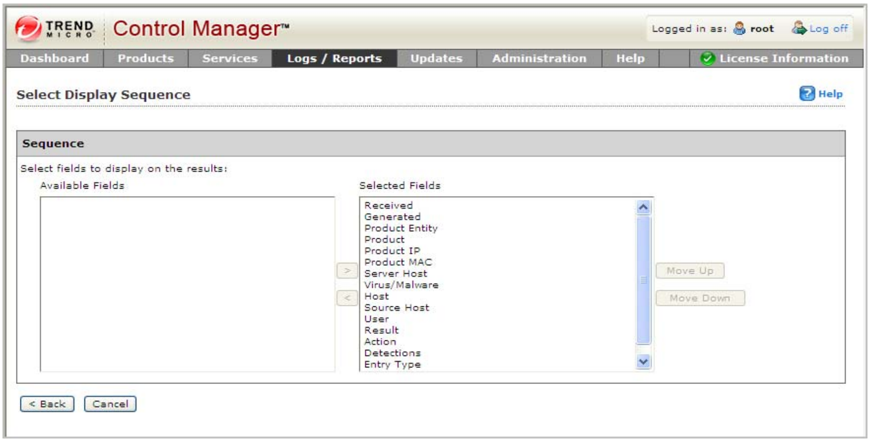
□ Save this query to the saved Ad Hoc Queries list.

Query Name: Detailed Virus/Malware Information_2010_05_20_

[< Back] [Query] [Cancel]

Specify the display and sequence for the information the query returns:

1. Click **Change column display**. The Select Display Sequence screen appears.



Selected Fields
Received
Generated
Product Entity
Product
Product IP
Product MAC
Server Host
Virus/Malware
Host
Source Host
User
Result
Action
Detections
Entry Type

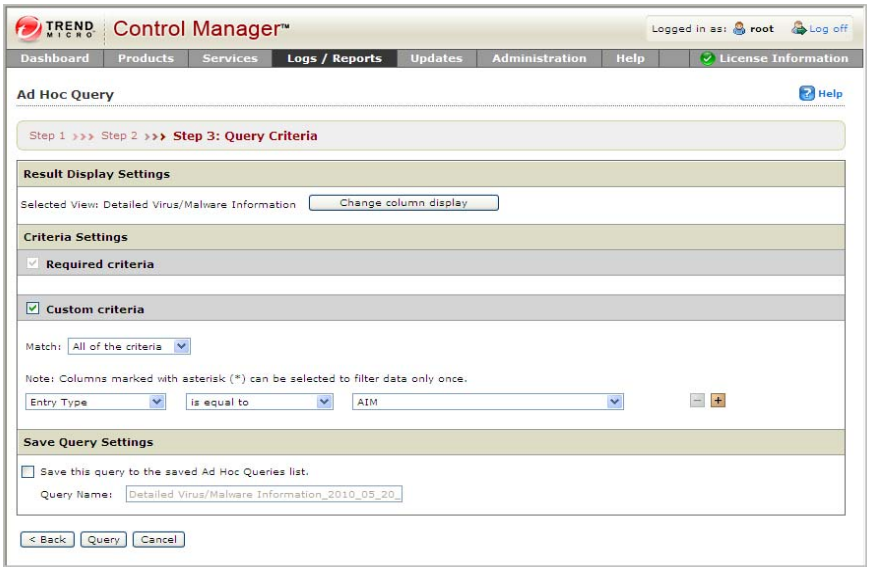
2. From the **Available Fields** list, select the data view columns to display when the query returns information. Selected columns highlight.

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 in which the information displays.

3. Click the **Add** button 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**. The Query Criteria screen appears.

Step 4: Specify the Filtering Criteria:



Ad Hoc Query

Step 1 >>> Step 2 >>> **Step 3: Query Criteria**

Result Display Settings

Selected View: Detailed Virus/Malware Information

Criteria Settings

☑ Required criteria

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Entry Type | is equal to | AIM

Save Query Settings

□ Save this query to the saved Ad Hoc Queries list.

Query Name: Detailed Virus/Malware Information_2010_05_20_

When querying for summary data (any data view with the word Summary in the title), you must specify items under Required Criteria.

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.

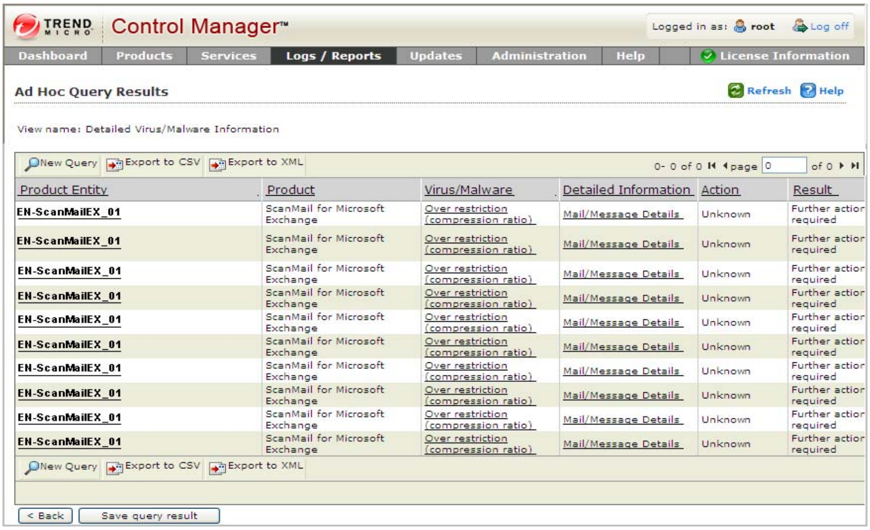
- **i.** From the left-most drop-down list, select the column to filter.
- **ii.** From the middle drop-down list, select the matching condition for the filter.
- **iii.** In the right-most field, provide the filter criteria. A list box or text box appears here depending on the column selected to filter.
- **iv.** Click the + icon to add another filter criterion for the data view.

Step 5: Save and Complete the Query:

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 **Logs/Reports > Saved Ad Hoc Queries** screen.

3. Click **Query**. The Results screen appears displaying the results of the query.

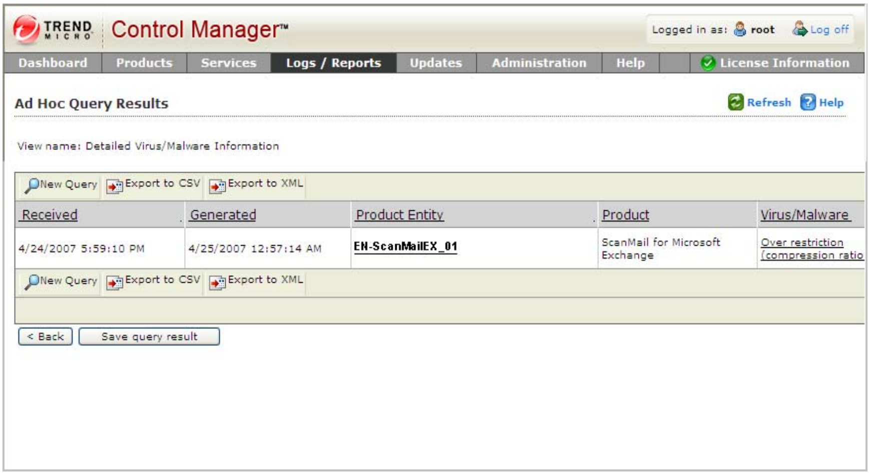


Ad Hoc Query Results

View name: Detailed Virus/Malware Information

Product Entity	Product	Virus/Malware	Detailed Information	Action	Result
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actior required

For more detailed information about a given item, click the underlined link for the item.



Ad Hoc Query Results

View name: Detailed Virus/Malware Information

Received	Generated	Product Entity	Product	Virus/Malware
4/24/2007 5:59:10 PM	4/25/2007 12:57:14 AM	EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio

Step 6: Export the query results to CSV or XML:

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**. The saved query appears on the Saved Ad Hoc Queries screen.

Working With Saved and Shared Ad Hoc Queries

Path: Logs/Reports > Saved 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 screen, 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 type, 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. Modifying a saved Ad Hoc query requires the following steps:

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

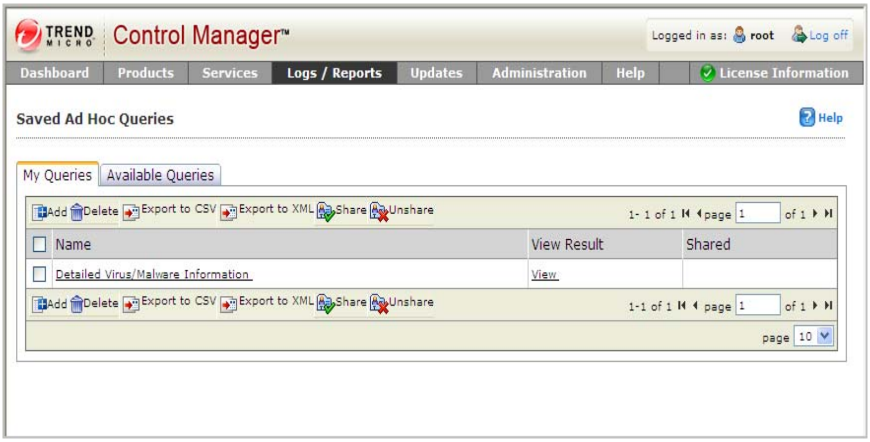
Step 4: Save and complete the query

Step 5: Export the data to CSV or XML

To edit a saved Ad Hoc query:

Path: Logs/Reports > Saved Ad Hoc Queries

1. Navigate to the Saved Ad Hoc Queries screen.



☐ Name	View Result	Shared
☐ Detailed Virus/Malware Information	View	

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:

1. From the New 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 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**. The Select Data View screen appears.

Step 2: Specify a data view for the query:

1. Select a data view from the **Available Data Views** list. For more information on data views, see *Understanding Data Views* on page 9-5.
2. Click **Next**. The Query Criteria screen appears.

Step 3: Specify the display sequence:

Specify the display and sequence for the information the query returns:

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 the **Add** button 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**. The Query Criteria screen appears.

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.

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:

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 **Logs/Reports > My Reports** screen.

3. Click **Query**. The Results screen appears displaying the results of the query.

Step 6: Export the query results to CSV or XML:

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.

To share a saved Ad Hoc query:

Path: Logs/Reports > Saved Ad Hoc Queries

1. Navigate to the Saved Ad Hoc Queries screen.
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.

To access the Available Queries tab:

Path: Logs/Reports > Saved Ad Hoc Queries | Available Queries

1. Navigate to the Saved Ad Hoc Queries screen.
2. Click **Available Queries**. The Available Queries tab appears.
3. Use the queries to view information or to export shared queries.

Deleting Logs

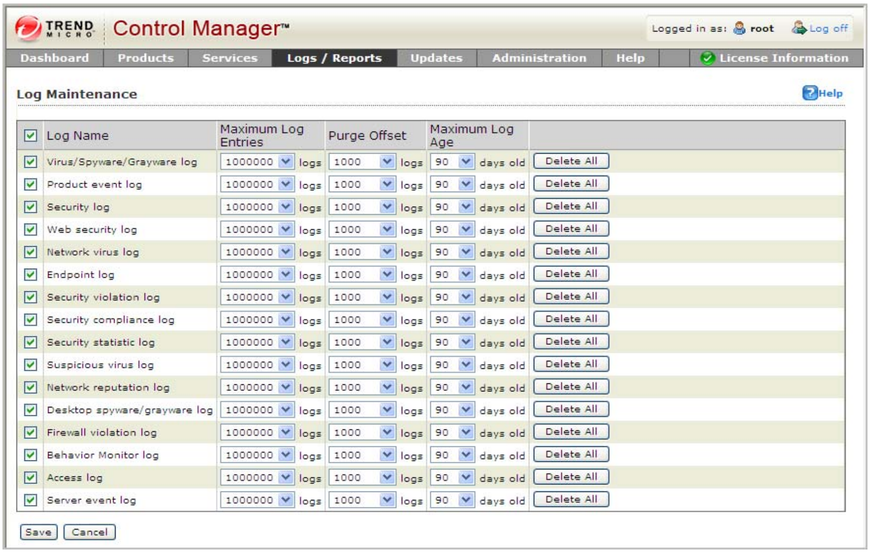
Use the Log Maintenance screen to immediately delete logs or to configure automatic log deletion for the following log types:

- Virus/Spyware/Grayware logs
- Product event logs
- Security logs
- Web security logs
- Network virus logs
- Endpoint logs
- Security violation logs
- Security compliance logs
- Security statistic logs
- Suspicious virus logs
- Network reputation logs
- Desktop spyware/grayware logs
- Firewall violation logs
- Behavior monitoring logs
- Access logs
- Server event logs

To delete logs immediately:

Path: Logs/Reports > Settings > Log Maintenance

1. Navigate to the Log Maintenance screen.



☑	Log Name	Maximum Log Entries		Purge Offset		Maximum Log Age		
☑	Virus/Spyware/Grayware log	1000000	logs	1000	logs	90	days old	Delete All
☑	Product event log	1000000	logs	1000	logs	90	days old	Delete All
☑	Security log	1000000	logs	1000	logs	90	days old	Delete All
☑	Web security log	1000000	logs	1000	logs	90	days old	Delete All
☑	Network virus log	1000000	logs	1000	logs	90	days old	Delete All
☑	Endpoint log	1000000	logs	1000	logs	90	days old	Delete All
☑	Security violation log	1000000	logs	1000	logs	90	days old	Delete All
☑	Security compliance log	1000000	logs	1000	logs	90	days old	Delete All
☑	Security statistic log	1000000	logs	1000	logs	90	days old	Delete All
☑	Suspicious virus log	1000000	logs	1000	logs	90	days old	Delete All
☑	Network reputation log	1000000	logs	1000	logs	90	days old	Delete All
☑	Desktop spyware/grayware log	1000000	logs	1000	logs	90	days old	Delete All
☑	Firewall violation log	1000000	logs	1000	logs	90	days old	Delete All
☑	Behavior Monitor log	1000000	logs	1000	logs	90	days old	Delete All
☑	Access log	1000000	logs	1000	logs	90	days old	Delete All
☑	Server event log	1000000	logs	1000	logs	90	days old	Delete All

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: 90 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.

To configure purge log settings:

Path: Logs/Reports > Settings > Log Maintenance

1. Navigate to the Log Maintenance screen.
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 10

Working with Reports

Query logs from all managed products registered to Control Manager from the Ad Hoc Query screen.

This chapter contains the following topics:

Working With 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 5.5 continues to support report templates from previous Control Manager versions, however Control Manager 5.5 allows administrators to design their own custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager 5.5 categorizes report templates according to the following types:

- **Control Manager 5 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 Control Manager 5 templates, see Understanding Control Manager 5 Templates on page 10-3.
- **Control Manager 3 templates:** Includes all templates provided in Control Manager 3.0 and Control Manager 3.5. For more information on Control Manager 3 templates, see Understanding Control Manager 3 Templates on page 10-9.

Understanding Control Manager 5 Templates

Control Manager 5 report templates use database views as the information foundation for reports. For more information on data views, see Understanding Data Views on page 9-5. The look and feel of generated reports falls to the report elements. Report elements consist of the following.

TABLE 10-1. Control Manager 5 Report 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 Control Manager 5 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 Control Manager 5 report 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 10-2. Control Manager 5 Pre-defined Templates

TEMPLATE	DESCRIPTION
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)

TABLE 10-2. Control Manager 5 Pre-defined Templates

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)

TABLE 10-2. Control Manager 5 Pre-defined Templates

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)

TABLE 10-2. Control Manager 5 Pre-defined Templates

TEMPLATE	DESCRIPTION
TM-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)

TABLE 10-2. Control Manager 5 Pre-defined Templates

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)

TABLE 10-2. Control Manager 5 Pre-defined Templates

TEMPLATE	DESCRIPTION
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 Control Manager 3 Templates

Control Manager 3.0/3.5 added 65 pre-generated report templates divided into six categories: Executive Summary, Gateway, Mail Server, Server, Desktop, and Network Products.

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.

Use the **Report Category** list on the Control Manager 3 Report Templates screen to peruse the six categories of reports listed below:

TABLE 10-3. 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)
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 10-4. 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 10-5. 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)

TABLE 10-5. Mail Server Product Reports and Report Types

MAIL SERVER PRODUCT REPORTS	REPORT TYPES
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 10-6. 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 10-7. Desktop Product Reports and Report Types

DESKTOP 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)
OfficeScan Client Information Reports	• Detailed summary • Basic summary
OfficeScan Product Registration Report	Registration status

TABLE 10-7. Desktop Product Reports and Report Types

DESKTOP PRODUCT REPORTS	REPORT TYPES
Comparative reports	• 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 10-8. Network Product Reports and Report Types

NETWORK PRODUCT REPORTS	REPORT TYPES
Network VirusWall Reports	Policy Violation report, grouped by (Day, Week, Month)
	Service Violation report, grouped by (Day, Week, Month)
	Most commonly detected violative clients (10, 25, 50, 100)
Trend Micro Total Discovery Appliance Reports	Incident summary report, grouped by (Day, Week, Month)
	High risk clients (10, 25, 50, 100)
	Summary of known and unknown risks report

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.

Adding Control Manager 5 Report Templates

Control Manager 5 templates allow greater flexibility for report generation than previous versions of Control Manager templates. Control Manager 5 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 Control Manager 5 custom template requires the following steps:

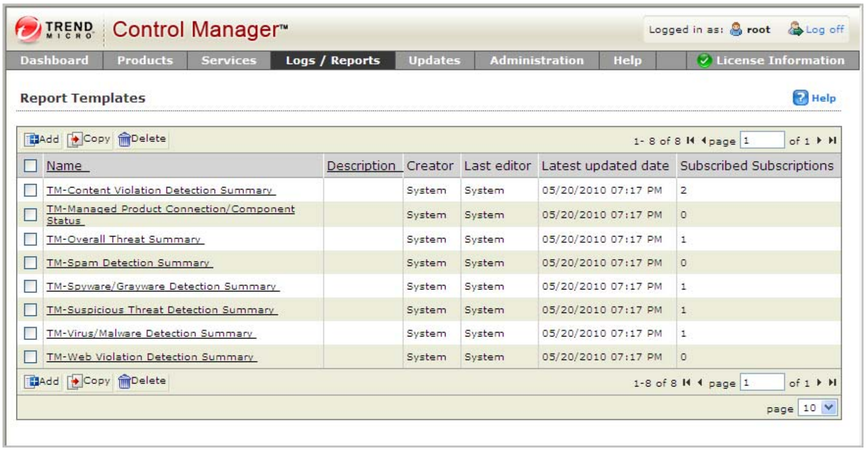
1. Access the Add Report Template screen and name the template.
2. Specify the template component to add to the report template.
3. Specify the data view for the template.
4. Specify the query criteria for the template.
5. Specify the data to appear in the report and the order in which the data appears.
6. Complete report template creation.

To add a Control Manager 5 report template:

Step 1: Access the Add Report Template screen and name the template:

Path: Logs/Reports > Report Templates

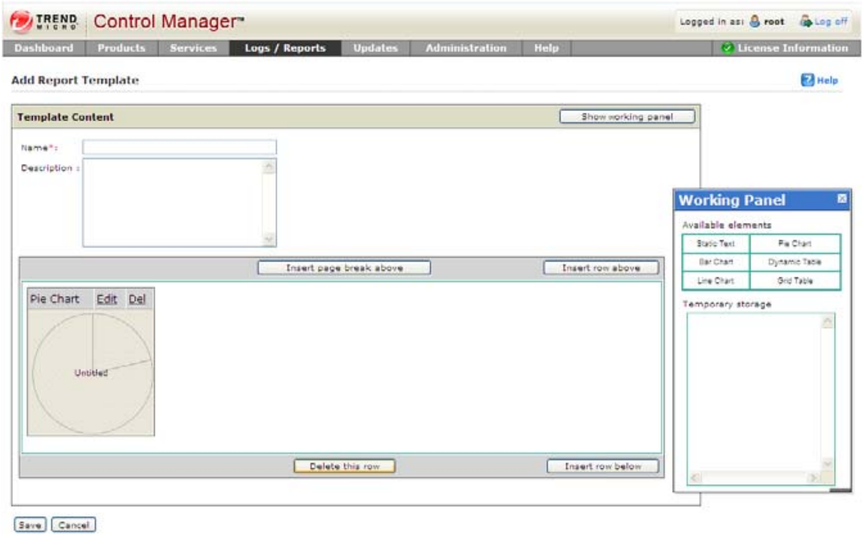
1. Navigate to the Report Templates screen.



Report Templates

□	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
□	TM-Content Violation Detection Summary		System	System	05/20/2010 07:17 PM	2
□	TM-Managed Product Connection/Component Status		System	System	05/20/2010 07:17 PM	0
□	TM-Overall Threat Summary		System	System	05/20/2010 07:17 PM	1
□	TM-Spam Detection Summary		System	System	05/20/2010 07:17 PM	0
□	TM-Spyware/Grayware Detection Summary		System	System	05/20/2010 07:17 PM	1
□	TM-Suspicious Threat Detection Summary		System	System	05/20/2010 07:17 PM	1
□	TM-Virus/Malware Detection Summary		System	System	05/20/2010 07:17 PM	1
□	TM-Web Violation Detection Summary		System	System	05/20/2010 07:17 PM	0

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:

1. Drag-and-drop a report template element from the Working Panel to add 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

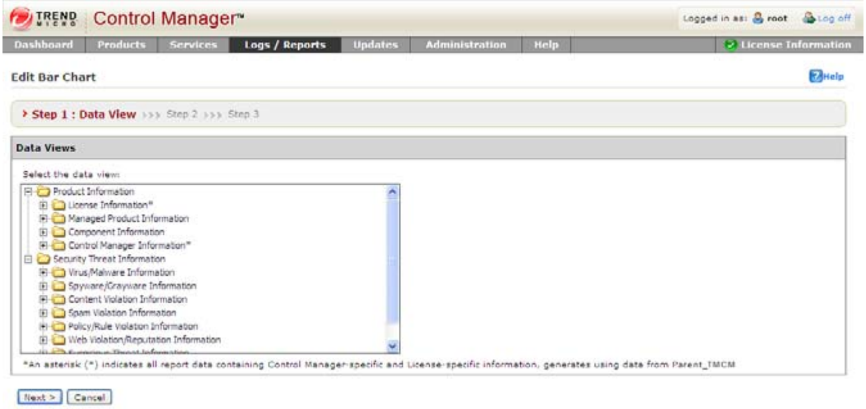
2. Add multiple components to make the report comprehensive. You can add up to three components per page and 100 report components to a report template.

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:

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. Selecting **Static Text** opens the Edit Static Text screen.



Edit Bar Chart

› Step 1 : Data View >>> Step 2 >>> Step 3

Data Views

Select the data view:

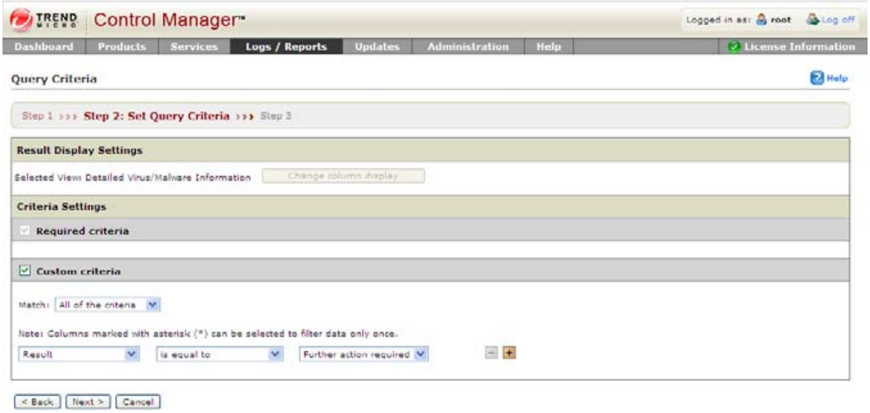
- Product Information
  - License Information*
  - Managed Product Information
  - Component Information
  - Control Manager Information*
- Security Threat Information
  - Virus/Malware Information
  - Spyware/Grayware Information
  - Content Violation Information
  - Spam Violation Information
  - Policy/Rule Violation Information
  - Web Violation/Reputation Information

*An asterisk (*) indicates all report data containing Control Manager-specific and License-specific information, generates using data from Parent_TMCM

2. Select the data to query from the **Data Views** area.

   For more information on Data Views, see Understanding Data Views on page B-2.

3. Click **Next**. The Step 2: Set Query Criteria screen appears.



Query Criteria

Step 1 ››› **Step 2: Set Query Criteria** ››› Step 3

Result Display Settings

Selected View: Detailed Virus/Malware Information

Criteria Settings

☑ Required criteria

☑ Custom criteria

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Result | is equal to | Further action required

Step 4: Specify the query criteria for the template:

Tip: 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.

1. Click **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.

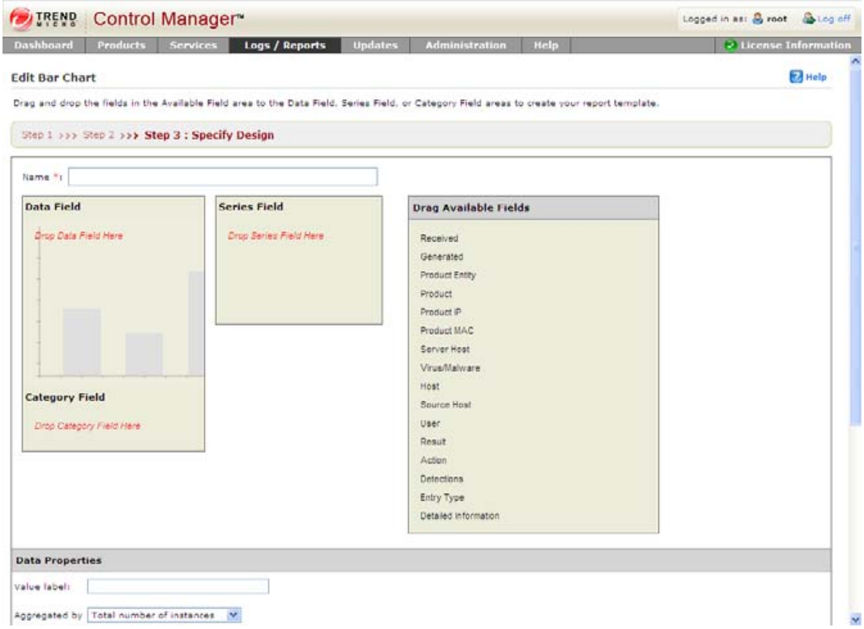
Step 5: Specify the data to appear in the report and the order in which the data appears

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

Configure bar chart settings:

1. Click **Next**. The Add Bar Chart > Step 3 Specify Design screen appears.



Edit Bar Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *:

Data Field

Series Field

Category Field

Drag Available Fields

Received
Generated
Product Entity
Product
Product IP
Product MAC
Server Host
Virus/Malware
Host
Source Host
User
Result
Action
Detections
Entry Type
Detailed Information

Data Properties

Value label:

Aggregated by: Total number of instances

2. Type a name for the bar chart in the **Name** field.

3. Drag-and-drop 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 display settings for the Data Field:
   a. Type a meaningful label for the Data Field.

   b. Specify how data displays for Data Field from the **Aggregated by** drop-down 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 display settings for the Series Field:
   a. Type a meaningful label for the Series Field.
6. Specify the display settings for the Category Field:
   a. Type a meaningful label for the Category Field.

   b. Specify how to sort data in the chart from the **Sorting** drop-down lists:

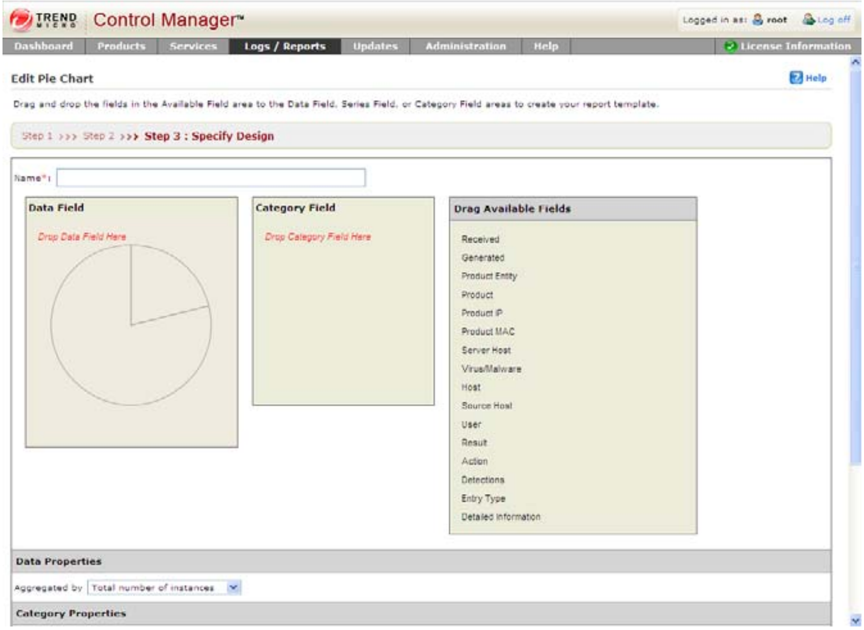
      - **Aggregation value:** Specifies data sorts from the data appearing in the Category fields.
      - **Category name:** Specifies data sorts from the alphabetical value of Category names.
      - **Ascending:** Specifies data sorts in ascending order.
      - **Descending:** Specifies data sorts in descending order.

   c. Specify how many items display in the Categories Field by selecting **Filter summarized result** and specifying a value in the **Display top** text box. 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.

Configure pie chart settings:

1. Click **Next**. The Add Pie Chart > Step 3 Specify Design screen appears.



Edit Pie Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name*:

Aggregated by: Total number of instances

2. Type a name for the pie chart in the **Name** field.
3. Drag-and-drop 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 display settings for the Data Field.

   a. Type a meaningful label for the Data Field.

   b. Specify how data displays for Data Field from the Aggregated by drop-down 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 display settings for the Category Fields:

   a. Type a meaningful label for the Category Fields.

   b. Specify how to sort data in the chart from the Sorting drop-down lists:

      - **Aggregation value:** Specifies data sorts from the data appearing in the Category fields.
      - **Category name:** Specifies data sorts from the alphabetical value of Category names.
      - **Ascending:** Specifies data sorts in ascending order.
      - **Descending:** Specifies data sorts in descending order.

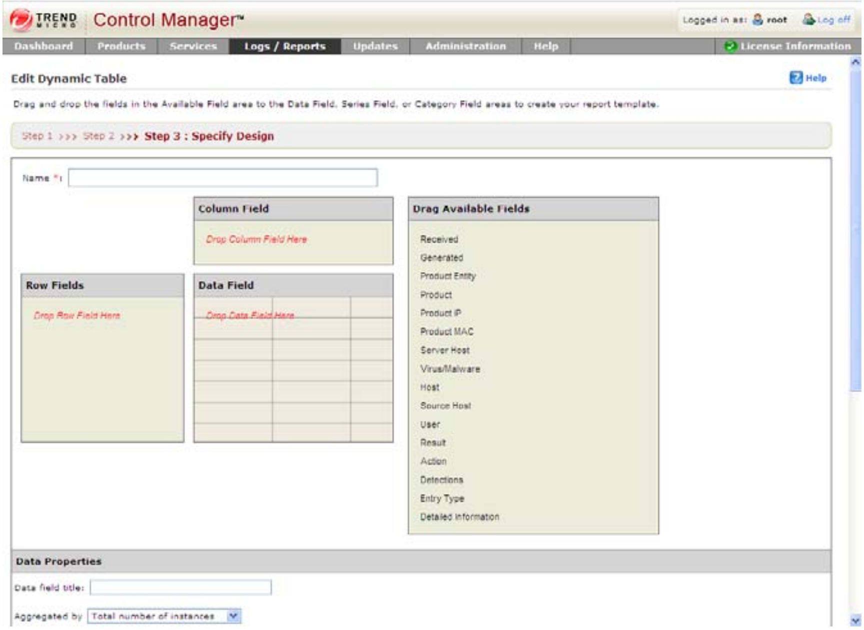
   c. Specify how many items display in the Categories Field by selecting **Filter summarized result** and specifying a value in the **Display top** text box. Default value is 10.

   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.

Configure dynamic table settings:

1. Click **Next**. The Add Dynamic Table > Step 3 Specify Design screen appears.



Edit Dynamic Table

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name *:

Column Field: Drop Column Field Here

Row Fields: Drop Row Field Here

Data Field: Drop Data Field Here

Drag Available Fields:
- Received
- Generated
- Product Entity
- Product
- Product IP
- Product MAC
- Server Host
- Virus/Malware
- Host
- Source Host
- User
- Result
- Action
- Detections
- Entry Type
- Detailed Information

Data Properties

Data field title:

Aggregated by: Total number of instances

2. Type a name for the table in the **Name** field.
3. Drag-and-drop items from the Drag Available Fields list to the following areas:
   - **Data Properties:** Specifies the total count for data appearing in the table
   - **Row Properties:** Specifies how the data is separated horizontally in the table

     You can drag two Available Fields to Row Properties
   - **Column Properties:** 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 and drops the following fields to the Data, Row, and Column Properties:

   - Data Properties: Detections

- Row Properties: Virus/Malware and Action
- Column Properties: Host

4. Specify the display settings for the Data Properties:

   a. Specify how data displays for Data Fields from the Aggregated by drop-down 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 display settings for the Row Properties.

   a. Specify how to sort data in the table from the Sorting drop-down lists:

   - **Aggregation value:** Specifies data sorts from the data appearing in the rows.
   - **Header title:** Specifies data sorts from the alphabetical value of rows.
   - **Ascending:** Specifies data sorts in ascending order.
   - **Descending:** Specifies data sorts in descending order.

   b. Specify how many items display in the Categories Field by selecting **Filter summarized result** and specifying a value in the **Display top** text box. Default value is 10.

6. Specify the display settings for the Column Properties.

   a. Specify how to sort data in the table from the Sorting drop-down lists:

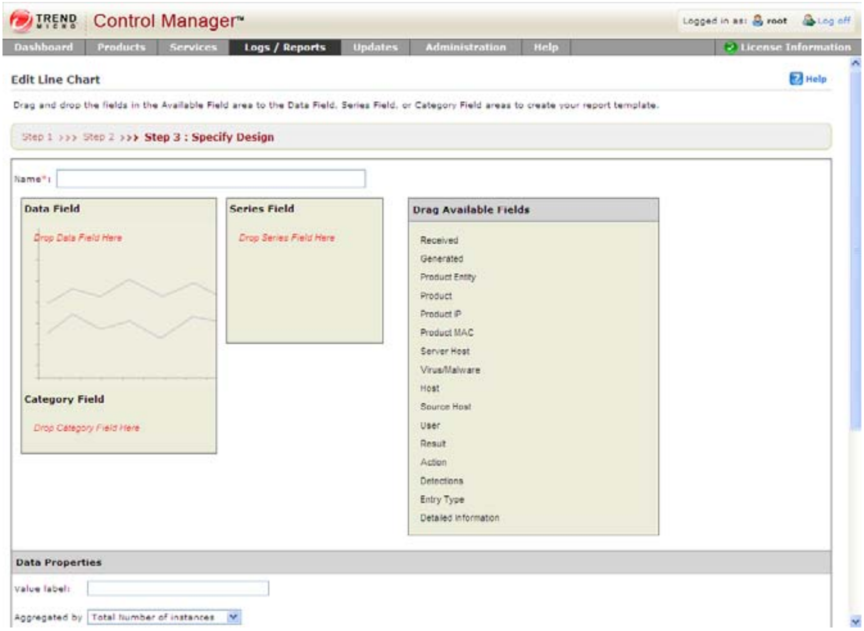
   - **Aggregation value:** Specifies data sorts from the data appearing in the columns.
   - **Header title:** Specifies data sorts from the alphabetical value of columns.
   - **Ascending:** Specifies data sorts in ascending order.
   - **Descending:** Specifies data sorts in descending order.

b. Specify how many columns display by selecting **Filter column** and specifying a value in the **Display quantity** text box. Default value is 10.

7. Click **Save**. The Add Report Template screen appears.

Configure line chart settings:

1. Click **Next**. The Add Line Chart > Step 3 Specify Design screen appears.



Edit Line Chart

Drag and drop the fields in the Available Field area to the Data Field, Series Field, or Category Field areas to create your report template.

Step 1 >>> Step 2 >>> Step 3 : Specify Design

Name*:

Data Field

Drop Data Field Here

Category Field

Drop Category Field Here

Series Field

Drop Series Field Here

Drag Available Fields

Received
Generated
Product Entity
Product
Product IP
Product MAC
Server Host
Virus/Malware
Host
Source Host
User
Result
Action
Detections
Entry Type
Detailed Information

Data Properties

Value label:

Aggregated by: Total Number of instances

2. Type a name for the line chart in the **Name** field.

3. Drag-and-drop 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 and drops the following fields to the Data, Series, and Category Fields:

- Data Properties: Detections
- Category Properties: Generated
- Series Properties: Virus/Malware

4. Specify the display settings for the Data Field.

a. Type a meaningful label for the Data Field.

b. Specify how data displays for Data Field from the Aggregated by drop-down 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 display settings for the Category Field.

a. Type a meaningful label for the Category Field.

b. Specify how to sort data in the chart from the Sorting drop-down lists:

- **Aggregation value:** Specifies data sorts from the data appearing in the Category fields.
- **Category name:** Specifies data sorts from the alphabetical value of Category names.
- **Ascending:** Specifies data sorts in ascending order.
- **Descending:** Specifies data sorts in descending order.

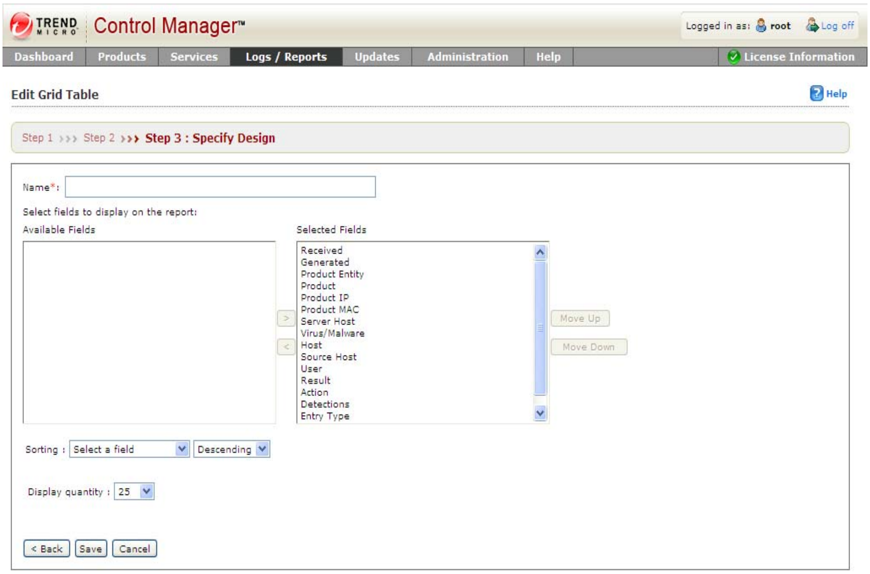
c. Specify how many items display in the Categories Field by selecting **Filter summarized result** and specifying a value in the **Display top** text box. Default value is 10.

d. Select **Aggregate remaining items** to put all remaining items into the group "Other" on the graph.

6. Specify the display settings for the Series Field:
   - a. Type a meaningful label for the Series Field.
7. Click **Save**. The Add Report Template screen appears.

Configure grid table settings:

1. Click **Next**. The Add Grid Table > Step 3 Specify Design screen appears.



Edit Grid Table

Name*:

Select fields to display on the report:

Available Fields

Selected Fields

Received
Generated
Product Entity
Product
Product IP
Product MAC
Server Host
Virus/Malware
Host
Source Host
User
Result
Action
Detections
Entry Type

Sorting : Select a field | Descending

Display quantity : 25

   - a. Type a name for the table in the **Name** field.
   - b. Specify which columns appear in the table and in which order the columns appear.
   - c. Specify how the columns sort.
   - d. Specify the number of items that appear in the table.
   - e. Click **Save**. The Add Report Template screen appears.

Step 6: Complete report template creation:

1. Add or remove Report Template Elements as you require.
2. Click **Save**.

Adding One-time Reports

Control Manager supports generating one-time reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a one-time report is similar for all report types and involves the following:

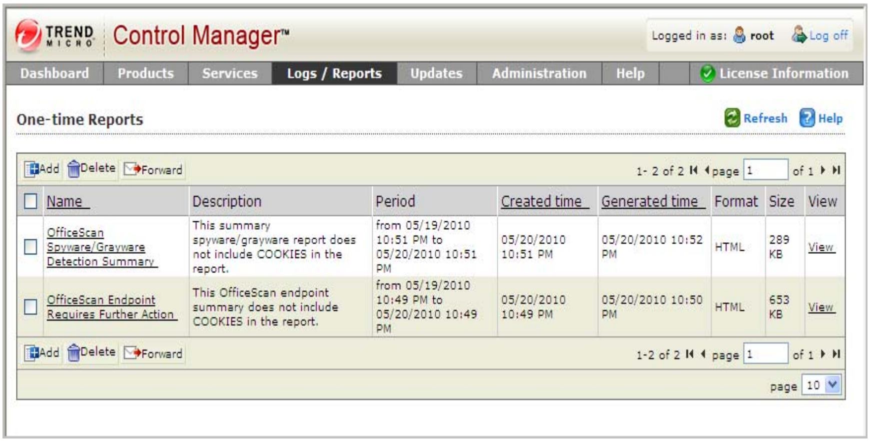
1. Access the Add One-time Report screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

To add a one-time report:

Step 1: Access the Add One-time Report screen and select the report type:

Path: Logs/Reports > One-time Report

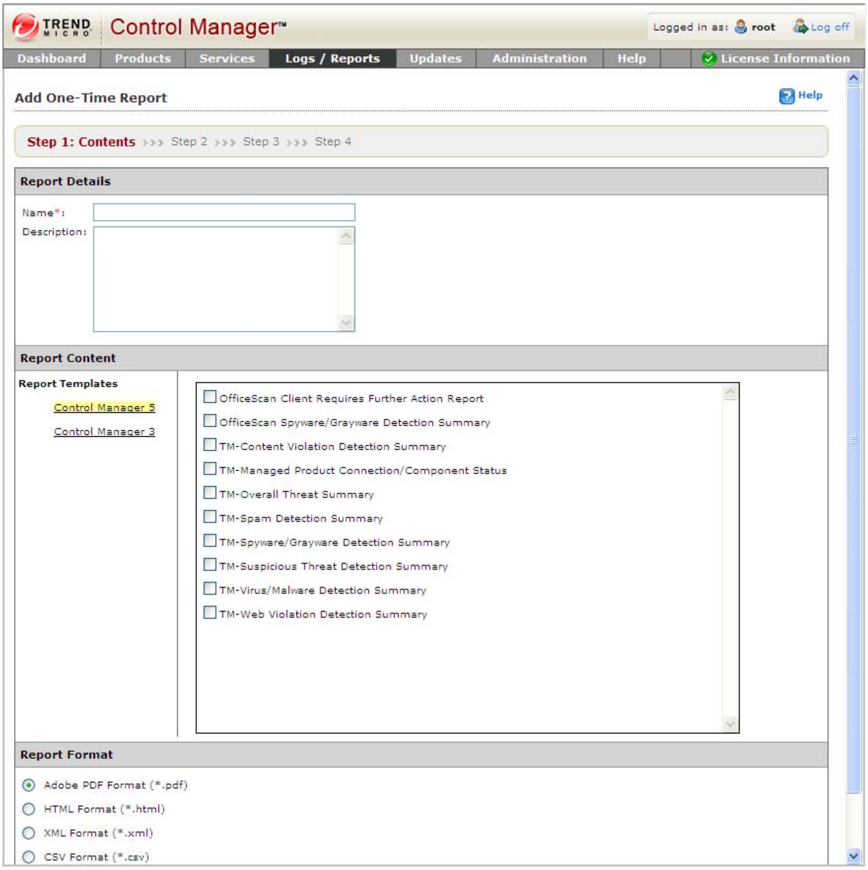
1. Navigate to the One-time Report screen.



One-time Reports

□	Name	Description	Period	Created time	Generated time	Format	Size	View
□	OfficeScan Spyware/Grayware Detection Summary	This summary spyware/grayware report does not include COOKIES in the report.	from 05/19/2010 10:51 PM to 05/20/2010 10:51 PM	05/20/2010 10:51 PM	05/20/2010 10:52 PM	HTML	289 KB	View
□	OfficeScan Endpoint Requires Further Action	This OfficeScan endpoint summary does not include COOKIES in the report.	from 05/19/2010 10:49 PM to 05/20/2010 10:49 PM	05/20/2010 10:49 PM	05/20/2010 10:50 PM	HTML	653 KB	View

2. Click **Add**. The Add One-time Report Profile > Step 1: Contents screen appears.



Add One-Time Report

Step 1: Contents >>> Step 2 >>> Step 3 >>> Step 4

Report Details

Name*:

Description:

Report Content

Report Templates

Control Manager 5

Control Manager 3

□ OfficeScan Client Requires Further Action Report
□ OfficeScan Spyware/Grayware Detection Summary
□ TM-Content Violation Detection Summary
□ TM-Managed Product Connection/Component Status
□ TM-Overall Threat Summary
□ TM-Spam Detection Summary
□ TM-Spyware/Grayware Detection Summary
□ TM-Suspicious Threat Detection Summary
□ TM-Virus/Malware Detection Summary
□ TM-Web Violation Detection Summary

Report Format

● Adobe PDF Format (*.pdf)
○ HTML Format (*.html)
○ XML Format (*.xml)
○ CSV Format (*.csv)

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:

   Control Manager 5 report template:

   a. Select the Control Manager 5 template to generate the report.

If the existing reports do not fulfill your requirements, create one from the Report Templates screen. See Adding Control Manager 5 Report Templates on page 10-15 for more information.

Control Manager 3 report template:

a. Click **Control Manager 3** under Report Content. The Control Manager 3 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 Control Manager 3 template data on which to base the template.

6. Select the report generation format:

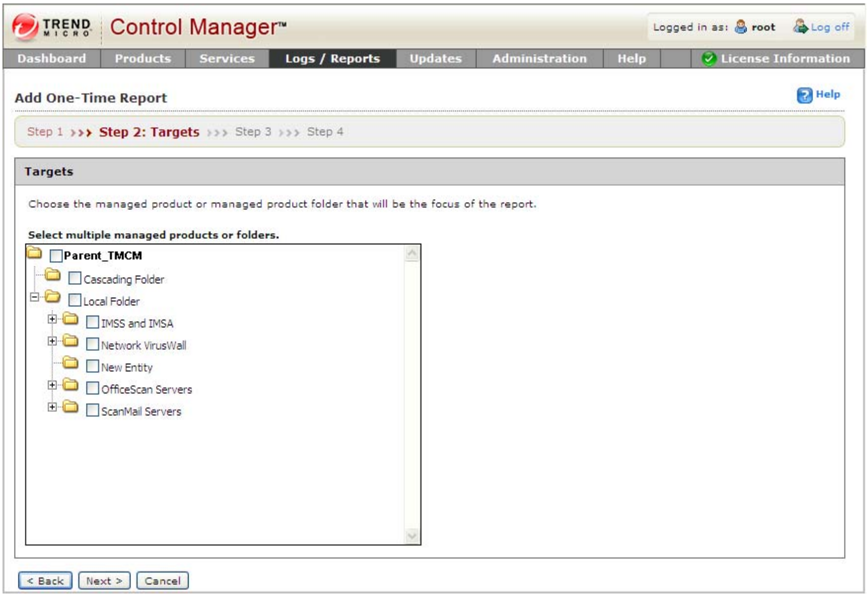
Control Manager 5 report formats:

- Adobe PDF Format (*.pdf)
- HTML Format (*.html)
- XML Format (*.xml)
- CSV Format (*.csv)

Control Manager 3 report formats:

- Rich Text Format (*.rtf)
- Adobe PDF Format (*.pdf)
- ActiveX
- Crystal Report Format (*.rpt)

7. Click **Next**. The Add One-Time Report Profile > Step 2: Targets screen appears.



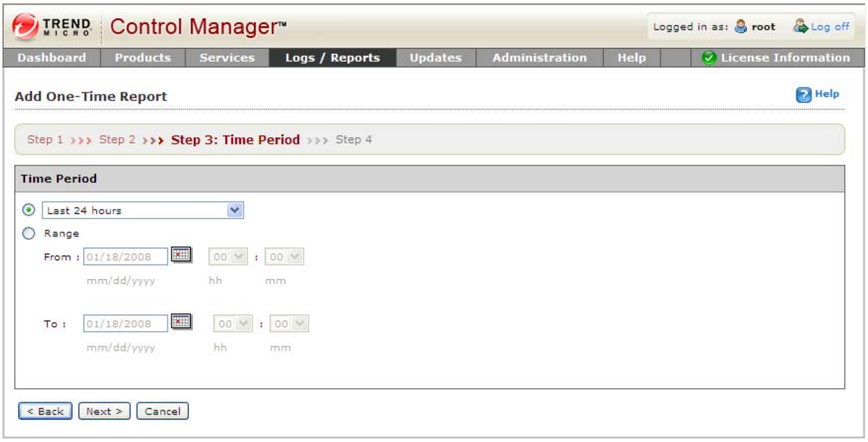
Choose the managed product or managed product folder that will be the focus of the report.

Select multiple managed products or folders.

Step 2: Specify the product/products from which the report data generates:

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 Profile > Step 3: Time Period screen appears.



Step 3: Specify the date that the product/products produced the data:

1. Specify the data generation date:

   From the drop down list select one of the following:

   - All dates
   - Last 24 hours
   - Today
   - Last 7 days
   - Last 14 days
   - Last 30 days

   Specify a date range:

   a. Type a date in the **From** field.

   b. Specify a time in the accompanying **hh** and **mm** fields.

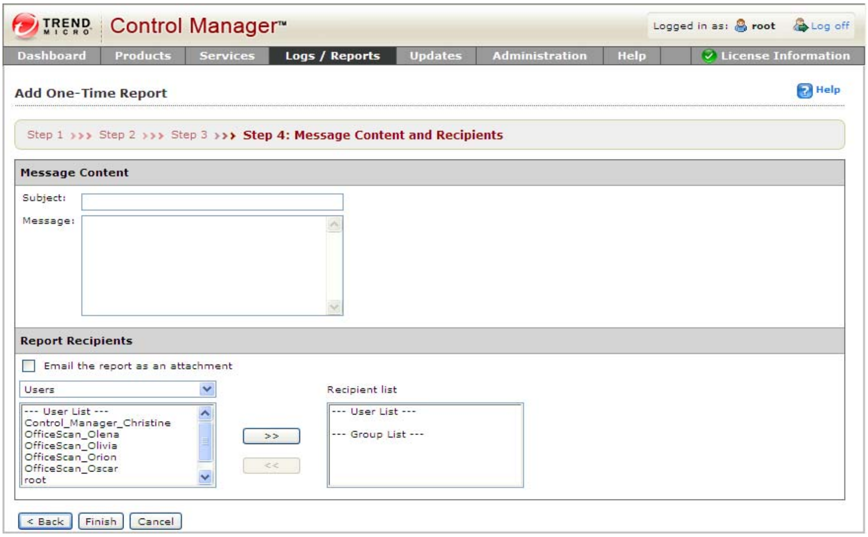
   c. Type a date in the **To** field.

   d. Specify a time in the accompanying **hh** and **mm** fields.

Tip: 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 Profile > Step 4: Message Content and Recipients screen appears.



Add One-Time Report

Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Message Content and Recipients**

Message Content

Subject:

Message:

Report Recipients

□ Email the report as an attachment

Users

--- User List ---
Control_Manager_Christine
OfficeScan_Olena
OfficeScan_Olivia
OfficeScan_Orion
OfficeScan_Oscar
root

Recipient list

--- User List ---

--- Group List ---

Step 4: Specify the recipient of the report:

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.

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a scheduled report is similar for all report types:

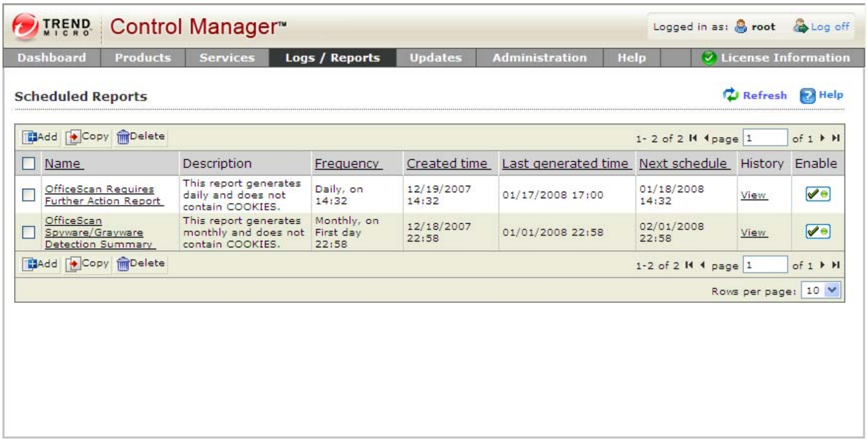
1. Access the Add Scheduled Report screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

To add a scheduled report:

Step 1: Access the Add Scheduled Report screen and select the report type:

Path: Logs/Reports > Scheduled Reports

1. Navigate to the Scheduled Reports screen.



Scheduled Reports

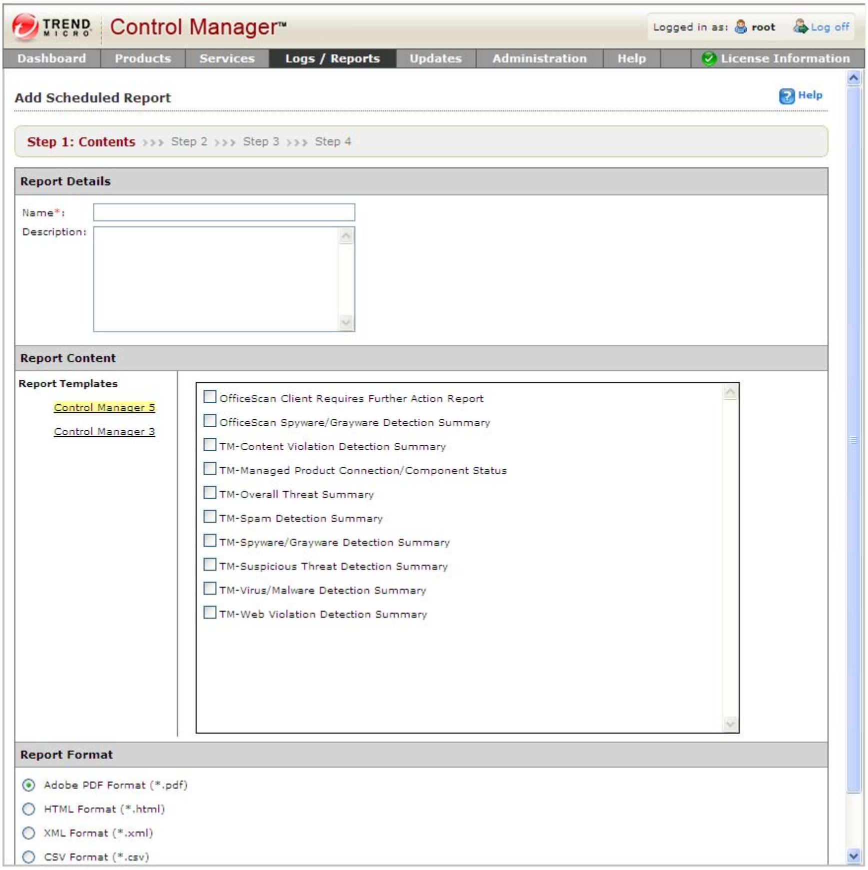
1- 2 of 2 page 1 of 1

□	Name	Description	Frequency	Created time	Last generated time	Next schedule	History	Enable
□	OfficeScan Requires Further Action Report	This report generates daily and does not contain COOKIES.	Daily, on 14:32	12/19/2007 14:32	01/17/2008 17:00	01/18/2008 14:32	View	✓
□	OfficeScan Spyware/Grayware Detection Summary	This report generates monthly and does not contain COOKIES.	Monthly, on First day 22:58	12/18/2007 22:58	01/01/2008 22:58	02/01/2008 22:58	View	✓

1-2 of 2 page 1 of 1

Rows per page: 10

2. Click **Add**. The Add Scheduled Report Profile > Step 1: Contents screen appears.



Add Scheduled Report

Step 1: Contents >>> Step 2 >>> Step 3 >>> Step 4

Report Details

Name*:

Description:

Report Content

Report Templates

Control Manager 5

Control Manager 3

□ OfficeScan Client Requires Further Action Report
□ OfficeScan Spyware/Grayware Detection Summary
□ TM-Content Violation Detection Summary
□ TM-Managed Product Connection/Component Status
□ TM-Overall Threat Summary
□ TM-Spam Detection Summary
□ TM-Spyware/Grayware Detection Summary
□ TM-Suspicious Threat Detection Summary
□ TM-Virus/Malware Detection Summary
□ TM-Web Violation Detection Summary

Report Format

● Adobe PDF Format (*.pdf)
○ HTML Format (*.html)
○ XML Format (*.xml)
○ CSV Format (*.csv)

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:

   Control Manager 5 report template:

   a. Select the Control Manager 5 template to generate the report.

If the existing reports do not fulfill your requirements, create one from the Report Templates screen. See Adding Control Manager 5 Report Templates on page 10-15 for more information.

Control Manager 3 report template:

a. Click **Control Manager 3** under Report Content. The Control Manager 3 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 Control Manager 3 template data on which to base the template.

6. Select the report generation format:

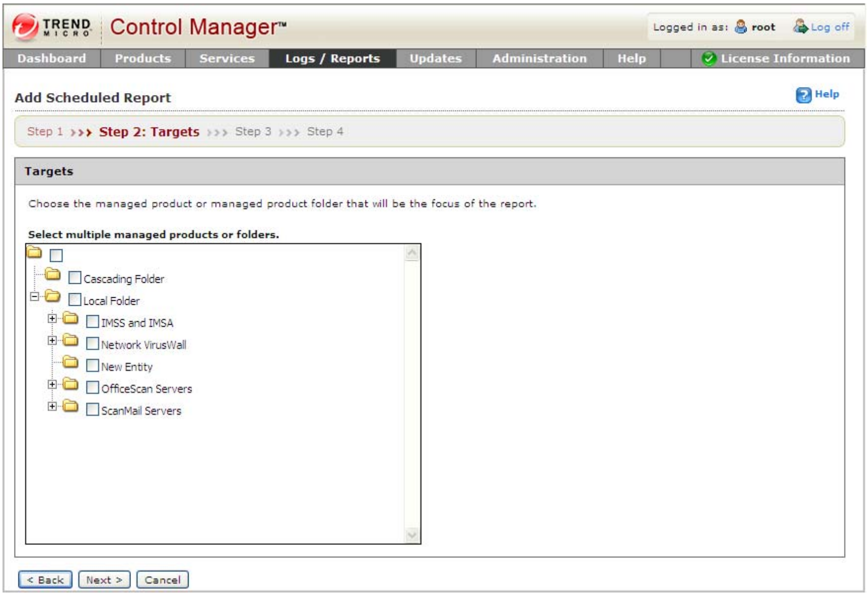
Control Manager 5 report formats:

- Adobe PDF Format (*.pdf)
- HTML Format (*.html)
- XML Format (*.xml)
- CSV Format (*.csv)

Control Manager 3 report formats:

- Rich Text Format (*.rtf)
- Adobe PDF Format (*.pdf)
- ActiveX
- Crystal Report Format (*.rpt)

7. Click **Next**. The Add Scheduled Report Profile > Step 2: Targets screen appears.



Add Scheduled Report

Step 1 ››› Step 2: Targets ››› Step 3 ››› Step 4

Targets

Choose the managed product or managed product folder that will be the focus of the report.

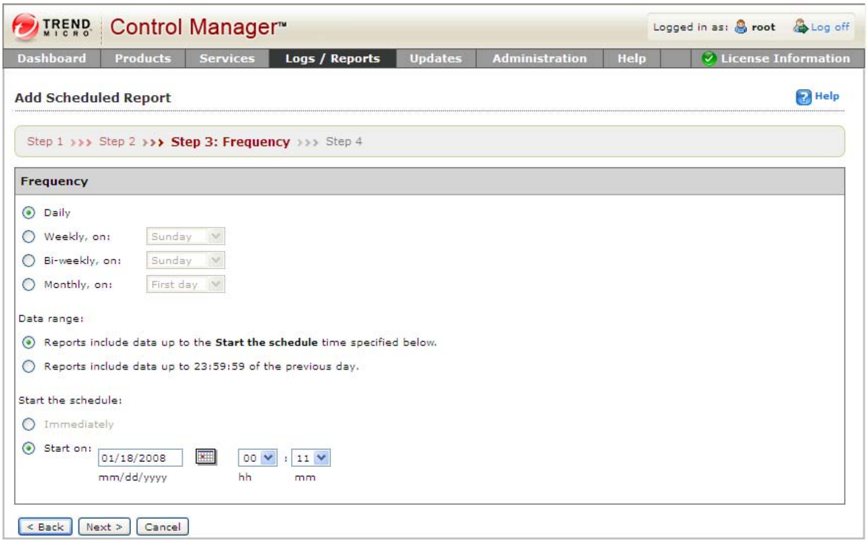
Select multiple managed products or folders.

- □
  - □ Cascading Folder
  - □ Local Folder
    - □ IMSS and IMSA
    - □ Network VirusWall
    - □ New Entity
    - □ OfficeScan Servers
    - □ ScanMail Servers

Step 2: Specify the product/products from which the report data generates:

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 Profile > Step 3: Frequency screen appears.



Add Scheduled Report

Step 1 >>> Step 2 >>> **Step 3: Frequency** >>> Step 4

Frequency

● Daily

○ Weekly, on: Sunday

○ Bi-weekly, on: Sunday

○ Monthly, on: First day

Data range:

● Reports include data up to the **Start the schedule** time specified below.

○ Reports include data up to 23:59:59 of the previous day.

Start the schedule:

○ Immediately

● Start on: 01/18/2008 (mm/dd/yyyy) 00 (hh) : 11 (mm)

Step 3: Specify the date that the product/products produced the data:

1. Specify how often reports generate:
   - **Daily:** Reports generate daily.
   - **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 day of the month, the 15th of the month, 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.

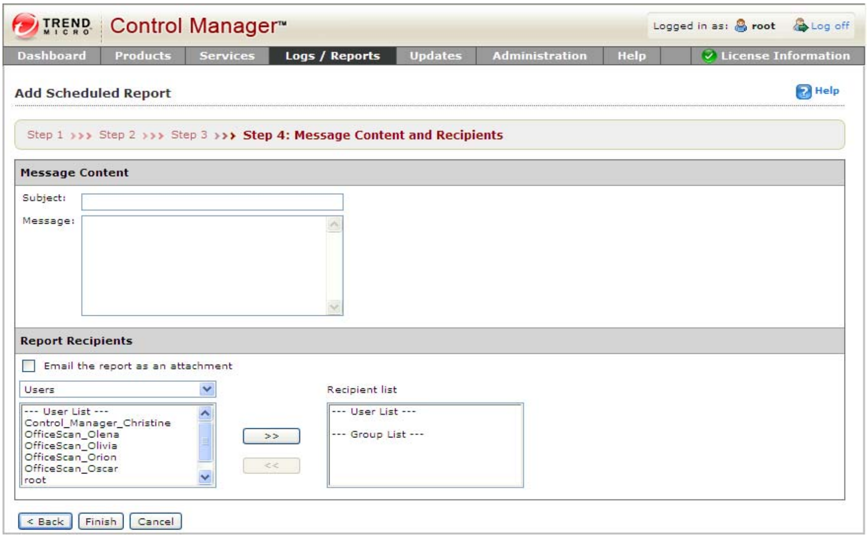
3. Specify when the report schedule starts:
   - **Immediately:** The report schedule starts immediately after enabling the report.
   - **Start on:** The report schedule starts on the date and time specified in the accompanying fields.

   a. Type a date in the **mm/dd/yyyy** field.

   b. Specify a time in the accompanying **hh** and **mm** fields.

Tip: 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 Profile > Step 4: Message Content and Recipients screen appears.



Step 4: Specify the recipient of the report

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.

To enable/disable scheduled reports:

Path: Logs/Reports > Scheduled Reports

1. Navigate to the Scheduled Reports screen.
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

To view reports:

1. Move the cursor over **Logs/Reports** from the main menu. A drop down menu appears.
2. Select one of the following from the drop down menu:

   One-time Reports:

a. Click One-time Reports from the drop-down menu. The One-time Reports screen appears.

b. Click the link for the report you want to view from the View column.

Scheduled Reports:

a. Click **Scheduled Reports** from the drop-down menu. The Scheduled Reports screen appears.

b. Click the link for the report you want to view from the **History** column. The History screen for that report appears.

c. Select the report to view from the History screen.

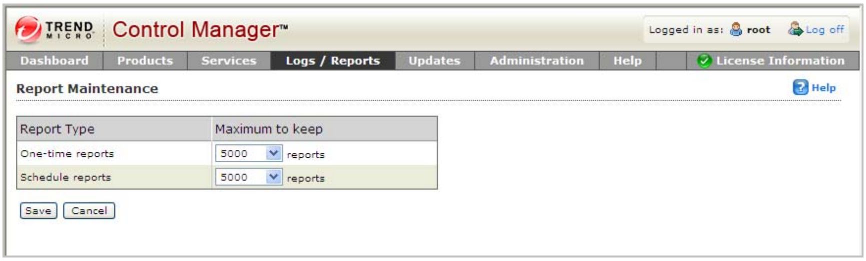
Configuring Report Maintenance

Configure Report Maintenance settings to delete reports.

To configure report maintenance:

Path: Logs/Reports > Settings > Report Maintenance

1. Navigate to the Report Maintenance screen.



Report Type	Maximum to keep
One-time reports	5000 reports
Schedule reports	5000 reports

2. Specify the maximum number of one-time and scheduled reports to keep.

3. Click **Save**.

Section 3

Administering Control Manager

Chapter 11

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 5.5/5.0/3.5 use 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 11-1. Agent Comparison

FEATURE	MCP AGENTS	CONTROL MANAGER 2.X AGENTS
Outbreak Prevention Services (OPS)	Yes	Yes
Single Sign-on (SSO)	Yes	No
One-way/two-way communication	Yes	No
NAT support	Yes	No
Cluster node support	Yes	No
Agent polls Control Manager for updates and commands	Yes	No
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	No	Yes

TABLE 11-1. Agent Comparison

FEATURE	MCP AGENTS	CONTROL MANAGER 2.X AGENTS
Work and idle state support	Yes	Yes
Agent/Communicator heartbeat	Yes	Yes
Notification: Virus pattern expired	Yes	Yes
Notification: Agent unable to update components	Yes	Yes
Notification: Agent unable to deploy components	Yes	Yes
Notification: Product service stopped	Yes	Yes

Each managed product has its own agent responsible for the following:

TABLE 11-2. MCP / 2.x Agent Comparison

MCP AGENTS	2.X AGENTS
Polling commands for the managed product from 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, Communicators, and child server use the following connection status icons:

TABLE 11-3. Status Icons for Managed Products

CONNECTION STATUS DESCRIPTION	MANAGED PRODUCT	
Product service is running	✅	
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 11-4. Status Icons for Communicators

CONNECTION STATUS DESCRIPTION	COMMUNICATORS
TMI service is running	✅

TABLE 11-4. Status Icons for Communicators

CONNECTION STATUS DESCRIPTION	COMMUNICATORS	
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 11-5. Status Icons for Child Servers

CONNECTION STATUS DESCRIPTION	CHILD	
TMI service is not running	Status is not changed	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 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:

TABLE 11-6. Security Level Behavior for MCP

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 11-7. 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 Scheduler

The Agent Communication Schedule determines the periods when the agent sends information to 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, the 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.

Tip: Use the Agent Communication Scheduler 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:** within the working hour
- **Inactive:** idle hour or not within the Working hour
- **Abnormal:** disconnected

Refer to Understanding Connection Status Icons on page 11-5 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 in the Agent/Communicator Scheduler 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:

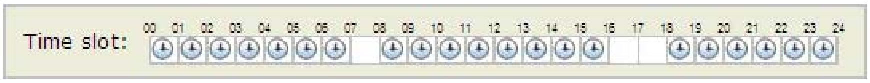


FIGURE 11-1. Schedule Bar

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 11-8. 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 on 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

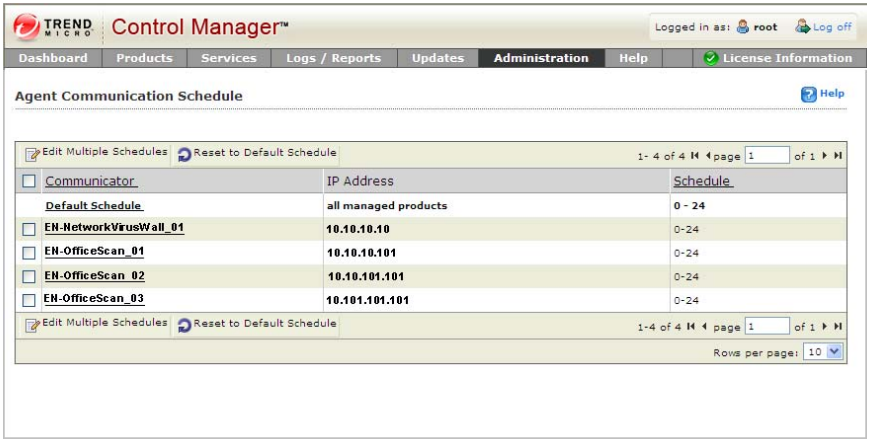
You can define up to three sets of schedules that specify when the managed product interacts with the Control Manager server.

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.

To set an agent communication schedule for a managed product:

Path: Administration > Settings > Agent Communication Schedule

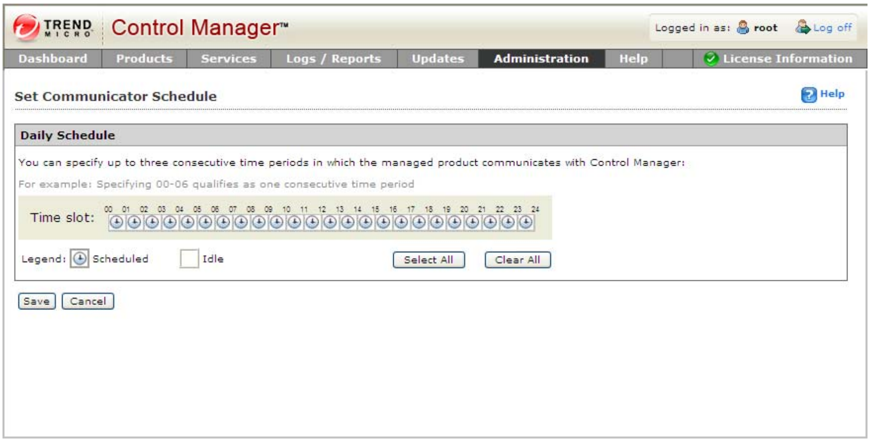
1. Navigate to the Agent Communication Screen.



Agent Communication Schedule

☐	Communicator	IP Address	Schedule
	Default Schedule	all managed products	0 - 24
☐	EN-NetworkVirusWall_01	10.10.10.10	0-24
☐	EN-OfficeScan_01	10.10.10.101	0-24
☐	EN-OfficeScan_02	10.10.101.101	0-24
☐	EN-OfficeScan_03	10.101.101.101	0-24

2. Select the managed product schedule to modify. The Set Communicator Schedule screen appears.



Set Communicator Schedule

Daily Schedule

You can specify up to three consecutive time periods in which the managed product communicates with Control Manager:

For example: Specifying 00-06 qualifies as one consecutive time period

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, select the setting to apply and click **Reset to Default Schedule**

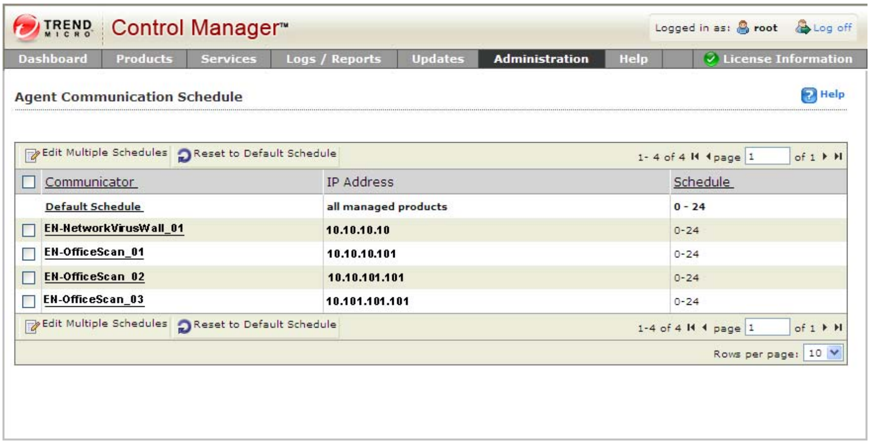
Modifying the Default Agent/Communicator Schedule

Use the Default Agent/Communicator schedule to automatically set the agent/communicator schedule.

To modify a managed product Communicator schedule:

Path: Administration > Settings > Agent Communication Schedule

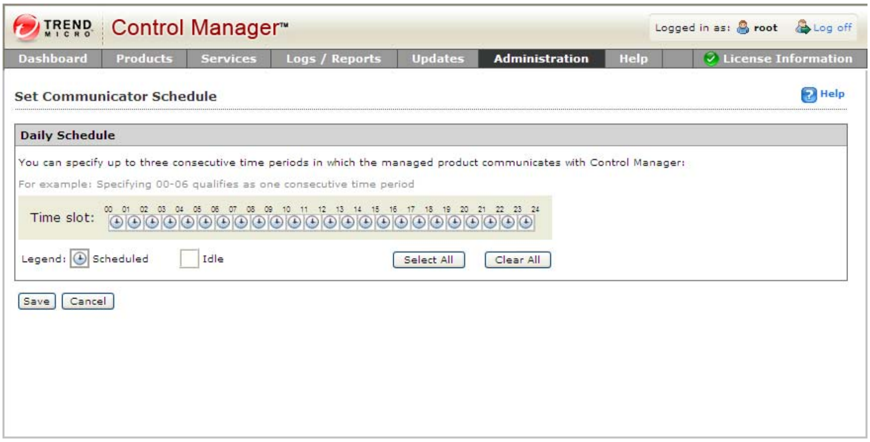
1. Navigate to the Agent Communication screen.



Agent Communication Schedule

	Communicator	IP Address	Schedule
	Default Schedule	all managed products	0 - 24
□	EN-NetworkVirusWall_01	10.10.10.10	0-24
□	EN-OfficeScan_01	10.10.10.101	0-24
□	EN-OfficeScan_02	10.10.101.101	0-24
□	EN-OfficeScan_03	10.101.101.101	0-24

2. On the working area, click **Default Schedule**.



Set Communicator Schedule

Daily Schedule

You can specify up to three consecutive time periods in which the managed product communicates with Control Manager:

For example: Specifying 00-06 qualifies as one consecutive time period

Time slot:

Legend: Scheduled Idle

3. On the **Daily Schedule**, change the appropriate time slots.

4. Click **Save**.

Configuring the Agent/Communicator Heartbeat

Use the Heartbeat Setting screen to define the frequency and maximum delay times (in minutes) for Control Manager server and agent 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:

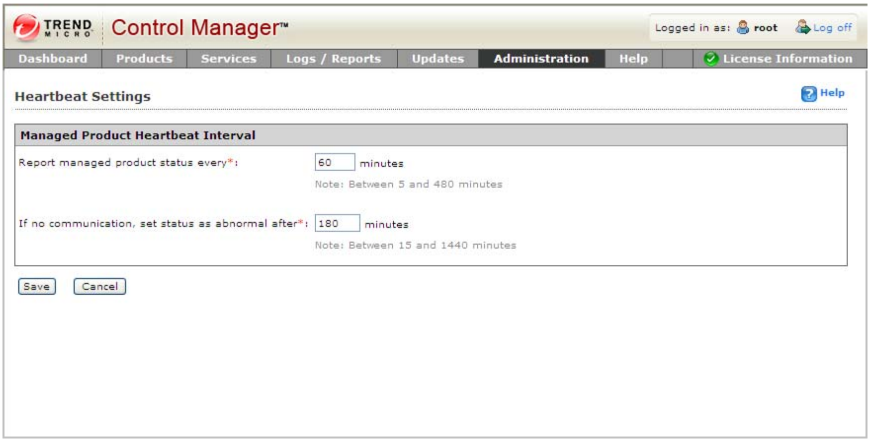
Frequency: 3 minutes

Maximum delay: 5 minutes

To set the heartbeat Frequency and Maximum delay times:

Path: Administration > Settings > Heartbeat Settings

1. Navigate to the Heartbeat Settings screen.



Heartbeat Settings

Managed Product Heartbeat Interval

Report managed product status every*: 60 minutes

Note: Between 5 and 480 minutes

If no communication, set status as abnormal after*: 180 minutes

Note: Between 15 and 1440 minutes

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 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 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).

To restart Control Manager services:

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).

To change the external communication port on the Control Manager server:

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.

To change the external communication port on the managed product server:

1. Open TMI.cfg using a text editor. Typically, you can find a managed product `TMI.cfg` in the `<root>:\Program Files\Trend\Common\TMI` directory.
2. Modify the `OuterPort` value to match the Control Manager server's `CCGI_Config.xml` value.
3. Modify the `HostID` value to match with the new port. For example, `HostID=12.1.123.123:2222`.
4. Stop and restart the Trend Micro Management Infrastructure service.
5. Repeat steps 1 to 5 for all managed product servers.

WARNING! **Modify all TMI.cfg in your Control Manager network (server and agents) to the OuterPort value. Otherwise, the server and agent communication will not work.**

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.

To change the Control Manager security level:

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.

To change the Communicator Heartbeat protocol to TCP:

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.

To verify Control Manager is using two-way communication:

Note: This procedure uses the default installation settings for Control Manager.

1. Click **Start > Programs > Microsoft SQL Server**. The SQL Server Enterprise Manager dialog box appears.
2. Click **Microsoft SQL Servers > SQL Server Group > (Hostname of the Control Manager server) > Databases > DB_ ControlManager > Tables**.
3. Locate **CDSM_Entity**.
4. Locate and verify the following from CDSM_Entity:
   - Locate the **Token** column. Information in the column appears in the following format: “URLTOKEN:**2**; http;10.1.2.3;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.

To verify Control Manager is using two-way communication from the web console:

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.

Chapter 12

Managing Managed Products

This chapter presents material administrators need when managing the Control Manager network.

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, SMEX or FW) 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 12-1. Product Directory Options

MENU ITEMS	DESCRIPTION
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.

TABLE 12-1. Product Directory Options (Continued)

MENU ITEMS	DESCRIPTION
Logs	Click this menu item, after selecting a managed product/directory, to query and view product logs. If you select a managed product, you can only query logs for that specific product. Otherwise, you can query all the products available in the 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	**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 in the Product Directory

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).

Group managed products according to geographical, administrative, or product-specific reasons. The following table presents the recommended grouping types as well as their advantages and disadvantages.

TABLE 12-2. 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
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 12-3. 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 divisions. For example, have two Control Manager servers that manage the production and testing groups.

TABLE 12-3. Considerations when grouping managed products or child servers

STRUCTURE	DESCRIPTION
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 structure supports group configuration.

The Product Directory provides a user-specified grouping of managed products. This grouping enables you to administer managed products using the following tasks:

- Configuring managed products
- Request products to perform Scan Now (if the managed product supports this command)
- View product information and details about the managed product's 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, antispam rule, and program updates

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

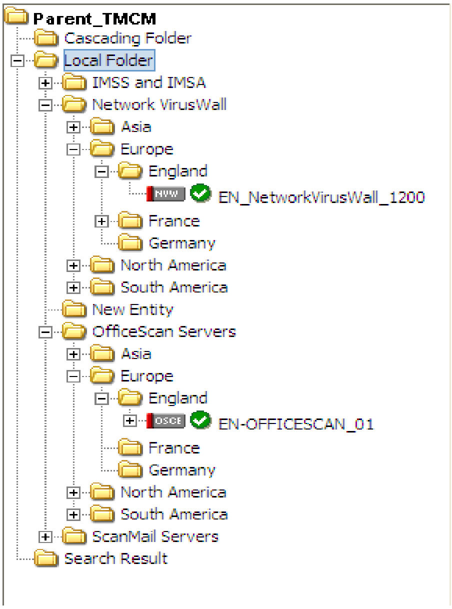
TABLE 12-4. Considerations for the structure

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.

TABLE 12-4. Considerations for the structure (Continued)

CONSIDER	EFFECT
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 to individual products. A well-structured directory therefore simplifies the designation of recipients.
Outbreak Prevention Policy (OPP) deployment	OPP deployment depend on deployment plans for efficient distribution of Outbreak Prevention Policy.

A sample Product Directory appears below:



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

Note: All newly registered managed products usually appear in the **New Entity** folder regardless of the agent type.

TABLE 12-5. Managed Product Icons

ICON	DESCRIPTION
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	ServerProtect Information Server
🖥	ServerProtect Domain

TABLE 12-5. Managed Product Icons (Continued)

ICON	DESCRIPTION
NT	ServerProtect for Windows (Normal Server)
NW	ServerProtect for NetWare (Normal Server)
IMSS	InterScan Messaging Security Suite
IWSS	InterScan Web Security Suite
ISNT	InterScan VirusWall for Windows
ISUX	InterScan VirusWall for UNIX
SMEX	ScanMail for Microsoft Exchange
SMLN	ScanMail for Lotus Notes
NVW	Network VirusWall
FW	NetScreen Global PRO Firewall
✓	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 12-6. 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	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.

To access the Product Directory:

- Click **Products** on the main menu. The Product Directory screen appears.

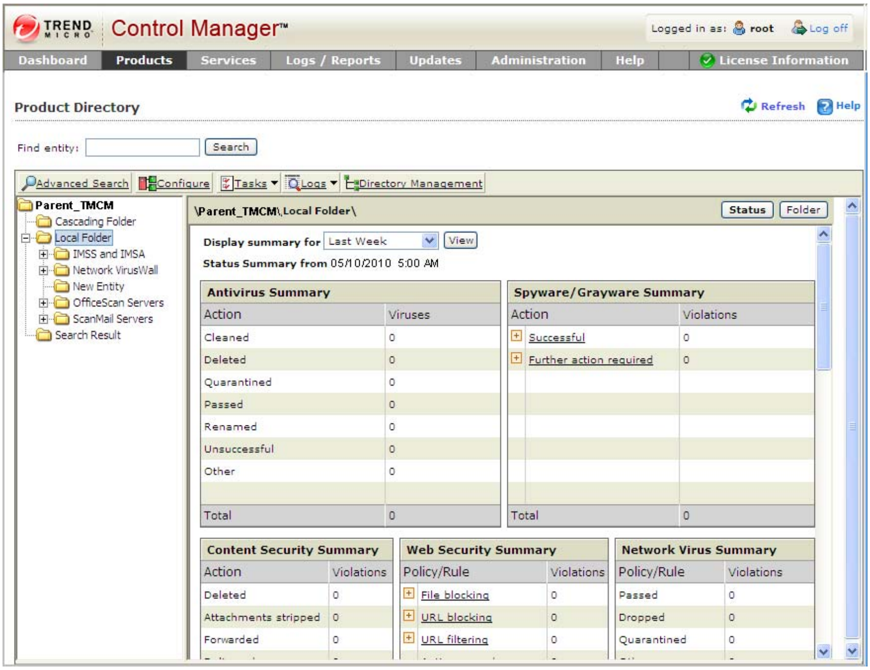
Manually Deploying Components Using the Product Directory

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.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu. The Product Directory screen appears.



Display summary for Last Week

Status Summary from 05/10/2010 5:00 AM

Antivirus Summary

Action	Viruses
Cleaned	0
Deleted	0
Quarantined	0
Passed	0
Renamed	0
Unsuccessful	0
Other	0
Total	0

Spyware/Grayware Summary

Action	Violations
Successful	0
Further action required	0
Total	0

Content Security Summary

Action	Violations
Deleted	0
Attachments stripped	0
Forwarded	0

Web Security Summary

Policy/Rule	Violations
File blocking	0
URL blocking	0
URL filtering	0

Network Virus Summary

Policy/Rule	Violations
Passed	0
Dropped	0
Quarantined	0

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 in the Command Tracking screen to view details for the Deploy Now task.

Viewing Managed Product's Status Summaries

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 **Summary** tab)
- Through the Product Directory

To access through the dashboard

- Upon opening the Control Manager web console, the **Dashboard > Summary** tab 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.

To access through the Product Directory:

1. Click **Products** on 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.

To configure a product:

1. Click **Products** on 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.

   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.

To issue tasks to managed products:

1. Click **Products** on the main menu. The Product Directory screen appears.
2. Select the managed product or directory to issue a task.
3. Mover 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.

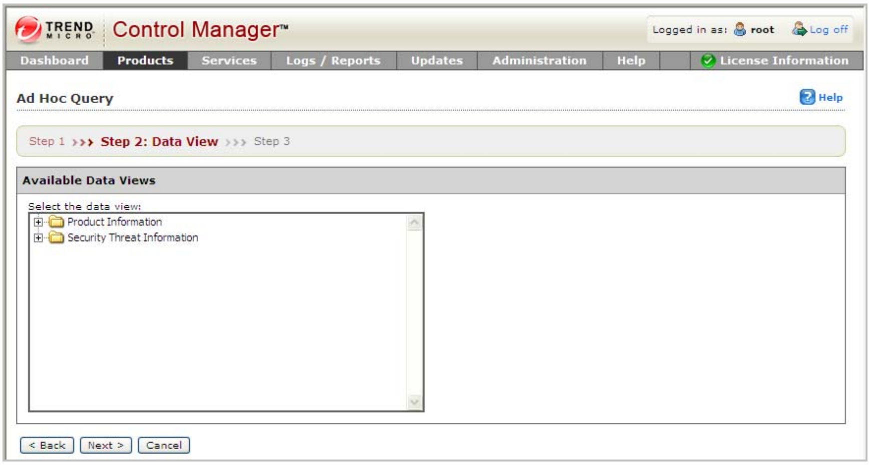
Querying and Viewing Managed Product Logs

Use the Logs tab to query and view logs for a group or a specific managed product.

To query and view managed product logs:

1. Click **Products** on 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.

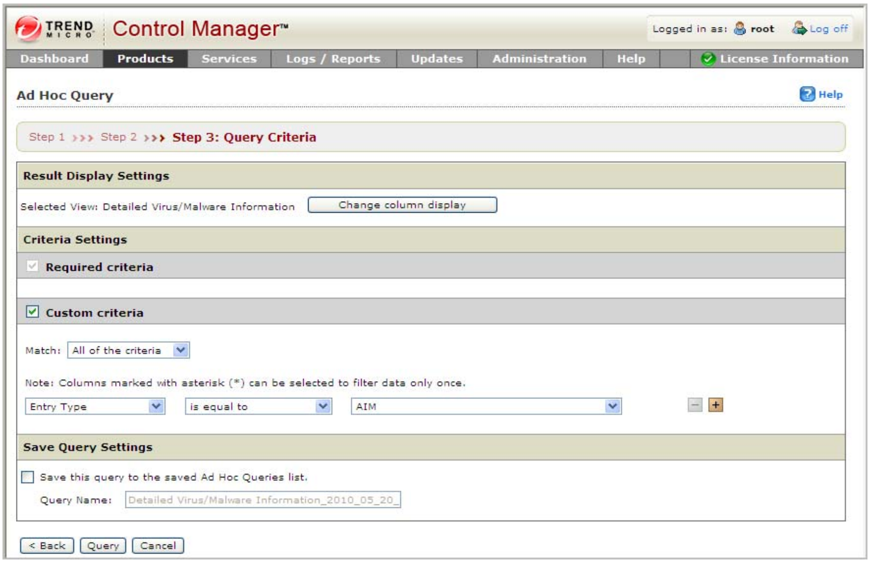
4. Click **Logs** from the drop-down menu. The Ad Hoc Query Step 2: Select Data View screen appears.



5. Specify the data view for the log:

   a. Select the data to query from the Available Data Views area.

b. Click **Next**. The Step 3: Query Criteria screen appears.



Selected View: Detailed Virus/Malware Information

Match: All of the criteria

Note: Columns marked with asterisk (*) can be selected to filter data only once.

Entry Type | is equal to | AIM

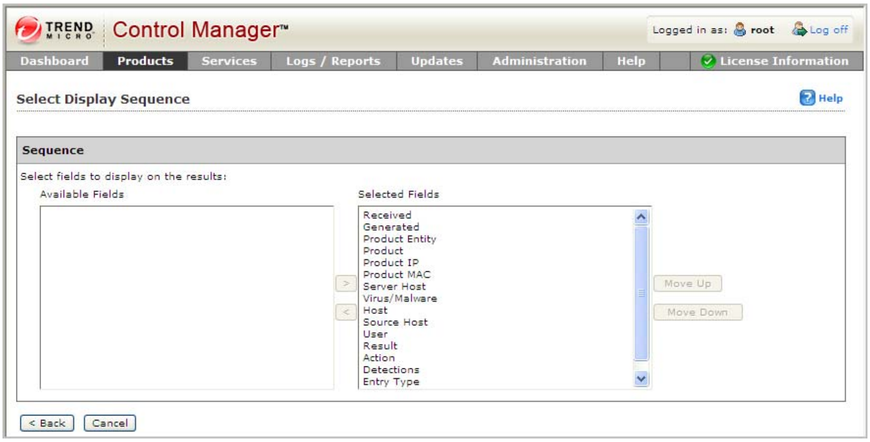
□ Save this query to the saved Ad Hoc Queries list.

Query Name: Detailed Virus/Malware Information_2010_05_20_

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.



Received
Generated
Product Entity
Product
Product IP
Product MAC
Server Host
Virus/Malware
Host
Source Host
User
Result
Action
Detections
Entry Type

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. To 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. To save the report as a CSV file:

a. Click **Export to CSV**.

b. Click **Save**.

c. Specify the location to save the file.

d. Click **Save**.

11. To save the report as an XML file:

a. Click **Export to XML**.

b. Click **Save**.

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. A single screen can display 10, 15, 30, or 50 query results per page.

12. To 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.

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 using the Directory Manager

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.

To recover managed products removed from the Product Directory:

- Restart Trend Micro Control Manager service on the managed product server. For more information, see *Stopping and Restarting Control Manager Services* on page 11-18.
- **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 12-19 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.

To change agent connection re-verification frequency:

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

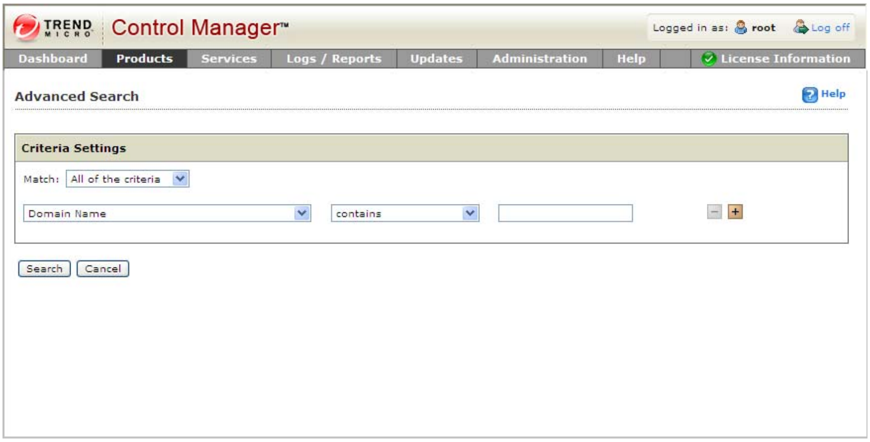
Use the Search button to quickly locate a specific managed product in the Product Directory.

To search for a folder or managed product:

1. Access the Product Directory.
2. Type the entity display name of the managed product in the Find Entity field.
3. Click **Search**.

To perform an advanced search:

1. Access the Product Directory.
2. Click **Advanced Search**. The Advanced Search screen appears.



Advanced Search

Criteria Settings

Match: All of the criteria

Domain Name | contains

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

To refresh the Product Directory:

- In the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

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 12-7. 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

Directory Manager provides several options:

- Add directories to the Product Directory
- Rename directories in the Product Directory
- Move managed products or directories in the Product Directory

Note: The keep permissions check box allows a folder to keep its source permission when moved.

- Remove managed products or directories from the Product Directory

Use these options to manipulate and organize managed products in your Control Manager network

To use the Directory Management screen:

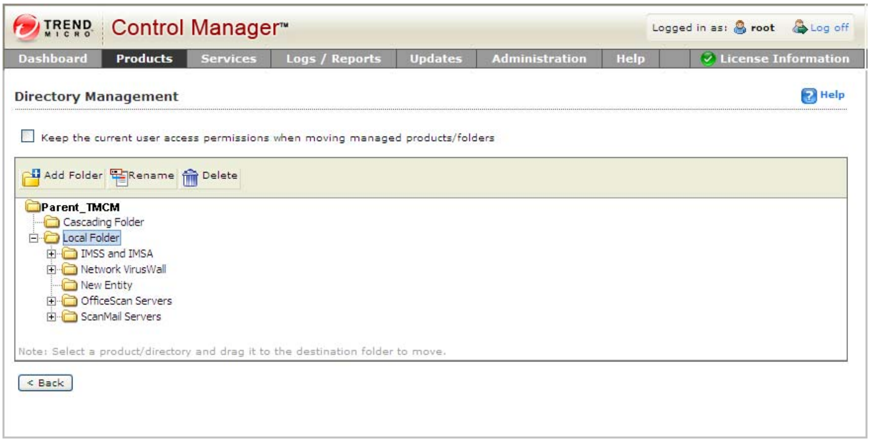
- Select a managed product or directory and click **Rename** to rename a managed product or directory
- Click + or the folder to display the managed products belonging to a folder
- Drag-and-drop managed products or directories to move the managed products or directories in the Product Directory
- Click **Add Folder** to add a directory to the Product Directory

Accessing Directory Management

Use Directory Management to group managed products together.

To access the Directory Management:

1. Click **Products** from the main menu. The Product Directory screen appears.
2. Click **Directory Management** from the Product Directory menu. The Directory Management screen appears.



□ Keep the current user access permissions when moving managed products/folders

Note: Select a product/directory and drag it to the destination folder to move.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.

To create a folder:

Path: Products | Directory Management

1. Navigate to the Directory Management screen.
2. Select **Local Folder**.
3. Click **Add Folder**. The Add Directory dialog box appears.
4. Type a name for the new directory in the **Directory name** field.
5. 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 from the Directory Manager.

To rename a folder or managed product:

Path: Products | Directory Management

1. Navigate to the Directory Management screen.
2. Select the managed product or directory to rename.
3. Click **Rename**. The Rename Directory dialog box appears.
4. Type a name for the managed product or directory in the **Directory name** field.
5. Click **Save**.
6. Click **OK**. The managed product or directory displays in the Product Directory with the new name.

Note: Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

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.

To transfer or move a folder or managed product to another location:

Path: Products | Directory Management

1. Navigate to the Directory Management screen.
2. On the working area, select the folder or managed product to move.
3. Drag-and-drop the folder or managed product to the target new location.
4. Click **Save**.

Deleting User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager. 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.

To delete a user-defined folder:

Path: Products | Directory Management

1. Navigate to the Directory Management screen.
2. Select the managed product or directory to delete.
3. Click **Delete**. A confirmation dialog box appears.
4. Click **OK**.
5. Click **Save**.

WARNING! **Take caution when deleting user-defined folders. You may accidentally delete a managed product that you do not want to remove.**

Chapter 13

Activating 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 5.5, 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 Managed Product License Management screen. Administrators can add new Activation Codes to the list and redeploy renewed Activation Codes.

Activation Code 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.

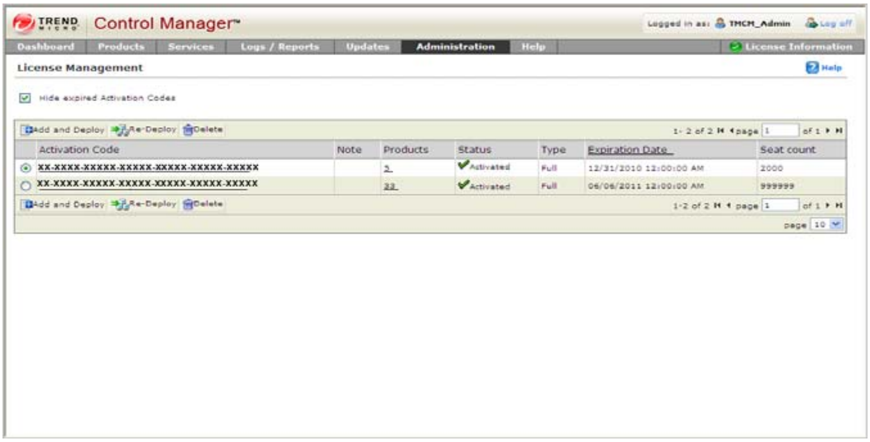
Activating Managed Products

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.

To register and activate managed products:

Path: Administration > License Management > Managed Products

1. Navigate to the **License Management** screen.

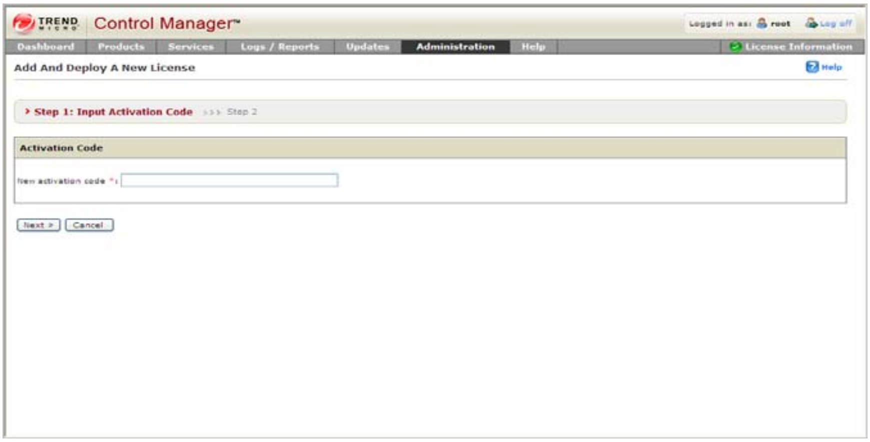


License Management

☑ Hide expired Activation Codes

	Activation Code	Note	Products	Status	Type	Expiration Date	Seat count
●	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX		5	✓Activated	Full	12/31/2010 12:00:00 AM	2000
○	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX		33	✓Activated	Full	06/06/2011 12:00:00 AM	999999

2. Click **Add and Deploy**. The Step 1: Input Activation Code screen appears.



Add And Deploy A New License

› Step 1: Input Activation Code ››› Step 2

Activation Code

New activation code *:

3. Type an Activation Code for the product you want to activate in the New activation code field.

4. Click **Next**. The 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 Managed Products License Management screen appears, with the new Activation Code listed in the table.

Renewing Managed Product Licenses

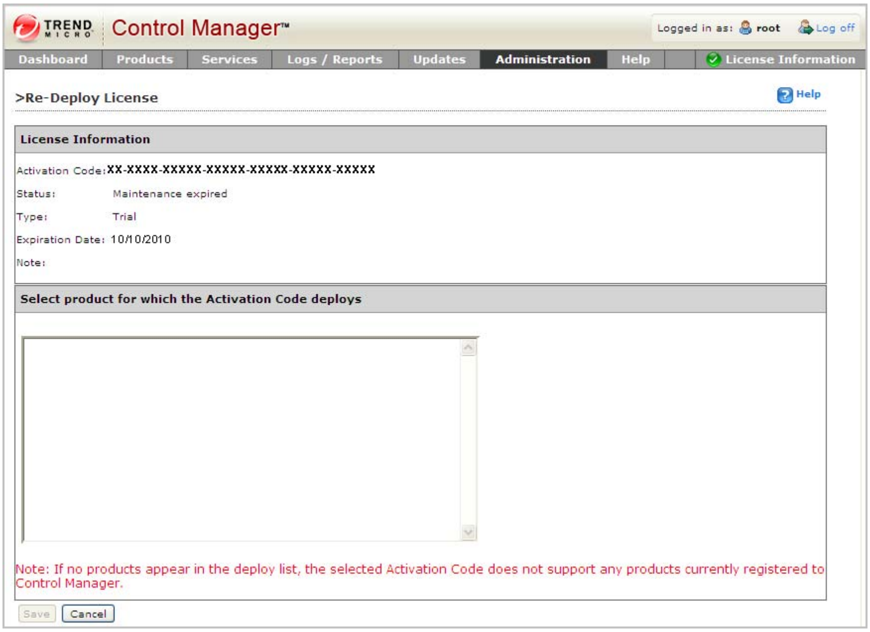
Control Manager can deploy or redeploy Activation Codes to registered products from the Product Directory or from the Managed Product License Management screen.

To renew managed product licenses from the License Management screen:

Path: Administration > License Management > Managed Products

1. Navigate to the **License Management** screen.
2. Select an Activation Code from the list.

3. Click **Re-Deploy**. The Re-Deploy License screen appears.



>Re-Deploy License

License Information

Activation Code: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Status: Maintenance expired

Type: Trial

Expiration Date: 10/10/2010

Note:

Select product for which the Activation Code deploys

Note: If no products appear in the deploy list, the selected Activation Code does not support any products currently registered to Control Manager.

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.

To renew managed product licenses from the Product Directory:

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. Select a product from the Supported Products list and click the **Next >>** button to open the License Profiles screen.

6. 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.
7. 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.

Activating Control Manager

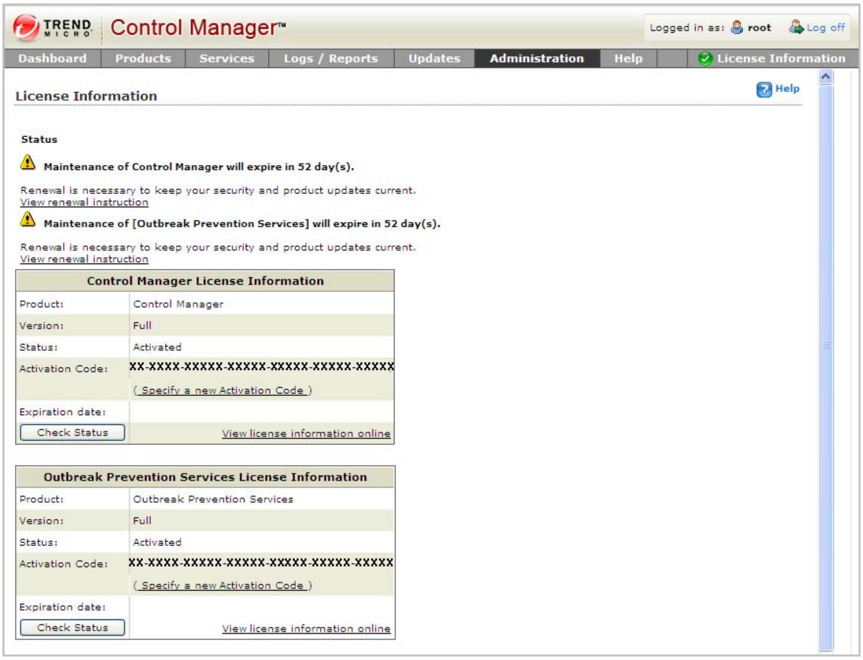
Activating Control Manager allows you to use all of the product's features, including downloading updated program components. You can activate Control Manager after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

Tip: After activating Control Manager, log off and then log on to the Control Manager web console for changes to take effect.

To register and activate Control Manager:

Path: Administration > License Management > Control Manager

1. Navigate to the **License Information** screen.



License Information

Status

⚠ **Maintenance of Control Manager will expire in 52 day(s).**

Renewal is necessary to keep your security and product updates current.
View renewal instruction

⚠ **Maintenance of [Outbreak Prevention Services] will expire in 52 day(s).**

Renewal is necessary to keep your security and product updates current.
View renewal instruction

Control Manager License Information	
Product:	Control Manager
Version:	Full
Status:	Activated
Activation Code:	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX (Specify a new Activation Code)
Expiration date:	
Check Status	View license information online

Outbreak Prevention Services License Information	
Product:	Outbreak Prevention Services
Version:	Full
Status:	Activated
Activation Code:	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX (Specify a new Activation Code)
Expiration date:	
Check Status	View license information online

2. On the working area under **Control Manager License Information**, click the **Activate the product** link.
3. Click the **Register online** link and follow the instructions on the Online Registration website.
4. In the **New box**, type your Activation Code.
5. Click **Activate**.
6. 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.

To renew maintenance using Check Status Online:

Path: Administration > License Management > Control Manager

1. Navigate to the **License Information** screen.
2. On the working area under the product or service to renew, click **Check Status**.
3. Click **OK**.

Note: Log off and then log on to the web console for changes to take effect.

To renew maintenance by manually entering an updated Activation Code:

Path: Administration > License Management > Control Manager

1. Navigate to the **License Information** screen.
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**.

Note: Log off and then log on to the web console for changes to take effect.

Chapter 14

Managing Child Servers

This chapter presents material administrators will need when managing the Control Manager network.

This chapter contains the following topics:

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.

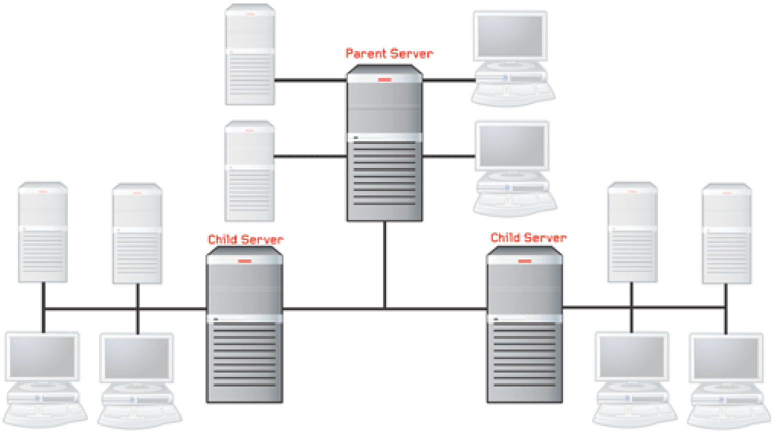


FIGURE 14-1. The cascading management structure uses two-tier parent-child architecture

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 5.5 Advanced supports the following as child Control Manager servers:

- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition

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

Aside from its own managed products, a parent server indirectly manages a large number of managed products handled directly by child servers.

The following table lists the differences between parent and child servers.

TABLE 14-1. 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).

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 14-2. Parent and child server relationship

ACTION	✓ PARENT ✓ CHILD	✓ PARENT 🚧 CHILD	✗ PARENT ✓ CHILD	✗ PARENT 🚧 CHILD	STAND-ALONE SERVER
Direct unregistration	●				
Registration					●
Uninstall Control Manager (save Database)	●	●	●	●	●
Uninstall Control Manager (delete 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 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 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 three 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 Control Manager Parent Settings screen to register or unregister from a Control Manager parent server.

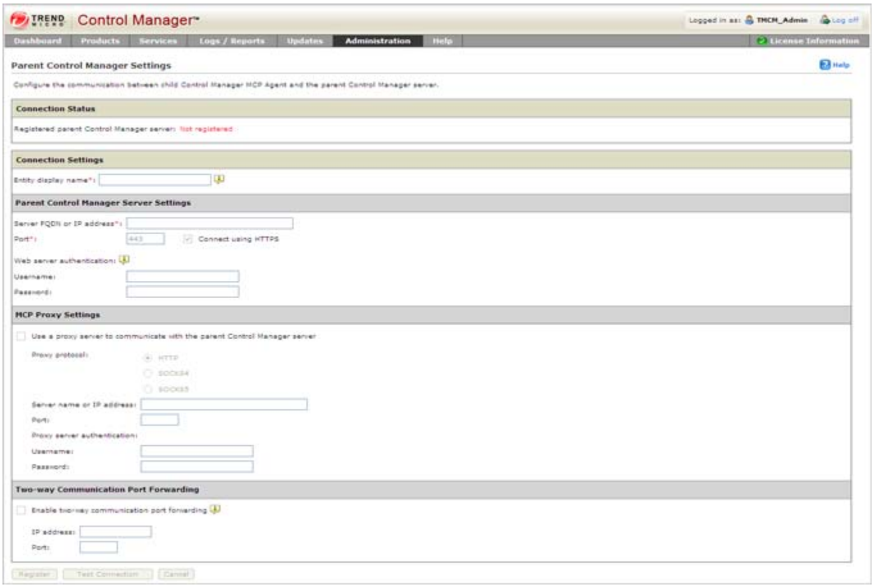
Registering a Child Server

Use the Control Manager Parent Settings screen to register or unregister from a parent Control Manager server.

To register a child server:

Path: Administration > Settings > Parent Control Manager Settings

1. Navigate to the Parent Control Manager Settings screen.



Parent Control Manager Settings

Configure the communication between child Control Manager MCP Agent and the parent Control Manager server.

Connection Status

Registered parent Control Manager server: Not registered

Connection Settings

Entity display name*:

Parent Control Manager Server Settings

Server FQDN or IP address*:

Port*: 443 ☑ Connect using HTTPS

Web server authentication:

Username:

Password:

MCP Proxy Settings

☐ Use a proxy server to communicate with the parent Control Manager server

Proxy protocol: ● HTTP ○ SOCKS4 ○ SOCKS5

Server name or IP address:

Port:

Proxy server authentication:

Username:

Password:

Two-way Communication Port Forwarding

☐ Enable two-way communication port forwarding

IP address:

Port:

2. Configure Connection Settings:
   - Type the name the child server displays in the parent Control Manager in the **Entity display name** field. By default, the entity display name is the server computer's DNS name.
3. Configure 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.

Tip: 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.

Tip: If you change any of the settings in 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.

To check the status on the Control Manager web console:

1. Click **Products** on 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.

Note: Control Manger 3.5 servers require `castool.exe` to unregister from Control Manager 5.5 servers.

To unregister a child Control Manager server:

Path: Administration > Settings > Parent Control Manager Settings

1. Navigate to the Parent Control Manager Settings screen.
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.

To access the Cascading Folder:

1. Click **Products** on 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.

To view the child server status summaries:

Path: Products

1. Navigate to the Product Directory screen.
2. Select a child server.

   All child servers send status summaries to the parent server. The timing is based on the time interval setting in `SystemConfiguration.xml` file.

   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.

To configure log upload setting:

Path: Products

1. Navigate to the Product Directory screen.
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 scheduled.
   - Select **Upload logs as soon as they are available** 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.

   - Select **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**.

Tip: 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.

To enable or disable child server connection:

Path: Products

1. Navigate to the Product Directory screen.
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**.

Note: A disabled child server does not send logs to the parent server.

However, a disabled child server does queue logs on its local server (that is, on the disabled child server itself).

Issuing Tasks to Child Servers

Use the Task menu item to perform any of the following actions to specific or all child servers.

- Deploy Pattern Files/Cleanup Templates and Antispam Rules
- Deploy engines
- Deploy program files
- Open the child server’s web console

To issue a task:

Path: Products

1. Navigate to the Product Directory screen.
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. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

   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 Control Manager 3 report templates.

To view reports generated using Control Manager 5 report templates, using single sign-on, log on to the child Control Manager's web console.

To view child server reports:

Path: Products

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 in 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 Report**. A new browser window opens that displays the reports content.

Refreshing the Product Directory

To refresh the Product Directory:

- While at the Product Directory, click the **Refresh** icon on the upper right corner of the Product Directory screen.

Renaming a Child Server

Use the rename option to change a child server’s entity display name.

To change a child server:

Path: Products > Directory Management

1. Navigate to the Directory Management screen.
2. Select the child server to rename.
3. Click **Rename**. The Rename Directory dialog box appears.
4. Type a name for the child server in the **Directory name** field.
5. Click **Save**. A confirmation dialog box appears.
6. Click **OK**. The child server displays in the Product Directory with the new name.

Recovering 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.

To recover Control Manager 3.5 child servers accidentally removed from the Directory Manager:

1. From the child server's command prompt screen, execute the force unregistration command:

   ```
   castool /e
   ```

2. Re-register the child server to the parent server.

Chapter 15

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 on page 15-2
- Backing Up db_ControlManager Using osql on page 15-7
- Backing Up db_ControlManager Using SQL Server Management Studio on page 15-10
- Shrinking db_controlmanager_log.ldf Using SQL Server Management Studio on page 15-11
- Shrinking db_ControlManager.mdf and db_ControlManager.ldf Using SQL Commands on page 15-13

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

A major contributor to database expansion is the eManager managed product. An average eManager log is about 3,000 bytes. For example:

Given a low-volume of email traffic environment (for example, 100 msg per 10-hour per day), if eManager blocks 1,250 messages each day, there would be 1,250 x 3,000 or 3,750,000 bytes per day in the Security Content Violation log.

The required database expansion in this case would be 5MB per day or 150MB per month.

All other Trend Micro products managed by Control Manager would only generate a database growth of approximately a few kilobytes per day per system.

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.

Understanding the db_ControlManager Tables

To access all tables in the Control Manager database, use a Microsoft Access project (*.adp /*.ade).

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 15-1. Directory Manager Tables

DIRECTORY MANAGER 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 15-2. 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 15-3. Managed Product Tables

MANAGED PRODUCT TABLES	DESCRIPTION
tb_EntityInfo	Stores the managed product information
tb_VirtualEntity	Stores TVCS1.x agent registration information

TABLE 15-4. Log Tables

LOG TABLES	DESCRIPTION
tb_TempLog	Stores the raw data of product logs

TABLE 15-4. Log Tables

LOG TABLES	DESCRIPTION
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 15-5. 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 15-6. Report Tables

REPORT TABLES	DESCRIPTION
• tb_ReportScheduleTask • tb_ReportTaskQueue	Stores and handles report generation tasks
tb_ReportItemTracking	Stores report template file catalog

TABLE 15-7. 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.

To generate a database backup using osql:

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.

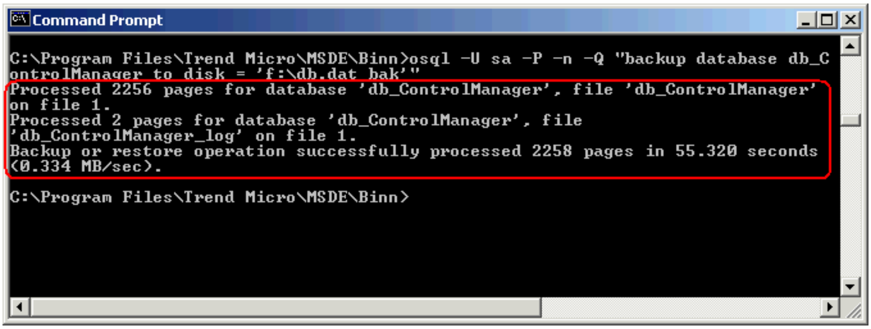
{Control Manager database}: name of the Control Manager database

{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:



```
C:\Program Files\Trend Micro\MSDE\Binn>osql -U sa -P -n -Q "backup database db_C
ontrolManager to disk = 'f:\db.dat_bak'"
Processed 2256 pages for database 'db_ControlManager', file 'db_ControlManager'
on file 1.
Processed 2 pages for database 'db_ControlManager', file
'db_ControlManager_log' on file 1.
Backup or restore operation successfully processed 2258 pages in 55.320 seconds
(0.334 MB/sec).

C:\Program Files\Trend Micro\MSDE\Binn>
```

If the backup file `db.dat_bak` already exists, the command `osql` inserts new records into the existing file to back up new information.

Tip: 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.

To restore the backup database:

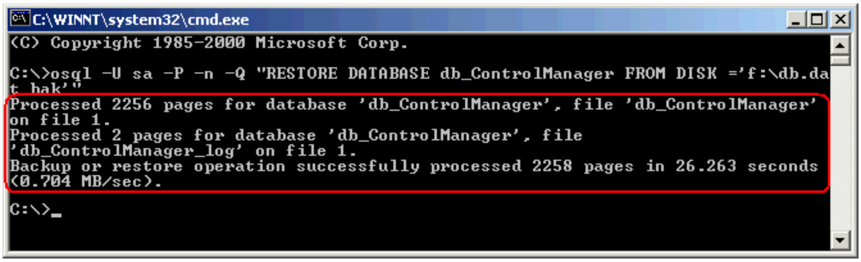
1. Stop Control Manager.
2. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
3. Right-click **<Control Manager service>**, and then click **Stop**.
4. Click **Start > Run**.
5. Type `cmd` and then click **OK**.
6. On the Command prompt, execute the following commands:

```
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:



```
(C) Copyright 1985-2000 Microsoft Corp.

C:\>osql -U sa -P -n -Q "RESTORE DATABASE db_ControlManager FROM DISK ='f:\db.da
t_bak'"
Processed 2256 pages for database 'db_ControlManager', file 'db_ControlManager'
on file 1.
Processed 2 pages for database 'db_ControlManager', file
'db_ControlManager_log' on file 1.
Backup or restore operation successfully processed 2258 pages in 26.263 seconds
(0.704 MB/sec).

C:\>_
```

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.

To back up db_ControlManager using the SQL Server Management Studio:

1. From the Control Manager server, click **Start > Programs > Microsoft SQL Server 2005 > Enterprise manager** to access the SQL Server Management Studio.
2. On the console, click **Microsoft SQL servers > SQL server group > {SQL server} (Windows NT) > Databases**. {SQL server} is the SQL Server host name.
3. Right-click **db_controlmanager** and then click **All tasks > Backup Database…**.
4. On the **SQL Server Backup - db_controlmanager**, specify the database name and description.
5. Under Backup, select **Database - complete**.
6. Under Destination, click **Add** to specify the backup file destination.
7. On **Select Backup Destination**, provide the database backup name and path where it will be saved and then click **OK**.
8. On the **SQL Server Backup - db_controlmanager**, click **OK** to start the db_ControlManager backup.
9. Click **OK** when the message "The backup operation has been completed successfully." appears.

Tip: 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).

Restoring Backup db_ControlManager Using SQL Server Management Studio

Use the SQL Server Management Studio to restore the backup Control Manager database.

To restore backup db_ControlManager:

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** and then click **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."
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 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.

To shrink the db_controlmanager_log.ldf file size on Windows Server 2008/2005 SP 3:

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.

To shrink the db_controlmanager_log.ldf file size on Windows Server 2005 :

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.

Shrinking db_ControlManager.mdf and db_ControlManager.ldf Using SQL Commands

Execute the following SQL commands if you are using MSDE or if you prefer to use SQL commands to prevent `db_ControlManager.mdf` and `db_ControlManager.ldf` from occupying excessive disk space.

To shrink db_ControlManager.mdf and db_ControlManager.ldf, execute these SQL commands using a SQL query tool:

```
Alter Database db_controlManager set recovery
FULL

Backup log db_controlManager with truncate_only

DBCC shrinkDatabase(db_controlManager)
```

Note: The third command might take longer depending on the size of the database.

```
EXEC sp_dboption 'db_ControlManager', 'trunc. log
on chkpt.', 'TRUE'

Alter Database db_controlManager set recovery
simple

Alter Database db_controlManager set auto_shrink
on
```

Section 4

Services and Tools

Chapter 16

Using Trend Micro Services

This chapter provides details about the various services available when using 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

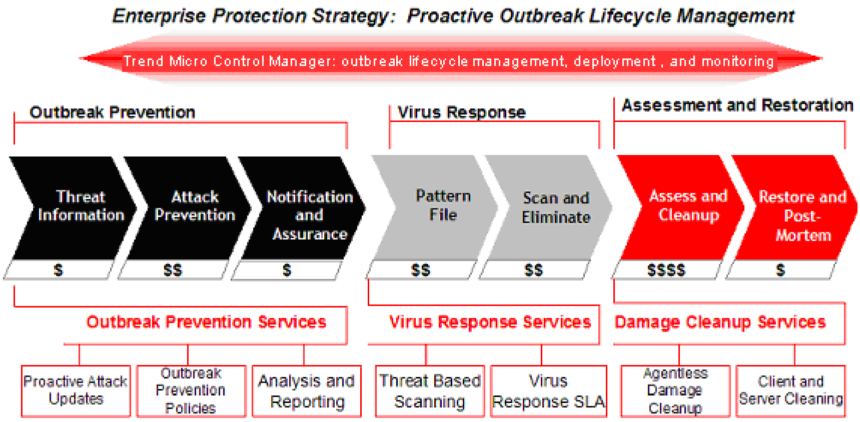


FIGURE 16-1. Enterprise Protection Strategy

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

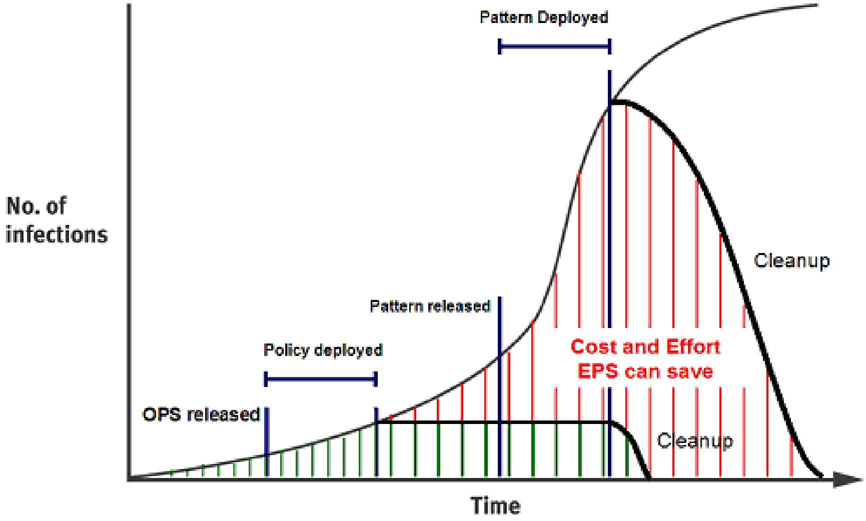


FIGURE 16-2. Cost vs. Effort

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.

Introducing Outbreak Prevention Services

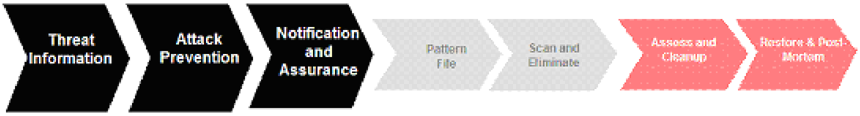


FIGURE 16-3. Outbreak Prevention Services

Understanding 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 delivers 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 16-1. 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

After activating Outbreak Prevention Services, administrators still need to start Outbreak Prevention Mode to protect the network during a virus outbreak.

To activate Outbreak Prevention Services:

Path: License Information

Path: Administration > License Management > Control Manager

1. Navigate to the License Information screen.
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 Status page to instantly know the state of the following service status items:

TABLE 16-2. 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 page also provides an easy way to view the Control Manager components and the version that are currently in use.

To view the Outbreak Prevention Services status:

Path: Services > Outbreak Prevention

1. Navigate to the Outbreak Prevention screen.

This page automatically refreshes to make sure the top threat and status information is current.

Preventing Virus Outbreaks and Understanding the 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 Control Manager 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 Control Manager can deploy policies at all layers to protect critical points during a virus outbreak.

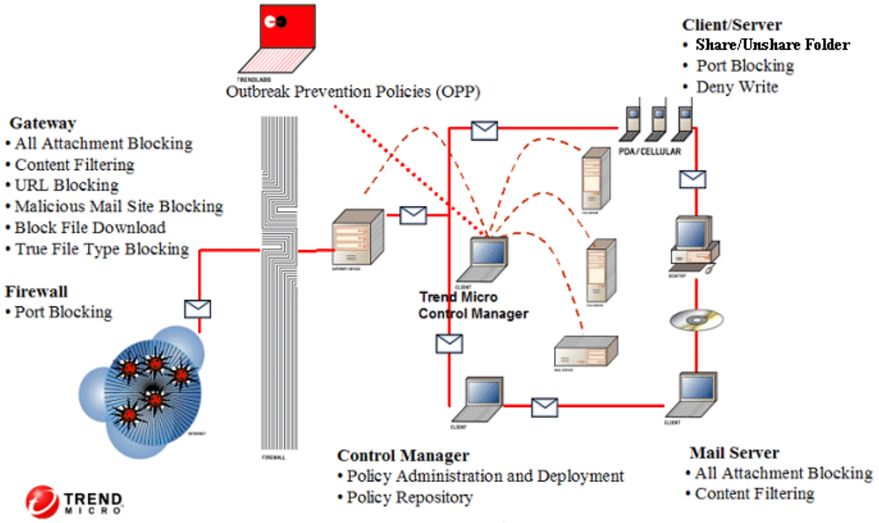


FIGURE 16-4. Deploying OPP

Accessing the Outbreak Prevention Services Settings Screen

To access the Outbreak Prevention Services Settings screen:

Path: Services > Services

1. Navigate to the Outbreak Prevention Settings screen.

   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.

To Update Outbreak Prevention Policies Manually:

Path: Services > Outbreak Prevention

1. Navigate to the Outbreak Prevention screen.

   This page 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.
3. Click **OK** twice after downloading the Outbreak Prevention Policies.

To avoid additional maintenance tasks, schedule Control Manager to automatically check for and download the latest Outbreak Prevention Policies.

Tip: 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.

To Schedule Updates to Outbreak Prevention Policies:

Path: Services > Settings

1. Navigate to the Outbreak Prevention Settings screen.
2. On the working area, click the **Download** tab.

3. Under Scheduled policy download settings, select the **Enable scheduled policy update** check box.
4. From the Download frequency list, choose the number of minutes for Control Manager to check for updated Outbreak Prevention Policies.
5. Under Download source, click the source that contains the latest Outbreak Prevention Policies. By default, this is the Trend Micro ActiveUpdate server. If you choose another Internet source, type the location in **Other update source**.
6. Click **Save**.
7. Click **OK**.

Starting Outbreak Prevention Mode

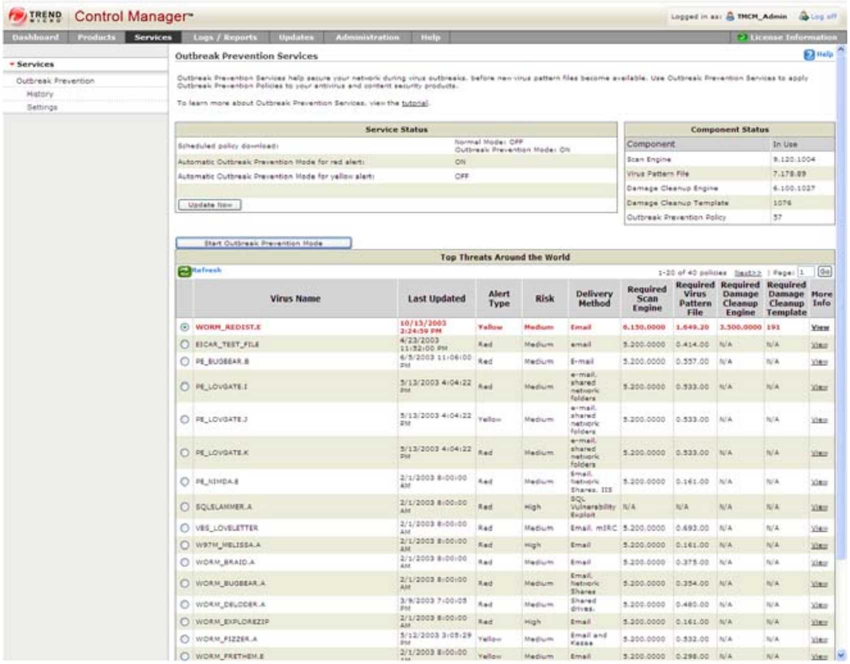
During a virus outbreak, start Outbreak Prevention Mode to deploy attack-specific Outbreak Prevention Policies and minimize the chance of your network becoming infected. Start Outbreak Prevention Mode to counter a single, specific threat.

To start Outbreak Prevention Mode:

Path: Services > Outbreak Prevention

1. Navigate to the Outbreak Prevention screen.

   This page automatically refreshes to make sure the top threat and status information is current.



Outbreak Prevention Services

Outbreak Prevention Services help secure your network during virus outbreaks, before new virus pattern files become available. Use Outbreak Prevention Services to apply Outbreak Prevention Policies to your antivirus and content security products.

To learn more about Outbreak Prevention Services, view the tutorial.

Service Status	
Scheduled policy download:	Normal Mode: OFF Outbreak Prevention Mode: ON
Automatic Outbreak Prevention Mode for red alert:	ON
Automatic Outbreak Prevention Mode for yellow alert:	OFF

Component	In Use
Scan Engine	9.120.1004
Virus Pattern File	7.178.89
Damage Cleanup Engine	6.100.1027
Damage Cleanup Template	1076
Outbreak Prevention Policy	57

Top Threats Around the World

	Virus Name	Last Updated	Alert Type	Risk	Delivery Method	Required Scan Engine	Required Virus Pattern File	Required Damage Cleanup Engine	Required Damage Cleanup Template	More Info
●	WORM_REDIST.E	10/13/2003 2:24:59 PM	Yellow	Medium	Email	6.150.0000	1.649.20	3.500.0000	191	View
○	EICAR_TEST_FILE	4/23/2003 11:32:00 PM	Red	Medium	email	5.200.0000	0.414.00	N/A	N/A	View
○	PE_BUGBEAR.B	6/5/2003 11:06:00 PM	Red	Medium	E-mail	5.200.0000	0.557.00	N/A	N/A	View
○	PE_LOVGATE.I	5/13/2003 4:04:22 PM	Red	Medium	e-mail, shared network folders	5.200.0000	0.533.00	N/A	N/A	View
○	PE_LOVGATE.J	5/13/2003 4:04:22 PM	Yellow	Medium	e-mail, shared network folders	5.200.0000	0.533.00	N/A	N/A	View
○	PE_LOVGATE.K	5/13/2003 4:04:22 PM	Red	Medium	e-mail, shared network folders	5.200.0000	0.533.00	N/A	N/A	View
○	PE_NIMDA.E	2/1/2003 8:00:00 AM	Red	Medium	Email, Network Shares, IIS	5.200.0000	0.161.00	N/A	N/A	View
○	SQLSLAMMER.A	2/1/2003 8:00:00 AM	Red	High	SQL Vulnerability Exploit	N/A	N/A	N/A	N/A	View
○	VBS_LOVELETTER	2/1/2003 8:00:00 AM	Red	Medium	Email, mIRC	5.200.0000	0.693.00	N/A	N/A	View
○	W97M_MELISSA.A	2/1/2003 8:00:00 AM	Red	High	Email	5.200.0000	0.161.00	N/A	N/A	View
○	WORM_BRAID.A	2/1/2003 8:00:00 AM	Red	Medium	Email	5.200.0000	0.375.00	N/A	N/A	View
○	WORM_BUGBEAR.A	2/1/2003 8:00:00 AM	Red	Medium	Email, Network Shares	5.200.0000	0.354.00	N/A	N/A	View
○	WORM_DELODER.A	3/9/2003 7:00:05 PM	Red	Medium	Shared drives.	5.200.0000	0.480.00	N/A	N/A	View
○	WORM_EXPLOREZIP	2/1/2003 8:00:00 AM	Red	High	Email	5.200.0000	0.161.00	N/A	N/A	View
○	WORM_FIZZER.A	5/12/2003 3:05:29 PM	Yellow	Medium	Email and Kazaa	5.200.0000	0.532.00	N/A	N/A	View
○	WORM_FRETHEM.E	2/1/2003 8:00:00 AM	Yellow	Medium	Email	5.200.0000	0.298.00	N/A	N/A	View

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** twice 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 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 the **Do not block permitted port numbers specified in the Outbreak Prevention settings** check box 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 on 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

To edit an Outbreak Prevention Policy:

Path: Services > Outbreak Prevention

1. Navigate to the Outbreak Prevention screen.

   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 the **Do not block permitted port numbers specified in the Outbreak Prevention settings** check box 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 16-3. 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.

TABLE 16-3. Virus Alert Criteria

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.

To set Automatic Outbreak Prevention Mode:

Path: Services > Settings

1. Navigate to the Outbreak Prevention Settings screen.

   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 the **Enable automatic outbreak prevention** check box.
   - To set Automatic Outbreak Prevention Mode for yellow alert viruses, under Yellow Alert Viruses, select the **Enable automatic outbreak prevention** check box.

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 the **Stop OPP automatically after the prevention duration expires** check box 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.

To configure Outbreak Prevention Mode download settings:

Path: Services > Settings

1. Navigate to the Outbreak Prevention Settings screen.

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 5-23.
- To deploy the virus pattern file only, select the **Exclude Scan Engine Deployment** check box.

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 on the management console.

To stop Outbreak Prevention Mode:

Path: Services > Outbreak Prevention

1. Navigate to the Outbreak Prevention screen.

   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 16-4. 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 ID of the Control Manager user that applied the policy
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.

To view Outbreak Prevention Mode history:

Path: Services > History

1. Navigate to the Outbreak Prevention History screen.
2. To view the status of a specific Outbreak Prevention Policy, click **View** in the same row. The status window displays the number of viruses detected by your antivirus products.

Using Outbreak Prevention Mode

Outbreak Prevention Mode Introduction

This tutorial guides you through starting Outbreak Prevention Mode, and is divided into the following topics:

- Step 1: Identifying the Source of the Outbreak on page 16-20
- Step 2: Evaluating Existing Policies on page 16-21
- Step 3: Starting Outbreak Prevention Mode on page 16-22
- Step 4: Follow-Up Procedures on page 16-23

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 16-5. 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 status 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 Using Event Center on page 8-2.

For creating scheduled policy downloads, see Updating Outbreak Prevention Policies on page 16-11.

What best describes your Control Manager server's capabilities?

- 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 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.

To start outbreak prevention answer the following:

- **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 5-23.

- **Which entry points do you want this policy to block?**

  The products involved in this stage are:

  - InterScan eManager
  - InterScan WebProtect for ICAP

- 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.

To evaluate or modify any of the product settings:

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 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 17

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 5.5 supports the following tools:

- Using Agent Migration Tool (AgentMigrateTool.exe) on page 17-2: to migrate Control Manager agents to a Control Manager 5.5 server
- Using the Control Manager MIB File on page 17-2: 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 17-3: use the NVW Enforcer MIB file with an application (for example, HP OpenView) that supports SNMP protocol
- Using the Appliance Firmware Flash Utility on page 17-3: use the Appliance Firmware Flash Utility (AFFU) to update Network VirusWall Enforcer devices
- Using the DBConfig Tool on page 17-4: use the DBConfig to change the user account, password, and the database name for the Control Manager database

Using Agent Migration Tool (`AgentMigrateTool.exe`)

The Agent Migration tool provided in Control Manager 5.5 Standard or Advanced Edition migrates agents administered by a Control Manager 5.5, 5.0, or 3.5 server.

To use the Agent Migration tool:

- Run `AgentMigrateTool.exe` directly on the destination server from the following location:

  `<root>\Program Files\Trend Micro\Control Manager\`

Note: For MCP agents, the Agent Migration Tool supports Windows-based and Linux-based agent migration.

For Control Manager 2.x agents, the Agent Migration Tool can only migrate Windows-based agents. Please contact Trend Micro Support for migrating non-Windows based agents (see *Contacting Technical Support on page 19-2*).

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.

To use the Control Manager MIB file:

Path: Administration > Tools

1. Navigate to the Tools screen.
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.

To use the NVW Enforcer SNMPv2 MIB file:

Path: Administration > Tools

1. Navigate to the Tools screen.
2. On the working area, 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 Appliance Firmware Flash Utility

Use the Appliance Firmware Flash Utility (AFFU) to update the device BMC firmware, BIOS, and program file. The utility is a graphical user interface tool that provides a user-friendly method of uploading the latest program file and boot loader for Network VirusWall Enforcer appliances.

To access the AFFU:

Path: Administration > Tools

1. Navigate to the Tools screen.
2. On the working area, click **AFFU**.
3. On the File Download screen, select **Save**, specify a location on the server, and then click **OK**.
4. Extract the AFFU file to the server.
5. Execute the AFFU file.

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.

Control Manager 3.5 only supports SQL authentication.

To use the DBConfig tool:

1. From the Control Manager server, click **Start > Run**.
2. Type **cmd**, and then click **OK**. The command prompt dialog box appears.
3. Change the directory to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\DBConfig`).
4. Type the following:

   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"

Section 5

Removing Control Manager and Contacting Support

Chapter 18

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):

- 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 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.

Remove the Control Manager Application

Manual removal of the Control Manager application involves the following steps:

1. *Stopping Control Manager Services*.
2. *Removing Control Manager IIS Settings*.
3. *Removing Crystal Reports, PHP, FastCGI, TMI, and CCGI*.
4. *Deleting Control Manager Files/Directories and Registry Keys*.
5. *Removing the Database Components*.
6. *Removing Control Manager and NTP Services*.

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).

To stop Control Manager services:

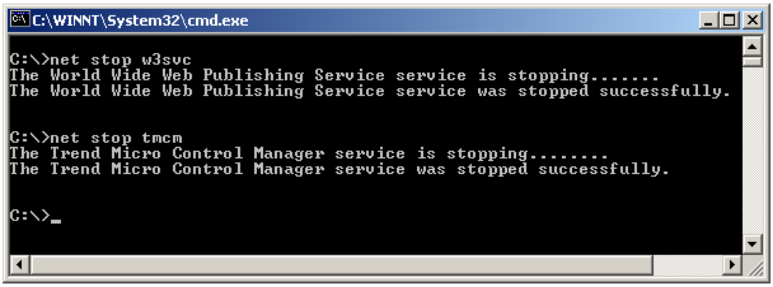
1. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
2. Right-click `<Control Manager service>`, and then click **Stop**.

To stop IIS and Control Manager services from the command prompt:

Run the following commands at the command prompt:

```
net stop w3svc

net stop tmcm
```



```
C:\>net stop w3svc
The World Wide Web Publishing Service service is stopping.......
The World Wide Web Publishing Service service was stopped successfully.

C:\>net stop tmcm
The Trend Micro Control Manager service is stopping........
The Trend Micro Control Manager service was stopped successfully.

C:\>_
```

FIGURE 18-1. 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.

To remove Control Manager IIS settings:

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
   - Viewer9
   - TVCS
   - Jakarta
   - WebApp
6. On IIS 6 only:
   - **a.** Right-click the IIS website you set during installation.
   - **b.** Click **Properties**.
7. Click 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.

To remove Crystal Reports:

1. On Control Manager server, click **Start > Settings > Control Panel > Add/Remove Programs**.
2. Scroll down to Crystal Reports Runtime Files, then click **Remove** to remove the Crystal Reports related files automatically.

To remove PHP and FastCGI:

1. On 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.

To remove TMI and CCGI:

1. Download the Microsoft service tool `Sc.exe` to the Control Manager server:

   http://support.microsoft.com/kb/251192/en-us
2. Run `Sc.exe` and type the following commands:

   ```
   sc delete "TrendCGI"
   ```

   ```
   sc delete "TrendMicro Infrastructure"
   ```

Deleting Control Manager Files/Directories and Registry Keys

To manually remove a Control Manager server:

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

To remove Control Manager ODBC settings:

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 window, click the **System DSN** tab.

4. Under **Name**, select **ControlManager_Database**.
5. Click **Remove**, and click **Yes** to confirm.

To remove the Control Manager SQL Server 2005 Express database:

1. On Control Manager server, click **Start > Control Panel > Add/Remove Programs**.
2. Scroll down to **SQL Server 2005 Express**, then click **Remove** to remove the Crystal Reports related files automatically.

Tip: Trend Micro recommends visiting the website for Microsoft for instructions on removing SQL Server 2005 Express if you have any issues with the uninstallation: http://support.microsoft.com/kb/909967

Removing Control Manager and NTP Services

To remove Control Manager and NTP services:

1. Download the Microsoft service tool `Sc.exe` to the Control Manager server:

   http://support.microsoft.com/kb/251192/en-us

2. Run `Sc.exe` and type the following commands:

   ```
   sc delete "TMCM"
   sc delete "TrendMicro_NTP"
   ```

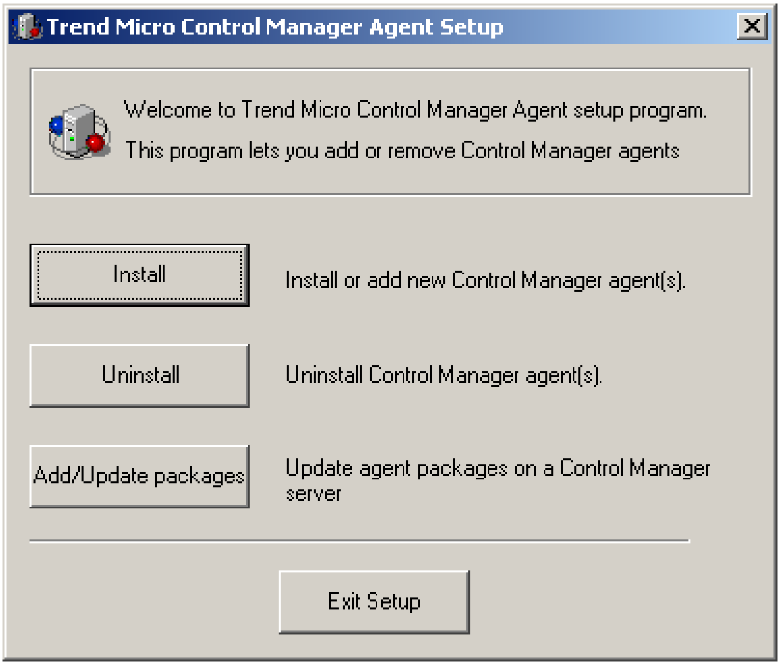
Removing a Windows-Based Control Manager 2.x Agent

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.

To remove a Windows-based Control Manager 2.x agent:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Settings** from the drop-down menu. A sub-menu appears.
3. Click **Add/Remove Product Agents**. The Add/Remove Product Agents screen appears.
4. Click **Use RemoteInstall.exe** and install the application.
5. Using Microsoft Explorer, go to the location where you saved the agent setup program.
6. Double-click the `RemoteInstall.exe` file. The Control Manager Agent setup screen appears.



Welcome to Trend Micro Control Manager Agent setup program.

This program lets you add or remove Control Manager agents

Install or add new Control Manager agent(s).

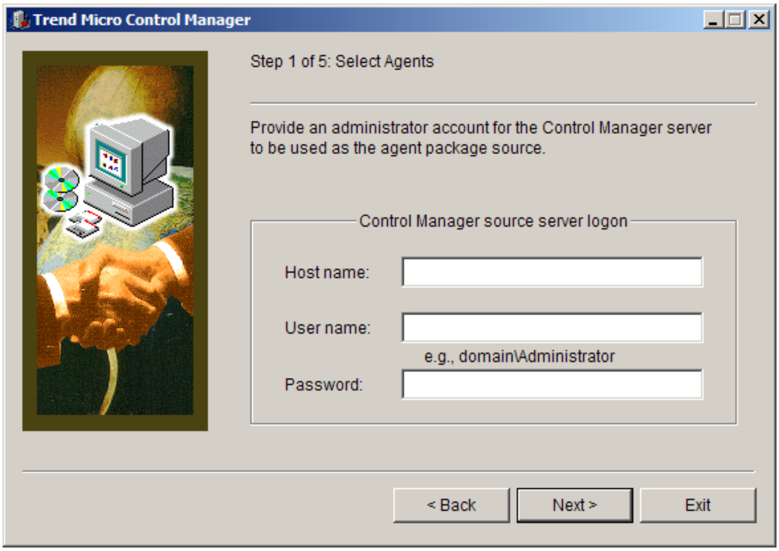
Uninstall Control Manager agent(s).

Update agent packages on a Control Manager server

FIGURE 18-2. Trend Micro Agent setup program

7. Click **Uninstall**. The Welcome screen appears.

8. Click **Next**. The Control Manager source server log on screen appears.



Step 1 of 5: Select Agents

Provide an administrator account for the Control Manager server to be used as the agent package source.

Control Manager source server logon

Host name:

User name:

e.g., domain\Administrator

Password:

FIGURE 18-3. Control Manager source server logon

9. Specify and provide Administrator-level logon credentials for the Control Manager server e. Type the following information:
   - **Host name**
   - **User name**
   - **Password**
10. Click **Next**. Select the product whose agent you want to remove.
11. 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.

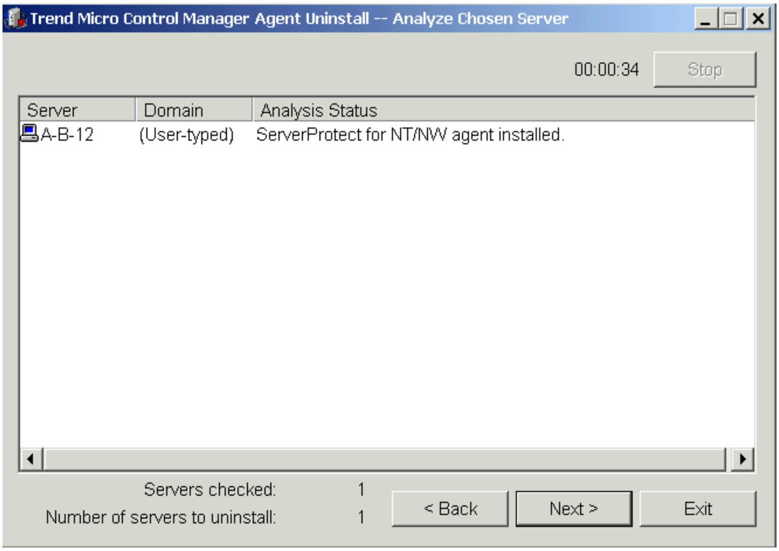
To specify a server name directly:

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.

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**.

12. Click **Back** to return to the previous screen, **Exit** to abort the operation, or **Next** to continue.
13. Provide Administrator-level logon credentials for the selected servers. Type the required user name and password in the appropriate field.
14. Click **OK**. The Uninstallation List screen provides the following details about the target servers: server name, domain, and the type of agent detected.



Trend Micro Control Manager Agent Uninstall -- Analyze Chosen Server

00:00:34

Server	Domain	Analysis Status
A-B-12	(User-typed)	ServerProtect for NT/NW agent installed.

Servers checked: 1

Number of servers to uninstall: 1

FIGURE 18-4. Analyze chosen Control Manager server

15. 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.

16. Click **OK**, and then at the Removing Agents screen, click **Exit**.

Chapter 19

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 on page 19-2
- Contacting Technical Support on page 19-2
- TrendLabs on page 19-3
- Other Useful Resources on page 19-3

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/support

Contacting Technical Support

In addition to phone support, Trend Micro provides the following resources:

- Email support:

  http://us.trendmicro.com/us/products/customer-service/
- On-line help: configuring the product and parameter-specific tips
- Readme: late-breaking product news, installation instructions, known issues, and version-specific information
- Knowledge Base: technical procedures provided by the Support team:

  http://esupport.trendmicro.com/support
- Product updates and patches:

  http://downloadcenter.trendmicro.com/

To locate the Trend Micro office nearest you, go to:

http://us.trendmicro.com/us/about/contact/

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^{SM} 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://us.trendmicro.com/us/about/company/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

Section 6

Appendixes

Appendix A

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 installation, 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	10.1.114.225	
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	

TABLE A-1. Server Address Checklist

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 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 ID	`root`	
Encryption key location	`C:\MyDocuments\E2EPulic.dat`	

Note: You can use any User ID in lieu of the Root account User name. However, Trend Micro recommends using the Root account, because deleting the User ID 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 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, Setup 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 the 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

TABLE A-2. Control Manager Configuration Files

CONFIGURATION FILE	DESCRIPTION
`CastoolConfiguration.xml`	Used by `CasTool.exe`
`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
`Entity.cfg`	Managed product configuration file

TABLE A-3. Control Manager Processes

PROCESSES	DESCRIPTION
`CasTool.exe`	A command line program used to establish a cascading Control Manager environment. This tool is only used by Control Manager 3.5.
`ProcessManager.exe`	"Trend Micro Control Manager" service. It launches and stops other Control Manager core processes.
`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 at the Control Manager web console, into actual commands.
`LogReceiver.exe`	Receives managed product logs and messages.

TABLE A-3. Control Manager Processes

PROCESSES	DESCRIPTION
`LogProcessor.exe`	Receives new messages from managed products and receives the entity information from 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.
`EntityEmulator.exe`	Allows Control Manager to use Trend VCS agents.
`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.
`dmserver.exe`	Provides the Control Manager web console log on page and manages the Product Directory (Control Manager-side).
`LWDMServer.exe`	Manages the Product Directory (managed product-side).

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
`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					
	3.X Ent	3.X Std	5.0 Adv	5.0 Std	5.5 Adv	5.5 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	●	●	●	●	●	●
Communicator Scheduler	●	●	●	●	●	●
Component download granularity	●	●	●	●	●	●
Configuration by group	●	●	●	●	●	●

TABLE A-4. Product Version Comparison

FEATURES	CONTROL MANAGER VERSION					
	3.X ENT	3.X STD	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD
Configure multiple download sources	●	●	●	●	●	●
Consistent managed product and Control Manager UI	●	●	●	●	●	●
Control Manager MIB files (previously called HP Open-View 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					●	●
Manage antivirus and content security products	●	●	●	●	●	●
Manage services	●	●	●	●	●	●
Managed product license manager			●		●	
Managed product reporting	●		●		●	

TABLE A-4. Product Version Comparison

FEATURES	CONTROL MANAGER VERSION					
	3.X ENT	3.X STD	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD
Web console rendering enhancement					●	●
Microsoft SQL Express or Microsoft SQL2005			●	●	●	●
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	●		●		●	
Remote and Local Agent Installation	●	●	●	●	●	●
Remote management	●	●	●	●	●	●
Reporting	●		●		●	
Secure communication between Server and Agents	●	●	●	●	●	●

TABLE A-4. Product Version Comparison

FEATURES	CONTROL MANAGER VERSION					
	3.X ENT	3.X STD	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD
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	●	●	●	●	●	●
Supports Trend VCS agents	●	●				
Syslog notification			●		●	
Threat Intelligence-Oriented Dashboard					●	●
Trend Micro InterScan for Cisco Content Security and Control Security Services Module (ISC CSC SSM) integration	●	●	●	●	●	●
Trend Micro Network VirusWall 1200 integration	●	●	●	●	●	●
Trend Micro Network VirusWall 2500 integration	●	●	●	●	●	●

TABLE A-4. Product Version Comparison

FEATURES	CONTROL MANAGER VERSION					
	3.X ENT	3.X STD	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD
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 5 report templates and to Ad Hoc Query requests.

This appendix contains the following sections:

Understanding Data Views

Control Manager 5.5 allows direct queries to the Control Manager database. Data views are available to Control Manager 5 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 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 B-1. 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.

Product Information

Product Information Data Views provide information about Control Manager, managed products, components, and product licenses.

TABLE B-1. Product Information Data Views

DATA VIEW	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 product or managed product clients.
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 B-2. Security Threat Data Views

DATA VIEW	DESCRIPTION
Overall Threat Information	Displays summary and statistical data about the overall threat landscape of your network.
Virus/Malware Information	Displays summary and detailed data about malware/viruses managed products detect on your network.

TABLE B-2. Security Threat Data Views

DATA VIEW	DESCRIPTION
Spyware/Grayware Information	Displays summary and detailed data about spyware/grayware managed products detect on your network.
Content Violation Information	Displays summary and detailed data about prohibited content managed products detect on your network.
Spam Violation Information	Displays summary and detailed data about spam managed products detect on your network.
Web Violation Information	Displays summary and detailed data about Internet violations managed products detect on your network.
Policy/Rule Violation Information	Displays summary and detailed data about policy/rule violations managed products detect on your network.
Suspicious Threat Information	Displays summary and detailed data about suspicious activity managed products detect on your network.

Data Views: Product Information

Displays information about Control Manager, Managed Products, components, and licenses.

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-3. 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 Service
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.

TABLE B-3. Product License Status Data View

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-4. 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-5. 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**
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

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-6. 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 products
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-7. 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 a client (for example OfficeScan client) 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 host name of a computer with a client (for example OfficeScan client) 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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) installed.

TABLE B-7. Product Status Information Data View

DATA	DESCRIPTION
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 client’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 a client (for example OfficeScan client) uses. Example: up-to-date, out-of-date
Engine Status	Displays the status of the scan engines the managed product or a computer with a client (for example OfficeScan client) 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 client’s version number. Example: OfficeScan **10.0**, Control Manager **5.0**

TABLE B-7. Product Status Information Data View

DATA	DESCRIPTION
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 a client (for example OfficeScan client) has in the network environment. Example: server, client
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.

ServerProtect and OfficeScan Server/Domain Status Summary

Displays summary information about client/server managed products. Examples: pattern file out-of-date, scan engine out-of-date,

TABLE B-8. ServerProtect and OfficeScan Server/Domain Status Summary Data View

DATA	DESCRIPTION
Product Entity	Displays the entity display name for a managed product.
Domain	Displays the domain to which the managed product belongs.
Endpoints	Displays the number of endpoints in a domain.

TABLE B-8. ServerProtect and OfficeScan Server/Domain Status Summary Data View

DATA	DESCRIPTION
Patterns Out-of-Date	Displays the number of endpoints with out-of-date pattern files.
Patterns Up-to-Date Rate (%)	Displays the percentage of endpoints with up-to-date pattern files.
Engines Out-of-Date	Displays the number of endpoints with out-of-date scan engines.
Engines Up-to-Date Rate (%)	Displays the percentage of endpoints with up-to-date scan engines.

Product Event Information

Displays information relating to managed product events. Examples: managed products registering to Control Manager, component updates, Activation Code deployments

TABLE B-9. 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**

TABLE B-9. Product Event Information Data View

DATA	DESCRIPTION
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.

Component Information

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-10. 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 a client (for example OfficeScan client) installed.

TABLE B-10. Engine Status Data View

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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) 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 client'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 client's version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Product Role	Displays the role the managed product or a computer with a client (for example OfficeScan client) has in the network environment. Example: server, client
Engine	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine

TABLE B-10. Engine Status Data View

DATA	DESCRIPTION
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-11. 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 a client (for example OfficeScan client) 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 host name of a computer with a client (for example OfficeScan client) installed.

TABLE B-11. Pattern/Rule Status Data View

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 a client (for example OfficeScan client) 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 client’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 client’s version number. Example: OfficeScan **10.0**, Control Manager **5.0**
Product Role	Displays the role the managed product or a computer with a client (for example OfficeScan client) has in the network environment. Example: server, client
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

TABLE B-11. Pattern/Rule Status Data View

DATA	DESCRIPTION
Pattern/Rule Updated	Displays the time of the latest pattern file/rule deployment to managed products or endpoints.

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-12. 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

TABLE B-12. Product Component Deployment Data View

DATA	DESCRIPTION
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
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.

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-13. 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.

TABLE B-13. Engine Status Summary Data View

DATA	DESCRIPTION
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-14. 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.

Control Manager Information

User Access Information

Displays Control Manager user access and the activities users perform while logged on to Control Manager.

TABLE B-15. 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-16. 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-17. 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

TABLE B-17. Command Tracking Information Data View

DATA	DESCRIPTION
User	Displays the user who issued the command.
Updated	Displays the time of the latest status check of all commands for the selected Control Manager.
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-18. 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.

TABLE B-18. Detailed Command Tracking Information Data View

DATA	DESCRIPTION
Command Status	Displays the status of the command: successful, unsuccessful, in progress
Updated	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

Summary Information

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-19. 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

TABLE B-19. Overall Virus/Malware Summary Data View

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

Overall Virus/Malware Type Summary

Provides broad summary for virus/malware detections. Example: type of virus/malware (Trojans, hacking tools), number of unique viruses/malware on your network, total number of instances of viruses/malware on the network

TABLE B-20. Overall Virus/Malware Type Summary Data View

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.
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

TABLE B-20. Overall Virus/Malware Type Summary Data View

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-21. 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

TABLE B-21. Virus/Malware Source Summary Data View

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-22. 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

TABLE B-22. Virus/Malware Endpoint Summary Data View

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 Detections Over Time Summary

Provides a summary of virus/malware 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 virus, total number of instances of viruses/malware on the network

TABLE B-23. Virus/Malware Detections Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.
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
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

TABLE B-23. Virus/Malware Detections Over Time Summary Data View

DATA	DESCRIPTION
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
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-24. 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

TABLE B-24. Virus/Malware Action/Result Summary Data View

DATA	DESCRIPTION
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
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

Detailed Information

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-25. 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.

TABLE B-25. Detailed Virus/Malware 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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) installed.
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

TABLE B-25. Detailed Virus/Malware Information Data View

DATA	DESCRIPTION
Endpoint	Displays the IP address or host name of the computer affected by viruses/malware.
Source	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)
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 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-26. 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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) installed.
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.

TABLE B-26. Endpoint Virus/Malware Information Data View

DATA	DESCRIPTION
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-27. 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 a client (for example OfficeScan client) 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.

TABLE B-27. Web Virus/Malware Information Data View

DATA	DESCRIPTION
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.
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-28. 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.

TABLE B-28. Email Virus/Malware 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
Virus/Malware	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
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

TABLE B-28. Email Virus/Malware Information Data View

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

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-29. 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 a client (for example OfficeScan client) installed.
Product	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE B-29. Network Virus/Malware Information Data View

DATA	DESCRIPTION
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.
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.

TABLE B-29. Network Virus/Malware Information 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
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

Summary Information

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-30. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Spyware/Grayware	Displays the name of spyware/grayware managed products detect.

TABLE B-30. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
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-31. Spyware/Grayware Source Summary Data View

DATA	DESCRIPTION
Source Host	Displays the name of the computer where spyware/grayware originates.

TABLE B-31. Spyware/Grayware Source Summary Data View

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-32. Endpoint Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Endpoint	Displays the host name or IP address of the computer affected by spyware/grayware.

TABLE B-32. Endpoint Spyware/Grayware Summary Data View

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-33. Spyware/Grayware Detection Over Time Summary Data View

DATA	DESCRIPTION
Date/Time	Displays the time that the summary of the data occurs.

TABLE B-33. Spyware/Grayware Detection Over Time Summary Data View

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-34. 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 Information

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-35. 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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) installed, that is affected by spyware/grayware.

TABLE B-35. Detailed Spyware/Grayware Information Data View

DATA	DESCRIPTION
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 a client (for example OfficeScan client) 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.
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

TABLE B-35. Detailed Spyware/Grayware Information Data View

DATA	DESCRIPTION
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-36. 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.

TABLE B-36. Endpoint Spyware/Grayware 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 a client (for example OfficeScan client) 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 a client (for example OfficeScan client) 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.
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.

TABLE B-36. Endpoint Spyware/Grayware Data View

DATA	DESCRIPTION
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

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-37. 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 a client (for example OfficeScan client) 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.
Endpoint	Displays the IP address or host name 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.

TABLE B-37. Web Spyware/Grayware Data View

DATA	DESCRIPTION
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.
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-38. 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
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.

TABLE B-38. Email Spyware/Grayware Data View

DATA	DESCRIPTION
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-39. 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.

TABLE B-39. Network Spyware/Grayware 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 a client (for example OfficeScan client) 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.
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.

TABLE B-39. Network Spyware/Grayware Data View

DATA	DESCRIPTION
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 end-point 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

Summary Information

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-40. 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

TABLE B-40. Content Violation Policy Summary Data View

DATA	DESCRIPTION
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-41. 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

TABLE B-41. Content Violation Sender Summary Data View

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

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-42. Content 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 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

TABLE B-42. Content Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
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-43. 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
Detections	Displays the number of violations with the specified action taken by managed products.

Detailed Information

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-44. 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.
Policy Settings	Displays the settings for the policy that an email violates.
File Location	Displays the location of the file that violates a policy.

TABLE B-44. Detailed Content Violation Information Data View

DATA	DESCRIPTION
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
Filter Action	Displays the action the detecting filter takes against email in violation of a policy. Example: clean, quarantine, strip
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.

Spam Violation Information

Summary Information

Overall Spam Violation Summary

Provides a summary of spam detections on specific domains. Example: name of the domain receiving spam, the number of endpoints receiving spam, the total number of spam violations on the network

TABLE B-45. Overall Spam Violation Summary Data View

DATA	DESCRIPTION
Recipient Domain	Displays the domain that receives 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-46. Spam Recipient Summary Data View

DATA	DESCRIPTION
Recipient	Displays the name of the recipient who receives spam.
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-47. 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

TABLE B-47. Spam Detection Over Time Summary Data View

DATA	DESCRIPTION
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 Information

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-48. 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.

TABLE B-48. Detailed Spam Information Data View

DATA	DESCRIPTION
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-49. Spam Connection Information Data View

DATA	DESCRIPTION
Received	Displays the time that Control Manager receives data from the managed product.

TABLE B-49. Spam Connection Information Data View

DATA	DESCRIPTION
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

Detailed Information

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-50. 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 a client (for example OfficeScan client) 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

TABLE B-50. Detailed Firewall Violation Information Data View

DATA	DESCRIPTION
Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol the intrusion uses. Example: HTTP, SMTP, FTP
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 targets.
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

Detailed Endpoint Security Violation Information

Provides specific information about the endpoint security 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-51. 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.
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 violation of the policy/rule.
Endpoint IP	Displays the IP address of the computer in violation of the policy/rule.
Endpoint MAC	Displays the MAC address of the computer in violation of the policy/rule.
Policy/Rule	Displays the name of the policy/rule in violation.
Service	Displays the name of the service/program in violation of the policy/rule.
User	Displays the user name logged on to the endpoint when a managed product detects a policy/rule violation.

TABLE B-51. Detailed Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Enforcement Action	Displays the action a managed product takes to protect your network. Example: block, redirect, pass
Remediation Action	Displays the action a managed product takes to solve the policy violation. Example: file cleaned, file quarantined, file deleted
Description	Displays a detailed description of the incident by Trend Micro.
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 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-52. 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.

TABLE B-52. Detailed Endpoint Security Compliance 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
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.
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-53. 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.
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

TABLE B-53. Detailed Application Activity Data View

DATA	DESCRIPTION
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.
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.
Policy/Rule	Displays the policy/rule the suspicious threat violates.

TABLE B-53. Detailed Application Activity Data View

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

Web Violation/Reputation Information

Summary Information

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
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

TABLE B-54. Overall Web Violation Summary Data View

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 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

TABLE B-55. Web Violation Endpoint Summary Data View

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

TABLE B-56. Web Violation URL Summary Data View

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

TABLE B-59. Web Violation Detection Summary Data View

DATA	DESCRIPTION
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
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 Information

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.

TABLE B-60. Detailed Web Violation Information Data View

DATA	DESCRIPTION
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.
Endpoint	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.

TABLE B-60. Detailed Web Violation Information Data View

DATA	DESCRIPTION
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 compliances 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.

TABLE B-61. Detailed Web Reputation Information Data View

DATA	DESCRIPTION
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.
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.

TABLE B-61. Detailed Web Reputation Information Data View

DATA	DESCRIPTION
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

Suspicious Threat Information

Summary Information

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.

TABLE B-62. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
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 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
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

TABLE B-62. Overall Suspicious Threat Summary Data View

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 equals 10.
Mitigations	Displays the number of endpoints Network VirusWall Enforcer devices or Total Discovery Mitigation Server take action against.
Cleaned Endpoints	Displays the total number of endpoints Total Discovery Mitigation Server cleans.
Clean Endpoint Rate (%)	Displays the percentage of endpoints Total Discovery Mitigation Server 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.
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

TABLE B-63. Suspicious Source Summary Data View

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
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.
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

TABLE B-64. Suspicious Threat Riskiest Endpoints Summary Data View

DATA	DESCRIPTION
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.
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

TABLE B-65. Suspicious Riskiest Recipient Summary Data View

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

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

TABLE B-66. Suspicious Sender Summary Data View

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 threats 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

TABLE B-67. Suspicious Threat Protocol Detection Summary Data View

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 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
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 threats detections over a period of time (daily, weekly, monthly). Example: time and date of 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

TABLE B-68. Suspicious Threat Detection Over Time Summary Data View

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
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 Information

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 for the mitigation server.
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
Endpoint IP	Displays the IP address of the endpoint the suspicious threat affects.

TABLE B-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
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.
Source IP	Displays the IP address of the source where the suspicious threat originates.
Source Host	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	Displays the MAC address of the source where the suspicious threat originates.
Source Domain	Displays the domain of the source where the suspicious threat originates.
VLAN ID	Displays the VLAN ID 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
Threat Confidence Level	Displays Trend Micro's confidence that the suspicious threat poses a danger to your network.
Detected By	Displays the filter, scan engine, or managed product which detects the suspicious threat.
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.

TABLE B-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
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 Total Discovery Appliance detects a violation.
Browser/FTP Client	Displays the Internet browser or FTP endpoint where the suspicious threat originates.
Channel Name	Displays the protocol that the instant messaging software or IRC use for communication.
File	Displays the name of the suspicious file.
File in Compressed File	Displays whether the suspicious threat originates from a compressed file.
File Size	Displays the size of the suspicious file.
File Extension	Displays the file extension of the suspicious file. Example: .wmf, .exe, .zip
True File Type	Displays the "true" file type which is detected using the file's header not the file's extension.
Shared Folder	Displays whether the suspicious threat originates from a shared folder.
Authentication	Displays whether authentication was used.
BOT Command	Displays the command that bots send or receive to or from the control channel.
BOT URL	Displays the URL that bots receive their commands from.
Constraint Type	Displays the reason that a file cannot be scanned correctly.

TABLE B-69. Detailed Suspicious Threat Information Data View

DATA	DESCRIPTION
Mitigation Result	Displays the result of the action the mitigation server takes against suspicious threats.
Mitigation Action	Displays the action the mitigation server takes against suspicious threats. Example: File cleaned, File dropped, File deleted
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

Overall Threat Information

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-70. 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
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

TABLE B-70. Network Security Threat Analysis Information Data View

DATA	DESCRIPTION
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-71. 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

TABLE B-71. Network Protection Boundary Information Data View

DATA	DESCRIPTION
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-72. 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

TABLE B-72. Security Threat Entry Analysis Information Data View

DATA	DESCRIPTION
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 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-73. Security Threat Endpoint Analysis Information Data View

DATA	DESCRIPTION
Endpoint	Displays the name of the computer affected by the security threat/violation.

TABLE B-73. Security Threat Endpoint Analysis Information Data View

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.

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-74. 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.

TABLE B-74. Security Threat Source Analysis Information Data View

DATA	DESCRIPTION
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.

Index