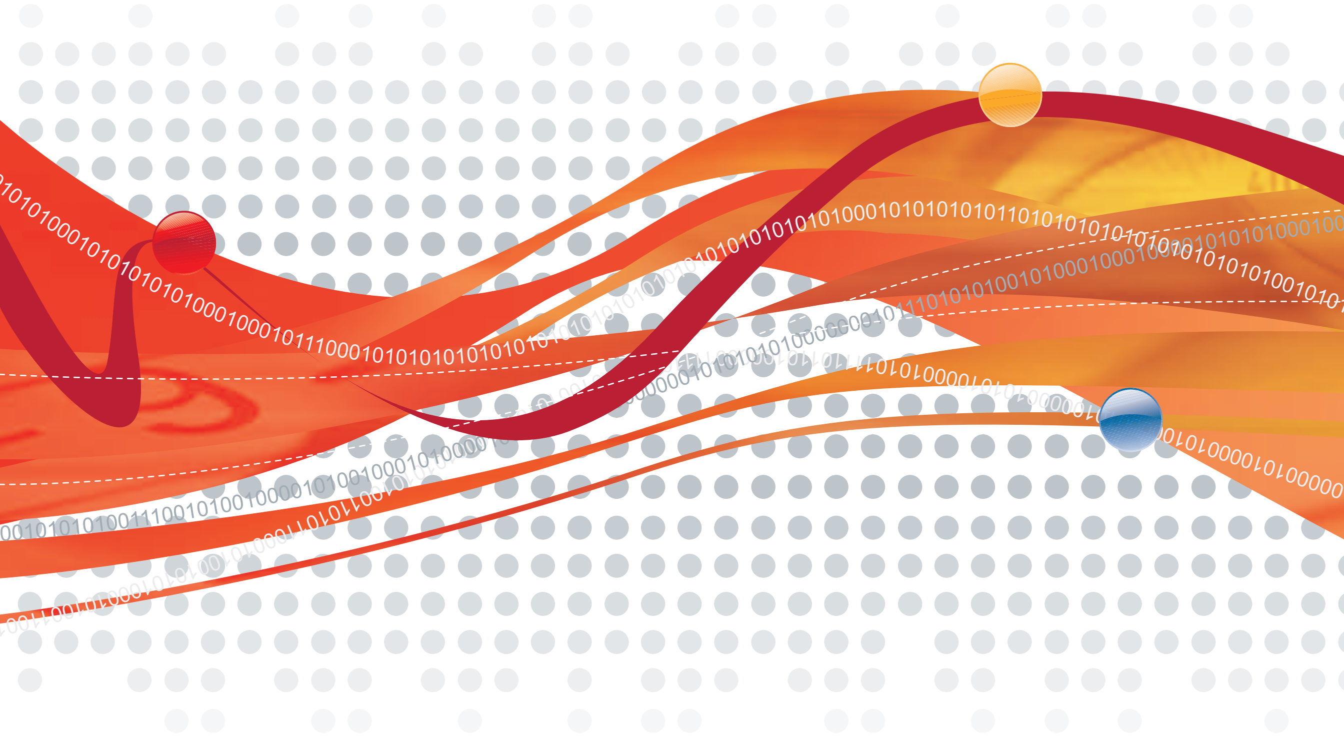
TREND MICRO™

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 Trend Micro's Web site at:

www.trendmicro.com/download/documentation/

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. TMEM53360/70921

Release Date: February 2008

The Administrator's Guide for Trend Micro Control Manager™ is intended to introduce the main features of the software, installation instructions for your production environment, 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 starting on page 11-2 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 Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Preface

What's New in This Version . . . . P-ii
Control Manager Documentation . . . . .P-vi
About this Administrator's Guide . . . . P-vii
Audience . . . . .P-viii
Document Conventions . . . . .P-ix

Chapter 1: Introducing Trend Micro Control Manager™

Control Manager Standard and Advanced 1-2
How to Use Control Manager 1-2
Understanding Trend Micro Management Communication Protocol ... 1-3
Reduced Network Loading and Package Size 1-4
NAT and Firewall Traversal Support 1-5
HTTPS Support 1-5
One-way and Two-way Communication Support 1-6
One-way Communication 1-6
Two-way Communication 1-6
Single Sign-on (SSO) Support 1-7
Control Manager Architecture 1-7

Chapter 2: Planning and Implementing the Control Manager Deployment

Identifying Deployment Architecture and Strategy 2-2
Understanding Single-Site Deployment 2-2
Understanding Multiple-Site Deployment 2-5
Installation Flow 2-9
Supported Operating Systems 2-9
Testing Control Manager at One Location 2-10
Server Distribution Plan 2-12
Understanding Administration Models 2-12
Understanding Control Manager Server Distribution 2-12
Single-Server Topology 2-13
Multiple-Server Topology 2-13

Network Traffic Plan 2-13
Understanding Control Manager Network Traffic 2-13
Sources of Network Traffic 2-14
Traffic Frequency 2-14
Logs 2-14
Managed Product Agent Heartbeat 2-14
Network Protocols 2-15
Sources of Network Traffic 2-15
Log Traffic 2-15
Trend Micro Management Communication Protocol Policies 2-16
Trend Micro Management Infrastructure Policies 2-16
Product Registration Traffic 2-17
Deploying Updates 2-18
Understanding Deployment Updates 2-18
Data Storage Plan 2-19
Database Recommendations 2-19
ODBC Drivers 2-19
Authentication 2-20
Web Server Plan 2-20
Web Server Configuration 2-20

Chapter 3: Installing Trend Micro Control Manager for the First Time

System Requirements 3-2
Minimum System Requirements 3-2
Recommended System Requirements 3-4
Installing a Control Manager Server 3-4
Verifying Successful Installations 3-22
Verify a Successful Control Manager Server Installation 3-22
Post-installation Configuration 3-24
Registering and Activating Control Manager 3-24
Configuring User Accounts 3-24
Downloading the Latest Components 3-24
Setting Notifications 3-25
Registering and Activating Your Software 3-25
Activating Control Manager 3-25
Converting to the Full Version 3-26

Renewing Your Product Maintenance ... 3-26

Chapter 4: Upgrading Servers or Migrating Agents to Control Manager 5.0

Upgrading to Control Manager 5.0 ... 4-2
Upgrading Control Manager 3.0 or 3.5 Servers ... 4-2
Upgrading and Migrating Scenarios ... 4-2
Rolling Back to Control Manager 3.0/3.5 Servers ... 4-10
Planning Control Manager Agent Migration ... 4-11
Migration Scenarios for Control Manager 2.x Agents ... 4-13
Control Manager 2.5x Agent Migration Flow ... 4-14
MCP Agent Migration Flow ... 4-15
Migrating Control Manager 2.5x and MCP Agents ... 4-15
Migrating the Control Manager Database ... 4-17
Migrating Control Manager SQL 2005 Database to Another SQL 2005 Server ... 4-17

Chapter 5: Getting Started with Control Manager

Using the Management Console ... 5-2
Understanding The Function-locking Mechanism ... 5-3
Accessing the Management Console ... 5-4
Assigning HTTPS Access to the Control Manager Management Console ... 5-5
Accessing the HTTPS Management Console ... 5-6
Logging Off from the Management Console ... 5-6
Configuring Control Manager User Access ... 5-7
Understanding Account Types ... 5-8
Root Account Information ... 5-11
Adding Account Types ... 5-11
Editing Account Types ... 5-13
Understanding User Accounts ... 5-14
Setting Access Rights ... 5-15
Adding a User Account ... 5-16
Editing a User Account ... 5-21
Disabling a User Account ... 5-22
Deleting a User Account ... 5-22
Adding a User Group ... 5-22

Editing a User Group 5-25
Deleting a User Group 5-25
Understanding the Product Directory 5-26
Grouping Managed Products Using Directory Manager 5-27
Default Folders for the Product Directory 5-30
Managing Child Servers 5-30
Configuring Child Servers 5-31
Registering or Unregistering Child Servers 5-32
Downloading and Deploying New Components 5-35
Manually Downloading Components 5-37
Configuring Scheduled Download Exceptions 5-45
Understanding Scheduled Downloads 5-46
Configuring Scheduled Downloads and Enabling Scheduled Component Downloads 5-47
Configuring Scheduled Download Settings 5-55
Configuring Scheduled Download Automatic Deployment Settings 5-56
Understanding Deployment Plans 5-57
Configuring Proxy Settings 5-60
Configuring Update/Deployment Settings 5-62
Setting "Log on as batch job" Policy 5-63

Chapter 6: Monitoring the Control Manager Network
Viewing Summary Screens in Control Manager 6-2
Using Command Tracking 6-3
Understanding Command Details 6-4
Understanding Details for Individual Products or Services 6-4
Querying and Viewing Commands 6-5
Using Event Center 6-8
Customizing Notification Messages 6-11
Enabling or Disabling Notifications 6-14
Configuring Notification Methods 6-15
Configuring Notification Recipients and Testing Notification Delivery 6-17
Configuring Virus Outbreak Alert Settings 6-19
Configure Special Virus Alert Settings 6-20
Configure Special Spyware/Grayware Alert Settings 6-21

Configure Network Virus Alert Settings 6-21
Configure Potential Vulnerability Attack Detected Settings 6-22
Using Logs 6-23
Understanding Control Manager Generated Logs 6-24
Understanding Managed Product Logs 6-24
Understanding Log Aggregation 6-27
Querying Log Data 6-28
Understanding Data Views 6-29
Performing an Ad Hoc Query 6-30
Working With Saved and Shared Ad Hoc Queries 6-39
Editing Saved Ad Hoc Queries 6-40
Sharing Saved Ad Hoc Queries 6-43
Working With Shared Ad Hoc Queries 6-43
Deleting Logs 6-44
Configuring Automatic Log Deletion Settings 6-45
Working With Reports 6-47
Understanding Control Manager Report Templates 6-47
Understanding Control Manager 5.0 Templates 6-47
Understanding Control Manager 3.0 Templates 6-54
Adding Control Manager 5.0 Report Templates 6-57
Adding One-time Reports 6-71
Adding Scheduled Reports 6-77
Enabling/Disabling Scheduled Reports 6-84
Viewing Generated Reports 6-84
Configuring Report Maintenance 6-85

Chapter 7: Administering Managed Products

Understanding Agents 7-2
Understanding Communicators 7-3
Understanding Connection Status Icons 7-4
Understanding Control Manager Security Levels 7-6
Using the Agent Communication Scheduler 7-8
Understanding the Agent/Communicator Heartbeat 7-9
MCP Heartbeat 7-9
Using the Schedule Bar 7-10
Determining the Right Heartbeat Setting 7-11
Configuring Agent Communication Schedules 7-11

Modifying the Default Agent/Communicator Schedule 7-13
Setting the Agent/Communicator Heartbeat 7-15
Stopping and Restarting Control Manager Services 7-16
Modifying the Control Manager External Communication Port 7-16
Modifying the Security Level for TMI Agents 7-18
Modifying the Communicator Heartbeat Protocol 7-19
Verifying the Communication Method Between MCP and Control Manager 7-19
Understanding the Product Directory 7-20
Grouping Managed Products in the Product Directory 7-22
Default Folders for the Product Directory 7-24
Accessing the Product Directory 7-26
Manually Deploying New Components Using the Product Directory 7-27
Viewing Managed Product's Status Summaries 7-28
Configuring Managed Products 7-29
Issuing Tasks to Managed Products 7-29
Querying and Viewing Managed Product Logs 7-30
Recovering Managed Products Removed From the Product Directory 7-35
Changing Control Manager 2.x Agent Connection Re-Verification Frequency 7-36
Searching for Managed Products, Product Directory Folders or Computers 7-36
Refreshing the Product Directory 7-37
Understanding the Directory Management Screen 7-37
Using the Directory Management Screen Options 7-38
Accessing Directory Management 7-39
Creating Folders 7-40
Renaming Folders or Managed Products 7-40
Moving Folders or Managed Products 7-41
Deleting User-Defined Folders 7-41
Activating and Registering Managed Products 7-43
Activating Managed Products 7-43
Renewing Managed Product Licenses 7-45
Activating Control Manager 7-47

Renewing Control Manager or Managed Service Maintenance 7-49
Managing Child Servers 7-50
Understanding the Parent Server and Child Server Communication 7-52
Registering or Unregistering Child Servers 7-53
Unregistering a Child Server 7-55
Accessing the Cascading Folder 7-56
Viewing the Product Directory Status Summaries 7-57
Configuring Log Upload Settings 7-57
Enabling or Disabling Child Server Connection 7-58
Issuing Tasks to Child Servers 7-59
Viewing Child Server Reports 7-60
Refreshing the Product Directory 7-61
Renaming a Child Server 7-61
Recovering Child Servers Accidentally Removed from the Cascading Manager 7-62
Registering a Child Control Manager Server to a Parent Control Mananger Server 7-62
Understanding the Control Manager Database 7-64
Understanding the db_ControlManager Tables 7-64
Backing Up db_ControlManager Using osql 7-68
Restoring Backup db_ControlManager Using osql 7-69
Backing Up db_ControlManager Using the SQL Server Enterprise Manager 7-70
Restoring Backup db_ControlManager Using SQL Server Enterprise Manager 7-71
Shrinking db_controlmanager_log.ldf Using SQL Server Enterprise Manager 7-72
Shrinking db_ControlManager.mdf and db_ControlManager.ldf Using SQL Commands 7-73

Chapter 8: Using Trend Micro Services

Understanding Trend Micro Services 8-2
Understanding Enterprise Protection Strategy 8-3
Highlighting the Value of EPS 8-4
Introducing TrendLabs Message Board 8-5

Participating in the World Virus Tracking Program 8-5
Introducing Outbreak Prevention Services 8-6
Understanding Outbreak Prevention Services 8-6
Benefits of Outbreak Prevention Services 8-7
Activating Outbreak Prevention Services 8-7
Viewing Outbreak Prevention Services Status 8-8
Preventing Virus Outbreaks and Understanding the
Outbreak Prevention Mode 8-9
Understanding Outbreak Prevention Policies 8-10
Accessing the Outbreak Prevention Services
Settings Screen 8-10
Updating Outbreak Prevention Policies 8-11
Starting Outbreak Prevention Mode 8-12
Editing an Outbreak Prevention Policy 8-13
Setting Automatic Outbreak Prevention Mode 8-14
Configuring Outbreak Prevention Mode
Download Settings 8-16
Stopping Outbreak Prevention Mode 8-16
Viewing Outbreak Prevention Mode History 8-17
Using Outbreak Prevention Mode 8-18
Outbreak Prevention Mode Introduction 8-18
Step 1: Identifying the Source of the Outbreak 8-18
Step 2: Evaluating Existing Policies 8-19
Step 3: Starting Outbreak Prevention Mode 8-20
Step 4: Follow-Up Procedures 8-22

Chapter 9: Using Control Manager Tools

Using Agent Migration Tool (AgentMigrateTool.exe) 9-2
Using the Control Manager MIB File 9-2
Using the NVW 1.x SNMPv2 MIB File 9-3
Using the NVW Enforcer SNMPv2 MIB File 9-3
Using the NVW System Log Viewer 9-4
Using the NVW 1.x Rescue Utility 9-4
Using the Appliance Firmware Flash Utility 9-4
Using the DBConfig Tool 9-5

Chapter 10: Removing Trend Micro Control Manager

Removing a Control Manager Server 10-2
Manually Removing Control Manager 10-2
Remove the Control Manager Application 10-3
Stopping Control Manager Services 10-3
Removing Control Manager IIS Settings 10-4
Removing Crystal Reports, TMI, and CCGI 10-5
Deleting Control Manager Files/Directories and Registry Keys 10-6
Removing the Database Components 10-7
Removing Control Manager and NTP Services 10-7
Removing a Windows-Based Control Manager 2.x Agent 10-7

Chapter 11: Getting Support

Before Contacting Technical Support 11-2
Contacting Technical Support 11-2
TrendLabs 11-3
Other Useful Resources 11-3

Appendix A:

Server Address Checklist A-2
Ports Checklist A-3
Control Manager 2.x Agent installation Checklist A-4
Control Manager Conventions A-4
Core Process and Configuration Files A-5
Communication and Listening Ports A-7
Trend Micro Control Manager Product Features A-8

Appendix B:

Product Information B-2
Security Threat Information B-2
Data Views: Product Information B-3
License Information B-3
Managed Product License Status B-3
Managed Product License Information Summary B-5
Detailed Managed Product License Information B-6
Managed Product Information B-7

Managed Product Distribution Summary B-7
Managed Product Status Information B-8
ServerProtect and OfficeScan Server/Domain
Status Summary B-9
Managed Product Event Information B-10
Component Information B-11
Managed Product Scan Engine Status B-11
Managed Product Pattern File/Rule Status B-13
Managed Product Component Deployment B-14
Scan Engine Status Summary B-15
Pattern File/Rule Status Summary B-16
Control Manager Information B-16
User Access Information B-16
Control Manager Event Information B-17
Command Tracking Information B-18
Detailed Command Tracking Information B-19
Data View: Security Threat Information B-19
Virus/Malware Information B-20
Summary Information B-20
Detailed Information B-26
Spyware/Grayware Information B-34
Summary Information B-34
Detailed Information B-39
Content Violation Information B-48
Summary Information B-48
Detailed Information B-51
Spam Violation Information B-53
Summary Information B-53
Detailed Information B-55
Policy/Rule Violation Information B-57
Detailed Information B-57
Web Violation/Reputation Information B-63
Summary Information B-63
Detailed Information B-68
Suspicious Threat Information B-71
Summary Information B-71
Detailed Information B-80

Overall Threat Information B-83
Complete Network Security Risk Analysis Information B-83
Network Protection Boundary Information B-84
Security Risk Entry Point Analysis Information B-85
Security Risk Destination Analysis Information B-87
Security Risk Source Analysis Information B-87

Index

Preface

Preface

This Administrator's Guide introduces Trend Micro Control Manager™ 5.0, guides you through the installation planning and steps, 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 P-ii
- *Control Manager Documentation* on page P-vi
- *About this Administrator's Guide* on page P-vii
- *Audience* on page P-viii
- *Document Conventions* on page P-ix

What's New in This Version

Trend Micro Control Manager 5.0 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.

The following new features are available in version 5.0:

- *Improved Reporting and Logs* on page P-ii
- *Improved User Access Control* on page P-ii
- *Improved Product Directory Management and Monitoring* on page P-iii
- *Intelligent Component Monitoring* on page P-iii
- *Product License Deployment Support* on page P-iii

Improved Reporting and Logs

Control Manager 5.0 provides an Ad Hoc Query feature, allowing users to query managed product or Control Manager information from the Control Manager database through data views.

Users can now create their own report templates. Using drag-and-drop functionality for columns, rows, bars, and pie graphs makes creating your templates quick, efficient, and easy.

Improved User Access Control

Control Manager 5.0 provides improved user access control through the following ways:

- Customized account types allow Control Manager administrators to specify which menu items users can access from the Control Manager Web console.

  Example: The Control Manager administrator creates an account type that allows users to access only the product tree and the logs and reports section of the Web console. No other areas of the Control Manager Web console will display for users with that account type.

- Customized user accounts allow administrators to specify which products/directories a user can access, as well as specifying what actions the user can perform on products/directories to which the user has access.

  Example: Bob and Jane are both OfficeScan administrators. Both have identical account type permissions (they have access to the same menu items in the Web console). However, Jane oversees operation for all OfficeScan servers, while Bob on the other hand only oversees operation 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 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.

Improved Product Directory Management and Monitoring

Control Manager 5.0 provides improved product management and monitoring through the Product Directory. The improvements are as follows:

- OfficeScan-like view for products with multiple clients
- Parent Control Manager servers can now manage products that are controlled by their child Control Manager servers.
- Supports searching for managed products or managed product clients by name
- When moving managed products in the product tree, access rights can be maintained from the product's previous location

Intelligent Component Monitoring

Control Manager 5.0 displays only the components for managed products a user has access rights to and which are registered to Control Manager. Previous Control Manager versions displayed all components for all products.

Product License Deployment Support

Control Manager now supports the deployment and re-deployment of Activation Codes to managed products. Control Manager license management supports the following:

- Managed products can register their Activation Code (AC) to Control Manager
- Control Manager administrators can view the status of all ACs of registered managed products or ACs that other users input. They also can see which managed products use the AC.
- Control Manager administrators can add new ACs and deploy the ACs to selected managed products.

- Control Manager administrators can select an existing AC and deploy the AC to selected managed products.
- Control Manager administrators can renew ACs and then deploy them to related managed products that have used the AC.
- Control Manager administrators can delete ACs when the AC is not used by any managed products or in the process of deploying the AC.

Log Aggregation Support

Control Manager supports sending a log aggregation command to managed products. Managed products drop information you deem unnecessary and send the aggregated log to Control Manager.

Increased Managed Product Support

Control Manager has expanded support to the following Trend Micro managed products:

TABLE PREFACE-1. Managed Product Support

MANAGED PRODUCT NAME	VERSION
OfficeScan	8.0
ScanMail for Microsoft Exchange	8.0
PortalProtect for Sharepoint	Supported on 2007 and x64 OS
ScanMail for Lotus Domino	OS/AS 400 support
ServerProtect for Linux	3.0
ServerProtect for Microsoft Windows/Novell NetWare	X64 OS
InterScan Gateway Security Appliance	• 1.5 • 1.5 + SP1
InterScan Messaging Security Suite	• 7.0 • 7.0 + SP1
InterScan Web Security Appliance	3.0
InterScan Web Security Suite	3.0

TABLE PREFACE-1. Managed Product Support

MANAGED PRODUCT NAME	VERSION
InterScan WebProtect for ISA	• 5.0 • 5.01
Network VirusWall Enforcer 2500	2.0
Network VirusWall Enforcer 1200	2.0
InterScan Messaging Security Appliance 5000	• 1.0 • 7.0
Total Discovery Appliance	• 1.0 • 2.0 (under development)
ServerProtect for Linux	2.5

Control Manager Documentation

The Trend Micro Control Manager™ documentation consists of the following:

TABLE PREFACE-2. Control Manager Documentation

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Control Manager management 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 Web site: *http://esupport.trendmicro.com/support*
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, installation tips, known issues, and product release history.
Installation Guide	Printed documentation provided in the package contents and PDF form that is accessible from the Trend Micro Enterprise DVD or downloadable from the Trend Micro Web site. The Installation Guide contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running".
Administrator’s Guide	PDF documentation that is accessible from the Trend Micro Solutions CD for Control Manager or downloadable from the Trend Micro Web site. 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. See *About this Administrator’s Guide* for a summary of the chapters available in this book.
Tutorial	PDF documentation that is accessible from the Trend Micro Solutions CD for Control Manager or downloadable from the Trend Micro Web site. The Tutorial contains hands on instructions of how to deploy, install, configure, and manage Control Manager and managed products registered to Control Manager.

Note: Trend Micro recommends checking the Update Center at *http://www.trendmicro.com/download/* for updates to the Control Manager™ documentation and program file.

About this Administrator's Guide

The Trend Micro Control Manager™ Administrator's Guide provides the following information:

TABLE PREFACE-3. Administrator's Guide High-Level Overview

TASK	DESCRIPTION
Pre-Installation	*Chapter 1: Introducing Trend Micro Control Manager™*: Provides an overview of Control Manager product architecture, and a description of all features
	Chapter 2: Planning and Implementing the Control Manager Deployment: Provides deployment and product application information and Trend Micro recommendations on the optimal deployment of Control Manager
Installation	*Chapter 3: Installing Trend Micro Control Manager for the First Time*: Provides first-time installation procedures for Control Manager
	Chapter 4: Upgrading Servers or Migrating Agents to Control Manager 5.0: Provides information and procedures for upgrading to Control Manager from previous versions

TABLE PREFACE-3. Administrator’s Guide High-Level Overview

TASK	DESCRIPTION
Post Installation	*Chapter 5: Getting Started with Control Manager*: Provides information on basic Web console navigation, creating and importing users, updating the server and managed products
	Chapter 6: Monitoring the Control Manager Network: Provides information on interpreting and monitoring the Control Manager environment, such as, configuring notifications, generating reports, and collecting logs
	Chapter 7: Administering Managed Products: Provides information on managing the Control Manager network and managed products
	Chapter 8: Using Trend Micro Services: Provides information on using Control Manager services, such as, EPS and OPS
	Chapter 9: Using Control Manager Tools: Provides information on using Control Manager tools, such as, Agent Migration tool and Cascading Management Structure Tool
	Chapter 10: Removing Trend Micro Control Manager: Provides information on removing Control Manager from your computer
	Chapter 11: Getting Support: Provides information about contacting Trend Micro if you have questions or need support
Appendices	• *Appendix A: System Checklists*: Provides printable checklists for numerous Control Manager tasks • *Appendix B: Understanding Data Views*: Provides a description of the data columns used in Ad Hoc Queries and report templates

Audience

The Control Manager 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.

Document Conventions

To help you locate and interpret information easily, the Control Manager documentation (Administrator's and Installation Guide) uses the following conventions.

TABLE PREFACE-4. 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
Tip:	Provides best practice information and Trend Micro recommendations
WARNING!	Provides warnings about processes that may harm your network

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

This chapter contains the following topics:

- *Control Manager Standard and Advanced* on page 1-2
- *How to Use Control Manager* on page 1-2
- *Understanding Trend Micro Management Communication Protocol* on page 1-3
- *Control Manager Architecture* on page 1-7

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 5.0 Advanced supports the following as child Control Manager servers:

- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition
- Control Manager 3.0 SP6 Standard or Enterprise Edition

Control Manager 5.0 Standard servers cannot be child servers.

For a complete list of all features Standard and Advanced Control Manager servers support see *Trend Micro Control Manager Product Features* on page A-8.

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 This helps 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

TABLE 1-1. Control Manager Features

FEATURE	DESCRIPTION
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 management console access and component download
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager management 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 management console to the managed products. System administrators can run manual scans from the management console. This command system is indispensable during a virus/malware outbreak.
Centralized update control	Update virus patterns, anti-spam 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 Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with managed products. MCP has several new 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. The 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 re-connection 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, "Control Manager Components," on page 1-7 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 **management console** • A **mail server** that delivers event **notifications** through email messages Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure **Event Center** to send notifications through email messages, Windows event log, MSN Messenger, SNMP, Syslog, pager, or any in-house/industry standard application used by your organization to send notification. • A **report server**, *present only in the Advanced Edition*, that generates antivirus and content security product reports A Control Manager report is an online collection of figures about virus/malware and content security events that occur on the Control Manager network.

TABLE 1-2. Control Manager Components

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 uses one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.
Trend Micro Infrastructure	Handles the Control Manager server interaction with older managed products The Communicator, or the Message Routing Framework, is the communication backbone of the Control Manager system. It is a component of the Trend Micro 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 to 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. Hence, install agents on the same computer as managed products.
Web-based management console	Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™ The Control Manager management console is a Web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible Web browser.

Chapter 2

Planning and Implementing the Control Manager Deployment

Administrators must take several factors into consideration before deploying Control Manager to their network. This chapter helps you plan for Control Manager deployment and manage a Control Manager test deployment.

This chapter contains the following topics:

- *Identifying Deployment Architecture and Strategy* on page 2-2
- *Installation Flow* on page 2-9
- *Supported Operating Systems* on page 2-9
- *Testing Control Manager at One Location* on page 2-10
- *Server Distribution Plan* on page 2-12
- *Network Traffic Plan* on page 2-13
- *Sources of Network Traffic* on page 2-15
- *Deploying Updates* on page 2-18
- *Data Storage Plan* on page 2-19
- *Web Server Plan* on page 2-20

Identifying Deployment Architecture and Strategy

Deployment is the process of strategically distributing Control Manager servers to your network environment to facilitate and provide optimal management of antivirus and content security products.

Deploying enterprise-wide, client-server software like Control Manager to a homogenous or heterogeneous environment requires careful planning and assessment.

For ease of planning, Trend Micro recommends two deployment architectures:

- **Single-site deployment:** Single-site deployment refers to distributing and managing child servers and managed products from a single Control Manager located in a central office. If your organization has several offices but has fast and reliable local and wide area connection between sites, single-site deployment still applies to your environment.
- **Multiple-site deployment:** Multiple-site deployment refers to distributing and managing Control Manager servers in an organization that has main offices in different geographical locations.

Note: If you are using Control Manager for the first time, Trend Micro recommends the use of a Control Manager Advanced parent server to handle single-site and multiple-site deployments.

Understanding Single-Site Deployment

Single-site deployment refers to distributing and managing child servers and managed products from a single Control Manager located in a central office.

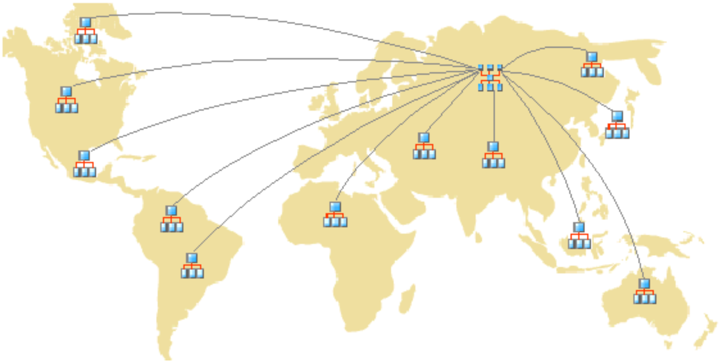


FIGURE 2-1. A single-server deployment using Control Manager Advanced parent server and mixed child servers

Before deploying Control Manager to a single-site, complete the following tasks:

- Determine the number of managed products and cascading structures
- Plan for an optimal server-managed products/cascading structure ratio
- Designate the Control Manager Standard server or Control Manager Advanced server

---

Note: Control Manager 5.0 Advanced supports the following as child Control Manager servers:

- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition
- Control Manager 3.0 SP6 Standard or Enterprise Edition

Control Manager 5.0 Standard servers cannot be child servers.

Determining the Number of Managed Products and Cascading Structures

Determine how many managed products and cascading structures you plan to manage with Control Manager. You will need this information to decide what kind and how many Control Manager servers you need to deploy, as well as where to put these servers on your network to optimize communication and management.

If you have a heterogeneous network environment (that is, if your network has different operating systems, such as Windows and UNIX), identify how many managed products are Windows or UNIX-based. Use this information to decide whether to implement a Control Manager cascading structure environment.

Planning for an Optimal Server-managed Products/Cascading Structure Ratio

The most critical factor in determining how many managed products or cascading structures a single Control Manager server can manage on a local network is the agent-server communication or parent and child server communication.

Use the recommended system requirements as a guide in determining the CPU and RAM requirements for your Control Manager network.

Designating Control Manager Servers

Based on the number of managed products and cascading structure requirements, decide and designate your Control Manager server. Decide whether to designate an Advanced or Standard server.

Locate your Windows servers, and then select the ones to assign as Control Manager servers. You also need to determine if you need to install a dedicated server.

When selecting a server that will host Control Manager, consider the following:

- The amount of CPU load
- Other functions the server performs

If you are installing Control Manager on a server that has other uses (for example, application server), Trend Micro recommends that you install on a server that is not running mission-critical or resource-intensive applications.

Note: Both OfficeScan and Control Manager use IIS to communicate with clients and agents/child servers, respectively. There is no conflict between these two applications, but since both of them are using IIS resources, Trend Micro recommends installing Control Manager on another computer to reduce the performance stress on the server.

Depending on your network topology, you may need to perform additional site-specific tasks.

Understanding Multiple-Site Deployment

As with single-site deployment, collect relevant network information and identify how this information relates to deploying Control Manager to your multiple sites.

Given the uniqueness of each network, exercise judgment as to how many Control Manager servers would be optimal.

Deploy Control Manager servers in a number of different locations, including the demilitarized zone (DMZ) or the private network. Position the Control Manager server in the DMZ on the public network to administer managed product or child servers and access the Control Manager management console using Internet Explorer over the Internet.

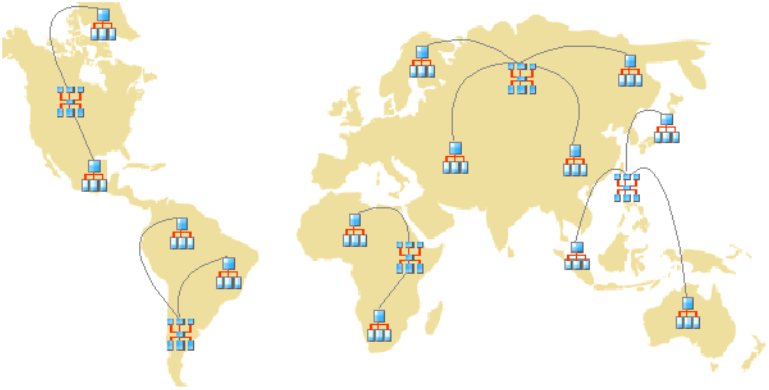


FIGURE 2-2. A multi-site deployment using multiple Control Manager Advanced parent servers and mixed child servers

Consider the following for multi-site deployment:

- Group managed products or child servers
- Determine the number of sites

- Determine the number of managed products and child servers
- Plan for network traffic
- Plan for an optimal server-managed products/cascading structure ratio
- Decide where to install the Control Manager server

Grouping Managed Products or Child Servers

Consider the following when you group managed products and child servers:

TABLE 2-1. Considerations Grouping Managed Products or Child Servers

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

Determining the Number of Sites

Determine how many sites your Control Manager deployment will cover. You need this information to determine the number of servers to install, as well as where to install the servers.

Gather this information from your organization's WAN or LAN topology charts.

Determining the Number of Managed Products and Child Servers

You also need to know the total number of managed products and child servers Control Manager server will manage. Trend Micro recommends gathering managed product and child server population data per site. If you cannot get this information, even rough estimates will be helpful. You will need this information to determine how many servers you need to install.

Planning for Network Traffic

Control Manager generates network traffic when the server and managed products/child servers communicate. Plan the Control Manager network traffic to minimize the impact on an organization's network.

These are the sources of Control Manager-related network traffic:

- Heartbeat
- Logs
- Communicator schedule
- Managed product registration to Control Manager server

  Control Manager servers, by default, contain all the product profiles available during the Control Manager release. However, if you register a new version of a product to Control Manager, a version that does not correspond to any existing product profiles, the new product will upload its profile to the Control Manager server.
- Child server registration to Control Manager parent server
- Downloading and deploying updates

Planning for an Optimal Server-managed Products/Cascading Structure Ratio

When deploying Control Manager across the WAN, the Control Manager server in the main office administers child servers and managed products in the remote office. If you will have managed products or child servers in the remote office reporting to the server in the main office over the WAN, you need to consider the diversity of the network bandwidth in your WAN environment. Having different network bandwidth in your WAN environment can be beneficial to Control Manager. If you have managed products or child servers both on the LAN and across the WAN reporting to the same server, reporting is staggered naturally; the server prioritizes those with the faster connection, which, in almost all cases, are the managed products or child servers on the LAN.

Use the recommended system requirements as a guide in determining the CPU and RAM requirements for your Control Manager network.

Designating Control Manager Servers

Based on the number of managed products and cascading structure requirements, decide and designate your Control Manager server.

Locate your Windows servers, and then select the ones to assign as Control Manager servers. You also need to determine if you need to install a dedicated server.

When selecting a server that will host Control Manager, consider the following:

- The amount of CPU load
- Other functions the server performs

If you are installing Control Manager on a server that has other uses (for example, application server), Trend Micro recommends installing on a server that does not run mission-critical or resource-intensive applications.

Note: Both OfficeScan and Control Manager use IIS to communicate with clients and agents/child servers, respectively. There is no conflict between these two applications, but since both of them are using IIS resources, Trend Micro recommends installing Control Manager on another computer to reduce the performance stress on the server.

Deciding Where to Install the Control Manager Server

Once you know the number of clients and the number of servers you need to install, find out where to install your Control Manager servers. Decide if you need to install all your servers in the central office or if you need to install some of them in remote offices.

Place the servers strategically in certain segments of your environment to speed up communication and optimize managed product and child server management:

- **Central office:** A central office is the facility where majority of the managed products and child servers in the organization are located. The central office is sometimes referred to as *headquarters*, *corporate office*, or *corporate headquarters*. A central office can have other smaller offices or branches (referred to as 'remote offices' in this guide) in other locations.

Tip: Trend Micro recommends installing a parent server in the central office.

- **Remote office:** A remote office is defined as any small professional office that is part of a larger organization and has a WAN connection to the central office. If you have managed products and child servers in a remote office that report to the server in the central office, they may encounter difficulties connecting to the server. Bandwidth limitations may prevent proper communication to and from the Control Manager server.

  The network bandwidth between your central office and remote office may be sufficient for routine client-server communication, such as notifications for updated configuration settings and status reporting, but insufficient for deployment and other tasks.

Installation Flow

Setting up your Control Manager system is a multi-step process that involves the following:

Step 1: Planning the Control Manager system installation (server distribution, network traffic, data storage, and Web server considerations).

Step 2: Installing the Control Manager server. During installation of the Control Manager server, provide a location for backup and restoration files.

Step 3: Installing Control Manager agents.

Supported Operating Systems

The following operating systems support the Control Manager server and agent installation:

Control Manager Server

- Windows 2000 Server SP 3/SP 4
- Windows 2000 Advance Server SP 3/SP 4
- Windows 2003 Server Standard Edition SP 1/SP 2
- Windows 2003 Server Standard Edition R2 without patches/SP 1
- Windows 2003 Server Enterprise Edition SP 1/SP 2
- Windows 2003 Server Enterprise Edition R2 without patches/SP 1

- WOW, 64 bit architecture of Windows 2003 Standard/Enterprise

Older Control Manager Agents

TABLE 2-2. Older Control Manager Agents Supported Operating Systems

MICROSOFT	OTHERS
• Windows XP Professional Version • Windows 2000 Server • Windows 2000 Advanced Server • Windows NT 4.0 + SP3 • Windows NT 4.0 + SP6a or later • Windows 2003, Standard Edition, Enterprise Edition	• Novell Desktop 9 • AIX • Red Hat Linux 6.2, 7.1, 7.2 • RedHat Enterprise Linux 4.3 • Turbolinux 6.5, 7.0 • SuSE Linux 6.3, 7.2, 7.3 • SuSE Enterprise 9.2 • AS/400 • OS390 • Others: GateLock, Linux 6.x kernel, Solaris 2.6, 2.7, 2.8, Debian 3.1 4

Testing Control Manager at One Location

A pilot deployment provides an opportunity for feedback to determine how features work and the level of support likely needed after full deployment.

Tip: Trend Micro recommends conducting a pilot deployment before performing a full-scale deployment.

Piloting Control Manager at one location allows you to accomplish the following:

- Gain familiarity with Control Manager and managed products
- Develop or refine the company's network policies

A pilot deployment is useful to determine which configurations need improvements. It gives the IT department or installation team a chance to rehearse and refine the deployment process and test if your deployment plan meets your organization's business requirements.

A Control Manager test deployment consists of the following tasks:

Preparing for the Test Deployment

Complete the following activities during the preparation stage:

Step 1: Decide the Control Manager server and agent configuration for the test environment.

- Establish TCP/IP connectivity among all systems in a heterogeneous trial configuration.
- Verify bidirectional TCP/IP communications by sending a ping command to each agent system from the manager system and vice versa.

Step 2: Evaluate the different deployment methods to see which ones are suitable for your particular environment.

Step 3: Complete a System Checklist used for the pilot deployment.

Selecting a Test Site

Select a pilot site that best matches your production environment. Try to simulate, as closely as possible, the type of topology that would serve as an adequate representation of your production environment.

Creating a Rollback Plan

Create a disaster recovery or rollback plan (for example, how to roll back to Control Manager 3.0/3.5) in case there are some difficulties with the installation or upgrade. This process should take into account local corporate policies, as well as IT resources.

Beginning the Test Deployment

After completing the preparation steps and System Checklist, begin the pilot deployment by installing Control Manager server and agents.

Evaluating the Test Deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential *pitfalls* and plan accordingly for a successful deployment.

You can implement the pilot evaluation plan into the overall production installation and deployment plan.

Server Distribution Plan

Understanding Administration Models

Early in the Control Manager deployment, determine exactly how many people you want to grant access to your Control Manager server. The number of users depends on how centralized you want your management to be. The guiding principle being: the degree of centralization is inversely proportional to the number of users.

Follow one of these administration models:

- **Centralized management:** This model gives Control Manager access to as few people as possible. A highly centralized network would have only one administrator, who then manages all the antivirus and content security servers on the network.

  Centralized management offers the tightest control over your network antivirus and content security policy. However, as network complexity increases, the administrative burden may become too much for one administrator.

- **Decentralized management:** This is appropriate for large networks where system administrators have clearly defined and established areas of responsibility. For example, the mail server administrator may also be responsible for email protection; regional offices may be independently responsible for their local areas.

  A main Control Manager administrator would still be necessary, but he or she shares the responsibility for overseeing the network with other product or regional administrators.

  Grant Control Manager access to each administrator, but limit access rights to view and/or configure segments of the Control Manager network that are under their responsibility.

With one of these administration models initialized, you can then configure the Product Directory and necessary user accounts to manage your Control Manager network.

Understanding Control Manager Server Distribution

Control Manager can manage products regardless of physical location and so it is possible to manage all your antivirus and content security products using a single Control Manager server.

However, there are advantages to dividing control of your Control Manager network among different servers (including parent and child servers for Advanced Edition users). Based on the uniqueness of your network, you can decide the optimum number of Control Manager servers.

Single-Server Topology

The single-server topology is suitable for small to medium, single-site enterprises. It facilitates administration by a single administrator, but does not preclude the creation of additional administrator accounts as required by your Administration plan.

However, this arrangement concentrates the burden of network traffic (agent polling, data transfer, update deployment, and so on) on a single server, and the LAN that hosts it. As your network grows, the impact on performance also increases.

Multiple-Server Topology

For larger enterprises with multiple sites, it may be necessary to set up regional Control Manager servers to divide the network load.

For information on the traffic that a Control Manager network generates, see *Understanding Control Manager Network Traffic* on page 2-13.

Network Traffic Plan

To develop a plan to minimize the impact of Control Manager on your network, it is important to understand the Control Manager network generated traffic.

The following section helps you understand the traffic that your Control Manager network generates and develop a plan to minimize its impact on your network. In addition, the section about traffic frequency describes which sources frequently generate traffic on a Control Manager network.

Understanding Control Manager Network Traffic

To develop a plan to minimize the impact of Control Manager on your network, it is important to understand Control Manager network generated traffic.

Sources of Network Traffic

The following Control Manager sources generate network traffic:

- Log traffic
- Trend Micro Management Infrastructure and MCP policies
- Product registration
- Downloading and deploying updates

Traffic Frequency

The following sources frequently generate traffic on a Control Manager network:

- Logs
- MCP polling and commands
- Trend Micro Management Infrastructure policies

Logs

Managed products send logs to Control Manager at different intervals – depending on their individual log settings.

Managed Product Agent Heartbeat

By default,managed product agents send heartbeat messages every sixty minutes. Administrators can adjust this value from 5 to 480 minutes (8 hours). When choosing a heartbeat setting, choose a balance between the need to display the latest Communicator status information and the need to manage system resources.

The default setting will be satisfactory for most situations, however should you feel the need to customize these settings, familiarize yourself with the following considerations:

- **Long-interval Heartbeats (above 60 minutes):** the longer the interval between heartbeats, the greater the number of events that may occur before the Control Manager console displays it

  For example, if a connection problem with an agent is resolved between heartbeats, it then becomes possible to communicate with an agent even if its 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 increases the amount of network bandwidth used.

Note: Before adjusting the interval to a number below 15 minutes, study your existing network traffic to understand the impact of increased use of network bandwidth.

Network Protocols

Control Manager uses the UDP and TCP protocols for communication.

Sources of Network Traffic

Log Traffic

Constant sources of network traffic in a Control Manager network are ‘product logs’, logs that managed products regularly send to the Control Manager server.

TABLE 2-3. Control Manager Log Traffic

LOG	CONTAINS INFORMATION ABOUT
Virus/Spyware/Grayware	Detected virus/malware, spyware/grayware, and other security threats.
Security	Violations reported by content security products.
Web Security	Violations reported by Web security products.
Event	Miscellaneous events (for example, component updates, and generic security violations).
Status	The environment of a managed product. The Status tab of the Product Directory displays this information.
Network Virus	Viruses detected in network packets.
Performance Metric	Used for previous product versions.
URL Usage	Violations reported by Web security products

TABLE 2-3. Control Manager Log Traffic

LOG	CONTAINS INFORMATION ABOUT
Security Violation	Violations reported by Network VirusWall products
Security Compliance	Client compliances reported by Network VirusWall products
Security Statistic	The difference between security compliances and security violations calculated and reported by Network VirusWall products
Endpoint	Violations reported by Web security products

Trend Micro Management Communication Protocol Policies

The Trend Micro Management Communication Protocol (MCP) is the latest part of the communications backbone of Control Manager. MCP implements the following policies:

MCP Heartbeat: The MCP heartbeats to Control Manager ensure that Control Manager displays the latest information, and that the connection between the managed product and the Control Manager server is functional.

MCP Command Polling: When an MCP agent initiates a command poll to Control Manager, Control Manager notifies the agent to send managed product logs or issues a command to the managed product. Control Manager also interprets a command poll as a passive heartbeat verifying the connection between Control Manager and the managed product.

Trend Micro Management Infrastructure Policies

The Trend Micro Management Infrastructure (TMI) is part of the communications backbone of Control Manager and generates its own 'housekeeping' traffic. TMI implements two policies:

- **Communicator Heartbeat:** The Communicator, the message routing framework of TMI, polls the Control Manager server at regular intervals. This ensures that the Control Manager console displays the latest information, and that the connection between the managed product and the Control Manager server is functional.

- **Work-hour policy:** The work-hour policy defines when a Communicator sends information to the Control Manager server. Use the Communication Scheduler to define this policy; a user can set three periods of inactivity – also called 'off-hour' periods. There are two types of information, however, that do not follow the Communicator Scheduler:

  - Emergency messages
  - Prohibited messages

  TMI sends emergency messages to the Control Manager server – even when the Communicator is in an off-hour period. However, TMI never sends prohibited messages to Control Manager – even when the Communicator is active.

Product Registration Traffic

Product profiles provide Control Manager with information about how to manage a particular product. Managed products upload profiles to the Control Manager server the first time they register with the server.

Each product has a corresponding product profile, and in many cases, different versions of a product have their own version specific profile. Profiles contain the following information:

- Category (for example, antivirus)
- Product name
- Product version
- Menu version
- Log format
- Update component information– updates that the product supports (for example, virus pattern files)
- Command information

By default, Control Manager servers contain all the product profiles that were available when the managed products released. However, when a new version of a product registers with Control Manager, the new product uploads its new product profile to the Control Manager server.

Deploying Updates

Understanding Deployment Updates

Updating a Control Manager network is a two-step process:

Step 1: Obtain the latest update components from Trend Micro. Control Manager can download components either directly from the Trend Micro update server, or from an alternative location.

Step 2: Deploy these components to the managed products.

Control Manager deploys update components to managed products, including:

- Pattern files/Cleanup templates
- Engines (scan engines, damage cleanup engines)
- Anti-spam rules
- Product programs (depending on the product)
- Network virus pattern files (Network VirusWall products only)

Note: Control Manager can only update damage cleanup templates/engines after activating Damage Cleanup Services.

Trend Micro strongly recommends regularly updating these components to help ensure managed products can protect your network against the latest threats. For product program updates, refer to the specific program’s documentation.

Deploying updates to managed products is a bandwidth intensive operation. If possible, it is important to perform deployments when it will have the least impact on the network.

You can stagger the deployment of component updates using Deployment Plans.

Furthermore, check that the network connection between your Control Manager server and managed products can accommodate the updates. This will be a factor to consider when deciding how many Control Manager servers your network needs.

Data Storage Plan

Control Manager data must be stored in an SQL database. If you install Control Manager on a server that does not have its own database, the installation program provides the option to install the Microsoft SQL Express. However, due to the limitations of SQL Express, large networks require an SQL server.

Note: Control Manager uses SQL and Windows authentication to access the SQL server.

Database Recommendations

If you install Control Manager and its SQL server on the same computer, configure the SQL server to use a fixed memory size equivalent to two-thirds of the total memory on the server. For example, if the server has 256MB of RAM, set 150MB as the fixed memory size for the SQL server.

Install the Control Manager SQL database on the Control Manager server itself, or on a separate server (for example, a dedicated SQL server). If Control Manager manages over 1,000 products, Trend Micro recommends using a dedicated SQL server.

Note: For instructions on how to manage SQL resources, and other sizing recommendations, refer to Microsoft SQL documentation.

ODBC Drivers

Control Manager uses an ODBC driver to communicate with the SQL server. For most instances, ODBC version 3.7 is sufficient. However, to use a Named Instance of SQL 2000, version 2000.80.194.00 is required.

The Control Manager setup program can verify the ODBC driver version if the SQL server is installed on the Control Manager computer. For remote SQL servers, verify the driver manually to ensure that Control Manager can access the database.

Authentication

Control Manager uses mixed-mode authentication for accessing the SQL database rather than Windows authentication.

Web Server Plan

Web Server Configuration

The Web server information screen in the Control Manager setup program presents similar server identification options as the host ID definition screen: host name, FQDN, or IP address. The decision considerations for the Web server name are the same:

- Using the host name or FQDN facilitates Control Manager server IP address changes, but makes the system dependent on the DNS server
- The IP address option requires a fixed IP

Use the Web server address to identify the source of component updates. The SystemConfiguration.xml file stores this information and sends it to agents as part of a notification for these agents to obtain updates from the Control Manager server. Update source related instructions appear as follows:

```
Value=http://<Web server
address>:<port>/TvcsDownload/ActiveUpdate/<component>
```

Where:

- **Port:** The port that connects to the update source. You can also specify this on the Web server address screen (default port number is 80)
- **TvcsDownload/ActiveUpdate:** The Control Manager setup program creates this virtual directory in the IIS specified Web site
- **Component:** This depends on the updated component. For example, when the virus pattern file is updated, the value added here is:

  Pattern/vsapi.zip

  Pattern corresponds to the \\. . . Control Manager\WebUI\download\activeupdate\pattern folder on the Control Manager server. *Vsapi.zip* is the virus pattern in compressed form.

Chapter 3

Installing Trend Micro Control Manager for the First Time

This chapter guides you through installing Control Manager server. In addition to listing the system requirements for the Control Manager server the chapter also contains post-installation configuration information as well as instructions on how to register and activate your software.

This chapter contains the following topics:

- *System Requirements* on page 3-2
- *Installing a Control Manager Server* on page 3-4
- *Verifying Successful Installations* on page 3-22
- *Post-installation Configuration* on page 3-24
- *Registering and Activating Your Software* on page 3-25

System Requirements

Individual company networks are as individual as the companies themselves. Therefore, different networks have different requirements depending on the level of complexity. This section describes both minimum system requirements and recommended system requirements, including general recommendations and recommendations based on the size of networks.

Minimum System Requirements

The following table lists the minimum system requirements for a Control Manager server.

Note: Control Manager 5.0 Advanced supports the following as child Control Manager servers:

- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition
- Control Manager 3.0 SP6 Standard or Enterprise Edition

Control Manager 5.0 Standard servers cannot be child servers.

Please refer to the managed product documentation for detailed agent system requirements.

TABLE 3-1. Control Manager server hardware minimum system requirements

HARDWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
CPU	Intel™ Pentium™ III 600MHz or higher • Single CPU • Dual CPU • Quad CPU
Memory	• 2GB RAM minimum • 4GB RAM recommended

TABLE 3-1. Control Manager server hardware minimum system requirements

HARDWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
Disk space	• 790MB for Control Manager Standard/Advanced Version • 300MB for SQL 2005 Express (Optional)

TABLE 3-2. Control Manager server software minimum system requirements

SOFTWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
Operating system	• Microsoft™ Windows™ 2000 Server SP 3/SP 4 • Windows 2000 Advanced Server SP 3/SP 4 • Windows 2003 Server Standard Edition SP 1/SP 2 • Windows 2003 Server Enterprise Edition SP 1/SP 2 • WOW, 64 bit architecture of Windows 2003 Standard/Enterprise • VMWare ESX 3.x
Web server	• Microsoft IIS server 5.0 (For 2000 platform) • Microsoft IIS server 6.0 (For 2003 platform)
Database	• Microsoft Data Engine (MSDE) 2000 + SP3 • Microsoft SQL Server 2000 (2000 + SP3 is recommended) • Microsoft SQL Express 2005
Others	• Microsoft .NET Framework 2.0 (included in Control Manager package) • Windows Installer 3.1 (included in the Control Manager package) • VC2005 Redistribution (included in Control Manager package) • MDAC 2.8 SP1 or above for SQL Express (not included in the Control Manager package)
Management console	• Browser- Windows Internet Explorer 6 or higher • Java VM- Microsoft Version 5.0.0.3805 or higher • JRE 1.4.2 or 1.5.0

Please refer to the URL below to download the latest Control Manager 2.x agents:

http://www.trendmicro.com/en/products/management/tmcm/evaluate/requirements.htm

Recommended System Requirements

Observe the following system requirements to obtain optimum Control Manager performance:

General Recommendations

- Do not install Control Manager on a Primary Domain Controller (PDC), a Backup Domain Controller (BDC), or on a server with any other Trend Micro product. This can result in severe performance degradation.
- Physical memory is a system resource – all applications on the server share it. Scale the memory with the processor; do not overpopulate with memory

TABLE 3-3. General Control Manager server recommendations

HARDWARE/SOFTWARE SPECIFICATION	RECOMMENDED REQUIREMENT
Network adapter	100Mbps, 32-bit, adapter for both the Control Manager server and managed product. Preferably one designed for bus mastering, direct memory access (DMA)
File system	NT File System (NTFS) partition
Monitor	VGA monitor capable of 1024 x 768 resolution, with at least 256 colors.

Installing a Control Manager Server

After deciding the topology to use for your network, you can begin to install your Control Manager server. See *Server Address Checklist* on page A-2 to help you record relevant information for installation.

You need the following information for the installation:

- Relevant target server address and port information

- Control Manager registration key
- Security Level you want to use for Server-Agent communication

The following are database-related considerations:

- Decide if you want to use an SQL server with Control Manager. If the SQL server is located on a server other than the Control Manager server, obtain its IP address, FQDN, or NetBIOS name. If there are multiple instances of the SQL server, identify the one that you intend to use
- Prepare the following information about the SQL database for Control Manager:
  - User name for the database
  - Password

Note: Control Manager uses both Windows authentrication and SQL authentrication to access the SQL server.

- Determine the number of managed products that Control Manager will handle. If an SQL server is not detected on your server, Control Manager will install SQL 2005 Express SP 2, which can only handle a limited number of connections

Installing Control Manager requires performing the following steps:

Step 1: Install all required components

Step 2: Specify the installation location

Step 3: Register and activate the product and services

Step 4: Specify Control Manager security and Web server settings

Step 5: Specify backup settings and configure database information

Step 6: Set up root account and configure notification settings

Tip: Trend Micro recommends upgrading to version 5.0 instead of doing a fresh installation.

To install a Control Manager server:

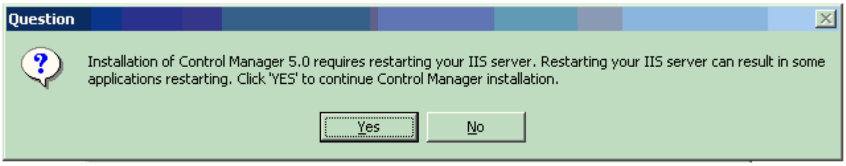
Step 1: Install all required components

1. On the Windows taskbar, click **Start** > **Run**, and then locate the Control Manager installation program (Setup.exe). If installing from the Trend Micro Enterprise DVD, go to the Control Manager folder on the DVD. If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your computer. The installation program checks your system for required components.

   If the installation program does not detect the following components on the server, dialog boxes appear prompting you to install the missing components:

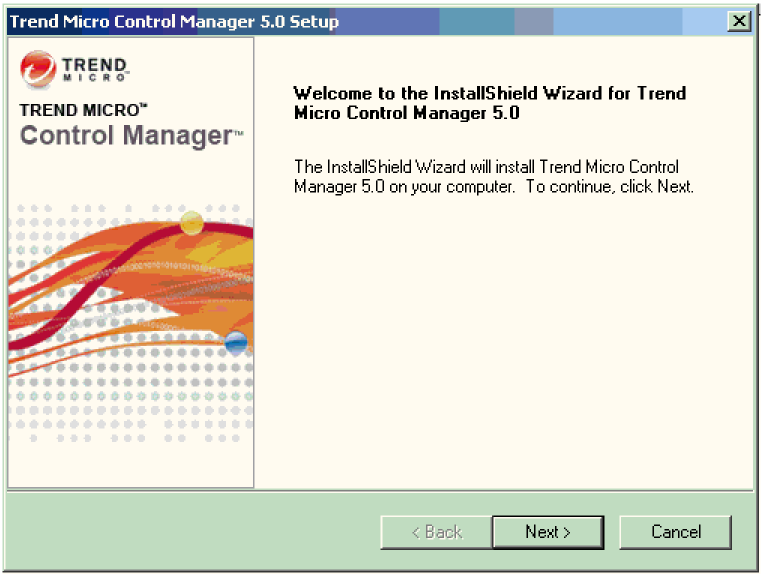
   - **Windows Installer 3.1:** This component is included in the Control Manager installation package
   - **MDAC 2.8 SP1 or higher:** This component is not included in the Control Manager installation package
   - **.Net Framework 2.0:** This component is included in the Control Manager installation package
   - **Visual C 2005 SP1 Redistribution Package:** This component is included in the Control Manager installation package

2. Install all missing components. The IIS confirmation dialog box appears.



Installation of Control Manager 5.0 requires restarting your IIS server. Restarting your IIS server can result in some applications restarting. Click 'YES' to continue Control Manager installation.

3. Click **Yes** to continue the installation. The Welcome screen appears.

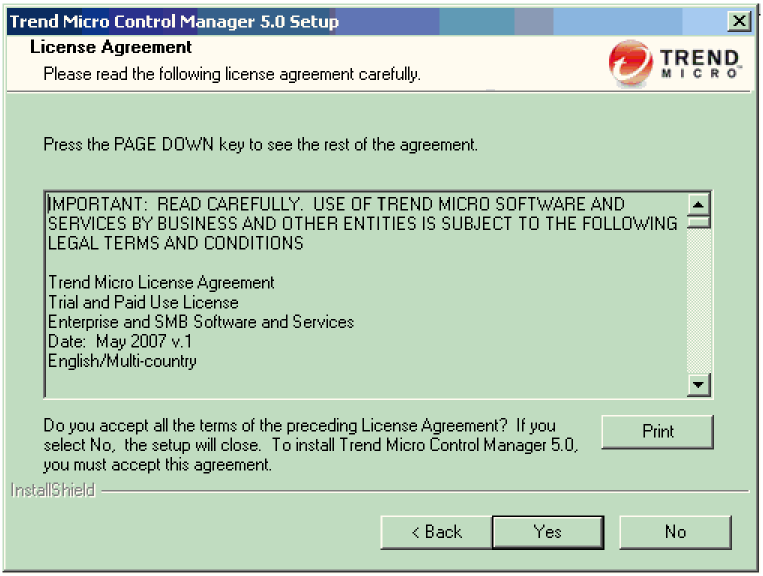


Welcome to the InstallShield Wizard for Trend Micro Control Manager 5.0

The InstallShield Wizard will install Trend Micro Control Manager 5.0 on your computer. To continue, click Next.

The installation program checks your system for existing components. Before proceeding with the installation, close all instances of the Microsoft Management Console. For more information about migration, see *Planning Control Manager Agent Migration* on page 4-11.

4. Click **Next**. The Software License Agreement appears.



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

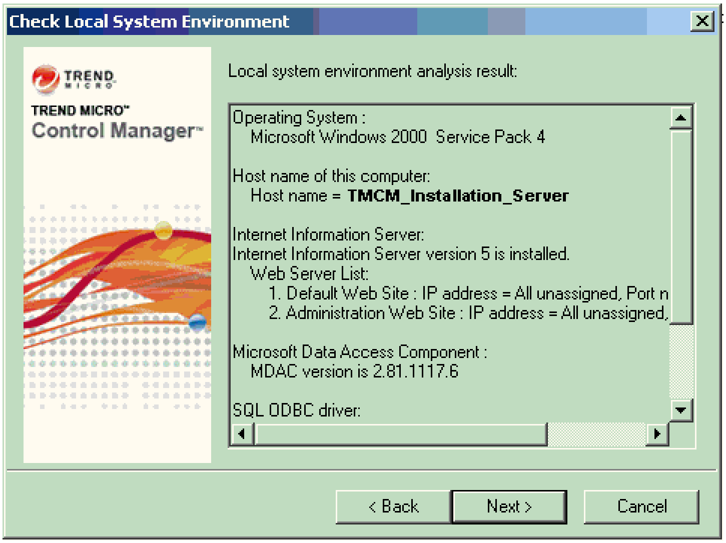
IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement
Trial and Paid Use License
Enterprise and SMB Software and Services
Date: May 2007 v.1
English/Multi-country

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Trend Micro Control Manager 5.0, you must accept this agreement.

FIGURE 3-1. Choose Yes to agree with the License Agreement

If you do not agree with the terms of the license, click **No**; the installation will discontinue. Otherwise, click **Yes**. A summary of detected components appears.


Check Local System Environment

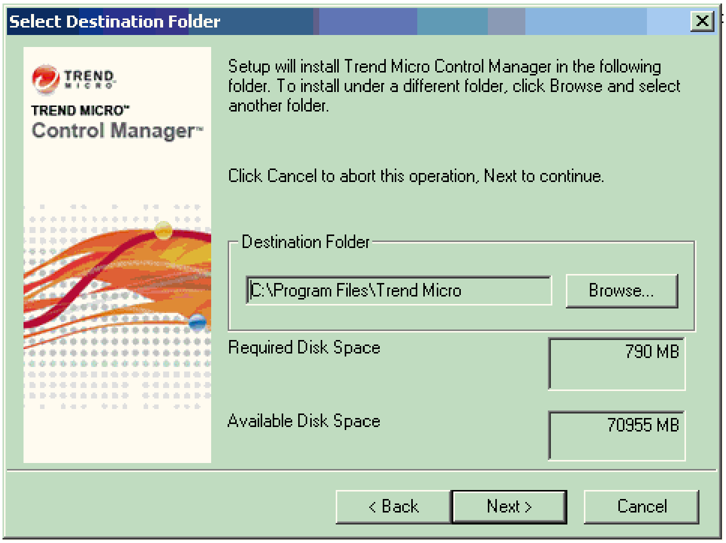
Local system environment analysis result:

```
Operating System :
   Microsoft Windows 2000  Service Pack 4

Host name of this computer:
   Host name = TMCM_Installation_Server

Internet Information Server:
Internet Information Server version 5 is installed.
   Web Server List:
      1. Default Web Site : IP address = All unassigned, Port n
      2. Administration Web Site : IP address = All unassigned,

Microsoft Data Access Component :
   MDAC version is 2.81.1117.6

SQL ODBC driver:
```

FIGURE 3-2. Displays local system environment information

Step 2: Specify the installation location

1. Click **Next**. The Select Destination Folder screen appears.



Select Destination Folder

Setup will install Trend Micro Control Manager in the following folder. To install under a different folder, click Browse and select another folder.

Click Cancel to abort this operation, Next to continue.

Destination Folder: C:\Program Files\Trend Micro

Required Disk Space: 790 MB

Available Disk Space: 70955 MB

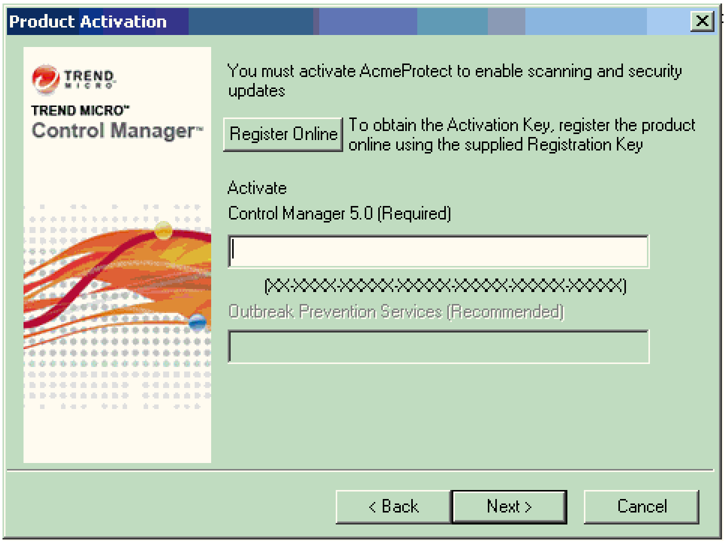
FIGURE 3-3. Select a destination folder

2. Specify a location for Control Manager files. The default location is `C:\Program Files\Trend Micro`. To change this location, click **Browse**, and then specify an alternate location.

Note: The setup program installs files related to the Control Manager communication, (the Trend Micro Management Infrastructure and MCP) in predetermined folders in the Program files folder.

Step 3: Register and activate the product and services

1. Click **Next**. The Product Activation screen appears.



You must activate AcmeProtect to enable scanning and security updates

To obtain the Activation Key, register the product online using the supplied Registration Key

Activate

Control Manager 5.0 (Required)

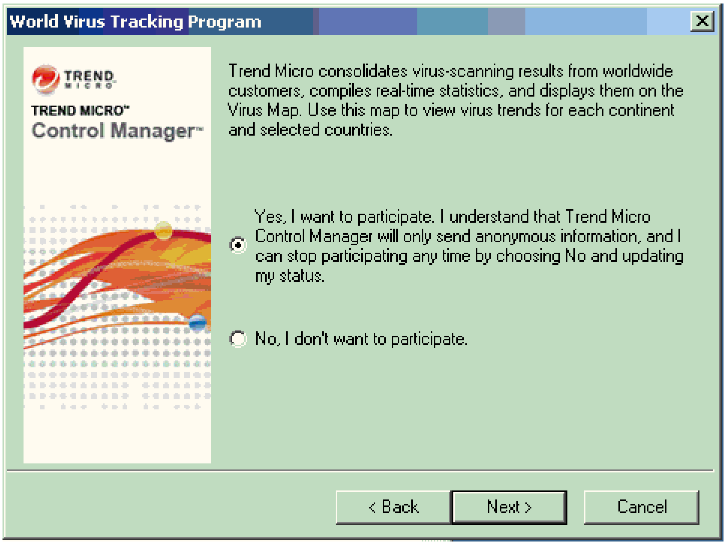
(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Outbreak Prevention Services (Recommended)

FIGURE 3-4. Enter the Activation Code to activate Control Manager and services

2. Type the Activation Code for Control Manager and any other additional purchased services (you can also activate optional services from the Control Manager console). To use the full functionality of Control Manager 5.0 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 that you use to register your software online to the Trend Micro Online Registration Web site and obtain an Activation Code.

3. Click **Next**. The World Virus Tracking screen appears.



World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries.

● Yes, I want to participate. I understand that Trend Micro Control Manager will only send anonymous information, and I can stop participating any time by choosing No and updating my status.

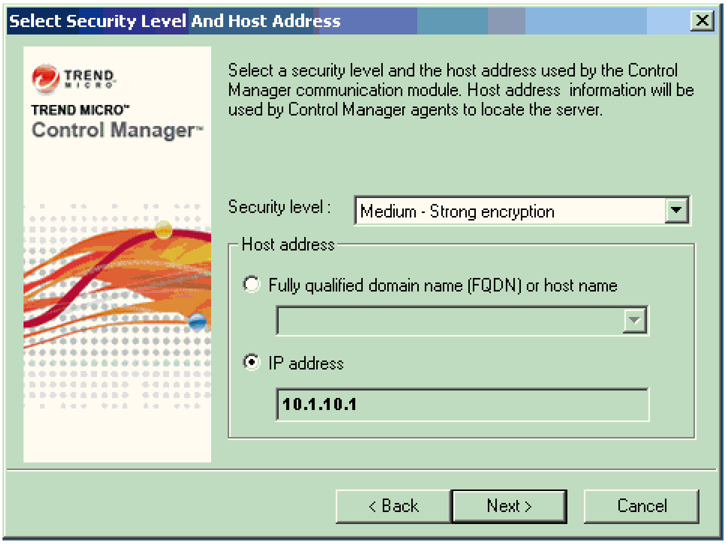
○ No, I don't want to participate.

FIGURE 3-5. Participate in the World Virus Tracking Program

4. Click **Yes** to participate in the World Virus Tracking Program. You can add your data to the Trend Micro Virus Map by choosing to participate in the World Virus Tracking Program. When you choose to participate, Trend Micro Control Manager will only send anonymous information through HTTP, and you can stop participating any time by choosing No and updating your status on the Control Manager management console.

Step 4: Specify Control Manager security and Web server settings

1. Click **Next**. The Select Security Level And Host Address screen appears.



Select Security Level And Host Address

Select a security level and the host address used by the Control Manager communication module. Host address information will be used by Control Manager agents to locate the server.

Security level : Medium - Strong encryption

Host address

○ Fully qualified domain name (FQDN) or host name

● IP address

10.1.10.1

FIGURE 3-6. Select a security level

2. From the Security level list, select the security level for Control Manager communication with agents. The options are as follows:
   - **High:** All communication between Control Manager and managed products use 128-bit encryption with athentication. This ensures the most secure communication between Control Manager and managed products.
   - **Medium:** If supported, all communication between Control Manager and managed products use 128-bit encryption. This is the default setting when installing Control Manager.
   - **Low:** All communication between Control Manager and managed products use 40-bit encryption. This is the least secure communication method between Control Manager and other products.
3. Select a host address for agents to communicate with Control Manager:

Tip: Trend Micro recommends installing Control Manager using a host name. Installing using an IP address can cause issues if the IP address of the Control Manager server requires changing. Control Manager does not support changing the installation IP address. This results in an administrator having to reinstall Control Manager if the server's IP address must change. Installing using a host name avoids the issue.

To use a FQDN/host name:

a. Select **Fully qualified domain name (FQDN) or host name**.

b. Select or type an FQDN or host name in the accompanying field.

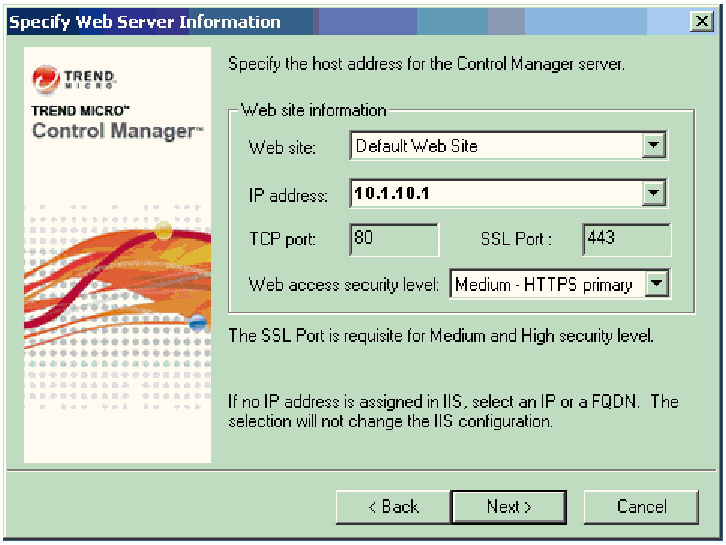
To use an IP address:

a. Select **IP address**.

b. Type an IP address in the accompanying field. Separate multiple entries using a semi-colon (**;**).

4. Click **Next**. The Specify Web Server Information screen appears.

The settings on the Specify Web Server Information screen define communication security and how the Control Manager network identifies your server.



Specify Web Server Information

Specify the host address for the Control Manager server.

Web site information

Web site: Default Web Site

IP address: 10.1.10.1

TCP port: 80

SSL Port : 443

Web access security level: Medium - HTTPS primary

The SSL Port is requisite for Medium and High security level.

If no IP address is assigned in IIS, select an IP or a FQDN. The selection will not change the IIS configuration.

FIGURE 3-7. Specify Web server information

5. From the **Web site** list, select the Web site to access Control Manager.
6. From the **IP address** list, select the IP address or FQDN/host name you want to use for the Control Manager Management Console. This setting defines how the Control Manager communication system identifies your Control Manager server. The setup program attempts to detect both the server's fully qualified domain name (FQDN) and IP address and displays them in the appropriate field.

   If your server has more than one network interface card, or if you assign your server more than one FQDN, the names and IP addresses appear here. Choose the most appropriate address or name by selecting the corresponding option or item in the list.

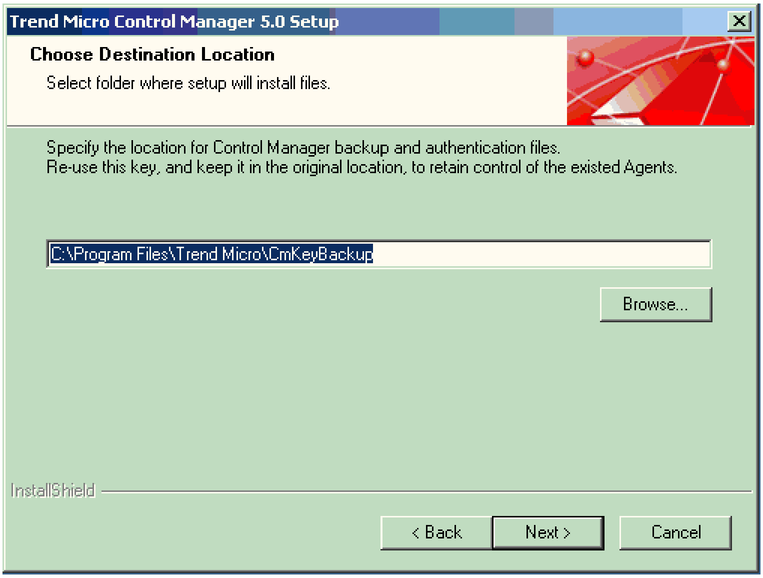
   If you use the host name or FQDN to identify your server, make sure that this name can be resolved on the product computers; otherwise the products cannot communicate with the Control Manager server.
7. From the Web access security level list, select the security level for Control Manager communication. The options are as follows:

- **High - HTTPS only:** All Control Manager communication uses HTTPS protocol. This ensures the most secure communication Control Manager and other products.
- **Medium - HTTPS primary:** If supported all Control Manager communication uses HTTPS protocol. If HTTPS is unavailable, agents use HTTP instead. This is the default setting when installing Control Manager.
- **Low - HTTP based:** All Control Manager communication uses HTTP protocol. This is the least secure communication method between Control Manager and other products.

8. If you selected **Low - HTTP based**, and if you have not specified an SSL Port value in the ISS administration console, specify the access port for Control Manager communication in the **SSL Port** field.

Step 5: Specify back up settings and configure database information

1. Click **Next**. The Choose Destination Location screen appears.



Trend Micro Control Manager 5.0 Setup

Choose Destination Location

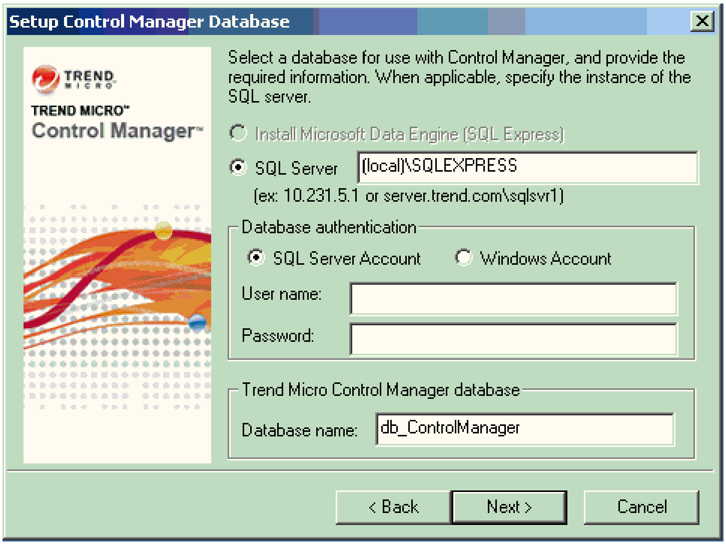
Select folder where setup will install files.

Specify the location for Control Manager backup and authentication files.
Re-use this key, and keep it in the original location, to retain control of the existed Agents.

C:\Program Files\Trend Micro\CmKeyBackup

FIGURE 3-8. Choose a destination location for back up and authentication files

2. Specify the location of the Control Manager backup and authentication files (for more information see the *Control Manager files that should be backed up* on page 4-7). Click **Browse** to specify an alternate location.
3. Click **Next**. The Setup Control Manager Database screen appears.



Select a database for use with Control Manager, and provide the required information. When applicable, specify the instance of the SQL server.

○ Install Microsoft Data Engine (SQL Express)

● SQL Server (local)\SQLEXPRESS

(ex: 10.231.5.1 or server.trend.com\sqlsvr1)

Database authentication

● SQL Server Account ○ Windows Account

User name:

Password:

Trend Micro Control Manager database

Database name: db_ControlManager

FIGURE 3-9. Choose the Control Manager database

4. Select a database to use with Control Manager.
   - **Install Microsoft SQL Express:** the setup program automatically selects this option if an SQL server is not installed on this computer. Do not forget to specify a password for this database in the field provided.

Tip: The Microsoft SQL Express is suitable only for a small number of connections. Trend Micro recommends using an SQL server for large Control Manager networks.

   - **SQL Server:** the setup program automatically selects this option if the program detects an SQL server on the server. Provide the following information:

- **SQL Server (\Instance):** this server hosts the SQL server that you want to use for Control Manager. If an SQL server is present on your server, the setup program automatically selects it.

  To specify an alternative server, identify it using its FQDN, IP address, or NetBIOS name.

  If more than one instance of SQL server exists on a host server (this can be either the same server where you are installing Control Manager, or another server), you must specify the instance. For example: `your_sql_server.com\instance`
- **SQL Server Authentication:** provide credentials to access the SQL server. By default, the User name is **sa**.

WARNING! For security reasons, do not use an SQL database that is not password protected.

5. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is **db_ControlManager**.
6. Click **Next** to create the required database. If the setup program detects an existing Control Manager database you have the following options:
   - **Append new records to existing database:** the Control Manager you install retains the same settings, accounts, and Product Directory entities as the previous server. In addition, Control Manager retains the root account of the previous installation - you cannot create a new root account.

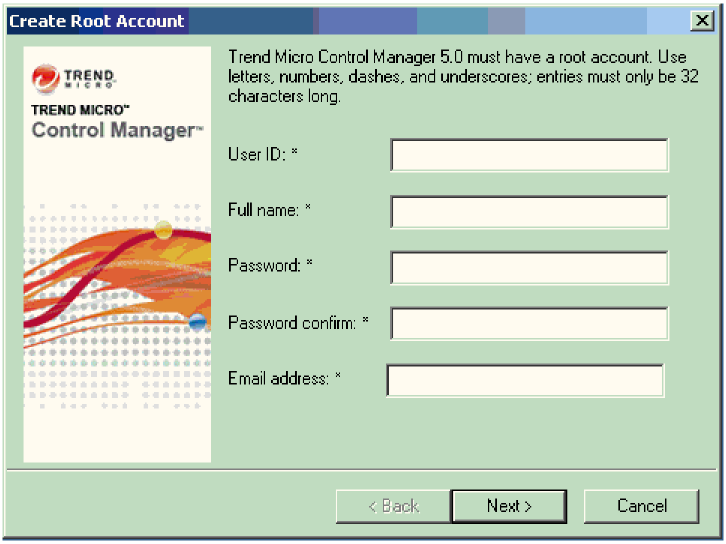
   Note: When installing Control Manager 5.0, you cannot select **Append new records to existing database** for previous Control Manager database versions.

   - **Delete existing records, and create a new database:** the existing database is deleted, and another, using the same name, is created
   - **Create a new database with a new name:** you are returned to the previous screen to allow you to change your Control Manager database name

   Note: If you append records to the current database, you will not be able to change the root account. The Root account screen appears.

Step 6: Set up root account and configure notification settings

1. Click **Next**. The following screen appears:



Create Root Account

Trend Micro Control Manager 5.0 must have a root account. Use letters, numbers, dashes, and underscores; entries must only be 32 characters long.

User ID: *

Full name: *

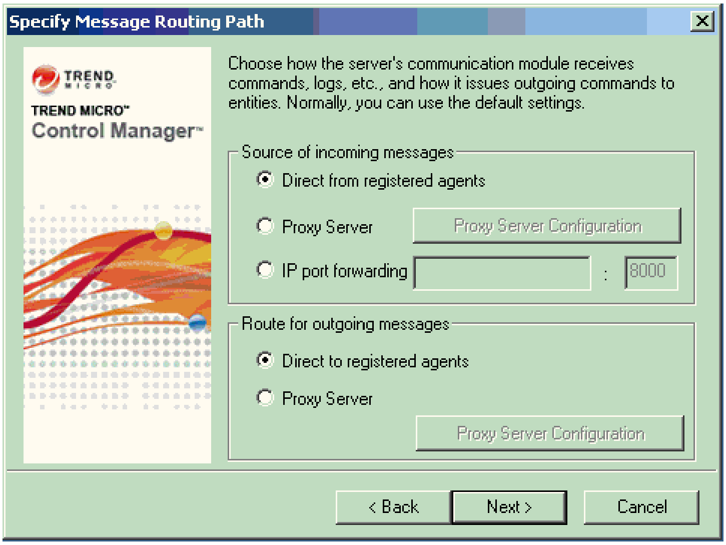
Password: *

Password confirm: *

Email address: *

FIGURE 3-10. Enter information for the Control Manager root account

2. Provide the following required account information:
   - User ID
   - Full Name
   - Password
   - Password confirmation
   - Email address
3. Click **Next**. The Specify Message Routing Path screen appears. This screen only appears if the host server does not have TMI installed.



Specify Message Routing Path

Choose how the server's communication module receives commands, logs, etc., and how it issues outgoing commands to entities. Normally, you can use the default settings.

Source of incoming messages

● Direct from registered agents

○ Proxy Server [Proxy Server Configuration]

○ IP port forwarding [ ] : [8000]

Route for outgoing messages

● Direct to registered agents

○ Proxy Server

[Proxy Server Configuration]

FIGURE 3-11. Define routes for messages or requests

4. Define the routes for incoming and outgoing messages or requests. These settings allow you to adapt Control Manager to your company's existing security systems. Select the appropriate route.

Note: Message routing settings are only set during installation. Proxy configurations made here are not related to the proxy settings used for Internet connectivity–though the same proxy settings are used by default.

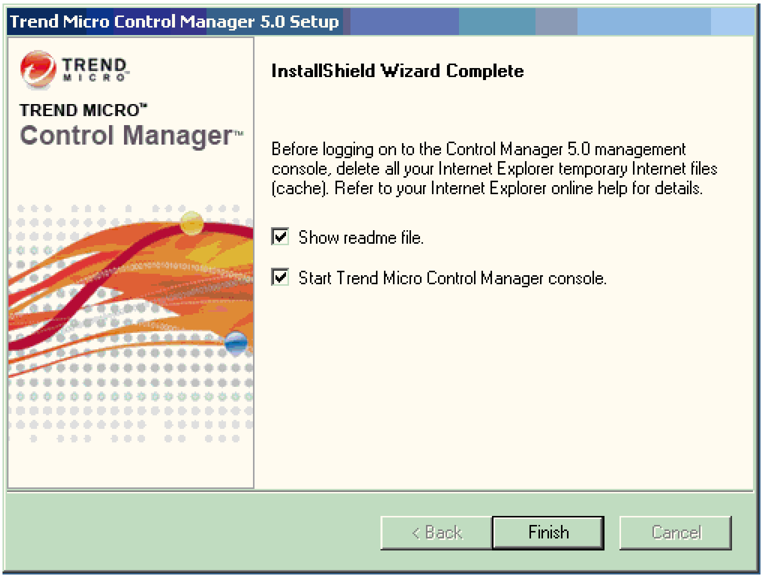
Source of incoming messages

- **Direct from registered agents:** the agents can directly receive incoming messages.
- **Proxy server:** uses a proxy server when receiving messages. For additional details about using and configuring proxies, see *Configuring Proxy Settings* on page 5-60.
- **IP port forwarding:** this feature configures Control Manager to work with the IP port forwarding function of your company's firewall. Provide the firewall server's FQDN, IP address or NetBIOS name, and then type the port number that Control Manager opened for communication.

Route for outgoing messages

- **Direct to registered agents:** Control Manager sends outgoing messages directly to the agents.
- **Proxy server :** Control Manager sends outgoing messages through a proxy server. For additional details about using and configuring proxies, see *Configuring Proxy Settings* on page 5-60.

5. Click **Finish** to complete the installation.



Trend Micro Control Manager 5.0 Setup

InstallShield Wizard Complete

Before logging on to the Control Manager 5.0 management console, delete all your Internet Explorer temporary Internet files (cache). Refer to your Internet Explorer online help for details.

☑ Show readme file.

☑ Start Trend Micro Control Manager console.

FIGURE 3-12. Setup complete

Verifying Successful Installations

Follow the procedures below to confirm that Control Manager server has successfully installed.

Verify a Successful Control Manager Server Installation

To confirm a successful Control Manager server installation, check the following:

The following folders appear under the `Program Files\Trend Micro` directory:

- Common\TMI
- Common\CCGI
- Control Manager

The setup program creates the following services:

- Trend Micro Control Manager

- Trend Micro Common CGI
- Trend Micro Management Infrastructure
- Trend Micro Network Time Protocol

The following processes are running:

CCGI processes:

- Jk_nt_service.exe
- Java.exe

IIS process:

- Inetinfo.exe (Internet Information Services)

ISAPI filters:

- CCGIRedirect
- ReverseProxy
- TmcmRedirect

TMI processes:

- CM.exe (TMI-CM)
- MRF.exe (Message Routing Framework Module)
- DMServer.exe (TMI-DM full-function)

Control Manager processes:

- ProcessManager.exe
- LogReceiver.exe
- MsgReceiver.exe
- LogRetriever.exe
- CmdProcessor.exe
- UIProcessor.exe
- ReportServer.exe
- NTPD.exe
- DCSProcessor.exe
- CasProcessor.exe

Post-installation Configuration

After successfully installing Control Manager, Trend Micro recommends you perform the following post-installation configuration tasks.

1. Register and activate Control Manager
2. Configure user accounts and account types
3. Download the latest components
4. Set notifications

Registering and Activating Control Manager

After successfully installing Control Manager, please check the license status and expiration date on the management console, by clicking **Administration** > **License Management > Control Manager**. If the status is not *Activated* or is expired, obtain an Activation Code and activate your software (on the Web console, click **Administration > License Management > Control Manager > Specify a new Activation Code**). If you experience issues with your Activation Code, please contact technical support. For more information, see *Registering and Activating Your Software* on page 3-25.

Configuring User Accounts

Create Control Manager user accounts based on your needs. Consider the following when creating your accounts:

- The number of different user types (Administrators, Power Users, and Operators)
- Assign appropriate permissions and privileges to each kinds of user types
- For users to take advantage of the cascading management structure, they need to have Power User rights or greater

For more information, see *Configuring Control Manager User Access* on page 5-7.

Downloading the Latest Components

After installation, manually download the latest components (Pattern files\Cleanup templates, Engine updates) from the Trend Micro ActiveUpdate server to help maintain the highest security protection. If a proxy server exists between a Control Manager server and the Internet, configure the proxy server settings (on the Web console, click

Administration > Settings > Proxy Settings). For more information, see *Downloading and Deploying New Components* on page 5-35.

Setting Notifications

After installation, configure the events that will trigger notifications to monitor significant virus/malware attacks and related security activities. Besides specifying notification recipients, choose notification channels and test them to make sure they work as expected (on the Web console, click **Administration > Event Center**). For more information, see *Using Event Center* on page 6-8

Registering and Activating Your Software

Activate the Control Manager server to keep your security and product updates current. To activate your product, register online and obtain an Activation Code using your Registration Key.

If you install Control Manager for the first time:

- You have purchased the full version from a Trend Micro reseller, the Registration Key is included the product package

  Register online and obtain an Activation Code to activate the product
- You install an evaluation version

  Obtain a full version Registration Key from your reseller and then follow the full version instructions to activate the product.

Activating Control Manager

Activating Control Manager allows you to use its full functionality, including downloading updated program components. You can activate Control Manager after obtaining an Activation Code from your product package or by purchasing one through a Trend Micro reseller.

Note: After activating Control Manager, log off and then log on for changes to take effect.

To register and activate Control Manager:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Management**. A sub-menu appears.
3. Click **Control Manager**. The License Information screen appears.
4. Click the **Activate the product/Specify a new Activation Code** link.
5. In the **New** box, type your Activation Code. If you do not have an Activation Code, click the **Register online** link and follow the instructions on the Online Registration Web site to obtain one.
6. Click **Activate**, and then click **OK**.

Converting to the Full Version

Upgrade your Control Manager to the full version and activate it to continue to use it beyond the evaluation period. Activate Control Manager to use its full functionality including downloading updated program components.

To convert to the full version:

1. Purchase a full version Registration Key from a Trend Micro reseller.
2. Register your software online.
3. Obtain an Activation Code.
4. Activate Control Manager according to the instructions in the procedure above.

Renewing Your Product Maintenance

Renew maintenance for Control Manager or its integrated related products and services (Outbreak Prevention Services) using one of the following methods.

To renew your product or service maintenance, first obtain an updated Registration Key. The Registration Key allows you to acquire a new Activation Code. The procedures for renewing your product maintenance differ depending on whether you are using an evaluation or full version.

To renew product maintenance using Check Status Online:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Management**. A sub-menu appears.

3. Click **Control Manager**. The License Information screen appears.
4. On the working area under **Control Manager License Information**, click **Check Status Online**, and then click **OK**.
5. 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:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **License Management**. A sub-menu appears.
3. Click **Control Manager**. The License Information screen appears.
4. On the working area under **Control Manager License Information**, click the **Activate the product** link.
5. Click the **Specify a new Activation Code** link and follow the instructions on the Online Registration Web site.
6. In the **New** box, type your Activation Code.
7. Click **Activate**.
8. Click **OK**.

Chapter 4

Upgrading Servers or Migrating Agents to Control Manager 5.0

Upgrading existing Control Manager 3.0 or 3.5 servers to Control Manager 5.0 requires careful consideration and detailed planning. Likewise, the same is true when migrating MCP and older Control Manager agents to a Control Manager 5.0 server.

This chapter contains the following topics:

- *Upgrading to Control Manager 5.0* on page 4-2
- *Planning Control Manager Agent Migration* on page 4-11
- *Migrating the Control Manager Database* on page 4-17

Upgrading to Control Manager 5.0

The following table lists the considerations when upgrading to the Standard or Advanced Edition:

TABLE 4-1. Considerations when upgrading to Control Manager 5.0

CAPABILITY	STANDARD EDITION	ADVANCED EDITION
Upgrade Control Manager 3.0 or 3.5 servers	Yes	Yes
Retain the reporting functions	No	Yes
Upgrade a Standard edition to Advanced Edition To upgrade from a Standard Edition to an Advanced Edition, obtain an Advanced Edition Activation Code (AC), and then reinstall Control Manager (only reinstall, do not uninstall and then reinstall). During installation, provide the new Advanced Edition AC.	Yes	N/A
Convert an Enterprise/Advanced Edition to Standard Edition	N/A	Yes

Upgrading Control Manager 3.0 or 3.5 Servers

Trend Micro recommends installing Control Manager 5.0 over the previous installtion of Control Manager 3.0/3.5. This way all your previous settings, logs and reports, and Product Directory remain the same. However, before upgrading verify that the server where Control Manager installs has sufficient system resources.

WARNING! Always back up the existing server before performing the upgrade.

Upgrading and Migrating Scenarios

Control Manager supports three scenarios for upgrading or migration:

- Scenario 1: Upgrading a Control Manager 3.5 Server to Control Manager 5.0
- Scenario 2: Migrating to a Fresh Control Manager 5.0 Installation Using the Agent Migrate Tool

- Scenario 3: Upgrading or Migrating a Cascading Environment

Scenario 1: Upgrading a Control Manager 3.5 Server to Control Manager 5.0

When upgrading Control Manager 3.5 directly to Control Manager 5.0, administrators can choose to backup Control Manager or backup the entire operating system of the server where Control Manager installs. Backing up the operating system is more work intensive but provides better security to prevent data loss.

To upgrade by backing up the previous Control Manager server and database:

1. Backup the existing Control Manager 3.5 database.
2. Backup all the files under \Trend Micro\CmKeyBackup\*.*.
3. Backup all folders of the current Control Manager 3.5 server.
4. Backup the registries of the current Control Manager 3.5 server.
5. Install Windows Installer 3.1, if necessary.
6. Install MDAC 2.8 SP1, if necessary.
7. Install Control Manager 5.0 over Control Manager 3.5.

Note: See Table 4-3, "Control Manager files that should be backed up," on page 4-7 for steps 2 through 4.

To upgrade by backing up the entire operating system of the server and the Control Manager database:

1. Backup the operating system of existing Control Manager 3.5 server.
2. Backup the existing Control Manager 3.5 database.
3. Install Windows Installer 3.1 (If necessary)
4. Install MDAC 2.8 SP1 (If necessary)
5. Install Control Manager 5.0 over Control Manager 3.5.

Scenario 2: Migrating to a Fresh Control Manager 5.0 Installation Using the Agent Migrate Tool

This scenario involves installing Control Manager 5.0 on a separate server from the existing Control Manager server. This allows you to slowly decommission the previous server. See *Planning Control Manager Agent Migration* on page 4-11 for more information about migrating agents.

To migrate a Control Manager 3.5 server to a fresh installation of Control Manager 5.0:

1. Backup the existing Control Manager 3.5 database.
2. Perform a fresh installation of Control Manager 5.0 on a different computer.
3. Use the Agent Migration Tool to migrate entities from the Control Manager 3.5 server to the Control Manager 5.0 server.

Note: The Agent Migration Tool only supports migrating managed products. The Agent Migration Tool does not support migrating logs, reports, or the Product Directory structure from the previous server.

Scenario 3: Upgrading or Migrating a Cascading Environment

Control Manager provides two methods for updating a cascading environment. The first involves unregistering and then re-register the child Control Manager servers. The other method involves creating a file (CascadingUpgrade.ini) to insert on the child server.

TABLE 4-2. CascadingUpgrade.ini Variables

VARIABLE	PARENT CONTROL MANAGER SETTINGS SCREEN	DESCRIPTION
PARENT CONTROL MANAGER SERVER SETTINGS		
Host	Server FQDN or IP address	The host name or IP address of the parent Control Manager server.
Port	Port	The port number used to communciate with the proxy server.
Protocol	Connect using HTTPS	The protocol used to communicate with the parent Control Manager server.

TABLE 4-2. CascadingUpgrade.ini Variables

VARIABLE	PARENT CONTROL MANAGER SETTINGS SCREEN	DESCRIPTION
WebServerUser	Web server authentication	The user name required for the Web server's authentication.
WebServerPassword		The password required for the Web server's authentication.
MCP PROXY SETTINGS		
Enable	Use a proxy server to communicate with the parent Control Manager server	Specify **1** to indicate you use a proxy server. Specify a **0** if you do not use a proxy server.
Type	Proxy protocol	The protocol used to communicate with the proxy server.
Host	Server name or IP address	The host name or IP address of the proxy server.
Port	Port	The port number used to communciate with the proxy server.
ProxyServerUser	Proxy server authentication	The user name required for the proxy server's authentication.
ProxyServerPassword		The password required for the proxy server's authentication.

To upgrade or migrate a cascading environment by unregistering child servers:

1. Unregister all child Control Manager servers from the parent Control Manager server.
2. Backup the parent Control Manager server.
3. Backup all child Control Manager servers.
4. Upgrade the parent Control Manager server.
5. Upgrade all child Control Manager servers.
6. Register all child Control Manager servers to the parent Control Manager server.

To upgrade or migrate a cascading environment using CascadingUpgrade.ini:

1. Backup the parent Control Manager server.
2. Backup all child Control Manager servers.
3. Create the following file using a text editor:

   CascadingUpgrade.ini file

   Use the following format for the CascadingUpgrade.ini file:

   ```
   [Common]
   Host=
   Port=
   Protocol=
   WebServerUser=
   WebServerPassword=

   [Proxy]
   Enable=
   Type=
   Host=
   Port=
   ProxyServerUser=
   ProxyServerPassword=
   ```
4. Insert a CascadingUpgrade.ini file in the Control Manager folder of each child Control Manager server.
5. Upgrade the parent Control Manager server.
6. Upgrade all child Control Manager servers.

TABLE 4-3. Control Manager files that should be backed up

CONTROL MANAGER 3.0/3.5 INFORMATION	LOCATION
Database	Use the SQL Enterprise Manager or osql to back up the Control Manager database. Refer to the Control Manager *Back up db_ControlManager using SQL Enterprise Manager / osql* online help topics for detailed steps.
Authentication information (ensures that managed products reporting to the Control Manager server will report to the same server if Control Manager is restored)	`\Program Files\Trend Micro\CmKeyBackup\*.*`

Configuration files	`\Program Files\Trend Micro\Control Manager\Settings\*.*`
	`\Program Files\Trend Micro\Control Manager\DataSource.xml`
	`\Program Files\Trend Micro\Control Manager\CascadingLogConfiguration.xml`
	`\Program Files\Trend Micro\Control Manager\Settings\DMregisterinfo.xml`
	`\Program Files\Trend Micro\Control Manager\Settings\EntityEmulator.xml`
	`\Program Files\Trend Micro\Control Manager\Settings\ProductUIHandler.xml`
	`\Program Files\Trend Micro\Control Manager\Settings\SystemConfiguration.xml`

GUID information	`GUID value in \Program files\Trend Micro\COMMON\TMI\TMI.cfg`

TABLE 4-3. Control Manager files that should be backed up

CONTROL MANAGER 3.0/3.5 INFORMATION	LOCATION

Managed product information	`\Program Files\Trend Micro\common\tmi\mrf_entity.dat`
	`\Program Files\Trend Micro\common\tmi\mrf_entity.bak`

ActiveUpdate files	`\Program Files\Trend Micro\Control Manager\webui\download\Activeupdate`

Table 4-3. Control Manager files that should be backed up

Control Manager 3.0/3.5 Information	Location

Control Manager registry	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\`
	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI\`
	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MSDE`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDE`
	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI`
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer`

Rolling Back to Control Manager 3.0/3.5 Servers

If upgrading to Control Manager 5.0 is unsuccessful, perform the following steps to roll back to your Control Manager 3.0/3.5 system.

Scenario 1: Rolling Back a Control Manager 3.5 Server to Control Manager 5.0

To rollback from a Control Manager server and database backup:

1. Remove the Control Manager 5.0 server
2. Install Control Manager 3.5 server
3. Restore the Control Manager 3.5 database with the backup database.
4. Restore all the Control Manager 3.5 folders with the backed up folders.
5. Restore Control Manager 3.5 registries with the backed up registries.
6. Restore all the files under \Trend Micro\CmKeyBackup\*.*.
7. Apply Control Manager 3.0/3.5 service packs and hot fixes.
8. Import the old certificate.

To rollback from an entire operating system of the server and the Control Manager database backup:

1. Restore the Control Manager 3.5 database with the backup database.
2. Restore the operating system of the server with the backed up operating system.

Scenario 2: Rolling Back from a Fresh Control Manager 5.0 Installation Using the Agent Migrate Tool

See *Planning Control Manager Agent Migration* on page 4-11 for more information about migrating agents.

To rollback to a Control Manager 3.5 server from a fresh installation of Control Manager 5.0:

1. Restore the Control Manager 3.5 database with the backup database.
2. Use the Agent Migration Tool to migrate entities from the Control Manager 5.0 server to the Control Manager 3.5 server.

Scenario 3: Rolling Back a Cascading Environment

To rollback a cascading environment by unregistering child servers:

1. Unregister all child Control Manager servers from the parent Control Manager server.
2. Rollback the parent Control Manager server.
3. Rollback all child Control Manager servers.
4. Apply Control Manager service packs and hot fixes.
5. Register all child Control Manager servers to the parent Control Manager server.

To rollback a cascading environment that used CascadingUpgrade.ini to upgrade:

1. Unregister all child Control Manager servers from the parent Control Manager server.
2. Rollback the parent Control Manager server.
3. Rollback all child Control Manager servers.
4. Apply Control Manager service packs and hot fixes.
5. Register all child Control Manager servers to the parent Control Manager server.

Planning Control Manager Agent Migration

There are two ways to migrate agents to a Control Manager 5.0 server:

- **Rapid upgrade**

  Rapid upgrade works using the following approach:

TABLE 4-4. Rapid Upgrade

ORIGINAL SERVER/AGENT	ACTION
Control Manager 3.0 SP 6 with Control Manager 2.5x agents	Registers Control Manager 2.5x agents to Control Manager 5.0 server; Control Manager agents maintain their original Product Directory structure

TABLE 4-4. Rapid Upgrade

ORIGINAL SERVER/AGENT	ACTION
Control Manager 3.0 SP 6 with mixed agents	**Control Manager agents:** Registers Control Manager 2.5x agents to Control Manager 5.0 server; Control Manager agents maintain their original Product Directory structure MCP Registers MCP agents to Control Manager 5.0 server; MCP agents maintain their original Product Directory structure
Control Manager 3.5/5.0 with MCP agents	Registers MCP agents to Control Manager 5.0 server; MCP agents maintain their original Product Directory structure
Control Manager 3.5/5.0 with mixed agents	Control Manager agents: Registers Control Manager 2.5x agents to Control Manager 5.0 server; Control Manager agents maintain their original Product Directory structure MCP Registers MCP agents to Control Manager 5.0 server; MCP agents maintain their original Product Directory structure

Trend Micro recommends rapid upgrade for migrating agents in a laboratory setting or in relatively small networks, preferably during test deployments (see *Testing Control Manager at One Location* on page 2-10). However, since you cannot stop the migration once it starts, this method works best for smaller deployments, since the degree of difficulty increases with the size of the network.

- **Phased upgrade**

  Trend Micro recommends a phased upgrade for large, single-server Control Manager 3.0/3.5 networks. This is essential for multiple-server networks. This method offers a more structured approach to migrating your system, and follows these guidelines:

  - Start migration on systems with the least impact on the existing network, and then proceed to the systems with progressively greater impact
  - Upgrade the old network in well-planned stages, rather than all at once

    This will simplify any troubleshooting that may be required.

  Phased upgrade involves the following steps:

a. Install Control Manager 5.0 on a server that does not have any previous Control Manager version installed (preferably without any managed products).

b. Run the AgentMigrateTool.exe tool on the Control Manager 5.0 server.

Use the Control Manager agent installation together with the Using Agent Migration Tool (AgentMigrateTool.exe) to plan the upgrade of agents on existing Control Manager networks. The Agent Migration tool can generate a list of servers with Control Manager agents. Doing so eliminates the need to manually select the agent servers.

Migration Scenarios for Control Manager 2.x Agents

The following agent migration scenarios are possible:

- Single-server migration:

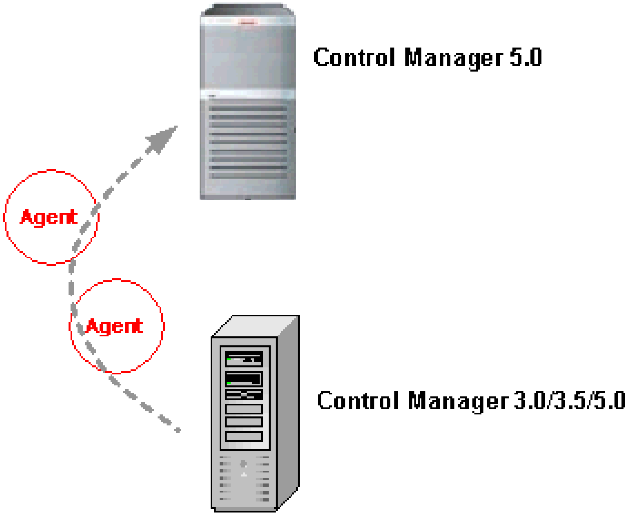


FIGURE 4-1. Migration of agents belonging to a single server

You can use both Rapid and Phased migration in this instance. See *Upgrading to Control Manager 5.0* on page 4-2.

- Consolidation of different servers/agents:

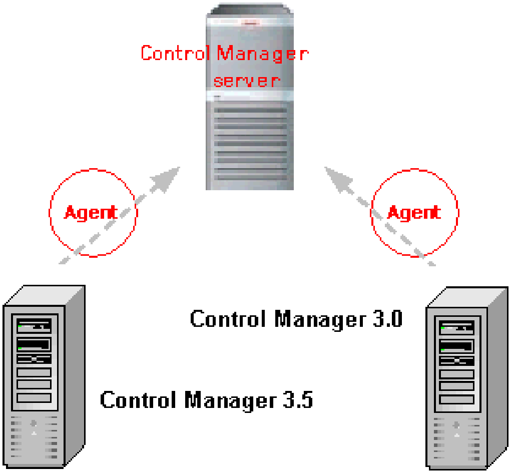


FIGURE 4-2. Migration of agents belonging to multiple servers

Because of new Control Manager access control features, functions previously handled by separate Control Manager servers - to restrict user access to specific segments of the antivirus network - can now be combined in a single Control Manager server.

Control Manager 2.5x Agent Migration Flow

During Control Manager 2.5x agent migration, the agent migration tool performs the following:

1. Stops the Trend Micro Infrastructure service
2. Obtains the Product Directory information from the Control Manager 3.0 or 3.5 server
3. Removes the agent information from the Control Manager 3.0 or 3.5 database and TMI.cfg
4. Retains the Control Manager 2.5x agent version (no upgrade takes place)
5. Writes the agent information to the Control Manager 5.0 database and TMI.cfg
6. Restarts the Trend Micro Infrastructure service

If AgentMigrationTool.exe cannot complete or finish the Control Manager 2.5x agent migration, it removes the agent information from the Control Manager 5.0 database and TMI.cfg and then writes them back to the Control Manager 3.0/3.5 database.

MCP Agent Migration Flow

During MCP migration, the agent migration tool performs the following:

1. Stops the Trend Micro Management Infrastructure service of the destination server.
2. Obtains the Product Directory information from the Control Manager server.
3. Retains the Control Manager agent version (no upgrade takes place).
4. Writes the agent information to the database of the destination server.
5. Restarts the Trend Micro Management Infrastructure service of the destination server.
6. Stops and then restarts the Trend Micro Control Manager service of the destination server.
7. Requests the source server to issue a Change Server command and waits for polling by the MCP agent.

Migrating Control Manager 2.5x and MCP Agents

Use `AgentMigrateTool.exe` to migrate Windows-based agents originally administered by Control Manager 3.0 server, Control Manager 3.5 server, or Control Manager 5.0 server. When migrating agents, 2.5x agents migrate first, then MCP agents migrate.

If an agent migration is unsuccessful, the following occurs:

- The agent continues to be managed by the source server
- Agent logs are on both the source and destination servers

Migrated logs will not show logs unless the agents register to the destination server. Destination Control Manager server purges migrated logs when purge triggers.

Note: Run `AgentMigrateTool.exe` directly on the destination server — a Control Manager 5.0 server to which you migrate the agents.

To migrate Control Manager 2.5x or MCP agents:

1. Using Windows Explorer, open the Control Manager 5.0 root folder. For example:

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

2. Double-click `AgentMigrateTool.exe`.

Note: Remember to start the destination Control Manager server's Remote Registry service or agent migration will not be successful.

3. Click **Configure Source Server Settings** on the main menu.
4. On the Configurations screen under **Source server**, type the **IP address** of the *source server*—Control Manager 3.0, Control Manager 3.5, or Control Manager 5.0 server hosting the agents that will migrate.
5. Under **System Administrator Account**, specify the administrator **user name** and **password** used to access the source server, and then click **Connect**.
6. On the main window, click **Add** > or **Add All >>** to migrate agents from the **Source** to the **Destination** list.
7. Select all or one of the following options:
   - **Retain tree structure:** `AgentMigrateTool.exe` instructs the destination server (that is, a Control Manager 5.0 server) to retain the original Product Directory structure of the selected managed products
   - **Migrate logs:** `AgentMigrateTool.exe` copies the logs of the selected managed products from the source to the destination server
   - **Enable HTTPS:** `AgentMigrateTool.exe` notifies migrating agents to use HTTPS to register to Control Manager. If you do not select this option, agents use HTTP to register to Control Manager

   These options apply to agents listed in the Destination list.

Tip: Trend Micro recommends enabling the **Retain tree structure** and **Migrate logs** options when migrating all agents from the source server.

Migrating managed products that use Control Manager 2.1 agents prevents the destination server from querying the old logs of the migrated managed product. Trend Micro recommends upgrading to Control Manager 2.5 agents before running `AgentMigrateTool.exe`.

The following products use the Control Manager 2.1 agent:

- InterScan eManager 3.50 (all applicable platforms)
- InterScan eManager 3.52 (all applicable platforms)
- ScanMail eManager 5.0 (all applicable platforms)
- ScanMail eManager 5.1 (all applicable platforms)
- InterScan Messaging Security Suite 5.1 for Windows

8. Click **Migrate**.

`AgentMigrateTool.exe` migrates the agent(s) listed in the Destination list.

Migrating the Control Manager Database

You have two ways to migrate a Control Manager database:

- Install Control Manager 5.0 on a Control Manager 3.0/3.5 server. Tthis is the recommended method

  The Control Manager 5.0 setup automatically upgrades the database to version 5.0. Refer to Control Manager 2.5x agent migration on *page 4-14* for more details.
- Manually transfer the Control Manager 3.0/3.5 database to Control Manager 5.0 server

Migrating Control Manager SQL 2005 Database to Another SQL 2005 Server

Modify a number of parameters in TMI.cfg to move a Control Manager database from an SQL 2005 server to another SQL 2005 server.

To migrate an existing database to another SQL 2005 server:

1. Using Windows Services, stop the following Control Manager services:
   - Trend Micro Management Infrastructure
   - Trend Micro CCGI
   - Trend Micro Control Manager

2. Copy the Control Manager database from the old SQL Server to the new SQL Server.

   Note: Control Manager encrypts the `CFG_DM_DB_PWD` value. Trend Micro recommends configuring the target SQL server with the same authentication account used to access `db_ControlManager`, as well as keeping the same ID and password combination.

3. Open `<root>\Program Files\Trend Micro\COMMON\TMI\TMI.cfg` using a text editor.

   Note: Back up `TMI.cfg` to roll back to the original settings.

4. Replace the `CFG_DM_DB_DSN=Server=` parameter value with the name of the destination SQL Server.
5. Retain the old ID and password. Otherwise, update the values for the following parameters:

   `CFG_DM_DB_ID`

   `CFG_DM_DB_PWD`
6. Save and close `TMI.cfg`.
7. Click **Start** > **Programs** > **Administrative Tools** > **Data Sources (ODBC)** to open the ODBC Data Source Administrator.
8. Activate the **System DSN** tab and then configure the **ControlManager_DataBase** data source.
9. On the Microsoft SQL Server DSN Configuration, select the **destination server** to modify the **Which SQL Server do you want to connect to?** value and then click **Next**.

   If the destination server is not available from the list, type the **server name**.
10. On the next window, select **With SQL Server authentication using a logon ID and password entered by the user** and **Connect to SQL Server to obtain default settings for the additional configuration** options.
11. Type the same **ID** and **password** available in `TMI.cfg` and then click **Next**.
12. Click **Finish** to save the new configuration and close Microsoft SQL Server DSN Configuration.

13. Click **OK** to close ODBC Data Source Administrator.
14. Using Windows Services, restart all Control Manager services.

Log on to the management console and access the Product Directory to check if all managed products are registered. If so, then you have successfully moved database to the destination SQL Server.

Chapter 5

Getting Started with Control Manager

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

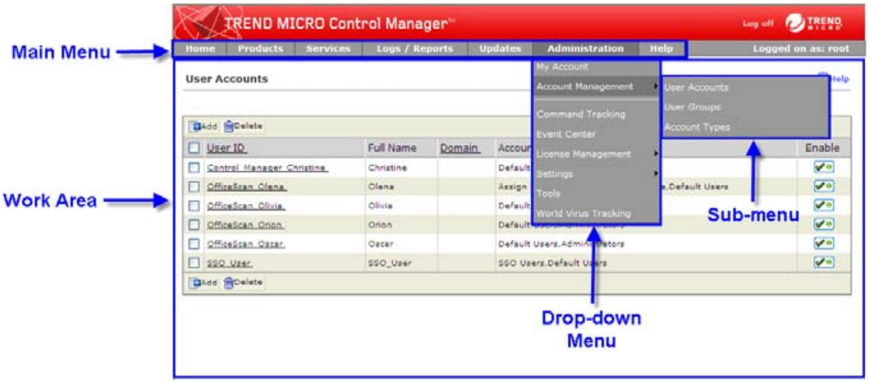
This chapter contains the following topics:

- *Using the Management Console* on page 5-2
- *Configuring Control Manager User Access* on page 5-7
- *Understanding the Product Directory* on page 5-26
- *Managing Child Servers* on page 5-30
- *Downloading and Deploying New Components* on page 5-35

Using the Management Console

The management console consists of the following elements:

- **Main menu:** Provides links to the Home, Products, Services, Logs/Reports, Updates, Administration menus to administer Control Manager and managed products and links to the Control Manager online help, the Trend Micro Knowledge Base, Trend Micro Security Information, and the About screen for Control Manager
- **Working area:** Administer managed products or child server settings, invoke tasks, or view system status, logs, and reports



User Accounts

Add Delete

□	User ID	Full Name	Domain	Accoun	Enable
□	Control Manager Christine	Christine		Default	✓
□	OfficeScan Olena	Olena		Assign ,Default Users	✓
□	OfficeScan Olivia	Olivia		Default	✓
□	OfficeScan Orion	Orion		Default	✓
□	OfficeScan Oscar	Oscar		Default Users,Admin tors	✓
□	SSO User	SSO_User		SSO Users,Default U rs	✓

Add Delete

FIGURE 5-1. Control Manager Management Console

TABLE 5-1. Contents of the Control Manager Main menu

MAIN MENU	
Home	Provides an at a glance summary of your network and includes shortcuts to detailed information screens and reports.
Products	Includes options to administer Managed Products, Communicators, and Child servers.
Services	Includes TrendLabs Message Board posts and available services (Outbreak Prevention Services and Vulnerability Assessment)
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.

TABLE 5-1. Contents of the Control Manager Main menu

MAIN MENU	
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 ten security threats • Control Manager version, build number, and copyright information

Understanding The Function-locking Mechanism

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

TABLE 5-2. 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 management console cannot access the Directory Manager nor the User Manager option.

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

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

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

Note: 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** dialog box appears. Clicking **OK** opens the management console Log On screen.

Accessing the Management Console

You have two ways to access the management console:

- Locally on the Control Manager server

  To access the management 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 field provided.

  c. Click **Enter**.

- Remotely using any compatible browser

  To access the console remotely:

  a. Type the following at your browser's address field to open the Log on page:

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

  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 **Enter**.

Upon opening the console, the initial screen will show the status summary for your whole Control Manager system. This is identical to the status summary generated from the Product Directory. User rights determine the Control Manager functions you can access.

Note: You can only access one instance of the management console. Control Manager does not allow the same Control Manager management console in more than one browser.

Assigning HTTPS Access to the Control Manager Management Console

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 management 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, 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. Select **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 management console using HTTPS, the following message appears:

> *You must view this page over a secure channel*

Accessing the HTTPS Management Console

If you want to encrypt the configuration data as it passes from the Web-based console to the Control Manager server, assign HTTP to Control Manager Web access and then alter the management console URL to use the HTTPS protocol through port 443. Type the URL for encrypted communication (HTTPS) in the following format:

```
https://{host name}:443/ControlManager
```

Where:

`{host name}` is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name.

`443` is the port allotted during an HTTPS session.

When you access a secure Control Manager site, it automatically sends you its certificate, and Internet Explorer displays a lock icon (🔒) on the status bar.

Logging Off from the Management Console

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

- Click **Log Off** on the header.
- Press the **CTRL** and **W** keys simultaneously.

Configuring Control Manager User Access

The Control Manager User Manager from previous versions of Control Manager now consists of four sections:

TABLE 5-3. Control Manager User Account Options

SECTION	DESCRIPTION
My Account	The My Account screen contains all the account information 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 Control Manager 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.

Understanding Account Types

In previous versions of Control Manager, four user account types exist. Control Manager 5.0 uses these account types as **default** account types:

- Operator
- Power User
- Administrator/Root

Control Manager 5.0 introduces 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 *To edit a user account:* on page 5-21.)

2. Specify which menu items the user can access. (If the default account types are not sufficient, see *To add an account type:* on page 5-11 or *To edit an account type:* on page 5-13)

3. Specify the account type for the user's account. (Step 7 of the *To edit a user account:* on page 5-21.)

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

TABLE 5-4. User Account Access

MENU ITEM	OPERATOR	POWER USER	ADMINISTRATOR
HOME	●	●	●

Table 5-4. User Account Access

Menu Item			Operator	Power User	Administrator
Products			●	●	●
Services					●
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			●	●
	Settings	Schedule Download Exceptions		●	●
		Update / Deployment		●	●

TABLE 5-4. User Account Access

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			●
		Control Manager Parent Setting			●
		Event Center Settings			●
		Heartbeat Settings			●
		Proxy Settings			●
		Timeout Settings			●
		Add/Remove Product Agents	●	●	●
	Tools				●
	World Virus Tracking				●

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, 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.

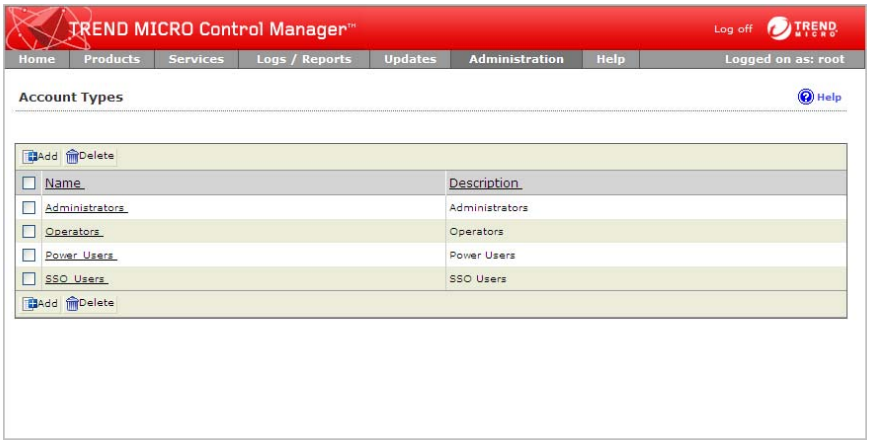
Note: Control Manager accounts log on to Control Manager only, and not the entire network. Control Manager user accounts are not the same as network domain accounts.

Adding 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.

To add an account type:

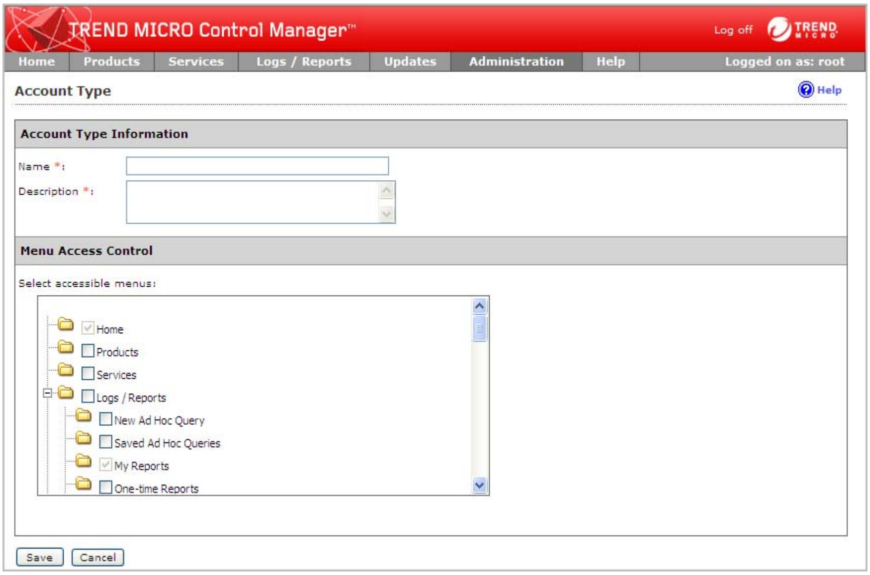
1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
3. Click **Account Types** from the sub-menu. The Account Types screen appears.



Account Types

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

4. 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:

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

5. Type a unique account type name in the **Name** field.
6. 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 which users the account type proves most useful.

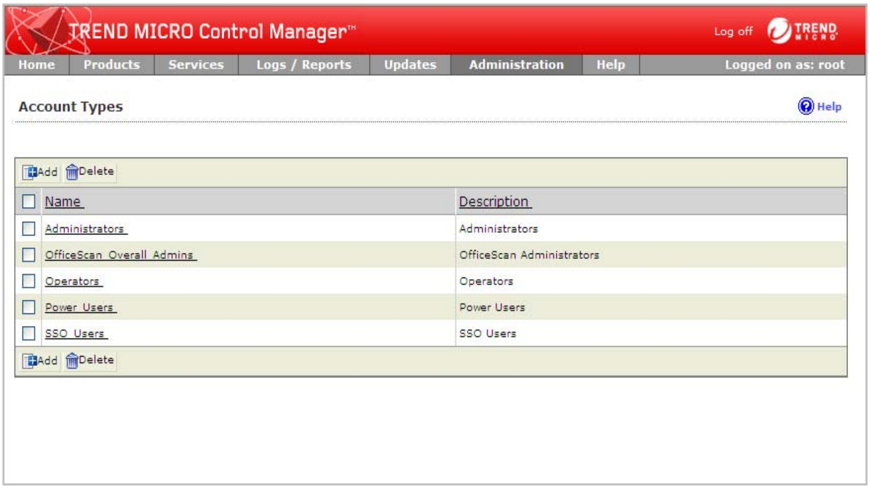
7. Select the accessible menu items for the account type. The following menu items are accessible to every account type: **Home**, **My Reports**, and **My Account**.
8. Click **Save**. The Account Type screen appears and the new account type appears in the Account Type list.

Editing Account Types

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

To edit an account type:

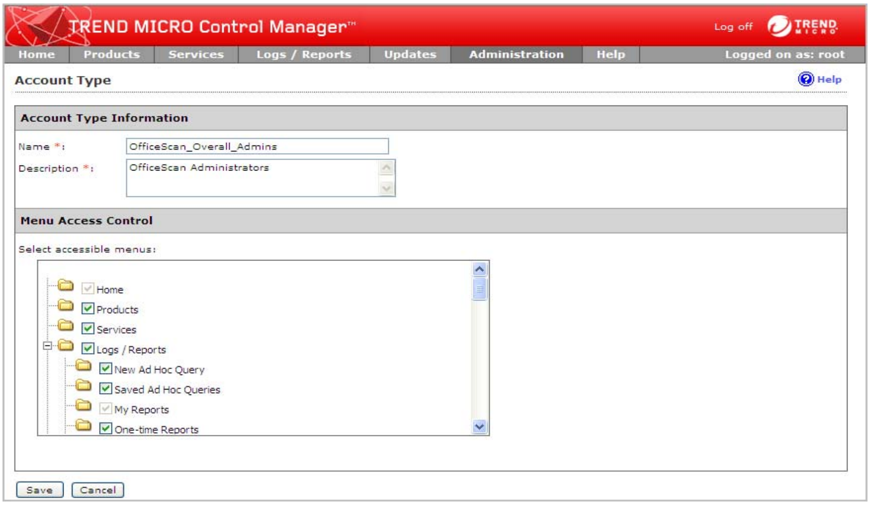
1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
3. Click **Account Types** from the sub-menu. The Account Types screen appears.



Account Types

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

4. 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:

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

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

Understanding User Accounts

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

Tip: When administrators specify which products a user can access, the administrator is also specifying what information a user can access from Control Manager. This applies to component information, logs, product summary information, security information, and information available for reports and 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 operation for all OfficeScan servers, while Bob on the other hand only oversees operation 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 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 5-5. Control Manager User Account Options

SECTION	DESCRIPTION
Execute	This right permits the user to run commands on managed products in assigned folders. The following are associated with this privilege. • Start Scan Now • Deploy pattern files/cleanup templates • Enable Real-time Scan • Deploy program files • Deploy engines • Deploy license profiles
Configure	This 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 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.

Adding a User Account

Add user accounts to do the following:

- Allow administrators to specify which products/directories other users can access
- Allow other users to log on to the Control Manager management 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 *To edit a user account:* on page 5-21.)

2. Specify which menu items the user can access. (If the default account types are not sufficient, see *To add an account type:* on page 5-11 or *To edit an account type:* on page 5-13)

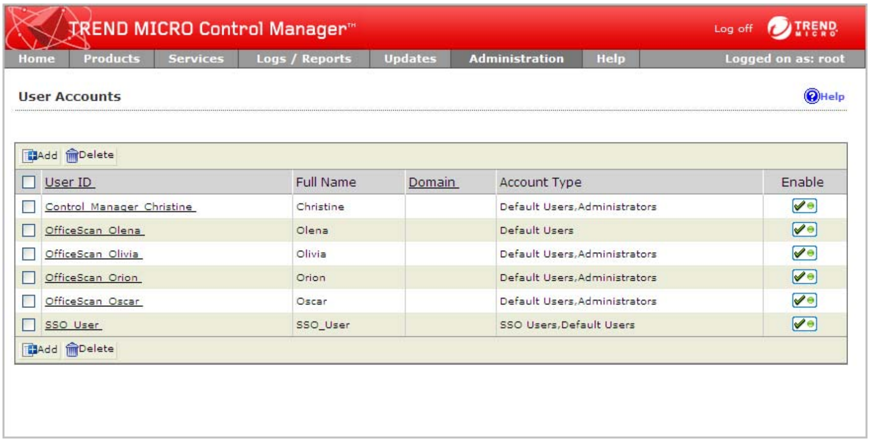
3. Specify the account type for the user's account. (Step 7 of the *To edit a user account:* on page 5-21.)

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:

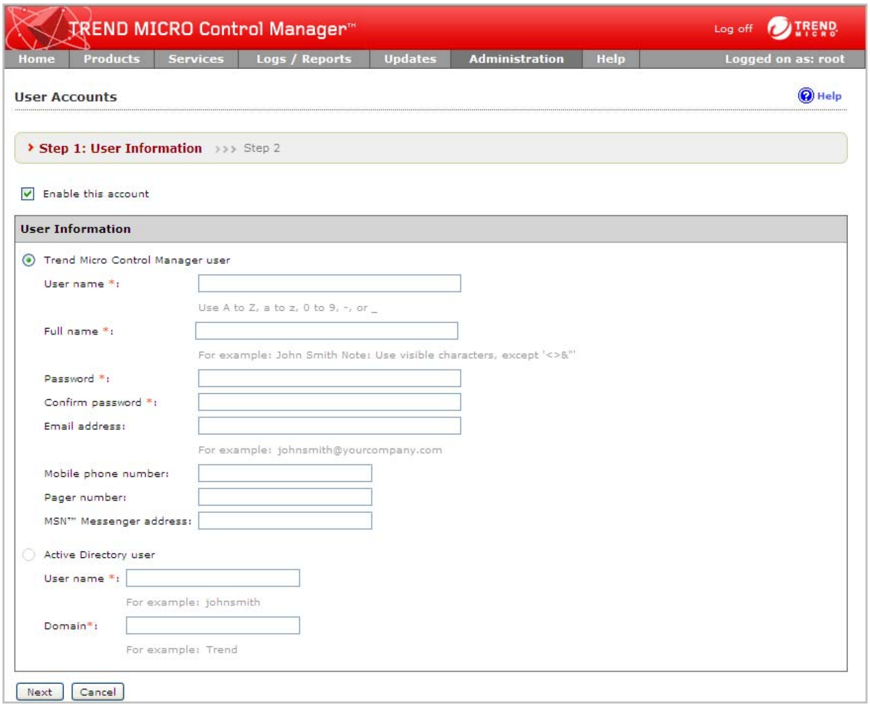
1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
3. Click **User Accounts** from the sub-menu. The User Accounts screen appears.



User Accounts

□ User ID	Full Name	Domain	Account Type	Enable
□ Control_Manager_Christine	Christine		Default Users,Administrators	✓
□ OfficeScan_Olena	Olena		Default Users	✓
□ OfficeScan_Olivia	Olivia		Default Users,Administrators	✓
□ OfficeScan_Orion	Orion		Default Users,Administrators	✓
□ OfficeScan_Oscar	Oscar		Default Users,Administrators	✓
□ SSO_User	SSO_User		SSO Users,Default Users	✓

4. In the working area, click **Add**. The Add User Account 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

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

6. Select the type of user to add:

   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.

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.

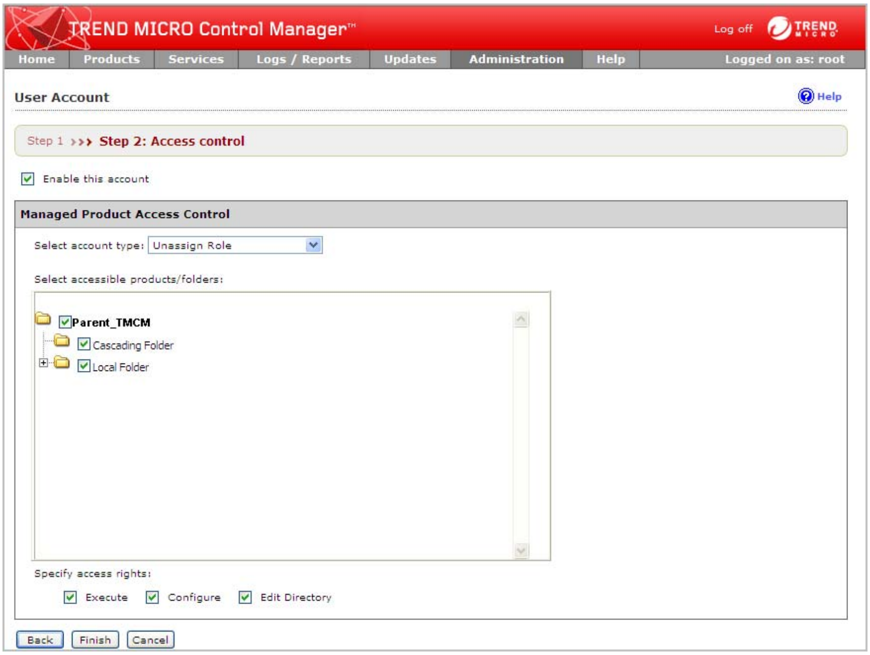
a. Select **Active Directory user**.

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.

7. Click **Next**. The Add User Account 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

8. 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.

9. 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.

10. Select the rights to assign the to the user. These rights determine the actions 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 sub-accounts.

11. Click **Finish**.

Editing a User Account

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 sub-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 sub-set 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:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
3. Click **User Accounts** from the sub-menu. The User Accounts screen appears.
4. Click **Edit** beside the account to modify. The Edit User Account screen appears.
5. Modify the account information, and then click **Next>>**.
6. Modify the accessible folders and access rights.
7. Click **Apply**.

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:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **Account Management** from the drop down menu. Another menu appears.
3. Click **User Accounts** from the menu. The User Accounts screen appears.
4. Click the status icon (a green check) under the Enable column of the User Accounts table. The status icon changes to a red dash.

Deleting a User Account

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 where the user account was part of recipient list.

To delete a user account:

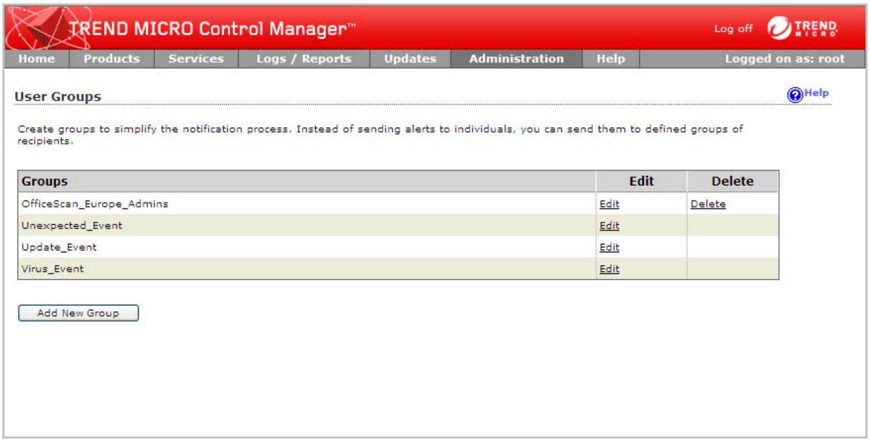
1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **Account Management** from the drop down menu. Another menu appears.
3. Click **User Accounts** from the menu. The User Accounts screen appears.
4. Click the check box accompanying the account to delete.
5. Click **Delete**.

Adding a User Group

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. 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 them 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:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
3. Click **User Groups** from the menu. The User Groups screen appears.

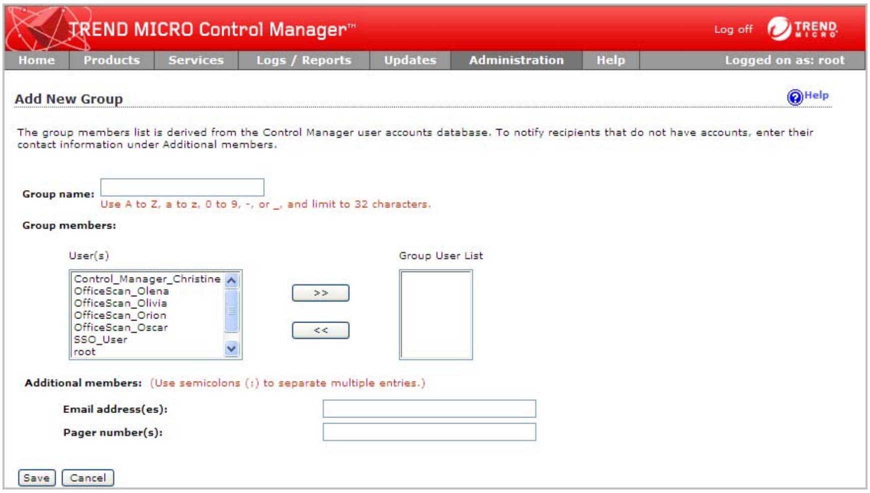


User Groups

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
OfficeScan_Europe_Admins	Edit	Delete
Unexpected_Event	Edit	
Update_Event	Edit	
Virus_Event	Edit	

4. 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)

Control_Manager_Christine
OfficeScan_Olena
OfficeScan_Olivia
OfficeScan_Orion
OfficeScan_Oscar
SSO_User
root

Group User List

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

Email address(es):

Pager number(s):

5. Type a descriptive name for the group in **Group name**.
6. 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.

7. 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.

8. Click **Save**.
9. 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:

1. Mouseover **Administration** on the main menu. A drop-down menu appears.
2. Mouseover **Account Management** from the drop-down menu. A sub-menu appears.
3. Click **User Groups** from the sub-menu. The User Groups screen appears.
4. On the working area, click **Edit** beside the group to modify.
5. Change the entries as required.
6. Click **Save**.
7. 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 where the user group was added to the recipient list.

To delete a user group:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **Account Management** from the drop down menu. Another menu appears.
3. Click **User Groups** from the menu. The User Groups screen appears.
4. Click **Delete** beside the group to delete.
5. Click **OK** to delete the user group.
6. Click **OK**.

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 management console Product Directory section. These icons represent Trend Micro antivirus, content security products, 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 status’ for your managed product.

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

Table 5-6. Product Directory Options

Menu Items	Description
Advanced Search	Click this button to specify search criteria to perform a search for one or more managed products.
Configure	Click this button, after selecting a managed product/directory, to log on to the Web-based console and configure a managed product.
Tasks	Click this button, after selecting a managed product/directory, to perform specific function (such as deploying the latest components) to a specific or groups of managed product or child servers. Initiating a task from a directory and Control Manager sends requests to all managed products belonging to that directory.
Logs	Click this button, 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.

TABLE 5-6. Product Directory Options

MENU ITEMS	DESCRIPTION
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 clients found in the directory.

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

Grouping Managed Products Using Directory Manager

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

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

TABLE 5-7. 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 5-8. Considerations when Grouping Managed Products or Child Servers

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

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

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

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

- **User access**

  When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire Directory. Granting access to a specific managed product only grants access to that specific product.

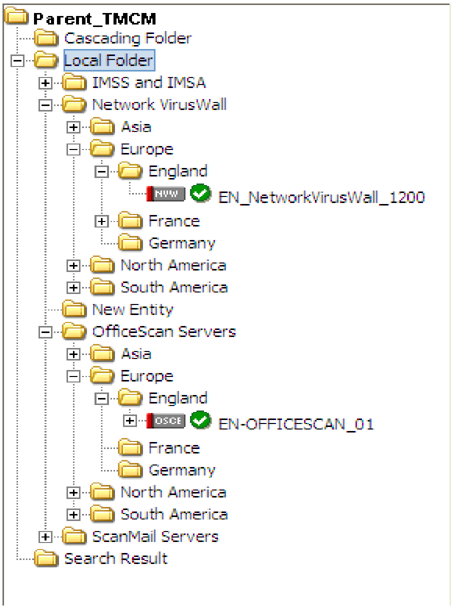
- **Deployment planning**

  Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.

- **Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments**

  OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

A sample Product Directory appears below:



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

Refer to the Control Manager *Understanding Product Directory* online help topic for the list of Product Directory icons.

FIGURE 5-2. Sample Product Directory

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. For example, grant access rights to mail administrators to configure the Mail folder.

Default Folders for the Product Directory

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

TABLE 5-9. 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.

Managing Child Servers

Control Manager provides a cascading management structure, which allows control of multiple Control Manager servers from a single parent server. A parent server is a Control Manager server that manages Standard or Advanced Control Manager servers, referred to as child servers. A child server is a Control Manager server managed by a parent server.

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

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

TABLE 5-10. Parent and child server feature comparison

FEATURE	AVAILABLE IN PARENT	AVAILABLE IN CHILD
Support two-tier cascading structure	Yes	No
Administer managed products	Yes	Yes
Handle multiple child servers	Yes	n/a
Issue global tasks	Yes	No
Create global reports	Yes	No

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).

Configuring Child Servers

The cascading management structure, using the Control Manager management console, allows you to manage, monitor, and perform the following actions to all child servers belonging to a parent server:

- Monitor the Antivirus, Content Security, and Web Security summaries
- Query Event or Security logs
- Initiate tasks
- View reports
- Access the child server management console

The cascading structure can effectively manage your organization's antivirus and content security products - nationwide or worldwide.

Tip: Trend Micro recommends the management of no more than 200 child servers and 9,600 managed products for one Control Manager parent server.

Registering or Unregistering Child Servers

Registering or unregistering child servers does not give the same result as enabling or disabling child servers. The former permanently cuts the parent and child server connection, while the latter temporarily suspends the connection between the two.

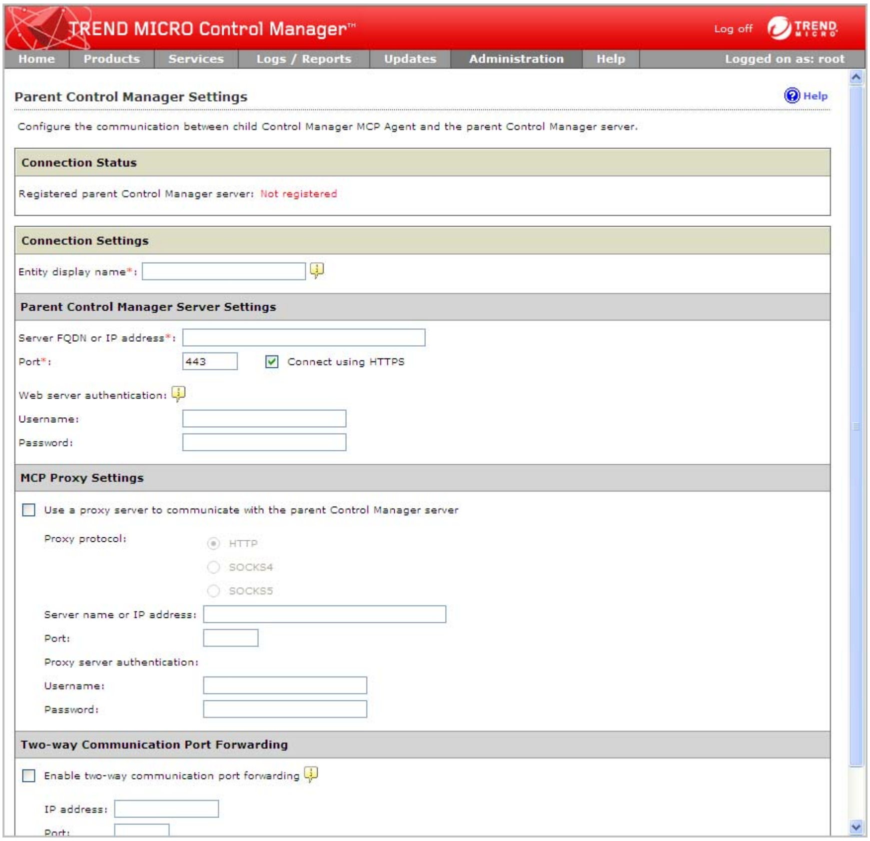
For example, if you registered *child server xyz* to *parent server a*, unregister *xyz* from *a* and register it to *parent server b*. *Parent server b* manages *xyz*. *a*'s cascading structure tree removes *child server xyz* from the list.

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*

To register a child server:

1. Mouseover **Administration** in the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Parent Control Manager Settings** from the sub-menu. The Parent Control Manager Settings screen appears.



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:

4. Configure **Connection Settings**:
   - Type the name the child server displays in the parent Control Manager in the **Entity display name** field.
5. 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.

6. 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** and complete the following settings:

   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.

7. Configure **Two-way Communication Port Forwarding**:

   a. If you will use port forwarding with MCP agents, select **Enable two-way communication port forwarding** and complete the following settings:

   b. Type the forwarding IP address in the **IP address** field.

   c. Type the port number in the **Port** field.

8. To verify the child server can connect to the parent Control Manager server, click **Test Connection**.

9. Click **Register** to connect to the parent Control Manager server.

To unregister a child Control Manager server:

1. From the child server, mouseover **Administration** in the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Parent Control Manager Settings** from the sub-menu. The Parent Control Manager Settings screen appears.
4. Click **Unregister** at the bottom of the screen.

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 virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

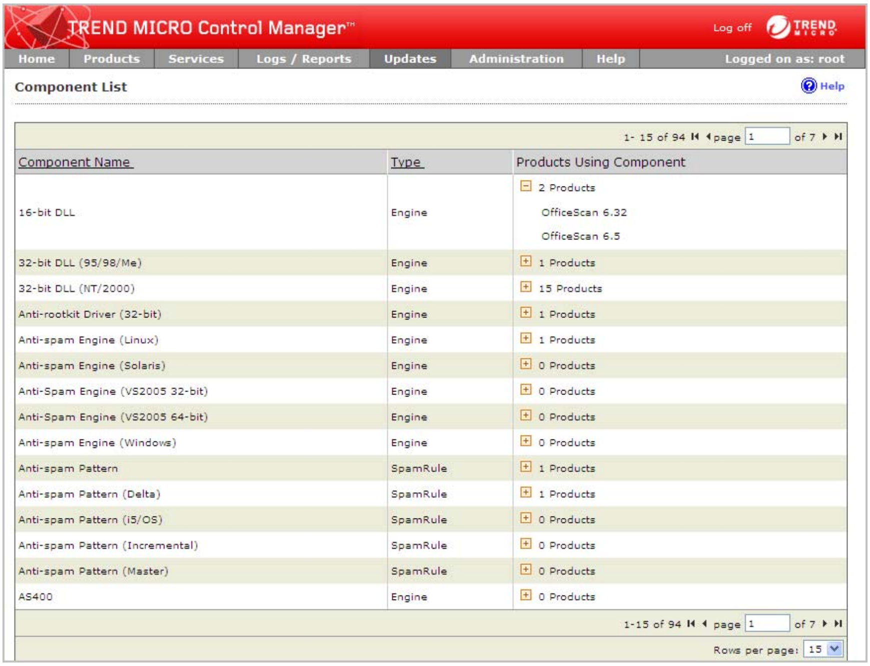
The following are the components to update (listed according to the frequency of recommended update):

- **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
- **Anti-spam rules:** Anti-spam rules are the Trend Micro-provided files used for anti-spam 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
- **Product program:** Product specific components (for example, Service Pack releases)

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 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 Name	Type	Products Using Component
16-bit DLL	Engine	⊟ 2 Products OfficeScan 6.32 OfficeScan 6.5
32-bit DLL (95/98/Me)	Engine	⊞ 1 Products
32-bit DLL (NT/2000)	Engine	⊞ 15 Products
Anti-rootkit Driver (32-bit)	Engine	⊞ 1 Products
Anti-spam Engine (Linux)	Engine	⊞ 1 Products
Anti-spam Engine (Solaris)	Engine	⊞ 0 Products
Anti-Spam Engine (VS2005 32-bit)	Engine	⊞ 0 Products
Anti-Spam Engine (VS2005 64-bit)	Engine	⊞ 0 Products
Anti-spam Engine (Windows)	Engine	⊞ 0 Products
Anti-spam Pattern	SpamRule	⊞ 1 Products
Anti-spam Pattern (Delta)	SpamRule	⊞ 1 Products
Anti-spam Pattern (i5/OS)	SpamRule	⊞ 0 Products
Anti-spam Pattern (Incremental)	SpamRule	⊞ 0 Products
Anti-spam Pattern (Master)	SpamRule	⊞ 0 Products
AS400	Engine	⊞ 0 Products

FIGURE 5-3. 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.

This is the Trend Micro recommend method of configuring 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

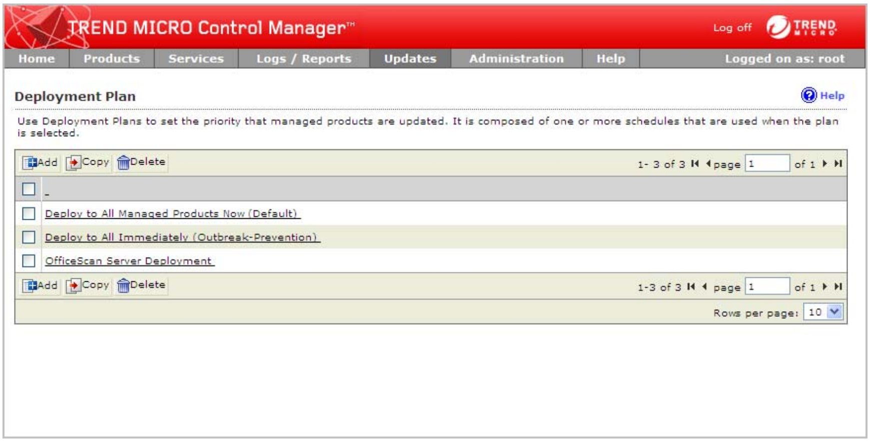
Step 5: Configure the automatic deployment settings

Step 6: Complete the manual download

To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Deployment Plan** from the drop-down menu. The Deployment Plan screen appears.

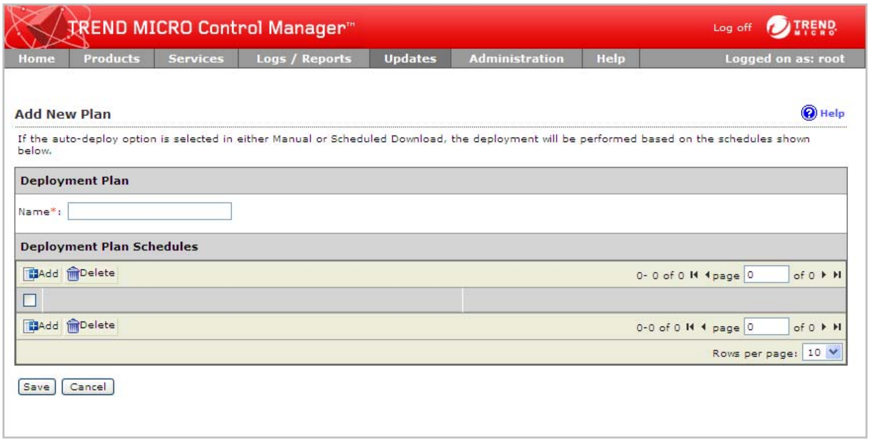


Deployment Plan

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.

- □ Deploy to All Managed Products Now (Default)
- □ Deploy to All Immediately (Outbreak-Prevention)
- □ OfficeScan Server Deployment

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



Add New Plan

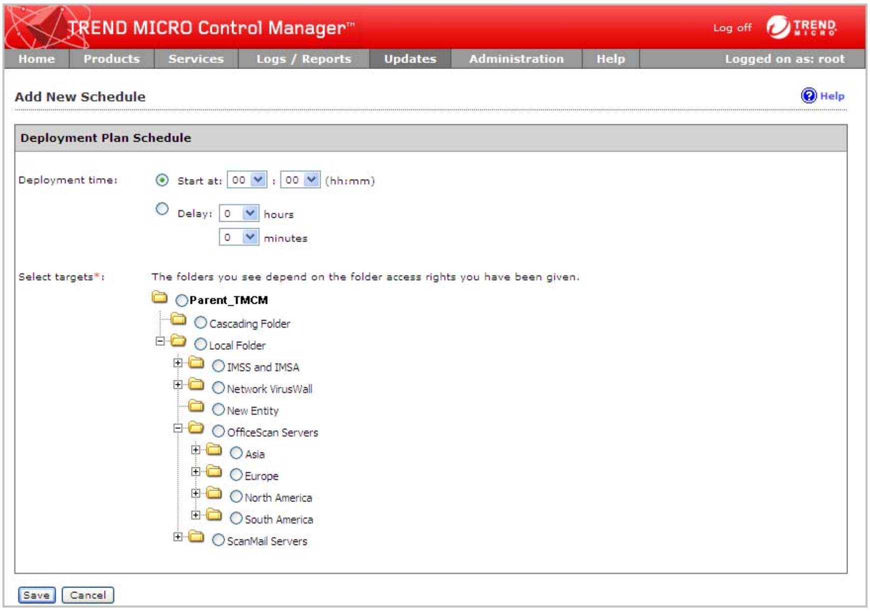
If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Deployment Plan

Name*:

Deployment Plan Schedules

4. On the Add New Plan screen, type a deployment plan name in the **Name** field.
5. 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

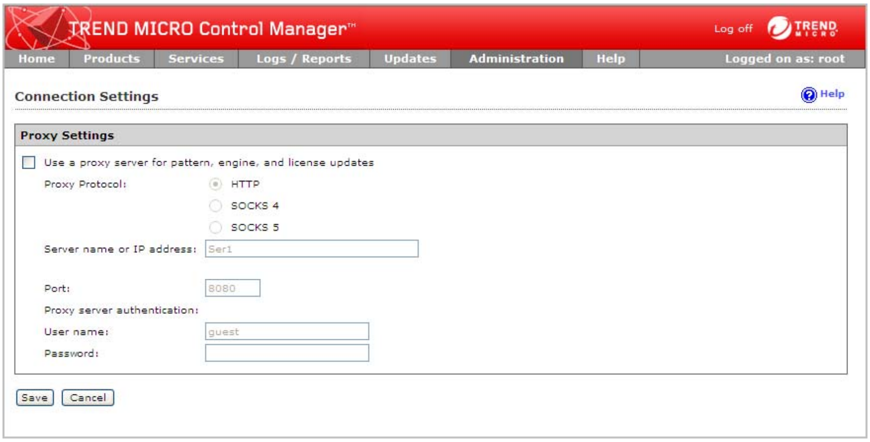
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at** - Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

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

1. Mouseover **Administration**. A drop-down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.



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: Ser1

Port: 8080

Proxy server authentication:

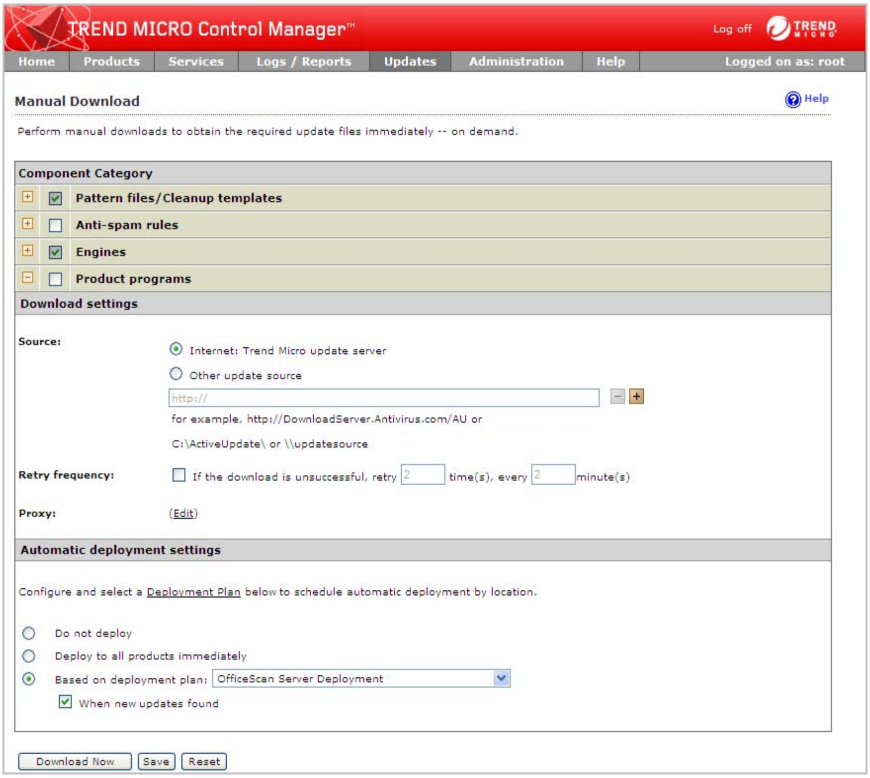
User name: guest

Password:

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

Step 3: Select the components to update

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Manual Download**. The Manual Download screen appears.



Manual Download

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

Component Category

- ☑ Pattern files/Cleanup templates
- □ Anti-spam rules
- ☑ Engines
- □ Product programs

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: OfficeScan Server Deployment
  - ☑ When new updates found

3. From the Components 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 Anti-spam rules**
      - **All Engines**
      - **Product programs**

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 additional update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number or 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, 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, 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.

---

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 the **Command Details** to view details from the Command Details screen.
3. Click **OK** to return to the Manual Download screen.

Accessing Manual Download

Use the Manual Download screen to immediately obtain new components.

To access the Manual Download screen:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Manual Download**. The Manual Download screen appears.

Configuring Manual Download Settings

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

To configure manual download settings:

1. Access the Manual Download screen.
2. On the working area under Download Settings:
   a. Select components that you want to download.
   b. Select the update source:
      - **Internet:** Trend Micro update server to 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 additional update source. You can configure up to five update sources.

c. Select **Retry frequency** and specify the number or 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.

---

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

3. Click **Save**.

Configuring Manual Download and Automatic Deployment Settings

Use the Automatic Deployment Settings group to set how Control Manager deploys updates.

To configure manual download Automatic Deployment Settings:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Manual Download**. The Manual Download screen appears.
3. Select when to deploy downloaded components from the Schedule area:
   - **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

---

Tip: 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.

For Damage Cleanup Services and Vulnerability Assessment, Control Manager automatically deploys components (damage cleanup template, damage cleanup engine, vulnerability assessment pattern, and vulnerability assessment engine) whenever newer versions are available.

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.

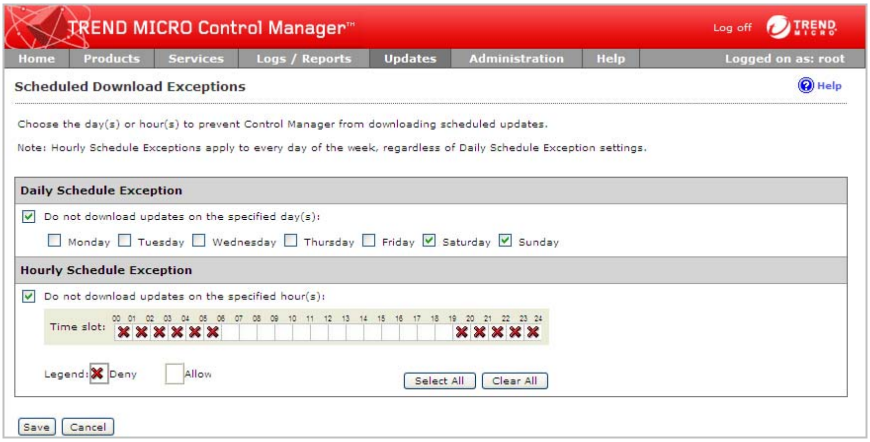
This feature is particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

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:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Scheduled Download Exceptions**. The Scheduled Download Exceptions screen appears.



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

4. Do the following:
   - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, Control Manager blocks all downloads for the selected day(s).
   - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, Control Manager blocks all downloads for the selected hours.
5. Click **Save**.

Understanding 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 downloads 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

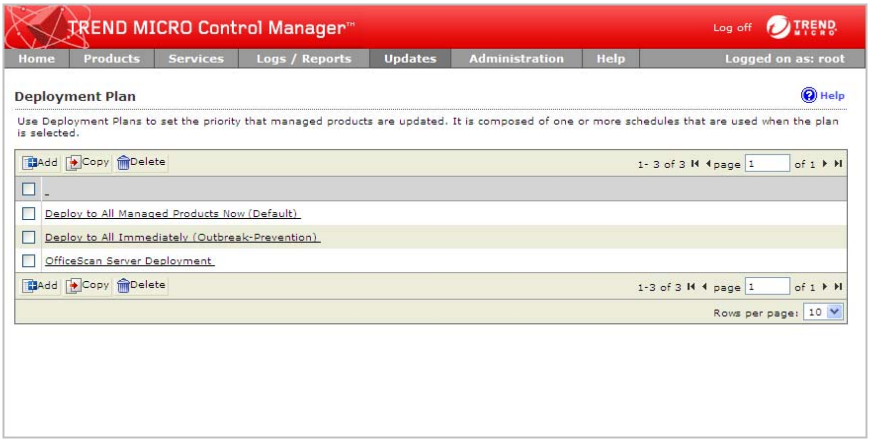
Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

Configuring Scheduled Downloads and Enabling Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Deployment Plan** from the drop down menu. The Deployment Plan screen appears.



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.

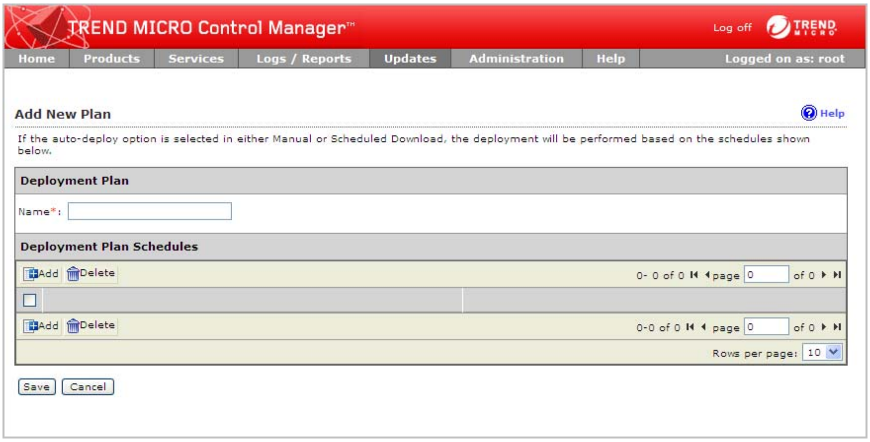
□ _

□ Deploy to All Managed Products Now (Default)

□ Deploy to All Immediately (Outbreak-Prevention)

□ OfficeScan Server Deployment

3. 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

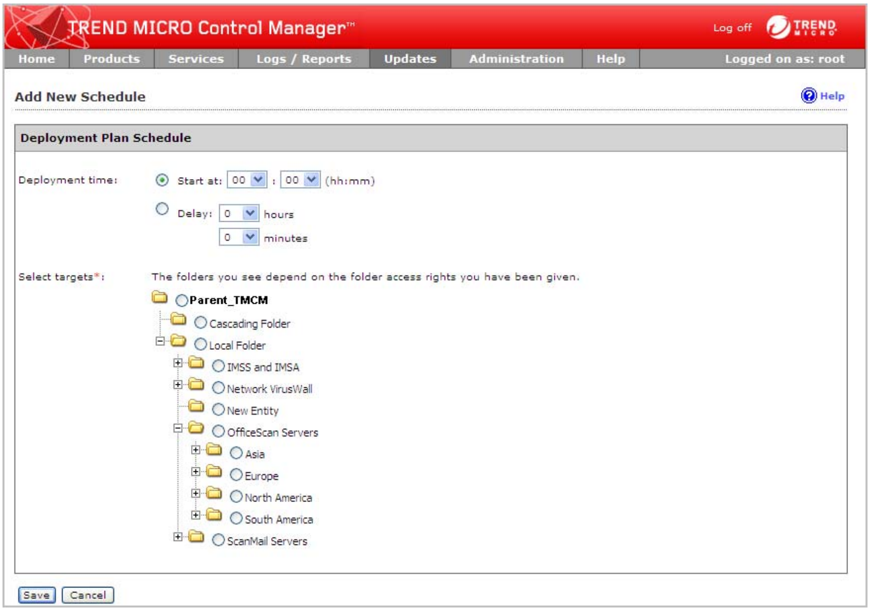
Name*:

Deployment Plan Schedules

□

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

5. 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

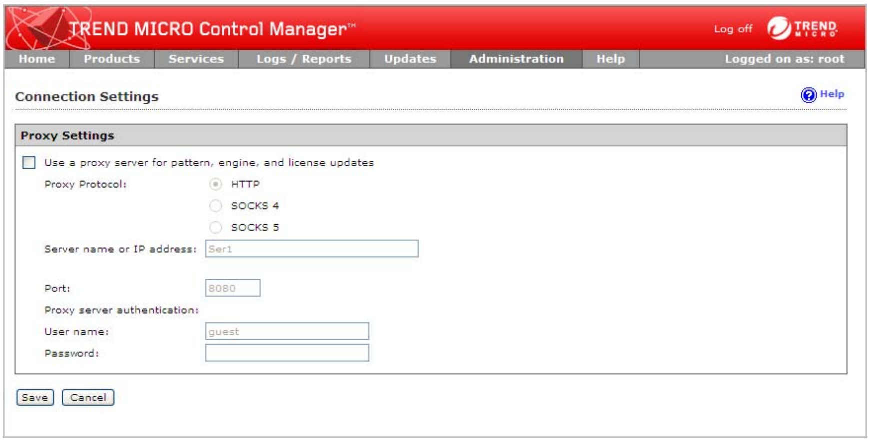
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at** - Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

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

1. Mouseover **Administration**. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.



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: Ser1

Port: 8080

Proxy server authentication:

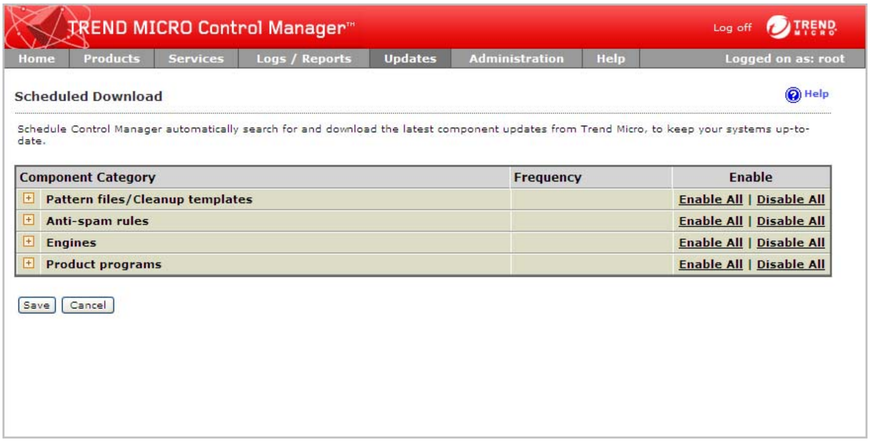
User name: guest

Password:

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

Step 3: Select the components to update

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.



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
+ Anti-spam rules		Enable All | Disable All
+ Engines		Enable All | Disable All
+ Product programs		Enable All | Disable All

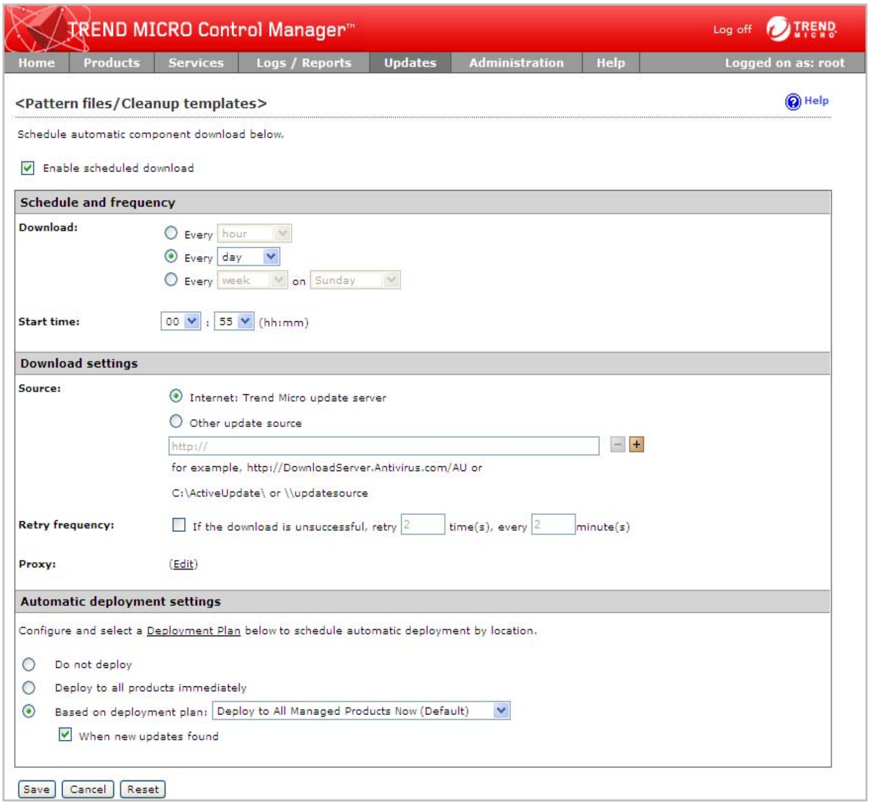
3. From the Components area select the components to download.

   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 Anti-spam rules**
      - **All Engines**
      - **Product programs**

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



<Pattern files/Cleanup templates>

Schedule automatic component download below.

☑ Enable scheduled download

Schedule and frequency

Download:
○ Every hour
● Every day
○ Every week on Sunday

Start time: 00 : 55 (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

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 additional update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number or 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, 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:

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules**
        - **All Engines**
        - **Product programs**

        The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.
4. 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.
5. 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:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules**
      - **All Engines**
      - **Product programs**

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

Under Download settings:

4. 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 Internet 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.
5. 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.

---

6. 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.
7. 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:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules**
      - **All Engines**
      - **Product programs**

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

Under Automatic deployment settings

4. 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.

5. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
6. Click **Save**.

Note: The settings in Automatic Deployment Settings only apply to components used by managed products.

For Damage Cleanup Services and Vulnerability Assessment, Control Manager automatically deploys components (damage cleanup template, damage cleanup engine, vulnerability assessment pattern, and vulnerability assessment engine) whenever newer versions are available.

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 performs the deployment plan according to manual or scheduled download settings.

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

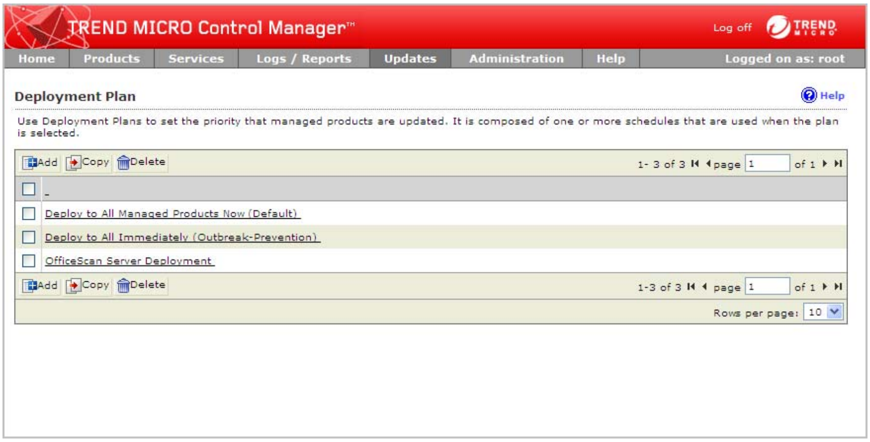
- Assign deployment schedules to folders, not specific products.

  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 are independent of each other.

  For example, if you have three folders that you want to update at five 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.

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Deployment Plan** from the drop down menu. The Deployment Plan screen appears.

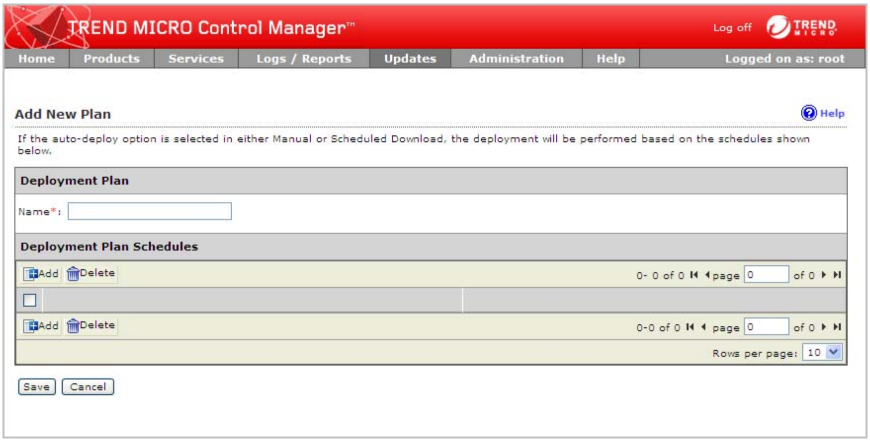


Deployment Plan

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.

□ Deploy to All Managed Products Now (Default)
□ Deploy to All Immediately (Outbreak-Prevention)
□ OfficeScan Server Deployment

3. 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.

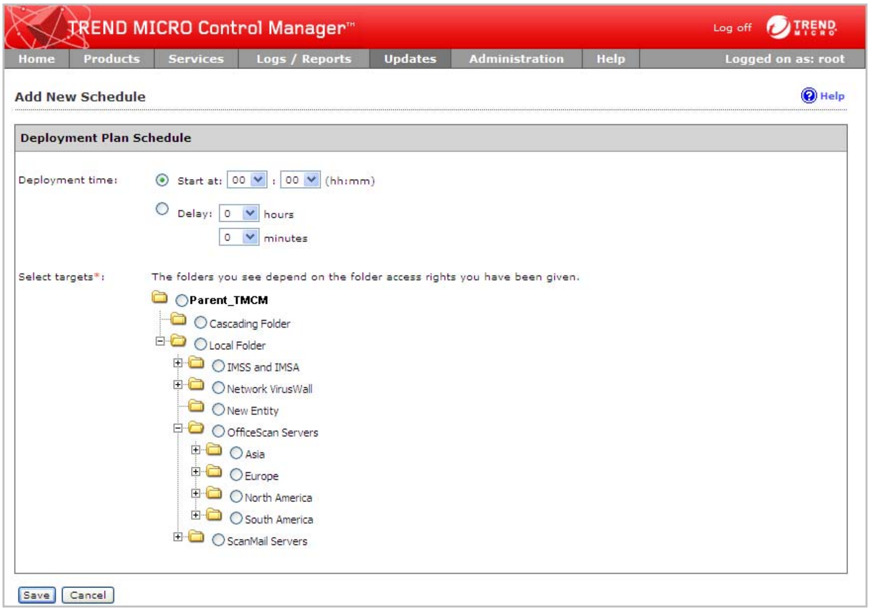
Deployment Plan

Name*:

Deployment Plan Schedules

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

5. 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

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay**: After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at**: Performs the deployment at a specific time

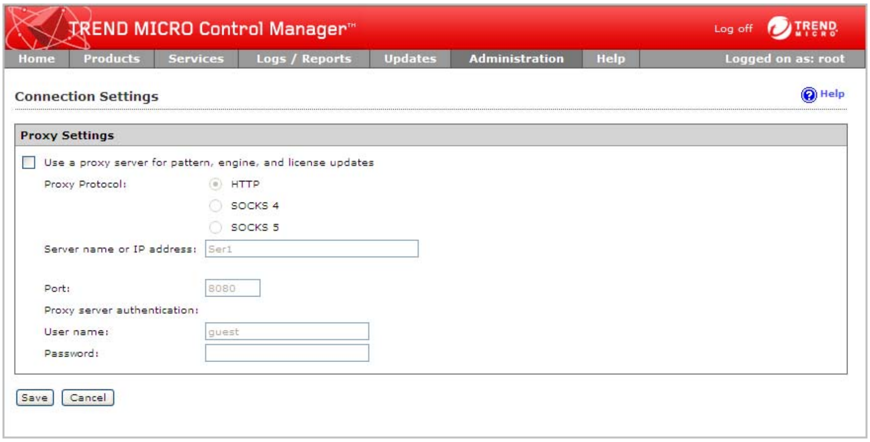
     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Configuring Proxy Settings

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

To configure proxy server settings:

1. Mouseover **Administration**. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.



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: Ser1

Port: 8080

Proxy server authentication:

User name: guest

Password:

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

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server (http://cm5-p.activeupdate.trendmicro.com) or other Internet 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.

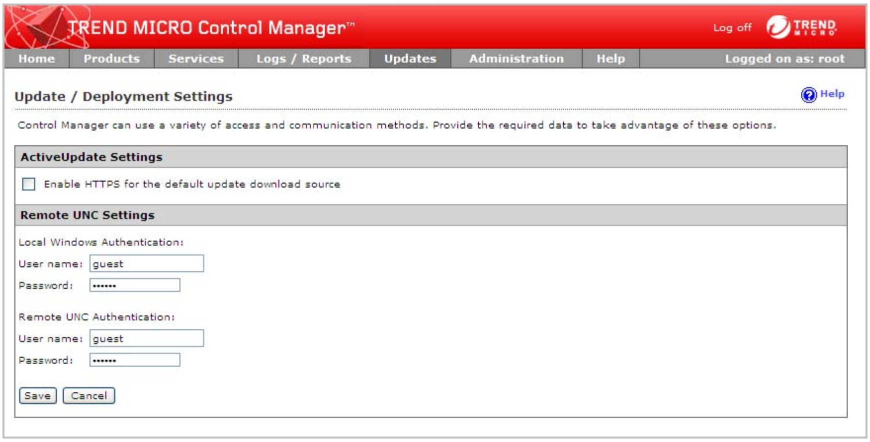
The local Windows authentication refers to the active directory user account in the Control Manager server. The account should have:

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

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

To enable HTTPS download:

1. Mouseover **Updates** from the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Update/Deployment Settings**. The Update/Deployment Settings screen appears.



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: ••••••

Save Cancel

4. Select **Enable HTTPS for the default update download source**.

5. Click **Save**.
6. Access Manual Download or Scheduled Download.
7. On the working area under **Download settings > Source group**, select **Internet: Trend Micro update server** or specify your organizations component source server in the **Other Internet source** field.
8. Click **Save**.

To enable UNC download:

1. Mouseover **Updates** from the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Update/Deployment Settings**. The Update/Deployment Settings screen appears.
4. Type the **Local Windows Authentication** and **Remote UNC Authentication** user names and passwords.
5. Click **Save**.
6. Access Manual Download or Scheduled Download.
7. On the working area under **Download settings > From group**, select **File path** and then specify the shared network folder.
8. 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.

Chapter 6

Monitoring the Control Manager Network

Control Manager provides several options to monitor the Control Manager network. Summary screens, notifications, logs, and reports all provide ways for you to monitor the network.

This chapter contains the following topics:

- *Viewing Summary Screens in Control Manager* on page 6-2
- *Using Command Tracking* on page 6-3
- *Using Event Center* on page 6-8
- *Using Logs* on page 6-23
- *Working With Reports* on page 6-47

Viewing Summary Screens in Control Manager

Control Manager summary screens provide an easy manner for administrators to view managed product component information and network protection information.

Home Screen

Use the Home screen for an at-a-glance summary of the product network Control Manager manages. The Home screen contains the following sections:

TABLE 6-1. Home and Summary Screen Information

SECTION	DESCRIPTION
Antivirus Summary	Displays summary information for all registered managed products with antivirus protection/detection capabilities. For example, OfficeScan, InterScan Messaging Security, or Total Discovery.
Spyware/Grayware Summary	Displays summary information for all registered managed products with spyware/grayware protection/detection capabilities. For example, OfficeScan, InterScan Messaging Security, or Total Discovery.
Content Security Summary	Displays summary information for all registered managed products with content protection/detection capabilities. For example, InterScan Messaging Security, or Total Discovery.
Web Security Summary	Displays summary information for all registered managed products with Web protection/detection capabilities. For example, OfficeScan, InterScan Web Security, or Total Discovery.
Network Virus Summary	Displays summary information for all registered managed products with network virus protection/detection capabilities. For example, Network VirusWall Enforcer, or Total Discovery.
Violation Status	Displays summary information for all clients which violate administrator created policies of Network VirusWall Enforcer.
Component Status	Displays component summary information for all registered managed products. Only component information for products registered to the Control Manager server display. For example, the Control Manager server has only OfficeScan servers, so only OfficeScan components display.

Tip: Clicking the underlined numbers that display in the right-hand column of each table opens a detailed summary screen with information for the row.

Example: In the Antivirus Summary table, clicking the corresponding number for the row **Cleaned** opens a Detailed Information screen. The Detailed Information screen displays information about all the computers that have been cleaned.

Using 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 allows 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 6-2. 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 currently perform the command
All	The total number of managed products and child servers to which Control Manager issued the command

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

Understanding Command Details

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

- Managed products or services involved
- **Started:** Indicates the date and time when the Control Manager server issued the command to the managed product or child server as well as additional command information

  For example, when you invoke a Manual Download, the Issued field will contain the Parameter information about the component the Control Manager was or was not able to download. A Manual Download Command Detail can have a Parameter called "engine". This 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 was not able to perform the command
- **In Progress:** Indicates the number of managed products or child servers that currently perform the command

Understanding Details for Individual Products or Services

- **Last Reported:** Indicates the date and time when the managed product sends a response to the Control Manager server
- **Server/Entity:** Indicates the host name of the child or managed product server
- **Status:** Indicates the status of the issued command

For example, the Status is Skip when you invoke a Deploy patterns/rules to a child server, and the child server already contains the latest pattern file.

These are the Status values:

TABLE 6-3. **Command Details status**

SUCCESSFUL	IN PROGRESS	UNSUCCESSFUL
Skip	Submit	Time Out
Not supported	Tracking	Cancelled
Successful	Accepted	Not Available
		Unsuccessful

- **Description:** Explains the Status

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

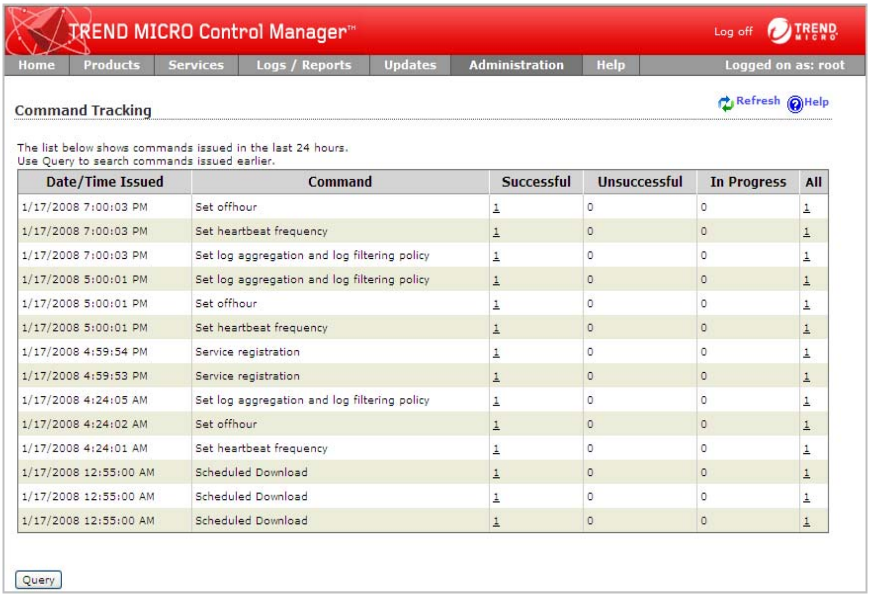
Querying and Viewing Commands

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

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

1. Mouseover **Administration** on the main menu. A drop down menu appears.

2. Click **Command Tracking** from the drop down menu. The Command Tracking screen appears.

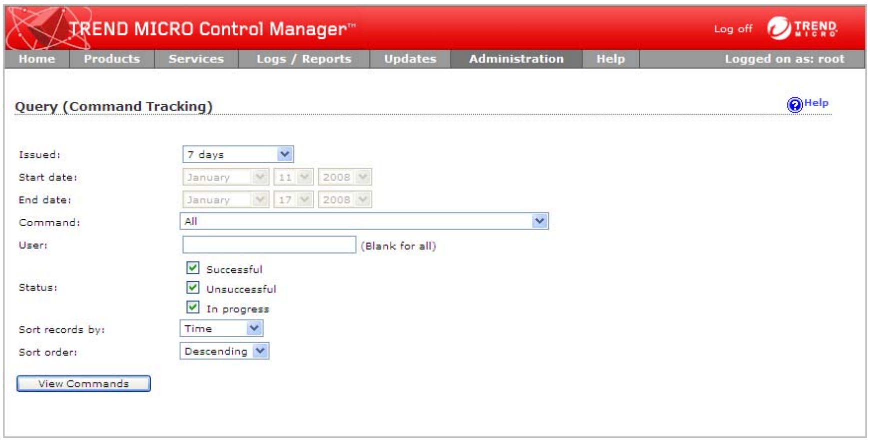


Command Tracking

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

Date/Time Issued	Command	Successful	Unsuccessful	In Progress	All
1/17/2008 7:00:03 PM	Set offhour	1	0	0	1
1/17/2008 7:00:03 PM	Set heartbeat frequency	1	0	0	1
1/17/2008 7:00:03 PM	Set log aggregation and log filtering policy	1	0	0	1
1/17/2008 5:00:01 PM	Set log aggregation and log filtering policy	1	0	0	1
1/17/2008 5:00:01 PM	Set offhour	1	0	0	1
1/17/2008 5:00:01 PM	Set heartbeat frequency	1	0	0	1
1/17/2008 4:59:54 PM	Service registration	1	0	0	1
1/17/2008 4:59:53 PM	Service registration	1	0	0	1
1/17/2008 4:24:05 AM	Set log aggregation and log filtering policy	1	0	0	1
1/17/2008 4:24:02 AM	Set offhour	1	0	0	1
1/17/2008 4:24:01 AM	Set heartbeat frequency	1	0	0	1
1/17/2008 12:55:00 AM	Scheduled Download	1	0	0	1
1/17/2008 12:55:00 AM	Scheduled Download	1	0	0	1
1/17/2008 12:55:00 AM	Scheduled Download	1	0	0	1

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



Query (Command Tracking)

Issued: 7 days

Start date: January 11 2008

End date: January 17 2008

Command: All

User: (Blank for all)

Status: ☑ Successful ☑ Unsuccessful ☑ In progress

Sort records by: Time

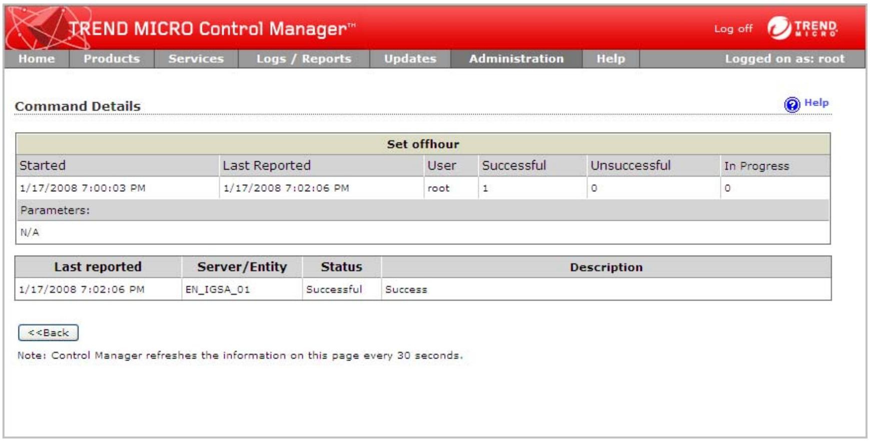
Sort order: Descending

4. On the Query (Command Tracking), specify **values** for the following parameters:
   - **Issued:** Specify the scope of 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 that you want to monitor
   - **User:** 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
5. 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 their Command Details.



Command Details

Set offhour					
Started	Last Reported	User	Successful	Unsuccessful	In Progress
1/17/2008 7:00:03 PM	1/17/2008 7:02:06 PM	root	1	0	0
Parameters:					
N/A					

Last reported	Server/Entity	Status	Description
1/17/2008 7:02:06 PM	EN_IGSA_01	Successful	Success

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

Using Event Center

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

The Event Center categorizes events according to the following types:

TABLE 6-4. Event Center Events

INFORMATION	DESCRIPTION
Alert	Provides warning about viruses/spyware/grayware detected by antivirus managed products. For more information, see Table 6-5, "Alert Events," on page 6-9.
Outbreak Prevention Services	Provides information about policy application and update information about Outbreak Prevention Services (OPS). Outbreak Prevention Services notification types group the following service events: • Active Outbreak Prevention Policy received • Outbreak Prevention Mode started • Outbreak Prevention Mode stopped • Outbreak Prevention Policy update unsuccessful • Outbreak Prevention Policy update successful

TABLE 6-4. Event Center Events

INFORMATION	DESCRIPTION
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 components update results (successful or unsuccessful). For more information, see Table 6-6, “Update Alert Events,” on page 6-10.
Unusual	Provides information about product options or service activation and deactivation. For more information, see Table 6-7, “Unusual Alert Events,” on page 6-10.
Security Violation	Provides warning about email message content violations and client Web violations. For more information, see Table 6-5, “Alert Events,” on page 6-9.

TABLE 6-5. 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 1200)

TABLE 6-5. Alert Events

ALERT	DESCRIPTION
Potential vulnerability attack detected	Applicable to packet scanning products (for example, Network VirusWall 1200)

TABLE 6-6. 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.

TABLE 6-7. 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.

TABLE 6-8. Security Violation Events

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

TABLE 6-8. Security Violation Events

ALERT	DESCRIPTION
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 6-9. Common Notification Message Variables

TAGS	DESCRIPTION
Common variables used by all event notifications	
%cmserver%	Control Manager server host name
%computer%	Network name of the client 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 action result of the action taken by the managed product. Example: successful, further action required

TABLE 6-10. Virus Notification Message Variables

TAGS	DESCRIPTION
Virus variables: Used by alert or Outbreak Prevention Service event notifications	
%egnver%	• Scan engine version. • Used by the alert event category as well as the Active Outbreak Prevention Policy received and Outbreak Prevention Services started notification types. 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 notification types, 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 notification types. 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 notification types, 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.
%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.

TABLE 6-10. Virus Notification Message Variables

TAGS	DESCRIPTION
%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 6-11. Special Notification Message Variables

TAGS	DESCRIPTION
Special variables: Used by Damage Cleanup Services, Network VirusWall 1200, and Vulnerability Assessment task completed-related events	
%action%	Network VirusWall 1200 action (pass, drop, or quarantine) on network virus.
%description%	Error description used by the potential vulnerability attack detected, Damage Cleanup Services task completed, and Vulnerability Assessment task completed events.

Control Manager can send notifications to 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 6-12. Notification Delivery Methods

DELIVERY METHOD	DESCRIPTION
Email	Messages sent to a mailbox belonging to the organization's email message system or to a 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 (Small Network Management Protocol) trap is a method of sending notifications to network administrators that use management 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.

TABLE 6-12. Notification Delivery Methods

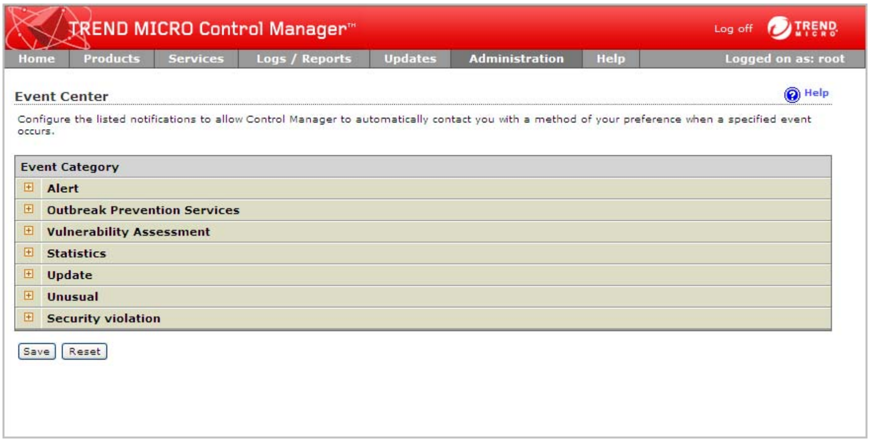
DELIVERY METHOD	DESCRIPTION
Trigger Application	Any in-house or industry-standard application used by your organization to send notification. For example, your organization is using a batch file that calls the net send command. Use the **Parameter** field to define commands applied by the trigger application.
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.
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)

Enabling or Disabling Notifications

Enable or disable notifications from the Event Center screen.

To enable or disable notifications:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.



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

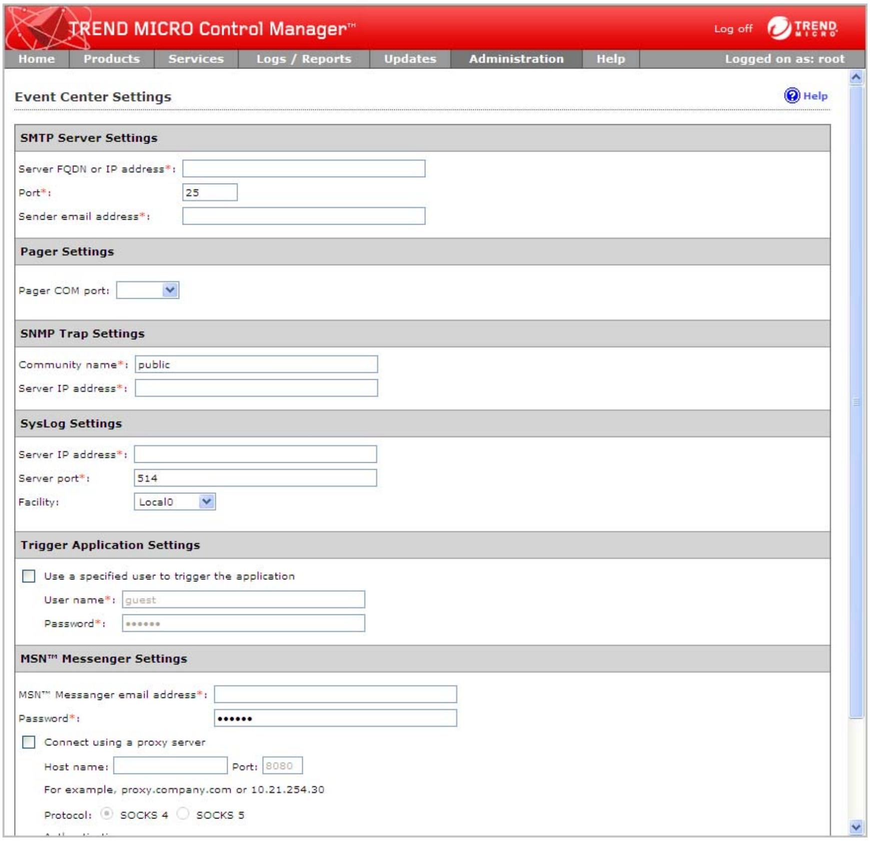
3. Expand the Event Category containing the event notification to enable/disable.
4. Do one of the following:
   - Select/clear specific event check boxes.
   - Select/clear the **Event** check box to select all notifications for an entire section.
5. Click **Save**.

Configuring Notification Methods

Use the Event Center screen to configure notification methods for all notification types.

To configure notification method settings:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **Settings** on the drop down menu. A sub-menu appears.
3. Click **Event Center Settings** from the sub-menu. The Event Center Settings screen appears.



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

4. 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 .Net Passport 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.

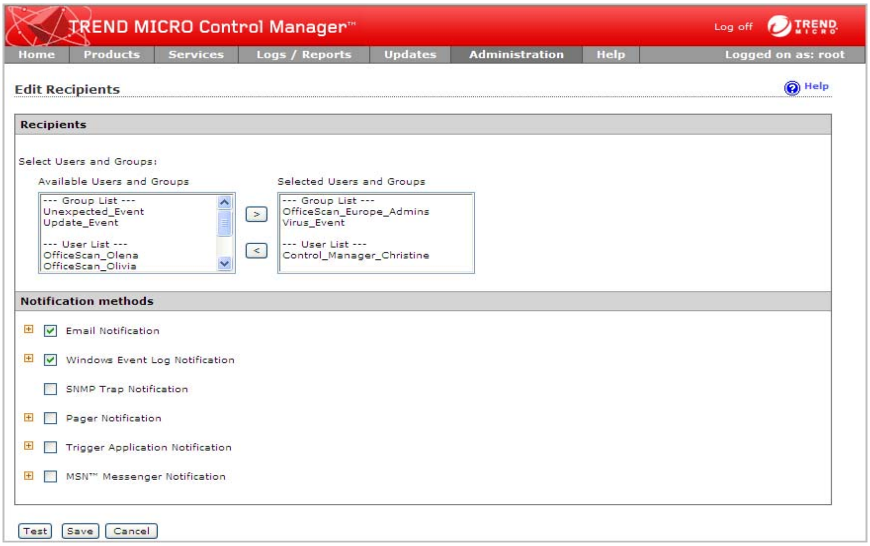
5. Click **Save**.

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:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.
3. Expand the Event Category containing the event notification to configure.
4. Click the **Recipients** link of the event to configure. The Edit Recipients screen appears.



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

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

5. Under Recipients, specify 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.

6. Select the check box of the corresponding **notification method** you prefer:

   Configure the notification method settings through the Event Center Settings screen. Refer to *Configuring Notification Methods* on page 6-15.

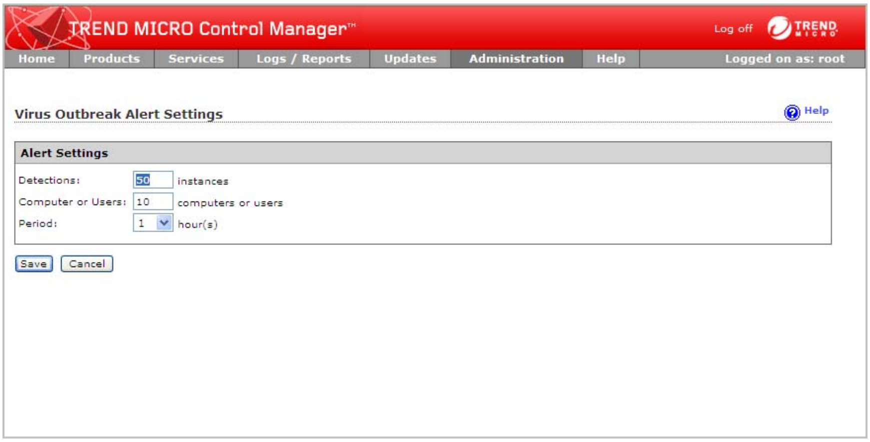
7. Expand the notification method and provide a **notification message** in the corresponding message fields.
8. Click **Test** to experiment if your system is able to deliver the notifications.
9. Click **Save**.

Configuring Virus Outbreak Alert Settings

Outbreak alerts provide a system-wide perspective of the virus/malware outbreak.

To configure virus outbreak alert settings:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.
3. 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)

4. Under Alert Settings, provide the following:
   - **Detections**: The number of viruses that triggers an outbreak alert
   - **Computer or Users:** The number of computers/users infected

- **Period**: The period of consideration for virus count parameter

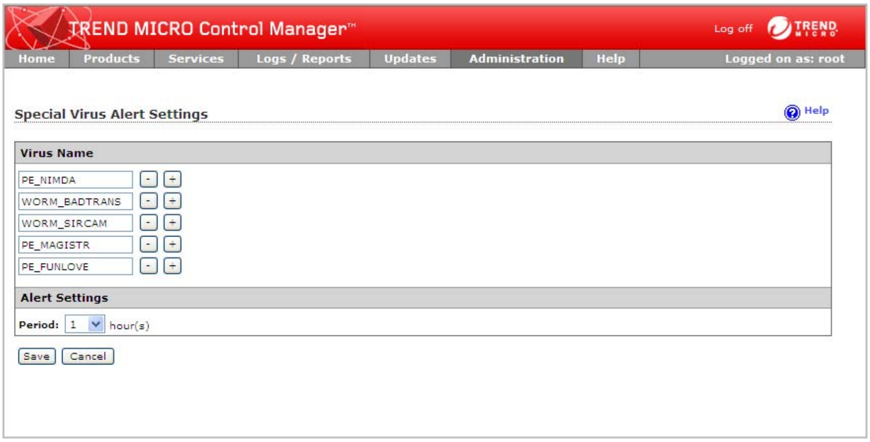
5. Click **Save**.

Configure Special Virus Alert Settings

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.

To configure special virus alert settings:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.
3. 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)

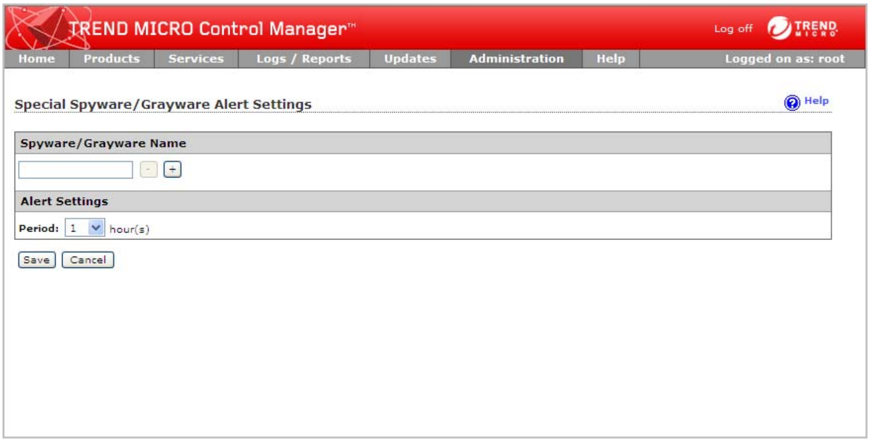
4. Type the **virus names** you want to monitor. You can specify up to 10 viruses.
5. Under Alert Settings, specify the **Period** (in hours) using the drop down list box.
6. Click **Save**.

Configure Special Spyware/Grayware Alert Settings

Configure Control Manager to send notifications whenever it detects spyware/grayware on your system. Special spyware/grayware alert notifications provide an early warning of potential spyware/grayware item.

To configure special spyware/grayware alert settings:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.
3. 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)

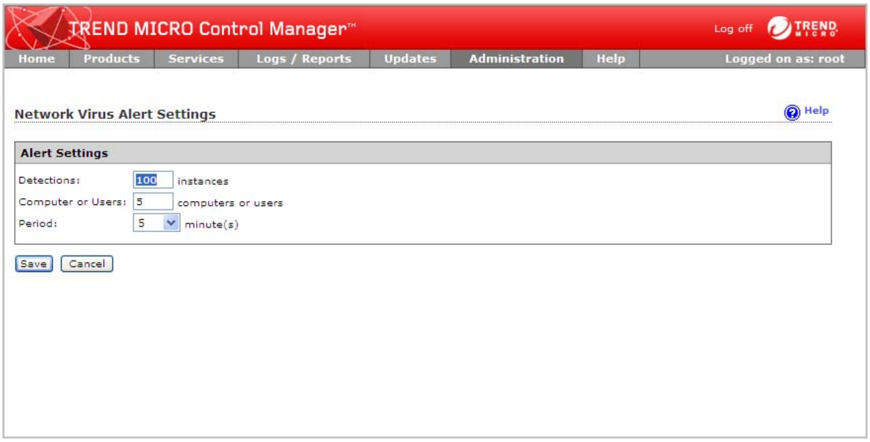
4. Type the spyware/grayware names that you want to monitor. You can list up to 10 items of spyware/grayware.
5. Under Alert Settings, specify the **Period** (in hours) using the drop down list box.
6. Click **Save**.

Configure Network Virus Alert Settings

Network virus alerts provide a system-wide perspective of a potential network virus outbreak.

To configure network virus alert settings:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.
3. 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)

4. Under Alert Settings, provide the following:
   - **Detections**: The number of viruses that triggers an outbreak alert
   - **Computer or Users:** The number of computers/users infected
   - **Period**: The period of consideration for virus count parameter
5. Click **Save**.

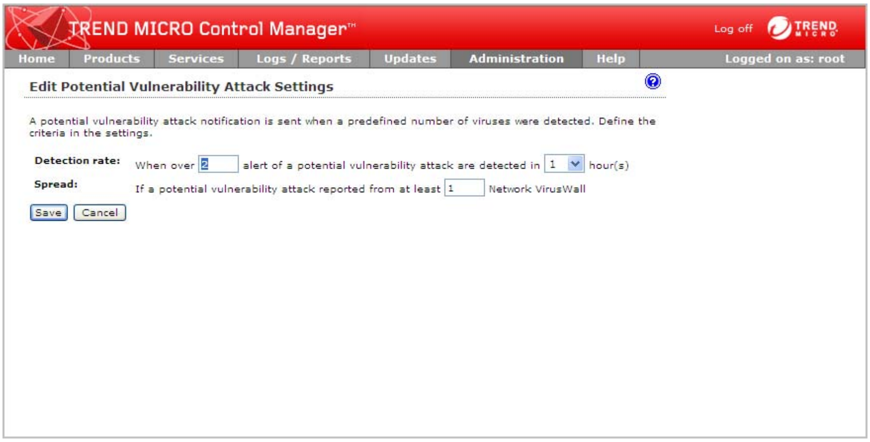
Configure Potential Vulnerability Attack Detected Settings

Potential vulnerability attack alerts provide a system-wide perspective of a potential attack caused by system vulnerabilities.

To configure potential vulnerability attack detected settings:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Event Center** from the drop down menu. The Event Center screen appears.

3. 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

4. Under Alert Settings, provide the following:
   - **Detections**: The number of viruses that triggers an outbreak alert
   - **Computer or Users:** The number of computers/users infected
   - **Period**: The period of consideration for virus count parameter
5. Click **Save**.

Using Logs

Although Control Manager receives data from various log types, Control Manager now allows users to query the log data directly from the Control Manager database. The user 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 server generates two kinds of server logs: Access and System Event.

TABLE 6-13. Control Manager Server Logs

SERVER LOGS	DESCRIPTION
Access logs	These logs record user actions that occur when using the Control Manager management console, including everything from logging on to the console to renaming folders in the Directory.
Server Event logs	These logs record all non-user related events that occur on the Control Manager server.

Understanding Managed Product Logs

Managed product logs provide you with information about the performance of your managed products. You can obtain information for specific or groups of products administered by the parent or child server. With Control Manager's data query on logs and filtering capabilities, administrators can now focus on the information they need.

Aside from the Windows Event log, managed products generate different kinds of logs depending on their function.

TABLE 6-14. Managed Product Logs

SERVER LOGS	DESCRIPTION
Event logs	Refer to actions initiated by either a user or the computer. Query all or any of the following events: • Virus outbreak • Module update • Enabling a service • Disabling a service • Security violation • Unusual network virus behavior

Table 6-14. Managed Product Logs

Server Logs	Description
Security logs- Virus / Web security	Indicate the source of the infection or intrusion, also referred to as the channel. You can view logs according to the type of channels infected: • Content security violation • Virus found in download traffic • Virus found in email messages • Virus found in files • Web security violations • Network security violations
Status logs	Contain information about the environment of a managed product or child server. The Status tab uses this information.

The following table shows the logs that managed products send to Control Manager:

Table 6-15. Control Manager Managed Products Logs

Managed Product	Event Log	Virus/ Spyware/ Grayware Log	Security Log	Web Security Log	Network Virus Log	Status Log	URL Usage	Endpoint Log	Security Violation Log	Security Compliance Log	Security Statistic Log
InterScan eManager	●		●			●					
InterScan Messaging Security Suite	●	●	●			●					
InterScan Web Security Suite	●	●		●		●					

Table 6-15. Control Manager Managed Products Logs

Managed Product	Event Log	Virus/ Spyware/ Grayware Log	Security Log	Web Security Log	Network Virus Log	Status Log	URL usage	Endpoint Log	Security Violation Log	Security Compliance Log	Security Statistic Log
InterScan WebProtect for ICAP	●	●		●		●	●				
InterScan for Cisco CSC SSM	●	●	●	●		●					
OfficeScan	●	●		●		●		●			
ServerProtect	●	●				●					
ServerProtect for Linux	●	●				●					
ScanMail eManager	●		●			●					
ScanMail for Domino/Lotus Notes	●	●				●					
ScanMail for Microsoft Exchange	●	●				●					
Network VirusWall 2500	●				●	●			●	●	●
Network VirusWall 2500 Enforcer	●				●	●			●	●	●
Network VirusWall 1200	●				●	●			●	●	●

TABLE 6-15. Control Manager Managed Products Logs

MANAGED PRODUCT	EVENT LOG	VIRUS/ SPYWARE/ GRAYWARE LOG	SECURITY LOG	WEB SECURITY LOG	NETWORK VIRUS LOG	STATUS LOG	URL USAGE	ENDPOINT LOG	SECURITY VIOLATION LOG	SECURITY COMPLIANCE LOG	SECURITY STATISTIC LOG
Network VirusWall 1200 Enforcer	●				●	●			●	●	●

Tip: More logs mean abundant available information about the Control Manager network. However, these logs occupy disk space. You must balance the need for information with your available system resources.

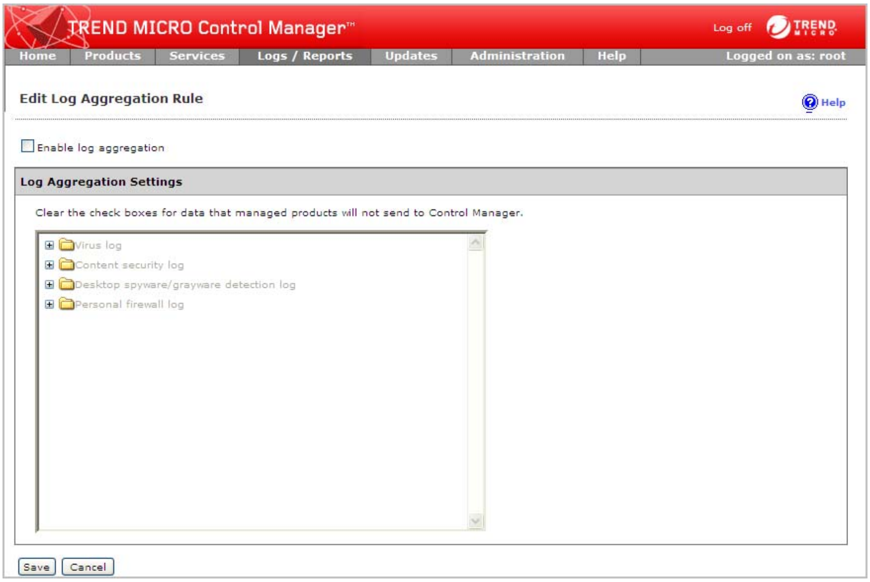
Understanding Log Aggregation

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:

1. Mouseover **Logs/Reports**. A drop down menu appears.
2. Mouseover **Settings** from the drop down menu. A sub-menu appears.
3. Click **Log Aggregation Settings** from the sub-menu. The Log Aggregation Settings screen appears.



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

4. Select **Enable log aggregation**.
5. Clear the check boxes for data that managed products will not send to Control Manager.
6. Click **Save**.

Querying Log Data

Control Manager now supports gathering only the data an administrator needs from Control Manager and managed product logs. Control Manager supports this through the use of Ad Hoc queries. 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). Using Ad Hoc queries to pull data directly from the database provides 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 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 CSV or XML

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 separates Data Views into two major categories: Product Information and Security Threat Information. See *Appendix B: Understanding Data Views* on page B-1 for more information about Data Views. The major categories separate further into several sub-categories, with the sub-categories separated into summary information and detailed information.

The Control Manager Web console displays the Data Views and the information available from each Data View.

TABLE 6-16. Control Manager Major Data View Categories

MAJOR DATA VIEW CATEGORY	DESCRIPTION
Product Information	Displays information about: • Control Manager • Managed products • Managed product components • Product license information
Security Threat Information	Displays information about security threats that managed products detect: • Overall Security Risks • Malware/viruses • Spyware/grayware • Content violations • Spam • Web content violations • Policy/Rule violations • Suspicious threats

Note: For more information about the available data views Control Manager supports, see *Appendix B: Understanding Data Views* on page B-1.

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 for the information. After specifying the data view, users can further narrow their search by specifying filtering criteria for the request.

When performing an Ad Hoc query the user first specifies whether to query the Control Manager server the user is currently logged on to, or to query the managed products the Control Manager manages. The managed products could include other Control Manager Child servers.

After selecting the managed products/directory from which the data originates, select a data view for the query. For more information on data views see *Understanding Data Views* on page 6-29.

After selecting the data view, specify the query filter criteria, the specific information the query displays, and the order in which the information displays.

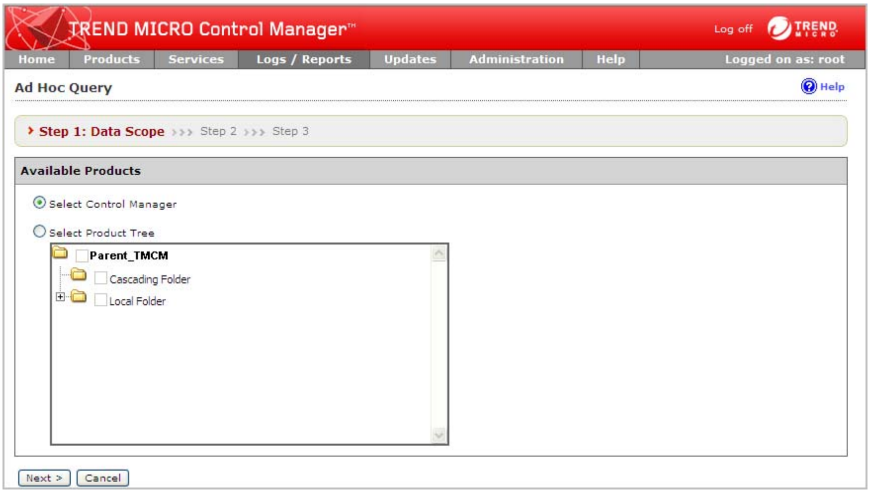
Note: Control Manager supports specifying up to 20 criteria for filtering Ad Hoc Query data.

Finally specify whether to save the query for future use. Control Manager supports sharing of saved queries, so other users can benefit from useful queries.

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 the Control Manager returns meet that criteria.

To perform an Ad Hoc query:

1. Mouseover **Logs/Reports** on the main menu. A drop-down menu appears.
2. Click **New Ad Hoc Query** from the drop-down menu. The Ad Hoc Query screen appears.



Step 1: Specify the Origin of the Information:

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.

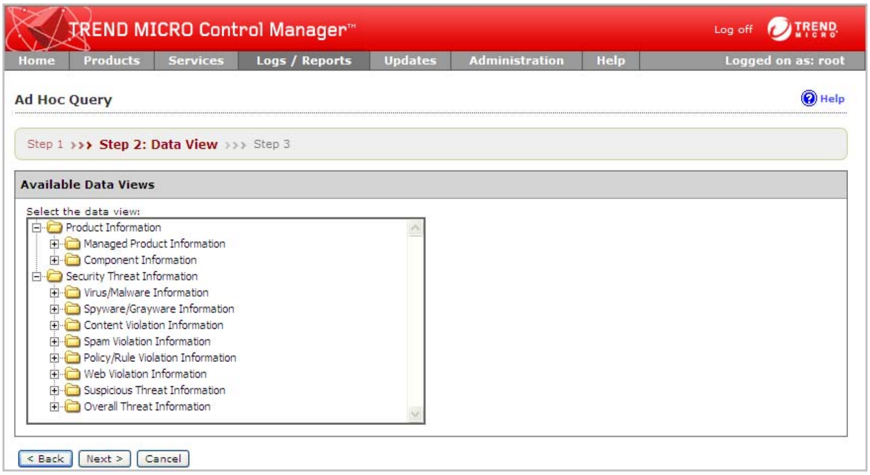
   - **Select Product Tree:** Specifies that information originates from the managed products the Control Manager server manages.

     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 on the following screen.

For example, by selecting OfficeScan in the product directory only data views associated with desktop protection display in the Available Data Views list.

2. Click **Next**. The Select Data View screen appears.



Ad Hoc Query

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

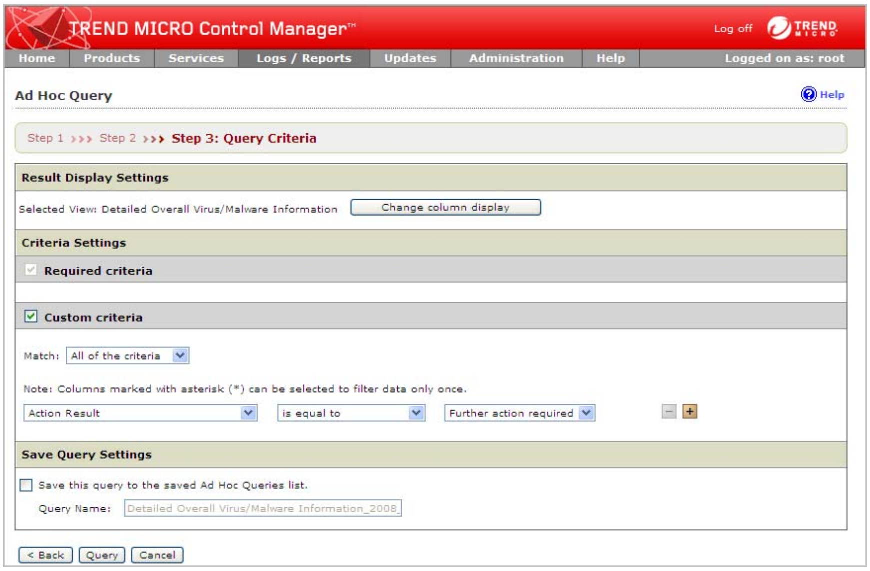
Available Data Views

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 Information
  - Suspicious Threat Information
  - Overall Threat Information

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 6-29.
2. Click **Next**. The Query Criteria screen appears.



Ad Hoc Query

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

Result Display Settings

Selected View: Detailed Overall 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.

Action Result | is equal to | Further action required

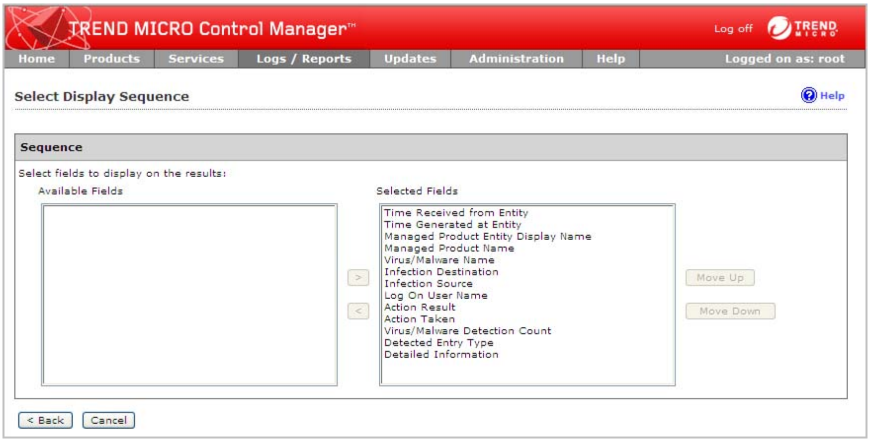
Save Query Settings

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

Query Name: Detailed Overall Virus/Malware Information_2008

Step 3: Specify the Display Sequence:

1. Specify the display and sequence for the information the query returns:
   a. Click **Change column display**. The Select Display Sequence screen appears.



Select Display Sequence

Sequence

Select fields to display on the results:

Available Fields

Selected Fields

Time Received from Entity
Time Generated at Entity
Managed Product Entity Display Name
Managed Product Name
Virus/Malware Name
Infection Destination
Infection Source
Log On User Name
Action Result
Action Taken
Virus/Malware Detection Count
Detected Entry Type
Detailed Information

b. 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.

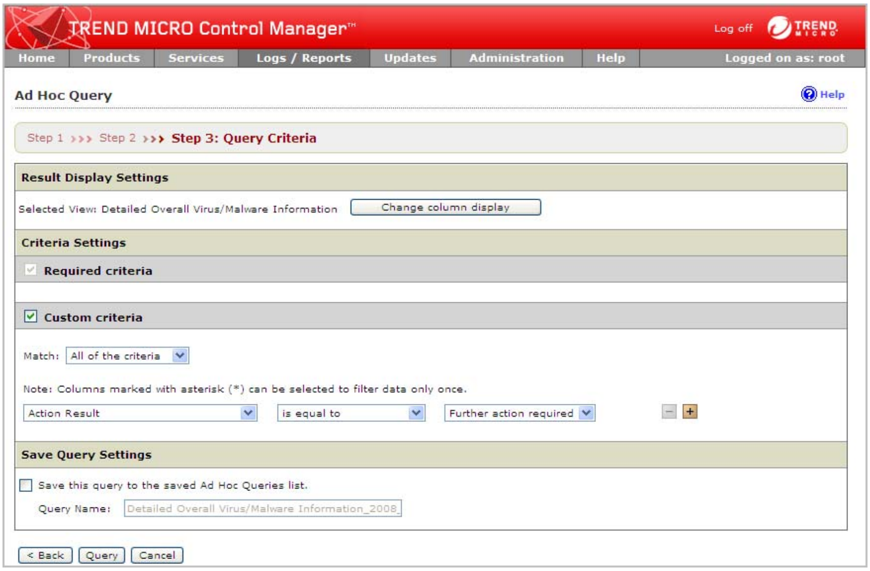
Selecting and adding one column at a time is one method that allows users to specify the sequence which the information displays.

c. Click the **Add** button to include the fields in the **Selected Fields** list. Selected columns appear in the Selected Fields list.

d. Continue selecting and adding columns until you have all the columns you require.

e. 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.

f. Click **Back**. The Query Criteria screen appears.



Ad Hoc Query

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

Result Display Settings

Selected View: Detailed Overall 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.

Action Result | is equal to | Further action required

Save Query Settings

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

Query Name: Detailed Overall Virus/Malware Information_2008

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.

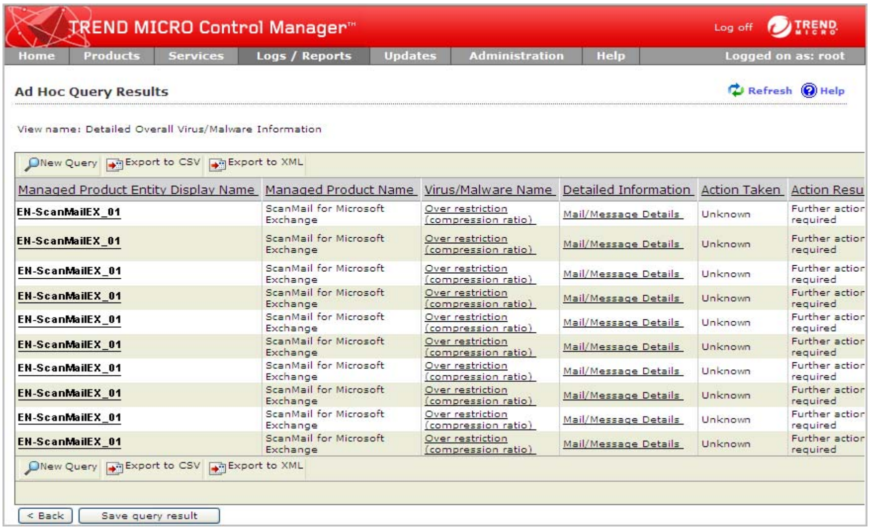
- **i.** From the left-most drop-down list, select the column to filter.
- **ii.** From the middle drop-down list, select the matching condition for the filter.
- **iii.** In the right-most field, provide the filter criteria. A list box or text box appears here depending on the column selected to filter.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

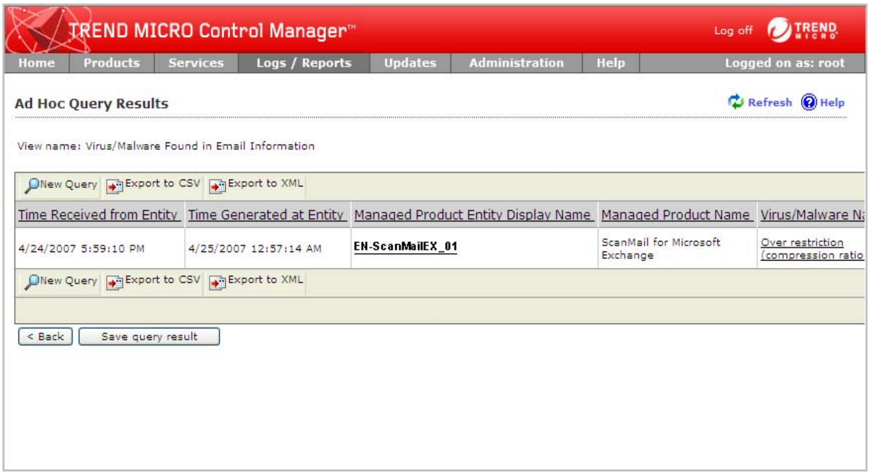


Ad Hoc Query Results

View name: Detailed Overall Virus/Malware Information

Managed Product Entity Display Name	Managed Product Name	Virus/Malware Name	Detailed Information	Action Taken	Action Resu
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required
EN-ScanMailEX_01	ScanMail for Microsoft Exchange	Over restriction (compression ratio)	Mail/Message Details	Unknown	Further actio required

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



Ad Hoc Query Results

View name: Virus/Malware Found in Email Information

Time Received from Entity	Time Generated at Entity	Managed Product Entity Display Name	Managed Product Name	Virus/Malware Na
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

Control Manager supports saving an Ad Hoc query a user creates. Saved Ad Hoc queries appear on the **Logs/Reports > 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

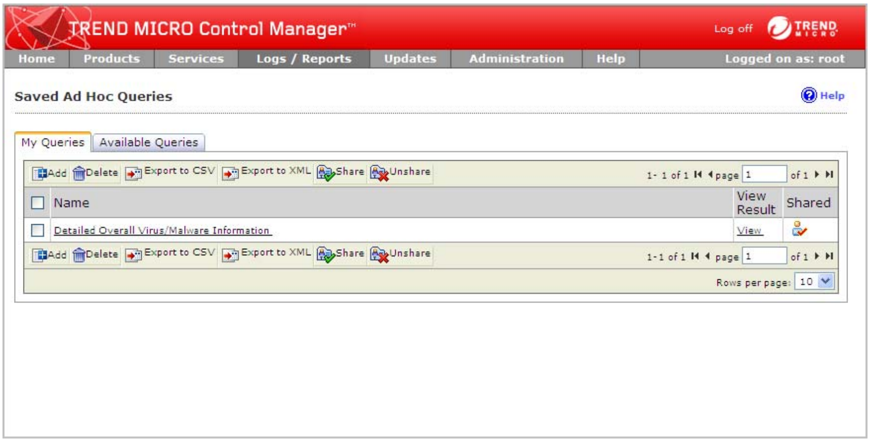
Step 3: Specify filtering criteria, and the specific information that displays

Step 4: Save and complete the query

Step 5: Export the data to CSV or XML

To edit a saved Ad Hoc query:

1. Mouseover Logs/Reports. A drop-down menu appears.
2. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.



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

3. 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 6-29.
2. Click **Next**. The Query Criteria screen appears.

Step 3: Specify the display sequence:

1. Specify the display and sequence for the information the query returns:
   a. Click **Change column display**. The Select Display Sequence screen appears.

   b. 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.

   c. Click the **Add** button to include the fields in the **Selected Fields** list. Selected columns appear in the Selected Fields list.

d. Continue selecting and adding columns until you have all the columns you require.

e. 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.

f. 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:

1. Mouseover **Logs/Reports**. A drop-down menu appears.
2. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.
3. Click the check box for the associated Ad Hoc query to share.
4. 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:

1. Mouseover **Logs/Reports**. A drop-down menu appears.
2. Click **Saved Ad Hoc Queries**. The Saved Ad Hoc Queries screen appears.
3. Click **Available Queries**. The Available Queries tab appears.

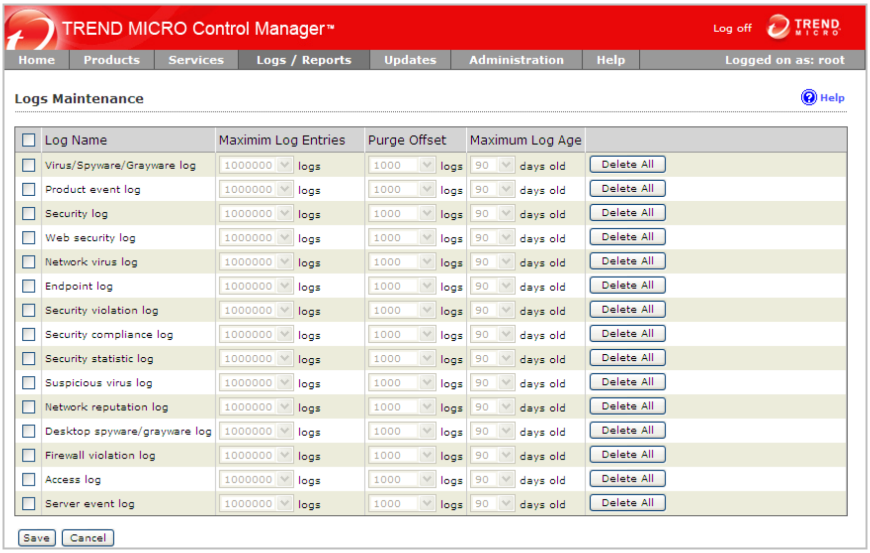
Deleting Logs

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
- Access logs
- Server event logs

To delete logs immediately:

1. Mouseover **Logs/Reports** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A submenu appears.
3. Click **Log Maintenance** from the submenu. The Log Maintenance screen appears.



Logs Maintenance

□	Log Name	Maximim 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
□	Access log	1000000 logs	1000 logs	90 days old	Delete All
□	Server event log	1000000 logs	1000 logs	90 days old	Delete All

4. Select the corresponding check box for the logs you want to delete.
5. 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: 45 to 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:

1. Mouseover **Logs/Reports** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Log Maintenance** from the submenu. The Log Maintenance screen appears.
4. Select the corresponding check box for the logs for which you want to configure settings.

5. Specify the maximum number of logs that Control Manager retains in the **Maximum Log Entries** column.
6. 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.
7. In **Maximum Log Age**, specify the age of logs that Control Manager deletes automatically.
8. Click **Save**.

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 introduces radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control Manager 5.0 continues to support report templates from previous Control Manager versions, however Control Manager 5.0 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 5.0 categorizes report templates according to the following types:

- **Control Manager 5.0 templates:** User-defined customized report templates that use direct database queries (database views) and report template elements (charts/graphs/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 5.0 templates, see *Understanding Control Manager 5.0 Templates* on page 6-47.
- **Control Manager 3.0 templates:** Includes all templates provided in Control Manager 3.0 and Control Manager 3.5. For more information on Control Manager 3.0 templates, see*Understanding Control Manager Report Templates* on page 6-47.

Understanding Control Manager 5.0 Templates

Control Manager 5.0 report templates use database views as the information foundation for reports. For more information on data views, see *Understanding Data Views* on page 6-29. The look and feel of generated reports falls to the report elements. Report elements consist of the following:

TABLE 6-17. Control Manager 5.0 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 graph	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 5.0 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 the Control Manager 5.0 report templates Trend Micro provides the following predefined report templates.

Note: Access the Report Templates screen to view the Trend Micro predefined templates.

TABLE 6-18. Control Manager 5.0 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 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 (Bar chart) • Content Violation Sender Summary (Grid table) • Action Result Summary (Pie chart)
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)

TABLE 6-18. Control Manager 5.0 Pre-defined Templates

TEMPLATE	DESCRIPTION
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)
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)

TABLE 6-18. Control Manager 5.0 Pre-defined Templates

TEMPLATE	DESCRIPTION
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 6-18. Control Manager 5.0 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 6-18. Control Manager 5.0 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) • Virus/Malware Infection Destination Summary (Grid table) • Top 25 Infection Sources (Bar chart) • Virus/Malware Infection Source Summary (Grid table) • Top 25 Infection Destinations (Bar chart) • Virus/Malware Infection Destination Summary (Grid table) • Action Result Summary (Pie chart) • Virus/Malware Action/Result Summary (Grid table)
TM-Web Violation Detection Summary	Provides the following information: • Web Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Client in Violation Count Grouped by Day (Line chart) • URL in Violation Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Overall Web Violation Summary (Grid table) • Top 25 Clients in Violation (Bar chart) • Web Violation Client IP Address Summary (Grid table) • Top 25 URLs in Violation (Bar chart) • Web Violation URL Summary (Grid table) • Filter/Blocking Type Summary (Pie chart)

Understanding Control Manager 3.0 Templates

Trend Micro Control Manager 3.0/3.5 added 65 pre-generated report templates divided into six categories: Desktop, Fileserver, Gateway, Mail Server, Executive Summary, 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 3.0 Report Templates screen to peruse the six categories of reports listed below:

TABLE 6-19. 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
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 6-20. 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 6-21. 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) • Viruses, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month)

TABLE 6-21. Gateway Product Reports and Report Types

GATEWAY PRODUCT REPORTS	REPORT TYPES
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary • OPS deployment rate for IMSS

TABLE 6-22. 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 • Most commonly detected viruses (10, 25, 50, 100) • Top senders of infected email (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 6-23. 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)

TABLE 6-23. Server Based Product Reports and Report Types

SERVER BASED PRODUCT REPORTS	REPORT TYPES
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

TABLE 6-24. Server Based 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 5.0 Report Templates

Control Manager 5.0 templates allow greater flexibility for report generation than previous versions of Control Manager templates. Control Manager 5.0 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 5.0 custom template requires the following steps:

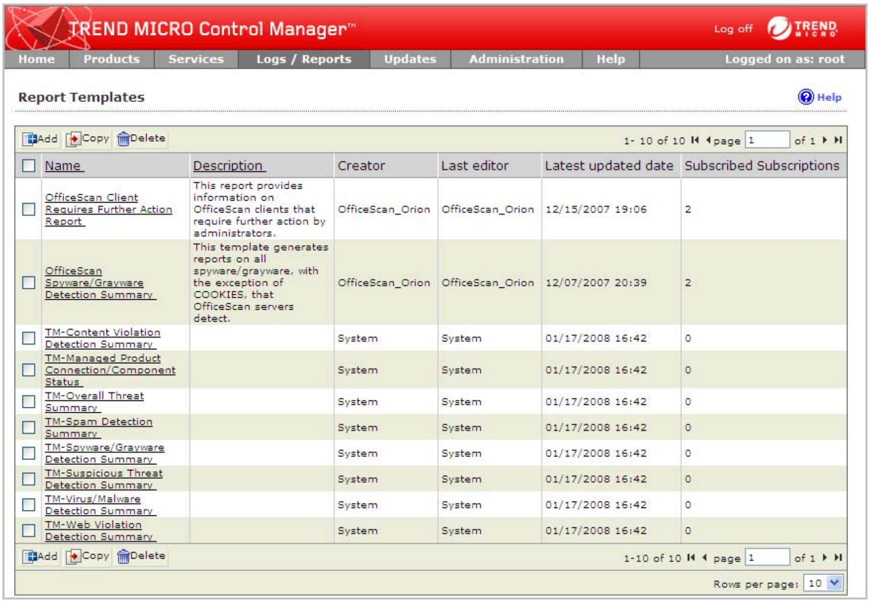
1. Access the Add Report Template screen and name the template.
2. Specify the template component to add to the report template.
3. Specify the data view for the template.

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 5.0 report template:

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

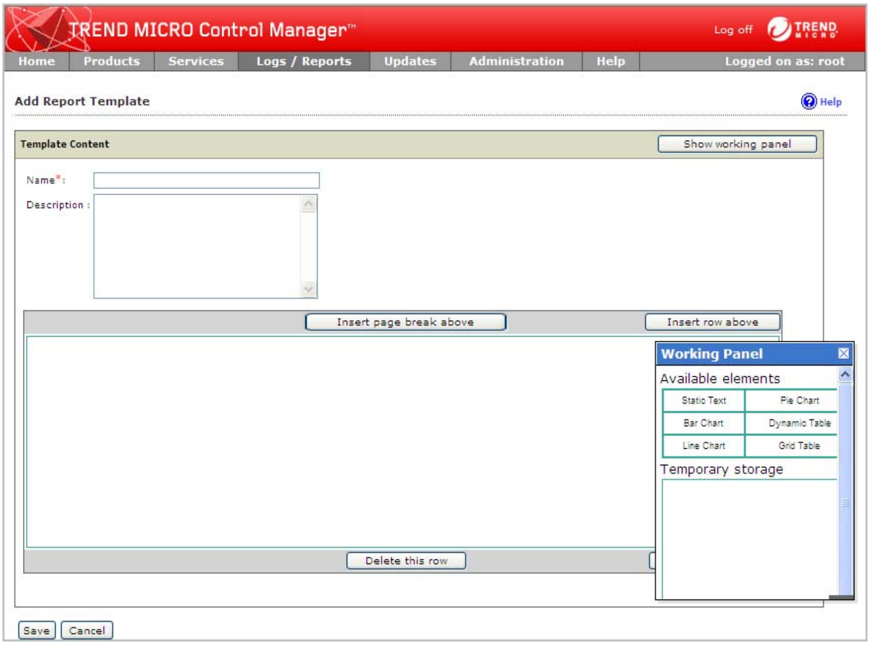
1. Mouseover **Logs/Reports**. A drop-down menu appears.
2. Click **Report Templates** from the menu. The Report Templates screen appears.



Report Templates

□	Name	Description	Creator	Last editor	Latest updated date	Subscribed Subscriptions
□	OfficeScan Client Requires Further Action Report	This report provides information on OfficeScan clients that require further action by administrators.	OfficeScan_Orion	OfficeScan_Orion	12/15/2007 19:06	2
□	OfficeScan Spyware/Grayware Detection Summary	This template generates reports on all spyware/grayware, with the exception of COOKIES, that OfficeScan servers detect.	OfficeScan_Orion	OfficeScan_Orion	12/07/2007 20:39	2
□	TM-Content Violation Detection Summary		System	System	01/17/2008 16:42	0
□	TM-Managed Product Connection/Component Status		System	System	01/17/2008 16:42	0
□	TM-Overall Threat Summary		System	System	01/17/2008 16:42	0
□	TM-Spam Detection Summary		System	System	01/17/2008 16:42	0
□	TM-Spyware/Grayware Detection Summary		System	System	01/17/2008 16:42	0
□	TM-Suspicious Threat Detection Summary		System	System	01/17/2008 16:42	0
□	TM-Virus/Malware Detection Summary		System	System	01/17/2008 16:42	0
□	TM-Web Violation Detection Summary		System	System	01/17/2008 16:42	0

3. Click **Add**. The Add Report Template screen appears.



4. Type a name for the report template in the **Name** field, under Report template.
5. Type a description for the report template in the **Description** field, under Report template.

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:

Note: For every component except Static text, the Add Database View > Step 1: Set Query Criteria screen appears. Selecting Static text opens the Add Static Text screen.

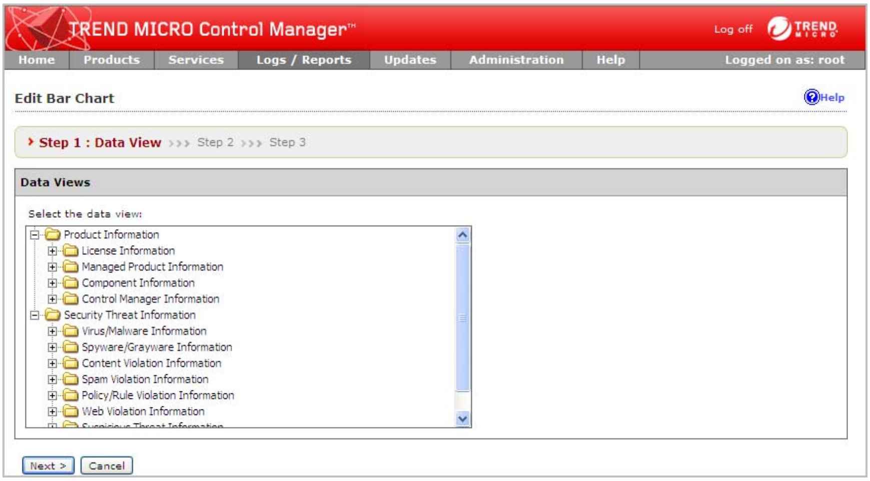
- **Bar chart:** Report data displays in a bar chart
- **Pie chart:** Report data displays in a pie chart
- **Dynamic table:** Report data displays in a table similar to a pivot table

- **Grid table:** Report data displays in a table like an Ad Hoc Query table
- **Line chart:** Report data displays in a line chart
- **Static text:** Text a user inserts into the template. This could be a summary of the information that the report presents.

2. Add multiple components to make the report comprehensive. You can add up to 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> screen appears.



Edit Bar Chart

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

Data Views

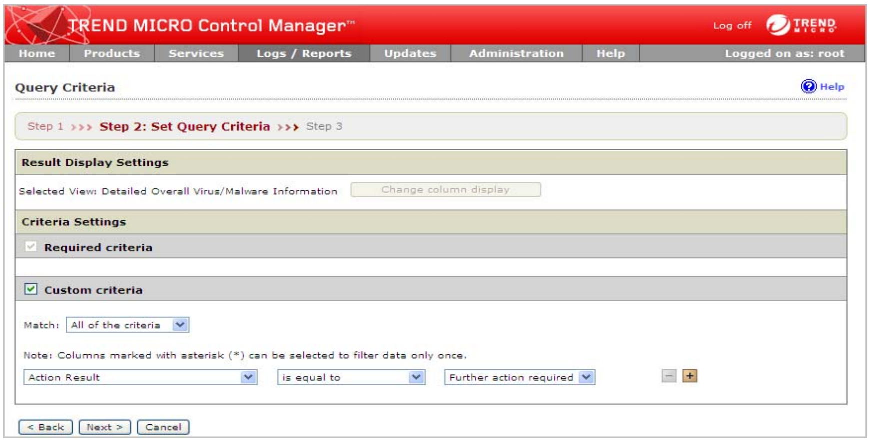
Select the data view:

- 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 Information
  - Suspicious Threat Information

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

   For more information on Data Views, see *Appendix B: Understanding Data Views* on page B-1.

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



Query Criteria

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

Result Display Settings

Selected View: Detailed Overall 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.

Action 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

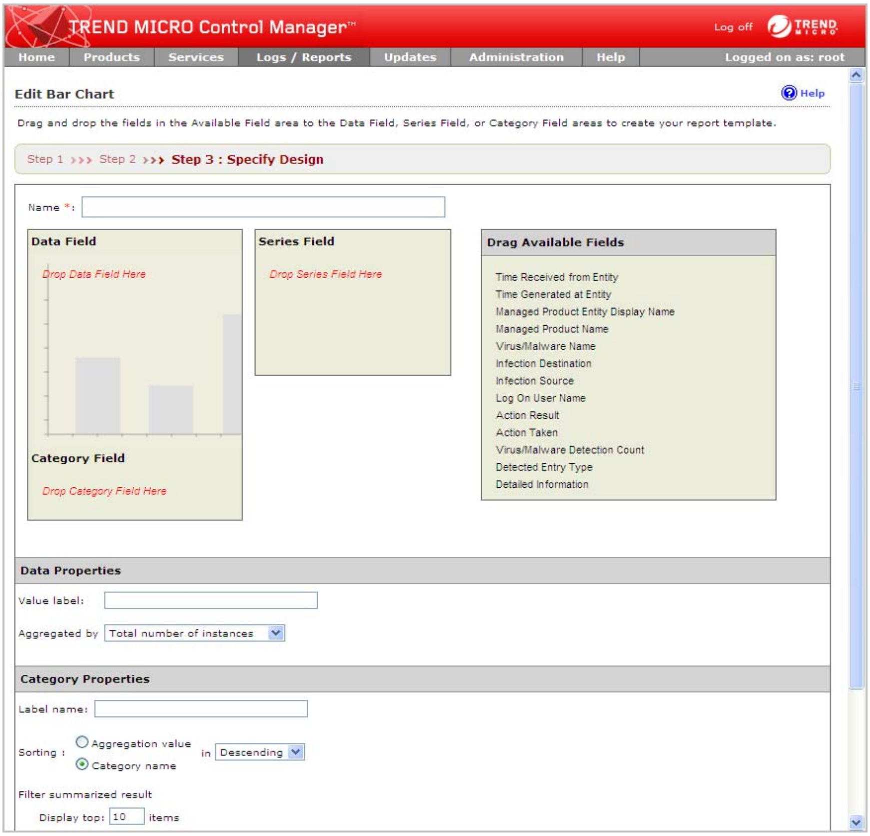
Depending on the selection for the report element specify the data to display in reports:

- Bar chart
- Pie chart

- Dynamic table
- Grid table
- Line chart

Configure bar chart settings:

1. Click **Query**. 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

Drop Data Field Here

Category Field

Drop Category Field Here

Series Field

Drop Series Field Here

Drag Available Fields

Time Received from Entity
Time Generated at Entity
Managed Product Entity Display Name
Managed Product Name
Virus/Malware Name
Infection Destination
Infection Source
Log On User Name
Action Result
Action Taken
Virus/Malware Detection Count
Detected Entry Type
Detailed Information

Data Properties

Value label:

Aggregated by: Total number of instances

Category Properties

Label name:

Sorting : ○ Aggregation value ● Category name in Descending

Filter summarized result

Display top: 10 items

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:

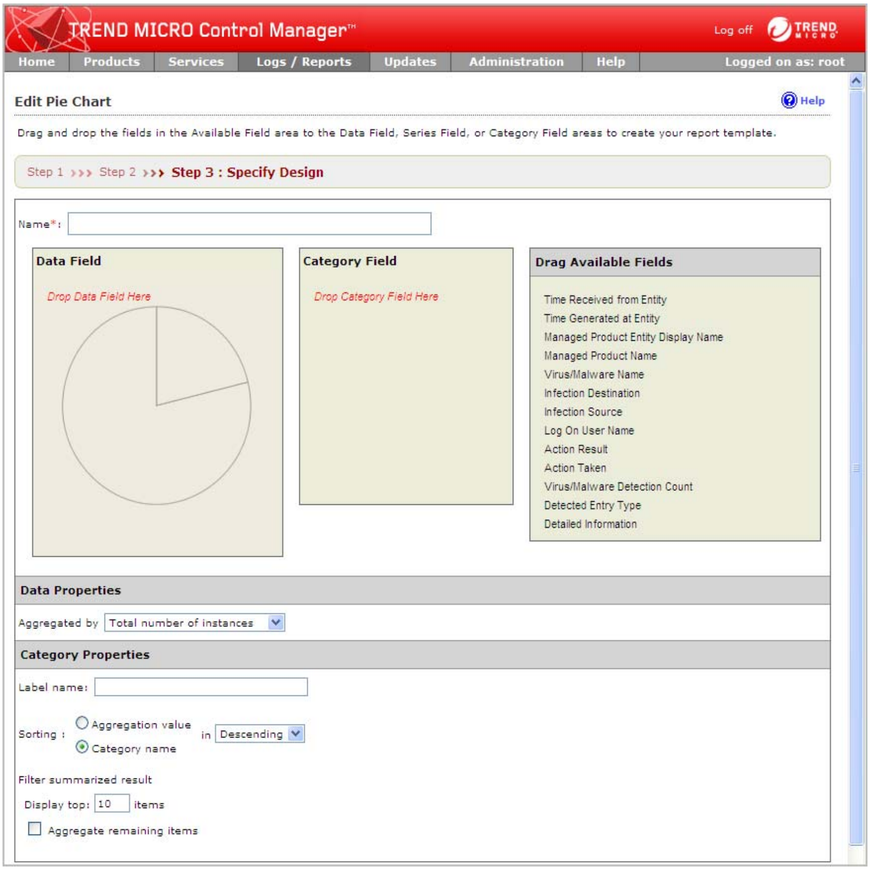
      - **Aggregation value:** Specifies data sorts from the data appearing in the Category fields.
      - **Category name:** Specifies data sorts from the alphabetical value of Category names.
      - **Ascending:** Specifies data sorts in ascending order.
      - **Descending:** Specifies data sorts in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

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

Configure pie chart settings:

1. Click **Query**. 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*:

Data Field

Category Field

Drag Available Fields

- Time Received from Entity
- Time Generated at Entity
- Managed Product Entity Display Name
- Managed Product Name
- Virus/Malware Name
- Infection Destination
- Infection Source
- Log On User Name
- Action Result
- Action Taken
- Virus/Malware Detection Count
- Detected Entry Type
- Detailed Information

Data Properties

Aggregated by: Total number of instances

Category Properties

Label name:

Sorting : ○ Aggregation value ● Category name in Descending

Filter summarized result

Display top: 10 items

□ Aggregate remaining items

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

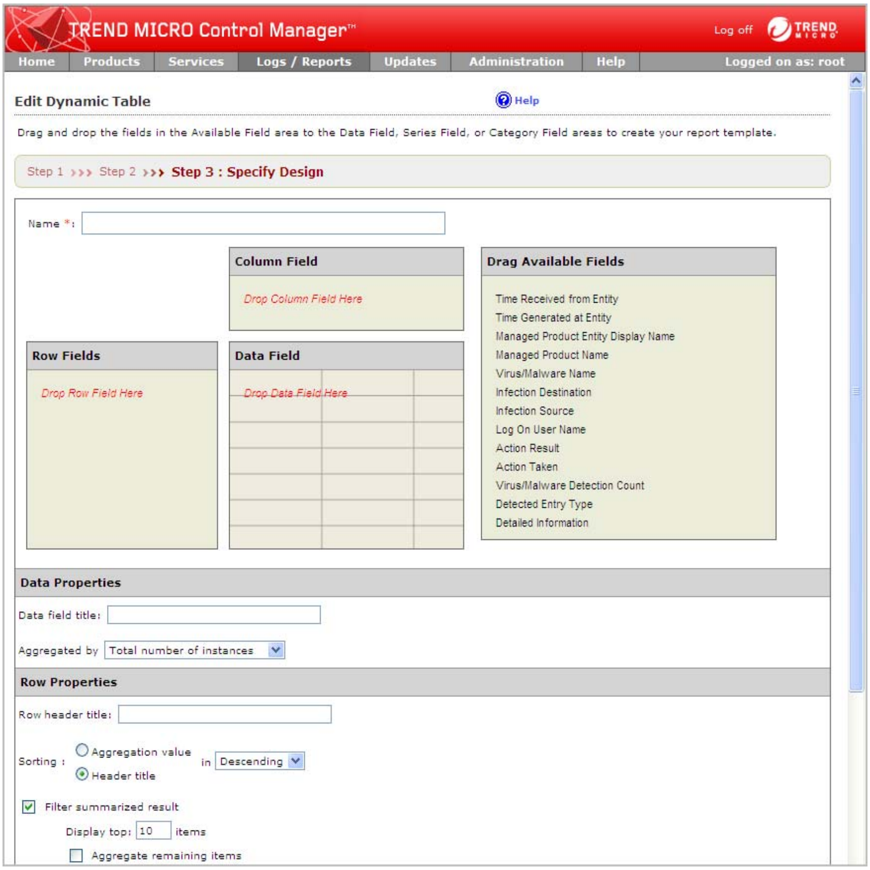
Example: To provide a graph that displays virus distribution across your network Data Fields would represent the total number of viruses in your network. Category Fields would represent how the total number of viruses would be broken down as a percentage.

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

Configure dynamic table settings:

1. Click **Query**. 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

Drag Available Fields
Time Received from Entity
Time Generated at Entity
Managed Product Entity Display Name
Managed Product Name
Virus/Malware Name
Infection Destination
Infection Source
Log On User Name
Action Result
Action Taken
Virus/Malware Detection Count
Detected Entry Type
Detailed Information

Row Fields
Drop Row Field Here

Data Field
Drop Data Field Here

Data Properties

Data field title:

Aggregated by: Total number of instances

Row Properties

Row header title:

Sorting : ○ Aggregation value ● Header title in Descending

☑ Filter summarized result

Display top: 10 items

☐ Aggregate remaining items

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 Overall 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: Virus/Malware Detection Count
- Row Properties: Virus/Malware Name and Action Taken
- Column Properties: Infection Destination

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.

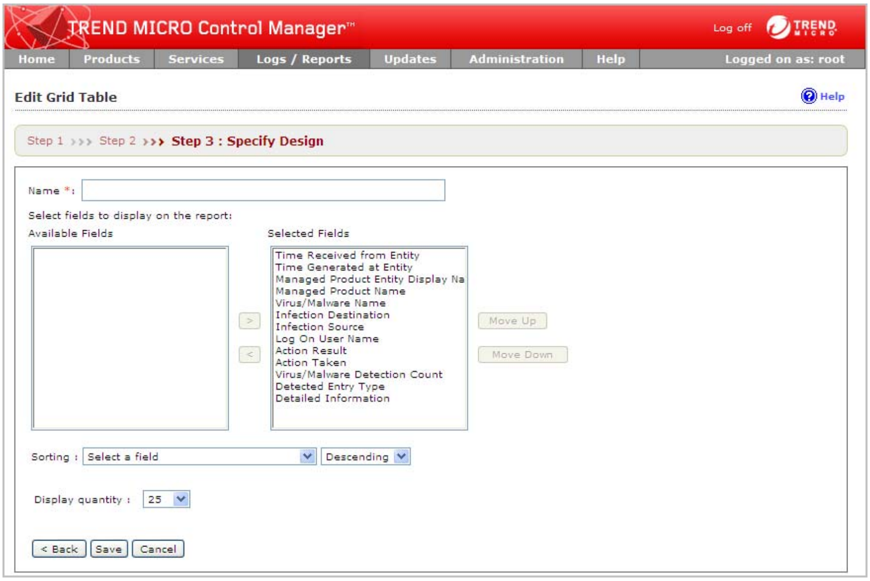
- **Header title:** Specifies data sorts from the alphabetical value of columns.
- **Ascending:** Specifies data sorts in ascending order.
- **Descending:** Specifies data sorts in descending order.

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 grid table settings:

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



Edit Grid Table

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

Name *:

Select fields to display on the report:

Available Fields

Selected Fields

Time Received from Entity
Time Generated at Entity
Managed Product Entity Display Na
Managed Product Name
Virus/Malware Name
Infection Destination
Infection Source
Log On User Name
Action Result
Action Taken
Virus/Malware Detection Count
Detected Entry Type
Detailed Information

Sorting : Select a field | Descending

Display quantity : 25

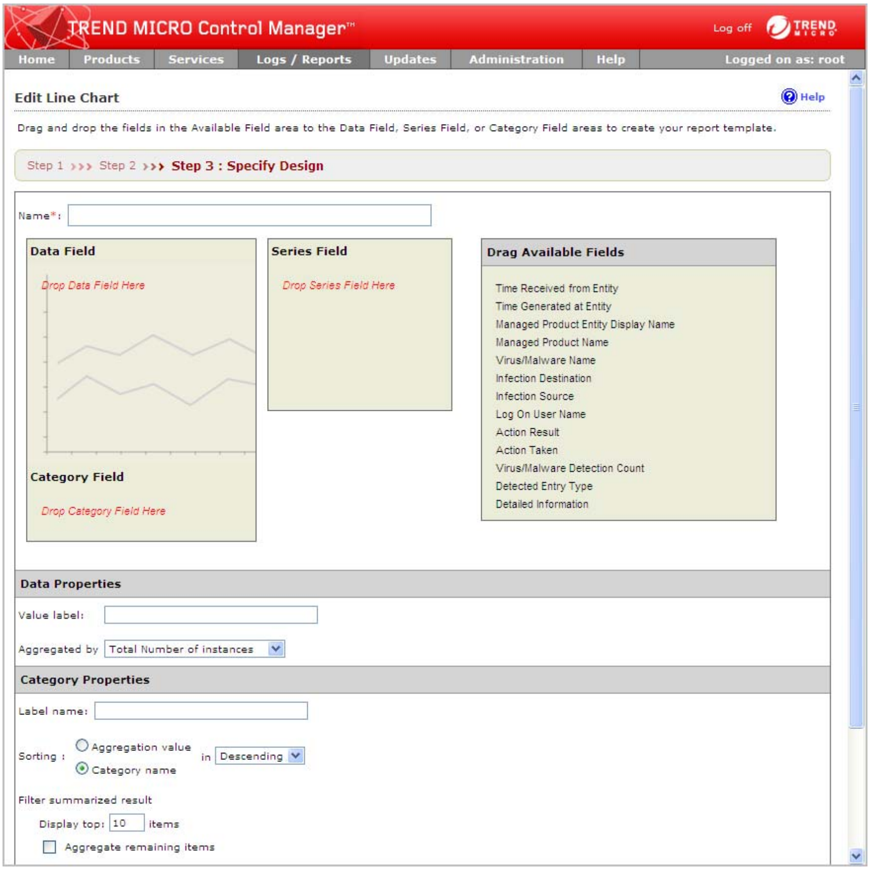
a. Type a name for the table in the **Name** field.

b. Specify which columns appear in the table and in which order the columns appear.

c. 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

Series Field

Drop Series Field Here

Category Field

Drop Category Field Here

Drag Available Fields

- Time Received from Entity
- Time Generated at Entity
- Managed Product Entity Display Name
- Managed Product Name
- Virus/Malware Name
- Infection Destination
- Infection Source
- Log On User Name
- Action Result
- Action Taken
- Virus/Malware Detection Count
- Detected Entry Type
- Detailed Information

Data Properties

Value label:

Aggregated by: Total Number of instances

Category Properties

Label name:

Sorting : ○ Aggregation value ● Category name in Descending

Filter summarized result

Display top: 10 items

□ Aggregate remaining items

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 Overall 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: Virus/Malware Detection Count
- Row Properties: Virus/Malware Name
- Column Properties: Time Generated at Entity

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 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.

7. 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

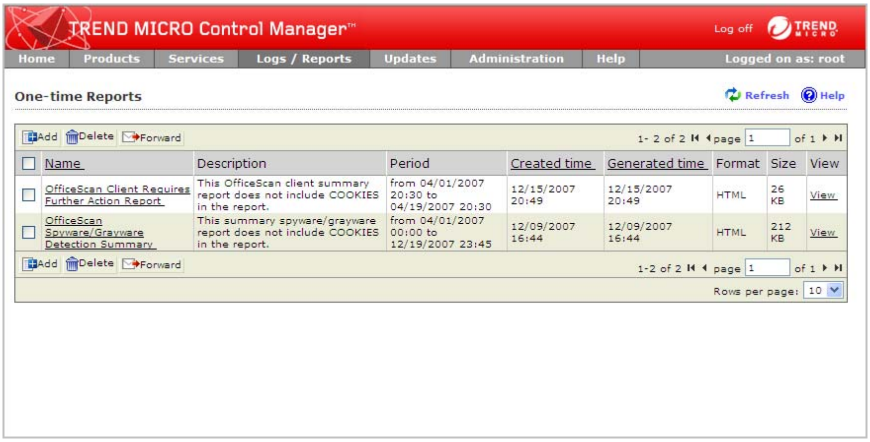
Control Manager supports generating one-time reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 report templates. The process for creating a one-time report is similar for 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:

1. Mouseover **Logs/Reports**. A drop down menu appears.
2. Click **One-time Report** from the menu. The One-time Reports screen appears.



One-time Reports

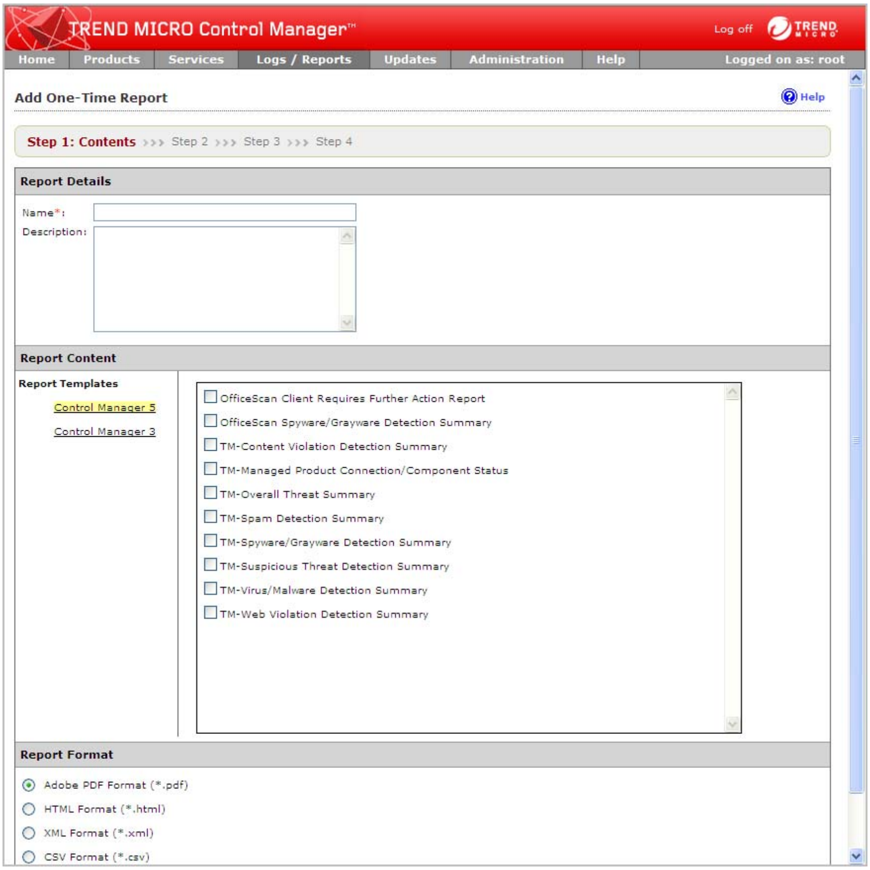
1- 2 of 2 page 1 of 1

☐	Name	Description	Period	Created time	Generated time	Format	Size	View
☐	OfficeScan Client Requires Further Action Report	This OfficeScan client summary report does not include COOKIES in the report.	from 04/01/2007 20:30 to 04/19/2007 20:30	12/15/2007 20:49	12/15/2007 20:49	HTML	26 KB	View
☐	OfficeScan Spyware/Grayware Detection Summary	This summary spyware/grayware report does not include COOKIES in the report.	from 04/01/2007 00:00 to 12/19/2007 23:45	12/09/2007 16:44	12/09/2007 16:44	HTML	212 KB	View

1-2 of 2 page 1 of 1

Rows per page: 10

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



Add One-Time Report

Help

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)

4. Type a name for the report in the **Name** field, under Report Details.
5. Type a description for the report in the **Description** field, under Report Details.
6. Select the Control Manager template to generate the report:

   Control Manager 5.0 report template:

   a. Select the Control Manager 5.0 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 5.0 Report Templates* on page 6-57 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.

7. Select the report generation format:

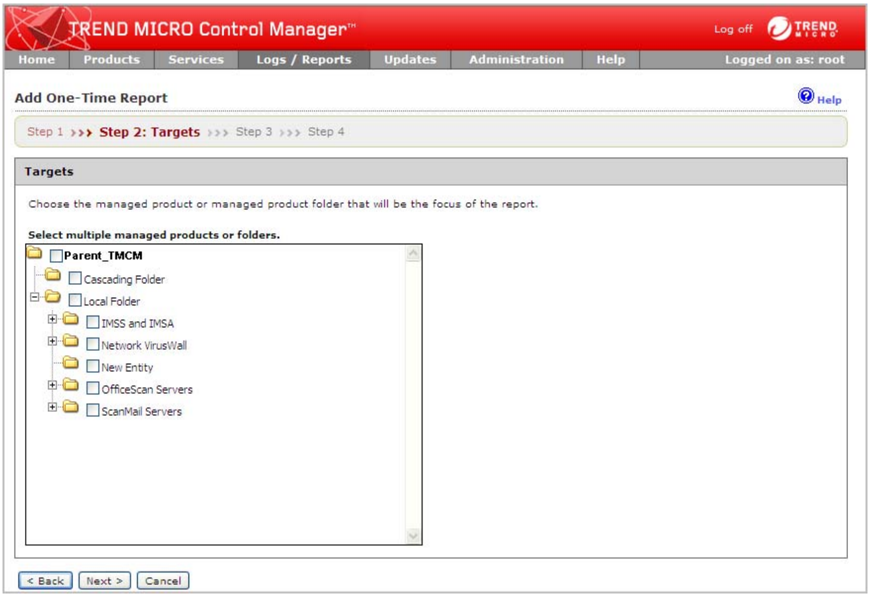
   Control Manager 5.0 report formats:

   - 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)

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



Add One-Time Report

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

Targets

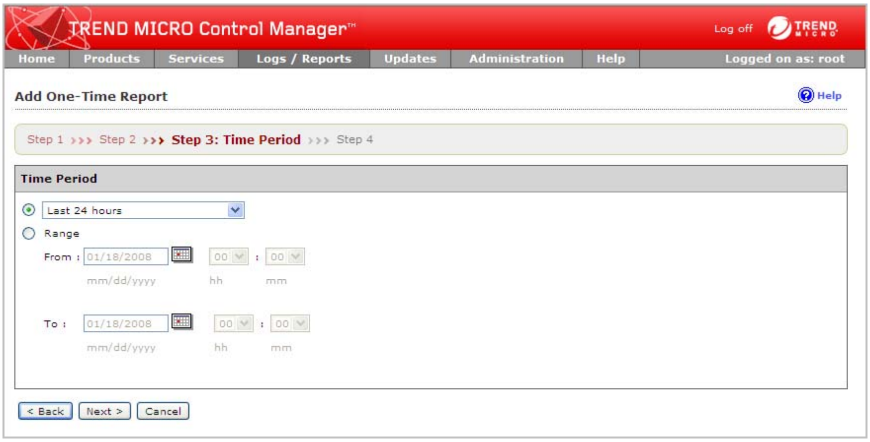
Choose the managed product or managed product folder that will be the focus of the report.

Select multiple managed products or folders.

- □ **Parent_TMCM**
  - □ 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: Time Period screen appears.



Add One-Time Report

Step 1 >>> Step 2 >>> **Step 3: Time Period** >>> Step 4

Time Period

● Last 24 hours

○ Range

From : 01/18/2008 mm/dd/yyyy 00 hh : 00 mm

To : 01/18/2008 mm/dd/yyyy 00 hh : 00 mm

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.

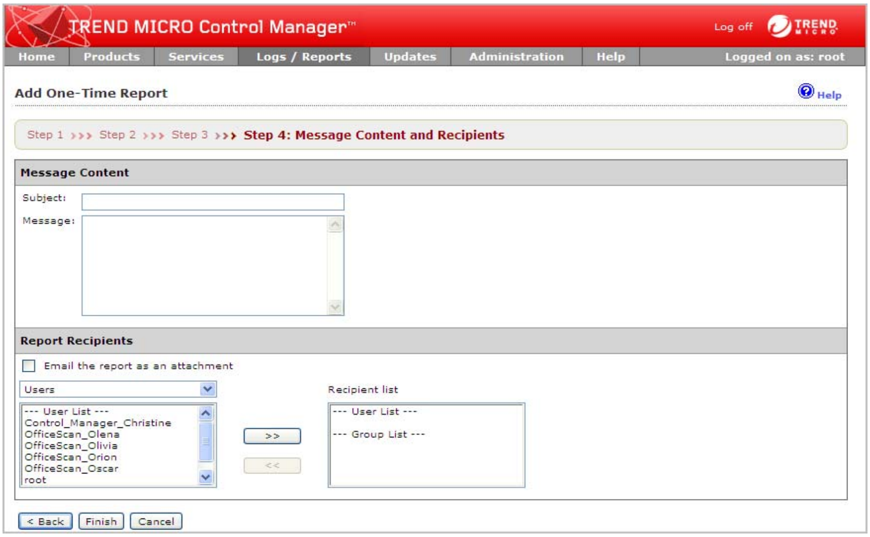
b. Specify a time in the accompanying **hh** and **mm** fields.

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.



--- 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

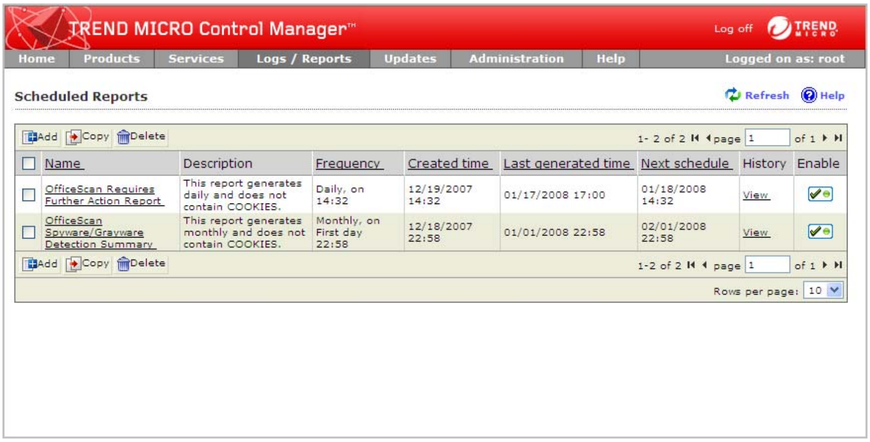
Control Manager supports generating scheduled reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 report templates. The process for creating a scheduled report is similar for 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:

1. Mouseover **Logs/Reports**. A drop down menu appears.
2. Click **Scheduled Reports** from the menu. The Scheduled Reports screen appears.



Scheduled Reports

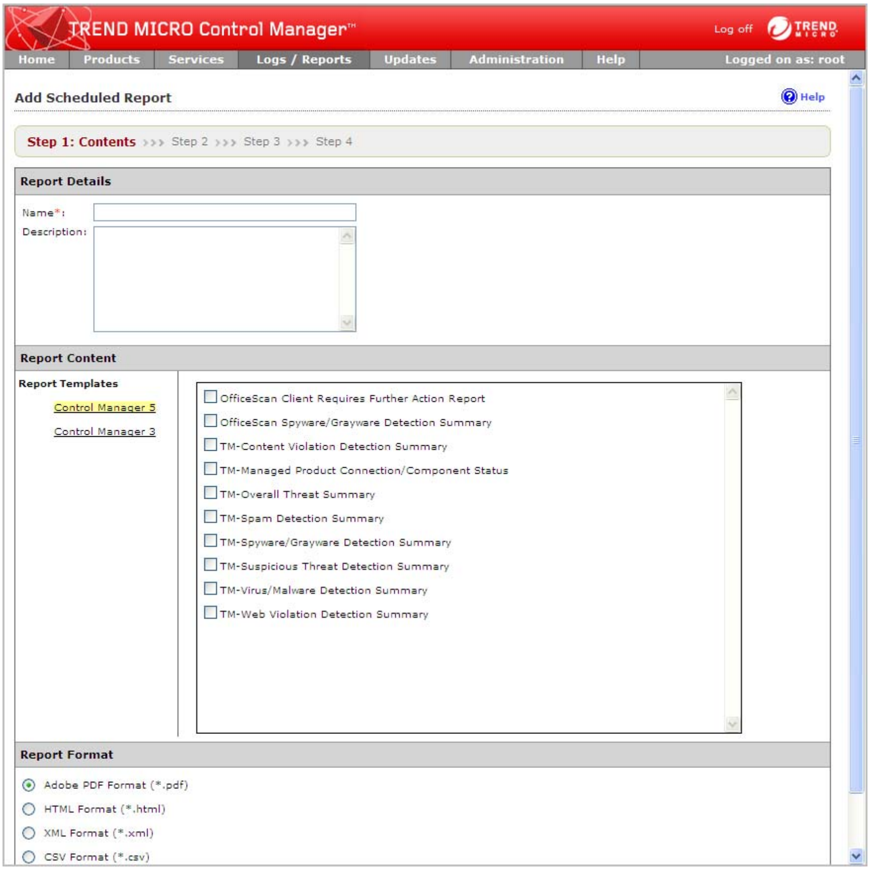
1- 2 of 2 page 1 of 1

□	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

3. 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)

4. Type a name for the report in the **Name** field, under Report Details.
5. Select the Control Manager template to generate the report:

   Control Manager 5.0 report template:

   a. Select the Control Manager 5.0 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 5.0 Report Templates* on page 6-57 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:

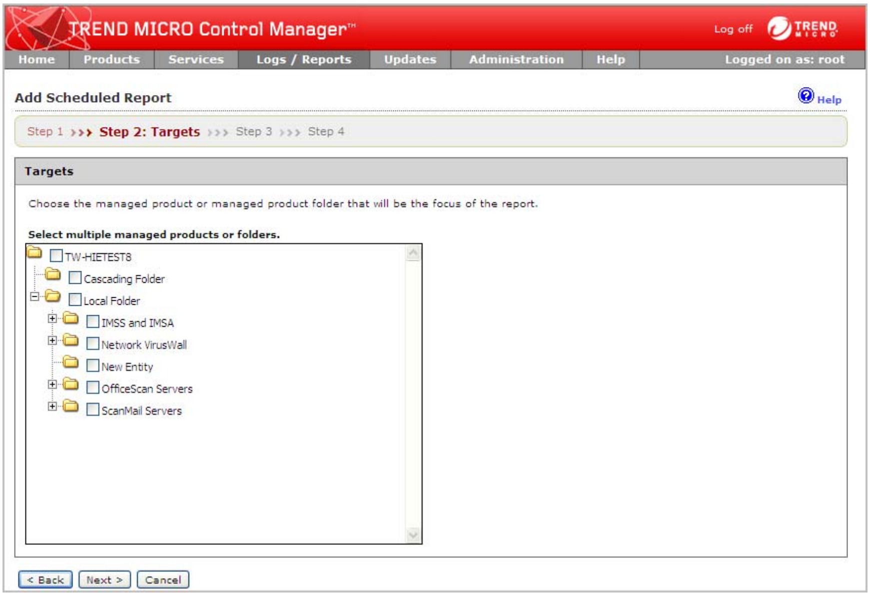
Control Manager 5.0 report formats:

- 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

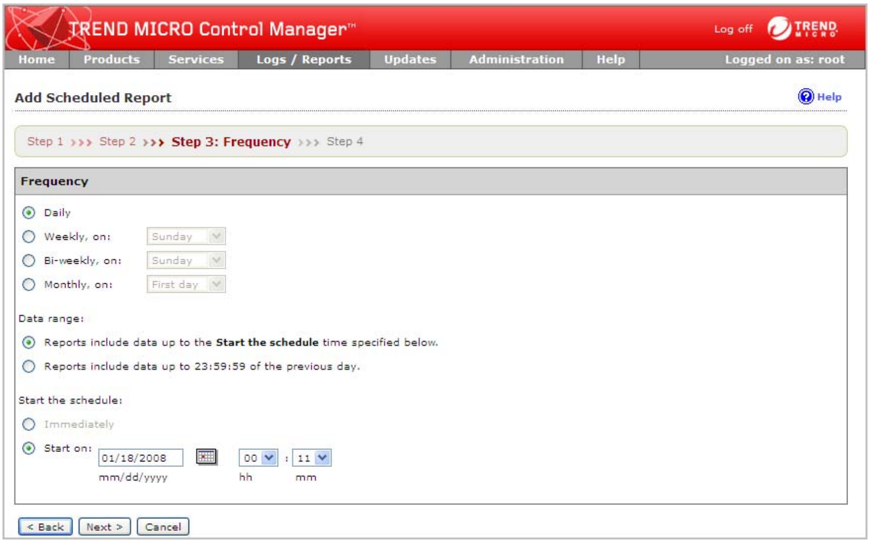
Choose the managed product or managed product folder that will be the focus of the report.

Select multiple managed products or folders.

- □ TW-HIETEST8
  - □ 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: Time Period 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.

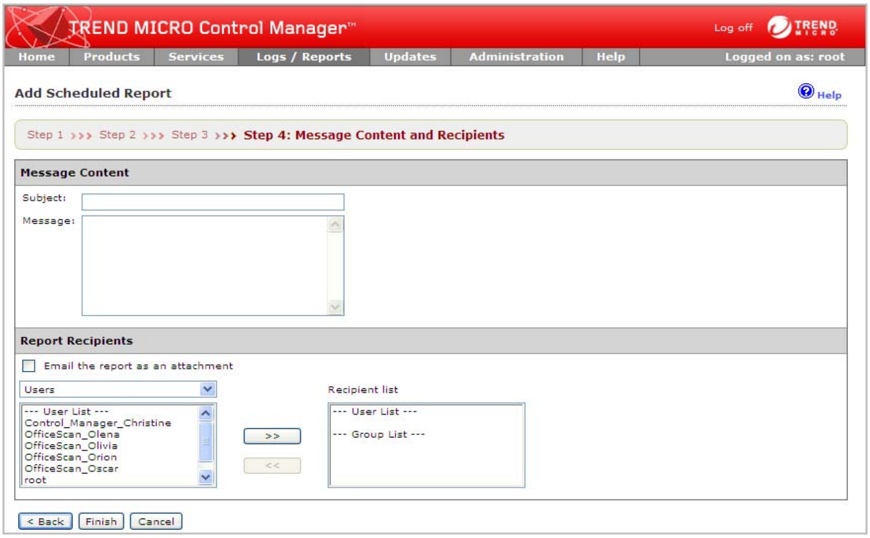
3. Specify when the report schedule starts:
   - **Immediately:** The report schedule starts immediately after enabling the report.
   - **Start on:** The report schedule starts on the date and time specified in the accompanying fields.

   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:

1. Mouseover **Logs/Reports**. A drop down menu appears.
2. Select **Scheduled Reports** from the drop down menu. The Scheduled Reports screen appears.
3. 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. Mouseover **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.

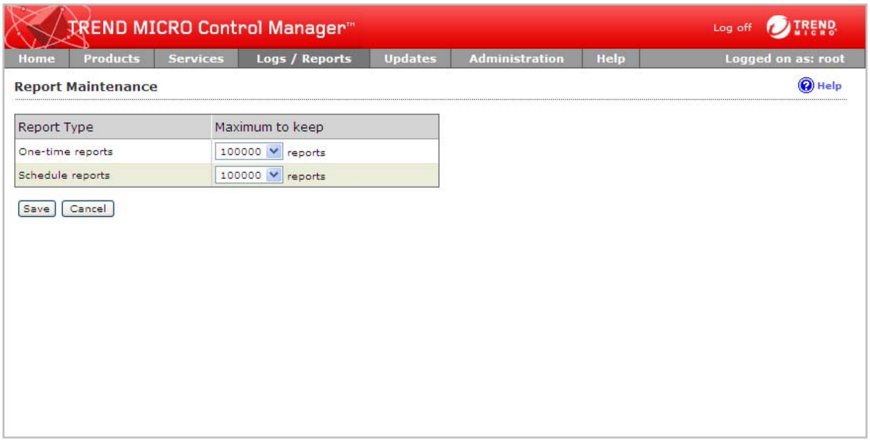
c. Select the report to view from the History screen.

Configuring Report Maintenance

Configure Report Maintenance settings to delete reports.

To configure report maintenance:

1. Mouseover **Logs/Reports**. A drop-down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Select **Report Maintenance**. The Report Maintenance screen appears.



Report Type	Maximum to keep
One-time reports	100000 reports
Schedule reports	100000 reports

4. Specify the maximum number of one-time and scheduled reports to keep.
5. Click **Save**.

Chapter 7

Administering Managed Products

This chapter presents material administrators will need to manage the Control Manager network.

This chapter contains the following topics:

- *Understanding Agents* on page 7-2
- *Understanding the Product Directory* on page 7-20
- *Activating and Registering Managed Products* on page 7-43
- *Managing Child Servers* on page 7-50

Understanding Agents

Control Manager 3.0 SP6/3.5/5.0 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** - Trend Micro's next generation agent supporting 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 7-1. 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
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

TABLE 7-1. Agent Comparison

FEATURE	MCP AGENTS	CONTROL MANAGER 2.X AGENTS
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 7-2. 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	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 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. There are currently only two instances where an agent must operate remotely:

- Trend Micro OfficeScan Corporate Edition, installed on a NetWare server
- NetScreen firewall management

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 7-3. 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	✖	

Table 7-3. Status Icons for Managed Products

Connection Status Description	Managed Product	
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 7-4. Status Icons for Communicators

Connection Status Description	Communicators	
TMI service is running	✓	
TMI service is not running	⊖	Within heartbeat's maximum delay setting
	⊗	Beyond the heartbeat's maximum delay setting
Idle mode following the Agent/Communicator Scheduler	⊖	
The socket or network connection between the Communicator and managed product is broken	⊗	
Unable to resolve the DNS name between the Communicator and Control Manager server	⊗	

Table 7-5. 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	✓	

TABLE 7-5. Status Icons for Child Servers

CONNECTION STATUS DESCRIPTION	CHILD
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 management 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 7-6. 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		●	●

TABLE 7-6. Security Level Behavior for MCP

FEATURES	SECURITY LEVEL		
	HIGH	MEDIUM	NORMAL
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 TMI.cfg of the Control Manager server including all managed products and child servers. Otherwise, the server and agent communication will not work.

TABLE 7-7. 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)

TABLE 7-7. Security Level Behavior for Older Agents

SECURITY LEVEL (FOUND IN TMI.CFG)	SECURITY LEVEL SELECTION (DURING INSTALLATION)	END-TO-END AUTHENTICATION	MESSAGE-LEVEL ENCRYPTION
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: In an event 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. However, check boxes are not available.

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 7-4 for details.

Note: In addition to providing periodic heartbeat to the Control Manager server, the agent also sends real-time managed product status information to the server.

MCP Heartbeat

To monitor the status of managed products, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the managed product and to check for commands to the managed product from Control Manager. The Control Manager Web console then presents the product status. This means that the managed product’s status is not a real-time, moment-by-moment reflection of the network’s status. Control Manager checks the status of each managed product in a sequential manner in the background. Control Manager changes the status of managed products to offline when a fixed period of time elapses without a heartbeat from the managed product.

Active heartbeats are not the only means Control Manager determines the status of managed products. The following also provide Control Manager with the managed product’s status:

- Control Manager receives logs from the managed product. Once Control Manager receives any type of log from the managed product successfully, this implies that the managed product is working fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the managed product to retrieve the pending command. If server connects to the managed product successfully, it also indicates that the product is working fine and this event counts as a heartbeat.
- In one-way communication mode, the MCP agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The MCP heartbeats implement in the following ways:

- **UDP:** If the product can reach the server using UDP, this is the lightest weight, fastest solution available. However, this does not work in NAT or firewall environments. In addition, the transmitting client cannot verify that the server does indeed receive the request.
- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the managed product applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains managed product activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Agent/Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots 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:

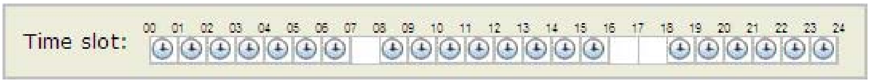


FIGURE 7-1. Schedule Bar

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 4:00 PM, and from 6:00 P.M. to 12:00 P.M.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

TABLE 7-8. 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 management 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.

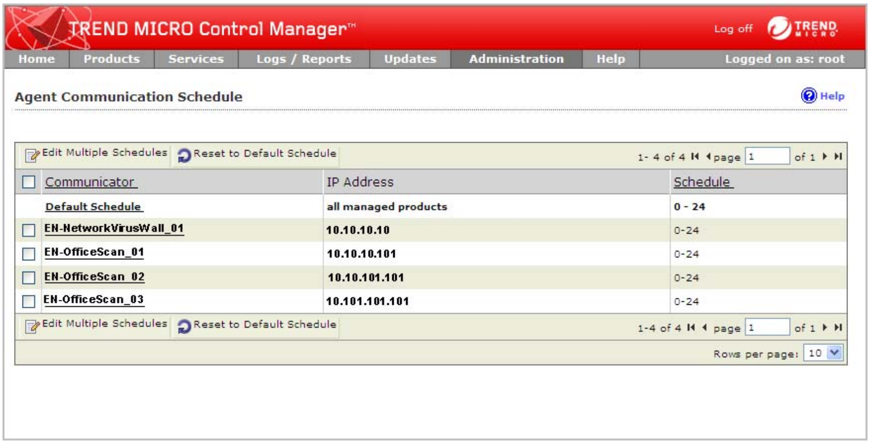
Configuring Agent Communication Schedules

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:

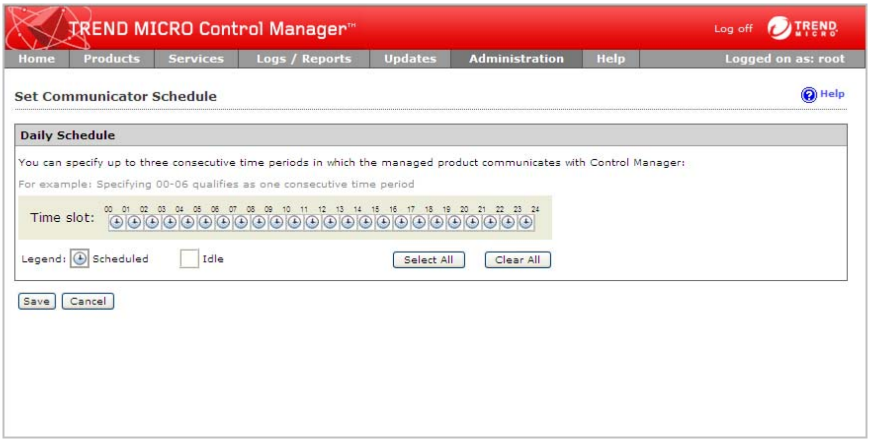
1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Agent Communication Schedule** from the sub-menu. TheAgent Communication Schedule screen appears.



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

4. 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

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: ◷ Scheduled □ Idle

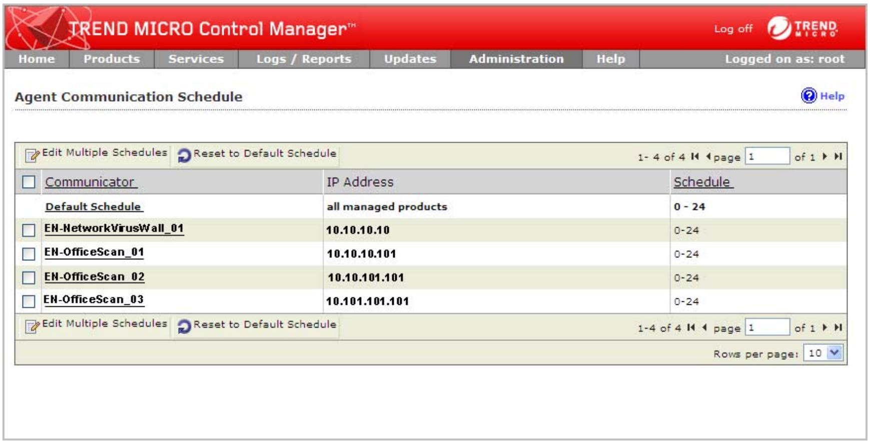
5. Define the schedule. Specify a new time or use the default setting:
    - To specify a new setting, toggle the appropriate time slots in the schedule bar and then click **Save**
    - To use the default setting, select the setting to apply and click **Reset to Default Schedule**

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:

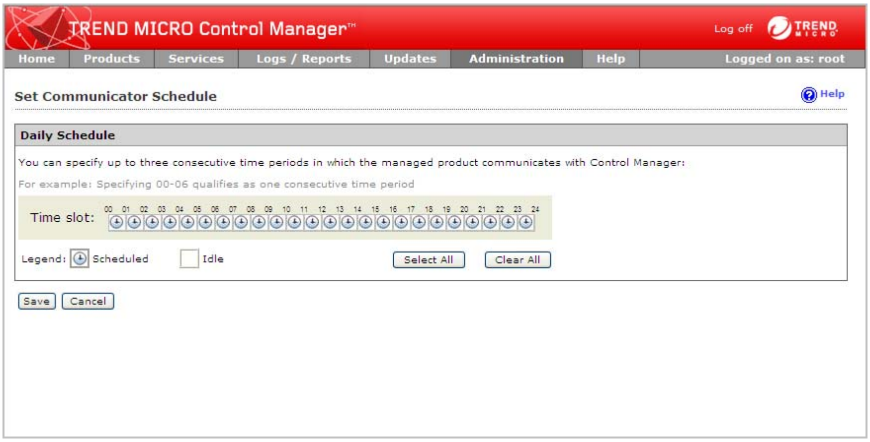
1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Agent Communication Schedule** from the sub-menu. TheAgent Communication Schedule screen appears.



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

4. 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

5. On the **Daily Schedule**, toggle the appropriate time slots.
6. Click **Save**.

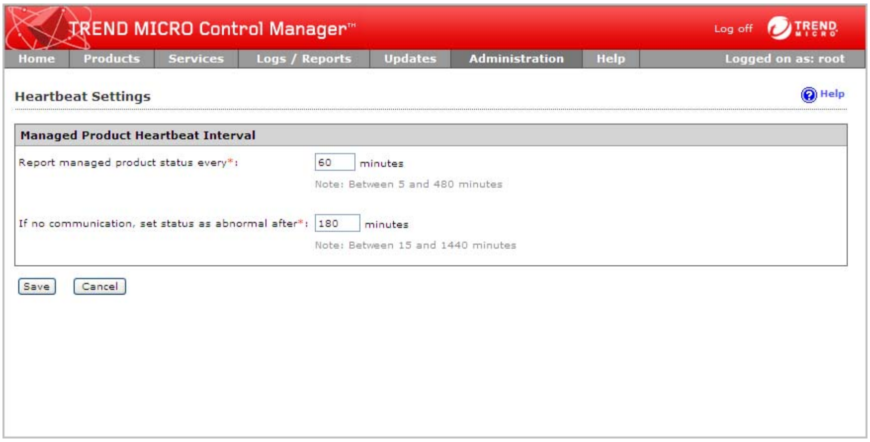
Setting the Agent/Communicator Heartbeat

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 predefined values:
Frequency: 3 minutes
Maximum delay: 5 minutes

To set the heartbeat Frequency and Maximum delay times:

1. Mouseover **Administrator** on the main menu. A drop-down list appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Heartbeat Settings** from the sub-menu. The Heartbeat Settings screen appears.



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

4. On the working area, leave the default values or specify new settings for the following:
   - **Report managed product status every:** Defines how often the Communicator responds to Control Manager server messages. The permitted 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 Communicator before changing its management console status to (inactive). The allowable 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.

5. 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 CCGI
- 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, Damage Cleanup 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).

Changing the external communication port is a two-step process.

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/directory in the Product Directory. The item highlights in the Product Directory.
3. Click **Folder**. The information in the work area changes.
4. Select **Connection Information View** from the Folder drop-down list. The **Mode** column displays which communication mode, the MCP agent on, the managed product uses.

Understanding 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 management 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 status’ 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 7-9. Product Directory Options

MENU ITEMS	DESCRIPTION
Advanced Search	Click this button to specify search criteria to perform a search for one or more managed products.
Configure	Click this button, after selecting a managed product/directory, to log on to the Web-based console and configure a managed product.
Tasks	Click this button, after selecting a managed product/directory, to perform specific function (such as deploying the latest components) to a specific or groups of managed product or child servers. Initiating a task from a directory and Control Manager sends requests to all managed products belonging to that directory.
Logs	Click this button, 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 clients found in the directory.

Note: Managed products belonging to child Control Manager servers cannot have tasks applied 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 model needs. For example, you can group products by location or product type (messaging security, Web security, file storage protection).

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

TABLE 7-10. 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 7-11. Considerations when Grouping Managed Products or Child Servers

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

TABLE 7-11. Considerations when Grouping Managed Products or Child Servers

STRUCTURE	DESCRIPTION
Administrative responsibility	Group managed products and child servers according to system or security personnel assigned to them. This allows group configuration.

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

- Configuring managed products
- Request products to perform Scan Now (if the managed product supports this command)
- View product information, as well as details about its operating environment (for example, product version, pattern file and scan engine versions, operating system information, and so on)
- View product-level logs
- Deploy virus pattern, scan engine, anti-spam rule, and program updates

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

- **User access**

  When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. You can grant access to multiple segments.

  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. You could also select specific managed products from different segments.

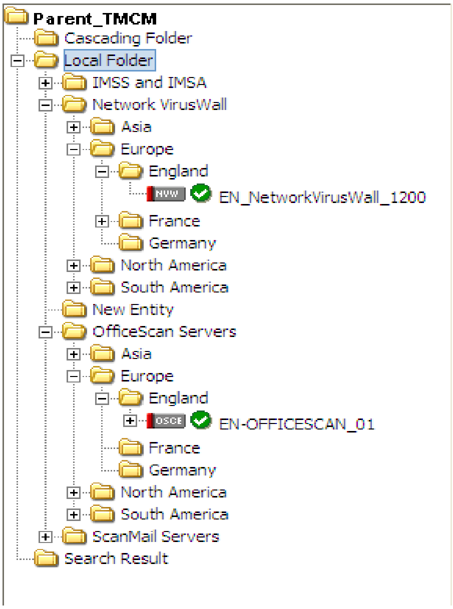
- **Deployment planning**

  Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.

- **Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments**

  OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

A sample Product Directory appears below:



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

Refer to the Control Manager *Understanding Product Directory* online help topic for the list of Product Directory icons.

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. For example, grant access rights to mail administrators to configure the Mail folder.

Default Folders for the Product Directory

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

TABLE 7-12. Product Directory Default Folders

STRUCTURE	DESCRIPTION
Root	All managed products and child Control Manager servers fall under the Root directory.

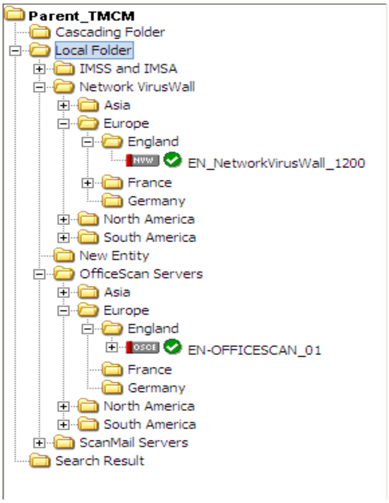
TABLE 7-12. **Product Directory Default Folders**

STRUCTURE	DESCRIPTION
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.

As shown in this sample Product Directory, managed products identify the registered antivirus or content security product, as well as provide the connection status.

Product Directory icons:

TABLE 7-13. Managed Product Icons

PRODUCT DIRECTORY TREE	ICON	DESCRIPTION
 Parent_TMCM Cascading Folder Local Folder IMSS and IMSA Network VirusWall Asia Europe England NVW ✓ EN_NetworkVirusWall_1200 France Germany North America South America New Entity OfficeScan Servers Asia Europe England OSCE ✓ EN-OFFICESCAN_01 France Germany North America South America ScanMail Servers Search Result	or	New entity or user-defined folder name
	EMAN	InterScan eManager
	OSCE	OfficeScan Corporate Edition
	SPNT	ServerProtect Information Server
		ServerProtect Domain
	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

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

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.

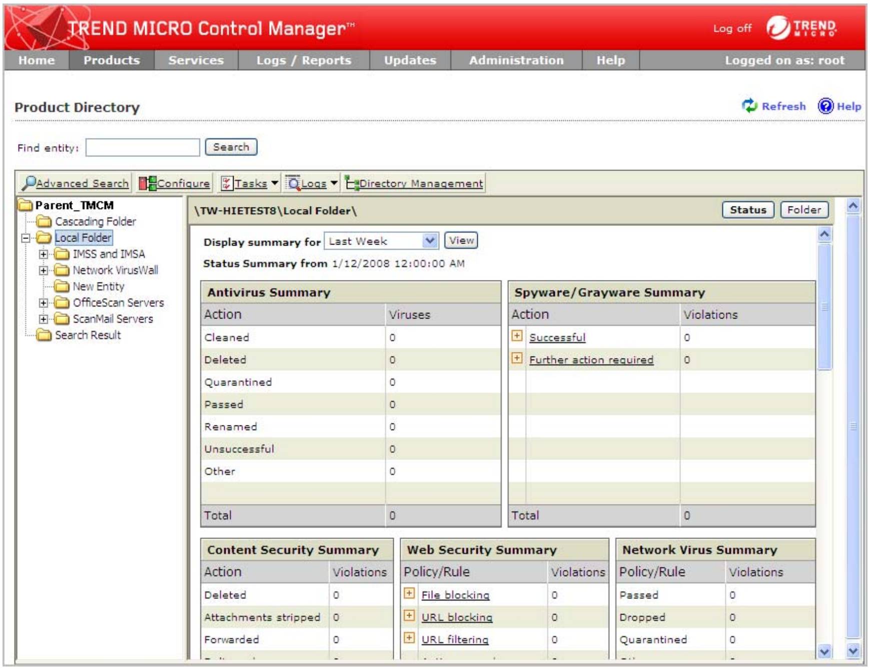
Manually Deploying New Components Using the Product Directory

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 specific 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.



Product Directory

Find entity:

\TW-HIETEST8\Local Folder\

Display summary for Last Week

Status Summary from 1/12/2008 12:00:00 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. Mouseover **Tasks** from the Product Directory menu. A drop down menu appears.
4. Select **Deploy <component>** from the drop down menu.
5. Click **Next>>**.
6. Click **Deploy Now** to start the manual deployment of new components.
7. Monitor the progress through the Command Tracking screen.
8. 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 Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, 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 available 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. Access the Product Directory.
2. Select the desired managed product from the product tree. The product status appears in the right-hand area of the screen.
3. Mouseover **Configure** from the product tree menu. A drop-down menu appears.
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 structure.

   b. Click **Replicate**. The selected managed product's settings replicate to the target managed products.

   Configure <Managed Product Name>: The managed product's Web-based 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/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:

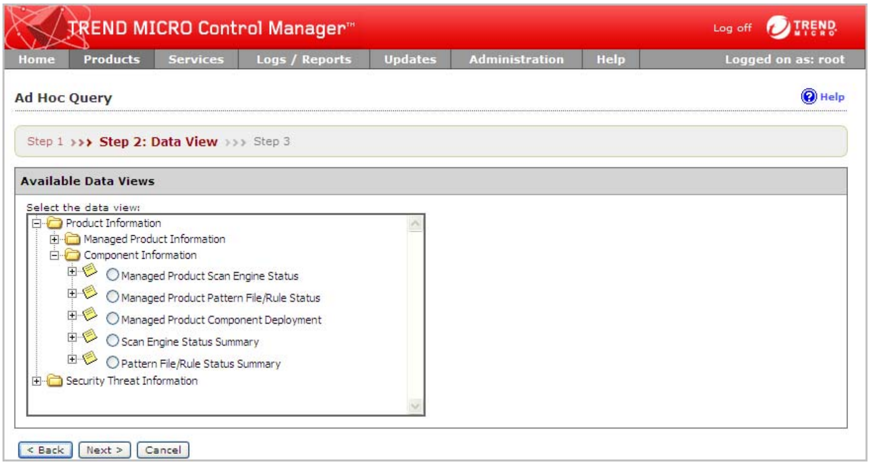
1. Access the Product Directory.
2. Select the managed product or directory to issue a task.
3. Mouseover **Tasks**. A drop-down menu appears.
4. Click a task from the list. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Querying and Viewing Managed Product Logs

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

To query and view managed product logs:

1. Access the Product Directory.
2. Select the desired managed product or folder from the Product Directory.
3. Mouseover **Logs** in the Product Directory menu. A drop-down list appears.
4. Click **Logs** from the drop down menu. The Ad Hoc Query Step 2: Select Data View screen appears.



Ad Hoc Query

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

Available Data Views

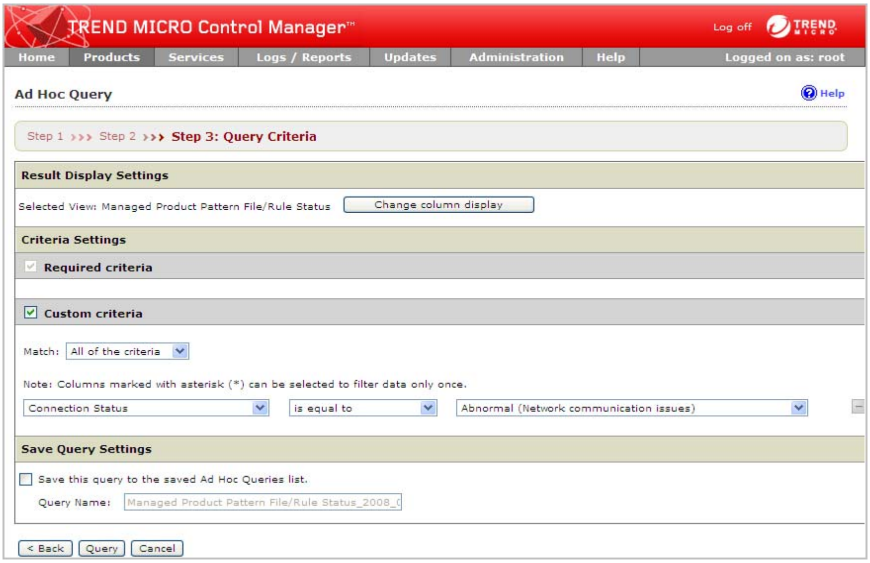
Select the data view:

- Product Information
  - Managed Product Information
  - Component Information
    - ○ Managed Product Scan Engine Status
    - ○ Managed Product Pattern File/Rule Status
    - ○ Managed Product Component Deployment
    - ○ Scan Engine Status Summary
    - ○ Pattern File/Rule Status Summary
- Security Threat Information

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.



Ad Hoc Query

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

Result Display Settings

Selected View: Managed Product Pattern File/Rule Status [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.

Connection Status | is equal to | Abnormal (Network communication issues)

Save Query Settings

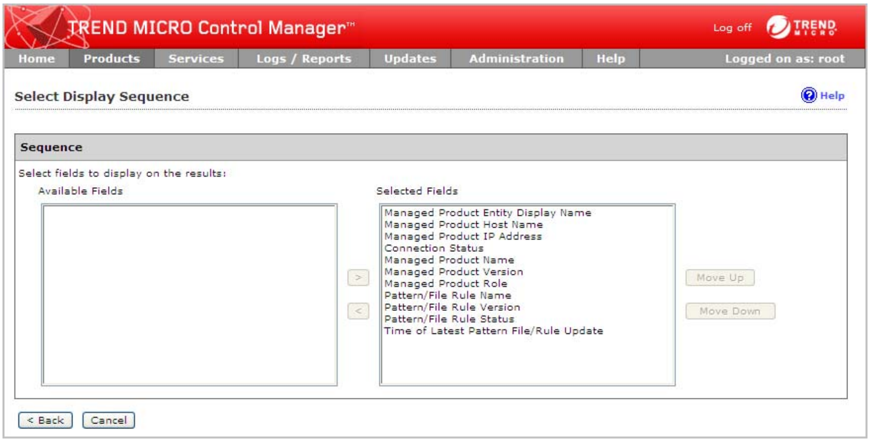
□ Save this query to the saved Ad Hoc Queries list.

Query Name: Managed Product Pattern File/Rule Status_2008_(

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.



Selected Fields:

Managed Product Entity Display Name
Managed Product Host Name
Managed Product IP Address
Connection Status
Managed Product Name
Managed Product Version
Managed Product Role
Pattern/File Rule Name
Pattern/File Rule Version
Pattern/File Rule Status
Time of Latest Pattern File/Rule Update

b. Select a query column from the Available Fields list. The selected item highlights.

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 to CSV:

a. Click **Export to CSV**. A dialog box appears.

b. Click **Save**. A Save as dialog box appears.

c. Specify the location to save the file.

d. Click **Save**.

11. To save the report to XML:

a. Click **Export to XML**. A dialog box appears.

b. Click **Save**. A Save as dialog box appears.

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**. 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.

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 a Control Manager server's managed products records are lost, the 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 7-16
- **Wait for the Agent to re-register itself:** By default, the older Control Manager agents verify their connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.

  Refer to *Changing Control Manager 2.x Agent Connection Re-Verification Frequency* on page 7-36 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

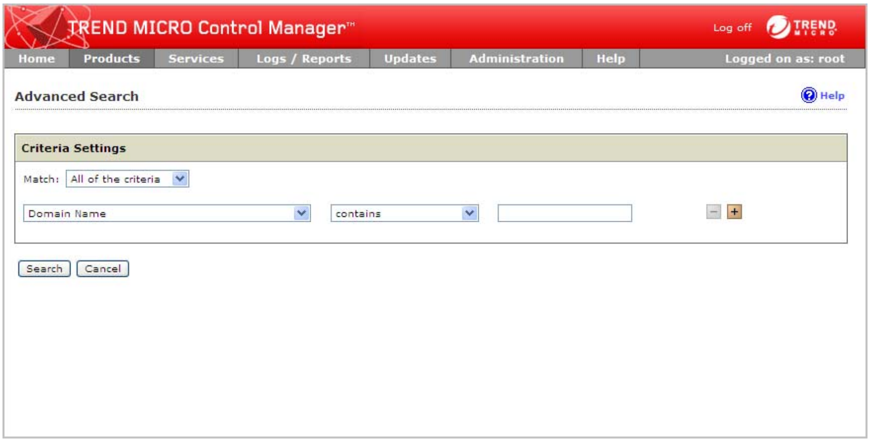
Use the Search button to quickly find and locate a specific managed product in the Product Directory.

To search for a folder or managed product:

1. Access 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 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 model 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 7-14. 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/directories in the Product Directory

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

- Remove managed products/directories from the Product Directory

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

To use and apply changes in the Directory Management screen:

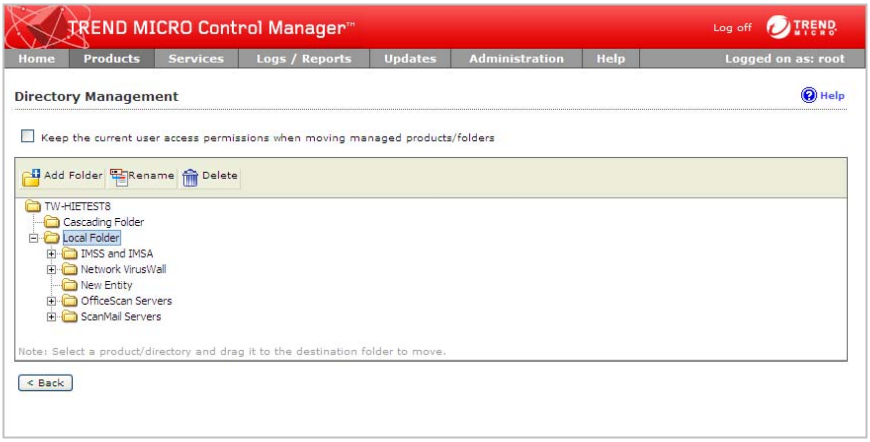
- Select a managed product/directory and click **Rename** to rename a managed product/directory
- Click + or the folder to display the managed products belonging to a folder
- Drag-and-drop managed products/directories to move the managed products/directories in the Product Directory
- Click **Add Folder**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

1. Access the Directory Management screen.
2. Select **Local Folder**. The Local Folder highlights.
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:

1. Access the Directory Management screen.
2. Select the managed product/directory to rename. The item highlights in the Product Directory.
3. Click **Rename**. The Rename Directory dialog box appears.
4. Type a name for the managed product/directory in the **Directory name** field.
5. Click **Save**. A confirmation dialog box appears.
6. Click **OK**. The managed product/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/folder, the managed product/folder keeps the permissions from its source folder. If you clear the Permission Keep check box, and then move a managed product/folder, the managed product/folder assumes the access permissions from its new parent folder.

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

1. Access 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.

To delete a user-defined folder:

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:

1. Access the Directory Management screen.
2. Select the managed product/directory to delete. The item highlights.
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.**

Activating and Registering Managed Products

To use the functionality of Control Manager 5.0, managed products (OfficeScan, ScanMail for Microsoft Exchange), and other services (Outbreak Prevention Services, Damage Cleanup Services, or Vulnerability Assessment), you need to obtain Activation Codes and activate the software or services. Included with the software is a Registration Key that you use to register your software online to the Trend Micro Online Registration Web site 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 the full functionality of the software.

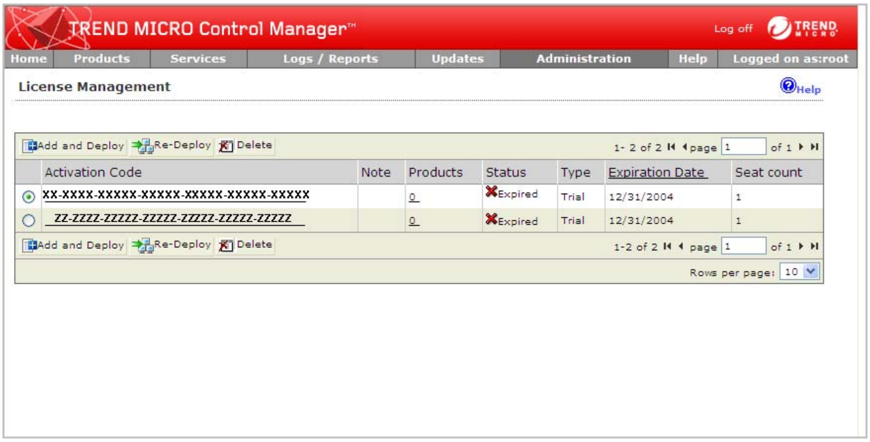
Activating Managed Products

Activating managed products allows you to use their full functionality, 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:

1. Mouseover **Administration** from the main menu. A drop down menu appears.
2. Mouseover **License Management** from the drop down menu. A sub-menu appears.

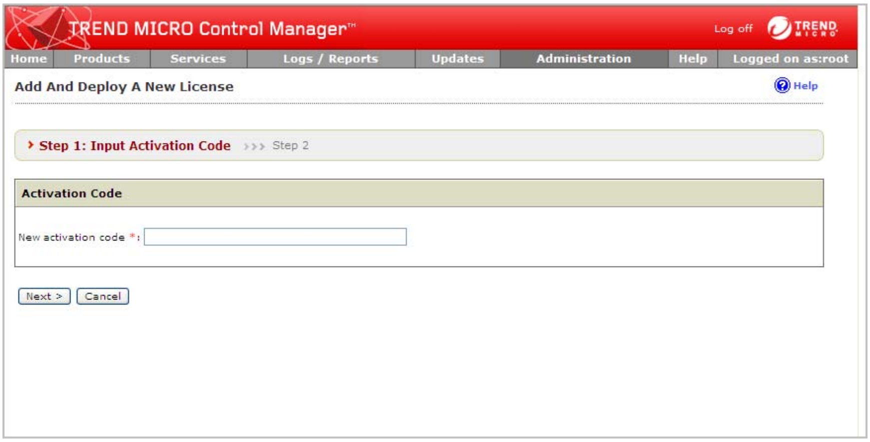
3. Click **Managed Products** from the sub-menu. The Managed Products License Management screen appears.



License Management

	Activation Code	Note	Products	Status	Type	Expiration Date	Seat count
●	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX		0	✗Expired	Trial	12/31/2004	1
○	ZZ-ZZZZ-ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ		0	✗Expired	Trial	12/31/2004	1

4. Click **Add and Deploy**. The Add And Deploy A New License 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 *:

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

6. Click **Next**. The Add And Deploy A New License Step 2: Select Targets screen appears.

Note: If no products appear in the list, the selected Activation Code does not support any products currently registered to Control Manager. This could mean that the managed product does not support receiving Activation Codes from Control Manager servers.

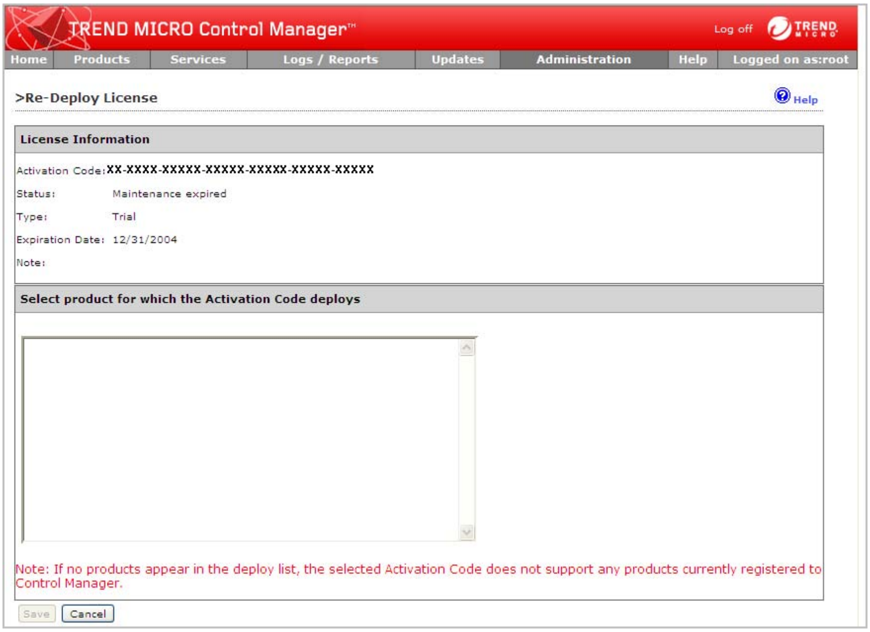
7. Select the managed product to which to deploy the Activation Code.
8. Click **Finish**. The Managed Products License Management screen appears with the new Activation Code listed in the table.

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:

1. Mouseover **Administration** from the main menu. A drop down menu appears.
2. Mouseover **License Management** from the drop down menu. A sub-menu appears.
3. Click **Managed Products** from the sub-menu. The Managed Products License Management screen appears.
4. Select an Activation Code from the list.
5. 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: 12/31/2004

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.

6. 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. A drop down menu appears.
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.

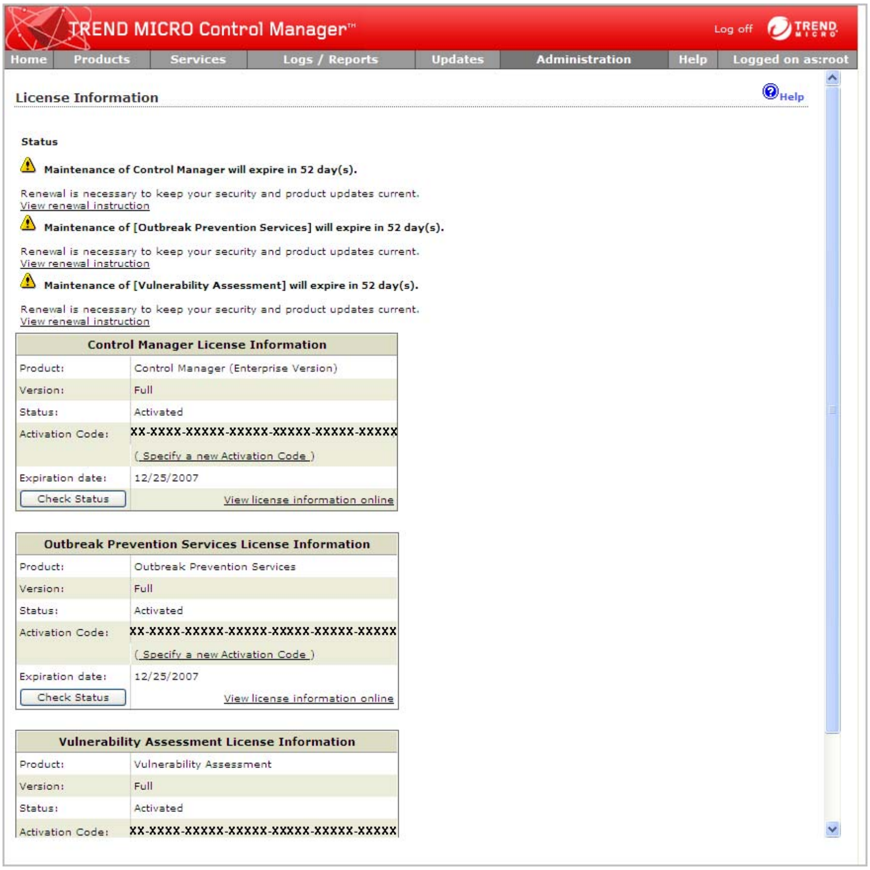
Activating Control Manager

Activating Control Manager allows you to use its full functionality, 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:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **License Information**. A sub-menu appears.
3. Click **Control Manager**. The License Information screen appears.



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

⚠ Maintenance of [Vulnerability Assessment] 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 (Enterprise Version)
Version:	Full
Status:	Activated
Activation Code:	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX (Specify a new Activation Code)
Expiration date:	12/25/2007
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:	12/25/2007
Check Status	View license information online

Vulnerability Assessment License Information	
Product:	Vulnerability Assessment
Version:	Full
Status:	Activated
Activation Code:	XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

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

Renewing Control Manager or Managed Service Maintenance

Renew maintenance for Control Manager or its integrated related products and services (that is, Outbreak Prevention Services, Vulnerability Assessment, or Damage Cleanup 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:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **License Information**. A sub-menu appears.
3. Click **Control Manager** from the sub-menu. The License Information screen appears.
4. On the working area under the product or service to renew, click **Check Status**.
5. Click **OK**.

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

To renew maintenance by manually entering an updated Activation Code:

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Mouseover **License Information**. A sub-menu appears.
3. Click **Control Manager** from the sub-menu. The License Information screen appears.
4. 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 Web site).
5. In the **New box**, type your Activation Code.
6. Click **Activate**.
7. Click **OK**.

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

Managing Child Servers

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

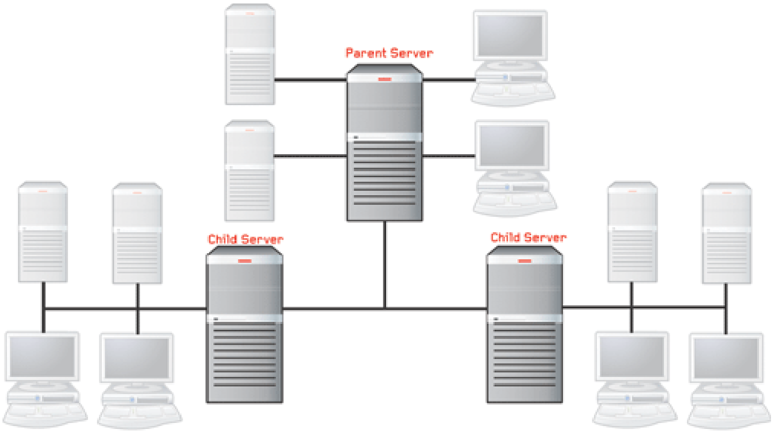


FIGURE 7-2. The cascading management structure uses two-tier Parent-Child architecture

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

Note: Control Manager 5.0 Advanced supports the following as child Control Manager servers:

- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition
- Control Manager 3.0 SP6 Standard or Enterprise Edition

Control Manager 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 7-15. Parent and child server feature comparison

FEATURE	AVAILABLE IN PARENT	AVAILABLE IN CHILD
Support two-tier cascading structure	Yes	No
Manage Advanced servers	Yes	No
Administer managed products	Yes	Yes
Handle multiple child servers	Yes	N/A
Issue global tasks	Yes	No
Create global reports	Yes	No

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 cascading management structure, using the Control Manager management console, allows system administrators to manage, monitor, and perform the following actions to all child servers belonging to a parent server:

- Monitor the Antivirus, Content Security, and Web Security summaries
- Query Event or Security logs
- Initiate tasks
- View reports
- Access the child server management console

The cascading structure can effectively manage your organization's antivirus and content security products - nationwide or worldwide.

Tip: Trend Micro recommends the management of not more than 200 child servers and 9,600 managed products for one Control Manager parent server.

Understanding the Parent Server and Child Server 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 7-16. 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 force 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, re-install 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, re-install 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

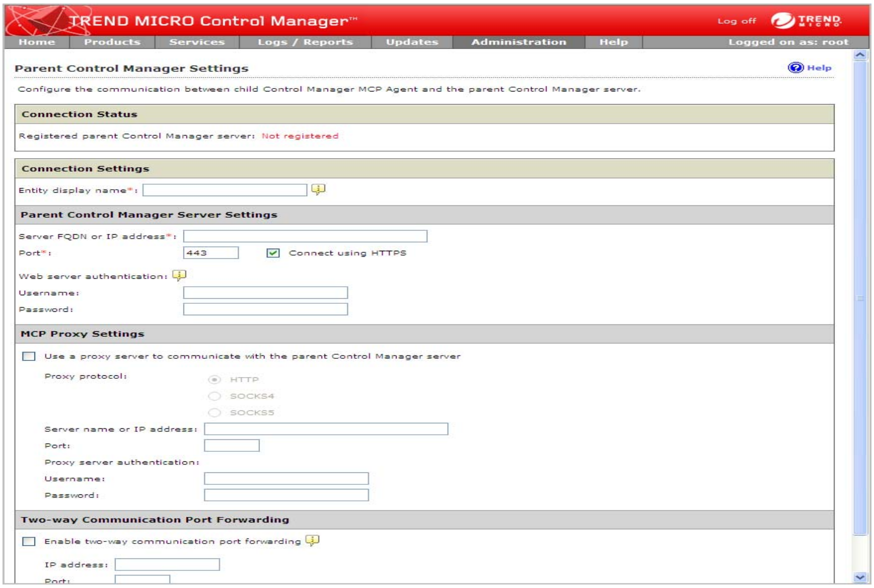
The action to register or unregister child servers does not generate the same result as to enable or disable child servers. The former permanently cuts the parent and child server connection, while the latter temporarily suspends the connection by maintaining the heartbeat connection between two servers.

For example, if you registered child server xyz to parent server a, unregister xyz from parent server a and register it to parent server b. Parent server b manages xyz. a's cascading structure tree removes xyz from the list.

Use the Control Manager Parent Settings screen to register or unregister from a Control Manager 5.0 parent server.

To register a Control Manager child server to a Parent Control Manager server:

1. Mouseover **Administration** in the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Parent Control Manager Settings** from the sub-menu. The Parent Control Manager Settings screen appears.



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:

4. 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.

5. 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.

6. 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.

7. 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.

8. To verify the child server can connect to the parent Control Manager server, click Test Connection.

9. 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 management 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. The former permanently cuts the parent and child server connection, while the latter temporarily suspends the connection by maintaining the heartbeat connection between two 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

Use Parent Control Manager Settings screen to unregister a child server from a parent server.

Note: Control Manger 3.0 and 3.5 servers require castool.exe to unregister from Control Manager 5.0 servers.

To unregister a child Control Manager server:

1. From the child server, mouseover **Administration** in the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Parent Control Manager Settings** from the sub-menu. The Parent Control Manager Settings screen appears.
4. 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 only access the Product Directory through the parent server management console.

To access the Cascading Folder:

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

Viewing the Product Directory Status Summaries

The Product Directory screen displays the Antivirus, Spyware/Gryaware, 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 Product Directory status summaries:

1. Access 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 elapsed time has passed. 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:

1. Access the Product Directory.
2. Select a child server from the Product Directory. The item highlights.
3. Mouseover **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 that 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:

1. Access the Product Directory.
2. Select a child server from the Product Directory. The item highlights.
3. Mouseover **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 Anti-spam Rules
- Deploy engines
- Deploy program files
- Open the child server's Web console

To issue a task:

1. Access the Product Directory.
2. Select a child server from the Product Directory. The item highlights.

3. Perform one of the following:

   Issue a task to the child server

   a. Mouseover **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. Mouseover **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:

1. Access the Product Directory.
2. Select a child server from the Product Directory. The item highlights.
3. Mouseover **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:

1. Access the Directory Management screen.
2. Select the child server to rename. The item highlights in the Product Directory.
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

In an event when you have accidentally unregistered a child server, you need to unregister and then re-register the child server to the parent server.

To recover Control Manager 3.0/3.5 child servers accidentally removed from the Directory Manager:

1. From the child server's Windows 2000 command interpreter, execute the force unregistration command:

   ```
   castool /e
   ```

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

Registering a Child Control Manager Server to a Parent Control Mananger Server

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

To register a Control Manager child server to a Parent Control Manager server:

1. Mouseover **Administration** in the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Parent Control Manager Settings** from the sub-menu. The Parent Control Manager Settings screen appears.
4. 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.
5. 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.

6. 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** and complete the following settings:

   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.

7. Configure Two-way Communication Port Forwarding:

   a. If you will use port forwarding with MCP agents, select **Enable two-way communication port forwarding** and complete the following settings:

   b. Type the forwarding IP address in the **IP address** field.

   c. Type the port number in the **Port** field.

8. To verify the child server can connect to the parent Control Manager server, click **Test Connection**.

9. 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 management 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.

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 management 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 7-17. 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 management console; this is useful for auditing management console accesses
CDSM_SystemEventlog	Stores system logs generated by internal processes

TABLE 7-18. 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

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

TABLE 7-19. Managed Product Tables

TABLE 7-20. Log Tables

LOG TABLES	DESCRIPTION
tb_TempLog	Stores the raw data of product logs
tb_AV*Log	Stores product log * corresponds to Virus, Event, Status, PEInfo, WebSecurity. These tables store the product status log as well as the pattern and engine version, update and deploy time, and the unhandled virus count.
tb_InValidLog	Stores unidentified log information
• tb_TotalWebSecurityCount • tb_TotalVirusCount • tb_TotalSecurityCount • tb_TopTenSource • tb_TopTenDestination • tb_TopTenVirus	Stores virus summary information for Status Summary and reports
tb_LogPurgePolicy	Stores purge log settings
tb_LogPurgeCounter	Stores purge log counter
• tb_InstanceForVirusOutbreak • tb_InstanceForSpecialVirus • tb_InstanceForVirusOutbreak	Stores log instances used in alert notifications

TABLE 7-21. Notification Tables

NOTIFICATION TABLES	DESCRIPTION
• tb_Alert_NTF_JobList • tb_Event_NTF_JobList	Stores notification queue list
tb_EventNotificationFilter	Stores Event Center configuration

TABLE 7-21. Notification Tables

NOTIFICATION TABLES	DESCRIPTION
• 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 7-22. Report Tables

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

TABLE 7-23. 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 Windows 2000 command interpreter, 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.

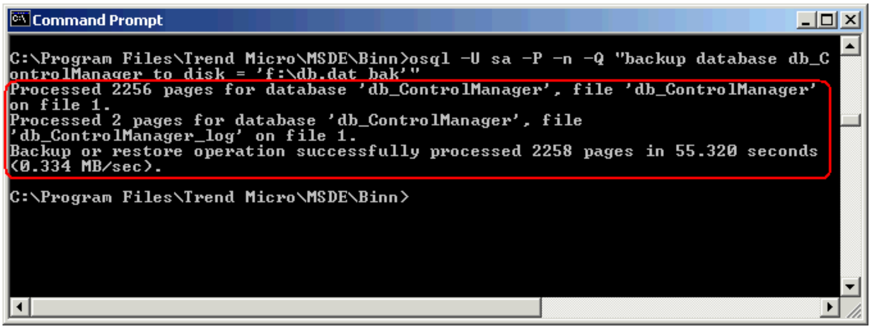
{Control Manager database}: name of the Control Manager database

{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 to 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:

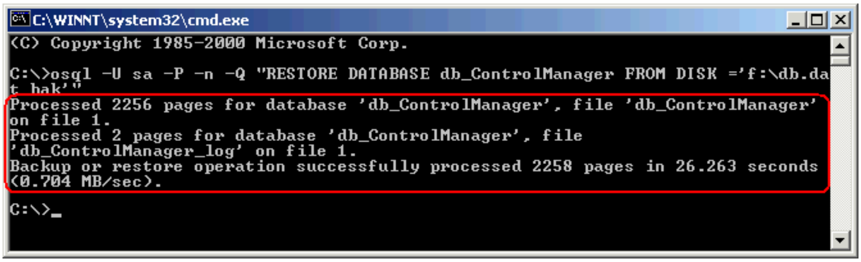
1. Stop Control Manager.
2. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
3. Right-click **<Control Manager service>**, and then click **Stop**.
4. Click **Start > Run**.
5. Type `cmd` and then click **OK**.
6. On the Windows 2000 command interpreter, execute 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 the SQL Server Enterprise Manager

When using SQL Server, use the SQL Server Enterprise Manager to back up the Control Manager database.

To back up db_ControlManager using the SQL Server Enterprise Manager:

1. From the Control Manager server, click **Start > Programs > Microsoft SQL server > Enterprise manager** to access the SQL Server Enterprise Manager.
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 back ups of the Control Manager database. Always back up when you are about to modify the Control Manager database (for example, adding installing a managed product).

Restoring Backup db_ControlManager Using SQL Server Enterprise Manager

Use the SQL Server Enterprise Manager 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 **Start > Programs > Microsoft SQL server > Enterprise manager** to access the SQL Server Enterprise Manager.
5. On the console, click **Microsoft SQL servers > SQL server group > {SQL server} (Windows NT) > 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, 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 Enterprise Manager

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:

1. Back up the Control Manager database using the SQL Server Enterprise Manager.
2. Purge the transaction log.
3. On the SQL Server, click **Start > Programs > MS SQL Server** to open the Query Analyzer.
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
```

Chapter 8

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* on page 8-2
- *Understanding Enterprise Protection Strategy* on page 8-3
- *Introducing TrendLabs Message Board* on page 8-5
- *Participating in the World Virus Tracking Program* on page 8-5
- *Introducing Outbreak Prevention Services* on page 8-6
- *Preventing Virus Outbreaks and Understanding the Outbreak Prevention Mode* on page 8-9
- *Using Outbreak Prevention Mode* on page 8-18

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 new approach combines the following services:

- **TrendLabs Message Board -** A real-time message board that quickly provides latest update component information and characterizes new viruses so they can be identified and quickly eliminated
- **Outbreak Prevention Services** - Industry-unique services that provide Outbreak Prevention Policies to help deflect, isolate, and stem outbreak attacks
- **Damage Cleanup Services** - Comprehensive services that help clean and repair systems infected by Trojan viruses or worms
- **Vulnerability Assessment** - provides system administrators or other network security personnel with the ability to assess security risks to their networks

Trend Micro's 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

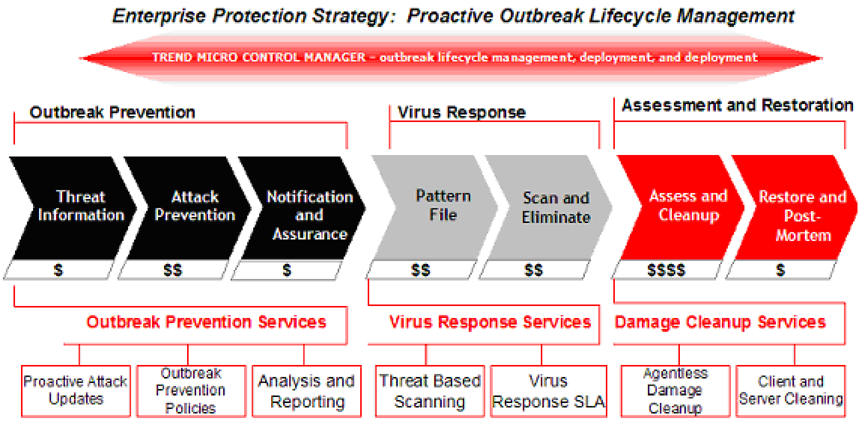


FIGURE 8-1. Enterprise Protection Strategy

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

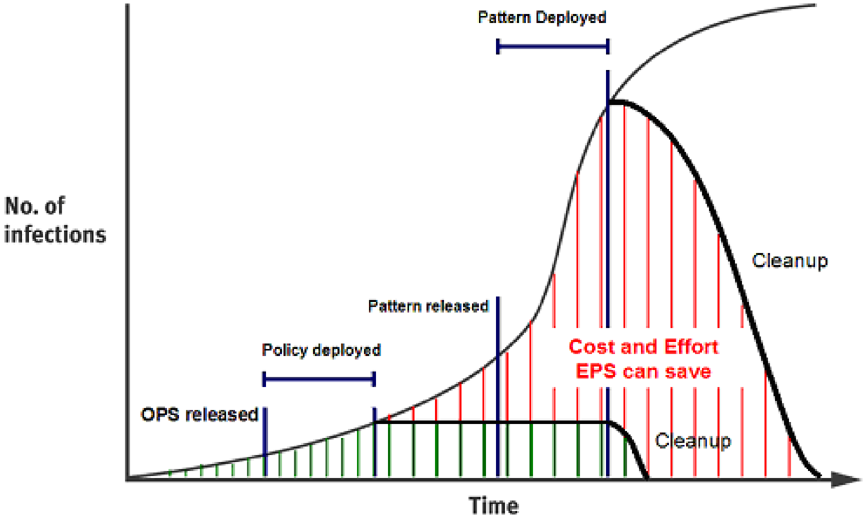


FIGURE 8-2. Cost vs. Effort

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 lifecycle 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 TrendLabs Message Board

As a Control Manager user and Trend Micro customer, you can receive alerts from TrendLabs(SM) about emerging virus outbreaks before they affect your system.

The Trend Micro TrendLabs Message Board provides version numbers and the times when TrendLabs releases update components (such as virus pattern files, scan engines, damage cleanup templates and Outbreak Prevention Policies) to identify the threats against which you should protect yourself with Control Manager.

Participating in the World Virus Tracking Program

The Trend Micro Virus Map displays information about actual virus infections detected by HouseCall, our online virus scanner for PCs, and managed products registered to Trend Micro Control Manager. You can view this dynamic map to analyze worldwide virus trends in real time and help predict virus outbreaks, and prevent them proactively.

You can add your data to the Trend Micro Virus Map by choosing to participate in the World Virus Tracking Program. When you choose to participate, Trend Micro Control Manager will only send anonymous information (through the HTTPS protocol and port 443), and you can stop participating any time by choosing No and updating your status on the Control Manager management console.

To participate in the World Virus Tracking Program:

1. Click **Administration** on the main menu.
2. On the left-hand menu, click **World Virus Tracking Program**.
3. On the working area, click **Yes, I want to participate...**.
4. Click **Save**.

Introducing Outbreak Prevention Services

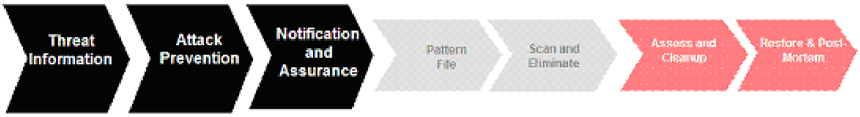


FIGURE 8-3. Outbreak Prevention Services

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 predefined, 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 8-1. 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:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Registration, click **License Information**.
3. On the working area under Outbreak Prevention Services License Information, click the **Activate the product** link.

4. Do the following:
   - **If you don't 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
5. 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 8-2. 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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. 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.

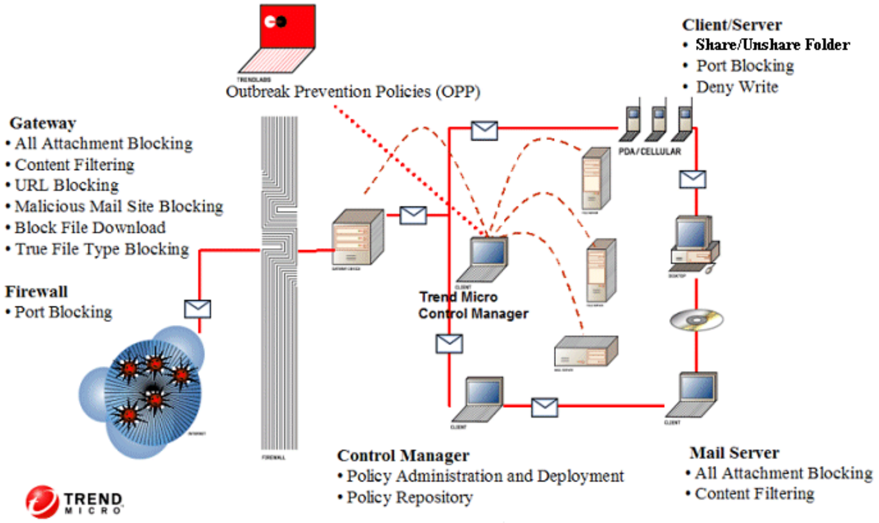


FIGURE 8-4. Deploying OPP

Accessing the Outbreak Prevention Services Settings Screen

To access the Outbreak Prevention Services Settings screen:

1. Click **Services** on the main menu.

2. On the left-hand menu under Services, click **Outbreak Prevention > Settings**.

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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.
3. On the working area under Service Status, click **Update Now** to download the latest Outbreak Prevention Policies.
4. 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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention > Settings**.
3. On the working area, click the **Download** tab.
4. Under Scheduled policy download settings, select the **Enable scheduled policy update** check box.
5. From the Download frequency list, choose the number of minutes for Control Manager to check for updated Outbreak Prevention Policies.
6. 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**.

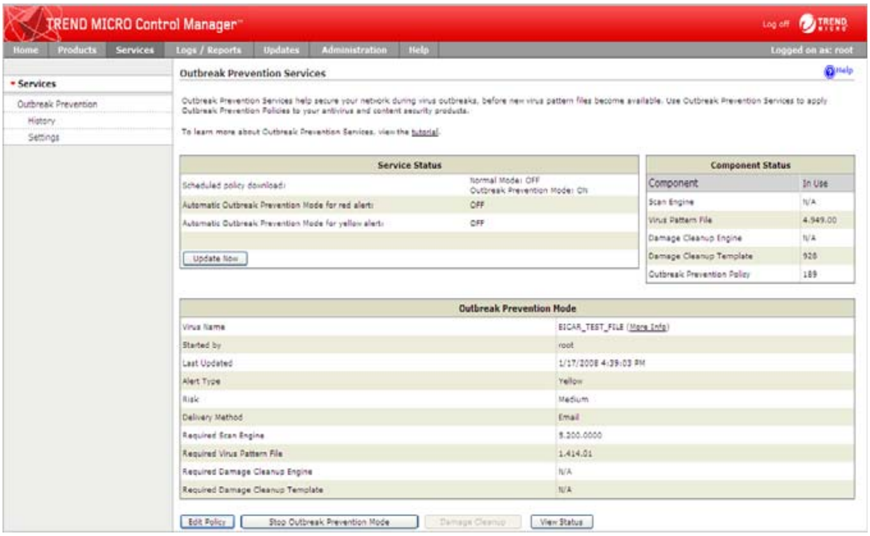
7. Click **Save**.
8. Click **OK**.

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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. 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:	OFF
Automatic Outbreak Prevention Mode for yellow alert:	OFF

Component Status	
Component	In Use
Scan Engine	N/A
Virus Pattern File	4.949.00
Damage Cleanup Engine	N/A
Damage Cleanup Template	928
Outbreak Prevention Policy	189

Outbreak Prevention Mode	
Virus Name	EICAR_TEST_FILE (More Info)
Started by	root
Last Updated	1/17/2008 4:39:03 PM
Alert Type	Yellow
Risk	Medium
Delivery Method	Email
Required Scan Engine	8.200.0000
Required Virus Pattern File	1.414.01
Required Damage Cleanup Engine	N/A
Required Damage Cleanup Template	N/A

3. 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).
4. Click **OK** twice after downloading the Outbreak Prevention Policies.

5. 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.
6. Click **Start Outbreak Prevention Mode**.
7. Under Outbreak Prevention Policy, in the Policy in effect for list, choose the number of days that Control Manager continues in Outbreak Prevention Mode.
8. From the Deployment plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products.
9. 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.
10. Configure managed product settings or click **Recommended Settings**.
11. Click **Activate**.
12. 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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.
3. On the working area, click **Edit Policy**.
4. Under Outbreak Prevention Policy, in the Policy in effect for list, choose the number of days that Control Manager continues in Outbreak Prevention Mode.

5. 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, mouseover **Updates**, and then click **Deployment Plan**).
6. **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.
7. 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.

8. 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 8-3. 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 8-3. 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:

1. Click **Services** on the main menu.
2. Click **Settings**.
3. Click the **Automatic Outbreak Prevention Mode** tab.
4. 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.
5. From the Prevention duration list, choose the number of days that Outbreak Prevention Mode is active.
6. From the Deployment plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products.
7. Do the following:
   - Under Excluded products, select managed products that will not receive Outbreak Prevention Policies. Important: 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.

- To automatically trigger Damage Cleanup Services, under Damage Cleanup, select the **Enable Damage Cleanup Services** check box. Click **Damage Cleanup** to configure Damage Cleanup Services settings.
- To automatically trigger Vulnerability Assessment, under Vulnerability Assessment, select the **Enable Vulnerability Assessment** check box.
- Select the **Stop OPP automatically after the prevention duration expires** check box to automatically stop OPP.

8. 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:

1. Click **Services** on the main menu.
2. Click **Settings**.
3. 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 5-57.
   - To deploy the virus pattern file only, select the **Exclude Scan Engine Deployment** check box.
4. 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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**.
3. Click **Stop Outbreak Prevention Mode**.
4. 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 8-4. 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:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention > History**. 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:** Identify the source of the virus outbreak
- **Step 2:** Evaluate existing policies
- **Step 3:** Start Outbreak Prevention Mode
- **Step 4:** Follow-up procedures

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 8-5. 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.
TrendLabs Message Board	The Trend Micro TrendLabs Message Board provides the version numbers and the time TrendLabs releases the antivirus and content security components. This helps identify malware threats and provides update information about your Control Manager system.
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 Web site.

TABLE 8-5. Identifying the Source of the Outbreak

ALERT METHODS	DESCRIPTION
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 6-8.

For creating scheduled policy downloads, see*Updating Outbreak Prevention Policies* on page 8-11.

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 5-57.

- **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 9

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\
```

This chapter provides instructions on how to use the following Control Manager tools:

- *Using Agent Migration Tool (AgentMigrateTool.exe)* on page 9-2
- *Using the Control Manager MIB File* on page 9-2
- *Using the NVW 1.x SNMPv2 MIB File* on page 9-3
- *Using the NVW Enforcer SNMPv2 MIB File* on page 9-3
- *Using the NVW System Log Viewer* on page 9-4
- *Using the NVW 1.x Rescue Utility* on page 9-4
- *Using the Appliance Firmware Flash Utility* on page 9-4
- *Using the DBConfig Tool* on page 9-5

Using Agent Migration Tool (`AgentMigrateTool.exe`)

The Agent Migration tool provided in Control Manager 5.0 Standard or Advanced Edition migrates agents administered by a Control Manager 3.0, 3.5, or 5.0 server (see *Migrating Control Manager 2.5x and MCP Agents* on page 4-15).

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 11-2).

Using the Control Manager MIB File

Download and use the Control Manager MIB file with an application (for example, HP^{TM} OpenView) that supports SNMP protocol.

To use the Control Manager MIB file:

1. Access the Control Manager management console.
2. Click **Administration** on the main menu. A drop-down menu appears.
3. Click **Tools**.
4. On the working area, click **Control Manager MIB file**.
5. On the File Download screen, select **Save**, specify a location on the server, and then click **OK**.
6. On the server, extract the Control Manager MIB file **`cm2.mib`**, Management Information Base (MIB) file.
7. Import `cm2.mib` using an application (for example, HP OpenView) that supports SNMP protocol.

Using the NVW 1.x SNMPv2 MIB File

Download and use the NVW 1.x SNMPv2 MIB file with an application (for example, HP OpenView) that supports SNMP protocol.

To use the NVW 1.x SNMPv2 MIB file:

1. Access the Control Manager management console.
2. Click **Administration** on the main menu. A drop-down menu appears.
3. Click **Tools**.
4. On the working area, click **NVW 1.x SNMPv2 MIB file**.
5. On the File Download screen, select **Save**, specify a location on the server, and then click **OK**.
6. On the server, extract the NVW 1.x SNMPv2 MIB file **`nvw.mib2`**, Management Information Base (MIB) file.
7. Import `nvw.mib2` 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:

1. Access the Control Manager management console.
2. Click **Administration** on the main menu. A drop-down menu appears.
3. Click **Tools**.
4. On the working area, click **NVW Enforcer SNMPv2 MIB file**.
5. On the File Download screen, select **Save**, specify a location on the server, and then click **OK**.
6. On the server, extract the NVW Enforcer SNMPv2 MIB file **`nvw2.mib2`**, Management Information Base (MIB) file.
7. Import `nvw2.mib2` using an application (for example, HP OpenView) that supports SNMP protocol.

Using the NVW System Log Viewer

Use the NVW System Log Viewer to open Network VirusWall logs for Network VirusWall products.

To use the log viewer:

1. Access the Control Manager management console.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.
3. Click **Tools**.
4. On the working area, click **NVW System Log Viewer**.
5. Using the log viewer, import logs from the Network VirusWall device.

Using the NVW 1.x Rescue Utility

Uploading the Network VirusWall program file with the Network VirusWall 1.x Rescue Utility performs the same function as uploading the program file through the command line interface. The utility, however, is a user-friendly, Windows based option for those who prefer to use a graphical user interface.

To access the Network VirusWall 1.x Rescue Utility:

1. Using Windows Explorer, open the Control Manager 3.5 root folder. For example:

   <root>\Program Files\Trend Micro\Control Manager\WebUI\download\tools
2. Double-click the `NVW1.x_Rescue_Utility.exe` application.

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 2500 appliances.

To access the AFFU:

1. Access the Control Manager management console.
2. Mouseover **Administration** on the main menu. A drop-down menu appears.
3. Click **Tools**.

4. On the working area, click **AFFU**.
5. On the File Download screen, select **Save**, specify a location on the server, and then click **OK**.
6. Extract the AFFU file to the server.

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 WA)

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" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"

Example 2: DBConfig -DBName="db" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"

Chapter 10

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* on page 10-2
- *Manually Removing Control Manager* on page 10-2
- *Removing a Windows-Based Control Manager 2.x Agent* on page 10-7

Removing a Control Manager Server

You have two ways to remove Control Manager automatically (the following instructions apply to a Windows 2000 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 re-install Control Manager on the server and retain all system information, such as agent registration, and user account data.

If you re-installed 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 2000.

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)

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, 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 CCGI
- 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).

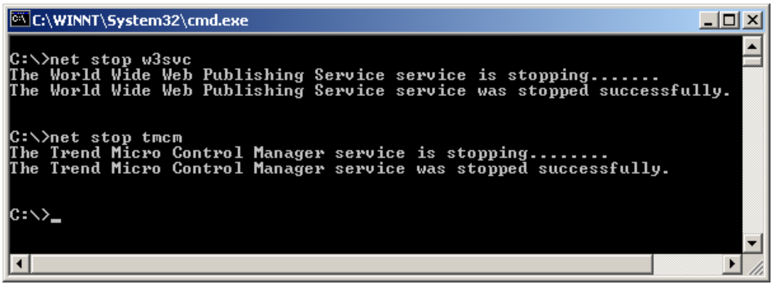
To stop Control Manager services:

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 10-1. 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\mmc.exe %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. Right-click the IIS Web site you set during installation.
7. Click **Properties**.
8. Click the **ISAPI Filters** tab.
9. Delete the following ISAPI filters:
   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy
10. 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
11. Click **OK**.

Removing Crystal Reports, TMI, and CCGI

Removal of TMI and CCGI is optional. Use Add/Remove Programs to uninstall Crystal Reports.

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 TMI and CCGI:

- Use Microsoft's service tool Sc.exe to remove TMI and CCGI: *http://support.microsoft.com/kb/251192/en-us*

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
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 > Settings > 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 Microsoft's Web site 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:

- Use Microsoft's service tool **Sc.exe** to remove Control Manager and NTP services: *http://support.microsoft.com/kb/251192/en-us*

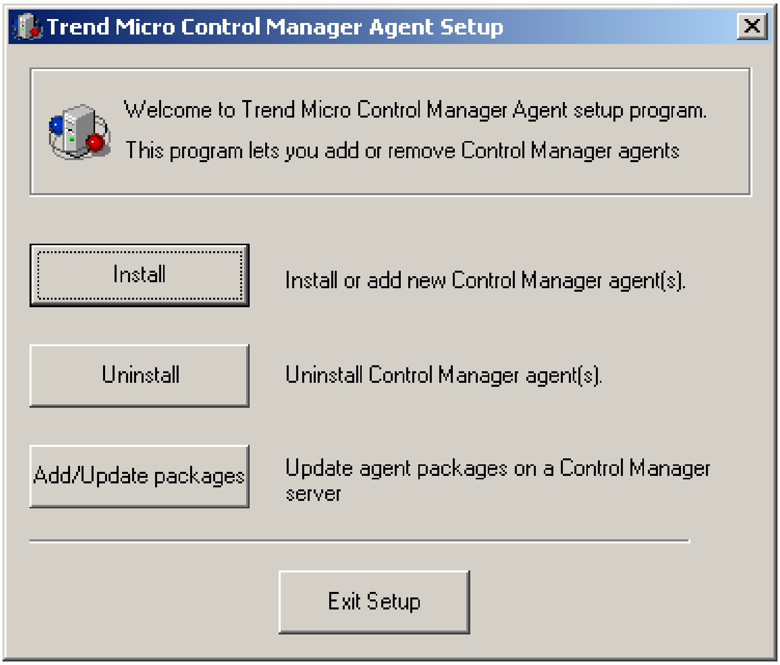
Removing a Windows-Based Control Manager 2.x Agent

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.



Trend Micro Control Manager Agent Setup

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).

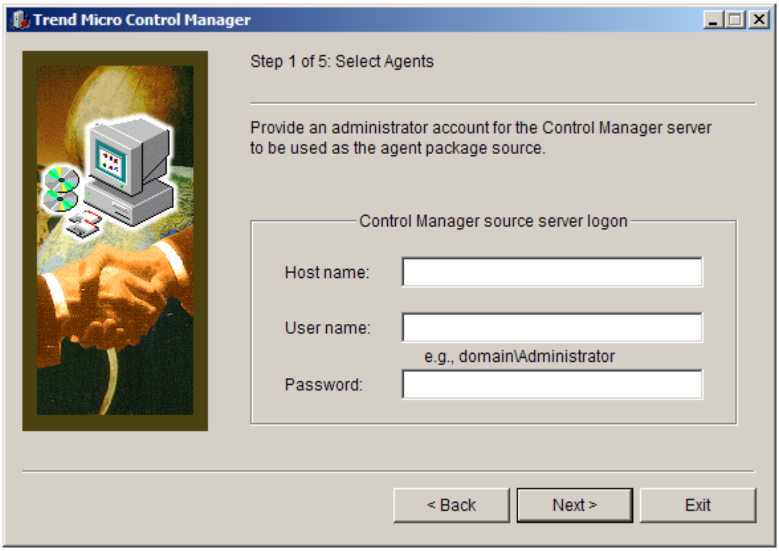
Uninstall Control Manager agent(s).

Update agent packages on a Control Manager server

FIGURE 10-2. Trend Micro Agent setup program

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

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



Trend Micro Control Manager

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 10-3. 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.

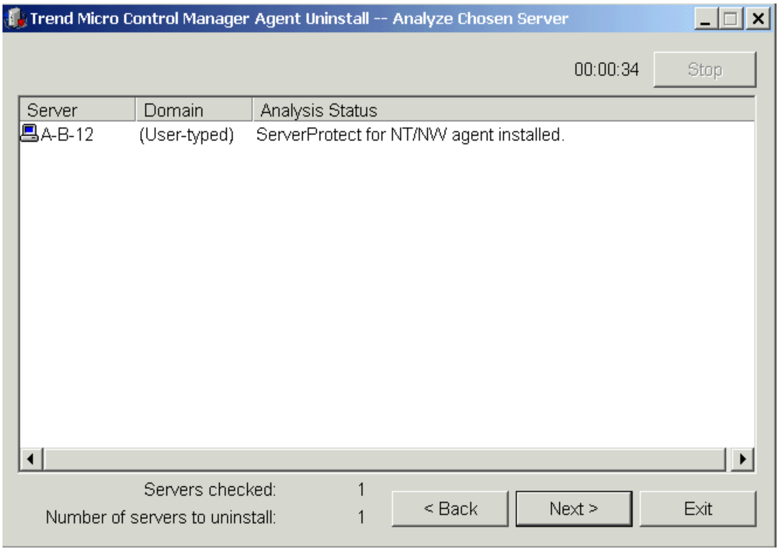
To specify a server name directly:

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 10-4. 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 11

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 11-2
- *Contacting Technical Support* on page 11-2
- *TrendLabs* on page 11-3
- *Other Useful Resources* on page 11-3

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 Web site**: our Technical Support Web site contains the latest information about all Trend Micro products. The support Web site 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

  `support@trendmicro.com`

- 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 information procedures provided by the Support team:

  `http://esupport.trendmicro.com/support`

- Product updates and patches

  `http://www.trendmicro.com/download/`

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

`http://www.trendmicro.com/en/about/contact/overview.htm`

To speed up the problem resolution, when you contact our staff please 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 2000 or SQL 7.0)
- 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 has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

`www.trendmicro.com/en/security/trendlabs/overview.htm`

Other Useful Resources

Trend Micro offers a host of services through its Web site, www.trendmicro.com.

Internet-based tools and services include:

- The World Virus Tracking Center - monitor virus incidents around the world
- HouseCall™ - Trend Micro online virus scanner
- Virus risk assessment – the Trend Micro online virus protection assessment program for corporate networks

Appendix A

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* on page A-2
- *Ports Checklist* on page A-3
- *Control Manager 2.x Agent installation Checklist* on page A-4
- *Control Manager Conventions* on page A-4
- *Core Process and Configuration Files* on page A-5
- *Communication and Listening Ports* on page A-7
- *Trend Micro Control Manager Product Features* on page A-8

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 them here for easy reference.

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	
SMTP server information (Optional; for email message notifications)		
IP address	10.1.123.225	
Fully qualified domain name (FQDN)	mail.company.com	

Information required	Sample	Your value
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	
Management Console and Update/Deploy components	80	
Firewall, "forwarding" port (Optional; used during Control Manager Agent installation)	224	
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
	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 management 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.

These are the configuration files used by the Control Manager server:

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.
ssleay32.dll	Handles the Control Manager security levels.
TMUpdate.dll	Performs ActiveUpdate functions.

CONFIGURATION FILE	DESCRIPTION
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.
CastoolConfiguration.xml	Used by CasTool.exe.
SystemConfiguration.xml	Control Manager system configuration file
CascadingLogConfiguration.xml	Log upload configuration file used for child servers
TMI.cfg	Trend Micro Infrastructure configuration file.
Entity.cfg	Managed product configuration file.

PROCESSES	DESCRIPTION
CasTool.exe	A command line program used to establish a cascading Control Manager environment.
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 management console, into actual commands.
LogReceiver.exe	Receives managed product logs and messages.
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.

Processes	Description
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 management console log on page and manages the Product Directory (Control Manager server-side).
LWDMServer.exe	Manages the Product Directory (client-side — managed products).

Communication and Listening Ports

These are the default Control Manager communication and listening ports.

Type	Communication Port
Internal communication	10198
External communication	10319
Damage Cleanup Services and Vulnerability Assessment communication	20901, 20902

Service	Service Port
ProcessManager.exe	20501
CmdProcessor.exe	20101

SERVICE	SERVICE PORT
UIProcessor.exe	20701
LogReceiver.exe	20201
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
CasProcessor.exe	20801
DcsProcessor.exe	20903

Trend Micro Control Manager Product Features

FEATURES	CONTROL MANAGER			
	3.X ENT	3.X STD	5.0 ADV	5.0 STD
2.x and MCP agent interfaces with the managed products	●	●	●	●
Ad Hoc Query			●	●
Automatic component (for example, patterns/rules) update	●	●	●	●
Cascading management structure	●		●	
Central database for all virus log and system events	●	●	●	●
Centralized, Web-based, virus management solution for the enterprise	●	●	●	●
Child server monitoring	●		●	
Child server task issuance	●		●	
Command Tracking	●	●	●	●
Communicator Heartbeat	●	●	●	●

FEATURES	CONTROL MANAGER			
	3.X ENT	3.X STD	5.0 ADV	5.0 STD
Communicator Scheduler	●	●	●	●
Component download granularity	●	●	●	●
Configuration by group	●	●	●	●
Configure multiple download sources	●	●	●	●
Consistent managed product and Control Manager UI	●	●	●	●
Control Manager MIB files (previously called HP OpenView MIB)	●	●	●	●
Customized user types			●	●
Deployment Plans	●	●	●	●
Directory Manager	●	●	●	●
Enhanced Security Communication	●	●	●	●
Event Center	●	●	●	●
Improved Navigation	●	●	●	●
Improved User Interface	●	●	●	●
InterScan Web Security Service integration	●	●	●	●
Logging Enhancements			●	●
Manage antivirus and content security products	●	●	●	●
Manage services	●	●	●	●
Managed product license manager			●	
Managed product reporting	●		●	
Microsoft SQL Express or Microsoft SQL2005			●	●
MSDE or Microsoft SQL 7/2000	●	●	●	●
MSN Messenger notification	●	●	●	●
Notification and Outbreak Alert	●	●	●	●

FEATURES	CONTROL MANAGER			
	3.X ENT	3.X STD	5.0 ADV	5.0 STD
Outbreak Commander / OPS - Automatic Download and Deployment of OPP	●	●	●	●
Outbreak Commander / OPS - Manual Download and Deployment of OPP	●	●	●	●
Outbreak Commander / Outbreak Prevention Services (OPS)	●	●	●	●
Passive Support for 3rd Party Product	●		●	
Remote and Local Agent Installation	●	●	●	●
Remote management	●	●	●	●
Reporting	●		●	
Secure communication between Server and Agents	●	●	●	●
Single sign-on (SSO) for managed products which support SSO	●	●	●	●
SNMP trap notification			●	
SSL support for ActiveUpdate	●	●	●	●
SSL support for management console	●	●	●	●
Support Control Manager agents 2.x agents	●	●	●	●
Support HTTPS communication between server, agents, and managed products	●	●	●	●
Support MCP agents	●	●	●	●
Supports Trend VCS agents	●	●		
Syslog notification			●	
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	●	●	●	●

Features	**Control Manager**			
	3.X Ent	**3.X Std**	**5.0 Adv**	**5.0 Std**
Trend Micro Product Registration server integration	●	●	●	●
TrendLabs Message Board	●	●	●	●
User account management	●	●	●	●
Vulnerability Assessment	●	●	●	●
Windows Authentication			●	●
Work-hour control	●	●	●	●

Appendix B

Appendix B: Understanding Data Views

Database views are available to Control Manager 5.0 report templates and to Ad Hoc Query requests.

This appendix contains the following sections:

- *Data Views: Product Information* on page B-3
  - *License Information* on page B-3
  - *Managed Product Information* on page B-7
  - *Component Information* on page B-11
  - *Control Manager Information* on page B-16
- *Data View: Security Threat Information* on page B-19
  - *Virus/Malware Information* on page B-20
  - *Spyware/Grayware Information* on page B-34
  - *Content Violation Information* on page B-48
  - *Spam Violation Information* on page B-53
  - *Policy/Rule Violation Information* on page B-57
  - *Web Violation/Reputation Information* on page B-63
  - *Suspicious Threat Information* on page B-71
  - *Overall Threat Information* on page B-83

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

Managed 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. Managed Product License Status Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Service	Displays the name of the managed product service. Example: Vulnerability Assessment, 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.
Activation Code Count	Displays the number of Activation Codes a managed products uses.
License Expiration Date	Displays the date the license expires for the managed product

Managed Product License Information Summary

Displays detailed information about the Activation Code and information on managed products that use the Activation Code. Examples: seat count the Activation Code allows, trial or full product version, user-defined description about the Activation Code

TABLE B-4. Managed 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.
Managed Product/Service Count	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
Managed Product Type	Displays the type of managed product the Activation Code provides. Example: Trial version, Full version
License Expiration Date	Displays the date the license expires for the managed product
Seat Count	Displays the number of seats the Activation Code allows.

Detailed Managed Product License Information

Displays information about the Activation Code and information on managed products which use the Activation Code. Examples: managed product information, evaluation or full product version, license expiration date

TABLE B-5. Detailed Managed Product License Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Service	Displays the name of the managed service. Example: Vulnerability Assessment, Web Reputation Service
License Status	Displays the status of the license for managed products. Example: Activated, Expired, In grace period
Managed 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 Date	Displays the date the license expires for the managed product.
Seat Count	Displays the number of seats the Activation Code allows.
Description	Displays the description for the Activation Code.

Managed Product Information

Managed 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. Managed Product Distribution Summary Data View

DATA	DESCRIPTION
Registered to Control Manager	Displays the Control Manager server to which the managed product is registered.
Managed Product Category	Displays the threat protection category for a managed product. Example: Server-based products, Desktop products
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
Managed Product Count	Displays the total number of a specific managed product a network contains.

Managed 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. Managed Product Status Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Host Name	Displays the name of the server on which the managed product installs.
Managed Product IP Address	Displays the IP address of the server on which the managed product installs.
Managed Product MAC Address	Displays the MAC address of the server on which the managed product installs.
Managing Control Manager Entity Display Name	Displays the entity display name of the Control Manager server to which the managed product is registered.
Managing Server Entity Display Name	Displays the entity display name of the managed product server to which a client is registered.
Domain Name	Displays the domain to which the managed product belongs.
Managed Product Connection Status	Displays the managed product's connection status to Control Manager. Example: Normal, Abnormal, Offline
Pattern File Status	Displays the status of the pattern files/rules the managed product uses. Example: up-to-date, out-of-date
Scan Engine Status	Displays the status of the scan engines the managed product uses. Example: up-to-date, out-of-date

TABLE B-7. Managed Product Status Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Build Number	Displays the build number of the managed product. This information appears on the About screen for products. Example: Version: 5.0 (**Build 1219**)
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
OS Name	Displays the operating system of the computer where the managed product installs.
OS Version	Displays the version number of the operating system of the computer where the managed product installs.
OS Service Pack	Displays the service pack number of the operating system of the computer where the managed product 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
Managed Product Entity Display Name	Displays the entity display name for a managed product.

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

DATA	DESCRIPTION
Domain Name	Displays the domain to which the managed product belongs.
Managed Server/Client Count	Displays the number of managed product servers or managed product clients.
Pattern File Out-of-Date Server/Client	Displays the number of managed product servers/clients with out-of-date pattern files.
Pattern File Up-to-Date Rate (%)	Displays the percentage of managed product servers/clients with up-to-date pattern files.
Scan Engine Out-of-Date Server/Client	Displays the number of managed product servers/clients with out-of-date scan engines.
Scan Engine Up-to-Date Rate (%)	Displays the percentage of managed product servers/clients with up-to-date scan engines.

Managed 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. Managed Product Event Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data about the managed product event.
Time Generated at Entity	Displays the time that the managed product generates data about the event.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE B-9. Managed Product Event Information Data View

DATA	DESCRIPTION
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
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

Managed Product Scan 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. Managed Product Scan Engine Status Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Host Name	Displays the host name of the server on which the managed product installs.
Managed Product IP Address	Displays the IP address of the server on which the managed product installs.

TABLE B-10. Managed Product Scan Engine Status Data View

DATA	DESCRIPTION
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their clients.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
Scan Engine Name	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine
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**
Scan Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Time of Latest Scan Engine Update	Displays the time of the latest scan engine deployment to managed products or clients.

Managed Product Pattern File/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. Managed Product Pattern File/Rule Status Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Host Name	Displays the name of the server on which the managed product installs.
Managed Product IP Address	Displays the IP address of the server on which the managed product installs.
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their clients.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Managed Product Role	Displays the role the managed product has in the network environment. Example: server, client
Pattern File/Rule Name	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Pattern File/Rule Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: **3.203.00**, Anti-spam Pattern: **14256**
Pattern File/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date

TABLE B-11. Managed Product Pattern File/Rule Status Data View

DATA	DESCRIPTION
Time of Latest Pattern File/Rule Update	Displays the time of the latest pattern file/rule deployment to managed products or clients.

Managed 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. Managed Product Component Deployment Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Managed Product Version	Displays the managed product's version number. Example: OfficeScan **8.0**, Control Manager **3.5**
Connection Status	Displays the connection status between the managed product and Control Manager server or managed products and their clients.
Pattern File/Rule Status	Displays the pattern file/rule currency status. Example: up-to-date, out-of-date
Pattern File/Rule Deployment Status	Displays the deployment status for the latest pattern file/rule update. Example: successful, unsuccessful, in progress
Time of Latest Pattern File/Rule Deployment	Displays the time of the latest pattern file/rule deployment to managed products or clients.

TABLE B-12. Managed Product Component Deployment Data View

DATA	DESCRIPTION
Scan Engine Status	Displays the scan engine currency status. Example: up-to-date, out-of-date
Scan Engine Deployment Status	Displays the deployment status for the latest scan update. Example: successful, unsuccessful, in progress
Time of Latest Scan Engine Deployment	Displays the time of the latest scan engine deployment to managed products or clients.

Scan Engine Status Summary

Displays summary information about scan engines managed products use. Examples: scan engine name, scan engine rate, and the number of scan engines out-of-date

TABLE B-13. Scan Engine Status Summary Data View

DATA	DESCRIPTION
Scan Engine Name	Displays the name of the scan engine. Example: Anti-spam Engine (Windows), Virus Scan Engine IA 64 bit Scan Engine
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**
Scan Engines Up-to-Date	Displays the number of managed products with up-to-date scan engines.
Scan Engines Out-of-Date	Displays the number of managed products with out-of-date scan engines.
Scan Engine Up-to-Date Rate (%)	Displays the percentage of managed products with up-to-date scan engines. This includes scan engines that return N/A as a value.

Pattern File/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 File/Rule Name	Displays the name of the pattern file or rule. Example: Virus Pattern File, Anti-spam Pattern
Pattern File/Rule Version	Displays the version of the pattern file or rule. Example: Virus Pattern File: **3.203.00**, Anti-spam Pattern: **14256**
Pattern Files/Rules Up-to-Date	Displays the number of managed products with up-to-date pattern files or rules.
Pattern Files/Rules Out-of-Date	Displays the number of managed products with out-of-date pattern files or rules.
Pattern Files/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
Time of Activity	Displays the time that the activity starts.
Log On User Name	Displays the name of the user who initiates the activity.

TABLE B-15. User Access Information Data View

DATA	DESCRIPTION
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
Activity 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
Time of Event	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
Event 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
Time of Command	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
Issuer of Command	Displays the user who issued the command.
Time of Latest Status Update	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
Time of Command	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
Managed Product Entity Display Name	Displays the managed product to which the command was issued.
Issuer of Command	Displays the user who issued the command.
Command Status	Displays the status of the command: successful, unsuccessful, in progress
Time of Latest Status Update	Displays the time of the latest status check of all commands for the selected Control Manager.
Result Detail Description	Displays the description Control Manager provides for events.

Data View: Security Threat Information

Displays information about security threats that managed products detect: viruses, spyware/grayware, phishing sites, and more.

Virus/Malware Information

Summary Information

Overall Virus/Malware Summary

Provides overall specific summary for virus/malware detections. Example: name of virus/malware, number of clients 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 Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Unique Infection Destination Count	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. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	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. The Unique Infection Source Count equals 2.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

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 Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.
Unique Infection Destination Count	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. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	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. The Unique Infection Source Count equals 2.
Virus/Malware Detection count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Virus/Malware Infection 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 Infection Source Summary Data View

DATA	DESCRIPTION
Infection Source	Displays the IP address/host name of the computer where viruses/malware originate.
Unique Infection Destination Count	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. The Unique Infection Destination Count equals 3.
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Infection Destination Summary

Provides a summary of virus/malware detections from specific clients. Example: name of client, number of specific virus/malware instances on the client, total number of instances of viruses/malware on the network

TABLE B-22. Virus/Malware Infection Destination Summary Data View

DATA	DESCRIPTION
Infection Destination	Displays the IP address/host name of the computer affected by viruses/malware.
Unique Infection Source Count	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. The Unique Infection Source Count equals 2.
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

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 clients 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
Summary Time	Displays the time that the summary of the data occurs.
Unique Virus/Malware Count	Displays the number of unique virus/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.
Unique Infection Destination Count	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. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	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. The Unique Infection Source Count equals 2.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

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
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Unique Infection Destination Count	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. The Unique Infection Destination Count equals 3.
Unique Infection Source Count	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. The Unique Infection Source Count equals 2.
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Detailed Information

Detailed Overall 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 client with viruses/malware

TABLE B-25. Detailed Overall Virus/Malware Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the IP address/host name of the computer affected by viruses/malware.
Infection Source	Displays the IP address/host name of the computer where viruses/malware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects viruses/malware.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required

TABLE B-25. Detailed Overall Virus/Malware Information Data View

DATA	DESCRIPTION
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.
Detected 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

Virus/Malware Found in Hosts Information

Provides specific information about the virus/malware instances found on clients. Example: the managed product that detects the viruses/malware, the type of scan that detects the virus/malware, the file path on the client to detected viruses/malware

TABLE B-26. Virus/Malware Found in Hosts Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.

TABLE B-26. Virus/Malware Found in Hosts Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the name of the computer affected by viruses/malware.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects viruses/malware.
Detecting Scan Type	Displays the type of scan the managed product uses to detect the virus/malware. Example: Real-time, scheduled, manual
Detected File Name	Displays the name of the file managed products detect affected by viruses/malware.
File Path	Displays the file path on the infection destination where managed products detect the virus/malware.
File in Compressed File	Displays the name of the infected file/virus/malware in a compressed file.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE B-26. Virus/Malware Found in Hosts Information Data View

DATA	DESCRIPTION
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Found in HTTP/FTP 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 client that downloads the virus/malware.

TABLE B-27. Virus/Malware Found in HTTP/FTP Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the IP address/host name of the computer on which managed products detect viruses/malware.

TABLE B-27. Virus/Malware Found in HTTP/FTP Information Data View

DATA	DESCRIPTION
Source URL	Displays the URL of the Web/FTP site which the virus/malware originates.
Log On User Name	Displays the log on name of the user with a virus/malware instance.
Inbound/Outbound Traffic/Connection	Displays the direction of virus/malware entry.
Internet Browser/FTP Client	Displays the Internet browser or FTP client where the viruses/malware originates.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Found in Email 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. Virus/Malware Found in Email Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.

TABLE B-28. Virus/Malware Found in Email Information Data View

DATA	DESCRIPTION
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Recipient	Displays the recipient of email message containing viruses/malware.
Sender	Displays the sender of email message containing viruses/malware.
Log On User Name	Displays the log on name of the user with a virus/malware instance.
Email Subject Content	Displays the content of the subject line of the email message containing viruses/malware.
Detected File Name	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.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE B-28. Virus/Malware Found in Email Information Data View

DATA	DESCRIPTION
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Virus/Malware Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Virus/Malware Found in Network Traffic 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. Virus/Malware Found in Network Traffic Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Virus/Malware Name	Displays the name of viruses/malware managed products detect. Example: NIMDA, BLASTER, I_LOVE_YOU.EXE
Infection Destination	Displays the IP address/ host name of the computer affected by viruses/malware.

TABLE B-29. Virus/Malware Found in Network Traffic Information Data View

DATA	DESCRIPTION
Infection Source	Displays the IP address/host name of the computer where viruses/malware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects viruses/malware.
Inbound/Outbound 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
Destination Host Name	Displays the host name of the computer affected by viruses/malware.
Destination Port	Displays the port number of the computer affected by viruses/malware.
Destination MAC Address	Displays the MAC address of the computer affected by viruses/malware.
Source Host Name	Displays the host name of the computer where viruses/malware originates.
Source Port	Displays the port number of the computer where viruses/malware originates.
Source MAC Address	Displays the MAC address of the computer where viruses/malware originates.
Detected File Name	Displays the name of the file managed products detect affected by viruses/malware.
Action Result	Displays the results of the action managed products take against viruses/malware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against viruses/malware. Example: File cleaned, File quarantined, File deleted

TABLE B-29. Virus/Malware Found in Network Traffic Information Data View

DATA	DESCRIPTION
Virus/Malware Detection Count	Displays the total number of viruses/malware managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk Detection Count equals 10, while the Unique Virus/Malware count equals 1.

Spyware/Grayware Information

Summary Information

Overall Spyware/Grayware Summary

Provides overall specific summary for spyware/grayware detections. Example: name of spyware/grayware, number of clients 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 Name	Displays the name of spyware/grayware managed products detect.
Unique Spyware/Grayware Destination Count	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. The Unique Spyware/Grayware Destination Count equals 3.
Unique Spyware/Grayware Source Count	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. The Unique Spyware/Grayware Source Count equals 2.

TABLE B-30. Overall Spyware/Grayware Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Detection Count	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
Spyware/Grayware Source	Displays the name of the computer where spyware/grayware originates.
Unique Spyware/Grayware Destination Count	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. The Unique Spyware/Grayware Destination Count equals 3.
Unique Spyware/Grayware Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

TABLE B-31. Spyware/Grayware Source Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Destination Summary

Provides a summary of spyware/grayware detections from specific clients. Example: name of client, number of specific spyware/grayware instances on the client, total number of instances of spyware/grayware on the network

TABLE B-32. Spyware/Grayware Destination Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Destination	Displays the host name or IP address of the computer affected by spyware/grayware.
Unique Spyware/Grayware Source Count	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. The Unique Spyware/Grayware Source Count equals 2.
Unique Spyware/Grayware Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

TABLE B-32. Spyware/Grayware Destination Summary Data View

DATA	DESCRIPTION
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

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 collected, number of clients 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
Summary Time	Displays the time that the summary of the data occurs.
Unique Spyware/Grayware Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.
Unique Spyware/Grayware Destination Count	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. The Unique Spyware/Grayware Destination Count equals 3.

TABLE B-33. Spyware/Grayware Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Spyware/Grayware Source Count	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. The Unique Spyware/Grayware Source Count equals 2.
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

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
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Unique Spyware/Grayware Destination Count	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. The Unique Spyware/Grayware Destination Count equals 3.

TABLE B-34. Spyware/Grayware Action/Result Summary Data View

DATA	DESCRIPTION
Unique Spyware/Grayware Source Count	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. The Unique Spyware/Grayware Source Count equals 2.
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Detailed Information

Detailed Overall 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 client with spyware/grayware

TABLE B-35. Detailed Overall Spyware/Grayware Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

TABLE B-35. Detailed Overall Spyware/Grayware Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Spyware/Grayware Destination	Displays the name of the computer affected by spyware/grayware.
Spyware/Grayware Source	Displays the name of the computer where spyware/grayware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects spyware/grayware.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.
Detected Entry Type	Displays the entry point for the spyware/grayware that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)

TABLE B-35. Detailed Overall Spyware/Grayware Information Data View

DATA	DESCRIPTION
Detailed Information	Used only for Ad Hoc Queries. Displays detailed information about the selection. In Ad Hoc Queries this column displays the selection as underlined. Clicking the underlined selection displays more information about the selection. Example: Host Details, Network Details, HTTP/FTP Details

Spyware/Grayware Found in Hosts

Provides specific information about the spyware/grayware instances found on clients. Example: the managed product that detects the spyware/grayware, the type of scan that detects the spyware/grayware, the file path on the client to detected spyware/grayware

TABLE B-36. Spyware/Grayware Found in Hosts Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Spyware/Grayware Destination	Displays the computer that is affected by spyware/grayware.

TABLE B-36. Spyware/Grayware Found in Hosts Data View

DATA	DESCRIPTION
Spyware/Grayware Source	Displays the name of the computer where the spyware/grayware originates.
Log On User Name	Displays the user name logged on to the spyware/grayware destination when a managed product detects spyware/grayware.
Detecting Scan Type	Displays the type of scan the managed product uses to detect the spyware/grayware. Example: Real-time, scheduled, manual
Affected Resource	Displays the specific resource affected. Example: application.exe, H Key Local Machine\SOFTWARE\ACME
Affected Resource Type	Displays the type of resource affected by spyware/grayware. Example: registry, memory resource
Spyware/Grayware Risk Type	Displays the specific type of spyware/grayware managed products detect. Example: adware, COOKIE, peer-to-peer application
Spyware/Grayware Risk Level	Displays the Trend Micro-defined level of risk the spyware/grayware poses to your network. Example: High security, Medium security, Low security
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted

Spyware/Grayware Found in HTTP/FTP

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 client that downloads the spyware/grayware

TABLE B-37. Spyware/Grayware Found in HTTP/FTP Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Spyware/Grayware Destination	Displays the IP address/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.
Inbound/Outbound Traffic/Connection	Displays the direction of spyware/grayware entry.
Internet Browser/FTP Client	Displays the Internet browser or FTP client where the spyware/grayware originates.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects spyware/grayware.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required

TABLE B-37. Spyware/Grayware Found in HTTP/FTP Data View

DATA	DESCRIPTION
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Found in Email

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. Spyware/Grayware Found in Email Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.

TABLE B-38. Spyware/Grayware Found in Email Data View

DATA	DESCRIPTION
Recipient	Displays the recipient of email message containing spyware/grayware.
Sender	Displays the sender of email message containing spyware/grayware.
Log On User Name	Displays the user name logged on to the infection destination when a managed product detects spyware/grayware.
Email Subject Content	Displays the content of the subject line of the email message containing spyware/grayware.
Detected File Name	Displays the name of the file managed products detect affected by spyware/grayware.
File in Compressed File	Displays the file name of the spyware/grayware occurring in a compressed file.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

Spyware/Grayware Found in Network Traffic

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. Spyware/Grayware Found in Network Traffic Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spyware/Grayware Name	Displays the name of spyware/grayware managed products detect.
Inbound/Outbound 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
Spyware/Grayware Destination	Displays the IP address/host name of the computer affected by spyware/grayware.
Spyware/Grayware Destination Host Name	Displays the host name of the computer affected by spyware/grayware.
Spyware/Grayware Destination Port	Displays the port number of the computer affected by spyware/grayware.
Spyware/Grayware Destination MAC Address	Displays the MAC address of the computer affected by spyware/grayware.
Spyware/Grayware Source	Displays the IP address/host name of the computer where spyware/grayware originates.

TABLE B-39. Spyware/Grayware Found in Network Traffic Data View

DATA	DESCRIPTION
Spyware/Grayware Source Host Name	Displays the host name of the computer where spyware/grayware originates.
Spyware/Grayware Source Port	Displays the port number of the computer where spyware/grayware originates.
Spyware/Grayware Source MAC Address	Displays the MAC address of the computer where spyware/grayware originates.
Log On User Name	Displays the user name logged on to the spyware/grayware destination when a managed product detects spyware/grayware.
Detected File Name	Displays the name of the file managed products detect affected by spyware/grayware.
Action Result	Displays the results of the action managed products take against spyware/grayware. Example: successful, further action required
Action Taken	Displays the type of action managed products take against spyware/grayware. Example: File cleaned, File quarantined, File deleted
Spyware/Grayware Detection Count	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. The Spyware/Grayware Detection Count equals 10, while the Unique Spyware/Grayware Count equals 1.

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 in Violation	Displays the name of the policy that clients violate.
Filter Type	Displays the type of filter that triggers the violation. Example: content filter, phishing filter, URL reputation filter
Unique Policy Violation Sender Count	Displays the number of unique email message addresses sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. The Unique Policy Violation Sender Count equals 3.
Unique Policy Violation Recipient Count	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. The Unique Policy Violation Recipient Count equals 2.
Policy Violation Detection Count	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. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.

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
Policy Violation Sender	Displays the email message address sending content that violates managed product policies.
Policy Violation Detection Count	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. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.
Unique Policy Violation Recipient Count	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. The Unique Policy Violation Recipient Count equals 2.
Unique Policy in Violation Count	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. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.

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 collected, number of clients 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
Summary Time	Displays the time that the summary of the data occurs.
Unique Policy in Violation Count	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. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.
Unique Policy Violation Sender Count	Displays the number of unique email message addresses sending content that violates managed product policies. Example: A managed product detects 10 violation instances of the same policy coming from 3 computers. The Unique Policy Violation Sender Count equals 3.
Unique Policy Violation Recipient Count	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. The Unique Policy Violation Recipient Count equals 2.
Policy Violation Detection Count	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. The Policy Violation Detection Count equals 10, while the Unique Policy in Violation Count equals 1.

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 Taken	Displays the type of action managed products take against email message in violation of content policies. Example: forwarded, attachments stripped, deleted
Email Count	Displays the number of email messages with the specified action taken by managed products.

Detailed Information

Detailed Overall 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 Overall Content Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.

TABLE B-44. Detailed Overall Content Violation Information Data View

DATA	DESCRIPTION
Managed Product Name	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	Displays the email address sending content that violates managed product policies.
Email Subject Content	Displays the content of the subject line of the email that violates a policy.
Policy in Violation	Displays the name of the policy an email violates.
Policy Settings	Displays the settings for the policy that an email violates.
Detected File Name	Displays the name of the file that violates a policy.
Detecting Filter Type	Displays the type of filter that detects the email in violation. Example: content filter, size filter, attachment filter
Detecting Filter Action	Displays the action the detecting filter takes against email in violation of a policy. Example: clean, quarantine, strip
Action Taken	Displays the type of action managed products take against email in violation of content policies. Example: deliver, strip, forward
Policy Violation Detection Count	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 clients 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 Recipient Count	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. The Unique Recipient Count equals 3.
Spam Violation Detection Count	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. The Spam Violation Detection Count equals 10.

Spam Recipient Summary

Provides a summary of spam violations on specific clients. Example: name of client, total number of instances of viruses/malware on the client

TABLE B-46. Spam Recipient Summary Data View

DATA	DESCRIPTION
Recipient Name	Displays the name of the recipient who receives spam.

TABLE B-46. Spam Recipient Summary Data View

DATA	DESCRIPTION
Spam Violation Detection Count	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. The Spam Violation Detection Count equals 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 collected, number of clients 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 Domain Count	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. The Unique Recipient Domain Count equals 1.
Unique Recipient Count	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. The Unique Recipient Count equals 3.
Spam Violation Detection Count	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. The Spam Violation Detection Count equals 10

Detailed Information

Detailed Overall 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 Overall Spam Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	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.
Email Subject Content	Displays the content of the subject line of the email containing spam.
Policy in Violation	Displays the name of the policy the email violates.
Action Taken	Displays the type of action managed products take against spam found in email. Example: deliver, forward, strip
Spam Violation Detection Count	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. The Spam Violation Detection Count equals 10.

Spam Connection Information

Provides specific information about the spam violations 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
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Spam Source IP Address	Displays the IP address of the mail server where spam originates.
Detecting Filter Type	Displays the type of filter that detects the email in violation. Example: Real-time Blackhole List (RBL+), Quick IP List (QIL)
Action Taken	Displays the type of action managed products take against spam to prevent spam from entering the email server. Example: drop connection, bypass connection
Spam Violation Detection Count	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. The Spam Violation Detection Count equals 10.

Policy/Rule Violation Information

Detailed Information

Detailed Overall Firewall Rule 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 Overall Firewall Rule Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	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
Security Risk Level	Displays the Trend Micro assessment of risk to your network. Example: high security, low security, medium security
Inbound/Outbound Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol the intrusion uses. Example: HTTP, SMTP, FTP
Source IP Address	Displays the IP address of the computer attempting an intrusion on your network.

TABLE B-50. Detailed Overall Firewall Rule Violation Information Data View

DATA	DESCRIPTION
Destination Port	Displays the port number of the computer under attack.
Destination IP Address	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 Taken	Displays the type of action managed products take against policy violations. Example: file cleaned, file quarantined, file passed
Policy/Rule Violation Detection Count	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. The Policy/Rule Violation Detection Count equals 10.

Detailed Overall 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 Overall Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.

TABLE B-51. Detailed Overall Endpoint Security Violation Information Data View

DATA	DESCRIPTION
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Client in Violation	Displays the host name of the computer in violation of the policy/rule.
IP Address of Client in Violation	Displays the IP address of the computer in violation of the policy/rule.
MAC Address of Client in Violation	Displays the MAC address of the computer in violation of the policy/rule.
Policy/Rule in Violation	Displays the name of the policy/rule in violation.
Service in Violation	Displays the name of the service/program in violation of the policy/rule.
Log On User Name	Displays the user name logged on to the client when a managed product detects a policy/rule violation.
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.
Policy/Rule Violation Detection Count	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. The Policy/Rule Violation Detection Count equals 10.

Detailed Overall 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 Overall Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Client in Compliance	Displays the host name of the computer in compliance of the policy/rule.
IP Address of Client in Compliance	Displays the IP address of the computer in compliance of the policy/rule.
MAC Address of Client in Compliance	Displays the MAC address of the computer in compliance of the policy/rule.
Policy/Rule in Compliance	Displays the name of the policy/rule in compliance.
Service in Compliance	Displays the name of the service/program in compliance of the policy/rule.
Log On User Name	Displays the user name logged on to the client when a managed product detects a policy/rule compliance.

TABLE B-52. Detailed Overall Endpoint Security Compliance Information Data View

DATA	DESCRIPTION
Description	Detailed description of the incident by Trend Micro.
Policy/Rule Compliance Detection Count	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. The Policy/Rule Compliance Detection Count equals 10.

Detailed Overall 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 Overall Application Activity Data View

DATA	DESCRIPTION
Time Received from Entity	The time at which Control Manager receives data from the managed product.
Time Generated at Entity	The time at which the managed product generates data.
Managed Product Entity Display Name	The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	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.

TABLE B-53. Detailed Overall Application Activity Data View

DATA	DESCRIPTION
Inbound/Outbound 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.
Host Name of Clients in Compliance	Displays the host name of the computer in compliance of the policy/rule.
Suspicious Threat Source IP Address	Displays the IP address of the source from which the suspicious threat originates.
Suspicious Threat Source MAC Address	Displays the MAC address of the source from which the suspicious threat originates.
Suspicious Threat Source Port	Displays the port number of the source from which the suspicious threat originates.
Source IP Group Name	
Source Network Zone	
Suspicious Threat Destination IP Address	Displays the IP address of the client the suspicious threat affects.
Suspicious Threat Destination Port	Displays the port number of the client the suspicious threat affects.
Suspicious Threat Destination MAC Address	Displays the MAC address of the client the suspicious threat affects.
Destination Group Name	Should this be Destination IP Group Name?
Destination Network Zone	

TABLE B-53. Detailed Overall Application Activity Data View

DATA	DESCRIPTION
Policy/Rule in Violation	Displays the policy/rule the suspicious threat violates.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 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 in Violation	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 Clients in Violation Count	Displays the number of unique clients in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. The Unique Clients in Violation Count equals 4.

TABLE B-54. Overall Web Violation Summary Data View

DATA	DESCRIPTION
Unique URLs in Violation Count	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. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.
Web Violation Detection Count	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. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.

Web Violation Client Host Summary

Provides a summary of Web violation detections from a specific client. Example: IP address of the client in violation, number of policies in violation, the total number of Web violations on the network

TABLE B-55. Web Violation Client IP Address Summary Data View

DATA	DESCRIPTION
Host of Client in Violation	Displays the IP address/host name of clients in violation of Web policies.
Unique Policies in Violation Count	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies in Violation Count equals 1.
Unique URLs in Violation Count	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. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.

TABLE B-55. Web Violation Client IP Address Summary Data View

DATA	DESCRIPTION
Web Violation Detection Count	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. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

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 in Violation	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 Clients in Violation Count	Displays the number of unique clients in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. The Unique Clients in Violation Count equals 4.
Web Violation Detection Count	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. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

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
Web Violation Detection Count	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. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

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 collected, number of clients in violation, the total number of Web violations on the network

TABLE B-58. Web Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.

TABLE B-58. Web Violation Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Policies in Violation Count	Displays the number of the policies in violation. Example: A managed product detects 10 policy violation instances of the same policy on 2 computers. The Unique Policies in Violation Count equals 1.
Unique Clients in Violation Count	Displays the number of unique clients in violation of the specified policy. Example: A managed product detects 10 violation instances of the same URL on 4 computers. The Unique Clients in Violation Count equals 4.
Unique URLs in Violation Count	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. The Web Violation Detection Count equals 10, with the Unique URLs in Violation Count equal to 1.
Web Violation Detection Count	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. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Detailed Information

Detailed Overall 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-59. Detailed Overall Web Violation Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Inbound/Outbound Traffic/Connection	Displays the direction of violation entry.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP
URL in Violation	Displays the name of the URL that violates a Web policy.
Client Host	Displays the IP address/host name of the client that violates a policy.
Filter/Blocking Type	Displays the type of filter/blocking preventing access to the URL in violation. Example: URL blocking, URL filtering, Web blocking
Policy in Violation	Displays the name of the policy the URL violates.

TABLE B-59. Detailed Overall Web Violation Information Data View

DATA	DESCRIPTION
File in Violation	Displays the name of the file that violates the policy.
Web Reputation Rating	Displays the relative safety, as a percentage, of a Web site according to Trend Micro.
Action Taken	Displays the type of action managed products take against policy violations. Example: pass, block
Web Violation Detection Count	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. The Web Violation Detection Count equals 10, with the URLs in Violation Count equals 1.

Detailed Overall Web Reputation Service Information

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-60. Detailed Overall Web Reputation Service Information Data View

DATA	DESCRIPTION
Time Received from Entity	The time at which Control Manager receives data from the managed product.
Time Generated at Entity	The time at which the managed product generates data.
Managed Product Entity Display Name	The entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	The name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE B-60. Detailed Overall Web Reputation Service Information Data View

DATA	DESCRIPTION
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.
Inbound/Outbound 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.
Host Name of Clients in Compliance	Displays the host name of the computer in compliance of the policy/rule.
Suspicious Threat Source IP Address	Displays the IP address of the source from which the suspicious threat originates.
Suspicious Threat Source MAC Address	Displays the MAC address of the source from which the suspicious threat originates.
Suspicious Threat Source Port	Displays the port number of the source from which the suspicious threat originates.
Source IP Group Name	
Source Network Zone	
Suspicious Threat Destination IP Address	Displays the IP address of the client the suspicious threat affects.
Suspicious Threat Destination Port	Displays the port number of the client the suspicious threat affects.

TABLE B-60. Detailed Overall Web Reputation Service Information Data View

DATA	DESCRIPTION
Suspicious Threat Destination MAC Address	Displays the MAC address of the client the suspicious threat affects.
Destination Group Name	Should this be Destination IP Group Name?
Destination Network Zone	
Policy/Rule in Violation	Displays the policy/rule the suspicious threat violates.
URL in Violation	Displays the URL considered a suspicious threat.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Information

Summary Information

Overall Suspicious Threat Summary

Provides specific information about suspicious threats on your network. Example: the rule/violation in violation, summary information about the source and destination, the total number of suspicious threats on the network

TABLE B-61. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Policy/Rule in Violation	Displays the name of the policy/rule in violation.
Protocol	Displays the protocol over which the violation takes place. Example: HTTP, FTP, SMTP

TABLE B-61. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Unique Suspicious Threat Destination Count	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. The Unique Suspicious Threat Destination Count equals 2.
Unique Suspicious Threat Source Count	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. The Unique Suspicious Threat Source Count equals 3.
Unique Suspicious Threat Recipient Count	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. The Unique Suspicious Threat Recipient Count equals 2.
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. 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. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.
Mitigation Count	Displays the number of clients Network VirusWall Enforcer devices or Total Discovery Mitigation Server take action against.

TABLE B-61. Overall Suspicious Threat Summary Data View

DATA	DESCRIPTION
Cleaned Client Count	Displays the total number of clients Total Discovery Mitigation Server cleans.
Clean Client Rate (%)	Displays the percentage of clients Total Discovery Mitigation Server cleans compared to the total Suspicious Threat Violation Detection Count.

Suspicious Threat 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-62. Suspicious Threat Source Summary Data View

DATA	DESCRIPTION
Suspicious Threat Source IP Address	Displays the IP addresses of sources where suspicious threats originate.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. 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. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Destination Count	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. The Unique Suspicious Threat Destination Count equals 2.

TABLE B-62. Suspicious Threat Source Summary Data View

DATA	DESCRIPTION
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat Riskiest Destination Summary

Provides a summary of the clients 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-63. Suspicious Threat Riskiest Destination Summary Data View

DATA	DESCRIPTION
Suspicious Threat Destination IP Address	Displays the IP addresses of computers affected by suspicious threats.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. 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. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Source Count	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. The Unique Suspicious Threat Source Count equals 3.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat 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-64. Suspicious Threat Riskiest Recipient Summary Data View

DATA	DESCRIPTION
Suspicious Threat Recipient	Displays the email address of the recipient affected by the suspicious threat.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. 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. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. 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. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.

Suspicious Threat 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-65. Suspicious Threat Sender Summary Data View

DATA	DESCRIPTION
Suspicious Threat Sender	Displays the email address for the source of policy/rule violations.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. 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. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Recipient Count	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. The Unique Suspicious Threat Recipient Count equals 2.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 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-66. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Protocol Name	Displays the name of the protocol over which the suspicious threat occurs. Example: HTTP, FTP, SMTP
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. 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. The Unique Policies/Rules in Violation Count equals 1.
Unique Suspicious Threat Destination Count	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. The Unique Suspicious Threat Destination Count equals 2.
Unique Suspicious Threat Source Count	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. The Unique Suspicious Threat Source Count equals 3.
Unique Suspicious Threat Recipient Count	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. The Unique Suspicious Threat Recipient Count equals 2.

TABLE B-66. Suspicious Threat Protocol Detection Summary Data View

DATA	DESCRIPTION
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. 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. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 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 collected, summary information about the source and destination, the total number of suspicious threats on the network

TABLE B-67. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Summary Time	Displays the time that the summary of the data occurs.
Unique Policies/Rules in Violation Count	The number of policies/rules the source computer violates. 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. The Unique Policies/Rules in Violation Count equals 1.

TABLE B-67. Suspicious Threat Detection Over Time Summary Data View

DATA	DESCRIPTION
Unique Suspicious Threat Destination Count	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. The Unique Suspicious Threat Destination Count equals 2.
Unique Suspicious Threat Source Count	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. The Unique Suspicious Threat Source Count equals 3.
Unique Suspicious Threat Recipient Count	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. The Unique Suspicious Threat Recipient Count equals 2.
Unique Suspicious Threat Sender Count	Displays the number of unique where suspicious threats e. 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. The Unique Suspicious Threat Sender Count equals 3.
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.

Detailed Information

Detailed Overall 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-68. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Time Received from Entity	Displays the time that Control Manager receives data from the managed product.
Time Generated at Entity	Displays the time that the managed product generates data.
Managed Product Entity Display Name	Displays the entity display name for a managed product. Control Manager identifies managed products using the managed product's entity display name.
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange
Mitigation Server Entity Display Name	Displays the entity display name for the mitigation server. Control Manager identifies managed products using the managed product's entity display name.
Inbound/Outbound 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-68. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Suspicious Threat Destination IP Address	Displays the IP address of the client the suspicious threat affects.
Suspicious Threat Destination Port	Displays the port number of the client the suspicious threat affects.
Suspicious Threat Destination MAC Address	Displays the MAC address of the client the suspicious threat affects.
Suspicious Threat Source IP Address	Displays the IP address of the source where the suspicious threat originates.
Suspicious Threat Source Host Name	Displays the host name of the source where the suspicious threat originates.
Suspicious Threat Source Port	Displays the port number of the source where the suspicious threat originates.
Suspicious Threat Source MAC Address	Displays the MAC address of the source where the suspicious threat originates.
Domain Name	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.
Risk Type	Displays the specific type of security risk 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 in Violation	Displays the policy/rule the suspicious threat violates.
Recipient	Displays the recipient of the suspicious threat.
Sender	Displays the sender of the suspicious threat.

TABLE B-68. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Email Subject Content	Displays the content of the subject line of the email containing spyware/grayware.
URL in Violation	Displays the URL considered a suspicious threat.
Log On User Name	Displays the user name logged on to the destination when a managed product detects a suspicious threat.
Instant Messaging/IRC User Name	Displays the instant messaging or IRC user name logged on when Total Discovery Appliance detects a violation.
Internet Browser/FTP Client	Displays the Internet browser or FTP client where the suspicious threat originates.
Channel Name	Displays the protocol that the instant messaging software or IRC use for communication.
File Name of Suspicious File	Displays the name of the suspicious file.
Suspicious 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.

TABLE B-68. Detailed Overall Suspicious Threat Information Data View

DATA	DESCRIPTION
Constraint Type	Displays the reason that a file cannot be scanned correctly.
Mitigation Result Description	Displays the result of the action the mitigation server takes against suspicious threats.
Mitigation Action Taken	Displays the action the mitigation server takes against suspicious threats. Example: File cleaned, File dropped, File deleted
Suspicious Threat Violation Detection Count	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. The Suspicious Threat Violation Detection Count equals 10.

Overall Threat Information

Complete Network Security Risk Analysis Information

Displays information for overall security risks affecting your desktops. Examples: name of the security risk, total number of security risk detections, number of clients affected

TABLE B-69. Complete Network Security Risk Analysis Information Data View

DATA	DESCRIPTION
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Security Risk Name	Displays the name of security risk managed products detect.
Detected Entry Type	Displays the entry point for the security risk that managed products detect. Example: virus found in file, HTTP, Windows Live Messenger (MSN)

TABLE B-69. Complete Network Security Risk Analysis Information Data View

DATA	DESCRIPTION
Unique Security Risk/Violation Destination Count	Displays the number of unique computers affected by the security risk/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Destination Count equals 2.
Unique Security Risk/Violation Source Count	Displays the number of unique computers where security risks/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Source Count equals 3.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Network Protection Boundary Information

Displays information for a broad overview of security risks affecting your entire network. Examples: managed product network protection type (gateway, email), type of security risk, number of clients affected

TABLE B-70. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Managed Product Category	Displays the category to which the managed product belongs. Example: desktop products, mail server products, network products
Managed Product Name	Displays the name of the managed product. Example: OfficeScan, ScanMail for Microsoft Exchange

TABLE B-70. Network Protection Boundary Information Data View

DATA	DESCRIPTION
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Unique Security Risk/Violation Destination Count	Displays the number of unique computers affected by the security risk/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Destination Count equals 2.
Unique Security Risk/Violation Source Count	Displays the number of unique computers where security risks/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Source Count equals 3.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Security Risk Entry Point Analysis Information

Displays information with the entry point of security risks as the focus. Examples: managed product network protection type (gateway, email, desktop), name of the security risk, time of the last security risk detection

TABLE B-71. Security Risk Entry Point Analysis Information Data View

DATA	DESCRIPTION
Detected Entry Type	Displays the point of entry for security risks managed products detect. Example: Virus found in file, FTP, File transfer

TABLE B-71. Security Risk Entry Point Analysis Information Data View

DATA	DESCRIPTION
Managed Product Name	Displays the name of the managed product which detects the security risk. Example: OfficeScan, ScanMail for Microsoft Exchange
Security Risk Category	Displays the specific category for security risks managed products detect. Example: Antivirus, Anti-spyware, Content filtering
Unique Security Risk/Violation Destination Count	Displays the number of unique computers affected by the security risk/violation. Example: OfficeScan detects 10 virus instances of the same virus on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Destination Count equals 2.
Unique Security Risk/Violation Source Count	Displays the number of unique computers where security risks/violations originate. Example: OfficeScan detects 10 virus instances of the same virus, coming from 3 sources, on 2 computers. The Security Risk/Violation Detection Count equals 10, while the Unique Security Risk/Violation Source Count equals 3.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10, while the Unique Virus/Malware Count equals 1.

Security Risk Destination Analysis Information

Displays information with affected clients as the focus. Examples: name of the client, the broad range of how the security risk enters your network, number of clients affected

TABLE B-72. Security Risk Destination Analysis Information Data View

DATA	DESCRIPTION
Security Risk/Violation Destination	Displays the name of computers affected by the security risk/violation.
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Security Risk Name	Displays the name of security risk managed products detect.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10.
Time of Latest Infection/Violation	Displays the time and date of the last security risk/violation detection on the computer affected the security risk/violation.

Security Risk Source Analysis Information

Displays information with the security risk source as the focus. Examples: name of the security risk source, the broad range of how the security risk enters your network, number of clients affected

TABLE B-73. Security Risk Source Analysis Information Data View

DATA	DESCRIPTION
Security Risk/Violation Source	Displays the name of the computer where the cause of the security risk/violation originates.

TABLE B-73. Security Risk Source Analysis Information Data View

DATA	DESCRIPTION
Security Risk Category	Displays the broad category of the security risk managed products detect. Example: Antivirus, Anti-spyware, Anti-phishing
Security Risk Name	Displays the name of security risk managed products detect.
Security Risk/Violation Detection Count	Displays the total number of security risks/violations managed products detect. Example: OfficeScan detects 10 virus instances of the same virus on one computer. The Security Risk/Violation Detection Count equals 10.
Time of Latest Infection/Violation	Displays the time and date of the last security risk/violation detection on the computer affected the security risk/violation.

Index

Symbols

"Log on as batch job" policy 5-63

A

access rights
- setting 5-15

account types
- adding 5-11
- editing 5-13
- understanding 5-8

activating
- Control Manager 3-24–3-25
- Outbreak Prevention Services 3-11

activating Control Manager 3-25

Activation Code 3-25

Ad Hoc Query 6-30
- shared 6-39

adding
- account types 5-11
- user accounts 5-16
- user groups 5-22

address, checklist A-2

Administrator's Guide P-vi
- about P-vii

AG. See Administrator's Guide

agent
- installation
  - checklist A-4

Agent Migration Tool 9-2
- migrating agents 9-2

AgentMigrateTool.exe. See Agent Migration Tool

agents
- removing Windows-based 10-7

audience P-viii

Automatic Deployment
- configuring 5-44

automatic deployment settings
- Scheduled Download 5-56

B

back up. See backing up Control Manager 2.5/3.0 information

C

cascading management structure
- feature comparison 5-31

checklist
- agent installation A-4
- ports A-3
- server address A-2

child Control Manager server
- unregister 5-35

child server 7-52

child servers
- configuring 5-31
- managing 5-30, 7-50
- registering 5-32, 7-53
- unregistering 7-53

client logs 6-24

command polling
- MCP 2-16

command prompt
- Control Manager, stopping service from 10-4

Command Tracking 6-3
- query and view commands 6-5

communication
- one-way 1-6
- parent-child server 7-52
- two-way 1-6, 7-19

comparison
- cascading management structure 5-31

components
- downloading 5-35

configuration
- Web server 2-20

configuring 5-43, 5-54
- child servers 5-31
- managed products 7-29
- Manual Download and Automatic Deployment settings 5-44
- Outbreak Prevention Mode download settings 8-16
- Scheduled Download
  - automatic deployment settings 5-56
- Scheduled Download Exceptions 5-45

Scheduled Download Settings 5-55
Scheduled Downloads 5-47
user accounts 3-24, 5-7
Control Manager 1-1
accounts 5-7
activating 3-24–3-25
Administrator's Guide P-vi
agent 1-8
antivirus and content security components 5-35
architecture 1-7
basic features 1-2
child servers 7-50
command prompt, stopping service from 10-4
configuring accounts 5-7
installation steps 3-5
installing 3-1, 3-6
latest documentation P-vii
mail server 1-7
managed product 5-26, 7-20
management console 5-2
manually removing 10-2
MCP 1-8
migrating database 4-17
notifications 6-13
PDF documentation P-vii
registering 3-24–3-25
remove manually 10-3
removing overview 10-1
removing server 10-2
removing Windows-based agent 10-7
report server 1-7
report types 6-47
security levels 3-13, 3-15
server 1-7
SQL database 1-7
supported operating systems 2-9
system requirements 3-2
testing pilot deployment 2-10
Trend Micro Infrastructure 1-8
verifying installation 3-22
Web server 1-7
Web-based management console 1-8
Control Manager 2.5x agent migration flow 4-14
Control Manager agents
supported operating systems 2-10
Control Manager antivirus and content security components
Anti-spam rules 5-35
Engines 5-35
Pattern files/Cleanup templates 5-35
convention
document P-ix
convert
full version 3-26
creating
folders 7-40
user groups 5-22
users 5-16
customizing
notification messages 6-11

D

data storage
plan 2-19
data views
product information B-3
security threat information B-19
understanding 6-29
database
recommendations 2-19
deleting
logs 6-44
user accounts 5-22
user groups 5-25
deployment
architecture and strategy 2-2
multiple-site 2-5
single-site 2-2
Directory Manager 5-27, 7-22, 7-37
grouping managed products 5-27, 7-22
disable notifications 6-14
disabling
user accounts 5-22
documentation P-vi
download components
manually 5-37
downloading and deploying components 5-35

E

editing

- Outbreak Prevention policies 8-13
- user accounts 5-21
- user groups 5-25

email 6-13
enable notifications 6-14
enable Scheduled Component Downloads 5-47
Enterprise Protection Strategy 8-3
evaluating existing policies 8-19
Event Center 6-8
- Alert 6-8
- Outbreak Prevention Services 6-8
- Unusual 6-9
- Update 6-9

F

firewall traversal support 1-5
flow
- migrating Control Manager 2.5x agent 4-14
- migrating MCP agents 4-15

folders
- creating 7-40
- moving 7-41
- renaming 7-40

full version
- convert 3-26

H

heartbeat
- MCP 2-16
- TMI 2-14

I

installation P-vii
- flow 2-9

Installation Guide P-vi
installation steps
- Control Manager 3-5

installing
- Control Manager 3-1, 3-6
- steps 3-5
- verifying Control Manager server 3-22

K

Knowledge Base P-vi
- URL P-vi

L

logs 6-23
- Ad Hoc Queries 6-30
- aggregation 6-27
- deleting 6-44
- traffic 2-15

M

Main menu 5-2
managed products
- configuring 7-29
- default folder 5-30, 7-24
- issue tasks 7-29
- moving 7-41
- recovering 7-35
- renaming 7-40
- searching for 7-36
- support P-iv
- viewing logs 7-30
- viewing status 7-28

management console
- access 5-4
- access HTTPS 5-6
- accessing locally 5-4
- accessing remotely 5-4
- assigning HTTPS 5-5
- function-locking mechanism 5-3

managing
- child servers 7-50

manual
- remove
  - MSDE 10-7

Manual Download 5-43
manual download
- configuring settings 5-43

manual download settings 5-43
manually
- remove Control Manager 10-3

manually download components 5-37
manually uninstalling 10-2
MCP 1-8
- command polling 2-16
- heartbeat 2-16
- migration flow 4-15
- policies 2-16

understanding 1-3
verifying communication method 7-19
MCP benefits
HTTPS support 1-5
NAT and firewall traversal 1-5
one-way and two-way communication 1-6
reduced network loading and package size 1-4
menu
Main 5-2
MIB file
Control Manager 9-2
NVW 1.x SNMPv2 9-3
NVW Enforcer SNMPv2 9-3
MIBs browser 6-13
migrating 4-11
Control Manager 2.5x agent migration flow 4-14
Control Manager SQL 2000 4-17
database 4-17
different servers/agents 4-13
MCP agents 4-15
phased upgrade 4-12
rapid upgrade 4-11
scenarios 4-13
single-server migration 4-13
steps 4-15
strategy 4-11
Trend VCS, Control Manager 2.x, and MCP Agents 4-15
minimum system requirements 3-2
modifying
account types 5-13
moving
folders 7-41
managed products 7-41
multiple-site deployment
understanding 2-5

N

NAT traversal support 1-5
network traffic
sources 2-15
network traffic plan 2-13
notification messages
customizing 6-11
notifications 6-13
configure recipients 6-17
configuring 6-15
enabling or disabling 6-14
special virus alert settings 6-20
test notification delivery 6-17
virus outbreak alert settings 6-19
NVW 1.x Rescue Utility 9-4
NVW System Log Viewer 9-4

O

ODBC
settings, Control Manager 10-7
one-way communication 1-6
online help P-vi
operating systems
supported 2-9
Outbreak Prevention Mode 8-9
configuring download settings 8-16
setting automatic 8-14
starting 8-12
stopping 8-16
viewing history 8-17
Outbreak Prevention policies
editing 8-13
policies
Outbreak Prevention 8-10
updating 8-11
Outbreak Prevention Services 8-6
accessing 8-10
activating 3-11, 8-7
benefits 8-7
viewing status 8-8
outbreaks
identify the source 8-18

P

pager 6-13
parent and child server feature comparison 5-31
parent server 7-52
phased upgrade 4-12
pilot deployment
testing 2-10
policies
MCP 2-16
TMI 2-16

port
- checklist A-3

post installation P-viii
preface P-i
pre-installation P-vii
Product Directory
- deploying components 7-27

product registration
- traffic 2-17

Q

querying commands 6-5

R

rapid upgrade 4-11
readme file P-vi
recommendations
- database 2-19

recommended system requirements 3-4
recovering
- managed products 7-35

registering
- child servers 7-53
- Control Manager 3-24–3-25

registering a child server 5-32
Registration Key 3-11, 3-26
remove
- manual
  - Control Manager 10-3
  - Microsoft Data Engine 10-7

removing
- Control Manager manually 10-2
- Control Manager server 10-2
- Control Manager Windows-based agent 10-7

renaming
- folders 7-40
- managed products 7-40

renew product maintenance 3-26
report maintenance 6-85
report templates 6-47
reports 6-47
- create report templates 6-57
- deleting 6-85
- one-time reports 6-71
- scheduled reports 6-77
- templates 6-47
- viewing reports 6-84

re-verification frequency
- changing 7-36

rolling back
- to Control Manager 3.0/3.5 server 4-10

root account 5-11

S

Scheduled Download
- configuring
  - automatic deployment settings 5-56

Scheduled Download Exceptions
- configuring 5-45

Scheduled Download Frequency
- configuring 5-54

Scheduled Download Schedule
- configuring 5-54

Scheduled Download Schedule and Frequency 5-54
Scheduled Download Settings
- configuring settings 5-55

Scheduled Downloads 5-46
- configuring 5-47

searching
- managed products 7-36

security levels 3-14
server
- address, checklist A-2

server distribution plan 2-12
server logs 6-24
setting
- access rights 5-15

shared
- Ad Hoc Queries 6-39

single-site deployment
- understanding 2-2

Small Network Management Protocol. See SNMP
SNMP 6-13
SolutionBank-see Knowledge Base P-vi
spyware/grayware
- special alert settings 6-21

SSO 1-7
starting
- Outbreak Prevention Mode 8-12

stopping

Outbreak Prevention Mode 8-16
system requirements 3-2
minimum 3-2
recommended 3-4

T

TMI
heartbeat 2-14
policies 2-16
tool
AgentMigrateTool.exe 9-2
Control Manager MIB file 9-2
NVW 1.x Rescue Utility 9-4
NVW 1.x SNMPv2 MIB file 9-3
NVW Enforcer SNMPv2 MIB file 9-3
NVW System Log Viewer 9-4
traffic, network 2-13
traversal support
NAT and firewall 1-5
Trend Micro services 8-2
Trigger Application 6-14
Tutorial P-vi
two-way communication 1-6, 7-19

U

understanding
multiple-site deployment 2-5
single-site deployment 2-2
unregister
child Control Manager servers 5-35
unregistering
child servers 7-53
updates
deploying 2-18
updating
Outbreak Prevention policies 8-11
Upgrading 4-2
upgrading 4-2
backing up Control Manager information 4-7
considerations 4-2
Control Manager servers 4-2
URLs
Knowledge Base P-vi
user account
Access 5-8
user accounts
adding 5-16
configuring 3-24
deleting 5-22
disabling 5-22
editing 5-21
user groups
adding 5-22
deleting 5-25
editing 5-25
users
adding accounts 5-16
adding groups 5-22
deleting accounts 5-22
deleting groups 5-25
disabling accounts 5-22
editing accounts 5-21
editing groups 5-25

V

verifying
communication method between MCP and Control Manager 7-19
Control Manager server installation 3-22
viewing
managed products logs 7-30
managed products status 7-28
Outbreak Prevention Mode history 8-17
Outbreak Prevention Services status 8-8
viewing commands 6-5

W

Web server
configuration 2-20
plan 2-20
who should read this document
audience P-viii
Windows event log 6-13
World Virus Tracking 3-12
World Virus Tracking Program 8-5